Vol.2013-IOT-22 No.8
2013/8/1

岡山大学における電子メールシステムのトラブルと対策

山井 成良[1,a)]　岡山 聖彦[1]　藤原 崇起[1]　大隅 淑弘[1]

概要：
岡山大学では，Gmail を用いた学生用電子メールシステムを 2009 年 4 月から運用している．また，教育・研究用電子計算機システムを更新に伴い，新しい教員用電子メールシステムを 2011 年 4 月から運用している．本稿ではこれらの電子メールシステムの運用方法を説明するとともに，これまでの運用において発生したトラブルのうち，重要なものについて報告する．

キーワード：
電子メール，迷惑メール対策，tempfailing，Gmail

Trouble and Solution of E-mail System in Okayama University

Nariyoshi Yamai[1,a)]　Kiyohiko Okayama[1]　Takaoki Fujiwara[1]　Yoshihiro Ohsumi[1]

Abstract:
Okayama University has been operating student e-mail systems using Gmail since April 2009. As for teachers and staff, we have been operating the new e-mail system along with the renewal of education and reseach computer system since April 2011. In this paper, we introduce how to configure and operate these e-mail systems. In addition, we exlain some issues of e-mail systems we have experienced during their operation.

Keywords: E-mail, anti-spam method, tempfailing，Gmail

1. はじめに

岡山大学（以下，本学）は学生数約 14,000 人，教職員数約 2,600 人，11 学部を擁する，地方大学としては比較的大規模の総合大学である．主要なキャンパスとしては岡山市内の津島キャンパス（医療系を除く学部，情報統括センター，事務局など），鹿田キャンパス（医療系学部，岡山大学病院など），東山キャンパス（教育学部附属学校園），芳賀キャンパス（産学官融合センター），倉敷市の倉敷キャンパス（資源植物科学研究所など），瀬戸内市の牛窓キャンパス（理学部附属臨海実験所），鳥取県三朝町の三朝キャンパス（地球物質科学研究センター，岡山大学病院三朝医療センター）がある．

本学では情報統括センター（以下，当センター）が全構成員に対するオフィシャルな電子メールサービスを提供している．このうち，学生用電子メールサービスについては，現在では Google 社が提供する Gmail に全面移行し，現在に至っている．また，教職員用電子メールサービスについては 2011 年 4 月に教育・研究支援システム（教育研究用電子計算機システム）の更新に伴い，構成や機能が全面的に変更された．これらとは別に事務用電子計算機システムの一部として事務職員用電子メールサービスが提供されている．導入当初は情報企画課が運用していたが，2010 年の当センター発足に伴い当センターが運用している．さらにこれらとは別に，部局や学科，あるいは研究室単位で独立した電子メールサービスが存在する．当センターではこれらのサービスの運用には直接携わらないが，管理者が必ずしも十分な運用スキルを持っているとは限らないため，これらのサービスに対しても当センターができる範囲でのセ

[1] 岡山大学情報統括センター
Center for Information Technology and Management, Okayama University
3-1-1, Tsushima-naka, Kita, Okayama 700–8530, Japan
[a)] yamai@okayama-u.ac.jp

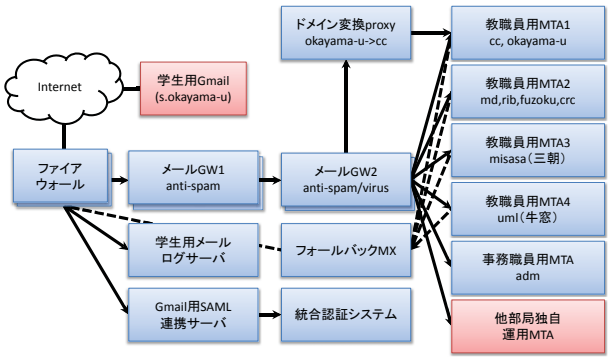

図 1 岡山大学における電子メールシステム構成
Fig. 1 E-mail System Configuration in Okayama University.

