Vol.2010-CSEC-49 No.3
2010/5/11

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

甲斐俊文[†]　　佐々木良一[††]

ボットネットの被害が増大してきており，ボットマスター（ハーダ）まで追跡することが重要な課題となっている．そのため追跡経路の分析を行い５つに分類できることを示した．このうち有効な追跡経路はボットネットによって異なるが，有効な通信経路であっても，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．現在，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統計的に調査している．現時点での調査結果から，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割程度と見積もれることが明らかになった．

Modeling and Statistics of Tracking-path for an Effective Botnet Traceback

Toshifumi Kai[†]　and Ryoichi Sasaki[†]

The damage of botnet is increasing, and it is an important problem to track bot masters. We analyzed tracing paths of bo tnet and classified these under 5 p atterns. And if there are ter minals of bulletproof p roviders o r end user s on a path , tracing on th e path is difficult. No w we ar e examining a r atio of bo tnet using a terminal of bul letproof providers and end user s. We hav e examined a ratio of botn et us ing a ter minal of bulletproof p roviders and end us ers. As a result, we e stimated th e ratio of the botn et which used ter minals of end us ers at around 30% f rom 10% , bulletp roof pr oviders at least 20%, and normal server managers at around 50% from 40%.

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充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いまだ現れていない[1][2].

我々は，ボットネットを管理しているボットマスター（ハーダとも言う）まで追跡可能としなければ十分な抑止効果は挙げられないと考えている．そこで，その手がかりとなるボットネットの追跡に着目し，効果的なボットネット追跡システムを実現するために，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，ボットマスター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辿る行為である．従って，ボットマスターによる手続きや通信の経路が，追跡経路となる．この考えに基づくと，ボットマスターからの命令伝達経路，Command & Control サーバ（以下 C&C サーバ）の契約経路，DNS サーバへの C&C サーバ完全修飾ドメイン名（FQDN）登録経路，DNS サーバの契約経路，ドメイン名の契約経路の５つが追跡経路となる．なお，有効な追跡経路はボットネットによって異なる．例えばドメイン名を使用しないで C&C サーバへアクセスするようなボットネットは DNS サーバを使用しないため，追跡経路は限られる.

ボットネットの追跡可能性は，追跡経路上にある装置の管理者の特性に大きく左右される．例えば，追跡経路上の端末の管理者がボットマスター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．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.

我々は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するために，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統計的に調査している．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，対策の方針を固める上で重要なものであると考えている.

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

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

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章で調査結果に対する考察を述べる．

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，ボットマスター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挙げる．その手順を踏まえて，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．

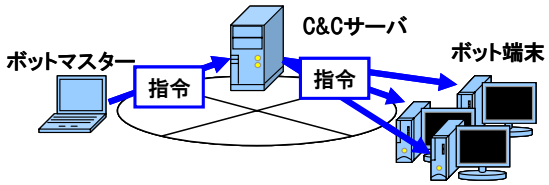

図 1　ボットネットの構成

ボット端末は C&C サーバと接続し，ボットマスターからの指令を待つ．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言われており，その他にも 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 サーバの他に，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異なるが，ボットマスター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．

また，ボットマスター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．踏み台サーバは例えば ssh サーバや http proxy サーバなどを利用することで実現でき，ボットマスター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，単にボット型マルウェアを配布するだけでなく，以下のような C&C サーバやドメイン名に関する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
- 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

