情報処理学会論文誌　Vol. 52　No. 3　1136–1143 (Mar. 2011)

効果的なボットネット追跡に関する調査と検討

甲斐俊文[†1]　佐々木良一[†2]

ボットネットの被害が増大してきており，ボットマスタ（ハーダ）まで追跡することが重要な課題となっている．ボットネットごとに通信経路は異なるが，経路上に防弾業者や一般ユーザの端末がある場合には追跡は困難になる．そこで我々は防弾業者や一般ユーザの端末を使用しているボットネットの割合を推定するために，統計調査を実施した．その結果，ユーザ端末を使用しているボットネットの割合は 1 割から 3 割程度，防弾業者サーバ端末については少なくとも 2 割以上，専門のサーバ管理者に管理されている端末は 4 割から 5 割程度と見積もられることを示す．また，ボットネットに使用されている端末の国別の傾向について調査した結果も示し，これらの調査に基づいてボットネット追跡の方針を検討する．

Statistics and Studies for an Effective Botnet Traceback

Toshifumi Kai[†1] and Ryoichi Sasaki[†2]

The damage of botnet is increasing, and it is an important problem to track bot masters. We analyzed tracing paths of botnet and classified these under 5 patterns. And if there are terminals of bulletproof providers or end users on a path, tracing on the path is difficult. Now we are examining a ratio of botnet using a terminal of bulletproof providers and end users. We have examined a ratio of botnet using a terminal of bulletproof providers and end users. As a result, we estimated the ratio of the botnet which used terminals of end users at around 30% from 10%, bulletproof providers at least 20%, and normal server managers at around 50% from 40%. And we argue about a policy of botnet traceback.

†1 パナソニック電工株式会社
Panasonic Electric Works Co., Ltd
†2 東京電機大学
Tokyo Denki University

1. はじめに

ボットネットは様々なサイバー攻撃やサイバー犯罪に関わっており，対策が求められている．現在，ボットネットに対する様々な対策が講じられており，一定の成果が報告されている．しかし既存の対策で十分に被害が抑えられてはいない．このため，通信解析によるボットネット通信のフィルタリングやボットネットの制御奪取など，様々な観点から対策方法が提案されているが決定的な対策は現れていない[1),2)]．

我々はボットネットを管理しているボットマスタ（ハーダともいう）を追跡可能としなければ十分な抑止効果はあげられないと考えている．そこで効果的なボットネット追跡を実現するために，追跡経路の整理と追跡可能性の調査・分析を行ってきた．

ボットネットの追跡は，ボットマスタがボットネットを構築したり運用したりした際の手続きや通信の痕跡をたどる行為である．したがって，ボットマスタによるボットネットに対する手続きや通信が，追跡の手がかりとなる．我々はまず，この考えに基づいて追跡経路を整理した．

ボットネットの追跡可能性は，追跡経路上にある端末の管理者の特性に大きく左右される．たとえば，追跡経路上の端末の管理者がボットマスタを隠匿することをサービスにしているような防弾（bullet-proof）業者である場合には，追跡は非常に困難である[3)]．また，追跡経路上の端末が一般的なユーザ PC の場合も，追跡は難しい．しかし，追跡経路上の端末が専門の管理者によって管理されているサーバの場合には，追跡のための仕組みの導入や管理者間の情報共有により，追跡できる可能性がある．したがって，ボットネットに使用されている端末が，どういったタイプの管理者により管理されている割合が多いかを把握する必要がある．このようなアプローチは従来行われてこなかったものであるが，追跡の方針を固めるうえで重要である．

そこで，我々は防弾業者や一般ユーザの端末を使用しているボットネットの割合の統計調査を実施し，ボットネットで使用されている端末の管理者の面から追跡可能性を推定した[4)]．また，ボットネットに使用されている端末の国別の傾向についても調査した．そして，これらの調査結果に基づいて，ボットネット追跡技術の研究開発や追跡の仕掛けを普及させる際の方針に関する検討を行った．

本稿の 2 章にボットネットの追跡経路モデルを示す．3 章では管理者に着目したボットネット構成端末の分類と追跡可能性について述べる．4 章ではこの分類に基づいてボットネットで使用されている端末の統計調査を行った結果を示し，5 章で調査結果に基づいたボット

ネット追跡の方針について議論する．

2. ボットネットの追跡経路の整理

ボットネットの追跡経路を明らかにするために，まずボットネットの構成を示す．次に，ボットマスタがボットネットを構築する手順とボットを制御する手順をあげる．その手順をふまえて，ボット端末の検知を基点とした追跡経路を整理する．

2.1 ボットネットの構成

図 1 に示すようにボットネットはボット型のマルウェアに感染した端末（以下，ボット端末と呼ぶ）と，ボットの管理と制御を行うための Command & Control サーバ（以下，C&C サーバと呼ぶ）により構成される．ボット型のマルウェアとは，ボットマスタからの指令によって制御される機能を持つマルウェアである．

