

大規模キャンパスネットワークにおける MAC アドレス認証の管理手法

田島 浩一 近堂 徹 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〒739-8526 東広島市鏡山 1-4-2

E-mail: { tashima, tkondo, kishiba, ohigashi, norita, kouji, ray }@hiroshima-u.ac.jp

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、いわゆる利用者認証として全学電子認証システムと連動するネットワーク利用者認証機能を提供するとともに、機器認証の機能として MAC アドレス認証を提供している。これらの認証機能は、全学で約 450 台整備したキャンパスネットワークのエッジスイッチにあたる、各建物のフロア毎に設置したスイッチにて実現しており、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。利用者認証は導入の抵抗や運用しやすさから WEB 認証がよく用いられ、本学でも利用者認証に用いているが、全ての機器のネットワーク接続を認証利用とさせるため、この認証利用に対応できない機器への対策として MAC アドレス認証を併用している。WEB 認証については、これまでにさまざまな研究や実装および製品化が行われ、認証クライアントの接続許可や生存確認方法は主に IP 層で行われており、実用的な方法が確立されている。しかしながら MAC アドレス認証の場合にはレイヤーが異なるため、IP 層での方式をそのまま適用することができない問題があり、この問題にも配慮した MAC 認証を管理するシステムが必要とされる。本稿では、この MAC 認証でのログアウト処理にまとめるとともに、その実現方法について述べ、性能測定結果などを示す。

キーワード MAC アドレス認証, 認証システム, MAC アドレス管理

A Management Method of MAC Address Authentication in Large-Scale Campus Networks

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

Information Media Center, Hiroshima University
1-4-2 Kagamiyama, Higashi-Hiroshima, Hiroshima, 739-8511 Japan

E-mail: { tashima, tkondo, kishiba, ohigashi, norita, kouji, ray }@hiroshima-u.ac.jp

Abstract The operation of the new campus network ‘HINET2007’ began in Hiroshima University since FY 2008. The network user authenticate function that synchronizes with official campus digital authentication service system is offered as a user authentication system. The MAC address authentication is being offered as a function of the equipment authentication. These authentication functions were constructed by the edge switching HUB on about 450 campus networks achieved with the switching HUB of each floor in each building set up. This campus network provides the secure network infrastructure. The WEB based network authentication system was often chosen and, because of the easiness of uses, introduction and operation. We also are using it for the user authentication. To limit the authentication use in hole campus network, the MAC address authentication is used as assistance to the equipment that cannot use the WEB authentication use. Various researches, product have been developed about the WEB authentication system, and practicable method has been established. However, the method in the IP layer cannot be applied as it is because the layer is different at the MAC address authentication, the system that manages the MAC address authentication that considers this problem is required. In this paper, we describe summary of the logout processing in this MAC authentication. Additionally, the achievement method is described and the some performance measurement results are shown.

Keyword MAC Address Authentication, Authentication System, MAC Address Management Method of MAC Address

1. はじめに

大学のキャンパスネットワークをはじめとする組織内のイントラネットワークは、組織のポリシーにより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事で、セキュリティの保証された利用環境が構築できる。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改め、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]の運用開始し、あわせてユーザ端末は原則として**認証利用する事を必須**とした。認証利用を原則とする場合、認証のためのシステムやネットワーク構成の複雑化など、導入や運用にはある程度のコスト増加はやむをえず[3][4]、あわせて異なるアクセスレベルを**ゾーン**として定義し利用者がそれを選択可能な運用を行っている[5]。

利用者認証による認証利用では、利用者への導入の抵抗や、運用のしやすさから **WEB 認証**がよく用いられ、本学でも利用者認証に用いている。なお、キャンパスネットワークの隅々まで全ての機器の接続を認証利用とさせるには、**WEB 認証**に対応できない機器への対策として、**MAC アドレスによる認証**(以降は **MAC 認証**と呼ぶ)を併用する事とした。このような **WEB 認証**の困難な機器には、ルータをはじめとするネットワーク機器やプリンタ、IP 電話機が含まれ、事前にこれらの **MAC アドレス**を登録しておき、それらの機器がネットワークに接続された際に **MAC 認証**が行われ、ネットワーク利用が可能になるのが一般的な **MAC 認**

証の利用方法であり、この方法を用いている。

本稿では、この **MAC 認証**の運用に必要な認証システムについて、以下の構成で述べる。まず、2では本稿の対象とする **MAC 認証**および **MAC 認証システム**について、3では、そこで必要となる **MAC 認証管理システム**についての構成や必要となるサーバ間の連動について述べる。4において、評価を行い、最後に5にてまとめを示す。

