プライバシーと視認性を考慮した迷惑メール対策と効果

岡田　正　　寺元貴幸　　日下孝二　　最上　勲
（津山工業高等専門学校　総合情報センター）
E-mail: {okada, teramoto, kusaka, mogami}@tsuyama-ct.ac.jp

概要　津山高専では、電子メールの本文に立ち入ることなく、どこからのメールを拒否しているか容易に確認可能な、迷惑メール拒否システムを運用している。特別なプログラムを必要とせず、ログファイルの監視だけで運用できるシステムについて、その基本方針・設定内容から効果までを紹介する。

１．はじめに

電子メールはそのプロトコル名 SMTP[1]通りの simple さの故に広く実装され、情報交換手段として不可欠の仕組みになっている。しかし、その simple さは、悪用するのも容易であることを意味し、望まないメールを送りつけられたり、コンピュータウイルスを添付されたり、送信元を詐称されたりと、数々の問題を引き起こしている。インターネット創生期の相互に信頼できる良き時代は終わり、何らかの防御が必要な時代になっているのは悲しいことである。

津山高専では、学内ネットワーク構築当初から、極力規制をしない方針で運用してきた[2]。しかし、2004 年３月頃の Bagle/ Netsky ウイルスが猛威をふるったのを期に、電子メールの受信制限に踏み切った。制限を行うとき、電子メールは私信であり本文に立ち入ったチェックを行うべきではないと考えた。また、どんな制限を行っているかを完全に把握でき、実際にどのメールを拒否したか容易に確認できることも重要である。

本報告では、プライバシーに配慮して本文をチェックすることなく、付加的なプログラムの導入が不要で、設定と保守が簡単に行えて、制限結果を容易に監視できる迷惑メール対策を報告する。制限に対する基本の考え方から、Postfix[3]による具体的な設定内容、そしてその効果を数年間の迷惑メールのデータを示しながら述べたい。

２．受信制限の基本方針

大量の迷惑メールを送りつけられて、何とかならないのかとの要望がシステム管理者に寄せられる。しかし、電子メールは個人宛の私信であり、管理者といえどもみだりに内容を確認すべきではない。一般の迷惑メール制限対策は、フィルタリングプログラムを導入したり、ブラックリストデータベース[4]の情報を使うといったものである。これらは、制限内容の主要部を第三者の手にゆだねており、何を拒否しているのかを完全に把握するのが困難である。

津山高専では、2003 年夏の Blaster ウイルスに続き、2004 年春の Bagle/ Netsky ウイルスの猛威を受け、何らかの受信制限を行わなければならいと考えた。ただ、電子メールという重要なサービスに制限をかけるのであるから、どのような方針で何を制限しているのか、管理者が完全に把握していて、明確に説明できることが必要である。そこで、受信制限の導入に当たって、次のような基本方針をたてた。

(1)プライバシー保護

本文の内容を使ったチェックを行わない。逆に言えば、標準ログに残る情報のみで制限をかける。ただし、管理者に届いたメールについては本文も使い、迷惑メールかどうかの判断に利用する。

(2)設定内容と制限結果の完全な把握

どのような制限を設定しているか、その結果どのメールを拒否したかを完全に把握する。すなわち、管理下にある SMTP サーバ上のみで設定からログ管理までを、我々自身の手で行えるようにしたい。

(3)管理・保守の容易さ

システム管理者であれば容易に設定でき、通常のログファイルを見るだけで状況を把握できるものとする。

(4)管理経費不要

特別なプログラムを導入したり、パターンファイルの更新のために契約したりといった、特別な費用をかけたくない。また、高機能なサーバを新たに導入しないと配送遅延が生じることも避けたい。

(5)完全性を求めないこと

一つの迷惑メールも許さない完璧なシステムを求めると、実現が困難になったり正当なメールを拒否することになりかねない。完全性を求めるのではなく、極力排除できるが、多少の漏れは許容する。

(6)その他

津山高専はマルチホーム接続を行っているので、２系統で同一の制限をかけることができるようにすることも必要となる。

３．Postfix による受信制限の設定

２．で述べた基本方針は一見して実現が難しいようであるが、迷惑メール送信元を調査すると、我々が従来から使ってきたメール配送プログラム Postfix[3]を使うことで十分に実現できると予想できた。すなわち、Postfix の設定ファイル（わかりやすい様式のテキストファイル）を編集するだけで、多数の細かな各種制限を簡単に設定でき、軽い負荷で処理可能となる。ここで電子メールの受信過程を簡単に述べて、どのような制限が可能かを示す（今回利用した機能を中心としたもので、完全な説明ではない）。

