情報ネットワークのセキュリティ向上について(2)

～ブロードバンドルータの発展利用と簡易認証技術～

Introduction of Security Improvement for Communication Network, Part II

— A Secure Campus LAN Model by Applied Usage of Broadband Routers and Simplified Authentication Systems —

佐藤　亮一*・佐藤　雄二**・平賀　保博**

Ryoichi SATO*, Yuji SATO** and Yasuhiro HIRAGA**

Abstract

In this report, a couple of security improvement methods for TCP/IP network systems have been introduced. First, to realize a secure-designed network environment in elementary or junior high school campus, an easy network separation method by using general type broadband routers with NAT or IP masquerading and DHCP server functions have been applied. A key procedure used here is a simple cascading connection of the routers. Next, in order to restrict the campus LAN connection from unspecified users, usage of some simplified authentication technologies, MAC address filtering, simplified authentication function of a special type router, and RADIUS authentication technology, has also been introduced. From an information-secure point of view, these authentication technologies are very useful under troublesome local network environment constructed by many PCs without Windows Domain Administration management.

1．はじめに

ブラスターワームの大量発生［1］や大手ブロードバンド接続業者等での個人情報漏えい事件［2］以来，企業や大学のみならず一般家庭でのPC・ネットワーク環境や小中学校の教育現場においても，様々な面で情報セキュリティの重要性が増加している．これまでに著者らは，PC・ネットワークのクライアントユーザとして，基本的な3つのルール（**1．脆弱性が見つかったら必ずOSのアップデートを行なう，2．ウィルス対策ソフトウェアを導入する，3．2．で導入したソフトウェアのウィルス定義ファイルの更新を頻繁に行なう**）を実行し，かつブロードバンドルータをインターネットとPC（あるいはLAN）との間に設置するだけで，ウィルス感染や情報漏えい防止に役立つことを示してきた［3］，［4］．また，上記対策の内容は，特別に高度なLANやコンピュータの知識を必要としないため，一般ユーザはもちろんのこと，初歩

2004.11.30　受理

*新潟大学教育人間科学部　生活環境学科目

**新潟大学教育人間科学部　技術部

的な教育を行なうことで中高校生でも比較的容易に上記セキュリティ対策技術を習得できることも述べてきた.

ところで,近年,大手企業や大学の多くにおいては,インターネットとLANとの間に非常に高いセキュリティレベルをもつファイアウォールを設置しているため,LANの外側からの経路でウィルス/ワームに感染する例はほとんど見られない.むしろネットワーク経由以外で内部にもちこまれるウィルス/ワーム(に感染したPC)が,ウィルス感染・繁殖のソースとなる場合が多い.例えば,著者らが所属する新潟大学では,学内ウィルス感染例の大多数が「外部から持ち込んだウィルスチェックをかけていないノートPCを,(ほとんどの場合無許可で)学内LANに接続した場合」である.いったん学内でウィルス感染が起こると,新規に購入した(セキュリティ対策をしていない)PCなどは,直接情報コンセントにケーブルを接続した瞬間に感染してしまう.

小中学校の教育現場においては,高セキュリティレベルのファイアウォールが導入されているケースはあまりないので,外部および内部両方からのウィルス感染が混在していると考えられる.本稿では,学校LANを対象とし,その外部および内部からのウィルス感染や不正アクセスを防止するための簡単な方法を説明し,(大学のLAN環境下での)実施例(設定例)もあわせて紹介することを目的とする.

はじめに,外部からのウィルス感染ルート(および不正アクセスルート)を断つ方法として,ブロードバンドルータを2台カスケード接続する方法を示す.この方法を用いると,学校LANの一部をその他の部分と分けることができるので,より安全なLAN環境を確保できる.例えば,「成績管理用PCのある教務室を他の教室のネットワークと分離して,教務室内の教員以外はネットワーク経由で成績管理用PCにアクセスできないようにする」といった具体的な適用例が考えられる.

一方,内部からのウィルス感染に関しては,まず以下のようなルールを決めて実行することが重要になる.すなわち,はじめて学校LANにつなぐPCに対して,

1.まずウィルスチェックをかけて「感染の有無」を確認する.

2.1.で感染なしと判断されたPCのみを「登録」し,学校LAN接続を許可する.

1.のウィルスチェックに関しては,[5],[6]等のURLにウィルスチェックおよび駆除を行なうソフトウェアを配布しているので有効に利用されたい.1.のウィルスチェックをパスしたPCに対してはすぐにLAN接続を許可してもよいが,重要な情報の漏えい防止やネットワーク管理の観点から,2.に示した「登録」するシステムにしておく方がよい.ここでの「登録」とは,PC一台一台に対する「登録」と,PCではなくユーザ一人一人に対する「登録」のどちらも指す.セキュリティレベルを向上するためには,両方の登録が望ましいが,いずれか一方でもよい.本稿では,LANやサーバ管理の高度な知識や技術[7]-[9]をもたなくても,**Web画面上の操作等により容易に「登録」作業を行なえる簡易認証システム**の例をいくつか紹介する.これら簡単設定の認証システムは少しの手順を勉強するだけでよいので,多忙な教員の方々でも最小限の努力でシステム運用をはじめられる.本稿では,PCに対する登録方法として,「MACアドレスフィルタリングを用いる方法」,ユーザの登録としては,「特別なブロードバンドルータがもつ認証機能を用いる方法」,そしてより一般的な「RADIUS認証技術を用いる方法」を示し,すぐに学校LAN環境で適用できるように,設定手順の例を,図表を用いて説明する.

