社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2007－DSM－47 (4)
2007／9／21

キャンパスネットワークへの認証システムの導入

前田 香織　　河野英太郎　　北村俊明

広島市立大学大学院情報科学研究科
〒731-3194 広島市安佐南区大塚東 3-4-1

概要
利用者認証は一時的な持込み PC の利用や共同利用場所（端末室など）だけでなく，大学構成員の居室をも含む日常的なネットワーク利用においても必要になっている．本稿では，広島市立大学で必要となった日常的なネットワーク利用の認証システムについて，その導入経緯，および懸案となった Web 認証機能に関する評価や問題点について報告する．また，システム導入前後の学内ネットワークの利用状況の変化や運用形態の変化について述べる．

Installation of a Network Authentication System in Campus Network

Kaori MAEDA　　Eitaro KOHNO　　Toshiaki KITAMURA

Graduate School of Information Sciences, Hiroshima City University
3-4-1 Ozuka-Higashi, Asa-minami, Hiroshima, 731-3194, Japan

Abstract
Network authentication is necessary to improve network security not only in temporal use of a campus network by visitors and educational use at terminal rooms but also in laboratories of teachers and students for their daily use. In our university, the network authentication in daily use of the campus network is required, too. In this paper, we describe the process of installation of a network authentication system and its performance evaluation. Also, we mention the drastic change of network usage before and after network authentication and some problems of the current authentication product.

1．はじめに

大学など教育機関のネットワークの利用者の認証システムの導入が進んでいる．特に，複数が共同利用する教育端末室や公開端末室など教育内容や利用環境に応じて柔軟に対応できるようにという要求から，大学独自の利用認証システムが開発されている[1][2]．また，大学構成員の持ち込み端末の利用や学会などのイベント開催時における情報コンセントや無線LANの提供のための利用者認証システムも多々開発されている[3][4][5]．さらに，各社から製品として認証装置が市販されるようになった．特にここ１～２年は，サブネット単位に個別に装置を設置するのでなく，複数サブネットを同時に管理できるようスイッチと連動して動作する認証スイッチの開発が目覚しい．

従来，利用者認証システムの導入場所は特定，または不特定の複数の利用者がネットワーク利用するところが多く，広島市立大学（以降，本学）でも，2004 年より持ち込み端末の利用可能場所である学生会館（食堂），図書館，情報処理センターの一部，中庭において，製品 FEREC[6]により有線，または，無線 LAN の利用者認証を開始した[7]．2006 年 3 月には，キャンパスネットワークサービスと商用の無線 LAN アクセスサービス（NTT-西日本フレッツスポット）とを連携した無線 LAN 利用を始めた[8]．利用者アカウントによるサービスの振り分け装置を設置し，地域の ISP の VLAN サービスと連動することにより，２つ

のサービスを共存するサービスである.

一方,従来は固定的にキャンパスネットワークを利用する場所として,利用者認証を行っていなかった教員や学生の居室,研究スペースにおいても利用者認証の重要性が高まっている.本学においてもこのような必要性が生じてきたため,2007年6月から2学部で教員の居室や研究室でのキャンパスネットワーク利用の認証を開始した.行政機関や民間企業と異なり,大学ではネットワークを利用するPCが多種であること,利用目的や方針が多様であることから,一律の方針で利用者認証システムを導入することは容易とはいえない.本稿ではこのような環境での利用者認証システムの導入経緯と導入後の運用状況について報告する.

本稿では,2章で本学における利用者認証システムの導入の背景と認証システム要件ついて述べ,3章でシステムの構成を述べる.さらに4章で導入直後とその後の利用状況を,5章で今後の課題についてまとめる.

2. 利用者認証システム導入の経緯

2. 1 背景

本学ではネットワークに接続する機器の台数の多い情報科学部では,研究室や実験室単位でサブネットを割り当て,その中でIPアドレスの管理をしている.その他の2学部(国際学部と芸術学部),平和研究所と事務局では,PCなどをキャンパスネットワークに接続する際には,教員または事務局職員がアドレス管理者として,情報処理センターにIPアドレスを申請し,固定アドレスが割り当てされてきた.

しかし,長い間に以下のような事態が生じていた.

- 申請されたIPアドレスがその管理者が退職,異動した後も使用され続けている.
- 申請されたIPアドレスが申請当初とは異なる場所やPCで使われている.
- 複数の利用者がPCローカルの認証なく利用している.

