ウィルスチェックサーバ導入とメール爆弾対策の効果

Effects of Introduction of Virus Check Server and Countermeasures for Mail Bomb

山守 一徳†, 杉浦 徳宏†
Kazunori YAMAMORI† and Tokuhiro SUGIURA†

三重大学
Mie University

本学では，大学の入口を通過する全メールにウィルスが含まれていないかチェックするウィルスチェックサーバを稼動させている．最近，コンピュータウィルスが含まれるメールが急増しており，ウィルスチェックサーバが不可欠な状態になっている．まず，本論文ではその効果を述べる．さらに，最近，学内のドメイン名でかつ存在しないユーザ名を宛先としてメールを大量に送りつけてくるメールサーバに対するDoS攻撃(メール爆弾)を受けるようになってきており，本学ではそのメール爆弾に対する対策を実施した．実施した方法は，Postfixとネットワーク監視装置を用いる方法である．本論文では，その方法と効果についても述べる．
キーワード: DoS攻撃，メール爆弾，SPAMメール，コンピュータウィルス，Postfix

Our university is using a virus check server. It checks computer virus with all mails which pass at the entrance of our university. Recently, the mails including computer virus are increasing. Therefore, the virus check server is necessary strongly. First, this paper describes the effects of virus check server. Moreover, we are received the DoS attack (Mail bomb) to mail servers recently which sends many mails with recipient addresses of our university's domain and unknown user's name. Therefore, we performed the countermeasure for the mail bomb. The adopted method uses Postfix software and a network monitoring device. This paper also describes the method and its effects.
keyword: DoS attack, Mail bomb, SPAM mail, Computer virus, Postfix

1. はじめに

電子メールは便利な情報伝達手段である反面，不正利用者によるいたずらが多くなってきている．特に，メールにウィルスを付けて送りつけてくる場合や，存在しないメールアドレスで大量にメールを送りつけてくることが多くなってきている．本学では，コンピュータウィルスの学内侵入を防ぐために，メールゲートウェイを通過する全メールに対し，コンピュータウィルスが含まれていないかチェックするウィルスチェック機能を2000年9月に稼動させた．本論文では，導入した効果についてまず述べる．

また，不正中継をさせようとするメールを送りつけて来る迷惑な行為や，存在しないユーザのメールアドレスへ向かってメールを大量に送りつけて来るメール爆弾が増えてきている．この種のメール爆弾はメールサーバに対するDoS(Denial of Service)攻撃になっており，これを受けるとウィルスチェックサーバが過負荷状態となり，本来の機能を果たせなくなる．そのため，本学ではさまざまな改善を加えた．

† 情報処理センター
〒514-8507 三重県津市上浜町1515
Information Processing Center
〒514-8507 1515 kamihama-cho, tshu-shi, Mie, JAPAN
E-mail: {yamamori,sugiura}@cc.mie-u.ac.jp