2.ネットワークの分割

図1に示すように,一般の小中学校における学校LANは,インターネットとの接続にADSLを利用し,その内側に1台のブロードバンドルータを導入することで,インターネット側(WAN側)と学校構内側(LAN側)とを分離している.この場合,LAN側すなわちブロードバンドルータ配下のプライベートネットワークに接続される各部屋のPCやサーバは,全て同一のネットワークセグメントへの所属となる.ところで,学校現場から「情報の安全を確保したいので,成績管理用PCを置いてある教務室と,他の教室のネットワークとを切り離して利用したい」という声を聞くことがある.一般に,このような内部ネットワークの一部を他のネットワークから「完全」独立させるには,ADSL回線をもう一本開くと共に配線工事等を必要とする.

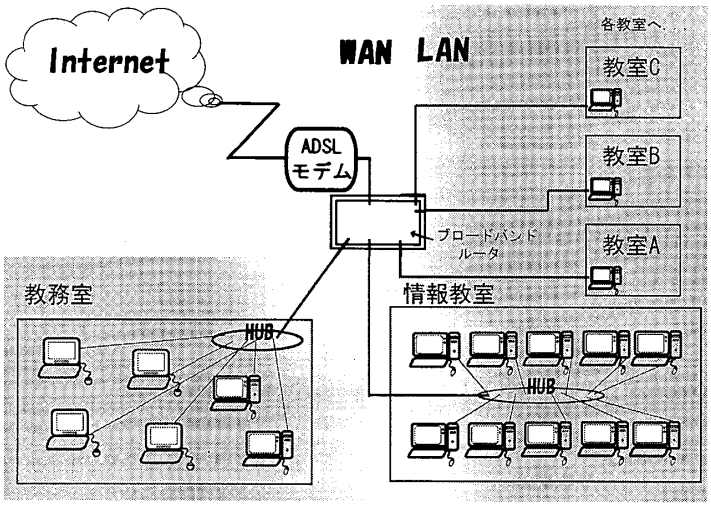


図1　学校LANの接続例

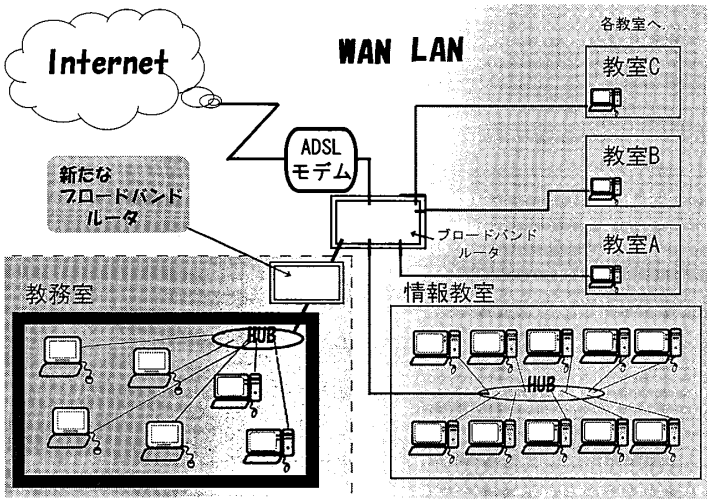


図2　ブロードバンドルータを用いた学校LANの分割例

本稿では，特別な工事を必要としない「ブロードバンドルータを2台カスケード接続（直列接続）する方法」を紹介する（図2参照）．この簡易方法を用いると，学校LANを容易に2つ（以上）に分割することができるので，上記のような現場からの要望に，簡単かつ安価で対応することができる．

一般に市販されているブロードバンドルータは，NAT（IPマスカレード）機能およびDHCPサーバ／クライアント機能を有しているので，図2に示すようにインターネットに接続されている1段目のブロードバンドルータのLAN側に，新たに2段目のブロードバンドルータを接続することで，1段目ルータのLAN側とは異なるセグメントをもつネットワークを簡単に作ることができる（図2では，教務室内のLANが，他の部屋と異なるセグメントをもつことになる）．このようなブロードバンドルータのカスケード接続により，2段目ルータのLAN側（教務室内）のPCからは，1段目ルータのLAN内（情報教室や他の教室）に接続されたPCへのアクセスは可能だが，逆に1段目LANから2段目LANへのアクセスは基本的にできなくなる．

上記の構成を実現する際，2段目のブロードバンドルータのネットワーク設定が，一般に家庭で使用する場合の設定と若干異なるので，以下に㈱マイクロ総合研究所のOPT-Rを用いた場合の設定例を示す．

WAN側の設定

「－WANポートの設定－」→「動作モード設定」で「DHCPクライアント」の「IPアドレス自動取得」を選択する（図３）．最後に「設定」で，さらに「設定の更新」をクリックすることで変更した設定が保存され，その後画面の指示にしたがって再起動させると設定が有効になる．

LAN側の設定

２段目ルータのLAN側に割り当てるプライベートIPアドレスが１段目LAN側のIPアドレスと同じセグメントになる場合，NATがうまく動作しないので設定変更が必要となる．

① まず，「－LANポートの設定－」→「DHCPサーバの設定」を選ぶ．先頭IPアドレスの第３オクテット注の数字を変えることでセグメントを変更できるので，ここでは「先頭IPアドレス／サブネット」を192.168.100.2/24とする．

② 「ゲートウエイ」も192.168.100.1に変更し，DNSは１段目のブロードバンドルータから情報を取得できるので「WAN側から取得したDNS情報を優先する」にチェックを入れる（図４）．

③ 最後に「設定」，「設定の更新」をクリックすることで設定が保存され，その後画面の指示にしたがって再起動させると設定が有効になる．

以上で，図２に示すような学校LAN内の分割に必要な設定は完了するが，１段目および２段目の両方のブロードバンドルータに文献［３］，［４］で紹介した「パケットフィルタリング機能」を用いたポート制限設定をしておくと，より安全なネットワーク環境が構築できる．表１に最近の代表的なコンピュータウィルス／ワームとそれらの使用するポート番号をまとめたので，参考にしていただきたい．

