# ボットネットワーク対策について

武藏 泰雄[†]

[†]熊本大学総合情報基盤センター・ネットコミュニケーション研究部

**概要:** ボットネットワークとは、コンピュータウィルスやワーム等に乗っ取られた PC によって構成される分散クラスタリングネットワークの総称です。最近のネットワークセキュリティ研究分野では、ボットネットワークの対策技術が重要になって来ておりまして、本報告では、ボットネットワークを構成するボットについての簡単な説明と、本大学におけるボットネットワーク対策の今後について議論していきたいと思います。

## 1. 背景

コンピュータセキュリティあるいはネットワークセキュリティ研究分野において、最近ボットネットワークが注目されています[1-5]。ボットネットワークとは「ボット」呼ばれるウィルスのワーム感染によって乗っ取られた PC によって構成される、一種の分散クラスタ型ネットワークの総称です。ボットネットワーク構成するボットは一般の通常 PC である場合が多いと言われています。それは多くの理由が考えられ、インターネット上の多くのサーバについてはセキュリティ対策が十分とは言えませんが、情報漏洩事件の頻発や個人情報保護法の施行、それに情報セキュリティ管理システム（ISMS）の ISO 化等でプロアクティブな対策の重要性が一般に浸透して来ており、PC に比べ、サーバは攻撃しにくくなったためと、また相対的に見て管理の甘い PC は、管理の甘いサーバに比べれば圧倒的その数に多いためであると考えられます。

ボットネットワークのボットとは、「ロボット」の「ボット」であり、操り人形のことを指します。つまりウィルスのワーム活動で次に犠牲になる PC（犠牲端末または犠牲 PC と言う）をネットワーク上で探索し、管理が甘い点（ システムの欠陥）を攻撃して、PC 内部に侵入させ、そして乗っ取りが成功したらコントローラ（人形師）にインターネットリレー（IRC）等を介して通知し、次の指示を待つ状態になります。コントローラは、ボットと化した犠牲 PC を分散システムとして連結（クラスタリング）してボットネットワーク単位で操作できるようにします[1-3]。

ボット化した PC から発見されたウィルスを解析することにより、ボットには様々なセキュリティ上問題がある機能が搭載されていることが知られるようになりました。例えば、(1) サービス妨害(DoS)攻撃用の基地（踏台とも言う）としての機能や、 (2) 機密情報や個人情報の盗聴・漏洩（スパイ的活動）、及び(3)迷惑メールの発信・中継等の機能が代表的なものです[1-3]。(1)については、2002 年末～2004 年前半に DoS 攻撃が本大学でも多く検知され、その対策を行った経緯があります。一つはボット化した PC から他組織や機関を DoS 攻撃した例や本大学の DNS サーバが逆引きアクセスの集中攻撃を受けた例があります[6]。(2)については、個人情報保護法の施行前に盛んにボットネットワークの開発が行われていた形跡が見出されています。例えば 2005 年 2 月には W32/Mytob.A[7] ボットワーム型ウィルス（ボットワームと言う）が発見されています。このボットワームの製作者は 2005 年 8 月ごろに W32/Mytob の発展版である W32/Zotob[8]をリリースした直後にトルコ及びリビア警察当局に逮捕されています。(3)の迷惑メールについては、著者も頭痛めているものの一つであり、ある程度の対策的な解決しなければならないものの一つです。最近のインターネット上の E-mail に関するトラフィックにおいて 60～70%が迷惑（spam）メールと言われている。メールサーバ側や PC 側でパッシブなフィルタリング対策等が行われ良好な結果を得ているものの、それでも一向に迷惑メールはなくなりません。それらの多くの理由の一つにボットネットワークの関与が挙げられます[1-3]。

この迷惑メールの機能を理解するために、どの様に迷惑メールが配送されるのか考えてみます。以前はメールサーバ側で第三者中継を前もって（プロアクティブに）防ぐことで、一時的に迷惑メールを撲滅できると考えられました。しかし 2004 年 3 月から流行した W32/Netsky.Q[9]大量メール送信型ワーム（MMW）に代表されるように、独自のメールサーバ機能を持つウィルス・ワームが広く拡散するようになりました。このメールサーバ機能を一般に SMTP エンジンと呼ぶことがあります。この SMTP エンジンがボットワームに組み込まれていることが最近の研究結果で判明しています[1,3]。

