RICOH

企業におけるIPv6ネットワーク利用

2003年12月2日

（株）リコー　マルチメディア研究所

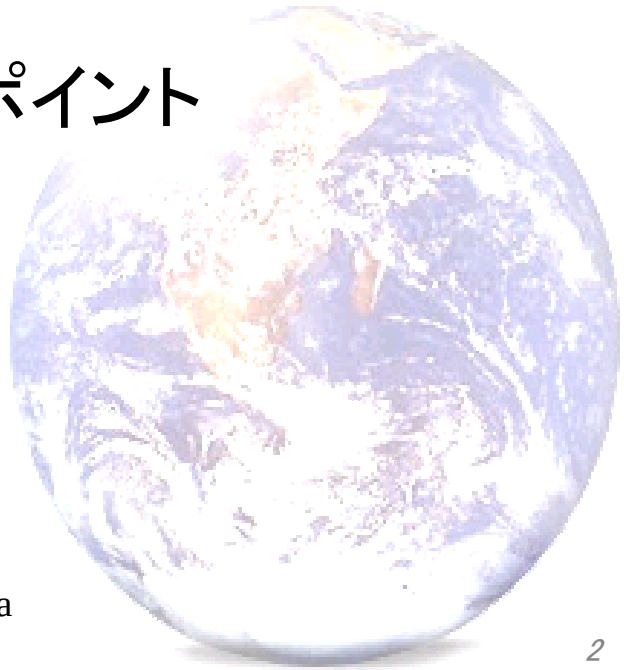
西田　明宏

nishida@src.ricoh.co.jp

目次

RICOH
Image Communication

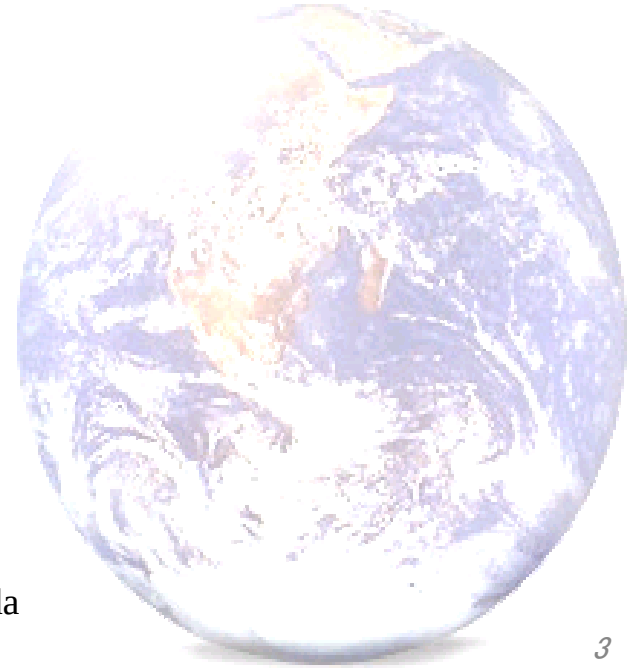
1. IPv6開発動機の振り返りと現状
2. 企業ネットワークのIPv6対応の意義
3. IPv6技術の標準化動向
4. IPv6関連製品の商品化状況
5. IPv6技術のおさらい
6. 企業ネットワーク移行の検討ポイント
7. 移行事例紹介
8. まとめ



IPv6開発動機の振り返り

RICOH
Image Communication

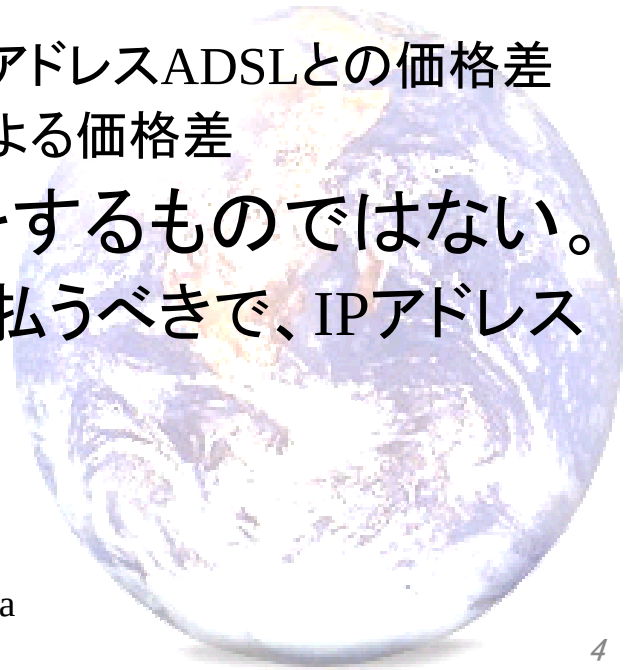
- IPv6開発の動機
  - インターネットの普及に伴うIPv4アドレスの枯渇予想
  - 「どうせ作り直すのならば、IPv4の使いづらい部分を再設計しよう」



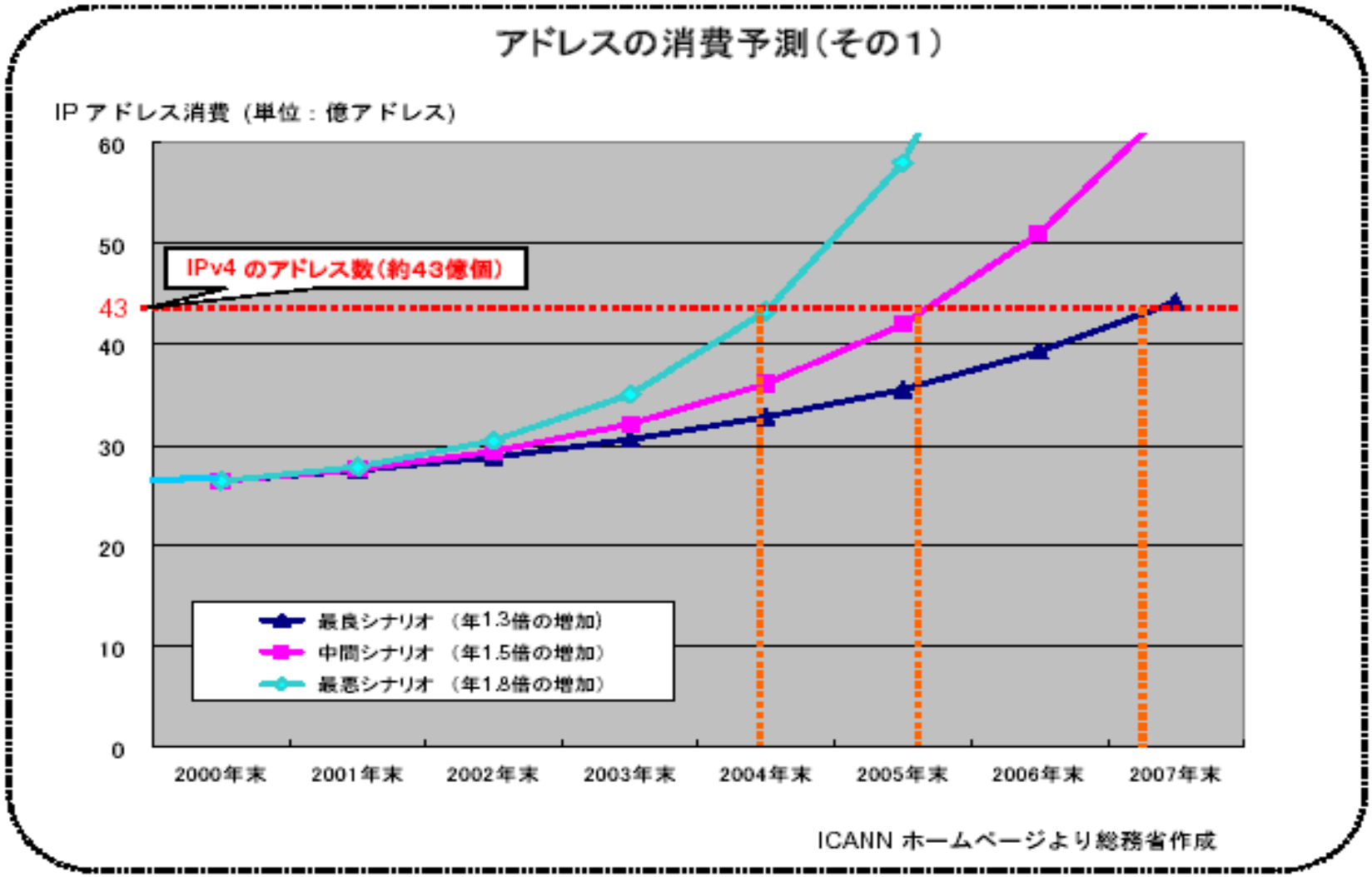
IPv4アドレスの枯渇予想

RICOH Image Communication

- IPv4アドレスの枯渇は遠のいた
  - CIDR、プライベートアドレスの導入
  - NAT技術の普及
  - IPv4グローバルアドレス割り当ての厳格化
- 現在、IPv4アドレスは実質的に有料
  - 例:
    - ダイナミック割り当てADSLと固定IPアドレスADSLとの価格差
    - 企業向けサービスのIPアドレス数による価格差
- しかし、本来IPアドレスに課金をするものではない。
  - お客はネットワーク帯域にお金を払うべきで、IPアドレス空間にお金を払うべきではない。

