



# IPv6 入門

## — Internet Protocol Version 6 —

(社)日本ネットワークインフォメーションセンター

(Japan Network Information Center)

江面 祥行 (EZURA, Yoshiyuki)

奥谷 泉 (OKUTANI, Izumi)

ezura@nic.ad.jp, izumi@nic.ad.jp



2

## 構成

- IPv6への道のり
  - インターネットへの道のり
  - インターネットプロトコル(IPv4)
  - IPv4 が抱える問題
- IPv6の基礎
  - 次なるプロトコルへ(IPv6)
  - IPv4からIPv6への移行
  - IPv6への対応
- IPv6アドレスポリシー
  - IPv6アドレスの分配
  - IPv6アドレスポリシーのこれから

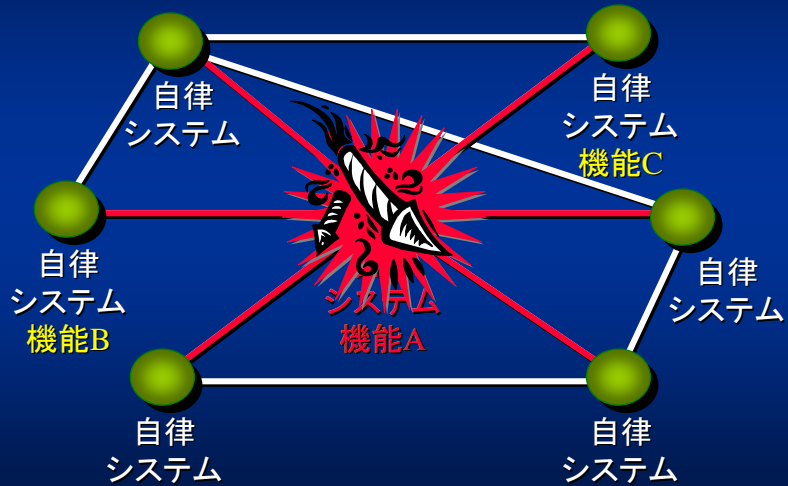
## IPv6への道

インターネットへの道のり

## ARPA Project

- アメリカ国防総省の「核戦争にも耐えられるネットワークを！」の一声で新しいネットワーク技術の開発がスタート
  - 障害に強い分散型のネットワーク
  - 単純だが確実な転送のできるプロトコル
- 1970年代に TCP/IPが開発された
- 現在まで30年に及ぶインターネットの歴史の根源

## 核戦争にも耐える？



## internet から The Internet へ

- アメリカの研究所、大学などの相互接続からスタート
- 企業、一般団体などへ拡大
- 国境を超えて全世界的なネットワークへ
- 目的も軍事→学術研究→商用などの一般利用へ

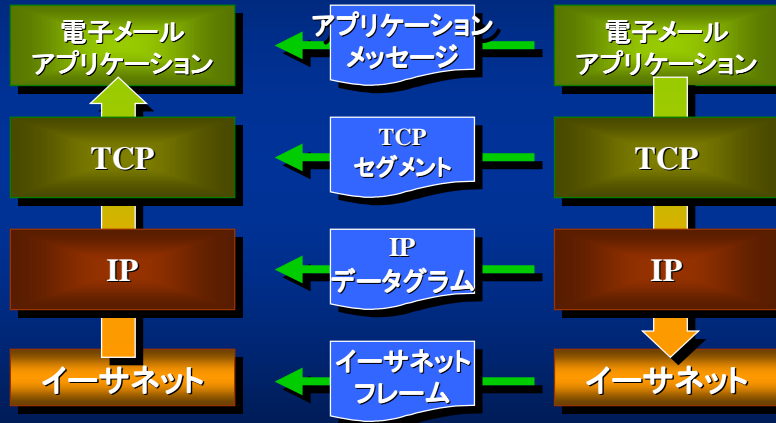
## IPv6への道

インターネットプロトコル(IPv4)

## ネットワークでのプロトコル

- 情報をネットワークを通した相手とやりとりするための手順
  - 電子メールを相手のメールボックスに届けるのってどういうやりとりがあるの？
  - WWWサーバにアクセスしてホームページを見てるとき、ブラウザはサーバと何をやりとりしているの？
  - ネットワークケーブルを通して通信しているみたいだけど、どうなってるの？

## 電子メール送信の裏側



## インターネットのプロトコル

アプリケーション層	電子メール SMTP	WWW HTTP	telnet	ftp
トランスポート層	TCP		UDP	
インターネット層	<b>IP = Internet Protocol</b>			
ネットワーク インタフェース層	イーサネット	ATM	FDDI	

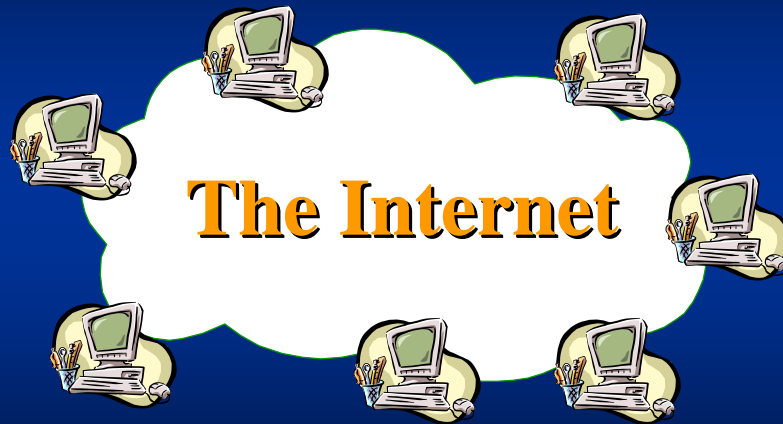
## インターネットプロトコル(IP)

- アプリケーションからの情報を、ネットワークフレームサイズに収まるように分割する
- 情報の送り先などの**ヘッダ**を付加する
- 分割した情報とヘッダ情報を**IPデータグラム**として構成する
- IPデータグラムを始点ホストから終点ホストまで転送する。

## IPデータグラムとヘッダ



## 送り先をどう特定する？



## IPアドレス

- 電話は電話番号で相手を特定する
- 手紙は住所と名前で相手を特定する
- IPネットワークにも相手を特定するための何かが必要！

**IPネットワーク上での住所 → IPアドレス**

## IPv4アドレス

- インターネット上でホストを一意に特定するための番号
- 32ビットの0と1による数値

11001010	00001100	00011110	00100110
----------	----------	----------	----------

- IPで通信をするすべてのホストにIPアドレスは存在する

## IPv4アドレスの表記

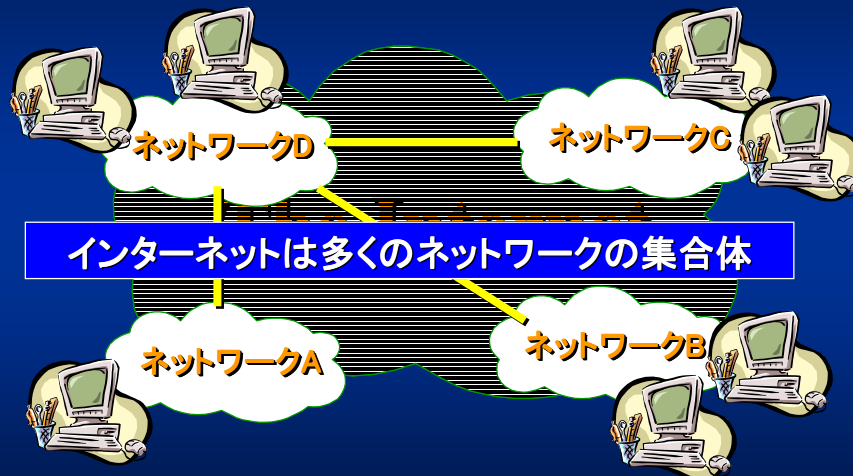
- 8ビットずつを10進数であらわし、ピリオドで区切った4つの数字
- 8ビットなので、それぞれは0から255

