平成15年度機器・分析技術研究会参加登録システムの構築と運用について

伊藤 篤 （工学部技術部 第一技術系第一班）

1. はじめに

平成15年度機器・分析技術研究会が三重大学工学部主催のもと同年11月20日，21日の2日間にわたり三重大学三翠ホールで開催された。この研究会は，平成8年に全国の技術研究会から機器・分析の分科会が独立して開催されるようになってから今回で第八回を迎える。参加者は，全国41の大学，高専，研究所から145名の技術系職員を迎え，口頭発表21件，ポスター発表37件の発表が行われた。研究会の広報と参加登録の受付は，Webを利用して行えるようシステムを構築した。このような広報と参加登録のWeb利用は，事務作業の軽減と情報の即時性などで開催者側，参加者側双方に利点を供する。研究会Webサイトのトップページを図1に示す。数年前より参加登録の受付はWeb上で行われており，Webサイトと参加登録システムの構築，運用はそれぞれの開催機関ごとに工夫され行われてきた。一般にWebブラウザをインターフェースとして情報を登録，閲覧する技術は，この数年に見られるサーバ機器の低価格化とGNUやLinuxなどに代表されるオープンソースのプロジェクトと成果により，低コストかつ技術的にも比較的容易にシステムの構築が可能となってきた。ただしインターネットを使う都合上，OSとサービスを提供する複数のプログラムには，最新のセキュリティ対策とシステムとしての総合的な堅牢性の確保に留意することが不可欠である。三重大学では平成 15 年4月に情報セキュリティポリシーが施行されシステム管理者の責任が明確化されたこともあり，トラブルの回避と障害発生時にはこれまで以上に迅速な対応が求められている。今回のシステム構築に際しては，全てのプログラムを独自に開発することに加え，これまでに構築・運用経験のあるOSとサービスを用いることでセキュリティ確保とシステム障害への迅速な対応体制を目指した。今回の参加登録受付け期間中は，幸いにもセキュリティ問題や障害に見舞われることなく無事運用することが出来たので，システムの構築と運用面での出来事や工夫，問題点と解決したこと，今後の課題などについて報告する。

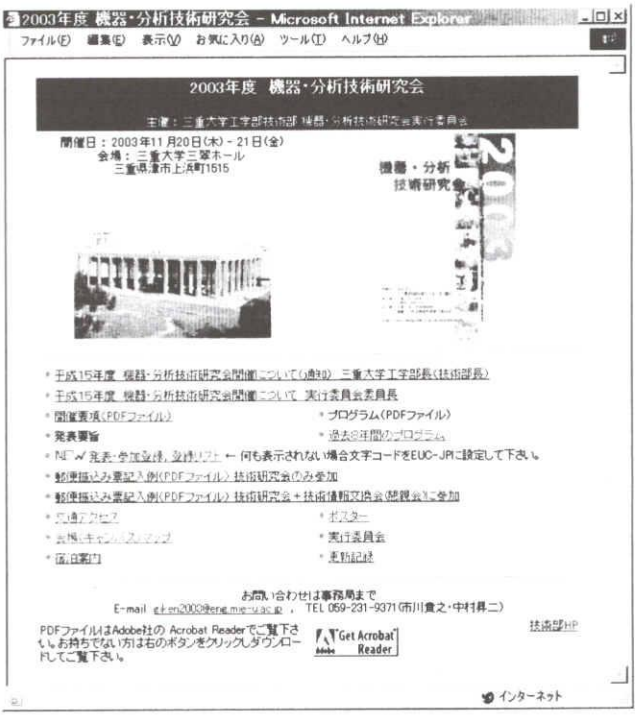

図1 研究会ホームページ

2－1 参加登録システムの概略と構成

今回予想される参加登録者数は過去の実績から判断し約100名，機関数40として参加登録システムを構築した。システムに求められる要件としては，①ユーザの使用機器，OSなどによらずWebブラウザをインターフェースに容易な操作でデータ登録が可能なこと ②登録内容の確認は登録者自身が登録直後に可能なこと ③書面による参加登録申し込みと整合性を保つこと ④メールアドレス等個人情報の保護を図ること ⑤登録者の利便性を図るとともに悪意のある第三者のネットワーク上での攻撃を防御すること ⑥システムの運用と監視，メンテナンス性に優れ安定して稼動すること ⑦現在運用中の技術部Webサーバで稼動すること などが前提条件とされた。これらの多くが一般に各種ネットワークサーバとそのサービスに求められる条件と同一ではあるが，具体的にどのツールを組み合わせて構築するかは多くの選択肢がある。今回はサーバ機器の制約上，そのOSであるLinux上で稼動するツールを選択することが求められた。そこでこれまでにも部内グループウェアで開発，運用経験のあったWebサーバApache，プログラミング言語PHP，リレーショナルデータベースPostgreSQLを組み合わせて構築することとした。

