ISP の回線を利用したネットワーク環境の構築

宮崎大学　工学部教育研究支援技術センター
森　圭史朗

はじめに

業務支援を行っていた産学連携支援センターにおいて，入居している企業に対してのインターネット環境に QTNet の光回線（BBIQ）が導入されることとなった．産学連携支援センターからブロードバンドルータ導入の準備するよう通知を受け，支援先と構築するネットワーク環境の検討を行った．単に光回線を導入するのであれば，ブロードバンドルータを用いてネットワーク構築を行ったが，Web サーバやメールサーバ等の運用を行う必要が生じたため，FreeBSD を用いた PPPoE 認証を行う NAPT サーバを構築することにした．

本報では，各種サーバ（Web サーバやメールサーバ等）とブロードバンドルータ（PPPoE 認証と NAPT）の機能を一体化させたサーバによるネットワーク環境を構築したことについて報告する．

キーワード：FreeBSD　FTTH　PPPoE　NAPT　MPD　IPFW

1. 概要

構築したネットワークの概略図を下の図 1 に示す．

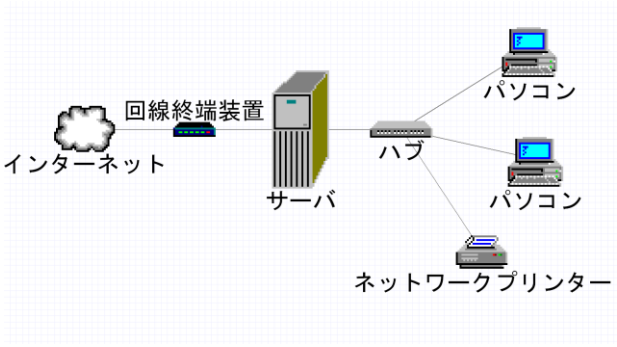

図 1　概略図

1.1　目的

図 1 のネットワークは，図の中心にあるサーバ部分がすべての制御を行う．サーバは，インターネット（サーバより左側）へ接続するために行う PPPoE 認証と各種サーバ（DNS，メール，Web 等）の運用を行う．そして，プライベートネットワーク側（サーバより右側）では，NAPT と DHCP サーバによりプライベート IP アドレスを用いたネットワーク環境を構築する．NAPT によって構築されたプライベートネットワークは，インターネット上からのアクセスができないネットワーク環境にすることで，ファイル共有等を安全に行えるようにする．

1.2　PPPoE（PPP over Ethernet）

PPPoE とは，PPP の機能を Ethernet を通して利用するためのプロトコル（規約）である．ADSL や光ファイバ通信（FTTH）サービス提供を行っている ISP（プロバイダ）のほとんどがこの PPPoE を利用してユーザ一認証を行っている．通常，LAN の MTU 最大値は 1500byte であるが，PPPoE が実装されるネットワークでは，PPPoE ヘッダ部分 8byte を差し引いた 1492byte が最大値となる．

1.3　MTU（Maximum Transmission Unit）

MTU とは，ネットワーク上で 1 回に送信可能なパケットサイズの上限である．MTU は，大きすぎると送信するためのパケット再分割が必要になり，スループット速度（通信速度）が低下する．また，小さすぎてもパケット送信回数が増えてしまうため，スループット速度は低下する．

1.4　NAPT（Network Address Port Translation）

NAPT とは，WAN 側に与えられている 1 つのグローバル IP アドレスを LAN 側にある複数のプライベート IP アドレスで共有することである．IP マスカレードと呼ばれることもある．NAPT は，IP アドレスだけでなく TCP や UDP のポート番号も含めて変換を行うため，グローバル IP アドレス 1 つで複数のプライベート IP アドレスを運用できる．

1.5　グローバル IP とプライベート IP アドレス

グローバル IP アドレスは，インターネット上に存在する IP アドレスで世界中のいかなるところからでもアクセス可能な IP アドレスである．逆にプライベート IP アドレスは，インターネット上に存在しない IP アドレスである．インターネットが普及する以前は，インターネットに接続するすべてのネットワーク機器にグローバル IP が使用されていたが，IP アドレス枯渇問題が表面化した現在では，企業内や家庭内のようにインターネット上からアクセスする必要がないネットワーク

