# PSH パケットと SYN パケットの関係に着目した踏み台攻撃の検出手法の提案

染川　敦*，鈴木　秀和，渡邊　晃（名城大学）

Proposal of a Detection Method on Stepping-stone Attacks Focusing on the Relation between PSH Packet and SYN Packet

Atsushi Somekawa, Hidekazu Suzuki, Akira Watanabe (Meijo University)

## １．はじめに

PC が遠隔操作され，犯罪予告のメールを送信されることにより，PC の所有者が誤認逮捕されたことが社会問題になった．

アカウントやパスワードを不正に入手することで，ターゲットに対して不正アクセスすることが可能になる．このような攻撃を踏み台ホストを介して実行されると，ターゲットからは踏み台ホストに攻撃されているように見える．この場合，踏み台ホストは加害者とみなされる可能性がある．

本稿では，踏み台攻撃時には踏み台ホストからターゲットに対して TCP コネクション確立要求があることに着目し，踏み台ホストが踏み台にされていることを検出する手法を提案する．

## ２．踏み台攻撃の概要

踏み台攻撃はリモートログインをいくつか経由することにより攻撃者の特定を困難にするが，複数の踏み台ホストを経由した場合も検出原理は同じであるため，本稿では踏み台ホストが 1 台の場合について記述する．

本稿において対象とする踏み台攻撃モデルを Fig.1 に示す．攻撃者（Attacker）は踏み台ホスト（Stepping-stone）を介してターゲット（Target）にアクセスする．このとき，攻撃者は何らかの方法を用いて，あらかじめ踏み台ホストおよびターゲットのアカウントやパスワードを入手しているものとする．攻撃者から踏み台ホストへの通信は Telnet や SSH などのリモートログインプロトコルを用いるが，踏み台ホストからターゲットへの通信はそれだけでなく，FTP などのプロトコルも検出対象とする．

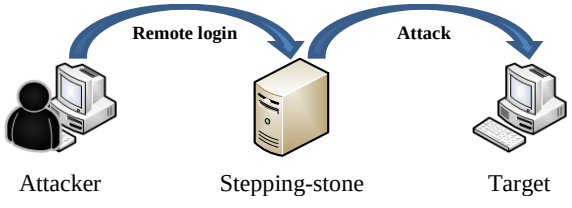



Fig.1　A stepping-stone attack model

## ３．提案方式

Fig.2 に提案方式の原理を示す．まず攻撃者が踏み台ホスト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．次に，攻撃者は踏み台ホストに対してターゲットへのアクセスを行うためのコマンドを投入する．コマンドの最後の文字が入力されると，踏み台ホストはコマンドを解読して，ターゲットに対して TCP コネクションの確立を行う．そこで，踏み台ホストはその間リモートログインパケットの監視を行いつつ，他のホストへ新たな TCP コネクションが確立されようとするのを監視する．リモートログインパケットの受信とコネクション確立要求の送信との間の時間が一定時間内であれば，踏み台ホストが踏み台にされていると判断する．

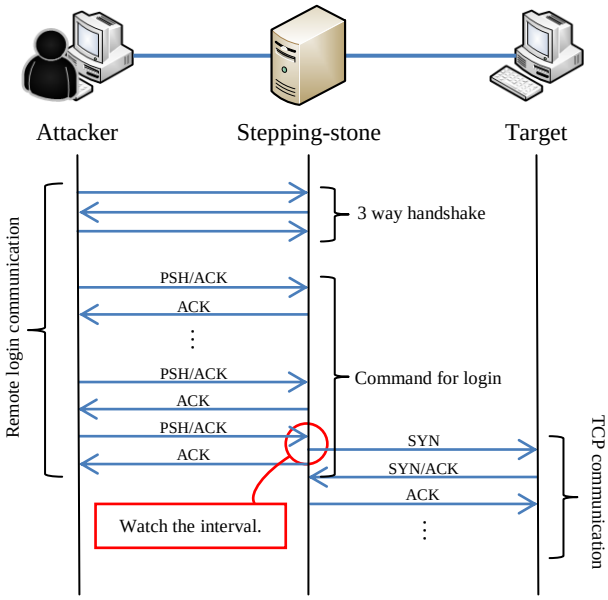



Fig.2　The sequence of a proposal system

攻撃者からのリモートログインコマンドの最後の文字を含むパケットには，アプリケーションに処理を依頼するための PSH フラグがセットされている．踏み台ホストは PSH フラグがセットされたパケットを受信するとアプリケーションの処理を実行し，ターゲットに対する TCP コネクションを確立する SYN パケットを送信する．本提案はこの原理を利用したものである．

