L2 認証スイッチを用いたネットワークの構築と運用
Construction and Operation of a Network System Using Authentication L2 Switches

徐　浩源[1]、古門 麻貴[2]
Hao Yuan XU[1], Maki FURUKADO[2]

横浜国立大学総合情報処理センター[1]
Information Processing Center, Yokohama National University[1]
横浜国立大学経営学部情報センター[2]
Information Center, Faculty of Business Administration, Yokohama National University[2]

240-8501　横浜市保土ヶ谷区常盤台 79
79, Tokiwadai, Hodogaya-ku, Yokohama 240-8501, Japan
haoyuan@ynu.ac.jp[1], furukado@ynu.ac.jp[2]

概要

インターネットが日常化した現在、大学の自習室やホールなどの不特定多数の人が出入りするオープンエリアで各自が用意したノート PC などを、自由に情報コンセントや無線 LAN に接続してインターネットなどにアクセスしたい、というニーズが高まっている。しかし従来の DHCP 方式だけで、ネットワーク利用時にユーザ確認をしない接続サービスを提供することは、重大なセキュリティ問題を引き起こす恐れがある。本文は、L２認証スイッチを用いて、ネットワーク接続時にユーザ確認を行う“認証ネットワークシステム”の構築例を報告する。さらに、接続場所を移動しても、全学レベルのユーザデータベースで認証を行った上でアクセスログも管理できる仕組みについて紹介する。

キーワード

L2 認証スイッチ、認証ネットワーク、DHCP、RADIUS、NIS

1　はじめに

ここ数年、総合情報処理センターは、本学のネットワークおよび教育基盤システムを整備し、情報処理教育、学術研究および事務運営などを円滑に行うため、これらのシステムの運用・保守および利用者支援と指導を行ってきたが、現在は特にネットワークのセキュリティ強化・管理に力を入れている。

各部局においてセキュリティの問題は、日々深刻化している現状が報告されている。ネットワークにおけるセキュリティ強化と安全確保は必須のものであり、現在、総合情報処理センターは、ネットワークセキュリティ強化のため、全学のセキュリティポリシーの策定を急いでいる。

本学のネットワーク接続環境は、各部局および各研究室独自の認証基準で運営されているが、現在のところオープンエリア（各学部講義棟、大学会館、教育文化ホールなど）においては、利用者は無認証でネットワークを利用することができる。このような環境はセキュリティの観点からみて大変危険であり、一刻も早くネットワーク利用時における認証システムを導入することが必要であると考えた。

本文では、上記オープンエリアのうち、経営学部および図書館に認証ネットワークシステムを構築した概要を報告する。

2　システムの特徴と構成

現在、認証ネットワークシステムについて、UNIX 系システムに認証機能を備えたゲートウェイ型認証システムや IEEE802.1x を実装したスイッチを利用するシステムなどが提案されている。これらのシステムには、ハード的な制約やクライアント端末に認証のための専用ソフトを導入しなくてはならないというソフト的な制約がある。また、これらの機器の大半は高価であり、予算上の制約から、本学における認証ネットワーク導入として、日立電線製認証機能付 L2 スイッチを利用する方式を採用した。このスイッチには２種類の認証モードがある。Shared Port Mode（シェアードモード）と Designated Port Mode（デジグネイティッドモード）である。どちらのモードもクライアント端末に Web ブラウザさえあれば認証を行うことができる。今回は特定のサブネットにおいて認証ネットワークを構築するため、シェアードモードを用いた。

認証ネットワークの設計においては、主に以下の点に着眼した。(1) 総合情報処理センターのユーザデータベースに登録しているユーザであれば、学内にあるどこの認証ネットワークにおいても、認証を受け、ネットワークに接続できる環境にすること、

(2) 障害に強い認証ネットワークシステムの構築を目指すこと、(3) セキュリティ強化を図るため、利用者の Web アクセスを必要なときに解析できるように、Web アクセスログを強制的に取れるシステムとすること、である。

認証ネットワークの構成は、下記の通りである(図1参照)。クライアント端末に IP アドレスを自動的に配布する DHCP サーバと、クライアント端末の認証リクエストを認証データベースに問い合わせを行わせる Radius サーバを、それぞれ二重化した。これらのサーバは、集中管理を行うため総合情報処理センターのネットワーク室に設置した。また L2 認証スイッチは、講義棟などのローカルネットワークサイドに設置した。この L2 認証スイッチは、従来の VLAN 構成をそのまま利用することができるトランク制御が可能なため、必要な場所へ認証ネットワークを構築することが容易であった。

