

# IPv4 アドレスの枯渇問題と IPv6 利用の推進

## *IPv4 Address Exhaustion and IPv6 Promotion*

石島 悌\* 平松 初珠\*

*Dai Ishijima Hatsumi Hiramatsu*

(2010年6月24日 受理)

キーワード：IP アドレス, IPv4, 枯渇, NAT, IPv6, パケットフィルタ

### 1. はじめに

インターネットはさまざまな社会活動になくてはならない社会基盤、いわゆる「情報インフラ」として認識されている。まるで、蛇口をひねれば水が出るように、あるいはコンセントにプラグをさせば電気が使えるのと同様に、インターネットにアクセスすることによって、情報を収集したり発信することが可能となっている。また、インターネットにアクセスする手段も、従来より用いられてきたパソコンだけでなく、携帯電話やスマートフォン、携帯ゲーム機あるいはデジタル放送対応テレビなど、多様化が進んでいる。

黎明期においては、限られた数の学術研究機関からしか利用できなかったインターネットは、その創始者たちの予想をはるかに越えた発展をとげている。その発展とは、単に利用者が増えただけにはとどまらない。インターネット上で利用可能なサービスも多様化が進展している。

総務省が調査した利用統計情報<sup>1)</sup>によると、日本国内におけるインターネットの普及は、1990年代に大学や企業での利用が進み、そして、2000年代前半には、家庭や小規模事業所へと広がっていった。現在では、インターネットを単に利用しているかどうかという普及の視点ではなく、サービスをどのように活用しているかに注目が集まっている状況である。

インターネットは、この20年ほどで、社会のすみずみにまで浸透していったが、その急激な広がりと同

時に、問題点もいくつか指摘されるようになってきた。その一つが、インターネットに接続できるコンピュータの台数に限りがあり、その限界が露呈しはじめていることである。この問題は、IPv4 アドレス枯渇問題<sup>2)</sup>として、主にサービス提供者や通信事業者の間で注目を集めている。

本稿では、まずこの「IPv4 アドレス枯渇問題」について説明する。そしてその解決策の一つとして、現在広く使われているネットワークアドレス変換<sup>3)</sup> (Network Address Translation: NAT) について説明し、これだけでは十分な解決にならないことを述べる。次に、根本的な IPv4 アドレス枯渇問題の解決策として有望視されている IPv6<sup>4,5,6)</sup> について説明する。また、そのように有望視されながら、実際には普及が進んでいない現状とその原因について解説する。最後に、当研究所における IPv6 の利用の事例をあげ、府内の事業者、特にインターネットを積極的に活用して情報発信を行っている中小事業者にとって IPv6 利用時の指針となるものを示す。

### 2. IPv4 アドレス枯渇問題

先に述べたように、インターネットの黎明期においては、限られた台数のコンピュータしか接続されていなかった。そのため、十分な台数のコンピュータを接続できると考えられていた当時の予想が覆ってしまっているのが現状である。

インターネットで利用されている通信規約(プロトコル)であるインターネット・プロトコル (Internet

\* 情報電子部 制御情報系

Protocol; IP) においては、インターネットに接続するコンピュータには一意に決まる番号を付与することになっている。この番号のことを IP アドレスと呼んでいる。

現在、広く用いられているプロトコルである IPv4<sup>7)</sup> (Internet Protocol version 4) においては、この IP アドレスが  $2^{32}$  に限られている。これは、およそ 40 億である ( $2^{32}=2^2 \times (2^{10})^3 \doteq 2^2 \times (10^3)^3 \doteq 40$  億)。

インターネットの黎明期では、インターネット接続数どころかコンピュータそのものの台数がこれを超えるほどにはならないと考えられていた。しかし、その後の情報技術の進展はとどまるところを知らず、地球上には、はるかに多くのコンピュータが存在する。このおよそ 40 億という数字は、地球上の人口よりも小さな数である。日本のように、一人がパソコン、携帯電話など複数台のコンピュータを持ち、それらがインターネットに接続されているという社会には、もはや対応できないといって過言ではない。

