本郷キャンパスネットワークの更新について

浜　　正　樹

1．システム更新について

1-1．システム更新の経緯

本郷キャンパスでは，文京女子短期大学時代よりインターネットへの接続を開始し，10年程度経つ。その間，インターネット利用や情報処理教育，更に一般教育でのコンピュータ利用が定着してきたと言えるであろう。

しかし，2004年春の時点で本郷キャンパスのネットワークは，FDDI や 10Base-FX といった旧式のネットワーク規格の機器を基幹に据えており，利用者の増加に伴う帯域の不足，IP アドレスの枯渇，セキュリティ機能の不足やネットワーク機器の保守契約切れによる障害時の復旧遅延など様々な問題が浮き彫りとなってきていた。また，情報教育環境も経年変化による端末の故障，肥大化した OS やアプリケーションに対する端末性能の不足やカスタマイズシステムの保守性の低下など様々な問題を抱えており，教育面での要求に応えることが難しくなってきていた。

上記の事情に鑑み，補助金で買い取った機器の法定償却年数（ネットワーク機器 9 年・情報機器 5 年）を消化した2004年夏季に，本郷キャンパス全体のネットワークおよび情報教育環境の更新を行った。

本紀要論文では，今回システム更新におけるネットワークシステムの導入について，その導入システムの方針，導入システムの概要，運用開始後の障害および今後の課題について報告する。

1-2．導入システムの方針

2003年頃，システム更新に向けて仕様策定を開始した当初には，まだ経営学部の移転が決まっておらず，外国語学部・短期大学の利用者を想定して語学教育への応用に耐え得るシステム仕様を策定していた。その後，経営学部の移転が決まり，デザイン教育やプログラミング環境の整備など仕様の追加を行った。

経営学部の本郷への移転に伴う大きな変化と言えば，学生数がほぼ倍増し総数約2000名を抱えることである。また，従来の女子教育から共生を理念とする共学に転換すると共に，大学・短大教育のみならず大学院や生涯学習センターを中心にリカレント教育にも広く門戸を開いていく方針であるため，ユーザー層も大きく変化することが予想された。

上記の状況変化を想定して，ネットワークインフラのリニューアルについては，次に述べる

点を重要視することにした。まず，ユーザー数の増加に伴うネットワーク利用の負荷増大やユーザー層の変化によるセキュリティ問題の顕在化を予想して，「シンプル・セキュア・シームレス」を主眼に置き，現行の10Mbps 帯域中心のネットワークから 1Gbps 帯域を基幹に据えたネットワークへの転換を行うことにした。

更に，多彩なユーザーが行う教育・研究は，マルチメディア素材の利用など様々な要求な生じると思われるので，マルチキャストや Qos/Cos 機能を利用して柔軟に応用可能なネットワーク構成を実現することにも重点をおく。

また，所謂大学生や大学院生だけでなく，ニュースチューデントとよばれる様々なバックグラウンドの大学利用者が増加することを受け，オープンネッワークゾーンも設けて情報コンセントや無線 LAN の利用も可能にする。その一方で，オープンネットワークの利用者の認証や利用経路には充分な注意を払いセキュアな運用を行う。

1-3．導入システムの要求概要

1-2 で述べた導入システムの方針を基に，ネットワークはギガビットイーサネットを採用し，全学的にフロアや教室まで VLAN によるネットワークの論理分割を行うことにした。また，動画・音声などストリーミングによる利用が想定されるエリアを中心に，マルチキャストと Qos/Cos 機能についても適確な配置を設計することにした。

更に，インターネット端末，無線 LAN や情報コンセントなどを束ねるオープンネットワークエリアは，外来者も利用可能なため学内 LAN との分離を図る必要がある。そのため，認証ゲイトウェイを採用することにした。

また，今回の導入では，調達物品のみならず，メールサーバなどの既存物品と既存のネットワーク配線の利用によってシステムの構築を行うことにより，コストダウンを図ることも大きなポイントである。

2．ネットワークシステム

2-1．基幹ネットワークの構成

基幹ネットワークは，各校舎間を 1Gbps 以上の帯域を確保して繋ぐことを目標に既存の光ファイバー配線を利用することにした。また，本学では同じの校舎ビル内でも教育系・研究系・事務局系などの利用が混在しているため，各フロアや主要な部屋まで VLAN によるネットワーク分割によってセキュリティを確保できることを必須要件とした。以下，その他の要件などについて述べる。

