社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2006－CSEC－34 (27)
2006／7／20

BOTNETからのスパムメールに対する応答遅延方式の提案

関山 智也† 小林 義徳† 高橋 正和‡ 佐々木 良一†

†東京電機大学工学部 〒101-8457 東京都千代田区神田錦町 2-2
‡インターネットセキュリティシステムズ株式会社 〒141-0021 東京都品川区上大崎 3-1-1 JR 東急目黒ビル
E-mail: †{sekiyama, kobayashi}@isl.im.dendai.ac.jp, sasaki@im.dendai.ac.jp ‡mtakahashi@isskk.co.jp

あらまし 近年，スパムメールが増加している傾向にあり，そのことにより様々な問題が発生している．また，現在ではBOTNETを利用したスパム送信方法が主流となっており，全体の約8割を占めるとも言われている．このBOTNETを利用したスパムメール送信方法は従来の対策では防ぐことが難しいという特徴がある．本研究では，BOTNETを利用したスパムメール送信に対する対策として，応答遅延を利用した対策を提案する．また，評価を行った結果，その効果は局地的なものではなくネットワーク全体的に見て効果があることが確認出来たので報告する．
キーワード BOTNET，スパムメール，遅延，ネットワークセキュリティ，コンピュータウィルス

A Proposal of Response Delay Method for Spam Mail from BOTNET

Tomonari SEKIYAMA† Yoshinori KOBAYASHI† Masakazu TAKAHASHI‡ and Ryoichi SASAKI†

† School of Engineering, Tokyo Denki University 2-2 Kandanishikicho, Chiyoda-ku, Tokyo,101-8457 Japan
‡ Internet Security Systems K.K. JRtokyumeguroBuilding, 3-1-1 Kamioosaki, Shinagawa-ku, Tokyo,141-0021 Japan
E-mail: †{sekiyama, kobayashi}@isl.im.dendai.ac.jp, sasaki@im.dendai.ac.jp ‡mtakahashi@isskk.co.jp

Abstract Recently, increasing spam mails have been becoming causes of many problems. About 80 % of spam mails have been sent from BOTNET. It is difficult to decrease the bad influence caused by the spam mails from BOTNET with existing anti spam system. Therefore, in this paper we propose the method named Response Delay Method to protect from the spam mail from BOTNET. Additionally, we report the evaluated result which shows that the method has an effect on not only a part of network but also the network whole.
Keyword BOTNET, SPAM, delay, Network Security, Computer Virus

1. はじめに

近年，インターネットや携帯電話が急激に普及し仕事や日常生活にメールを使うことが多くなった．そのことにより今まではチラシや手紙などで送られていたダイレクトメールを，コストがかからず簡単に使用できるメールで送るようになり急激にスパムメールが増加した．この影響でプロバイダのメールサーバに過剰な負荷が掛かり，システムがダウンするなどの深刻な影響が出ている．また，企業などでは受信するメールの7割から8割はスパムメールであるとも言われており[1]，大量のメールから必要なメールを探し出すために時間がかかり，仕事に支障が出るなどといった事も起きている．さらに最近ではスパムメールがフィッシング詐欺のために利用される事も多くなってきており，今後はさらに被害が拡大することが予想される．

スパムメールの主な対処として，フィルタリングを行い，メールの受信者が見なくてすむようにしているが，この対策だけでは，サーバへの負荷やネットワークの負荷が増大する問題は解決できない．

一昔前，スパム送信者は第三者中継メールサーバを利用してスパムメールを送信することが多かったが，最近では BOTNET というネットワークを使い送信するようになった．2003 年の夏ごろからこの BOTNET を使ったスパムメールが主流となり現在のスパムメールの7割から8割はこの BOTNET を介して送られていると言われている[2]．

そこで，本研究では BOTNET を介して送られてくるスパムメールによって，サーバへの負荷やネットワークの負荷が増大する問題の対策として，応答遅延方式という方式を提案し，その評価を行った．この方式はスパム送信者との SMTP 通信の応答に遅延時間を設けることによって，スパムメール流量を低減させるもので，その効果は局地的なものではなくネットワーク全体的に見て効果がある．

2. BOTNET とは

BOTNET とは，攻撃者が作り出すネットワークのことで，図 1 にあるように攻撃者，攻撃者の命令を送信する指令サーバ，BOT に感染した PC 群で構成される．

