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～

Introduction of Security Improvement for Communication Network
～Simplified Method by Using Broadband Router～

佐藤雄二[1]，平賀保博[1]，佐藤亮一[2]
Yuji SATO[1], Yasuhiro HIRAGA[1] and Ryoichi SATO[2]

Abstract

In this report, a simplified security improvement method for communication TCP/IP network has been introduced. In the method, a popular type broadband router has been utilized not only to separate the global network and the local or private network, but also to interrupt the infection route for some kind of computer virus. In addition, so as to try to obtain better security condition, we have also introduced the advanced security improvement method based on the simplified authentication function attached to some special type broadband routers. From a practical point of view, the effective through put speed of some representative broadband routers has been finally discussed.

1．はじめに

近年，ブロードバンド通信の普及に伴い，情報セキュリティへの関心が高まってきた。特に，この2003年夏に大量発生したコンピュータウィルス・ブラスターワーム問題［1］により，日本中のみならず世界中の情報ネットワークおよびコンピュータが深刻な被害を受け，改めて情報セキュリティ対策の必要性，重要性を認識させられた［2］。現在の日本におけるインターネット・PCユーザの多くは，一般的なオフィスソフトウェア（例えば，インターネット・エクスプローラ，一太郎，ワード，エクセル，パワーポイント等）の使用に関しては，数年前と比較すれば，かなり高いレベルにまでスキル向上を成し遂げている。しかしながら，ブラスターワームの事例からわかるように，情報セキュリティに関する意識は未だに高くなく，ADSL（非対称デジタル加入者線）を利用したインターネット常時接続のような，セキュリティ面では最も危険なネットワーク使用をしているにもかかわらず，各々のPCに対してOSのアップデート（例えば，ウィンドウズ・アップデート等）やコンピュータウィルス対策ソフトウェア（例えば，ノートンアンチウィルス等）の導入すら行っていないユーザが今なお非常に多いということが，今回明らかになった。数年前のニムダワーム［3］の教訓がほとんど生かされていなかったわけである。

2003.12．1　受理
1　新潟大学教育人間科学部 技術部
2　新潟大学教育人間科学部 生活環境学科目

ところで，ここ数年の小中学校の教育現場においては，情報リテラシー教育，特にインターネットを利用した情報収集を中心とした教育がさかんに行われてきたが，情報セキュリティ教育に関する議論は，著者らの知る限り，あまり行われていなかった。恥ずかしながら，著者らが所属する新潟大学教育人間科学部においても，文系学生向け情報関連科目では，つい最近までコンピュータウィルス対策に主眼をおいた情報セキュリティに関する内容を含んでいなかった。

さて，今回のワーム事件から学べることは，コンピュータウィルスに対する最も有効な手段は，インターネットを使うユーザ一人ひとりのセキュリティに対する意識とそのスキルを向上させることである。しかし，これらの向上は決して容易なことではなく，ファイアウォールのような情報機器を導入すれば一夜にして達成できるという単純な問題でもない。各々が自分の能力に合わせて時間をかけて徐々に習得していくものだからである。そこで，まずその第一歩として提案したいのが，

１．OSに脆弱性が見つけられたら，速やかにOSのアップデート作業を行う。

２．コンピュータ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う。

の３点の厳守である。勿論，この他にSobig.Ｆ等のメール添付型ウィルスの感染を防ぐためには，知らない人から送られてきたメールの添付書類（添付ファイル）は絶対に開かないこと等，細かな注意事項を上げればきりがないが，少なくとも上記３点をユーザ各々が責任をもって確実に実行することで，情報ネットワークのセキュリティレベルは大幅に向上する［４］。一般のネットワーク・PCユーザ各々に上記3点のような簡単な手順の実行を習慣づけてもらうためにも，小中学生の年代から，情報リテラシー教育，情報処理技術教育に加え，情報セキュリティに関する知識，スキルも身につけられる教育システムに，早急に移行していかなければならない。

本稿では，上記３点の厳守という基本に加え，情報ネットワークの本当に初歩的な知識さえ教育すれば，中学生，高校生でも比較的容易にブラスター型コンピュータウィルス防御環境づくりが可能であることを，安価な市販ブロードバンドルータ（１万円程度～）を用いた簡易ウィルス対策方法［５］の一例により示し，情報セキュリティ教育の一助とすることを目的とする。さらに，MACアドレス制限機能，ユーザ認証機能を有する少し特殊なブロードバンドルータ（多少高価で５万円程度）を用いれば，さらなるセキュリティ向上が可能であることを，設定例をまじえて紹介する。

次章以下では，はじめにブロードバンドルータを利用したプライベートネットワーク構築方法を示す。次に，パケットフィルタリング設定を適切に行うことにより，ブラスターワームの感染拡大を容易に防げることを説明する。さらに，最近は簡易認証機能（ユーザ認証，MACアドレス制限による認証等）を有するブロードバンドルータも市販されはじめているので，その有効性，実用性を検証する。最後に，安価な市販ブロードバンドルータでも，小中学校における小規模（40台程度）コンピュータ教室のブロードバンド通信に十分耐えうる性能（速度）を有することを，大学での実践例と簡単なネットワーク実験により示す。

２．簡易コンピュータウィルス対策の手順

本章では，市販ブロードバンドルータを用いたコンピュータウィルス（主にブラスター型ウィルス）に対して安全なネットワーク環境の構築手順を，段階毎に説明していく。

２．１　プライベートネットワークの構築

はじめに，図１に示すように，対象とするネットワーク環境をブロードバンドルータの外側（インターネット側 or WAN側）と内側（プライベートネットワーク or LAN側）に分離する。ここでは，家庭や学校内のネットワークがプライベートネットワークに対応する。インターネットに直接接続するためのルータ外側のIPアドレスを**グローバルIPアドレス**，ルータ配下の閉じたネットワーク用IPアドレスを**プライベートIPアドレス**といい，これらを適切に入力する。なお，ブロードバンドルータ配下に接続されたPCには，全てこのプライベートIPアドレスを割り当てるようにし，プライベートIPアドレス⇔グローバルIPアドレス変換機能，すなわち**NAT（Network Address Translation）**機能を利用して，プライベートIPアドレスを割り当

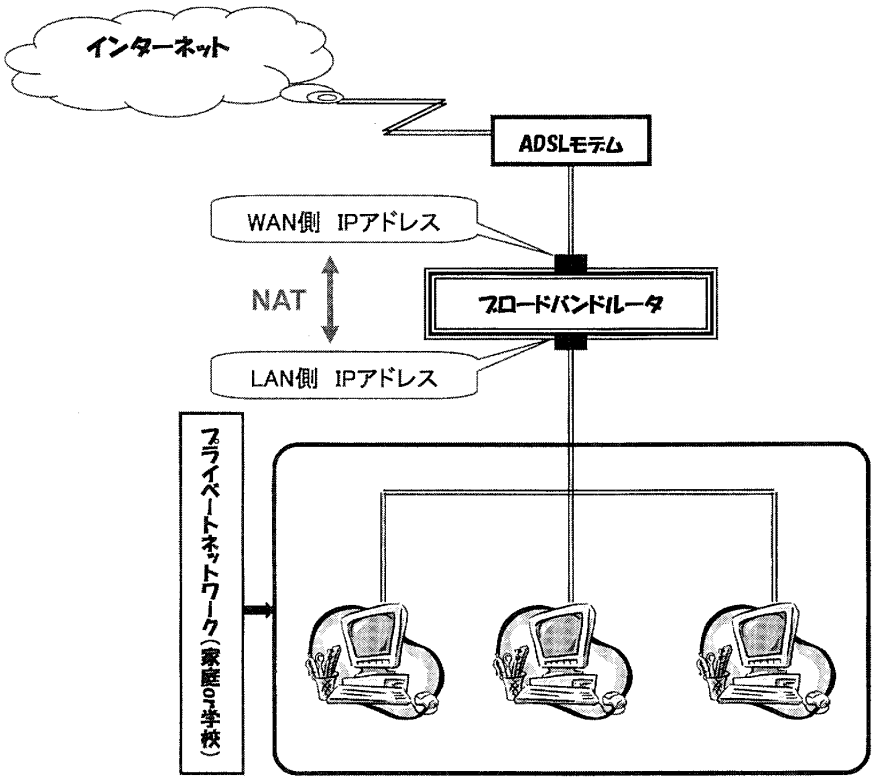


図1　プライベートネットワークの構築

てられたPCが，インターネットに接続できるようにする（通常インターネットにおいて，プライベートIPアドレスが送信元あるいは受信元となっている場合，その間の通信パケットは途中経路ですぐに破棄される取り決めになっている）。