以上のように、インターネットの接続に必須となる IP アドレスの数が足りなくなっていることが IPv4 アドレス枯渇問題である。

現在の予想では、2011 年秋ごろに新しく IPv4 アドレスを割り当てることができなくなるとの統計上の予測が出されている<sup>8)</sup>。図 1 にこれまでの IPv4 アドレスの消費動向とおおよその IPv4 アドレスの枯渇時期の予測を示す<sup>9)</sup>。この図では、右肩下がりの線が未使用の IPv4 アドレスの数を示している。この線が x 軸に交差するときが IPv4 アドレスが枯渇するときを示しており、それは 2011 年後半である。また、図 2 に IPv4 アドレスが枯渇する日付を予測している「IPv4 アドレス枯渇時計」を示す<sup>10)</sup>。現在の IPv4 が全く使えなくなるわけではないが、何かしらの対策を講じなければ、新たにインターネットを利用する際に制限を設ける必要に迫られるだろう。

なお、ほぼ同時期 (2011 年 7 月) に、現在広く利用されている地上波アナログ TV 放送は終了し、地上波による TV 放送はデジタル化されることになっている<sup>11)</sup>。TV 放送を受信するためには、デジタル放送に対応した機器の導入が必須であり、アナログ放送にしか対応していない機器では、TV 放送の受信が不可能となる。

その一方で、IPv4 アドレスが新たに割り当てられなくなるからといって、現在使用しているコンピュータでインターネットの利用が不可能となるということはない。

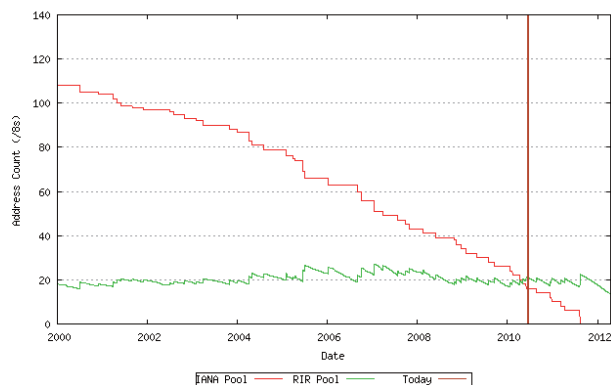


図 1 残り IPv4 アドレスの予測



図 2 IPv4 枯渇時計

### 3. NAT による IPv4 の有効利用

#### 3.1 NAT とは

限られた IPv4 アドレスを有効活用する手段として、一つの IPv4 アドレスを複数のコンピュータで共用する方法が現在幅広く用いられている。この方法は NAT あるいは IP マスカレード (IP masquerade) と呼ばれている。

NAT では、インターネットとの接続点にのみ、インターネットで一意に決められた IPv4 アドレスを割り当てる。この IPv4 アドレスのことをグローバル IP アドレスと呼ぶ。それ以外のコンピュータには、組織内で自由に割り当てることができる IPv4 アドレスを付与する。こちらの IPv4 アドレスをプライベート IP アドレスと呼ぶ。

NAT を用いることによって、インターネット接続に必要な IP アドレスの数を、実際に使用するコンピュータの数より少なくすることが可能となる。このことにより、NAT はグローバル IP アドレスの浪費を減らす非常に有効な手段として認識されている。

NAT は、インターネットにおける通信の大部分が非対称であることを利用して設計されている。ここでの非対称性とは、通信を行うコンピュータが対等な関

係であるピア・ツー・ピア (Peer to Peer: P2P) 型ではなく、サービスを提供するサーバと提供されるクライアントで構成されるクライアント・サーバ型であるという意味である。

クライアント・サーバ型の通信では、クライアントからの要求によって通信が開始される。NAT を介した通信においては、この通信開始時にアドレス変換表が作成される。アドレス変換表には、通信を開始したコンピュータのプライベート IP アドレスと通信相手のグローバル IP アドレスなどの対応関係が記録される。アドレス変換表は通信の終了時か一定時間が経過した後で廃棄される。

NAT における非対称性はセキュリティの確保にも使われている。NAT を介した通信では、通信は NAT の内側にあるコンピュータからしか原則的に開始することはできない。このことは、インターネットから組織内部への通信を破棄していることとなり、結果として NAT はネットワークにおけるファイアウォール (防火壁) の役割を果たしている。

その一方で、NAT による通信の非対称性が問題となることもある。NAT の内側にはサーバを設置することが困難であり、H.323 規格などに準拠したテレビ会議システムなども NAT を超えて利用できないことがある。もちろん、P2P 型のサービスも、通信経路上に NAT が存在すると、たちまち利用が困難となる。

