# IPv6 オペレーション研究会

# 第一次中間報告

# 1.はじめに

近年、IPv4 のアドレス枯渇が深刻な問題として取り上げられている。この解決策として膨大なアドレス空間を持つ次世代の IP プロトコルである IPv6 が提案された。しかし、これまでとは異なる新しいアドレス体系を採用するためには、その移行に際してさまざまな問題点を生じることは明らかである。

現在の IPv4 ネットワークに関する運用技術は、インターネットがごくわずかのネットワークでしか使われていない時代から現在に至るまで、長い時間を掛けて蓄積されてきた。しかし、IPv4 から IPv6 への移行については、IPv4 の利便性を損なわない形で移行してゆく必要があり、IPv6 ネットワークの運用について事前に十分な検討をしなくてはならない。このためには、IPv4 での現状の運用形態や利用技術を十分理解し、IPv6 でどのようにその技術を適用できるか、そして新しく必要となるものは何かを洗い出し、問題となる部分については、あらかじめ検討しておくことが必要である。

IPv6 オペレーション研究会は、このような問題意識を持った有志があつまり、IPv4 ネットワークから IPv6 ネットワークへの移行、そして、IPv6 ネットワークとなったときの考えられるネットワークモデル、必要技術、運用方法などを運用者の立場から検討し、来るべき時期にスムーズに IPv6 ネットワークを利用が開始できることを目的として 2001 年 1 月に組織された。

研究会発足後、実効的な結果をスムーズにだすために、いくつかの少人数で構成されたサブグループに分けられ議論を行うとともに、サブグループ間の意見交換を行うめの全体ミーティングを数回行った。これに加え、日本国内で IPv6 の普及活動を行っている IPv6 デプロイメントコミッティと連携することで、より多くの有識者との意見交換を行いながら検討を進めた。

本文書では、当研究会が発足してから、現在に至るまでに検討された内容について報告し、IPv6 ネットワークで必要となる運用技術とそれらに関連した検討が必要な事項に関して、問題提起を行う。

# 2.トランジッション WG

## 2.1.目的

本 WG では､インターネットが現在の状態から IPv6 を基盤とする次世代のネットワークシステムに移行する際に必要な技術、検討項目、あるいは課題について洗い出す。

## 2.2.背景

インターネットにおいて実ネットワークの構築・運用に携わるオペレータ、あるいはエンジニアにとって IPv6 はまだまだ未知の世界であり、すでに存在する安定したネットワークを IPv6 対応にするための移行、すなわち「トランジッション」に大きな不安や問題を抱えているのも事実である。

このような背景から、実ネットワークを構築・運用するオペレータの視点から、IPv6 への移行に際して必要になる技術や検討項目、あるいは課題について洗い出し、次期ネットワークシステムへのスムーズな移行への橋掛かりとなることを目指して本 WG の発足に至った。

## 2.3.検討項目

- IPv6 への移行ストーリーのフェーズ分け
- フェーズ毎の課題の洗い出し
- 各フェーズにおいて必要になる技術の洗い出し

## 2.4.検討の視点：

本 WG では、まず IPv6 への移行にあたって、検討の視点を分類した。検討はユーザあるいはサービス提供者などの視点が考えられるが、本 WG では、検討の視点を以下のように分類する。

- ホームユーザ
  - 個人、あるいは So-Ho など、家庭などでインターネットに接続するケース
- 組織ユーザ
  - 企業や大学など、なんらかの組織がインターネットに接続するケース
- サーバ・ホスティング
  - データセンターなどに設置されるサーバ、あるいはホスティング事業者など
- アクセスプロバイダ
  - ダイヤルアップ、CATV、ADSL、あるいは専用線などエンドユーザにサービスを提供する ISP
- バックボーンプロバイダ
  - 二次 ISP、あるいは大企業などに対してトランジットを提供するケースなど
- 新サービス、新エリア

- これまで IPv4 の世界では提供されていなかった、IPv6 独自の機能やサービスなど

以下に検討の視点の分類について、イメージ図を掲載する。

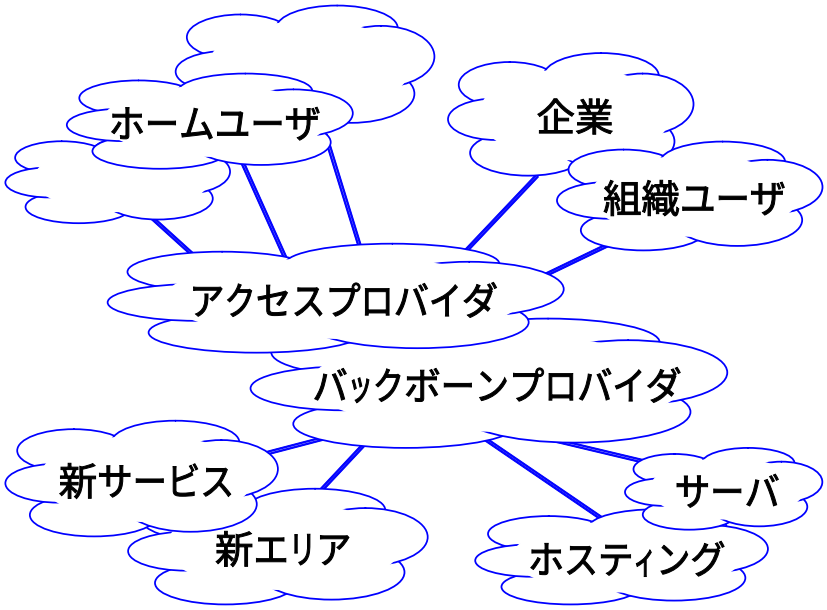


**図 1　ネットワークの構成要素**

### 2.5.移行のフェーズ分け

IPv6 への移行は、ある日突然すべての機器が IPv6 になるわけではなく、順次、少しずつ IPv6 対応の機器、あるいはサービスが普及していくことが予想されている。本 WG では、これらの移行のシナリオを IPv6 の普及率でおおよそのフェーズ分けを行い、以下のように 3 分類して議論を行った。

(1)Phase1（IPv6 導入期）

IPv4：IPv6 が 9:1 程度までの段階、ほとんどの機器が IPv4 で通信を行い、わずかに IPv6 対応の機器が導入され始めた段階を意味する。本フェーズでは IPv6 というプロトコルが利用できることが重要であり、まずは「使ってみることができる」ことを主とするフェーズである。

(2)Phase2（IPv6 普及期）

IPv4:IPv6 が 5:5 程度、すなわち多くの機器が IPv6 に対応するようになってきており、IPv6 のサービスもごく普通に利用されているが、同時に IPv4 の機器、サービスが残っている段階。本フェーズではすでに多数の IPv6 機器がインターネットに接続され、商用を含む多数の（現状と同じかそれ以上に多くの）サービスも IPv6 で提供されていることになる。したがって、単に使えるだけではなく、品質、安定性などの面が重視される。

(3)Phase3（IPv4 衰退期）

IPv4:IPv6 が 1:9 程度。このフェーズでは、すでに多くの機器が IPv6 対応しており、一部の時代の流れにおくれた機器やサービスが IPv4 でかろうじて残っている段階。

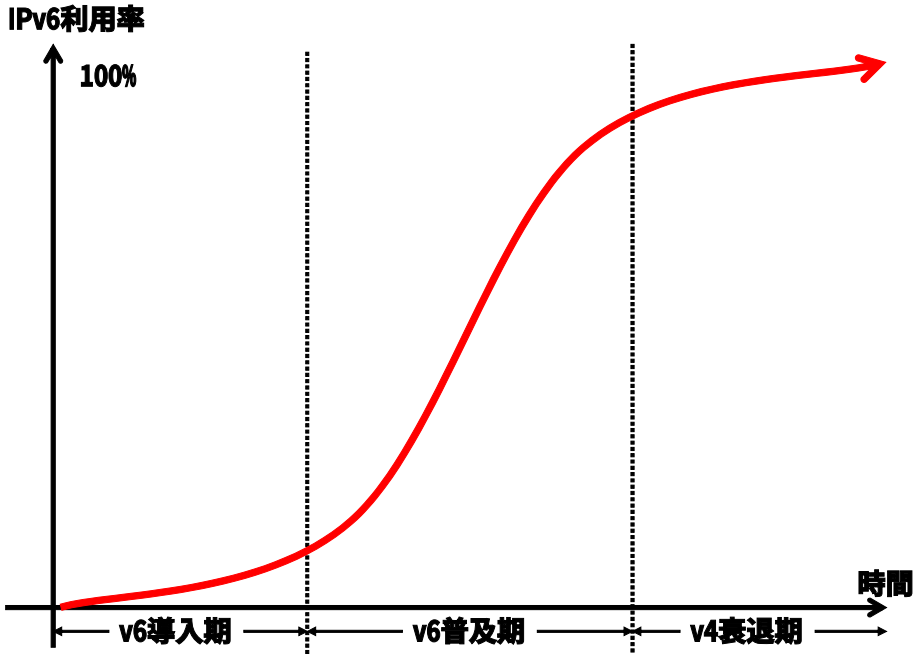


図 2　IPv6 の導入フェイズ

**2.6.検討の具体的な内容：**

以下では、議論において洗い出された、各フェーズで必要とされる技術、検討項目、あるいは課題について述べる。ただし、ここでは特にユーザーネットワークに関する IPv6 の移行について詳しくブレークダウンしてある。残りの視点については次回以降の検討で深めて行く予定である。ご了承いただきたい。

2.6.1.Phase1：IPv6 導入期

(1)ホームユーザの IPv6 導入

ホームユーザの環境において IPv6 を利用するためには、まず PC のネットワーク環境が IPv6 対応する必要がある。このため、OS(Operating System)やインターネットを利用するための基本ソフトウェア（Mail、Web、DNS）などの IPv6 対応が必須である。特に Windows XP では簡単な操作で IPv6 プロトコルスタックが利用できるようになっており、今後、Windows XP、もしくはその後継機種の普及が期待される。

また、ホームユーザでは家庭にホームルータを利用しているケースが増えてきている。このような環境ではホームルータが IPv6 に対応する必要があり、家庭用の ISDN や ADSL ルータのデュアルスタック化が必要である。

