Vol.2015-IOT-30 No.10
2015/7/4

埼玉大学における光ファイバ直収型ネットワークの運用経験について

小川康一[†1]　吉浦紀晃[†1]

埼玉大学では，2007 年より光ファイバ直収型のネットワーク，Fiber To The Laboratory（以下，FTTL）を運用してきた．FTTL は学内 1,800 か所の部屋とサーバ室との間を光ファイバで直接接続する形態である．本論文では，FTTL の運用効果について述べるとともに，問題点を踏まえ 2012 年 3 月から運用を開始した全学情報基盤システム（Saitama Education and Research Network，以下，SERN）における取り組みについて述べる．

Operational Experiences of IT Services using Optical Fiber Network at Saitama University

Kohichi Ogawa[†1]　Noriaki Yoshiura[†1]

Saitama University has used the network named as FTTL (Fiber To The Laboratory) since 2007. This network consists of the optical fibers from one server room to about 1,800 locations on campus. The network operators of Saitama University had several problems in the network operation and had to solve the problems without reference cases. In March 2012, network equipment of the network was replaced. This replacement requires deep discussion on new network design and specification with careful consideration of the network operation from 2007 to 2012. This paper reports the process of designing the new network and also reports replacement and operation for the new network in March 2012.

1. はじめに

埼玉大学（以下，本学）は，首都圏にある国立大学である．5 つの学部（教育学部・教養学部・経済学部・工学部・理学部）が 1 つのキャンパスの敷地内にある．大学の構成員は，学生が約 10,000 人，教職員が約 1,000 人である．

本学の情報基盤システムは，学内ネットワークを構成する「基幹ネットワーク」，メールや Web, DNS，認証機能などを提供する「基幹サーバ」，パソコンを利用した演習を行うための「教育研究用システム」の 3 つで構成される．本論文では，この情報基盤システムのことを「全学情報基盤システム」と呼ぶ．本学では，情報メディア基盤センター（以下，センター）が全学情報基盤システムの調達および管理運用を行っている．2015 年現在，センターの組織はセンター長 1 名，専任教員 2 名，併任教員 1 名，専任の運用スタッフ2名, 併任の運用スタッフ1名で構成されている．

本学は，国立情報学研究所の学術情報ネットワーク（Science Information NETwork，以下，SINET）[1] の接続拠点となっており，埼玉県内の大学や研究機関におけるインターネットの接続中継点となっている．

本学では学内ネットワークを構成するネットワーク機器の老朽化に伴い，2007 年から大学全体のネットワークを刷新する必要があった．新たな取り組みとして検討を進めた構想は，大学構内の各部屋とネットワーク機器を設置するサーバ室とを光ファイバにより直接結ぶことであった．本学では，この取り組みを各家庭に光ファイバを敷設する“Fiber To The Home” (FTTH)になぞらえて，“Fiber To The Laboratory”（以下，FTTL）[2][3]と呼んでいる．

FTTL を導入した狙いは，大学の情報基盤システムの運用スタッフが不足していることにある．多くの国公立大学では，運用スタッフである情報系センターの職員が不足している状況にある．少数の運用スタッフで管理を行うためには，障害が発生しにくいシステムの導入が前提である．障害が起きた場合でもトラブルシューティングが容易で，メンテナンスし易いことが重要である．利用者の端末がある部屋とネットワーク機器の途中に複数の機器が存在する場合，ループなどの障害自体が隠蔽され，発生要因が発見しにくくなる．一方，FTTL で必要となる機器は，光ファイバと LAN ケーブルとを変換するメディアコンバータだけであり，障害点となるネットワーク機器が途中に介在しない．このため障害箇所の特定が容易になっている．

多くの国公立大学では，レンタルにより全学の情報基盤整備を行っている．レンタル期間は大学により異なるが，本学は 5 年単位の調達である．導入にあたっては仕様書の作成を行い，政府調達による競争入札方式をとっている．

本論文では，全学情報基盤システムのうち基幹ネットワークに焦点をあて，本学のネットワークの特徴である FTTL と FTTL 上で稼動する動的認証 VLAN を中心に，導入時期により 2 つに分けて述べる．2007 年から 2011 年までを第一期，2012 年から現在までを第二期と呼ぶ．第一期と第二期を通じて FTTL と動的認証 VLAN の運用経験から得られた教訓について述べる．

†1 埼玉大学情報メディア基盤センター
Information Technology Center, Saitama University

ⓒ2015 Information Processing Society of Japan

2. 本学のネットワークの特徴

本章では，2007 年に導入し，現在も運用を継続している FTTL と FTTL 上で稼働している動的認証 VLAN について述べる．

2.1 光ファイバ直収ネットワーク（FTTL）

FTTL は本学の建物 44 棟にある部屋，約 1800 か所をシングルモード光ファイバで接続する光ファイバ直収ネットワークである．ネットワーク構造は，大学の中心に位置するサーバ室を中心としたスター型構成である．

光ファイバの配線は，ネットワーク機器が置かれたサーバ室と，建物内の光中継盤を経由し，サーバ室と各部屋が光ファイバにより直接結ばれている（図 1）．図中の「MC」はメディアコンバータ，「光」は光ファイバを表す．