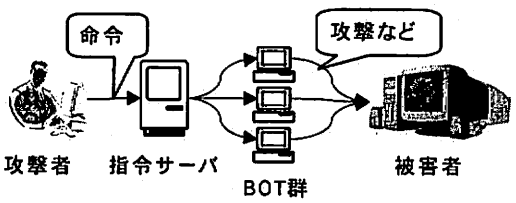

図 1　BOTNET 概要

ここで BOT とは攻撃者からの命令を受けその命令に従って動作をするプログラムであり，「DDoS 攻撃」，「BOT 本体の更新」，「スパムメール送信(中継)」，「特定の広告の参照」，「キーロガー」など様々な機能が実装されている．命令の通信は IRC プロトコルが使われることが多く，この場合指令サーバが IRC サーバ，BOT に感染した PC 群は IRC クライアントとして動作する．攻撃者はこのネットワークを利用し上記のような様々な悪事を働くことが出来る[3]．

この BOT プログラムには様々な亜種が膨大に存在し，前述したように BOT 本体の更新機能があることも多く頻繁に更新が行われるため，アンチウィルスソフトなどによる検知が難しくなっている．

また，最近ではこの BOTNET をスパムメール送信業者に貸し出すことが商売になっているとも言われており，そのことが BOTNET を利用したスパム送信の増加の要因の一つだと考えられる[4]．ちなみに BOTNET を利用したスパム送信は，下記の図 2 のようになっており，SPAMMER は BOT をプロキシとして利用してメールを送っていると考えられている[4]．

BOTNET を利用したスパム送信では，従来多く見られた第三者中継メールサーバを利用したスパムメール送信のように一箇所から大量のメールを送信するのではなく，多くの PC から少量ずつスパムメールが送られてくるため，発信元の PC を突き止めることが難しいといった特徴がある．さらに，PC を突き止めたとしても一般の PC であるため IP が変わってしまうことも頻繁にあると考えられ，特定がさらに困難になっている．

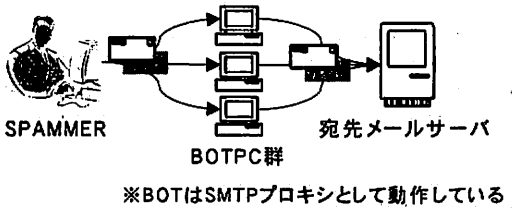

図 2　BOTNET を利用したスパム送信

さらに，この BOTNET を利用したスパム送信方法は，最近注目されているスパムメール対策である「Outbound Port 25 Blocking」(以下 OP25B) [5]を回避することも可能になっている．OP25B とはユーザが所属 ISP のメールサーバを経由せずに，直接外部にメール送ろうとする通信（宛先のポートが 25 番ポート）を遮断する対策のことである．下記の図 3 のように ISP A のメールサーバにメールを送るときは同じ ISP A 内の BOT だけを利用し，BOT と SPAMMER との間の通信に 25 番ポート以外を使えば OP25B を回避することが可能である．

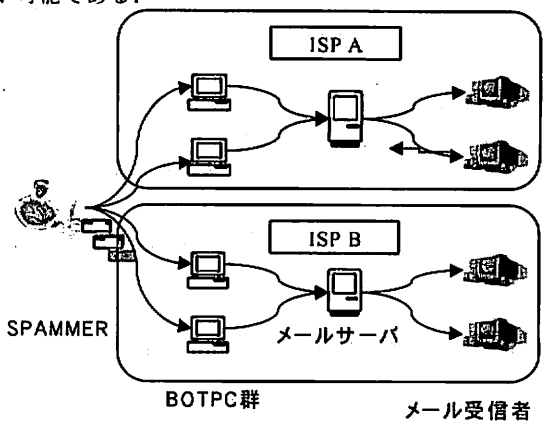

図 3　OP25B 回避方法の例

3. 提案方式

1 章で説明したように，近年スパムメールが非常に問題になっており，そのスパムメール送信の主流になっているのが BOTNET を利用したスパムメール送信方法である．そこで，本研究ではこの BOTNET を利用したスパムメールの流量を減らすことを目的に，応答遅延方式という対策を提案する．この対策において，スパムメールの流量の減少は局地的なものではなく，ネットワーク全体的に見て効果があることが大切であると考えている．なお，この対策はスパムメールを受信するメールサーバで実装する対策である．

