大規模キャンパスネットワークにおける MAC アドレス認証端末の移動管理

Management of MAC Address Authenticated Host for Large-Scale Campus Networks

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

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

広島大学 情報メディア教育研究センター
Information Media Center, Hiroshima University

概要

イントラネットワークへのセキュリティ対策として，認証ネットワークと呼ばれるユーザ端末のネットワーク接続に認証を用いる事で，権限の確認や利用記録を行い，不正利用を防止する対策が現在では多くの組織で導入されている．認証操作では利用者へのユーザビリティの高い利用として，利用者が自身の ID を認証用の WEB ページへ入力して認証を行う WEB 認証や，ユーザ端末のネットワーク接続時に端末の MAC アドレスの登録の有無により認証を行う MAC アドレス認証等が利用されている．WEB 認証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，実用的な方法が確立されているが，MAC アドレス認証は IP アドレスが不定な状態でも認証が行えるため，WEB 認証の手法をそのまま適用することができない．そこで本稿では，MAC アドレス認証の利用についてこの問題について整理するとともに，大規模キャンパスネットワークでの運用を前提とした MAC アドレス認証の運用方法として，MAC 認証したユーザ端末に不具合の生じる移動を管理する事による対策について述べ，構成事例と性能評価について報告する．

キーワード

MAC アドレス認証，キャンパスネットワーク，認証システム

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におけるセキュリティ対策として，認証ネットワークが現在では多くの組織で導入されている．認証ネットワークでの認証方法として利用者へのユーザビリティの高い WEB ブラウザを用いた認証（以下では WEB 認証と示す）が多く利用されているが，WEB 認証が困難な機器や WEB ブラウザを内蔵しない機器でも認証可能な MAC アドレス認証（以下では MAC 認証と示す）も利用される．

WEB 認証は，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ており，認証操作を行う WEB アクセスによりユーザが認証して利用する端末（以下ではユーザ端末と示す）の IP アドレスを自動取得し，認証成功後の接続状態の確認等をこの IP アドレスで行なうといった実用的な方法が確立されている．しかしながら MAC 認証の場合にはユーザ端末が送信したパケットの送信元

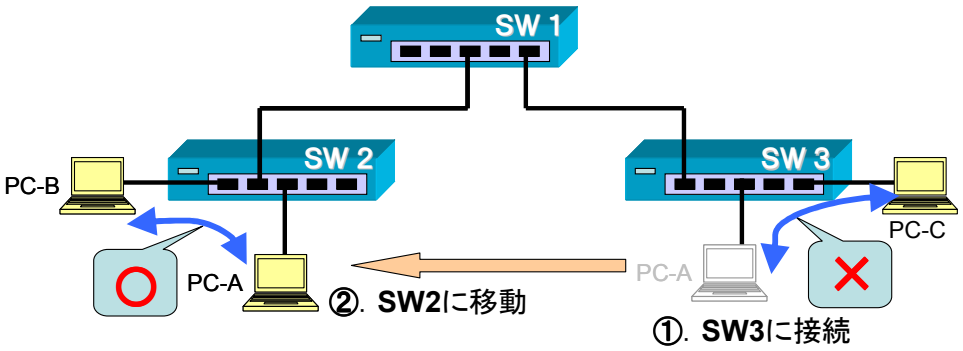

図 1　MAC 認証したユーザ端末の移動による通信障害の例

MAC アドレスによる認証のため，場合によってはネットワークに接続したユーザ端末が DHCP で IP アドレスを取得する際のリクエストパケットで認証が行われるなど，IP アドレスが不定の状態が当然ながら含まる．そのため，WEB 認証では可能であったユーザ端末の IP アドレスへ PING や ARP によっての接続状態を確認する方法をそのまま適用することができず，MAC 認証ではユーザ端末の接続終了を検出する事が困難である．

広島大学で運用されているキャンパスネットワーク HINET2007[1]では，ユーザ端末は原則として認証利用する事を必須としており，WEB 認証での利用を推奨とするものの，キャンパスネットワークの隅々全てで認証利用とするために約 460 台の認証スイッチで WEB 認証と MAC 認証を併用して提供しているが，MAC 認証したユーザ端末の接続終了の扱いについては 2 章に示す導入時には想定していない問題点が生じた．

