TCP の特徴を利用した踏み台攻撃の検出手法の検討

100430078　染川 敦
渡邊研究室

1. はじめに

クラッカーが目標のコンピュータに不正アクセスなどの攻撃をする際，ほとんどの場合は自分のコンピュータから直接ではなく，アカウントやパスワードを不正に入手して遠隔操作できる他のコンピュータを踏み台にして攻撃する．このような攻撃を踏み台ホストを介して実行されると，被害ホス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，踏み台攻撃時において攻撃ホストから踏み台ホストへはリモートログインパケットが，踏み台ホストから被害ホストに対しては 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検討する．

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さらに困難にする．しかし，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図 1 に示す．攻撃ホストは踏み台ホストを介して被害ホストにアクセスする．このとき，攻撃ホスト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被害ホス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．攻撃ホスト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，踏み台ホストから被害ホス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．

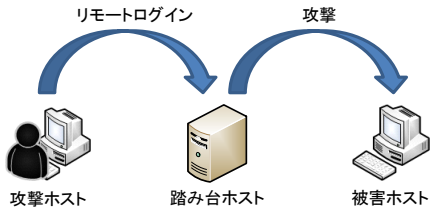


図 1: 踏み台攻撃のモデル

3. 検討方式

図 2 にリモートログインプロトコルの代表である telnet を例にして検討方式の原理を示す．まず攻撃ホストが踏み台ホストへリモートログインする．次に，攻撃ホストは踏み台ホストに対して被害ホストへのアクセスを行うためのコマンド（telnet[IP アドレス]）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，被害ホストに対して 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．踏み台ホストがリモートログインパケットを受信してから TCP コネクション確立要求のパケットを送信するまで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．

攻撃ホスト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，被害ホストに対する TCP コネクションを確立する SYN パケットを送信する．本検討はこの原理を利用したものである．

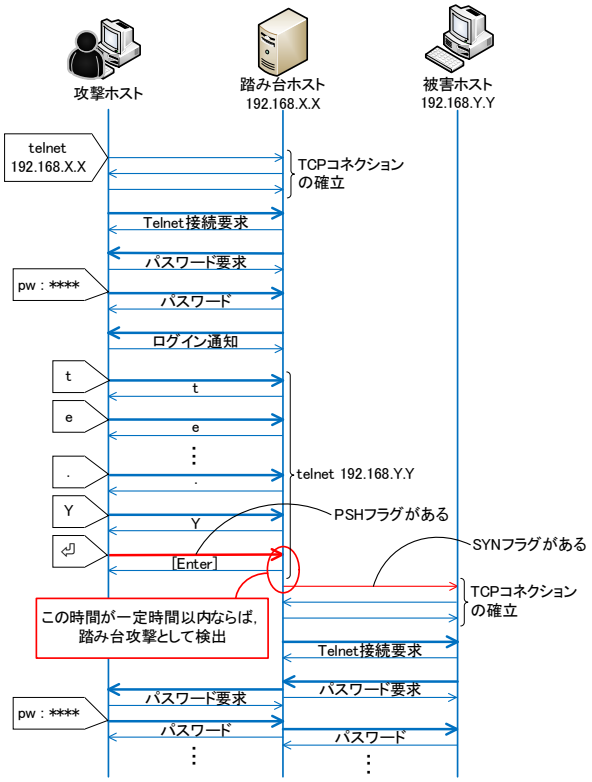


図 2: telnet による踏み台攻撃のシーケンス

4. むすび

攻撃ホストから踏み台ホストへのリモートログインパケットと，踏み台ホストから送信される被害ホストへの 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方法を検討した．今後は一定時間の閾値の検討と検討方式を実装する方法について考察する．

参考文献

[1] 竹尾大輔，他：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，情報処理学会論文誌，pp. 644-655 (2007).

TCPの特徴を利用した踏み台攻撃の検出手法の検討

名城大学　理工学部　情報工学科
渡邊研究室
100430078　染川敦

Watanabe Lab.

