クラウドコンピューティング活用のための大規模キャンパスネットワーク

近堂 徹[1,a)]　田島 浩一[1]　岸場 清悟[1]　吉田 朋彦[1]　岩田 則和[1]　大東 俊博[1]　西村 浩二[1]
相原 玲二[1]

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．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 2014 年 8 月より新キャンパスネットワーク HINET2014 の運用を開始した．HINET2014 では，従来より提供している全教員の個別ファイアウォールに対し学内外から接続を可能とする VPN サービスの追加，研究室と商用クラウドサービスを SINET 経由で直結する L2VLAN サービスの追加等により，クラウドコンピューティングの活用を支援するための機能を充実させた．本稿では，これら機能について述べるとともに，現在運用中の HINET2014 の性能測定結果について示す．

A Large Scale Campus Network System for Taking Advantages of Cloud Computing

Tohru Kondo[1,a)]　Koichi Tashima[1]　Seigo Kishiba[1]　Tomohiko Yoshida[1]　Norikazu Iwata[1]
Toshihiro Ohigashi[1]　Kouji Nishimura[1]　Reiji Aibara[1]

Abstract: In universities, campus network systems which have convenience and user-friendliness while ensuring stability and security has been mandatory. Functions for taking advantages of public cloud computing are strongly required to the current campus networks. In Hiroshima University, a new campus network system HINET2014 has been launched at August 2014. HINET2014 is newly providing functions for cloud computing such as VPN service connecting devices outside or inside of the university to dedicated firewall networks for all academic staffs, L2VLAN service directly connecting networks between a laboratory in the university and public cloud services through SINET. In this paper, we describe these distinguishing features which bring flexible environment in the campus network, and demonstrate measurement results of the system.

1. はじめに

大学などの高等教育機関では，教育研究活動のための高度で柔軟なキャンパスネットワークが求められる．単にネットワーク接続性を提供するだけでなく，ICT を活用した授業支援や学外者も含めた BYOD，基幹業務系での利用など，その利用形態は多種多様となっている．そのため，高いセキュリティ・安定性を確保しつつユーザの利便性を損なわないキャンパスネットワークが必要となる．

近年では，大学等でもクラウドコンピューティングを導入する動きが顕著になりつつあり，アカデミッククラウド環境整備の議論があるなか，今後はより大量のデータ流通への対応や高セキュリティ・耐障害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 [1]．このような背景から，キャンパスネットワークに対する大学の主要インフラとしての重要性は増すばかりである．

広島大学では 2008 年度からキャンパスネットワークの管理方法を一新し，全学整備および一元管理によるキャン

[1] 広島大学情報メディア教育研究センター, Information Media Center, Hiroshima University
[a)] tkondo@hiroshima-u.ac.jp

パスネットワークを構築・運用してきた [2]．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するとともに，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構成員に提供する．さらに，研究室を含むすべての利用場所で何らかの利用者認証を要求し機器管理を行うことで，利用者の制限や接続機器の把握を行ってきた．

これまでの運用で上述の管理体制が利用者へも浸透し，障害時やセキュリティインシデント時などの迅速な調査・対応にも一定の効果が得られている [3]．2014 年夏には，これまでの運用で得られた課題や知見をもと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，これまで提供してきた機能に加え，クラウドコンピューティングの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，今回導入した新たな機能およびこれらの効果について考察する．

本稿の構成は以下の通りである．まず 2 章では，これまで運用してきたキャンパスネットワークの変遷について述べる．3 章では HINET2007 の考え方を踏襲し，新たに性能面・機能面で向上させた HINET2014 の概要について述べる．特に，従来より提供する各教員の個別ファイアウォールに学内外から接続を可能とする VPN サービス，教員単位で商用クラウドサービスと直結することができる L2VLAN サービスを中心に紹介する．4 章では，基幹ネットワークに関する性能測定について示し，最後に 5 章でまとめを記す．

2. 広島大学におけるキャンパスネットワークの変遷

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，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．

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 に始まり，ATM を基幹とする HINET95，Gigabit Ethernet を基幹とする HINET2001 と更新を重ねてきた．HINET2001 は，主要 3 キャンパスにそれぞれ 1 台の L3 スイッチ（ルータ）を配置し，主要な建物には約 50 台の L2 スイッチを配置し同一キャンパス内の L3 スイッチと Gigabit Ethernet で接続していた．L2 スイッチは配下のネットワークは部局による整備管理とし，ネットワークについても原則サブネットを部局単位で管理する体制で運用を行ってきた．