OSに用いたLinuxは，UnixライクなOSとしてネットワークサーバをはじめ，最近では基幹系サーバにも導入され豊富な情報と開発環境に特徴を持つ。Webサービスを提供するApacheは最も普及しているWebサーバであり，多くの機能がモジュール化され用途に応じて選択して組み込むことが出来る特徴を持つ。参加登録システムをプログラミングしたPHPはHTML埋め込み型のサーバサイド・スクリプト言語でWebサーバApacheのモジュール化や豊富なデータベースインターフェースと優れたエラーハンドリング，セッション管理などに特徴を持つ。本システムでは運用・管理上の利便性からPHPモジュールをApacheの起動時に共有ライブラリとして動的に組み込むDynamic Shared Module方式をとった。登録データの保存，管理はデータベースを用いて行った。そのメリットは，複数アクセス時の排他制御とトランザクション管理，データ保全の信頼性，データ量の増加と検索性に優れたメリットを持つ。PostgreSQLはRDBMS(Relational Data Base Management System)で多くのプラットフォーム上で使われており Structured Query Languageに準拠しマルチバイト文字対応やトランザクション処理，バックアップなど多くの機能で商用データベースにも匹敵する優れた特徴を持つ。PHPとはインターフェースのモジュール化により安定した動作環境が実現されている。

2－2 サービスの連携と動作の仕組み

参加登録システムの機能を分担するPHP, PostgreSQL, Apacheは，相互に連携して動作している。参加登録時の各サービスの連携と動作の仕組みを図2に示す。最初に①ユーザがWebブラウザより参加登録システムにアクセス、つまりWebサーバにHTTP接続要求を行うと、②Apacheが接続要求のあったHTMLコンテンツを呼び出し、③内部に記述されたスクリプトがPHPにより解析・実行される。データベースへのアクセスが必要な場合は、④PHPのPostgreSQL関数によりSQL文によるクエリー実行問い合わせが行われ⑤PostgreSQLはデータベースへのアクセス処理を行い結果を返す。⑥再度、PHPからSQL文による問い合わせを行い、検索結果を得て⑦PHPで結果をHTML化しApacheがWebブラウザに返送する。Apacheは②，⑦，PHPとプログラムは③，④，⑥，⑦，PostgreSQLは⑤の動作を分担，連携して実行されている。

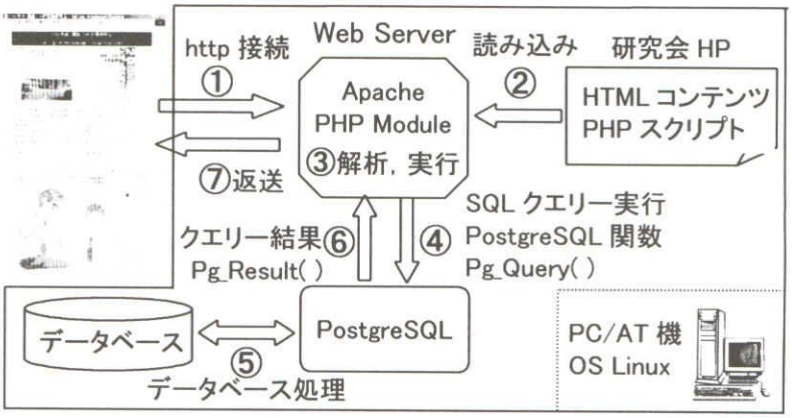

図2 各サービスの連携と動作の仕組み

3－1. 参加登録プログラム

一般にWeb上で実現させるサービスと運用方法は，利用者と提供側で双方の利便性，サービス期間・内容，機器，セキュリティ，メンテナンス時間などの要件を考慮し決定される。本件では，これらの要件を考慮しユーザに提供するサービスはデータ登録と閲覧のみとした。仮に登録済みデータの修正と削除を登録者にサービスする場合は，ユーザの識別・認証が必要でありPHPでは標準クラスライブラリPEARのAuthクラスを用いてサービスが可能である。しかし本件の場合は登録内容とボリューム，件数を考慮すると修正，削除の件数は少ないと予想され，認証サービス実施にともなうユーザの利便性とシステム運用・管理者の手間とを比較した結果，行わないこととした。プログラ

