埼玉大学 FTTL の構築

Construction of FTTL in Saitama University

伊藤 和人†, 田邊 俊治†, 小川 康一†, 吉浦 紀晃‡, 重原 孝臣†, 前川 仁‡
Kazuhito Ito†, Toshiharu Tanabe†, Koichi Ogawa†, Noriaki Yoshiura‡,
Takaomi Shigehara†, Hitoshi Maekawa‡

kazuhito@mail.saitama-u.ac.jp

†埼玉大学情報メディア基盤センター
‡埼玉大学大学院理工学研究科
〒338-8570 さいたま市桜区下大久保 255
† Information Technology Center, Saitama University
‡ Graduate School of Science and Engineering, Saitama University
255 Shimookubo, Sakuraku, Saitama 338-8570

概要

埼玉大学では平成 19 年 3 月に新基幹ネットワークとしてコアスイッチを中心に据えて講義室、研究室等の全室を光ファイバでコアスイッチに直収するスター型構成の FTTL を導入した。FTTL 採用に至った経緯、FTTL の設計、運用を事例紹介する。

キーワード

基幹ネットワーク, スター型ネットワーク, Fiber to the laboratory, 認証 VLAN

1. はじめに

大学の教育研究活動の計算機ネットワークに対する依存度はますます増大しており、高品質で安定なネットワークを提供することが大学の情報系センターの責務となっている。

これまで埼玉大学では、部局・学部学科の建物ごとにルータを設置し、バックボーンスイッチとルータ間をギガビット光イーサネットにより冗長性を考慮してリング状に接続するネットワーク構成を用いてきた。建物内(ルータ以下)は、ルータから各階へ、各階から各部屋へと、スイッチ(ハブ)を UTP ケーブルで多段配線して講義室・研究室・事務室等で計算機を接続している(図 1)。この既存ネットワークについて、以下に述べる問題が顕在化してきた。

1.1. 建物の制約を受ける LAN 構成

建物の新築や改築、組織の改組などにより、学部学科、事務といった組織が横断的に共用する建物が増加しており、1 つの建物、1 つの階に複数の組織が雑居したり、1 つの組織が複数の建物に分散する例が増えてきている。ところが、既存のネットワーク構成では、建物もしくは階が LAN の単位となっており、各組織に閉じた LAN を実現することが困難である。LAN を延伸するために独自に建物間に光ファイバを敷くケースも現れた。このようなネットワーク構成の変更が今後場当たり的に行われていくことは、ネットワーク管理上も、経費上も好ましいことではない。この問題の根源は、既存ネットワークでは建物のような物理的制約を受けない柔軟な LAN 構成が不可能なことにある。