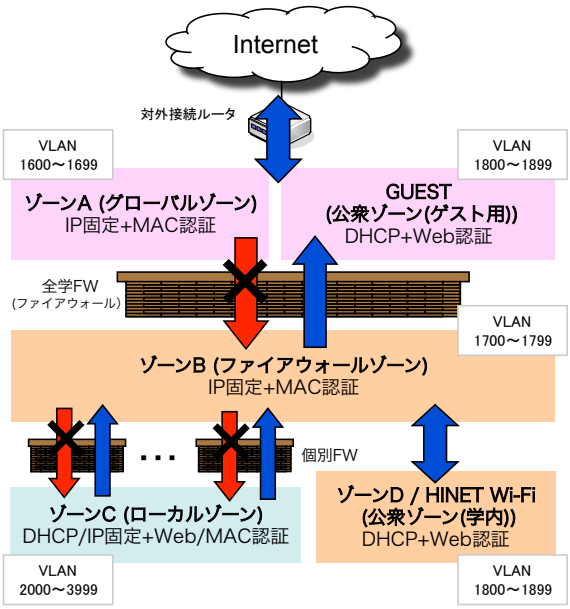


図 1 ゾーン間のアクセス制御概念

2008 年度より運用を開始した HINET2007 では，それまでの運用を刷新し，新たな方針で設計・運用を行ってきた．特徴としては次の通りである．

全学的な一元管理体制

全学整備の範囲を各フロアのポートまで拡大し，基幹ネットワークからフロアスイッチまでの約 500 台を一元管理とした．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，利用者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．

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た．2,000 という数字は本学教員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の提供が可能となる．

VLAN を活用した柔軟な仮想配線の提供

個別ファイアウォール機能を提供した場合，同一ファイアウォール配下としたい部屋が同一フロアや同一建物とは限らない．IEEE802.1Q(TagVLAN) 機能により，既存配線を有効に活用しながら，キャンパス間をまたがる同一ネットワークの構築や部屋内の共有スペースで複数ネットワークの提供を可能としている．

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．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．

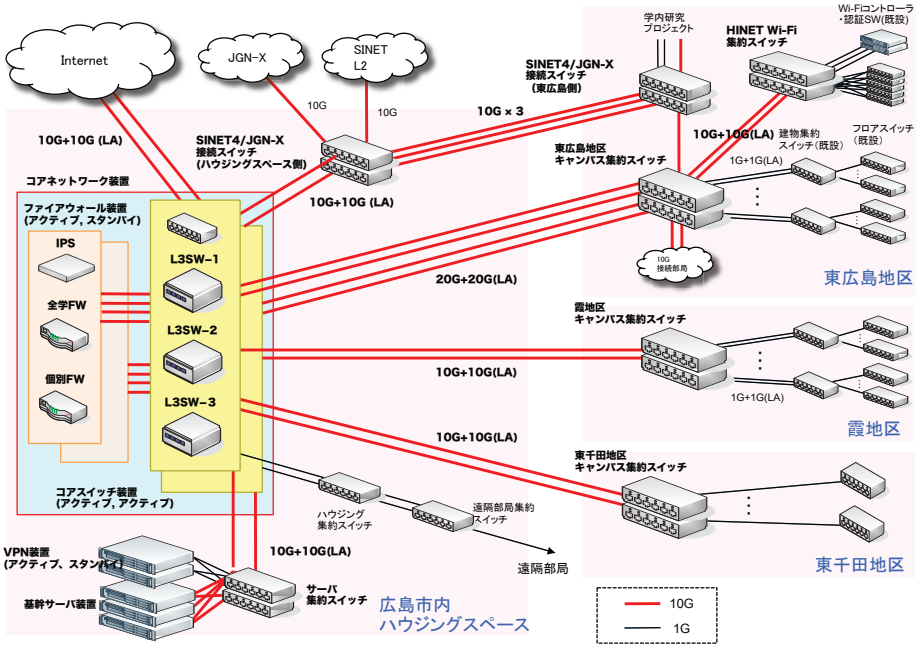


図 2　基幹ネットワーク構成

HINET2007 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た．図 1 にゾーンの概要と利用している VLANID の範囲を示す．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．

HINET2007 は 6 年間にわたり運用を行い，管理一元化による障害時やセキュリティインシデント時などの迅速な調査・対応にも一定の効果が得られている．フロアスイッチのポート単位まで障害を集約して把握できるとともに，ホスト単位で管理者が明確になることで脆弱性診断やインシデント時の管理者へのリーチが容易にできるようになった．

