学生のためのインターネット利用環境

車古　正樹

金沢大学総合情報処理センター

〒　920-1192 金沢市角間町

TEL:076-234-6912　　FAX:076-234-6918
shako@gipc.kanazawa-u.ac.jp

キーワード

ユーザ認証，DHCP，インターネット，学生管理，ネットワーク，ファイアウオール

はじめに

学生が自由にインターネットを利用できるようにするための環境を整備した。その環境を整備するにあたり，次のことを考慮した。

- 共通スペースにパソコンを配置する。
- 持ち込みパソコンを利用できるようにする。
- 希望するユーザ ID を発行する。
- ウイルス感染の防御と不正アクセスの防御を行う。
- できる限り人手がかからないシステムとする。
- すべてのインターネット利用ログを記録し 1 年間保存する。

これらのシステムと実際に利用した問題点について報告する。

1 ネットワークシステム構成

学生用インターネット利用環境の概念図を図１に示す。

1.1 情報コンセント設置場所

図書館，総合教育棟，総合情報処理センターなど全学的な建屋には全学生が利用できるように，部局のラウンジや教室などの共通スペースにはその部局の学生のみが利用可能できる情報コンセントと無線 LAN を設置した。

1.2 ソフトウェア

Check Point 社製 VPN-1/FireWall-1 11 式を各部局に配置し，各ファイアウオールに次の 3 つのセグメントを構築した。

- サーバ類を接続するＤＭＺセグメント
- 事務用端末を接続するＶＰＮセグメント
- 学生用端末を接続するＤＨＣＰセグメント

上記セグメントは全てプライベートアドレスからなり，NAT により外部と通信する。

1.3 学生用端末を接続するＤＨＣＰセグメント

各セグメントを管理するにあたり次のことを考慮した。

- 接続された端末は DHCP により IP アドレスを習得する。
- アクセス制御はファイアウオールポリシーにより全てのファイアウオールについて一元管理を行う。
- 外部との接続はクライアント認証(ユーザ ID とパスワード)により 1 時間許可する。
- 電子メール(HTTP,ftp は将来)については，ウイルスチェックを必ず行う。
- 外部との通信ログには IP アドレス，サービスなど以外にユーザ ID も記録する。

2. 利用者管理システム

このシステムを構築するにあたり次のことを考慮した。

- 維持管理するための労力をできる限り少ないシステムとする。
- 利用したい人にのみユーザ ID を発行し，システム資源の有効利用と不正利用の減少を図る。
- 学生自身が操作し,学生が希望するユーザ ID を与える。
- メール利用と情報コンセント利用を統一して管理する。
- 非常勤講師など学生以外も利用できるシステムとする。

2.1 利用者管理システム概要

利用者登録管理するシステムを図２に示す。主なプログラムの機能は下記のものである。

2.1.1 管理用プログラム

管理用プログラムは主として次の機能を有する。

- 4,10 月の一括処理：在学生データと照合し,削除データの作成とマスターデータベースの更新
- 随時処理：学生以外のデータの追加と利用者取り消し処理
- 利用者リスト処理：利用者リストの表示
- 検索機能：検索によるデータ表示

2.1.2 ユーザ登録プログラム

ユーザ登録プログラムは主として次の機能を有する。

- 登録にはバッチモードとリアルタイムモードがあり，４，５月はバッチモードで運用，それ以外はリアルタイムモードで運用
- プログラムの利用は学生証で認証
- 新規ユーザ登録：ユーザ ID，パスワード，転送先入力など
- 既存ユーザ変更：パスワードの変更，転送先変更

3. 学生の利用

DHCP 配下に設置された共同利用端末や持込パソコンのための情報コンセントを利用することができる。

3.1 インターネット利用

インターネット利用において，学内のホームページ参照以外でファイアウオール超えする場合は，学生用ホームページを起動し，認証画面からユーザ ID とパスワードを入力し，“ sign on ”する。この時の認証に用いるファイアウオールは IP アドレスにより該当するファイアウオールを自動リンクする。1 時間以内の利用の場合は，“ sign off ”して終了する。

