

2005 年 IPv6 移行ガイドライン

データセンター、IX 編

2005 年 3 月

IPv6 普及・高度化推進協議会

移行 WG データセンターSWG

目次

はじめに	3
1. セグメントの特徴	4
データセンターセグメントの特徴.....	4
データセンターの現状分析	4
データセンターの主要サービス.....	5
データセンターの IPv6 対応状況.....	5
IX の現状分析	6
IX の IPv6 対応状況.....	6
IX の IPv6 サービスの状況	7
2. 移行モデルと導入シナリオ	8
データセンターの移行モデル	8
アドレッシング	8
ルーティング	10
ユーザへの提供方法	10
ホスティングサービスの移行モデル	14
課題	20
IX の移行モデル	26
IX の移行モデルパターン	28
3. 普及期の想定課題	35
移行課題(総論)	35
データセンターの普及期想定課題	35
データセンターの移行課題(総論)	36
IX の普及期想定課題.....	43
移行 WG データセンターセグメント 検討メンバ	46
お問い合わせ先	46

はじめに

本ドキュメントは、データセンターや IX に携わるサービス提供者やベンダーを対象に、データセンター及び IX におけるネットワークサービスに IPv6 を導入する際に、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、考え方の例を示すものであり、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ました。

1.セグメントの特徴

データセンターセグメントの特徴

ここでは、データセンターおよび IX における IPv6 移行の状況を把握し、事業者の現状の課題分析と移行モデルの検証、移行の際の課題を議論します。

データセンター事業や IX 事業は、ISP 事業者との接続が密接に関係していますが、ISP との接続形態は様々です。

次ページ以降で、データセンター、IX のそれぞれについて、現状の分析を行っていきます。

データセンターの現状分析

データセンターの定義

データセンターとは、コンテンツ配信事業者などのコンテンツ配信サーバファームを収容する、ハウジングサービスとインターネットへの接続性(コネクティビティサービス)を提供する事業のことです。

本ガイドラインの対象

古くからある電算機センターなどを含める広義のデータセンターという言葉もありますが、ここで取り扱うのは、インターネットへの接続性を提供する、いわゆる、インターネットデータセンター(iDC)とします。

iDC 事業者

iDC 事業者には、大きく分けて以下の 2 種類が存在します。

- ・ インターネットサービスプロバイダ (ISP) の事業の一環で提供するケース
- ・ ISP 事業を展開していない、独立系事業者が提供するケース(キャリア系事業者、外資系事業者)

各 ISP が提供するようなケースでは、ISP のバックボーンのネットワーク装置なども置かれるこ

とが多く、Network Operation Center(NOC)と呼ばれることもあります。また、ユーザ設備だけではなく、データセンター事業者の基幹サーバも置かれます。たとえば、コネクティビティサービスの付加サービス関連サーバや、ホスティングサービスで構成される基幹サーバ(DNS など)、監視系サーバ(SNMP など)があります。

データセンターの主要サービス

データセンターの主要サービスには、以下のものがあります。

ハウジングサービス

サーバやネットワーク機器を収容するラックを提供。空調管理や電源供給も行われる。収容機器に対する、一次保守も提供されることがほとんど(電源の OFF/ON、ランプの状態確認など)。入退室管理には、生体認証技術(指紋認証、静脈認証など)も採用されている。IPv6 移行には関係ないので、本ガイドラインでは取り扱わない

コネクティビティサービス

ハウジングサービスで契約したラックへ、インターネットへの接続性を提供するサービス。100Mbps や 1Gbps での提供が主流であるが、帯域制御装置などを用いた、狭帯域サービスもある(10Mbps 以下の数 Mbps のサービスなど)

ホスティングサービス

データセンター事業者のサーバ設備において、Web や Mail サービスを提供するサービス。ユーザが自らサーバの運用や監視を行う必要がなく、事業者側で一元的に運用や監視を行う、いわゆるアウトソーシング型のサービス

本ガイドラインでは、コネクティビティサービスとホスティングサービスの IPv6 移行を扱います。

データセンターの IPv6 対応状況

IPv6 対応状況

形態はさまざまではありますが、全国 101 社の IDC 事業者のうち、約 3 割の 33 社が IPv6 サービスを提供しています(出典:インプレス インターネットデータセンター比較・検討・導入ガイド 2004 年秋号)。提供サービスとしては、IPv6 接続サービス、IPv6 ホスティングサービスが中心で、

一部トンネリングのサービスも提供されています。また、一部 IDC では、有償での IPv6 接続サービスを出しています。

データセンターの IPv6 サービスの状況

データセンター内のバックボーンネットワークがデュアルスタックにどう移行していくかは不明です。現在、ほとんどの事業者で IPv6 の別ネットワークを構築しているため、二重投資しているケースがほとんどで、運用面などでもコスト増になっています。IPv6 のフルルートトランジットが高額すぎる現状もあります。

値決めが難しい(既存サービスよりも明らかに高額になる)という側面もあります。コンシューマ一向けの IPv6 トラフィックが流れなければ、移行しにくく、設備更改のタイミングを逃すと、数年導入が遅れる可能性もあります。

IX の現状分析

IX は、ISP が相互に接続するためのネットワーク接続環境を提供するものであると定義できません。サービス形態は、GbE 接続、FE 接続をベースに、10GbE 接続なども出てきています。

現在、国内の実験と商用の IX において、IPv6 の接続試験サービスが、既存の IPv4 の IX サービス利用者向けに無償で提供されています。

本ガイドラインでは、レイヤ 2-IX を取り扱います。

IX は大きく分けて、学術系 NW と商用 NW の相互接続実証実験 IX (WIDE プロジェクト)、IX 専業事業者 (JPIX、JPNAP、地域 IX 事業者など) の 2 種類存在します。

IX のサービスとしては、ISP 事業者間の接続性を確保するために、レイヤ 2 スイッチのポート接続で提供しています。主流は、100Mbps から、1Gbps に移行しており、現在では、10Gbps のサービスも出てきています。監視系サーバなども配備されており、ネットワークの監視や障害通知などを行っています。

IX の IPv6 対応状況

IX の IPv6 対応状況は次の通りです。

NSPIXP6 (WIDE プロジェクト、<http://www.wide.ad.jp/>)

NSPIXP 研究会 (DIX-IE、NSPIXP3) 参加事業者なら、NSPIXP6 には無償で接続できる。

DIX-IE では、デュアルスタックにすでに対応済み

JPIX(日本インターネットエクスチェンジ、<http://www.jpix.co.jp/>)

JPIX 利用事業者であれば、無償で利用できる

JPNAP6(インターネットマルチフィード、<http://www.mfeed.co.jp/>)

JPNAP6(東京)については、試行サービス期間中は sTLA 割振りを受けていれば誰でも無償で利用できる。また JPNAP 大阪利用事業者であれば、試行期間中はデュアルスタックサービスのみ無償で利用できる

IX の IPv6 サービスの状況

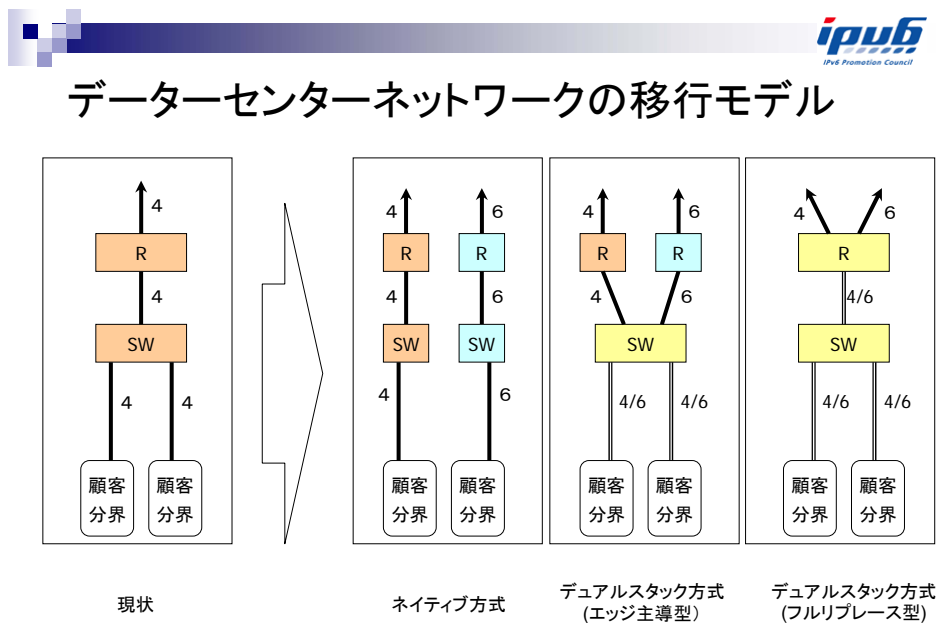
ほとんどが、検証や実験目的で提供中です。業界の流れに遅れないように対応しているケースも多く見受けられます。運用や監視、機器の冗長化については、品質を落としたサービス形態になっています。簡単にデュアルスタックにしていけませんが、ISP 事業者と密接に関係するため、IX 事業者だけでは決めにくく、ISP 事業者とのヒアリングなどで、IPv6 移行をやっていく必要があります。

また、IPv6 への踏ん切りがつきにくく、値決めは、ポート単位でしかやりようがないこと、ISP の設備更改のタイミングなどにより影響を受けることなどが指摘できます。

2. 移行モデルと導入シナリオ

データセンターの移行モデル

データセンターネットワークの移行モデルは、下のように図示することができます。



2004/12/21

IPv6普及・高度化推進協議会 移行WG 総会資料

14

以下では、アドレッシング、ルーティング、ユーザーへの提供方法の3つの観点から、データセンターの移行モデルを解説します。

アドレッシング

アドレスの初期割り振りサイズ

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、sTLA を取得する方向で進めた方がよいと言

えます。

sTLA を取得する場合に「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」という条件があるので、割当計画を十分に考えることをお勧めします。

IPv6 アドレス空間の確保

独自に/32 以上の IPv6 アドレスを APNIC より取得する方法と、上位 ISP の IPv6 アドレスの一部を取得する方法がありますが、独自に/32 以上の IPv6 アドレスを取得する方法を推奨します。

理由としては、独自に/32 を取得した方が、冗長性確保や経路制御の自由度が高いこと、上流 ISP から IPv6 アドレスを取得した場合、その上流 ISP から別の ISP に乗り換えるときに必ずリナバが発生することが挙げられます。