(2)企業ユーザの IPv6 の導入

企業ユーザにおいても、前述のようにユーザの PC 環境の仕組みが IPv6 に対応する必要があることは当然である。同時に、企業ユーザなどではファイヤウォールの存在が必須であり、その IPv6 対応が急務である。多くの企業ではファイヤウォールに様々な機能を付加して利用しているが、IPv6 導入期は IPv6 を利用できるようにすることが優先であり、ファイヤウォールにおいても、最低限のアクセスフィルタなどが利用できることが求められる。

また、企業ユーザにおいては、一般的に外部向けのメールサーバ、ウェブサーバを準備しており、また、社内外において DNS を利用している。IPv6 対応においても、これらのサーバや DNS サービスの IPv6 対応が必要である。また、DNS においては、非人間的なアドレスを登録するために、便利なツールや仕組みが提供される必要がある。

(3)サーバ・ホスティングにおける IPv6 の導入

サーバにおいては OS やサーバアプリケーションの IPv6 対応が必要である。特にサーバ系では Unix 系の OS が使われているほか、最近では Windows NT や XP なども多く利用されるようになってきている。これらの OS、およびその上で動くアプリケーションが IPv6 対応になる必要がある。また、ウェブサービスではクライアントの IP アドレスを判断するように CGI やその他の仕組みを導入しているケースもある。このように IPv4 アドレスを利用している独自の仕組みについても IPv6 化の必要がある。

また、サーバ・ホスティング事業者の場合、その管理系（MRTG、SNMP、MIB） も重要な検討項目である。これらの管理系ツール、あるいは管理プロトコルの IPv6 対応も併せて必要である。

(4)アクセスプロバイダにおける IPv6 の導入

一部のアクセスプロバイダでは IPv6 サービスを開始している。IPv6 サービスはトンネルサービスを利用するもの、および専用線のサービスを利用するものが中心である。ここで、例えば専用線サービスなど通常のルータで対応可能な範囲についてはすでに、かなりのレベルで IPv6 対応が進んでいると考えられる。また、特に初期の IPv6 サービスではトンネルサービスが多く利用されることが予想されており、同サービスを提供するアクセスプロバイダにとっては、商用レベルでのトンネル終端装置が必要になる。

また、個人ユーザなどに対してはダイヤルアップや CATV、ADSL での接続性の提供も課題である。これらのサービスを本格化するためには、IPv6 におけるアドレス割り当ての方式やアドレッシングのルール化が必要である。また、フレッツ系サービスや ADSL サービスなど、アクセスラインを他事業者に依存している場合、そのアクセスラインの IPv6 対応も必要である。

(5)バックボーンプロバイダにおける IPv6 の導入

バックボーン ISP における IPv6 対応はかなりの範囲で進んでいるとされている。多くのルータベンダではすでに主要な製品の IPv6 対応を進めており多くがβリリース、一部では正式リリースされている。バックボーン ISP ではこれらの IPv6 ルータを用いて独立なネットワークを構築し、IPv6 コネクティビティを提供するサービスを開始している。

なお、本格的に IPv6 サービスを展開するためには、IPv6 による OSPF や ISIS などバックボーン内部の管理を行うための IGP の開発、および安定化も重要なファクターである。

(6)新サービス・新エリア

家電・車など、様々な分野で期待されているが、新エリアについては未知の分野であること、また Phase1 は「まずは使えること」が重視されるフェーズであることから、新サービス・新エリアについては Phase2 以降で検討することとした。

### 2.6.2.Phase2：IPv6 普及期

Phase2 では IPv4:IPv6 の比率が 5:5 程度を考えており、そのため、多くのインターネットユーザがごく普通に IPv6 を利用するような状況を想定している。このフェーズでは、Phase1 での「まずはえること」という状況から、「商用のサービスが安定して使えること」という、品質を重視するようになることが重要なポイントである。

(1)ホームユーザへの IPv6 の普及

Phase2 では、すでに多くの PC が IPv6 対応になっていることが想定される。またホームルータを利用しているケースでは、そのデュアルスタック化も進んでいる。このフェーズでは、広く、一般のユーザが IPv6 を利用するようになることから、ユーザが IPv6 を意識せずに利用できる環境、すなわち Plug&Play、自動設定が問題なく利用できるようになっている必要がある。

また、Phase2 では、新エリアから、例えば家電などの IPv6 のみをサポートする機器(以下、v6 only node)が登場する可能性がある。ホームユーザのネットワークではこれらの v6 only node も自動的にネットワークを利用できるように接続できることが必要である。

(2)企業ユーザへの IPv6 の普及

企業ユーザでは、Phase2 に向けて本格的に IPv6 を利用するようになる。特に企業ユーザが「全体重をかけて」インターネットを利用する場合、ファイヤウォールの機能はきわめて重要であり、IPv6 における「商用の」ファイヤウォールの登場は必須である。ファイヤウォールではこれまでの IPv4 の機能と同等のアクセス制御が full ACL、wire speed でできることが期待される。一方で、IPv6 では P2P(Peer-to-Peer)モデルの浸透により、新しいセキュリティモデルが必要になる。これについてはさらに議論が必要であるが、P2P に対応してどのような機能が必要になるか、について検討が必要であ

る。

また、企業においては、社内システムや業務系のアプリケーションを多く利用している。企業内のユーザが IPv6 対応を進めるにあたっては、IPv4 との重複管理を避けるため、IPv6 への統合化が進められることが予想される。したがって、社内システムや業務系のアプリケーションも IPv6 対応化が求められる。

新エリアからはオフィス機器が IPv6 に対応し、ネットワークを利用したサービスが開始される可能性がある。例えば、FAX やコピー機、電話、など、多くの危機が IPv6 を利用することがある。そのため、Plug&Play に代表される動的なネットワーク設定やオフィス機器に関する通信のセキュリティモデルの確立なども課題になりそうである。

(3)サーバ・ホスティングにおける IPv6 の普及

サーバ・ホスティング事業者においては、商用品質のウェブサービス、あるいはコンテンツ提供サービスを提供するために、サーバやアプリケーションの IPv6 化に加えて、ロードバランサやキャッシュサーバなどのアクセラレータについても IPv6 対応が必須である。また、管理システムについても単純なプロトコルの IPv6 対応ばかりではなく、例えば Open View やその他の商用、もしくは商用レベルのネットワーク管理システムが IPv6 対応になる必要がある。

サービス面については、コンテンツ配信ネットワーク（CDN）などの普及が進んでいるが、IPv6 化に向けて、これらのサービスの IPv6 対応が必要である。

(4)アクセスプロバイダにおける IPv6 の普及

多数のユーザが IPv6 サービスを利用するようになるにつれ、アクセス系のメディア、例えばダイヤルアップや CATV、ADSL など IPv6 利用が必須になる。特にアドレス割り当ての方法や、その際にユーザ側に不用意な設定が発生しないような仕組みが必要である。現在の IPv6 の標準化においては、これらの個人ユーザの環境においてアドレスを割り当てる統一的な仕組みやユーザにネットワークが割り当てられたときのユーザ側の設定については明確に定められていない。これらの仕組みについても早期に解決が必要である。

また、個人ユーザなどの場合、認証系のサーバ、あるいはプロトコルの IPv6 対応も重要な課題である。RAS、RADIUS の v6 化などは早急に必要になると思われる。その他、個人ユーザの課金情報や接続情報などのアドレスに依存するようなレジストリシステムについても IPv6 対応の検討が必要である。

(5)バックボーンプロバイダにおける IPv6 の普及

バックボーン ISP においては、インターネットを支える基幹網であるため、早期から IPv6 対応が進められている。IPv6 普及期においてももっとも最初に成熟するのはバックボーン ISP であると思われる。一方、IPv6 バックボーンを商用品質で運用するためには、現在よりもはるかに大規模なバックボーントポロジにおいて安定して動作する IGP の利用が必須である。また、既存のネットワークにシー

ムレスに IPv6 ネットワークを展開するためには、Core ルータにおいて IPv6 プロトコルスタックが安定して動き、デュアルスタックで問題なく動作する必要がある。

なお、既存の IPv4 バックボーン上にシームレスに IPv6 ネットワークを展開するひとつの方法として、MPLS バックボーン上で Core LSR を共有し、Edge LSR において IPv6 サービスを展開する方法も提案されている。

(6)新サービス・新エリア

新サービス、新エリアとして家電や車、電話などの新しいインターネットデバイスが登場する可能性がある。これらの新 IPv6 ノードは、既存のホームネットワーク、あるいは企業ネットワークに対して、Plug&Play やセキュリティなど、さまざまな要望がでることが想定される。ただし、いずれも通信モデルから、既存のものとは大きくかけ離れたものになることが想定されるため、ここではこれ以上の議論は行わないこととした。

#### 2.6.3.Phase3：IPv4 衰退期

本フェーズは IPv6 が普及し、かつほとんどの機器やサービスで IPv4 から IPv6 への移行が完了している時期である。同フェーズでは時代の流れとしてほとんどが IPv6 対応になっており、実質的に残りの IPv4 機器、IPv4 サービスがすべて IPv6 対応に置き換わるのは時間の問題であると予想される。

技術面について、同フェーズに関して予測、予想をすることは極めて難しいが、本 WG の議論では、特に企業ユーザで、独自に社内システムを構築しているケース、あるいは業界・業際ネットワークにおいて独自プロトコルを TCP/IP 上で利用しているケースなどで、IPv6 対応が遅れることありうると指摘された。これらのシステム・プロトコルでは、独自仕様、独自開発であることが多く、そのため、あらたに IPv6 対応にするための設計・開発・導入・置き換えが多大な負担になりうるためである。

### 2.7.考察

本 WG では IPv6 移行の各フェーズにおいて、ホーム・企業ユーザ、プロバイダなど、いくつかの視点から必要な技術、検討項目、課題について議論した。本 WG の議論では、バックボーンプロバイダの IPv6 対応が順調に進んでおり、アクセスプロバイダについても IPv6 の商用サービスを提供できるまでに対応が進んでいる、もしくは目処がついているとの意見が強かった。一方、ユーザの視点から見た場合、ホームユーザは何らかのタイミングで PC を買い換える、もしくは OS をアップグレードするなどによって IPv6 に対応できるチャンスが多くあるものの、特に企業ユーザなどでは独自開発、独自仕様の社内システムがあること、あるいは業務系の独自プロトコルが動いていることなど、移行に際して非常に大きな労力を必要とすることが指摘された。