2-1-1．機種選定

今回の導入にあたって入札を行った際，基幹ネットワーク用のシャーシ型スイッチについては 3 種類の機種（Foundry BigIron 8000/4000，Cisco 6506，Nortel Passport 8600）の提案があり，その全てが高い転送能力と充分なバックプレーン帯域を有すものであった。

しかし，選定には本学のネットワーク用途を想定して，単に高速・高帯域というハードウェ

ア性能面だけでなく，バランスの取れた配置設計がなされているかを重視した。

特に，留意した点はスイッチのモジュール構成を一部敢えてフルスペックにしなかったことである。スイッチには，モジュールごとに提供するポート数を選ぶことが可能である。フルスペックの状態では，モジュール内の各ポートの合計した帯域幅よりもバックプレーンの提供する帯域幅の方が大きい。即ち，全ポートで最大帯域を利用してデータ転送を行うことが可能である。

しかし，本学の様にネットワークのハードユーザーの人数がそれ程多くなく，学内からの同時接続で高いスループットを要求されることが多くない場合，すべてのモジュールがフルスペックな構成は却って投資の無駄を生じる。そこで今回は，一部に Over Subscribe 構成と呼ばれる非フルスペックなモジュール構成を利用してネットワーク全体で最適な配置を行った。

具体的には，Foundary BigIron を採用して，以下のモジュール構成と配置を行った。

1. 8 ポートモジュール（フルスペック構成）
   - 基幹スイッチ間接続
   - 教室用スイッチ間接続
   - サーバネットワーク
2. 16ポートモジュール（Over Subscribe 構成）
   - フロアスイッチ間接続
   - 小規模サーバネットワーク

今回採用しなかった他の 2 機種の提案は，フロアスイッチへの接続にもフルスペックのモジュールを提供しておりコスト面からもメリットが少なかった。

また，先程もふれたように，スイッチによるネットワークの論理分割が運用面で重要視されるため，VLAN を含めた設定変更方法が簡便であることも大きな選定ポイントである。この観点からも，ネットワーク機器のデファクトスタンダードである Cisco 製品とコマンドラインインターフェースの書式が良く似ている Foundary Network 社製品は充分その要求に応えられるものであった。

2-1-2．リング構成

本学のような中規模程度の大学ネットワークの場合，ネットワークの中心に高性能スイッチを設置してスター型トポロジーで構成することが一般的な手法である。

しかし，本学のネットワーク利用状況を検討してみると，ネットワークの中心拠点となる B 館には教育系と研究系が集中しているものの，事務局系はセンター館と S 館にその居室の殆どが配置されている。従って，トポロジー的に見てネットワーク通信が必ずしも B 館を経由することが必要ではなく，センター館と S 館間での通信の確保が効果的であるとも推定される。そこで，B 館・センター館・S 館の 3 拠点に基幹スイッチを設置して，リングトポロジーを構成したネットワークを採用することにした。それぞれのスイッチ間は全 2 重の1000

GBase-SX を 2 本接続して 4Gbps の帯域を確保した。

また，リング構成の採用により，ネットワーク全体の冗長構成も可能になった点も大きなメリットである。特に，ルーティングプロトコルには OSPF を採用し，拡張性の確保も行った。今後の保健医療技術学部との接続にも大きなメリットがあると考えている。

2-1-3．マルチキャスト

本学の語学教育やデザイン教育の用途に対しては，いずれマルチキャストのような同時一斉配信が必要になることも考えられるので，基幹スイッチでマルチキャストパケットもルーティングする機能を持たせることにした。ルーティングプロトコルには，PIM-Dense Mode を採用している。

また，マルチキャストの運用には L3 スイッチでのルーティングのみならず，L2 レベルで受信端末まで宛先を特定する必要がある。そこで，基幹ネットワークと後述する教室ネットワークやフロアネットワークの機器まで IGMP Snooping 機能を提供し，コンピュータ教室での効率的なマルチキャストデータ受信を可能にした。