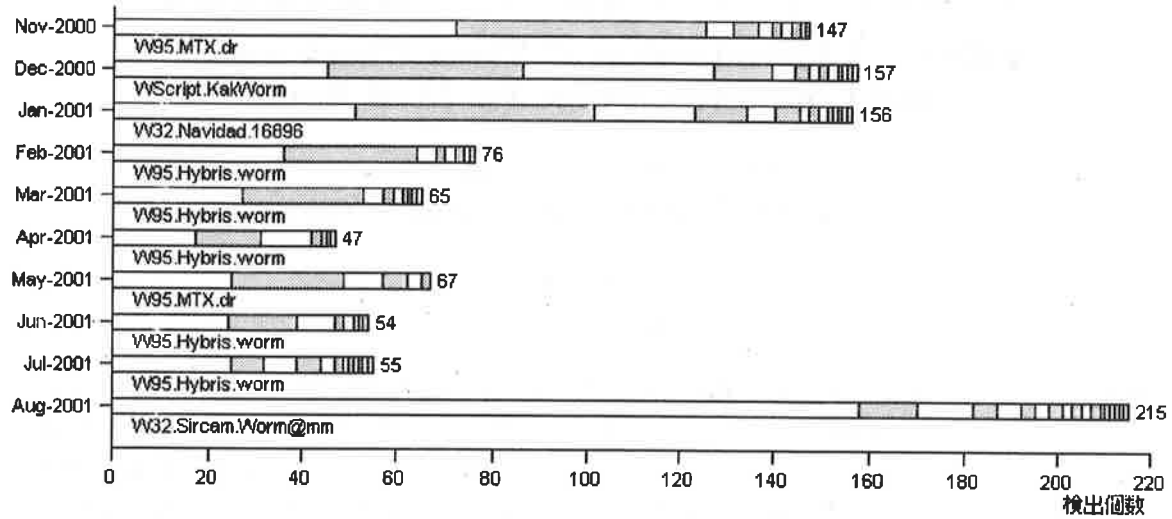

図 1: 月毎の検出されたウィルス数と最多のウィルス名

これまでにさまざまな文献[1]でSPAMメール対策のためのメールサーバの設定方法は紹介されているが，メール爆弾に対する根本的対策はまだ存在していない．本論文では，採用した防御策とその効果について述べる．メール爆弾を完全に防ぐことは難しく，どこの組織でもその対策に苦労しているはずであり，本学での対策が参考になれば幸いである．

2. ウィルスチェックサーバの効果

2.1. ウィルスチェックサーバの設置

本学では，学外から学内へのメールおよび学内メールサーバ間を行き来するメールが，ウィルスチェックサーバを通過するようにするために，メールを受け取る全てのドメイン名のMX指定をウィルスチェックサーバへ向けるように指定した．学内から学外へのメールはウィルスチェックサーバを通過しない．この方式の詳細は，参考文献[2]で述べられている．本学では特に，ウィルスチェックサーバが止まった時のための迂回経路や，ウィルスチェックサーバと迂回経路の両方が停止した時に学内メール通信のみ確保する最悪経路も用意しているため，MX行が3行書きになっているのが特徴である．導入したウィルスチェックサーバは，Symantec社のNortonAntiVirus for Solaris Gatewaysである．

2.2. ウィルスチェックサーバの導入効果

2000年11月の本格稼動以降に検出されたウィルスの数を図1に示す．

2001年8月より急激に検出数が増えているのは，SirCamウィルスが増えたため，8月7日に，AntiVirus for Solaris GatewayをVersion2.2からVersion2.5へバージョンアップしSirCamウィルスを検出できるようにしたためである．その日以前にもSirCamウィルスは確実にやってきていたが，検出もれを起こしていた．

この図1からわかるように，ウィルスの検出数はかなり多く，これらが学内に入り込む前に駆除することができたことを考えれば，ウィルスチェックサーバの導入効果は大変大きかったと言える．なお，ウィルスチェックサーバを通過するメールは毎月約25万件，全学内者は約9000人である．

3. メール爆弾防御策

メールサーバへのDoS攻撃となるメール爆弾や存在するユーザに向けたメール爆弾が増加している．不正中継をさせようと送りつけられるメールも相変わらず多い．ここでは，本

学で実施した防御策について述べる．

3.1. ウィルスチェックサーバの負荷軽減策

本学では，不正中継されないように設定し忘れているマシンが学内に存在する可能性を考慮し，学外からメールを受け取れるマシンを限定している．基本的に全メールサーバは，学外入口に設置したメールゲートウェイを通過しないとメールを受け取ることができない．そのため，不正中継に利用されることはあり得ない状態になっている．しかし，メールゲートウェイの役目を担っていた Norton AntiVirus for Solaris Gateways は，メール受信ハンドシェークの段階で不正中継拒否するようには相手から見えないことから，不正中継させようとするメールが後を断たなかった．また，不正中継を拒否するタイミングが，ウィルスチェックを実施した後になっていることから，ウィルスチェックサーバの負荷が，不正中継させようとする迷惑メールのために過負荷状態になっていた．

そこで，ウィルスチェックサーバの前段にメールゲートウェイを置き，そこで不正中継させようとするメールを拒否した後に，ウィルスチェックサーバへメールを転送するように改良を加えた．

さらに，ウィルスチェックサーバから本来の学内メールサーバへ転送する処理においても，学内メールサーバが止まっていたりすると転送を再試行する処理を繰り返し，そのためウィルスチェックサーバに負荷がかかっていた．そこで，そのメール転送負荷を減らすために，ウィルスチェックサーバの後段にもメールゲートウェイを置き，ウィルスチェックサーバはその後段メールゲートウェイへ確認済みのメールを転送し，その後段メールゲートウェイが本来の学内メールサーバへメールを転送するように改良を加えた．改良後のメールの流れを図 2 に示す．

