ユーザレベルでの動的ファイアウォール管理支援システムに関する研究

04G475　矢原 雅俊　（最所研究室）

本研究では、ネットワークサーバを一元管理するネットワーク管理支援システムの技術を応用した、ユーザレベルでの動的ファイアウォール管理支援システムの開発を行う。本システムを用いる事で、DHCP サーバで IP アドレスが割り当てられるホストのファイアウォールの設定を動的に行う事が出来る。

1　はじめに

ネットワークセキュリティを向させる方法の一つにパケットフィルタリングがある。WAN と LAN の間に Firewall サーバを置き、そこを通過するパケットのヘッダ情報を検査し、通過させるかを判断する。DHCP サーバから IP アドレスを取得するようなネットワーク環境においては、IP アドレスは毎回変わってしまうので、ユーザ毎にパケットフィルタリングの設定を行うことできない。DHCP サーバのログ情報には IP アドレスと MAC アドレスの対応情報が記述されている。そこで事前にユーザと MAC アドレスの対応関係を管理しておけばユーザを特定することができる。さらに、事前にユーザ毎のパケットフィルタリングの情報を情報として管理しておけば、ユーザ特定後 Firewall サーバに反映することができる。

そこで、本研究ではユーザレベルでの動的ファイアウォール管理支援システムの開発を行った。本システムは、高橋巧氏 [1] と共同研究で行った際に得た技術を利用して開発した。具体的には、情報管理とユーザインタフェースの技術を利用した。

2　システムの設計と概要

システムの構成を図 1 に示す。本システムでは、事前にユーザがデータベースである情報管理サーバに、MAC アドレスとユーザ名の対応情報、フィルタリング情報を登録しておく。ユーザがネットワークに接続すると、DHCP サーバのログファイルからユーザの IP アドレスと MAC アドレスが判明する。事前に登録しておいた MAC アドレスとユーザ名からフィルタリング情報を検索し、Firewall サーバに反映する。

3　情報管理サーバ

本システムでは、情報管理サーバとして関係データベースである MySQL を用いる。管理情報を以下に示す。

- ユーザ情報
  ユーザ名、パスワード、メールアドレス

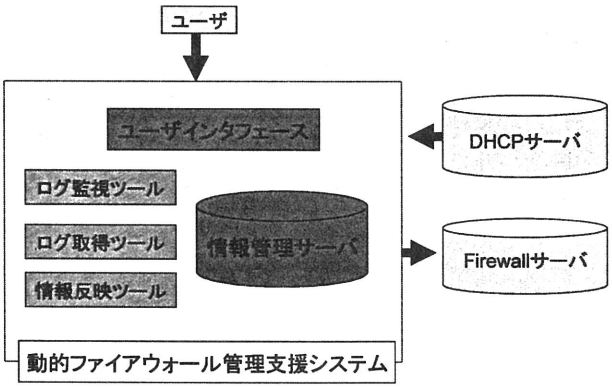

図 1: システム構成図

- MAC アドレス情報
  MAC アドレス、ユーザ名
- DHCP ログ情報
  MAC アドレス、IP アドレス、IP アドレス貸しだし開始時間、IP アドレス貸しだし終了時間、以前の IP アドレス貸しだし終了時間
- フィルタリング情報
  ユーザ名、チェイン、プロトコル、IP アドレス、送信先ポート番号、送信元ポート番号、ターゲット、管理者が指定したターゲット、アプリケーション名
- アプリケーション情報
  アプリケーション登録ユーザ、アプリケーション名、プロトコル、送信先ポート番号、送信元ポート番号
- 反映待ち情報
  ユーザ名、チェイン、プロトコル、IP アドレス、送信先ポート番号、送信元ポート番号、ターゲット、管理者が指定したターゲット、アプリケーション名
- 管理ポート情報
  プロトコル、ポート番号、使用不可ユーザ

アプリケーション情報とは、アプリケーション毎に使用するプロトコルやポート番号の情報である。この情報を用いることにより、ユーザがアプリケーションを指定するだけでフィルタリング情報を設定できる。反映待ち情報とは、ユーザが新たにフィルタリング情報を設定した時に、Firewall サーバに反映されるまで管理される情報である。管理ポート情報では、ユーザ毎に設定可能なプロトコルとポート番号を管理している。これによりユーザのレベルに合わせて、使用できるポートの範囲を制限することができる。

