サイエンティフィック・システム研究会
システム技術分科会 2008 年度第 2 回会合資料

2009 年 1 月 29 日

日本最大規模のキャンパス認証ネットワーク
～ HINET2007 の構築と運用 ～

広島大学情報メディア教育研究センター
西村 浩二,
相原 玲二, 近堂 徹, 大東 俊博,
田島 浩一, 岸場 清悟, 岩田 則和
kouji@hiroshima-u.ac.jp

[Abstract]
広島大学では平成20年度より新キャンパスネットワークHINET2007の運用を開始した。HINET2007では、全学約450 台のエッジスイッチが全学電子認証システムと連携してすべてのネットワーク利用者を認証するほか、全教員数に相当する約2,000 個の独立したファイアウォール機能を有するなど、安全かつ柔軟な環境を提供している。
本報告では、HINET2007の概要とその構築手法、それぞれの機能の性能評価の結果、移行を支援する体制やシステムについて述べる。

[Keyword]
利用者認証、仮想ネットワーク、アクセス制御、リナンバリング

1 はじめに

大学などの高等教育研究機関では、さまざまな教育研究を実施するために高度かつ柔軟なネットワークが求められる。大規模な組織では、学部や学科などの部局単位でサブネットを構成し、サブネット内の管理運用は当該組織が責任を持つことを条件に、自由度の高い運用を許してきた経緯がある。しかし、ネットワークがライフライン化するにつれ、インターネット上で発生するセキュリティの問題も複雑化していることから、大幅な管理方針の見直しが迫られている。

このような背景のもと、広島大学では平成19年度からセキュアでスケーラブルなキャンパスネットワークHINET2007の構築を開始し、平成20年5月から運用を開始した[1]。HINET2007では、これまでの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移行するとともに、利用形態により分類される「ゾーン」という概念を導入し、それぞれの目的に応じた学内外からのアクセス制御を提供する。さらに、すべてのネットワーク接続点(ポート)において接続機器の利用者を特定するための認証を行うことで、セキュリティレベルの底上げ、維持を図っている。またこれらの運用管理を支援するための体制作りやシステムの開発を行っている。

本稿では、HINET2007 の概要と運用・移行の方針、設計・構築のポイント、移行の支援体制とシステムについて述べる。

2 HINET2007 の概要

今回構築したHINET2007の概要を図1に示す。主な特徴は以下のとおりである[2]。

(1) 全学的な一元管理体制
これまでのサブネット管理は多くがボランティアにより行われていた。その結果、サブネットにおいて発生したセキュリティの問題に対する責任の所在があいまいになったり、サブネットによって対応に違いが生じたりする原因となった。HINET2007 では全学的な一元管理体制をとるため、建物集約スイッチやフロアスイッチの全ポートを管理対象とし、各部屋の情報コンセントへの接続状況を把握できるようにしている。

(2) VLAN による柔軟な仮想配線の提供
柔軟な組織体制で教育研究が行われる場合、同一の組織や研究グループが必ずしも同一の建物内や

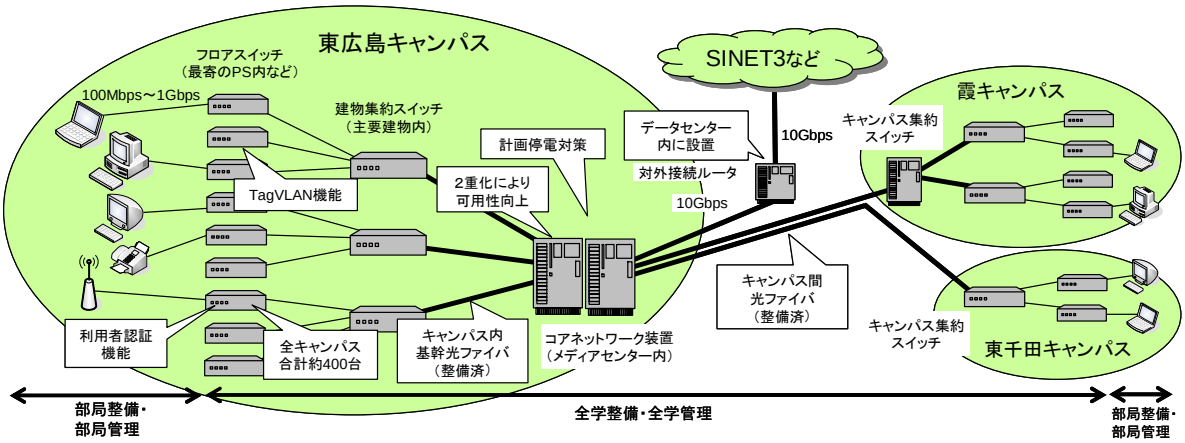


図 1　HINET2007 概要図

フロア内に分布しているとは限らない。HINET2007 では IEEE802.1q(Tag VLAN)を従来以上に積極的に活用し、地理的条件の影響を受けないネットワーク構築を可能としている。

