IPv6 移行ガイドライン

(ISP セグメント)

2004 年 5 月

IPv6 普及･高度化推進協議会

移行 WG ISP SWG

目次

はじめに

本ドキュメントは、中小 ISP の構築運営に携わる Operator、SIer を対象に、中小 ISP が今後 IPv6 を導入するにあたり、検討すべき一般的な項目、指針、方法について記述しています。

ここで記載される内容は、1 つの考え方を示すものであり、唯一の解ではありません。読者が、自らの指針により IPv6 の導入を検討する際、このドキュメントを参考に応用が図れるよう記述しています。

■検討メンバ

SWG チェア
中井（NTT コミュニケーションズ）

リーダ
アドレス&ルーティング担当
石原（KDDI）
ネットワーク担当
石川（NTTPC コミュニケーションズ）
松平（富士通）
サーバ担当
橘（あにあにどっとこむ）

検討メンバー
荒野（インテックネットコア）
石原（東芝）
猪俣（富士通）
岡本（eAccess）
金山（インテックネットコア）
川島（NEC アクセステクニカ）
国武（RINT）
鈴木（日立製作所）
須田（知多メディアスネットワーク）
竹山（eAccess）
中原（NEC）
難波（古河電工）
松岡（NTT PF 研）

(あいうえお順、敬称略)

■お問い合わせ先

本ガイドラインに関するお問い合わせは、以下のアドレスまでメールでご連絡を下さい。

IPv6 普及・高度化推進協議会 移行 WG／e-mail: wg-dp-comment@v6pc.jp

1. セグメントの特徴

■対象とする ISP

ISP は、サービスの提供対象、提供地域、サービス内容から、以下のように分類することができます。

提供対象

ホールセール（Flet's、eAccess、ACCA など）、リテール（OCN、Nifty、DION、BIGLOBE など）

地理的範囲

グローバル（UUNET、VERIO など）、ナショナル（OCN、Nifty、DION、BIGLOBE など）、リージョナル（地域 ISP）

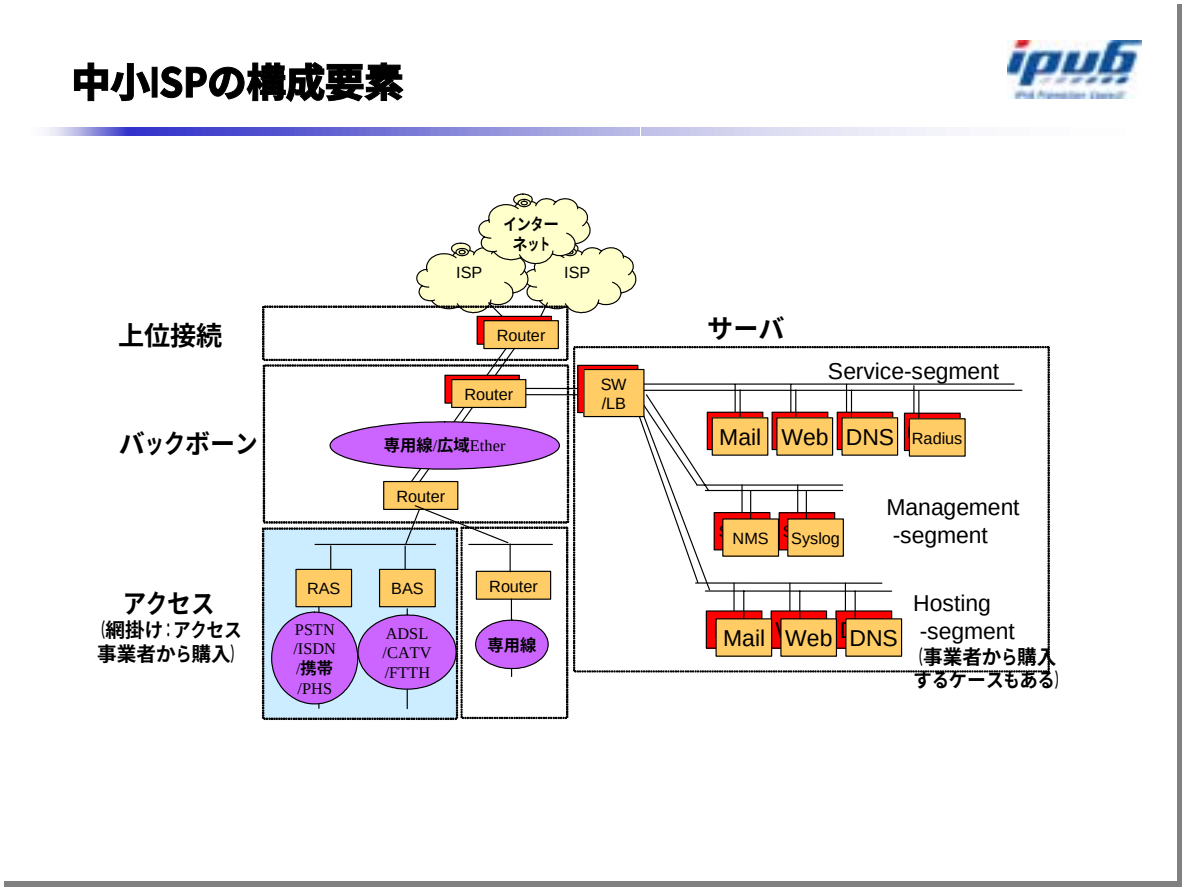
サービス内容

IP コネクティビティ、アプリケーション（ASP）、運用管理代行（MSP）

このドキュメントでは、以下のような特徴を持った、一般的な中小 ISP を対象として議論を進めます。

・構成要素の一部を他事業者から購入し、一般コンシューマを顧客としている（リテール）
・全国規模まではいかない準大手（ナショナル～リージョナル）
・IP コネクティビティと基本的なアプリケーション（DNS、Web、電子メール）を提供

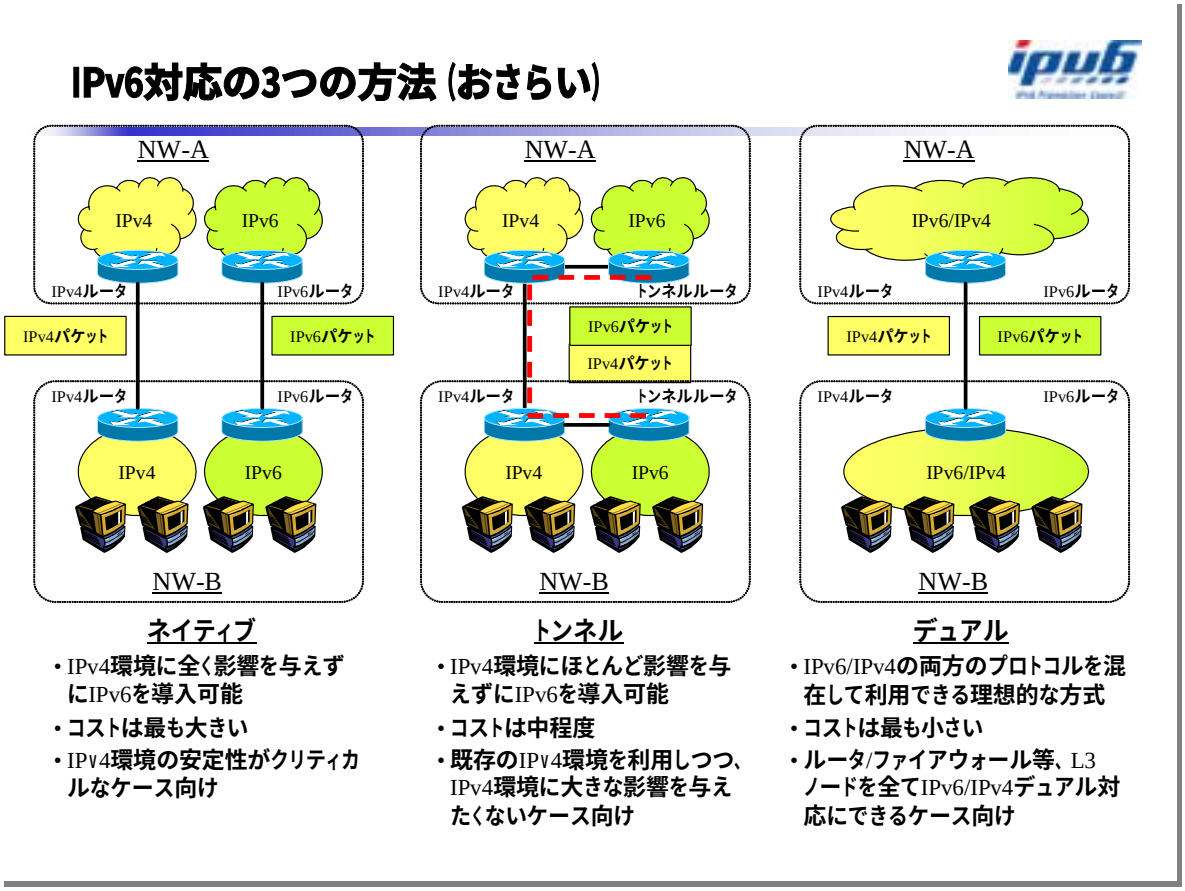
■中小 ISP の構成要素



一般的な中小 ISP のネットワーク構成は、図のようになっています。ダイヤルアップ、ADSL、FTTH といったアクセスサービスについては、アクセス事業者から購入し、ユーザからの直接専用線接続とともに、専用線や広域イーサネットで構成された自社のネットワークバックボーンにつなぎこみ、これを上位の ISP 経由でインターネットに接続しています。

バックボーンにはサーバセグメントを接続、このサーバセグメントは、サービス全体を対象とした DNS、電子メールサーバ、Web サーバを配置したサービスセグメント、さらにネットワーク管理システムや syslog サーバを配置した管理セグメント、そしてユーザに対するホスティングサービスのための Web サーバ、電子メールサーバ、DNS を運用するホスティングセグメントで構成されています。

■IPv6 対応の 3 つの方法（おさらい）



IPv6 対応の接続方法には、ネイティブ、トンネル、デュアルの 3 種類があります。ISP における IPv6 対応とは、この 3 つの手法のうちいずれか（または複数）を使って、上位接続、自社バックボーン、ユーザとの接続について、IPv6 通信を実現することです。

ネイティブは、IPv4 環境に全く影響を与えずに IPv6 を導入可能ですが、ISP にとっての移行コストは 3 つのうち最大となります。これは、IPｖ4 環境の安定性がクリティカルなケース向けと言えます。

トンネルでは、IPv4 環境にほとんど影響を与えずに IPv6 を導入可能です。コストは中程度で、既存の IPｖ4 環境を利用しつつ、IPv4 環境に大きな影響を与えたくないケース向けです。

デュアルは IPv6/IPv4 の両方のプロトコルを混在して利用できる理想的な方式で、コストは最も小さいと考えられます。しかし、ISP 内部で使われるルータ/ファイアウォール等、L3 ノードを全て IPv6/IPv4 デュアル対応にする必要があります。

■中小 ISP にとっての IPv6 移行とは

では、中小 ISP における IPv6 移行とは、何を意味するのでしょうか。まず、中小 ISP が IPv6 に移行する動機としては、

・先進サービスへの早期対応
・利用者ニーズへの対応
・国家施策、ISP 業界動向への対応

が考えられます。これを前提とすると、移行に際しては、IPv6 サービスでこれまでの IPv4 サービスを置き換えていくのではなく、IPv6 サービスを新サービスとして追加するという考え方が自然です。つまり、IPv6 をつかった新サービスがよいものであれば、ユーザは自然にそちらに移行していくはずです。つまり、ダイヤルアップから ADSL などの常時接続や、一般電話から一般電話と IP 電話の混在へとユーザが移行してきたのと同様な現象が起こるはずです。