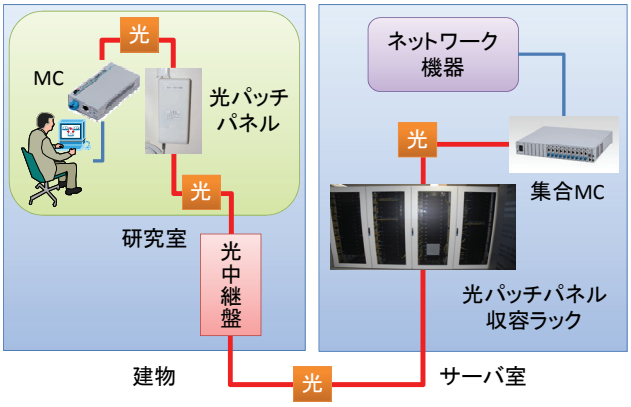

図 1　FTTL の概要
Figure 1 An overview of FTTL

サーバ室は光ファイバ敷設にあわせて，講義室を改装し構築した．サーバ室には，各建物と接続する光ファイバケーブルが集線されている．

図 3　各部屋の光パッチパネル（左）と
メディアコンバータ（右）
Figure 3 Optical patch panel (left) and media converter (right) for room

利用者の各部屋には 2 芯の光ファイバ 1 本が敷設されており，光パッチパネル（図 3 左）に収容している．各部屋には，LAN ケーブルをメディア変換するメディアコンバータ(図 3 右)を設置する．メディアコンバータは光パッチパネルと光パッチコードで接続して利用する．メディアコンバータは速度に応じて 10/100M 対応メディアコンバータ，もしくはギガビット対応メディアコンバータを用意してある．

サーバ室には，各建物の中継盤に接続された光ファイバの幹線が 4 つの光パッチパネル収容ラックに集線されている．光パッチパネル収容ラックと集合メディアコンバータ間を光ファイバパッチケーブルで接続している．集合メディアコンバータとネットワーク機器とは LAN ケーブルで接続している．

2.2 FTTL の運用管理

FTTL の運用は，部屋とサーバ室が直接光ファイバで接続されているため，物理的な接続を識別する必要がある．部屋の各光パッチパネルに固有の「光コンセント番号」を割り当て，管理を行っている．光コンセント番号は，3 つの識別番号で構成される．1 つ目の識別番号は，サーバ室の光パッチパネル収容ラックのトレイ番号を表し，図 4 のような各トレイを指す．2 つ目の番号は建物を表す．最後の端末番号はトレイの収容位置を表す．利用者は，障害時や新規のネットワーク設定希望の際には部屋の光コンセント番号を伝えればよく，調査の手間が少なくなっている．

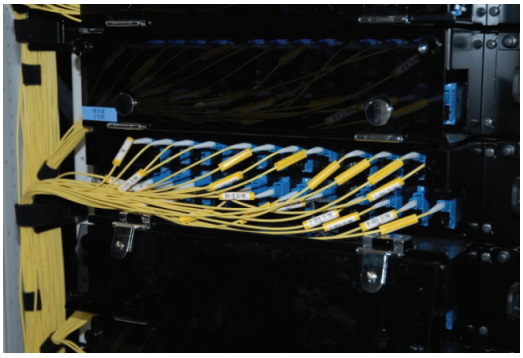

図 4　光パッチパネル収容ラックのトレイ
Figure 4 A tray of optical patch panel in racks

2.3 動的認証 VLAN の採用

本学では，動的認証 VLAN と固定 VLAN の 2 種類のネットワークを運用している．動的認証 VLAN とは，利用者がネットワークに接続する際に認証が必要なネットワークである．動的認証 VLAN の認証方法は，端末のブラウザを用い ID とパスワードを入力する「Web 認証」と，あらかじめ MAC アドレスを認証サーバに登録し，登録した MAC アドレスにより認証を行う「MAC アドレス認証」の 2 通りがある．一方，固定 VLAN とは部屋に対して特定のサブネットを割り当てるネットワークである．実際にはメディアコンバータの先にあるネットワーク機器のポートに設定する．固定 VLAN は認証なしで利用できる．

ⓒ2015 Information Processing Society of Japan

動的認証 VLAN を採用した理由は，ネットワークセキュリティの確保にある．本学は，一時的にせよ不特定多数の人が構内に出入り可能である．動的認証 VLAN を採用すれば，ネットワークを利用する際は認証が必要になる．利用者の特定が容易になり，万一のセキュリティインシデントに対しても即座に対応できる．

2.4 全学統一認証アカウント

全学情報基盤システムでは，本学の構成員に「全学統一認証アカウント」と呼ばれるアカウント（ID とパスワード）を発行し，動的認証 VLAN をはじめシステムを利用する際の認証に用いる．アカウントは LDAP（Lightweight Directory Access Protocol）を用いた認証サーバに格納し利用する．

全学統一認証アカウントには利用者の所属するグループ（学部学科など）ごとにネットワークを VLAN 単位で関連付けている（表 1）．一時的にネットワークを利用する来訪者には「一時アカウント」を発行し，利用する VLAN を制限のあるネットワークに割り当てることで正規の利用者と区別している．

全学統一認証アカウントと VLAN の関連付けは，無線 LAN アクセスポイントで接続した際に割り当てるネットワーク情報としても用いられる．つまり，有線 LAN で Web 認証した場合と，無線 LAN で認証した場合の両方で同一のネットワークを利用可能である．

表 1　アカウントと VLAN の対応表
Table 1 Table of accounts and VLANs

アカウント名	区別	職位	VLAN	VLAN ID
taro	正規	教員	教員VLAN	200
s15ab001	正規	学生	学生VLAN	300
・・・	・・・	・・・	・・・	・・・
user001	一時	一時	一時利用VLAN	500