3.1. 提案方式の特徴

2 章で述べたような BOTNET の特徴をふまえ，これに対応する為に以下のような特徴を持った方式を考案した．概要を以下に示す．

(1) コンテンツフィルタリングによるスパムチェックでスパムメールの送信元を判別し，不審者リストに登録する
(2) 不審者リストに載っている PC との通信の応答に対して遅延時間を設ける

ここで，(2)について切断や拒否ではなく遅延時間を利用するという事が本研究の特徴である．遅延時間を利用する理由は以下の点で有利であると考えられるためである．

(a) メールサーバの負荷
(b) ネットワーク全体のスパム流量
(c) 正規ユーザへの影響

(a)ついて考えると，切断した場合クライアントは直ぐに次のコネクションを張ろうと試みることが予想される．ここでサーバではさらに切断をするので，この動作が繰り返されコネクション要求が多発し，その結果としてサーバの負荷が上がってしまうことが考えられる．

これに対し遅延時間を設けた場合を考えると，クライアントは応答が来るまでの間（遅延時間分）何もせずに待機することになり，次のメールを送信するためにコネクション要求を出すといったことが出来ない．このため，メールサーバの負荷においては切断よりも有利だと考えることが出来る．ただし，遅延の場合でもスパムチェックを行うことにより余計な負荷が掛かるため対策を取らなかった場合と比べると負荷が上がる可能性がある．

(b) ついて考えると，下記図 4 のように宛先メールサーバが複数ある場合，他のメールサーバに対して直ぐに次のメールを送信できるため，ネットワーク全体としてみるとスパムメール流量があまり減らないという事態が予想される．これに対し遅延時間を設けた場合は，クライアントは応答が来るまでの間何もせずに待機することになるので，次のメールを送信することが出来ない．よってネットワーク全体のスパム流量においても切断より有利だと考えることが出来ると考えられる．

(c) ついて考えると，切断では正規ユーザが誤って不審者リストに登録されてしまったら全くメールを送信できなくなってしまうのに対し，遅延の場合は少量であればほぼ問題なくメールを送信出来る．一般の正規ユーザは一度に大量のメールを送信することは少ないと考えられるため影響はほとんどないと考えられる．

これらの 3 つの点を確認するため，実際にプログラムを開発し，実験により確認する．

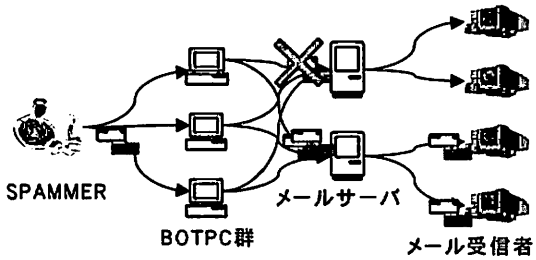

図 4　スパム送信の例

3.2. 提案方式の処理フロー

次に，提案方式を実装したメールサーバのフローを説明する．フローの概要は下記の図 5 に示した通りである．図中のホワイトリストは IP を要素として持っており，不審者リストは IP と時刻を要素として持っている．

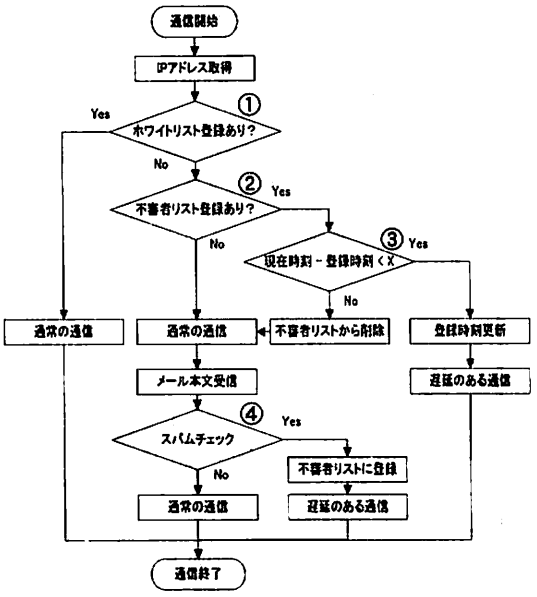

図 5　実装メールサーバのフロー

まず，クライアントと提案方式を実装したメールサーバとの間で通信が開始されると，サーバではクライアントの IP アドレスを取得する．次に，その IP アドレスがホワイトリストに登録されているかどうかをチェックし（図 5 ①），登録されているようならば通常の通信を行って通信を終了する．ホワイトリストにはメールサーバに大量にメールを送ってくると予想されるプロバイダなどのメールサーバの IP アドレスを登録しておく．大量にメールを送信してくるメールサーバとの通信に対して遅延が生じてしまうと，そのメールサーバではメールをなかなか送ることが出来ずに溜め込んでしまうということが起こりえる．そういった事態を回避するためにこのホワイトリストを用いた処理は必要になる．