具体的な申請方法は ISP SWG の資料を参照してください。

顧客に提供する IPv6 アドレス

現行のアドレスポリシーでは、顧客に提供する IPv6 アドレスは、エッジスイッチに直接接続する場合は/64、ルータ接続の場合は /64 で接続し、その下に /48 を構成します。

アドレッシング(200 個、/48、2 年問題)

/32 以上の IPv6 アドレスを APNIC より取得する場合、以下のような条件があります (<http://www.nic.ad.jp/ja/translation/ipv6/20040714-01.html>)。

- ・ LIR であること
- ・ エンドサイトでないこと
- ・ /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。
- ・ 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

データセンター事業者の中では条件 4 が障害となっていると思われる場合が多いですが、以下のようなケースを考えると上記の条件は簡単にクリアできます。

- ・ 1 ユーザー(ラック 1 個)に/48 を 1 個割り当てる
- ・ 多くの共有型ホスティングサービスは IPv4 アドレスを節約する方法をとっているが(name based virtual hosting)、IPv6 ではアドレス空間を無理に節約する必要がない

インフラやユーザに対するアドレス割当

<http://www.nic.ad.jp/ja/translation/ipv6/20040714-01.html> では、次のように示されています。

非常に規模の大きな申請者を除き、通常は/48 を割り当てる。

例) 1 ユーザ(1 ラック)に/48

仕様により唯一のサブネットが必要であることがわかっている場合は/64

例) サーバーセグメントには/64

例) ルーターへルーター間には/64

唯一のデバイスが接続することが確実にわかっている場合は/128

例) ルーターのループバックには/128

ISP SWG でも同様の記述があるので参照してください。

ルーティング

基本ポリシーとしては、既存の IPv4 網に影響を与えない方法を選択した方がよいと言えます。また、できるだけトンネルを利用しない方法を選択し、IPv6 をルーティングしている機器では、IPv4 をルーティングさせないようにした方がよいと考えられます。

EGP には、BGP4+を利用します。ただし、現状では IPv4 と IPv6 の両方のルーティングテーブルを持ったときの安定度に不安が残ります。

IGP では、OSPFv3 を推奨します。初期段階では RIPng でもよいですが、扱うルーターの台数が増えた場合は OSPFv3 に移行した方がよいと言えます。ISP-SWG でも同様の記述があるので参照してください。

ユーザへの提供方法

ユーザに対する IPv6 の提供シナリオとしては、IPv6 ネイティブ方式、あるいは IPv4/IPv6 デュアルスタック方式(エッジ主導型)を経て、IPv4/IPv6 デュアルスタック方式(フルリプレース型)へ進んでいくことが考えられます。それぞれについて、下に説明します。

ネットワーク(ユーザへの提供方法)

- スモールスタート
- ゴールはIPv6/IPv4 デュアルスタック(フルリプレース型)

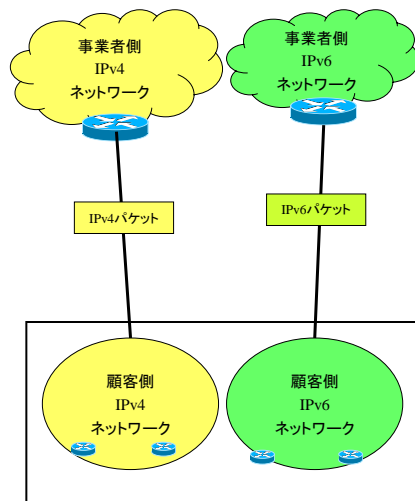
時期	ポイント	EGP	IGP	ネットワーク形態、利用方法等
スタート	外部接続の構築	BGP4+	static RIPng	実験や検証
nヶ月後	小規模IPv6ネットワークの構築	BGP4+	RIPng OSPFv3	IPv6 ネイティブ方式で顧客に提供
	デュアルスタックネットワークへの移行	BGP4+	OSPFv3 RIPng	エッジ部分をデュアルスタック化
n年後	現状での完成形	BGP4+	OSPFv3	ネットワーク全体をデュアルスタック化

IPv6 ネイティブ方式

IPv6 用のコネクティビティを別に用意し、ユーザに提供します。

IPv6ネイティブ方式

- IPv6 用のコネクティビティを別に用意し、ユーザに提供する。(IDCからみたサービスとしてはシングルスタックになる)
- 事業者からみたメリット
 - 既存のIPv4ネットワークに影響を与えることなく構築が可能
 - IPv6ネットワークとしては、小規模なことからスタートできるのでハードルは低い。
- 事業者からみたデメリット
 - コストがかかる。IPv6ネットワークの成長に伴いその増分は増大する。
- 注意する点
 - 既存のIPv4 のコネクティビティとこのIPv6コネクティビティを顧客側でL2 接続し、デュアルスタック環境にすることもありますが、L2ループになる可能性があるので十分注意する。



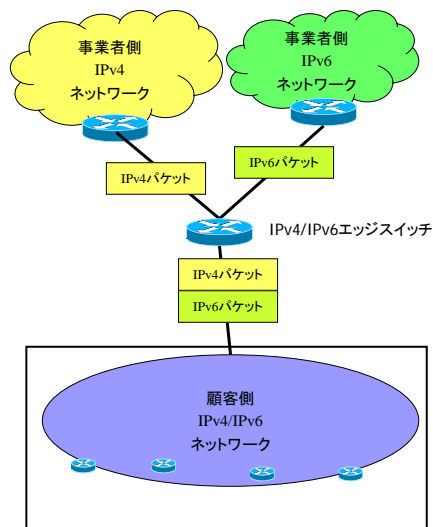
IPv6/IPv4 デュアルスタック方式（エッジ主導型）

エッジスイッチを IPv6/IPv4 ルーティング可能にし、ユーザへはデュアルスタックで提供します。



IPv6/IPv4デュアルスタック方式(エッジ主導型)

- エッジスイッチを IPv6/IPv4 ルーティング可能にし、ユーザーへはデュアルスタックで提供する。エッジスイッチより上位は別ネットワークにする。エッジスイッチはL2/L3のどちらでも可能。
- 事業者からみたメリット
 - 網全体を作り替えることなく、低コストで顧客にデュアルスタックが提供可能
- 事業者からみた課題
 - 既存のIPv4ネットワークのIGPIに影響を与えないような設計
 - IPv4ネットワーク側にIPv6パケットが流入しないような設計
 - 現在利用している冗長化のためのプロトコルがこの方式のときに正常に動作するかどうか



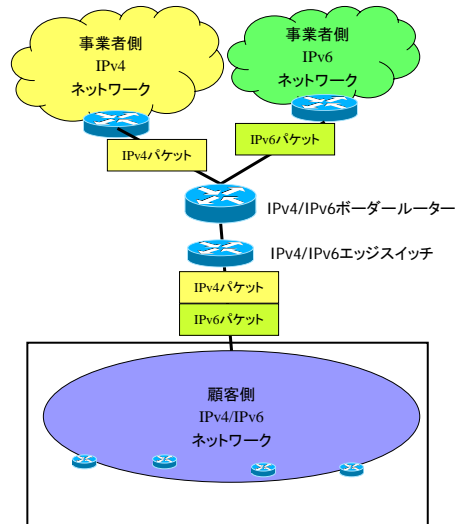
IPv6/IPv4 デュアルスタック方式（フルリプレース型）

ネットワーク全体を IPv4/IPv6 デュアルスタック化します。



IPv6/IPv4デュアルスタック方式(フルリプレース型)

- ネットワーク全体をIPv4/IPv6デュアルスタック化する。
- IPv6普及期～5:5期には主流の形
- IDCネットワーク全体を最初から構築する場合はこの方法が良い。



2004/12/21

IPv6普及・高度化推進協議会 移行WG 総会資料

22

トンネル方式

データセンターと顧客側ルータとの間でトンネルする方式も考えられますが、推奨できません。



トンネル方式

■ 構内トンネル方式

- データセンター内にIPv6/IPv4トンネルルータを用意し、顧客側ルータとの間でトンネルする。
- 方式としてはありえるが、品質に疑問にあることと故障時の切り分けが難しくなることから推奨しない。

■ トンネルに対する考え方

- 基本的にトンネルを利用しない方法でネットワークを設計する。
- もし、トンネルを導入する場合は自ネットワーク内に閉じたトンネルの利用等、品質等の課題を加味した上で導入する。

2004/12/21

IPv6普及・高度化推進協議会 移行WG 総会資料

23

Autoconfiguration 関連の注意点

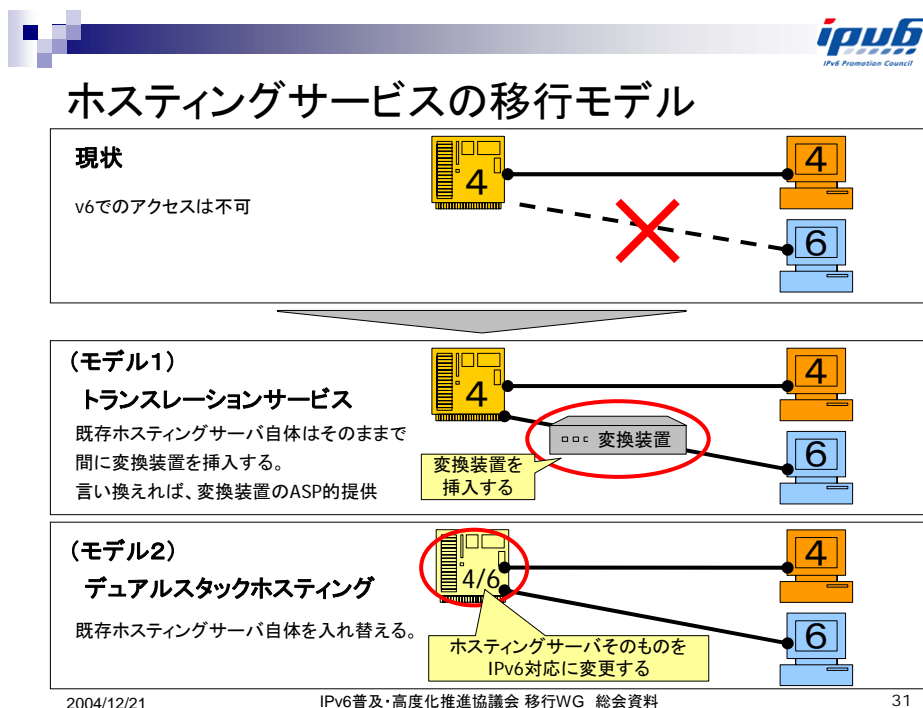
Router Advertisement (RA、DHCPv6)等の IPv6 で使われる Autoconfiguration 技術は、サーバfarmやネットワークへの影響を考えた上で注意深く設定する必要があります。場合によってはそれらのパケットを破棄するような設定を行う必要があります。

