# 不正パケット遮断システムの ユーザインタフェースに関する研究

05G470 長野 一樹 (最所研究室)

ネットワークに関するトラブルの中のひとつである情報流出の防止を目的とした不正パケットを自動的に遮断するシステムを提案し，そのユーザインタフェースについて述べている．IDS を用い，Snort の不正パケットパターンデータベースにて LAN 内からの上りパケットパターンをチェックし，不正パケットがあれば管理者へ通知・または該当 PC のパケット遮断を行う．本研究では，ネットワーク管理者の負担の軽減の為に視覚的な機能を提案し，ユーザインタフェースに関する部分の実現を目指す．

## 1 はじめに

LAN が広く一般化し大企業をはじめ，中小企業さらには家庭内にも浸透するようになった．企業などで構築された数十台，数百台規模の LAN 内でネットワークトラブルの原因になっている PC を見つけ出すのは非常に困難な状況になる．しかし，ネットワーク管理者には，ネットワークの仕組みや様々なトラブル事例など豊富な知識と経験を持ち，LAN 内部で起こっていることを想定してトラブルに対応しすみやかに解決への糸口を見つけ解決されることが要求され，大きな負担となっている．

その対策として，本研究では侵入検知システム (IDS) である Snort と L2 スイッチを用い，不正パケット遮断システムを構築する．これを用いてネットワーク管理者の負担の軽減し，ネットワーク関するトラブルの中のひとつである LAN 内からの不正なパケットの送信を防ぐ事を目的とした不正パケットを遮断するシステムを実現する事にした．本研究ではそのユーザインターフェイスとそれに付随するセキュリティポリシに関する部分の実現を目指す．

なお，パケット遮断を実現する機構については共同研究者の串間氏によって開発されている [1].

## 2 不正パケット遮断の概要

本システムのシステム構成を Figure 1 に示す．また，本論文中では LAN の管理をするネットワーク境界に置かれたシステムを NMC(Network Management Computer) と呼ぶ．

不正パケット遮断の概要を記述する．LAN 内の PC からの上りパケットが Layer 2 Switch(L2 スイッチ) を通りネットワーク境界にある NMC にてパケットパターンのチェックをされる．不正なパケットがあれば，その危険度に応じて L2 スイッチを用いて，そのパケットを発したホストからのパケットを遮断する．あるいは警告を発するなどの処理を行う．この時，不正パケットを発する PC 特定と遮断のために，NMC が IP アドレスを元に MAC アドレスを調べ，LAN 内の L2 スイッチに該当 PC のパケット遮断命令を送る．また，

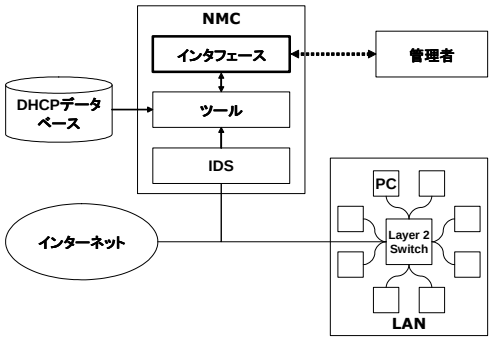


図 1: システム構成

NMC のパケットチェックには不正パケットデータベースを持つ Snort [4] を用いる．

本研究におけるユーザインタフェースは専門的な知識のいるネットワークの管理をより簡単に使いやすくするためのものであり，Figure 1 におけるインタフェースを実現する．

## 3 セキュリティポリシ

本研究ではセキュリティポリシとして，NMC が不正パケット発見時，情報の漏洩防止のためにユーザに対する自動で行う処理を提案する．

不正パケットには，すぐにパケット遮断すべき危険度の高いものや，それほど危険度の高くないものがある．前者は即時にネットワークから切断すべきだが，後者のそれほど危険度の高くない不正パケットを発する PC まで即時にネットワークから切断していては，ネットワーク管理者にとって負担増大に繋がる．

これを解決するためには，後者のそれほど危険度の高くない不正パケットを発する PC のユーザを NMC 内にログを残しておき，不正パケットを発し続けるようならば，ネットワークから切断することや，切断前には NMC から自動で不正パケットを発しないような対策を促す警告をユーザに知らせることなどが考えられる．

このことを実現するために，不正パケットを発する

ユーザに対する処理のレベルを3つに分類する (Figure 2)．これは，不正パケット検出時における処理を遮断タイミングとして各レベルにより，Snort の不正パケットデータベース [3] の危険度に基づく即時遮断の判断，規定回数，規定時間後の遮断の条件により分類するものである．