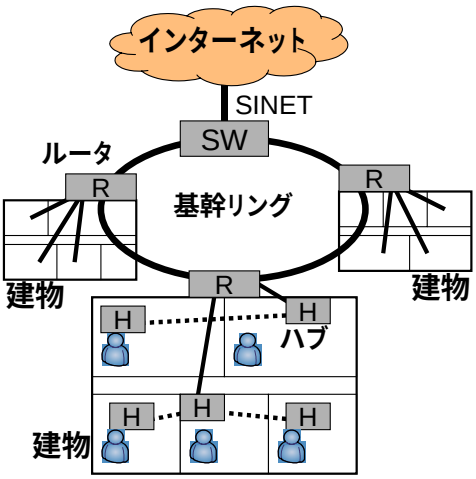

図 1 従来の基幹ネットワーク

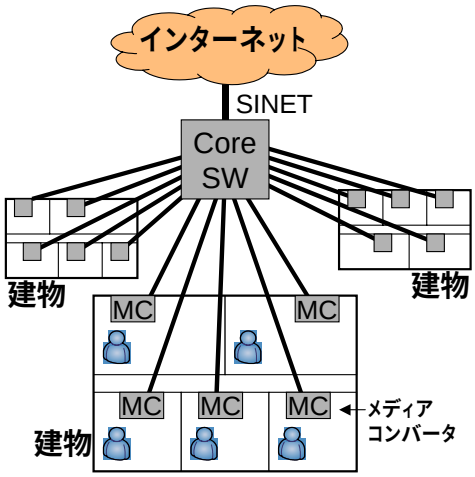

図 2 スター型ネットワーク

1.2. 恒常的な管理コスト

末端の機器にネットワーク接続トラブルが生じた場合、その解決には、ルータから何段のスイッチを経由しており、各スイッチがどこに設置されているのか知る必要がある。しかし、この情報を全ての末端機器について少数のセンター教職員が把握・管理することは極めて困難である。そこで、ルータ以下のネットワーク接続についてネットワークを利用する組織に管理を依頼している。これまでの運用では組織=サブネットであるため、各組織の管理者をサブネット管理者と称し、ルータ以下のトラブル(スイッチやスイッチ間配線の不具合)にはサブネット管理者と協力して対応している。学部学科などでは、教育研究に計算機を用いるユーザが自身のネットワーク環境維持をモチベーションとしてサブネット管理者となる例が多かった。しかし、ネットワークの利用者、利用頻度ともに増加した結果、サブネット管理者のボランティア的要素が増し、その負担も大きくなって来ている。

1.3. 脅威への対応の遅れ

ウィルス等に感染した情報機器は高速なネットワークを背景に広範囲に悪影響を及ぼす。学外に悪影響が及ぶ前に対処する必要があり、学内数箇所でトラフィックを観測し、異常通信を検出した機器のユーザに連絡して対応を要請している。しかし、ユーザへの連絡に人手を介するため対応が遅れたり、そもそもサブネット管理者の協力がないと当該機器のユーザが分からないといった問題が生じている。

2. FTTL の導入

前述の背景の下、本学情報システム更新に向けて次期基幹ネットワーク構成を検討し、従来の多段型ネットワークを廃して、コアスイッチと各情報機器を直結するスター型ネットワークを導入することとした。学内の講義室、オープンスペース、教員室、研究室、事務室など部屋を単位としてルータを介さずにコアスイッチから直接ネットワークを配線する(図 2)。将来の拡張性を考慮して配線には光ファイバを用いており、各家庭まで光ファイバを敷設する Fiber To The Home (FTTH)に倣い Fiber To The Laboratory (FTTL)と称している。光ファイバの敷設先は必ずしも Laboratory(研究室)ばかりではないが、敷設先の大半が研究室であることから FTTL としている。

光ファイバの末端(部屋)側には現行のイーサネット機器を接続するためのメディアコンバータ(MC)を設置し、既存の情報機器やスイッチ (ハブ)などのネットワーク機器がそのまま流用できるようにする。コアスイッチは部屋数分のポートを備えており、光ファイバの他端(コアスイッチ側)をやはり MC を経由していずれかのポートに直収する。

任意の複数ポートを集めて LAN を構成する機能をコアスイッチに装備することで、建物によらず部屋単位で組織に閉じた LAN を実現することが可能となる。また、認証 VLAN の機能により、認証 ID に応じて異なる LAN に接続した情報機器が同一ポート上に同居することが可能となる。これは、オープンスペースなどで同時に接続する情報機器間の不要なアクセスを遮断する効果がある。さらに、FTTL により、異常通信を行っている情報機器がどの部屋にあるか一目瞭然となり、認証 VLAN の場合には、どのユーザか、といったことまで直ちに知ることができる。

光ファイバの敷設先は 2000 室程度となり、巨額の工事費が必要なため情報システムレンタル契約に組み込むことが困難である。また、FTTL 自体は標準的なレンタル期間を超えて利用するものであることから、FTTL 導入は情報システム更新と別に行うこととした。必要な費用

