白梅学園大学・短期大学情報教育研究
2008, No. 11, 1－6.

メールサーバ上での迷惑メール対策

倉澤　寿之

はじめに

電子メールが普及するにつれ、迷惑メールの量も増えているといわれている。アメリカのシマンテック社のレポート[1]では、2007年の９月から10月の段階で、メール流量のおよそ70%が“spam”（英語で迷惑メールを意味する）であると推計している。本学のメールサーバにおいて、後述する迷惑メール対策により拒絶された外部からのメールアクセスは、2007年12月から2008年２月の間で、週当たりおよそ21,600件であり、拒絶されずに着信したメールアクセスは約7,300件である。拒絶したメールのすべてが迷惑メールであるとはいえないし、着信したメールのある程度は迷惑メールが含まれているから、正確な数字とはいえないが、75%あるいはそれ以上の割合で迷惑メールが届いていると推定できる。

そうした状況をふまえて、インターネットの各サイトのメールサーバ管理者にとって、迷惑メール対策は重要な業務のひとつになってきている。一方、メールサーバ上で迷惑メールへの対処を行うと、その副作用も生じてくる。本来拒絶すべきでないメールを誤って拒絶してしまう、といったことである。本稿では、本学の迷惑メールへの対処の方法について紹介するとともに、その際に生じるリスクに対する対処の方法についても述べる。

クライアント上及びサーバ上での迷惑メール対策

迷惑メールへの対策は、各ユーザのクライアントパソコン上でメールソフト（MUA: Mail User Agent）の機能を使って行われるものと、メールサーバ上でメール転送システム（MTA: Mail Transfer Agent）の機能やその周辺で動くソフトウエアの機能を使って行われるものに大別される。

クライアント上での対策は、メールサーバに届いたメールをクライアントパソコンにダウンロードする際、何らかの方法で迷惑メールかどうかを判定し、迷惑メールと判定されたメールは予め決められた方法で処理される、といったものである。迷惑メールかどうかの判定には、単に送信元メールアドレスやメールのタイトルや本文に含まれるキーワードを検索する、といったものから、迷惑メールの特徴を学習していくものなどもある。判定後の処理としては、メールに迷惑メールであるという目印をつける、特定のフォルダなどに隔離する、あるいは削除してしまう、といったことが挙げられる。

こうしたクライアント上での対策は、迷惑メールを受信した後のものであり、ユーザの目に触れにくくなるという精神衛生上の効果はあるとしても、その処理に計算機の資源が消費されてしまう。メールサーバの管理者としては、できるだけメールサーバが迷惑メールを処理しなくて済むようにしたいところである。

メールサーバ上での対策としては、外部からのメール着信があった段階で、メール転送システムが自身の持つデータベースや外部にあるデータベースと照合して、メール発信元のホストを受け入れるか拒絶するか判断する、というものが代表的である。こうした機能は、通常、メール転送システム自身（たとえばsendmailやpostfix）が持っている。また、メールを受け取ると同時にその内容を別プログラムによりチェックして、迷惑メールと判定されたものは受け取りを中止する、という形のものもある。これらの対策ではメール着信時に拒否することになるので、メールサーバが迷

惑メールを処理することによる時間やディスク容量などの資源の浪費を最小限に抑えることができるという利点を持つ。しかし、その反面、拒否すべきでないメールを拒否してしまい、結果的に必要なメールが届かないという副作用が起こるリスクも抱えることにもなる。

さらに、メールサーバ上では、メールを受け取った後、ユーザのメールボックスに配送する段階で迷惑メールかどうかの判定を行うこともある。この用途で最もよく使われているのが“SpamAssassin[2]”である。“SpamAssassin”はフィルタプログラムの一種であり、入力されたメールが迷惑メールかどうかの判定を行い、判定結果をメールヘッダに書き加えて出力する。この判定結果はユーザが目で見て対処することもできるし、他のプログラム（たとえば“procmail”）で削除や隔離などの処理をするために、その判定結果を利用することもできる。

