情報処理学会論文誌　Vol. 52　No. 12　3766–3774 (Dec. 2011)

ボットネット多段追跡システムにおける最終段階追跡方式の提案と評価

名雲 孝昭[†1]　甲斐 俊文[†2]　佐々木 良一[†3]

これまで，ボットネットの追跡はボットに感染している端末（ボット PC）の検知だけであり，実際に命令を行ったハーダ PC までたどり着くことができなければ根本的対策とはならないにもかかわらず，データの不足など困難な要因が多く適切な対策の提案はなかった．そこで著者らは，ボットネットのハーダ PC の追跡を可能とするための第 1 歩として，ボットネット多段追跡システムという，3 つに分かれた追跡システムの最終段階として，DDoS などの攻撃を受けてから攻撃者であるハーダ PC を特定する方法を提案する．また，その有用性を実際にボットデータを使って評価する．さらに，どのぐらいの確率でハーダ PC までたどり着けるかを推定できるようにするためボットネット追跡性評価シミュレータを開発した．あわせて，別途収集したデータとこのシミュレータを組み合わせることにより，種々の対策をとった場合に追跡可能性がどのように改善されうるかを評価したので報告する．

Proposal and Evaluation of Final Step Tracing Method in Botnet Multistep Tracing System

Takaaki Nagumo,[†1] Toshifumi Kai[†2]
and Ryoichi Sasaki[†3]

Technique to trace Botnet has been limited to detect a Bot PC which is the terminal infected with Bot. However, for achieving basic countermeasure, the method to trace back Herder PC has been expected, though it is very difficult caused by shortage of data etc. As a first step, we proposed multistep tracing system to detect the PC of real attacker. This paper deals with the proposed method for final step to detect the PC and the experiment using the real Bot. Futhermore, to enable us to tracing Herder PC in Botnet, we develop Botnet traceability evaluation simulator to estimate how much probability to be able to reach Herder PC. We report evaluation method and the result on traceability probability to Herder PC when various measures were taken.

1. はじめに

近年，ボットネットによる被害が増大している[1)]．ボットネットとは，ボットプログラム（以下ボットという）に感染させられることにより，第三者の PC からロボットのように自由に操作できるようになってしまった PC（以下ボット PC という）などで構成されたネットワークのことである．ボット PC を使った攻撃手法は，DDoS（Distributed Denial of Service）攻撃，スパムメールの送信，通信盗聴，キーロギング，新しいマルウェアの拡散などがあげられる．その目的は，会員サイトやゲームの ID・パスワードなどの個人情報の収集から，サービスを停止させる業務妨害まで多岐にわたる[2)]．

これらボットネットに対して現在まで様々な調査・分析[3)–5)] や，対策手法が検討されてきた．特に，IRC（Internet Relay Chat）の通信分析や挙動解析から，ボット PC の検出方法はいろいろ研究されている[6),7)]．また，その先の C&C サーバの特定も研究対象となりつつある[8)]．それぞれ効果は一定に出ているという報告はあるが，それだけではいまだボットネットによる被害は抑えきれていない．その理由として，あるボット PC による通信をフィルタリングなどで防いだり，見つけてボットを取り除いたりしたとしても，ボットネットを統制するハーダ PC を取り除かない限り，また別のボット PC が出現するため，根本的対策となりえていないからである．また，通常の Anti Virus ソフトや IDS（Intrusion Detection System）でボットを検知する場合，少しでもプログラムや挙動が変わっているとボットだと判定できないという理由もある．特に，新しい脆弱性をつくような最新のボットなどに対しては，そもそも登録されていないため，この困難性がより顕著となる．

そこで著者は，当然重要視されるべきであるが，現実的でないとされ従来研究が行われてこなかった，ハーダ PC の追跡，検知に目を向けた．これにより，その管理下にあるボット PC や C&C サーバを無効化し，大幅に被害を減らせると考えているからである．また，ハーダとなった不正者を逮捕することは同様な不正に対する抑止効果も期待できる．そこで，ボットネットを技術的に追跡可能であるかといった実験評価，および評価シミュレータによるボットネット追跡可能性の評価を行う．

†1 NTT 情報流通プラットフォーム研究所
NTT Information Sharing Platform Laboratories, NTT Corporation
†2 株式会社パナソニック電工
Panasonic Erectric Works Co., Ltd.
†3 東京電機大学
Tokyo Denki University

