卒業論文

IPv6
モノとモノとがつながる世界

日本大学法学部　管理学科　4 年
学籍番号：0250107
青木 将裕

目次

1.はじめに

日本のブロードバンド普及率は 30%にも達しようとし、家庭では確実にいつでもインターネットとつながる状況になってきている。接続方法も ADSL、CATV、FTTH など多様化もしている。今後はネット家電の本格化、テレビ放送のデジタル化、IP(インターネット)電話の進展などに伴い、さらにネットワークが人々の生活に溶け込んでいくことが考えられる。

これまでは情報収集などの目的を持ち、意図的にインターネットに繋ぎに行くのが中心だったが、これからは外出先から家庭の機器が操作できるとか、取りためた画像や動画などを他の場所で表示するとか、データ通信ということをあまり感じさせない利用形態も進んでいくだろう。インターネット上の一般家庭サービスもこれまでの PC 向けとは違った物が次々に登場するに違いない。

このようなネットワーク技術の進化の中でネイティブ・インターネットと呼ばれる本来の機能を発揮するインターネットを実現するためのプロトコル IPv6 が本格的な導入期を迎えました。現在のインターネットに使われている IPv4 は 20 年以上も前に標準化され 32 ビットのアドレス空間を持っていますが世界的にインターネット利用者数の増加が著しく IP アドレスの枯渇が問題視されました。

このような枯渇を食い止めるために 15 年ほど前から次期バージョンの開発を進め IPv6 を規定しました。v6 では 128 ビットのアドレス空間というほぼ無限大のアドレス空間を持ちコレによって双方向のストレスのない通信、ユビキタス・ネットワークをといった新しいインターネットの展望が拓けだんだんとその利用が始まっています。

第 2 章では IPv6 の前に IP とはそもそもどんな物でどんな機能を持っていているのか。そしてどのような経緯で IPv6 が研究され登場してきてそれに向けてどのような動きがあるのかなどを述べる。

第 3 章では IPv6 がどのような機能を備えているのか、実際利用するには何が必要であるのかなどを述べる。

第 4 章では IPv6 の現状はどうなっているのか、機器の標準化やサービスの普及状況などとともに述べる。

第 5 章ではこれまでの章をふまえて、現状の IPv6 の課題や普及に向けてどうすればよいのか。また普及へのロードマップを述べる。

第 6 章ではそして IPv6 が普及すると社会がどう変わるのかについて述べる。

2. IP とは何か

IP とはインターネットプロトコルの略で「通信規約」などと訳されます。IP はインターネット技術の構造の中核に位置しネットワークインタフェースの違いを吸収してトランスポートプロトコルやアプリケーションなどに対して統一した通信機能を提供します。この構造ゆえに、データリンク層としてイーサネットや ADSL、無線 LAN など、どのようなものが使われていても同じようにアプリケーションのサービスを利用できるようになっているのです。

インターネット上にさまざまな新しいサービスが次々と登場する一方でギガビットイーサネットなど新たな通信基盤が開発されるとそれをいち早く取り込んでより高機能なネットワークに成長を続けることができるのは、このことによります。IP の役割は大きく分けて次の二つです。

1.アドレスの割り当て（addressing）
2.進路制御（routing）

2.1.アドレスの割り当て

アドレスの割り当てはネットワークに接続されるノードに識別番号を割り当てる仕組みです。この識別番号をインターネットでは IP アドレスと呼び 32 ビットの整数が用いられています。IP アドレスは正確には濃度の各通信インターフェイスに対して割り当てるものです。したがってルータなどのように複数のインターフェイスを持つノードの場合には一つのノードに複数インターフェイス割り当てられることになります。インターネット上のすべてのノード（正確にはインターフェース）を区別できるように、原則としてインターフェイスに与えられる IP アドレスに重複があってはなりません。そこで、ユニークな IP アドレスを割り当てる仕組みが用意されています。IP アドレスの割り当ては IANA お中心とする割り当て組織によって行われていますが、これだけの台数のノードがインターネットにあるわけですから、一台一台割り当てていたら大変である。

そこで大学や会社などの組織ごとにまとまった数の IP アドレスを割り当て、各組織が割り当てのだから組織内のノードに IP アドレスを割り当てるようになっています。実際には、上位何ビットかを割り当て組織が決め、残りのビットは組織で自由に利用する方式がとられています。無論、組織の規模によって必要となる IP アドレスの数が異なるので、上位のビット数を変えることによって組織内で自由にできる IP アドレスの数を変えています。割り当て組織によって決められる上位のビットをネットワーク部、組織で自由に出来る下位のビットをホスト部と呼び、以前には組織の規模に応じて次のような三つのクラスに分けて割り当てていました。

●クラス A

ネットワーク部は 8 ビット・ホスト部は 24 ビット

ネットワーク内の最大接続ホスト台数は 16、777、214 台

インターネット全体で 128 組織に割り当て可能

●クラス B

ネットワーク部は 16 ビット・ホスト部はビット

ネットワーク内の最大接続ホスト台数は 65、534 台

インターネット全体で 16、384 組織に割り当て可能

●グラス C

ネットワークは 24 ビット・ホスト部は 8 ビット

ネットワーク内の最大接続ホスト台数は 254 台

インターネット全体で 2、097、152 組織に割り当て可能

2.2.経路制御

経路制御は IP アドレス表された宛て先に、どのような道筋をたどって到達するのかを決定する仕組みです。IP で使われている系を制御では基本的にあて先から次の行き先となるノードを決定する方法が用いられています。これをホップバイホップ型のダイナミックルーティングと呼びます。

インターネット上の全てのノードは、原則として宛て先と次の行き先（IP アドレス）のペアを格納した経路表をもち、この経路表参照しながら次に行くノードを決定しています。宛て先に相当する部分は、この IP アドレス単位で記憶したのでは膨大な数になってしまい格納するにも参照するにも大変です。そこで前述の IP アドレス割り当てに従って、グループ単位で記憶されています。これは大阪駅の案内板に、「東京方面はまず東京へ」と書いてあるようなものです。東京の秋葉原に行きたい場合でも、大阪駅では、この案内で十分なのです。秋葉原への行き方は、東京駅に着いてから調べればよい。

ホスト部のアドレスを全て 0 にしたアドレスをネットワークアドレスといいます。このネットワークアドレスを上位何ビット目までがネットワーク部なのかを示すネットマスク、そしてそのネットワークアドレスで示されるグループへ到達するために次に行くべきインターフェイスの IP アドレスの、3 つの情報を経路表は格納しています。経路には、この 3 つの情報がインターネット上に存在する全てのネットワークについて格納されていることになります。

2.3.登場の背景～IPv4 運用の限界

現在のインターネット利用されている IP は、RFC71 に規定された。IP ｖ 4 である。この RFC は、1981 年 9 月に発行されています。その誕生からすでに約 20 年以上ものでかなりの期間が経過しています。この間にコンピュータの技術も、大きく進歩し、IPv4 が設定された時代には想定できなかった。様々な利用形態が、登場してきているのである。たとえば携帯型コンピュータの向上もその 1 つです。現在のインターネット技術では、携帯して持ち歩くような移動ノードをｲ取り扱うためには別な工夫が必要です。しかし、最も大きな変化はインターネットの急激な普及である。この結果、現在のインターネットの規模は、設計当初の予測をはるかに超えたものになっているのである。

インターネットの拡大に伴って、推測される濃度の数だけでなく、IP アドレス割り当てを受けて、インターネットに接続する組織の数も大きく増加しました。その結果として IETF が、1990 年代前半に IPv4 では今後のインターネット維持することが難しいと判断し。次の 3 つの検討を開始したのです。

●今後のインターネット発展の予測と IPv4 によって維持できる期間
●IPv4 の延命策
●新たな IP の設定と移行計画を策定

また、この検討にあたっては、新たな IP を設計して移行するまでの時間的猶予を予測しながら短期的な買いとして新しい IP を用意するという方策をとらず、今後数 10 年のインターネットを支える。次世代 IP を設定することを目標としたのです。
下の図は検討段階の流れである。

年月		動向
1992 年 6 月		神戸で開催したインターネット学会で IP の後継プロトコルが 3 案提出される。これを機に後継　プロトコルを広く応募
1994 年 7 月		カナダノードロントで開催された標準化団体（IETF）の会議でアイディアが一本化
1995 年 12 月		アメリカ､ダラスで開催された IETF の会議でアイディアが RFC1883 として承認。　　標準化作業スタート
1996 年 2 月		米ハンプシャー大学が IPv6 製品の相互接続試験を開始
7 月		世界規模の IPv6 実験ネットワーク『6bone』が稼動
1997 年 7 月		仕様変更を盛り込んだ新規格が草書として承認
1998 年 12 月		アメリカ､オーランドで開催された IETF の会議で草書が RFC2460 として承認。標準化作業が第 2 段階に進む
1999 年 7 月		IP アドレス管理機関（IANA)が正式に IPv6 の割り当てを開始
8 月		IIJ が IPv6 を活用したインターネット接続サービスを国内で始めて開始
2001 年 7 月		WINDOWS XP にて IPv6 がサポートされる

IPv4 の見解として、IP アドレスの数の不足がよく言われるが、本当の問題は、ルータの経路表の爆発にある。確かに 32bit で表現できる。アドレスの数は 43 億程度なので、家庭の現地製品や携帯電話などがインターネットに直接接続されるようになっていけば、当然 IP アドレスは不足する。しかし、経路表の大きさの問題は、もっと深刻だった。原則として全てのノードにはインターネット全体に関する経路表を持たなければならないから、接続されるネットワークの数が増えるにつれて、経路表が大きくなり、記憶容量の観点からだけでも大きな問題だ。また、ルータは中継のたびに経路表を参照するため、経路表が大きくなると、中継制度に直接大きな影響を与えることになる。

そこで、IPv4 の延命策として、最初に考えられたことは、IP アドレスの割り当ての無駄を減らすとともに、経路表を小さく、維持する方法でした。これらクラスの概念がない CIDR（Classless Inter-Domain Routing）です。

2.3.1.CIDR の導入

クラス A、クラス B、クラス C、というクラス分けに基づく IP アドレス割り当て方法では、組織に対して割り当てる IP アドレスの数が 8bit 単位になり、本当にその組織が必要とする IP アドレスの数と実際に割り当てられる IP アドレスの間に隔たりが生じました。例えばクラス C では、250 台程度のコンピュータしか接続できませんから、多くの組織はこれでは足りません。このため 65000 台規模のネットワーク構成可能なクラス B の割り当てを受けることになったのですが、これだけの台数のノードを接続する組織は稀です。その結果として組織に割り当てた後、使われない IP アドレス空間が生じて

しまいました。

そこで、それまでのクラス別の割り当てを廃止し、ネットワークのビット数を可変にして組織の規模に見合った適切な数の IP アドレスを割り当てられるようにしたのです。それと同時に、CIDR では経路表を小さく維持できるように工夫をしています。

例えば次のようなネットワークを考えてみます。ルータの左側には 4 つのネットワークがありますが。これらのネットワークアドレスの上位 22bit はすべて同じです。このようなネットワーク構成の時、ルータの右側にあるノードの経路表では、ルータの左側の 4 つのネットワークを宛先とするエントリは、すべてネクストホップが同じということになります。とすると、これらを 1 つのエントリにまとめることができれば、経路表の大きさを小さくすることが可能になります。これが経路情報の集約です。

経路情報集約するためには、このように、集約可能なネットワークが近くに集まっている必要性があります。そこでそれまでのように組織が要求した順に片端から IP アドレス割り当てのでなく、こうしたネットワークの接続構造を考慮して割り当てるように工夫されるようになりました。

この具体的な方法は次のようなものです。世界中をアメリカ大陸アジア太平洋地域ヨーロッパおよびアフリカの 3 つの地域に分割し。それぞれに IP アドレスの大きなブロックを割り当てます。そしてさらに各地域で、国、プロバイダといったネットワークの接続構造に沿ってブロックを分割し、割り当てていくのです。この方策により、1 時期爆発的に大きくなっていた経路表も安定した大きさに維持されるようになっています。

2.3.2.NAT の登場

IP アドレス不足に対するもう 1 つの延命策は、NAT（Network Address Translation）の導入です。これは組織の出入り口となるゲートウェイにだけグローバルアドレス割り振り、組織内部のコストに組織内のみで通用するプライベートアドレスを割り振ることによって、グローバルアドレスを節約しようと、いうものです。

組織内部のコストは外部と通信する時、出入り口のゲートウェイは送信元アドレスのプライベートアドレスを自分のグローバルアドレスに付け替えて、送り出し、通信相手から返信が届くと送信先アドレスを要求元のプライベートアドレスに、付け替えて送り届けます。

外部の通信相手から見ると、組織内部のコストは見えず、これに出入り口のゲートウェイとやりとりしているように見えます。また、内部のホストは出入り口のゲートウェイを意識することなく、外部のホストにアクセスできます。

2.4. IPv6 に向けて、

このように、IPv4 の延命策としてさまざまな方法は考えられ、一時期の危機的状況は脱したわけであるが、2018 年の前後 8 年には限界が訪れると予測され、それまでに新しい IP を開発し、移行していかなければならないのである。特にインターネットは北米を中心に普及が広まっていたという経緯があることから、北米以外の 1 部の国や地域は既に IP アドレスが不足するという事態に直面している。また、NAT のような技術もクライアント／サーバ型のアプリケーションではなく、直接ノード同士の通信しあうようなピアツーピア型のアプリケーションの登場によって、限界に達しつつある。

こうした背景のなかで、IP 武力が登場し。そこへ向けての移行が始まったのです。IPv6 は、単純にアドレスの数や経路表の大きさの問題を解決するだけではなく、今後 50 年以上インターネットの中核として機能できるように、次の点を行動して設定されました。

●IPv4 の流れを受け継ぐ
　◇基本的な動作を同じ
　◇より単純化されたプロトコル。

●これまでの問題点を解決
　◇アドレス空間の不足
　◇マルチキャスト、モバイル

●運用の簡素化
　◇プラグアンドプレイ
　◇セキュリティ

●長期間の利用が可能。
　◇拡張性が高い

●運用側の容易な移行

IP アドレスが 128bit で表現され、膨大な数のノードを接続できることから、IPv6 の導入の効果として、よくコンピュータだけではなく、家電製品や携帯電話など、様々なものが接続できるようになるということが中心に語られる。しかしそれだけではなく、実はこのような新しい可能性が込められているのである。そして、この新しい IP が、機能することで、従来は考えられなかったさまざまな新しいサービスが登場し、インターネットを基盤とした新しい社会や構成できるようになるのである。

3.IPv6 とは

現在の電子メールや www など、様々な場面でインターネットが利用されるようになって来ました。この根幹を支える技術が IP（インターネットプロトコル）です。IPv6 は IP アドレスの枯渇などインターネットの急速な発達で見えてきた不都合な点を解決し、今後も長期にわたって使用できるように検討され、開発が進められて来た物です。