新サービスとして IPv6 サービスを中小 ISP が始める際には、以下のような点が課題となります。まず、IPv6 サービス関連コストです。このコストとしては、オペレーションコスト、機器のアップグレードコスト、ユーザサポートコストなどが代表的です。既存の IPv4 サービスに対する悪影響が発生すれば、これもコストとなります。IPv6 関連の市場が、近い将来にかなりな規模になることは疑いのないところですが、現状では単独のサービスとしての IPv6 サービスがいつコスト回収するかを予測するのは難しく、この点から中小 ISP としてはスモールスタートをすることが望ましいと考えられます。

さらに間接コストとして、新サービスのための人材やノウハウといったリソースが必要となります。特に中小 ISP は少人数で運用しているケースが多く、実験サービスなどを通じて本格的なオペレーションに必要な人材の育成やノウハウの蓄積を進めたり、場合によっては他社のアウトソーシングサービス利用を考える必要が生じるでしょう。

2. BCP（今すぐ出来ること）

■BCP の範囲と検討方針

以下では、中小 ISP がすぐ自力で実現可能な実験あるいは商用の IPv6 サービス提供方法について解説します（「自力」とは中小 ISP が現状、世に出回っている技術、製品、サービスを使ってできる範囲を示しており、標準化されてない技術、世に出ていない製品等、一般的に中小 ISP が独自の力で行えない方法は対象外としています）。

提供する IPv6 サービスとしては、コネクティビティ、DNS、Web、メールを想定し、IPv4 サービスへの影響、コスト面の合理性を考慮しながら、考えられる選択肢のそれぞれにつき、メリットとデメリットを解説します。

■IPv6 コネクティビティサービス（商用、実験）の現状

現在、IPv6 対応接続サービスはおよそ以下のように行われています。

ISP サービス

・専用線（ATM、STM）：ネイティブ、デュアル、トンネル
・LAN（DC）：トンネル、ネイティブ
・ADSL：トンネル、デュアル
・FTTH：トンネル
・CATV：デュアル（実験）、ネイティブ（実験）
・無線 LAN：デュアル（実験）
・ダイヤルアップ：デュアル（実験）

IX

・DIX-IE（実験）、JPIX（実験）、JPNAP6（実験）

中小 ISP の IPv6 対応では、主に以下のような点を検討する必要があります。

アドレッシング

・取得アドレス
・割り振り/割り当て

ルーティング

・EGP
・IGP

ネットワーク接続

・上位接続
・バックボーン
・アクセス

サーバ

・サービスサーバ
・インフラサーバ
・運用管理サーバ

■アドレッシング

(1) アドレスの初期割り振りサイズ

用途

ISP において、IPv6 アドレスは、IPv4 と同様に、以下のような 2 つの用途で利用されます。

・顧客に対して配布するアドレス空間（ユーザ用）
・自ネットワーク運用管理のためのアドレス空間（インフラ用）

取得アドレス空間

ISP による取得が考えられる IPv6 アドレスには、以下の 2 通りがあります。次ページ以降で説明するように、この 2 つの選択肢から、自社ネットワークの規模、接続要件、運用管理のしやすさ等を考慮して選択することになります。

	サイズ	取得手段
sTLA	最小割り振り/32（/35）	APNIC からの割り振り（JPNIC は申請取次実施）
NLA	/33～ /47	sTLA、NLA 保有者から割り振り

お断り：現在 sTLA、NLA という表記は行われていませんが、これらに代わる用語が存在しないため、ここでは便宜上使用しています。

(2) sTLA、NLA の比較

sTLA、NLAの比較

	sTLA	NLA
BGP4+	●インタネットとの経路制御が可能（マルチホーム） ▲取得申請に一定の条件 ▲下位ISP含め/48登録義務 ▲取得空間のDNS逆引き管理義務	●上位ISPの配布条件によっては取得、運用は容易 ●Peer（隣接ISPのアドレス空間に対する経路の交換）は可能 ▲インターネットとの冗長性経路の確保は制限を受ける ▲sTLAへの移行工数大
nonBGP4+	●運用が簡単（後にBGP4+も可能） ▲取得申請に一定の条件 ▲インターネットとの冗長性経路の確保が困難 ▲下位ISP含め/48管理義務 ▲取得空間のDNS逆引き管理義務	●上位ISPの配布条件によっては取得、運用は容易 ●運用が簡単 ▲インターネットとの冗長性経路の確保が困難 ▲sTLAへの移行工数大

- sTLAを取得/運用するハードルは高くなく、中小ISPもsTLAを取得するケースが一般的となるであろう

sTLA と NLA の違いは表の通りです。

sTLA は NLA と比較した場合、経路制御の自由度という点で大きなメリットがあります。また、sTLA を取得/運用するハードルは高くないことから、中小 ISP も sTLA を取得するケースが一般的となるであろうと考えられます。

(3) アドレス取得条件

sTLA のアドレス取得

sTLA のアドレス取得条件は、RIR のアドレスポリシーに定められています。現在のポリシーは、全 RIR にほぼ共通ですが、APNIC を例とすると、以下のような条件となります。

・APNIC 会員、もしくは JPNIC アドレス管理指定事業者であること

・APNIC アドレスポリシーに合致すること

このアドレスポリシーでは、IPv6 アドレス（sTLA）の初期割り振り資格を次のように定めています。

a) LIR(Local Internet Registry, いわゆる ISP のことを指す)であること

b) エンドサイトでないこと

c) /48 を割り当てた組織に対し, IPv6 インターネットへの接続性を 提供する計画があること。その際、インターネットに対する経路 広告は、割り振られたアドレス一つに集成すること。

d) 2 年以内に最低でも 200 の/48 の割り当てを行う計画があること。

NLA のアドレス取得

NLA のアドレスは、以下のように基本的には割り振りを行う上位 ISP（/32 保有 ISP 等）の裁量にまかされていて、その ISP の割り振りポリシーを満たすことが条件となります。一般的には次のようになります。

・通常、上位 ISP の IPv6 接続サービス利用とセットになる
・割り振られるアドレス空間は、上位 ISP のポリシーによるが、1 年後（及び 2 年後）の /48 予定数に基づくケースが多い
・割り振られるアドレス空間、接続要件など勘案して上位 ISP を決定する

(4) sTLA での経路制御方法

sTLA を取得した場合、上位との経路制御については BGP4+の利用とスタティックルーティングの 2 つの選択肢があります。BGP4+を使うと、IPv6 インターネットとの経路制御が可能となります。上位 ISP が 1 つの場合はスタティックルーティングで十分ですが、将来の BGP4+運用への準備をしておくことも必要です。

(5) sTLA 保持者の義務

顧客へのアドレス割り当て報告

sTLA を取得した場合、エンドユーザ顧客には通常/48 のアドレス空間を割り当てますが、その際には、APNIC にその情報を登録する義務が生じます。APNIC への/48 割り当て報告は、メールによって行います。Tech-c、Admin-c のための Person Object、および inet6num Object を登録します。

(6) sTLA 空間 DNS 逆引き

また、sTLA 保持者には、取得した sTLA の DNS 逆引き空間を管理する義務が生じます。

(7) NLA 取得方法

NLA のアドレスは、上位 ISP(sTLA 、NLA) より取得します。 アドレスの割り振りは、通常､上位 ISP の IPv6 接続サービス利用とセットになります。IPv6 接続における上位 ISP は、IPv4 の上位 ISP と同一である必要はありません。

割り振られるアドレス空間の大きさは、上位 ISP のポリシーによりますが、割り振り対象者の 1 年後（及び 2 年後）の/48 予定数に基づくケースが多く見られます。 割り振られるアドレス空間、接続要件など勘案して上位 ISP を決定するのがよいと考えられます。

(8) NLA での経路制御方法

NLA の場合、IPv6 インターネットへの接続性は、NLA を取得した上位 ISP から取得します。

現状日本ではインターネット全体の経路集約の観点から、多くの AS で/35 より長い prefix のフィルタが一般的に行われています。なお、IPv6 実験ネットワーク 6bone の運用規則を定めた RFC2772（6Bone Backbone Routing Guidelines）ではパンチングホールを禁止しています。

ルーティングについても、上位 ISP のポリシーによって異なります。上位 ISP へのデフォルト経路をスタティックで設定する場合と、BGP4+で IPv6 フル経路を受領できる場合があります。インターネットエクスチェンジ（IX）やプライベートピアリング経由で、特定の ISP に対する経路の冗長化は可能です。将来 AS 間の暗黙のコンセンサスが崩れれば、パンチングホールによる経路数肥大の影響が危惧されます。

(9) NLA から sTLA への移行

当初 NLA でスタートした ISP が sTLA に移行する契機としては、経路の安定性からマルチホームを導入する場合と、NLA のアドレス消費が進み、より大きなアドレス空間（sTLA）が必要になった場合が考えられます。

移行は、たとえばまず sTLA を取得、次に上位 ISP、IX との接続、および sTLA 経路広告を行い、リナンバリング作業を実施します。この際、自社のネットワークだけでなく顧客サイトにおいてアドレス移行作業が生じます。具体的な作業については Tips を参照してください。

(10) アドレッシング手法

取得したアドレスの構成に際しては、以下の 3 つの要素を考える必要があります。

・顧客へのアドレッシング
・ネットワークインフラにおけるアドレッシング
・サーバセグメントにおけるアドレッシング

顧客へのアドレッシング

エンドユーザ顧客に対するアドレスの割り当ては、RIR(APNIC)の IPv6 アドレスポリシー（http://ftp.apnic.net/apnic/docs/ipv6-address-policy）に準拠して行ってください。このアドレスポリシーでは、原則的に 1 接続に対して/48 を割り当てることとなっていますが、顧客環境が 1 セグメントのみの場合に/64 を割り当てたり、1 端末のみの場合には/128 を割り当てることも選択肢として記述されています。現状の IPv6 接続サービスでは、(ADSL 等) コンシューマ向け接続は/48 あるいは/64 の割り当てが一般的となっています。

留意点としては、/48 の場合には RIR への whois 登録が必要であること、一方/64 の場合、エンドユーザへの追加割り当て処理の頻度が増すこと、確保するアドレス予備空間によっては経路集成が難しくなること、等があげられます。

ネットワークインフラにおけるアドレッシング

IPv6 では、IPv4 と比べ、アドレス空間が広大であるため、容易で余裕を持ったプランニングが可能となります。まず、ホスト数を意識する必要がなく、サブネットはすべて/64 で構成するのが一般的です。この他、ISP では、インフラ用として POP 毎に/48 を割り当てることができます。全般的に、アドレス利用効率より、ISP 内部経路の集成を優先して考えることができます。

sTLA（/32）の場合 7132 個の/48（利用率 10.9%)を割り当てれば、追加割り振りを受けられます（HD-Ratio（利用率 0.8 の場合）より)。

ISP は/48 単位で APNIC データベースに登録する必要がありますが、登録数が HD-Ratio：0.8 を超えれば、申請によりただちに、アドレス空間が 2 倍となる追加割り振りが受けられます。

顧客用アドレスも経路集成が行えるように、接続 POP 毎に集約してアサインすることが望ましいと考えられます（IPv4 と考え方は同じ)。当初、センタのサーバで顧客向けトンネルを終端するケースでは、顧客がデュアルサービスに移行する（エッジへ収容替え）際のリナンバを考慮しておく必要はあります。

サーバセグメントにおけるアドレッシング

サーバセグメント用のアドレス空間確保では、1 つの LAN セグメントに対して、/64 を割り当てます。将来予想される使われ方（ソースアドレス選択等）に対応できるよう、1 つの LAN セグメントに複数の/64 を確保するのもよいと考えられます。

■ルーティング

(1) EGP

EGP には BGP4+を利用します。フルメッシュ、ルートリフレクタ、コンフェデレーション等、IPv4 BGP と同じ技術の使用が可能です。

(2) BGP ルーティングトポロジー

外部接続(eBGP)では、プロトコル毎に回線を分ける（IPv6 ネイティブリンクを追加）か、デュアルセグメント上で IPv4、IPv6 それぞれ別のルータでピアリングするかについては、接続先のポリシーに従います。内部接続(iBGP)におけるピアトポロジーも IPv4 のそれとは独立にできます。

