2 ブロッキング，スロットリング

中京大学情報科学部情報科学科
鈴木 常彦　tss@sccs.chukyo-u.ac.jp

本稿では技術的な面から spam メールへの対策を解説する．spam 対策にあたって重要なことは「断固とした姿勢で臨む」ことである．spam はインターネットにおける癌であり，放置すればその負荷と信用破壊☆1 により，やがてインターネットを崩壊させるだろう 1)．

spam が迷惑メールという名で過小評価され，対策が後手に回っている背景には，メール利用者のメールボックスに届く spam が氷山の一角（図 -1）であり，真のリスクと被害が感じられにくい点が挙げられる．しかし spam は存在しない宛先への大量のトラフィックを生んでおり，サーバや回線にとっての脅威となってきていることを理解する必要がある．

■ ブロッキング（Blocking）

spam を受信してしまうことは，回線やサーバの資源を消費するのみならず，「2.4 バウンスメール対策」（pp.762-766）で問題とする第三者へのバウンス問題を引き起こす．

昔のシンプルなネットワークにおいては，受取人のメールアドレスが存在しない場合，メールを受信せずセッションを終了させることが可能であった．しかし，昨今のネットワークにおいては，ウイルス対策サーバの中継や，ファイアウォールの外（DMZ）☆2 から中への転送などのセキュリティ対策が，逆に受取人の存在確認を困難にしてきているのは皮肉なことである．

このような状況において，インターネットの資源全体を spam から守るために，最前段のメールサーバ（MTA）において spam を受信しないための対策が必要とされる．spam を受信しなければバウンス問題も発生しない．メール転送プロトコルである SMTP セッションの開始時あるいはセッション中に spam を判定し，spam の受信を拒否する手法を本特集では「2.3 フィルタリング」（pp.758-761）のフィルタリングと区別してブロッキングと総称し，以下に解説を行う☆3．

【ORBL（Open Relay Black List）】

ブロッキングの手法として古くから利用されてきたのが，ORBL（Open Relay Black List）あるいは DNSBL（DNS Black List）である．多様なポリシーの DNSBL サイトが有志あるいは商用で運用（表 -1 参照）されており，第三者不正中継（Open Relay）が可能であるサーバ，あるいは spam 送信の前科があるサーバなどのリストが

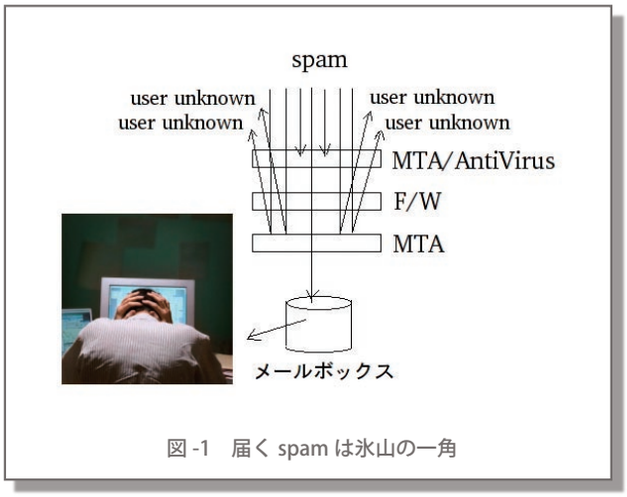

図 -1　届く spam は氷山の一角

☆1 phishing 詐欺などにより電子メールというシステム全体の信用が崩壊寸前である．
☆2 非武装地帯 (DeMilitarized Zone) のことで，組織内ネットワークと組織外ネットワークとの中間に設けられるセグメントを指す．
☆3 フィルタリングやブロッキングは同義ととることもできる．これらの用語について正確な区別や定義が定着しているわけではない．

http://www.spamcop.net/bl.shtml
http://blacklist.jippg.org/
http://ordb.org/
http://dsbl.org/
http://www.mail-abuse.com/

表 -1　ORBL サイトの一例

```
> dig 38.217.129.24.list.dsbl.org a

;; QUESTION SECTION:
;38.217.129.24.list.dsbl.org.  IN     A

;; ANSWER SECTION:
38.217.129.24.list.dsbl.org.2048 IN    A      127.0.0.2
```