3.1.IPv6 の機能

いままで述べてきたように、現在使われている IPv4 にはさまざまな問題点が出てきたことが分かった。ここでは、新しく出てきた IPV6 がどのような機能を持っているのかを説明する。IPvV6 が、インターネットプロトコルバージョンシックスの略であるということは説明したが、なぜ v4 のつぎが v6 なのかという疑問があると思う。IPv5 というものは存在しない、v5 の IP は、「ST‐2」という実験的なプロトコルのために使われてしまっているからである。ST-2 とは、Internet stream Protocol version 2 の略であり、帯域保証付きのプロトコルである。ジム・フォージー氏によって 1979 年に開発された。なお ST と同様の歴史的背景から v7、v8、v9 も実験的プロトコルにバージョン番号が割り振られている。IPv4 以前を見てみると、バージョン 0 は予約 1～3 は未使用である。つまり、IPv4 が最初の IP なのである。なお、v9 以降については、10 番から 14 番は予約、15 番は未使用となっている。こうしたことから遠い将来に IPv6 の後続バージョンがつくられるときには、IPv10 になるのかもしれない。

IPv6 の新しい大きな機能としては、膨大なアドレスの領域、PnP 機能、IPSec の標準装備がある。

3.1.1.膨大なアドレス空間

IPv6 の最大の特徴は、IP アドレスの数を大幅に増やしたことである。IPv4 では約 43 億個のアドレスが使えるということは上でも述べた。これだと、人類が 1 人個使ったら、アドレスが、無くなってしまう。それにこれからは IP につながる機器を 1 人がいくつも持つというような時代がやってくる。そこで IPv6 では、IPv4 の持っているアドレスの数の 7900 兆倍にして、さらに 100 兆倍にした数になる。人類 1 人当たり 5600 兆の 100 兆倍使えるので、ほぼ無限大の空間だと言ってよいだろう。例えば IPv6 のアドレス 1 つの 1mm だとすると、全体の IPv6 の長さは、約 837 万光年である。銀河系大きさが約 10 万光年なので、そのけた違いの大きさが分かるだろう。

アドレスの数が増えたことにより、現在の IPv4 とはアドレスの表記も変わってくる。現在の表記方法は、例えば 192.168.11.1 などのようなアドレスになっている。IPv6 のアドレスの表記方法は、2001:db8::88 のようになる。v4 では 10 進法で 3 桁の 4 つ区切りだった表記方法が v6 では 16 進法で 4 桁の 8 つ区切りとなり長くなったため省略方法などにも決まりがある。詳しくは下の図で説明する。

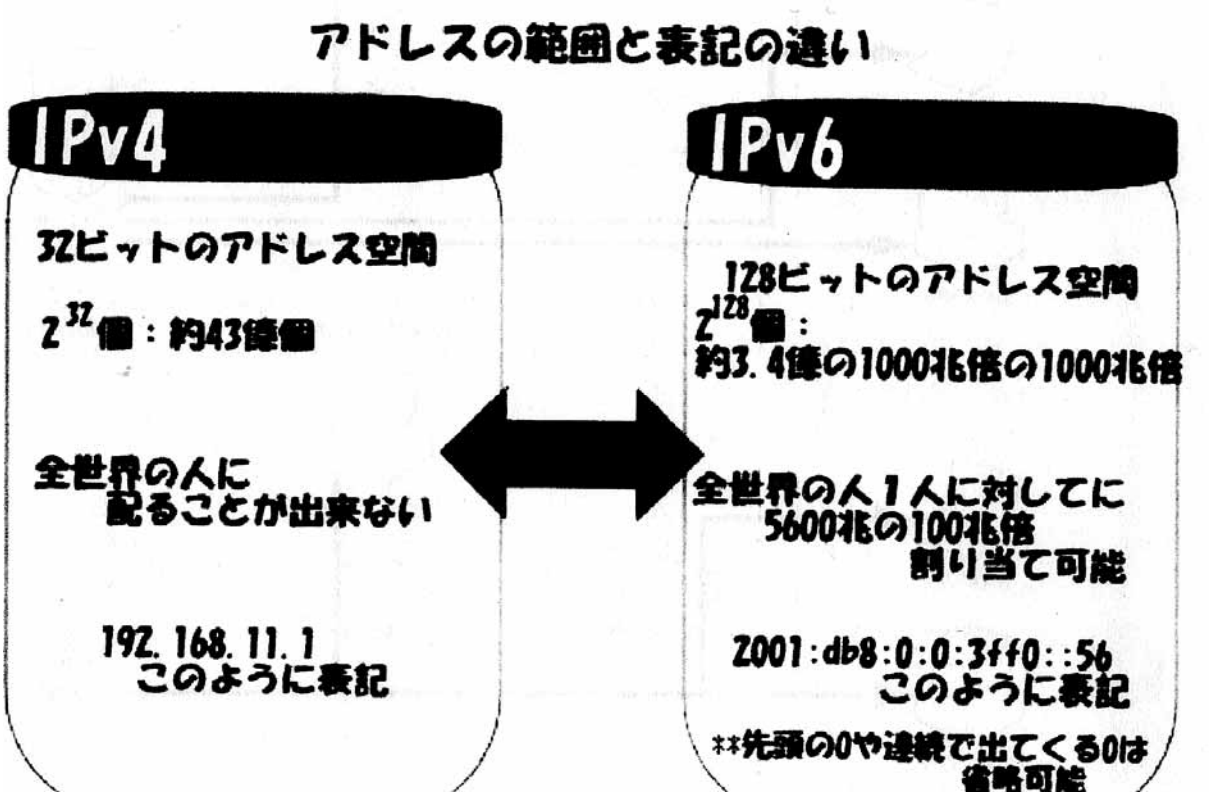
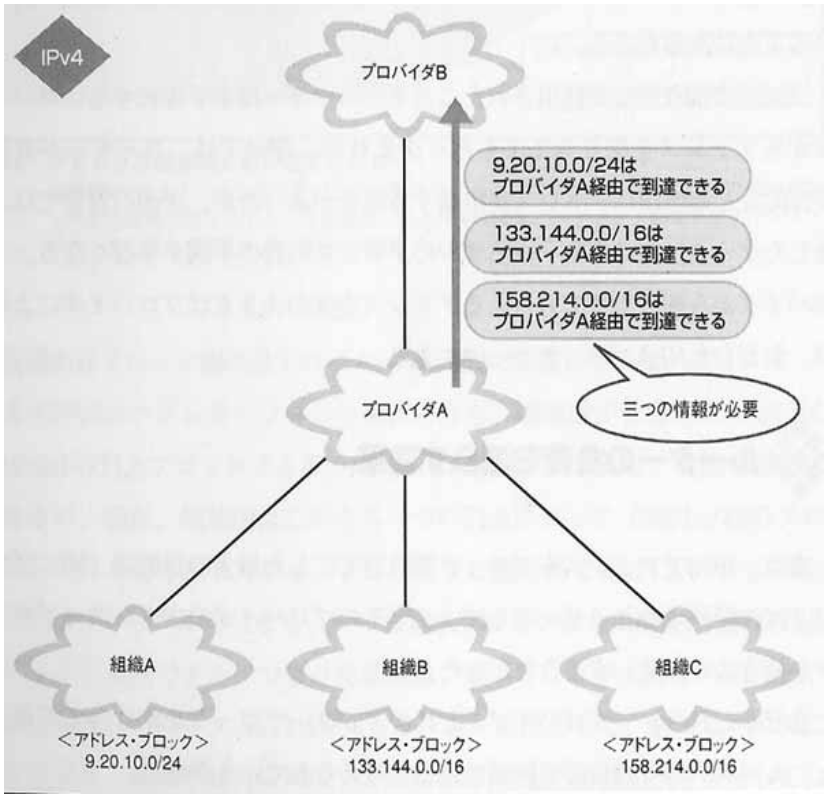


図 3.1.1.a　IPv4 と IPv6 の違い

IPv6 では、128bit 領域のうち、上位 64bit がネットワークそのもの識別しとして用いられ、下位 64bit は、そのネットワークにおける識別しとして用いられる。ネットワークを表す上位 64bit は、いくつかのフィールドに分かれている。これは IPv4 にはなかった特徴で、IPv6 アドレスのポイントである。この膨大な IP アドレスの管理は現在では ICANN(Internet Corporation For Assigned Names and Numbers)が行っている。1998 年までは IANA（Internet Assigned Number Authority ）が行っていた。インターネットは米国防総省の実験ネットワークからスタートした経緯もあり、それ以前は米国政府の管轄化にあった。インターネットのアドレス資源（IP アドレス、ドメインネームなど）の割り当ては、米国政府団体の 1 つである全米科学財団（NSF：National Science Foundation）から委託を受けた Network Solutions 社（.com／.net／.org ドメインの管理を担当）と IANA、残りのドメインの管理を担当）の 2 つの組織によって行われていた。だが、米国政府はインターネットの広がりとともにアドレス管理の民間への委託を進める方針を取り、1998 年 10 月の NSF と 2 組織との契約期間終了を機に、非営利団体である ICANN への業務移管を実施した。ICANN 自体は IANA のメンバーを中心に設立された組織で、IANA の業務をほぼそのまま引き継いでいる。



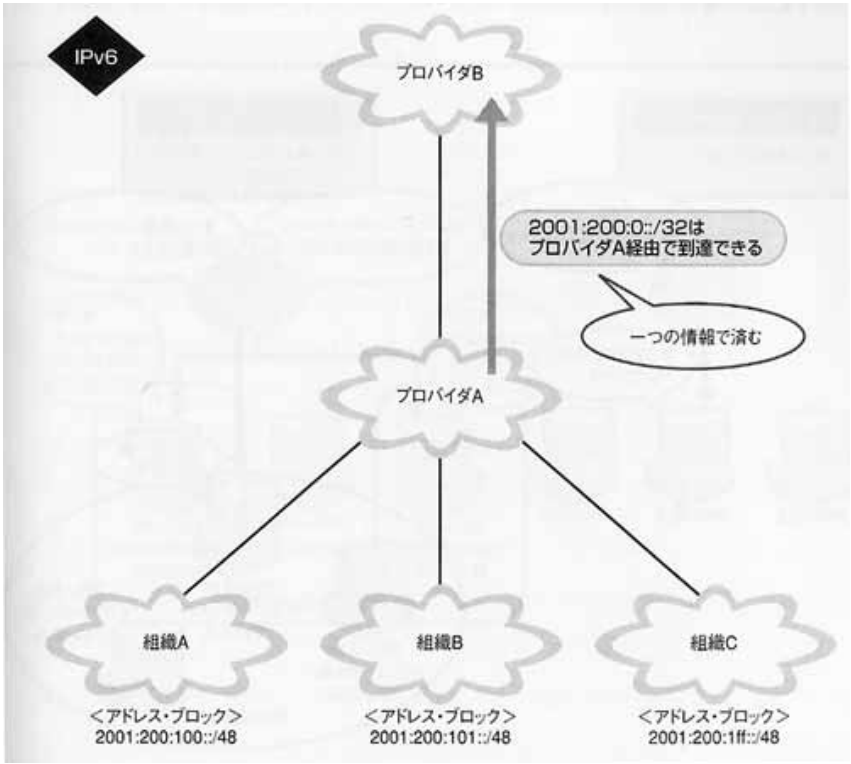


図 3.1.1.b　ルータの負荷が軽減される仕組み（入門 IPv6 ネットより引用）

3.1.2.PnP 機能（プラグアンドプレイ機能）

つい最近までは IP アドレスを設定するには、パソコン OS の TCP/IP 設定画面を開き、「202.145.119.10」といった IP アドレスをキーボードで、入力していた。ところが、現在はこうした作業しなくて済みようになっている。パソコン OS が IP アドレスを自動的に取得・設定する機能を持っているからだ。この機能のおかげで、パソコンに IP アドレスを設定する手間が省ける。また誤った設定を施すことからも解放されるのである。この機能は、DHCP のおかげで可能になったものである。

もちろん IPv6 でも、この考え方は継承されている。コンピュータの IP アドレスは、他の IP アドレスと重複することのないユニークなアドレスでなければならない。そこで、何らかの方法で、ほかのコンピュータと重複しない IP アドレスを取得する必要がある。IPv6 が動いているコンピュータは、自分に設定すべき IP アドレスの手がかりをネットワークに求める。ネットワークから手がかりをもとに、重複の無い IP アドレスを作成し。それを自らに自動設定するのである。

この線をつなげば、すぐにネットワークにつながるという機能は、非常に重要な機能となる。それは、情報家電などがネットワークに接続されるときに、複雑なネットワークの設定が必要になるということは命取りだからである。

この PnP という機能は、一般的に、「つなぐだけで、特に設定もなく物を動かす技術」の総称であり、パソコンに拡張ボードや周辺機器をつなぐと同時に、ドライバを組み込む Windows の機能も同じ名前である。

IPv6 における PnP の最終的な目的は、電源を入れたり、ケーブルに接続したりするだけで、すぐに通信環境をセットアップすることである。現在、IPv6 ソフトに実装されている。PnP の機能は、自分の IPv6 アドレスの生成と設定。そして、デフォルト・ゲートウェイの探索と設定である。

3.1.2.1.DHCP 方式

DHCP （Dynamic Host Configuration Protocol）とはネットワーククライアントに対して、IP アドレスやサブネットマスクなどのネットワーク情報を動的に割り当て可能にするプロトコル。本来 TCP/IP ネットワークでは、IP アドレスなどのネットワーク設定を各クライアントごとに行わないと正しく通信できないが、この DHCP を利用すれば、クライアント側の設定は一律「サーバから必要な情報を取り出す」という構成にしておき、ネットワークの利用時に必要な情報を割り当てられるようになる。

ユーザらすれば、面倒なネットワーク設定を省略することができ、管理者からすれば、一元的なネットワーク管理が可能になる。Windows 9x や Windows NT 4.x、MacOS などで DHCP のクライアントモジュールが標準添付されるようになり、広く利用され

るようになった。ダイヤルアップでインターネットサービスプロバイダに接続する場合なども、DHCP を利用して IP アドレスを始めとするネットワーク設定を行うのが一般的である。

この DHCP 方式は、上でも述べたように、IPv4 でおもに使われていた方法である。DHCP サーバへの登録作業には、少しのミスで、多くのコンピュータがネットワークにならなくなってしまうという問題がある。しかも、このような管理の負荷は、コンピュータの数が増えれば増えるほど重くなる。

3.1.2.2.RA 方式

RA（Router Advertisement）とは IPv6 で、一般的に使われている。アドレス配布方法である。IPv6 でも DHCP は使えるが、あまり普及していない。アドレスの表記でも述べたように、IPv6 のアドレスは、上位 64bit のプレフィックスと、買い 64bit のインターフェイス ID に分かれている。同じ LAN のセグメントに接続されていれば、プレフィックスの値は、同じである。管理者は、ルータにプレフィックスを登録するだけでよい。パソコンの台数が多くても少なくても、LAN セグメント単位で管理すればよいので、管理は楽になる。しかも DHCP では、専用のサーバを LAN ごとに設置する必要があるが、RA では特別な機器は必要ない。IPv6 ルータが、配布機能を持っているからだ。下の図では、DHCP と RA の違いをまとめてみる。