3.2 NAT の限界

NAT は IPv4 アドレスの有効活用という面だけでなく、セキュリティの確保にも役立つので広く使われている。小規模事業者や一般家庭におけるブロードバンド回線の接続点でも、ADSL モデムや光回線の終端装置と併用されていることが多く、一般的にはブロードバンドルータとして市販されている。

以上の点を踏まえ、IPv4 アドレスをさらに効率的に利用する手段として、ネットワーク利用者ごとに NAT を配置するのではなく、通信事業者側で NAT を用意する方法が検討されている。この方法はキャリアグレード NAT (Carrier Grade NAT; CGN) あるいは大規模 NAT (Large Scale NAT; LSN) と呼ばれている。

このように、通信事業者が NAT を用意することは、IPv4 アドレスの効率的利用につながる。その一方で、IPv4 アドレスを大幅に節約するために大規模な NAT を運用することは難しいといわれている。

NAT では、通信時にアドレス変換表が作成されるが、この変換表の大きさには上限がある。この上限に達した場合、通信が行えなくなる。

近年、高速・大容量化されたインターネットを使って、さまざまなサービスが実用化されている。これらのサービスは、短時間により多くのデータをやりとりするために、通信処理の並列化が行われている。たとえば、地図情報を提供するサービスであれば、画面に表示する情報を一つの画像データとしてやりとりするのではなく、升目状に区切ってそれらを同時並行で送信する。

このような処理は NAT にとってはより負荷のかかるものとなる。NAT で一つの通信ごとに一つのアドレス変換表が消費されるからである。アドレス変換表の大きさは NAT によって異なるが、小規模事業者や一般家庭で用いられるような比較的安価な装置では数百程度である。NAT の変換表の上限は、NAT によって集約できるコンピュータの数の上限に関係している。仮に、一台のコンピュータによって 50 の通信処理が同時に行われるのであれば、アドレス変換表の上限が 1000 の場合、接続できるコンピュータは 20 台に制限される。

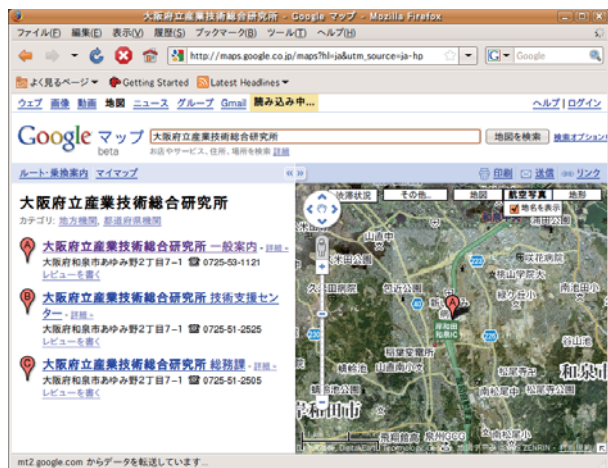


図 3 (a) 正しく画面表示されている地図情報サイト

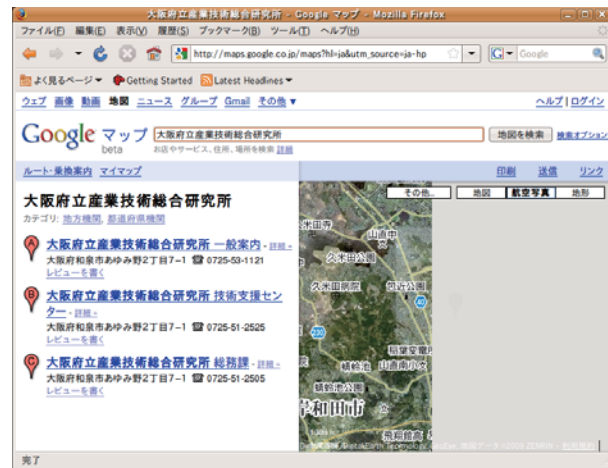


図 3 (b) NAT 変換表の上限を超えると表示が乱れる



図3にアドレス変換表の上限が問題にならない場合と、問題になる場合の地図情報サイト (Google Maps) の表示例を示す。図3(a)では、並列処理されている通信が問題なく行われ、画面に表示される情報に欠落はない。一方、図3(b)は、NATのアドレス変換表の大きさを20に制約した場合で、地図の右側の情報が欠落して表示されない。

以上のようなNATの問題点を避けるために、大規模NATでは、IPv4アドレスの集約度を下げたり、あるいはNATの性能を向上させるなどの対応が必要となる。また、P2P型のサービスを使いたい利用者にはNATによる集約を行わないなどの配慮が必要となる。