リスト 1　ORBL サイト dsbl.org への DNS 問合せ例

DNS サーバ（DNSBL）に登録されている．

MTA では，SMTP セッションを張ってきた相手の IP アドレスをこれらの DNSBL に問い合わせ，問題のあるサイトを示すレコードが存在していればセッションを中断させる．リスト 1 の例は，IP アドレス 24.129.217.38 が，38.217.129.24.list.dsbl.org として DNSBL に登録されていることを示すものである．

ORBL には，不正なサーバの IP アドレスに隣接する健全なサーバもブロックごと登録されてしまう問題が指摘されるが，アドレスブロックの管理者とユーザに対し連帯責任を問う点を逆に評価することもできる．どのような接続拒否を行うかは ORBL の責任ではなく，ORBL を利用する MTA 管理者のポリシーの問題である．

なお，D. J. Bernstein の djbdns に含まれる rbldns[2] により自前の DNSBL を運用することができる．

【お馴染みさん方式】

昔の spam は第三者不正中継サーバを用いたものが多く ORBL が有効であったが，最近はウイルスに感染し spam 送信の踏み台となった PC（ゾンビと呼ばれる）からの spam が大多数を占めるため，不正中継サーバのリストだけでは有効性は低く，ゾンビのいる ADSL 等の動的割り当てアドレスブロックをリストアップした DNSBL が有効となってきている．

こうした状況においては，ゾンビからの SMTP セッションの特徴をとらえてブロックする手法が有効である．ゾンビは spam の大量配信のみを目的としたプログラムをウイルス等により植えつけられており，その振る舞いは通常の MTA の振る舞いとは異なることが観測されている．メール配送の手順を定めた RFC821，RFC2821 によれば，すぐに送信できなかったメールは一定時間後に再送信しなければならない（MUST☆4）が，ゾンビはこれに従わない．前野は「ゾンビは spam を再送しない」という仮説に基づき，1 回目の SMTP セッションに一時拒否エラーを返し（tempfailing），再送を行ってきたものだけを受信する，いわゆる「お馴染みさん方式」（あるいは「一見さんお断り」方式）を提唱した[3]．すべての相手に再送を強いるのは効率が悪いため，信用できる相手をホワイトリストに登録する点が，従来のブラックリスト方式とは逆の発想となっている．

東海インターネット協議会（TIC）でもこの方式をもとにした spam 対策を 2003 年 11 月より適用し，spam セッションの大半を受信拒否することに成功している[4]．

本方式はわずかなコストで spam を拒否できるというメリットがある一方で，再送信しない MTA からのメールの不着や，再送信による遅延が欠点として指摘されている．しかし再送信しない MTA というのは，もとより自ら信頼性を放棄しているのであって，そうした MTA がオンライン予約システムなどに用いられていること自体が問題視されるべきであろう．また，「一見さん」のメールが遅延することが問題になるケースは少なく，トレードオフは十分成立すると考えられる．

【Greylisting】

お馴染みさん方式と同様に Tempfailing を行う手法に Greylisting（http://www.greylisting.org/）と呼ばれるものがある．Greylisting では再送を受信する際の基準として，セッション中に得られる差出人（mail from:），受取人（rcpt to:），接続相手の IP アドレスの 3 情報（Triplet）を検査する．Triplet はデータベースに格納され，セッション中にポリシーにしたがって過去のデータと照合され受信可否の判断がなされる．

【PTR の検査】

送信元 IP アドレスの PTR 値の検査を行い，お馴染みさん方式等のブロッキングを適用する相手を絞り込む手法も広く使われている．

通常，MTA の IP アドレスは身許を明らかにするために，その IP アドレスに付与されたドメイン名が PTR レ

☆4　本稿を通して，MUST，SHOULD 等の大文字で書かれた助動詞は RFC におけるキーワードであることを示す．

```
166.34.0.192.in-addr.arpa.   6H IN PTR   www.example.com.
www.example.com.             2D IN A     192.0.34.166
```

PTR 値に対応する A レコードがもとの IP アドレスを含んでいる

リスト 2　パラノイド検査

```
adsl-3-163-41.mia.bellsouth.net
catv-50623ae1.catv.broadband.hu
0x535d6a06.hrnxx14.adsl-dhcp.tele.dk
ppp83-237-228-174.pppoe.mtu-net.ru
pl710.nas926.o-tokyo.nttpc.ne.jp
```

