ProScan
ANTIVIRUS

ProScan® Anti-Virus for Mail Server バージョン6.0.3

アンチスパム設定ガイド

promark

株式会社プロマーク

2008年7月　第2版

目次

第1章 ProScanアンチスパムオプションの概要

ProScan Anti-Virus for Mail Server (以降、「**ProScan Anti-Virus**」または「**ProScan**」と表記) は、オプション機能として、迷惑メールを検出するアンチスパム機能を備えています。アンチスパム機能は、アンチスパム・オプションライセンスを購入し、現在お使いの**ProScan**にセットすることですぐに利用することが可能です。余計なインストール作業もなく、簡単に利用を開始できます。

このアンチスパムの機能は次のとおりです。

- メールのチェック時に、ウイルスだけでなく、スパムメールかどうかのチェックを行います。
- ウイルスチェック同様、グループ単位にスパムチェックを行うかどうかを指定できます。
- スパムチェックの基本は、送信元MTAのドメイン識別方式を採用しています。その他、RBLやWBL、サブジェクトのパターンマッチングを行うことも可能です。
- スパム判定は、2種類のレベルで判定します。スパムと判定されたメールには、ヘッダ情報に任意のヘッダを追加することができます。また、Subjectに任意の文字列を追加することが可能です。その他、ウイルス検出時と同じように、配送を止めたり、任意のディレクトリに保存したり、受信者に通知メールを送ったりすることが可能です。.

ProScanのアンチスパム検出の核は、送信元MTAのIPアドレスを逆引きして得られる、ドメイン名を元に行うことです。（S25R方式）一般的なアンチスパムソフトとは異なり、メールの内容については一切チェックを行いませんのでご注意下さい。

1.1. ProScanのアンチスパム機能の利用方法

アンチスパムオプションを利用するには、オプションライセンスが必要となります。ダウンロードパッケージには30日間有効なオプションライセンスも一緒に同梱されておりますので、新規にProScanを導入する方はご利用下さい。また、すでにProScanをご利用の方で今回初めてアンチスパム機能を試してみる方は、弊社営業（sales@promark-inc.com）までご連絡いただければ、30日間有効な評価ライセンスを発行いたします。

