SMTP セッションフィルタとグレイリストを併用した迷惑メール対策

陳 春祥[†] 佐々木 宣介[†] 田中 稔次朗[†]

本論文では，迷惑メールのヘッダおよびシステムに記録されたウィルスメールのヘッダに対する分析を行い，正常なメールとウィルスメールおよび迷惑メールについて接続してきたメールクライアントの振舞いの違いを明らかにした．この特徴的な振舞いの違いを利用し，ウィルスおよび迷惑メールの本文を受信せずにそのメールを拒否する対策を考案し，SMTP セッションフィルタおよびグレイリスト方式を用いていくつかの対策をメールサーバに実装して実験を行った．同時にグレイリスト方式により生じるメール受信の遅延を改善するための対策の実装も行った．対策後のウィルスおよび迷惑メールに対するブロック率はそれぞれ平均 97%と 91%であった．

Using SMTP Session Filtering and Greylisting to Counter Spam Mail

Chun-Xiang Chen,[†] Nobusuke Sasaki[†] and Toshijiro Tanaka[†]

In this paper, we analyzed the feature of the virus and illegitimate mail header. The analysis results show that the difference between the legitimate and illegitimate mails (say spam mail) is evident. Based on the analysis results, we elaborately designed a mail SMTP session filtering and a greylisting scheme to counter virus and spam mails. The scheme is expressed concretely as several rules. We implemented the rules with Postfix at mail server side. The experiment results show that the countermeasure we have presented is quite powerful, and the virus mail of 97% and spam mail of 91% have been rejected without receiving the contents of the mail.

1. はじめに

インターネットの急速な普及にともない，電子メールをはじめネットワークを介した情報のやりとりが日常生活にも欠かせない存在になってきた．一方，電子メールは通常の郵便と比較すると，送信する側の費用的負担が小さく，労力もかからないため，受信側にとってはまったく不用であるにもかかわらず，一方的に送られてくる宣伝などのメール（以下，迷惑メールと呼ぶ）が後を絶たない[1)]．さらに電子メールを媒体としたコンピュータウィルスにより無差別に送られてくるウィルス付きのメール（以下，ウィルスメールと呼ぶ）も含め，ユーザにとって不用もしくは有害なメールが急増している[2)]．このような状況の中，何らかの対策を講じなければ，目を通さなくてはならない必要なメールが，大量に送られてくる迷惑メールに埋もれて見落とされてしまう状況になり，電子メールによる円滑なコミュニケーションの障害となってしまう．

本論文では，このような迷惑メールおよびウィルスメールについて，実際に届いたメールのヘッダ情報やメール送受信時の挙動を分析することにより，これらのメールの送信手口を探り，ある程度の規模の組織における公式メールサーバにおいて，安定的に運用が可能となるよう対策方法を検討した．そして，実験用システムを構築して実装実験を行い，実験結果により対策の有効性を示すとともに，我々の大学の公式メールサーバに実装を行った際の運用のノウハウについて述べる☆．

本論文の構成は以下のとおりである．まず，2 章で迷惑メール対策の動向について述べ，3 および 4 章でそれぞれ迷惑メールの特徴および対策ルールについて論じる．5 章では具体的な実装方法について述べる．6 章では実験結果を示し，考察を行う．最後の章で結論を述べる．

† 県立広島大学経営情報学部
Faculty of Management and Information Systems, Prefectural University of Hiroshima

☆ 筆者らが所属していた広島県立大学は 2005 年 4 月に県立広島大学に統合され，メールシステムを含むネットワークシステムも新システムに更新された．本論文は更新前の広島県立大学ネットワークのシステムにおいて行った対策とその結果の分析を報告するものである．なお，更新後の新ネットワークシステムにおいても，現在同様の対策が実施されている．

2. 迷惑メール対策の動向

現在迷惑メールは，さまざまな手段で取得したメールアドレスのデータベースを利用して，自動化されたシステムで大量に送信されている．迷惑メールにおいては送信元の情報が詐称されている場合が非常に多いことも特徴である．また，ランダムに宛て先を生成し，メールを大量に送りつけるケースもある．ランダムに作成された実在しない宛て先は，結局受信側でさまざまな形でシステムエラーメール[1]を引き起こす．極端な場合，これらの迷惑メールやシステムエラーメールの処理でシステムに対する負荷が増大し，メール配送の遅延や障害をもたらすこともある．

本章では，これまでの迷惑メール対策および最近の対策動向について述べる．

2.1 従来の SMTP セッションフィルタリング

電子メールの配送は SMTP（Simple Mail Transfer Protocol）[7] という規約に基づいてやりとりされる．メールの本文を受信する前に送信サーバと受信サーバのホスト情報や送信元や送信先などの情報が交換される（この段階を SMTP セッションという）．受信サーバでは SMTP セッションで得られた情報の内容によって，そのメールを拒否することが可能である．たとえば，いわゆるオープンリレー（Open Relay）を許しているメールサーバや，迷惑メールの送信に利用されているメールサーバを監視する組織があり，これらの組織が提供しているデータベースがある[3)~6)]（本論文ではこれらのデータベースをオープンブラックリスト（OBL）と称する）．この OBL の情報を参照して，オープンブラックリストに登録されているサーバからの送信であれば，メール本文の受信を拒否するといった動作である．このほかにも，SMTP セッションの段階で送信元情報が明らかに詐称されていることが分かる場合に受信拒否を行うなどの対策を併用することも可能である．

