2007－CSEC－39 (1)
2007／12／14

# 能動型不正接続防止システムの検討

三村 守† 中村 康弘†

†防衛大学校 情報工学科
239-8686 神奈川県横須賀市走水 1-10-20

g45042@nda.ac.jp yas@nda.ac.jp

**あらまし** 近年，コンピュータネットワークを介した情報漏洩やウィルス感染が問題となっている．これらの問題が起きる要因の１つに，脆弱性対策などを十分に行っていない機器をネットワークに不正接続することが考えられる．しかし，既存の対策手法では，接続が許可された承諾機器を NAT (Network Address Translator) 機能を持つルータとして動作させることによる未承諾機器の不正接続は検出できない．また，既存の対策手法は特別な機器やソフトウェアを必要としたり，ネットワーク構成に依存する場合もある．本稿では，能動的にエッジルータの ARP テーブルを監視し，NAT による不正接続をも検出し，無力化することができる能動型不正接続防止システムを検討する．また，検討したシステムを実装し，検証実験により効果を確認する．

# An Examination of an Active Disapproval Connection Prevention System

Mamoru Mimura† Yasuhiro Nakamura†

†Department of Computer Science, National Defense Academy
1-10-20, Hashirimizu, Yokosuka-shi, Kanagawa 239-8686, Japan

g45042@nda.ac.jp yas@nda.ac.jp

**Abstract** Recently in computer networks, there are many problems such as a leakage of confidential information, computer virus and so on. One of the causes is connecting weak devices that have security holes to LAN. However, the previous methods cannot detect unauthorized devices by NAT (Network Address Translator) of the authorized device. Besides, the previous methods might require the specific hardware or software, and might depend network topology. In this report, we propose the active disapproval connection prevention system that watches ARP table on edge routers, can detects NAT and invalidates that. We implement the system, and the results of verification experiment show its effects.

## 1 はじめに

近年，コンピュータネットワークを介した情報漏洩やウィルス感染が問題となっている．これらの問題が起きる要因の１つに，ネットワーク利用者の故意または過失により，脆弱性対策などを十分に行っていない機器をネットワークに接続することが考えられる．このような問題への対策として，古くは Kerberos などの機器認証，MAC (Media Access Control) アドレスや利用者認証に基づく機器認証および近年では検疫ネットワークを構築する手法が用いられている．しかしながら，十分な検証の上で接続が許可された承諾機器であっても，複数のネットワークインターフェースを持ち，NAT (Network Address Translator) 機能を持つルータとして動作させることで，検証が十分ではない未承諾機器を当該 LAN に接続できてしまう．よって，このような NAT による不正接続をも検出し，無力化することができるネットワーク監視システムが必要である．

本稿では，このような未承諾機器の接続を不正接続と呼び，この問題に関する対策について検討する．

## 2　不正接続の検出方式

この章では不正接続の検出方式に関係する既存の手法の特徴を考察する．

### 2.1　NAT の検出

著者らはトレースパケットを送信して能動的に IP ヘッダの TTL (Time To Live) を取得し，これにより NAT 検出を行う能動的検出手法を提案した [1]．TTL はパケットの生存時間を意味し，ルータを経由するごとに 1 ずつ減算される．図 1 を例に著者らの手法を説明する．監視対象であるホスト A は LAN の運用ポリシに反し，NAT ルータとして機能している．検出システムは NAT の内側にあるホスト B から送信されたパケットを傍受すると，その TTL からホップ数が 2 であることを記録するとともに，送信元 IP アドレスに対しトレースパケットを送信する．この時のトレースパケットの宛先は，ホスト A の IP アドレスとなる．ホスト A からの応答パケットの TTL から，ホスト A までのホップ数が 1 であることが検出できる．これが記録してある対象パケットのホップ数より小さい場合には，先の送信パケットは NAT の内側から中継されたものと判定できる．本稿では，NAT 検出のために能動的に送信するパケットをトレースパケットと呼ぶ．また，その応答として監視対象から送信されるパケットを応答パケットと呼ぶ．

### 2.2　関連研究

intraPOLICE[2] などの既存の未承諾機器検出システムでは，NAT を利用した不正接続を検出することができない．また，MAC アドレスを傍受する必要があるため，すべてのセグメントでパケットを傍受する必要がある．文献 [3] の情報コンセントによる不正アクセス防止方式では，IP アドレスや MAC アドレスの偽造にも対応することができる．しかし，ネットワーク全体にそのような機能をもつ情報コンセントを導入する必要がある．文献 [4] では DHCP を用いた方式が提案されている．これらの方式では，

