

## 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

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

広島大学情報メディア教育研究センター

**あらまし** 2008 年度より使用開始した広島大学の新キャンパスネットワークは、それまでのサブネット管理方式をやめ、移行時には原則として IP アドレスが変更となる。そのため、約 1 年間の移行期間を設け、利用者の都合に合わせて随時移行を可能とした。新ネットワークでは、利用者に割り当てた約 2000 の VLAN を、新フロアスイッチの約 14000 ポートへ順次設定する必要がある。本稿では、移行支援体制の構築および新たに設計した申請処理ツールなど、移行の技術的手法について述べる。

## A Technical Method for Shifting Campus Network at Hiroshima University

Toshihiro OHIGASHI Tohru KONDO Seigo KISHIBA Koichi TASHIMA  
Norikazu IWATA Kouji NISHIMURA Reiji AIBARA

Information Media Center, Hiroshima University

**Abstract** A new campus network system opening at FY2008 in Hiroshima University has adopted the uniform management of the network. In the new campus network system, about 2,000 VLANs are assigned to users, and a processing that sets the VLANs to each port is required for 14,000 ports of a new floor switch. A transitional period for the campus network is one year. In this paper, we demonstrate a technical method for shifting campus network.

### 1 まえがき

2008 年度より広島大学では、それまでの部局単位で運用されるサブネット管理方式をやめ、全学的な一元管理方式の新キャンパスネットワーク HINET2007[1][2] の運用を開始した。HINET2007 では教員数程度 (約 2,000) の独立したファイアウォール機能を提供し[3]、それを割り当てられた教員は VLAN 機能を使用し希望する場所で内部ネットワークを構成できる。異なる建物や地区でも同一 VLAN、すなわち同一ファイアウォール配下に収容できるため、遠隔地にある同一研究室などでの利便性が向上する。さらに、ネットワークに接続する機器または利用者の全

てに対して認証を要求するため、セキュリティの保証された利用環境が実現できる。

HINET2007 への移行では、新たに設置したフロアスイッチの約 14,000 ポートへ利用者の VLAN を順次設定する必要がある。さらに、MAC アドレス認証で接続する機器を VLAN 毎に事前に登録する必要もある。設定後には旧ネットワーク (HINET2001) のフロアスイッチから HINET2007 フロアスイッチへの LAN 配線の接続変更などの作業が生じるなど、移行における作業は膨大である。本稿では、HINET2007 への移行に係わる申請受付および支援体制の構築、申請処理ツールなど、移行の技術的手法について述べる。

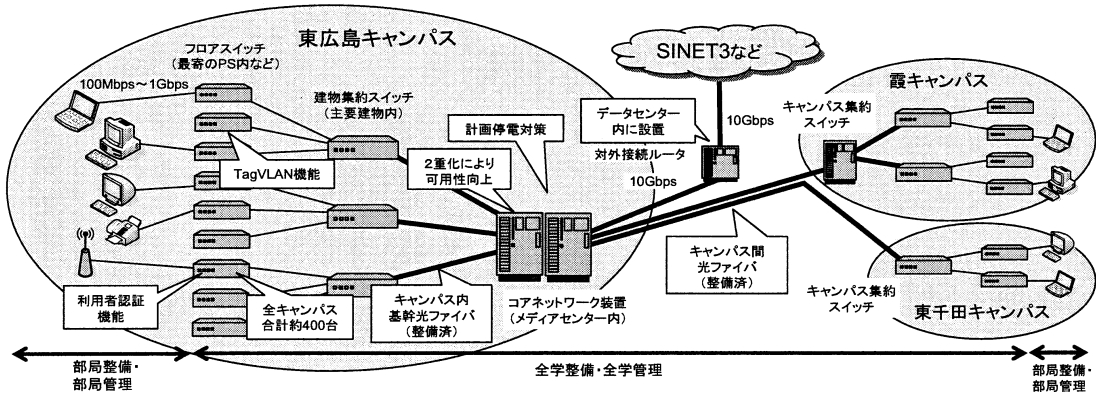


図1. HINET2007の概要図

## 2 HINET2007 概要

### 2.1 全学的な一元管理

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、霞、東千田)および附属学校、呉・竹原などの小規模遠隔部局に整備されている。HINET2007 では図 1 のように全キャンパスに合計約 40 台の建物集約スイッチおよび約 400 台のフロアスイッチを整備し、基幹ネットワークからフロアスイッチの各ポートまでを全学で管理している。フロアスイッチから各部屋へのフロア配線は部局が整備および管理を担当する。