以上のような簡単な設定をすることで，ブロードバンドルータの外側（WAN側）からのブラスターワーム侵入を防止できる。

2．2　パケットフィルタリングの設定

2．1の設定のみの場合，インターネット側からの侵入は防げるが，プライベートネットワーク内にブラスターワームが発生した場合，インターネットに向かってウィルスを流すこととなる。すなわち，ウィルス被害者が加害者になってしまう。著者らの経験では，このような問題のほとんどは，持ち込んだPCがウィルス感染していた場合，およびそれから学校LANの他のPCに感染した場合に発生しており，学校やネットワークセキュリティ責任者の社会的責任が問われる。したがって，通常はネットワーク接続を許可する前に，必ずその都度ウィルスチェックをかけるようにしなければならない。しかし，間違って（誰かが無許可で！）ウィルス感染したPCをプライベートネットワークに接続しても，そのウィルスがプライベートネットワーク（学校内）を越えてインターネットに流出しないようにすることができれば，被害は最小限（プライベートネットワーク内のみ）で済む。これを実現する方法の一つが**パケットフィルタリング機能**である（製品によっては，**ファイアウォール機能**の一部として扱われている）。この機能は，現在市販のブロードバンドルータのほとんどに標準で備わっている。

マイクロソフト社のサポートページ［1］によれば，ブラスターワームおよびその亜種は，ウィンドウズNT系OS（NT，2000，XP）でリモートプロシージャコール（RPC）用ポート（TCPポート135）が開いている場合に，そのポートを使って感染していく。したがって，TCPポート135をブロードバンドルータ出口で塞いで（閉じて）しまえば，簡単にワーム拡大を防ぐことができる。以下，表1にその設定例を示す。

表１　TCPポート１３５を閉じる場合の設定

インターフェイス	プロトコル	動　作	送信元IPアドレス	送信先IPアドレス
WAN側 （WAN⇒LAN）	TCPポート １３５	常　時 ブロック	全て（ANY）	全て（ANY）
LAN側 （LAN⇒WAN）	TCPポート １３５	常　時 ブロック	全て（ANY）	全て（ANY）

ここで，上記設定はブラスターワームを想定し，TCPポート１３５のみを閉じる場合の設定としている。また，TCP，UDP等のプロトコルおよびポートに関しては，文献［６］，［７］で簡単・詳細に説明されているので，参考にしてほしい。

なお，サーバーのリモート管理やファイル転送に用いるTELNETやFTPのサービスは，通信が暗号化されないため，使用頻度が高くないのであれば，同様に閉じておいた方がよい。これらの代替として，通信が暗号化されるSSH（SecureSHell）を用いることが推奨されている。Windows用ではPutty（TELNET端末/FTPの代替）［８］やWinSCP（FTPの代替）［９］等のアプリケーションが有名で，いずれも暗号の強化されたSSH２対応である。なお，Mac OS XはUNIXベースなので，SSHは標準となっている。

３．設定例（㈱マイクロ総合研究所のSuper Opt 70を用いた場合）

本章では，㈱マイクロ総合研究所のブロードバンドルータ「Super Opt 70」を用いて，TCPポート１３５を閉じる設定例等を具体的に示す。

３．１　IPの設定例

３．１．１　WAN側の設定

１．LAN側のポートの一つにPCを接続し，ウィンドウズ上で「コントロールパネル」→「ネットワーク接続」→「ローカルエリア接続」→「プロパティ」を開き，「インターネットプロトコル（TCP/IP）」内の「プロパティ」で，「IPアドレスを自動で取得する」を選択する。

２．次に，インターネット・エクスプローラ（IE）を立ち上げ，ブロードバンドルータのアドレスhttp://192.168.0.1にアクセスして，ルータの設定画面を開く。

３．左側の欄から「動作モード設定」を選び，「DHCPクライアント」，「PPPoEクライアント」，「IPアドレス固定」から選択する（図２（ａ）参照）。

４．固定（グローバル）IPアドレスを割り当る場合は，「IPアドレス固定（１～16）」を選んでIPアドレス，デフォルトゲートウェイ，WAN側IPマスカレード変換用IPアドレス（IPアドレスと同じでよい），サブネットマスク，LAN側変換後の先頭IPアドレス（デフォルトでよい），DNSアドレスを入力する（図２参照（ｂ）参照）。最後に「設定」をクリックし，設定を保存する。