## 4. IPv6 とそのアドレス空間

コンピュータを識別するための番号が足りないのであれば、その番号、いいかえるとその桁数を増やせばよいことは容易に想像できることである。

コンピュータとは直接関係しないが、このような事例が実際に行われたことがある。1999年に、大阪市域(市外局番が06の地域)において、電話番号逼迫対策(電話番号が加入者増に追いつかなくなる現象への対策)として、市内局番の4桁化が行われた。このときは同時に加入者が増加してきた携帯電話ならびにPHSの電話番号も10桁から11桁に増やされた。同様の措置は、割り当て可能な電話番号が加入者増に追いつかなくなった地域でも行われている。

### 4.1 IPv6 アドレスとそのアドレス空間

インターネットにおいても、求められている対策は根本的には同じである。ただし、インターネットにおいては、「現状からは予測できないような爆発的な利用者の増加」を考慮に入れるべきとの配慮から、もっと劇的なアドレス空間の拡張が必要であると考えられた。そして、その考えに基づいて新しい通信規約であるIPv6(Internet Protocol version 6)の規格化が1990年代に始まった。

IPv6では、コンピュータに割り当てるアドレスは128ビット幅と規定された。これは、IPv4の4倍の幅である。なお、幅が4倍となることはアドレス空間が4倍となること、すなわちIPアドレスが約40億から約160億になることを意味しているのではない。アドレス幅が4倍となることは桁数が4倍となることを意味している。

128ビットを10進数に換算すると、 $2^{128} = 2^8 \times (2^{10})^{12} \approx 2^8 \times (10^3)^{12} \approx 300 \times 10^{36}$ となる。IPv6を使用すれば、天文学的な数のコンピュータをインターネットに接続す

ることが可能となる。

### 4.2 IPv6 の普及が進まない要因

最初に説明したIPv4アドレスの枯渇問題を解消するために、コンピュータに割り当てることのできるアドレスが豊富なIPv6を利用することが望まれている。しかし、IPv4アドレスの枯渇があとおよそ一年といわれている現在においても、IPv6の普及は十分であるとはいえない。

IPv6の普及が進まない理由はいくつかある。まず、地上波デジタル放送のように、ある時点から、現在のIPv4が使えなくなるといった、非常に強い動機づけ、言い換えると強制力がないことをあげることができるだろう。現在、IPv4を利用して、自組織内でグローバルIPアドレスが不足しているといった理由がなければ、当分の間はIPv6を利用する必要はない。

ただし、IPv4アドレスの枯渇が現実のものとなり、通信相手がIPv6しか利用できないという状況になれば、IPv6への対応は不可避である。

次に理由としてあげられるのはIPv6利用に関する情報がIPv4にくらべ格段に少ないことである。特に、セキュリティに関連する情報が少ないことは致命的である。

IPv4ではNATによる通信の非対称性により、比較的簡単にセキュリティを確保することができる。インターネットで公開したいネットワークと公開の必要のないネットワークの間にNATを配置するだけで、公開の必要がないネットワークへの外部からのアクセスを簡単に抑止することができるからである。

一方IPv6では、IPアドレスが豊富にあるため、NATに相当する仕組みは必要でなく、実装もされていない。このため、仮にセキュリティに配慮せずに組織のネットワークをIPv6対応にしてしまうと、公開の必要のないネットワークをインターネットにさらけ出してしまうことになる。このような事態は好ましいことではなく、何らかの形でセキュリティを担保する仕組みが必要となってくる。

### 4.3 大阪府産技研におけるIPv6の利用

現在、市販されている多くのネットワーク機器はIPv6に対応しており、セキュリティにあまり配慮する必要がないのであれば、IPv6を利用することはさほど困難なことではない。

当研究所では、インターネット接続事業者がIPv6接続サービスを提供しはじめた2001年から、インターネット接続においてIPv6の利用をはじめた。ウェブサーバなどのサーバ機器においては、10年前でも

IPv6の実装がほとんど完成しており、プロバイダから提供されたIPv6アドレスの一つをサーバに割り当て、サーバ機器の設定にIPv6対応する部分を追加するだけで、IPv6によるサービスを提供することが可能となった。