HINET2007 ではフロアスイッチのポートまでを管理するため、全フロアスイッチの全ポートに対してコネクタ ID と呼ぶ識別番号を図 2 のように割り当てている。コネクタ ID はフロアスイッチに割り当てられたスイッチ ID とポート番号の連結によって表現されている。スイッチ ID はフロアスイッチの物理的な位置情報から決められることから、不具合が生じた際コネクタ ID を基に問題があるフロアスイッチの位置を即座に把握でき、迅速な対応が可能となる。

### 2.2 ゾーン構成

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って区別される「ゾーン」という概念を導入した。ゾーンのアクセス制限は VLAN 毎に設定可能な個別ファイアウォール機能[3]および全学ファイアウォールによって実現している。個別ファイアウォール機能の実現方法については文献[3]で詳細な説明をしている。主要なゾーンは表 1 に示される 4 種類であり、

#### ●スイッチID

地区-建物番号-階-スイッチ通番

#### ●コネクタID (物理コネクタID)

地区-建物番号-階-スイッチ通番-ポート番号

コネクタID  
 例) 1-012-02-1-09  
 スイッチID

図2. コネクタIDの構成

利用者はこれらのゾーンに対応する VLAN を割り当てられる。さらに、コネクタ ID に対応するポートに VLAN ID を設定することによってゾーンに対応するネットワークを利用できる。正確には、コアネットワーク装置から該当するフロアスイッチまでのスイッチの設定を行う必要がある。また、利用者は該当ポートの Tag または Untag 設定が選択できるため、一つのコネクタ ID に対して複数の VLAN の設定を対応させることも可能となっている。

主要 4 ゾーンのうちゾーン A および B は固定のグローバル IP アドレスと対応する FQDN を情報メディア教育研究メディアセンター (以後、メディアセンターと呼ぶ) から機械的に割り当てられる。利用者は独自に運営している DNS サーバを利用することによって、独自の FQDN をゾーン A または B のホストに設定することができる。このような場合に DNS の逆引き設定を独自の

表 1. HINET2007 で提供する主要ゾーン種別

ゾーン名 略称	グローバルゾーン ゾーン A	ファイアウォールゾーン ゾーン B	ローカルゾーン ゾーン C	公衆ゾーン ゾーン D
主な用途	学外向けサーバ接続	学内共有サーバ接続	一般クライアント接続	オープンスペース
外部 IP アドレス	グローバル 固定割当	グローバル 固定割当	グローバル 固定割当	グローバル DHCP 割当
内部 IP アドレス	外部 IP アドレスと同じ	外部 IP アドレスと同じ	プライベート(NAPT) DHCP または固定割当	外部 IP アドレスと同じ
学外へのアクセス	制限なし	制限なし	原則制限なし (NAPT による制限あり)	制限なし
端末認証	MAC アドレス認証	MAC アドレス認証	Web 認証または MAC アドレス認証	Web 認証
VLAN ID	1600～1699	1700～1799	2000～3999	1800～1899

FQDN に変更するサービスを提供している。また、DHCP サーバ機能によってゾーン C のプライベート IP アドレスおよびゾーン D のグローバル IP アドレスは自動で割り当てられる。

### 2.3 利用者認証

HINET2007 ではセキュリティを確保するため、どのゾーンに接続する場合でも利用者には何らかの認証を要求する。具体的には、Web 認証または MAC アドレス認証のいずれかが適用される。Web 認証では、外部 Web ページを閲覧時に、https 接続のみ許可した認証ページにリダイレクトされる。広島大学全学電子認証システム[4]の LDAP サーバに登録されている ID とパスワードを Web ブラウザに入力されたものと照合することで利用者を認証する。MAC アドレス認証は、事前に LDAP サーバへ登録されている MAC アドレスを持つ機器に対して Web 認証なしで接続を許可する方法である。これは原則としてプリンタなどブラウザ機能を持たない機器を対象にしている。

## 3 ネットワーク移行の方針

HINET2007 への移行時には原則として IP アドレスの変更作業が生じるため、約 1 年間の移行期間を設け、利用者の都合に応じて移行時期を決定できるようにしている。そのため、1 年間は旧ネットワーク HINET2001 と HINET2007 のフロアスイッチを並行運用し、HINET2007 のフロアスイッチのポートへ VLAN ID の設定が完了した利用者から順次 LAN 配線を差し替えることで移行できるようにした。これにより、利用者の都合が良い時間に移行できる。さらに、もし何らかの設

