津山高専における迷惑メールの独自対策とその効果

平田 克己* 岡田 正*

TNCT Independently Blocking of Spam E-Mail and Its Effects

Katsumi HIRATA and Tadashi OKADA

E-mail has become a necessary means of communication for various businesses and daily lives. In recent years, spam e-mail has increased as e-mail has become more popular, and now, the spam is an object of public concern. Like a letter or a card, an e-mail should not be censored and restricted. Without blocking the spam, however, unmanageable spam or computer virus attached the spam may damage computers and their networks. In our college, blocking of the spam has been implemented on our mail servers since 2004. We adopted not content-based but IP-based filtering to respect the privacy of users. The blocking only needs functions of Postfix mail server program without optional software and/or hardware. And it can be configured, maintained, and monitored by our own hands. In this paper, after basic policies of the blocking and actual configurations of Postfix are explained, effects and problems are discussed.

Key words: blocking spam e-mail, Postfix, no optional software and/or hardware, independently administration

1．はじめに

電子メール（以下，メールという）は様々な業務や日常生活において欠かすことのできない通信手段の一つとなりつつある．一方，これを悪用して，相手に望まないメールを送り付ける，いわゆる迷惑メールが爆発的に増えてきており，社会問題にまで発展している[1)]．

メールの歴史は古く，インターネットが一部の研究者の間で使われていたころから用いられてきた．はじめはUUCP（Unix to Unix Copy Protocol）などのプロトコルが使われていたが，1980 年頃からはSMTP（Simple Mail Transport Protocol）[2)]が広く使われるようになり，その後基本的な仕組みはほとんど変わらずに現在に至っている．SMTP は，その名前が示すようにシンプルであるため，広く実装されてきたが，その反面，悪用もしやすい．特に，近年家庭でのインターネット常時接続が普及し出したのを境に，迷惑メールをまき散らすようなウイルスの蔓延もあり，急激に迷惑メールが増えてきている．これに対し，メールサーバやメールを読み書きするメーラソフトで迷惑メールを遮断が試みられているものの，迷惑メールを送る側とそれを遮断する側とのいたちごっこが続いており，いずれも決め手となるものがない状況にある．

迷惑メールを遮断する方法としては，メールの送信元（From ヘッダ）によりフィルタリングしたり，メール内容を解析するという方法がよく使われている．送信元フィルタリングでは，送信元を簡単に詐称することができるため，それほど効果はないようである．また，本文の内容によりフィルタリングするためには，メールサーバで通信内容にまで立ち入ることになり，あまり好ましくない．本来メールは，手紙やはがきのように信書である側面も持っていると考えられるからである．さらに，ある人にとっては迷惑なメールであるかも知れないが，別の人にとっては有用な情報である可能性もある．したがって，メールサーバなどの通信経路で一括して何らかの制限をかけることは，できれば実施すべきではない．

本校では，従前より極力規制をしない方針でネットワークを運用してきた[3)]．しかし，数年前からウイルスの蔓延によるコンピュータやネットワークへの被害に頭を悩ませてきた．このことを受けて，2004 年度から段階的にメールの受信制限を導入してきた．本校で実装した方法は，追加のソフトウェアやハードウェアを導入することなく，メール配送プログラム Postfix[4)]が本来持っている機能だけで実現可能であり，学内のシステム管理者だけで簡単に設定・保守・監視できるものである．

本論文では，本校で実施している迷惑メール対策

原稿受付 平成 19 年 8 月 27 日

＊ 情報工学科

の基本方針とメールサーバの具体的設定内容について説明した後，その有効性と問題点について，実際のメール受信状況のデータの評価を通して検討する．

2．迷惑メール対策方法

2．1　基本方針

外部から送られてくる迷惑メールの受信制限を導入するにあたり，以下の基本方針をたてた[5]．

(1) プライバシーの保護

本校における電子メールは，公の設備を用いたサービスとはいえ，そのほとんどが個人宛の私信であり，業務上の機密事項や個人のプライバシーに関わるような事項が含まれている．そのため，システム管理者といえどもみだりにその内容に立ち入るべきではない．このような考えのもと，本文の内容による制限は行わない．ただし，差出人や宛先といった，手紙に例えたときに，封筒の外側に書かれるような情報は用いることにする．