ボット端末は C&C サーバと接続し，ボットマスタからの指令を待つ．C&C サーバの実現手段として IRC サーバや Web サーバが使用されているといわれており，そのほかにも P2P プロトコルを利用したボットネットも存在している．

また，C&C サーバのほかに，ボット感染端末に新しいマルウェアコードを配布するためのダウンロードサーバと呼ばれるサーバも利用される．ただし，C&C サーバとダウンロードサーバは役割の違いはあるが，ボットマスタから送られるデータをボット端末に届けるという点では違いがないため，本稿ではダウンロードサーバも C&C サーバの一種として扱う．

ボット端末が C&C サーバと接続を行う際には，DNS による名前解決の仕組みが利用される場合が少なくない．これは 1 台の C&C サーバが使えなくなった場合でも，別の C&C サーバにボット端末を接続させるということが容易に実現できるためである．DNS による名前解決を行うボットネットでは，C&C サーバの完全修飾ドメイン名（FQDN）をボット端末が把握している必要がある．加えて，インターネット上にこの FQDN に対応する A レコードが設定された DNS コンテンツサーバが存在している必要がある．さらに，FQDN はホスト名，サブドメイン名，ドメイン名から構成されるが，C&C サーバの FQDN に含まれるドメイン名に，そのボットネット固有のドメイン名が使用されている場合もある．

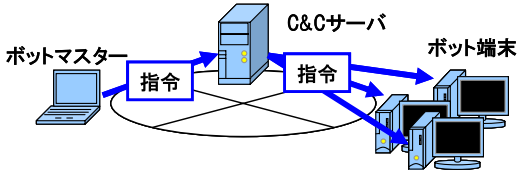

図 1　ボットネットの構成
Fig. 1　A structure of a botnet.

また，ボットマスタは踏み台サーバを経由して C&C サーバにアクセスする場合も多いと考えられる．指令を送信したり，ボット端末を管理したりするために直接 C&C サーバに接続すると，アクセス元の IP アドレスから身元を知られてしまう可能性がある．踏み台サーバを使うことでこれを避けることができる．踏み台サーバはたとえば ssh サーバや http proxy サーバなどを利用することで実現でき，ボットマスタは踏み台サーバを経由して C&C サーバにアクセスすることで，自身の操作している端末の IP アドレスを隠蔽することができる．なお，踏み台サーバもダウンロードサーバと同様に，本稿では C&C サーバの一種として扱う．

2.2 ボットネット構築の手順

図 2 に示すように，ボットネットを構築するには，単にボット型のマルウェアを配布してインターネットに接続されている端末をボット端末にするだけでなく，C&C サーバやドメイン名に関して以下のような準備をする必要がある．

- C&C サーバの準備
- DNS サーバの準備
- DNS サーバへの A レコード登録

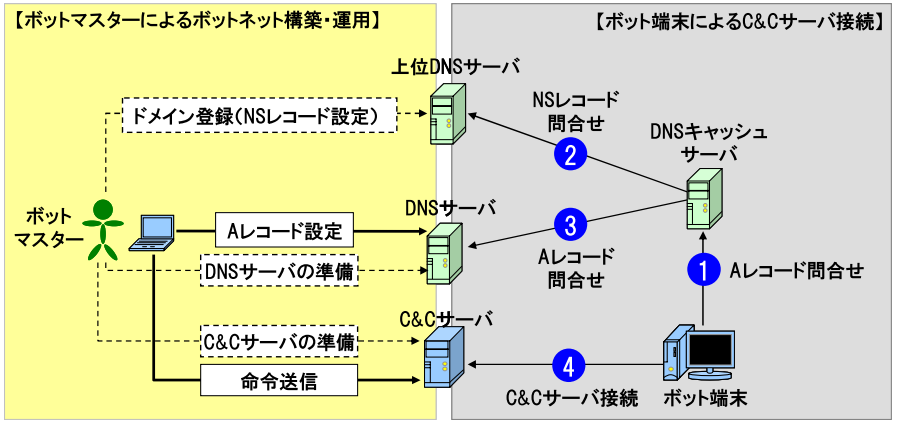

図 2　ボットネット構築・運用とボット端末による C&C サーバ接続手順
Fig. 2　Setting and maintenance of a botnet.