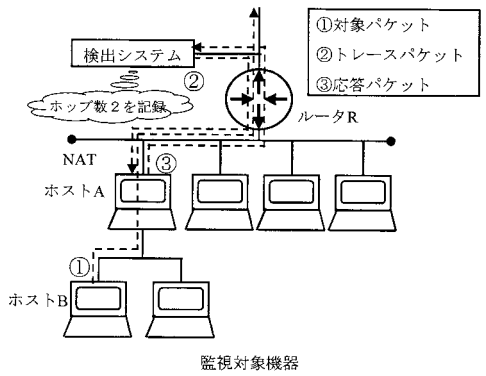


図 1: 能動的 NAT 検出手法

ネットワークに DHCP を導入する必要があり，さらにそれがルータとして動作する必要がある．また，認証に必要なソフトウェアをすべての承諾端末に導入する必要がある．このように，従来の方式では特別な機器やソフトウェアを新たに導入する必要がある．

## 3　不正接続の無力化手法

この章では不正接続の無力化手法をまとめ，特徴を考察する．

### 3.1　ルータによるフィルタリング

不正接続を無力化する手法として，ルータやスイッチでパケットをフィルタリングする手法が考えられる．しかし，この手法はルータ上で実装を行う必要があり，既存のネットワークに導入するためには構成を変更する必要が生じる可能性がある．

### 3.2　偽造 ARP パケットによる手法

IP アドレスから MAC アドレスを求めるためには，イーサネットでは ARP (Address Resolution Protocol) が利用される．ARP テーブルが汚染される問題 [5] を利用した不正接続の無力化手法が実用化されている．すなわち，偽造した ARP パケットをネットワークに送信し，対象ホストの ARP テーブルを汚染し，MAC アドレスの解決を阻害することによって無力化する．この手法は ARP REQUEST を利用する手法と，ARP REPLY を利用する手法に

分類される．ARP REPLY を利用する手法はさらに，無力化したいホストの ARP テーブルを書き換える手法と，それ以外のホストの ARP テーブルを書き換える手法が考えられる．これらの偽造 ARP パケットによる手法は，ルータやスイッチを経由しない同一セグメント内でのみ有効である．したがって，監視対象ホストがあるすべてのセグメントで対策手法を実装する必要がある．

### 3.3 プロトコルの脆弱性による手法

ARP テーブルが汚染される問題のほかにも，文献 [5] には多くの TCP/IP に係る既知の脆弱性が示されている．これらのプロトコルの脆弱性を，不正接続の無力化に応用することが考えられる．著者らは文献 [5] に示された脆弱性の中でも，TCP 接続の強制切断の問題に着目した．この手法では無力化できる通信は TCP に限定されるが，ルータによるフィルタリングや偽造 ARP パケットによる手法のように，ネットワーク構成や設置場所に関する制限が少ないという利点がある．

## 4 能動型不正接続防止システム

この章では開発目標を述べ，不正接続の検出手法と無力化手法を検討し，能動型不正接続防止システムを試作する．さらに，試作した能動型不正接続防止システムの各機能と動作概要を説明する．

### 4.1 開発目標

本稿では特定の環境に依存せず，様々なネットワークに柔軟に対応することができる不正接続防止システムの開発を目標とする．その要件を次に示す．

- NAT による不正接続を検出できる．
- 監視対象の OS やアーキテクチャに依存しない．
- ネットワーク構成の変更が不要である．
- 大規模なネットワークにも容易に対応できる．