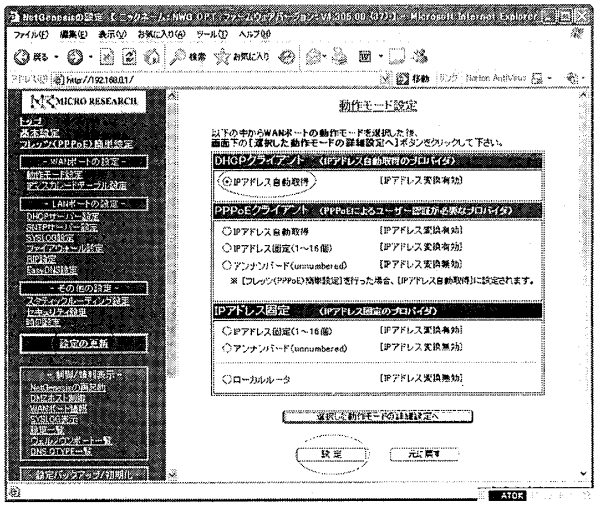


図３　WAN側の設定

図４　LAN側の設定

注 192.168.[100].2
第３オクテット

表1　代表的なコンピュータウィルス／ワームとそのポート番号（2003年1月以降）

名　称	発見年月	特　　徴	対象ポート
Sobig	2003/01	トロイの木馬型の不正プログラム．自身のコピーを添付したメールに送信して自己増殖していく．	
SQL Slammer	2003/01	マイクロソフトの「SQL Server 2000」の脆弱点を突いて侵入し，DoS攻撃などを行なうワーム型不正プログラム．	
MSBlaster	2003/08	TCPポート135を使ってDCOM RPCの脆弱性（マイクロソフトセキュリティ情報MS03-026参照）を悪用するワーム．	TCP 135 TCP 4444 UDP 69
Welchia (Nachi)	2003/09	MSBlasterの亜種．MSBlaster同様の活動に加え，「WebDAVセキュリティホール」と呼ばれるセキュリティホールも利用する．	TCP 135 TCP 80
Swen	2003/09	独自のSMTPエンジンを利用して自分自身を拡散する大量メール送信型ワーム．	
Bagle	2004/01	リモートウェブサイトにアクセスする大量メール送信型のワーム．このワームは，発見したあらゆる連絡先に対し，自身のSMTPエンジンを利用して電子メールを送信する．	TCP 6677
Mydoom	2004/01	大量メール送信型のワーム．感染すると，TCPポート3127から3198をオープンし，バックドアを仕掛ける．	TCP 3127 -3198
Netsky	2004/02	大量メール送信型のワーム．独自のSMTPエンジンを使用し，ハードドライブ，およびマッピングされているドライブで発見したアドレスに対し，自分自身を電子メールで送信する．	
Sasser	2004/04	マイクロソフトセキュリティ情報MS04-11で回折されている脆弱性の悪用を試みるワーム．このワームは，ランダムに選択されたIPアドレスをもつコンピュータをスキャンすることによって，上述の脆弱性に未対応のシステムを探し出して拡散する．	TCP 445

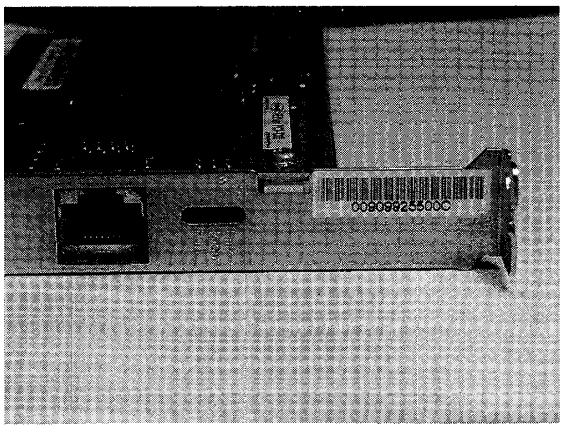
3．簡易認証技術

一般に，数十台以上のデスクトップ型PCを備えたPC実習室等でユーザ管理を行なう場合，「Windowsドメイン」を構築して，ユーザ毎にログオンのIDとパスワードを与えて管理するのが望ましい．Windowsサーバを用いたWindowsドメイン構築の実現により，各ユーザと各PCの一元的な効率良い管理が可能となるからである．しかしながら，Windowsドメインの構築およびその管理には比較的高度な技術［7］が要求されるため，学校現場において多忙な一般教員が管理を行なうのはかなりむずかしい．また，移動しながら使用することの多いノート型モバイルPCに対しては，異なるネットワーク環境での利用が想定されるため，上記Windowsドメインによるユーザ管理はあまり適さない（ただし，管理不可能ではない）．

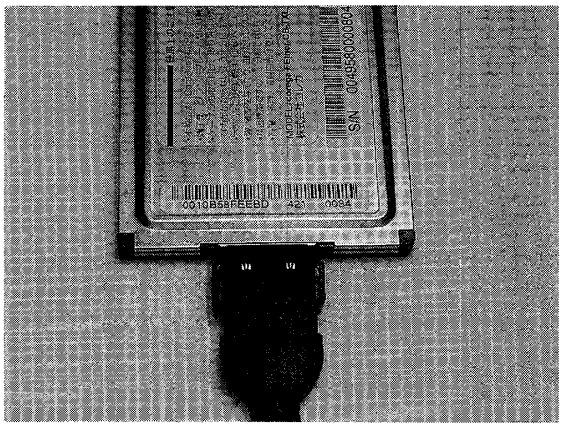
そこで本章では，各種ブロードバンドルータに備わっている簡易認証機能を利用することで簡単なネットワーク管理を行なうことが，上記ユーザ管理の代替的な役割を果たすこと，およびネットワークセキュリティ向上に役立つことを説明していく．