2.2 コンテンツフィルタリング

あるメールが迷惑メールであるかという判断は，そのメールの受信者によって基準が異なることもあり，ユーザ側でのキーワード指定，あるいは学習によるメールコンテンツフィルタリングという対策が講じられており，クライアント用の製品も発売されている．最近ではベイズ理論に基づいた学習型コンテンツフィルタリング手法[19]（代表的なものとしては，SpamAssassin[8] と bsfilter[9]）が開発され，効果があると報告されている．

しかし，これらはいったんメールの本文を受信するために，無駄な通信が発生してしまう．そのため，通信量または通信時間に応じた課金システムでは，受信者に余分な費用が発生する．また，実在しないユーザ宛やメールボックスの容量制限などの事情により新たにシステムエラーメールが発生する可能性が高く，メールシステムに負荷を与えるという問題は解消できない．このような理由から，迷惑メール対策としては，いったん完全に受信した後での対策を行うよりは，外部ネットワークとの境界に設置されているメールサーバにアクセスがあった時点で判定を行い，メールの本文を受信せずに拒否することができる方がより望ましいと思われる．

2.3 チャレンジ・レスポンス方式

この方式[1] では，受信側のメールサーバはメールを受け取ったら，すぐに配送せず，一時的に保管しておき，送信者に照会用のメールを返信する（チャレンジ）．照会メールには照会の方法（たとえば，特定の URL への WEB アクセス，画像ファイルに照会用のコードを埋めこむなど）が書かれる．送信者は照会メールを参照して返信する（レスポンス）．照会方法は，メール自動送信プログラムなどが内容を参照して機械的に自動返信することが難しい方法が利用される．

この方式においては，個別にレスポンスが必要なので，大量に送信する迷惑メール業者には，多大なコストがかかるようになる．しかし一方で，正常なメール送信者でもレスポンスを強いられる．さらに送信元が詐称されている迷惑メールの場合は，チャレンジメールが関係のない第 3 者に送られ，間接的な迷惑メールが発生してしまう．

2.4 送信サーバ認証方式

この方式では，何らかの形で送信元メールサーバをあらかじめドメインネームシステム（DNS）にメール送信が可能なサーバとして登録し，その情報を利用して受信を許可するかどうかを決定する方式である．たとえば，Sender ID（Microsoft(R) の Caller ID と米 POBOX 社の SPF 方式を統合したもの）[10),11)]，米 Yahoo!が提唱した DomainKeys [20),21)] がある．

しかし，この方式は DNS の各ドメインに対して，SenderID，DomainKey のためのデータの追加が必要になる．さらに SenderID 方式においては，メールをそのメール受信者の別のアドレスへ転送したりする際に問題が起きる．また，出張先やホットスポットなどのローミング環境で利用ができないなどの問題がある．

2.5 グレイリスト方式

電子メールの送信において，送信先のメールサーバが何らかの原因で一時的に受信不能な状態であれば，

そのメールを保持して後程（10 分，20 分，30 分など）再送信を試みるという動作をするように推奨されている[7]．しかし，多くの迷惑メールでは，迷惑メール送信者は効率良く高速に大量のメールを送ることを企図しているため，一時エラーとなった宛先については，送信をあきらめて再送信してこない場合が多いという報告がある[12),13)]．これを根拠にグレイリスト方式では初めて送ってきたメールに対して，受信側サーバは一時エラーと返事をし，後程再送信するようにと送信側に伝え，電子メールの規約（RFC2821[7)]）の推奨どおり，一定時間が経過した後に再び送信してきた場合はすぐにそのメールを受信する．送信元サーバの情報は一定期間の間，データベースに登録しておき，その間は同じサーバからのメールは同様にすぐに受信する．この方式には最初のメールの配送は必ず一定時間以上の配送遅延が生じてしまうという問題がある．

2.6 存在しない宛て先への迷惑メール対策

この対策は本来迷惑メールに対するものではないが，迷惑メールは，往々にして総当たりで生成されたアドレス宛に送ってくるために，送信先不明などの理由で大量のシステムエラーメールが発生する可能性があり，それを抑制するものである．メールゲートウェイ[2)]（以下，MG という）を導入している環境では，メールゲートウェイ上でその MG が管轄するすべてのドメインおよびサブドメインのユーザアカウントが参照できるようにしておけば，実在しないユーザ宛のメールは，MG の段階でそのメール本文を受信せず，受信拒否をすることが可能になる[2)]．その結果，存在しないユーザに対するメールは受信自体を拒否することにより，システムエラーメールの発生を抑制することができる．これは，分散システムにおける NIS（Network Information System）や，LDAP（Lightweight Directory Access Protocol）や，Kerberos などの手法を用いれば，メールゲートウェイ上でユーザアカウントの参照を可能にすることができる[2)]．

2.7 ね ら い

ここまでいくつかの対策を述べてきたが，まだ迷惑メールを根絶する決定的な対策はないというのが現状である．迷惑メールのブロック率を上げるために対策の基準を厳しくすると[14),15)]，正常なメールを迷惑メールと誤判定してしまう可能性が上がる．また認証方法を導入すると，正常なメール送信者にもコストをかけてしまう．本論文では，クライアントユーザ側の使い勝手に影響が少ないように可能な限りメールサーバ側で対策を行い，ある程度の規模の組織の公式メールサーバにおいて安定的に運用が可能となるような実装方法を探ってみる．また，メールの内容に関するチェックは基本的に各ユーザの判断で行うべきという観点から，メール本文に対するチェックを行うことは避け，あくまでメール送信の際のサーバ情報，送信時の振舞いなどに焦点を置くこととする．

