平成25年度　卒業論文

邦文題目

TCPの特徴を利用した踏み台攻撃の検出手法の検討

英文題目

Researches on Detection Method of Stepping-stone Attacks Focusing on TCP Features

情報工学科　渡邊研究室

(学籍番号: 100430078)

染川　敦

提出日: 平成26年2月13日

名城大学理工学部

内容要旨

攻撃者が不正アクセスを含むサイバー攻撃を他のコンピュータに実行する時，攻撃者自身の身元の特定を困難にするため，複数の踏み台ホストを経由して攻撃を実行する．踏み台ホストを介して実行される攻撃は攻撃者の特定が困難なだけでなく，踏み台ホストの所有者が加害者とみなされる可能性があり問題視されている．本稿では，このような攻撃を検出するため，踏み台ホストから攻撃ホストへのリモートログインパケットの ACK の送信と踏み台ホストから被害ホストへの TCP コネクション確立要求のパケットの送信が一定時間以内に行われることに着目した．また，踏み台ホストの CPU 使用率を変化させて提案方式の評価を行った．

目 次

第1章　はじめに

インターネットの普及に伴いサイバー犯罪が問題となっている．近年のサイバー犯罪の中でも特に不正アクセスは増加傾向にある．攻撃者が目標のコンピュータに不正アクセスをする際，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を実行する．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．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．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．

従来の踏み台攻撃検出手法ではコンテンツベース方式やタイミングベース方式などがある．コンテンツベース方式は，踏み台ホストの前後のリモートログインパケットのデータ内容が一致していることを検出する手法である．しかし，この方式は SSH などの暗号化されたリモートログインプロトコルが使用されている場合は検出できない．タイミングベース方式はリモートログインのキーストロークの特徴に着目した検出手法であり，踏み台ホストの前後のリモートログインストロークに時間的な相関関係があることを検出する．この方式は暗号化されたリモートログインプロトコルが使用されている場合でも検出が可能だが，時間的な相関関係を検出に利用するため数十秒の検出時間がかかる．また，近年の研究では，ネットワークをモニタリングして通信をアクセス制御する手法 [1] や，仮想マシン (VM) 内において，VM のメモリ解析を行って取得したゲスト OS 内の情報を用い，踏み台攻撃を行っているプロセスからのパケットのみを破棄するパケットフィルタ xfilter [2] を設置する手法があり，ネットワークの形態に応じた様々な踏み台攻撃の対策が研究されている．

本稿の提案方式と類似する手法としてコネクションベース方式 [3] がある．コネクションベース方式は踏み台ホストに対するリモートログイン操作の終了と同期して踏み台ホストから被害ホストに対して TCP コネクションの確立要求があることに着目しており，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 パケットを監視して踏み台攻撃を検出する．この方式は暗号化されたリモートログインプロトコルを用いた踏み台攻撃をリアルタイムに検出することができる．しかし，攻撃者が UNIX のコマンドである sleep コマンドなどの方法で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 コネクションの確立要求の間の時間を意図的に長くするよう

な攻撃をした場合，検出できない可能性がある．

本稿では，踏み台攻撃時において踏み台ホストから攻撃ホストへはリモートログインパケットの ACK 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．

以降，2 章でコネクションベース方式について述べる．3 章では提案方式について説明し，4 章で評価を行う．そして，5 章でまとめを行う．

第2章　既存研究

2.1　コネクションベース方式の概要

前述のコネクションベース方式では，踏み台ホストが存在するネットワーク上に通信を監視する Detector を設置し，踏み台攻撃を検出する．図 2.1 にコネクションベース方式の原理を示す．

1. 攻撃ホストが踏み台ホストへ TCP コネクションの確立を行う．
2. 攻撃ホストは被害ホストへのアクセスを行うためのコマンドを踏み台ホストに投入する．
3. 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，被害ホストへ TCP コネクションの確立要求のパケットを送信する．
4. 踏み台ホストが被害ホストに対して TCP コネクションの確立を行う．
5. Detector 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 コネクションの確立されようとするのを監視する．
6. リモートログインパケットの受信と TCP コネクションの確立要求のパケットの送信との間の時間が一定時間以内であれば，Detector はこの状況を踏み台攻撃と判断する．