そこで本稿では，大規模キャンパスネットワークでの運用を前提とした MAC 認証の運用方法について述べ，構成事例と性能評価について報告する．以下では，MAC 認証利用における運用上の問題点について 2 章で整理し，3 章でこの問題へ対処としてユーザ端末の移動管理を行う MAC 認証システムの構成について述べ，4 章で性能評価を行い，最後に 5 章でまとめについて述べる．

2. MAC 認証の運用上の問題点

本章では MAC 認証の運用上の問題点をまとめる．

2.1. MAC 認証したユーザ端末の移動による重複ログイン問題

認証スイッチでは，MAC 認証したユーザ端末が接続しているポートから離脱しても，前述のとおり存在の確認ができない事からユーザ端末の MAC アドレスが認証状態のまま接続していたポートに残り続ける．一部例外として，移動先が同一認証スイッチの別のポートであった場合に，認証スイッチによってはローミング機能を持ち，移動前のポートでの MAC 認証状態の解除と移動後のポートでの MAC 認証状態の開始が自動的に処理可能な場合がある．

他方，移動が異なる認証スイッチ間での場合は，図 1 に示す様な MAC 認証の状態が残る事による通信の障害が生じる．図 1 は，①の操作で一度 SW3 に接続した PC-A が，②の操作で SW2 へ移動して接続した状態を示している．ここで SW3 は，PC-A が移動した後も PC-A の離脱を検出できないため，SW3 は PC-A 宛のパケットを PC-A が接続していたポートに転送し続ける．そのため，PC-C と PC-A との間では通信が不可能な状態が生じる．この場合でも，移動先では PC-B と PC-A の通信など SW2 での折り返し通信や，PC-A が SW2 に移動したことを MAC アドレスの学習により検出可能な上位の SW1 側と PC-A との通信は正常に可能である．PC-A の利用者から見ると，移動先の他の端末との通信やアップリンクの通信に問題ないため気づきにくい障害である．

しかしながらこの様な不具合に気づいた利用者より，不具合が起きているという連絡が所属している情報センター窓口まで時々来ていたが，気づきにくい障害であるためキャンパス内では潜在的にもっと多くの箇所で同様の障害が起きていたと推測している．そのため MAC 認証したユーザ端末が認証スイッチ間を移動した場合には，MAC 認証の重複ログイン状態が継続しないように，移動の前に接続していたスイッチ側において接続終了の処理（以下ではログアウト処理と示す）が必要である．

2.2. MAC 認証利用時におけるユーザ端末の意図しないログアウト処理の影響

認証スイッチによっては，ARP キャッシュの保持時間程度の無通信状態が続くと強制的にログアウト処理が行える機能がある．しかし利用中であるにもかかわらず不必要に MAC 認証のログアウト処理を行うと，以下に示すユーザ端末が一時的に通信できない通信断が生じる事と，WEB 認証併用時のリダイレクトの問題が生じる．

・通信断による通信のロス　ログアウト処理で一時的に認証断が発生した際にも，MAC アドレスの登録が有効で再度の認証が可能であれば，認証断後の次のパケット送信時に MAC 認証が行われ通信可能な状態に戻る．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，ログアウト処理による通信断は，文献[2]の結果より最下位機種で，平均 62[msec] (最大 106[msec])程度の通信断が生じる．この間に認証スイッチでは，ログアウト処理（ブロックする様にフィルタを変更する処理）と MAC 認証処理（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）の内容を考慮するとやむをえない時間程度であるが，スイッチのバッファでも回避できていないパケットロスが発生する．

・WEBリダイレクト発生の問題　WEB 認証では，ユーザへの利便性のために未認証時の WEB アクセスを認証ページへ誘導するリダイレクト機能がよく用いられるが，この機能を MAC 認証と同一ポートで併用利用すると次の問題が生じる．MAC 認証したユーザ端末で MAC 認証の認証断の時にユーザが WEB アクセスを行っていると，ユーザ端末が未認証状態のため，その直後の WEB アクセスにリダイレクトが発生し，表示するページが認証ページに置き変わってしまい，WEB のセッションが途切れる事や HTTP の POST により送信したデータが失われる場合がある．