3. 迷惑メールの特徴

メールの配送は，コストおよび管理の面から，組織内に専用のメールサーバを用意して，ユーザの個々の端末からはいったんそのメールサーバに送信し，それらのメールを一括して配送するのが一般的である☆．またメールのような重要なサービスを担うサーバにおいては，高い信頼性を必要とするため，そのサーバに割り当てられたドメインネームアドレス（FQDN：Fully Qualified Domain Name）からそのサーバの IP アドレスへの検索ができるように，またその逆，IP アドレスから FQDN への検索もできるように，DNS に登録しておくのが一般的である．それに対して利用者の端末については，端末の情報を DNS に登録しない場合が少なくない．

SMTP に基づいてメール本文を送るまでの送信側のクライアント（SMTP クライアント）と受信側のサーバ（SMTP サーバ）のやりとりの手順を簡単にまとめると次のようになる．まず SMTP クライアントから SMTP サーバに接続要求を送り，サーバからの接続許可を受けた後に，3 つのパラメータを送信する．(1) HELO（あるいは EHLO）コマンドを用いてクライアントのホスト名あるいはクライアントのサポートしている機能などが分かるような内容を送る．(2) MAIL FROM コマンドで，実際の送信者アドレスを送る．(3) RCPT TO コマンドで実際の受信者アドレスを送る．

しかし，SMTP の規約ではこれらのパラメータの真偽を確認する手順に関しては定めておらず，あくまでも送信側の自己申告になる．迷惑メール送信業者の場合は，(1)，(2) の送信元に関する内容を偽装するような行動が多く見られる．このような送信元情報の詐称については電子メールを媒体としたウィルスメールにも共通している．送信元が詐称されている場合には，次のような問題も発生する．受信側でウィルスメールや迷惑メールであると判明したり，何らかのエラーが発生したりして送信元にそのメールを返送するようなこともありうるが，この場合に，送信元の詐称により，

☆ ユーザの端末から直接に受信者側の受信サーバに送ることもありうるが，加入プロバイダあるいは自組織のメールサーバを経由した送信が一般的である．

実際に送信していない第 3 者に返すことになり間接的な迷惑メールになってしまう．その詐称された送信元も存在しないメールアドレスであれば，さらなるエラーメールが発生する．

筆者宛に 2002 年 1 月から 2004 年 6 月までの間に届いた迷惑メール（3,102 通），正常なメール（2,855 通）および本学のウィルスチェックサーバに記録された大量のウィルスメール（3,4431 通）のヘッダ情報に対して解析を行い，これらのメールの特徴を探ってみた．**表 1** にこの解析の結果を示す．ただし，A，B，C，D の複数の条件を同時に満たすメールもあるので，A，B，C，D 間の重複がある．また，今回の解析で使用した OBL は，文献 3) および 4)（オープンプロキシーなども含む）である．ダイナミック IP アドレスのリストとして使用したのは文献 6) の dul.dnsbl.sorbs.net である．これらのデータベースに該当の対象がすべて収集されることは困難であること，リストが実態と一致しないこともあるため，解析結果の数値は厳密なものとはいえず，一種の目安であるが，迷惑メール，ウィルスメールおよび正常なメール間の特徴を示すものと考えてよい．

表 1 から迷惑メールおよびウィルスメールの SMTP セッション時の振舞いが正常なメールとは明らかに違った傾向を持っていることが分かる．迷惑メールの送信者は送信元の情報を隠して素早く大量にメールを送信することを狙っているため，このような違いとなって現れると考えられる．また，ダイナミック IP アドレスのクライアントから送信されたメールはウィルスメールと迷惑メールであることが判明した．

これらの分析結果からは，A〜D にあてはまるメールは大部分が迷惑メールまたはウィルスメールであると考えられ，これらの傾向の違いを利用した SMTP セッションフィルタにより，迷惑メール対策を行うことが可能であることが分かった．

表 1 ウィルスおよび迷惑メールヘッダの統計 (%)
Table 1 Statistics of spam and virus mail header (%).

	A	B	C	D	E
迷惑メールの場合	24.11	39.31	55.68	13.59	20.20
正常メールの場合	0.60	1.40	0	0	98.40
ウィルスメールの場合	59.76	27.79	47.27	11.50	9.63

A ：HELO コマンドの内容が，RFC[7] の必須事項に従っていないメール（たとえば，送信先のドメイン名や IP アドレスを HELO の内容とする場合や，存在しないドメイン名を MAIL FROM の内容として送ってくる場合など）の割合．
B ：送信元サーバの FQDN の登録がない割合．
C ：オープンブラックリストに登録されているサーバから送信された割合．
D ：ダイナミック IP アドレスのクライアントから直接送信されてきた割合．
E ：A，B，C，D のいずれの条件も満たさないメールの割合．

