社団法人 電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE

FPN における渡り歩きの検出方法の検討

竹尾 大輔† 渡邊 晃‡

†‡名城大学大学院理工学研究科 〒468-8502 愛知県名古屋市天白区塩釜口 1-501

E-mail: †m0432028@ccmailg.meijo-u.ac.jp, ‡wtnbakr@ccmfs.meijo-u.ac.jp

あらまし 近年, イントラネット内部の不正アクセスが増加傾向にある. クラッカーが不正アクセスを行う場合, 多段の踏み台ホストを経由する“渡り歩き”を行っているケースが多い. 現在我々は, セキュリティ対策と運用管理負荷軽減を両立したシステムを実現する FPN(Flexible Private Network)の構築を目指している. FPN 環境下では, 異なるアクセスポリシを持つ各ユーザおよびホストが部署単位や役職単位でグループ化されており, 異なるグループ間の通信は拒否される. しかし, 複数のグループに帰属するホストを踏み台にすることで, 本来アクセスしてはならない別のグループのホストへアクセスできてしまう可能性がある. 本研究では, このような渡り歩きを検出する方法について検討する.

キーワード 渡り歩き, 不正アクセス, 侵入検知, ネットワークセキュリティ, FPN

Researches on Detection Method of Island Hop in Flexible Private Network

Daisuke TAKEO† and Akira WATANABE‡

†‡Graduate School of Science and Technology, Meijo University

1-501 Shiogamaguchi, Tenpaku-ku, Nagoya-shi, Aichi, 468-8502 Japan

E-mail: †m0432028@ccmailg.meijo-u.ac.jp, ‡wtnbakr@ccmfs.meijo-u.ac.jp

Abstract In recent years, illegal access inside intranet is increasing. When crackers access the target host illegally, they usually hop through many hosts witch we call it "Island Hop". We have been developing FPN (Flexible Private Network) which realizes secure and simple management systems. Under the FPN environment, each user having different access policies are grouped according to their post or their jobs, and the communication between different groups is refused. However, the user can access to the host of different groups using Island Hop technology. In this paper, we examine how to detect such Island Hop.

Keyword Island Hop, Illegal Access, Intrusion Detection, Network Security, Flexible Private Network

1. はじめに

近年, 企業などのイントラネット内部の不正アクセスが増加傾向にあり[1], 企業情報が流出するなどの内部犯罪による事件が発生している. 外部からの不正アクセスや攻撃に対してはファイアウォールなどの機器を導入したり, ホストの要塞化を行うことでセキュリティ対策を取っているが, イントラネット内部のセキュリティ対策はあまり取られていないのが現状である.

ネットワーク上の不正アクセスを発見するシステムとして, IDS（Intrusion Detection System；侵入検知システム）がある. IDS とは, ネットワークを流れる通信やホストに対するアクションを監視し, 不正なアクセスを検知するシステムのことである. 侵入検知を行うと, システムに対する攻撃を監視・記録して存在する脅威の程度を確認でき, 得られた記録を分析することでセキュリティポリシやシステムの設定を見直すことができる. それにより被害の発生の防止や軽減を図ることができ, ユーザに監視システムの存在を知らしめて不正行為を抑制することもできる.

しかしながら, セキュリティ対策技術を導入していてもクラッカーは不正アクセスを試みる. 一般にクラッカーが不正アクセスを行う場合, 多段の踏み台ホストを経由する“渡り歩き”（Island Hop）を行っているケースが多く見られる. 渡り歩きは主にリモートログインなどの TCP サービスが用いられる場合が多い. 個々のリモートログインが正常なものである場合, IDS ではそれ自体を不正と見なすことは難しい. また, 管理者が管理目的で渡り歩きを行っているのか, クラッカーが不正な渡り歩きをおこなっているのか, 判断

材料が無いためにこれらを区別することも難しい．

現在我々は，イントラネット内のセキュリティ対策と運用管理負荷の軽減を両立したシステムを実現するFPN(Flexible Private Network)の構築を目指している[3]-[7]．FPN 環境下では，異なるアクセスポリシを持つ各ユーザおよびホストが部署単位や役職単位でグループ化されており，異なるグループに跨ったホスト間通信は拒否することができる．しかし現状では，複数のグループに帰属するホストを踏み台にすることで，本来アクセスしてはならない別のグループのホストへアクセスできてしまう可能性がある．この問題を解決するには，渡り歩き自体を検出することと，渡り歩きが正常であるか不正であるかを判断することが求められる．

著者らは，FPN 環境下での渡り歩きを検出する方法についてこれまで提案してきたが[4],[8]，本研究では，従来の提案方式の課題であった，FPN 環境に依存しない普遍的な渡り歩き検出方法の検討を行う．そして新旧提案方式の比較から渡り歩き検出機能の評価を行う．

以降，2 章で渡り歩きを検出する条件を述べ，本研究で提案する渡り歩き検出方法の概要を説明する．3 章では渡り歩き検出機能の実装方法について述べ，4 章でその評価を行う．そして最後に 5 章でまとめる．

2. 渡り歩き検出方法

本章では，まず 2.1 節で本研究で想定する渡り歩きモデルを定義し，2.2 節では従来の提案方式の概要を，2.3 節では本研究で提案する渡り歩き検出方法の基本原理を説明する．

2.1. 渡り歩きモデル

本研究で想定する渡り歩きモデルのネットワーク構成を**図 1** に示す．渡り歩きモデルの構成要素として，Attacker，Foot Hold，Target がある．Attacker（攻撃者ホスト）は渡り歩きを行うホストである．Foot Hold（踏み台ホスト）は Attacker がリモートログインするホストである．Target（ターゲットホスト）は Attacker が Foot Hold を介して最終的にアクセスするホストである．各ホストは LAN によって接続されており，Attacker はクライアント型のホスト，Foot Hold と Target はサーバ型のホストを想定している．このとき Attacker が Foot Hold を介して Target にアクセスすることを，渡り歩きと定義する．

2.2. データー致方式の概要

従来の提案方式（以下，データー致方式と呼ぶ）では，Telnet による渡り歩きを想定している（**図 2**）．Telnet による渡り歩きでは，Telnet パケットがネットワーク上を流れることになるが，図 2 の Attacker が，送信元が Attacker，宛先が Foot Hold の Telnet パケットを送信する場合を考える．このパケットを Foot Hold が受信すると，Foot Hold では送信元が Foot Hold，宛先が Target，データは受信パケットと同一の Telnet パケットが生成され，Target へと送信される．このデーター致方式では，IP アドレスは異なるが，データは同じである送受信パケットが踏み台となるホストでほぼ同時に発生していることに着目し，踏み台となる可能性のあるホスト自身，或いはその直前に設置される機器において送受信パケットを監視することで渡り歩きを検出する．

データー致方式には 3 つの大きな問題が存在する．

① 渡り歩きが検出できるのは，Attacker・Foot Hold 間で TCP コネクションが確立された後である．これは不正な渡り歩きを検出する場合に，不正なコネクションが確立されてからでないと検出できないことを意味している．

② 短い間に送受信される Telnet パケットのデータを比較することで渡り歩きを検出しようとしているため，リモートログインとして，通信が平文で行われる Telnet に限定しているが，SSH などの暗号化されたリモートログインを用いられると渡り歩きの検出はできない．

③ Foot Hold・Target 間の通信が FTP であるなど，リモートログイン以外を用いられると渡り歩きを検出できない．

以上のことを踏まえ，次節で今回検討する渡り歩き検出方法の基本原理を説明していく．

2.3. 基 本 原 理

データー致方式では，連鎖状に Telnet によるリモートログインを行う渡り歩きを想定したが，Attacker か

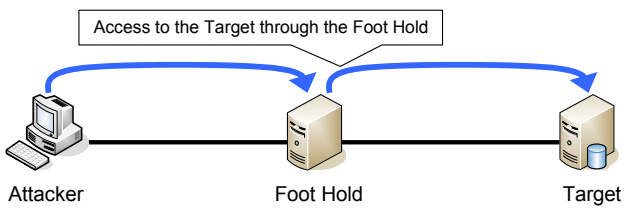


図 1　渡り歩きモデル
Fig.1　Model of Island Hop.