## ４．おわりに

踏み台ホスト宛のリモートログインパケットと，踏み台ホストから送信される TCP の SYN パケットを監視することにより，踏み台攻撃を検出する手法を提案した．今後は提案方式を実装する方法について検討を進める．

## 文　献

(1)竹尾．他:情報処理学会論文誌, Vol.48, No.2, pp.644-655, 2007.

# PSHパケットとSYNパケットの関係に着目した踏み台攻撃の検出手法の提案

名城大学　理工学部
染川敦　鈴木秀和　渡邊晃

Watanabe Lab.

# 研究背景

不正アクセスの増加

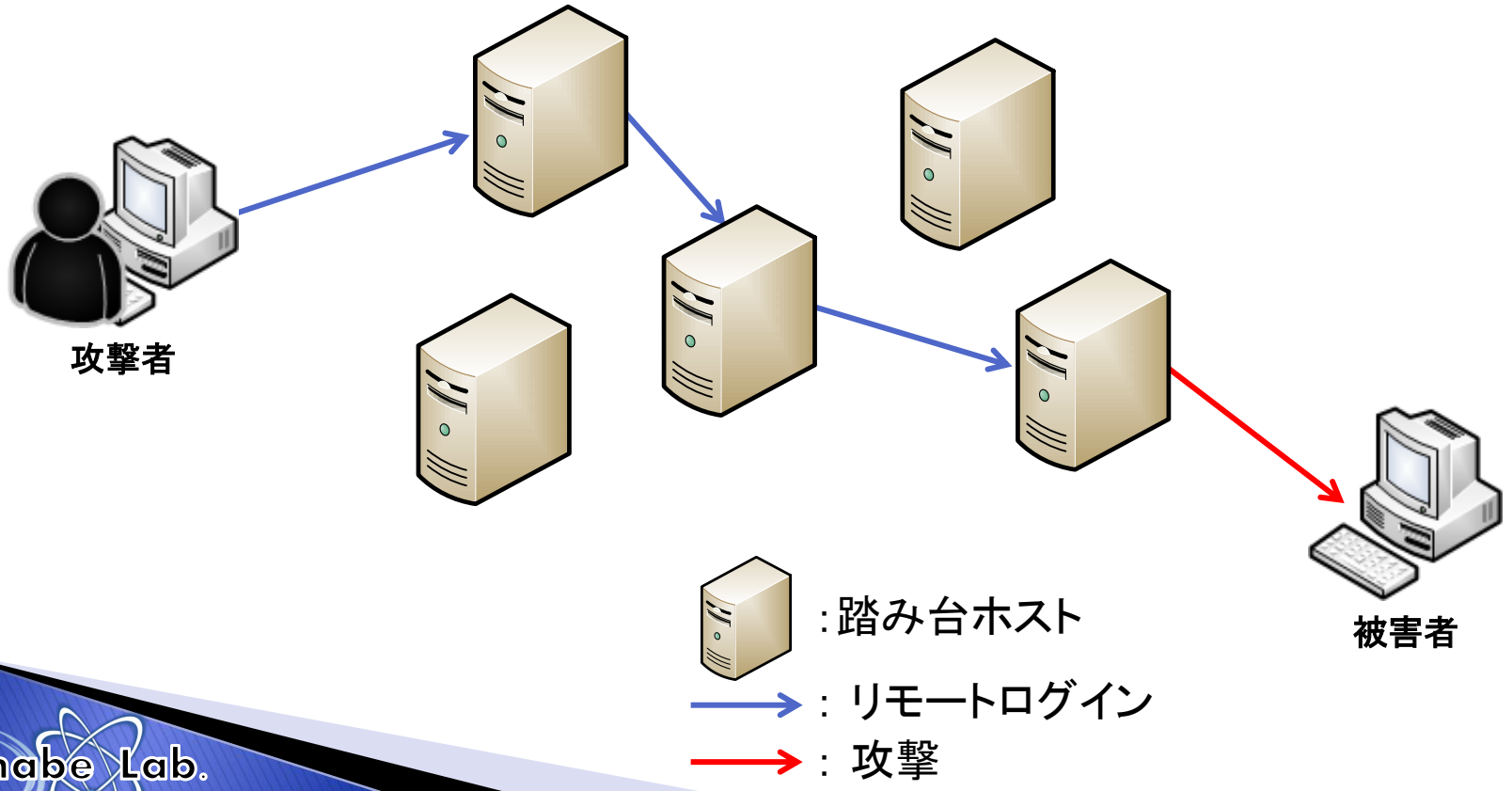
これらの攻撃は主に踏み台を介して実行される

踏み台のユーザが加害者になることもある

Watanabe Lab.