2.5 動的認証 VLAN の仕組み

動的認証 VLAN は，認証機能を持つスイッチのほかに，ネットワーク認証サーバ，認証サーバ（LDAP），DHCP サーバが必要である．このうち，ネットワーク認証サーバは Web 認証時の LDAP の問い合わせと，MAC アドレス認証時の認証に用いられる．動的認証 VLAN における Web 認証の流れを図 5 に示す．図中の各番号は以下の通りである．

(1) **利用者が端末を起動する**

(2) **DHCP サーバから認証前 VLAN の IP アドレスを取得する**

認証前 VLAN とは Web ブラウザで認証する前のネットワークである．この認証前 VLAN がないと利用者の端末は認証画面を取得することができない．

(3) **利用者が端末のブラウザを起動する**

(4) **認証画面のリダイレクト**

認証スイッチに来た通信を取得して認証ページにリダイレクトし，認証画面を表示させる．

(5) **利用者への認証画面の提示**

(6) **全学統一認証アカウントの入力**

(7) **認証スイッチからネットワーク認証サーバへ問い合わせ**

(8) **ネットワーク認証サーバから認証サーバへの問い合わせ**

(9) **認証サーバからネットワーク認証サーバへの応答**

(10) **ネットワーク認証サーバから認証スイッチへの応答**

(11) **利用者へ認証成功の表示**

利用者のブラウザに認証が成功した旨を表示する．

(12) **認証後 VLAN の IP アドレス取得**

認証後 VLAN とは，認証が成功した後に利用者が実際に利用するネットワークで，全学統一認証アカウントで各アカウントに紐付けられた VLAN である．

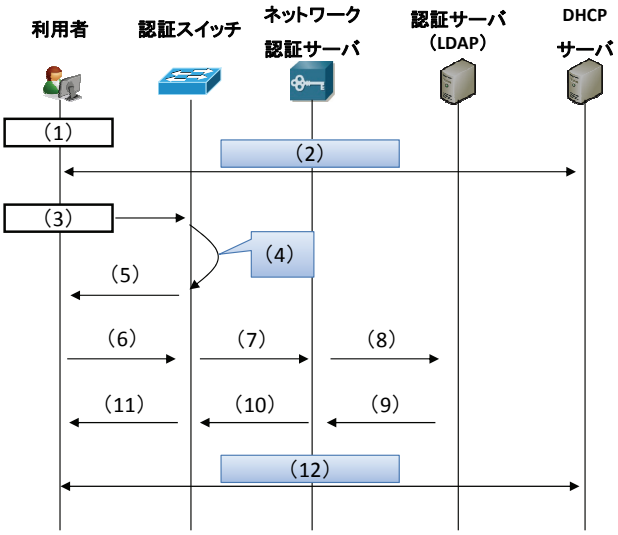

図 5　動的認証 VLAN のパケット配送シーケンスの例
Figure 5 An example of client authentication process and sequence of packet forwarding between each network equipment and authentication servers.

なお，動的認証 VLAN における MAC アドレス認証は，MAC アドレスを認証スイッチかネットワーク認証サーバのどちらかにあらかじめ登録しておき，照合することで認証を行う．

3. 第一期（2007 年～2011 年）

本章では第一期で運用した基幹ネットワークの構成，運用状況と問題点，問題点に対する対策について述べる．

3.1 基幹ネットワークの構成

第一期で運用したネットワーク構成を図 6 に示す． サーバ室内にある集合メディアコンバータでメディア変換した LAN ケーブルは，基幹スイッチに直接収容した．基幹スイッチ間の経路情報交換は，ルーティングプロトコルの

ⓒ2015 Information Processing Society of Japan

OSPF（Open Shortest Path First）を利用した．動的認証 VLAN は基幹スイッチで動作させた．動的認証 VLAN は，VLAN インターフェースを各基幹スイッチに収容する必要があった．どの基幹スイッチ配下でも同一の VLAN を利用可能にするため，MSTP（Multi Spanning Tree Protocol）[4]を稼動させた．上位の 2 台の基幹スイッチは 1 台の L2 スイッチに接続し 2 台のファイアウォールに接続した．

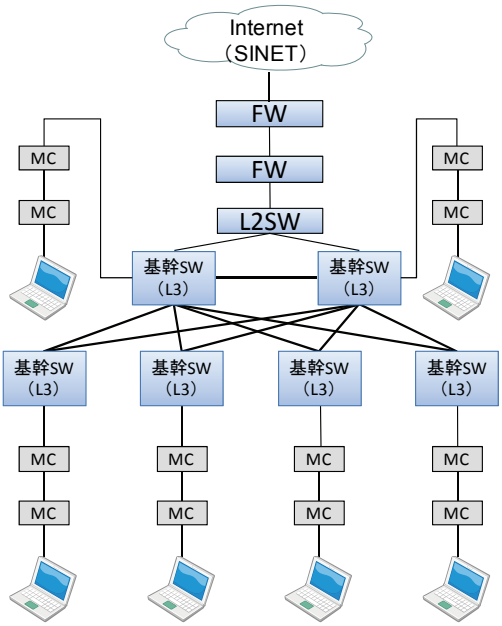

図 6　2007 年～2011 年のネットワーク構成
Figure 6 Network topology from 2007 to 2011

第二期における主要なネットワーク機器は以下の通りである．

- 基幹スイッチ（6 台）
  アルカテル・ルーセント社　：OmniSwitch7800
- レイヤ 2 スイッチ（1 台）
  アルカテル・ルーセント社　：OmniSwitch6300
- 無線 LAN アクセスポイント（80 箇所）
  Trapeze Networks 社：MP-372-JP