に対し，プライベート IP が使用されている．表 1 にプライベート IP アドレス範囲を示す．

表 1　プライベート IP アドレス範囲

クラス	アドレス範囲
クラス A	10.0.0.0 - 10.255.255.255
クラス B	172.16.0.0 - 172.31.255.255
クラス C	192.168.0.0 - 192.168.255.255

2. 構築したネットワーク環境

図 2 に構築したネットワーク環境のネットワーク図を示す．①～②のインターネットから回線終端装置までは，光ケーブルで ISP が準備する．

③～⑥までの 2 つのファイアーウォール間は，FreeBSD を用いて 1 台のパソコンで構築する．FreeBSD で構築したサーバは，2 つの LAN カードを使用してインターネット 側（WAN 側）とプライベートネットワーク側（LAN 側）にそれぞれ分ける．サーバから WAN 側への通信は，PPPoE 認証サーバにより常にインターネットと接続された状態を保つ．回線終端装置から構築したサーバまで（②と③の間）及びプライベートネットワーク内（⑥～⑧）では，LAN ケーブルでそれぞれのネットワーク機器を接続する．

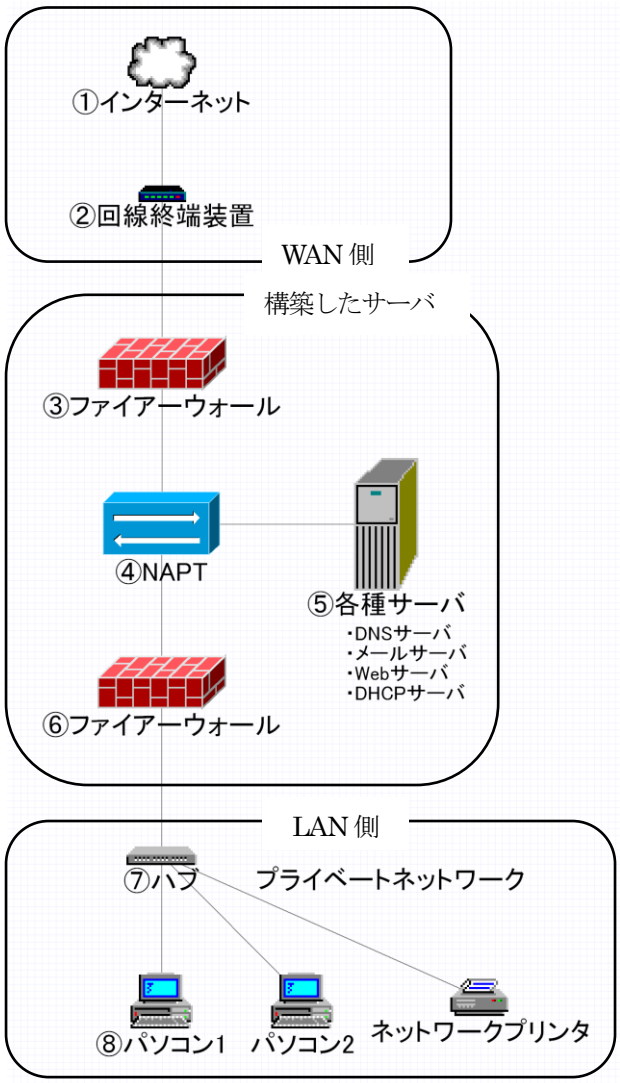

図 2　ネットワーク図

③はグローバル IP に対するファイアーウォール，⑥はプライベート IP に対するファイアーウォールである．③のファイアーウォールは，インターネット上からのアクセス制限を行い，⑥のファイアーウォールは，プライベートネットワーク内のアクセス制限を行う．⑤の各種サーバは，Bind9，Apache2，Postfix，DHCP 等のインターネット及びプライベートネットワークに提供するサーバソフトウェアの運用を行う．DNS サーバとファイアーウォールの設定により，WAN 側及び LAN 側から各種サーバへのアクセスは， WAN 側からの場合はグローバル IP，LAN 側からの場合はプライベート IP からのアクセスとなる．④の NAPT は， プライベートネットワークからインターネットへアクセスする際，プライベート IP からグローバル IP に変換する．

⑦，⑧のプライベートネットワーク内では，ユーザーがパソコンを LAN に接続しただけでインターネット利用を可能にするため， DHCP サーバが自動的にネットワーク機器のインターネットプロトコル（TCP/IP）の設定を行う．