さらに，前段メールゲートウェイは，ウィルスチェックサーバが止まっていた場合には，後段メールゲートウェイへ転送するようにし，

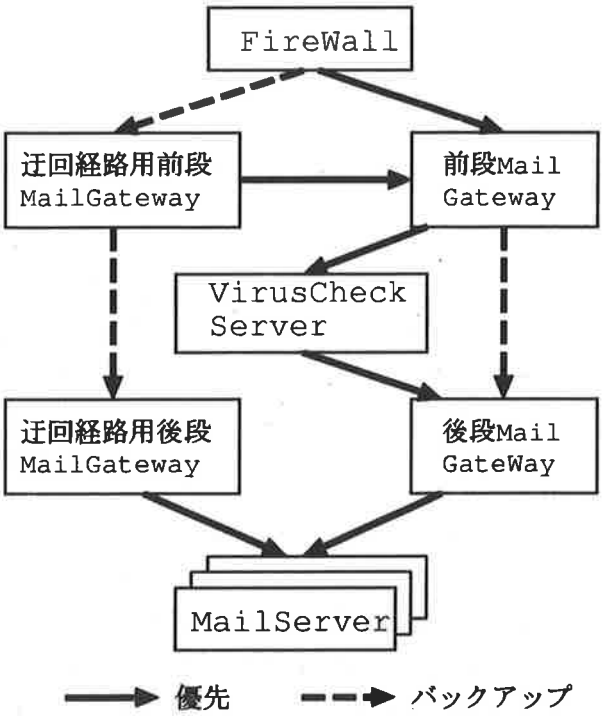

図 2: メールの流れ

メールが滞ることを避けた．なお，ウィルスチェックサーバが転送先を 1 ヶ所しか指定できず迂回経路を設定できないという機能面での問題がある．これに対しては，実際には，前段メールゲートウェイと後段メールゲートウェイはポート番号を違えて同一のマシンで実行しており，前段メールゲートウェイと後段メールゲートウェイは，ほぼ同時に稼動状態または停止状態にあると想定される．そのため，ウィルスチェックサーバは，前段メールゲートウェイからメールを受け取った後に後段メールゲートウェイに転送できずにメールが滞ることはほぼないと考えられる．

3.2. 迂回経路の改善策

MX 行の書き換えによってメール経路をメールゲートウェイに集約させる方式においては，MX の優先順位に従わずにメールを発信して来る相手が存在するという問題がある．発信が意図的であるか否かは不明である．特に，本学の場合，メールゲートウェイを 2 重化するために迂回経路が設けてあり，優先順位を下

げて迂回経路を設定してあるにもかかわらず，迂回経路側へメールを発信して来ることがある．その量は，メール爆弾のなかった2001年5月の1か月間で，本来のメールゲートウェイに届いたメールの数が247648件，その時，迂回経路のメールゲートウェイに届いたメールの数は，2144件存在した．これまで迂回経路は，ウィルスチェックサーバが止まった時のための迂回経路であったため，迂回経路へ発信してきたメールは，ウィルスチェックを実施されずに学内に入り込んでいた．

これを解決するには，ウィルスチェックサーバをもう1台用意し，迂回経路側にもウィルスチェックサーバを導入する方法があるが，ウィルスチェックサーバは高価であるため得策とは言えない．また，負荷分散装置を導入する方法もあるが，負荷分散装置自身の故障対策が必要となる．そこで，ウィルスチェックサーバに前段および後段のメールゲートウェイを導入したことを機会に，迂回経路へ発信してきたメールは，ウィルスチェックサーバの前段メールゲートウェイへ転送するようにした．その前段メールゲートウェイが止まっている場合に限り，配下のメールサーバへ配送するように改善した．