今回は特にボットネットワークに組み込まれている SMTP エンジンについて、我々の最近の研究をご

紹介し、ボットネットワークから発信される迷惑メールを以下に速やかに検知し、どう対策するかについて議論したいと思います。

## 2. 迷惑メールの種類

迷惑メールは、spam メールとウィルス付メールの 2 種類に大別できます。

### 2.1 spam メールついて

Spam メールは、現在では ICT 化社会における最もポピュラーで、しかも悩ましいものの一つです。メールソフトを起動すると、そのほとんどが spam メールと称する、未承諾広告メール、ドラッグやポルノサイトへの勧誘、フィッシング（詐欺）メールであり、いちいち手で消すのが面倒な朝の日課になってしまっている人も多いと思います。著者も御多分に漏れず数百通から多い時は数千通にもなります。ある程度フィルタを入れてはいますが、それでも spam だけしか受信してない事もよくあります。

初期の段階の spam メールの発信源はインターネット上のメールサーバを悪用する、所謂第三者（不正）中継が常套手段だったため、メールサーバに組織外からの中継設定をやめる様に努力した結果、相当な割合で spam メールの発信源を減らすことができる様になりました。しかし spam メールは一向減らず、次々とやってきます。確かに第三者中継そのものは、その対策方法が広く浸透したこと、メールサーバプログラムが初期の設定で第三者中継をしないようになったことで、設定に不備のあるメールサーバは減少していますが、対策が進むつれ設定に不備のあるメールサーバを探す努力が spam メール発信者の努力で続けられ、最終的には管理の甘いサーバを乗っ取りそこから発信する様になりました。大学や企業の様な組織では、各部署や研究室にファイルやメールサーバが稼動している場合があり、意外と管理が甘いものが多く、結局それが spam メールを存続させる一因となっていました。

現在では、これらの管理の甘いメールサーバも spam フィルタ等を導入して対策を施した結果、次第に減ってきています。しかし spam 発信者は、今度は、ボット化された PC から spam メールを発信する様になっています。さて、ここで気づかれたかと思われますが、この乗っ取られた PC を見つけること自体がボットネットワークの技術的対策の一つになります。その鍵を握るのは、次節で説明する大量メール送信型ワームに関する DNS 流量の解析から明らかになります[11,12]。

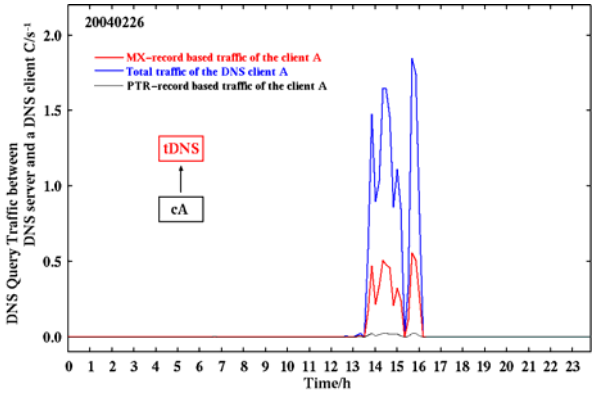


**Figure 1.** Traffic of the DNS query access between the top domain DNS server and the DNS client A through February 26th, 2004. The blue, black, and red lines show the total-, PTR-, and MX-record based DNS traffic, respectively ($s^{-1}$ unit).