3. サーバ構成

サーバのパフォーマンスに関わる主なハードウェア構成を表 2 に，OS 及び各種サーバソフトウェア構成を表 3 に示す．

表 2　サーバのハードウェア構成

デバイス名	仕　様
CPU	Pentium4　2.6GHz　512KB
Memory	PC133 SDRAM-DIMM　1.5GB
HDD	3.5 インチ IDE 160GB 7200rpm UATA100
LAN	Intel 82550 Pro/100 PCI　100BASE-TX （WAN 側と LAN 側にそれぞれ 1 つずつ）

表 3　OS 及び各種サーバソフトウェア構成

OS	FreeBSD-6.1
Firewall	IPFW（OS 付随）
PPPoE	MPD-4.1
NAPT	IPNAT（IPFILTER - 4.1.8 の一部）
各種サーバ	Bind9，Apache2，Postfix，DHCP 等

サーバOSは, FreeBSD-6.1を導入する. FreeBSDは, デフォルト(初期設定)インストールがCD1枚で済み, 必要最低限のパッケージしか導入されないため, HDDの容量を節約でき, パソコン全体の負荷が軽くて済む.

ブロードバンドルータとしての機能する部分は, MPD4 + IPNAT + IPFWのソフトウェア構成で運用する. PPPoE認証サーバは, OSに備わっているuser-pppを用いてもPPPoE認証は行えたが, プライベートネットワークからのicmp（ping等）を許可していないホストに対し, 接続が確立できないという問題があるので, MPD4を導入する. NAPTは, NATDの場合, CPU負荷が大きくスループット速度が不安定であることから, IPFILTERのNAPT機能であるIPNATにする. ファイアーウォールは, 各種サーバとプライベートネットワーク機器に対し帯域制限を設けるため, OSに備わっているIPFWを用いる.

各種サーバソフトウェアは, 一般のサーバ構築方法と同じ方法でインストールを行う. サーバソフトウェアは, セキュリティホールが出現した際, 早急に対処できるようにそれぞれの開発元から直接ソースコードをダウンロードしてコンパイル, インストールする.

4. サーバ構築

4.1 カーネルの再構築

FreeBSD-6.1をインストール後, 始めにカーネルの再構築を行う. カーネル再構築のための設定ファイルは, 32bitOSと64bitOSでは異なる場所にあるので注意する. IPNAT + IPFWを導入する場合は, カーネルの設定ファイルに以下のオプションを追加し, コンパイル, インストールを行う.

```
options     NETGRAPH
options     NETGRAPH_BPF
options     NETGRAPH_ETHER
options     NETGRAPH_IFACE
options     NETGRAPH_PPPOE
options     NETGRAPH_SOCKET
options     IPFILTER
options     IPFIREWALL
options     IPFIREWALL_VERBOSE
options     DUMMYNET
```

4.2 PPPoE認証サーバMPDの導入

PPPoE認証は, ISPが提供するサービス内容によって設定内容が異なる. 以下にある3つのファイル（mpd.conf, mpd.links, mpd.secret）は, BBIQ回線に対してのMPD4の設定内容である.

mpd.confファイルの設定内容

```
startup:
default:
  load BBIQ
BBIQ:
  new -i ng0 BBIQ PPPoE
  set iface route default
  set iface disable on-demand
  set iface idle 0
  set iface mtu 1492
  set iface enable tcpmssfix
  set bundle disable multilink
  set auth authname ユーザー名*1)
  set link no acfcomp protocomp
  set link disable pap chap
  set link accept chap
  set link keep-alive 10 60
  set link max-redial 0
  set bundle no noretry
  set ipcp no vjcomp
  open
```

mpd.confファイルで設定されている主な内容

- ng0デバイス名で起動
- ISP指定のゲートウェイに設定
- 接続状態の維持
- MTU値は1492
- 断片化パケットの処理
- ログインIDによる認証
- PPPoEクライアントとして動作
- ネットワーク切断後の自動再接続

mpd.linksファイルの内容

```
PPPoE:
  set link type pppoe
  set pppoe iface fxp0
  set pppoe service "whatever"
  set pppoe enable originate
  set pppoe disable incoming
```

mpd.linksファイルの内容は, ほとんどの部分をサンプルファイルから引用する. インターフェース（fxp0）の部分のみがLANカードの種類によって異なる.

