SCIS 2013 The 30th Symposium on Cryptography and Information Security
Kyoto, Japan, Jan. 22- 25, 2013
The Institute of Electronics, Information and Communication Engineers

C&C サーバ振る舞い情報抽出・分析システムの提案
Behavior Tracing System for Botnet C&C Servers

仲間 政信* 橋本 正樹* 辻 秀典* 田中 英彦*
Masanobu Nakama Masaki Hashimoto Hidenori Tsuji Hidehiko Tanaka

あらまし 近年，ボットネットはインターネットに対する重大な脅威となっているため，これに対抗する様々な技術が検討されている．この中で"Sinkholing"は，DNS やルーティングの仕組みを利用することで，ボットクライアントから C&C サーバへの通信を研究機関等が管理する環境へリダイレクトし，ボットクライアントを C&C サーバから遮断する技術であり，代替 C&C サーバを構築することができれば，ボットネット全体のサイズ測定や動作分析，情報収集，さらにはボットクライアントに対する停止命令送信が可能となる．代替 C&C サーバを構築するためには，C&C サーバの振る舞い情報が必要となるが，近年のボットネットでは，C&C サーバの IP アドレスが短期間で変更されるため，特定 IP アドレスをキーにセッションを監視することが困難となり，C&C サーバの IP アドレスを追跡し，その振る舞いを抽出するための作業コストが課題となっている．本研究では，既存研究にて提案されている C&C サーバコマンド抽出アルゴリズムを利用し，ボットクライアントが接続する C&C サーバの不特定多数の IP アドレスを特定・抽出し，抽出した IP アドレスを用いて C&C サーバの振る舞い情報を自動的に抽出するシステムの提案と，抽出データを分析する手法に関する検討を行う．

キーワード ボットネット，Sinkholing，C&C サーバ，振る舞い情報抽出

1 はじめに

近年，ボットネットはインターネットにおける重大な脅威として深刻な問題となっている．例えば，2007 年にエストニアで発生した集中的な DDoS 攻撃はボットネットによるものであり，攻撃対象となったエストニアでは，インターネットの利活用が進んでいることと関連し，大規模な被害をもたらした[1]．また，Shadow Server Foundation[2]によると 2012 年 5 月 7 日時点におけるボットネット感染端末台数は 50,000 台から 250,000 台，C&C サーバの観測台数は1500台から6000台と依然大規模となっており，ボットネットを遮断する等の対策を講じることが社会的に重要となっている．

本研究では，C&C サーバ振る舞い情報抽出の作業コストの課題を解決するために，既存研究にて提案されている C&C サーバコマンド抽出アルゴリズムを利用し，ボットクライアントが接続する C&C サーバの不特定多数の IP アドレスを特定し，さらに当該IPアドレスを用いてC&Cサーバの振る舞い情報を自動的に抽出するシステムの提案と，当該システムを利用し抽出したデータを分析する手法について検討を行う．

本稿の構成は，まず第 2 章でボットネットの概要と対策，現状の課題を紹介する．第 3 章で本研究に関わる関連研究を紹介し，第 4 章で本研究における提案システムの説明を行う．第 5 章では提案システムでの評価方法と，制限事項等の考察を述べ，第 6 章で本研究のまとめを述べる．

2 研究の背景

本章では，ボットネットの概要と，現状実施されている対策方法やその課題について触れ，本研究に関連するボットネット対策技術”Sinkholing”の有効性について述べる．

* 情報セキュリティ大学院大学，〒221-0835 神奈川県横浜市神奈川区鶴屋町 2-14-1, 2-14-1 Tsuruya-cho, Kanagawa-ku, Yokohama-city, Kanagawa 221-0835, JAPAN

2.1　ボットネットとは

ボットネットは,「ボット」と呼ばれるウイルスやワーム，トロイの木馬，rootkit などのマルウェアの機能が統合された「拡張されたマルウェア」から構成されたネットワークを指す．ボットの特徴は，端末に感染後，C&C サーバや他の感染マシンと通信を行うことであり，このネットワークが「ボットネット」である．ボットネットのネットワーク構成には，中央集権型（centralized）と分散型（de-centralized）に分けられる．中央集権型と分散型のボットネットを図１，図２に示す．

