ボットによる遠隔操作の解析

090430070 朴明模
渡邊研究室

1. はじめに

近年、ウイルスやワームに加えて、ボットネットによる被害が増大している。多くの場合は IRC(Internet Relay Chat) のメカニズムを通信基盤として利用しており、数百台から数万台の規模のものが確認されている。本稿ではハニーポットと wireshark を使用して得られたパケットデータのモニタからボットの動きの分析を行ったので報告する。

2. ボットネット

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。

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、ハーダー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はハーダーの手先となってしまい、意識せず犯罪に荷担することがある。

3. ハニーポットによる分析

グローバルアドレス上にウイルスソフトの入ってないハニーポット PC を置き、故意に感染するかどうかを調査した。Wireshark でその動作の分析をした。OS には windowsSP2 と windowsSP3 を使用した。

表 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の分析結果である。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。これは感染元がスキャンをすぐあきらめるためだと思われる。ウイルスへの感染を待ったが結局ウイルスには感染しなかった。近年の OS はウイルスの対策が進んでおり、ネット上に設置するだけでは感染しないようである。

4. ボットによる故意の感染

ネット上のボットを入手して分析を行った。実験を行うために PC 内に VM を 2 台たてた。ボットとしては Prorat を選択した。Prorat をメールに添付して他の PC へ送った。メールを受け取った PC 添付ファイルを開くことによりウイルスに感染した。感染した PC は送信元の命令に従うようになった。いろいろな機能があるがその中で keylog を指定すると、感染した PC 側のキーボードから入力した情報が全て見られるようになり ID や password が全てわかることを確認した。

5. prorat の動作解析

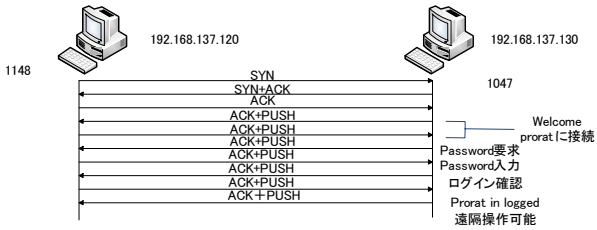


図 1: prorat ログインのシーケンス

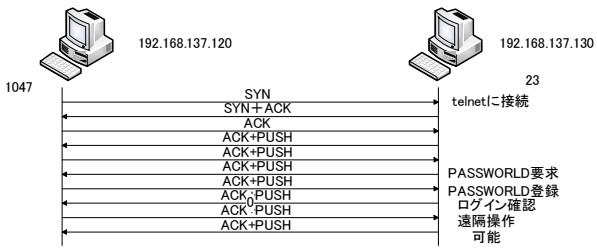


図 2: telnet ログインのシーケンス

図 1 は prorat に感染後の動きを図 2 は telnet の動きを wireshark で分析したものである。porat に接続するためには ID と password が必要である。ID と password の設定は最初の感染された側に接続時に行う。ID は相手の IP アドレスで、password は自分が最初設定したものになり、変更ができる。感染の結果 telnet とログインのシーケンスが全く同じであるのが分かった。だが prorat には telnet にない機能（keylog、format, データの管理など）がある。prorat は telnet の機能をそのまま使い、それにプラスされたものであると考えられる。

6. まとめ

ハニーポットを利用してボットの情報を収集した。またボットに自ら感染させて動作を Wireshark で解析をした。そして Telnet を利用して踏み台の解析やボットとの比較を行った。

