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

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

広島大学情報メディア教育研究センター

あらまし 平成20年度より広島大学で運用を開始した新キャンパスネットワークは，全学電子認証システムとも連動するネットワーク利用者認証機能を提供している。この利用者認証は，全学で約450台整備したエッジスイッチにて実現しており，一時利用者のみならず定常利用者を含む全利用者に対してネットワーク接続時の利用者認証を行うことで，セキュリティの保証された安全な利用環境を実現している。全学的なネットワークインフラとして利用者認証機能を提供するためには安定かつ強固なシステム構築が必要となる。本稿では，認証機能を提供するキャンパスネットワークの構築手法について述べるとともに，現在運用中のキャンパスネットワークでの同時認証性能測定などについて示す。

Performance Evaluation of a Large Scale Campus Network System with User Authentication Function

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

Information Media Center, Hiroshima University

Abstract A new campus network system operating at FY 2008 in Hiroshima University provides user authentication function which work closely with a campus digital authentication service. The user authentication implements campus-wide 450 floor switches, and provides the secure network infrastructure not only for guest users but for university members. In this paper, we describe the construction of a large scale campus network system with user authentication function. Moreover, we show the performance evaluation with results of a simultaneous access experiment.

1　はじめに

大学などの高等学術機関では，教育研究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一方で，大学の主要インフラとしての重要度が増すに従い，セキュリティや帯域不足，管理体制など様々な問題が生じるようになってきている。特に，セキュリティに関する問題は顕著である。大学のネットワークという性質上，持ち込み端末を含む多種多様な端末が接続され，利用者のコンピュータリテラシーも必ずしも一定とはいえない状況の中，セキュリティを確保するためのコストが非常に高くなってきている[1][2]。そのため，高いセキュリティを確保しつつユーザの利便性を損なわない，オープンかつスケーラブルなキャンパスネットワークが望まれている。

平成20年度より広島大学で運用を開始したHINET2007[3]はセキュアでスケーラブルなキャンパスネットワークを目指し構築した新しいキャンパスネットワークである。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，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利用者に提供する[4]。さらに，研

究室を含むすべての利用場所で機器接続の際に何らかの利用者認証を要求し，機器管理を行う。これにより，セキュリティの保証された安全な利用環境を実現している。全学的なネットワークインフラとして利用者認証機能を提供するためには，定常的利用はもとより PC 演習室や事務系端末などの一斉認証要求に耐え，安定した運用が行えなければならない。本稿では特に，利用者認証機能に関する部分に焦点を当て，実現方法と実際に運用中のネットワークを用いた主要サービスの性能測定について述べる。

本稿の構成は以下の通りである。まず，2 では新キャンパスネットワーク HINET2007 の全体概要について述べる。3 では，利用者認証に主眼を置いてシステムの実現手法について述べる。4 において，提供する利用者認証機能に関連する性能測定について述べ，最後に 5 にてまとめを記す。

2 HINET2007 の概要

今回構築したキャンパスネットワーク HINET 2007 の概要を図 1 に示す。主な特徴は以下に示す通りである。

(1) 全学的な一元管理体制

接続機器や接続形態の多様化によって，これまでの部局単位でのサブネット管理体制では管理者への負担が非常に大きなものとなり，継続的維持が困難となってきていた。

HINET2007 では，各部屋の情報コンセント単位での接続状況の把握を全学的に行うため，主要フロアに設置する接続機器まで全学管理としている。

(2) VLAN による柔軟な仮想配線の提供

既存配線を有効に活用するために，IEEE802.1q(TagVLAN) 機能による仮想配線機能を提供している。

(3) 個別ファイアウォール機能の提供

これまでサブネット管理者の管理負担を増大させていた研究室内設置のファイアウォール機能（ブロードバンドルータ等を含む）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。利用者の利用形態（研究室単位や教員単位）に応じたファイアウォールを提供するため，約 2,000 の個別ファイアウォール（NAPT）機能と DHCP サーバ機能を実現している。ファイアウォールの構成方法については文献[5]にて詳しく説明しているためここでは割愛する。