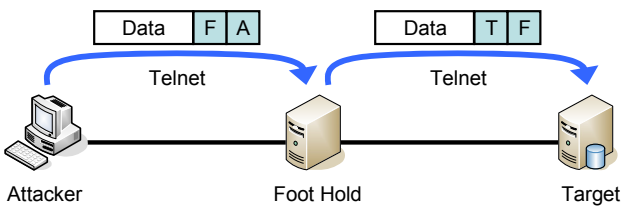


図 2　従来の提案方式
Fig.2　Conventional proposed method.

ら（Target の直前の）Foot Hold まではリモートログインでアクセスし，そこから Target へはリモートログインだけでなく FTP などのサービスを利用することも考えられるため，Attacker・Foot Hold 間の通信はリモートログインによるもの，Foot Hold・Target 間の通信はあらゆる TCP サービスによるものがあり得る．本方式は，Attacker が Foot Hold へとリモートログインしており，そこから Target へとリモートログインを含めた各種 TCP サービスでアクセスするという状況を想定し，これを Foot Hold 上で検出するものである．この方式をコネクション検出方式と呼ぶことにする．

既に Attacker と Foot Hold の間でリモートログインのコネクションが確立している状態で，Foot Hold がリモートログインの通信パケットを受信した後の極短い間に Foot Hold から Target にコネクション確立要求を送信する場合，Attacker がリモートログインを用いて Foot Hold に TCP サービスを起動するコマンドを送信した可能性があり，渡り歩きの可能性があると言える（**図 3**）．しかしこの状況に加えて，コネクション確立要求が送信される直前にキーボードのエンターキープレスイベントやマウスの左ボタンクリックイベントが発生していた場合，管理者が Foot Hold を直接操作して通信を行おうとしている可能性があり，渡り歩きの可能性は低い．

この基本原理に従い，渡り歩き検出に必要な 3 つの処理を個別に説明する．

● パケット受信処理の監視

Foot Hold が受信する TCP パケットを監視し，Telnet や SSH，rlogin などのリモートログインの通信パケットを検出する．検出した時刻をリモートログイン受信記録として保存していく（**図 4**）．

基本的に検出対象は PSH パケットである．なぜなら，リモートログインの通信パケットはローカルホストで入力された 1 文字分のデータであり，受信したらすぐにアプリケーションに渡す必要があるために，PSH フラグがセットされているからである．また，例えばここでリモートログインの SYN パケットを受信したとしても，それは Attacker から Foot Hold へのリモートログイン自体のコネクション確立要求であるので，この SYN パケット受信直後に渡り歩きに至ることはない．しかしリモートログインのコネクションを管理する目的で SYN，FIN パケットを監視することは有用である．

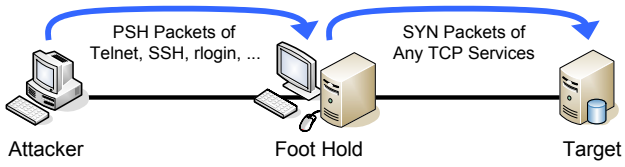


図 3　監視対象
Fig.3　Target for observation.

本提案ではリモートログインの通信パケットのデータを参照しないため，監視対象を Telnet 以外にも広げることができ，データ一致方式の問題点②が解決できる．

● パケット送信処理の監視

Foot Hold が送信する TCP パケットを監視し，あらゆる TCP サービスの通信パケットを検出する．パケット送信時にリモートログイン受信記録を参照し，現在時刻と比較し，一定時間内に送信が行われていれば，渡り歩きと判断する．しかし，後述するキー入力記録を参照してキー入力から一定時間内であれば，つまりキー入力と PSH パケット受信の両方のイベントが発生していた場合は渡り歩きではないと判断する（**図 5**）．

送信処理の場合，検出対象は SYN パケットのみでよい．なぜなら，Attacker からのコマンドを受けて Foot Hold が TCP サービスを起動して Target と通信する場合，必ず初めにコネクション確立要求を送信するので，これを検出すればよいからである．また，宛先 IP アドレスが Attacker である送信パケットは対象としない．Attacker が Foot Hold を介して自分自身にアクセスしたとしても，それは渡り歩きではないからである．

SYN パケットを検出することで，データ一致方式の問題点①が解決できる．そしてあらゆる TCP サービスを検出対象とすることで，データ一致方式の問題点③が解決できる．

● キーボード・マウス入力の監視

Foot Hold のキーボードとマウスを監視し，キーとクリックの入力を検出する．検出した時刻をキー入力記録として保存していく（**図 6**）．

検出対象はキーボードのエンターキーとマウスの左クリックとする．管理者がアプリケーションを用いて通信を行う場合，これらの入力が通信開始のトリガーとなる可能性が高いからである．渡り歩きの可能性がある通信パターンが発生していても，この場合の通信を除外することで渡り歩きの誤検知を減らせることが期待できる（しかしながら Foot Hold はサーバを想定しているため，管理者を含めたユーザが Foot Hold を直接操作するという状況はクライアントに比べて少ないだろう）．

上記のように，各処理は簡単な条件分岐をするだけであり，フローチャートの条件分岐の条件を満たさなかった段階で処理は終了する．

図 7 に本方式の処理の流れを示す．まず Attacker が Foot Hold へリモートログインするためにコネクションの確立を行う．このときやり取りされるパケットは

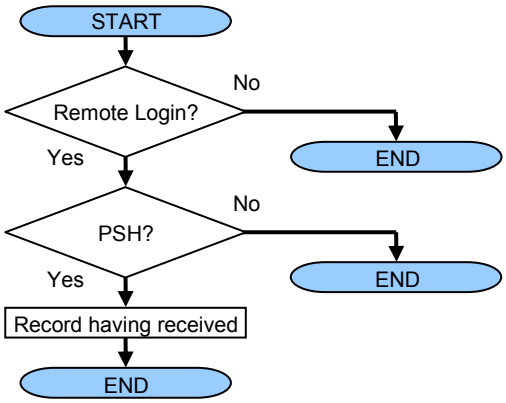


図４　パケット受信処理監視フローチャート
Fig.4　Flow chart of packet receive process.

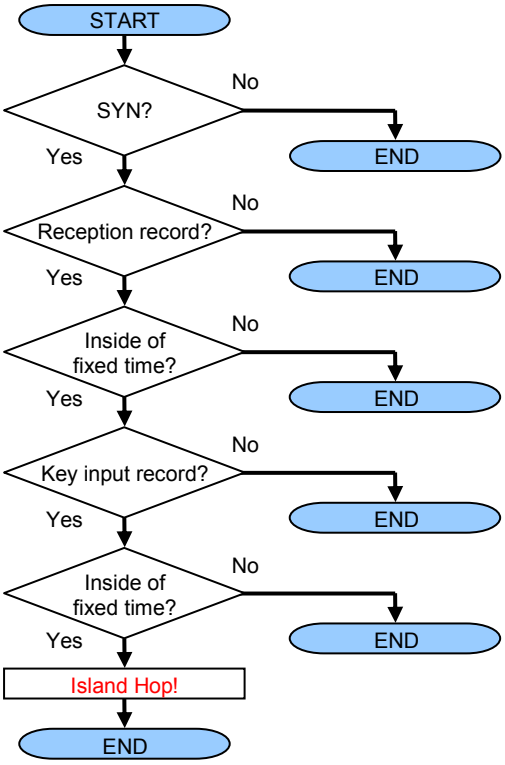


図５　パケット送信処理監視フローチャート
Fig.5　Flow chart of packet send process.

