ネットワーク接続申請・登録システムの開発

平山かほる（工学部　技術部情報システムグループ）

1 はじめに

2003 年 4 月より学内において情報セキュリティポリシーが施行され、ウィルス等により引き起こされるネットワーク障害の原因となる PC を学内ネットワークから排除しなければならなくなった。学内にネットワーク障害を起こす PC が発生した場合、総合情報処理センターによりIPアドレスの緊急遮断が行われ、全学部ネットワーク管理委員会へ、その旨がメールにて通知される。工学部では各学科のネットワーク管理者が学部ネットワーク管理委員会のメンバーであるため、ネットワーク障害を起こした PC が接続されている学科のネットワーク管理者が、該当 PC のある研究室・講座等の PC 管理者へ連絡し、該当 PC のネットワークからの切断やウィルス駆除等の対応状況をメールにて学部のネットワーク管理委員会へ連絡する。総合情報処理センターからの通知より 1 時間が経過しても該当 PC の対応状況がメールにて連絡されない場合は、他学科のネットワーク管理者もしくは技術部情報システムグループメンバーが対応にあたる。そのため、学科ネットワーク管理者は学内ネットワークに接続する学部内 PC の IP アドレス情報（PC 管理者、連絡先、PC の設置場所など）を把握していなければならない。

我々は工学部ネットワーク委員会より Web による IP アドレス情報管理の依頼を受け、HTML ファイルによるIPアドレス情報の管理を行った。しかし、IP アドレス情報の新規登録、変更・廃止がある毎に HTML ファイルを作成し、アップロードをするには作業時間の問題があり迅速に対応することが出来ない。そこで、Web ブラウザをインターフェイスにデータベースを利用するシステムを開発したので報告する。

2 システムに要求される条件

システムは Web 上で、(1)学内ネットワークに障害を及ぼす学部内 PC が発生した場合の緊急対応にあたるための必要情報を取得でき、(2)システム上でそのデータの入力が可能である。その際、(3)ユーザのケアレスミスによって誤った操作がされた場合でも登録データに被害が及ばないようデータベースの保護を実現する。という条件を満たさなければならない。そこで、これらの条件を基礎としてデータベースの設計・構築および PHP のプログラミングを行った。

3 動作環境およびしくみ

3-1 動作環境

ソフトウェアは開発後の運用・管理を考慮し、現在技術部内で使用しているグループウェアや業務運用・管理システムと同様の環境を用いた。また、Apache, PHP, PostgreSQL については rpm パッケージを使用した。

ハードウェア

PC/AT 互換機、CPU Intel Pentium III 1GHz、メモリ 512MB、HDD 40GB

ソフトウェア

OS : TurboLinux 8 Server、Web サーバ : Apache-1.3.27、プログラミング言語 : PHP-4.2.3、リレーショナルデータベース : PostgreSQL-7.2.2

3-2 動作のしくみ

クライアントから①HTTP リクエストによる接続要求があると、サーバ側では Apache にロードされている PHP の PostgreSQL 接続関数が libpq を通じて②データベースサーバ（postmaster）に接続要求を行う。この接続要求があるとデータベー

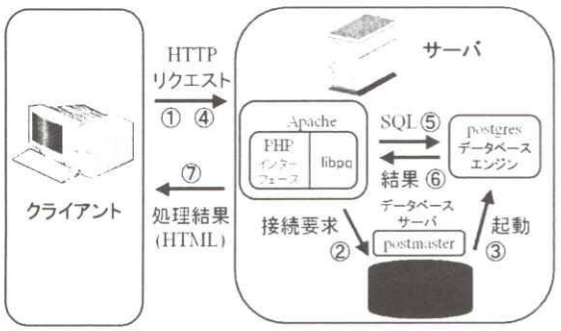

図 1. 動作のしくみ

スサーバは③データベースエンジン(postgres)を起動する。続いてクライアントから④HTTP リクエストがあると、PHP から⑤SQL 文がデータベースエンジンに渡される。データベースエンジンにより処理された結果⑥, ⑦がクライアントに返される。以上の動作を図 1 に示す。

4 ネットワーク接続申請・登録システム

ここでは、システムの設定、データベース、プログラム構成、機能、セキュリティについて述べる。

4-1 設定

Apache

- **接続制限**

```
<Directory "/var/www/html/filename">
Options None
Allow Override None
Order deny, allow
Deny from all
Allow from IP address
</Directory>
```

