平成25年度　卒 業 論 文

邦文題目

ボットによる遠隔操作の解析

英文題目

Analysis of remote-controlled bot

情報工学科　渡邊研究室

(学籍番号: 090430070)

朴明模

提出日: 平成 25 年 2 月 13 日

名城大学理工学部

内容要旨

ボットはハーダーにより遠隔操作され、spam メール、DDoS 攻撃、情報の流出などの悪意ある行為を行うウイルスである。ボットはほかのウイルスと違って、金銭的な利益を目的にする場合が多い。ボットに感染された人は感染されたかどうか分からない。ボットを分析するためにハニーポットと wireshark を利用してパケットを一つ一つ確認しながらボットの動きや特徴を分析した。そして自分がハーダーになって自分の PC にウイルスを埋め込んで、遠隔操作を行った。遠隔操作に使われたプログラムは prorat である。prorat は遠隔操作はもちろん DDos 攻撃や keylog 攻撃などの攻撃ができるプログラムである。prorat を利用して遠隔操作を行って、結果を解析した。

目 次

第1章　はじめに

最近インターネットが多くの家庭に普及して多くの人々が使用している。インターネットによって、多くの情報を得ることが可能になった。しかし一方では、多く誤差が発生している。代表的なのがウイルスである。ウイルスは 1985 年パーソナルコンピュータウイルスから始めてこれまで多くのウイルスが生じてきている。ボットもそのウイルスのひとつである。ボットネットは、1993 年 eggdrop に初めて出た。以来、最近 20 年間 frobot、texbox、machbot、phip bot など進化したボットが出現し、最近ではあまりにも多くの亜種のボットが出現であり、対応を非常に難しくしている。毎日 5000 種の新規悪性コードが出現している。全世界的に、C & C サーバー（Command & Control：ボットゾンビたちに命令を下し、制御するためのサーバ）と、悪意のあるボットは広範囲に分布しており、特定の地域に密集される様相を見せている。超高速インターネットが設備の整った環境では、従来に比べて 1/10 の PC だけ利用しても、より強力な DDoS などの攻撃が可能になるので、高速インターネットが整っている地域は、ボットネット感染地として好まれている。世界的にボットに感染してゾンビ PC に変わる PC の数が増加しており、ボットネットの規模も大きくなっている。ボットネットによる攻撃がさらに深刻化する理由は、犯罪化の様相を帯びているからである。 2007 年に発生したアイテム取引先サービスの障害発生と現金の要求脅迫事故のように、サービスの障害発生を口実にサービスプロバイダーを脅迫して金品を奪うか、個人の金融情報を収集およびスパム送信を介して対価を受け取る事故が頻繁に発生している。このようにボットにより大きな問題が生じている。今回の研究では、ハニーボットとワイヤシャークを利用してボットの特徴とボットの動きを分析した。自分が直接ハーダーになって、自分の pc を prorat を使用して、ボットに感染させ、遠隔操作をしてみた。telnet と prorat を比較した結果、遠隔操作までの接続は全く同じであった。

第2章　ボットとボットネット

2.1　ボットとボットネットの定義

ボットとはコンピューターに害をもたらすプログラムの中でも、感染したパソコンを遠隔から操ることを主な目的としたものである。ボットネットとはボットに感染したコンピュータで構成されるネットワークのことである。