次に，IP アドレスがホワイトリストに登録されていなかった場合は（図 5 ①），その IP アドレスが不審者リストに登録されているかどうかをチェックする（図 5 ②）．不審者リストに登録されていなかった場合はメール本文のデータを受信するまでは通常の通信を行い，本文のデータに対してスパムチェックを行う（図 5 ④）．ここでスパムと判定された場合は，IP と現在の時刻を不審者リストに登録し，その後遅延のある通信を行い，スパムでないと判定された場合は通常の通信を行う．

また，不審者リストに登録されていた場合は（図 5 ②），次に現在の時刻とリストに登録されている時刻の差を計算する（図 5 ③）．ここで，この時刻の差が一定時間以上であると，その IP は変化していまっている可能性が高いと判断し，不審者リストに登録がなかっ

た場合と同じ処理を行う．時刻の差が一定時間未満であった場合はその IP は変化していないであろうと判断し，不審者リストの登録時刻を更新してその後遅延のある通信を行う．

3.3. 提案方式の処理フロー

上記 3.2 節「提案方式の処理フロー」にも「遅延のある通信」とあったように，提案方式ではメール送信の通信に対して遅延時間を設ける処理を行う．ここではこの「遅延のある通信」がどういったものであるかについて説明する．概要を下記の図 6 に示した．

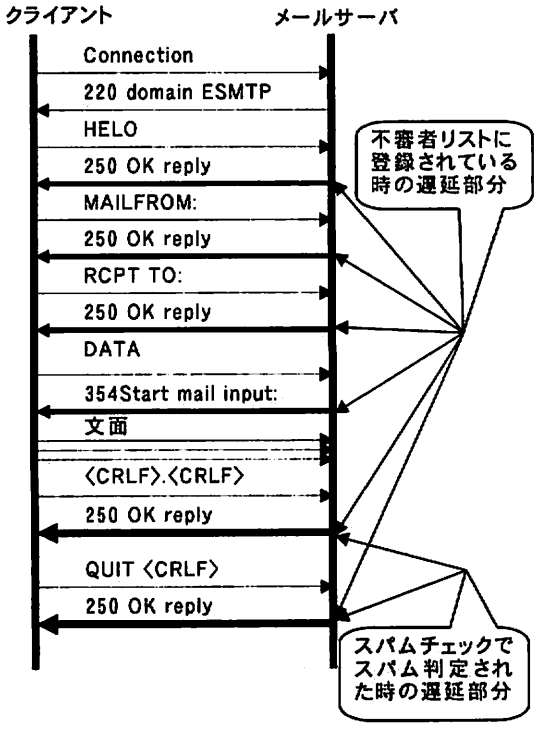

図 6　通信の様子

図 6 は提案方式を実装したメールサーバとクライアント間の通信の様子を表したもので，SMTP と呼ばれるプロトコルに基づいて通信を行っている．メールサーバではクライアントから「HELO」や「MAIL FROM:」といったコマンドを受け取った後，それに対しての応答を返すまでの間に遅延時間を設ける．ここで，遅延時間を設ける箇所を一箇所ではなく，全てのコマンドに対する応答に分散させることで，クライアントがタイムアウトで切断してしまうといった事態が起こりにくくなるようにしている．

また，3.2 節「提案方式の処理フロー」で説明した内容には，「遅延のある通信」が不審者リストに登録されていた場合と，スパムチェックでスパムと判定された場合の 2 種類があった．図 6 にあるように，不審者リストに登録されていた場合は，全ての応答に遅延時間を設けることが出来るが，スパムチェックでスパムと判定された場合は，メール本文を受信してスパムチェックをする段階が図中の「<CRLF>.<CRLF>」の後であるため，その後の 2 つの応答のみに遅延時間を設けるようになっている．