これらはいずれも管理者不在のPCなどが存在している状態である.特に教員や職員が申請し,実際には学生が利用しているPCは共同利用のものが多く,利用者の特定が困難な状況となっていた.場所によっては学外者が出入りできる部屋もあり,極めて問題のある状況となっていた.

さらに,国際学部と芸術学部ではネットワークの配線や機器の制約で,教員と学生の居室や研究室ごとにサブネット分割されていないため,問題が発生した際の波及範囲が広いことも問題であった.

このような背景から,利用者認証の機構を導入し,問題発生時の利用者の特定を可能にすること,認証により利用者のネットワーク利用に対する意識(安全性等に関して)を高めることを目的として,これら2学部に利用者認証システムを導入することとした.

2. 2 認証システムの要件

現行の利用者認証の方式として,a) MACアドレス認証,b) IEEE 802.1x認証,c) Webブラウザ認証が一般的である.今回導入する学部では,利用者のPCがWindows, Mac, PC Unix(Linuxなど)と同一種類ではなく,クライアントソフトの導入が必要なb)の方式は難しい.また,対象の学部ではMACアドレスを申請することは必ずしも容易ではなく,その手順を確立できないので,a)の方式も難しい.結果的に本学では利用者の環境を選ばないc)を使用することとした.

認証の安全性と利用者のスキル等を考慮して,本学におけるWebブラウザ認証システムの要件として以下を掲げた.

1) 認証にはhttpsを用いる.
2) 認証ページの強制表示(ネットワーク利用開始時に認証用のWebページへhttpリダイレクトする)機能をもつ.このとき,httpとhttpsのいずれがトリガになってもhttpsでリダイレクトすること.
3) 1台の認証スイッチで同時ログイン/ログアウト数20を想定して支障なく使用できる(1台の利用者総定数は100).

3. 認証システム構成検討と事前評価

3. 1 システム構成

認証システムの構成概要を図1に示す.導入必要な時期(2007年6月)に2.2のシステム要件をほぼ満たすものとして,認証スイッチに日立電線株式会社のAPRECIA 4348GT [9]を採用することとした.

認証スイッチと利用者のPC等の間には既存のスイッチが入っているケースもある.安全性を考えると,認証スイッチの配下に別のスイッチが設置されないことが望ましいが,配線の制約から今回は部分的には既設置のスイッチを避けられなかった.

認証システム導入に伴い,利用者のPC類は

プリンタや公開Webサーバ等を除いてDHCPによる自動割り当てに変更した．DHCPサーバは冗長化構成をとっている．アドレスのリース時間は講義室では10分，その他教員の居室等は30日としている．

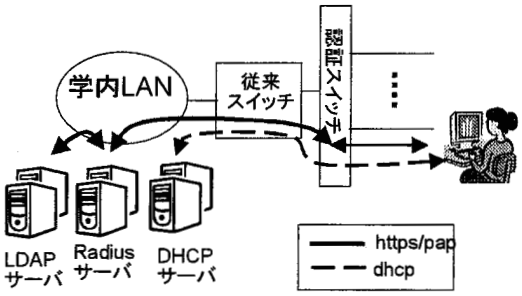

図1．認証スイッチ構成

認証の有効時間に関しても考慮が必要なポイントである．現行の多くの認証スイッチでは，ログアウトの判定を一定時間でのタイムアウトかICMPによるポーリングタイムアウトによって行っている．しかし，後者は利用者端末にICMPを許可するよう設定が必要で，本学のようにエンドユーザに設定を委ねることを避けたいことやユーザのネットワーク利用安全性向上の観点から望ましくない．このことから，本学では前者を採用したが，タイムアウト時間の設定も配慮が必要である．教員は多くの場合，自分専用でPCを利用しているため，短いタイムアウト時間では使い勝手が悪い．結局，1コマ分の講義時間は越える時間とし，現在は2時間とした．

しかし，複数の学生が共同利用しているPCの場合，タイムアウト時間内には改めて認証プロセスを経ることなく，既に認証済みのユーザの権限で利用することができてしまう．そのため，本学では自分の利用が終わったら，ログアウトするように指示し，ログアウト忘れによるトラブルについて周知するように努めた．

3．2　計画変更

利用認証システムの導入に向けて準備を進めている過程で，導入するWebブラウザリダイレクト機能をもつファームウェア（Ver. 6.19.02）にバグが導入直前に見つかり，当初予定したとおりの構成で運用開始することができなくなった．バグの1つは，認証後に表示されるべきログアウト用画面が表示されないというもので，ログアウト操作を徹底しようとする本学の運用にとっては非常に問題であった．そのため，急遽，外部Webサーバを設置し，認証等の画面表示はそれに委ねることで認証プロセスを実現し，バグが回収されるまでの期間の暫定措置とした．