- 固有ドメイン名の登録と上位 DNS サーバへの NS レコード登録

C&C サーバはホスティングサービスなどを利用してボットネット用にボットマスタが用意した端末の上で動作している場合もあるし，不正侵入したサーバやボット端末上に IRC サーバや Web サーバを起動し，それを C&C サーバとして利用している場合もある．また，無料利用ができる IRC サーバや Web サーバを C&C サーバとして利用している場合もある．

ボット端末から C&C サーバへの接続の際に FQDN を利用する場合には，DNS サーバを準備し，C&C サーバの IP アドレスと FQDN を対応付けた A レコードを DNS サーバに登録する必要がある．

DNS サーバの準備は C&C サーバの場合と同様である．有料でサービス提供されている DNS サーバを利用するか，不正侵入したサーバやボット端末を利用するか，無料の DNS サービスを利用するかである．そしていずれかの方法で準備した DNS サーバへアクセスし A レコードの設定を行う．

C&C サーバの FQDN に固有のドメイン名を使用する場合には，固有ドメインの登録と上位 DNS サーバへの NS レコード設定が必要である．固有ドメインは直接レジストラへ登録したり登録代行業者（リセラ）を介して登録したりする．この際，用意した DNS サーバとドメイン名を対応付けるための NS レコードは，レジストラや登録代行業者が運用している DNS サーバに登録されることになる．

3. ボットネットの追跡可能性

C&C サーバへの命令送信や DNS サーバへの A レコード設定などの通信に対する追跡経路については，踏み台型通信（stepping stone）の追跡を行うことになる．踏み台型通信の追跡は，基本的にはボットマスタからのボット端末や DNS サーバに至るまでの通信を，順番に遡ってたどっていくことになる．このためには C&C サーバ，DNS サーバ，踏み台になっている端末の通信ログやアクセスログの保存，踏み台の前後の通信の関連付け，および踏み台間での連絡（あるいは情報共有）を行う必要がある．

また，連鎖している踏み台の通信を順番に遡って追跡する方法だけでなく，追跡通信タイミングや通信メッセージの長さなどを手がかりに，いくつかの踏み台を飛び越えて追跡する手法も提案されている[5]．

文献 5) にあるように，ボットネットの通信追跡は，手がかりとなるボットネット通信のトラフィック量が少ない，複数の踏み台を介して通信されている，暗号化されている可能性がある，他の通信と混在している，といった面からの難しさもある．しかしどんなに追跡が容易な通信であったとしても，ボットネットを構成するサーバとして利用されている端末の管理者の協力なしには追跡を行うことはできない．

なお，契約をともなう追跡経路の場合，追跡はネットワーク上での通信をたどる行為ではなく，契約情報から真の契約者を割り出す行為である．たとえばボットマスタが固有ドメイン名を取得する場合，直接レジストラへ登録したり登録代行業者（リセラ）を介して登録したりする．こうした業者が協力しなければ契約者を割り出すことはできない．

3.1 追跡可能性を考慮した端末の分類

通信に対する追跡経路については，ボットネットのサーバとして利用されている端末の管理者の協力を得られることが追跡のための条件である．このためボットネットのサーバとして使用する端末をボットマスタがどのように準備したかは重要ではなく，誰によって管理されている端末であるかが重要である．

そこで，インターネットに接続している端末を，管理者による追跡協力の可能性を考慮して，大きく 3 つに分類した．1 つ目は専門の管理者が管理しているサーバ系の端末，2 つ目は一般的なユーザが使用している端末，3 つ目はボットマスタやスパムメール送信者を保護するサービスを提供している業者（防弾業者）の端末や無管理状態の端末である．

専門の管理者が管理しているサーバとは，一般企業や団体・大学などがインターネットに対して公開しているサーバやホスティング事業者が提供しているサーバである．こうした専門の管理者が管理しているサーバ端末がボットネットで利用されている場合であれば，通信ログやアクセスログが残っている可能性があり，それを手がかりに追跡できる場合があると考えられる．また，将来的にボットネット追跡システムが確立した場合の導入もしやすい．

一般ユーザの端末とは，ADSL や FTTH などの回線で家からインターネットに接続しているようなユーザの端末である．一般ユーザの端末がボットネットで利用されている場合，ログが保存されていることは期待できず，また追跡のための調査もスキルの問題で期待できない．追跡システムの導入も個人ユーザではスキル面と費用面で困難が予想される．

防弾業者とは，ホスティング事業者の一種ではあるものの，顧客に提供しているサーバなどの端末が悪用され，外部から苦情が来てもそれを無視する業者を指す．また，無管理状態の端末も同様に，その端末が悪用されて苦情が出ても，管理者がいない（あるいは管理者に連絡が届かない）ため，対処がなされない．こうした端末がボットネットで利用されている場合，追跡への協力はまったく期待できない．

4. 統計調査

通信に関する追跡の実行可能性があるボットネットの割合を推定するために，管理者の面からの端末の分類に従って，ボットネットで使用されている DNS サーバと C&C サーバの統計調査を行った．また，国別の傾向について分析した結果についても示す．

4.1 調査方法と調査結果

4.1.1 一般ユーザ端末の推定

一般ユーザの端末数の推定のために，まずボットネットに使用されている DNS サーバと C&C サーバとして利用されている端末の IP アドレスを収集した．次にこの IP アドレスのうち，一般ユーザの端末に該当する台数を推定するという手順をとった．