2. MAC 認証システム

MAC 認証の運用に必要な認証システムをはじめとするシステムの構成やその動作概要、および、運用上の問題点などについてまとめる。

2.1. 認証システムの構成

ユーザ端末への **MAC 認証**機能の提供には、一般に**認証スイッチ**と呼ばれる認証機能を有するスイッチングハブに設定を行い、教員の居室や研究室等を主に1部屋を1ポートで収容するエッジスイッチとして設置し、ポート単位(部屋の単位)で認証によるアクセスの許可・不許可をコントロールする。

現在のキャンパスネットワークで稼働中のネットワーク認証システムの構成を図1に示す。システム構成図の **HINET2007** のネットワーク内には、認証スイッチ約450台が設置されている。認証システムのサーバ構成は、認証スイッチからの認証に用いる **RADIUS**サーバをはじめとして、認証ログなどの利用記録を収集するログ管理サーバ、そのほか監視や認証スイッチや **VLAN**の管理を行うサーバ群により構成されている。

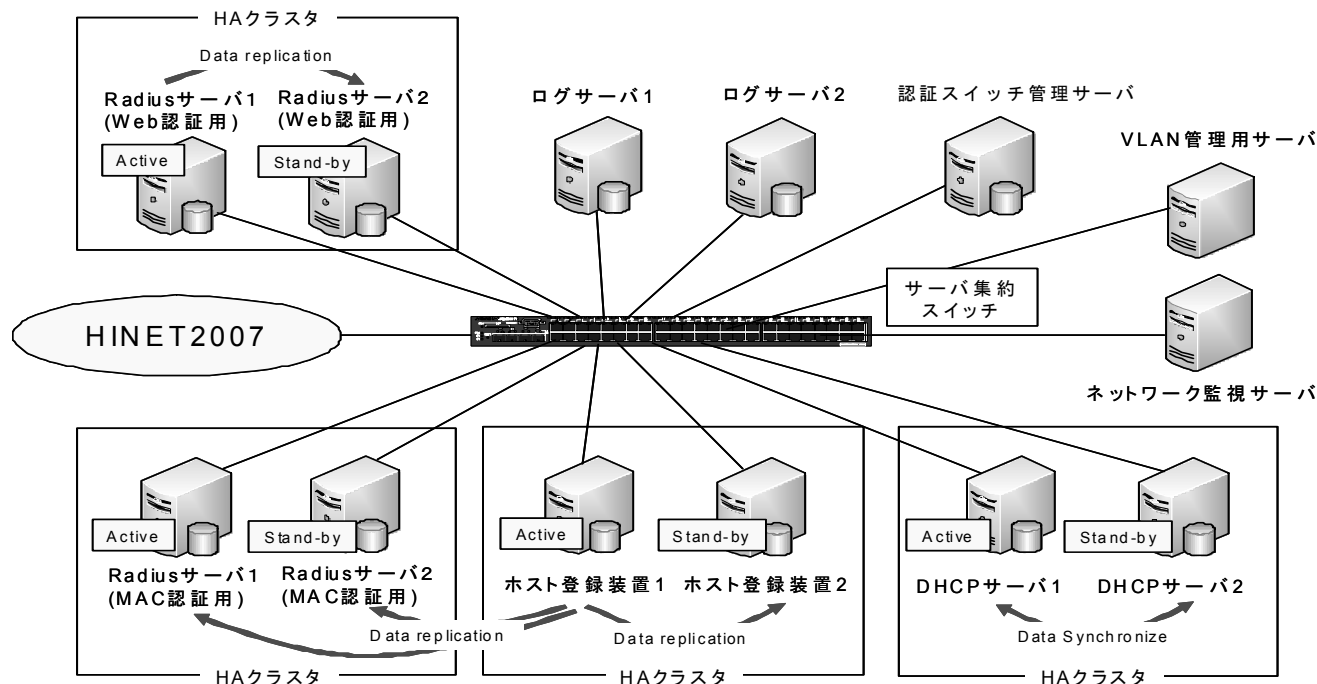


図1. 認証システムのサーバ構成図

HINET2007 のネットワークで MAC 認証が発生すると、図 1 の HINET2007 内の認証スイッチより MAC 認証用の RADIUS サーバで認証が行われる。MAC 認証用 RADIUS サーバは、内部に MAC アドレスを保持するデータベース（以降では DB と略す）をそれぞれに内臓および 2 台で同期して保持しており、そこで参照による登録の有無による認証の可否を判定する。