これにより，通常時には，全てのメールをウィルスチェックできるようになった．かつ，メールの転送経路の2重化も達成できている．

3.3. メールゲートウェイによるメール爆弾防御策

宛先として，ドメイン名は存在する学内ドメイン名を記述し，ユーザ名は存在しないユーザ名を機械的に自動生成して，メールを大量に送りつけるというメールサーバに対するDoS攻撃を受けるようになってきている．特に，発信元のIPアドレスについてもさまざまな多数の箇所から同時に送りつけてくるDDoS(Distributed Denial of Service)攻撃の場合には，IPアドレスを限定してファイアウォールで遮断することも困難である．大量に受取人が存在しないメールを集中して送りつけてくると，メールサーバのプロセス数が増え，マシンが過負荷になってしまう．特に，3.1.で述べたウィルスチェックサーバの負荷軽減策を施す前は，ウィルスチェックサーバが過負荷となり，本来のメール配送が滞る状態となった．そこで，ウィルスチェックサーバの負荷軽減策を施すだけでなく，前段メールゲートウェイにメール爆弾防御策を施すことにした．実現に当たっては，メールゲートウェイに，Sendmail[3]の代わりにPostfix[4]を採用した．Postfixは，Sendmailよりもプロセスが軽いと言われており，メール爆弾に対する防御策も設定がしやすい．他にqmail[5]やExim[6]を用いることも考えられたが，PostfixはSendmailとの互換性が良く，これまでSendmailを利用していたため，移行し易さからもPostfixを採用した．以下では，防御策とその設定の仕方について述べる．なお，記述に用いたPostfixのバージョンは，Snapshot-20011008である．

3.3.1 差出人および届け先アドレスによるフィルタリング

(1-a) 差出人アドレスが存在しないドメイン名の場合は受け取り拒否

メール爆弾の場合，差出人アドレスも存在していない偽名である場合があり，届け先ユーザが存在しない場合のUserUnknownエラーメールを返す処理もエラーとなり，負荷を増大させる要因となっていた．そのため，差出人アドレスが存在するドメイン名であるかチェックを行うこととした．また，ドメイン名が存在するかのチェック作業はDNS検索を伴うため負荷がかかり，その負荷を軽減させるために，差出人アドレスの記述はFQDN(Fully Qualified Domain Name)の形式であることを前もって要求した．

Postfixでの設定方法は，main.cfの設定ファイルの中に，

```
smtpd_sender_restrictions = reject_non_fqdn_sender,reject_unknown_sender_domain
```

と記述する．

(1-b) 特定の差出人アドレスは受け取り拒否

差出人アドレスが，存在するドメイン名である場合でも，メール爆弾の場合には受け取り自

身を拒否したい．この設定を施す前は，メール爆弾のメールのリターン先を特定することができた時には，ファイアウォールでIPアドレス限定によるReject設定を行い，UserUnknownエラーメールを返す処理を止め，UserUnknownメール自身が再び，UserUnknownメールとなって戻ることを避けていたが，それだけでは，充分な防御にはなっていなかった．そこで，迷惑メールの差出人アドレスが限定できる場合には，受け取りを拒否することとした．

Postfixでの設定方法は，拒否する差出人アドレスと空白文字を置いてREJECTという文字を，ファイル(*A*)内に列挙し，(1-a)での設定と合わせ，main.cfの設定ファイルの中に

```
smtpd_sender_restrictions = reject_non_fqdn_sender,reject_unknown_sender_domain,dbm:A
```

と記述する．

(1-c) 届け先アドレスが，本学に存在しないドメイン名の場合は受け取り拒否

Postfixでは，サーバの属するドメイン名(mydomain変数)やサーバのFQDNホスト名(myhostname変数)，リレーを許可するホストまたはネットワーク(mynetworks変数)，ローカル配送をするドメイン名(mydestination変数)の変数を設定すれば，不正中継に使われることがない設定となる．その点はSendmailによる設定よりも安心ができる．しかし，本学に存在しないサブドメイン名宛で届け先アドレスを指定してくる迷惑メールがあり，そのためさらに，MXレコードの指定があり，その指定先がメールゲートウェイ宛に設定してあるドメイン以外へのメールは，受け取りを拒否することとした．これにより，以前に存在したがその後存在しなくなったドメイン名について，後段メールゲートウェイの中の転送先メールサーバのリストの中に残っていたとしても，MXレコードが消された時点で受け取りを拒否することができる．

Postfixでの設定方法は，main.cfの設定ファイルの中に，

```
smtpd_recipient_restrictions = permit_mx_backup,permit_mynetworks,reject
```

と記述する．

(1-d) 特定の届け先アドレスは受け取り拒否

届け先アドレスを自動的に生成してメールを大量に送りつけるというメール爆弾の場合，その生成規則が正規表現で記述できることがある．その表現が本来の正しいメールアドレスと明らかに区別できるならば，Postfixでは，正規表現によるメールアドレスを記述し，受け取り可否を指定することができるため，大変有効な防御策となる．そこで，正規表現で指定して受け取り判定ができる場合には，その指定を随時追加することとした．

