2

IPv4枯渇対策の方法と種別

IPv4によるインターネットは非常に規模が大きいので、IPv4枯渇対策として様々なアイデアが検討されています。本章では、現在議論されているIPv4枯渇対策にはどういったものがあるか、そしてそれらの技術は、主にどういった組織が検討し必要とするかといった点を説明します。

2.1 IPを巡る3つの立場とそれぞれの対策

IPv4のアドレス枯渇は、広範な人々に影響をもたらします。**図2.1**はインターネットを取り巻く人々やサービスを３つのグループに分けたものです。

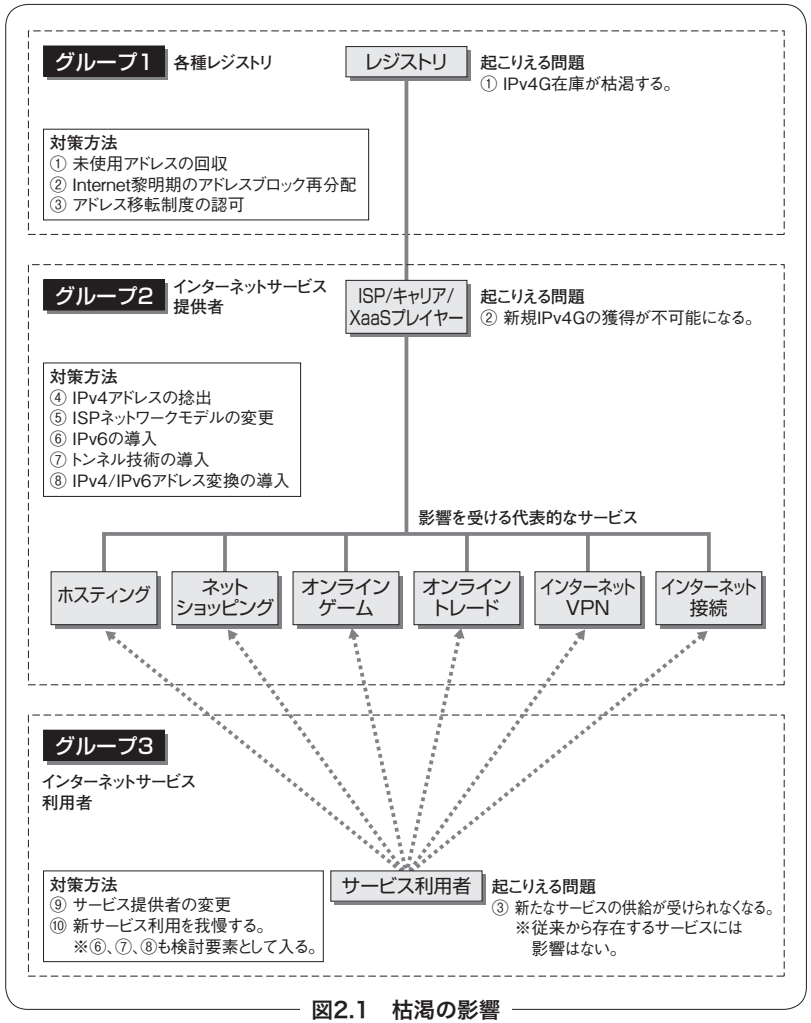


図2.1　枯渇の影響

１番目のグループは、IPアドレスを管理する組織や団体の集合であり、IANA、APNIC、JPNIC等が含まれます。２番目のグループはサービス提供者であり、インターネットのインフラを利用したサービスを顧客に提供することで収益を上げている企業群です。そして、最後のグループが一般消費者やユーザ企業など、インターネット上のサービスを利用する人達の集まりです。それぞれのグループごとに、どういった対策が検討されているかを整理してみましょう。

レジストリにとっての課題と対策

図2.1の「グループ1」は各種のレジストリで構成されます。このグループがIPv4G枯渇に陥ると、新規にIPアドレスの取得を希望する「グループ２」に対して、新たにIPを提供することができなくなるという問題が発生します。このグループでは現在、以下の対策案を検討しています(個々の対策案については後述します)。

① 未使用アドレスの回収
② インターネット黎明期のアドレスブロックの再分配
③ アドレス移転制度の認可

ISPの課題と対策

「グループ２」はインターネットサービスの提供者です。レジストリが新規IPv4Gの供給をできなくなると、最も影響を受けるのはこのグループに属する企業であると考えられます。なかでも一番早く影響を被るのは、キャリア系ではないASP/CSP/IDC (アプリケーション／コンテンツサービス提供者、データセンター事業者)、つまり独立系のXaaS (Software/Pratform/Hardware/Infrastructure as a Services など)プレイヤーであると予想されます。

彼らのビジネスモデルは、本来ユーザの所にあるべきサーバ等の資

産をインターネット上の“クラウド”に配置することで、管理費や初期投資費用を削減するというメリットを提供することで成り立ちます。このビジネスモデルを継続するためには、インターネットからIPv4Gによる接続性を確保することが大切です。

そして独立系のXaaSプレイヤーは、キャリア系XaaSプレイヤーと競争しなければなりません。キャリア系プレイヤーの大半は自社でISP事業を行っているので、ISP事業の方で保有しているIPv4Gからアドレスを捻出するといったことが可能ですし、独立系のXaaSプレイヤーは上流のISPからIPv4Gの“貸し渋り”を受けるかもしれません。このような理由から、ビジネス面で最も影響を受けやすいのは、独立系ASP/CSP/IDCのXaaSプレイヤーであると予想されているわけです。

次に影響を受けると予想されているのが、一般消費者を主要顧客とするISP事業者です。彼らのビジネスモデルはもちろんインターネットへの接続性を提供することですが、少し見方を変えると、IPv4Gを消費者に契約期間のあいだ貸し出すことであるとも考えられます。メールサービス等で収益を上げるケースはありますが、事業収益の大半はこのインターネット接続事業が占めています。新規のIPv4Gがなくなれば商材がなくなり、新規加入者を増やすことができず、事業拡大ができなくなることを意味します。こうしたことから、今現在議論されているIPv4枯渇対策案の大半は、グループ２の救済策になるといっても過言ではないでしょう。

このグループ向けには現在、以下の対策案が検討されています。

④ IPv4アドレスの捻出
⑤ ISPネットワークモデルの変更
⑥ IPv6の導入
⑦ トンネル技術の導入
⑧ IPv4/IPv6アドレス変換（トランスレーション）技術の導入

ユーザの課題と対策

「グループ３」はインターネットサービスの利用者です。このグループは法人企業と個人消費者に大別でき、それぞれとりうる対策は違ってきます。

このグループ向けに現在検討されている対策案には、グループ２と同様の技術が含まれますが、それらを適用する場合、求められる機器の性能要件がグループ２に比べて若干低くなります。

