九州芸術工科大学のネットワークとセキュリティ

藤村, 直美
九州大学デザイン基盤センター情報基盤室

平山, 善一
九州大学デザイン基盤センター情報基盤室

https://doi.org/10.15017/1470674

出版情報：九州大学情報基盤センター広報 : 学内共同利用版. 4 (2), pp.70-78, 2004-08. 九州大学情報基盤センター
バージョン：
権利関係：

九州芸術工科大学のネットワークとセキュリティ

藤村直美，平山善一

1. はじめに

九州大学(九大と略す)と九州芸術工科大学(芸工大と略す)は平成15年(2003年) 10月1日に統合した。これに伴って、芸工大は九大の大橋キャンパスとして、芸工大の情報処理センターは九大の情報基盤センター大橋分室として位置づけられた。大学の統合に対応するために平成15年8月23日～25日に芸工大の学内ネットワークを九大の学内ネットワークの一部として組み込む作業を行った。今回の大学統合によって、芸工大の学内ネットワークはある意味で歴史の幕を閉じたこととなる。本稿では、これまでの芸工大におけるネットワークの変遷と管理・運営、セキュリティに対する取り組みについて報告する。

芸工大の学内ネットワークシステムを略称として KIDNET と呼んでいる。KIDNET は、学術研究、情報処理教育、図書館システム及び事務処理システムを統合する上で欠かせない重要な情報基盤であり、情報処理センターのネットワークサーバ群および情報処理教育システムをはじめ学内のほとんどすべての計算機間の通信を支えてきた。KIDNET の形態は大きく分けて、平成 2 年 (1990年)3月に設置した Ethernet(イエロー)ケーブルを使ったバス型ネットワーク、平成6年 (1994年) 3月に補正予算で既存の Ethernet ケーブルを FDDI の基幹ネットワークで相互接続したリング型ネットワーク、平成 13 年 (2001 年) 9月に補正予算で全面更新を行った情報処理センターのギガビットスイッチを中心としたスター型ネットワークの3つに分けることができる。以下、これらのネットワークの構成と特徴について紹介する。なお、参考までにこれまでのネットワークに接続されている (ネットワーク接続装置等を除いた) 計算機接続台数の推移を表1に示す。

表1　年度別計算機接続台数

年　　度	接続計算機台数	備　考
平成6年4月	214	FDDI ネットワーク構築
平成7年4月	331	
平成8年4月	455	
平成9年4月	701	
平成10年4月	978	
平成11年4月	1,218	
平成12年4月	1,481	
平成13年4月	1,665	

平成 13 年 10 月	1,701	ギガネットワーク構築
平成 14 年 4 月	1,745	
平成 15 年 9 月	1,596	大学統合
平成 16 年 4 月	1,842	

2. ネットワークの変遷

2.1. Ethernet によるネットワーク（第一期）

平成 2 年（1990 年）3 月に情報処理センター（以後、センターと略す）の計算機システムを三菱電機製の MELCOM-COSMO 700Ⅲ/MP から富士通製の FACOM A-700 SX/UTS という UNIX システムに更新した。これを機会に、学内の全ての建物に Ethernet ケーブルを張り巡らして、学内ネットワークを整備した。この時、A-700 と一緒に導入した富士通製の ΣSTATION （Σ230/C12) を貸し出し用ワークステーションとして学内に配布したこともあって、本格的な学内ネットワークの運用が始まった。

幹線の Ethernet ケーブル(500m)を情報処理センターから主要な建物間に引き、各建物内は 1 階から最上階までの廊下天井裏に Ethernet ケーブルを配線し、支線ネットワークを構築した。幹線と支線ネットワークはブリッジまたはリピータで接続し、幹線と距離が離れている建物は、光リピータで接続した単一のネットワークであった。IP アドレスとして当時はクラスＢの 133.22.0.0 を使っていた。各部屋に設置している端末までは、天井裏の Ethernet ケーブルにトランシーバを取り付けて、そこから AUI ケーブルを引き出すという方式であった。このため、天井裏から各部屋の壁に AUI ケーブルを引き出すための穴を殆どすべての部屋に開けた

