フィールド調査によるボットネットの挙動解析

高橋正和[†1] 村上純一[†2] 須藤年章[†3]
平原伸昭[†4] 佐々木良一[†5]

近年，ウィルスやワームに加えて，ボットネットが報道されることが増えているが，セキュリティ専門家でもボットネットに対する調査と理解は進んでいないのが現状である．このため，総務省および JPCERT/CC の支援を受け，ISP（Telecom ISAC Japan），セキュリティベンダ，研究機関からなるボットネット研究チームを組織し，ボットネットのフィールド調査を行った．調査の結果，ボットネットは従来問題とされていたウィルスやワームと異なり，感染後もコントロールが容易であり頻繁に変更が行われていること，単に攻撃を行うだけではなくスパイウェアとして情報の収集に利用されていること，等が分かった．なお，今回の調査で取得したボットの実に 80%が未知のものであることも分かった．これは，ボットのソースコードや開発環境が流通していることにより，新種のボットや亜種が次々と開発されていること，特定の目的に絞った開発が行われていることを示しており，従来の検体に対するシグネチャを用意する方式では，限界があることも明らかになった．また，本調査では，ボットの感染率を推定する手法を提案し，ISP における感染率を調査したところ，2%〜2.5%程度の IP アドレスがボットに感染していることが判明した．本稿では，研究チームの調査によって判明した，ボットネットの実態を明らかにするとともに，現在のセキュリティ対策における課題と，ボットネット対策の基本的な考え方を提唱する．

Behavioural Analysis of Botnet Based on Field Research

Masakazu Takahashi,[†1] Jun-ichi Murakami,[†2]
Toshiaki Sudou,[†3] Nobuaki Hirahara[†4] and Ryoichi Sasaki[†5]

Today, BOTNET has been bringing up as an issue, as well as virus and worms, but the investigation and understanding about BOTNET are not improved yet. Due to this situation, a BOTNET Research team has been organized by ISP (Telecom ISAC Japan), Security Vendors, and researcher groups with supports of the Ministry of Public Management and JPCERT/CC. Field research appears that behavior of BOTNET is different from existing virus and worms; e.g., (1) BOTNET is easily controlled by HERDER, (2) it keeps being upgraded (version up) and changed often, (3) BOTNETs are not only used for attack but also for collecting information as a spy-ware. We also found that 80% of BOTs obtained during the research was unknown. This indicates; (a) new and variety of BOT have been developing and also source codes of BOTs and developing environment are widely spread, (b) many BOTs may developed for certain purpose, (c) pattern matching Ant-Virus techniques may not work effectively. In the research, we developed an infection rate estimation technique, and thereby found that 2 – 2.5% of IP address space were infected to BOTs. In this note, we identify and analyze the actual situation of BOTNET based on the result of field work, and also provide basis of countermeasures against BOTNET and raise the issues for the current security measures.

†1 インターネットセキュリティシステムズ株式会社
Internet Security Systems K.K
†2 株式会社ラック
LAC Co., Ltd.
†3 NTT コミュニケーションズ株式会社 IP ネットワークサービスセンター
NTT Communications Corporation Customer Service Department
†4 トレンドマイクロ株式会社
Trend Micro Incorporated
†5 東京電機大学情報セキュリティ研究室
Information Security Laboratory, Tokyo Denki University

1. はじめに

近年，ウィルスやワームに加えて，ボットネットによる被害が増大している．ボットネットとは，ボットと呼ばれるある種のウィルスが構成するネットワークの総称であり，多くの場合は，IRC（Internet Relay Chat）のメカニズムを通信基盤として利用するもので，文献 1) によれば数百台から数万台の規模のものが確認されている．

一般的なウィルスやワームは，いったん感染活動を始めると，自動プログラム（Auto man）として，あら

かじめプログラムされた活動を続けるのに対し，ボットは，ボットネットの所有者（一般に HERDER と呼ばれる）の指令によって様々な活動を行う．ボットを更新する指令も存在し，これを利用することで，ボットをいっせいに変更することも可能である．

ボットネットの主な機能として，DDoS 攻撃（Distributed Denial of Service Attack），SPAM（Mass Mail）の送信，クレジットカード番号等の収集が確認されているが，ボットネットの脅威は，ボットネットを使った攻撃の影響の大きさと，対策および対応の困難さに集約することができる．

たとえば，ボットネットを DDoS に利用した場合，数百台という小規模のボットネットで，2000 年の Yahoo 等に対する DDoS 攻撃と同レベルの攻撃を行うことが可能であるといわれている[2),3)]．

また，SPAM の送信にボットネットを利用した場合，SPAM を停止させるためには，数百〜数万のボットに対応しなければならないことに加えて，IP アドレスあたりの SPAM 送信数が少なくなることから，SPAM 対策を回避できる点が問題となっている．

さらに，ボットネットの最大の問題点といえるのは，被害の潜在化である．ワームやウィルスが，何らかのアクションをとることで，その存在が明らかになるのに対し，ボットは，極力その存在を知られないように活動し，アンチウィルスによる検出と除去の回避を試みる．このため，ボット感染者がボットの感染に気づく可能性は低く，脅威が潜在化（潜伏）していると考えられている．

2004 年に複数の国内の ISP（Internet Service Provider）でメールのトラブルが発生したが，これはボットネットを利用した SPAM メールの影響であると考えられている．従来の SPAM が特定のメールサーバを中継して送出されていたのに対して，このケースでは，世界各国の多数の IP アドレスから SPAM が送出されており，通常 ISP が SPAM 対策として行っている，IP アドレスによるフィルタリングや，送信元への対処の要請といった方法では対応が困難であったことから，日本でもボットネット対策の必要性が認識されるようになった．