その一方で改善点もみえてきた．ひとつは可用性・耐障害性の向上である．HINET2007 では対外接続拠点を広島市内のデータセンターに設置する一方，基幹装置を東広島キャンパスに設置していた．そのため，東広島キャンパス以外のすべての通信が必ず東広島キャンパスを経由することによる経路の冗長性や，毎年の法定停電における電源供給対応などが課題となり，より効率性と安定性を考慮する必要があった．今後，多くのサービスでクラウドを活用することを考えるとこの点は無視できない．また設定管理を一元化したことで，利用申請から利用開始までの設定期間を如何に短くするか，個別ファイアウォール配下への学外からの接続に対する要望等，利便性の向上についても検討が必要であった．

3. 新キャンパスネットワーク HINET2014 の概要

本章では，HINET2007 での運用経験を踏まえ，2014 年夏に更新を行った新キャンパスネットワーク HINET2014 について概説する．今回の更新対象となった基幹ネットワーク構成およびサーバ構成と主な特徴について述べる．

3.1 ネットワーク構成

基幹ネットワーク構成を図 2, 主要な機器仕様を表 1 に示す．今回の更新ではコアネットワーク装置およびキャンパス集約スイッチまでを更新対象とし，建物集約スイッチおよびフロアスイッチについては既設機器をそのまま活用する方針とした．なお，利用者に提供するネットワーク（VLAN や IP アドレス）は HINET2007 の設定情報を引継いでいる．これにより，利用者への変更作業等は原則発生しない．

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・スタンバイ構成による構成としている．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．

コアネットワーク装置の内部構成を図 3 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，

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

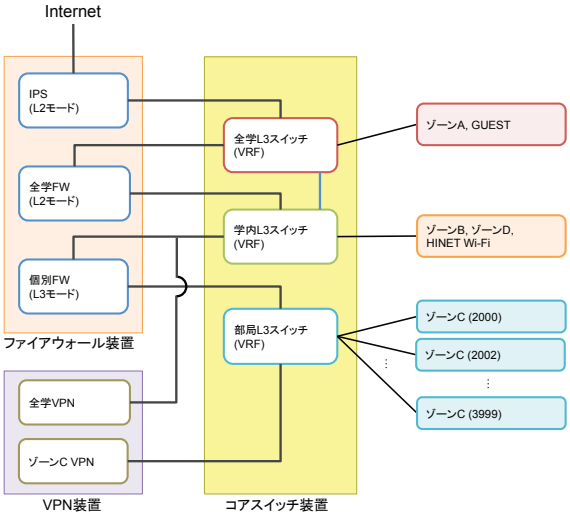


図 3 基幹ネットワーク装置の内部構成

全学ファイアウォールと部局ファイアウォールでは，外向きの通信に対しては同一のインスペクションルールを適用しているため，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，2,000 の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．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．これらのアドレス割当ポリシーは HINET2007 での情報を引継いでいるため，文献 [4] を参照されたい[*1]．

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する．また，アドレス配布は RA のみをサポートしている．

[*1] 一部は後述する図 5 に記載している

表 2 基幹サービスにおける主なソフトウェア仕様

サービス名称	ソフトウェア
利用者認証サービス	Free Radius 2.1.12-4.el6_3 Open LDAP 2.4.33-3.el6
DHCP サービス	ISC-DHCP 4.2.5p1 相当
ネットワーク構成管理サービス（障害検知）	Zabbix 2.2.4-1.el6
ログ管理サービス	Amazon S3, Redshift

3.2 基幹サービス構成

HINET2014 では関連する基幹サービスも更新対象とした．図 4 に基幹サービス構成図，表 2 に主なソフトウェア仕様を示す．Web 認証/MAC 認証/シングルサインオン認証を担う認証サービス，DHCP サービス，ネットワーク構成管理サービス，ログ管理サービス，ネットワーク利用申請サービスの 5 つのサービスを 3 台の基幹サーバ装置に仮想化して動作させている．そのうえで，各サービス毎に二重化して異なる筐体に分散配置することにより負荷分散と耐障害性を向上させている．

このうち，DHCP サービスは約 2,000 のゾーンに対して各ゾーン最大 120 アドレス（ネットワーク全体では最大約 24,000 アドレス）を割り当てる DHCP 機能を担い，ログサービスはフロアスイッチの認証ログやファイアウォールログ等を保存するために利用される．認証サービスは Radius サーバおよび LDAP サーバとネットワーク認証をシングルサインオン対応させるための SP より構成される．サービスの多くは HINET2007 での機能を引継ぐ形としているが，サーバ台数を集約し，かつ高負荷が予想されるサービスを一部クラウドリソースを使うなどして効率化を行った．詳細については，次節以降で述べる．