*1) 設定ファイルにあるユーザー名及びパスワードは, ISPから郵送されてくるログインIDである.

mpd.secret ファイルの内容

```
# Authname          Password
ユーザー名          パスワード
```

mpd.secret は，ISP から与えられたログイン ID を登録する．また，管理者以外は，ファイルの内容を確認できないようにパーミッションを 600 に変更する（-rw-------）．

3 つのファイル作成後， mpd デーモンを-b オプション（バックグラウンド動作）で起動し，動作確認を行う．ネットワークインターフェースにng0が追加され，ISP のゲートウェイの IP アドレスとサーバの IP アドレスが取得出来ていることを確認する．

4.3 NAPT（IPNAT）の設定

IPNAT では，プライベートネットワークからインターネットへアクセス際に行うプライベート IP からグローバル IP への変換，及び MTU 値の設定を行う．以下に設定内容を示す．IPNAT の MTU 値は，MSS[*2)]の値から設定される．

```
map ng0 192.168.1.0/24 -> 0/32
                    portmap tcp/udp auto mssclamp 1452
map ng0 192.168.1.0/24 -> 0/32 mssclamp 1452
```

インターネットからサーバにアクセスのあったポート（tcp5000）を，プライベートネットワークの IP アドレス（192.168.1.2）へ転送するポートフォワーディングを設定する場合は，以下を追加する．

```
rdr ng0 0.0.0.0/0 port 5000 -> 192.168.1.2 port 5000 tcp
```

4.4 ファイアーウォール（IPFW）の設定

ファイアーウォール（IPFW）は，行番号の小さい方から順次検索され，ルールが一致したところで処理が行われる．ルールは，IP アドレスの許可→UDP ポートの許可→TCP ポートの許可→ICMP の許可→ルールに該当しないパケット破棄の順番で設定を行った．以下に IPFW のルールを示す．

確立済み TCP パケットと断片化パケットの許可

```
00100 allow tcp from any to any established
00200 allow ip from any to any frag
```

帯域制限

```
00300 pipe 1 config bw 20Mbit/s
00400 pipe 2 config bw 1024Kbit/s
```

プライベートネットワーク内のパソコンからダウンロードする場合の最大スループット速度は，20Mbit/s

```
00500 pipe 1 ip from any to 192.168.1.0/24 out via fxp1
```

プライベートネットワークから各種サーバへのアクセス許可

```
00600 allow ip from 192.168.1.0/24 to me via fxp1
00700 allow ip from me to 192.168.1.0/24 via fxp1
```

DNS サーバの許可．サーバ及びプライベートネットワークからインターネットへの UDP アクセス許可

```
00800 allow udp from any to me 53
00900 allow udp from me to any keep-state via fxp0
01000 allow log udp from any to any keep-state via fxp1
01100 check-state
```

最大スループット速度 1Mbit/s でのメール, Web サーバへのアクセス許可．サーバ及びプライベートネットワークからインターネットへの tcp アクセス許可

```
01200 allow log tcp from any to any setup via fxp1
01300 pipe 2 log tcp from any to me 25 limit src-addr 5
01400 pipe 2 tcp from any to me 80
01500 allow tcp from me to any setup
```

サーバ及びプライベートネットワークから icmp の許可

```
01600 allow icmp from any to any via fxp1
01700 allow icmp from any to any in via fxp0
01800 allow icmp from any to any out via fxp0
```

ルールに該当しないすべてのパケットを破棄

```
01900 deny log ip from any to any
```

4.5 各種サーバの設定

各種サーバは，インストール方法が一般のサーバ構築方法と同じであるものについては省略する．各種サーバの中で DNS サーバについては，プライベートネットワークから各種サーバへアクセスするための設定を追加する．DNS サーバは，インターネット上とプライベートネットワークからのアクセス用の 2 つのゾーンファイルに分け，named.conf ファイルに view オプションを用いてスプリット DNS にする．以下に DNS サーバの設定内容を示す．

