Telnetによる渡り歩きの検出方法の検討

11300J083　竹尾大輔
渡邊研究室

1. はじめに

近年，不正アクセスなどのイントラネット内部の犯罪が増加傾向にある．クラッカーが不正アクセスを行う場合，Telnetによる渡り歩きを行っているケースが多い．渡り歩きを検出することが出来れば，多くの不正アクセスを防止することが可能であると考えられる．

不正アクセス対策技術の一つとして，IDS（Intrusion Detection System：侵入検知システム）があるが，不正な渡り歩きを検出することは難しい．

本論文では，正常か不正かをも判別できる渡り歩き検出方法について報告する．

2. 渡り歩き検出方法

2.1 CCGIにおける渡り歩き検出

CCGI（Closed Communication Group for Intranet：閉域通信グループ）における渡り歩き検出の例として，図1のようなグルーピングによってアクセスを制限された CCGI があったとする．このネットワークでは，同一グループであるホスト同士は通信可能であるが，異なるグループであるホスト同士は通信することは出来ない．グループ A のみに属するホスト X が，グループ B のみに属するホスト Z に直接アクセスすることは出来ないが，グループ A と B に属するホスト Y はどちらにもアクセスすることが可能である．ここで X が Y を介して Z にアクセスすると，不正な渡り歩きをしたことになる．

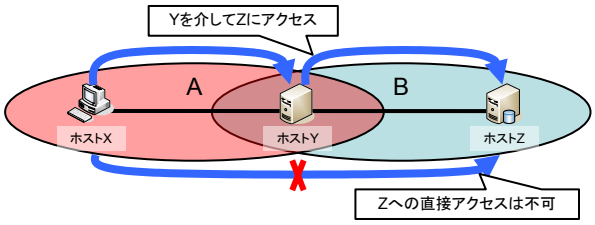


図1　CCGI上での渡り歩きの概念図

2.2 渡り歩き検出処理の流れ

本提案では，踏み台となる可能性のあるホストにおいて，送受信パケットの内容を比較する．Telnetによる渡り歩きでは Telnet コマンドのパケットが流れることになるが，IP アドレスは異なるが，同一データである送受信パケットがほぼ同時に発生することに着目している．パケットの監視は IP 層で行う．渡り歩き検出処理の流れは以下の通りである（図2）．これにより不正な渡り歩きを検出することが出来る．

① 受信パケットが Telnet であればその内容を保存し，タイマを起動する．
② 所定の時間内に Telnet の送信パケットが発生したとき，上記 Telnet の内容と比較する．
③ 内容が一致した場合，受信パケットの送信元 IP アドレスと送信パケットの宛先 IP アドレスからグルーピング関係をチェックし，正常なログインであるか不正な渡り歩きであるかを判断する．
④ 不正な渡り歩きと判断した場合，受信パケットを破棄し，アラートを発生する．
⑤ 所定時間内に渡り歩きが検出されない場合，監視処理を終了する．

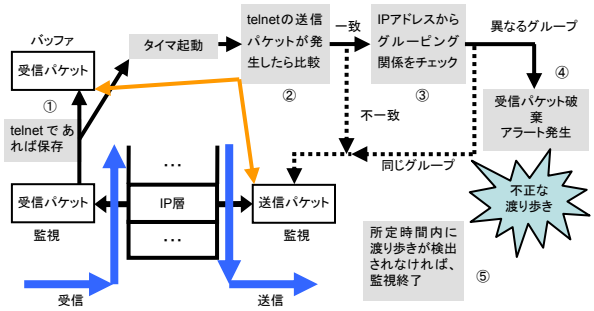


図2　渡り歩き検出処理の流れ

3. 渡り歩き検出機能の評価

表1に IDS と提案方式の渡り歩き検出に関する機能比較を示す．提案方式では，送受信パケットを監視することで渡り歩きを検出でき，IP 層で直接パケットを監視するので検出までの時間が速く，CCGI のグルーピング情報を用いることで正常・不正の判断ができる．

表1　IDS と提案方式の機能比較

	NIDS	HIDS	提案方式
渡り歩き検出	不可	可能	可能
リアルタイム性	高い	低い	高い
正常・不正の判断	不可	可能※	可能

（NIDS：ネットワーク IDS，HIDS：ホスト IDS）
※提案方式と同じ条件下の場合

4. おわりに

本研究では，Telnetによる渡り歩きを検出する方法を検討した．これにより渡り歩きが正常か不正かをも判別できるので，不正アクセスを防止することが可能となる．今後の課題としては，渡り歩き検出処理の効率化とトレースバックへの応用である．

参考文献

[1] 白井雄一郎，白濱直哉，又江原恭彦，柳岡裕美：インターネットセキュリティ　不正アクセスの手法と防御，ソフトバンクパブリッシング(2001).
[2] 武田圭史，磯崎宏：ネットワーク侵入検知，ソフトバンクパブリッシング(2000).