(2) 設定内容と制限結果の完全な把握

商用の遮断ソフトなどでは，どのような方法で遮断がなされているかが隠匿され，ブラックボックスになっている場合が多い．これは，商業上の都合であり，その方法を開示することによって，悪者に手の内を見せることになるし，あるいは特許にかかわる技術が含まれている場合もある．しかし，メールという重要なサービスに制限を加える以上，システム管理者はその制限状況に責任を持つ必要がある．このようなことから，我々自身の手で設定からログの監視までを行うことができ，どのような設定をしていて，その結果どのメールを遮断したかを完全に把握できるようにする．

(3) 管理・保守の容易さ

(2) を達成するためにも，システム管理者に過度の負担がかからないよう，特別なソフトを用いなくとも，容易に設定することができ，通常のログファイルの監視だけで，その状況を簡単に把握できるものにする．

(4) 管理や導入に追加の経費が不要

これまで用いている OS とそれに付随して通常インストールされているプログラム，およびメール配送プログラム以外に追加でソフトウェアの導入をしたり，定期的にブラックリストを更新するために契約を結んだりする必要がないものにする．また，高性能なハードウェアを導入しなければ，配送遅延が生じるような方法は避ける．つまり，通常のシステム管理にかかる人手以外に，新たに費用がかからないようにする．

(5) 完全性を求めない

迷惑メールとはいえ，最低限決められたメール配送規則にのっとって送られてくるため，迷惑でないメールとを見分けて，完全に自動で遮断することは困難である．迷惑メールを送る側も日々工夫をしており，また，完全性を求めすぎるあまり受信制限を厳しくし過ぎて，正当なメールまでをも遮断してしまう可能性もある．迷惑メールが 1 通や 2 通届いたからと言って，即被害が出るというものでもない．迷惑メールが気にならない程度まで遮断できれば良いものとする．

(6) ２系統での同一の制限が可能

本校ではインターネット接続回線を 2 系統有しており，それぞれで外部向けメールサーバが稼働している．そのため，両系統に同一の制限を容易にかけられるものにする．

2．2　メールの配送過程と受信制限

(1) ～ (6) の基本方針を全て満たすものとして，本校にて従来から用いてきたメール配送プログラムである Postfix の機能を用いることにより十分実現可能であると考えた．メール配送プログラムとしては，Sendmail[6]が古くから広く用いられ，多くのサーバに標準でインストールされてきた．様々な環境に対応できるように幾多の改良がなされ，多くの機能が追加されている．その結果，プログラムが非常に複雑化し，セキュリティホールも次々と発見されるようになった．また，その高機能さゆえ，設定ファイルが非常に複雑で，相当高度な技術を持った者でないと，完全な管理が難しいとまで言われている．例えば，設定ファイルを作るための専用のプログラムが，別に開発されているくらいである．

このような問題に対処するために，qmail[7]や Courier[8]，exim[9]といった，安全で管理がしやすく，現在のインターネット環境に合ったメール配送プログラムが開発された．Postfix もその一つであり，特に Sendmail からの移行がしやすいという特長がある．さらに，他の後発のメール配送プログラム同様，設計段階よりセキュリティや機能拡張を考慮して開発されているため，簡単な設定により迷惑メールや不正アクセスに対処することができる．

Postfix の設定のほとんどは，main.cf という設定ファイルを編集するだけで済む．このファイルは極めてシンプルなテキストファイルであり，メールサーバとしての基本設定から，ホストやドメインごとのアクセス制御，その他迷惑メールの拒否設定に至るまで，多数の細かい制御を簡単に設定することができる．特に，迷惑メールの拒否設定に関しては，送信元ホストの IP アドレスやドメイン名に応じた不正中継対策や，DNS を利用したブラックリストデータベースによる制限，さらにはメール本文の内容によるフィルタリングも可能となっている．本校では，メールの内容による制限はしないとの基本方針を立

てているので, 特に送信元ホストの IP アドレス等により制限する機能を採用している.