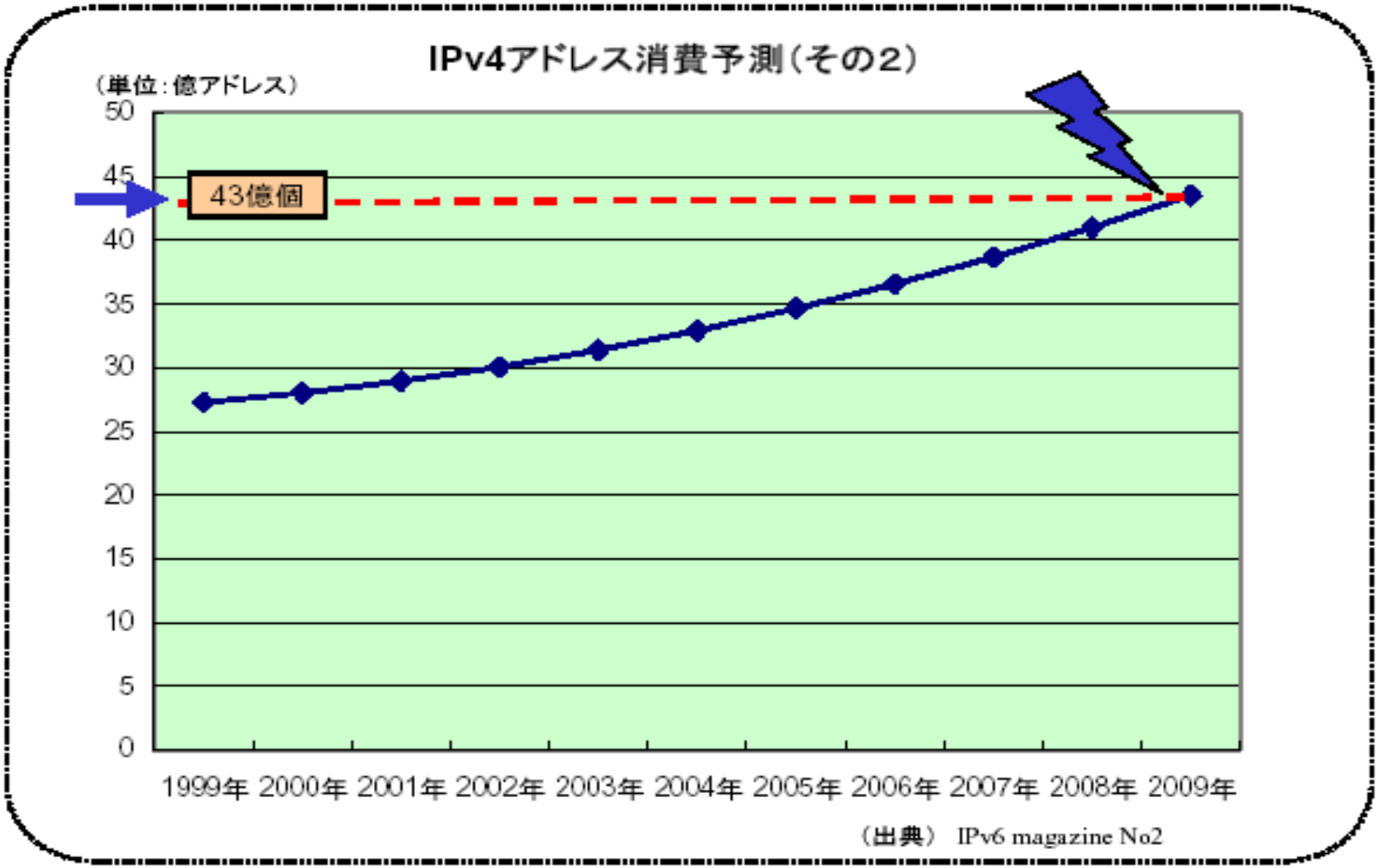


IPアドレス消費予測

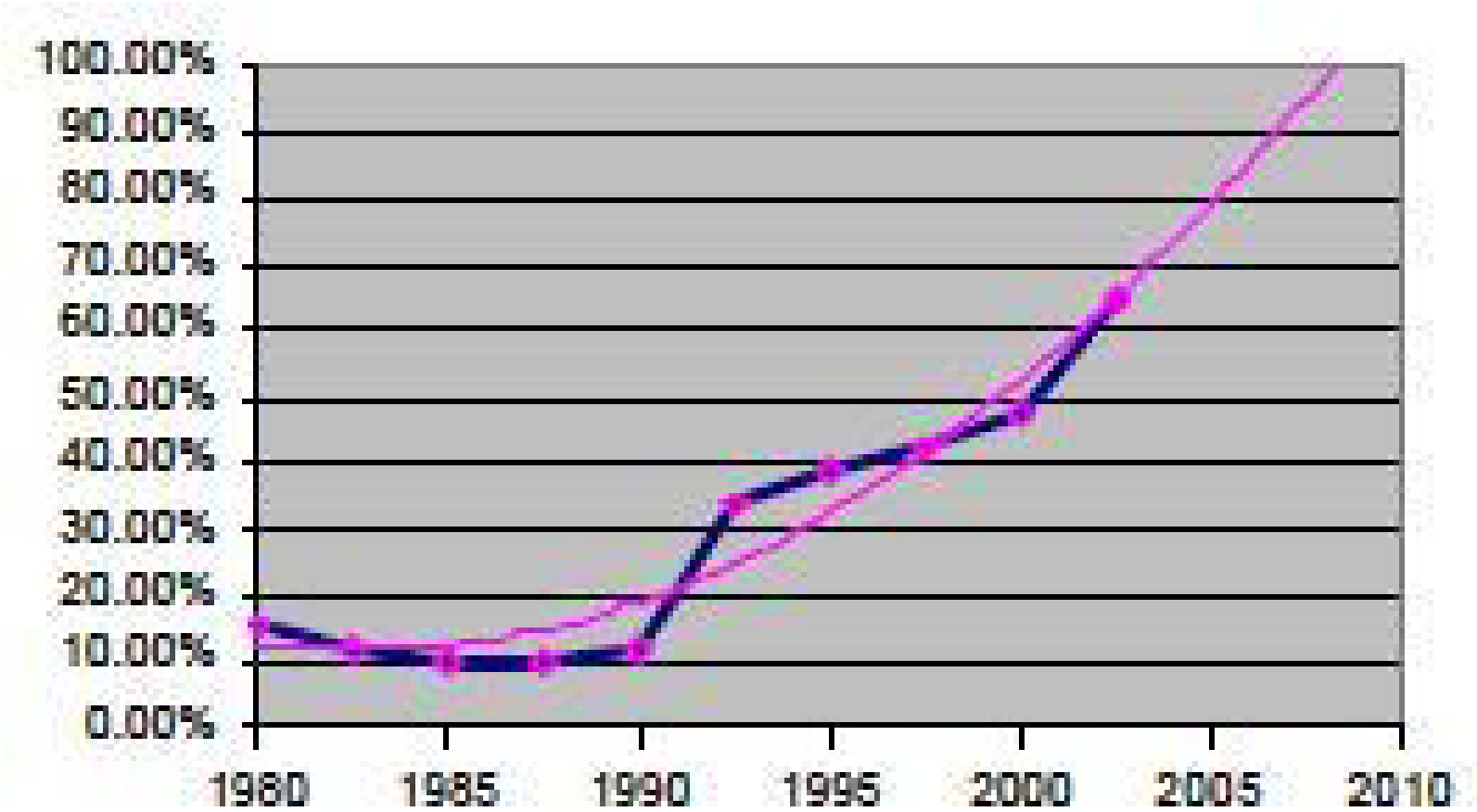


出展：総務省　http://www.soumu.go.jp/s-news/2002/020807_17.html

IPアドレス消費予測



IPアドレス消費予測

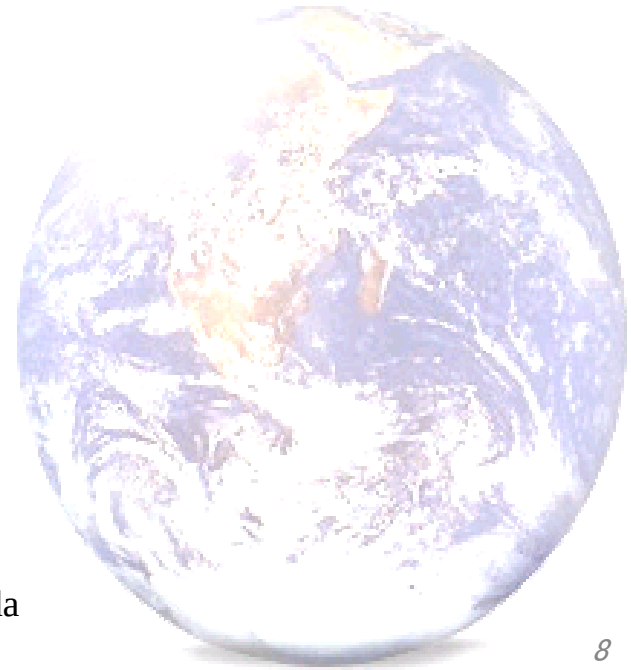


Cisco Systems K.K, Networkers 2003, IPv6 Workshop資料より

インターネット技術の作り直し

RICOH
Image Communication

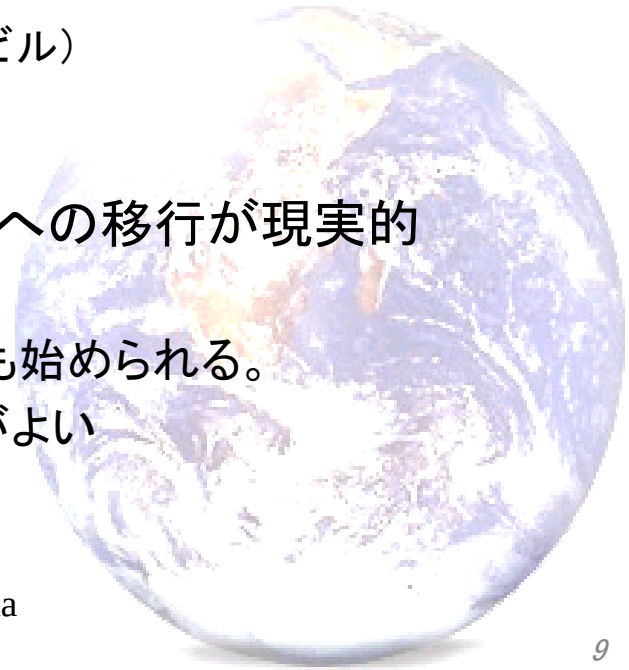
- どうせ作り直すのならば、IPv4で不便な点を再設計してしまおう。
  - IPアドレスの自動設定
  - Path MTU
  - IPSecの必須化
  - Mobile-IP
  - Multicast



企業ネットワークのIPv6対応の意義

RICOH Image Communication

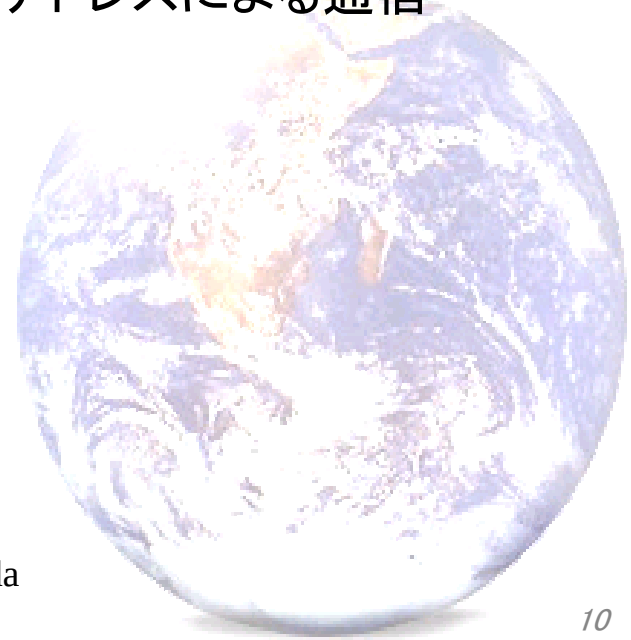
- 2003年末の現在、企業ネットワークをIPv6対応する意味は？
  - パソコンを使用したWeb/Mailの利用目的だけならば、移行する意味は、さほどない。
- ではずっとIPv4ですむのか
  - 各種予測によれば、遅くても2008年には移行が必要となる。
- それではどこに意義を見出す？
  - 近未来のIPアドレス枯渇対策
  - 新規アプリケーションのため
    - ビル管理デバイスのIP化（松下電工汐留本社ビル）
    - SIP, VoIPの利用
    - IPSec、Mobile-IPの利用