(4) すべての利用場所で利用者認証を要求

(1)で示した一元管理を実現するためには，接続機器を個別に管理し，ホスト単位での利用者を明確にする必要がある。これを実現するために，主要フロアに設置する接続機器に利用者認証機能を持たせ，すべての場所で機器の接続に際し何らかの認証を要求する。その仕組みについては次節にて詳しく説明する。

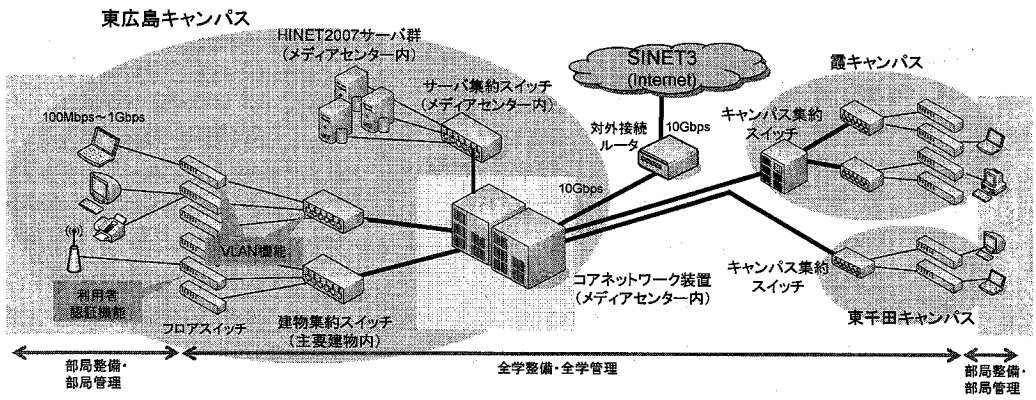


図 1. HINET2007 概要図

今回の整備では，約 40 台の建物集約スイッチと約 400 台のフロアスイッチ，合計 450 台を整備し，各スイッチのポートまでを全学整備・全学管理としている。

3　利用者認証ネットワークの提供

本節では，利用者認証ネットワークの提供に焦点をあて，必要なシステム要件について示した後，構築したシステムの構成について述べる。

3.1 システム要件

前節に示したように，すべての場所で利用者認証を要求するため，広島大学の構成員数である約 20,000 人が利用する認証ネットワークとなる。大学のような学術機関でこのような認証ネットワークを実現しようとする場合，考慮しなければならない点がいくつかある。

まず一点目に，異なる OS が混在する環境においても同一の認証プラットフォームを導入する必要がある。つまり，古い Windows OS や Mac OS，Unix などの利用者も存在は無視できず，既に点在しているスイッチ等（いやゆる島ハブ）を含む研究室内の既存ネットワークシステムとの親和性も考慮した認証プラットフォームでなければならない。このことより，IEEE802.1x 認証機能は運用面でも大きな負担となるため，Web ブラウザの基本機能のみで利便性を損なわずに認証できなければならない。また，Web ブラウザを持たない機器（サーバやプリンタなど）に対する接続認証についても考える必要がある。

二点目に，今回は職員等が利用する事務用端末も約 1,400 台接続されるため，始業時間前後には短時間での端末の接続と大量の認証要求が発生することが予想される。図 2 に HINET2007 構築前のキャンパスネットワークにて事前調査した，5 分間隔の端末の増減数を示す。この結果からも分かるように，8 時 20 分から 35 分の間（15 分間）で約 600 台の端末が稼動開始している。このデータを採取したのは月曜日であったが，このような傾向は休日を除く他の曜日でも観測されており，これらに対する一斉認証要求を処理できなければならない。また整備したスイッチ 450