また、インターネットに公開しない所内ネットワークにおいても、ネットワーク機器をIPv6対応のものに交換した2006年より、IPv6の利用を開始した。このときの作業は、ネットワーク機器のマニュアルに記載されているとおりにIPv6に関する設定を追加しただけである。IPアドレスの表記などに違いはあるものの、本質的な部分はIPv4でもIPv6でも違いはないので大きな混乱はなかった。

以上の公開ネットワークや所内ネットワークでのIPv6利用については参考文献<sup>12)</sup>を参照して欲しい。

IPv6の利用において障壁となったのは、公開ネットワークと所内ネットワークとの接続において、IPv4におけるNATと同等のセキュリティを確保することである。

## 5. IPv6におけるセキュリティの確保

### 5.1 パケットフィルタによるセキュリティ

当研究所では、インターネットとの接続点に、外部ファイアウォールと内部ファイアウォールの二つのファイアウォールを配置している。インターネット接続点の配置の概略を図4に示す。

外部ファイアウォールでは、パケットフィルタの設定により、インターネットに公開するウェブサーバなどの各種サーバを保護している。パケットフィルタとは、IPアドレスやデータの種類によって、その通信の可否を判断する仕組みである。そして、内部ファイ

アウォールでは、パケットフィルタとNATを利用することによって、インターネットに公開する必要のない所内ネットワークを保護している。

NATの仕組みは、3章でも述べたとおり、内部ネットワークから外部ネットワークへの通信が発生したときにアドレス変換表を作成し、外部ネットワークから内部ネットワークにデータが到着した際に、変換表を参照して通信の可否を判断するというものである。従って、これと同じ仕組みをパケットフィルタに書き換えることができれば、NATと同等のセキュリティを確保できることになる。

パケットフィルタにはそれを動作させる機器によってさまざまな実装がある。パケットの種類やIPアドレスなどにしか着目しない静的フィルタだけでなく、最近では通信の状態遷移を把握し、通信の可否を判断する動的フィルタを利用することが可能である。

動的フィルタは、通信の状態を記憶しているため、これを使うとNATとほぼ同等の操作が可能となる。また、通信のうち、データ中にその通信状態が記録されるもの(TCPパケット)もある。これについては静的フィルタでもNATに近い動作が可能となる。

所内ネットワークからインターネットへの通信のうち、データ中に通信状態が記録されないもの(UDPパケット)は、ホスト名とIPアドレスを対応づけるDNS関連の通信と時刻を同期させるためのNTP関連の通信だけである。そして、これらの通信では、所内ネットワークに接続されたコンピュータとインターネット上のサーバの間で、直接データをやりとりすることはない。IPv4においてもIPv6においても、一度、内部ファイアウォールで中継する形としている。つまり、IPv6において、所内ネットワークとインターネットとの間で、直接このような通信をやりとりする必要はない。このため、内部ファイアウォールでは、インターネットと内部ファイアウォール、および内部ファイアウォールと所内ネットワークとの間で必要な通信のみを許可し、その他の通信はすべて破棄することにした。

一方、通信状態が記録されているTCPパケットのうち、メールなど大部分のものは、一度、内部ファイアウォールで受け取り、インターネットあるいは所内ネットワークに中継するという処理を行っている。単純に内部ファイアウォールを通過させる必要のあるものは、所内ネットワークから外部のウェブサイトにアクセスする通信のみである。

以上のことから、内部ファイアウォールでは、所内ネットワークからインターネットに出て行く通信と、

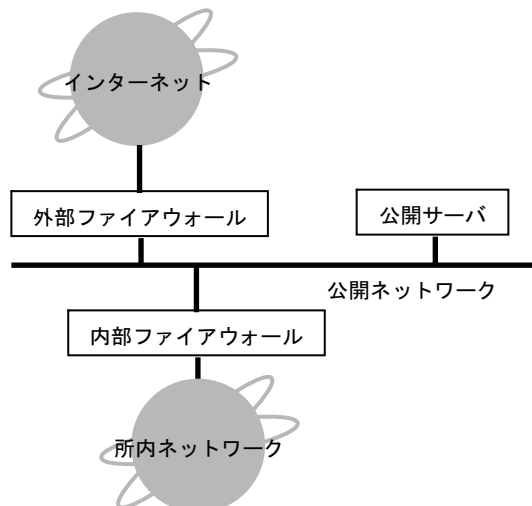


図4 ネットワーク構成概略図

通信状態が記録済みの TCP パケットのみを通過させることにした。これによって、IPv6 においてセキュリティレベルを低下させることなく、所内ネットワークとインターネットを接続することが可能となった。さらに、内部ファイアウォールが通信状態を記録する必要がないため、NAT における変換表の限界のような問題も発生しない。