本学メールサーバ上で実施している迷惑メール対策

本学の教職員用メールサーバ（mail.shiraume.ac.jp）で行っている迷惑メール対策は以下の通りである。なお、本稿執筆時現在、本学のメールサーバは、メール配送システムとして“Postfix-2.2.10”を、迷惑メール判定フィルタとして“spamassassin-3.1.9”を使用している。

（1）メール着信時にアクセス元ホストの情報から受け取りを拒否ないし保留する

①Real Time Block Listによる受け取り拒否

Real Time Block Listとは、迷惑メールを発信したサイトの情報のデータベースである。インターネット上にこうしたデータベースがいくつか作られており、メール配送システムはアクセス元ホストがこうしたデータベースに登録されていた場合、メール配送のための接続を拒否するように設定することができる。本学のメールサーバでは、“Realtime Blackhole List Japan（rbl.jp）[3]”の提供するデータベースを参照している。

②独自のデータベースによる受け取り拒否

これまで本学に迷惑メールを送信してきた記録をもとに、独自に作成したデータベースがあり、それに基づいてアクセス元ホストからの接続を拒否している。このデータベースは、テキストファイルにして約3万行あり、ドメイン名とIPアドレス範囲がその内容である。なお、現在このデータベースには、集中的な迷惑メールと見なされるメールアクセスが発生した場合などを除いて、新たなデータの登録は行っていない。その理由は受け取り拒否と受け取り保留の違いについての項で述べる。

③S25R（Selective SMTP Rejection）による受け取り保留

浅見（2004）[4]の提唱する“S25R”と呼ばれる方式を利用している。“S25R”は、迷惑メールのほとんどがエンドユーザ向け接続回線から送られてくるという経験則を利用し、アクセス元ホストのドメイン名の特徴に基づいてアクセスを許すかどうか決定する。具体的には、ドメイン名の個別ホストを識別する部分に、一定の様式で数字が使われていたり、“adsl”や“dsl”といった文字列が含まれていたりする場合など、エンドユーザ回線からの接続であると判断して、そのアクセス元ホストからの接続要求に対して一時的な拒否を返答し、受け取りを保留するものである（拒否と保留の違いについては後述）。この方法は、本質的な対処方法とはいえないが、実際上の効果は大いにある。しかし、エンドユーザ回線からであっても自宅にメールサーバを設置している場合もあるし、エンドユーザ回線と似たドメイン名を持っていてもレンタルサーバである場合などがあるため、必要以上に制限してしまうことも少なくない。そのため、後に述べるように、この方式による接続制限の結果を定期的にチェックする必要がある。

④独自のデータベースによる受け取り保留

本学宛に迷惑メールを送ってきたサイトのIPアドレス範囲のデータベースを作成し、メールの受け取り保留を行っている。②で述べた受け取り

拒否のデータベースとは異なり、このデータベースは現在頻繁に情報が追加されている。

(2)ユーザのメールボックスへの配送時に隔離する

上記（1）のプロセスを経て着信したメールは、ユーザごとのメールボックスへ配送されるわけであるが、この時に“SpamAssassin”による判定を行い、迷惑メールと判定されたメールを通常のメールボックスとは別の場所に隔離することができる。（1）と異なり、この機能はすべてのユーザで自動的に行われるわけではなく、この機能の利用を望んだユーザだけについて処理が行われる。具体的には、倉澤（2003）[5]で作成したメール転送システムのインターフェイスの一部を使ってこの機能の利用の有無を選択できるようになっている（図1）。ここで利用を選択すると、そのユーザの.procmailrcファイルに、“SpamAssassin”による判定を行うための記述と、迷惑メールと判定されたメールを SPAM フォルダに移動するための記述が追加され、迷惑メールは通常のメールボックスには配送されなくなる。