2. ボットネット追跡の前提

ボットネット追跡を行うにあたって，対象とするボットネットの構成をまとめ，追跡の流れを示す．

2.1 ボットネットの構成

ボット PC はハーダもしくはボットマスタとよばれるボットネットを統制する者の PC（以下ハーダ PC という）から，C&C（Command and Control）サーバとよばれる指令サーバを中継して命令を受け取り，いっせいに前述のような攻撃を開始する（**図 1**）．さらに，C&C サーバとハーダ PC の間には踏み台があるとされている．これは，ハーダ PC が追跡を困難にさせるため，ネットワーク上の別の端末から攻撃命令を送るためのものである．またこのほかにも，ボットネットの実行プログラムを配布するためのダウンロードサーバもボットネットの構成の 1 つであるが，本論文では C&C サーバと同様に扱う．

2.2 ボットネット多段追跡について

ボットネットの多段追跡は，著者らの研究室で提案され研究が進められてきたもので，ボットネットの攻撃の流れとは反対に，被害端末からハーダ PC まで追跡するものである．これは主に 3 段階に分かれており，それぞれ被害端末からボット PC，ボット PC から C&C サーバ，C&C サーバからハーダ PC となっている．ここで，第 1 段は，IP トレースバック[9] とよばれる技術で追跡を行う．第 2 段は，特定の IP アドレスやドメインのブラックリストと照合して追跡を行う[10),11)]．最終段階の追跡では，第 2 段で C&C サーバが特定され，パケットキャプチャができる前提におけるハーダ PC の追跡について，踏み台間の渡り歩き検出手法[12)] などを用いることで追跡を進める．本論文では，特にこの最終段階追跡について検討を行う．

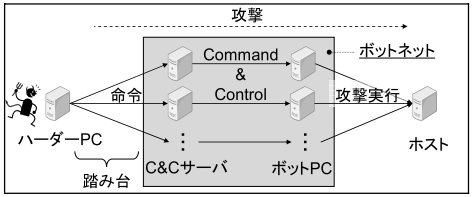

図 1　ボット PC を使った攻撃の流れ
Fig. 1　The attack flow with bot PC.

3. 最終段階追跡方式の提案

3.1 末端踏み台 PC の追跡

C&C サーバのパケットログが何らかの方法で取得ができていることを前提とする．ただし，すべての C&C サーバで取得できる必要はなく，5 章で述べるように特定の確率を満たせばよい．また，以下では特に IRC を用いたボット追跡について議論する．

C&C サーバへ直接命令した踏み台 PC（以下末端踏み台 PC という）の，ネットワーク管理者による追跡フローチャートを**図 2** に示す．ここで末端踏み台 PC の特定までそのログ情報を利用する．ただし，② における攻撃命令の判定は，通信の文字列中に「flood」などのようなキーワード，IP アドレス，ドメイン名などが含まれていたり，自然文でないようなものであったりする場合に yes と判定するものとする．なお，攻撃命令文はボットにより変わることがあるが，本研究では代表的なボット命令文[2)] で検討する．

また，実際はボットが使う IRC に用いられるポート番号が，IRC の規定ポート番号（6667 番など）ではなく，HTTP のポート番号（80 番や 8080 番）に扮するようなアプリケーション情報の偽装が実際に報告されている[13)]．この偽装により，ボットが使用する IRC 通信を選出しにくくするだけでなく，ファイアウォールなどで IRC の規定ポートを閉じている企業内で，ボットネットが IRC 通信を強制的に行うためだと考えられる．アプリケーション情報の偽装に対応するためには，C&C サーバがあるネットワーク上にアプリケーション特定

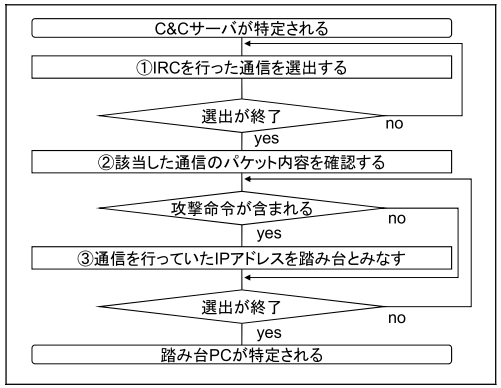

図 2　踏み台 PC の特定フローチャート
Fig. 2　Flowchart to identify stepping stone.

