

教育支援機能を強化したキャンパス情報ネットワークの構築

Development of Campus Information Network System Enhancing the Learning and Instructional Support

升屋 正人*, 下園 幸一*, 高橋 至*, 相羽 俊生*,
古屋 保*, 小田 謙太郎*, 森 邦彦*

Masato MASUYA*, Koichi SHIMOZONO*, Itaru TAKAHASHI*, Syunsei AIBA*,
Tamotsu FURUYA*, Kentaro ODA*, and Kunihiko MORI*

鹿児島大学 学術情報基盤センター*

Computing and Communications Center, Kagoshima University*

鹿児島大学の学内ネットワークシステムは、1994年にFDDIキャンパス情報ネットワーク、1996年にATMネットワーク、2001年にギガビットキャンパス情報ネットワーク、2009年に高度情報通信基盤システムと、4世代にわたり整備、更新されてきた。2015年に整備した第5世代のキャンパス情報ネットワーク（KNIT5）では、通信の高速・大容量化への対応や情報セキュリティ対策の拡充に加え、無線LANによる教育支援機能の強化を図った。

キーワード：キャンパス情報ネットワーク、無線LAN、セキュリティ

The campus information network system of Kagoshima University has been replaced four times since 1994 when it was first installed. In the 5th generation system – KNIT5, that was the most recent replacement in 2015, we aimed to handle its traffic growth, to improve its security, and particularly to enhance its function of the learning and instructional support by the wireless LAN system.

Keywords : Campus information network system, wireless LAN, security

1. はじめに

キャンパス情報ネットワークの企画・開発・運用・管理は、国立大学法人の情報系センターにとって重要な業務の一つである。鹿児島大学においても1993年6月にインターネットに接続して以来、教育、研究、業務運営など、大学におけるすべての活動にキャンパス情報ネットワークが不可欠なものとなっており、前身となる組織（情報処理センター・総合情報処理センター）から継続して学術情報基盤センターが担当してきた。

本論文では、学術情報基盤センターが設計・構築を行い2015年9月に更新した鹿児島大学の第5世代のキャンパス情報ネットワーク（以下、KNIT5と呼ぶ）について、第4世代までの

キャンパス情報ネットワークにおける課題をどのように解決したのかを述べる。KNIT5では、増加するトラフィックへの対応や、情報セキュリティ対策の拡充に加えて、それ以前のキャンパス情報ネットワークではあまり考慮されてこなかった教育支援機能、特に、学生の授業外の学修支援機能の強化を目指した。

2. これまでのキャンパス情報ネットワーク

鹿児島大学は9学部10研究科からなり、約9,000名の学部学生と約1,500名の大学院生が在籍する総合大学である。約2,500名の教職員と併せて、13,000名が所属する県内最大級の事業所でもある。主要な3つのキャンパス（郡元キャンパス、桜ヶ丘キャンパス、下荒田キャンパス）のほか、十数余の学外施設を有し、常勤教職員が配置されている約100棟のすべての建

*〒890-0065 鹿児島市郡元1-21-35
1-21-35, Korimoto, Kagoshima 890-0065
E-mail: {masatom, simozono, taka, aiba, furuya, odaken, mori}@cc.kagoshima-u.ac.jp

物がキャンパス情報ネットワークに接続している。これまで、5世代にわたってキャンパス情報ネットワークの構築・更新を行ってきた。

2.1 第1世代～第2世代

鹿児島大学において全学にわたるネットワークがはじめて構築され、運用が開始されたのは1994年10月である。これは国の平成5年度補正予算によるもので、同時期に全国の国立大学においてキャンパス情報ネットワークが整備されている。その際、KNIT (Kagoshima University Network for Information and Telecommunication: ニット) の愛称が定められた。鹿児島大学における第1世代のキャンパス情報ネットワークであるため、以下KNIT1と呼ぶ。また、2年後の1996年12月からは平成7年度補正予算により整備されたATMネットワークの運用が開始された¹⁾。以下これをKNIT2と呼ぶ。

KNIT1では、鹿児島大学の主要な3つのキャンパスのそれぞれに、基幹部として光ファイバによる100 MbpsのFDDIループを、支線部として10BASE-5ケーブル(イエローケーブル)による10 Mbpsのイーサネットを採用した。支線ケーブルに接続したトランシーバからAUIケーブルが延長され、直接、または、ハブを介して端末が接続される。インターネットには学術情報ネットワーク(SINET)のノードが設置された郡元キャンパスから接続し、郡元キャンパスと桜ヶ丘キャンパス、郡元キャンパスと下荒田キャンパスはそれぞれ通信事業者の専用線によりATM 6 Mbpsで接続した。