リスト 3　spam を送信してきたゾンビの PTR 値

コードの値として DNS で検索できるように設定される．さらに，詐称が容易な PTR の値（DNS の逆引き）に対し，そのドメイン名の A レコードの値（DNS の正引き）にもとの IP アドレスを含むように正しく DNS の設定が行われるべきである．パラノイド検査と呼ばれる DNS 問合せはこの PTR と A レコードの整合性を検査するものである．

これにより，DNS というシステムの信頼性の範囲において，MTA の身許の認証が提供される（リスト 2）．ただし，実際の適用にあたっては，後述するように第三者の DNS への影響の問題があり，パラノイド検査は避けて PTR のみを検査するのが穏当だろう．

多くの spam は管理レベルの低いネットワークから発信されており，こうしたネットワークの IP アドレスには PTR 値がついていないか，ついていても A レコードの値と一致しない場合が多い．さらに PTR 値が適切に設定されている場合でも，そのラベルから MTA に固定的に割り当てられた IP アドレスではないことが容易に推測されるものが多い（リスト 3）．

PTR 値の検査は目安に過ぎないが，一時拒否の対象を絞りこむのには有効である．一方で厳格にブロッキングに用いるには，世の中の DNS の設定はあまりにも不適切なものが多い．最新の送信者認証技術を持ち出す以前に，世の中の DNS 管理者たちにはもっと適切な DNS の運用を心がけていただきたいものである．

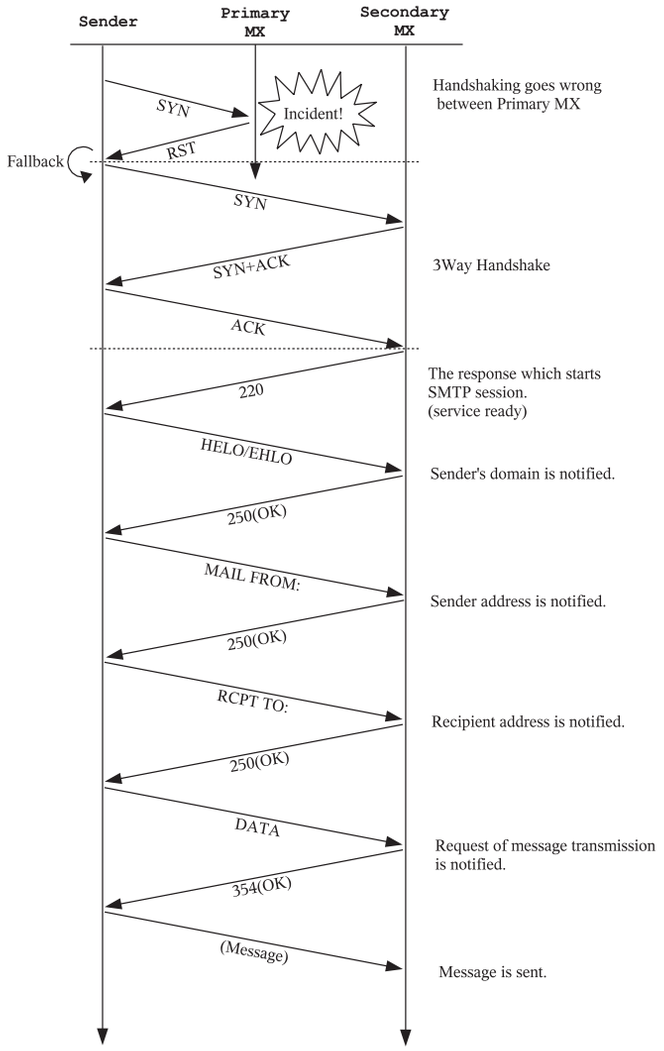

図 -2　5-Way-Handshake

【5-Way-Handshake】

山口，鈴木らはお馴染みさん方式の一時拒否による遅延を解消する手法[5]を提案している．MTA をプライマリとセカンダリの 2 台用意し，プライマリ MTA への SMTP セッションの TCP 3-Way-Handshake において最後の段階で ACK の代わりに RST を応答し，セカンダリ MTA へのフォールバックを誘発させる（図 -2）．