- **ライセンスの設定**

  antispam.keyというファイルが、定位置にあるか確認します。定位置はProScanのライセンスキーファイルと同じ場所になります。

  【Linux,Solarisの場合】　`/var/opt/proscan/db/keys/antispam.key`

  【xBSDの場合】　`/var/proscan/db/keys/antispam.key`

- **ライセンスの確認**

  オプションライセンスが有効かどうかlicenseviewerコマンドで確認します。

```
# /opt/proscan/bin/licenseviewer -s
ProScan License Viewer Ver.6.0.3.8
All Rights Reserved,Copyright(C) 2003-2008 Promark Inc.

ProScan License Information:
 Registration Code = PSHB01-9999-431-862-454
 Expire date       = 2007/03/31 (expires in 142 days)
 Number of domains = 10
 Number of users   = 100

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

  上記のように、オプションライセンスの表示がきちんと表示され、「Registered」または「Trial」になっていればOKです。正しい表示がされず、「This is invalid license.」のように表示される場合は、ライセンスを正しく認識していませんので、ライセンスキーファイルを確認してください。また、「Expired」となっている場合には、有効期限が切れていますので、正規ライセンスを購入するか、ライセンスの継続を行ってください。

- **ライセンスの継続**

  ライセンスの有効期限が切れている場合には、弊社営業までご連絡頂き、ライセンスの継続購入を行ってください。

手続きが済み次第、継続ライセンスをお送りしますので、そのキーファイルを既存のantispam.keyと置き換えてください。アンチスパムのオプションキーファイルはPSHB4で始まる23桁のコードをファイル名としていますので、それをantispam.keyとして上書き保存してください。

- **ProScan設定ファイルの変更**

  デフォルトではアンチスパムオプションは無効となっていますので、ライセンスを設定後、アンチスパムが利用できるようにProScanの設定変更を行います。これについては第3章で詳しく説明します。

- **動作確認**

  ProScanのアンチスパム機能は、説明していますとおり、スパムメールを転送しても検出しません。これは、送信元がspammerでないからです。具体的なテスト方法は第4章で詳しく説明します。

1.2. ProScanアンチスパムの検出率

ProScanのアンチスパム機能の検出率は、弊社テスト環境での実績で約95%となっております。（テスト環境のOSはFreeBSD、MTAはPostfixです。）特殊な設定を行っているわけではなく、ホワイトリストやブラックリストの設定も行っておりません。

もし、90%以下の検出率となるような場合は、設定に何か問題があることが考えられますので、設定を見直すことをお勧めいたします。

1.3.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 スパム検出の仕組み

この章では、ProScanのアンチスパム機能の詳細について説明し、理解を深めて貰いたいと思います。

ProScanのアンチスパム機能は、他ベンダーのアンチスパム検出の仕組みとは根本的に異なるため、その仕組みを理解しないと、正しい設定を行うことができずに、その性能を十分に発揮することができません。この章では、その仕組みを詳細に説明しますので、設定に役立てて頂きたいと思います。

他ベンダーの製品と異なる点を以下に列挙します。

- メールの中身でなく、送信元MTAを基準に判定を行う
- メールのFromやToアドレスでの判定は行わない
- コンテンツに影響されないため、日本語、英語のスパムの区別無く判定可能

2.1. メール送信元ドメイン識別方式（S25R方式）

ProScan®のアンチスパム機能はSMTP接続してきたクライアント（MTAやMUA）のIPアドレスを逆引きしてそのFQDN（ドメイン名）を元に判定する方式(S25R方式)を採用しています。これは、正当なメールは、きちんとDNSに登録されたメールサーバより送られると言う仮定に基づいています。

通常、企業やISPが使用しているメールサーバはメールを送受信するためにその名前をDNSに登録し、インターネット上に公開しています。メールを送信するだけでは送信者のIPアドレスはDNSに登録する必要がないのですが、大抵の場合、そのメールサーバが受信も兼ねているため、DNSに名前が登録されています。

ProScanのアンチスパム機能はこれを利用し、ドメイン名がメールサーバらしくない場合にそこから送られたメールをスパムと判定することにしています。

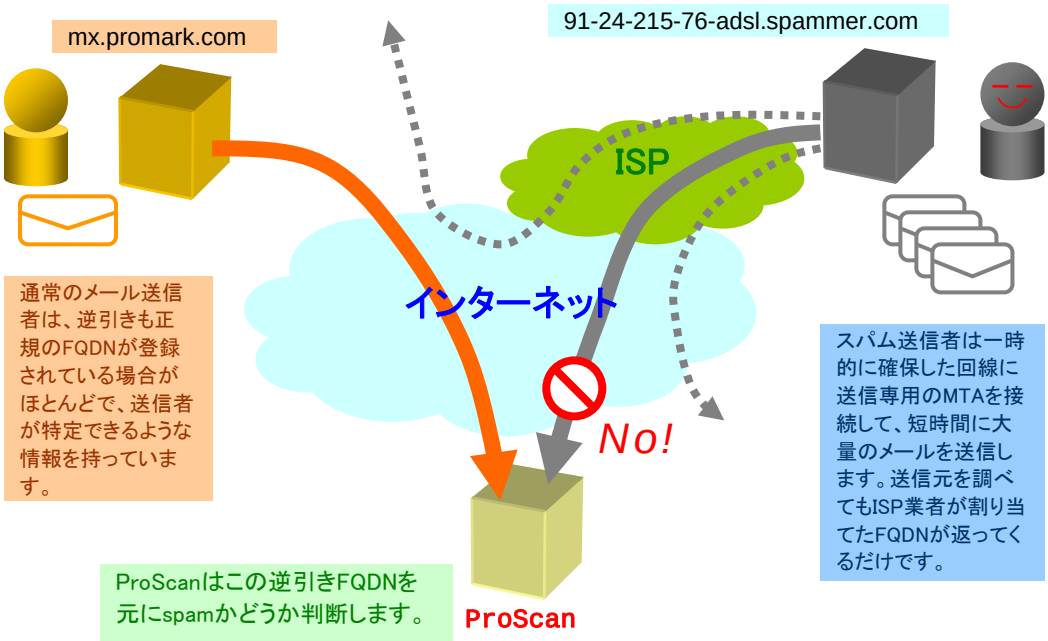


図1　ProScan でのスパムメール判定方式

但し、例外もあります。例えば、送信専用のMTAを設けているような場合（メールマガジンなどのサービスを行っている場合）やごく小さい企業などが逆引き設定の権限を与えられない固定IPを使用している場合、ProScanを搭載したMTAを利用するユーザがSMTP接続してメールを送信する場合などです。これらの場合には、逆引きができないか、逆引きができても、正当なMTAの名前としてDNSに登録されていない場合が多いため、スパムと判定されてしまいます。ProScanではこれらの場合にもメールをスパムと判定させない仕組みを搭載しています。

それでは、ドメイン識別の判定について詳しく説明します。

ドメイン識別方式の判定は以下のように行われます。

1. ProScanがMTAからメールをチェックするために受信するとSMTP接続元のIPアドレスを受け取ります。
2. 受け取ったIPアドレスを逆引きします。逆引きできない場合には、FQDNをIPアドレスとします。逆引きできた場合には、再度、得られたFQDNで正引きし、同じIPが得られた場合は正しいFQDNとして登録します。異なったIPが得られた場合は、逆引きできない場合と同様、FQDNをIPアドレスとします。
3. チェックを行うメールには、送信元MTAまたはMUAのIPアドレスと、FQDNを必ず情報として持っています。IPアドレス＝FQDNの場合には、逆引きができなかったということになります。
4. 各種WBLフィルターを通過したメールのFQDNをパターンマッチによりスパムらしいと判断します。それらのパターンを以下に示します。

   ①逆引きできないメール（FQDNがIPアドレス）

   ②FQDNの最下位（左端）の名前が、数字以外の文字列で分断された二つ以上の数字列を含む

   例:220-139-165-188.dynamic.hinet.net
   evrtwa1-ar3-4-65-157-048.evrtwa1.dsl-verizon.net
   a12a190.neo.rr.com

   ③FQDNの最下位の名前が、5個以上連続する数字を含む

   例:YahooBB220030220074.bbtec.net
   pcp04083532pcs.levtwn01.pa.comcast.net

   ④逆引きFQDNの上位3階層を除き、最下位または下位から2番目の名前が数字で始まる

   例:398pkj.cm.chello.no
   host.101.169.23.62.rev.coltfrance.com

   ⑤逆引きFQDNの最下位の名前が数字で終わり、かつ下位から2番目の名前が、1個のハイフンで分断された二つ以上の数字列を含む

   例:wbar9.chi1-4-11-085-222.dsl-verizon.net
   m226.net81-66-158.noos.fr

   ⑥FQDNが5階層以上で、下位2階層の名前がともに数字で終わる

   例:m500.union01.nj.comcast.net
   d5.GtokyoFL27.vectant.ne.jp

   ⑦FQDNの最下位の名前が「dhcp」「dialup」「ppp」「adsl」または「dsl」で始まり、かつ数字を含む

   例:dhcp0339.vpm.resnet.group.upenn.edu
   dialupM107.ptld.uswest.net
   PPPbf708.tokyo-ip.dti.ne.jp
   adsl-1415.camtel.net

浅見秀雄氏の考案による「Selective SMTP Rejection (S25R)方式」に基づきプロマークで独自に実装を行ったものです。参照→http://www.gabacho-net.jp/anti-spam/

これらFQDNのパターンマッチで引っかかったものの内、救済措置がとられなかったものは、低精度のスパムとして処理されます。

救済措置とは、グレイチェック、DRAC DB、WBLです。これらについては次に詳しく説明します。

2.2. グレイチェック

ProScanのグレイチェックは、２つの特徴を備えています。それは、通常のグレイリスト方式をさらに細かく分割して、ホワイトリストよりのグレイリストをライトグレイリスト、ブラックリストよりのグレイリストをダークグレイリストと呼んでいます。ライトグレイリストは別名、自動ホワイトリストと言い、よりスパムの誤判定を防ぐための機能となっています。２つのグレイリストはProScanが自動的に生成するリストですので、WBLのように自由に設定することはできません。

FQDNのドメイン識別でスパムらしいと判定された場合に、そのメールを一時的に拒否することで、よりスパムメールとしての確度を高めています。通常のMTAであれば、一時エラーを返されたメールは、キューに残され、十数分後、MTAの再送スケジュールに従って再送されます。そのため通常のメールは若干遅れて届くことになりますが、一旦届けば以降は遅れることなく届くことになります。一方、スパムメールはまず、再送を行いませんので、メールを受け入れなくなりスパムメール自体を目にする事が少なくなります。また、送信者を偽装していたり、送信業者は、送りぱっなしが多いため、SMTP接続時のエラーは有効となります。

グレイチェックを有効にした場合のその動きを詳しく説明します。

グレイチェックが機能するのは、メールの受信をProScanの応答により直接拒否できるMTAのみとなっています。現状では、qmail版、Sendmail Libmilter版、Postfix 2.2以降でBefore Queue Filterのみとなっています。SendmailやPostfixでのAfter Queue Filterでは、MTAが一旦受信を行ってしまうので、グレイチェック機能が働きません。

1．まず最初にライトグレイリストをチェックします。このリストに登録されているIPアドレスからのメールはスパムと判定しません。

2．ドメイン識別でスパムと判定された場合、ダークグレイリストをチェックします。

3．ダークグレイリストは、FQDNのパターンでスパムと判定されたメールの送信元IPアドレス,Message-ID,From,To をハッシュ化したものをキーとして受信時刻と共に記録しています。ダークグレイリスト内に同一キーのエントリが存在しない場合は、メールを一時エラーで返却し、情報を記録します。同一エントリーが存在する場合には、既に一時エラーで返されたメールが再送により送られてきていることを示すので、その再送間隔を調べます。再送間隔が再送受け入れ許可時間を過ぎている場合は、そのメールを通常のメールとして受信します。過ぎていない場合には、受信時刻をリセットし再度、一時エラーを返します。

4．ダークグレイリストのチェックで、再送受け入れを行った場合、そのメールを送信したMTAはFQDNのパターンではスパムらしいと判断されたのですが、適切な再送を行ってきたため問題のないMTAと判断し、ダークグレイリストよりエントリを削除し、ライトグレイリストにそのエントリを移します。これにより、一旦受け入れを行ったMTAに関しては、自動的にホワイトリストに登録されるようなイメージとなります。

ライトグレイリストに登録されてしまったスパム送信元（たまに再送を行うスパマーがいるようです）は、リストから除外するためのコマンドを用意しています。（付録参照）

2.3. DracDBについて

DRAC DBのチェックは、主にMUAからの送信メールをスパムと誤判定することを防ぐために、POP Before SMTPのデータベースを利用します。POP認証を通ったSMTP接続はドメイン識別を実施しない仕組みとなっています。現在、利用できるDRAC DBは、BerkeleyDBのbtree,hashタイプのものと、IPアドレスをテキスト形式(text)のリストで持っているもの、どのタイプかわからない場合に利用するダンプモードに対応しています。ダンプモードの場合は、stringsコマンドのようにバイナリデータファイルの中身のテキスト部分を抜き出し、IPアドレス文字列にマッチするようなパターンを抽出してチェックします。（stringsコマンドでDBを表示させたときにIPアドレスが表示されれば、ダンプモードでチェック可能です。）

テキスト形式の場合は、以下のようなフォーマットの場合に対応しています。