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

ボットによる遠隔操作の解析

情報工学科
渡邊研
朴明模

研究の背景

- ボットによる被害が増大している

1. 迷惑メール送信
2. ボット感染活動
3. ホームページ攻撃

研究の目的

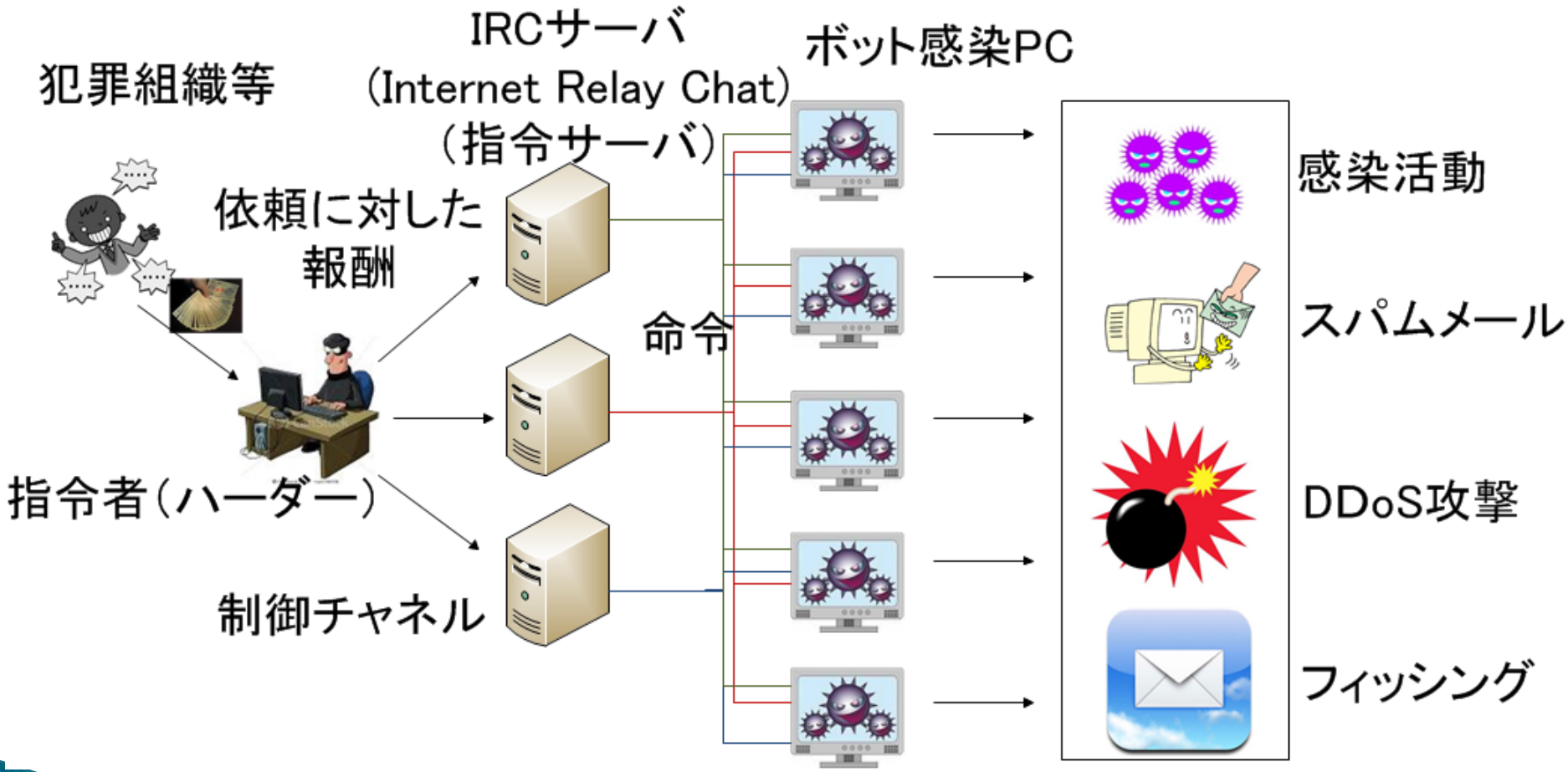
- ボットの解析

1. ハニーポットによる解析
2. 解析ソフト
3. 遠隔操作

ボットとボットネット

- ボットとはコンピューターに害をもたらすマルウェアの中でも、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。