研究背景

不正アクセスの増加

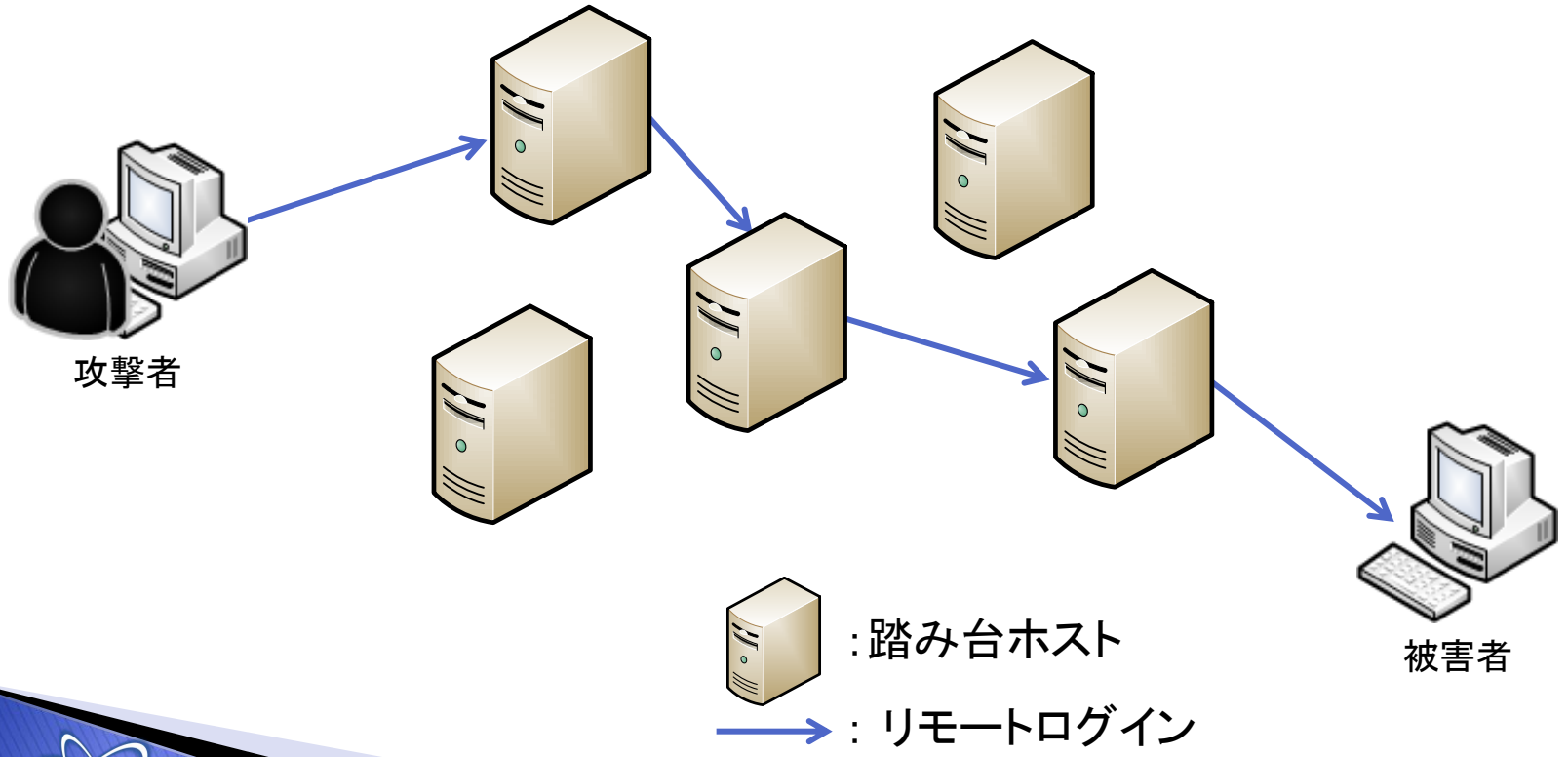
踏み台ホストを介して実行

踏み台ホストのユーザが
加害者になる可能性がある

Watanabe Lab.

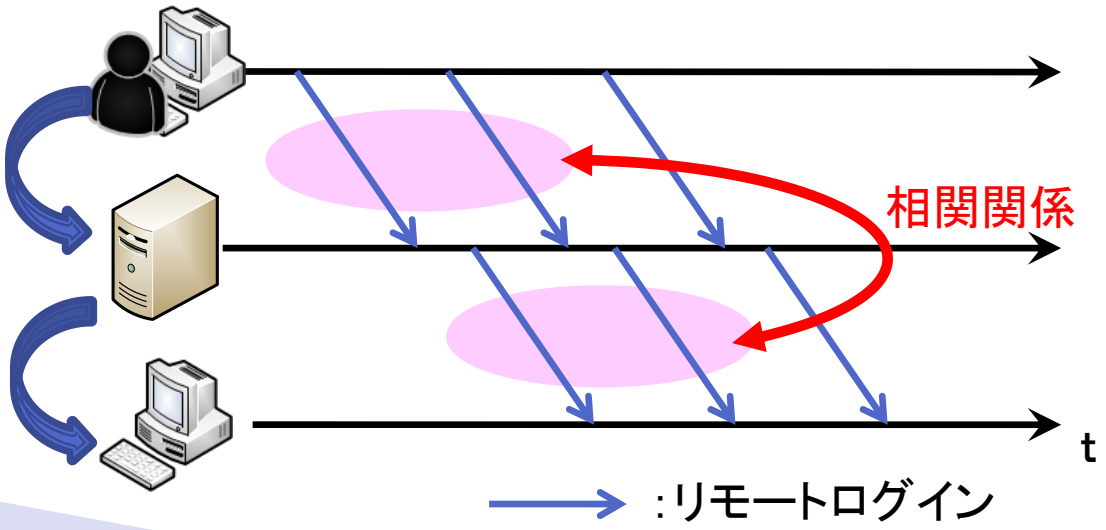
踏み台攻撃とは

何らかの方法（ウイルス，ソーシャルエンジニアリング等）で踏み台ホスト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．



既存研究

- コンテンツベース方式
  - 踏み台ホストの前後のパケットのデータ内容が一致していることに着目した手法
  - 暗号化されたパケットは検出不可
- タイミングベース方式
  - 踏み台ホストの前後のリモートログインに時間的な相関関係があることに着目した手法
  - 検出に数十秒必要