キュリティ対策を行う必要がある．

これらの電子メールサービスにおいて，様々な技術的あるいは政策的な要因によりシステムの構成や運用方法に工夫を行っている．本稿では，本学において当センターが管轄している電子メールサービスの運用方法を説明する．また，電子メールサービス運用の過程において様々なトラブルが発生した．本稿ではこれらのうち比較的重大なものとその対策を紹介する．なお，未解決の課題については文献 [1] を参照されたい．

2. 岡山大学における電子メールシステムの構成と運用

岡山大学における電子メールシステムの構成を**図 1** に示す．前節で述べたように，当センターが提供している電子メールサービスとして，(1) 学生用電子メールサービス，(2) 教職員用電子メールサービス，(3) 事務職員用電子メールサービスの 3 種類が存在する．また，それ以外に (4) 当センターが提供していない電子メールサービスも存在する．(2) から (4) の電子メールサービスに共通して提供されているサービスとして，迷惑メール対策とウイルス対策がある．これらの対策は図 1 における 2 種類のゲートウェイ（図中のメール GW1，メール GW2）によって実施されている．2 種類のゲートウェイのうちの前段（メール GW1）は迷惑メール対策専用のもので，後段（メール GW2）は迷惑メール対策およびウイルス対策用のものである．また，ファイアウォールや 2 種類のゲートウェイは処理速度や耐障害性の向上を図るため二重化している．さらに，教職員用電子メールサービスやメールゲートウェイ 2 用のフォールバック MX が別途稼働している．

以下では，(1) から (4) の各サービスについて説明する．

2.1 学生用電子メールサービス [2]

2009 年 4 月以前は学生用電子メールサービスについても当センターが提供をしていたが，たとえば携帯電話からの読み書きなどの機能を素早く提供することができ，サービス提供コスト [*1] の削減が可能になるなど，多くの利点が存在したため，2008 年度に大学執行部の経営判断により無償メールサービスの導入方針が決定された．検討時点で利用可能な無償メールサービスは Google 社が提供する Gmail，Yahoo Japan 社が提供する Yahoo!メール，Microsoft 社が提供する Windows Live@Edu の 3 種類が存在したが，1 人当たりのメールボックス容量が大きいこと，電子メール以外の様々なサービスを利用できること，多言語対応が充実していることなどの理由により Gmail を選択し，試行期間を経て 2009 年 4 月から正式に全学生を対象に新しいドメイン s.okayama-u.ac.jp で運用を開始した．なお，教職員用電子メールサービスについては，電子メールの内容やアクセス履歴が Google 社側で利用される可能性を考慮し，希望者のみ t.okayama-u.ac.jp ドメインで Gmail を利用できるようにしている．

Gmail 用に新たに追加した機器には，統合認証システムとの間で ID，パスワードを同期させるための SAML 連携サーバおよび Gmail で送受信した電子メールを記録するための学生用メールログサーバがある．

2.2 教職員用電子メールサービス

2011 年 4 月の教育・研究支援システムの更新以前では，教職員用電子メールサービスを全学に提供するため，メインキャンパスである津島 (cc) キャンパスだけではなく，鹿田 (md)，倉敷 (rib)，三朝 (misasa)，東山 (fuzoku)，芳賀 (crc)，牛窓 (uml) 各キャンパスにも 1 台ずつメールサーバを設置していた．しかし，メールサーバの台数が多いとそれに応じて管理コストが増加するため，2011 年 4 月の教育・研究支援システムの更新では比較的ネットワーク環境が整備されている鹿田，倉敷，東山，芳賀各キャンパス用のメールサーバを統合し，4 台のメールサーバ（図 1 中の教職員用 MTA1〜4 [*2]）で電子メールサービスを提供している．このうち，三朝，牛窓用はそれぞれ同キャンパス内に設置し，その他の 2 台は当センター内に設置して運用している．この 2 台を統合しなかったのは user@{md,rib,fuzoku,crc}.okayama-u.ac.jp のいずれかと user@cc.okayama-u.ac.jp を同時に利用しているユーザが存在していたためである．

また，従来は特殊な用途を除いて user@okayama-u.ac.jp のような okayama-u.ac.jp ドメインのアドレスは使用していなかった．しかし，試行期間を経て 2012 年 4 月より user@okayama-u.ac.jp は user@cc.okayama-u.ac.jp の代わりとして用いることができるようになった [*3]．この運用変更に伴い，津島用メールサーバで両方のアドレスを扱え

[*1] メールゲートウェイのライセンス料など．
[*2] 図中では POP/IMAP サーバなど他のサーバも含めて代表的に MTA(Mail Transfer Agent) として記載している．
[*3] 将来は user@okayama-u.ac.jp を公式アドレスとする予定．

