spam 対策に特化した SMTP wrapper の実装と検証

広瀬雄二　　大駒誠一
yuuji@koeki-u.ac.jp　　okoma@ae.keio.ac.jp
東北公益文科大学

2004 年 9 月 24 日

この数年で UBE(Unsolicited Bulk Email) いわゆる spam は脅威的な増加の一途をたどり，それに対処するための計算機資源，ネットワーク資源の多くが浪費されている．それらに対抗する目的で電子メイル本文を走査し，統計的手法に基づいて不要と予想されるものをふるい落とす「spam フィルタ」が数多く研究・開発され，既に欠かせないもとのしての認識も高まっている．そのいっぽうで，要らないメイルに対して spam フィルタをかける計算機負荷や，一度本文を受け取ってしまうと送信者から見たら送信成功と思われてしまう問題が存在する．本稿ではメイルの送信者の SMTP セッション時の情報だけを元に，メイル本文を見ることなく即座に受信拒否を行なう手法を提案する．さらに，MTA の種類に依らずその手法を実現する SMTP wrapper を実装して実際に運用した結果を示す．
キーワード: SMTP セッションフィルタ, SMTP ラッパー, spam フィルタ

Implementation and Verification of SMTP Wrapper for Spam Rejection

HIROSE Yuuji　　OKOMA Seiichi
yuuji@koeki-u.ac.jp　　okoma@ae.keio.ac.jp

Tohoku University of Community Service and Science

We receive excessively high amount of UBE(Unsolicited Bulk Email), so called spam, in these years. Many researchers have contrived ‘spam filter’ which scans the body of email and decides whether it is spam or not by statistical analysis. However, it becomes problem that those unnecessary computing load is raising and that receiving message body for analyzing let spammers assume they succeeded in sending spam. In this paper, we propose an SMTP wrapper which rejects unsolicited emails by SMTP session parameters without seeing message body, and also report the practical performance of its implementation, ‘antibadmail’, which is generic MTA wrapper specialized in bad mail rejection.
Keywords: spam rejection, SMTP session filter, SMTP wrapper

1 背景

電子メイルがゴミまみれになって久しい．UBE (Unsolicited Bulk Email)，いわゆる spam はもはや社会問題に発展している．メイルサーバレベル，あるいはメイル受信者レベルにおいて，受け取ったメッセージの本文をフィルタプログラムに通し，「クロ」つまり受け取りたくないものであると判定されたものを除外したりすることも一般的になっている．このような，本文を走査する「コンテンツフィルタ」は統計学的手法を用いることで高い認識成功率が得られるようになってきた．そのいっぽう，その機能が高度であればあるほど，メッセージ 1 通に対する計算機負荷は高くなる．全体のメイルに対する spam の割合が過半数を超えたとも言われる中，将来的に spam フィルタを動かす負荷は全世界のサーバの資源を圧迫して行くことは想像に難くない．

また，コンテンツフィルタでは，MTA 的に見ていったんメッセージ全体を受け取って SMTP 接続を終了してしまうため，送られたものが spam と分かってももはや送信者にそのことを伝える術がない[1]．このことは，ウィルスを排除するメイルスキャナにも当てはまる．とくにメイルスキャナでは，ウィルスを発見するとそのメッセージヘッダに書かれた差出人アドレスを信用してそこにバウンスを返すものが多い．もちろんそれは詐称されたものがほとんどなので，身に覚えのないエラーを送られた側は迷惑であるし，それが存在しないアドレスならダブルバウンスを生み，ネットワーク負荷を無駄に浪費することにつながる．

以上のことから，電子メイル送受信時に関して，

- SMTP セッション時に spam と分かるならその場で直ちにエラーを返すべき
- 一度受信を完了したら下手にバウンスを返してはならない

という事が重要であると言える．

そこで本稿では，SMTP セッション時に可能な限り spam を排除して直ちにエラーを返す手法を提案し，ならびにその機能を MTA の種類を問わずに導入するのに有効な SMTP wrapper の ‘antibadmail’ を実装し実運用環境に適用した結果を報告する．