(3) 個別ファイアウォール機能の提供

外部からのセキュリティの脅威からネットワーク機器を保護するため、研究室にファイアウォール機能を持つ機器(ブロードバンドルータなどを含む)を設置するケースが多く見られた。しかし、複数の建物に部屋が分散している場合は機器間を VPN で接続するなど、設定や管理が煩雑であるという問題もあった。そこで HINET2007 では、約 2,000 個の個別ファイアウォールをネットワークの機能として提供している。

(4) すべての接続場所において利用者認証を要求

これまでサブネット管理者が行ってきた接続機器の管理を全学的な一元管理とするため、約 450 台のすべての建物集約スイッチとフロアスイッチに利用者認証機能を持たせ、ネットワークの利用に際して何らかの認証が要求されるようにしている。

3　管理・運用・移行の方針

3.1　ゾーン構成とアクセス制御

先に述べたように、HINET2007 では各部局等のセキュリティレベルの底上げと均一化を図るため、これまでのサブネット単位に分散した独自管理から全学的な一元管理へと大きく運用方針を転換した。これにともなって、利用形態により学内外からのアクセスの可否パターンで区別される「ゾーン」という概念を導入した。主要なゾーンは表 1 に示す 4 種類である。またこれらのゾーン間および外部ネットワーク(インターネット)間のアクセス制御の概要を図 2 に示す。IEEE802.1q を利用することで、ゾーンは基本的にキャンパスや建物、フロアなどの地理的条件に影響を受けることなく、自由に構成することができる。

表 1　HINET2007 が提供するゾーン種別

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
ゾーン外からの アクセス	学内外とも制限なし	学外から不可 ゾーンAを除く学内から可	同一ローカルゾーン以外 から不可	学外から不可 ゾーンAを除く学内から可
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

3.2　運用方針

表 1 に示すように、HINET2007 では原則としてすべての接続端末に認証が求められる。認証方式は Web 認証と MAC アドレス認証のいずれかで、ゾーンによって利用できる認証方式は異なっている。Web 認証はネットワークを利用する都度 Web ブラウザを使用して利用者認証を行うが、MAC アドレス認証を行うには事前に利用者と被認証機器の MAC アドレスの対応を申請しておく必要がある。また図 2 におけるローカルゾーン(ゾーン C)では、約 2,000 個の個別ファイアウォール機能を提供している。基幹スイッチ等の設定はあらかじめ行っておき、利用者の申請に応じてフロアスイッチ等の VLAN 設定を変更することで、希望する場所で個別ファイアウォール機能が利用できるようにしている。ただし、ファイアウォールのポリシー設定については以下のような運用方針を定めている。

- 個別ファイアウォールの例外設定(特定ポートへのアクセス許可など)は受け付けない。
- 個別ファイアウォールのローカル側／グローバル側アドレスの希望は受け付けない(情報メディア教育研究センター(以下、メディアセンター)が指定)。
- 希望すればフロアスイッチの下流ポートへ Tagged で接続ができるが、VLAN ID の希望は受け付けない(メディアセンターが指定)。

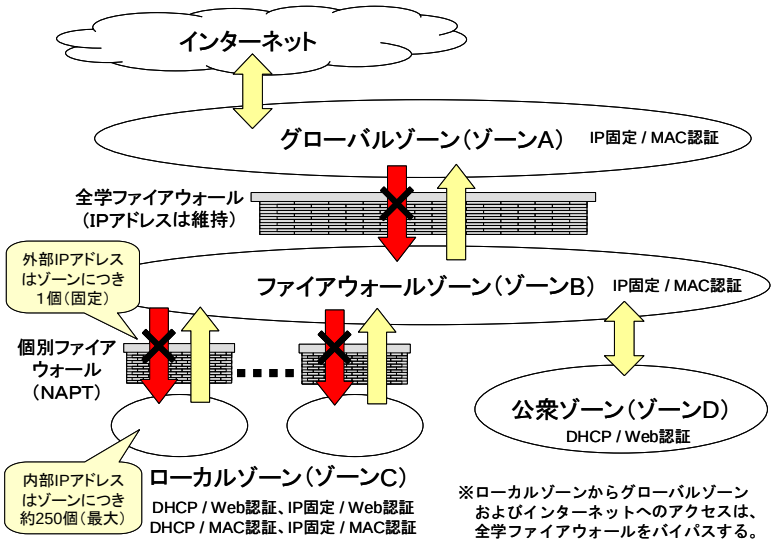


図 2　ゾーン間のアクセス制御

3.2　運用方針

HINET2007 はこれまでのキャンパスネットワークに比べて、全端末の IP アドレスのリナンバリングが必要である、ネットワークの利用に先立って認証が必要であるなど、運用方法が大幅に異なるため、全学が一括して移行することは困難であると判断した。そのため、既存の HINET2001 との並行運用期間を定めた上で、その期間内で利用者が研究科や専攻、研究室の単位で移行時期を決定できるようにした。並行運用の期限は 2008 年度末としており、2009 年 3 月末に HINET2001 を停止する予定である。