- 当面はIPv4とのデュアルスタックネットワークへの移行が現実的
- 移行には時間がかかる。
  - IPv6利用ノウハウ蓄積・技術評価はすぐにでも始められる。
  - 移行準備はできるだけ早く取り掛かったほうがよい



IPv6技術の標準化動向

RICOH Image Communication

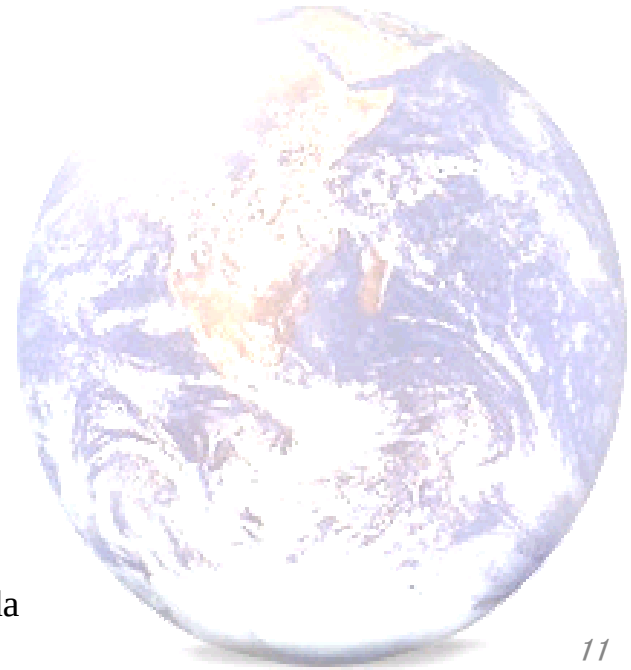
- IPv6技術の標準化はどうなっているか？
  - IETFにて議論は依然進行中
  - 通常の使用に必要な技術はだいたいReadyとなっている。
  - ほぼ固まっているもの
    - EUI64によるアドレス自動設定
    - リンクローカル/集約可能グローバルアドレスによる通信
      DHCPv6もほぼFixし、実装待ち
    - ISPサービスに必要な技術
  - まだ固まっていないもの
    - サイトローカル(相当)のアドレス
    - DNS自動設定
    - その他の技術
      - マルチホーム技術等



IPv6関連製品の商品化状況

RICOH Image Communication

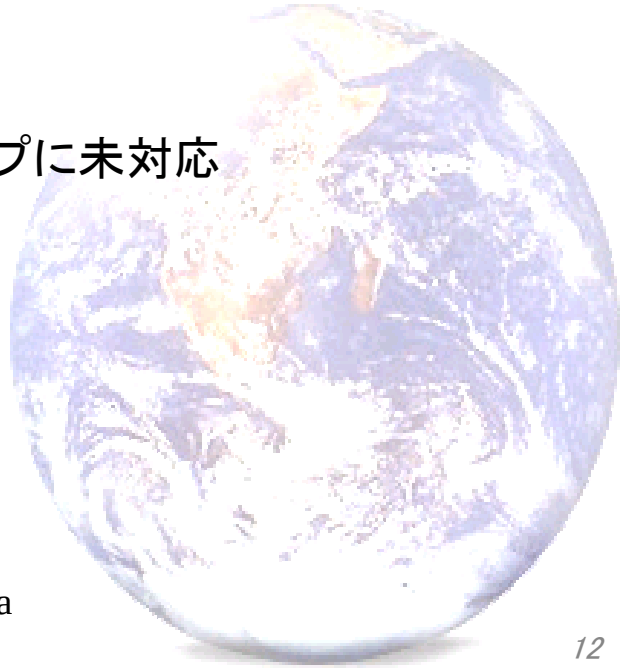
- ハードウェア
  - 主要なパーツは揃いつつある。
  - しかし、選択肢には乏しい
  - ISP
    - (日本では)OK
    - IPVPNは未対応(トンネリングで回避は可能)
    - ダイアルアップは未対応
  - ルーター
    - 大規模ルーターはOK
    - ブロードバンドルーターは一部OK
  - プリンタ
    - プリンタサーバーが1機種のみ
  - ファイアウォール
    - ルーターによるパケットフィルタリング
    - Firewall-1、NetScreen
  - NAS
    - 未対応