電子メールの送信は、SMTP クライアントが SMTP サーバに TCP/25 で接続要求を出すところから始まる。この時点で、次の制限が可能である。

[A]特定の IP アドレスまたは FQDN の許諾

[B]FQDN を持たないクライアントの許諾

次に所定のコマンドを交換し、誰から(From)誰宛(To)のメールであるかを受け取る。この段階では、次の制限が可能である。

[C]存在しないドメイン名からの許諾

[D]存在しないユーザ名の許諾

これらの制限で拒否されなかった場合は、ヘッダと本文の転送が始まる。ヘッダや本文についても確認と制限の設定が可能であるが、先に述べた本文に立ち入らないという方針から、ここではこれ以上の説明は行わない。

Postfix では、[A]から[D]について、さらに細かな設定が行えるので、実際に使っている具体的な設定パラメータ名とともに紹介する。

[A]と[B]に関して

smtpd_client_restrictions により設定でき、クライアントに関して 10 種類の制御が可能であり、次の２種類を使用している。

[A]check_client_access（IP アドレス・ホスト名・ドメイン名による制御が可能で、hash または 2.1 以降なら CIDR で指定）

[B]reject_unknown_client（IP アドレスが逆引きできないか、逆引きした結果のホスト名に A レコードがない場合に拒否）

[C]に関して

smtpd_sender_restrictions により設定でき、"MAIL FROM"について 16 種類の制限が可能である。

check_sender_access（送信者のメールアドレス・ドメイン名による制御が可能で、hash で指定）

reject_unknown_sender_domain（送信者のアドレスのドメイン部分が A レコードでも MX レコードでもない場合に拒否）

[D]に関して

local_recipient_maps により、受信可能なユーザ名を確認する。インターネットに直接接続される外部接続専用サーバでは、自分自身はメールを受け取らず、すべて内部の SMTP サーバに送って確認するよう設定する。この制限は、

迷惑メール対策に関係なく従来から行っていた。

最後に、これらの制限により正当なメールを拒否することがあるので注意を要する。最も多いのは、[B]のによるものである。本来なら、送信元の管理者が DNS サーバに SMTP クライアントを正しく設定すべきなのに、これを怠っているために起こる。これについては、発見したらその IP アドレスを許可リストに登録して対応している。[A]に関しては、十分な量の問題クライアント情報が蓄えられ、この分析に基づき設定すれば、受け取るべきクライアントを拒否することは起こっていない。

４．受信制限の導入と効果

３．で述べた制限設定を、一気に導入したわけではない。SMTP クライアントの状況や設定後の効果などを確認しながら、１年以上にわたって慎重に規制を強めてきた。迷惑メールの分析で分かったのは、そのほとんどは、DHCP で割り振られた IP アドレスか FQDN を持たないホストが、ウイルスに汚染されたり第３者中継を許す設定のため、直接 SMTP 接続を試みることで発生している。従って、これら不正な SMTP クライアントからのアクセスをいかに防ぐかがポイントとなる。

電子メール受信拒否の効果を現す例を**図１**に示す。**図１**は、システム管理者の一人（岡田）に届いた迷惑メールについて、一月あたりの件数と１通あたりの平均バイト数とを、４年半にわたって示している。システム管理者には、個人宛のメールとともに、公式 Web サイトやメーリングリストの管理者宛のメールも届いており、津山高専で最も多く迷惑メールを受け取っている。このため、制限のための情報収集を行う対象としたり、制限設定の効果を検証するのにふさわしいと考えている。

