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

SPAM 門前払い・SMTP レベルでの受信拒否方策の検証

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

1　背景

インターネットのサービスの一つである電子メイルは欠かせない道具になっている。コンピュータに触れる人間であれば多くの人が利用している。それを悪用し、望んでいない人に対して広告文などを含む大量のメッセージを送りつける悪徳業者があとを絶たない。大量に送られる望まれないメッセージのことを UBE(Unsolicited Bulk Email) といい、一般的には SPAM と呼ばれている。SPAM を受信しても気分を害するだけなので、受信した全てのメイルの本文を機械的に走査して SPAM を選別・除外するプログラム「SPAM フィルタ」が数多く研究・開発されている。

SPAM フィルタは受信メイルの内容を検査するため、メイルサーバから見た場合いったんメイルを受け取ることになる。このため、SPAM でもそうでない場合でも受信者のいるメイルサーバの資源を利用することになる。

本稿では、SPAM 送信者の挙動を元に、メイル受信を行なう前の段階で受け取りを拒否する方策についていくつか提案し、その効果を検証する。

2　SMTP レベルでの受信拒否

SMTP[1]では、接続を受ける時、メイル本文をクライアントとなるホストから実際に受ける前に HELO, MAIL FROM, RCPT TO の 3 つの情報をクライアントから受け取る。

HELO[2]　クライアントのホストの識別名を送る (通常はホストの FQDN またはそれに準じる名前にする)

MAIL FROM　本来の差出人アドレスを指定する

RCPT TO　実際の受取人アドレスを指定する

正常なメイルであれば、これらの情報は全て正しいものがサーバに送られる。しかし SPAM 送信者は「**身元を隠したがる** 」 、「**アドレスを偽造したがる**」という性質があるため、HELO/MAIL FROM は嘘の情報を入れる場合がほとんどである。これら 2 つと DNS 登録情報に虚偽、あるいは異常設定を持つホストからのメイル受信を拒否することで SPAM 流入を未然に防げると予想できる。

3　SMTP レベルでの拒否の実装

前述の予測を元に、SMTP 接続時に以下のことを検査し、「クロ」と判定したものを完全に受信拒否するものを実装する。

1. ブラックリストに登録された IP アドレスからの接続か
2. HELO で指定された文字列が
   (a) 特定のブラックリスト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

[1] Simple Mail Transfer Protocol; 電子メイルを授受するときメイルサーバ同士がやりとりするときのプロトコル。

[2] 現在では拡張 SMTP 用の EHLO を送ることが多いが本稿では HELO/EHLO を代表する意味で HELO を利用する。

から発せられるものはSPAMである可能性が高い)

(c) IPアドレスの場合、でたらめなIPアドレスになっているか

(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 (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) 虚偽に使われやすい国別トップレベルドメインを名乗っているか (このルールは厳しいのでDNS逆引きレコードが未定義の場合のみ適用する)

3. MAIL FROMが特定のブラックリストパターンにマッチするか

4. MAIL FROMがドメイン部 (@記号以降) を含む正しい形式か

5. MAIL FROMのドメイン部が実在するドメイン名か

6. RCPT TOが特定のブラックリストパターンにマッチするか

実際に上記のルールを適用し、受信拒否を行なうメイルサーバを構築して実地試験を行なった。

3.1 SMTP anti-badmailの実装

qmail-1.03 [1] のSMTPデーモンプログラムである`qmail-smtpd.c`に3節の拒否ルールを処理できる実装を追加した。なお、各ルール実装のうち5は既存のmfcheckパッチ [2] を拡張し、「信頼できるクライアント」からの接続のときは全てのメイルを受理する機構を追加した。また、6は既存のbadrcpttoパッチ [3] を拡張し、ブラックリストにドメイン部のみを指定すると、それに一致するもの全てを除外できる「ワイルドカード指定」を可能にした。