Postfixでの設定方法は，正規表現の届け先アドレスと空白文字を置いてREJECTまたはOKという文字を，ファイル(*B*)内に列挙し，(1-c)での設定と合わせ，main.cfの設定ファイルの中に，

```
smtpd_recipient_restrictions = regexp:B,permit_mx_backup,permit_mynetworks,reject
```

と記述する．また，正規表現でなく，具体的な固定文字列で届け先アドレスを指定し，受け取り可否を指定することもできる．ある特定の届け先メールアドレスに届けられるメール爆弾を受け取り拒否したい場合に有効であり，逆に先の正規表現の範囲の中から例外的に受け取り可と指定したい場合にも有効に用いることができる．そこで，その指定も随時追加することとした．

Postfixでの設定方法は，特定の届け先アドレスと空白文字を置いてREJECTまたはOKという文字を，ファイル(*C*)内に列挙し，上での設定と合わせ，main.cfの設定ファイルの中に，

```
smtpd_recipient_restrictions = dbm:C,regexp:B,permit_mx_backup,permit_mynetworks,reject
```

と記述する．

3.3.2 IPアドレスおよびHELOハンドシェークによるフィルタリング

(2-a) 特定のクライアントホストからの接続要求は受け取り拒否

ORBS(Open Relay Behaviour modification System)やMAPS RBL(Mail Abuse Preven-

sion System Realtime Blackhole List) などのデータベースを利用したOpen Relay SMTPサーバ(ブラックリストサーバ)からの接続要求を拒否することがPostfixでできるが，そこまで指定すると迷惑メールでないメールも受け取り拒否してしまう弊害が考えられるため，独自にブラックリストを作成し，そこからの接続要求は拒否することとした．独自にブラックリストを作成する場合，Open Relay状態であるか否かに依存せず，迷惑メールを出してきたことがあるという実績から判断するため，拒否の効果が高く，自分たちで受け取り判断をコントロールできるメリットがある．

Postfixでの設定方法は，特定のクライアントホストのFQDNかIPアドレスと，その後ろに空白文字を置いてREJECTまたはOKという文字を，ファイル(D)内に列挙し，main.cfの設定ファイルの中に，

```
smtpd_client_restrictions = dbm:D
```

と記述する．

(2-b)HELOハンドシェークの不正は受け取り拒否

最初にHELOを発信して来ない相手に対しては，直ちに受け取りを拒否することとし，受け側の負荷を軽減させるようにした．また，HELOハンドシェークの中で，発信側が名乗ってくるホスト名が文法的に正しくない名前である場合も，受け取りを拒否することとした．これも受け側サーバの負荷を軽減させるためである．

Postfixでの設定方法は，main.cfの設定ファイルの中に，

```
smtpd_helo_requied = yes
smtpd_helo_restricted = reject_invalid_hostname
```

と記述する．

3.3.3 エラー発生時に対する対策

(3-a)SMTPネゴシエーション中に受け取り拒否を返す場合，遅延させて返答

DoS攻撃される場合，一時期に大量のメールを送られるため，受け手が過負荷状態になる．そこで，受け取り拒否する相手との通信は，応答速度を遅らせれば，大量メールを受ける時期的な集中を避けることができる．そのため，受け取り拒否のエラーコードを返答する時に，指定された秒数が経つまでその返事を返さないようにする．この機能は，Postfixの中に標準で組み込まれているので，秒数を指定するだけで良い．

Postfixでの設定方法は，main.cfの設定ファイルの中に，

```
smtpd_error_sleep_time = X
```

と記述する．Xは遅延させる秒数である．

(3-b) 1セッション内に閾値回数のエラーを起こすと返答を遅延させて通信．さらにエラーを閾値回数を超えて起こすと通信を切断

1セッションの通信内において，受け取り拒否などのエラーを起こすような相手は，攻撃を仕掛けてくるような怪しい相手であると判断し，2つの閾値を設けて応答を変える．まず，最初の閾値の回数のエラーを起こすと，それ以降の返答を返す時に指定時間待ってから返すようにする．次に，2つ目の閾値の回数を超えてエラーを起こすと，通信を遮断させる．この機能は，Postfixの中に標準で組み込まれているので，閾値回数を指定するだけで良い．

Postfixでの設定方法は，main.cfの設定ファイルの中に，

```
smtpd_soft_error_limit = Y
smtpd_hard_error_limit = Z
```

