

IPv6”再”入門

基礎編

松本 存史

NTT 情報流通プラットフォーム研究所

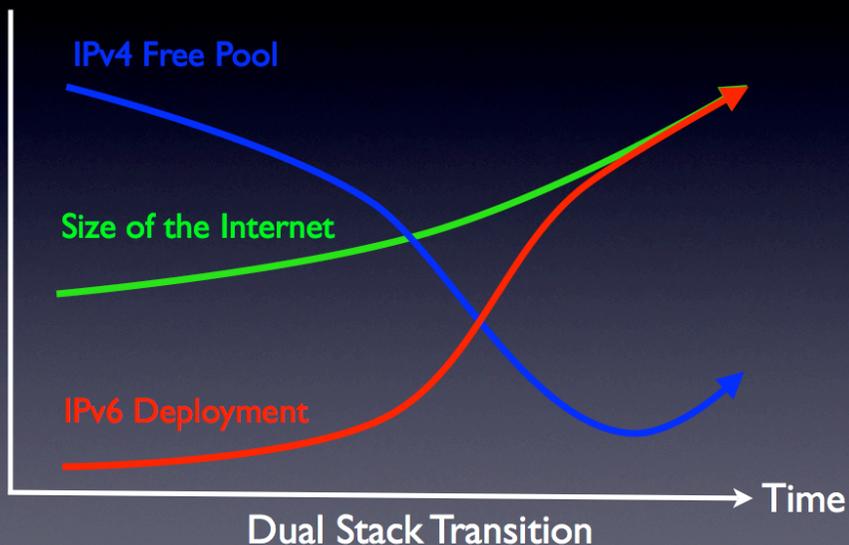
IPv6”再”入門とは

- 昔、IPv6を学んだ方
- IPv6を学ぼうとして途中で挫折した方
- を対象として
- “IPv6の今”について解説します

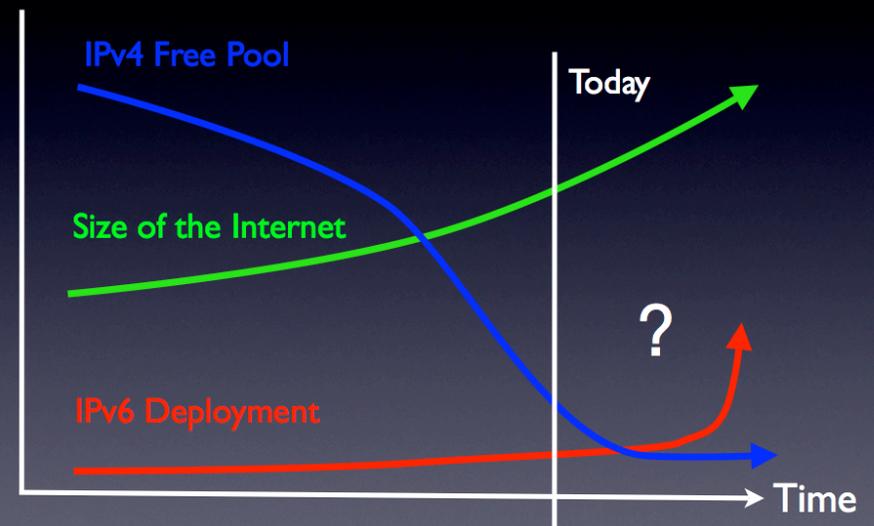
IPv6普及プランと現実

- IPv4アドレスが枯渇する頃にはとっくに普及しているはずだった
- しかし現実には枯渇は目前だが普及はほとんどしていない

The Plan



The Reality



なぜこうなった？

- 移行プランが無かった、もしくは現実的じゃなかった
- 現実的なコストの見積もりが無かった
- 現場の人々からのサポートが無かった
- IPv6の仕様が現実的じゃなかった