上では IPv6 アドレスの後半 64bit である。インターフェイス ID は、コンピュータ自身が作ると、説明したが、その方法は以下の通りである。

それは、パソコンの LAN カード上の ROM に書き込まれている MAC アドレスと呼ぶ 1 種のアドレスを利用するというものがある。MAC アドレスは、IEEE に登録したメーカー固有の 24bit のアドレスと、メーカーが責任を持って重ならないように割り当てた 24bit のアドレスを組み合わせた 48bit のアドレスである。LAN カードを製造するメーカーは、1 枚 1 枚。ユニークになるように、Mac アドレスを LAN カードの ROM に焼き付けて出荷している。この Mac アドレスもユニーク青をそのまま利用して、インターフェイス ID を作っているので重複することは無い。Mac アドレスは 48bit であるのに対し、インターフェイス ID は 64bit、つまり 16 ビットの情報が足りない。

そこで、Mac アドレス 26 ビットを追加してインターフェイス ID を作り出す。その際、IEEE が定めた「EUI-64」と呼ぶ書式に従うように追加する。具体的には、Mac アドレスを前半 24bit。後半 24bit に分割し、その中間 26bit の固定長サンドイッチ状に挟み込む。

3.1.3. IPSec の標準装備

IPSec とは Internet Security Protocol の略でありネットワークの情報暗号化技術である。SSL（Secure Socket Layer）という Web 上の暗号化技術や PGP（Pretty Good Privacy）という電子メールの暗号化技術などもありますが、これらはあくまでもブラウザやメールなどの特定のアプリケーション独自に暗号化する技術であるが、IPSec は IP の段階で暗号化するので上位のアプリケーションなどでは特に暗号化などを気にしなくてもすむようになる。

これらは IPv4 でもあった技術ではあるが、IPv4 下では NAT との相性の悪さや、IPSec の後付による障害などがあった。しかし IPv6 の世界では IPSec の実装が必須になっているため、IPv6 を話すことのできる端末は、すべて IPSec を利用する下地を与えられることになる。端末間の通信を IPSec で守ることが、これまでよりも飛躍的に行いやすくなる。

ここまでは IPSec をひとまとめに呼んでいたが、IPSec には実際にはいくつもの技術を組み合わせて実現されている。そこでここでは、IPSec 全体がどのようにきのうするのか、それを実現している技術がどのように実現されているのかを説明する。はじめに IPSec で実現できる機能は次の通り

1. アクセス制御
   接続元のアドレスなどに基づいて接続要求の許可や不許可を設定します。
2. 通信データの完全性の保証
   通信データが送信元と送信先の間で改竄されていないことを保証します。
3. 通信相手の認証
   データを送ってきた相手が、なりすました別人でないことを保証します。あるアドレスから送られてきた IP データグラムが、確かにそのアドレスから送られてきたことを保証します。
4. リプレイ攻撃への対処
   通信の傍受者がトランザクションのログをとっておき、後でそのログと同じことを繰り返してそのトランザクションの結果を得ようとすることを、リプレイ攻撃と呼びます。IPSec を用いて、このような攻撃を防ぐことができる。
5. 通信内容の秘匿
   通信している内容を、意図しない者から見られないように暗号化する。

これらの機能は、IPSec という大枠の中で、次のような構成要素が連携して実現しています。

1. セキュリティプロトコル
2. 認証・暗号アルゴリズム
3. セキュリティアソシエーション
4. セキュリティポリシー管理
5. 鍵交換

IPSec 各説明する前に、これらの要素がどのようなものが簡単に説明する。

3.1.3.1. セキュリティプロトコルと認証・暗号アルゴリズム

IPSec の主要な機能は IP データグラムの認証と暗号化ですが、実際の認証や暗号化にはセキュリティプロトコルが使用されます。セキュリティプロトコルには、認証に使われる AH(Authentication Header)と、暗号化に使う ESP(Encapsulating Security Payload)の 2 つがあります。これらのプロトコルは、IP データグラムにそれぞれのオプションを追加して、安全な通信を実現します。

セキュリティプロトコルはさまざまな認証・暗号アルゴリズムを利用して通信を保護します。セキュリティプロトコル自身は、決まった認証・暗号アルゴリズムを使用するわけではありません。ユーザが必要に応じて認証・暗号アルゴリズムを選択し、設定できるようになっています。セキュリティプロトコルと認証・暗証アルゴリズムは、いわば認証・暗号化のための道具だといえます。

3.1.3.2.セキュリティアソシエーション

IPSec では、論理的な通信路として、送信元、送信先、使用するセキュリティプロトコルなどを定義したセキュリティァソシエーション(Security Association :SA)というものを設定しておき、通信に使用します。セキュリティアソシエーションは、いわば安全な通信路を提供する論理的なコネクション(パイプ)です.たとえば、2 台のコンピュータが 1 本のケーブルでつながっているときに、仮想的に別のケーブルでコンピュータの間を直接するようなものだ。普通のパケットは通常のコンピュータを通るのですが、IPSec を使うように設定したパケットだけは、保護されている仮想的なケーブルを通って安全に相手のコンピュータに配送されます。

3.1.3.3.セキュリティポリシー管理

ネットワークにおけるセキュリティポリシーとは、主に「何を」「何から」「どうするか」を規定する物です。IPSec は、送信するすべてのパケットに適応することもできますが、たとえば POP3 のパケットだけ ESP を使って暗号化したり、経路制御プロトコルのメッセージ交換だけを AH を使って認識する。といった使い方もできます。このような IPSec は、パケットの送信アドレス、受信アドレス、ポート番号などによって「何を何から」守るのかを設定できるとともに、IPSec を使用するかどうか、また使

用するときにはどのような設定をするのか、といった「どのように守るか」を設定することができます。これらはいずれもセキュリティポリシーとして管理されます。

またパケットの送信時には、

●セキュリティポリシーにしたがって IPSec を使用するかどうか判断する。

●IPSec の使用時には SA から IPSec の設定情報を取り出す。

●IPSec の設定を適用し、セキュリティプロトコルを使って実際に認証・暗号化を行う。

といった手順を経ることとなる。

SA という考え方と SA をどのように使用するかを決定するセキュリティポリシーという考え方は、IPSec の機構の中で最も重要な物なので、これらの概念を理解することは IPSec を理解する上でも重要となる。

3.1.3.4.鍵交換

IPSec では、通信内容の暗号化や通信相手の認証など、さまざまな場面で暗号が使われる。暗号を使うときには事前に送信元と送信先が相互の鍵(パスワード)を共有するように設定する必要があり、この作業を鍵交換と呼びます。鍵交換は手作業でも設定できるが、設定に多くの労力がかかるため、限られた局面を除き、ほとんどの場合は IKE(Internet Key Exchange)という機構を使って自動的に交換する。

IPSec では、認証・暗号鍵が SA を構成するときのパラメータになっているため、IKE は認証・暗号鍵だけではなく SA のパラメータ全般を交換するようになっている。このため、IPSec において鍵交換と言った場合、SA を設定するまでを指すことになる。

このように IPSec の機能が細分化されているのは、ある機能に弱点が見つかった場合やより強力なセキュリティ機能が必要になった場合でも、ほかの機能に影響を与えずに交換や追加が可能だからである。ある暗号アルゴリズムに欠陥が見つかった場合に、IPSec のスタック全体を交換しなければならないとすれば、たいへんなコストがかかる。

しかし、暗号アルゴリズムだけを簡単に交換できれば問題をすぐに修正することができる。このように、IPSec は機能が非常によく構造化されているのですが、またそれゆえに全体像の把握が難しくなっているという側面がある。

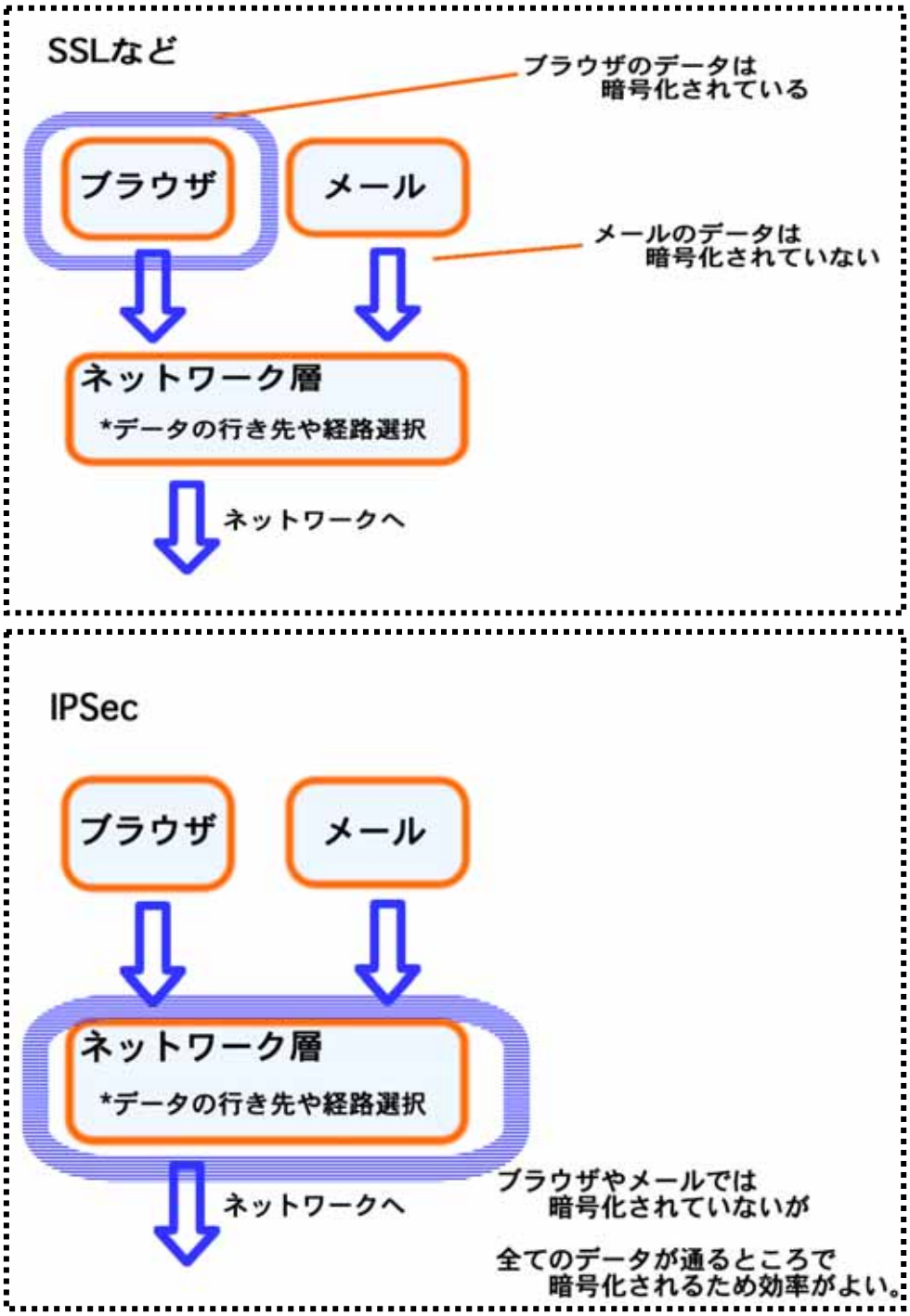


図 3-1 SSL などの暗号化と IPSec の違い

この IPSec では共有鍵暗号方式がとられている。公開鍵暗号（こうかいかぎあんごう、Public key cryptosystem）とは、暗号化と復号に別個の鍵（手順）を使い、暗号化の為の鍵を公開できるようにした暗号方式のことである。

暗号は通信の秘匿性を高めるための手段だが、それに必須の鍵もまた情報であり、鍵自体を受け渡す過程で盗聴されてしまうリスクが暗号の秘匿性のネックであった。この問題に対して、暗号化鍵の配送問題を解決したのが公開鍵暗号 Diffie-Hellman 法（以下、DH 法という）である。

1976 年に、ウィットフィールド・デフィー (Whitfield Diffie)、マーティン・ヘルマン(Martin Hellman)によって、初めて公表された。DH 法で利用者 A と利用者 B が共通かぎ K を共有するまでの手順は、次のとおりである。

(1)　素数 p と、 p よりも小さいある自然数αが公開されていて、利用者 A と利用者 B がともに知ることができる。

(2)　利用者 A は、 p よりも小さい任意の自然数 XA を選び、秘密かぎとして保持するとともに、次の式で得られる公開かぎ YA を利用者 B に送る。

$$YA = \alpha^{XA} \bmod p$$

ここで、x mod y は 整数 x を整数 y で割った余り（剰余）である。

(3)　利用者 B は、 p よりも小さい任意の自然数 XB を選び、秘密かぎとして保持するとともに、次の式で得られる公開かぎ YB を利用者 A に送る。

$$YB = \alpha^{XB} \bmod P$$

(4)　利用者 A は、利用者 B の公開かぎ YB を使って、次の式によって共通かぎ K を得る。

$$K = YB^{XA} \bmod P$$

(5)　利用者 B は、利用者 A の公開かぎ YA を使って、次の式によって利用者 A と同じ共通かぎ K を得る。

$$K = YA^{XB} \bmod P$$

DH 法によるかぎ共有を利用して、図に示すように、安全でない通信経路を利用す

る 2 者間で機密情報を送信する仕組みを作る。まず、利用者 A と利用者 B は DH 法を使って、共通かぎ K を共有する。次に、利用者 A は平文を共通かぎ K を使って暗号化して送信する。利用者 B は受信した暗号文を共通かぎ K を使って復号して、元の平文を得ることができる。

例としてここでは素数ｐを 17、自然数αを 10 として計算してみる。

<table>
<tr><td colspan="2">素数 P＝17　自然数α＝10</td></tr>
<tr><td>たかし</td><td>ひろゆき</td></tr>
<tr><td>XA=12　と置く

$YA = a^{XA} \bmod P$　なので

YA は$10^{12} \div 17$の解の余り
YA=13</td><td>XB＝5　と置く

$YB = a^{XB} \bmod P$　なので

YB は$10^{5} \div 17$の解の余り
YB＝6</td></tr>
<tr><td colspan="2">ここで YA と YB を交換する</td></tr>
<tr><td>$K = YB^{XA} \bmod P$
$= 6^{12} \bmod 17$
＝13</td><td>$K = YA^{XB} \bmod P$
$= 13^{5} \bmod 17$
＝13</td></tr>
</table>

このように 2 人が共通の平文を得ることができた。この計算ではたかし、ひろゆきが自ら決めた数字（XA と XB）は送信しないために第三者に読み取られることはない。しかし、その自ら決めた数字を使って暗号を解くために、第 3 者は送信されるすべての数字を読み取ることができたとしても暗号を解くことができない。実際には自然数も素数も桁数の多いものを使うのでスーパーコンピュータを使って総当りで計算させても億単位の年数がかかるので解読は無理とされている。