中小 ISP の場合、特殊な事情を除き IPv6/IPv4 とも同一の AS が一般的ですが、仮に異なった場合、ルータによっては同一ルータで 2AS の BGP プロセスが起動できない場合があります。

(3) BGP Peer

BGP Peer については、次の 2 点に注意が必要です。

NLRI （Network Layer Reachability Information）の受領

到達性情報を他のプロトコルに依存するべきではないという理由から、IPv6 NLRI を IPv4 Peer で扱わないことをお勧めします。 つまり、IPv4 ルーティングは IPv4 アドレスで Peer し、IPv6 ルーティングは IPv6 アドレスで Peer すべきです。

Peer アドレス

Peer アドレスは、グローバルアドレスとリンクローカルアドレスが考えられます。eBGP では、基本は IX、接続先のポリシーに従うべきですが、アドレスポリシーでは、IX に non-routable な IX 用グローバルアドレスを割り当て可能であることが決まっています。eBGP の仕様上、リンクローカルアドレスでの安定動作が難しい場合があるため、選択が可能な場合は、Global Address の利用を推奨します。

iBGP では、グローバルアドレスを使用します。

(4) BGP ルーティングポリシー

ルーティングフィルタについては、各ピアの設定にプレフィックスフィルタを導入し、s/pTLA 以外をフィルタアウトすべきです。また、AS Path フィルタを併用することが望まれます。6to4 プレフィックス（2002：：/16）は通しますが、/32 保有 ISP で/35 のパンチングホールは行わないようにすべきです。すでに利用廃止となったサイトローカルアドレスの通信は、念のため外部接続インタフェースにてフィルタリングすることが望まれます。

IPv6 におけるプレフィックスの正当性確認については、s/pTLA の情報を、各 RIR あるいは 6bone のデータベースにて確認します。

上位 ISP からの経路受領

IPv6 フル経路の受領は、上位 ISP の IPv6 接続サービス（商用、実験）の利用か、WIDE 等の実験研究組織との接続によって実現できます。経路の安定性の点から、一定の接続サービスレベルを保ちたい場合、1 つは商用の IPv6 サービスの利用を推奨します。

(5) IGP

IGP の選択肢としては、OSPFv3、i/IS-ISv6、RIPng、Static がありますが、コアとなる IGP は、IPv4 と同様に Link State 方式の動的ルーティングを推奨（OSPFv3 は既に大手 ISP での運用実績もある）します。

Link State 方式では、経路収束が早い、経路集成が可能であるという 2 つの利点があるからです。ただし、初期導入（トンネルのみ）等の小規模のケースでは Static、RIPng 利用もありえます。まず Static か RIPng で始め、将来、HOP 数や扱うルータ台数が増えた場合に OSPFv3 へ切り替えることもできます。

(6) IGP の選択

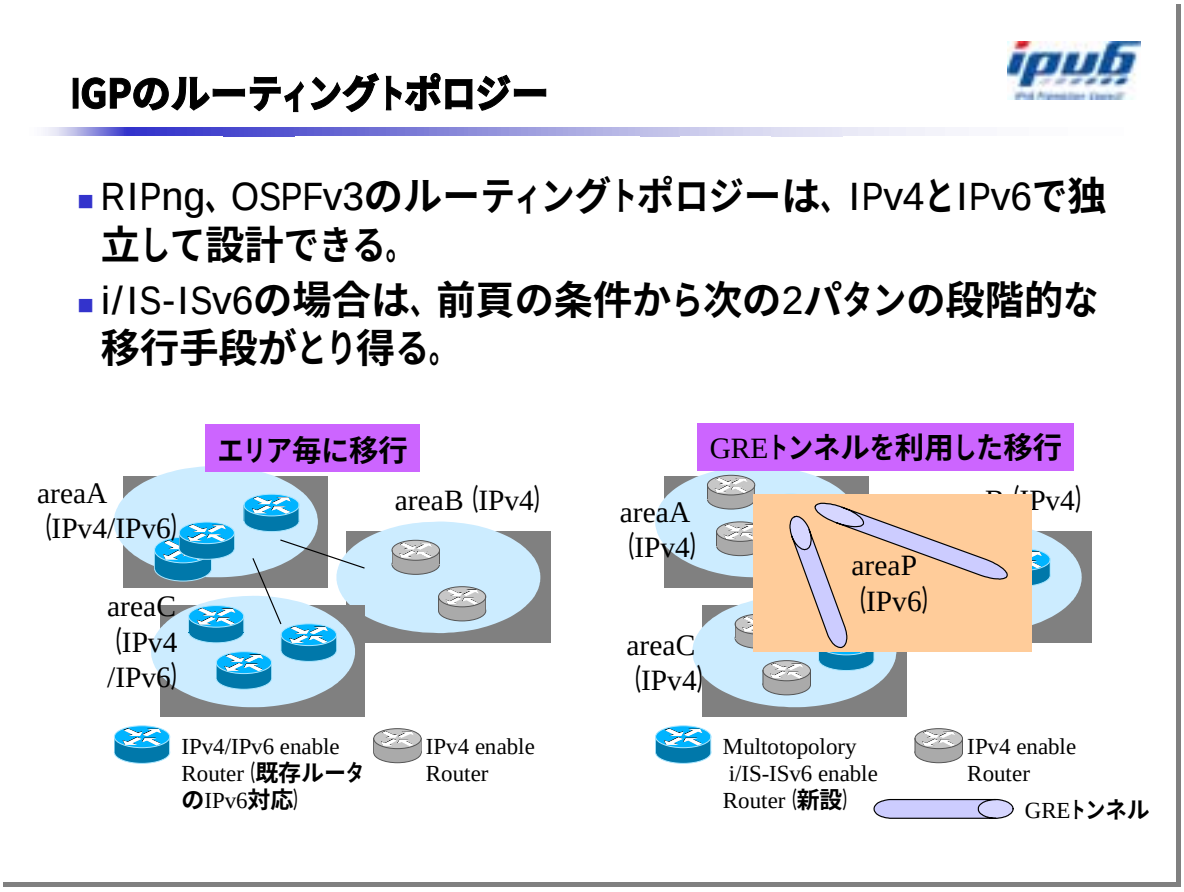
IPv6 における IGP の選択に関しては、IPv4 で使用しているプロトコルの IPv6 版を選ぶことが運用経験の観点でベターです。つまり IPv4 で RIP を使っている場合は RIPng を選択し、OSPFv2 を運用している場合は OSPFv3 を選ぶということです。

ただし、IPv4: i/IS-IS → IPv6: i/IS-ISv6 の場合、次の 2 つの制約があり、段階的な移行には向きません。

- 同一 area 内で、IPv6 ルーティングトポロジーと IPv4 ルーティングトポロジーとを独立させるためには、multitopology i/IS-IS の採用が必要（i/IS-IS を用いて IPv6 対応するためには、同一 area 内で動作している IPv4 の i/IS-IS ルータ全てを IPv6 でも動作させる必要がある）
- ルーティング情報のトランスポートが OSI プロトコルであるため、IPv6 over IPv4 トンネルでは扱えない。従って、GRE トンネル等 IP プロトコルに依存しないトンネル技術の採用が必要となるが、その場合、IPv6、GRE、IPv4 のトリプルスタック構成となりオーバヘッドが増加する。

これらが問題となるケースでは、IPv4: i/IS-IS → IPv6: OSPFv3 がよいと思われます。

(7) IGP のルーティングトポロジー



RIPng、OSPFv3 のルーティングトポロジーは、IPv4 と IPv6 で独立して設計できます。i/IS-ISv6 の場合は、前項の条件から、「エリア毎に移行」と「GRE トンネルを利用した移行」の 2 パターンの段階的な移行手段がとり得ます。

(8) エンドユーザとの経路制御

IPv6 では、IPv4 と比べエンドユーザがプレフィックスを持つケースが増えるため何かしらの経路制御が必要となりますが、ダイナミックルーティングを使用する場合、ユーザから広告される経路が ISP 内部に影響を与えないようフィルタする必要があります。

また、複数ユーザが共有するセグメント上で RA を使用する場合、あるユーザが誤って RA を出しても、他ユーザに伝播しないよう、スイッチやモデム等でフィルタする、もしくは完全な策ではありませんが、上位ルータでは router-preference を high に設定する必要があります。

■ネットワーク

(1) 上位接続

上位 ISP が提供するメニューは、以下のように分類できます。

接続方式：トンネル型、ネイティブ型、L2 共有型、デュアル型
ルーティングプロトコル：BGP4+、Static

上位接続用ルータの構成パターンは、IPv6 サービス専用、あるいは IPv4 サービスと v6 サービスで共用が考えられます。

なお、ここで言う「専用」の意味は、IPv4 サービスユーザのトラフィックを乗せないという意味であり、そのルータで IPv6 しか動かさないという意味ではありません。当面、ルータ管理（SNMP など）のため、IPv6 サービス専用ルータもデュアルスタックで動かすことにならざるをえません。

上位 ISP の提供メニューには、それぞれ以下の特徴があります。

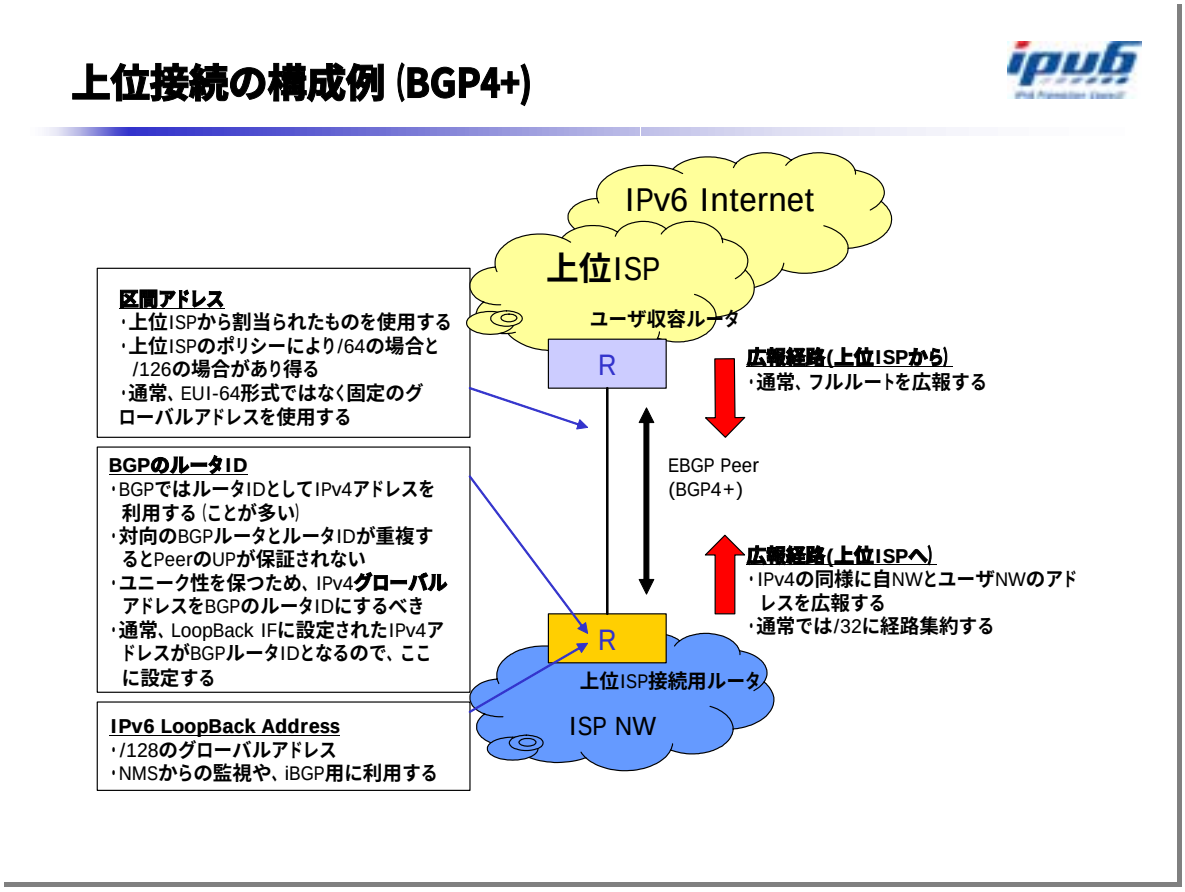
トンネル型、L2 共用型
IPv4 の付加サービスとして課金される場合が多い。

デュアル型
新たに回線は必要なく、IPv4 と IPv6 サービスを両方購入するより安い。

ネイティブ型
IPv6 用に回線が必要なため、上位 ISP との接続点が地理的に離れているとコスト高になる。

以上に加え、使用可能なルーティングプロトコル（BGP4+、Static）、料金、将来のメニュー変更への対応等を検討し、上位 ISP を選択することになります。

ISP 側の上位接続用ルータについては、上位接続ルータの不具合が既存サービスすべてに影響を及ぼすため、新サービス（IPv6）と安定運用が必須な既存サービス（IPv4）ではルータを分離しておいた方が運用上の安心感はある（デュアル型以外で可能）と言えます。IPv6 サービス専用のルータを設置する場合には、その設備投資がデメリットとして挙げられます。