当時は学内ネットワークに接続する計算機が約 80 台と少なかった。これは UNIX ワークステーションが高価で一般利用者は容易に手に入れることができなかったためと思われる。そこでネットワークの利用を促進するため、センターのレンタル費用で導入した UNIX ワークステーションを利用者に貸し出す運用を行った。この仕組みは学内ネットワークの普及に大きく貢献したが、その後、平成 14 年（2002 年）に、パソコンの高性能化と低価格に合わせて貸し出しワークステーションの仕組みを廃止したが、それまでは分散システムの主役であった。

2.2. FDDI によるネットワーク（第二期）

平成 6 年（1994）3 月に補正予算でネットワークの整備を行った。この時は学内の主要な建物に 7 つの FDDI ノード(Cisco7000 ルータ)を設置し、これらを 100Mbps の二重化した光ケーブルで接続して基幹ネットワークとした。さらに各建物の支線ネットワークは、第 1 期のものをそのまま利用し、1 階から最上階まで配線された 10Mbps の Ethernet ケーブルを FDDI ノードに接続した。全体

としてはFDDIによる基幹ネットワークと合計11セグメントからなる支線ネットワークを統合したループ型ネットワークとなった。

その数年後の補正予算で全国的にATMスイッチを中心としたネットワーク整備が進められた時に、芸工大ではATMスイッチによるネットワークの導入は適当でないという判断から要求を見送ったため、このFDDIネットワークは7年間も使用することになった。7年も使用していると、導入当時に比べて、接続計算機数や利用者数の増加、ネットワーク利用の多様化等により、ネットワーク上の通信量は年々増加し、端末側が10Mbpsの共用型ネットワークであるバス型LANでは、例えば次のような問題が発生して、対応しきれなくなった。

(1) 各建物に配線している1本のEthernetケーブルに200台を超える計算機を接続した建物が数箇所あり、応答が悪くなると共に、新規の端末接続用のIPアドレスが不足するようになった。
(2) 共用型ネットワークでは、ネットワーク上を流れる通信データを他人が簡単に傍受することができ、十分なセキュリティを確保することができない。
(3) 建物の支線ネットワークに障害が発生した場合に、200台を超える計算機が接続されていると、トラブルの原因究明に膨大な時間と労力を必要とする。実際にHUBの不良による支線ネットワークの障害で、Ethernetケーブルを数箇所も切断して原因究明に当り、復旧までに2日間も要したこともあった。
(4) 10Mbpsの共用型ネットワークでは、動画や音声を含むマルチメディア通信を使った教育や研究が行えない。

2.3. ギガビットスイッチによるネットワーク（第三期）

EthernetとFDDIネットワークによる問題点を解消するために、ネットワークの更新のための予算を要求していたが、平成12年度の補正予算によってネットワークの更新を行うことができることになった。この時のネットワーク更新にあたっては、これまでの利用形態がそのまま継続できることを条件に次の4点を基本方針としてネットワークを設計した。

(1) キャンパス内の基幹ネットワークと支線ネットワークを高速化し、マルチメディア通信を使った教育や研究に十分耐えられるネットワーク構成にする。
(2) キャンパス内の全ての建物の各部屋に情報コンセントを敷設する。情報コンセントは最低でも100Mbpsを占有できる通信路を確保するために、教官研究室には1個、複数の学生が出入りする研究室には2〜3個を目安に敷設する。(3号館、5号館の一部及び地域共同研究センターには既に情報コンセントが敷設されていたのでそれを流用する。)
(3) マルチメディアデータを含む学内のあらゆるデータを格納するために高速大容量のネットワークディスクアレイ装置を導入する。
(4) セキュリティの強化を図るため、必要な機器を導入する。