- **PHP の遮蔽**

```
AddType
application/x-httpd-php-source .html
```

PHP

- **セーフモード有効**

```
safe_mode = On
```

- **エラー表示なし**

```
display_errors = Off
```

- **エラーメッセージを Web サーバのエラーログに記録**

```
log_errors = On
```

- **エラーメッセージの HTML タグを出力**

```
html_errors = On
```

- **スクリプトエラーをシステムロガーに送る**

```
error_log = syslog
```

- **グローバル変数を不使用**

```
register_globals = Off
```

- **ファイルアップロード可能**

```
file_uploads = On
```

- **最大アップロードファイルサイズ設定**

```
upload_max_filesize = 2M
```

PostgreSQL

- **ログを syslog のみに出力**

```
syslog = 2
```

- **他のホストからの接続拒否**

```
tcpip_socket = false
```

- **接続したクライアントの詳細情報をサーバログに出力**

```
log_connections = true
```

- **サーバログに送られるデバッグ出力有効**

```
debug_print_query = true
```

4-2 データベース

2の(3)を実現するために、ネットワーク接続申請情報を登録するデータベースとそのデータを本登録するデータベースに分けて設計した。前者を申請用データベースとし、後者を登録用データベースとする。それぞれのデータベースのテーブル定義を表1に示す。登録用データベースのデータは申請用データベースのデータから生成し、申請

表 1. データベースのテーブル定義

データベース名	申請用			登録用
テーブル名	申請者	申請IPアドレス	CSV形式ファイル	登録IPアドレス
列 名	申請者ID パスワード 申請者名	IPアドレス1 IPアドレス2 管理者名 設置場所 メール 電話 学科名 申請者ID 申請者名 申請日時 その他	ファイル名 コメント 学科名 申請日時	IPアドレス 管理者名 設置場所 メール 電話 学科名 申請者ID 申請者名

用データベースのデータは登録用データベースのデータを生成後、削除する。それぞれのデータベースへのアクセスについては 4-4 機能で述べる。

4-3 プログラム構成

本システムは環境設定、認証、本体、アップロードファイル操作の4つのプログラムによって構成されており、システムの利用者は全て同じプログラムを使用している。

4-4 主な機能

本システムにはネットワーク管理委員会メンバーである学科ネットワーク管理者（申請者）が使用する機能とシステム管理している技術部情報システムグループメンバー（管理者）が使用する機能がある。前者と後者の機能の違いはネットワーク接続申請によって申請用データベースに登録したデータを登録用データベースに登録する機能と登録データベースのデータを変更・削除の機能の有無である。システムの機能とデータベースの関連を図2に示す。破線で囲んだ機能は管理者のみが使用できる機能である。データベースから機能への破線矢印はデータの読込を示し、逆に機能からデータベースへの破線矢印はデータの書込・変更・削除を示す。これから解るように登録用データベースに変更を行う機能は管理者のみが利用できる機能であり、申請者が登録用データベースに変更を加えることはない。

システムにアクセスし、ユーザ認証後、図3のトップ画面「セグメント一覧」が表示される。この画面はセグメントごとにIPアドレスの情報を表示する「詳細」、IP アドレス検索を行う「IP アドレス検索」およびネットワーク接続申請を行う「申請一覧」からなる。

ネットワーク障害を引き起こすPCが発生した場合、この「詳細」または「IP アドレス検索」機能を使用し、該当するPC の IP アドレス情報を引き出すことになる。

図4はネットワーク接続申請のトップ画面である。新規の申請や申請するPCのIPアドレスが連続し、IP アドレス以外の他の入力項目が全て同じ場合の申請、または件数の少ない申請などは「入力」を、登録されているデータを利用し、必要な項目のみを変更する場合は「データ検索」を利用する。また入力件数が多い場合などは CSV 形式のファイルを利用した「CSV ファイル」による機能を用いる。この機能は登録データベースから学科ごとにデータをCSV形式のデータファイルにし、ダウンロ