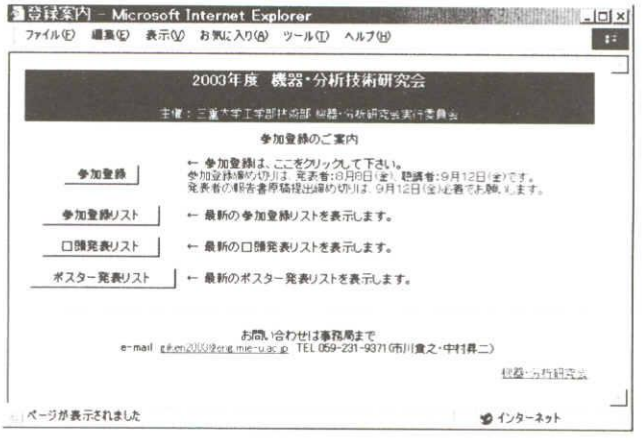

図3 参加登録トップページ

ムの動作は，ユーザがWebブラウザで参加登録サイトにアクセスすると，プログラムは最初に変数と関数の定義後，図3に示す参加登録トップページを生成する。同ページは，参加登録，参加登録リスト，口頭発表リスト，ポスター発表リストフォームボタンと説明文から構成される。ここで□はフォームボタンを表す。ユーザが参加登録を選択すると，フォームが送信され図4に示す参加登録入力ページが生成される。同ページは名前，所属機関など18項目の入力ボックスと入力確認フォームボタンから構成される。ユーザが必要項目を入力後，入力確認 を選択すると，フォームが送信され入力項目・文字数チェック，タグ等の無効化，特殊記号全角変換処理を行った後，入力確認ページが生成される。同ページは入力項目の表示と本登録フォームボタンから構成される。ユーザが本登録を選択すると，フォームが送信され重複登録チェックと登録ナンバー割り振り後にデータベースへの書き込み処理が行われる。エラーなく書き込みが完了した場合は，そのメッセージを表示しシステム管理者宛に登録内容をメール送信する。これらの機能はユーザ側からはWebブラウザにより操作されるが，そのプロトコル HTTP はステートレスな接続であり，複数の利用者からの同時アクセスに対する個々のセッションを区別することは出来ない。そこで本プログラムでは，PHP バージョン4から標準で実装されたセッション管理機能を用いてプログラミングを行った。ユーザが各リストの閲覧を目的に参加登録リスト，口頭発表リスト，ポスター発表リストのいずれかを選択すると，フォームが送信され各リストページが生成される。参加登録リストページを図5に示す。同ページは，最新30件のデータ表示と前の30件，次の30件フォームボタンから構成される。口頭発表リストページを図6に示す。同ページとポスター発表リストページはデータ表示のみとした。