これらの要件を，可能な限り特別な機器を必要とせずに実現するシステムの開発を目指す．

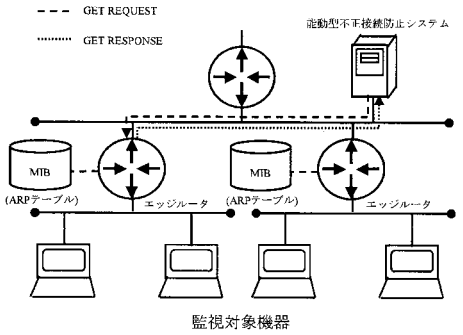


図 2: SNMP を利用したエッジルータの ARP テーブルの監視

### 4.2 エッジルータの ARP テーブルの監視

既存の不正接続の検出方式では，監視対象が設置されたすべてのセグメントでパケットを傍受する必要がある．このため，膨大な数のセグメントを有する大規模なネットワークでの運用は難しい．この問題を解決するため，SNMP (Simple Network Management Protocol) を利用して，監視対象が接続するエッジルータの ARP テーブルを能動的に監視する手法を採用する．エッジルータの ARP テーブルの変化が検出できれば，異なる MAC アドレスの機器が接続されたことが検出できると考えられる．この仕組みを図 2 を用いて説明する．SNMP はネットワーク機器を管理するためのプロトコルであり，最近のルータやハブには SNMP エージェントの機能を備えたものが多い．そこで，不正接続防止システムを SNMP マネージャとして動作させ，エッジルータの SNMP エージェントに対して GET REQUEST を送信する．ここで要求する MIB (Management Information Base) は，標準 MIB の at (Address Translation) グループである．at グループには ARP テーブルに関する情報がリアルタイムに記録される．エッジルータは現在の ARP テーブルの状況を，GET RESPONSE で不正接続防止システムに送信する．これにより，エッジルータの ARP テーブルの状態を知ることができる．不正接続防止システムでは，エッジルータの ARP テーブルから監視対象の MAC アドレスを得ることができる．この能動的手法を利用すれば，複数のセグメントの MAC アドレスを 1 箇所で監視することが可能であると考える．

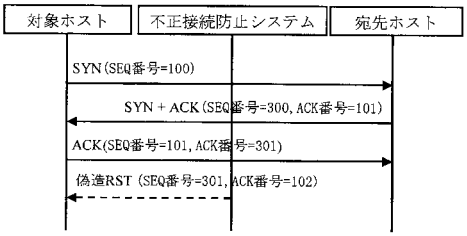


図 3: TCP 接続の強制切断

## 4.3 NAT の検出

既存の未承諾機器検出システムでは NAT を利用した不正接続を検出することができない．この問題を解決するため，文献 [1] で提案した能動的 NAT 検出手法を能動型不正接続防止システムに実装する．

## 4.4 TCP 接続の強制切断

不正接続を無力化する手法として，TCP 接続の強制切断の問題を利用する．図 3 のように不正接続防止システムが，監視対象ホストの通信を傍受できる位置でパケットを監視し，偽造した RST (Reset) パケットを送信して通信を無力化する．防止システムは対象ホストの TCP パケットを傍受し，その SEQ (Sequence) 番号から ACK (Acknowledge) 番号を算出し，偽造した RST パケットを送信する．RST パケットを受信した対象ホストの TCP 接続は切断される．これにより，対象ホストの TCP 通信を無力化することができると考えられる．この手法はトランスポート層の仕組みを利用するため，偽造 ARP パケットによる手法のように監視対象ホストのセグメントを考慮する必要がない．複数のセグメント設置された監視対象ホストに一括して対処することができる．また，この手法では宛先ホストを装って通常の TCP 通信を行うため，対象ホストにファイアウォールが導入されていても有効に機能すると考えられる．

## 4.5 能動型不正接続防止システム

以上の 3 つの機能を統合した能動型不正接続防止システムの構成を図 4 に示す．能動型不正接続防止システムは，「NAT 検出」，「不正 MAC 検出」および「無力化」の 3 つのモジュールから構成されている．

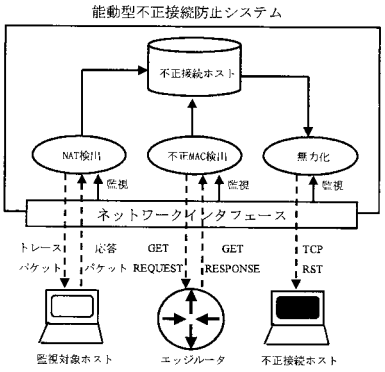


図 4: 能動型不正接続防止システムの構成

「NAT 検出」モジュールは先に示した能動的 NAT 検出手法で NAT 接続ホストを検出し，検出したホストを不正接続ホストに登録する．「不正 MAC 検出」は SNMP を利用して監視対象が接続するエッジルータの ARP テーブルを取得し，同じ IP アドレスに対応する MAC アドレスが一致していることを確認する．MAC アドレスに変化があった場合には不正接続とみなし，検出したホストを不正接続ホストに登録する．「無力化」モジュールはネットワークを流れるすべての TCP パケットを監視し，不正接続ホストの TCP パケットを検出した場合には，RST パケットを送信して強制切断する．試作したシステムのネットワーク上の動作位置は，監視対象のパケットがすべて傍受できる位置にする必要がある．

