希望者に対応した迷惑メール対策と効果：山口大学における実施事例

久長　穣†，杉井　学†，長　篤志‡，三池　秀敏‡

†山口大学大学情報機構メディア基盤センター

‡山口大学大学院理工学研究科

あらまし　電子メールは，大学においても教育研究活動はもちろん管理運営の中で，情報交換の代表的でかつ重要なツールとなっている．その一方で，迷惑メールに爆発的な増加により，業務メールが埋もれてしまい支障をきたしている．電子メール環境を正常に保つためには，迷惑メールを排除する仕組みが必要不可欠である．迷惑メールを排除する仕組みが幾つか提案されてきたが，通常メールを迷惑メールとする誤判定等が少なからず存在する．迷惑メールの誤判定に対する組織内の各構成員の受け止め方は千差万別であり，また、対策を全構成員に適用するためにはコストの問題も存在し、迷惑メール対策の導入を困難にしている．

我々は，電子メールの利用状況を考慮し、一律な対策ではなく、希望者に対してのみ対策を行うことで，組織内に比較的容易に迷惑メール対策を導入でき，十分な効果を上げることができた。本稿では，迷惑メール対策の具体的な導入事例について述べるとともに，大学における迷惑メール対策のあり方について議論する．

キーワード　迷惑メール対策，キーワード判定，特徴スコア判定，barracuda SPAM Firewall, postfix, LDAP 認証

Effectiveness of Spam E-Mail Countermeasure Reflecting User's Demands: A Case Study in Yamaguchi University

Yutaka HISANAGA †, Manabu SUGII †, Atsushi OSA ‡, Hidetoshi MIIKE ‡

† Media and Information Technology Center, Yamaguchi University

‡ Graduate School of Science and Engineering, Yamaguchi University

Abstract E-mail is a typical and an important information tool in management for educational research activity at university. Explosive increase of a large amount of spam e-mails has brought a crisis of e-mail communications. A mechanism is required to exclude spam e-mails. Conventional countermeasures for spam e-mails commit a misjudgment to the normal e-mails. The misjudgment and the increase of the financial cost prevent to introduce an effective countermeasure to the spam e-mails.

Considering situation of e-mail environment, recently, we introduced a spam e-mail measure reflecting user's demands. We were able to introduce the measure rather easily, and to decrease the cost, and finally to achieve an enough effect. In this paper, we introduce a case study and discuss about the effective spam e-mail measures.

Keyword spam mail measures, barracuda SPAM Firewall, postfix, LDAP authentication

1. はじめに

電子メールは，教育・研究・事務と大学活動の中での情報交換の重要なツールとなっており，利用者数や利用頻度も増加してきている．その一方，学外から多量のメールが送信されてきており，ほとんどが迷惑メールと言える利用者も存在している．近年，通常の電子メールの増加に加え，迷惑メール数が異常に増加している．山口大学で電子メールの利用者数は１日平均約 7,200 人で，配信される電子メールの総数は迷惑メールを含めて 30 万通にもなっている．その中で，８～９割程度が迷惑メールと想定される．大量の迷惑メールは，利用者にとって通常の電子メールを見つけ出すことを困難にし，業務に支障をきたすケースも起きている．

迷惑メール対策の技術的手法は数多く提案されており[1-8]，迷惑メールの対策手法は次のものに分類できる．

（１）　電子メールの配送方式にもとづく対策
（２）　電子メールの内容にもとづく対策
（３）　メールの付加情報にもとづく対策

（１）の電子メールの配送方式にもとづく対策の代表的なものに，**(1a) 迷惑メールの多くが再送処理をしないことに着目した graylisting** がある．受信メールを一旦，保留エラーを返して送信サーバにメールの再送を行わせる．通常メールであれば再送信されるが，迷惑メールであれば再送しないことを利用している．かなりの効果が報告されている[1]．一方で，迷惑メールでも再送に対応してきており，大手プロバイダーなど再送サーバがその都度異なるものなどあり，対策が有効に働かないことがある．そのため，管理者において，必要に応じてホワイトリスト，ブラックリストに登録する必要がある．また，**(1b) 送**