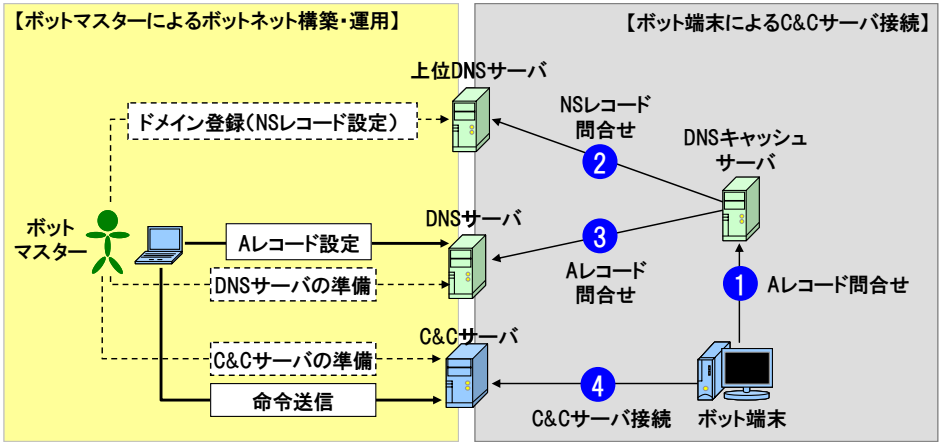

図 2　ボットネット構築・運用とボット端末による C&C サーバ接続手順

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ー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，無料利用が出来る 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（リセラー）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．

2.3 ボットネットの追跡経路

ボットネットの追跡は，ボットマスター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辿る行為である．従って，ボット端末への指令の伝達だけでなく，前節で示したボットネット構築の手順が追跡経路となる．ただし，C&C サーバや DNS サーバを見つける作業が先に必要になる．

ボット端末の通信やボットコードを解析することで，C&C サーバの FQDN や IP アドレスを把握することができる．なお，ボット端末の通信やボット型マルウェアのコードは，ハニーポットや実際の感染端末から取得できる．

C&C サーバの FQDN が分かれば，NS レコードが設定されている DNS サーバと A レコードが設定されている DNS サーバを見つけることができ，加えて C&C サーバの IP アドレスも取得できる．

これらの情報を元にして，下記の５つの追跡経路が考えられる．

- NS レコードが設定されている DNS サーバから，固有ドメイン名登録者を追跡
- A レコードが設定されている DNS サーバから，A レコード設定の経路を追跡
- A レコードが設定されている DNS サーバから，DNS サーバ準備の経路を追跡
- C&C サーバから，ボットネットへの指令送信経路の追跡
- C&C サーバから，C&C サーバの準備経路を追跡

全てのボットネットにおいてこの５つの追跡経路が有効であるわけではないが，ボットネットへの指令送信経路は，どんなボットネットでも追跡経路として有効である．

なお，固有ドメイン名登録者の追跡や，サービスを利用する形での DNS サーバや C&C サーバの準備の追跡は，契約情報を追跡していくことになる．一方，A レコード設定や指令送信経路，または不正侵入で DNS サーバや C&C サーバを準備した場合などは，ネットワーク上での通信を追跡することになる．

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ーからのボット端末や DNS サーバに至るまでの通信を，順番に遡って辿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[3].

文献 3)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出来ない．

なお，契約を伴う追跡経路の場合，追跡はネットワーク上での通信を辿る行為ではなく，契約情報から真の契約者を割り出す行為である．例えばボットマスター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（リセラー）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ー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ー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・大学等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，追跡への協力は全く期待できない．

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，DNS サーバと C&C サーバの統計調査を行った．

4.1 調査方法

4.1.1 一般ユーザ端末の推定方法

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，一般ユーザの端末数を推定した．

ボットネットに使用されている端末の IP アドレスは, ボットネットで使用されている FQDN のブラックリストを利用して収集した．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 にて公開されているものを使用した[4]. この Web サイト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．抽出した 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い合わせを行い, FQDN の A レコードが登録されている DNS サーバと C&C サーバの IP アドレスを取得した．

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[5]. S25R 方式はスパムメール対策の方法の一つであり，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ー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みなすことにした．

参考のために，ボットネットとは無関係のノーマルな FQDN リストに対しても同様の調査を行った．このノーマルな FQDN はインターネットの検索エンジン（Google）にて，ボットネットと関係の無いキーワードとして”cat”および”shop”を検索し，検索結果の上位に挙がったリンクから得たものである. この FQDN から A レコードが登録されている DNS サーバと Web サーバの IP アドレスを取得し，同様の方法で一般ユーザ端末の判定を行った．