セカンダリ MTA への再送は RFC2821 で MUST となっており，通常の MTA はこれに従うがゾンビはこれに従わない．ただし，DNS の MX レコード（受信 MTA の指定）を無視してセカンダリ MTA を直撃する spam も多い．このため，山口，鈴木らの手法ではプライマリでのハンドシェイクの失敗とセカンダリへのハンドシェイクを連続した 5-Way-handshake としてとらえることによ

り，spam 判定を行う．

なお，一部のウイルス対策サーバやファイアウォールがセカンダリへのフォールバックを行わないことが判明している．こうした製品を最前段の MTA として利用するのは，自ら信頼性を落とすことになることを知っていただきたい．

■ スロットリング（Throttling）

spam の特徴は高速大量配信である．このため，いちいち再送を行わないという特徴のほかに，timeout が短いという特徴が見られる．つまり，SMTP セッションの応答をゆっくり返すと，待ち切れずにセッションを放棄するのである．この特徴を利用した spam 対策が throttling あるいは tarpitting と呼ばれる手法である．

RFC2821 に従えば，送信側は TCP ハンドシェイクの後，SMTP セッションにおいて最初に受信側が返す 220 greeting message を最低 10 分待つべきである（SHOULD）．しかし，spam の送信ホストはこれをわずかな時間しか待つことができない．SMTP のそれぞれの応答を返す前に 10 ～ 15 秒程度の sleep を挟むことにより，70% から 80% の spam はセッションを放棄することが確認されている [4), 6)]．

■ ブロッキング手法への批判

Tempfailing や throttling に spammer が対応してきたらどうするのだ，という批判がある．確かに対応可能である．再送すればよいし，Timeout は延ばせばよい．PTR も適切に設定されたホストを用いればよい．しかしそれにはコストがかかるのである．もとより spammer は確実な配送は求めていない．彼らは安く大量に spam をばら撒きたいのである．彼らにコストを強いるとすれば十分意義がある対策なのである．

また，インターネットというものは Best Current Practice で動いている．すでにインターネットは危機的状況にあり，将来，送信者認証（「2.5 送信者認証・課金」（pp.767-772）で解説）がうまく機能するまで手をこまねいているわけにはいかない．いや送信者認証をうまく機能させるためにも，ブロッキング技術を先行して導入していかなければならないのである．

■ ブロッキングの問題点

spam 対策はそれ自体が第三者への公害となる可能性があることもよく理解しておかなくてはならない．最近，セッション中の MAIL FROM: や ヘッダ From: のドメインパートを DNS で検索し，存在しないドメインだった場合に spam と見なす対策がよく見られるようになってきている．しかし，差出人が詐称されているメールが大量に発信され，受信サイトの多くがこの対策をとっていたらどうなるだろうか？　詐称されたドメインに大量の DNS 問合せが殺到することになる．送信元の IP アドレスのパラノイド検査も同様であり，この観点からすれば，送信元の IP アドレスの PTR のみを検査するのが妥当であろう．

今日の技術者は知った技術を闇雲に適用するのではなく，自らの行為の意義や影響をよく自分の頭で考え，Best Current Practice を選択することができなくてはならない．

参考文献
1）http://www.cavebear.com/cbblog-archives/000051.html
（邦訳 http://www.suzuki.sccs.chukyo-u.ac.jp/dyingnet.html）
2）http://djbdns.qmail.jp/djbdns/rbldns.html
3）前野年紀：MTA でできる spam 撃退術，情報処理学会 第 45 回プログラミング・シンポジウム報告集，pp.135-145(2004).
4）鈴木常彦，後藤邦夫，山口榮作，石川雅彦：MTA による spam 対策の実践報告，情報処理学会 研究報告，2004-DSM-034, pp.61-64(2004).
5）山口榮作，鈴木常彦：Handshake を利用した spam 対策システム，国公立大学センタ情報システム研究会 大学情報システム環境研究，Vol.8, pp.60-68(2005).
6）前野年紀，鈴木常彦：spam 送信ホストの見分けかた，情報処理学会 第 9 回分散システム／インターネット運用技術シンポジウム報告集，pp.25-29(2004).

（平成 17 年 6 月 13 日受付）