る方法を検討した．その結果，津島用メールサーバでの各ユーザに対する受信アドレスを追加する方法も考えられたが，運用中のサービスへの影響を最小にするため，最終的には別途ドメイン変換を行うプロクシ（ドメイン変換 proxy）を導入した．

各メールサーバでは，システム更新以前では主としてディスク容量の懸念から POP サービスのみを提供していたが，システム更新後では従来の POP に加えて，IMAP や Web メールのサービスも提供している．また，統合認証システムを設定することにより，1 つのメールボックスに対して別名アドレスや転送先アドレスを設定したり，あるいは 1 人のユーザに対して追加メールアドレス（追加のメールボックス）を申請 [*4] したりすることができる．

電子メール発信時のユーザ認証としては，以前は POP before SMTP を用いていたが，現在は submission ポート上で SMTP AUTH によるユーザ認証を行っている．

2.3 事務職員用電子メールサービス

現在の事務職員用電子メールサービスは事務用電子計算機システムの更新に伴い，2008 年 3 月から稼働を開始している．この電子メールサービスでは独自のドメイン (adm) のみを扱い，アカウント情報も統合認証システムとは独立したものを用いている．事務用ネットワークの内部にサーバが設置されているため，基本的には学内の端末からしかアクセスできないように構成されている．詳細な構成については省略する．

現在，事務用電子計算機システムの更新を計画しており，2014 年 3 月からは新しい電子メールシステムが稼働する予定である．

2.4 他部局運用電子メールサービス

岡山大学では現在のところ電子メールサーバの設置や運用は部局で自由に行うことができる．そのため，当センターで存在を把握していない電子メールサービスが存在する可能性がある．また，そのような電子メールサービスの中には設定が不適切であったり脆弱性を持つソフトウェアを使っていたりする可能性もある．そこで，当センターではファイアウォールや 2 種類のメールゲートウェイを用いてこのような電子メールサービスに対しても最低限のセキュリティは確保できるようになっている．詳細については次節で述べる．

3. 電子メールサービスにおけるセキュリティ対策

前節で述べたように，本学では当センターが存在を把握していない電子メールサービスが存在するため，セキュリティ対策は学内の全ての電子メールサービスに適用可能である必要がある．これらの対策にはファイアウォールや 2 種類のメールゲートウェイが用いられている．本節では，これらの機器を用いたセキュリティ対策について詳細に述べる．

[*4] 追加メールアドレスは当センター承認後に作成される．

```
$ORIGIN sub.okayama-u.ac.jp.
@     IN MX 0  mta
      IN MX 10 mailgw1.okayama-u.ac.jp.
      IN MX 20 mta
mta   IN A     150.46.XXX.YYY ; 末端メールサーバ
```

図 2 SMTP 接続誘導のための DNS レコード設定例
Fig. 2 Example of DNS records for SMTP connection redirection.

3.1 SMTP 接続遮断による迷惑メール対策

他部局で運用されているものを含め，ユーザが直接使用するメールサーバ（以下，末端メールサーバ）を外部からの攻撃から防護するため，本学では外部からの SMTP 接続を末端メールサーバが直接処理するのではなく，代わりにメールゲートウェイが処理する方法を採用している．その実現方法として，ファイアウォール等のネットワーク機器で SMTP に関するパケットをメールゲートウェイにリダイレクトする方法がよく用いられる．しかし，本学では**図 2** に示すような MX レコードを各ドメインに対して設定しておき，末端のメールサーバへの SMTP 接続要求に対してファイアウォールが RST パケットを送出して意図的に失敗させることにより，メールゲートウェイへ誘導するようにしている [3].

この設定により，学外の送信メールサーバが sub.okayama-u.ac.jp ドメイン宛の電子メールを送信する場合，以下のように動作する．送信メールサーバはまずプライマリ MX である末端メールサーバ (mta) に送ろうとするが，ファイアウォールにより SMTP 接続が遮断されるため送信に失敗し，セカンダリ MX であるメールゲートウェイ 1 (mailgw1.okayama-u.ac.jp) に再送を試みるように動作する．これは実質的には tempfailing[4] の一種として動作し，多くの迷惑メール送信メールサーバはプライマリ MX への送信失敗時にセカンダリ MX への再送を試みないことから，迷惑メール対策として十分有効である．我々の以前の実験では約 8 割の迷惑メールがこの機能によりメールゲートウェイ 1 で受信されることなく廃棄されていることが分かっている [5].