3.2. IPv6 を利用する

新しいインターネットプロトコルを利用するためには、次にあげる構成要素が揃わなくてはなりません。

1.ネットワーク機器
2.OS の対応
3.アプリケーション
4.ISP のサービス

それぞれの現状を、ここで簡単にまとめる。しかし、IPv6 の研究開発が進むにつれて、次々と新しい成果が発表されているので、最新の情報もあわせてチェックするようがあると考えられる。

また少し変わった方法であるが、現状のルータや設定のままで IPv6 を使うこともできる。FreeBit 株式会社の「Feel6」（http://start.feel6.jp/）というサービスを使うと PC にグローバルアドレスが割り当てることができれば現状の IPv4 のルータでも IPv6 に接続ができるというものもある。

3.2.1. ネットワーク機器

IPv6 では IPv4 で利用していたイーサネットなどの既存のネットワーク媒体を使用できる仕組みがある。また、IPv6 と IPv4 は同じイーサネットで「相乗り」ができる。これはちょうど、AppleTalk と TCP/IP が同じイーサネットで共存できるのと同じ。

専用ルータについては、すでに IPv6 対応の製品がいくつか販売されている。有力メーカーの Cisco Systems 社も正式に対応を開始し、そのほかのメーカーからも新製品がでている。また、IPv6 対応の実験ファームウェアを提供しているメーカーも多いので、試験的にファームウェアを入れ替えて利用することも可能である。

3.2.2. OS の対応

BSD 系 UNIX、Linux、Solaris、Windows2000、WindowsXP、MacOSX では、すでに IPv6 スタックが用意され、利用できる。

3.2.3. アプリケーション

UNIX では、WWW、電子メール、FTP など、既存の主要なサービスのサーバやクライアントを IPv6 で利用可能です。Windows 系は、クライアントであれば主要なサービスが IPv6 に対応しています。

3.2.4. ISP のサービス

これまでにも実験目的のバックボーンネットワークが運用され、そこで使用する IPv6 アドレスが配付されてきましたが、試験的なものであったので、商業目的に使用することはできなかった。しかし 2000 年からは、正式な sTLA アドレスの配付が開始され、ほとんどの ISP がこのアドレスを取得している。そのうちの数社は実験的なものも含め、商用サービスを開始している。また、ISP の本格的な運用には、大量のトラフィックを転送できる性能の高い IPv6 対応のルータが販売され、sTLA 組織が相互に接続する IPv6 の IX 拠点がつくられることが欠かせない条件となっているが、ルータも徐々にリリースされ、IX 拠点も整ったので、ISP のサービスもしだいに拡充していくと考えられる。

国内の ISP では IIJ、NTT、パワードコム、KDDI など多くの ISP で IPv6 が利用可能になっている。

4. IPv6 の現状

2001 年 3 月に発表された「e-Japan 重点計画」の目玉施策として、光アクセス網及び DSL 網の整備推進が示され、それとともに IPv6 ネットワークの普及推進が盛り込まれた。

具体的な目標として、「少なくとも 3000 万世帯が高速インターネットアクセス網 に、また 1000 万世帯が超高速インターネットアクセス網に常時接続可能な環境を整備する」ことや、「インターネット端末やインターネット家電が普及し、それらがインターネットに常時接続されることを想定し、十分なアドレス空間を備え、プライバシーとセキュリティの保護がしやすい IPv6 を備えたインターネット網への移行を推進する」ことが掲げられた。

以来、IPv6 への注目は徐々に高まり、国内における IT・通信関係の各種メディアでは常に重要なキーワードの 1 つとして扱われるまでになった。

その後、推進計画は e-Japan 2002 に引き継がれ、IPv6 普及に向けた官民一体の取り組み、日本の先進性は世界でも認められ、高い評価を得ている。

一方、海外でも欧州や中国など、各々の国・地域のタスクフォースが中心となり国際会議などさまざまな活動が行われている。特に中国は今後インターネットの普及が本格化しようという状況下で、既存の IP アドレスの不足は大きな障害となり得ることから、高い関心を持って国を挙げた取り組みを始めつつある。さらに、2003 年夏には、それまで IPv6 にはあまり関心を示していなかった米国でも、国防省が 2008 年までに完全 IPv6 移行を目指し、2003 年秋からの関連調達を IPv6 対応とすることを盛り込んだことで、急速に関心が高まり始めている。

また 2004 年には、一般コンシューマ向けの展示会として名高い International CES（International Consumer Electronics Show、ラスベガスで 2004 年 1 月開催）でも IPv6 のフォーラムが設けられ、一般のインターネットユーザーに対してもキーワードレベルからの浸透が始まっていることが伺える。

IPv6 は次世代インターネットの基盤として、e-Japan 重点計画が目標年次とする 2005 年を終え現状はどうなっているのか。

4.1.製品

まず上でも述べたように、必要に機器がそろわなければサービスを享受することはできないのでどの程度の対応製品がどんな形でどのくらいの数が市場に出ているかを調べてみる必要がある。

4.1.1. 規格統一

IPv6 のような新しい技術を含む分野において、その対応製品が幅広く使われるようになるためには、製品同士の接続性を確保することが非常に重要です。そもそも IPv6 には仕様自身に曖昧な点が多く製品間での細かな仕様の違いにより繋がらない、使えないなどといった問題が生じるおそれがあるし、今後製品が増えるにつれてその可能性は確実に拡大し市場の紺アランや健全なビジネスの阻害に繋がると考えられる。

そういったことを無くすために、IPv6 Ready Logo Program というものがある。これは細かい仕様などを統一仕様という動きで IPv6 Ready Logo Committee(IPv6 Forum)の一員として IPv6 普及・高度化推進委員会のサーティフィケーション WG が参加し IPv6 機器同士の接続性を確認する為の検査仕様や検査ツールを中立的な立場で開発している。ここで一定のテストを通った物に対してロゴが与えられる。ここで述べる対応製品とはこのテストに通り認定を受けた物である。

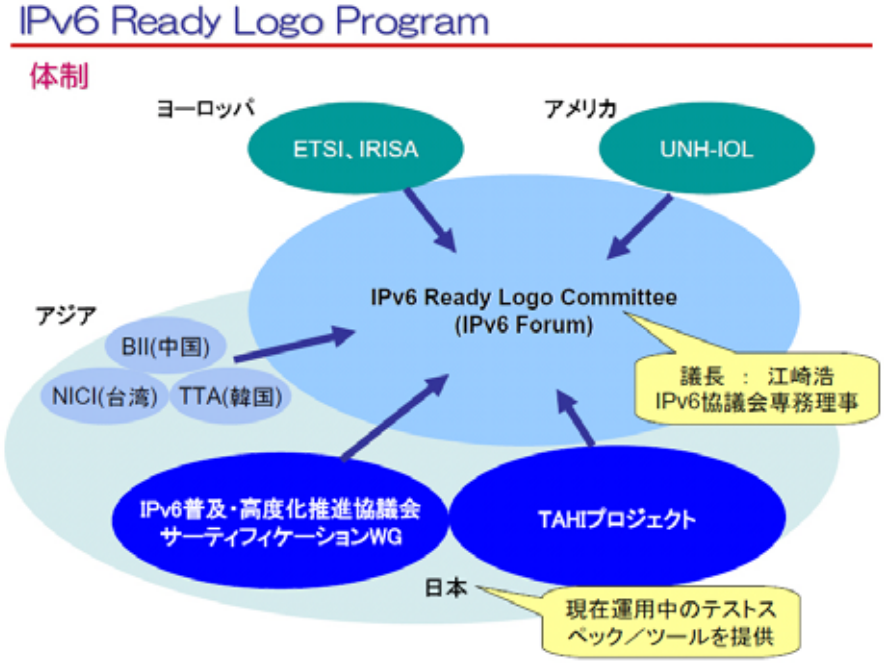


図 4.1.1.a　IPv6 Ready Logo Program の体制

またこのロゴ認証には 2 つのクラスがあり、Phase-1 と Phase-2 に分かれている。
それぞれの違いは次の通り。

●Phase-1
　IPv6 仕様の最も基本的な部分に限定し、
あらゆる機器が基本的に満たすべき IPv6 の機能への適合性を見る。

●Phase-2
Phase-1 に比べて、より実用的、専門的機能について、
IPv6 の機能への適合性を見る。

ロゴの取得には以下のような手順を踏む

1. IPv6 Ready Logo Program に関する詳細情報、テストに関する情報、テストツール等を入手（ただし全て英語）http://www.ipv6ready.org/
2. セルフテストのための環境を構築（テストツールの稼働環境は FreeBSD）相互接続テストのためのホスト、ルータ等も同様に用意
3. 各ベンダ社内にて試験を実施（セルフテスト、相互接続テスト）
4. IPv6 Ready Logo Committee に審査を申請
5. 審査に合格すればロゴ ID、ロゴデータが発行される

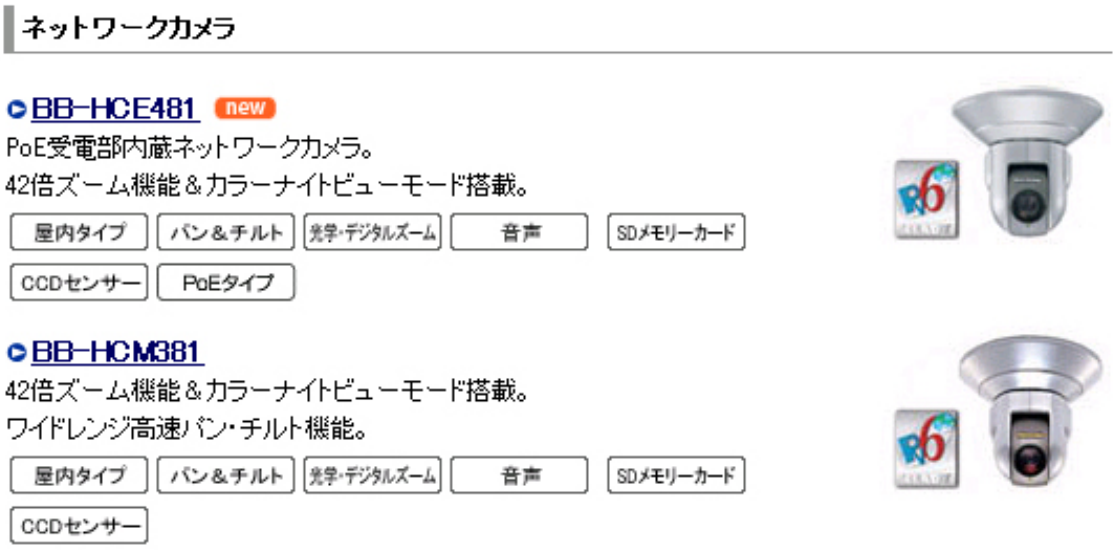


図 4.1.1.b ロゴ取得後の使用例（Panasonic）

4.1.2.商品普及

この規格統一がなされた商品、あまり一般向けの商品でないことがまだまだおおいが着実にその数を増やしてきている。2005 年 10 月現在で Phase-1 製品は 191 製品、Phase-2 製品は 19 製品が発売されている。以下はその推移のグラフ。

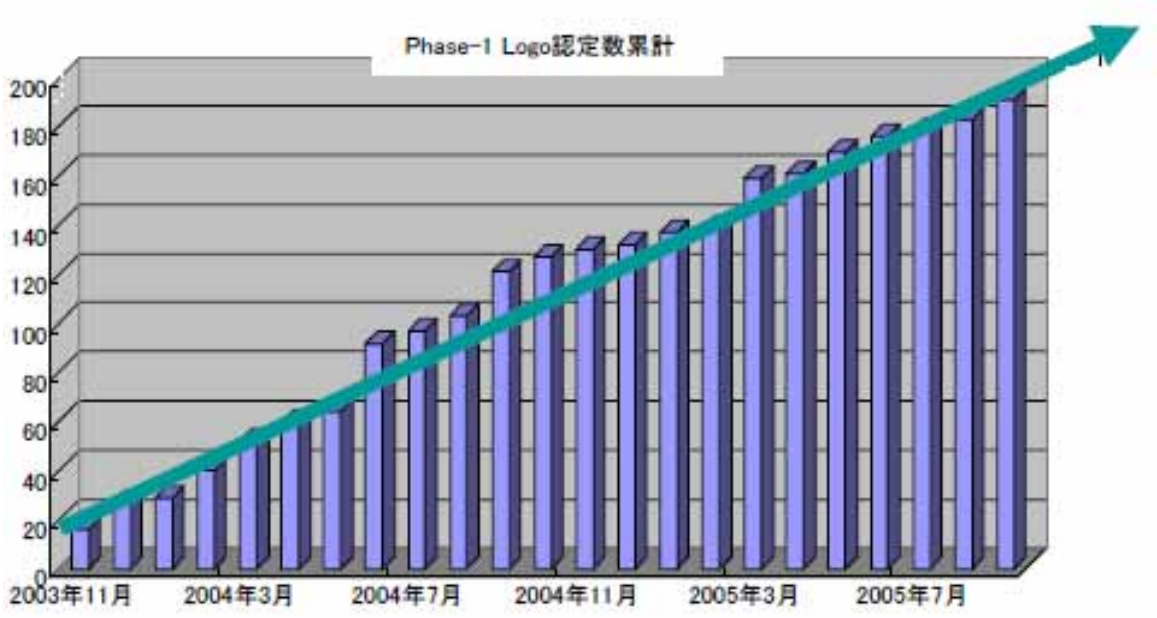


図 4.1.2.a　Phase-1 取得製品の推移

図 4.1.2.b　Phase-2 取得製品の推移

このロゴ取得製品は日本製品が多く Phase-1、Phase-2 どちらも日本製品の取得率が一番となっている。

●Phase-1		●Phase-2	
日本：	90 製品	日本：	8 製品
アメリカ：	26 製品	アメリカ：	6 製品
台湾：	22 製品	韓国：	2 製品
韓国：	22 製品	台湾：	2 製品
その他：	31 製品	デンマーク：	1 製品

図 4.1.2.c　国別ロゴ取得製品数

4.2.サービス

品はこれだけ増えてはいるが、サービスはどうだろうか。企業向けのサービスは製品でも紹介したようにだんだんと現れているようだが、家庭でのサービスはまだ少ない。少ない理由としては、まだ IPv6 でないとできない、という事例が少ないからのようである。以下の章では導入事例について研究していきたい。

4.2.1.企業での導入事例

ここでは 4 つの導入事例、株式会社プラネットの CD 試聴機、KDDI 研究所の所内の IPv6 化、日本ユニシスの IC タグなどを活用したデータ収集の基盤、そしてフリービットが共立メンテナンスに提供した IP フォンの事例を示す。