別の視点からは、IPv6 への移行にあたって新サービス・新エリアと呼ばれる分野が非常に期待されている。例えば、IPv6 を用いた家電製品のネットワーク利用やインターネットカー（車）の登場など、様々なアプリケーションが考えられているのも事実である。これらの新エリアは、新たに市場を形成するものであり、それ自身が IPv6 への移行に関する問題を抱えるものではないが、例えば、ホームネ

ットワークへの IPv6 家電の接続など、他のネットワークへの影響を伴うことが予想される。本 WG でも今後、新エリアについても広くサーベイを行っていきたい。

# 3.アドレスポリシーWG

## 3.1.目的

日本の ISP が次々と IPv6 商用／試験サービスが開始するにつれ、現在暫定的に制定されている「Provisional IPv6 Assignment and Allocation Policy Document」の不備が明らかになってきた。そこで本 WG は IPv6 アドレスポリシーを検討し、早期に世界に向けて提案し、グローバルポリシーとして成立させることを目的とする。JPNIC や IPv6 普及・高度化推進協議会と連携しつつ、活動を行った。

## 3.2.背景

2002 年 2 月現在、有効な IPv6 アドレスポリシーは「Provisional IPv6 Assignment and Allocation Policy Document」である。

http://www.apnic.net/drafts/IPv6/IPv6-policy-280599.html

このポリシーは RIR(Regional Internet Registry)が 1999 年 5 月に RFC2374 をもとに暫定的に制定したものである。1999 年 7 月にはこのポリシーをもとに RIR が割り振りを開始した。2001 年 10 月末現在で、103sTLA がアドレスを取得している。

このポリシーは主に sTLA 取得条件等を規定しているが、基本的には次の２点で問題をはらんでいる。

(1)全面的に IPv4 の考え方を踏襲しており、IPv6 の特徴を考慮していない

例えば、典型的には「追加割り振り 80%」ルールがある。これは、LIR(Local Internet Registry)がアドレスの追加申請を行う場合に、その 80%を使用しきったら、次のアドレスを申請できるというルールであり、アドレス枯渇が問題になる IPv4 では有効な考え方である。

しかし、アドレス量が豊富な IPv6 において、この 80%は意味を持たないばかりか、経路集約やアドレスの内部管理という意味で ISP に大きな負担を与えている。IPv4 と IPv6 の特徴をよく勘案しつつ、IPv4 の考え方を踏襲すべき部分、IPv6 の特徴を考慮した考え方を採用する部分などを考慮する必要がある。

(2)未規定部分が多い

例えば、Assignment の大部分、初期割り振り/35 以降の割り振り方法(TLA になるやり方も含めて)、LIR から二次 ISP への割り振りなど、未規定部分が多い。日本の ISP がアドレス管理実務を実行するには不明なところが多く、不都合がある。

そこで、(1)(2)を解決するような新ポリシーの提案を、IPv6 ネットワーク的に最も進んでおり、最も新ポリシーを必要としている、日本から行うこととした。昨今、アドレスポリシーはグローバルにも RIR が開催するオープンポリシーミーティングなど、ボトムアップに提案、議論、決定される流れとなっており、このプロセスの中で、日本からの提案を APNIC, RIPE/NCC, ARIN に持ち込むこととした。

以下を主なポイントとしている。

- 具体的ポリシーの緊急性
- 経路集成の重要性の認識
- アドレス節約の非重要性の認識
- 経路集成を考慮した割り振りアドレス条件と割り振り量
- 割当て基準や NLA 相当組織への割り振りの明確化

主体・とりまとめとしては、日本のアドレス管理を総括している JPNIC が代表し、本 WG では素案検討／ドラフト作成などに貢献を行った。

### 3.3.議論の流れ

(1)国内でのコンセンサス形成期(2001 年 6-7 月)

2001 年 2 月 13 日　　WG 開催（富山）

2001 年 5 月 11 日　　WG 開催（IIJ）

2001 年 6 月 14 日　　WG 開催（富士通）

JPNIC IP-USERS にて提案。JPNIC コミュニティとしておおむね趣旨を了解し、本件を APNIC などのレジストリに提案していくことを決議

2001 年 7 月 14 日　　WIDE 研究会にて発表・議論

2001 年 7 月 26 日　　JANOG BOF にて発表・議論

この間、JPNIC IP-USERS メーリングリストを通じて、意見募集し、最終的には 2001 年 8 月初旬 JPNIC IP アドレス検討委員会にてとりまとめて APNIC に意見として提出した。

(2)APNIC Member Meeting 台北・Policy SIG(2001 年 8 月)

8 月下旬の APNIC 会議では、日本からの提案以外に RIR 提案の計２つの提案がまな板の上にのった。RIR の提案は、日本の提案より大分きびしめのルールが記載されていた。

会議中にはこの２つの決着を図ることはできず、RIR／日本及び世界の IPv6 関係者(Steve Deering, Randy Bush など)の人々が集まっての夜通しの議論を通じて、２つの提案が１つにマージされた。このマージ案には双方の要望事項が折半した形で盛り込まれていた。

翌日マージされた提案がミーティングに再提案され、コンセンサスをえた。ただしポリシーはグローバルであるべきであり、RIPE 及び ARIN 会議にも提案し、コンセンサスをえることが条件とされた。

(3)RIPE 会議及び ARIN 会議(2001 年 10 月)

RIPE 会議、ARIN 会議が続いて行われ、ここに APNIC コンセンサスの提案を行った。RIPE 会議では他の提案が行われ、両者でも多少の温度差はあるものの、結論として、

- 日本からのポリシー緊急性の要求は認識
- 今後グローバルメーリングリストを作りそこで議論

ということが決議された。ドラフティングのためのタスクフォースを作り、12 月にはそれまでの議論をまとめて、interim policy を作成という方向性が、各リージョンの IPv6 WG/アドレス policy SIG chair (Thomas Naten: ARIN IPv6 WG chair, David Kessens: RIPE IPv6 WG chair, 荒野高志: APNIC Address Policy SIG chair)の間で合意された。

なお、グローバルメーリングリスト「global-v6@apnic.net」は APNIC がホストしている。

(4)ポリシー文書の提案と公開(2001 年 11-12 月)

ポリシー議論で曖昧なサマリーをもとにして議論していても焦点がずれる可能性があるため、具体的なポリシードラフトをベースに議論する必要があった。状況的には、単に誰かがドラフトを書いてくれるのを待っていても見込みがなかったということもあり、日本チームでドラフトを草案した。ドラフトは最初日本語で書かれ、それを JPNIC によって英訳するというプロセスをとった。

このドラフトはドラフティングタスクフォースに提案され、それを受けたタスクフォースではソルトレイクシティでの IETF（＋含む電話参加）でのタスクフォース会議などを経て、1 ヶ月程度検討が行われた。

最終的なドラフトは 2001 年 12 月 22 日にグローバルメーリングリストに提案された。ドラフトには草案に参加した日本メンバの個人名が謝辞の項に載っている。

(5) メーリングリストや RIPE 会議での議論(2001 月 12 月-2002 年 2 月)

その後、再度 RIPE 会議やメーリングリストでの議論を通じ、少しずつではあるが、議論が進展しつつある。ただ、初期割り振りの基準などでかなり意見に乖離が見られるような重要項目があったが、徐々にメーリングリスト上で調整を図っていった。

(6) APNIC 会議／ARIN 会議(2002 年 3-4 月)

3 月の APNIC 会議、4 月の ARIN 会議においては、この調整の結果として主要な項目を含む全体のポリシーについて、大まかにコンセンサスをとることができた。

(7)4 月 13 日現在の状況

以下のステップを残すのみとなった。

- APNIC/ARIN 会議を通じてコンセンサスを得た部分をドラフトに反映させる
- 4 月末に行われる RIPE 会議でのコンセンサス形成
- このあとに RIR による正式なドラフティングとドキュメントの承認

### 3.4.成果

#### 3.4.1.ポリシー提案根拠のための試算

ポリシーの提案において、なんらかの数値的な根拠は重要となる。そこで、ラフに数字的感覚を共有するためにいくつかの試算を行った

(1) IPv6 空間量と独立ブロック量

仮に 2000::/3 (FP=001)だけを考えただけでも（全体の 1/8 相当量)、この量は以下の独立組織に割り振りができる。

**試算 1**

65,000 カスタマを持つ ISP の場合、そのブロックは/32 に相当し、この規模の ISP は約 5.4 億収容可能である。

**試算２**

100 万カスタマを持つ ISP の場合、そのブロックは/28 に相当し、この規模の ISP は 3,400 万収容可能である。

**試算３**

典型的な組み合わせを考える。
1800 万カスタマ ISP(/24+/28+/32)が 52 万　＋
100 万カスタマ ISP(/28+/32)が 840 万　＋
それ以下の small ISP(/32)が 2.7 億

この結果、仮に最小割り振りサイズを/32 と規定した場合でも、おそらく十分な数の ISP ビジネスセクターにアドレスを割り振れると考えてよい。

(2)外部経路数と最小割り振りブロック

試算 3 の条件が将来、技術的に可能か？という疑問がある。すなわち、試算 3 の場合には、外部経路総数が 2.8 億という数になるわけであり、それがその時代で処理できるか？という問題である。現在の経路数が 11 万程度ということを考えると、桁違いに多い数である。これに関しては現時点では全く答えは不明と言わざるをえない。

ただ確かなことは、最低限 AS holder の数だけの経路はアナウンスされるということは間違いがないであろう。すなわち、1 AS holder あたりに割り振られる prefix 数を減らしたほうが安全だろうということが予想できる。例えば、10 万 AS がそれぞれ 2.0 prefixes/AS を保有した場合には 20 万 prefixes ですむ。