4. 実験

提案方式の有用性を証明するために実験を行った．ここでは対策なしや遅延ではなく切断した場合に対する，本提案方式を利用した場合の有用性の検証を行う．

4.1. 実験概要

下記の図 7，図 8 のような 2 つの実験モデルを構成し実験を行った．図 7 は宛先メールサーバに対して経由させる BOT を特に意識しないモデル．図 8 は宛先メールサーバに対して経由する BOT を特定の BOT にするという OP25B の回避を想定したモデルである．また，BOTPC 群と一般ユーザ群にはそれぞれに 30 台の PC があるという想定になっている．

実験方法は 2 つの実験モデルにおいて，実験用メールサーバにて，提案方式を実装した場合，切断の場合，対策なしの場合の 3 種類を変化させ，実験用メールサーバや SPAMMER に及ぼす影響を測定した．ここで，SPAMMER は実験用メールサーバで対策なしの場合に 3 つのメールサーバに均等にメールが送られるよう BOT を経由してメールを送信する．また，今回の実験ではスパムチェックに bsfilter[6]というベイズ理論に基づくフィルタリングツールを利用し，SPAMMER が送信するメールを正常だと誤判定する確率を 10%，一般ユーザのメールをスパムだと誤判定する確率を 15%という設定で実験を行った．

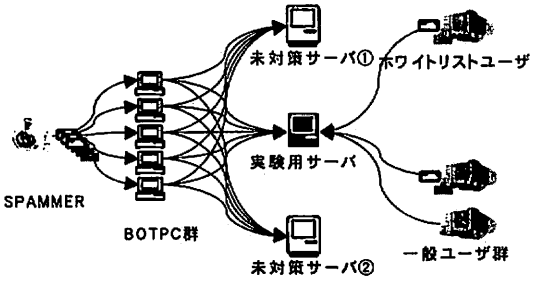

図 7　実験モデル①

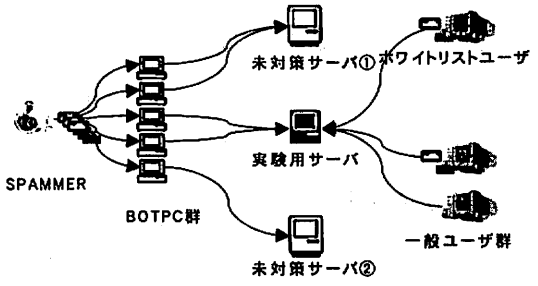

図 8　実験モデル②

4.2. 実験機材

実験にはそれぞれ以下の用途で計 11 台の Windows マシンを用いた.

- SPAMMER 用 PC(WindowsXP 1 台)
- BOT 用 PC(WindowsXP 3 台)
- 一般ユーザ用 PC(WindowsXP 2 台)
- 一般ユーザコントロール用 PC(WindowsXP 1 台)
- ホワイトリストユーザ用 PC(WindowsXP 1 台)
- 実験用サーバ用 PC(WindowsXP 1 台)
- 未対策サーバ用 PC(WindowsXP 2 台)

BOT 用 PC と一般ユーザ用 PC には 1 台の PC に複数の IP を割り当て, それぞれ PC が 30 台あるようなモデルを仮想的に構成した.

4.3. 実験用ソフトウェアの開発

この実験を行うにあたり幾つかのソフトウェアを用意する必要があったので, 以下のソフトウェアを開発した. 開発したソフトウェアとその概要を以下に示す.

1. 提案方式を実装したメールサーバ
   - メールサーバソフト XMAIL を改変
   - PostgreSQL と連携
   - スパムフィルタソフト Bsfilter の組込み
   - 言語 : C++ (Microsoft VisualStudio.Net2003)
   - 開発ステップ数 : 約 300 ステップ
2. 提案方式で遅延ではなく切断するメールサーバ
   - 同上
3. SPAMMER 用ソフトウェア
   - 言語 : Java (J2SDK 1.4.2_10)
   - 開発ステップ数 : 約 2200 ステップ
4. BOT 用ソフトウェア
   - 言語 : Java (J2SDK 1.4.2_10)
   - 開発ステップ数 : 約 1200 ステップ
5. CPU 使用率測定ソフトウェア
   - 言語 : C++ (Microsoft VisualStudio.Net2003)
   - 開発ステップ数 : 約 300 ステップ

なお, 4 の BOT 用ソフトウェアは簡単な TCP プロキシソフトウェアで, TCP セッションを中継するだけのソフトウェアである. 3 の SPAMMER 用ソフトウェアは実際の SPAMMER が行っていると考えられる基本的なメール送信処理と実験結果を得るためのデータを取得収集するソフトウェアである.

