事務基幹サーバのクラウド化を支援するキャンパスネットワーク

近堂　徹[†],　　宮原　俊行[‡],　　相原　玲二[†]

[†]広島大学情報メディア教育研究センター

[‡]広島大学学術・社会産学連携室情報化推進グループ

{tkondo,tmiyahar,ray}@hiroshima-u.ac.jp

概要　大学におけるキャンパスネットワークは，大学の主要インフラのひとつとして高いセキュリティと安定性を確保しつつ，ユーザの利便性を損なわないことが必要である．一方でその上で動くアプリケーションやサーバについては，民間企業だけでなく学術機関においてクラウドを導入する動きが顕著になってきている．特に，今後はパブリッククラウドサービスを柔軟かつ安全に利用できることが強く求められ，キャンパスネットワークに対する役割も変わりつつある．広島大学では，2013 年度より財務会計システムや人事・給与システムなどの管理運営サービスをパブリッククラウド等に移行するの取り組みを進めてきた．本稿では，これらの事務基幹サーバのクラウド化を支えるキャンパスネットワークについて紹介するとともに，クラウドへの移行を通じて得られた成果や課題について述べる．

1　はじめに

大学などの高等教育機関におけるキャンパスネットワークは，教育研究活動から管理運用業務に至る様々な活動を支える主要インフラとしての必要性が高まるばかりである．近年では，ICT を活用した授業支援や学外者も含めた BYOD(Bring Your Own Device)，基幹業務系での利用など，その利用形態は多種多様でとなっている．単にネットワーク接続性を提供するだけでなく，高いセキュリティと安定性を確保しつつユーザの利便性を損なわないことが求められる．

一方で，キャンパスネットワークの上で動くアプリケーションやサービスなどはクラウドコンピューティング導入による効率化の動きが顕著になってきている．大学等でもアカデミッククラウド環境整備の議論が進むなか，学術情報基盤の強化・充実にはクラウド化への対応を含むネットワークの高度化は避けて通れない課題となっている [1]．今後は，より大量のデータ流通への対応や耐障害性・高信頼性に優れたネットワーク基盤への要求が明確となっている．

広島大学では 2013 年度より，財務会計・出張旅費などの財務系システムや人事給与・労務管理などの人事系システム等の事務基幹システムをパブリッククラウド等へ移行し，運用の効率化への取り組みを進めている．移行にあたっては，クラウドサービスのセキュリティや信頼性，コストなどの検討だけでなく，大学内外からクラウドサービスへアクセスするためのネットワークについても検討を行ってきた．また，この成果や技術動向を踏まえ 2014 年 8 月にキャンパスネットワークの更新を行った．新しいキャンパスネットワークでは，これまでのキャンパスネットワークが提供してきた機能に加え，クラウドコンピューティングを活用をコンセプトにいくつかの機能拡張を実施している．

本稿では，新キャンパスネットワーク (HINET2014) の概要について述べ，事務基幹サーバのクラウド移行に対する HINET2014 での実現方法について紹介するとともに，その成果と課題について考察する．

2　広島大学のキャンパスネットワーク

本学のキャンパスネットワークの規模等を明らかにするために，これまでのキャンパスネットワークの変遷について述べる．広島大学のキャンパスネットワークは，主要 3 キャンパス（東広島キャンパス，霞キャンパス，東千田キャンパス），附属学校（翠地区，東雲地区，三原地区，福山地区）および小規模遠隔部局（呉，竹原，宮島，東京オフィス等）の拠点から構成される．構成員数は，教員約 1,800 人，職員約 3,300 人，学生約 15,000 人（附属学校の児童，生徒約 4,000 人は含まない）の規模である．

広島大学での本格的なキャンパスネットワークは FDDI を基幹に採用した HINET93（1994 年稼働）に始まり，ATM を基幹に採用した HINET95（1995 年稼働），Gigabit Ethernet を基幹とする HINET2001（2001 年稼働）と更新を重ねてきた．いずれにおいても，原則サブネットを部局単位に割当てを行い，各部局で管理する体制で運用を行ってきた．2008 年度から運用を開始した HINET2007[2] ではそれまでの管理方