中小 ISP における上位接続の構成例としては、図のようなものが考えられます。

(2) バックボーン

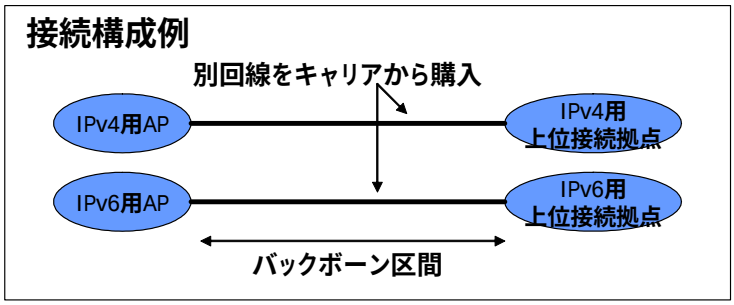
中小 ISP のバックボーンは、「上位接続ルータ設置拠点とアクセスポイントを接続する回線」と定義できます。ここでの「アクセスポイント」とは、アクセス回線業者との接続点を意味します。この場合、アクセスポイントにルータがあるとはかぎりません。中小 ISP では一般に、バックボーン回線を他の通信事業者から購入しています。最近では、広域イーサネットサービスを購入する場合が多く見られます。バックボーン用回線購入がバックボーン構築と同義となる場合もあります。

バックボーン構成は、別回線（IPv6 サービス専用）型、トンネル型、回線共用（L2 分離）型、デュアル型の 4 つに分類することが可能です。

①別回線（IPv6 サービス専用）型

別回線 (IPv6サービス専用) 型

- IPv6用に別回線を購入するパターン
- 別サービスのトラフィックの影響を受けない点がメリット
- 新たに回線を引くことになるので回線コストが高くなる点がデメリット



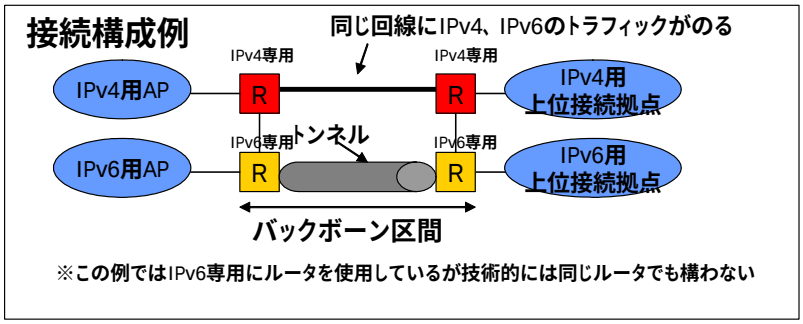
これは、IPv6 用に別回線を購入するパターンで、別サービスのトラフィックの影響を受けない点がメリットです。しかし、新たに回線を引くことになるので回線コストが高くなる点がデメリットとなります。

②トンネル型

トンネル型

- 従来からよく言われている移行時の構成だが、中小ISPを対象とした場合には次のような問題点がある

問題点
・中小ISPではアクセスポイントにルータがあるとは限らない
・ルータがあったとしてもIPv6対応とは限らない
・運良くIPv6対応にできるルータがあったとしても既存サービスへの影響を見積もる必要がある
・APの数にもよるが、トンネル用のルータを新設するにはそれなりの設備投資が必要



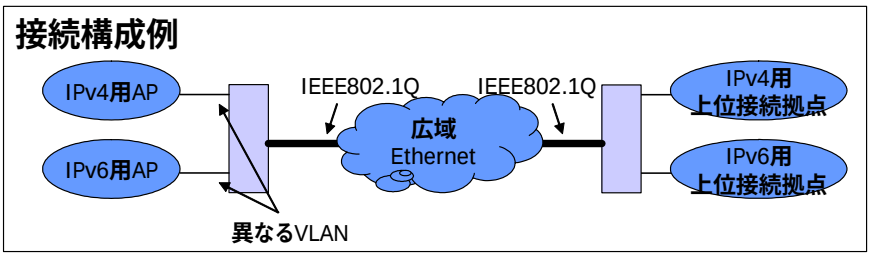
従来からよく言われている移行時の構成ですが、中小 ISP を対象とした場合には次のような問題点があります。

・中小 ISP ではアクセスポイントにルータがあるとは限らない。
・ルータがあったとしても IPv6 対応とは限らない。
・運良く IPv6 対応にできるルータがあったとしても既存サービスへの影響を見積もる必要がある。
・アクセスポイントの数にもよるが、トンネル用のルータを新設するにはそれなりの設備投資が必要。

③回線共用（L2 分離）型

回線共用（L2分離）型

- L2の技術を利用しIPv4の既存サービスとIPv6サービスを論理的に分離する
  - EthernetではVLAN、ATMではVP/VCなどを利用する
- バックボーン用回線をIPv4サービスとIPv6サービスで共用することにより回線コストを低くおさえられる

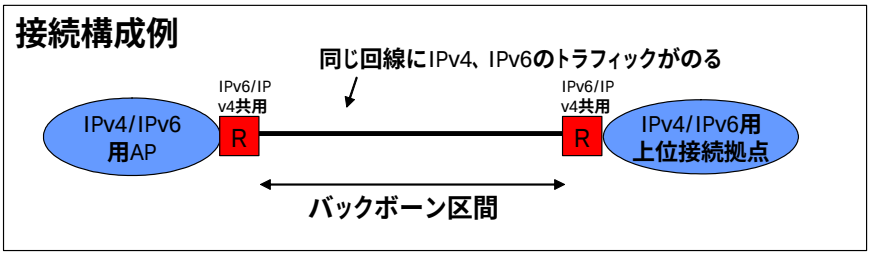


レイヤ 2 の技術を利用し IPv4 の既存サービスと IPv6 サービスを論理的に分離するもので、イーサネットでは VLAN、ATM では VP/VC などを利用します。バックボーン用回線を IPv4 サービスと IPv6 サービスで共用することにより、回線コストを低く抑えられるメリットがあります。

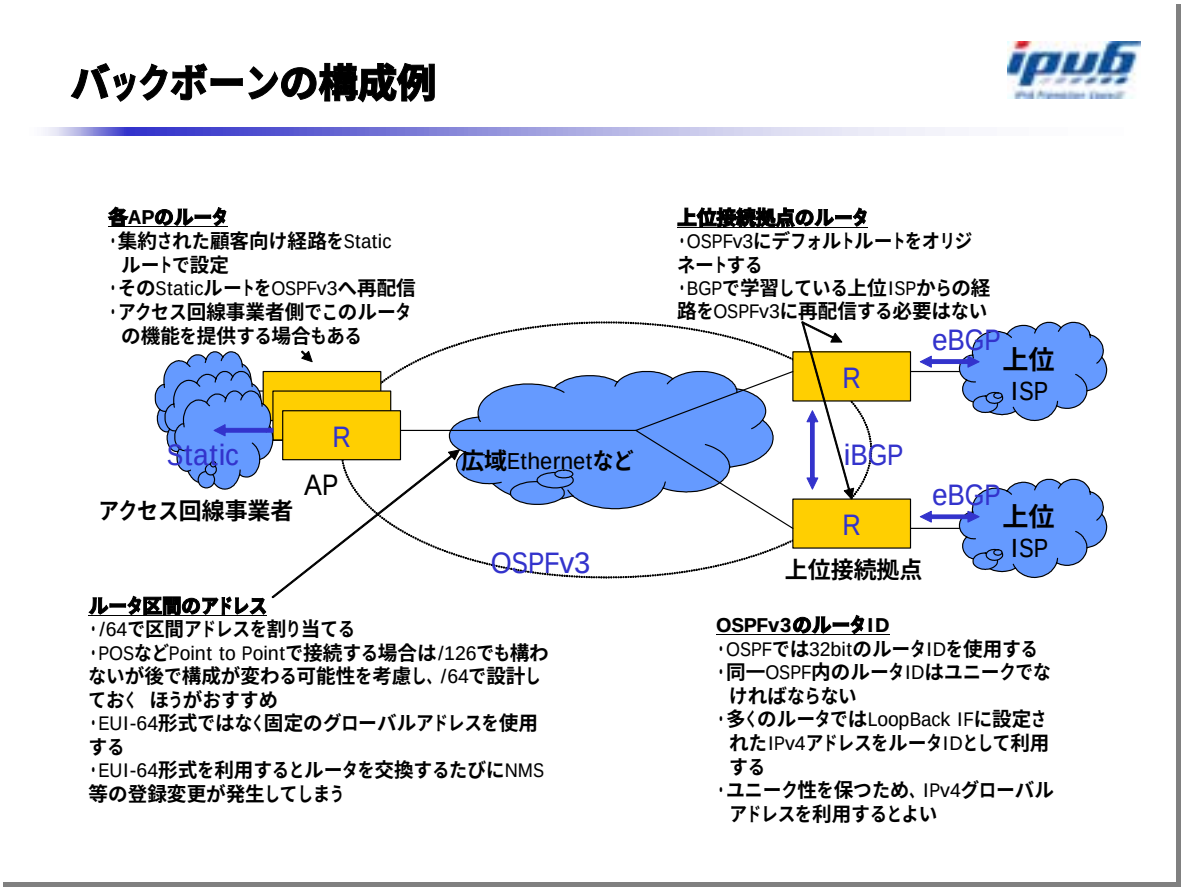
④デュアル型

デュアル型

- IPv4サービスとIPv6サービスの統合
  - バックボーン回線を共用でき回線コストを下げられる他、ルータも共用するため最もコストメリットが高い
- IPv4サービスへの影響が危惧されるが、大手ISPの一部ではこの構成が始まっている
  - ただし、中小ISPの場合APにルータがあるとは限らないため、この構成が無理なケースもある



IPv4 サービスと IPv6 サービスを統合的に提供するものです。バックボーン回線を共用でき回線コストを下げられるほか、ルータも共用するため最もコストメリットが高い方法です。IPv4 サービスへの影響が危惧されますが、大手 ISP の一部ではこの構成が始まっています。ただし、中小 ISP の場合、アクセスポイントにルータがあるとは限らないため、この構成が無理なケースもあります。



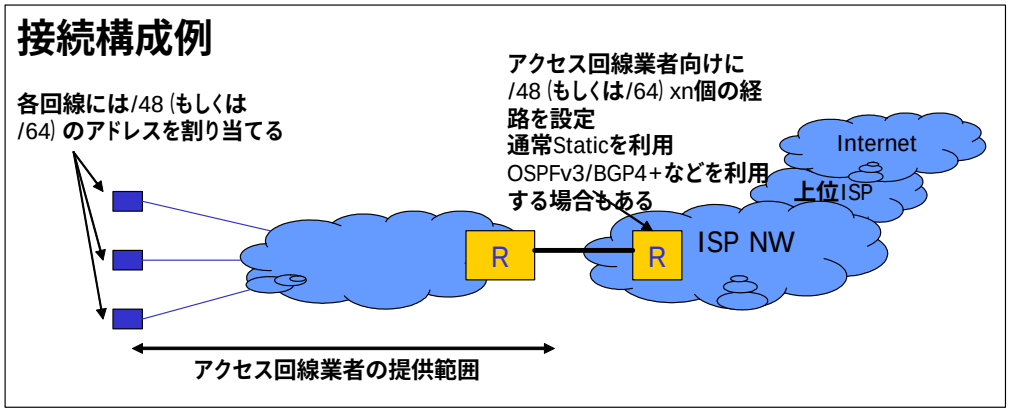
中小 ISP におけるバックボーンの構成例としては、図のようなものが考えられます。