3.3 主な特徴

HINET2014 では，原則として IP アドレスや VLAN の割当ポリシーは変更しない一方で，HINET2007 における運用の知見を活かしていくつかの機能拡張・追加も行っている．以下に主な特徴を述べる．

基幹装置のデータセンター設置

今回の更新では基幹装置の主要部分をデータセンターへ移設した．これにより，従来課題となっていたトラフィックの経路最適化を行うことができ，対外接続拠点であるデータセンターを中心とした完全なスター型ネットワークとなった．データセンターと各キャンパス間の帯域も増強し，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．また，BCP 対策として商用回線によるバックアップも計画している．

ネットワーク利用申請とフロアスイッチ設定の自動化

2 章でも述べた通り，フロアスイッチのポート利用

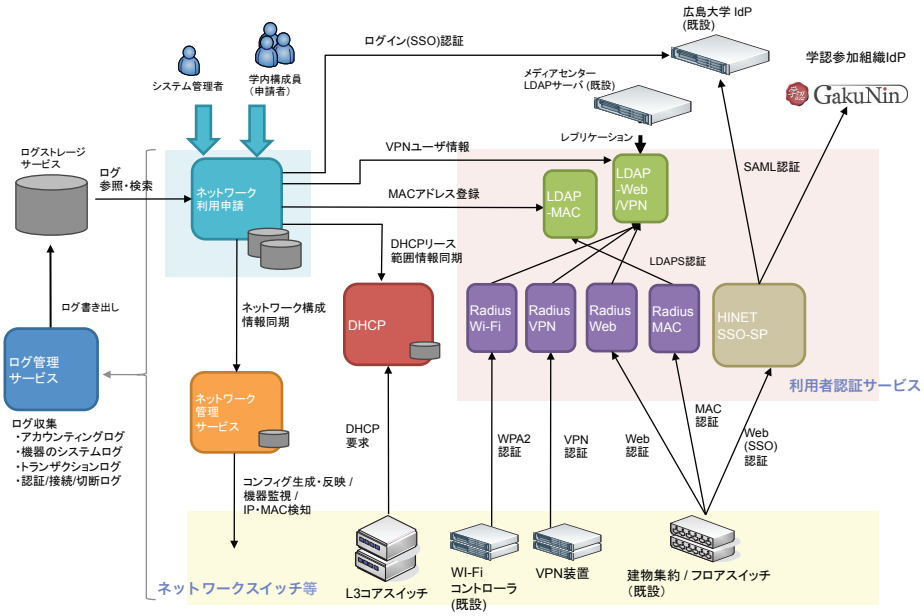


図 4 基幹サービス構成

申請や接続する機器の MAC 認証のための MAC アドレス登録は各構成員の申請が必要となっている．HINET2007 では，フロアスイッチへの VLAN 設定については委託業者による手動設定を行っていたため．申請から利用開始まで 1〜2 営業日を要していた [5]．HINET2014 ではこの問題点を解決するために，ネットワーク利用申請と連携したフロアスイッチの自動設定が可能な設計とした．

個別ファイアウォールに接続可能な VPN サービス

HINET2014 では通常の学内接続の VPN に加え，2,000 の個別ファイアウォール（ゾーン C）に対してセキュアに接続可能な VPN サービスを新たに導入した．詳細については 3.4 節で説明する．

SINET4/JGN-X における L2 接続の強化

2 節で述べた通り，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 L2 で構成され，VLANID は全学一元管理となっている．HINET2014 では，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．詳細については 3.5 節で説明する．

ログ保存・検索のためのクラウドサービス活用

これまで述べている通り，DHCP アドレス払い出し，Web 認証/MAC 認証やファイアウォール通信など，基幹機能を一元管理としているため，そこで生成されるログも膨大なものになる．HINET2007 でもログ収集・検索機能は有していたが，ログ保存容量の肥大化とともに検索性能の鈍化がみられるようになっていた．HINET2014 では，この問題を解決するために，ログの保存と管理のために外部のパブリッククラウドサービスを利用し，検索も全てクラウドリソースを活用することとした．