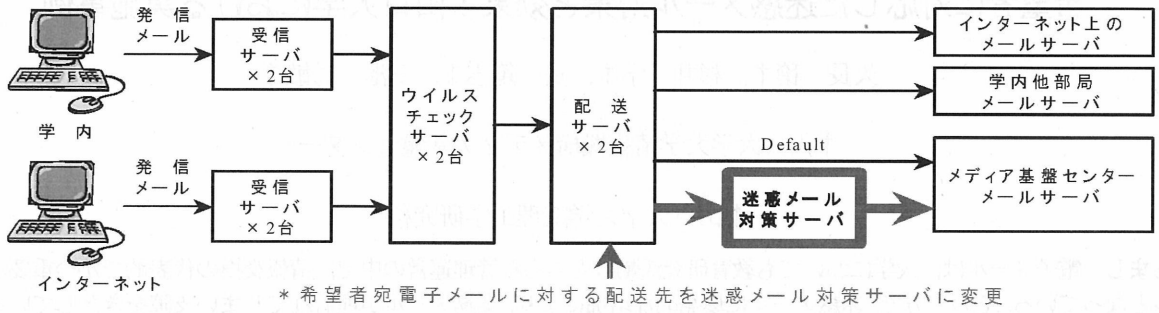

図1　迷惑メール対策サーバの配置

信サーバの DNS の逆引きが不詳なものは迷惑メールと判定する方法がある．しかしながら，DNS(Domain Name System)に逆引きが登録されていても迷惑メールであるもの，DNS に逆引きの登録されていないが通常メールであるものも存在している．これらの方法で、迷惑メールと判断された場合は、送信エラーとなり、発信者に返送され、受信者にはメールが送信されたことに気づかない問題がある。

（2）のメールの内容にもとづく対策には以下の方法がある．**(2a) メールに含まれるキーワードによる判定：**送信者アドレス，件名，本文などに含まれるキーワードや URL により判定する．この場合，新しい迷惑メールに対応するため，判定するためのキーワードのリストを常に更新しておかなければならない．また，これらのキーワードを含むからと言って，直ちに迷惑メールと判定出来ないものも存在する．**(2b) 電子メールの特徴抽出による判定：**電子メールの特徴を抽出し，それらに得点付けをして，一定得点以上を持つ電子メールを迷惑メールと判定する．特徴の抽出方法，それらの得点付け，閾値の設定などを適切に決める必要がある．新しい迷惑メールに対応するために，これらの値を常に更新しなければならない．**(2c) 利用者の分類による判定：**利用者に迷惑メールと通常メールとを分類させることで，迷惑メールを学習させて判定する．この場合，迷惑メールを利用者がある程度分類し，判定基準になる評価関数を適切に定めなければならない．

（3）の電子メールの付加情報にもとづく対策は，電子メールの不正送信を防ぐため，送信サーバを認証するなどの新しい対策方法である．実現すると有効であると思われるが，インターネット上の全てのメールサーバが対応しなければ，適切な判定ができない．**(3a) Sender ID：**発信メールアドレスの送信サーバのリストを DNS に登録しておき，受信側で送信サーバのリストを確認し判定する．**(3b) DKIM(Domain Keys Identified Mail)：**メールに送信サーバのデジタル署名を付けて送信し，受信側で署名を確認し判定する．

完全に迷惑メールのみが駆除できる仕組みは，現在のところ存在していない．少なからず迷惑メールを通常メールに（False Positive），通常メールを迷惑メールと（False Negative）誤判定してしまう場合があり，迷惑メール対策には必ず誤判定に対するリスクが存在する．また、誤判定されたことをメールの受信者が気づかない場合が存在する。これらのリスクを最小限にするための，メールシステムの管理者の負担は大きい．

一方，電子メールは通信の一つであり，通信の秘密，通信の公平性の観点から対策方法を十分考慮する必要がある．特に，大学では広範囲で自由な教育・研究活動を支えるため，各研究者の自主性と独立性が確保された電子メール環境が必要であり，多くの利用者が迷惑メールの駆除を望んでいると考えられるが，迷惑メール対策を望んでない場合もある．利用者によっては迷惑メール対策に対する考え方が大きく異なっている．そのため，大学の情報センター等で，一律に迷惑メール駆除対策が実施できない状況が有ると考えている．