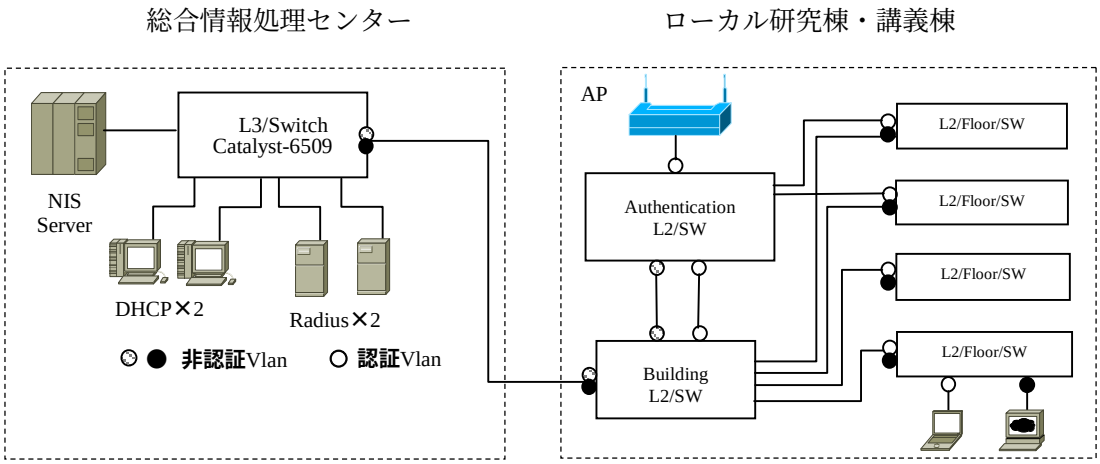

図 1　認証ネットワーク構成

3　システムの仕組み

3.1　認証の仕組み

今回採用したシェアードモードでは、認証スイッチの各ポートの配下にある複数端末の認証を同時に行うことができる。具体的には、ポートに接続している島ハブやスイッチ配下のクライアント端末および無線アクセスポイント配下のクライアント端末が、認証スイッチに Web でアクセスすることから、複数ユーザを同時に認証することが可能である。

図 2はクライアント端末が認証を受けるまでの動作概要を示している。

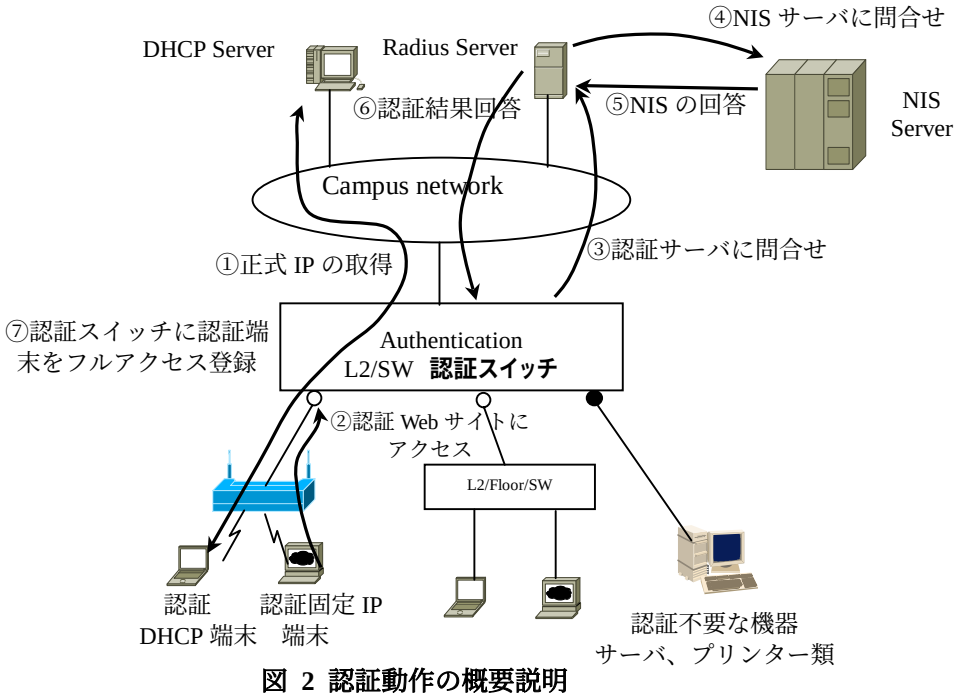

図 2 認証動作の概要説明

① IP アドレス取得：　　DHCP 端末の場合、運用系 DHCP サーバから IP アドレスを取得する。

② 認証 Web サイトにアクセス：　端末から Web ブラウザにて認証 Web サイトにアクセスし、ユーザ ID とパスワードを入力する。
③ Radius サーバに認証問合せ：　認証 Switch が Radius サーバに対しユーザ ID とパスワードを問合せる。
④ NIS サーバに問合せ：　Radius サーバが NIS サーバに対しユーザ ID とパスワードを問合せる。
⑤ NIS サーバの回答：　NIS サーバが Radius サーバの問合せに回答する。
⑥ Radius サーバの結果応答：　Radius サーバが認証スイッチへ認証許可/不許可を応答する。
⑦ 認証端末をフルアクセス登録：認証成功であれば通信可能、認証失敗であれば通信不可能。