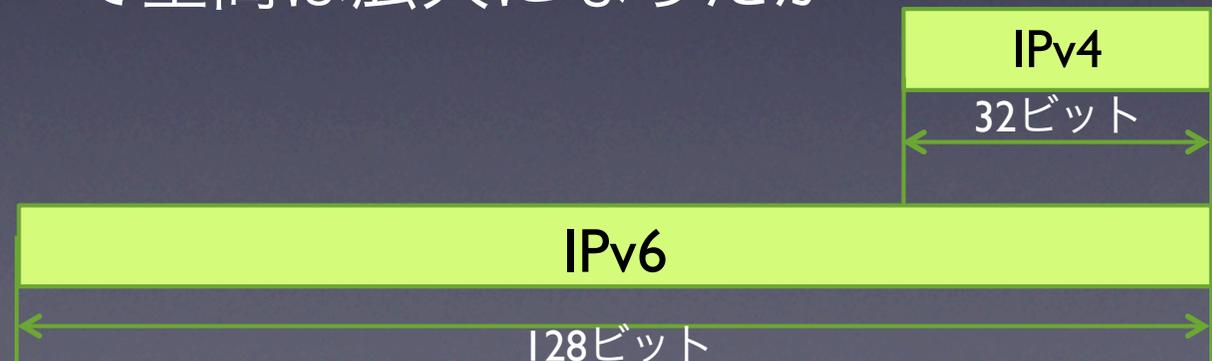
IPv6の今

- IPv6誕生当初とは大分変わった
 - 仕樣的にも
 - IPv6への期待/認識も
- IPv6の現在の正しい認識を
 - いくつかのIPv6神話が崩壊した

IPv6の基本仕様

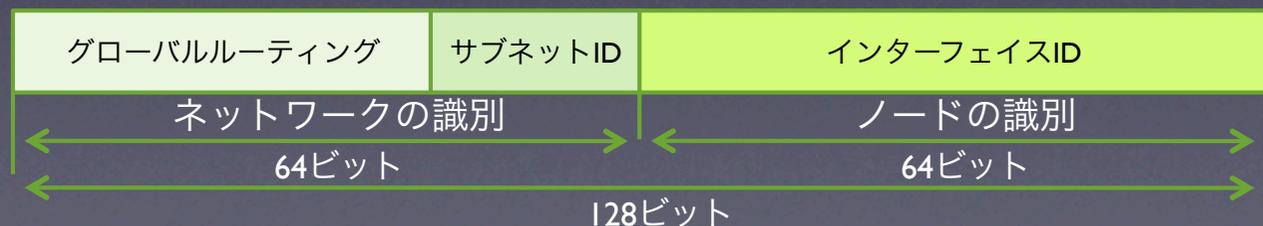
神話: IPv6アドレス空間は十 二分に大きい

- 128ビットのアドレス
 - IPv4 : IPv6 = バケツの体積 : 太陽の体積
 - 約340澗個 (澗 = 1036)
- 全てのノードにIPv6アドレスを付与
- 確かにIPv4に比べて空間は広大になったが



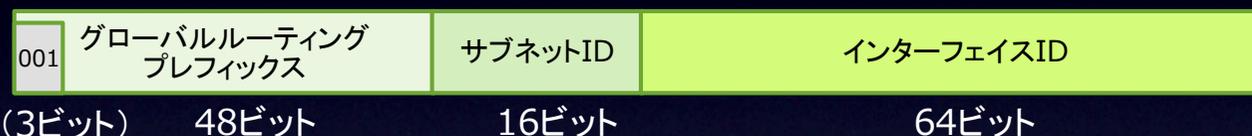
現実: IPv6アドレス空間は十二分に大きいとは言えない

- 64bitスペースが全てのLANに。
 - つまり空間の半分は無くなるということ
 - Point-to-Pointリンクに/64を使ったり
- さらにユーザ当たり/48または/56の配布を想定
- RIRは/32以上の空間を配布
- 15年後には、これをIPv4のレガシー/8空間の繰り返しだと思うようになるかも。



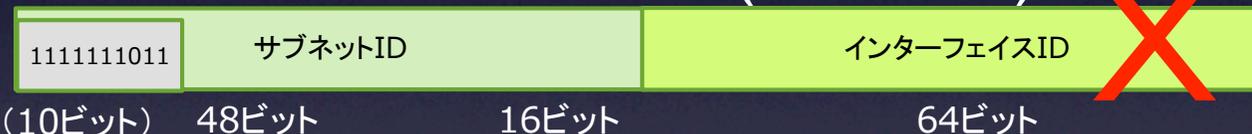
神話: IPv6アドレスには サイトローカルスコープがある

- グローバルユニキャストアドレス(2000::/3)



・インターネットへの接続の際に仕様

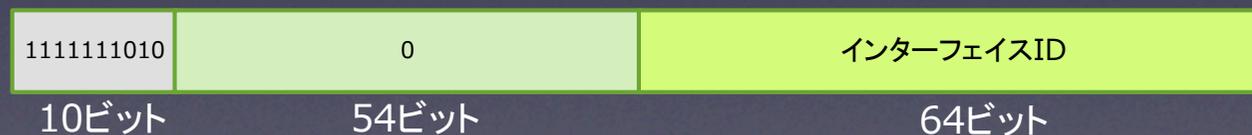
- サイトローカルアドレス(fec0::/10)



・インターネット未接続サイトなどでの利用を想定

× 廃止

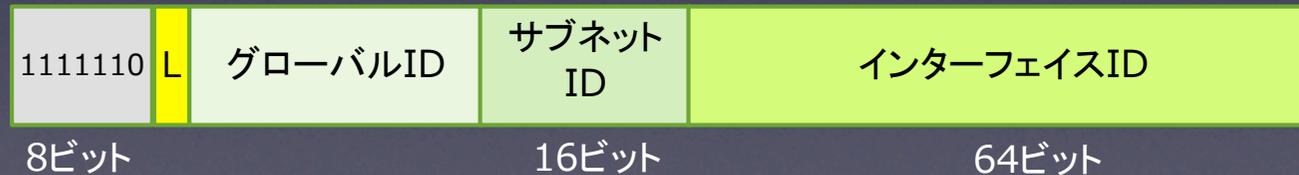
- リンクローカルアドレス(fe80::/10)



・同一リンク (セグメント) 内にて一意なアドレス

現実: IPv6アドレスには サイトローカルスコープは廃止

- サイトローカルアドレスは廃止
 - サイトの定義が曖昧で使いにくい
 - 多サイトと重複の可能性がある
 - (マルチキャストアドレスは今まで通り)
- 新たにULA(Unique Local IPv6 Unicast Address)が誕生
 - スコープはGlobal, 利用範囲は経路制御で制限