Telnetによる渡り歩きの検出方法の検討

Researches on Detection Method of Island Hop Using Telnet

名城大学理工学部
渡邊研究室
11300J083　竹尾大輔

1　はじめに

研究背景

不正アクセスなどイントラネット内部の犯罪が増加

－－＞　多くの場合、Telnetによる渡り歩きが行われている

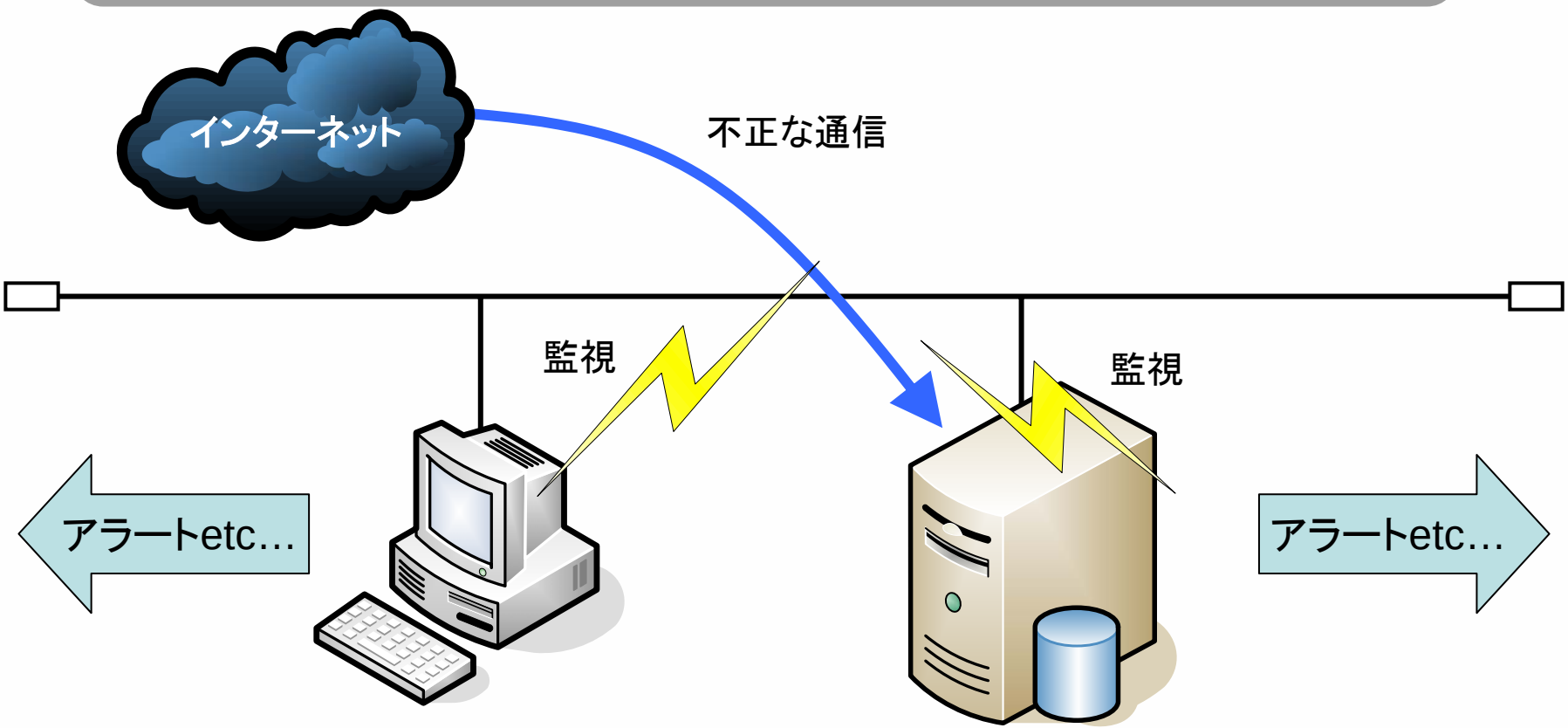
- 渡り歩き検出で不正アクセスの防止
- 既存技術では不正な渡り歩きの検出が困難

