ProScan

ANTIVIRUS

ProScan for Mail Server バージョン6.0.5

管理者ガイド

promark

株式会社プロマーク

2021年3月　第23版

目次

第1章 ProScan® for Mail Serverの概要

ProScan® for Mail Server (以降、「**ProScan®**」と表記) は、サーバーを経由するメール トラフィックとサーバーのファイル システムに対してウイルス チェックを行います。Linux、FreeBSDのいずれかのOSとsendmail（含むLibmilter）、Postfix（含むmilter）、qmailのいずれかのメール プログラムを搭載したサーバに対応します。

この製品の機能は次のとおりです。

- マウントされているすべてのファイル システム、および送受信されるメールのウイルス チェックを行います (メールはサーバーのSMTPトラフィックの一部として扱われます)。
- 感染ファイル、感染の疑いがあるファイル、破損しているファイル、パスワードで保護されているファイル、エラーのためウイルス チェックできないファイルを検知します。
- ファイル システムおよびメールの感染オブジェクトからウイルスを駆除します。(駆除可能な場合のみ)
- サーバーのファイル システムおよびメールで検知された感染オブジェクト、感染の疑いがあるオブジェクト、および破損しているオブジェクトをすべて検疫ディレクトリに移動します。ウイルスを駆除したファイル、パスワードで保護されているファイル、エラーのためウイルス チェックできないファイルも検疫場所に移動できます。.
- 送信者と受信者のグループにあらかじめ設定されたルールに従ってメールを処理します。
- 添付オブジェクトの名前とタイプに基づいて、メールの二次フィルタリングを行い、個別のルールに基づいてフィルタリングしたオブジェクトを処理します。
- 感染オブジェクトや感染の疑いがあるオブジェクトが添付されたメールの情報を、その送信者、受信者、グループ管理者に通知することが可能です。
- ProScan®のモジュール、エンジン、ウイルス データベースを更新することができます。更新ファイルは、株式会社プロマークの更新用サーバーからダウンロードされ自動で反映されます。（自動反映を停止することも可能です。）

  このウイルス データベースは、感染オブジェクトの検知に使用します。ウイルス チェックを行うと、ウイルス データベースの内容に基づいて、各ファイルがウイルスに感染していないかどうか分析すると同時に、ウイルス固有のコードと各ファイルのコードを比較します。

  新種のウイルスは毎日のように発生します。ウイルス データベースを毎日更新し、常に最新の状態にしておくことをお勧めします。
- オプションでアンチスパム機能を利用することも可能です。

  アンチスパム判定は、S25R方式をメインに、RBL、ホワイト&ブラックリスト、グレイチェック機能を有しています。

1.1. ProScan®のモジュール

ProScan®は以下の6つのモジュールから構成されています。

- **proscan**

  ProScanのランチャです。ウイルスチェックエンジン（savapi）の起動を行います。
- **savapi**

  ウイルスチェックエンジンです。proscanms,proscanfsがソケット接続によりウイルスデータベースを検索して、メールまたはファイルのチェックを行います。(ドイツAvira社よりOEM提供を受けています。)
- **proscanms(qmail-queue),proscanlm**

  メールスキャナです。メール本文や添付されているファイルのウイルスをスキャンを行います。MTAの種類によりフロントエンドが異なります。qmail用はqmail-queue、milter用はproscanlmを利用します。
- **proscanfs**

  ファイルスキャナです。ローカルファイルシステムのファイルをスキャンします。コマンドラインで呼び出して使用します。
- **proscanup**

ウイルスパターンデータベースの更新及びProScanモジュールの更新を行います。弊社サイトに接続し、更新ファイルがあればダウンロードし、アップデートを行います。

1.2. ライセンス ポリシー

ProScan®は、次の項目を条件としたライセンスを用意しています。

- **製品使用期間** (通常は購入日から1年間)
- **ユーザー** (Eメール アドレス) **の数**
- **ドメイン**（Eメール アドレスの@以降）**の数**

ライセンスは、上記すべての項目の組み合わせとなります。ユーザ数、ドメイン数を無制限としたオープンライセンスも用意しております。

1.3. ハードウェアとソフトウェアの要件

ProScan®を使用するには、次の要件を満たすシステムが必要です。

・ハードウェア要件：

- 64bit IA版CPU 1.6GHz以上
- 1GB以上のRAM
- 1GB以上のHDD空き容量

・ソフトウェア要件：

- 次のいずれかのOS：
  - glibc-2.4以上を有するLinux
  - FreeBSDバージョン10.3以上
- メール システム (sendmailバージョン8.11以降：Libmilterを利用する場合には8.14以降、qmailバージョン1.03、Postfixバージョン2.1以降：milter版を利用する場合には2.3以降、のいずれか)
- wgetプログラム (http://gnu.org/software/wget/wget.html) — proscanupを使ったウイルス データベースの更新に必要。

1.4. 配布キット

ProScan®は、弊社の販売代理店経由または弊社よりご購入いただけます。

基本的にはダウンロード販売のみで、お客様にダウンロードして頂き、ご自身でインストールして頂きます。ダウンロードサイト（http://www.promark-inc.com/proscan/download.html）からのパッケージは標準で1ヶ月（30日）間の評価ライセンス（5ドメイン25ユーザ）を同梱しています。評価の後、正規ライセンスキーをご購入頂き製品版と同様にご利用いただけます。(評価中の機能制限はございません。)

正規ライセンスご購入後は以下のものを弊社よりお送りいたします。

- 管理者ガイド
- ライセンス キー
- ライセンス証書
- ソフトウェア使用権許諾契約書

1.4.1. ライセンス契約

本ライセンス契約 (LA) は、お客様 (個人または法人) と製造元 (株式会社プロマーク) との間で、お客様が購入したウイルス対策製品の使用条件について締結するものです。

ライセンス契約の条件を必ずお読み下さい。

本契約の条件に同意しない場合は、㈱プロマークから本ソフトウェア製品のライセンスが供与されません。

ソフトウェアのインストールを行うと、お客様は本契約条件に同意したとみなされます。

1.4.2. オプションライセンスについて

ProScanのオプション機能（アンチスパム）を利用するには、オプションライセンスが必要となります。オプションライセンスもライセンスキーファイルの形態で提供されます。別途、ご購入ください。（ダウンロードパッケージにはオプションライセンスの評価キーも同梱しています。）

1.5. ご購入ユーザー様用のヘルプ デスク

プロマークでは、本ソフトウエアをご購入頂いた方にProScan®を最大限に活用いただけるようさまざまなサービス パッケージを用意しております。

ご購入頂いた方は、契約期間中、次のサービスをご利用いただけます。

- インターネット経由でのウイルス データベース更新
- 製品アップグレード サービス
- ソフトウェアのインストール、構成、および使用法に関するEメールでのサポート
- プロマークの新製品および新種のコンピュータ ウイルスに関する情報の入手 (弊社のニュースレターの購読をお申し込みの場合のみ)

弊社サポートでは、OSや弊社製品以外の各種技術の操作や使用法についてはお答えできません。

1.6. 本書の表記について

本書では、重要な部分を強調するために、次の表記を使用しています。

表記	意味
太字	メニュー名、コマンド、ウィンドウ名、ダイアログ ボックスの要素など
 メモ	補足情報、注意事項など
 注意	きわめて重要な情報
 **操作手順** 1. ステップ1 2. …	実行すべきアクション
 **課題**	このプログラムを使用するタスクの例
 **解決方法**	タスクを解決するための手順
[**スイッチ**] — スイッチの機能	コマンド ライン スイッチ
`Info message text`	構成ファイルのテキスト、およびProScan®で表示される情報メール

第2章 ProScan®の代表的な導入パターン

メール サーバーの元のアーキテクチャの種類に応じて、ProScan® を導入するパターンを選択できます。

- **メール システムが動作している単独のメール サーバーに導入するパターン。**サーバーにメール システム (sendmail、qmail、Postfix) をインストール・設定している場合に適しています (6ページの2.2を参照)。
- **専用サーバーに二次フィルタとして導入するパターン。**プライマリ メール サーバーに、本製品がサポートしていないOSとメール システムを稼動させている場合に適しています (8ページの2.4を参照)。
- **メール システムが動作している単独のサーバーに二次フィルタとして導入するパターン。**メール サーバーにProScan® Anti-Spamなどのメール フィルタリング ツールをインストールしている場合に適しています (7ページの2.3を参照)。

どのパターンで導入しても、メールをフィルタリングできるだけでなく、マウントされているすべてのファイル システムのウイルス チェックを行えます。

次に、それぞれの導入パターンについて説明する前に、ProScan®の動作アルゴリズムを理解できるよう、その内部アーキテクチャについて解説します。

2.1. ProScan®の内部アーキテクチャ

ProScan®を使用するには、その動作アルゴリズムを理解しておくことが重要です。

ここでは、ProScan®の内部アーキテクチャについて解説します。サーバーのファイル システムのウイルス チェックはきわめてシンプルであるため、メールのウイルスをチェックするアーキテクチャに焦点を当てます。

ProScan®は、メールのウイルス チェックを行い、フィルタリングすることだけを目的として開発されています。メールの受信とルーティングを行うメール エージェントとしての機能は備えていません。メール エージェント機能は、サーバーにインストールされたメール システムが行います。ProScan®は、インストールするとメール システムと統合します。

ここではsendmailメール システムを例に挙げ、sendmailと統合されたProScan® Anti-Virus for Mail Serverの内部的な動作アルゴリズムについて詳しく説明します (図1を参照)。

ProScan®をsendmailメール システムと統合すると、**sendmail.cf.listen**という構成ファイルが新たに作成されます。この構成ファイルを使ってsendmailを起動すると、sendmailは受信したメールをProScan®に渡し、ProScan®がこのウイルス チェックを行います。一方、元の構成ファイル (sendmail.cf) を使用してsendmailを起動すると、ProScan®が先にウイルス チェックを行ったメールを受信し、配信します。

つまり、動作アルゴリズムは次のようになります。

1. sendmailが、SMTPプロトコルを使用してメールを受信します (構成ファイルは**sendmail.cf.listen**)。sendmailはキューを作成して受信メールをこの中に格納し、ウイルス チェックを行うため、LMTPプロトコルを使用してこのメールをproscanmsモジュールに渡します。
2. proscanmsモジュールが設定に従ってメールを処理します。ウイルス チェックと修復は、次のように行われます。
    - proscanmsモジュールがメールを受信します。受信時にメールの解析処理を行い、ヘッダ解析、マルチパートメール解析を行います。
    - 解析したメールはウイルスチェックのため一時的なディレクトリに保存されます。
    - WBLリストが定義されている場合には、ブラックリストに送信元MTAが登録されいる場合は、無条件でメールを破棄します。
    - proscanmsがローカル ソケットを使用して、メール ファイル名をsavapiモジュールに渡します。
    - savapiは受け取ったファイル名からウイルス データベースとファイル内容を照合してウイルス チェックを行い、ウイルスを検出します。
    - proscanmsが、ファイルのステータスを表す結果コードをsavapiから受け取ります。
    - ウイルスメールでなかった場合には、spamチェックが行われます。（オプション）

- proscanmsが、構成ファイルの設定パラメータに基づいてオブジェクトを処理します。オブジェクトの処理方法はそのステータスによって異なります。
- 正常なメールは、Filter処理を行います。

3. 処理されたメール自体、およびウイルス チェックの結果に関する通知が、SMTPによってsendmailメール システム (構成ファイルとしてsendmail.cfを使用) に渡されます。sendmailはこのメール トラフィックをローカル ユーザーに配信するか、または他のメール サーバーにルーティングします。
4. 配送処理が終了すると、一時ディレクトリのファイルは消去されます。

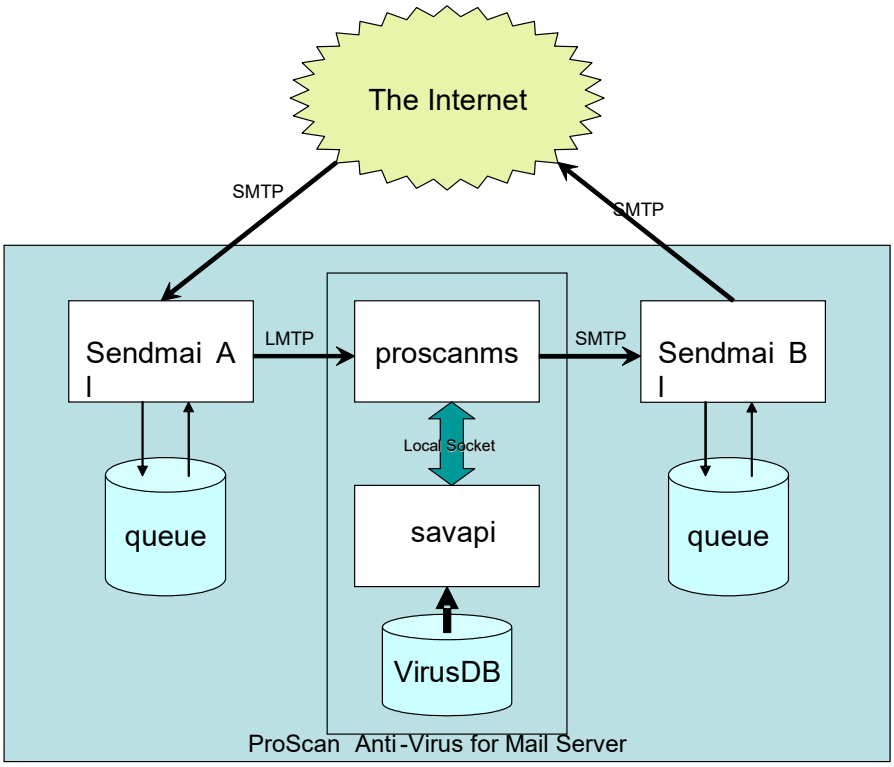


図1 ProScan® Anti-Virus for Mail Serverの内部アーキテクチャ

2.2. メール システムと同じサーバーに導入する

ここでは、メール システムと同じサーバーへのProScan®の導入とその設定について説明します。

ProScan®をメール システムと同じサーバーで実行するには、そのサーバーがサポート対象のOS (Linux、FreeBSD) を搭載している必要があります。

対応しているメール サーバーは、sendmail、qmail、Postfixです。

この導入パターンは、メール サーバーの負荷の変動が少ない環境に適しています。

上記のいずれかのメール システムと同じサーバーでProScan®を実行するパターンについて、詳しく解説します (図2を参照)。受信メールも送信メールも次の手順でまったく同じように処理されます。

1. ほかのサーバーまたはほかのLANから、SMTPプロトコルを経由してメールのストリームが入ってきます。
2. メール システムがメールを受信し、ウイルス チェックを行うため、ProScan®に渡します。
3. ProScan®が設定に従ってメールを処理し、その処理結果の通知と共にメールをメール システムに返します。
4. メール システムが外部サーバーまたはLANのメールボックスにメールをルーティングします。

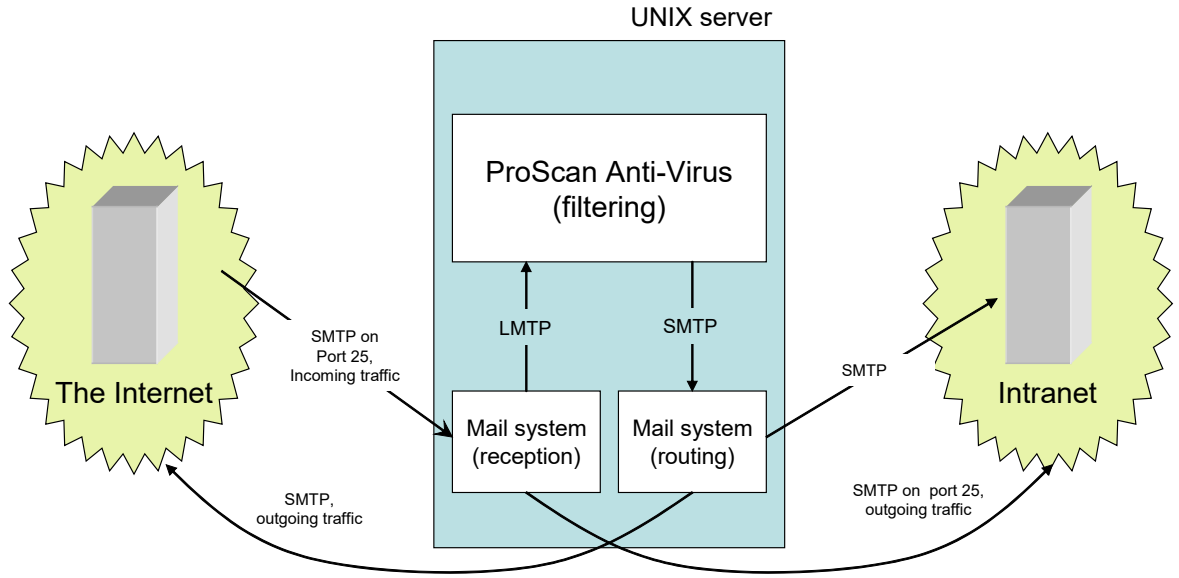


図2　ProScan®の動作（メール システムと同じサーバーで動作する場合）

ProScan®をインストールする場合は、上記の図を参照し、インストール中またはインストール直後に次の設定を行う必要があります。

- ProScan®が処理の対象とするメール サーバーのポート
- ProScan®がフィルタリングしたメールの受信に使用するメール システムの用ポート

2.3. 二次フィルタとして導入する

ProScan®は、一次フィルタとしても二次フィルタとしても使用できます。ProScan®のインストールする前に、メール サーバーがすでにメール トラフィック フィルタの機能を備えている場合は、一次フィルタと二次フィルタをそれぞれどちらにするかを指定する必要があります。その際、フィルタリング方法を基準にして決定します。

一次フィルタ（ここではMX1と呼ぶ）は、送信者のIPアドレスに基づいてメールをフィルタリングするもので、サーバーの25番目のポートに最初のフィルタとしてインストールされます。一次フィルタは、入ってくるメールを受信し、フィルタリングしたうえで二次フィルタに渡し、二次フィルタがこれを処理します。**二次フィルタ**（ここではMX2と呼ぶ）は、一次フィルタと同じホストにインストールされますが、割り当てられるIPアドレスとポート番号は異なります。

送信者のIPアドレスに基づいて処理を行うフィルタがサーバーにインストールされていない場合は、ProScan®を一次フィルタとしてインストールできます。ProScan®がウイルス チェックを行ったメール送信元IPアドレスはすべて同じになるため、ウイルス チェック後のメールをIPアドレスでフィルタリングしても効果はありません。

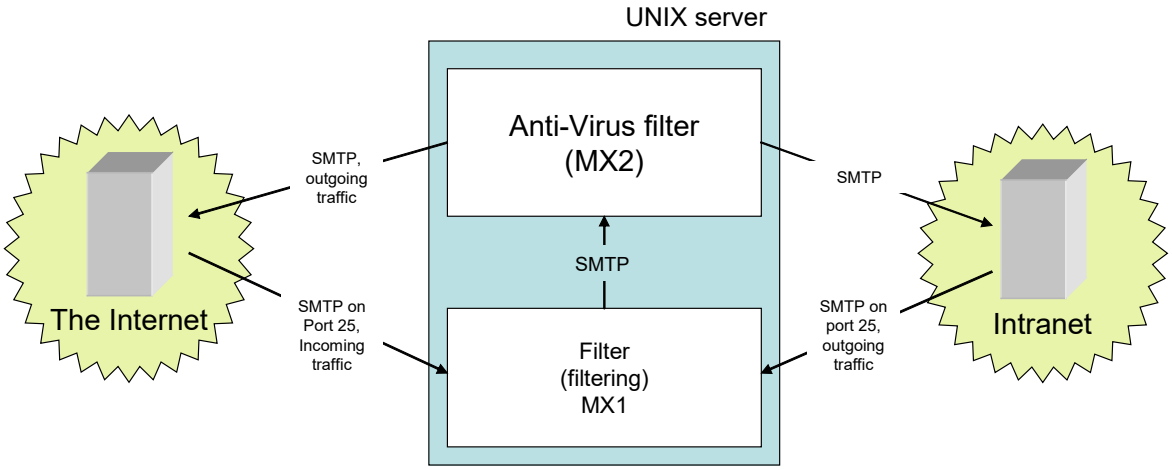


図3　ProScan®の動作（メール システムと同じサーバーで二次フィルタとして動作する場合）

一次フィルタと二次フィルタを次のように設定します。

・一次フィルタ (MX1) の設定

フィルタをインストールするホストの名前：mx1.yourhost.domain

フィルタのIPアドレス：任意

フィルタのインストール先ポート番号：25

メール送信先ホストの名前：mx2.yourhost.domain:10026

・二次フィルタ (MX2) の設定

フィルタをインストールするホストの名前：mx2.yourhost.domain

フィルタのIPアドレス： 127.0.0.1

フィルタのインストール先ポート番号：10026

メールの受信元ホストの名前：mx1.yourhost.domain

MX1とMX2には別々のホスト名を割り当てる必要があります。helo/ehloのホスト名が同じ場合、サーバーがメールを受け付けないためです。また、MX1とMX2の間に双方向の信頼関係を確立する必要があります。確立していない場合はメールを配信できません。

2.4. 専用サーバーに導入する

メール サーバーがWindowsなどのサポート対象外のOSを実行している場合でも、ProScan®Anti-Virus for Mail Serverでメールをフィルタリングし、ウイルス チェックを行えます。

このような場合は、Linux、FreeBSD、を実行する専用サーバーにProScan®をインストールします。

メールを受信し、Windows搭載のメール サーバーに転送するには、専用サーバーにProScan®とメール システム (sendmail、qmail、Postfix) の両方をインストールし、ProScan®をそのメール システムと統合します (15ページの4.4を参照)。

この導入パターンでは、次のように処理が行われます (図4を参照)。

- UNIX OSを実行しているサーバーがメールを受信します。
- qmailなどのメール システムがLMTPプロトコルを経由してProScan®にメールを転送し、ProScan®がこのウイルス チェックを行います。
- ウイルス チェック完了後、ProScan®が処理結果通知と共にそのメールをメール システムに戻し、メール システムがそのメールをメインのメール サーバーに転送します。メール サーバーは、そのメールを配信するか、さらにルーティングします。

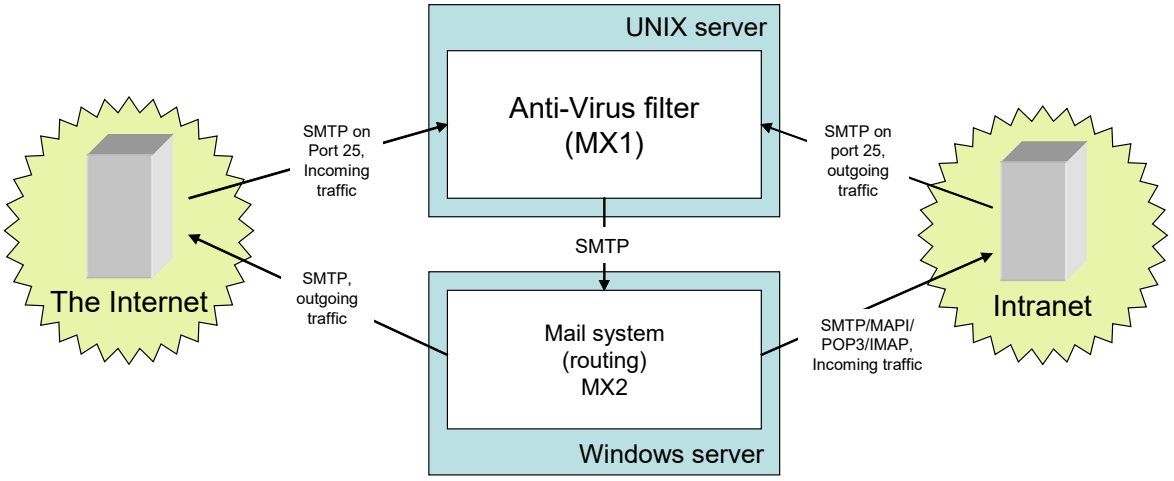


図4　ProScan®の動作（専用サーバー上で動作する場合）

この図では、ProScan®がインストールされているサーバーがメール トラフィックを受信・転送する一次サーバーです。Microsoft Exchangeが動作しているサーバーは二次サーバーとしてメールの配信だけを行います。