コネクションベース方式

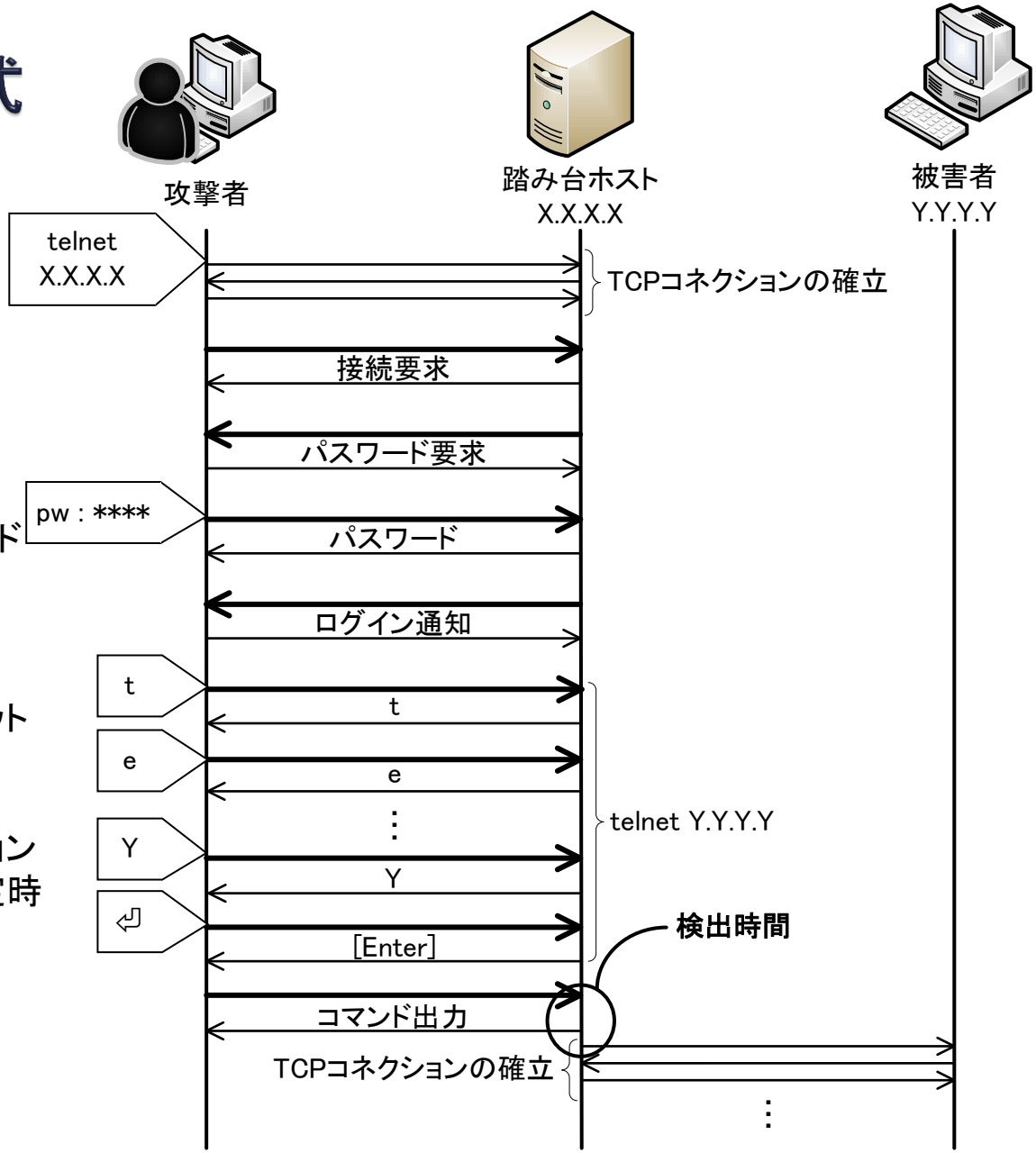
① 攻撃ホスト→踏み台ホスト
TCPコネクションの確立を行う

② 攻撃ホスト→踏み台ホスト
リモートログインする

③ 攻撃ホスト→踏み台ホスト
被害ホストにアクセスするためコマンドを送信

④ 踏み台ホスト→被害ホスト
TCPコネクションの確立要求のパケットを送信

コマンドの最後のパケットとTCPコネクションの確立要求のパケットの間の時間が一定時間以内であれば踏み台攻撃と判断する



コネクションベース方式

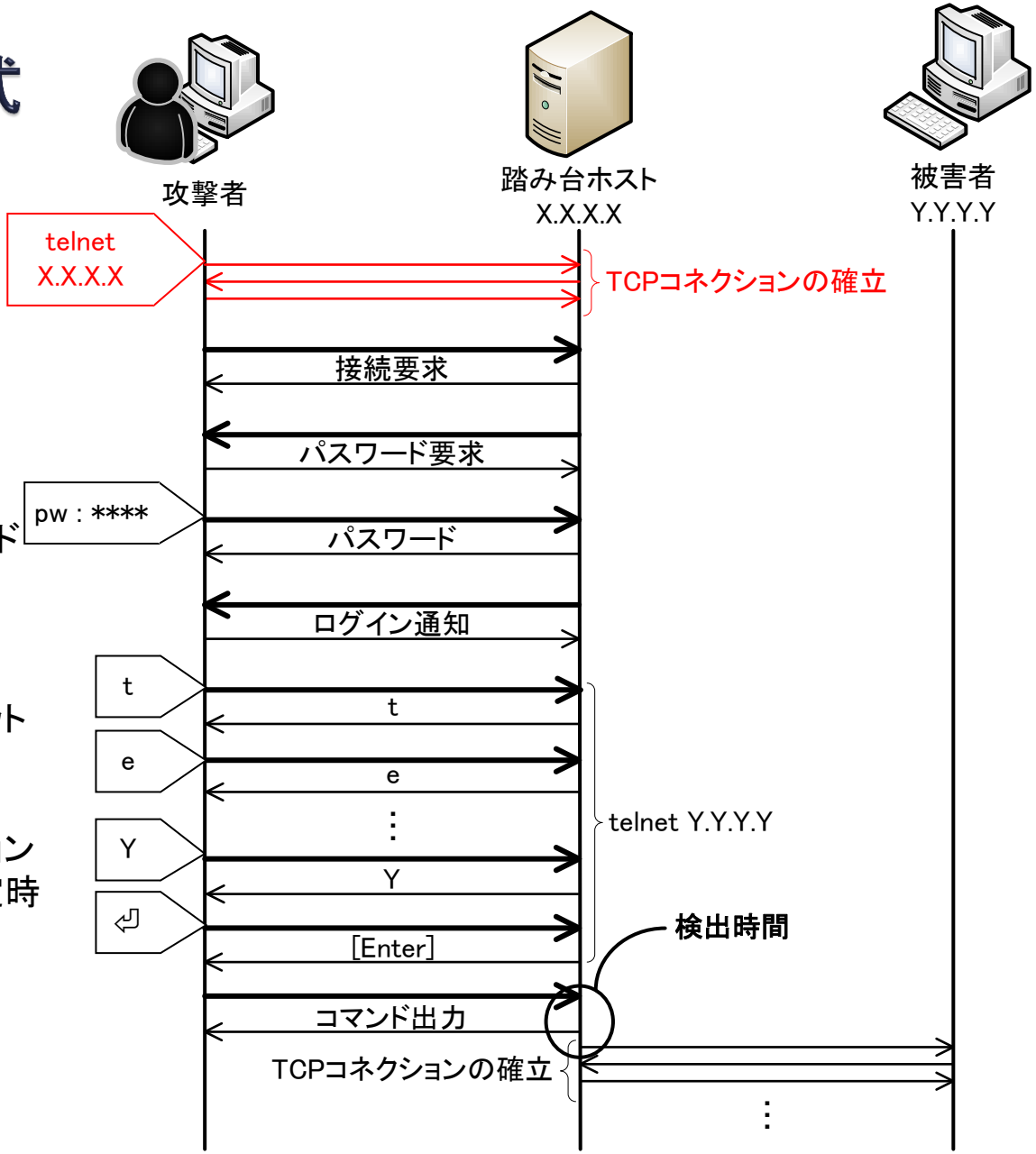
① 攻撃ホスト→踏み台ホスト
TCPコネクションの確立を行う

② 攻撃ホスト→踏み台ホスト
リモートログインする

③ 攻撃ホスト→踏み台ホスト
被害ホストにアクセスするためコマンドを送信