### 2.2 大量メール送信型ワームの DNS 流量解析

大量メール送信型ワームとは、電子メールの添付ファイルを悪用して送信先の PC 等にウィルス自身を感染させるウィルスの一種です。また感染すると大量のウィルス付メールを送信するため、大量送信型ワームまたはマス・メーリング・ワーム（MMW）と呼ばれています。次に大量メール送信型ワームの種類について分類したいと思います。

初期型の大量メール送信型ワーム（MMW）は、ドメインネームシステム（以下 DNS と言う）サーバに登録された正統なメールサーバに、ウィルスを添付したメールを中継させて拡散するものが主流でした。これをサーバ依存型 MMW と呼びます。サーバ依存型については、spam メールの不正中継の防止設定と同様に、サーバの中継時に第三者中継かどうか調べること、またサーバにウィルス駆除ソフトを導入することによりかなり割合でその拡散を防ぐことができるようになりました。つまり初期の spam メール対策と似たような対処方法を採用することにより防げたのです。しかしメール型ウィルスは更にそのワーム活動を進化させます。

第二世代の大量メール送信型ワームは、サーバ依存型ではなく、独自にメールサーバ機能を持つものでした。つまり正統なメールサーバを介さず、直接次の犠牲 PC の所属するメールサーバへ、ウィルス付メールを送信することができ、現在もまだ検知されています。メールサーバは、最終的にメールを受信する場合、基本的に無条件に受け付けます。もちろん最終的にメールを受信するメールサーバにウィルス駆除ソフトまたは目標となった PC にウィルス検知駆除ソフトが導入してあれば防げることできま

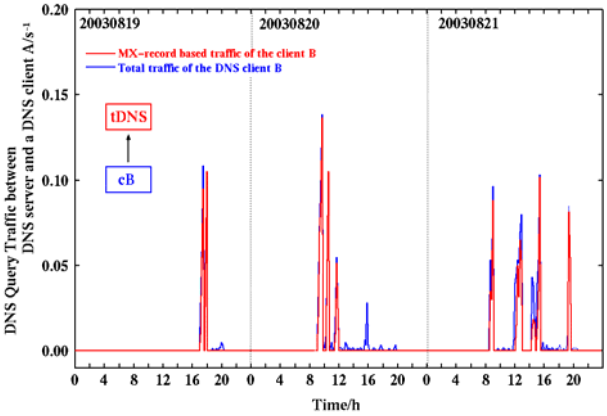


**Figure 2.** Traffic of the DNS query access between the top domain DNS server and the DNS client B through August 19th to 21st, 2003. The blue line shows the total the total DNS traffic and the red line indicates the MX-record based DNS traffic ($s^{-1}$ unit).

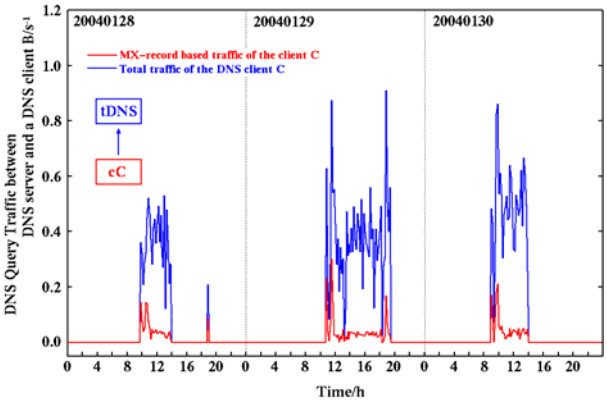


**Figure 3.** Traffic of the DNS query access between the top domain DNS server and the DNS client C through January 28th to 30th, 2004. The blue line shows the total the total DNS traffic and the red line indicates the MX-record based DNS traffic ($s^{-1}$ unit).

す。しかしウィルス駆除ソフトの検知システムは大部分がパターン整合型であったため、ウィルスのパターンが間に合わない所謂 W32/Netsky MMW[9]の様な感染速度が極めて高速な（ゼロデイ型）の MMW の出現により、ウィルス駆除ソフトメーカのみならず、大学や企業等のありとあらゆる組織の管理者や PC 利用者は大量のウィルスメールを受信することになりました。ところでメールサーバの機能を「SMTP エンジン」と呼び、通常のメールサーバの SMTP エンジンと大量送信型ワームの SMTP エンジンの動作の相違について調査してみましょう。

