ファイアウォールシステムの更新について

山口由紀子　河口信夫

Ⅰ．はじめに

名古屋大学の学内 LAN 名古屋大学キャンパス情報ネットワーク（以下，NICE と呼ぶ）とインターネットを接続するファイアウォールシステムは，平成 13 年度の NICE Ⅲの構築の際に設置したものである。ファイアウォールシステムはこれまで学外からの危険な通信を遮断することで NICE の安定運用に貢献してきた。しかしながら，設置から 4 年が経過し，NICE 内のウィルスに感染したパソコンが大量のスキャンパケットを発生したり，学外から NICE 内の特定の端末に対して大量のパケットが送信されたりしてファイアウォールシステムが過負荷となってダウンするなど，ファイアウォールシステムの能力不足が顕在化してきた。ファイアウォールシステムがダウンしてしまうと，NICE とインターネットとの通信ができなくなるため，学内のネットワーク利用者への影響が大きい。

そこで，情報連携基盤センターでは平成 17 年度総長裁量経費に申請して採択され，ファイアウォールシステムを更新することになった。新しいファイアウォールシステムは，ネットワーク装置とそのアクセスリストを管理するシステムで構成されている。本稿では新しいファイアウォールシステムの詳細について紹介する。

Ⅱ．現在のファイアウォールシステムと問題点

図 1 に現在のファイアウォールシステムの構成を示す。設計当時（平成 13 年）はギガビット対応の高性能なファイアウォールシステムが存在していなかったため，ワークステーションにファイアウォールソフトウェア（FireWall-1）を搭載したシステムを並列に配置することでスループットの向上を図った。さらにＦＷ 4 台を並列で利用するための負荷分散装置も併せて導入したため，結果として多数の装置を組み合わせた複雑な構成となってしまった。

ファイアウォールシステムは，設置以来，全学メール受信サーバと連携した SMTP（電子メール送信プロトコル）の遮断，ウィルス感染サーバとの通信遮断など，NICE の安定運用に貢献してきた。しかし，設置からほぼ 4 年が経過し，インターネット環境の高速化や接続端末の高性能化に伴ってファイアウォールシステムの性能不足が顕在化してきた。NICE 内のウィルスに感染した端末が大量のパケットを発信して負荷分散装置やファイアウォールシステムのメモリ枯渇が発生し，NICE がインターネットと接続できなくなるという障害がしばしば発生した。最近の事例を調査したところ，平成 16 年 4 月以降は，セキュリティホールを狙った学外からの大量のポートスキャンや，NICE 内の特定の端末への集中的なアクセスなど，学外からの攻撃が原因となっ

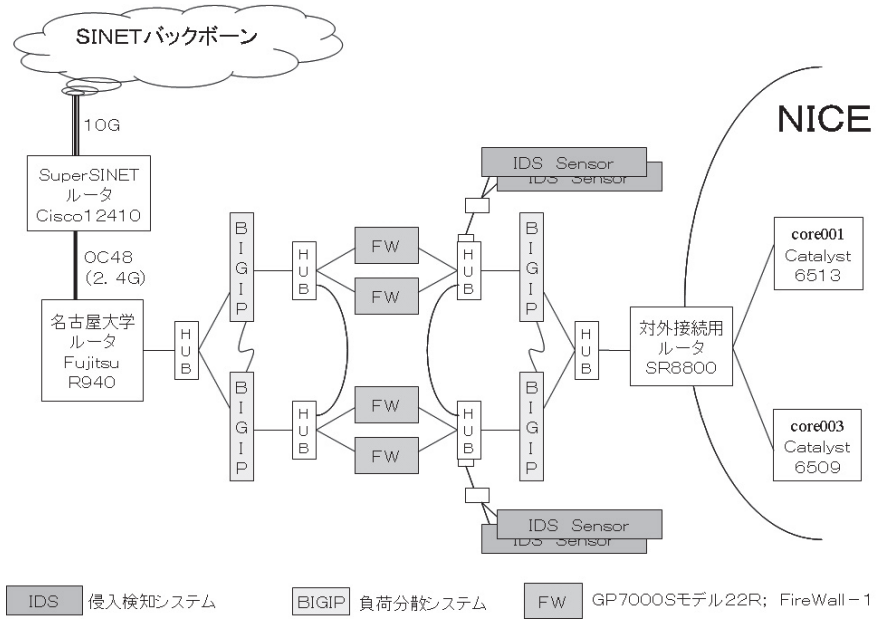

図１　現在のファイアウォールシステム構成図

た障害が 15 件も発生していた。このような状況から名古屋大学は国立情報学研究所が提供しているスーパー SINET に接続しているが，ファイアウォールシステムがボトルネックとなってスーパー SINET の高速回線を十分に利用できていないことがあきらかとなった。そこで情報連携基盤センターでは，平成 17 年度総長裁量経費に応募し，採択されたことからファイアウォールシステムを更新することとなった。