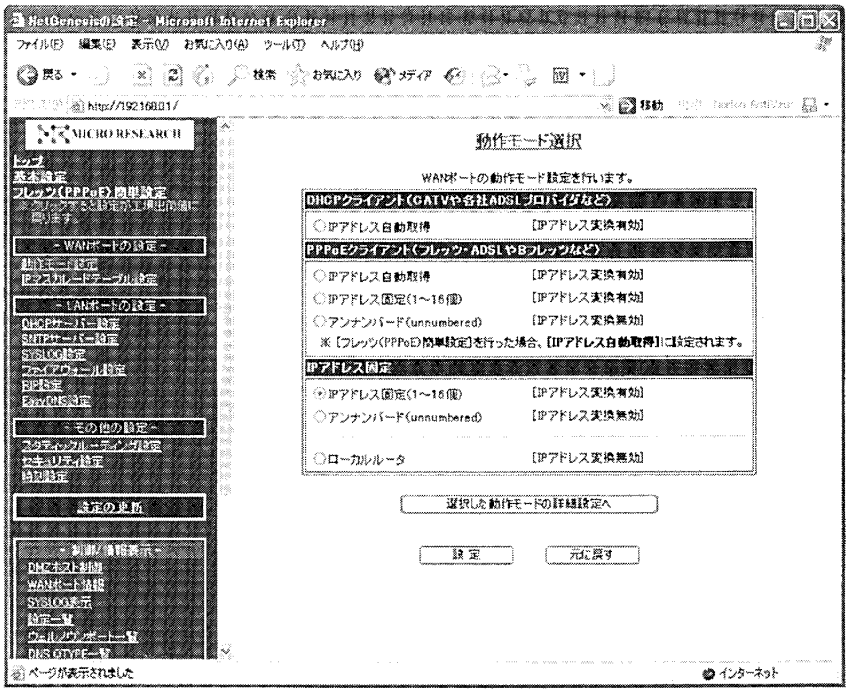
３．１．２　LAN側の設定

１．WAN側の設定と同様に，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，設定画面を開く。

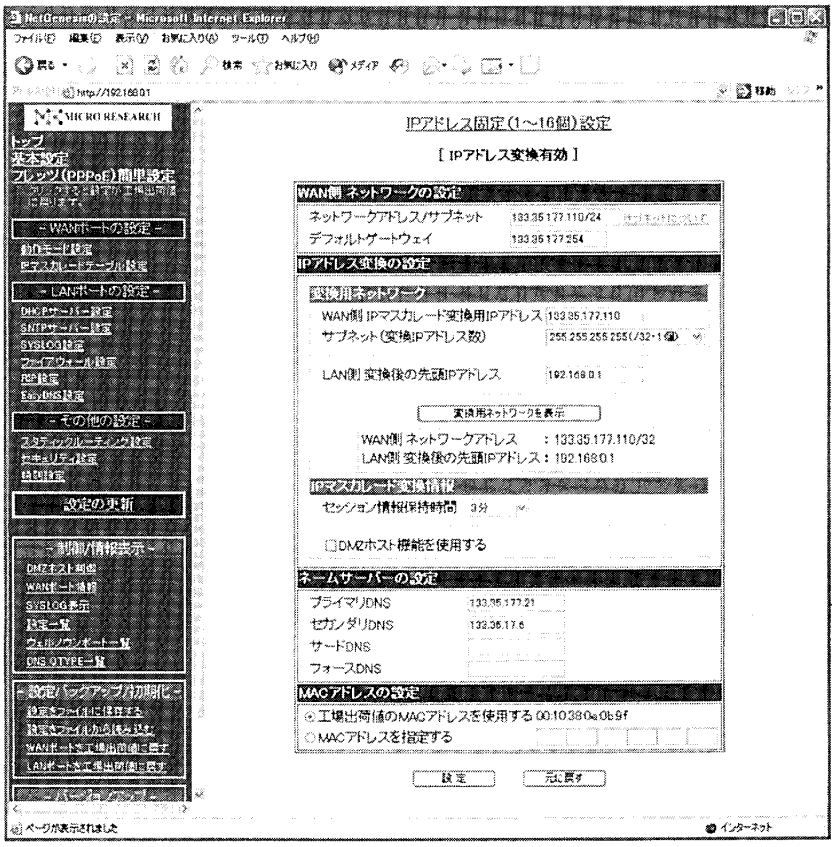
２．左の欄から「LANポートの設定」から「DHCPサーバーの設定」を選ぶ。先頭IPアドレス/サブネットが192.168.0.2/24となっていることを確認する（デフォルト値）。

３．これでプライベートアドレス内に接続したPCに自動的にプライベートIPアドレスを割り当てるDHCPサーバー機能が動作する。接続可能とするクライアント数を「付与IPアドレス数」に入力する。ここでは最大の64と入力している（図３参照）。