グループ２と共通する対策は次の３つです。

・IPv4/IPv6アドレス変換技術の導入（上記の⑧）
・トンネル技術の導入（上記の⑦）
・IPv6の導入（上記の⑥）

このほか、グループ３独自の対応策として、次の２つが考えられます。

⑨ サービス提供者の変更
⑩ 新サービスの利用を我慢する

では、以上10個の対応策について、概要を説明していきましょう。

2.2 様々なIPv4枯渇対策方法

未使用アドレスの回収

IPv4Gは多くの場合、アドレスブロック単位で割り当てられるので、実際には使用されていないアドレスが多数存在しています。そうした未使用アドレスの返却をレジストリが要請し、返却してもらうという対策案があります。

しかしながら、この対策は「あまり効果は見込めない」といわれています。なぜなら、割り当てられているアドレスブロックを、数字の先頭から順番に使っているケースが少ないという実態がある一方で、集約可能な単位でレジストリに返却されなければ、再利用するのは難しいからです。仮に、10.0.0.0/8というアドレスブロックがあったとしても、10.0.0.1から順番に詰めて使っている企業は少なく、10.10.0.1、10.20.0.1といったように、拠点や組織ごとにセグメント分けしている例が多くあります。このため、連続して未使用なアドレスブロックがそれほど存在しているとは期待できず、あまり多くを確保できないと考えられています。

それでは、「アドレスを綺麗に並べ換えることができるか」といわれると、これもけっこう難しいことです。返却を迫られる組織にとって、アドレスの並べ換えは非常に手間のかかる作業となります。ルータ等に設定しているアドレスの再設計と実機への再設定が必要となり、また、設定変更による障害発生のリスクも伴うからです。返却を求められた組織が、そうしたコストやリスクを負担してまで並べ換えを実施してくれるというのは、なかなか考えづらいのが実情です。

「だったら、細切れのまま返却してもらえばいいじゃないか」と思う人がいるかもしれませんが、そう簡単な話ではありません。細切れの経路情報がインターネット上のBGP（Boarder Gateway Protocol）に広報されると、経路情報が増大してしまうからです。BGPの経路情報は既に30万ルートを超えており、そこに細切れの経路情報が流入したら、BGPルータのメモリを拡張するなど、追加投資が必要になるといった問題も発生してしまいます。

インターネット黎明期のアドレスブロックの再分配

インターネットの黎明期に割り当てられたアドレス空間や、試験目的で予約されているアドレスブロックを再分配しようという計画もあります。インターネットの黎明期には、/8ブロックがごく一握りの関係者の間で大量に割り当てられ、そういったアドレスブロックが約40個ほど存在しています。

しかしその多くは、口頭や法的義務を問わないメールでのやりとりを通じて割り当てられ、正式な管理者がいなかったり、実際にどの程度使われているのかを把握するのが困難といった問題があります。現在ではIANAやRIRが存在しますが、黎明期のIPアドレスはそうした管理組織が不在の状態で割り当てられていたので、返却を要請しようにも、そもそも返却を迫る法的根拠が見当たりません。つまり、このアドレスはIANA等から借りたのではなく、「私のものだ」と主張できるということです。それを回収するには、自発的な返却に頼らざるをえず、あまり大きなボリュームの返還は見込めないといわれています。

一方、試験目的で予約されているアドレスには、「クラスE」として定義されている240.0.0.0 ～ 255.255.255.255のアドレスブロックが該当します。これらは黎明期のアドレスとは異なり、特定の組織に割り当てられていることもないので、いったん方針が決まってしまえば、利用するのはそれほど難しくないように思えます。しかし、このアドレスは試験目的であり、実際のネットワークには使わないことを前提としていたので、IPアドレスとして設定することを許可していない機器も多くあり、実機への実装という点ではハードルが高いと考えられます。

この場合、ソフトウェア対応により使用を許可することは可能と考えられますが、インターネット上のすべての機器やファイアウォールが対応する必要があり、公衆インターネット上での運用は難しいと思われます。このため、後述する「ラージスケールNAT」と呼ばれるアドレス変換装置をISP内部で利用するときの、特別なアドレスブロックの１つとして利用することが検討されています。

アドレス移転制度の認可

IPアドレスとは「必要とする人が、必要な時に、必要な期間だけ借りて使うもの」と一般的に認識されるようになってきました。このため、レジストリから割り当てられたアドレス空間を売買したり、レジストリの許可なしに他の組織へ譲渡することは認められていませんでした。理由は、レジストリが介在せずにアドレスが譲渡されると、レジストリのデータベース(DB)の信頼性が損なわれるおそれがあるからです。

IPアドレスは「インターネット通信を可能にする」という役割のほかにもう１つ、「犯罪発生時等の通信発信者の特定に利用される」という重要な側面があります。例えば、企業システムへの不正アクセスやネットオークションでの詐欺行為など、インターネットを利用した不正行為が発生した場合、その通信に使われたIPアドレスは、捜査の手掛かりや犯罪の証拠として扱われることがあります。一見、「匿名の世界」と思われがちなインターネットですが、レジストリのDB情報からISPを特定しIPアドレスを辿っていけば、発信者を特定することが可能です。情報を発信した国や機器、組織を探り出す手段になるのです。もし、このような犯罪を検挙・抑止する機能がなかったら、どんなに優れた技術であっても、実ビジネスへの適用を誰もが躊躇するでしょう。レジストリDBの信頼性は、インターネットの存続にとって抜き差しならない重要事項なのです。

万一、レジストリDBの情報が信頼性を低下させてしまったら、インターネットが匿名で無法地帯となってしまう可能性があります。実際、モデムによる通信が一般的だったころの「クラッカー」と呼ばれていた昔の侵入者達は、身元の発覚を防ぐため、電話の通話記録管理がずさんな国を探し出し、そこから海外の企業へ不正侵入を試みていました。今では信じられないかもしれませんが、人手による電話交換対応が行われていた時代には、通話記録が残されていないこともあったのです。

インターネットが発信者を特定できなくなれば、不正侵入が明るみに出ても身元を特定できず、検挙に至る可能性が低下して犯罪が増加傾向となり、企業は不正アクセスの脅威に今以上に脅えることになるでしょう。そうなってしまえば、インターネットのビジネス活用は徐々に影を潜め、インターネットの利用そのものが低迷してしまう懸念も生じます。

しかし、こうしたリスクはあるにしても、アドレス枯渇が迫るにつれて、「レジストリを介さない企業間等の個別交渉を認めよう」という声が次第に大きくなってきました。その風潮を背景として、アドレス譲渡の方法として「金銭契約によるアドレス売買」の検討が開始されました。本章執筆中の2009年６月現在では、RIPEにおいて既に試行されており、APNICを除く他のRIRでも追随する方向で検討が進んでいます。金銭的なインセンティブが働くようになれば、企業は不要なアドレスを喜んで売却するようになると考えられますが、金銭的譲渡には様々な問題を伴うことも認識しておかなくてはいけません。