感染と被害

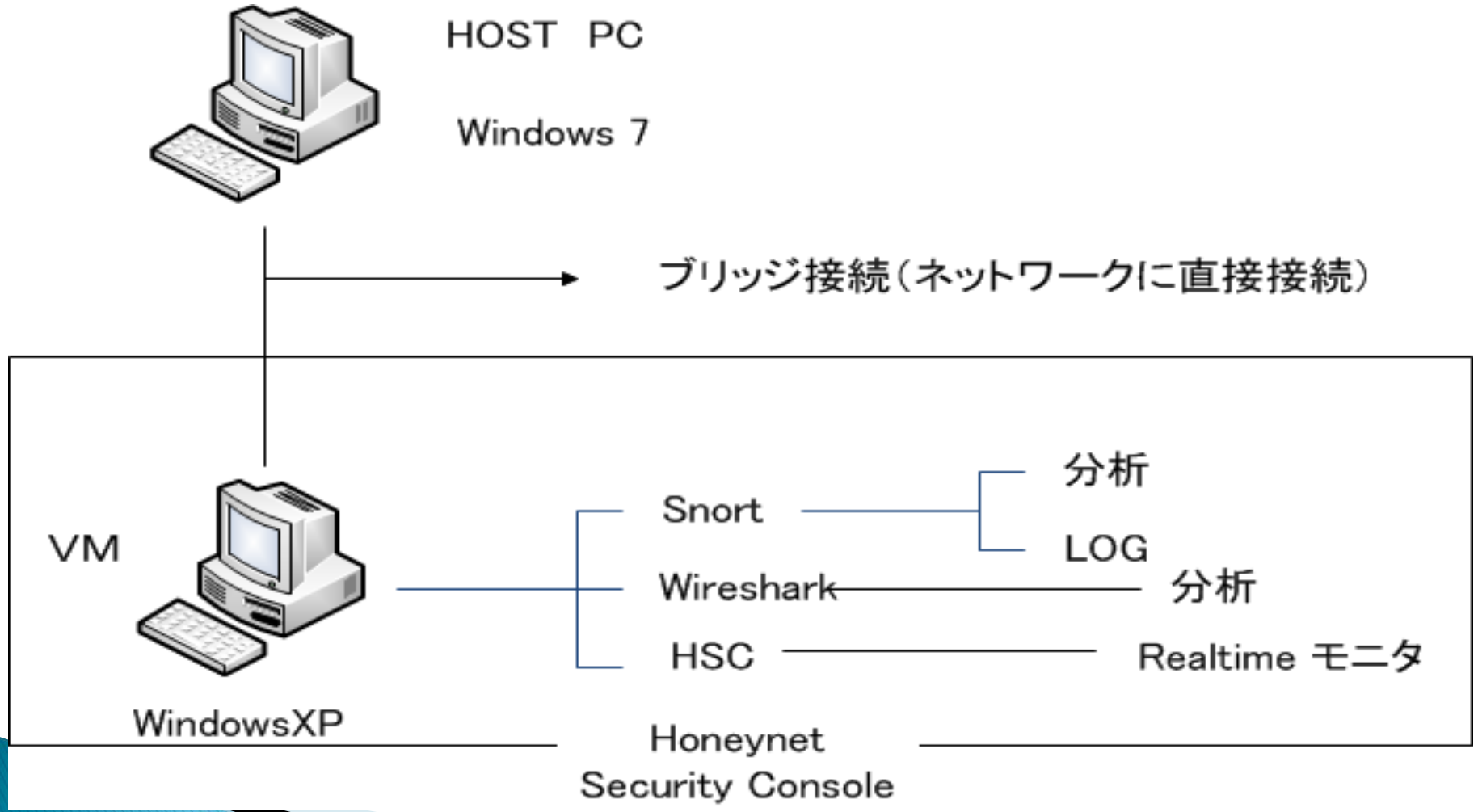

IRCサーバ
(Internet Relay Chat)
(指令サーバ)
ボット感染PC
犯罪組織等
依頼に対した
報酬
命令
指令者(ハーダー)
制御チャネル
感染活動
スパムメール
DDoS攻撃
フィッシング

ハニーポットの条件

感染されやすい

- firewallを無効にする
- Updateをしない