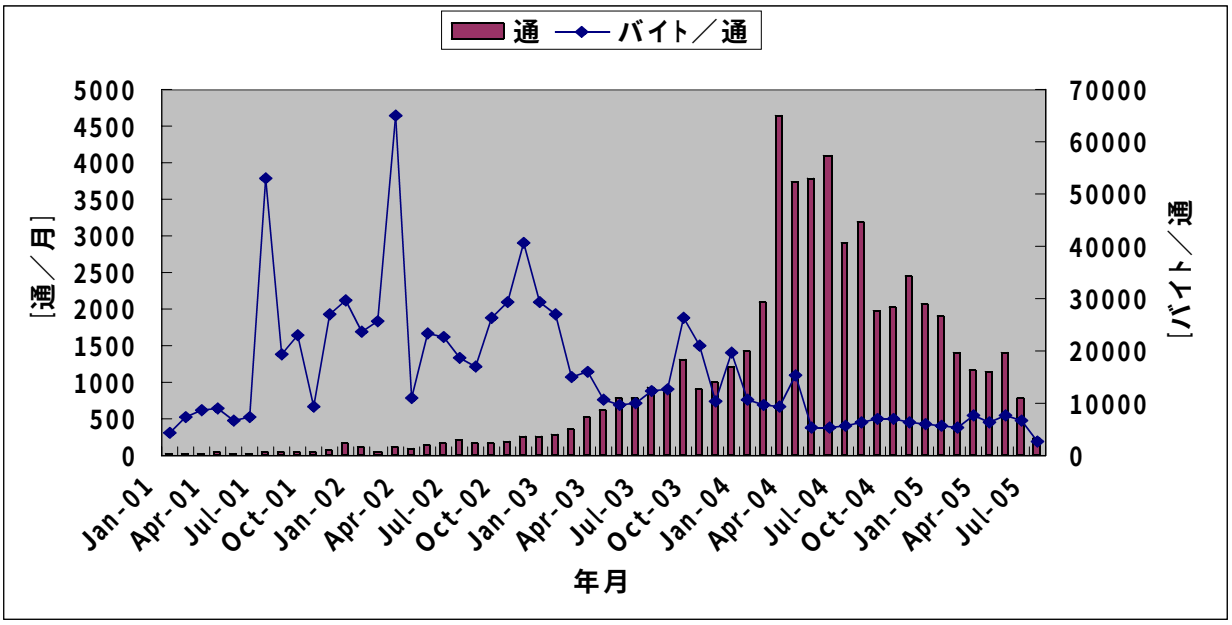

図１　迷惑メールの受信件数と一通あたりのバイト数

迷惑メールの件数は 2003 年頃から増え始めて、2004 年３月には 5000 通弱に達している。制限をかけなければ増え続けたであろうが、制限を加えることで徐々に減少しているのが分かる。なお、ウイルス添付メールは大容量であり、１通あたりのバイト数が大きい月はウイルスをたくさん受け取ったと見ることができる。

受信制限を導入した後も、一時減ったものが増加に転じるということを繰り返している。これは、制限を徐々に強めたためで、規制を強めると一時

期減るが、増加の力が強くて増えている。規制設定を導入した時期と項目は、次のようになっている。

2004 年４月：クライアント名による制限開始[A]

2004 年７月：ドメイン名による制限開始[C]

2004 年９月：クライアントの逆引きによる制限開始[B]

2005 年２月：クライアント名を補完した連続制限開始[A]

2005 年６月：CIDR によるブロック制限

CIDR によるブロック単位の制限が最も強力で、これを導入後は、３年前程度の水準まで迷惑メールの受信数を減らすことができた。これらの処理は、特別なプログラムやサーバを導入することなく実現しており、所期の目的を達している。

５．あとがき

電子メールの本文に立ち入ることなく、特別なプログラム等を使わないで実現できる迷惑メール拒否システムについて報告した。我々の方法は、ごく普通の設定を行っているだけで、新たな経費をまったくかけることなく、ほぼ気にならない水準まで迷惑メールを阻止できている。

ただ、本来ならこのような努力は必要ないものである。正しく設定された SMTP クライアントおよびウイルスに汚染されないパソコンばかりであれば、このような電子メールは届かないはずである。さらに、プロバイダが正規の SMTP サーバ以外のパケットを外に出さないようにしたり（例えば、Outbound Port 25 Blocking）、インターネットに接続するホストを DNS に正しく登録するといった、ごく当たり前の管理ができていないことを実感している。技術者を教育する機関として、何が問題になっているかを積極的に伝え、自然に正しい設定ができるよう教育することの重要性を痛感している。

参　考　文　献

[1]RFC2821(Simple Mail Transfer Protoco): ftp://ftp.rfc-editor.org/in-notes/rfc2821.txt

[2]岡田・寺元・矢野:“全校ネットワークの敷設と運用”、情報処理教育研究発表会論文集、**１３** pp.31-34（1993-8）.

[3]The Postfix Home Page: http://www.postfix.org/

[4]List of All Known DNS-based Spam Databases: http://www.declude.com/junkmail/support/ip4r.htm