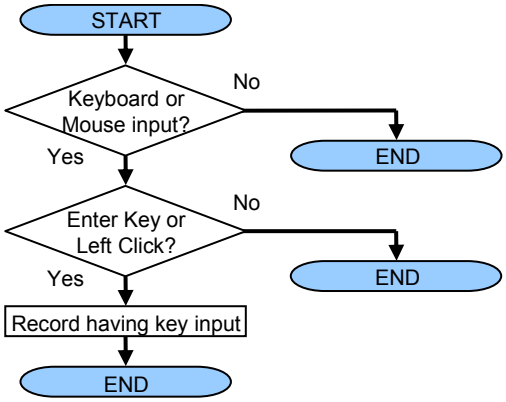


図６　キーボード・マウス入力監視処理フローチャート
Fig.6　Flow chart of keyboard and mouse input.

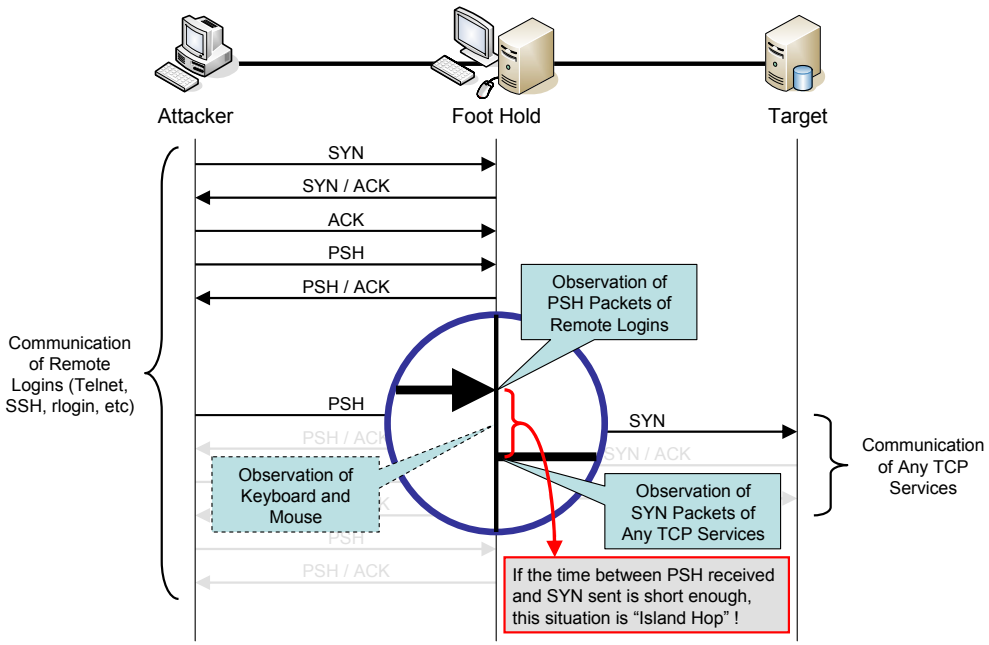


図７　渡り歩き検出の流れ
Fig.7　Flow of Island Hop detection.

監視対象ではない．その後のリモートログイン通信の監視を行いつつ，Foot Hold から新たな TCP コネクションが確立しようとするのを監視する．リモートログイン通信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十分短ければ，この状況は“渡り歩き”である．

3. 渡り歩き検出機能の実装

本章では提案方式の実装方法について述べる．3.1 節ではデーター致方式の実装をまず述べる．3.2 節では具体的な実装方法について述べる．

3.1. データー致方式の実装

データー致方式の実装に関しては，FreeBSD において BPF（BSD Packet Filter）というインタフェースを用いた動作検証用プログラムを開発している．BPF とは，データリンク層へ直接アクセスできるインタフェースのことで，FreeBSD に標準搭載されている．このプログラムにより，Telnet のみを用いた渡り歩きを検出できることを確認している．本来は後述の新提案方式と同様に OS に組み込むことを想定していた．

3.2. 実 装 方 法

コネクション検出方式を実現するためには，送受信パケットの監視とキーボード・マウス入力の監視を行う必要がある．送受信パケットの監視は libpcap などのライブラリ，あるいは前述の BPF を使用してキャプチャすることで可能であるが，キーボード・マウス入力のリアルタイムな監視，及びパケット監視との連携をアプリケーションレベルで行うのは困難である．よって本方式は OS のカーネルに組み込むことで実現することにする．これにより送受信パケットとキーボード・マウス入力の監視を完全にリアルタイムに監視でき，イベントを取りこぼすこともなく，それぞれのイベントが発生した時刻の正確な差を計測することが可能となる．また本方式はホスト上に実装するため，ホスト型 IDS の形式を取っているが，カーネル内部で直接パケットを扱えるため，インライン型 IDS のように渡り歩き検出時にパケットを破棄するなどの操作も可能である．

次に実装箇所を示す．まず送受信パケットの監視は IP 層で行う．本方式はパケットの TCP ヘッダ（宛先ポート番号フィールド，コントロールフラグフィールド）を参照するため，トランスポート層でパケットを監視することも考えられるが，Attacker や Target の特定のために送信元 IP アドレスと宛先 IP アドレスも監視するべきであるので，IP 層を選んだ（**図 8**）．キーボード・マウスの監視は，キー状態が入力デバイスからカーネルへ通知される箇所で行う．

実装する OS は，オープンソースであり，IP 層の処理を含めたネットワークコードに関する資料が多い FreeBSD を選んだ．本方式の主要な処理ごとにモジュール化し，それぞれ適当な箇所で呼び出されるようにする．

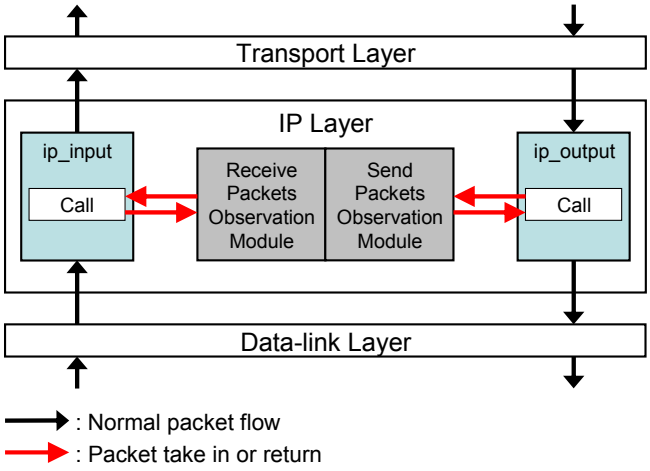


図 8　送受信パケットの監視位置
Fig.8　Observation points of send and receive packets.

4. 機 能 評 価

現段階では実装および動作実験ができていないため，ここではデーター致方式とコネクション検出方式を比較して理論的な部分の評価を行う．

4.1. 評 価 条 件

両方式それぞれの機能，利点・欠点を評価項目とし，比較表からコネクション検出方式で期待できる利点を示す．

4.2. 比較と評価

表 1 に提案方式の比較表を示す．既に述べてきたように，データー致方式では Telnet のリモートログインによる渡り歩きしか検出できないが，コネクション検出方式では，Attacker・Foot Hold 間の通信はリモート

表 1　提案方式の比較
Table.1　Comparison of the proposed method.