3.2　運用時に発覚した問題点

3.2.1　動的認証 VLAN の設定上限とリソース不足

基幹スイッチでは，仕様上動的認証 VLAN が 256 個までしか利用できない事がシステムの調達後に発覚した．スイッチの基本条件として MSTP や OSPF を稼働させる必要があり，動的認証 VLAN を多く稼働させるとリソース不足を生じさせる恐れがあった．実際の処理負荷を考えると，256 個以下の範囲で動的認証 VLAN を運用せざるを得なかった．大学がネットワークを利用する上での設定変更や，新規の設定を行って拡張することを無視した設計となっていた．利用者の環境に即した設計ではなく，調達した機器に合わせた設計になっていることがわかった．

3.2.2 動的認証 VLAN の不具合

動的認証 VLAN の運用では，ネットワーク稼働当初から 2 つの不具合が発生した．

1 つ目の不具合は，動的認証 VLAN のうち Web 認証で発生した．認証前 VLAN と認証後 VLAN はネットワークが異なるため，端末側で IP アドレスの再取得を行う必要がある．第一期の基幹スイッチでは，認証前と認証後のネットワークの切替えにブラウザで動作する Java アプレットを採用していた．このアプレットは，Java Virtual Machine のバージョンや利用者の環境に依存しており，バージョンによっては認証画面が表示されない不具合を引き起こした．

2 つ目の不具合は，基幹スイッチのリソースの枯渇問題であった．第一期では，動的認証 VLAN での利用を積極的に推進したため，多数の利用者が同時に認証した．結果，基幹スイッチは認証に多くのリソースを消費し，メモリ上の認証処理を行うためのバッファを使い果たす現象が発生した．バッファを使い果たすと，動的認証 VLAN が利用不能となり，基幹スイッチの再起動が必要となる．再起動が行われる際には，準備を含めて 30 分程度学内ネットワークが停止した．利用者はネットワークが利用できなくなり，研究活動や業務が停止するなどの影響があった．

3.3　問題点への対策

3.3.1 動的認証 VLAN の設定上限数の対策

動的認証 VLAN 数の制限に対応するため，VLAN 数を少なく運用する必要が生じた．そこで考え出した方法は，性質の異なる 5 つの VLAN を学科などの組織単位で割り当てることであった．5 つの VLAN は，学生が所属する「学生 VLAN」，教員が所属する「教員 VLAN」，学科のプリンタなどを共有する「内向け VLAN」，研究室の学生を所属させる「研究室 VLAN」，学外に公開するサーバを設置するための「外向け VLAN」である．VLAN ごとに Access Control List（以下，ACL）を設定して通信を制御した．ACL は，VLAN に割り当てられたサブネットとサブネットを許可もしくは制限するものであった．ACL は表 2 の通りである．

表 2　各認証 VLAN の ACL ルール
Table 2 Access control rules of each authentication VLANs

送信元 / 受信先	教員 VLAN	学生 VLAN	研究室 VLAN	外向け VLAN	内向け VLAN
教員 VLAN	―	拒否	拒否	拒否	拒否
学生 VLAN	拒否	―	拒否	拒否	拒否
研究室 VLAN	許可	拒否	―	拒否	拒否
外向け VLAN	許可	許可	許可	―	許可
内向け VLAN	許可	許可	許可	拒否	―

ⓒ2015 Information Processing Society of Japan

3.3.2 基幹スイッチのリソース不足の対策

基幹スイッチのリソース不足に対応するため，同一の VLAN を利用する箇所を同じ基幹スイッチに集めた．この方法により，MSTP に組み入れる VLAN の数を少なくした．この集約はサーバ室内での物理配線の差し替えにより実施した．この集約は基幹スイッチでの物理配線の差し替えにより行った．結果，動的認証 VLAN で MSTP を利用しても基幹スイッチのリソースが低下することなく，パケット転送に支障がなくなった．しかし，物理配線の入れ替えには VLAN を設定する時間に比べて多くの時間がかかった．VLAN を利用できる環境にも関わらず，物理配線の差し替えによりネットワーク構成の変更を行うことは VLAN の利点を活用し切れない結果となった．

3.3.3 動的認証 VLAN の不具合対策

1 つ目の不具合の対策は，利用者の端末にインストールされている Java Virtual Machine のバージョンを，動的認証 VLAN でサポートされているバージョンに合わせてもらうことであった．全学に周知を行ったが，利用者の環境が多様で対応に時間がかかった．

2 つ目の不具合の対策は，バッファの利用量が一定以上を越えた場合には基幹スイッチでバッファをリセットすることであった．スイッチメーカはバッファをリセットする処理を基幹スイッチのファームウェアに組み込み，バッファ枯渇による基幹スイッチの不具合を回避可能となった．この対応は一定の効果を発揮したが，完全に不具合が解消されることはなく，時々スイッチを再起動せざるを得ない状況が発生した．