```
219.13.6.6:allow,RELAYCLIENT="",RBLSMTPD=""      1163392316
203.181.44.22:allow,RELAYCLIENT="",RBLSMTPD=""   1163393480
192.168.100.100:allow,RELAYCLIENT="",RBLSMTPD=""         1163394950
```

図2　DracDBのテキストタイプの例

先頭のフィールドにIPアドレスが書かれていて、コロン(：)または空白、セミコロン、カンマ、改行で区切られて

いるフォーマットを読み込みます。上記は、open-smtpで使用されているものですが、他の実装でもフォーマットが同じであれば問題ありません。

また、POP Before SMTPでなくSMTP認証をご利用のお客様は、申し訳ございませんが、現状ではProScanでのサポートは行っていません。別途、POP before SMTPの設定（SMTP認証を利用している場合でもPOPを試用している場合には、SMTPとは関係なくPOPの動作からDBを更新できます。単にSMTPサーバがDBを参照しないだけですので運用には問題ございません。）をして頂くか、WBLによる回避をお願いします。

2.3. RBLによる判定

RBLはDNSタイプのものを最大32ホスト設定できます。指定したIPがRBLサイトで引けるかどうかを判定しています。FreeのRBLサイトがありますが、日本語のスパムにはほとんど対応していませんので、RBLによる検出はあまり効果がありません。IIJなどが行っている有料サービスを利用しますともう少し良い結果が出ると思いますが未検証です。（動作実績は報告を受けています。）

RBL,WBL,Subjectマッチによりスパムと判定されたメールは高精度フラグが付きます。現状、デフォルト設定では、高精度判定は5～10%ほどにとどまっていて、より多くのチューニングが必要となります。

2.4. スパムWBL

ProScanでは、WBLの指定が2種類あります。一つは、スキャン前に実施するもので、送信元のMTAまたはMUAのIPアドレスから判定するものですべてのスキャンに影響するものです。もう一つは、スパムチェック時にのみ影響するものです。どちらも送信元のIPアドレスを判定の材料にしていますので、メールのFromアドレスでないことにご注意下さい。

スパムWBLは、メールのアドレスはチェックしません。あくまでも送信元のMTAまたはMUAのIPアドレスを逆引きしたものを基準としています。

スパムWBLは、チェックしたメールがスパムと判定されたかどうかでホワイトリストを参照するか、ブラックリストを参照するか変わってきます。以下のフローを参照してください。

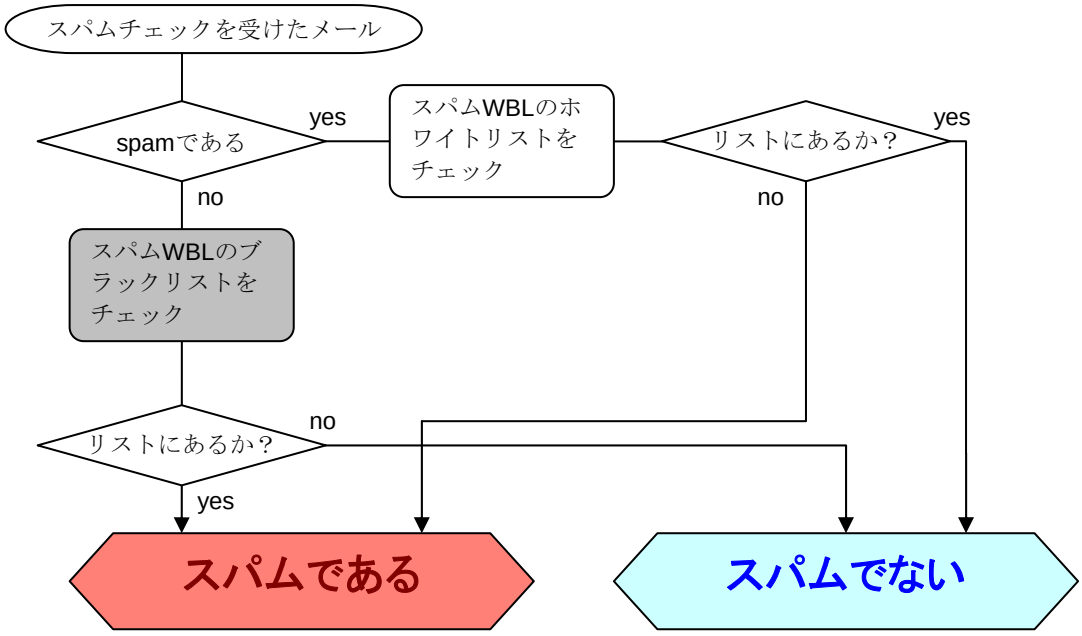


図3　スパムWBLでの判定フロー

スパムWBLでは、FQDNを元に設定パターンと比較しますので逆引きできない場合はIPアドレスを指定します。IPアドレスも正規表現で指定しますので、アドレスによっては注意が必要です。例えば、“61.202.34.12”というIPアドレスを指定するのに、そのままWBLRejectに記述しますと、“61.202.34.120”～“61.202.34.129”もマッチしてしまいます。また、「.」ドットは正規表現のメタキャラクタなので、“204.25.1.2”をそのまま設定してしまうと“204.25.102.12”や“204.25.192.45”などのアドレスも一致していまいますのでご注意下さい。より正確を期すために、「^204¥.25¥.1¥.2$」のような正規表現で記述してください。

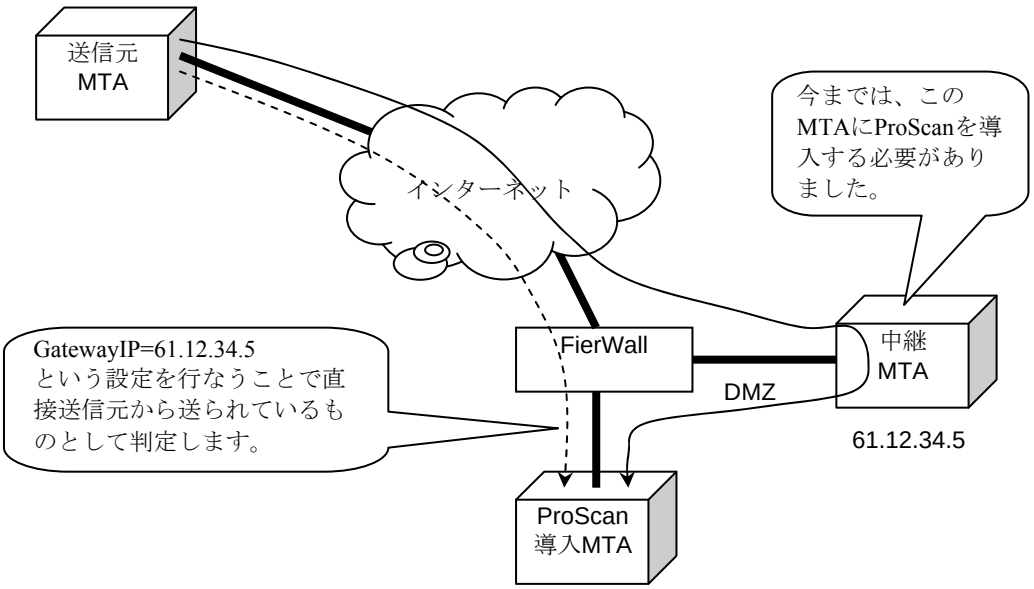
2.5. Subjectパターンマッチ

ProScanのスパムチェックにおいて唯一、メールのコンテンツ(内容)によりチェックを行っているのが、このSubjectヘッダの内容をパターンマッチでチェックしているものです。

このパターンに登録した内容にマッチするSubjectを持つメールは高精度スパムとして判定されます。このパターンは他の設定同様、Posix正規表現により記述でき、さらに複数のパターンを設定できますので、他のスパムチェックロジックと併用することで、より高い検出率を得ることが可能です。

2.6. 外部から直接メール受信していないMTAでの設定

FireWall経由や外部MTAを経由している内部MTAにおいてProScanを利用する場合に、[smtpscan.general]セクションのGatewayIPパラメータにその経由MTAのIPアドレスを指定することで、本来の送信元をチェックすることが可能です。



複数のMTAを経由する場合には、現状ではspamチェックできません。

第3章 アンチスパムの設定ポイント

ここでは、リファレンス的な内容は説明いたしません。設定の詳細については「ProScan管理者ガイド」を参照してください。設定のポイントについて設定例を中心に説明します。

「ProScan管理者ガイド」につきましては、弊社ホームページよりをダウンロード可能となっております。
http://www.promark-inc.com/download/ProScan/Mailserver/documents/ProScan_Administrator_Guide.pdf より
ダウンロードして、ご覧下さい。

3.1. テスト運用のススメ

ProScanのパッケージインストール時に、アンチスパムオプションを評価利用するかどうか聞かれますが、テスト環境でのみの評価利用や、既にProScanのアンチスパム機能を熟知している場合であれば、そのままインストールと同時にオプションを有効にして構いません。しかしながら、既存のメールシステムにおいてアンチスパム機能の評価を行いたい場合には、インストール時に設定するのではなく、これから説明する内容で、テスト的な評価を実施されることをお勧めします。

3.1.1. テストグループの作成

まず、アンチスパムのテスト行うアドレス用のグループを作成します。スパムを良く受け取るアドレスを幾つか抽出できるとテストしやすいと思います。そのアドレスは、利用者がいて定期的にメールを受信しメールの内容を目視できることが必要です。要は人間がProScanのアンチスパムが正しくメールをスパムと判定しているか確認できる必要があるということです。そうすることにより、ProScanのアンチスパム機能を正しく評価できることになります。

例えば、「spam_check」というグループ名を付けると仮定して、実際の設定方法を示します。

