岡山大学における電子メールのセキュリティ対策

山井 成良[*1]　大隅 淑弘[*2]　林 伸彦[*3]　宮下 卓也[*4]　岡本 卓爾[*5]

岡山大学総合情報処理センター
〒700-8530 岡山市津島中3-1-1
TEL: 086-251-7231
FAX: 086-251-7244

Security Countermeasures for E-mail in Okayama University

Nariyoshi Yamai[*1]　Yoshihiro Oosumi[*2]　Nobuhiko Hayashi[*3]
Takuya Miyashita[*4]　Takuji Okamoto[*5]

Computer Center, Okayama University
Naka 3-1-1, Tsushima, Okayama 700-8530, JAPAN
Phone: +81 86 251 7231
Facsimile: +81 86 251 7244

*1 yamai@cc.okayama-u.ac.jp
*2 oosumi@cc.okayama-u.ac.jp
*3 haya@cc.okayama-u.ac.jp
*4 t_myst@cc.okayama-u.ac.jp
*5 okamoto@in.it.okayama-u.ac.jp

概要

大学におけるネットワーク管理において最も重要な問題のひとつがセキュリティ対策である．この中でも特に電子メールはSPAMなどの不正利用の原因になりやすい，部局・学科・研究室など多くの場所でサーバを独自に管理している，発信時にユーザ認証機能がなく発信者アドレスの詐称が容易である，などの理由により，このセキュリティ対策が最も重要な問題になっている．本稿では，岡山大学における電子メールのセキュリティ対策を述べる．

キーワード:

電子メール，セキュリティ対策，ネットワーク管理

1 はじめに

平成12年初めに発生した官公庁ホームページ改竄事件をはじめ，クラッカーによる官公庁や大学を対象とした不正アクセスが最近非常に増えてきている．この事件では複数の大学においてセキュリティ対策が不十分な計算機が不正侵入されて踏台攻撃に使われており，このような攻撃を防止するために十分なセキュリティ対策がますます重要になってきている．

一般に大学では部局毎にセキュリティポリシーが異なるため，本来は各部局で独自にセキュリティ対策を講じることが望ましい．しかし，多くの大学では文系の学部など必要なネットワーク機器や管理者を十分に確保できない部局もあるため，総合情報処理センターなどのネットワーク管理組織が各部局の独自性を十分考慮して全ての部局に共通するセキュリティ対策を講じる必要がある．

大学内で使われているネットワークサービスのうち，セキュリティ対策が不十分なものは数多くあるが，中でも電子メールは研究・教育活動に直結し，部局・学科・研究室など多くの場所でサービスが提供されているため，最も重要である．しかし，そのセキュリティ対策には広範囲な知識に基づく複雑な設定が要求されるため，電子メールサーバの管理者だけで対策を行うことは現実的には困難であり，ネットワーク管理組織主導による電子メールのセキュリティ対策が急務となっている．

このような事態に対処するために，岡山大学では平成11年度より総合情報処理センターが中心となって電子メールサーバの運用に関する全学的なセキュリティ対策を実施している．この対策では，部局等に設置されている電子メールサーバの設定を変更することなくセキュリティを強化することが可能で，SPAMに関する苦情が皆無となるなど大きな効果を挙げている．本稿ではその具体的な対策方法について述べる．

また，電子メールでは一般に発信時に利用者の設定した発信者アドレスがそのまま用いられるため，発信者アドレスを詐称した不正なメッセージを容易に発信できる点が問題となる．岡山大学総合情報処理センターでは平成11年度より学生が利用する計算機システムにおいてこの対策を行っており，現在に至るまで有効に機能している．本稿ではこの対策方法についても述べる．

2 電子メールサーバにおける問題点

電子メールはインターネット上で最も古くから用いられ，また現在でも最も普及しているアプリケーションの1つである．大学においても研究・教育活動に直結した最も重要なサービスとなっており，部局，学科，研究室あるいは個人単位で多くの電子メールサーバが稼働している．特にUNIX系のOSでは，標準的に電子メールサーバがインストールされており，管理者が知らないうちに稼働していることも多い．