4 自動更新システム

本システムでは、Firewall サーバに Netfilter[2] を用いている。iptables コマンドを利用する事で、Netfilter の設定を変更することができる。図 2 にコマンドの例を示す。この例では、192.168.1.9 というマシンに対して、WWW(tcp の 80 番ポート) と DNS(udp の 53 番ポート) の利用許可を示している。

```
1:    iptables -P FORWARD DROP
2:    iptables -A FORWARD -p tcp -s 192.168.1.9 --dport 80 -j ACCEPT
3:    iptables -A FORWARD -p udp -s 192.168.1.9 --sport 53 -j ACCEPT
4:    iptables -A FORWARD -p udp -s 192.168.1.9 --dport 53 -j ACCEPT
```

図 2: iptables コマンドの例

4.1 DHCP ログの監視

本システムは、ユーザが DHCP サーバに IP アドレスを割り当てられた時に、フィルタリングの設定を有効にする。対象とした DHCP サーバは、ユーザに貸し出した IP アドレスと MAC アドレスの情報を、リースファイルとして dhcpd.leases (以降 ログファイル) に記録している。本システムでは、tail -f コマンドを用いることにより、ログファイルに追加された部分を取り出している。

DHCP サーバは、ログファイルのデータサイズが大きくなると、ログファイルを dhcpd.leases~ という名前に変更し、新たに dhcpd.leases を作成する。UNIX システムでは、名前の変更が起こっても tail -f コマンドは元のファイルを見続けてしまう。この様な状況を回避するためにログファイルを監視し、変更された場合は tail -f コマンドを再起動する。

4.2 DHCP ログ解析

本システムでは、ログファイルで現在割り当てられている IP アドレスと MAC アドレスの情報を情報管理サーバで管理する。これらの情報に基づき、設定を有効にするべきユーザと無効にするべきユーザを判断する。

ログファイルを解析することで、ユーザの IP アドレス、MAC アドレス、貸し出し開始時間、貸し出し終了時間を取得する。取得した情報を元に情報管理サーバに問い合わせる。問い合わせの結果、ログ情報に自分の MAC アドレスが管理されていなければ新規に登録する。また、問い合わせた結果、自分の MAC アドレスがあった場合貸し出し延長の可能性がある。この場合は、今回の貸し出し開始時間と前回の貸し出し終了時間を比較する。DHCP サーバは、貸し出し終了時間の少し前に貸し出し延長を行う。そのため、貸し出し延長の場合は、今回の貸し出し時間が前回の貸し出し終了時間より前の時刻を記録している。貸し出し延長の場合は、時間に関する情報だけを更新しておく。同時に貸し出し終了ユーザの情報、反映待ち情報も取得する。以上の情報を反映する。

4.3 情報反映

本システムでの情報反映は、ログファイルが更新された際に行う。新規で IP アドレスを割り当てられた場合、ユーザの DHCP ログ情報を新規で情報管理サーバに追加し、フィルタリング情報を Firewall に反映させる。その際、すでに貸し出しが終わっている IP アドレスに関する、情報管理サーバに登録されている DHCP ログ情報を削除する。また、反映待ち情報も同様にこの段階で反映する。

IP アドレス貸し出し延長の場合、貸し出しを延長する IP アドレスの時間に関する DHCP ログ情報のみを更新し、貸し出し終了 IP と反映待ち情報の処理を行う。

5 まとめ

本研究では、ネットワークサーバを一元管理するネットワーク管理支援システムの開発で得られた技術を用いて、ユーザレベルでの動的ファイアウォール管理支援システムを開発した。また、それを利用することで Firewall サーバの情報を動的に更新することができた。

今後の課題としては、1 台の PC に対して複数のユーザがいる場合の支援などについても検討していく。

参考文献

[1] 高橋巧, “ネットワーク管理支援システムのユーザインタフェースに関する研究”, 香川大学工学部卒業論文集, 2006.

[2] サーバ構築研究会,“Red Hat Linux8 で作るネットワークサーバ構築ガイド 8.0 対応,” 秀和システム, 2003.