		データー致方式（旧提案方式）	コネクション検出方式（新提案方式）
渡り歩き検出		可能	可能
	対象となるA-F間の通信	Telnetのみ	Telnet, SSH, rlogin など全てのリモートログイン
	対象となるF-T間の通信	Telnetのみ	全てのTCPサービス
検出できるタイミング		コネクション確立後	コネクション確立前
リアルタイム性		高い	高い

(注)
A-F間：Attacker・Foot Hold間
F-T間：Foot Hold・Target間

ログイン，Foot Hold・Target 間の通信は全ての TCP サービスである渡り歩きが検出できる．

データ一致方式では Telnet のコネクションを確立しなければ渡り歩きを検出できないが，コネクション検出方式ではコネクションを確立する前に検出できる．

両方式共に OS のカーネル内部で監視するため，検出のリアルタイム性は高い．

5. ま と め

本研究では，普遍的な渡り歩き検出方法について検討した．コネクション検出方式を適用することで，FPN 環境下でなくとも渡り歩きが検出できることを示した．また，データ一致方式に存在する問題点についても解決することができた．

FPN における不正な渡り歩きを検出するためには，本方式に加えて渡り歩きの正常・不正の判断をしなければならない．これに関しては，FPN で設定した各通信のアクセスポリシを比較することで可能である．また FPN 環境でなくても，事前に正常・不正パターンを定義した IP アドレスリストなどを用意することで，渡り歩きの正常・不正の判断ができると思われる．

今後の課題として，リモートログインの PSH パケットを受信してから一定時間の間に SYN パケットが送信されるまでの監視時間を適切な値に設定する必要がある．コマンドを受理してから実際にコネクションを確立するまでの時間の統計を取るなど，この値を求める必要がある．これはキーボード・マウス入力監視についても同様である．

参　考　文　献

[1] 2003 CSI/FBI Computer Crime and Security Survey, Computer Security Institute． http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2003.pdf

[2] Flexible Private Network, Watanabe Lab. Division of Information Sciences, Meijo University． http://www-is.meijo-u.ac.jp/%7Ewatanabe/research/fpn.html

[3] 鈴木秀和，渡邊晃，“GSCIP を構成する DPRP の仕組みの検討，”第 66 回情報処理学会全国大会，分冊 3，no.5V-1，pp.479-480，March 2004.

[4] 竹尾大輔，渡邊晃，“GSCIP を構成する渡り歩き検出機能の仕組みの検討，”第 66 回情報処理学会全国大会，分冊 3，no.5V-2，pp.481-482，March 2004.

[5] 増田真也，渡邊晃，“閉域通信グループにおける暗号通信方式の検討，”第 66 回情報処理学会全国大会，分冊 3，no.5V-3，pp.483-484，March 2004.

[6] 保母雅敏，渡邊晃，“多段構成ネットワークにおける鍵配送方式の一検討，”第 66 回情報処理学会全国大会，分冊 3，no.6V-2，pp.495-496，March 2004.

[7] 前羽理克，渡邊晃，“生体認証を利用したセキュアネットワーク通信，”第 66 回情報処理学会全国大会，分冊 3，no.6V-6，pp.503-504，March 2004.

[8] 竹尾大輔，渡邊晃，“TELNET による渡り歩きの検出方法の検討，”平成 15 年度電気関係学会東海支部連合大会，no.360，pp.180，Oct. 2003.

FPNにおける渡り歩きの検出方法の検討

- Researches on Detection Method of Island Hop in Flexible Private Network -

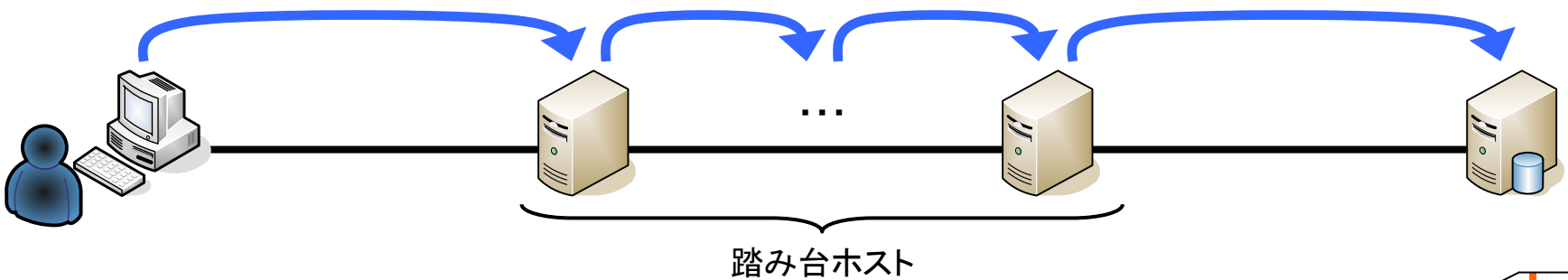
名城大学大学院理工学研究科
竹尾大輔　　渡邊　晃

背景

- 増加する企業内の不正アクセス
  - 外部からの不正アクセス　→　FW，要塞化
  - 内部のセキュリティ対策は甘い
- IDSでネットワークを監視
  - 不審な通信の発見
  - 内部犯罪の抑制

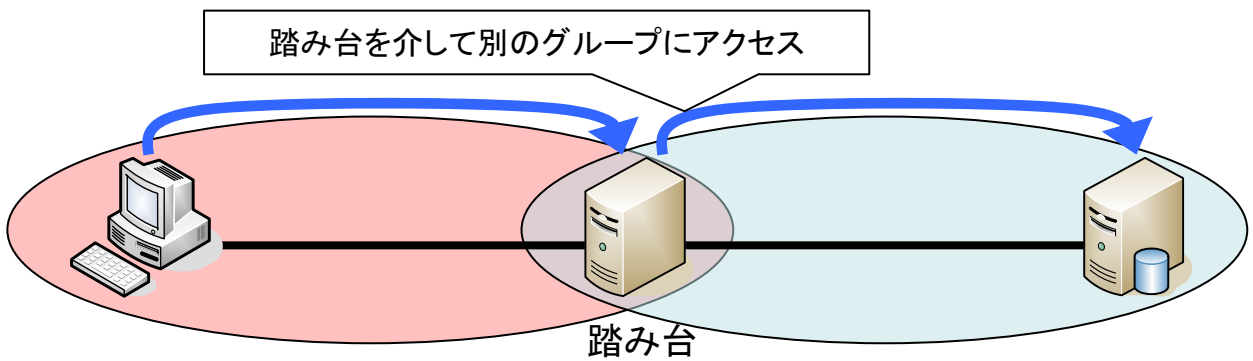
背景

- クラッカーは渡り歩きを行う
  - 多段の踏み台ホストを経由
  - 個々の通信の正常・不正の判断
    - 正常な通信を不正と見なすことは難しい
  - 渡り歩きの正常・不正の判断
    - 管理者による正常な渡り歩きか？クラッカーによる不正な渡り歩きか？
    - 判断材料が無い



FPNの概要と問題点

- Flexible Private Network
  - セキュリティ対策と運用管理負荷軽減の両立
  - ユーザ・ホストが部署単位などでグループ化
    - 異なるグループのホスト間通信を拒否できる
- 多重帰属しているホストを踏み台にする
  - 別のグループのホストにアクセスできる可能性



