現実のインターネット — 実験に使用する用語集 —

1 はじめに

ここでは，家庭内においてネットワークを構築するときに必要なネットワークの用語について解説をする．現在，基本のネットワークはTCP/IP である．そして，このネットワークは階層構造を持っている．したがって家庭内で使用する機器やソフトが，どのレイヤで動作しているのかを知ると，理解が容易になる．しかし，実際販売されている機材やソフトは，利用者への便利さを追求するため，この階層構造を越えて動作している例が多い．

2 データリンク層に属するもの

データリンク層は，一つのネットワークを構成するために存在する．TCP/IP ではMac アドレスで，これを管理している．

2.1 ブリッジ (Bridge)

ブリッジはLAN のセグメント間（サブネットワーク）を相互接続する機器である．OSI 参照モデルのデータリンク層で動作する．TCP/IP ではIP で透過的になる．従って，あるホストがブリッジで接続されたネットワーク上にある別のホストにむけてIP データグラムを送るとき，そのホストはブリッジの存在を意識することなく相手に向けて送出すればそのデータグラムはそのブリッジをまたいで相手に転送される．したがってルーティングなどを一切考慮しなくて済む．そのためネットワークケーブルの接続が500 メートルを越えるようなばあい (10base-T の場合)，ネットワークを延長するために，ブリッジを利用する．

ブリッジは，本来，LAN の普及とトラフィックの増大により，リピータハブで構成された既存のネットワークではパケットの衝突 (コリジョン) が増え，パフォーマンスが低下するという事態が起こってきた．このためコリジョンドメインを制限して，ネットワークを効率化するために作られた．

ブリッジでは，受信したパケットの宛先とMAC アドレスが登録されたアドレステーブルとを照らし合わせ，該当する端末が存在しているポートにパケットを中継する．受信したポートと同じポートに宛先の端末があればパケットを破棄するので，ブリッジを超えたセグメントに不要なパケットは中継されない．ただし，アドレステーブルに存在しない送信先を持つパケットが来た場合は，受信ポート以外の全ポートにブロードキャストする．

なお，同時に，ブリッジはMAC 層のプロトコル変換もできる．例えば無線LAN で使われるブリッジはイーサネットのMAC プロトコルと無線のプロトコルの変換を行っている．

なお，最近はスイッチングハブとファイヤウオールによるVPN の利用が広まるにつれ，無線ハブ以外のブリッジは利用されなくなっている．

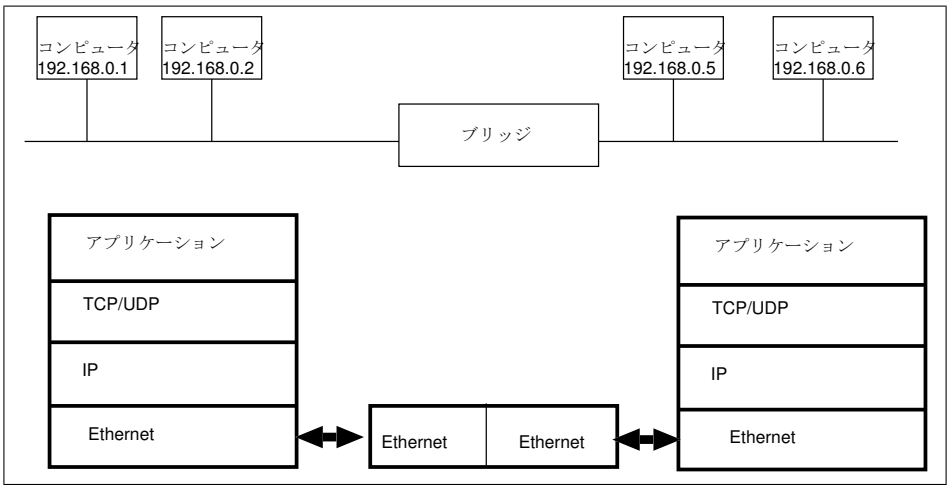

図 1: bridge

2.2 PPP (point to point protocol)

ダイヤルアップ接続や公衆電話回線を使ったデータ通信では，シリアル通信回線を媒体に使っているが，このような回線上で TCP/IP 通信を実現するために考案されたのが SLIP プロトコルである．しかし SLIP では，使用する IP アドレスなどをお互いに設定しておく必要があり，エラー検出やデータ圧縮，セキュリティ機能などがないので，非常に使いづらいという欠点があった．また TCP/IP 以外のプロトコルを使用することもできない．現在では，これらの欠点を解消した，PPP が広く一般的に普及している．

PPP は，あるポイントと他のポイントを 1 対 1 に接続するためのプロトコルである．OSI 参照モデルのデータリンク層にあたる．そして，PPP を利用することにより，距離が離れた 2 つのネットワークを論理上 1 つのネットワークとして利用することができる．したがって論理的にはブリッジと同じ機能をもつ．いわば VPN の 1 つの形態と言える．

なお，通常は TCP/IP を利用しているが，それ以外のネットワーク層以上のさまざまなプロトコルが利用できる．認証機能や圧縮機能もある．専用線のように常時接続の形態から，データの発声にあわせて接続と切断を繰り返すような使用方法も対応できる．また，誤り訂正やデータの回復に様々な配慮がされている．

