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

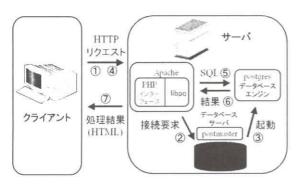


図 1. 動作のしくみ

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		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 管理置人工名 設一工話 電料者者 日申請請の他	ファイル名コメント学科名申請日時	IPアドレス 管理番場ル 電場ル 電料者者 申請 申請

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。

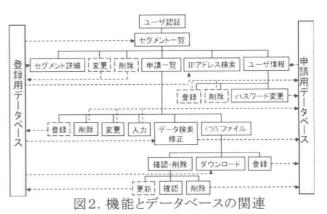
4-4 主な機能

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



	BACYDR 2-YO VI					
OR	. WE 240	can e		2001	3 .5	
						- 3
	工学	部使用セグ	メント一覧(管理者用	R)		
		「アアドレス被雷	•R-X - 1-11-1	###17865A		
3×1-7-21	инчиеноста дожно	●日一覧 使のか	クル、「ネットワーク雑株甲様一覧」高されれば画面左下の「中接一覧」を	画の 入力 セクシック。	27. 48882	
λ716. (A7	()をクリックします。"年間を飲い	一門がました。"と表示と	されれば曲数至下の「平師一其」を	クリックして人力内容の	entro tra	
						2-796
ヤガチル	管理責任者	29軍場所	康格先(E-mail)	內線器号	531	1017
192 168 1 () [B186]	管理者:	.eg	test #0mie~uac jp	1111	神神間	用 点
				2222	19 95705	N A
192 168 2 0 [8148]	管理者b	SAME.	test,b@mie-u.ac.jp	2222	1.3(44) (St)	A 4
192 168 2 0 (BFM)	管理者b 管理者c	が使	test_c@mie-uec.jp	3333	技術部	
			110000000000000000000000000000000000000		- 1110000	R A
192 168 3 0 (BM)	管理者に	cfR	test_c@mie-u.ec.jp	3333	快級問	T B R L R L
192.168.3.0 [BM]	管理者c 管理者d	cHR cHR	test_c@mier-usc_jo test_d@mier-usc_jo	3333 4444	技術部	R A
192 168 3 0 (BM) 192 168 4 0 (BM) 192 168 5 0 (BM)	營債各c 營債各d 營債名。	c#2 d#2 +22	test_c@mier-uac.jp test_d@mier-uac.jp test_e@mier-uac.jp	3333 4444 5350	対象部 対象部 対象部	王 田 田 土 王 田 田 土 王 田 田 土

図3.「セグメント一覧」画面

										· 21
Om	* 2 1	, 48	MULTIN CO		.m. (3 0 3	9 1	3	:3	
			ネットワーク接	統申請(管	理者用)					
(X	力 - 製鋼の入力	. 適 億したアフド:	スの入力(他の入力維吾が)	ETMC#4), #1	Bの3ない入力な	200 ₩				
	章 成在の登録									
[C	\$V294A ++ C\$	マルパテータファー	ルを利用した申請 (根デー)	のダウンロードもこ	55から)				# 6 T	
									-	
	タファイルによる		(単級。たデータファイルが)		中類学		m ·		,	t 2
test cay	SVRSEJ - XJ	7-171-6	テストファイル		A STATE OF THE PARTY OF THE PAR		200			理者
and the con-	171. (200 5.00		n NAVU Z HOLZ BRANCH Z W	and the second	W-875-/ 6 W		B. T T. H	Yes		
IP7FL2	管理責任者	特質場所	連絡先(E-mail)	内總督兒	所属23.1	中国区分			また	1917
DALLY.				1,3696.00	Contract Contract	- HH.	TT. 89			T E
	Willia.	.10	test a@mieruac in	3111	1916/00	新規	中田		TEA	対策
192 188 1 5	10.000	*88			2000		10000		既直	
	10.000	*85			2000		10000		TEA .	
192 168 1 5	yqu.	VALUE	test e@mieru ec jn	31111	技術部	Mist	10000		·既有	計 数 登 前 文 定 計 数
	10.000	.ex			2000		10000		THE S	計 施 登 商
192 168 1 5	yqu.	VALUE	test e@mieru ec jn	31111	技術部	Mist	10000		·既高	# # # # # #
192 168 1 5 192 168 1 4	管理課。 管理課。	.ex	teet e@mie-uac jo	1111	技術部	新线	10000	18 4	- M.A	計 施 食 商 京 克 新 施 食 商
192 168 1 5	yqu.	VALUE	test e@mieru ec jn	31111	技術部	Mist	10000	18 4	· 既有	財 服 食 品 京 支 新 服 食 品
192 188 1 5 192 188 1 4	管理課。 管理課。	.ex	teet e@mie-uac jo	1111	技術部	新线	10000	18 4	- M.A	財 服 食 品 京 支 新 服 食 品

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/