2.2. MAC アドレスの登録と削除

ユーザ端末の MAC アドレスの登録や削除は、一部の特殊なゾーンを除いた一般利用されるゾーンでは、利用者自身で図 1 の **ホスト登録装置** にアクセスし、MAC アドレスの登録や削除を直接行う。

登録操作により登録した MAC アドレスが直ぐに DB に反映し MAC 認証で直ぐに利用可能になる事は、利用者にわかりやすく、そのように運用するのが一般的と考えられ、登録操作で MAC アドレスの入力を間違った場合でもその間違いを気づいて修正した事などではユーザの利用には支障は出にくいと考えられる。他方、登録操作とは異なり削除操作では、間違っただけで削除した場合、その操作を行っている端末を間違っただけで削除してしまい登録システムへのアクセスに支障がでる懸念など、削除の反映には工夫が必要であると考えられる。現在の運用では、登録を削除した MAC 認証ホストの MAC アドレスは、MAC 認証用の RADIUS サーバの DB からの削除のみを行い、そのタイミングで MAC 認証により接続中であっても MAC 認証のログイン状態の解除(以降では**ログアウト処理**と呼ぶ)は行わず、次の MAC 認証ができない(接続しなすと MAC 認証での利用ができない)方針とした。なお、登録を削除された MAC 認証ホストについては、後述の 2.3 節、2.4 節のユーザ端末への影響から、利用者が少ないと考えられる深夜に一括して削除された MAC アドレスについての切断処理を行う事としている。

2.3. MAC 認証でのログアウト処理の影響

MAC 認証の利用終了の検出処理は、前述のとおりユーザ端末の離脱を確実に検出する事が困難であるため、スイッチの機能や別途の追加機能により以下の運用方法を検討した。(なお今回導入した認証スイッチのデフォルトの設定では、ログイン後の一定時間後に切断処理が行われる)

ログアウトの運用方法 1 として、導入した認証スイッチに設定できる最長のログイン時間である 1 日(24 時間)で切断処理をおこなう方法。方法 2 として、深夜に全ての MAC 認証についてログアウト処理を行う方法。方法 3 として、ログアウト処理はしない。について検討を行った。方法 1 と 2 では事前に周知することでログアウト処理されることをユーザに許容してもらう方法であり、後述の 2.4 節の影響を考慮すると運用

に適さないと判断。残る方法 3 ではログアウト処理を行わないため利用者への支障は出ないかまたはそれに等しいと考えて運用を続けたが、2.6 節の問題のためログアウト処理は何らかの方法が必要となり、ログアウト処理のユーザ端末への影響について評価を行った。

2.4. 通信中のユーザ端末でのログアウト処理によるパケットロスの評価

MAC 認証のログアウト処理により、ユーザ端末は一時的に通信できないタイミングが生じる。その時点で登録済みの MAC アドレスであれば、切断後の次のパケットの送受信時など次の通信開始時に MAC 認証が行われる通信可能な状態になる。この切断処理の通信への影響を具体的に把握するため、パケットロスの測定による評価を行った。

測定方法は、表 1 の 2 台の端末間で連続した通信を行い、1 台を MAC 認証で接続しておき、送受信中に MAC 認証の 1 台にログアウト処理を行い、パケットロスの測定を行った。なお評価に用いた認証スイッチは、本キャンパスネットワークで利用している認証スイッチで下限の性能である AX1230-24 (ファームウェアバージョン 1.3.D Build:127) を用いた。

表 1. 測定用端末のスペック

	接続	スペック
PC - A 送信側	MAC 認証	Core2DUO 3 GHz / Mem 4GB / GbEther / Fedora 8
PC - B 受信側	認証なし	Core2DUO 2.53 GHz / Mem 3GB / GbEther / Fedora 8

パケットの送受信にはネットワーク性能測定ツールの iperf [6]を用い、UDP 1Mbps (1470 byte を、11.7ms に 1 パケット送信)で 10 秒間送信し、その間に行った切断処理によるシーケンス番号の飛びとパケット受信の間隔を tcpdump で 10 回測定した。なお、切断処理を行わない場合の測定では 2 台の端末間のロスは 0 であり、また、測定の方の切断処理を行った場合もパケットシーケンスの飛びは 10 秒間の測定中に 1 回で、切断処理の時のみであった。