ただし、ProScan®をインストールする前に、メール サーバーで送信者のIPアドレスに基づいてメールをフィルタリングを行っていた場合は、ProScan®をインストールしたサーバーを二次サーバーとして指定します。ProScan®をインストールしたサーバーを一次サーバーにすると、二次サーバーが受信するメールのIPアドレスはすべて同じになり、IPアドレスを基準にしてフィルタリングを行う二次サーバーの効果がありません。

LANにメール サーバーを複数設置している場合、MXレコード パラメータまたは転送パラメータの値を、二次サーバーではなく一次サーバーに指定する必要があります。

・一次フィルタ (MX1) の設定

フィルタをインストールするホストの名前：mx1.yourhost.domain

メール転送用ホストの名前：mx2.yourhost.domain

・二次フィルタ (MX2) の設定

フィルタをインストールするホストの名前：mx2.yourhost.domain

メールの受信元ホストの名前：mx1.yourhost.domain

第3章 ProScan®をインストールする

ProScan® Anti-Virus for Mail Serverのインストールを始める前に、次の手順でシステムを準備してください。

- システムがProScan®のハードウェア要件とソフトウェア要件を満たしているかどうか確認します。（1.3. ハードウェアとソフトウェアの要件）wgetなどのアプリケーションがインストールされていない場合は、インストールを事前に行ってください。インストールしないと、アップデート機能を利用できません。
- サーバーにインストールされているメール システムの構成ファイルのバックアップを作成します。
- インターネット接続を設定します。Proxy経由で接続する方は、Proxyサーバの情報を控えておいてください。
- **root**ユーザー、またはUID (universal identifier) がゼロであるユーザーとしてシステムにログインします。

ProScan®のインストールは、サーバーの停止中またはメール トラフィックが最も少ない時間帯に行うことをお勧めします。

インストール前に以下の内容をチェックしておいてください。

通知メールの送信者アドレス	
ProScan管理者のメールアドレス	
defaultグループ管理者のメールアドレス	
wgetのパス	
対象ドメイン	
正規ライセンスのパス	
Registration Code	

3.1. 一般的なインストール

ここで説明するインストール方法は、主にLinux OSを想定しています。

ProScan®のパッケージは、OS＋MTA種別ごとのアーカイブ形式になっています。このアーカイブの中はディレクトリ ツリー構造になっており、パッケージ ファイル群とインストール スクリプト**install.sh** (以降、「**インストーラ**」と表記) が格納されています。このインストーラでインストールを実行します。

パッケージは、tar+gzパッケージ形式となっています。

サーバーへのProScan®のインストールは、次の手順で行われます。

1. ProScanインストールに必要なディレクトリを作成します。
2. パッケージ ファイルをサーバーにコピーします。(必要な設定は対話形式で行われます)
3. メール システムと統合します。
4. レジストレーションコードの設定を行います。(正規ライセンスを持っている場合のみ)
5. ライセンスキーファイルの設定を行います。(正規ライセンスを持っている場合のみ)
6. Crontabに自動アップデート設定を行います。
7. ProScanを起動します。
8. MTAを再起動します。
9. ウイルス データベースをインストール・更新します。

次に、インストール手順について説明します。

3.1.1. インストールを開始する

サーバーにProScan®をインストールするには、次の手順で行ってください。

1. アーカイブ形式のパッケージを、サーバーのファイル システム上のディレクトリにコピーします。
2. **tar zxvf <archive name>**コマンドを使用してアーカイブをアンパックします。配布パッケージが配置されているディレクトリ ツリー、およびインストーラがアーカイブから展開されます。
3. 展開したディレクトリに移動し、インストール スクリプト**install.sh**を実行します。

3.1.2. メール システムとの統合

ProScan®をインストールすると、メール システムと自動的に統合されます。（ディストリビューションによっては自動で統合されない場合もございます。その場合は、ここの説明を読み、手動で設定をお願いいたします。）

sendmailのメール システムを使用している場合は、ProScan®のインストール後、ProScan®のインストール時に作成される構成ファイル **(sendmail.cf.listen)** を使用してメール システムを起動するよう起動スクリプト **(/etc/init.d/sendmail_proscan)**が自動生成されます。

qamilのメールシステムを使用している場合は、/var/qmail/binのqmail-queueがProScan用のqmail-queueに置き換わり（シンボリックリンクされます）、オリジナルのqmail-queueはqmail-queという名前にリネームされます。

Postfixのメールシステムを使用している場合は、master.cf,mailn.cfが書き換えられ、ProScanを経由してチェック＆配送が行われるようになります。

Sendmail Libmilterメールシステムを使用している場合には、sendmail.cfが書き換えられ、Milterモジュールとしてproscanlmが登録されます。

3.1.3. Registration Codeの設定

インストール中に、Registration Codeの設定を促すプロンプトが現れます。既に、Codeをお持ちの場合はそのCodeを登録してください。登録したコードはファイル**(/var/opt/proscan/db/keys/regist.code:**Linuxの場合)に格納されます。ProScan起動時にはこのコードとライセンスキーファイルのコードがマッチするか検査されます。

評価時には、設定不要です。

Registration Codeは弊社において、お客様のライセンス情報を管理する上で非常に重要なものです。紛失したり、他のプロダクトではご利用なさらないようよろしくお願いいたします。

3.1.4. ライセンス キーのインストール

ProScanは起動時に、設定ファイルに書かれたディレクトリにライセンス キー (proscan.keyというファイル) があるかどうか検索します。ライセンス キーは、ProScan®の実行に不可欠なファイルです。このファイルがライセンスの種類を判別し、プログラムの使用をユーザーに許可します。ライセンス キーをインストールしなければ、ProScan®を使用できません。

ライセンスを取得済みの場合は、[y]とタイプし、続いてライセンスキーファイルのフルパスを指定します。もし、ファイルが見つからない場合は、評価ライセンスでインストールを続行します。

評価時やライセンス購入後まだ、ライセンスキーファイルを入手していない場合には、内蔵している30日間評価ライセンスが自動で利用されます。その場合は、[n] をタイプしてパスの指定をスキップし、インストールを続行します。

後日ライセンス キーを受け取ったら、ProScan®の構成ファイルの**LicensePath**パラメータ(63ページのA.2を参照) で指定されているキー格納用ディレクトリにコピーし、ProScanを再起動してください。

ライセンス キーは検知されたものの、有効でない場合は、インストールしても、ProScanは起動できません。

3.1.5. ウイルス データベースをインストール・更新する

インストール時、ウイルス データベースのダウンロードを必ず実施します。ウイルスデータベースがないとProScanは動作しません。かならず最新のウイルスデータベースをダウンロードしてからご利用ください。ウイルスの検知と感染オブジェクトの修復は、このウイルス データベースのレコードに基づいて実行されます。各レコードには、現時点で認識しているウイルスの説明とそのウイルスに感染したファイルの修復方法が記録されています。

ProScanインストーラはインストールが完了すると、cronにウイルスアップデートの自動起動設定を行います。デフォルトでは1時間に1回の割合でアップデートサイトに接続を行います。プロマークのアップデートサイトには最低でも1日1回パターンファイルの更新が行われています。

ウイルス データベースは毎時更新することをお勧めします。新種のウイルスは毎日のように発生するため、データベースを常に最新の状態にしておくことが重要です。ウイルス データベースの更新については、20ページの5. 1を参照してください。

3.1.6. インストールを完了する

ここまでの手順を完了すると、それを通知するメッセージがコンソールに出力されます。パッケージの構成ファイルには、ProScan®プログラムの起動に必要な設定情報がすべて含まれています。次のパラメータは、プログラムのインストール時に設定されます。

- ProScan®が動作するホストの名前
- 次のディレクトリへの完全パス
- ウイルス データベースの保存先ディレクトリ
- ライセンス キーの格納ディレクトリ
- savapiモジュールとともに使用されるソケット ファイル
- 一時ファイルの配置ディレクトリ
- 管理するドメイン名
- 管理者のメールアドレス
- 通知メール送信アドレス
- defaultグループ管理者のアドレス
- proscanを起動するユーザ

その他のパラメータにはデフォルトで既定値が設定されます (13ページの4.1を参照)。ただし、管理者はProScan®の使用を開始する前に、管理者は一部の設定値を変更する必要があります。たとえば、ProScan®とメール システムの統合に関するパラメータはきわめて重要です。このパラメータを設定しなければ、メールのウイルス チェックは行われません。ProScan®の使用を開始する前に設定が必要なパラメータについては、第4章を参照してください。

ウイルス データベースのダウンロードなど、何らかの一部のインストール手順をスキップした場合 (たとえば、ウイルス データベースをダウンロードできなかった場合等)は、後でそのステップだけを実行できます。

第4章 インストール後の設定作業

インストール実行中、ProScan®のインストール先システムを解析し、一部の構成パラメータを自動的に設定します。その他の構成パラメータには、ウイルス チェック プログラムの動作に最適なデフォルト設定が割り当てられます (13ページの4.1を参照)。

ProScan®の機能をフルに使用するには、さらに次の作業を行うこと良いでしょう。

- ProScan®のグループ設定
- 通知メールのテンプレート作成

ここでは、ProScan®のデフォルト設定について説明します。また、ProScan®の使用に必要な構成について詳しく説明します。

4.1. ProScan®のデフォルト設定を使用する

ProScan® Anti-Virus for Mail Serverのパラメータは、すべて**proscan.conf**ファイルにあります。**proscan.conf**はデフォルトの構成ファイルです。

独自の構成ファイルを作成し、そのファイルを現在の作業に使用したり、デフォルトの構成ファイルとして指定することもできます。

ここでは、このファイルのデフォルトのパラメータについて詳しく説明します。この章の説明を読めば、自社の現在の条件下で最大の性能を引き出すためにProScan®の構成変更が必要かどうか判断できます (構成変更については、32ページの第6章を参照)。

サーバーのファイル システムをウイルスから保護するための設定

デフォルトでは、コマンド ライン スイッチを指定せずに**proscanfs**モジュールを起動すると、サーバーのファイル システムのウイルス チェックが行われます。

感染ファイル、感染の疑いがあるファイル、破損しているファイルを検知すると、それを通知するメッセージをコンソールとレポート ファイルに出力します。(設定によります)

デフォルトの設定では、検知した感染ファイルの削除を行いません。

サーバーを経由するメールのウイルス チェックを行う設定

ProScan®をメール システムと統合しなければ、メールのウイルス チェックを行うことはできません。ここでは、メール システムと統合されたProScan®のデフォルト動作の設定について説明します。

インストール直後の構成ファイル**proscan.conf**には**default**グループのみ設定されています。このグループは、メールのウイルス チェックについて次のルールを設定しています。

- すべての受信メールと送信メールのウイルス チェックを行います。
- 感染メールを検知した場合、受信者とグループ管理者に通知メールを送付します。

送信者へは、メールアドレスが詐称されている可能性があるため、デフォルトでは通知メールを送信しません。

- さらに受信者に関しては、元のメールから感染パートを削除して添付した形で通知メールを送付します。また、送信者に対しては、メールが正しく送付されたように処理します。 (discard)
- その他、メールに対するウイルス チェックの結果、感染の疑いがあるファイル、破損しているファイル、またはパスワードで保護されたファイルを検知した場合やウイルス チェックできないメールがあった場合、同様にそれを示す通知が受信者およびグループ管理者に送信されます。
- ProScan®によって実行されたアクションは、すべてログファイルに記録されます。

4.2. ウイルス データベースをインストール・更新する

ProScan®をサーバーにインストールしたら、ウイルス データベースをすぐにインストール・更新することをお勧めします。（通常はインストール時に自動で行い、その後はcronで自動で行う設定になります。）

ウイルス データベースをインストールまたは更新するには、**proscanup**モジュールを実行します。コマンド ラインで次のように入力します。

```
/opt/proscan/bin/proscanup -V  または  /usr/local/proscan/bin/proscanup -V
```

ウイルス データベースがプロマークの更新用サーバーからダウンロードされ、構成ファイルで指定されている専用のディレクトリに格納されます。

ウイルス データベースは毎日更新することをお勧めします。新種のウイルスは毎日のように発生するため、ウイルス データベースを常に最新の状態にしておくことが重要です。ウイルス データベースの更新については、20～21ページの5.1.1～5.1.2を参照してください。

上記のほかに、proscanupdater.shというスクリプトも用意しています。このスクリプトは、パターンアップデートが実際に行われた場合のみ通知メールを送ることが可能です。インストーラはこちらを自動設定しますが、初期状態では、起動されるたびにメール送信を行うモードになっていますので、silent設定を行い、通知が必要な場合のみメールを送付するようにしてください。

4.3. メール システムに手動で統合する

基本的にインストーラを利用すれば、すべて自動で統合されます。しかしながら、インストーラが想定していないシステムや、条件などではうまく統合されない場合が考えられます。その場合、ProScan®をメール システムと手動で統合する必要が出てきます。以降ではその手順について、各メールシステムとの統合方法を詳しく説明します。

インストールに成功した場合にも、どのような変更が行われたかを理解するためにお読みいただくことをお勧めいたします。

4.3.1. Sendmailメール システムへの統合

ProScan®をSendmailメール システムに統合するには：

1. インストール時に作成された**sendmail.cf.listen**ファイルの98番目のルールを、次のように変更します。

```
SParseLocal=98
R$* $#proscanms[tab character]$@ $1 $: $1
```

メールキューのディレクトリを以下のように変更します。

```
O QueueDirectory=/var/spool/mqueue.proscan
```

2. ファイルにproscanmsの記述を追加します。次に例を示します。

```
Mproscanms, P=/opt/proscan/bin/proscanms, F=PSXmnz9F, S=EnvFromSMTP,
R=EnvToSMTP, E=¥r¥n, L=2040,
T=DNS/RFC822/SMTP,A=proscanms -r ${client_addr}
```

3. 必要に応じてProScan®を構成します (17ページの4.4.5を参照)。

4. 起動スクリプトに次の2つのプロセスを追加します。

```
/usr/sbin/sendmail -bd -q30m -C /etc/mail/sendmail.cf.listen
/usr/sbin/sendmail -q5m -C /etc/mail/sendmail.cf
```

sendmailバージョン8.12以降を使用し、構成ファイルとして**submit.cf**を指定している場合は、起動スクリプトに次の3つのプロセスを追加します。

```
/usr/sbin/sendmail -bd -q30m -C /etc/mail/sendmail.cf.listen
/usr/sbin/sendmail -q5m -C /etc/mail/sendmail.cf
/usr/sbin/sendmail -q30m -C /etc/mail/submit.cf
```

ProScanインストール時にsendmail_proscanという起動スクリプトが生成されます。

ProScan®をSendmail Libmilter システムに統合するには：

1. インストール時に作成された**sendmail.cf**ファイルのInputMailFiltersオプションを設定します。

```
O InputMailFilters=proscanlm
```

2. フィルタープログロムの定義を追加します。

```
Xproscanlm, S=local:/var/run/proscan.sock, F=T, T=S:5m;R:5m;E:5m
```

または、mcファイルに以下を追加して、sendmail.cfファイルをmakeしなおします。

```
INPUT_MAIL_FILTER(`proscanlm', `S=local:/var/run/proscan.sock, F=T,
     T=S:5m;R:5m;E:5m')
define(`confINPUT_MAIL_FILTERS', `proscanlm')
```

さらに、8.12以上をお使いの場合で、送信用MTA（MSA）をご利用の場合は、有効にして置いてください。ローカルホストの587番ポートでSMTP接続が受けられないとProScanが通知メールを送信することができません。

4.3.2. qmailメール システムへの統合

ProScan®をqmailメール システムに統合すると、**qmail-queue**プログラムの代わりにProScan®のqmail-queueモジュールが使用されます。メールを送信したりキューに入れたりする場合は、ProScan®のqmail-queueが元のqmail-queueプログラムを呼び出します。

ProScan®をqmailメール システムに統合するには：

1. **/var/qmail/bin/**ディレクトリの**qmail-queue**というファイルの名前を**qmail-que**に変更します。
2. **/opt/proscan/bin**ディレクトリの**qmail-queue**を**/var/qmail/bin**ディレクトリにシンボリック リンクを作成します。
3. **qmail-queue**と**qmail-que**に対して次のアクセス権を設定します。

```
-rws--x--x    1 qmailq   qmail      12504  4月 25  2003 qmail-que
lrwxrwxrwx    1 root     root         28  4月  7 23:51 qmail-queue ->
                                                    /opt/proscan/bin/qmail-queue
```

4. **/opt/proscan/bin/qmail-queue**に対して次のアクセス権を設定します。

```
-rws--x--x    1 root     root        94960  5月 12 18:27 qmail-queue
```

5. 必要に応じてProScan®を構成します (17ページの4.4.4を参照)。
6. メール システムを再起動します。

4.3.3. Postfixメール システムへの統合

ProScan®をPostfixメール システムに統合するには：

1. 使用しているPostfixメール システムのバージョンが**snapshot_20000529**以降であるかどうか確認します。これより古いバージョンを使用している場合は、Postfix の Web サイト (www.postfix.org) から新しいバージョンをダウンロードします。
2. Postfixメール システムの構成ファイルである**main.cf**に、次の行を追加します。

```
content_filter = lmtp:localhost:10025
```

3. Postfixメール システムの構成ファイルである**master.cf**に、次の行を追加します。myhostnameは必ずPostfixのメールホスト名を設定します。filterというユーザでフィルタープログラムを起動するように設定しています。

```
localhost:10025 inet n n n - 10 spawn user=filter
argv=/opt/proscan/bin/proscanms
localhost:10026 inet n - n - 10 smtpd -o content_filter= -o
myhostname=localhost
```

4. **filter**というユーザーを作成して**filter**グループに追加し、filterユーザーに対するホーム ディレクトリを作成します。filter以外のユーザにする場合には、filterを別ユーザに置き換えて設定を行ってください。インストーラは無条件でfilterユーザとなります。

【Linuxの場合】

```
mkdir /var/spool/filter
groupadd filter
useradd filter -s /bin/false -d /var/spool/filter -g filter
```

```
chown filter.filter /var/spool/filter
```

【FreeBSDの場合】

```
mkdir /var/spool/filter
pw groupadd -n filter
pw useradd -n filter -d /var/spool/filter -s /usr/bin/false -g filter
chown filter.filter /var/spool/filter
```

Postfixの構成ファイルの例については、74ページのA.12を参照してください。

5. ProScanのディレクトリをfilterユーザが読み書きできるように、オーナ変更します。

【Linuxの場合】

```
chown -R filter:filter /var/opt/proscan
```

【FreeBSDの場合】

```
chown -R filter:filter /var/proscan
```

6. 必要に応じてProScan®を構成します。

ExecUser=filterとするのを忘れないようにしてください。

7. メール システムを再起動します。

PostfixのBefore Queue Filter機能を使用するには：

ProScanバージョン6.0.3.8より、Postfixの2.2以降に実装された、Before queue filter機能を利用できるようになりました。（今までは、After queue filterで、一旦、Postfixがキューにメールを受信した後にFilter機能でチェックを行っていました。）そのため、Postfixでは有効でなかった、グレイチェックやWBL等のメールの受信拒否が可能となりました。以下にその設定方法を記述します。なお、詳細につきましては、Postfixのドキュメント等を参照してください。

1. Postfixのバージョンが2.2以上であるか確認します。
2. main.cfの修正を実施します。ProScanインストール時に追加されるcontent_filterパラメータを削除します。これにより、メールは通常配送となります。
3. master.cfの修正を行ないます。まず最初の行の次に

```
smtp      inet  n       -       n       -       20      smtpd
```

以下のオプションを追加します。

```
        -o smtpd_proxy_filter=127.0.0.1:10025
        -o smtpd_client_connection_count_limit=10
```

ProScanインストール時に追加されたエントリ10025ポートのproscanms起動パラメータに-sを追加します。

```
localhost:10025 inet n n n - 10 spawn user=filter
argv=/opt/proscan/bin/proscanms -s
```

10026ポートのエントリに関しましてはそのままとします。

4. Postfixの再起動を行い設定を有効にします。

Postfi milterインターフェースを使用するには：

ProScanバージョン6.0.3.9より、Postfixの2.3以降に実装された、milterインターフェースを利用出来るようになりました。以下にその設定方法を記述します。

1. Postfixのバージョンが2.3以上であるか確認します。
2. main.cfに以下の行を追加します。最後の行のmilter_default_actionパラメータは、milterプログラム

に異常があった場合の動作を指定します。acceptは、異常が合った場合は通常の配送を行うことを示しています。この他、reject（受信拒否）、tempfail（一時エラー）が設定可能です。

```
smtpd_milters = unix:/var/run/proscan.sock
non_smtpd_milters = unix:/var/run/proscan.sock
milter_default_action = accept
```

3. master.cfに以下の行を追加します。

```
127.0.0.1:10026 inet    n       -       n       -       10      smtpd
    -o myhostname=proscan.promark-inc.com
```

4. Postfixの再起動を行います。

4.3.4. メール システムと統合するようにProScan®を構成する

ProScan®をメール システムと統合するには、ProScan®を構成するという重要な作業が残されています。インストーラはこの作業を自動で行います。

構成作業を行うには、ProScan®の構成ファイルを直接変更します。

ProScan®をメール システムと連動するように設定するには：

ProScan®の構成ファイルで次のように設定します。

- 通知の送信元アドレスを指定します。
  NotifyFromAddress=admin@yourhostname.jp
- [**smtpscan.general**] セクションで転送用メール システムを指定します。転送用メール システムの構造は、**protocol:host:port**です。

  protocol — メールの送信に使用されるプロトコル (**smtp**または**qmail**)。
  host — メール送信元のホスト名またはIPアドレス、またはメール プログラムの名前。

  メール プログラムの名前は丸かっこで囲みます。また、この名前には任意のキーを含めることができます。

  port — ポート番号 (デフォルト値は25)。
  たとえば、次のように指定します。

  smtp:localhost:10025または**qmail:(/var/qmail/bin/qmail-que)**

  o sendmailの場合

  ```
  ForwardMailer=smtp:(/usr/sbin/sendmail -bs -C /etc/mail/sendmail.cf)
  ```

  o qmailの場合

  ```
  ForwardMailer=qmail:(/var/qmail/bin/qmail-que)
  ```

  o Postfixの場合

  ```
  ForwardMailer=smtp:localhost:10026
  ```

  o Sendmial Libmilterの場合

  ```
  ForwardMailer=smtp:localhost:587
  ```

  ※587番ポートでListenしていない場合には、25番ポートを指定して下さい。

- 構成ファイルのdefaultグループ定義の [**smtpscan.group**] セクションで、ユーザーのグループに対して次のように指定します。

  ```
  AdminAddress=admin@yourhostname.jp
  ```

- [**smtpscan.limits**] セクションで、savapiが行う処理のタイムアウト (単位：秒) を指定します。次に例を示します。

  ```
  MaxCheckTime=60
  ```

4.4. 管理対象ドメインリストを作成する

ProScanでは、管理対象となるドメインをあらかじめ登録しておく必要があります。通常インストール時に指定したドメインがファイルに登録されています。ファイルの場所は、proscan.confの[Path]セクションのDomainListパラメータで指定されたパスにあります。このリストの使われ方は、[smtpscan.license]セクションのDomainCheckパラメータにより変わってきます。

DomainCheck=yesの設定を行っている場合：

このリストに書かれているドメインが含まれているメールのみチェック対象となります。それ以外のメールはスキャンされませんのでご注意ください。

DomainCheck=noの設定を行っている場合：

このリストにないアドレスを含むメール（From,Toともに）を送受信した場合には、ProScanはライセンス違反としてログファイルに記録します。

登録できるドメイン数はライセンスによります。（インストール時にドメインを設定した場合はこの作業を省略可能です。また、途中で増減する場合には、リストの編集作業をそのつど行ってください。）