④ 踏み台ホスト→被害ホスト
TCPコネクションの確立要求のパケットを送信

コマンドの最後のパケットとTCPコネクションの確立要求のパケットの間の時間が一定時間以内であれば踏み台攻撃と判断する



コネクションベース方式

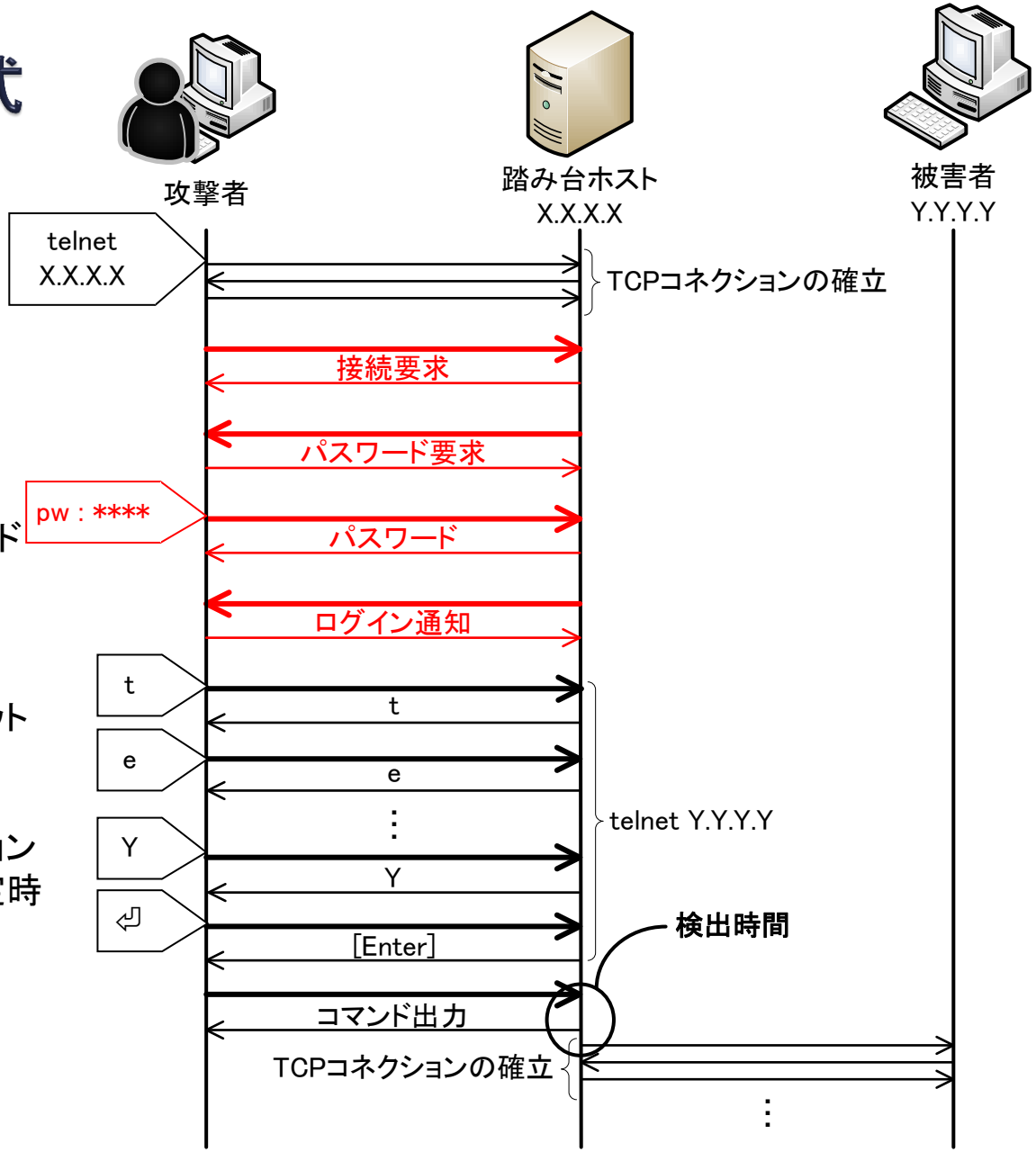
① 攻撃ホスト→踏み台ホスト
TCPコネクションの確立を行う

② 攻撃ホスト→踏み台ホスト
リモートログインする

③ 攻撃ホスト→踏み台ホスト
被害ホストにアクセスするためコマンドを送信

④ 踏み台ホスト→被害ホスト
TCPコネクションの確立要求のパケットを送信

コマンドの最後のパケットとTCPコネクションの確立要求のパケットの間の時間が一定時間以内であれば踏み台攻撃と判断する



コネクションベース方式

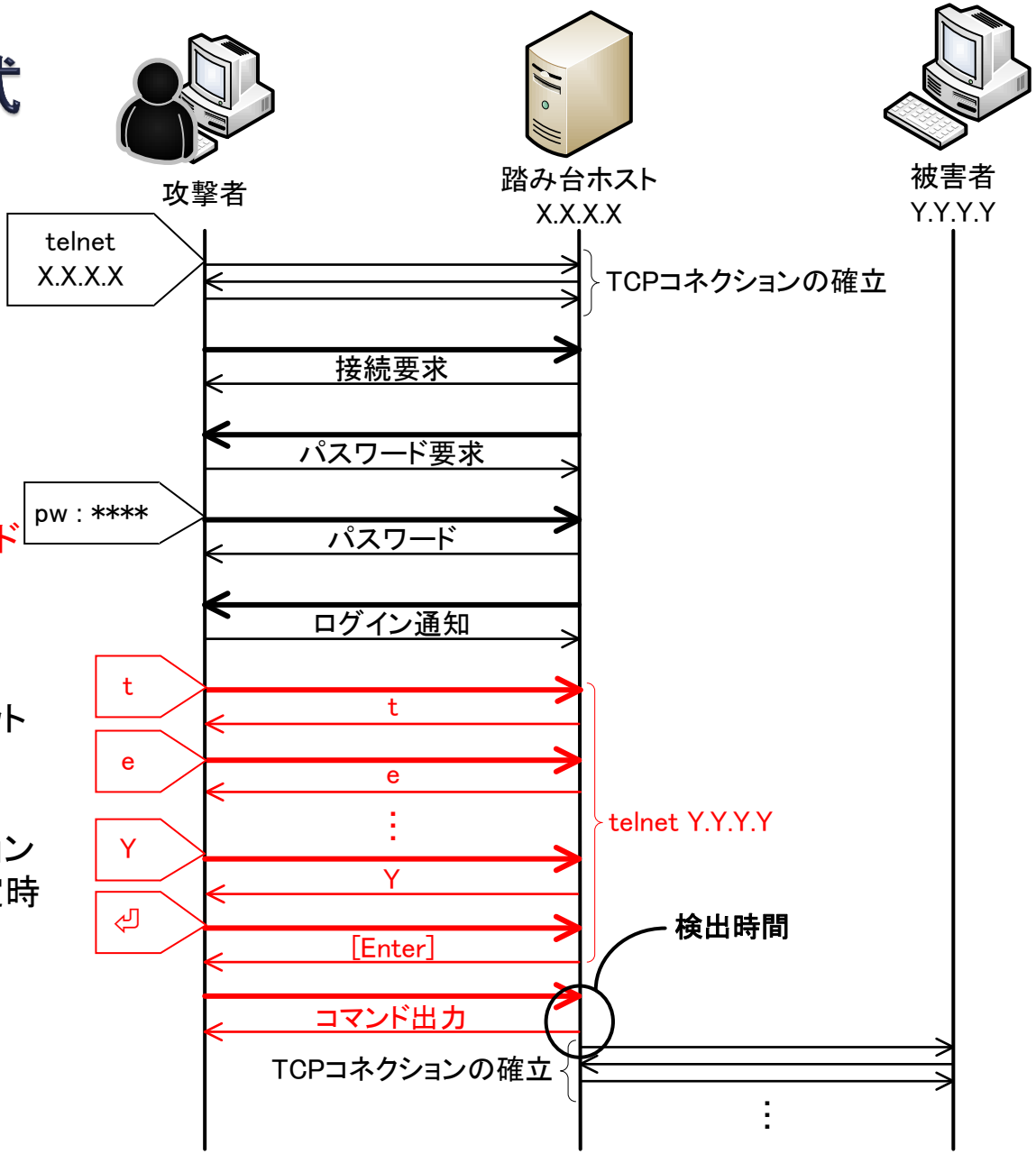