Figure 1 にとあるメールサーバ（DNS クライアント A とします）と学内の DNS サーバ（tDNS）との間の DNS クエリ流量の時系列変化を示しています。DNS クエリの流量の成分としてアドレス(A) レコード型、ポインタ (PTR) レコード型、及びメールエクスチェンジ(MX) レコード型 DNS クエリパケット流量成分の 3 種類がよく知られています。

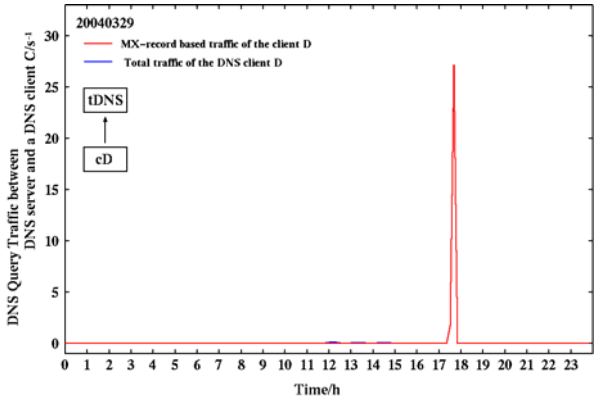


**Figure 4.** Traffic of the DNS query access between the top domain DNS server and the DNS client D through March 29th, 2004. The blue line shows the total the total DNS traffic and the red line indicates the MX-record based DNS traffic ($s^{-1}$ unit).

**Table 1.** The total number of lines for MX, A, and PTR records per a day in the syslog file in tDNS, relating to the DNS client accesses from cA-D.

| day | MX | A | PTR |
|---|---|---|---|
| cA, Feb. 26th, 2004 | 2922 | 6675 | 139 |
| cB, Aug. 19th, 2003 | 190 | 36 | 0 |
| cC, Jan. 28th, 2004 | 807 | 4823 | 0 |
| cD, Mar. 29th, 2004 | 17346 | 1115 | 0 |

A レコード型 DNS クエリパケットは DNS クライアントが DNS サーバに対してホスト・ドメイン名（FQDN 言う）を IP アドレスに変換依頼するためのパケットです。このアドレス変換機能は DNS の基本機能であり、正引きアクセス又は標準名前解決と呼びます。一方、PTR レコード型の場合は IP アドレスから FQDN に変換されますので、ちょうど A レコード型の場合の逆になります。そのため逆引き名前解決と呼ばれます。

更に MX レコードでは、ドメイン名をメールサーバの FQDN に変換します。これはメールアドレスの@の右側部分が主としてドメイン名だけで構成されているからです。一般にネットワークプログラムがサーバ等に接続する場合は IP アドレスが必要となります。するとメールが配信される時にはドメインしかないので、最初にドメイン名を FQDN に変換し、その後得られた FQDN を IP アドレスに変換します。

Figure 1 では A レコード型 DNS クエリパケットの他に PTR レコード及び MX レコードが含まれています。一方 Figure 2-4 に示した DNS クライアント

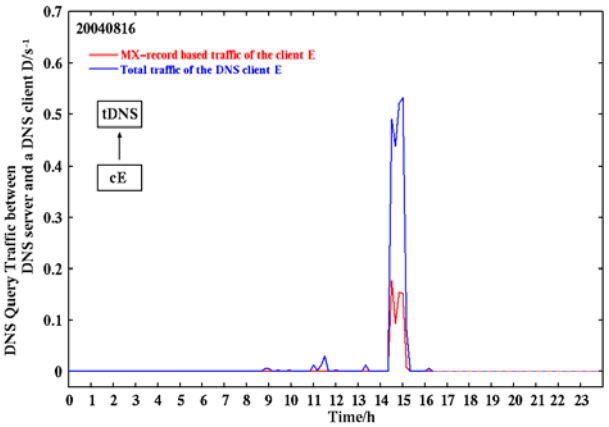


**Figure 5.** Traffic of the DNS query access between the top domain DNS server and the DNS client E through August 16th, 2004. The blue line shows the total the total DNS traffic and the red line indicates the MX-record based DNS traffic ($s^{-1}$ unit).