以上2つの理由より ARP キャッシュの保持時間での自動切断などによる不必要なログアウト処理はユーザ端末への影響が大きく可能な限りさけるべきである．なお，WEB リダイレクトの問題は，問題が生じることを確認した時点では発生しても確率は極めて低いと考えていたが，学内で先行して認証利用を開始した一部の部局からセンター窓口に続けて苦情が寄せられたため，利用経過時間等でのログアウト処理や，利用者の少ない深夜にログアウト処理を一括で行っていた運用を中止し，それ以降は，夜間に全ての認証スイッチで MAC 認証の認証状態を確認して 2.1 節の重複ログインが見つかった場合のみログアウト処理を行う設定 [2] のみとした．

2.3. MAC アドレス詐称へのセキュリティ対策

MAC アドレスを用いた認証方法には，MAC アドレスの詐称による問題が懸念される．Linux やブロードバンドルータ等の機器では，ネットワークインタフェースにあらかじめ設定されている MAC アドレスとは異なる MAC アドレスとして動作させる事が可能であり，この機能により認証可能な MAC アドレスを詐称し，認証を回避してネットワークを利用する方法が可能である．この問題への対策として 2 つの方針で対策を講じている．

・MAC 認証が可能な場所の制限　学外からの訪問者や不特定多数の利用が想定される教室や会議室等の他，キャンパス内主要箇所で利用可能な全学予算で整備した大学公式の無線 LAN 等では，WEB 認証での利用のみ可能とし MAC 認証利用は不可とした．

・MAC 認証で利用するユーザ端末の利用範囲の制限　MAC アドレスの登録時に認証利用が可能な範囲を限定し，範囲内のみで利用可能となる方法を取っている．具体的には，単独の部屋や同じ研究室の部屋数箇所などを，1 つの管理者（研究室の場合は主にその研究室の教員）による管理範囲としてゾーンと呼び，このゾーン毎に別の VLANID を割り当てて独立させ，MAC 認証時には MAC アドレスとこの VLANID の組み合わせで認証する方法としている．そのため，異なる管理者の部屋からは VLANID が異なるため詐称による認証が不可能になる．

これらの対策により，MAC 認証の詐称による不正アクセスが発生した場合にも，発生場所の部屋がゾーンの範囲で限定され，また，利用者も特定のゾーン内の構成員に限定される事で，MAC 認証を利用する事におけるセキュリティ対策のコストと効果を考慮した結果，このような運用形態 [3] とした．

2.4. MAC 認証の運用上の問題点のまとめ

2.2 節より不必要な MAC 認証のログアウト処理は影響が大きく，また，2.1 節の重複ログイン問題も避けるべき問題であるため，MAC 認証のログアウト処理は障害が生じるユーザ端末の移動による重複ログイン状態が発生する時にのみ実行する方針とした．ここで， MAC 認証したユーザ端末がある認証スイッチから離脱する場合は，離脱と移動の 2 つに分けられ，離脱であった場合にログアウト処理を行わない事で認証スイッチに認証状態が残り続ける事の影響を検討したが，ARP キャッシュの保持時間程度無用なパケットの転送が続くのみで障害とはなら無いためである．

なお関連技術に，認証ネットワークにおけるユーザ端末の移動に関して無線 LAN でのローミング技術があり，無線 LAN スイッチとこれに対応した無線 LAN アクセスポイントを組み合わせ，アクセスポイント間のユーザ端末の移動を，無線 LAN スイッチ側で行いスムーズなローミングを提供する技術である．中でも標準化された 802. 11r では高速にローミングするために認証手続きを高速に行う方式等が定義されているが，対応しているアクセポイントのみで動作可能な事とユーザ端末側がこの方式に対応していなければならないという理由など，現在のキャンパスネットワークでは利用できる技術となっていない．