まず、売買が可能になると、IPアドレスが資産的価値を持つことになるので、課税対象となるかもしれません。売買する意志のない企業にとって、IPアドレスが新たな課税対象になる可能性もあります。また、価格規制や法的整備が不充分だと、経済犯罪に悪用されるおそれもあります。例えば、グループ企業間でIPアドレス１つを10億円で売買するといったように、資産移動、財務操作、マネーロンダリングが不動産などよりも簡単にできてしまうからです。

このように、アドレス移転制度は、金銭収入が見込める場合には、

黎明期のアドレスブロックの回収に役立てることを含め、ある程度の効果を期待できますが、その一方、事前に整備すべき制度や実施後の課題も多々あり、正式な導入に至るまでにはもう少し時間がかかりそうです。

IPv4アドレスの捻出

各組織内で不要となったサービスや機器に設定されているIPv4GをIPv4Pに変更するなどして、IPv4Gを捻出するという方法です。通信事業者や大企業では、数千個単位のIPv4Gを社内で使用している例もあり、自助努力によってある程度のIPv4Gの捻出が可能であると見られています。

とはいえ、この方法は基本的に“一回限り”となります。恒久的に十分なアドレス数を捻出できるケースは、ごく希であると思われます。

ISPネットワークモデルの改造

この方法は小手先の対策ではなく、ISP事業者とユーザの間に構築されているIP網の構造自体に改造を加えようという大掛かりなものです。

まず、現在のインターネットの構造を簡単に表現すると、**図2.2**のようになります。一般家庭にはCPE（Customer Provided Equipment）と呼ぶ通信装置が設置されています。通常、CPEにはHGW（ホームゲートウェイ）やブロードバンドルータが該当し、CPEからISPへ接続されています。そして、宅内のLAN側にはIPv4Pが割り当てられ、ISP側にはIPv4Gが設定されています。つまり、1世帯に1つのIPv4Gが割り当てられている状態です。これでは、IPv4Gが枯渇したとたんに、ISPは加入者を増やすことができなくなってしまいます。

そこで、IPv4Gを節約するための3つの案が検討されています（**図2.3**）。ただし、本書の執筆時点ではまだ審議中であり、技術的な詳細を述べても無効になるおそれがあるので概要だけを解説します。

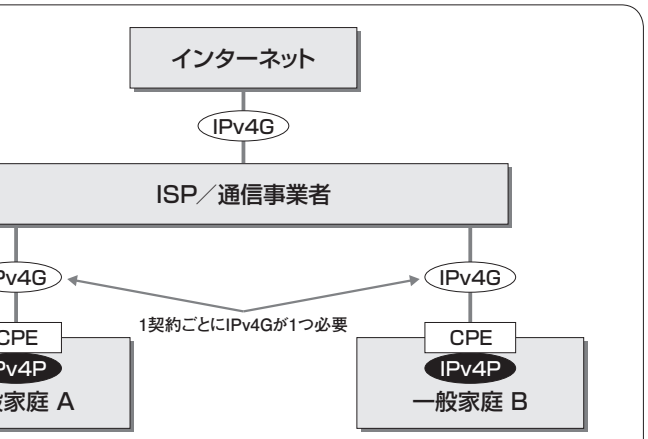


図2.2 現在のインターネットの構造

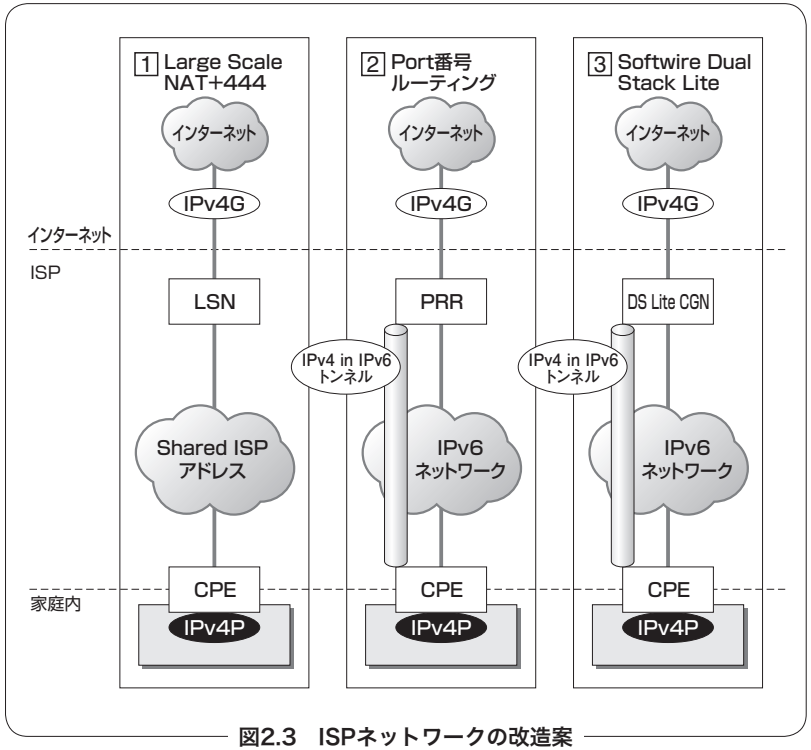
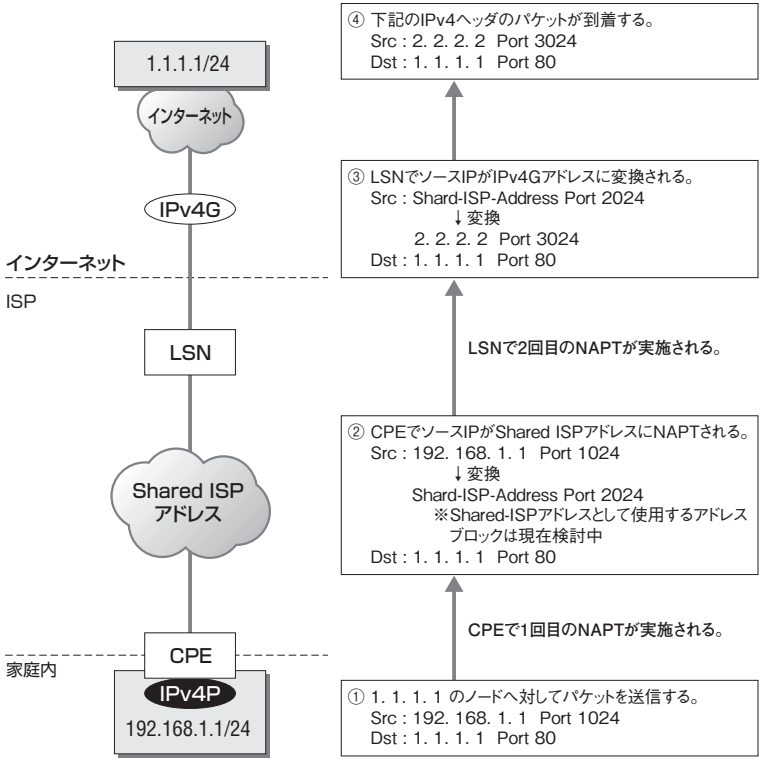