① 攻撃ホスト→踏み台ホスト
TCPコネクションの確立を行う

② 攻撃ホスト→踏み台ホスト
リモートログインする

③ 攻撃ホスト→踏み台ホスト
被害ホストにアクセスするためコマンドを送信

④ 踏み台ホスト→被害ホスト
TCPコネクションの確立要求のパケットを送信

コマンドの最後のパケットとTCPコネクションの確立要求のパケットの間の時間が一定時間以内であれば踏み台攻撃と判断する



コネクションベース方式

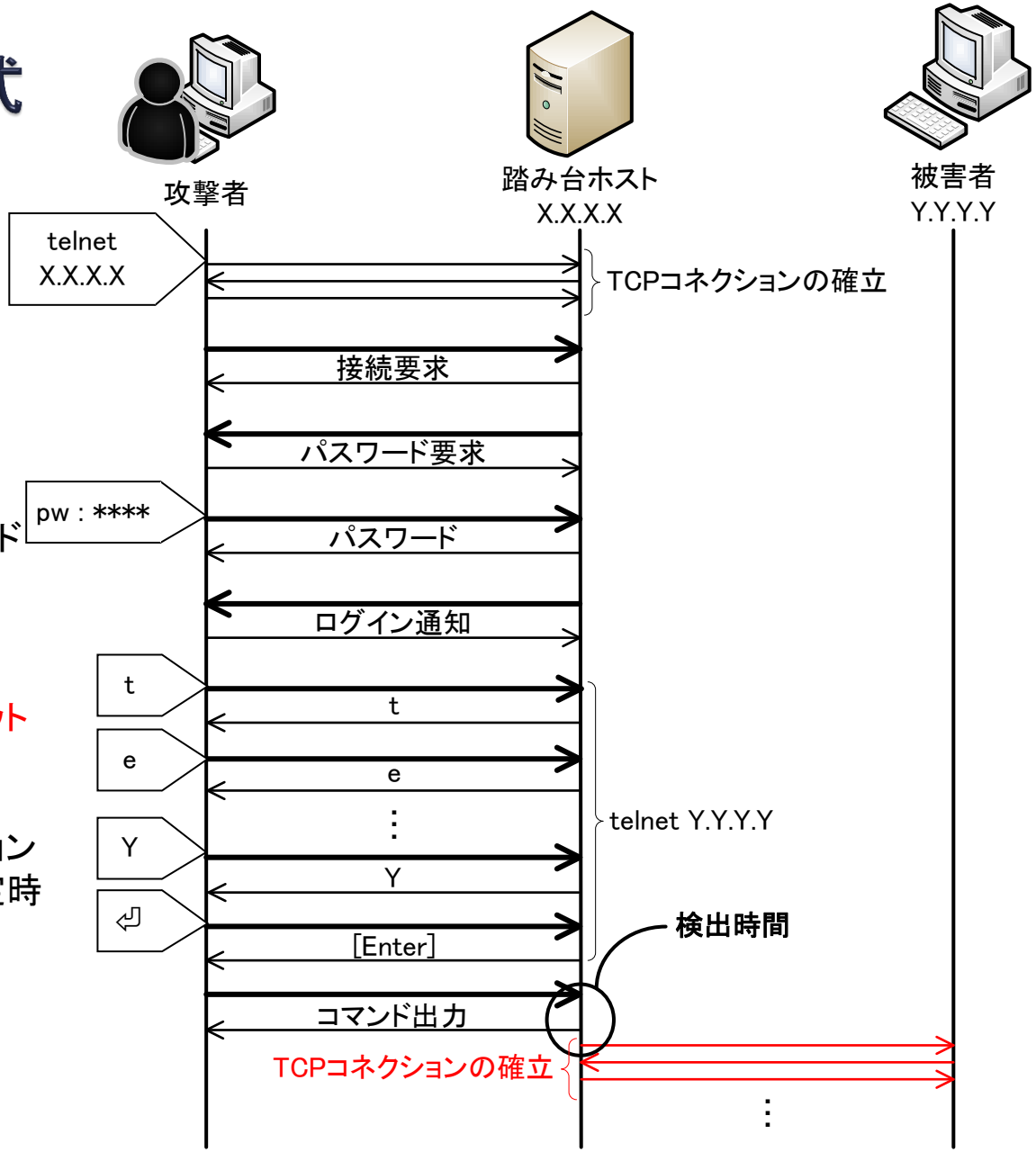
① 攻撃ホスト→踏み台ホスト
TCPコネクションの確立を行う

② 攻撃ホスト→踏み台ホスト
リモートログインする

③ 攻撃ホスト→踏み台ホスト
被害ホストにアクセスするためコマンドを送信

④ 踏み台ホスト→被害ホスト
TCPコネクションの確立要求のパケットを送信