Ⅲ．新しいファイアウォールシステム

新しいファイアウォールシステムは単純なスイッチとそのアクセスリストを管理するためのサーバで構成することにした。また，NICE から SINET ルータまでのすべての接続を二重化してトランクすることによりボトルネックの解消を図ることにした。

図２に新しいファイアウォールシステムの構成を示す。ファイアウォール装置としてレイヤ３スイッチ Catalyst3750 を利用する。今回の更新に併せて，NICE とファイアウォールとを接続する対外接続ルータについても同じく Catalyst3750 に更新する。また，SINET と名古屋大学を接続するルータも更新する予定であることから，NICE の基幹ルータ（core001，core003）から SINET ルータまでのすべての接続を直接ギガビット２回線で接続し，各スイッチでそれらをトランクすることにより，２ギガビットの回線速度を実現する予定である。

従来のファイアウォールシステムはファイアウォールソフトウェア（FireWall-1）を利用していたため，通信の遮断や解除を行うためのアクセスコントロールのポリシー記述はソフトウェアが提供する GUI を利用して行ってきた。図３に FireWall-1 でのポリシー記述の例を示す。この GUI では同種のポリシーをまとめて記述したり，コントロール対象のアドレスやポートをグルー

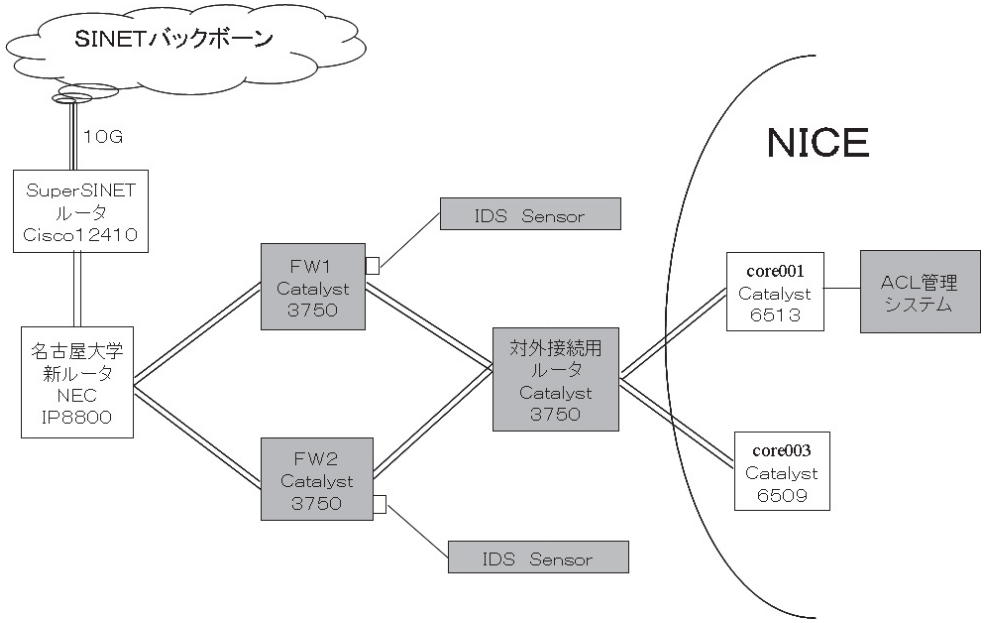

図２　新ファイアウォールシステム構成図

プ化して記述できるため，アクセスコントロールの管理を容易に行うことができる。図４にグループの詳細記述例を示す。ここでは Windows の NetBIOS 関連のプロトコルをグループ化してまとめて遮断するための記述を行っている。