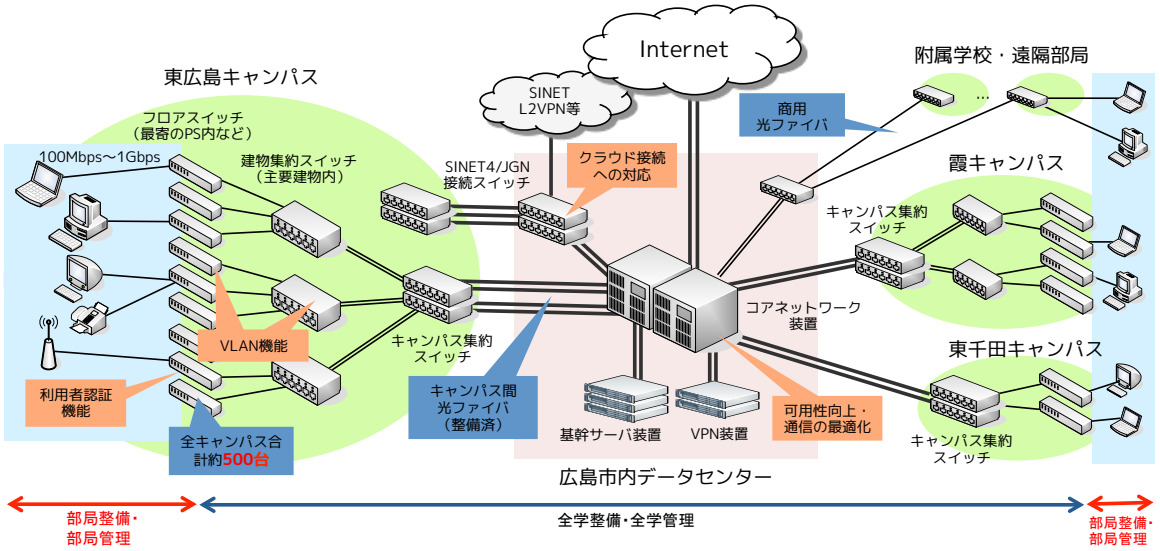

図 1: HINET2014 の概要

法を一新し，全学整備および一元管理によるキャンパスネットワークを構築・運用してきた．基幹ネットワークだけでなくフロアスイッチ（2014 年 10 月時点で約 500 台）を対象とした整備を実施し，部局単位でのサブネット管理体制から全学的な一元管理体制へと移行した．ネットワーク構成については，学内外からのアクセス可否パターンおよび利用形態により区別される「ゾーン」という概念を導入し，利用形態に応じたゾーンを各構成員に提供している．さらに，研究室を含むすべての利用場所で Web 認証もしくは Mac 認証による利用者認証を要求し機器管理をおこなうことで，利用者の制限や接続機器の把握を行ってきた．これらは 3 章で述べる新キャンパスネットワーク HINET2014 でも同様の機能を引き続き実現しているため，詳細については後述する．

3　キャンパスネットワーク HINET2014

本章では，2014 年 8 月より稼働を開始した新キャンパスネットワーク HINET2014 について紹介する．

3.1　概要と主な特徴

ネットワーク構成を図 1，主要な機器仕様を表 1 に示す．コアスイッチ装置および各キャンパス集約スイッチは全てスタック接続かつリンクアグリゲーションによるアクティブ・アクティブ構成とし，ファイアウォール装置と VPN 装置については HA (High Availability) によるアクティブ・スタンバイ構成としている．これにより，装置やリンクの故障に対する冗長性を確保した．