ここで，メールを送信するクライアントと受信するサーバの間におけるメール配送過程について説明する．クライアントは，プロバイダや各機関が提供するメール送信用サーバであったり，個人で構築した自宅メールサーバであったり，あるいは，迷惑メールを大量に送信するように悪者によりウイルスを仕掛けられたクライアント PC であったりする．一方，サーバはメールを受信するサーバであり，本校で学外からメールを受け取る場合は，外部向けに設置されたメールサーバを指すことになる．クライアントもサーバもいずれも，メール配送プログラムがその処理を担っており，逆に学内から学外に向けてメールを送信するような場合は，立場が逆になるだけである．ここでは，学外からメールを受信する場合に的を絞って述べる.

クライアントのうち，勝手に迷惑メールを送信するようなウイルスを仕掛けられた PC のことを俗に「ゾンビ PC」と言う．悪者が複数のゾンビ PC を裏でコントロールし，ボットネットと呼ばれるネットワークを形成して，組織的に迷惑メールをばらまいていることが知られている．近年の常時高速接続環境の普及により，このボットネットがますます蔓延し，問題となっている.

Fig.1 は，メールの配送過程を示したものである．まず，クライアントからサーバに TCP/25 で接続要求を出す．この時，クライアントの IP アドレスがサーバに伝わる. サーバから接続 OK の応答が来たら，クライアントは HELO（Hello）コマンドでクライアントの FQDN（完全修飾ドメイン名）を, MAIL FROM コマンドで送信元のメールアドレスを，RCPT TO コマンドで宛先のメールアドレスを順次送る．HELO コマンド以降で得られる，クライアントの FQDN と送信元および宛先メールアドレスとは, いずれも“自己申告”であり，嘘を付いている可能性があることに注意しなければならない．つまり，通常信用できるのは, 接続要求の段階で得られる IP アドレスだけである．これらのやりとりのあと，クライアントは DATA コマンドに続けてメールの本体（ヘッダと本文）を送る．さらに，本校の場合は，外部向けメールサーバで受け取ることになったすべてのメールは, 内部向けサーバへ転送される.

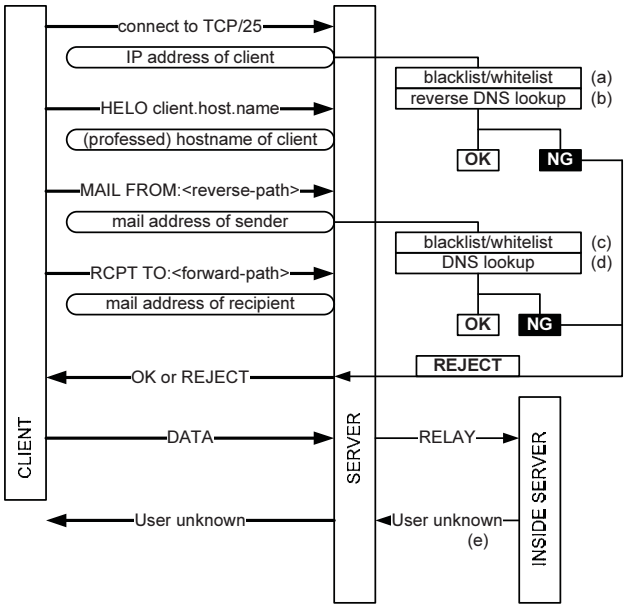

Fig.1 A diagram illustrated of receiving an e-mail from a client by a Postfix server and accepting or rejecting according the configurations from (a) to (e).

以上のやりとりの中で，メール本文に立ち入らずに迷惑メールかどうかを判定する材料としては，クライアントの IP アドレス（または FQDN）と差出元のメールアドレスである．まず，はじめの接続要求で得られるクライアントの IP アドレスから，

（a）　特定の IP アドレスまたは FQDN の制限

（b）　FQDN を持たないクライアントの制限

が可能である．次に，MAIL FROM で得られる送信元メールアドレスから，

（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

が可能である．さらに，RCPT TO で得られる宛先のメールアドレスから，

（e）　存在しないユーザ向けのメールを制限

が可能である．最後の（e）については，ユーザ情報が登録されている内部向けメールサーバに転送されて初めて判定できるものである．それ以外の（a）～（d）に関しては，いずれも，外部向けサーバにてメール本体を受信する前に判定し，受け取りを拒否することができる.