目的

正常・不正の判断が可能な渡り歩き検出方法を提案

2　IDS（侵入検知システム）

- IDS（Intrusion Detection System）とは
  不正なアクセスを監視・検知するシステム



IDSでの渡り歩き検出

ネットワーク型IDS

「渡り歩き」は検出困難

－－＞ Telnetの動作自体は不正ではないため

ホスト型IDS

「渡り歩き」は検出可能

－－＞ ログやコマンドヒストリを監視

リアルタイム性に欠ける

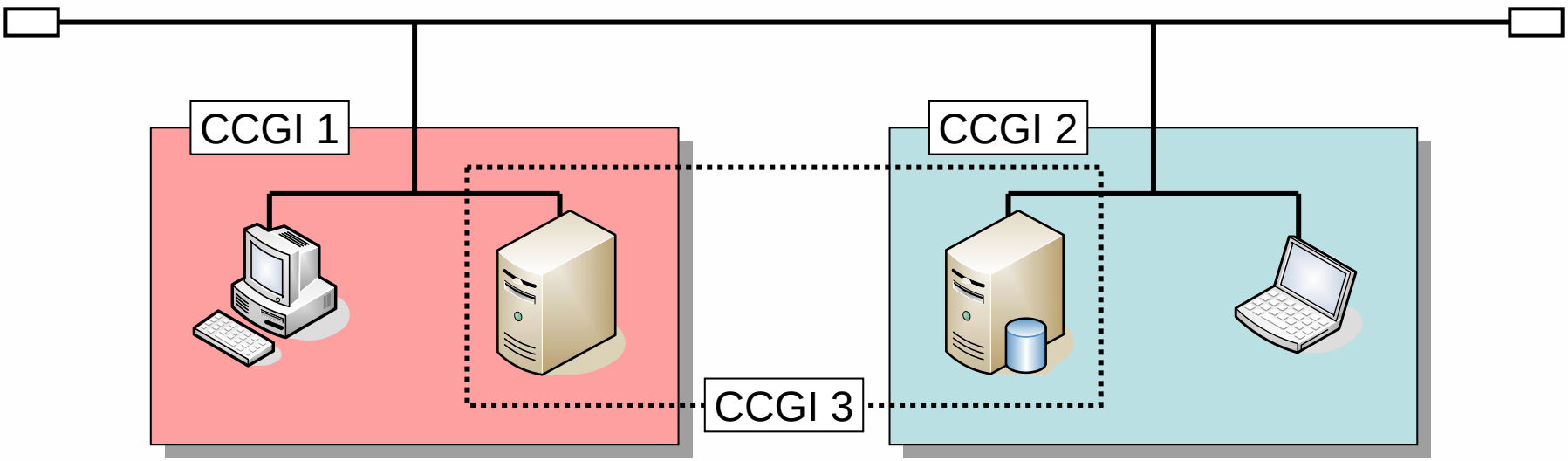
－－＞ 出力されたログから検出しているため

正常であるか不正であるかは判断できない

－－＞ 判断材料が無いため

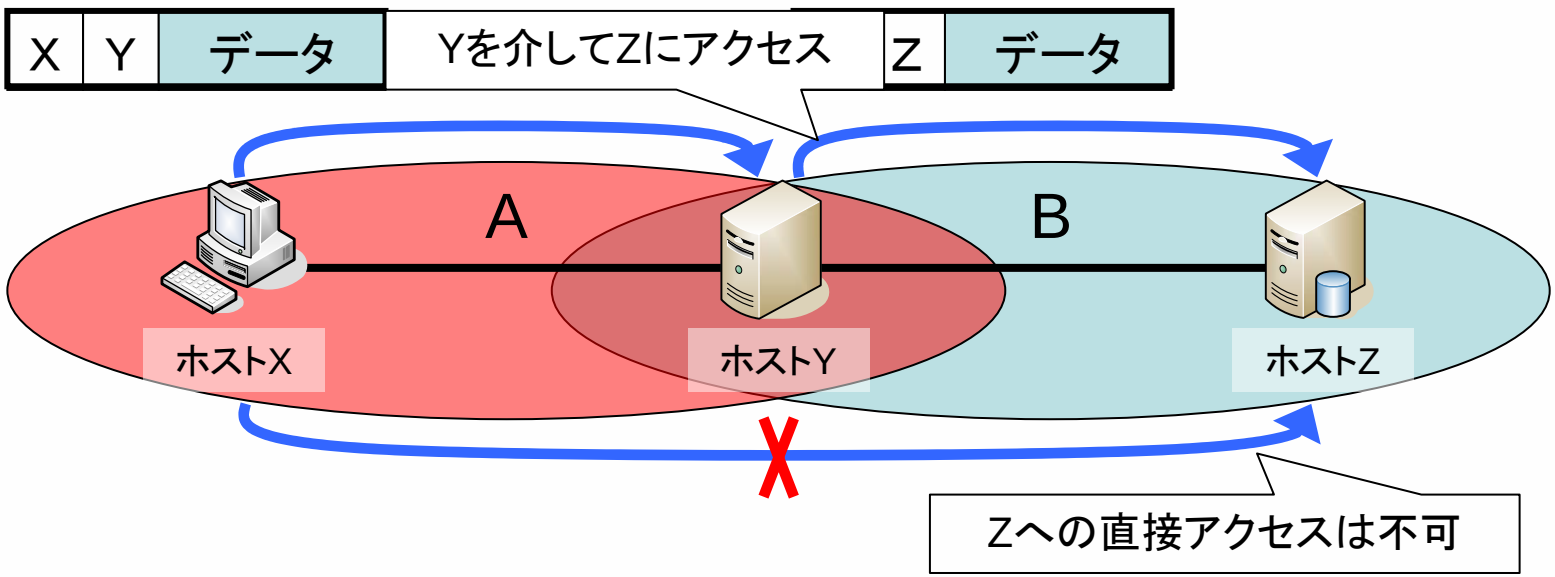
3　渡り歩き検出方法

- 閉域通信グループにおいて渡り歩きを検出
  - 閉域通信グループ[3]
    (Closed Communication Group for Intranet : CCGI)
    - ホストがグルーピングにより管理されている
      - グループ情報を用いることで正常・不正の判断が可能