表 2. パケットロスの測定結果

	Min	Max	平均
パケットロス[個]	3	9	5.3
受信間隔[ms]	35	106	62.4

測定結果では、平均 62[ms] (Max 106[ms])程度の通信断であり、認証スイッチの処理である、切断処理によるフィルタ設定、認証していない MAC アドレスの検出、外部 RADIUS サーバでの認証処理、認証成功後のフィルタ解除処理、のような一連の処理を考慮する

とこれまでの認証スイッチ認証時間等の性能評価[7]を考慮すると、特段やむをえない程度のロスであるとは考えられる。

2.5. ログアウト処理のユーザ端末への影響まとめ

前述のログアウト処理によるロスのユーザ端末の通信への影響を考慮すると、平均や最小値は低いものの当然ばらつきがあり、一定数の長いロスは当然発生する。2.4 節の測定結果より、ログアウト処理によるロスは、認証スイッチ実機での測定よりスイッチのパケットのバッファ等で回避されないため、ロスが避けられてない。

MAC 認証が可能なゾーンでは WEB 認証も併用可能とするため WEB 認証ページのリダイレクトを設定しており、切断処理により MAC 認証がログアウト状態となると、その時点での HTTP 通信にリダイレクト発生し認証ページが表示される。

ユーザ端末でこのタイミングで WEB を利用していた場合には、WEB のセッションが切れる場合や、POST したデータを失う事が想像されるが発生確率はきわめて低いと考えていたが、新キャンパスネットワークの運用開始時に、先行して利用を開始した部局からこの様な苦情がセンター窓口寄せられていた。

大規模キャンパスネットワークで多数の利用者が長期間、この環境で利用することを考慮すると、この影響は大きく対策が必要であり、3 章での MAC 認証管理システムによるログアウト処理を行う事とした。

2.6. MAC 認証の重複ログイン対策

MAC 認証のログアウト処理を行わない場合、同一 MAC アドレスが異なる認証スイッチにログインした状態が生じる。例えば 2 箇所の認証スイッチで、2 重にログイン状態となったユーザ端末があっても、それらスイッチの上位側のスイッチでは MAC アドレスの学習アルゴリズムにより、後で学習したポートにのみその MAC アドレスが存在するようになるため、ユーザ端末がポートを移動して複数ログイン状態になったとしても、上位のスイッチを経由するようなインターネット等へのアクセスには不具合が生じない。また、同時にログイン状態のスイッチで、後でログイン状態となった方では実際にユーザ端末が接続しているため、同じく不具合は生じない。不具合が生じるのは、実際に存在しないログイン状態の認証スイッチで、そのスイッチで折り返す通信では、認証スイッチは直下にユーザ端末が MAC 認証で存在している状態であるため、存在していないポートにパケットが転送される事になり正常な通信が行えない。そのため、重複ログイン状態への対策もまた必要である。

3. MAC 認証管理システム

2 章より MAC 認証管理システムには、登録の削除を行った MAC アドレスへのログアウト処理、および重複したログイン状態の MAC 認証状態へのいずれもログアウト処理による対策が求められる。

3.1. MAC 認証管理システムの機能

ログアウト処理は、図 1 の構成図の認証スイッチ管理サーバにチェックの実行とログアウト処理を行うプログラムを作成し実装を行った。登録システムとの整合処理である、登録装置より削除された MAC 認証でログインしているホストのログアウト処理は、以下のようを行う。

－登録装置との整合処理：

- 1) 管理サーバよりフロアスイッチにアクセスしログイン中の MAC 認証ホストを一覧取得し保存
- 2) 取得したホスト一覧について MAC 認証用 RADIUS サーバ内 DB に存在するかどうかを検証
- 3) 登録されていないログインについてログアウト処理を行う
- 4) 全ての認証スイッチ約 450 台について 1) ～ 3) を繰り返す

－重複 MAC 認証ホストのログアウト処理：

- 5) 前の処理の 1) で得られた全 MAC 認証ホストより同一 MAC アドレスを検出
- 6) 重複ログインが見つかった場合は、その MAC アドレスの全てログインに対して同様にログアウト処理

ここで、「重複 MAC 認証ホストのログアウト処理」の 6) では、ログイン時刻の古い方のみをログアウト処理させる方法では、例えば、スイッチ A でログイン後にスイッチ B へ移動してログイン、さらにスイッチ A に戻っていた場合には、先にログインした古い方のスイッチ A のみ削除となり不十分となる。そのためログインの前後にかかわらず全てのログインに対してログアウト処理を行う。