結果として、第三期では情報処理センターに設置したギガスイッチと各建物のエッジスイッチをGbEで接続したスター型LANとなった。これによって端末側まで100Mbpsの通信帯域を確保することができた。また、第1期及び第2期で敷設した10MbpsによるEthernetの利用を完全に廃止した。平成16年5月現在、大橋キャンパスではこのネットワークで運用を行っているので、次節で現ネットワークシステムの詳細について述べる。

3. 現ネットワークシステムの構成

現在使用しているネットワークでは、ネットワーク機器(バックボーンスイッチ、エッジスイッチ、対外接続ルータ)、ネットワークディスクアレイ、各種サーバマシン、学内情報掲示システム（案内役）を導入したが、ここではネットワーク機器の概要について報告する。

3.1. バックボーンネットワーク

基幹となるバックボーンネットワークは、キャンパス内の通信が集中するため、高速/大容量のスイッチングルータを導入した。このスイッチは、障害に対する冗長性を持たせるために、CPU 及び電源部を二重化しており、障害が発生した場合でもスイッチを止めることなく活性挿抜が可能である。これによって基幹ネットワークの障害発生によるキャンパス全体のネットワークへの影響をできるだけ少なくしている。バックボーンネットワークから各建物に設置した支線ネットワークのエッジスイッチ(合計27台)には1Gbpsで接続し、完全なスター型ネットワークとなっている。

3.2. 支線ネットワーク

各建物内の支線ネットワークは、2ポートのギガビットイーサネットと32～80ポートの10Mbps/100Mbps自動認識可能なエッジスイッチで構成している。エッジスイッチの設置台数は合計27台で、これらのスイッチと各部屋に敷設した情報コンセントをカテゴリ5E UTPケーブルで接続している。情報コンセントが多い部屋については、中継用のスイッチ(Catalyst 2912)を設置した（3号館、5号館の一部、地域共同研究センター、講義室等)。

情報コンセントは、一部の建物を除いて殆ど敷設されていなかったので、新たに475箇所に敷設した。情報コンセントの設置場所と個数については、教官研究室1個、複数の学生が集まる研究室は2～3個を基本条件にした。

エッジスイッチは、基幹スイッチと連携して複数の建物に分散した学科及び部局毎に仮想ネットワーク(VLAN)を構成している。現在、情報処理センター、環境設計学科、工業設計学科、画像設計学科、音響設計学科、芸術情報設計学科、応用情報伝達講座、地域共同研究センター、付属図書館、事務局及び講義室等の公共の施設毎に合計11のVLANで構成し、運用している。

VLANはネットワークへの物理的な接続でなく、スイッチのソフトウェアによ

って実現できる仮想ネットワークであり、スイッチのポート単位でVLANを構成している。このVLAN機能により、同一VLAN内での機器の移動が生じた場合でも、機器のネットワーク情報を変更することなくそのままの設定で利用することができる。この仕組みを利用して、講義室で授業を行う教員が自分の研究室で準備していたノートパソコンをそのまま講義室に持参して情報コンセントに接続すると、そのまま続けて使用できるという運用を行っている。

3.3. 学外接続ルータ

従来のネットワークでは、学外接続のルータとしてパソコンにフリーのUNIXを乗せて運用してきたが、今回の更新において専用のルータ(Juniper M5)を導入した。このルータは、基幹ネットワークスイッチに接続する1000BASE-SXポート、ATMスイッチにOC-3で接続するポートを有している。このルータは芸工大の規模から見るとやや過剰なぐらいの性能を有するが、これは将来のトラフィック増を見込んでのことである。

3.4. 学内情報掲示システム（案内役）

第3期のネットワークの更新に併せて、学内情報掲示システム、通称「案内役」を導入した。これは休講情報、講義情報、補講情報、学生呼び出しなどを電子的に掲示するもので、多次元デザイン実験棟、センター、5号館1階にKIOSK端末を、また多次元デザイン実験棟、センターにはプラズマディスプレイによる掲示版も設置した。このシステムを使用することで、学生はこれらの掲示板やKIOSK端末だけでなく、パソコンのブラウザ、携帯電話からも休講情報などを得ることができるようになり、大変好評であった。