CCGI上での渡り歩き検出

- XとYがグループA、YとZがグループBに帰属
- IPアドレスは異なるがデータは同じであるパケットが発生
  - 踏み台となるYでパケットを監視して検出する



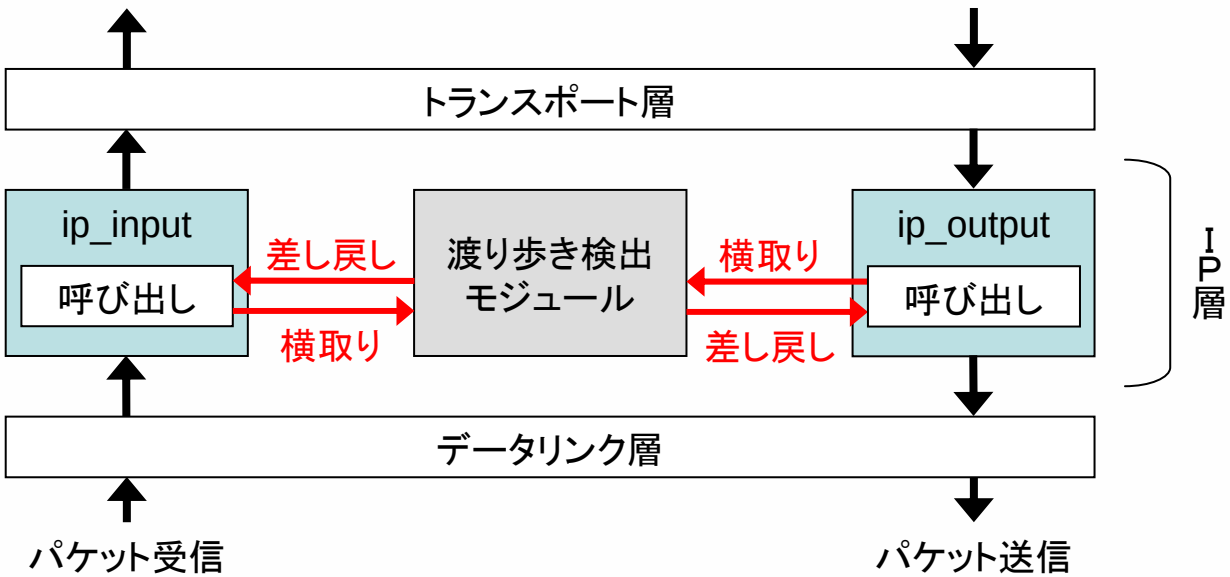
実現方法

ホスト上で監視

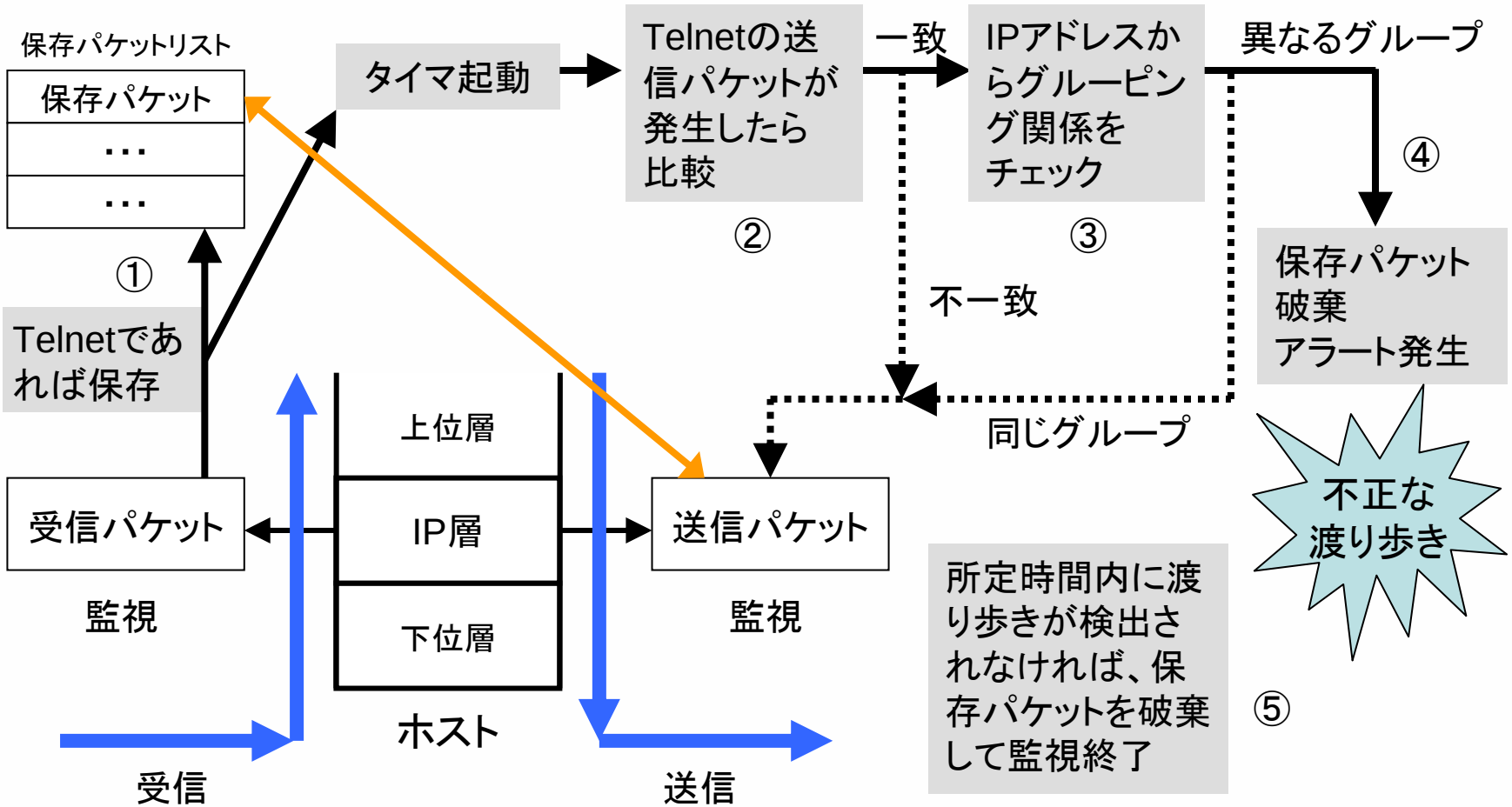
- 送受信パケットの監視が可能

IP層で直接パケットを監視

- リアルタイム性を高める
- パケットの操作が可能



渡り歩き検出処理の流れ



4　渡り歩き検出機能の実装

- 提案方式の有効性を確認するプログラムを試作し、実験を行った

開発

- IP層に関する情報が多いFreeBSDにて開発
- 本来はカーネルへ組み込むが、難易度が高い
- 実験では、データリンク層からパケットをコピーすることで渡り歩き検出を試みた

5　機能評価

- 試作プログラムにより、不正な渡り歩きを検出可能なことが確認できた

IDSとの比較

- 数値による比較は困難
- 機能比較に留める

表　IDSとの機能比較

	ネットワーク型	ホスト型	提案方式
リアルタイム性	高い	低い	高い
渡り歩き検出	不可	可能	可能
正常・不正の判断	不可	可能※	可能

※提案方式と同じ条件下の場合

6 おわりに

まとめ

- Telnetによる渡り歩きの検出方法を検討
- 実験により提案方式の有効性を確認
  - ✓ 正常か不正かをも判別できる
  - ✓ 不正アクセスの防止に役立つ

今後の課題

- 検討した方法の効率化
- IP層本来の機能との整合性
- 渡り歩きのトレースバックへの応用

おわり