自社で利用している RA が外部に流れていないか、顧客側から流れてくる RA によって予期しない IPv6 アドレスが付与されていないか、などを考えなければなりません。

ホスティングサービスの移行モデル

ホスティングサービスの移行

ホスティングサービスの IPv6 化を行う場合、最終形態としては、デュアルスタックのホスティングサービスに移行していくこととなりますが、過渡期のサービスとしては、IPv6 の問い合わせをプロトコル変換し、IPv4 通信に代理応答する、トランスレーションサービスによる IPv6 移行モデルもあります。



ホスティングサービスは、大別して 4 種類あります。

高級版ホスティング

1-1: 専用ホスティング

1-2: 共用ホスティング

廉価版ホスティング

2-1: 共用ホスティング

2-2: IA サーバ利用共用ホスティング

以下では、それぞれについて説明します。

1-1: 高級版 専用ホスティング

ホスティングとは言うものの、実質的に、ハウジング+顧客サーバとほぼ同様の扱いとなります。専用サーバを用い、インストール、設定、運用はすべて個別に対応します。移行手順は、デュアルスタックホスティングへの移行となります。

1-2: 高級版 共用ホスティング

共用ではありますが、中身は相互に独立しているサービスです。VMWare のように PF レベルでの独立、あるいは chroot-jail のように OS レベルでの独立が行われています。

IP アドレスは各々に付与されています。独自のアプリケーションもインストール可能です。運用もある程度個別に対応してもらえるケースが多い形態です。

このタイプの IPv6 移行における課題は、ユーザが独自にインストールしたアプリケーションが IPv6 対応していない場合の扱いをどうするか、一部のユーザだけを IPv6 移行することが可能かどうか(とくに chroot-jail のケース)、といった点です。

2-1: 廉価版 共用ホスティング

アプリケーション(設定)レベルで共用されているサービスです。apache の virtual_host、sendmail の sendmail.cw などを利用したものなどがあります。Web、Mail など利用できるサービスが規定されています。

この場合、IP アドレスも共用で、FQDN は CNAME、アプリケーションレベルは HTTP HostHeader などです。アプリケーションの独自インストールは不可で、CGI も限定利用の場合もあります。

このタイプの IPv6 移行における課題は、一部のユーザだけを IPv6 移行することがまず不可能であるということ、移行後はユーザごとに IPv6 アドレスを付与したいということです。

2-2: 廉価版 IA サーバ利用共用ホスティング

これは基本的に 2-1 と同じです。ホスティング事業者が管理用のツールなどを独自開発していることも多くあります。

このタイプの IPv6 移行における課題は、一部のユーザだけを IPv6 移行することはまず不可能で、移行後はユーザごとに IPv6 アドレスを付与したいということ、さらに独自開発 GUI ツールの IPv6 対応も課題です。

トランスレーションサービス

トランスレーションサービスでは、ホスティングサーバは既存のままで、間に IPv4/IPv6 プロトコル変換装置を挟みます。プロトコル変換装置の ASP 的提供と言えます。これは、過渡期のサービスで、将来的にはデュアルスタック化を行うケースに用いられることが想定されます。

プロトコル変換装置は、NAT-PT 型、TRT 型、アプリケーション・プロキシ型の 3 つに分類されます。ここでは、名前解決は別個実施を想定しており、いわゆる DNS プロキシ (totd など) を用いる形ではありません。

以下に、それぞれのプロトコル変換装置を説明します。

NAT-PT 型

NAT-PT は Network Address Translator - Protocol Translator の略です。NAT の延長で、プロトコル変換まで行うというものです。3 層 (IP レイヤ) での変換で、オーバーヘッドは少なめですが、ウィンドウ制御・再送制御は行いません。

TRT 型

TRT は Transport Relay Translator の略で、名のとおり、トランスポート層 (4 層、TCP・UDP 層) で変換を行います。オーバーヘッドは NAT-PT に比べればやや大きいですが、アプリケーション・プロキシ型ほど大きいわけではありません。ウィンドウ制御・再送制御も行います。

アプリケーション・プロキシ型

アプリケーションレベルで変換を行います。アプリケーション (http/https、smtp 等) ごとに用意する必要があります。必要な全てのプロトコルが揃うとは限りませんが、オーバーヘッドが大きい方法です。ただし、変換性能・親和性は最も高いと言えます。

トランスレーションサービス：導入パターン（1）

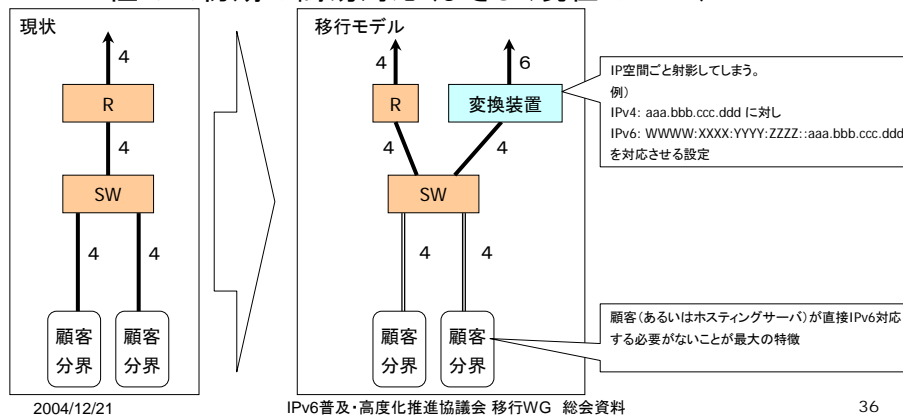
これは、変換装置を上位に配置するものです。



トランスレーションサービス：導入パターン（1）

■変換装置を上位に挟むパターン（STEP1）

- 上位でがっさり変換をかけてしまうパターン
- 極めて初期の簡易対応（まさしく現在のBCP）



トランスレーションサービス：導入パターン（2）

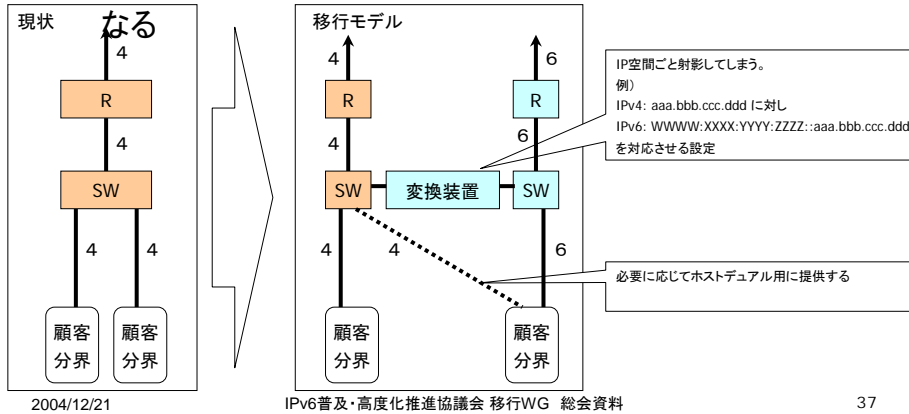
デュアルホストが増えてくるころのパターンで、実際にはこれが最初の一步です。



トランスレーションサービス: 導入パターン(2)

■変換装置を挟むパターン(STEP2)

- デュアルホストが増えてくるころのパターン
- 実際にはSTEP1は極論で、最初の一步はこのモデルに



トランスレーションサービス: 導入パターン(3)

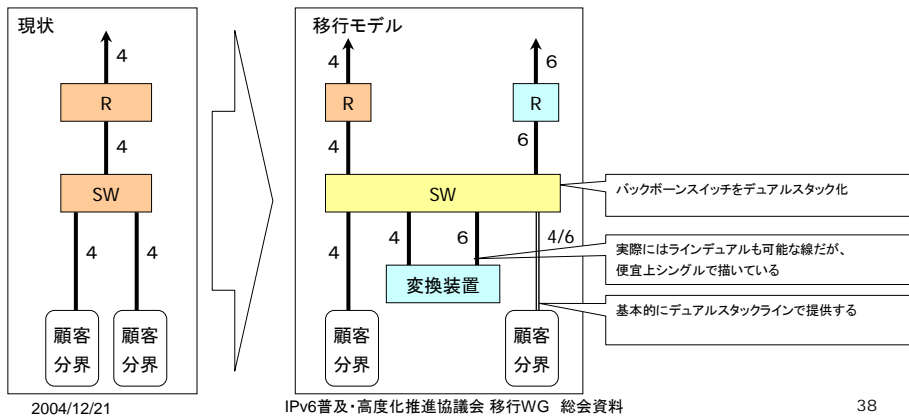
デュアルホストが本格化するころのパターンです。



トランスレーションサービス: 導入パターン(3)

■変換装置を用いるパターン(STEP3)

- デュアルホストが本格化するころのパターン



デュアルスタックホスティング

デュアルスタックホスティングは、iDC ホスティングサーバをデュアルスタック化することです。必要な範囲から順次移設していき、将来的には既存システム全部を iDC に移設します。更改のタイミングに合わせるケースがほとんどです。