図2.3 ISPネットワークの改造案

1 Large Scale NAT+444

1番目の改造案は、「ISPネットワークにLSN（Large Scale NAT）を適用する」というモデルであり、「LSN+444」と呼ばれています。LSNはCGN（Carrier Grade NAT）という言葉でも知られています。

このネットワークモデルにおいては、宅内LANにはIPv4Pを使用し、



長所
- CPEの構成変更が不要
- 他の2つの技術に比較して短い期間で導入可能

短所
- SIP等のようにペイロード部分にアドレス表記が存在するパケットではLSN側で対応する必要がある。
- すべてのアプリケーションの動作を保証できるものではない。
- 多段NATの使用はP2Pやオンラインゲーム等で通信不具合が発生する可能性がある。
- アドレス変換のアクセスログを取得する仕組みが必要になる。
- LSNで変換されると、ソースIPアドレスがすべてLSNのアドレスとなってしまい、不正アクセスの追及が難しくなる。

図2.4 Large Scale Nat+444の動作例

はじめにCPEの部分でNAPTを行い、LSNでもさらにNAPTを行います。「多段NAT」と呼ばれる構成にすることで、これまで1世帯につき1つ必要だったIPv4Gを、複数世帯で共有できるようになり、IPv4Gの節約につながると期待されています。

また、ISP内で用いるアドレスをIPv4G以外のものを使用することで、IPv4Gを節約することも同時に検討されており、その空間で用いるアドレスブロックも検討されています。1つは、IPv4の240.0.0.0から始まるクラスEのアドレスの利用。もう1つは、IANAから専用のアドレスブロックを割り当ててもらうという案です。「240.0.0.0のアドレスについては設定不可能」となっている機器も多いので、IANAからのアドレスブロック取得を前提に検討が進められています。

このネットワークモデルの動作例を**図2.4**に示します。

また、参考URLには以下があります。

- LSNを導入したNAT444モデルの仕様
  http://tools.ietf.org/html/draft-shirasaki-nat444-isp-shared-addr-01
- Large Scale NATに関する要求仕様
  http://www.ietf.org/internet-drafts/draft-nishitani-cgn-02.txt
- NAT444モデルでCPEとLSNの間で使用するアドレスブロックに関する内容
  http://www.ietf.org/internet-drafts/draft-shirasaki-isp-shared-addr-02.txt

※「コラム・LSNの単独利用」(p.37)参照

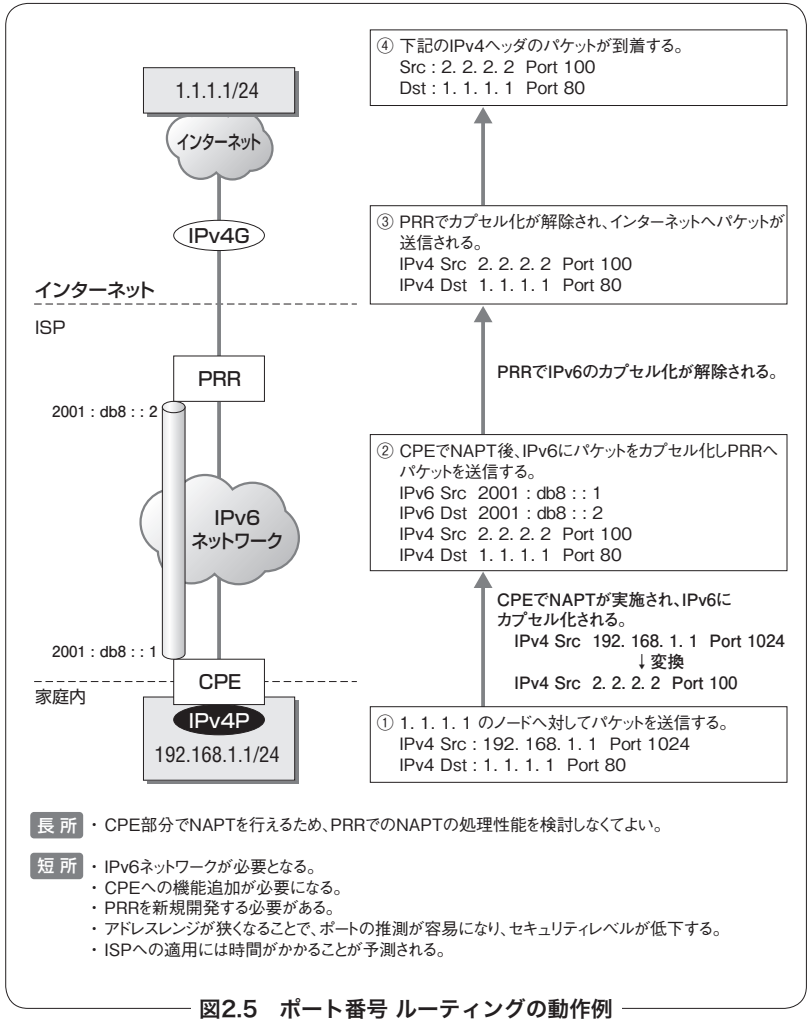
2 Address + Port Routing

2番目の改造案は、「TCP/UDPのポート番号用のビット列の一部をIPv4ヘッダとして利用し、IPv4アドレスを拡張しよう」というアイデアです。例えば、UDP/TCPのポート番号は16bitありますが、これを8bitに制限し、余った8bitをIPv4アドレスに付与して、IPv4アドレス

レンジを拡大しようという試みです。

この技術は大きく分けてNAPT、パケットのカプセル化および解除機能、シグナリング機能という３つの独立した技術要素で構成されます。そして「拡張されたポート番号＋IPv4アドレスルーティング」を処理するための装置として、PRR（Port Range Router）の開発が検討されています。しかし、LSNについては具体的な製品が登場してきていますが、PRRはまだ開発中であり、実際に導入されるまでには時間がかりそうです。