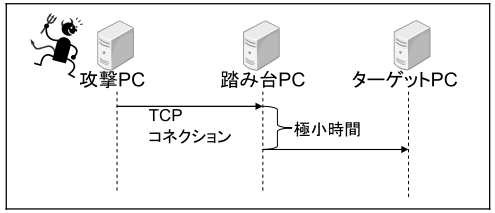

図 3　渡り歩きのモデル
Fig. 3　Model of island hop.

機能を持つファイアウォールなどがあればよい．このようなファイアウォール（たとえば日立システムアンドサービスの PaloAlto シリーズなど[14]．以下「AP 特定機能付 FW」という」）があれば，攻撃命令コードが送られてきた際のログを的確に残しておくことができる．

3.2　ハーダ PC の追跡

続いて末端踏み台 PC からハーダ PC まで追跡を進める．これは，前述のとおり C&C サーバへの指令は踏み台 PC を経由して送信されていることが想定されるためである．ハーダ PC は踏み台 PC 間を Telnet や SSH などの遠隔操作用のプロトコルを用いたソフトウェアを使って渡り歩いているとされる．

踏み台 PC 間をたどっていくには，渡り歩きの検出手法[12] を適用する．渡り歩きは，渡り歩きを行う攻撃 PC，攻撃 PC がリモートログインする踏み台 PC，最終的にアクセスされるターゲット PC というモデルで考えられている（**図 3**）．まず攻撃 PC が踏み台 PC へリモートログインするために，TCP コネクションの確立を行う．続いて，踏み台 PC 宛のリモートログインの通信パケットを検出した後のごく短い間に，踏み台 PC からのターゲット PC 宛の新たな TCP コネクション確立要求を検出した場合，攻撃 PC が踏み台 PC に TCP サービスを起動するコマンドを送信した可能性があり，渡り歩きをした可能性があるといえる．この提案方式をネットワーク型機器として実装して動作確認を行ってみると，踏み台攻撃の検出が確認できる[12]．

ここで，攻撃者 PC をハーダ PC，ターゲット PC を C&C サーバにおきかえ，監視端末を AP 特定機能付き FW とすることで，本提案手法でも利用することが可能となると考え実験により確認することとした．

表 1　使用したソフトウェア
Table 1　The used software for experiment.

ボット	RxBot 7.6 Agobot 3
パケットキャプチャ	Wire Shark 1.0.3
IRC サーバ	irc 2.10
IRC クライアント	Riece 5.0.0

4. 実　　験

4.1　実験目的

隔離したネットワークとボットプログラム，PC 端末を用意し，攻撃を起こしてから C&C サーバから踏み台 PC の追跡が技術的にできるかを模擬実験する．提案方式において確実に踏み台 PC を見つけることができれば，ハーダ PC まで特定することができると見なせる．

4.2　実験環境

PC を 3 台用意し，それぞれ PC1，PC2，PC3 とする．PC1 の仮想マシン（以下 VM とする）上でハーダ PC と攻撃対象 PC を，PC2 の VM 上で踏み台 PC と C&C サーバを動かした．なお，このボットプログラムは VM 上で動作していると判断すると自身を消す機能があるため，PC3 の実機上においてボットプログラムを実行した．使用したソフトウェアは**表 1** のとおりである．

ここでボットプログラムとして採用したボットは，基本的に IRC 接続型のプログラムであり，各々の IP アドレスやボットパスワードなどの設定を自分で変更することができるので，本実験に採用した．そのソースコードはインターネットで取得したものである．

4.3　実験手順

ボットの動作確認を含めて，以下の 9 つの手順を踏んだ．ただし，手順 ⑧，⑨ については図 2 のフローチャートを前提に確認するものとする．

① C&C サーバでパケットキャプチャを開始する．
② ボット PC でボットプログラムを実行する．
③ ボット PC が C&C サーバの IRC へ接続することを確認する．
④ ハーダ PC から踏み台 PC へ Telnet で攻撃命令を送る．
⑤ 踏み台 PC が C&C サーバへ転送することを確認する．
⑥ ボット PC が C&C サーバの IRC 上で命令を受け取ることを確認する．

⑦ ボット PC が攻撃対象 PC を攻撃することを確認する．
⑧ C&C サーバ上で IRC 通信を選出する．
⑨ C&C サーバ上からパケット内容を見て踏み台 PC の IP アドレスを特定する．
実験環境と実験手順を**図 4** に載せる．