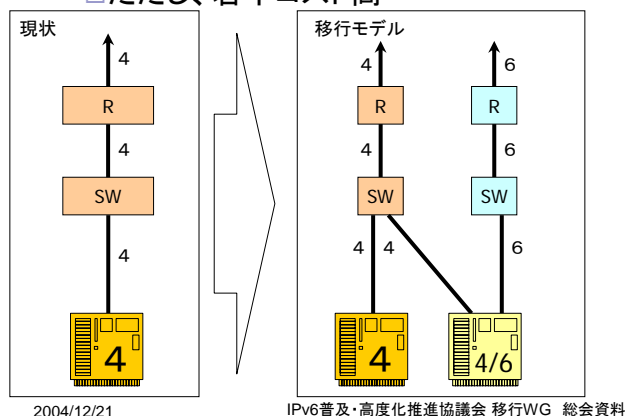
デュアルスタックホスティング：導入パターン（STEP 1）

ホストデュアルスタックホスティングと呼ばれる方法です。

デュアルスタックホスティング：導入パターン（STEP 1）

■ホストデュアルスタック ホスティング

- ネットワーク構成としてはもっともシンプル
- ただし、若干コスト高



40

デュアルスタックホスティング：導入パターン（STEP 2）

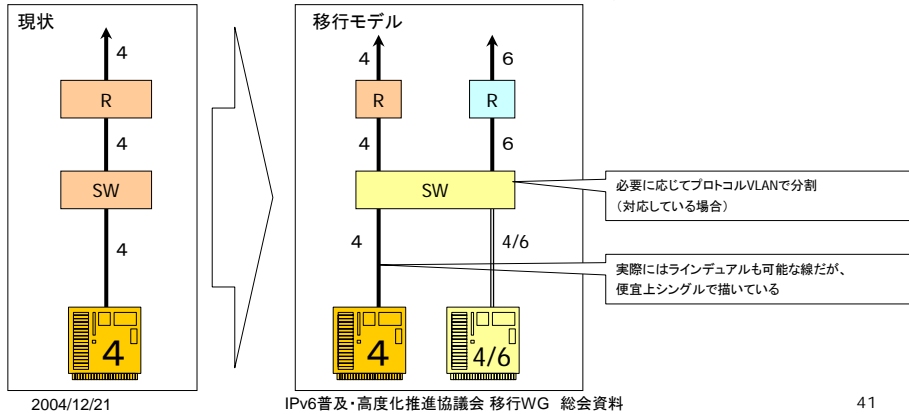
こちらは、ケーブルデュアルスタックホスティングという方法です。



デュアルスタックホスティング:導入パターン (STEP2)

■ケーブルデュアルスタック ホスティング

- ファーストステップとしてはこちらでも可
- ユーザ分界に極めて古い機器がある場合には要注意



課題

IPv6 移行に共通の課題

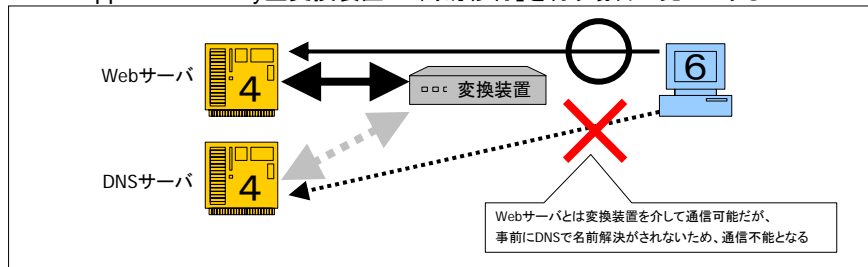
トランスレーションサービスとデュアルスタックホスティングに共通の課題として、一部を移行する場合に名前解決ができなくなる可能性が出てきます。



IPv6移行に共通の課題

■ DNSの問題

- 既存システムの一部のみをIPv6移行する場合、DNSがIPv6移行範囲に含まれていない場合、IPv6名前解決ができない可能性がある
- Application Proxy型変換装置で「簡易移行」を行う場合に発生しうる



- 対策:
 - (1) まずDNSをIPv6移行対象とする
 - (2) 受け皿となるデュアルスタックDNSサービスを整備しておく

もう1つ考えられる問題として、OSIモデルに則っていない実装で、単に変換装置を入れただけでは問題になる場合があります。端的な例は7層情報に生IPアドレス(3層情報)を書いたパターンです。

よくあるケースは、HTMLソースにと書いてある場合や、SNMP_TRAPに、発信元を示す情報がIPアドレスで書いてある場合です。

対策として、7層を変換する機器等で対処できなくはないですが、根本的な解決になりません。正しくFQDNで書くことを徹底する必要があります。

トランスレーションサービスの課題

トランスレーションサービスでは、以下のような課題があります。

- ・すべてのプロトコルを変換できるか
- ・経路暗号化された通信についても変換可能か
- ・ホスト認証への対応
- ・L4-7スイッチのv6対応状況
- ・踏み台になる可能性(アクセス元の隠匿)
- ・アクセスログの問題
- ・サービスとして成り立つか(収支見合い)

以下では、それぞれについて説明します。

すべてのプロトコルを変換できるか

これについては、NAT-PT 型、TRT 型の変換装置であれば、基本的に問題ありません。http、smtp、ssh などの基本的なプロトコルはサポートされています。mms、rtsp 等のストリーミングプロトコルも対応しています。アプリケーション・プロキシ型の変換装置も、必要なプロトコルは揃っています。製品例としては、Web だと apache の reverse proxy、DNS だと nameproxy (Windows) があります。

プロトコルが規定されていない場合は、個別に定義して作ることも可能で、アプリケーション・プロキシ型の場合、「選択的に移行可能」という長所にもなります。結論としては、ほぼ対応しているという問題ありません。

経路暗号化された通信についても変換可能か

基本的には右から左へスルーするだけなので、問題はありません(ペイロードは見ない)。ただし、HTTPS のようにホスト認証がセットになっているものは要注意です(次項目参照)。

結論としては、暗号化のみであれば問題なしと言えます。

ホスト認証への対応

NAT-PT 型、TRT 型では問題なく通信可能です。ただし、生 IP アドレスで認証している場合や、別 FQDN を割り当てている場合は問題が発生します(名前と証明書内容が食い違う)。アプリケーション・プロキシ型は対応していません。また、プロトコル変換機に、移行対象サーバとは別のサーバ証明書をインストールする必要があります。

結論としては、移行時は同一 FQDN を利用しなければ、別証明書問題が発生するので、注意が必要です。

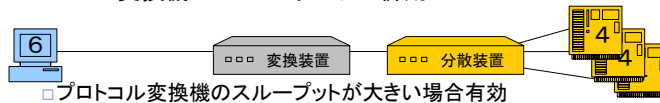
L4-7 スイッチの v6 対応状況

全般的にこのジャンルでの IPv6 対応製品はまだ少ないのが実情です。

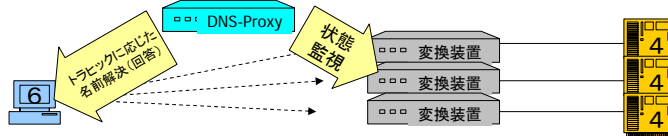
トランスレーションサービスの課題

■L4-7SWのv6対応状況

- ロードバランサのIPv6対応製品はまだ少ない(F5 BIG-IPなど)
- リバースプロキシは複数種類ある
 - (NetCache、Apache、Orenosp Secure Reverse Proxy など)
- 代替手段
 - プロトコル変換機とロードバランサの併用



- プロトコル変換機のスループットが大きい場合有効
- DNS-Proxyとの連動も



■結論：ベンダーの実装は、まだこれから
2004/12/21 IPv6普及・高度化推進協議会 移行WG 総会資料

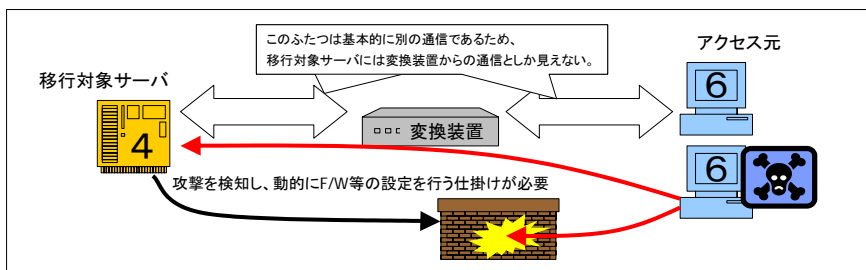
踏み台になる可能性(アクセス元の隠匿)

トランスレーションでは、真のアクセス元が変換装置に隠匿されてしまうという問題があります。

トランスレーションサービスの課題

■踏み台になる可能性(アクセス元の隠匿)

- いずれの形式にせよ、移行対象サーバには変換装置のアドレスしか見えない
- 真のアクセス元は、変換装置に隠匿されてしまう



- 結論：隠匿は必ず発生する
- 対策：(1) 変換装置でのログ取得・ログ管理(次項目)
 (2) 動的フィルタリングの実装

アクセスログの問題

アクセス元が隠匿されるため、移行対象サーバ上のログのみではアクセス解析が不可能です。したがって、変換装置上でのログ取得/ログ管理が必要不可欠です(この場合、時刻同期も必須です)。

また、取得可能なログの形式に若干の問題があります。ここでは、必要なログは「apache の combined_log」を想定しています(マーケティング等で用いられる Web アクセス解析を想定)。すると、アプリケーション・プロキシの場合、基本的に移行対象アプリケーションと同様のログが取得可能です。NAT-PT型、TRT型の場合は、「NAT結果のみ」か「全パケットのキャプチャ」か、いずれかになってしまい、移行対象サーバ上のログとの突合、あるいはキャプチャ解析が必要になります。

結論としては、NAT-PT/TRT の場合に若干問題があります。対策には、http など特定プロトコルに特化して、必要な形式のログ取得できる NAT-PT/TRT の開発が必要になります。

サービスとして成り立つか(収支見合い)

トランスレーションサービスは、一般ユーザから見ると、難しそうな技術には見えにくいですが、事業者観点からすれば、必要な機器は追加投資になります。フリーソフトで組めなくはないですが、商用利用には不安があります。細かい苦労がある割に、見込める収入は少ない可能性もあります。

したがって、結論としては、ビジネスモデルの検討には慎重を要します。顧客が IPv6 に価値を見出してくれるかどうか、基盤に取り込んで付加価値向上につなげられるか、といった点を考慮しなければなりません。

デュアルスタックホスティングサービスの課題

デュアルホスティングサービスの課題には、以下のものがあります。

- ・(IPv6に限らない)ホスティングサービス自体の課題
- ・一部だけの移行の可否
- ・ファイアウォールへの影響
- ・サービスとして成り立つか(収支見合い)

以下では、これらを解説します。

(IPv6に限らない)ホスティングサービス自体の課題

ホスティングサービス自体の課題として、狭義のホスティング(画一的サービス)にできるか、できなかったときは、運用可能かというものがあります。ただし、ここで解説しているのは、基本的には既存ホスティングサービスの IPv6 移行であり、上記課題は解決済みであるという前提に立っています。

「一部ユーザのみの移行」を除けば(次項目)、IPv6 移行することによって新たにこの問題が発生することはありません。

一部だけの移行の可否

共用ホスティングにおいて、一部ユーザが導入しているアプリケーションが IPv6 非対応の場合、そのユーザだけ IPv6 移行をしない、という選択が可能かどうかという問題です。これは、高級版共有ホスティングで想定される仕様であればおそらく可能です。そうでなければ、IPv6 対応・非対応で共用の組み直しを行う必要があります。