[1] ほとんどの spam は FROM アドレスが詐称されているのでメッセージのヘッダにある差し出し人情報は信用できない．Received ヘッダには送信したホストの IP アドレスが記されているが，そのホストが SMTP 接続を受ける保証はない．

2 SMTP セッションフィルタ

2.1 古来のセッションフィルタ

spam が問題化し始めた 1990 年代後半には，第三者不正中継 を許可する設定 (Open Relay) に陥っているメイルサーバを介して spam がばらまかれた．そのため，Open Relay になっているメイルサーバの IP アドレスを全世界的に集めてそこに登録された IP アドレスからの受信を拒否するような動きが見られた．現在でもそうしたデータベースは数多く公開されていて，MAPS[3] や SORBS[4] などはその代表的なものである．しかし，それらは運営されている国 (主に欧米) の価値基準によってデータの登録が行なわれているため，アジア圏の IP アドレスブロックが無用に大きなレンジで登録されることもあり，日本のメイルサーバ管理者が使うには不都合が多い．実際，筆者の契約しているプロバイダの固定アドレスブロックも SORBS の「動的割り当てアドレスデータベース」に登録されているので，送信に支障を来たしている事実がある．

国民同士の交流のあまり無い国どうしならともかく，日本人にとってアジア圏の IP アドレスが簡単に登録されるデータベースは利用しづらい．日本人の利用するメイルサーバであれば，日本人の判断基準で作成されるデータベースの方が望ましい．一般化すれば，当該国の地理交流特性を加味したデータベースをその国の人間が管理するものであるのが望ましい．

2.2 求められるセッションフィルタ

クライアントからの SMTP 接続時には，最低でもサーバ側に以下の 3 パラメータが送られる [2]．

- HELO(EHLO)
  クライアントの識別名．通常クライアントの FQDN だが必須ではない
- MAIL FROM
  実際の送信者のメイルアドレス[2]
- RCPT TO
  実際の受信者のメイルアドレス[2]

[2] メッセージの本体に現れる From: ヘッダ，To: ヘッダとは異なり，転送された場合などの最終的な宛先を示す SMTP のパラメータである．

これらに加えて，サーバ側では，接続してきたクライアントの

- IP アドレス
- その IP アドレスの逆引き (PTR) レコード

も送信側に関する情報として利用できる．これらのうち RCPT TO 以外の情報は送信者側の身元，あるいはその一部を示す値であるから，spam 送信者は**隠したり偽造したりしたがる**傾向がある[3]．この性質を利用すると，SMTP セッションの本文を受け取る前の段階で多くの spam が拒否できることが予想される．

この予想に基づき筆者は 2002 年 12 月から qmail[1] の SMTP デーモンプログラム (`qmail-smtpd.c`) にパッチを当てる形で上記の 5 要素をもとにメッセージの受信/拒否を決定するシステムを構築・改良してきた．また，それを運用しその有効性を確認することができた (qmpatch[7, 8])．今回は，qmail だけでなく SMTP デーモンの外側に被せる形で，qmpatch と同等以上の spam 拒否機能を持つ SMTP wrapper “antibadmail” を新規に実装し，qmail 以外の全ての MTA でも統一的な spam 拒否が可能となることを目指した．

3 システム構成

本研究で構築した MTA をとりまくシステム構成を図 1 に示す．外部からの SMTP 接続をいったん tcpserver[4]で受け，クライアントのアドレスに応じた環境変数を設定した上で antibadmail に制御を渡す．antibadmail は，SMTP クライアントとのチャネル，Local MTA とのチャネル両方を開いたまま，クライアントからのリクエストを MTA に送り，それに対する MTA からの応答コードをクライアントに返す．このとき，antibadmail は tcpserver から与えられたクライアントアドレスに関する情報と，SMTP の 3 パラメータ HELO(EHLO), MAIL FROM, RCPT TO に着目し，以下の基準でクライアントからのメッセージ送信を許可するか拒否するか決定する．

