TELNET による渡り歩きの検出方法の検討

A Study on the detection of island hop by TELNET

竹尾大輔　Daisuke Takeo　渡邊晃　Akira Watanabe（名城大学）

１．研究の目的

インターネットが普及して以来、数々の不正アクセス事件が発生し、ネットワーク管理者はその対策に追われている。不正アクセスの検知技術の一つとして「IDS（Intrusion Detection System：侵入検知システム）」がある。IDS とは、パケットやアクセスを監視し、データベースと比較することで不正や異常を判断するシステムである。しかし既存の IDS では、TELNET の渡り歩きを検出することができない。本研究では、不正アクセスの多くのケースで TELNET による渡り歩きが介在していることに着目し、これを検出する方法を検討する。

２．渡り歩き

渡り歩きとは、本来アクセスできないホストに、踏み台を介して不正にアクセスすることである。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閉域通信ネットワークがあったとする。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、渡り歩きをしたことになる。

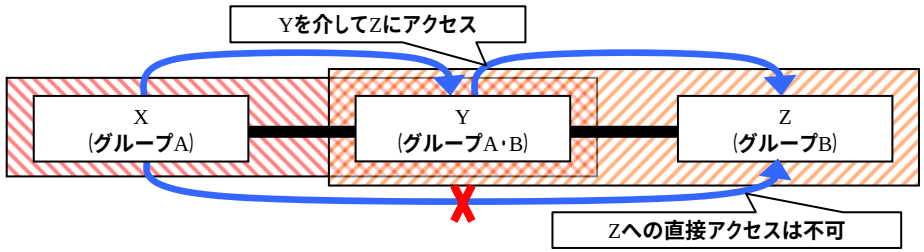


図１：閉域通信ネットワーク上での渡り歩きの概念図

３．パケットの監視

渡り歩きを検出するには、踏み台になる可能性のあるホストでパケットを監視する必要がある。図１ではホストＹでパケットの監視をすることになるが、そこでの監視位置と検出処理内容を以下に示す。

- 監視位置
  - 受信パケットは MAC 層から IP 層へ渡される前に、送信パケットは IP 層から MAC 層へ渡される前にチェックを行う。
- 検出処理
  - 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。
  - 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。
  - 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の関係をチェックし、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。
  - 渡り歩きと判断した場合、送信パケットを破棄し、管理者にアラームをあげる。
  - 所定時間内に渡り歩きが検出されない場合、最初の処理に戻る。

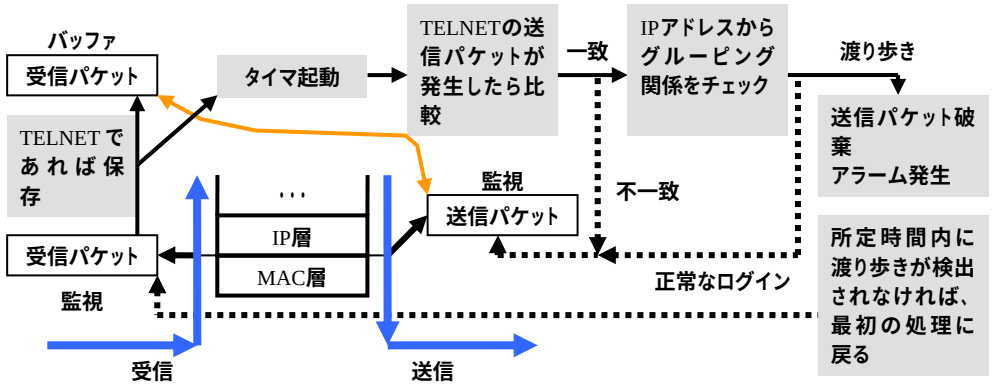


図２：パケット監視の流れ

４．まとめ

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。今後は検討した方法を実装し、その有効性を確認する。また、TELNET 以外の手段を用いた場合や、TELNET クライアントを用いて他サービスに接続した場合、TELNET サービスが 23 番ポート以外で稼動している場合などの検討も行う。