ProScanのドメインは、メールアドレスの@以降の部分を言います。

ドメインは、そのメールシステムで扱うすべてのドメインを登録してください。バーチャルドメインも必ず登録してください。サブドメイン、ホスト名を含むドメインも同様です。このリストに登録されているドメインのうち、先頭からライセンスのドメイン数のみが対象となります。ライセンス数をオーバしたドメインについては、対象外となりますのでご注意下さい。

また、このファイルは内部ドメインを判断するためにも利用されますので、NotifyInternalOnlyパラメータを利用する場合には、内部ドメインを記述して下さい。

無制限ライセンスでも管理対象ドメインリストは必要です。但し、NotifyInternalOnlyパラメータを使用しない場合には、代表となるドメインのみ記述でも構いません。

第5章 ProScan®機能概要

ProScan®を使用すると、送受信メールやその添付ファイルのウイルス チェックを完全に行えます。それ以外にも以下のような機能でProScan®は構成されています。

1. ProScanのアップデートを行います。
2. サーバーを経由するメールのウイルス チェックを行います。
3. サーバーのファイル システムへのウイルス侵入を防ぎます。
4. ライセンス管理を行い、適切な処理を行います。

大きく４つの処理にわけて説明します。

この章で説明する処理に関しては､インストール後の設定作業を完了していることを前提とします (13ページの第4章を参照)。

5.1. ProScan®のアップデート

ProScan®は本体のモジュール群、AVエンジン、ウイルスデータベースの更新を行うことが可能です。

これらのモジュール、データはプロマークの更新用サーバーからダウンロードできます。更新用サーバーのURLを次に示します。

http://update.promark-inc.com/updates/
http://update.promark-inc.com:8001/updates/

ウイルス データベースをダウンロードできるサーバーのアドレスは、設定ファイルに記述されています。

複数のサーバを指定することも可能です。その場合は、カンマで区切って複数のサーバを指定して下さい。
ウイルス データベースの更新は、**proscanup**モジュールが起動するproscan_avupdate.shが実行します。

proscanupモジュールの設定は、**proscan.conf**構成ファイルの [**updater.***] オプションですべて行えます (63ページのA.2を参照)。

複雑なLANを組んでいる場合は、最新のウイルス データベースを毎日ダウンロードして所定のネットワーク ディレクトリに格納し、クライアント コンピュータがそのディレクトリからダウンロードできるようにネットワークを設定することをお勧めします。

ウイルス データベースの更新は、**cron**を使用して実行するか (20ページ5.1.1を参照)、またはコマンド ラインから実行します (21ページの5.1.2を参照)。

インストーラは自動でcron設定を行います。crontabに既に別のプログラムを登録している場合には、それらがきちんと登録されているか確認してください。（インストーラが書き換えて止めていないように。インストーラはインストール時にバックアップを/tmp/crontab.proscanとして残しています。）

また、環境によっては直接ダウンロードサイトに接続できない場合も考えられますので、HTTP Proxyを経由したダウンロードも可能となっております。ProScanでは、モジュールとパターンファイルで別々のダウンロード方法を採用しておりますが、どちらもHTTPによるダウンロードとなっております。モジュールに関してはwgetプログラムによりダウンロードを行いますので、wgetの設定方法はwgetのマニュアルもあわせてご覧ください。

5.1.1. アップデート設定

ProScanのアップデート設定は**proscan.conf**構成ファイルの [**updater.options**] セクションで､適切な値を設定します。次に例を示します。各パラメータ値の詳細は付録Aを参照してください。

```
[updater.options]
KeepSilent=yes
UpdateHost=update.promark-inc.com
UpdatePort=80
UpdateProtocol=HTTP
```

```
ReloadApplication=yes
ExtraWgetOptions=
ShowExternalCmdOutput=no

[updater.report]
ReportFileName=/var/opt/proscan/log/updater.log
```

5.1.2. cronによる自動アップデート方法

cronプログラムを使用すると、ProScanの更新をスケジューリングできます。インストール時にインストール時刻の“分”をcronの設定とし、1時間に1回その時刻になるとproscanupが起動します。

1. proscan.confの設定を行います。
2. cronプロセスの動作ルールを設定するためのファイルを開きます（**crontab -e**）。
3. 次の行を入力します。

```
0 * * * * /opt/porscan/contrib/proscanupdate.sh
```

4. cronによる実行が行われると結果をメールで知らせます。

インストール時に設定した場合には、上記作業は不要です。インストール時の時刻設定は、アップデートが集中しないように、インストール時の時刻の分を設定しています。(例：10:23にインストールを行えば毎時23分にproscanupが起動されるように設定されます。)

5.1.3. コマンドラインからアップデートする方法

ProScan®の更新処理は、コマンド ラインからいつでも実行できます。コマンド ラインで次のように入力します。コマンドラインパラメータについては付録A.10を参照してください。

```
proscanup -V
```

5.1.4. モジュールの自動反映について

ProScanはモジュールの自動更新機能も備えています。アップデートコマンドが実行されると、プロマークのアップデートサイトに接続し、モジュールリストを取得します。このリストの内容に従い、現在のモジュールが古い場合に、新規モジュールをダウンロードし入れ替えることが可能です。この機能を利用するとProScanを常に最新版の状態に保つことができます。

自動反映手順

1.アップデートサイトに接続
2.モジュールリストを取得（PSHB01.lst等のプロダクトコードのついたリスト）
3.現在のモジュールのバージョンとリストのバージョンを比較
4.リストのバージョンが新しい場合に、ダウンロードを行う（newディレクトリにダウンロード）
5.ReloadApplication=yesの場合にモジュールの自動反映を行う
6.自動反映を行う際に、現状のモジュールのバックアップをoldディレクトリに退避、新しいモジュールのサイズ、実行可能かチェックを行い、正しい場合のみ反映を行う仕組みになっています。
7.必要に応じて、ダウンロードしたスクリプト（post_update.sh）の実行も行います。

5.2. メール・スキャンについて

ProScan® Anti-Virus for Mail Serverの主要な機能は、送受信または転送されるメールのウイルス チェックを行い、フィルタリングすることです。この処理は、**proscanms**モジュールで行います。

proscanmsモジュールを使用すると、ウイルスに感染したメールを検知し、非感染メールとウイルスを駆除したメールだけをウイルス チェックの結果通知と共に配信できます。

添付ファイルの種類に基づいてフィルタリングするオプションを利用すれば、メールを処理するサーバーの負荷を軽減できます。これらの機能は、ProScan®に備わった機能のほんの一部です。その他の機能については、以降のメールのウイルス チェックの中で説明します。

proscanmsモジュール関連の設定値は、構成ファイル**proscan.conf**の [**smtpscan.***] オプションですべて行えます (63ページのA.2を参照)。

次に、メールのウイルス チェックに関する一般的な処理について説明します。

5.2.1. ProScanのメール・スキャンの仕組み

ProScanのメールスキャナは各MTAの仕様に合わせて呼び出されます。

- Sendmailの場合は、ルールセット98で配送エージェントとして呼び出されます。
- Sendmail Libmilterの場合は、filterプログラムとしてLocalソケット経由で呼び出されます。filterプログラムは、デーモンとして起動されている必要があります。
- Qmailの場合は、qmail-smtpdまたはqmail-injectからqmail-queueが呼び出されることを利用し、qmail-queueの代わりにProScanのqmail-queueを呼び出します。また、場合によっては（qmailの拡張アドレスを使った場合など）qmail-localからqmail-queueが呼び出されることもあります。この場合は、チェック済みのメールを再度チェックすることになるので、それを止めるためにパラメータによりコントロールすることも可能です。
- Postfixの場合は、content_filter機能を利用して、LMTPプロトコルで呼び出されます。またはSMTPプロキシ機能を利用してSMTPプロトコルで呼び出されます。（-sオプション利用時）

Sendmail,Postfixは標準入出力を利用してLMTPプロトコルでメールの受信を行い、Qmailはファイルディスクプリタ0、ファイルディスクプリタ1でエンベロープデータとメールメッセージを受信します。また、Sendmail Libmilterの場合は、ローカルソケット経由でMilterAPIを使用しメッセージのチェックが行われます。

proscanms(qmailの場合はqmail-queue)はMTAから起動されると、パイプを通してメールメッセージを受信します。現時点はSMTP,LMTP,qmail形式での受信が可能です。
受信後、以下のような順序でチェックを行います。

1．DomainCheckパラメータを調べます。ドメインチェックを行う場合にはFromまたはToアドレスが対象ドメインかどうか調べます。
2．メールは一度に複数のあて先を指定することが可能ですので、ProScanでもその対応を行っています。複数あて先の場合は、FromとToのペアごとにチェックを行います。これはFromとToでグループの所属チェックを行うため、どのグループに所属するかあて先ごとにチェックする必要があるためです。
3．Fromがドメイン対象外の場合、Toのドメインを調べます。
4．ドメイン対象外であったり、評価版で更新期限が過ぎている場合にはスキャンを行いません。
5．チェック対象の場合には、グループ定義を調べます。グループ定義はFromとToアドレスで行われ、所属グループがなければデフォルトグループの定義を使用します。グループのCheckパラメータが”no”の場合にはスキャンを行いません。
6．まず最初にWBLリストにより接続元MTAのチェックを行います。ブラックリストに記載されているMTAからの接続であれば、メールは破棄（返送も転送もしない）されます。ホワイトリストに登録されている場合は、以降のチェック処理を選択できます。（例えばウイルスチェックのみ行うとか）
7．スキャンする場合には、AVエンジンに対してスキャン依頼をかけ、結果を受け取ります。エンジンのエラー等正しくスキャンできなかった場合には、配送を行わないように”not scan”の結果ステータスとなります。
8．spamチェックを行う場合には、ここでチェックされます。

９．メールの各種判定を行います。優先順位は以下の通りです。これらはAND条件ではチェックできませんので、最初にマッチした条件でメールが処理されます。例えば感染メールの添付ファイル名はチェックされません。

優先順位	判定内容
1	ウイルススキャン
2	spamチェック
3	Filter題名
4	Filter添付ファイル名
5	Filter添付ファイルMIMEタイプ
6	Filterファイルサイズ
7	Filterヘッダパターンマッチ

１０．　すべてのチェックにパスしたメールにはOKステータスが割り当てられます。

１１．　OKステータスでない場合には、通知メールの処理が行われます。グループ定義の内容にしたがって通知メールが送付されます。

5.2.2. メール配送処理

チェックが終了すると、メールのあて先ごとに、ステータス調べ配送処理が行われます。（OKステータスのメールを実際に配送します。）

配送処理の仕組みを以下に示します。

メール配送は、MTA統合時に設定した、ForwardMailerパラメータを基に行われます。（17ページの4.4.4参照）

ForwardMailerパラメータに設定された内容が、ソケット接続の場合には指定ホストの指定ポートに対して、指定したプロトコルでメールを配送します。例えばPostfix標準である以下のような設定の場合、

ForwardMailer=smtp:localhost:10026

localhostのポート10026に対してソケット接続して、SMTPプロトコルでメール配送を行います。
また、プログラム起動の場合には指定プログラムを起動し、パイプによりプロセス間通信でメール配送を行います。現在サポートしているプロトコルはLMTPとqmail形式のみです。例えばqmailの場合は以下のような設定を行い、オリジナルのqmail-queueに対して配送依頼をかけます。

ForwardMailer=qmail:(/var/qmail/bin/qmail-que)

配送が完了後、配送したメールのアドレスをチェックしアドレスの自動カウントを行います。

5.2.3. フィルタ設定について

ProScanではウイルスチェック以外に、メールのコンテンツフィルター機能も備えています。

パラメータ	チェックコンテンツ	内容
BySubject	Subjectヘッダ	サブジェクトがPosix正規表現で指定した文字列にマッチした場合
ByFilename	マルチパートのファイル名	ファイル名がPosix正規表現で指定した文字列にマッチした場合
ByMIMEtype	Content-Typeヘッダ	Content-TypeヘッダがPosix正規表現で指定した文字列にマッチした場合
BySize	メールサイズ	メールのサイズが指定サイズよりも大きい場合
ByHeader	メールヘッダ	メールヘッダ部分がPosix正規表現で指定した文字列にマッチした場合

上記フィルタ条件を指定し、マッチした場合はfilteredステータスが割り当てられ、[smtpscan.action.filtered]で指定されたアクションを実行します。
Subject,FilenameはMIMEエンコードされている場合、デコードを行った結果でチェックします。現在サポートしているMIMEエンコードは文字コードISO-2022-JP,UTF-8,ASCII、タイプBase64,QuatedPrintableのみです。

5.2.4. アドレスの自動カウントについて

ProScan®バージョン6では、ライセンスタイプがユーザ数指定の場合に、アドレスを自動的にDBの記録し管理しています。チェックするメールがDBに記録されていない場合、DBに自動的に登録します。この時、ライセンス数を超える場合にはライセンス違反としてログに記録します。
メールのアドレスをチェックする条件は以下の通りとなっています。

- スキャンしたメール
- かつ、受信者に配送
- かつ、FromまたはToアドレスがdomainsファイルに登録されているドメイン

この条件に一致したメールのアドレスのみをDBに登録し、1ユーザライセンスとしてカウントします。登録するアドレスは、FromまたはToを指定することが可能です。

このDBに登録されたアドレスのうち、利用者がいなくなった場合等の不要なアドレスは、Licenseviewerコマンドのrオプションにて削除することが可能です。

5.2.5. Proxyスキャナ機能

Proxyスキャナ機能は、アンチウイルスエンジンのプロセスをあらかじめ起動しておき、fork時のオーバヘッドを少しでも低減するための機能です。トラフィックの多いメールサーバにProScanを導入する場合には、非常に有効な機能です。Max200プロセスまで起動させることが可能ですが、起動数を多くするとそれだけマシン資源を消費しますので、マシンの性能に合わせた設定をされることをお勧めいたします。

5.2.6. spamチェック機能

ProScan®バージョン6.0.3より、spamチェック機能が搭載され、オプションライセンスを購入することで利用できるようになりました。spamチェック機能の概要は以下の通りです。

- MATのPOP before SMTP対応DB（DRAC DB）に対応
- RBLチェックが可能
- メールヘッダのspamメール特有の特徴抽出を行いspamを判定（S25R方式採用）
- ホワイトリスト、グレイリスト、ブラックリストに対応
- グレイリストはspamメールの一時拒否を行い、再送により自動的に受け入れるオートホワイトリスト機能を備える（再送受け入れ時間は設定可能）
- Subjectのパターマッチング機能搭載
- spam判定結果をヘッダ、サブジェクトに記録
- ProScanの特徴であるグループ単位にこれらの設定が可能
- メールヘッダ情報のフィルタリング機能搭載

詳細については、「6.2.メールのスパムチェック機能を設定する」をご参照ください。

5.3. ファイル システムのウイルス チェックについて

サーバーのファイル システムをウイルスから保護するには、**proscanfs**モジュールを使用します。**proscanfs**はサーバーのファイルに対してウイルス チェックを行い、感染ファイルや感染の疑いがあるファイルを検知すると、設定に従って処理します。オブジェクトの処理としては、ログやサーバー コンソールへの出力、管理者への通知などのような情報提供と、ウイルスの駆除、オブジェクトの検疫場所への移動、感染オブジェクトの除去などのオブジェクト変更があります。

proscanfsモジュール関連の設定は、構成ファイル**proscan.conf**の [**scanner.***] オプションですべて行えます (63ページのA.2を参照)。

サーバーのファイル システムのウイルス チェックは、コマンド ラインから手動で実行するか、標準の**cron**ユーティリティを使用してスケジューリングを設定します。ウイルス チェックは、サーバーのすべてのファイル システムに対して実行することも、特定のディレクトリやファイルだけをチェックすることもできます。

次にサーバーのファイル システムをウイルスから保護するための典型的な作業について、詳しく説明します。

サーバー全体のウイルス チェックを行うと、大量のリソースを消費し、ウイルス チェックの実行中、サーバーのパフォーマンスが低下することに留意してください。ウイルス チェックとほかのプロセスを同時に実行することはお勧めできません。サーバー全体ではなく、特定のディレクトリに対してウイルス チェックを行うとこの問題を回避できます。

5.3.1. 指定ファイルのスキャンを行う

特定のファイルに対してウイルススキャンを行うには、コマンドラインから以下のコマンドを投入してファイルをスキャンします。

```
/opt/proscan/bin/proscanfs /home/hoge.doc
```

スキャンの結果は以下のように表示されます。

```
/opt/proscan/bin/proscanfs /home/hoge.doc
ProScan now starting!
ProScan File scanner Ver.6.0.4.6 starting...
All Rights Reserved,Copyright(C) 2003-2015 Promark Inc.
ProScan version ------------------------------
 version       : 6.0.4.6
 engine version : 8.3.42.42
 VDF version    : 7.12.132.140
 VDF signatures : 13204235
File scan setting ----------------------------
 log_level      : 7
 directory scan : yes
 symlink scan   : yes
 scan level     : 7
 repair         : no
 action         : none
 save directory : /var/opt/proscan/save
 show level     : 3
 report address :
 output         :
 exclude mask   : /dev/
 include mask   :
File scan start ------------------------------
Current working directory : /var/lib
```

（次ページへ続く）

```
scan results -------------------
 directories :       0
       files :       1
      alerts :       0
    infected :       0
   protected :       0
      repair :       0
      delete :       0
        move :       0
     exclude :       0
--------------------------------
  start time : 16:47:35
    end time : 16:47:35
   scan time : 00:00:00
--------------------------------
```

1つのファイルを処理したことを示しています。
また、mbox形式のメールファイルをスキャンすると以下のようになります。

```
/opt/proscan/bin/proscanfs /home/test/mbox
ProScan now starting!
ProScan File scanner Ver.6.0.4.6 starting...
All Rights Reserved,Copyright(C) 2003-2015 Promark Inc.
ProScan version ----------------------------
 version       : 6.0.4.6
 engine version : 8.3.42.42
 VDF version    : 7.12.132.140
 VDF signatures : 13204235
File scan setting --------------------------
 log_level     : 7
 directory scan : yes
 symlink scan   : yes
 scan level     : 7
 repair        : no
 action        : none
 save directory : /var/opt/proscan/save
 show level     : 7
 report address :
 output        :
 exclude mask   : /dev/
 include mask   :
File scan start ----------------------------
Current working directory : /var/lib/clamav

File: /home/test/mbox
Date: 2015/05/12 15:11:40   Size: 3,852,615 byte
Result: infected! >>> Mailbox_[From: MAILER-DAEMON@proscan.promark-inc.com
(Mail Delivery System)][Subject:Undelivered Mail Returned to Sender].mim -->
file2.mim --> eicarcom2.zip --> eicar_com.zip <<< Eicar-Test-Signatur

scan results -------------------
 directories :       0
       files :       1
      alerts :       1
    infected :       1
   protected :       0
      repair :       0
      delete :       0
        move :       0
     exclude :       0
--------------------------------
  start time : 16:47:35
    end time : 16:47:35
   scan time : 00:00:00
--------------------------------
```

5.3.2. ディレクトリをスキャンする

proscanfsの-r オプションを使うと、ディレクトリは再帰スキャンが可能となります。-r オプションを付けてディレクトリのスキャンを行うと、ディレクトリ配下のファイルもスキャンし、ディレクトリがあればさらにそのディレクトリ配下をスキャンしていきます。（再帰スキャン）

以下、実行例です。

```
# /opt/proscan/bin/proscanfs -r /home/test
ProScan now starting!
ProScan File scanner Ver.6.0.4.6 starting...
All Rights Reserved,Copyright(C) 2003-2015 Promark Inc.

File: /home/test/1074743081-RAV8116
Date: 2004/01/22 13:09:43    Size: 379,372 byte
Result: infected! >>> pop3wGTtTO.mail --> LOVE.zip --> LOVE-LETTER-FOR-YOU.TXT.vbs <<<
VBS/LoveLetter.D

File: /home/test/54MO2h028638
Date: 2004/04/21 16:19:23    Size: 41,813 byte
Result: infected! >>> file0.mim --> file1.txt <<< Worm/NetSky.P.Expl

File: /home/test/virus/body_virus.txt
Date: 2004/03/28 22:32:35    Size: 445 byte
Result: infected! >>> file0.txt <<< Eicar-Test-Signatur

File: /home/test/mbox
Date: 2004/05/12 15:11:40    Size: 3,852,615 byte
Result: infected! >>> Mailbox_[From: MAILER-DAEMON@proscan.promark-inc.com (Mail Delivery
System)][Subject:Undelivered Mail Returned to Sender].mim --> file2.mim --> eicarcom2.zip
--> eicar_com.zip <<< ...

File: /home/test/NetSky.D.mail
Date: 2004/03/03 23:56:50    Size: 25,536 byte
Result: infected! >>> virus-20040302-012631-42056-02-4.gz -->
virus-20040302-012631-42056-02-4 --> file2.mim --> document_excel.pif <<<
Worm/Netsky.D.Dam

File: /home/test/Netsky.D.error.mail
Date: 2004/03/04 00:15:43    Size: 31,102 byte
Result: infected! >>> file2.mim --> document_excel.pif <<< Worm/Netsky.D.Dam

scan results --------------------
 directories :     251
       files :    4994
      alerts :       6
   scan time : 00:03:14
--------------------------------
```

5.3.3. その他のファイルスキャン機能

ローカルファイルシステムのスキャンには、さまざまな付加機能があります。それらの機能について一覧でまとめて以下に示します。詳細については第6章で説明します。

機能	コマンドラインスイッチ	内容
リンク先チェック	s/S	シンボリックリンク先のファイルもチェックするかどうか指定します。デフォルトではチェックします。
対象外ファイル指定	E	スキャン対象外にするファイルをPosix準拠の正規表現で記述します。複数指定はコロン(:)で区切ってください。
対象ファイル指定	I	スキャン対象とするファイルをPosix準拠の正規表現で記述します。複数指定はコロン(:)で区切ってください。
対象オブジェクト指定	m	対象となるオブジェクトを指定します。
アクション指定	C/D/M	オブジェクトにマッチした場合の処理を指定します。Cはチェックのみ、Dは削除、Mは指定ディレクトリに移動します。
結果出力	o <filename>	結果の出力先を指定します。

メール送付	a <addoress>	結果をメールで送付します。
ログファイル指定	l <filename>	ログファイル名を指定します。デフォルトは filescanner.logです。
ログレベル指定	L <level>	ログの出力レベルを指定します。
レポートレベル指定	n <level>	コンソールに出力するレベルを指定します。

5.4. ライセンス キーを管理する

ライセンス キーは、ProScan®の使用権をお客様に供与するものです。ライセンス キーには、ライセンスの種別、有効期限、保護対象ドメイン数またはユーザ数の上限 (ライセンス種別によって異なる)、販売店の情報など、お客様が購入したライセンスに関する必須情報がすべて記述されています。

ライセンスを供与されたお客様は、契約期間中、ProScan®のほかに次のサービスをご利用いただけます。

・最新VDFファイルによるウイルスチェック機能

・E-Mailによるテクニカル サポート

・毎日のウイルス データベース更新

・製品のパッチ プログラム入手

・新バージョンへのアップグレード

・新種のウイルスに関する最新情報の入手

ライセンスが失効すると、これらのサービスを自動的に利用できなくなります。サーバーのファイル システムのウイルス チェックは引き続き実行できますが、ウイルス データベースを更新する機能が利用できなくなるため、ライセンス失効時点のデータベースしか使用できません。

ライセンス キーに保存されている情報を定期的に確認し、有効期限を常に把握しておいてください。

5.4.1. ライセンス キーの情報を表示する

ProScan®には**licenseviewer**という特別なモジュールが用意されています。**licenseviewer**を使用すると、ライセンス キーの詳細情報を表示できます。