4.4. 実験方法

まず, 様々な測定を行う前に実験用メールサーバで対策なしの場合に, 下記図 9 のように SPAMMER とそれ以外のメール流量がそれぞれ毎秒約 3 通, 毎秒約 1.5 通になるような効率で実験用メールサーバにメールが送信されてくるように SPAMMER や一般ユーザ, ホワイトリストユーザのメール送信パラメータを設定した. これは, SPAMMER の送るメール流量がネットワーク全体のメール流量に対して約 66%となるように設定してある. このような割合で設定した理由は, [1]などさまざまなニュースサイトに見ると, 企業などで受信するメールのうちスパムメールが締める割合が約 7 割といったような記事が多かったためであり, これらを参考にして約 66%という想定で実験を行った.

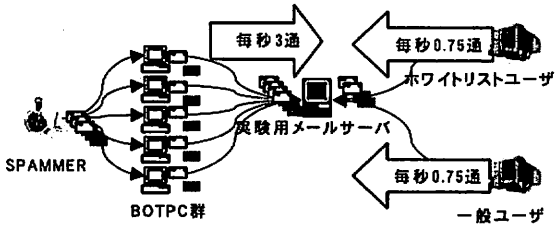

図 9 設定送信効率

次に, 先に設定したメール送信パラメータ設定を用い以下の各測定パターンで 5 分間ずつメールを送り続け, 測定項目を測定した.

- 測定パターン
  - (1) 対策なし
  - (2) 切断方式
  - (3) 提案方式
    - 遅延時間 250ms
    - 遅延時間 500ms
    - 遅延時間 1000ms
- 測定項目
  - (1) 各サーバへの SPAMMER のメール送信効率
  - (2) 実験用メールサーバへのホワイトリストユーザおよび一般ユーザの送信効率
  - (3) 実験用サーバでの CPU 使用率

4.5. 実験結果

実験結果は下記の 4 つの表のようになった. 表 1, 表 2 はそれぞれの 2 つのモデルにおいて実験用メールサーバへ送られてくるメールの平均送信効率 (単位時間当たりに送信されるメール数) と平均 CPU 使用率を各測定パターン別に比較した表であり, 表 3, 表 4 は SPAMMER の各サーバへの平均送信効率とその合計を比較した表である. また図 10 は SPAMMER の送信効率と提案方式を実装した場合の遅延時間の長さの関係をグラフにしたものである.

表 1 実験用サーバへの影響比較 (モデル①)

対策方式 / 測定項目	対策なし	切断方式	提案方式		
			遅延 250ms	遅延 500ms	遅延 1000ms
SPAMMER [通/s]	2.87	0.013	1.2	0.79	0.49
ホワイトリスト [通/s]	0.67	0.67	0.68	0.67	0.68
一般ユーザ [通/s]	0.67	0.35	0.65	0.63	0.62
CPU 使用率 [%]	9.34	17.1	11.1	10.8	10

※ 2～4 行は実験用サーバへの平均送信効率
※ 5 行は実験用サーバの平均 CPU 使用率

表 2　実験用サーバへの影響比較（モデル②）

対策方式 / 測定項目	対策なし	切断方式	提案方式		
			遅延 250ms	遅延 500ms	遅延 1000ms
SPAMMER [通/s]	2.98	0	1.13	0.71	0.43
ホワイトリスト [通/s]	0.67	0.67	0.67	0.67	0.67
一般ユーザ [通/s]	0.67	0.32	0.64	0.61	0.63
CPU 使用率 [%]	9.37	16.53	12.13	10.08	9.04

表 3　SPAMMER の送信効率比較（モデル①）

対策方式 / 測定項目	対策なし	切断方式	提案方式		
			遅延 250ms	遅延 500ms	遅延 1000ms
未対策サーバ① [通/s]	2.8	3.43	1.17	0.71	0.41
未対策サーバ② [通/s]	2.86	3.5	1.18	0.72	0.49
実験用サーバ [通/s]	2.87	0.01	1.2	0.79	0.49
ネットワーク全体 [通/s]	8.53	6.54	3.55	2.22	1.39