KNIT2では、基幹部をATMスイッチで構成し、主要な建物に設置したレイヤ2スイッチを光ファイバによりATM 155 Mbpsで接続した。ATMスイッチは各部局に1台ずつ設置し、郡元キャンパス内のATMスイッチは総合情報処理センター(現学術情報基盤センター)に設置した2台のATMスイッチのいずれかと光ファイバによりATM 622 Mbpsで接続するとともに、隣り合ったATMスイッチと155 Mbpsで接続して光ケーブル障害時の迂回路を設けた。桜ヶ丘キャンパスに設置した2台のATMスイッチはATM 155 Mbpsで接続し、一方が郡元キャンパスのATMスイッチに通信事業者の専用線

によりATM 6 Mbpsで接続、下荒田キャンパスに設置した1台のATMスイッチは同じくATM 6 Mbpsで郡元キャンパスのATMスイッチに接続した。キャンパス間の回線はKNIT1のものを移行して用いた。

KNIT2の支線部は、主要な建物に設置したレイヤ2スイッチに光ファイバで接続したリピータハブ(100BASE-TX)で構成し、リピータハブの各ポートと情報コンセントの配線はカテゴリ5のUTPケーブルである。

KNIT1とKNIT2は、各キャンパスの最上位で接続してキャンパス間接続を共有し、学内に2つのキャンパス情報ネットワークが存在する形で平行した運用を行った。その後、運用終了までにキャンパス間接続はATM 135 Mbpsまで増速している。

2.2 第3世代

キャンパス情報ネットワークの最初の大規模更新を行ったのは、2001年9月である。KNIT1機器の老朽化が問題となり、国の平成12年度補正予算により費用が措置され更新が可能となった。同時期に多くの他の国立大学でもギガビット・イーサネットを用いたネットワークへの更新が行われている。このとき整備したキャンパス情報ネットワークを以下KNIT3と呼ぶ。

KNIT3は、KNIT1の更新ではあったが既設機器や既設配線は利用せず、すべて新たな機器と新たな配線で構築し、情報コンセントも2,000箇所以上に新設した。このとき新設した情報コンセントは現在も使用している。KNIT1とKNIT2の基幹部及び支線部は順次廃止することとし、2005年までにすべての情報コンセントのKNIT3への収容を完了した。このときKNIT2のリピータハブは安価なスイッチングハブに更新してKNIT3に接続した。

KNIT3の基幹部はレイヤ3スイッチで構成した。郡元キャンパスでは、総合情報処理センター(現学術情報基盤センター)に設置した2台のコアスイッチに、各部局に設置した部局スイッチをそれぞれ光ファイバにより2系統の1000BASE-LXで接続した。部局スイッチの上流との合計帯域は4 Gbpsとなる。桜ヶ丘キャンパスでは2台の部局スイッチを2系統の1000BASE-LXで接続し、下荒田キャンパスに

は部局スイッチを1台設置した。キャンパス間接続についても、ギガビット・イーサネットでの接続に変更し、1 Gbpsに増速した。

KNIT3の支線部は、光ファイバにより部局スイッチと1000BASE-SX/LXで接続した建物スイッチ(レイヤ2スイッチ)で構成し、すべての情報コンセントを100BASE-TXとした。複数の建物スイッチを設置する建物については、集線用建物スイッチを設置して光ケーブル配線の集約を図った。建物スイッチと情報コンセントの間の配線はエンハンストカテゴリ5のUTPケーブルである。また、KNIT1やKNIT2と異なり、ポート単位のVLAN設定が可能となるため、情報コンセントごとにVLAN設定を行い、トラフィックを論理的に分離した。

運用面では、プライベートIPアドレスで利用するプライベートネットワークを導入するとともに、グローバルIPアドレスを利用するネットワークとして、標準で外部からのアクセスを許可するグローバルネットワークと、標準で外部からのアクセスを禁止するセキュリティネットワークを設定した。プライベートネットワークについては、MACアドレスを登録したホストに対するIPアドレスの動的割り当てを行う全学DHCPサーバを導入した。

また、KNIT3ではセキュリティ対策の充実のため、2台で冗長構成とした高性能の全学ファイアウォールのほか、各部局用にファイアウォールを用意し、細かなポリシー制御を可能とした。また、無停電電源装置のランニングコスト削減を図るため、バッテリー寿命が13年のものを導入した。

その後、2009年8月まで運用したKNIT3では、認証アプライアンスによるWeb認証の仕組みを導入し、認証付き情報コンセント及び認証付き無線LANの運用を開始した。これをオープンネットと呼んでいる。認証付き無線LANは認証付き情報コンセントに無線LANブリッジを接続することで実現できる。使用する無線LANブリッジは1台数万円程度の安価な装置を用いることにし、学術情報基盤センターの経費や部局の経費などで少しずつ毎年設置台数を増やした。また、メールアドレスによる簡易認証を用いてアクセスの許可を行うFREESPOT²⁾について、2007年より導入し、こちらも毎年設置台数を増やした。

