研究計画書

Extrusion Detectionによる ボットネット検出システムの研究

慶應義塾大学環境情報学部

自署:_____
学籍番号 70342926
サイバーインフォマティクスプログラム希望
平成 18 年 12 月 14 日

概要

ボットネットは DDoS 攻撃をはじめ，迷惑メールの送信など様々な活動の原因となる．しかし，ボットネットは，ボットが世界中に分散している点や活動方法を即座に変更できるという特性から，有効な対策が困難である．本研究は，管理サーバとの通信の連続性や同時多発性，想定されていない通信の発生といったボットネットの特性を活用することで，いままで困難であったボットの検出を試みる．さらに得られた結果をインターネット全体で共有し，効果的なボットの発見及び削減を目指す．本研究の成果により，インターネット全体におけるボットネットのノード数軽減が期待できる．

1 はじめに

インターネットの利用範囲は WWW や E-mail に留まらず，音声，動画の配信，インターネット家電などのより社会や生活に密着した方向へと広がっている．こうした状況の中，ボットネットはインターネットの可用性を脅かし，迷惑メールを不特定多数に送信するなどのさまざまな被害を生み出している．ボットネットとは攻撃者により不正に管理されているノードの集合であり，構成ノード数は多いものでは 100 万以上にのぼる．

ボットネットによる初めての大規模な事件は 2000 年 2 月に発生した *DistributedDenialofService* 攻撃 (以下 DDoS 攻撃) である．DDoS 攻撃とは複数のホストから大量のトラフィックを送りつけサービスを停止させる攻撃である．この攻撃により，Amazon.com や Yahoo!などの Web サイトが数時間停止するという被害が発生した．また，ボットネットは経済的利益を得る目的としても利用されている．2006 年 5 月には，攻撃者が大量のノードからクリック課金型の Web 広告を不正クリックするという詐欺行為を行っているとの報告がされた [1]．この詐欺行為も DDoS 攻撃の事件と同様にボットネットが用いられている．

ボットネットは多様な機能，高い拡張性を持ち，インターネット上の大きな脅威として，注目されている [2] [3] [4]．従来，ボットネットの活動を観測する手法として，ファイアウォールや侵入検知システムといった技術が用いられてきた．しかし，これらの技術ではボットネットを通じた攻撃を観測できても，ボットネットそのものには対応できない．さらに，現時点ではボットネットそのものに対する有効な対応策が存在しないため，ボットネットは今後も進化と拡大を遂げると考えられている．

本研究では，これらの背景を踏まえてボットネットの脅威を軽減するためのシステムを提案する．

2 ボットネット

本節ではボットネットの概要について述べ，その対策を検討するためにボットネットによって行われる攻撃・活動について整理する．

2.1 ボットネットの概要

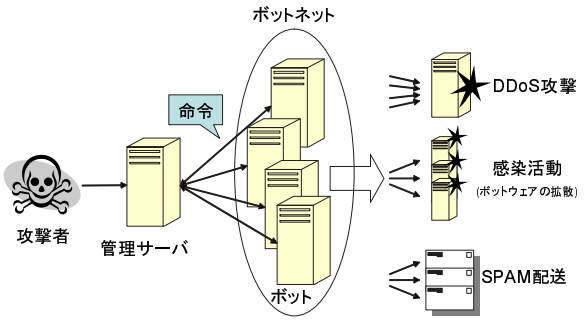

図 1: IRC 型ボットネットの構成要素

ボットネットとは，攻撃者によって管理されるノードの集合である．現在主流となっている，IRC[5] 型ボットネットの構成要素を図 1 に示す．ボットネットに加入したノードは**ボット**と呼ばれ，**攻撃者**からの命令により，ノードの所有者が意図しない通信や行動を行う．ボットネットの活動例を表 1 に示す．**ボットウェア**とは，ワームやウィルスなどの総称であるマルウェアの一種であり，特にボットネットのために作られたソフトウェアである．また，**管理サーバ**とは，攻撃者がボットの管理をする際に，命令をボットに伝達するための中継ノードである．図には管理サーバは 1 台しか存在しないが，管理サーバが冗長化されているボットネットや，管理サーバが存在せずボット間の P2P ネットワークを用いて命令を伝達しているボットネットもある．