いくつかの大学での迷惑メール対策の状況報告や聞き取り調査等から、迷惑メール対策を導入している大学の多くは全構成員に対して一律な迷惑メール対策が実施されている。誤判定があることを確認できない場合もあるが、誤判定が判明した場合には管理者が対応している。希望者に対してのみ対策を実施している大学は若干であった。また、迷惑メール対策を導入していないところでは、導入コストの大きさを問題としていた。

山口大学では，2006 年 9 月より，迷惑メール対策の導入の容易さ、リスク回避、及び、コスト削減の観点から希望者に対して，電子メールの内容にもとづく迷惑メール対策をおこなうサービスを開始した[9]．本稿では，希望者のみに対する迷惑メール対策のその後の状況と，効果について述べるとともに，利用者と管理者の双方にとって適切な，迷惑メール対策のあり方について議論する．

2. 迷惑メール対策システム

2.1. 迷惑メール対策の概要

山口大学における迷惑メール対策は，2006 年 9 月から希望者へサービスの提供を開始した．学内にはメディア基盤センター以外に他部局のメールサーバも多々運用されているが，メディア基盤センターが運用するシステムが大学の公式メールサーバとして認知され，ほとんどの学内の構成員が利用している経緯がある[．このことから、メディア基盤センターが運用しているメールサーバ宛の電子メール(username@yamaguchi-u.ac.jp 等)のみを対策の対象とした．迷惑メール対策に用いた機器は希望者のみに対して対策を行うことができ、コスト的にも導入が可

能であった，バラクーダ社製の Spam Firewall 400 である．山口大学における電子メールの配送経路の中で，ウイルス検査後，宛先メールサーバに配送する配送サーバとメディア基盤センターメールサーバとの間に配置し，迷惑メール対策希望者の電子メールがこの機器を通過するようにした（図１）．この位置に配置することで，学内，学外から発信された電子メールが迷惑メール対策の対象となる．サービスはタグ付け機能(2006 年 9 月提供)、隔離及びパラメータ変更機能（2007 年 3 月提供）の順で提供した。スコア値の閾値も固定でサービスを開始した．

迷惑メール対策サーバは，電子メールの内容を検査し，次の条件の場合，迷惑メールと判定している．

・スコア：電子メールの特徴をスコア化し,あらかじめ設定された閾値を超えた場合．閾値は利用者が変更できる．
・インテント：特定のキーワード（URL）を含んだ場合
・ホワイトリスト・ブラックリスト：発信者アドレスがリストに存在する場合．利用者が登録・削除を行える．

迷惑メールと判定されたものは，次のアクションを行う．

タグ付け：件名に特定文字を挿入し電子メールを配送する．特定文字は[YU-SPAM-CHK]に設定した．

隔離：電子メールを配送せず，迷惑メール対策サーバ内で保留する．１日１回（15:35 に設定），保留メールのリストを利用者に配送する．利用者はこのリストあるいは対策サーバの Web ページから必要な保留された電子メールの配送を指示し，配送させる．保留された電子メールは，対策サーバのディスクの残量により古い電子メールから自動的に削除される．

拒否：電子メールを配送せず，エラーメールを発信者に返信する．

上記のアクションは利用者が適宜選択でき，これらを組み合わせることもできる．また，利用者は迷惑メール判定のスコアの閾値はアクション毎に個別に設定できる．対策をメディア基盤センターメールサーバに限定したためメールアドレスに含まれるユーザ名毎に利用者が特定でき，利用者認証は LDAP(Lightweight Directory Access Protocol)と連携できる．現時点（2007 年 9 月 23 日現在）の迷惑メール対策利用者を表１に示す．

表１．2007 年 9 月 23 日時点の迷惑メール対策利用者数

教職員総数	2,122 名
学生総数	10,695 名
１日あたり平均メール利用者数	7,200 名
迷惑メール対策登録者	778 名
（うち学生）	78 名
隔離設定者	215 名