# 踏み台攻撃とは

何らかの方法（ウイルス，ソーシャルエンジニアリング等）で踏み台にリモートログインできるようにしておき，攻撃時に踏み台を渡り歩いて攻撃する攻撃手法．被害者からは踏み台に攻撃されているように見える．



# ユーザの対策

- 踏み台にされないための対策
  - 使わないポートは閉めておく

ウイルスに感染するとポートを開けられる可能性がある

- ウイルスに感染しないための対策
  - セキュリティソフトを使う
  - OSやアプリケーションソフトを最新の状態に保つ

ウイルスは亜種が次々と作られている

# リモートログイン

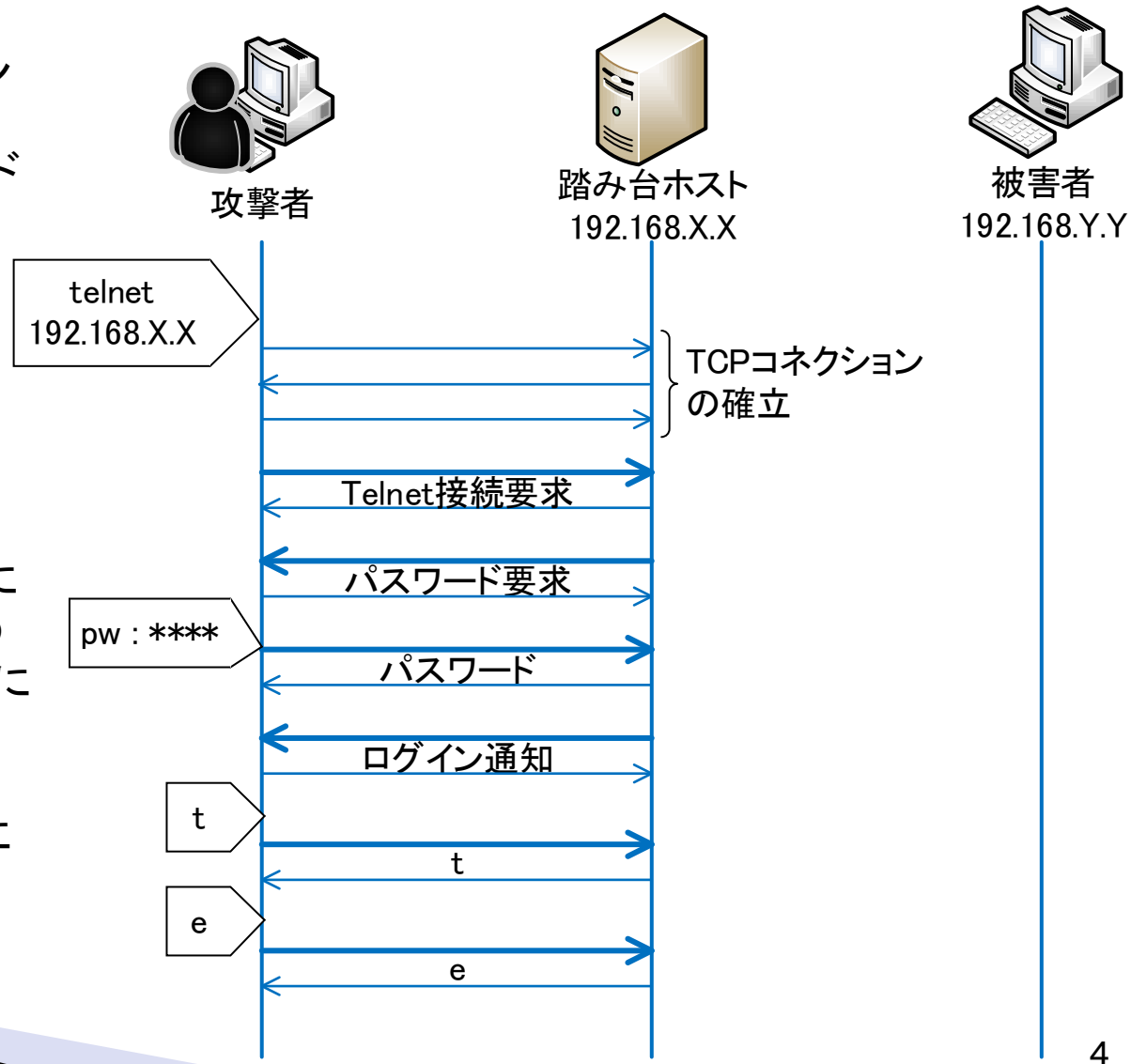
Telnetを例にしたリモートログイン

① 攻撃者が[コマンド：telnet IPアドレス] を入力する

② TCPコネクションが確立され，Telnet接続要求が送られると，踏み台ホストからパスワード要求が来る

③ パスワードを入力し，ログインに成功すると踏み台ホストを目の前にあるかのように使えるようになる

④ Telnetはキーを入力するたびにサーバ側に送信される