具体的な移行作業は、フロアスイッチ等の設定変更とフロア配線の差し替えである。フロアスイッチ等の設定変更にはコネクタの指定を受けるための申請、ゾーンの指定を受けるための申請、そしてコネクタとゾーンとを関連づけるための申請の 3 つのステップが必要であるが、手続きの詳細については MAC アドレスの登録を含めて後述する。フロア配線の差し替えについては、ほとんどの場合はフロア内の最寄りのパイプスペースに新旧のスイッチが設置されているため、すべての申請が完了した後、利用者の都合がよいときに旧スイッチから新スイッチへ配線を差し替える。その後その配線に接続されている機器の IP アドレスを変更し、接続テスト(認証テスト)が完了すれば移行が完了となる。

4　設計・構築のポイント

本節では、HINET2007 を設計・構築する際に特に考慮した事項について概要を述べる。個々の事項の詳細については、それぞれで引用されている文献を参照されたい。

4.1　個別ファイアウォール機能の実現

HINET2007 のコアネットワーク装置周辺の構成を図 3 に示す。装置やリンクの故障に備えて、基幹部分は概ね二重化されている。さらに L3 コアスイッチの内部構成を図 4 に示す。今回導入した L3 コアスイッチ(Cisco Catalyst 6509)には、ファイアウォールモジュール(FWSM)を 3 基搭載している。さらに 2 つの独立した L3 機能(VRF と MSFC)とポリシールーティングを駆使して、各ゾーンに提供する接続性(アクセス可否の制御)を実現した。L3 コアスイッチに搭載する FWSM は、1 基を全学ファイアウォール用、2 基を個別ファイアウォール用に割当てている。FWSM は 1 基あたり、20 の仮想ファイアウォール(VFW)が設定可能であり、それぞれの VFW には 50 の内部ネットワーク(内部インタフェース)が設定できる。FWSM を 2 基使用することで、2,000 の内部ネットワークを構成した。ただしこの方法では、同一 VFW の内部ネットワーク間は VFW のルーティング機能により通信可能となるため、互いの内部ネットワークが通信できないようにフィルタを設定している。各内部ネットワークは一部の例外を除いて /24 のサイズであり、原則として DHCP 機能が提供されている。外部へは NAPT 機能によりそれぞれ異なる外部 IP アドレスに変換されてアクセスを行う。

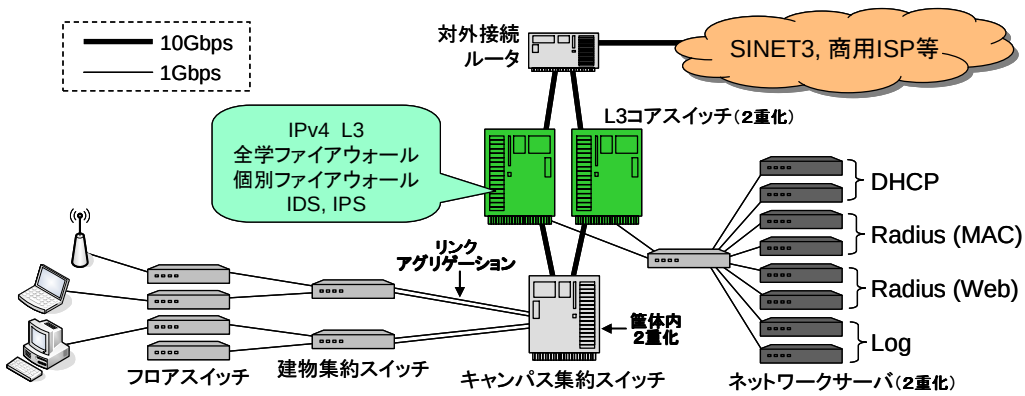


図 3　基幹ネットワーク構成図

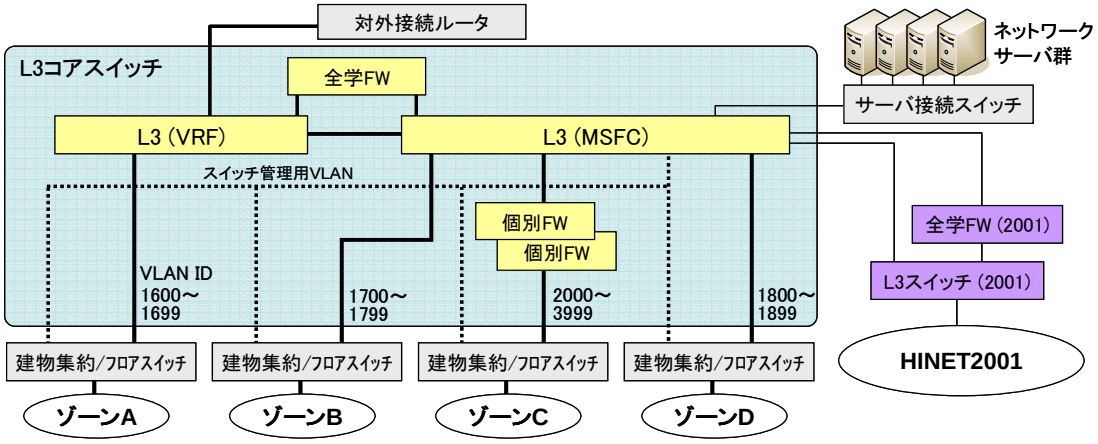
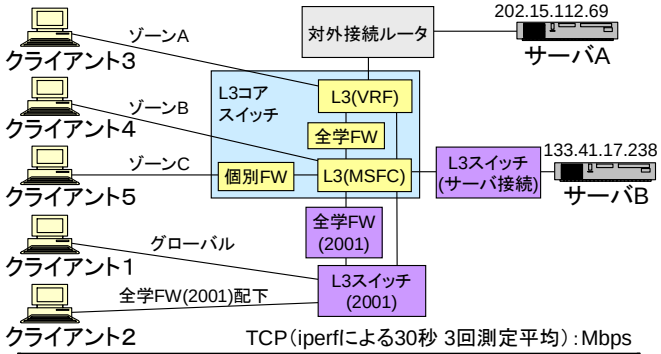