- ログは全てのファイアウオールを一括で記録し，かつ，ユーザ ID を含めて記録する。
- パスワードを忘れた場合はセンター窓口に本人が申しでる。ユーザ ID を削除し，1 週間利用停止とする。停止期間が過ぎれば登録が可能となる。
- 削除した利用者 ID は 180 日間保持され，同一人の場合は再利用が可能である。なお，この機能は学部生から大学院生になり，学籍番号が変更になった場合も同一人として扱われる。

3.2 電子メール利用

電子メールについてはウイルス対策やセキュリティ対策などを十分考慮して運用している。

- 認証方式は apop のみとしている。
- 利用可能な容量は 1MB までである。これは共同利用端末でフロッピーディスクを利用することを考慮した容量である。
- pop サーバと smtp サーバは別のものを利用している。指定できる smtp サーバはファイアウオールポリシーで制限している。
- 受信・送信共に必ずウイルスチェッカー経由となる。

4 問題点

半年以上の運用を経てほぼ満足のいくシステムであることが確認されたが，次のことを考慮することが必要である。

- リアルタイム登録は，登録者が約 1,000 人を超えたあたりから登録に 1 分以上かかるようになり現実に即しない。現在は日 1 回のバッチ処理で運用しており，近い内に LDAP 認証に変更しリアルタイム登録を可能とする。
- 運用を開始してから管理の便利さにより部局の学生がいる研究室への拡張要望があるがそれに応えれるよう検討を要する。
- 一部 PC の OS で https での認証できないため，特別に http で認証を行っているが調査検討を有する。
- http や ftp をウイルスチェックすると非常にレスポンスが悪く，かつ，一部タイムアウトとなるサイトがあり，現在はウイルスチェックを行っていない。メーカに調査改善を依頼中である。

