津山高専における迷惑メール独自対策の長期検証

岡田　正*　　米澤将人**

Long-term Evaluation of TNCT Independently Blocking of Spam E-mail

Tadashi OKADA* and Masato YONEZAWA**

We reported a unique blocking system of spam e-mail using Postfix mail server proguram six years ago. In this report, a subsequent improvement and an effect of the blocking are reported on a long-term view. We introduce additional refusal rules not only in delivery servers connected to the Internet but in the intramural last receiving server in order to improve a blocking efficiency. Although very slight superfluous restriction has occurred, the mail delivery system by which spam e-mail hardly enters within our campus is realizable without optional software and/or hardware.

Key Words: Blocking Spam E-mail, Postfix, Long-term Evaluation of Blocking Efficiency

１．はじめに

電子メール・ウェブサイト等の安全で安定な運用は，あらゆる組織の情報交換と情報発信に必須なものとなっている．津山高専では，オープンソースソフトウェア(OSS: Open Source Software[1])を活用し，安全なネットワークサーバを安価に自前で構築し，15 年以上にわたって安定に運用している [2]．構築・運用にあたっては，単に業務を遂行するためだけでなく,ここで得られた技術情報や運用ノウハウを，学生教育・地域協力にも波及させ，多面的な教育・研究活動へと発展させてきた[3]．

ネットワークサーバの運用では，セキュリティを重視した上で，複数人での管理を考え原則として標準的で分かりやすい設定を心がけている．この方針の唯一の大きな例外は，先に報告した電子メールサーバの設定である[4]．迷惑メールを学内に入れないことを目的に，津山高専独自の拒否方針をもうけ，固有の設定情報を使った運用を 10 年近く続けて効果を上げている．

本報告では，前回の報告以降に行った追加設定やログ情報を紹介し，迷惑メール独自対策の効果を長期的に検証する．２章では，津山高専独自の迷惑メール対策を，前回報告した以降の追加設定を含めて述べる．３章ではログ情報に基づき迷惑メールの長期にわたる受信状況を紹介し，４章では独自対策効果の検証と課題について考察する．

原稿受付　平成２５年８月３０日

*情報工学科

**専攻科電子・情報システム工学専攻

２．津山高専の迷惑メール独自対策

津山高専の電子メールサーバに実装している迷惑メール拒否方法は，SMTP(Simple Mail Transfer Protocol, RFC5321[5])手順に基づいて，可能な限り初期の段階で拒否することで効率を上げるものである．前報で報告したとおり[4]，

(a) 特定の IP アドレスまたは FQDN(Fully Qualified Domain Name)の制限
(b) FQDN を持たないクライアントの制限
(c) 特定のメールアドレス／ドメイン名の制限
(d) 存在しないドメイン名の制限
(e) 存在しないユーザ向けのメール制限

について，OSS のメール配送プログラム Postfix[6]の機能を使って記述している．このとき許可／拒否リストを，津山高専に届いた迷惑メールの情報を使って作成することも特徴であ．

当初登録に使う情報は，システム管理者である本報告筆頭著者（岡田）に届いた電子メールから抜き出していた．その後，拒否設定の精度が向上するにつれて,個人に届く迷惑メールが少なくなったので，対外接続メールサーバのログを利用して，登録に使う情報を増加させた．すなわち，卒業した学生利用者や退職教職員宛に届き"User unknown & host name

not found"となる電子メールを探し，client と from から迷惑メールと判断されるもの（DHCP(Dynamic Host Configuration Protocol)で割り振られたアドレス，ドメイン情報に矛盾があるクライアントなど）を拒否リストに登録している．

しかし，IP アドレスの追加だけでは，巧妙に送りつけられる賞金・アダルト・違法物品等の電子メールを防ぐことに限界があった．そこで，プライバシー保護の方針にやや反する面があることを承知で，2008 年 5 月 12 日から学内の電子メールサーバにおいて Postfix の header_checks[7] を有効にして，電子メールの一部内部情報を制限設定に利用することにした．

設定の特徴として，迷惑メールに含まれるヘッダの特定パターンに一致した電子メールを，拒否して捨てるのではなく，独自コマンドを埋め込むことで管理領域にファイルとして保存できるようにした．これにより，迷惑メールだけを自動で選別・保存し，万一間違いがあっても手動で送信先に配信可能となっている．