3.2　ネットワークの設計について

認証スイッチのポートに無線アクセスポイント(AP)を導入することも可能である。無線 LAN のクライアント端末に対し、ポートローミング機能を利用することができる無線の認証済端末であれば、再認証することなく通信可能である。ただし、同一認証スイッチ内の同一 VLAN へのローミングに限る。端末がローミングしたことは、認証スイッチのログに記録される。

認証スイッチの仕様ではスイッチ 1 台あたり最大 300 端末が同時接続可能であるが（1 ポートに 300 端末接続も可)、実際推奨される接続数は 100 端末である。また IP 固定端末、DHCP 端末の両方に対応している。クライントは標準的な Web ブラウザを実装していればよく、OS には依存しない。

一方、非認証ネットワーク内の端末が、認証ネットワーク内の一部共用機器（プリンターなど）と通信したい場合は、認証ネットワーク内の機器の MAC アドレスを認証スイッチに登録する。この登録によって、機器のパケットは認証なしに LAN 上を行き来することができるようになり、機器と非認証ネットワーク内の端末間の通信が可能となる。また、Windows 系ドメイン・コントローラ・サーバ（DC）が非認証ネットワーク内にあり、ドメインに参加するクライアント端末が認証ネットワーク内にある場合は、認証スイッチに DC の IP アドレスを登録する。この登録によって、クライアント端末と DC 間のパケットは、認証なしに LAN 上を行き来することができるようになり、クライアント端末と DC 間の通信が可能となる。

4　システムの運用

4.1　ログイン

クライアント端末のブラウザから認証 Web サイトへアクセスし、ユーザ ID とパスワードを入力する（図 3参照)。認証に成功するとネットワークの利用を開始できる。認証 Web サイトの URL は、認証スイッチに登録する。

4.2　ログアウト

認証ネットワークにログインしたユーザがいつログアウトしたかについての情報は、ネットワーク利用状況を把握する上で重要である。ユーザが認証ネットワークからログアウトしたことを、認証スイッチが認識する方法は、次の 5 通り用意されている。

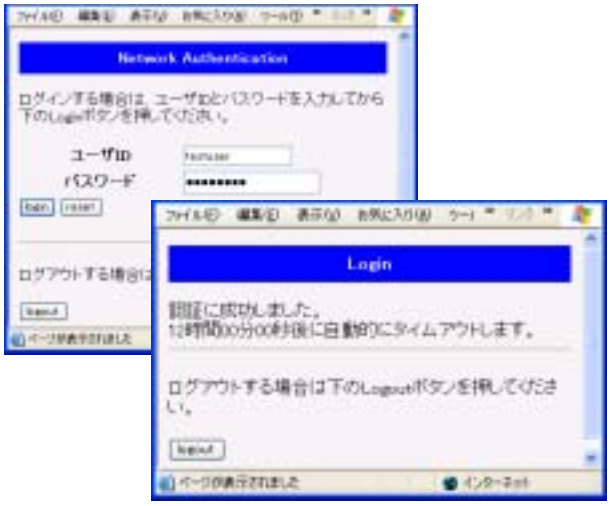

図 3：ログイン画面と認証成功画面

(1) 認証 Web サイトからログアウトを実施：
　ユーザが認証 Web サイト上のログアウトボタンをクリックしたとき
(2) 認証スイッチ接続ポートのリンクダウン：
　ユーザが利用しているクライアント端末が、直接認証スイッチのポートに接続している場合に、認証スイッチとクライアント端末の接続が切れたとき
(3) ping によるタイムアウト：
　認証スイッチからユーザが利用しているクライアント端末へ、定期的に ping ボーリングし、一定時間 ping の応答がなかったとき
(4) Max time 指定によるタイムアウト：
　ユーザが認証ネットワークへログインしてから Max Time 経過したとき（ネットワーク切断前、クライアント端末への予告はない）
(5) クライアント端末から特定パケットを認証スイッチへ送信：
　ユーザが利用しているクライアント端末から認証スイッチへ、ネットワークの利用を終了することを知らせるための特別なコマンドが送信されたとき（特別なコマンドは、事前に認証スイッチに設定する）

ユーザがログアウトしたことを把握する最も確実な方法は(1)であるが、ログアウトするために、再度認証 Web サイトにアクセスすることをユーザに期待することは難しい。そこで(1)以外の方法を有効に利用した。