ただし外部経路数に関しては、（もし行われるならば）/48 パンチングホールマルチホームの影響がアドレスポリシーよりずっと大きい可能性がある。これは現在の IPv4 において、経路総数の半数がこれらの/24 パンチングホールであることからも十分危惧されることである。
マルチホームの詳細については 4 章を参照のこと。

(3)内部経路への配慮
IPv6 においては外部経路もさることながら、内部経路についても十分な配慮が必要である。IPv4 のダイヤルアップサービスなどではダイヤルアップルータ単位、すなわち数千ユーザ単位に 1 つもしくは少数のアドレスプリフィックスが割当てられるため、自然に内部経路が集約できる。一方、IPv6 では常時接続／静的アドレス割り当てが通常となるため、下手な設計を行うと/48 単位（すなわち 1 ユーザ単位）のアドレス集約しか行えない可能性がある。注意して設計を行うとともに、それをアドレスフラグメントをおこさなくて済むようなポリシーが必要となる。

ここでは内部経路数の試算を行った。

**試算その１**

ISP-A：420 万 customers = /26 相当
Aggregation 単位が
/48 だと IGP 420 万経路
/44 だと IGP 26 万経路
/40 だと IGP 16000 経路
/38 だと IGP 4100 経路

**試算その 2**

ISP B 1.3 億 customers = /21 相当
/38 でも IGP 13 万経路

現在、OSPF などの IGP で処理可能な経路数はせいぜい数千から数万といわれている。拡張を考えると、最低でも/38 レベルの aggregation が可能なように想定すべきであろう。

(4)追加割り振り基準

3.1 で述べたように追加割り振り基準を十分にゆるくする必要があり、この基準の根拠を示す必要がある。

仮に 50PoP(ほぼ都道府県数、中国の省の数 38)をもつ ISP に/32 を割り振られたと想定し、ここで初期設計として/38 を各 PoP に仮に分散したとする。ここで、この/38 を割り当てなおすこともなく、追加割り振りが可能な基準を求めることとする。

最悪シナリオは

- 49PoP がユーザ数 1　　（ほぼ/33+/34 を仮確保）
- 1PoP が 16000 を超えたとき (/34 を消費)

である。このとき、/38 の aggregation を確保したまま追加割り振りができるようにしたい。この場合、25%以下の追加割り振り基準が必要となる。

実際にはこのシナリオのような極端なケースはおそらく存在しないが、申請時間を考慮した「のりしろ」が一般には必要となり、25%以下という数値は（少なくともこの程度の最小割り振りサイズなどを想定した場合には）妥当であると考えられる。

### 3.4.2.ポリシードラフトの内容

12 月にグローバルメーリングリストに提案したドラフトの内容を紹介する。具体的なドラフトについては

ftp://ftp.cs.duke.edu/pub/narten/global-IPv6-assign-2001-12-22.txt

を参照のこと。

(1)基本的な考え方

アドレス管理には５つのゴールがある。

- 一意性　　uniqueness
- レジストリ DB への登録　　registration
- 経路の集成　　aggregation
- アドレスの節約　　conservation
- 公平性　　fairness

これらのゴールは相互にコンフリクトするが、これらの要素を上手にバランスさせることが重要である。この部分は従来の IPv4 アドレスの考え方を踏襲している。

しかし IPv6 が IPv4 とくらべて異なるのは、経路集成の優先度は高く、それにくらべアドレス節約の優先度は低いということである。この優先度については今後見直される。

ポリシーの項目的には以下の５項目を決める。

- 初期割り振り (基準／サイズ)
- 追加割り振り (基準／サイズ)
- LIR-to-ISP 割り振り
- 割当て
- DB 登録

(2)初期割り振り基準

申請を行う組織は、少なくとも/36 のプレフィックスが直ちに(つまり 3 ヶ月以内)必要であることを証明すれば、初期割り振りを受けることができる。HD-Ratio（後述）が 0.8 とすると，これは 776 sites(= 18.9% of /36)という値となる。

（注）この点については 2002 年 3-4 月の APNIC 及び ARIN 会議でのコンセンサスでは、以下のように変更されている。

- 776 サイトはエントリーバリアとしては高すぎる
- 第 3 者にアドレスを割当し、それを DB 登録するような LIR を対象とする
  （すなわちエンドユーザは含まない）
- ２年間のうちに少なくとも 200 の/48 を割当、登録すること
- 割り振りを受けたものが上記を満たせない場合にはアドレス返還を求められる場合がありうる

(3)初期割り振りサイズ

/32 のアドレスブロックの割り振りを受けることができる。それ以上の大きさのアドレスブロックが必要な申請組織は、その必要性を合理的に証明できる根拠資料を提出することで、必要なサイズの割り振りを受けることができる。これは次の式で表すことができる。

S(0) = shorter(/32, eval(必要なプレフィックス サイズ))

(注)eval(必要なプレフィックス サイズ)とは割振りを申請する申請者の要求プレフィックスサイズである。

(4)追加割り振り基準

追加割り振りは、組織(ISP/LIR)が、/48 を単位とするサイト数という観点で過去のアドレス使用の評価基準を満たした場合に実施される。HD-Ratio は、下に示す既存のアドレス ブロックの利用率を評価するために用いられる。

HD Ratio とは次の式で表される。

$$HD = \frac{\log(\text{number of allocated objects})}{\log(\text{maximum number of allocatable objects})}$$

例：HD ratio=0.8 のとき

| | ホスト数 | % |
|---|---|---|
| /36 | 776 | 18.9% |
| /35 | 1351 | 16.5% |
| /28 | 65536 | 6.3% |
| /24 | 602249 | 3.6% |

(5)追加割り振りサイズ

"n"番目の追加割り振り S(n)のサイズは次のようになる。

S(n) = shorter(S(n-1)-1, eval(two_years_req))

ここで、S(n-1)-1 は前回割り当てられたアドレス ブロックのサイズより

1 ビット短いプレフィックス アドレス ブロックのサイズを表し、eval(two_years_req)は申請組織の 2 年間の必要量に対する評価を表す。

(6)LIR-to-ISP 割り振り

組織(ISP/LIR)がアドレス空間を下位 ISP に割り振るための特定のポリシーはない。各 LIR 組織は、LIR に割り振られたアドレス ブロック全体の効率的な利用を確保するため、下位 ISP のための独自のポリシーを作成することができる。しかし、LIR は、下位 ISP からエンドユーザへの割り当てを含み、すべての/48 の割り当て状況を把握し、追加割り振りが必要になった場合に HD-Ratio が評価できるように割り当て状況を RIR/NIR に報告する必要がある。

(7)割当て

64 ビット目以降のアドレス空間は、IETF 領域[RFC2460]である。48 ビット目以降のアドレス空間はポリシー領域であり、IETF の推奨事項[RFC3177]および以下の割り当てを推奨する RIR の合意事

項[RIRs-on-48]となっている。したがって、割当サイズは

- 非常に規模の大きな申請者を除き、通常は/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
- 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

RIR/NIR は、LIR/ISP が実際にどのアドレス サイズを割り当てるかについて関与しない。そのため、RIR/NIR は、IPv4 の場合と異なりユーザーネットワークの詳細情報を要求しない。

ただし、単一のサイトが追加の/48 アドレス ブロックを必要とする場合、その要求の妥当性を示す文書および資料を提出して割り当てを請求できる。複数または追加の/48 の請求は、RIR/NIR レベルで処理と検討(つまり妥当性の判断)が行われる。

また、組織(ISP/LIR)は、IPv6 サービスオペレータのサービス インフラストラクチャとして、PoP ごとに/48 を割り当てることができる。PoP に対するそれぞれの割り当ては、PoP を利用するエンドユーザの数にかかわらず 1 つの割り当てとみなされる。一方、オペレータの社内業務に対して別途の割り当てを取得できる。

(8)DB 登録

IPv6 アドレス割り振りを受けた組織は、IPv6 アドレス割り当てを行う際、パブリック データベースにその割り当てに関する情報を登録しなければならない。情報は割り当てた/48 ネットワーク単位で登録される。各レジストリは個人情報の扱いに十分注意を払うべきである。

本件検討に基づいて 7/1 から世界各地域の RIR で新ポリシーが施行されている

http://www.nic.ad.jp/ja/pressrelease/2002/20020702-01.html

### 3.5.課題

2002 年 3 月 APNIC 会議、4 月の ARIN 会議／RIPE 会議、及びグローバルメーリングリスト上の議論を通じて、ポリシーの決着を図る。実際の交渉状況については、本 WG の手を離れていると考えており、必要に応じ、適宜検討を行うこととする。

また、アドレスポリシー関連の議論としては、常にここで終わりというようなことはないわけであり、今後、

- ユニークアドレスを必要とする企業ネットワークへのアサインメント
- 運用経験上で必要であるとわかってきたポリシー

などについても、適宜提案を行っていく。

# 4.ルーティング WG

## 4.1.目的

本 WG では、IPv6 が ISP のルーティング運用にどのような影響を与えるかを検証し、どのような対応が必要なのか課題を洗い出す。

## 4.2.背景

ISP の運用者にとって経路の管理は頭の痛い問題である。経路制御の観点から言うと、アドレスをある程度地域毎に集約して、経路数を減らしたいが、アドレスの不足、ネットワークのトポロジの変更などにより、なかなか集約化が図れない。

IPv6 では豊富なアドレスを利して、この運用上の問題を解決できるのではと期待される。アドレス割当の管理組織もアドレスの集約を考慮したアドレスポリシーを策定している。しかし、IPv6 の導入は新たな問題を引き起こすかもしれない。たとえば、インターネットに接続される端末数の増加は、絶対的な経路数の増加を招く。

研究会では運用者の立場から、IPv6 のルーティング管理に与えるインパクトを評価し、問題を解決するモデルを検討していくこととなった。

## 4.3.議論のポイント

ISP のルーティング運用は、ユーザや POP の経路を管理する自網内の運用(Intra-domain)と、他の ISP との経路交換における運用(Inter-domain)の大きく二つに分けられる。双方とも大きな問題であるが、当面は IPv6 のユーザ数が少ないことを考えると、Inter-domain の課題の方が先にあきらかになってくる。そのため、Inter-domain の問題に絞って、検討を行った。

