KAINS のこれまでとこれから

総合メディア基盤センター　大野　浩之
井町　智彦
北口　善明

1 はじめに

金沢大学の情報通信ネットワークは，「金沢大学学術統合ネットワークシステム（KAINS：Kanazawa University Academic Integrated Network System）」と称され，総合メディア基盤センター（以下，本センター）において，設計・構築・運用が行われています．KAINS は，2016 年度に大規模なシステム更新を予定しています．本稿では，それに先立ち KAINS の現状と，今後の展望について述べたいと思います．

2 KAINS の現在

2.1 KAINS11

現在の KAINS は，「KAINS11」と称します．2011 年に抜本的な再整備を行いましたので，この呼称が付いています．

KAINS11 の整備における最大の特徴は，基幹ネットワークを含むネットワークの重要部分をリース化したことです．KAINS11 より前に使用していた機器は，2001 ～ 2003 年度に行われた整備当時のもので，その末期には老朽化による故障などが多発していました．それまでのネットワーク機器は全て買取りでしたので，故障の度に費用確保・調達等の手続きが発生し，対応が迅速にできないことも多々ありました．現在は，そういった障害対応も，リース化を実現した部分に限られますが，作業・費用ともに契約内で賄うことができますので，学内における業務に支障をきたすことも非常に少なくなっています．

KAINS11 の整備に際して，SINET4 経由のインターネット接続を 10Gbps に増速し，キャンパス間通信も 10 ～ 20Gbps と広帯域な回線とすることで，キャンパス内全域のバックボーンが 10Gbps 以上となりました．また，利用者のパソコン等をつなぐ支線ネットワークにおいても，ほぼ全てを 1Gbps 接続が可能な環境としており，ネットワーク環境の拡充を図っています．

2.2 シンプルなネットワーク構造

KAINS11 は，本センター，自然科学 1 号館および附属病院東病棟の 3 拠点においた Layer-3 スイッチ（以下，L3SW）を起点とする，シンプルなスター型構成となっています（図 1）．L3SW とは，IP アドレスによって通信先のネットワークを選択する通信機器で，いわゆるルータに相当するものです．本センターに配置された L3SW が角間中地区と角間北地区を担当し，自然科学 1 号館に配置されたものが角間南地区，附属病院東病棟に配置されたものが宝町・鶴間地区をそれぞれ担当します．

かつては L3SW が全学の主要建屋毎に配置されていました．これは部局ネットワークを相互接続するネットワーク構成であったことが一因で，部局および建屋毎にネットワークが構築されていました．しかしながら，KAINS11 では，本センターによって部局整備部分を含む全学でのネットワーク整備を進める方針としたことで，このようにシンプルな形でネットワーク構成を実現することができました．L3SW は構造・設定が複雑であり，また高価でもありますので，運用・管理および維持の観点からも現在の形態の方がより望ましいといえます．また，これら 3 台の L3SW は仮想的に連結されており（仮想シャーシ機能），運用者からみるとあたかも 1 台の巨大な L3SW のように見えますので，そのことも確実な運用に貢献しています．