「信頼できるクライアント」からの受信を許可する機構は、MAIL FROM以外の情報が不適切な場合にも有効である。たとえば、SMTP送信サーバのDNS登録レコードが不正であったり、HELO文字列の設定が不適当であったとしても、クライアントのIPアドレスやドメイン名が、用意した信頼リスト (ホワイトリスト) に一致する場合にはメイルを受信することができる。

4 ブラックリストの作成

4.1 SPAM送信の経験的動向分析

国内外を問わずSPAM送信者は存在する。しかし、そのSPAM送信手法は国内外で大きく異なっていることが観察された。

国外SPAM ダイヤルアップ・xDSLなどの動的割当ホストから手当たり次第に送る。DNS逆引き登録は未登録、またはプロバイダの動的割当ホスト名を指していることが多い。FROMアドレスは常に偽造する。全くランダムなFROMアドレスのこともあるが、ドメイン部を実在するものにしつつローカル部 (@記号より前) を乱数生成したものにすることが多い。HELO文字列は乱数で生成したものや実在するドメインを詐称するものがある。

国内SPAM 国外SPAMのような手段によるSPAMはかなり少ない。これは、携帯電話に附随するメイルの普及が日本で格段に進んでいるのが理由の一つと考えられ、SPAM送信者のターゲットはより購読層の多い携帯電話系メイルに移行しているためと考えられる。数少ない国内SPAMでは、正規に取得した無料プロバイダの正しいメイルアカウントを利用して、正々堂々と送って来るものが散見される。これは送信手順が一般プロバイダの正規のメイルサーバから送られるため、SMTPレベルでは悪意によるものかは見分けられない。

4.2 作成した拒否リスト

上記の傾向を踏まえ、SMTPサービスデーモンが参照するブラックリストを作成する。ブラックリストには以下の4種類が存在する。

badhelo 拒否したい HELO 文字列のリスト。yahoo.com など詐称されやすいもの、“pc1”, “server” などのインストール後放置された PC のもつ典型的なホスト名や、通常はありえないサーバ (受信) 側のホスト名・IP アドレス等を列挙する。部分文字列によるワイルドカード指定も可能。

badmailfrom 拒否したい FROM アドレスのリスト。@yahoo.com など詐称されやすいものや実際にしつこく送って来る FROM アドレスを列挙する。ワイルドカード指定も可能。

badrcptto 拒否したい RCPT(宛先) のリスト。存在しない宛先にしつこく送って来る SPAM などを拒否するために指定する。

smtp.cdb SMTP 接続クライアントの IP アドレスまたはドメイン名に応じて「信頼すべき」か「受信拒否すべき」かを定義したリスト[3]。「信頼すべき」サーバとして、例えば yahoo.com の本物のサーバを登録すると、そこからは @yahoo.com という FROM アドレスを持つメイルを受信許可できる。

4.3 SMTP サーバに実装した拒否ルール

SMTP サービスデーモン (`qmail-smtpd.c`) に以下の拒否ルールを埋め込み実装した。

FROM アドレスの検査 存在しないドメイン名、メイルアドレスとして成立しないもの (@記号の無いもの[4]) は拒否する。

HELO 文字列の検査 RFC 1123 では HELO に基づく受信拒否を禁止しているものの、明らかにでたらめと分かるパターンは SPAM だと判定できることは間違い無い。HELO でホスト名と見なせない、「ドットの無いランダムな文字列」、「ドットは含むが存在し得ないトップレベルドメイン」、「嘘の IP アドレス」などを HELO 文字列として送って来たクライアントからのメイルは受信拒否する。

[3] 実際には tcpserver のルールファイル

[4] エラーメイルに用いられる NULL アドレスなどは許可する

5 運用実験結果

筆者の運営する利用者数 34 名のサイトで 2003 年 11 月 19 日から 11 月 26 日の 7 日間に接続を受けた SMTP 全ての受信許可/拒否結果は表 1 のようになった。