２．３　Postfix における実際の設定

前節で挙げたそれぞれの制限に対する，Postfix での実際の設定について述べる．なお，これらの制限はすべて，Postfix の設定ファイルである main.cf に記述し，必要に応じてテキストベースのリストファイルを作成することによって実現できる．設定ファイルの中で, smtpd_client_restrictions パラメータを設定することによって TCP/25 への接続要求段階での制限（(a) と (b)）を，smtpd_sender_restrictions パラメータを設定することによって MAIL FROM コマンド段階での制限（(c) と (d)）とを，それぞれ設定することができる．これらのパラメータに多数の制御パラメータを付加することによって，その動作を細かく制御可能である.

（a）　特定の IP アドレスまたは FQDN の制限

check_client_access パラメータを設定し, hash 形式か CIDR（Classless Inter-Domain Routing）形式でその

配送可否を指定したリストを用意しておけば，IP アドレスやホスト名またはドメイン名ごとに配送の可否（OK か REJECT）を指定することができる．制御パラメータは，その記述順序が優先順序となるので，次の（b）の制限より優先させて，特定のクライアントだけ配送可とすることもできる．つまり，このリストは，ブラックリストとホワイトリストとの両方の働きをするものである．

（b）　FQDN を持たないクライアントの制限

reject_unknown_client パラメータを設定すれば，IP アドレスを DNS に問い合わせた（逆引きした）結果，FQDN が見つからないか，見つかったとしても A レコードがない場合に，配送を拒否することができる．

（c）　特定のメールアドレス／ドメイン名の制限

check_sender_access パラメータを設定すれば，hash 形式で記述されたリストに従って，送信元のメールアドレスやドメイン名ごとの配送可否を指定することができる．また，（a）と同様に，次の（d）の制限によらず優先的に配送可と指定することもできる．

（d）　存在しないドメイン名の制限

reject_unknown_sender_domain パラメータを設定すれば，送信元メール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，配送を拒否することができる．

（e）　存在しないユーザ向けのメールを制限

外部向けメールサーバには，インターネット側と学内側とのメールの中継機能しか持たせていない．そのため，外部向けメールサーバはユーザ登録情報を持っていない．存在しないユーザ向けのメールは内部メールサーバに配送された際，User unknown が外部向けサーバに返され，エラー通知メッセージが送信元アドレスに送られる．

２．４　リストファイルの保守

本校には学外接続が 2 系統あり，それぞれに外部向けメールサーバが稼働している．その両方の Postfix に対して上記（a）～（e）の制限を設定している．このうち，（a）と（c）に対しては，拒否したい IP アドレスや FQDN，あるいはメールアドレスやドメイン名のリストを作成し，適切に更新する必要がある．これについては，管理者がメールの中身を確認可能な管理者自身宛てに届いた迷惑メールや，存在しないユーザ宛てに送られてきた迷惑メールの送信元情報を用いて適宜リストを更新している．

また，本来届くべきメールが上記の制限により迷惑メールであると誤判定される場合がある．これは，送信元ホストが DNS サーバに正しく設定されていないことにより，（b）によって配送拒否されてしまうことがそのほとんどである．これについては，ログ監視や利用者からの連絡により発見し次第，拒否したくないクライアントとして，その IP アドレスを（a）に追加するようにしている．（a）や（c）については，十分に吟味をして拒否したいクライアントを追加することにより，誤判定による拒否がないように注意する必要がある．

３．受信制限の効果

本校では，２．で述べた迷惑メール制限を 2004 年度から導入した．最初の 1～2 年は，送信元ホストの状況や効果を確認しながら，段階的に制限を強めてきた．すべての制限を導入した後も，ログや管理者宛てに届いたメールを継続的に監視し，その効果を確認している．