※SPAMMER の各サーバへの平均送信効率とその合計

表 4　SPAMMER の送信効率比較（モデル②）

対策方式 / 測定項目	対策なし	切断方式	提案方式		
			遅延 250ms	遅延 500ms	遅延 1000ms
未対策サーバ① [通/s]	3.03	3.65	1.29	0.88	0.53
未対策サーバ② [通/s]	3.05	3.64	1.28	0.88	0.52
実験用サーバ [通/s]	2.98	0	1.13	0.71	0.43
ネットワーク全体 [通/s]	9.06	7.29	3.7	2.47	1.48

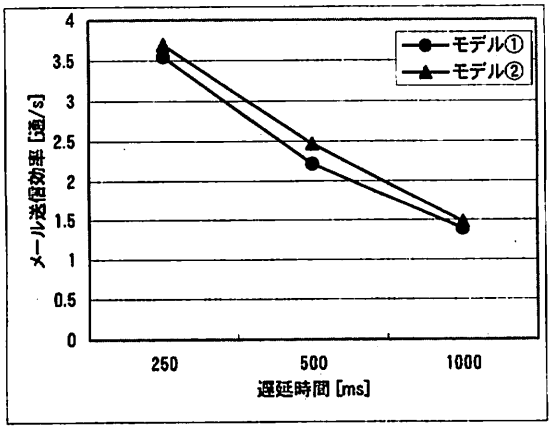

図 10　遅延時間と SPAMMER の送信効率の関係

表 1（モデル①の場合）を見ると，切断方式の場合は，SPAMMER からのメール送信効率は約 0 通/s となりほとんどなくなっているが，CPU 使用率は対策なしの場合に対して 1.83 倍と大きく上がってしまっていることが分かる．それに対して提案方式を実装した 3 つのパターンは SPAMMER からのメール送信効率が対策なしの場合に対して 0.17～0.42 倍と下がっていることに加えて，CPU 使用率は 1.07～1.19 倍とそれほど上がっていないことが分かる．また，SPAMMER からのメール送信効率は遅延時間が長いほどより下がっているということも分かる．さらに，一般ユーザに注目して見ると，切断方式の場合は送信効率が半減してしまっているが，提案方式の場合はほとんど変化がないことが分かる．これらの結果は表 2（モデル②の場合）でも同様である．

次に表 3 を見ると，切断方式の場合は対策なしの場合と比較して，SPAMMER から実験用サーバへの送信効率が約 0 通/s となりほとんど送れなくなっている．しかし，その他の 2 つの未対策サーバへの送信効率が上がってしまい，ネットワーク全体としてみると送信効率が対策なしの場合に対して 0.77 倍とあまり下がっていないことが分かる．それに対して本提案方式を実装した 3 つのパターンは実験用サーバだけでなく，その他 2 つの未対策サーバへの送信効率も低下しネットワーク全体で 0.16～0.42 倍とかなり送信効率が抑えられているということが分かる．これらの結果は表 4（モデル②の場合）でも同様である．また，図 10 を見るとネットワーク全体の送信効率はモデル①，モデル②共に遅延時間が長いほどより下がっていることが分かる．

5. 評価

実験結果より，未対策の場合や切断した場合と提案方式を比較すると表 5 のように整理することができる．これは 3 章の仮定した内容とほぼ同じ傾向になっている．

表 5　提案方式の比較評価

対策方式 / 評価項目	対策なし	切断	提案方式
メールサーバの負荷	○	×	△
ネットワーク全体のスパムメール流量	×	△	○
正規ユーザへの影響	○	×	○

メールサーバの負荷という点は表 1，表 2 の CPU 使用率の項目を見ると，切断した場合のように大幅に上がってしまうことは無いものの若干上がってしまったため，今後改善する必要がある．

ネットワーク全体のスパムメール流量という点は表 3，表 4 をみて分かるように提案方式の場合が最も低減させることが出来たので有用性があると考えることが出来る．また図 10 から遅延時間が長いほど有効で

あるということも分かる．

正規ユーザへの影響という点は表 1，表 2 の一般ユーザの項目をみると，切断した場合に送信効率が半減しているのに対し，提案方式ではほとんど送信効率が低下しなかったため，問題ないと考えられる．