定上の不具合が生じた場合に HINET2001 へ配線に戻すことで不具合が解消するまでの間も継続してネットワークを利用できるという利点もある。

現在、広島大学には教員約 1,800 人、職員約 3,300 人、学生 15,000 人（附属学校の児童、生徒約 4,000 人は含まない）の構成員が存在する。HINET2007 ではゾーンの概念など、それまでのサブネット管理方式と大幅に異なるため、キャンパスネットワークの機能や移行手順、使用方法などを周知することが重要となる。そこで、Web で公開している情報ページ[2]に移行手順や技術情報を掲載、移行手順についての説明会を全学または部局毎に開催するなどして周知を図っている。

### 3.1 登録システム

HINET2007 への移行では、各部屋の情報コンセントへコネクタ ID を割り当てる「コネクタ ID 申請」とゾーンに対応する VLAN ID の取得およびコネクタ ID に対応するポートへの設定を行う「ゾーン申請」をすることになる。これらの申請を受付・管理するために、HINET2007 では Web インタフェースによる HINET2007 登録システム（以下、登録システム）を設計し、導入している。このシステムは申請者を広島大学全学電子認証システムの ID とパスワードによって認証し、ゾーン申請および MAC アドレス認証用の機器の登録をできる。ゾーン申請時に管理者および副管理者（最大 2 名）の ID を登録し、その後の登録内容の修正を許可する。

登録システムでは、ゾーン申請時に VLAN ID や IP アドレスなど設定情報が自動割当され、コ

ネクタ ID への設定依頼が自動的に送られる。膨大な移行関連作業を軽減するために、コネクタ ID に対応するポートへの VLAN 設定は契約している業者（設定業者）へアウトソーシングしている。特に煩雑な作業になる MAC アドレスの登録・削除は、登録システムを使って即座に行えるようにしている。登録システムではコネクタ ID を登録する機能もあるが、フロアスイッチの残ポート数の把握などの理由で、原則として部局単位のコネクタ ID 申請を受けてメディアセンターの教職員が入力することとした。

### 3.2 初期移行受付・支援体制

移行初期において、それまでのサブネット管理で運用された様々なネットワーク構成から、多数の例外処理が生じると予想された。上記の登録システムでは全ての例外処理に対応できるとは限らないため、自動受付の登録システムを運用するリスクを避け、人手による申請受付から開始することにした。手動での受付によって得られた課題および知見は登録システムにフィードバックされ、HINET2007 の安定運用時に活用される。手動での受付の詳細は 4. で述べる。

HINET2007 への移行では部局ごとに移行計画部局責任者を設置し、移行に関する部局内での取りまとめを担当してもらっている。具体的には、部局管理であるフロアスイッチから各部屋へのフロア配線の把握、コネクタ ID 申請などの部局単位の申請、ゾーンの概念や移行手順の構成員への周知（説明会の開催依頼を含む）などを担当し、メディアセンターと連携して円滑な移行を実現する。

ゾーン申請による設定が完了した際、HINET2001 から HINET2007 への LAN 配線の差し替えおよび IP アドレスの変更などの移行作業が生じる。これら移行作業は原則として申請者本人が行う方針であるが、申請者から要請があった場合には技術センター<sup>1</sup>およびメディアセンターのスタッフによる支援を行える体制を構築している。

## 4 受付処理の実際

3.1 で述べたように、HINET2007 では人手による受付処理から開始している。受付処理は日替わ

<sup>1</sup> 技術センターは全ての技術職員が所属し、技術的支援業務を全学的に行う組織である。

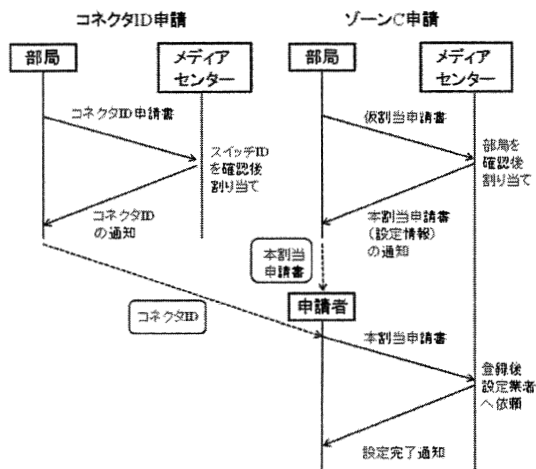


図3. コネクタID申請とゾーンC申請

りの担当制にし、メディアセンター教員 5 名が担当している。また、コネクタ ID 申請およびゾーン申請は、事務手続きにおいて広く普及している Microsoft 社の Excel によって作成した申請書を使って行う。申請書はメールで受け付けることとし、申請メール毎に付加されるメーリングリスト (ML)番号で申請を管理をする。