FPNの問題解決

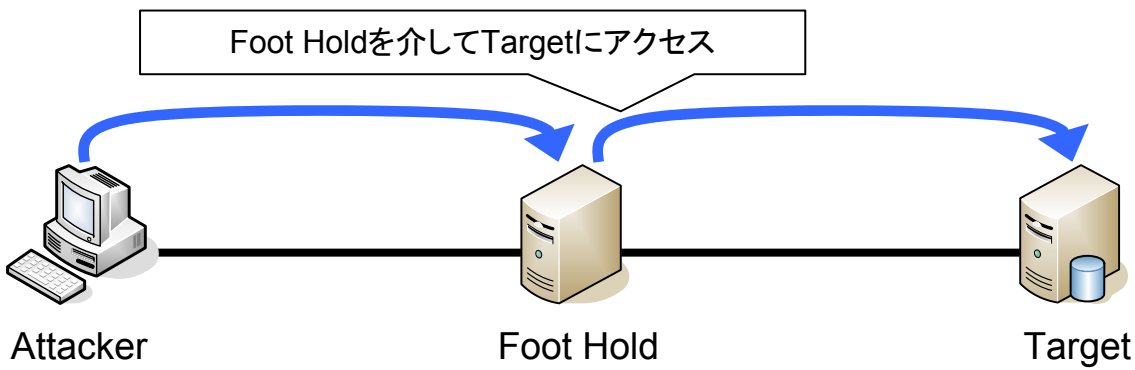
- 問題解決に要求されること
  1. 渡り歩き自体を検知
  2. 渡り歩きの正常・不正の判断

本研究の主題

- FPN環境下での渡り歩き検出方法を提案してきた
- 普遍的な渡り歩き検出方法を検討
  - 提案方式の性能評価実験
  - 新旧提案方式の比較による機能評価

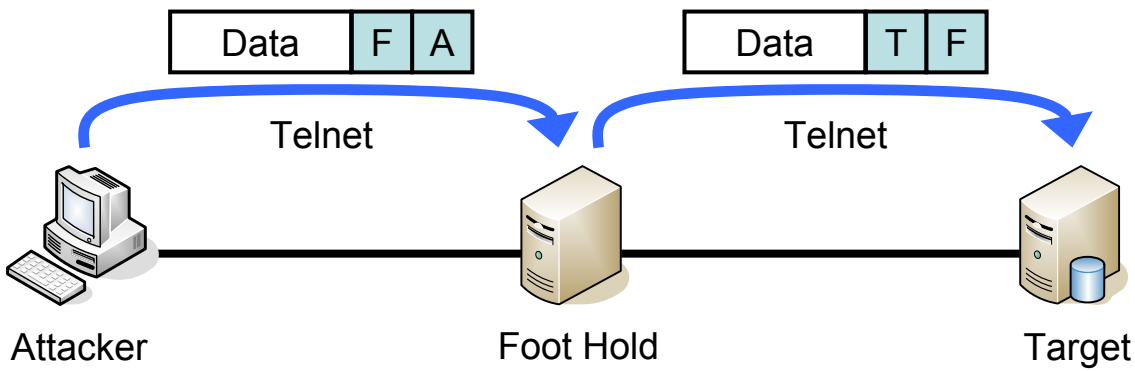
渡り歩きモデル

- 渡り歩きモデルの構成要素
  - Attacker（攻撃者ホスト）　：クライアント型
  - Foot Hold（踏み台ホスト）　：サーバ型
  - Target（ターゲットホスト）　：サーバ型

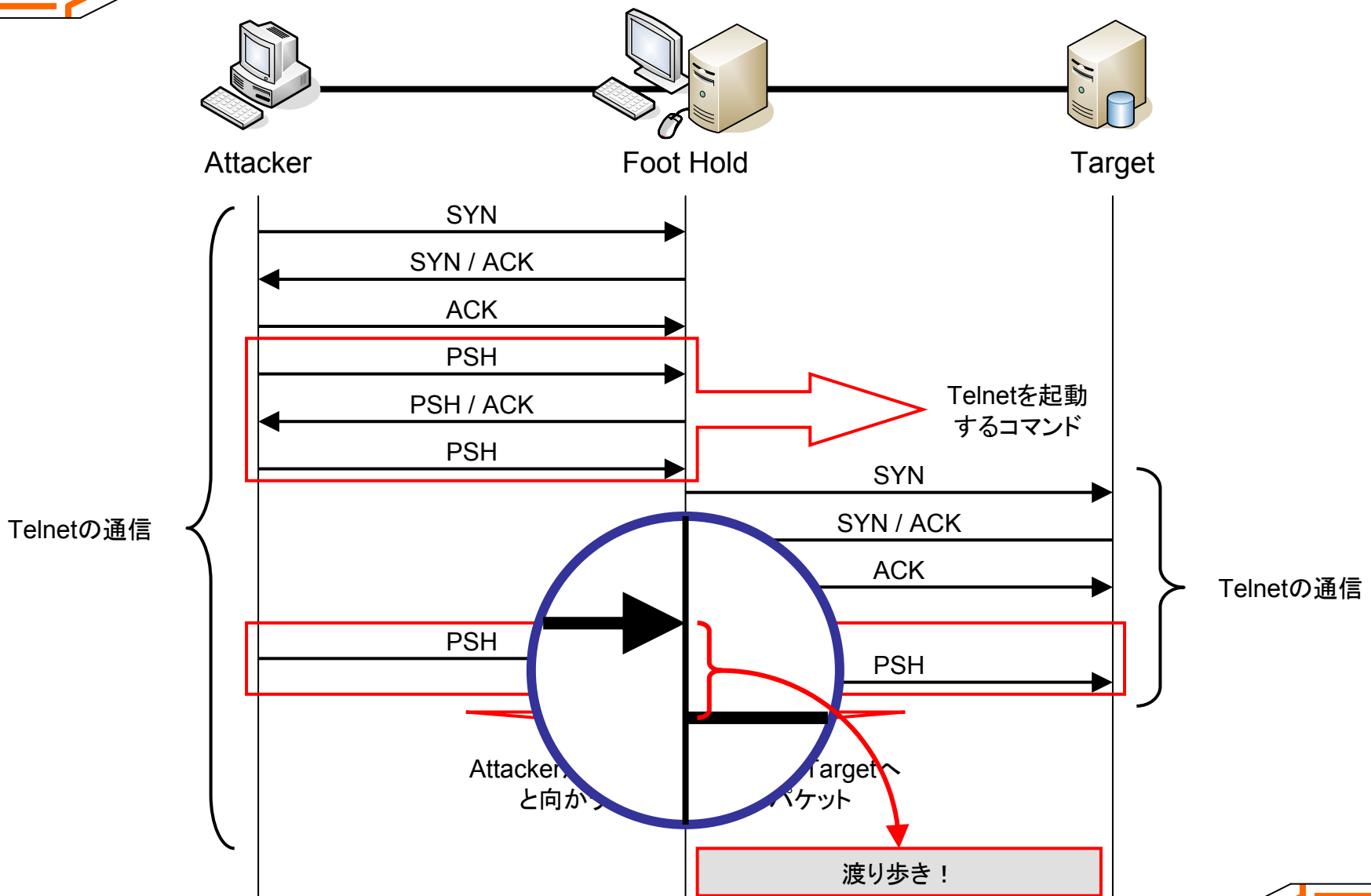


データー致検出方式

- Telnetによる渡り歩きを検出
  - IPアドレスは異なるがデータは同一の送受信パケットがFoot Holdでほぼ同時に発生している
  - Foot Holdで送受信パケットを監視