- 古いOSを使う(windowsXPのsp2とsp3を使用)

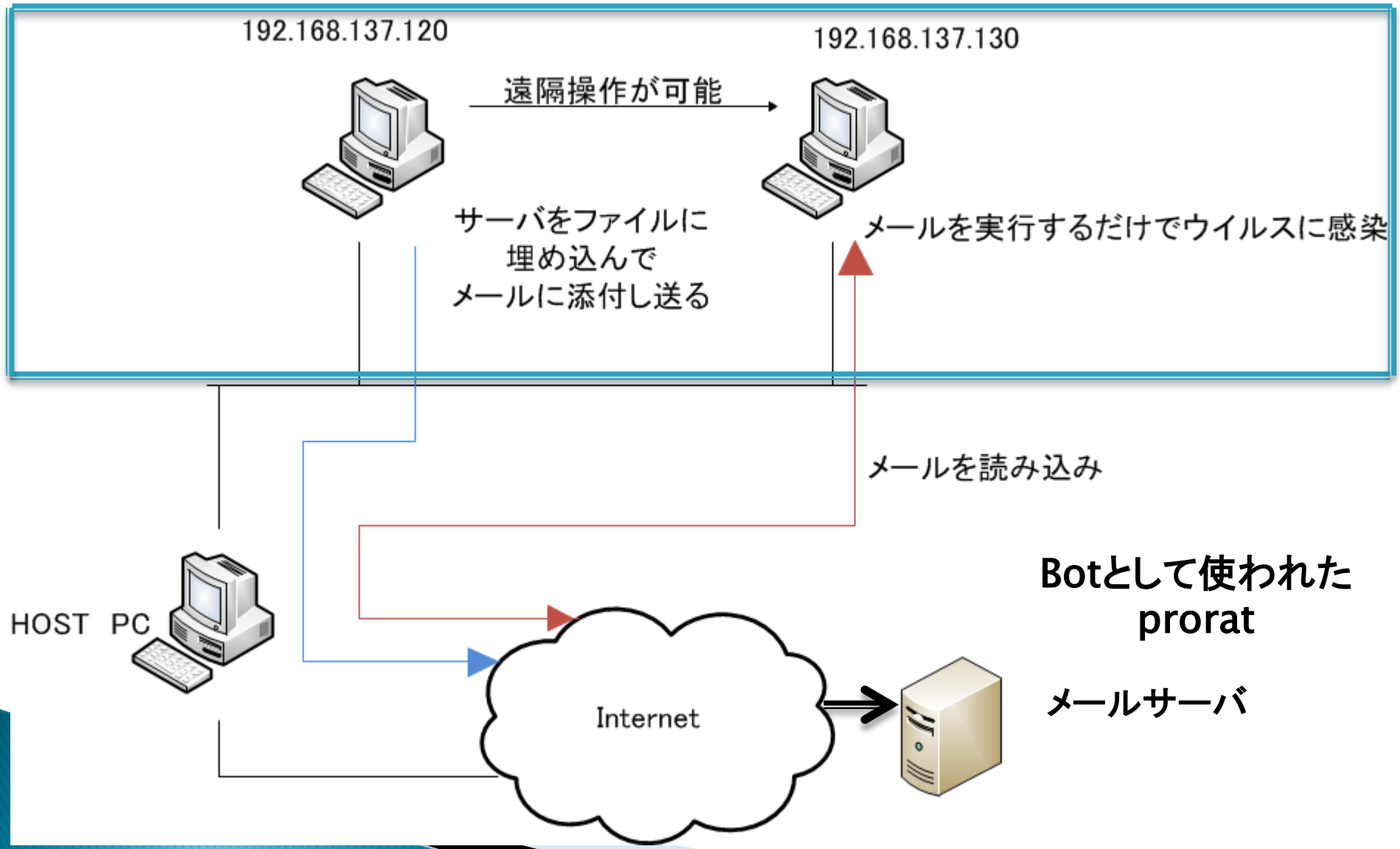
ハニーポットの構成


HOST PC
Windows 7
ブリッジ接続（ネットワークに直接接続）
VM
WindowsXP
Snort
分析
LOG
Wireshark
分析
HSC
Realtime モニタ
Honeynet
Security Console