4.4 実 験 結 果

手順 ④ の攻撃命令で**図 5** のとおり ping flood を行った．ここでは，踏み台 PC から攻撃対象へ ping 数，パケットサイズ，タイムアウト時間を指定して攻撃を行った．結果，手順 ⑧ で IRC 通信を選出後，手順 ⑨ において WireShark で同等のパケット内容が確認され，その攻撃命令を出したのがその IP アドレス 192.168.0.10 であることが確認された．そのほかにも syn flood，download 命令も同様の手順で確認することができた．

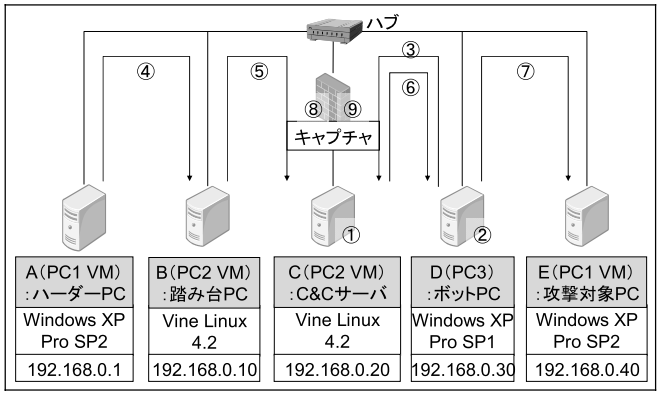

図 4　実験環境と実験手順
Fig. 4　The environment and procedure for experiment.

```
:isl!~isl@192.168.0.10 PRIVMSG #pwn :
   .pingflood 192.168.0.40 100 4096 30
PRIVMSG #pwn:
   [PING]:Sending 100 pings to 192.168.0.40.
   packet size: 4096, timeout: 30(ms).
PRIVMSG #pwn :
   [PING]:Finished sending pings to 192.168.0.40.
```

図 5　攻撃命令のパケット内容（Rxbot）
Fig. 5　The packet data for attack command.

4.5 実 験 評 価

このように AP 情報の偽装を行っていない場合に，C&C サーバから踏み台 PC を技術的に特定することができた．偽装などがあっても AP 特定機能付 FW を用いると，偽装突破はもちろん，時間差攻撃や暗号化など通常困難とされる追跡にもこの提案手法を応用していくことができる．

5. 評価シミュレータ

本章では，4 章のような追跡をネットワーク管理者間で行っていった場合，具体的にどの程度追跡できるかを評価する．

5.1 ハーダ PC 追跡可能確率計算式

先に述べたとおり，ハーダ PC が 1 台だと仮定すると，ボット PC との間には，C&C サーバや複数の踏み台 PC 群が経由されている可能性があり，ハーダ PC から下位層に行くに従って枝分かれする多分木構造となっている．ただし，同時に存在するボット PC がすべて同じハーダ PC 管理下にいるとは限らず，現実的には複数のハーダ PC があると想定すべきである（**図 6**）．このとき，ある端末からあるハーダ PC まで追跡する道を経路，すべての経路の総数を経路数とよぶ．

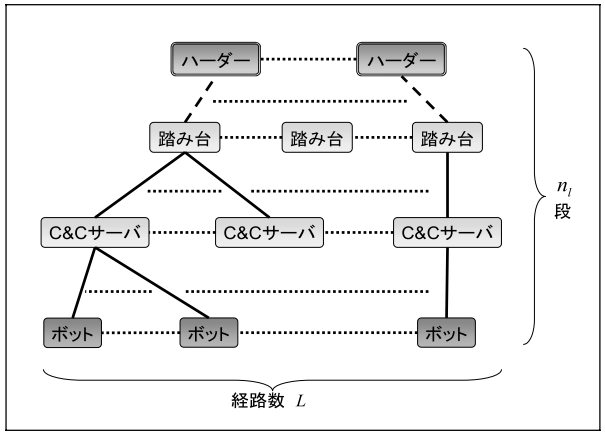

図 6　考えうるボットネット構造
Fig. 6　The considerable botnet structure.