2-1-4．Qos

今後，本学でも教材や学生作品として音声・動画データの配信の頻度が高くなっていくと思われる。一方，本学のネットワークはイーサネットであるため，すべてのパケットは全く平等に扱われ，大量のデータが送受信されると輻輳を起こしてネットワークの遅延を起こす。

しかし，音声・動画データを配信する場合，データの遅延やデータロスはそのまま音質や画質に大きく影響する。そこで，基幹ネットワークのスイッチにも Qos と呼ばれる通信データの優先度や帯域の確保を行う機能を導入することにした。この機能により，着目する通信データに対して，以下の 2 つの方法でそのトラフィックを制御できる。

1．重みづけによるトラフィックごとの帯域分割

2．トラフィックの厳密な順序づけによる配信

以上の Qos 機能については，今後の本学でのネットワーク利用状況を観測しながらきめ細かい調整を行っていく予定である。

2-2．教室ネットワーク

2-2-1．配置設計と要件

教室ネットワークとは，コンピュータ教室に設置するスイッチと端末および基幹ネットワーク用スイッチとの間で形成されるネットワークである。教室ネットワークが，一般の企業ネットワークなどと異なる大きな点は，バースト的に発生するネットワーク負荷の増大である。特に，授業の開始時刻や終了時刻には，ファイルサーバのネットワーク接続箇所にトラフィックが集中することが特徴といえる。実際に，本郷キャンパスの旧システムでは 1 年生の初回授業の一斉ログオン操作に支障をきたしたケースもある。また，ふじみ野キャンパスにおける旧デザイン専用教育システムでは，ファイルサーバへの課題作品の一斉提出時には教室ネットワーク全体が停止してしまうケースが頻発し大きな問題となっていた。

これらの問題点を解決し，今後更に増大するであろう負荷を軽減するために，教室ネットワークの構成には以下の要件を必須とした。

1. 教室ごとに１つのスイッチで端末全台に接続し，基幹ネットワークまで直接アップリンクする
2. 基幹ネットワークへのアップリンクは 1Gbps 以上の帯域を提供する
3. 端末側には100Mbps 以上の帯域を提供する
4. スイッチのモジュール構成はフルスペックとする

特に，後述するデザイン専用の情報処理教育システムIIを提供する教室では，専用ファイルサーバと端末が同じスイッチに接続されることを必須要件とした。この要件により，データ量の大きくなりがちな CG 系のファイルの読み書きもストレスなく運用できる環境が提供できる。

実際の設置においては，基幹ネットワークへの接続は，ギガビットイーサネットを 2 本利用して帯域と耐障害性を確保した。

2-2-2．機種選定とその他の要件

教室ネットワークにおいても，教材利用やデザイン作品の提示などを考慮すると，マルチキャストおよび Qos 機能の充実と安定性は非常に重要なポイントとなる。

入札段階で提案された機種のうち，同一メーカーのものとして Foundry　FastIron と Foundry　FastIronEgde が候補に挙がった。当初は，コストパフォーマンスに勝る Foundry FastIronEgde の購入が検討されたが，その後の調査で FastIronEgde は Qos 処理を CPU で行うため，実際の運用ではスイッチング機能が著しく低下してしまうことが判明した。教室ネットワークの構成は，その用途から見ても完全に要件を満たした上で実用に充分な性能を提供しなければならない。そこで Qos 処理を ASIC ベースで行うことのできる FastIron の採用を決定した。

2-3．フロアネットワーク

2-3-1．要件と機種

フロアネットワークとは，各フロア，教室および事務室などへ提供するエッジネットワークのことである。このレベルのネットワーク機器には，L2 機能のみの必須要件でも充分であるが，基幹ネットワークや教室ネットワークで重要視したマルチキャスト対応と Qos 機能についても必須とした。また，基幹ネットワークや教室ネットワークに比較して，コストパフォーマンスに検討の重点を置き，安価な SMC Networks 社製品の採用を決定した。

以上のフロアネットワーク敷設によりキャンパス全体で音声・動画などマルチメディアデータの配信に対応できることになったといえる。

2-4．VLAN

2-4-1．用途と要件

ネットワークのグループとしても最も基本的な分割の１つは，ブロードキャストドメインで

あると言える。このネットワーク分割の手段としては，通常 L3 レベルのルータでの分割が基本であるが，最近ではスイッチによる VLAN と呼ばれる論理的な分割手段も普及している。VLAN には，大きく分けて以下の 2 つの規格がある。