参　考　文　献

[1]　白井雄一郎、白濱直哉、又江原恭彦、柳岡裕美　著、『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　著、『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

A Study on the detection of island hop by TELNET

名城大学理工学部

竹尾大輔
渡邊　晃

1. 研究の目的

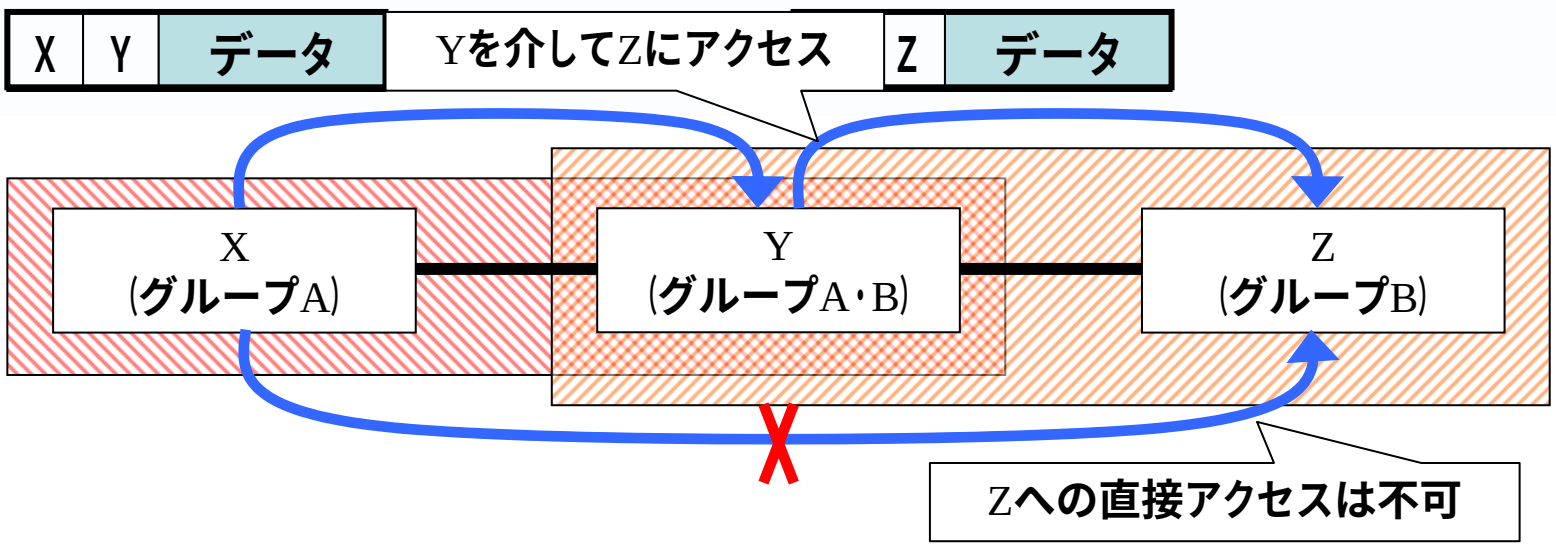
- 背景
  - 不正アクセス事件の多発
    - 盗聴、改ざん、なりすまし、DoS攻撃、etc
  - 不正アクセス時には必ず渡り歩きが行われる
- 既存技術
  - IDS (Intrusion Detection System：侵入検知システム)
    - ネットワークを監視し、不正や異常を検出
    - 渡り歩きは検知できない

提案

- TELNETによる渡り歩きを検出
  - 不正アクセスの多くでTELNETによる渡り歩きが介在
  - IDSで実現されていない機能を補完
  - 渡り歩き検知により不正アクセス防止に役立つ
- 対象ネットワーク環境
  - 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ので、渡り歩きの検出が容易
    - CCGIの機能として組み込みが可能