2.2　ボットとボットネットの感染・被害

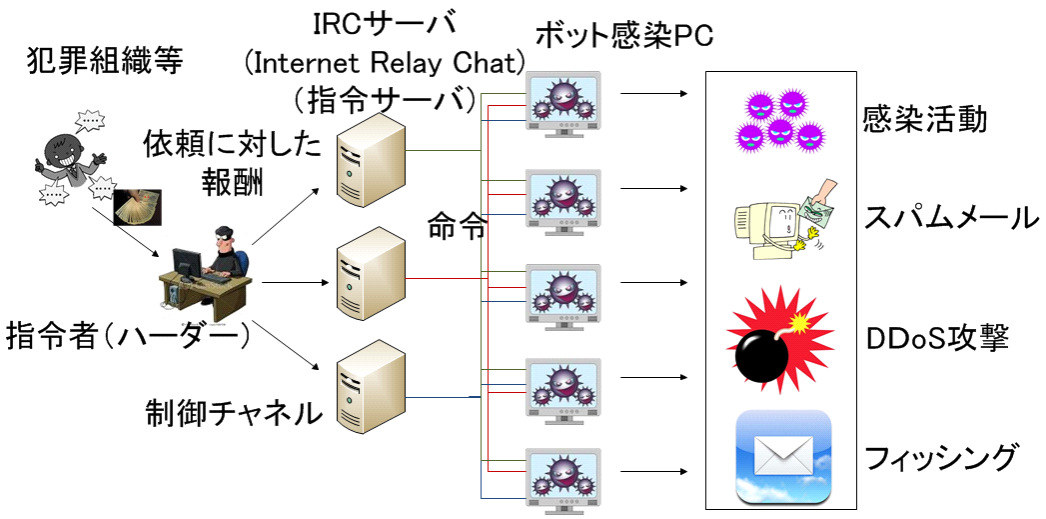

図 2.1　ボットの概要

ハーダーはボット感染 PC へ指令を中継する時に同報性のある IRC プロトコルを用いることが多い。ボットに感染した全てのパソコンはハーダーにより、1 回の指令で IRC サーバを介して同時に操られてしまう。IRC サーバが仮に、潰されても控えの IRC サーバに即座に切り替えられる。ボットは、指令者からの命令に従いあらゆる悪意ある活動を行う。ボットに感染したユーザがハーダーの手先となってしまい、意識せず犯罪に加担することがある。被害は他の PC の対して感染活動を行う。そしてスパムメールを送る。スパムメールの中にはウイルスが埋め込まれる場合がある。ウイルスが埋め込まれたメールは開いただけでウイルスに感染される場合がある。そして DDoS 攻撃をやフィッシング（詐欺）などがある。