4. 第二期（2012 年～現在）

本章では，第一期の教訓を踏まえ，第二期で導入した基幹ネットワークの構成，運用状況と問題点，問題点に対する対策について述べる．

4.1 ネットワーク構成

第二期では，第一期を踏襲し，FTTL と動的認証 VLAN は引き続き運用することとした．第二期ではシステムの名称を SERN（Saitama Education and Research Network）と名付けた．基幹スイッチで各 VLAN のネットワークインターフェースを持ち，レイヤ 3 レベルでのパケット転送を行う．動的認証 VLAN は，ボックス型のレイヤ 2 スイッチを多数配置することにした．この方針は，動的認証 VLAN の処理負荷をできるだけ細かい単位で分散するためである．小さなスイッチに機能を分散させることでネットワークの安定化を狙った．

具体的なネットワーク構成を図 7 に示す．図内うち，SINET スイッチ，ファイアウォール（FW），基幹スイッチ間はすべて 10 ギガイーサネットにより接続されている．認証スイッチは BOX 型スイッチを 45 台設置し，基幹スイッチはシャーシ型スイッチを 2 台設置し冗長構成をとった．

設計当初，基幹スイッチの冗長化に第一期と同様，STP（Spanning Tree Protocol）の導入を検討した．しかし，既に 2011 年には VLAN 数が動的認証 VLAN，固定 VLAN をあわせて 500 以上あった．今後も VLAN の増加が見込まれ，大量の VLAN を持つネットワークで STP を運用することは基幹スイッチにとって過負荷となり，パケット転送に支障が出る可能性がある．RSTP（Rapid Spanning Tree Protocol）[5]などのように STP の処理負荷の軽減を図ったものが存在するが，複数のレイヤ 3 スイッチを 1 台のレイヤ 3 スイッチとして扱うことができる機能として，シスコシステムズ社の Catalyst で VSS(Virtual Switching System) [6]とよばれる冗長構成技術を採用し STP を不要とした．

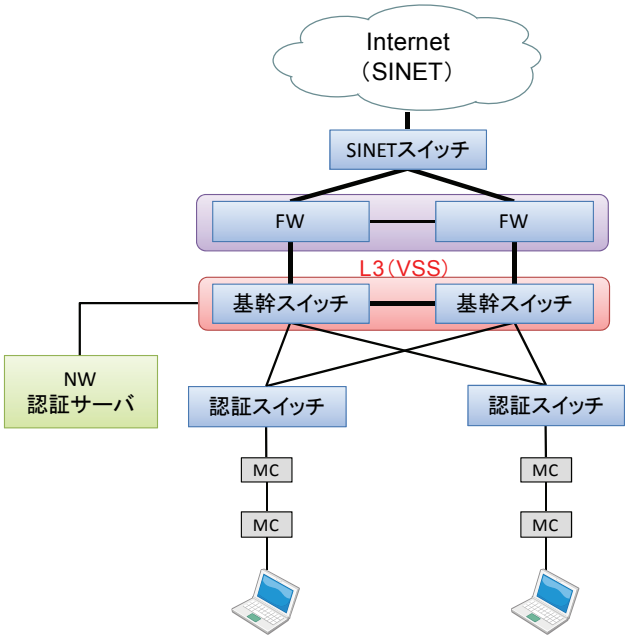

図 7　2012 年～現在のネットワーク構成
Figure 7 Network topology from 2012 to 2015

第二期における主要なネットワーク機器は以下の通りである．

- 基幹スイッチ（2 台）
  シスコシステムズ社　Catalyst6500
- 認証スイッチ（45 台）
  日立金属株式会社 Appresia13200
- 無線 LAN アクセスポイント（300 箇所）
  シスコシステムズ社　Aironet 1142

4.2 運用時に発覚した問題点と対策

4.2.1 動的認証 VLAN の障害

動的認証 VLAN では，認証前のネットワークと認証後のネットワークが異なるため．IP アドレスの付け替えが必要となる．第二期では，認証前に利用する DHCP のリースタイムを短くすることで IP アドレスを付け替えている．実際には，DHCP のリースタイムを当初 10 秒と設定したところ，端末の OS の違いにより動作が異なった．Mac OS の端末で

は問題がなかったが，Windows の端末では割り当てた IP アドレスが DHCP サーバから取得した後にすぐ消失し，Web 認証に用いる画面が端末のブラウザ上に表示できないという問題が発生した．そこで，現在は DHCP のリースタイムを 1 分にしている．現在も 1 分のまま運用しているが，特に問題は発生していない．

4.2.2 同一の認証前 VLAN の利用による脆弱性

同一の認証前 VLAN の利用により，障害が発生する事例があった．ある利用者の研究室で「端末が時々ネットワークに接続できなくなる」という障害が発生した．図 8 に障害時の接続構成の概要を示す．調査したところ，障害のあった端末は MAC アドレス登録を行っており，正しくネットワークに接続していた．障害が発生するときを狙って，認証スイッチでパケットキャプチャを行ったところ，障害のあった端末と同一の認証スイッチ内で 1 台の不審な端末を特定した．不審な端末は，障害のある研究室とは別の研究室にある学生のものであった．学生は，2 つの LAN カードをもつパソコンを所持しており，各 LAN カードで別々のメディアコンバータに接続していた．1 つの LAN カードは MAC アドレス登録をせずに利用し，意味もわからずに本来障害のあった端末に割り当てるべきグローバル IP アドレスを設定していた．この障害は，45 台ある認証スイッチで 1 台につき 1 つの認証前 VLAN を設定していたために発生した障害である．同一のスイッチの認証前 VLAN 配下では，端末同士が通信可能になっていた．幸い，パケットの盗聴やウイルスの感染などは見受けられなかった．