その他のバグとして，特定ブラウザからF5キー等で認証画面のリロードを継続的に実施されると，認証スイッチがハングアップ状態に陥るというものもあり，エンドユーザのキー操作で簡単に認証スイッチ全体が機能しなくなる点も問題であった．

外部Webサーバを併用するという変更により，通信開始までの認証フローは図2のようになる．本来はリダイレクトに関する部分（3と7）はなく，認証画面表示（4）や成功画面の表示部分（8）も認証スイッチが担う．

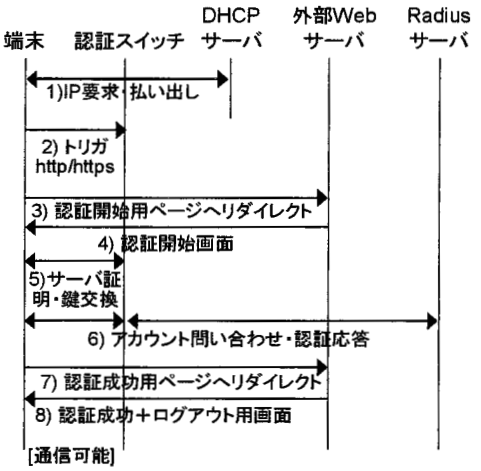

図2．外部Webサーバ併用時の認証フロー

3．3　事前テスト

今回導入した認証スイッチ単独での同時認証数（同時に認証操作を行っても失敗するユーザが出ない数）は過去の実績等から10程度と聞いていた．外部Webサーバ併用になったため，本学での構成において改めて同時認証数を検証した．検証の環境は図3のとおりである．同時接続ユーザ数を10，15，20と増加させ，以下の4項目についてそれぞれ5回ずつ調べた．検証では約10名の操作者が手動で操作することで同時ログイン等を行った．

1) httpアクセス時の認証画面表示までの時間
2) https（1024bit）アクセス時の認証画面表示までの時間

3) 同時ログイン操作時の認証成功・失敗数と結果表示までの時間
4) 同時ログアウト操作時の成功・失敗数と結果表示までの時間

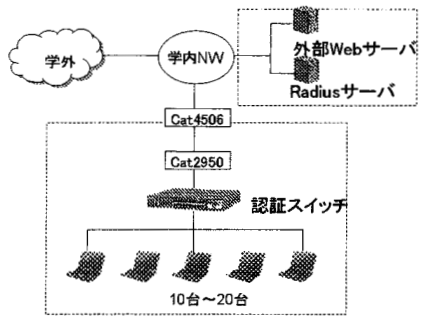

図3. 検証時の構成図

結果を表1と表2に示す. 各表の各値は各項目の平均値である. 表1は検証項目 1)と 2)に関する結果で, 画面表示時間は成功したもののうちの最遅時間の平均, CPU 使用率は最大値の平均である. 表2は検証項目 3)と 4)に関する結果で, ログイン・ログアウト時間は成功したもののうちの最遅時間の平均である.

表1より, 同時操作者が 10 名程度であれば数秒で表示されることがわかった. 認証スイッチの CPU は同時操作者 15 名を超えるとほぼ常に 100%となり, 項目 3)と 4)の検証時においては 10 名でも 100%であった.

表1. 認証開始画面表示に関する結果

		10 人	15 人	20 人
認証開始画面表示まで時間(秒)	http	3.6	5	6.4
	https	6.6	7.6	11.8
認証スイッチ CPU 使用率(%)	http	75%	97%	100%
	https	100%	100%	100%
外部 Web CPU 使用率(%)	http	0.8%	1.6%	1.4%
	https	1.4%	1.0%	1.2%

表2より, 同時操作者 10 名でも数%がログインやログアウトに失敗している. 認証スイッチの過負荷によるものである. その後, 失敗者が発生しない限界数を調べたところ, 後述のログアウトに関するバグも発生せず, 全員がログインやログアウトに成功する同時操作者の限界数は 8 名であった.

本検証時に, スイッチの過負荷時に, 画面上で「ログアウトしました」と表示されているにもかかわらず, 認証スイッチ内ではログイン状態で登録されたままになる現象が発生し, 後にバグと判断された. この現象はユーザがログアウトしたと思っても, システムではログイン状態が保持されたままになっており, そのユーザアカウントのまま別ユーザが利用できてしまう. 過負荷の状態が起きなければこの問題は発生しないが, このバグは本学の「ログアウトの徹底」という方針をシステムそのものが壊してしまう状況になってしまった. バグ修正はされるものの, 時期は未定である.