４．この他に，「DNS」，「ドメイン名」，「リース時間」を必要に応じて入力し，「設定」をクリックする。



（a）　「動作モード設定」



（b）　「IPアドレス固定」の設定例

図2　WANポートの設定

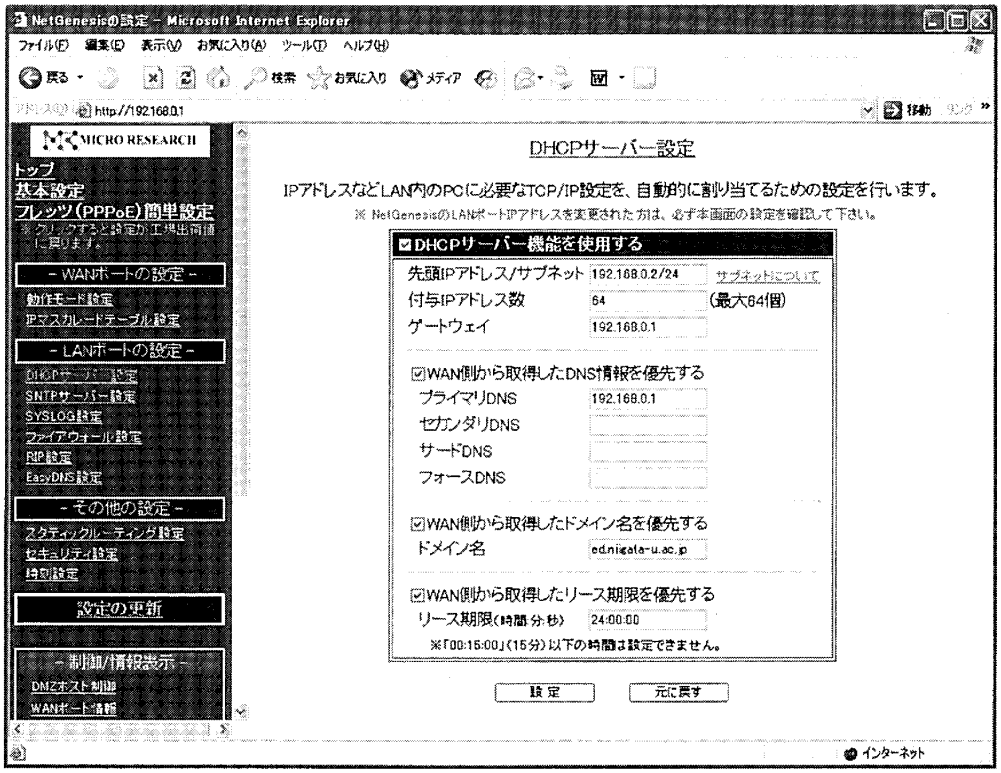


図3　LANポートの設定（DHCPサーバー設定）

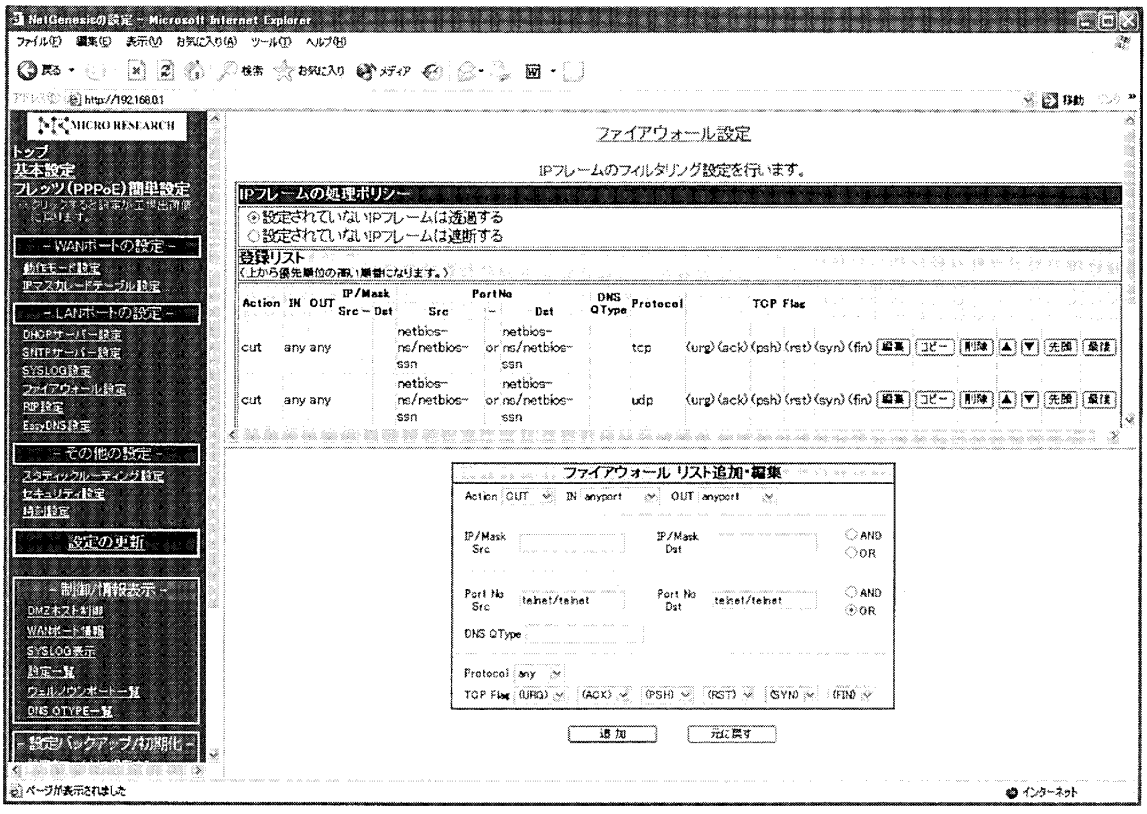


図4　TELNETの制限

3．2　パケットフィルタリングの設定例

ここでは，一般アプリケーションであるTELNETと，今回のブラスターワームで悪用される可能性のあるTCPポート１３５を例に，その制限方法を紹介する。

3．2．1　TELNETの制限

1．3．1のIPの設定例と同様にルータの設定画面を開き，「LANポートの設定」→「ファイアウォール設定」を選択する。
2．「登録リスト」の一番下に何も書かれていない欄があるので，その欄の「編集」をクリックする。
3．「ファイアウォール リスト追加・編集」で，Action「Cut」, IN「Any point」, OUT「Any point」, Port No Src「telnet/telnet」, Port No Dst「telnet/telnet」, Protocol「Any」を入力し，「追加」をクリックする（図4参照)。
4．以上のような操作を行うと，ファイアウォール設定の登録リストにポリシーが追加され，TELNETが禁止される。なお，IN「Any point」, OUT「Any point」としているので，この例ではTELNETはWAN→LAN, LAN→WANの両方向で制限されている。

3．2．2　TCPポート１３５の制限

3．2．1と同様に，ブラスターが悪用しているTCPポート１３５を制限する設定を行う。
1．「LANポートの設定」→「ファイアウォール設定」を選択し，「登録リスト」下の何も書かれていない欄から「編集」をクリックする。
2．「ファイアウォール リスト追加・編集」で，Action「Cut」, IN「LAN port」, OUT「WAN port」, Port No Src「135/135」, Port No Dst「135/135」, Protocol「TCP」を入力し，「追加」をクリックする（図5参照)。
3．以上の操作で，ファイアウォール設定の登録リストにポリシーが追加され，TCPポート１３５がLAN→WANの方向で禁止される。
4．図6にセキュリティポリシー追加後の「ファイアウォール リスト追加・編集」を示す。

4．より高いセキュリティレベル確保のために

これまでに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を適切に使用することにより，ネットワークのセキュリティレベルは大幅に改善される。しかしながら，さらに（企業と同等に近い）高いセキュリティレベルを求める場合は，「認証」技術を組み合わせる必要がある。一般に用いられている認証技術には，1．MACアドレス認証，2．ユーザID認証があり，通常は両技術を適切に組み合わせて使用する。

MACアドレス［6］,［7］とは，NIC（ネットワークカード）に固有のアドレスのことで，NIC一枚一枚で異なる。ルータははじめにこのアドレス情報を基に情報のやりとりをはじめる。したがって，ブロードバンドルータに接続を許可するNICのMACアドレスを登録しておき，登録したNICを備えたPCのみがインターネットに接続できるようにすることができる。一方，Radiusはユーザ認証技術の一つで，簡単に言えば，事前にユーザ登録・パスワード登録をしたユーザのみがネットワーク使用を許可される仕組みだが，詳細は文献［11］を参照してほしい。

数年前までは，1．の実現にはインテリジェント・スイッチングハブ（十万円程度～），2．にはRadiusサーバーおよびRadius認証対応ルータ（またはスイッチ）（共に数十万円～）［11］が必要だった。しかし，最近これら高価なネットワーク機器に代替する比較的安価な製品が市販されたので，本章ではその「認証機能付」ネットワーク機器の紹介と簡単な設定例を示す。

4．1　MACアドレス認証によるクライアントPCの接続許可

これまで，有線LAN用のネットワーク機器の中では，高価なインテリジェントハブにのみMACアドレス認証によるネットワーク接続制限機能が備わっていた。しかし，最近の急激な無線LANシステムの普及に