表 1: ボットネットの活動例

活動名	活動内容と被害
DDoS 攻撃	TCP SYN フラッディング攻撃等によるサービス妨害やネットワーク輻輳
迷惑メールの中継・送信	迷惑メールの中継や送信による他のユーザへの迷惑行為
攻撃者の踏み台	SOCKS サービスなどの提供による攻撃者の活動幇助（証拠隠滅等）
ボットウェアの拡散	セキュリティホールを利用した他のノードへの攻撃によるボットネットの拡大
ノードの情報取得	ボットが感染したホストから情報を不正取得（キーロガー等）
Web 広告詐欺	Web へのアクセスを行い Web 投票や Web 広告のクリックをによる投票数操作や詐欺

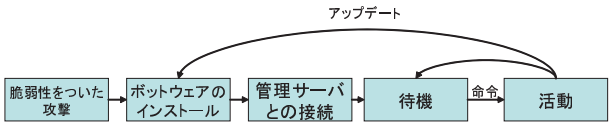

図 2: ボットのライフサイクル

2.2 ボットの活動

ボットの動作概要を図 2 に示す．まず，何らかの脆弱性を持つノードは，他のボット，あるいは攻撃者から脆弱性を利用してボットウェアが送り込まれる．ノードにボットウェアがインストールされると，そのノードはボットとなり，攻撃者からの命令を待機するために管理サーバと接続する．そして，ボットは管理サーバから命令を受け取るまで待機し続ける．攻撃者から管理サーバ経由で命令を受けると，表 1 で挙げた様々な活動を実行する．命令実行後は再び，管理サーバからの命令を待機する．基本的にボットはこれらの動作の繰り返しである．また，ボットはアップデート命令を受け取ると，新しいボットウェアを取得し，自分自身を更新する．これにより攻撃者は，ボットウェアの機能拡張や管理サーバの設定変更などができる．

3 ボットネットに関する対策とその問題点

本節ではボットネットに関する既存の対策として，ボットを加入させない，管理の停止を試みる，ボットを減らすという 3 つの手法に着目してそれぞれの概要と問題点を述べる．

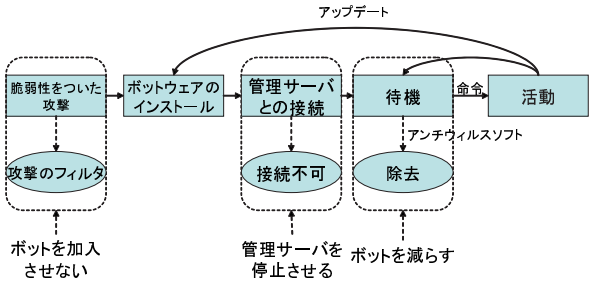

図 3: ボットの活動モデルと既存の手法の関係

3.1 ボットネットの規模を縮小する手法

ボットネットの規模を縮小する手法は，ボットを発見して，ボットウェアを駆除あるいはボットをネットワークから切り離し，ボットネットの規模の縮小を目指す．

ボットを発見するための主な手法の 1 つは，被害者側ネットワークに設置された侵入検知システム (IDS) である．たとえば，DDoS 攻撃であれば攻撃を受けているノード，迷惑メール中継であれば，メールを受け取ったユーザは，ボットに用いられている可能性のあるノードの IP アドレスを得られる．

ボットからの攻撃を検知したネットワークの管理者は，ボットのノードが管理されている ISP などの組織に連絡をするが，連絡に対して消極的な組織も存在する．その背景には，多くの組織が IP アドレスの割当を動的に行っている点や，連絡された情報の信憑性の確認にかかる調査コストや難しさある．そのため，連絡を行っても確実に有効な成果が出るとは限らず，効果には限界がある．