4.1.2 防弾業者の端末および無管理状態の端末の推定方法

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[6]．１つはサイバー犯罪グループ Russian Bus iness 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，一種の防弾業者とみなすことができる．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，もう一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．例えば 2010 年 1 月 31 日時点で掲載されている 1644 件の IP アドレスのうち，560 件（34%）が約 9 ヶ月前（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と同じくボットネットの FQDN から取得した DNS サーバと C&C サーバの IP アドレスを対象とした．また，ノーマルな FQDN も同じものを使用した．

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，上限値はわからない．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 サーバか稼動している場合は，専門サーバ管理者とみ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，ボットマスター自身が 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，ボットマスターが IRC サーバの設定を自由にカスタマイズでき，例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．

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み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[7]. 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毎に公開しており，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．

4.2 調査結果

前述の一般ユーザ端末や防弾業者の端末の推定のために，2009 年 12 月に実施した調査結果を表 1 と表 2 に示す．表 1 は FQDN の A レコードが登録されている DNS サーバに関する判定結果であり，表 2 はボットネットの場合は C&C サーバ，ノーマルな FQDN の場合は Web サーバに対する判定結果である．

また，専門のサーバ管理者の端末を推定するために実施した調査の結果を表 3 と図 3 および表 4 に示す．

表 1　DNS サーバの端末分類調査の結果

	ボットネット	ノーマル
調査した FQDN 件数	703	192
DNS サーバの発見件数	353	192
S25R 方式の一般ユーザ端末判定ルールに合致した件数	111(31%)	27(14%)
RBN ブラックリストに掲載されていた件数	85(24%)	0(0%)
C&C サーバブラックリストに掲載されていた件数	10(3%)	0(0%)
上記の何れにも該当しない件数	204(58%)	165(86%)

表 2　C&C サーバの端末分類調査の結果

	ボットネット	ノーマル
調査した FQDN 件数	703	192
IP アドレスの取得件数	167	100
S25R 方式の一般ユーザ端末判定ルールに合致した件数	47(28%)	17(17%)
RBN ブラックリストに掲載されていた件数	36(22%)	0(0%)
C&C サーバブラックリストに掲載されていた件数	34(20%)	0(0%)
上記の何れにも該当しない件数	80(48%)	83(83%)

表 3　カスタマイズされてない IRC サーバ調査の結果

	S25R のルールに該当	S25R のルールに非該当
C&C サーバ件数　※	269	1137
カスタマイズされていない IRC サーバが起動している件数	117(43%)	558(49%)
上記に該当しない件数	152(57%)	579(51%)

※Emerging Threats より 2009/4/24 に取得

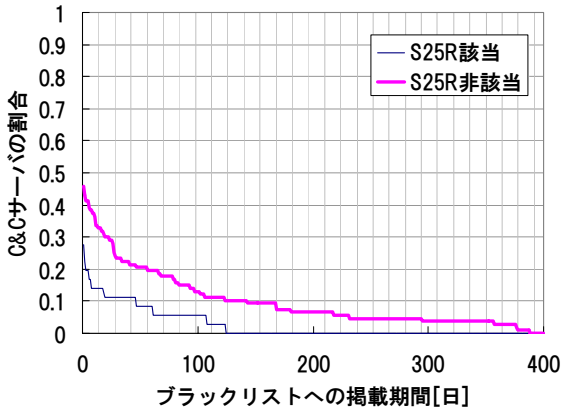

図 3　C&C サーバの寿命分析

表 4　C&C サーバの寿命分析の結果

	S25R のルールに該当	S25R のルールに非該当
C&C サーバ件数 ※	36	107
ブラックリストへの掲載期間が7日未満の件数	30(83%)	65(61%)
ブラックリストへの掲載期間が7日以上の件数	6(17%)	42(39%)

※Cyber-TA より 2009/7/5 に取得

5. 考察

5.1 調査結果からの推定

5.1.1 一般ユーザ端末の推定

表 1 と表 2 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，ノーマルな FQDN での結果をみると，DNS サーバの 14%，Web サーバの 17%が該当している．このノーマルな 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．仮に全て 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．

