通信制限の spam 送信抑制効果の評価

2008MI198 斉藤 啓介
指導教員　後藤 邦夫

1　はじめに

近年，PC，インターネットの普及により PC の利用年齢層の低下の傾向が見られる [5][6]． 本研究では迷惑メール対策として未完成である先行研究 [4] の中から，TCP のパケットロスによるスパムメール抑止力を minigk を使用して実験し評価することを目的とする．本研究は先行研究で実験されるはずであったが，スパムメール対策プログラムが完成しておらず，のメールの受信側で実行されるパケットロスで，スパムメーラーに送信を諦めさせる．

2　実験方法と実験環境

本研究での実験方法と環境，パケットロスプログラム minigk について，ここで説明する．**図 1** に全体的な流れを示す．PC1 のスパムメーラーが DNS サーバーより MX レコードを引き，PC2 にメールを送る．PC2 で受信したところを minigk で PC2 の SMTP サーバーに送られるパケットの横取りをする．

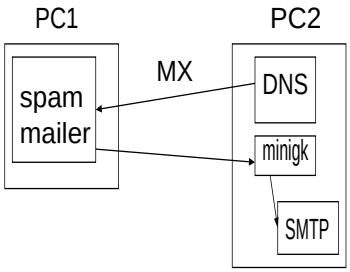

図 1　minigk の位置

2.1　実験方法

本研究では，クロスケーブルを用いた閉じた環境を作りだし，メールの送受信時に通信制限をすることでパケットロス時の効果を実験する．多くのスパムメールが世界的にシェアの多い Windows を対称にしているという想定のもとで実験を行う．実験環境として，Windows，Ubuntu を用いて実験する．クロスケーブルを用いて閉じたネットワークを実現する．IP アドレスを固定し，受信側である Ubuntu の方に DNS サーバーを構築する．メールの送受信を行い，受信側でメールのパケットロスをする．

2.2　minigk について

minigk とは後藤研究室で作成された GateKeeper(以下 GK と呼ぶ) [4][7] から，パケットロスする部分を抽出したプログラムである． minigk では GK での通信制限機能のパケットロス率の変化とホスト内部での動作が特徴で，本来の GK とは違い段階的通信制限機能はない．今回の通信では，IP ヘッダーのプロトコル番号 6，TCP ポート 25 の通信をパケットロスさせることでメール送信のみパケットロスする実験をした．また，minigk では SourceIP，DistinationIP を指定することができるが，設定無しにするとポート番号に該当する全通信をパケットロスする．今回は，特定の IP アドレスに対して攻撃するものであるが，どこから攻撃されるか分からないため，本研究では全通信を対象とした．

2.3　実験

今回実験をしたのは以下のメール送信パターンである．

- Linux から Windows

受信側の minigk を持つ方に DNS サーバーを構築し，スパムメーラーの内蔵 SMTP サーバーを利用することで，閉じた環境でのメール送信を可能とする．受信する側で minigk を起動させ，パケットロス率を変更させながら，スパムメーラーの動向を探る．

次に，スパムメーラーを利用し，大量に送信したメールに対して TCP でパケットロスを発生させる．スパムメーラーに関して一部をここで説明する．スパムメーラーの特徴としては，内蔵の SMTP サーバーや DNS サーバーを持ち手軽にメールを大量送信することができる．内蔵の機能以外にも外部 SMTP サーバーを利用することができ，多機能である．

- Rapid-Emailer[1]
  無料版で HTML を添付してメールの送信ができる．商品のニュースを大量に送るときに用いられる．
- Atomic Free Bulk Mailer[2]
  直接接続でメール送信をできる．
- Kingsmailer[3]
  自分で SMTP サーバーを構築することができる．

実験によって確認することは以下の 2 点がある．

- パケットロスによる通信制限で，スパムメーラーの送信は成功するか．
- 通信制限の中，スパムメールの送信に成功した場合，送信の可否に関わらず送信完了までどのくらい時間がかかり，メールの送信成功率はどのくらいなのか．

3　実行結果と評価

スパムメーラーごとによって差があるが，図 2 と図 3 に Atomic Free Bulk Mailer の実験結果を示す．この

結果は図 2 が 5 回のメール送信可否結果の平均値で，縦軸はメールの数，横軸はパケットロス率を示し，図 3 が縦軸は送信可否に関わらず送信完了まで時間，横軸はパケットロス率を示す．実験では，スパムメーラー内部の SMTP サーバーを用いて送信している．また，試用版を使っているため，同時送信可能数が 50 までと限られている．