2.2. 希望者のみに迷惑メール対策を行う方法

迷惑メール対策希望者は，メディア基盤センターの Web ページより「迷惑メール対策」をクリックし対策ページに進む．対策ページには，対策の概要，登録方法，リスク，および参考情報を掲示している．希望者が登録ページを開き「迷惑メール対策をする」をチェックし登録することで，迷惑メール対策が有効となる．なお，登録ページを開く際にメディア基盤センターのユーザ名とパスワードがたずねられる．

図１の配送サーバの MTA(Mail Transfer Agent)は postfix を利用している．通常，postfix は DNS の MX レコードを検索しメディア基盤センターメールサーバに電子メールを配送する．postfix は，main.cf ファイルのパラメータ transport_maps に指定したファイルにメールアドレスと他メールサーバを登録すると，通常の配送経路ではなく，そのメールアドレスは登録した他メールサーバに配送されるようになる．この仕組みを利用して，迷惑メール対策登録者のみの電子メールを迷惑メール対策サーバに配送している．利用者が迷惑メール対策を登録すると，配送サーバ上の transport_maps に指定したファイルに登録者のメールアドレスと迷惑メール対策サーバのアドレスを自動的に登録するプログラムを開発した．

2.3. 迷惑メール対策導入にあたっての基準

迷惑メール対策を新たに導入するにあたり、希望者のみに迷惑メール対策を適応することから、次の基準を定めた．特に，以下の(1)～(4)を必須であると考えた．

(１) 利用者が迷惑メール対策の可否を選択できるか？希望しない者には対策を実施せず，希望者にのみ迷惑メール対策を実施するため，標準では対策を行わず，希望すれば対策が開始される仕組みが必要である．

(２) 利用者が対策方法(タグ付け，隔離，拒否)を選択で

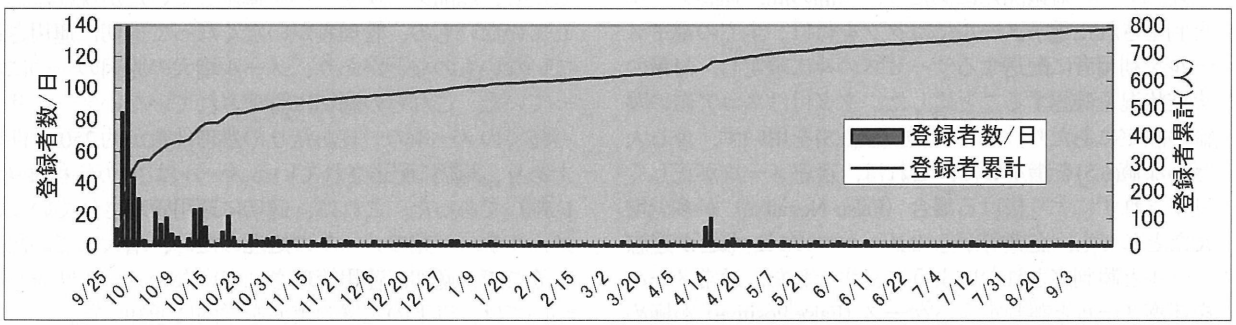

図２　迷惑メール利用者数の推移 2006/2/25～
2006/9/26 タグ付サービス開始　全構成員にメールで通知、2007/4/12 隔離サービス開始　全構成員にメールで通知

き，さらに調整できるか？許容リスクは利用者の考え方や通信している電子メールの内容によって異なるので，リスクの調整が利用者毎に設定できなければならない．安全に迷惑メール対策をおこなうためには，全メールを配送する，つまり，タグ付け機能のみが利用可能であり，隔離，拒否は無効にできる必要がある．

(3) メディア基盤センターの LDAP 認証と連携できるか？利用者に選択・設定してもらうためには利用者認証が必須である．認証が個別なものであると，別途認証の管理業務及び ID パスワードが発生することになり，管理者・利用者の両者にとって運用を大変困難にする．認証は既存のものと共通にしなければならない．