2．渡り歩き

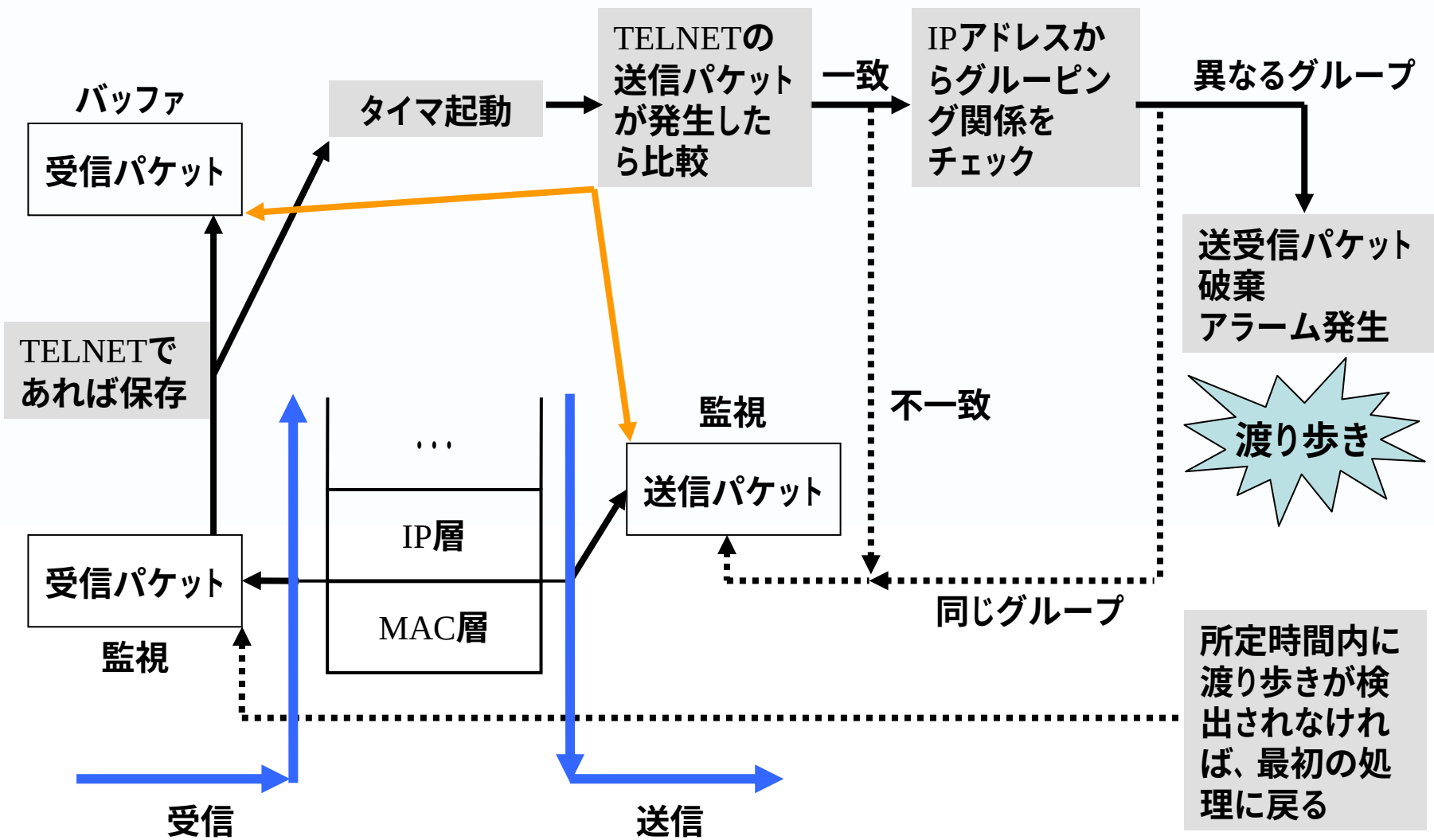
- 渡り歩きの定義
  - 本来アクセスできないホストに、踏み台を介して不正にアクセスすること
- 閉域通信グループにおける渡り歩き



3．パケットの監視方法

- 基本原理
  - 踏み台となるホストで監視
  - 送受信パケットの内容を比較
- 監視位置
  - MAC層とIP層の間で監視
    - IP層以上のレイヤーに変更の必要無し
  - 受信パケット
    - MAC層からIP層へ渡される前にチェック
  - 送信パケット
    - IP層からMAC層へ渡される前にチェック