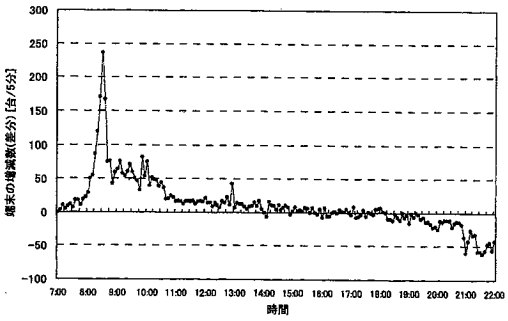


図 2. HINET2001 における端末の増減数

台から定常的に認証要求が発生するため，システム全体として DHCP サーバの IP 払い出し性能や利用者認証の同時認証に対する耐性および安定性を確保しなければならない。

三点目に，システムとして認証情報の維持・管理手法を考える必要がある。約 20,000 人の利用者が日常的に利用するネットワークの認証情報であり，常に最新の状態で保持・管理しなければならない。

3.2 システム構成

前節に示した要件を考慮して構築した認証ネットワークシステムの主な機器の名称と仕様を表 1，サーバ構成図を図 3 に示す。このうち，DHCP サーバは約 2,000 のゾーンに対して各ゾーン最大 120 アドレス（したがって，ネットワーク全体では最大約 24,000 アドレス）を割当てる DHCP 機能を担い，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等を保存するために利用される。ホスト登録装置および Radius サーバは利用者認証において利用される。以下に利用者認証機能の詳細について説明する。

図 1 に示した建物集約スイッチおよびフロアスイッチは，いずれも認証機能を持つ L2 スイッチであり，それらスイッチの各ポートから直接，研究室等の部屋へ配線される。認証ポイントは，フロアスイッチの各物理ポートとなり，フロアスイッチを経由する通信の際に認証が必要となる。認証は，Web 認証および MAC アドレス認証に対応する。Web 認証では https 接続のみ許可しており，認証画面へのアクセスは，外部 Web ページ

表 1. 主要機器の名称または仕様

機器	仕様
フロアスイッチ	Alaxala ax2430s
建物集約スイッチ	
サーバ集約スイッチ	
Radius サーバ	CPU : Xeon X5355 2.66GHz x 2, Memory: 4GB, FreeRADIUS1.1.7, OpenLDAP 2.3.41
DHCP サーバ	CPU: Xeon X5355 2.66GHz x 2, Memory: 4GB, ISC-DHCP3.0.5

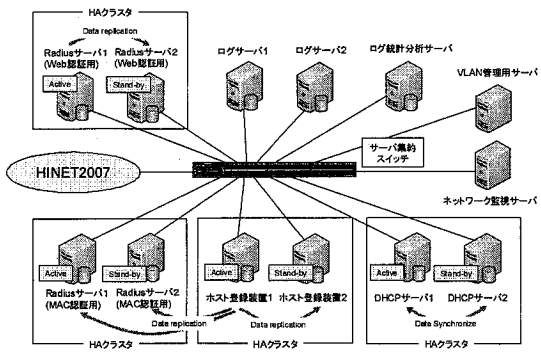


図 3. 認証システムのサーバ構成図

を閲覧時に自動的にリダイレクトされる。なお，整備したスイッチ 450 台のサーバ証明書には国立情報学研究所 UPKI イニシアティブの UPKI サーバ証明書プロジェクト[6] が発行する中間 CA 証明書を導入している。

端末の認証時に発生するフロアスイッチからの認証情報は，図 3 に示す Radius サーバによって処理される。システムでは Web 認証用と MAC 認証用の Radius サーバを設置しており，各々の認証方式に応じた Radius サーバが参照される。Web 認証の Radius サーバは，自サーバ上で動作するバックエンドデータベースである LDAP サーバとメディアセンター外部 LDAP サーバを参照することで利用者の認証情報を提供する。自 LDAP サーバは，既存の全学電子認証システムのレプリケーションとなっている。全学電子認証システムは，教務システムや会計システム，学生情