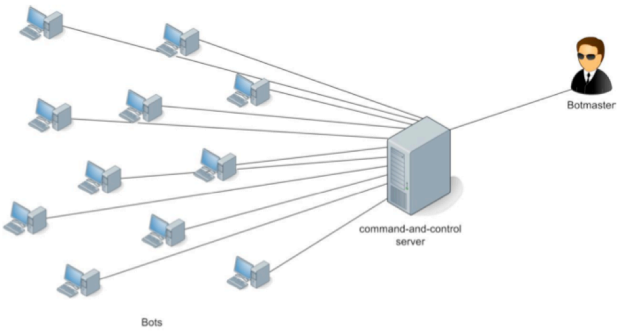

図 1　中央集権型ボットネット

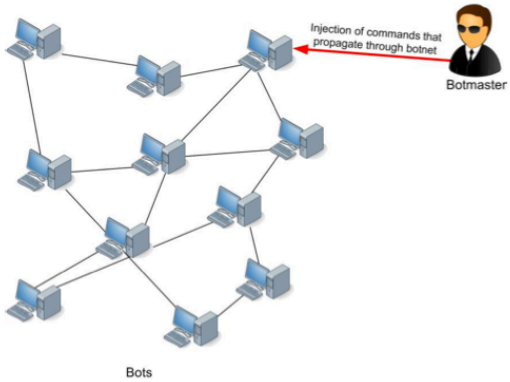

図 2　分散型ボットネット

2.2　ボットネット対策

European Network and Information Security Agency[3]は，ボットネットに対し次のような対策があるとしている．

- Blacklisting
- C&C サーバの直接遮断
- パケットフィルタリング
- Sinkholing

Blacklisting は，悪意のあるホストや，疑わしい動作をするサブネット等の情報をブラックリスト化し，リストに含まれるアドレスの通信を遮断する方式である．この方式は，LAN や端末のブラウザ上で利用することを想定したものであるが，ボットネットの柔軟性，例えば，C&C サーバの頻繁な変更等に対して，ブラックリストの更新が追随しきれない課題がある．

C&C サーバを直接遮断する方式は，IP アドレス等の情報から，実際に設置されているサーバを特定し，当該サーバを停止，またはネットワークから遮断させる方式である．この方式は，確実に C&C サーバを遮断するができるが，膨大な台数存在する C&C サーバを追跡する作業コストが課題である．

パケットフィルタリング方式は，Blacklisting でも利用される悪意のあるホスト，疑わしい動作をするサブネット等のブラックリスト情報と共に，ネットワーク上を流れるパケット，通信フローにおける特定のルール（シグネチャ）に一致する通信を，悪意がある通信と位置づけ，当該通信を遮断する方式である．ネットワークの経路上に設置することで容易に対策を講じることが可能であるが，Blacklisting 同様，シグネチャの管理／更新が課題で，誤検知を低減する工夫も必要となる．誤検知の種類には，悪意のある通信を遮断しないフォルス・ネガティブと，正常な通信を検知・遮断するフォルス・ポジティブの 2 種類があるが，いずれにせよ，悪意のある通信を遮断できない可能性や，正常な通信を検知・遮断してしまい，のちの誤検知への対応作業等が発生する課題を抱えている．

Sinkholing は DNS による名前解決やルーティングを意図的に変更し，悪意のあるドメインやホストへの接続を，管理されたネットワーク・ドメインへ強制的に接続させ，ボットクライアントを C&C サーバとの通信から遮断する方式である．Sinkholing を実現するためには，ボットクライアントが C&C サーバへ接続するためのアルゴリズムを事前に解析する必要がある．そのため，他の手法と比較しても実現は容易ではないが，Sinkholing を実現することができれば，ボットクライアントを確実にボットネットから切り離すことができる(図 3).