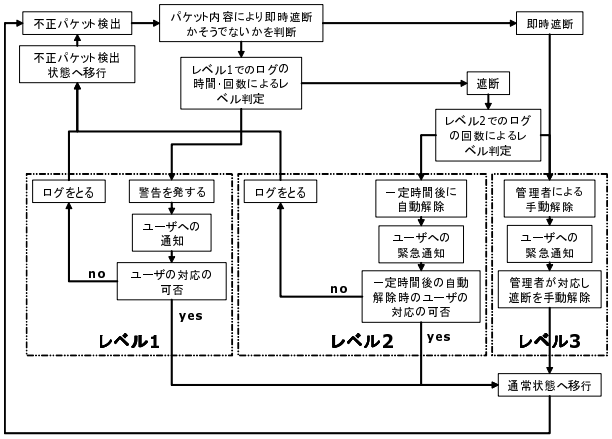


図 2: 処理レベル詳細

そして，LAN 内のユーザは各状態・各レベルをこのルールの下，NMC にリアルタイムで変更されている．

以上のような処理系を実装することによって，ユーザ自身で解決できるものと，ネットワーク管理者に頼らなければ解決できないものとに振り分けることができ，可能な限りユーザに不正パケット発信の防止を行わせ，管理者の負担を減らすことが出来る．

## 4　グラフィカルなインタフェースの実現手段

本研究における，ユーザインタフェースに求められるものは，視認性・操作感もちろんのこと，わかりにくいネットワークに関する情報をいかにわかりやすくするかにある．また，操作がより直感的なグラフィカルな表現を用いることで，ネットワーク管理者の負担を軽減させる．

本研究では Flash を用いる．実現手段として Flash を用いることの利点は，NMC 上に Flash ファイルを置くことにより，LAN 内の PC に全てに専用のサーバソフト，クライアントソフトをインストールする必要がなく，ブラウザで LAN 内のどの PC からでも NMC に置かれた Flash にアクセスできるようになる．また，動的でグラフィカルなコンテンツの作成に強く，ユーザが NMC に対して行った動作の結果をリアルタイムで反映させることができる．

## 5　ユーザインタフェースの各機能

より簡単に使いやすくするための，本研究におけるインタフェースにて必要な機能として，条件による自動パケット遮断とその条件変更機能，またそのパケット遮断の自動解除，NMC にて対応できなかった場合に管理者が手動でのパケット遮断や，管理者の指示による手動解除，例外パケット登録機能，自動通知機能，LAN 内のユーザを管理するためのユーザの登録機能，不正パケットを発した際にグラフィカルに管理者へ情報を提供するためのマップ表示機能 [2]，ユーザの不正パケット発信履歴を残すためのログ機能，ログ情報をもとにしたグラフ機能，LAN 内のユーザを一覧を検索するためのデータベース検索機能を提案する．

## 6　まとめと今後の課題

本研究では，セキュリティポリシの策定，インタフェース機能の提案と作成を行った．セキュリティポリシに策定では，各ユーザに対する Snort の不正パケットデータベースの危険度に基づく処理レベルの決定，携帯電話へのメールの自動送信，そして不正パケットの例外パケット登録について提案した．インタフェース作成では，一見してわかりにくいネットワーク状況を PHP との連携が容易な Flash を用いて視覚的にわかりやすいインタフェースを作成し，必要機能を提案した．ユーザフレンドリなインタフェースの実現のため，マップ表示，データベース検索，システムのログ情報のグラフ化などを提案した．

今後の課題として，本システムをよりユーザフレンドリなものとする為，様々なユーザに実際に利用してもらい，必要機能の追加や不必要な機能の削除やメニュー画面の構成など，管理者やユーザからの意見を参考にユーザインタフェースの調整も必要である．

## 参考文献

[1] 串間竜治, “レイヤ 2 スイッチを用いた不正パケット遮断システムの研究”, 香川大学大学院工学研究科修士論文, 2006 年.

[2] 吉岡梅, “Flash 8”, ソーテック社, 2006 年.

[3] Snort.ORG, “Snort - the de facto standard for intrusion detection/prevention”, http://www.snort.org/, 2007 年 2 月 19 日.

[4] 日本 Snort ユーザ会 (Japan Snort Users Group), “日本 Snort ユーザ会”, http://www.snort.gr.jp/, 2007 年 2 月 3 日.