この方法は代表的な tempfailing 技法である greylisting[6] と同様の効果を持ちながら，再送判定が不要である，再送待ち時間によるオーバヘッドが小さい，などの利点を有する点で greylisting より優れている．ただし，直接セカンダ

リ MX に迷惑メールを送る手口については無力である．実際，迷惑メール送信者の手口として，優先度を無視して優先度が低い MX に直接配送する方法 *5 が知られており，本学ではその対策として末端メールサーバを最も優先度が低い MX としても登録している．

メールゲートウェイ 1 は電子メールを受け取ると，署名ベースフィルタリングを行ったうえでメールゲートウェイ 2 に中継する．その際，メールゲートウェイ 1 が迷惑メールと判定した電子メールについては Subject ヘッダの先頭に [Spam] が挿入される．メールゲートウェイ 2 では独自のエンジンに基づく迷惑メール判定およびウイルスチェックを行う．その際，ヘッダの先頭に [Spam] が含まれていればマイナスのスコアを付け，[Spam] が二重に Subject ヘッダに含まれないようにしている．ただし，その場合でもメールゲートウェイ 2 では他のルールに基づく迷惑メール判定も行う．

3.2 バウンスメールの送信防止策

岡山大学に限らず多くのユーザが存在するドメインでは，宛先アドレスが存在しない（宛先不明）ため配送できない電子メールが多数到着する．特に新年度が始まってしばらくすると卒業生や退職教職員のメールアドレスが無効になるため，その時期には宛先不明メールの受信件数が増加する．

一般に，電子メールを一旦受信したメールサーバはその後その電子メールが配送不能であると判明した場合，差出人アドレス（Reverse-Path）にバウンスメール（配送不能通知メール）を返送しなければならない [7]．配送不能メールの大部分が迷惑メールであり，また迷惑メールの大部分では差出人アドレスが詐称されている事実を考慮すると，バウンスメールは実質上迷惑メールの一種であり，本学のメールサーバがバウンスメールを返送する状況はできる限り避けなければならない．本学の構成ではメールゲートウェイ 1，2 で処理を行った後に末端メールサーバに配送するため，特にメールゲートウェイ 1 が宛先不明メールを受信しないようにする必要がある．

これに対して，メールゲートウェイで宛先アドレスが存在するかどうかを確認し，存在しない場合には「550 User unknown」のような恒久的なエラーを返す方法がよく用いられている．たとえば，大分大学では学内の利用者情報を一元管理し，メールゲートウェイでこの利用者情報を参照して配送可能かどうかを判定していた [8]．しかし，本学では当センターが存在を把握していないメールサーバが存在する可能性があるため，この方法を採用することができない．そこで**図 3** に示すように，メールゲートウェイが透過的に宛先アドレスの存在を末端メールサーバに問い合わせ，配送不能の場合には送信メールサーバに末端メールサーバからの応答をそのまま通知するようにした [9]．この機能は本来はメールゲートウェイが宛先不明メールに対して迷惑メールやウイルスへの対策処理を行わないようにすることにより負荷の軽減を図るためのものであるが，この機能を活用することによりバウンスメールの抑制も行うことができる．

*5 優先度が低い MX では迷惑メール対策が不十分である可能性があるため．

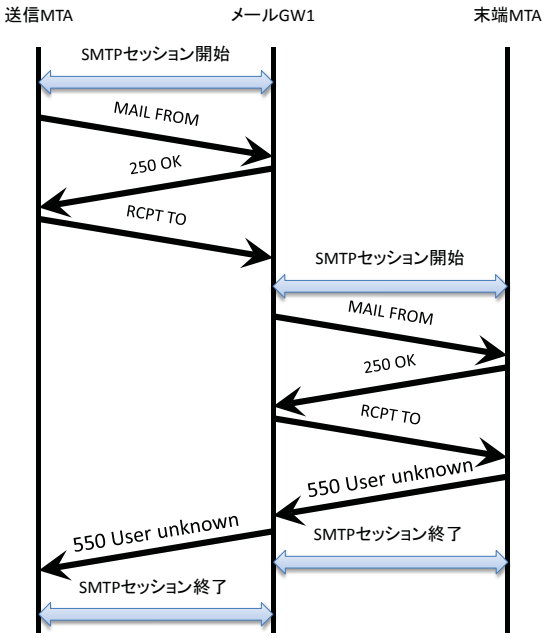

図 3 メールゲートウェイによる宛先アドレス存在確認
Fig. 3 Destination Address Checking Process by Mail Gateway.