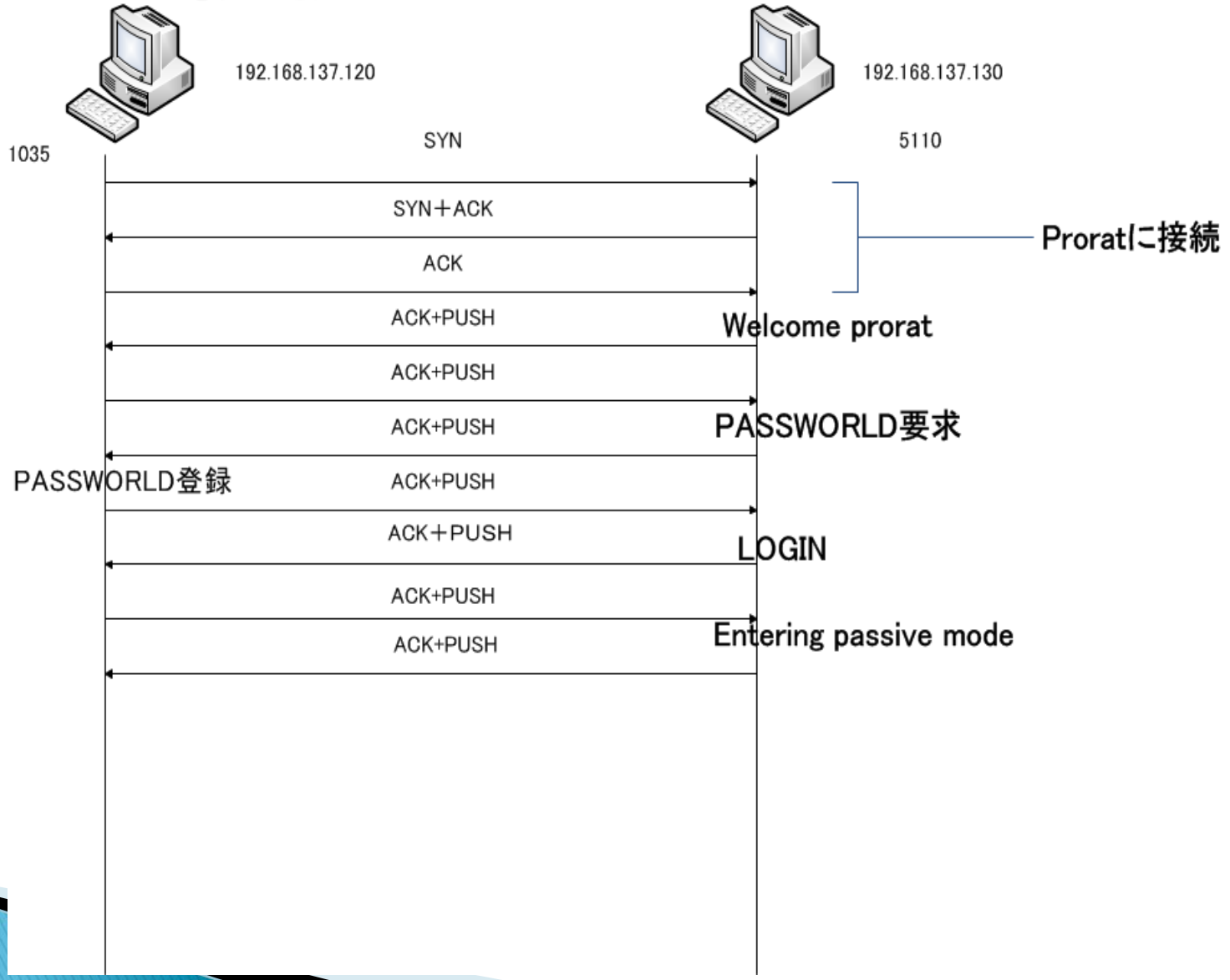
ハニーポットへアクセス件数

	windowsXP SP2	windowsXP SP3	合計
TCP	2298	811	3109
IRMP	196	68	264
RAW	43	11	54
UDP	17	5	22
合計	2554	895	3419