次に送信までにかかった時間を**図 2** にメールの送信可否の平均値，**図 3** に送信可否に関わらず送信完了までの時間の平均値を示す．

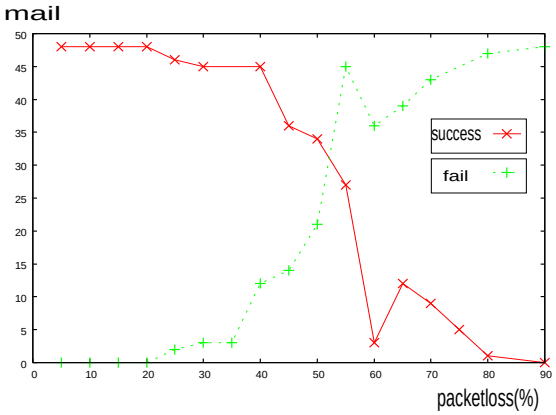

図 2　メール送信可否

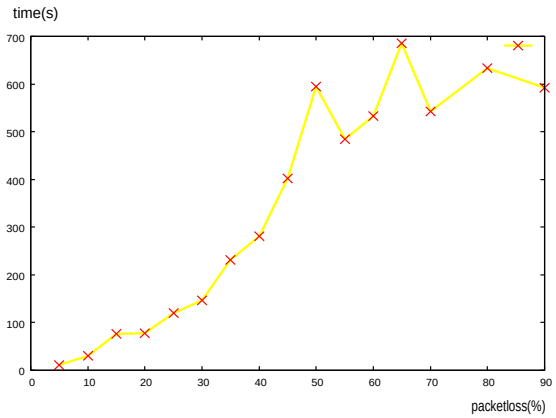

図 3　送信完了までの時間

送信結果のばらつきはメール送信可否が 1〜2，送信完了時間が平均値から 3〜5 秒と誤差はあまりなかった．スパムメーラーの送信失敗エラー出力によって，送信失敗は主に Time Out か Send error であったことがわかっている．これによりパケットロスにより，通信速度を遅くすることが証明できた．スパムメーラー本体の送信までの時間によって得られた結果からメール損失は確認でき，送信までの時間が minigk を使用する前よりも遅くなっている．50% 以上のパケットロス率でかなりの迷惑メール送信を遅くすることが可能となっており，送信を諦めるまで粘り強く送りつづけることが判明した．また，パケットロス率 90% 以上で送信ができなくなったため，送信を諦めることがあり諦めるまでの時間が増加していったことから，パケットロスにスパムメール抑止効果があると言える．

4　おわりに

本研究の結果から，スパムメーラーの対策として，パケットロスの手段は有効であり，スパムメール抑止に繋がることが考えられる．送信始めから終了までの時間は他のパケットロス設定よりも短くなっているところがあり，全て諦めるのが一番遅くなるというわけでは無い．

スパムメール対策の今後の課題として，以下の二点を挙げる．

- インターネット上でのメール送受信
  実際に使われている環境に近づけるためにも，実環境のメールサーバの設置は必須となる．
- メールでの自動段階的通信プログラムの完成
  自動で通信制限段階を判断し，処理リストの自動更新のできるプログラムが今後必要とされる．

これらの課題を実現するのがセキュリティの向上につながるといえる．

参考文献

[1] Absolute Futurity: Rapid-Emailer V2.0.2 (accessed Dec. 2011). http://www.absolutefuturity.com/rapid-emailer.htm.

[2] AtomPark Software Inc.: Atomic Mass Mailer Built in SMTP (accessed Dec. 2011). http://www.amailsender.com/massmailer/.

[3] SharewareDreams: Kingsmailer (accessed Dec. 2011). http://www.kingmailer.com/.

[4] 加藤雅斗，松本征也，南部勝巳：ゲートキーパーへの迷惑メイル対策機能の追加，卒業論文，2010 年度卒業論文，南山大学情報通信学科 (2010).

[5] 警察庁 National Police Agency：インターネットの観測結果等 (accessed Jun. 2011). http://www.npa.go.jp/cyberpolice/detect/pdf/20110428.pdf.

[6] 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) (accessed Jun. 2011). http://www.npa.go.jp/cyberpolice/detect/pdf/080723.pdf.

[7] 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，2009 年度修士論文，南山大学数理情報研究科数理情報専攻 (2010).