3.2. MAC 認証システムの実装

認証スイッチへのログアウト処理や、MAC 認証でのログイン中ホスト一覧の取得では、スイッチに対してインタラクティブな操作を行うため、スクリプト言語の EXPECT を用い、SSH/TELNET でのスイッチへのログインと各種のコマンド実行およびその実行結果の取得を行う。

これらの処理結果は、キャンパスネットワークの管理者の ML に送信するとともに、スイッチの管理コマンド実行によるログアウト処理であるため通常のログアウトとはメッセージが異なり、ログ管理システムからメッセージ種別による絞込みで過去の処理の検索等も通常の運用として行う事が可能である。

4. システム評価

ログアウト処理を行う認証スイッチ管理サーバは、表1のPC-Bのホストであり、標準的な性能のPCを用いて運用を行っている。なおこのサーバは管理用であるためネットワーク接続には認証は用いない。

4.1. 登録システムとの整合処理の評価

チェックを行う時点でMAC認証中のホストと登録システムに登録されているMACアドレスとの比較を行い、チェックの時点で登録システムに登録されていないホストは、すなわちその時点で未登録のホストの切断処理は、毎日AM4:00より処理を開始し、およそ30分程度の時間で確認および未登録MAC認証の切断処理を行っている。表3に処理を開始した2009/12/08の週以降の週単位での処理数を示す。

表3. 登録削除による切断処理数

週間	処理数
12/08～12/14	8
12/15～12/21	13
12/22～12/28	7
12/29～01/04	2
01/05～01/11	6
01/12～01/18	1
01/19～01/25	8
01/26～02/01	4
02/02～02/08	4

週で集計した数を見ると、削除処理されるMAC認証はおよそ1日に多くても1件～数件程度であり、現在は新旧のネットワーク併用期間で新ネットワークに移行していない残り35%程度のホスト分が今後増加すること事を考慮しても特に処理性能の要求される処理数にはならないと考えている。登録削除による切断処理はこのまま現在の運用方法を継続し状況を確認するとともに、年度末に予想される機器の更新や部屋など居室の変更に伴い生じる変更についても引き続き評価を行う。利用者向けの説明に、このような定時の処理を行っていることを示しているため、特にこれに関する不具合の連絡は来ていない。

4.2. MAC認証の重複ログイン処理の評価

この処理は、4.1節の整合処理とあわせて同時に行っており、すべての認証スイッチにログイン中のMACアドレスについて調査するため、同時に重複ログインの検出も可能である。

表4にこの処理を開始した2009/12/08の週以降の週単位での処理数を示す。4.1節の整合処理と同様に1日1～数件程度の処理であり、移行の状況を考慮しても処理性能を要求される処理ではない。

表4. MAC認証の重複ログイン処理数

週間	処理数
12/08～12/14	4
12/15～12/21	12
12/22～12/28	8
12/29～01/04	2
01/05～01/11	10
01/12～01/18	10
01/19～01/25	8
01/26～02/01	16
02/02～02/08	16

4.3. リアルタイムの重複ログイン対策の検討

現在の運用では4.2節の重複ログイン処理も深夜に一括して実行しているが、多重ログイン状態はユーザ端末が移動する日中に生じると考えられる。この処理を日中でもリアルタイムに随時行い、重複ログインを検出する場合、その方法は基本的な動作としては、3.1節の「重複MAC認証ホストのログアウト処理」と同様の処理で実行可能である。以下の試行と評価は現在評価中の段階であり、テスト用として設置している認証スイッチを対象に動作の確認と測定評価を行っている段階である。

まず重複ログインをリアルタイムに検出するため、MAC認証のログインとログアウトのログをトレースし、ログイン状態を把握し管理する事で、対応可能である。この機能を実装するためには、図1の構成図でログサーバまたはRADIUSサーバでMAC認証に関するログを選択的に管理サーバへ送信する仕組みが必要となる。ここでサーバ間のメッセージをセキュアに送信する方法として、OpenSSLとサーバ証明書を用いたSSLによるメッセージ送信を用いた場合、表1の2台でPC-AからPC-Bに送信した場合、20回の試行結果では、89[ms]±3[ms]で随時ログイン/ログアウト状態の伝達が可能である。その後、ログアウト処理が発生した場合、認証スイッチに対してログアウト操作を行うが、これに要する時間は、同じく20回の試行結果では、平均1.446[s](Min:1.171[s] Max:2.252[s])程度でログアウト処理が完了している。これらの時間とあわせて、ログイン状態を管理しているperlによる管理プログラムで、MACアドレスを高速検索のためハッシュ化して管理している状態から検索する時間についても、ログアウト処理よりも十分短いと想定され、長くても3秒程度で処理が完了すると考えられる。3秒間の通信断は、前述のロスの評価からは十分に大きい値であるが、この通信できない時間は、ユーザ端末が移動し接続を変更した直後に生じるため、通信中のロスというよりは、接続開始時の待ち時間が延びることとなり、ユーザ端末の通信の影響は比較的少ないと想像される。

