ポート番号に基づく透過的なパケットフィルタに関する研究

本村　真†,寺澤　卓也†
東京工科大学メディア学部†

1. はじめに

近年、インターネットの普及とともに、教育機関においてはネットワークを用いた授業が増加している。ところが、実際にはかなりの数の学生が授業中に授業とは関係のないネットワーク利用をしている。

これらの不要なネットワーク利用は、学生が授業に集中するのを妨害し、また、ネットワークトラフィックの増大を招く。授業でネットワークを利用する際の妨げにもなる。

そこで、教室で教員がノートパソコンなどからパケットフィルタの設定 Web ページにアクセスし、フィルタリングのルールを変更することによって、ネットワークのアクセスコントロールを可能にするシステムを提案する。また、クライアントでの特別な設定を不要とするために、パケットフィルタリングを行うシステムを、透過型の構成とする。

2. 透過型システムの実現

ここで言う透過型システムとは、そのシステムがネットワーク上において、ノードとして存在するのではなく、線の一部として存在するということである。

透過型の利点は、クライアント PC 側に設定を必要とせず、またアクセス制御をされていると意識させないアクセス制御を可能とすることである。

透過型システムを構成する方法としては PC をブリッジにする[1]、Squid による透過型プロキシサーバを用いる[2]、L4 スイッチと組み合わせる[3]などの方法がある。

本研究では、次に述べる要因のため、ブリッジを用いて透過型システムを構築する。

3. パケットフィルタ

現在、パケットフィルタリングソフトウェアには、Linux などの UNIX 系の OS に対応している、ipfwadm や ipchains や iptables などが存在する。それ以外にも、パケットフィルタに対応したファイアーウォールやプロキシサーバなどが存在する。本研究では、Linux の最新カーネルに対応していること、Web プロキシサーバである squid では Web クライアントのパケットフィルタは可能でもネットワークゲームなどのパケットフィルタは不可能なことから、パケットフィルタリングには iptables を用いる。

4. システムの実装

本研究で提案するシステムは、教室毎に設置されることを前提としている。これを、Linux PC で実現する。

VineLinux2.5 をインストールした PC を用意し、そして、ブリッジ動作中にパケットフィルタリングを可能にするためのパッチ[4]をカーネルにあて、ブリッジを有効にしてカーネルを再構築した。また、Linux 上で実際にブリッジを行う仮想インターフェイスを作成する bridge-utils[4]というツールをインストールした。

パケットフィルタリングは、iptables でフィルタリングルールの生成を行う。また、フィルタリングルールの設定を、Web ベースで行えるように CGI で用意した。CGI は C 言語で作成した。

図 4.1：設定ページ

CGI で作成した設定ページを図 4.1 に示す。このページは、最低限の設定を行う初期設定ページ、ポート番号や宛先などから設定を行う個別設定ページ、特定のアプリケーションの設定を

Research on a transparent packet filter based on port numbers
†Makoto MOTOMURA, Takuya TERASAWA
†School of Media Science Tokyo University of Technology

行うアプリケーション設定ページ、現在のフィルタリングルールを表示するページ、フィルタリングルールを初期化するページの４つから構成した。

5．実験

実装した透過型アクセス制御システムについて評価実験を行った。

まず、最小限のネットワーク環境で FTP サーバから、1 台のクライアント PC を用いて 500MB のファイルを 5 回転送しその平均スループットを計測した。これにより、システムが設置されたネットワークのスループットに、システムがどれくらい影響を与えるかどうかを調べる。その結果、システムを用いてもネットワークのスループットには運用する際に影響が出るほどではなかった。

次に、アクセス制御の検証を行った。その結果、遮断したいアプリケーションが使用しているポート番号が分かれば、遮断することは簡単であることが分かった。

最後に、CGI で作成した設定ページは、ページの説明を見てパケットフィルタを設定できるかを調査した。調査結果は表 5.2 に示す。

表 5.1：アンケート結果

	強く思う	そう思う	どちらでもない	あまり思わない	強く思わない
①	4	3	1	0	0
②	3	2	3	0	0
③	4	3	1	0	0
④	7	1	0	0	0

①初期設定ページの説明を見て、初期設定をすることができた
②個別設定ページから、許可（拒否）したいポートや IP アドレスを設定できた
③アプリケーション設定ページから、特定のアプリケーションの許可（拒否）を設定ができた
④設定されたルールが有効に適用された

以上のことから、個別設定のページの説明に問題があり設定を行いづらかったと考えられるが、他のページに関しては問題なく設定を行うことができ、その設定が有効に適用されたと全員が感じたことが分かった。

6．まとめ

本論文ではブリッジを用いた透過型パケットフィルタリングによる簡易なアクセス制御システムを提案・実装した。

しかし、今回実現させたシステムだけでは、本学の教室のようなネットワーク設定において、完全なパケットフィルタリングによるアクセス制御は行われない。なぜかならば、Web プロキシサーバを通るパケットをフィルタリングができないからである。Web プロキシサーバを通るパケットは、デスティネーションアドレスがプロキシサーバのアドレスになっているため、学外のサイトへのアクセスのみを制限するようなフィルタリングができない。

また、HTTP トラフィックに関しては、他のプロトコル同様 IP アドレス及びホスト名でのフィルタリングは可能であるが、iptables の仕様で URL でのフィルタリングは不可能である。

Web プロキシサーバを通るパケットのフィルタリングを行うには、パケットの TCP データ部分を解析する必要がある。これは URL がパケットに内包されているため、パケットを解析し URL を取り出すことが可能になれば、これを用いて URL でのフィルタリングも可能になると考えられる。方法としては、Linux カーネルのパケットフィルタリングを行っている部分を改造することが考えられる。他には、iptables のコマンドの１つで、ユーザ空間にパケットを引き出すことができる queue コマンドを用いてパケットをユーザ空間に引き出し、TCP データ部分を解析する方法が考えられる。

今後の課題は、このプロキシサーバを通るパケットのアクセス制御を可能にし、同時に URL 指定でのアクセス制御も可能にすることである。

参考文献

[1] cutie：『LinuxBOX をブリッジとして動かす』（http://cutie.dip.jp/pc/linux/bridge/）.

[2] 早川　仁：『squid による透過型プロキシ』（http://www.linux.or.jp/JF/JFdocs/TransparentProxy.html）.

[3] 伊藤　求,伴　好弘,鳩野 逸生：『透過プロキシーシステムを用いた HTTP フィルタリングの効果について』（情処研報 Vol.2002, No.95, 2002-DSM-27, pp.43-46, Oct. 2002）.

[4] buytenh：『bridge - Linux ethernet bridging』（http://bridge.sourceforge.net/）.