```
_group spam_check
[smtpscan.group]
Check=yes
SpamCheck=yes
Recipients=^yamada@.*,^sato@.*
AdminAddress=root@domain.com

[smtpscan.wbl]
[smtpscan.action]
[smtpscan.notify]
[smtpscan.filter]
```

※*上記4つのセクションは従来のアンチウイルスの設定と同じです。*

これらの設定を、「_defaul」グループの前に設定します。

このグループは、あて先が「yamada@」と「sato@」で始まるアドレスとなります。この２つのアドレスに届いたメールのチェックに関する設定となります。この二人が送信するメールについてはdefaultグループでのチェックになりますのでご注意下さい。

3.1.2. テストグループでのスパムチェック設定

テスト用グループでは、最小限設定が必要なもののみ設定します。まずは正しく動作させることに重点を置きます。この時点ではグレイチェックの実施やWBLの設定は行わず、ドメイン識別でのチェックが問題ないか確認するための設定を行います。DracDBは設定すべき内容が分からない場合は、未設定でも構いません。

```
[smtpscan.spam]
DracDB=text:/home/vpopmail/etc/open-smtp
GrayCheck=no
RBLcheck=yes
RBLHostName=dnsbl.njabl.org
SubjectCheck=
WBLAccept=
WBLReject=
```

```
[smtpscan.spam_action.low]
AddHeader=X-ProScan-SPAM: low detect
AddSubject=[SPAM:low]
Deliver=yes
Notify=no
Save=no

[smtpscan.spam_notify.low]

[smtpscan.spam_action.high]
AddHeader=X-ProScan-SPAM: high detect
AddSubject=[SPAM:high]
Deliver=yes
Notify=no
Save=no