動作例(**図2.5**)ならびに参考URLは下記のとおりです。



長所
- CPE部分でNAPTを行えるため、PRRでのNAPTの処理性能を検討しなくてよい。

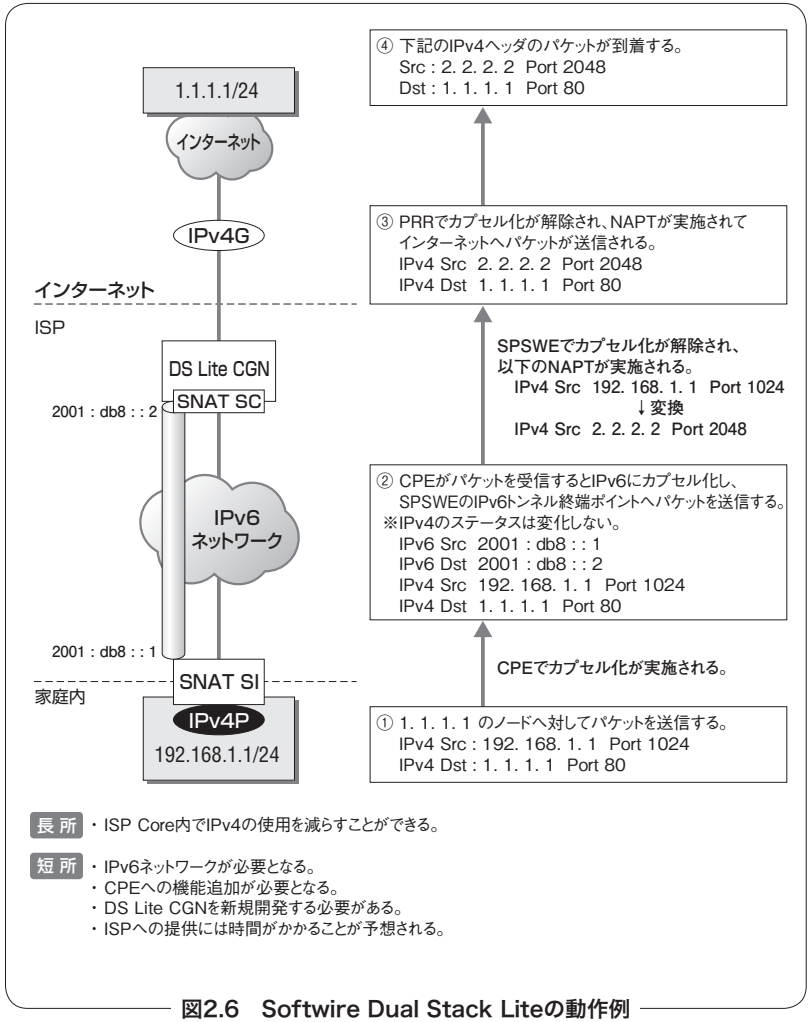
短所
- IPv6ネットワークが必要となる。
- CPEへの機能追加が必要になる。
- PRRを新規開発する必要がある。
- アドレスレンジが狭くなることで、ポートの推測が容易になり、セキュリティレベルが低下する。
- ISPへの適用には時間がかかることが予測される。

図2.5 ポート番号 ルーティングの動作例

[参考 URL] http://tools.ietf.org/html/draft-ymbk-aplusp-04

3 Softwire Dual Stack Lite

３番目の方法は、２つの技術を用いて、ISPコアネットワーク内で



長所
- ISP Core内でIPv4の使用を減らすことができる。

短所
- IPv6ネットワークが必要となる。
- CPEへの機能追加が必要となる。
- DS Lite CGNを新規開発する必要がある。
- ISPへの提供には時間がかかることが予想される。

図2.6 Softwire Dual Stack Liteの動作例

[参考 URL] http://tools.ietf.org/html/draft-ietf-softwire-dual-stack-lite-01

利用されているIPv4Gを節約する案です。下記の方法が検討されています。

・NAPTを用いて、１つのIPv4Gで多数の加入者のトラフィックを処理する。
・ISP コアネットワークをIPv6で構築し、IPv4トラフィックについてはトンネル技術を用いて伝送する。

この２つを可能にするため、CPEのほか、DS Lite CGN（Dual Stack Lite Carrier-grade NAT）と呼ばれる装置において、以下のような処理を行うことが検討されています。

まず、CPEにはSI（Softwire Initiator）と呼ばれる機能を追加し、SIとDS Lite CGNのSC（Softwire Concentrator）の間でIPv6トンネルを形成します。CPEが宅内LANからIPv4パケットを受信すると、IPv6パケットにカプセル化して、DS Lite CGNのSCへ転送します。CPEのSIからDS Lite CGNのSC宛にパケットが届くと、DS Lite CGNのなかでIPv6カプセル化が解除されます。そして、DS Lite CGNは、あらかじめ設定された内容に基づいてIPv4PをIPv4Gへと変換（NAPT）します。

動作例（**図2.6**）ならびに参考URLは前ページのとおりです。

IPv6の導入

IPv4枯渇対策としては、様々な方法が議論されていますが、抜本的な解決策として期待されているのが「IPv6の導入」です。IPv6については次章以降で詳細に解説しますので、ここでは簡単な説明に止めます。

IPv6を機器に実装するには２つの方法があります。**図2.7**に示した「IPv6オンリーノード」と「デュアルスタックノード」です。

また、IPv4しか喋らないノードを「IPv4オンリーノード」、IPv6しか喋らないノードを「IPv6オンリーノード」、IPv4とIPv6の両方を喋ることができるノードを「デュアルスタックノード」と呼び分けています。デュアルスタックノードはどのタイプのノードとも接続できますが、

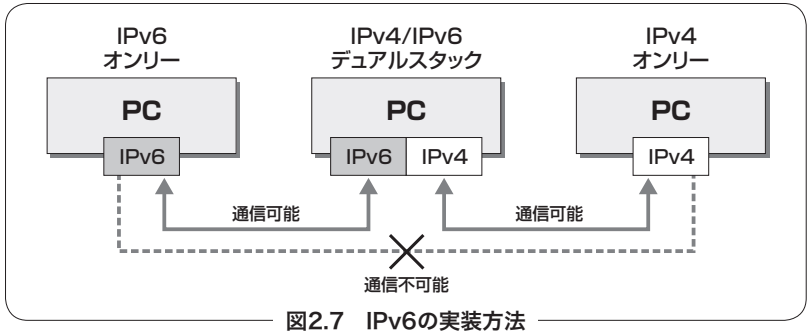


図2.7　IPv6の実装方法

各オンリーノードは同一のプロトコルタイプを利用するノード同士でしか通信を行うことができません。ただし、後述するIPv4/v6変換技術を使えば、異なるオンリーノード同士の通信も可能になります。

現在はIPv4しか喋らないIPv4オンリーノードが主流ですが、今後IPv4枯渇が問題になってくると、徐々にデュアルスタックノードに移行し、IPv4が完全に枯渇した後はIPv6オンリーノードが増えていくと考えられます。

では将来、「すべてのノードがIPv6オンリーノードと通信できるようになるか」というと、そうではありません。2003年以降に発売されたOSの大半はIPv6に対応していますが、Windows MEやWindows 95といった旧いOSにはIPv6対応の予定もありません。これらのOSを使っている企業がIPv6で通信するには、OSを入れ換える必要があります。しかし、そうした旧いOSが走っている旧式のハードに最新のOSを入れると、動作が遅くなるなど実用性に問題を生じます。そうかといって、すべての機器を買い換えるにはコストがかかるので、IPv4オンリーの機器も、そのまま長期間存在し続けると想定しておく必要があります。