## 5.2 動作の確認

Windows Vista や Mac OS X あるいは Linux や BSD といった最近の OS が搭載されているコンピュータは特に設定を行わなければ、IPv6 と IPv4 の両方のプロトコルが扱え、利用可能であれば IPv6 が優先して使われる。ネットワーク機器を IPv6 に対応させておけば、これらの OS が搭載されたコンピュータでは自動的に IPv6 アドレスなど、インターネットの利用に必要な設定が行われる。所内ネットワークに IPv6 が利用可能なコンピュータを接続し、インターネット上のウェブサイトに IPv6 でアクセスできることを確認した。この様子を図 5 に示す。

また、セキュリティについては、所外で IPv6 が利用可能なネットワークから接続テストを実施した。電子メールや公開ウェブサイトの閲覧など、必要な通信は通過させ、また必要のないものはすべて破棄していることをログによって確認している。実際に IPv6 の利用を始めたが、セキュリティ上問題となる点はなかった。

## 6. おわりに

大阪府産技研では、2001 年度より可能な範囲から IPv6 の利用をすすめてきた。そして、これまでの運用技術の集大成として、インターネットから所内ネットワークの隅々にいたるまで IPv6 を利用できる環境を整備した。

IPv4 アドレスはあと一年ほどで枯渇することが予測されているが、だからといって今から慌てて IPv6 環境を整備する必要性は高いとはいえ、一般的にはそのような切迫感も乏しい。これは、通信事業者などのサポートによって、現在 IPv4 を使っている利用者には、大きな影響を与えることが少ないと考えられているからである。

しかし、IPv4 が枯渇した時点から、新たにインターネットに参加する利用者にとっては、IPv6 による通信が主流になることが予想される。このことは、インターネットを利用してサービスを直接提供している組織には大きな影響を与えるかもしれない。インター



図 5 所内ネットワークから IPv6 で所外に接続

ネットに公開しているサーバを自前で運用している組織では、新たな利用者へのサポートとして IPv6 の利用が必要となるだろう。

現段階においては、IPv6 は IPv4 にとってかわるものではなく、二つの通信プロトコルをうまく使うことが求められる。逆に二つのプロトコルを利用できるのであれば、片方がつかえないときのバックアップの手法としても活用することが可能であろう。本稿がインターネットを情報発信の手段として活用している組織の一助になれば幸いである。

## 参考文献

- 1) 総務省：情報通信統計データベース，<http://www.soumu.go.jp/johotsusintokei/statistics/statistics05a.html>
- 2) IPv4 アドレス枯渇タスクフォース：IPv4 アドレス枯渇について，<http://www.kokatsu.jp/blog/ipv4/>
- 3) P. Srisuresh and K. Egevang: Traditional IP Network Address Translator (Traditional NAT), RFC3022, <http://www.ietf.org/rfc/rfc3022.txt>
- 4) S. Deering and R. Hinden: Internet Protocol, Version 6 (IPv6) Specification, RFC2460, <http://www.ietf.org/rfc/rfc2460.txt>
- 5) Silvia Hagen：IPv6 と IPv4, IPv6 エッセンシャルズ，豊沢聡訳，オライリージャパン，(2003)
- 6) N. R. Murphy and D. Malone: IPv6 Network Administration, O'Reilly, (2005)
- 7) J. Postel: Internet Protocol, RFC791, <http://www.ietf.org/rfc/rfc0791.txt>
- 8) 日本ネットワークインフォメーションセンター：IPv4 アドレスの在庫枯渇に関して，<http://www.nic.ad.jp/ja/ip/ipv4pool/>
- 9) Geoff Huston: Projected RIR and IANA Consumption (/8s), <http://www.potaroo.net/tools/ipv4/index.html>
- 10) 株式会社インテックシステム研究所：IP アドレス枯渇問題を可視化・IPv4 枯渇時計，<http://xn--kjqv5ah3lmt6a.com/index.html>
- 11) 社団法人日本民間放送連盟：地上デジタルテレビ完全移行，<http://www.nab.or.jp/chidejika/>
- 12) 石島 悌，平松初珠：大阪府産技研での IPv6 利活用について，大阪府立産業技術総合研究所報告，No.20, (2006) 21.