(3) アクセス

中小 ISP が提供する IPv6 サービスのアクセス回線としては、ADSL や FTTH、ダイヤルアップなどが想定されます。中小 ISP では、これらをアクセス回線事業者から購入しサービスを提供する形態が一般的となっており、本ドキュメントでも、この形態を対象として扱います。

アクセス回線業者との接続

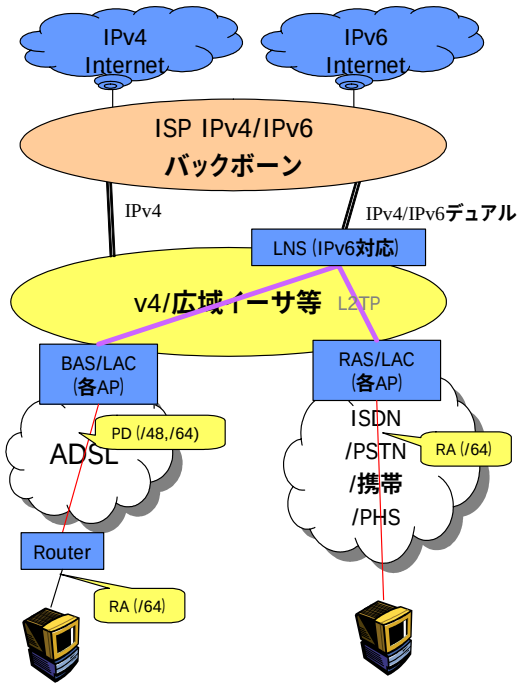
- 各アクセス回線（PPP等）はアクセス回線事業者のNW内で終端するモデルが主流になると予想される
- PPP等をISP側で終端するモデルはレアケースとした



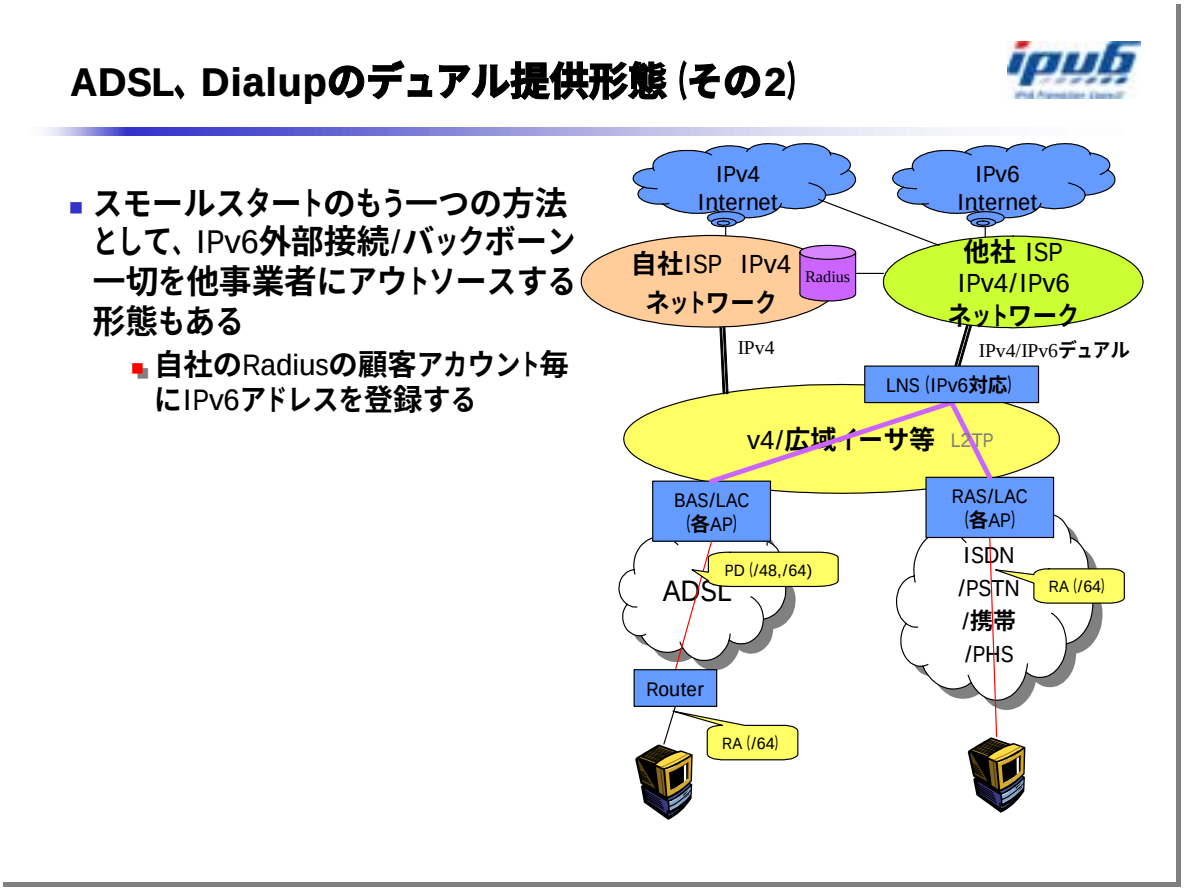
今後、各アクセス回線（PPP 等）はアクセス回線事業者のネットワーク内で終端するモデルが主流になると予想されます。PPP 等を ISP 側で終端するモデルはレアケースとしました。

ADSL、Dialupのデュアル提供形態（その1）

- 現状、アクセス回線事業者の各APにあるBAS/RASからL2TPでIPv6対応のLNSに集約するケースが一般的である
  - 各APのBAS、RASをIPv6対応する必要が無いため
- 中小ISPは、従来同様、アクセス回線事業者とデュアル接続することで、ADSL、ダイヤルアップのデュアルサービスが提供可能である



現状の IPv6 対応では、アクセス回線事業者の各アクセスポイントにある BAS/RAS から L2TP で IPv6 対応の LNS に集約するケースが一般的です。これは、各アクセスポイントの BAS、RAS を IPv6 対応する必要がないためです。中小 ISP は、従来同様、アクセス回線事業者とデュアル接続することで、ADSL、ダイヤルアップのデュアルサービスが提供可能となります。



スモールスタートのもう 1 つの方法として、IPv6 外部接続/バックボーン一切を他事業者にアウトソースする形態もあります。この場合、自社の Radius の顧客アカウント毎に IPv6 アドレスを登録します。

(4)トンネルでの提供形態

IPv6 over IPv4 トンネル

IPv4 固定グローバルアドレスが必要となる分、全体のサービス料金は高めとなります。しかし、数多くの ISP で提供済みで、１台のトンネルサーバを用意するだけで、比較的安価かつ簡単に提供可能となります。

DTCP（Dynamic Tunnel Configuration Protocol）

IPv4 動的アドレスでの利用が可能で、認証機能が備わっています（Radius を用い既存アカウントとの連携が可能）。すでに、IPv4 ISP フリーで提供中の ISP があります。1 台のトンネルサーバを用意するだけで、比較的安価かつ簡単に提供可能です。

■サーバ

(1) サーバの分類

ISP におけるサーバは、以下のように分類できます。

サービスサーバ

利用者が実際に使用するアプリケーションサーバで、Web、メールなどがあります。用途に応じて種々のカスタマイズが施されており、たとえば、ISP 広報用 Web、ホスティング、接続サービスにバンドルされる Web やメールなどがあります。

インフラサーバ

サービス利用にあたり共通的に必要となるサーバで、DNS や Radius がこれにあたります。最も信頼性が要求される部分です。

運用サーバ

ISP 運用に必要となるサーバで、NMS、SNMP などです。利用者が直接アクセスする対象ではなく、IPv6 対応は必須ではありません。

(2) サーバの IPv6 対応

現在の、サーバの IPv6 対応状況としては、まずサーバとして使用されている OS の多くは、デュアルスタック構成可能（Linux, FreeBSD, Solaris 等）です。アプリケーションについては、既存の IPv4 アプリケーションの殆ど（Web、メール、DNS 等）が IPv6 対応を完了しています。DNS、Web に関しては、ISP の商用・実験サービスでの提供実績がすでにあります。

(3) IPv6 対応手法

サーバの構成方法としては、IPv4 サービスサーバのデュアル化、IPv6 サービス専用サーバの新規追加の 2 通りが考えられます。デュアル化により IPv4 パフォーマンスに影響が払拭できないケースでは後者を選択します。デュアル化の際、OS、アプリのバージョンアップによりサービス断の影響が大きい場合も同様です。

サーバは、IPv6 サービス専用の新規デュアルセグメントに設置します。これは、脆弱性等の対応速度が異なるであろう IPv6 サーバと IPv4 サーバを同一セグメントに収容した場合、IPv4 サーバに影響が及ぶ可能性があるからです。これは、バックボーンに比べるとそれほど大きなコスト要因ではありません。

IPv6 サーバセグメントでの ICMPv6 のフィルタリングには注意が必要です。IPv6 でのフラグメント処理は、中間ノードでは行わず、Path MTU Discovery（ICMPv6 type2 メッセージを使用）により、送信元端末が配送可能なサイズに分割するため、途中のルータで ICMPv6 type2 メッセージをフィルタしてはなりません。

(4) DNS

DNS の IPv6 対応には、IPv6 アドレスが解決できることと、それが IPv6 経由で実行できることの 2 つの側面があります。IPv6 での名前解決には、当然ながらホスト名から IPv6 アドレス（正引き、AAAA レコード）、IPv6 アドレスからホスト名（逆引き、ip6.arpa.ドメイン）の 2 つがあります。

利用する DNS 実装については、BIND9 を推奨します。BIND9 では、IPv6 を完全にサポートしています。商用提供により、実績も積まれています。ただし、BIND8 でも同じことは可能になりました。また、名前解決のみなら BIND4 でも OK（IPv4 経由）です。

ISP における IPv6 対応の方法としては、DNS はもっとも重要なサーバでサービス断は許されないため、IPv6 用に新規にデュアルサーバを 2 台用意します（プライマリ、セカンダリ）。リゾルバとゾーン管理は兼用でもかまいません。

これを IPv6 専用リゾルバとして提供します。IPv4 経由の問い合わせは既存のサーバを利用してもらいます。また、顧客の要望に応じて、逆引き委譲や、顧客の管理する DNS のセカンダリとしての提供も行ないます。

(5) Web

Web サーバは、ISP の広報用 Web、接続サービスにバンドルされる Web、Web ホスティングに分類されます。

ソフトウェアの対応については、Apache2.0 以降で標準対応済みで、ISP での利用実績もあります。

対応方法としては、まず ISP の広報用 Web から対応すべきです。DNS に比べるとクリティカルなものではないですが、安全性を重んじる場合にはデュアルスタックのサーバを新設します。Apache2.0 以降であれば既存のサーバをデュアル化する手もあります。

ISP サービスにバンドルされる Web と Web ホスティングのデュアル化はもう少し先になりそうです。これは、中小 ISP の場合、ホスティング事業者のサービスを利用しているケースが多く、そのホスティング事業者のデュアル化がまだだという事情によるからです。

自力による解決策として、新規にデュアルサーバを新設した場合が考えられますが、サーバの数が多く、コンテンツの移設に稼動がかかるほか、コンテンツのミラー、同期の仕組みも必要となり運用工数が増す問題が生じます。