コマンドの最後のパケットとTCPコネクションの確立要求のパケットの間の時間が一定時間以内であれば踏み台攻撃と判断する



コネクションベース方式

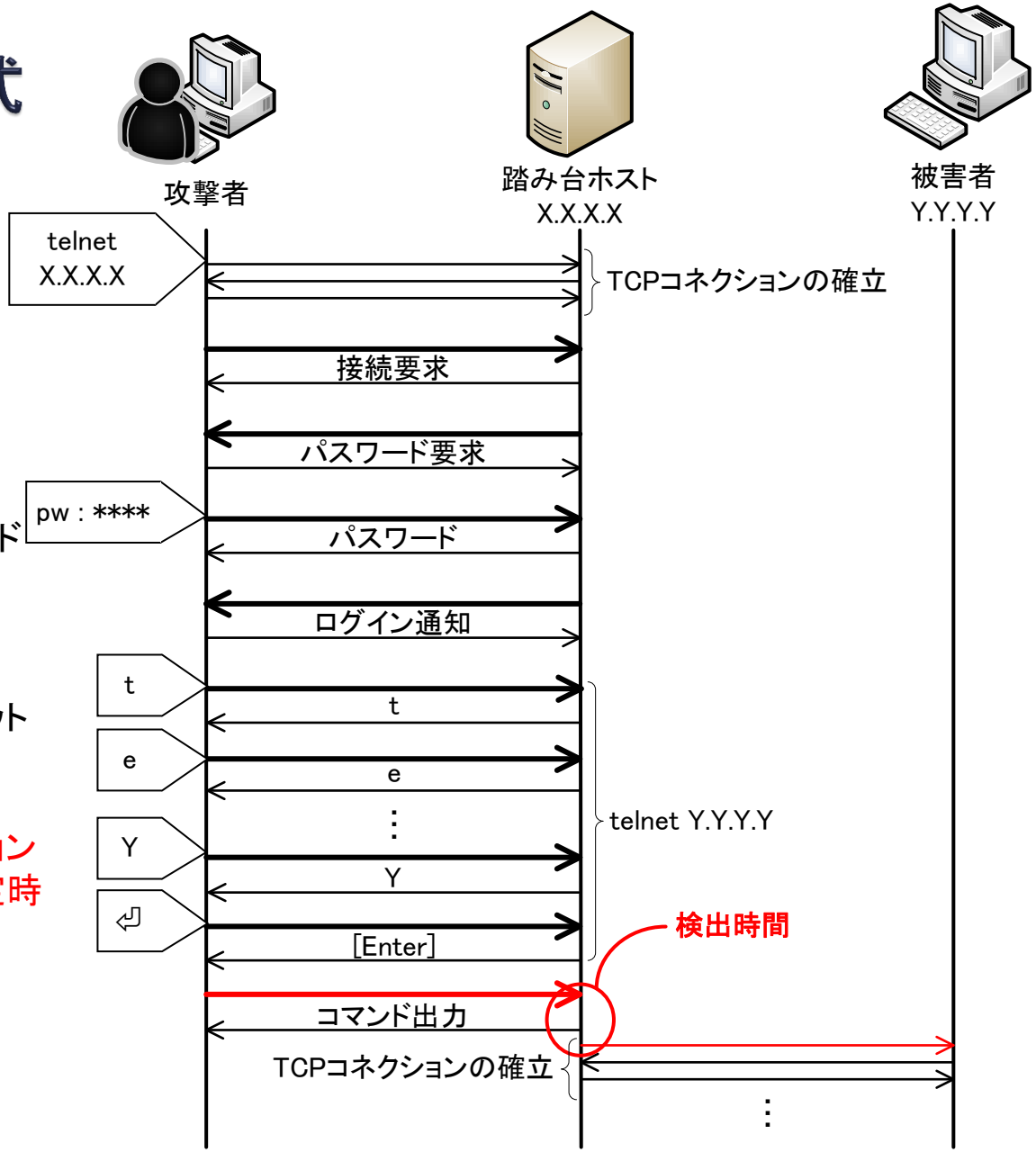
① 攻撃ホスト→踏み台ホスト
TCPコネクションの確立を行う

② 攻撃ホスト→踏み台ホスト
リモートログインする

③ 攻撃ホスト→踏み台ホスト
被害ホストにアクセスするためコマンドを送信

④ 踏み台ホスト→被害ホスト
TCPコネクションの確立要求のパケットを送信

コマンドの最後のパケットとTCPコネクションの確立要求のパケットの間の時間が一定時間以内であれば踏み台攻撃と判断する

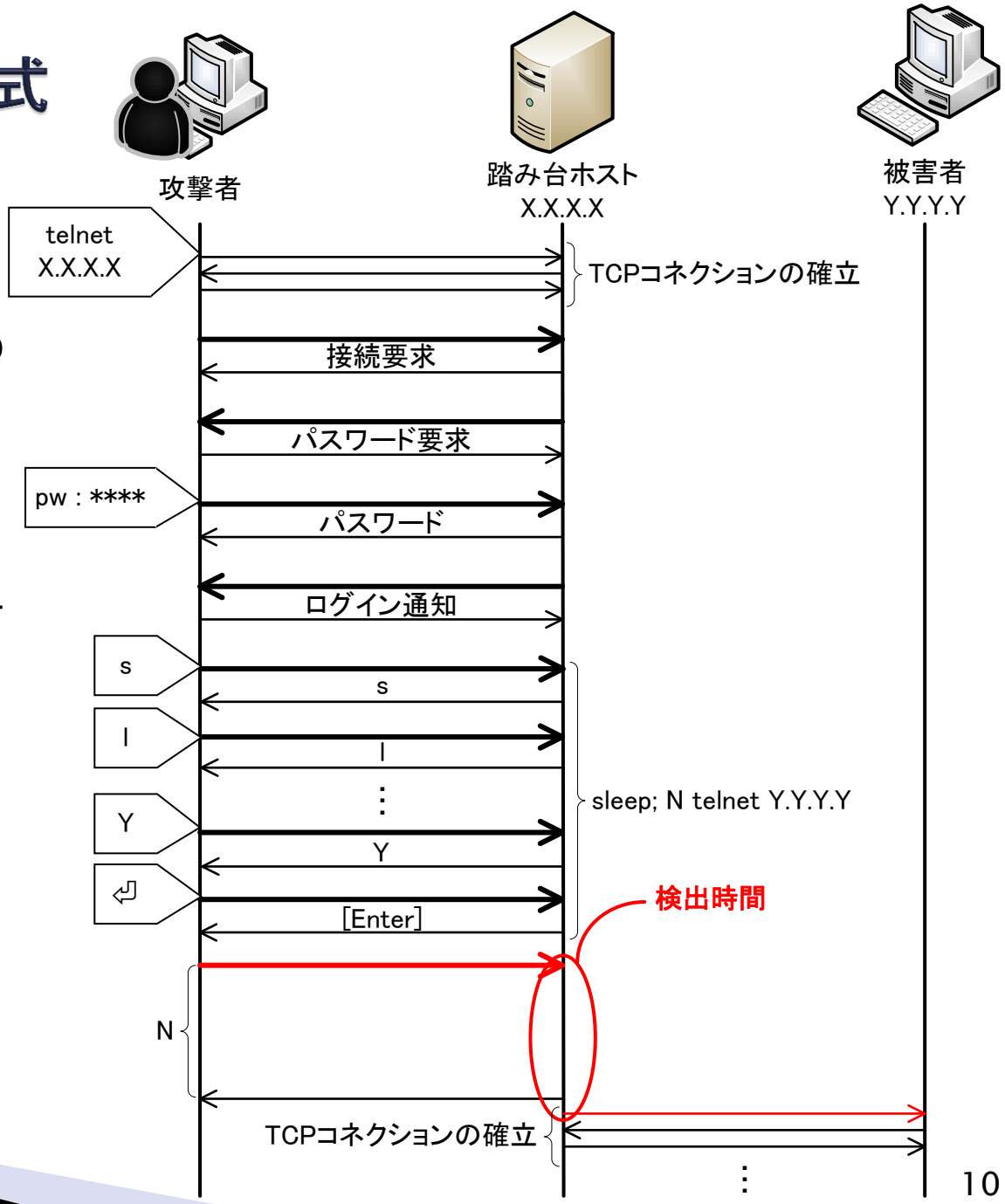


コネクションベース方式の課題

リアルタイムに検出できるが、sleepコマンドを用いた攻撃の場合は検出不可

