

# 大学の情報系センターに必要と思うこと

小川 康一

国立大学法人埼玉大学 情報メディア基盤センター専門技術員

概要：大学の情報系センターは、予算や人的リソースが限られ、非常に厳しい立場におかれている。その上、セキュリティ対策などの新たな対応が求められている。本稿では、実務に携わる技術職員の立場から、埼玉大学での取り組みを紹介するとともに、今後の大学情報系センターのあり方について述べる。

キーワード：大学情報系センター、光直収ネットワーク、システム運用技術、セキュリティ対策

## 1. はじめに

大学の情報系センターは、周囲を取り巻く様々な環境の変化により厳しい立場にある。最近では、サイバー攻撃による情報漏えいなどの事案が多発しており、セキュリティ対策が急務となっている。業務量が減るばかりか、情報系センターに求められる要請や多種多様なサービス導入の要望は年々増加傾向にある。しかし、現状は予算や人的リソースが限られている。本稿では、このような厳しい環境下において、埼玉大学での独自の取り組みを紹介するとともに、今後の大学情報系センターのあり方について述べる。

## 2. 埼玉大学における全学情報基盤システムの運用

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、学部生 7,020 名、大学院生 1,111 名、教職員 773 名（2016 年 5 月 1 日現在）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。我々は、この情報基盤システムのことを「全学情報基盤システム」（Saitama university Education and Research Network, 以下 SERN）と呼んでいる。本学では、情報メディア基盤センター（以下、センター）が SERN 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、派遣職員 1 名、非常勤の事務職員 3 名で構成されている。

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）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。本学をはじめ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。少数の職員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必要となる。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で介在しない。このため障害箇所の特정이容易になっている。

## 3. 本学の基幹ネットワークの特徴

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。

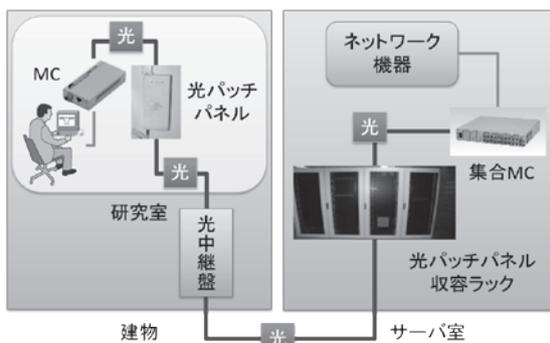


図1 FTTLの概要

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2 各部屋の光パッチパネル（左）とメディアコンバータ（右）

利用者の各部屋には2心の光ファイバ1本が敷設されており、光パッチパネル（図2左）に收容している。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2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いる。

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收容ラックに集線されている。光パッチパネル收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。

このように、本学のネットワークは光ファイバで部屋とサーバ室とが直接接続されている。FTTLは、集中管理ができるというメリットは大きいですが、メディアコンバータを必要とするため、結果的には非常にコストが高いネットワークであるといえる。

## 4. センター運営上の工夫

### 4.1 人員体制

人員不足の問題は、人件費になるため予算とも関連する。前章で述べた通り、本学のセンターには2人しか主担当者がいないため、人手不足が深刻であった。そこで、2015年から話し合いを進め、センターに所属していない他の学科の技術職員にセンターの業務を支援してもらう協力体制をとった。開始から約1年になるが、窓口の対応や技術面での支援、どうしても複数でやらなければならない作業など、都合をつけて対応していただいている。この活動は副産物として、センターで獲得した知識をもとに所属先で発生したネットワーク障害を解決したり、セキュリティなどの啓蒙活動などを行っていただいたりと、相乗効果が生まれている。

### 4.2 セキュリティ対策

本学のセキュリティインシデントについては、日々たくさんのインシデントが発生しており、対応に苦慮している。最近多くみられるのは、「偽装メールによる偽サイトへの誘導」である。この事例は、利用者が送られた偽装メール内のURLをクリックし、偽サイトに誘導され、IDとパスワードを搾取されてしまう事案である。このインシデントは非常に多く発生している。

このインシデントは、ただIDとパスワードが盗まれるだけでなく、悪意を持った者が、盗んだIDとパスワードを利用して大量のメールを配信する事案に繋がっている。このようにして大量のメールが配信されると、本学の送信メールサーバの処理が追いつかなくなることがあり、大学のメール機能が麻痺する事もある。

本学ではActiveMailをWebメールとして利用しており、こちらを狙った偽装メールが

横行している。図3は偽装メールの例であるが、利用者が落ちていて読めば、内容がおかしいと判断できるが、急いでいる教員はきちんと読まずに焦ってメール本文中のURLをクリックしてしまうようである。

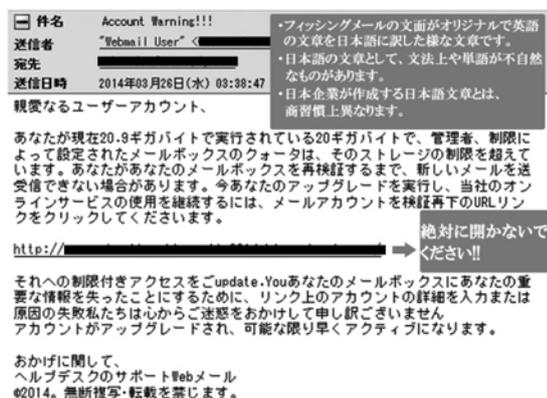


図3 ActiveMailの偽装メール  
(出典：クオリティア社ホームページ<sup>1)</sup>)