## 4.4.検討項目の洗い出し

IPv6 になったとしても、基本的な経路制御の方式は変らない。OSPFv2 が OSPFv3 に、BGP-4 が BGP-4+になるだけで、その仕組みは IPv4 の延長上にある。このことはつまり、IPv4 での課題が IPv6 のネットワークでも問題になりうるということである。

IPv6 になるからこそ、問題が鮮明になるものもある。拡張されたアドレス空間、IPv4 以上の階層的な割当は、IPv4 より経路集約を容易にするが、そのことは逆に経路集約の例外を認めにくい状況も作る。

本 WG ではこのような観点から影響を受けるものとして、以下の項目を選定し、検討を行った。

- トラフィックコントロール
- マルチホーム

### 4.5. トラフィックエンジニアリング

ある程度の規模、特に AS を持つような ISP は、複数の ISP と接続をもち、通信を分散している。冗長性が一番の目的であるが、もうひとつの重要な項目として、その通信量を各接続回線に分散して、通信コストを低減する目的がある。これをトラッフィックエンジニアリングという。

トラフィックエンジニアリングの手法の一つとして、経路情報の制御が考えられる。ISP は回線毎に流す経路情報を変えることで、戻ってくるトラフィイクの量を制御する。そのためには、経路情報を分割する必要がある。IPv4 ではそのアドレス空間の消費を抑えるため、ISP に対して小出しの割振りを行っている。そのため、割振りブロックを複数運用することになり、回線毎への経路広告の分散を行うことができた。

IPv6 ではアドレスの集約化が図られ、ほとんどの ISP にとってせいぜい２，３個のアドレスブロックで利用するアドレスのすべてをまかなえる。しかし、アドレスの集約化はその流すポイントへのトラフィックの集中を招く。そこで、このような環境において、どのような対策を考えられるかの検討を行った。

#### 4.5.1. トラフィック分散技術

トラフィックエンジニアリングの手法として一般的なのが、経路の分散広告である。割り振られたブロックの用途、数などを考慮し、広告先を変えることで、戻りの通信量を制御できる。ただし、ブロック数が少なければ、当然その制御の効果も低くなる。

一本の回線への依存を低くするには、できるだけ接続する回線もしくは BGP の Peering 数を増やすという方法もある。この手法の応用として、異なる地域で同一の ISP と複数のリンクを持つことで、通信量を分散するホットポテトといわれる手法もある。

しかし、回線コストを考えるとある程度接続ポイントを限定せざるを得ない。地域への BGP の運用を分散するのが難しいという側面もある。結局は IX（相互接続点）のような接続回線に通信量が集中することになる。日本国内のような限定的な地域では有効である手法だが、国際ゲートウェイのようにある程度接続先を限定せざるを得ない場合は、分散は難しくなる。

BGP の属性(attribute)を利用することもできる。attribute の値を変えることで、ISP はその経路の到達性をある程度制御することができる。ISP の一部はこの値を公開し、通信量の制御に実際に利用している。ただし、他 ISP との接続が多くなると、その制御は難しくなる。また、制御のポリシーが他の ISP の運用に依存することになるので、安定した運用になりにくい。

#### 4.5.2.IPv6 での運用

上記の手法は IPv6 でも有効であるが、その効果は IPv4 よりも低くなることが懸念される。前述のとおり、IPv6 ではより経路の集約が進むため、外部に流す経路数もかなり大きな規模の ISP であってもせいぜい２か３程度である。このような環境下では一つの経路に依存する通信が多くなり、広告を変更することによる制御が難しい。

割り振りブロックを分割して経路広告をすることもできる。IPv6 はアドレスフォーマットが長く、経路を分割することも容易ではある。しかし、これはインターネット上の経路集約という思想に反する。IPv6 では割り振られる Prefix Length が固定化されており、フィルタ設定を簡単に行えるため、到達性を保証できない可能性も高い。

#### 4.5.3.結論

トラフィックエンジニアリングに対するほかの有効な手段がない以上、経路の分散広告は行われることになる。インターネット上での経路爆発を防ぐためには、何らかの基準を設けてそれを遵守するような仕組みが必要なのかもしれない。また、MPLS の利用など、この問題を解決するための代替となる手段の検討も重要であろう。

### 4.6.マルチホーム

マルチホームとは利用者が ISP に二つ以上の回線を持ち、インターネットシステムの冗長性を図る手段である。一番簡単な方法は ISP から割振りをうけず、独立したアドレス(Provider Independent : PI) を取得し、接続した ISP それぞれから経路情報をインターネット上に流すことである。しかし、この手段はインターネット上の経路情報数の増加を招き、インターネット全体の運用を考えるとあまり望ましい手段とはいえない。また、昨今 PI の取得も難しくなっている。

このほかの手段として、NAT を用いて異なる ISP から割り当てられたアドレスを使い分けるという手法もある。ただし、利用できるアプリケーションが制限され、システムが複雑になるというような弊害も発生する。マルチホームの運用にはなかなか有効な手段が存在せず、利用者や ISP にとって悩ましい問題となっている。

#### 4.6.1.IPv6 での課題

IPv6 では上記のような PI のようなアドレスが規定されていない。そのため、IPv6 では単純なネットワークによるマルチホームが行いにくい状況にある。NAT の利用も IPv6 の end to end 通信の実現という特長を生かすという面から見ると、適用が難しい。

上記の他にもマルチホームを実現する方法はいくつかある。ひとつは RFC3178(IPv6 Multihoming Support at Site Exit Routers)で提案されているマルチホームの手法である。RFC3178 ではマルチホ

ームをする ISP 同士が互いの回線上に、物理もしくは論理的にリンクを確保することにより冗長性の確保を行う。

しかし、本構成はマルチホームの構成に参加する ISP 間での協力が必要になる。また、責任分界が不明確になるという問題点もあり、汎用的な運用は難しい面がある。

この他、パンチングホールという手法もある。これは割り振られて経路のうち一部を切り出し、経路を個別に流す方法である。しかし、パンチングホールは前述のトラフィックエンジニアリングの項目で記されているように、経路爆発の危険性を高める。

#### 4.6.2.結論

現在考えられる手法はどの方法も決め手に欠く。今後新しい手法を確立する必要があるだろう。しかし、PI によるマルチホームが技術的には一番シンプルに実現でき、有効なのは事実である。ただし、経路爆発の回避もインターネットの重要な課題である。

ルートサーバなど社会的に重要なシステムなどは、万人にとってマルチホームが必須になる。しかし、その重要性は人によって異なる。たとえば社会的には重要でなくても、企業のビジネスにとって必須である場合もある。有効なマルチホーム手法がない現在、マルチホームを可能とするシステムに対するなんらかの利用基準が必要となるかもしれない。

### 4.7.今後

今回、ISP 間の問題についての議論を中心に行ったが、ISP 内の経路制御重要な課題であり、今後検討が必要になるだろう。また、検討した内容についても解決策を示すところまでにはいたっていない。今後は IPv6 の特長を生かしてなにか有効な手法がないかの模索を行っていきたい。

# 5.UNI 検討 WG

## 5.1.目的

本 WG では、主に小サイト向(家庭、SOHO など)アクセスサービスにおいて、大規模運用に実現するための必要な技術項目を運用面から整理し、有効な仕様を検討する。

## 5.2.背景

IPv6 では基本的通信レベルでは仕様・方式が整ってきているが、ADSL やダイヤルアップなど小サイト収容のアクセスサービスを大規模に展開には、単に通信を中継するだけでなく様々な制御（自動設定、認証、課金など）が必要となる。

IPv4 のアクセスサービスでは、これらの運用要件を実現するために、PPP によるアドレス割当、認証連携機能(RADIUS)等、技術方式が確立されている。IPv6 では本件のような運用機能については、機能的に不明な部分が多い。

このような背景から、端末開発、ISP 運用の面から、利用モデルや必要な機能を検討・整理し、機器ベンダーや、標準化作業への提言を行った。

## 5.3.検討の対象

議論する前提として、以下の項目をフォーカスした。

- 利用者の収容にかかわる、方式(認証、制御など)、機器(NAS, CPE など)のモデルと課題
- 現在必要な機能を検討
- ユーザサイトからの over IPv4 トンネルは除く
- 移動通信は除く

## 5.4.IPv6 によるネットワーク利用環境の変化

IPv6 のユーザ収容を検討するにあたり、ユーザのネットワーク環境がどのように変化するか、前提を明確にする必要がある。本 WG での検討課題を洗い出すために、ネットワーク環境の想定を行った。

### 5.4.1.想定する利用者

家庭や SOHO における利用者モデルを、以下の特徴があると定義した。

- 通信に関するスキルレベルが低い
- 移動が少ない（引越し程度は許す）
- ISP に直接収容される利用者(Site)の数が多い
- 1 サイトでの利用者数は多くない
- ISP への参加、離脱の機会が多い

### 5.4.2.IPv6 導入時のネットワーク環境

上記のようなユーザが利用する IPv6 のネットワーク環境を想定した。

(1)デュアルスタック環境

IPv6 の普及の初期から中期には IPv4 の端末がまだ多く使われている。Windows XP でも現状 IPv6 対応になっているアプリケーションは少ない。IPv6 の発展期には、ネットワークは IPv6/IPv4 の双方をサポートしたデュアルスタック環境が必要になる。

(2)利用アドレスの増加

IPv4 のインターネットでもネットワークに接続された端末は多くなってきている。今後情報家電の利用などますますこの傾向は高くなる。

(3)固定 Global Address の需要増加

インターネットの常時接続が普及し、アドレスの利用が潤沢にできるようになると、IPv4 の NAT で利用が制限されている P2P の通信が増えるようになる。また、情報家電の制御など家庭へのインターネット上からのアクセスも一般的になる。

インターネット上から家庭内のネットワーク端末を特定するためには Global Address が固定的に割り振られる必要がある。IPv6 のネットワークではその特長から、固定アドレス利用はより多くなる。