2.3 タグ VLAN を用いた柔軟な運用

前述した L3SW の配下には，多数のネットワークが接続されています．無線 LAN のように IP アドレスを自動割り

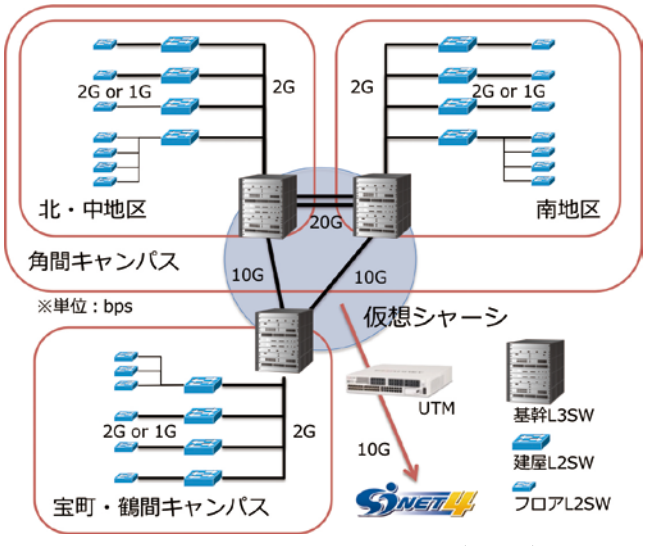

図 1　KAINS11 のネットワーク構成（主要部）

当てするネットワークと，研究室等で使用している固定 IP アドレスのネットワークは別のネットワークですし，各部局等に割り当てているサブネットワーク群もそれぞれが別のネットワークです．原理的には，L3SW からはネットワーク毎に LAN ケーブルを配線しなければならないのですが，実際に配線されているのはそれより遥かに少ない本数です．これは，複数のネットワークの通信を重畳して送受信しているためで，この技術をタグ VLAN（Virtual LAN）と呼びます．タグ VLAN では，各ネットワークの通信にタグと呼ばれる番号を付け，そのタグを元に L3SW およびそこに接続された Layer-2 スイッチ（以下，L2SW）で通信を重畳したり分離したりしています．

KAINS11 では，基幹系でのほぼすべての通信に，このタグ VLAN を用いています．タグ VLAN 自体はごく一般的な技術であり，従来の KAINS でも多用されてきましたが，KAINS11 ではそれを一層積極的に用いることで少ない機材や配線で多様な通信を可能にしています．また，部局内のフロア L2SW までを包括管理することにより，VLAN 設定も全学的に柔軟に追加・削除が可能になっています．

現時点では，研究室間を結ぶ専用の配線やサブネットが異なるために配線されたものなどが残っている建屋がいくつか存在しています．複数の回線が存在する環境は利用面においては柔軟性がなく，運用面においては煩雑故の運用ミスの可能性が高いため，VLAN を用いたネットワーク構成に段階的な移行を実施しています．

2.4　セキュリティ制御機器の統合

KAINS11 以前のネットワークでは，外部のウェブサーバとの通信にプロキシサーバを経由する構成となっており，プロキシサーバにてダウンロードファイルのコンピュータウィルスチェックを実施していました．上記以外の通信に関しては，外部からの通信を必要な機器のみに制限してセキュリティを確保する必要があり，別途ファイアウォール機器を導入していました．このファイアウォール機器は，全学用と合わせて部局用のものも存在しており，対外接続のためのセキュリティ機器が複数存在する環境でした．複数の機器による運用では，コストの面と運用の面で不利な点があり，KAINS11 では統合脅威管理（UTM）の導入により改善を図りました．

UTM（Unified Threat Management）は，複数の異なるセキュリティ機能を一つの機器（ハードウェア）に統合するもので，統合的なセキュリティ制御が可能になります．インターネットからの脅威に対する対策として代表的な対策には以下のものがあります．

- ✧　ファイアウォール機能
- ✧　侵入検知／侵入防止
- ✧　コンピュータウィルスチェック
- ✧　迷惑メール処理

KAINS11 で導入した UTM では，迷惑メール処理以外の機能をまとめて処理しています．迷惑メール処理に関しては処理負荷が比較的大きいことから別システムでの対処としています（図 2）．また，仮想的にセキュリティ機能を複数設定可能であるため，複数のファイアウォール機器の統合が実現できました．セキュリティポリシーの異なるネットワークに対して，それぞれセキュリティ制御機能を提供しています．

さらに，ファイアウォール機能においても，アプリケーション毎での制御機能を利用し，P2P ファイル共有サービスなどを制限することを実現しています．これまでのファイアウォール機器では，IP アドレスとポート番号（メールサービスやウェブサービスなどを識別するために TCP や UDP で利用される番号）の組み合わせでの制御が基本でした．KAINS11 で導入した UTM では，通信の振る舞いから利用しているアプリケーションを特定することができ，同じウェブサービスの通信であっても制御を変更することが可能です．学術ネットワークとして不要と判断できるサービスに関しては，この機能を用いて制御しています．