次にこれらのルールをフィルタリングに用いることを検討した．まず C と D にあてはまるメールについては，収集した範囲のメールではすべて迷惑メール，ウィルスメールであり，これらのメールは不要なメールとして拒否してもよい．A については，正常なメールの中にもごく一部に A に分類されるものがあるが，A は RFC で「必須」としている条件に従っていないものであることから，拒否ルールに加えてよいと考えられる．B も，拒否するルールとして利用可能と考えられるが，A，C，D に比べると正常なメールがここに含まれる割合が高くなっている．そのため，このルールの適用は慎重に行う必要がある．

また，正常なメールはほぼすべて E に分類されるが，迷惑メールとウィルスメールも相当の割合で E に分類されるものが残る．したがって，E に分類されるメールに対しても対策を行うためには，ヘッダ情報を利用しない対策を適用する必要がある．この部分の対策をグレイリスト方式に任せることとした．

適用の順番なども含めた詳細について，次章で述べる．

4. 対策ルール

実装対象のメールシステムの構成を**図 1** に示す．図の「内部メールサーバ」は，複数の部局がメールサーバを運用しているようなシステム構成における内部メールサーバ群と考えてもよい．迷惑メール対策の実装対象サーバは外部ネットワークとの境界に設置されている MG である．メール利用者数は約千名で，メールの配送経路は次のとおりである．

- 外部からのメールは，MG が受け取り，内部ウィルスチェックサーバへ送り，ウィルスの有無をチェックしてから内部メールサーバへ配送される．
- 内部ユーザからのメールはウィルスチェックサーバが受け取り，ウィルスチェック後に，外部宛のメールは MG に送信し外部へ送出する．内部宛のメールは内部メールサーバへ送信する．内部メールサーバはウィルスチェックサーバからのメールし

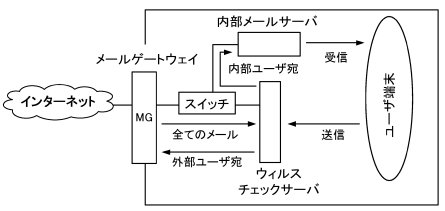

図 1 メールサーバの構成
Fig. 1 Configuration of mail servers.

か受け取らないように設定する．以上のようにすべてのメールは必ずウィルスチェックを受ける☆．

MG 上での迷惑メール対策実装は，SMTP セッションフィルタリングとグレイリストを併用した実装となる．実装したルールは以下のとおりである．

(1) MG では，サーバ内部にはユーザアカウントのデータを持たないが，内部ユーザアカウントを参照できるようにして，実在しない内部ユーザ宛のメールの受信はすべて拒否する[2]．

(2) 接続してきたメールクライアントの挙動が明らかにメール送受信に関する RFC に従っていない場合，その接続を拒否する．不正な例の一例としては，HELO の内容として，メール送信先である本学のメールサーバのアドレスとドメインや，または存在しないドメイン名を送信することがあげられる．

(3) オープンブラックリスト（OBL）を利用して，OBL に登録されているクライアントからの接続を拒否する．

(4) ダイナミック IP アドレスのメールクライアントからの直接接続は拒否する．ほとんどのインターネットサービスプロバイダは加入者に対して電子メール配信のサービスを提供しているため，このルールを適用しても正規なユーザにはおおむね問題がないと考えられる[6),15)]．ただし，固定 IP アドレスを持たない機器から，正規のメールが送信されるケースがわずかではあるが存在するため，この制限を使用せずに，次のグレイリスト方式にすべて任せることも考えられる．

(5) グレイリスト方式[12)] を導入する．初めて送ってくるメールに対しては一時エラーと返事をし，一定時間が経過した後に再送信してきた場合はそのメールを受信する．また，一度正常に受信した送信元からのメールは，一定期間の間は，信頼できる送信元として次回以降の送信の際にはすぐに受信する．ただし，グレイリストによって初めてのメールの際に受信に遅延が生じてしまうという欠点があるため，それを改善するために，SMTP セッションの情報をもとに信頼できると判断できる送信元からは，一時エラーとせずにただちに受信する（「信頼できるホスト」の判定条件については後述）．

(6) 無条件で受信する送信元，受信先，無条件で拒否する送信元などのリスト（いわゆる，ホワイトリスト，ブラックリスト），を手動で作成してチェックを行う．

☆ 外部宛のメールはウィルスチェックサーバから直接 MG に送られるが，例外は，内部メールサーバで運用されているメーリングリストから外部アドレスへのメール送信で，ウィルスチェックサーバからいったん内部メールサーバへ届いた後，メーリングリストによって外部アドレス宛に送信されるメールは内部メールサーバから直接 MG に送られる．

5. 実　　装

提案した対策ルール (1)〜(6) を図 1 の MG において実装を行った．MTA（Mail Transfer Agent）として postfix-2.1.4[16)] を利用した．

ルール (1) は MG を内部のユーザアカウント管理サーバと連携させることで，ユーザが実在しているかのチェックが可能とした．ユーザから MG へのリモートアクセスなどの直接利用はないので，ユーザアカウント以外の情報（パスワードやホームディレクトリなど）は MG から参照できないようにセキュリティの向上に配慮する．ルール (2)〜(4) および (6) は，Postfix の SMTP セッションチェック機能を利用した[18)]．ルール (5) は外部ポリシーサーバを呼び出す方式で実現した．