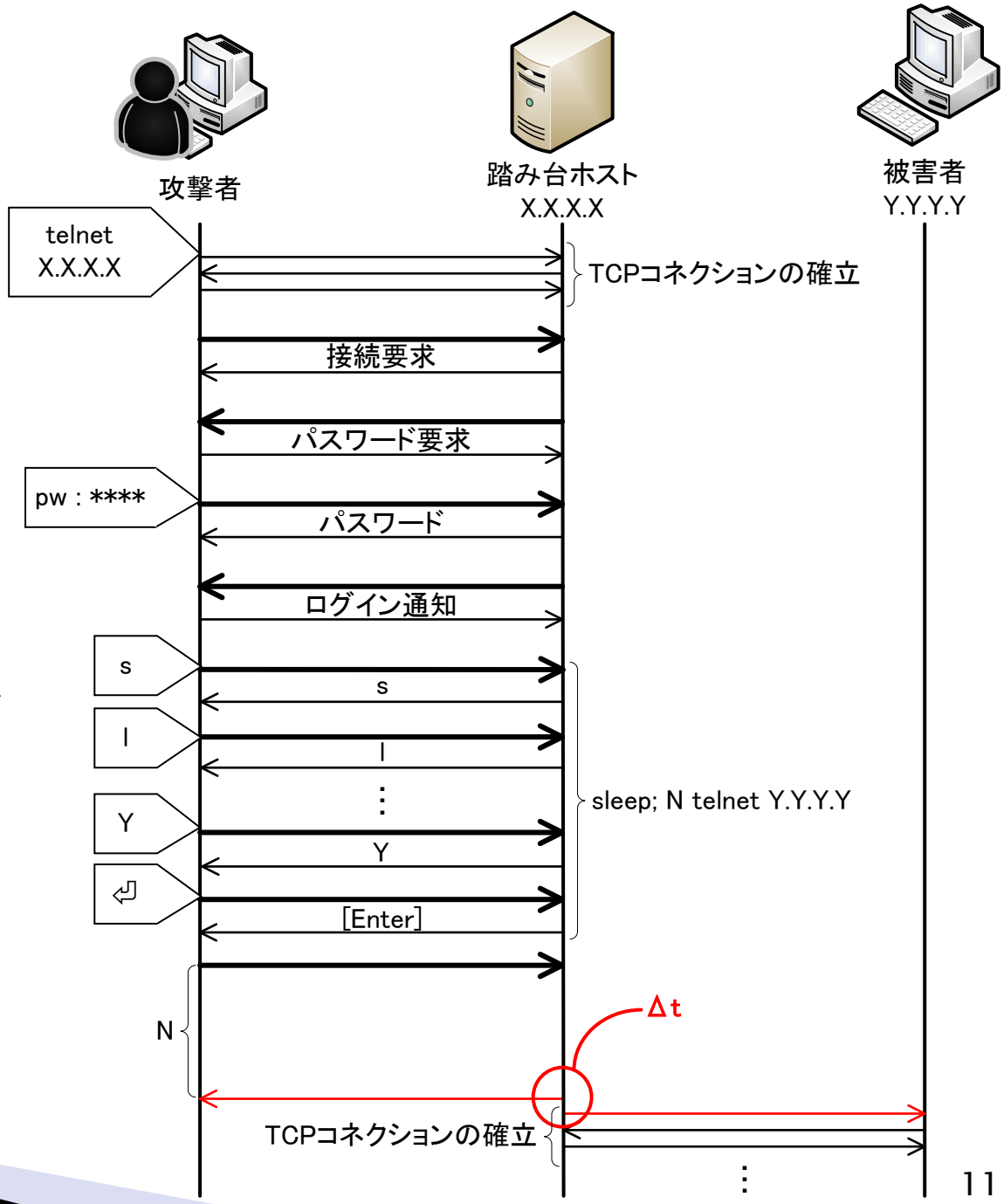
※sleepコマンド：

指定された時間、プロセスの実行を延期するコマンド



提案方式

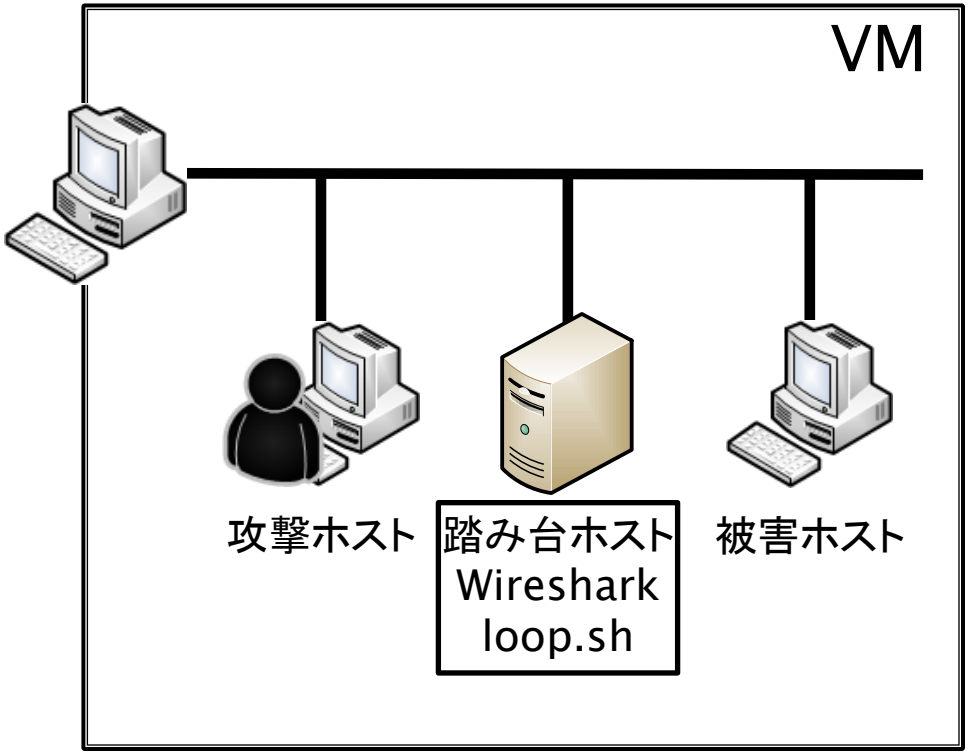
- 検出原理
  - 被害ホストへのTCPコネクションの確立要求の直前に踏み台ホストから攻撃ホストへのACKの返信があることに着目し、踏み台攻撃を検出
  - リモートログインのコマンドの送信にsleepコマンドを用いた場合も検出可能



測定方法

踏み台ホストのCPU使用率を変化させてΔtの測定を行った

- 測定条件
  - 仮想環境内で測定
  - リモートログインのプロトコルはtelnetを使用
  - Wiresharkでパケットを監視
  - CPU使用率は10%間隔で測定
  - 試行回数は10回