また、現在ライセンス対象となっているドメイン、ユーザの情報を表示することができます。

これらの情報は、サーバーのコンソールに出力できます。

コマンド ラインで次のように入力します。

```
licenseviewer -s
```

次のような情報がサーバーのコンソールに出力されます。

```
ProScan License Viewer Ver.6.0.5.0
All Rights Reserved,Copyright(C) 2003-2018 Promark Inc.

ProScan License Information:
 Registration Code = PSHB05-1307-720-314-826
 Expire date       = 2019/03/24 (expires in 819 days)
 Number of domains = 0
 Number of users   = 0

Option License Information:
 Option            = Antispam
 License Status    = Registered
```

ユーザ数を条件としたライセンスの場合、あるユーザがライセンス数としてカウントされているかどうか (つまり、そのユーザのアドレスがDBにあるかどうか) を随時確認できる追加オプションが用意されています。

sergey@localhostというユーザがDBに登録されているユーザであるかどうか確認するには：

コマンド ラインで次のように入力します。

```
licenseviewer -u sergey@localhost
```

次のような情報がコンソールに出力されます。DBに登録されていない場合でもライセンス対象でないとは限りません。このコマンドはDB内のアカウント情報を調べるためだけに存在します。

```
ProScan License Viewer Ver.6.0.5.0

All Rights Reserved,Copyright(C) 2003-2018 Promark Inc.

sergey@localhost not regist
```

DBに登録されている全てのユーザを参照するには：

コマンドラインで次のように入力します。

```
licenseviewer -u all
```

DBに登録されている不要なユーザを削除するには：

コマンドラインで次のように入力します。

```
licenseviewer -r test@domain.jp
```

または、正規表現で指定する場合には、以下のように行います。

```
licenseviewer -R @domain.jp
```

どのアドレスが削除されるか確認するには、tオプションを使います。

```
licenseviewer -t -R @domain.jp
```

6.0.3.4より、正規表現パターンで削除するアドレスを指定できるようになりました。一括削除や日本語コードで削除できないようなアドレスには、こちらを試して下さい。

管理対象のドメインを確認するには：

コマンドラインで次のように入力します。

```
licenseviewer -d all
```

5.4.2. ライセンスを更新する

ProScan®のライセンスを更新すれば、ウイルス データベースの更新をはじめとするProScan®の機能をすべて引き続きご利用いただけます。

ライセンス期間は、ご購入時に選択したライセンスの種別によって異なります。

ProScan® のライセンスを更新するには：

ご購入元に連絡し、ProScan®のライセンス更新料をお支払いください。

または

プロマークに直接連絡してライセンスを更新します。販売部門（sales@promark-inc.com）宛にEメールを送信してください。

購入したライセンス キーはインストールする必要があります。インストールするには、キー格納用ディレクトリにライセンス キーをコピーし、サーバーを再起動します。キー格納用ディレクトリとは、構成ファイルの**LicensePath**パラメータで指定したディレクトリのことです。proscan. keyを置き換えることで新たに1年間利用が可能となります。

5.4.3. 更新通知について

ProScan®ではライセンス関連の通知をProScan自身が管理者に送付することができます。

以下の３つのパターンについて通知を行います。

条件	対象ライセンス	タイミング
更新期限が過ぎている場合	すべてのライセンスが対象	proscan起動時 proscanup起動時（但し、以下条件の時のみ） 午前0時台に起動された場合のみ通知メールを送ります。cronによる起動で午前0時台に起動されない場合は通知は送られません。 期限切れ後、3日間だけ通知されます。
更新期限間近 LicenseWarningNotifyDaysパラメータに指定している日数になったときから、更新期限まで	すべてのライセンスが対象	proscan起動時 proscanup起動時（但し、以下条件の時のみ） LicenseWarningNotifySendTimeパラメータに指定されている時刻台に起動されたときのみ通知メールを送ります。
ユーザ数オーバ間近 LicenseWarningNotifyUsersパラメータに指定しているユーザ数に残りライセンス数が達したとき。	ユーザ数ライセンス、評価ライセンスが対象	同上

各パラメータのデフォルト値は以下の通りです。

パラメータ	デフォルト値
LicenseWarningNotifDays	14
LicenseWarningNotifUsers	5
LicenseWarningNotifySendTime	6

これらの通知を抑止することはできません。

ライセンスに関する通知は、プロマーク社にも自動的に送付されます。

5.5. コンフィグレーションの反映

ProScanのメールスキャナは、各MTAから呼び出されるとQUITコマンドを受け取るかタイムアウトするまでプロセスが終了しません。特に、Sendmail Libmilter版では、デーモンとして動作し続けますので設定ファイルを変更した場合に反映処理が必要となります。（qmail-queueは、セッション毎に起動されていてその都度、設定ファイルを読み込みます。）

設定変更したコンフィグレーションの反映には以下のコマンドで行います。コマンドラインより実施してください。

```
#killall -USR1 proscanms ※または、proscanlm
```

killallコマンドのないOSをご利用の場合には、起動しているすべてのproscanmsプロセスにUSR1シグナルを送信してください。なお、qmailシステムをご利用の方はMTAの性質上、毎回の起動となりますのでこの作業は不要です。

第6章 詳細設定

ここでは、ProScan®に備わった各種機能の詳細設定について説明します。13ページの第4章で説明したパラメータは必須の設定であり、設定しなければProScan®を使用できません。それに対して詳細設定は、管理者が任意で設定する項目です。詳細設定機能を利用すれば、ProScan®の機能を拡張し、また、作業環境に合わせてProScan®を細かく設定できます。

構成ファイルでは外部構成ファイルを読み込む機能が搭載されています。_include ディレクティブで、ファイルを指定することにより、別の構成ファイルの内容を読み込み処理されます。また、パラメータにファイルが指定でき、そのファイルにデータを記述することが可能です。ProScanの構成ファイルには、セクション単位にパラメータを指定します。そのパラメータに以下のような形式を使用することで外部ファイルに内容を持つことが可能です。

パラメータ名=file:ファイル名

複数のパラメータで同じ内容を持つ場合や、8000文字制限のために指定できないような場合に有効です。但し、多用しますとリソースを消費しますので、パフォーマンスに影響が出る場合がございますのでご注意下さい。

6.1. メールのウイルス チェック機能を設定する

各メールのウイルス チェックを行う場合は、送信者と受信者のアドレスや送受信者が属しているグループのパラメータに基づいてルールを選択します。したがって、アドレスを適切にグループ分けすることが重要です。

メールは、その送信者と受信者のアドレスが共に存在するグループに所属します。ProScan®は両方のアドレスがグループのアドレス リストに登録されているかどうか確認します。送信者と受信者のアドレスの組み合わせが存在するグループが見つかると、そのグループに指定されたルールに基づいて処理されます。

ProScan® は、**proscan.conf**ファイルの内容に基づいてウイルス チェックとフィルタリングを行います。
グループにメールのアドレスが存在するかどうかは、**POSIX regex**で確認します (この規格の詳細については、man 7 regexを参照してください)。

デフォルトでは、メールの処理ルールを指定する [smtpscan.group] セクションが構成ファイルに含まれます。このグループにはドメイン名および送信者と受信者の名前が登録されていないため、指定したルールはすべてのメールに適用されます。defaultグループのパラメータを変更し、新しいグループを作成することもできます。

構成ファイルにほかのグループを追加 (33ページの6.1.1を参照) すると、メールの次の手順で処理されます。

1. メールのアドレスが管理者の定義したグループに所属しているかどうか確認します。

   メールのアドレスは送信者アドレス、受信者アドレス両方をチェックします。[Domains]パラメータがあれば、送信者あるいは受信者のアドレスどちらか（OR条件）に指定ドメインがあれば、そのグループに所属するとみなします。また、Senders,Recipientsパラメータがあれば、送信者のアドレスがSendersにあり、かつ、受信者のアドレスがRecipiensにあれば（AND条件）そのグループに所属するとみなされます。Domainsパラメータを省略した場合には、Senders,Recipientsパラメータが使われます。
   Senders,Recipientsパラメータは省略すると、すべてを表す「.*@.*」が指定されているものとみなされます。その所属するユーザー アドレス グループが見つかった場合、そのグループに指定されたルールに基づいて処理されます。

処理対象のメールの送受信者のアドレスが複数のグループに所属する場合は、最初のグループのパラメータが適用されます。

2. 管理者が定義したアドレス グループに送受信者のアドレスが所属していない場合、メールは**default**グループに指定されたルールに従って処理されます。

受信メールに対するProScan®のアクションの順序を図 6 に示します。

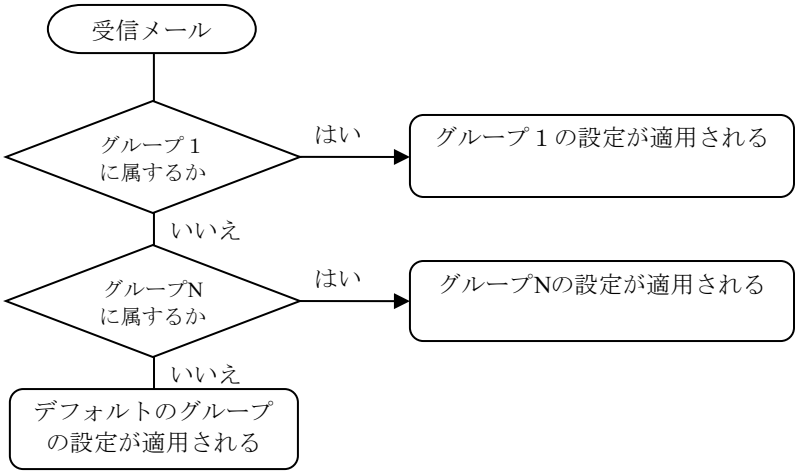


図6 ProScanのグループ設定によるメールの処理

6.1.1. ユーザー グループを作成する

デフォルトでは、サーバーのすべての送信者と受信者を含む **[smtpscan.group]** が構成ファイルに用意されています。このグループには、次の処理ルールが設定されています。

- すべてのメールをチェックします。
- 感染したメール、感染の疑いがあるメール、破損しているメール、パスワードで保護されたメール、ウイルス チェックが不可能なメールの情報をその受信者、グループ管理者に通知します。
- 受信者の通知メールには、元メールの添付は行いません。
- 感染したメール、感染の疑いがあるメール、破損しているメール、パスワードで保護されたメール、ウイルス チェックが不可能なメールは、破棄されます。（バウンスされません）

特定の送信者と受信者に独自のルールを設定してメールを処理する場合は、グループを作成する必要があります。

新しいユーザー グループを作成するには：

1. 構成ファイルに **_group new_group_name** ディレクティブを作成し**[smtpscan.group]**セクションを作成します。

グループディレクティブは以下のような形式で記述します。

```
_group Group1
(Group1の定義)
_group Group2
(Group2の定義)
_group default
(defaulグループの定義)
_end_group
```

グループ内に定義できるセクションは**[smtpscan.group][smtpscan.action][smtpscan.notify][smtpscan.filter][smtpscan.spam][smtpscan.spam_action][smtpscan.spam_notify][smtpscan.wbl]**の8種類です。この中で **[smtpscan.group]** は必須です。defaultグループの定義は削除しないでください。defaultグループの定義は、グループ定義のどの位置にあっても必ず最後に評価されます。

2. グループに含める受信者と送信者のアドレス (アドレス マスク) を指定します。指定するには、**Senders**と**Recipients**のパラメータをカンマで区切って入力します。または、ドメイン名を**Domains**パラメータに指定します。
3. **Users**パラメータを使うと外部ファイルでアドレスを指定できます。その場合は**Users**パラメータにファイルを指定します。ファイルには1行に1アドレスを記述します。ProScan起動時にこのファイルを読み込み、自動的にDBを作成します。(作成する場所は、そのファイルと同じディレクトに作成します。そのため、ProScanの起動ユーザがDBを作成可能な権限を持っている必要があります。)

   または、**userdbadm**コマンドを利用すると、ProScan稼動時にでも動的にDBを変更することが可能です。

   メールを処理する際にこのDBを参照し、どのグループに所属するか判断します。従って、ユーザファイルを変更した場合には必ず、DBの反映処理(再起動またはuserdbadmによる処理)が必要となります。なお、アドレスの大文字小文字は区別しません。

アドレスマスクの設定には**POSIX regex**規格を使用します。

Recipientsまたは**Senders**のパラメータを指定しない場合は、自動的に「**.*@.***」に設定されます。この場合、ヌルアドレス(<>)にはマッチしませんので、マッチさせたい場合は「^$」としてください。

RecipientsとSendersのどちらも指定しなければ、このグループのルールがすべてのメールに対して適用されます。(defaultグループと同様)特定のグループをグループ リストから削除せずにウイルス チェックの対象から除外する場合は、Domainsパラメータに適当な名前のドメイン(存在しないもの)を設定することにより可能です。グループの送信者と受信者のアドレスのマスクを設定すれば、再びウイルス チェックの対象となります。

また、Usersパラメータに指定するファイルの拡張子は".db"以外のものにしてください。ProScanは起動時に、このパラメータに設定してあるファイルを読み込み、拡張子を取り除いて、".db"を付けたDBファイルを自動的に生成します。そのため、拡張子が".db"ですと同じファイル名となってしまい、問題が発生します。

6.1.2. メールのウイルス チェックと駆除のモード

特定の送受信者のグループのメールに対してウイルス チェックを行うには、サーバー管理者がグループ パラメータで該当するモードを有効にする必要があります。

有効にするには、proscan.conf構成ファイルで、チェックするグループに**Check=yes**を設定します。Checkモードを有効にすると、そのグループに属する送信者と受信者のメールに対しウイルス チェックを行います。ただし、感染メールを検知するだけでウイルスは駆除されません。

6.1.3. メールに適用するアクション

メールに適用されるアクションは、次の2つの要素によって決定します。

・ウイルス チェック後のオブジェクトのステータス (45ページの6.2.2を参照)

・構成ファイルで特定のオブジェクトのステータスに設定されているアクション

オブジェクトのステータスは、ウイルス チェック直後のsavapiプロセスによって割り当てられます。ウイルス チェック後に適用されるアクションは、サーバー管理者が設定します。これらの設定は構成ファイルの各グループ定義内の[smtpscan.action]セクションで指定します。

ProScan®では、本来配送されるべき配信メールと受信者への通知メールに対して適用するアクションを指定できます。メールの送信者および管理者には、通知のみ設定できます。

配信メールには、次のいずれかのアクションを設定できます。

配送(unchange) – メールをそのまま配信します。
拒否(reject) – メールをエラーとしてバウンスします。
破棄(discard) – メールはバウンスしません。(配信もされません)

通知メールのアクションは次の通りです。

添付(unchange) － オリジナルのメールを添付します。
駆除(delete) － オリジナルメールの対象オブジェクトのパートを削除したメールを添付します。
削除(remove) － メールを添付しません。

すべてのオブジェクト タイプに共通のアクションを指定することも、それぞれのタイプに個別のアクションを指定することもできます。また、通知メールのあて先ごと（管理者、受信者、送信者）の設定も可能です。

すべてのオブジェクト タイプに共通のアクションを設定するには：

RecipientActionパラメータに値を設定します。これらは、すべてのオブジェクト タイプに共通のアクションを指定するパラメータです。
例：

```
[smtpscan.action]
AdminNotify=yes
RecipentNotify=yes
SenderNotify=no
RecipientAttachReport=remove
RecipientAction=discard
```

管理者、受信者には通知メールを送ります。送信者には送りません。受信者への通知メールには何も添付されず、元メールは破棄されます。

オブジェクトの個々のタイプに異なるアクションを設定するには：

[smtpscan.action.<object_type>]セクションを作成し、それぞれのアクションを指定します。

例：

```
[smtpscan.action.infected]
AdminNotify=yes
SenderNotify=no
RecipientNotify=yes
RecipientAction=discard
RecipientAttachReport=delete
```

この設定では、ウイルス感染オブジェクトの場合のみ、元メールから感染パートを削除したメールを受信者への通知メールに添付します。その他のオブジェクトはすべて、メールから除去します。

暗号化されたファイルを添付したメールをそのまま配信するには：

[smtpscan.action.protected]セクションを作成し、それぞれのアクションを指定します。

例：

```
[smtpscan.action.protected]
AdminNotify=no
SenderNotify=no
RecipientNotify=no
RecipientAction=unchange
RecipientAttachReport=remove
```

この設定では、暗号化オブジェクトの場合のみ、元メールをそのまま配信します。

暗号化されたファイルはProScan®では正しく内容を検査することができません。そのため、ウイルスメールが暗号化されている場合もございます。上記設定を行う場合、これらのウイルスメールも受信者に配送されることになりますのでご注意ください。

上記のアクション以外に、**検疫ディレクトリのオブジェクトを遮断**することもできます。

メールのオブジェクトを検疫ディレクトリに移動するには：

グループの構成ファイルに次のパラメータを設定します。

```
[smtpscan.action]
QuarantinePath=/var/opt/proscan/quarantine
Quarantine=yes
```

6.1.4. 送信者、受信者、管理者に通知する

ProScan®では、メールの送信者、受信者、グループ管理者にオブジェクトのステータス (感染の疑いあり、感染、駆除済み、破損など) を通知できます。通知には、送信モード、生成パラメータ、表示するテキストを設定できます。**通知の送信**は、次の構成パラメータによって指定します。

- **RecipientNotify** – 通知をメールの受信者に送信します。
- **SenderNotify** – 通知をメールの送信者に送信します。
- **AdminNotify** – 通知をグループ管理者に送信します。

以上のパラメータを**[smtpscan.action]**セクションに記述するとステータスを問わず、すべてのオブジェクトに関する通知の送信を指定します。特定のステータスのオブジェクトに関する通知を送信するには、**[smtpscan.action.<object_status>]**セクションを作成し上記パラメータを設定します。

たとえば、グループに次のように設定します。

```
[smtpscan.action.error]
RecipientNotify=yes
SenderNotify=no
AdminNotify=yes
```

スキャンエラーのオブジェクトの通知だけを管理者および受信者に送信します。

通知を送信するには、**[smtpscan.general]** セクションの **[NotifyFromAddress]** パラメータで送信元アドレスも指定する必要があります。

デフォルトでは、ステータスを問わず、すべてのオブジェクトに関する通知が送信されます。通知には、配布キットに含まれるテンプレート (/etc/opt/proscan/template/ja/notify_sampleに保存) のテキストが記述されます。

通知に表示されるテキストを変更するには、次のいずれかの処理を行います。

・付属テンプレートのテキストを変更します。

・新しいテンプレート ファイルを作成し、ファイルの完全パスを **[smtpscan.notify]** セクションの **Template** パラメータとして指定します。

テンプレートのテキストには、次のマクロを使用できます。マクロは**savapi**プロセスの応答に基づいてそれぞれの値に自動的に置き換えられます。

マクロ名	内容
%SENDER%	メールの送信者のアドレス
%RECIPIENT%	メールの受信者のアドレス
%MSGID%	メールのID番号
%SUBJECT%	メールの件名

%RCVDATE%	メールを受信した日付と時刻。日付と時刻の表示形式を変更できます。詳細については、63ページのA.2を参照してください。
%SNDDATE%	メール送信日時（内容は%RCVDATE%に同じ）
%VIRUSNAME%	ウイルス名
%VIRUSINFO%	ウイルス情報
%SCANSTATUS%	スキャン結果（localeセクションで設定したメッセージ）
%HEADER%	メールのヘッダ情報（ヘッダ部分すべて）
%VERSION%	ProScanのバージョン情報
%TODAY%	通知メールを処理した日付（形式は%RCVDATE%に同じ）
%NOWTIME%	通知メールを処理した時刻（形式は%RCVDATE%に同じ）

MIMEタイプ、メールの件名、コードページなどの通知の生成に関するパラメータは、構成ファイルの**[smtpscan.notify]** セクションで設定します。

日本語のテンプレートを利用する場合には、charsetパラメータで指定された文字コードに変換されて送信されます。テンプレートファイル自体は必ずEUCコードで作成してください。

また、管理ドメイン（Domainsファイルに設定したドメイン）のみに通知を行う機能があります。
[smtpscan.action.<object_status>]セクションのNotifyInternalOnlyパラメータで、送信者、受信者ごとに内部ドメインの場合にのみ通知を行う設定が可能です。
例えば、送信者通知を行う場合、送信者が管理ドメインに属する場合のみ通知メールを送付するには、以下のように設定します。

```
[smtpscan.action]
SenderNotify=yes
NotifyInternalOnly=sender
```

設定可能なパラメータは以下の通りです。

設定値	内容
sender	送信者通知を行う場合、送信者が管理ドメインに属する場合のみ通知を行う。
recipient	受信者通知を行う場合、受信者が管理ドメインに属する場合のみ通知を行う。
both	上記両方の動作を行う。
none	ドメインに関係なく、通知を行う。

6.1.5. savapi異常時のメール配送について

ウイルススキャンエンジンが何らかの理由で停止したときに、ウイルスチェックができなくなります。その際にメールを配送するか、一時エラーとしてMTAに通知するかの設定が可能です。（6.0.4.7より）
[smtpscan.general]セクションのAVEdownThroughパラメータで指定します。
ように設定します。

```
[smtpscan.general]
AVEdownThrough=yes
```

設定可能なパラメータは以下の通りです。

設定値	内容
yes	savapi異常時もメール配送を行う。
no	savapi異常時にMTAに一時エラーというステータスを返す。

6.1.6. WBL設定

ProScan®ではグループごとにWBL設定が可能です。ウイルススキャンに先立ってチェックされますので、ブラックリストを定義しておけば、チェック前に拒否することが可能です。

WBL設定は、[**smtpscan.wbl**]セクション内で行います。IPアドレス、ホスト名、ネットワークに対してそれぞれ、Reject、Acceptが設定可能です。カンマで区切って複数の指定が可能です。ホスト名での指定はPosix正規表現でパターン指定できます。
以下に設定例を示します。

- **IPアドレス指定で拒否する場合**

```
AcceptIP=192.168.0.3,21.34.56.78
RejectIP=192.168.100.1
```

- **ホスト名で指定する場合**

```
AcceptName=hoge.localdomein.com
RejectName=¥.black¥.virus¥.com
```

- **ネットワークで指定する場合**

```
AcceptNet=192.168.10.0/24
RejectNet=18.234.0.34/29
```

また、バージョン6.0.3.4からホワイトリストを設定した場合には、以降の処理を選択することが可能となりました。例えば、ある特定のMTAから送られるメールはウイルスチェックのみするといった設定が可能となります。これは、AcceptLevelパラメータにより指定します。

AcceptLevel	処理内容
0	何もチェックせずにメールを配送
1	ウイルスチェックのみ行う
2	アンチスパム機能が有効な場合、スパムチェックも行う
3	フィルタのSubjectチェックも行う
4	フィルタの添付ファイル名チェックも行う
5	フィルタのMIMEタイプチェックも行う
6	フィルタのメールサイズチェックも行う
7	フィルタのヘッダ部チェックも行う
9	通常と同様すべてのチェックを行う（デフォルト）

さらに、WBLでRejectした場合の配送処理を選択することも可能です。RejectActionパラメータでReject時の配送処理を指定してください。何も設定しない場合には”discard”が選択されます。

RejectAction	処理内容
discard	メールを破棄し送信者へエラーを通知しません。（デフォルト）
reject	メールをエラー処理したことを送信者へ通知します。（MTAにエラーとなったことを伝え、MTAからエラーメールが送信者へ送られます）

6.2. アンチスパム機能を設定する

ProScan®にオプションとして装備された、アンチスパム機能について説明します。

ProScanのアンチスパム機能は、メールの送信元MTAのIPアドレスを元に各種判定を行うのが基本となっています。スパムメールは、世の中にあるまっとうなMTAから送られることはほとんどないことに着目し、送信元MTAの信頼度をメールの配送ヘッダから抽出するような仕組みを採用しています。

基本的には、以下のような順番でチェックを行います。

1. グループでスパムチェック（SpamCheck=yes）をするかどうか判定します。（必ずウイルスチェックが有効になっている必要があります。スパムチェックだけをすることはできません。）
2. スパムチェックする場合に、有効なライセンスがあるかどうかチェックします。
3. 実際にスパムチェックを接続元IPを元にして行います。