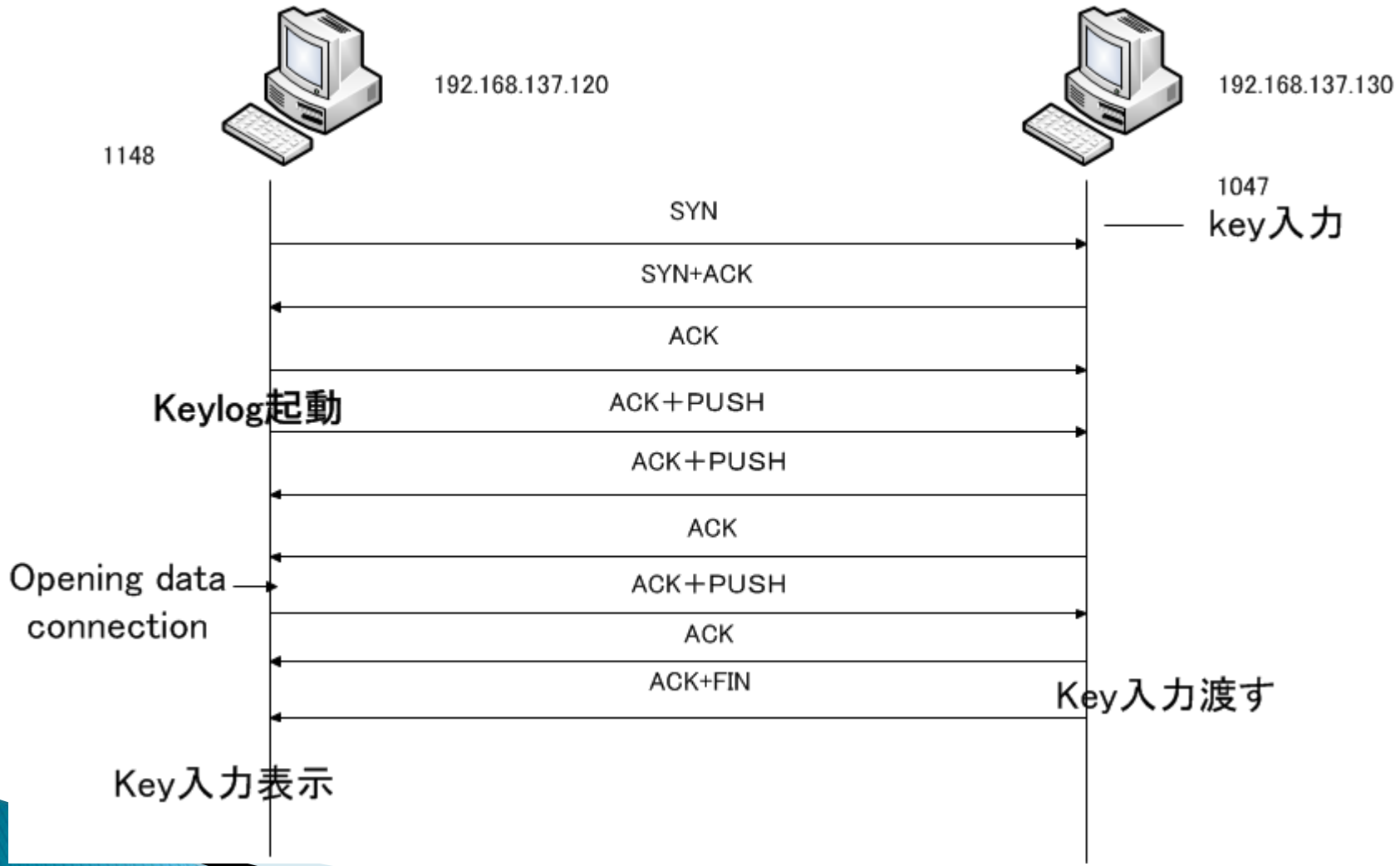
ボットによる故意に感染



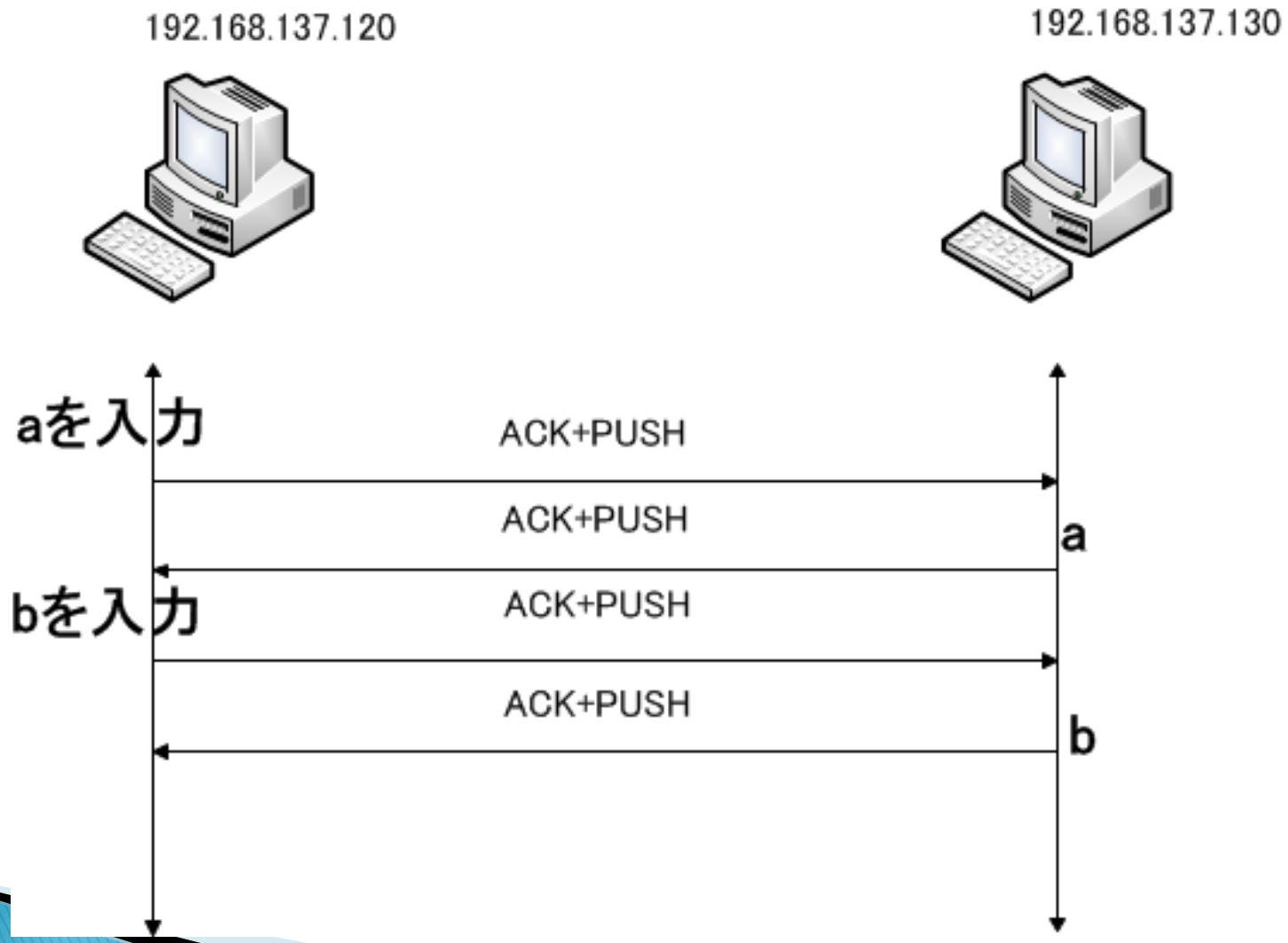
Proratに接続


192.168.137.120
192.168.137.130
1035
SYN
5110
SYN＋ACK
ACK
Proratに接続
ACK+PUSH
Welcome prorat
ACK+PUSH
ACK+PUSH
PASSWORLD要求
PASSWORLD登録
ACK+PUSH
ACK＋PUSH
LOGIN
ACK+PUSH
Entering passive mode
ACK+PUSH