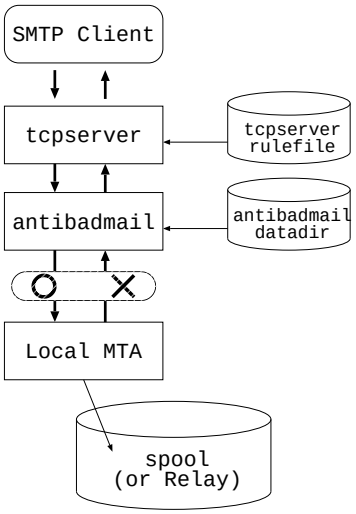

図 1: antibadmail システム構成

1. tcpserver のルールデータベースにより「ブラックリスト」のマーク (環境変数 BADHOST) が設定されているか
2. DNS の逆引きレコードが偽造になっているか
3. HELO で指定された文字列が
   (a) HELO 文字列ブラックリスト (badhelo) 中の特定のパターンにマッチするか
   (“yahoo.com”, “hotmail.com” を HELO 文字列に指定するものは spam である)
   (b) ドットを含む FQDN らしき文字列になっているか
   (“pc123” など個人 PC に適当につけた名前からのものはウィルスの可能性が高い)
   (c) IP アドレスの場合，
   - known ホスト[5]であれば，実際の IP アドレスと一致するか
   - unknown ホスト[6]であれば常に不許可

   (d) 受信サーバの IP アドレスや FQDN，メイルドメインになっているか

[3]悪事を働くのに正しい身分証明書を見せる可能性が低いのと同様．

[4]UCSPI-TCP[5] に含まれる TCP 接続専用のスーパーデーモン．アクセス制御やデーモンプロセス起動時の環境変数設定機能を持つ．

[5]正しく PTR レコードが登録されているホスト

[6]PTR レコードが未定義または A レコードと一致しない不正な名前が登録されている IP アドレスであるホスト

(HELO で相手のアドレスを指定するのは不正なクライアント)

(e) 受信者 (RCPT TO) アドレスと一部または全体がマッチするか

(f) 虚偽に使われやすくなおかつ交流の可能性の低い国別トップレベルドメインを名乗っているか (unknown ホストにのみ適用)

(g) HELO で名乗ったホストが実在するドメインか (unknown ホストにのみ適用)

4. MAIL FROM が特定の送信者ブラックリスト (badmailfrom) に含まれるパターンにマッチするか

5. MAIL FROM がドメイン部 (@記号以降) を含む正しい形式か

6. MAIL FROM のドメイン部が実在するドメイン名か

7. RCPT TO が宛先ブラックリスト (badrcptto) に含まれるパターンにマッチするか

上記 3a および，4 には `hotmail.com` などの詐称されやすい著名なドメインも含めることになる．ただし，そのままでは本当に `hotmail.com` のサーバから送られた正しい `@hotmail.com` ドメインのメイルが届かなくなるため，正しい逆引き名が `*.hotmail.com` となるサーバからは`@hotmail.com` を MAIL FROM にもつメイルは受信するようにする．これは，tcpserver のルールファイルで GOODMAILFROM 変数を以下のように設定することで効果が得られる (実際には 1 行で記述).

```
=.hotmail.com:allow,
GOODMAILFROM="@hotmail.com"
```

HELO 文字列に関しても，本物のサーバに対してだけ許可するための変数 GOODHELO を設定することで同様の効果が得られる．

特殊なケースとして，利用者のうち誰かが以前利用していたメイルアドレスを，現在利用しているアドレスに転送するような場合がある．このとき以前利用していたサーバで十分な spam 対策を施していない場合，数多くの spam が転送されて届くことになる．かといって，転送元の組織にあるメイルサーバを「IP アドレスのブラックリスト」に追加するわけにはいかない．そこで，典型的な転送元メイルサーバに関して,「転送を受理する送信者メイルアドレス (のワイルドカード)」を指定できるようにした (PASSONLY 変数).