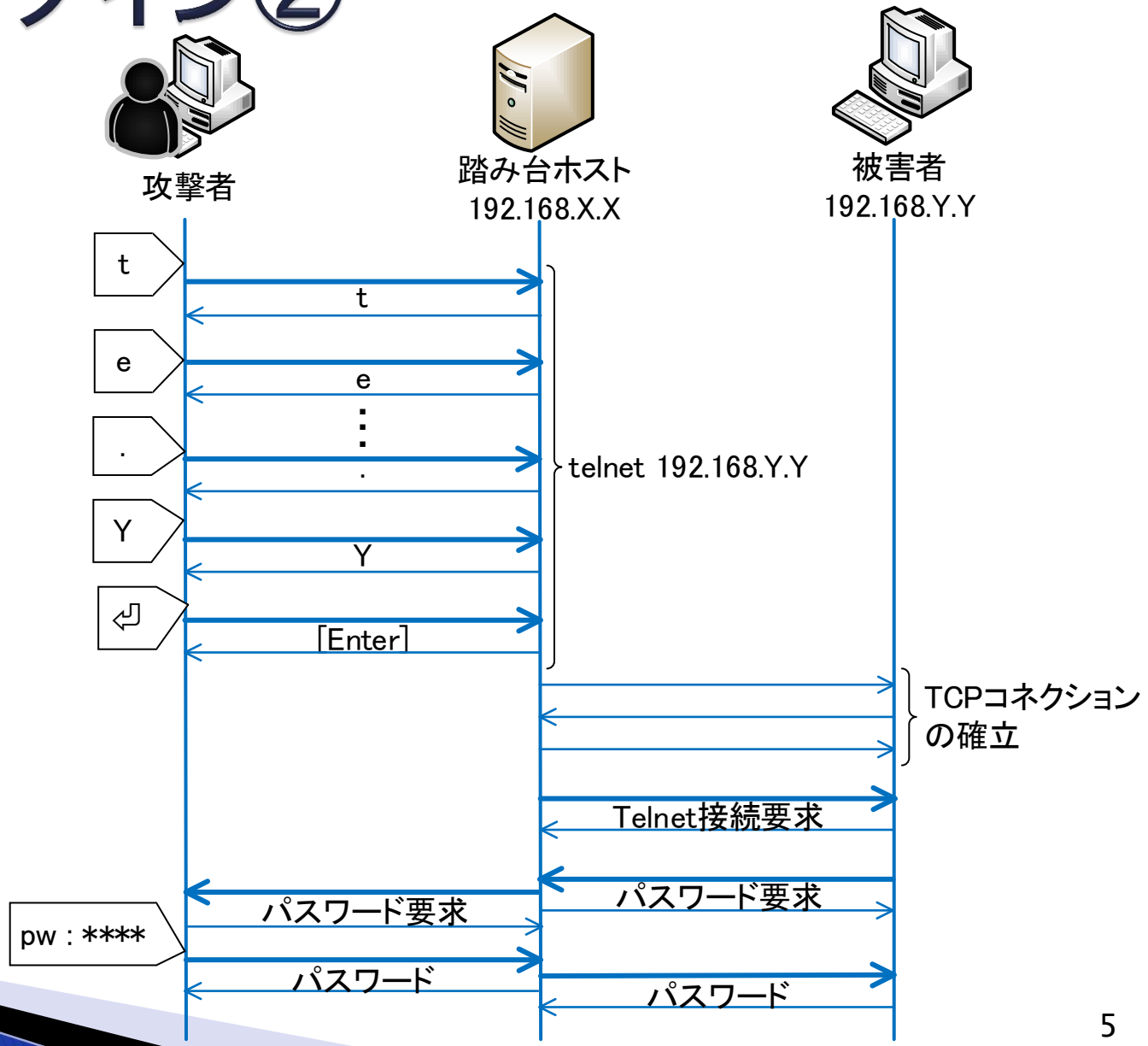


# リモートログイン②

⑤ コマンドの入力が終了すると踏み台ホストから被害者に向けてコマンドが出る

⑥ 踏み台ホストと被害者の間でTCPコネクションが確立され，踏み台ホストからTelnet接続要求が送られる

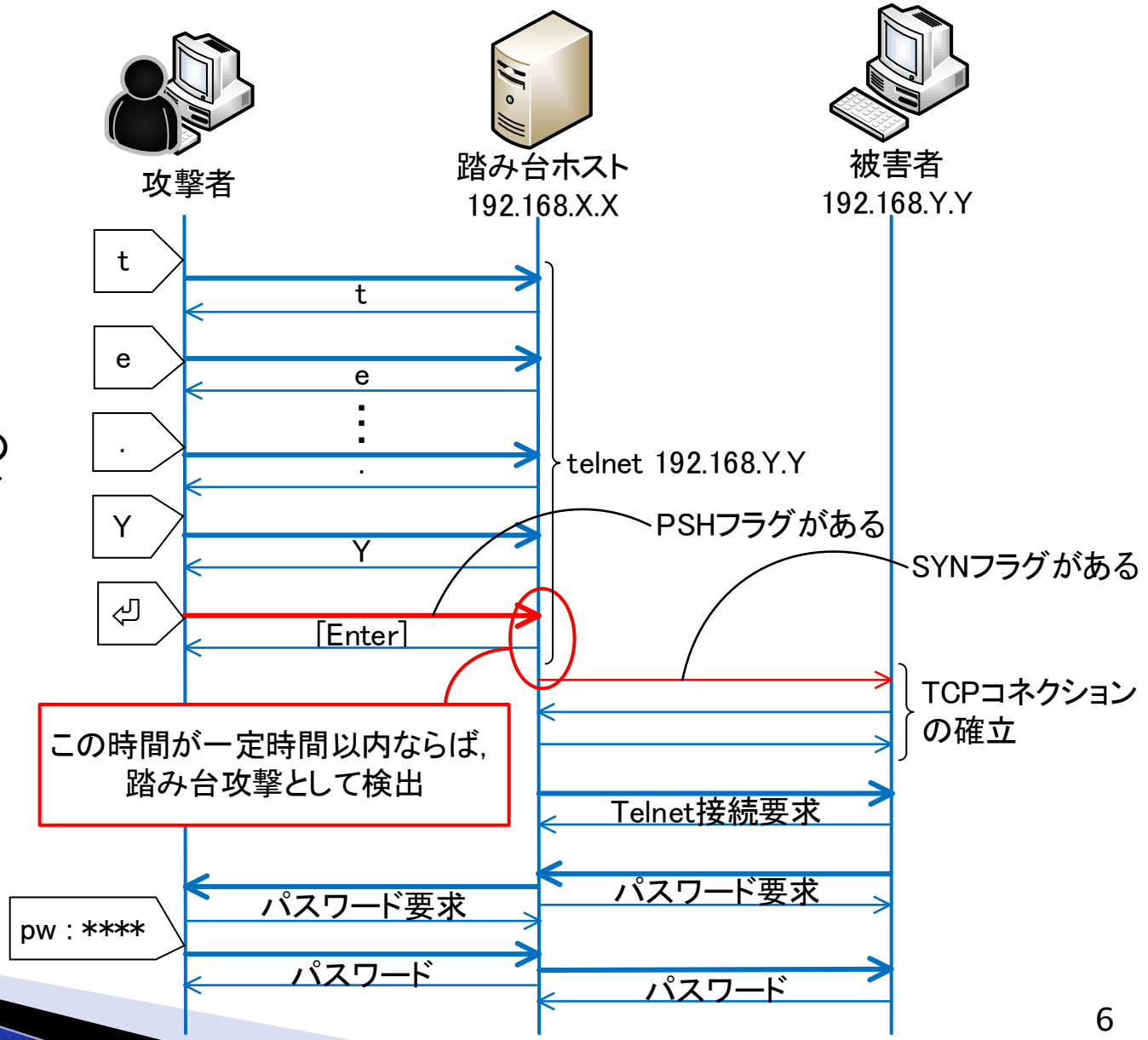
⑦ 攻撃者は踏み台ホストを介して被害者に対して通信を開始する