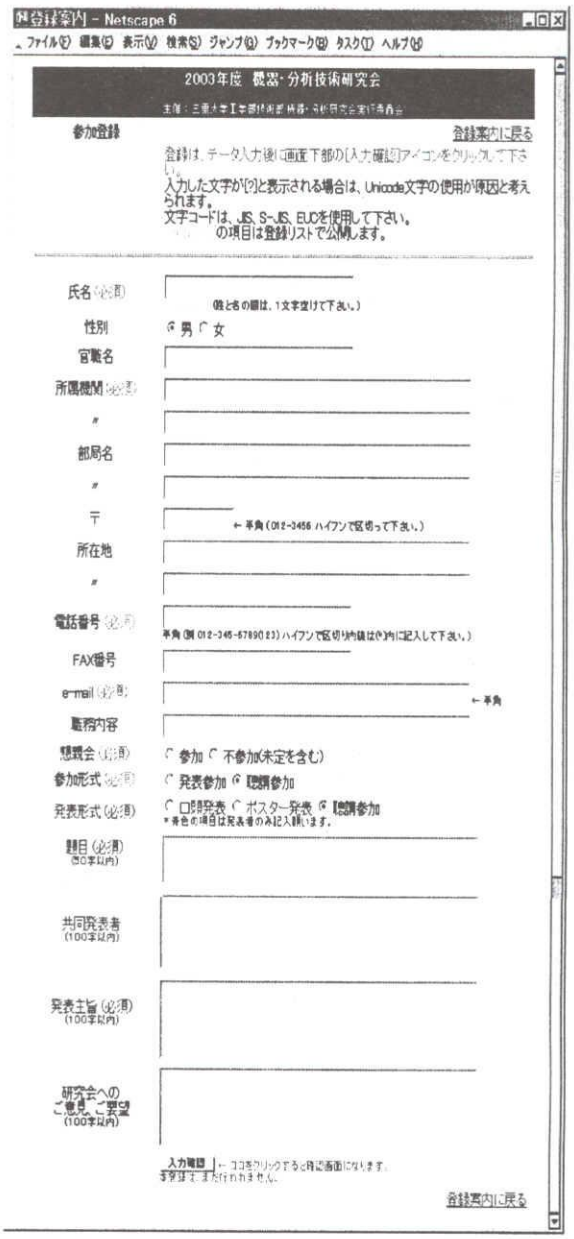

図4 参加登録トップページ

図5 参加登録リストページ

図6 口頭発表者リストページ

3－2 管理・メンテナンス用プログラム

参加登録プログラムはデータの登録と表示のみに機能を限定したため，登録データの修正，削除，非公開データを含む全登録データの表示，登録確認メールの作成などの管理・メンテナンスに必要な機能は，アクセス制限を行い別プログラムとした。これによりシステム管理者が許可した者以外のデータの修正，削除，非公開データの閲覧を制限した。

4. データベース

本システムでは，ユーザによるWebからのデータベース利用は一つのテーブルへのデータ登録と閲覧のみの簡単なものである。データベースへのアクセス権限は nobody とし，文字コードは参加登録プログラムと同じ日本語EUCコードとした。参加登録テーブルのデータ型を表1に示す。背景が灰色の項目は必須項目で NOT NULL 制約を設定した。最初の[No.]項目は各レコードに割り振った連番で，その生成にはデータ追加時に自動でインクリメントされるようにSERIAL型を用いた。登録日時は TIMESTAMP 型を用い，性別，郵便番号，参加形式(発表，聴講)，発表形式(口頭，ポスター)，懇親会参加は固定長の CHAR 型を用いた。それ以外のデータ型は全て VARCHAR 型を用い，レコード長は過去の研究会報告集に掲載されているデータを調査し決定した。名前は旧姓の掲載例があり，機関名と部局名はカタカナ名称も多く，電話・FAX 番号は内線の記載例もあり，連名者は3機関に渡るものもあり，それぞれに余裕を持たせたレコード長を定義した。今回の登録では，最多連名者数は12名，機関数は4機関であったが幸いにもレコード長不足による登録トラブルはなかったようである。データベースのバックアップは稼働中でもバックアップが可能な pg_dump を用いて適時行った。

表1 参加登録テーブルのデータ型

カラム名	データ型(レコード長)
No.	integer
日時	timestamp
名前	character varying(30)
性別	character(2)
官名	character varying(30)
機関名	character varying(50)
機関名2	character varying(50)
部局名	character varying(50)
部局名2	character varying(50)
〒	character(10)
住所	character varying(50)
住所2	character varying(50)
TEL	character varying(30)
Fax	character varying(30)
メール	character varying(50)
職務内容	character varying(50)
参加形式	character(10)
懇親会	character(6)
発表形式	character varying(14)
題目	character varying(150)
共同発表者	character varying(300)
発表主旨	character varying(300)
その他	character varying(300)

5. 運用とセキュリティ

ネットワークサービスのセキュリティ確保と対策は，OSと各デーモン Apache，PHP，PostgreSQL および PHP で作成したプログラムの全てで行う必要がある。OSと各種デーモンのセキュリティ対策は，ディストリビュータによるセキュリティアナウンスに従い速やかに実施した。Webサイトを公開している半年間でのセキュリティアナウンス総数は32件であった。サービスと直接関係するものでは，PHP の「透過セッションIDサポートにクロスサイトスクリプティングの脆弱性」が報告された。本システムのPHPでは，当初よりクッキー使用不可時のURL自動書き換え設定である php.ini の session.use_trans_sid=Off で運用していた。ここで囲み文字は設定を表す。またクロスサイトスクリプティングとSQLインジェクション対策としてフォーム入力にはhtmlspecialchars()関数による特殊文字のHTMLエントリ変換と ereg_replace()関数による特殊文字の全角変換を行っており問題は発生しなかった。PHP 本体は Apache のモジュールとして組み込まれ，同一プロセスの元に nobody 権限で実行され安全性に配慮した運用を行っている。PHP全般の動作設定は php.ini に記述され，①グローバル変数制限の register_globals=Off ，②外部ホストへのアクセスを制限する allow_url_fopen=Off ，③システム実行制限 safe_mode=On ，④Webサーバ変数の優先 variables_order="EGPCS"，⑤ユーザ入力の引用符等文字列のエスケープ設定 magic_quotes_gpc=On，⑥エラー非表示 display_errors=Off，⑦エラー記録 log_errors=On で運用した。Apache の運用では PHP の遮蔽を行い httpd.conf で AddType application/x-httpd-php .html とした。この設定では全てのコンテンツが PHP Engine を通じてパースされるためにレスポンスの低下が懸念されたが，実用上問題ないことが確認されたので安全性を考慮し実施することとした。システムと各デーモンの監視は，通常のシステムログに加え PostgreSQL の設定ファイル postgresql.conf の syslog=2, debug_print_query=true, logconnection=true として稼働状況を監視した。