4.2.1.1.株式会社プラネット

株式会社プラネット(以下：プラネット)は、音楽ソフト業界におけるシステムの開発と情報処理サービスシステムの提供を一貫して行ってきた企業だ。近年、試聴のニーズは年々増加しており、こうした背景からデジタル試聴システムの開発・提供に力を入れてきた。

「実際に CD を利用した試聴機では、一度にセットできる枚数は 10 枚程度と限られてしまいます。そのため店舗がセットしたメディアが顧客の嗜好とミスマッチすることも起こりうるのです。さらに CD ですと、当然ながら店内すべての CD を試聴することはできません。私たちはこれをなんとか解消して、"立ち読み"の音楽版、いわば"立ち聞き"が実現できるような環境にしたいと考えました」。(川上氏)

プラネットは、"立ち聞き"を実現するために、まずストリーミングで音楽を再生する PDA を使った試聴機を開発した。

「PDA 試聴機は、無線 LAN を内蔵し CD のバーコードをかざすことで、MP3 音源を再生する仕組みです。音源は、JMD（ジャパンミュージックデータ）が提供するも

のを利用しており、現在約 110 万曲にも及びます。試聴は、著作権に抵触しない 45 秒ですが、店内を回りながら気に入った CD をどれでも試聴できるという点で、従来の試聴機とは一線を画するものになったと思います」。（川上氏）

しかし、実際に店舗に導入してみると、貸し出すための個数を確保する必要があるという課題が明確になった。そこで、改良版として提供したのが PDA を埋め込んだ壁掛けタイプの試聴機や 15 インチのタッチパネル型の試聴機だ。これらの壁掛けタイプのシステムは、ヒットチャートの閲覧、検索などの機能も充実しており、すでに多くの店舗で活用されている。

「長年の経験により蓄積されたデータからも"試聴"によって、確実に購買率が上がることが分かっています。そのため、"試聴"を戦略的かつ効果的に利用することが、店舗作りの上でも非常に重要です」。（多田氏）

プラネットは、販売チャンスを確実に向上させる"試聴"と既存の情報サービスの融合で、CD ショップやレコードメーカーにより高付加価値のサービスを提供することを目指している。

ただしここまでの製品ならば従来の IPv4 を使ってもできる。なぜ IPv6 を使ったのかというところに問題がある。

プラネット多田氏は次のように述べている。

「IPv6 による第一のメリットは、セキュリティの高さです。音や映像といった権利を取り扱うサービスにおいて、セキュリティレベルの強化は最も重要です。そのため、あらかじめ IPSec によるセキュリティの強度に配慮されたプロトコルである IPv6 は、より最適なサービスを提供する環境を実現する上で不可欠となります」。

「第二に IPv6 は、ピアツーピアの情報流通が前提となります。素材そのものが、個人の趣味や嗜好といった対象を扱うため、最適な情報を個々に Push することも視野に入れたサービスの構築を目指しています。 そして、今後映像も含めたより大容量の情報の取り扱いを考えた場合、マルチキャスト配信やセキュリティの強化などを実現するためには IPv4 では、コストの負荷が大きすぎることが課題でした。これらを IPv6 ベースで構築すればより低コストで運用できることが試算から明らかとなったのです。

また今後、IP 電話の普及が起爆剤となり、グローバル IP 対応が一般的になると思います。それによって、様々な端末が IPv6 ベースで通信することが当たり前になると想定しています」

と述べているように IPv6 を使う利点としてここではセキュリティ、Push 型配信、コストということがあげられている。この製品はまだ試験段階ということだが、同社は CD ショップ向けの POS システムも開発しており、IPv6 を使うことによって店舗に訪問するお客様の顧客情報を持たなくても、個々の端末に対する情報の提供や双方向の情報交換が可能になりさらにコストとダウンも望めるということで期待がもたれる。

図 4.2.1.1.a　HOTNAVI™（株式会社プラネット）

4.2.1.2.KDDI 研究所所内の IPv6 化

通信事業者である KDDI のグループ企業として研究開発を行っている KDDI 研究所は、2004 年 9 月末に所内ネットワークでの IPv4 利用を厳しく限定し、ほとんどを IPv6 オンリーに切り替えた。これは期間の限られた実験ではなく、実稼動ネットワーク環境の切り替えである。その過程で、さまざまな課題が明らかになってきた。

KDDI 研究所が、埼玉県上福岡市にある端末約 200 台規模の研究所を IPv6 化するきっかけとなったのは、研究所長である浅見徹氏の一声だったという。上福岡の研究所内のネットワークは数年前から IPv4/IPv6 のデュアルプロトコル環境だった。DNS、メール、Web の各サーバも IPv4 と IPv6 のデュアルプロトコル構成になっていたが、端末として IPv6 を使うのは IPv6 関連の研究用のものだけに限られており、一般的な端末には IPv4 しか導入していない状況だった。

浅見氏の考えは、「IPv6 で新しいサービスを開発していく立場にあるにもかかわらず、IPv6 を使っていないのはおかしい」。そこで研究所の完全 IPv6 化プロジェクトがスタートした。

一般端末に IPv6 プロトコルを追加してデュアルスタックにするだけでは、結局 IPv4 が使われることになってしまう。そこで、KDDI 研究所では、一般端末を IPv6 オンリーとすることにした。同研究所では、ユーザ端末のほとんどが、Windows 2000 や Windows 98 を含む Windows ファミリを利用していた。UNIX や Linux を使う研究所員もいるが、こうした人でも業務書類等の関係から Windows 端末は必ず利用しており、リモートで UNIX や Linux のアプリケーションを動かしている。同研究所では、これらすべての Windows 端末を Windows XP に統一し、さらに IPv6 だけを有効とした。これらの端末で所員は、Web、電子メール、FTP により、日常業務を行う。

ここでの大きな成果はコストダウンなどではく問題点の発見だった。たとえば WindowsXP SP2 が IPv6 の構成に問題があったり、WindowsXP ファイル共有が未対応、ウイルス対策ソフトの未対応、JAVA アプレットの未対応など様々な問題点が見つかった。

以上のような問題に悩まされたものの、KDDI 研究所では IPv6 ネットワークの利用を続けている。しかし、日常作業用端末を WindowsXP 環境に統一したことにより IPv6

対応は、プロトコルを実装した段階で、アプリケーションでの対応がこれから重要になること認識した。

「今回、IPv6 化をやってみて感じたのは、業務を限定して IPv6 化すれば、IPv4 と変わらずに仕事をすることはできるということ。これが今の IPv6 のレベルだと思う。ただし、もう少し便利にやりたいときに、IPv6 ではまだ不十分なことが多い」と久保氏は話す。

IPv6 は、固定アドレスを使ったアクセス制御やピアツーピア通信に便利といったメリットがある。今後ピアツーピア・アプリケーションがどのように展開していくか、セキュリティやプライバシーの問題も含めて注目していきたいという。

4.2.1.3.日本ユニシスでの導入事例

日本ユニシスは、IC タグなどを活用したデータ収集・管理のためのアプリケーション基盤に、IPv6 ネットワークサービスを組み合わせた「データ共有プラットフォーム」を、2005 年第 1 四半期から推進し始めた。

これは、無線 IC タグなどを利用した在庫管理、トレーサビリティなどのアプリケーションのための、ミドルウェアとネットワークサービスを提供するものだ。

データ共有プラットフォームは、各種のデバイスから得られたデータをアクセスコントロールとセキュリティをかけた状態で共有および活用するというコンセプトで作られた。構成する要素は、同社が開発したデバイスデータを処理するミドルウェア「Information Wharf」、NTT コミュニケーションズが開発したセキュリティ技術「m2m-x」、そしてデータを利用する際の標準的なサービスを備えたアプリケーションソフトウェア基盤である。このプラットフォームを活用することで、多様なデバイスから得られたデータの処理、データの状態に応じたビジネスロジックの起動、ユーザとのアクセス権限管理という 3 つのことができる。

RFID によるモノの追跡管理を通じた業務の効率化や付加価値実現への関心は、この 1～2 年で急速に高まりつつある。政府レベルの実証実験がいくつか実施されてきたが、一般企業においても試験導入や本格運用を検討する企業が増えている。

こうしたプロジェクトによる RFID の利用方法は、アプリケーションこそ違っても、RF ID の追跡管理という点ではほとんど共通だ。今回のデータ共有プラットフォームは、こうした共通なソフトウェアコンポーネントをミドルウェアとして切り離し、在庫管理やトレーサビリティなど、外部のアプリケーションとの間でデータをやり取りするための、XML をベースとした汎用的なインターフェイスを提供している。こうすることで、RFID 関連のプロジェクトに要する時間とコストを節約することが狙いだ。一から作るのと比較して、開発工数が 1/3 くらいになり、ミドルウェアを使用するので運用保守も簡易化できるという。

さらに IPv6 を採用し、ネットワークまで含めたプラットフォームを提供することで、

1 社に閉じたシステムではなく、メーカー、卸売業者、小売店など、地理的にも散在する複数の事業者にまたがった大規模なシステムの構築を容易にすることも狙っている。

このシステムでは「さまざまなデバイスから得られたデータを一元管理し、バリューチェーン上の各種ステークホルダーが、事前の設定に応じてデータを共有することが可能。さまざまな事業体にわたるシステムで、Web サービスのインターフェイスを通じ、収集したそれぞれのデータを適切な者のみが利用する仕組みをつくることができる」と、日本ユニシスのエンタープライズソリューション事業部、ユビキタスディベロップメントリーダー、末永俊一郎氏は話す。

このプラットフォームは、実は RFID の利用に特化したものでもない。バーコードをはじめとした ID 管理システムやセンサーなど、さまざまなデバイスから入力された情報を管理し、アプリケーションに対して提供することができる。このため、柔軟性の高いシステムが構築できる。

たとえば、まずバーコードでシステムを構築し、将来に RFID へ移行する場合にも、システムを修正することなく対応することができる。バーコードと RF ID が混在するようなシステムを構築することも可能だ。RFID のチップやリーダー／ライターをシステム構築後に任意の時点で変更することもできる。さらには、企業におけるファイルサーバ上のデータを、コピー機やプリンタから適切な認証の下で出力するような仕組みもつくることができる。

今回のデータ共有プラットフォームで IPv6 を採用した理由について、末永氏は、「IPv6 を使ってセキュリティと P2P を実現しておくことが、今後を考えたときには妥当だろう」と考えた、という。

システムがさまざまな組織にまたがる場合、現在の IPv4 では基本的にはアプリケーションレベルのセキュリティしか実現できない。特に RFID リーダー／ライターやセンサーは、任意の遠隔地点に設置される可能性があるため、事前にネットワーク構成をすべて計画した上で導入することは極めて困難だ。

IPv6 であれば、IPSec を利用して、任意の機器同士がピンポイントで安全に通信する仕組みを構築することができる。システムをいったん構築した後に、接続地点が加わったり、廃止されたりしても、容易に対応することができる。今回のプラットフォームでは、NTT コミュニケーションズの光あるいは ADSL による IPv6 接続サービスを用い、さらに m2m-x を利用している。これは、NTT コミュニケーションズにより提供されるデバイス間の接続管理とセキュリティ確保のサービスで、集中的なセキュリティポリシーを、分散配置されたデバイス間の通信に、自動的に適用することができる。もちろん、IPv6 のプラグアンドプレイ機能によって、RFID リーダーやセンサーをネットワークに接続するだけで、通信が可能になるというネットワークメンテナンス面での利点もある。

m2m-x では、ネットワークセキュリティポリシーを通信事業者が運用するため、利

害関係が交錯する事業者にまたがるシステムにも適用しやすい。NTT コミュニケーションズでは、日本国内だけでなく、海外でも IPv6 サービスを展開しているため、国際的なシステムにも利用できる、という。

今回の導入事例ではコストとセキュリティ、拡張性という面が導入への引き金となっていたようだ。

4.2.1.4.共立メンテナンス

共立メンテナンスは学生寮・社員寮運営の最大手。全国 320 カ所で「ドーミー」「ドミール」といった名称の寮を運営する。同社は 2004 年 6 月から、運営する寮に順次 IP 電話を導入した。2005 年 1 月末にその数は 1 万 6500 台に達した。IP 電話導入の狙いは、（1）寮生の電話代削減とインターネット接続環境の改善、（2）通信コストや機器管理費削減の二つ。だが、注目すべきは、大規模多拠点へのスピード展開にある。導入開始からわずか半年で全国 100 以上の寮に、1 万台以上の IP 電話を導入。この展開に役立ったのが IPv6 だ。

共立メンテナンスが導入したのが、IPv6 対応の IP セントレックス・サービス「FreeBit OfficeOne」。フリービットが手がける ASP（application service provider）方式のサービスで、8 社のコンペから選んだ。このサービスを選んだのは、回線コスト削減が見込めただけではなく、機器を自前で持つ必要がなかったため。管理・運用コストの削減も見込めた。

同社は、過去に数億円を無駄にしたことがあった。寮生のインターネット接続用に 1999 年導入した HomePNA1.0 対応機器だ。約 250 棟に導入したが、1M ビット/秒の通信速度はあっという間に陳腐化。こうしたリスクを負わないため、これから導入するシステムは、自前で機器を持たないことが前提だった。

電話も同様だ。かつて、頻繁に変わる電話料金への対応に追われた経緯があり、できれば自前の施設は持ちたくなかった。「電話とインターネットの二つのサービスを一気に改善したい」（共立メンテナンス取締役の竹本泉情報マネジメント部長）。これらの要望を満たしたのが、フリービットのサービスだった。

こうして導入したのがネットワーク。IPv6 と IPv4 が混在するのが特徴だ。寮には IP 電話導入に伴い、100M ビット/秒の LAN を敷設。WAN には B フレッツを導入し、この回線を音声と共用。大規模な寮は、B フレッツを 2 回線に増設した。音声系は IPv6、データ系は IPv4 に統一し、同一のネットワーク上で扱う。これは、必ずしも寮生全員がインターネットに接続するわけではないため、2 系統の LAN を敷設すると無駄になるからだ。ただし、IPv6 と IPv4 のネットワークはタグ VLAN により論理的に分かれている。使用する IP 電話は、岩崎通信機に特注した。IP 化により共立メンテンナンスが NTT 東西地域会社へ支払っていた回線コストが億円単位から数千万円単位に激減。年間 2000 万から 3000 万円かかっていた PBX の保守料も不要になった。さらに「寮

生の電話代が従来に比べて半分から 1/3 に減った」（共立メンテナンス情報マネジメント部情報システム室・ネットワーク事業室の吉住昌弘室長）。

共立メンテナンスの導入事例の特徴は、その驚異的な導入スピード。このスピードに貢献したのが IPv6 だ。実証実験を開始した 2004 年 6 月から半年後の 12 月末には、早くも 1 万台超を導入。そもそも IPv6 を採用した理由は、（1）2 万台の端末へグローバルアドレスを割り当てる、（2）管理・運用のため即座に端末が特定できる、（3）設定が容易、といった条件を満たしたためだ。IPv4 では 2 万台分のグローバルアドレスを取得するのが難しい。NAT や NAPT を使ったプライベートアドレスの使用では、センター側から端末の特定が難しい。そして（3）の設定が容易というメリットが、IP 電話の劇的なスピード展開を可能にした。