一方、現実的な解として、デュアルスタック化したリバースプロキシの設置があります。これにより、IPv6 から IPv4 の既存サーバへのアクセスを提供することが可能となる他、コンテンツの移設も考慮しなくてよいため、IPv6 アクセスの少ない段階では良い解決策になります。

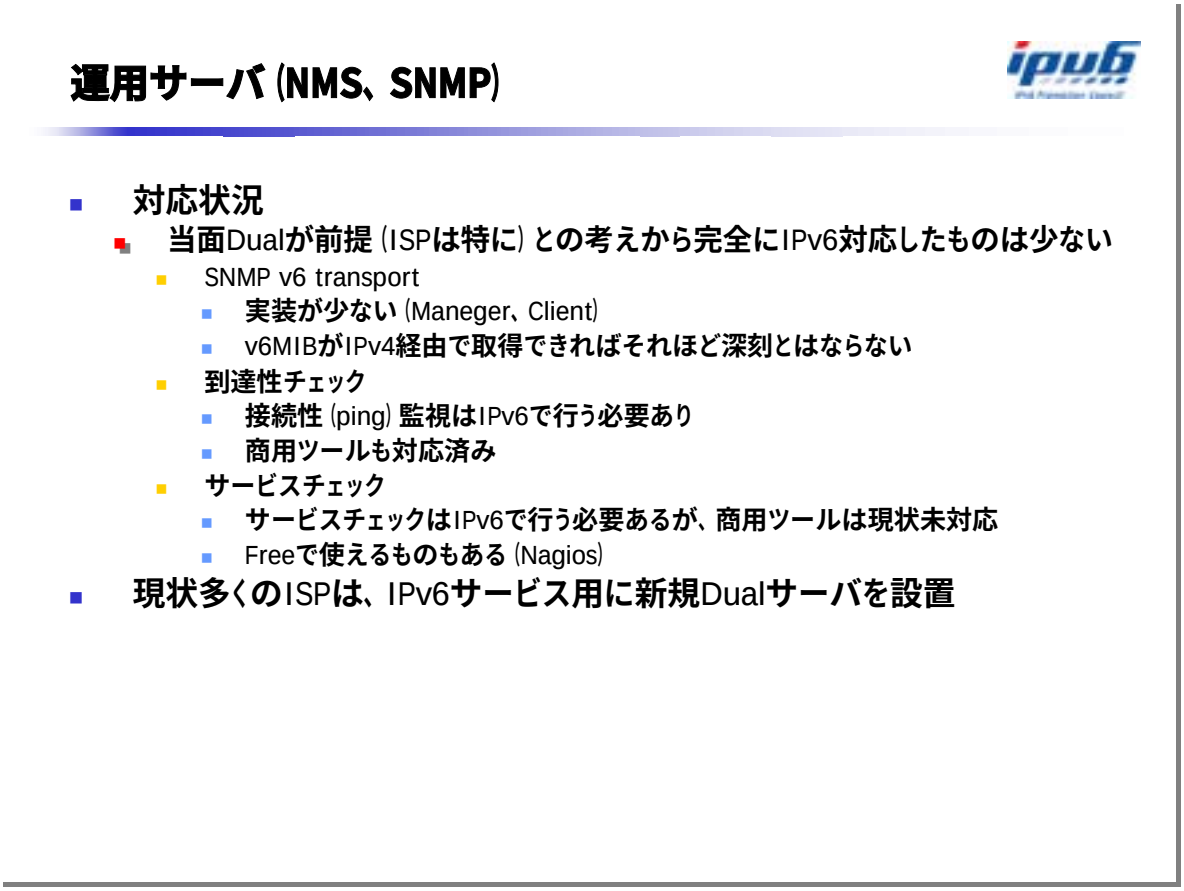
(6) Mail

メールサーバのソフトウェアについては、Sendmail8.1 以降で IPv6 に標準対応しています。Qpopper は IPv6 対応パッチで対応可能です。ただし、DNS、Web と比べ、利用実績は少ないと言えます。

現状の BCP としては、ウィルス駆除ソフトが IPv6 未対応であるため、ISP サービスとしての提供は控えるべきです。つまり、現状では、SMTP、POP サーバを IPv6 対応にしない、DNS の MX レコードのホスト名に IPv6 アドレスを持たせない、という対策を行います。

上記の問題がクリアされた場合の IPv6 対応方法としては 2 通りがあります。まず、既存のメールアカウントで行う場合、デュアルサーバを新設し、既存の IPv4 サーバのディスクを NFS 等で共有します。また、新たなメールアカウントを用いる場合、デュアルサーバを新設します。

(7) 運用サーバ（NMS、SNMP）



運用サーバ（NMS、SNMP）の IPv6 対応については、当面デュアルスタックネットワークが前提(ISP は特に)との考えから完全に IPv6 対応した製品は少ない状況です。特に SNMP の IPv6 トランスポートは、マネージャ、クライアントともに実装が少ない状況です。しかし、IPv6 MIB が IPv4 経由で取得できればそれほど深刻とはなりません。

到達性チェックについては、接続性（ping）監視は IPv6 で行う必要があり、商用ツールも対応済みです。

サービスチェックは IPv6 で行う必要がありますが、商用ツールは現状では未対応です。フリーで使えるものがあります（Nagios）。

現状の多くの ISP は、IPv6 サービス用に新規デュアルサーバを設置しています。

3. 5:5 のときの想定形態と課題

■5:5 のときの想定形態と課題

IPv4 と IPv6 の比率が 5 対 5 になる時期には、次のような状況と課題が考えられます。

機器のデュアル比率の増加

デュアルシステムとしての安定動作と、アプリケーションの IPv6 から IPv4 へのフォールバック動作が問題なく動作することが必要となります。また、現在 IPv4 でできて IPv6 でできていないことへの対策、つまり、DNS 自動検出方法、SNMP の IPv6 トランスポート対応、ウィルスソフトの IPv6 対応、Stateful な AutoConfiguration（DHCPv6）、エンドサイトのマルチホーム接続、PI アドレスによるマルチホーム接続、ICMPv6 のフィルタリングが課題になります。

IPv6 トラフィックの増加

ルータ、SW、IDS、FW、負荷分散装置の処理パフォーマンスの向上が求められます。

IPv6 オンリー機器の出現

IPv6 しか話さない機器が登場した場合には、IPv4 オンリー機器との通信の有無と、通信する場合の手法について確認する必要があります。また後述しますが、IP 電話の IPv6 移行も考えられます。トランスレータが必要となる場合、その種類と設置場所を考える必要があります。

nonPC 機器のインターネット利用

Zero-conf の内容整理と実現手段を考えるとともに、簡便なセキュリティ確保手段を生み出さなくてはなりません。

外から中へのアクセス

外から中へのアクセスでは、動的な穴あけプロトコルの標準化が望まれます。また、IPsec の相互接続性向上と、ISP によるセキュリティマネジメント手法の確立（後述）も求められている一つです。さらに、遠隔からのメンテナンスや計測に必要な、狭帯域ですが重要な制御系トラフィックの保護手法を見出す必要があります。

P2P トラフィックの増加

P2P トラフィックの増大に伴い、トラフィックコントロール手法（ファイル交換と IP 電話の区別など）が要求されるようになっていきます。

放送と通信の融合

家庭までのマルチキャストのデフォルト化に向けた段階的なプランを考える必要があります。また、ベストエフォートサービスとの品質差別化手法（QoS、ポリシールーティング（後述）等）も確立する必要が出てくるでしょう。

モバイル機器との IP 通信

特に、リンク変更時のシームレスな Mobile IPv6 の動作が求められます。

その他

名前解決技術（DNS、UPnP、SIP 等）とそれらの使い（分け）方や、Privacy Extension の使い方、運用過程で出てくる問題への ISP 間コンセンサスの形成（パンチングホールの基準確立やプロバイダエッジでの Ingres フィルタの推奨など）が課題となります。さらに、各セグメント（Home、Unmanaged、Managed）が想定する形態へ ISP としての対応が求められます。

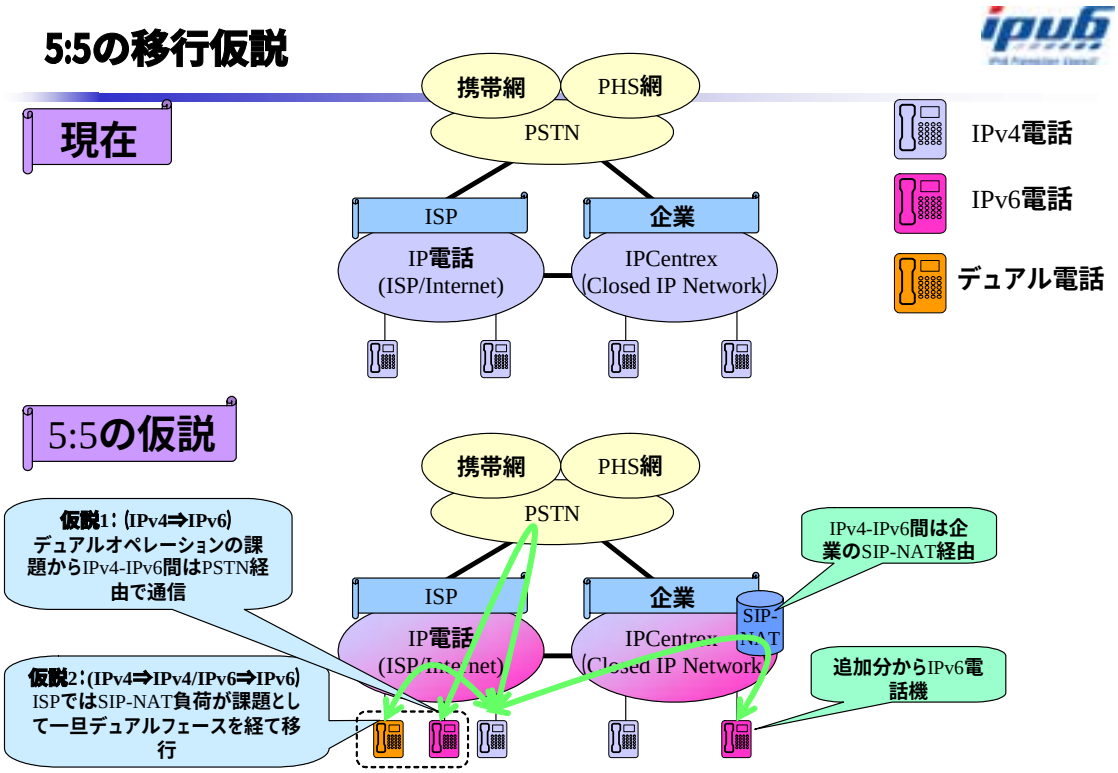
■IP 電話の IPv6 移行

IP 電話の IPv6 移行に関する ISP にとっての課題には、ISP の提供している IP 電話サービスの移行と、企業 IP Centrex との相互接続の 2 つがあります。

具体的には、まず IP 電話サービスの移行の過程でデュアル電話機は存在しうるかどうかにより、課題となる点が異なってきます。もしデュアル電話機が出たときには SIP サーバ、クライアント間のプロトコル選択のメカニズムとフォールバックを含めたオペレーションの信頼性は十分かという問題があります（下の図の仮説１参照）。

また、IPv6 オンリーの電話機が出たときには、IPv4 機器との接続方法をどうするかという問題があり、特に SIP-NAT などのトランスレータが負荷に十分耐えられるかという点が課題になります（下の図の仮説 2 参照）。

ただし、現状中小 ISP の多くが大手 ISP の IP 電話サービスを購入（SIP サーバをアウトソース）しており、中小 ISP が IP 電話の IPv6 移行を意識するケースは少ないと考えられます。



■セキュリティ

セキュリティ

- 想定される状況
  - アプリケーションによって、アクセス元の範囲が異なる。
  - アクセス元が固定アドレスとは限らない。
  - 異なるセキュリティレベルのものが同一LAN上に置かれる可能性が大きい。
  - 全ての機器がEnd-to-Endの認証･暗号機能を持っているわけではない。
- ISPに対する、何かしらのプレゼンス管理と動的で簡便な閉域性確保手段の提供要求は多い