11001010	00001100	00011110	00100110
----------	----------	----------	----------

**202 . 12 . 30 . 38**



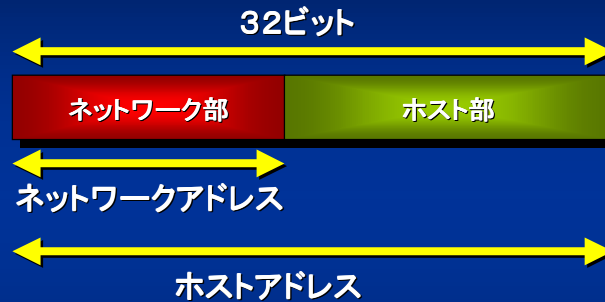
## 相手までの道筋は？



## ネットワークの識別

- IPアドレスによって通信相手を特定するだけでは、IP データグラムを届けることはできない
- インターネットはネットワークの集合なので、相手がどのネットワークにいるのかが分からなければいけない
- IPアドレスで、相手のネットワークの識別と、相手ホストの特定ができるとうれしい！

## IPアドレスの意味付け



- IPアドレスを「ネットワークを表す部分」と「ホストを表す部分」に分割

## ネットワーク部の大きさは？



- ネットワーク部の大きさによって使えるネットワークアドレスの数とホスト数が決まる
  - 8ビットならネットワーク256、ホスト1600万
  - 16ビットならネットワーク、ホスト共に6万5千
- さまざまなネットワークに対応するためには固定にしないほうがいい

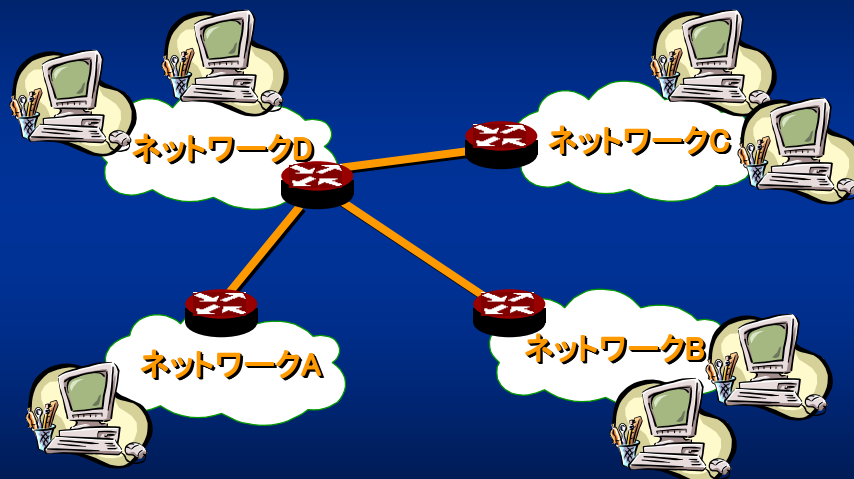
## ネットワークアドレス表記

- IPアドレスの先頭のクラス識別ビットを見ればアドレスクラスがわかり、どこまでがネットワーク部かを判別できる
- ネットワークアドレスはホスト部を0で埋めた形で表記する
  - 10.0.0.0 (クラスA) 00001010.00000000.00000000.00000000
  - 172.16.0.0 (クラスB) 10101100.00010000.00000000.00000000
  - 192.168.1.0 (クラスC) 11000000.10101000.00000001.00000000

## IP データグラムの転送



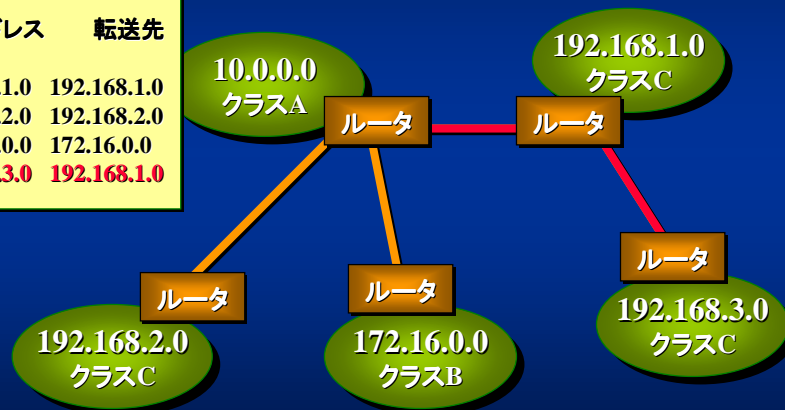
# IPデータグラムの転送経路は？



# IPデータグラムの転送経路は？

**経路表**

終点アドレス	転送先
192.168.1.0	192.168.1.0
192.168.2.0	192.168.2.0
172.16.0.0	172.16.0.0
<b>192.168.3.0</b>	<b>192.168.1.0</b>



## 経路制御

- IPデータグラムをどのルータに投げればよいのか？ → 経路制御
- 各ルータは最終あて先ネットワークと、それに対応する中継ルータの一覧情報を保持する → 経路表
- つまり、ネットワークが増えれば経路表のエントリ数も増える

## IPv6への道

IPv4 が抱える問題

## どんな問題があるの？

- 経路数の増加
  - ネットワークの数が増えると経路情報が増える
  - 経路情報が増えるとルータの負荷が増大する
- アドレスが需要に対応できないかも...
  - 電話番号の桁数より少ない
  - 携帯電話からのインターネット接続、常時接続サービスの普及

## 32ビットってどのくらいの大きさ？

- 32ビット =  $2^{32}$  乗  $\approx$  約40億
- 世界人口を60億人とすると...
  - みんなにあげるにはちょっと足りない...
- 携帯電話や家庭用ゲーム機、インターネット常時接続サービスなどを考えると、今後さらにIPアドレス要求は大きくなる

## 解決へ向けて

- CIDRの導入
- プライベートアドレスの導入

## CIDR導入前の仕組み

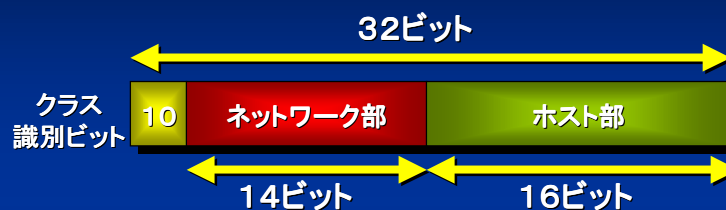
- クラスフルなアドレス構造
- 固定されたネットワークアドレス

## いくつかのパターン: クラスA



- **クラス A** アドレス (大規模ネットワーク用)
  - ネットワーク内に**1600万**のホストを持つことができる
  - インターネット全体で**128**のネットワークに割り当てることができる