図 4　L3 コアスイッチ設定概要図

コアネットワーク装置の設計にあたっては、ファイアウォールが通信に与える影響を調べるため、HINET2007 導入の前後で通信速度の測定を行った[3]。HINET2007 を導入することによる HINET2001 への影響は見られなかった。HINET2007 導入後の測定結果を図 5 に示す。利用者はクライアント 1,2 の環境からクライアント 3,4,5 の環境に移行することになる。クライアント 1, 2 からクライアント 3,4 へはほぼ



TCP（iperfによる30秒 3回測定平均）：Mbps

	サーバA		サーバB	
	送信	受信	送信	受信
クライアント1	471	517	704	709
クライアント2	--	365	691	615
クライアント3	637	685	712	878
クライアント4	--	348	696	801
クライアント5	--	292	--	433

図 5 スループット(HINET2007 移行後)

同様な結果となっているが、クライアント 5 の通信速度はやや低くなっている。これは 1 基の FWSM に 20 の VFW を設定し、1,000 の内部ネットワークを構成しているためと思われるが、実用上は問題ないと判断している。

4.2 利用者認証機能の実現

移行が完了するとHINET2007は広島大学の構成員約20,000名が日常的に利用する認証ネットワークとなる。認証システムの設計においては、次の 2 点を特に考慮した。1 点目は、大学には新旧さまざまな OS、ネットワーク機器が混在している点である。広島大学では、以前より利用者認証機能を持つ情報コンセントシステムの開発、運用を行っていた経験[4]から、Web ブラウザを用いた利用者認証を基本とし、Web ブラウザを持たない機器に対しては利用者を特定した上で Mac アドレス認証を行うこととした。2 点目は、事務職員が利用する事務用端末の起動時間が始業時間前後に集中するという点である。図 6 に HINET2001 において観測した端末増減数の時間推移を示す。この結果から、8 時 20 分から 35 分の 15 分間に約 600 台の端末が接続されていることがわかる。またこの負荷は一部(事務棟)の認証スイッチに集中するため、認証スイッチ自身の性能も考慮する必要がある。

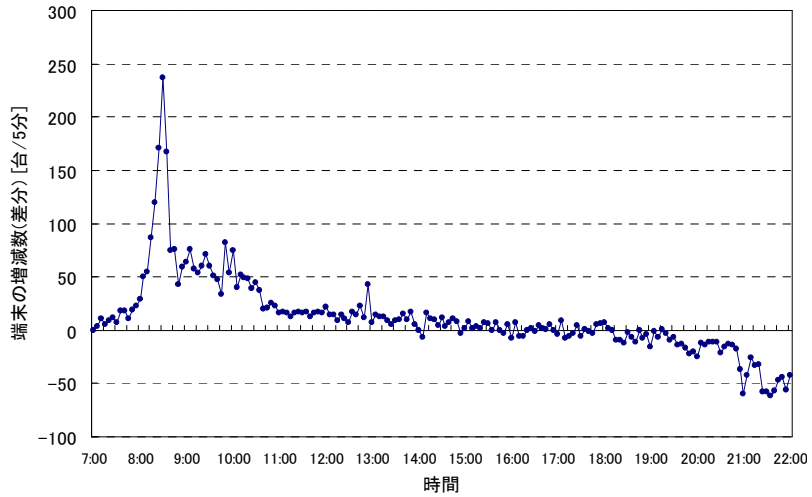


図 6 HINET2001 における端末の増減数

これらの要件を実現するため、図7に示す認証システムを構築した。DHCPサーバは約2,000の各ゾーンに対して最大120アドレスを割当てる機能を、ログサーバはフロアスイッチの認証ログやファイアウォールログを保存する機能を提供する。ホスト登録装置およびRadius サーバは、MACアドレス登録および利用者認証で利用する。各サーバは高可用性が要求されるため、HA(High Availability)クラスタを構成し、冗長化されている。フロアスイッチ(Alaxala AX2430S)は認証機能を持つL2スイッチで、本スイッチの各ポートが認証ポイントとなる。Web 認証と MAC アドレス認証に対応し、Web 認証では外部 Webページへのアクセスが認証ページにリダイレクトされる。認証ページはhttps接続でのみ提供しており、約450台の認証スイッチが使用するサーバ証明書には国立情報学研究所のサーバ証明書プロジェクト[5]が発行する中間CA証明書を採用した。