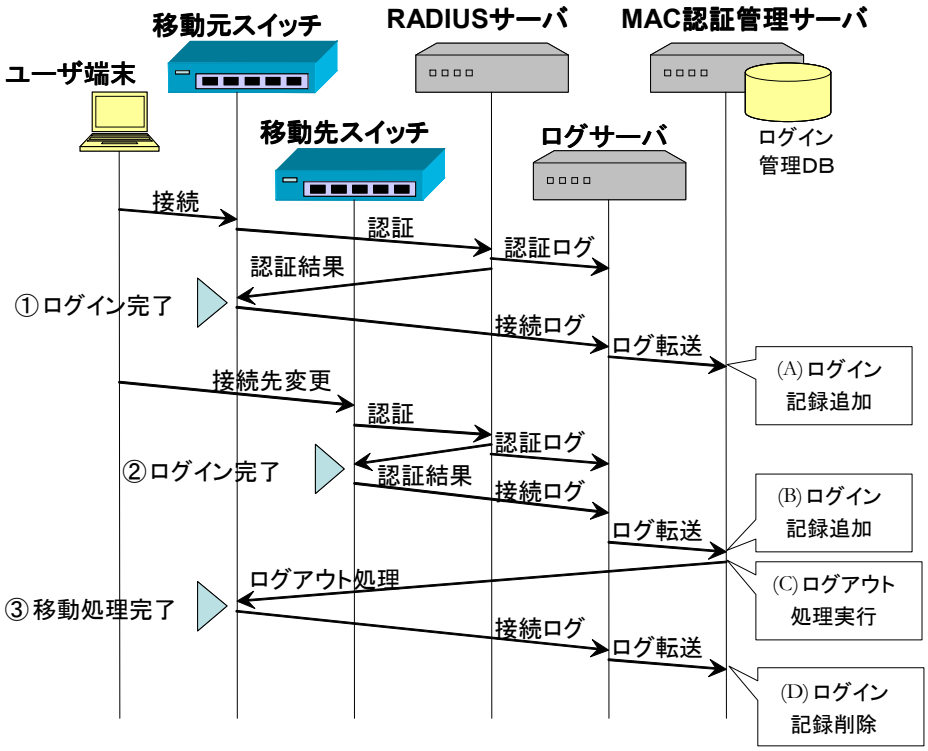

図 2　MAC 認証したユーザ端末の移動時における処理フロー

3. MAC 認証したユーザ端末の移動管理

本章では構築した MAC 認証管理サーバにより MAC 認証したユーザ端末の移動の管理と，移動検出時のログアウト処理について構成例およびその動作を示す．

3.1. MAC 認証システムの全体構成

MAC 認証システムには，MAC 認証で利用する MAC アドレスを登録する手段が必要であり，本学での構成例 [4] や 新潟大学での実装 [5] の報告の通り，ある程度の管理権限を持つ管理者に登録機能を提供する事で，ネットワークを管理する側の管理コストの低減とユーザ側の利便性の両方に配慮した構成が可能である．本稿での MAC 認証システムもそのような登録システムを併用する事を前提としている．

図 2 にユーザ端末が移動元スイッチに接続後に移動先スイッチへ移動した場合の MAC 認証システムを含めた全体の処理フローを示す．なお処理概要は以下のとおりである．

・ユーザ端末の移動元スイッチへの接続　ユーザ端末が移動元スイッチに接続し，RADIUS サーバで認証が行われ, 利用開始可能状態 である図 2 の①の時点まででユーザ端末側としては接続処理が完了する．MAC 認証管理サーバでは，①でログイン完了した接続ログをログサーバより取得し，ログイン状態を保持管理するための内部のログイン管理ＤＢへ登録する．

・ユーザ端末の移動先スイッチへの接続　ユーザ端末が移動先スイッチに移動して接続する場合も，ユーザ端末側からみると②のログイン完了までほぼ同様の接続処理がおこなわれ，MAC 認証管理サーバでは移動後の接続ログと以前のログイン記録より移動を検出する．移動の検出があると，移動元に残っている認証状態を MAC 認証管理サーバより直接スイッチを制御してログアウト処理を行う．その後で，このログアウト処理により生じる移動元スイッチからの接続ログ（ログアウトのログ）を受け取る事よって，MAC 認証管理サーバは該当するログイン記録の削除を行う．

3.2. MAC 認証管理サーバの構成

図 2 の MAC 認証システムの全体構成において，RADIUS サーバおよびログサーバは既設のサーバであり，ここに MAC 認証管理サーバを追加して MAC 認証システムとして動作する構成とした．