3.1 PCの認証（登録）－MACアドレスフィルタリング

はじめにMACアドレスについて説明する．MACアドレスとは，ネットワークでホストを識別するためにネットワークカード（NIC）に固有で付けられた番号をいう．NICに対して48ビットの識別符号が付けられており，「00:11:22:AA:BB:CC」といった形式で表される．前半の「00:11:22」がベンダー固有のIDで，後半の「AA:BB:CC」がNICの連番となり，世界中に１つしかないユニークな番号である（図5(a)，(b)参照）．MACアドレスフィルタリングは，このユニークな番号を識別することにより，ネットワーク接続を許可するかどうかを判別する認証技術である．



(a)　PCI-BUS用（デスクトップ用）のNIC



(b)　PC-CARD用（ノート用）のNIC

図5　NICに示されているMACアドレス

なお，MACアドレスがNICに書いていない場合は，コマンドプロンプトよりipconfigコマンド（図6）もしくはarpコマンド（図7）を実行することにより，MACアドレスを調べることができる．ipconfigコマンドは，操作しているPC(NIC)のMACアドレスを調べるときに使用し，arpコマンドは，他のPC(NIC)のアドレスを知りたい場合にpingコマンドと併用して用いる．

```
コマンド プロンプト
(C) Copyright 1985-2001 Microsoft Corp.

C:¥Documents and Settings¥user1>ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : TECH123
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : ed.niigata-u.ac.jp

Ethernet adapter ローカル エリア接続:

        Connection-specific DNS Suffix  . : ed.niigata-u.ac.jp
        Description . . . . . . . . . . . : 3Com 3C920 Integrated Fast Ethernet
Controller (3C905C-TX Compatible)
        Physical Address. . . . . . . . . : 00-B0-D0-35-5A-C9
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.0.2
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.0.1
        DHCP Server . . . . . . . . . . . : 192.168.0.1
        DNS Servers . . . . . . . . . . . : 192.168.0.1
        Lease Obtained. . . . . . . . . . : 2004年11月12日 8:36:19
        Lease Expires . . . . . . . . . . : 2004年11月13日 8:36:19

C:¥Documents and Settings¥user1>
```

図6　ipconfigコマンドの実行例

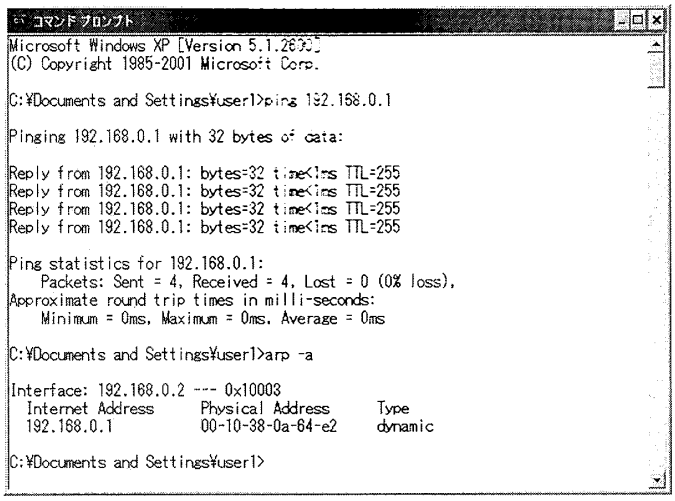


図7　arp コマンドの実行例

数年前までは,「MACアドレスフィルタリング機能」は非常に高価なインテリジェントハブのみに備わっていた機能だった．しかしながら，近年は比較的安価な無線LANブロードバンドルータの一部（例えば，㈱IOデータ機器のWN-AG/BBR-S，実売2万円程度）の有線LANポートにも備わるようになった［4］．最近，さらに低価格のMACアドレス認証付き有線ブロードバンドルータ㈱IOデータ機器NP-BBRP（実売4千円程度）が発売されたので，本稿ではこのルータを用いたフィルタリングの設定例を示す．

MACアドレスフィルタリングの設定例

① LANポートの一つにPCを接続し，IEを立ち上げてルータhttp://192.168.0.1にアクセスして設定画面を開き，上欄のメインメニューから「LAN側設定」を選ぶ．

② 「DHCPサーバ」の「割り当てする数」は，実際にこのブロードバンドルータに接続を許可するPCの台数を入力する．また「割り当てを指定するIPアドレス」で「設定ページへ」ボタンをクリックし，「IPアドレス」と「MACアドレス」を入力して「追加」ボタンをクリックすると，「割り当てを指定するIPアドレスリスト」に追加される（図8参照）．

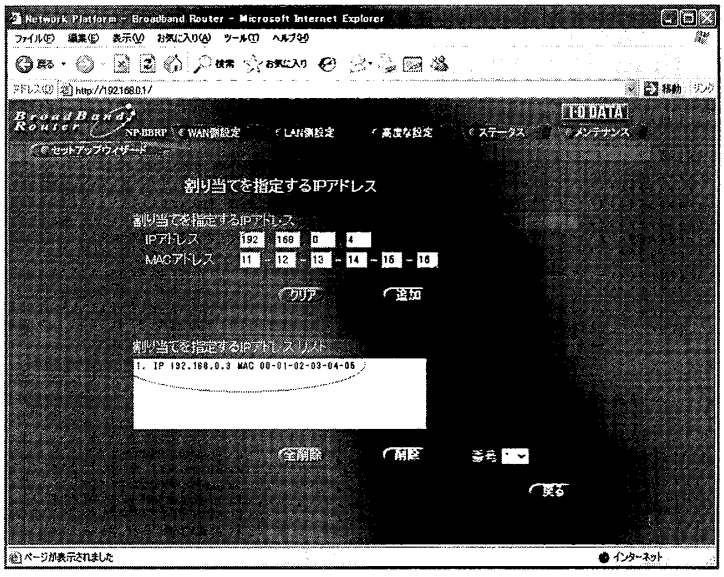


図8　MACアドレスフィルタリングの設定

③　②の手順で，各 NIC の MAC アドレスが登録されるので，「LAN 側設定」に戻って「設定」をクリックする．以上の設定により，登録された NIC のインストールされた PC 以外は，ネットワーク利用不可能とすることができる．