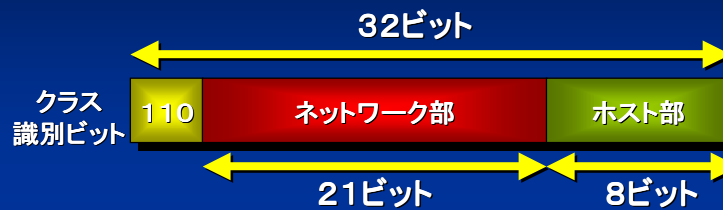
## いくつかのパターン: クラスB



- **クラス B** アドレス (中規模ネットワーク用)
  - ネットワーク内に**65536**のホストを持つことができる
  - インターネット全体で**16384**のネットワークに割り当てることができる



## いくつかのパターン: クラスC



- **クラスC** アドレス (小規模ネットワーク用)
  - ネットワーク内に**256**のホストを持つことができる
  - インターネット全体で**200万**のネットワークに割り当てることができる

## 経路情報の数を抑制するには？

**1つのネットワークに対して  
1つのネットワークアドレスを割り当てる**

## 1 ネットワーク1クラス

- 1000個のホストを持つネットワーク
  - クラスC(ホスト数256)だと足りない
  - クラスB(ホスト数6万5千)だと多すぎる？
- クラスCを4つあげれば足りるけど、経路情報も4つになってしまう
- じゃあクラスBをあげよう！

## アドレスの節約を考慮すると...

- クラスBを奮発していたけど、クラスBネットワークは1万6千しか作れない
- 仕方ないのでクラスCを複数個あげる

**当然、経路情報が急増！！**

## クラスを捨てろ！

- クラスは8ビット単位でしかネットワークの大きさを定義できないので、アドレス利用の無駄が大きい
- アドレスクラスは経路情報爆発の原因の一つ
- ルータの性能的限界があるので経路情報はなんとか抑えたい

## CIDR

- CIDR...Classless Inter-Domain Routing
- ネットワークアドレスの区切りを8ビットごとではなく、どこでも区切れるようにする
- IPアドレスの先頭ビットでクラスを識別する手法は廃止

クラスフル から クラスレス へ

## CIDR表記

202 . 12 . 30 . 38

11001010	0001100	00011110	00100110
----------	---------	----------	----------



ネットワークアドレス

先頭ビットが110なので、クラスフルな考えのもとでは「クラスC」

ネットワークアドレスは24ビット  
ホスト数 256

## CIDR表記

202 . 12 . 30 . 38 / 22

11001010	0001100	000111	10	00100110
----------	---------	--------	----	----------



ネットワークアドレス

**202. 12. 30. 38 / 22**  
というCIDR表記のもとでは  
ネットワークアドレスは22ビット  
ホスト数 1024

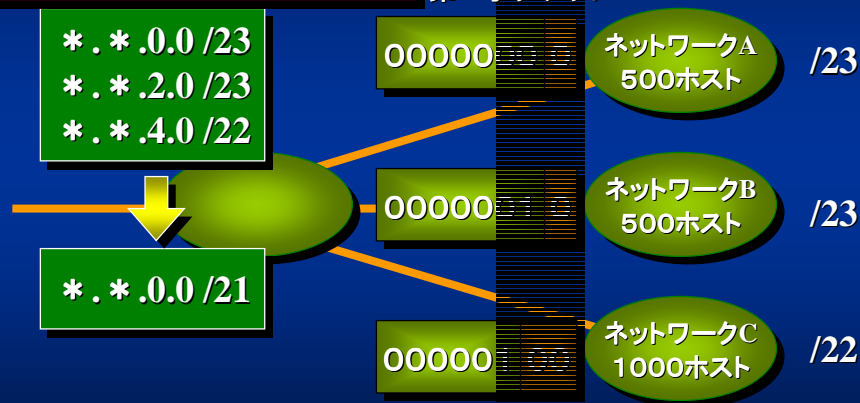
## CIDRなら...

- ネットワークに対してちょうどよい大きさのアドレスを割り当てることができる
- 複数のクラスフルアドレスを割り当てていたネットワークも一つのアドレスブロックにできるので経路情報を節約できる
- ネットワークトポロジに従った割り振りを行うことでさらに経路情報を減らせる

## 経路情報の集約

Aggregation (集約・集成)

第3オクテット



## 無駄はなくしたけど...

- CIDRの導入により、アドレス割り当ての無駄は減少
- 経路情報はうまく集約(aggregate)できた
- でも...インターネットの発展に対して32ビットのアドレスは小さすぎる

## なにかもっといい方法は...

- IPアドレスはインターネットに接続しているすべてのホストに一意につけられていなければならない
- じゃあ、インターネットに直接接続する必要のないホストには割り当てなくてよい？
  - 社内ネットワークのみに接続しているホスト
  - プロキシサーバを介してインターネットにアクセスしているホスト

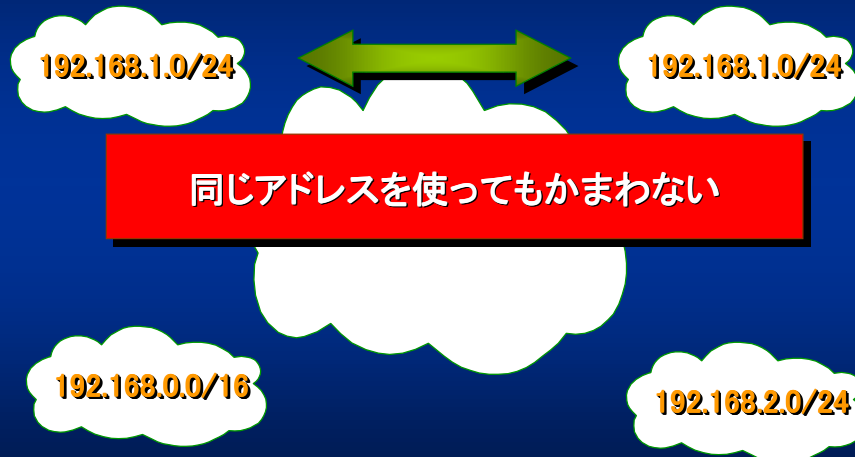
## グローバルとプライベート

- IPアドレスには、インターネット上で一意に割り当てられなければならない**グローバルアドレス**と、閉じた環境の中で自由に使える**プライベートアドレス**がある
- プライベートアドレスを用いたネットワークはインターネットに直接接続できない
- プライベートアドレスは異なるネットワークで同じアドレスを使うことができる

## プライベートアドレス

- RFC1918 で以下のアドレスがプライベートアドレスとして定義されている
  - 10.0.0.0 ~ 10.255.255.255 (10.0.0.0 /8)
  - 172.16.0.0 ~ 172.31.255.255 (172.16.0.0 /12)
  - 192.168.0.0 ~ 192.168.255.255 (192.168.0.0 /16)
- プライベートアドレスはインターネットに直接接続しない限り自由に使ってよい