補正予算により導入されたKNIT3では、KNIT1やKNIT2と同様、維持経費の確保と更新経費の確保が問題となった。維持経費については、毎年のように学長裁量経費等の学内予算の獲得のための働きかけを行うとともに、保守経費の削減のため、保守業務委託の入札を行った。これにより、納入業者と異なる業者が保守を行うことになったが、ネットワーク構成等を熟知しているKNIT2の納入・保守業者が落札し、ハードウェアメーカの協力を得て業務に当たったため、大きな混乱は生じなかった。更新経費については、概算要求による獲得を目指したが見通しが立たない状況が続き、その間にも機器の老朽化が進んで故障時に修理が不能となる可能性が拡大した。

2.3 第4世代

更新経費の確保の問題を解決するため、毎年の保守経費を經常経費化し、6年間(72ヶ月)の賃貸借により新しいキャンパス情報ネットワークへの更新を行うことにして、「高度情報通信基盤システム」の名称で調達を行った。それが、2009年9月より運用を開始した第4世代のキャンパス情報ネットワークシステムである³⁾。以下、KNIT4と呼ぶ。

KNIT4の調達に際しては、それまでの保守経費の範囲で行うことになるため機器コストを削減しなければならない。このため、各部局に設置していた部局スイッチを廃し、コアスイッチと建物スイッチを直接接続することにした。ただし、それには新たな光ファイバ配線が必要となる。そこで、3つのキャンパスのコアスイッチを設置する場所から各建物の建物スイッチ設置場所まで、それぞれ8芯のシングルモード光ファイバを目的積立金により整備した。

利用者から見ると、KNIT3とKNIT4で違いはなく、プライベートネットワーク、グローバルネットワーク、セキュリティネットワークの運用に大きな変更はない。一方、オープンネットについては、2013年6月にL2TP/IPsec VPN装置を導入してWeb認証を迂回する設定を追加し、VPNを設定済みの機器から利用について毎回のWebブラウザの起動を省略可能とした。

KNIT3の運用中にトラフィックは増加しつつあったが、十分な費用を確保することができ

ず、KNIT4では帯域を増やすことができなかった。情報コンセントと建物スイッチの間の配線はKNIT3で敷設したUTPケーブルをそのまま使用し、情報コンセントは100BASE-TXである。ただし、コアスイッチ接続用の2ポートの1000BASE-LXポートに加えて2ポートの1000BASE-Tポートを有する建物スイッチを導入した。これにより、建物スイッチあたり2つだけではあるが、ギガビット・イーサネットに対応した情報コンセントを可能とし、サーバなど大容量の通信を行う機器の収容に対応した。

KNIT4の基幹部は、新たな光ファイバ配線を用いることで、KNIT1～KNIT3とは大きく異なる単純なスター型構成とした。2台のコアスイッチからそれぞれ建物スイッチを1000BASE-LXで接続して冗長化を図った。中間にスイッチが入らないことで、セキュリティインシデント発生時のMACアドレス取得が容易になったが、ループ発生によるブロードキャストストームの被害の影響範囲が大きくなった。これについては、建物スイッチのループ対策機能で対応した。

KNIT4では、セキュリティ対策で大きな変更があった。アプリケーション制御機能を有するファイアウォールの導入である。IPアドレスやTCP/UDPポートを指定した通常の制御に加えて、ネットワークアプリケーションを認識して制御できる装置である。この装置により、第三者の著作権を侵害する可能性が大きいP2Pソフトによる通信を遮断した。また、Web認証について、ファイアウォールの機能を用いて実現することにし、専用装置にかかる費用を削減した。オープンネット用の無線LANブリッジについては使用を継続した。

なお、KNIT1～KNIT3では買取による調達であるため機器の所有権が大学にある。このため、保守が必要な場合は別途契約が必要になるが、更新後も機器を継続して使用することができた。一方、賃貸借で調達したKNIT4では大学に所有権が無いため、賃貸借期間終了後は機器を返却することになる。しかし、建物スイッチなど別用途で継続使用できる場合があるため、KNIT4では賃貸借期間終了後の譲渡を仕様書に明記し、期間終了後に全機器の所有権を取得した。残置されることになる機器については、既設機器の撤去及び指定する機器の廃棄を次回調達の要件として加えることにした。

3. 第4世代の課題

更新経費と維持経費の問題を解消し、KNIT3の更新を果たしたKNIT4ではあったが、次のような課題が顕在化、または、生じるようになった。

3.1 トラフィック増に対応できていない

学外接続部について、2011年度に10ギガビット・イーサネットに対応した装置を追加導入して、SINET4ノード機器への接続を1Gbps(1000BASE-T)から10Gbps(10GBASE-LX)に変更した。SINET4内の上流回線の帯域は2.4Gbpsであるため、利用できる帯域が10倍になったわけではないが、上流回線の帯域を十分に活用できる体制となっていた。ところが、2016年4月から運用が開始されるSINET5では、上流回線の帯域が100Gbpsとなり、100ギガビット・イーサネットでの接続も可能となる。10Gbpsでの接続ではその広帯域を十分に活用できない。