なお，このルータ「㈱IO データ機器 NP-BBRP」の場合は，上記手順で253台の PC を登録することが可能である．

3.2　ユーザ認証(1)　－認証機能付ブロードバンドルータの利用

前節で説明した MAC アドレスフィルタリングによる認証は，安価なブロードバンドルータで実現可能で，かつ設定手順が非常に簡単である点が優れている．本節では文献［4］でも紹介した認証機能付の業務用ブロードバンドルータ「センチュリー・システムズ㈱XR-410/TR2（4 万円程度）」を，比較のため再度紹介する．なお，具体的な設定に関しては，文献［4］を参照していただきたい．このルータの認証機能は，ユーザ ID とパスワードによる本格的な認証機能を有しているので，MAC アドレスフィルタリング認証での「登録された PC を，関係者以外のユーザ（組織部外者）に使用される」という問題は起こりにくい．ただし，図 9 に示すように，このルータの認証機能で登録できるユーザ数は最大64なので，学校現場においては生徒用ではなく，教職員用の認証に使用するのが現実的である．

図 9　業務用ルータの認証機能の最大登録ユーザ数

3.3　ユーザ認証(2)　－RADIUS 認証専用ルータの利用

前節で示したユーザ ID とパスワードによる認証方法で，登録ユーザ数に制限のない方法の一つに，本節で紹介する「RADIUS 認証」がある［10］,［11］．RADIUS とは「Remote Access Dial In User Service」の略で，Livingston Enterprise 社が自社製品のために開発したプロトコルを一般化した規格である．本来，コンピュータを遠隔利用する際に用いられたユーザ認証技術で，ユーザはダイヤルアップ接続によりネットワーク・アクセス・サーバ（Network Access Server: NAS）を介して RADIUS サーバより認証を受ける．

現在はダイヤルアップ接続自体があまり行なわれないこともあり，LAN内にNASに相当するRADIUS認証対応のクライアント・ルータ（あるいはクライアント・スイッチ）を置き，その配下のプライベートネットワークのユーザに対する認証に用いるケースが多い．なお，RADIUSプロトコルでは，ユーザの認証と共に，そのユーザが利用できるサービスの範囲を知らせる処理も行なう．

図10に示すように，実際にRADIUSプロトコルを使用するには，RADIUS用のサーバとNASに相当するクライアントが必要となる．本稿では，RADIUSシステムの設定を説明するために，RADIUSサーバとして，RADIUS専用機「センチュリー・システムズ㈱RA-350」とLinux OSをインストールした汎用PCを用いた．また，クライアントにはRADIUSクライアント機能をもつ「同社XR-410/TX2」（前節で紹介した業務用ルータ）を使用した．

ここで，RADIUSサーバとして，RADIUS専用機と汎用Linux PCを比較してみる．専用機のメリットは，ネットワーク接続したPC上のWeb画面から簡単に各種設定・ユーザ登録ができるので，特別な知識を必要とせず簡単にRADIUSサービスを行うことが出来る．さらに，HDD等の可動パーツをもたないのでメンテナンスが非常に楽である．一方，Linux PCの場合は，まずLinux OS（UNIX OS）の知識が必要となるので，認証とは別の次元の問題となる．逆に，専用機のデメリットは，この機種では（搭載されているメモリの関係から）認証可能なユーザ数が1,024までで，これ以上のユーザ登録が行なえないこと，ログの記録方法に自由度があまりないことが挙げられる．Linux PCではユーザ登録数やログに関する上記のような問題は生じない．

本稿ではWeb画面上での簡単な設定が可能なRADIUS専用機を使用したシステムを推奨する．以下に，その具体的な設定例を示す．

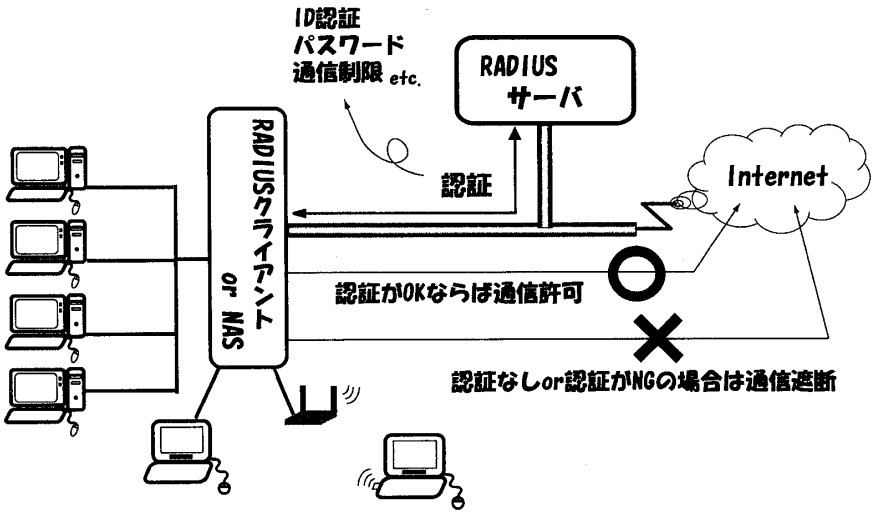


図10　RADIUS認証システムの例

RADIUS専用機（RADIUSサーバ）RA-350の設定

① LAN側のポートの一つにPCを接続し，IEを立ち上げてルータのアドレスhttp://192.168.0.254:880にアクセスし，設定画面から「RADIUSサーバ設定」を選ぶ（図11）．

② RADIUSサーバ設定から「基本設定」を選び，「ポート番号」欄はクライアントとのやりとりを行うポート番号「1645/1646」，「認証方式」欄は「PAP/CHAP」を選択，必要に合わせて「認証ログ設定」でログをとる設定をする．設定後「設定変更」をクリックする（図12）．