一方，電子メールはセキュリティ上最も問題が多いサービスの1つである．例えば，従来より標準的に用いられて，現在でも最も利用されているMTA(Mail Transfer Agent)であるsendmail[1]では巨大なプログラムであるため潜在的なセキュリティホールが多く，実際にも多くのセキュリティホールが報告されている．これらのセキュリティホールの多くは，もしこれを攻撃されると管理者権限を不正取得されるものであり，これを看過できない．

また，別のセキュリティ上の問題点として，SPAMの不正中継がある．従来，sendmailの標準的な設定では第3者によるメッセージの中継を許していたため，この設定のまま放置しSPAMの不正中継に利用されているサーバが現在でも数多く存在する．このような不正中継を許すと，そのサーバがSPAMの発信元であると誤解され，その管理組織の社会的信頼性が損なわれるだけでなく，そのサーバから発信される通常のメッセージまで受取を拒否されることもある．また，SPAMを受け取った多くの受信者やその所属組織から，それを中継したサーバの管理者だけでなくネットワーク管理組織にも苦情が寄せられ，その対応に追われることになる．

これらの問題点は，MTAをセキュリティホールを塞いだものにバージョンアップし，またMTAの設定を適切に行うことによって解決することができる．しかし，MTAのバージョンアップは頻繁に行われているため，常に最新のバージョンを導入しているサーバ管理者は少ないのが実情である．また，特にsendmailでは設定ファイルsendmail.cfの設定内容が多岐に渡るため，セキュリティ対策を確実に行うには広範囲な知識に基づく複雑な設定が要求される．更に，管理者が知らないうちに稼働しているサーバでは，MTAのバージョンアップや適切な設定が期待できない．このような理由により，

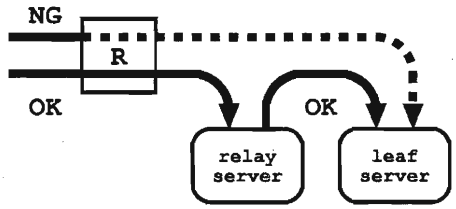

図 1: 対外接続ルータにおけるフィルタリング設定

全てのサーバ管理者が十分なセキュリティ対策を行うことは，たとえ十分な広報活動を行ったとしても事実上困難である．

3　セキュリティ対策方法

前節で述べたような問題に対して，岡山大学では平成11年度当初より大学全体を対象とした電子メールサーバのセキュリティ対策を実施している．本対策では，図1に示すように，セキュリティ対策を施した特定のサーバ（中継サーバ）だけが大学外の計算機からコネクションを確立できるように対外接続ルータにおいてフィルタリングを行い，このサーバが学内宛の全てのメッセージを一旦受け取り，これを本来受け取るべきサーバ（末端サーバ）に中継するようにしている．これにより末端サーバは外部から直接アクセスできないため，たとえセキュリティホールが残っていたり不正中継防止対策が不十分であったりした場合でも，外部の計算機から直接不正アクセスされる危険性は回避できる．

本対策では，メッセージを正しく配送できるようにするためにDNSで特別の設定を行う必要がある．例えばドメインsub.domain.okayama-u.ac.jpに計算機mailserverを新たに設置してこれを末端サーバとして使用する場合，ドメインsub.domain.okayama-u.ac.jpのDNSに図2のようなレコードを追加する．

ここで，150.46.XXX.YYYはmailserverのIPアドレス，mailrelay.okayama-u.ac.jp(以下，単にmailrelayとする)はセキュリティ対策を施した中継サーバをそれぞれ表すものとする．このように設定すると，外部の計算機がmailserver宛にメッセージを送ろうとした場合，以下のように動作する．

```
$ORIGIN sub.domain.okayama-u.ac.jp.
mailserver IN A      150.46.XXX.YYY
           IN MX 10  mailserver
           IN MX 100 mailrelay.okayama-u.ac.jp.
```

図 2: DNSの設定

1. 発信元のメールサーバはmailserverのMXレコードを見て，そのうち最も優先度が高いmailserverに直接メッセージを送信しようとする．
2. 対外接続ルータはmailserver宛のメッセージ送信を拒否する．
3. 発信元のメールサーバはmailserver宛のメッセージ送信が失敗したので，MXレコードのうち次に優先度が高いmailrelay宛にメッセージを送信する．
4. mailrelayはこのメッセージを一旦受け取り，mailrelay自身より優先度が高いmailserver宛にこれを中継する．
5. mailserverはmailrelayからメッセージを受け取り，スプールに格納する．