３．１　迷惑メール件数の推移

Fig.2 は，システム管理者の一人（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とについて，2001 年 1 月から 2007 年 7 月にわたる推移を示している．件数（棒グラフ）を見ると，2002 年ごろからじわじわと増え始め，2003 年後半ごろから爆発的に増えてきていることがわかる．その後，2004 年 4 月から段階的に減り始め，2005 年後半以降はおよそ 100 件／月のレベルで落ち着いている．本論文で報告している迷惑メール制限をちょうど 2004 年 4 月から段階的に導入したことを考えると，この制限により迷惑メールを効果的に遮断できていると言うことができる．2007 年に入ってからの平均が約 95 件／月で，1 日あたりに換算すると，3～4 件程度である．最も多く迷惑メールを受け取っていると考えられる管理者で，2007 年 7 月では全受信メールの 3.3%が迷惑メールであり，ほとんど気にならないレベルである．

次に，迷惑メール 1 件あたりのバイト数（折れ線グラフ）を見ると，2004 年くらいまでは月によって非常に大きくなっていることがわかる．このような月は，サイズの大きなウイルスが添付されたメールを受け取っていたと考えられる．その後は月によって多少山があるものの，以前ほど大きくなることはなくなった．このことは，効果的に迷惑メールが遮断できている結果であるともいえる．一方，迷惑メールの形態自体が変わってきていることの反映でもある．日々進歩している迷惑メール対策に対抗して，迷惑メール送信者もその内容や送信手法を工夫していることも事実である．

最近では，メール本文の検査による迷惑メール遮断を回避しようと，内容を全て画像ファイルにしたものや，文字を並べて意味のある言葉や絵の形を作る，いわゆるアスキーアートを用いたものなど，様々な手法が現れている．さらには，画像ファイルを PDF 形式にしているものも報告されている [10),11)]．最近は PDF 形式の書類を添付して送る場合が増えてきてお