以上の検査を経て，antibadmail が「クロ」と判定したものに関しては，MTA に本文 (DATA) を渡す前に，クライアントに SMTP 応答コード 5xx[7]を返し受信拒否する．このとき，MTA には QUIT を送信してセッションを終了する．

その他,「spam でも何でもいいから全て受け取りたい」というケースもあるため，特定の宛先アドレスにはフィルタなしで全て通過させることもできる．さらに，信頼できる別のサーバから転送されて来たメイルの経路 (Received ヘッダ) による拒否判定を目的として，メッセージのヘッダ部分を先に吟味してから MTA に受け渡すかどうかを決定することも可能であるが，本稿の主眼から外れるためここでは触れない．

4 ブラックリストの構築

4.1 構築時のポリシー

本来電子メイルは，国境を超え全ての人とやりとりできる可能性を持つものである．しかしそれは性善説が全域に通用した時代のことで現在は異なる．本研究でとりあげている運用環境では，以下のポリシーによりブラックリストを登録している．

1. 著名なメイルサービス (とくに無料のもの) のドメイン部は詐称されたものがほとんどなので badmailfrom データベースに登録すると同時に，本物のサーバから受け取れるように tcpserver のデータベースに GOODMAILFROM 変数を登録する

2. 通過した spam を送って来たホストを調べ

   - 自サイト利用者の交友が無さそうな国の ISP ならアドレスブロック全て
   - 交友がありそうな国 (主に日本) なら，動的割り当てブロックのみを一時的に (適宜判断)

それぞれブラックリスト (BADHOST) に登録

[7]恒久的エラーを意味する．つまり，受信しない．

3. 既存の badhelo/badmailfrom データベースに一致するパラメータを送って来たものは「前科者」として，以降の送信を拒否するように tcpserver のルールデータベースの BADHOST として自動登録する．

本稿の運用環境のブラックリストは，qmail にいくつかの spam 拒否パッチを当てて運用し始めた 2000 年頃からの蓄積物である．作成開始時から qmpatch 導入後しばらくまでの間は，典型的な詐称アドレスや異常 HELO の登録作業が大半を占めたが，それらの多くが拒否できるようになったのちは，大量発信の拠点となる BADHOST を登録する作業が大半を占めるようになった．

筆者らの構築するブラックリストは「国内のプロバイダのアドレスは慎重に，国外のものは大胆に」というポリシーで登録が行なわれている．第三者となるサイトの管理者がこれを利用する場合，そのサイトの利用者にとって身近な国外ドメインが含まれてしまう危険性もあるが，その場合でも tcpserver のルールデータベースにそのドメインを信頼する変数定義を付加することで簡単に回避できる．

4.2 データベースの構成

IP アドレスに基づくブラックリストデータベースは tcpserver 用のルールファイルとして登録する．いっぽう，SMTP の 3 パラメータと照合するブラックリストデータベースは「datadir 形式」で登録する．datadir 形式とは，そのエントリ名が Unix ファイルシステムの 1 ファイルとして存在する形式である．たとえば，MAIL FROM アドレスとして `foo@bar.baz`, `*@foo.bar`, `*@*.foo.bar` (*は任意の文字列) を拒否したいときは，所定のディレクトリにそれぞれ

```
foo@bar.baz
@foo.bar
.foo.bar
```

という名前の空ファイルを作成する．1 つのエントリの追加と削除が，他のエントリの存在性に影響しないため antibadmail 走行中に更新作業を行なっても良い．

実運用環境では，複数管理者によるデータベースの共有を効率化するため，1 行 1 エントリで記述したテキストファイルを CVS のレポジトリに入れて管理している．そしてテキストファイルを datadir 形式に変換するユーティリティを利用して antibadmail に与えている．

表 1: 受信許可/拒否の実数

接続総数	受信許可	受信拒否
8635	3498(40.5%)	5137(59.5%)

表 2: 受信拒否根拠

MAILFROM による拒否		2142
内訳	存在しないドメイン	228
	不正な文字を使用	224
	badmailfrom にマッチ	1710
RCPT TO による拒否		1546
内訳	存在しないユーザ	1055
	badrcptto にマッチ	491
HELO による拒否		1866
内訳	badhelo にマッチ	1110
	上記以外のドットなし	145
	相手のドメインと一致	585
	unknown ホストからの badhelo	147
	不在ドメイン (unknown ホスト)	71
	その他不正な HELO	11
IP アドレスに基づく拒否 (BADHOST)		1552