また，提案方式を実装した場合にメールサーバの負荷が若干上がること関しては，現在スパムチェックソフトとして利用している bsfilter による負荷が問題だと考えられる．今回の実験結果から，通常のメールに対するスパムの誤検知率が 15%と高くても，一般ユーザにはほとんど影響がないことがわかったので，bsfilter よりも若干精度が低くても，負荷が少ないアルゴリズムを採用しているスパムフィルタソフトなどを利用すれば，対策なしの場合よりも負荷を少なくすることが出来るであろう．なお，ここでスパムチェックソフトは提案方式のためだけに利用されることを前提としている．フィルタリングによるメールの拒否やスパムの振り分けなど従来の目的のために利用する場合は，別途他の精度の高いソフトを使う必要があるだろう．

6. 類似研究との比較

本論文における提案方式を考案した後に，文献を調査したところ，類似の方式を提案している論文が見つかった[7]．ここではその論文と本論文の違いについて説明する．

まず，我々の研究は BOTNET を利用したスパムメールに対する対策という目的であるのに対して，[7]では従来の第三者中継メールサーバなどを使ったスパムメールなどが対象となっている．次に，我々の研究では受信側の負荷やネットワークに対する負荷も考慮した内容となっているが，[7]は後述するようにそういった内容にはなっていない．

[7]では我々と同様に応答遅延という処理を行っているが，我々は SMTP の応答に遅延時間を設けているのに対して，[7]では TCP レベルでの遅延を行っていて，ウインドウサイズを小さくして TCP の ACK に対して遅延時間を設けるといった処理になっている．一般的に TCP レベルのタイムアウトは SMTP と比較してタイムアウトになる時間が非常に短く，長い時間遅延を入れることが出来ないため，ウインドウサイズを小さくすることで ACK の回数を増加させ，それに対して遅延を入れることで合計の遅延時間を長くさせるとともに，送信者にフラグメントによる負荷をかけてしまおうという内容になっている．この対策を，BOTNET からのスパムメールに対してとることを考えると問題となる点が幾つかある．まず，ウインドウサイズを小さくすることにより送信者に負荷をかけるという点だが，BOTNET を利用する場合は，BOT となっている PC に負荷がかかるだけであり，SPAMMER には影響を及ぼさないばかりか，受信側で細かく区切られたデータを再構築するために余計な負荷が掛かってしまうことが考えられる．またネットワークにも余計な負荷が掛かってしまうという欠点も考えられる．

また[7]ではスパムフィルタによって TCP に遅延を入れたりする対象を判定すると書いてはあるが，それらを含めた実験や評価は行わず，先に説明した TCP に関する処理のみの実験や評価しか行っていない．それに対し，本論文では全体的なシステムの実装とそれを用いた実験，評価を行っているのでその点でも本論文には新規性があると考えられる．

7. おわりに

本論文では，BOTNET を介して送られてくるスパムメールに対する対策として，ネットワーク全体的に見て効果があることが大切であるという考えを基に，応答遅延方式という対策を提案し，その評価を行った．その結果，提案方式に有用性を示すことが出来た．

今後は，SPAMMER が取り得る送信パターンや，送信パラメータの変化などに関して調査，考察し，提案方式の改善や追加実験をしていくことを考えている．

文　献

[1] 日経 BP 社，“迷惑メール防止策レポート，”日経コミュニケーション特別広報別冊，Oct.2005. http://www.nikkeibp.co.jp/sj/report/27/

[2] 勝村 幸博，“スパムの 75%以上は“ゾンビ”から送られてくる，” ITPro，Dec.2005. http://itpro.nikkeibp.co.jp/article/NEWS/20051215/226337/

[3] 警察庁 @police，“ボットネット(botnet)に注意，”分析レポート，Jan.2005.

[4] 小山 覚，” ボットネット実態調査結果 "Our security depends on your security.", " Black Hat Japan 2005，Tokyo，Japan，Oct.2005.

[5] JEAG(Japan Email Anti-Abuse Group), "Outbound Port25 Blocking についての JEAG recommendation, " Feb. 2006.

[6] nabeken，“bsfilter/bayesian spam filter/ベイジアンスパムフィルタ，” Mar. 2006. http://bsfilter.org/

[7] Kang Li, Calton Pu, Mustaque Ahamad, "Resisting SPAM Delivery by TCP Damping, " Conference on Email and Anti-Spam, California, USA, Jul.2004.

[8] http://itpro.nikkeibp.co.jp/article/COLUMN/20051007/222473/