IPv6関連製品の商品化状況

RICOH Image Communication

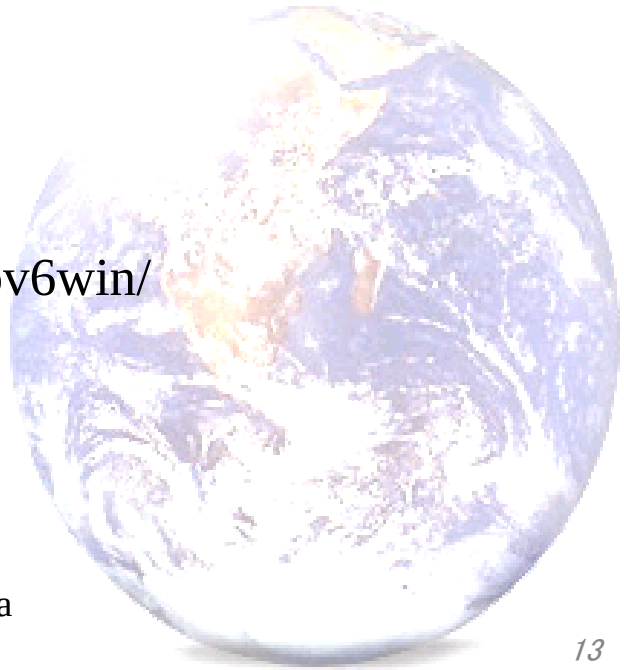
- ソフトウェア
  - こちらも主要な機能は揃ってきた
  - しかし、選択肢はハードウェア同様乏しい
    - フリーソフト(+IPv6パッチ)のみというケースも多い
  - まだ対応製品がない分野も多い
  - OS
    - ほとんどのOSでOK(Windows XP, Mac OS X, Linux, *BSD, Solaris, HP-UX, …)
  - DNSサーバー
    - BIND9
    - ほとんどのOSがIPv6でのDNSルックアップに未対応
  - DHCPサーバー
    - ルーター組み込み
    - サーバー用の実装はこれから
  - Webサーバー
    - Apache 2.0



IPv6関連製品の商品化状況

RICOH Image Communication

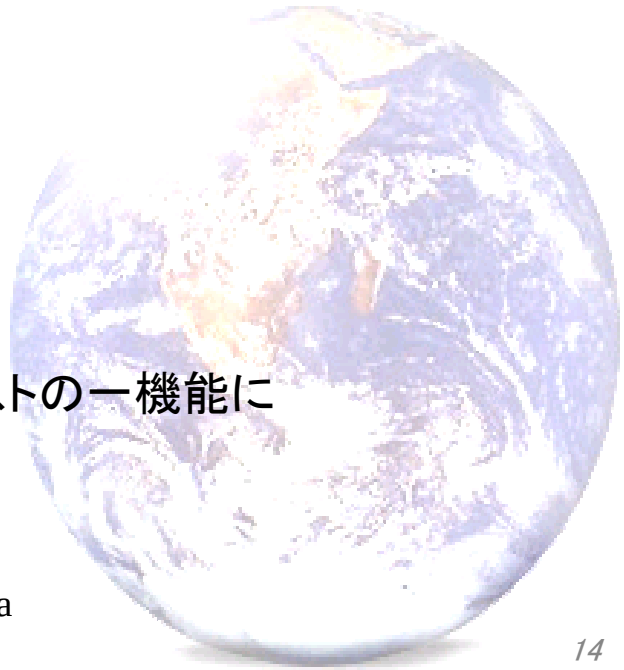
- Webブラウザ
  - IE
- メールサーバー
  - イー・ポスト　SPA-PRO　(http://www.mps.ne.jp/com/e-post/)
- メールクライアント
  - Winbiffくらい？
- グループウェア
  - 未対応
- セキュリティ関連ソフト(ウイルス対策)
  - 未対応
- Windows上のIPv6対応ソフトウェア
  - http://www.ipv6style.jp/jp/statistics/ipv6win/



IPv6技術のおさらい

RICOH Image Communication

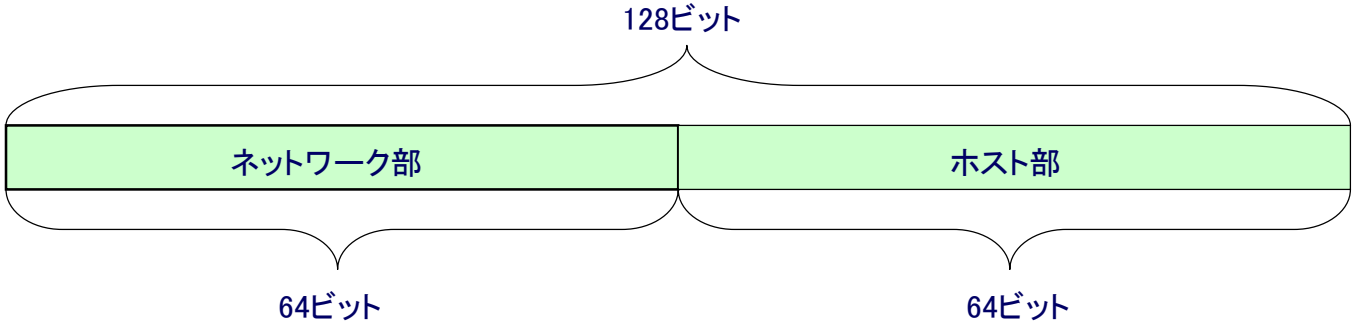
- アドレスの種類
  - IPv4
    - ユニキャストアドレス
      - 旧クラスA,B,C
    - マルチキャストアドレス
      - 旧クラスD
    - ブロードキャストアドレス
  - IPv6
    - ユニキャストアドレス
    - エニーキャストアドレス
    - マルチキャストアドレス
      - ブロードキャスト機能はマルチキャストの一機能に



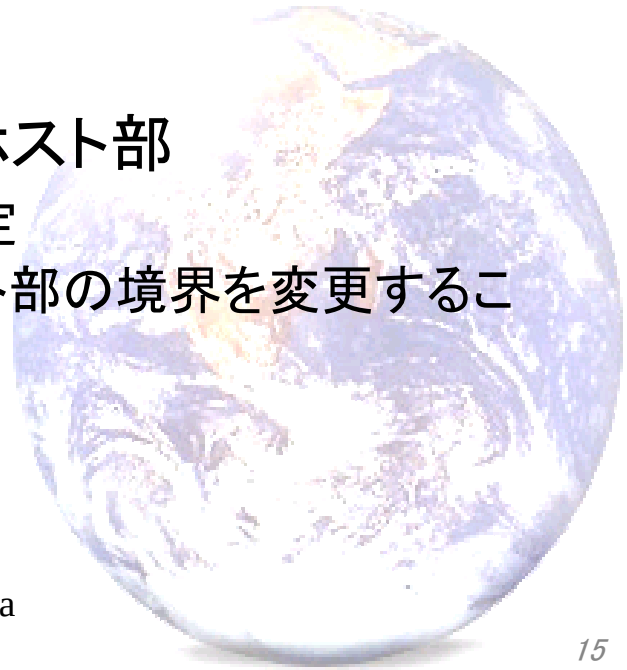
IPv6ユニキャストアドレス

RICOH Image Communication

- IPv6アドレス
  - IPv4の32ビットから128ビットへ



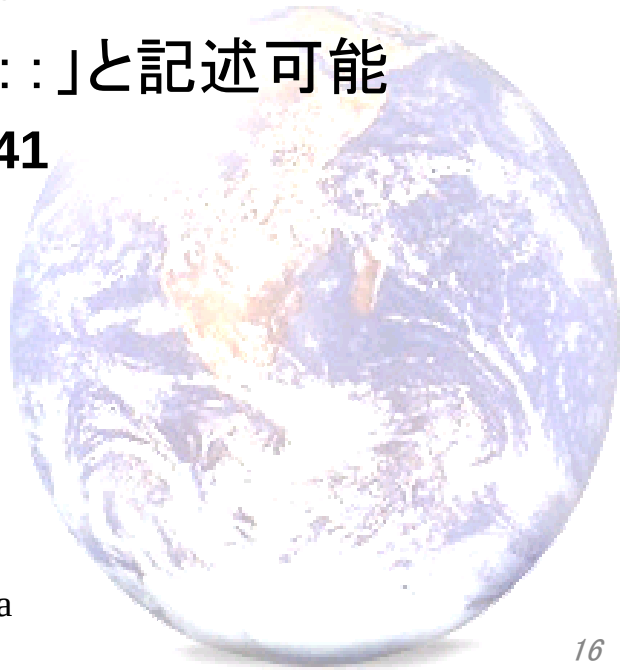
  - 64ビットネットワーク部、64ビットホスト部
    - ネットワークとホストのビット数は固定
    - IPv4のように、ネットワーク部とホスト部の境界を変更することはできない
      - ネットマスクを設定する必要はない



IPv6アドレスの表記法

RICOH Image Communication

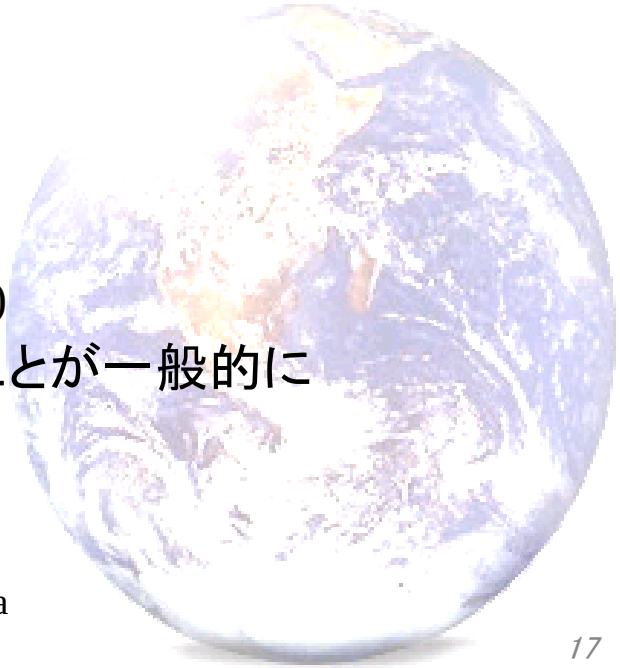
- アドレス表記法
  - 16ビット毎に区切って16進数で表現し、コロンでつなげる。
    例) 2031:0000:130F:0000:0204:76ff:fe9c:c041
  - 各パートの先頭の0は省略可能
    例) 2031:0:130F:0:204:76ff:fe9c:c041
  - 0の連続する部分は一箇所のみ「::」と記述可能
    例) 2031::130F:0:204:76ff:fe9c:c041