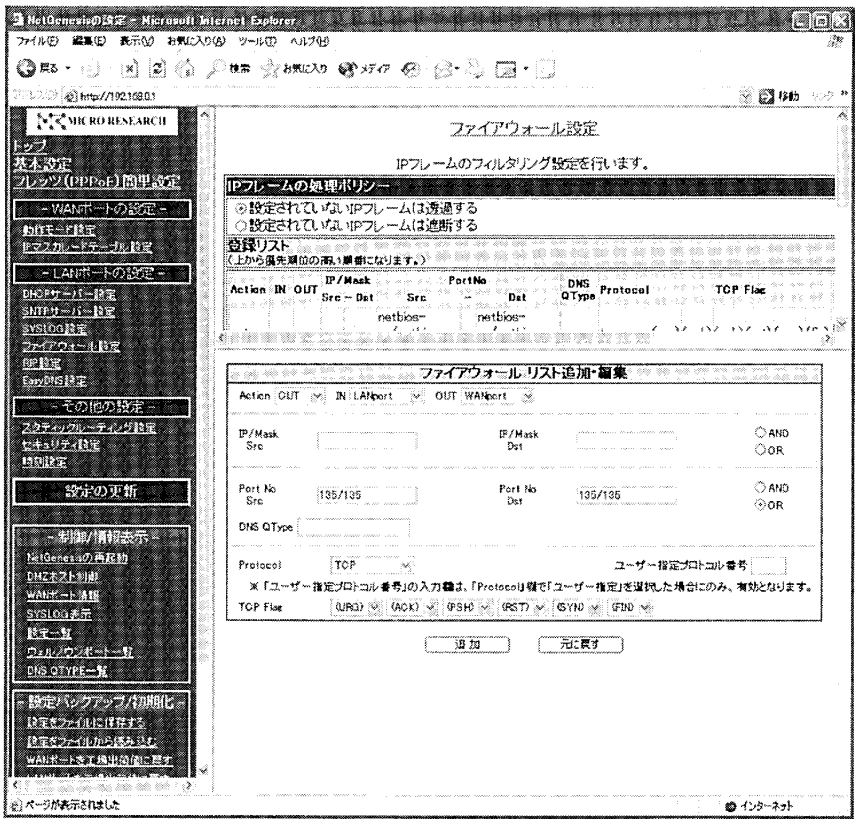


図5 TCPポート１３５（RPC）の制限

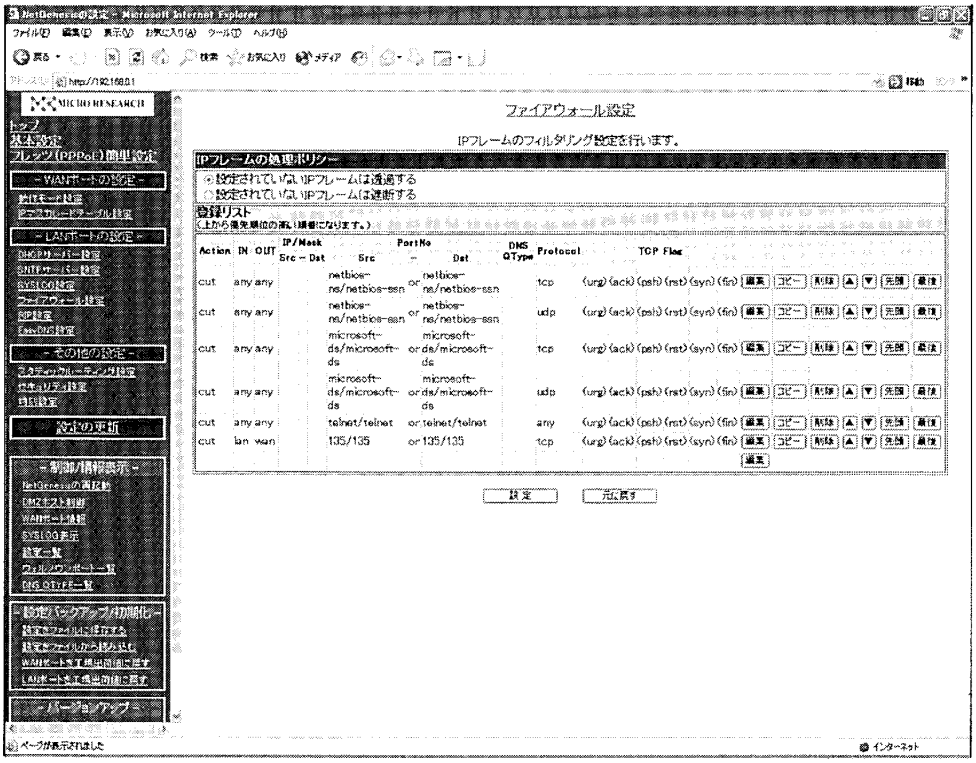


図6 TELNETおよびTCPポート１３５（RPC）制限後のリスト

伴い，無線LAN通信ポートにのみに適用されていたMACアドレス制限機能が，有線LANポートにまで拡張された製品が市販されはじめた。ここで紹介する㈱IOデータ機器のWN-AG/BBR-Sは，そのような無線LANブロードバンドルータの一つで，２万程度で市販されている。以下にそのMACアドレス制限の設定例を示す。

1．他製品と同様に，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，左欄のメインメニューから「アクセス制御」を選ぶ（図７（ａ）参照)。
2．「MACアドレス テーブル」の「追加」ボタンをクリックし，「名前（何でもよい)」と「MACアドレス」を入力する。MACアドレスは通常各NICに記載されているが，もしも見つからない場合は登録したいNICを備えたPCをLANポートに接続して，arpコマンドを用いて得ればよい。
3．２．の手順で，各NICのMACアドレスが登録されるので，最後に「MACアドレス フィルタ」で「許可」を選んで，「設定」をクリックする（図７（ｂ）参照)。以上の設定で，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を利用できない。

４．２　ユーザIDとパスワードを用いた認証によるユーザの接続許可

Radius認証のような本格的なユーザID認証システムではないが，比較的少人数のユーザを対象とした場合の簡易的なユーザID認証機能を備えたブロードバンドルータが市販されているので，その紹介と簡単な設定例を示す。

４．２．１　ユーザ認証機能の設定例

センチュリー・システムズ㈱のブロードバンドルータXR-410/TR2（５万円程度）は，「ゲートウェイ認証機能」と呼ばれる簡易ユーザID機能を備えており，このルータを経由して外部にアクセスする場合に「ユーザ認証」を必要とすることで，利用ユーザの管理ができる。以下にその設定例を示す。

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」を選ぶ。
2．基本設定の「使用／未使用」欄は「使用する」，「認証方法」欄は「ローカル」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８（ａ）参照)。
3．ユーザの登録はユーザ設定でユーザIDとパスワードを登録する（図８（ｂ）参照)。