ボットネットについては，“Honey Net Project” [1)] や，“Dos-resistant Internet Subgroup” [2)] の文献があるが，ISP や CSIRT（Computer Security Incident Response Team）が対策を立案するためには不十分な内容であることから，独自の観測と研究を行う必要性が認識された．このため，総務省および JPCERT/CC の支援を受け，ISP（Telecom ISAC Japan），セキュリティベンダ，研究機関からなるボットネット研究チームを組織し，ボットネットのフィールド調査を行うことにした．

具体的な調査項目は以下のとおりである．

1) ハニーポットを使った検体の収集
2) ボットに感染したハニーポットの観察
3) ボットのソースコード調査
4) インターネット上の文献の調査

本稿では，調査 1)，2) によって判明した内容を中心に，3)，4) の成果をふまえて，ボットネットの実態を明らかにする．また最後に，現在のセキュリティ対策における課題と，ボットネット対策の基本的な考え方を提唱する．

2. ボットネットについて

IPA では，ボットを次のように定義している[4)]．

> ボットとは，コンピュータウイルスの一種で，コンピュータに感染し，そのコンピュータを，ネットワーク（インターネット）を通じて外部から操ることを目的として作成されたプログラムです．
> 感染すると，外部からの指示を待ち，与えられた指示に従って内蔵された処理（後述）を実行します．この動作が，ロボットに似ているところから，ボットと呼ばれています．

前述のとおり，ボットネットを使った攻撃としては，DDoS，SPAM の送信，情報収集活動等がある．LURHQ Threat Intelligence Group のレポート[5)] や，今回実施したボットのソースコード解析によれば，代表的なボットの 1 つである Phatbot（別名：Agobot/Gaobot）にはおよそ 90 種類のコマンドが実装されている．

現段階では，多くのボットネットは IRC メカニズムを通信チャネル（以下，IRC チャネル）として利用

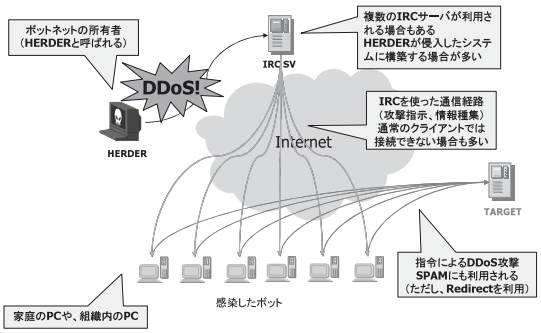

図 1 ボットネットの構成
Fig. 1 Composition of botnet.

しているため，IRC ボットと呼ばれることもあるが（**図 1**），Phatbot の一部は WASTE および Gnutella P2P を利用することが報告されている[5]．

なお，ボットが利用する IRC チャネルは，ボットネット用に独自に構築されたものが多く，一般に公開されている IRC チャネルが利用されることはほとんどない[1]．

3. 調 査 方 法

本研究は，第 1 期（2005 年 2 月〜3 月）として文献の調査とソースコードの解析を行い，第 2 期（2005 年 4 月〜6 月）として，ハニーポットを使ったボットネットの実態調査を実施した．

3.1 ハニーポットによる検体収集・解析

本研究では，ハニーポット（**図 2**）を構築し，検体の収集と解析を行った．ハニーポットへのトラフィックは，各 ISP から割当てを受けた 192 個の不連続な IP アドレスを，トンネリング技術（GRE-G: Generic Routing Encapsulation Gateway）を利用してハニーポットに誘導した．ハニーポットから外部への攻撃を避けるため，メールサーバ（Mail Server）と DNS サーバ（DNS）をハニーポット内に設置するとともに，ファイアウォール（FW）を使って，フィルタリングを行った．

ハニーポットで収集した検体は，トレンドマイクロ社により解析を行い，随時パターンファイルの更新を行うとともに，検体に含まれる IRC サーバ等のアドレスを FQDN（Fully Qualified Domain Name）や IP アドレスとして抽出を行った．

（1） 検体の収集

ハニーポットは，最も脆弱な Windows システムと考えられる Windows 2000（SP なし）を利用し，ボットやワーム等に感染すると，システムを停止し，その段階のファイルシステムを保存したうえで，検体を抽出するように実装した．

収集した検体は，トレンドマイクロ社のアンチウィルス製品が検知した検体を既知，検知しない検体を未知とした．なお，収集した検体をトレンドマイクロ社に提供することにより，未知であった検体も，1〜2 日でパターンファイルに組み込まれている．

（2） バックグラウンドトラフィックの調査

ハニーポットは，WEB へのアクセスやメールの取得・送信といった，外部へのアクセスをいっさい行わない．このため，外部からハニーポットに向けたトラフィックを観察することで，システムの存在に関係なく送られてくるトラフィック（バックグラウンドトラフィック）を観測することができる．また，感染活動に利用する攻撃パターンや，脆弱性についても調査を行う．

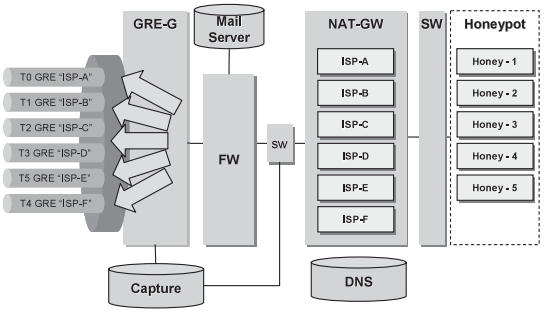

図 2 ハニーポットのネットワーク構成
Fig. 2 Network composition of honey pot.