## プライベートアドレスの利用



## プライベートアドレスの活用

- プライベートアドレスのネットワークは直接インターネットに接続できないが、プロキシサーバやNATを用いることで間接的に接続可能





## 問題は解決したか？

- CIDRは有効に機能し、割り当ての節約・経路情報の集約はある程度成功
  - でも根本的にアドレスが足りない
- NATとプライベートアドレスでアドレスはかなり節約されている
  - NATでは動作しないIPアプリケーションも多い
- 細分化、ヘッダ処理は依然存在
- 機能拡張は後付け機能なので互換性や普及がイマイチ

## じゃあ作り直そう

- という流れで IP というプロトコルの見直しからやろうじゃないか、ということに。

→ IPv6 へ

## IPv6の基礎

次なるプロトコルへ(IPv6)

## IPv4 からIPv6へ

- IPv4は20年以上にわたりインターネットを支えてきた基幹技術
- しかし有限な資源であるためIPv4は必ずいつかは足りなくなる
- 根本的な解決を目指してIPv6へ

## IP Next Generation

- 1991年7月
  - IPアドレスが足りなくなる、という研究を受けて IETFが調査開始
- 1992年11月
  - RFC1380 アドレスの先行き調査結果
  - 次世代のインターネットプロトコル検討開始
- 1993年12月
  - RFC1550 IPngへの機能要求

## IPv6への道

- 1995年1月
  - RFC1752 SIPPをベースにアドレスを128bit化
  - IPng(next generation)から IPv6 (IP version 6)へと正式に改名
- 1995年12月
  - RFC1884 IPv6 Addressing Architecture
    - 1998年7月に RFC2373 として改定
- 1998年末 IPv6関係RFC大改定
  - RFC2460 IPv6 Specification, etc...

## 機能的要求

- たくさんのアドレス
- 集約できる経路情報
- 単純なヘッダ構成、細分化の防止
- プラグ & プレイによる簡単な設定
- セキュリティやリアルタイム性確保などの機能の標準実装
- IPv4からの単純で柔軟な移行

## 機能的要求

- たくさんのアドレス
- 集約できる経路情報
- 単純なヘッダ構成、細分化の防止
- プラグ & プレイによる簡単な設定
- セキュリティやリアルタイム性確保などの機能の標準実装
- IPv4からの単純で柔軟な移行

## IPv6 のアドレス空間

- アドレスの長さは128ビット！
  - IPv4 の4倍の長さ
  - IPv4 の $2^{96}$ 倍のアドレス数
- $2^{128}$ 個のアドレス数
  - だいたい  $3.4 \times 10^{38}$  個
  - ばら撒いても陸地  $1\text{cm}^2$ あたり  $2.2 \times 10^{20}$ 個
- とにかく想像できないくらいたくさん！

## IPv6のアドレス表記

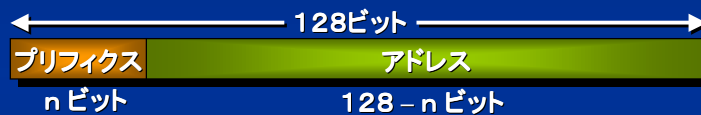
- 128bitはとっても長い！
- IPv4と同じように書くと...
  - 123.123.123.123.123.123.123.123.123.123.  
123.123.123.123
- 16ビットごとに区切って16進数で書く
- 区切り文字は“:”(コロン)
  - FFDC:BA98:7654:3210:FEDC:BA98:7654:3210

## IPv6 のアドレス省略表記

- 連続する 0 のブロックは省略できる
  - 1080 : 0 : 0 : 0 : 8 : 800 : 200C : 417A  
1080 : : 8 : 800 : 200C : 417A
  - 0 : 0 : 0 : 0 : 0 : 0 : FF01 : 9123  
:: FF01 : 9123
- 省略できるのは1ヶ所だけ
  - 0 : 0 : 0 : FF01 : 9123 : 0 : 0 : 0  
:: FF01 : 9123 : 0 : 0 : 0
  - FF01 : 9123 :: ← こうは書けない

## IPv6 アドレスの種類

- アドレス形式プリフィクス
  - IPv6 アドレスの種類を指定



001	集約可能なグローバルユニキャストアドレス
1111 1110 10	リンクローカルユニキャストアドレス
1111 1110 11	サイトローカルユニキャストアドレス
1111 1111	マルチキャストアドレス
プリフィクス以外がall 0	エニキャストアドレス

## 機能的要求

- たくさんのアドレス
- **集約できる経路情報**
- 単純なヘッダ構成、細分化の防止
- プラグ & プレイによる簡単な設定
- セキュリティやリアルタイム性確保などの機能の標準実装
- IPv4からの単純で柔軟な移行

## 経路情報の集約

- 経路情報を集約するためには...
  - クラスレスなアドレス構造
  - ネットワークの構造に応じた割り振り
  - 同じネットワークには連続したアドレスブロックを割り振る
- IPv6 は IPv4 での経験を元に集約可能 (**Aggregatable**) なアドレス構造となっている。

## 集約可能グローバルユニキャストアドレス

- ネットワークポロジに応じた階層構造を持つアドレス



FP	アドレス形式プリフィクス「001」
TLA ID	最上位階層集約子
NLA ID	次階層集約子
SLA ID	サイト階層集約子
インタフェースID	インタフェース識別子

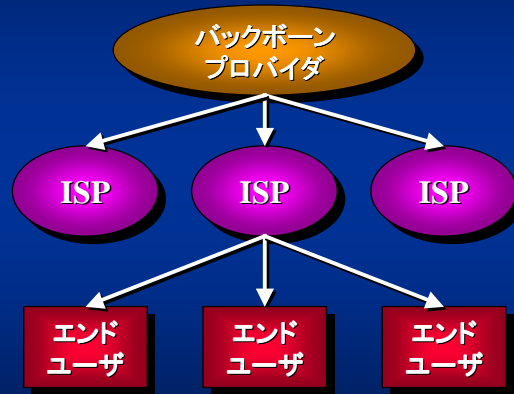
## 割り振りサイズ

- 一番大きい割り振り単位の TLA は大きすぎる





## 階層的な割り振り



## アドレス割り振りの例



## 機能的要求

- たくさんのアドレス
- 集約できる経路情報
- **単純なヘッダ構成、細分化の防止**
- プラグ & プレイによる簡単な設定
- セキュリティやリアルタイム性確保などの機能の標準実装
- IPv4からの単純で柔軟な移行

## IPv4 のヘッダ



- IHL(ヘッダ長)、オプション
  - 可変長が諸悪の根源
- TOS
  - 使われていない
  - でも優先付けは必要
- ID、フラグ、オフセット
  - 細分化があるから
- プロトコル
  - 上位層プロトコルは知らなくていい
- ヘッダチェックサム
  - 意味ない

## IPv6 のヘッダ

Ver	クラス	フローラベル	
	ペイロード長	次ヘッダ	中継制限
発信元IPアドレス			
送信先IPアドレス			

- クラス、フローラベル
  - 優先度の設定
- ペイロード長
  - 基本ヘッダより後ろの長さ
- 次ヘッダ
  - オプションヘッダが続く場合の種類
- 中継制限
  - データグラムの最大中継数