その他のインシデントとして、「外部からの攻撃と対処」がある。これは、学内の端末がウイルスに感染して、外部のサイトを攻撃する事案である。これは主に外部からの通報によって発覚することが多い。

このようなインシデントが日々発生する状況を受け、本学でも遅ればせながらセキュリティ対策実施手順書を今年制定、施行した。この狙いは、インシデント発生時の対応フローと役割の明確化にある。部局連絡担当者と部局総括責任者、センターやCISOとの連携を明確化した。



図4 セキュリティ講習会の様子  
(左：一般利用者向け、右：責任者向け)

セキュリティ教育の取り組みとして、定期的にセキュリティ講習会(図4)を行っている。しかし、講習会の参加者が講習後に前述のActiveMailの偽装メールに引っかかるといふ事案が発生し、根気よく開催しなければ

1 <http://www.qualitya.co.jp/phishing/>

ならないと考えている。学生についてはまだ対応が進んでおらず、来年度からE-Learningでの対応を進める予定である。

セキュリティの啓蒙活動としては、大学で教職員が参照するグループウェアがあり、こちらで最新のセキュリティ注意喚起など周知を行っている。しかし、グループウェアに掲示しても見ない教員がいるため、事務職員がメールなどで周知することも期待している。

本年度は新たな試みとして、パソコンの目につく所に貼付する「セキュリティ注意喚起シール」を作成中である。図5は現在のシールの製作中のイメージである。本学のマスコットキャラクターである「メリンちゃん」を入れて利用者に親しみやすくし、連絡先を明記して一覧性を図るなどの工夫をしている。実際に効果があるかの検証はこれからである。

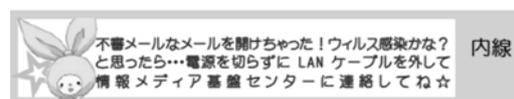


図5 注意喚起シール(製作途中のもの)

セキュリティの内部監査としてチェックリストによる点検を行っている。現在は外部公開しているサーバを中心にポートスキャンを行い、実際のネットワーク管理者、サーバ管理者にチェックリストを送付し、内容を確認する方法をとっている。回答の内容次第では、詳細な確認をセンターが実施する方法をとっている。

#### 4.3 運用における創意工夫の視点

システム運用技術は、創意工夫を行う余地のある研究分野である。私は、新しい技術や要請への挑戦の一環として、「システム管理運用の研究」に取り組んでいる。これまで情報系センターで経験した様々な知見について、整理し発表することを継続している。

実際、得た知見を発表させていただきながら、その過程で色々な知識が得られている。このような研究的視点が重要であると考えており、学会参加を積極的に行っている。主に情報処理学会のインターネットと運用技術研究会(IOT研究会)や電子情報通信学会のインターネットアーキテクチャ研究会(IA研究会)に参加し、論文作成や口頭発表を行っている。研究会に参加される先生方や研究者との情報交換や議論の中で新しい発見があり、モチベーションの維持に役立っている。

## 5. 今後の情報系センターに必要と思うこと

実務に携わる職員として、私が考える今後の情報系センターに必要と思われる要素を3つ挙げてみたい。

1つ目は、業務をタスク単位で切り出しておくことである。このためには業務の内容を整理する必要があるが、切り出しておくこと、たとえば派遣職員の方に定型的な業務を依頼することや、外部のサービスを利用するなど、選択肢の幅が広がる。また、切り出したタスクの中で、ある程度妥協できるタスクも出てくる。なんでもかんでも情報系センターでやらなければならないというのではなく、ここは思い切って「なくす」「減らす」ということも考える時期ではないだろうか。

2つ目は、技術伝承と技術レベルの維持である。これは運用技術の「火」をたやさないということである。組織内部でのOJTに限界はあるが、ノウハウを残していくべきだと考えている。

3つ目は、属人化を減らす努力と工夫である。私は、個人でその人でなければできないという形にならないように複数体制で情報共有を行っている。ちょっとしたことでもメールを構成員全体が参加するメーリングリストに流すようにしている。

前述の通り、情報システムの管理運用にはまだまだ工夫できる余地があると考えており、視野を広げるためにも研究的な視点を持って考えることも重要であると感じている。

## 6. まとめ

大学の情報系センターには課題が山積しているが、業務の見直しとタスク切り出しによる協業協働体制を築くこと、システム運用の自動化、外部サービスの効果的な活用が必要である。技術要素として Software Defined-Network や IoT デバイス、ロボットなどの活用も視野に含まれてくると考えている。運用技術については創意工夫による効率化はまだできる余地がある。今後少数で運用できる技術革新があるかもしれないが、最終的に大学の内部に少数でもいいので、受け継ぐ人材という資産を残すことが重要である。つまり、各大学や利用者の立場に立って考える人が必要ということである。

## 7. おわりに

本稿では、本学の情報センターにおける取り組みについて実務サイドからの視点を述べた。今後の情報系センターに対する環境は益々厳しいものになると予想される。最近では、人工知能やセンサー、IoT デバイスなどの技術革新のスピードが目覚しく、そう遠くない未来に情報基盤の運用に携わる技術者もロボットに置き換わる時代が来る可能性が高い。しかし、情報基盤を使うのは「人」であり、そして対応するのは「人」であるべきだと私は考える。コンピュータやロボットなど機械にはできず、人の能力を必要とする局面は必ずある。今、我々は厳しい環境におかれているからこそ、逆に新しいアイデアは必ず生み出せるものと信じている。

- i 小川康一, 吉浦紀晃, “埼玉大学における光ファイバ直取型ネットワークの運用経験について”, 情報処理学会研究報告インターネットと運用技術(IOT), 2015.