しかし、廉価版共有ホスティングであれば、そもそも「一部のユーザが独自アプリケーションをインストール」という事象が発生しません。

結論として、対応は可能と想定されます。

ファイアウォールへの影響

ファイアウォールが共用の場合は要注意です。ホスティングが専有か共有かにはよらず、IPv6 処理を追加することでスループット低下の恐れがあります。

しかし、ファイアウォールを無理にデュアルスタックにする必要はありません。ラインシングル・ホストデュアル型の移行形態が可能です。ただし初期費用に注意を要します。

サービスとして成り立つか(収支見合い)

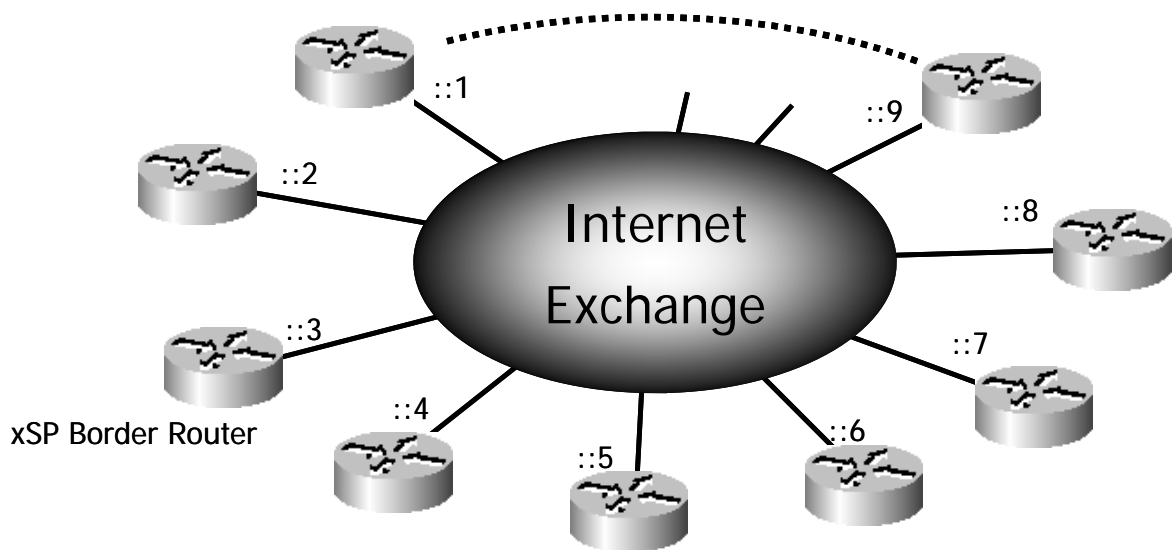
廉価版ホスティングの現行価格は月額3000円レベルです。現状では IPv6 を求めるユーザはいないと思われます。つまり、増額は非常に難しい状況です。

高級版ホスティングの場合、現行費用は月額10万円レベルで、直近のターゲットとしてはこちらになるはずですが。ただし、さらに料金増が可能かどうかは疑問です。

結論としては、高級ホスティングの付加価値サービス的に実施することになるかもしれません。

IX の移行モデル

IX 用の IPv6 アドレス



IX では、同一の LAN セグメント上に各 ISP の外部接続用ルータが接続されています。各ルータの IX への接続インタフェースには、IX の運用者によるポリシーに基づいて割り当てた、同一サブネット(上図では A:B:C:D::/64)の中のアドレスを付与します。

IX 用 IPv6 アドレスの要件

ISP のように割り振りされたアドレスについては下流の組織にアドレスブロックを割り当てする必要はありません。必要なサイズは、既存の IX であれば、/64(がいくつか)で十分であるので、ISP に割り振られるサイズ(/32) は IX に対して割り振るには適切ではありません。

しかし、IX の本来の性格上、IX のアドレスは特定の ISP に依存せず、中立／独立であるべきであるため、RIR から直接割り当てが行われることが好ましいと言えます。

特定の ISP などの LIR から割り振りを受けた場合には、その中立性が損なわれるほか、IX 用のアドレスがその ISP のアドレス空間の一部としてグローバルに広告されてしまうという問題点もあります。

IX 用 IPv6 アドレスの割当て

現状では、RIR から適切なサイズのアドレス空間 (/48) の IPv6 アドレスが直接 IX に対して割当てられています。日本においては、APNIC から割り当てが行われていますが、JPNIC において申請の代行を行っています。申請方法については、JPNIC のホームページで参照可能です。

<http://www.nic.ad.jp/ja/translation/apnic/apnic-portable-assignment-request-form-j.html>

なお、RIR では、まとまったアドレス空間が IX 用割り当てとして確保されています。

例) APNIC 2001:07FA:: /32
RIPE 2001:07F8:: /32
ARIN 2001:0504:: /30

これらを用いて、適切なポリシーに基づきフィルタをかけることが可能です。

IX 用アドレスの広告について

IPv4/IPv6 共通に IX 用に使用されているアドレスの広告について言えるのは、IX 上の隣接したルータ同士の BGP セッションのみに用いられるため、広告する必要性が少ないということです。

中立性という観点から、特定の ISP から広告されることは好ましくありません。また、特定の ISP が IX 上以外から広告した場合、ルーティングトラブルを起こす危険性がありますし、IX セグメント外からの IX 上のルータへの攻撃防御の危険性がある (TCP の脆弱性をついた RST パケットの送付など)。以上から、一般的にグローバルへの広告が停止されています。

IX 用 IPv6 アドレスの広告については、各 RIR から IX 用として割り当てされるアドレスについては、グローバルへの広告をしないという条件でアドレス割り当てをしていることもあり、グローバルなインターネット経路表への広告は「禁止」です。

IX 用の IPv6 アドレスの課題

ここで、リンクローカルアドレス vs IX 用グローバルユニキャストアドレスという課題があります。先に述べたように IX 用アドレスはグローバルに広告する必要性が少なく、また通常は同一リンク上での通信しか行われなため、リンクローカルアドレス利用についても検討されています。この場合、リンクローカルアドレス宛のパケットはルータによる転送が禁止されているため、IX 用アドレスを広告することによる問題を厳密に回避できます。

その一方で、IX 用のアドレスを、その運営主体が責任をもって管理することが難しいという問題があり、古い実装では、リンクローカルアドレスによる BGP+ に対応していないことも指摘できます。さらに、同一のルータで複数の BGP+ による接続を行う場合、アドレスの設計によっては重複する可能性があります。また、IX へ隣接しているノードへの到達性が失われるため、死活監視が困難である。

これらの課題もあり、現状ではどちらを使用するかは IX の運営主体に任されているケースが多

いと言えます。

IXの移行モデルパターン

IX事業者設備（スイッチ）

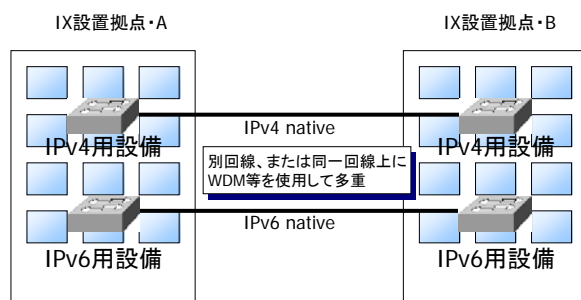
IX事業者の移行モデルには、別回線(IPv6 サービス専用)型移行、VLAN分離型移行、デュアル型移行があります。

別回線(IPv6 サービス専用)型移行

これは IPv4 と IPv6 で、別の機器と回線を用いるものです。



(1)IX事業者:別回線(IPv6サービス専用)型移行



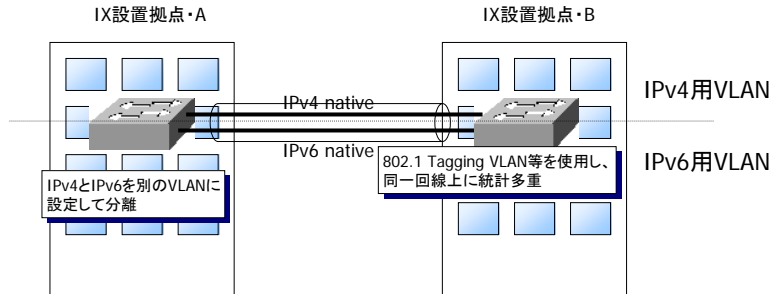
- IPv4, IPv6で別機器、別回線を用いる形態。
- 筐体(スイッチ)や拠点間の回線については既存設備とは別に準備が必要となるため、IX事業者に追加の設備コストが発生する。
- IPv4, IPv6が混在しないため、IPv6トラフィックの影響を心配する必要がない。
- 運用面/料金面でも既存のIPv4と分離される。
- デュアルスタックでの利用不可のため、xSP事業者にも追加の設備コストが必要。

VLAN 分離型移行

IPv4 と IPv6 同一機器と回線で接続しますが、VLAN で 2 つのプロトコルを分離します。



(1)IX事業者:VLAN分離型移行



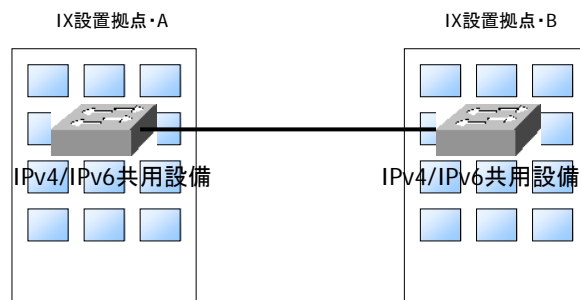
- 同一機器、同一回線を用いて、IPv4, IPv6をvLANにて分離する形態。
- 筐体(スイッチ)や拠点間の回線については既存設備を共用するため、IX事業者追加の設備コストは発生しない。
- VLANの管理など運用面での手間が発生。
- IPv4, IPv6のトラフィックが混在しないため、IPv6トラフィックが及ぼす影響を心配する必要がない。
- 料金面では既存のIPv4と分離される。
- デュアルスタックでの利用不可のため、xSP事業者にも追加の設備コストが必要。

デュアル型移行

この場合、IPv4 と IPv6 の分離は行いません。デュアルスタックで双方を通します。



(1)IX事業者:デュアル型移行



- 同一機器、同一回線を用いて、IPv4, IPv6を分離せずに提供する形態。
- IX事業者追加の設備コストは不要。
- 運用面/料金面での差別化は困難。
- IPv6のトラフィックによるIPv4トラフィックへの影響がある可能性がある。
- デュアルスタックでの提供が可能のため、xSP事業者は追加ポートの負担を必要としない。