SPAMフォルダに隔離されたメールは、通常のPOP3プロトコルによるアクセスでは読み出せない。つまり、誤って迷惑メールと判定されたメールがあった場合、POP3を使うユーザは読み出せなくなってしまうわけである。そのため、この機能を利用するユーザには、IMAP4プロトコルを利用できるメールソフトないしウェブメールの併用を呼びかけている。

拒否と保留

外部ホストから本学メールサーバに対して行われたメール配送のアクセスを拒絶する場合、二つの方法を使い分けている。一つはSMTP (Simple Mail Transfer Protocol) のエラーコード554を返すことで、もう一つは同じく450のエラーコードを返すことである。５で始まるエラーコードは、SMTPでは永続的なエラーを意味するため、554を受け取った外部ホストは配送できる見通しがないと判断して、同じメールの再送を試みることなく、発信者にエラー通知する。一方、４で始まるエラーコードは一時的なエラーを意味するので、450を受け取った外部ホストは一定時間ごとに再送を試みるのが一般的である。本稿ではこれらを拒否と保留として表現している。

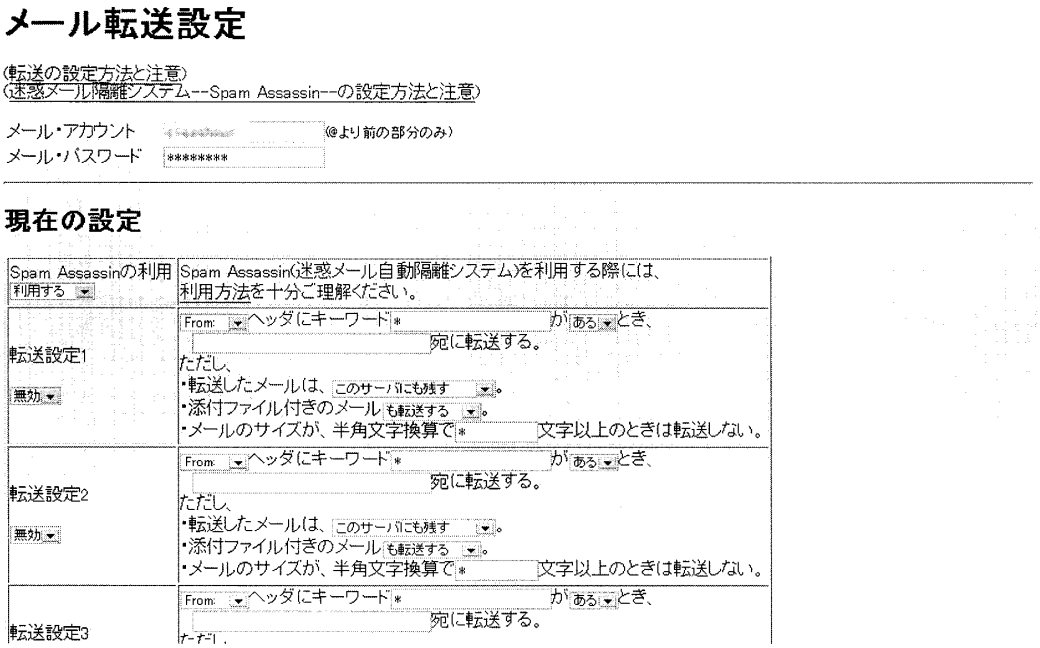

図1

一時的なエラーの通知を受けたとき、迷惑メール配送元ホストと「まっとうな」メール配送元ホストでは、経験則ではあるが、挙動が異なっている。「まっとうな」ホストは、通常10分から１時間程度の間隔で、数時間から数日の間、再送を試みる。これに対して、迷惑メールホストは、１回限りでまったく再送を試みないか、あるいは数秒からせいぜい数十分の間隔で２回ないし３回程度だけ再送を試みる、というのが大部分である。したがって、一時的なエラーを通知した際の再送状況をチェックしていれば、本来受け取るべきメールを誤って保留にしてしまっているケースを発見しやすくなるのである。そのため、現在は受け取りを拒絶するためのデータベースに迷惑メール送信サイトの情報を新たに追加する際、拒否のためのデータベースではなく、保留のためのデータベースを使っている。