MAC 認証管理サーバでは，ログサーバからのログの取得に OpenSSL を用い，SSL により通信路の暗号化と 2048 ビット長のサーバ証明書によるサーバ確認を行う．認証スイッチへのログアウト処理は，スクリプト言語の expect を用い，スイッチのコンソールへ SSH (最下位機種では SSH 非対応のため telnet)を起動してログインし，管理コマンドをスイッチ上で直接実行する方法とした．

その他，ユーザ端末が意図せずに移動を繰り返す場面として，無線ＬＡＮの利用時に複数のアクセスポイント

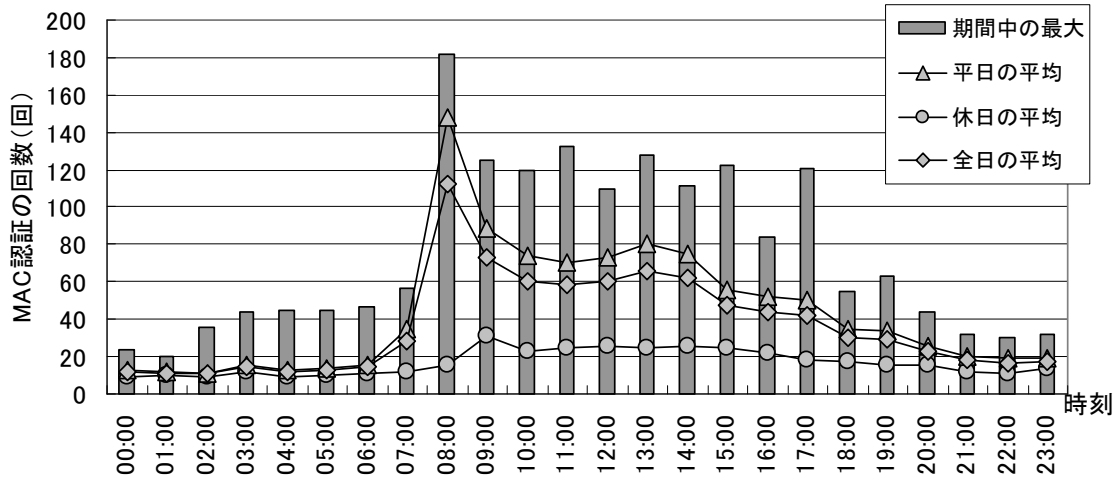

図 3　1 時間毎の平均 MAC 認証回数と最大認証回数 (2011 年 6 月)

間で移動を繰り返す事が予想されたため，同じ認証スイッチ間を行き来する移動で，移動して元の場所に戻るまでの時間が 30 秒以内の場合には，一定時間（初期設定では 60 分間）ログアウト処理は行わない制限を設けるなど，ログアウト処理の動作アルゴリズムを適宜見直す事を考慮して，接続ログの監視および認証スイッチへの管理操作の発行を行う管理プログラムはスクリプト言語の perl で実装した.

4. 性能評価

現在運用中のキャンパスネットワーク全体での利用を対象とするため，はじめにその様子について述べる.

MAC 認証用として用意している MAC 登録システムのデータベースには，登録済みの MAC アドレス数が 2011 年 6 月 30 日の時点で 9724 台が登録されている. また，本システムが処理すべきイベント数である MAC 認証の利用開始数（接続開始のログ数）について，2011 年 6 月の 1 ヵ月間の様子を図 3 に示す．グラフは時間帯毎のそれぞれ 1 時間の間に行われた MAC 認証の回数で，折れ線グラフに，「平日」，土日祝の「休日」と期間中全体の「全日」, について 1 時間毎の平均回数を示しており，時間帯毎の期間中最大値を棒グラフで図中に示している. グラフより 1 時間の間に処理すべき総数は図 3 より最大でも 200 程度，1 日の処理数は最大認証回数の累計でも 2000 件程である．データベースへの登録 MAC アドレス数に比べて認証回数が多くない理由は，多くの MAC 認証で利用しているユーザ端末がサーバの様に同一のポートで固定的に利用されるものが一定数あるため，移動等による MAC 認証によるログインが発生しにくい利用が多いと推測される．逆に，図 3 の認証数は多くは移動等で MAC 認証接続開始を行うユーザ端末であると考えられる．なお，WEB 認証の場合は，始業時刻の午前 8:30 前後に特に集中する傾向 [6] がみられたが MAC 認証は 8 時頃にそれ以降と比べて 1.5 倍程度の差はあるものの，始業から終業時刻の間は平均的に認証が行われており，ピーク値でも 10 分間に 30 台程度の認証数であった.

