Qmail vs. spam

木村博美

筑波大学） 加速器センター

概要

Qmail[1]は簡潔なプログラムの集まりであり、色々と手を加えることが比較的容易です。このことは spam 対策をする上でも有効です。本稿では加速器センターで実施した spam 対策について報告します。

1　はじめに

加速器センターは筑波大学の一施設です。メイルサーバには 1998 年から Qmail を使用しており、現在のメイルアドレスは約 60 です。年々増加する spam に対し、様々な対策を実施してきました。図 1 に 2003 年の受信メイルの統計を示しますが、受信拒否したメイル数の増加は spam の増加を反映しています。

現在のメイルサーバで受信メイルを配送するまでの流れは次のようになっています。

- tcpserver – IP アドレスでのアクセス制限
- rblsmtpd – 外部ブラックリストの参照
- qmail-smtpd – エンベロープでの制限
- anti-virus – ウイルスの除去
- spamassassin – ヘッダと本文での制限
- qmail-queue – メイルの配送

2　受け取らない工夫

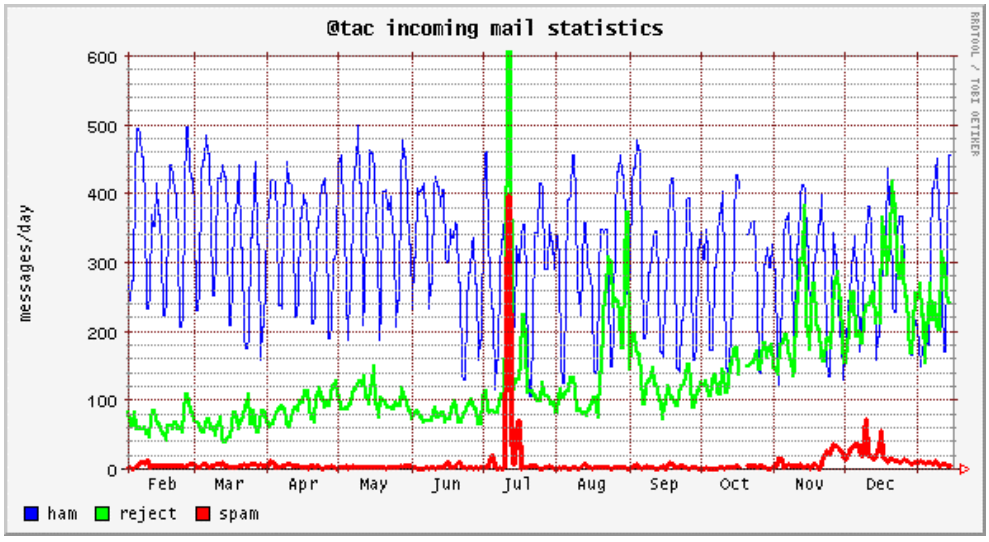

図 1.） 受信メイルの統計

ham（青）は受け取ったメイルの内 spam でなかったもの
reject（緑）は受け取りを拒否したメイル
spam（赤）は受け取ったメイルの内 spam と判定したもの

2.1 tcpserver

IP アドレスでのアクセス制限を掛けるために SMTP ポートは tcpserver で受けています。メイルサーバのログや受け取った spam のヘッダなどから、自前のブラックリスト／ホワイトリスト（図 2）を作成しており、SMTP で接続されると先ず、tcpserver によりこのリストが検索されます。

```
# ホワイトリスト（rblsmtpd を通過させる）
130.158.:allow,RBLSMTPD="",TCPREMOTEHOST="tsukuba.ac.jp"

# ブラックリスト（rblsmtpd でエラーを返させる）
123.456.7-8.:allow,RBLSMTPD="Blocked … (2003/11/20)"

# デフォルト
:allow
```

図 2. tcpserver 用リスト（抜粋）

Tcpserver は deny を指定すれば、IP 接続を切断できますが、相手が普通の MTA の場合にはかなりの回数リトライされるのであまり効果的ではありません。そこで全て allow で通し、次の rblsmtpd で SMTP エラーを返させ、セッションを閉じるようにしています。