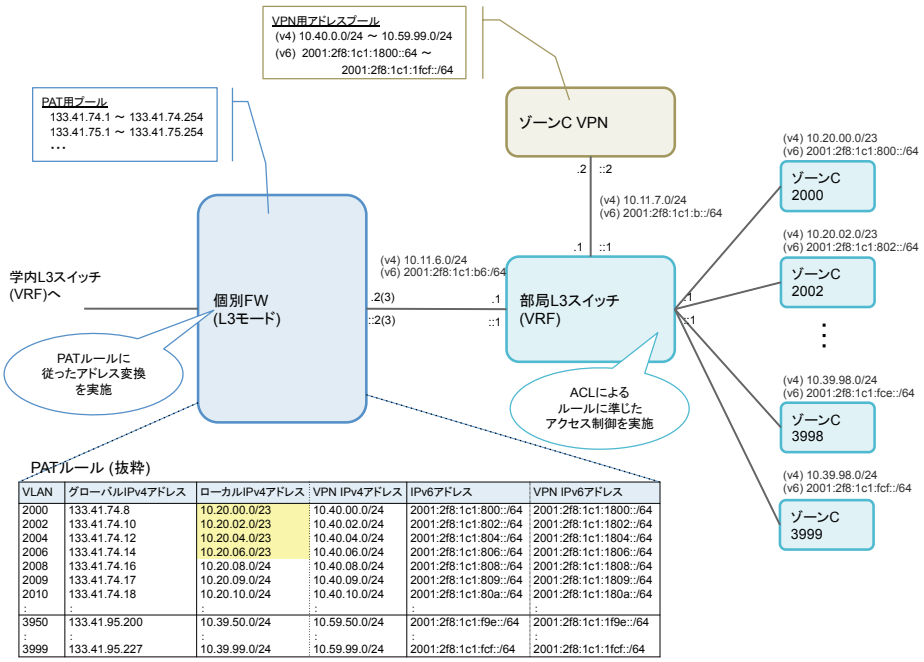
すべてのゾーンで IPv6 を標準サポート

HINET2014 ではファイアウォール装置で IPv6 のポリシーも同時に設定している．これにより，HINET2007 では限られたゾーンでのみサポートしていた IPv6 の適用範囲を拡大し，ゾーン C に対しても標準でサポートできるように設計した．ファイアウォールのポリシーは IPv4 に準拠する形で定義している．運用については，段階的試行を経て全学展開を計画している．

3.4 個別ファイアウォールに接続可能な VPN サービスの提供

3.1 節で述べた通り，HINET2014 では 2,000 存在するゾーン C に対して個別のファイアウォール機能と DHCP 機能を提供し，原則として同一ゾーン C 内での通信は一切許可しないポリシーで運用を行っている．つまり，ゾーン C 内のプリンタや NAS といった機器に対してキャンパス内 Wi-Fi 環境からであってもアクセスすることはできず，それを実現にするためには対象機器をゾーン B エリアに設置するしか方法がなかった．今回，この課題を改善するために，個別ファイアウォールに対して接続可能な VPN を新たに提供し，ユーザ単位で任意のゾーン C と通信できるように設計した．

同様の機能を実現するためには，動的 VLAN を導入しフロアスイッチに対してユーザ ID に応じた VLANID を動的に設定する方法も考えられる [6] が，エッジスイッチでの VLAN 切替動作の安定性やブロードキャストドメインの範囲拡大など課題も多い．本手法では，従来の HINET における固定 VLAN での運用を変えることなく，必要に応じて VPN 接続を利用することで，学内外に問わず柔軟



VLAN	グローバルIPv4アドレス	ローカルIPv4アドレス	VPN IPv4アドレス	IPv6アドレス	VPN IPv6アドレス
2000	133.41.74.8	10.20.00.0/23	10.40.00.0/24	2001:2f8:1c1:800::/64	2001:2f8:1c1:1800::/64
2002	133.41.74.10	10.20.02.0/23	10.40.02.0/24	2001:2f8:1c1:802::/64	2001:2f8:1c1:1802::/64
2004	133.41.74.12	10.20.04.0/23	10.40.04.0/24	2001:2f8:1c1:804::/64	2001:2f8:1c1:1804::/64
2006	133.41.74.14	10.20.06.0/23	10.40.06.0/24	2001:2f8:1c1:806::/64	2001:2f8:1c1:1806::/64
2008	133.41.74.16	10.20.08.0/24	10.40.08.0/24	2001:2f8:1c1:808::/64	2001:2f8:1c1:1808::/64
2009	133.41.74.17	10.20.09.0/24	10.40.09.0/24	2001:2f8:1c1:809::/64	2001:2f8:1c1:1809::/64
2010	133.41.74.18	10.20.10.0/24	10.40.10.0/24	2001:2f8:1c1:80a::/64	2001:2f8:1c1:180a::/64
:	:	:	:	:	:
3950	133.41.95.200	10.39.50.0/24	10.59.50.0/24	2001:2f8:1c1:f9e::/64	2001:2f8:1c1:1f9e::/64
:	:	:	:	:	:
3999	133.41.95.227	10.39.99.0/24	10.59.99.0/24	2001:2f8:1c1:fcf::/64	2001:2f8:1c1:1fcf::/64