45 台ほどある認証スイッチで，1 台のスイッチにつき 1 つの認証前 VLAN を運用することは，セキュリティ上問題となることがわかった．そこで，各認証 VLAN として設定が必要なポートの 2 つにつき 1 つの認証前 VLAN を設定した．対策により同様の障害は発生しなくなった．

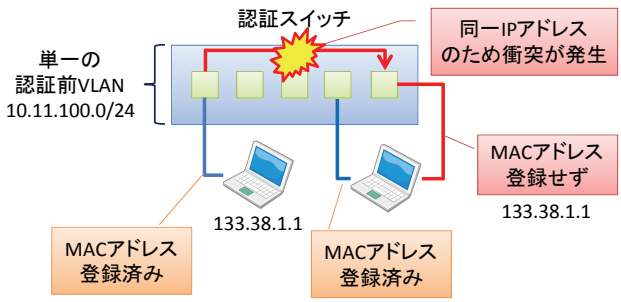

図 8　認証スイッチでの障害事例
Figure 8 Failure case of authentication switch

5. 第一期と第二期の運用経験に基づく教訓

本章では，第一期と第二期を通じて獲得した FTTL と動的認証 VLAN の運用経験に基づく教訓について述べる．

5.1 要件定義の問題

教訓の一つは，要件定義の重要性である．第一期は，ほとんど要件定義がなされていない状態であった．第一期で起きた問題のほとんどは，調達前に盛り込むべき仕様が正しく記載されていなかったことにある．運用スタッフが今以上に少なく，要件定義に時間がかけられなかった背景があった．

第二期では，第一期の反省を踏まえ，全学情報基盤システムを構成する要素ごとに専任のチームを結成して要件定義に時間をかけた．教員と運用スタッフが 1 名ずつペアになって，基幹ネットワーク，基幹サーバ，教育研究用システムの 3 つのチームに分けて仕様書の検討を行った．仕様書作成に十分な時間をかけることが可能となり，品質の高い仕様書が作成できた．

このように要件定義を徹底することで，システムの完成度を高め，障害が少ないシステムを構築可能なことを経験した．

5.2 IP アドレス設計の徹底

動的認証 VLAN の導入には，各 VLAN に割り当てる IP アドレスの設計を十分行う必要がある．

本学の各 VLAN は，グローバル IP アドレスで運用している．クラス B をサブネット分割で各 VLAN に割り当てている．第一期では，各 VLAN の IP アドレスプールに余裕があったが，端末や利用者の増加など，利用環境の変化によって IP アドレスが足りなくなる現象が顕著になった．

第二期では，昨今のスマートフォンやタブレットの普及によって，1 人あたりの端末保有台数は増加傾向にある．1 人当たりの端末保有台数増加は，IP アドレスの消費の増加につながる．結果，無線ネットワークの利用が拡大し IP アドレスが足りなくなる危険性がある．

動的認証 VLAN のうち，教員 VLAN や研究室 VLAN など合わせて 10 の認証 VLAN において割り当てるネットワークの拡張作業もしくは付け替え作業を実施している．作業にあたっては，ネットワークが一時的に利用不能となるため，利用者への負担が大きい．

IP アドレスの割り当て不足は，第一期に行った動的認証 VLAN の設計時の不備にある．動的認証 VLAN を採用する際には，各ネットワークセグメントの IP アドレスが充足した状態になるようアドレス設計を検討する必要がある．また，拡張が容易になるように割り当てたネットワークセグメントの前後を空けておく工夫も必要となる．

5.3 メディアコンバータの電源供給問題

FTTL を構成する場合にはメディアコンバータの電源配置に配慮する必要がある．

FTTL は，光ファイバを利用しているため，ネットワークの利用にはメディアコンバータが必要となる．メディアコンバータは電源を必要とする．つまり，FTTL は電源供給が断たれるとシステムとして機能しない．この弱点は，

東日本大震災の計画停電で明らかになった[7]．サーバ室という場所に一箇所に集中している点も弱点となった．2014年秋に大学当局の理解と協力を得て，サーバ室向けの自家発電設備を導入した．同時に学内の要所にも発電設備が整備された．今後，発電設備を活用した災害時の対応について実地訓練を検討している．

5.4 各 VLAN における責任者の明確化

FTTL のような集中管理型のネットワークに変更した場合，大学内の組織と連携してネットワーク管理体制を別途構築しておく必要がある．

本学で FTTL を運用した結果，個々の部屋とネットワークの接続拠点であるセンター管轄のサーバ室とを直接接続したため，部局の管理者の存在が希薄となった．結果，管理責任者が不明になった部局もあり，利用者が問い合わせる窓口を失う結果となった．現在は各部局ごとの善意によって管理の協力を頂いている．現在，VLAN 単位の責任者を配置し，センターと連携して管理運用にあたる体制を検討中である．

6. FTTL と動的認証 VLAN の考察

本章では, 本学で 2007 年から運用してきた FTTL と動的認証 VLAN についての考察を述べる．

6.1 FTTL の利点と欠点

FTTL のコンセプトは，部屋とサーバ室とを直接光ファイバで結ぶことにより，サーバ室での集中管理を可能とし運用管理を効率化するという狙いがあった．

FTTL の利点は 2 つある．利点の 1 つ目は，サーバ室での管理が可能であるため，トラブルシューティングを行う際に建物や部屋を行き来することがないなど，迅速な解決に役立つことである．しかし，いつでも FTTL で問題が解決するわけではない．サーバ室でトラブルが完結する場合もあるが，障害の原因が不明な場合や利用者の環境に起因する障害もあるため，実際には現地に赴く必要がある．