表2. 同時ログイン・ログアウト

	10 人	15 人	20 人
ログイン時間(秒)	18	16.2	19
ログイン失敗数 (人)	0.4	7.6	16
	4%	51%	80%
ログアウト時間(秒)	13	15.75	16.6
ログアウト失敗数 (人)	3.4	10.8	16.8
	34%	72%	84%

4. 導入経過

4. 1 事前告知

2 学部での認証システムの導入は全学の委員会で協議, 学部への持ち帰りのプロセスを経て, 全学の了解事項として導入作業を始めたが, エンドユーザへの影響は大きいため, 事前調査や告知を念入りに行った. 以下はその流れである.

約 1 年前 : 認証システム導入に関する協議開始, 全学承認
約 1 ヶ月前 : 初回の認証システム導入に関する案内と認証対象外機器調査開始
3 週間前 : 2 回目の案内と調査依頼
3 週間前 : 認証システム導入に伴うネットワーク利用停止案内
1 週間前 : 認証システム導入に伴う PC の設定詳細案内

最後の詳細案内は文書としても配った. 認証システム導入の 1 ヶ月前から, 少しずつタイミングをずらして何度も案内を出したことで,

エンドユーザの関心は高まったが，現実には「何か変更がある」という程度のことが周知されたに過ぎず，後述のような切り替え直後の混乱は避けられなかった．

４．２　切り替え直後

切り替え直後は，「ネットワーク接続できない」現象に直面するエンドユーザが続出することが予想され，その対応のために嘱託職員２名と常駐 SE2 名に加え，納入業者の関係者４名が本学で待機し，エンドユーザ対応に備えた．

切り替え作業は夜に行い，翌日は朝から予想通り，ユーザ対応に追われた．表３はその対応件数である．その後も日に数件ずつ問い合わせがあった．

表３．認証導入直後のユーザ対応件数

当日	午前	午後
	２０	２７
翌日	１２	
翌々日	５	

問い合わせの多くは以下のような内容であった．

- 設定方法が分からない．説明資料もない
- DHCP の設定がわからない
- 認証画面が表示されない
- アカウントがわからない
- パスワードがわからない
- アカウントがない
- プリンタが使えない

集中的な問い合わせの発生は予想どおりで，メールや配布文書で案内済みの内容関する対応がほとんどであった．プリンタなど PC 以外の機器に関しては事前の認証対象外の申請がなされていないものであった．今回の認証システムの導入で当面影響を受けるエンドユーザ数が約１５０名なので，約 1/3 が円滑に移行できなかったことになる．

非常勤教員や研究生などがアカウント申請をせずに共同利用の PC を使用していた者が予想外に多く，また，無線 LAN のアクセスポイントが多々設置されていたことなどが発覚した．これらの把握は認証システム導入の効果による．

その他，DHCP 設定を上位側のネットワークに対して設定したアクセスポイントが見つかるなど，想定外の事態もあった．

４．３　運用状況

その後の 2 ヶ月余の運用状況について報告する．利用方法などに関する問い合わせは当初の１週間くらいでほぼなくなった．図４と図５は 2 台のスイッチのログイン数とログアウト数を認証システム導入後 39 日間に 10 分間隔で集計し，時間別に平均したものである．

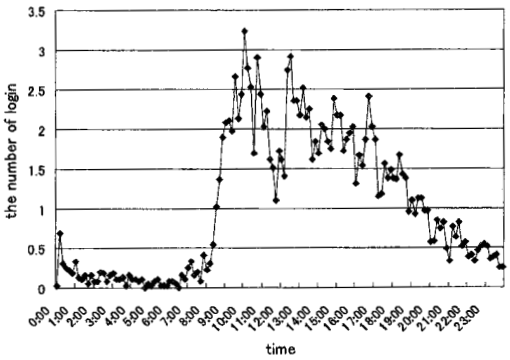

図 4．時間ごとのログイン数の推移

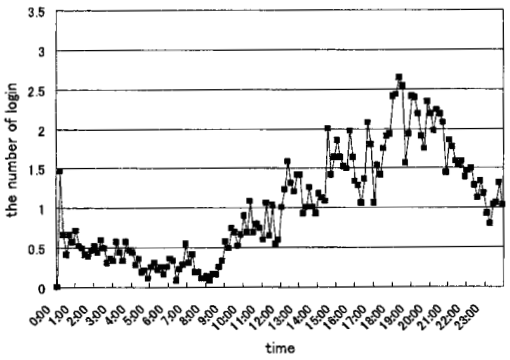

図５．時間ごとのログアウト数の推移

図４と図 5 より，本学においてはログインやログアウトに支障をきたすような同時利用は生じていない．同様のログから，同時ログインと同時ログアウト数を集計したところ，約 2 ヶ月の利用期間で同時ログインや同時ログアウトが発生したのは 2 名同時が最大で，そのうち日時分秒まで一致したものが２回，１秒ずれが 17 回，２秒ずれが 470 回あった（いずれも２台のスイッチのうち，多い方を記載）．ログアウトは同時が 59 回（数回を除き，タイ