（3） ボットの解析

収集した検体を使って，アンチウイルスプログラムのシグネチャを更新する．さらに，検体に含まれる IRC サーバ等のアドレスを抽出し，DNS サーバにおける抽出したアドレスのアクセス割合を，ISP に問い合わせ，ボットの感染率を推定する．

3.2 ボットに感染したハニーポットの観測

感染したハニーポットを放置し，トラフィックを観察することで，ボットネットの挙動を調査する．なお，前述のとおり，ハニーポットからの攻撃パケットは，インターネットには出ないように調整した．

（1） 感染時の動き

ボットが感染する際に，どのような手法を用いるのか，また，感染直後にどのような活動を行うかを観測する．

（2） DDoS 攻撃

DDoS 攻撃がどのように行われるのか，また，どの程度行われているのかを観測する．

（3） SPAM 送信

SPAM の送信を観測し，どのような方法で SPAM が送信されているかを観測する．

（4） ボットの更新

ボットは，頻繁に更新が行われていると考えられているが，更新がどのように行われるのかを観測する．また，更新の頻度についても観測を行う．

（5） 情報収集

今回の調査では，メールの送信，WEB のアクセス，サーバへの接続等のハニーポットに情報が蓄積される操作を行わないことから，情報収集に対する調査は割愛した．

（6） その他

その他の機能については，今回の観測対象としなかった．

4. ハニーポットによる調査結果

ハニーポットにおける検体の収集結果と，これに基づいた感染率（見なし感染率），バックグラウンドトラフィック等の調査を行った．

4.1 感染活動の実際

図 2 の SW において，外部からハニーポットへのトラフィックを計測したところ，**表 1** のように，平均で 0.28 Kbps に達した．この値を，各 IP アドレスが受け取るバックグラウンドトラフィック（操作にかかわらず定常的に流れているトラフィック）と想定した場合，日本に割り当てられている全 IP アドレス（約 3,000 万）では，8.4 Gbps のバックグラウンドトラフィックに相当する．

ハニーポットで収集した検体は，ハッシュ値によって分類し，つねに最新の状態に維持したアンチウィルスソフトが検出した検体を既知の検体，検出しなかった検体を未知の検体とした．

今回の調査で収集した検体数（**表 2**）は，1 日あたり 758 件/88 種類であった．既知・未知で分類すると，検出数では既知の検体がおよそ 90%を占めるが，収集した検体種別のおよそ 80%が未知のものであった．

この観測結果では，活発な活動を行っているボット・ワームは 20 種類程度であるが，これと平行して約 70 種類のボットやワームが感染活動を行っていることになる．

なお，収集した検体に対して，トレンドマイクロ社が解析を行ったところ，80%がボットと分類された．

4.2 見なし感染率

収集した検体の中から，検出数が多い検体 100 種を選び，検体の静的な解析により検体に埋め込まれた FQDN のリストを作成した（以下，ボット FQDN リスト）．FQDN を個別に確認したところ，公開された IRC サーバ等の一般的にアクセスが行われる FQDN は存在しなかったことから，これらの FQDN の名前解決を行う IP アドレスはボットに感染していると考えることにした（見なし感染）．

そこで，一定期間内に DNS サーバに対して名前解決を行った総 IP アドレス数と，リストに含まれる FQDN の名前解決を行った IP アドレス数の比を “見なし感染率” と定義した．

Telecom ISAC Japan を通じて，ISP に “見なし感染率” の調査を依頼した結果が**表 3** である．

4.3 ボットネットが利用する IRC サーバ

ボット FQDN リストについて，各 FQDN の DNS 登録状況および IP アドレスの調査を行った．

表 1 バックグラウンドトラフィック
Table 1 background traffic.

	IPアドレスあたり	日本全体 (3000 万)
平均	0.28Kbps	8.4Gbps
ピーク	2.58Kbps	77.4Gbps

表 2 検体検出数
Table 2 Number of specimen material detection.

	トータル		一日あたりの平均	
	件数	種類	件数	種類
検出数	31,846	3,705	758.2	88.2
既知	28,309	767	674.0	18.3
未知	3,537	2,938	84.2	70.0

収集期間：2005/4/21〜5/12 (42日間/192IPアドレス)

表 3 ボットの見なし感染率
Table 3 Considering infection rate of bots.

	調査時期	みなし感染率
ISP A	2005年5月11日	2.64%
	2005年6月 7日	2.10%
ISP B	2005年5月11日	2.44%

表 4 複数の IRC チャネルを持つボット
Table 4 Bot with two or more IRC channels.

分類	数	割合
分析の対象としたボット	100	---
複数のIRCサーバのFQDNを持つボット	19	19%

まず，複数の IRC サーバの FQDN が埋め込まれているボットに着目すると，19%のボットが複数の IRC サーバの FQDN を持っていた（**表 4**）．

次にボットから抜き出した FQDN に対して，DNS の登録状況を調査した（**表 5**）．

68 個の FQDN のうち，明らかに Dynamic DNS を利用しているものは，19 個（28%）を占めた．また，DNS service を利用しているものは，15 個（22%）となっており，この 2 つをあわせると 50%となった．

ホスティングサービスと，ゲーム関係のサイトも複数確認された．

そのほか，FQDN を調べた中で特徴的なものを**表 6** にまとめた．

複数の IP アドレスが割り当てられている FQDN は，DNS Service を利用しているものが多く，最大 5 個の IP アドレスが割り当てられていた．

正引きと逆引きが異なるケースは，ADSL 等でインターネットに接続している PC を IRC サーバとして利用していると思われるものが確認された．

表 5 FQDN が属するドメインの分類
Table 5 Classification of domain where FQDN belongs.

種別	数	割合
Dynamic DNS	19	28%
DNS Service	15	22%
不明	13	19%
Game Hosting	7	10%
Hosting	5	7%
ISP	5	7%
Ircd ,Unix Shell Hosting Hosting	4	6%
総計	68	100%

表 6 FQDN の分析（68FQDN を対象）
Table 6 Analysis of FQDN (68FQDNs).