HINET の主な特徴は以下に示す通りである．

表 1: 基幹ネットワーク装置の主な機器仕様

機器名称	機種	数量
コアスイッチ装置	Cisco Catalyst 6807-XL	2
ファイアウォール装置	Cisco ASA5585-X / SSP60	2
VPN 装置	Cisco ASA5545-X	2
キャンパス集約スイッチ	Alaxala AX3830（東広島）	2
	Alaxala A2530S (霞, 東千田)	各 2
基幹サーバ装置	DELL PowerEdge R620	3

基幹装置のデータセンター設置　学内に存在する様々なサービスが今後クラウドを利用していくことを想定し，HINET2014 では基幹装置の主要部分をデータセンターへ設置している．これにより，対外接続拠点であるデータセンターから各キャンパスが接続される完全なスター型ネットワークとなり，対外接続に対するトラフィックの経路最適化を実現している．データセンターと各キャンパス間は自設の光ファイバを用いて最大 40Gbps（東広島～データセンター）の帯域を確保した．

ゾーニングによるネットワーク設計　HINET では学内外からのアクセス可否パターンおよび利用形態により区別される「ゾーン」という概念を導入している．図 2 にゾーンの概要を示す．構成員の多くが研究室単位でゾーン C を申請し，その中に PC やプリンタ，NAS 等を設置して管理・運用するのが一般的な利用形態となっている．学外公開が前提となるサーバはゾーン A，複数のゾーン C やゾーン D から利用する可能性のあるプリンタや NAS 等の学内限定ホストはゾーン B に設置する形で運用している．構成員はネットワーク利用申請サービスを通して各種の申請を行う．

個別ファイアウォール機能の提供 約 2,000 の個別ファイアウォール (NAPT) 機能と DHCP サーバ機能をキャンパスネットワークの機能として全学的に提供し，管理・維持コストの削減を図っている．2,000 という数字は本学教員等の数を勘定して設定したものであり，1 教員 1 個別ファイアウォール（ゾーン C）の提供が可能となる．また，ゾーン C の管理者によって構成員の ID をネットワーク利用申請サービスで事前登録することにより，特定のゾーン C の機器と直接接続可能な VPN サービスも提供している．

全学的な一元管理体制 全学整備の範囲を基幹ネットワークからフロアスイッチまでとし，約 500 台のフロアスイッチを一元管理とした．ポート総数としては，18,000 ポートとなる．各ポートにはコネクタ ID とよぶラベルを情報コンセント毎に付与し，ネットワーク利用申請サービスからの申請に基づきポートの設定をメディアセンターで一括して行う．

すべての利用場所で利用者認証を要求 多様な機器に対応するために，Web 認証もしくは MAC 認証による利用者認証を行っている．Web 認証は学認によるシングルサインオンに対応している．認証ポイントはフロアスイッチとし，認証後はワイヤーレートでの通信が可能である．

SINET4/JGN-X における L2 接続の強化 HINET ではコアネットワーク装置から各フロアスイッチまでは全てレイヤ 2 ネットワークで構成している．この利点を生かし SINET4/JGN-X 等の実験プロジェクトおよび商用クラウド接続を強化している．