## 4.6 能動型不正接続防止システムの実装

提案システムを，C 言語を用いて実装した．実装したシステムのパケット処理の動作アルゴリズムを図 5 に示す．実装したシステムはインタフェースに到着するすべてのパケットをキャプチャし，監視対象ホストからのパケットを監視する．キャプチャしたすべてのパケットに対して以下の処理を実施する．まず，パケットの送信元 IP アドレスが不正接続ホストに該当するかを判定する．不正接続ホストに登録されたホストからの TCP パケットに対しては，RST パケットを送信し，接続を遮断する (無力化)．トレースパケットに対する応答パケットの場合は，記録してあるホップ数と比較し，ホップ数が一致しない場合はその送信元 IP アドレスを不正接続ホストに登録する (アクティブ NAT 検出)．次に，トレー

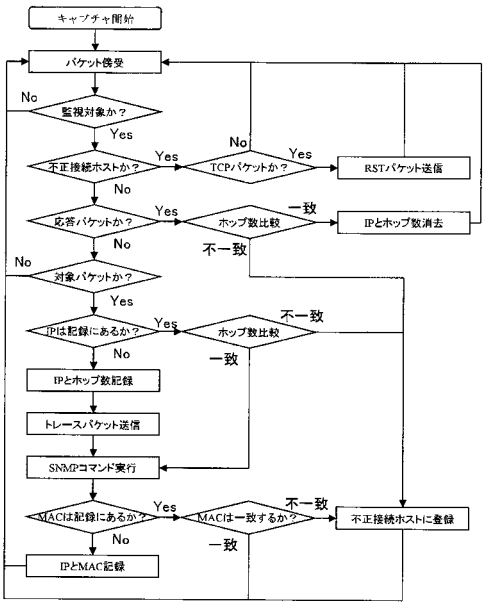


図 5: 能動型不正接続防止システムの動作アルゴリズム

スパケットを送信する対象パケットを限定する．対象パケットの限定は，トラフィックの増加量を制御するために必要である．抽出した対象パケットの送信元 IP アドレスが記録にない場合は，IP アドレスとホップ数を記録するとともにトレースパケットを送信し，SNMP コマンドを実行する．送信元 IP アドレスが記録にある場合はホップ数を比較し，ホップ数が一致しなければその送信元 IP アドレスを不正接続ホストに登録する (パッシブ NAT 検出)．ホップ数が一致した場合は，SNMP コマンドを実行する．最後に，SNMP コマンドを実行して MAC アドレスを取得し，記録してある MAC アドレスと比較する．MAC アドレスの記録がない場合は，その送信元 IP アドレスと MAC アドレスを記録する．MAC アドレスが一致しない場合は，その送信元 IP アドレスを不正接続ホストに登録する (不正 MAC 検出)．

# 5 検証実験

この章では試作したシステムについて検証実験を行い，不正接続ホストの検出を試みる．また，TCP 接続の強制切断の効果を確認する．

## 5.1 検出精度

提案システムと，セグメントごとに設置が必要な従来型システムの検出精度を比較する．実験に使用するネットワークの構成を図 6 に示す．各ホストおよびルータは 100BASE/T イーサネットで接続されており，固定の IPv4 アドレスが割り当てられている．監視対象はセグメント 2 のホスト A およびホスト B，セグメント 3 のホスト C およびホスト D とする．ホスト D は NAT によりホスト E を接続している．提案システムをセグメント 1 で動作させ，各ルータの snmpd を有効にする．従来型システムは，セグメント B およびセグメント C で動作させる．実験は次の手順で実施した．

1. ホスト A，B，C および D からホスト F に http で通信する．
2. ホスト A，B および C の MAC アドレスを変更する．
3. ホスト B，D および E は再びホスト F と http で通信する．
4. ホスト A についてはホスト B と，ホスト C についてはホスト D と http で通信する．