PPP は，転送するパケットにプロトコルの種類を表わすヘッダ (PPP ヘッダ) を付け，PPP パケットを組み立てて通信する．つまり，この PPP ヘッダにより，受信側でパケットを元のプロトコルに戻して LAN などのネットワークに流せるようにしている．PPP では，仮想的な同期通信用の通信経路を定義してあり，すべてのデータは，一旦，この同期通信用のデータに変換される．そしてこれをさらに実際の通信に利用する機器 (アナログモデムや TA など) に合わせて変形される．

2.3 PPPoE

PPP プロトコルを Ethernet 上で利用するプロトコルが PPPoE である．インターネット関連の技術標準を策定する IETF により，RFC 2516 として標準化されている．

PPP はもともと，電話回線や ISDN 回線など，発呼を要する通信回線を介してネットワークに接続するために開発されたが，これを LAN などの「つなぎっぱなし」の環境でも利用できるようにしたものが PPPoE である．通常の PPP と異なり，ネットワークカードの持つ固有の「MAC アドレス」によって双方のコンピュータを識別し，その間に仮想回線を展開している．

PPPoE を利用すると，LAN 上からもユーザ認証や IP アドレスの割り当てなどが可能になる．これを

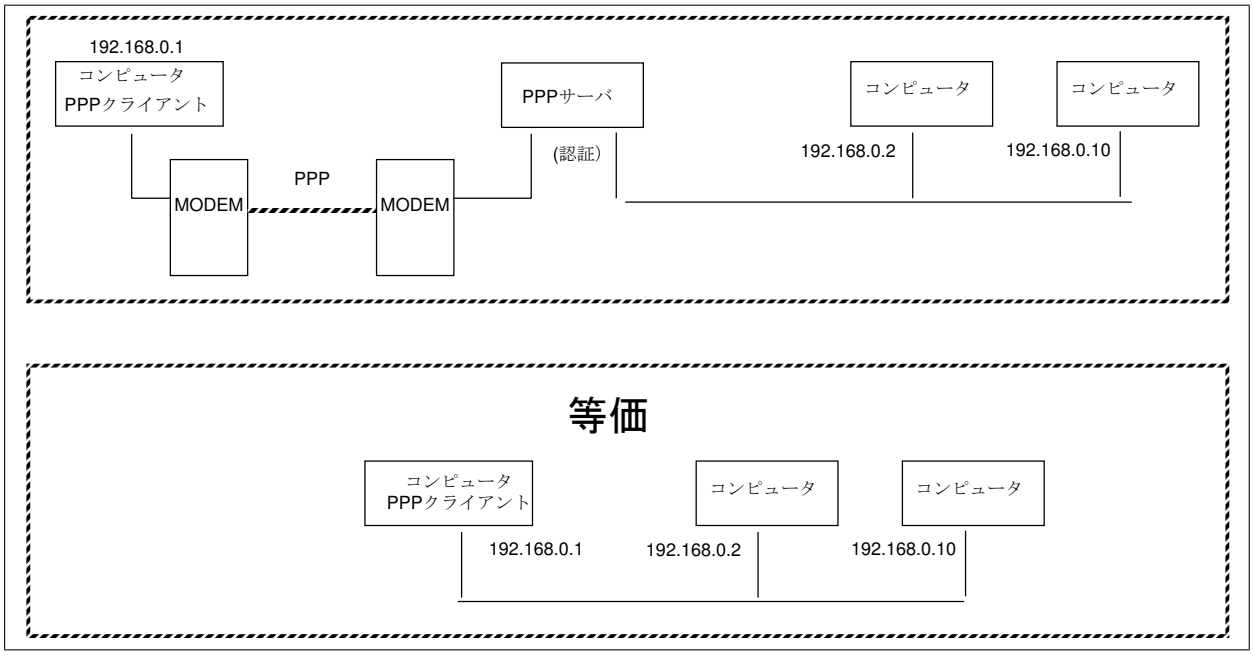

図 2: PPP

利用すれば，ADSL や CATV，光ファイバーなどによる常時接続サービスにおいて，接続するプロバイダを簡単に切り替えられるようになる．日本国内でも多くの ADSL 接続サービスが PPPoE を採用している．

3　ネットワーク層に属するもの

ネットワーク層は，異なるネットワーク相互を接続するために存在する．TCP/IP では IP アドレスで管理している．そして TCP/IP の骨格は，IP アドレスおよびネットワークを接続するためのルーティングである．

3.1　ルータ

通信経路が記述されたルーティングテーブルに従って，データを宛先のネットワークまで中継する機械をルータという．OSI 参照モデルのネットワーク層のプロトコルを解析して転送を行なう．ネットワーク層のアドレスを見て，どの経路を通して転送すべきかを判断する経路選択機能を持つ．

TCP/IP では，IP アドレスをみて，経路選択をする．経路選択を行うとき，手動で経路を書き込むのを静的経路制御 (Static Routing)，自動的に経路選択をおこなうのを動的経路制御 (Dynamic Routing) と呼んでいる．TCP/IP の創世記は静的経路制御が利用されていた．ネットワーク管理者は，経路をルータに書き込むのが仕事であった．現在は，経路があまりにも複雑になったため，通常動的経路制御が利用される．