ボットネットに使用されている DNS サーバと C&C サーバとして利用されている端末の IP アドレスの収集は次の手順で行った．まず，ボットネットで使用されている FQDN のブラックリストを入手した．このブラックリストはインターネット上の Web サイトである Malware Domain List で公開されているものを使用した[6]．このブラックリストには様々なサイバー攻撃に関連している FQDN が掲載されているが，その中からボットネット名のカテゴリに含まれている FQDN のみを抽出した．この作業は 2009 年 12 月 28 日に実施し，703 件の FQDN を得ることができた．これらの各 FQDN について，インターネット上の DNS ルートサーバから順番に問合せを行い，FQDN の A レコードが登録されている DNS サーバの IP アドレスを取得した．また，その A レコードを参照することで C&C サーバの IP アドレスを取得した．この IP アドレスの取得作業も同日に 1 度のみ実施し，703 件の FQDN のうち DNS サーバの IP アドレスは 353 件，C&C サーバの IP アドレスは 167 件について取得することができた．

なお，この取得作業で DNS サーバや C&C サーバの IP アドレスが発見できなかった FQDN は，少なくともこの作業中にボットネットによって使用されていなかったといえる．また，ボットネットによっては 1 つの FQDN に割り当てている C&C サーバの IP アドレスを短期間に切り替える方式をとっているものもあると考えられるが，この調査では各 FQDN に対して最初に取得することができた IP アドレスを収集の対象とした．したがって，この IP アドレスリストは調査時点でボット端末が接続することができた C&C サーバのリストに相当する．

一般ユーザ端末の推定には，S25R 方式で用いられている判定方法を利用した[7]．S25R 方式はスパムメール対策の方法の 1 つであり，メールサーバに SMTP でアクセスしてきた端末が，ADSL 回線やケーブルネットワークなどのエンドユーザ用回線に接続された一般ユーザ端末かどうかを判定してアクセス制御を行う．判定は IP アドレスの逆引き FQDN を取得し，ADSL 回線やケーブルネットワークで使用される FQDN の特徴と合致するかどうかによって決まる．このための判定ルールは 6 種類あり，我々はボットネットに使用されている DNS サーバと C&C サーバとして利用されている端末についても，これと同じ判定ルールに合致するものを一般ユーザ端末と見なすことにした．

以上の方法に基づいて調査した結果を**表 1** に示す．また，端末が設置されている国別の台数について**図 3** に示す．端末が設置されている国については，MaxMind 社が配布している GeoLite Country を用いて IP アドレスから判別した．なお，国名は国名コードで示している．

表 1 で示したように，一般ユーザ端末の推定のために行った S25R 方式での判定に，ボットネットで使用されている DNS サーバの 31%，C&C サーバの 28%が該当した．ただし，比較のためにボットネットとは関係のない Web サーバの FQDN を 192 件収集して調査したところ，DNS サーバの 14%，Web サーバの 17%が S25R 方式での判定に該当した．こ

表 1　S25R 方式による一般ユーザ端末判定結果
Table 1　Result of end-user terminal investigation.

	S25R の判定ルールに合致	非合致
DNS サーバ数	111(31%)	242(69%)
C&C サーバ数	47(28%)	120(72%)

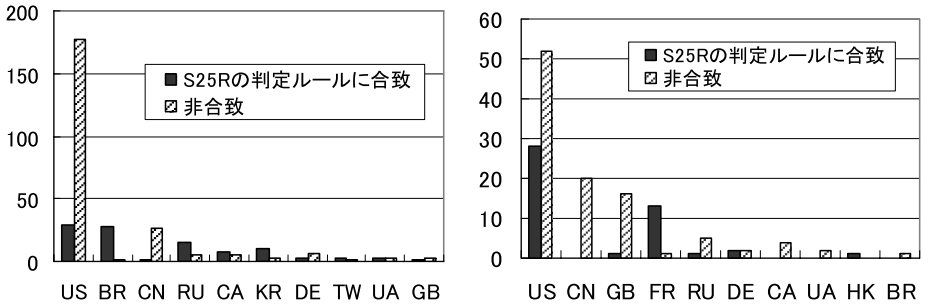

図 3　国別の S25R 方式による一般ユーザ端末判定結果（左図：DNS サーバ，右図：C&C サーバ）
Fig. 3　Result of end-user terminal investigation (Left: DNS server, Right: C&C server).