保存された電子メール（ファイル）を随時点検し，本当に迷惑メールであるかどうかを確認するとともに，送りつけた IP Address を対外接続電子メールサーバに登録することで，極力前の段階で拒否できるようにする．

これでも一部の迷惑メール（特に，日本語で書かれたもの）は拒否設定をすり抜けていた．そこで，2012 年 6 月 4 日からは内部電子メールサーバで Postfix の body_checks[6] も有効にした．ここでの設定は，悪質で影響の大きいもののみに限定し，少数の短いパターンとすることで，処理負荷を押さえている．

3．迷惑メールの長期受信状況

迷惑メールの受信状況の推移を，月単位（図１）と日単位（図２）で示す．

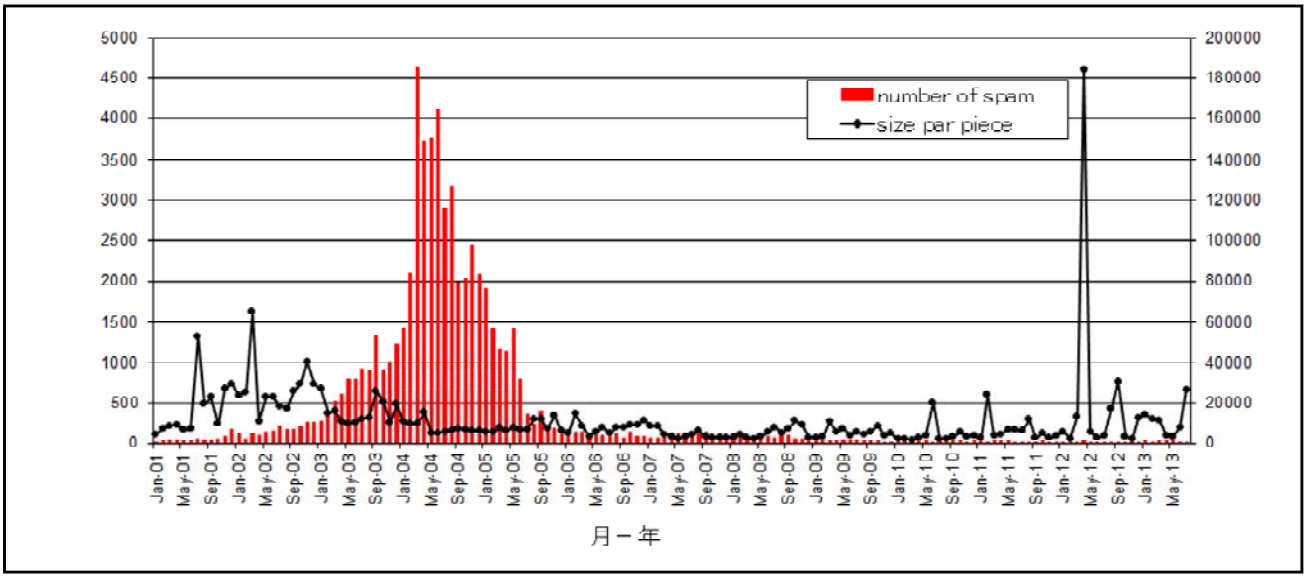

図１　迷惑メール受信状況の推移（月単位）

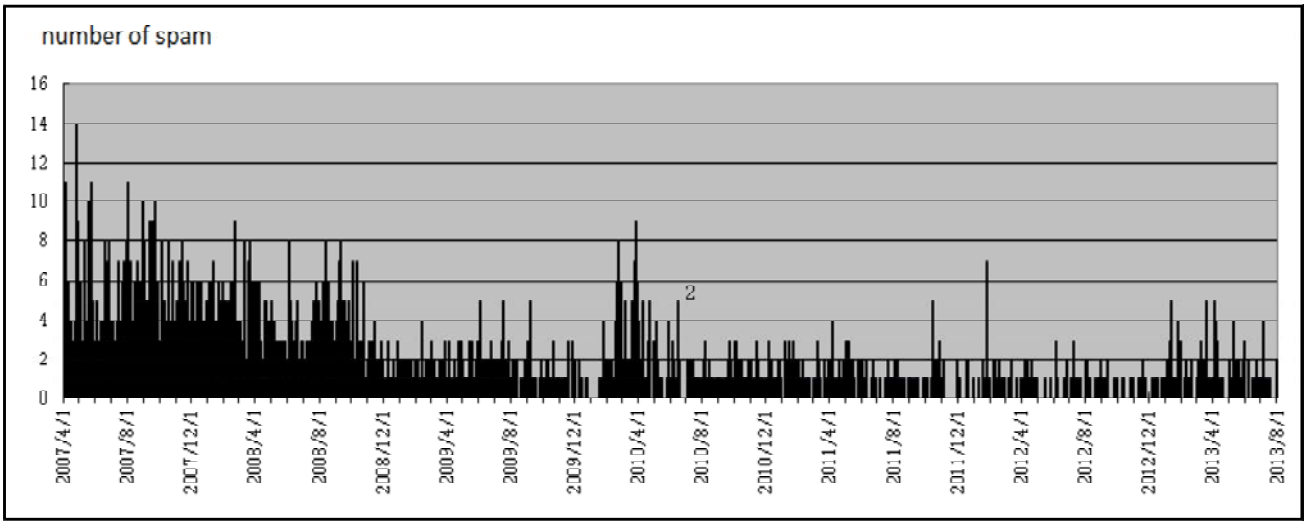

図２　迷惑メールの受信状況の推移（日単位）

図1は,システム管理者の一人である筆頭著者(岡田）に届いた迷惑メールの件数とその1件あたりの平均バイト数を，前報で報告した受信状況を含めて2001年1月から2013年7月までの12年7ヶ月分を示したものである．前報報告時点で月100通前後だった迷惑メールが，header_checks 導入以降は数十通に下がり，現在は 10 通前後となっている．平均バイト数については，件数が減ったので，添付ファイル付きメールを受け取った月は大きな影響を受けているのがわかる．

図1では長期間のデータをまとめて示しているため，大量に届いていた時期と重なっていてわかりにくい．そこで，一日ごとの受信状況を2007年4月1日から2013年8月1日まで示したのが図2である．過去2年で見ると，2012年1月25日に7件受け取ったのが最大で，一週間届かない週もある．ただ，拒否リストを追加しているにもかかわらず，その後漸減しているわけではない．5 件程度受け取る日もあり，新たなパターンで迷惑メールを送りつける状況が続いているのが見て取れる．