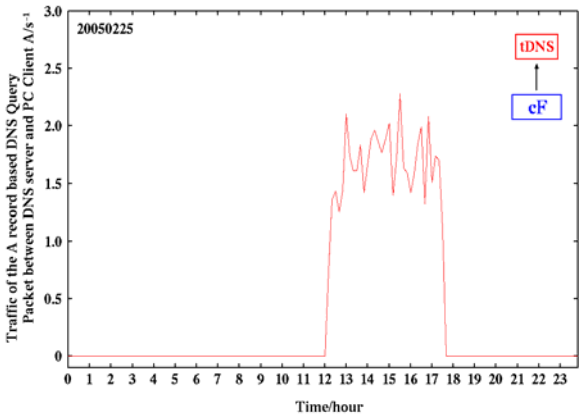


**Figure 6.** The traffic of the A record based DNS query packet access between the top domain DNS (tDNS) server and the DNS client F at February 25th, 2005 ($s^{-1}$ unit)

B-D は、それぞれ W32/Sobig.F [10]、Mydoom.A [11] 及び Netsky.Q [9]に感染した PC であり、これらの PC からの DNS クエリパケット流量には、A レコード型の DNS クエリパケット流量の他に MX レコード型が含まれてものの、PTR レコード型 DNS クエリパケット流量成分は含まれていません。実際 1 日当たりの流量を Table 1 に示しています。Table 1 からも PTR レコード型 DNS クエリパケット流量の有無の違いがメールサーバと大量メール送信型ワームとの違いであることが判ります。

この結果は、PC からの DNS クエリパケット流量中の MX レコード型及び PTR レコード型 DNS クエリパケットの有無を調べるだけで、その PC に SMTP エンジンが存在していることを示しています。つまり PC から MX レコード型 DNS クエリパケットが送信の有無を見ればその第二世代大量メール送信型ワームに感染した PC の IP アドレスを検知・特定することができることが判ったのです。

実際この方法を使った検知システムを本大学の DNS サーバに実装して動作確認したところ多数の大量メール送信型ワームによる MX レコード型 DNS クエリパケットの流量が観測され、それらのパケットの送信元アドレスを調べることで感染 PC を割出し、かつ自動的に該当 IP アドレス管理者にメールで通報するシステムを実装することで、W32/Netsky の大流行を未然に抑えることができました[12c]。

このシステムの最大の利点は、その時点でリリースされた大量メール送信型ワームについてすべて対応できたという点です。言い換えればワーム・ウィルス用のパターンデータが不要という長所があります。

この検知方法の欠点は、プロバイダの様なネットワークの分離が明確でない、またはグローバル IP アドレスが動的に割り当てられる様な組織のネットワークに向いていないということです。大学や企業等の組織内とその外が明確に分離されていること多く、サーバの有無や PC の所在をある程度事前に把握できるので、サーバや PC の所在データベースを構築すれば不確実な検知方式の補完技術を開発するのは困難ではありません。つまり狭い範囲の LAN 内で限れば効果を挙げることができるが、プロバイダ（ISP）等の内外の分離が不明確な場合は、この方法は向いていないと言うことです。つまり検知の結果が不確実である可能性が少しでも残っているため、もっと高度な補完技術が必要だからです。ベイズ理論用いた統計処理を行うフィルタ等を用いるなどの補完技術の開発研究が複数のグループから報告されています[13,14]。

しかしこれらの補完技術も第二世代のみにしか通用しないのかも知れません。次節では第三世代について述べます。

## 3. ボットネットワーク対策

### 3.1 第三世代の大量メール送信型ワーム

第一世代の大量メール送信型ワームは、インターネット上の第三者中継可能なメールサーバに依存するものでした。第二世代のワームは、独自の SMTP エンジンを持ち、ワーム活動時に DNS サーバに MX レコード型 DNS クエリパケットを送信するものでした。第三世代の大量メール送信型ワームはどのようなものでしょうか。実は W32/Mydoom.A ワ

