ファイアウォール設定支援システムの構築

01T222　串間竜治（最所研究室）

ファイアウォールは、現在セキュリティにおける重要なシステムとなっている。本研究では、ファイアウォールの設定の負担を軽減させるシステムの設計と実装を行った。

1．はじめに

現在、インターネットの普及率は急増しており、2003 年末には国民の 6 割以上がインターネットを利用したことがあると報告されている[1]。しかしそれに伴い、PC に進入しデータを盗む、Web を改ざんするなどの不正アクセスや、様々な活動を行うコンピュータウイルスの被害も増加している。
不正アクセスや、コンピュータウイルスに対処する方法の一つとして、不要なパケットを遮断するファイアウォールがある。ファイアウォールは一般に(1)全てのパケットの通過を禁止し、必要なものだけを許可する方法と、(2)全てのパケットの通過を許可し、不必要なものだけを禁止する方法がある。安全性の面から(1)を用いるほうが好ましいのであるが、必要なアプリケーションごとに個別に設定する作業は煩雑な上、特に初心者にとって、自分の利用したいアプリケーションを動作させるには、どのように設定すれば良いかわからないことが殆どである。さらに、新たなアプリケーションを利用する場合、この面倒な作業を繰り返さなければならない。だからといって、必要でないものまで許可してしまえば、ファイアウォールの意味がなくなってしまう。このように安全性と利便性は相反するものである。そこで、本研究ではユーザフレンドリなインタフェースを用意し、わかりやすく、簡単にファイアウォールの設定ができるシステムの開発を目指す。本論文でするシステムは、Red Hat Linux[2]の Netfilter (iptables)[3]の設定支援を目的とし、インタフェースをとして Web を用い、それを制御するために PHP[4]を利用する。また、データ管理のためのデータベースに MySQL[5]を使用する。

2．パケットフィルタリング

Red Hat Linux では、Netfilter と呼ばれるパケットフィルタリングを行う手段が提供されている。IP パケットフィルタルールを設定・管理・検査するために使われるコマンドが iptables である。iptables は、個々のルールを 1 つずつ Netfilter に反映させる。次に示す例は、基本的に全てのパケットを遮断するが、例外的に通過させるパケットを指定するものである。通過させるものは、WWW サービス(TCP の 80 番ポート)、FTP サービス(TCP の 20 番、21 番ポート)とする。なお、以下の例はコマンドで入力した場合のものである。

```
# iptables -P INPUT DROP     (1)
# iptables -P FORWARD DROP   (2)
# iptables -P OUTPUT DROP    (3)
# iptables -A INPUT -p tcp --dport 80 -j ACCEPT (4)
# iptables -A OUTPUT -p tcp --sport 80 -j ACCEPT
                                                (5)
# iptables -A INPUT -p tcp --dport 20:21 -j ACCEPT
                                                (6)
# iptables -A OUTPUT -p tcp --sport 20:21 -j
ACCEPT (7)
```

(1) INPUT チェインのポリシーは DROP
(2) FORWARD チェインのポリシーは DROP
(3) OUTPUT チェインのポリシーは DROP
(4) 外部から入力される 80 番ポート宛の TCP プロトコルの許可
(5) 内部から出力される 80 番ポートからの TCP プロトコルの許可
(6) 外部から入力される 20 番、21 番ポート宛の TCP プロトコルの許可
(7) 内部から出力される 20 番、21 番ポートからの TCP プロトコルの許可

3．設定ファイルの書式

iptables の設定ファイルは、/etc/sysconfig/iptables に保存されている。ファイルの書式は単純で、以下の2パターンのエントリを追加する順に記述するだけである。

```
:<chain> <policy>          (1)
<iptables command line>    (2)
```

(1) チェインに対するポリシーを設定する。例えば、<chain>に INPUT などのチェインを、<policy>に ACCEPT などの指定する。
(2) iptables に与えるコマンドラインそのものを設定する。