は大学の経常経費から捻出することを覚悟して調達を開始したが、幸いにも平成 18 年度特別教育研究経費(概算要求)の配分を受け、費用の大部分を賄うことができた。

3. FTTL の設計

光ファイバを敷設し、MC を設置してネットワークを利用する部屋の実数調査を行った。これは、部屋側とコアスイッチ側の MC 数およびコアスイッチの必要ポート数を把握して新情報システムの仕様を決定するための基礎データとなる。想定するコアスイッチでは、100Mbps(以下 100M)対応ポートと 1Gbps(以下 1G)対応ポートを排他的に混載可能である。100M ポートに比べて 1G ポートの搭載スペースが大きく、1G ポートを増やすとより多くのコアスイッチが必要となり、高額になる。そこで、コアスイッチ台数の必要最少化を念頭に、100M ポートの利用を標準とし、特別な事情で 1G の容量が必要な部屋を申請してもらい、重要度とポート構成を考慮して情報教育用講義室や研究室を中心に 1G ポートに収容する部屋を決定した。これに基づき、仕様として 100M ポートを 1800 以上、1G ポートを 48 以上とした。

コアスイッチとしてアルカテル・ルーセント社 OmniSwitch 7800 [1]を 6 台使用する構成となった。OmniSwitch 7800 の主な仕様を以下に示す。

- 4094 個の VLAN
- 認証 VLAN 対応(256 個)
- VLAN 間アクセスコントロール可能(ACL)
- ポート単位で認証/非認証(固定)を切り替え

3.1. 認証 VLAN

認証 VLAN とは、ネットワーク利用時に利用者が自分の ID とパスワードを入力して本人確認(認証)を行い、ID に対応して予め決めておいた VLAN に情報機器を接続する仕組みである。大学の在籍者(教職員、学生)の全員に ID と初期パスワードを配布し、原則としてネットワーク利用時には認証を行うこととした。利用者認証および接続先 VLAN の取得には LDAP を使用し、負荷分散のため複数の LDAP サーバを設置している。サーバやプリンタなどは、ID/パスワードではなく MAC アドレスによって認証を行い、MAC アドレスに対応して予め決めておいた VLAN に接続する。

OmniSwitch では LAN 間のネットワーク通信を単方向または双方向に制限することが可能であり、認証 VLAN を用いると、教員、学生といった利用者の資格に応じて適切なアクセス制限を課すことができる。例えば、物品購入処理や成績報告のサーバ用の事務系 VLAN や研究室のサーバ用の研究室 VLAN を作成し、それぞれサーバを VLAN に接続しておく。こうすると、教員 ID で接続した VLAN から事務系 VLAN と自分の研究室 VLAN へアクセス許可、研究室所属学生 ID で接続した VLAN から自分の研究室 VLAN へアクセス許可、事務系 VLAN へアクセス禁止、のような運用が可能となる。

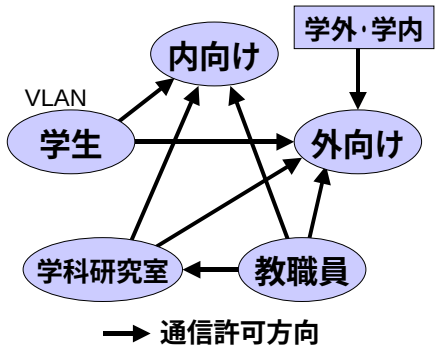

図 3 学科認証 VLAN の種類とアクセス制御

理想的には利用者 1 人に 1 つの VLAN を用意できれば、不要な利用者間アクセスを LAN レベルで遮断することができ、情報漏洩や計算機ウィルス伝染のリスクを大きく下げることが期待できる。しかし、最大認証 VLAN 数が 256 個である制約から、VLAN の粒度を荒くせざるを得ない。そこで、学科ごとに図 3 に示すように VLAN を作成し、VLAN 間アクセス制御を設定した。図 3 中に矢印で示した向きのアクセスのみを許可する。また、図 3 には示していないが、各 VLAN から学外(インターネット)、学内他学科の外向け VLAN、web やメールなど学内向け各種サーバへのアクセスなどは当然許可する。