大学全体にこの仕組みを使った情報提供を行いたいという要望があり、平成16年（2004年）4月からこのシステムを新しいCampusmate/Portalシステムとし、大橋キャンパスだけでなく、箱崎キャンパスも対象に情報提供を行えるようにした。ただし、箱崎キャンパス向けはまだデータ入力の体制が十分にできていないためか、実際には情報提供は行われていない。今後の活用を期待したい。

4. 対外接続回線の種類と速度の変遷

芸工大の対外接続の変遷を表2に示す。芸工大を最初に広域ネットワーク(電話回線を利用したJUNET）に接続したのは昭和63年（1988年）であるが、その後、藤村がWIDEプロジェクトへ参加し、芸工大のネットワークをWIDEインターネットに接続した平成3年3月末が、インターネットに接続した最初である。以後、次に示すように次第に回線速度を改善してきており、現在は1Gbpsで箱崎キャンパスと接続している。最初の専用線接続時の19.2Kbpsに比べると5万倍以上高速になっており、一方、年間の支払額としては、一時期500万円を超えていた時期もあるが、現在は最初の19.2kbpsの専用線の頃の

年間 15 万円弱の５倍少々にしか過ぎない。この回線速度の改善と価格の推移は感慨深いものがある。

表２　KIDNET 対外接続ネットワークの変遷

年月	回線種別	キャリア	通信速度	接続先	接続機器
1988.8	電話回線	NTT	2400bps	JUNET	Σ230
1991.4	専用線	NTT	19.2Kbps	WIDE	Σ230
1992.4	専用線	NTT	64Kbps	WIDE	Σ230
1994.4	専用線	QTNeT	192Kbps	WIDE	S-4/2
			64Kbps	SINET	Cisco3102
1995.8	専用線	QTNeT	1.5Mbps	SINET, WIDE	FMV-466D3 (BSD/OS)
1999.4	ATM 線	QTNeT	44Mbps	同上	Dell(FreeBSD), ASX-200WG
2000.12	ATM 線	QTNeT	135Mbps	同上	同上
2002.4	ATM 線	QTNeT	44Mbps	同上	同上
2003.3	ダーク ファイバ	NTT	1Gbps	SINET, QGPOP	WDM(LE-501), SW(9006SX/SC)
2003.8	ダーク ファイバ	NTT	1Gbps	KITE	WDM(LE-501), 基盤センターコアスイッチ

5. 運用管理

新ネットワークでは、ネットワーク監視装置を導入している。この監視装置ではネットワーク全体を構成している機器を階層化したマップとして表示し、障害の程度により色分けして表示することが可能である。これによって、障害が発生した機器を簡単に見分けることができる。また、ネットワーク監視用のソフトウェアで、各スイッチのリアルタイムパフォーマンス状況をグラフで表示できたり、装置及び各ポートの異常を自動的に検出して知らせてくれる。このシステムの導入で一番効果があったのは、不正 IP アドレスを使用している計算機の発見であった。

本学の場合は、グローバルな IP アドレスを使用しており、利用者が間違って他人の IP アドレスを使用することがたまに起こる。従来の FDDI ネットワークでは、不正 IP アドレス使用の計算機を見つけるのは容易ではなかったが、スイッチ型ネットワークではスイッチにネットワーク経由でログインしてコマンドを 2, 3 個ほど、実行するだけで簡単に発見することができる。

ネットワークを運用開始してから、定期的に各スイッチの通信状態（送受信数、

エラー発生件数等)を調査して判明したこととして、高速なネットワークを整備したにも係らず、100Mbps の情報コンセントに 10Mbps の HUB を接続して利用している箇所が結構存在していることである。このような接続を行っているところは、スイッチから HUB への送信エラーが多発している。8 ポートの 10/100Mbps の SW-HUB が安価になっているので、ネットワークを快適に利用するためにも従来の低速な HUB の使用は止めて、是非 SW-HUB を購入するように推奨している。