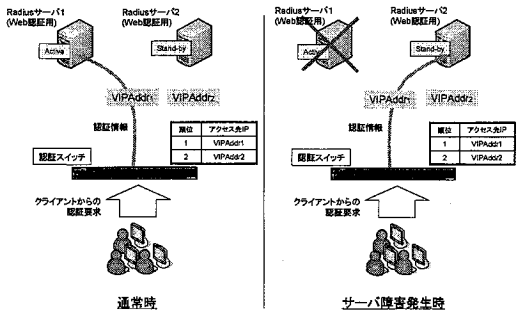


図 4. サーバの HA クラスタによる冗長化

報システムなどに利用され，全構成員が登録されている。メディアセンターLDAP サーバは，一時利用のゲストアカウントの管理・参照のために利用される。Radius サーバからの問い合わせ順は，自 LDAP サーバを参照した後，レコードが存在しない場合，メディアセンターLDAP サーバが参照される。一方，MAC 認証の Radius サーバは，自サーバ上で動作する LDAP サーバに保持された MAC アドレスを参照する。MAC アドレスは，利用者自身がホスト登録装置を利用したネットワーク経由で登録，または管理者による登録となっている。

新キャンパスネットワークにおける認証機能の提供は高可用性が要求されるため，各 Radius サーバは，各々が HA(High Availability)クラスタを構成し，冗長化を行っている。構成方法を図 4 に示す。稼動系が何らかのサーバ障害で停止した場合，待機系が仮想 IP を引き継いでフェイルオーバー行う。フロアスイッチの認証要求先には仮想 IP を指定しておくことで，サーバ障害を意識する必要なく，フロアスイッチの設定情報はそのままで認証要求先のサーバを切り替えることが可能となる。

端末のログアウトは，利用者自身による Web ブラウザからの明示的なログアウト操作のほか，フロアスイッチからの生存確認を基に行われる。生存確認方法は，フロアスイッチ直接収容の端末の場合はリンクダウンの検出，スイッチングハブなどを経由する端末の場合は ARP ポーリングによる接続監視による自動ログアウトが行われる。

現在のARPポーリングはWeb認証端末のみが対象となる。フロアスイッチから1分間隔で送られるARPリクエストに対する応答がない端末を対象に，1秒間隔で3回連続してARPリクエストが送信される。それでも応答がない場合，端末が切断されたと認識され，フロアスイッチ側で強制ログアウト操作が行われる。

4 システム性能測定

前節に示したように，利用者認証機能を安定して提供するためには，多数の利用者が接続した場合のシステム性能が重要な要素となる。そこで本節では，約2,000のファイアウォールにて提供するDHCPサーバの払い出し性能，Radiusサーバと認証スイッチに対する同時認証性能について示す。

4.1 DHCPサーバのIP払い出し性能測定

まず，約2,000のファイアウォールに対して提供するDHCPサーバのIPアドレス払い出し性能について，実運用中のDHCPサーバを用い測定を行った。

測定内容は，DHCPクライアントが動作するLinux-PC (CPU: Core2Duo 3.00GHz / Memory: 4GB) を，稼動中のフロアスイッチに接続し，このPCよりDHCPリクエストを複数同時に送出することで行った。接続するネットワークは実験用に確保したサブネットマスク/23のネットワークとし，DHCP割当数は最大503個に設定している。なおDHCPクライアントには，スクリプト言語perlのDHCPライブラリを用いて複数台からの同時取得要求をエミュレートし，クライアントPCでパケットキャプチャすることで，DHCPリクエスト(DHCP- DISCOVER)の送信からアドレスの取得(DHCP- OFFER)までの時間を応答時間として測定した。