キャンパス間接続について、WDM装置の導入により、光ファイバ1芯で複数のギガビット・イーサネットによる接続を実現し、郡元キャンパスと桜ヶ丘キャンパスの間を合計8Gbps、郡元キャンパスと下荒田キャンパスの間を合計4Gbpsとした。KNIT3に比べれば4～8倍となったが、トラフィックが必ずしも均等に配分されるとは限らないリンクアグリゲーションによる接続であるため、帯域を十分に使用できない。

情報コンセントについて、利用者側機器のギガビット・イーサネット対応が一般的になっているにも関わらず、100Mbpsでしか接続できない100BASE-TXであった。プライベートクラウドの運用⁴⁾を行い学内のサーバを集約しつつある中で、利用者のPCとの間の大量のデータ転送が遅い問題が顕在化しつつあった。建物スイッチあたり2ポートの1000BASE-Tポートが用意されてはいるが、その使用には配線変更を伴う。また、数に限りがあるため希望箇所すべてで利用できるわけではなく、積極的な周知を行うことができていなかった。

3.2 情報セキュリティ対策が十分とは言えない

情報セキュリティに関しては、可用性に問題のある状態が KNIT1 の時代から 20 年以上にわたり継続し、解決できずにいた。インターネットへの接続部が郡元キャンパスであるため、その法定点検のための計画停電の影響を桜ヶ丘キャンパスと下荒田キャンパスが受けるのである。同時に停電となる郡元キャンパスでは問題とはならないが、停電ではない桜ヶ丘キャンパスと下荒田キャンパスでインターネットが 1 日使えない状態になる。1 年に 1 日とは言え、その影響は大きく、ネットワークが欠かせないものとなるにつれ、その改善の要求は増大してきていた。

また、KNIT4 では、機密性確保に重要な役割を果たすファイアウォールの運用性及び保守性の低下が問題となった。

KNIT3 から KNIT4 の移行に際し、KNIT3 の全学ファイアウォールと部局ファイアウォールのポリシーを KNIT4 の全学ファイアウォールに移行した。ところが、レビューを十分に行わなかった結果、多数の重複するポリシーが存在する長大なアクセスリストを運用することになった。各部局からのファイアウォールポリシー変更の申請をそのまま受け入れていた運用にも問題があった。不要になったポリシーの削除を申請してくる部局は皆無であり、意味のない TCP/UDP ポートの許可・遮断やポリシーの重複は減るどころか増加する一方であった。各部局ではどのような申請をしたかの記録も記憶も有しておらず、問い合わせに応じようにも長大なアクセスリストから該当部分を拾い上げるのに困難を極めた。また、ファイアウォールの管理機能の性能が低く、アクセスリストを 1 行変更して適用するのに 5 分以上の時間を要し、緊急対応が必要な場合などに支障が生じていた。

3.3 学生がキャンパス情報ネットワークを十分に利用できない

学生には完全な社会的責任能力があるとは言えず、不法行為等が行われた場合には大学側にも監督責任が生じる。このため、KNIT2 までは

ゼミや研究室に配属され指導教員による監督が可能な場合を除き、学生にはキャンパス情報ネットワークを使用させていなかった。

その後、教員が授業を行う教室の中でノート PC 等によりインターネット接続を行う場合を想定し、事前のホスト登録が不要な認証付き情報コンセントと、認証付き情報コンセントに無線 LAN アクセスポイントを接続することで実現した認証付き無線 LAN の運用であるオープンネットを KNIT3 より開始した。オープンネットは学術情報基盤センターが教職員と学生に対して発行している ID とパスワードで利用できる。接続時の ID は記録され利用者の特定が可能であることから、教職員、学生の別なく利用を可能とし、学生の自習目的での利用を許容した。インシデント発生時には学術情報基盤センターが ID から使用者を特定し、各部局に連絡する形で対応を行うこととした。これにより、KNIT4 の頃には、オープンネットは、多くの学生にとってキャンパス情報ネットワークを利用できる唯一の方法として広く認知されるに至っていた。

しかし、キャンパス情報ネットワークとして調達した機器で運用していたのは、認証付き情報コンセントまでである。認証付き無線 LAN は学術情報基盤センターのほか各部局において、臨時的経費により安価な無線 LAN ブリッジを導入して認証付き情報コンセントに接続することで実現しており、学術情報基盤センター及び各部局の教職員による運用であった。このため、以下のような問題があった。

- 集中管理機能が貧弱で動作状態の確認も十分にできない。
- 同時遠隔設定に対応しておらず設定変更が難しい。
- 複数の機器が協調して動作する機能がなく、場合によっては干渉による帯域低下が発生する。
- 保守契約が無い場合障害対応及び修理費用は各部局の負担となる。
- 利用できる教室と利用できない教室がある。

表 1 最大帯域（単位：Mbps）の変遷。20年間で基幹部は400倍、情報コンセントは100倍、キャンパス間は13,000倍以上になった。

世代 期間	KNIT1 1994–2001	KNIT2 1996–2001	KNIT3 2001–2009	KNIT4 2009–2015	KNIT5 2015–2021
基幹部（バックボーン）	100	622	4,000	8,000	40,000
基幹部（コア-エッジ間）	100	100	2,000	2,000	10,000
支線部（情報コンセント）	10	100	100	100*	1,000
キャンパス間（郡元-桜ヶ丘）	6	135	1,000	8,000	80,000
無線 LAN			300	300	1,300