(4)割当アドレスは/64 or /48

IPv6 のネットワークの最小セグメントは/64 である。セグメント分けの必要がなければ、通常は/64 で十分である。

セグメントが複数必要な場合、その割り当てをうけることも可能である。インターネットの基準では/48 をサイト毎に割り当てるため、そのサイズが標準となる。

(5)自動設定が必須(利用アドレス、DNS 等)

IPv6 のネットワークでは情報家電など、自動設定が必要な簡易端末が増える。また、ネットワークの利用者層が広がり、スキルレスな利用者が増えることになり、その点からも自動設定の必要性が高くなる。

### 5.4.3.端末特定機能が必要

増加する端末の管理、P2P 通信への対応のため、DNS のような端末を特定するシステムが必要となる。セキュリティの面からも端末の特定は重要である。その際、ネット端末の利用するアドレス等を管理システムに登録する仕組みもあわせて必要になる。

#### 5.4.4.IPv6 実現への課題の整理

上記で整理した、利用者、環境に対応するために、ISP が解決しなければならない課題として、以下を検討することとした。

(1)ISP からユーザ接続サイトへのアドレス割当

IPv6 では LAN 内での自動設定については規格が存在するが、まだサイト間でのアドレス割当の手法が確立していない。そのため ISP がユーザサイトにアドレス割当の自動設定を行おうとしたとき有効な手法がない。アドレスはユーザサイトに対して固定的に割当てる必要があるので、サイトに対する認証との連携も必要になる。

(2)リゾルブ用 DNS の自動設定

アドレスと同様に DNS に関しても自動設定の仕様が規定されていない。IPv4 のインターネットではリゾルブ用 DNS は ISP 側が用意するのが一般的であるが、端末に設定する DNS は CPE が代行するケースもある。実際に DNS のリゾルブが行う契機は、端末からのリクエストであるので、端末仕様まで含めて検討する。

### 5.5.ユーザサイトに対するアドレス自動割当の検討

#### 5.5.1.接続タイプの類型

アドレス割り当てに関する対象を明確にするために、接続回線の形態、ISP から見た CPE タイプの類型の整理を行った。

(1)接続形態

- P-P 接続
  - ISP から見て接続サイトが 1 リンクに 1 箇所
  - Dialup, ADSL など
- マルチアクセス接続
  - ISP から見て接続サイトが 1 リンクに複数
  - CATV, Hot-Spot など

(2)CPE タイプ

- ホスト接続タイプ
  - 通信するホストが ISP 側回線に直接接続するタイプ
  - ホストは基本的に 1 台
- ブリッジタイプ
  - ISP 側回線と通信するホストの間に装置が存在するが、セグメントは同じタイプ
  - ホストは 1 台以上ありうる
- ルータタイプ

- ISP 側回線と通信するホストの間に装置が存在し、セグメントも異なる
- ホストは 1 台以上ありうる

マルチアクセス接続の場合、1 リンクを複数のサイトでシェアするため、アドレス割当対象サイトをリンク以外の認証で特定する必要がある。本検討を進めていくにあたり、構造がシンプルな P-P 接続での方式検討を行い、マルチアクセス接続は今後の検討とすることにした。

### 5.5.2.アドレス割当の手法

現在選択可能なアドレス割当方式を洗い出し、その評価を行った。

(1)PD(Prefix Delegation)

サイト間での Prefix 割当を行うために、新規に検討されている規格。Prefix を割当てるために特化しているため、割当機能は満たしている。また ICMP をベースとするため、PPP など特定のリンク方式に依存しないことも利点となる。

しかし、基本はルータからのリクエストを想定しているので、ブリッジタイプ、ホスト接続などへの適用には向かない。この他、割当後の確認や、認証との連携など仕様的に検討が必要な部分もある。IETF での仕様が Draft 段階で、検討が停滞している点も問題になる・

(2)RA(Router Advertisement)

セグメント内の Prefix 割当のために規定され、すでに実装も多く存在する。

だが、Prefix が/64 以外の場合も課題となる。また、あくまでも同一リンク上での割当のみが対象であり、ルータタイプの接続には適用できない。これには CPE を MSR として機能させるというアイデアもある。

(3)DHCPv6

IPv4 での DHCP による割当を IPv6 対応にしたもの。アドレス割当の方式としては機能できる。ただし、DNS アドレスの伝達や、Keepalive など実装上重い。また、基本的に同一リンク内での割当に適用となる。IETF では比較的長く検討されているが、なかなか RFC まで収束していない。

(4)IPv6CP

IPv4 での PPP 上の IPCP による割当方式を IPv6 対応にするもの。IPv4 の PPP 接続ではほとんどこの方式でアドレス割当を行っているためわかりやすい。一方 PPP でしか利用できないという欠点がある。Layer3 での設定を Layer2 で解決するため、Layer Violation になるとの批判がある。IETF では Draft も存在せず、仕様について否定的である。

#### 5.5.3.まとめ

(1)CPE がホスト接続タイプ

アドレス割当の対象が ISP から見て Layer3 敵に直接接続されているため、RA, DHCPv6 をそのまま用いることができる。大規模な運用を考えると、実装上軽い RA が推奨される。ただし、より高度でステートフルな管理が必要な場合、DHCPv6 の利用も考えられる。

(2)CPE がブリッジタイプ

ホスト接続と同様な整理となる。また、Layer3 的にはサイトが分かれるが、MSR のような手法もこの接続と同様な結果が得られる。

(3)CPE がルータタイプ

PD が規格としては一番妥当であるが、いまだ Draft 状態である。まだ、有効な仕様はさだまっていないといえる。今後 PD を軸に規格の評価を進め、規格化への要望をまとめていく。

（注）PD に対して要望される機能は、IETF での議論を経て、DHCP のオプション機能としても検討されている。(draft-ietf-troan-dhcpv6-opt-prefix-delegation-01.txt)

現在はこの DHCP オプションが仕様として有力となっている。

### 5.6.ユーザサイトに対するリゾルブ用 DNS の自動設定の検討

#### 5.6.1.リゾルブ用 DNS 設定の手法

DNS 自動の方式として以下の案を検討した。

(1)DHCPv6

IPv4 と同様な仕様である。仕様としては充分だが、アドレス割当などを含み、端末がサポートするには実装上重い面がある。

(2)Site-local Anycast

DNS で利用するアドレスをあらかじめ固定して、端末側にあらかじめ組み込んでおく方式。実装が軽く、利用しやすい。サイト内での利用しか規定されていないのが問題となる。

(3)IPv6CP

IPv4 での PPP 上の IPCP による割当方式を IPv6 対応にするもの。PPP でしか利用できない欠点がある。Layer3 での設定を Layer2 で解決するため、Layer Violation になるとの批判があり、IETF では議論されていない。

(4)SLP(Service Location Protocol)

メールサーバやその他のサーバも含めて、複数のサービスサーバの場所を伝達するために検討されているプロトコル。DNS 以外もフォーカスしているので、実装上重い。また、SLP のサーバ伝達を最初に行わなければならず、結局 DNS サーバアドレスの伝達と同様の問題が発生する。

### 5.6.2.まとめ

実装上軽いという点から、Site Local Anycast が推奨される。適用範囲が Site 内に限定される問題に対しては、Site 境界を接続回線、ISP 内など柔軟に拡張することで対応できる。また、本検討ではあくまでもエンド端末への設定であったが、ホームサーバなどへの伝達には DHCP, SLP も適用可能である。

## 5.7.今後の課題

アドレス割当に関しては、確定的な仕様がないこともあり、今後要望を明確にしていく必要がある。また、仕様の決定については、IETF での議論が不可欠であり、IPv6 WG への提案をおこなっていきたい。

UNI 関連の検討はいまだ課題が多い。今後、

- サイト内のルーティング
- 利用アドレスの登録システム
- 家庭内ネットワークでのアドレス割当

などについて検討していきたい。

# 6.企業ネットワーク WG

## 6.1.目的

企業のイントラネットは、ネットワーク、端末管理、セキュリティ管理などの様々な要素で構成されている。

本 WG では企業ネットワークにおける IPv6 導入について議論し、運用モデルを作成する。また、企業が IPv6 の採用に踏み切るために必要な運用のケーススタディを行い、メリットのリストアップも行う。

## 6.2.背景

IPv6 においては 2 章から 4 章において説明がなされているように、サービスの提供や各技術の運用における課題など、個々の整理は進み始めている。しかし、実際に利用するユーザに対してどの様な技術が求められ、それがどの程度実用に耐える状態であるかについての検討がなされていなかった。また、実際のユーザをターゲットに IPv6 化を進めるにあたって、どの技術が足りないか、どういった運用をしていくべきかのポリシーの検討も進んでいなかった。

2 章から 4 章の議論が進むにつれ、企業ネットワークの SIer の立場から、今後の SI において IPv6 をどの様にユーザに提供していくかに関して議論をしていく必要があるとの認識が出され、同様な課題を持つ、SIer、ISP、NSP、ルータベンダなどの様々な分野のスペシャリストを集めて議論を開始した。

## 6.3.議論の流れ

### 6.3.1.検討の基本ラインの定義

検討当初に挙げた検討項目下記の通りである。

- ネットワーク構成（アドレス計画/ルーティング）
- DNS（リゾルバ/レジストレーション）
- セキュリティ
- トランジション
- アプリケーション
- 運用管理・監視
- ISP 接続

また、検討のターゲットとして下記を挙げた。主に、議論の方向性を明確にし、本検討でまとめる運用モデルを提供するユーザ像、整理すべき技術ポイントを絞り込む目的で定義した。

(1)議論の対象

- ネットワーク規模別の IPv6 化における違い
- IPv6 化するときの課題
- ユーザーネットワークの ISP への接続

(2)移行モデルを検討するネットワーク規模の定義

- 大企業
  - 日本全国にサイトを持つような企業
  - uplink を複数持つような企業
- 中企業
  - ある地域に複数のサイトを持つ企業
- SOHO
  - 一つのサイトから成立している個人企業
  - ホームオフィス等

