



組織への IPv6 導入プロセス

2011/10/15 IPv6勉強会 #01

自己紹介

- ▶ 村嶋修一/MURA
- ▶ 千葉県松戸市在住
- ▶ 独立系Sierでアプリケーション/インフラ/ネットワークのSA/コンサルっぽい事しています
- ▶ 本/雑誌書いています
- ▶ IPv6勉強会代表
- ▶ MS MVP for Windows Server Networking 改め
Virtual Machine: Networking
- ▶ <http://www.vwnet.jp>
- ▶ mura@vwnet.jp
- ▶ twitter: @Murashima
- ▶ facebook : <http://www.facebook.com/#!/S.Murashima>



こんな本書きました



Agenda

- ▶ 1 IPv4とIPv6の比較
- ▶ 2 IPv6導入状況
- ▶ 3 IPv6を導入しないとどうなるか
- ▶ 4 IPv6の導入シナリオ

いきなり結論

- ▶ IPv6を導入しなくても、すぐに問題が出るわけではないが、**じわじわと真綿で首を絞めるように影響が出てくる**
- ▶ IPv4とIPv6は互換性が無いし、考え方も違うので、**スキルチャージに時間が必要**
- ▶ すぐに導入するしないにかかわらず**検討は早く開始**するのが吉
- ▶ 少なくとも**リスク分析**だけは早々に済ませ、その結論に基づいた**導入時期や方針を見定めておく**必要あり

1 IPv4とIPv6の比較

IPv4 と IPv6 の比較(1)

	IPv4	IPv6	備考
OSI7階層	L3:ネットワーク層	L3:ネットワーク層	IPv4/IPv6とも同じ
Ether Type	0x0800	0x86DD	L2から見たL3識別 IPv4/IPv6で異なる
プロトコル番号	1:ICMP 6:TCP 17:UDP	58:IPv6-ICMP 6:TCP 17:UDP	L3から見たL4識別 ICMPが違うだけ
ポート番号	プロトコルに依存	プロトコルに依存	L4から見た上位層識別 IPv4/IPv6とも同じ
IPアドレスのビット長	32ビット	128ビット	IPv4/IPv6で異なる
表記方法	8ビットごとにピリオドで区切った10進で表現	16ビットごとにコロンで区切った16進表現	IPv4/IPv6で異なる
短縮記法	先頭の0を省略できる	先頭の0を省略できる 連続した0は1か所だけ::と省略できる	IPv4/IPv6で異なる

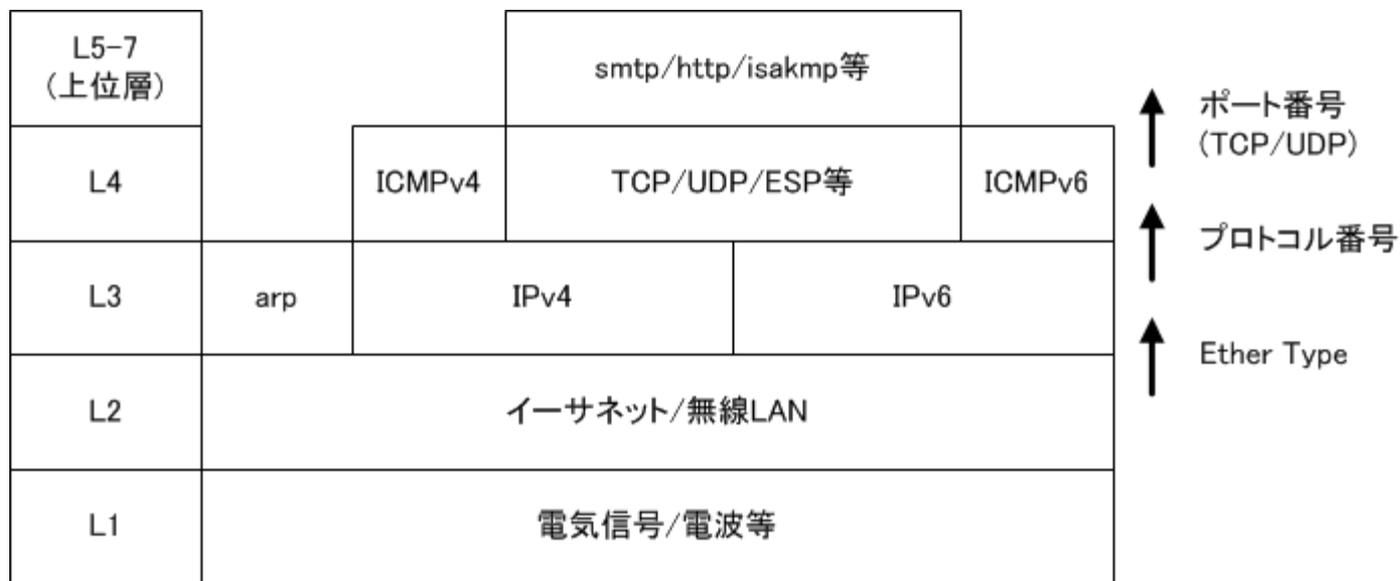
IPv4 とIPv6の比較(2)