本対策では，DNSの設定変更が必要であるが，末端サーバやMUA(Mail User Agent)の設定は原則的に変更する必要はないため，管理者が末端サーバを適切に管理できない場合でも有効である．また，DNSの設定変更についても，

- 岡山大学では，文系の学部を中心に多くの部局を対象として総合情報処理センターがDNSの管理を行っており，末端サーバ管理者の負担とならない．
- 独自にDNSを管理している部局については，総合情報処理センターがDNS管理者との連絡体制を確立しており，またDNS管理者の技術レベルが比較的高いため，総合情報処理センターの依頼によりDNSの設定変更を確実に実施することができる．
- MTAのバージョンアップとは異なり，DNS設定変更は1度だけでよい．

などの点で従来の対策より効果的である．

なお，この対策では，副作用として自宅や外出先から学内の電子メールサービスを利用している一部の利用者はSMTPサーバの設定変更が必要となる場合がある．例えば普段SMTPサーバとして学内の電子メールサーバを指定しているノートPCの場合，これをそのまま民間プロバイダに接続して学外の利用者にメッセージを発信しようとすると，第3者によるメッセージの不正中継と見なされ拒否される．従って，この場合SMTPサーバとして民間プロバイダの電子メールサーバを指定するように設定変更が必要である．

4 セキュリティ対策の評価

前節で説明したセキュリティ対策を実施してから約1年半が経過した．対策実施後は，以前は総合情報処理センターに頻繁に寄せられていたSPAMの苦情が皆無になるなど，本セキュリティ対策は当初予想した通りの効果を発揮している．

しかし，これまでの運用経験を通じて，本対策を実施する上で注意すべき点がいくつかあることが判明した．以下ではこれらのうち主要なものを紹介する．

注意すべき点のうち，最も重要なものは，中継サーバや末端サーバがダウンした場合の影響である．本対策では，中継サーバが全てのメッセージは一旦受け取るため，中継サーバがダウンすると末端サーバへのメッセージ中継が滞り，全学の電子メールサービスに大きな影響を与えることになる．幸いにも，これまでの運用で中継サーバが長時間停止することはなかったが，耐故障性を高めるに中継サーバを複数台用意することが望ましい．また，末端サーバがダウンすると，そのサーバが再び動作するまでの間は配送されるべきメッセージが全て中継サーバに溜るため，中継サーバはこれを溜められるだけの十分なディスク容量を用意しておく必要がある．

注意すべき2つめの点は，ORBS (the Open Relay Behaviour-modification System) [2]やMAPS (Mail Abuse Preven System) RBL (Realtime Blackhole List) [3]の利用である．これらのシステムは不正中継に利用される可能性のある計算機を登録しており，sendmailでは登録された計算機からのメッセージ配送を拒否するように設定することができる．岡山大学でもいくつかの末端サーバが同システムを利用していたが，本対策実施後はたとえ同システムに登録された計算機からメッセージが配送された場合でも，一旦中継サーバが中継するため，末端サーバではこれを拒否することができない．この問題に対する対策として，中継サーバ自身が同システムを利用するように設定変更する方法も試したが，同システムに登録されていることに気づいていない学外の一般利用者から本学宛のメッセージが配送されないとの苦情が多数寄せられ，その対応に追われるようになったため，現在では同システムを利用していない．もし，どうしても同システムを利用したい末端サーバがある場合には，対外接続ルータでこの末端サーバだけ直接外部からメッセージを受け取れるようにする必要がある．

注意すべき3つめの点は，外部から発信されたメッセージを末端サーバが受け取るまでの時間である．本対策では中継サーバを経由するため正常な状態でもある程度の配送遅れが生じるが，停電復旧直後など中継サーバの負荷が高い時には更に配送遅れが大きくなる場合がある．また，対外接続ルータが末端サーバ宛のメッセージ送信を拒否する際，発信側MTAによっては対外接続ルータが出すICMP_UNREACH_FILTER_PROHIBメッセージを適切に処理せずタイムアウトとなるまで待つため配送遅れが生じる．しかし，いずれの場合も配送遅れは数分程度であり，大きな問題とはならない．