(4) 迷惑メールのパターンファイルを定期的に自動で更新できるか？管理者が介在しなくても更新できる仕組みが必要である．

(5) 迷惑メール対策の精度が優れているか？

(6) メディア基盤センターメールサーバ全利用者の 1/3 の約 5000 人が利用可能であるか？

(7) 機器の障害時，速やかに復旧できるか？

(8) 導入時の初期経費及び後年度のパターンファイル更新経費は支払い可能か？

導入を検討した機器は（1）以外の他の条件を満たしていた。経費的に導入可能なものと、明らかに高額なものがあった。いずれも，（1）が満たせないため，対策を希望した者のメールに対してのみ迷惑メール対策を行うことで，対策利用者の絶対数を少なくすることができ，導入のための調整が容易になる。全メールアドレス登録者数で機器を選択する場合、導入した機器の 1 ランク上の機器を導入しなければならなかった．利用者数が少なくなったことで、最低ランクの機器を導入することでよく、対策機器等の導入経費やライセンス料の負担が軽減された。

2.4. 迷惑メール対策の効果

2006 年 9 月 26 日から迷惑メール対策を開始した。開始に先立って，事前に各種委員会において，迷惑メール対策開始に関する報告を行ったが，利用希望者のみのサービスであるため，異論はなく，容易に了承が得られた．

迷惑メール対策開始にあたり，当面の間，迷惑メールと判定された電子メールにはタグを付け，全ての電子メールを利用者に配送するサービスのみに限定し，対策の実施状況を確認することにした．タグ付けスコア値の閾値の設定にあたり，メーカ推奨値(3.5)を用いず，少し大きめな値(6.5)を選定した，これは，迷惑メールが正しく判定されずにすり抜ける場合（False Negative）が多少増えたとしても，企業等からのメールマガジンなどが迷惑メールと誤判定されないように、すなわち，通常メールを迷惑メールと誤判定するケース（False Positive）が極めて少なくなるように設定した．

幾人かの対策利用者の状況について，2007 年 10 月 17 日までに寄せられた報告・要望を以下に示す．

報告

① 振分けされている電子メールは明らかに迷惑メールばかりで問題ない．
② 多少のリスクがあっても，迷惑メールは見たくない．
③ 公開アドレスの場合，タグ付で 758 件，その他の SPAM で 48 件，非公開アドレスの場合，タグ付で 0 件，その他で 0 件の状況である．
④ SPAM メール 201 通の中で，11 件がそのまま通過した．正常なものを SPAM と判定されたものはない．
⑤ 企業からのメールマガジンがスパムと判定された．
⑥ Web メールで「IMAP サーバとの接続が切断されました.」とメッセージが出て固まった．
⑦ メーラの迷惑メール対策機能と組み合わせれば，迷惑メールをほぼ完全に駆除できている．

要望

① タグ付けするのではなく，拒否して欲しい．
② ブラックリストに登録して欲しい．
③ 学内からの電子メールは対策しないでほしい．

おおむね好意的な報告・要望が多く、対策に否定的なものはなかった。報告・要望については，予想していたとおり，利用者毎に迷惑メール対策に対する考え方が異なっていることが分かる．要望から，利用者がタグ付け以外の隔離，拒否サービスの設定，スコア値の閾値の変更，利用者毎にホワイトリスト・ブラックリストを設定等の機能の提供を希望している．迷惑メール対策に登録した利用者の推移を図２に示す．

前述の報告・要望のとおり，隔離サービスや利用者による設定変更サービスが必要であることから，2007 年 4 月 12 日より隔離サービスの提供を開始した．隔離サービスを提供してから，対策利用者がさらに増加した．

2.5. 学内メールサーバへの対応

迷惑メール対策はメディア基盤センター宛てのメールに対して対策を行ってきた。一方、他部局のメールサーバについては、Open Relay 防止及びウイルス対策については、以前より実施してきているほかは、管理できていない状況が続いていた。全学のメール環境を統一的に運用・管理するため、他部局のメールサーバからメディア基盤センターのメールサーバに移行していただく措置を実施し、多くの他部局メールサーバは移行してきている。しかし、以前メールサーバを運用していたが現在は運用していないもの、管理者がいなくなって適切に運用されていないものなどがあり、メール増大の原因の一つになっていた。これらの適切に管理されていないメールサーバ宛てのメールの一日あたりの処理件数が約 250 万件以上あり、実際に配送されているメールは 30 万件程度（約 1 割）であった。これは、適切に運用管理されていないメールサーバ宛のメールの処理のため、増大していた。