コネクションベース方式の特徴として，踏み台攻撃をリアルタイムに検出できるが，sleep コマンドを用いた場合，踏み台攻撃を検出できない．次節で sleep コマンドの概要について説明する．

2.2　sleep コマンドの概要

本稿における sleep コマンドとは，UNIX コマンドラインプログラムの sleep である．sleep コマンドは指定された時間プロセスの実行を延期するコマンドである．図 2.1 では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要求のパケットの送信が延期されてしまうため，踏み台攻撃を検出できなくなる．

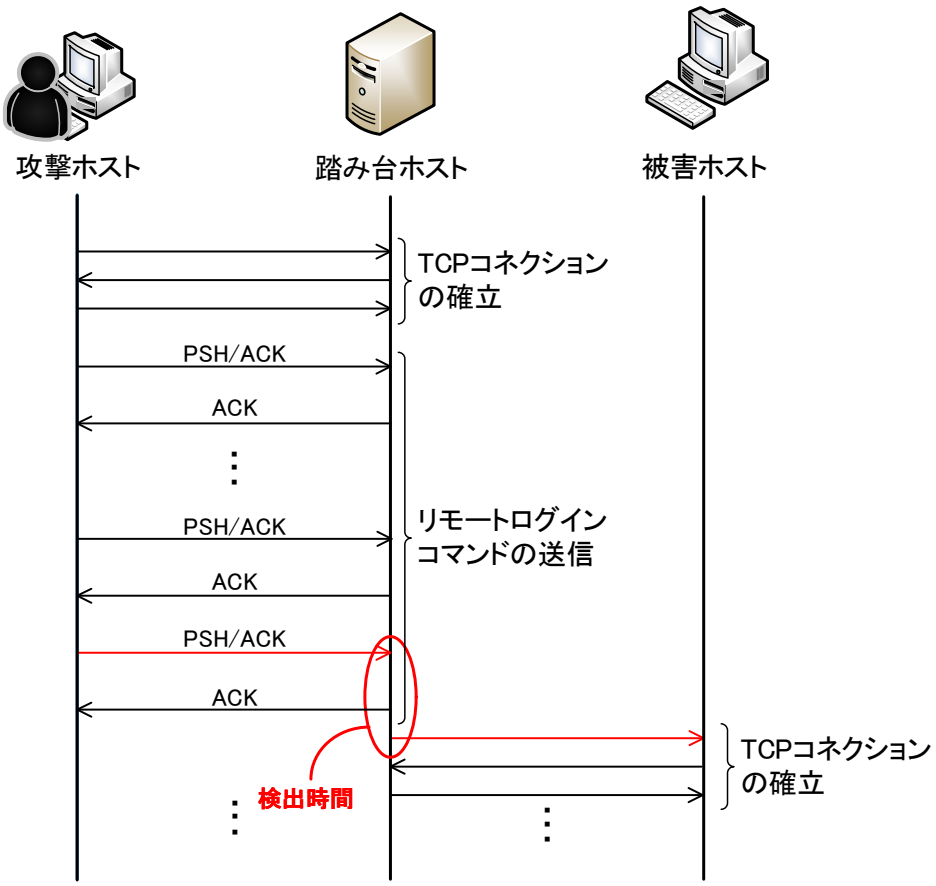

図 2.1　コネクションベース方式の原理

第3章　提案方式

3.1　提案方式の検出原理

攻撃ホストが踏み台ホストへリモートログインした後，そこから被害ホストに対してあらゆる TCP 通信があることを想定すると，踏み台攻撃発生時には必ず踏み台ホストから TCP コネクションの確立が必要である．また，その直前には TCP コネクションの確立要求の通信のトリガとなるコマンドを乗せたリモートログインパケットが送信され，被害ホストが受信すると被害ホストから踏み台ホストへそのパケットの ACK が送信されるはずである．提案方式では，踏み台ホストから攻撃ホストへのリモートログインパケットの 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要求のパケットの送信が一定時間以内に行われることを検出する．sleep コマンドを用いたリモートログインが行われた場合，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 コネクションの確立要求のパケットの間時間が長くなるが，リモートログインパケットの ACK の送信が TCP コネクションの確立要求のパケットが送信される直前にあるため，本稿の提案方式では sleep コマンドを用いた攻撃も検出することができる．