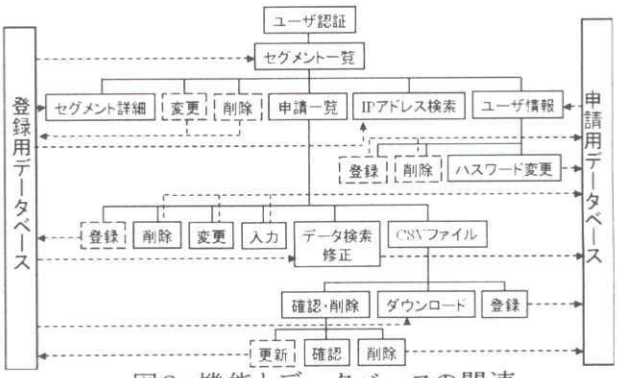

図2. 機能とデータベースの関連

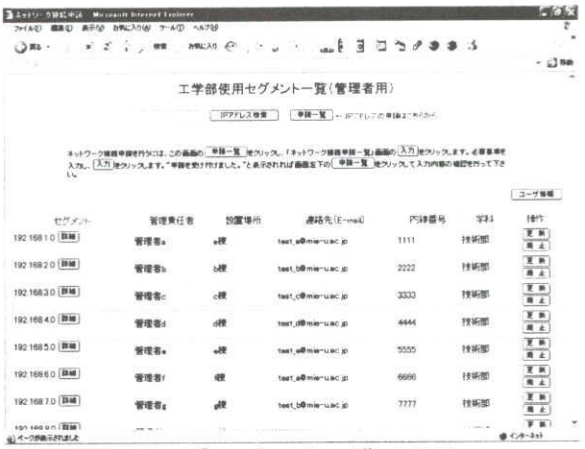

図3.「セグメント一覧」画面

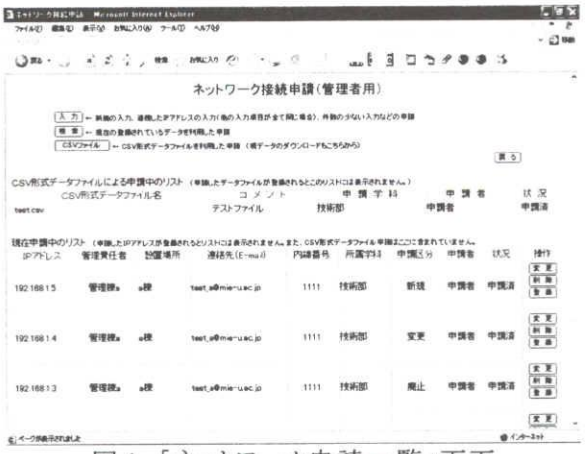

図4.「ネットワーク申請一覧」画面

ードできる機能も備えている。

以上がこのシステムの主な機能である。

4-5 セキュリティ

クロスサイトスクリプティング対策としてhtmlspecialchars()と strip_tags()を、SQL インジェクション対策として addslashes()を、また外部コマンドの実行対策として escapeshellcmd()を行っている。

サーバへの接続はディレクトリ接続制限により学部内 PC からの接続のみとしている。ユーザ認証には PHP の Basic 認証を使用し、ネットワーク管理委員会メンバーのみに利用を限定している。また、データベースの全てのテーブルへのアクセス権は nobody を設定している。そのほか、システムログによるサーバへの不正なアクセスの監視も行っている。セキュリティとは意味合いが少し異なるが、1日1回データベースのバックアップをとり、データベースに障害が起きた場合のリストアに備えている。

5 今後の課題

ネットワーク接続申請には3種類の方法を提供しているが、そのなかの CSV 形式ファイルによる申請は他の申請方法とデータの整合性を図っておらず、どのように整合性を図るか今後の課題である。現在は学科ごとに CSV ファイルを登録しているため、同一申請者による複数の申請(CSV 形式ファイルと他のどれかによる)は発生していない。

ユーザ認証はパスワードがネットワーク上をそのまま流れるため、データベースの Basic 認証または PHP のクラスライブラリを利用した認証の検討が必要である。また、より強固なセキュリティを図るためデータベース単位の接続制限(HBA の設定)も検討する必要がある。その他、ネットワーク障害を起こしている PC が発生した場合、より迅速な対応を図るために登録 IP アドレスに含まれる PC の設置場所と建物の配置図をリンクさせる機能を追加する予定である。

6 おわりに

本システムの開発により、ネットワーク障害を起こしている学部内 PC への対応が迅速かつ確実に行われている。また、この対応に必要なデータを Web により容易に登録できるようになった。

本システムは 2004 年 6 月 7 日(初期版)からサービスを開始しており、現在稼働しているシステムは二度の改良を重ねたものである。今後も利用者からの意見を取り入れ、さらにシステムの改良を行う必要がある。

参考文献

[1] 石井達夫, “PHP×PostgreSQL で作る最強 Web システム”, 技術評論社

[2] 石井達夫, “PC UNIX ユーザのための PostgreSQL 完全攻略ガイド”, 技術評論社

[3] 日本 PHP ユーザ会 Web サイト, http://www.php.gr.jp/

[4] 日本 PostgreSQL ユーザ会 Web サイト, http://www.postgresql.jp/