と記述する．Yが最初の閾値，Zが2つ目の閾値である．本学では，Yは1，Zは2で運用している．

このように設定すると，迷惑メールは，一度に複数の届け先を指定してくることが多いため，rcpt to: の複数回の繰返しを発生させているが，その繰返し中にエラーが発生した場合，それ以降のエラーを返す回数を減らし，それ以降の通信を遮断する効果がある．

(3-c) エラーログの届け先の変更

エラーメールの届け先をPostmasterと指定しているとメール爆弾を受けた時に，Postmasterに大量のエラーメールが届き，Postmasterが困ってしまう．特にPostmasterは，通常は特定の人のアドレスへ転送するように設定さ

れているので，その人のメールボックスの許容量を超えることもあり得る．そこで，エラーメールはPostmaster宛でなく，メールボックスを持つ特定のユーザ名宛に指定するのが良い．そして，必要な時にはメールボックスを空にすることができるのが良い．

Postfixでの設定方法は，main.cfの設定ファイルの中に，

```
bounce_notice_recipient = ユーザ名
2bounce_notice_recipient = ユーザ名
delay_notice_recipient = ユーザ名
error_notice_recipient = ユーザ名
```

と記述する．

もしも，ユーザ名にrootを用いた場合，rootユーザ用にメールボックスが存在することが重要である．このようにしておくと，メール爆弾を受けた時に，エラーメールが溜まるメールボックスを限定することができ，Posmatster宛のメールとは明確に区別することができる．

3.4. 迂回経路におけるメール爆弾防御策

前段メールゲートウェイにおいて，メール爆弾防御策を施すことは，ウィルスチェックサーバの負荷軽減に繋がるだけでなく，学内の全てのメールサーバに対するメール爆弾を防御できるはずである．しかし，それには，迂回経路のメールゲートウェイにおいても，同様のメール爆弾防御策を行う必要がある．すなわち，前段メールゲートウェイでメール爆弾防御策を施し，迂回経路のメールゲートウェイでメール爆弾防御策を施していない場合，メール爆弾のメールは前段メールゲートウェイで受け取り拒否された後に，迂回経路のメールゲートウェイを通過して学内のメールサーバに届いてしまうからである．そこで，迂回経路も迂回経路用前段メールゲートウェイと迂回経路用後段メールゲートウェイに分け，迂回経路前段メールゲートウェイに前段メールゲートウェイと同様のメール爆弾防御策を施した．

迂回経路用前段メールゲートウェイと迂回経路用後段メールゲートウェイは，ポート番号を違えて同一マシン上のPostfixで実現しており，迂回経路用前段メールゲートウェイと迂回経路用後段メールゲートウェイは，ほぼ同時に稼動状態または停止状態にあると想定される．

ちなみに，Postfixでは受け取ったメールの転送先をrelayhost変数に指定する．さらに，指定した転送先が止まっていた場合にどこにも転送できない時のための転送先をfallback_relay変数に指定する．relayhost変数には，複数の転送先を書くことも可能である．転送に用いるポート番号も指定ができる．

3.5. メール爆弾検出策

メールゲートウェイでメール爆弾のメールを受け取り拒否する設定を施したとしても，その設定は自動ではなく，アクセス拒否をすり抜ける新種のメール爆弾が現れれば，設定を手動で追加する必要がある．そのため，メール爆弾がすり抜けていないかを検出する必要がある．そこで，メールゲートウェイに直結するHUBのポートから流れ出る単位時間あたりのバイト数を監視し，閾値以上のトラフィックが起きた場合に，管理者へメールで連絡するようにした．それには，カナダのロランインターナショナルテクノロジーズ社製kinnetisというネットワーク監視装置を用いて実現した．この製品は，SNMP機能付きHUBのポートのトラフィックを常時監視することができる．ただし，トラフィックのチェックだけでは，大容量のメールを受信した場合にメール爆弾のように見えてしまうことから，誤検出されることがある．そのため，閾値以上のトラフィック発生のメールを受信した時には，メールゲートウェイのログを調べ，メール爆弾であるか否かを見極める必要がある．管理者の目の止まるようにログを画面に流しておくのも効果があるが，その方法のみでは管理者の負担になるためメール連絡と併用するのが良い．

なお，RealSecureなどの不正アクセス検出ソフトの中には，DoS攻撃検出の機能があるため，その検出能力を使用することも考えられるが，メール爆弾の場合は，正しいメールの受け取りと区別することが困難である．ち