利点の 2 つ目は，各部屋のネットワークがサーバ室に集線されているため，利用者がネットワークを利用する上で幅が広がる点である．複数の部屋を束ねて 1 つの LAN を作りたい場合はサーバ室側だけの作業で完結する．これまでに LAN を構築した研究室は 20 件程度ある. LAN 構築以外に具体的な要望として実現したものには，いくつかの部屋で物理的にファイアウォールを経由させたい，スイッチに通したいという要望があった．このような要望にも柔軟に対応可能であった．

FTTL の欠点は，導入コストである．FTTL では，光ファイバの敷設費用やメディアコンバータの導入が必須である．メディアコンバータは 1 つが 10 万円程度と高額なため, 導入コストが高い．また，建物内に光中継盤やサーバ室にパッチパネル等の設備を収容する場所の確保が必要となる．光ファイバについては，切断や建物改修で再度敷設する際にかかる費用は UTP の配線を行う場合に比べて数倍から数十倍の差がある. 本学の場合は, キャンパスが分散せず, 1 箇所にまとまっていたことが FTTL の導入に適していたと考えられる．FTTL を導入する際には，全体的な費用対効果を確認しながら，導入の検討をする必要がある．

FTTL の運用にはメディアコンバータの故障についても注意を払う必要がある．メディアコンバータの故障率は, 1 年間あたり 10 件程度, このうち利用者の故意によるものが 2，3 件程度である．これまでに利用者の認識不足で，ファイバのコネクタを破損することや，メディアコンバータの一部を破損することがあった．これ以外にも，部屋の模様替えで部屋に敷設された光ファイバを切断する例が見られた．ネットワークの利用が少ない部屋ではメディアコンバータの故障発見が遅れることがあった．

6.2 動的認証 VLAN の利点と欠点

動的認証 VLAN の利点は 3 つある．利点の 1 つは，有線 LAN，無線 LAN に関わらず同じネットワークを利用可能なため，利用者が部屋を移動しても同一のネットワーク資源を利用できる点である．場所に関係なく作業を継続可能な点が優れている．

動的認証 VLAN の利点の 2 つ目は，一般的なレイヤ 2 スイッチと MAC アドレス認証とを併用することにより，1 つの物理線上で複数のネットワークを利用可能な点である．

動的認証 VLAN の利点の 3 つ目は，セキュリティインシデント対応に有効な点である．本学では年に数件，学内の端末がウイルスに感染し，外部ネットワークへ攻撃することがあり，外部機関からの通報がある．この際，動的認証 VLAN の認証ログや DHCP サーバのログを利用することによって，容易に利用者や感染端末の特定が可能となっている．

動的認証 VLAN の欠点は 3 つある．欠点の 1 つ目は，ネットワーク機器により動的認証 VLAN の設定可能数が制限されていることである. 動的認証 VLAN を導入する際にはネットワーク機器の仕様を十分確認しておく必要がある．一見, 機器の仕様上は動的認証 VLAN の数が多く利用可能と表記されていても，システムとして稼動させた場合には動かない場合があるので注意が必要である．

欠点の 2 つ目は, 第二期で発覚した認証前 VLAN の脆弱性を考慮すると多数の認証前 VLAN が必要になる点である. 1 つのポートで 1 つの認証前 VLAN を構築した場合は, スイッチに設定可能な VLAN 数を超える可能性がある．一般的なスイッチでは，VLAN 設定の上限が 4096 個までという制限がある．本学の運用方法のように基幹スイッチに認証 VLAN を設定する場合，基幹スイッチの VLAN 設定数が膨大になることが懸念される．

欠点の 3 つ目は，動的認証 VLAN 特有の認証前 VLAN と認証後 VLAN の扱いである．認証前 VLAN から認証後 VLAN へ切り替わる際，利用者の端末の IP アドレスの付

け替えが発生する. 付け替えの方法には注意が必要である. 第一期の運用では, 付け替えの方法をソフトウェアに頼り, 端末環境によっては動作しないことが問題であった. この教訓を踏まえ, 2011 年からの運用では端末に依存せず, ブラウザのみで認証を完遂できるシステムにした.

7. 関連研究

大学における大規模な VLAN の運用は, 広島大学[9]をはじめ, 岡山大学[10], 京都大学[11]で行われている. 特に岡山大学では, 大規模認証ネットワークの運用に関して, 管理運用を通じて得られた経験が述べられている[12][13]. 大学における光ファイバ網を用いた学内ネットワークの運用例は, 光直収ネットワークを構築した群馬大学の Fiber To The Desk, "FTTD" [14]がある. 本学がサーバ室の集合メディアコンバータを通じてスイッチと接続しているのに対して, FTTD では研究室のメディアコンバータとサーバ室にあるコアスイッチとを直接光ファイバで接続している点が異なる. 琉球大学では, GE-PON を活用した試み[15]を行っている. 運用に工夫が必要であるが, 本学の FTTL と比較してコストが低減できる可能性がある. 大規模な VLAN 運用には, システム化によるサポートが有効である[16]. 近年, Software Defined Networking（以下, SDN）と呼ばれるネットワーク運用手法が登場し注目を集めている. SDN は, 多数の VLAN を少数の運用スタッフで管理する場合には有効な技術である. 広島大学では, VLAN 設定の自動化[17]に取り組んでおり, 大学の情報系センターの人的リソースが削減される中で有効な方法である.