4. 1. 同時処理性能の測定

本システムの処理対象である MAC 認証したユーザ端末の移動の検出からログアウト処理が完了するまでの処理時間について，負荷テストとして同時に処理する台数を増やし，処理に要する時間の測定を行った.

測定方法は，図 2 の構成でユーザ端末として MAC 認証用クライアントを用意し，①の移動元の認証スイッチへの指定の台数分の MAC アドレスでパケット送信し MAC 認証でログインした状態から，②の移動先へ同じく指定の台数分の MAC アドレスでのパケット送信を行い移動した状態を再現し，③の移動処理を発生させその処理が完了までに要する時間についての測定を，運用中の認証ログ及び接続ログを収集するログサーバを用い，接続ログの時刻表記より求めた．測定で使用した機器の仕様は表 1 に示すとおりである.

これらの機器構成により 1 度に移動する MAC 認証のユーザ端末数が 5 台 ～ 30 台の場合について測定を行い，その結果を図 4 に示す．グラフは，横軸の各台数において 5 回の試行を繰り返して測定を行い，処理時間の平均値を折れ線グラフで，各台数での処理でその最大と最小の処理に要した時間をエラーバーで表示している. 同時処理台数の 5 ～ 30 台の様子では，同時に処理する台数の増加に応じて処理時間が増加する傾向は確認できるが，30 台の同時移動の際にも平均 8～12 秒程度，最も

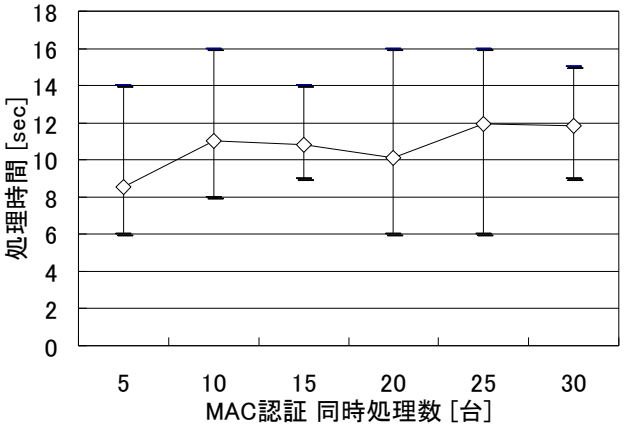

図 4　MAC 認証ユーザ端末の同時移動時の処理時間

表 1　測定に使用した機器の仕様

RADIUS サーバ（MAC 認証用 ）	
CPU	Inte Xeon X5355 @2.66GHz x2
Memory	4GB
OS	CentOS 5.0
Package	FreeRADIUS 1.1.7, OpenLDAP 2.3.41
ログサーバ（ 認証ログおよび接続ログ用 ）	
CPU	Intel　Xeon　X5355 @2.66GHz x2
Memory	4GB
OS	CentOS 5.0
Package	PostgreSQL 8.1.9
MAC 認証管理サーバ	
CPU	Intel Core2Duo E6550 @2.33GHz
Memory	3GB
OS	Fedora 8
Package	FreeRADIUS 2.0.5
MAC 認証用クライアント	
CPU	Intel Core i7 2600 @3.4GHz
Memory	8GB
OS	CentOS 5.6
認証スイッチ	
機種名	Alaxala 2430S
CPU	PowerPC 533MHz
Memory	256MB
ログサーバ（ 比較用 ）	
CPU	Pentium D 3.0 GHz
Memory	256MB
OS	CentOS 5.5