* 建物スイッチ1台あたり2ポートのみ1,000 Mbps対応可能。

また、最初の導入から時間が経過し、故障頻度が増えつつある一方で、無線LANを搭載したノートPC、スマートフォン、タブレット等を学内で使用する学生が増加していた。最近では、授業時間外の学修の支援を目的として多くの大学で無線LANの整備が進められている。本学においても学修支援機能を強化するため、上述の問題点を解決し、全学的な無線LANを整備することが喫緊の課題であった。

一方、主に学外者による利用を想定し、民間回線を経由してインターネットに接続するFREESPOT機器も多く設置していた。こちらも臨時的経費により整備したもので、学術情報基盤センター教職員による設置・運用である。オープンネット無線LANと近接して設置した箇所もあり、限られた無線LANチャンネルの有効利用の観点から適切とは言えない運用となっていた。全学的な無線LANの整備に当たっては、FREESPOTの機能も集約する必要があった。

4. 第5世代での課題の解決

キャンパス情報ネットワークに空白期間は許されない。KNIT4の賃貸借期間の終了に伴って調達することになるKNIT5では、KNIT4で表面化した上述のような様々な課題を解決しなければならない。ところが費用は、経常経費化していることもあり、最大でもKNIT4と同額である。経常的経費の上積みは極めて困難であることから、諸々の課題を限られた費用の中で解決することになった。

ちなみに、上述の課題の解決等を行わず、同等の性能、機能の製品により単純に機器のみを

更新した場合の費用をKNIT4構築業者に算出させたところ、KNIT4とほぼ同額であった。しかも、これには、臨時的経費で導入を進めた無線LANブリッジの更新費用は含まれない。困難な状況であったが、われわれはKNIT4における3つの課題について、それぞれ以下のように対応しKNIT5を構築した。

4.1 トラフィック増への対応

増加するトラフィックへの対応として、全情報コンセントの1000BASE-T対応を行うことにした。KNIT4に比べて10倍となる。表1に基幹部、支線部、キャンパス間、無線LANそれぞれについて最大帯域の変遷を示す。

情報コンセント接続ポートの強化により建物スイッチの機器コストが上昇することになるため、キャンパスコアとの冗長接続を廃することで、建物スイッチの上流接続に必要なモジュールにかかるコストと、2台のキャンパスコアにかかるコストを半減した。可用性が低下する可能性があるが、KNIT4においては障害発生に起因して建物スイッチの冗長接続が機能した例はなく、運用期間中に数回あった基幹部のメンテナンス時にのみわずかにその機能が活用できたに過ぎない。また、キャンパスコアを複数台のボックス型スイッチで構成し、いくつかの建物毎に物理的に異なるキャンパスコア構成機器と接続することで、障害発生時の影響範囲を限定させることにした。キャンパスコアを複数のボックス型スイッチで構成することによりシャーシ型に比べてコストを低減した。

学外接続はSINET5の運用開始を見越して40ギガビット・イーサネットに対応した。当初

は100ギガビット・イーサネットも検討したが、コスト的に現実的ではなく、用意できる費用の範囲内で可能な最大帯域となる40ギガビット・イーサネットを採用した。2015年9月から2016年2月までは10GBASE-LXでのSINET4への接続を継続し、2016年3月より40GBASE-LRでSINET5に接続する。将来の40GBASE-LR×2ポートでの接続にも対応し、SINETとの最終的な合計接続帯域は80 Gbpsを予定している。接続帯域でSINET4の8倍、上流回線の帯域が2.4 Gbpsから100 Gbpsに増速されるとすれば、2.4 Gbpsが80 Gbpsとなるため33.3倍の帯域となる。

さらに、キャンパス間の接続も増速した。郡元キャンパスと桜ヶ丘キャンパスの間はWDM装置により合計80 Gbps（40 Gbps×2）、郡元キャンパスと下荒田キャンパスの間はWDM装置により合計40 Gbps（10 Gbps×4）とした。いずれもKNIT4に比べて10倍である。

4.2 情報セキュリティ対策の強化

郡元キャンパス停電時の全学的な可用性の向上と、KNIT4で問題となったファイアウォールの運用性及び保守性の低下の問題について、KNIT5では以下の通り対応した。

4.2.1 郡元キャンパス停電の影響回避

長年の懸案事項であった郡元キャンパスの停電の影響が桜ヶ丘キャンパスと下荒田キャンパスに及ばないようにする対策をKNIT5で初めて導入した（図1）。

基幹システムのコアスイッチに各キャンパスの建物スイッチを集約するキャンパスコアを接続する構成とし、その上で基幹システムの無停電化を行う。これにより、郡元キャンパスの停電の影響を回避した。基幹システムは郡元キャンパスに置かれるが、郡元キャンパスのキャンパスコアシステムとはラック及び電源ともに分離し、基幹システムには停電時に外部から発動発電機等により電源供給を行う。全学ファイアウォールをはじめ、DHCPサーバやDNSサーバ等のキャンパス情報ネットワークの利用に必要な機器についても基幹システム内に設置し、停電時の電源供給を行うことにした。