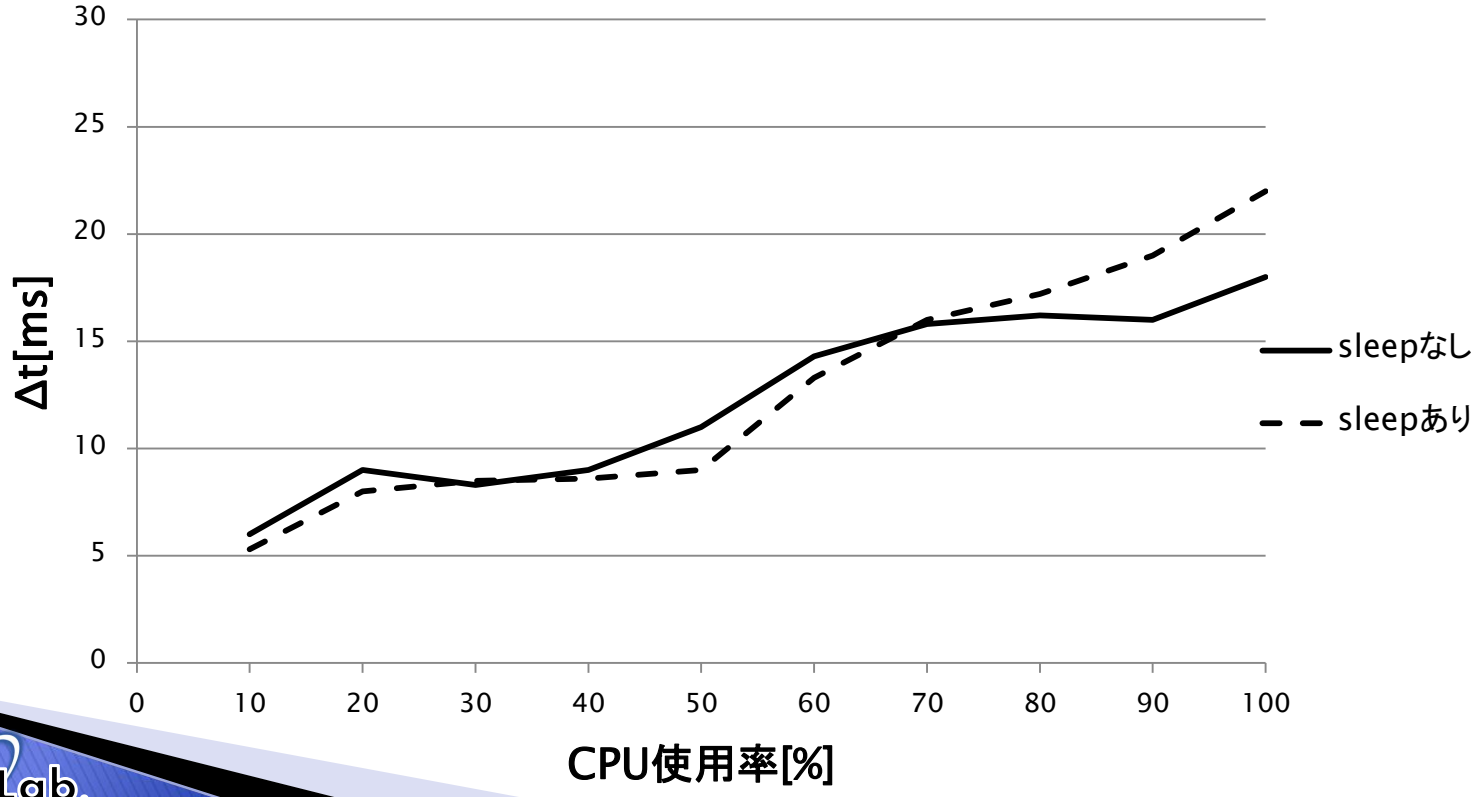


- CPU使用率の制御方法
  ① 無限ループするプログラムloop.shを起動
  ② コマンドcpulimitで上記のプログラムに使用するCPU使用率を制御

VMのホスト	
CPU	Core2 Quad (2.83GHz)
RAM	1GB
OS	Ubuntu12.10

測定結果

- ΔtとCPU使用率はほぼ比例
- sleepコマンドによる攻撃も通常時の攻撃と同様に検出可能
- CPUの状態に応じたΔtの閾値の検討が必要



まとめ

- 踏み台攻撃の検出原理
  - 踏み台ホストから攻撃ホストへのリモートログインのACKの送信と、踏み台ホストから被害ホストへのTCPコネクションの確立の間隔から踏み台攻撃を検出する
- 今後の予定
  - Δtの閾値の検討
  - 提案方式の実装方法の検討
  - 誤検知発生率の調査