の 192 件の FQDN は，Google の Web サイト検索で “cat” と “shop” という単語をそれぞれ検索し，その結果得られた上位サイトの URL から抽出した．

ボットネットとは関係のない Web サーバの FQDN での該当割合は，ADSL などの回線下の端末で運用されている DNS サーバや Web サーバが存在している割合と S25R 方式での判定の誤検知の割合の和であると考えられる．仮にすべて S25R 方式の誤検知であり，かつボットネットの FQDN での該当割合の中にも同程度の誤検知が含まれているとしても，ボットネットで使用されている DNS サーバの 17%，C&C サーバの 11%が一般ユーザ端末に該当することになる．このことから，この調査結果に従えばボットネットのサーバとして一般ユーザ端末が利用されている割合は，1 割から 3 割程度と推定される．

国別の判定結果を見ると US，CN，GB などの国は S25R 方式での一般ユーザ端末の判定に合致していない件数が多い．一方で BR，FR，RU，KR，などの国は S25R 方式での一般ユーザ端末の判定に合致している件数が多い．これらの国では一般ユーザの端末が乗っ取られ，ボットネットのサーバとして利用される割合が多いと考えられる．

4.1.2　防弾業者の端末および無管理状態の端末の推定

防弾業者の端末や無管理状態の端末の推定には，Emerging Threats が公開している 2 種類のブラックリストを用いた[8]．1 つはサイバー犯罪グループ Russian Business Network（RBN）が管理している端末の IP アドレスリストである．RBN の端末は犯罪を行うために用意されており，一種の防弾業者と見なすことができる．RBN 以外の防弾業者の端末に関しては，ブラックリストが公開されていない．そこで，他の防弾業者の端末の推定のために，もう 1 つのブラックリストとして C&C サーバの IP アドレスリストを用いた．このリストには長期間削除されずに掲載されている IP アドレスが多数存在する．たとえば 2010 年 1 月 31 日時点で掲載されている 1,644 件の IP アドレスのうち，560 件（34%）が約 9 カ月前（2009 年 4 月 24 日時点）のリストにも掲載されていた．C&C サーバとして長期にわたって活動している端末は，防弾業者の端末あるいは無管理状態の端末と推測できる．

この推定にも，一般サーバ端末の推定の際に使用した DNS サーバと C&C サーバの IP アドレスを使用した．これらの IP アドレスのうち，Emerging Threats から取得した上述の 2 種類のブラックリストに掲載されていた件数を調査した．なお，Emerging Threats からのブラックリストも 2009 年 12 月 28 日に取得したものを使用した．

以上の方法に基づいて調査した結果を**表 2** に示す．また，国別にどちらかのブラックリストに該当する端末の台数について分析した結果を**図 4** に示す．

表 2 で示したように，防弾業者の端末や無管理状態の端末の推定のために行った RBN ブラックリストによる判定では，ボットネットで使用されている DNS サーバの 24%，C&C サーバの 22%が該当している．したがって，この分類に該当する端末が利用されている割合は少なくとも 2 割以上と推定される．加えて，C&C サーバブラックリストによる判定では，DNS サーバの 3%，C&C サーバの 20%が該当した．このことは RBN 以外の防弾業者の端末や長期間無管理状態の端末がボットネットのサーバとして使用されている可能性を示している．

国別の判定結果を見ると BR や GB でボットネットに利用されている端末は，ブラックリストに掲載されている割合が多く，国ごとのばらつきがある．ただし，判定に用いたブラックリストがすべての防弾業者や長期にわたって活動している C&C サーバを含んでいるわけではないため，図 4 で非掲載としてカウントした端末が必ずしも防弾業者や無管理のサーバに該当しないわけではない．

表 2　ブラックリスト掲載数調査結果
Table 2　Result of blacklist publication investigation.

	RBN ブラックリストに掲載	C&C サーバブラックリストに掲載	非掲載
DNS サーバ数	85(24%)	10(3%)	259
C&C サーバ数	36(22%)	34(20%)	104

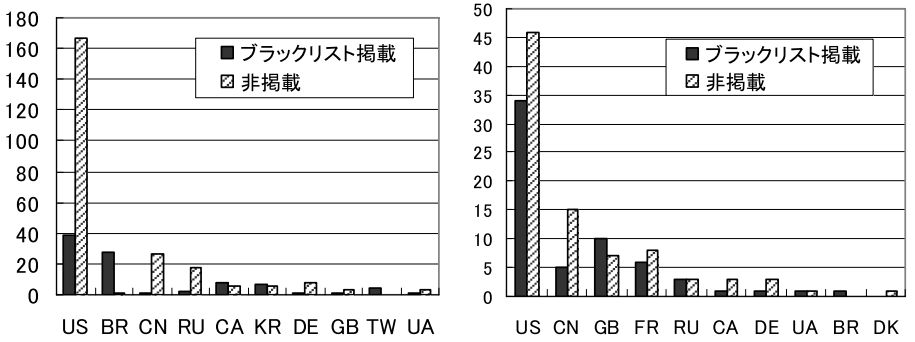

図 4　国別のブラックリスト掲載数調査結果（左図：DNS サーバ，右図：C&C サーバ）
Fig. 4　Result of blacklist publication investigation (Left: DNS server, Right: C&C server).