IPv6ユニキャストアドレスの種類

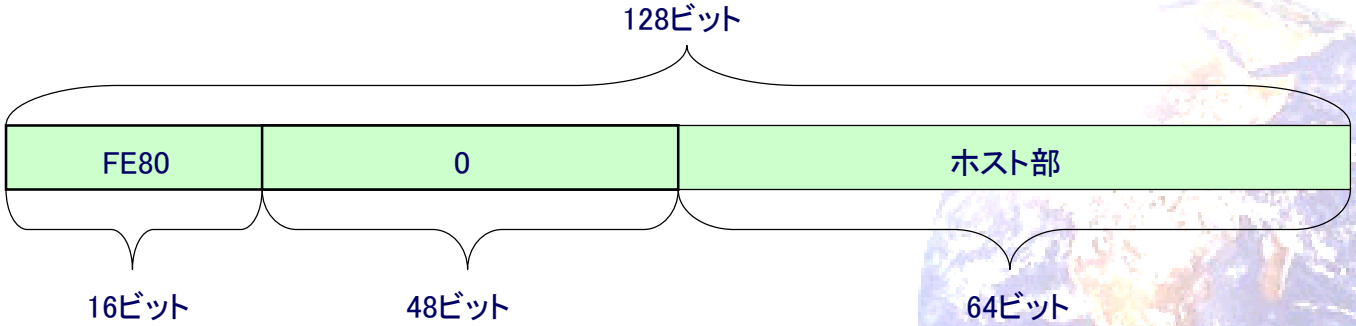
RICOH Image Communication

- IPv4では?
  - いわゆるIPアドレス
  - ループバックアドレス(127.0.0.1)
  - その他、マルチキャストアドレスを振ることができたり、複数のIPアドレスを振ることはできたが、通常の端末では、それほど一般的ではない。
- IPv6では？
  - まずリンクローカルアドレス
  - 集約可能グローバルアドレス
  - その他のアドレス
    - プライバシーアドレス
    - サイトローカルアドレスは使わない（後述)
  - 複数のユニキャストアドレスが振られることが一般的に



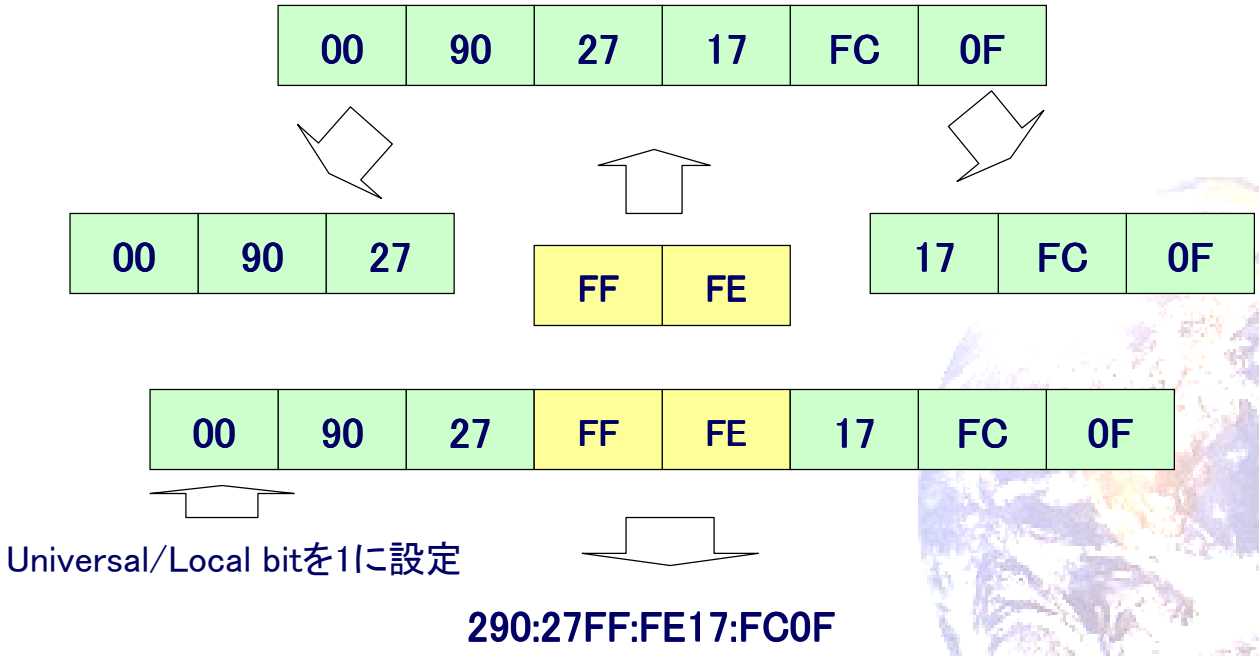
リンクローカルアドレス

- リンクローカルアドレス
  - 接続されたセグメント内でのみ利用可能なアドレス
  - 通常はIPアドレス自動設定等のために用いられる。



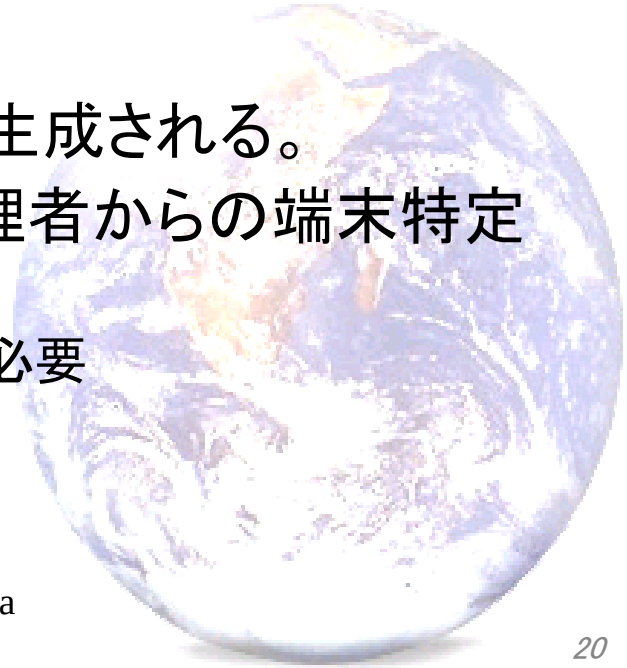
ホスト部のアドレスの振り方

- EUI-64
  - Ethernet等で利用されているMACアドレスから自動生成



ホスト部のアドレスの振り方

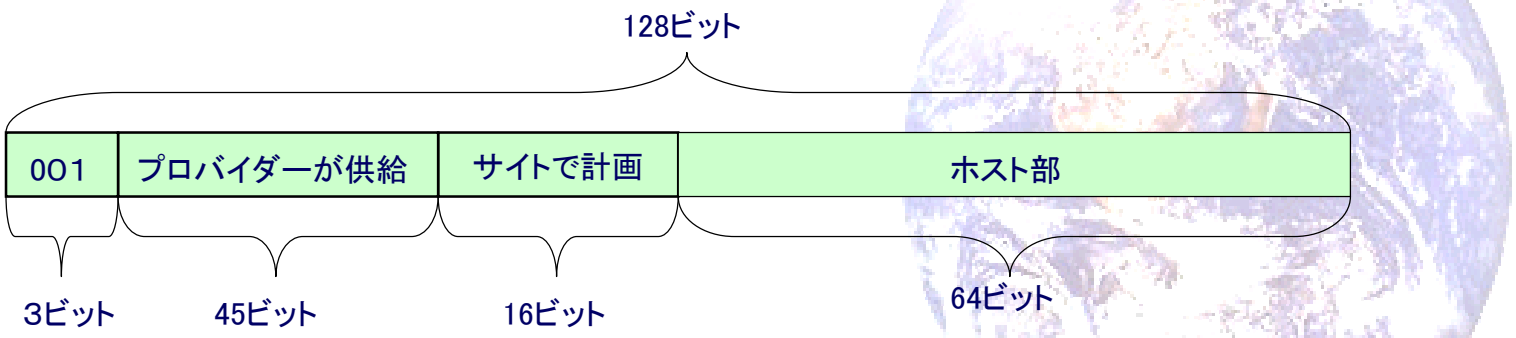
- スタティックに設定
  - ポート番号にあわせる
    - WWWサーバー → 例）2001:240:2c::80
  - 覚えやすいアドレスを振る
    - 例）2001:240:2c::CAFE:CAFE:CAFE
- プライバシーアドレス
  - RFC3041
  - 毎回異なるホスト部のアドレスが生成される。
  - 家庭ではよいが、組織の場合管理者からの端末特定が難しくなる弊害も
    - 使ってよいことにするかルール化が必要