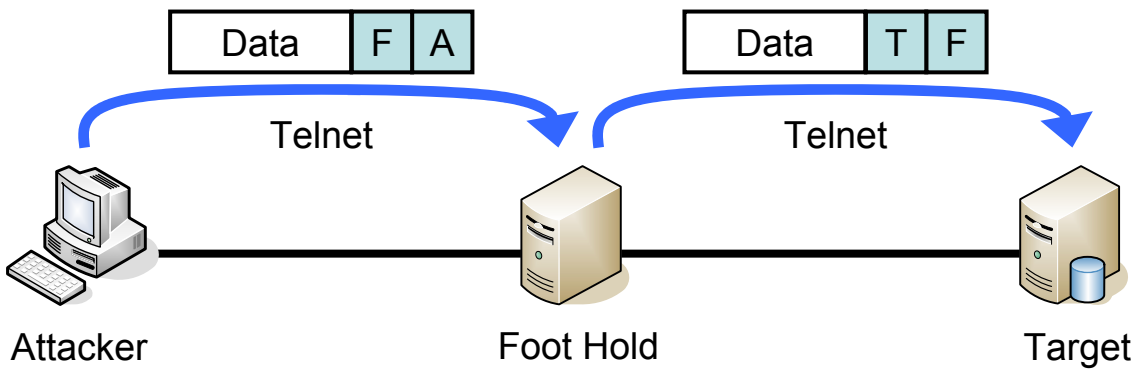


データー致検出の流れ


Attacker
Foot Hold
Target
SYN
SYN / ACK
ACK
PSH
PSH / ACK
PSH
Telnetを起動
するコマンド
Telnetの通信
SYN
SYN / ACK
ACK
PSH
PSH
Telnetの通信
渡り歩き！

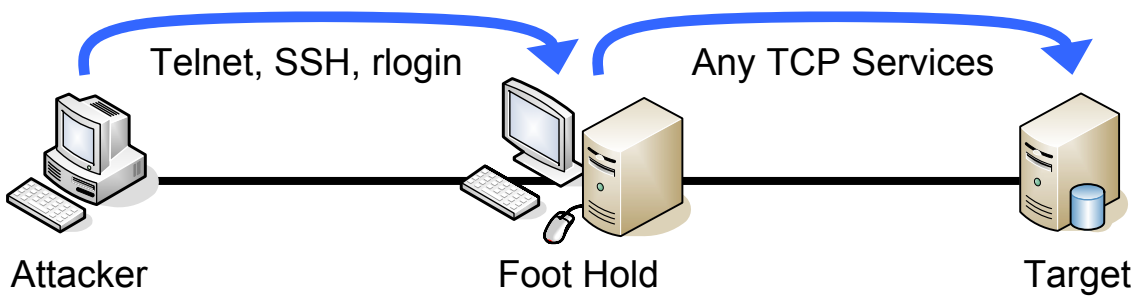
データー致検出方式の問題点

- データー致検出方式の3つの問題
  - ① 検出できるのはTCPコネクション確立後
  - ② 通信が平文であるTelnetのみ対象
  - ③ Foot Hold･Target間の通信はTelnetのみ対象

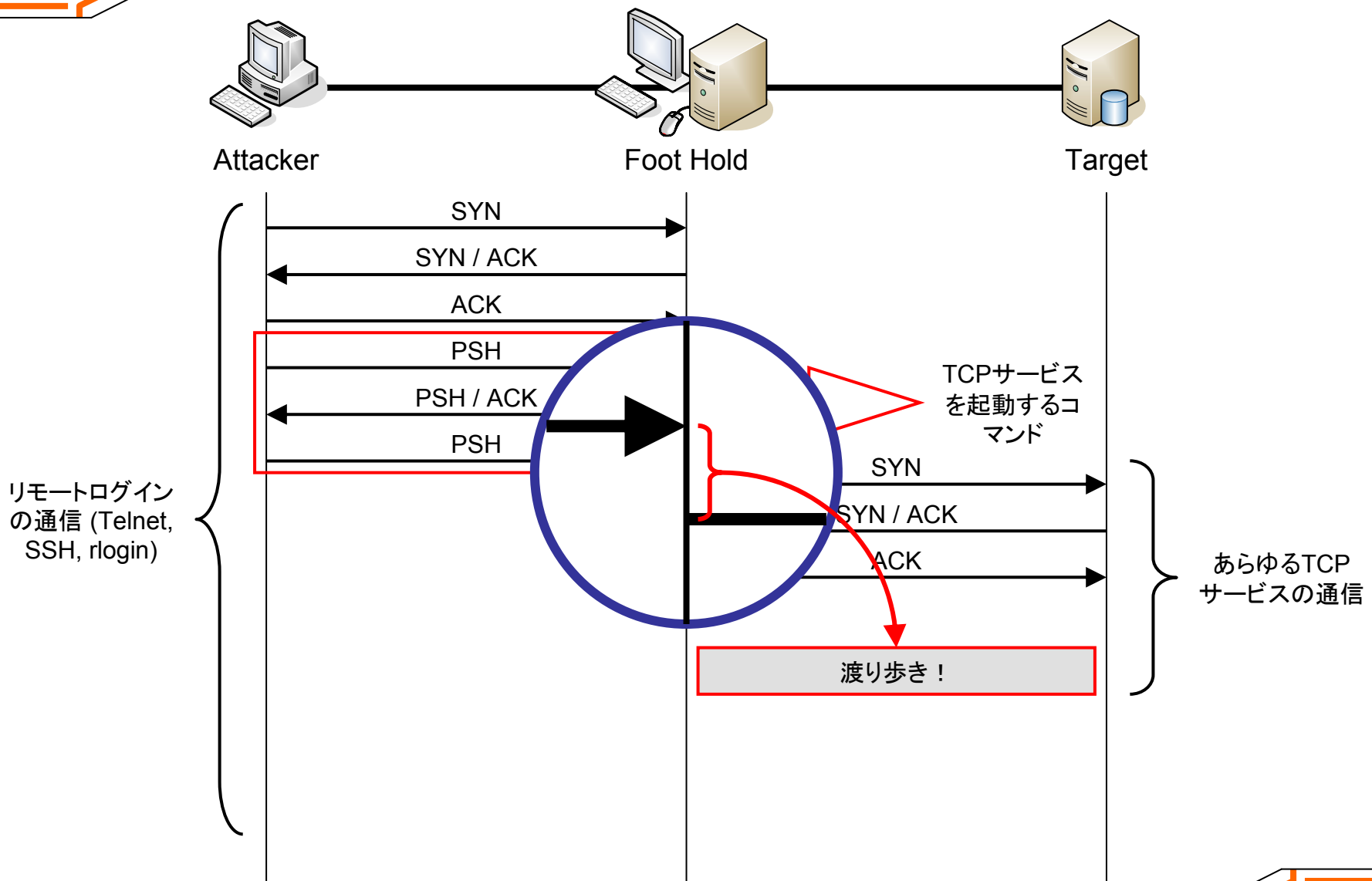


コネクション検出方式

- Attacker･Foot Hold間の通信
  - 各種リモートログイン（SSH，Telnet，rlogin）
- Foot Hold･Target間の通信
  - あらゆるTCPサービス
- AttackerがFoot Holdにリモートログインし，各種TCPサービスでTargetへアクセス
  - Foot Hold上で検出