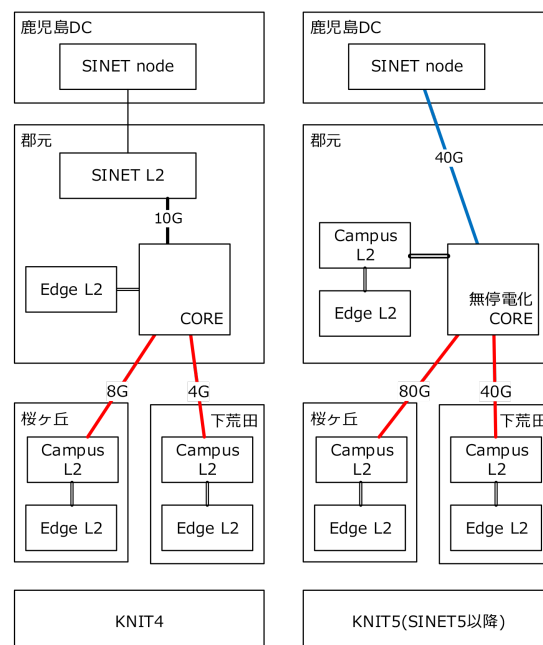


図1 主要ネットワーク機器の配置図。左はKNIT4、右はKNIT5。KNIT4では郡元キャンパスに設置された基幹システムのコアスイッチが郡元キャンパスの集線スイッチの役割も果たしていた。KNIT5では、基幹システムのコアスイッチと郡元キャンパスの集線スイッチの役割を果たす郡元キャンパスコアを分離し、基幹システムを無停電化した。

なお、基幹システムは1ラックで構成されており、SINET及び各キャンパスとの通信回線と設置場所が確保できれば設置場所は任意である。コストの点から導入時の開始は断念したが、データセンターや他大学など学外に置くことも可能である。原子力発電所からおおよそ45 km、活発に活動している活火山からおおよそ10 kmの位置にあり、豪雨や台風の被害も受けやすい鹿児島大学よりも、災害の発生可能性が低い場所に設置することでBCP対策とすることもできる。

4.2.2 ファイアウォールポリシーの整理

複雑かつ長大になったファイアウォールのポリシーについて、まずは単純化することにし、図2を原則としてポリシーの見直しを行った。

KNIT4では、インターフェースやVLANを単位として1台のファイアウォール装置でポ

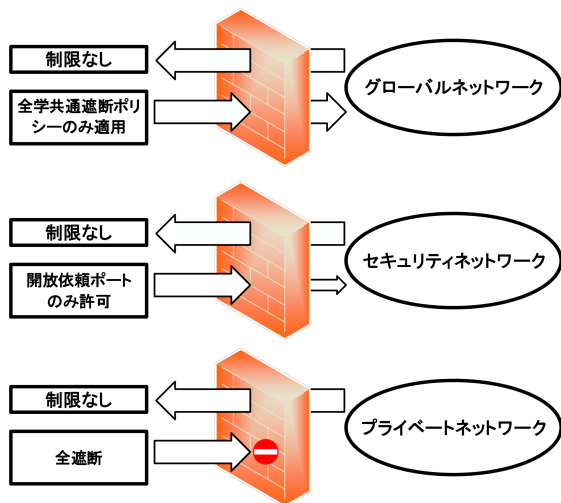


図 2 KNIT5 ファイアウォールポリシーの原則。内部→外部には制限を設けず，外部→内部については各ネットワークの運用形態に応じたポリシーを設定する。

ポリシーを制御しており，ポリシーがインターフェースや VLAN の数だけ存在した。このため類似のポリシーであっても独立して扱う必要がある。ポリシーの設定や把握に時間がかかるという問題があった。類似のポリシーを持つインターフェースや VLAN を，複数のファイアウォール装置によりグループ化して扱うことができれば，ネットワーク構成やポリシーの把握が容易になる。そこで KNIT5 では，内部に複数の仮想ファイアウォールの機能を持つことができる装置を導入してその機能を活用し，ネットワーク構成やポリシーを把握しやすくした。

すべてのポリシーは，保護の対象となるネットワークと外部との境界部で設定し，内部と外部との間の通信のみが制御の対象となる。これまでのポリシー設定では，例えば，WAN1・WAN2・DMZ1・DMZ2・LAN1・LAN2 の 6 つ

のインターフェースがある場合，それぞれのインターフェースの組み合わせ毎にポリシーを設定していた。この例の場合は 15 組のポリシー設定が必要となる。これをそれぞれ内外のみのポリシー設定とすれば設定の組は 6 組でよい。