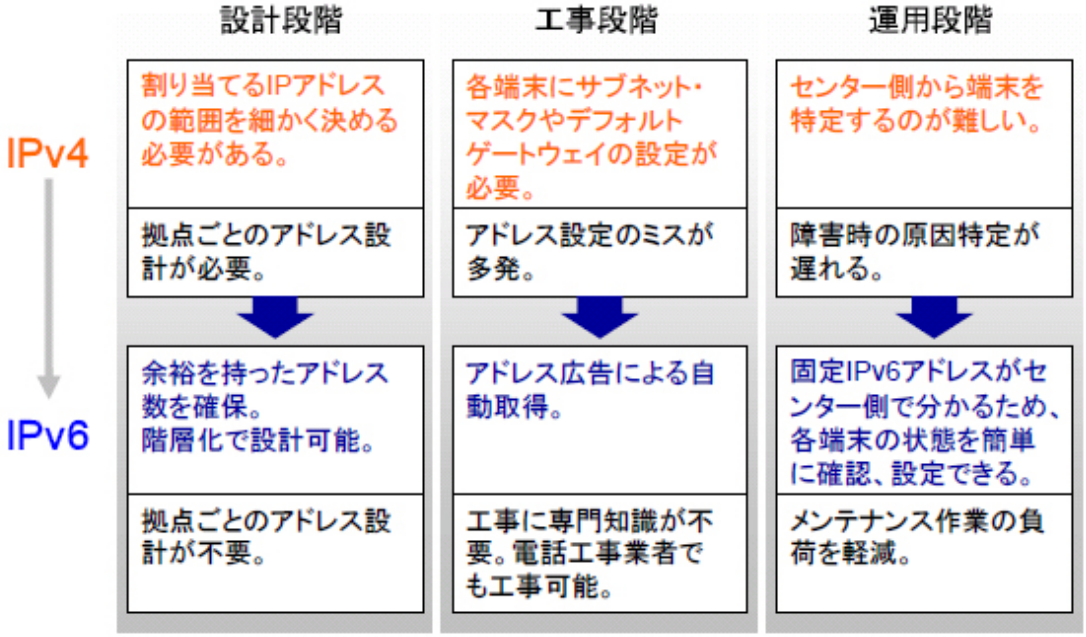
実証実験では、当初は IPv6 ではなく、IPv4 のグローバルアドレスを一時的に導入した。トラフィック・パターンなどを事前に把握するためだ。だが、ここでの最初の作業で手間取った。作業は、従来からの電話業者が行った。電話の専門家ではあっても、IP ネットワークの専門家とは限らない。そのため数が多いとミスも起こりやすい。IP 電話に割り振る IP アドレスなどを手入力する際、「アドレスの重複などを探し出す作業自体が大変だった」（フリービット OfficeOne 事業部営業推進グループの廣川聡敏アシスタントマネージャー）。

寮は全国展開しており、導入時は地元の業者が設定する。また、実際に居住者が居る部屋で作業しなければならないこともあり、短時間で作業を終わらせることが大前提。こんな事情から IPv6 以外の選択肢はあり得なかった。IPv6 では一意に端末を特定できるし、端末側にアドレスを入力する手間が省ける。IPv6 電話機側の設定には TCP/IP の設定は要らず、内線番号を登録するだけで終わる。「IPv6 の場合、電話機の設定が再起動時間も含めて 1 台当たりわずか 3 分。設定作業は 1 分以内に終わる」（フリービットの廣川アシスタントマネージャー）。

設定も柔軟に変更できる。訪問者があった際、管理者が自室にいるとは限らない。そこで、寮長室以外に管理室と食堂の IP 電話も同時に鳴らしたい、といった対応も「30 秒で設定できる」（フリービットの廣川アシスタントマネージャー）。PBX を使っていた当時は「見積もりを取るなどしていると、設定変更のために 1 週間かかることもあった」（共立メンテナンスの吉住室長）。こうした対応が迅速にできるのも、全 IP 電話機に IPv6 のグローバルアドレスを割り振ったため。設定変更時やトラブル時は、該当の IP 電話を Web ブラウザによる管理画面（写真 1）から即座に特定できる。また電話機のファームウェア更新や再起動もセンター側からできる。

良いことづくめに見えるが、電話自体の機能はまだ発展途上。寮生から要望が多かった留守番電話機能は、ようやく 4 月に実現のめどが立った。コードレス子機が欲しい、といった要望も上がっている。電話機自体の機能向上が今後の課題だ。

この事例ではコスト、拡張性に加えて迅速に設定できるということもポイントの一つのようだ。ここでは IPv4 を使ったときとどう違うのかを図にしたものをこのシステムの提供元である FreeBit から引用する。



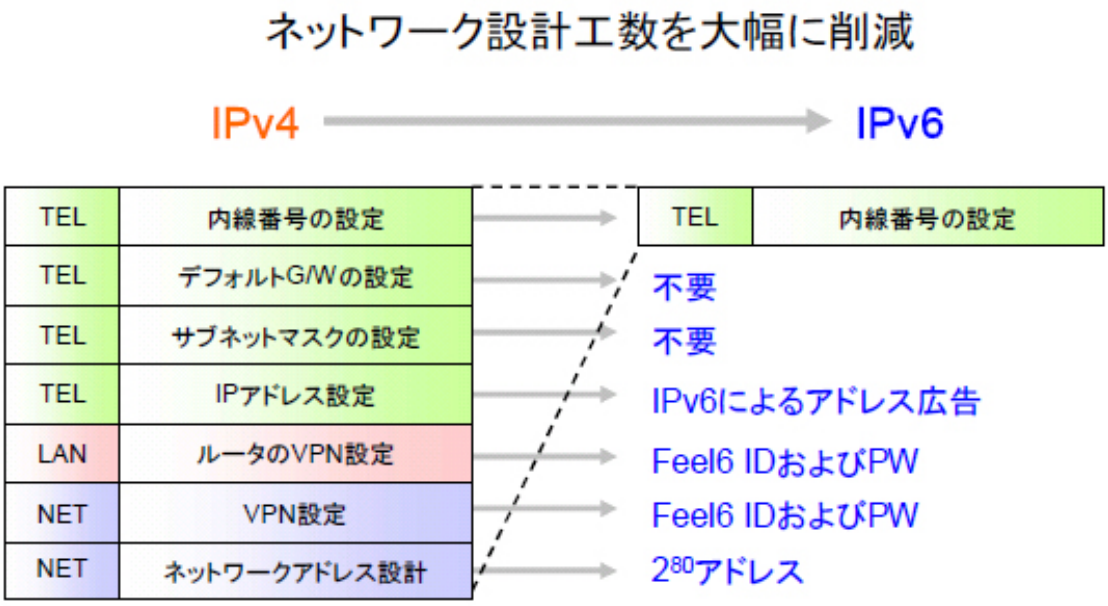


図 4.2.1.4.a　IPv6 の利点（FreeBit からの引用）

4.2.2.家庭での導入

企業での導入事例はまだ少ない物の着実に実用段階にまであがってきているが、家庭ではどうだろうか。実際家庭での正式導入で効果を上げた例はほとんどないといえる。がその普及に関して推進させていこうという動きが出てきた、下で示す FreeBit の IPv6 接続サービスと KDDI の実験やウイルスバスター2006 が初めてコンシューマ向きのウイルス対策ソフトウェアで IPv6 に対応したことからもその動きが伺える。

4.2.2.1.FreeBit の Feel6

まずこの Feel6 とはなにか。『FB Feel6 接続サービスは、フリービット株式会社が開発した、Feel6 Technology を利用して、「誰もが技術を意識することなしに今日からすぐに IPv6 を ” 感じる ” ことができる」環境をご提供することを目的としたサービスです。

FB Feel6 接続サービスが他の接続サービスと異なる点は、接続自体ではなく IPv6 でつながったらどのような世界になるのか？という事を実際に味わっていただくことに焦点を置いていることです。 その為、特別な環境を準備する必要が無く、日常インターネットを使っている人であれば誰でも ” カンタン ” に利用できるようにするという部分に様々な努力を行なっています。

最新の情報が自然に送られてきたり、パソコンにたまっているメールが会社のパソコンやケイタイからチェックできたり、湘南からのラジオ放送を受信できたり、様々な IPv6 ならではの体験を準備しております。』

目的としては『現在、IPv6 技術への期待は大きくなってきていますが、IPv6 への対応を担う通信機器メーカー/通信キャリア/ISP サイドでは、市場が見えない IPv6 に対して大規模な設備投資を行うことは難しく、IPv6 に対する動きは「ネガティブスパイラル」に入ろうとしている。

この「ネガティブスパイラル」を脱却するために、ISP Enhancer としての中立的存在として、様々な技術を ISP に対して提供を行ってきたフリービットと、日本を代表するインターネットの推進者である WIDE プロジェクト（http://www.wide.ad.jp ）が協力し、2003 年 3 月から 9 月末まで、Feel6 の技術を利用した大規模な IPv6 実証実験「Feel6 Farm」を行い、日本の ISP が「IPv6 Ready」であることを世界に対して証明しました。

そして、フリービットが新たに提供する IPv6 接続サービスとしてスタートしたのが「FB Feel6 接続サービス」なのです。』（FreeBit Feel6 Web サイトより）

多くの人に使ってもらい、それだけ早く IPv6 の推進を図っていこうという目的のために作られたサービスがこの Feel6 なのである。

サイトに行けば自動でこのコンピュータで使えるかどうかを診断してくれる。ちなみにコンピュータにグローバルアドレスが割り当てられないと実際には使えない。ル

ータをかませないで接続するかブリッジ接続する、もしくは IPv6 対応のルータにするなどしないとつなぐことは難しい。

実際に提供しているサービスはいくつかあるが特にメールの Push 配信とリモートアクセスは現在の IPv4 では難しい機能だと考えられる。

1.Push 配信とはサーバから配信方法である。たとえばメールなどは自動的にサーバから送られてくるように感じられるが、実際にはある一定の時間毎にこちらからサーバにアクセスして、その結果メールが届いていればもらってくるという形をとっている。ところが Push 配信ではサーバの方から直接データを送ってくるのだ。あまり利点が感いられないかもしれないが、たとえばリアルタイムにメールが送られてくるし、最も重要なのはこちらからサーバにアクセスするという余計な通信を減らすことができる。これは今後たくさんの機器が繋がることによって起きると考えられる、データ量の増大に大変効果的である。

2.リモートアクセスとは外部の端末から自宅のコンピュータなどを操作またファイルのアップロードやダウンロードなどができる機能である。これは確かに IPv4 でも実現可能かもしれないが、接続の簡単さが違う。従来の IPv4 であればルータの設定や NAT の問題など克服しなければならないことが山のようにあったが、これを使えば煩わしい個々の設定はほとんどいらない。リモートアクセスは、IPv6 の特徴の一つである「インターネット上から機器を特定してアクセスができる」という点を活用している。

このように FreeBit では IPv6 の実際目で見える形での利点を示すことによって IPv6 の導入を促進し、さらには IPv6 の持っているネガティブスパイラルを壊そうとしている。

図 4.2.2.1.a　実際に使っている所

4.2.2.2.KDDI 実験

KDDI のインターネットサービス「DION」は、次世代ネットワークへの対応強化の一環として、IPv6 で動作する各種アプリケーションの利用シーンを調査。提供サービス機能の技術・運用検証を行うため、モニターによる実証実験を行った。ネット家電をはじめ、様々な企業が IPv6 導入によるユビキタスサービスへの期待が高まる中、「DION」の本格的なサービス提供を前提にした取り組みに、一段と注目が集まる。

KDDI では、1000 人のモニターを募集し、2003 年 6 月から開始した ADSL による試験サービスを 2004 年 5 月に終了。IPv6 回線の上で様々なアプリケーションを試験的に提供し、今後のコンシューマ向けの商用サービスの検討に入った。

今回の実験は、P2P（ピア・ツー・ピア）と外から家への接続の 2 つの観点で検証され、提供されたアプリケーションは、TV 電話、ネットワークカメラ、セットトップボックス、PDA を利用する 4 つだ。

サーバ不要の P2P 接続で TV 電話やインスタントメッセージ、付箋紙、音声伝言板といったプライベート通信ソフトも提供している。ネットワークカメラは、外出先から PDA で屋内に設置したネットワークカメラを制御して、家の中の様子をチェックすることができる。このように IPv6 のメリットを体感できるようなアプリケーションを提供する実験が、一般利用者向けに行われたことは、ユビキタスサービスの実現を印象付けるものとして業界でも大きな注目を集めた。

今回の実験の被験者は全く IPv6 について知らない人が 3 割、聞いたことがある人が 3 割、従業者が 3 割と幅広い人が参加した。その結果、家の外から宅内のセットトップ

ボックスを呼び出してビデオ予約などが行なえるようにするシステムについて、「8 割以上のユーザが特別な設定なしに利用に成功しており、サポートが必要なのは約 4%に過ぎなかった」ことを報告。IPv6 により NAT 越えなどの面倒な設定が不要になり、ユーザ簡単に利用環境を構築できることが裏付けられたとした。一方で IPv6 ベースのテレビ電話の場合はサポートを必要としたユーザの割合が約 3 割に達したとのことだが、これも内容のほとんどは「通話相手が IPv4 ユーザ場合の、相手側の設定に関するもの」だということで、IPv6 側の設定に関する問い合わせはほとんどなかったという。

この 2 つに実験やサービスにより家庭においては『簡単』『便利』という点をアピールできたのではないかと考える。特に『簡単』に関しては重要で、IPv6 はこれから家庭の特に家電で使われたり、コンピュータを使えない人が使う機器にも組み込まれる。そのときに煩雑な設定があっては使えないし、スイッチをつけたらすぐ使える。まさに懐中電灯と同じくらいの簡単さが必要なのだ。

5．課題

前章の普及の状況から見るに、企業での普及はまずまずであるが家庭ではほとんど普及していない。しかし普及の下地ができはじめているというところまで現在到達しているようだ。しかし家庭においては導入コストの割には受けられるメリットが少なすぎるといった問題もあるだろう。そして、ほとんどの特に家庭環境での仕様を考えているユーザは、現状の IPv4 を使ったサービスにほぼ満足している状況である。では何が普及に向けて必要なのかここでは今後の普及に向けての課題、普及へのロードマップを示していきたいと思う。

5.1.ノウハウの蓄積

企業の場合ノウハウの蓄積がない。ということがネックになるかもしれない。これはどういうことか。IPv6 は出来てから十数年が経ってはいるが、実際に使用されてきた例がまだまだ少ない。よって何か不慮の事故が起きたときにすぐに対処が出来るのか。といったところでなかなか導入に踏み切れないといったところがある。何か新しいシステムを導入するときに必要でない限り、あまり最新の技術を盛り込まないということが決まりのようになっているのだ。