経路制御を行うことで，ネットワークが全世界に飛び交うことができる．ルーティングを間違って書き込んだためにネットワークを落とした管理者の数は数知れない．

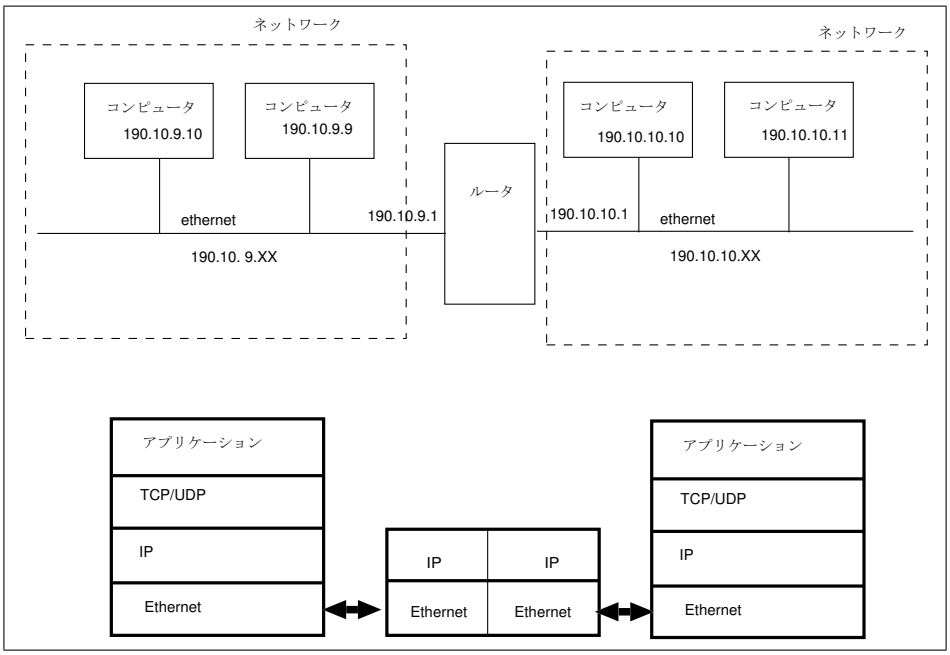

図 3: ルータ

3.2 プライベートアドレス

IPV4 は 32bit のアドレスをもち，重ならないように，割り振りは NIC が管理している．その中で，組織内部のネットワークアドレスとして自由に利用できる IP アドレスがプライベートアドレスである．プライベートアドレスは RFC1918 で規定されている．

プライベートアドレスとしては，以下のものが利用できる．

Class A × 1　　10.0.0.0〜10.255.255.255

Class B × 16　　172.16.0.0〜172.31.255.255

Class C × 256　192.168.0.0〜192.168.255.255

これらのアドレスについては，Internet 側ではルーティングしないことになっている．また，組織外へこのアドレスを持つパケットを送出することも禁止されている．しかし，組織内であれば，このアドレスについては，誰に断わることなく自由に割り当てて使うことができる．

なお，以前は，Internet に接続されるすべてのノードにユニークな IP アドレスを割り当てていたが，Internet が急速に普及するにつれて，この IP アドレスが枯渇する危険性が出てきた．そこで，組織内部だけのクローズな環境では，その組織だけで通用する IP アドレスを利用し，Internet にアクセスする場合だけ本来のユニークなアドレス（こちらはグローバルアドレスと呼ぶ）を割り当てる方法が一般化している．プライベートアドレス空間からグローバルアドレス空間をアクセスできるようにするしくみとしては，IP マスカレードや NAT(Network Address Translator) が利用される．

なお，家庭内の小さなネットワークではクラス C のアドレスが利用される．また大きな企業では，クラス B のアドレスを利用すべきだが，なぜかクラス A を利用している例が多い．

3.3 DHCP

各クライアントに，起動時に動的に IP アドレスを割り当て，終了時に IP アドレスを回収するためのプロトコルである．

TCP/IP では，各マシンごとに異なる IP アドレスを割り当てる必要がある．しかし，クライアント数が多くなると，管理の手間が大きくなる．そこで，各マシンごとに IP アドレスを設定する必要がなくても済むプロトコルが考案された．これが DHCP である．

このサービスを利用するために，各サブネットごとに DHCP サーバを 1 台たちあげておく．そして，DHCP サーバは，IP アドレスを DHCP クライアント用にいくつかまとめて用意しておく．

各マシンは，ネットワークの接続のときに DHCP のクライアントを立ち上げておく．すると以下のようにネットワークに接続される．

1. 自動的に DHCP のサーバを検索し，接続する．
2. 次にサーバは，空いている DHCP 用の IP アドレスを登録し，DHCP のクライアントに伝える．
3. DHCP のクライアントは，その IP アドレスを利用してネットワークが立ち上がる．