このように設定をわかりやすくすることで，ミスを減らすとともに，保守業者や次期システムの構築を担当する業者によるネットワーク構成の把握を容易にした。ポリシー見直しの結果，KNIT4 におけるファイアウォールポリシーが 911 行であったのに対し，KNIT5 では 882 行に削減できた。全体としては削減数は多くないが，仮想ファイアウォールを 9 台用いることで類似のポリシーをまとめることができ，1 台あたりのポリシーは最大 327 行に抑えることができた。

4.3 全学無線 LAN の整備による教育支援機能の強化

KNIT3～KNIT4 にかけて臨時的経費により順次設置を進めたオープンネット用の無線 LAN ブリッジと FREESPOT 用の無線 LAN アクセスポイントをすべて撤去・更新し，さらに，未整備であった学内の全教室に無線 LAN を整備した。台数は 350 台になる。すべての教室で利用できるようにすることで，授業はもちろんのこと，学生の授業時間外の学修支援機能の強化を図った。

装置としては VLAN と対応したマルチ SSID 機能と集中管理に対応した無線 LAN アクセスポイントを使用し，1 台の無線 LAN アクセスポイントから表 2 に示すサービスを提供することにした。

表 2 無線 LAN アクセスポイントから提供されるサービス

サービス	SSID	Passphrase	対象
ゲストネット	KNIT5-GUEST	なし	一般
オープンネット	KNIT5-OPEN	学内限定公開	在籍者 (Web 認証・VPN 認証)
スタッフネット	KNIT5-STAFF	教職員のみ公開	登録済ホスト (教職員限定)
Wi ² 300	Wi2/Wi2_club	契約者に公開	契約者 (au Wi-Fi 加入者含む)
ソフトバンク Wi-Fi	0001softbank ほか	契約者に公開	契約者
部局 Wi-Fi	部局ごと	部局ごと	部局内のみ

4.3.1 ゲストネット

従来提供していた FREESPOT については、機器を廃止するため同様の仕組みは使用できない。このため、空港などで行われているサービスを参考に、鹿児島大学独自の公衆無線 LAN サービスであるゲストネットを開始することにした。接続機器の MAC アドレスを保存することで各種インシデントに備えている。インターネット接続回線としては SINET ではなく、民間 ISP の回線を用い、キャンパス情報ネットワーク内は独立した VLAN を設定した。

4.3.2 オープンネット

オープンネットは従来提供しているものと同様のサービスを継続した。学術情報基盤センターが教職員と学生に発行している ID により、Web 認証および VPN 認証を行うことで利用できる。Web 認証はファイアウォールの Captive Portal 機能で、VPN 認証は新規に導入した L2TP/IPsec VPN 装置により実現した。

4.3.3 スタッフネット

授業支援機能の強化として、登録したホストであれば ID による認証なしにすべての教室で接続ができるスタッフネットを新たに設けた。各部局でプライベートネットワークへの接続を承認されたホストを学術情報基盤センターが追承認することとし、部局でのホスト登録により学内の無線 LAN が利用できるすべての教室での接続を可能とした。

4.3.4 公衆無線 LAN サービス

複数の SSID と VLAN を設定できる新無線 LAN システムの機能を活用し、KNIT5 では民間の通信事業者により提供されている公衆無線 LAN サービスも提供することにした。ワイヤードワイヤレス社の Wi² 300 と、ソフトバンク社のソフトバンク Wi-Fi である。前者は au Wi-Fi 契約者が標準で利用できる公衆無線 LAN であり、携帯電話主要キャリアのうち 2 社いずれかの公衆無線 LAN サービス契約者であれば、学内のすべての教室において無線 LAN

を利用できることになる。事業者のネットワークとはキャンパス情報ネットワークの最上流で接続し、キャンパス情報ネットワークとは独立した VLAN を設定することで通信を分離した。

4.3.5 部局 Wi-Fi

以上のサービスに加えて、部局独自の運用を行う部局 Wi-Fi も複数設定している。これは、部局内に設置されている無線 LAN アクセスポイントに限定して、部局独自の SSID、パスワードにより、部局独自の VLAN に接続できるようにしたものである。学術情報基盤センターのほか、教育学部附属学校などで運用している。

4.3.6 無線 LAN の利用状況

運用開始以来、これまでの最大接続台数は 2016 年 2 月 1 日の 1,510 台である。曜日や時間帯による変動はあるが、ピーク時の台数は増え続けており、今後もますます増加することが想定される。

サービス毎の接続数では、全接続機器のおよそ半数がオープンネット、およそ 4 分の 1 がゲストネットに接続しており、部局 Wi-Fi や公衆無線 LAN への接続数がそれに続く。一方、利便性が高いはずのスタッフネットの接続数は多くない。これは、サービスがまだ認知されていないためと考えられる。