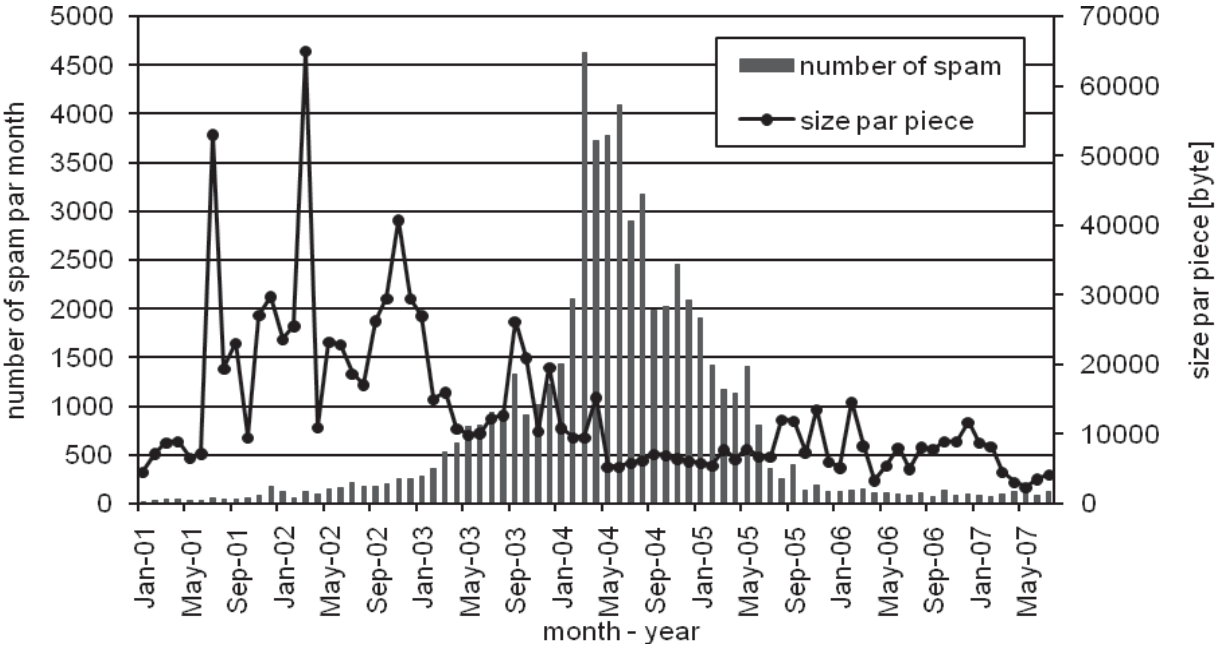

Fig.2 Changes in number of spam mail (bar chart) and size of the mail (line chart) between January 2001 and June 2007.

り，メールの中身の検査だけでは迷惑メールかどうかを判定するのはなかなか難しいようである．

３．２　受信制限状況

本制限により，外部から送信されてきたメールがどのように処理されているかについて検討する．Fig.3 は, 2007 年 6 月 16 日～23 日の一週間に本校外部向けのメールサーバにあったアクセスのうち，どのような理由でどれだけが拒否あるいは配送されたかの内訳を示したものである．これは，Postfix の標準的なログから簡単に解析できるものである．(a)～(e) は，それぞれ２．で述べた制限 (a)～(e) に対応している．(f) は，クライアントが接続を切ったもの，(g) が内部のメールサーバに配送されたものである．すなわち，(g) は迷惑メールではないと判定され，内部に転送したものである．この内訳を見ると，送られてくるメールの内 8 割強が迷惑メールであることになる．実際，世間では全メールに占める迷惑メールの割合は 6～8 割にものぼるとも言われており，これと比べても本制限による迷惑メールの判定は妥当なものであると言える．

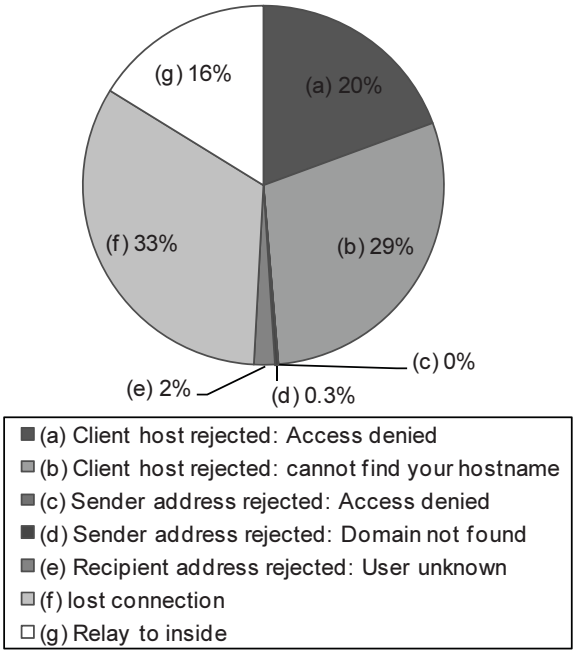

Fig.3 The details of processing for incoming SMTP connection from outside by Postfix between June 16 and June 23, 2007.

(a) と (b) は，TCP/25 接続要求の際の IP アドレス情報を使った制限であり，これらの占める割合が比較的大きい．一方 (c) と (d) の割合は非常に小さい．これは，(c) と (d) がいくらでも詐称できる MAIL FROM コマンドで渡される差出元メールアドレスの情報を用いているからである．迷惑メール送信者は，メールアドレスを次から次へと変えている，あるいは，実在するドメイン名を騙っていることが多く，これらによる制限にはあまり引っかからない．この内訳の中で最も大きい (f) については，HELO や MAIL FROM，RCPT TO コマンドに対するサーバからの応答待ちの最中に，クライアント側から切断しているものである．迷惑メール送信者は，できるだけたくさんのメールをばらまきたいため，少しでも時間がかかるような場合は，すぐに切断して次へ行くように設定しているようである．実際，メールサーバにわざとディレイの設定をして，迷惑メールを遮断しようとする試みも報告されている [12].