遅い場合でも 16 秒前後で処理が完了している． 事前の統計から予想される同時処理すべき台数は十分処理可能であると確認されたが，実際には使い始めに若干の時間

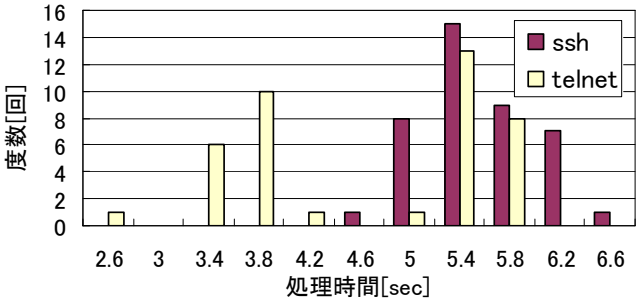

図 5　MAC 認証のログアウト処理に要する時間

の間，通信相手によっては不具合を感じる事がある程度の処理時間を要するため， MAC 認証したユーザ端末を移動させた場合は，使い始めに十数秒程度一部の通信に不具合が出る事があると案内しておく運用でカバーする事としている．なお，測定時における MAC 認証管理サーバで保持する MAC アドレスのログイン数は，すべての測定において 10000 台登録された状態から動作を開始しており，測定の間に MAC 認証ログインの失敗やログアウト処理の失敗等は発生しておらず，測定自体で問題は確認されなかった．しかしながら測定結果の図 4 の様子から同時処理台数に因らない，処理時間のばらつきや処理に要する最大の時間についての考察を行う．

4.2. MAC 認証のログアウト処理における処理要素毎の考察

移動の検出からログアウト処理完了までの処理時間を考察するため，その間に行われる処理を列挙し，それぞれサーバでの処理時間およびサーバ間でのログ等の転送時間等について考察を行う．

A. MAC 認証用クライアントの処理時間 MAC 認証用クライアントでは，1 台の LinuxPC で複数台 MAC 認証を行わせるため，ネットワークインタフェースの MAC アドレスを 1 回の認証毎に修正し，10 ～ 20 [msec] の間 PING コマンドで認証のためのパケット送信しこれを指定台数分繰り返し行っている．1 つの MAC 認証の処理あたり，20～30 [msec] 程度の処理時間を必要とするため，台数が少ない場合は測定結果への影響は小さいが，移動台数が 30 台の測定においては，最も遅い測定に 1 秒弱ほどの処理遅れを生じさせる．

B. RADIUS サーバでの認証時間　文献 [6] の結果より，既設の MAC 認証用 RADIUS サーバの構成では，1 秒間に 650 以上の同時認証処理が可能で，RADIUS 認証に要する時間は多重度が高い場合でもは数十 [msec] の処理時間で完了するため，全体の処理時間への影響はごく小さい．

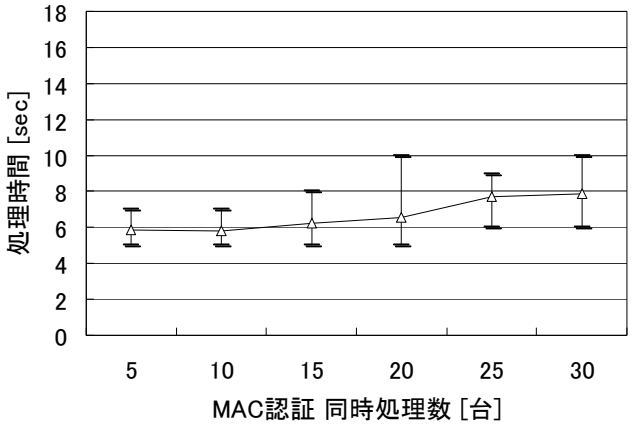

図 6　比較用ログサーバでの MAC 認証ユーザ端末の同時移動時の処理時間

C. MAC 認証管理サーバでの処理　ここでの処理は重複ログインの検出と検出後のログアウト処理である．まず重複の検出等ログイン管理 DB を用いる処理は，文献[4]の結果より，MAC 認証管理サーバに 10000 台がログイン中の状態で，ログイン記録からの参照とログイン／ログアウト記録の書き込みに要する時間は，それぞれ平均 3.4[msec]と平均 20[msec](最大 25[msec], 最小 19[msec])程度であり，全体の処理時間への影響はごく小さい．