4.1.3　専門のサーバ管理者の端末の推定

上記の判定で正確に一般ユーザの端末と防弾業者や無管理状態の端末を推定できれば，残

りが専門のサーバ管理者の端末となる．しかし，上記の判定には不確定要素も多く，かつ防弾業者や無管理状態の端末の割合についてはブラックリストにマッチするものだけを計数するため下限値は推定できるが，上限値は分からない．そこで，以下の 2 つの方法で専門のサーバ管理者の端末の割合を推定した．

1 つ目は，C&C サーバ上でカスタマイズされていない IRC サーバが稼動している場合は，専門サーバ管理者と見なすという推定方法である．

ボットネットの C&C サーバとして IRC サーバを利用する場合，ボットマスタ自身が IRC サーバを設置するケースと，一般に公開されている IRC サーバを利用するケースがある．前者の場合，ボットマスタが IRC サーバの設定を自由にカスタマイズでき，たとえばポート番号をデフォルトのものから変更したり，パスワードによるサーバへのアクセス認証などを設定したりすることが可能である．ただし，IRC サーバを設置可能な端末を準備する必要がある．後者の場合，IRC サーバのカスタマイズはできないが，IRC サーバを設置するための端末を準備する必要がない．こちらの方が手間やコストが少ないが，専門のサーバ管理者により管理されている端末上でボットネットを運用することになる．

IRC サーバの設定がカスタマイズされているかどうかを調査するために，Emerging Threats が公開している C&C サーバの IP アドレスリストを取得し，各 IP アドレスに対して，IRC のデフォルトポート（tcp/6667）でパスワードなしでアクセスを試み，アクセスできる件数を調べた．なおカスタマイズされていない IRC サーバを，ここでは公開 IRC サーバと呼ぶことにする．

2 つ目は，C&C サーバの寿命が短ければ専門のサーバ管理者により管理されていると見なす推定方法である．これは専門のサーバ管理者によって監視されている端末の場合，C&C サーバとして使用されても短期間で管理者が気づき，C&C サーバとしての機能を除去される可能性が高いためである．反対に，先述のように長期間 C&C サーバとして稼動している端末は，防弾業者の端末あるいは無管理状態の端末である可能性が高い．

この調査のために，Cyber-TA で公開されている C&C サーバの IP アドレスを取得し，分析した[9]．Cyber-TA はハニーポットによって検出した C&C サーバの IP アドレスを過去の日付ごとに公開しており，これを利用することで各 C&C サーバの寿命（利用期間の日数）を分析することが可能である．

以上の方法に基づいて調査した結果を**表 3** と**表 4** に示す．また，国別に分析した結果を**図 5** および**図 6** に示す．

表 3 で示したように，カスタマイズされていない IRC サーバが起動している C&C サーバの割合は，S25R により一般ユーザ端末と判定されなかった端末に関しては約 49%であった．これらはポート番号やパスワードによるアクセス制御がないため，誰でも使用できるように公開されている IRC サーバである．公開されている IRC サーバの中にも防弾業者の端末や無管理状態の端末が使用されている場合もあると考えられるが，多くの場合，こうした公開型のサーバは専門のサーバ管理者に管理されていると我々は考える．したがって，一般ユーザ端末も含む C&C サーバ全体のうち，4 割程度以上が専門のサーバ管理者の端末と推定される．また，表 4 で示したようにブラックリストへの掲載期間が 7 日未満であっ

表 3　公開 IRC サーバ調査結果
Table 3　Result of open-IRC server investigation.

	公開 IRC サーバ	その他
C&C サーバ数	558	579
割合	49%	50%

表 4　C&C サーバ寿命分析結果
Table 4　Result of C&C server life-time investigation.

	7 日未満	7 日以上
C&C サーバ数	65	42
割合	61%	39%

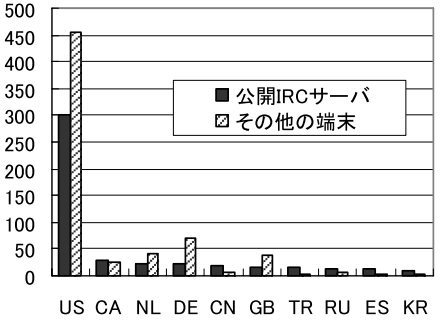

図 5　国別の公開 IRC サーバ調査結果
Fig. 5　Result of open IRC server investigation.

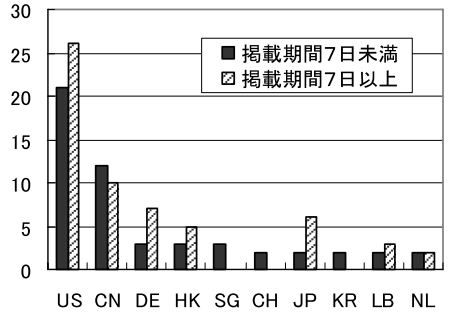

図 6　国別の C&C サーバ寿命分析結果
Fig. 6　Result of C&C server life-time investigation.