IX 事業者設備 移行シナリオ

「別回線型」は設備投資が必要となりますが、運用／料金を切り離して IPv4 サービスと IPv6 と提供可能であり、また IPv6 トラフィックの影響を懸念する必要がないため、実験サービスなど初期の提供形態としては適しています。

ただし、追加の設備投資を避けたい場合、「VLAN 分離型」の形態での導入も考えられます。

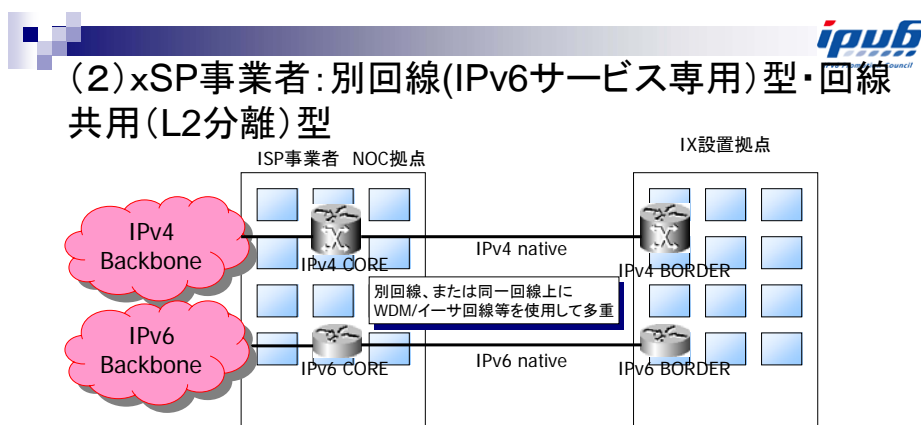
IPv6 普及期～5:5 の時期にかけ、相当のトラフィックが出てきた場合は、コスト等あらゆる面から、「デュアル型」の形態で提供されることになる想定されます。

xSP 事業者

xSP事業者のIX接続における移行シナリオは、別回線(IPv6 サービス専用)型、回線共用(L2分離)型、トンネル型、デュアル型の4つに大別できます。

別回線(IPv6 サービス専用)型・回線共用(L2分離)型

これはIPv6をIPv4とは切り離された形で用意する形態です。



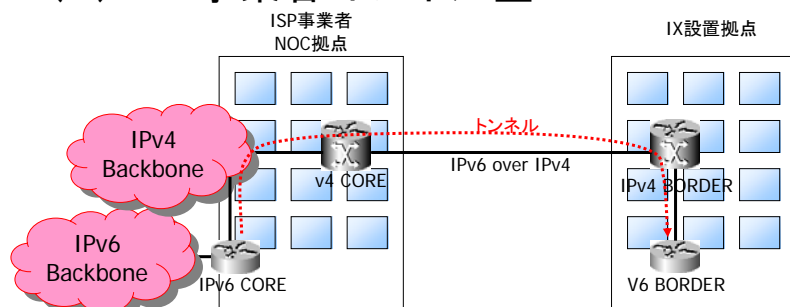
- IPv6回線をIPv4回線とは別に準備する形態。
- 回線コスト削減のため、L2(VLAN)サービスやWDM装置を使用し、同一回線上に多重することも可能。
- すでにIPv4のIXに接続するためにIX設備設置拠点へ設備を設置している場合でも、追加の設備投資が発生。
- IPv6トラフィックがIPv4におよぼす影響を避けることができる
- 現状ではこの形態を用いているのが多数。

トンネル型

これはIPv4 回線にトンネリングによりIPv6 も通すという形態です。



(2)xSP事業者:トンネル型



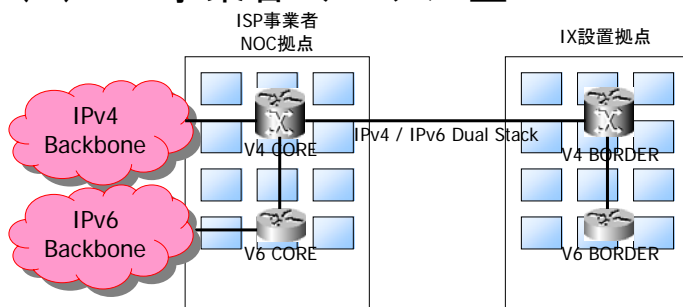
- IPv6接続ルータ間をIPv6 over IPv4トンネルにて接続する形態。
- アクセス回線を共有することができる。
- IPv4網の障害の影響を受けた場合、切り分けが困難なため、あまり推奨されない。

デュアル型

これはデュアルスタックでIPv4 とIPv6 を通す形態です。



(2)xSP事業者:デュアル型



- IPv6接続ルータ間をデュアルスタック回線にて接続する形態。
- 旧型の機器ではIPv6とIPv4との混在のおよぼす影響が未知であるため、敬遠されるケースがある。
- IPv6の普及期、5:5の時期以降はこの形態になると推測される。

xSP 事業者 移行シナリオ

xSP 事業者が IPv6 で IX に接続するためには、IPv6 ネットワークを IX 事業者設備設置拠点まで延伸する必要があります。

しかし、現状の IPv4 ネットワークは停止することができない重要なインフラとなっているため、初期の段階ではリスクをおかさず IPv4/IPv6 別網での構築が行われます。アクセス回線のコスト削減のためには、イーサ回線や波長多重を使用することができます。トンネルを使用することも可能ですが、切り分けが困難となるため、あまり推奨されません。

IPv6 普及期～5:5 の時期にかけ、相当のトラフィックが出てきた場合は、IX 事業者設備と同様、「デュアル型」の形態での提供が想定されます。

xSP 事業者が設備を更改する場合には、これらの移行シナリオを前提に設備を選定することが求められます。

xSP 事業者 IX 接続設備

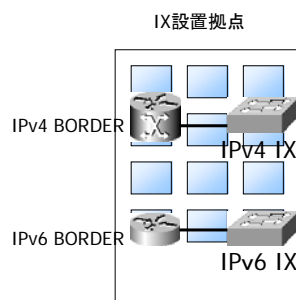
xSP 事業者の IX における接続設備の移行シナリオは、別回線型(別ルータ)、別回線型(別インタフェース)、デュアル型の 3 種類が考えられます。

別回線型(別ルータ)

これはIPv4、IPv6 で別個のルータを用意するパターンです。



(3)xSP事業者IX接続設備:別回線型(別ルータ)



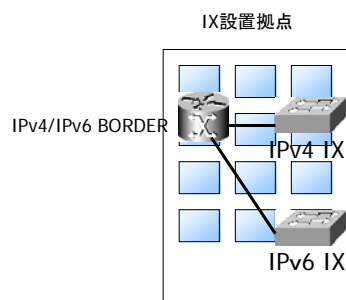
- xSPルータをIPv4、IPv6で別に準備する形態。
- IPv4、IPv6が混在しないため、IPv6トラフィックの影響を心配する必要がない。
- 既存のIPv4網と分離して運用することが可能。
- BGPに対応しているルータをIPv4/IPv6とで二重に準備が必要

別回線型(別インタフェース)

この場合、ルータは1台ですが、別インタフェースで行います。



(3)xSP事業者IX接続設備:別回線型(別インタフェース)



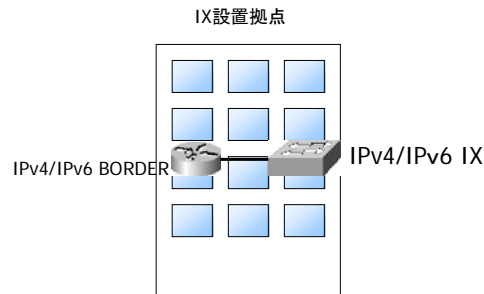
- xSPルータをIPv4, IPv6ともに一台で兼用するが別インタフェースにて接続する形態。
- インタフェースを、個別に準備する必要があるが、IPv4とIPv6で個別にトラフィックをコントロールすることが可能。

デュアル型

この場合は、1台のルータ、1つのインタフェースでIPv4とIPv6を接続します。



(3)xSP事業者IX接続設備:デュアル型



- xSPルータをIPv4, IPv6ともに一台で兼用し1つのインタフェースにて接続する形態。
- IX側がデュアルスタックに対応していることが必須。現状では、ほとんどのIX事業者設備が対応していないため、この形態での接続は少ない。
- 設備コストはIPv4とIPv6とのトラフィック総量に依存
- IPv4 / IPv6を分離してトラフィックを管理するのが困難

2004/12/21

IPv6普及・高度化推進協議会 移行WG 総会資料

77

xSP 事業者 IX 接続用設備 移行シナリオ

移行シナリオは前セクションとほぼ同様で、初期の段階ではリスクをおかさず IPv4/IPv6 別ルータでの接続が主流です。IPv6 普及期～5:5 の時期にかけ、「IPv4/IPv6 デュアルスタック」の形態で接続になると想定されます。

ただし、同一のインタフェースに IPv4/IPv6 が混在する場合、トラフィックのマネージメントが困難になるため、「同一ルータ・別インタフェース」の形態で運用される可能性もあります。また、IPv4 と IPv6 それぞれでトラフィックを取得する方法を確立する必要があります。

3. 普及期の想定課題

移行課題（総論）

普及期のときには IPv6 化が正当化される可能性があります、それでも移行が困難な面も残ります。

移行しなければならない理由は、以下の通りです。

- ・ 他社との差別化あるいは他社に遅れをとらないために
- ・ IPv6 のみにサービスを提供するxSP の出現

しかし、移行したくない理由も以下のようなものがあります。

- ・ コスト増 (IPv6 化にともなって必要となる追加機材、IDC なら追加フルルート購入等)
- ・ アドレス問題 (IPv6 アドレスをアップストリーム依存となると変更が不可能、IDC やホスティングサービスにおける、サーバ系のアドレスリナンバは事実上不可能)
- ・ 安定性 (IDC では、ルータやスイッチ以外の Middle Box が構成要素として入るので、それらの相互接続性や運用性の確保が難しい)
- ・ 運用面 (v4 と v6 のそれぞれの運用へのコストおよび人材の分配)

データセンターの普及期想定課題

データセンターの IPv6 普及のタイミング

iDC のタイプによって IPv6 への取り組みの熱意が異なります。

政府系や地方公共団体に密着している iDC (3 セク iDC) の IPv6 化は必須になるでしょう。電子政府関連の動向次第ですが、IPv6 化が必須になる可能性は高いと考えられます