図 5　VPN 接続可能な個別ファイアウォールのアドレス設計

な接続を実現した．

具体的な VPN サービスは以下の 2 種類を提供する．

全学 VPN　学内 L3 スイッチに接続されるセグメントであり，全学ファイアウォールのネットワークにもアクセス可能．ゾーン C へはアクセス不可．

ゾーン C VPN　部局 L3 スイッチと接続されるセグメントであり，全学ファイアウォールのネットワークに加えて予め指定された特定のゾーン C のみと通信可．その他のゾーン C へはアクセス不可．

全学 VPN は全てのユーザが同じセグメントに接続されるのに対し，ゾーン C VPN はユーザ毎に接続されるセグメントが異なり，通信できるゾーン C も限定される．なお，プロトコルとしては SSL-VPN と L2TP/IPsec をサポートするが，ゾーン C VPN を実現するためには SSL-VPN での接続が必須となっている．

VPN 接続を考慮したゾーン C のアドレス設計を図 5 に示す．ユーザ単位で任意のゾーン C と接続させるために，予め VPN 装置側にゾーン C とは独立した 2,000 のアドレスプールを設定し，各アドレスプール毎に通信許可するゾーン C を 1 対 1 で定義する ACL を部局 L3 スイッチに設定している．この設定に加え，VPN 装置でのユーザ認証を行う際に特定のユーザ属性を参照させることで，IP アドレスを払い出すアドレスプールを制御する．これにより，ユーザ単位で接続できるゾーン C を制御することが可能となる．なお，VPN 端末に対してゾーン C のネットワークを直接提供する構成も考えられるが，ブロードキャストドメイン拡大による端末への影響が懸念される点や VPN

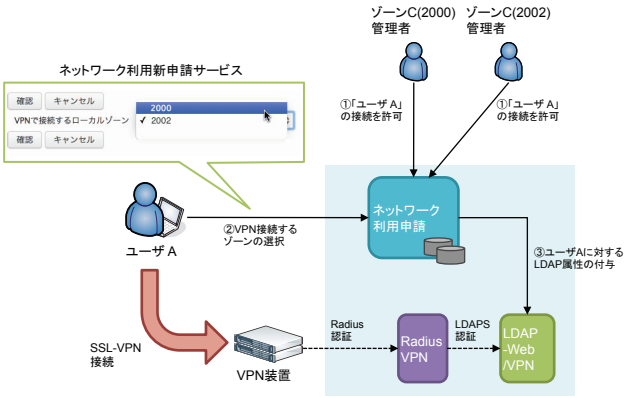


図 6　ゾーン C VPN の設定手順

装置に対して 2,000 の VLAN 設定が必要になるなど，総合的に検討したうえで本方式を採用した．

Radius 属性の設定には，ネットワーク利用の各種申請を担うネットワーク利用申請サービスを利用する．図 6 に申請サービスを利用した VPN の設定手順について示す．

具体的な手順は以下の通りである．各ゾーン C の管理者が，該当ゾーン C に対して接続を許可するユーザを予め登録しておく．VPN 接続するユーザは自身の ID で申請サービスにログインすることで，許可されたゾーン C のリストからどのゾーンと通信するかを設定することができる．ゾーン C を選択すると，対応する属性値がユーザの属性として追加される．いずれのゾーン C も選択しない場合は，全学 VPN へ接続されることとなる．よって同一の接続先 FQDN で，全学 VPN とゾーン C VPN を切り替えることができるようになっている．