1. ポートベース VLAN：スイッチのポートをグループ化する
2. TagVLAN：パケットにつけたタグでグループ化する

本学の場合，サーバセグメントなどを中心にポートベース VLAN で基本構成を行い，キャンパス全体に点在する事務局ネットワークなどは TagVLAN で構成することにした。この 2 種類の VLAN を組み合わせることにより非常にきめ細かいネットワーク構成が可能となった。

また，日常の運用のなかでも特別な用途が発生した時，新たに VLAN を構成することにより自在なネットワーク提供が可能となった。このような VLAN 運用は，ネットワーク管理者による大学の要求に密着したオペレーションを目指す上で最も大きな武器の 1 つである。

2-4-2．VLAN 構成

2005年 9 月26日現在の本郷キャンパスの VLAN 構成は以下のようになっている。

VLAN 構成表

基幹 VLAN	B 館 3F VLAN	B 館 Call-3 VLAN
DMZ VLAN	B 館 4F VLAN	多目的ホール VLAN
Web カメラシステム VLAN	B 館 5F VLAN	マルチメディアラウンジ VLAN
ネットワークバックアップ VLAN	B 館 6F VLAN	インターネット端末 VLAN1(カフェ)
マネージメント VLAN	B 館 7F VLAN	インターネット端末 VLAN2（教室）
サーバ VLAN	B 館 8F VLAN	情報教育研究センター VLAN
隔離ネットワーク VLAN	D 館 2F VLAN	事務局 VLAN1
実験ネットワーク VLAN	D 館 3F VLAN	事務局 VLAN2
S 館 2F VLAN	D 館 4F VLAN	事務局 VLAN3
S 館 3F VLAN	D 館 5F VLAN	学籍情報 VLAN
S 館 4F VLAN	D 館 7F VLAN	就職資料室 VLAN
S 館 5F VLAN	S 館 CTR VLAN	就職情報 VLAN
S 館 6F VLAN	B 館 CTR-1 VLAN	国際交流センター VLAN
S 館 7F VLAN	B 館 CTR-2 VLAN	図書館 VLAN1
C 館 3F VLAN	B 館 CTR-3 VLAN	図書館 VLAN2
C 館 6F VLAN	B 館 CTR-4 VLAN	専門学校 VLAN
C 館 8F VLAN	B 館 CTR-5 VLAN	生涯学習センター VLAN
C 館 9F VLAN	B 館 CTR-6 VLAN	NAVAC VLAN
C 館 10F VLAN	B 館 CTR-7 VLAN	記念館 VLAN
B 館 1F VLAN	B 館 Call-1 VLAN	CLEC VLAN
B 館 2F VLAN	B 館 Call-2 VLAN	仁愛ホール VLAN

2-5．オープンネットワーク

2-5-1．目的と設置場所

インターネット接続が浸透した今，外来者も含めた様々なユーザーが大学内でのネットワーク利用に対してモビリティを要求してくることは当然予想できることである。

そこで，B 館 2F マルチメディアセンター，B 館 8F 多目的ホール，B's ラウンジおよび B's Cafe に以下の設備を設置してネットワークへの接続を提供した。

1．B 館 2F マルチメディアセンター

・情報コンセント　20基
・インターネット接続端末（Windows）　15台
・インターネット接続端末（iMac）　10台
・無線 LAN　1 基

2．B 館 8F 多目的ホール

・情報コンセント　102基

3．B's ラウンジ

・無線 LAN　1 基

4．B's Cafe

・インターネット接続端末（Windows）　3 台

2-5-2．認証ゲイトウェイ

インターネットおよび学内 LAN への接続が容易であることは便利であるが，同時に学外者のネットワークの悪用を誘発する恐れもある。そこで，B 館 2F マルチメディアセンター，B 館 8F 多目的ホール，B's ラウンジからのネットワークアクセスについては基本的に HTTP と HTTPS サービスのみを許可し，更に認証ゲイトウェイによるアクセス制限を掛けることにした。