各 VLAN の利用者および利用目的を以下に示す。

- 教職員 VLAN
  学科所属教員、学科事務員、技術職員が認証後に接続する。学科教職員のみが利用するサーバ等は、この VLAN に収容する。
- 学科研究室 VLAN
  研究室に所属する学生(主に学部 4 年生と大学院生)が認証後に接続する。教職員と学生が共用するサーバやプリンタ等は、この VLAN に収容する。
- 学生 VLAN
  学科所属の学部生(1～3 年生)が認証後に接続する。
- 内向け VLAN
  学科の教職員、学生のみにアクセスを許可したいサーバやプリンタ等を収容する。
- 外向け VLAN
  原則として本 VLAN のみが学外および学内他学部・他学科・他部署からのアクセスを許可する。学科メールサーバや web サーバなど、外部からのアクセスを許可する必要のある機器を収容する。

学科ごとに設ける学生 VLAN は、学科の内向け VLAN へのアクセスを当該学科学生に限定する目的のほかに、学部･学科間の計算機ウィルス伝染等を防ぐ効果がある。

学生が 4 年生になって卒業研究などにより研究室に配属されると、学生 VLAN ではなく学科研究室 VLAN に接続するように登録変更する。

上記の VLAN 構成では、学科教員間や研究室間のアクセスは制限できないので、例えば送信元制御のないプリンタを VLAN に接続すると他の教職員がプリント可能であったり、Windows ネットワークで他の研究室のコンピュータが見えたりすることになる。この点について各学部等の教員に事前にヒアリングを行い、学科内の教員･研究室に限定されれば許容できるとの意見に基づき、学科を単位として VLAN を構成することとした。

小講座制の学部や事務組織などは上記とは異なった VLAN 構成を採用しているが、合計して 150 程度の認証 VLAN を設定して利用している。

3.2. 認証ポートと固定ポート

OmniSwitch のポートは、ネットワーク接続の際に ID または MAC アドレスによる認証を必要とし、ID または MAC アドレスに応じて VLAN に接続する設定の他に、認証を必要とせず既定の LAN に直ちに接続する設定を選択することができる。前者の設定を認証ポート、後者の設定を固定ポートという。

例えば研究室(実験室)を固定ポートにすると、研究室内では PC、プリンタ、サーバなどがすべて認証なしに同一の VLAN に接続する。この VLAN は、前述の認証 VLAN と異なったものにすることができ、同学科の他研究室からのアクセスを遮断する運用も可能となる。複数の固定ポートが同一の VLAN になる設定ができるので、別々の建物にある複数の実験室を研究室の 1 つの VLAN にまとめることも可能である。

認証ポートの場合、事前にコアスイッチに MAC アドレスを登録しないとサーバやプリンタは利用できない。サーバ機を交換したり、プリンタを新規購入しても MAC アドレス登録を済ませないと利用開始出来ない。固定ポートでは、サーバやプリンタを MAC アドレスで認証する必要がなく、MAC アドレスの登録も不要となる。そのため、固定ポートの積極的な活用を推奨している。

3.3. 無線 LAN

講義室やオープンスペースでは無線 LAN によるネットワーク接続を利用する。無線 LAN スイッチ Trapeze [2] を利用し、OmniSwitch にはタグ VLAN(802.1Q)により接続する。Trapeze により 802.1X 認証を行い、利用者 ID が所属する認証 VLAN に対応するタグを付与する。OmniSwitch 内でタグを認証 VLAN に再マッピングすることで有線ネットワーク利用時と同じ認証 VLAN および VLAN 間アクセス制御を適用する。

3.4. グローバル IP アドレスによる運用

IP アドレスを認証キーとして学外サーバからライセンスを取得して動作するソフトウェアを利用するケースがある。この場合、グローバル IP アドレスを先方のライセンスサーバに登録するとともに、学内ではそのグローバル IP が確実にライセンス登録者の計算機のみに割り当てられることを保証する必要がある。

幸い埼玉大学はクラス B のグローバル IP アドレス空間を取得しており、FTTL と従来ネットワークの併用期間においてもほとんど全ての情報機器にグローバル IP アドレスを割り当て可能である。グローバル IP アドレスの利用により、NAT 等の利用に起因する問題を排除することができる。