申請書および申請内容を把握するための台帳 (Excel で作成) は WebDAV[5]を利用して共有し、受付処理担当者が遠隔地にいる場合でも認証をすれば処理が可能のようにしている。さらに処理の漏れを防ぐために、進捗管理ファイルを用意し、ML 番号毎に処理の状態 (処理前、設定中、設定済など) および担当者名を記入するようにしている。

### 4.1 処理手順概要

HINET2007 の申請はコネクタ ID 申請によりコネクタ ID を取得し、そのコネクタ ID に対してゾーン申請をする手順になる (ゾーン C 仮割当申請は除く)。それぞれの処理では、2 名以上の担当者のチェックを受けた上で進める方針にし、記入ミスを見落としに備えている。以下にそれぞれの申請の処理手順の概要を示す。

#### コネクタ ID 申請

部屋にある情報コンセントにコネクタ ID を対応付けるための申請であり、部局単位でとりまとめて申請する。図 3 にコネクタ ID 申請の処理の流れを示す。申請書では情報コンセント毎に地区、建物番号、階、部屋番号などの情報と接続予定ス

スイッチの ID を記入する。受付処理担当者は記入されたスイッチ ID と地区などの情報を照合して、記入ミスがないことを確認した上でフロアスイッチの空きポートから順次割り当てていく。対応するコネクタ ID を記入されたファイルを部局へ送付し割当が完了する。

### ゾーン C 申請

ゾーン C の申請は仮割当申請と本割当申請から構成されている。図 3 はコネクタ ID の割当を含めたゾーン C 申請の処理の流れを示している。仮割当申請は部局単位でとりまとめて受け付ける。仮割当申請書に記入された教員のそれぞれについて、VLAN ID や IP アドレスなどの設定情報を記入した本割当申請書を作成する。最後に、本割当申請書を送付し仮割当申請を完了する。割り当てるゾーン C の外向きの IP アドレスの連続性を確保するため、部局毎にある程度のまとまった単位で IP アドレスを確保しておき、それらを順次割り当てる方針にしている。これは電子ジャーナルなど IP アドレスによるアクセス制限を利用したサービスを意識したものである。

本割当申請は利用者単位で受け付け、本割当申請書に記載された情報を利用してゾーン C のコネクタへの設定および MAC 認証用のアドレスの登録を行う。具体的には、申請書にはゾーン C を利用する全ての情報コンセントのコネクタ ID、各コネクタ ID の Tag または Untag の選択、MAC アドレス認証をする機器の情報が記載される。

### ゾーン AB 申請

ゾーン A またはゾーン B の申請はホスト単位（利用者単位）で受け付ける。ゾーン AB 申請の処理は図 3 のゾーン C の本割当申請に対応する。申請書には設定する情報コンセントのコネクタ ID、各コネクタ ID の Tag または Untag の選択、登録ホストの MAC アドレスなどが記載される。受付処理担当者は VLAN ID や IP アドレス、FQDN の情報を申請書に記入し、設定業者へ設定を依頼した上で申請者を送付する。もし、独自の FQDN を利用するために DNS の逆引き登録を希望する場合は、メディアセンター側で DNS の逆引きの変更を行う。

### ゾーン D 申請

ゾーン D の申請は部局単位で受け付ける。ゾーン D 申請の処理は図 3 のゾーン C の本割当申請に対応する。Web 認証のみサポートしておりホ

ストの登録は生じないため、ゾーン D 申請書には設定する情報コンセントのコネクタ ID、各コネクタ ID の Tag または Untag の選択の情報が記載される。受付処理担当者は VLAN ID の情報を申請書に記入し、設定業者へ設定を依頼した上で申請者を送付する。

## 4.2 受付処理支援ツール

4.1 で説明した受付処理及び関連する設定の負荷を軽減するため、登録装置とは別に受付処理を支援するツールを作成した。

### ゾーン C 本申請書生成ツール

ゾーン C の仮割当情報からゾーン C 本割当申請書を VLAN ID 別に作成できる Excel のマクロを作成している。ゾーン C の本割当申請書は、VLAN ID によって異なる IP アドレスなどの設定情報を記入した上で、VLAN ID に対応するファイル名へリネームする必要がある。この作業を手動で行う際には膨大な時間を費やし、ミスが混入しやすい状況であったため、このツールを利用して改善した。

### ゾーン C 本申請登録支援ツール

部局単位で一斉に移行をする際、円滑な設定作業を行うためにゾーン C 本割当申請書を取りまとめて提出してもらっていた。この場合、多数の本割当申請書を処理する必要があり、人手では限界がある。そこで、多数の本割当申請書を一括で処理できる Excel のマクロを作成している。ただし、TagVLAN 機能の使用する場合に関しては、申請者の記入ミスが生じる可能性があるため、自動登録はせずに設定例のみ提示する。