誰もがそこに怖じ気づいていたらことは進まないがこの問題は実験や導入が現在進んでいるので時間とともに解決するというという考えもあるが、それだと消極的すぎるのでほかの案も示せば、第一に多少のリスクを負っても使ってみる価値があると思わせるような、コスト面での利点だったり、機能面だったりを充実させる。これはいきなりは難しいかもしれないので、どちらかといえば時間が解決してくれるという物と似ているかもしれない。もう一つは、簡単な場所での導入だ。たとえば比較的被害が少なくイレ

ギュラーなことが起こりにくい、例えばオープンに公開されない、閉じたネットワークでの導入などがしやすいのではないか。しかもこの場合の利点は対処がしやすいだけではない。開かれたアプリケーションではこちらが IPv6 でも相手が IPv4 ではあまりメリットがないが、閉じた中での運用ならばどちらも IPv6 なので多くの利点が享受できるといったメリットもあるのだ。例えばガリバーでは、朝礼を行うガリバー事業本部（千葉県浦安市新浦安）から、衛星へ映像を送るスカパーの放送センター（東京都江東区青海）の間で IPv6 を用いる。さらに高層ビルに囲まれてスカパーを受信できないガリバーの稲毛海岸店（千葉市）へ、スカパーの放送センターから地上回線で映像を送るのにも IPv6 を用いるといったことをしている。

このような小さいところからの導入を続けていくことによって、大規模な実験や導入事例だけではわからなかった問題点が見つかり、それがノウハウの蓄積に繋がっていくのではないか。

5.2.安全面の問題

安全面の面ではプライベートアドレスがなくなることにより内部のコンピュータをピンポイントで継続的に攻撃出来るといった点がある。さらに IPSec の標準装備だけでは十分ではないといった問題点なども抱えている。コンピュータ単体を認識できるといった利点がそのまま裏返しでデメリットになるのだ。

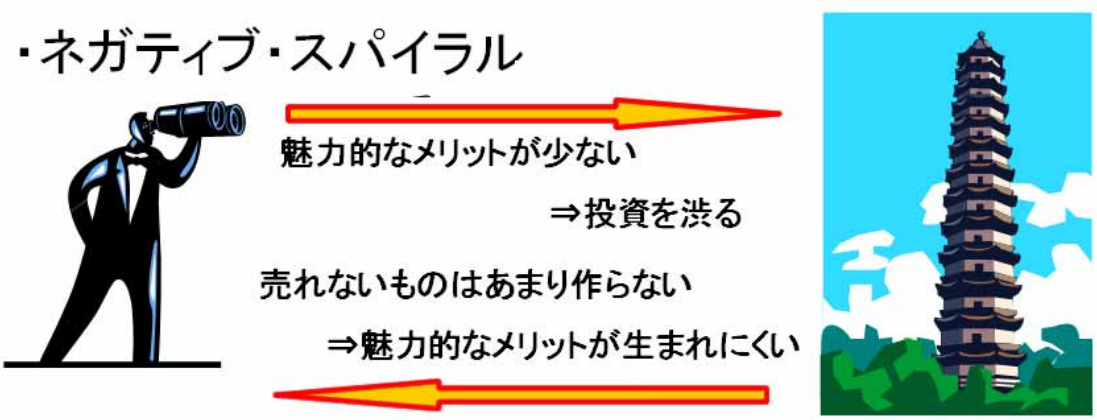
そのうえ安全面の問題は IPv6 今以上に大きな問題にあると考えられる。セキュリティの不完全はほとんどの物が通信可能になるといった状態において、ほとんどの物が望まれない外部のものによって、変更、操作などが出来てしまうからだ

これに対応するには、最近の小型 IPv6 ルータでも実装されているステートフル・パケット・インスペクション型のダイナミック・フィルタの使用がある。これにより、NAPT 同等、もしくはそれ以上のセキュリティを確保することができる。高機能な高価なファイヤウォールも IPv6 対応を進めている。

5.3.キラーアプリ、サービスの登場

これも普及においては大きな問題だ。鶏と卵の話があるように、IPv6 の普及においてもどちらが先かという問題がある。4 章で出てきたネガティブスパイラルというのがそうである、魅力的なアプリがなければ投資を渋るし、売れなければ作る側が研究をしなくなる。といった物である。企業でも家庭でも利点をいい形で示していけていると思うのでこの問題はあまり考えなくてもいいのかもしれないが、これからも研究やアピールに力を入れていかないとまだまだ新たに IPv6 を導入していこうという流れを作り出せないかもしれない。

このアプリケーションの開発には IPv6 普及･高度化推進委員会なども力を入れていて、2003 年から毎年 IPv6 アプリコンテストを行っている。参加も簡単で一般人の参加も出来き、アイディアペーパーの枚数も A4 用紙 2 枚までにまとめて書くので、大量の文章が必要だったり研究が必ずしも必要ではないというところも参加のボーダーが低いところである。このように広く一般からの考えも積極的に取り入れようというところからもアプリケーションの力がいかに必要かということが伺える。



5.4.普及に向けての必要性

ここでは、今までの利点、問題点などをふまえながらどのように普及が進んでいくかを考える。まず導入の必要性について家庭の場合と企業の場合についてまとめていきたいと思う。

5.4.1.企業においての現状での必要性

すでに一部の企業では IPv6 対応環境の導入が始まっているが、残念ながら IPv6 でないとどうしても実現できないというインパクトの強い導入事例はまだ見当たらないようだ。

それよりも、現在の IPv4 環境の構築で苦労してきた部分を、IPv6 ならもっと簡単に実現できるという、地道ではあるが堅実な側面からの IPv6 の導入が進んでいる。

たとえば、企業同士の合併や、1 つのプロジェクトに複数企業が参加して 1 つのネットワークを構築するといった場合、それぞれの企業や部門で NAT が使われていると、IP アドレスの重複問題で手間取るケースがある。しかし、グローバル IP アドレスをもっと手軽に利用できる環境が整っているならこうした混乱は起こらないはずだ。また、インターネットに接続する組織が増えると、そこに到達するための経路情報も増加することになり、ルータが経路情報を検索するときの負荷も大きくなる。

さらに、業務の都合上、取引先や提携先からも社内 LAN にアクセスできるようにしたいとか、保険の外交員のような立場のスタッフにも社内 LAN へのアクセスを認めたいといった場合、セキュア通信のための設定をもっと簡単にできる環境が必要になってくる。

もう一つはやはりコスト面だろう。まだまだ機器の価格自体は高い物が多いが、設定や保守の便利さ、導入時の時間、手間など総合的に考えてみると、IPv6 二部があるのではないか。実際に共立メンテナンスの事例でも億単位の通信費が 2．3 千万になっている。機器個々の値段の高さは数年でペイ出来るであろう。

5.4.2.家庭での現状での必要性

現時点では、従来の IPv4 を使い続けていても、大半の個人ユーザがすぐに困るというケースはまだ見当たらないが、NAT（Network Address Translator）を使ってプライベート IP アドレスをグローバル IP アドレスに変換して通信している場合、たとえばインターネット上の対戦ゲームなどを楽しむことができない。また、グローバル IP アドレスを割り当てている ISP の中には、セキュリティ上の問題からユーザ同士の通信に制限を加えているケースもある。このような状況で困っているというユーザの立場で考えると、NAT を使わずにもっと手軽にグローバル IP アドレスを利用したいというニーズが出てくるし、グローバル IP アドレスを使った場合でもセキュリティ面で不安にならないようにしてほしいだろう。

さらに今後、家電製品や携帯情報端末（モバイル機器）がインターネットにつながって情報家電（情報端末）となった場合、すべての端末間で双方向なアクセスを可能にするには、やはりグローバル IP アドレスが必要になるし、マルチメディアコンテンツの急増で、インターネット上のトラフィックが急増している今、高品質な通信をもっと手軽に実現するための仕組みも必要になる。

5.5.普及に向けてのシナリオ

企業については明確な利点やコスト計算、導入目的などがしっかりしているので、導入はこれから進んでいくだろうと思われる。家庭での普及シナリオはどのような段階が考えられるだろうか？時間とともに IPv4 と IPv6 の利用が 5:5 になるまでのシナリオを考えてみたいと思う。はじめは

●ISP、ネットワークが対応しているか？
●ルータが対応しているか
●PC が対応しているか
という軸で考えてみる。

時間 1：現在の段階

●現状では一般家庭における IPv6 機器の普及はほぼ無い。
●IPv6 ネットワークも一般家庭用は登場したものの利用はほとんど無い。
●PC は Windows XP SP1 から対応している。

この状況から考えると、v6 ネットワークに接続できる世帯はかなり限られていると考えられる。また現在の家庭内のネットワークの状況はモデムを使ったダイヤルアップ接続に PC やゲーム機などの NonPC 機器の接続やルータを使った常時接続の家庭内 LAN などが考えられる。

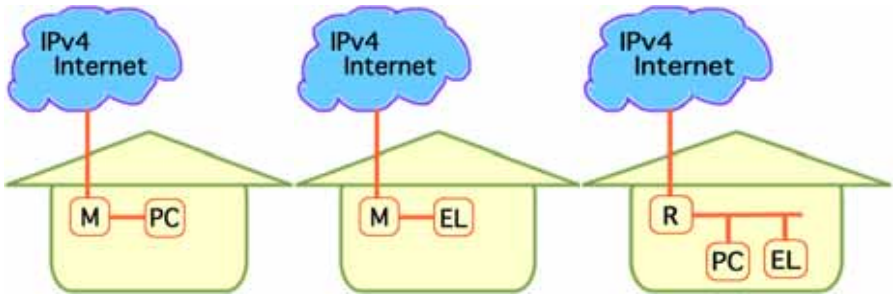


図 5.5.a　現在の状況

*M=モデム　EL=家電製品

時間 2：最初の一歩

●ルータを買ったらデュアルスタック対応製品だった。

●PC を買ったらデュアルスタック対応だった。

まだまだ、環境はそろってはいないが対応製品は登場し始めている。メーカーは来るべき v6 ネットワークに対応した製品を出し始めている。後も家庭におけるコンピュータの台数は一人一台に近づいていくと考えられていて、ネットワークに繋ぐにはルータが必要になってくる。そこで購入したルータや PC が対応していて（購入者が意識するかしないかに関わらず）家庭に環境がそろう。ということが考えられる。ただしここでは必ずしも IPv6 が使われるということは示してはいない。

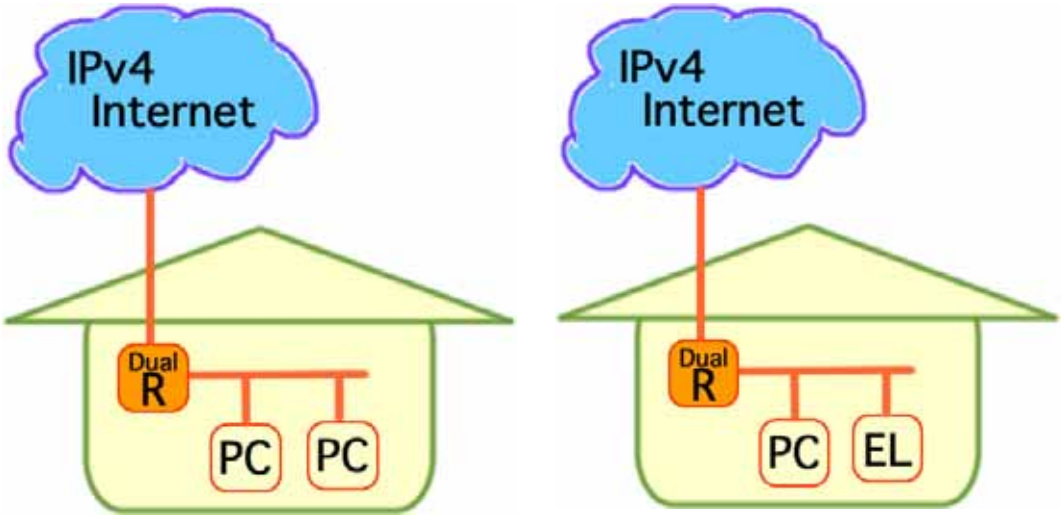


図 5.5.b　はじめの一歩

時間 3：サービス開始

●IPv6 対応家電などが出始める

●ISP も一般的にデュアルスタックに対応

●IPv6 しか使えない製品も出てくる

下地として機器がそろい始める家庭が少しずつ増えてくるころに IPv6 のサービスが開始される。（一部の家電や IP 電話など）

基本的な機器がそろっている家庭が増えているので家電の導入がしやすい。

使っている家庭が増えてくれば、サービスにあわせてルータや PC、プロバイダ契約の変更を検討する家庭も出てくる。

この時期の v4 と v6 の比率は 9：1 程であるとの試算がある。

この流れは以下のような道筋で考えた

意識しないで下地が揃っていく

↓

サービスの開始がしやすい

↓

サービスを使う家庭が増える

↓

新たなサービス＆サービスの向上

↓

下地の揃っていなかった家庭でも購入が検討される

↓

更なる新しいサービスなどが登場

というような段階を経て IPv4 と IPv6 の利用状況が 5：5 の段階まで進むと考えられます。しかしまだ当分は v4 のネットワークが使われなくなるということは考えられていない。

6.終わりに～繋がった先にある世界は

ここまで研究してきて、IPv6 という言葉は浸透していない物のその足音は年々大きくなっているという感じであった。家庭での実用はまだもう少し先のようだが研究が進みルータなど対応製品や IPv6 にふれることの出来るサービスや ISP の対応など下地の面では完成しつつある。これから IPv6 を使ったどのようなサービスが考えられるのだろうか。現状ではやはりその数を活かして様々な物に IP を振り分けるという観点から家庭の機器を外からコントロールするなどの利用方法がよく聞かれる。ここではどのようなサービス出てくるかを考えてみたいと思う、

私もやはりその数の点に注目して考えてみたが、いろいろな物に取り付けてデータをもらうのではなくそれを集めることを考えてみたい。例えば人が動けばそれだけでかなりの情報が集められる。例えば天候や気温、人の量や、心拍数だって大切な情報になるだろう。ここでは究極形かもしれない人間のデータを考えてみた。人間はいってみればセンサーの固まりのような存在である。このセンサーが 1 万や 2 万ではなく 1 億以上も日本中にあるのだ。例えば気温のデータがとれればかなり詳しい気温分布のデータがとれることだろう。

しかし、いきなり人間に発信器気を取り付けるというのは、実際にロンドンなどで事例がある物のなかなか抵抗があるし、そもそも倫理的に問題があるようにも感じる。なのでここでは次に多いと感じる『車』をとりあげてみたいと思う。

15 年度の統計調査では日本を走る車（大型、特殊、二輪など含む）は 7739 万台にもなる。これはやく 70m間隔で日本全土に車を配置できる計算になる。しかも日本全国人のいるところには必ずといってある物だといえる。これをセンサーとして使えるのではないか。さっきの人の例のように気温の分布もはかることも出来るし、ワイパーが動いている車の位置がわかれば、かなり正確な降雨地域の特定が出来る。しかしその利点はそれだけではない。