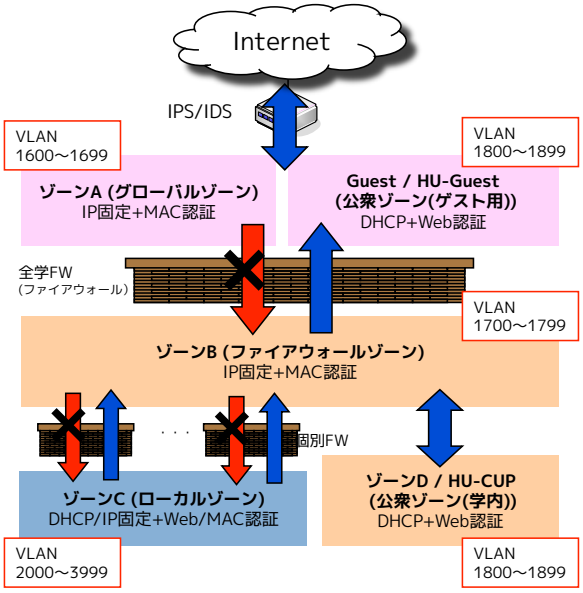

図 2: HINET におけるゾーン構成

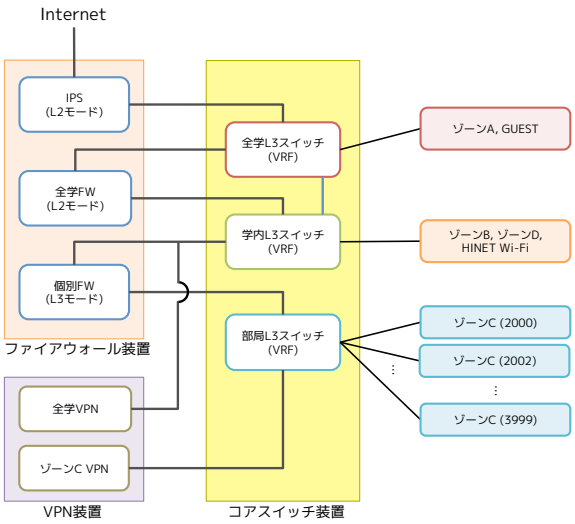

図 3: コアネットワーク装置の構成

3.2 基幹ネットワーク構成

コアネットワーク装置の内部構成を図??に示す．基本方針は以下の通りである．コアスイッチは VRF 機能により 3 つの独立した仮想 L3 スイッチを定義し，L3 スイッチ間の相互通信はファイアウォール装置経由で行う．ただし，ゾーン C からゾーン A および学外宛の通信については，学内 L3 スイッチにてポリシールーティングにより，全学ファイアウォールをバイパスするように設計した．また，インターネットとの接続点には IPS を導入し，P2P など悪意あるトラフィックに対する抑制を行っている．

次に個別ファイアウォール機能（ゾーン C）の実現について述べる．個別ファイアウォールは 1 教員 1 ゾーン C を割当できるように 2,000 個のゾーン C を提供できる設計としている．2,000VLAN の収容および個別ファイアウォールへのルーティングは部局 L3 スイッチで行う．部局 L3 スイッチでは，ACL を設定することで，ゾーン C 間の通信ができないように設定している．IPv4 については，個別ファイアウォールで 2,000 の NAPT 機能を提供し，ゾーン C あたり 1 つの外部 IP アドレスとなって外部へのアクセスを行う．また，原則全てのゾーン C に対してリレー機能により DHCP を提供している．IPv6 については，NAPT 機能は提供せずファイアウォール機能のみを提供し，アドレス配布は RA のみをサポートしている．

4　事務基幹サーバのクラウド移行

本章では，HINET における事務ネットワークの構成について述べるとともに，事務基幹サーバのクラウド化への対応方法について示す．

4.1　事務におけるネットワーク構成

ネットワーク構成を示す前に，本学における事務組織構成について説明する．事務組織は研究科等の部署から構成されており，約 30 程度の部署が存在している．同一部署が建物やキャンパスをまたいで構成されている場合も少なくない．事務組織全体でおおよそ 1,300 台の事務用端末が配備され，職員がこれらの端末を利用して日々の業務を行っている．事務端末およびサーバの管理・運用は学術・社会産学連携室情報化推進グループの所掌となっている．