また、キャリア系や ISP 系、あるいはバックボーンを持つ大規模な iDC は、IPv6 化が比較的容易に実施可能です。バックボーンの IPv6 化が進んでいれば iDC 自体の IPv6 化は容易です。形態にもよりますが、カスタマへの単純な IPv6 コネクティビティの提供も容易です。

しかし、独立系でかつホスティングの延長の、比較的中小規模な iDC では、IPv6 化が困難です。

これらの iDC は、たとえばアップストリームが IPv6 化していれば、アドレスがアップストリームからとなるので浮気がやりにくなります。また、カスタマからの IPv6 化への合理的な要望など、IPv6 化することについての必然性が出てくる、そして IPv6 化に必要なコストをまかなうことが可能となる、といった時点で IPv6 化を実施するでしょう。

つまり、iDC はカスタマの要望および周囲の状況次第です。また、iDC のカスタマは、エンドユーザであるアクセス系が IPv6 化されていないければ自身の IPv6 化を必要としない可能性が高いと考えられます。しかし、IPv6 のみで提供されるサービスが出現すれば別の展開も考えられます。

データセンターの移行課題（総論）

総論としては、iDC にとってもそのカスタマにとっても IPv6 化を正当化することはまだ難しいと言えます。つまり、経営面からいうとコスト増となるためにそれに見合うだけのメリットがないと積極的には移行に取り組めません。メリットには、技術的なものもあり得ますが、それについては iDC としてはかえって少ないと言えます。移行課題として、以下の点が挙げられます。

- ・現行の IPv6 アドレスの割り振り規則
- ・相互接続性を確認する機材の増加(相互接続性の確認の場合分けが倍以上に増える)
- ・カスタマに提供している様々なツールの IPv6 化(トラフィック情報、連絡先情報などの情報提供ツールや、カスタマ情報、連絡先情報、DNS やメールをはじめとしたサーバ情報など、カスタマ側の情報更新ツール)

普及期の想定

では、普及期となったときの iDC の形態はどのようになるでしょうか。

IPv4 のみの iDC	比較的小規模な IDC がそこそこの数存在する
IPv4 と IPv6 のデュアルスタックの IDC	大半の IDC がこうなる
IPv6 のみの IDC	ほとんど想定できない

iDC のカスタマとして想定される形態は次のようになるでしょう。

IPv4 のみのカスタマ	古くからのサービス提供者
IPv4 と IPv6 のデュアルスタックのカスタマ	大半の xSP
IPv6 のみのカスタマ	新たなビジネス展開をするための xSP が登場することは十分考えられる

IPv6 Ready データセンターへのプロセス

バックボーンの IPv6 化は比較的容易です。カスタマエッジの IPv6 も、実現形態次第ではありますが、比較的容易です(ネイティブの提供、トンネルによる提供)

逆に、カスタマ側の IPv6 化は、カスタマの実装に依存します(カスタマ側のエッジの機器、特に Middle Box)

問題は、エッジルータ、ファイアウォール、ロードバランサの IPv6 対応です。

普及期に向かうための想定課題

IPv6 トラフィックの増加

特にデュアルスタックルータの問題として、以下があります。

- ・増え続けるルーティングテーブルへの対応
- ・機器によって IPv6 ルーティングはソフトウェア処理で行なっている場合がある
- ・IPv6 のバーストラフィックのときに、IPv4 を安定してルーティングできるか？

また、IPv6 で安定して動作する冗長化プロトコルは、OSPFv3、VRRP IPv6、ESRP、HSRP などのうちどれかがまだはっきりしていません。

トラフィックパターンは、データセンターからユーザに向かっていくトラフィックが多い現在のトラフィックパターンから変化する可能性もあります(例:IPv4とIPv6でトラフィックパターンが違う、新たなアプリケーションの出現によるトラフィックパターンの変化)。

SLA 問題

顧客に対して SLA を定めている場合に、データセンター側のバックボーン等がデュアルスタックネットワークに移行しても、その SLA を変更せずに提供できるかという問題があります。適切な冗長化の採用、さらに、IPv6 と IPv4 で別の SLA が必要かどうかの検討も要求されます。

放送と通信の融合、nonPC 機器のインターネット利用

通信・放送融合による放送連動デバイスの増加や情報家電機器デバイスの増加により、データセンターにサーバを設置する事業者が増えてくると、データセンターが果たす役割がますます大きくなっていくことが想定されます。

ホスティングサービスの想定シナリオ

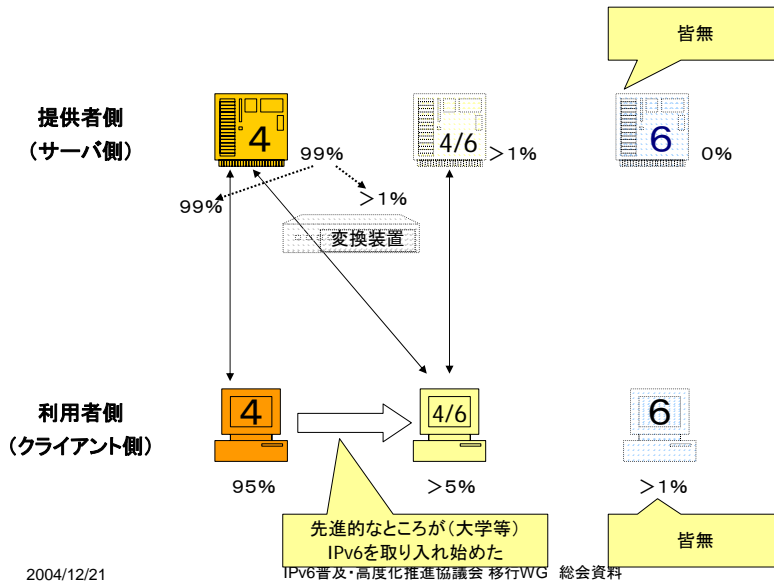
ホスティングサービスに関しては、現状と普及期で、以下のような状況になると想定できます。

現状モデル

提供者側 ほぼすべてのサーバが IPv4 Only
ユーザ側 ほぼすべてのユーザが IPv4 Only
 先進的なユーザが一部 IPv4/IPv6 デュアル環境



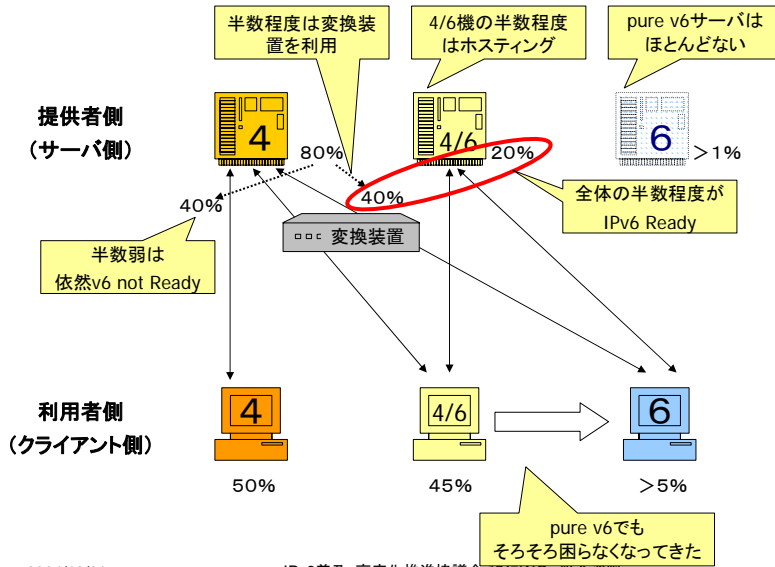
現状モデル



普及期想定モデル

提供者側 v6 Ready 率 50%
 トランスレータによる「簡易移行」率が比較的高い
 サイトを新しく作る場合は v6 対応させるケースがほとんど
ユーザ側 v4/v6 デュアル化が進んできた。v6 Ready 率 50%程度
 pure v6 への移行を検討している段階

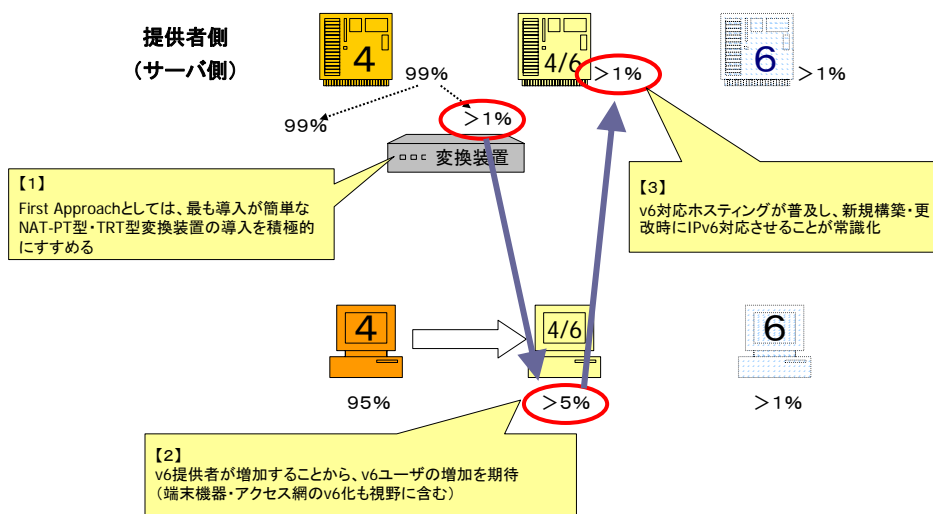
普及期想定モデル



移行シナリオ

移行シナリオは、以下のようにサーバ側、ユーザ側のIPv6 への移行の影響を受けます。

移行シナリオ



ホスティングサービス移行の技術的課題

普及期にかけてのホスティングサービス移行に関する技術的問題は、以下の通りです。

共通の問題

OSI 参照モデルに則らないシステムへの対応が問題となります。HTML ファイルのレベルなら「コンテンツフィルタ」で回避は可能ですが、独自に作りこんだ製品は問題が複雑になる可能性があります。

また、DNS の問題については、DNS を真っ先に移行すればよいだけなので問題はありません。DNS 貸しサービスはどここの ISP でもやっていますが、IPv6 のみの対応は、現状では皆無に等しい状況だということもあります。