次に header/body_checks の効果について述べる(ログの詳細は省略)．管理領域に保存したファイルは，通常月あたり数十通である．しかし，状況によって大きく変動するのが，この制限の特徴である．例えば，特定利用者が標的になって，同じような電子メールが大量に届き一定期間増加することがある．あるいは，新たな教職員を新規利用者として登録し，その方が前任組織から電子メールを転送されることがあり，組織によっては迷惑メールが大量に含まれていて多くのファイルが溜まることがある．いずれにしても，header/body_checks により，巧妙な迷惑メールを拒否するのに効果のあることを確認できた．

4．独自対策効果の検証と課題

3章で示したように，最も大量に迷惑メールを受け取るであろうシステム管理者に，現在では，数日に1通，月に10通前後届く環境を実現できている．月平均 4000 通程度の電子メールを受け取っているなかで，まったく気にならないレベルである．システム管理者以外の利用者で，迷惑メール拒否の効果を感じられるのは，他組織との異動を経験された場合であろう．本校に赴任された方または他機関に転出された方から，本校で迷惑メールを読むことがほとんどない(なかった)との感想を複数聞いており，本校の対策が有効に機能しているからだと考えている．

次に，本校のメールサーバ全体としての受信状況を，前報と同様に制限条件ごとに比較検討する．アクセス解析を行ったのは，前報とほぼ同じ時期の2013年6月15日から6月22日の一週間である．内部に転送した割合は 16 %と変わらなかったものの，制限条件の割合は大きく変わった．

まず，2章の条件(b)が 29 %から 55 %へと大きく増加した．これは，FQDN を持たないクライアントからのアクセスで，IP ベースのインターネット管理に起因する継続した問題である．インターネットの普及に伴い，適切に管理されていないパソコン等の存在が増えている結果と考えられる．後で述べる過剰制限を生じる原因の一つともなっており，引き続き注視していく必要がある．

一方，IP アドレスを拒否する2章の条件(a)は，20 %から 8 %へ減少した．正規に登録されている IP アドレスについては，OP25B(Outbound Port 25 Blocking)[8)]の導入など適切な管理が進むという良い面の反映であろう．また，途中で接続を切るクライアントは33 %から18 %へと，こちらも減少している．これは，迷惑メールを送りつける手法が洗練されてきて，時間のかかる接続をいやがるという悪い面が読み取れる．