4. 電子メールサービス運用におけるトラブル

当センターでは前節までで述べた構成および方法で電子メールサービスの運用を行ってきたが，その過程で様々なトラブルや課題に遭遇している．これらのうち，他組織でも参考になると思われるものについていくつか紹介する．

4.1 ファイアウォールによる書換え

2010 年 6 月に学外から本学に送られてきた電子メールの内容がすべて “Your mail AA.AA.AA.AA:AAAA-¿BB.BB.BB.BB:BBBB is dropped for scan engine not ready” （A は送信元，B は宛先の IP アドレスおよびポート番号を表す）に書き換えられる障害が発生した．当初はメールゲートウェイ 1，2 のいずれかが原因であると考え，設定やログを見直したが原因を特定できなかった．そこで，さらに障害の発生したメール中のヘッダを解析した結果，メールゲートウェイ 1 を通過する前の段階で書換えが発生していることが判明し，その前段のファイアウォールが原因であると推定するに至った．メールの書き換え被害を防止するため，学外からの電子メール受信を遮断して

ファイアウォールを調査したところ，アクティブ系，スタンバイ系の 2 基構成のうち，障害発生時にはスタンバイ系が使われていたことが判明した．そこで，これをアクティブ系に手動で切り換えたところ障害が解消されたことを確認したため，学外からの電子メール受信を再開した．障害発生から約 80 分の間に受信した電子メールが影響を受け，また障害復旧までに約 2 時間を要した．

その後，再発防止のため，ファイアウォールの設定を調査したところ，以下の事実が判明した．事象発生当時，本来であれば全面的に機能を停止させていたはずのウイルス対策機能を学内から学外への SMTP トラフィックに対してのみ停止しており，外部から内部への SMTP トラフィックに対してウイルス対策機能が動作する状態になっていた．また，ウイルス対策機能の設定でメモリの最大使用率を 70%（デフォルト値）としていたため，学外から短時間に多数の電子メールを受信したことによりメモリ使用量が 70%まで増加し，その結果他の処理に使用するメモリが不足してアクティブ系で再起動が発生したと推測される．一方，スタンバイ系においてもフェイルオーバが発生した直後にメモリ不足になったが，アクティブ系とは異なりウイルス対策機能のみ停止した状態に陥った．このファイアウォールではウイルス対策機能が停止した場合の動作はデフォルトで「Drop」となっており，この設定により上記のような書換えが発生していた．

この障害は単純な設定ミスに起因するもので，ウイルス対策機能の全面停止により解決することができたが，その他にもメモリ最大使用率やウイルス対策機能が停止した場合の動作のデフォルト値も要因になっている．特にウイルス対策機能が停止した場合の動作は「Drop」か「Permit」しか選ぶことができず，いずれも問題がある．この種のトラブルを防止するためには，意図した動作を行うように設定や動作を確認することは当然であるが，使用しない機能の動作についても十分に理解したうえで万一動作した場合に備えて設定を見直しておくことが重要である．

4.2 学内メールサーバのブラックリスト登録

2012 年 12 月から 2013 年 1 月にかけて，当センターで管理しているメールサーバから発信した電子メールが多くのドメインで受信拒否される障害が発生した．調査の結果，メールゲートウェイ 2 がいくつかのブラックリストに登録されていることが判明した．また，それだけでなくフォールバック MX も同様にブラックリストに登録されていることが判明した．調査の結果，いくつかの原因が判明した．以下では各原因について述べる．