誤った拒否・保留への対処

メールの受け取りを拒否する迷惑メール対策を行っている場合、本来拒否すべきでないメールを拒否してしまうリスクが常にある。この点に関して本学では、管理者によるメール送受信記録（ログ）のチェックと、ユーザからの通報の２つの方法で対処している。

(1)ログのチェック

メールの送受信記録のうち、保留された記録を管理者が一日に１回ないし２回ずつチェックして、本来受け取るべきメールが拒絶されていないかどうかモニターしている。ただし、一日あたり数千件に上る記録にすべて目を通すことはできないので、同じ外部ホストから同じユーザ宛に複数回のアクセスがあった場合だけをログから抜き出している。前述したように、一時的なエラー応答に対して迷惑メール送信元ホストは再送動作をわずかの回数・期間しか行わないが、「まっとうな」ホストは比較的粘り強く再送しようとするため、数回以上の再送が行われた記録だけに着目すれば、実際上十分なのである。

なお、ログのチェックは一時的なエラー応答を返した場合、つまり保留した場合の記録だけに限っており、永続的なエラー応答を返した場合、つまり拒否した場合の記録は通常チェックを行っていない。永続的なエラー応答を返した場合、「まっとうな」ホストであっても再送動作を行わないため、１回のみのアクセス記録となって、それらすべてに目を通すのが困難だからである。また、永続的なエラー応答を返す対象のデータベースは比較的古くから運用しているものであるため、それらを拒否することに問題がないと経験上判断していることもある。

(2)ユーザからの通報

誤った拒否・保留への対処方法の２つ目は、ユーザから「自分のところに届くはずのメールが届かない」という通報を受け付けることである。ただ、ユーザの立場で考えると、届くはずのメールが届かないという事態が生じたとしても、それが迷惑メールと誤認されて拒絶されているのか、他の原因（たとえばメールアドレスの間違いなど）で届かないのかは区別がつかないため、直ちに管理者に問い合わせたり苦情を言ったりという行動は取りにくいであろう。さらに、自分宛にメールが発信されていることを知らなければ、「届くはず」という認識を持つこともできないので、そもそもこの問題に気づかない可能性もある。

そこで、自身のアドレスに着信しようとしてメールサーバに拒絶された記録をユーザが調べることができるような仕組みが必要となる。以下、自分宛で拒絶されたメールをユーザ自身が一覧する仕組みとして開発された「メールブロックチェック」について紹介する。

「メールブロックチェック」の特徴

「メールブロックチェック」は、本学メールサーバとなっているコンピュータのウェブサーバ（Apache）上で動くCGIスクリプトであり、以

下の機能を持っている。

①ユーザ認証

メールサーバに登録されたアカウントとパスワードを使って、ユーザ認証を行う。他のユーザ宛に届けられようとしたメール記録を見せてしまうのはプライバシー確保の上で問題があると考えられるので、認証されたユーザ宛のメールのみを対象とする（図２）。

②拒否・保留記録の切り出しと表示

メールアクセス記録から、当該ユーザのアカウントに配送されようとして拒絶されたメールの記録を抜き出し、表示する（図３）。このとき表示されるのは、ブロックの種類（「拒否」「保留」「不明」のどれか)、日時、メールの送信者アドレス、アクセス元ホストの（逆引き）ドメイン名とIPアドレス、SMTPセッション開始時にアクセス元ホストが名乗った名前などである。ユーザに対しては表示されないが、内部的にはこのほかに当該メールを処理した際のプロセス ID などの情報も保持しており、管理者が当該の記録を見つけやすくするために利用されている。