分類	数	割合
複数のボットに参照されるIRCサーバ	15	22%
複数のIPアドレスを持つIRCサーバ	13	19%
名前解決ができないFQDN	23	34%
到達できないIPが割り当てられたFQDN	10	15%
正引きと逆引きが異なるFQDN	22	32%

5. 感染したハニーポットの観測結果

ここでは，ボットに感染したハニーポットの動作を観測した結果を記載する．

5.1 感染時の代表的な動作

（1） 感染方法

今回用意したハニーポットは，メールの取得や，WEB の閲覧といったアクティブな活動をいっさい行っていない．このため，今回収集した検体は，ネットワークワームと同様の感染形態を持つものに限られる．つまり，脆弱性を持ったシステムに対する攻撃が唯一の感染手段である．

今回の調査で観測された攻撃で利用された脆弱性は**表 7** のとおりである．

MS Blast が利用した MS03-026（RPC: Remote Procedure Call に対する Buffer Overflow）と，Sasser が利用した MS04-011（LSASS: Local Security Authority Subsystem Service Buffer Overflow）が半分以上を占めている．

また，Share Access（Windows のリソース共有の脆弱な設定）も，約 24%を占めており，有力な感染手段となっていることがうかがえる．

（2） 実行ファイルのコピー

ボットは，攻撃に成功すると，本体（実行ファイル）のコピーを試みる．今回観測した結果では，検体が

表 7 攻撃に利用された脆弱性
Table 7 Vulnerabilities used for attacks.

脆弱性	概要	検出数	割合
MS03-026[6),7)]	RPC BO	371,142	31.50%
MS04-011[8),9)]	LSASS BO	313,754	26.70%
Share Access	SMB weak cnfg	278,586	23.70%
MS03-039[10),11)]	RPCSS BO	212,503	18.10%
MS04-007[12),13)]	ASN.1 BO	1,046	0.10%
MS02-045[14)]	SMB BO	24	0.00%
MS03-043[15),16)]	Messenger BO	12	0.00%

表 8 実行ファイルのコピー方法
Table 8 Method of copying execution files.

コピー方法	カウント	割合
感染元へのGET-TFTP	5566	81.9%
感染元からのTCP接続	1214	17.9%
感染元への逆接続	12	0.2%
合計	6792	100.0%

*対象期間 5/19 19:00 - 5/24 14:*00

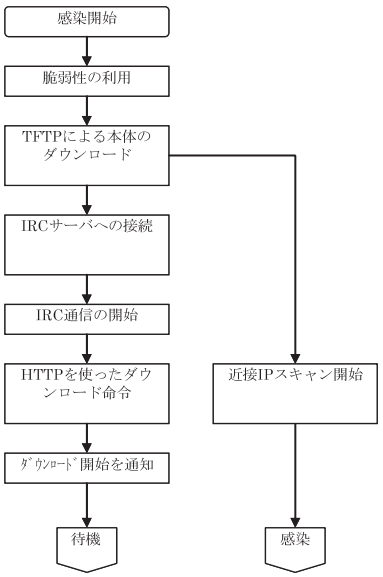

図 3 ボット感染時の基本動作
Fig. 3 Basic operation when Bot is infected.

TFTP による感染元からの実行ファイルの取得（コピー）が約 80%を占めた（**表 8**）．

（3） その他の動作

感染活動を観察したボットは，おおむね**図 3** の動きをすることが分かった．今回観測された特徴的な動きとして，“感染直後に，感染した IP アドレスの近傍 IP アドレスに対してスキャン（感染行為）を行う点”，“IRC サーバへの接続直後に，実行ファイルを更新する点” をあげることができる．

表 9 IRC サーバが利用するポート
Table 9 Port that IRC server uses.

TCP PORT 番号	出現数	割合
6667	958	48%
5562	582	29%
5122	151	8%
65348	114	6%
4150	42	2%
6663	26	1%
65267	25	1%
10362	22	1%
31337	10	1%
その他 19 種	56	3%
計 28 種	1,986	100%

表 10 Phatbot の DDoS コマンド
Table 10 DDoS commands of Phatobot.

コマンド	機能
ddos.httpflood	HTTP フラッディングを実施する
ddos.phaticmp	ICMP フラッディングを実施する
ddos.phatsyn	SYN, URG フラグがセットされたパケットによるフラッディングを実施する
ddos.phatwonk	オープンポートに対する SYN パケットと ACK パケットによるフラッディングを実施する
ddos.stop	フラッディングの実施を中止する
ddos.synflood	SYN フラッディングを実施する
ddos.targa3	フラグメントパケットによるフラッディングを実施する
ddos.udpflood	UDP フラッディングを実施する

5.2 IRC サーバが利用するポート

一般的な IRC サーバでは TCP のポート 6667 を用いて接続する．今回の調査では 6667 は 48%を占め，最もよく利用されるポートであったが，他のポートを利用するものも残りの半数を占めている（**表 9**）．

5.3 DDoS 攻撃

DoS 攻撃は，IRC 経由で命令が出される．今回の観測では，数分で終了する DoS 攻撃が観測されたが，長時間にわたる DoS は観測されなかった．

ボットソースコードの解析により，数種類の DDoS 攻撃が実装されていることが確認されている（**表 10**）が，今回観測された DDoS 攻撃は，すべて Synflood（syn，pan）を使ったものであった．

今回の調査で観測された DDoS 攻撃のターゲットは，他のボットネットが利用する IRC サーバと考えられるものに限られ，商用サイト等への攻撃は観測されなかった．

他のボットネットへの DDoS 攻撃は，HERDER と IRC サーバ間の通信を DDoS によって遮断することにより，HERDER を IRC チャネルから追い出し，その後自らが HERDER として IRC チャネルに接続することでボットネットの管理権限を取得すること，つまり，ボットネットの乗っ取りを意図して行われているものと考えている．

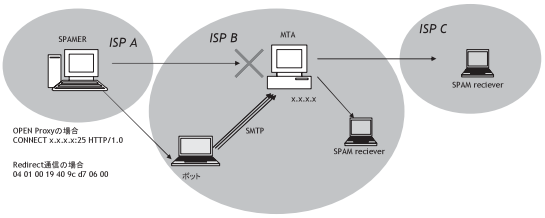

図 4 ボットを使った SPAM の送信
Fig. 4 SPAM transmission that uses Bot.

表 11 リダイレクトポートの割合
Table 11 Ratio of Redirectport.