## いろんな機能はオプションで

- IPv6 ヘッダは基本情報のみでサイズ固定
- 拡張機能は独立ヘッダとして連結する



基本ヘッダは固定長なので処理が単純  
 必要な機能情報だけを付加できる  
 将来的な拡張にも柔軟に対応可能

## フォワーディングパケット細分化禁止

- フォワーディングパケット細分化によるパケット数増加は、ルータ負荷の原因
  - ネットワークにはMTUが存在する
  - 出力側I/FのMTUが入力側I/FのMTUより小さい時にフラグメント（パケット分割）が発生し、パケット数が増加する
- 経路途中での細分化を起こさないようにするためには...
  - MTU以上のIPデータグラムを送ってはいけない
  - 始点から終点までで経由するすべてのネットワークのMTUを調べ、その最小値をデータグラムサイズとする
- IPv6 は経路上の最小MTUを探索する

## 機能的要求

- たくさんのアドレス
- 集約できる経路情報
- 単純なヘッダ構成、細分化の防止
- **プラグ & プレイによる簡単な設定**
- セキュリティやリアルタイム性確保などの機能の標準実装
- IPv4からの単純で柔軟な移行

## ルーターが教えてくれるさ！

- IPv6なら、ネットワークに接続するとルーターが設定に必要な情報をインタフェースに教えてくれる
- インタフェースはルーターからのネットワーク情報と、自分のインタフェースIDでアドレスを生成



ネットワークID

インタフェースID

128ビットの IPv6 アドレス

## なんでこんなに簡単なの？

- ネットワークインタフェースにはもともと一意な番号が割り振られている
- それを利用すればインターネット上で一意なアドレスを作るのは容易
- インタフェースIDだけで64ビットもある
- ネットワークIDの目的は、ネットワークの位置識別

## プラグ&プレイとDHCPは何が違うの？

- DHCP (Dynamic Host Configuration Protocol) はあらかじめプールされたアドレスの割り当てを受けるもの
  - DHCP用アドレスを予約しておく必要がある
  - 毎回違うアドレスが割り当てられる可能性もある
- IPv6の自動設定はインタフェースが持つIDにネットワーク情報を付加してアドレスを生成するもの
  - アドレスは最初からインタフェースが持っている
  - 同じネットワークならアドレスは変わらない

## 機能的要求

- たくさんのアドレス
- 集約できる経路情報
- 単純なヘッダ構成、細分化の防止
- プラグ&プレイによる簡単な設定
- セキュリティやリアルタイム性確保などの機能の標準実装
- IPv4からの単純で柔軟な移行

## プロトコルレベルでの機能拡張

- セキュリティ機能
  - 通信するホスト間の認証と機密性を保持
  - IPsec を標準装備 (IPv4ではオプション)
- 通信の優先度を指定可能
  - リアルタイム通信が必要なものには高い優先度を設定
  - 利用方法などはまだ研究段階

## IPsec

- 通信を行う相手が正しい相手であるかどうかの確認ができる。(認証)
- 通信内容を経路途中で覗き見されないようにすることができる。(暗号化)
- IPv6 の拡張ヘッダを用いて実装

## 機能的要求

- たくさんのアドレス
- 集約できる経路情報
- 単純なヘッダ構成、細分化の防止
- プラグ & プレイによる簡単な設定
- セキュリティやリアルタイム性確保などの機能の標準実装
- IPv4からの単純で柔軟な移行

## IPv6の基礎

IPv4からIPv6への移行



## IPv4からIPv6への移行

- 移行を行うために必要なことは何か？
- IP のプロトコル変更により必要となるサービスのな変更は何か？
- どのタイミングでどのように移行すればよいのか？
- IPv4 は使えなくなってしまうのか？

## 移行による影響



アプリケーション層	メール SMTP	WWW HTTP	アプリケーション	ルータ制御 アプリケーション
トランスポート層	TCP	UDP	オペレーティング システム	ルータ制御 OS
インターネット層	IP			経路制御部
ネットワーク インタフェース層	イーサ ネット	ATM	ネットワーク インタフェース	ネットワーク インタフェース

**IPを用いるすべての部分に変更が必要！**

## 変更が必要な点

- アプリケーション
  - IPv6 のアドレス表記の入出力
  - TCP/IP とのアプリケーションインタフェース部分
- オペレーティングシステム
  - IPv6 のアドレス表記の理解
  - IPv6 固有の機能の実装
  - インタフェースドライバの IPv6 対応
- ルータ
  - IPv6 の経路情報の管理

## DNS のIPv6 対応

- インターネットの基幹サービスはDNS
  - DNS はドメイン名と IP アドレスの変換を行う
  - DNS の正引き(ドメイン名→ IP アドレス)に対して IPv6 の情報を登録(AAAA レコード)
  - DNS の逆引き( IP アドレス→ドメイン名)のために IPv6 のアドレス空間を新しく作成
- DNS の実装である BIND は対応済み

## 移行の流れ

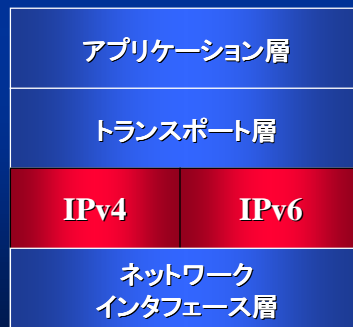
- あるタイミングでインターネット上のすべてのネットワークを IPv4 から IPv6 へ一斉に置き換えることはできない
- ネットワーク単位で移行を進める
- ネットワークの中でも IPv4 と IPv6 を少しずつ置き換えていく
- いずれ全てが IPv6 の世界に移行する

## IPv4とIPv6の共存

- デュアルIPスタック
  - IPv4 と IPv6 の両方のプロトコルスタックを同時に扱う
- トンネリング
  - IPv6プロトコルをIPv4データグラムとして送出することで、IPv4ネットワークの中を転送

## デュアルIPスタック

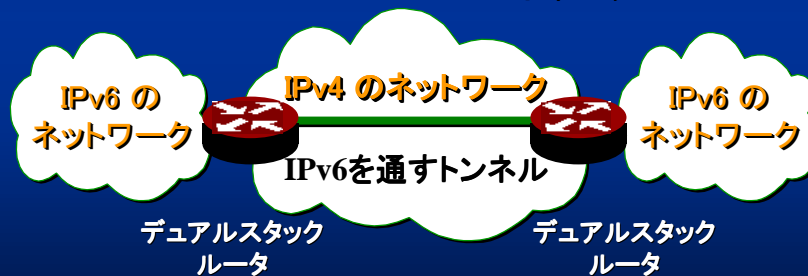
- IPv4 と IPv6 の両方を扱えるホスト、ルータが可能
- ネットワーク内で IPv4 と IPv6 を共存
- 徐々に全体を IPv6 へと移行させていく