③ RADIUSサーバ設定から「クライアント」を選び，「クライアントの新規追加」をクリックしてクライアントの「IPアドレス」と「secret」を入力し，「実行」をクリックする．これでクライアント登録ができる．なお，「secret」はサーバ，クライアント間の共有鍵である（図13）．

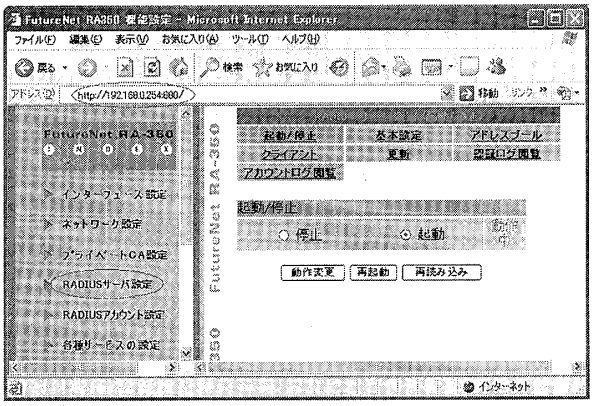


図11 RADIUS サーバの設定 ①

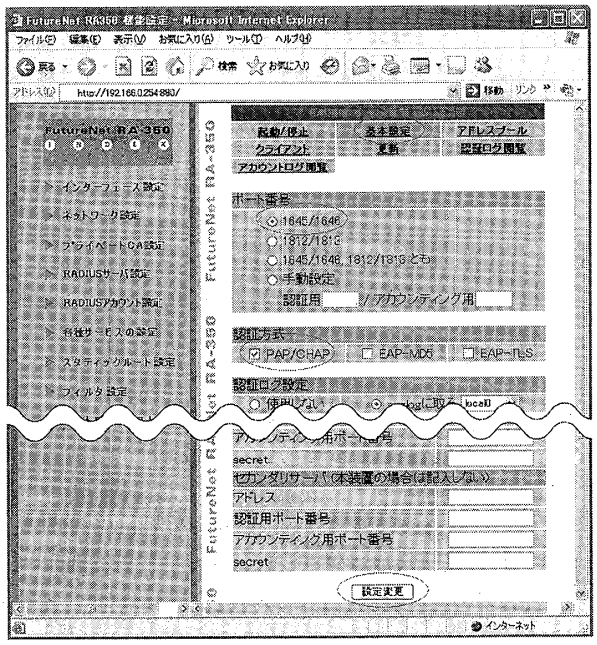


図12 RADIUS サーバの設定 ②

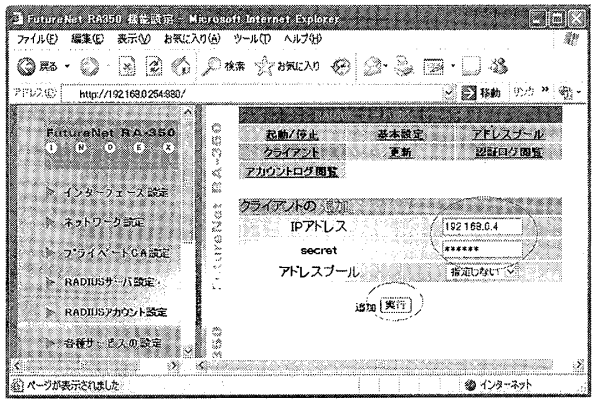


図13 RADIUS サーバの設定 ③

RADIUSサーバRA-350へのユーザ登録

① RADIUSサーバへのユーザ登録は設定画面から「RADIUSアカウント設定」を選ぶ（図14）.

② RADIUSアカウント設定から「ユーザ」を選択し,「表示」をクリックする．既にユーザが登録されていれば一覧が出る．新たにユーザ登録する場合は「新規追加」をクリックし,「ユーザ名」,「パスワード」を入力し,「実行」をクリックして登録を完了する（図15）．なお，専用機RA-350ではCSV形式のファイルによるアカウントの一括登録が可能なので,「保存」および「復旧」からアカウントの一括保存および登録が出来る（図16(a), (b)）.