TCP PORT 番号	カウント	割合
3186	57761	37%
6329	56650	36%
3104	19525	13%
24853	9968	6%
47257	5878	4%
7430	4853	3%
その他 78 種	1427	1%

5.4 SPAM の送出

SPAM の送出は，DDoS とは異なり IRC チャネルは利用されない．ボットがプロキシまたはリダイレクタとしての機能を持っており，これを使ってメールが送信される（**図 4**）．なお，利用されるポートは，**表 11** のような分布をしており，一定ではない．

実際の送信は，まず，SPAM 送信者とボットの間で，リダイレクトまたは，プロキシが確立される．次に，SPAM 送信者からボットに向けた通信は，ターゲットとなるメールサーバへと転送され，メールサーバからの応答は，SPAM 送信者へ転送される．

なお，Phatbot では，6 種類のリダイレクトコマンドが用意されていることが確認されている．

次に SPAM の送信数に着目する．5/13〜5/18 日の 6 日間で観測された SPAM 送信要求を，要求を行ったソース IP アドレスごとに累計を行ったものが**図 5** である．送信要求の 73%は，100 通以内のものであり，これは 1 つの IP アドレスあたりの SPAM 送信数を減らすことによって，anti-spam 技術の回避を意図したものと考えられる．

5.5 ボットの更新

1 日平均 3.4 回/IP アドレスのボットの更新（Update/Download）が観察されており，多いときでは 1 日で 6 回/IP アドレスに達した．なお，ダウンロードに失敗しているケースも，観察されている．

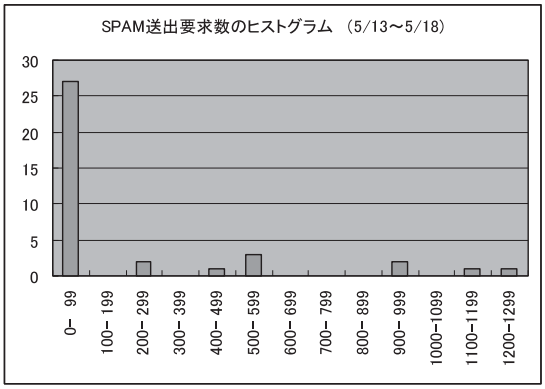

図 5 SPAM 送信要求数のヒストグラム
Fig. 5 Histogram of SPAM transmission.

```
*advscan dcom135 260 5 0 -b -r -s
.advscan dcass 400 3 999 -r -s
.advscan dcom135 100 3 0 -r -b -s
.advscan dcom135 175 2 999 -b -r -s
ntscan 200 2000 -a -b -s
.ntscan 130 999 -a -b
ipscan r.r.r dcom2 86400 256 8000 -s
ipscan s.s.s dcom2 -s
```

図 6 観測されたボットネットの感染指示
Fig. 6 Infection instruction of observed Botnet.

```
advscan scanner thread dealy timeout –[abrs]
  scanner 感染を行うツール名
  thread 感染のために生成するスレッド数
  delay 感染行為の間隔（秒）
  timeout 感染活動を実施する時間（分）
  -a Class Aを対象とした感染行為
  -b Class Bを対象とした感染行為
  -r ランダムなIPアドレスの生成
  -s Silent Scan:感染行為の発見を避けるために
    感染結果の報告を抑制する
```

図 7 advscan のパラメータ
Fig. 7 Parameter of advscan.

5.6 ボットの感染活動

今回の調査で観測された感染コマンドは次のようなものであった（**図 6**）．また，文献 1) で紹介されている advscan のパラメータを**図 7** に記載する．

今回の観測結果において，advscan に着目すると次のような特徴があることが分かった．

- 感染活動を行う範囲を限定している場合が多い．
- 感染活動を行う時間を限定している場合が多い．
- 数秒の間隔をおいて感染活動が行われている．

6. ソースコード調査

ボットネットの実態を把握することを目的として，代表的なボットである Phatbot（別名：Agobot/Gaobot）のソースコード解析を行い，ボットの機能や特徴について調査を行った．

調査の結果，すでに文献 5) で述べられている機能に加え，① デバッガや仮想環境（VMware 等）上では動作しない，② 難読化機能が組み込まれている，さらに，③ GUI によるボットの設定ツールが用意されており，特にプログラミングの知識がなくても，容易に目的に沿ったボットを作成できることが分かった．

6.1 ボットネットソースコード流通の実情

ボットのソースコードを調べると，100 種類以上のソースコードを容易に収集することができた．また，Phatbot のソースコードは，開発環境も含めて流通していることが分かった．

6.2 ボットを使った情報収集

ボット（Phatbot）のソースコード調査の結果，Phatbot は，起動時にスニッファ用スレッドを生成し，下記のデータを収集する．

- FTP 通信中のサーバ，ユーザ名，パスワード
- HTTP 通信による PAYPAL へのアクセス
- IRC 通信中のオペレータ権限の委譲に関する通信
- 脆弱性の存在するサーバとの通信
  （下記の文字列を含む通信）
  - OpenSSL/0.9.6
  - Serv-U FTP Server
  - OpenSSH_2

6.3 ボットの自己防衛

ボット（Phatbot）は，自身の検出や駆除を避けるために様々な機能を実装していることが確認された．以下に代表的な自己防衛機能を記載する．

（1） デバッガ/VMware の検出

今回の調査において，Phatbot は，起動時にデバッガおよび VMware の検出を試み，これが検出された場合プログラムの実行を終了することが分かった．

（2） ポリモーフィックエンジン

Phatbot は，ポリモーフィックエンジンが用意されており，これを簡単に利用することができる．ポリモーフィックとは，暗号化によって実行ファイルを変更する技術で，アンチウィルスによる検出を避ける目的で利用される．

（3） 実行ファイルの難読化

逆アセンブルによる解析を避けるため，実行ファイルの難読化技術（UPX: the Ultimate Packer for eXecutables 等）が用意されている．