これらを元に、主に考えられる課題として、下記を整理していくこととなった。

- IPv6 からの移行形態
- IPv4 との共存方法
- IPv4 に比較した IPv6 網の構築技術の変化

### 6.3.2.議論の進展による定義の変化

IPv6 に移行する企業網のモデルを進める中で、ネットワーク規模別の定義は、ネットワークに管理者が居るかどうかの方が、実際の構築において影響が大きい事が明らかとなってきたこと、SOHO でも個人に近いネットワークのモデルは、UNI の WG で検討が成されていることなどから、移行モデルを検討する規模の定義を下記の通り見直した。

移行モデルを検討するネットワークの定義

- 大規模網　＝　ネットワーク管理者が存在するもの
- 小規模網　＝　ネットワーク管理者が不在もしくはスキルが無いもの

## 6.4.検討のポイント

企業にとってネットワークは、ISP 等とは違い、本来は収益を伸ばすためのツールであり、戦略的にネットワークを構築するという概念があまりない。そのため新規の設備投資が行われにくい。

これを簡単にいうと、ISP とは違って新たに別のネットワークを構築して試す事が出来ず、「今あるネットワークを移行する必要がある。」ということである。また、企業内の設備およびアプリケーショ

ンは一般ユーザに比較して置き換え期間が長く、そのため IPv4 との併存利用の期間も長くなると考えられる。設備のリース期限に合わせて IPv6 に対応した機器を徐々に採用していく場合もあり、その面からも共存期間を長めに取った移行戦略が必要である。

これらのことから、トランスレータやトンネリングなどの移行技術は企業にとって重要であり、それは長期間にわたって安定して運用される必要がある。

しかし、セキュリティや運用監視等については、企業網内で IPv6 対応の機器が増えるに従い、徐々に整備していくのでは不十分である。安定性や機能面において、IPv4 で構築したものと同レベル以上のものが当初から求められる。長期的にはスケーラビリティや運用性で優れていなければならない。セキュリティポリシーについても、IPv4 において企業が求めるレベルを達成する必要がある。

このような基本的認識を元に下記の結果をまとめた。議論結果の導き方として、まず始めに検討対象とするネットワークモデルを定義し、そこで求められる技術的なポイント、具体的には、ルータ、サーバ、クライアント等の各ノードの IPv6 対応、ネットワーク構成に対するアドレッシングおよび経路制御などを議論し、各ネットワークモデルにおける現状整理、課題整理を行った。さらに、ISP への接続、セキュリティ、個々のアプリケーション、管理・監視系、といったポイントに対して個別に結果をまとめた。

- ネットワークモデル
- ISP 接続
- セキュリティ
- アプリケーション

## 6.5.ネットワークモデル

### 6.5.1.大規模網

(1)管理モデル

大企業のネットワークは、その成り立ち、つまり元々どの様なネットワークの導入経緯があるかで、二つの管理モデルに大別できる。一つはシステム管理部門が全社に画一的に一定のポリシーを持って提供するタイプと、もう一つは部門の単位で必要に応じてネットワークを構築するタイプである。

前者の場合は、画一的なポリシーを確立する目的のもと、予算に応じて導入が決定され、導入する際には全部門に同時に提供される。そのため、一般には IPv6 の導入が決定されたら、その導入が一気に進む可能性が高い。

後者の場合は、各部門が自立的に IPv6 の接続を求めるため、部門ごとに構築される時期がずれる。また、導入する際の技術レベルもまちまちとなる。

(2)アドレス計画

大企業においても、基本的には/48 の空間が初期に割り当てられるが、65,000 のサイトを構成することが出来るために通常はこれで不足は無いと思われる。例えば/48 の割り当て例として下記のモデルを想定することが出来る。

**/48 の割り当て例**

- 前提
  - 日本全国規模の企業
  - 全国に 50 組織

- 各割当数
  - /49　　pool（先々のために予約
  - /56　　各組織 128 個(7bit)の/56 を各々の組織で分割
    バックボーンに一つの/56
  - /64　　256 個(8bit)の組織配下の部門

これは割り当ての一つの例であるが、各サイト内部の端末数の増加によって IPv4 のようにサブネットマスクの変更などが起こる可能性が IPv6 においてはほぼ無いと考えると、充分に大きな企業であっても、/48 の範囲でアドレッシングが可能であることがわかる。

(3)経路制御

大規模網では OSPF のような link-state 型の IGP を採用して、末端のサイトを複数の網に帰属させることで冗長化を図ることがあるが、IPv4 における OSPFv2 と IPv6 における OSPFv3 がほぼ同じプロトコルであること、既に商用の製品も出ていることから無理なく構築できる。

(4)各ノードのスタック

後に述べるように大企業では IPv6 対応が早期には難しい、独自のインプリをしたアプリケーションを使っているケースも多く見られる。そのため汎用のアプリケーションをインストールしたパソコンとの相互接続が求められる。

ルータに関しては両方のトラフィックの混在を想定して、IPv6/IPv4 デュアルスタックであることが必須となる。一般の端末においては、トランスレータを導入しない場合には、長期間 IPv6/IPv4 のデュアルスタックとなる事が想定される。これは企業外部のインターネットから IPv4 のサーバやホストが事実上無くなったとしても、企業内に IPv4 を用いたアプリケーションが残る限り続く事となる。もちろん、企業内と企業外のどちらが先に IPv4 が無くなるかはケースバイケースであり、現時点では予測できないが、企業活動としては最後まで残ることを想定して構築していく必要がある。

#### 6.5.2.小規模網

(1)管理モデル

小企業ではその企業がネットワークに求めている質によって大きな差があるが、本検討において想定した、管理者が不在もしくはあまりスキルを持っていない、かつ特殊なアプリケーション等を使っていないモデルの場合には、IPv6 導入のために、基本的にはその組織を丸ごと、既存設備を全てアップグレードするという観点が強くなると考えられる。パソコン OS のような汎用品の IPv6 対応が、ユーザの要求とは別に進むために、IPv6 がサポートされているソフトウェア／ハードウェア製品が出そろった時期に移行するケースが出てくるだろう。

(2)アドレス計画

大企業と同様に/48 の空間が割り当てられるが、セグメントが一つの場合は/64 が一つで充分である。数個のセグメントの場合でも、割り当てられるアドレスの個数から言えば、特に設計に神経質になる必要は無い。

(3)経路制御

ISP との接続点は一カ所であるケースがほとんどと考えられるため、その接続点のルータをデフォルトルータとして設計すればよく、IGP を使うとしても OSPF までは必要とされない。

(4)スタック

独自のアプリケーションを採用していなければ、製品として提供されるもので自然と IPv6/IPv4 デュアルスタック化が進み、主な通信が IPv6 に軸足を移していくこととなる。

### 6.6.ISP 接続の移行

ISP に接続する回線にどの様な IPv6 インターネットへの接続性が用意されるかであるが、いくつかのステップが予想できる。

#### 6.6.1.フェーズ分け

本研究会では、IPv6 の導入状況のフェーズ分けを行っている。（第二章）ISP 接続の移行を議論するにあたって、このフェーズにしたがって、モデルを議論した。

(1)フェーズ 1

現在用いている回線の上にトンネル(IPv6 over IPv4)接続を用意する方法がある。これのメリットは、現在の接続性に関する安定性や運用性を損なうことなく IPv6 を導入することが可能である事である。デメリットとしては、IPv6 用にトンネル接続が可能な新たなルータを追加すること、性能面やセキュリティ面で十分な考慮が必要なことである。

(2)フェーズ 2

フェーズ 1 の発展型として複数の方向が考えられる。一つはゲートウェイとなっているルータのファームウェア(もしくはソフトウェア)をバージョンアップする等でIPv6をサポートする方法である。ただし、ISP 側の設備も当初は既存 IPv4 接続性の信頼性のために IPv6 Native を提供することが難しいため、企業のゲートウェイから ISP の上位の IPv6 対応ルータまでトンネルによる接続を行う。

もう一つは、同一回線上に IPv6 と IPv4 をデュアルで提供するが、両端とも HUB 等を置いて IPv4 と IPv6 のルータを並列に置く方法である。

前者のメリットは基本的に追加コストが無い事であるが、ファームウェアをバージョンアップする際に十分な安定性が確認できなければならない。後者の場合は既存の IPv4 の接続性に与える影響をほぼ押さえる事が出来るが、新たにルータや HUB を導入するコストが発生する。

(3)フェーズ 3

ゴールの時期となり、IPv4/IPv6 デュアルスタックのルータを導入して、両方のコネクティビティがネイティブになる。デメリットはやはり安定性を確認する必要があることだが、今後の製品の洗練により解決される問題である。IPv6 と IPv4 を同じレベルで利用することが可能であるため、長期的にはこの状態となる。

### 6.7.セキュリティ

IPv4 においては、企業におけるセキュリティはファイヤウォールのような単一のポリシーにより、全ての網内ノードを守るという手法が取られている。IPv6 の重要なメリットとして、End to End の接続性を確保する事による peer-to-peer のアプリケーションが実現できることがある。しかし、IPv4 企業網におけるセキュリティポリシーをそのまま採用すると、IPv6 の End to End 通信のメリットは享受できない。

本検討では、IPv6 を本格的に運用する時代に向けて、IPSec により端末が個別に暗号化などをすることで通信内容等のセキュリティを確保し、企業のゲートウェイルータにおいてフィルタリングを行うことで、例えば企業活動に必要な End to End 通信は実現し、それ以外はせき止めていくというモデルを提案している。

しかし、企業のセキュリティ管理ポリシーを大きく変える事や、組織外からの到達性があることには、非常に強い抵抗感を多くの企業ネットワーク管理者が持つことが容易に想像できる。また、各端末の通信が IPSec により暗号化されることで、ネットワーク管理者が通信の内容や到達性の管理をする事が出来なくなる。従って、今後の検討において企業のセキュリティポリシーに対する考え方をより深く議論すべきとの課題を残した。

IPv6 においてメリットとされる IPSec であるが、実際にはあまり実装は進んでいない、実装されていても複数の実装間での相互接続性が無い、などの問題が指摘された。また、センサーのような組み

込み系の小規模なネットワークデバイスでは実装が重く、実装されないという可能性もある。

## 6.8.アプリケーション

### 6.8.1.アプリケーションの分類

まず始めに、下記のような分類を行った。

- 一般的なソフトウェア
  - web(http), mail(smtp, pop3, IMAP4), ftp,
  - telnet ssh, bind, ストリーミング, IRC,
  - チャット, etc.
- 企業独自開発系
  - DB 系, EDI, ERP, CAD/CAM/CAE, スパコン
- 管理系
  - RADIUS, TACACS, SNMP, NTP, etc.