ームについて調査を行った時点である疑問わいていたのですが、そこにヒントが隠されていました。

Table 1 には W32/Sobig.F、W32/Mydoom.A、及び W32/Netsky.Q のそれぞれ A レコード型及び MX レコード型 DNS クエリパケットの流量が示されていますが、W32/Mydoom.A ワームの場合だけ他のワームに比べて MX レコード型よりも A レコード型の DNS クエリパケット流量が多くなっています。また Figure 5 に W32/Mydoom.S に感染した PC からの DNS クエリパケットの流量の時系列変化を示しています。このワームの MX レコード型及び A レコード型 DNS クエリパケットの流量はそれぞれ 351 及び 947/日です。そこで DNS パケットのクエリコンテンツを調査すると、下記の様なキーワードが発見されます[11]。

| | |
|---|---|
| **mx**.xxxxxx.co.jp | **mail1**.xxxxx.co.jp |
| **mail**.xxxxx.co.jp | **relay**.xxxxx.co.jp |
| **smtp**.xxxxx.co.jp | **ns**.xxxxx.co.jp |
| **mx1**.xxxxxx.co.jp | **gate**.xxxxx.co.jp |
| **mxs**.xxxxx.co.jp | .... |

これらのドメイン名の先頭のキーワードは典型的なメールサーバのホスト名です。この結果は、ワームが感染した PC のディスク内から収集したメールアドレスのドメイン名に、“mx”, “mail”, “smtp”, “mx1”, “mxs”, “mail1”, “relay”, “gate”等の典型的なメールサーバのホスト名を付けて A レコード型 DNS クエリパケットを DNS 送信して IP アドレスが回答として得られれば、MX レコード型 DNS クエリパケットを送信しなくてもワーム活動ができることを示しています。

以上の結果から、A レコード型 DNS クエリパケットのみを使ってメールサーバの名前解決をする大量メール送信型ワームが存在する、または近い将来その様なワームがリリースされる可能性が示されました。

### 3.2 W32/Mytob.A の出現

2005 年 2 月 25 日にとある PC からの大量の不審な A レコード型 DNS クエリパケット流量が検知されました（Figure 6）。この DNS パケットのクエリコンテンツを解析すると Figure 7 に示すように、”mx”, “ns”, “mail”, “smtp”, “gate”, “relay”の 6 つキーワードが見つかりました[12]。これらのキーワードのみを含む A レコード型 DNS クエリパケット流量とこの PC からの A レコード型 DNS クエリパケットの流量とについて相関分析を行ったところ、相関係数（$R^2$）が 0.999 となり、両流量間に明きからに強い相関があることが判明しました(Figure 8)。この PC から W32/Mytob.A が検出されています[7]。

| 1 | | 2 | | 3 | | 4 | | 5 | |
|---|---|---|---|---|---|---|---|---|---|
| m | 9975 | ma | 7506 | mai | 7404 | mail | 7399 | mail. | 5894 |
| s | 1569 | mx | 1883 | smt | 872 | smtp | 872 | smtp. | 491 |
| p | 566 | sm | 888 | mx1 | 583 | mx1. | 451 | mail1 | 229 |
| a | 542 | in | 265 | mx0 | 402 | rela | 195 | mailh | 201 |
| c | 490 | re | 237 | mx. | 378 | mx2. | 167 | mail2 | 200 |
| i | 462 | po | 231 | rel | 196 | inbo | 134 | relay | 190 |
| n | 403 | ns | 153 | mx2 | 171 | spam | 101 | mailg | 162 |
| b | 395 | sp | 143 | inb | 134 | mx01 | 92 | inbou | 133 |
| r | 363 | co | 132 | pop | 118 | www. | 91 | mail- | 129 |
| e | 341 | ba | 120 | spa | 108 | serv | 79 | mails | 108 |
| | | | | www | 96 | mx3. | 79 | smtp1 | 96 |
| | | | | bar | 85 | pop. | 76 | mx01. | 90 |
| | | | | ser | 82 | barr | 73 | mail0 | 74 |
| | | | | mx3 | 82 | post | 69 | barra | 73 |
| | | | | pos | 75 | emai | 67 | smtp- | 72 |
| | | | | mx- | 70 | gate | 64 | serve | 70 |
| | | | | gat | 67 | filt | 51 | email | 67 |
| | | | | ema | 67 | mx0. | 49 | mail3 | 65 |
| | | | | cor | 62 | mx4. | 47 | | |
| | | | | web | 57 | | | | |
| | | | | ns. | 55 | | | | |
| | | | | mta | 55 | | | | |

**Figure 7.** Statistics of the query contents for the A record based DNS query packets from the client F at February 25th, 2005.