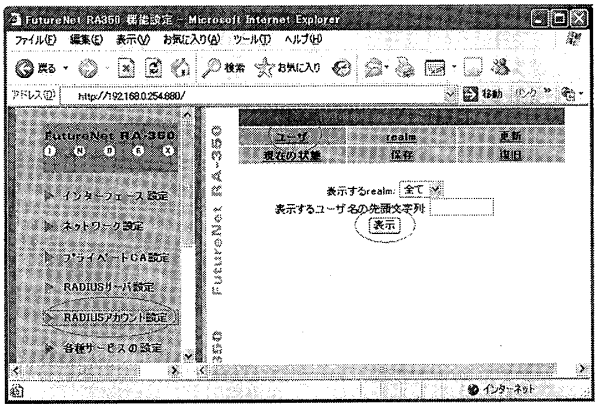


図14　RADIUSサーバへのユーザ登録 ①

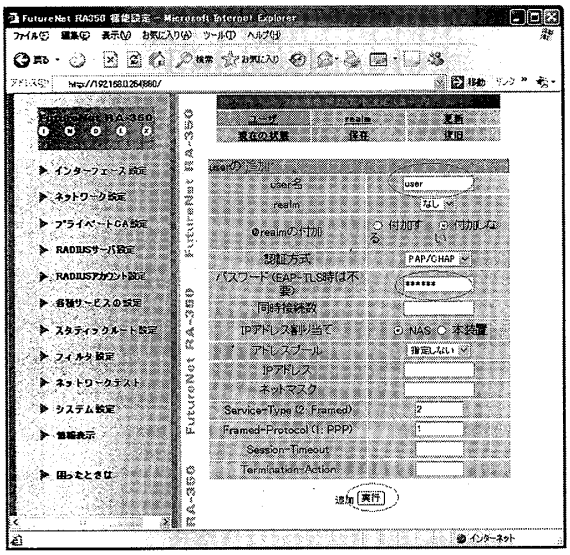
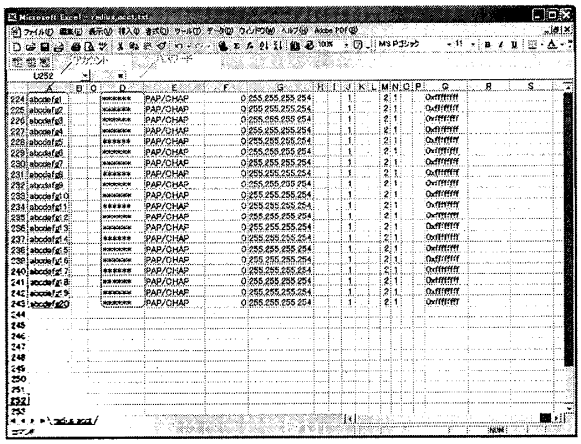


図15　RADIUSサーバへのユーザ登録 ②

(a)



(b)

図16　CSV形式による「保存」と「復旧」

RADIUSクライアントXR-410/TX2の設定

① LAN側のポートの一つにPCを接続し，IEを立ち上げてルータのアドレスhttp://192.168.0.254:880にアクセスし，設定画面から「ゲートウェイ認証設定」を選択.

② 基本設定の「本機能」欄は「使用する」,「認証」欄は「する」,「80/tcp監視」欄は「行う」を選択す

る．URL 転送については，今回は確認のため XR-410 TR2があらかじめもっているログイン確認画面を利用し，強制認証後にログイン出来た旨表示するようにした．「認証方法」欄は「RADIUS サーバ」を選択する．「接続許可時間」については実情にあわせて選択する（図17参照）．

③ 次に，ゲートウエイ認証設定のメニューから RADIUS 設定を選び，プライマリサーバ設定の「IP アドレス」欄には RADIUS サーバの IP アドレスを入力．「ポート番号」欄には RADIUS サーバとのやりとりを行うポート番号を設定し，「secret」欄にはサーバとの共有鍵を入力する．サーバ共通設定の「NAS-IP-Address」欄には XR-410/TR2の IP アドレスを入力する（図18参照）．なお，RADIUS 専用機 RA-350との組み合わせでは，最大1,024のユーザ登録が可能である．