このように，DHCP サーバが立ち上がっていると，各マシンは DHCP クライアントを立ち上げるだけで，ネットワークに接続できる．

なお，同時にゲートウェイアドレスやドメイン名，サブネットマスクや DNS サーバなどの情報をクライアントに通知することもできる．

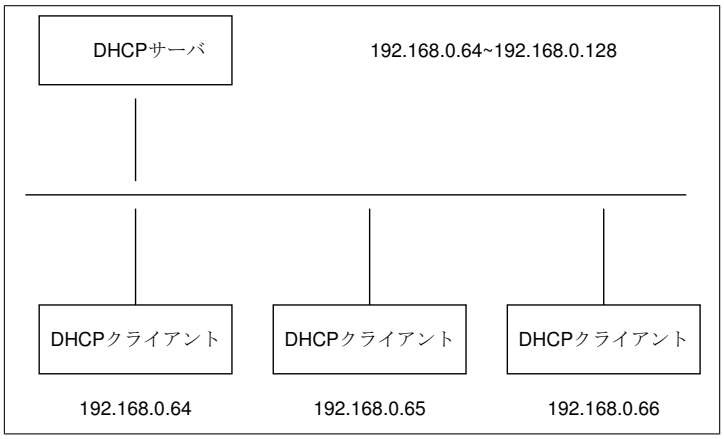

図 4: DHCP

4　トランスポート層に属するもの

トランスポート層は，アプリケーションデータの信頼性をもたせるために存在する．アプリケーションはポート番号で管理されるため，この層は，ポート番号と接続方法（セッション）がコントロールできる．

4.1　ファイヤウォール　(firewall)

インターネットなど外部ネットワークと LAN など内部ネットワークとの接点に設置され，ネットワークの接続をコントロールする機能を専門に提供するハードウェアである．

ルータは，ネットワーク層において IP のコントロールをする機械であるのに対し，ファイヤウォールは，トランスポート層におけるネットワークのコントロールをする機械と考えられる．TCP/IP では，ポート番号がコントロールできる．一方，TCP/IP は階層構造をもっているため，ファイヤウォールはトランスポート層以下のコントロール，具体的には，セッション，ポート番号，IP アドレス，MAC アドレスのコ

ントロールが可能である．したがって，ファイヤウォールでは，NAT や IP マスカレードやルーティングなどが同時に行える．

ルータがファイヤーウォールの機能を兼業で提供している場合が多いが，専用機は他の機能は持たずに IP フィルタリングや NAT などの動作のみを行なう．一般に，大規模なネットワークや高いセキュリティを必要とする組織などで導入されることが多いが，最近は各家庭に入ることも多い．また多くのブロードバンドルータは，この機能を持つ．

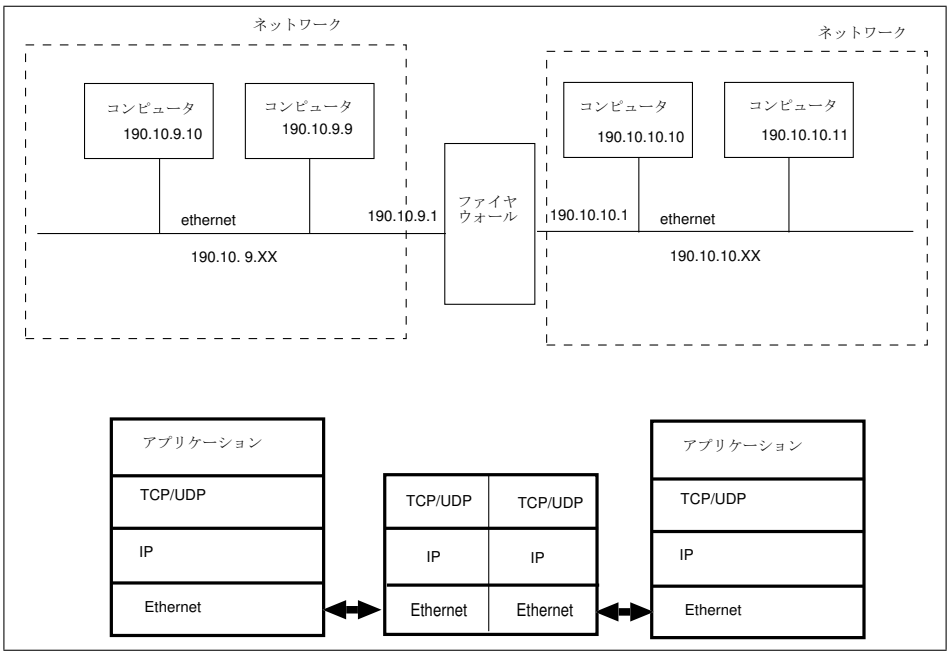

図 5: ファイヤウォール

4.2 NAT と IP マスカレード と パケットフィルタリング

プライベートアドレスからグローバルアドレスをアクセスするときに，IP アドレスの書き換えを利用する．これを NAT(Network Address Translator) と呼ぶ．NAT は一対一のアドレス変換がされる．

また，IP アドレスに加えて，TCP や UDP のポート番号も変換する技術を IP マスカレードと呼んでい．IP マスカレードを利用すると，1 つのグローバルアドレスで，複数のホストが同時にインターネットに接続可能になる．

現在，ルータに接続する PC にはプライベートアドレスが付与されるが，これではインターネットに接続できない．そこで，グローバルアドレスが割り振られたルータが，LAN の複数の PC に対して，データの送受信を行うために IP アドレスの変換作業を行う必要がある．そのため，IP マスカレード機能が利用される．