6. セキュリティについて

6.1. ファイアウォール

平成 3 年（1991 年）にインターネットに接続した当時は学内から学外、学外から学内ともに何ら規制せずに自由に通信できるようにした。当時、東京工業大学が外部との通信を規制してインターネットの運用を開始したが、奇異に感じたものである。今から思えば先見の明があったと思うが、当時は通信を規制しないことが当然であるかのように考えられていた。しかしながら平成 7 年（1995 年）の秋頃、外部から学内のある学科の計算機の管理者権限を乗っ取られ、その計算機を踏み台として海外の計算機を攻撃するのに使われるという事態が発生した。これを機会に学内の計算機を外部に剥き出しにしておくと悪意のある攻撃から守れないことを確信した。

最初に狙われやすいポートへの通信を遮断することとし、平成 8 年（1996 年）1 月に対外接続部分で telnet、tftp、smtp のポートを閉じた。そのため学外から学内の計算機へ telnet で直接通信できなくなるので、中継用計算機を準備し、学外からは一旦この計算機にログインしてから、改めて学内の計算機にログインする仕組みに変更した。ただしまだ ssh は学内に向けて直接通信できるようにしていた。

その後、さらに外部からの攻撃が悪質になり、平成 8 年 8 月にさらに pop2、pop3、login、nfsd のポートも閉じた。しばらくはこれで持ちこたえていたが、平成 13 年（2001 年）2 月に、echo、chargen、ssh、whois、domain、finger、sunrpc、netbios、exec, shell、printer、uucp、callbook、canna、x11 などを追加で遮断した。これで学外から学内の計算機を使用するためには必ず ssh で中継用計算機を経由しないといけなくなった。この中継用計算機は教職員と大学院生、卒業研究生にはアカウントを発行するが、学部学生には発行しないので、若干のサービス低下を招いた。

こうして対外接続におけるポートを次第に閉じてセキュリティを維持してきたが、さらに外部からの攻撃が悪質かつ組織的になってきたために、これでも現実的ではない状況になった。そこで、平成 14 年（2002 年）2 月 18 日（月）から対外接続における規制の基本方針を次のように根本的に変更した。

- 原則として、学外からは業務上必要な通信のみ通過させる。すなわち、その他のトラヒックは学外から学内向けには通さない。
- WWW サーバはできるだけ情報処理センターのものを使用する。

・研究室における WWW サーバの運用は、できるだけ控える。万一、研究室で WWW サーバを運用する際は、情報処理センターにファイアウォールの設定変更を依頼する。また、常にセキュリティ対策を行い万全の体制で運用を行う。
・不必要な WWW サーバは停止させる。
・研究室などで運用するメールサーバもきちんと保守できるだけの技術を維持できていない場合は運用を中止し、センターのメールサーバを利用する。

すなわち、原則として学外から学内への通信は遮断する。したがって、外部からアクセスするサービスを提供する計算機についてはファイアウォールの設定変更依頼をセンターに行う必要がある。これに伴って、当初の見込み通り、例えば FTP はパッシブモードでないと通信できないなど、若干の影響は出たが、やむを得ないと判断している。

平成 14 年 1 月に当時の瀧山学長の要請で情報セキュリティ講習会を開催した。全教職員が参加を期待されたが、最終的に約 6 割の教職員が参加した。これによって、上記のネットワークの運用方針の変更などを含め、様々な状況を適切に伝達することができ、学内のコンピュータセキュリティに関する意識を向上することができた。その後、平成 16 年（2004 年）5 月現在でも、対外接続の基本方針は原則としてクローズという方針を堅持しており、九大との統合においても、大橋キャンパス内の計算機を守るために、箱崎キャンパスも原則として外部と見なして、ファイアウォールを運用している。