図5にDHCPによるアドレス取得時間の測定結果を示す。横軸は生成した同時リクエスト数であり，縦軸は各同時リクエスト時の最小/平均/最大の応答時間を表す。それぞれ，クライアント数毎の測定点において6回測定した平均値を代表値としており，この測定においても，すべての処

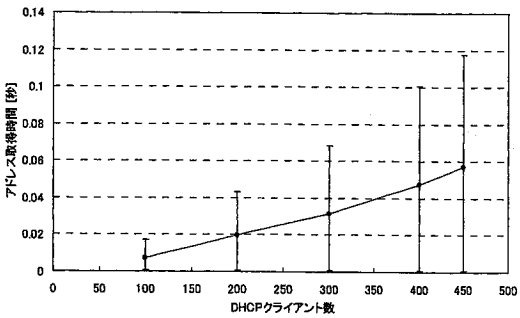


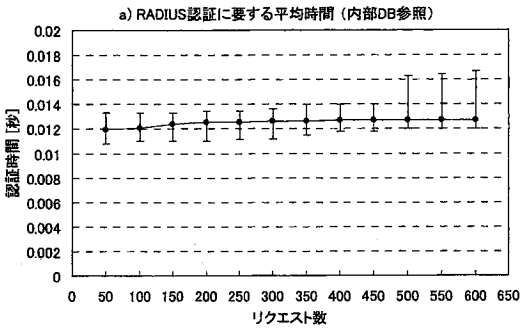
図5. DHCPサーバの応答時間

理（異なるIPアドレスの取得）に成功していることを確認している。この結果より，450台からのDHCPによるアドレス取得の一斉要求に対しても最大で0.12秒以内で処理が完了していることが分かる。このことから，現状より数倍の規模のDHCP払い出し処理も可能であると考えられ，全学的に提供するDHCPサーバとして十分運用に耐えられるものであると判断できる。

4.2 Radiusサーバの同時認証性能測定

次に，フロアスイッチからの認証問い合せ処理を行うRadiusサーバの同時認証性能を調べた。本測定においても，実運用中のRadiusサーバを用い，Web認証とMAC認証の場合それぞれについて行った。本実験におけるWeb認証の場合は，メディアセンターLDAPサーバに格納されたゲストアカウントを認証ID/パスワードとして利用する。またMAC認証の場合は，Radiusサーバ内の自LDAPサーバに格納されたMACアドレスを用いて認証が行われる。ゲストアカウントによるWeb認証の場合（外部DB）とMACアドレス認証（内部DB）の場合で特性が異なることが予想されるため，それぞれについて測定を行った。なお測定時間は，比較的利用者が少ない夜間（19時から22時）に実施した。

測定内容は，用意したLinux-PC (CPU: Core2Duo 2.33GHz / Memory: 3GB) を図3のサーバ集約スイッチの空きポートに接続し，このPCから，FreeRADIUS[7]に付属のRADIUSクライアントを用いて複数の同時認証要求を生成し，



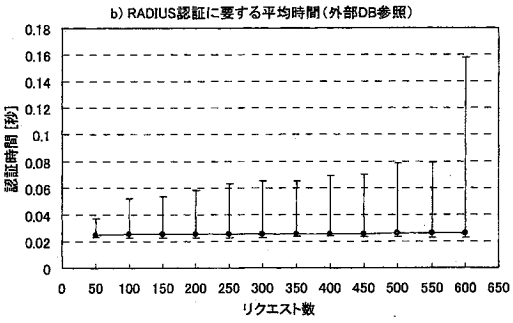


図 6. Radius サーバの認証応答時間

認証要求ごとの Radius サーバからの応答時間を測定した。

Radius 認証の同時認証要求に対する応答時間の測定結果を図 6 に示す。横軸は生成した同時リクエスト数であり，縦軸は各同時リクエスト時の最小/平均/最大認証時間を表す。それぞれのクライアント数毎の測定点において 6 回測定した平均値を代表値としている。なお，この測定においても，すべての認証処理が成功していることを確認している。