無線 LAN アクセスポイントあたりの接続機器数は、設置場所によって異なる。ピーク時接続機器数が最も多いのは、桜ヶ丘キャンパスの講義室に設置した機器で 107 台、次いで法文学部講義室の 100 台である。いずれの講義室も収容人員が多い。3 番目に多いのは郡元キャンパスの生協中央食堂に設置した機器で、最大 97 台が接続している。これらのほか、ピーク時に 50 台を超える機器が接続している無線 LAN アクセスポイントは 20 台ある。これら接続機器数上位の無線 LAN アクセスポイントは、そのほとんどが収容人員が多い講義室に設置されている。これらの場所では、日常的に接続機器数が多いが、利用者から不具合の申告はなく、支障なく利用できていると考えている。

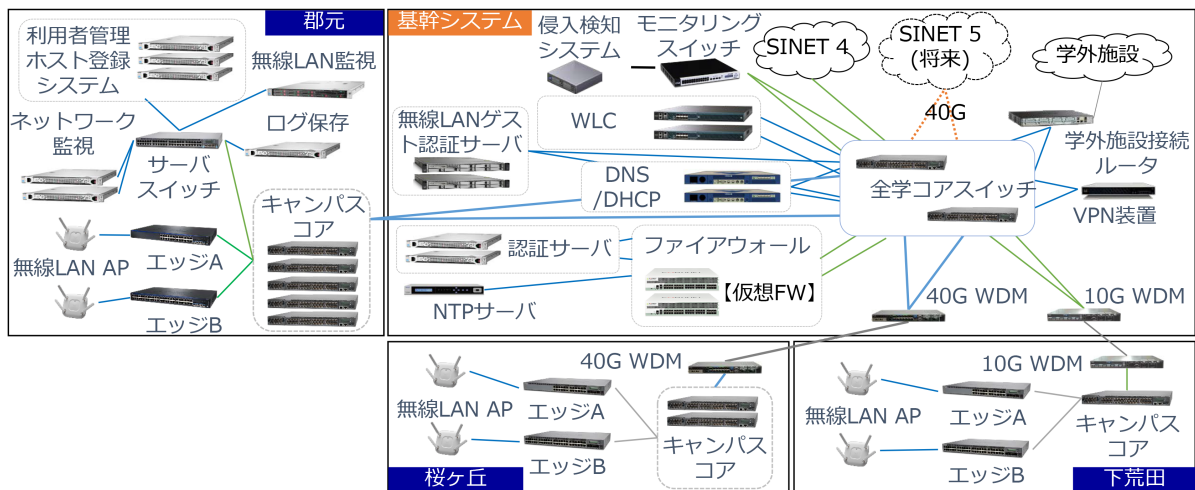


図3 KNIT5 機器構成図.

5. まとめ

2015年9月からの運用を開始したKNIT5(図3)では、KNIT4で課題となった問題の解決に限られた費用の中で果たすことができた。特に、無線LANアクセスポイントの全教室への整備と新たなサービスの提供開始により、教員の授業支援機能及び学生の授業外の学修支援機能を充実させることができ、教育支援機能の強化を果たすことができたと考えている。しかしながら、無線LANアクセスポイントのさらなる増設、標的型攻撃への対応など、すでに見えつつある新たな課題もある。

費用は削減される一方であるにもかかわらず、新たな要求は増加する一方である。すべてのニーズを満たすことは不可能であるため、優先順位を設定し、メリハリを付けたキャンパス情報ネットワークの構築が今後必要になるものと思う。この時、何を優先するべきかについて利用者と十分に協議及び調整の必要があるが、合意に至るにはかなりの困難が想定される。

幸いにして今はまだそこまで深刻な事態には陥っていない。われわれは、セキュリティと利便性を共に高くし、大学のすべての構成員が快適にキャンパス情報ネットワークを利用できるよう今後も尽力したいと考えている。

参考文献

- (1) 二宮公紀, 高橋至, 伊尻ひろ子: 鹿児島大学 ATM ネットワークの構築と導入さ

れた新技術, 大学情報システム環境研究, Vol. 1, pp. 51-65 (1998) .

- (2) FREESPOT 協議会: FREESPOT・公衆無線LANサービス, <http://www.freepot.com> (参照 2016-02-12) .
- (3) 山之上卓: 鹿児島大学のキャンパスネットワークの特徴, 鹿児島大学学術情報基盤センター「年報」, No. 5, pp. 40-43 (2009) .
- (4) 下園幸一, 高橋至, 升屋正人: 仮想化技術を用いたホスティング・ハウジングサービスの集約, 学術情報処理研究, No. 14, pp. 77-88 (2010) .

著者略歴



升屋 正人 1991年東京大学理学部卒業, 1996年同大学院農学生命科学研究科博士課程修了, 同年4月岡崎国立共同研究機構分子科学研究所非常勤研究員, 1997年11月鹿児島大学工学部情報工学科助手, 2000年4月同大学総合情報処理センター助教授, 2003年4月同大学学術情報基盤センター助教授, 2006年11月同教授. 博士(農学) .

(著者多数のため以降略)