ゲートキーパーへの迷惑メイル対策機能の追加

2007MI097 加藤 雅斗　　2007MI128 松本 征也　　2007MI165 南部 勝巳
指導教員　後藤 邦夫

1　はじめに

近年，インターネットの普及に伴い，その安全性が大きな問題となっている．

また，spam(スパム) メールと呼ばれる，ネット上で手に入れたメールアドレスに向けて，営利目的のメールを無差別に大量配信するものが急増していて，メール使用者にとって必要な通常のメールよりも，これらスパムがはるかに多く届くといった事態にもなり，こちらも大きな社会問題となっている．

これら 2 つの事柄から，本研究では既存手法である「段階的通信制限システムの拡張」[2] のゲートキーパー (以下，GK とする) を用い，spam メール対策としてモジュールの追加に重点を置いて進めていく．GK とは，パーソナルコンピュータ (以下，PC とする) をブリッジとして用い，リアルタイムに通信をフィルタリング，そして攻撃の量と時間に応じてパケットの到着時間を遅らしたり，スループット制限を設定したり，送信パケット数を減らしたり，最終的には受信したパケットをすべて落とすという段階的に通信を制限する安価で拡張性の高い防御を重視したものである．

拡張については，spam メールかどうかの判定をした IP アドレスのリスト (以後, スパムチェックリスト) の作成, 及び, ブラックリストとの照合, SPF レコード, MX レコードによる逆引き判定，Domain Name System(以下，DNS) による逆引き判定，その他あやしいホストへの嫌がらせルールを自動追加を目的としている．

なお，実験は共同で行い，加藤は主に GK 及び GK との連携，パケットキャプチャの部分を，松本は主にスパムチェックリスト，DNS の部分を，南部は主に SPF レコード，MX レコードの部分を担当した．

2　システムの概要

この節では，本研究のシステム概要の基本的な考え方と，既存手法である GK の基本的なネットワーク構成について述べる．

2.1　既存システムの概要

GK は外部ネットワークと内部ネットワーク間で IP アドレスをつけずにブリッジとして動作させ，フレーム通過時に通信を制限する．IDS はスイッチでミラーリングされたネットワーク上を流れるパケットを監視し，検知した攻撃の種類，攻撃元の IP アドレスなどの情報を専用回線を介して GK に渡す．GK はこの情報に従ってリアルタイムに通信制限をする．GK と IDS の専用回線以外のネットワークインタフェースは IP アドレスを持たず，ネットワークへの影響が無く，攻撃対象にならないという利点を持つ．GK では受信したパケットに

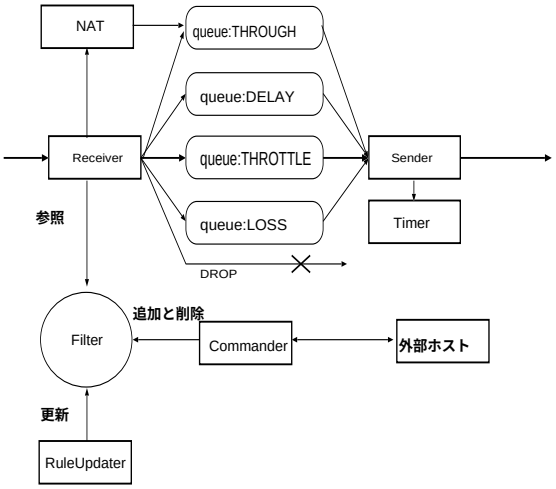

図 1　GK の構成図

任意の通信制限を起こすことができる．外部ホストは Commander にアクセスし，フィルタリングルール操作の依頼をすることで，任意の通信制限を起こす．(図 1 参照)

本研究ではこの機能を使って，GK で通信制限をする．GK でできる通信制限は以下の 5 段階に分かれる．

- THROUGH (素通し)
  通常の通信処理と同じ役割を果たす．正常なパケットのみをこの状態で通す．
- DELAY (遅延)
  任意の数秒の遅延を起こす．
- THROTTLE (スループット制限)
  帯域幅を絞り，パケット損失を起こす．
- LOSS (パケット損失)
  任意の確率でパケットを破棄し，パケット損失を起こす．
- DROP (パケット破棄)
  全てのパケットを破棄する．

GK では，攻撃と判断され，抑止効果が見込まれる通信は THROUGH の経路から外れ，DELAY，THROTTLE，LOSS の状態を段階的に移行し，様子を見る．最終的に，抑止効果が見込まれない通信は，DROP の状態に移行させる．また，DELAY，THROTTLE，LOSS の状態に移行した通信に対しても，断続的に行われるようなら DROP の状態に移行させる．