## トンネリング(1)

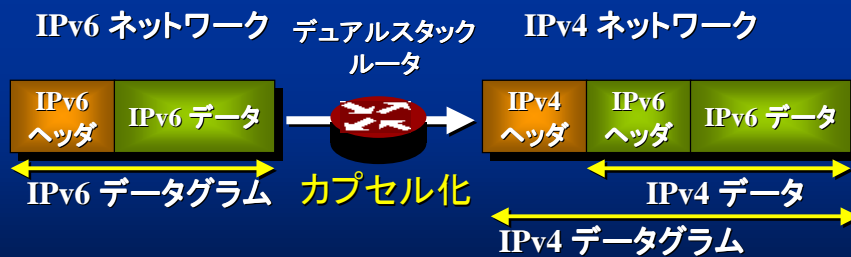
- IPv4 の世界で IPv6 ネットワークが通信をするためには？

### IPv6 over IPv4 トンネリング



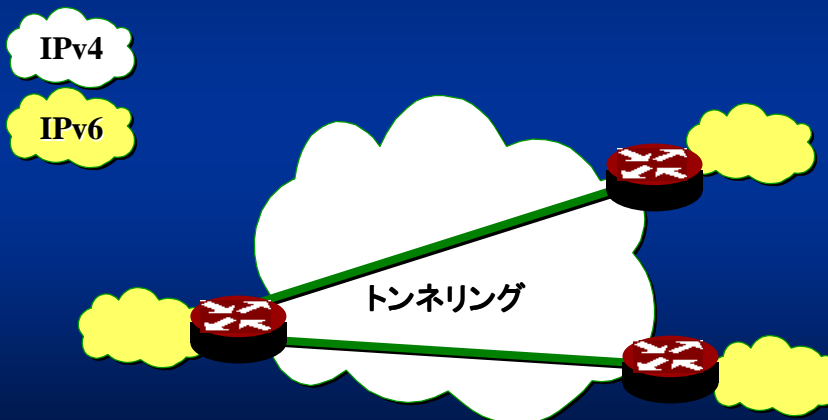
## トンネリング(2)

- 異なるプロトコルパケットを、通信経路のプロトコルでカプセル化して相手ネットワークまで転送する技術



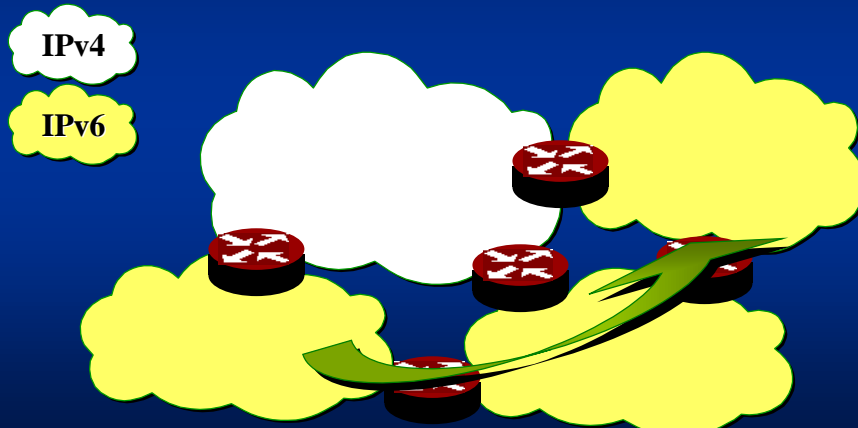
## 移行のストーリー(第1段階)

- IPv6 over IPv4 トンネリング



## 移行のストーリー(第2段階)

- ネイティブなIPv6プロトコルでの通信

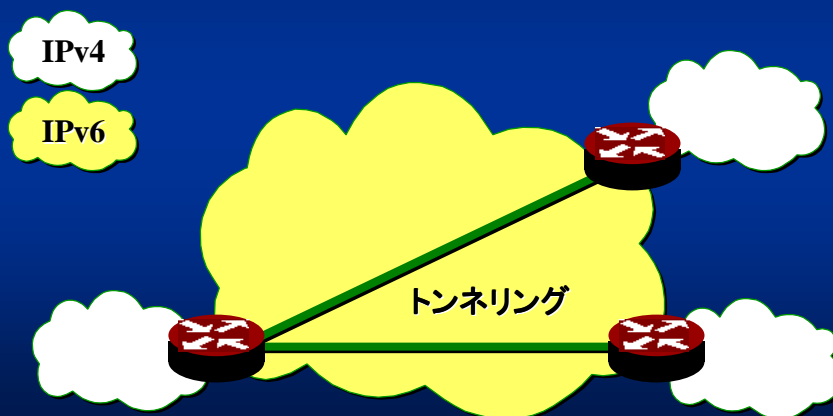


Internet Week 2001 [2001/12/5]

©Copyright 2001 Japan Network Information Center

## 移行のストーリー(第3段階)

- IPv4 over IPv6トンネリング



Internet Week 2001 [2001/12/5]

©Copyright 2001 Japan Network Information Center

## IPv4 は使えなくなるのか？

- IPv4 は徐々に IPv6 で置き換えられていくと考えられるが、IPv4 が使えなくなるわけではない
- インターネットの基幹が IPv6 に置き換えられてもトンネリングなどを用いて通信することは可能
- IPv6 への移行はいずれ必ず行われる。IPv4 に特化しないサービス・ネットワーク運用を視野に入れておく必要はある

## IPv6の基礎

IPv6への対応

## 基本ネットワーク・アプリケーションの IPv6 対応

- 最も対応が進んでいる分野
  - DNS (BIND9以降)
  - HTTP (Apach 2.0以降)
  - SMTP ( Sendmail 8.10以降)

## ルータ/L3スイッチの IPv6 対応

- ルータ
  - バックボーン向け大型ルータからSOHO向けルータまで、ほぼ全ての領域で対応
  - 2002年には主要製品のIPv6対応が完了
- L3スイッチ
  - 対応が進行中
  - 順調に製品が登場しているが、選択肢は限られる



## OS/プロトコルスタックの IPv6 対応

- OS
  - Windows XPでIPv6標準実装
  - BSD/OS, Solaris, FreeBSD4, Linux
- プロトコルスタック(通信プロトコル・ソフトウェア)
  - KAME(BSD UNIX用)
  - USAGI(Linux用)

## IPv6対応が遅れている分野

- アプリケーション
  - OSのIPv6対応を待っている状態
- ネットワーク管理製品
- セキュリティ管理製品
  - ファイアウォールなど

## 接続サービスの IPv6 対応

- 既に国内大手ISPは sTLA を取得
- 実験フェーズから商用サービスフェーズへ
  - トンネリング接続サービスが多い
  - IPv6 専用ネイティブ接続、デュアルスタック接続も登場
- データ・センターのIPv6対応も始まった

## 6bone

- IPv6 のプロトコル設計段階から運用されている実験用ネットワーク
- 実験用のアドレスブロック pseudo-TLA (pTLA) を割り振っている
- IPv6 のプロトコル仕様の検証、各実装の相互接続性、ソフトウェア・ハードウェアの動作検証に果たした役割は大きい
- 日本でも 6bone に接続する形で 6bone-jp が WIDE Project 主導の元で運用されている

## 6bone-jp と NSPIXP-6

- 6bone-jp
  - WIDE が 6bone から pTLA を取得し運用
  - 接続する組織は WIDE から NLA を取得
- NSPIXP-6
  - 1999年8月に運用開始された IPv6 によるインターネット相互接続点
  - IPv6 による基幹ネットワーク構成のための基盤