た C&C サーバの割合は，S25R により一般ユーザ端末と判定されなかった端末に関しては約 61%であった．

短期間で C&C サーバとしての機能を終えているような端末は，サーバ管理者によって機能停止させられたか，ボットマスタが C&C サーバとして適していないと考えて利用をやめたケースがありうる．いずれの理由にしても，一般ユーザ端末でなく，かつブラックリストへの掲載期間が短い C&C サーバは，専門のサーバ管理者によって管理されている端末上で動作していたと我々は考える．したがって，一般ユーザ端末も含む C&C サーバ全体のうち，専門のサーバ管理者の端末はこちらの調査結果からは 4 割から 5 割程度と推定される．

これは公開型のサーバの面から推定した割合と合致し，かつ一般ユーザ端末の推定結果および，防弾業者の端末や無管理状態の端末の推定結果とも矛盾しない．

国別の判定結果を見ると，一般ユーザ端末や防弾業者の端末の場合とは違い，専門のサーバ管理者の端末と推定される端末は，各国に存在していることが分かる．専門のサーバ管理者の端末は設置されている国によらずボットネットに悪用される可能性があると考えられる．

5. 考　　察

5.1 ボットネット追跡の方針

前章の調査結果から，我々はボットネットのサーバとして利用されている端末の割合を，一般ユーザ端末が 1 割から 3 割程度，防弾業者の端末や無管理状態の端末は 2 割以上，専門のサーバ管理者の端末は 4 割から 5 割程度と推定した．また，専門のサーバ管理者の端末は各国でボットネットに利用されている一方，一般ユーザ端末および防弾業者の端末や無管理状態の端末は国によって利用されている割合に大きな差があると推定した．

この推定結果には次節で述べる誤差が存在する可能性があるが，その誤差が大きくないと仮定すると，ボットネット追跡技術の研究開発や普及に対して次のような指針が得られる．

まず，ボットネット追跡の普及初期には，専門のサーバ管理者の端末に対象を絞って追跡を行えるようにするべきである．これは 3.1 節で述べたように専門のサーバ管理者であれば追跡への協力を得やすく，かつ推定結果からボットネットに利用されている割合が 4 割から 5 割程度と大きいため，このタイプの端末に対象を絞ってもある程度追跡が可能となるためである．また，こうしたサーバの場合，通信ログだけでなく端末のログも追跡に利用できる可能性がある点で，より精度の高い追跡を行うことができる．

すべてのサーバ管理者からの協力を得られるかどうかに関しては今後の課題であるが，もし協力を得られることができると仮定すると，次のことがいえる．ボットマスタが C&C サーバや DNS サーバに接続する際にいくつの踏み台を介しているかは明らかになっていないが，直接接続している場合には，追跡により 4 割から 5 割のボットマスタに到達できる可能性がある．また，踏み台を使用している場合でも，その踏み台が専門のサーバ管理者の端末である割合が同様に 4 割から 5 割程度であれば，踏み台が 1 台の場合で 16%から 25%程度，2 台の場合で 6%から 12%，5 台の踏み台を中継している場合でも 1%から 3%程度到達できる可能性が見込める．

また，今回の調査により，一般ユーザの端末，防弾業者の端末や無管理状態の端末もボットネットで高い割合で利用されていることや，ボットネットで利用されている端末が各国に分散していることを確かめることができた．したがって，さらに高い追跡成功率を得るためには，異なるタイプの端末を監視する方式を連動させ，各国間でボットネット追跡のための連携を行うことが必要になる．このような追跡を実現させるための技術の例として，奈良先端大学が開発に取り組んでいる InterTrack があげられる[10),11)]．

5.2 推定結果の誤差について

一般に，ハニーポットを用いてボット感染端末の通信解析を行うことで，ボット感染端末が直接接続する C&C サーバの FQDN や IP アドレスを調べることができる．一方で，ボットネット追跡を行う技術やシステムが確立していないため，ボット端末が直接接続する C&C サーバ以外の C&C サーバの FQDN や IP アドレスを調査することは非常に困難である．このため，4 章の調査で用いたブラックリストにより取得できる C&C サーバの FQDN や IP アドレスは，C&C サーバの中でもボット端末が直接接続している C&C サーバが大半を占めていると考えられる．したがって，4 章の調査はボット端末が直接接続する C&C サーバに偏った調査といえるが，このような偏りがない調査に必要となるデータ（ブラックリスト）を得ることは現状では難しい．なお，5.1 節ではボット端末が直接接続する C&C サーバとそれ以外の C&C サーバの間で，専門のサーバ管理者の端末が使用されている割合に差がないことを仮定して考察した．