2.2　新システムの概要

本研究の新システム (以後，spam センサ) では，既存システムの GK を外から利用して，spam メール対策を

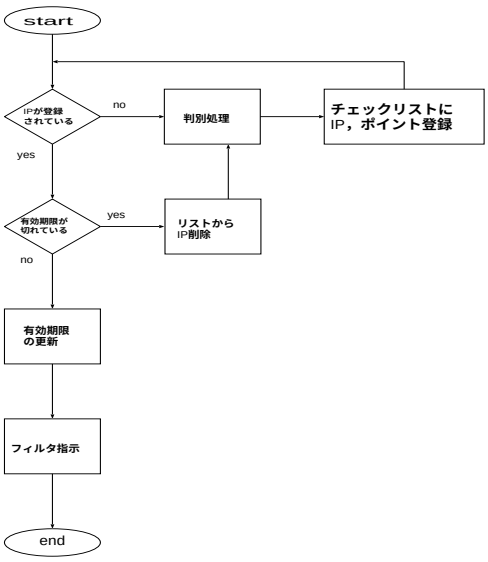

図 2　spam センサフローチャート

実現する．

そして本研究の主な目的は，以下の 4 点である．

- パケットキャプチャした IP アドレスが，危ないかどうかの判断
- 危ない通信へのいやがらせ
- スパムチェックリストの強化
- メイルサーバへの spam メールの減少

本研究の具体的な流れは，まずメールサーバにメールが届く前に次節で述べるパケットキャプチャプログラムにより，IP アドレス，ドメイン名を取得する．その IP アドレスについて以下の順序で，spam メールかどうかの判別処理をする．その後 IP アドレスをスパムチェックリストに登録する．スパムチェックリストについては，3.2 節にて詳しく説明する．

判別処理の手順は以下の通りである．

1. spamhaus のブラックリストとの照合
2. DNS サーバとの逆引き，及び正引き
3. MX レコードによる判別
4. SPF レコードによる判別

各判別処理で問題があった場合，GK により適した処理をする．(図 2 参照)

2.3　spam センサ

本研究で提案する spam センサについて説明する．spam センサでは，送られてきたメールから IP アドレスをパケットキャプチャし，IP アドレスが危ないものかどうか判断をする．spam センサで実行する判別の一つひとつでは，spam メールと判断するには不十分であるため，私達が独自で基準を定め，その基準を超えたものを spam メールと判断する．各処理で問題があると判別された場合に，その IP アドレスにポイントを加算し，スパムチェックリストに登録する．判別された IP アドレスには有効期限を設け，有効期限が切れている IP アドレスは再度判別処理をし，有効期限が切れていない IP アドレスからのメールについては，ポイントを倍にして登録する．ポイントに応じて GK での遅延処理をする．ポイントが多い IP アドレスほど遅延時間を多くする．また，ポイントが一定異常に達し spam メールと完全に判断した IP アドレスについては，完全なパケットロスをする．GK への命令の追加は，判別処理をした結果，必要に応じて自動で追加される．

2.4　IP アドレスの取得方法

本研究において重要な IP アドレスの取得方法について述べる．SMTP 通信のみを取得するために，TCP ポート 25 のパケットのみを取得するパケットキャプチャプログラムを作成した．このプログラムではメールのヘッダ情報を入手することができる．また，入手した情報から必要なデータだけを切り出すプログラムを作成し，パケットキャプチャプログラムと連動することにより，より重要な情報のみを入手することに成功した．ここで述べる重要な情報とは，SMTP 通信で発生する相手側ホストの情報が入っている HELO，及び EHLO の部分，送信元のメールアドレスが分かる MAIL FROM の部分のことである．ここで得られた IP アドレスの情報やメールアドレスの情報を元に，spam センサを実行する．

2.5　spamhaus

spamhaus とは，web 上でフリーに公開されているサイトであり，nslookup コマンドを用いてブラックリストデータベースに登録されているか確認できる．「Address:127.0.0.X」(X はブロックリストプロバイダによって異なる) のようなアドレスが返ってくれば，ブラックリストに存在する．応答がない場合は，ブラックリストに存在しない．

2.6　DNS

DNS とは，IP アドレスとドメイン名を対応させるシステムである．IP アドレスからドメイン名がわかるか，また逆にドメイン名から IP アドレスがわかるかどうか判別する．

2.7　SPF レコード

電子メールにおける送信ドメイン認証のひとつで，現在もっとも多く利用されている送信ドメイン認証の仕組である．差出人のメールアドレスが他のドメインになりすましていないかどうかを検出することができる．メール受信サーバは受信中のメールの MAIL FROM の送信ドメインをを元に DNS からドメイン名情報を取得して SPF レコードの内容とメールの送信元 IP アドレスを照合する．照合の結果 IP アドレスが SPF レコードの内容にマッチすれば認証成立となる．