[smtpscan.spam_notify.high]
```

上記設定は、「yamada@」と「sato@」に届いたメールがドメイン識別でスパムと判定された場合、ヘッダと題名を加工し、通常通り受信者に配送するようになっています。そのため、受信者は、届いたメールの題名に[SPAM:low]という文字列が追加されている場合は、本当にそのメールがスパムかどうか自身の目で確かめ判断してください。もし、誤判定がある場合はその原因を追究する必要があります。また、通常メールを受信している中で明らかにスパムメールであるのに、spamと判断されていないメールについても、その原因を追究する必要があります。原因を見極める方法についてはトラブルシューティングの章で説明します。

同時に、ログレベルの設定も確認してください。spam関連のログは現在のログレベルに+256すれば出力されるようになります。もし、HDDの容量に余裕があるのであれば、デバッグログを採取しておくことをお勧めします。

3.1.3. テスト運用

設定が完了し、有効なライセンスが存在するとスパムチェックを開始します。

テスト運用を開始したら、送信されてくるメールを注意深く監視してください。スパムメールをすべて別ホルダに集めて、SubjectにSPAMと付く割合を測定します。これが95%に近い値となれば、設定は正しく、スパム検出にも問題ないと言えます。

スパムメールにも関わらず、スパムと検出できない場合は、トラブルシューティングの章を参考に、設定に間違いが無いかどうか確認してください。9割以上の検出率がありますので、ほとんどのスパムメールを判定可能ですので、スパムメールを逃す場合には、その理由を確認してください。

テストはスパムメールの量にもよると思いますが、ある程度数が集まる方が良いので最低でも2週間ぐらいは続けてください。

3.1.4. テスト結果の評価

テスト用のグループでしばらく運用して、スパムメールを正しく検出できているか、検出率はどの程度か評価して頂きたいと思います。

スパムの検出率は、以下のように行うと簡単に算出できます。

- 届いたメールをすべてチェックし、スパムメールのみを別のフォルダに移します。
- スパムメールフォルダの中のSubjectに設定した文字列（上記例では"[SPAM:"が含まれているものの数を数えます。
- 以下の式で検出率を算出します。

$$\text{（スパム検出率）\%} = \frac{\text{（スパムと判定されたメール数）}}{\text{（全スパムメールの数）}} \times 100$$

※弊社テスト環境での実績値は、118706通のスパムメールから、115808通を検出しており、約97.6%の検出率となっています。(2007/06/19～2008年6月30日現在)

3.2. defaultグループへの反映

テストでの評価に問題がなければ、すべてのユーザに影響するdefaultグループへの反映を行います。

defaultグループへ反映する場合は、基本的にテスト運用時と同様の設定を行いますが、万が一、お客様へのメールに[SPAM]判定文字列が付いてしまうのを避けるために、低精度のSubjectへの文字列追加は、安定運用されるまで控えておいた方が良いかもしれません。

defaultグループへの反映は、すべての利用者に影響するため、その導入は慎重に行う必要があります。新しい設定を試す場合には、必ずテストグループで実施して、その効果を確認後、導入するようにしてください。

defaultグループへの反映前に、利用者にスパムチェックを導入することを周知徹底してください。特に、誤認識（spamでないのにspamと判定する）や、誤判定（spamなのにspamと判定しない）の場合の対応方法などは事前にユーザへお知らせしておいた方が良いでしょう。

3.3. ログの確認

利用者からのクレームが無い場合も、ログの確認は実施してください。安定するまでは、デバッグログを採取しておくと、問題が起きたときに、問題解決に役立つと思います。また、デフォルトではスパムチェックのログは出力されないような設定になっていますので、デバッグログを採取しない場合も必ずReportLevelは8191に設定して下さい。

3.3.1. スパムメールのログ

あるスパムメールを受信した際のログ出力を以下に示します。

テスト環境の構成は、OS:FreeBSD 4.8、MTA:Postfix2.1です。動きを明確にするためデバッグログを採取するように設定しています。（ReportLevel=32767での記録です）

```
[2006/11/15 09:07:44]-[34051.37] Connect id=7CHB8k.034051.00000024
[2006/11/15 09:07:44]-[34051.37] LMTP[W]: 250 2.0.0 OK
[2006/11/15 09:07:44]-[34051.37] LMTP[R]: MAIL FROM:<uht@db-cycles.co.uk>
[2006/11/15 09:07:44]-[34051.37] LMTP[W]: 250 2.1.0 <uht@db-cycles.co.uk>... Sender OK
[2006/11/15 09:07:44]-[34051.37] LMTP[R]: RCPT TO:<yamada@xxxxx.jp>
[2006/11/15 09:07:44]-[34051.37] LMTP[W]: 250 2.1.0 <yamada@xxxxx.jp>... Recipient OK
[2006/11/15 09:07:44]-[34051.37] LMTP[R]: DATA
[2006/11/15 09:07:44]-[34051.37] LMTP[W]: 354 Enter mail, end with "." on a line by itself
[2006/11/15 09:07:44]-[34051.37] [DEBUG] get received IP done(61.80.27.211)
[2006/11/15 09:07:44]-[34051.37] [DEBUG] get received IP (61.80.27.211)
① [2006/11/15 09:07:44]-[34051.37] Connect from 61.80.27.211 id=7CHB8k.034051.00000024
[2006/11/15 09:07:44]-[34051.37] [DEBUG] Get FQDN from ip address.(61.80.27.211 => 61.80.27.211)
[2006/11/15 09:07:44]-[34051.37] LMTP[W]: data read complete
[2006/11/15 09:07:44]-[34051.37] [DEBUG] domain check.(db-cycles.co.uk) --> NG
[2006/11/15 09:07:44]-[34051.37] [DEBUG] multipart boundary string:
                                          --------------030301030400050800060107(38)
[2006/11/15 09:07:44]-[34051.37] [DEBUG] Read Mail Part.1
[2006/11/15 09:07:44]-[34051.37] [DEBUG]  Filename(T):file0.html
[2006/11/15 09:07:44]-[34051.37] [DEBUG] Read Mail Part.2
[2006/11/15 09:07:44]-[34051.37] [DEBUG]  Filename(T):accomplice.gif
[2006/11/15 09:07:44]-[34051.37] [DEBUG]  Filename(D):accomplice.gif
[2006/11/15 09:07:44]-[34051.37] [DEBUG] Check darkgray list.
[2006/11/15 09:07:44]-[34051.37] [DEBUG] key1=61.80.27.211(0xd31b503d),
                                         key2=2060388,file=/var/proscan/db/darkgray.lst
[2006/11/15 09:07:44]-[34051.37] From:<uht@db-cycles.co.uk> --> To:yamada@xxxxx.jp>
[2006/11/15 09:07:44]-[34051.37] [DEBUG] domain check.(xxxxx.jp) --> OK
[2006/11/15 09:07:44]-[34051.37] [DEBUG] Group Check: default
                                 [From:uht@db-cycles.co.uk=.*](1) AND [To:yamada@xxxxx.jp=.*@.*](1)
② [2006/11/15 09:07:44]-[34051.37] Check default group configuration
[2006/11/15 09:07:44]-[34051.37] WBL check
[2006/11/15 09:07:44]-[34051.37] [DEBUG] WBL soruce IP 61.80.27.211(0xd31b503d)
[2006/11/15 09:07:44]-[34051.37] [DEBUG] WBL soruce Name 61.80.27.211
[2006/11/15 09:07:44]-[34051.37] [DEBUG] WBL accept IP 127.0.0.1(0x100007f)
[2006/11/15 09:07:44]-[34051.37] [DEBUG] WBL accept Net 192.168.1.0(0x1a8c0) mask 24(0xffffff)
[2006/11/15 09:07:44]-[34051.37] [DEBUG] WBL accept Net 61.197.232.208(0xd0e8c53d)
                           mask 29(0xf8ffffff)
[2006/11/15 09:07:44]-[34051.37] [DEBUG] WBL accept Net 192.168.11.0(0xba8c0) mask 24(0xffffff)
[2006/11/15 09:07:44]-[34051.37] [DEBUG] WBL accept name localhost
[2006/11/15 09:07:44]-[34051.37] [DEBUG] SAVAPI scan result = 0,
                           filename = /var/proscan/tmp/7CHB8k.034051.00000024, mode = 2
[2006/11/15 09:07:44]-[34051.37] Part.1 >>> file0.html --> checked
[2006/11/15 09:07:44]-[34051.37] Part.2 >>> accomplice.gif --> checked
[2006/11/15 09:07:44]-[34051.37] [DEBUG] SPAM check: 0,yes,1
```