	自分	家族	知人	契約者	第三者
個人ファイルサーバ	○	△	△	×	×
ビデオ予約	○	○	×	△	×
IP電話	○	○	○	○	○
ゲーム	○	○	○	×	△
エアコン操作	○	○	×	○	×

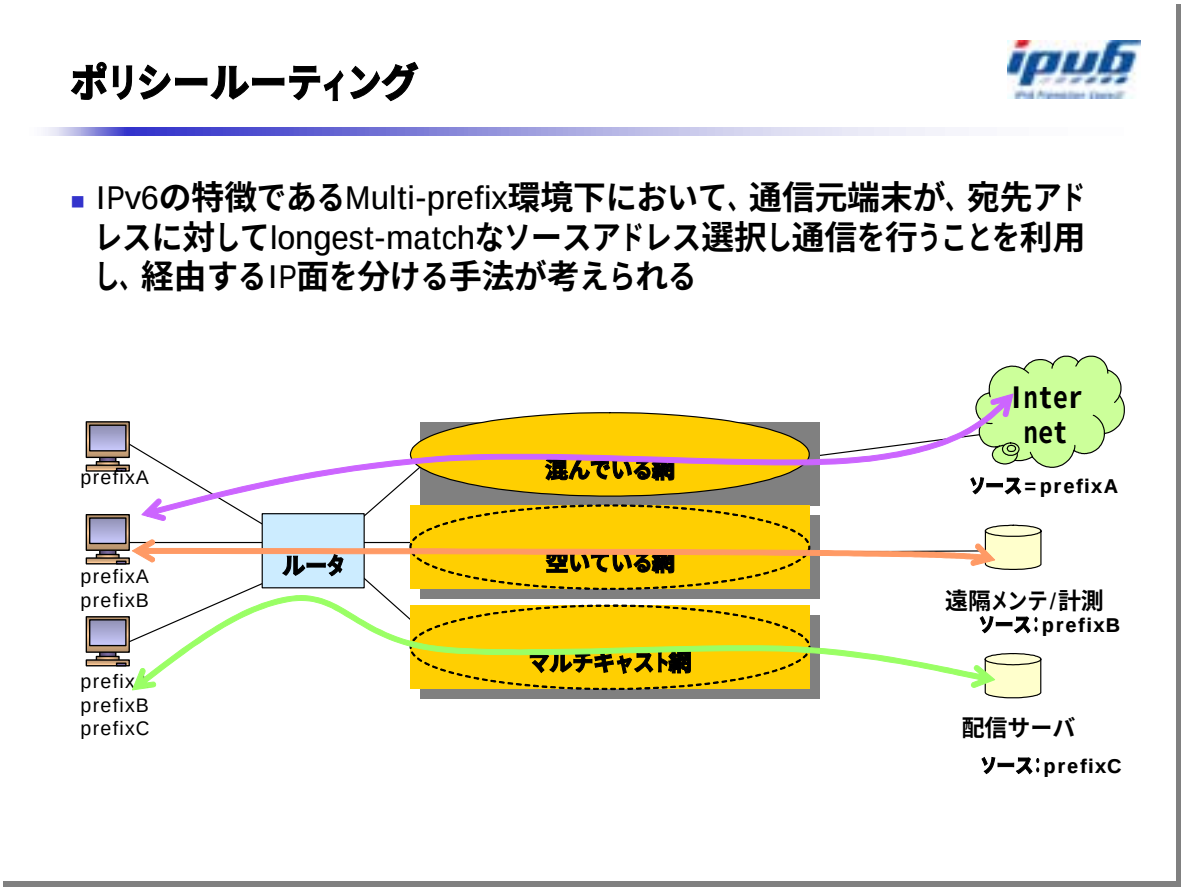
○許可
△ケースによる
×不許可

IPv6 のセキュリティに関しては、IPv4 と比べ以下のような点が明らかになってくると考えます。

・アプリケーションによってアクセス元の範囲が異なる。
・アクセス元が固定アドレスとは限らない。
・異なるセキュリティレベルのものが同一 LAN 上に置かれる可能性が大きい。
・すべての機器がエンドツーエンドの認証・暗号機能を持っているわけではない。

このような状況では、ISP における、何かしらのプレゼンス管理と動的で簡便なアクセス制御、閉域性確保の手段が強く要求されるようになるでしょう。

■ポリシールーティング



IPv6 では、各端末に、複数のネットワークプレフィックスを与えることができます。これによって複数のアドレスをもたせることが可能です。そして、宛先アドレスに対して longest-match なソースアドレスを選択し、通信を行うことが可能です。この仕組みは RFC3484 で規定されています。これを利用し、通信経路を分離選択することが可能になると考えられます。

4. Tips & Tricks

■アドレス関連

ルータ、サーバのアドレスは手動設定することをお勧めします。EUI-64 の利用によるアドレス自動構成では、NIC が変わるとアドレスも変わってしまうためです。

また、DNS 登録、フィルタリング設定の手間軽減のために、分かりやすいネーミングルールを考える手もあります。

・::1、::53、::80、::cafe など、0～9、a～f を自由に組み合わせてポート番号や名前を表現

・:c726:a00:3:82 で東京 03-広島 082 間の ATM リンクを表現するなど

ただし、こうした分かりやすいアドレスは攻撃対象になりやすいことも考慮したほうがよいと思われます。

■リナンバリング方法

同一インタフェースに複数の IPv6 アドレスが付与可能であることを利用して、新旧アドレスを共存させる過程を経たリナンバリングが可能です。

手順としては、まず新アドレスを取得、次に新アドレスで接続性(ルーティング)設定を行います。そして IPv6 ノード(ルータ及び端末)へ新アドレスを付与します。この際、旧アドレスも削除せずに付与しておきます。端末レベルではアドレス自動構成を使います。これと併せて、DNS 登録変更作業等を行います。次に、旧アドレスを削除し、旧アドレス接続性(ルーティング)を削除します。

上記の手順により、IPv4 のリナンバと比べ、サービス断の影響が少なく段階的なリナンバが可能となります。

■sTLA 取得方法

sTLA の取得に際しては、まず申請 Web を参照します。

http://www.apnic.net/services/ipv6_guide.html　(APNIC)
http://www.nic.ad.jp/ja/ipv6/index.html　(JPNIC)

次に各機関へ Web で申請します。APNIC 会員は APNIC へ、JPNIC アドレス管理指定事業者は JPNIC への申請となります。申請内容の確認作業終了後、2004 年 2 月現在、1 ヶ月前後で割り振りを受けることができます。

sTLA 割り当ての歴史的経緯

1999 年に定められた最初の sTLA への割り振りポリシーでは、初期の最小割り当てを/35 としていましたが、2002 年 7 月 1 日の改定により、これが/32 に変更されました。既存/35 取得の sTLA 保持者の/32 へのアップグレードは任意となっており、新ポリシー後も/35 を保持する sTLA が存在しています。したがって、現在は/32、/35 の sTLA が共存しています。

5. 付録（アクセス）

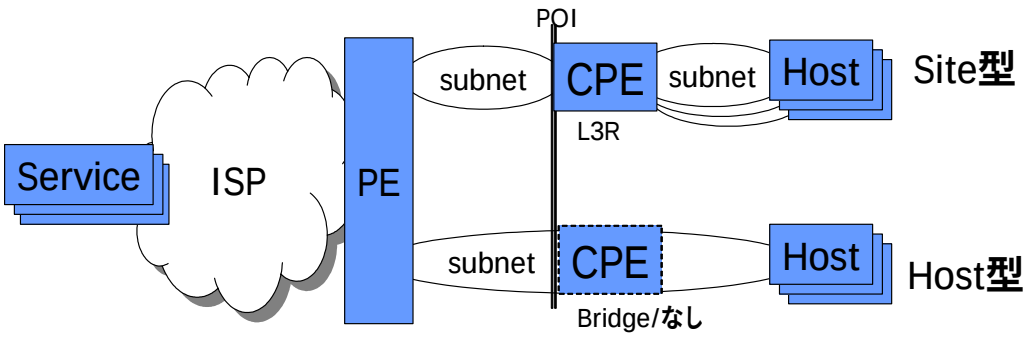
■接続回線(L1)種別

接続回線 (L1) 種別

- Point-to-Point型
  - ADSL
  - FTTH
  - ISDN
  - PSTN (一般電話網)
  - 移動体通信(携帯/PHS)
  - (FWA(SpeedNet等を想定))等
- Broadcast型
  - CATV
  - 無線LAN(HotSpot等を想定)等