ムアウトによるもので,手動ログアウトのような負荷はない），1秒ずれが17回，2秒ずれが32回だった．どのケースもログインやログアウトの失敗が起こる8名をかなり下回り，本学の利用状況では懸案の同時複数利用による認証スイッチの過負荷は生じていない．

本学では認証の対象となる範囲の利用者数は多く見積もっても約２００名で,教員単独や学生数人がPCを共同利用するような小さな研究室で日常的にキャンパスネットワークを利用するのであれば,今回導入の認証スイッチでも十分に利用可能である．

５．おわりに

前述のように,性能に関しては同時利用がほとんど発生しない本学のような環境では導入の認証スイッチで問題は生じない．しかし,「同時利用10人までの実績がある」や「60人の実習室で利用実績あり」などの認証スイッチの利用実績は改めて確認すべきと再認識した．事前テストを通じて，Webリダイレクトによるhttpsを用いた認証機器の性能は予想以上に悪いことを知り,実習室等で利用できているという実績についても，認証にかかる時間（待たされる時間）や再試行の回数も含めて確認すべきであろう．

機能面でも課題を多々抱えている．特に，ログアウトに関する処理が不十分である．実態としてログアウトをする利用者は少ないが，「利用後はログアウトする」というのが本来の利用方法である．現行の機器がその機能や性能に関してどれくらい吟味した実装となっているかは甚だ疑問である．実際，導入した機器においても,同時ログアウトも同時ログインと同様の負荷がかかるにも関わらず同時ログアウトに関する性能評価はなく，また，同時ログアウトによるスイッチの過負荷時には,システム上はログアウトできていないのに,ログアウトの画面が表示されるなどのバグも表面化した．

Webリダイレクト機能をもち，実習室等で多人数が同時ログインする環境でも円滑に利用できるような性能をもつ認証スイッチの開発を期待している．

謝辞

事前テストの実施やデータ採取を（株）日立中国ソリューションズ，（株）ハイエレコン，ネットワンシステムズ（株），日立電線（株）の関係各位にお世話になりました．特に本稿の執筆にあたり,日立中国ソリューションズの中島賢治氏と丸山和俊氏にはデータ集計などで手伝っていただきました．ここに記して感謝の意を示します．

参考文献

[1] 大谷誠，江口勝彦，渡辺健次，“IPv4/IPv6デュアルスタックネットワークに対応したネットワーク利用者システムの開発,”情報処理学会研究報告，Vol.2006, No.97，pp.19-24, 2006.

[2] 佐藤貴彦，久保田真一郎，升屋正人，“教育用Windows端末の利用者認証システム,”情報処理学会研究報告，Vol.2006, No.42, pp.91-96, 2006.

[3] 木澤政雄,山井成良,岡山聖彦,土居正行,河野圭太，大隈淑弘，“部外者の利用を考慮した情報コンセントアクセス制御システム”情報処理学会研究報告，Vol.2006, No.42, pp.97-102, 2006.

[4] 石橋勇人，山井成良，安部広多，阪本晃,松浦敏雄，“利用者ごとのアクセス制御を実現する情報コンセントアクセス不正利用方式”情報処理学会論文誌，Vol.42, No.1，pp.79-88, 2001.

[5] 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.1，pp.662-670, 2002.

[6] （株）ネットスプリング，FEREC, http://www.ferec.jp/, 2007.

[7] 河野英太郎，前田香織，井上智生，北村俊明，岩根典之，末松伸朗，“学究活動に不可欠になったキャンパスネットワーク構築の一事例,”情報処理学会研究会報告，Vol.2005, No.31, pp.61-66, 2005.

[8] 大学キャンパスにおける共用無線ＬＡＮサービスの開始について, http://www.hiroshima-u.ac.jp/top/press/h1801-12/p_84f839.html, 2006.

[9] 日立電線株式会社，Aprecia, http://www.apresia.jp/, 2007.