第3章　ハニーポットによる感染調査

3.1　ボットの情報収集のためたてたハニーポット

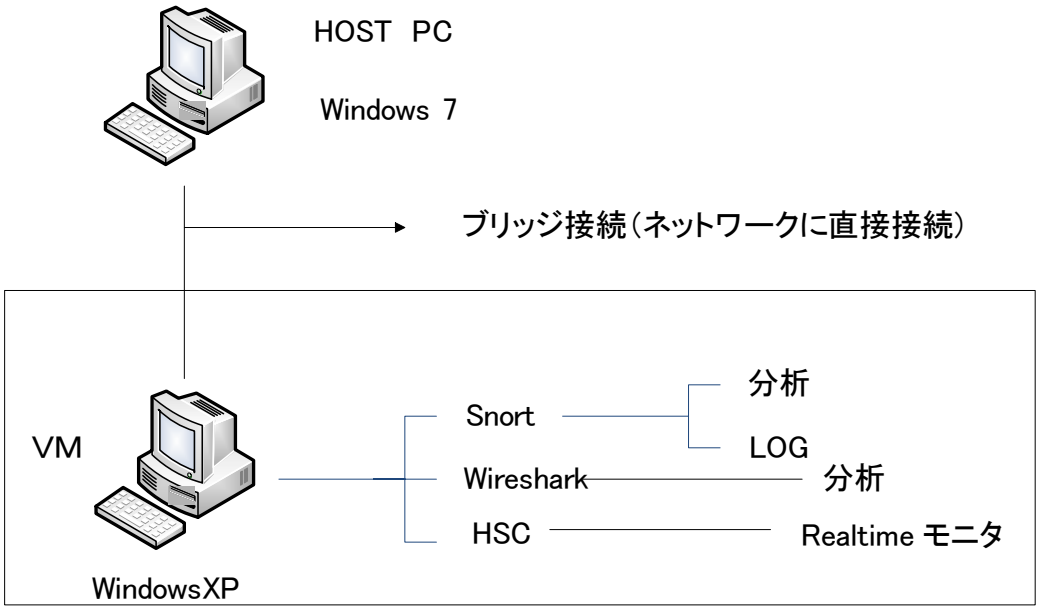

図 3.1　ハニーポットの構成

図 2.2 に示すように VM をたててその中にハニーポットをたてた。VM の中にハニーポットをたてた理由は VM の中にたてるとウイルスに感染され、OS が使えなくなっても簡単に回復できるからである。実際に何回もウイルスに感染されて OS が使えなくなった。そのたびに OS をインストールした。この方が簡単で便利だったので VM の中にハニーポットをたてた。流れを説明する前に firewall を無効にし、ウイルス対策プログラムも off にしておいた。そして port 番号もボットに感染されやすい番号 80,1234,12345 などを空けておいた。この理由はボットに感染されやすくするためでる。研究室でグローバルアドレス上ウイルスソフトの入ってないハニーポット PC を 2 台置いた。1 台は windowsXP service pack3,2 台目は windowsXP service pack2 である。windowsXP を利用してボットに感染するまで放置しておいた。感染されたら wireshark で分析を行おうとした。ハニーポットの動作としてインターネットを通る全てのパケットは snort によって分析され、log されるようにした。さらに hsc(honeynet security consoles) を利用してパケットの動きを realtime で見えるようにした。

しかし、設定のまちがいで snort で分析ができなくなって分析は全部 wireshark で行った。

3.2　ハニーポットと wireshark

ハニーポットを利用して収集した情報である。

表 3.1　ハニーポットへアクセス件数

	windowXP SP2	windowsXP SP3	合計
TCP	2298	811	3109
IPMP	196	68	264
RAW	43	11	54
UDP	17	5	22

表 1 は 3 ヶ月間収集したデータである。収集したデータの分析結果（protocol によってアクセスしてきた件数と windows の service pack の比較）を示す。アクセスしてきた件数をみると OS のバージョンが新しい SP3 の場合よりバージョンの古い SP2 は圧倒的に多いことがわかる。それは感染させる側が port や ip を変えながらスキャンをするが応答の問題でこれ以上しても無駄だと思ってすぐ諦めたからだと考えられる。ウイルスへの感染を待ったが結局ウイルスには感染されなかった。近年の OS はウイルスの対策が進んでおり、ネット上に設定するだけでは感染しないようである。2 か月をかけて設置した hsc は使えなくなった。