   - DracDBが設定されていればチェックを行います。DBにある場合は、通常メールと判定します。
   - RBLチェックを行う場合は、RBLサイトにチェックリクエストを行い、スパム送信MTAか判定します。スパムと判定されれば、高レベルのスパムメールと判定します。
   - グレイリストチェックを行う設定になっていれば、自動ホワイトリストをチェックします。このリストは、グレイリストから自動的に救済されたIPアドレスのDBとなっています。ここでIPアドレスが見つかれば、通常メールと判定します。

   Postfixのafter queue filterを利用している場合には、一旦PostfixがSMTPセッションをクローズするため、グレイリスト方式の一時拒否はできません。Postfixで一時拒否を行うにはBefore queue filterの設定（16ページの4.4.3参照）を行ないご利用ください。詳細につきましてはPostfixのドキュメントをお読みください。また、同様の理由でSendmail版におきましても利用できません。Sendmailをご利用の方は、Libmilter機能をご利用下さい。Libmilterではグレイリスト方式の利用が可能です。

   - 経路ヘッダの情報、接続元IPアドレスから逆引きを行い送信元MTAのFQDNを得ます。このFQDNを元にスパムメール送信MTAらしいかどうか判定します。ここで、スパムメールらしいと判定された場合には、グレイリストチェックを行う場合には、グレイリストへのIPアドレス追加処理を行い、そうでない場合には低レベルなスパムメールとして判定します。
   - 最後に、サブジェクトのパターンチェックを行います。登録パターンにマッチすれば、高レベルのスパムメールと判定します。

4. スパムメールの判定は、現時点では高、低の２レベルです。スパムメールと判定されなかったメールは、再度スパム用のブラックリストによりチェックがされ、そこでも問題なければ通常のメールと同様に以降の処理がなされます。
5. 高、低いずれかのレベルのスパムメールと判定された場合には、ホワイトリストをチェックし、救済措置が取られます。
6. 最終的にスパムメールと判定された場合にはスパム･アクションの設定に従い、処理が行われます。アクション設定は、レベル毎にも定義できますし、全てのレベル共通の設定も可能です。
7. 設定できるアクションは、スパムメールの退避（Save）、配送（Deliver）、通知（Notify）、ヘッダ追加（AddHeader）、サブジェクト追加（AddSubject）の5種類です。

6.2.1. アンチスパムライセンスを設定する

ProScan®のアンチスパム機能は、オプション機能として提供されます。オプションライセンスの購入前に30日間の評価ライセンスを利用することが可能です。

アンチスパム・オプションライセンスはProScan新規導入時には評価ライセンスが自動で設定されます。アップグレードした方は弊社販売代理店または直接弊社にお問い合わせください。なお、評価ライセンスの適用は1回までとさせて頂いております。

- 入手したライセンスをantispam.keyとしてライセンスディレクトリにコピーします。
- licenseviewerにより、正しく認識されていることをご確認ください。
- 正規ライセンスの場合、ProScanのレジストレーションコードと同じでない場合は動作いたしません。
- 正規ライセンスの有効期限が切れた場合には、チェック動作も停止します。

6.2.2. DracDBを設定する

POP before SMTPを設定されているMTAをご利用の場合、MUAからのSMTP接続をスパムと判定しないために、POP before SMTPが作成したDrac DBを許可リストとして利用することが可能です。これは、ProScanのアンチスパム機能が、送信元のIPアドレスを基準にスパム判定を行っているための処置です。

Drac DBの種類によっては利用できない場合がございます。その場合、弊社サポートまでご連絡ください。利用可否を検討いたします。

Drac DBを利用するには、グループ定義内の**[smtpscan.spam]**セクションに**DracDB**パラメータを設定します。

```
[smtpscan.spam]
DracDB=btree:/etc/mail/dracd.db
```

“DBタイプ：DBファイル名”の形で指定します。DBタイプを省略した場合には、btreeが設定されたものとみなします。DBタイプはbtreeのほかにhash,text,dumpを指定できます。それ以外のタイプには対応していません。textの場合は、プレーンなテキストファイルで行頭のIPアドレスでチェックします。（デリミタは、コロン・セミコロン・カンマ・空白・改行のいずれかです。）dumpの場合は、バイナリデータ中のテキスト部分の中からIPアドレスにマッチする文字列を抽出し（stringsコマンドと同様の機能）チェックします。また、btree,hashタイプでチェックに失敗した場合（主にDBのバージョン違い）には、自動的にdumpタイプで再チェックを行います。ログにエラーが記録されている場合には、DBタイプの見直しを行なってください。

6.2.3. RBLを設定する

RBL(Realtime Black List)は、DNSのクエリ形式でIPアドレスの問い合わせを行うと、そのIPアドレスがスパム送信として使われるものかどうかの判定結果を返します。ボランティアのサービスとして世界中でそのデータベースが公開されています。
通常、問い合わせに対する応答があれば、何らかの問題があるMTAであると言えますので、ProScanのアンチウイルス機能では、問い合わせに対する肯定応答があったものをスパムと判定しています。
RBLを利用するには、グループ定義内の**[smtpscan.spam]**セクションに**RBLcheck**、**RBLHostName**パラメータを設定します。デフォルトではRBLチェックを行わない設定になっています。

```
[smtpscan.spam]
RBLcheck=yes
RBLHostName=dnsbl.njabl.org
```

RBLHostNameはフリーで公開しているデータベースサイトを指定してください。RBLサイトはカンマで区切ることにより複数指定可能です。（最大32ホスト）
このRBLでスパムと判定された場合は、高レベルの判定結果が与えられます。

6.2.4. グレイリストを設定する

グレイリストは、ホワイトリストとブラックリストの中間の機能を有しています。ProScanでは、メール送信元がスパムらしいと判定された場合に、グレイリストチェックを行うかどうか判断し、行う場合には一時的にメールの受け取りを拒否します。拒否した場合に、そのIPアドレスをグレイリストに登録します。ProScanのアンチスパム機能では、メールの送信元IPアドレス、エンベロープFrom、エンベロープTo、Message-IDヘッダの値をハッシュ化したものと、記録時刻を合わせてリストに登録します。（このリストをよりブラックリストに近いということでダークグレイリストと呼んでいます。）
スパムメールは短期間で再送されたり、1回きりで再送されないパターンが多いので、有る程度の時間（デフォルトでは20分）を置いた後の再送で、このリストに同一メールの記録があれば、スパムメールでないと判定します。（判定した結果はライトグレイリストと呼ばれるリストに移されます。以後、そのIPアドレスからのメールはスパムで無いと判定されます。自動救済措置です。）時間内での再送信や同一MTAからの送付でも異なるメールの場合には、さらに一時拒否します。
グレイリストを利用するには、グループ定義内の**[smtpscan.spam]**セクションに**GrayCheck**パラメータを設定します。デフォルトでは、グレイリストチェックを行う設定にはなっていません。

```
[smtpscan.spam]
GrayCheck=no
```

グレイリストの運用では以下の点に注意して下さい。

- この機能は、通常のメールをスパムと判定する誤認識を防ぐのが目的です。そのため、この機能を利用するとスパムメールを判定する確立が低くなります。
- 再送間隔が短いMTAの場合は、再送許可時間を短くしないとメールを受け取れない可能性があります。
- 再送の度に、異なるIPアドレスのMTAから送付されるような場合には、メールの受け取り時間がかかる可能性があります。
- Spamによっては、再送を行ってくるものもあります。その場合は、WBLRejectパラメータで拒否する必要があります。

6.2.5. メールのヘッダをチェックする

メールのヘッダの内容に対して以下の２つの設定をすることが可能です。
[smtpscan.spam]セクションのHeaderCheckとHeaderPermitです。

【HeaderCheck】
このパラメータにはspamと判定したいヘッダ情報のパターンをPosix正規表現で指定することが可能です。ここで指定したパターンがヘッダ内にあるメールはspamと判定されます。

【HeaderPermit】
このパラメータにはspamと判定したくないメールのヘッダ情報のパターンをPosix正規表現で指定します。

このヘッダチェックは、S25R方式チェックの前に判定されますので、RBLやdracチェック、ホワイトリストチェックの判定を覆すこのはできません。

6.2.6. サブジェクトパターンを設定する

スパムメールとして判定するためのサブジェクトパターンを設定することが可能です。
この設定には**Posix正規表現**が利用でき、複数の設定はカンマで区切ることに可能です。

サブジェクトに「未承諾広告※」が含まれるメールをスパムと判定するには：

[smtpscan.spam]セクションの**SubjectCheck**パラメータを指定します。

例：

```
[smtpscan.spam]
SubjectCheck=未承諾広告※
```

複数指定時には8000バイト以内でカンマ区切りで1行にまとめて記述してください。
このチェックでスパムメールと判定された場合には、高レベルの判定結果が与えられます。

6.2.7. スパム用WBLを設定する

スパムの用のWBLは以下のような機能を有しています。

- スパムと判定されなかったメールに対してブラックリストの処理で最終判定が下されます。
- スパムと判定されたメールに対してホワイトリストの処理で救済が行われます。

ブラックリスト、ホワイトリストは**Posix正規表現**のパターンで指定します。複数の場合はカンマで区切って1行（8000文字以内）で記述してください。（多数のパターンを指定する場合には、file:パラメータで外部ファイルに指定することが6.0.3.8より可能となりました。）

「dip.t-dialin.net」からのメールをスパムと判定する：

[smtpscan.spam]セクションの**WBLReject**パラメータを指定します。

例：
```
[smtpscan.spam]
WBLReject=¥.dip¥.t-dialin¥.net
```

「plala.or.jp」からのメールはスパムと判定しない：

[smtpscan.spam]セクションの**WBLAccept**パラメータを指定します。

例：
```
[smtpscan.spam]
WBLAccept=¥.plala¥.or¥.jp
```

6.2.8. スパムメールに適用するアクション

スパムメールに適用されるアクションは、スパム判定レベルにより分けることができます。現在は、高･低の2種類(43ページ6.2.8参照)となっていますが、これらを区別せずにアクションを設定することも可能です。

設定できるアクションは、スパムメールの退避（**Save**）、配送（**Deliver**）、通知（**Notify**）、ヘッダ追加（**AddHeader**）、サブジェクト追加（**AddSubject**）の5種類です。

アクションの意味と設定内容を下表に示します。

アクション	パラメータ	設定内容
スパムメールの退避	Save	SavePathで指定されたディレクトリにスパムと判定されたメール本文を退避します。ファイル名はオブジェクトIDが付けられています。
配送	Deliver	スパムメールを配送するかどうかを指定します。 yesの場合は配送し、noの場合は配送しません。（discard処理）
通知	Notify	スパムメールを受け取る受信者に対して通知メールを送るかどうか指定します。 yesの場合は通知メールを送ります。Deliverとともにyesとすると2通のメールが受信者に届くことになりますので注意してください。
ヘッダ追加	AddHeader	スパムメールのヘッダに任意のヘッダ文字列を追加します。 必ず、「ヘッダフィールド: 文字列」の形式で指定して下さい。 ヘッダフィールド名は「X-xxxx」となるようにしてください。
サブジェクト追加	AddSubject	スパムメールのサブジェクトの先頭に文字列を追加します。 未設定の場合は何も追加されません。

高レベルのスパムメールを退避せずに、ヘッダ情報とサブジェクトに文字列を追加し配送する：

[smtpscan.spam_action.high]セクションに以下のような設定を行います。

例：
```
[smtpscan.spam_action.high]
Save=no
Deliver=yes
Notify=no
AddHeader=X-spam-status: high
AddSubject=[SPAM:High]
```

通知メールの設定は、以下のように行います。

[smtpscan.spam_notify.high]セクションに以下のような設定を行います。

例：
```
[smtpscan.spam_notify.high]
Subject=spam detected : %SUBJECT%
Charset=ISO-2022-JP
ContentType=text/plain
Template/etc/opt/proscan/template/Japanese/spam_high
```

サブジェクト、テンプレートに利用できるマクロはウイルス通知の場合と同じです。
（36ページ6.1.4参照）

6.2.9. スパム判定レベルについて

ProScanでは、２つのレベルでスパムを判定します。

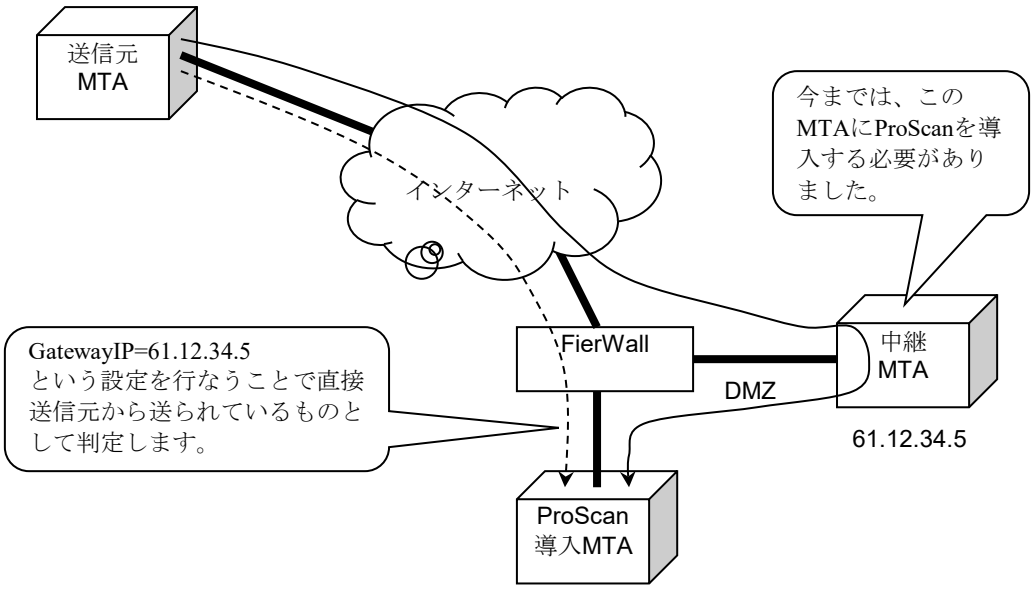
- 高レベル(high) ・・・ 間違いなくスパムである（WBL,RBL,サブジェクトパターンでスパムと判定）
- 低レベル(low) ・・・ かなりの確立でスパムである（メールの経路情報から判定）

100%スパムと判定するのは現実的に不可能で、あくまでも目安とお考え下さい。

6.2.10. ゲートウェイを経由するメールのスパム判定

内部MTAやFireWallを経由するようなSMTP接続の場合、今までのProScanではspam判定を行なうことが出来ませんでした。ProScanではこのような場合でも、メールのRecievedヘッダ情報を元に判定が可能です。[smtpscan.general]セクションのGatewayIPパラメータに経由するMTAのIPアドレスを指定することで、接続元がこのパラメータに一致する場合、一つ前の経由MTAのIPアドレス情報を送信元としてチェックを行います。(一つ前がローカルIPの場合は、さらにさかのぼって送信元とします。)

これにより、さらに導入の範囲が広がります。



このような形態でもProScan for Antispamオプションを利用できるようになりました。

中継MTAのIPアドレスは、直接受信しているアドレスが、スキップする場合の送信元IPはメールのヘッダ情報より抽出します。

6.2.11. DHA攻撃対応機能を設定する

DHA(Directory Harvest Attack)攻撃に対応する機能を標準搭載しています。このDHA攻撃は、スパマーが、正規のSMTPプロトコルを使って、辞書生成した数千というメールアドレスを送信し、組織から有効なメールアドレスを収集しようとする攻撃です。正規の手続きを踏んでいるため、単純に拒否することは難しいのが現状です。ProScanのアンチスパム機能では、事前に受け取るべきアドレスの一覧を作成しておき、その内容に基づいて、エラー宛先をカウントし、一定数以上（DHALimit）のエラーが含まれる場合に、そのセッションを一時エラー（tempfail）とする機能を有しています。また、受け取るべきアドレスでない場合のアクションも指定可能です。

DHA対応を利用するには、**[smtpscan.general]**セクションに**DHACheck**、**DHALimit**、**DHAAction**、**RecipientsFile**パラメータを設定します。デフォルトではDHAチェックを行わない設定になっています。

```
[smtpscan.general]
DHACheck=yes
DHALimit=10
DHAAction=userunknown
RecipientsFile=/etc/opt/proscan/local_user.txt
```

エラーを許容する数はDHALimitに設定します。動作させる前に、DBを作成します。DBは、userdbadmコマンドで自動的に生成することが可能です。追加や削除などは、起動中でもこのコマンドを使うことで可能です。既にファイルが用意されているのであれば、以下のようなコマンドでDBを作成できます。

```
/opt/proscan/userdbadm -g DHA -N /etc/opt/proscan/local_user.txt
```

グループ名のDHAは固定です。このコマンドで/etc/opt/proscan/local_user.dbというファイルが生成されます。以降、追加がある場合には-Aオプションを利用してアドレスを追加していきます。（詳細については付録.Bを参照下さい。）

6.3. サーバーのファイル システムのウイルス チェック機能を設定する

サーバーのファイル システムのウイルス チェックを行うパラメータは、次の設定項目でグループ分けされています。

- ウイルス チェックの対象範囲 (45ページの6.3.1を参照)
- ウイルス チェック・駆除のモード (45ページの6.3.2を参照)
- ファイルに適用するアクション (46ページの6.3.3を参照)
- 処理結果レポートの生成 48ページの6.6を参照)

次に、これらの各グループについて説明します。

6.3.1. ウイルス チェックの対象範囲

ウイルス チェックの対象範囲は、次の３つの要素に分けられます。

- **ウイルス チェック パス** — ウイルス チェックを行うディレクトリとファイル
- **ウイルス チェック対象外オブジェクト** — ウイルスチェック対象外となるファイル名
- **ウイルス チェック対象オブジェクト** — ウイルスチェックを行うファイル

デフォルトでは、ファイル システムでチェック可能なオブジェクトがすべて対象となります。（但し、/dev配下と、/proc配下はチェック対象外です。）

サーバーのすべてのファイル システムをチェックするには、コマンド ラインでルートファイルシステム「/」を指定します。但し、これはシステムに大きな負荷を与えます。

ウイルス チェック パスを指定するには、次のいずれかの方法を使用します。

- モジュールを起動する際、完全パスを使用して、ディレクトリやファイルを指定します。複数のディレクトリやファイルを指定する場合は、空白で区切ります。
- パスの一部をウイルス チェック対象から除外するには、構成ファイル**proscan.conf**内で、ウイルス チェック対象から除外するファイル マスクとディレクトリ マスクを指定します (**[scanner.options]** セクションの**Exclude**パラメータ)。
- 逆に、指定パスのみチェックする場合には、**Include**パラメータでそのファイルまたはディレクトリを指定します。
- ディレクトリに対する再帰的ウイルス チェックを有効にします。有効にするには、**[scanner.options]** セクションの**Recursion**パラメータを変更するか、またはコマンド ラインで**-r**キーの設定を変更します。

相対パスでのチェックも可能です。

6.3.2. ファイルのウイルス チェックと駆除のモード

感染ファイルの発見時のアクションは、サーバのファイルシステムをウイルスから守る上で重要な設定項目です。

このオプションは、デフォルトでは”none”になっており、ウイルス チェックでウイルス、感染の疑いがあるファイル、暗号化アーカイブの検出のみ行います。通知は、コンソールとレポートにメッセージを出力するという形で行われます (48ページの6.5を参照)。

ウイルス チェックを完了すると、すべてのファイルに次のいずれかのステータスが割り当てられます。

- **Ok —** このファイルでウイルスは検知されませんでした。
- **Infected —** このファイルはウイルスに感染しています。

- **Suspicious —** このファイルのコードは、未知のウイルスのコードに類似しています。
- **Error—** 何らかの原因で正しくスキャンできませんでした。
- **Protected —** このファイルはパスワードで保護されています。

6.3.3. ファイルに適用するアクション

ファイルに適用できるアクションは、そのステータス (45ページの6.2.2参照) によって異なります。デフォルトでは、一定のステータスのファイルの感染が検知された場合にのみ通知が行われます。このような通知メッセージは、コンソールとレポートに出力されます。

なお、ステータスが**Infected**、**Suspicious**、**Protected**および**Error**のファイルに対しては、次のアクションを設定できます。

- **特定のディレクトリに移動する —** 特定のステータスのファイルをあらかじめ設定したディレクトリに移動します。これらのファイルは、パス名、属性そのままで移動されます。(**move**)
- ファイル システムから**ファイルを削除する**。(**delete**)
- チェックのみで**何もしない**。(**none**)

ファイルに適用するアクションを選択するには、次のいずれかの方法を使用します。

- デフォルトのアクションは、構成ファイル**proscan.conf**の [**scanner.object**] セクションで設定します。詳細については、63ページのA.2を参照してください。
- 代替構成ファイルでアクションを設定し、モジュール起動時にその代替構成ファイルを指定します。

モジュール起動時にコマンド ラインで構成ファイルを指定しなかった場合は、**proscan.conf**で指定したパラメータが使用されます。**proscan.conf**をモジュール起動時に明示的に指定する必要はありません。

- 現在のセッションに適用するアクションを設定するには、proscanfsモジュール起動時に、コマンド ラインのキーを使用します (70 ページのA.3を参照)。

6.4. savapiプロセスの動作を設定する

これまでに説明してきたとおり、メールのウイルス チェックは、savapiとproscanms(qmail-queue,proscanlm)の2つのモジュールが連携して行います。

savapiは、ランチャプログラムであるproscan実行時に呼び出されます。(savapiを直接起動することも可能です。)

proscanmsがsavapiにアクセスするとすぐに接続が確立されます。

プロセスの動作に関するパラメータは、**proscan.conf**構成ファイル **([aveserver]** セクション)で設定できます。

6.4.1. savapiをリロードする

proscanupによるアップデート時にエンジンの更新が行われている場合には、savapiプロセスを自動的に再起動します。

通常の運用動作ではsavapiプロセスの再起動は必要ありません。起動パラメータ（下記参照）の変更を行った場合のみ再起動してください。再起動は、インストール時に組み込まれる起動スクリプトを利用してください。

再起動：`# /etc/init.d/proscan restart`

変更した場合にsavapiの再起動が必要なパラメータ一覧

セクション	パラメータ	内容
path	LocalSocketPath	ソケットパス
	LicensePath	ライセンスパス
	TempPath	一時ディレクトリパス
aveserver	ExecUser	起動ユーザ
	ProxyMode	Proxyスキャナモード
	ProxyScanners	Proxyスキャナ数
	ReportFilename	ログファイル名
	ReportLevel	ログレベル
updater.options	UpdateHost	アップデートホスト
	HTTPproxyServer	Proxyサーバ名
	HTTPproxyPort	Proxyサーバポート番号
smtpscan.group	Users	グループユーザを定義するファイル（userdbadmコマンドを利用する場合はこの限りでない）

6.4.2. savapiを終了する

savapiプロセスを終了するには、proscanモジュールでstopオプションを付けて実行します。これによりsavapiを終了させます。

停止：`# /opt/proscan/bin/proscan stop`

savapiプロセスの終了に**kill –9**コマンドを使用してしないでください。このコマンドを実行すると、savapiプロセスを終了しますが、一時ファイルや作業ファイルが一部残るため、手動で削除しなければなりません。

6.5. 日付と時刻の表現形式を変更する

ProScan®の実行時、各モジュールに関するレポートが生成され、それと同時にユーザーと管理者にさまざまな情報が通知されます。これらの情報には必ず、その情報の生成日時が付加されます。

デフォルトでは、strftime規格に準拠した次の日時形式が使用されます。

%H:%M:%S — 日付の表示形式

%d/%m/%y — 時刻の表示形式

管理者は、日時の表現形式を変更できます。変更するには、構成ファイル**proscan.conf**の [**locale**] セクションで行います。設定可能な形式は次のとおりです。

%I:%M:%S %P — 12時間表示の時刻形式 (**TimeFormat**パラメータ)
%y/%m/%dおよび%m/%d/%y — 日付の形式 (**DateFormat**パラメータ)