## IPv6アドレスポリシー

IPv6アドレスの分配

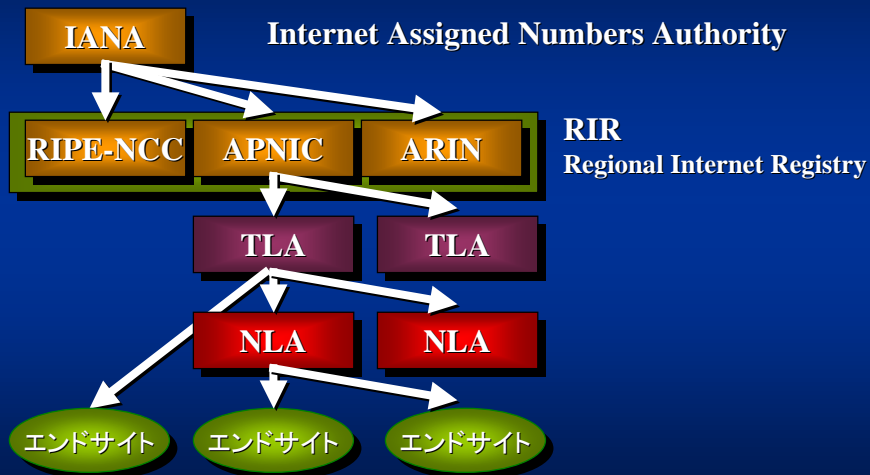
## IPv6 sTLA 割り振り

- IPv6 割り当て/割り振り暫定ポリシーに基づいた、sub-TLA (sTLA) アドレスの割り振りが1999年7月に開始
- 2000年1月20日よりJPNICはJPNIC 会員（現、IP指定事業者）を対象としてAPNIC への申請取り次ぎサービスを開始
- ISPがsTLAアドレスを取得して IPv6 接続サービスを始めつつある

## IP アドレスの階層的配分

- インターネット上で一意な IP アドレスを割り振るために、階層的なレジストリ構造が作られている
- ユーザは好きなアドレスを勝手に利用することはできず、必ずレジストリにアドレスの利用申請を行い、それにより配分されたアドレスを利用しなければならない

## IPv6 アドレスの割り振り階層



## sTLA割り振り条件

- 既に IPv6 ネットワークを運用し、他の3つ以上の sTLA IPv6 ネットワークとピアリングしていること
  - に加えて、以下のどちらかを満たすこと
- 上流ISPから受け取ったIPv6 アドレスを40の SLA 顧客サイトに割り当てていること
- sTLA を割り振られてから12ヶ月以内に IPv6 サービスを提供すること

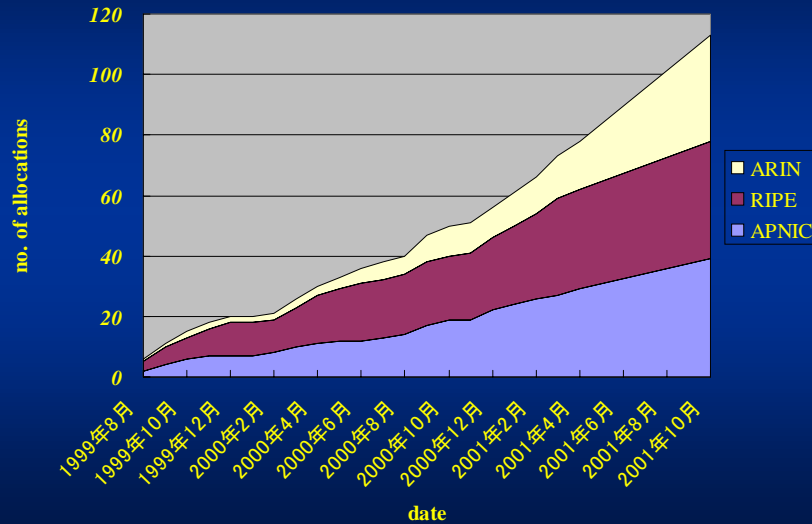
## sTLA の初期の割り振り条件

- 新しいIPv6ポリシーが、今の割り振り条件の意図を汲んで実装されるまでの期間(Bootstrap期間)適用(当初の、世界全体でsTLA割り振り組織が100になるまでから延長)
  - 申請組織のネットワークが、他の3つ以上のASとピアリングしていること
  - sTLA の割り振りを受けてから12ヶ月以内に IPv6 サービスを提供すること
- に加えて、以下のどちらかを満たすこと
  - IPv4のトランジットプロバイダであって、40以上の顧客に IPv4 アドレスを割り当て済みであること
  - 6bone に6ヶ月以上参加し、pTLA を3ヶ月以上運用していること

## sTLAの割り振りを受けるには

- sTLA は、RIR(日本の場合、APNIC)が直接割り振る
- APNIC は APNIC 会員にのみ sTLA の割り振りを行う
  - APNIC から割り振りを受けるためには APNIC 会員になる必要がある
- JPNIC は APNIC 会員なので、JPNIC IP指定事業者は、JPNIC を通して申請を行うことで APNIC 会員にならずに sTLA を申請可能

## sTLA 割り振りの推移



Internet Week 2001 [2001/12/5]

©Copyright 2001 Japan Network Information Center

## sTLA 割り振りの現状

- APNIC... 2001:200::/23
  - 40組織
- ARIN... 2001::400::/23
  - 21組織
- RIPE-NCC... 2001:600::/23
  - 48組織

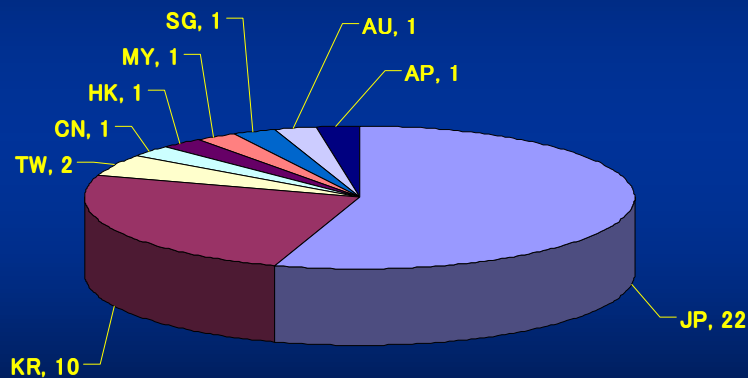
2001年10月16日現在

<http://www.dfn.de/service/ipv6/ipv6aggis.html> より

Internet Week 2001 [2001/12/5]

©Copyright 2001 Japan Network Information Center

## APNIC Allocations by Country



## 割り振り基準を満たさない場合

- sTLA の割り振り基準を満たすのは、インターネットの基幹を構成する大手のISP
- 一般的な ISP は、sTLA を持つ組織からNLAの割り振りを受ける
- sTLA を割り振られた組織が NLA 以下にどのように割り振りを行うかはその組織のポリシー
  - ただし、グローバルな割り振りポリシーに従う必要はある



## JPNICのsTLA申請取り次ぎ

- Webインタフェースでの申請  
<http://www-v6.nic.ad.jp/v6/ipv6req.pl>
- 手数料は5万円 (JPNIC手数料 + APNIC sTLA 割り振り手数料)  
※ただし、割り振りが行われなかった場合は不要
- 手数料の請求は審議終了後
- 申請のやりとりは英語

## JPNIC IPv6 窓口

- IPv6 sTLA 申請、IPv6 に関するお問い合わせなどは...