3.2 ボットの新規加入を防ぐ手法

ボットの新規加入を防ぐ手法は第 2 節で述べたようにボットネットがボットの集合によって構成されている点に着目し，ボットネットにボットを加入させないことで，ボットネットの規模拡大を防ぐ．既知の攻撃パターンを元に攻撃を防ぐ Intrusion Prevenstion System(IPS) や，パーソナルファイアウォールはこの手法に属する．

しかし，ワームやウィルスに対して関心が高まっている現在も，シグネチャデータベース更新が追いつかないため，それらの被害が絶えない点を考えると，効果的な手法ではない．

3.3 管理の停止を試みる手法

管理者はボットに命令出来なければ，ボットネットを用いた活動ができない．ボットネットを無効化する手法として，管理サーバを停止させる取り組みがある．現在，多くのボットネットが攻撃者とボットの通信方法として IRC を使用しているため，IRC サーバを停止できれば，ボットは命令を受け取れず，ボットネットの活動を停止できる．そこで，ボットネットの調査を行っている組織である Shadow Server[3] は，IRC サーバの所属している組織に連絡を行い，いくつものボットネットを停止させている．だが，こ

れは第 3.1 節の手法と同様に，連絡に消極的な組織の存在が問題となる．

さらに，ボットネットのなかにはボットが複数の管理サーバに接続する種類もあり，１つのコネクションが切れたらさらに別の管理サーバに接続するボットも存在する．また，ボットネットの観測結果 [4] によると，ボットネットの管理方法は IRC から P2P へと移行している事実が報告されており，今後，管理の停止がいまよりも困難になると予想されている．

これらの背景から，管理サーバの停止という手法は現在多く取られている手法であるが，管理サーバ対策を進めると同時に，管理サーバを用いないタイプのボットネットの対策も進める必要がある．

4　ボットネット対策システムの提案

第 3 節で述べた手法は，一定の成果を上げてはいるが，決定的な対策となっているとはいえない．本研究では，ボット及びボットと推測したノード情報の共有と，管理ネットワーク内に存在するボットを発見するシステムを提案し，世界中のボットに対する迅速な対応を目指す．

本節ではまず，既存の対策の問題点を整理し，改善すべき点を踏まえたうえでシステムを提案する．

4.1　現在の対応策に関する考察

第 3 節で述べた現在の対策を受けて，本研究では，大きく 2 つの点に注目する．

- 多くの対策が侵入検知を用いる点

  問題点

  ボットネット対策に関らず，既存のネットワークの脅威を防ぐ研究は，侵入検知に注目するものが一般的であった．侵入検知とは，特に外部から内部の攻撃に注目し，それに見合った検出方法や，トラフィック監視方法を取る手法をいう．例えば，DDoS 攻撃の被害者であれば侵入検知システムを用いて，攻撃元のノードを把握できる．しかし，侵入検知では Web の広告詐欺などの正常な通信に見せかけたボットネット活動の検出は困難である．

  さらに，第 3.1 節で述べたように，侵入検知によって得られるボットの情報は，世界中の組織に拡散しており対応が困難である．

  本研究での解決策

  本研究では，侵「入」検知ではなく**侵「出」検知 (Extrusion Detection)** の手法を用いる．侵入検知が被害者側サイトでの運用を想定しているのに対して，侵出検知はボットの存在する攻撃者側の管理ネットワークの境界での運用を想定する．侵出検知は，管理ネットワーク内のノードの通信をすべて監視できるため，ボットと管理サーバの通信や，平常時のトラフィック傾向との比較など，侵入検知とは異なった視点でのボットの検知が可能になる．

  さらに，侵出検知によって検知されるボットは，管理ネットワーク内に存在することとなり，発見したボットに対して即座に対応することも可能である．

- 組織間の連携不足

  問題点

  ボットネットを構成するノードは，国や組織に関係なく世界中に広がっている．これがボットや管理サーバを発見しても対応が困難である大きな理由である．ボットの数を減らす手法や管理サーバを停止させる手法において，ボット感染ノードが接続しているネットワークの管理者が適切な対応をしなければボットネットに対する効果はない．

  現在，日本では Telecom-ISAC[6] が，率先して組織間でのインシデント共有を行っている．このような取り組みは組織間に広がるボットネットに対して有効であるが，ボット情報の一般公開はなされておらず，また，加入している組織もボットネットの規模を考えると多くない．