3.2　提案方式の検出手順

図 3.1 に提案方式のシーケンスを示す．

1. 攻撃ホスト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．
2. 攻撃ホストは被害ホストにアクセスを行うため，踏み台ホストへコマンドを送信するが，パケットの送信ごとに踏み台ホストから攻撃ホストへ ACK の送信がある．
3. コマンドの最後の文字の ACK が送信されると，踏み台ホストはコマンドを解読して，被害ホストへ TCP コネクションの確立要求のパケットを送信する．
4. コマンドの最後の文字の ACK と被害ホストへの 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ならば，踏み台攻撃と判断する．

また，この一定時間を Δt とする．

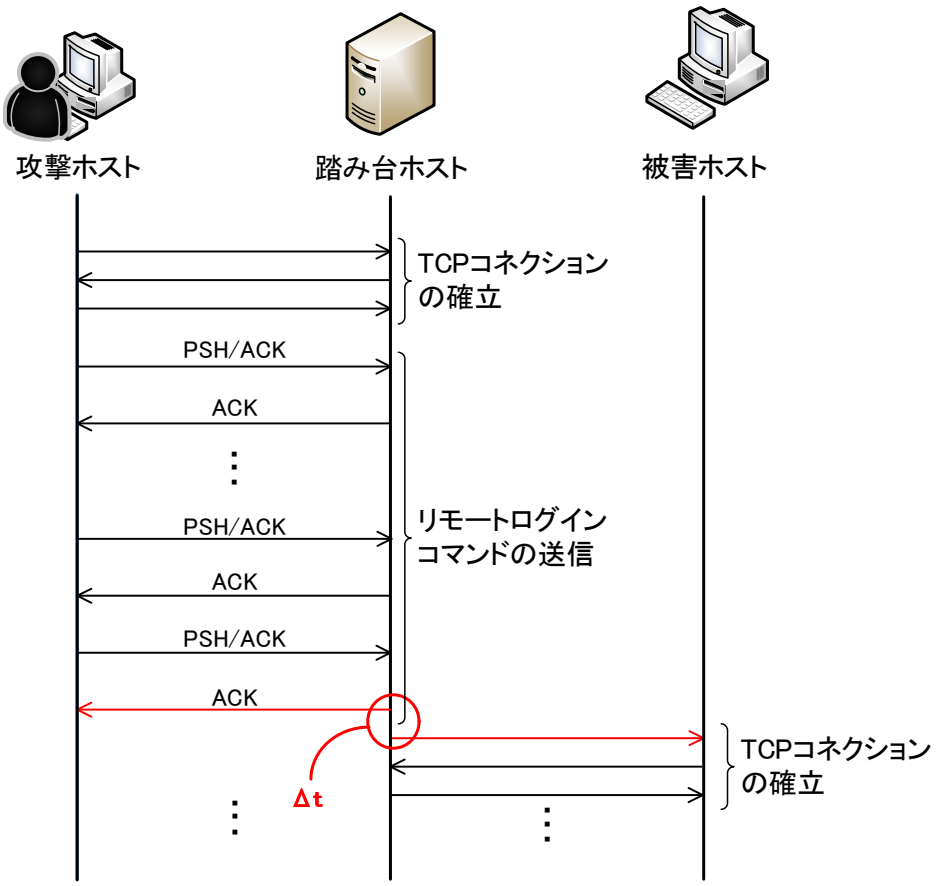

図 3.1　提案方式のシーケンス

第4章　評価

本稿の提案方式は踏み台ホストの CPU の状態によって Δt が変化する可能性があるため，検出時間の測定には，踏み台ホストの CPU 使用率を考慮する必要がある．測定に使用した踏み台ホストの仕様は表 4.1 であり，測定は仮想環境内で行った．また，リモートログインのプロトコルは telnet を使用し，CPU 使用率を変化させて評価を行った．図 4.1 に Δ t と CPU 使用率の関係を示した．