Lビット : 0=登録制 (将来利用) 1=ランダム生成による独自割り当て

神話: IPv6はセキュアだ

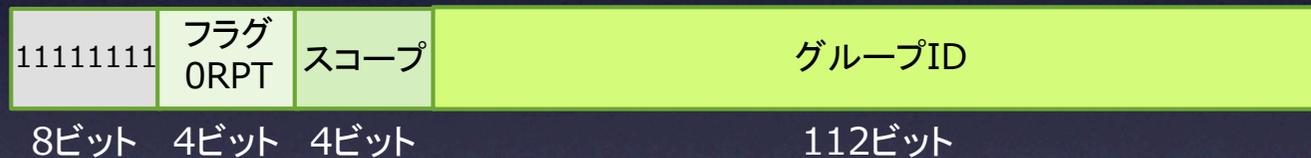
- IPv6ではIPsec実装が必須
- IPv4ではNATがあるため、IPsecが実質利用できなかった
- IPv6はアドレス空間が広大なため、アドレススキャンが困難

神話: IPv6はセキュリティ面 では変化無し

- IPsec実装必須といっても
 - 結局実装されていないものも多く、PKIもやはり未整備
- IPv6にNATが無いとしても
 - NAT-64(トランスレータ)装置があれば同じ事
 - Firewall, HGWでIPsecがデフォルトでブロックされることも多い
- アドレススキャンは難しくなっても
 - botnetによるスキャンもあるし、アドレス情報が取引されるようになるだけ

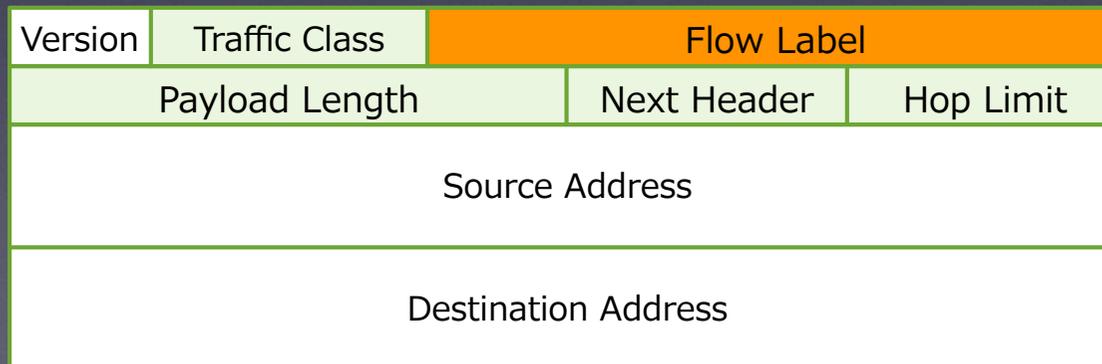
神話: QoS/マルチキャストは IPv6が有利

- IPv6の基本機能にマルチキャストが含まれている
- マルチキャストアドレス空間が広大である
膨大な数のチャンネルが利用可能



- FlowLabelというQoS用のフィールドが定義

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

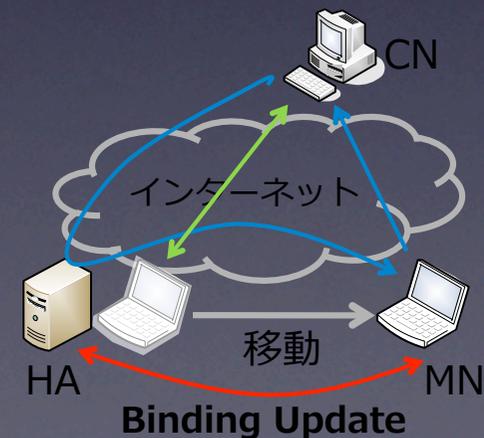


現実: QoS/マルチキャストは IPv4とあまり変わらない

- IPv4に比べてIPv6のマルチキャストの利点はほぼ無い
 - 端末での実装は既にIPv4でも普及、中継網で有効化するかどうかだけの問題
 - チャンネル数もIPv4時代で既に十分
- QoS機能も現状では、特に利点が無い
 - FlowLabelというフィールドが定義されているが、利用方法は明確になっておらず、実質利用されていない

神話: IPv6はモバイルに有利

- IPv6ではIPv4よりも効率的なモバイル通信が可能
- IPv4では三角形路が常に発生していた
- しかし、IPv6では二者間の直接通信が可能
- IPv4ではNATが存在し、MobileIP通信が困難だった
- IPv6ではサイトごと、丸ごと移動できるネットワークモビリティ機能も存在する



現実: IPv6でもモビリティの 利用は困難

- 現時点で、MobileIPv6に対応した実装は少ない
 - Windows (Vista)ではサポートされていない
 - 移動ノードとしても、また固定ノードとしても
- また、利用できるネットワーク環境も少ない？
 - MobileIPv6関連拡張ヘッダーを遮断している環境では利用できない
- そもそもIPモビリティのニーズが無い？