この結果から，Radius 認証における一斉認証要求に対する許容台数を見積もることができ，600程度の同時認証には1秒以内に全ての処理が完了している。この値より，3 節にて示した，事前確認している事務系端末からの一斉認証におけるサーバ側の応答には問題なく，現状より数倍の規模の認証にも耐えうる値であると判断できる。なお，サーバークライアント間の RTT は，平均 0.17[ms]であり，測定結果の時間への影響

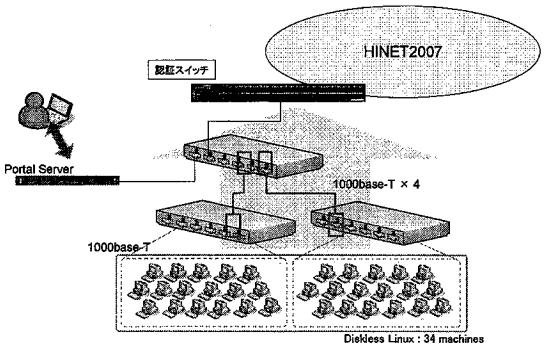


図 7. フロアスイッチの認証性能測定図

は十分小さいと推測できる。

4.3 認証スイッチの同時認証性能測定

LAN スイッチの Web 認証機能を使用する場合，一斉利用開始時における認証性能の問題が指摘されている[2]。そこで，実運用状態となった HINET2007 フロアスイッチの Web 認証性能を定量的に評価した。測定構成を図 7 に示す。測定では，稼動中のフロアスイッチの 1 ポートに認証性能評価システム[8]を接続し，34 台のクライアント PC (CPU: Pentium4 3GHz / Memory 1GB) から同時認証セッションを生成する。34 セッション以上については1台の PC で複数セッションを生成することで仮想的な認証セッションを生成している。クライアント PC では，http による外部 Web ページへ接続から，フロアスイッチでリダイレクトされる認証ページを受信し，https による認証情報の送信と応答の受信までを自動化している。本測定では，http による外部 Web ページ接続から認証応答メッセージが返ってくるまでの和を認証時間として計測した。なお，クライアント PC からは https 接続（鍵長 1024 ビット）でフロアスイッチにアカウント情報を送信する。アカウントは，メディアセンターLDAP サーバに格納されたゲストアカウント 100 個を利用した。

同時認証セッション数に対する認証時間測定結果を図 8 に示す。横軸が生成セッション数で，縦軸が全セッションの最小/平均/最大認証時間

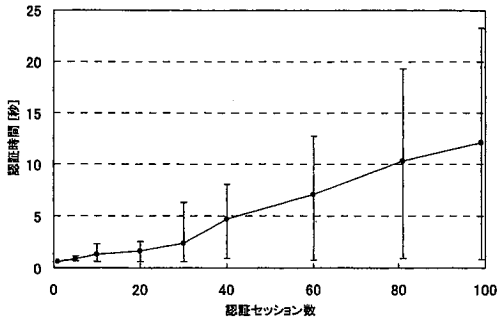


図 8. 同時認証セッションに対する認証時間
(https 接続, 鍵長 1024 ビットの場合)

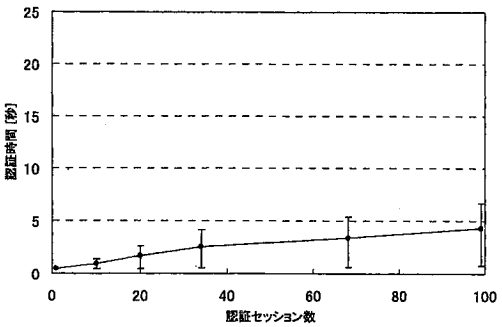


図 9. 同時認証セッションに対する認証時間
(http 接続の場合)