なお、リストにアドレスを登録する際には hinfo[2]を使って調べています。

2.2 rblsmtpd

送信元が自前のブラックリスト（現在 740 エントリ）に該当した場合は、環境変数 RBLSMTPD が設定されているので、SMTP の 550 エラーを返し、セッションを閉じます。リストに無い場合には、外部のブラックリストを調べ、該当したら同様に 550 エラーを返します。ただし、外部のブラックリストはアドレス範囲を広めに登録されることがあり、小さい会社などが誤って判定されることがあるので、その場合には自前のホワイトリストに登録します（現在 120 エントリ）。

また、外部のブラックリストは spammer の攻撃などで運用を停止することがあるので、定期的にチェックする必要があります（例えば http://www.sdsc.edu/~jeff/spam/cbc.html）。

2.3 qmail-smtpd

SPAMCONTROL[3]パッチによりエンベロープの From と To のチェックを強化しています。ただ、From は詐称されていることが多いのであまり有効ではありません。To に関しては、卒業生のメイルアドレスなどの受け取りたくないアドレスを badrcptpatterns というファイルに登録しておくと、SMTP の 550 エラーを返しセッションを閉じます。この機能がないと、smtpd がエラーメイルを生成し、送信元に返そうとしますが、元々送信元は詐称されているので、結局エラーメイルが自ホストの postmaster に配送されてしまいます。Postmaster 宛てのメイルを無視しないためにも無駄なエラーメイルは極力生成しないようにしています。

2.4 対策の効果

図 3 に受信拒否メイルの内訳を示します。外部ブラックリストは 4 月から使用していますが、ほぼ一定の効果を挙げています。自前リストや badrcptpatterns による拒否は spam が集中している場合に効果がありました。12 月から自前リストの効果が上昇しているのは、11 月に導入した SpamAssassin からのフィードバックと、リストに登録する際のアドレス範囲を広げたためです。

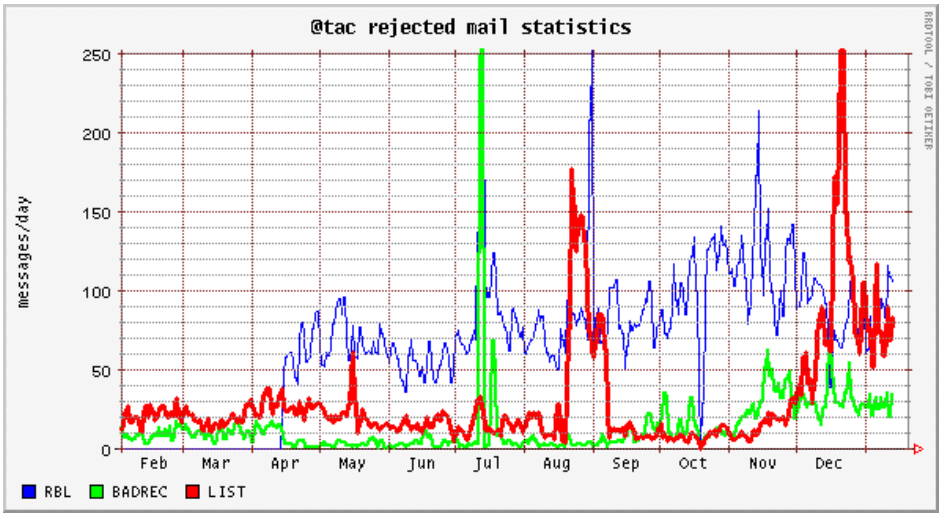

図 3. 受信拒否メイルの内訳

RBL（青）は外部ブラックリストによる拒否
BADREC（緑）は badrcptpatterns による拒否
LIST（赤）は自前ブラックリストによる拒否

3 受け取ってしまったら

3.1 SpamAssassin[4]

最近では worm/virus に感染した PC が open proxy に仕立てられるケースが多いので、送信元 IP アドレスとエンベロープのチェックでは spam 対策は不充分になってしまいました。そこで、ヘッダと本文をチェックするために 2003 年 11 月から SpamAssassin を使用しています。メイルを受信する度に SpamAssassin を起動するのは効率が悪いので、spamd デーモンを起動しておき、spamc コマンドでチェックしています。単に spam 判定をするだけなら、図 4 のようなスクリプトで qmail-queue を置き換えれば良いのですが、しばらく使ってみた結果、かなりの精度で spam 判定できたので、現在は図 5 のようなスクリプトで spam メイルを隔離し、ユーザに配送しないようにしています。また、隔離した spam メイルを定期的にチェックし、送信元を自前リストに追加しています。

```
#!/bin/sh
/usr/local/bin/spamc | /var/qmail/bin/qmail-queue.org
```