  すなわち，ボットネットの対策には組織間の連携が必須であるが，現状では十分に連携できていない．

  本研究での解決策

  本研究では，侵出検知と**ボット情報の共有**により，組織間で連携が不足している問題に対応する．

  まず，侵出検知により，管理ネットワーク内に所属するボットを発見できる．さらに，インターネット全体で各ネットワークにおいて発見されたボット情報の共有を行い，侵出検知で発見されたボットの情報と，既存の侵入検知の手法で検知された攻撃元ノード情報により，より効果的なボットの検出が可能となる．

4.2　提案するシステムの概要

図 4 に第 4.1 節をふまえた上で，本研究が提案するシステムを示す．**ボットネットのための侵出検知システム**は管理ネットワーク内のボットらしきふるまいを監視するモジュールの集まりである**ふるまい監視モジュール郡**，ボットの情報を蓄積する**ボットリストデータベース**と，ふるまい監視モジュール郡からの情報を元に管理ネットワーク内のボットを発見する**統合スコア算出モジュール**で構成する．

本システムは，侵出検知を用いて，被害者側ではなく攻撃を行う側に注目し，侵入検知だけでは検知できなかった管理ネットワーク内のボットネットの活動検知を可能にする．各ネットワークがそれぞれの管理ネットワーク内におけるボットを発見するため，ボットを発見した後，容易に対応が可能である．

4.3　統合スコア算出モジュール

統合スコア算出モジュールはふるまい監視モジュール郡からの情報を元に管理ネットワーク内のボットらしきノードを発見する．また，発見したボットの情報をネットワー

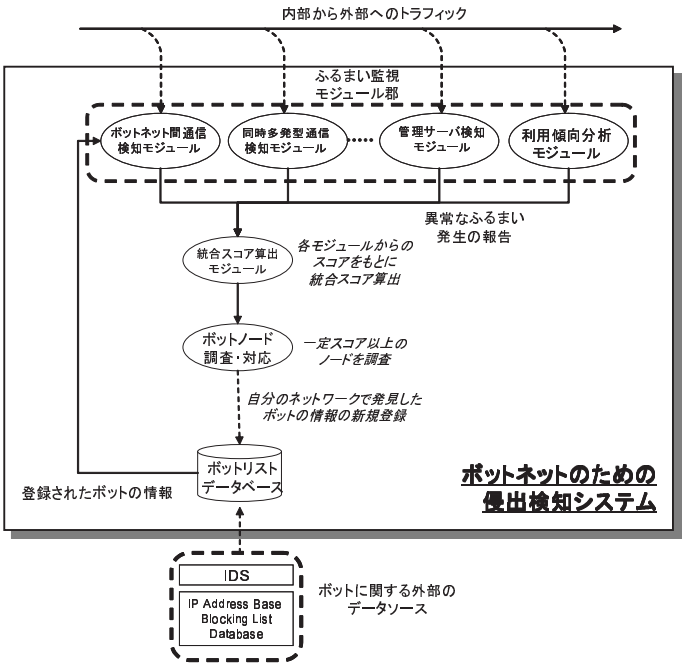

図 4: ボットネットのための侵出検知システム図

ク管理者に通達し，発見したノードがボットであるかの判断を求める．

ふるまい監視モジュール郡の各モジュールは，異常を検知すると，統合スコア算出モジュールに対して，ボットの疑いのあるノード情報を通知する．通知の際にふるまい監視モジュール郡の各モジュールは，各モジュールにとってどれだけ異常な行動を検知したかを通知する．ボットネット間通信検知モジュールを例に取ると，ノードに対して 1 度だけ外部のボットリストデータベースに登録されているノードから通信が送られてきたのであれば，ボットネットからの攻撃である可能性があり，ノードがボットである可能性は低いと推測できる．しかし，同様の通信が頻繁に行われ，更に通信が内部から外部に向けたものであると，ボットネットとの通信である可能性があり，ノードはボットである可能性が高いと推測できる．