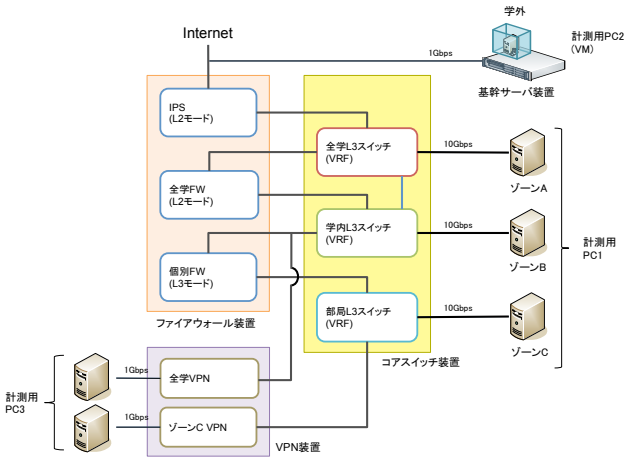


図 7 実験構成図

3.5 L2VLAN サービスによる商用クラウドの活用

HINET では，建物間やキャンパス間などで閉域接続を可能にする L2VLAN サービスも提供している．このサービスを活用し，多地点の情報コンセント間で L2 ネットワークを構築することで，セキュアかつ高速なデータ転送等が可能になっている．HINET2014 では，L2VPN を利用した SINET4/JGN-X 等の実験プロジェクト接続や商用クラウドサービスの利用を促進するために，柔軟な L2 サービスを提供できるような構成とした．これにより，各研究室の情報コンセントまで L2VLAN で外部ネットワークと直結することが可能となっている．なお，L2VLAN サービスの利用には部局等からの申請が必要であり，接続する機器は MAC 認証を必須としている．

本サービスによる SINET クラウドサービスと研究室との直接接続は既に利用されている．SINET4 との広島大学との接続点は 10Gbps，各キャンパス集約スイッチの下流は 1Gbps であるが，ファイアウォール装置などを経由することなく通信することが可能となっている．また，L3VPN によりクラウドサービスに接続する場合には MTU サイズ問題が発生するが，本サービスで接続した場合その問題は発生しない．

なお，利用者の申請に基づき学内の任意の情報コンセントへ L2VLAN を設定するサービスは 2008 年以来実施中であり，SINET クラウドサービスとの接続も通常の運用の一環として実施している点に特徴がある．

4. 基幹ネットワーク性能評価

基幹ネットワーク装置では，ファイアウォール装置で 2,000 の NAPT 機能や IPS 機能を提供し，部局 L3 スイッチでもゾーン C 間・VPN 装置との通信を制御するための ACL やポリシールーティングの設定を行っている．本章では，これらの設定通信に与える影響を見積もるために実施したスループット計測について述べる．

表 3 測定に利用した機器諸元

	計測用 PC1	計測用 PC2 (VM)	計測用 PC3
CPU	Intel Core i7 3.4GHz	QEMU vCPU 3.0GHz	Intel Core i7 3.4GHz
メモリ	16GB	1GB	16GB
NIC	10G-SR	1000Base-T (vNIC)	1000Base-T
OS	CentOS 7.0	CentOS 6.5	

4.1 計測環境

図 7 に実験構成図を示し，表 3 に測定に使用した機器諸元を示す．図では記載を省略しているが，計測用 PC1 は東広島キャンパス集約スイッチ直下に 10G-SR インタフェースで接続し，コアスイッチ装置を経由する場合は東広島〜データセンター間の往復通信が発生している．また，計測用 PC2 は基幹サーバ装置内に VM として準備した．したがって，ネットワーク帯域が 1Gbps かつ基幹サービス用の VM が動作している状態であることに注意が必要である．計測用 PC3 も東広島キャンパス集約スイッチ直下に 1000base-T インタフェースで接続し，学内ゾーン D エリアから VPN 装置に SSL-VPN 接続している．

測定には iperf[*2]を用いて，TCP シングルセッションと 16 同時セッションの 2 パターン (IPv4 通信, IPv6 通信) についてそれぞれ 60 秒間の測定結果を基準値としている．

4.2 ゾーン間スループット計測

まずゾーン間のスループット計測を行うため，PC1 と PC2 を利用した計測を行った．表 4 に IPv4 通信の計測結果，表 5 に IPv6 通信の計測結果を示す．本測定は HINET2014 運用開始前に計測した結果である．なお，表中の”—” はファイアウォールによりアクセス制限が行われているケースである．

これらの結果より，ファイアウォールを経由しない L3 通信については，IPv4, IPv6 ともに良好な結果が得られていることが分かる．セッション数を増やすことで，スループットが向上し，インタフェースの限界値である 10Gbps に近いスループット結果が出ている．

一方で，ファイアウォールを経由する場合は，IPv4 については同時セッション数を増やすことで L3 通信の結果に近い値が得られたものの，IPv6 については期待するパフォーマンスが得られなかった．16 セッション同時の場合であっても，最大で 2Gbps 程度となっているため，設定および機器性能の両観点から確認を行っている．なお，IPv4 と IPv6 のトラフィックを同時に発生させた場合，IPv4 の通信性能劣化は発生しないことは確認している．