認証ゲイトウェイの用途に適した仕様としては，IEEE802.1X と呼ばれる規格が最適であると考えられているが，現在に至るまで実際の製品として市場で定着しているとは言い難い状況にある。また，その他にも認証スイッチなど様々なメーカー独自のソリューションがあるものの，そのコストの高さや独自実装製品の管理技術を修得することは運用面でデメリットが大きいと判断された。

上記の状況の中で今回の導入では，情報処理学会の分散システム/インターネット管理技術研究会でも注目を浴びていた OpenGate [1) 2)] を採用した。OpenGate は，佐賀大学学術情報基盤センターで開発されたネットワーク利用認証ゲートウェイシステムで，ユーザー名とパスワードによる個人認証が可能である。以下に挙げる点が特長である。

1．GUI として Web ブラウザを利用しており，多様な OS の端末に対応可能

2．認証完了後，JavaScript による監視ウインドウが起動し，Web ブラウザの終了と同時にネットワークを閉鎖できる

3. 利用開始時と利用終了時に，日時・ユーザ名・IP アドレス等をログ記録可能
4. 汎用のソフトウェアを前提としており，既存ネットワークへの挿入も容易
5. GPL で配布されたフリーソフトである

実装は，FreeBSD4.x 以降で行われ，CGI を経由して ipfw と呼ばれるファイアウォールソフトの通過ルールの開閉を行う。堅牢で安定性が高い上，シンプルな仕組みなため Perl の知識があればカスタマイズが容易であることも大きな利点である。

また，何よりも大学のネットワーク管理という文化の中で開発されて実運用に耐えてきたソフトウェアである点が非常に魅力的であった。

本郷キャンパスでは，OpenGate 用に200人分のユーザーを登録し，そのパスワードを毎日作成し，情報教育研究センターのカウンターで記名・証明書提示と引き換えにパスワード手交を行っている。

2-5-3．無線 LAN

本システム導入の前の調査でも無線 LAN アクセスポイントの設置は要求度が非常に高いものであった。しかし，通信媒体が無線であるということは，セキュリティ面での大きなハンディキャップを持つため運用面では細心の注意が必要である。

本学では，旧来の IEEE802.11b（11Mbps）と導入時に最新の規格であった IEEE802.11g（54Mbps）の双方に対応可能なアクセスポイントを設置し，以下の設定を行っている。

1. WEP：64/128bit 共通鍵による暗号化通信
2. ANY 接続拒否：本学提供の ESS-ID を知っている者のみ通信可能
3. プライバシーセパレータ：無線 LAN 端末間の通信の禁止

なお，本学で採用したアクセスポイントは，WEP よりセキュアな運用が可能な TKIP や AES にも対応しているが，無線 LAN 端末側でこれらの暗号通信に未対応のものが持ち込まれることを想定して今回の導入では設定を見送った。また，無線 LAN 経由のアクセスはすべて OpenGate による認証を行っている。

3．インターネット/イントラネット管理システム

3-1．システム概要

今回の導入では，移設利用するメールゲイトウェイと Web メールサーバを除く以下のサーバ群の導入を行った。

1. ファイアウォール
2. 外向き DNS/WWW サーバ
3. 学内向け DNS サーバ
4. ストリーミングサーバ（オンデマンド）
5. ストリーミングサーバ（ライブ）

6. 教材データベースサーバ
7. バックアップサーバ
8. ウイルス対策サーバ

この節では，上記のサーバ群の内，本学にとって特徴のあるものについて概要を述べる。

ファイアウォールは，Fortigate 社の製品を採用した。特に，所謂ファイアウォールとしてのフィルタリング機能の他に，アンチウイルス機能，VPN ゲイトウェイ機能およびポリシールーティング機能を有す点が特長である。

本学では，HTTP/POP3/IMAP/FTP といった主要なサービスについてアンチウイルス機能を有効にしている。VPN ゲイトウェイ機能については，ベンダーからのリモートメンテナンスの他に，ネット試験など最近の Web ベースの試験への対応にも利用している。また，現在本郷キャンパスはインターネットへの接続口を，SINET（1.5Mbps）および ADSL（8 Mbps）の 2 種を有しており，ポリシールーティング機能を用いて Web 閲覧など利用者の多いサービスを ADSL 側に振り分けるなどして負荷分散する運用を行っている。