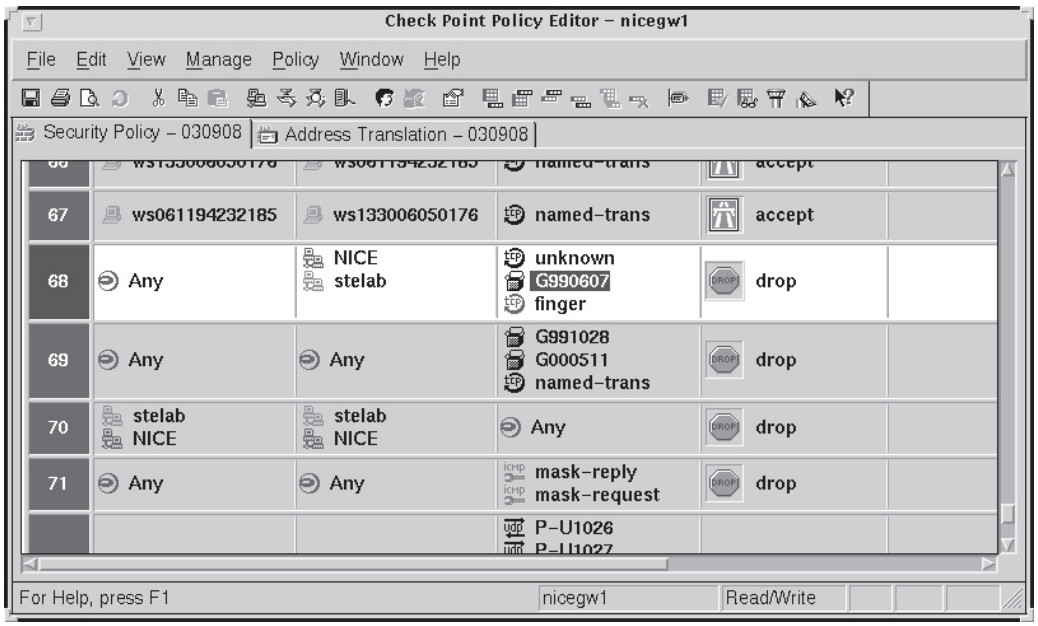

図３　FireWall-1 でのポリシー記述例

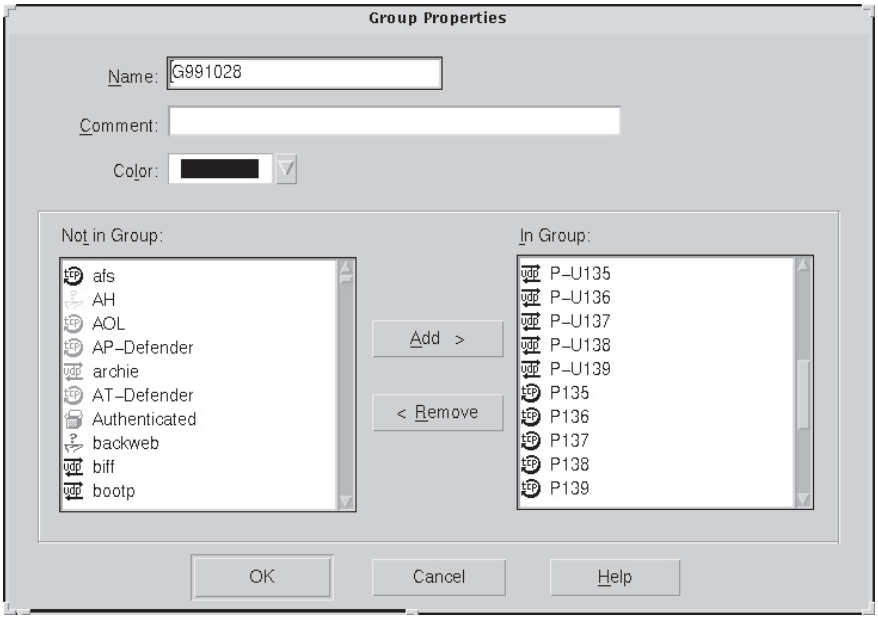

図４　グループ G991028 の記述

一方，今回ファイアウォールシステムとして導入する Catalyst3750 は純粋なスイッチであるため，アクセスコントロールのポリシー記述のための GUI などのツールが提供されないだけでなく，アクセスコントロールのすべてをスイッチ固有の管理コマンドで記述する必要がある。スイッチの管理コマンドではグループ化などの機能がないため，発信元，受信先，プロトコル（ポー