HINET ではこれらの事務組織を管理するためのネットワークを図 4 のように構成している．大きく分けて 4 つのエリアに分けられる．一つ目が事務端末ネットワークであり，これは部署単位でゾーン C（合計で約 30 程度）を割り当てている．これにより，建物やキャンパスを越えるような事務組織であっても同一ネットワークとして収容することができる．また，ゾーン C 間では通信を行うことができないため，部署内でのみ共有するファイルサーバ等も設置することも可能となっている．二つ目めが事務端末ネットワークからのみアクセスできる事務管理サーバセグメントである．主に端末を管理するためのサーバや事務組織でのみ利用するファイルサーバ等が設置されている．これにはひとつのゾーン C を割当て，部局 L3 スイッチの ACL により特定のゾーン C からのみアクセス許可を行う例外設定を加えることで実現している．三つ目がゾーン A セグメントである．これは事務管理サーバのうち，学外アドレスに対しても公開しているサーバ群が設置されている．広島大学の教員用ポータルサイトや研究者総覧等が該当する．四つ目がゾーン B セグメントである．これは事務管理サーバのうち，学内アドレス限定で公開しているサーバ群が設置されており，財務会計システムや人事・給与システムが該当する．

このうち，ゾーン A セグメントおよびゾーン B セグメントのサーバに関して，現行システムのハードウェア更新のタイミングで順次パブリッククラウド等への移行を進めている．移行にあたっては本学が定める「広島大学クラウドサービス利用ガイドライン」[1]に従い，セキュリティやネットワーク要件を確認しつつ作業を進めた．次節では，パブリッククラウド接続を含めたネットワーク構成について述べる．

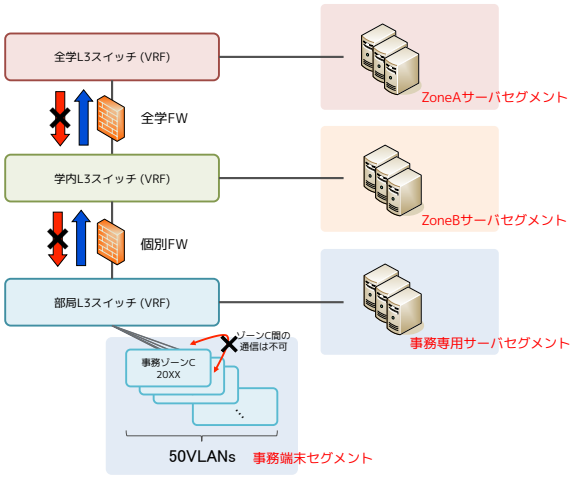

図 4: 事務ネットワークの内部構成

4.2　パブリッククラウドとの接続

図 5 にクラウド接続との構成図を示す．本学では現在，マイクロソフト社が提供する Microsoft Azure および Amazon.com が提供するアマゾンウェブサービスの 2 つの IaaS サービスと接続し各種サービスを稼働させている．クラウド上で稼働している主要なサービスを表 2 に示す．

各クラウドとの接続は L3VPN(IPsec-VPN) およびインターネット経由で接続している．L3VPN は事務端末ネットワークから事務職員がアクセスする際に利用する一方，それ以外の学内外からの一般構成員のアクセスはインターネット経由で http/https にで行われている．クラウド内はサービスおよびアクセス範囲を考慮し，複数の VPC(Virtual Private Network) を構築し，それぞれを L3VPN で接続する形とした．このようにすることで，特定の事務ネットワークからのみ別経路でクラウド上のリソースにアクセスすることができ，ネットワーク全体のセキュリティ設定などに大きな影響を与えることなくクラウドを利用することが可能となっている．また，一般構成員のアクセスに対してゾーン B 相当（学内 IP アドレスからの接続）を保証するために，フルトンネリングによる VPN 接続サービスを提供している．

表 3 に，本学と Microsoft Azure との L3VPN 接続におけるスループットおよび RTT の計測結果を示す．なお，Azure は Ubuntu 14.04LTS,1core,175GB のインスタンスを利用し，VPN 装置には Cisco 892FSP を利用している．帯域は Iperf[2] を用いて TCP 片方向 60 秒間の測定結果となっている．