6.6. ProScan®のレポート機能

ProScan®の各モジュール動作結果はすべてレポートに記録され、そのレポートがログファイルに出力されます。ログファイルは各モジュールごとに持つ事ができ、設定ファイルで指定できます。しかしながら、ログファイルを指定するまでの処理で問題があった場合（設定ファイルの読み込み処理など）には、標準エラー出力に出力されます。但し、メールスキャンモジュールは標準エラー出力を持たないのでどこにもエラー出力されない状況でした。バージョン6.0.3からsyslog機能を利用して、ログファイルがオープンされるまでの間の問題もログに記録できるようになりました。

サーバーのファイル システムに対するウイルス チェックの結果は、コンソールにも出力されます。デフォルトでは、コンソールとレポートに同じ情報が出力されます。コンソールとレポートに出力する情報を変更するには、追加設定を行う必要があります。詳細については、50ページの6.6.4を参照してください。

出力される情報は、レポートレベルで変更できます。ProScan®はレベルをビットの重み付けであらわします。論理和をとることで出力させたい情報を選択することが可能です。

次の表に、レポート情報レベルのリストを示します。

レベル	レベル名称	意味
0		0 を指定すると何も出力されなくなります。
+1	エラー関連	エラー（アクションを実行できないためにプログラムが停止する）に関する情報のみ出力。
+2	コンフィグ関連	Proscan。Confファイル読み込み時の処理を出力。
+4	ライセンス関連	ライセンスに関わる情報を出力。
+8	メールスキャン関連	メールのスキャン関連の処理を出力。
+16	AVエンジン関連	ウイルス チェック関連メッセージを出力。
+32	通知メール関連	通知メールの処理に関する情報を出力。（proscanms）
+64	メール配送	メール配送に関する情報を出力。（proscanms）
+128	アップデート関連	アップデートに関連する情報を出力。（proscanup）
+256	スパム関連	スパムチェックに関連する情報を出力。（proscanms）
+8192	デバッグ情報	デバッグに関する情報を出力。

レベル１～４は各モジュール共通です。８～64はproscanmsモジュールが出力します。128はproscanupが出力します。proscanfsが出力するメッセージは上記とは別にコントロールされます。

上記の情報レベルに従って出力される情報は、一般に次の形式で表示されます。

```
[date time]-[pid.num] STRING
```

パラメータの説明：

[*date time*] — システムによって生成されるパラメータ。このパラメータは、日付と時刻（管理者が設定した形式）とレポート情報レベル（レベルの先頭の文字）で構成されます。

日付と時刻の形式は、構成ファイル**proscan.conf**の [**locale**] セクションで変更できます。

[*pid.num*]－プロセスIDと同一プロセス内の通番です。

STRING — レポートの行。形式はメールの種類によって異なります。メッセージの種類は次のとおりです。

- ウイルス チェックに関するメッセージ (6.6.2を参照)
- その他のメッセージ (モジュールの起動、ウイルス データベースの読み込み、リターン コードなど。6.6.3を参照)
- コンソールに出力されるメッセージ (6.6.4を参照)

それぞれのメッセージの種類と形式については、後述します。

6.6.1. syslog機能

ProScanバージョン6.0.3より、syslog機能を利用できるようになりました。そのため、ログファイルオープンまでの間に発生した問題もログに記録できるようになりました。また、通常のレポート出力もsyslog機能を利用して行うことが可能です。

各モジュール起動時からProScanのレポート出力機能が始まるまでの間のレポート出力はsyslogdのuser.infoファシリティで行われます。syslog機能を利用する場合にはあらかじめこのファシリティでのログ記録ができるようにsyslog.confの設定を行って下さい。

また、ProScanの通常のレポート出力をsyslogdで行うには、各モジュールのReportFileパラメータでsyslogと設定し、Priority,Facilityパラメータで出力先を指定して下さい。

6.6.2. メール チェックに関するメッセージの形式

メール チェックに関するメッセージは、各種モジュールとproscanfsとsavapiに対してのみ生成されます。

メール チェックに関するメッセージは次のとおりです。

・スキャン結果メッセージ

```
scan result: result
```

・ウイルス感染時のサブメッセージ

```
>>> archive_file_name <<< virus_name
```

パラメータの説明：

result – ウイルスのチェック実行後に、ファイルに割り当てられるステータス。このパラメータの種類については、後述の表に示します。

archive_file_name — チェックしたファイル名です。圧縮アーカイブの場合には展開後のファイル名が ”-->” に続いて表示されます。Infectedの場合のみ表示されます。

virus_name — ウイルスの名前。Infectedの場合のみ表示されます。

結果(result)	意味
ok	このファイルは感染していません。
infected	このファイルは1つ以上のウイルスに感染しています。
suspicious	このファイルは、未知のウイルスに感染している疑いがあります。
error	エラーが発生したため、このファイルのウイルス チェックを実行できません (例：破損しているアーカイブなど)。
protected	このファイルは暗号化されているため、ウイルス チェックできません。
other	上記以外の理由でチェックできません。
not scan	システム的なエラーでウイルスチェックできません。
spam	スパムとして判定されたメールです。

6.6.3. その他のメッセージの形式

ウイルス チェックに関するメッセージ以外にも、モジュールの起動やライセンス キーの読み込みなどの情報を示すメッセージが生成されます。これらのメッセージの形式は次のとおりです。

- モジュールの起動およびウイルス データベースに関するメッセージ
- 読み込んだライセンス キーに関するメッセージ
- メール配送に関するメッセージ
  `Deliver (<from_address> ==> <to_address>)`
- 通知メール配信に関するメッセージ
  `Notify type Status (<from_address> ==> <to_address>)`
  type — "A"管理者 "R"受信者 "S"送信者のいずれかをあらわします。
  Status — 通知を送る原因となったステータス番号
- グループに関するメッセージ
  `Check group_name group configuration`
  group_name —グループ定義名
- ファイルに適用したアクションに関するメッセージ

6.6.4. コンソールに出力されるメッセージの形式

メッセージをコンソールに出力できるのは、**proscanfs**と**proscanup**です。

proscanfsモジュールの起動時にコマンド ラインで**-q**キーを使用するかどうかによって、**proscanfs**モジュールでコンソールに情報を出力するかどうかが決まります。このキーを指定すると、コンソールに情報が出力されません。**proscanup**モジュールの動作に関するメールをコンソールに出力するには、構成ファイルで**KeepSilent=no**と指定するか、**-V**オプションを使用します。

proscanfsモジュールのコンソールに出力される情報の内容は、変更できます。変更するには、構成ファイル(**proscan.conf**または代替構成ファイル) に [**display**] セクションを追加します。詳細については、63ページのA.2を参照してください。

このセクションでは、アーカイブのオブジェクトに対するウイルス チェック情報、およびモジュールの処理の進行状況を表示するかどうかを設定できます。

ウイルス チェック レポートの情報レベルを変更するには、[**display**] セクションを追加したうえで、コマンドラインで**–L <option>**キーを指定します。

6.6.5. レポートファイルのローテートについて

各種レポートファイルは、運用中にどんどん肥大化しますので、ProScanではローテートスクリプトを標準で提供しています。インストール時に${ProScan binディレクトリ}/contrib/rotate_log.shというスクリプトがインストールされますのでこれをcronで1日1回（または、サイトの状況に合わせて1週間に1回等適当な間隔で）起動するように設定して下さい。スクリプトは4世代までバックアップを持つようになっています。（それ以上をご希望の方は各自で修正してください。）

以下、crontabへの設定例です。1日1回午前0時にローテートを行う場合。

```
0 0 * * * /opt/proscan/contrib/rotate_log.sh > /dev/null 2>&1
```

第7章 設定例

この章では、実際の業務で行うことを想定した設定を例に課題と解決方法として説明します。

7.1. メールのウイルスチェックを行う

メールに感染したウイルスを検出するのがProScanのメイン機能ですが、それ以外にもさまざまな機能を持っていることは今までの説明で理解できたと思います。ここではさらに事例を踏まえて、それらの具体的な設定方法について説明していきたいと思います。

7.1.1. 非感染メールとウイルス駆除済みメールだけを配信する

ここで説明する構成は、ユーザーが送信者であるか受信者であるかを区別しない場合に使用します。たとえば、感染していないメールとウイルスを駆除したメールだけを配信するように設定する場合は、この方法が便利です。

課題：

- サーバーを経由するすべてのメールのウイルス チェックを行い、ウイルスをすべて駆除します。
- ウイルスを駆除したメールを受信者に配信します。

駆除されたメールは添付ファイル形式でのみ受信者に送付することが可能です。

- ウイルスを駆除したメール、駆除できずに削除したメール、感染の疑いがあるメール、破損しているメール、およびウイルス チェックが不可能なメールに関する情報をその送信者、受信者、および管理者に通知します。
- ログを**/tmp/report.log**ファイルに出力します。

解決方法：次の手順で行ってください。

1. ProScan®構成ファイルのdefault group定義内の**[smtpscan.group]** [smtpscan.action] パラメータを次のように設定します。

```
[smtpscan.group]
Check=yes
AdminAddress=admin@localhost.jp
[smtpscan.action]
NotifyInternalOnly=none
AdminNotify=yes
SenderNotify=yes
RecipientNotify=yes
RecipientAttachReport=delete
RecipientAction=discard
```

[smtpscan.action]セクションは、オブジェクトの種類（検査の結果）ごとに指定することも可能です。その場合は、[smtpscan.action.infected]のように記述します。

2. 処理結果の出力先を**/tmp/report.log**にファイル設定します。

```
[smtpscan.report]
ReportFileName=/tmp/report.log
ReportLevel=15
```

7.1.2. 感染メールを配信する

感染メールを含むすべてのメールを特定のユーザー グループに配信しなければならない場合は、この構成を使用します。

課題：

- すべてのメールのウイルス チェックを行います。
- **urgent**以外のグループに属するユーザーの感染メールからウイルスを駆除します。
- **urgent**以外のグループに属するユーザーのウイルスを駆除できなかったメール、感染の疑いのあるメール、および破損しているメールをQuarantineディレクトリに移動します。
- 遮断したメール、ウイルスを駆除したメール、削除したメール、感染の疑いがあるメール、破損しているメール、およびウイルス チェックが不可能なメールの情報をその送信者、受信者、および管理者に通知します。
- **urgent**グループに属するユーザーが受信者の場合は、感染メールを含めたすべてのメールを配信します。その際、ウイルスに感染している疑いがあることを示す通知を一緒に送信します。

この課題を解決するには、次の手順で行ってください。

1. defaultグループの[**smtpscan.group**][**smtpscan.action**]構成パラメータを次のように設定します。

```
[smtpscan.group]
Check=yes
AdminAddress=admin@localhost.jp
[smtpscan.action]
QuarantinePath=/var/db/quarantine
Quarantine=yes
NotifyInternalOnly=none
AdminNotify=yes
SenderNotify=yes
RecipientNotify=yes
RecipientAttachReport=delete
RecipientAction=discard
```

2.urgentグループの[**smtpscan.group**][**smtpscan.action**]構成パラメータを次のように設定します。

```
[smtpscan.group]
Check=yes
AdminAddress=admin@localhost.jp
[smtpscan.action]
NotifyInternalOnly=noen
AdminNotify=no
SenderNotify=no
RecipientNotify=yes
RecipientAttachReport=unchange
RecipientAction=unchange
```

7.1.3. 受信者へのメール配信を遮断する

一般に、管理者は一部のメールを遮断する必要があります。

たとえば、あるメールがウイルスに感染している疑いがあるが、そのメールには保持しなければならない重要データが含まれているとします。このデータは、ウイルス駆除を実行すると失われてしまうおそれがあります。このような場合、メールを隔離し、専門家に分析してもらうなどの処置が必要になります。

課題：

- サーバーを経由するすべてのメールのウイルス チェックを行い、すべてのウイルスを駆除します。
- 感染メール、感染の疑いがあるメール、パスワードで保護されたメール、およびウイルス チェックが不可能なメールの配信を遮断します。
- 遮断されたメール、ウイルスを駆除したメール、削除したメール、感染の疑いがあるメール、破損しているメール、およびウイルス チェックが不可能なメールの情報をその送信者、受信者、および管理者に通知します。

解決方法：次の手順で行ってください。

構成ファイル**proscan.conf**でパラメータを次のように設定します。

```
[smtpscan.group]
Check=yes
AdminAddress=admin@localhost.jp
[smtpscan.action]
QuarantinePath=/var/opt/proscan/quarantine
Quarantine=yes
NotifyInternalOnly=none
AdminNotify=yes
SenderNotify=yes
RecipientNotify=yes
RecipientAttachReport=remove
RecipientAction=discard
```

7.1.4. 添付ファイルのタイプに基づいてメールをさらにフィルタリングする

メールには、ウイルス感染の危険を伴うタイプのファイル (例：実行ファイル) が添付されている場合があります。感染を防止するために、オブジェクトの名前やタイプに基づいてメールをフィルタリングし、別のディレクトリに隔離して分析することをお勧めします。

一方、感染の危険がないオブジェクトもあります。メールのウイルス チェックを行うサーバーの負荷を軽減するには、感染の危険がある添付ファイルのタイプや名前を前もって検知し、隔離したうえでウイルス チェックを行うことをお勧めします。

課題：

- **users**グループに対して、次の作業を行います。
  - このグループのメールのウイルス チェックを行います。
  - 添付ファイルをフィルタリングし、実行ファイルを検疫ディレクトリに移動します。
  - 感染メールがあれば修復します。ウイルスの駆除が不可能なオブジェクトはメールから除去します。ただし、グループ管理者には、その感染オブジェクトを変更せずに配信します。
  - グループ管理者と受信者にだけ、遮断したオブジェクトの情報を通知します。

- 除去したオブジェクト、感染オブジェクト、破損しているオブジェクト、パスワードで保護されたオブジェクト、およびウイルス チェックが不可能なメールの情報を管理者、送信者、および受信者に通知します。

・その他の受信者に対して、次の作業を行います。

- サーバーを経由するすべてのメールのウイルス チェックを行い、ウイルスをすべて駆除します。
- ウイルスを駆除できなかった感染メール、感染の疑いがあるメール・オブジェクト、破損しているメール・オブジェクト、およびウイルス チェックが不可能なオブジェクトを検疫ディレクトリに移動します。
- パスワードで保護されたファイルをウイルスに感染している疑いがあるという通知と共に受信者に配信します。
- 除去されたオブジェクト、感染オブジェクト、破損しているオブジェクト、遮断されたオブジェクト、およびウイルス チェックできないオブジェクトの情報を受信者、送信者、および管理者に通知します。管理者には、オブジェクトのタイプにかかわらず、すべてそのままの状態で通知に添付します。

この課題を解決するには、次の手順で行ってください。

1. userグループの[**smtpscan.group**]セクション構成パラメータを次のように設定します。

```
[smtpscan.group]
Check=yes
AdminAddress=admin@localhost.jp
[smtpscan.action]
Quarantine=no
NotifyInternalOnly=none
AdminNotify=yes
SenderNotify=yes
RecipientNotify=yes
RecipientAttachReport=delete
RecipientAction=discard
[smtpscan.action.filtered]
QuarantinePath=/var/opt/proscan/quarantine
Quarantine=yes
NotifyInternalOnly=none
AdminNotify=yes
SenderNotify=yes
RecipientNotify=yes
RecipientAttachReport=delete
RecipientAction=discard
[smtpscan.filter]
ByFilename=.*¥.exe
```

2. defaultグループの[**smtpscan.group**] セクションパラメータを次のように設定します。

```
[smtpscan.group]
Check=yes
AdminAddress=admin2@localhost.co.jp
[smtpscan.action]
QuarantinePath=/var/opt/proscan/quarantine
Quarantine=yes
NotifyInternalOnly=none
AdminNotify=yes
SenderNotify=yes
```

```
RecipientNotify=yes
RecipientAttachReport=remove
RecipientAction=discard
[smtpscan.action.protected]
QuarantinePath=/var/opt/proscan/quarantine
Quarantine=yes
NotifyInternalOnly=none
AdminNotify=yes
SenderNotify=yes
RecipientNotify=yes
RecipientAttachReport=remove
RecipientAction=discard
```

7.1.5. パスワードプロテクトされているメールをそのまま配信する

ProScan®では、暗号化された添付ファイルのスキャンを行うことができないため、そのようなファイルが添付されたメールを受けたときには、Protectedステータスを割り当てます。標準ではProtectedステータスのメールは、ウイルス感染ファイルと同じように扱われ、受信者に配信されることはありません。しかしながら、業務の内容によっては、そのようなメールを頻繁にやり取りする場合も考えられますので、そのようなメールをそのまま受信者に配送することも必要な場合があります。

このとき注意しなければならないのは、添付ファイルの内容はスキャンされていないため、本当のウイルスに感染している可能性があるということです。受信者には十分注意するよう促すルールが必要かもしれません。

課題：次の手順で行ってください。

- パスワード保護されたメールをそのまま受信者に配信します。
- 受信者に合わせて通知メールを送り、スキャンされていないことを通知します。

解決方法：

ProSca構成ファイルのグループ定義内に、**[smtpscan.action.protected]**パラメータを次のように設定します。

```
[smtpscan.action.protected]
NotifyInternalOnly=none
AdminNotify=no
Quarantine=no
QuarantinePath=/var/opt/proscan/quarantine
RecipientAction=unchange
RecipientAttachReport=remove
RecipientNotify=yes
SenderNotify=no
```

7.1.6. 登録アドレスのみチェックを行う

ProScan®では、グループ設定により登録してあるアドレスがFromまたはToにある場合のみチェックを行うことが可能です。グループ設定のRecipients,Senders,Domainsと同様にUsersというパラメータで指定します。Usersパラメータで指定するのは、アドレスのリストを指定したファイル名です。

課題：

- 登録したアドレスだけをスキャンの対象とする。
- 登録アドレスは/etc/opt/proscan/usersファイルに書かれている。
- このファイルに書かれているアドレスのみウイルススキャンの対象とする。

解決方法：次の手順で行ってください。

1. 設定ファイルのグループ定義内の[smtpscan.group]セクションでUsersパラメータに/etc/opt/proscan/usersファイルを指定します。（ファイルは事前に作成しておきます。）
2. ウイルスチェック等オプション設置を行います。
3. ProScanの再起動を行い、アドレスリストからDBファイルを作成します。

DBファイルを更新するために再起動を行うか、userdbadmコマンドで反映を行って下さい。

7.2. ファイル システムのウイルス チェックを行う

サーバーのファイル システムをウイルスから保護するには、**proscanfs**モジュールを使用します。**proscanfs**はサーバーのファイルに対してウイルス チェックを行い、感染ファイルや感染の疑いがあるファイルを検知すると、設定に従って処理します。オブジェクトの処理としては、ログやサーバー コンソールへの出力、管理者への通知などのような情報提供と、ウイルスの駆除、オブジェクトの検疫場所への移動、感染オブジェクトの除去などのオブジェクト変更があります。

proscanfsモジュール関連の設定は、構成ファイル**proscan.conf**の [**scanner.***] オプションですべて行えます (63ページのA.2を参照)。

サーバーのファイル システムのウイルス チェックは、コマンド ラインから手動で実行するか、標準の**cron**ユーティリティを使用してスケジューリングを設定します。ウイルス チェックは、サーバーのすべてのファイル システムに対して実行することも、特定のディレクトリやファイルだけをチェックすることもできます。

次にサーバーのファイル システムをウイルスから保護するための典型的な作業について、詳しく説明します。

サーバー全体のウイルス チェックを行うと、大量のリソースを消費し、ウイルス チェックの実行中、サーバーのパフォーマンスが低下することに留意してください。ウイルス チェックとほかのプロセスを同時に実行することはお勧めできません。サーバー全体ではなく、特定のディレクトリに対してウイルス チェックを行うとこの問題を回避できます。

7.2.1. コマンド ラインからディレクトリのウイルス チェックを行う

ProScan®は、サーバーの特定のディレクトリに対してウイルス チェックを行えます。

課題：**/home/user**ディレクトリのウイルス チェックを再帰的に行い、ウイルス感染ファイルを検知した場合は除去します。

/home/userディレクトリ内にあるファイルを再帰的に検査（ディレクトリがあればその中身も）チェックします。

処理結果をメールでadmin@proscan.comに送付します。

解決方法：コマンド ラインで次のように入力します。

```
#proscanfs -r -M -a admin@proscan.com -L 15 -q /home/user
```

7.2.2. ディレクトリの毎日のウイルス チェックをスケジューリングする

ProScan®などスケジューリングされたプログラムは、cronユーティリティで実行します。

課題：毎日0:00に、構成ファイル**/etc/opt/proscan/scanhome.conf**で指定されているウイルス チェ

ック パラメータを使用して**/home**ディレクトリのウイルス チェックを行います。

解決方法：次の手順で行ってください。

1. **/etc/opt/proscan/scanhome.conf**という構成ファイルを新規作成し、必要なウイルス チェック関連パラメータを指定します (43ページの6.2を参照)。

2. cronプロセスの動作ルールを設定するためのファイルを開き (**crontab -e**)、次のように入力します。

```
* 0 * * * /opt/proscan/bin/proscanfs -c /etc/opt/proscan/scanhome.conf
/home
```

7.2.3. オブジェクトを別のディレクトリ (検疫場所) に移動する

ProScan®では、サーバーのファイル システムで検知されたすべての感染オブジェクトを特別なディレクトリに移動するように設定できます。

この機能は、ディレクトリのウイルス チェック中に重要なデータを保存したファイルの感染が検知された場合場合などに利用できます。これは、ウイルスを駆除するとデータの一部が失われるおそれがあるためです。このような場合には、感染オブジェクトをいったん特別なディレクトリに隔離します。

サーバーのファイル システムに検疫ディレクトリを常に配置しておく場合は、構成ファイルのExcludeパラメータでそのディレクトリの完全パスを指定すると、そのディレクトリがウイルス チェックの対象から除外されます。

課題：**/tmp/download** 配下のすべてのファイルをウイルス チェックし、感染オブジェクトを完全パスの情報と共に**/tmp/infected**ディレクトリに移動します。このとき、反復的なウイルス チェックは無効にします。さらに、感染オブジェクト、感染の疑いのあるオブジェクト、および破損したオブジェクトの情報を、レポート ファイルに出力します。

解決方法：次の手順で行ってください。

コマンド ラインで次のように入力します。

```
#proscanfs -m 1 -M -d /tmp/infected /tmp/download
```

ProScan®の検査時の移動は、パス情報を持ったまま指定ディレクトリ先に移動します。ファイルの属性情報もそのままです。

第8章 よく寄せられる質問

ここでは、ProScan®のインストール、設定、および使用法に関する質問とその回答を示します。

質問：ProScan®は、Xアーキテクチャのプロセッサ (PowerPC、Alpha、PA-RISCなど) をサポートしていますか。

現在のバージョンではサポートされていません。

質問：ProScan® は、Linuxのディストリビューション上で動作しますか。

ProScan® for Mailserver は、RedHat、Debianの各ディストリビューション上でテスト済みです。パッケージは、これらのOS用に作成されています。
サポートしているOSのバージョンについては、2ページの1.3を参照してください。

ご使用のディストリビューションがサポート対象のOSと完全な互換性を保持している場合(たとえば、CentOSはRedHat Linuxと互換性がある)、重大な問題が発生する可能性はきわめて低いと言えます。

ProScan®は、プロマークのサポート対象リストに掲載されていないディストリビューション上では、正しく動作しない可能性があります。正しく動作しない場合、一般にその原因はOSの特性にあります。たとえば、ご使用のディストリビューションで別のバージョンのライブラリが使用されていたり、システム初期化スクリプトが異なる場所に配置されている可能性があります。このような場合、プロマークのテクニカル サポート サービスではサポートできません。