Postfix での実装（設定ファイル）の詳細を**表 2** に示す．これらの記述が上から順に実行され，それぞれのルール適用の順番もこの設定の記述どおりの順番となる．対策ルールの対応関係は以下のとおりである．2 行は自ネットワーク（つまり本学の内部ネットワーク）からなら，メールのリレーなどをすべて許可する．3〜5，8 行がルール (2) の実装に該当する．ルール (2) では SMTP セッション中の HELO，MAIL FROM および RCPT TO の 3 つのパラメータをチェックする．各行の先頭のパラメータの意味の詳細および受け取る引数は文献 18) を参照されたい．8 行では HELO の内容に関して明示的なブラックリストかホワイトリスト

表 2 ルールの実装
Table 2 Implemented rules.

smtpd_recipient_restrictions =	···1
permit_mynetworks,	···2
reject_non_fqdn_sender,	···3
reject_unknown_sender_domain,	···4
reject_unauth_destination,	···5
check_client_access hash:	
/etc/postfix/client_WB_lists,	···6
check_recipient_access hash:	
/etc/postfix/recipient_whitelists,	···7
check_helo_access regexp:	
/etc/postfix/helo_checks_regexp,	···8
reject_rbl_client relays.ordb.org,	···9
reject_rbl_client list.dsbl.org,	···10
reject_rbl_client sbl.spamhaus.org,	···11
reject_rbl_client dul.dnsbl.sorbs.net,	···12
check_policy_service inet:127.0.0.1:10023,	···13
permit	···14

を正規表現で登録する．たとえば本学のドメイン名やIP アドレスを HELO の内容として送ってくるメールは，RFC の必須事項に従っておらず明らかに怪しいので，helo_checks_regexp に “hiroshima-pu.ac.jp REJECT You’re lying about who you are.” と登録しておき，明示的に拒否および拒否の理由を伝える．5行目は不正中継を禁止するための設定であり，Postfix のデフォルト設定ではこの行が有効になっているが，*smtpd_recipient_restrictions* を用いて明示的に設定する場合には，上の行から順番にチェックを行い，条件にあてはまった行でチェックを終了してしまうので，*reject_unauth_destination* よりも先の行で意図しないオープンリレーを許可してしまうことのないよう，適用する順番に注意が必要である．6 および 7 行目はルール (6) の設定に該当する．9〜11 行目はそれぞれルール (3) の実装になり，12 行はルール (4) の実装となる．13 行目はルール (5) のグレイリスト方式の実装となる．すべてのチェックをパスした接続は 14 行の時点で許可される．

13 行のグレイリストの実装については，Postgrey [17]（バージョン 1.16）というポリシーサーバを用いて実装を行ったが，グレイリストによる遅延を改善するため，次の「信頼できる」条件：

- 送信ホストが FQDN を持ち，なおかつ FQDN の正引きの結果をさらに逆引すると元の FQDN と一致すること，
- HELO の内容が FQDN と一致するか，送信者側の属性やサポートする機能を示すものか，

をすべて満たす場合にはグレイリスト方式を適用せず，すぐに次の 14 行目により受信される．ただし，Postfix および Postgrey のオリジナルの機能だけではこの遅延改善の判定を実現することができないため，Postgrey のソースコードを修正し，機能拡張を行った．なお，グレイリストの処理の中でもホワイトリスト，ブラックリストを用意して，特定の送信元からの送信を制御できるようになっている．Postgrey 付属の postgrey_whitelist_recipients および postgrey_whitelist_clients という 2 つのホワイトリスト以外に，postgrey_greylist_clients ファイルを追加した．このファイルの記述書式は postgrey_whitelist_clients と同じである．このファイルに登録したクライアントは上記の「信頼できる」ホストとせず，グレイリストにより処理される．また，グレイリストの設定としては，一時エラーの後，300 秒以上間を置いて再送信してきたメールを受信し，正常に受信した送信元から 3 日間はただちに受け取ることとした．

6. 実験結果および考察

前述の (1)〜(6) の対策ルールを実装し，試験的な運用（2004 年 8 月〜9 月）を行い，その効果を確認してから，本学情報教育センター運営委員会の承認を経て 10 月から正式な対策ポリシとして運用を始めた．本章では実験の結果，分析および考察について述べる．

6.1 実験結果

本実験では迷惑メール対策が主な対象であるが，この対策は一部のウィルスメールにも有効である．そこで対策適用前後の迷惑メール，ウィルスメールおよびシステムエラーメールの変化に着目し分析を行った．対策適用前の 6 月，7 月と適用後の 8，9，10 月の比較を**図 2**，**図 3**，**図 4** に示す．図 2 は，筆者らの個人宛に届いた迷惑メールの数を集計したものである．図 3 は，本学の内部ウィルスチェックサーバが検知したウィルスメールの数で，全ユーザ宛の総数の集計である．図 4 はシステム管理者宛に届いたシステムエラーメールの集計である．ただし図 4 では，受信者のメールボックスの容量制限によるシステムエラーの数は計上していない．このエラーメールは，本学内部の

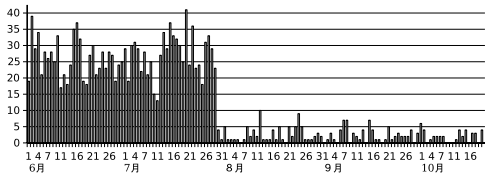

図 2 迷惑メール数の推移（2004 年 6 月〜10 月，1 日単位）
Fig. 2 The number of spam mails received per day.