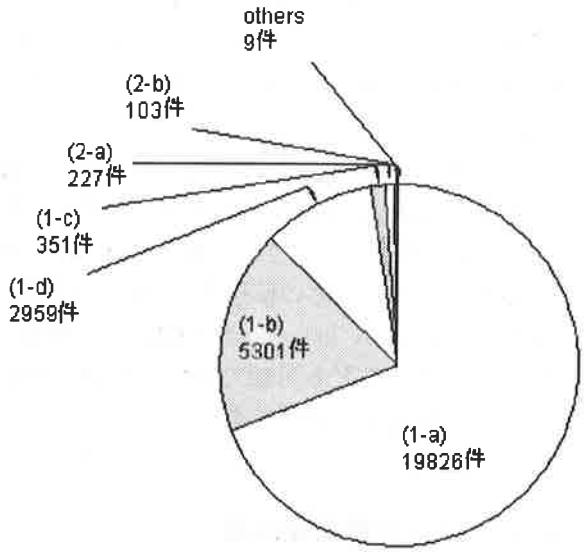

図 3: 受け取り拒否の種類別件数

なみに，RealSecure では，メール爆弾を検出できない．

4. メール爆弾防御策の効果

3.3. における設定の効果について，2001 年 8 月 7 日から 9 月 6 日の 1 か月間に受け取り拒否したメール 28776 件を分類した結果を図 3 に示す．効果が一番大きいのが，(1-a) 差出人アドレスが存在しないドメイン名の場合は受け取り拒否の設定である．28776 件中 19826 件が From：の欄に存在しないドメイン名を付けてくるメールであった．次に効果が大きいのが，(1-b) 特定の差出人アドレスは受け取り拒否の設定である．迷惑メールの From:の欄には，特定の差出人アドレスが書いてある場合が多い．28776 件中 5301 件が (1-b) の設定により拒否された．次に効果が大きいのは，(1-d) 特定の届け先アドレスは受け取り拒否の設定である．存在しないユーザに頻繁に送ってくる迷惑メールや，メール爆弾の届け先アドレスを正規表現によって拒否できたメールが多く存在する．28776 件中 2959 件が (1-d) の設定により拒否された．次に効果が大きいのは，(1-c) 届け先アドレスが，本学に存在しないドメイン名の場合は受け取り拒否の設定である．28776 件中 351 件が (1-c) の設定により拒否された．次に効果が大きいのは，(2-a) 特定のクライアントホストからの接続要求は受け取り拒否の設定である．迷惑メールの From: の欄が From:<> と記述されており，その場合のクライアントホストの多くは特定することができた．28776 件中 227 件が (2-a) の設定により拒否された．From:<> を拒否条件にするという方法が考えられるが，RFC(Request For Comments) の規約に違反するため，Postfix の中にも指定方法は存在しない．それに代わって (2-a) の設定が有効である．次に効果が大きいのは，(2-b)HELO ハンドシェークの不正は受け取り拒否の設定である．HELO ハンドシェークの不正は思った以上に存在する．28776 件中 103 件が該当した．

最も問題となっている短時間に集中して大量のメールを送ってくるメール爆弾に対しての効果については，攻撃されている最中に設定を行うことになるため経験的ではあるが，(1-d) 特定の届け先アドレスは受け取り拒否の中の正規表現による拒否が，メール爆弾に対し最も効果が大きかった．メール爆弾の場合，受け取り拒否しても機械的に次のメールアドレスに向けて発信してくる．そのため，拒否する記述に成功すればその効果は大きく，素早く記述できることが重要である．その点で，Sendmail では def ファイルから cf ファイルを生成するステップが必要であることと，cf ファイルが理解できず正しく動作するのか不安が付きまとうという問題がある．一方，Postfix ではわかりやすく安心感がある．また，Sendmail では，(1-d) 特定の届け先アドレスは受け取り拒否の中の正規表現による拒否の設定をすることが困難であり，Postfix では設定が可能である．以上のことより，Postfix を採用して良かったと言える．

また，存在しないユーザのメールアドレスへ向かってメールを大量に送りつけて来るメール爆弾以外にも，特定の存在するユーザに大量のメールを出してメールボックスを一杯にするメール爆弾に対しても，この防御策は有効に働く．自分のメールアドレスに大量メールを投げられた時に，メールサーバ上のメー