したがって、IPv6の導入は確実に始まりますが、ただちにIPv6一色の世界になるわけではありません。IPv4オンリー、IPv6オンリー、デュアルスタックノードの３種類が、しばらくの間は共存していくことになります。

トンネル技術の導入

IPv4環境にIPv6を導入する場合、すべての機器をデュアルスタックノードにすることができれば話は簡単です。しかし実際のネットワーク環境では、旧い機器が混在し、またその台数が多ければ「一部の機器ではどうしてもIPv4だけを実行させ続けなければならない」といった必要が生じるケースもあるでしょう。特に中継区間には、多数のネットワーク機器が存在するので、それらをすべてIPv6に対応させるには長い期間と莫大なコストがかかります。このような状況に有効なのが「トンネル技術」です。

トンネル技術が必要になるケースは決まっています。次の条件に該当する場合です。

・送信元ノードから送信先ノードまでのパス上に、異なるIPバージョンで通信を行う区間が存在する場合

現在はIPv4で構成されたネットワークがほとんどであり、IPv6ノードはところどころに散在している状態です。このような状況でIPv6ノード同士の通信を成立させるには、トンネル技術が必要となります。

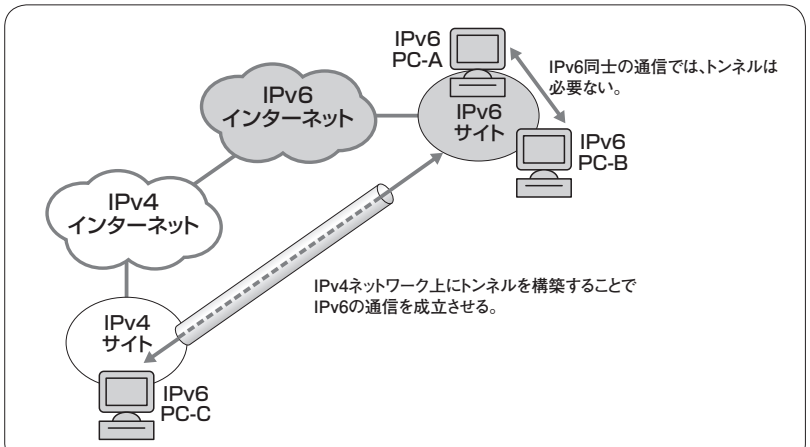


図2.8 トンネル技術が効果を発揮する状況

例えば、**図2.8**のようなネットワーク環境の場合、PC-AとPC-BはIPv6のネットワーク上に存在しているので、この２台のノードが通信するためにトンネル技術は必要ありません。しかし、PC-AからPC-Cに通信を行おうとすると、途中のネットワークがIPv4で構成されていますが、IPv4ネットワークにIPv6のトラフィックを直接流すことはできません。そこで、IPv4ネットワークの出口とIPv6ネットワークの入口の区間にトンネルを構築します。IPv6パケットはこのトンネルに入るときにIPv4でカプセル化され、トンネル内ではIPv4のパケットとして転送されます。トンネルの出口でカプセル化が解除され、IPv6パケットに戻って通信が成立します。

トンネル技術の動作概要は**図2.9**のとおりです。なお、トンネル技術の詳細については、４章の4.7節と4.8節で解説します。

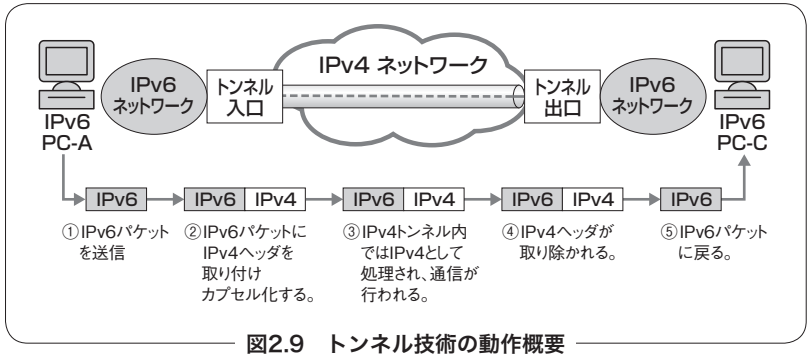


図2.9 トンネル技術の動作概要

IPv4/IPv6アドレス変換技術の導入

IPv6を導入する際にトンネル技術を利用したとしても、すべての問題が解決されるわけではありません。世の中にはIPv4しか喋ることのできない機器が大量に存在します。例えば、10年以上前に発売されたネットワーク機器やPC等の中には、既にメーカーが倒産してしまっていたり、機器のサポート期間が切れているといった理由から、IPv6対応の予定がないものがあります。また、それくらい昔に導入されたも

のであっても、今なお正常に動作している機器は世の中にたくさん存在します。

そのような機器が、やがて登場すると考えられるIPv6オンリーノードと通信したくても、IPv4とIPv6は異なるプロトコルなので、直接通信を行うことはできません。たとえトンネル技術を用いたとしても、それはパケットの中継網で有効な技術であるため、問題を解決することができません。

そこで必要になるのが、IPv4のパケットをIPv6に、IPv6パケットをIPv4パケットへと、相互変換してくれるIPv4/IPv6アドレス変換技術です。つまり、トンネル技術とIPv4/IPv6アドレス変換技術は、**図2.10**のように使い分ける必要があるということです。

なお、IPv4/IPv6アドレス変換技術については、４章の4.9節で詳細を解説します。

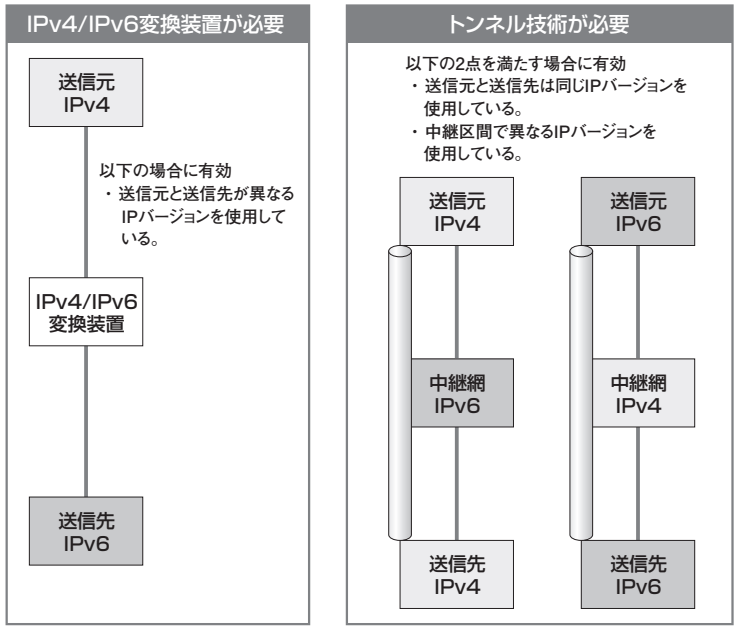


図2.10　トンネル技術と変換技術の使い分け

サービス提供者の変更

サービスを利用する側にとって、サービスの提供者、例えばISPやIDCを変更するというのは立派な対策案になりえます。もし、法人ユーザが新規事業所を開設する際に、「今契約しているISPではネット接続ができない」と言われたら、他のISPに切り換えるでしょう。一般消費者も同じことで、引っ越し先ではネット接続を提供できるISPに契約を変更することを考えるでしょう。