IPv6の設計思想

神話: IPv6はプラグアンド プレイ対応が利点

- プラグアンドプレイ="つなげばすぐに使える"
- 現実：既にIPv4でDHCPが実現している
 - むしろ、IPv6では複雑になった
 - DHCPv6ではdefault routeは設定できずRAと要併用
 - 逆にRAですべてを設定する事もできない

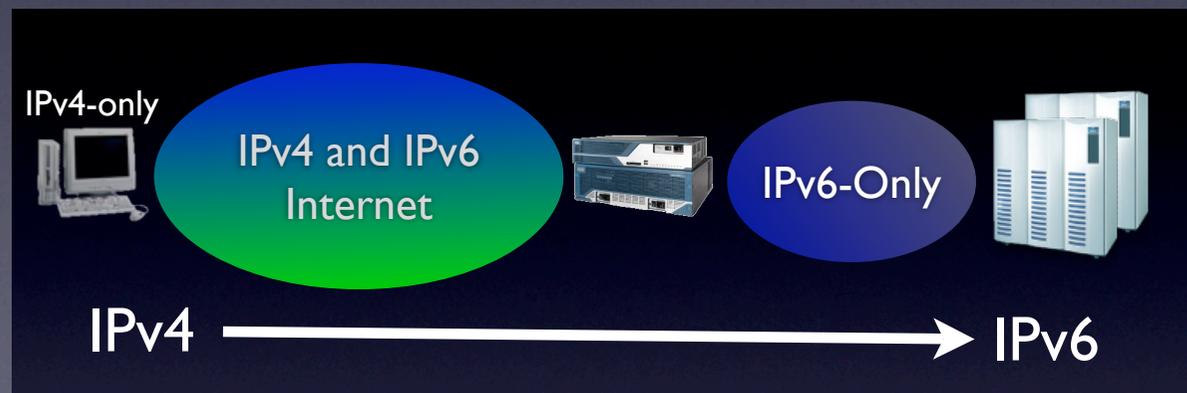
	RA	DHCPv6
アドレス設定	○	○
DNS	△	○
default route	○	X
その他	MTU,特定経路	SIP,NIS,ドメイン名

神話: IPv6ではNATの無い 世界が訪れる

- IPv6インターネットでは全ての端末にIPv6アドレスを付与する
- End-to-End透過性への回帰
 - 「End同士が、間に何も無いがごとく通信できる」
 - IPv4当初の思想でもある
 - しかしNATにより崩壊した
- IPsecによりend-to-endのセキュリティを実現

現実: IPv6-IPv4NATによる NATが残り続ける

- IPv6-onlyなサイトはIPv4インターネットに到達不能
- IPv4-onlyなサイトは今後10年は残り続ける
- 全てのIPv6サイトはIPv4アドレスとALG付き6-4NATが必要
 - 6-4NAT配下のIPv4端末とはEnd-to-End透過な通信は困難
- 結局、短期的/中期的にはIPv6はIPv4-IPv6 NATの使用を増加させる