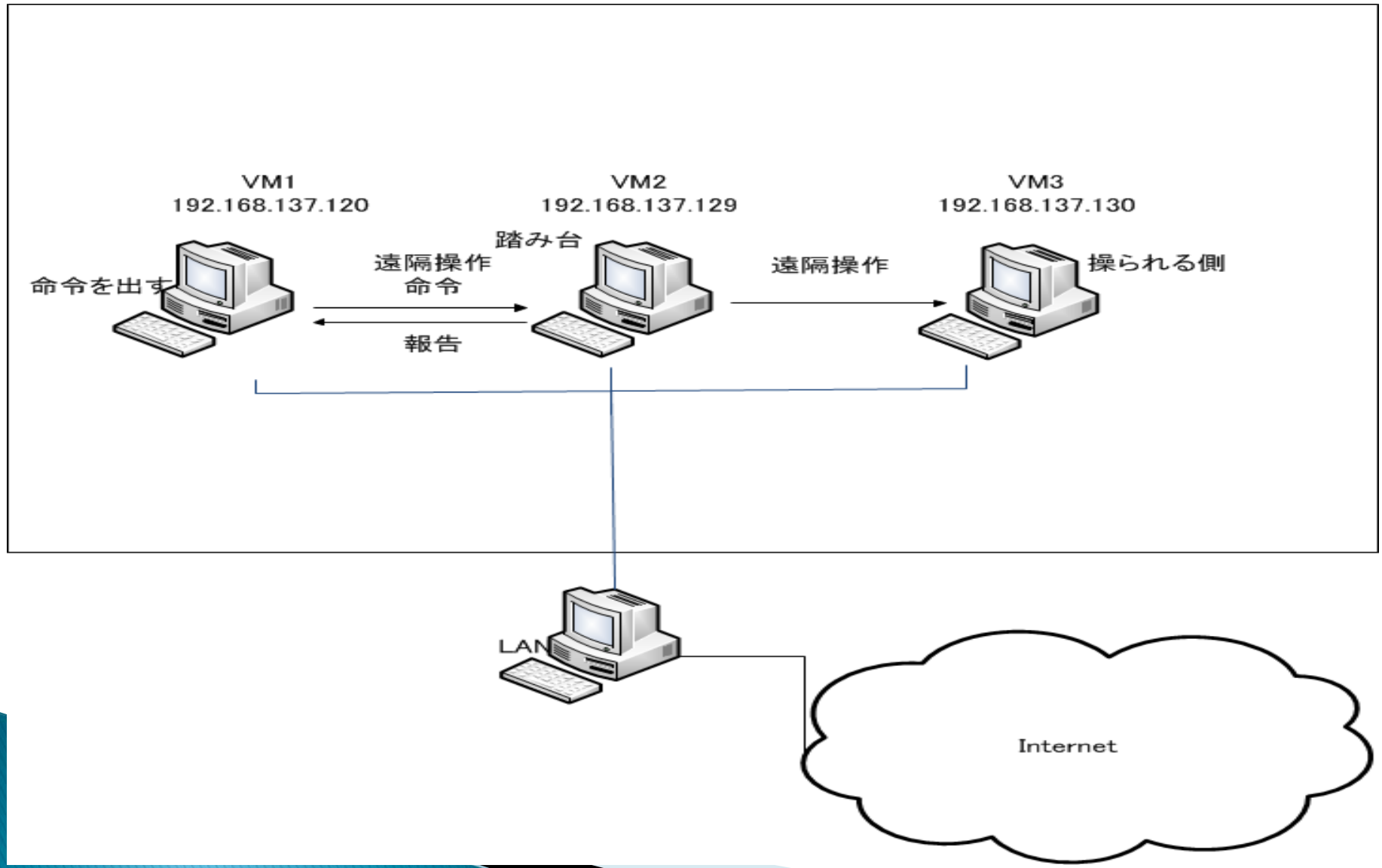
Proratのkeylog解析



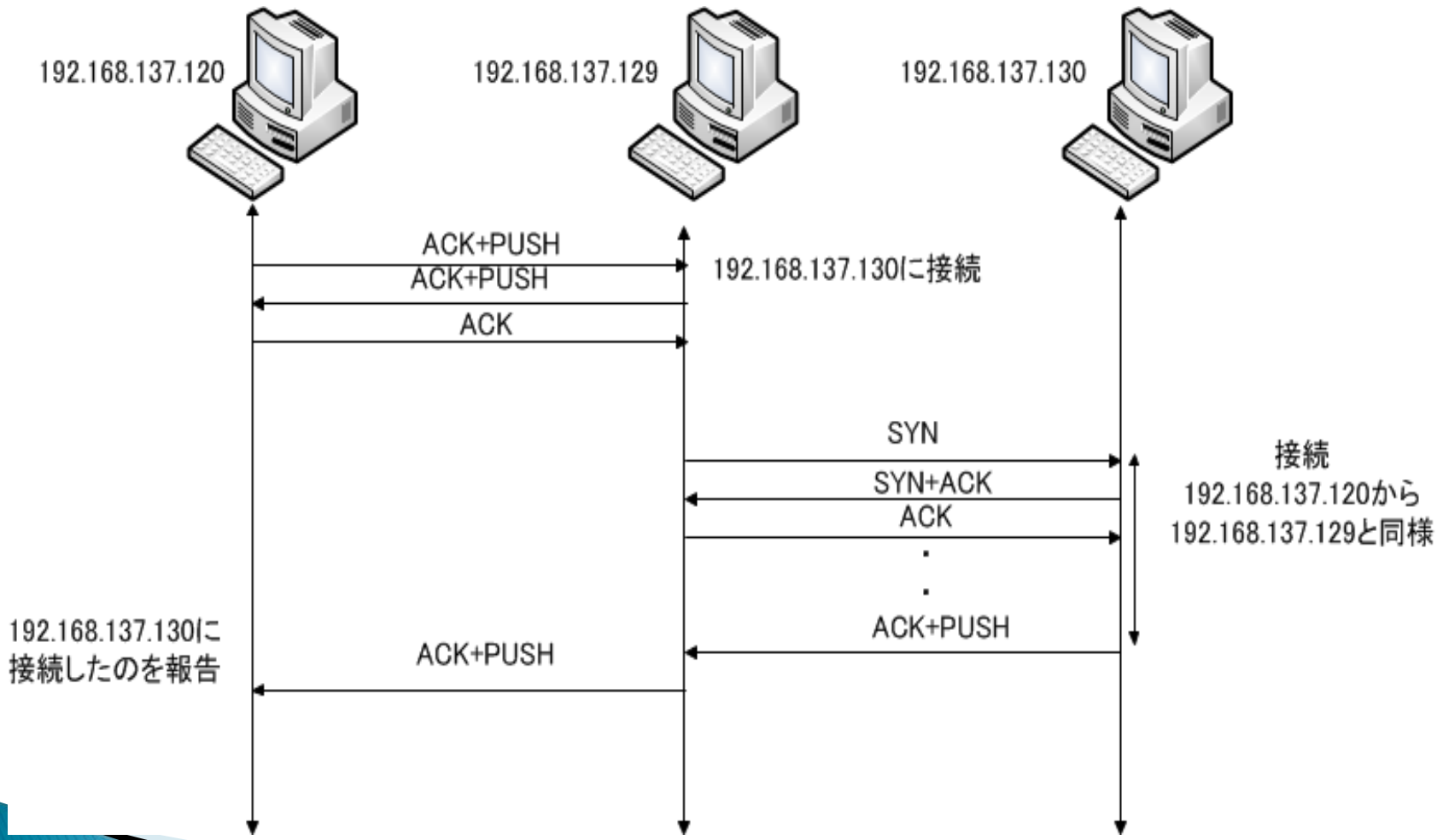
Proratの遠隔操作



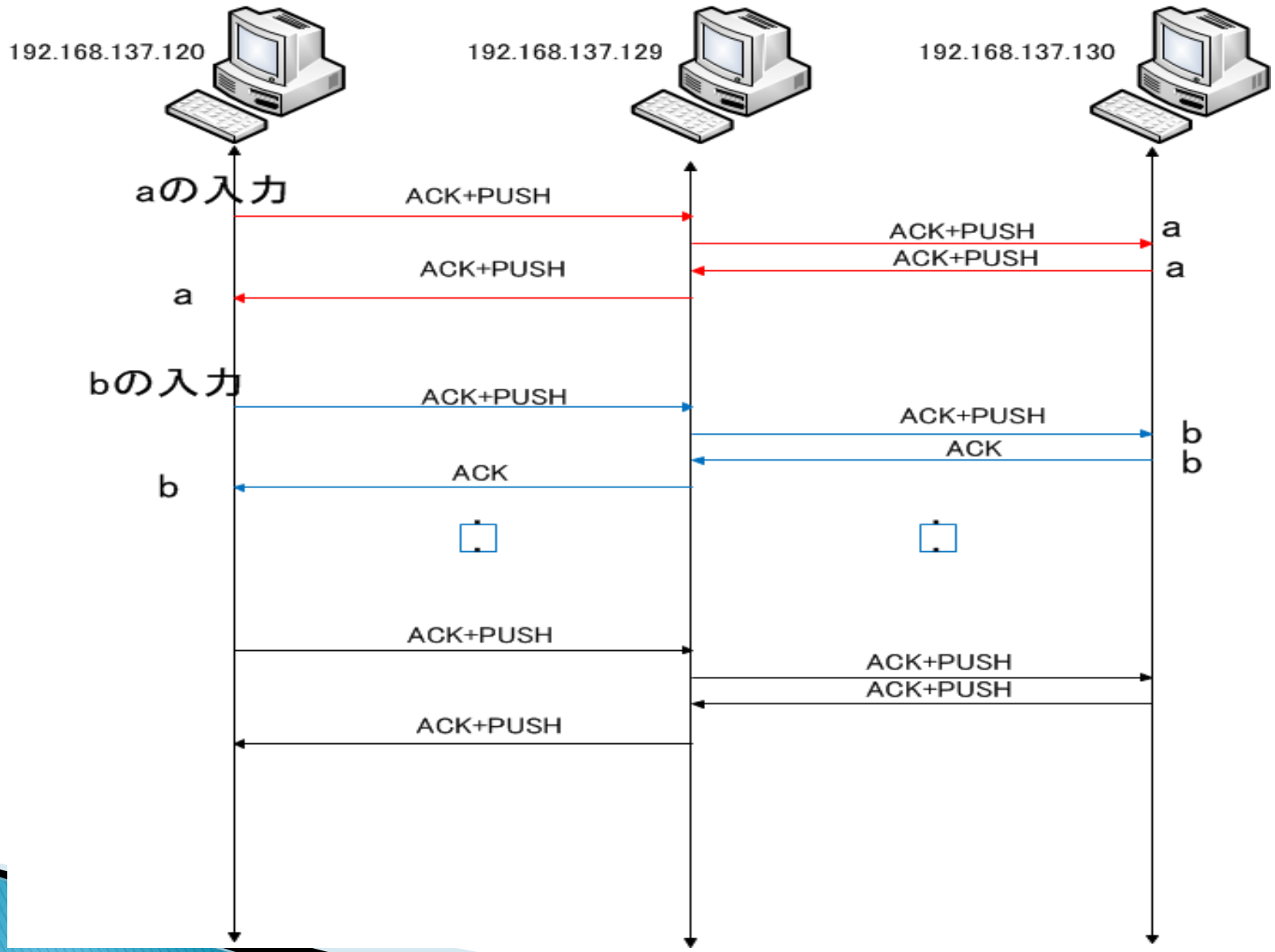
遠隔操作を利用した踏み台攻撃



解析


192.168.137.120
192.168.137.129
192.168.137.130
ACK+PUSH
ACK+PUSH
192.168.137.130に接続
ACK
SYN
SYN+ACK
ACK
接続
192.168.137.120から
192.168.137.129と同様
ACK+PUSH
192.168.137.130に
接続したのを報告
ACK+PUSH

解析


192.168.137.120
192.168.137.129
192.168.137.130
aの入力
ACK+PUSH
ACK+PUSH
a
ACK+PUSH
ACK+PUSH
a
a
bの入力
ACK+PUSH
ACK+PUSH
b
ACK
ACK
b
b
ACK+PUSH
ACK+PUSH
ACK+PUSH
ACK+PUSH

まとめ

- ハニーポットを利用してボットの情報を収集した。
- ボットに自ら感染させて動作をwiresharkで分析した。
- Proratはtelnetをベースにしてつくられたアプリケーションである。

参考文献

- 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
- 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

ご清聴
ありがとうございました。