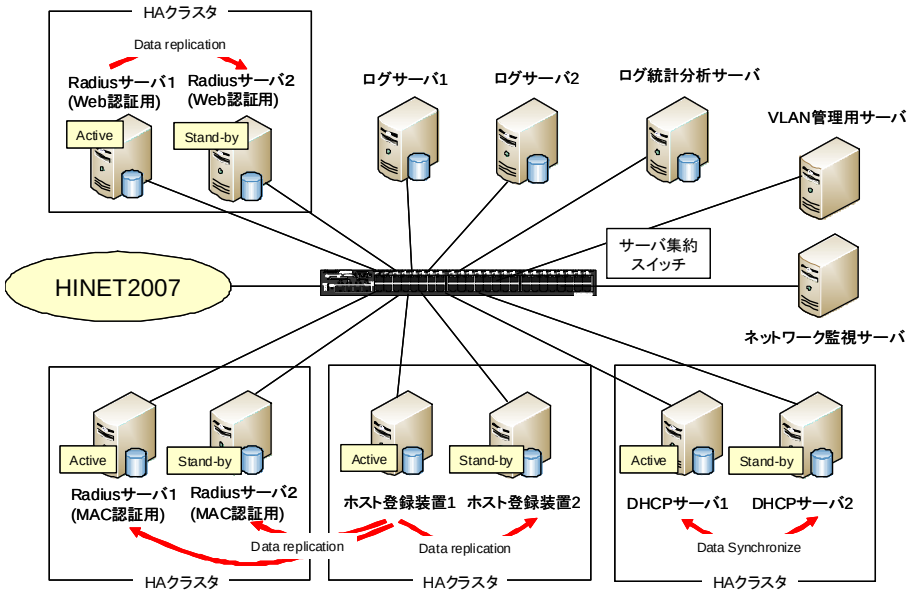


図7 認証システムの構成

構築する認証システムが要求どおりに機能することを確認するため、仕様策定段階あるいは構築段階において、以下の性能評価を行った[6]。

(1) DHCPサーバのIPアドレス払い出し性能

同時リクエスト数を変化させて、すべてのリクエストへの応答が完了するまでの時間(最小／平均／最大)を測定した。測定結果を図8に示す。この結果から、450台からの同時リクエストに対して最大0.12秒以内に処理が完了していることがわかる。

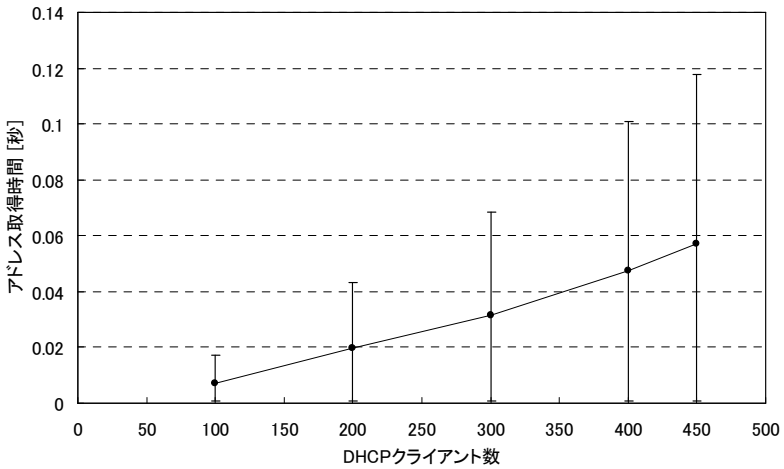


図8 DHCPサーバの応答時間

(2) Radius サーバの同時認証性能

Web 認証用 Radius サーバは外部 LDAP を、MAC アドレス認証用 Radius サーバは内部 LDAP を参照するため、それぞれについて同時リクエスト数を変化させて、すべての認証が完了するまでの時間(最小／平均／最大)を測定した。測定結果を図 9 に示す。この結果から、600 台の同時認証でも 1 秒以内に処理を完了できる性能を有することがわかる。