2.8　MX レコード

MX レコードには，そのドメインのメールサーバに関する情報が登録されている．相手の IP アドレスが MX のリストにあるかどうかで判別する．MX レコードを設

定することによりメールサーバの優先度を決めて，効率良くメールを受けとることができる．

3 システムの実現

この節では，spam メール対策として実行している各判別処理の仕組みについて説明する．

3.1 システムの構成

本研究では，PC の OS に Ubuntu10．04 を使用する．spam センサでは大きく分けて，パケットの受信処理，spam メールかどうかの判定処理，GK での処理の 3 つの処理から成り立っている．全ての処理の実現に，perl スクリプトを用いた．

本研究では spam センサをメイルサーバ外に設置する．メールサーバ内に設置すると，そのサーバにメールが届いてから処理をするため，そのサーバしか監視することができない．その反面，メールサーバ外に設置することで，サーバに届く前に処理をするため，全てのメールサーバを監視することができる．

3.2 スパムチェックリスト

スパムチェックリストは，送られてきたメールの IP アドレスや，ポイント，有効期限を記録しておくものである．スパムチェックリストでは，まず IP アドレスが登録されているかどうか確認する．登録されていない IP アドレスは判別処理をしてからポイント，有効期限を登録する．すでに登録されている IP アドレスについては有効期限を確認し，期限内の場合であればポイントを等倍して有効期限を更新する．また，期限が切れていた場合は再度判別処理をして有効期限を更新する．有効期限を設けることにより，スパムチェックリストの信憑性を保つことができると考えられる．

3.3 spamhaus ブラックリストでの判別方法

spamhaus ブラックリストの照合の際に必要な情報は，パケットキャプチャプログラムから IP アドレスを取得する．これを利用して照合をする．

spamhaus ブラックリストとの照合だが，ここで注意しなければならないのが，spamhaus ブラックリストは IP アドレスを逆順にしたものが登録されているということである．つまり，取得した IP アドレスを逆順にする必要がある．spamhaus ブラックリストに登録されている場合，規程のポイントを加算するものとする．spamhaus ブラックリストでの判別は，ブラックリストに誤登録があるため信憑性が薄く，ポイントの比重を低く設定した．

3.4 DNS での判別方法

IP アドレスが DNS サーバに登録してあるか逆引き，もしくは正引きをする．ここで逆引き，もしくは正引きができなかった場合に規程のポイントを加算する．DMS に登録されていないだけでは，spam メールと判断できないため，ポイントの比重を低く設定した．

DNS 逆引きできたかどうかは，name が正常に表示されていれば成功，そうでなければ失敗である．逆に DNS 正引きできたかどうかは，Address が逆引き時と同じものであれば成功，そうでなければ失敗である．

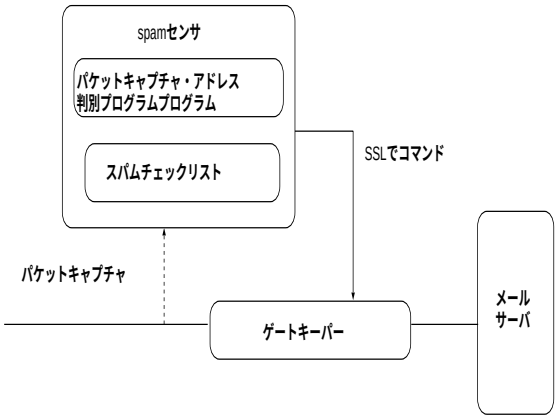

図 3　実験環境構成図

3.5 SPF レコードでの判別方法

ドメイン名から SPF レコードがあるかどうか確認する．この判別では，SPF レコードがあり IP アドレスが範囲内の場合，SPF レコードが無い場合，SPF レコードがあるが IP アドレスが範囲外の場合の 3 つの場合に分けてポイントを決める．SPF レコードがある場合は，問題がないのでポイントを加算しない．SPF レコードがあるが IP アドレスが範囲外の場合では，なりすましである可能性が高いためポイントの比重を高く設定した．また，SPF レコードが無いだけでは，spam メールと判断できないため，ポイントの比重を低く設定した．

SPF レコードを引いて SPF レコードがある場合は，docomo.ne.jp text = ”v=spf1 +ip4:203.138.203.0/24 all”のように spf が表示される，また，include と表示されたものはさらに SPF レコードを引く必要がある．

3.6 MX レコードでの判別方法

ドメイン名から MX レコードがあるかどうか確認する．MX レコードが無いだけでは，spam メールと判断できないため，ポイントの比重を低く設定した．

MX レコードを引いて MX レコードがある場合は，;; —HEADER— opcode: QUERY,status: NOERROR,id: 59978 の status の部分が NOERROR と表示され，ない場合は status の 部分が NXDOMAIN と表示される．