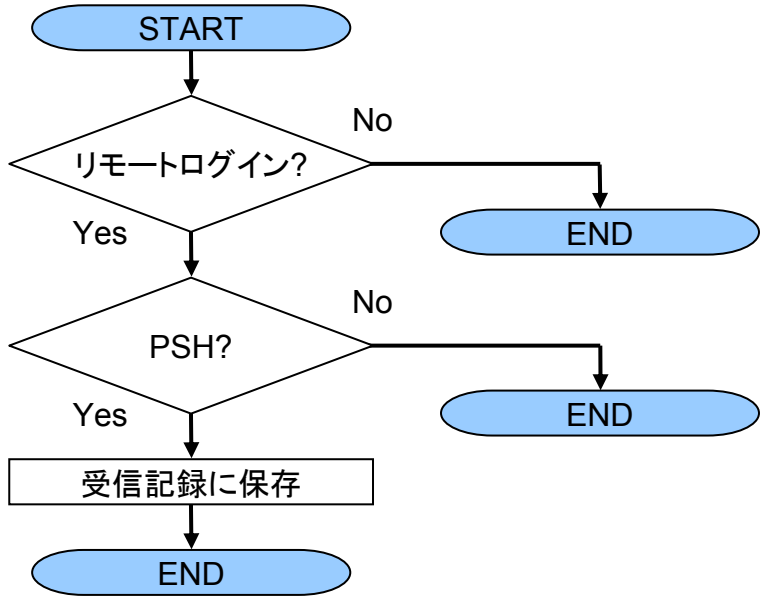


コネクション検出の流れ



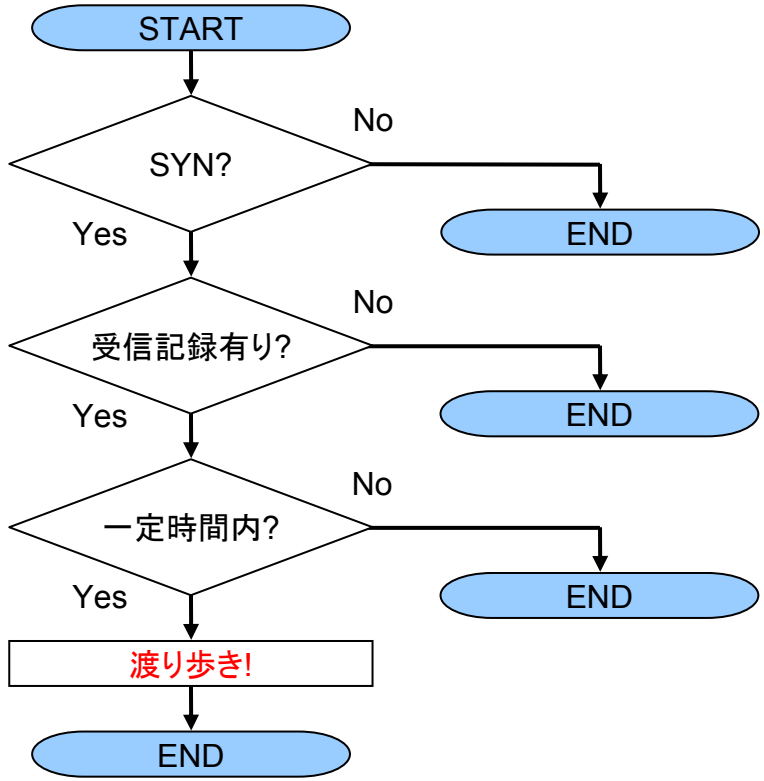
パケット受信処理の監視

- TCPパケットを監視，リモートログイン通信パケットを検出
- 検出時刻をリモートログイン受信記録に保存
- 検出対象はPSHパケットのみ
  - リモートログインの通信パケットはPSHフラグがセットされている
- すべてのリモートログインを検出できる



パケット送信処理の監視

- TCPパケットを監視，TCPコネクション確立要求を検出
- リモートログイン受信記録を参照，送信が一定時間内なら渡り歩き
- 検出対象はSYNパケットのみ
- コネクション確立前に，あらゆるTCPサービスによる渡り歩きを検出できる

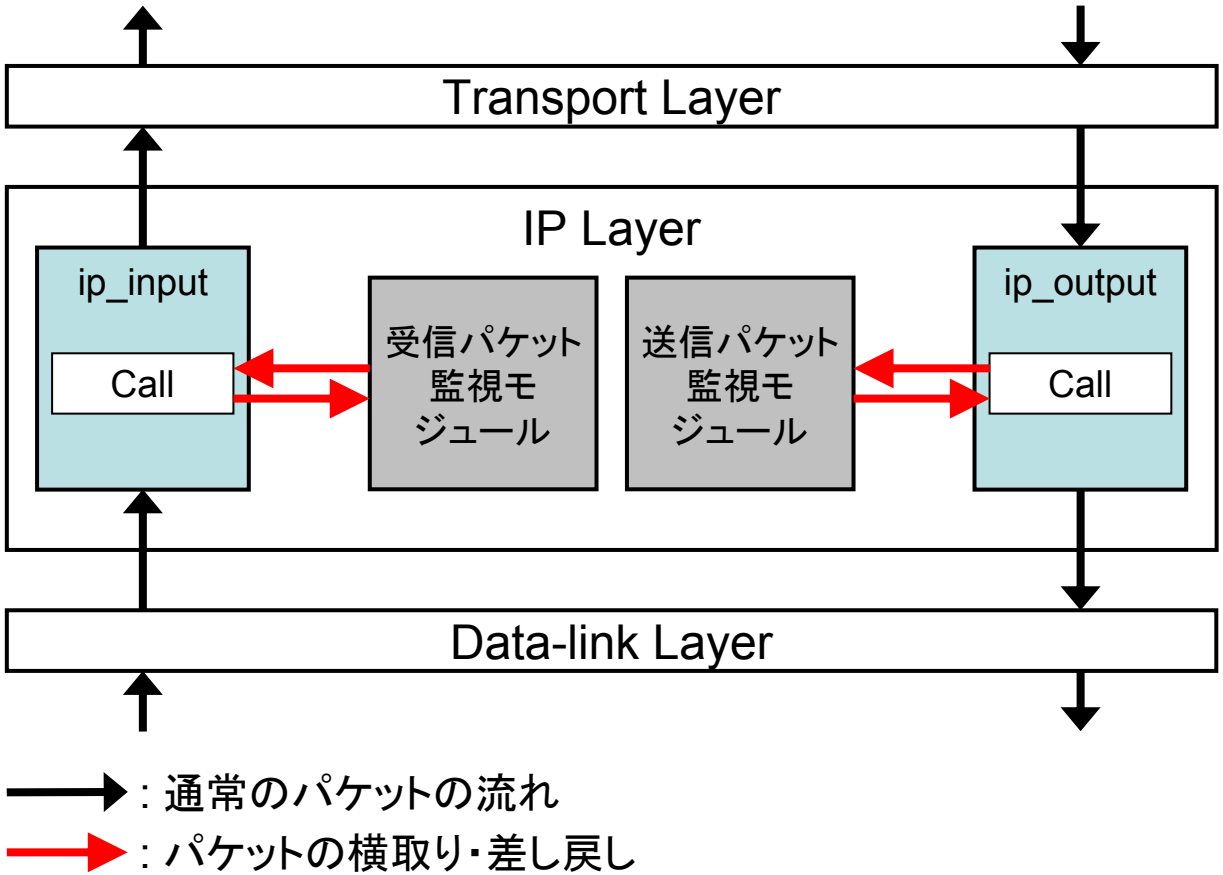


渡り歩き検出機能の実装

- リアルタイムに監視するために，OSのカーネルに実装する
  - イベントの取りこぼしが無い
  - 正確な検出時刻の比較が可能
  - 必要であればパケットの破棄も可能
- OSにFreeBSD 5.1Rを採用
  - ネットワークに関する資料が多い