### 6.8.2.一般的なアプリケーション

企業において一般的に利用されるのは一般ユーザ同様メールや Web であるが、これに関しては特に問題はないと考えられる。既に IPv6 対応をしている OS も発売されているため、IPv6 対応の進展は市場のニーズと時間の問題である。

### 6.8.3.企業独自開発系アプリケーション

IPv6 移行時の課題となるのは、カスタマーリレーション用のソフトウェアを始めとする、EDI、CAD/CAM/CAE、スーパーコンピュータ等の企業が独自にベンダーに開発を依頼しているようなアプリケーションである。これに関しては、5 年、10 年というスパンで移行を検討しなければならない。アプリケーションの耐用年数についても考慮する必要がある。

### 6.8.4.管理系アプリケーション

管理系のアプリケーションは必ずしもトランスポートが IPv6 でなくても、管理対象のアドレスとして IPv6 も扱えるように拡張できれば問題ないものもある。必要性は既に以前から言われてひさしく、対応も進んできているため、IPv6 対応の機器やソフトウェアの充実とともに、実装されていくと考えられる。

## 6.9.今後の課題

本検討を進めていく中で、企業において IPv6 を採用していくにあたっては、いくつかの重要な課題があることがわかった。現時点では、主にアプリケーション、セキュリティに関して、課題があると認識している。それぞれの課題に対して以下のように進めていくべきであると結論付けた。

(1)セキュリティ

IPv6 においては、グローバルアドレスをサイト内部にも用いることから、セキュリティモデルの変化があることが明確となった。しかし、IPv6 のメリットを享受しながらこれまでに企業等が作り上げてきたセキュリティポリシーを満たしていくためには、実際のユーザを交え、さらに一歩踏み込んだ議論が必要であることもわかった。特にセキュリティに関しては、企業だけでなく他の面からも重要であることが認識されており、セキュリティの観点からの横通しの検討が必須である。今後、多方面からセキュリティのあり方の議論を進めていきたい。

(2)アプリケーション

企業においては個別に作り込まれたアプリケーションが存在する。これらのアプリケーションは一般に用いられるアプリケーションと違い、個別に開発もしくは改造を行っていく必要がある。そのためには、それぞれのアプリケーションの耐用年数等を考慮して、移行していく必要がある。これら特別なアプリケーションを体系別に整理し、IPv6 移行に向けてより詳しい対応方針をまとめていきたい。

(3)企業エンジニアのスキルアップ

今後、企業が安心して IPv6 を採用するためのモデルを完成させていくと同時に、機器やソフトウェアを開発する側のとの連携、SIer のスキルの向上などが必要である。

## 7.おわりに

これまで、当研究会ではここで紹介した検討結果に達するまでに数多くのミーティングを行ってきた。そして、これらの結果は、JANOG ミーティングや Internet Week などを通じ国内で広くその内容を紹介してきた。それぞれのミーティングへの参加者は、日本国内外を問わず活躍する第一線の技術者、そしてオペレータばかりである。このため、ミーティングは、多忙の合間を縫って行われたが、ひとたびミーティングが始まれば、その議論は終わることを知らないかのごとく毎回深夜まで行われた。しかし、結論が終わるまでは誰一人としてミーティングの終わりを許さないという実に過酷なミーティングであった。ここに、IPv6、いやインターネットをより良くしてゆくのだという彼らの意気込みが溢れている。ここで、これらの多くのミーティングに参加して頂いたすべての人々に深く感謝したい。

しかし、ここまで記述した検討内容は、インターネット全体を見渡したときに見える非常に表面的な部分だけに特化されている。実際には、研究会で検討した結果をさらに細分化し、その項目ごとに検討を進めることが重要である。たとえば、家庭のネットワークでの IPv6 の利用なども必要であるほか、IPv6 で期待されている、車や携帯電話などのコンピュータ以外の新しいネットワークデバイスでの利用方法や運用方法に関する検討は、今後のインターネットを考える上でも重要である。

当然のことではあるが、インターネットは世界全域にわたって利用できるまれにみる全世界的ネットワークである。それが故、日本国内だけの検討だけでは十分ではない。これら日本で検討されたさまざまな事柄は自身を持って世界に発信できるレベルに達していると自負しおり、積極的に世界に向けて発信してゆく所存である。

# 8.Appendix

## Appendix 1: IPv6 オペレーション研究会：ボードメンバー一覧

| | | |
|---|---|---|
| チェア | 猪俣 彰浩 | 富士通 |
| | 向井 将 | パワードコム |
| ボードメンバ | 荒野 高志 | インテック・ネットコア |
| | 中川 郁夫 | インテック・ネットコア |
| | 近藤 邦昭 | インターネットイニシアティブ |
| | 藤本 幸一郎 | NEC |

## Appendix 2: ホームページ

http://www.bugest.net/IPv6-ops/

## Appendix 3:WG 開催状況

(1)報告会

2001 年 11 月 14 日　　中間報告

(2)トランジション WG

9/21(Fri) 泊まりこみ合宿において検討会を実施

11/14 報告会にて発表

(3)アドレスポリシーWG

| | |
|---|---|
| 2001 年 6-7 月 | 国内でのコンセンサス形成期 |
| 2001 年 2 月 13 日 | WG 開催（富山） |
| 2001 年 5 月 11 日 | WG 開催（IIJ） |
| 2001 年 6 月 14 日 | WG 開催（富士通） |
| 2001 年 7 月 14 日 | WIDE 研究会にて発表・議論 |
| 2001 年 7 月 26 日 | JANOG BOF にて発表・議論 |

(4)ルーティング WG

2000 年 2 月に、有志が集まり、運用を含めた議論をした。インターネットにおける IPv6 のインパクトを中心に検討をおこない、問題点を大まかに洗い出した。その後、問題点を深くほりさげていき、ISP の運用で起こりうる問題を、AS 間、ISP 内に大別した。同年 7 月、大別した問題をもとに、合宿をし、議論をした。その議論の元に同年 7 月 JANOG8 BoF にて、JANOG コミュニティに対し意見を求めた。

(5)UNI 検討 WG

2001 年 10 月 15 日　　WG 開催

2001 年 11 月 2 日　　WG 開催

2001 年 11 月 26 日　　WG 開催

2002 年 2 月 4 日　　WG 開催

## Appendix 4:WG 検討参加メンバ(ボードメンバは除く)

トランジション WG：Chair 中川

| | |
|---|---|
| 萩野 | インターネットイニシアティブ |
| 藤崎 | NTT |
| 山崎 | NTT Communications |
| 中川 | パワードコム |
| 石田 | メディアエクスチェンジ |

アドレス WG：Chair 荒野

| | |
|---|---|
| 前村 | イクアント株式会社 |
| 倉橋 | インターネットイニシアティブ |
| 楠田 | インテック・ウェブ・アンド・ゲノム・インフォマティクス |
| 中原 | NEC |
| 石橋 | NEC |
| 山崎 | NTT Communications |
| 上水流 | NTT Communications |
| 棚橋 | NTT Communications |
| 白崎 | NTT Communications |
| 友近 | NTT Communications |
| 新延 | NTT 西日本 |
| 浅井 | NTT 西日本 |
| 荒木 | 日本テレコム |
| 遠藤 | 日本テレコム |
| 長島 | 日本テレコム |
| 江面 | PSI |
| 高嶋 | パワードコム |
| 田中 | パワードコム |
| 中川 | パワードコム |
| 渡部 | パワードコム |

島田　　松下電器産業

ルーティング WG：Chair 向井

江面　　IRI
橘　　あにあにどっとこむ
前村　　イクアント株式会社
倉橋　　インターネットイニシアティブ
楠田　　インテック・ウェブ・アンド・ゲノム・インフォマティクス
中原　　NEC
石橋　　NEC
藤崎　　NTT
友近　　NTT Communications
棚橋　　NTT Communications
白崎　　NTT Communications
新延　　NTT 西日本
浅井　　NTT 西日本
表雅　　札幌医科大学
宮司　　札幌医科大学
永見　　東芝
荒木　　日本テレコム
遠藤　　日本テレコム
長島　　日本テレコム
小林　　ネクステック
中川　　パワードコム
高嶋　　パワードコム
渡部　　パワードコム
島田　　松下電器産業

UNI 検討 WG：Chair 猪俣

荻野　　IRI
野口　　ACCESS
廣海　　イーアクセス
矢萩　　イーアクセス
萩野　　インターネットイニシアティブ
山本　　インターネットイニシアティブ
楠田　　インテック・ウェブ・アンド・ゲノム・インフォマティクス

| | |
|---|---|
| 宮川 | NTT- Lab.(USA) |
| 白崎 | NTT Communications |
| 竹野内 | NTT Communications |
| 山崎 | NTT Communications |
| 川上 | NTT 東日本 |
| 新延 | NTT 西日本 |
| 森山 | NTT 西日本 |
| 伊藤 | キャノン |
| 石原 | KDDI |
| 進藤 | COSINE Communications |
| 尾上 | SONY |
| 永見 | 東芝 |
| 長島 | 日本テレコム |
| 佐久間 | PFU |
| 鈴木 | 日立 |
| 及川 | Microsoft |
| 酒井 | 松下電器産業 |
| 島田 | 松下電器産業 |
| 木村 | YAMAHA |

企業ネット WG：Chair 藤本

| | |
|---|---|
| 石橋 | NEC |
| 小野 | 松下電器産業 |
| 熊谷 | 電通国際情報サービス |
| 島田 | 松下電器産業 |
| 白橋 | ネットワンシステムズ |
| 橘 | あにあにどっとこむ |
| 中井 | NTT コミュニケーションズ |
| 廣海 | イー・アクセス |
| 藤田 | イー・アクセス |
| 細江 | 松下電器産業 |
| 村上 | 松下電器産業 |
| 山崎 | NTT コミュニケーションズ |