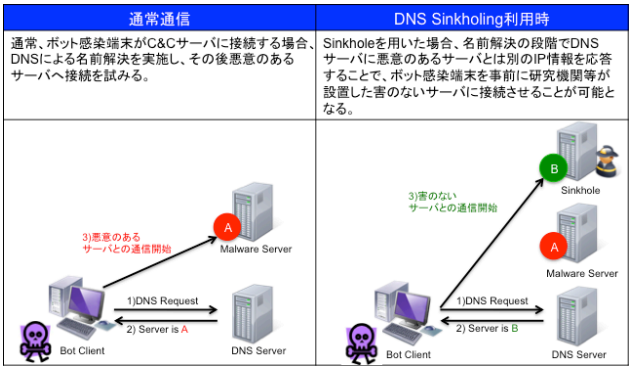

図 3　Sinkholing イメージ

実際のところ, 2007 年頃からボットネット遮断に対する動きが活発となってきているが，遮断のための手法に Sinkholing が多く利用されていることから，Sinkholing がボットネット遮断に有効な対策であることわかる（表 1）．

時期	ISP/ボットネット名	規模	手法	実施組織	備考
2008.11	McColo(ISP)		ISPの遮断		Srizbiに大きな打撃
2009.06	Pricewert(ISP)		ISP遮断	FTC(米連邦取引委員会)	Cutwailが一時的にダウン数時間で復活
2010.02	Waledac		ドメイン遮断	Microsoft	227ドメインを一時遮断（米バージニア州東地区連邦地方裁判所へ申請）
2010.10	Bredolab	3000万台	Sinkholing	オランダ国家犯罪局ハイテク犯罪チーム(THTC)	
2011.03	Rustock	100万台	Sinkholing	Microsoft	
2011.04	Coreflood	200万台	Sinkholing	米司法省(DOJ)連邦捜査局(FBI)	
2011.09	Kelihos	4万台	Sinkholing	Microsoft	

表 1 悪質 ISP/ボットネット遮断事例

Sinkholing はボットクライアントを C&C サーバから切り離すための技術だが, Sinkholing とあわせて C&C サーバと同様の振る舞いをする代替サーバを構築し，ボットクライアントを代替サーバに接続させることでボットネット全体のサイズ測定や動作分析，情報収集，さらにはボットに対する停止命令を送信することができる[4].

しかし，通常 C&C サーバのプログラムは流通しておらず，ソースやプログラム実行等による C&C サーバの振る舞い情報解析・入手は困難である．そのため，C&C サーバの振る舞い情報を抽出する手段として，ボットクライアントと C&C サーバとの通信を監視する方法が考えられるが，ボットネットによっては C&C サーバとして動作するホストを多数用意しており，短時間で接続する C&C サーバを変更するため[5]，振る舞い情報を抽出するためには，C&C サーバの IP アドレスの特定，当該 IP アドレスをキーにしたフローの抽出，さらにその抽出データ分析作業等，膨大な作業が発生するため，作業コストが現状の課題となっている．

3　関連研究紹介

本章では，提案システムで利用する関連研究の技術の紹介と，提案システムに関わる先行研究について述べる．

3.1　Sinkholing を利用したボットネット観測研究

Sinkholing の技術を利用した研究例として，Brett Stone-Gross ら[4]の研究がある．この研究では，実際に存在するボットネット「TorpigBot」の C&C サーバ接続時のメカニズムを解析し，インターネット上に存在するボットクライアントを研究機関が管理するホストにアクセスさせ，そのボットクライアントからのアクセスを 10 日間観測している．

TorpigBot のボットクライアントは C&C サーバに接続する際，ドメイン作成アルゴリズム（DGA：Domain Generation Algorithm）を利用する．DGA とは，ボットネットから独立してボットクライアント内部にて C&C サーバのドメイン名リストを作成するアルゴリズムである．ボットクライアントは名前解決が可能で，かつ，正しい C&C サーバの振る舞いをするサーバと接続されるまで，DGA で作成したドメイン名リストを順番にアクセスする．接続が成功すると，ボットクライアントは次のドメイン名リスト作成の契機まで，当該サーバを C&C サーバとして継続して接続する．