質問：tgz形式またはtar+gz形式のアーカイブを展開するには、どうすればよいですか。

.tgzまたは.tar.gz形式のアーカイブを展開するには、次のコマンドを使用します。

```
tar zxvf <archive_name>
```

詳細については、man (1)の**tar**プログラムの説明を参照してください。

質問：なぜキー ファイルが必要なのですか。キー ファイルがなくてもProScan®は動作しますか。

ライセンス キーがなければ、ProScan®は動作しません。
ProScan®のご購入を検討中の方には、一時キー ファイル (試用版キー) を提供しています。一時キー ファイルの有効期間は30日です。この期間が過ぎると、キーは無効になります。

質問：製品ライセンスが失効するとどうなりますか。

失効しても、ProScan®を引き続きご利用になれます。ただし、ウイルス データベース（VDF）更新機能は使用できません。つまり、古いデータベースを使用してのみ、感染オブジェクトを検出できます。
proscanupモジュールを使用してプロマークのWebサイトから最新のウイルス データベースをダウンロードきなくなります。proscanupを使用せずにダウンロードしたウイルス データベースをProScan®で使用することはできません。
したがって、新種のウイルスからファイルを保護することはできなくなります。
また、期限が切れたProScanに新しいVDFファイルを更新するとDEMOモードとなり、ウイルスチェック機能が働かなくなりますのでご注意下さい。

質問：ウイルス データベースを1時間1回更新するよう、crondを設定しています。しかし、proscanupがWgetプログラムを検知しません。なお、コマンド ラインから起動したときには、何の問題もありませんでした。

ここで重要な点は、crondユーティリティは独自の環境変数を使用するということです。この場合、Wgetプログラムへのパスが PATHパラメータの中で指定されていない可能性があります。
Wgetへのパスを追加するには、**/etc/crontab**ファイルのPATH環境変数を変更します。

質問：ProScan® for Unix Mail Serverをインストールし、Postfixメール システムに統合するまではすべて正常に完了したのですが、その後メールの配信が停止し、次のようなエラーがメールログに出力されました。

```
Sep 23 15:17:03 server postfix/lmtp[1678]:8238C38987:to=<user@server.org
<mailto:user@server.org>>, relay=none, delay=1, status=bounced
(localhost:host not found)
```

どうすればよいですか。

このような問題は、次の場合に発生します。

- DNSのlocalhostドメインが指定されていません (RFC 2606の必要要件)。RFCに従ってDNSを構成してください。詳細については、次のWebページを参照してください。
  http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc2606.html
- localhostが/etc/hostsファイルに指定されていません。通常は、これを**localhost=127.0.0.1**に設定します。localhostにこのアドレスを指定してください。

質問：ProScan®が動作しません。どうすればよいですか。

まず、その問題への対策がこのマニュアル (特にこの章) またはWebサイトに記載されているかどうかを確認します。
また、ProScan®の購入元にサポートを依頼するか、弊社のテクニカル サポート サービス (support@promark-inc.com) 宛にEメールを送信することもできます。
できるだけ早く回答を入手できるようにするため、次の点を守ってください。

1. メールサブジェクトにサーバのOS、問題が発生したモジュールの名前、および問題の概要を記述します。たとえば、「**Linux、正式ユーザー リストの設定を利用できない**」のように記述します。
2. Eメールをテキスト形式で作成します。HTML形式のメールは送信しないでください。
3. メール本文の先頭に、OSとProScan®パッケージの正確なバージョン、およびキー ファイルの名前を記述します。
4. 問題を簡潔に説明します。サポート サービス要員はEメールを読むとき、ユーザーが抱えている問題について何も知りません。サポート サービス要員が問題を十分に理解し、その現象を再現しなければ、サポートを行えません。
5. 次のデータを1つのアーカイブにまとめ、テクニカル サポート サービスに送信します。
   - メール エージェント (MTA) のすべての構成ファイル
   - **/etc/opt/proscant**ディレクトリのファイル
   - メール システムのレポート ファイル
   - ウイルス チェック モジュールのレポート ファイル (例：**/var/opt/proscan/log/proscan.log**)
   - **ps -ax**コマンドを実行してコンソールに出力された情報
   - キー ファイル
6. ご使用のシステムが次の条件に当てはまるかどうかを、Eメールに記述してください。
   - SCSIコントローラ搭載の有無
   - 非常に古いプロセッサや最新のプロセッサの搭載の有無、または複数プロセッサ構成の有無
   - RAMの容量が64 MB以下または2 GB以上であるかどうか
7. 毎日の概算トラフィック量、およびサーバーの負荷が一時的に高くなる時間帯があるかどうかを記述します。

質問：コンソールに出力された情報をファイルに保存するには、どうすればよいですか。

ProScan®の動作中にコンソールに出力された情報を保存するには、構成ファイルで適切な設定を行うか (63ページのA.2を参照)、またはコマンド ラインで次のように入力します。

```
$ some_app > ./text_file 2>&1
```

パラメータの説明：

some_app — ファイルに保存したい、アプリケーション、標準出力、およびエラー メールの行。
text_file — 情報の保存先ファイルへの完全パス。

例：
```
$proscanupr > ./updater.log 2>&1
```
上記の場合、proscanuprモジュールの標準出力メールとエラー メールが、カレント ディレクトリ内のupdater.logファイルに出力されます。

質問：侵入者にウイルス データベースを改ざんされる可能性はありますか。

侵入者がプロマークのWebサイトからウイルス データベースをダウンロードし、ウイルス格納用ディレクトリにコピーする可能性はあります。ただし、そのウイルス データベースはProScan®の実行時に使用されません。
ウイルス データベースにはそれぞれ一意の署名がなされており、ウイルス データベースを使用する際にProScan®が検査します。署名が不正であるか、ウイルス データベースの日付がライセンスの失効日より遅い場合、そのウイルス データベースは使用されません。

質問：インストール時にWebminモジュールをインストールしたのですが、アイコンがありません。

バージョン6.0.5よりWebminモジュールはインストールされません。Webminモジュールのサポートは終了しました。

質問：Proxy設定をしたのですが、アップデートできません。

アップデートできない理由は色々と考えられますが、Proxy経由で行う場合にはwgetのProxy設定が正しく行われているか確認してください。ProScanでのProxy設定はwgetのProxy設定に自動で反映されます。

第9章　ProScan®をアンインストールする

ProScan® をアンインストールするには、次の条件を満たしている必要があります。

・superuser権限 (**root**ユーザー、またはUID=0であるユーザー) を持っていること。ProScan®をアンインストールするときにこの権限がない場合は、**root**ユーザーとしてログオンする必要があります。

サーバーからProScan®をアンインストールするには、パッケージを展開したディレクトリに移動し、コマンド ラインで次のように入力します。

```
./uninstall.sh
```

uninstallerが起動すると、アンインストールタイプを問い合わせてきます。1番目はMTAの設定を元に戻す処理を行います。2番目はProScanの完全アンインストールです。

処理を選択すると自動的にアンインストールされます。アンインストールが完了すると、通知メッセージがコンソールに出力されます。

付録A. ProScan®に関する補足情報

この付録では、インストールしたProScan®パッケージのディレクトリ ツリー (A.1)、構成ファイルの内容 (A.2)、および各モジュールに関するコマンド ライン キーとリターン コード (A.3～A.11) について説明します。メール システムの構成ファイルとウイルス駆除のためのスクリプト ファイルの例を示します。

A.1 製品ファイルの配置ディレクトリ

デフォルトのパスをそのまま使用してProScan®をインストールすると、配布ファイルは次の場所に配置されます。（Linuxの場合）

/etc/opt/proscan/ — ProScan®の構成ファイル、および設定情報を保存したその他のファイルが配置されるディレクトリ
- **proscan.conf** — 構成ファイル
- **domains**— 対象ドメイン指定ファイル
- **template/japanese/notify_sample** — 通知テンプレート ファイル（日本語）

/opt/proscan/ — ウイルス チェック関連ファイルが配置されているメイン ディレクトリ。このディレクトリの下位には、次のディレクトリとファイルがあります。
- **/opt/proscan/bin/** — ProScan® for Mail Serverの実行ファイルが配置されるディレクトリ
  - **proscan** — ProScan® メインプログラム。
  - **savapi** — ProScan® Engine Serverプロセスの実行ファイル。
  - **proscanms** — ProScan® Proscanmsメール フィルタの実行ファイル。
  - **proscanfs** — サーバーのファイル システムのウイルス チェックを行うProScan® On-Demand Scanner モジュールの実行ファイル
  - **proscanup** — ウイルス データベースを更新するProScan® Proscanupモジュールの実行ファイル
  - **licenseviewer** — ProScan®のライセンス情報を表示する実行ファイル
  - **userdbadm** — ユーザDBを管理する実行ファイル

/var/opt/proscan/db/keys — ライセンスキーが配置されるディレクトリ
/var/opt/proscan/run/.savapi_x.0 — savapiプロセスに接続するために使用するローカル ソケット
/var/opt/proscan/run/.pid_savapi_xxx — **savapi**プロセスIDを含むファイル

FreeBSDの場合は、上記ディレクトリの/etc/opt/proscanを/etc/proscanに、/opt/proscanを/usr/local/proscanに、/var/opt/proscanを/var/proscanにそれぞれ置き換えて読んでください。以降も同じです。

A.2 ProScan®の構成ファイル

デフォルトでは、ProScan® には**proscan.conf**という構成ファイルが付属しています。**proscan.conf**では、多数のプログラム動作パラメータが指定されています。ここでは、この構成ファイルのすべてのパラメータ セクションについて詳しく説明します。パラメータにデフォルト設定が用意されていれば、その値があらかじめ指定されています。

バージョン6.0.3.8より、パラメータに外部ファイルを指定できるようなりました。そのため、今まであった1行8000文字の制限が解除されています。“file:フルパスファイル名”のように指定してください。

[path] セクションには、重要なファイルへのパスを定義するパラメータがあります。これらのファイルへのパスを正しく指定しなければ、ProScan®は動作しません。

LicensePath=/var/opt/proscan/db/keys — ライセンス キーが保存されているディレクトリへの完全パス
LocalSocketPath=/var/opt/proscan/run — savapiプロセスに接続するために使用するローカル ソケットおよびPIDファイルを格納するディレクトリへの完全パス
UserFile=/var/opt/proscan/db/.users.db — ライセンス管理用ユーザのDBファイルへの完全パス
TempPath=/var/opt/proscan/tmp — 一時ファイルを保存するディレクトリへの完全パス
WgetPath=/usr/sbin/wget — wgetコマンドへの完全パス（システムに合わせて設定）
LightGrayList=/etc/opt/proscan/lightgray.lst — グレイリストチェック時の自動ホワイトリストファイルへの完全パス
DarkGrayList=/etc/opt/proscan/darkgray.lst — グレイリストチェック時の一時拒否リストへの完全パス
S25RWhiteList=/etc/opt/proscan/s25r-white-list.txt — S25R方式のホワイトリストを定義したファイルへの

完全パス
CheckStartTimeFile= /var/run/filescan.start.time — 前回のファイルスキャン起動時間を退避するファイル

[locale] セクションには、メール通知の%SCANSTATUS%マクロを置き換えるテキストと日時の形式を指定するパラメータが含まれます。

ProtectedMessage — パスワードで保護されたオブジェクトを通知するメールの%SCANSTATUS%マクロを置き換えるテキストです。
SuspiciousMessage — 疑わしいオブジェクトを通知するメールの%SCANSTATUS%マクロを置き換えるテキストです。
ErrorMessage — スキャンに失敗したオブジェクトを通知するメールの%SCANSTATUS%マクロを置き換えるテキストです。
InfectedMessage — 感染したオブジェクトを通知するメールの%SCANSTATUS%マクロを置き換える使用するテキストです。
OtherMessage — ウイルス チェックに失敗したオブジェクトを通知するメールの%SCANSTATUS%マクロを置き換えるテキストです。
FilteredMessage — ファイル名、タイプ、サイズ、件名に基づいてフィルタリングされたオブジェクトを通知するメールの%SCANSTATUS%マクロを置き換えるテキストです。
SpamHighMessage — スパム高レベル判定時の%SCANSTATUS%マクロを置き換えるテキストです。
SpamLowMessage — スパム低レベル判定時の%SCANSTATUS%マクロを置き換えるテキストです。
TimeFormat=%H:%M:%S — メール通知に表示される、strftime規格に準拠した時刻の形式
12時間表示 (am/pm) に変更するには、**%I:%M:%S %P**と指定します。

DateFormat=%d/%m/%y — メール通知に表示される、strftime規格に準拠した日付の形式。
日付の形式は、**%y/%m/%d**または**%m/%d/%y**などに変更することもできます。

[scanner.options] セクションでは、サーバーのファイル システムのウイルス チェックに関するパラメータを指定します。

Recursion=yes — ディレクトリを再帰的にチェックするモード。このモードを無効にするには、このパラメータを**no**に設定します。この設定が**no**になっているとディレクトリのチェックは行われません。
Symlink=yes — シンボリックリンク先のファイルをチェックするモード。このモードを無効にするには、このパラメータを**no**に設定します。
SendMail=no — 結果をメールで送信するモード。このモードを無効にするには、このパラメータを**no**に設定します。送信先アドレスは、**ReportAddress**で設定します。
ReportAddress=E-Mail address — 結果をメールで送信するあて先。
MaxScanTime=300 — ファイルをスキャンするときのタイムアウト値。
SaveDirectory=Directory name — 感染オブジェクトの移動先ディレクトリ。
MaxRecursion=0 — 最大許容多重圧縮度を指定します。
MaxSize=0 — 最大ファイルサイズを指定します。
MaxRatio=150 — 最大許容圧縮率を指定します。
ReadTimeout=120 — ソケット読込時のタイムアウト値を指定します。
ArchiveScan=yes — アーカイブの個々のファイルをスキャンするかどうか指定します。
MailboxScan=yes — メールボックスファイルの個々のメールをスキャンするかどうか指定します。
MaxCheckLevel=50 — 最大ディレクトリ深度を指定します。
UpdateOnly=no — 前回スキャン時から更新されたファイルのみスキャンするかどうかを指定します。

[scanner.object] セクションでは、セクションでは、サーバーのファイル システムをウイルスから保護する際に各種の単独オブジェクトに適用するアクションを指定します。

ExcludeMask=mask1:mask2:...:maskN — ウイルス チェック対象から除外するファイル マスク。デフォルトでは、すべてのファイルが対象となります。このパラメータを指定した場合には、チェック中にこのマスクにマッチするファイルはチェックされません。
IncludeMask=mask1:mask2:...:maskN — ウイルス チェック対象とするファイルのマスク。デフォルトでは、すべてのファイルが対象となります。このパラメータを指定した場合には、ここで指定したファイルだけがチェックされます。
ScanLevel=1 — アクション対象となるオブジェクトを指定します。スキャン時にこのパラメータで設定したオブジェクトは、**MatchAction**で指定された処理が実行されます。指定方法は以下の4種類を論理

和で行います。（ビットの論理和です）デフォルトは15ですべてのオブジェクトが対象です。
- **0 —** 何もしません。チェックのみです。
- **1 —** ウイルス感染オブジェクト。
- **2 —** 暗号化オブジェクト。
- **4 —** 感染の疑いがあるオブジェクト。
- **8 —** スキャンに失敗したエラーオブジェクト。

MacthAction=action — 感染ファイルの検知時に実行するアクション。感染ファイルの修復モードが有効になっている場合、ウイルスを駆除できないオブジェクトにこのアクションが実行されます。アクションには、次の値のいずれかを設定できます。
- **none —** 何もしません。チェックのみです。
- **move —** ファイルを**SaveDirectory**に反復的に (完全パスを付加して) 移動します。
- **delete —** ファイルを削除します。

[**scanner.report**] セクションでは、proscanfsモジュールの処理結果レポートの生成に関するパラメータを指定します。

ReportFileName=/var/opt/proscan/log/filescanner.log — 処理結果を記録するレポート ファイルの名前
ReportLevel=3 — 処理結果のレポート内容を指定します。
- 1 — エラー
- 2 — スキャン結果
- 4 — サマリ
- 8 — 詳細

Facility=user — レポートをSyslogに出力する場合のファシリティを指定する。
Priority=notice — レポートをSyslogに出力する場合のプライオリティを指定する。

[**scanner.display**] セクションでは、モジュールの動作状況 (ウイルス データベース読み込み処理の進行状況およびウイルス チェック中のファイルに関する情報) をリアルタイムで出力するモードに関するパラメータを指定します。

ShowLevel=255 — ファイルチェック時の動作をコンソールに出力するレベルを設定します。
- 1 — エラー
- 2 — スキャン結果
- 4 — サマリ
- 8 — ウイルスチェック
- 256 — 詳細

OutputFileName=Filename — 出力先を指定します。このパラメータが設定されていないとコンソールに出力されます。[scanner.report]の内容との違いは、スキャンしたファイル情報を出力します。

[**aveserver**] セクションでは、**savapi**モジュールの動作および処理レポートの生成に関するパラメータを指定します。

ExecUser=root — AVエンジンの実行ユーザを指定します。
ProxyMode=no — Proxyモードで起動する場合にyesと指定します。デフォルトはnoです。
ProxyScanners=24 — Proxyモードの場合の起動プロセス数を指定します。Max80でデフォルトは24です。
ReportFileName=/var/opt/proscan/log/aveserver.log — AVエンジンの処理結果を記録するレポート ファイルの名前。
ReportLevel=3 — レポートの情報レベル
Facility=user — syslog出力時のFacilityを指定します。
Priority=notice — syslog出力時のPriorityを指定します。
Timeout=5 — AVEとの通信タイムアウト値を指定します。
AppendFile=filename — AVEの設定を追加するファイルを指定します。

[**updater.options**] セクションでは、**proscanup**モジュールの動作に関するパラメータを指定します。

ExtraWgetOptions — Wgetパッケージの情報オプション
KeepSilent=no — proscanupモジュールの動作情報をコンソールに出力するモード。このモードを有効にするには、このパラメータをYesに設定します。
UpdateHost=update.promark-inc.com — 更新用サーバーのホスト名を設定します。カンマで区切って複数

指定することが可能です。
UpdatePort=80 — 更新用サーバーのポート番号を設定します。
UpdatePlotocol=HTTP — 更新用サーバーのプロトコルを設定します。
ReloadApplication=yes — ProScan®のモジュールが更新された場合に、モジュールを自動で反映するかどうかを指定します。このパラメータがyesに設定されていると自動で最新モジュールに入れ替わります。
ShowExternalCmdOutput=no — 外部プログラム (例：Wget) の情報をコンソールに出力するモード。このモードを有効にするには、このパラメータをyesに設定します。
HTTPProxyServer=host_name — Proxy経由でのアップデートを行う場合にProxyサーバのホスト名またはIPアドレスを指定します。
HTTPProxyPort=8080 — Proxyサーバのポートを指定します。
S25RWhiteListUrl — S25R方式のホワイトリストのダウンロード先を指定します。noneを設定するとダウンロードを行いません。
RetryTimes=5— アップデートじのリトライ回数を指定します。
RetryInterval=10— アップデートじのリトライ時の間隔を秒数で指定します。
AviraProductFile — savapiのプロダクトファイルを指定します。（OS、バージョンによって異なります）

[updater.report] セクションでは、**proscanup**モジュール動作レポートの生成に関するパラメータを指定します。

ReportFileName=/var/opt/proscan/log/updater.log — モジュール処理結果を記録するレポート ファイルの名前
ReportLevel=1 — レポートの情報レベル
- 1 — 通常メッセージ
- 128 — デバッグメッセージ

Facility=user — syslog出力時のFacilityを指定します。
Priority=notice — syslog出力時のPriorityを指定します。

[smtpscan.license] セクションでは、**ProScan®**のライセンスに関するパラメータを指定します。

LicenseWarningNotifyUsers — Userライセンス数の残りがこのパラメータで設定した値以下になったら通知メールを送ります。デフォルトは5です。
LicenseWarningNotifyDays — 更新期限までの残り日数がこのパラメータで設定した値以下になるとProScan®の起動のたびに通知メールを送ります。デフォルトは14です。
LicenseWarningNotifySendTime — ユーザ数のリミットに近づいた事を知らせる通知メールを送信するタイミングを指定します。デフォルトは6です。この時刻にproscanupが起動されて、リミット通知を送る条件にマッチした場合に通知メールが送られます。
LicenseWarningNotifyAddress=root@localhost — ライセンス関連の通知先アドレスを設定します。省略すると**SupervisorAddress**が使用されます。
DomainCheck=yes — このパラメータがyesに設定してある場合は、domainsファイルに書かれているドメインのメールだけがライセンス対象となります。それ以外のメールはチェックされません。noの場合は全てのメールがチェック対象となります。
LicenseCountType=from — ライセンス自動カウントの対象となるアドレスを指定します。fromかtoです。デフォルトはfromです。

[smtpscan.limits] セクションでは、メールのウイルス チェックを制限するパラメータを指定します。

NotSendNotifyTo=MAILER-DAEMON@ — 通知を送信しないアドレス (アドレス マスク)、複数指定する場合には、カンマで区切って並べます。
MaxCheckTime=0 — savapiプロセスから応答が返されるまでの最大の待機時間。0を設定すると、無制限になります。
MaxRecipient=200 — 1つのメールの受信者の最大数。この数までウイルス チェックの対象となります。
MaxConnectTime=10 —savapiに接続するまでの最大待ち時間。
MaxRecursion=5 — アーカイブの再帰チェックをする深さ。デフォルトは5.。
MaxArchiveSize= 134217728— 圧縮されたアーカイブの展開後のファイルサイズ。（複数のファイルをアーカイブしていた場合には、展開されたファイルひとつひとつの最大サイズとなります。）
MaxRatio=150 —圧縮されたアーカイブの展開後のファイルサイズ比の最大値。（メール爆弾のような添付ファイルを防ぐためのものです。）デフォルトは150倍です。
Timeout=600 — メール受信時の無通信タイムアウト値を指定します。デフォルトは600秒です。

SpamCheckTime=1200 — グレイリストチェックを行う場合に、一時拒否したメールの再送受け入れ時間を設定します。

[**smtpscan.general**] セクションでは、**ProScan®**が処理したメールを配信するためのパラメータを指定します。

NotifyFromAddress=proscan@localhost — すべての通知の送信元アドレス
SupervisorAddress=proscan@localhost — デフォルトで使用される宛先アドレス
ForwardMailer=smtp:(/usr/sbin/sendmail -bs -C/etc/sendmail.cf) — その後のルーティングのためにすべてのメールと通知を渡すサーバーまたはプログラムの名前（インストーラにより、お使いのメールシステムに合わせた設定が行われます。変更しないで下さい。）
QmailLocalCheck=yes — qmailにおいてqmail-localから起動された場合にチェックを行うかどうかを指定します。デフォルトはyesですが、二重チェックとなり負荷が高くなるのでnoで運用されることをお勧めします。
RepairFile=no — ウイルス検出時にファイルの修復を試みるかどうかを指定します。デフォルトはnoです。
LibmilterSocket=local:/var/run/proscan.sock — Sendmail Libmilterにおいて利用するソケットのファイルを指定します。
DHACheck=no — SMTP接続時に受け取るべきアドレスをチェックするかどうかを指定します。受け取りアドレスは事前にDBに登録しておく必要があります。（DHAチェック機能はspamチェック機能と同様にMTAがメールをキューに格納する前にProScanでチェックするような構成の場合に有効です。）
DHALimit=20 — DHAチェックを行う場合に、１セッションあたりのエラー許容数を指定します。DHAは、一度に多くの辞書アドレスを使うので、大量のエラーが発生する場合には攻撃を受けていると考えられます。
DHAAction=userunknown — DHAチェックでエラーとなった場合のアクションを指定します。userunknown,discard,tempfailを指定できます。discardを指定した場合にはエラーを返しません。
RecipientsFile — 受け取るべきアドレスを設定したDBファイルを指定します。このファイルはuserdbadmコマンドで作成します。
GatewayIP — メールを内部で転送しているような環境で中継MTAをspamチェックで無視する場合にここに中継MTAサーバのIPアドレスを指定します。
HureMacroDetect=no — マクロのヒューリスティック検査を行うかどうかを指定します。
HureLevel=3 — マクロのヒューリスティック検査のレベルを指定します。
GatewayIP — メールGWのIPアドレスを指定します。ここからのメールは送信元MTAと判断しません。
ResolveIP=yes — IPアドレスの逆引きを行うか指定します。noの場合には逆引きを行いません。