6. アンケート調査

ポスター発表「機器・分析技術研究会Webサイトの構築と運用について」(1時間20分)で直接説明した13名に対し表2に示す11問の聞き取り調査を行った。その結果，ホームページ全般と参加登録面では特に問題はなく，参加登録直後に本人がWeb上で確認出来ることに良い評価を得た。登録情報のWeb掲載は，名前，機関名，発表内容，懇親会参加に限定したが，専門分野を掲載してほしいとの要望があった。参加登録の確認メールは，タイトルに1バイトの英文字を使用したためにスパムメールと勘違いされたケースもあり，メーラの対応状況を考慮すると今後は，2バイト文字を用いても良いと思われる。報告原稿の提出は，電子化とともに原稿自体のWeb掲載にも大多数の賛成が得られた。電子化とWeb掲載により研究会に参加出来なかった人も報告内容が閲覧出来るのでメリットは大きいと思われる。また，検索エンジンに登録されることにより，企業からの問い合わせがあった事例も多く聞かれる。報告内容のWeb掲載は，他の研究会で数年前から実施されていることもあり，本研究会でも早期の実施が課題とされる。事務局対応では，報告原稿と参加登録費受け取りの返事がなかったとの指摘があった。これらも今後の課題とされる。

表2　2003機器・分析技術研究会Webページと参加登録に関するアンケート調査

Q1. 入力項目数は？	多い : 2	適切 : 11	少ない : 0
Q2. 登録操作に要した時間は？	長い : 0	普通 : 13	短い : 0
Q3. 登録操作の反応時間は？	遅い : 0	普通 : 13	速い : 0
Q4. 登録操作は直感的に出来ましたか？	Yes : 13	? : 0	No : 0
Q5. 報告書原稿提出の電子化は？	賛成 : 11	考慮中 : 2	反対 : 0
Q6. 報告書のWeb掲載は？	賛成 : 11	考慮中 : 2	反対 : 0
Q7. 研究会ホームページの出来は？	○ : 12	△ : 1	× : 0
Q8. 事務局の対応は？	○ : 10	△ : 2	× : 1
Q9. 参加登録システムへの要望は？ Q10. 研究会ホームページへの要望は？ Q11. 事務局への要望は？			

7. 今後の課題

参加登録時におけるブラウザのReload機能誤用による重複登録の防止策として，セッション管理を用いてプログラミングを行った。これはユーザより改変される可能性のある変数の引き渡しでも有効である。しかし2つのブラウザからアクセスしたケースを想定出来ず重複登録1件を防ぎきれなかった。また登録時のメールアドレスはプログラムでチェックしなかったため，120件中4件の入力ミスがあった。これらはプログラムでの対策が可能であるが，運用中の変更は行わなかった。運営面では，締め切り後の参加および修正依頼が数件あり，HTMLとPDF版の資料作成に手間を費やした。また，今回の報告書原稿提出は郵送で行ったが，アンケート調査でも賛成意見が多く聞かれた電子化の導入が必要と思われる。

8. むすび

研究会参加登録システムを構築し，障害やトラブルに見舞われることなく無事運用することが出来た。今回の経験で，自分が過去に参加した研究会でも同様のシステムを構築，運用してきた人達の苦労を身をもって知ることが出来た。今後，データベースを中核とするこのようなシステムは，参加登録のみならず情報をリアルタイムに提供するさまざまな用途で使われると考えられる。現在開発中の業務運用・管理システムにも参考になる技術を多く得ることが出来たので，今後も安全で安定かつ使いやすいシステムの開発・構築を課題とする。

参考文献

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

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

[3] 「ＰＨＰ４徹底攻略実践編」，廣川類他，ソフトバンクパブリッシング/2002