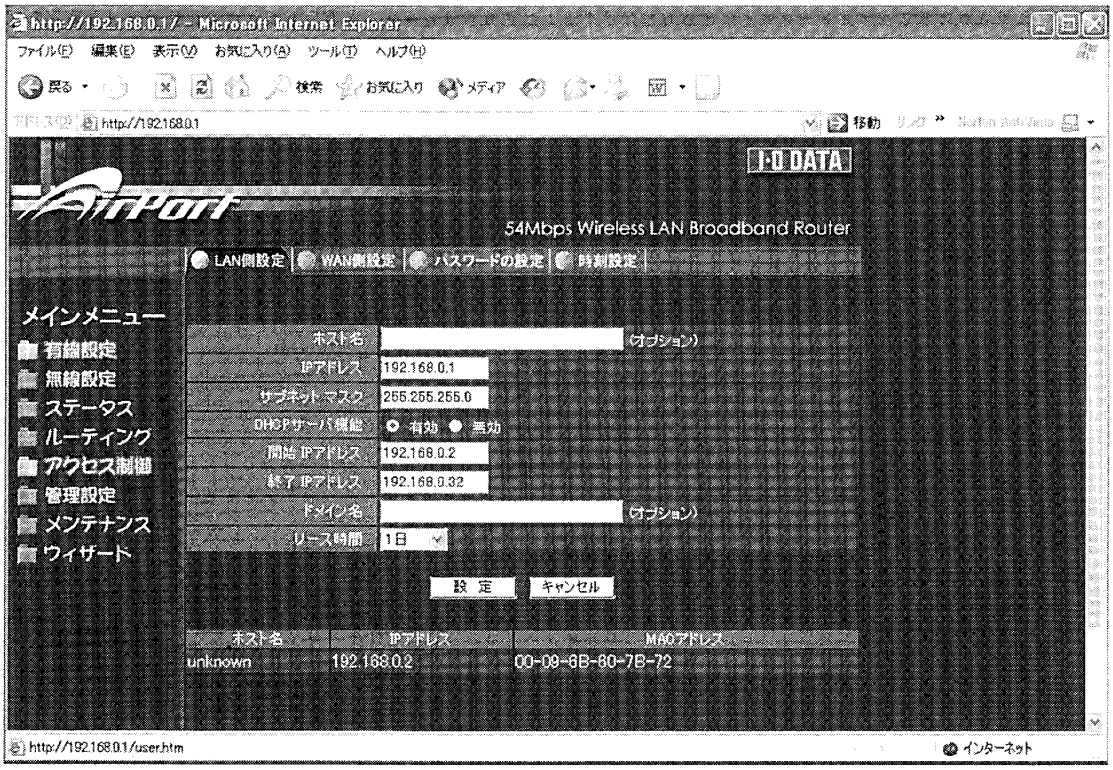
４．２．２　ユーザ認証機能の使用例

以下に，４．２．１で設定したユーザ認証機能を用いた場合のユーザ使用例を示す。

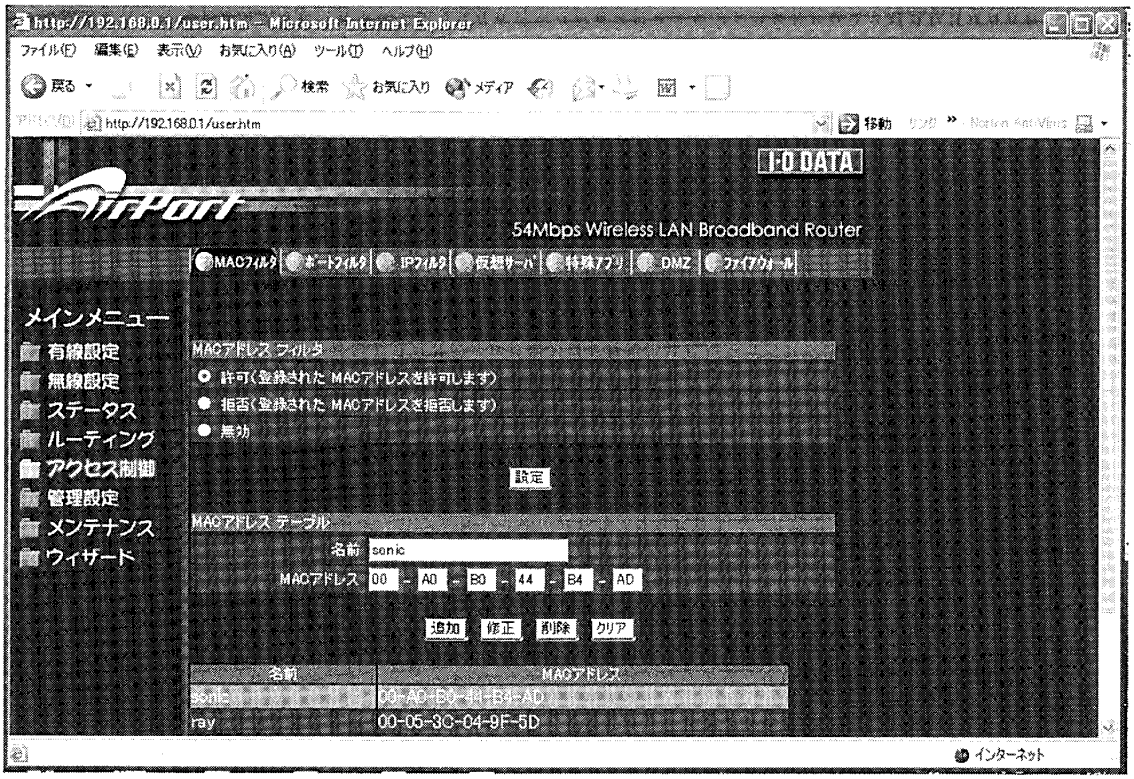
1．IEを立ち上げhttp://192.168.0.254/login.cgiにアクセスすると認証画面が表示されるので，「ユーザID」と「パスワード」を入力する（図９（ａ）参照)。
2．認証に成功すると，その旨のメッセージが表示される。基本設定の「接続許可時間」において，「認証を受けたWebブラウザのウィンドウを閉じるまで」を選択した場合には，このメッセージの画面を開いている間だけ接続できる（図９（ｂ）参照)。

５．各種ブロードバンドルータのデータ通信速度について

最後に，これまでに紹介したブロードバンドルータが，実際にどの程度実用に耐えうるかを確認するために，各ルータのデータ通信速度の測定を行った。ブロードバンドルータ各種の実質的なデータ通信速度を測定するために，図10に示すような構成のネットワークを構築した。ブロードバンドルータLAN側のプライベートネットワーク内部に100Mスイッチを介して６台のノートPC（Windows XPクライアント）を接続し，WAN側のプライベートネットワーク外部にはLinuxファイルサーバーを置いた。各ノートPCからファイル