そこで、適切に運用管理されていないメールサーバについては、以下の処置の実施を学内に通知した。

(1)メールの受信を行わない措置を 2007 年 6 月 1 日より実施することと．

(2)今後メールサーバを設置する場合は、センター長の承

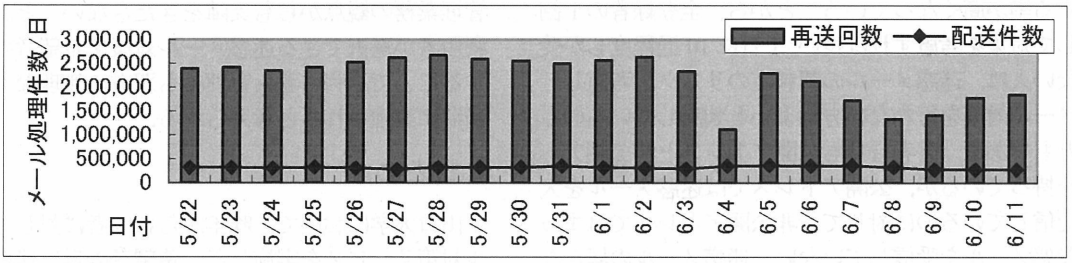

図3　適切に運用・管理されているメールサーバのみに受信を限定する措置の実施日前後の1日あたりのメールの処理件数の推移

認を必要とすること.

適切に運用・管理されていないメールサーバとは、「一定期間（1ヶ月間）連続して、メールの受信を行っていないサーバ」とした。逆に言うと適切に運用管理されているメールサーバは一定期間メールを1通でも受け取っていれば良い。ただし、当初は一定期間として、さかのぼって4月1日～5月31日の2ヶ月間とした。

この期間のメール配送サーバのログを解析することで、適切に運用管理されているサーバとそうでないサーバを調査分析した。適切に運用管理されているサーバは 63台、そうでないサーバは289台であった。適切に運用管理されているサーバについてのみ、学外からのメールを受信可能とする措置を、6月3日より講じた。この措置を実施後、一日当たりのメールの処理件数はおおむね50～70%減少した。措置を実施した前後のメールの処理件数を図3に示す。この措置で、メールの処理件数は減数できたが、さらに、減少させる必要がある。

3. 評価・議論

今回，希望者に対してのみ迷惑メール対策サービスを提供した．図4は2007年9月21日の1日中に一人当たり受信する電子メール数に対する利用者数を示す．他の日も同様な傾向を示している．この日の電子メール利用者数は6,269名であり、メールアドレス登録者数(15,034名)の42%で、全配送電子メール数は139,918通であった．この日10通未満の電子メールを受信する人は4,323名とメール受信者の69%で，迷惑メール対策を希望した人は2%ときわめて少ない。10～19通受信した人は525名と約8%で、迷惑メール対策を希望した人は14%と少ない。

多くの人が1日に10通程度しか受信しておらず、迷惑メール対策を必要としていないことが分かる．1日に20通以上のメールを受信している人は1,421名であり、メールアドレス登録者数に対して9%に留まっているにかかわらず、迷惑メール対策の希望者は41%以上になる。特に，1日辺りメールの受信量の多い利用者ほど対策を