TorpigBot の DGA の仕組みの詳細として，TorpigBot はドメイン作成時における日付(年月日)と任意の数値情報をベースに計算される．ボットクライアントは，まず始めに週の情報を利用した dw と呼ばれるドメイン名を作成する．dw は，作成時点における年・週の情報を元に作成される(日データは利用されない)．その後，ボットクライアントは，dw.com, dw.net, dw.biz といった TLD を付加したドメイン名を作成し，一通り dw ドメインに接続を試みて，接続が成功しなかった場合，次にドメイン作成時点における日情報を元に dd と呼ばれるドメインが作成される．ボットクライアントは，dw 作成時同様，dd.com, dd.net, dd.biz に接続を試みる．dd ドメインでの接続が成功しなかった場合, ボットクライアントは最終的に内部設定ファイルにハードコーディングされたドメイン名リストに対してアクセスを試みる．DGA 作成イメージと代替サーバ構成を図 4 に示す．

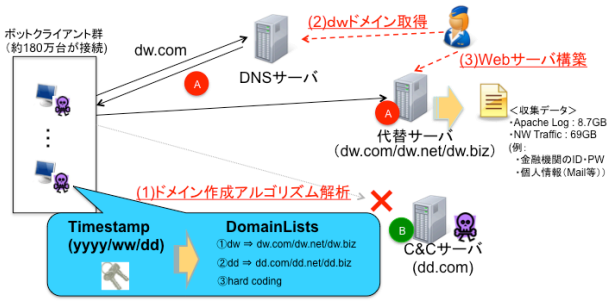

図 4　DGA イメージと代替サーバ構成

研究事例では，週情報から作成されるドメイン名（dw.com,dw.net）を取得・事前登録し，apache がセッティングされた Web Server を設置した．当該サーバでは，ボットからの接続要求を受信し，ログを取得するとともに，すべてのネットワークトラフィックを記録した．

当該サーバを 10 日間稼働させた結果，サーバに対し約 18 万台の端末が接続された．さらに，8.7GB 以上の Apache ログファイルと，69GB のネットワークトラフィックを収集することができ，当該データには，金融機関等の ID/パスワードや，その他詳細な個人情報も含まれていた．

3.2　ボットネットのコマンド抽出

ボットネットにおいて，ボットクライアントと C&C サーバとのネットワークトラフィックデータからボットネットの命令コマンドを抽出する研究として，Thorsten Holz ら[6]の研究がある．本研究では，ボットクライアントのネットワークトラフィックを観察し，C&C サーバからのコマンドと，それに応じたボットクライアントのレスポンス動作を抽出し，ボットクライアントの感染検知モデルを自動生成する手法を提案している．本研究におけるメリットは，ボットクライアントの実際の振る舞いから検知モデルを自動生成するため，検体に依存せず，様々なボットファミリーに対し少ない誤検知(false positive)で検知モデルを作成できることである．また，振る舞いから検知モデルを自動抽出するため，進化がめまぐるしいボットネットの世界で，新たに発生するボットネットに対し，素早い対応が可能であることもメリットの 1 つである．

本研究における成果は，416 個のボット検体を実際に動作させ，取得した通信データから 70 種類の検知モデルを作成している．さらに，当該検知モデルを検証用ネットワークトレーニングセット（うち，25%はボットネット通信）に対して適用し，88%の感染を検知できた．

本研究にてボット感染検知のために利用される C&C サーバからのコマンド情報，及び，コマンドに応じたレスポンス動作を抽出するプロセスを以下に記述する．

1. ボットクライアントのネットワークトラフィック取得
2. トラフィックプロファイルの作成
3. 変化点の抽出・プロット
4. Snippet の抽出
5. 階層型クラスタリングによる Snippet 分類
6. 最長共通部分列抽出アルゴリズムによるトークンシーケンスの抽出

はじめに，ボットクライアント上で C&C サーバとの通信や，それに応じたレスポンス動作等を含めたすべての通信データを取得する．その後，プロセス 1 で取得したネットワークトラフィックを分析し，単位時間毎のネットワークの振る舞い情報（トラフィックプロファイル）を算出する． トラフィックプロファイルとして算出する項目は，以下の 8 項目である．

① 総パケット数
② 総バイト数
③ UDP パケット数
④ HTTP パケット数
⑤ SMTP パケット数
⑥ 接続しに行った IP アドレス数
⑦ 接続しに行ったポート数
⑧ ペイロード中の非 ASCII バイト数