なお，NAT や IP マスカレードは，LAN から出て行くパケットと入ってくるパケットをコントロールできる．そして，おかしなパケットが LAN から外に出たり，逆に中に入り込まないようにチェックする仕事を，パケットフィルタリングとよぶ．

パケットフィルタを設定すれば，LAN からインターネットへのアクセスを任意に制御できるので，LAN 内の特定の端末からはインターネット上の Web ページを閲覧することができないといったアクセス制限が可能になる．

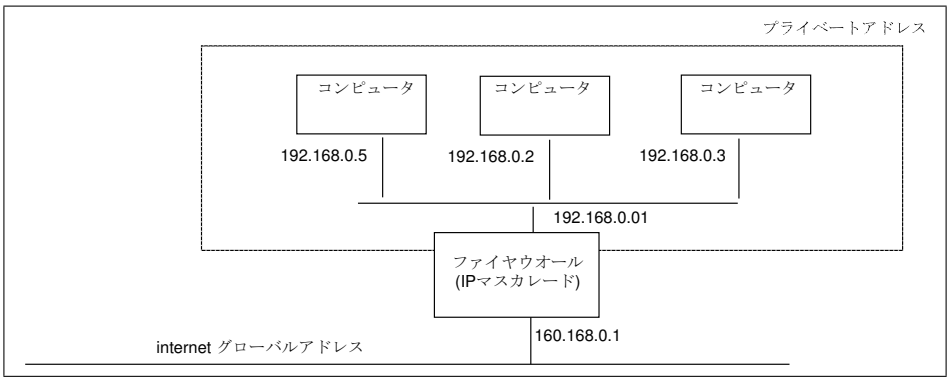

図 6: IP マスカレード

4.3 静的 IP マスカレード (ポートフォワーディング)

IP ルータでインターネットに接続している LAN 環境では，外から LAN 内のプライベートアドレスの振られた PC にはアクセスできない．そこで特定のアドレスのポート番号のアクセスを，プライベートアドレス内の PC に転送する仕組みをポートフォワーディングとよぶ．なお，静的 IP マスカレードやポートマッピング，ポートフォワーディングなど呼び方は様々である．

この例では，NAT として 192.168.0.1 の 80 番のポートが 190.10.10.1 の 80 番のポートにポートフォワードされている．グローバルネットワークから 190.10.10.1 のポート 80 にアクセスした場合，ポートフォワーディングされた 192.168.0.10 のポート 80 が対応する．なお，通常ポート 80 は Web サーバが利用しているため，Web サーバをアクセスすることになる．

この機能は，プライベートアドレスの内部のマシンがグローバルアドレスのマシンから呼び出す必要があるときに良く利用される．具体的には Web サーバやメイルサーバや FTP サーバである．

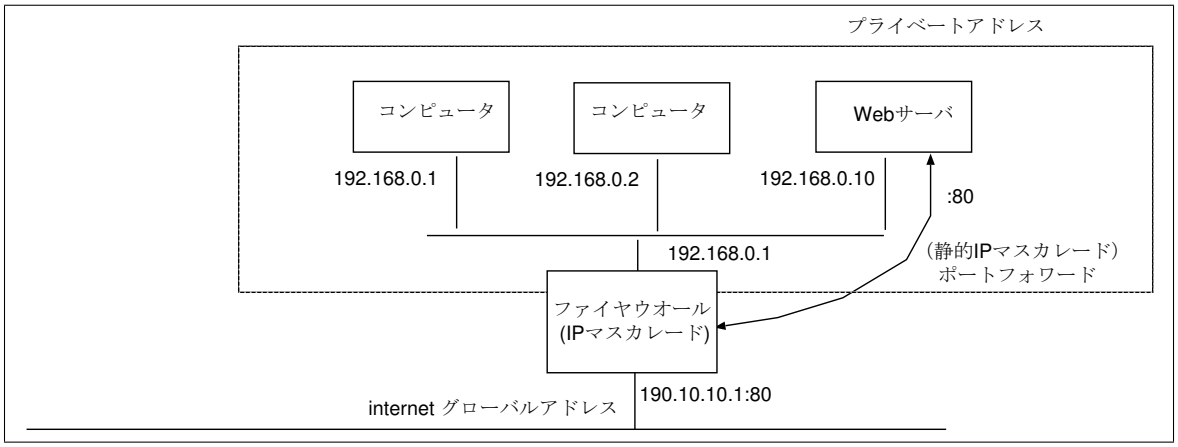

図 7: 静的 IP マスカレード (ポートフォワーディング)

5 アプリケーション層に属するもの

アプリケーション層では，ポート番号でアプリケーションを管理している．異なるアプリケーションは，異なるポート番号をアクセスする．

5.1 DNS (Domain Name System)

TCP/IP ネットワーク環境において，ホスト名から，対応する IP アドレスを取得できるようにするサービスである．ポート番号は 53 が利用される．

DNS サーバは，ホスト名と IP アドレスの対応関係を記述したデータベースを管理しており，クライアントからの要求に応じて，ホスト名からその IP アドレスを参照できるようにする．これによりユーザーは，憶えにくい IP アドレスではなく，ホストの名前を指定してネットワークにアクセスできるようになる．

図の例では，Web クライアントが test.co.jp を見にいく．DNS サーバは IP address 191.10.10.2 を返す．これが DNS である．