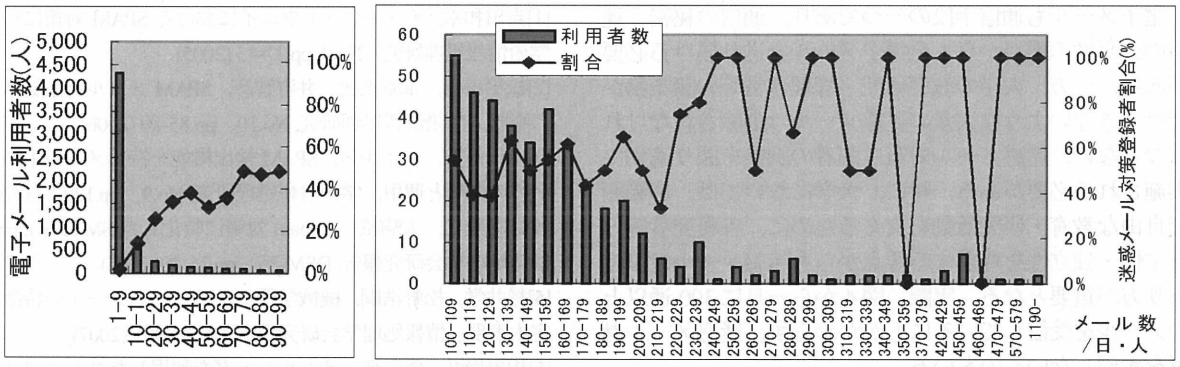

図4　1日に受信するメール数に対する利用者数と迷惑メール対策登録者数(2007/9/21)
1日100通以上受信する利用者は極端に少ないので，右の図で電子メール利用者総数のスケールを変えて表示している

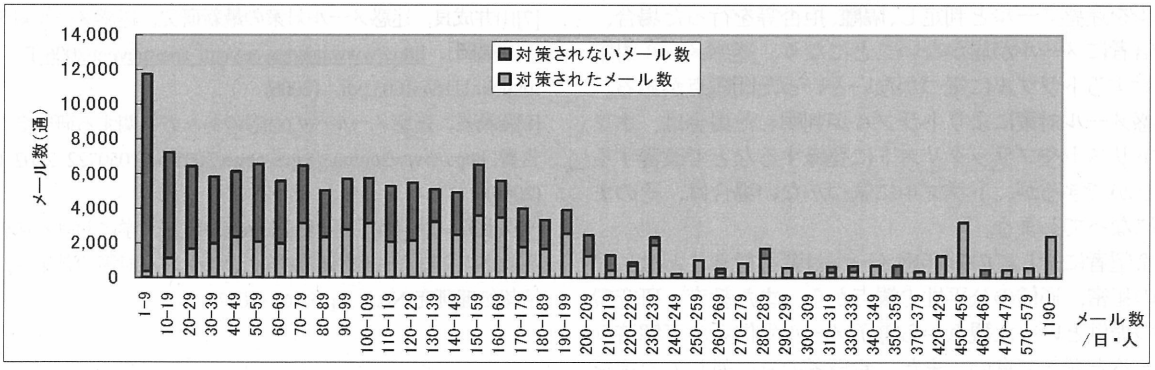

図5　1日に受信するメール数に対する対策されたメールとされないメール総数(2007/6/1)

希望する率が高くなっていることから、全登録者の1割に対して対策を考慮すれば良い。1日に10通程度しか受信しない人は，迷惑メールの誤判定のリスクを考慮し，迷惑メール対策を行わない方がよいと判断しているのももっともである．著者自身も公開アドレスと非公開アドレスを持っているが，公開アドレスでは迷惑メールを大量に受信しているのに対して，非公開アドレスではまったく迷惑メールを受信していない．迷惑メールの届かないメールアドレスがたくさんあることが予測される．

1日に受信する電子メールが10通を越えると，利用者数は極端に少なくなるが，図5に示すように電子メール総数はあまり変わらない．少数の利用者が大量に電子メールを受信していることが分かる．また，迷惑メール対策された電子メールの量も増加していることがわかる．迷惑メール対策を希望した利用者数は，全発行メールアドレスの 9%であるが，迷惑メール対策された電子メールは全受信電子メールの約45%におよんでいる．迷惑メールで困っている人は，大量に電子メールを受信する人であり，全メール利用者数に比べてそれほど多くないが，その少数の利用者が多くの電子メールを受信していることがわかる．

前述のとおり，一律な迷惑メール対策を適用することは，漏れなく対策が実施できる反面，誤判定によるリスクを許容できない人や電子メールの受信量が少ない人の反対を受けるのはもっともなことだと考えられる．1日に大量の電子メールを受信する少数の人に対して，利用者が選択できる対策を提供することで，全体としても十分効果を挙げることができることがわかる．