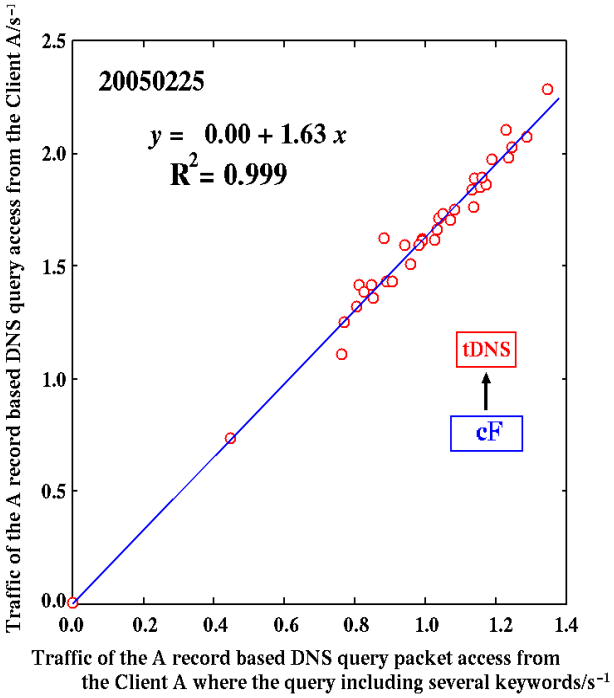


**Figure 8.** Total traffic of the A record based DNS query packet access from the client F versus traffic of the A record based DNS query packet access from the client A including the six keywords at February 25th, 2005 ($s^{-1}$ unit).

結局 2005 年初頭に A レコード型 DNS クエリパケットのみを送信する第三世代の大量メール送信型ワームが出現したことになります。このワームは、その後複数の亜種がリリースされた後、改良され W32/Zotob と呼ばれるボットワームに変化しています。この W32/Zotob.A 及びその亜種は感染力が強く現在でも学内の PC から発見されています。

## 4. 今後の展開

今回は大量メール送信型ワームの SMTP エンジン関する我々の研究を中心に説明致しました。最近のボットネットワークにもそれらワーム同様の SMTP エンジン機能が搭載されていると情報があるため、その真偽については現在調査研究中です。そして何らかの結果が得られると思われます。そしてボットワームが活動する際にネットワークアプリケーションプロトコルベースのパケット流量間の相関を調べることによってある程度プロアクティブなボットネットワーク対策が採れるのでないかと考えています。

## 謝辞

我々の研究はすべて総合情報基盤センターの設備を使って行われています。これらの研究が行えるのも本センター職員、そして熊本大学の教職員及び学生の皆様のご理解ご協力があってこそ成立する研究分野でもあります。この場を借りて厚く感謝申し上げます。

## 参考文献

[1] P. Barford and V. Yegneswaran: *An Inside Look at Botnets*, Special Workshop on Malware Detection, Advances in Information Security, Springer Verlag, 2006.

[2] J. Nazario, Defense and Detection Strategies against Internet Worms, I Edition; Computer Security Series, Artech House, 2004.

[3] (a) J. Kristoff, *Botnets, detection and mitigation: DNS-based techniques*, Northwestern University, 2005, http://www.it.northwestern.edu/bin/docs/bots_kristoff_jul05.ppt (b) J. Kristoff, "Botnets," NANOG 32, October,2004.