第4章　ボットの動作解析

4.1　構成

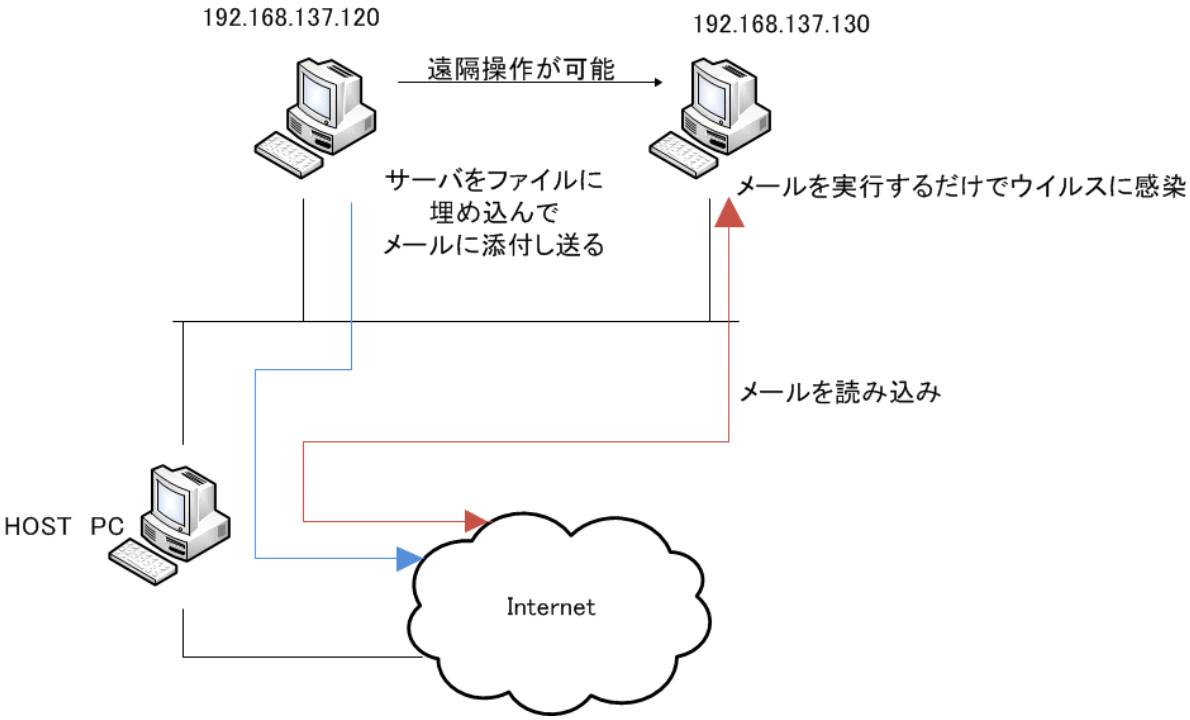

図 4.1　感染の構成

この実験は自分がたてた VM を利用して他の VM を感染させる実験である。ウイルスはメールに添付して相手に送った。メールによる感染が確認できてからはネットを切った。それはウイルスを利用して実験を行うためウイルスが外側に流れる恐れがあるからである。やり方はネット上のボットを入手して感染を行った。感染の仕方は HOST の PC の内に 2 つの VM をたてた。VM の IP アドレスはそれぞれ 192.168.137.120 と 192.168.137.130 である。129.168.137.120 が感染させる側で 192.168.137.130 が感染される側である。ボットとして使用したのは PRORAT である。PRORAT は遠隔操作、DDoS 攻撃や KEYLOG 機能、情報の取り出しなどいろいろな機能が入っているものである。順番を説明すると PRORAT を利用してサーバを生成する。サーバとはウイルスである。そのサーバを他のファイルに埋め込む。

それからそのファイルをメールに添付して 192.168.137.130 に送る。送られたメールを感染される側が実行するとウイルスに感染され遠隔操作ができるようになる。これで準備はできた。感染を確認するために感染される側に接続し、KEYLOG を試してみた。

4.2　prorat の解析

下の図は PRORAT を利用して行った KEYLOG のシーケンスである。最初に SYN から見ると SYN を送って相手のパソコンが生きているのか生きてないのかを確認した。返事が返って来たのでそこから PRORAT に接続した。PRORAT に接続したら感染された側から PASSWORD の要求が送られてきた。PASSWORD を入力したら感染された側からログインの確認ができたと返事送られてきた。返事が返って来たので遠隔操作ができるようになった。