UNIX 系の soft では BIND が良く利用される．

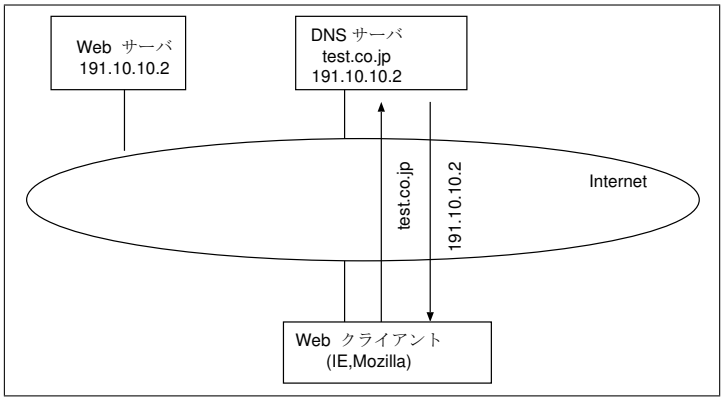

図 8: DNS

5.2 ダイナミック DNS (Dynamic Domain Name System)

ダイナミック DNS は，プライベートアドレス内に Web サーバや Mail サーバを立ち上げたいときに利用される．

本来は，DNS の内容に変更があったときにその変更を即座に通知したり，変更部分のデータだけを転送するなどの機能を持った DNS である．RFC1995，1996 などで定義されている．以前の DNS システムでは，データベースの内容が変更されても，事前に決めたある一定時間（リフレッシュ時間）たたないとそれが下位の DNS サーバへは反映されなかったが，ダイナミック DNS では，即座に変更を通知することができる．

したがって，IP アドレスが良く変化する Web サーバがあったばあい，以下のように運用する．

1. Web サーバは IP アドレスが変化したならば，それをダイナミック DNS サーバに通知する．
2. ダイナミック DNS サーバ は，登録されている DNS に IP アドレスを登録する．
3. Web クライアントは，一般の DNS サーバに DNS を引きにいく．
4. DNS サーバ は ダイナミック DNS サーバに対して問い合わせる．
5. DNS サーバ は 必要な IP アドレスを得る．
6. Web クライアント は 必要な IP アドレスを DNS サーバから得る．

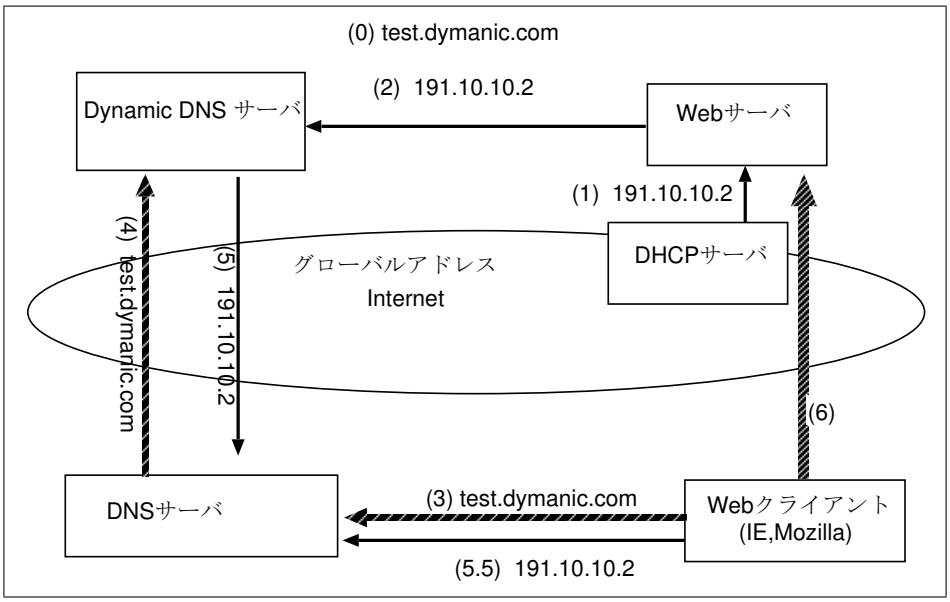

図 9: ダイナミック DNS

5.3 World Wide Web

TCP/IP において，もっとも良く使われるアプリケーションである．ポート番号に 80 番が利用される．元々は，欧州核物理学研究所（European Center for Nuclear Research．CERN）で開発されたドキュメントシステムである．ドキュメント中に他のドキュメントへのジャンプコマンド（リンク）を埋め込むことができる．このリンクとして，URL （Uniform Resource Locator）を使用し，Internet に参加している世界中の Web サーバのどのドキュメントにもジャンプすることができる．初期は，テキストのみの表示だったが，その後の仕様変更により，音声，静止画，動画，その他プログラムも表現できるようになった．

Web でドキュメントを提供するシステムは Web サーバと呼ばれる．クライアント側で Web サーバのドキュメントをブラウズするソフトウェアは Web クライアントと呼ばれる．

ドキュメントの記述には，HTML（Hyper Text Markup Language）と呼ばれるマークアップ言語を使用する．ある HTML 文書と他の HTML 文書をリンクするには，リンク先の URL を文書中の文字列とともに記述する．Web のドキュメントとしては，文字はもちろんのこと，静止画（GIF ファイルなど）や音声，動画など，あらゆるデータを提供することが可能である．