2.5　無線ネットワークの全学展開

KAINS における無線ネットワークの整備は，学生のパソコン必携化に合わせて，情報教育教室を中心に順次整備を進めてきました．当時の無線ネットワークのアクセスポイント（AP）は，家庭用に利用されているものとそれほど機能的に優れたものではなく，個々に設定投入が必要な機器がほとんどでした．そのため，昨今の無線ネットワークの需要に応じて，利用エリアの拡大を進めるには，運用面において難しい点がありました．

そこで，KAINS11 では，統合的な無線 AP の管理を実現するべく，全学規模の集中制御型無線ネットワークシステムを導入しました．2011 年度の初期導入では，角間キャンパス南地区のみが対象でしたが，集中制御による拡張性を生かし，徐々に他の地区における整備を進めることがで

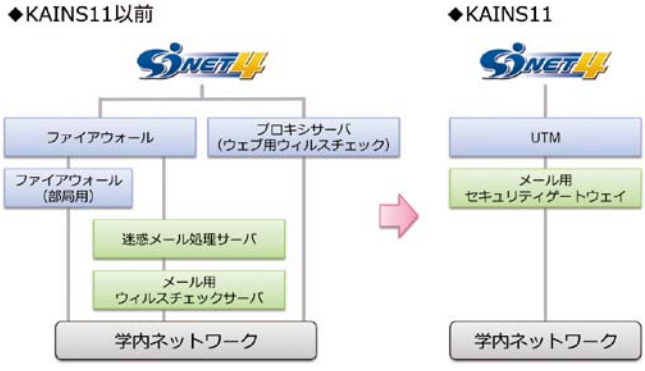

図 2　セキュリティ制御機器の統合

きました．2014 年度末時点において，ほぼ全てのキャンパス内建屋にて無線ネットワークが利用可能となっています．現在，提供している主な無線ネットワークサービスを表1に示します．

表1　本学の主な無線ネットワークサービス

SSID	仕　様
KAINS-WiFi	802.1x 認証，キャパス全域でローミング
eduroam	802.1x 認証，eduroam ID により参加組織での相互利用が可能
meetingroom	ペーパレス会議用
キャリア Wi-Fi	各携帯キャリアにより接続方法が異なる

KAINS-WiFi は，以前に提供していた全学用の無線ネットワークである lounge の後継サービスとして，2011 年度より提供を開始しました．lounge では，無線ネットワークへの接続後，インターネット利用に際してウェブ認証を必要としていましたが，新しい KAINS-WiFi では無線接続時の 802.11x 認証のみでインターネット接続を許可する仕様に変更しました．また，部局や地区毎にネットワーク設定を区切っていたものも一本化し，地区の移動によるネットワークサービスの再接続が発生しない構成になっています．

eduroam[1]は，国際無線 LAN ローミング基盤として広く国内外で利用されている無線ネットワークサービスで，利用する ID（eduroam ID）を持っていれば，国内外の参加組織において利用できます．本学では，この eduroam を外来者・来訪者向けの無線ネットワークサービスとしても活用し，2012 年度より提供しています．eduroam ID は，金沢大学 ID による認証にて簡単に取得することが可能で，利用期間は最大1年間となります．また，学内への来訪者に対して複数の eduroam ID が必要な場合などのために，本センターでは代理アカウント登録サービスを提供しています．学内で開催される学会等への参加者に対して，無線ネットワークを提供する必要がある場合にご利用ください．