認証スイッチへのログアウト処理のみを単体で動作させた場合の処理時間を図 5 に示す．図 5 の測定は，それぞれ SSH と telnet を用いて認証スイッチへ MAC 認証のログアウト操作を 50 回行った際の, 処理時間の区分毎の度数をグラフ化したものである．測定に用いている認証スイッチでは telnet および SSH での管理操作が可能であるが，グラフより telnet の場合には半分に近い時間で処理が完了する場合もあったが，可能な限りより安全な SSH を用いる．ここでの処理時間である 5〜6 秒程度は処理に要する時間の主要因の 1 つであった．

D. 接続ログの転送時間　接続ログの転送時間は，ログサーバでログを受け取りファイルへの書き出すまでの処理時間および出力されたログを MAC 認証管理サーバへ転送する処理時間が対象となる．

運用中のログサーバでは syslog 形式で認証スイッチから受け取ったログを，管理者向けの機能として用意しているログの検索や統計処理のために一度データベースに保管を行う事としており，あわせて運用中のある程度の負荷がかかった状態での測定であったため，図 4 の処理時間にはある程度遅延が予想されていた．運用中のサーバのためパケットダンプ等による測定が困難であったため, 比較用として syslog をファイルに書き出す動作のみを行うログサーバを別に用意し，認証スイッチからログサーバへ送信するログと同じログを比較用のログサーバに出力する構成で測定を行った．測定方法はログサーバが異なる点以外は 4.1 節と同じ条件で測定を行い，その結果を図 6 に示す．ログサーバを変えた際にも多少の処理時間の揺らぎは生じるが，図 4 の運用中のログサーバと比較すると処理時間のばらつきや遅延の程度が改善されているため，処理時間の短縮にはログサーバの見直しが必要であることが分かった．

ログサーバから MAC 認証管理サーバへのログ転送処理では，文献[2]の結果より今回の測定と同じ条件である 2048 ビット長のサーバ証明書を用いた SSL でのログの転送遅延は, 89[msec]±3[msec] であり全体の処理時間と比較すると処理時間への影響はごく小さい．

5. まとめ

本稿では，キャンパスネットワークでの MAC 認証の運用で問題として生じた，重複ログインの問題および不必要なログアウト処理を行わない方法として，MAC 認証したユーザ端末の移動を管理し，移動が検出された際にログアウト処理を実行する方法について実装ならびに評価を行った．特に，キャンパスネットワークでの実際の運用が本稿の目的であるため，MAC 認証利用者にとって不具合の少ない状態で利用できるようにすることに特に重点を置いて方針を決定した．

4.1 節の現行の運用環境での評価では, 処理に要する時間から利用開始時に十数秒程度，一部の通信に不具合が出る事があると案内して運用する事が必要であるという結果であったが，4.2 節の処理要素の考察より，B. の RADIUS サーバでの認証時間，C. の MAC 認証管理サーバでの重複ログインの検出処理, D. の接続ログの SSL での転送については十分短時間で処理可能であることが確認され，また，D のログサーバでの接続ログの処理について改善を行う事で図 6 の結果に近い処理時間が見込まれ，その場合には WEB アクセス等でユーザが通常待てる限界といわれる約 8 秒程度に改善が見込まれる．

その他，本稿で構築した MAC 認証におけるログアウト処理は, 本来は同様の機能が認証スイッチに実装され, 設定して利用できる環境が望ましいため，認証スイッチで実現する方法についても今後検討を行いたいと考えている．

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致します．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

(2350008900) 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

[2]田島, 近堂, 岸場, 大東, 岩田, 西村, 相原, ”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”, 電子情報通信学会技術研究報告. IA, インターネットアーキテクチャ 108(460), pp.265 - 270, 2009

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

[4]田島, 近堂, 岸場, 大東, 岩田, 西村, 相原, ”大規模キャンパスネットワークにおけるMACアドレス認証システム”, 情報処理学会 マルチメディア・分散・協調とモバイル(DICOMO)シンポジウム 2010 論文集, pp.1159 - 1165 ,2010.

[5] 浜元, 五十嵐, 青山, 三河, “ホスト登録システムを利用したネットワークアクセス認証システムの運用” , 情報処理学会研究報告 2010-IOT-9, pp. 1 - 6, 2010

[6]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