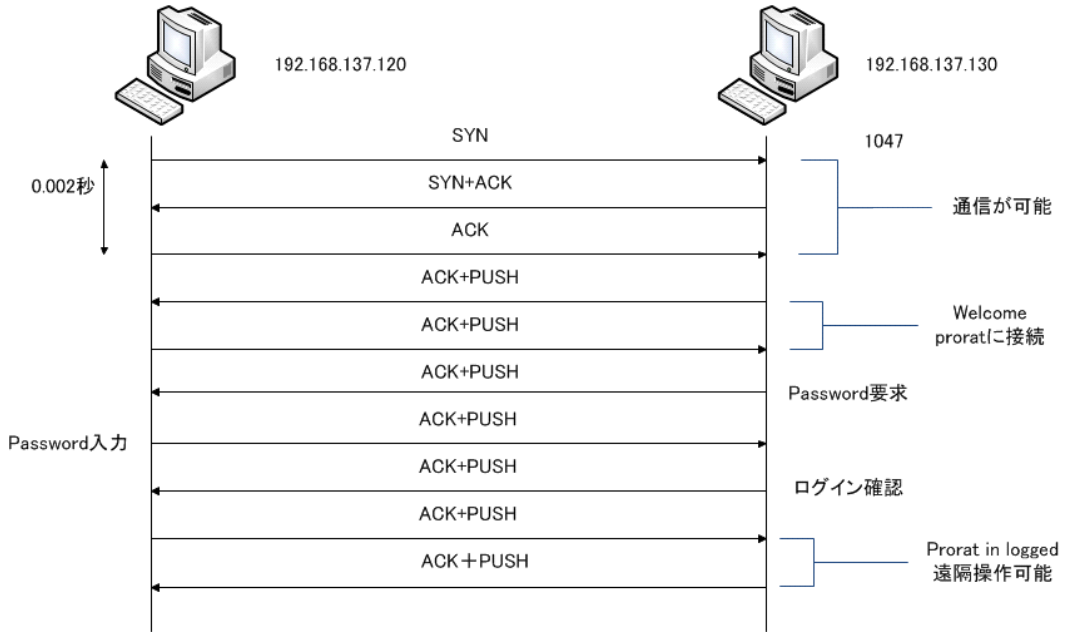

図 4.2　prorat の接続

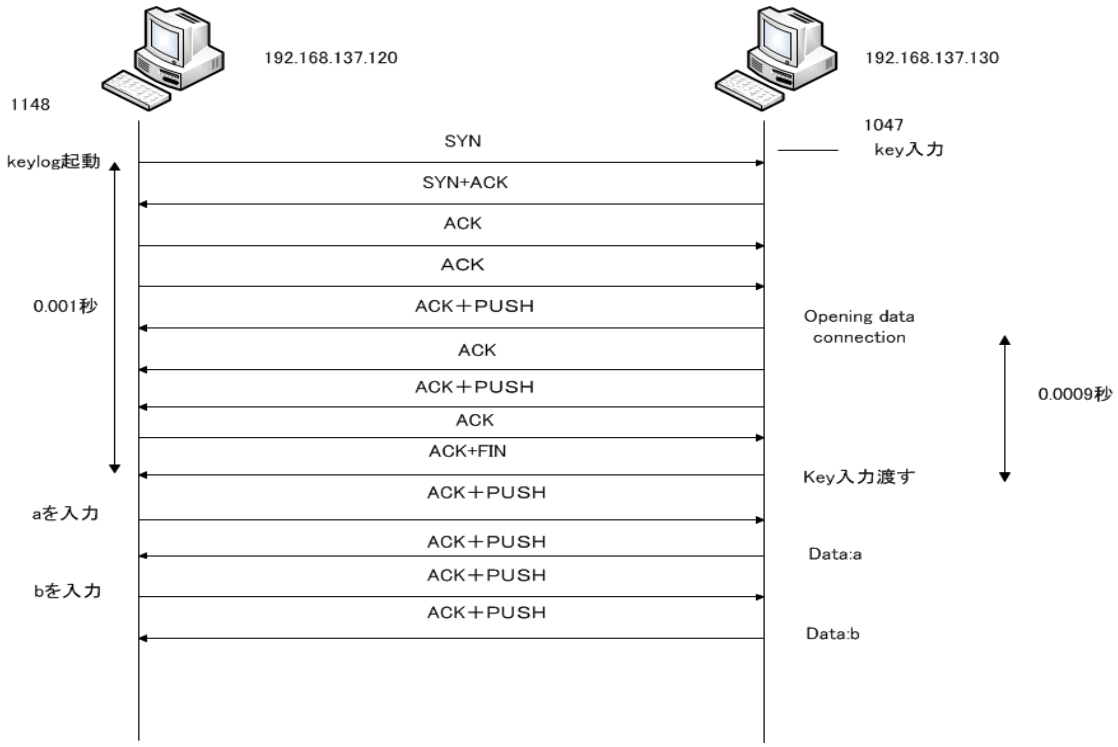

図 4.3　KEYLOG のシーケンス

keylog のシーケンスだがログインが確認できたので keylog を行った。その前に感染された側を利用して key 入力を行った。なぜなら感染された側が入力した情報を盗み出すためであった。key 入力が終わったら、keylog を起動した。syn から送られ syn+ack そして ack のやり取りがあった。これで相手との通信ができる。通信の確認後感染された側が data に接続し 192.168.1137.120 に key 入力を渡してくれた。全体的にかかった時間は 0.001 秒で key 入力の情報を受け取るまでの時間は 0.0009 秒であった。これで keylog のシーケンスは終わった。シーケンスの下にあるのは文字の入力である。a を入力したとき b を入力したときである。