5 適用結果

2004 年 8 月 17 日から 21 日の 5 日間，筆者が運営するサイト (利用者 38 名) で主メイルサーバに外部から届いたメイルを受信許可/拒否した結果を表 1 に示す．また受信拒否したものについて，それらがどのような根拠により拒否されたかの概要を表 2 に示す．ただし 1 通の拒否事例が複数の拒否根拠を持つことが多数あるため，各項目の合計が全体の拒否総数とは一致しない．

5.1 第一種の誤り

ブラックリストに登録してあるものは，利用者にとって受け取っても価値のないものとの実績を持つものであるので，ブラックリストにマッチした拒否事例は捨てられるべくして捨てられたものといえる (静的根拠)．いっぽう，IP アドレスや DNS 登録状況に基づく拒否は動的に決まるものであるため，その中には本来拒否すべきでないものが含まれる可能性がある．これについて動的根拠のみに基づく拒否事例を全数調査したところ 5 件あった．ただし，そのうち受け取るべきものであろうと推測できるものは **2 件**であった[8]．これらはホワイトリストに登録することで以後の受信が可能となる．

5.2 第二種の誤り

spam であるにもかかわらず通り抜けて受信してしまったものについて，全利用者の協力を得てその件数を調査したところ，47 件の報告が得られた．報告もれも考慮する必要があるが，これらが受け取ったものの総数に近いと仮定すると，試験期間内に拒否した 5137 通と合わせて，

$$\frac{5137}{5137+47} \cong 0.99$$

約 99%の spam が拒否できたことになる．たとえこの成功率が幾分落ちたとしても，すり抜けた先で高度なコンテンツフィルタを稼動させるための負荷を軽減できる有効性は失われない．

6 結論

SMTP 接続クライアントの，IP アドレス，その DNS 登録状況，ならびに SMTP セッションパラメータを検査することでほとんど (約 99%) の spam を撃退することが可能だと確認できた．この手法が spam 撃退に効果的である反面，現状では悪意のないサーバが，信頼できない不適切な設定になっていてこれを拒否してしまう可能性が残る．全ての (善意の) メイルサーバ管理者が正しい設定に修正し，なおかつ SMTP レベルでの拒否機能を導入することで spam 送信者側の効率を著しく落とすことが期待できる．

また，今回実装した antibadmail の成果より，Sendmail, Postfix, qmail など，MTA に依らず統一的な手法を用いた SMTP セッションでの spam 拒否が実現できることと，その有効性が確認できた．現状では MTA ごとに異なる spam 対策技法が追加実装され，その種ごとに違う設定法が要求されている．本稿での手法は SMTP セッションでの spam 拒否手法を任意にカスタマイズできるフレームワークとして全てのメイルサーバに有効な切り口といえる．

[8] 通常 spam は送信者アドレスがランダム文字列であったりするので中味を見ずともホワイトリストに登録すべきかどうかの判断は容易に下せることがほとんどである．

参考文献

[1] D. J. Bernstein; qmail; `http://cr.yp.to/qmail.html`

[2] Network Working Group, J. Klensin, Editor, AT&T Laboratories, April 2001; Simple Mail Transfer Protocol; Request for Comments(RFC) 2821

[3] MAPS; Stopping spam at its source; `http://mail-abuse.com/`

[4] SORBS; Fighting spam by finding and listing Exploitable Servers.; `http://www.dnsbl.au.sorbs.net/`

[5] D. J. Bernstein; A conform to UNIX Client-Server Program Interface, UCSPI-1996; `http://cr.yp.to/ucspi-tcp.html`

[6] Erwin Hoffmann, et al.; SPAMCONTROL; `http://www.fehcom.de/qmail/spamcontrol.html`

[7] HIROSE, Yuuji; qmail patches; `http://www.gentei.org/~yuuji/software/qmpatch/`

[8] 広瀬雄二, 大駒誠一; SPAM 門前払い・SMTP レベルでの受信拒否方策の検証; 平成 15 年度第 2 回 情報処理学会東北支部研究会 資料番号 14

[9] HIROSE, Yuuji; Anti bad-mail SMTP wrapper; `http://www.gentei.org/~yuuji/software/antibadmail/`