	IPv4	IPv6	備考
サブネットの概念	あり	あり	呼称は違うが基本的には同じ
サブネットマスクの表現	255.255.255.0(IPv4アドレスと同様に10進表現) /24(CIDR)	/64(プレフィックス)	IPv6はCIDR形式のみ
1セグメントで使用できるホストIDのビット長(一般論)	8ビット(/24)	64ビット(/64)	IPv4/IPv6で異なる
ユニキャストアドレスの構造	ネットワークID(可変) +ホストID(可変)	グローバルルーティング(48bits) +サブネットID(16bits) +インターフェイスID(64bits)	IPv4/IPv6で異なる
スコープの考え方	グローバル サイトローカル	グローバル サイトローカル リンクローカル ノードローカル	IPv4/IPv6で異なる
ローカルアドレス	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	fc00::/7	IPv4/IPv6で異なる

IPv4 とIPv6の比較(3)

	IPv4	IPv6	備考
IPアドレスの自動構成	DHCPv4	RA(ICMPv6)	IPv4/IPv6で異なる
DNSディスカバリー	DHCPv4	RA+DHCPv6	IPv4/IPv6で異なる
ノードに割り当てるIPアドレス	1つ	複数 GUA ULA リンクローカル	IPv4/IPv6で異なる
ゲートウェイアドレス	中継ノードに割り当てられたIPv4アドレス	中継ノード割り当てられたリンクローカルアドレス	IPv4/IPv6で異なる
近隣探査	arp	ND(ICMPv6)	IPv4/IPv6で異なる
特別な意味を持つIPアドレス	別紙	別紙	IPv4/IPv6で異なる
NAT	あり	なし	IPv4/IPv6で異なる
パケットフラグメント	あり	なし(ICMPv6 で通知)	IPv4/IPv6で異なる

OSI7階層



特別な意味を持つIPアドレス

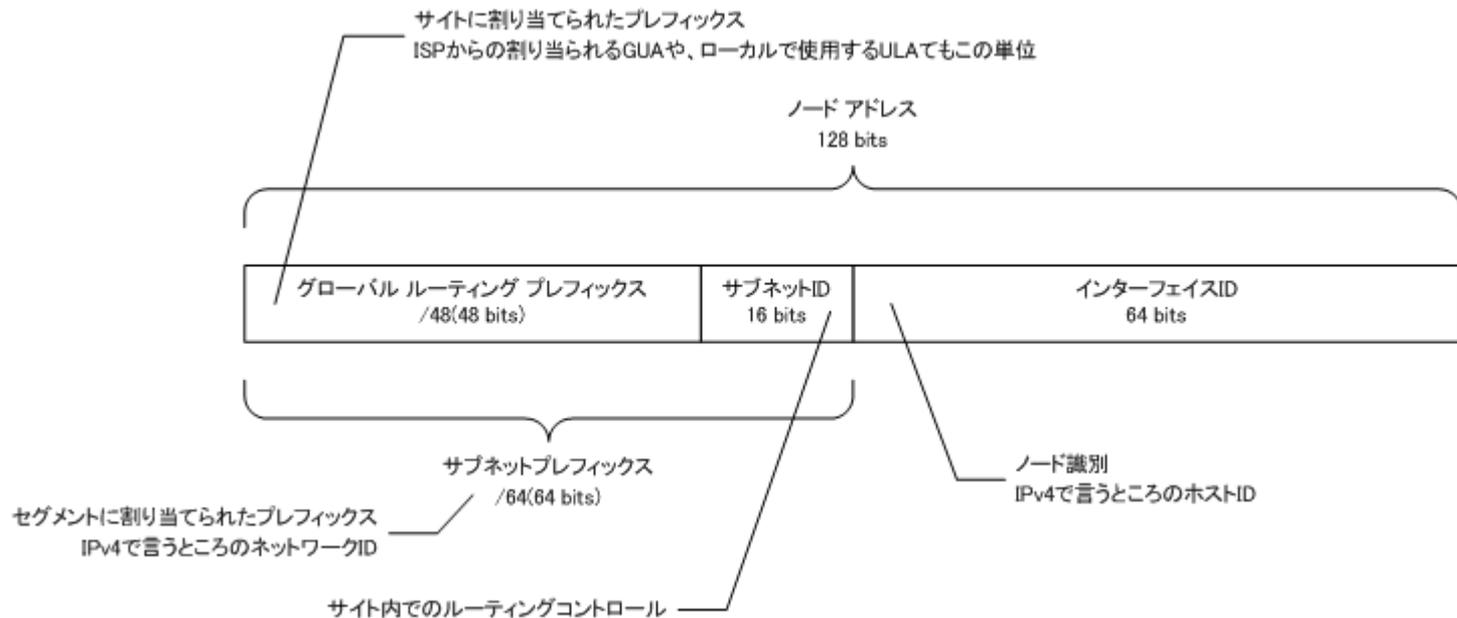
	IPv4	IPv6	備考
不定	0.0.0.0/0 (RFC5735)	::/0 (RFC4291)	
ループバック	127.0.0.1 (RFC5735)	::1 (RFC4291)	
マルチキャスト	224.0.0.0/4 (RFC5735)	ff00::/8 (RFC4291)	ff01::(ノードローカル) ff02::(リンクローカル) ff05::(サイトローカル)
ローカル	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16 (RFC5735)	fc00::/7 実際に使用できるのはfd00::/8 (RFC4193)	IPv6ではULAと呼び、計算で求める
グローバルユニキャスト	ローカル以外	2000::/3 (RFC4291)	IPv6ではGUAと呼ぶ
ドキュメント用	192.0.2.0/24 198.51.100.0/24 203.0.113.0/24 (RFC5737)	2001:db8::/32 (RFC3849)	資料などのドキュメントで使用する事が出来るグローバルアドレス
リンクローカル	169.254.0.0/16 (RFC5735)	fe80::/10 (RFC4291)	IPv4のリンクローカルはほとんど活用されていない