ここで，追跡を開始するボット PC からハーダ PC までの追跡確率を算出し，さらにそれらの値を経路数分計算することで，いずれかのハーダ PC まで到達できる確率 P を算出する．

まず，ある経路 l 段数 i における技術的な追跡可能確率（以下，追跡可能確率とよぶ）$\hat{p}_{li}$ は次式で算出することができる．

$$\hat{p}_{li} = t_{li}c_{li}$$

ここで，t_{li}：経路 l 段数 i における追跡成功確率，c_{li}：経路 l 段数 i における追跡に同意し協力してもらえる確率（以下，追跡協力確率とよぶ）とする．

今，経路の数が L，経路 l の段数が n_l だとするとハーダ PC 追跡可能確率 P は以下の式で算出できる．

$$P = 1 - \prod_{l=1}^{L}\left(1 - \prod_{i=1}^{n_l}\hat{p}_{li}\right) \tag{1}$$

ここで，我々の調査結果[15] より，経路 l 段数 i のコンピュータの管理者が bullet-proof とよばれるハーダなどに協力する業者（以下，防弾業者とよぶ）の場合，一般ユーザの場合，専門サーバ管理者の場合の 3 つに分けて考えることとした．それぞれの場合の比率を b_{li}，b'_{li}，b''_{li}，それぞれの場合の追跡成功確率を T_{li}，T'_{li}，T''_{li} とすると，t_{li} は次式で表せる．

$$t_{li} = b_{li}T_{li} + b'_{li}T'_{li} + b''_{li}T''_{li}$$

同様に我々の調査結果[15] から，$b_{li} = 0.2$，$b'_{li} = 0.3$，$b''_{li} = 0.5$ と推定された．

また，c_{li} の値は国内と海外で違うと考え

$$c_{li} = C_{li}\text{（国内の場合）} \tag{2}$$

$$c_{li} = f_{li}C_{li}\text{（海外の場合）} \tag{3}$$

とした．ここで，C_{li} は基本的な協力確率とし，海外の端末においてはこれに特定の係数（以下，海外端末係数とよぶ）f_{li} をかけるものとする．f_{li} の値はやや小さなものと考えられ，0.1 とおいた．また，追跡する端末が海外にある比率（以下，海外端末比率とよぶ）は a_{li} とすれば，c_{li} は次式で表される．

$$c_{li} = C_{li}(1 - a_{li}) + f_{li}C_{li}a_{li} \tag{4}$$

なお，L や n_l の値が大きいならハーダ PC 追跡可能確率 P は近似的に総和で表すことができる．

$$P \cong \sum_{l=1}^{L}\prod_{i=1}^{n_l}\hat{p}_{li} \tag{5}$$

これは，有用な追跡経路がいくつか存在すれば，他の経路からの追跡可能確率が 0 であっても，最終的なハーダ PC 追跡可能確率が大きくなるということを意味している．

以降で，示したハーダ PC 追跡可能確率計算式をシミュレーションプログラム化し，パラメータを設定して，実際にどの程度ハーダ PC を追跡できるかを評価する．

5.2　パラメータ設定

本節では，追跡を行うにあたって先の変数のパラメータ設定をまとめる．まずどの範囲であれば追跡可能かを知るため，n_l の値を 3 から 5 の範囲でシミュレーションを実施した．n_l の値が 3 でも追跡可能性が低ければ追跡をあきらめるべきだということが分かる．また，シミュレーション結果があれば追跡者が考える n_l の値の推定によって追跡するかどうかの判断に役立つと考えられる．なお，L は次節で述べる現実的な追跡のための経路数であり，最大でも 1,000 程度であろうと考えた．スタンダードケースを基準として，ネガティブケースは海外端末が多いと想定される場合であり，ポジティブケースは協力端末が多く，海外端末も低いと想定される場合である．それぞれのパラメータの値を**表 2** に示す．

表 2　設定したパラメータ値
Table 2　The configured parameter values.

パラメータ	ネガティブケース	スタンダードケース	ポジティブケース
L	1〜1000	1〜1000	1〜1000
n_l	3〜5	3〜5	3〜5
b_{li}	0.2	0.2	0.2
b'_{li}	0.3	0.3	0.3
b''_{li}	0.5	0.5	0.5
T_{li}	0.2	0.1	0
T'_{li}	0.2	0.1	0
T''_{li}	0.6	0.8	1
C_{li}	0.5	0.5	**0.9**
a_{li}	0.9	**0.7**	**0.7**
f_{li}	0.1	0.1	0.1

図 7　評価シミュレータ計算画面
Fig. 7　Screen for input to evaluation simulator.