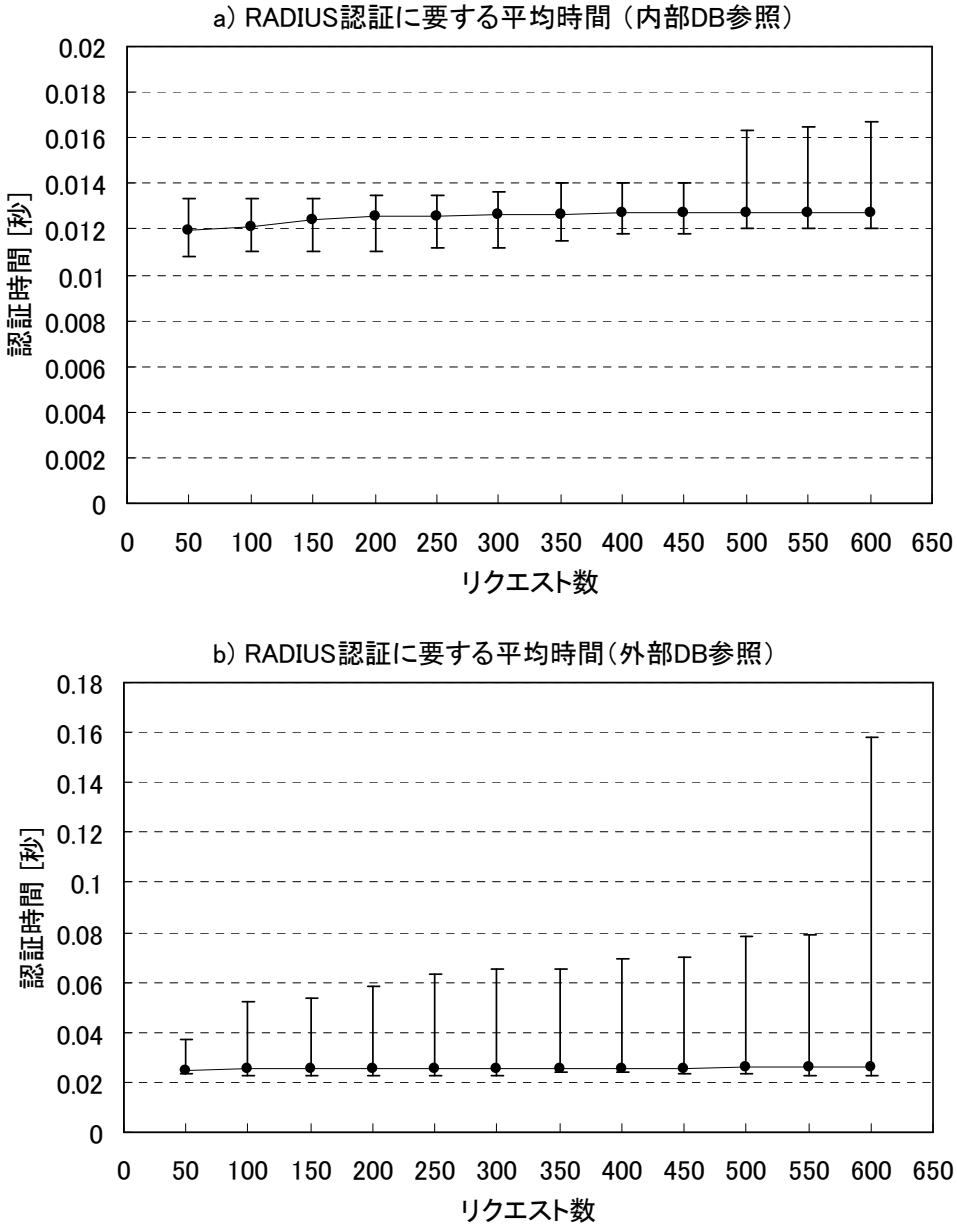


図 9 Radius サーバの応答時間

(3) 認証スイッチの同時認証性能

クライアントから http による外部 Web ページへのアクセス、フロアスイッチ内の認証ページへのリダイレクト、https(鍵長 2,048 ビット)による認証情報の送信、認証応答メッセージの受信までの時間の和を認証時間とし、同時認証セッション数を変化させて、すべての認証が完了するまでの時間(最小／平均／最大)を測定した。測定結果を図 10 に示す。この結果から、同時 100 セッションの認証要求に対しても最大 23 秒程度で処理が完了できることがわかる。