[*2)] MTU と MSS の関係式

MTU - 40 = MSS（1492 - 40 = 1452）

・スプリット DNS サーバの設定

プライベートネットワークからアクセス用

```
view "internal" {
        match-clients {    192.168.1.0/24;    };
        recursion yes;
                                .
                                .
                                .
                          (省略*3))
                                .
                                .
                                .
        zone "xxx.xxx.co.jp*4)" {
                type master;
                file "internal.zone";
        };

        zone "1.168.192.in-addr.arpa" {
                type master;
                file "192.168.1.rev";
        };
};
```

インターネット上からアクセス用

```
view "external" {
        match-clients { any; };
        recursion no;

        zone "xxx.xxx.co.jp" {
                type master;
                file "external.zone";
                allow-query { any; };
        };
};
```

4.6　システム起動

元々OS に含まれているサーバソフトウェアは，/etc/rc.conf ファイルにて起動ソフトウェアの選択と起動オプションを設定する．ソースコードから導入したサーバソフトウェアは，/usr/local/etc/rc.d ディレクトリ以下に起動スクリプトを作成し，サーバ起動時にサーバソフトウェアが自動で起動するようにする．

ここで注意すべき点は，PPPoE 認証するサーバを起動する際に，LAN カード（WAN 側）→ MPD → IPNAT の順序で起動させる必要がある．また，DHCP サーバは，プライベートネットワーク側の LAN カードに対して起動するように設定する．

*3) DNS キャッシュサーバと同様の設定であるため省略

*4) xxx.xxx.co.jp は，管理するドメイン名になる．

5. スループット速度測定

スループット速度は，WindowsXP のパソコンを用いて QTNet のネットワーク内にあるスループット速度測定サイトを利用して測定した．スループット速度測定に用いたパソコンのハードウェア構成を表 4 に示す．

表 4　スループット速度測定に用いたパソコンのハードウェア構成

デバイス名	仕　様
CPU	Pentium4　3.0GHz　HT　2MB
Memory	DDR-400　1GB
HDD	3.5 インチ IDE 200GB 7200rpm UATA100
LAN	オンボード LAN　SIS900　100BASE-TX

以下の 4 つの接続方法でスループット速度の測定を行った．

・PPPoE 認証による直接接続
・市販のブロードバンドルータ①経由
・市販のブロードバンドルータ②経由
・構築したサーバ経由

図 3～図 6 は，PPPoE 認証による直接接続，市販のブロードバンドルータ①経由，市販のブロードバンドルータ②経由，構築したサーバ経由の測定結果である．

PPPoE 認証による直接接続

下り回線

速度:92.00Mbps (11.50MByte/sec)　測定品質:99.2

上り回線

速度:27.96Mbps (3.495MByte/sec)　測定品質:93.1

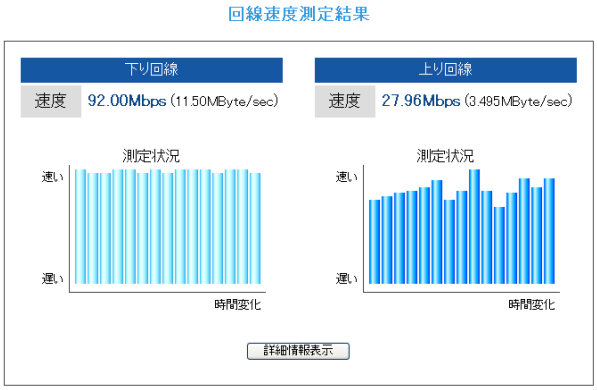

図 3　PPPoE 認証による直接接続の測定結果

下り回線は，スループット速度が十分に出ており安定しているが，上り回線のスループット速度は，Windows の PPPoE 認証の影響で 1/3 に低下してしまい，

不安定である.

市販のブロードバンドルータ①経由

下り回線

速度:92.59Mbps (11.57MByte/sec) 測定品質:99.1

上り回線

速度:81.70Mbps (10.21MByte/sec) 測定品質:99.9

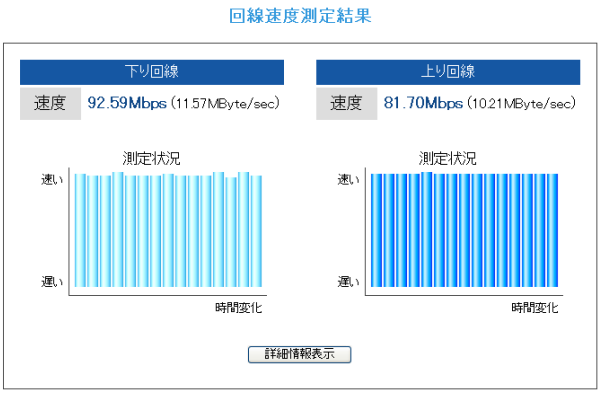

図 4　市販のブロードバンドルータ経由①の測定結果

市販のブロードバンドルータ①は, 1 万円程度した製品である. 上下回線ともに問題なくスループット速度が出ており, 安定している.