5.1.2 防弾業者の端末および無管理状態の端末の推定

表 1 と表 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．従って，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．

5.1.3 専門のサーバ管理者の端末の推定

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．従って，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．図 3 で示しているように，掲載期間が１日しかない C&C サーバも半数以上の割合である．

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，ボットマスターが 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有り得る．何れの理由にしても，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．従って，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．

5.2 ボットネット追跡の可能性

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ようなことが言える．

専門のサーバ管理者の端末の割合が大きいため，専門のサーバ管理者に追跡の仕組みを普及させるだけでも，多くのボットネットを追跡できる．ボットマスターが 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，追跡によりボットマスターに到達可能である．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のみであれば，同様にボットマスターまで到達可能である．

踏み台として一般ユーザの端末，防弾業者の端末，無管理状態の端末が使用されるとボットマスターまでの到達はできない．ただし，C&C サーバや DNS サーバの先までの追跡が実現できれば (a)抑止効果(b)踏み台のブラックリストの作成(c)さらなる追跡方法の研究への貢献，が期待できると我々は考えている．

ユーザ端末は国内の端末の場合は NAT の下にあることが多く, グローバルアドレスが必須となるような C&C サーバにはなりにくい．しかし調査結果からは一般ユーザの端末も C&C サーバとして数多く使われていると考えられる．一般ユーザ端末の場合は前述の通りユーザ自身に追跡作業や追跡システムの導入は期待できないため，工夫が必要になる．一般ユーザが回線契約している ISP（インターネット・サービス・プロバイダ）が追跡を行うという手が考えられるが，プライバシの問題が大きい．IP トレースバックシステムに関しては ISP に導入できるようプライバシを保護する技術と運用方法が提案されている[8]．ボットネットの追跡システムにおいてもプライバシを侵害しない仕組みができれば，一般ユーザ端末も含めた追跡を実現できる．

また，調査結果より防弾業者の端末がボットネットで利用されているケースも多いことが分かった．こうした業者が関わっているようなボットネットに関しては，通信の追跡は極めて困難であるため，司法機関（警察）に頼るか，追跡以外の方法で対策を講じる必要がある．

6. おわりに

ボットマスターがボットネットを構築する手順と運用手順を考慮して追跡経路が５つあることを整理した．このうち２つがボットマスターによる通信に対する追跡経路であった．通信に対する追跡では，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種類に分類した．そしてインターネット上で公開されている C&C サーバの IP アドレスや FQDN のリストを対象に調査を行った結果を基にして，一般ユーザの端末が１割から３割程度，専門のサーバ管理者の端末が４割から５割程度，防弾業者の端末および無管理状態の端末が２割以上であると推定した．

今後も調査を継続しつつ、推定値の信頼度を向上させていく必要があると考えている．また，専門のサーバ管理者の端末や一般ユーザの端末を対象とした追跡システムの開発を目指して、導入課題の整理を行う予定である。

参考文献

1) Zhaosheng Zhu, Guohan Lu, Yan Chen, Fu, Z.J., Roberts, P., and Keesook Han: Botnet Research Survey, Computer Software and Applications Conference, 2008
2) B. Stone-Gross, M. Cova, L. Cavallaro, B. Gilbert, M. Szydlowski, R. Kemmerer, C. Kruegel, and G. Vigna : Your Botnet is My Botnet: Analysis of a Botnet Takeover, Technical report, University of California, May 2009
3) Daniel Ramsbrock, Xinyuan Wang, Xuxian Jiang: A First Step Toward Live Botmaster Traceback, Proceedings of the 11th International Symposium on Recent Advances in Intrusion Detection, Sep 2008.
4) DNS-BH - Malware Domain Blocklist, http://www.malwaredomains.com/
5) 阻止率 99%のスパム対策方式の研究報告 ～Selective SMTP Rejection (S25R)方式～ http://gabacho.reto.jp/anti-spam/paper.html
6) Emerging Threats, http://www.emergingthreats.net/
7) Cyber-Threat Analytics, http://www.cyber-ta.org/
8) 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 IS P 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