# 検出原理

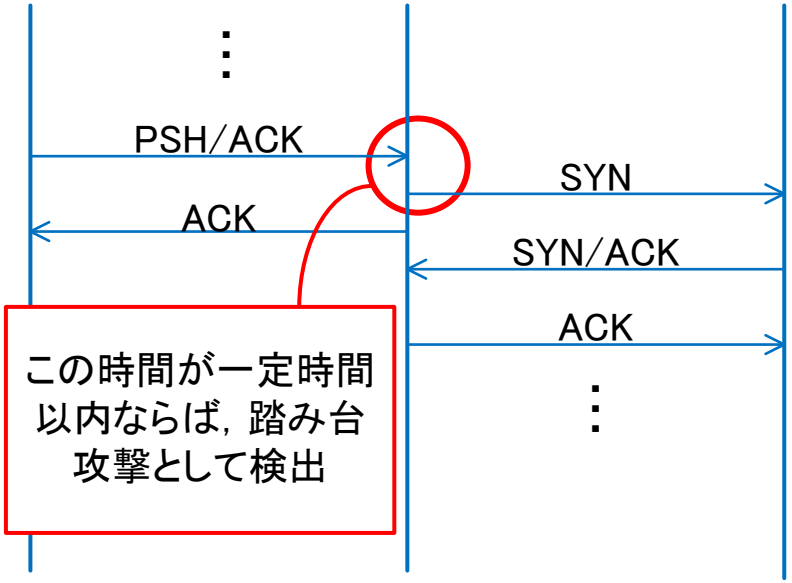
PSHフラグ：
アプリケーションに処理を
依頼するためのフラグ

SYNフラグ：
TCPコネクション確立要求の
初めのパケットにあるフラグ

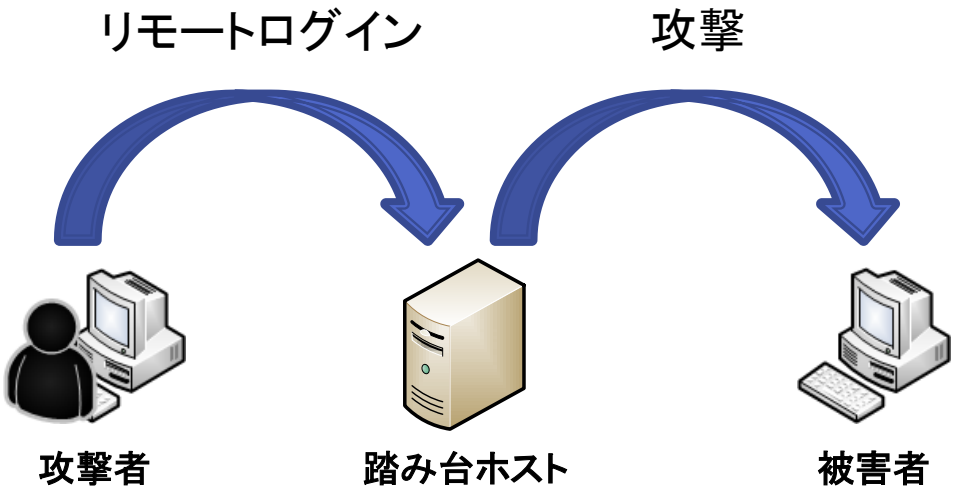


# 実験の目的

攻撃者から踏み台ホストへのリモートログインパケットと踏み台ホストから被害者へ送信されるTCPパケットの時間間隔を解析し，この時間間隔と踏み台攻撃の関連性を発見する.