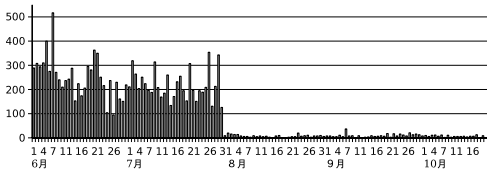

図 3 ウィルスメール数の推移（2004 年 6 月〜10 月，1 日単位）
Fig. 3 The number of virus mails received per day.

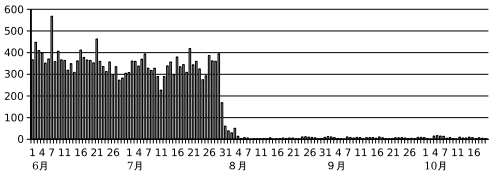

図 4 システムエラーメール数の推移（2004 年 6 月〜10 月，1 日単位）
Fig. 4 The number of system error mails per day.

表 3 実装方式の各ルールによるメールブロック率の内訳 (%)
Table 3 The blocking rate of each rule in detail (%).

対策ルール	平均ブロック率
ルール (1)：実在しないユーザ宛	23.9
ルール (2)，(6)：SMTP セッションチェック	17.4
ルール (3)：オープンブラックリスト	28.1
ルール (4)：ダイナミック IP クライアント	7.4
ルール (5)：グレイリスト	23.2

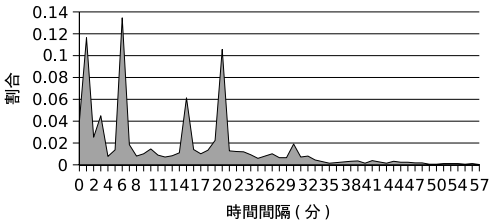

図 5 再送時間間隔の分布
Fig. 5 The ratio and retransmission interval of the mails.

サーバの状態に起因することが明らかなメールであるからである．

これらの図より，対策を開始した 8 月以降では，外部からのメール送信要求に対して，本文の受信前にあらかじめ明らかに疑わしいメールを拒否したため，ウィルスメールおよび迷惑メールが大幅に減少したことが分かる．また，システムエラーメールも同様に大幅に減少している．これは，組織の出入口である MG の段階で存在しないユーザ宛のメールも含む問題のあるメールを拒否したことによって，詐称された送信元（存在しないメールアドレスである場合も多い）に対してエラーメールを送信しようとして，さらなるシステムエラーメールを招くといった問題も結果的に回避できた効果によると考えられる．

本対策においては，メール本文を受信することなく拒否を行っているので，拒否したメールが迷惑メールであるかウィルスメールであるかを正確に知ることが困難である．そこで，対策適用前の迷惑メールとウィルスメールの 1 日の平均受信数と，対策適用後の平均受信数とを比較した．その結果，これらのメールのブロック率は迷惑メールが 91%，ウィルスメールが 97%という結果になった．

次に今回提案した対策ルールのブロック率について解析を行った．まず，どの対策ルールによってブロックされたのか集計を行った．グレイリスト方式を採用していることにより，同一のメールがメールログに複数回記録されることもあるが，同一メールは最終的には 1 件のメールとして数えた．本対策でブロックしたメールのすべてを 100%として，各ルールによるブロック率の内訳を**表 3** に示す．たとえば，OBL によってブロックしたメールはブロックしたすべてのメールのうちの 28.1%であり，グレイリスト方式のブロック率が 23.2%であった．

対策適用後，実際に受信した外部から本学ユーザ宛メールの 1 日あたりの平均数を N_a とし，本対策によってブロックしたメールの数を N_b とすると，外部から本学ユーザ宛のメールに対する平均ブロック率は $\frac{N_b}{N_a+N_b} \times 100\%$ となる．実験データよりこのブロック率が 35.5%であったことが分かった．つまり本学ユーザ宛のメールのうち，3 割強が迷惑メールであるといえる．

次にグレイリスト方式を適用した結果についての分析結果を述べる．グレイリスト方式によって一時エラーで拒否された全メールを 100%として，再送信してこなかった，または 300 秒以内の再送のみで，最終的に受信しなかったのが 62.2%であることが分かった．残りの 37.8%（この部分の数を G_r とする）が 300 秒以上の間隔をおいて再送信され，グレイリストを通過し受信された．再送されて最終的に受信した 37.8%のメールの再送時間間隔の分布を**図 5** に示す．この図から一時エラーを告げられたホストからの再送信はほとんど 1 時間以内に再送してくることが分かった．一部の送信クライアント（特に WEB メールを使用しているサイト）はほとんど待たずに数秒単位で再送してくることがあることも分かった．また，実際に受信したメール（N_a）に対して G_r の割合（$G_r/N_a \times 100\%$）は，実験データから約 4.4%であったことが分かった．つまり今回の実装したグレイリスト方式によって 4.4%のメールに遅延が生じたことが分かった．遅延時間の確率平均は 19 分であった．

6.2 考　　察

今回の実装では Postfix を用いた．Postfix は設定の容易さだけでなく，迷惑メール対策に利用可能なパラメータをたくさん用意していること（以下，UCE 制御パラメータという）[18]，OBL を参照可能なこと，さらに外部ポリシーサーバを連携できることから，今回の提案ルールの実装が容易に可能となった．本節でルールの実装と試験結果について考察する．