4.3　ログの管理

Radius サーバのログファイルには、クライアント端末の IP Address, Mac Address, ログイン・ログアウト時間が記録される（図 4を参照）。しかしこのログからは、ユーザのアクセス状況を把握することはできない。特に Web アクセスにおいて、掲示板への書き込みなどのいたずらなどにより、大きなトラブルへ発展する可能性もある。これらのことに対応するため、L3 スイッチで、認証ユーザの Web アクセスを強制的に Proxy サーバにリダイレクトさせることにより、Web アクセスログの収集可能な環境を構築した。

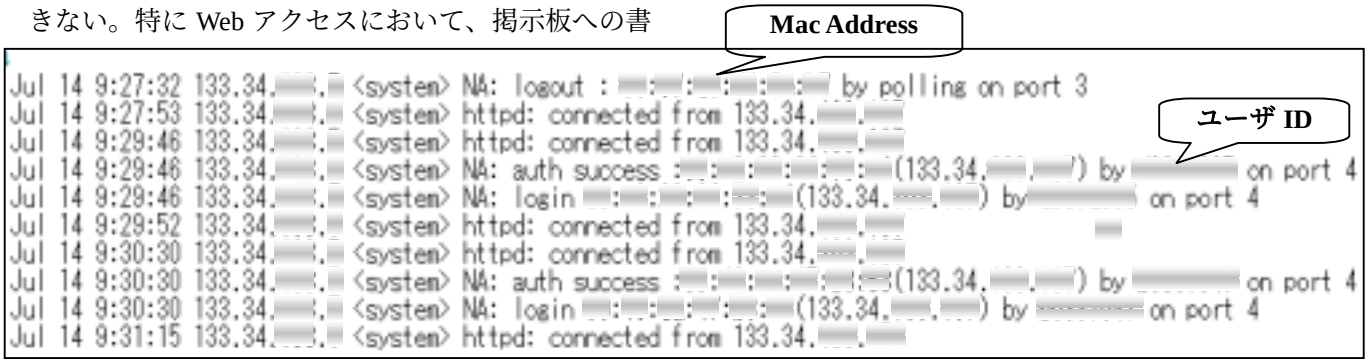

図 4：ログの一部

5　検証結果

クライアント端末が IP アドレスを取得する時間、クライアント端末が認証を受けるまでのレスポンス時間は以下の通りである（表 1参照）。

建物	IP Address を取得する時間	ブラウザを起動後、認証画面が表示されるまでの時間	ログインボタンをクリックしてから、認証結果が表示されるまでの時間
A	3.622	2.536	0.703
B	3.744	2.402	0.743
C	3.673	2.408	0.743
D	3.663	2.530	0.746

※各建物の各階ごとに 5 回データを採取し、建物ごとの平均値を算出（単位：秒）

表 1：検証結果

ユーザにストレスを感じさせない速度で認証作業が行えたといえよう。

6　問題点

システム構築時および構築後、問題となった点は、

(1) 認証スイッチ仕様（ROM への組込）から、認証 Web サイトのログイン画面を変更することができないこと（認証 Web サイトを、ユーザへの連絡事項や利用上の注意などの掲載に利用することができない）
(2) ユーザ認証に利用しているプロトコルが http であり、https プロトコルではないこと、
(3) ユーザが認証ネットワークからログアウトしたことを把握する方法として「4.2(3)ping によるタイムアウト」を利用しているため、クライアント端末のパーソナルファイアウォール機能（ping アタックをブロックする機能が含まれている）を解除しなくてはならないこと
(4) 膨大なアクセスログが発生するが、アクセスログの保管やログ解析のためのログ管理システムが、まだ構築されていないこと

などがあげられる。

7　おわりに

認証ネットワークシステムを構築したことにより、利用資格のないユーザによってネットワークを利用されるという問題は改善された。また，ネットワークトラブルが発生した場合も、Radius サーバと Proxy サーバのログを解析することにより、トラブル状況の事実確認を迅速に行うことが可能になった。今回の認証ネットワークシステムの導入対象は、経営学部と図書館であったが、今後は他学部講義棟などのオープンエリアにも導入していく予定である。本報告で紹介した認証ネットワークシステムが、オープンエリアのネットワーク管理者が抱える問題の一つといえる「ネットワーク利用者の把握」および「Web アクセスログ収集」についての一助になれば幸いである。

8　参考文献

[1] IPA 情報処理振興事業協会：http://www.ipa.go.jp/
[2] 只木進一、藤江博文、渡辺健次、渡辺義明：公開端末及び利用者移動端末の認証システムとそのディスクレスマシンによる運用、学術情報処理研究、No.5, 2001, P15～20
[3] 日立電線株式会社：http://www.hitachi-cable.co.jp/
[4] 日本アルカテル株式会社:http://www.ind.alcatel.co.jp/