電子メールも通信手段の一つであり，通信の秘密，通信の公平性の観点からも全電子メールを送り届ける必要がある．一方，大学の教育研究・管理運営等の諸業務が遂行できないような大量の迷惑メールは削除されなければならない．迷惑メール対策は両者の調整を図り適切に実施される必要がある．特に，大学においては，広範囲で自由な教育・研究活動を支えるために，各研究者等の自主性・独立性を尊重する観点からも迷惑メール対策のあり方が重要となる．実際、図4から一日に300通以上のメールを受信しているにもかかわらず、迷惑メール対策を希望しないものもいる。

全構成員に迷惑メール対策を一律に実施した場合，教育・研究活動に支障をきたす恐れがある．特に、通常メールを迷惑メールと判定し、隔離、拒否等を行った場合、受信者にメールが届かないことになり、迷惑メール対策に対するトラブルに気づかないといった問題点がある。迷惑メール対策によりトラブルが判明した場合は、ホワイトリストやブラックリストに登録するなどで改善することができるが、トラブルに気づかない場合は、そのままになってしまう。

希望者に対してのみ迷惑メール対策を行うことは，通信の秘密，通信の公平性の観点から，また教育・研究環境の提供といった観点から電子メール受信者の了解済みであると考えて良い．また，希望者のみに対して対策を実施しても十分対策の効果が上がることが確認できた．管理業務の観点からも支障をきたさないことが分かる．利用者が選択できる迷惑メール対策を希望者のみに実施することで，利用者も管理者も双方に無理なく，対策が適切に実施されると考えられる．

4. まとめ

山口大学において，昨年から希望者に対して迷惑メール対策サービスを実施した．希望者のみに迷惑メール対策を限定することで，導入に対しての反対がなく，また、コストの増大もなく、スムーズに対策が導入できた．導入当初は，希望者が選択すると迷惑メールにタグ付けし，全ての迷惑メールを配送するよう安全性を重視した．本年度から，希望者は，誤判定によるリスクを許容し，スコア閾値，ホワイトリスト，ブラックリストなどの調整を行い，タグ付け，隔離，拒否などの迷惑メールに対するアクション等も調整している．これらの作業を利用者自身が行うことで，電子メールシステム管理者の負担はサーバ機器の管理以外には発生していない．

今回の事例では，迷惑メール対策登録者がそれほど多くなかったにもかかわらず，電子メールシステムで扱う多くの電子メールに対して迷惑メール対策が十分なされていた．全構成員に対して迷惑メール対策をした場合に比べ、利用者数がわずかであるため、利用者に対するライセンス、システム性能等のコストを大幅に削減することができた．希望者に対策を限定することで，全体として十分な効果が得られたと言えよう．

文献

[1]吉田和幸，メールゲートウェイにおける SPAM 対策について，学術情報処理研究，No.9, pp.37-43 (2005)

[2]松平卓也，車庫正樹，井町智彦，SPAM メール対策システムの現状，学術情報処理研究, No.10，pp.85-89 (2006)

[3]本田修啓，ウイルス，SPAM 検出機能を持つメール中継システムの構築と運用，学術情報処理研究, No.9，pp.129-133 (2006)

[4]広瀬雄二，大駒誠一，spam 対策に特化した SMTP wrapper，情報処理学会研究報告, DSM-35，pp.25-30 (2006)

[5]杉井学，松野浩嗣，機械学習によるスパムメールの特徴の決定木表現，情報処理学会研究報告, DPS-130，(2007)

[6]相馬崇弘，南弘征，メールヘッダを利用したスパムフィルタとその結果について，全国共同利用情報基盤センター研究開発論文集，No.28, pp.15-20

[7]山井成良，迷惑メール対策の最新研究，迷惑メール対策セミナ［福岡］，http://www.iajapan.org/anti_spam/event/2006/Tfukuoka1115/pdf/03.pdf，(2006)

[8]総務省，迷惑メールへの対応のあり方に関する研究会最終報告書, http://www.soumu.go.jp/s-news/2005/pdf/ 050722_2_02_00.pdf, (2005)

[9]久長穣，杉井学，長篤志，三池秀敏，大学における迷惑メール対応のあり方～利用者毎のオンデマンド対策の効果～，学術情報処理研究, No.11, pp.55-62 (2007)