③ブロック解除要請の送信

届くべきメールが拒絶されていることを発見した場合、ユーザがワンタッチで管理者に通報できるようになっている。図３の中の「解除要請」ボタンがそれである。この通報を行うと、管理者宛に当該の拒絶に関する情報がメールとなって届くので、管理者がそれをもとに解除作業を行い、結

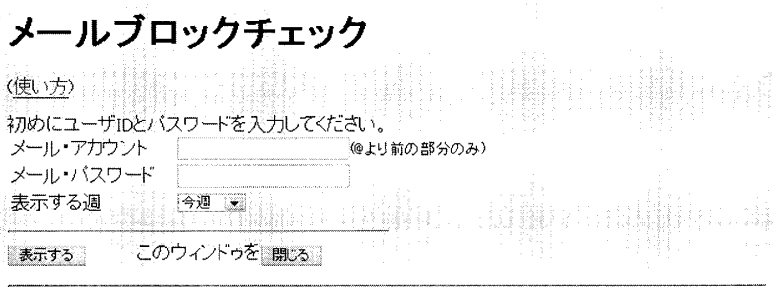

図２

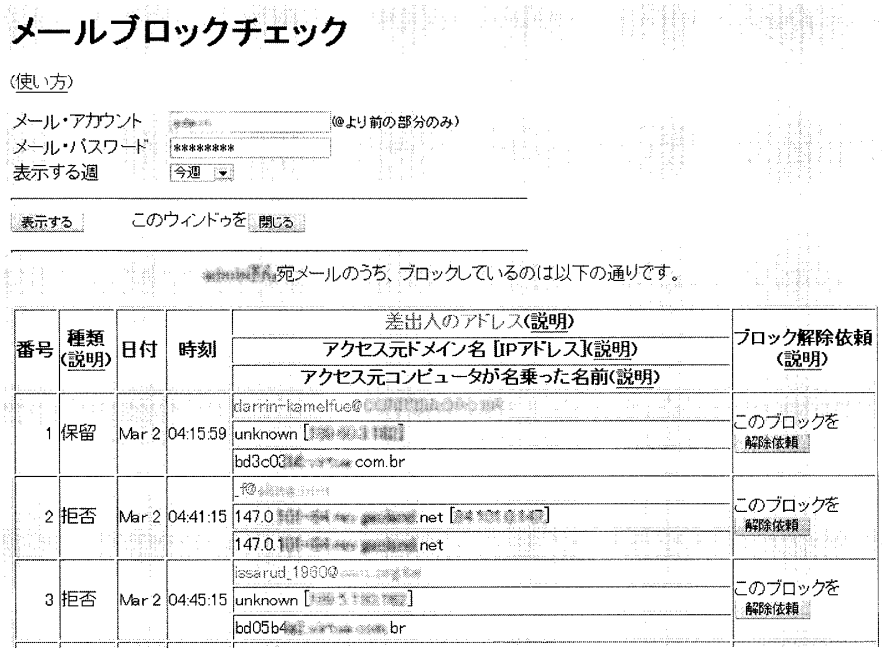

図３

果をユーザに通知することになる。

最後に

以上、本学メールサーバ上で行っている迷惑メール対策、及びそこから派生するリスクとその対処について述べた。電子メールはインターネットコミュニケーションの中核をなす重要なメディアであり、迷惑メールなどによってその機能が阻害されないように、今後とも注意していく必要がある。

文献

1 The October State of Spam report http://www.symantec.com/enterprise/security_response/weblog/2007/10/the_october_state_of_spam_repo.html

2 http://spamassassin.apache.org/

3 http://www.rbl.jp/

4 浅見秀雄　2004　阻止率99%のスパム対策方式の研究報告— Selective SMTP Rejection（S25R）方式 — http://www.gabacho-net.jp/anti-spam/anti-spam-system.html

5 倉澤寿之　2003　コンピュータネットワーク利用環境の整備（1）—ウェブインターフェイスによるメール転送設定—　白梅学園短期大学情報教育研究　第6号　3～8頁

（くらさわ　としゆき　短期大学心理学科）