集約可能グローバルユニキャストアドレス

RICOH Image Communication

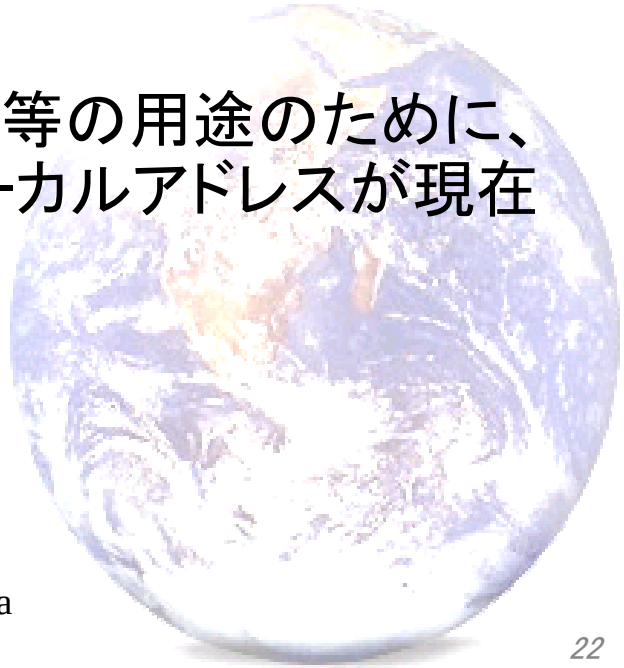
- アドレスの先頭48ビットはプロバイダーから入手
  - ADSL接続等では、先頭64ビットがプロバイダーから指定される場合もある。
- 続く16ビットがサイト内でのサブネット用
  - 65536サブネットを構成可能
  - といっても、現IPv4プライベートアドレスの総数(/24での換算)よりは小さい
  - この部分の設計が重要



現行のサイトローカルは廃止へ

RICOH Image Communication

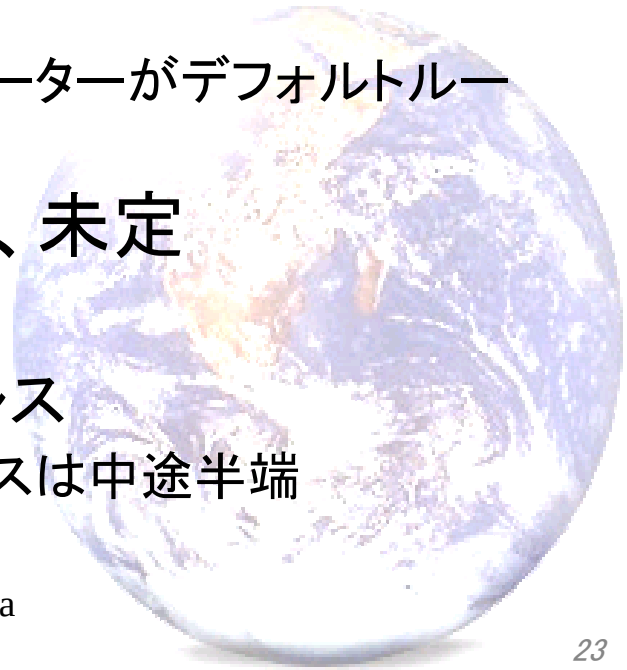
- 現在RFCにはサイトローカルアドレスが定義されている。
  - FEC0:/10
  - しかし、IETFでの議論において、廃止されることがほぼ決定。
  - 「サイト」の定義のむずかしさ、2つの「サイト」の境界ルーターの扱い、NATの利用を促進等の問題のため。
  - 現在RFCの改定作業中
- 現在の各種OSの実装では利用可能の場合があるが、利用しないほうがよい。
- ただし、プロバイダーに接続前に使う等の用途のために、グローバルにユニークな新サイトローカルアドレスが現在検討中



IPv6ホストの自動設定

RICOH Image Communication

- IPv6ホストの各種設定は、通常自動設定される。
  - リンクローカルユニキャストアドレス
    - EUI-64より自動生成
  - 集約可能グローバルユニキャストアドレス
    - EUI-64およびルーターからのRAメッセージ（あるいはホストからのRSメッセージ）により自動生成
  - デフォルトルーター
    - 受け取ったRAメッセージを出したルーターがデフォルトルーターになる。
- DNSサーバーの自動設定のみ、未定
  - DHCPv6-Liteによる設定
  - Well Known エニーキャストアドレス
    - Windows XPのエニーキャストアドレスは中途半端

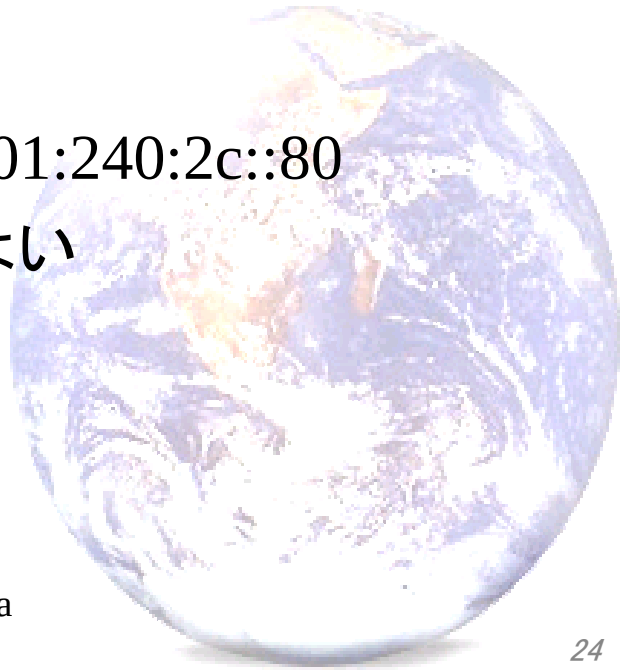


DNSサーバーの設定

- 正引きの設定
  - IPv4
    - Aレコード

      www　　IN A　　210.227.75.169
  - IPv6
    - AAAAレコード

      www　　IN AAAA　2001:240:2c::80
    - A6レコードは使わないほうがよい



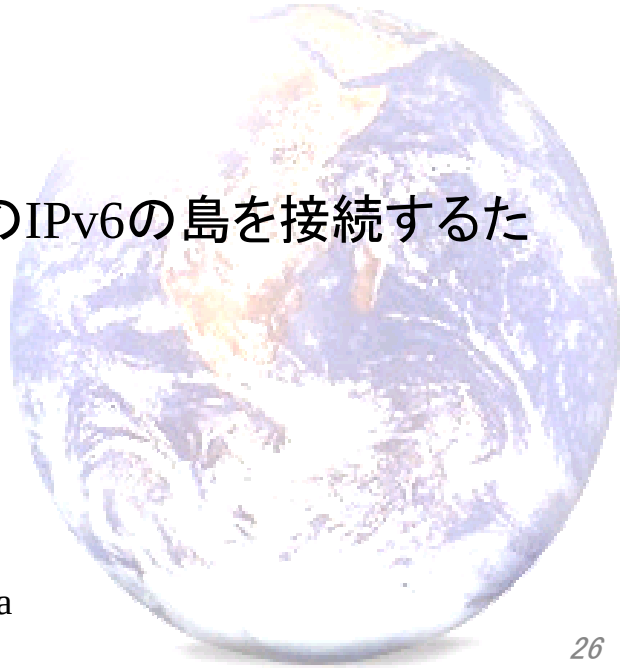
DNSサーバーの設定

- 逆引き
  - IPv4
    - inaddr.arpaドメイン
    - 169.75.227.210.in-addr.arpa　　IN　PTR www.ricoh.co.jp
  - IPv6
    - ip6.arpaドメイン
    - ip6.intは過去の互換性のため、設定しておくと良い
    - 0.8.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.c.2.0.0.0.4.2.0.1.0.0.2.ip6.arpa　　IN PTR www.example.co.jp

IPv6トンネリング技術

RICOH Image Communication

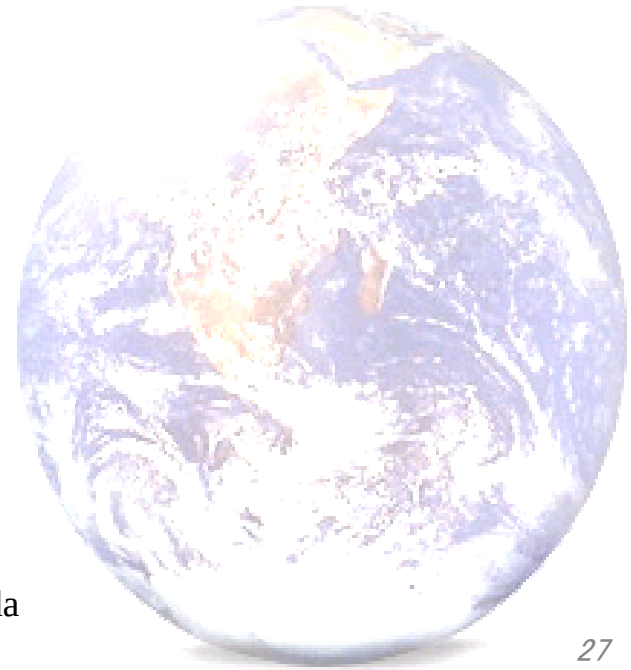
- 各種トンネリング技術
  - スタティックトンネリング
    - 企業の移行の過程では重要
  - 6to4
    - RFC3053で定義
    - 基本的にはIPv4グローバルアドレスをひとつ持つ小規模サイトを対象
    - www.6to4.jp
  - ISATAP
    - IPv4による大規模サイト内の、複数のIPv6の島を接続するための技術
  - Teredo
    - UDPを利用したトンネリング技術