表 1: 受信許可/拒否の実数

接続総数	受信許可	受信拒否
8031	4897(61.0%)	3134(39.0%)

このうち受信許可したものの中には、実際には SPAM であるものが素通りしているものもある。これについて利用者の協力を得て、受信してしまった SPAM の報告を受けたところ、期間中 63 通の受信が確認できた。得られた報告が通過 SPAM の全てではない可能性はあるが、約 98%の SPAM が拒否できたことになる。

受信拒否となったものの拒否根拠の内訳は表 2 のようになっている (複数根拠を含む)。

表 2: 受信拒否根拠

MAILFROM による拒否		1761
内訳	存在しないドメイン	110
	badmailfrom にマッチ	1640
	ドメイン部無し	11
RCPT TO による拒否		1009
HELO による拒否		375
内訳	badhelo にマッチ	224
	ドットなし	135
	あり得ないドメイン	16
IP アドレスに基づく拒否		316

MAILFROM による拒否が目立つのは「しつこく送り続けるドメイン」と大手無料メイルドメインのアドレスを詐称したものが大半を占めるからである (表 3 参照)。次いで RCPT TO による拒否が多いのは、当方のドメインを詐称し

表 3: 拒否した FROM アドレス上位 10

384	yume.otegami.com
220	hotmail.com
187	yahoo.com
62	msn.com
54	aol.com
51	sina.com
46	juno.com
33	earthlink.com
32	yahoo.com.hk
30	tom.com

てどこかから発せられた SPAM(もしくはワームの繁殖メイルなど) がエラーとなって大量に戻って来たことによる。エラーメイルが戻り始めるときに badrcptto リストに追加していることが効を奏している結果でもある。

6 考察

SMTP anti-badmail での運用実績から以下のことが観察できた。

しつこく送信してくるもの、大手のメイルドメインを詐称するものは効果的に撃退できた。

単発でなおかつ正しく逆引き登録されたプロバイダの IP アドレスから送って来るものは通過してしまうことが多い。

「受け取るべきメイル」を拒否した例を調べると、HELO 文字列に不適切なものを付けている例が多い。発見した場合は、「信頼できるホスト」リストに追加するか、そのドメインの管理者に通知して直してもらうしかない。

また、拒否リスト作成時の方針として以下のことが言える。

「知らない人からのメイルで親交が深まるかもしれない」という期待を抱いている限り抜本的な SPAM 対策は進められない。SPAM の FROM アドレスはそのほとんどが詐称したアドレスで、詐称されたドメインは無実であることが多い。しかし、実質的に縁遠い国に存在するドメインなら、その FROM アドレスは拒否リストに追加してしまっても実害は無いし、海外のダイヤルアップ端末から SPAM が来た場合、それが縁遠い国のものなら、該当するアドレス範囲をまるごと受信拒否リストに追加して実害はない。利用者の交信範囲を知り、地域依存型のブラックリストを作ることが効果的といえる。

7 結論

SMTP 接続クライアントの DNS 登録状況、HELO/MAIL FROM/RCPT TO を調査することで数多くの SPAM を拒否できることが分かった。しかし、多くの SPAM 送信者が恣意的に行なっている DNS 逆引き詐称登録・HELO ホスト名登録不備が、善意のサーバにも散見される。詐称する必要の無い善意のサーバの管理者が全て清く正しい設定にすることで SMTP レベルでの SPAM 拒否が格段に効果を増すといえる。全ての (善意の) メイルサーバ管理者が設定を見直し、SMTP レベルでの拒否実装を盛り込むことで SPAM 送信者の悪意ある送信行動を抑制できる。

参考文献

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

[2] Nagy Balazs;
mfcheck-3;
http://www.qmail.org/qmail-1.03-mfcheck.3.patch

[3] Ward Vandewege;
badrcptto;
http://patch.be/qmail/badrcptto.html

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