以上の評価結果から、事務用端末の一斉認証要求のような状況においても実用的な時間で認証処理を完了できることが確認できた。

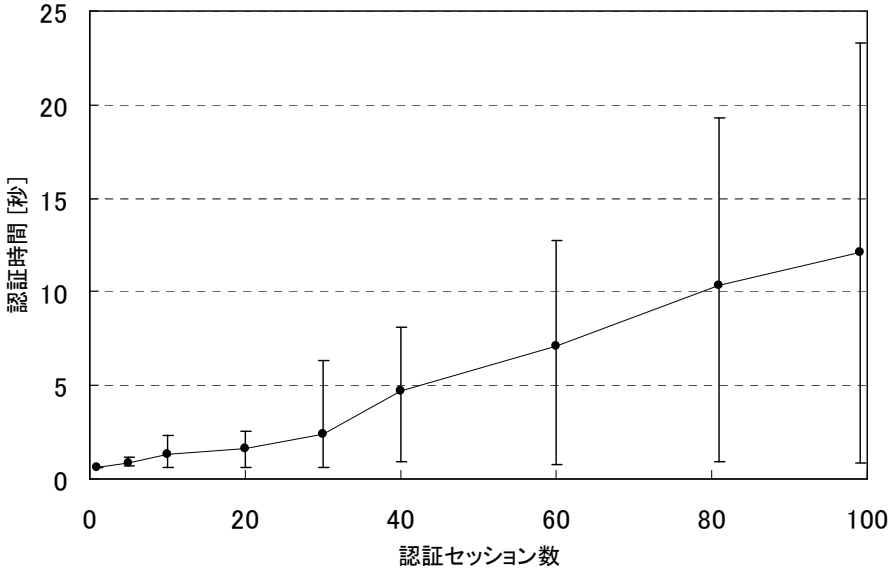


図 10 同時認証セッションに対する応答時間
（https 接続, 鍵長 2,048 ビット）

5 移行の支援体制とシステム

5.1 申請手順

ゾーン C を利用するには、コネクタ ID 申請、ゾーン C 仮割当申請、ゾーン C 本割当申請の 3 つが必要であり、図 11 のような手順で申請する[7]。HINET2007 では建物集約スイッチ、フロアスイッチの各ポートまでを一元的に管理するため、スイッチとポートにスイッチ ID とコネクタ ID と呼ぶユニークな識別番号を付している。利用者はコネクタ ID 申請において最寄りのスイッチ ID を指定するとポートが割り当てられ、コネクタ ID の通知と同時にコネクタ ID が印刷されたシールが送付される。利用者は指定されたポートに接続したフロア配線の情報コンセントにそのシールを貼り付け、以後のゾーン C 本割当申請でポートを指定するために使用する。ゾーン C 仮割当申請では VLAN ID の割当を行い、ゾーン C 本割当申請ではコネクタ ID の VLAN ID への対応付けと、必要に応じて MAC アドレス認証をするためのホスト登録を行う。一方、ゾーン A,B はコネクタ ID 申請の後、ゾーン C 本割当申請と同様な処理を行う。なお、ゾーン A,B は MAC アドレス認証のみである。

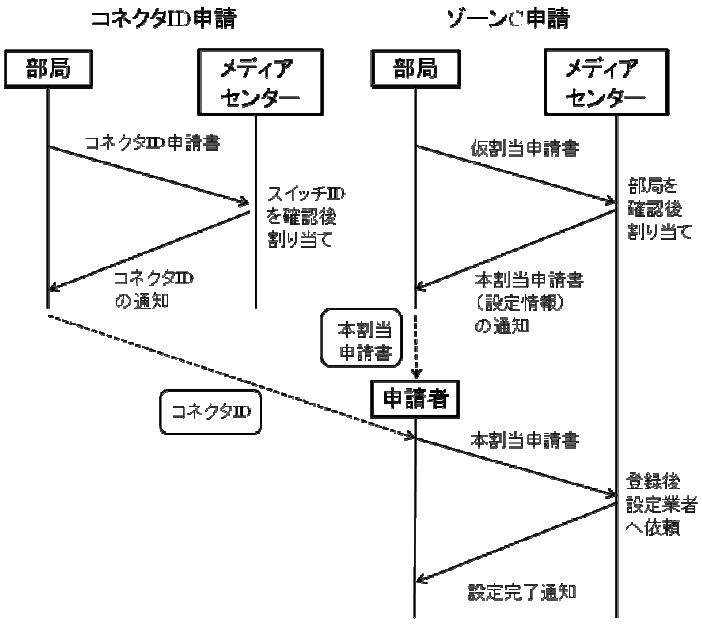


図 11 コネクタ ID とゾーン C の申請手順

5.2 支援体制

これまで支線ネットワークの整備およびサブネットの管理はそれぞれの部局等で独自に行われてきたことから、移行段階においてはさまざまな例外処理が必要になることが予想されたため、人手による申請受付を行うこととした。コネクタ ID 申請およびゾーン申請は Excel で書かれた申請書に必要事項を記入し、電子メールで受付アドレスに送付する。メディアセンターでは教員 5 名が日替わりで受付処理を担当し、設定担当(外注業者)に指示している。申請書およびコネクタ ID やゾーンの管理台帳は WebDAV を利用して共有し、受付処理担当、設定担当および移行支援担当が常時参照できるようにしている。

設定が完了した後の HINET2001 から HINET2007 への接続変更、IP アドレスの変更は現場での作業となる。これらの作業は原則として申請者本人が行うこととしているが、申請者からの要請があった場合にはメディアセンターの職員のほか、技術センターの職員が支援を行う体制を構築した。技術センターには学内の全技術職員が所属し、派遣先の部局等でそれぞれの専門に基づいた技術支援業務を行う組織である。技術センター職員は全学に分散配置されており、派遣先の事情に詳しいため、彼らの力を有効活用することとした。HINET2007 の仕様が確定した約 1 年前から、技術センターの職員に対して新旧ネットワークの違い、新ネットワークの特徴、運用方針などの講習会を実施して移行開始に備えた。

5.3 ホスト登録システム

移行段階ではコネクタ ID の割当、ゾーンの割当などを集中的に行うため、人手による受付処理を行っているが、申請から完了までに最大 2 営業日かかる。そのため、ゾーン C 移行後の認証方式の変更(Web 認証から MAC アドレス認証へ)、ゾーン A,B のホストの入れ替え(MAC アドレスの変更)などの軽微な変更については、申請後すぐに変更が反映されるようホスト登録システムを構築した。管理者または副管理者は、利用者認証の後に自らが管理するゾーン C あるいはゾーン A,B のホストの属性(現在は MAC アドレスのみ)を変更できるようになっている。ホスト登録システムには、ゾーン C の申請を受け付け、VLAN ID や IP アドレスの割り当てを行い、コネクタ ID の対応付けを行って、設定担当に設定依頼を自動的に送付する機能も持たせているため、移行期間終了後は順次機能の提供を開始する予定である