```
③ [2006/11/15 09:07:44]-[34051.37] [DEBUG] spam check:61.80.27.211
  [2006/11/15 09:07:44]-[34051.37] [DEBUG] drac check:btree:/usr/local/etc/dracd.db
  [2006/11/15 09:07:44]-[34051.37] [DEBUG] drac check:type=btree,file=/usr/local/etc/dracd.db
  [2006/11/15 09:07:44]-[34051.37] [DEBUG] db get type=btree, key=61.80.27.211
  [2006/11/15 09:07:44]-[34051.37] [DEBUG] rbl check:non spam(211.27.80.61.dnsbl.njabl.org.)
  [2006/11/15 09:07:44]-[34051.37] [DEBUG] rbl check_status:No address associated with hostname
④ [2006/11/15 09:07:44]-[34051.37] FQDN check:spam
  [2006/11/15 09:07:44]-[34051.37] SPAM result: 1
  [2006/11/15 09:07:44]-[34051.37] [DEBUG] SPAM WBL accept name
                        ^usen-219x123x158x58¥.ap-US¥.usen¥.ad¥.jp$
                        |¥.105¥.138¥.210¥.bn¥.2iij¥.net$
                        |¥.plala¥.or¥.jp$
  [2006/11/15 09:07:44]-[34051.37] Message-ID: <455B492A.2050407@db-cycles.co.uk>
  [2006/11/15 09:07:44]-[34051.37] SCAN result: spam
⑤ [2006/11/15 09:07:44]-[34051.37] spam detect(1): From:Micky Schaefer uht@db-cycles.co.uk
                                                    To:yamada@xxxxx.jp Subject:initiative
  [2006/11/15 09:07:44]-[34051.37] [DEBUG] check param: [smtpscan.spam_action.low]
  [2006/11/15 09:07:44]-[34051.37] [DEBUG] AddSubject: [[SPAM]]
  [2006/11/15 09:07:44]-[34051.37] [DEBUG] AddHeader: X-ProScan-SPAM: spam detect low
  [2006/11/15 09:07:44]-[34051.37] [DEBUG] modify subject: =?ISO-2022-JP?B?W1tTUEFNXV0=?= initiative
  [2006/11/15 09:07:44]-[34051.37] [DEBUG] Mail delivery status:200
  [2006/11/15 09:07:44]-[34051.37] Message checked
  [2006/11/15 09:07:44]-[34051.37] [DEBUG] Deliver mail
  [2006/11/15 09:07:44]-[34051.37] [DEBUG] Deliver to[0]:yamada@xxxxx.jp(200)
  [2006/11/15 09:07:44]-[34051.37] [DEBUG] Forward mail
  [2006/11/15 09:07:44]-[34051.37] [DEBUG] P=smtp,H=localhost,p=10026
  [2006/11/15 09:07:44]-[34051.37] [DEBUG] Deliver SMTP:
  [2006/11/15 09:07:44]-[34051.37] [DEBUG] LicenseStatus=0
⑥ [2006/11/15 09:07:44]-[34051.37] Deliver: <uht@db-cycles.co.uk> --> <yamada@xxxxx.jp> OK
  [2006/11/15 09:07:44]-[34051.37] LMTP[W]: 250 2.6.0 Message accepted
  [2006/11/15 09:07:47]-[34051.37] LMTP[R]: RSET
  [2006/11/15 09:07:47]-[34051.37] [DEBUG] reset Mail object(808c580)
```

内容説明：

① 送信元MTAのIPアドレスを示します。デバッグログ採取時には逆引きした結果が記録されます。デバッグログを採取していない場合は、このIPアドレスを実際に逆引きしてみてください。
② どのグループ設定で処理しているか記録します。テスト時にはテスト用に作成したグループを、defaultグループの場合は、defaultグループになっているか確認します。
③ スパムチェック一連の処理内容が記録されます。（デバッグログ採取時）
④ スパムチェックの結果、FQDNがスパムらしいと判定されています。
⑤ メールスキャンの結果、このメールはスパムであると判定されています。
⑥ スパムメール処理が通常配送だったので、メール配送は正常に行われたことを記録しています。

前頁のログ採取時の実際のメールのヘッダ部分を以下に示します。

```
Return-Path: <uht@db-cycles.co.uk>
X-Original-To: yamada@xxxxx.jp
Delivered-To: yamada@xxxxx.jp
Received: from localhost (localhost [127.0.0.1])
        by xxxxx.jp (Postfix) with SMTP id B06EF3836D
        for <yamada@xxxxx.jp>; Wed, 15 Nov 2006 09:07:44 +0900 (JST)
Received: from nzvqxeq (unknown [61.80.27.211])
        by xxxxx.jp (Postfix) with SMTP id 419403836C1
        for <yamada@xxxxx.jp>; Wed, 15 Nov 2006 09:07:42 +0900 (JST)
Received: from 61.80.226.64 ([61.80.226.64]) by nzvqxeq with Microsoft SMTPSVC(5.0.2195.6713); Wed, 15
Nov 2006 09:16:19 -0800
Message-ID: <455B492A.2050407@db-cycles.co.uk>
Date: Wed, 15 Nov 2006 09:06:50 -0800
From: Micky Schaefer <uht@db-cycles.co.uk>
User-Agent: Thunderbird 1.5.0.7 (Windows/20060909)
MIME-Version: 1.0
To: yamada@xxxxx.jp
Subject: =?ISO-2022-JP?B?W1tTUEFNXV0=?= initiative
Content-Type: multipart/related;
 boundary="------------030301030400050800060107"
X-ProScan-SPAM: spam detect low
```

Receivedヘッダに送信元MTAのIPアドレスが記録されています。ProScanは直前のMTAのIPアドレスでのみチェックします。

これらの情報からログの確認方法について、チェックポイントを説明します。

まず、送信元MTAのIPアドレスを逆引きして、そのFQDNを得ます。デバッグログを採取していない場合には、以下のようにサーバのコンソールからコマンドを打って確認してください。

```
# dig -x 61.80.27.211

; <<>> DiG 9.2.1 <<>> -x 61.80.27.211
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 53655
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;211.27.80.61.in-addr.arpa.     IN      PTR

;; AUTHORITY SECTION:
27.80.61.in-addr.arpa.  10800   IN      SOA     rev1.kornet.net.
domain.rev1.kornet.net. 2001071900 43200 3600 604800 43200

;; Query time: 1186 msec
;; SERVER: 192.168.100.3#53(192.168.100.3)
;; WHEN: Wed Nov 15 14:24:12 2006
;; MSG SIZE  rcvd: 101