まとめ

一部に改善が必要な部分もあるが，最初に考慮した以上に維持管理が便利であり評判も良い。これから如何にこのネットワークを拡張していくか計画しなければならない。

また，システムの一部に無線 LAN も組み込まれているがほとんど利用されていない。この活用方法についても考慮する必要がある。

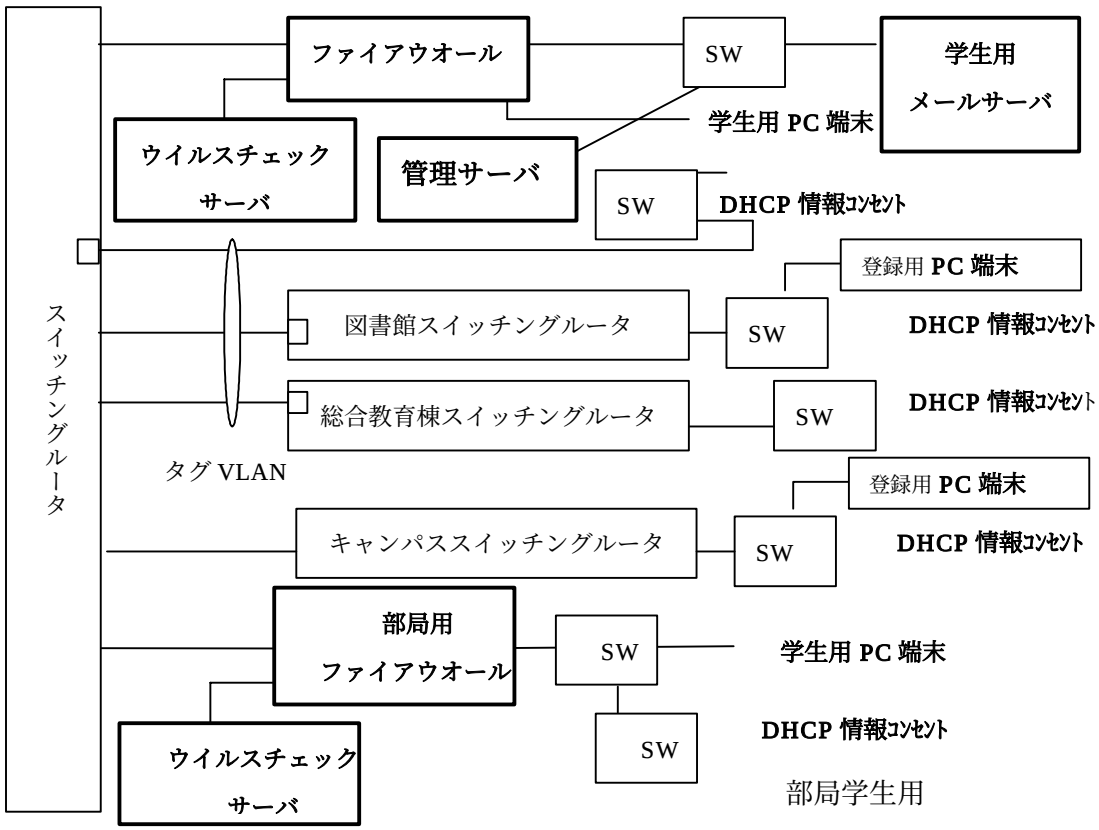

図 1　学生用インターネット利用環境

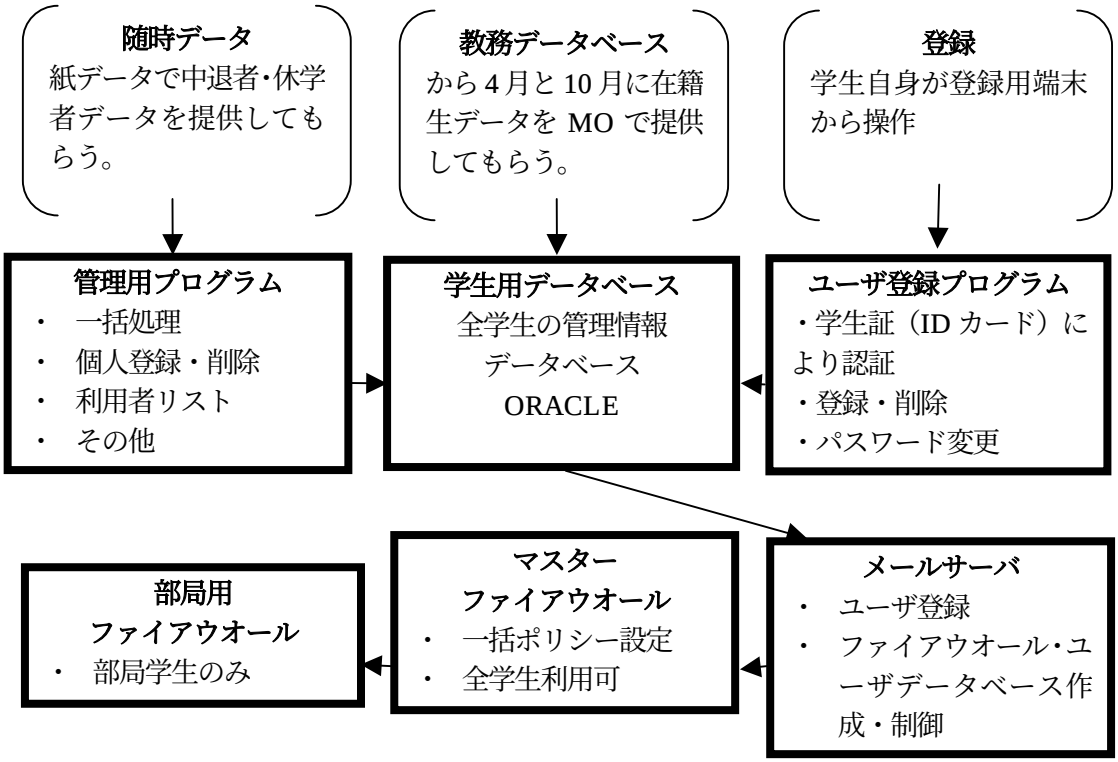
随時データ
紙データで中退者･休学者データを提供してもらう。
教務データベース
から 4 月と 10 月に在籍生データを MO で提供してもらう。
登録
学生自身が登録用端末から操作
管理用プログラム
・ 一括処理
・ 個人登録・削除
・ 利用者リスト
・ その他
学生用データベース
全学生の管理情報
データベース
ORACLE
ユーザ登録プログラム
・学生証（ID カード）により認証
・登録・削除
・パスワード変更
部局用
ファイアウオール
・ 部局学生のみ
マスター
ファイアウオール
・ 一括ポリシー設定
・ 全学生利用可
メールサーバ
・ ユーザ登録
・ ファイアウオール･ユーザデータベース作成・制御

図 2　学生管理システム