6 おわりに

本稿では、広島大学で構築した新キャンパスネットワーク HINET2007 の特徴、運用・移行の方針、設計・構築のポイント、移行の支援体制とシステムについて概要を述べた。HINET2007 の構築手法は、教育研究を遂行する上での自由度を一定のレベルで維持しつつ、全体的なセキュリティレベルの底上げを図る現実的なひとつのモデルとなると考えている。最後に、2008 年 5 月(申請受付は 4 月)から開始した移行の状況は表 2 のようになっており、2008 年 12 月末現在でコネクタ ID 登録数は 3,798、ゾーン C 割当数は 832 である。一方、HINET2001 の残存ホスト数は図 12 のように推移しており、移行のペースが鈍ってきているため、2009 年 3 月末の HINET2001 停止に向けて各サブネットの管理者に残存ホスト(MAC アドレス)の一覧を送付し、ラストスパートを呼びかけているところである。

[謝辞]

HINET2007 の構築および移行、運用に尽力いただ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します。

表 2 HINET2007 の移行状況

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
申請メール受付数	28	126	100	140	173	183	110	100	126			
コネクタ登録数	-	520	95	1215	608	493	230	178	530			
コネクタ削除数	-	28	2	1	6	20	14	0	0			
アドレス登録数	-	290	215	1044	745	934	354	173	83			
アドレス削除数	-	8	11	16	9	32	34	10	2			
ゾーンC割当数	76	322	56	36	154	61	42	33	52			

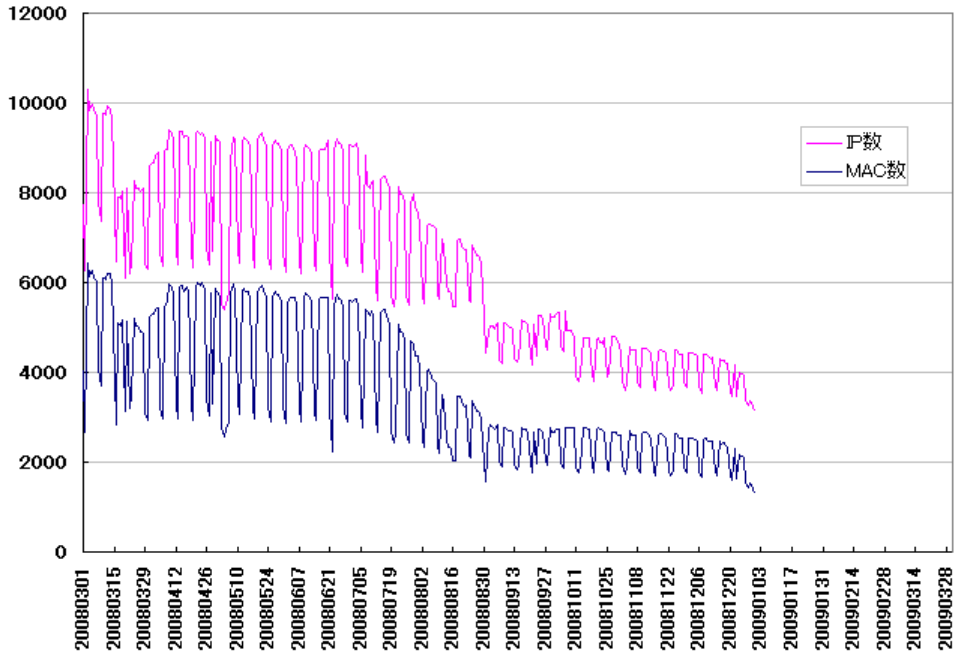


図 12 HINET2001 の接続ホスト数の状況

参考文献

[1] 広島大学情報メディア教育研究センター：
“HINET2007 情報”, http://home.hiroshima-u.ac.jp/infra/hinet2007info/.

[2] 相原 玲二, 西村 浩二, 岸場 清悟, 田島 浩一, 近堂 徹, “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-S117 (2008 年 3 月).

[3] 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 年 7 月).

[4] 西村 浩二, 秋成 秀紀, 野村 嘉洋, 相原 玲二, “遠隔機器制御プロトコルを用いた有線／無線 LAN 用情報コンセントシステム”, 情報処理学会論文誌, Vol.43, No.2, pp.662-670 (2002 年 2 月).

[5] 国立情報学研究所 UPKI イニシアティブ：サーバ証明書発行・導入における啓発・評価研究プロジェクト, http://upki-portal.nii.ac.jp/cerpj.

[6] 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”, 情報処理学会第 1 回インターネットと運用技術シンポジウム (IOTS2008), pp.121-128 (2008 年 12 月).

[7] 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 年 9 月).