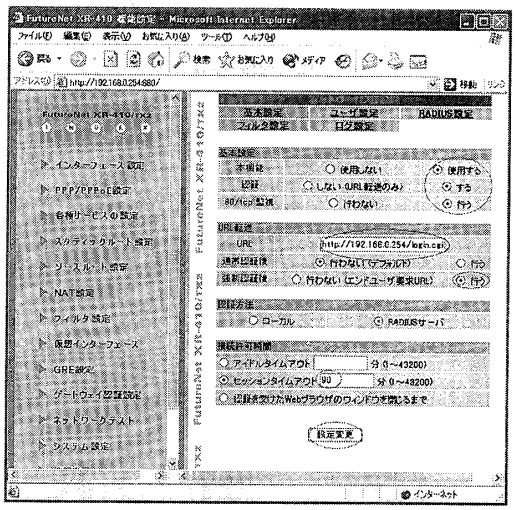


図17　RADIUS クライアントの設定 ①

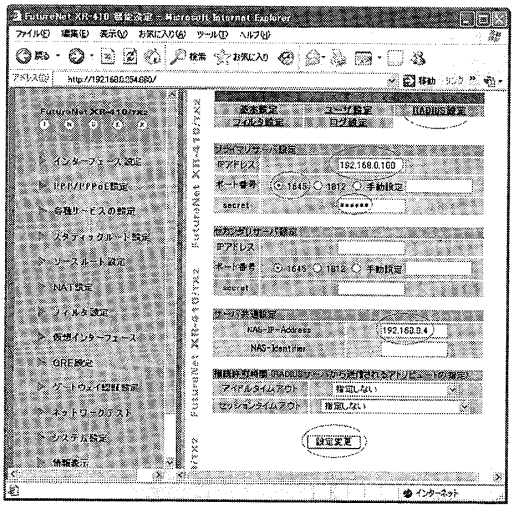


図18　RADIUS クライアントの設定 ②

PC ユーザの認証画面

実際の PC ユーザがこの認証機能を利用する際の認証画面の例を示す．

① PC を起動後に IE を立ち上げると，自動的に認証ウインドウが現れるので「ユーザ ID」と「パスワード」入力する（図19）．

② 認証に成功すると，その旨のメッセージが表示される（図20）．

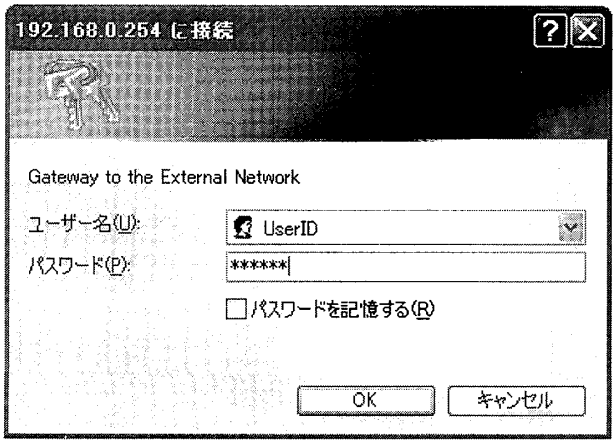


図19　認証画面 ①

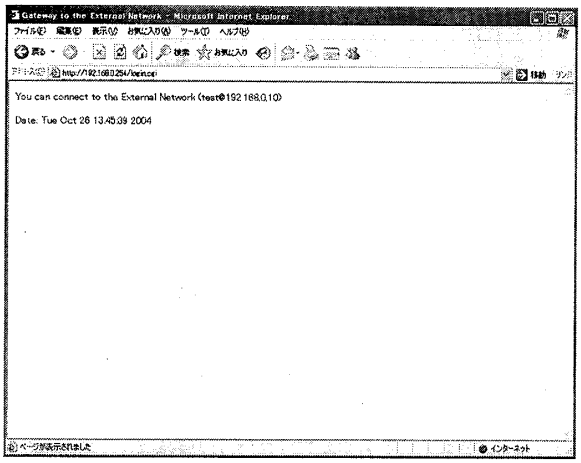


図20　認証画面 ②

3.4　3種類の認証方法の使用方法

前節までに，3種類の簡易認証技術を用いたシステム例を示した．各々に適したネットワーク環境を検討すると，表2に示されるような結論を得る．

ネットワークに接続するPCの数が非常に少なく（5～6台）で利用者が限られている場合は，MACアドレスフィルタリングで十分なので，ルータNP-BBRPの利用が適している．PCの登録数は253台まで可能であるが，現実的な同時利用可能なPCの台数は限られていること，MACアドレスの取得・登録に費やされる時間を考えると小ネットワーク向きの認証技術といえる．

利用PCの台数がやや多く，利用者数が64人までなら認証機能付ブロードバンドルータXR-410/TX2を利用した方がよいと思われる．一般のブロードバンドルータと比較すると，多少価格は高いが，60台程度のPCの同時利用が可能で，かつRADIUS認証システムのクライアントサーバ（NAS）も兼ねることができるので発展性がある．

最後に，RADIUS認証は，利用PC台数および利用者数共に多い場合に有効である．利用者数が1,000人程度までならば，今回紹介した専用機（RA-350）と業務用ブロードバンドルータ（XR-410/TX2）の組み合わせは，簡単な設定手順であること，導入時のコストパフォーマンスが高いこと，さらにシステム運営後のメンテナンス性が良いことで，非常に優れた組み合わせである．

表2　紹介した3種類の簡易認証システムに対する評価

認証方法（設定に用いたシステム）	評価 ○	評価 ×	適したネットワーク環境
MACアドレスフィルタリング（NP-BRP）	・安価 ・設定が簡単	・同時利用可能なクライアント数が少ない	ネットワークに接続するPC数は少なく（5～6台程度），利用者が限られている場合
業務用ルータの特別な簡易認証（XR-410/TX2）	・ルータのみでユーザの認証が可能 ・60台程度のPCの同時利用ができる ・設定が比較的簡単	・業務用ルータなので，価格が比較的高い	ネットワークに接続するPC数は60台程度まで実用的．利用者数は64人まで
RADIUS認証			
（汎用Linux PC ＋ XR-410/TR2）	・利用人数制限なし	・Linux（UNIX）の知識が必要	ネットワークに接続するPC数が多く，利用者数も1,000人程度まで想定される場合
（RA-350 ＋ XR-410/TR2）	・メンテナンス性良し ・設定が比較的簡単	・価格が比較的高い（RA-350） ・利用人数が1,024人まで	上記に加え，恒常的に認証システムを運用していく場合（メンテナンスの容易さが重要な因子）

4．むすび

本稿では，学校LANのセキュリティ向上のための第2ステップとして，以下の簡単な情報ネットワークのセキュリティ向上方法の提案を行なった．

1．「ブロードバンドルータをカスケード接続する方法」により，学校LANの一部を，他のネットワークと分離することで，外部からの安全性を高めることができることを紹介した．

2．学校LAN内部におけるネットワーク管理およびユーザ管理の重要性の観点から，3種類の「簡易認証

システム」を，それらの具体的な設定例と共に説明し，その有効性を明らかにした．

情報ネットワーク，情報セキュリティの重要性が増し，より高度なスキルが要求されている今日ではあるが，本稿で示したような非常に簡単で，わずかな努力により大きな効果を得ることのできる情報セキュリティ向上のための技術は少なくない．

教育現場の教員らの間においても，情報セキュリティにより関心をもち，「情報セキュリティは専門外」と決めつけずに，常にスキル向上に努力を続けていただきたい．本稿がそのきっかけになれば幸いである．

おわりに

情報教育に関する貴重な資料を提供していただいた本学教育人間科学部の小林昭三先生，鈴木賢治先生，情報セキュリティポリシーに関するご助言いただいた本学総合情報処理センターの長谷川誠先生に深謝いたします．また，図の作成を手伝ってくれた本学教育人間科学部技術科4年生の木島靖人君に感謝します．

参考文献

[1] http://support.microsoft.com/
[2] http://itpro.nikkeibp.co.jp/free/ITPro/Security/20040329/1/
[3] 佐藤亮一，“ブロードバンドルータを用いた学校LANのウィルス対策”，技術教室，農山漁村文化協会，2月号，2004.
[4] 佐藤雄二，平賀保博，佐藤亮一，“情報ネットワークのセキュリティ向上について～ブロードバンドルータを用いた簡易対策～”，新潟大学教育人間科学部紀要 自然科学編，第6巻，第2号，pp.149-164，2004.
[5] http://www.trendmicro.co.jp/hcall/index.asp トレンドマイクロ.
[6] http://www.symantec.co.jp/region/jp/sarcj/tools.list.html シマンテック.
[7] 清水理史他，“できるPRO Windows2000Server完全入門”，インプレス，2003.
[8] 高木弘幸他，“パソコンTCP/IP教科書”，アスキー出版局，1995.
[9] Cisco CCNA試験#640-607公式ガイドブック，ソフトバンク，2002.
[10] Jonathan Hassell，“RADIUS－ユーザ認証セキュリティプロトコル”，Oreilly，2003.
[11] http://www.cisco.com/japanese/warp/public/3/jp/service/tac/707/32-j.shtml