6.2. ウイルス対策

コンピュータウイルスの発展には目を見張るものがある。最初のコンピュータウイルスは昭和 63 年（1988 年）に作られたとも言われているが、最初に芸工大でコンピュータウイルスが発見されたのは今となっては定かではない。芸工大において、ウイルスが大きな問題として認識され、組織的な対応を始めたのは平成 13 年（2001 年）8 月からである。当時、SIRCAM、CODERED、NIMDA などが立て続けに流行し、学内でも台数は少ないながらウイルスに感染する例がでてきた。特に CODERED は平成 13 年（2001 年）8 月 6 日に問題になり、教授会の直前であったことから、教授会の席を借りて、直接教員にウイルスの説明と対応をお願いした。

芸工大では、ネットワークの運用を始めてメールを使えるようにして以来、常に一台の中継用計算機で学内と学外のメールの転送を中継する方針を堅持してきた。そのためウイルスが普及し始めたのを契機に平成 13 年 11 月にメール中継用計算機に加えて、ウイルスチェックサーバを導入した。これによって学外から学内向けと学内から学外向けのすべてのメールのウイルスチェックを行うことにした。当初はメールの内容をチェックするということに異議があるかもしれないと色々と心配もしたが、特段の異議の申し立てもなく、順調にウイルスチェックを行えるようになった。

学内と学外を行き来するメールのウイルスチェックを行うことにしても、

WWW 経由で感染する例や、学外に持ち出して感染して来る計算機などもあり、まだまだ十分とは言えない。各研究室などで導入している計算機にウイルス対策ソフトウェアを導入するように依頼をしたが、なかなかウイルス対策ソフトウェアは普及しなかった。そこで、情報処理センターでトレンドマイクロ社製のウイルスバスターを 1000 ライセンス分一括契約し、無料で配布することにした。これに要する費用は初年度が 100 万円弱で、2 年目以降が 50 万円弱となり、最大 1000 台で使用すると、契約更新時の費用が通常の 3150 円から 500 円程度まで低減できることになり、大学全体の経費を抑えることができる。

この試みも最初はなかなか普及しなかったが、無料で安全を手に入れることができるということで、平成 16 年（2004 年）5 月現在で、この仕組みを利用してトレンドマイクロのウイルスバスターを導入し、定期的にパターンファイルを更新している Windows 系の計算機は 600 台弱になっている。このことから当初のもくろみはそれなりに達成されて来ていると考えている。

7. おわりに

九州芸術工科大学のネットワークシステムについて概要を紹介した。これまで大きく分けて 3 段階のネットワークの変遷があった。これまでの 15 年あまりで IP アドレスの付け替えも、クラスＢからクラスＣ×１６に切り替えた時、スター型のネットワークに変更した時、大学統合の時と 3 回も経験した。通常はこれだけ過激にネットワークの構成を変更することはないような気もするが、大学の規模が適度であったこと、関係者の理解があったこともあって、順調にネットワークの構成変更、管理・運用を行ってこれたと考えている。

九大との統合でセンターは九州大学情報基盤センター大橋分室になった。これに伴って事務系の職員が 2 名から 0 名になった。技術系職員 3 名については、あらたにデザイン基盤センターの中に情報基盤室を作り、こちらに所属するようにした。現在の大橋キャンパスにおけるネットワークの運用については各種申請書の形式や代表者の名前は変わったが、実質的には従来通りの管理・運営を行っている。九大の一部になった今となっては必ずしも小回りが利かない面も出てきているが、これからもネットワークの動向に注意を払い、できるだけ快適なネットワーク環境を提供していきたいと考えている。

謝辞

現在九州大学大学院システム情報科学研究院の堀良彰氏には 1994 年 4 月の芸工大赴任以来、ネットワーク関連を中心に情報処理センターの管理・運用に多大の貢献をしてもらった。ここに記して心から感謝したい。またこれまで広域計算機ネットワークへの接続や運用については多くの関係者の方々にお世話になっている。この場を借りて改めて感謝の意を表したい。