その他、深夜に1日1度のみ実行する場合と異なり、リアルタイムに常時監視とログアウト処理を実行する場合、重複ログインの検出に加えて次のような状態の監視も必要になる。例えば、無線LANでの接続時に、別の部屋のアクセスポイントを掴んでしまい、一時的に接続がばたつく場合が当然想定される。そのため、1度重複が検出された場合に、同じ場所での移動が極短時間に再度検出された場合は切断処理を繰り返さず、既定の期間ログアウト処理を見合わせるようなアルゴリズムの追加が必要である。

図2. に変更を加えたリアルタイムの重複ログイン対策の処理フローは以下のように変更される。

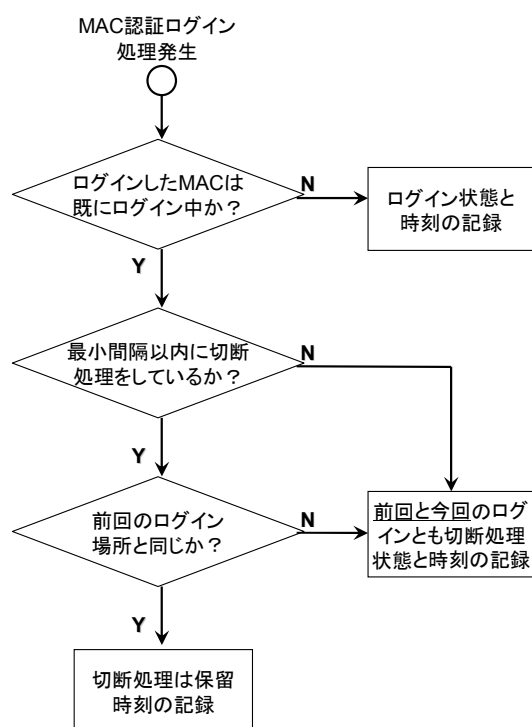


図2. リアルタイムの重複ログイン対策

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 での MAC 認証システムについて、その認証システムの概要とそれらの管理システムの構成についておよびその評価について述べた。

キャンパスネットワークとして利用者認証機能を安定的に提供する事が最重要であるため、本稿で示した MAC 認証管理システムの適用について運用を継続しながら現在も評価中である。評価で述べたとおり、現在はホスト数の接続状況からは一部の利用者が旧ネットワークを利用しているため、65%程度の負荷での運用であるが、処理を行うべき対象が比較的少ないため数倍程度の負荷でも継続可能であると考えている。

今回実装した MAC 認証管理システムで、全キャンパスを対象として運用中の 4.1 節 4.2 節の定時実行の整合処理については、利用者に運用方法を提示中であることもあり特に問題なく稼働中である。4.3 節の評価中のリアルタイムでの整合処理については、継続して評価を行いキャンパスネットワークでの運用できるように、利用者にわかりやすい動作でかつ十分の効果のあるアルゴリズムなど継続して試行と評価を行う。

本稿での MAC 認証管理システムは、ネットワーク側に機能を持つことを想定して実装を行ったが、当然ながら、利用者側で接続するポートを変える場合に、WEB 経由の管理画面から切断処理を自ら行い新しい方に接続を変えるといった操作も不可能な方法ではない。しかしながら、接続場所を変えるたびにこのような操作を忘れずにユーザ側が実行することが必要では運用上問題があると考えられるが、これらの方法についても継続して検討を行う。

まとめとして、現在行っている MAC 認証への管理システムでの対策により、MAC 認証の運用には特に問題はないと判断している。

謝辞

HINET2007 の構築および運用に尽力して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します。また、本研究の一部は日本学術振興会科学研究費補助金課題番号(18700063, 19300019)の支援を受けて実施しています。ここに記して謝意を表します。

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] 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
- [4] 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
- [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] NLNR/DAST: “The iperf project”, <http://dast.nlanr.net/Projects/Iperf/>.
- [7] 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