企業ネットワーク移行の検討ポイント

RICOH Image Communication

- IPv4/IPv6デュアルスタックへの移行を考える。
  - ここ数年は、IPv6のみのネットワークは非現実的
  - 特にサーバーをデュアルスタック構成に
  - もちろん、特殊専用用途のためのネットワークならばIPv6のみも有りうる
    - ビルの機器管理
    - 工場内部の機器コントロール



サブネット構成の考え方

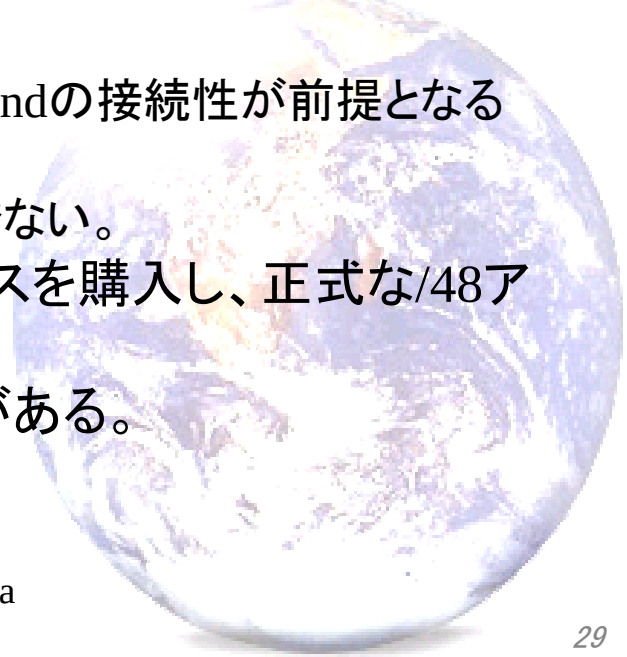
RICOH Image Communication

- IPv4のネットワークセグメント構成に合わせる。
  - IPv4とのデュアルスタック構成を前提とすると、IPv6にて接続可能ホスト数が増えるからといって、セグメント集約は考えないほうがよい。
  - 現在のIPv4ネットワーク数が65536以下ならば、/48の単一ネットワークでまかなうことが可能
    - それ以上ある場合は、複数の/48をプロバイダーからもらうことになる。
    - サブネット用に使える、/16の使い方を検討する。
      - 厳密な集約の必要はないが、ネットワークトポロジーにしたがって有る程度の集約は考慮すべき。

IPv6アドレスの選択

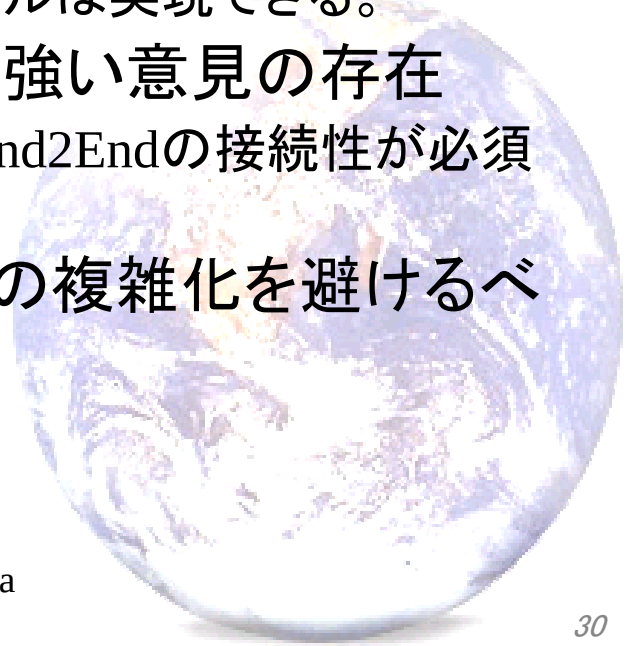
RICOH Image Communication

- どのIPv6アドレスを使うか
  - IPv4の時代の感覚で、組織内はサイトローカル、インターネットとの境界で集約可能グローバルアドレスに変換、としたくなるところだが、これは間違い。
  - 現行サイトローカルアドレスは廃止が決まっており、グローバルユニークなサイトローカルアドレスの導入が議論されているが、使えるとしてもまだ先。
  - イントラネットでも、IPv6のグローバルアドレスを振ることを前提とすべき
    - 今後のIPv6アプリケーションは、End to Endの接続性が前提となる可能性が高い。
    - 現行サイトローカルアドレスは使うべきでない。
  - 理想的には、まずISPからIPv6のサービスを購入し、正式な/48アドレスを入手するのがベスト
  - だめならば、6to4のアドレスを使う方法がある。



NATの利用について

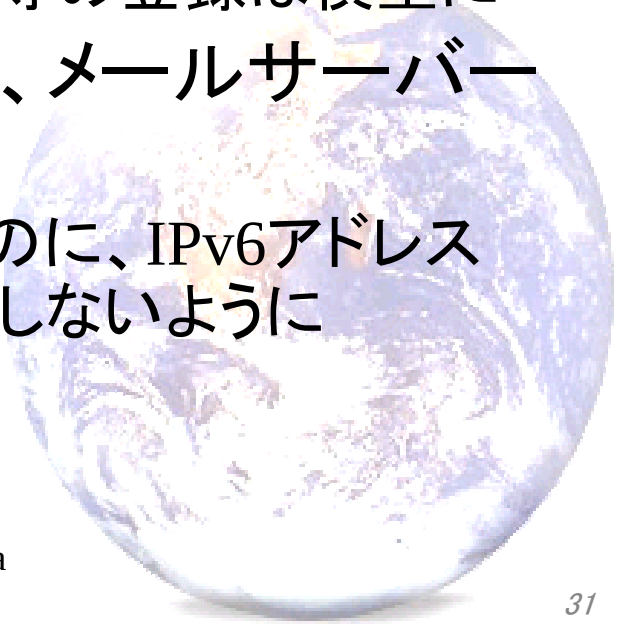
- IPv6ネットワークでのNAT（NAT-PT)の利用は慎重であるべき
  - NATを使う積極的理由はない。
    - アドレスの数は足りている。
  - NATでセキュリティが守れる、という意見もあるが完全ではない。
    - NATなしでも同等のセキュリティレベルは実現できる。
  - NATの利用を避けるべきという根強い意見の存在
    - 将来のキラーアプリケーションではEnd2Endの接続性が必須となるかもしれない。
  - NAT利用によるネットワーク構成の複雑化を避けるべき



DNSサーバー設定の注意点

RICOH Image Communication

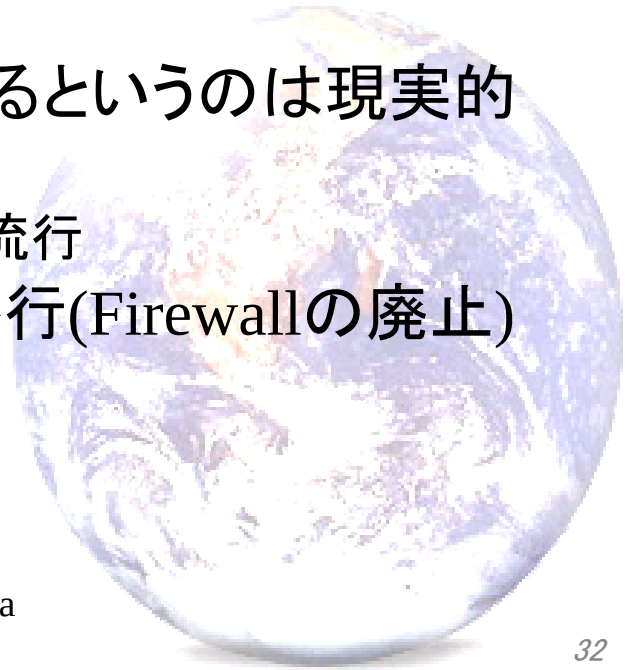
- 登録するのは、集約可能グローバルアドレスのみに
  - リンクローカルは登録しない
  - サイトローカルの使用そのものを薦めないが、もし利用した場合は、インターネットから参照可能なDNSツリーには登録しない。
  - その他、トンネリング用のアドレス等の登録は慎重に
- MXレコードを設定するときには、メールサーバーをデュアルスタックにしてから
  - SMTPはIPv4でしか利用できないのに、IPv6アドレスを引けるホスト名をMXとして登録しないように