[4] D. David, C. Zou, and W. Lee, “Model Botnet Propagation Using Time Zones”, Proceeding of the Network and Distributed System Security (NDSS) Symposium 2006; http://www.isoc.org/isoc/conferences/-ndss/06/ proceedings/html/2006/

[5] A. Schonewille and D. –J. v. Helmond, “The Domain Name Service as an IDS. How DNS can be used for detecting and monitoring badware in a network”, 2006; http://staff.science.uva.nl/~delaat/snb-2005-2006/p12/-report.pdf

[6] (a) Y. Musashi, R. Matsuba, and K. Sugitani, “Development of Automatic Detection and Prevention Systems of DNS Query PTR record-based Distributed Denial-of-Service Attack”, *IPSJ Technical Reports, Distributed System and Management 34th (DMS34)*, Vol. 2004, No. 77, 2004, pp.43-48. (b) Y. Musashi, R. Matsuba, and K. Sugitani, “Detection and Prevention of DNS Query PTR record-based Distributed Denial-of-Service Attack”, *Proceeding for the 3rd International Conference on Information (Info'2004*), Tokyo, Japan, 2004, pp.233-237. (c) Y. Musashi, R. Matsuba, K. Sugitani, and K. Rannenberg, “Detection and Prevention of DNS Query PTR record-based Distributed Denial-of-Service Attack”, *Information*, Vol.9, No.2, 2006, pp.339-349.

[7] http://www.trendmicro.com/vinfo/virusencyclo/-default5.asp?VName=WORM_MYTOB.A

[8] http://www.trendmicro.com/vinfo/virusencyclo/-default5.asp?VName=WORM_ZOTOB.A

[9] http://www.trendmicro.com/vinfo/virusencyclo/-default5.asp?VName=WORM_NETSKY.Q

[10] (a) R. Matsuba, Y. Musashi, and K. Sugitani, “Detection of Mass Mailing Worm-infected IP address by Analysis of DNS Server Syslog” *IPSJ SIG Technical Reports, Distributed System and Mangement 32nd (DSM32)* , Vol. 2004, No. 37, 2004, pp.67-72. (b) Y. Musashi, R. Matsuba, and K. Sugitani, “Indirect Detection of Mass Mailing Worm-Infected PC terminals for Learners”, *Proceeding for the 3rd International Conference on Emerging Telecommunications Technologies and Applications (ICETA2004*), Košice, Slovakia, 2004, pp.233-237. (c) Y. Musashi and K. Rannenberg, “Detection of Mass Mailing Worm-infected PC terminals by Observing DNS Query Access”, *IPSJ SIG Technical Reports, Computer Security 27th (CSEC27),* Vol. 2004, No. 129, 2004, pp.39-44

[11] (a) Y. Musashi, R. Matsuba, and K. Sugitani, “Detection, Prevention, and Managements of Security Incidents in a DNS Server”, *Proceeding for the 4th International Conference on Emerging e-learning Technologies and Applicatications (ICETA2005*), Košice, Slovakia, 2005, pp.207-211. (b) Y. Musashi, R. Matsuba, and K. Sugitani, “Prevention of A-record based DNS Query Packets Distributed Denial-of-Service Attack by Protocol Anomaly Detection”, *IPSJ SIG Technical Reports, Distributed System and Management 38th (DSM38)* , Vol. 2005, No. 83, 2005, pp.23-28.

[12] http://www.trendmicro.com/vinfo/virusencyclo/-default5.asp?VName=WORM_SOBIG.F

[13] http://www.trendmicro.com/vinfo/virusencyclo/-default5.asp?VName=WORM_MYDOOM.A

[14] D. Whyte, P.C. van Oorschot, E. Kranakis, "Addressing Malicious SMTP-based Mass-Mailing Activity Within an Enterprise Network", Carleton University, School of Computer Science, Technical Report TR-05-06 (May 2005).
http://www.scs.carleton.ca/research/tech_reports/2005/-download/TR-05-06.pdf

[15] K. Ishibashi, T. Toyono, K. Toyama, M. Ishino, H. Ohshima, and I. Mizukoshi, "Detecting Mass-Mailing Worm infected Hosts by Mining DNS Traffic Data", *Proceeding of the 2005 ACM SIGCOMM workshop on Mining network data*, Philadelphia, Pennsylvania, USA, 2005, pp.159-164.