トランスレーションサービスの場合

ホスト認証の問題とログ管理の問題のトレードオフがあります。しかしこれは、ログを簡単に管理できる NAT-PT 型変換装置の出現で解決できます。

また、踏み台アタックへの懸念については、動的フィルタリングの実装で解決できます。これは F/W 連携 IDS と同じ仕組みです。

デュアルスタックホスティングサービスの場合

これに特化した技術的問題は特にありません。

普及期の次の一歩

前述の普及期想定シナリオは、簡易移行による対応が大半でした。その次の段階に進むには、次のような課題が残されています。

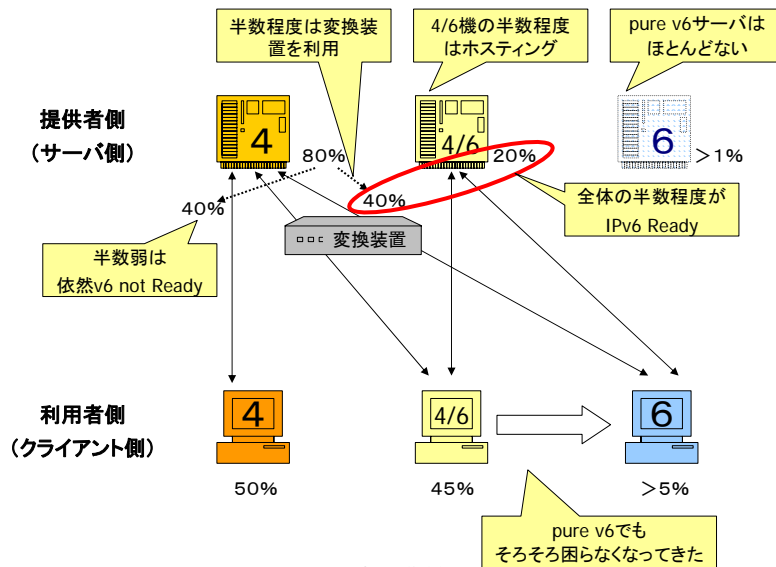
- ・ 簡易移行(トランスレーションサービス)を本移行(デュアルスタックホスティングサービス)にする方法
- ・ 未移行サーバを(簡易)移行させる方法
- ・ pure v6 への道(v4 の捨て方)

想定シナリオ

普及期の次の一步として想定するのは、次のような状況です。



想定シナリオ



2004/12/21

IPv6普及・高度化推進協議会 移行WG 総会資料

96

課題の解決に向けて (1)

普及期に未移行サーバを移行させる方法としては、ISP やiDC がトランスレータサービスをバンドル化することが考えられますが、コストをどのように正当化できるかという問題が残ります。

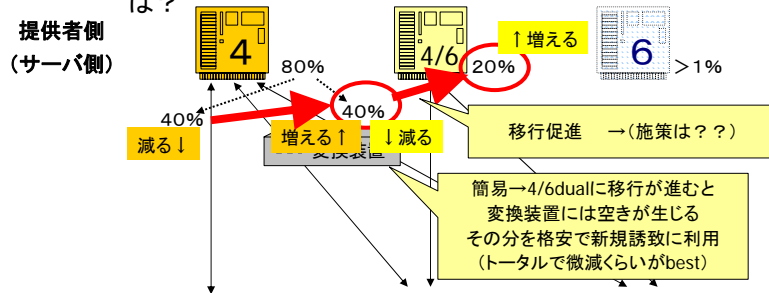


課題の解決に向けて(1)

■ 未移行サーバをどうやって移行させるか

□ ISP・iDCがトランスレータサービスをバンドル化

- トランスレータの利用ピークを超えて空いてきた部分を無償or格安提供
- 初期投資で費用回収していれば後は格安提供できるが、原資は？



2004/12/21

IPv6普及・高度化推進協議会 移行WG 総会資料

97

課題の解決に向けて (2)

簡易移行を本移行にするためのタイミングとしては、システムの更改がかぎとなります。



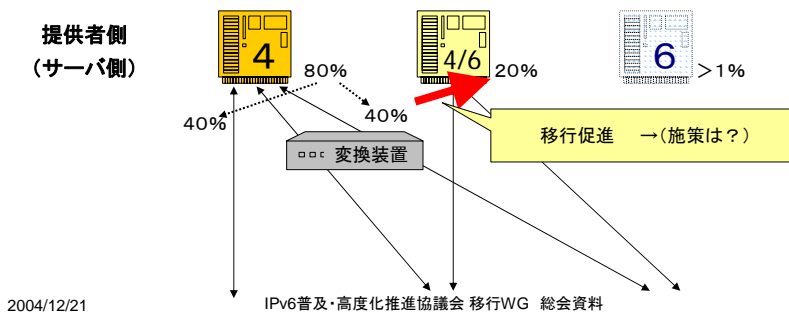
課題の解決に向けて(2)

■ 簡易移行をどうやって本移行にするか

□ タイミングとしては、システムの更改が鍵

- 新設サーバはDualStackが常識になっている(仮定)

□ ノウハウ蓄積・競争原理によるDualStackホスティング料金の低廉化



2004/12/21

IPv6普及・高度化推進協議会 移行WG 総会資料

98

課題の解決に向けて（3）

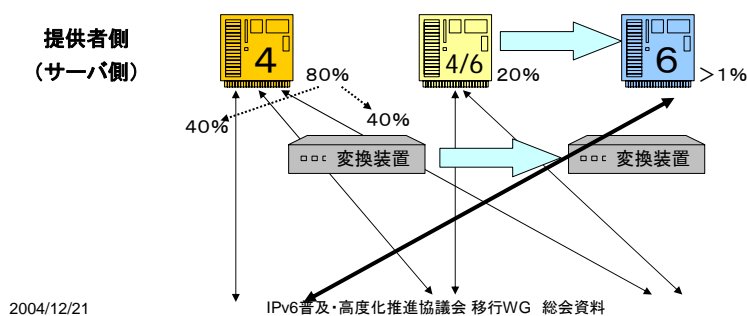
IPv4 を最終的に廃止し、サーバの pure v6 化を進めるには、トランスレータを逆向きに使用することも検討の視野に入っていきます。



課題の解決に向けて(3)

■ v4の捨て方

- トランスレータを逆向きに使用し、サーバのpure v6化を進める
 - 移行が進んで空いてきたトランスレータを利用できればなおhappy
 - v6>v4なので、射影アドレスは使えない(静的NATのようにいちいち手で設定してやらないといけない)が、このころには数も少ない、はず。



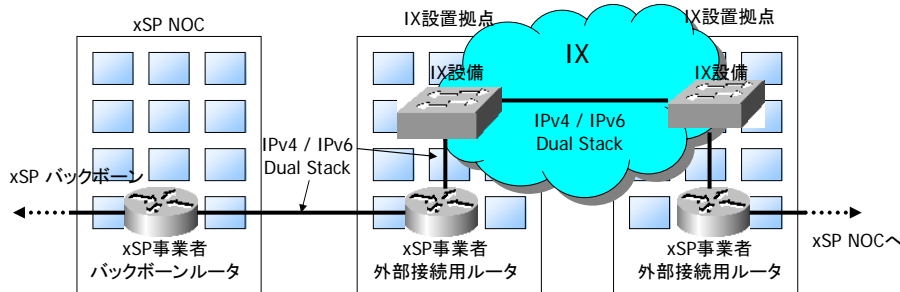
IXの普及期想定課題

普及期におけるIX構成

普及期には、IX事業者側、xSP事業者側ともにデュアルスタックで設備／回線を利用します。



普及期におけるIX構成



- 普及期においては、IX事業者側はIPv4とIPv6を区別／分離せずに設備／回線ともにデュアルスタックにてサービスを提供する。
- IX利用者であるxSP事業者側も同様にデュアルスタックで設備／回線を準備する。

IXの普及期に向かうための想定課題

リンクアグリゲーション時のIPv6 負荷分散

IXの普及期に向けては、リンクアグリゲーションのときのIPv6負荷分散が課題になります。

リンクアグリゲーション(LAG)を用いてIXスイッチ間を構成している場合に、IPv6通信ではMACアドレスによりトラフィック分散を行う装置が存在します。

現在はIPv6トラフィックが少ないため問題となりませんが、トラフィック量が増えてきた場合には、IXスイッチ間接続のトラフィックが片方の線に集中しトラフィック溢れを引き起こす可能性があります。

単一のプロトコルしか要らないユーザへの対応

IPv6(v4)はいらないと言われたときのプロトコルフィルタをどうするかという課題もあります。IXユーザが都合により、デュアルスタックIXであってもIPv6(またはIPv4)は不要と申し出る可能性が考えられます。現在のIXスイッチではプロトコルフィルタをできない機器が存在するため、そのようなユーザの要求を満たせない場合があります。

スイッチのパフォーマンス問題

IPv6 処理が IPv4 処理に比べてパフォーマンスが出ない機器が存在します。これについては、ベンダーへの改善要求が必要です。

IX 付与アドレス以外を使っても通信できてしまう問題

IX がユーザに割り当てた以外のリンクローカルアドレスでも BGP ピアが成立してしまいます。これは IX 側では事実を把握することが難しい問題です。

6bone アドレス (pTLA/pNLA) の移行

6bone や 6bone-jp が割り振りを行っていた実験用アドレス(3ffe::/16)については、2006 年 6 月 6 日に廃止されることが決まっているため、IX 上で交換している経路にこれらが含まれる場合には、アドレスのリナンバが必要となります。

参考文献

RFC3701 6bone (IPv6 Testing Address Allocation) Phaseout

(<http://www.ietf.org/rfc/rfc3701.txt>)

⇒移行方法としては、手設定によるリナンバが推奨されています。移行手順については、ISP-SWG 資料の Tips を参照してください。

ユーザ側における想定課題

ルータのパフォーマンス向上

IPv6 処理が IPv4 処理に比べてパフォーマンスが出ない機器が存在します。これはベンダーへの改善要求が必要です。

IPv6 only ユーザの出現

IPv4 アドレスが付与されなければ、ルータ ID のバッティングが起こる可能性があります。このため、IPv4 アドレスを付与して運用を行うように徹底する必要があります。

移行 WG データセンターセグメント 検討メンバ

(敬称略)

チェア

沖本 (NTT 西日本)

メンバ (敬称略、五十音順)

荒野 (インテックネットコア)

石井 (インターネットマルチフィード)

石田 (MEX)

石原 (KDDI)

植 (NTT スマートコネクト)

片山 (NTT 西日本)

谷崎 (NTT スマートコネクト)

西野 (JPIX)

平尾 (JPIX)

古川 (NTT 西日本)

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下さい。

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