[1] http://www.media.hiroshima-u.ac.jp/news/cloudguide

[2] http://sourceforge.net/projects/iperf

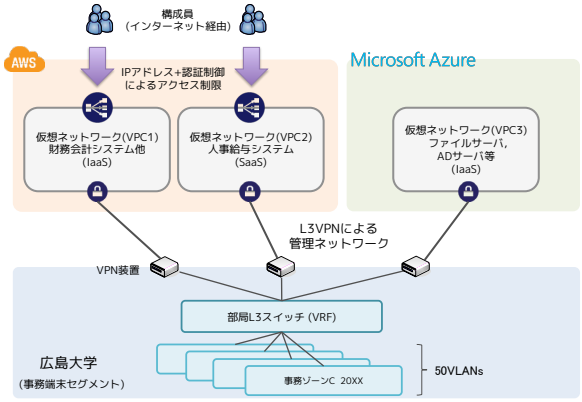

図 5: L3VPN によるクラウド接続

表 2: 主要なサービス稼働状況

サービス名	利用基盤	運用形態
財務会計システム	AWS	IaaS
人事・給与システム	AWS	SaaS
事務用ファイルサーバ，AD サーバ等	Microsoft Azure	IaaS

4.3 成果と課題

HINET はコアネットワーク機能をデータセンターに集約し，IP アドレスや VLANID 等の資源の一元管理を行いつつ，ゾーニングによるネットワーク利用形態を基本としてネットワークの単位を各事務組織や研究室といった細かな単位で柔軟に設定できることを特徴としている．ゾーニングの単位がクラウド利用の単位となり，クラウドの利用形態を必要に応じて柔軟に選択できることは大きなメリットである．

クラウド上のサーバをあたかもキャンパス内に設置されたサーバとして利用するには，接続の柔軟性に加え，通信帯域や遅延時間が重要な要素となる．今回，事務基幹サーバのクラウド接続については IPsec による L3VPN 接続環境を構築したため，VPN 接続のオーバーヘッドや MTU および MSS 長の問題が潜在している．現時点で実用上の問題は発生していないが，今後 SINET クラウドサービスを活用し，SINET 内を L2VPN 接続することも検討している．3.1 章で述べた通り，HINET はコアネットワーク装置を集約しキャンパス内は多数のレイヤ 2 ネットワークを利用者の申請に応じて設定している．SINET クラウドサービスによる商用クラウドの接続環境を任意のフロアスイッチに設定することは，通常の運用として容易に実現可能である．

表 3: スループットおよび RTT 計測

測定方向	帯域 (Mbps)	RTT (ms)
広島大 → Azure(東日本)	146	25.53
広島大 ← Azure(東日本)	117	28.41
広島大 → Azure(西日本)	149	32.48
広島大 ← Azure(西日本)	102	31.65

5 おわりに

本稿では，広島大学が 2014 年 8 月より運用を開始した新キャンパスネットワーク HINET2014 について述べるとともに，2013 年度より順次移行を行っている事務基幹サーバのクラウド化を支援するためのネットワーク構成について説明した．HINET の特徴はネットワーク資源の一元管理を行いつつ，ゾーニングによりネットワークの単位を各事務組織や研究室といった細かな単位で柔軟に設定できる点にある．

今後，ネットワーク利用の多様化に伴い，キャンパスネットワークに対する役割も変わりつつある．対外クラウド接続についても例外ではなく，大学においてもパブリッククラウドサービスを柔軟かつ安全に利用していくことが必須となる．インターネット接続性だけではなく，サービス連携を含めたネットワーク基盤としての活用を今後検討していく．

謝辞

キャンパスネットワークの構築および運用に尽力頂いている情報メディア教育研究センターおよび学術・社会産学連携室情報化推進グループの関係者各位に感謝致します．

参考文献

[1] 文部科学省, ”教育研究の革新的な機能強化とイノベーション創出のための学術情報基盤整備について－クラウド時代の学術情報ネットワークの在り方－（審議まとめ）”, 2014.

[2] 近堂徹, 田島浩一, 岸場清悟, 大東俊博, 岩田則和, 西村浩二, 相原玲二, ”利用者認証機能を備えた大規模キャンパスネットワークの性能評価”, 第 1 回 IOT シンポジウム 2008 論文集，pp.121-128, 2008.