を表す。各測定点において 3 回測定した平均値を代表値としている。例えば, 横軸 60 の場合は, 60 セッションの同時認証要求に対する認証時間の最小値/平均値/最大値が 0.5 秒/7 秒/13 秒であることを示している。また, 比較のために http 接続における同時認証性能の測定結果を図 9 に示す。なお, いずれの測定においても, すべての端末でログイン処理が成功していることを確認している。

図 8 の結果から, フロアスイッチにおける一斉認証要求に対する許容台数を見積もることができ, 数セッションの同時認証要求であれば 1 秒程度, 100 セッションの同時認証要求に対しても最大 23 秒程度で処理可能であることが分かる。また, 図 9 と比較してみると, 同時認証セッション数の増加および SSL 利用と鍵の長さが認証処理性能に影響を与えることが分かり, これはセキュリティと認証処理性能のトレードオフであるといえる。

前節における DHCP サーバおよび Radius サーバの測定結果も踏まえ, 認証ネットワークの性能について考える。100 クライアントの同時接続の場合, DHCP サーバの応答時間が 0.02 秒以下, Radius サーバの認証応答時間 (外部 DB 参照) が 0.1 秒以下で処理されていることを考えると, https による Web 認証処理が接続時のオーバヘッドのほとんどを占めていることがわかる。しかしながら, 1 つのフロアスイッチあたりの性能として, 100 セッションの同時認証においても 23 秒程度で実現できることから, 前節で示した事務用端末の一斉認証要求のような規模に対しても十分実用に耐えうる性能であると判断できる。さらに, 大規模な端末の同時認証が必要とされる場合やより短時間での認証性能が求められる場合は, フロアスイッチを追加し接続する端末を分散させることで性能改善を図ることも可能であり, 本結果はその指標のひとつとすることができる。

5 まとめ

本稿では, 利用者認証機能を有するキャンパスネットワーク HINET2007 の構築手法と稼動状態のネットワークを用いた性能評価について述べた。ネットワークインフラとして利用者認証機能を安定的に提供するためには, 全学規模での発生する多数の認証要求に対しても, 十分に処理できるシステムが必要となる。本稿では, 利用者の利便性の関わる DHCP サーバの IP アドレス払い出し性能および Radius サーバとフロアスイッチの認証性能について, 運用状態のネットワークでの評価について示した。測定では, 数十台規模のクライアント PC からの同時認証要求に対しても, 実用上問題なく処理可能であることを示した。なお, 2 節にて述べた約 2,000 の個別ファイアウォールの性能測定については文献[5]に掲載しているので, そちらを参照されたい。

HINET2007 では, フロアスイッチの全ポート

（総ポート数 約 14,000）を一元的に管理している。そのため，セキュリティインシデントやユーザからの問合わせに対して，適切かつ早急なトラブルシュートを実施するため枠組みが必要となる。そのためには，認証ログやシステムログの検索の効率化などが必須となるため，今後はこれらについても運用の中で検証していく。

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広島大学総務室情報化推進グループおよび情報メディア教育研究センターの関係者に感謝いたします。

参考文献

[1] 江藤，只木，渡辺，渡辺： “新しい教育用情報基盤の実現へ向けて－認証システムをベースとしたキャンパス規模のオープンネットワーク”,学術情報処理研究, No.6, pp.13--20, 2002

[2] 前田，河野，北村： "キャンパスネットワークへの認証システムの導入", 情報処理学会研究報告 2007-DSM-47(5), pp.19--24, 2007

[3] 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

[4] 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.

[5] 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”, 情報処理学会研究報告 2008-IOT-2, pp.29--34, 2008

[6] 国立情報学研究所 UPKI イニシアティブ: UPKI 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/.

[7] FreeRADIUS Project, http://freeradius.org/

[8] 近堂，田島，岸場，西村，相原: "PC クラスタによる認証スイッチの認証性能評価システム", 情報処理学会研究報告 2007-DSM-47(5), pp.25--30, 2007