（4） アンチウィルスプロセスの監視

Phatbot は，600 を超えるアンチウィルスプロセスのリストを持っており，このリストに含まれるプロセスを見つけると，これを停止させる．

(5) アンチウィルス関連ホストへのアクセス対策

Phatbot は，hosts ファイルに対して 36 のホスト名を書き込み，そのアドレスをループバックアドレス（127.0.0.1）に設定する．これにより，アンチウィルスのパターン更新等を防いでいる．

7. 調査結果の考察

7.1 ボットの脅威モデルの考察

(1) ネットワークワームの脅威モデル

ネットワークワームは，主に感染の速度と規模が脅威レベルを評価するうえでの指標となる拡散様態は，ロジスティック方程式

$$\frac{dM(t)}{dt} = \frac{1}{\theta}M(t)(\theta \cdot p - M(t)) \qquad (1)$$

で表せることが知られている[17]．なお，感染率を p，p から導き出したネットワークワームの最大感染 IP アドレス数を θ，時刻 t における感染数を $M(t)$ としている．

(2) ボットネットを使った感染活動

ボットの感染活動について，① 感染活動は命令によって実行され，新たに感染したボットは次の感染命令を受けるまで感染活動を行わないものとし，ハニーポットにおける観測結果から，② ボットの感染活動は限定された IP アドレスに対して，数秒の間隔（遅延）をもって感染活動を行う，③ ボットの感染活動を行う時間が指定されているとした場合，時刻 $t = 0$ におけるボットの数を θ，時刻 t におけるボットの数を $M(t)$，攻撃による感染確率を p，単位時間あたりの感染パケット送出数を r，指定された IP アドレスに対する感染活動を終了するまでの時間を $\max tA$，指定された感染活動時間を $\max tP$ とした場合，次の式で表すことができる．

$$M(t) = t \cdot \theta(t + p \cdot r) + \theta$$
$$0 \leqq t \leqq \min(\max tA, \max tP) \qquad (2)$$

たとえば，ワームとボットネットの拡散様態を比較した場合，ワームがロジスティック曲線で拡散していくのに対して，ボットネットは，感染活動時に一次関数的な増殖を行い，一定時間を経過した後に，感染活動を停止するという動きが繰り返し行われているものと考えられる．

ワームが乱数を基本とした感染活動を行うのに対し，ボットネットは重複の少ない分担が可能であることから，ワームと比較して，効率的な感染活動が可能である．

(3) ボットネットを使った DDoS

ボットネットの主要な脅威といわれる DDoS 攻撃と，ボットネットの規模について考察する．

ボットネットによる DDoS の効果を考える場合，ボットネットの規模に加えて，攻撃の効果と，どの程度の頻度で攻撃を行うかという点を考慮する必要がある．

たとえば，HTTP GET による DDoS 攻撃を行う場合は，攻撃の対象が静的な WEB ページの場合と，CGI 等の動的なページでは 1 アクセスあたりの攻撃の効果が大きく異なる．

また，UDP Flood 等のネットワーク帯域を使いきることを目的とした攻撃の場合，大規模なボットネットを利用する場合は，1 台あたりの送出パケットを抑制し，ボットの負荷を軽減することが可能である．一方で，文献 2) でも指摘されているように，現在のブロードバンドネットワークにおいては，小規模なボットネットでも容易に商用サーバを停止に追い込むことが可能である．

このような DDoS 攻撃の要素を考慮すると，時刻 t における DDoS 攻撃のターゲットに対する効果を $S(t)$，ボットの数を $M(t)$，単位時間あたりのボットの攻撃数を P，1 つの攻撃の効果を E とした場合，次の式で表すことができる．

$$S(t) = M(t) \cdot P \cdot E \qquad (3)$$

(4) ボットネットを使った SPAM 送出

ボットネットの主要な利用方法といわれている SPAM の送出と，ボットネットの規模について考察する．

2004 年に発生した国内の ISP のトラブルは，ボットネットによって短時間に大量の SPAM が送出されたことが原因であった．一方で，5.4 節「SPAM の送出」でも記載したようにボット 1 台あたりのメール送出数を減らすことで，anti-spam 技術の回避を図っていると考えられる動きもある．

SPAM 送信者の立場で考えた場合，一定時間で送出する SPAM の総数が興味の対象となることから，anti-spam の制限のない環境においては，ボットあたりのメール送出数を多くすることが可能であるため，小規模なボットネットでも大量の SPAM を送信することが可能といえる．一方で，anti-spam 技術を回避するためにボットあたりのメールの送出数を少なくした場合，大規模なボットネットを必要とすることになる．

このような SPAM 送出の特性を考慮すると，時刻 t における単位時間あたりの SPAM の送出数を $S(t)$，ボットの数を $M(t)$，単位時間あたりのボットのメール送出数を F とした場合，次の式で表すことができる．

$$S(t) = M(t) \cdot F \qquad (4)$$

7.2 ボットネットで利用される IRC サーバの構成

ボットネットが利用する FQDN を調べると，DDNS（Dynamic DNS）等の，変更が容易で厳密なオーナ情報を必要としないサービスを利用していることが多かった．

このように，直接 IP アドレスを利用せず，FQDN を使って IRC サーバを指定することにより，IRC サーバが停止した場合にも，DNS を書き換えることにより，容易にボットネットを復活させることが可能となっている．

また，1 つの FQDN に複数の IP アドレスが割り当てられている例も目立っている．複数の IP アドレスを割り当てることで，負荷の分散と，ボットネットの可用性が確保できることから，大規模なボットネットが，このような構成をとっているものと考えられる．

7.3 SPAM 送信とボットネットのレンタル

ボットネットを使った SPAM の送信は，当初 IRC チャネルを使って実施されるものと考えていた．今回の調査では，文献 1) に記載されているように，ボットネットを使った SPAM の送信が，リダイレクトを利用することが確認された．