# 実験モデル

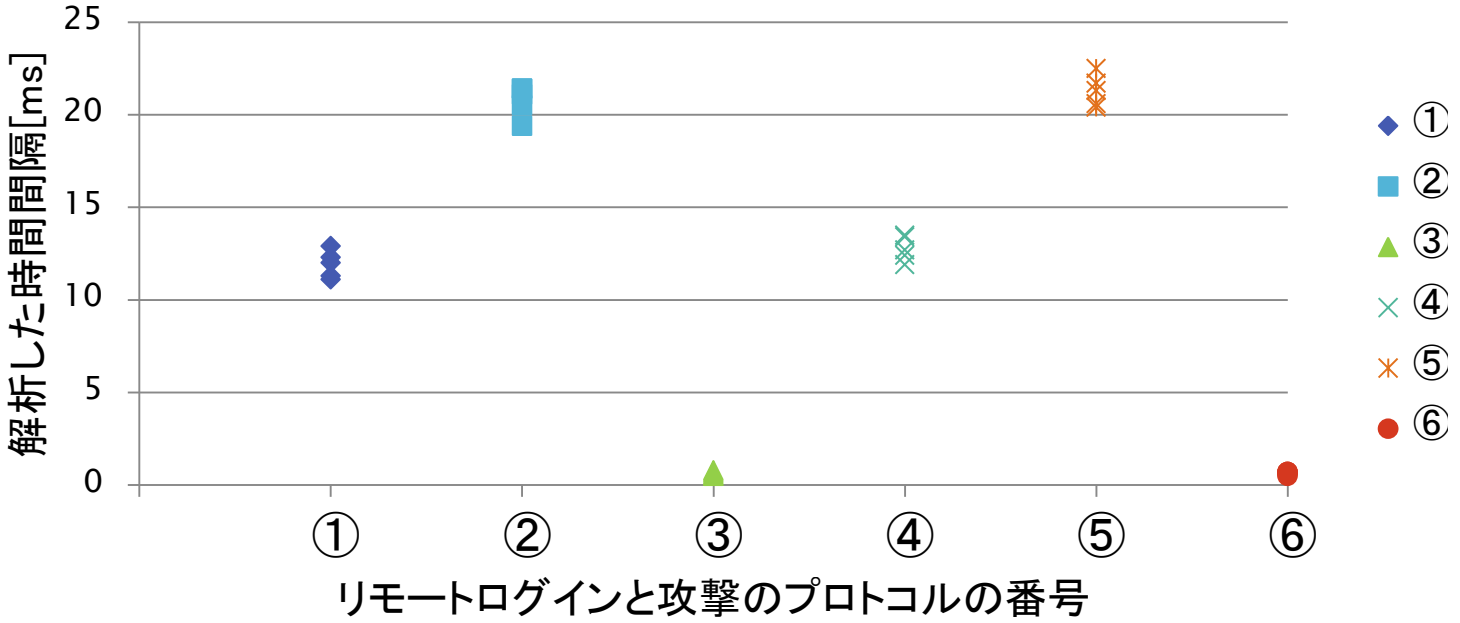



Wiresharkを用いて
パケットを監視

※仮想マシン上で実行

| リモートログイン | 攻撃 |
|---|---|
| Telnet | Telnet |
| SSH | SSH |
| | FTP |

# 実験結果




| | | 攻撃 | | |
|---|---|---|---|---|
| | | Telnet | SSH | FTP |
| リモートログイン | Telnet | ① 11.9 | ② 20.7 | ③ 0.6 |
| | SSH | ④ 12.8 | ⑤ 21.3 | ⑥ 0.6 |

試行回数5回
単位：ms

# 考察

- TCPコネクションの確立を要求するコマンドの最後のパケットにはPSHフラグがあり，そのパケットの受信とSYNフラグのあるパケットの送信の間には一定の短い時間があることが確認された
- リモートログインのパケットと攻撃のパケットの間の時間はほぼ固定である

- 課題
  - 本実験では他のアプリケーションが起動していない
  - 閾値の決定方法

# まとめ

- 踏み台攻撃の検出原理と解析
  - 踏み台ホスト宛のリモートログインパケットと踏み台ホストから送信されるTCP通信の間隔から踏み台攻撃を検出する
- 今後の予定
  - 他のアプリケーションを起動させたときの解析
  - 閾値の決定
  - 踏み台ホストへの実装方法の検討