市販のブロードバンドルータ②経由

下り回線

速度:27.87Mbps (3.484MByte/sec) 測定品質:89.9

上り回線

速度:30.15Mbps (3.769MByte/sec) 測定品質:93.0

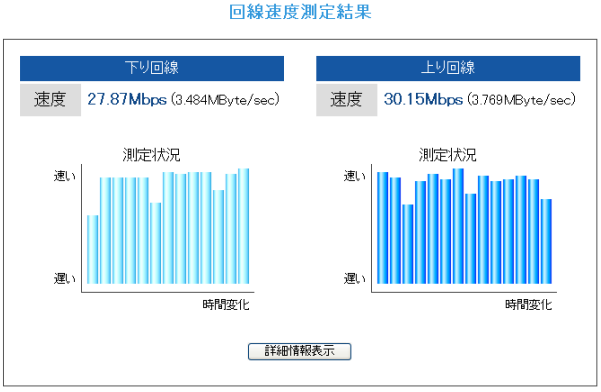

図 5　市販のブロードバンドルータ②経由の測定結果

市販のブロードバンドルータ②は, 6 千円程度の安価な製品である. 上下回線とも図 4 のブロードバンドルータ①の測定結果に比べ, スループット速度が不安定で 1/3 程度しか出ていない.

構築したサーバ経由の場合

下り回線

速度:92.07Mbps (11.51MByte/sec) 測定品質:99.4

上り回線

速度:81.36Mbps (10.17MByte/sec) 測定品質:99.0

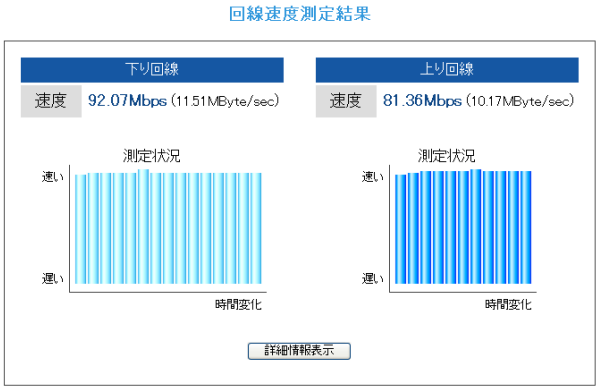

図 6　構築したサーバ経由の測定結果

構築したサーバは, 図 4 のブロードバンドルータ①と同様, 上下回線ともスループット速度が問題なく出ており, 安定している.

6. 結論

スループット速度測定結果より, 図 6 の構築したサーバ経由の上下回線のスループット速度は, 図 4 のブロードバンドルータ①経由の測定結果と比較しても大差がないことから, 構築したサーバによるスループット速度の低下は見られないことが分かる. 図 3 の Windows の PPPoE 接続と図 5 の安価なブロードバンドルータ経由は, 構築したサーバとブロードバンドルータ①経由の測定結果（図 4, 図 6）と比べ, スループット速度の低下や速度が安定しないといったパフォーマンスの低下が起きていることが分かる. FTTH 回線を最大限に活用したいのであれば, Windows の直接接続や安価なブロードバンドルータの利用は控えた方が良い.

また, ネットワーク構築にブロードバンドルータではなく FreeBSD を用いて構築したため, プライベートネットワークの通信内容を詳細に取得することが可能になり, ネットワーク内でのトラブル原因を特定しやすくなった. 更に, UNIX の OS を用いてネットワーク環境を構築していることから, ユーザーの希望に沿った新たな機能の追加やネットワーク環境の再構築が可能である.

以上のことから, FreeBSD で構築したネットワークは, 安価なブロードバンドルータを利用した時のようなパフォーマンスの低下が起きることなく, 柔軟なネットワーク環境の構築を行うことが出来る.