ここで，l 経路 i 段における段数 n_l，追跡協力確率 C_{li}，各場合におけるコンピュータ管理者比率 b_{li}，b'_{li}，b''_{li}，追跡成功確率 T_{li}，T'_{li}，T''_{li}，海外端末比率 a_{li}，海外協力係数 f_{li} は，他のパラメータで行ったシミュレーションの結果，経路数が十分な場合に差はあまりなく，大きな流れとして，それぞれすべて統一された値で計算を行うこととする．

5.3　確率の算出

上記のような計算を実施できるようにするため，評価シミュレータを開発した．画面デザインを XAML（Extensible Application Markup Language），計算機能を C#を用いて実装を行った．規模はおよそ 300 ステップである．この評価シミュレータに対し**図 7** のような入力画面を用いて，3 つのケースそれぞれにおけるハーダ PC 追跡可能確率を算出した．

続いて，3 つのケースそれぞれにおけるハーダ PC 追跡可能確率を算出し，経路数を軸として作成したグラフを**図 8**，**図 9**，**図 10** に示す．

まず，ネガティブケースについて考察を行う．条件が厳しいため，段数が 4（踏み台が 1 台）以降になると追跡は低確率で追跡は難しいが，段数 3（踏み台がない）場合は経路数を増やすことで追跡確率が線形的に増加することを示している．

続いて，スタンダードケースについて考察を行う．こちらは，ネガティブケースに比べて海外端末確率が少なくなっているため，段数が 4 の場合でも経路数を増やせば追跡の確率は上がっていくことを表している．また，段数が 3 のときであれば 200 経路ほどでも 80%弱の追跡が可能であると示している．さらに経路数を増やせば，600 経路ほどでその追跡確率

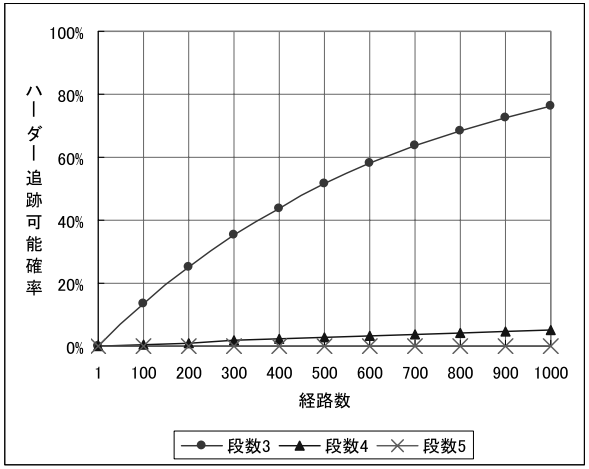

図 8　ネガティブケースの追跡可能確率
Fig. 8　The traceability probability in negative case.

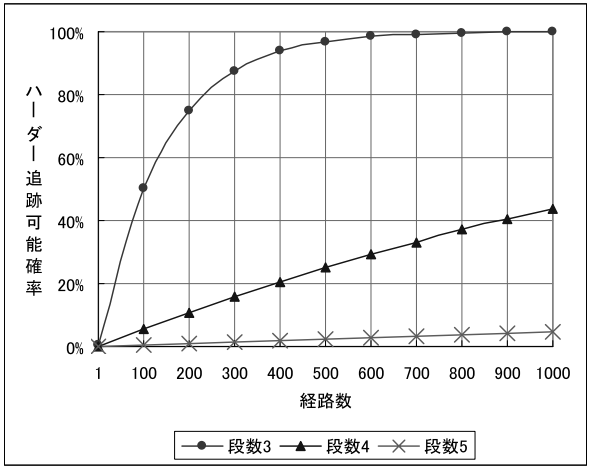

図 9　スタンダードケースの追跡可能確率
Fig. 9　The traceability probability in standard case.

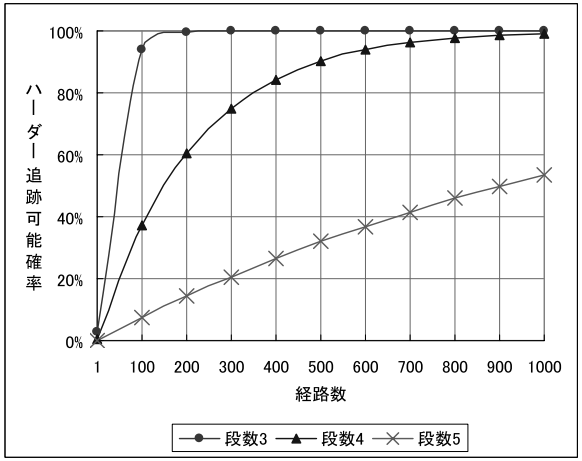

図 10　ポジティブケースの追跡可能確率
Fig. 10　The traceability probability in positive case.