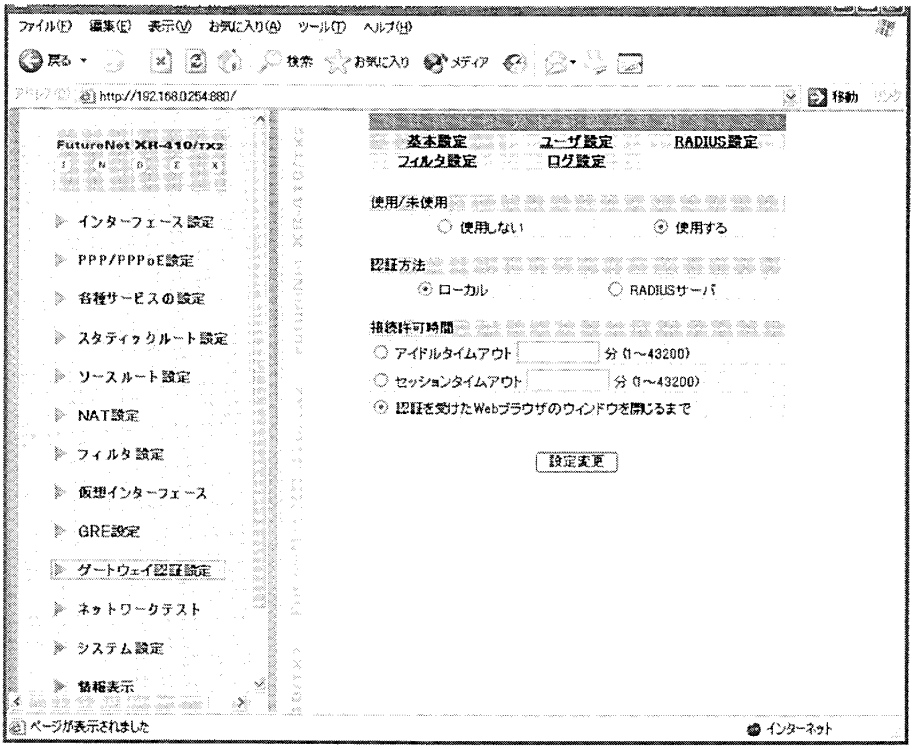


（a） メインメニュー

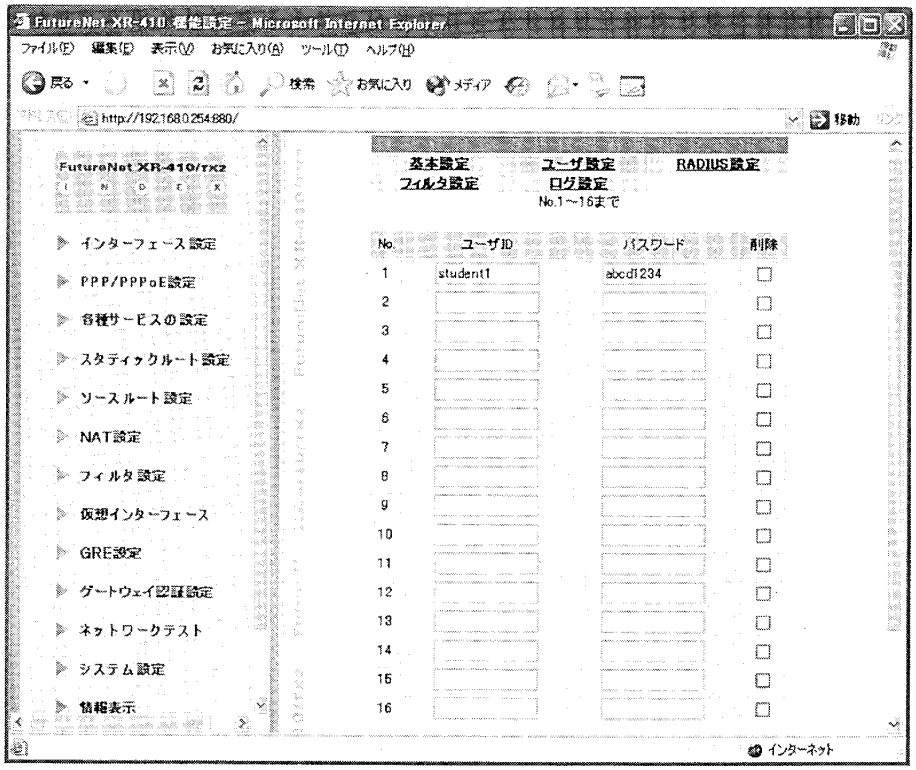


（b） MACアドレス フィルタ制限の設定

図 7 MACアドレス制限によるクライアント認証

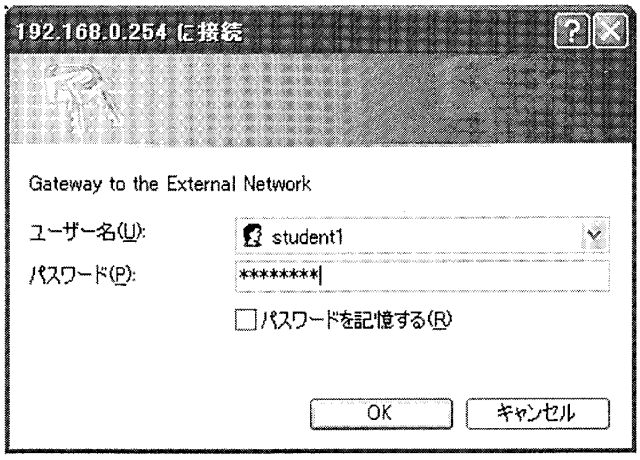


（a） 基本設定

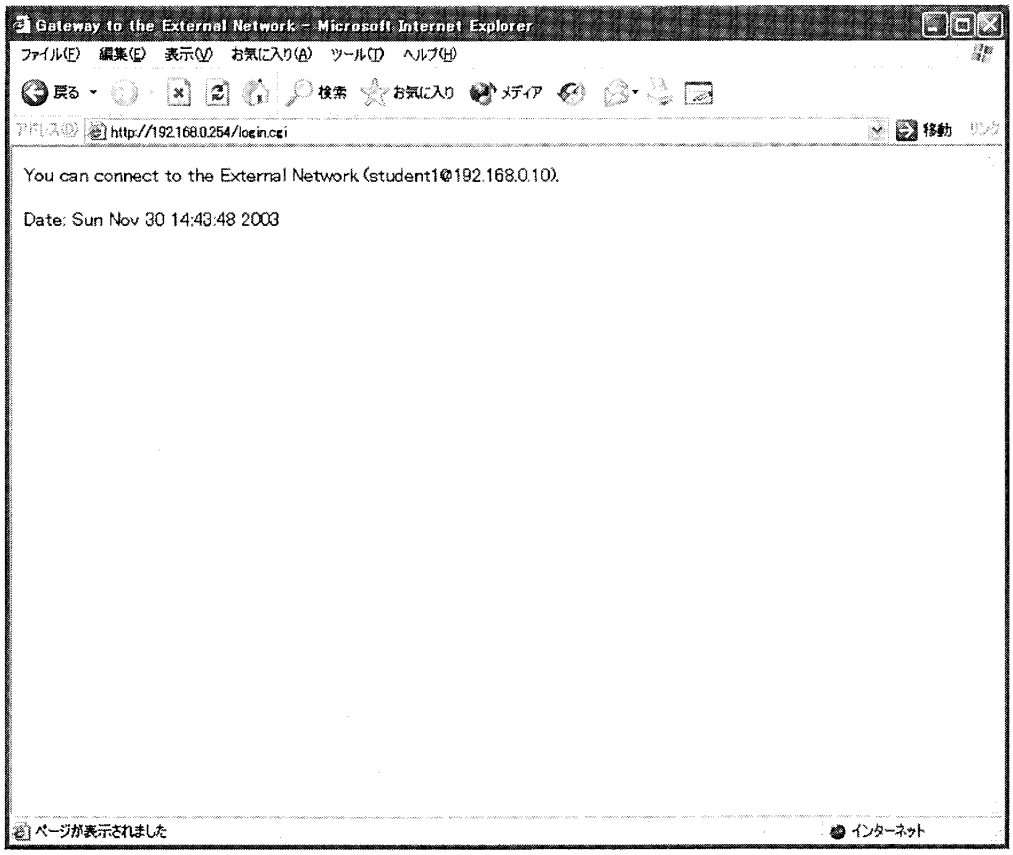


（b） ユーザ登録

図8 ゲートウェイ認証機能の設定



（a） ユーザIDとパスワードの入力



（b） 認証結果

図9 ゲートウェイ認証機能のユーザ利用例

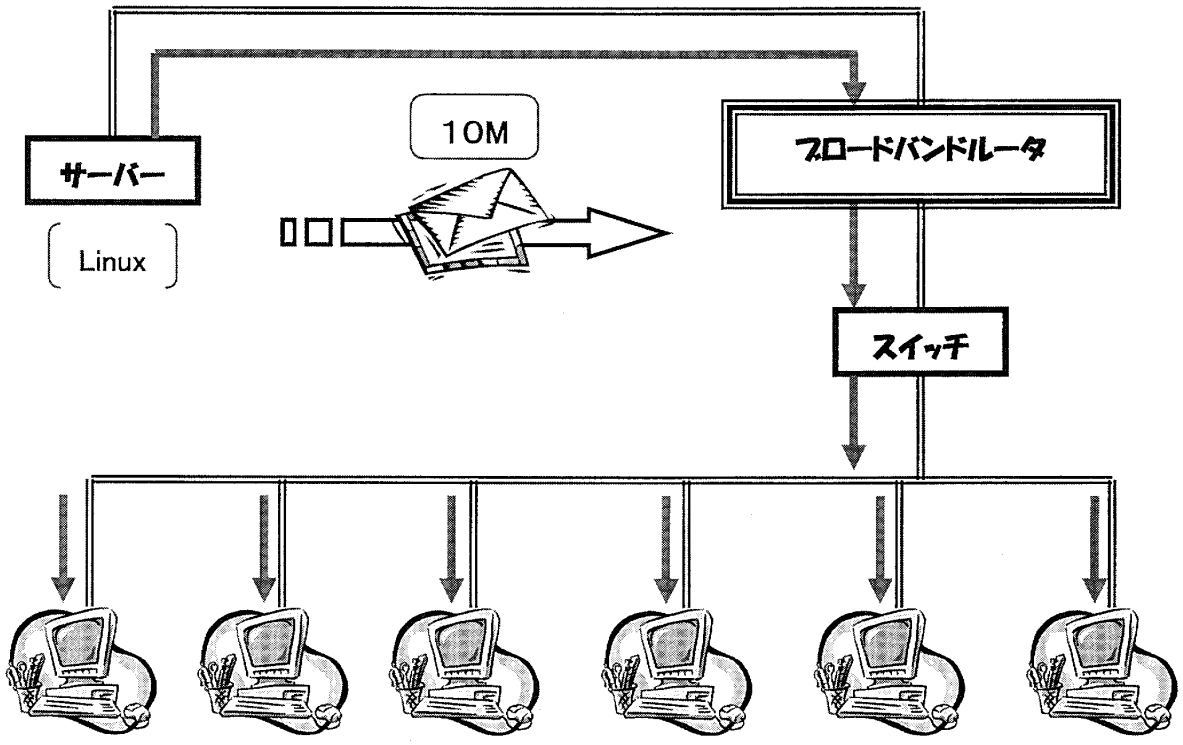


図10　ブロードバンドルータの通信速度測定環境

サーバーに同時アクセスし，10MBファイルのダウンロード完了時間を測定した。今回の実験に使用したブロードバンドルータは６機種で，測定結果は表２の通りで，全ての機種で優れた数値を得ることができた。なお，文献［５］においては，約90口の情報コンセントのある教室で同様のネットワークを構築して実験を行ったため，若干速度が遅く観測された。

表２　各ブロードバンドルータの通信速度測定結果

ルータ名	メーカ名	VPN機能の有無	MACアドレス制限の有無		ユーザ認証機能の有無		ダウンロード時間（10MB）
Net Genesis OPT	マイクロ総合研究所	無	無		無		約17秒
Super OPT70	マイクロ総合研究所	無	無		無		約６秒
MR104DV	OMRON	有（IPsec）	無		無		約５秒
RT57i	YAMAHA	有（PPTP）	無		無		約３秒
WN-AG/BBR-S（無線LANルータ）	IOデータ機器	無	有	OFF	無		約４秒（２台）
				ON			約４秒（２台）
XR-410/TR2	センチュリー・システムズ	有（IPsec）	無		有	OFF	約９秒
						ON	約10秒