ボットネットのレンタルスキームの多くは，ボットネットの IRC チャネルを貸し出すことではなく，ボットのリダイレクト機能を貸し出すことである．つまり，HERDER は，ボットの IP アドレスとリダイレクトポートのリストを販売し，SPAM 送信者はこのリストに基づいて，SPAM 送信プログラムを使い大量のメールを送信する．HERDER は，ボットのリダイレクトポートを頻繁に変更することにより，貸出し期間を経過した SPAM 送信者がボットネットを利用することを防止しているものと推定される．このため，頻繁にボットを更新し，リダイレクトポートを変更しているものと推定される．

8. ボットネットの基本的対策

ボットは，複合的な機能を持ち，短期間に新種・亜種が出るばかりでなく，すでに感染したボットも，その更新機能により新種・亜種に置き換えられている．

このため，従来の検体に対するシグネチャを用意する検出技法では，“パターンの作成が間に合わない” という問題が生じる．また，アンチウィルスベンダでは，感染規模を緊急度評価の指標にしているが，“同一種による大規模な感染が発生しにくくなっている” ことから，ボットの緊急度の評価が低くなってしまい，なかなか対策が行われない傾向にあり，単純なパターンファイルによる検出の限界が改めて明らかになった．

また，ボットネットの対策については，当研究プロジェクトでは，以下の 3 つのフェーズに分けて立案する必要があると考えている．

1) DDoS 等の攻撃を受けた際の対策（緊急対応）
2) 攻撃力を軽減するための対策（対処）
3) 利用される PC 等を減じるための対策（予防）

8.1 DDoS 等の攻撃を受けた際の対策

ボットネットによる DDoS 攻撃は，ボットと IRC サーバ間の通信を遮断することで，止めることができる．通信を遮断するためには，次の方法が考えられる．

- IRC サーバをダウンさせる．
- IRC サーバの FQDN のエントリを変更する．
- IRC サーバ向けの通信をブロックする．

この対応を行うためには，つねにボットを観測し，ボットネットに利用される IRC サーバを把握しておく必要がある．FQDN のエントリの変更は，一般に公開された IRC サーバ等の FQDN を確実に排除する必要があるが，サーバの所在地や暗号化の有無にかかわらず，ISP 等が提供している DNS サーバで実施できるため，有力な手法と考えられる．なお，一般公開された IRC が利用されている場合は，サーバ管理者に対処を依頼することも可能である．

8.2 攻撃力を軽減するための対策

攻撃力は，ボットネットの規模に比例する．このため，ボットの感染を減じることができれば，ボットネットの攻撃力を軽減することになる．

すでに述べたように，ボットに感染すると，アンチウィルスの活動を阻害し，検出や駆除を回避する．以下の対策をとることで，このような防衛策を回避できると思われる．

- ウィルスと同様に実行ファイルに複数のパターンを持たせる（ポリモーフィックエンジン，実行ファイルの圧縮等の利用）．
- プロセス名をランダムに変更する．
- 名前解決を独自に行う（hosts ファイルを利用しない）．

また，今回の調査では，ISP における DNS アクセスを使って，ボットの感染率を推定したが，この方法を利用することで，ボットに感染している IP アドレスを特定することが可能である．このため，感染している IP アドレスから利用者を特定し，利用者にボットの対策を働きかけることも効果があると考えられる．

8.3 利用される PC 等を減じるための対策

ボットの感染を防ぐためのセキュリティ対策を推進することで，将来ボットに感染する PC を減じることができる．

一方で，次の対策も効果が高いと考えられる．

- ISP に不正侵入防御装置（IPS）を導入する．
- インターネット接続点に ADSL モデムを利用することを禁止し，ファイアウォール機能が付いた ADSL ルータに限定する．

なお，IPS は，① 攻撃ごとの検知パターンを持つものと，② 脆弱性を利用した通信を検出するものが存在する．日々大量の亜種が確認されている状況においては，① の IPS は効果が薄く，② の IPS を利用する必要がある．

9. 今後の課題

9.1 通信メカニズムの移行の可能性

現在ボットネットは，IRC メカニズムを主要な通信チャネルとしている．今回の調査では，P2P メカニズムを主な通信経路として利用するボットネットはなかったが，サブチャネルとして P2P による通信を実装しているものが存在した．

たとえば，Phatbot の一部は，WASTE という 50〜100 台を限度としたハイブリッド型 P2P を利用する機能を持っており，ボットの周知に Gnutella P2P を利用する[5]．

今後，ボット対策が進んでいくと，ボットネットの主要な通信経路が，IRC メカニズムから P2P メカニズムに移行する可能性がある．主要な通信経路が P2P に移行した場合，次のような点が懸念される．

① 匿名性の向上

IRC メカニズムのようなスター型のネットワークでは，サーバの存在を突き止めることができれば，そこに接続するボットの IP アドレスを特定することができるが，P2P ネットワークの場合は，すべてのボットを把握できる観測ポイントは存在しないことになる．

このため，IRC メカニズムを利用する場合と比較して，ボットの匿名性をより高めることができる．

② ネットワークの高可用性化

IRC メカニズムを利用したボットネットでは，IRC サーバを失うとコントロールができなくなる．しかし，P2P 型のネットワークでは，サーバが存在しないため，この問題を解決できる可能性が高い．

③ DNS に依存しないネットワークの構築

P2P を利用する場合は，複数のリンクポイントの IP アドレスを保持し，そのいずれかがアクセス可能であれば，そこからリンクに入っていくことができるため，DNS をまったく使わないボットの実装も可能である．

④ トラフィック特性の改善（より大規模に）

ボットネットは，HERDER の指示によりいっせいにバージョンアップを実施するが，すべてのボットが，ほぼ同時に同じサーバから，ダウンロードを行うことになるため，サーバやネットワークの負荷が大きい．P2P ネットワークでは，隣接するボットがバケツリレー方式で転送するため，トラフィックの集中が発生せず，この問題を改善または，解決する可能性がある．