4.2.1 不適切な転送設定

まずメールゲートウェイ 2 のログを確認すると，バウンスメールの送信を試みた記録が多数認められた．そこでバウンスメールの原因となった配送不能メールの 1 段前の送信元を調べたところ，図 1 における MTA1 と MTA2 が大部分を占めた．当時の電子メールサービスでは，当センターが運用しているメールサーバは外部に電子メールを配送する際にメールゲートウェイ 2 でウイルス対策を行うように設定されていた．そこで追跡調査を行ったところ，MTA1, MTA2 においていずれも現在は存在しないアドレス宛に転送設定されていたことが判明した．そこで，それらの転送設定を解除するとともに，当センターが運用しているメールサーバがメールゲートウェイ 2 を経由せずに直接配送するように設定変更を行った．これにより転送設定が不適切な場合には各メールサーバがバウンスメールを配送することになるが，ログファイルの監視を行うことでバウンスメールの発生を検出し，直ちに対策できるようにした．

4.2.2 宛先アドレス存在確認のすり抜け

バウンスメール全体の 2%以下であるが，バウンスメールの原因となった配送不能メールの 1 段前の送信元がメールゲートウェイ 1 であるものが確認された．これは 3.2 節で述べた宛先アドレス存在確認の結果，問題ないと判断されてメールゲートウェイ 1 で一旦受け取った後，メールゲートウェイ 2 に配送され，メールゲートウェイ 2 が末端メールサーバに配送する際に配送不能エラーが生じたことを意味する．そこで，メールゲートウェイ 1 のログを精査したところ，(1) 稼働停止中の末端メールサーバの存在，(2) 宛先アドレス不明以外の理由で受信拒否する末端メールサーバの存在，の 2 つの要因が確認された．

上記の 2 つの要因のうち，(1) ではメールゲートウェイ 1 がこの末端メールサーバに配送すべき電子メールを受信する際に宛先アドレス存在確認を行うことができない．ところが，メールゲートウェイ 1 の仕様により，このような場合にはメールゲートウェイ 1 はこの電子メールを受信してしまう．その結果，後にメールゲートウェイ 2 が末端メールサーバに受信したメールを配送しようとしても失敗し，最終的には時間切れにより配送不能と判断してバウンスメールを送り返す．

また，(2) では，宛先アドレス存在確認には成功するため，メールゲートウェイ 1 はこのメールを受信する．その後，メールゲートウェイ 2 が末端メールサーバにこのメールを配送する際にたとえば Subject ヘッダが空であるなどの理由により迷惑メールと判定され，末端メールサーバが受信を拒否する．その結果，メールゲートウェイ 2 がバウンスメールを差出人アドレスに送り返すことになる．

さらに，元の電子メールが迷惑メールの場合には差出人アドレスが詐称されていることが多く，バウンスメールが配送できない．その結果，フォールバック MX からバウンスメールの再送を試み，フォールバック MX がブラックリストに登録される一因となったと推測される．

これらの要因のうち，(1) に対してはメールゲートウェ

イ 1 の仕様変更により対応した．これにより，末端メールサーバが宛先アドレス存在確認に対して応答しない場合，メールゲートウェイ 1 は送信元メールサーバに対して受信せずに一時的否定応答を返すように動作するため，バウンスメールの送信義務は送信元メールサーバが持つようになった．(2) についてはメールゲートウェイ 1，2 での対応が困難であることから，末端メールサーバで受信拒否をしないように設定変更を依頼することで対応した．

4.2.3 迷惑メールの転送

2.2 節で述べたように，当センターで管理・運用している電子メールサービスでは統合認証システムを用いてユーザが自由に転送設定を行うことができる．ところが，転送設定により通常メールに加えて迷惑メールも転送されることになるため，転送先サイトによっては本学のメールサーバを迷惑メールの送信元であると判定される場合がある．また，転送先アドレスが無効になった場合も同様の判定が行われる場合がある．これにより，本学のメールサーバがブラックリストに登録される結果につながる．このようなトラブルは本学に限らず既に多くの組織で発生している（たとえば [12] 参照）．この問題に対処するため，当センターではたとえば Gmail における MailFetcher[13] など，転送の代わりに POP3 により転送元メールボックスから転送対象のメッセージを取得するサービスの利用を推奨している．

また，他部局が管理するメールサーバがブラックリストに登録される事例も存在した．このメールサーバではメーリングリストを運用しており，登録メンバー以外からの投稿にはメンバー限定である旨の一種のバウンスメールを返送を行うように設定されていた．このため，このメーリングリスト宛に迷惑メールが送られると，詐称された送信元にバウンスメールが送られるため，これが迷惑メールと判定され，ブラックリストに登録されたと推測される．実際，登録メンバー外からの投稿を単に破棄するように設定したところ，ブラックリストへの登録は解除された．