セキュリティモデルの検討

RICOH Image Communication

- セキュリティ
  - 玄関モデルと金庫モデルの組み合わせで考える
  - 玄関モデル
    - Firewall等の機器を、サイトの境界に置くことでサイト内部の機器を守る。
  - 金庫モデル
    - サイト内の機器個々で守る。
  - 玄関モデルでセキュリティが守れるというのは現実的でなくなってきている。
    - 昨今の各種コンピュータウイルスの流行
  - もちろん、金庫モデルへの完全移行(Firewallの廃止)というのも非現実的



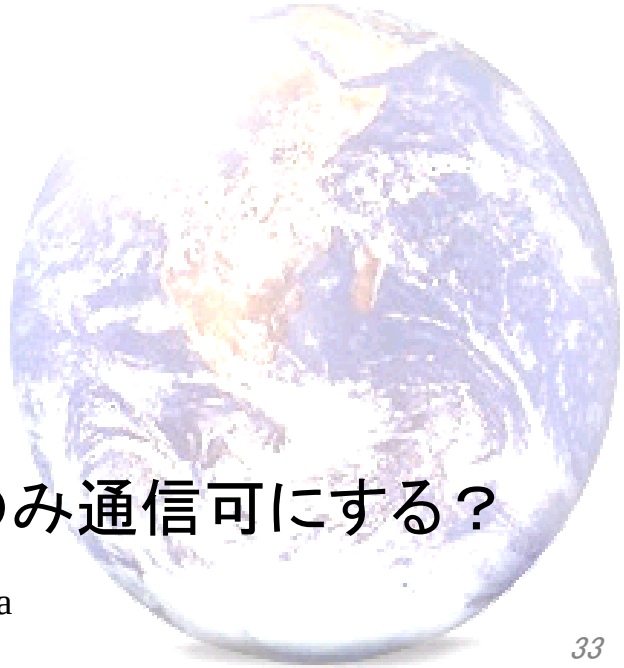
セキュリティ設定における注意点

RICOH Image Communication

- ICMPv6のフィルタリング
  - IPv6ネットワークでは、すべてのICMPv6をフィルタリングするのは危険

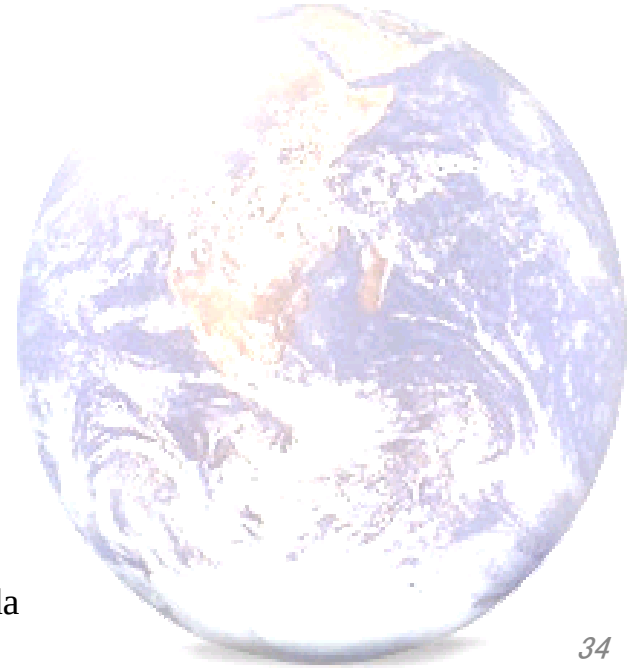
    例）Path MTUディスカバリが利かない

    → 通信の不安定化
- IPSecによる対外通信は企業で使えるか?
  - IPSecには2つの機能がある。
    - AH(Authentification Header)
      - 通信元のアドレスの認証
    - PS（Payload Security)
      - パケットの内容が暗号化
      - パケット中のデータ検査が利かない
      - 慎重な検討が必要
  - IPSecによる通信を認めるホストのみ通信可にする？

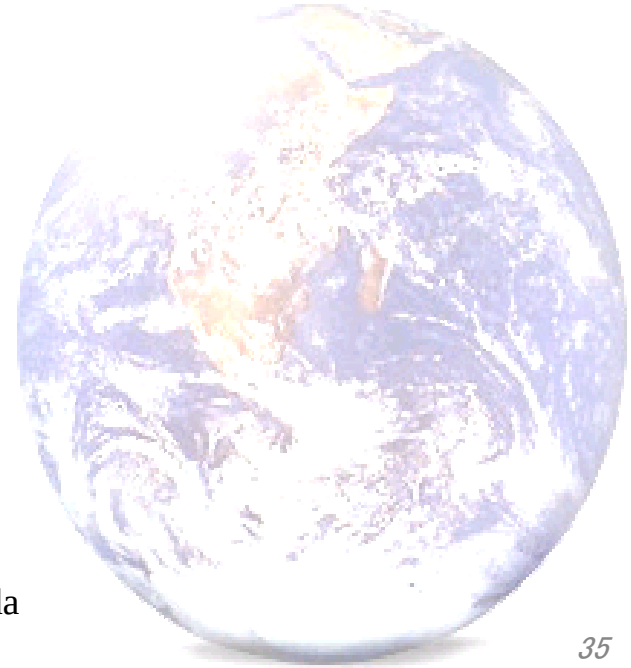


RICOH
Image Communication

IPv6への移行の考え方

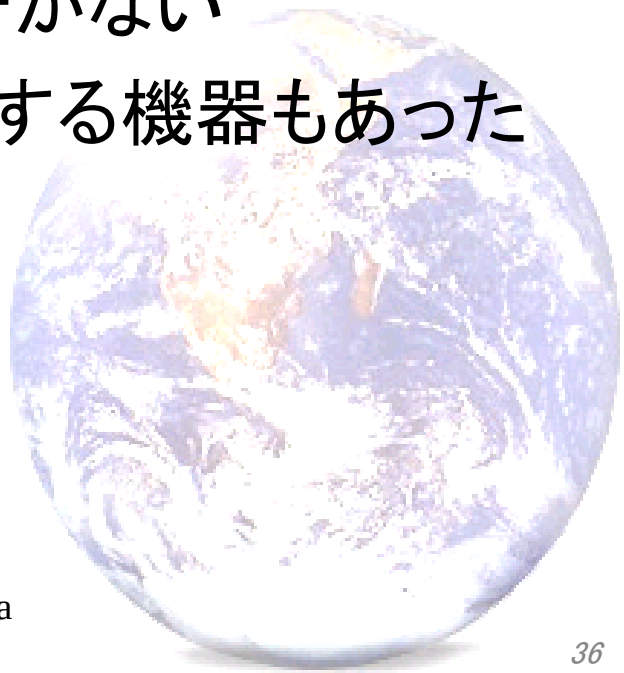


移行事例紹介



電通国際情報サービス(ISID)

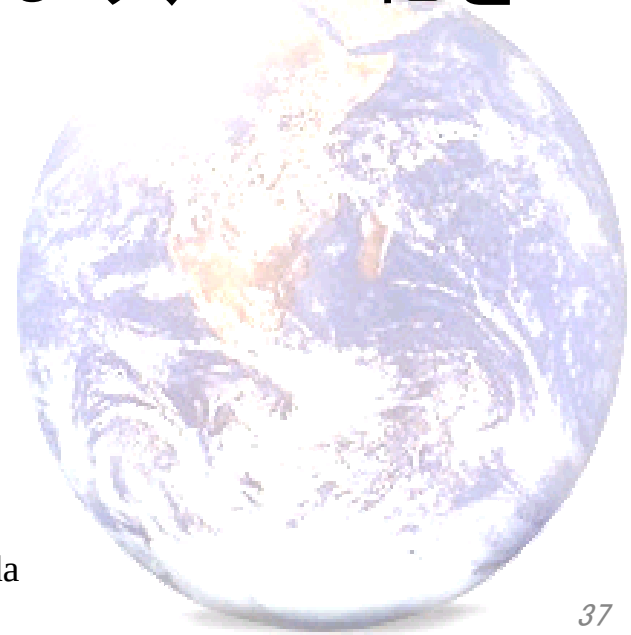
- 2001年の、全社の通信機器のリース切れによる入れ替えを期に、IPv4/IPv6デュアルスタックに移行
- 先行事例ならでの苦労・トラブルも
  - IPv6で利用可能なL3スイッチがない
  - IPv6パケットを流すと誤動作する機器もあった



IPv6非対応ルーター環境でのIPv6対応

RICOH Image Communication

- 某社の研究所における事例
- 事業所の主ルーターがIPv6非対応
  - 最新版にアップグレードすればIPv6利用可能だが、アップグレード費用が千数百万！
- IPv6対応ルーターの増設により、IPv6化を実施



まとめ

- IPv6に対応しなければいけない時代は、ここ数年のうちに必ずやってくる。
- まだ十分ではないが、IPv6化するための一通りの機器・ソフトウェアは揃ってきた。
- ここ数年から十数年はIPv4とIPv6のデュアルスタック環境が必要
- スムーズな移行の検討には時間がかかる
- IPv6アプリケーション利用の需要が発生してからあわてないように、なるべく早い移行の検討を！