図 4. qmail-queue スクリプト 1

ただし、SpamAssassin はソースが公開されているため、spammer も次々と対抗策を出してくるので、ML などで動向を見守る必要があります。

3.2 アドレス詐称

受け取ったメイルの中で最も困るは、我々のドメインを騙った spam のエラーメイルです。一日数通という場合もあれば、一日何千通という場合もあります。図 1 の 7 月のピークはまさしくそれでした。

私は一通でもそのようなメイルを受け取ったら、hinfo で送信元や中継ドメインの連絡先を調べ（大抵は abuse@ですが）、苦情メイルを送るようにしています。

```
#!/bin/sh
# spamc/spamd を使って spam 判定をし、設定レベル以上なら隔離（配送しない）
#  オリジナルの qmail-queue は qmail-queue.org に rename し、
#  この script を/var/qmail/bin/qmail-queue にコピーする
#       # chown qmailq:qmail qmail-queue
#       # chmod 4755 qmail-queue
#  （FreeBSD では script は setuid できないので 755 でも同じ）
# SpamAssassin の必要な設定
#       clear_headers
#       add_header spam Status _YESNO_, hits=_HITS_ ...
# $Id: qmail-queue.sa3,v 1.5 2003-12-25 14:57:46+09 hiromi Exp hiromi $

QMAILQ=/var/qmail/bin/qmail-queue.org          #  オリジナルの qmail-queue
SPAMC=/usr/local/bin/spamc                     # spamd が起動されていること
H822=/usr/local/bin/822header                  #  メイルヘッダを切り出すプログラム
QLEVEL=5                                       #  隔離レベル（整数で指定）
QDIR=/var/spam                                 #  隔離場所
nospamctl=/var/qmail/control/nospamcheck       # spamc を使用しないようにする設定ファイル
#  一時的に spamc を使用しないなら、環境変数 NOSPAMCHECK を設定する
##############################################################################
day=`date "+%Y%m%d-%H%M%S"`                    # current date,time
ofile=$QDIR/${day}.$$                  #  隔離する場合のファイル名
ifile=${ofile}.in                      #  メイルのオリジナル
umask 077
# root で起動された場合、あるいは$nospamctl ファイルが存在する場合、
#  あるいは環境変数 NOSPAMCHECK が設定されている場合はそのまま配送
if [ `id -u` -eq 0 -o -e $nospamctl -o ! -z "$NOSPAMCHECK" ]; then
   exec $QMAILQ
fi
if [ -e $ifile -o -e $ofile ]; then    #  作ろうとするファイルが既に存在する場合（sym link attack）
   exec $SPAMC | $QMAILQ               # spamc  経由で配送
fi
touch $ifile 2> /dev/null              #  ファイルが作成できない場合
if [ $? -gt 0 ]; then
   exec $SPAMC | $QMAILQ               # spamc  経由で配送
fi
cat - > $ifile                         #  メイルのオリジナルを残す
$SPAMC < $ifile > $ofile               # spam  判定
# spam  度を得る
line=`$H822 < $ofile| grep '^X-Spam-Status' |tail -n 1`
hits=${line#X*=}                       # strip 'X-Spam ... hits='
rate=${hits%%.*}                       # strip '.0 required= ...'
[ -z $rate ] && rate=0
if [ $rate -ge $QLEVEL ]; then         #  指定レベル以上の  spam  だったので配送せずに終了
   rm $ifile                           #  オリジナルだけを消去（$ofile が残る）
else
   cat $ofile | $QMAILQ                #  指定レベル以下なので、配送する
   rm $ifile $ofile                    #  一時ファイルを削除
fi
```

図 5.』 qmail-queue スクリプト 2

参考文献

[1] Qmail (http://www.qmail.org/)

[2] Hinfo (http://www.blars.org/hinfo.html)

[3] SPAMCONTROL (http://www.fehcom.de/qmail/spamcontrol.html)

[4] SpamAssassin (http://www.spamassassin.org/)