4.3　telnet との関係

telnet とはインターネットやイントラネットなどの TCP/IP ネットワークにおいて、ネットワークにつながれたコンピュータを遠隔操作するための標準方式また、そのために使用されたプロトコル。telnet サーバを立ち上げてあるコンピュータにネットワークにつながれた他のコンピュータから telnet クライアントを使ってログインし、そのコンピュータの目の前にいると同じよう操作することができる。これはボットプログラム telnet と同じ方式で遠隔操作や相手のパソコンにつながる方式は同じである。prorat は telnet をを利用したアプリケーションすなわちベースは telnet そのものである。

4.4　遠隔操作

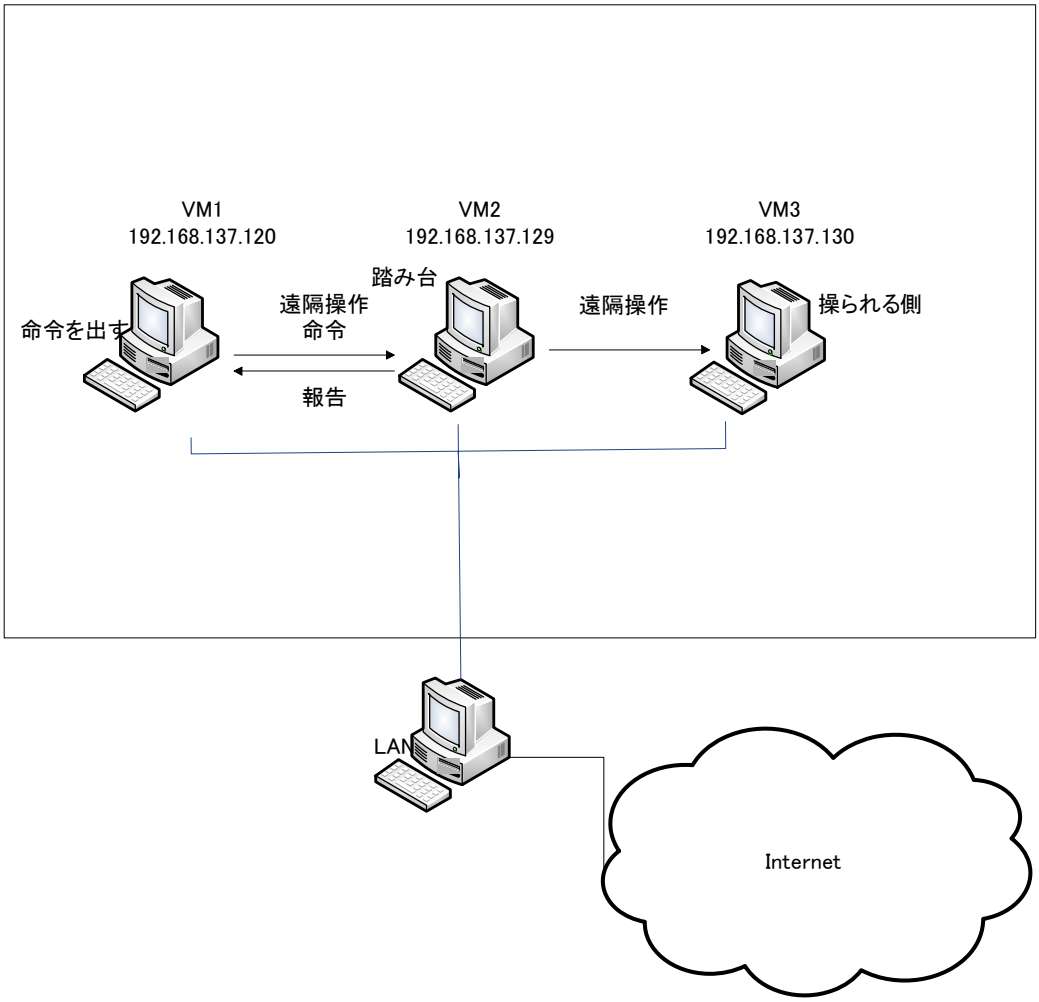

図 4.4　telnet の遠隔操作の仕組み

遠隔操作を行う前に、遠隔操作の仕組みには HOST の PC の内に 3 つの VM をたてた。その名を VM1,VM2,VM3 だとした。実験の順番は VM1 が遠隔操作をする側であった。VM2 が踏み台として使われるもの。VM3 が実際に操られる側であった。VM1 を利用して VM2 を遠隔操作できるようにした。コマンドを利用して telnet で遠隔操作ができるようにした。相手の IP アドレスや空いている PORT 番号と PASSWORD が分かれば接続ができる。接続が出きたら VM2 は VM1 から自由に遠隔ができる。それから自分は VM1 を利用して VM3 を遠隔できるようにした。VM1 を利用しているが実際は VM2 を遠隔で操作しているので VM2 を利用して VM3 を遠隔操作するようになっている。簡単にいうと自分は VM1 を利用しているが全体的にみると VM2 が VM3 を遠隔操作しているようになっている。