プロセス 2 で抽出したトラフィックプロファイルを，次に Change Point Detection(以下，CPD)アルゴリズムを利用し状態の変化を分析し，C&C サーバからのコマンドへのレスポンス動作が発生したと考えられるタイムインターバルを検出する．なお，本研究では実績値として 50 秒のタイムインターバルが有効であるとしている．

プロセス 3 で抽出した変化点を元に，C&C サーバからのコマンド送信，及び，そのコマンドへのレスポンス動作が含まれたと想定されるトラフィック情報の固まり（Snippet）を抽出する．Snippet の時間間隔は，レスポンス遅延を考慮し前タイムインターバルの 30 秒，タイムインターバル付近の検知を考慮し後タイムインターバル 10 秒の計 90 秒間を対象とする．Snippet の時間間隔の概要を図 5 に示す．

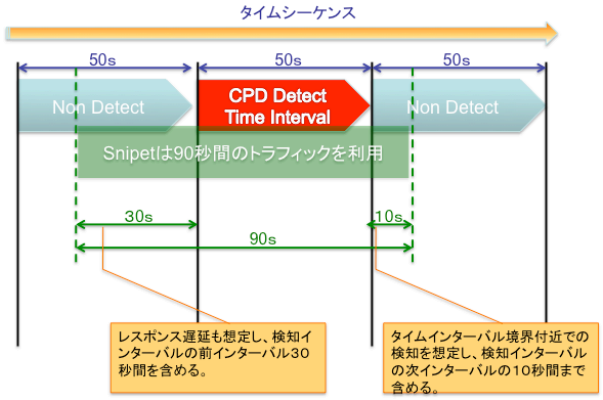

図 5　Snippet タイムインターバルの考え方

プロセス 4 にて Snippet を抽出後は，コマンドの種類によってレスポンス動作が変化することを想定し，プロセス 5 で Snippet のトラフィックプロファイル情報を元に Snippet をクラスタリングし，同様のコマンドが含まれていると想定される Snippet をグループにまとめる．その後，最終的にプロセス 6 にて同じコマンドが含まれていると想定される Snippet のグループから，最長共通部分列抽出アルゴリズムを利用して，C&C サーバからのコマンドであると想定される文字列の抽出を行う．

3.3　先行研究

ボットネットの C&C サーバ振る舞い情報を抽出する提案に関する先行研究を紹介する．

Meng ら[7]は，C&C Tracer というボットネットの振る舞い追跡システムの提案を行っている．C&C Tracer は，C&C サーバの特徴を抽出する CAFÉ(C&C active behavior feature extracting)，ドメインの自動名前解決を実施する DNSQ(domain name status querying)，C&C サーバの状態を分析する CSTA(C&C status tracing analyzer)の 3 つのコンポーネントから構成される．C&C Tracer は URL を動的に拡張し，C&C を追跡していくが，DNS からボットを検知するため，DNS を利用しないボットへの対応が難しい．

Lorenzo ら[8]は，ボットクライアントと C&C サーバ間の通信パターンからボット感染端末を検知する手法を提案している．本研究は，ボットクライアントと C&C サーバ間の通信を分析することで感染端末を検知することが目的であるため，C&C サーバの振る舞い情報抽出までは実現できていない．

4　提案システム

本章では，本研究における提案システムの位置づけと全体概要について述べ，提案システムの有効性について説明する．

4.1　提案システムの位置づけ

本研究では，既存研究である C&C サーバからのコマンド抽出アルゴリズムを利用し，抽出したコマンドから，C&C サーバの IP アドレスを特定し，当該 IP アドレスをキーとして，ボットクライアントと C&C サーバの振る舞い情報を抽出するシステムを提案する．