HTML 文書の解釈はブラウザ（Web クライアント）によって行なわれ，HTML 文書中に記述されたタグに基づいて表示がなされる．たとえば見出し文字の太さや大きさは，見出し行のレベルという形でタグ中に記述される．見出し行のレベルをどのように解釈して表示するかは，ブラウザに任されている．したがってブラウザが異なれば，表示も異なる可能性がある．

Web サーバは，多くのばあい Apatche が良く使われている．また，Web クライアントには多くの種類があるが，現在，Internet Explore がもっとも多くのシェアを持っている．しかし Windows と Mac でのみ動作する．一方，Mozilla は，殆んどの OS で起動できる．

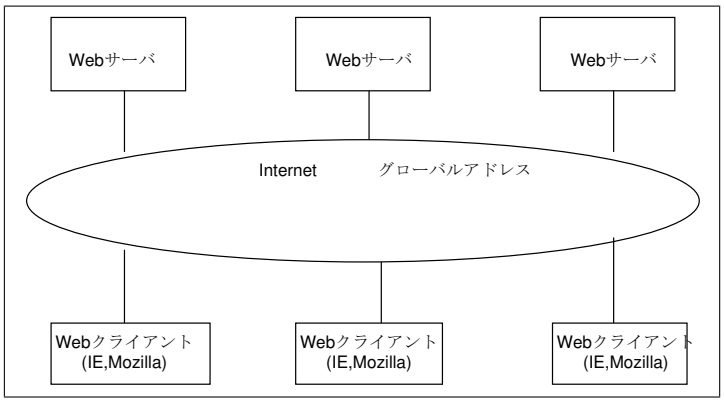

図 10: Web サーバ & クライアント

6 現実のネットワークの運用

6.1 ブロードバンドルータ

家庭などで ADSL や光ファイバーなど高速な回線でインターネットに接続する際に使うルータ．WAN 側のポートとして Ethernet ポートを持ち，LAN 側は Ethernet やシリアルポートなどを備える．通常，ADSL モデムや光終端装置などと一緒に使う．最近は，ADSL の普及が本格化しているため，ADSL モデムを内蔵した製品なども登場している．

ダイヤルアップルータなどと同様に，LAN 側のパソコンから利用できる DHCP サーバ機能や IP マスカレード機能を備えていて，また，ブロードバンドルータをコントロールする目的で Web サーバがあるものが多い．ブロードバンドルータの大きな特徴として，クライアントマシンに代わって PPPoE による認証を行なう機能がある．ADSL でよく使われる PPPoE プロトコルは，ルータ機能を持たない ADSL モデムでは処理できないため，通常はパソコン側に PPPoE 用の接続ソフトを用意する必要がある．しかし，ブロードバンドの PPPoE 機能を使用すれば，この手間が省ける．

通常は，ブロードバンドルータの IP マスカレードの機能を使用する．そのため，LAN 上の PC がインターネット上の Web サーバなどにアクセスしようとしてパケットを送り出すと，ブロードバンドルータはあたかもそれは自分が出したもののように，送り主のプライベート IP アドレスを自分のグローバル IP アドレスに書き換えてインターネット上に送り出す．ブロードバンドルータはそのパケットを実際に出した LAN 上の PC を覚えておき，そのパケットに対する返事がインターネット上のサーバから返ってきたら，宛先を自分のグローバル IP アドレスから元の送り主のプライベート IP アドレスに書き換える．そのパケットを LAN 上に送り出せばもとの持ち主に届くという仕組みになっている．IP アドレスの書き換えが“IP マスカレード”と呼ばれる技術である．

このようにブロードバンドルータは LAN とインターネットの接点の役割を果たし IP アドレスの変換を行うために，LAN から出て行くパケットと入ってくるパケットをいちいちチェックできる．この際におかしなパケットが LAN から外に出たり，逆に中に入り込まないようにチェックする仕事が,「パケットフィルタリング」である．パケットフィルタを設定すれば，LAN からインターネットへのアクセスを任意に制御できるので，LAN 内の特定の端末からはインターネット上の Web ページを閲覧することができないといったアクセス制限も可能になる．なお,「パケットフィルタリング」をもつ機器をファイヤウオールと呼ぶ．