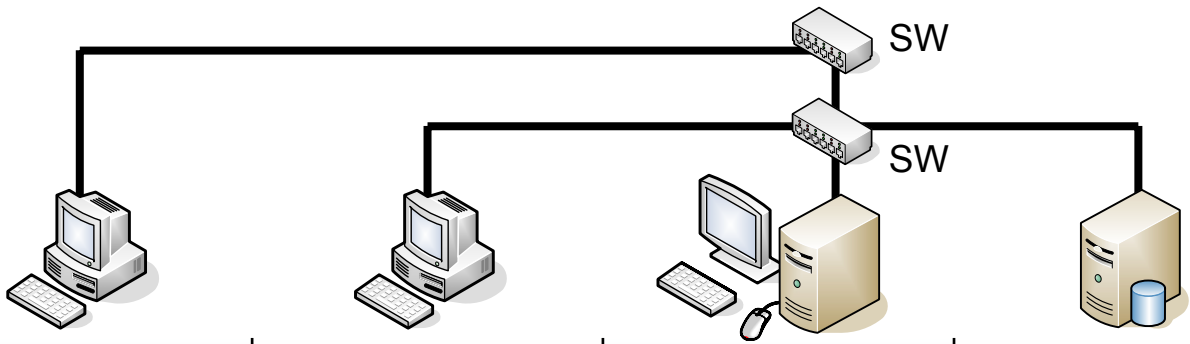
送受信パケットの監視位置

- 送受信パケットの監視はIP層で行う



実験環境

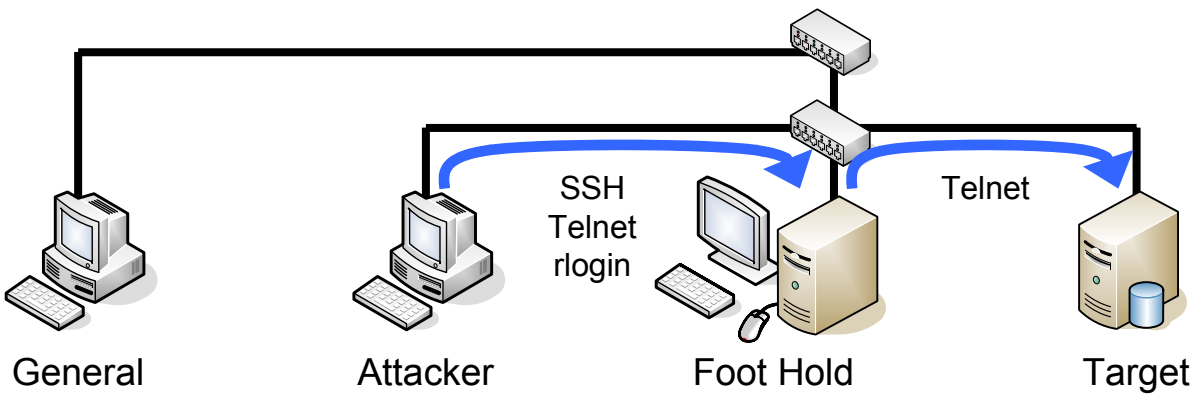
- 100BASE-TXのLAN
- Foot Holdに検出機能を実装



	General	Attacker	Foot Hold	Target
IPアドレス	172.18.16.90	172.18.16.42	172.18.16.45	172.18.16.34
CPU	Pentium4 2.4GHz	Celeron 2.0GHz	Pentium4 2.4GHz	Pentium4 1.8GHz
メモリ	512MB	512MB	256MB	256MB
OS	Windows XP Pro	Red Hat Linux 9	FreeBSD 5.1R	Fedora Core 1
起動サービス	-	-	SSH, Telnet, rlogin, FTP	Telnet, FTP

性能評価実験

- 検出機能の有効性とその性能の確認
  - 3種類のリモートログインによる渡り歩き
  - PSH受信-SYN送信の間の時間を計測

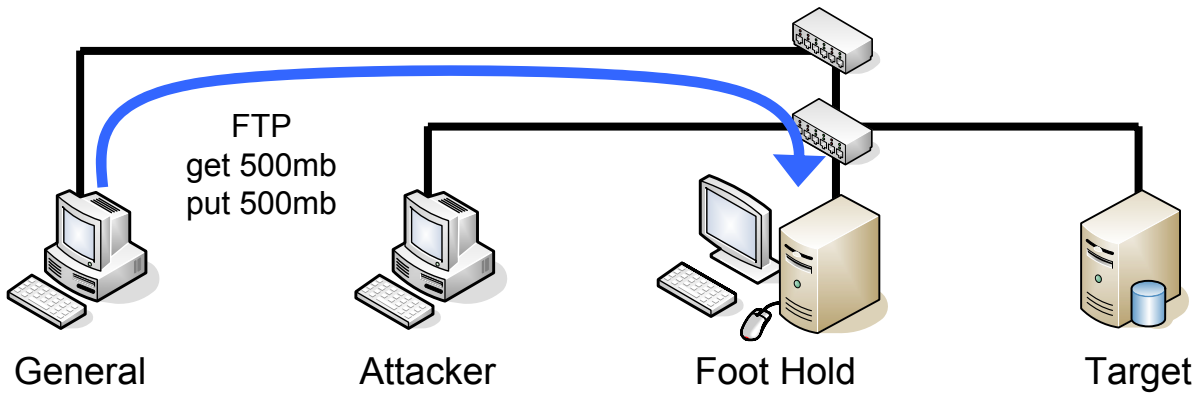


	Telnet直接起動	Telnet事前起動
SSH -> Telnet	13693.20(usec)	7228.05(usec)
Telnet -> Telnet	14985.65(usec)	7952.05(usec)
rlogin -> Telnet	15018.75(usec)	6553.55(usec)

※ 20回試行の平均

他処理への影響

- 検出機能の実装時/未実装時における，FTPを利用したダウン/アップロード時間測定
  - GeneralがFoot HoldにFTP接続
  - 500MBのファイルをダウン/アップロード



	実装時	未実装時
ダウンロード	45.1515(sec)	45.1520(sec)
アップロード	45.9155(sec)	45.9865(sec)

※ 20回試行の平均

提案方式の比較

- データー致検出方式とコネクション検出方式の機能比較

	データー致検出方式（旧提案方式）	コネクション検出方式（新提案方式）
渡り歩き検出	可能	可能
対象となるA-F間の通信	Telnetのみ	Telnet, SSH, rloginなど全てのリモートログイン
対象となるF-T間の通信	Telnetのみ	全てのTCPサービス
検出できるタイミング	コネクション確立後	コネクション確立前
リアルタイム性	高い	高い

(注)
A-F間： Attacker・Foot Hold間
F-T間： Foot Hold・Target間

考察

- アプリケーションによってPSH受信・SYN送信間の時間が変化
  - 同じアプリケーションでも起動方法によって変化
- コネクション検出方式ではAttackerを特定しづらい
  - 疑わしいAttackerのリストを管理者に報告
  - 平文のリモートログインはデータも監視
    - 改行コード‘0x0d’はコマンドの確定の可能性が高い
    - 例：>telnet 172.18.16.34↵

まとめ

- 普遍的な渡り歩き検出方法を検討した
  - FPN環境下以外で渡り歩きを検出できた
  - データー致検出方式の問題点を解決した
  - 導入による他処理への影響は無い
- 不正な渡り歩きの検出に関して
  - FPN環境下
    各通信に設定されたアクセスポリシを比較
  - FPN環境下以外
    事前にIPアドレスリストを用意しておく

今後の課題

- PSH受信から一定時間の間にSYN送信されるまでの監視時間を適切な値に設定する必要がある
  - コマンドを受理してから実際にコネクションを確立するまでの時間の統計を取る
  - マシンスペック差の考慮
    - CPUタイプ・クロック数，メモリ容量の報告

おわり