我が国の渋滞による損失は年間で 38 億時間、金額に直すと 12 兆円物損失がある。これらも IPv6 を使った自動車ネットワーク ITS（Intelligent Transport System）で解決していこうという物である。現在の VICS を使った混雑状況の把握は出発してから何時間も先につく目的地付近の混雑情報を知るにはあまり向かない。そこで毎日走る車の情報を一台ずつ取り出し、今動いている車は雨の休日のこの時間、どこへ向かうことが多いのかという情報を集め、しかもリアルタイムの位置情報とあわせれば、現在の詳しい情報とこの先何時間後の予測まで簡単にできるであろう。情報を集めてフィードバックとしてその情報の提供者に利益を還元する仕組みがここにはある。これが全国の車に標準装備となればそうとの経済効果を生み出せると思う。

またこの ITS はそれだけではなく、自らの車体情報から事故や故障情報を自動的に送信して適切な対処を受けたり、盗難車の情報を集めたり ETC と組み合わせていろいろな課金システムにも使われたりさまざまな可能性を秘めている。

ここまではきていない物のアメリカではテレマティクス（自動車をネットワークにつな

げる）として GM の「オンスター」などで緊急情報を発信するものがあるし、日本にも「HELPNET」というものが登場しているし、名古屋ではデンソーとの協力により県内の 1500 台のタクシーの情報を集めることもはじめている。

しかしこの完全な普及にはまだまだ前章で述べた課題のほかにも、法律や自動車団体との兼ね合いや個人情報の観点からもクリアすべき問題は多いと思う。特に位置情報はどこにいるかを知られてしまうといった点から快く思われないだろうし、すべての車に取り付けるとなると開発が完了してから、すべての車が入れ替わるまで長い時間がかかってしまう。

だがこのような問題を少しずつ乗り越えていくことによって、今一番の IPv6 先進国である日本がはじめの一歩を切り出し世界に向けて実用の手本を示し、より良い暮らしを提供していけるのではないだろうか。

《注釈》

1.はじめに

ADSL: Asymmetric Digital Subscriber Line

「加入者線」と一般に呼ばれる従来の電話回線（メタルケーブル）を利用し、専用のモデム経由で高速なデータ伝送を可能にしたデジタル技術（xDSL）の 1 つ。ADSL は、xDSL 技術のうち現在もっとも普及している方式で、データ伝送の向き（ユーザーから見て発信の「上り」と受信の「下り」）の速度の違いが「非対称（Asymmetric）」になる。1 対の加入者線で最大上り 512kbps、下り 8Mbps の速度で通信が可能。xDSL にはほかにも、複数対の加入者線を使う「HDSL」や、ADSL の超高速版の「VDSL」などもある。

FTTH: Fiber To The Home

電話局から各家庭までの加入者線を結ぶアクセス網を光ファイバ化し、高速な通信環境を構築する計画。「Fiber To The Home（ファイバ・トゥ・ザ・ホーム）」の略。1986 年に米国の地域電話会社サザン・ベルがフロリダ州で実験を行なったのが始まりで、日本では 1997 年に横浜市戸塚区で試験導入が開始されている。

2.IP とは何か

LAN: Local Area Network

同一フロア、同一のビルないしは近隣のビル内などにあるコンピュータ同士を、Ethernet などの比較的高速なデータ転送能力を持つ方法で接続したネットワーク。

ギガビットイーサ: Gigabit Ether

1000Mbps（＝1Gbit/sec）という高速ネットワークを実現する Ethernet の最新規格。

ノード: Node

ネットワークに接続されている端末やネットワーク機器のこと。

RFC: Request for Comments

インターネットに関する技術情報や仕様、運用規則などを定める文書。現在は IETF（Internet Engineering Task Force）が管理する。

IETF: Internet Engineering Task Force

Internet 上で開発されるさまざまな新しい技術の標準化を促進するために設立されたコンソシアム。IETF が発行するドキュメントは RFC（Requests For Comment）として知られる。

IANA: Internet Assigned Number Authority

インターネット上で利用されるアドレス資源(IP アドレス、ドメイン名、プロトコル番号など)の標準化や割り当てを行なっていた組織。1998 年 10 月、インターネット資源の管理・調整を行なう国際的な非営利法人 ICANN が設立されたため、IANA が行なっていた各種資源の管理は ICANN に移管された。現在では、IANA は ICANN における資源管理・調整機能の名称として使われている。

CIDR: Classless Inter-Domain Routing

IP アドレスの枯渇を防ぐため、既存のクラス分けを一時的に無視して経路を選択する仕組み

NAT: Network Address Translation

インターネットに接続された企業などで、一つのグローバルな IP アドレスを複数のコンピュータで共有する技術。組織内でのみ通用する IP アドレス(ローカルアドレス)と、インターネット上のアドレス(グローバルアドレス)を透過的に相互変換することにより実現される。最近不足がちなグローバル IP アドレスを節約できるが、一部のアプリケーションソフトが正常に動作しなくなるなどの制約がある。

ゲートウェイ: Gateway

ネットワーク上で、媒体やプロトコルが異なるデータを相互に変換して通信を可能にする機器。OSI 参照モデルの全階層を認識し、通信媒体や伝送方式の違いを吸収して異機種間の接続を可能とする。

3.IPv6 とは

ST‐2: Internet Stream Protocol Version 2

インターネット・ストリーム・プロトコル・バージョン 2。ST2 は、資源予約（帯域など）のためのプロトコルです。ST2 プロトコルは、IP バージョン 5 として定義されており（このため IPv4 を後継するのは IPv5 ではなく IPv6 になった)、現状のインターネット上で使っている IP バージョン 4（IPv4）とは異なります。このため、IPv4 と相互接続して、使うことはできません。資源予約は、送信者が行います。ルータでは、ハード・ステートによって、資源予約状態を保持します。これは、一度制御メッセージで資源予約がされると、資源予約解放メッセージが明示的に届くまで、状態を保持するものです。このプロトコルは、RFC 1819 として規定されています。

ICANN: Internet Corporation for Assigned Names and Numbers
　インターネット上で利用されるアドレス資源(IP アドレス、ドメイン名、ポート番号など)の標準化や割り当てを行なう組織。IANA の後継にあたる民間の非営利法人である。

NSF: National Science Foundation
　全米科学財団

アルゴリズム: Algorithm
　処理手順あるいは演算方式のこと。例えば、「暗号化のアルゴリズム」と言う場合は、暗号化するという問題を解決するための「処理手順」のことを指します。また、画像圧縮における「MPEG-2 のアルゴリズム」と言う場合は、MPEG-2 を実現するための「符号化（圧縮）演算方式」ということになります。したがってアルゴリズムとは、ある問題を解決する/実現するための一連の処理手順や演算方式を意味していると言えます。

POP3: Post Office Protocol 3
　メールサーバから電子メールを取得するプロトコルである POP のバージョン 3 のことです。POP には、バージョン 1 や 2 もありましたが、それらは現在ではほとんど使われておらず、また、POP3 との互換性もありません。そのため、現在では、単に POP といえば、POP3 のことを指すようになっています。
　　POP3 は、最初の仕様からいくつかの改良が行われたのちに現在の仕様になりました。POP3 でのユーザの認証は、ユーザ名とパスワードによって行われますが、認証コマンドについては RFC 1734 として標準化されています。また、メールサーバからメールを受信するときのプロトコルは、RFC 1939（STD53）に標準仕様として記述されています。

ESP: Encapsulating Security Payload
　暗号ペイロード和訳される ESP は IP パケットを暗号化するが、オプションで認証情報を付加することもできる。ただし、AH は IP ヘッダも含めて IP パケットの全体を認証できるのに対して、 ESP の認証情報では、IP ヘッダを認証することができない。

ISP: Internet Service　Provider
　インターネット接続業者。電話回線や ISDN 回線、データ通信専用回線などを通じて、顧客である企業や家庭のコンピュータをインターネットに接続するのが主な業務。

AppleTalk:アップルトーク

Apple 社の Mac OS に標準搭載されているネットワーク機能。また、AppleTalk のネットワーク機能を実現するプロトコル群の総称。AppleTalk ではファイル共有やプリンタ共有などのサービスが提供される。

Solaris:ソラリス

SunSoft 社(Sun Microsystems 社の子会社)が開発・販売している UNIX 系 OS。Sun Microsystems 社製のコンピュータで動作するほか、PC/AT 互換機で動作するバージョンもある。

TLA: Top Level Aggregator

文字通り最上位で経路を集約する組織に割り当てられます。具体的には、大手のプロバイダだと考えればよいでしょう。最初の 3 ビットは使えないので、TLA の実際の長さは 13 ビットです。10 進数に直すと、8,192 個の TLA が存在できることになります。

4.IPv6 の現状

e-Japan 重点計画

e-Japan 計画とは 2001 年 1 月 22 日に我が国は、すべての国民が情報通信技術(IT)を積極的に活用し、その恩恵を最大限に享受できる知識創発型社会の実現に向け、早急に革命的かつ現実的な対応を行わなければならない。市場原理に基づき民間が最大限に活力を発揮できる環境を整備し、5 年以内に世界最先端の IT 国家となることを目指す。と発表したもの。重点計画とは 3 月により具体的に政府が迅速かつ重点的に実施すべき施策の全容を明らかにするものである。

デュアルスタック: Dual Stack

2 つのプロトコル群のこと。例えば、IPv4 と IPv6 の 2 つのプロトコル群が存在する場合、両方のプロトコル群を備えた装置を IPv4/IPv6 のデュアル・スタックに対応したノード（ホストあるいはルータ）と呼びます。

IC タグ: IC tag

物体の識別に利用される微小な無線 IC チップ。自身の識別コードなどの情報が記録されており、電波を使って管理システムと情報を送受信する能力をもつ。

トレーサビリティ:Trace Ability

トレーサビリティとは、主に品質マネジメントシステムにおいて使用される定義です。ISO9000:2000 においては「考慮の対象となっているものの履歴、適用又は所在を適用できること」と定義されており、具体的には「処理の履歴」「材料及び部品の源」などが挙げられています。

ミドルウェア: middleware

OS 上で動作し、アプリケーションソフトに対して OS よりも高度で具体的な機能を提供するソフトウェア。OS とアプリケーションソフトの中間的な性格を持っている。

RFID: Radio Frequency Identification

微小な無線チップにより人やモノを識別・管理する仕組み。流通業界でバーコードに代わる商品識別･管理技術として研究が進められてきたが､それに留まらず社会の IT 化･自動化を推進する上での基盤技術として注目が高まっている。

グローバルアドレス:Global Address

インターネットに接続された機器に一意に割り当てられた IP アドレス。インターネットの中での住所にあたり、インターネット上で通信を行なうためには必ず必要である。IANA が一元的に管理しており、各国の NIC によって各組織に割り当てられる。

プライベートアドレス:Private Address

組織内のネットワークに接続された機器に一意に割り当てられた IP アドレス。NIC に申請を行わなくても組織内で自由に割り当てることができるが、インターネット上での一意性は保証されないため、そのままではインターネットを通じて通信を行なうことはできない。プライベートアドレスしか持たない機器がインターネットで通信を行なうには、グローバルアドレスを割り当てられた機器に NAT や IP マスカレード、プロキシなどの手段によって中継してもらう必要がある。

P2P: Peer to Peer

コンピュータ同士を直接接続して、お互いの持つ情報をやり取りする通信形式。Napstar では、ファイル検索は Napstar サーバで行い、その後 P2P 接続で PC 同士を接続する形式を取っている。

5.課題

NAPT: Network Address Port Translation(IP マスカレード)

インターネットに接続された企業などで、一つのグローバルな IP アドレスを複数のコンピュータで共有する技術。組織内でのみ通用する IP アドレス(ローカルアドレス)と、インターネット上のアドレス(グローバルアドレス)を透過的に相互変換することにより実現される。

6.終わりに

ITS: Intelligent Transport Systems

情報技術を用いて人と車両と道路を結び、交通事故や渋滞などの道路交通問題の解決をはかる新しい交通システム。

VICS: Vehicle Information and Communication System

FM 多重放送や道路上の発信機から受信した交通情報を図形・文字で表示するシステムのこと。VICS センターで編集・処理された渋滞や交通規制などの道路交通情報をリアルタイムに送信し、カーナビゲーションシステムに用意されている地図の上に重ね書きして表示する。

ETC: Electronic　Toll　Collection

料道路の料金所などに設置されたアンテナと自動車に搭載した端末(車載器)で通信を行い、自動車を止めずに有料道路の料金支払いなどを処理するシステム。料金の徴収に必要なコストを削減し、料金所で頻発する渋滞を緩和する目的で開発された。

テレマティクス: telematics

自動車などの移動体に通信システムを組み合わせて、リアルタイムに情報サービスを提供すること。Telecommunication(通信)と Informatics(情報科学)を組み合わせた造語だが、元々はドイツ語に由来するとの説もある。

《参考文献・URL》

〈書籍〉

萩野純一郎『IPv6 ネットワークプログラミング（ASCI 2003 年 2 月）
小島郁夫　『見る見るわかる IPv6』（ビジネス社 2002 年 4 月）
砂原秀樹（監修）増田康人　長橋賢吾　有賀征爾（著）
『使って学ぶ IPv6』（ASCII 2002 年 4 月）
江崎浩　『IPv6 教科書』（IDG ジャパン 2002 年 9 月）
IPv6 普及・高度化推進協議会 移行 WG
『IPv6 移行ガイドライン総集編』（2004 年 6 月）
後藤健　森弘好　本多美雄　他
『次世代通信のしくみ』（毎日コミュニケーションズ 2002 年 4 月）

〈URL〉

『IPv6 Style』2005 年 12 月 22 日　http://www.ipv6style.jp/jp/index.shtml
『IPv6 普及・高度化推進委員会』2005 年 12 月 22 日
http://www.v6pc.jp/jp/index.phtml
『Panasonic』2005 年 12 月 22 日　http://panasonic.biz/
『FreeBit-Feel6』2005 年 12 月 22 日　http://start.feel6.jp/index.html
『@IT』2005 年 12 月 22 日　http://www.atmarkit.co.jp/index.html
『MY COM PC WEB』2005 年 12 月 22 日　http://pcweb.mycom.co.jp/
『キーマンズネット』2005 年 12 月 22 日　http://www.keyman.or.jp/
『統計局』2005 年 12 月 22 日　http://www.stat.go.jp/index.htm
『アスキーデジタル用語辞典』2005 年 12 月 22 日　http://yougo.ascii24.com/
『デジタル用語辞典 e-Words』2005 年 12 月 22 日　http://e-words.jp/
『RBB Today』2005 年 12 月 22 日　http://www.rbbtoday.com/
『人力検索はてな』2005 年 12 月 22 日　http://www.hatena.ne.jp/q