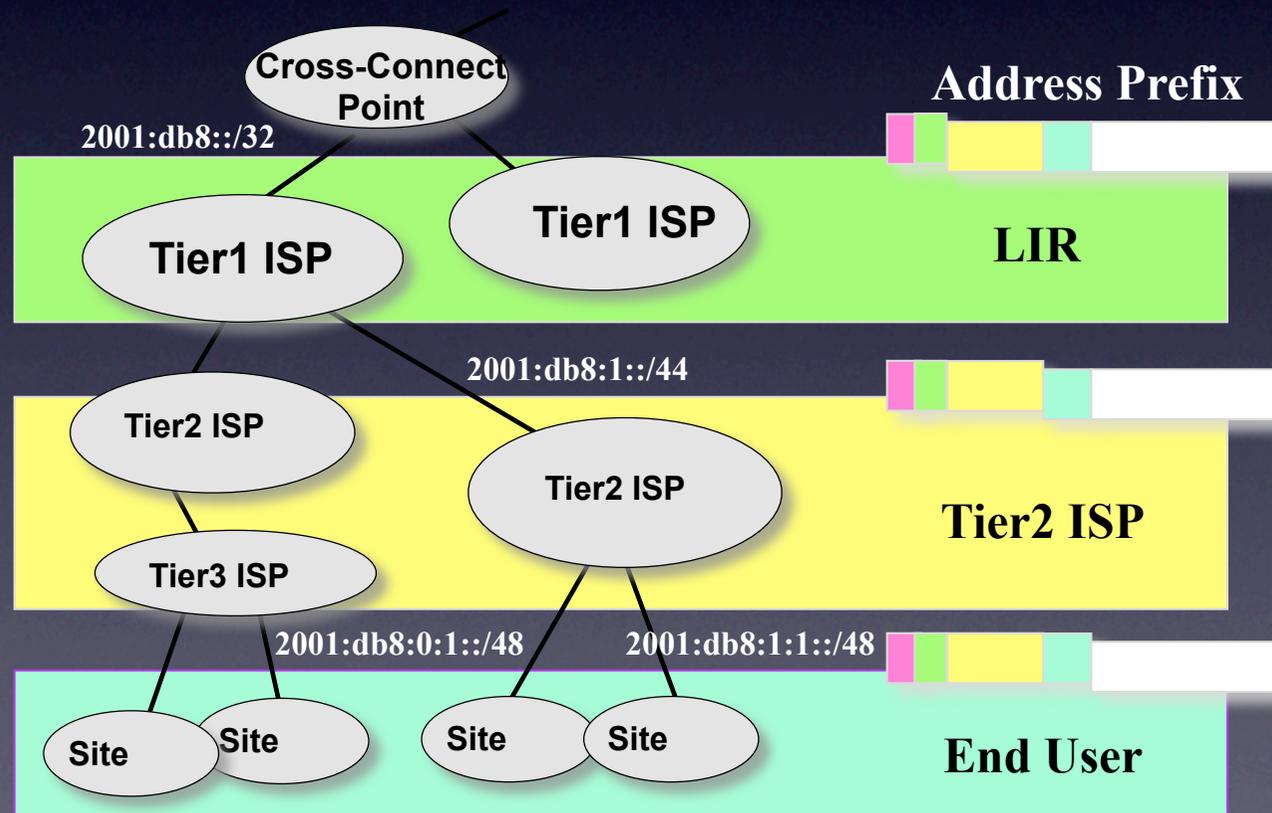


現実: IPv6-IPv6 NATの出現

- 現在、IETFでIPv6 NATが検討されている
 - 小規模サイトのマルチホーム用途
 - サイト内のトポロジー/ホスト数隠蔽
 - サイト内のリナンバリングの簡便化
 - サーバサイドのロードバランシング など
- 既にIPv6 NAT製品が市中に出回り始めている
- しかし、IPv4程はNATは蔓延らないかもしれない

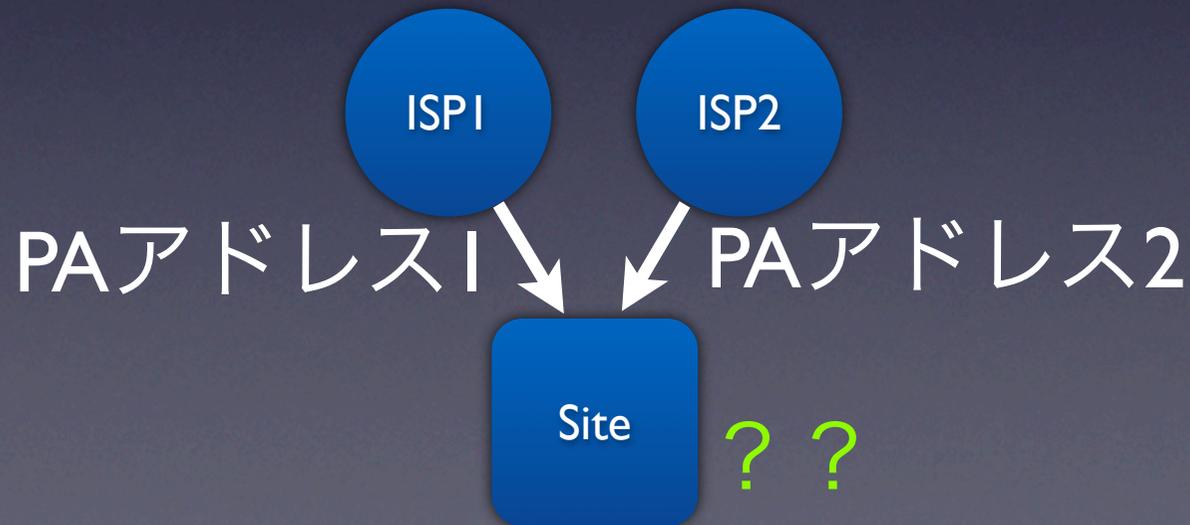
神話: IPv6で経路表爆発の 問題も解決

- IPv4では無計画なアドレス割当てにより、経路表が爆発
- IPv6では階層型アドレス割当てにより問題を解決



現実: 階層型アドレス割当ではマルチホームが実現不可

- 複数PAアドレスを用いたマルチホーム方式が未確立
 - PA: プロバイダ集約可能(Provider Aggregatable)
 - IETF multi6 wg, shim6 wgなどで検討されたが、現実的な解は出ず 2001年3月～



現実: IPv6ではより酷くなる

- IPv6でもPI(プロバイダ非依存)アドレスが配布開始 2006年夏
 - 主に現場からのニーズによってRIRが導入
- マルチホーム方式はIPv4と同等に、経路数はそれ以上に
- 当面の間、IPv4+IPv6のフルルートを取わなければならない
- 新たな方式検討がIETFで行われているが、後の祭りか？

IPv6への移行方法

普及展開

神話: IPv4端末とIPv6端末間の通信にはトランスレータを使う

- IPv4端末とIPv6端末との通信にはトランスレータを使う
- IPv4しか対応していないレガシーな端末は残る
- IPv4アドレス枯渇により、IPv6のみのサイトも出現する