パケット監視の流れ


バッファ
受信パケット
タイマ起動
TELNETの送信パケットが発生したら比較
一致
IPアドレスからグルーピング関係をチェック
異なるグループ
送受信パケット破棄
アラーム発生
渡り歩き
TELNETであれば保存
監視
送信パケット
不一致
IP層
MAC層
受信パケット
監視
同じグループ
所定時間内に渡り歩きが検出されなければ、最初の処理に戻る
受信
送信

4．まとめ

- TELNETによる渡り歩きの検出方法を検討

- 今後の研究課題
  - 検討した方法の実装、有効性の確認
  - 監視内容の拡張
    - TELNETサービスが23番ポート以外で稼動している場合
    - TELNETクライアントで他サービスに接続した場合
    - TELNET以外の手段を用いた場合
  - IDS製品への組み込み

おわり

0．参考資料

- 参考文献
- IDSの概念図
- 閉域通信グループ
- TELNETの説明

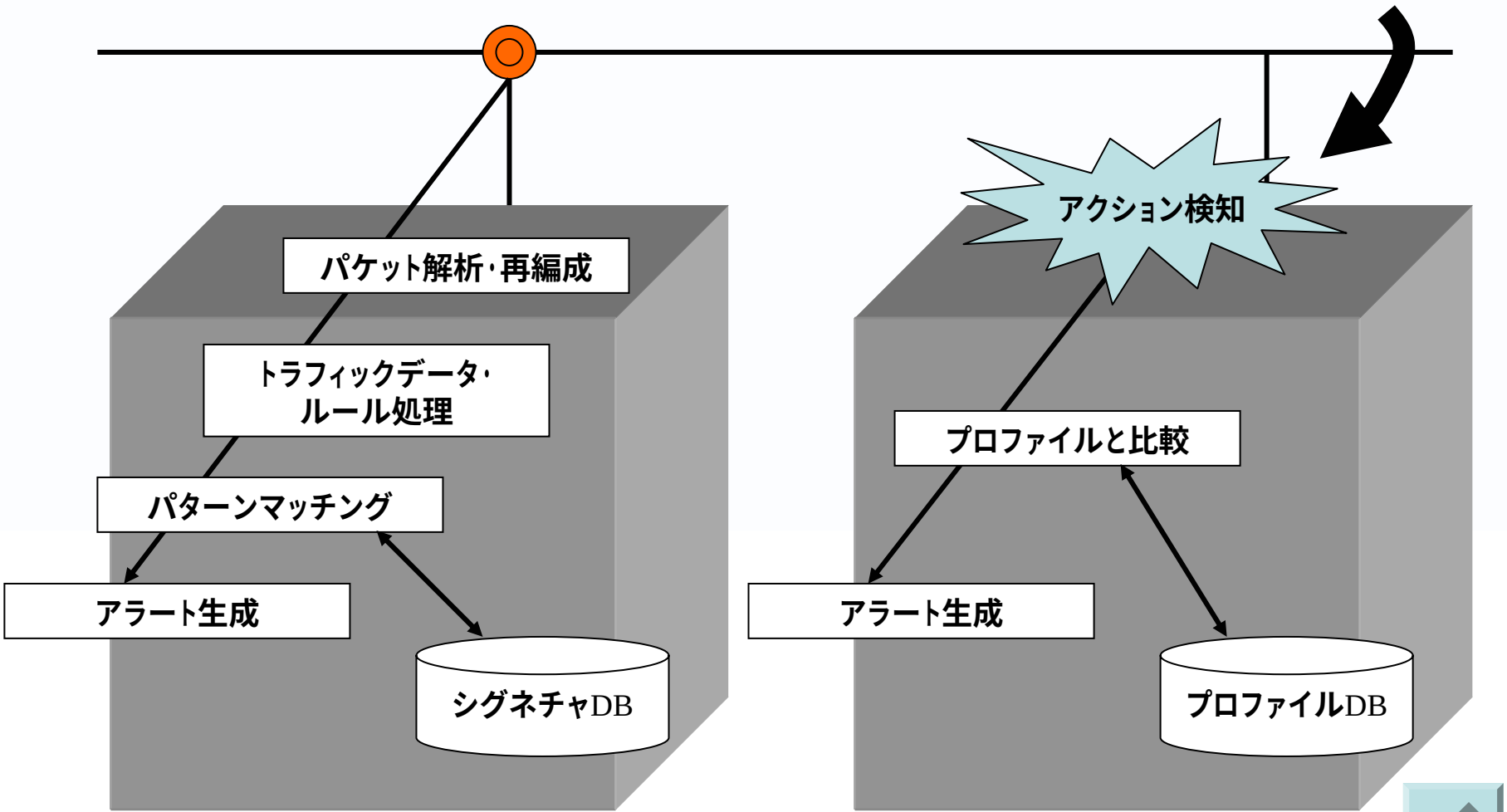
参考文献

[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

[3] **渡邊、厚井、井手口、横山、妹尾**
『暗号技術を用いたセキュア通信グループの構築方式とその実現』
情報処理学会論文誌 Vol.38 No.04-025、1997