**[ipv6-support@nic.ad.jp](mailto:ipv6-support@nic.ad.jp)**

- sTLA申請、IPv6 に関する情報は...  
<http://www.nic.ad.jp/jp/regist/ipv6/index.html>

## IPv6アドレスポリシー

IPv6アドレスポリシーのこれから

## IPv6のこれから

- インターネットが IPv4 から IPv6 へと移行するのは必然の流れ
- IPv4 のネットワークがいつまで主流であるかは予想が難しい
- IPv6 は拡張機能などで検討中の部分も多いが、基本的なプロトコル部分だけでも移行価値は大きい

## 現在のIPv6アドレスポリシー

- Provisional IPv6 Assignment and Allocation Policy Document

<http://www.apnic.net/drafts/ipv6/ipv6-policy-280599.html>

- 1999年5月にRFC2374をもとにRIRが暫定的に制定
- 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
- sTLA取得条件等を規定
- 基本的なところはIPv4を踏襲
- 未規定部分も多い
  - Assignmentの大部分
  - Initial allocation/35以降のallocation方法
    - TLAになるやり方も含めて未規定

## IPv6ポリシー新たな展開

- IESG/IABからのプロポーザル
  - 1-3bit, 48-128bitはtechnical boundaryでIETFの領域
  - 3-48bitはpolicy boundary
    - 新たにポリシーを決めていく
    - No more TLA/sTLA/NLA?
  - ARIN/RIPEなどのミーティングの雰囲気では、ほぼこの方向で決着していく見込み

## IPv6アドレスポリシーの課題(1)

- Provisionalなポリシー後の新たな規則は？
- Bootstrapフェーズ終了後は？
- sTLA取得組織の再申請の枠組みは？

## IPv6アドレスポリシーの課題(2)

- 現状の規則
  - 未規定部分が多くその議論、定義が必要

例) LIRからエンドユーザへの割り当て規則

割り当て審議の要否

→ v4と同じ？

エンドユーザの定義

80%ルールの妥当性(追加割り振り)

## IPv6アドレスポリシーの今後

- Bootstrapフェーズ終了後のIPv6アドレス管理規則の策定が急務
- **IPv4アドレス管理の踏襲の是非の議論**
- IPv6ネットワーク運用とアドレス管理について検討が必要
- 特に情報家電におけるIPv6アドレス利用に関する議論も必要

## 新ポリシーの提案(1)

- JPNICから「新IPv6アドレスポリシー提案」
  - 初期割り振り
  - 追加割り振り
  - LIRからISPへの割り振り
  - 割り当て
  - DB登録
  - 特別なケース
    - マルチホーム、IX

## 新ポリシーの提案(2)

- 日本国内の様々なコミュニティでラフコンセンサスを得た内容
  - JPNIC IP-USERS and IP-WG
  - IPv6 Operation Study Group
  - WIDE
  - JANOG
- 2001年8月のAPNIC Open Policy Meeting (台北)に日本の中のコンセンサスとして提案

## 新ポリシーの提案(3)

- IPアドレス管理の五大原則(一意性, 登録, 経路集成, 節約, 公平性)に基づく
- IPv4に比べて節約よりも集成に重きを置く
- ISPの実状を考慮した上で、割り振り割り当てサイズの適正化を図る

## 新ポリシーの提案(割り振り)

- 初期割り振り
  - 2つ以上のupstreamもしくは5つ以上のpeeringをもつIPv6サービスプロバイダ
- 追加割り振り
  - 50%使ったら、追加割り振り申請可能
  - アドレス使用量は顧客数でチェックされる
    - RIR/NIR/LIRの負担を軽くする

## 新ポリシーの提案(割り当て-1)

- 割り当てサイズ /48, /64, /128?
  - It's within the IETF boundary.
  - 上位レジストリはLIRやISPがエンドユーザにどのサイズを割り当てるかについて関与できない
- Multiple /48s
  - エンドユーザが/48を使い切ってさらにアドレスが必要な場合には、ユーザは次の/48を必要なjustificationをもって申請できる。このリクエストはRIR/NIRレベルで処理される

## 新ポリシーの提案(割り当て-2)

- エンドユーザの定義
  - company basis、location basis、ISP-contract basis ?
  - ISPとの接続単位
    - ただし明らかに同一LANに接続する複数契約は除く
- インフラへの割り当て
  - Basically /48 (1サイトへの割り当てと等価に考える)
  - 事務用途や別部門ネットワークは含まれない

## 新ポリシーの提案(DB 登録)

- すべての/48を登録する
- LIRはrps-distを実装したソフトを採用して、NIRやRIRのDBと協調動作させるのが望ましい
- ホームユーザへのプライバシー面での保護は別途考慮すべき



## 新ポリシーの提案(その後-1)

- 8月のAPNIC Open Policy Meeting (台北)において、RIRサイドからの対案との統合案が、AP地域でのコンセンサスに至った
  - 初期割り振りを /32 とする(IPv4からの移行の場合、既存ネットワーク規模勘案でより大きなブロックの割り振りも可能)
  - 追加割り当ての条件となる利用率指標として HD Ratio と呼ばれる算出方法を利用し、本指標 0.8 -- 0.85 の間を条件とする方向で今後検討していく
  - 追加割り振りサイズはその直前の割り振りサイズの2倍(プリフィクス長で1ビット少ないサイズ)を基本とする
- この統合案をRIPE/NCC, ARINなどの他の地域でも提案

## 新ポリシーの提案(その後-2)

- RIPE 40 (1-5 Oct-2001)
  - Mirjam, 荒野氏(JPNIC IP-WG) & David Pratt による提案
    - 現在の暫定ポリシーは直ぐにでも変更が必要
      - 現在の暫定ポリシーは、充分なものではない
      - IPv6のサービスを行っている日本のISPにとって、半年の遅れは待てない
    - RIRはワーキンググループと共に新しいポリシーのドラフト作成(現在は、既に行われている)
- ARINミーティング (28-31 Oct-2001)
  - RIPEとほぼ同様の結論

## 新ポリシーの提案

### (RIPE/ARINミーティングへの提案結果)

- 日本からのIPv6ポリシーの緊急性の要求は認識された
- 具体的なIPv6ポリシーとして年内を目標に策定することで合意
  - 今後グローバルメーリングリストを作りそこで議論
  - 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

## 新ポリシーの提案

### (グローバルメーリングリスト)

- IPv6ポリシーを議論するグローバルメーリングリストは既に作成されている
  - [global-v6@apnic.net](mailto:global-v6@apnic.net)
  - 登録方法/アーカイブは下記URLから  
[http://www.apnic.net/net\\_comm/lists/index.html](http://www.apnic.net/net_comm/lists/index.html)

## 参考資料

## 参考(関連サイト)

- IETF (Internet Engineering Task Force)
  - <http://www.ietf.org/>
- IETF IPng working group
  - <http://playground.sun.com/pub/ipng/html/ipng-main.html>
- 6bone
  - <http://www.6bone.net/>
- 6bone-jp
  - <http://www.v6.sfc.wide.ad.jp/>

## 参考(インターネットレジストリ)

- IANA
  - <http://www.iana.org/>
- ICANN
  - <http://www.icann.org/>
- APNIC
  - <http://www.apnic.net/>
- JPNIC
  - <http://www.nic.ad.jp/>

## 参考(関連 RFC)

- RFC2373: IPv6 Addressing Architecture
- RFC2374: An IPv6 Aggregatable Global Unicast Address Format
- RFC2401: Security Architecture for the Internet Protocol
- RFC2460: IPv6 Specification
- RFC2461: Neighbor Discovery for IPv6
- RFC2462: IPv6 Stateless Address Autoconfiguration
- RFC2463: ICMPv6 for IPv6