4.5　分析

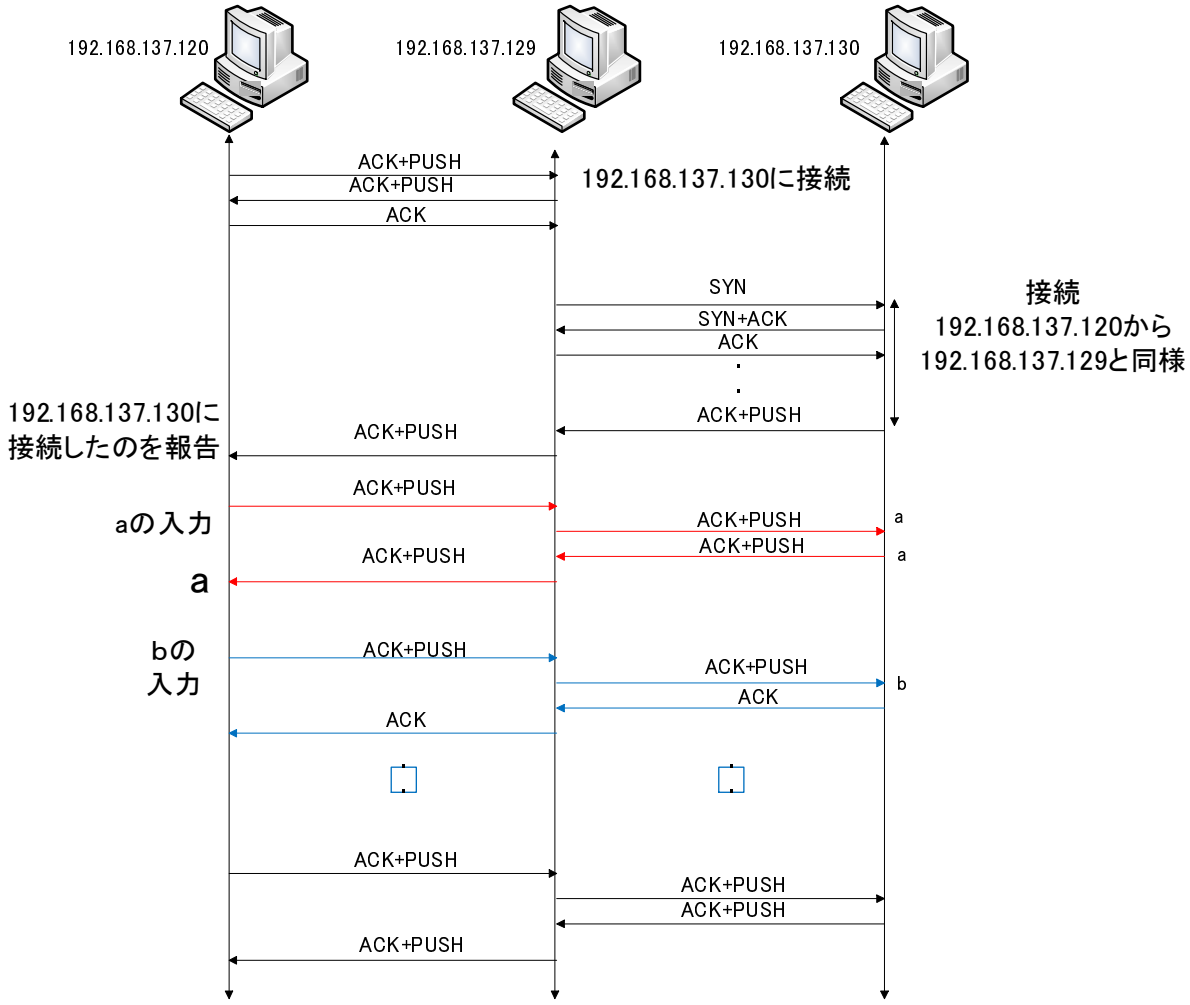

図 4.5　bot の解析

図をみると prorat を利用して 192.168.137.129 に接続した。接続は図 4.4 の接続と同様である。192.168.137.129 への接続が終わったら、192.168.137.130 へ接続を行った。感染した側が ack+push を踏み台に送る。それから踏み台の pc が 192.168.137.130 に syn を送り動いているのかどうかの確認をする。確認ができたらログインをする。ログインは図 4.4 と同様である。ログインが終わってから key 入力をした。感染した pc が a を入力する入力された文字は踏み台の pc に送られる。踏み台に送られた a はさらに感染された pc に送られる。感染された pc は a の文字を受け取り、返事をする。踏み台 pc に返事をし、さらにその返事は感染した側に送られる。これで文字の入力は終わる。これは telnet のログインとパケットの送り方とまったく同じである。ログインとパケットの送り方。telnet もログインするとき id

と password を利用してログインし、パケットも一文字ずつ飛ばす。これは prorat は telnet をベースにして作られたアプリケーションであるからだ。

第5章　まとめ