次に，内部メールサーバで header/body_checks を導入した効果を検討する．保存された電子メールを見ると，新たなソフトウェアやハードウェアを追加することなく，最小限のメール情報を使うだけで，巧妙な迷惑メールを排除できている．この方法で，最も気がかりなのは，処理によるサーバ負荷の増加である．日常的にメールサーバの負荷状況を監視していると，実行待ちジョブの平均数が一時的に3近くになることがある．このときプロセスを確認すると，外部から送られてきた電子メールを大量に処理している．しかし，処理自体は単純なテキスト検索で，現行サーバの CPU・メモリ等の資源で十分に対応できる．とはいえ，個別電子メールの内部情報を使うので，body_checks だけでも廃止できる状況にしたいと考えている．

最後に，過剰制限について検討する．2012 年 4 月から2013年3月の一年間（平成24年度）に，13件の過剰制限が発覚した．発覚した場合は，原因を調査し設定を修正するとともに，同様の過剰制限が起きていないかどうか maillog をさかのぼって確認している．少なくとも上記の期間において，発覚した以外の過剰制限は見つかっておらず，精度良く対処できていると考えている．

年間 100 万通に達する受信メールに対しごくわずかな件数であるとはいえ，電子メールの重要性から過剰制限は完全になくすのが理想である．過剰制限の原因は，逆引きできないクライアントから，または CIDR(Classless Inter-Domain Routing)指定した連続アドレスに含まれるクライアントからのアクセス

である．前者は外部の問題で，先に述べたようにこの拒否設定は外せないので，正当な FQDN を持つメールサーバを使って欲しいというしかない．後者は内部の問題で，CIDR による効率性を追求しながら，登録時に範囲をていねいに確認し過剰にならないよう心がけている．

過剰制限かどうか，何が原因かの解析は，maillog の検索で簡単に行える．さらに設定変更は，単一のテキスト形式設定ファイルを編集するだけである．過剰制限がわかれば，IP アドレスとして許可設定を行い，FQDN の有無にかかわらず，または CIDR 指定範囲に入るかどうかにかかわらず，受け取れるようにしてある．なお，ログ情報から，過剰制限を自動的に検出できないか検討しているものの，一般化できる有効な条件を見いだすに至っておらず，未だ適切な方法を実装できていない．

５．あとがき

本報告では，津山高専が 10 年近く運用している独自の迷惑メール対策について，前回報告した以降の状況を中心に設定と推移を述べた．特別なソフトウェアやハードウェアを必要とせず，制限の設定や保守が容易で，メールサーバの負担を軽くし，利用者の追加設定を必要としない制限方法をめざして，Postfix の機能だけを使って実装している．さらに，津山高専に届いた迷惑メールの情報を使い，徐々に制限を強めることで，迷惑メールがほとんど届かない環境を実現できた．

しかし，過剰制限をなくしたり，設定リストを保守するには，引き続きログ情報を監視したり，インターネットに関する情報収集が欠かせない．とりわけ，送信ドメイン認証[8)]を始めとした新しい技術が一般化すれば，速やかに対応しなければならない．さらに，IPv6 が普及すると現在の IPv4 ベールの設定が使えなくなる．このとき，どのような技術で迷惑メールを届かないようにするのか，電子メールにまつわる課題を継続して検討していく必要がある．

謝　辞

常日頃からネットワークサーバの運用・管理を始としたシステム管理業務に協力していただいている総合情報センター，特にシステム管理者の皆さまに感謝いたします．また，一部の教職員には過剰制限でご迷惑をおかけしており，この場を借りてお詫びいたします．

参　考　文　献

1）The Open Source Initiative：http://opensource.org/.

2）岡田正：安全で教育的な情報通信基盤の構築，論文集「高専教育」 第 24 号，pp.259-264（2001）.

3）平田克己，岡田正：学内情報ネットワークの独自運用と波及効果，平成 20 年度高専教育講演論文集，pp.245-246（2008）.

4）平田克己，岡田正：津山高専における迷惑メールの独自対策とその効果，津山工業高等専門学校紀要 第 49 号，pp.61-66（2007）.

5）http://www.rfc-editor.org/rfc/rfc5321.txt.

6）The Postfix Home Page：http://www.postfix.org/.

7）Postfix manual - header_checks（5）：http://www.postfix.org/header_checks.5.html.

8）迷惑メール相談センター｜ JADAC：http://www.dekyo.or.jp/soudan/.