また，本郷キャンパスでは，長らく外部公開用の Web サーバを所有していなかったため，コンテンツの公開時に他学部のサーバを間借りするなどの苦労をしていた。今回の導入で外国語学部・経営学部・短期大学すべてに Web 公開のインフラが整った点は評価できると考えている。

ウイルス対策についても，ウイルス対策ソフトをコンピュータ教室のみならず，教職員の利用する端末にも Web 経由でインストール可能な仕組みを提供している。

更に，今後の教材の電子化が普及することを想定して教材データベースも設置してあり，今後の活発な利用が望まれる。

3-2．ストリーミングサーバ

今回の導入で，旧インターネット/イントラネット管理システムに比べて新しく追加された機能は，ストリーミングシステムである。ストリーミングシステムは，音声・動画といったリアルタイムにデータを再現する必要のある通信のために用いられる。

今後のストリーミングコンテンツの増加を想定した上で，教材利用を主眼に置いたオンデマンド用と遠隔会議などを想定したライブ用とそれぞれ独立にサーバを用意した点も特長である。従来，ストリーミングサーバは高価であったが，サーバソフトとしては OS に附属してくる Windows Media Server 9 を採用することで，コスト面を低く抑えながらもファストストリーミング機能による高速配信機能も提供できることとなり，充分な費用対効果を実現できる選択であったと考えている。

また，ライブ配信のためには動画のエンコーディングを行うシステムが必要となる。学内のネットワークのどこからでも動画をエンコーディング可能なように，サイズがわずか205/156/61mm（D/H/W）のパソコンを利用したシステムを導入した。これにより，学内 LAN に接

続可能なエリア全てからデジタルビデオで撮影した動画を学内・学外に配信可能である。このシステムによる本郷－ふじみ野キャンパス間の遠隔会議などへの応用を行いたいと考えている。

4．ネットワーク障害と今後の課題

新ネットワークを導入して１年になり，設定ミスや機器故障による重大なネットワーク障害などは無く比較的順調な運用であるといえるが，幾つかの障害や問題なども発生した。この項では，それらの諸問題についてふれ今後の課題についても述べる。

4-1．インターネット接続のボトルネック

新ネットワークシステム導入直後に顕在化した問題は，インターネット接続がネットワーク全体のボトルネックとなってしまった点であった。ネットワーク更新の成果で学内 LAN の高速化が実現されたのであるが，そのため却って本学のインターネット接続用専用線への負荷が急激に増加した。実際，MRTG で計測すると SINET 側へのトラフィックはピーク時で 1.2 Mbps を記録し 1.5Mbps の専用線の帯域を殆ど消費してしまっていたことが判明した。

この問題の解消のために ADSL 回線を契約し，ポリシールートで Web アクセスを ADSL 側に振り分けたことで現在は安定したインターネット接続を提供できている。今後も，保健医療学部の増設など本郷キャンパスのユーザー数が増えていくことが見込まれるため，インターネット専用線の帯域確保については常に注意していく必要がある。

4-2．SMC スイッチのバグ

VLAN 機能とコストパフォーマンスに注目してフロアネットワークを中心に採用した SMC6724AL2 であるが，管理用の VLAN を用いて遠隔操作を行うと，その他の VLAN ネットワークが停止するというバグがあることが導入後に判明した。従って，VLAN の設定変更などは直接スイッチの設置場所に出向く必要があり運用面では大きなデメリットとなった。その後，メーカーに改善されたファームウェアの提供を受け問題は解決された。

4-3．ブロードキャストストームの発生

エンドユーザーのミスオペレーションにより，ブロードキャストパケットが大量にネットワークに流出し，事実上ネットワークが停止する障害が 2 度起きている。今後は，エンドユーザーへの教育を続けると共に，SNMP などを利用したネットワーク監視システムを構築し，ネットワーク停止の防止や障害の原因となっているセグメントの早期発見などを可能にしていく予定である。

参考文献

1） 利用と管理が容易で適用範囲が広い利用者認証ゲートウェイシステムの開発，渡辺義明，渡辺健次，江藤博文，只木進一，情報処理学会論文誌，Vol.42，No.12，pp. 2802-2809（2001）
2） Opengate ホームページ，http://www.cc.saga-u.ac.jp/opengate/