本研究の位置づけは，Sinkholing の技術と C&C サーバの代替サーバを利用し，ボットネットの解析を実施する際，代替サーバ構築のために必要となる C&C サーバの振る舞い情報の抽出を自動化させ，解析環境の構築を効率化させることである．先の研究から，DGA を利用したボットネットの場合，代替サーバを C&C サーバとして接続させるためには，ボットクライアントから接続に対し，C&C サーバとしての振る舞いを応答する必要がある．さらに，先の事例においては，HTTP の Post メソッドで接続する仕組みとなっていたため，サーバを待ち受け状態にしておくことで自動的に情報を収集することができたが，他のプロトコルが利用された場合等においては，対応することができないという課題がある．よって，振る舞い情報を効率的に抽出することで，代替サーバ構築の効率化に寄与することができると考える．また，本提案システムは，実際に発生したネットワークトラフィックから振る舞い情報の抽出をシステム化・自動化することから，進化の早いボットネットの世界において，既存ボットネットのみならず新たに発生した新種のボットネットに対しても，素早く対応することができる．

4.2　提案システム全体概要

提案システムにおいて，C&C サーバの振る舞い情報を抽出するためのプロセスを図 6 に示す．

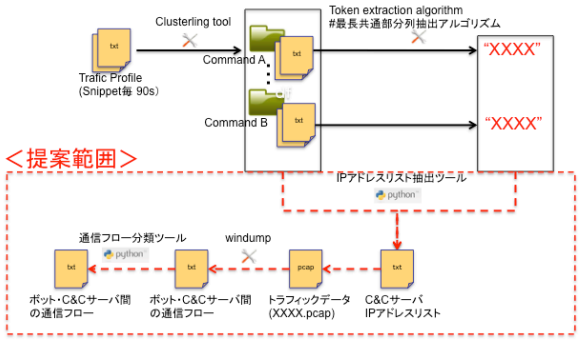

図 6　提案システムフロー

提案システムにおける実行プロセスと，それぞれのプロセスにおける実行内容は次の通りである．

1.　先の関連研究にて紹介した Thorsten Holz

ら[6]の研究において，抽出されたコマンドと Snippet 情報から，C&C サーバと想定される IP アドレスリストを抽出する．

2. プロセス 1 で抽出した IP アドレスリストをキーとし，再度トラフィックデータを精査し，ボットクライアントと C&C サーバが通信を行ったと想定される通信フローの抽出を行う．

3. 抽出した通信フローには，不特定多数の C&C サーバからの通信が含まれていると想定され，また，通信のフローの内容は重複したものが含まれると考えられるため，同様の通信パターンを整理し，最終的に C&C サーバの振る舞いパターンの種類を抽出する(図 7)．

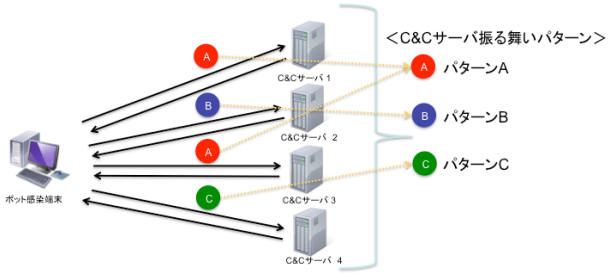

図 7　C&C サーバ振る舞いパターン抽出イメージ

4.3　提案システム実装イメージ

提案システムの構築を効率的に実施するため，構築方針は既存ツールを可能な限り流用するようにし，構築要件に対する要求を満たすものがない場合は，自ら作成する．なお，今回構築に使用する言語は，提供モジュールが多く，様々なプラットフォームで動作可能である Python を利用する．

提案システムを実装するにあたり，次の機能が必要となる．

機能1　pcap データテキスト変換
機能2　ネットワークプロファイル計算
機能3　ネットワークプロファイルの標準化
機能4　CPD の検出
機能5　snippet pcap/txt ファイル抽出
機能6　snippet ファイルクラスター分析
機能7　snippet パケットペイロード抽出
機能8　パケットペロードクラスター分析
機能9　最長共通部分列(LCS)抽出
機能10　C&C IP アドレス抽出
機能11　C&C ネットワークフロー抽出

提案システムにおける処理イメージとして，まず，事前のボットクライアントが導入された端末上で，C&C サーバとボットクライアントとの通信のネットワークトラフィックデータ(ファイル形式は pcap を想定)を取得する．その後，機能 1 にて当該 pcap ファイルを分析可能なテキスト形式のファイルに変換する(図 8)．