[**smtpscan.report**] セクションでは、**smtpscan**モジュールの処理結果レポートの生成に関するパラメータを指定します。

ReportFileName=/tmp/smtpscan.log — モジュールの処理結果を記録するレポート ファイルの名前
ReportLevel=8191 — レポートレベル
Facility=user — syslog出力時のFacilityを指定します。
Priority=info — syslog出力時のPriorityを指定します。

以降のセクションは、グループセクションとして、グループごとに個別設定が可能です。
必ず、_group ～ _end_group 内に記述する必要があります。

[**smtpscan.group**] セクションでは、グループの送信者と受信者のメールの処理に関するパラメータを指定します。

Check=yes — サーバーを経由するメールのウイルスをチェックします。このモードを無効にするには、このパラメータをnoに設定します。
AdminAddress=postmaster@localhost — グループ管理者のアドレス
Domains — グループのドメイン (ドメイン マスク)
Recipients — グループのメールの受信者のアドレス (アドレス マスク)
Senders — グループのメールの送信者のアドレス (アドレス マスク)
Users — グループのメンバーのアドレスを定義したファイル名
※ DomainパラメータとRecipients,SendersパラメータおよびUsersパラメータは排他設定です。
SpamCheck — スパムチェックを行います。このモードを無効にするには、このパラメータにnoを設定します。

[**smtpscan.wbl**] セクションでは、グループのメール受信時の処理に関するパラメータを指定します。

送信元MTAのIPアドレスを元にチェックを行います。

AcceptIP=127.0.0.1 — 許可IPアドレスを設定します。
AcceptName=localhost — 許可ホスト名を設定します。Posix正規表現が使えます。
AcceptNet=192.169.0.0/24 — 許可ネットワークを設定します。
AcceptLevel=9 — Accept時の以降の処理を指定します。レベルについてはドキュメント内を参照してください。
RejectIP=61.197.232.1 — 拒否IPアドレスを設定します。
RejectName=¥.ipt¥.aol¥.com$ — 拒否ホスト名を設定します。Posix正規表現が使えます。
RejectNet=192.168.100.0/28 — 拒否ネットワークを設定します。
RejectAction=discard — 拒否した場合のメールの扱いを設定します。メールを拒否しエラーを通知する（reject）、エラーを通知せずにメールを破棄する（discard）が選択できます。

[**smtpscan.action**] セクションでは、グループの感染メール受信時の処理に関するパラメータを指定します。

Quarantine=yes — メールのオブジェクトの検疫モード。このモードを無効にするには、このパラメータをnoに設定します。
QuarantinePath=/var/opt/proscan/quarantine — 検疫ディレクトリのパス
AdminNotify=yes — メール処理の結果を管理者に通知するモード。このモードを無効にするには、このパラメータをnoに設定します。
SenderNotify=yes — メール処理の結果を送信者に通知するモード。このモードを無効にするには、このパラメータをnoに設定します。
RecipientNotify=yes — メール処理の結果を受信者に通知するモード。このモードを無効にするには、このパラメータをnoに設定します。
RecipientAttachReport=delete — スキャン対象となったオリジナルメールの添付形態を指定するパラメータです。オリジナルのまま添付(unchange)、感染していた場合に、感染部分を削除したメールを添付(delete)、メールを添付しない(remove)が選択可能です。
RecipientAction=discard — スキャン結果でチェックされたオリジナルのメールを受信時にどのような処理を行うか指定するパラメータです。そのまま配送する(unchange)、拒否する(reject)、破棄する(discard)が選択できます。
NotifyInternalOnly=none — 通知メールを管理対象ドメインのみにする場合に設定を行うパラメータです。送信者（sender）、受信者（recipient）、送受信者両方（both）が管理対象ドメインに属する場合にはそれぞれ () 内のパラメータを指定します。ドメインに関係なく通知する場合にはnoneを指定します。

さらに、このセクションはオブジェクトのステータスごとに処理を指定することができます。次に概要を説明します。

[**smtpscan.action.<objects_status>**]というセクションを作成することで、各ステータスごとの処理を記述することが可能です。**<object_status>**には以下の6つが指定可能です。

- infected　ウイルス感染時
- protected　暗号化ファイルチェック時
- suspicious　感染の疑いがあるメールをチェック時
- error　スキャンできないとき
- other　ファイルが壊れているとき
- filtered　フィルタールールにマッチしたとき

[**smtpscan.notify**] セクションでは、オブジェクトのステータスを問わず、送信者、受信者、管理者への通知に共通のパラメータを指定します。

Template=/etc/opt/proscan/template/japanese/notify_sample — 通知テンプレートのファイル名。通知はこのテンプレートを利用して生成されます。
ContentType=text/plain — メールのMIMEタイプ
Subject=infected object — 通知メールの件名
Charset=ISO-2022-JP — テンプレートのコードページの名前

構成ファイルの [smtpscan.notify.<member>.<object_status>] のセクションは、特定のステータス(感染など) のオブジェクトと特定の通知受信者 (管理者、送信者、受信者) に対する通知パラメ

ータの指定をするだけのために作成し、使用します。これらのセクションのパラメータは、[smtpscan.notify] に記載されているパラメータと同じで、ユーザーは値を設定するだけです。したがって、感染メールの送信者に特別の通知パラメータを設定する場合は、[smtpscan.notify.sender.infected] セクションで設定します。

[smtpscan.filter] セクションでは、グループのメールのフィルタリングルールに関するパラメータを指定します。

以下のパラメータはBySizeを除いてすべてPOSIX正規表現で指定可能です。

BySubject — メールの件名をチェックします。
BySize — ファイルのサイズをチェックします。ここで指定したサイズより大きい場合に、アクションが実行されます。
ByFilename — 添付ファイル名をチェックします。
ByMIMEtype — 添付ファイルのMIMEタイプをチェックします。
ByHeader — メールのヘッダ部分をチェックします。

マッチした場合にアクションが実行されます。（Filteredオブジェクトとしてステータスがセットされます。）

[smtpscan.spam] セクションでは、グループのスパムチェックに関するパラメータを指定します。

DracDB=btree:/etc/mail/dracd.db — drac DBチェックを行う場合にDBタイプとDBファイルを指定します。DBタイプの省略時はbtreeが指定されたものとみなされます。タイプとしては、hash,text,dumpが指定可能です。プレーンなテキストファイルの場合はtextを指定して下さい。行頭のIPアドレスでチェックします。DBのタイプがわからない場合にはdumpでチェック可能です。（但し、dumpの効率は良くありません）
GrayCheck=no — グレイリストチェックを行う場合はyesを指定します。
RBLcheck=yes — RBLチェックを行う場合はyesを指定します。
RBLHostName=dnsbl.njabl.org — RBLチェックを行う場合に問合せ先ホスト名を設定します。
SubjectCheck=未承諾広告※ — サブジェクトのチェックパターンをPosix正規表現で設定します。
WBLAccept=*host_ name* — 一旦スパムと判定されたメールを救済するMTAを指定します。(正規表現)
WBLReject=*host_name* — あらかじめ判明しているスパム送信ホストを指定します。（正規表現）

[smtpscan.spam_action.<spam_level>] セクションでは、グループのスパムと判定されたメールに対するアクションに関するパラメータを指定します。

AddHeader=X-spam-status: <spam_level> — スパムと判定されたメールにヘッダ情報を追加します。
AddSubject=[SPAM] — スパムと判定されたメールのサブジェクトの先頭に追加します。
Deliver=yes — スパムと判定されたメールを配送する場合はyesと設定します。noの場合には配送されません。
Notify=no — メールがスパムと判定された場合に、通知メールを送るかどうかを指定します。yesの場合には通知メールが送られます。
Save=no — スパムメールを保存する場合にyesと指定します。
SavePath=/var/opt/proscan/spam — スパムメールの保存先を指定します。

[smtpscan.spam_notify.<spam_level>] セクションでは、グループのスパムチェックに関する通知メールのパラメータを指定します。

[smtpscan.notify]セクションと同じ設定です。

A.3 proscanfsモジュールに関するコマンド ライン キー

プログラムをコマンド ラインから起動する際、構成ファイルのパラメータを変更するには、コマンド ライン キーを使用します。以下に詳しく説明します。

ヘルプに関するオプション		
-h		proscanfsモジュールに関するヘルプをコンソールに出力します。
-v		プログラムのバージョンを表示します。
構成に関するオプション		
-c <file_path>		代替構成ファイル**<file_path>**を使用します。
ウイルス チェックに関するオプション		
-r/R		ディレクトリ再帰チェックの有効・無効を切り替えます。
-s/S		リンク先チェックの有効・無効を切り替えます。
-E <mask1:…>		対象外ファイルを指定します。
-I <mask1:…>		対象ファイルを指定します。
-m <objects>		対象となるオブジェクトを指定します。
	1	ウイルス感染ファイル
	2	暗号化されているファイル
	4	ウイルスの感染が疑わしいファイル
	8	チェックでエラーとなったファイル
-C		チェックのみの動作となります。
-D		上記オブジェクトにマッチした場合にそのファイルを削除します。
-M		上記オブジェクトにマッチした場合にそのファイルを移動します。 ※オプションC, D, Mは排他関係にあります。
-d <path>		Mオプションが指定された場合の移動先を指定します。
レポート生成に関するオプション		
–q		メッセージをコンソールに出力しません。
-o <fname>		処理結果を出力するファイルの名前を設定します。ファイル名を設定しない場合、コンソールに出力されます。
-a <address>		処理結果をメールで送付します。
-l <fname>		ログファイルを指定します。
-L <level>		ログに格納される情報を設定します。**<level>**に次の情報レベルを指定できます。
	1	エラーメッセージを出力します。
	2	スキャン内容を出力します。
	4	設定内容を出力します。
	8	ファイル処理に関するメッセージを出力します。
	16	詳細メッセージを出力します。
-n <level>		コンソールに出力するウイルス チェック レポートの情報レベルを設定します。**<level>**に次の情報レベルを指定できます。
	1	サマリ表示します。
	2	感染ファイルを表示します。
	256	非感染ファイルも出力します。

A.4 proscanfsモジュールのリターン コード

proscanfsモジュールの実行中に返されるコードは、次のとおりです。

0	正常終了しました。
1	オプションが足りません。
2	不正なパラメータです。
3	設定ファイルが読み込めません。
4	ログファイルがオープンできません。
5	ライセンスが異常です。
99	ファイルが指定されていません。

A.5 proscanモジュールのコマンド ライン キー

ヘルプに関するオプション	
-h	proscanモジュールのヘルプをコンソールに出力します。
-v	プログラムのバージョンを表示します。
構成に関するオプション	
-c <file_path>	代替構成ファイル**<file_path>**を使用します。
-u <user>	起動ユーザを指定します。

A.6 proscanモジュールのリターン コード

proscanモジュールの実行中に返されるコードは、次のとおりです。

0	モジュールは正常に起動しました。
0以外	proscan起動中のシステム エラーです。レポートを確認してください。

A.7 proscanmsモジュールのコマンド ライン キー

ヘルプに関するオプション	
-h	proscanmsモジュールのヘルプをコンソールに出力します。
-v	プログラムのバージョンを表示します。
構成に関するオプション	
-c <file_path>	代替構成ファイル**<file_path>**を使用します。
-r <IP_address>	送信元MTAのIPアドレスを設定するパラメータです。
-s	PostfixでBefore Queue Filter機能を使うときに指定します。

A.8 proscanmsモジュールのリターン コード

0	proscanmsモジュールは正常に起動しました。
65	メールをすぐに処理できなかったので、キューに保存されたことを知らせる警告がqmailメール システムに送信されました。
75	メールをすぐに処理できなかったので、キューに保存されたことを知らせる警告が sendmail/Postfixメール システムに送信されました。

A.9 licenseviewerモジュールに関するコマンド ライン キー

ヘルプに関するオプション	
-h	**licenseviewer**モジュールのヘルプをコンソールに出力します。
ライセンス キー処理時に使用されるオプション	
-s	インストールされているライセンス キーに関する情報をコンソールに出力します。
-c <file_path>	代替構成ファイル**<file_path>**を使用します。
-u <address>	**<address>**に指定されているEメール アドレスのユーザーがライセンスDBに登録されているかどうかを確認します。allを指定するとライセンスDBに登録されているユーザすべてを表示します。
-r <address>	**<address>**に指定されているEメールアドレスをライセンスDBから削除します。
-R <address regexp>	削除するアドレスを正規表現で指定します。
-t	正規表現で削除する際に実際の削除は行なわず、どのアドレスが削除されるか表示させるオプションです。
-d <domain>	**<domain>**に指定されているドメインが対象かどうかチェックします。allを指定するとすべてのドメインを表示します。
-k <file_path>	キー**<file_path>**に関する情報をコンソールに出力します。

A.10 proscanupモジュールに関するコマンド ライン キー

ヘルプに関するオプション	
-h	**proscanup**モジュールに関するヘルプをコンソールに出力します。
-v	プログラムのバージョンを表示します。
アップデート処理時に使用されるオプション	
-c <file_path>	代替構成ファイル**<file_path>**を使用します。
-U <URL>	アップデートサーバのURLをhttp://update.hoge.domain:8001の形式で指定します。
レポート生成に関するオプション	
-l <file_path>	モジュールの処理結果を**<file_path>**に記録します。
-r	設定ファイルの内容によらずモジュールの反映を行います。
-f	モジュールの強制ダウンロードを行います。
-q	メッセージをコンソールに出力しません。

-V　　メッセージをコンソールに出力します。

A.11 proscanupモジュールのリターン コード

proscanupモジュールの実行中に返されるコードは、次のとおりです。

0　　正常に処理が終了しました。

0以外　　更新処理に失敗しました。

A.12 Postfixメール プログラムのサンプル構成ファイル: master.cf

#

サービス	タイプ	Private	upriv (yes)	chroot(yes)	Wakeup (yes)	Maxproc (50)	command + args
#							
Smtp	inet	N	-	y	-	-	smtpd
Pickup	fifo	N	n	y	60	1	pickup
Cleanup	unix	-	y	y	-	0	cleanup
Qmgr	fifo	N	-	y	300	1	qmgr
#qmgr	fifo	N	-	n	300	1	nqmgr
Rewrite	unix	-	-	y	-	-	trivial-rewrite
Bounce	unix	-	-	y	0	0	bounce
Defer	unix	-	y	y	0	0	bounce
Flush	unix	-	y	y	1000?	0	flush
Smtp	unix	-	y	y	-	-	smtp
Showq	unix	N	y	y	-	-	showq
Error	unix	-	y	y	-	-	error
Local	unix	-	y	y	-	-	local
Virtual	unix	-	y	y	-	-	virtual
Lmtp	unix	-	y	y	-	-	lmtp
#this line added by ProScan							
localhost:10025	inet	N	n	n	-	10	spawn
user=filter argv=/opt/proscan/bin/proscanms							
localhost:10026	inet	N	-	n	-	10	smtpd
-o content_filter= -o myhostname=localhost.localdomain							

Before Queue Filterを利用する場合には以下の設定となります。

Smtp	inet	N	-	y	-	-	smtpd
-o smtpd_proxy_filter=127.0.0.1:10025 -o smtpd_client_connection_count_limit=10							
#this line added by ProScan							
localhost:10025	inet	N	n	n	-	10	spawn
user=filter argv=/opt/proscan/bin/proscanms -s							
localhost:10026	inet	N	-	n	-	10	smtpd
-o content_filter= -o myhostname=localhost.localdomain							

付録B. userdbadmコマンドについて

1. 概要

本コマンドは、ProScanのグループ機能において指定できる、ユーザDBをコントロールするためのものです。グループ設定においてアドレス指定（Usersパラメータ）を行った場合に、そのDBをメンテナンスするためのものです。新規・追加・削除をアドレスを直接指定したり、あらかじめ用意してあるファイル（標準入力も含む）から読み込んで指定したりすることが可能です。また、削除時には正規表現による指定も可能となっています。基本的にはProScanのコンフィグレーションファイルの内容に基づき設定を行います。DBの更新は排他制御を行っていますので、ProScan動作時にも更新が可能となっております。

また、バージョン6.0.3.8よりDHA機能のためのDB管理機能が搭載されました。

2. 書式

```
userdbadm -g group_name [-A|-N|-D[r]|-L][-c config_path]
                                  [-e exec_user][-q][-h|-v] address …
```

【オプション】

g	…	グループ名。コンフィグファイルに設定してあるものを指定。このグループのUsersパラメータが対象となる。Usersパラメータがない場合には無視される。グループ名にDHAを指定するとDHA機能のためのDBが対象となる。
A|N|D|L	…	処理。Aは追加、Nは新規、Dは削除、Lはリスト。Aは既存のDBに指定アドレスを追加する。既に存在している場合は無視される。NはDB一旦クリアし、指定アドレスで再作成される。Dは指定アドレスをDBから削除する。アドレスが存在しない場合には無視される。Dの場合のみ次のrオプションを指定することができる。LはDBの内容を標準出力にリストする。
r	…	正規表現指定。削除処理の場合に、パラメータを正規表現として利用。
c	…	ProScanコンフィグレーションファイルを指定。デフォルトはOSにより異なる。
e	…	実行ユーザ。デフォルトはコンフィグファイルの内容に従う。
q	…	メッセージを出力しない。エラーメッセージは標準エラー出力に表示される。
h	…	オプション表示。
v	…	バージョンメッセージ表示。

【パラメータ】

ファイルまたはアドレスを指定。複数指定する場合は空白で区切る。ファイル指定時に“－”ハイフンを指定した場合は標準入力より読み込む。rオプション指定時には正規表現を指定する。

【戻り値】

正常に処理した場合は0、エラーがあった場合にはメッセージを表示し、0以外の値となる。

3. 機能

グループ定義のUsersパラメータで指定したユーザDBをリアルタイムでメンテナンスします。このパラメータには通常、グループに所属するユーザ（メールアドレス）の一覧を記載したテキストファイルを指定します。ProScan起動時にこのファイルを読み込みユーザDBを作成し、メール送受信時にこのDBを参照することで、グループに所属するかどうかを判定しています。

本コマンドでは、このユーザDBおよびアドレス指定テキストファイルのメンテナンスを行うことができます。DB操作を行うとその結果がテキストファイルにも反映されるため、再起動時にもリアルタイムにメンテナンスした結果が有効となります。

gオプションでグループを指定し、処理を選択します。gオプションで指定するのは、ProScanの設定ファイルに指定したグループ名です。指定したグループ名が見つからない場合や、そのグループでUsersパラメータを有効にしていない場合は、何も処理を行いません。ProScan設定ファイルのデフォルトはOSにより異なりますが、インストール時に変更している場合には、cオプションで指定可能です。また、稼動中のProScanに影響を与えたくない場合などは別の設定ファイルを指定することも可能です。

ユーザDBへの処理は、新規（New）、追加（Append）、削除（Delete）、リスト出力（List）の4つが行えます。

新規処理は、パラメータで指定されたアドレスでユーザDBを作成しなおします。以前のデータは全て削除されますが、Usersパラメータに設定されているテキストファイルは「.back」拡張子を付けてバックアップされます。

追加処理は、パラメータで指定されたアドレスをユーザDBに追加します。既にユーザDBに存在するアドレスが指定された場合は無視されます。実際に追加されたアドレスは、テキストファイルにも追加されます。

削除処理は、パラメータで指定されたアドレスをユーザDBから削除します。アドレスが見つからない場合には何も行いません。複数のアドレスが指定された場合には、すべて削除されます。rオプションが指定された場合には、パラメータをPosix正規表現として扱います。ユーザDBのマッチするアドレスを全て削除します。更新後の内

容は他の処理同様、テキストファイルに反映されます。
リスト処理は、DBの内容を標準出力に出力します。
パラメータの指定は3通りあり、アドレスを直接指定する場合、アドレスが書かれたファイルを指定する場合、正規表現を指定する場合（削除処理の場合のみ）です。直接指定やファイル指定の場合は、空白で区切って複数指定することも可能です。また、アドレスとファイルの混在も可能です。本コマンドがアドレスと判定するのは“@”があるかないかなので、ファイル名に“@”が含まれるものは利用できません。ファイル指定で“－”（ハイフン）を指定した場合には、標準入力からアドレスを読み込みます。ファイルで指定する場合、アドレスは1行に1つで記述し、LFコードで改行しているもののみサポートします。
グループ名にDHAを指定すると、DHA機能ためのDBを管理できます。ProScan設定ファイルの[smtpscan.general]セクションのRecipientsFileパラメータに指定したDBファイルを対象に処理を実施します。その他の機能は、他のグループを指定したときと同じになります。

4. 利用例

以下に本コマンドの使用例を示します。

- ファイルを指定して新規作成処理

```
# userdbadm -g hoge -N /etc/opt/proscan/users/hoge.lst
Read configuration file(/etc/opt/proscan/proscan.conf)
Make new users DB(/etc/opt/proscan/hoge_user.db)
```

- アドレスを指定して追加処理

```
# userdbadm -g hoge -A foo@example.com test@example.com
Read configuration file(/etc/opt/proscan/proscan.conf)
Append new users to DB(/etc/opt/proscan/hoge_user.db)
```

- ファイルを指定して追加処理

```
# userdbadm -g hoge -A /etc/opt/proscan/users/hoge_append.lst
Read configuration file(/etc/opt/proscan/proscan.conf)
Append new users to DB(/etc/opt/proscan/hoge_user.db)
```

- アドレスを指定して削除処理

```
# userdbadm -g hoge -D hoge@example.com
Read configuration file(/etc/opt/proscan/proscan.conf)
Delete users from DB(/etc/opt/proscan/hoge_user.db)
```

- 正規表現でマッチするものを削除処理

```
# userdbadm -g hoge -D hoge@example.com
Read configuration file(/etc/opt/proscan/proscan.conf)
Delete users from DB(/etc/opt/proscan/hoge_user.db)
```

- リスト処理

```
# userdbadm -g hoge -L
test6@test.promark-inc.com
test5@test.promark-inc.com
test4@test.promark-inc.com
test3@test.promark-inc.com
test2@test.promark-inc.com
test@test.promark-inc.com
```

5. その他

内部的には、一旦アドレスをメモリに展開し、DBへの更新処理を行います。そのため、大量のアドレスを新規登録するような場合にはメモリを消費し処理時間もかかりますのでご注意下さい。（マシンの性能にも左右されますので相対的なものです。）
また、削除ではエントリの内容をクリアしているだけですので、DBファイルのサイズは変わりません。この場合はProScan再起動等で再作成され場合に実際のサイズになります。従いまして、削除後はタイミングを見計らってDBの再構築をお願いします。
eオプションで指定したユーザで実行されますのでファイル生成等はこのオーナでされます。省略時は設定ファイルに書かれているExecUserパラメータで指定されたユーザで実行されます。こちらも省略されている場合にはrootとなります。
ProScanでこのDBを参照するのは、メールを受信後、チェックする直前でFromおよびToアドレスがどのグループに所属するかを調べるときです。従いまして排他処理は行っていますのでユーザDBの破壊は起きませんが、タイミングによっては、変更した内容の反映が間に合わずに処理される場合がございます。

付録C. お問い合わせ先

ご質問やご意見がございましたら、代理店またはプロマークにご連絡ください。製品のインストールや管理について、どのようなことでもEメールにて承ります。お送りいただいたご意見やご提案は、弊社にて十分に検討いたします。

テクニカル サポート	テクニカル サポートの詳細については、 http://**www.promark-inc.com/index.html**をご覧ください。
その他、製品やサービスに関するお問い合わせ窓口	現在のところ電子メールによるお問い合わせのみです。 Eメール：**support@promark-inc.com**

ProScan or Mailserver
バージョン6.0.5

管理者ガイド　第23版

発行日　2021年3月8日
作成元　株式会社プロマーク

promark

株式会社プロマーク