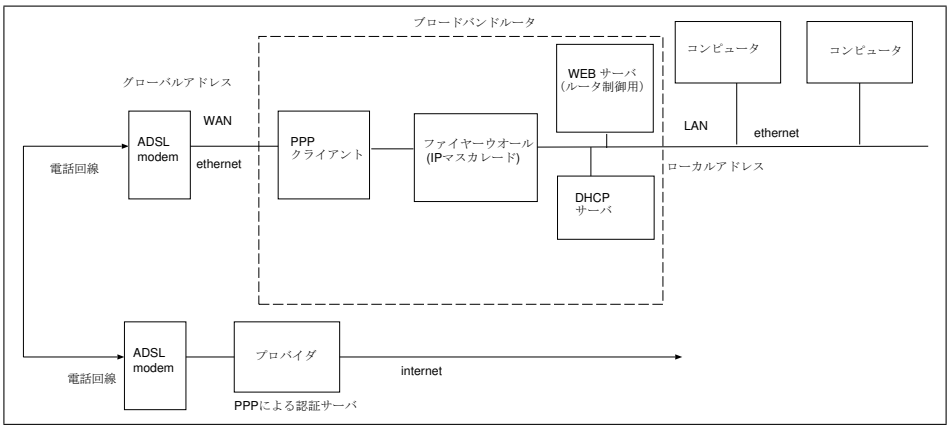

図 11: ブロードバンドルータ

6.2 プライベートアドレスに Web サーバを立ち上げたときのダイナミック DNS の利用方法

通常プライベートアドレスから外部のネットワークに接続するとき，外部からはグローバルアドレスが 1 つ割り当てられる．しかし，再接続されるたびに，グローバルアドレスが変更になる．そこで，このダイナミック DNS を利用して，Web サーバ を立ち上げることが可能になる．

具体的には以下のように運用される．

1. Web サーバは プライベートアドレス内にあり，192.168.0.10 で運用される．
2. DNS に test.dymanic.com が登録されている．
3. NAT と Web サーバは，Port forward されていて，グローバルアドレスからアクセスしたとき，Web サーバにアクセスされる．
4. NAT は，internel に接続されるとき 1 つのグローバルアドレスが与えられる．このとき，191.10.10.2 が与えられたとする．
5. NAT は，ダイナミック DNS サーバに 191.10.10.2 を登録する．
6. Web クライアントは，一般の DNS サーバに DNS を引きにいく．
7. DNS サーバはダイナミック DNS サーバに対して問い合わせる．
8. DNS サーバ は 191.10.10.2 を得る．
9. Web クライアント は 191.10.10.2 にアクセスにいく．
10. 191.10.10.2(NAT) はポートフォワードされている Web サーバ (192.168.0.10) にアクセスされる．

現在，個人がグローバルアドレスを取得するには，それなりのコストが必要になる．また，現在，いくつかのダイナミック DNS サーバは無料で運用されている．したがって個人で低価格で Web サーバを立ち上げるとき，ダイナミック DNS が良く利用されている．

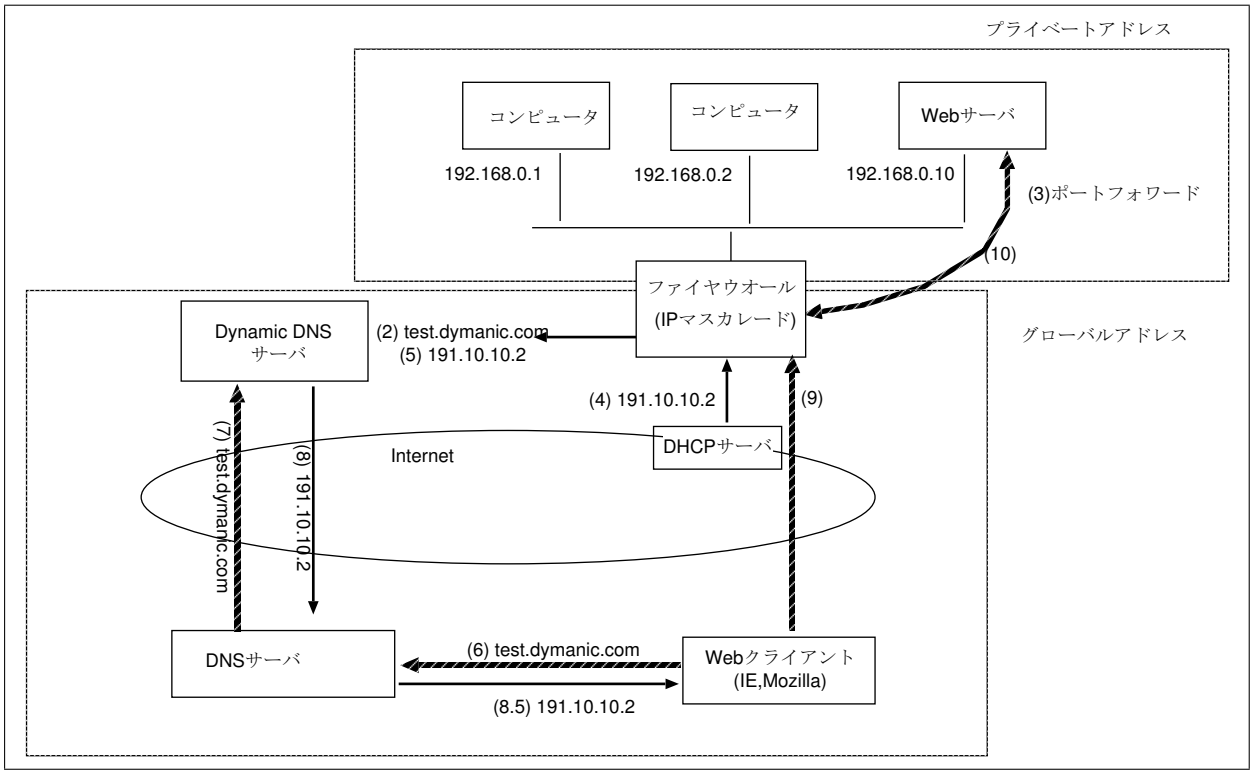

図 12: ダイナミック DNS とプライベートアドレス