測定では，前述の sleep コマンドを用いた攻撃も通常の踏み台攻撃と同様に検出が可能であった．図 4.1 の Δt の値は 10 回試行した平均である．測定結果より，Δt と CPU 使用率は緩やかに比例していることがわかる．したがって，Δt の閾値は踏み台ホストの CPU 使用率の値を考慮に入れる必要があり，今後の検討課題である．

表 4.1　踏み台ホストの仕様

	踏み台ホスト
CPU	Core2 Quad (2.83GHz)
RAM	1GB
OS	ubuntu12.10

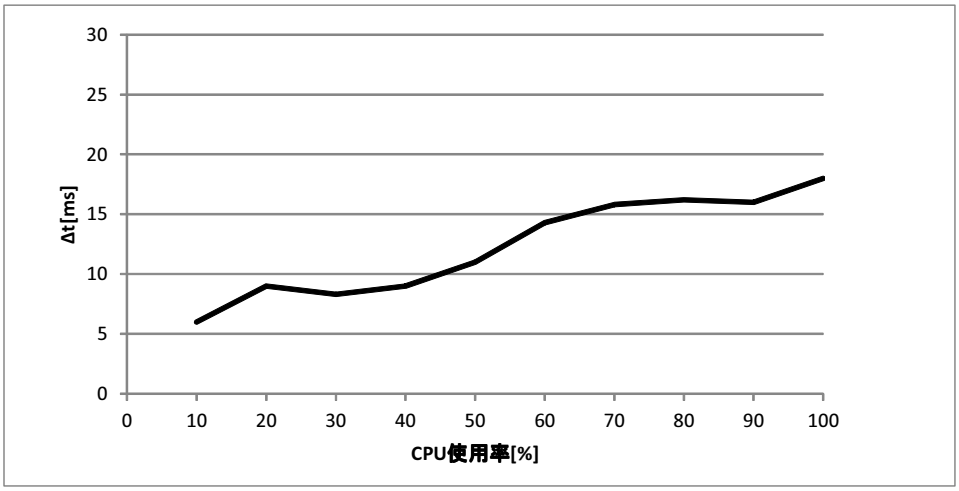

図 4.1　Δt と CPU 使用率の関係

第5章　まとめ

踏み台ホストから攻撃ホストへのリモートログインパケットの ACK の送信と，踏み台ホストから送信される被害ホストへの TCP コネクションの確立要求の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提案した．リモートログインのプロトコルである telnet を使用し，CPU 使用率を変化させて提案方式を評価した．今後は Δt の閾値の検討，提案方式の実装方法，誤検知発生率の調査を行う．

謝辞

本研究にあたり，多大なる御指導と御教授を受け賜りました，渡邊晃教授に心より感謝致します.

参考文献

[1] 安藤玲未，佐々木貴之，島　成佳，岡村利彦：踏み台攻撃防止のための通信状態ベースアクセス制御，コンピュータセキュリティシンポジウム 2013 論文集，pp.1018–1025(2013)

[2] 安積武志，光来健一，千葉　滋：踏み台攻撃だけを抑制できる VMM レベル・パケットフィルタ，情報処理学会論文誌，Vol.50，No.2，pp.1234–1241(2010)

[3] 竹尾大輔，伊藤将志，鈴木秀和，岡崎直宣，渡邊　晃：コネクションベース法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，Vol.48，No.2，pp.644–655(2007)

研究業績

学術論文

なし

研究会・大会等

1. 染川敦, 鈴木秀和, 渡邊晃, “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”, 平成 25 年度電気関係学会東海支部連合大会論文集, Sep.2013.