近年 bot による被害が増えている。それでその動きを分析するために wireshark や hsc そしてボットプログラムを利用して分析を行った。分析は最初は自然に感染するのを待ったが感染ができなくて自らボットプログラム（prorat) を利用して分析を行った。やり方はメールにウイルスを埋め込んで他の PC に送った。メールを受け取った PC はウイルスに感染され遠隔操作ができるようになった。遠隔操作をしながらパケットを分析した。今度は分析で終わったが、もし引き継ぎの人がおれば引き継いでもらいたい。

謝辞

本研究にあたり、渡邊教授からたくさんのことを教えていただいて心から感謝しております。そしてパソコンについて、ウイルスについも知ることができてありがたいと思います。一年間渡邊研究室に配属ができて感謝です。ほんとに渡邊教授に感謝します。

参考文献

[1] 竹尾大輔、他、情報処理学会論文誌：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

[2] 高橋正和、他、フィールド調査によるボットネットの挙動解析

[3] 静岡大学　西坦　正勝、侵入挙動の反復姓によるボット検知方式

[4] 日本データ通信協会　有村然う浩一、　ボット対策プロジェクト「サイバークリーンセンター」からみた国内のマルウェア対策

[5] Guofei gu,junjie Zhang ,Wenke Lee , Detectioing Botnet Command and Control Channels in Network Traffic

[6] イムチェテ、ボットネットの動向と対応技術の現状

[7] Edward Balas , 分散ハニーネット

研究業績

学術論文

なし

研究会・大会等

なし