以上のように本対策では注意すべき点が多少あるが，いずれも許容できる範囲にあり，総合的に評価すると本対策は電子メールのセキュリティ強化に極めて有効であると言える．

5 発信者アドレス詐称に関する問題点と対策

電子メールのセキュリティ対策として，他組織からの不正利用の防止も重要であるが，特に大学等の教育機関では，学生を主体とする自組織の利用者が不正利用を行わないようにすることも対外的な責務として重要である．そのためには，利用者に対してネットワークエチケットなど電子メールの正しい利用法についての教育が欠かせないが，それに加えて不正利用を抑制する技術的な仕組みを導入する必要がある．このような仕組みの1つとして，メッセージの発信時に利用者認証を行い，発信者アドレスの詐称を防止する方法がある．これは不正利用を直接防止するものではないが，不正利用が行われ

た場合でも発信者が特定できるため，不正利用を間接的に抑制する効果を持つ．

岡山大学総合情報処理センターでは，教育用計算機システムを対象として平成11年度後期より発信者アドレス詐称防止策を導入した．この防止策の詳細は文献[4]で述べられているが，以下でもその概要を紹介する．

岡山大学総合情報処理センターでは，教育用計算機システムとしてWindows95 を搭載したPCを学生に利用させている．このシステムには認証サーバが別途導入され，利用者名とパスワードを入力して認証を受けないとPCを利用できないようになっている．本防止策ではMTAにフロントエンドプログラムauth-smtpd を導入し，認証サーバと協調して発信者アドレスのチェックを行う．具体的な手順を以下に示す．

1. 利用者は，利用者名とパスワードをPCに入力する．PCは認証サーバと通信して利用者認証を行い，正規の利用者であることを確認すると，当該利用者による利用を許可する．このとき，認証サーバは当該PCのIPアドレスと利用者名の対を保持しておく．

2. 利用者は，PC上のMUAを用いてメッセージを作成し，発信する．MUAはセンターの電子メールサーバにSMTPで接続する．

3. 電子メールサーバでは，auth-smtpdがMUAからのSMTP接続を受け付け，IPアドレスに基いて発信元計算機が監視対象であるかどうかを調べる．

4. 発信元計算機が監視対象であれば，auth-smtpdはこれに対応する認証サーバ[1]に問い合わせてその利用者名を取得し，発信者詐称防止処理を行いながらMUAからのSMTPセッションをMTAに中継する．監視対象でなければ，MUAからのSMTPセッションを単にMTAに中継する．

5. MTAはauth-smtpdが中継したSMTPセッションを処理し，通常どおりメッセージの配送を行う．

発信者詐称を検出した場合の処理としては，エラーとして配送を拒否するなど種々の方法が考えられるが，本防止策では強制的に正しいアドレスに書き換える方法を採用した．これは以下のような点を考慮したためである．

- 利用者の殆どは電子メールのヘッダ形式に対する知識が不足しており，発信者詐称を見破れない危険性が高い．
- 教育用計算機システムは各計算機を多くの利用者が共有して利用するため，直前の利用者のアドレスがMUAの設定として残され，新しい利用者がメッセージを発信する際にそれをそのまま誤って用いる危険性が高い．
- エラーとして配送を拒否する方法では，エラーに直面した利用者がMUAを正しく設定し直してから同一内容を再送する必要があり，利用者のレベルを考慮すると負担が大きい．

本防止策を導入してから現在に至るまで約1年が経過するが，意図的な発信者アドレス詐称は前の利用者がログアウトせず，別の利用者がそのまま使用した場合を除き，幸いにも発生していない．但し，MUAの設定ミスを救済した事例は比較的多く発生しており，その意味で本防止策は有効に機能していると言える．

6　まとめ

本稿では岡山大学における電子メールのセキュリティ対策を紹介した．本対策は導入が比較的容易でありながら，その効果は極めて大きい．岡山大学では平成13年当初に教育・研究用計算機システムの更新を予定しているが，更新後もこのセキュリティ対策を強化していきたい．

参考文献

[1] http://www.sendmail.com/

[2] http://www.orbs.org/

[3] http://maps.vix.com/

[4] 石橋勇人，山井成良，安倍広多，大西克実，松浦敏雄："リモートアクセス環境における認証サーバを用いた電子メールの発信者詐称防止の一手法"，情報処理学会分散システム運用技術研究会研究報告，97-DSM-11-5，pp. 25–30，平成10年9月．

[1] PCの設置場所により異なる．