また，4.1.1 項および 4.1.2 項の調査では，C&C サーバの FQDN のブラックリストから C&C サーバの IP アドレスを収集して分析を行ったが，この収集は 1 度だけ実施した．これにより，調査時点でボットから接続され得た C&C サーバ群を対象にして分析を行ったことになる．C&C サーバの FQDN に対応している IP アドレスは短期間のうちに変更されることがあるため，調査のタイミングが違えば得られる IP アドレスも異なり，分析結果にも影響が出た可能性もある．今回の調査は端末利用割合の概数の推定にとどめたが，より精度の高い分析を行うためには，適切な期間を決めて複数回 IP アドレスの取得を行い，取得タ

イミングによるバラつきについても確認する必要がある．

6. おわりに

ボットネット追跡では，追跡経路上に存在している端末の管理者の協力を得ることが追跡には不可欠であるという観点から，端末を一般ユーザの端末，専門サーバ管理者の端末，防弾業者の端末あるいは無管理状態の端末という 3 種類に分類し，ボットネットに使用されている割合を推定した．また，国ごとの分布に関しての調査も行い，特に専門サーバ管理者の端末が各国に分散していることを示した．これらの結果を基に，ボットネット追跡の研究開発や普及に際して，最初は専門サーバ管理者の端末を対象とすることが効果的であるという指針を示した．また，より高い追跡率の実現のためには，国家間や異なる追跡方式間の連携を行う技術が必要になると考えられる．

参考文献

1) Zhu, Z., Lu, G., Chen, Y., Fu, Z.J., Roberts, P. and Han, K.: Botnet Research Survey, *Proc. 32nd Annual IEEE International Conference on Computer Software and Applications* (*COMPSAC '08*), pp.967–972 (2008).
2) Stone-Gross, B., Cova, M., Cavallaro, L., Gilbert, B., Szydlowski, M., Kemmerer, R., Kruegel, C. and Vigna, G.: Your Botnet is My Botnet: Analysis of a Botnet Takeover, *Proc. 16th ACM Conference on Computer and Communications Security*, pp.635–647 (2009).
3) Gostev, A.：今日の情報社会における脅威，2007 年第 3 四半期，ViruslistJP.com（オンライン），入手先 ⟨http://www.viruslistjp.com/viruses/analysis/?pubid=204791973⟩ (参照 2010-08).
4) 甲斐俊文，佐々木良一：効果的なボットネット追跡のための追跡経路モデル化と統計調査，コンピュータセキュリティ研究会（CSEC49），pp.1–7 (2010).
5) Ramsbrock, D., Wang, X. and Jiang, X.: A First Step Toward Live Botmaster Traceback, *Proc. 11th International Symposium on Recent Advances in Intrusion Detection*, pp.59–77 (2008).
6) DNS-BH – Malware Domain Blocklist, DNS-BH (online), available from ⟨http://www.malwaredomains.com/⟩ (accessed 2009-12).
7) 浅見秀雄：阻止率 99%のスパム対策方式の研究報告—Selective SMTP Rejection (S25R) 方式，Gabacho-Net（オンライン），入手先 ⟨http://gabacho.reto.jp/anti-spam/anti-spam-system.html⟩ (参照 2009-12).
8) Emerging Threats, Emerging Threats (online), available from ⟨http://www.emergingthreats.net/⟩ (accessed 2009-4-24).
9) Cyber – TA Research and Development Project: Cyber-Threat Analytics, Cyber-Threat Analytics (online), available from ⟨http://www.cyber-ta.org/⟩ (accessed 2009-7-5).
10) Hazeyama, H., Matsumoto, Y. and Kadobayashi, Y.: Message Forwarding Strategies for Inter-AS Packet Traceback Network, *Proc. 2nd Joint Workshop on Information security* (Aug. 2007).
11) 若狭賢他：インターネットにおけるトレースバックシステムの ISP 実ネットワークにおける大規模実証実験の紹介，コンピュータセキュリティシンポジウム 2009（CSS2009），pp.247–252 (2009).

(平成 22 年 5 月 21 日受付)
(平成 22 年 11 月 5 日採録)

甲斐　俊文（正会員）

平成 12 年九州工業大学情報工学部知能情報工学科卒業．平成 14 年九州工業大学大学院情報工学研究科博士前期課程修了．同年松下電工株式会社（現パナソニック電工株式会社）入社．トレースバック技術をはじめとするネットワークセキュリティ技術の研究開発に従事．

佐々木良一（フェロー）

昭和 46 年 3 月東京大学卒業．同年 4 月日立製作所入社．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．平成 13 年 4 月より東京電機大学工学部教授，平成 19 年 4 月より未来科学部教授．工学博士（東京大学）．平成 10 年電気学会著作賞受賞．平成 14 年情報処理学会論文賞受賞．平成 19 年総務大臣表彰等．著書に，『IT リスクの考え方』（岩波新書，2008 年）等．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会長，内閣官房情報セキュリティ補佐官．