現実: IPプロトコル変換方式 は存在しない

- IPv4-IPv6プロトコル変換の実際の利用方式であるNAT-PTは
廃止 2007.7
- パケットレベルの変換方式のRFC(2765)は現在も有効
- 廃止理由は沢山列挙されている(RFC4966)
- DNS-ALGへの依存性などのため
- 実質、今使用できるのはALG等のみ
- (現在、IETFでNAT-PTに替わるプロトコル変換方式を検討
中)

詳細は標準化最新動向編で

神話: キラーアプリがIPv6を 普及させる

- ウェブがインターネットを爆発的に普及させたように、何かのアプリケーションがIPv6を普及させるに違いない
- End-to-End通信を使ったアプリとか

現実: キラーアプリは 現れない

- IPv6誕生から10年以上が経過したが、キラーアプリは現れていない
 - Chicken-and-Egg問題に陥っている
- 時間が経つにつれ、IPv6の「新機能」が神話であることがわかってきた
- IPv4でもやろうと思えばできてしまう
 - 今やるならIPv4をサポートしないと流行らない
- IPv6の普及が転換点を超えれば、IPv6-onlyアプリは出るだろう

神話: Windows Vista/7になればIPv6は普及する

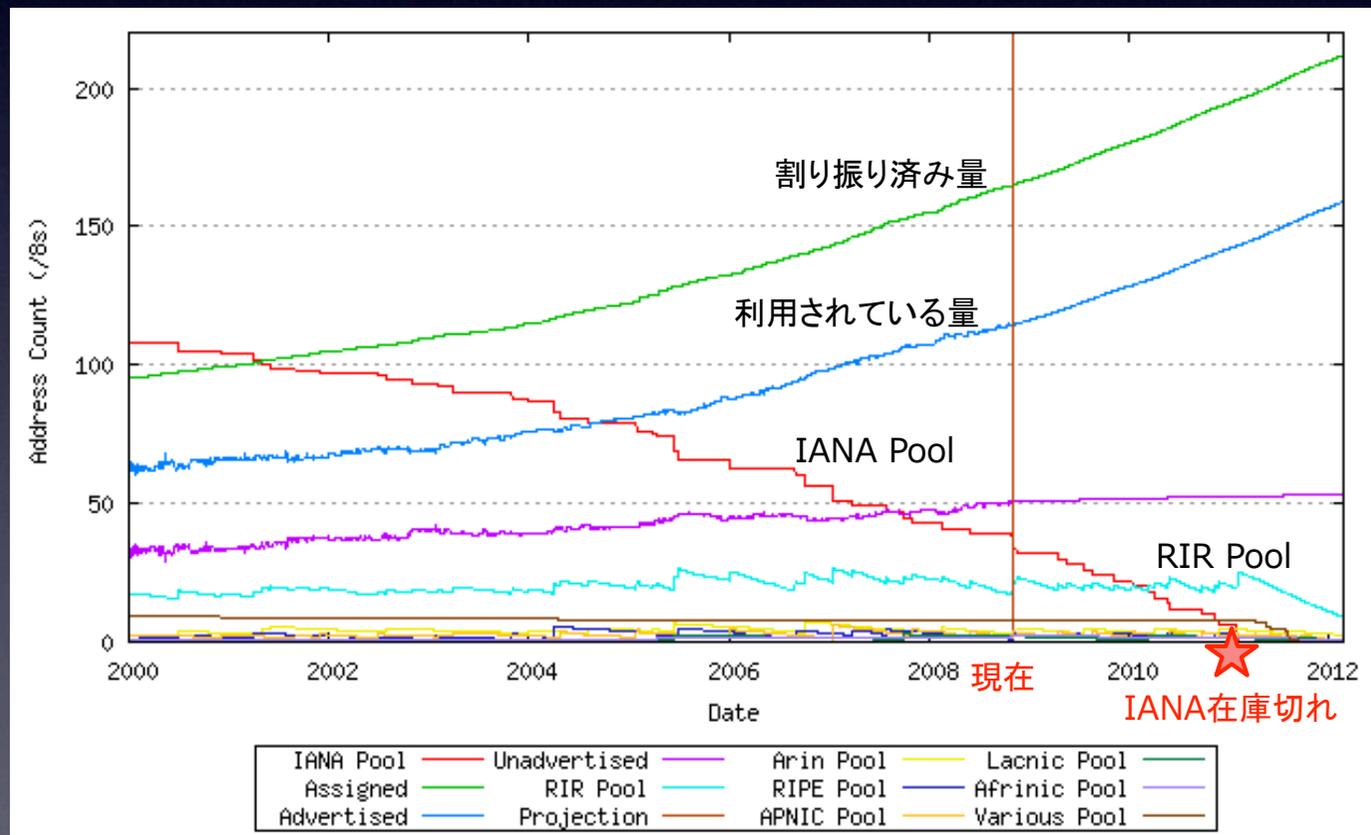
- VistaはデフォルトでIPv6がオン
- IPv4しか利用できない環境でもIPv6が使える
 - 6to4, Teredoなどの自動トンネル機能
- ほぼ全てのWindows付属アプリがIPv6対応
- Meeting SpaceなどP2PソフトはIPv6でのみ動作する

現実:Windowsだけでは IPv6は普及しない

- Windows Vista 2006年11月出荷開始
- 3年経ってもIPv6のトラフィックはIPv4の1/1000未満
- 接続先(コンテンツサーバ)のIPv6対応が必要
- コンテンツサーバがIPv6対応するためには、IPv4と同程度以上のアクセス品質が必要
- そのためにはISPのIPv6対応が必要