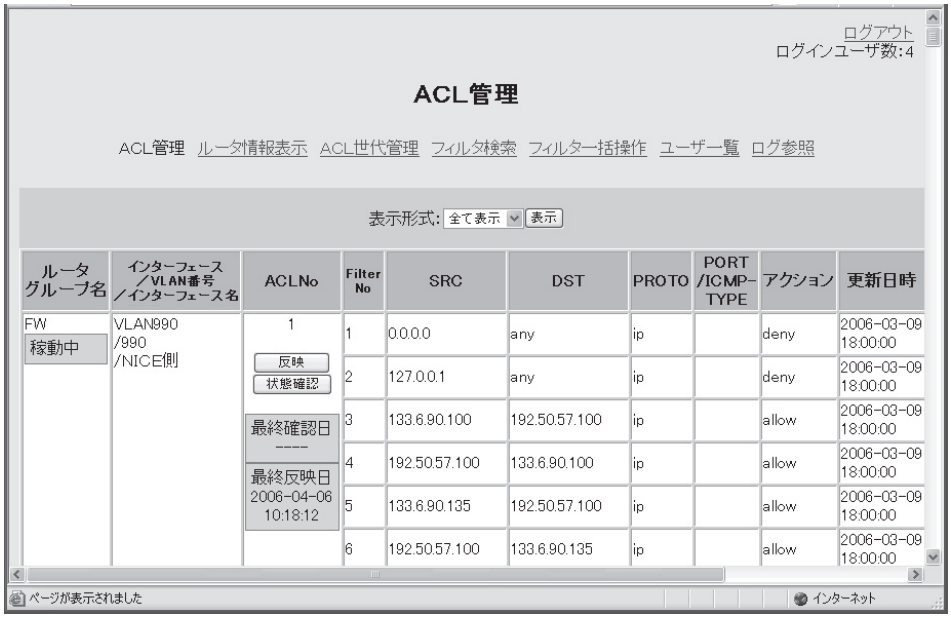

図５　ACL 管理サーバでのポリシー記述例

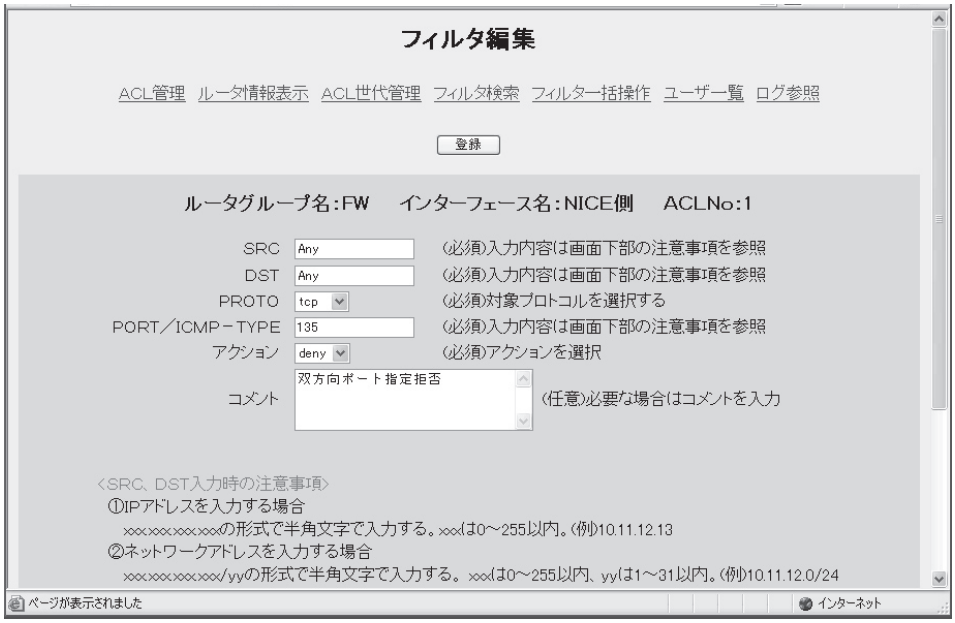

図６　フィルタ記述例

ト）のすべての組み合わせについて詳細に書き下す必要がある。

複雑なアクセスコントロールを正しく設定するためには，アクセスコントロールリストを管理するためのツールが不可欠となる。そこで今回の更新では，アクセスコントロールリスト管理システム（以下，ACL 管理システム）も併せて導入することとなった。図５に ACL 管理システムでのポリシー記述例を示す。

なお, 今回実現する ACL 管理システムは, ファイアウォールシステムのみを対象としているが, 将来的には NICE 内のすべてのスイッチを管理する予定である。

Ⅳ．おわりに

新しいファイアウォールシステムの構成について紹介した。原稿執筆現在は，機器の手配とアクセスコントロールリスト管理ソフトウェアの開発を行っている段階である。年度末（平成 18 年３月末）にはすべての装置，機能が実現され，テスト運用を行った後に現在のファイアウォールシステムと切り替える予定である。

（やまぐち　ゆきこ：名古屋大学情報連携基盤センター情報基盤ネットワーク研究部門）
（かわぐち　のぶお：名古屋大学工学研究科電子情報システム専攻
前名古屋大学情報連携基盤センター情報基盤ネットワーク研究部門）