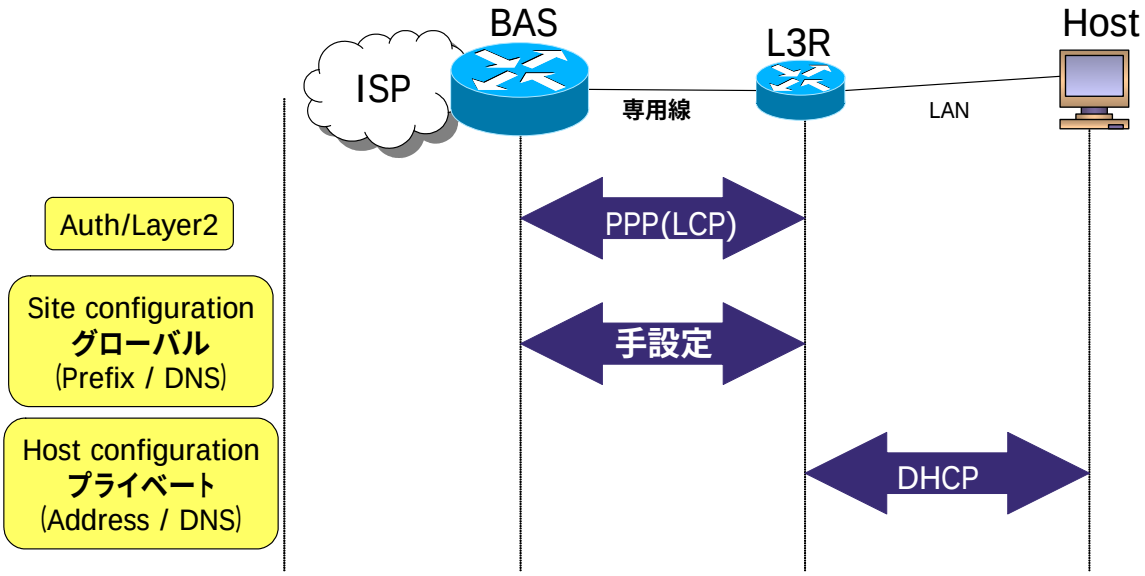
■IPv4 のモデル

IPv4のモデル（2つの型）

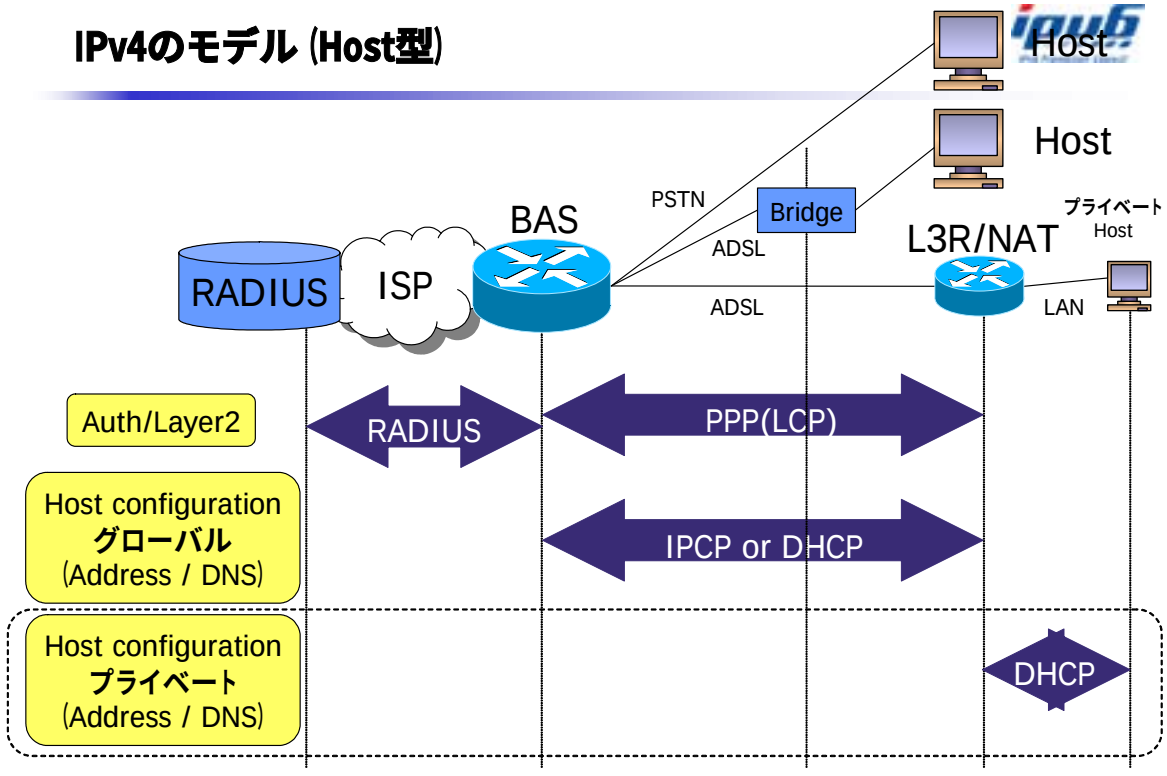


	CPEの種類	例
Site型	L3R(Router)	エコノミー型サービス、企業向け専用線型サービス
Host型	L2 Bridge/なし	ダイアルアップ接続型サービス、ADSL/FTTHサービスも多くはこのモデル（Host=NAT/Router）、Hotspot

IPv4のモデル (Site型)

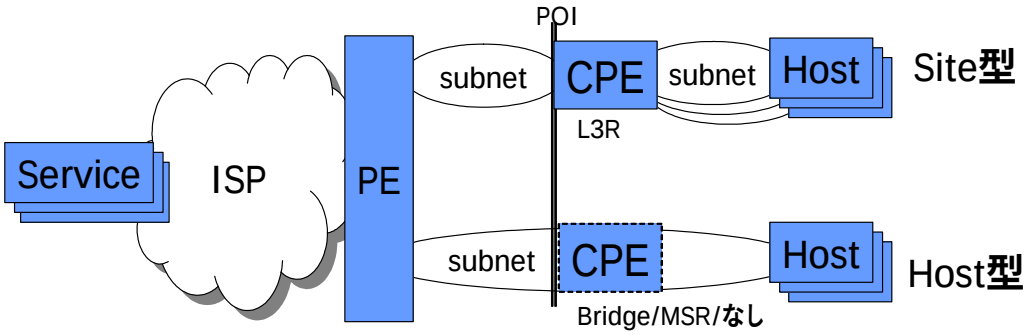


IPv4のモデル (Host型)



■IPv6 のモデル

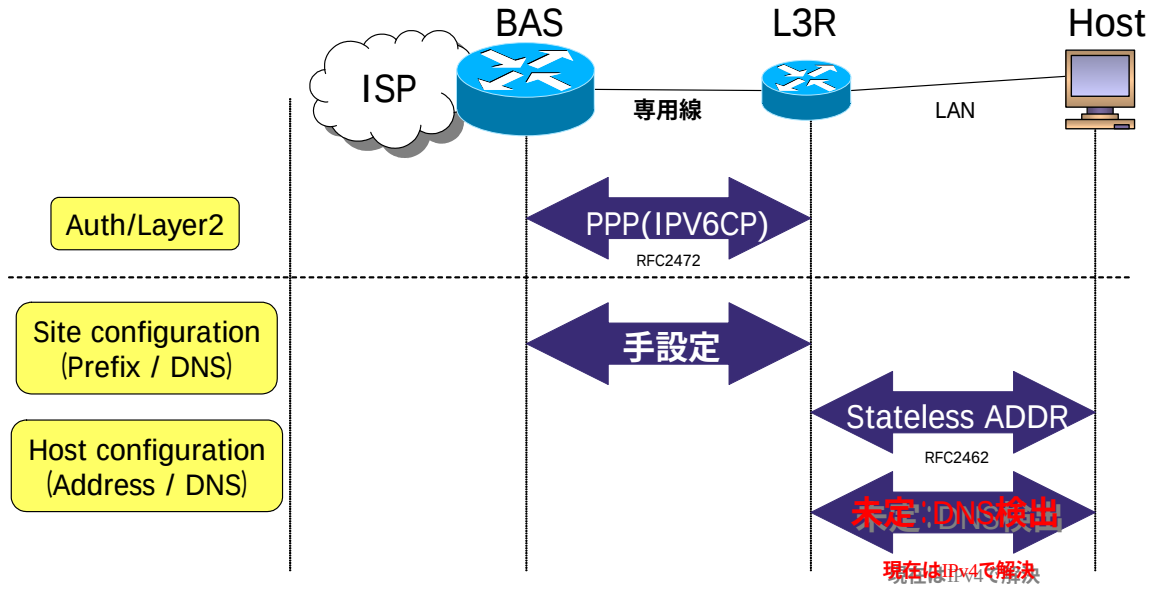
IPv6のモデル (2つの型)



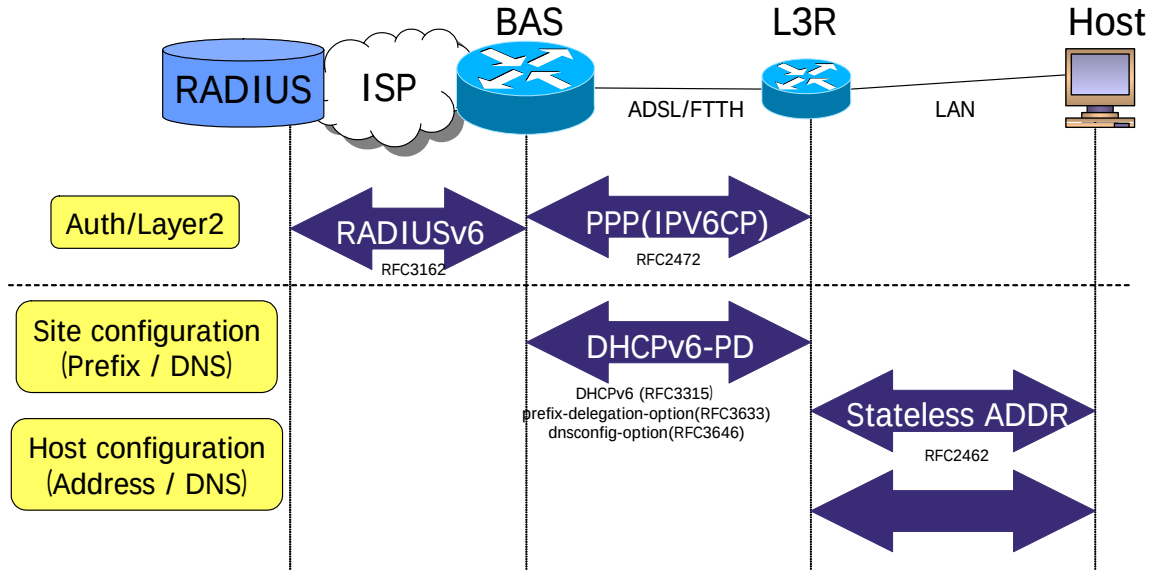
	CPEの種類	Prefix	例
Site型	L3R(Router)	/48,/64	企業向け専用線型サービス、ADSL/FTTHサービス
Host型	L2 Bridge/MSR/なし	/64	ダイアルアップ接続型サービス、3Gモバイルデータサービス、ADSL/FTTHサービス (/64限定) 、Hotspot

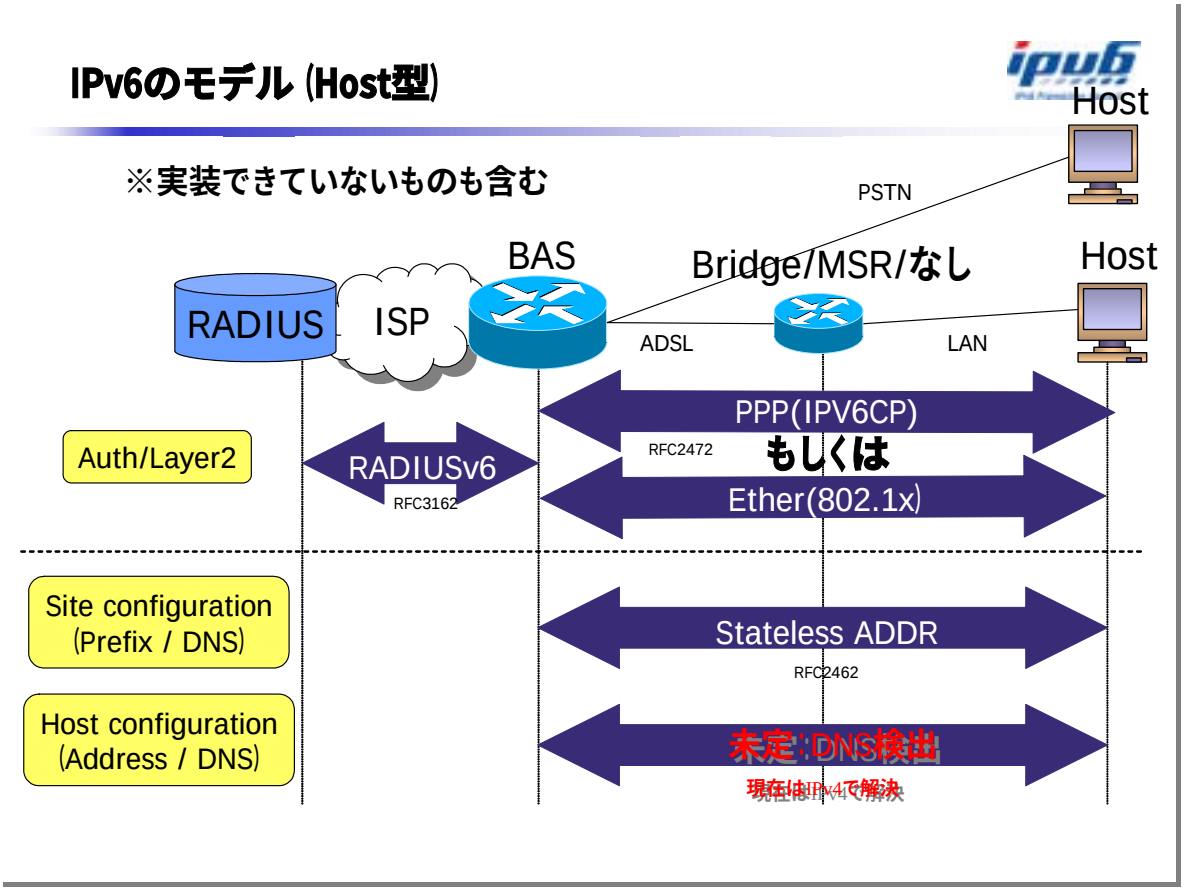
MSR=Multi-link Subnet Router

IPv6のモデル（Site型その1）



IPv6のモデル（Site型その2）





■現状の DNS 検出方法

現状のDNS検出方法

- Well-known DNS Address
  - draft-ohta-preconfigured-dns-00
- RA Extension
  - draft-jeong-dnsop-ipv6-dns-discovery-00
- Stateless DHCPv6
  - draft-ietf-dhc-dhcpv6-stateless-02
- DHCPv6 DNS Configuraiton Option
  - RFC3646

IPv6 移行ガイドライン（ISP セグメント）

平成 16 年 5 月発行

発　行　IPv6 普及・高度化推進協議会
連絡先　wg-dp-comment@v6pc.jp
URL　http://www.v6pc.jp/