#
```

上記例は、逆引きできなかった例です。逆引きできない場合は、スパムメールと判定されます。その他、FQDNがドメイン識別のパターンに該当するものがスパムメールとなります。

次のポイントは設定グループです。②の内容を確認し、アドレスの所属グループの設定で処理しているか確認します。もし異なったグループで処理している場合には、その前に表示されているグループマッチのログで問題点を確認してください。

第4章 トラブルシューティング

アンチスパムの設定を行ったにも関わらず、思ったようにスパムを検出しない場合や、内部から送信したメールがすべてスパムと判定されるなど、想定外の動きをする場合は、この章を参考にトラブル解決してください。

4.1. spamと判定されないメールの確認

明らかにスパムメールにも関わらず、ProScanでスパムメールと判定されない場合は以下の点を確認してください。

- **スパムチェックを行う設定になっているか**

  グループの設定でSpamCheck=yesとなっていないと、メールのスパムチェックは実施されません。

- **メールヘッダから送信元MTAのIPアドレスを調べ、逆引きしてFQDNを得た後、そのFQDNがスパムのパターンになっているか**

  ProScanのアンチスパム機能の検出率は約95%なので、残り5%はProScanのスパムパターンにマッチしないFQDNのMTAから送付されます。その場合は、通常のメールとして処理されます。

- **オプションライセンスが有効か**

  ライセンスの有効期限が切れている場合には、スパムチェックを行いません。licenseviewerコマンドで有効期限を確認してください。

- **スパムWBLでホワイトリストに載っていないか**

  ホワイトリストを設定している場合、そのパターンにメールの送信元MTAのFQDNが含まれていないか確認してください。正規表現のパターンマッチなので稀に一致している可能性があるかもしれません。

- **グレイチェックが有効で、ライトグレイリストにIPアドレスが登録されていないか**

  グレイチェックを有効にしている場合、自動的にホワイトリストに登録されていることがあります。その場合は、スパムと判定されません。

- **Subjectへ追加する文字列が設定されているか**

  ProScan自体はスパムと判定してるが、Subjectへの追加文字列が設定されていないため、メールを見ただけでは判断できないことも考えられます。

これらは、メールのヘッダやProScanのログを調べることにより確認できます。

4.2. spamと判定されてしまうメールの確認

ProScanのアンチスパムの基本が、コンテンツフィルターではなく、送信元のIPアドレス情報を元に行っているため、環境によっては、内部からのメールをspamと判定してしまう場合が多々あります。それを防ぐための仕組みも用意されているのですが、設定を正しく行わないと機能しないため、スパムメールで無いのにスパムの判定をされてしまう場合があります。スパムメールでないのspamと判定されてしまう場合には、以下の点を確認してください。

- **内部からの送信時に発生する場合**

  内部からのメール送信は、ほとんどがMUA（メールクライアント）からのものですが、端末個別にIPアドレスが振られていても、逆引き設定まで行われている場合は稀ですので、この様な状況が発生します。
  これを防ぐ一番簡単な方法は、WBL設定（これはスパムWBLでなく、ProScan全体のWBL設定です）において内部ネットワークの許可を行い、その場合のチェックをウイルスのみにすることです。
  例えば、内部のネットワークが192.168.0.0/24の場合には、以下のような設定を行うことで可能です。

```
[smtpscan.wbl]
AcceptIP=127.0.0.1
AcceptName=localhost
AcceptNet=192.168.0.0/24
AcceptLevel=1
```

これにより、内部ネットワークからのメール送信はウイルスチェックのみとなります。
もう一つは、DracDB機能を利用することです。これは、POP Before SMTPのデータベースを利用することで、認証をクリアしたSMTP接続はスパムチェックを行わないという機能です。POP Before SMTPを利用されている場合はこちらを利用することも可能です。
また、外部ネットワークから自サーバ経由でメールを送信することができるようにしている場合には、このDracDBを使わないと、すべてスパムと判定される可能性が高くなります。

現時点ではSMTP AUTHのDBを利用できるような仕組みは用意されておりません。

- **外部からの受信時に発生する場合**

取引先からのメール等、外部からのメールがspamと判定される場合は、送信元IPからFQDNを調べてその内容を確認します。ProScanのスパムパターンにマッチする場合は、そのFQDNをホワイトリストに登録して救済します。

メールアドレスをホワイトリストに登録しても救済されませんのでご注意下さい。

- **送信者のメールアドレス（エンベロープFrom）で救済したい**

ProScanのアンチスパム機能は、送信元のIPアドレスで行うため、メールのFromaアドレスやToアドレスで判定することはしません。これは、これらの情報が容易に偽装できるため、信頼性が低いためです。さらに最近のスパムメールは、自分のドメインを語って送られるもの多いので、すり抜けるスパムも多くなる可能性があります。しかしながら、ProScanでは、グループ定義を利用することで、Fromアドレスでのホワイトリスト作成が可能です。以下にその方法を説明します。

まずは、１つグループを作成します。このグループは、今まで利用していたグループと同じ内容を定義します。（グループを作成していなければ、defaultグループの内容となります。）

そのグループの[smtpscan.group]セクションにSendersパラメータを指定し、そこにスパムと判定したくないアドレスを登録します。また、SpamCheckパラメータをnoに設定します。

以上で完了です。

4.3. spamメールのテスト方法

ProScanのスパムチェックは、メールの内容でチェックを行うのではないので、テストをしようとスパムメールを転送しても、spamと判定されません。これは、送信元が普段ご自身が利用しているMTAとなるためです。

そこで、実際にそのメールがスパムと判定されるかのテスト方法を以下にご説明します。

```
Return-Path: <uht@db-cycles.co.uk>
X-Original-To: yamada@xxxxx.jp
Delivered-To: yamada@xxxxx.jp
Received: from localhost (localhost [127.0.0.1])
        by xxxxx.jp (Postfix) with SMTP id B06EF3836D5
        for <yamada@xxxxx.jp>; Wed, 15 Nov 2006 09:07:44 +0900 (JST)
Received: from nzvqxeq (unknown [61.80.27.211])
        by xxxxx.jp (Postfix) with SMTP id 419403836C1
        for <yamada@xxxxx.jp>; Wed, 15 Nov 2006 09:07:42 +0900 (JST)
Received: from 61.80.226.64 ([61.80.226.64]) by nzvqxeq with Microsoft SMTPSVC(5.0.2195.6713); Wed, 15 Nov 2006 09:16:19 -0800
Message-ID: <455B492A.2050407@db-cycles.co.uk>
```

上記は、明らかにspamメールとわかるメールのヘッダ情報の抜粋です。メールクライアントのヘッダ情報参照機能で確認したものです。着目するのは、Receivedヘッダの送信元MTAの情報です。これは自身のMTAがメールを受信した際に付加する情報ですので信頼性は高いです。

この例は、PostfixがMTAの場合の例ですので、一旦Postfixのsmtpdがメールを受信した後、ローカルホスト経由でProScanに渡しているため、Receivedヘッダが２つ追加されています。

【最初に受信したときのReceivedヘッダ】

```
Received: from nzvqxeq (unknown [61.80.27.211])
        by xxxxx.jp (Postfix) with SMTP id 419403836C1
        for <yamada@xxxxx.jp>; Wed, 15 Nov 2006 09:07:42 +0900 (JST)
```

ProScanはこの情報から、送信元MTAのIPアドレスを抽出して逆引きしますので、それと同じことを行えばテストは可能です。ProScanではチェックモジュールのproscanmsにこのIPアドレスを渡してメールの内容をチェックすることが可能です。proscanmsはLMTP（Local Mail Transfer Protocol）により、SMTPと同様のコマンドでメールの送信処理を行うことが可能です。その中でウイルスやスパムのチェックを行いますので、この機能を利用しスパムチェックをテストすることが可能です。

以下、その方法を説明します。

①proscanmsの起動（サーバのコンソールで）します。