9.2 継続的な調査および難読化解除の自動化

今回の調査においても，2 カ月ほどの間に，ボットネットのトレンドは変化しており，ボットネットが利用する IRC サーバや，ボットネットの動向を知るためには，ハニーポットによる検体収集と，収集したボットの解析を継続する必要があることを改めて認識した．

一方で，ボットには解析を避けるための，難読化等の手法が利用されており，ボットを解析するためには，時間と労力が必要であった．難読化解除を自動化することができれば，継続的な調査も容易になる．

謝辞 本研究は，JPCERT/CC「ボットネット調査プロジェクト」および，総務省「ボットネット被害の実態に関する調査研究」における調査・研究結果をまとめたものである[18),19)]．本研究を進めるにあたって有益な助言と協力をいただいた JPCERT/CC，Telecom ISAC Japan の関係者各位に深く感謝いたします．

参 考 文 献

1) The Honynet Project & Research Alliance: Know your Enemy: Tracking botnets. http://www.honeynet.org/papers/bots/
2) Handley, M. and University College London: Dos-resistant Internet Subgroup Report. http://www.thecii.org/dos-resistant/meeting-1/cii-dos-summary.pdf
3) Yahoo DDoS についての投稿. http://packetstormsecurity.nl/distributed/yahoo.txt
4) IPA セキュリティセンター：ボット対策，IPA：独立行政法人情報処理推進機：Information-Technology Promotion Agency, Japan. http://www.ipa.go.jp/security/antivirus/bot.html
5) LURHQ Threat Intelligence Group: Phatbot Trojan Analysis. http://www.lurhq.com/phatbot.html
6) RPC インターフェイスのバッファオーバーランによりコードが実行される (823980). http://www.microsoft.com/japan/security/bulletins/MS03-026e.mspx
7) JVNCA-2003-16 Microsoft Windows RPC にバッファオーバーフローの脆弱性.

http://jvn.jp/vn/JVNCA-2003-16/index.html
8) Microsoft Windows のセキュリティ修正プログラム (835732).
http://www.microsoft.com/japan/security/bulletins/MS04-011e.mspx
9) TRTA04-104A Microsoft Windows 環境に複数の脆弱性.
http://jvn.jpcert.or.jp/tr/TRTA04-104A/index.html
10) PCSS サービスのバッファオーバーランによりコードが実行される (824146).
http://www.microsoft.com/japan/security/bulletins/MS03-039e.mspx
11) Microsoft Windows RPC にバッファオーバーフローの脆弱性.
http://jvn.jp/vn/JVNCA-2003-16/index.html
12) ASN.1 の脆弱性により，コードが実行される (828028).
http://www.microsoft.com/japan/security/bulletins/MS04-007e.mspx
13) Microsoft Windows ASN.1 ライブラリに複数の脆弱性.
http://jvn.jpcert.or.jp/tr/TRTA04-041A/index.html
14) [MS02-045] ネットワーク共有プロバイダの未チェックのバッファが原因でサービス拒否が発生する.
http://support.microsoft.com/default.aspx?scid=kb;ja;326830
15) メッセンジャサービスのバッファオーバーランにより，コードが実行される (828035).
http://www.microsoft.com/japan/security/bulletins/MS03-043e.mspx
16) Microsoft Windows と Exchange Server に複数の脆弱性.
http://jvn.jpcert.or.jp/tr/TRCA-2003-27/index.html
17) 高橋正和，佐々木良一：ワームの特性に基づく拡散モデルの提案と適用，情報処理学会 CSS2004, pp.1–6（2004 年 10 月）.
18) Internet Week2005 講演資料「インターネットセキュリティトピックス」.
http://www.jpcert.or.jp/present/2005/InternetSecurityTrend20051209IWIP.pdf
19) Telecom-ISAC Japan「第 1 回 JPCERT/CC 共催セミナー」.
https://www.telecom-isac.jp/cgi-bin/download/dl.cgi/TI-J-010-F%81F%83%8C%83|%81[%83g.pdf

(平成 17 年 11 月 28 日受付)
(平成 18 年 6 月 1 日採録)

高橋　正和（正会員）

1961 年生．インターネットセキュリティシステムズ（株）勤務．著書に『有害プログラム—その分類・メカニズム・対策—』（共著，共立出版），『IT セキュリティソリューション大系』（下巻 2 編 6 章，9 章等，フジ・テクノシステム），『FreeBSD でインターネットサーバを立ち上げる』（共著，ディーアート），『ネットワークスペシャリスト試験合格ガイド』（共著，ビーエヌエヌ）等.

村上　純一

1983 年生．木更津工業高等専門学校電気工学科卒業，株式会社ラック勤務.

須藤　年章

1969 年生．愛媛大学工学部電気電子工学科卒業，NTT コミュニケーションズ株式会社勤務.

平原　伸昭

1975 年生．日本大学農獣医学部拓植学科卒業，トレンドマイクロ株式会社勤務.

佐々木良一（フェロー）

1971 年 3 月東京大学卒業．同年 4 月日立製作所入所．システム開発研究所にてシステム高信頼化技術，セキュリティ技術，ネットワーク管理システム等の研究開発に従事．同研究所第 4 部長，セキュリティシステム研究センタ長，主管研究長等を経て 2001 年 4 月より東京電機大学工学部教授．工学博士（東京大学）．1983 年電気学会論文賞受賞．1998 年電気学会著作賞受賞．2002 年情報処理学会論文賞受賞．2005 年システム制御情報学会産業技術賞受賞．著書に，『インターネットセキュリティ』（オーム社，1996 年），『インターネットセキュリティ入門』（岩波新書，1999 年），『情報セキュリティ事典』（代表編，共立出版，2003 年），等．IEEE，情報処理学会，電子情報通信学会等の会員．情報処理学会フェロー．情報処理学会コンピュータセキュリティ研究会顧問．日本セキュリティ・マネージメント学会常任理事，IFIP TC11 日本代表．