4.3 パスワード漏洩による迷惑メール送信

最近，何らかの理由によりパスワードが漏洩し，そのパスワードが悪用されて迷惑メールが大量送信される事例が何度か発生した．パスワード漏洩の原因は正確には分かっていないが，Drive by Download によりマルウェアに感染した可能性が高い．正規のユーザ名とパスワードが用いられているため，電子メール送信を直ちに不正と判断することは困難であるが，ログを見る限りボットネットを用いて複数の送信元から並行して迷惑メールを送信していると思われる．

そこで，このような手口への対策として，電子メール送信のログを常時監視し，複数の場所からの電子メールの大量送信については，一定の基準を超えた場合に迷惑メール送信と見なし，パスワード漏洩が疑われるユーザからの電子メール送信を自動的に拒否する仕組みを組み込むようにした．その結果，それ以降の同様の事例に対しては比較的早い段階で迷惑メールの配送を抑制することが確認された．

5. まとめ

本稿では岡山大学における電子メールサービスの構成および運用方法を述べた．また，これまでの運用経験において発生した主要なトラブルとその解決方法を紹介した．

2.3 節でも述べたように，現在岡山大学では事務用電子計算機システムの更新を計画しており，2014 年 3 月からは新しい電子メールシステムが稼働する予定である．これまでの運用経験を活かして，安全で使いやすい電子メールサービスを提供することが今後の課題として挙げられる．

参考文献

[1] 山井成良，岡山聖彦，藤原崇起，大隅淑弘: “岡山大学における電子メールシステムの運用と問題点，” 電子情報通信学会技術研究報告，Vol.113，No.94，IA2013-8，pp.43–48 (2013).
[2] 稗田　隆，河野圭太，岡山聖彦，山井成良，大隅淑弘，中島利行，深見清治，久保田将弘: “Google apps による岡山大学全学メールサービスの実現，” 学術情報処理研究，No.13，pp.111–115，学術情報処理研究編集委員会 (2009).
[3] 山井成良，宮下卓也，大隅淑弘，林　伸彦: “岡山大学における電子メールシステムのセキュリティ対策，” 情報処理学会分散システム/インターネット運用技術研究会研究報告，Vol.2002-DSM，No.26-11，pp.61–66 (2002).
[4] 山井成良，迷惑メール対策の概要 (online)，迷惑メール対策セミナー [新潟]，インターネット協会，入手先 <http://www.iajapan.org/anti_spam/event/2011/conf0527/pdf/01yamai.pdf> (2013.06.30).
[5] 山井成良，岡山聖彦，中村素典，清家　巧，漣　一平，河野圭太，宮下卓也: “Smtp セッションの強制切断による spam メール対策，” 情報処理学会論文誌，Vol.50，No.3，pp.940–949 (2009).
[6] E. Harris: The next step in the spam control war: Greylisting (online), available from <http://projects.puremagic.com/greylisting/whitepaper.html> (2013.06.30).
[7] J. Klensin: “Simple mail transfer protocol,” RFC5321, IETF (2008).
[8] 吉田和幸，矢田哲二，原山博文，伊藤哲郎: “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).
[9] 山井成良: バウンスメール対策，情報処理，Vol.46，No.7，pp.762–766 (2005).
[10] 北川直哉，高倉弘喜，鈴木常彦: “再送動作のリアルタイム検出による spam 判別手法の実装と評価，” 電子情報通信学会論文誌 (D)，Vol.J96-D，No.3，pp.552–561 (2013).
[11] D.J. Bernstein: qmail: the internet’s mta of choice (online), available from <http://cr.yp.to/qmail.html> (2013.06.30).
[12] www.ecc.u-tokyo.ac.jp [カテゴリ別一覧] @gmail.com 宛メールの遅延について (online)，入手先 <http://www.ecc.u-tokyo.ac.jp/announcement/2008/04/10_1026.html> (2013.06.30).
[13] Mail fetcher で別のアカウントからのメールを一元管理する - gmail ヘルプ (online)，入手先 <https://support.google.com/mail/answer/21289> (2013.06.30).