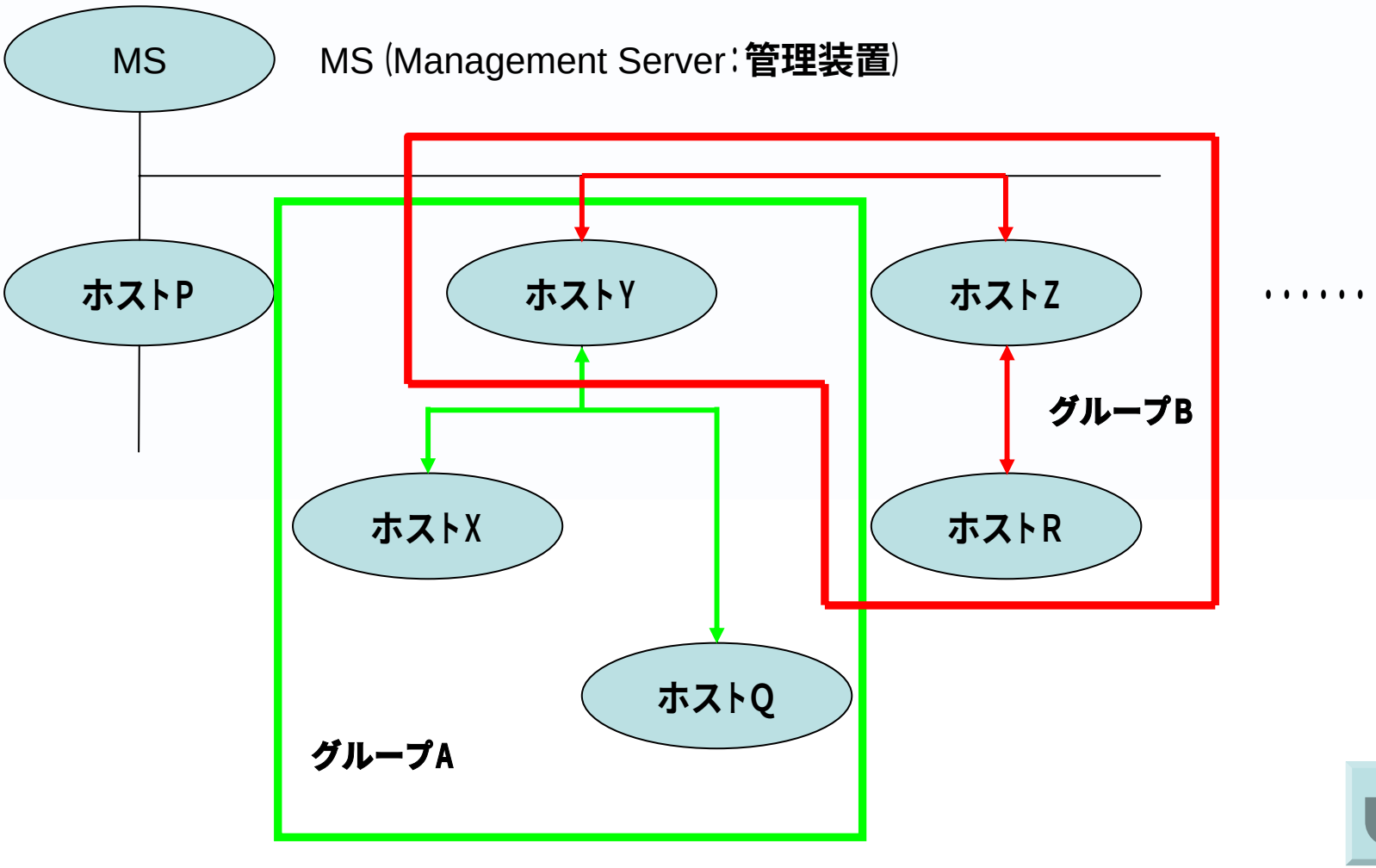
IDSの概念図



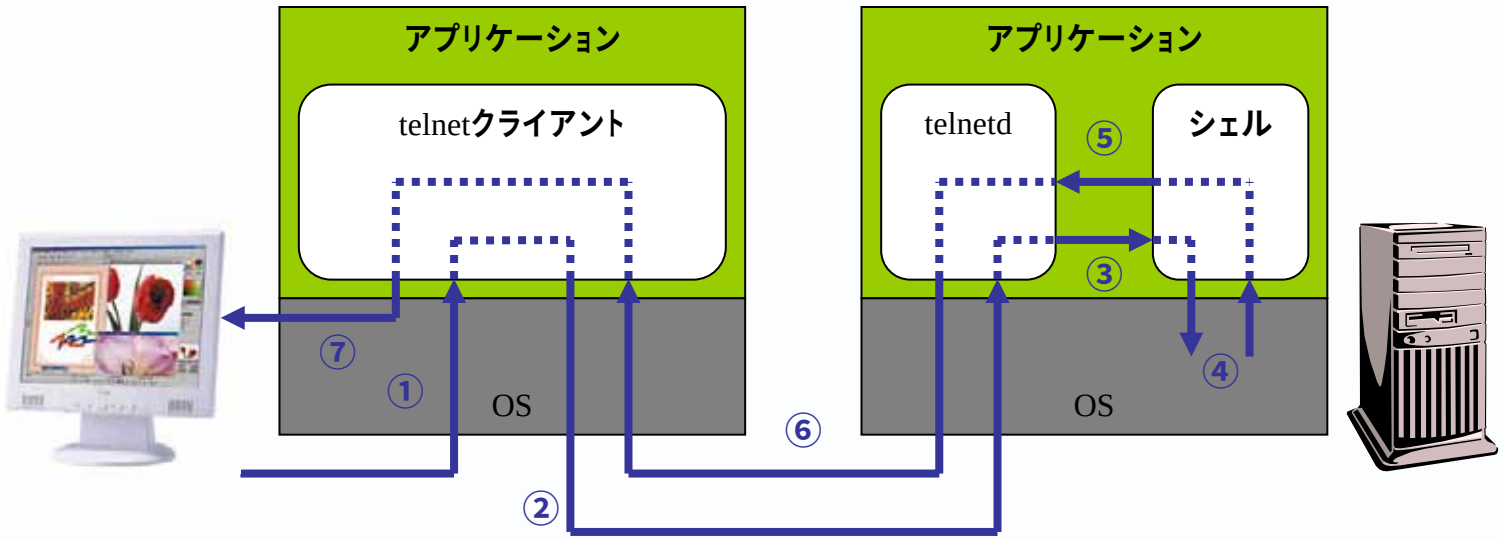
NIDS

HIDS

閉域通信グループ


MS
MS (Management Server：管理装置)
ホストP
ホストY
ホストZ
・・・・・・
グループB
ホストX
ホストR
ホストQ
グループA

TELNETの説明



透過モード