神話: IPv4アドレスは 枯渇する

- IPv4アドレス在庫はあと数年で枯渇する
- これは10年前からほぼ正確に予想されていた



現実: IPv4アドレスは市場 モデルに移行する

- IPv4アドレスは市場モデルに移行する
 - 既に多くのRIRで決定されつつある
 - レジストリーはアドレス割当てから権限付与へ
- 市場モデルでは、アドレスの需要が高まるほど、
アドレスの価格が高騰するだけ
 - 枯渇は無い

神話: IPv6移行は簡単

- 主要なOSはIPv6対応を完了させている
 - Linux, *BSD, Windows, MacOSX, Solaris,...
- ネットワーク機器もIPv6対応は昔からやっている
- 特に法人向けにはIPv6接続サービスを展開しているISPもある

現実: サーバ側の対応はIPv6アドレスを設定するだけではない

- DNSラウンドロビンによるロードバランスが利用できません
- IPv6ロードバランサはようやく出始めた程度
- バックエンドシステムは大丈夫か？
 - ロギングシステム
 - cookieにIPアドレス埋め込んだりしてるところも
- IPv6アドレスの地理情報がまだ実質存在しない

神話: ルータのIPv6対応

- ほぼ対応は終わっているが、100%ハードウェア処理ではない
 - 特にACLを追加した場合
- 全てのベンダーがASIC処理に邁進しているわけではない
- 全てのIPv4機能がサポートされているわけではない: MIB, SNMP over IPv6

神話: IPv6はIPv4のアドレス 空間が広がっただけ

- 結局、IPv6の新機能には期待できない
- ならば、IPv4のアドレス空間が広がっただけだと思えばいい

現実: IPv6とIPv4は細かいところの違いが潜む

- 途中経路でのフラグメント禁止
 - PMTU問題の発生に注意
- DNSラウンドロビンによるロードバランスが動作しない
- UDPのチェックサムが必須
 - IPv4-IPv6トランスレータに負荷がかかる
- DHCPでdefault routeを配れない
- NATは設計思想的にNG
 - 実装は広く普及してはいない

つまるどころ

“96ビット増えても魔法は起こらない”