キャリア Wi-Fi は，携帯電話事業者により提供される WiFi サービスで，2014 年度から本学の無線ネットワークを利用し，学内の一部（食堂など利用者が多く集まるエリア）にて提供を開始しています．これは携帯通信事業者側から学内に無線 AP の設置要望があり，無線 LAN における電波資源の競合を回避するための処置として実施しているものです．現在はソフトバンクモバイル株式会社による提供のみですが，今後，他の通信事業者による Wi-Fi サービスの提供も検討しています．

2.6　KAINS11 におけるネットワーク区分

KAINS11 では，提供するネットワークを利用するポリシー毎に区分けして定義しています．以下に，そのネットワーク定義をお伝えします．

◆ KAINS-B（KAINS Base network）

一般的な学内ネットワークで，グローバル IP アドレス（133.28.xxx.xxx）を使用します，すべての基盤となるネットワークになります．

◆ KAINS-D（KAINS DMS segment）

DMZ と呼ばれる公開サーバ等を配置するセグメントです．外部からアクセス可能なサーバ等を配置するため，KAINS-D から学内およびインターネットへの通信は厳しく制御されています．また，学内のみにサービスを公開するサーバ等に関しては，学外用とは区別して用意しています．

◆ KAINS-S（KAINS Socket）

居室やオープンスペースに設置されている情報コンセントによる有線ネットワークです．プライベート IP アドレスが自動設定され，利用に際してはネットワーク ID によるユーザ認証（web 認証）が必要になります．

◆ KAINS-W（KAINS Wi-Fi network）

SSID が KAINS-WiFi で提供される無線ネットワークです．接続時にネットワーク ID によるユーザ認証（802.1x 認証）が必要で，グローバル IP アドレスが自動設定されます．

◆ KAINS-V（KAINS for Visitor）

学会や共同研究員として本学に滞在する学外者・来訪者が使用するネットワークです．現在は，eduroam サービスにて代用しています．

3　KAINS のこれから

3.1　KAINS11 における課題

KAINS11 は，本センターにおいてキャンパス内のすべての建屋におけるフロア L2SW までを対象に，全学ネットワークの統合管理体制へ移行しています．これに伴い，全学的なネットワークサービスの提供が可能となっていますが，部分的なリース契約や段階的な改修により，恒常的なネットワークの安定運用の実現には至っていません．

また，無線ネットワークにおいてはネットワーク ID を用いたユーザ認証を実現していますが，有線ネットワーク（特に KAINS-B）では接続時の認証ができていない点が課題となっています．本学にて許可した利用者のみの制限を可能とし，セキュリティインシデント発生時など，発生元の利用者を特定し迅速な対応を実施するために解決しなければなりません．

これらの課題の解消を，2016 年度に実施する KAINS のシステム更新にて実施することを目指し，現在，次期

1. eduroam: http://www.eduroam.jp/

KAINS（KAINS16）の仕様策定作業を進めており，図3に示すような構想を持っています．以下に，KAINS16における主な取り組みを紹介します．

3.2　恒常的な安定運用を実現する全学リース化

KAINS11では，予算の関係上，基幹ネットワークを中心に一部の地区（主に角間キャンパス南地区）のみのリース化にとどまりました．そのため，買取り機器による運用地区では依然として機器の故障に対して迅速な対応を行えない可能性が残っていましたので，KAINS16においては，全学でのネットワークのリース契約を実現することを目標としています．

全学リース化により，予算確保等に伴う障害対応の遅れが解消され，ネットワークの統合管理体制も合わせて実現できると考えています．これらのことは，ますます重要となっている情報通信ネットワークにおいて，これまで以上に恒常的で安定した運用を可能にします．

3.3　端末接続セキュリティの向上と統合運用管理

KAINS16では，安心・安全なキャンパスネットワークの実現に向けて，有線ネットワークにおける接続認証の仕組みを導入する方針で仕様策定を進めています．これまでに導入していた，インターネット通信時にユーザ認証する仕組みからセキュリティを一段強化し，ネットワーク接続時にも認証を実施します．技術的にはネットワークインターフェイスに設定されるMACアドレスによる認証手法等を用い，利用者と機器情報の紐付けを実現します．