前記測定結果より，通信を暗号化してトンネリングを実現するVPN（仮想専用線）[10] 機能を備えたブロードバンドルータが高性能なCPUを搭載しているため，非常に高速なデータ通信速度を実現していることがわかった。ただし，簡易ユーザ認証機能を有する機種は，認証機能を重視しているためか，他のVPN対応ルータに比べると少し遅かった。しかしながら，ユーザ認証の有無による通信速度の差がほとんどなかった点は評価できる。一方，MACアドレス制限機能をもつ無線LANルータも，有線LANポート接続制限の有無による通信速度差はなかった。しかし，この機種は無線通信重視のためか，6台同時有線接続による実験が行えなかった（したがって，表2には2台同時接続時の結果を示している）。

以上の結果より，無線LANルータを除く5台の機種は，20～40台のPCを前提とした小中学校のコンピュータ教室等の環境下であれば，必要十分な速度性能を有しているものと考えられる。このことは，本学教育人間科学部における実績からも十分説明できる（付録参照）。

5．むすび

本稿では，市販ブロードバンドルータを利用してプライベートネットワークを構築し，簡単なパケットフィルタリング設定を行うことで，ブラスターワーム型のコンピュータウィルスの感染拡大を防ぐ方法を紹介した。ネットワーク・PCを使用する際，以下の3点

1．OSに脆弱性が見つけられたら，速やかにOSのアップデート作業を行う。

2．コンピュータ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う。

の重要性を理解させて，責任をもって実行するよう指導し，さらに本稿で示した一例のような情報ネットワークの初歩技術をきちんと教育すれば，中学生，高校生でも比較的容易に情報セキュリティ向上に必要なスキルを身につけられることを明確にした。これにより，情報セキュリティ教育の有効性および重要性を示した。

日本の中学校，高等学校では，情報リテラシーや本稿で述べたような基礎的な情報教育が中心であるが，世界における情報教育の水準は極めて高い。例えば，ネットワーク技術者資格の入門的位置づけであるシスコシステム社のCCNA（Cisco Certified Network Associate）認定制度［7］は，米国では主に高校生が対象とされているが，現在の日本では大学生でもその取得は決して容易ではない。インドや中国のIT教育水準も，日本をはるかに越えている［12］。

以上のことからも，日本がより高度な技術大国を目指すためには，まずは小中学校において，情報リテラシー教育だけではなく，情報セキュリティ，情報ネットワーク技術などのより高度な内容を含んだ情報教育が必須であり，その教育システムの一日も早い構築が望まれる。

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を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年生の芳賀洋介君に感謝します。

参考文献

［1］http://support.microsoft.com/
［2］http://www.ipa.go.jp/
［3］http://www.zdnet.co.jp/dict/security/virus/worm/02656.html
［4］新潟大学総合情報処理センター，第1回情報セキュリティ講習会資料，2003.
［5］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，No.619，pp.20-26，Feb.2004.
［6］高木弘幸 他，“パソコンTCP/IP教科書，”アスキー出版局，1995.

［7］Cisco CCNA試験 #640-607 公式ガイドブック，ソフトバンク，2002.
［8］http://www.chiark.greenend.org.uk/~sgtatham/putty/
［9］http://winscp.sourceforge.net/eng/
［10］伊藤幸雄 他，“図解・標準 最新VPNハンドブック，”秀和システム，2003.
［11］Jonathan Hassell，“Radius，”Oreilly，2002.
［12］榊原英資，“インドIT革命の驚異，”文春新書，2001.

付録

本報告で紹介した市販ブロードバンドルータを用いた対策は，文系学生向け情報基礎科目を円滑に行うために，本学教育人間科学部がこれまで（1999年～）に情報インフラ整備を行ってきた際のノウハウが基礎となっており，約100人超規模での同時インターネット接続時でもトラブルなしに講義，演習を行えた実績がある。

以下にその年表および技術的内容を示す。

●1999年 情報コンセントを備えた講義室を設置

105および204講義室に各々90および120口の情報コンセントを設置した。情報関係の演習における100人規模の同時アクセスを想定し，それに伴う膨大なトラフィック量の軽減策として，各講義室内のネットワークを物理的に半分にわけ，それぞれを異なるセグメントに接続することで対処を試みた。ここで，各セグメントにはPCベースのLinuxサーバーを設置し，そのDHCPサーバー機能を用いて，接続される全てのクライアントに「グローバルIPアドレス」を貸与するシステムを導入した。

●2000年 サービス設置

Proxyサービスを設置することにより，大容量プログラムダウンロード時のトラフィック量増加に起因する通信速度低下の軽減を試みた。105，204講義室内を物理的に二つのセグメントに分けていたため，各セグメント上のLinuxサーバー毎にProxyサービスを設定（Proxyサーバーを2台設置）する必要が生じた。この結果，通信速度低下はかなり軽減できたが，貸与されているIPアドレスのセグメントによって，各クライアントでネットワーク接続プロパティのProxy設定を変更する必要が生じた。

●2001年 NINESの更新

新潟大学学内LAN（通称NINES）が更新され，これまでの基幹100Mbps，末端10Mbpsから，基幹10Gbps，末端100Mbpsに飛躍的な通信速度の向上が実現された。

●2002年 プライベートネットワークへの変換

NINES更新に伴い，本学総合情報処理センターよりRadius認証機能付有線スイッチ（OmniStack）が供給され，認証機能を介したDHCPサービスが開始された。このため，105，204講義室内でのPCベースLinuxサーバーによるDHCPサービスの廃止を決めた。しかしながら，Radius認証機能付有線スイッチが10クライアント程度（厳密には6クライアント）での認証接続に失敗することが，スイッチ提供業者との共同実験により明らかとなったため，実用にはいたらず断念した。そこで以下に示す代替策をとった。

＜市販ブロードバンドルータの利用＞

PCベースのLinuxサーバーではHDDの故障の危険性があること（事実，3年目を迎えて，Linuxサーバーがやや不安定になっていた），セキュリティ対策としてプライベートネットワークを構築する必要性が出てきたこともあり，新たな代替えシステムを検討した。様々な雑誌の評価等を参考に，市販家庭向けブロードバンドルータ（㈱マイクロ総合研究所NetGenesis OPT，OPT-R）を試用してみたところ，十分実用に耐えうることが実験により検証されたため，その利用を決断した。以下にその利点を挙げる。

1．ディスクレス構成による安定したネットワークシステムの提供

2．NAT機能を利用したプライベートIPアドレス貸与

学外アタックから学内LANに接続されたサーバーおよびクライアントを防御するために，プライベートローカルIPを貸与する方法を取った。

3．ファイアウォール機能を利用した特定サービスの利用制限

講義室内からの特定サービス（ここではTELNET，FTP）の利用を制限可能となった。

4．高速な同時インターネットアクセススピードの実現

必要十分な通信速度を保ちつつ，ルータ1台あたり50台以上のクライアント同時利用を実現。105，204室以外の教室（例えば情報処理教室302室）にもOPT-Rを基とした同様のシステムを導入し，広範囲でDHCPサービスが利用可能となった。

●2003年　学部事務室，技術部内ネットワークのプライベートネットワーク化

市販家庭向けブロードバンドルータ（NetGenesis OPT70）を利用してプライベートネットワーク化した。近年は一般のUNIX，PCベースのサーバーのみならず，プリントサーバー（ネットワークプリンタ）を狙った外部からのアタックが頻繁に起きるようになった。事実上記2部署に設置されたプリンタサーバーが攻撃を受けたことが判明した。そこで，このセキュリティ対策として，ネットワークをプライベートネットワーク化して外部からのアタックを防御するシステムに変更した。