はほぼ 100%に近くなる．

最後に，ポジディブケースについて考察する．スタンダードケースに比べて追跡協力確率が大幅に上がっているため，段数が 5（踏み台が 2 台）の場合であっても，経路数により追跡数が増加する結果となった．また，段数が 4 の場合も経路数により追跡確率は上昇していき，経路数を 200 にすると 60%超，400 にすると 80%超の確率を示している．さらに，段数が 3 の場合は，経路数 100 でも 94%と高確率を示しており，以降の経路数ではほぼ 100%に近い値となるため，現実的に追跡が可能であることを表している．

5.4　現実を考慮した考察

現実的に，ハーダ PC を追跡するにはどの程度の規模が必要かを考察する．ここでは大学，企業，インターネットサービスプロバイダ（以下 ISP）という大きく 3 つに分けて検討を行う．

まずは大学間における協力で追跡ができるか考察する．IP アドレスの 2%から 2.5%はボットネットに感染しているという調査[16] から，各大学それぞれ必ずボットネットを追跡する経路を 1 つは持つとする．また，大学は平成 21 年 4 月において 758 校あるとされている[17]．大学であることから，協力確率は高く見込むことができると考え，ポジディブケースに照らし合わせると，前述のとおり段数が 4 までであれば少ない経路数でも十分に追跡が可能であるといえる．

続いて，企業間における協力で追跡ができるか考察する．ここでも，大学と同様に各企業それぞれ必ず追跡経路を 1 つは持つと仮定する．平成 21 年 2 月において上場企業は 4925 社あるとされている[18]．また，企業では協力確率が大学より低いと仮定し，初めにネガティブケースで考察を進める．上場企業のうち約 10%の 500 社から追跡を行うと，段数 3 については 50%を超える確率が算出されたため，追跡を進める意義があるといえる．続いてスタンダードケースで検討を進める．同様に 500 社から追跡を行うと，段数 3 の場合は 100%近く追跡ができる．また，段数 4 の場合でも，経路数次第では追跡できる可能性は十分あるといえる．

最後に，ISP が協力した場合の考察を行う．2006 年には，ISP が保有する IP アドレス数は 4,800 万個存在するとされており[19]，そのうち約 2%の 100 万台がボットに感染しているとする．さらにこの中で，約 1%の 10,000 経路を使った場合でも，シミュレータではポジディブケースにおいて段数 5 でも追跡確率 96.5%を示す結果となった．

これらの結果から，追跡協力確率を大きくするか，経路数を多くすることで，現実的に追跡が可能となることが示された．協力を増やすことは現状では難しいとされているが，ネットワーク管理者であっても内容を見ることのできない特殊な端末 HiGATE[20] などにより，個人情報保護や通信に秘密に関する法律上の可否を乗り越えていくことができるならば，十分に追跡が可能であると考えている．

また，海外の端末からの攻撃に関しては，今後協力できる体制ができることが望ましいが，当面は国内に入ってくる入り口でフィルタリングを行うことで対応をとっていくべきであろう．今後協力できる体制ができるなどしていけば，より確実にハーダ PC を追跡できると考えられる．

さらに，シミュレータに追跡コストを考慮した計算を実装することで，より現実的な追跡を検討していくことができる．

6. おわりに

ボットは非常に多種多様で，同じ分類のボットでも亜種が数多く存在し，その挙動も様々である．また新しいボットほど複雑な機能を持つものが多い．そしてこれまで，ボットネットによる被害が増える一方で，根本的な対策はいまだ提案されてきていなかった．しかし，ハーダ PC を追跡することが可能であれば，その被害を大幅に減らすことができるという観点から，ハーダ PC を技術的に追跡可能かという検討および実験を行った．また追跡が可