4.3 VPN 接続時のスループット計測

次に VPN 接続時のスループット計測について示す．計測では PC1 と PC3 を利用した．PC3 で全学もしくはゾー

*2 https://iperf.fr

表 4 ゾーン間 IPv4 スループット性能 (X → Y 方向) (単位: Gbps)

X \ Y	ゾーン A	ゾーン B	ゾーン C	学外
ゾーン A	8.15 / 9.30	-	-	0.65 / 0.94
ゾーン B	2.43 / 9.30	9.35 / 9.33	-	0.65 / 0.94
ゾーン C	2.58 / 9.24	2.54 / 9.16	-	0.65 / 0.94
学外	0.65 / 0.93	-	-	-

(1 セッション/16 セッション合計)

表 5 ゾーン間 IPv6 スループット性能 (X → Y 方向) (単位: Gbps)

X \ Y	ゾーン A	ゾーン B	ゾーン C	学外
ゾーン A	8.06 / 9.10	-	-	0.65 / 0.93
ゾーン B	2.01 / 1.91	9.22 / 9.20	-	0.65 / 0.63
ゾーン C	1.80 / 1.81	0.82 / 0.84	-	0.65 / 0.59
学外	0.65 / 0.92	-	-	-

(1 セッション/16 セッション合計)

ン C VPN に接続した状態で，ゾーン B とゾーン C のサーバに対してトラフィックを発生させることで測定した．なお，全学 VPN 接続時はゾーン C への接続は不可であるため，計測は行っていない．

表 6 に計測結果を示す．本結果は HINET2014 運用開始後に計測したものである．比較のために，VPN 未接続の PC3(ゾーン D) から PC1(ゾーン B) に対する計測結果も示す．なお，測定ではセッション数による違いは見られなかったため，本稿ではシングルセッションの測定結果のみを掲載している．

この結果より，VPN 接続では 240Mbps 程度のスループットとなっていることが分かる．これは，クライアント端末 (PC3) におけるソフトウェア処理負荷に起因している部分が非常に大きいと考えられる．実際に，VPN 接続を行いながら iperf を実行すると CPU 負荷率が 100%となっていた．今回のクライアント端末での計測では，IPv4 と IPv6 で結果に差異はなく，IPv6 でも IPv4 と遜色のないの性能が得られていることがわかる．

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 について述べた．特に，従来より提供する各教員の個別ファイアウォールに学内外から接続を可能とする VPN サービス，研究室と商用クラウドサービスを直結する L2VLAN サービスなど，柔軟かつ高度なキャンパスネットワークを実現する機能を中心に紹介した．

HINET2014 で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，ゾーニングによりネットワークの単位を各研究室や各教員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．3.5 節で示したように，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できる構成となっており，ゾーニングの単位で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となる．

表 6 VPN スループット性能（X → Y 方向) (単位: Mbps)

X \ Y	ゾーン B		ゾーン C	
	IPv4	IPv6	IPv4	IPv6
全学 VPN	245.0	240.3	-	-
ゾーン C VPN	242.3	240.3	242.0	240.7
VPN なし (ゾーン D)	934.0	921.3	-	-

基幹ネットワークにおける個別ファイアウォールおよび VPN サービスについて，運用状態におけるスループット性能測定を行い，本方式が性能に与える影響を定量的に示した．その結果，IPv4 では性能低下を起こすことなく実現できることが分かった．IPv6 通信については，実用上大きな問題にはならないと考えられるものの，IPv4 との差異の原因を調査中である．

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．今後は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今後活用していく予定である．

謝辞 本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の関係者に感謝致します．

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.

[3] 田島浩一, 岸場清悟, 近堂徹, 大東俊博, 岩田則和, 西村浩二, 相原玲二, ”広島大学におけるセキュリティ脆弱性診断の実施とその評価”, 学術情報処理研究, No.18, pp.16-23, 2014.

[4] 相原玲二, 西村浩二, 近堂徹, 岸場清悟, 田島浩一, ”全教員に個別ファイアウォール機能を提供するキャンパスネットワークの構築”, 情報処理学会研究報告 2008-IOT-2 (6), pp.29-34, 2008.

[5] 大東俊博, 近堂徹, 岸場清悟, 田島浩一, 岩田則和, 西村浩二, 相原玲二, ”広島大学における新キャンパスネットワークへの移行手法”, 情報処理学会研究報告 2008-IOT-3 (6), pp.31-36, 2008.

[6] 山井成良, 岡山聖彦, 大隅淑弘, 藤原崇起, 河野圭太, 稗田隆, ”岡山大学における大規模認証ネットワークの運用と課題”, 情報処理学会研究報告 2013-IOT-20(10), pp.1-6, 2013.