6.2.1 UCE 制御パラメータについて

UCE 制御パラメータには強力なものもある．たとえば，reject_invalid_hostname や reject_unknown_hostname，reject_unknown_client，strict_rfc821_envelopes などがある．8 月最初の実験段階では，これらのパラメータの一部を有効にして，たとえば，FQDN の登録されていないホストからのメール送信を拒否するように設定したが，一部の正常なメールサーバでも

これらの制御に引っかかってしまうことが何件かあった．しかし，これらのパラメータを使用しないと，明らかに迷惑メールとウィルスメールも増えてしまった．そこで，一律に拒否することはやめて，SMTP セッション中のパラメータが RFC821 が推奨する書式に従っていないホストや，FQDN の登録のないホストまたホスト名の正引きおよび逆引が一致しないホストについては，グレイリスト方式で対処することにした．その後は，FQDN の登録がないことにより正常なメールをブロックしてしまうようなことがほとんどなくなった．

6.2.2 各ルールのブロック率について

ブロック率の内訳（表 3）は対策ルールの適用される順番に依存しており，順番が変わるとブロック率の内訳も変わる．今回の実装では，実在しないユーザ宛のメールや，SMTP セッションの情報が明らかに怪しいメールなど，拒否すべきことが明らかなものを最初に判断して拒否し，グレイリスト方式は最後に判定に使用するように実装されている．しかし，グレイリスト方式が適用される順番が最後になっているにもかかわらず，ブロック率が 23.2%であり，大きな効果があるといえよう．

6.2.3 OBL の選択について

表 3 に示すように，OBL の使用は大きな効果がある．ただし，OBL はそれが運営されている国（あるいは管理者）の方針，データベースの登録ルールなどによって登録内容が異なることがあるので，参照するときには注意が必要である．また，このような無償のリストはときには使えなくなったり，更新されていなかったり，閉鎖されてしまったりということもあるので，定期的にチェックする必要がある．また，参照する OBL の数が多くなると DNS の検索に時間がかかってしまう．多数の OBL を一気に使用するのではなく，効果の有無を確認しながら加減すべきである．

6.2.4 グレイリストによるメール配送遅延について

1 回目の送信でグレイリストに拒否されたメールの再送時間間隔は，送信元の設定にもよるが，前節の分析では平均 19 分であった．グレイリスト方式では，各種の設定が正常な送信元でも最初の送信がグレイリストによってブロックされて遅延が生じてしまう．そこで我々は「信頼できるホスト」という尺度を導入し，「信頼できるホストなら，一時エラーとせずただちに受信」という遅延改善策を組みこんだ．その結果，受信した全メールに対して，グレイリストによって遅延が生じたメールは受信した全体のメールの 4.4%であった．この結果より，総合的に 91%の迷惑メールをブロックしたうえでメールの遅延を抑えることに一定の効果があったと評価できる．

6.2.5 誤判定について

本対策では多少の判定洩れがあっても，正規のメールを迷惑メールと誤判定することをできるだけ避けるようにしているが，多少の誤判定もある．

ここでは誤判定の事例についてまとめる．

誤判定については，基本的にはユーザからの「メールが届いていない」という問合せに応える形で対応を行った．また，希望するユーザには拒否したメールの一覧の記録を開示し，誤判定がないかチェックをしてもらった．

まず，送信元の問題（たとえば SMTP セッション時の情報が不正である）でブロックされてしまったが，送信元が対応してくれないなどというケースについては，それを救済するホワイトリスト（client_WB_lists）を利用する．このようなケースでの誤判定は 2 件あり，ホワイトリストに登録を行った．次にダイナミック IP アドレスのクライアントからのメールについては，運用中に 1 件の誤判定があった．送信元に対応を依頼したが，ホワイトリストに登録するといった対応も可能である．グレイリストの運用では主に再送してこなかったことが起因でトラブルが 3 件あった．これもグレイリストのホワイトリストに登録することで対応した．

また，ユーザの中には，誤判定が 100%発生しないという技術的な保証がない限り，自分宛のメールはすべて受けたいという要望もありうる．このため受信者ホワイトリスト（recipient_whitelists）を用意した．運用では約千名のユーザのうち，3 名のユーザからの要望があった．

誤判定の問題については，このように手動での登録により，十分対応可能であった．もちろん，利用者から「来るはずのメールが届いていない」などのような問合せがなかったからといって上記で対応した件数以外に誤判定がないとはいいきれないが，拒否した場合は MG の MTA が明確にその旨を送信元に伝えるようにしている．送信元と協力してトラブル解決を行うという方針で臨んだ．

以上の結果から，MG におけるウィルスメールおよび迷惑メール対策として，(1) から (6) の対策ルールは十分に機能したと評価することが適当である．

7. 終わりに

現在，プロバイダや各組織において，迷惑メール対策は大きな課題となっている．迷惑メールに対してさ

まざまな対策方式が提案されているが，正規のメールは拒否しないことと，ウィルスメールおよび迷惑メールは拒否することを両立可能な決定的な方法はいまだにない．対策基準を厳しくすると，正常なメールをブロックしてしまう可能性が高くなる．