能であるとするならば，現実的にどの程度追跡が成功するかという評価を，シミュレータを作成し検討した．

今後，より根拠あるパラメータ設定，コストを考慮に入れたシミュレータの開発など，実際に追跡を進めていくための問題解決を検討していく．

参 考 文 献

1) Symantec：インターネットセキュリティ脅威レポート VolumeVX，入手先⟨http://www.symantec.com/ja/jp/business/theme.jsp?themeid=threatreport⟩（参照 2011-02-01）．
2) The Honeynet Project: Know your Enemy, available from ⟨http://www.honeynet.org/papers/bots/⟩ (accessed 2011-02-01).
3) Abu Rajab, M., Zarfoss, J., Monrose, F. and Terzis, A.: A Multifaceted Approach to Understanding the Botnet Phenomenon, *Proc. Internet Measurement Conference 2006* (*IMC'06*), pp.41–52 (Oct. 2006).
4) Zhu, Z., Lu, G., Fu, Y.C., Roberts, Z.J and Han, P.K.: Botnet Research Survey, *Proc. Computer Software and Applications 2008* (*COMPSAC'08*), pp.967–972 (Aug. 2008).
5) Bailey, M., Cooke, E., Jahanian, F., Yunjing, X. and Karir, M.: A Survey of Botnet Technology and Defenses, *Proc. Cybersecurity Applications & Technology 2009* (*CATCH'09*), pp.299–304 (Mar. 2009).
6) Mazzariello, C.: IRC Traffic Analysis for Botnet Detection, *Information Assurance and Security, 2008* (*ISIAS'08*), pp.318–323 (Sep. 2008).
7) Masud, M.M., Al-khateeb, T., Khan, L., Thuraisingham, B. and Hamlen, K.W.: Flow-based identification of botnet traffic by mining multiple log files, *Distributed Framework and Applications 2008* (*DFmA'08*), pp.200–206 (Oct. 2008).
8) Yang, C.-H. and Ting, K.-L.: Detecting Botnets Using Command and Control Traffic, *5th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2009* (*IIH-MSP'09*), pp.856–860 (Sep. 2009).
9) コンピュータセキュリティ対策委員会：リアルタイムトレーシング手法に関する技術動向の調査研究，調査研究事業報告書 (2002).
10) 三原　元，佐々木良一：数量化理論と CCCDATAset2009 を利用したボットネットの C&C サーバ特定手法の提案と評価，マルウェア対策研究人材育成ワークショップ 2009（MWS2009），A6-1 (2009).
11) 中村暢宏，名雲孝昭，田中達哉，三原　元，佐々木良一：攻撃データ（CCC-DATAset2010）を利用したボットネットの C&C サーバ特定手法の再評価，マルウェア対策研究人材育成ワークショップ 2010（MWS2010），3F2-1 (2010).
12) 竹尾大輔，伊藤将志，鈴木秀和，岡崎直宣，渡邊　晃：コネクションベース方式による踏み台攻撃検出手法の提案，情報処理学会論文誌，Vol.48, No.2, pp.644–655 (2007).
13) SANS Institute: Bot C&C Servers on Port 80, available from ⟨http://isc.sans.org/diary.html?storyid=1865⟩ (accessed 2011-02-01).
14) 日立ソリューションズ：Palo Alto Networks PA シリーズ，入手先⟨http://www.hitachi-system.co.jp/paloalto/⟩（参照 2011-02-01）．
15) 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統計調査と方針検討，マルチメディア，分散，協調とモバイル 2010（DICOMO2010），pp.470–476 (2010).
16) 高橋正和，村上純一，須藤年章，平原伸昭，佐々木良一：フィールド調査によるボットネットの挙動解析，情報処理学会論文誌，Vol.47, No.8 (2006).
17) 文部科学省：公立大学について，入手先⟨http://www.mext.go.jp/a_menu/koutou/kouritsu/index.htm⟩（参照 2011-02-01）．
18) 株式会社上場サポート：日本の上場市場（上場会社数），入手先⟨http://www.iposupport.co.jp/ipo/01.html⟩（参照 2011-02-01）．
19) RBB TODAY：国内の IP アドレスのうち 3 割はソフトバンク BB が保有—サイバーエリアリサーチ調査，入手先⟨http://www.rbbtoday.com/article/2006/11/02/35520.html⟩（参照 2011-02-01）．
20) Sakurai, Y., Ashino, Y., Uehara, T., Yoshiura, H. and Sasaki, R.: HiGATE (High Grade Anti-Tamper Equipment) Prototype and Application to e-Discovery, *The 2010 ADFSL Conference on Digital Forensics, Security and Law* (*ADFSL 2010*) (July 2010).

(平成 23 年 2 月 9 日受付)
(平成 23 年 9 月 12 日採録)

名雲　孝昭

平成 21 年東京電機大学工学部情報メディア学科卒業．平成 23 年東京電機大学大学院未来科学研究科博士前期課程修了．同年日本電信電話株式会社入社．情報流通プラットフォーム研究所にてネットワークセキュリティ技術の研究開発に従事．

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．日本セキュリティ・マネジメント学会会長，内閣官房情報セキュリティセンター情報セキュリティ補佐官．