4 実験と評価

spam センサを用いて実験をし，評価をする．実験環境は Ubuntu10.04 をインストールした PC を 1 台用意する．

4.1 実験環境の構成

図 3 は実験環境について示した図である．GK とは独立に構成した，パケットキャプチャプログラムと判別プログラム，スパムチェックリストで構成された spam センサを用い，判別に対して GK を外から利用する形である．

4.2 実験の手順

本研究では，メールサーバを用意し，インターネット上にわざとアドレスを晒し，spam メールを誘い実験をする．パケットキャプチャをして IP アドレスを spam センサで判別をした結果，20 ポイント以上の場合にはパケットロスし，20 未満の場合はポイント分の遅延の命令を追加していく．その後，実際に遅延やパケットロスが発生しているかを確認する．

4.3 スパムチェックリストの拡張

実験をしていくと，スパムチェックリストの中身は増えていき，実験をすればするほど，spam メール対策として，完成されていく．スパムチェックリストに登録されている IP アドレスの中で，危ない通信と判断された IP アドレスについては，今後，有効期限がきれるまでパケットロスとする．これにより spam メール対策になる．

4.4 spamhaus ブラックリストでの照合

携帯電話や web 上で自由に登録できるメールアカウントから実際にメールを受信し，プログラムを実行した．

IP アドレスが spamhaus のブラックリストに登録されている場合は，ポイントを 1 加算する．今回の実験の結果，spamhaus のブラックリストに登録されているか照合し，判別することができた．

spamhaus に登録されている場合

```
Name:    27.212.223.111.zen.spamhaus.org
Address: 127.0.0.2
```

4.5 DNS を使った判定

携帯電話や web 上で自由に登録できるメールアカウントから実際にメールを受信し，プログラムを実行した．逆引きができるかできないかの判別をし，逆引きができない場合，ポイントを 1 加算する．実験の結果，逆引きできるもの，できないものが判断できた．

DNS 逆引き成功の場合

```
Name: web3314.mail.ogk.yahoo.co.jp
Address: 124.83.168.28
```

4.6 SPF レコードを使った判定

携帯電話や web 上で自由に登録できるメールアカウントから実際にメールを受信し，プログラムを実行した．ドメイン名に SPF レコードがあり，IP アドレスが範囲外である場合にはポイントを 20 加算し，SPF レコードが無い場合はポイントを 1 加算する．実験の結果，SPF レコードがあるもの，ないものが判別できた．

SPF レコードがある場合

```
spf.yahoo.co.jp. 900 IN TXT "v=spf1
include:spf01.yahoo.co.jp include:spf02
.yahoo.co.jp include:spf03.yahoo.co.jp
include:bulk-spf.yahoo.co.jp ~all"
```

4.7 MX レコードを使った判定

携帯電話や web 上で自由に登録できるメールアカウントから実際にメールを受信し，プログラムを実行した．MX レコードが無い場合は，ポイントを 1 加算する．実験の結果，MX レコードがあるもの，ないものが判別できた．

MX レコードがある場合

```
;; ---HEADER--- opcode: QUERY,
status: NOERROR, id: 59978
;; flags: qr rd ra; QUERY: 1,
ANSWER: 1, AUTHORITY: 7, ADDITIONAL: 12
```

MX レコードがない場合

```
;; ---HEADER--- opcode: QUERY,
 status: NXDOMAIN, id: 59978
;; flags: qr rd ra; QUERY: 1,
ANSWER: 1, AUTHORITY: 7, ADDITIONAL: 12
```

5 おわりに

本研究の結果から，spam センサを活用すると，GK での適切な処理によって，spam メールの抑止に繋がることが考えられる．また，spam メールと，メールユーザーにとって重要なメールとの判別をすることが容易になり，メール使用の手助けになるのではないかと考えられる．そして，今後の研究課題として，以下の 2 点があげられる．

- インターネットを使った実験をし，spam メール対策を実用的なものにする．
- spam メールの中でも，一定期間内に大量のメールを送信してくる攻撃者への嫌がらせ

上記の研究課題を完成させることによって，spam メールの対策はより実用性が高まるであろうと考えられる．

参考文献

[1] 警察庁セキュリティポータルサイト@police: わが国におけるインターネット治安情勢の分析について (平成 20 年度第 1/四半期) (http://www.npa.go.jp/cyberpolice/detect/pdf/080723.pdf)(accessed April 2010)

[2] 中西 忠夫, 坂口 由佳：段階的通信制限システムの拡張, 卒業論文, 南山大学数理情報学部情報通信学科 (2008).

[3] THE SPAMHAUS PROJECT: SPAMHAUS (http://www.spamhaus.org)(accessed April 2010)

[4] 福井 麻美: 通信制限システムにおける TCP セッションの途中切替えと安全なリモートアクセス機能の実装, 修士論文, 南山大学数理情報学部情報通信学科 (2009).