3.5. 事後検疫の導入

埼玉大学では、学生が用意するノート PC を用いて英語教育を行っている。そのため、自宅等でネットワーク接続した際に計算機ウィルスに感染した PC が FTTL に接続される可能性が高い。もちろん、教員や研究室等の PC がウィルスに感染することもある。ウィルス等に感染した計算機の異常なネットワーク通信(学内⇒学外)をファイアウォールで検出し、OmniSwitch では当該 MAC アドレスの PC を特殊 VLAN へ隔離することで、VLAN 内および学外への異常ネットワーク通信を遮断する。ウィルスに感染した PC がいったん VLAN に接続した後(事後)に検疫する仕組みであり、事後検疫という。

PC の利用者はインターネットアクセスができなくなったり、web ブラウザの表示が隔離中を示すページへ誘導されたりすることで自分の PC が隔離されていることを知る。ウィルス対策を行ったことを報告すると隔離が解除される。対策が不十分であれば再度隔離されることになる。

4. 運用

FTTL 稼動にあたり、コアスイッチの約 1800 個のポートのそれぞれを認証ポートと固定ポートのいずれに設定するか調査を行った。この調査に正しく回答するには、認証 VLAN の仕組み、VLAN 構成と VLAN 間アクセス制御(図 3)、および固定ポートの働きを理解する必要がある。従来のサブネット管理者に各学部・学科・部署の取りまとめ役をお願いしたが、認証 VLAN を理解してもらうための説明にかなりの時間を割いた。実際に各サーバや PC の設定変更作業を行って初めて認証 VLAN を正しく理解できる場合も多く、要請に応じてコアスイッチの設定をやり直すなど初期設定が無駄になっているケース

が発生している。しかし、設定変更により柔軟に LAN 構成を変えられることが FTTL の本来の目的であり、設定変更は常に起こりうることなので、そのための練習が本格稼動前にできたとも言えるだろう。

FTTL が稼動しても、いきなり全面的に FTTL に切り替えることは不可能であるため、FTTL と従来ネットワークを並行稼動し、約半年間の期限を定めて FTTL へ移行することとした。FTTL と従来ネットワークの IP アドレス空間を別けているため、移行により IP アドレスが変更される。特に学科等で運用しているサーバ類の IP アドレス変更のタイミングに合わせて適切に DNS データを変更することが重要であるため、学科・部署の移行スケジュールを立て、学科・部署担当者と当センター職員が連携をとりながら移行作業を行っている。これを機会に、これまで自前で運用してきたサブゾーン DNS をセンター管理の DNS サーバへ移管する学科・部署も出てきている。

FTTL の下での無線 LAN は導入直後から稼動しており、学生はノート PC を無線 LAN 経由で接続してネットワークを活用している。無線 LAN 接続のための PC 操作方法に関する問い合せは多数あったが、認証 VLAN に関するトラブルはほとんど発生していない。

FTTL への移行段階では検疫(事後検疫)は停止している。これは、認証 VLAN に接続できないといったトラブル時に問題特定を容易にするためである。移行の進捗状況を見ながら慎重にタイミングを見計らって検疫を有効化する予定である。

5. まとめ

本稿では、埼玉大学 FTTL 導入の経緯と設計を中心に報告した。本稿執筆時点(平成 19 年 8 月)では従来ネットワークから FTTL への移行を進めている段階であり、運用の実際や FTTL 性能については不確定な部分が多く残っている。

利用者側からすると FTTL の直接の効果は見えにくく、むしろネットワーク利用の度に認証が必要であるため利便性が下がったと感じるかもしれない。しかし、管理コスト削減や認証 VLAN による LAN 構成の柔軟化といった長期的なメリットが順々に明らかになってくると信じている。

謝辞

埼玉大学 FTTL 構築にあたり、本学情報メディア基盤センター、研究協力部情報基盤課、サブネット管理者の諸氏に多大なご支援を頂いた。ここに深謝する。

参考文献

[1] アルカテル・ルーセント OmniSwitch 7800, http://www1.alcatel-lucent.com/com/en/appcontent/opgss/OS7000_br_tcm228-288021635.pdf

[2] Trapeze 無線 LAN スイッチ, http://www.macnica.net/trapeze/index.html