2 章の例で保存されるファイルの内容は以下のとおりである。

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
-A INPUT -p tcp --dport 80 -j ACCEPT
-A OUTPUT -p tcp --sport 80 -j ACCEPT
-A INPUT -p tcp --dport 20:21 -j ACCEPT
-A OUTPUT -p tcp --sport 20:21 -j ACCEPT
COMMIT
```

4．システム構成

提案するシステムは、初心者でも簡単にファイアウォールを設定できることを目標としている。例えば、アプリケーションを指定するだけで、そのアプリケーションの使用するポートを自動的に開く機能を持たせる。熟知しているユーザのために、個別にポートを開くことができるようにもする。さらに、管理者用にアプリケーションとポート番号の対応データベースを編集できるようにする。

ユーザがユーザインタフェースを提供しているPHPへアクセスすると、PHPはデータベースであるMySQLへのアクセスを開始する。アクセスに成功すると、PHP は現在必要な情報またはデータベースの操作をSQL文としてMySQLへ問い合わせ、MySQLはPHPに結果を返す。PHPはその情報を整理し、必要に応じてユーザに提供したり、ファイアウォールの設定を変更したりする(図1)。

ユーザはファイアウォールの設定の確認・追加・削除ができ、管理権限がある場合は、アプリケーションのポート一覧データベースを変更することができる(図2)。

データベースに登録されているテーブルは、applicacion, config, usrと3つあり、それぞれアプリケーションのポート情報、ユーザのファイアウォールの設定情報(以後ユーザ設定と呼ぶ)、ユーザとIPアドレスの対応を保存している。このうちユーザが設定できるものはconfigのみである。

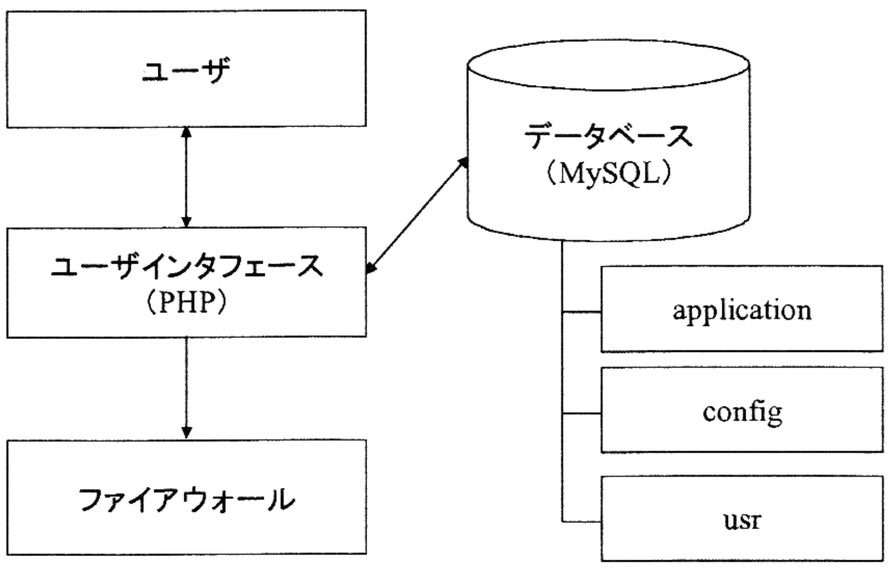

図1 システムの構成図

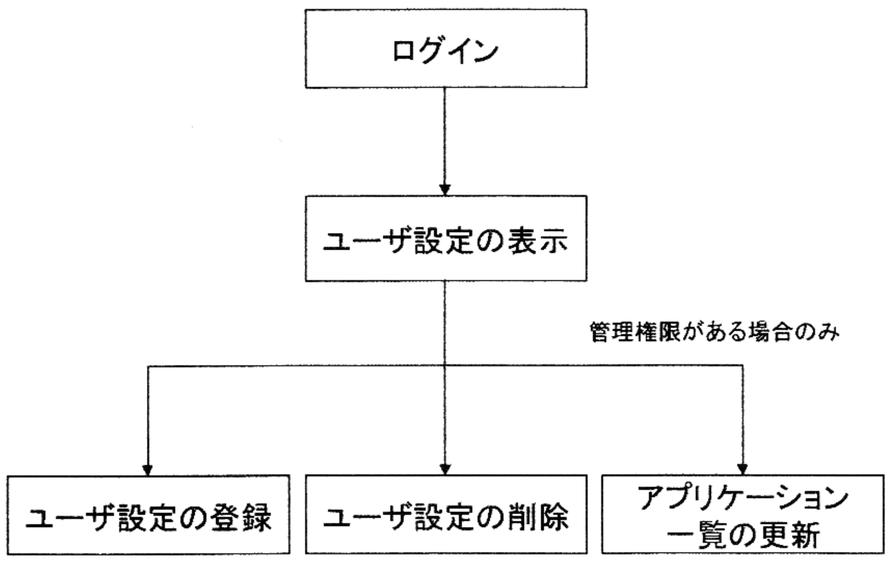

図2 システムの機能

5．ワークフロー

システムの機能のうち、ユーザ設定追加、アプリケーション一覧の更新を記述する。

5．1 ユーザ設定の登録

ユーザ設定の登録では、まずapplicationテーブルへアクセスし、登録されているアプリケーションの一覧をセレクトボックスに表示する。ユーザは、目的のアプリケーションがあればそれを選択し、アプリケーション追加ボタンを押すだけで設定できる。もし無ければ、個別にポート番号などを追加するフォームを用いて設定する。個別の設定には、かなりの知識を要するので、上級者向きになってしまう。初心者にはこのような場合、自分から設定できないことが生じる。これについては管理者との連絡手段を用意するなどが考えられるが、現時点では検討の段階である。

ここから送信された設定情報は、configテーブルへユーザのIPアドレスとともに記録され、iptables設定ファイルも更新する。

5．2 アプリケーション一覧の更新

アプリケーション画面一覧へは、ユーザレベルが管理権限である場合に進むことができる。ここでは、application テーブルへアクセスし、そのまま一覧を表示する。また、削除のためのボタンと、新たに追加するためのフォームも表示する。アプリケーション一覧が、更新された場合 application テーブルへ追加または削除される。

6．設定ファイルの自動生成

設定ファイルは、config テーブル、application テーブルの情報から生成する。まずconfigテーブルから、個別にポートを追加しているものを、設定ファイルの書式に従い出力する。次に、アプリケーションをキーに追加したものは、どのようなものがあったかを配列に保存しておき、そのアプリケーションの情報を application テーブルから探し出力する。

7．まとめ

本研究では、ファイアウォール設定支援システムとして、アプリケーションを選択するだけでポートを開くことのできるシステムを構築した。実装できなかった部分として、アプリケーション一覧の検索、複雑な設定、サービスの再起動があげられる。

参考文献

[1] 総務省, http://www.soumu.go.jp/
[2] RedHat, http://www.jp.redhat.com/
[3] サーバ構築研究会, Red Hat Linux 8 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年
[4] 日本PHPユーザ会, http://www.php.gr.jp/
[5] 日本MySQLユーザ会, http://www.mysql.gr.jp/