Gaurab Raj Upadhaya

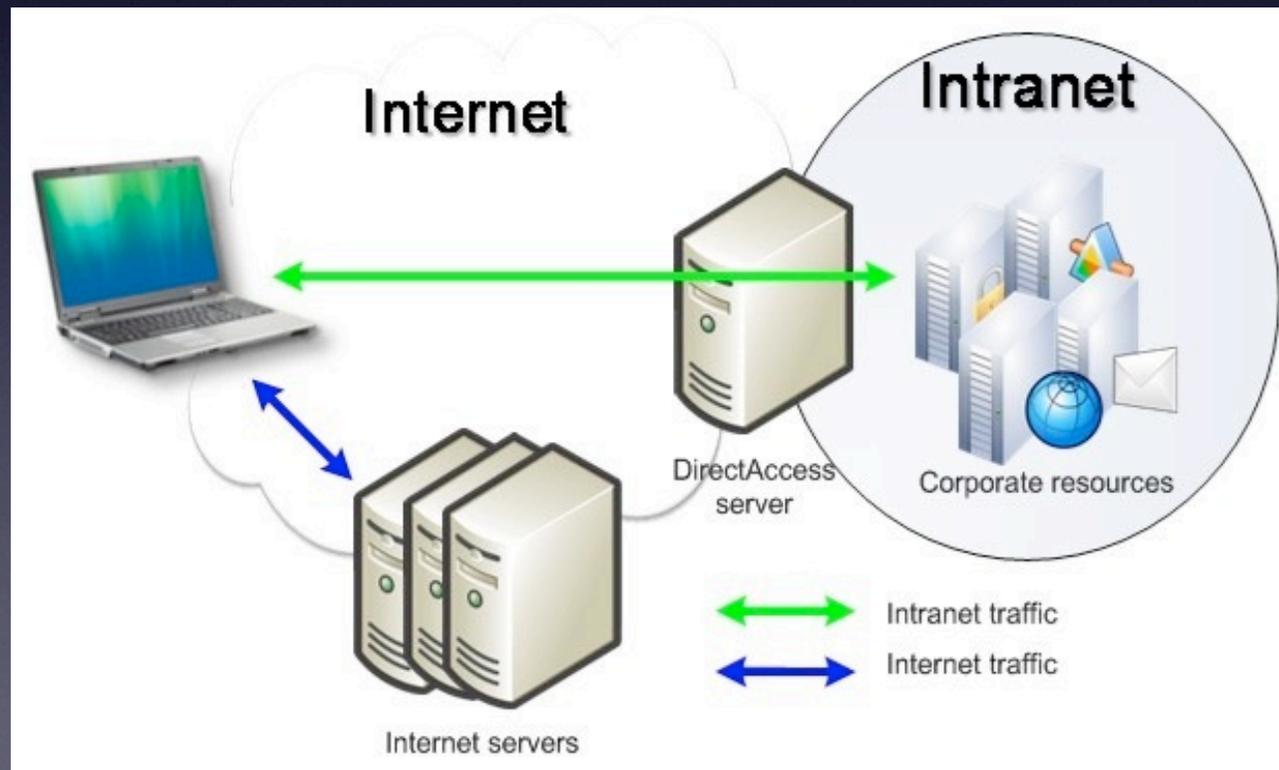
神話と現実を踏まえて

今どうするか？

- IPv4アドレスは枯渇／高騰する
- IPv4接続性の提供／取得は高騰する
 - IPv4アドレス市場における価格高騰
 - ロードバランサ、CGN等の導入によるコスト高
 - 帯域制限、セッション数制限によるコスト高
- 必要なIPv4/IPv6数を見積もって、コストと共にプラン検討を
- そのためにはIPv4延命策、IPv6移行方式についての知識が必要
 - また、他社のIPv6導入事例などの情報収集も必要

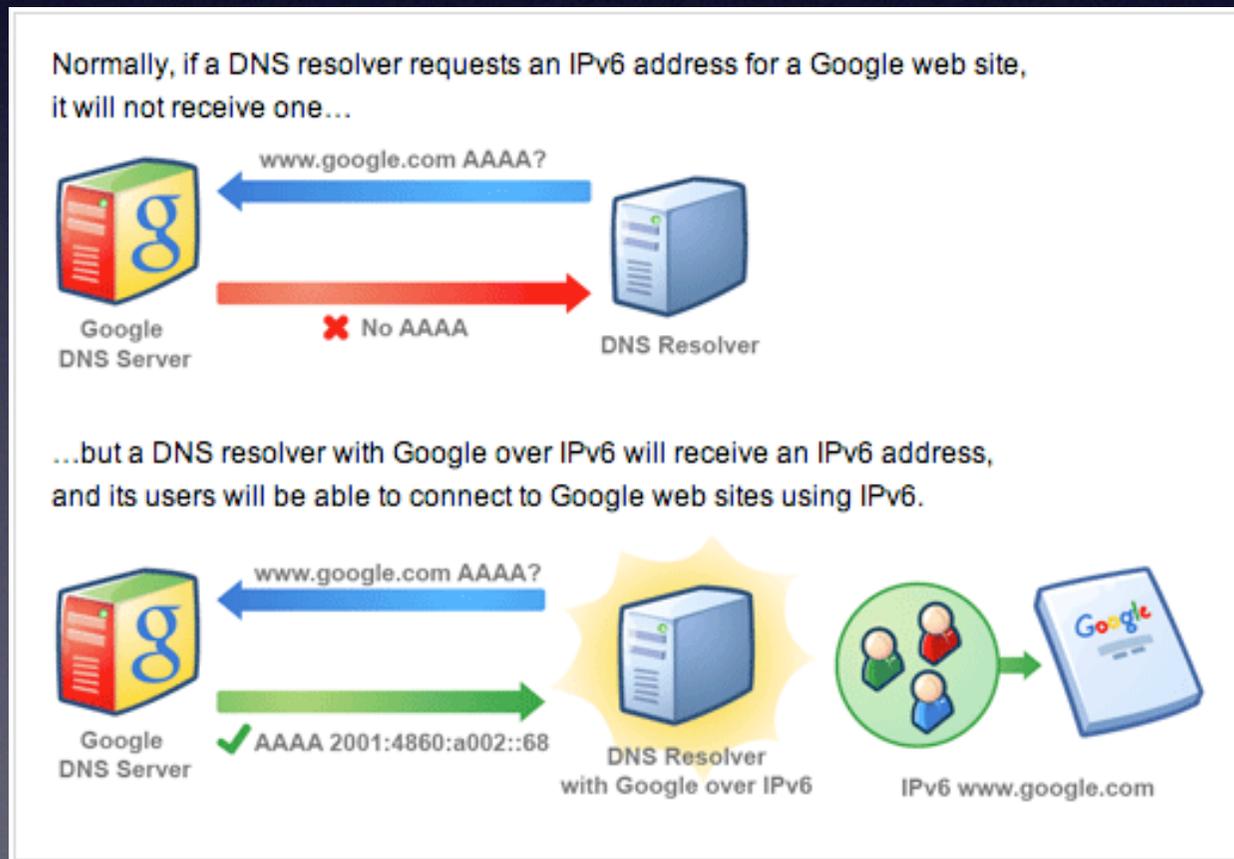
Direct Access

- IPv6+IPsecを用いたリモートアクセス方式
Windows7+WindowsServer2008R2で利用可能



GoogleのIPv6対応

- ホワイトリストを用いてサービス品質低下を防止
- 優れたIPv6回線を持つ相手へのみIPv6接続許可



参考文献 / 引用元

- Randy Bush, “IPv6 Transition & Operational Reality”, IEPG, July 2007.
- “Microsoft Direct Access”, <http://blogs.technet.com/ieitpro/archive/2009/03/22/directaccess-in-windows-server-2008r2-and-windows7.aspx>
- “Access Google services over IPv6”, <http://www.google.com/intl/en/ipv6/>
- “実践！ IPv6ネットワーク構築”, Internet Week 2008