また，これまで台帳管理などで割り当てていたIPアドレスの管理も，システム化して集中管理できる環境を目指します．これにより，部局管理者を設置することが困難となりつつある部局ネットワークにおける資源管理を本センターで引き取ることを実現し，統合的なネットワーク運用管理体制とします．合わせて全学的な自動アドレス設定環境を構築し，利用者のネットワーク設定を簡素化することで設定ミスによる通信不能障害を減少させたいと考えています．

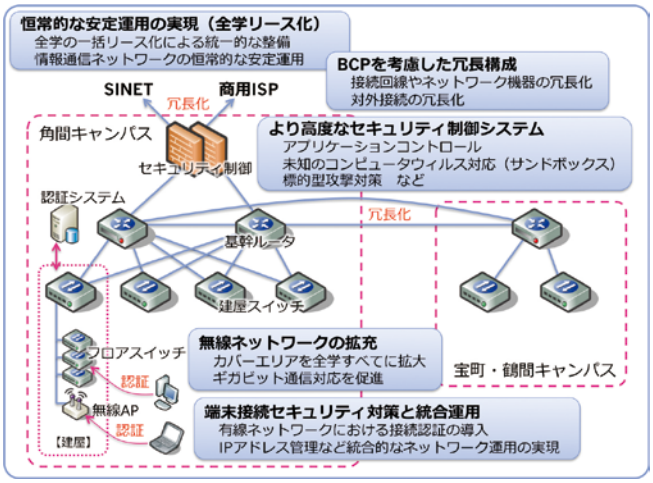

図3　KAINS16における構想

3.4　BCPに向けた接続回線の冗長化

2011年3月に発生した，東日本大震災を受け，大学においても事業継続計画（BCP：Business Continuity Planning）の必要性が議論されています．本学においても，必要最低限の通信やサービスを選定し，災害および障害時における通信を確保するために，冗長性のあるネットワーク構成を検討しています．

KAINS16においては，外部データセンターの利用を始め，キャンパス間接続や対外接続における冗長化，他大学やデータセンターへの重要データのバックアップを実現するに十分な通信帯域の拡張を考えています．特に2016年度から運用が始まるSINET5への接続帯域に関しては，外部データセンター利用を考慮して，現在の10Gbpsからの増速を計画しています．

3.5　無線ネットワークの拡充とギガビット対応

2011年度に提供を開始したKAINS-WiFiサービスは，同時接続ユーザ数が右肩上がりに増加しており，2015年4月時点では5,000ユーザを超えました．これは利用者の認知度が向上したことによる増加だけではなく，スマートフォンをはじめとしたスマートデバイスによる利用が増したことに起因していると思われます．このような傾向は今後も拡大していくと考えており，センサーデバイスも含め，利用者一人に対して複数のデバイスが接続される状況が一般的になると考えています．さらに，アプリケーションの高度化により，通信トラフィックの増加も考えられます．

そこでKAINS16では，無線LAN対応エリアの拡大と次世代の無線LAN規格である802.11acの導入を検討しています．802.11acは，ギガビット無線LANとも呼ばれており，条件次第では1Gbpsを超える通信が可能です．KAINS16の利用最終年度が2021年度であることを考えると，決して大きくない性能だと考えています．

4　おわりに

本稿では，KAINSの紹介として，KAINS11にて実現したこれまでの取り組みと，KAINS16にて実現を目指しているこれからの取り組みを紹介しました．キャンパスネットワークに求められる機能や信頼性は，ネットワークを利用した情報処理の重要性が増しているため，より高いものが求められます．実現するためには莫大な予算をつぎ込めば可能ではありますが，限られた中で創意工夫することが本センターに求められていると考えています．

KAINS16の仕様に関しては，本稿が発行された時点で決定していると思われます．今後も利用者のみなさまに不便な思いをさせないよう，より良いネットワーク環境の構築に向けて取り組んでいきたいと考えています．