本論文では，(1) 接続してきたメールクライアントの挙動を解析して得られた正規メール，ウィルスメールおよび迷惑メールの挙動が異なるという特徴を利用して SMTP セッションフィルタリングを行う，(2) OBL を参照する，(3) グレイリスト方式を適用する，などの対策を併用して，サーバ側でウィルスメールおよび迷惑メールの本文を受信することなく効率良く拒否するような対策を考案し，実装実験を行った．実験の結果から平均 97%のウィルスメールおよび 91%の迷惑メールを削減することができた．また，システムエラーメールの数も大きく低減させることができた．グレイリスト方式には，最初に送信されたメールに遅延が生じるという問題があったが，(4)「信頼できる」挙動と判断できるサーバからは遅延なくメールを受け取る，というルールも併用することにより，遅延（再送）が生じるケースを抑えることを可能とした．遅延が生じたのは，受信したメールに対して 4.4% であった．

ウィルスメールに対しては，多くの組織で専用のウィルス対策ソフトウェアを導入して，メールのチェックを行っているはずであるが，新種のウィルスが出現した場合にはウィルス対策ソフトのデータベース更新が終了するまではウィルスメールがすり抜けてしまう可能性が存在する．今回実装した手法は，データベースによるパターンマッチングによらないウィルスメール対策としても機能するため，専用のウィルス対策ソフトウェアの機能を補完するものとして利用することも可能と考えられる．

もちろん，今回の提案・実装ではブロック率が 91%ということで，完全に迷惑メールをブロックできるわけではないが，これは，ブロック率だけを追及するのではなく，正規のメールはできる限り拒否しないような安定運用を目指した結果である．また，迷惑メール送信業者も，受信側の対策をすり抜けるためにさまざまな手段を講じてくることが想定される．今後は，ブラックリストとホワイトリストのこまめな登録や，どのような挙動のときにグレイリスト方式で対応するかという設定の見直しなどのチューニングを行うことにより，ブロック率をさらに上げることが可能であると考えられる．今後の課題としては継続的に迷惑メールの送信手法やその他の対策方法などに留意し，対策方法を適宜に見直していく必要があると考えられる．

参 考 文 献

1) 岩永　学，田端利広，桜井幸一：チャレンジーレスポンスとベイジアンフィルタリングを併用した迷惑メール対策の提案，情報処理学会論文誌，Vol.45, No.8, pp.1939–1947 (2004).
2) 吉田和幸，矢田哲二ほか：spam メール対策と統合メール管理システムについて，情報処理学会論文誌，Vol.46, No.4, pp.1035–1040 (2005).
3) ORDB. http://www.ordb.org/
4) DSBL. http://dsbl.org/
5) The SPAMHAUS PROJECT. http://www.spamhaus.org/
6) SORBS. http://www.au.sorbs.net/
7) Klensin, J.: RFC 2821, SMTP: Simple Mail Transfer Protocol (Apr. 2001). http://rfc.net/rfc2821.html
8) SpamAssassin. http://spamassassin.apache.org/
9) bsfilter. http://bsfilter.org/
10) 松尾和洋：Web 世界を安全にする試み，情報処理学会会誌，Vol.45, No.9, pp.970–971 (2004).
11) Sender Policy Framework. http://spf.pobox.com/howworks.html
12) greylisting. http://greylisting.org/
13) お馴染さん方式. http://moin.qmail.jp/spam
14) 広瀬雄二，和田啓二：メールサーバーで行うスパム対策，*UNIX USER*, No.11, pp.44–55 (2004).
15) Asami, H.: Study Report of an Anti-spam System with a 99% Block Rate. Available at http://www.bcm.co.jp/site/security/04security09.htm
16) Postfix. http://www.postfix.org/
17) Postgrey. http://isg.ee.ethz.ch/tools/postgrey/
18) Postfix UCE controls. http://www.postfix.org/uce.html
19) Paul Graham: A Plan for Spam (Aug. 2002). http://www.paulgraham.com/spam.html
20) Sendmail: Sendmail and Yahoo! Mail Collaborate to Develop and Deploy DomainKeys. http://www.sendmail.com/company/news/20040224/
21) Yahoo: DomainKeys: Proving and Protecting Email Sender Identity. http://antispam.yahoo.com/domainkeys

(平成 17 年 7 月 8 日受付)
(平成 18 年 2 月 1 日採録)

陳　春祥（正会員）

1994 年大阪大学大学院工学研究科応用物理学専攻博士課程修了．博士（工学）．同年広島市立大学情報科学部助手．1997 年広島県立大学経営学部助教授．2005 年県立広島大学経営情報学部助教授．コンピュータネットワーク，通信システムの性能評価，情報セキュリティ等の研究に興味を持つ．電子情報通信学会，IEEE 各会員．

佐々木宣介（正会員）

1998 年東北大学大学院情報科学研究科博士後期課程修了．博士（情報科学）．同年静岡大学サテライト・ベンチャー・ビジネス・ラボラトリー研究員，2000 年広島県立大学助手，2005 年より県立広島大学講師．人工知能，ゲームプログラミング，情報セキュリティ等の研究に興味を持つ．電子情報通信学会，人工知能学会各会員．

田中稔次朗（正会員）

1976 年大阪大学大学院工学研究科応用物理学専攻博士課程修了．博士（工学）．1977 年鹿児島県立短期大学講師．1978 年助教授．1984 年教授．1997 年広島県立大学経営学部教授．2005 年県立広島大学経営情報学部教授．カオス理論とその工学への応用研究に関心があり，カオスニューラルネットワークによる情報処理の研究に従事．1979〜1980 年カリフォルニア大学サンタバーバラ校客員研究員．1990 年 MBC 賞受賞．日本物理学会，アメリカ物理学会，電子情報通信学会各会員．