サービスを利用する側にとって、ネット接続ができない不便さに比べれば、ISPの変更手続きはたいした手間ではありません。必要に迫られる時期がくれば、これは現実的な対応策になります。しかし、ISPやIDCといった「グループ２」の事業者視点で見ると、既存顧客というものはそれくらい簡単に他の事業者に乗り換えてしまうものだということを充分考慮しておく必要があります。

サービス利用を我慢する

冗談のように聞こえるかもしれませんが、ユーザにとっては「我慢する」というのも立派な対策です。だたし、ネットに一切つながずに、じっと耐え凌ぐばかりが我慢ではありません。

例えば、ある個人ユーザが、自宅のPCからブロードバンドルータ経由で、長年快適にインターネット接続を行っていたとします。ところが、IPv6を利用したくなったとき、自宅で契約しているISPがIPv6に対応していないことがわかりました。そこで、IPv6が利用できるようになった新しいモバイルブロードバンドに回線契約を切り換えて、それまでPCでできていたことを携帯電話で我慢する、といった我慢のタイプも考えられます。

あるいは、お気に入りのネットショップはIPv6に対応していないのに、契約しているISPがある日突然、IPv6でしか接続できなくなった

とします。しかたなく、IPv6で接続可能な２番目にお気に入りのネットショップで我慢する、といった我慢のタイプも考えられます。

それまでの自分の行動パターンや手段を少し変更することで、多少の不便を感じながらも我慢する。これも現実的な対応策といえます。しかしこの対策も、先ほどのサービス提供者の変更と同じく、ISPやIDCの事業者視点で見ると、機会損失につながるということを考慮しておくべきです。

コラム

v4の次はv5じゃないの？

「IPv4の次」ということであれば、「IPv5」と名づけるのが普通だと思いますが、なぜ「IPv6」になったのでしょう。疑問に思う人も多いのではないのでしょうか。

IPのバージョンナンバーはIANAが管理していますが、実は「v5」もしっかり存在しています。さらに「v8」とか「v9」の仕様も定義されています。これらの番号については下記のサイトに記載されています。

◦ **http://www.iana.org/assignments/version-numbers/**

今すぐ知りたい方のために、各バージョンナンバーに割り振られた内容を簡単に紹介しておきます。

Registry:

Decimal	Keyword	Version	Reference
0-1		Reserved	[JBP][RFC4928]
2-3		Unassigned	[JBP]
4	IP	Internet Protocol	[RFC791][JBP]
5	ST	ST Datagram Mode	[RFC1190][JWF]
6	IPv6	Internet Protocol version 6	[RFC1752]
7	TP/IX	TP/IX: The Next Internet	[RFC1475]
8	PIP	The P Internet Protocol	[RFC1621]
9	TUBA	TUBA	[RFC1347]
10-14		Unassigned	[JBP]
15		Reserved	[JBP]

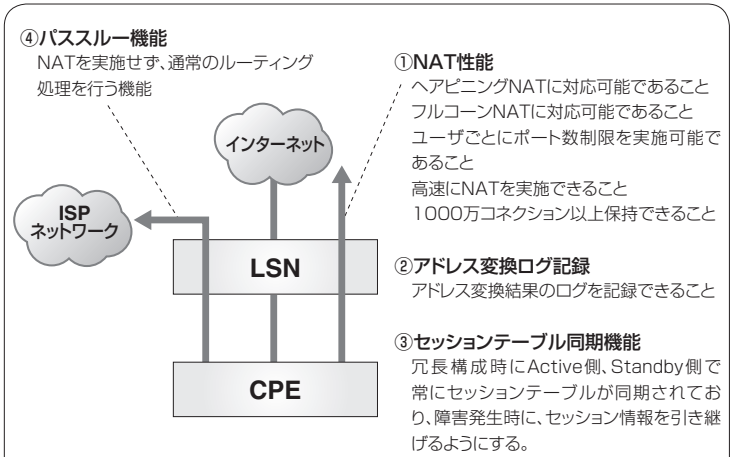
コラム

LSNの単独利用

LSNは現在、非常に注目されており、Large Scale NAT+444のモデルとは別に、単独での利用も検討されています。使われている技術を一言でいえばNATであり、決して目新しいものではありません。ISPによっては、インターネット接続部分などにNAT処理専用装置を設置した例が古くから見られました。しかし、ISPの内部に設置することになると、要求されるスペックがより厳しいものになります。

現在、LSNには下図のような機能が求められています。

NATの導入経験がある人には、特段目新しく感じる部分は少ないと思います。大きく異なる点は、膨大なコネクション数を保持する必要があるこ



■ **LSN導入の利点**

・IPv4Gを節約可能
・CPE、PC側の対応は不要

■ **LSN導入の懸念点**

・SIP等ペイロード部分にアドレス表記があるアプリケーションには、個別対応が必要
※パススルーでNATをさせないという対処方法も検討されている。
・変換後のアドレスがLSNで変換されるアドレスに集約される。
〔例〕 下記のように二世帯からのアクセスが発生した場合、Internet側ではすべて1. 1. 1. 1 からのアクセスに見える。
ユーザA 10. 1. 1. 1 : 1024 → 1. 1. 1. 1 : 1024
ユーザB 10. 2. 2. 2 : 1025 → 1. 1. 1. 1 : 1025

図 LSN

と、それに伴い、アドレス変換のログが大量に必要になるという点です。

この2点について、要求仕様のハードルが低ければ、従来の製品でNATを実施することも可能でしたが、一気に10倍前後に引き上げられたため、新製品を検討する必要が出てきました。本書の読者がLSNの導入を検討するときは、自分たちがどの程度の処理性能を必要とするかを、まずはじめに検討してみることをお勧めします。

LSNが必要かどうかを検討する際のポイントとしては、以下の要素が考えられます。それぞれの項目について、自社で必要とされる値を算定すれば、既存製品で対応可能か、それともLSNにすべきかの判断材料になるでしょう。

- NAT CPS（Connection Per Second）
- NATコネクションテーブル最大数
- ユーザ単位でのポート数制限機能
- 使用NAT技術
  - フルコーンNAT
  - ヘアピニングNAT
  - シンメトリックNAT
  - NAPT
- アドレス変換ログの記録容量