ふるまい監視モジュール郡から得られた情報を活用するために，統合スコア算出モジュールはふるまい監視モジュール郡から受けとった報告ごとにスコアへ変換し，それらを統合する．具体的な算出方法や評価の基準については研究課題とするが，統合されたスコアを報告を受けたノードのボットらしさとして扱う．これにより，複数の要素を用いてより精度の高いボットの発見を目指す．報告により一定以上のスコアとなったノードは，管理ネットワーク内のボットと判断され，管理者への連絡が行われる．ノードがボットであるという判断が決まれば，管理者はボットリストデータベースへのノード情報の登録を行う．また，応用として判断結果をもとにノードの通信を遮断することも可能であると考える．

4.4 ふるまい監視モジュール郡

ふるまい監視モジュール郡は，ネットワーク内部のボットらしきふるまいをするノードの存在を発見するモジュールの集合である．これらのモジュールは管理ネットワークの境界に設置され，ボットを発見するための様々な要素で内部から外部へのトラフィックを監視する．この要素ごとにモジュールを分割し，それぞれのモジュールは異常を発見すると，統合スコア算出モジュールに報告する．本節では，このモジュール郡が監視する様々な要素のうち 4 つのモジュールについて述べる．

1. **ボットネット間通信検知モジュール**
   ボットネット間通信検知モジュールはネットワーク内部のノードと外部のボットの通信を監視する．ボットとの通信の検知には通信相手のノード情報とボットリストデータベースから得られた情報を比較する．管理ネットワーク内においてボットリストデータベースに登録されているノードと継続的かつ頻繁に通信するノードは，ボットの可能性があると検知する．

2. **管理サーバ検知モジュール**
   ボットネットの特徴である管理サーバとの接続に注目する．かつて，ICMP で通信するボットネットも存在したが，近年のボットウェアは IRC による管理が主流であり，通信プロトコルには TCP が用いられている．TCP には一連の通信の流れを表すセッションという概念があり，通常 Web や E-mail の送信においてセッションは数秒から数分で終了する．だが，P2P ソフトウェアや，チャットソフトウェアでは，管理用の通信のためにセッションを継続するケースが多い．そこで，管理サーバ検知モジュールは，予め定義されたアプリケーション以外で長時間にわたるセッションを張っているノードは，ボットネットの管理サーバと通信しているボットの可能性があると検知する．

3. **同時多発型通信検知モジュール**
   ネットワーク内のノードが通信する間隔やタイミングを監視する．ボットネットの活動のいくつかは攻撃者から命令を受けると即座に活動を開始する．ネットワーク内に同じボットネットに所属しているボットが複数台存在していると仮定すると，DDoS 攻撃の場合であれば，内部の複数ノードからあるノードに対してのアクセスが急増する．そして，ランダムな対象への拡散活動であれば，内部の複数ノードからある特徴を持つパケットが急増する．同時多発型通信検知モジュールはパケットを送るタイミングや通信内容の共通性に着目し，ボットの可能性のがあるノードを検知する．

4. **利用傾向分析モジュール**
   各ネットワークには，ネットワーク毎の利用傾向が存在する．例えば，企業において就業時間外の深夜に Web のアクセスが発生したり，メールの送信が行われることは考えにくい．しかし，ボットネットに感染したノードは，人間の操作によらない通信を行う．利用傾向分

析モジュールは通常の通信パターンをトラフィックプロファイルとして定義し，プロファイルにない通信をするノードはボットの可能性があると検知する．

4.5 ボットリストデータベース

ボットリストデータベースの目的は，ボットのノード情報をインターネット全体で共有し，ボットの検知に使用することで，より効果的なボットの検知を達成することである．そのため，本データベースは管理ネットワークごとに設置するのではなく，インターネット上に共有する 1 つのデータベースとして設置する．