ルボックスからユーザが条件指定したメールについては廃棄しながらメールクライアントへ欲しいメールのみ読み込むというフリーソフト (例えば，Spam Buster) やシェアウェアソフト (例えば，SpamEater Pro) が存在するぐらいメール爆弾は広まっている．今回の防御策がうまく機能すれば，学内ユーザでそのソフトが必要になることはほぼないはずである．

また，この防御策は，メール爆弾でなく迷惑メールに対しても機能する．メール爆弾は常時送られてきている訳ではないが，迷惑メールは常時送られてきている．この防御策の設定により拒否されている迷惑メールは常に存在しており，その効果は大きい．世の中には，メールボックスを持つ自分のメールアドレスに迷惑メールが届けられないように公開用のメールアドレスを用意し，公開用のメールアドレスからメールボックスを持つメールアドレスに迷惑メールを転送しないようにガードするメールアドレス転送サービスという商売が存在している (例えばpobox.com)．本来は，メールボックスを持つメールアドレスが変わっても公開用のメールアドレスにメールが届けられるので自分宛のメールは確実に受信できるようにするために始まったサービスであるが，迷惑メール除けに使われるようになってきている．

また，この防御策に相当する商品も存在する (例えば，米Lyris Technologies Inc. 開発MailShield)．同じように受け取り拒否する条件を記述するものであり，それに比べれば，我々のPostfixを用いる方法は安価である．

5. まとめ

Sendmailを用いてもメール爆弾防御策を施すことは可能である．しかし，届け先アドレスがメールを受信して良いドメインでありながら，正規表現で記述される特定の届け先アドレスの場合は受け取りを拒否することは設定困難である．また，Sendmailは多数の変数があり，さまざまな設定が可能である反面，設定を間違えると不正中継に使われてしまう恐れがあるが，Postfixは不正中継されないことがデフォルト設定になっているので，気楽に設定ができる．また，defファイルとcfファイルの関係がないことから，Postfixを用いた場合には，わかりやすさから安心感があり，メール爆弾が届けられた時に素早い条件記述が可能である．よって，Postfixの利用はお勧めである．

本学のように，学外からのメールの受け取り窓口を一本化している場合には，メール爆弾からの防御は，メールゲートウェイを保護するだけでなく，学内の全てのメールサーバを保護できるという効果がある．実在する学内ユーザ向けのメール爆弾も受け取り拒否が可能である．また，メール爆弾ではない，受け手にとって迷惑なメールを受け取り拒否する効果も大きい．世の中に不正中継に使われるメールサーバが存在しなくなることは，現状では考えられないので，各自でメール爆弾対策やウィルス対策をする必要があり，本学の防御策はお勧めの方法である．

将来的には，メール爆弾攻撃を誤りなく検出し，その後自動遮断するような方法が必要であるが，今後の課題である．また，わずかではあるが，前段メールゲートウェイとSymantec社のNortonAntiVirus for Solaris Gatewaysのウィルスチェックサーバの間において，通信エラーを起こしている時があり，その原因を調査することも今後の課題となっている．

参考文献

(1) ”ネットワークとワークステーション管理のためのセキュリティガイド第2.2版”，富士通サイエンティフィック・システム研究会ネットワークWG発行,(2001-08)

(2) 山守一徳, 太田義勝:”SPAMメールの不正中継防止対策とウィルス対策”, 情報処理学会分散システム／インターネット運用技術シンポジウム2001論文集,(17),pp.109-114(2001-02)

(3) sendmail.org: http://www.sendmail.org/, (2001年9月1日現在).

(4) Postfix.org: http://www.postfix.org/, (2001年9月1日現在).

(5) qmail.org: http://qmail.org/, (2001年9月1日現在).

(6) Exim.org: http://www.exim.org/, (2001年9月1日現在).

著者略歴

山守 一徳 昭57名大・工・電気卒. 昭59同大学院修士課程(情報工学専攻)了. 同年(株)沖テクノシステムズラボラトリ入社. 平10三重大・情報処理センター・助手. ネットワークおよびデフォルメ地図自動生成に関する研究に従事. 情報処理学会, 電子情報通信学会, 形の科学会各会員.

杉浦 徳宏 平8名大・工・電子機械卒. 平13同大大学院博士課程了. 同年, 三重大・情報処理センター・助手. 画像計測, ロボットビジョン, 機械学習に関する研究に従事. 平8日本機械学会畠山賞. 日本機械学会, 日本ロボット学会, 人工知能学会各会員.

(2001年10月 4 日受付)
(2002年 1 月11日再受付)
(2002年 3 月13日採録)