提案システムと従来型システムの検出結果は表 1 のとおりである．ホスト B の検出結果から，どちらのシステムもセグメント 1 を経由する通信からは不正接続を検出できることがわかる．しかし，試作したシステムではホスト A およびホスト C を検出できなかったことから，セグメント 1 を経由しない不正接続は検出できないことを確認した．このように，試作したシステムはセグメント内のローカル通信を監視することはできない．また，ホスト D の検出結果から，従来型システムでは NAT を利用した不正接続は検出できないが，試作したシステムでは検出することができることが確認できる．

表 1: 不正接続検出結果

| ホスト | A | B | C | D |
|---|---|---|---|---|
| 提案システム | × | ○ | × | ○ |
| 従来型システム | ○ | ○ | ○ | × |

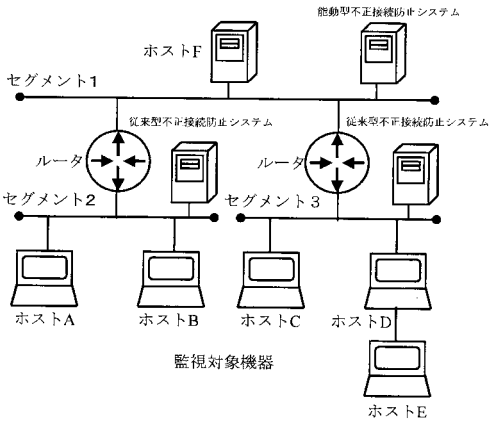


図 6: 実験ネットワークの構成

### 5.2 TCP 接続の強制切断

試作したシステムの TCP 接続の強制切断機能の効果を確認する．図 6 に示したネットワークにおいて，ホスト A，B，C および D からホスト F への接続の遮断を試みる．ホスト F へアクセスする際のプロトコルは http および ssh を使用する．ホスト C および D についてはファイアウォールを有効とし，アクセスに必要な最小限度のパケットのみの通過を許可する．ファイアウォールには WindowsXP については ICF (Internet Connection Firewall)，Linux については iptables を用いた．実験結果を表 2 に示す．各 OS においてファイアウォールが有効な場合にも，http および ssh のアクセスを遮断できることを確認した．

表 2: TCP 強制切断の実験結果

| ホスト | A | B | C | D |
|---|---|---|---|---|
| OS | Windows XP | Linux 2.6 | Windows XP | Linux 2.6 |
| Fire wall | ICF 無効 | iptables 無効 | ICF 有効 | iptables 有効 |
| 遮断 | ○ | ○ | ○ | ○ |

## 6 おわりに

本稿では，NAT による不正接続をも検出し，無力化することができる，能動型不正接続防止システムを検討した．また，能動型不正接続防止システムを試作し，検証実験により効果を確認した．試作したシステムは監視対象に依存せず，特別な機器やソフトウェアを必要としない．また，ネットワーク構成を変更する必要もなく，すべてのセグメントに設置する必要もない．しかし，無力化できるプロトコルは TCP に限定され，各セグメント内のローカル通信を監視および無力化することはできない．また，MAC アドレスの偽造等は検出することができない．試作したシステムは，大学等の様々なアーキテクチャや OS のホストが混在し，大規模で複雑なネットワーク等にも容易に適応することができる．したがって，大規模なネットワークでの専門知識を持たない一般のネットワーク利用者向けの対策として効果があるものと考えられる．

## 参考文献

[1] 三村 守，中村 康弘：TTL を用いた能動的 NAT 検出手法の実装と評価，情報処理学会論文誌，Vol.48，No.10，pp.3375–3385 (2007).

[2] intraPOLICE, http://www.lac.co.jp/business/sns/products/intrapolice/.

[3] 石橋 勇人，山井 成良，安倍 広多，大西 克実，松浦 敏雄：IP アドレス/MAC アドレス偽造に対応した情報コンセント不正アクセス防止方式，情報処理学会論文誌，Vol.40，No.12，pp.4353–4361 (1999).

[4] 齊藤 明紀，桝田 秀夫：ルータ上のパケットフィルタで端末間通信を処理するための DHCP サーバ構成法，情報処理学会論文誌，Vol.46，No.4，pp.1025–1034 (2005).

[5] 情報処理推進機構セキュリティセンター：TCP/IP に係る既知の脆弱性に関する調査報告書　改訂第 2 版，(2007).