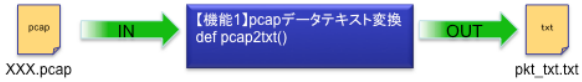

図 8　機能 1 入出力イメージ

ネットワークトラフィックデータをテキストデータへ変換後，機能 2 にてネットワークプロファイルの計算処理を実施する(図 9)．ネットワークプロファイルは，先行研究から 50 秒間のタイムインターバル毎に算出する．また，プロファイルの項目は先に挙げた 8 項目の計算を実施する(①総パケット数，②総バイト数，③UDP パケット数，④HTTP パケット数，⑤SMTP パケット数，⑥接続しに行った IP アドレス数，⑦接続しに行ったポート数，⑧ペイロード中の非 ASCII バイト数)．

図 9　機能 2 入出力イメージ

ネットワークプロファル計算処理完了後，機能 3 でプロファイルデータの標準化処理を行う(図 10)．ここでの標準化は，すべてのネットワークプロファイル中の最大値から比較した場合の比率となる．よって，算出したネットワークプロファイルデータから，各プロファイル項目の最大値を利用し，各タイムインターバルを標準化する処理を行う．

図 10 機能 3 入出力イメージ

機能 4 では，標準化されたネットワークプロファイルから CPD アルゴリズムを利用し，変化点の抽出を行う．変化点の判断方法は図 11 の通り，任意タイムインターバルから，前後 5 タイムインターバルの平均値を算出後，前後の距離を求め，先行研究にて算出済みの実績値で比較し，変化点の判断を実施する．最終的に変化点の判定された場合，当該タイムインターバルの通信時刻をアウトプットとして

出力する．(図 12)

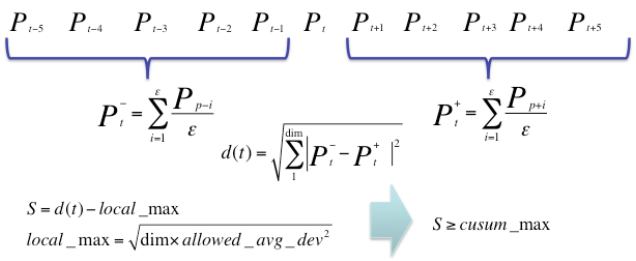

図 11　CDP アルゴリズム実施イメージ

図 12 機能 4 入出力イメージ

機能 5 では，CDP で抽出したタイムインターバルの時刻から Snippet の通信ファイルを抽出し，当該ファイルをテキスト形式に変換する(図 13).

図 13 機能 5 入出力イメージ

機能 6 では，抽出した Snippet のテキストファイルから，ネットワークプロファイルを再計算し，階層型クラスタリングの手法を利用して Snippet をグループ化する(図 14).

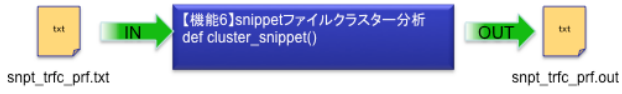

図 14　機能 6 入出力イメージ

機能 7 では，次プロセスでペイロードのクラスタ処理を実施するため，Snippet のテキストファイルからペイロードを抽出する(図 15).

図 15　機能 7 入出力イメージ

機能 8 では，機能 9 で最長共通部分列抽出のため，Snippet 中すべてのペイロードでの計算処理を省力化するため，ペイロード毎に再度クラスタリング処理を行う(図 16)．ここでのクラスタリングも階層型クラスタリングを利用する．

図 16　機能 8 入出力イメージ

機能 9 では，クラスタリングされたペイロード毎に最長共通部分列抽出アルゴリズムを適用し，各ペイロードクラスタの最長共通部分列を抽出する(図 17).

図 17　機能 9 入出力イメージ

機能 10 では，機能 9 で抽出した最長共通部分列を用いて，すべてのネットワークトラフィックから検索をかけ，当該文字列が存在する通信の IP アドレスを抽出する（図 18）.