３．３　今後の課題

本迷惑メール対策により，ユーザに届く迷惑メールを気にならないレベルにまで抑えることができた．送信元 IP アドレスやメールアドレスのブラックリスト（またはホワイトリスト）は管理者により適宜更新されているものの，Fig.2 を見る限り，ここ 1 年半くらいは一か月当たりの迷惑メール件数が 100 件前後を行ったり来たりで，なかなかこれ以上減少させることができていない．今以上に減少させるためには，今後，新たな制限設定の導入が必要であると考えられる．例えば，現在は用いていない HELO コマンドで得られるクライアントの FQDN 情報の利用である．この FQDN は自己申告であり，迷惑メール送信者はこれを詐称している可能性が高い．これと，TCP/25 接続要求時に得られる IP アドレス（から得られる FQDN）とを比較して，食い違っている場合は迷惑メールであると判断して，配送拒否するような方法が考えられる．

一方，本来は届くべき迷惑ではないメールに対する，誤った拒否も少しではあるが存在する．2006 年度の例では，年間で 15 件が過剰制限されている．一か月あたりに換算すると 1 件程度と，年間 140 万件（推定）のメール件数に比べて十分な精度であるとはいえ，できればなくしたい．この点については，正当なメールサーバの挙動を自動的に検出し，報告するシステムを導入するなど，さらに精度を高める必要がある．

４．おわりに

近年問題となっている迷惑メール対策に対して，本校では独自に受信制限を導入している．これは，メール送受信者のプライバシーを保護しつつ，学内のスタッフだけで導入・運用でき，特別な追加費用が不要であるといった特長を持っている．この受信制限により，迷惑メールをピーク時の 2004 年 3 月に対して，およそ 45 分の 1 も抑えることができている．また，誤った過剰制限もほとんどないことからも，本校においてこの迷惑メール対策は非常に効果的であることが確認できた．

本論文の手法は，追加費用が必要なく，オープンソースソフトウェアベースの仕組みであるため，地域連携で構築したサーバ [13] へも適用して効果を上げている．こちらのログ情報からもフィルタリング用のデータを得ている．しかし，迷惑メール送信者も，工夫を凝らして日々新しい手法で対抗してくることが予想される．このような攻撃に対して，今後も継続して柔軟に対処してゆく必要がある．

謝　　辞

本論文の執筆は，独立行政法人国立高等専門学校機構で実施された高専間教員交流による活動の一環として行われたものである．同機構並びに両高専をはじめとする関係者の皆様のご協力に深く感謝いたします．また，迷惑メール対策に関係された，本校総合情報センター関係者を始めとする，多くの教職員の皆様にも，この場を借りてお礼申し上げます．

参　考　文　献

1) 迷惑メール相談センター, http://www.dekyo.or.jp/soudan/,（財）日本データ通信協会
2) RFC2821，http://www.ietf.org/rfc/rfc2821.txt
3) 岡田，日下，寺元：津山高専の情報通信環境の運用管理，津山工業高等専門学校紀要，40 (1998) 7-15
4) The Postfix Home Page, http://www.postfix.org/
5) 岡田，寺元，日下，最上：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，第 25 回高等専門学校情報処理教育研究発表会論文集 (2005) 56-59
6) Sendmail.org -Sendmail Home-, http://www.sendmail.org/
7) qmail: the Internet's MTA of choice, http://cr.yp.to/qmail.html
8) Courier Mail Server, http://www.courier-mta.org/
9) exim Internet Mailer, http://www.exim.org/
10) Symantec Messaging and Web Security：シマンテックマンスリースパムレポート 2007 年 2 月, http://www.symantec.com/ja/jp/enterprise/security_response/whitepapers.jsp (2007)
11) Symantec Messaging and Web Security : The State of Spam A Monthly Report – July 2007, http://www.symantec.com/enterprise/security_response/whitepapers.jsp (2007)
12) 鈴木：ブロッキング，スロットリング（技術的側面から見た spam メール対策），情報処理，46，7 (2005) 754-757
13) 田渕，佐野，岡田：Web サイト公開支援システムの構築とオープンソースの効果，津山工業高等専門学校紀要，48 (2006) 55-60