### DNS 逆引き登録ツール

ゾーン A またはゾーン B 申請の際に生じる独自の FQDN へ DNS の逆引きを変更する作業を自動で行うツールである。HINET2007 ではゾーン A、B のホストについてあらかじめ FQDN の初期値を与え、DNS の順引きと逆引きの両方を登録している。本ツールでは、独自の FQDN を利用したい場合、DNS の順引きが変更されたことを確認してから逆引きの更新を行う。このようにすれば、DNS の逆引きと順引きが絶えず一致する状態になる。

### 申請情報解析ツール

WebDAV ではゾーン毎、コネクタの位置毎（キ

キャンパス単位)に申請情報を管理する台帳ファイルを共有している。申請情報解析ツールは、PerlのSpreadsheet::ParseExcelモジュールを利用し、全ての台帳をExcelファイルからcsvファイルへ変換する。csvファイルに変換することで他のプログラミング言語と連携が容易になり、移行状況の把握や必要な情報を検索することなどが容易になる。ここで生成したcsvファイルは登録システムへの入力としても利用される。

### 4.3 問題点

手動による受付処理を進めるにしたがって、申請書をExcelファイルにしたことによる問題が生じている。Excelファイルの申請書では入力内容の自動チェックが困難になり、受付処理担当者は全ての受付処理で申請者の記入ミスについて注意して確認する必要がある。また、申請書の改変が容易にできることも問題である。これらの問題、特に入力ミスに関しては、ミスのパターンを蓄積して登録システムにおける入力書式の自動チェックに役立てることができる。

HINET2007の移行日時について詳細な時間を調整しなければならないケースが生じた。通常HINET2001を並行運用していることから、HINET2007の移行ではポートの設定変更は特別に日時を指定する必要はなかった。しかしながら、本年度に建物の改修などでHINET2007のフロアスイッチを利用してHINET2001のネットワークへ接続している場合があり、このような場合は設定変更時にネットワークが一時的に寸断される。特に、設定変更に合わせてIPアドレスの変更が必要になるため、事前に設定変更時間の調整が必要になった。この際、設定業者と申請者の都合の調整が生じることから負担が大きい。もし、HINET2001との並行運用を行わなかったとしたら、全ての移行において同様の問題が生じることになる。これは、新旧ネットワークを並行運用した上での移行という方針が効果的に働いていることを意味している。これらの問題に対応するためには、登録システムもしくはそのサポートシステムにおいて詳細な移行時間までを申請者および設定業者間で調整できる機能を提供する必要がある。

## 5 むすび

本稿では、広島大学の新キャンパスネットワークHINET2007における移行技術について、移行

表 2. HINET2007 の移行状況

	4月	5月	6月	7月
申請メール受付数	28	126	100	140
コネクタID登録数	—	520	95	1215
コネクタID削除数	—	28	2	1
MACアドレス登録数	—	290	215	1044
MACアドレス削除数	—	8	11	16
ゾーンC割当数	76	322	56	36

支援体制や申請処理ツールなどを紹介した。2008年5月から本格的に開始されたネットワークの移行状況は、を表2のように7月までに1799ポートの設定が完了している。移行する教員数に対応するゾーンCは最大で2,000であるが、そのうち490が7月までに割り当てられている。今後も同程度以上のペースで移行が進めば、年度内に全ての移行が完了すると判断している。今後は、適切な時期に登録システムへ受付体制を移行し、その際の効率の向上について運用を通して検証していく。

### 謝辞

HINET2007の構築及び運用に尽力頂いている広島大学総務室情報化推進グループ、技術センターおよび情報メディア教育研究センターの関係者に感謝する。

### 参考文献

- [1] 相原, 西村, 岸場, 田島, 近堂: “利用者認証機能を持つ大規模キャンパスネットワークの構築”, 2008年電子情報通信学会総合大会 BS-8-7, pp.S-116-S-117, 2008年3月.
- [2] 広島大学情報メディア教育研究センター: “HINET 2007 情報”, <http://home.hiroshima-u.ac.jp/infra/hinet2007info/>.
- [3] 相原, 西村, 近堂, 岸場, 田島: “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”, 情処研究報告 2008-IOT-2, pp.29-34, 2008.
- [4] 相原: “広島大学における全学統合認証システムの構築と運用”, 統合認証シンポジウム, 佐賀大学, 2007年12月.
- [5] WebDAV Resources JP, <http://webdav.todo.gr.jp/>