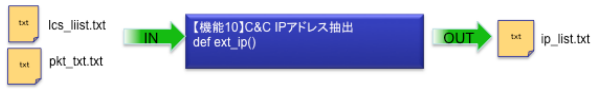

図 18　機能 10 入出力イメージ

機能 11 では，機能 10 で抽出した IP アドレスをキーとして，すべてのネットワークトラフィックから検索をかけ，当該 IP の通信のみを抽出する(図 19).

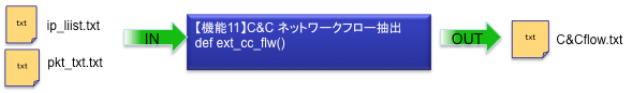

図 19　機能 11 入出力イメージ

5　評価

本章では評価方法と提案システムの制限事項について述べる．提案システムの有効性の確認方法は実際のボット感染端末のネットワークフローを利用した分析を実施し評価することを想定している．

5.1　実験環境

実験環境として，WindowsXP 端末を用意し，当該端末上に VMWarePlayer で動作するボット感染用端末を用意・管理された外部に攻撃パケットが流れない安全なネットワーク上に配置し，当該端末を Offensive Computing[9]よりダウンロードしたボ

ットクライアントに感染させ，特定期間動作させた後，ネットワークパケットを取得し，提案システムで分析を実施する．実験環境構成イメージは図 20 のとおりである．

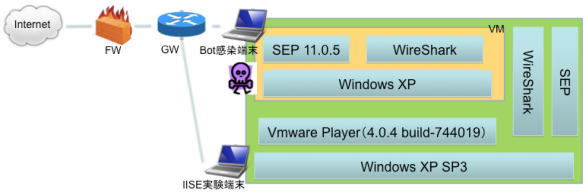

図 20　実験環境イメージ

5.2　評価方法

提案システムの位置づけは，ボットネットの C&C サーバ振る舞い情報の抽出を自動的に行うことで，人手の実施で課題となっていた作業コストを効率化させることである．よって，本提案システムの評価方法は，実際に手動で C&C サーバの追跡を，人手で実施した場合と，提案システムを利用した場合の作業コストと分析結果精度を比較する．

5.3　制限事項

提案システムでは，ネットワークトラフィックの状態変化により，C&C サーバから攻撃命令等のコマンド受信とそのレスポンス動作を，通常のネットワーク状態から乖離したか否かで検出している．そのため，ボットネットに起因しないネットワークトラフィックの異常が発生した場合，誤検知されてしまう可能性がある．

提案システムでは，C&C サーバからのコマンドを，同様のネットワークパケットをクラスタリングし，最長共通部分列（LongestCommonSubsequence）で抽出している．そのため，C&C サーバとボット端末間で暗号化通信が利用されている場合，想定されるコマンドを抽出できない可能性がある．

6　おわりに

ボットネットはインターネットに対する重大な脅威となっているため，対抗する様々な技術研究が重要な位置づけとなっている．本研究では，C&C サーバの振る舞い情報抽出にかかる作業コストの課題を解決するために，既存研究にて提案されている C&C サーバコマンド抽出アルゴリズムを利用して C&C サーバの IP アドレスを特定・抽出し，C&C サーバの振る舞い情報を自動的に抽出するシステムの提案を行っている．

今後は，HTTP や IRC 等の複数種類のボットクライアントでの検証を実施し、システムの精度を高めていく．

参考文献

[1] IPA,”サービス妨害攻撃の対策等調査”,2010 年 12 月

[2] ShadowServer Foundation. [Online], http://www.shadowserver.org/wiki/

[3] European Network and Information Security Agency,”Botnets : Detection, Measurement, Disinfection & Defenc”,2011

[4] Brett Stone-Gross,”Analysis of a Botnet Takeover”,The IEEE Computer and Reliability Societies P64-72,Jan.2011

[5] Thorsten Holz,”Measuring and Detecting Fast-Flux Serice Networks”,2008

[6]Peter Wurzinger,”Automatically Generating Medels for Botnet Detection”,ESORICS 2009 conference

[7]Meng-Han Tsai,2011, “C&C tracer: Botnet command and control behavior tracing’,IEEE

[8]Lorenzo,”Mining the Network Behavior of Bots” , 2009

[9]Offensive Computing. [Online] http://www.offensivecomputing.net/