パススルー機能については、ACL（Access Control List）やファイアウォールの「ポリシーベースNAT」で代用することも可能ですし、既にセッションテーブルの同期機能を実装した機器も多くあり、LSNに限った機能ではありません。筆者がいろいろな方と話をした限りでは、ただ漠然と「LSNを導入しなければならないのではないか」という不安にかられている人でも、よくよく話を聞いてみたら従来製品で十分対応可能というケースがありました。

LSNは、本書の執筆時点ではドラフト案が固まっていないこともあり、試作品レベルのものしか存在していません。また、従来製品に比べて高価になりそうです。従来製品で対応可能な場合には、価格面や安定性の面でLSNよりもよい結果になることもあるので、慌てることなく充分に検討することが肝要です。

2.3 各種対策案の技術比較

ここまでは、現在検討されているIPv4枯渇対策の概要を紹介しました。次に、グループ1とグループ2で検討されている方法を**表2.1**に沿って比較してみましょう。

表2.1 各種対策の比較

対策案	対策の種別	効果の永続性	適用に要する時間	効果予測
①未使用アドレスの回収	IPv4延命策	一時的	現在でも実施中	あまり期待できない
②インターネット黎明期のアドレスブロック再分配			実施には時間がかかる	あまり期待できない
③アドレス移転制度の認可			一部で試行されているが、本格実施までは時間がかかる見込み	法的整理等課題があるが、効果はあると期待されている
④IPv4アドレスの捻出			各組織により異なる	あまり期待できない
⑤ISPネットワークモデルの変更			LAN+444モデルは枯渇時期までに間に合う可能性がある それ以外の方法はさらに時間がかかるとの予想がある	LAN+444については具体的な製品も登場してきており、効果があると期待されている
⑥IPv4/IPv6アドレス変換技術の導入	IPv6導入策	永続的	各組織により異なる	IPv4/IPv6共存手段として期待されている
⑦トンネル技術の導入			各組織により異なる	IPv4/IPv6共存手段として期待されている
⑧IPv6の導入			各組織により異なる	抜本的対策として期待されている

IPv4延命策とIPv6導入策

対策の種別は大きく分けて「IPv4延命策」と「IPv6導入策」の2つに分類されます。IPv4延命策とは、その名が示すとおり、なんとかしてIPv4の延命を図り、現在使われている様々な資産を有効活用しようというアプローチです。「様々な資産」とは、IPv4で動作しているネット

ワーク機器やサーバ、クライアントなど、膨大な資産を指します。

表2.1では、①〜⑤の５つの対策について、「効果の永続性」が「一時的」と記載しました。過去にもNAT/NAPTによって枯渇の危機を免れたように、これらの対策をもってすれば、枯渇期限を数年間先延ばしすることは不可能ではありません。しかしながら、IPv4の母数が着実に減少し、消費速度が速まっている今日では、いずれまた対策案を検討する必要性に迫られることになります。

そこで、「抜本的な対策案を」ということで、IPv6の導入が真剣に検討されることになりました。IPv6の導入効果は永続的です。一度実施してしまえば、その膨大なアドレス数によって、事後の対策は半永久的に必要ないと言われています。

期待と効果の度合い

「適用」と「効果」の観点ではどうでしょうか。「①未使用アドレスの回収」と「④IPv4アドレスの捻出」については、現在でも各レジストリが不要なアドレスを返却するよう打診するなど、各組織がIPv4Gの節約を試みていますが、目覚しい成果は上がっていません。

「②インターネット黎明期のアドレスブロック再分配」については、/8のアドレスブロックがなんと40個もあるわけですから、もしこれが実現すれば大きな効果を期待できます。しかし、実際にはなかなか応じてもらえないので、「現時点ではあまり期待できない」と考えられています。ただし、もし③のアドレス移転制度が整備され、金銭譲渡に応じてくれれば、これらのアドレスブロックやIPv4が余っている団体から、IPv4を必要とする組織に対してIPv4を販売することが可能になるため、枯渇対策への効果が期待できるのではないかと言われています。しかしこの方法については、効果は期待できるものの、今まで金銭的価値の小さかったIPアドレスが金銭的価値を持つようになったら、どういった問題が発生するのかがまだまだ未知数であり、全世界的な本格施行にはもう少し時間がかかると見られています。

「⑤ISPネットワークモデルの変更」を実現する方法はいくつかあり、それぞれ得られる効果が違うものの、どの案であっても実現すれば高い成果を期待できます。しかし、ISPにとっては大規模な構造変化となるので、しばらく議論が続くと見られています。本書の執筆時点では、LSN＋444モデルを有力視する見方が多いようです。理由は、CPEの変更が不要であるという点と、用いられる主要技術がNAPTという枯れた技術であるため、新規開発を必要とする要素が少なく、他の案に比べて短時間での導入が可能と見込めるからです。

しかしLSN＋444でも他のモデルでも、それを採用したISPは、他方でIPv6による抜本的対策の導入検討を迫られることになります。ISP各社は、どのIPv4延命策を講じるべきか、あるいは、IPv6による抜本的対策に資金を集中するべきかという悩みを抱えています。各種の対策案について、不透明なIPv6トラフィック需要、時間、コストという３つの観点から、入念に比較検討しています。

事業者側の対策とユーザ側の対策

大切なことは、「どの対策案が優れているか」という優劣をつけることではありません。できることはすべてやらなければならないのです。効果予測の項に「あまり期待できない」と記載されている対策であっても、インターネットを支えている人達の間では、真剣に取り組まれています。IPv4枯渇が迫るなか、たった１個のIPv4Gでも有効活用しようと、様々な努力がなされています。それほど問題は切羽詰っており、確実にIPv4の枯渇が迫っているのです。インターネットの裏側で真剣な議論が交わされていることを認識しておくべきでしょう。

とはいえ、これだけの対策案が検討されているからといって、そのすべてを自社組織に当てはめる必要はありません。何が自分たちの所でできて、何ができないのかを選別する必要があるといえます。

表2.1の対策案①～⑤は、グループ１とグループ２に属する団体や組織が検討すべきことがらです。特にISPネットワークモデルの変更は、様々な技術要素が絡みますし、雑誌等でもしばしば特集が組まれ多く人々の興味を惹きますが、大半の企業ネットワークでは、あまり意識する必要はありません。せいぜい「CPEが別途必要になる」といった程度で済むケースがほとんどでしょう。また、契約しているISPが導入したからといって、自社でもLSNやPRRを購入する必要があるかというと、必ずしもそうとは限らないので、導入検討には慎重を期す必要があります。

本書では、企業ネットワークやサーバファーム、データセンターのインフラ等で必要とされる知識に的を絞ります。次章以降では、対策案⑥～⑧のIPv6導入策を実施する際に必要となる知識と、展開方法を紹介していきます。