本データベースの情報源は，本研究の侵出検知システムで発見されたボット情報と，外部からのボットの検知に利用できる情報である．侵出検知システムで発見されたボット情報とは第 4.3 節で述べたように，管理者によるボットと判断されたノード情報のことである．外部からのボットの検知に利用できる情報とは，インターネット上の IDS からのインシデント情報や，迷惑メール中継ノードの IP アドレスベースブロッキングリストが利用できる．IDS はボットウェアの拡散によく用いられるような攻撃や DDoS 攻撃を検知できる．それらの攻撃を送信したノードはボットであると推測し，IDS のインシデント情報をもとに本モジュールへのボット情報の追加を行う．また，ボットネットは迷惑メールの送信にも用いられるため，既存の迷惑メール送信者ブラックリストの利用も効果的と考えられる．これは，筆者による迷惑メール送信者ブラックリストと研究室ネットワークへの攻撃情報の比較予備実験からも推測されている．そこで，既存の迷惑メール送信者ブラックリストに登録されているノード情報も，ボットリストデータベースへの情報源として登録を行う．

5 期待される成果

本研究により，以下の成果が期待される．

- 侵出検知によるネットワーク内部のボット発見
- ボットリストを活用したボット発見精度の向上

これらの成果により，既存の研究では困難であった管理ネットワーク内のボット検出が可能になる．また，他のノードに対する攻撃情報をインターネット全体で共有し，ボットに加入したノードよる管理ネットワーク内からの攻撃を防止できる．

この成果を応用することで，あるボットネットのネットワークを迅速な把握が期待できる．また，インターネット全体におけるボットノード数の削減が期待できる．

6 今までの取り組み

6.1 研究会

学部 1 年次より徳田・村井・楠本・中村・高汐・湧川合同研究会に所属している．1 年次は，プログラミングの技術とネットワークについての知識を得るため，ネットワークの接続監視機器を製作し，組み込み機器の IPv6 化に取り組んだ．2 年次には組み込み機器への学習を続け，H8 マイコンを用いたコミュニケーション機器を作成し，また，BGP の情報を用いた帯域制御機構を製作した．3 年次より，セキュリティへの関心が高まり，ワームのシグネチャ自動生成機構を製作した．この研究成果を”IPS と連携した高速に伝播するワームのシグネチャ自動生成構の設計と実装” [研究成果 1] として第 13 回 DPS ワークショップで発表した．さらに，パケットスコアリングによるトラフィック制御機構に取り組んだ．

学外では国内最大規模のネットワークイベントである NetWorld+Interop Tokyo 2005 や，横浜市の小中学校へネットワークを敷設する活動であるネットディ等，ネットワークに関わるいくつかのボランティア活動を行った．

6.2 研究成果

研究成果として後述の論文を執筆した．

1. **金井 瑛**, 水谷 正慶, 白畑 真, 南 政樹, 村井 純. IPS と連携した高速に伝播するワームのシグネチャ自動生成構の設計と実装情報処理学会 第 *13* 回マルチメディア通信と分散処理ワークショップ論文集，November 2005.

7 政策・メディア研究科に進学を志望する理由

本研究はインターネット全体のセキュリティ向上を目指すものである．セキュリティへの要求を検討するには，様々な分野でのネットワーク利用場面や利用手段を考慮する必要があり，今後の動向を知る上でも他分野の研究が行われている環境が重要となる．また，研究を進める上で先進的に使われている実ネットワーク環境やコンピュータ資源を有する環境，それらを積極的に研究環境として用いることの体制，そして，インターネットを活用した分野の実践的経験を持つ研究指導者が必要である．以上の理由から私は政策・メディア研究科への進学を強く志望する．

参考文献

[1] Swa Frantzen. Clickbot, May 2006. http://isc.sans.org/diary.php?storyid=1334.

[2] The Honeynet Project & Reserarch Alliance, March 2005. http://www.honeynet.org/papers/bots/.

[3] Nicholas Albright. Researching Botnets, Febrary 2006. http://www.shadowserver.org/whitepapers/Botnets.pdf.

[4] Barford, Paul and Yegneswaran, Vinod. An Inside Look at Botnets. *To appear in Series: Advances in Information Security*, Springer 2006.

[5] J. Oikarinen, D. Reed. RFC 1459: Internet Relay Chat Protocol. May 1993.

[6] Telecom-ISAC Japan. *Telecom-ISAC Japan WWW*.