8. おわりに

本論文では, 光ファイバ直収ネットワーク FTTL と動的認証 VLAN の運用について, 2007 年から現在に至るまでの運用経験を述べた. 本学が身をもって経験したように, 要求仕様をよく検討せずに調達してしまうと, 調達後に仕様に制限があることが判明することや, 想定していた機能が正しく動作しない恐れがあることがわかった. 健全で信頼性の高いネットワークの構築においては, 要件定義に時間をかけることが重要である. 結果として運用時に大きな影響を及ぼし, 利用者に迷惑をかけることとなる.

構築前後のトラブルの顕在化を通して, 本学の規模のネットワークの維持管理には, 人手が重要であることを再認識した. 今後も少数の運用スタッフで効率よく管理できる方法を模索していきたい. 本学の様々な運用経験や対応策が, 他の環境におけるネットワーク構築・運用に少しでも役立てていただけると幸いである.

参考文献

1) 学術情報ネットワーク SINET4, http://www.sinet.ad.jp/
2) 伊藤和人, 田邊俊治, 小川康一, 吉浦紀晃, 重原孝臣, 前川仁 : 埼玉大学 FTTL の構築, 学術情報処理研究, No.11, pp.124-128 (2007).
3) 田邊俊治, 小川康一, 伊藤和人, 吉浦紀晃 : 光直収ネットワークによるキャンパスネットワークの管理運用, 第 9 回インターネットテクノロジーワークショップ論文集, pp.1-8 (2008).
4) IEEE : IEEE 802.1s, "Virtual Bridged Local Area Networks - Amendment 3: Multiple Spanning Trees" (2002).
5) IEEE : IEEE 802.1w, "Standards for Rapid Reconfigureration Spanning Tree" (2001).
6) Cisco システムズ : テクノロジー解説 Virtual Switching System(VSS)1440, http://www.cisco.com/web/JP/news/cisco_news_letter|/tech/vss/index.html
7) 小川康一, 吉浦紀晃 : 首都圏近郊の大学における計画停電の影響と対策, 情報処理学会論文誌 54(3), pp.1028-1037(2013).
8) Nick McKeown, Tom Anderson, Hari Balakrishnan, Guru Parulkar, Larry Peterson, Jennifer Rexford, Scott Shenker, and Jonathan Turner ACM SIGCOMM Computer Communication Review, Volume 38, Number 2(2008).
9) 大東俊博, 近堂徹, 岸場清悟, 田島浩一, 岩田則和, 西村浩二, 相原玲二 : 広島大学における新キャンパスネットワークへの移行手法, 情報処理学会研究報告, インターネットと運用技術（IOT）, 2008(87), pp.31-36(2008).
10) 岡山聖彦, 山井成良, 大隅淑弘, 河野圭太, 藤原崇起, 稗田隆 : 岡山大学における認証・ロケーションフリーネットワークの構築, 学術情報処理研究, No.15, pp.161-165(2011).
11) 高倉 弘喜,江原 康生,宮崎 修一,沢田 篤史,中村 基典,岡部寿男 : 安全なギガビットネットワークシステム KUINS-III の構成とセキュリティ対策, 電子情報通信学会論文誌. B, 通信 J86-B(8), pp.1494-1501(2003).
12) 山井成良, 岡山聖彦, 大隅淑弘, 藤原崇起, 河野圭太, 稗田隆 : 岡山大学における大規模認証ネットワークの運用と課題, 情報処理学会研究報告, インターネットと運用技術（IOT）, 2013-IOT-20(10), pp1-6(2013).
13) 山井成良, 岡山聖彦, 大隅淑弘, 藤原崇起, 河野圭太, 稗田隆 : 岡山大学における大規模認証ネットワークの運用と課題(2), 情報処理学会研究報告, インターネットと運用技術（IOT）, 2013-IOT-21(27), pp.1-6(2013).
14) 上田浩, 井田寿朗, 青木正文, 齋藤貴英, 酒井秀晃, 伊比正行, 高橋 仁, 船田 博, 矢島 正勝, 久米原 栄 : キャンパス内光直収ネットワークの構築と運用, 学術情報処理研究, No.14, pp.56-63 (2010).
15) 大川康治, 遠藤聡志, 谷口祐治, 久保田恵子, 庄司博光, 岸本克巳 : GE-PON を利用したキャンパスネットワークの構築と運用, 情報処理学会研究報告, インターネットと運用技術（IOT）, 2012-IOT-18(3), pp.1-5(2012).
16) 飯島智之, 新善文, 木村浩康, 木谷誠 : ON-API(Open Networking-Application Programming Interface)と ON-API を用いたネットワーク管理アプリケーションの開発, 情報処理学会論文誌 49(3), pp.1052-1060(2008).
17) 近堂徹, 田島浩一, 岸場清悟, 吉田朋彦, 岩田則和, 大東俊博, 西村浩二, 相原玲二 : 運用の効率化を目的としたネットワーク構成管理と自動設定の実現, 情報処理学会研究報告, インターネットと運用技術（IOT）, 2015-IOT-28(33), pp.1-6(2015).

ⓒ2015 Information Processing Society of Japan