```
# /opt/proscan/bin/proscanms -r 61.80.27.211
220 avtest.promark-inc.com LMTP ProScan Promark Inc.
```

②LMTPモードでの入力待ちになりますので、LHLOコマンドを投入します。

```
LHLO ns.promark-inc.com
250-avtest.promark-inc.com
250-ENHANCEDSTATUSCODES
250-XVIRCHECK
250-DSN
250 8BITMIME
```

③MAILコマンドでFromアドレスを投入します。何でも構いません。

```
MAIL from:<abcd@efgh.com>
250 2.1.0 <abcd@efgh.com>... Sender OK
```

④RCPTコマンドでToアドレスを投入します。ご自身のアドレスを使います。

```
RCPT to:<test@proscan.promark-inc.com>
250 2.1.0 <test@proscan.promark-inc.com>... Recipient OK
```

⑤DATAコマンドを投入します。内容は特に問いませんが、元メールのReceivedヘッダ以下を利用するのが簡単です。

```
DATA
354 Enter mail, end with "." on a line by itself
Message-ID: <455B492A.2050407@db-cycles.co.uk>
Date: Wed, 15 Nov 2006 09:06:50 -0800
From: Micky Schaefer <uht@db-cycles.co.uk>
User-Agent: Thunderbird 1.5.0.7 (Windows/20060909)
MIME-Version: 1.0
To: yamada@xxxxx.jp
Subject: =?ISO-2022-JP?B?W1tTUEFNXV0=?= initiative

本文の内容は何でも構いません。
test
.
250 2.6.0 Message accepted
```

⑥QUITコマンドで終了します。

```
QUIT
221 2.0.0 avtest.promark-inc.com Closing connection
#
```

⑦ログおよび配送されてきたメールでちゃんとspamと検出されている確認します。
以下は、ログの抜粋です。

```
[2006/11/20 09:48:45]-[30419.1] proscanav scannig start...
[2006/11/20 09:48:45]-[30419.1] [DEBUG] SAVAPI scan result = 0,
        filename = /var/opt/proscan/tmp/7CMBo3.030419.00000000, mode = 2
[2006/11/20 09:48:45]-[30419.1] [DEBUG] SPAM check: 0,yes,1
[2006/11/20 09:48:45]-[30419.1] [DEBUG] spam_check:61.80.27.211
[2006/11/20 09:48:45]-[30419.1] [DEBUG] rbl_check:non spam(211.27.80.61.dnsbl.njabl.org)
[2006/11/20 09:48:45]-[30419.1] [DEBUG] rbl_check_status:Name or service not known
[2006/11/20 09:48:45]-[30419.1] FQDN check:spam
[2006/11/20 09:48:45]-[30419.1] SPAM result: 1
[2006/11/20 09:48:45]-[30419.1] Message-ID: <455B492A.2050407@db-cycles.co.uk>
[2006/11/20 09:48:45]-[30419.1] SCAN result: spam
[2006/11/20 09:48:45]-[30419.1] spam detect(1): From:Micky Schaefer <uht@db-cycles.co.uk>
        To:yamada@xxxxx.jp Subject:[[SPAM]] initiative
[2006/11/20 09:48:45]-[30419.1] [DEBUG] check param: [smtpscan.spam_action.low]
[2006/11/20 09:48:45]-[30419.1] [DEBUG] AddSubject: [SPAM:Low]
[2006/11/20 09:48:45]-[30419.1] [DEBUG] AddHeader: X-ProScan-Status: spam detected low
[2006/11/20 09:48:45]-[30419.1] [DEBUG] modify subject: =?ISO-2022-JP?B?W1NQQU06TG93XQ==?=
        =?ISO-2022-JP?B?W1tTUEFNXV0=?= initiative
[2006/11/20 09:48:45]-[30419.1] [DEBUG] Mail delivery status:200
[2006/11/20 09:48:45]-[30419.1] Message checked
```

4.4. 誤ってライトグレイリストに登録されてしまったアドレスの削除

付録．Aを参照下さい。

4.5. Windowsでの確認方法

ヘッダ情報から直近のIPアドレスを抜き出します。（上にあるReceivedヘッダほど自分に近い情報になります。）
下記、ヘッダ情報からは213.21.176.178というのが分かります。

このIPアドレスを逆引きすると、スパムかどうかの判定ができます。例えば、213.21.176.178を逆引きしてみます。
Windowsのコマンドプロンプトを起動します。

nslookupというコマンドを打ち込みます。

```
C:¥Documents and Settings¥promark>nslookup
```

">"のようなプロンプトが返って来るので、

```
>set q=ptr
>213.21.176.178
```

と打つと以下のような結果が返ってきます。

```
Server: ns.promark-inc.com
Address: 61.197.232.227
Aliases: 227.232.197.61.in-addr.arpa

Non-authoritative answer:
178.176.21.213.in-addr.arpa     name = smtp.akmail.it

175.21.213.in-addr.arpa nameserver = dns1.aknet.it
175.21.213.in-addr.arpa nameserver = dns2.aknet.it
dns1.aknet.it   internet address = 213.21.141.2
dns2.aknet.it   internet address = 213.21.164.2
```

この“name = smtp.akmail.it”が逆引きの結果なので、このFQDNはsmtp.aknet.itであることがわかります。このnameが無い場合は逆引きが設定されていないということです。

逆引きが設定されていないか、例えば、213-21-176-178-akmail.itなどというIPアドレスが付いたFQDNの場合にはスパムと判定されます。

付録A. listadm.plスクリプトについて

1. 概要

本スクリプトは、ライトグレイリストに登録されているIPアドレスを参照・管理するためのスクリプトです。
誤って登録されたIPアドレスの削除を削除するために利用できます。

2. 書式

```
listadm.pl list
listadm.pl del IP_address
```

3. 機能

listの場合、DBファイルの中身を一覧表示します。
del IPの場合、指定したIPアドレスを削除します。
※ライトグレイリストへのパスを変更するには、スクリプトの変数($list)を書き換えて下さい。

4. 利用例

以下に本スクリプトの使用例を示します。

・リスト処理

```
# ./listadm.pl list
210.143.111.206
210.174.175.11
61.194.78.27
219.112.120.31
219.96.95.138
202.221.253.153
210.251.127.131
219.118.164.138
61.120.24.68
202.224.246.218
221.255.94.58
219.99.79.215
220.150.172.201
218.226.178.103
202.229.202.10
61.207.64.39
210.189.105.27
222.122.45.210
202.229.202.100
```

・削除処理

```
# ./listadm.pl del 71.144.111.105
entry delete
```

5. その他

本スクリプトは、http://www.promark-inc.com/download/ProScan/listadm.gzよりダウンロードしてください。
LinuxおよびSolaris用になっていますので、BSD系の方は、ライトグレイリストのパスを変更してご利用下さい。

付録B. 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/support/index.html**をご覧ください。 技術的な質問は下記までお問い合わせ下さい。 Eメール：**support@promark-inc.com**
ライセンスや製品の購入に関するお問い合わせ	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：**sales@promark-inc.com**
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：**info@promark-inc.com**

ProScan
アンチスパム設定ガイド　第２版

発行日　2008年7月1日
作成元　株式会社プロマーク

promark

株式会社プロマーク