表記と短縮方法

- ▶ 16ビットごとにコロンで区切った16進表現
 - ▶ 2001:0db8:0001:0000:0000:0000:0000:cafe
- ▶ 先頭の0は省略可能
 - ▶ 2001:db8:1:0:0:0:0:cafe
- ▶ 連続した0は1カ所だけ「::」に省略可能
 - ▶ 2001:db8:1::cafe

- ▶ 詳細ルールはRFC5952にあり

ユニキャストアドレスの構造



ユニキャストアドレスの例

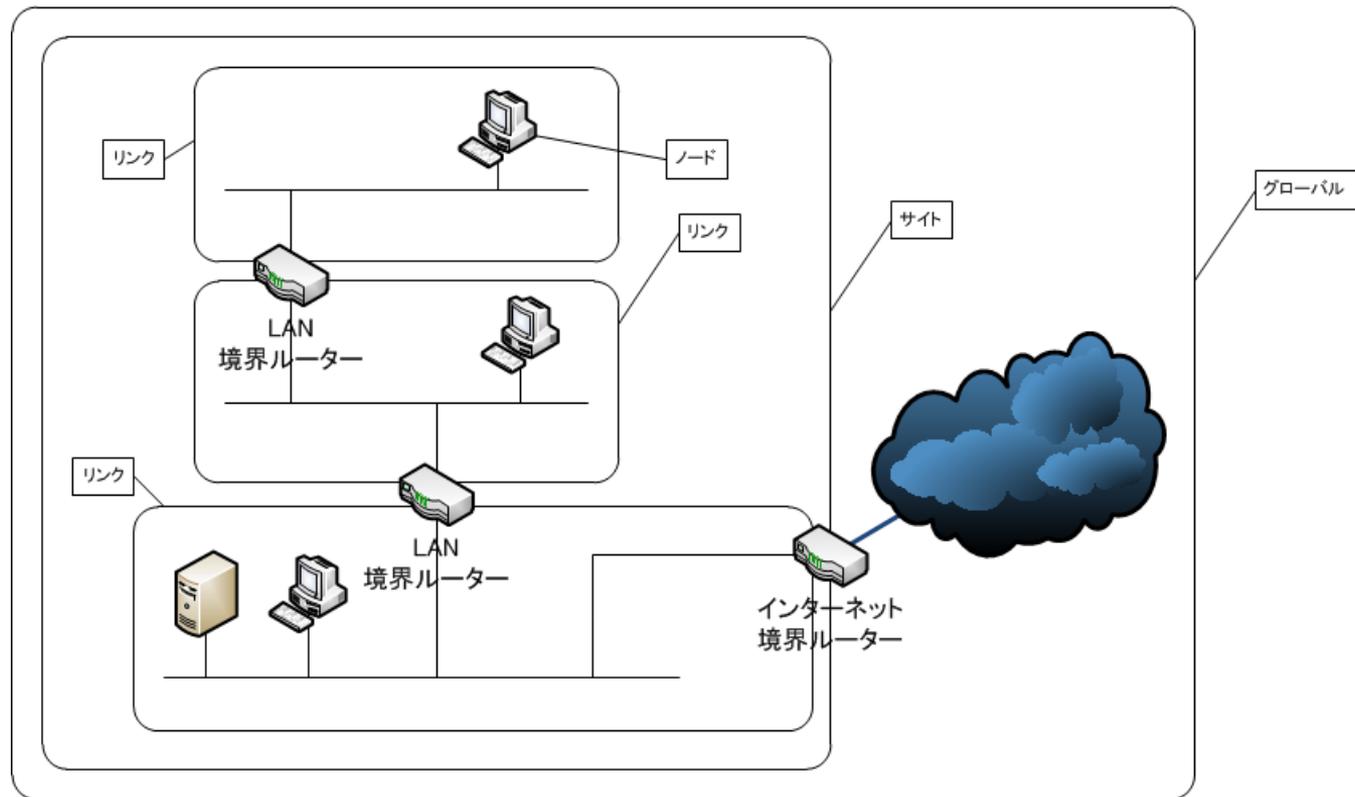
2001:db8:101d:1234:203d:d325:9e45:461d

グローバル ルーティング プレフィックス

サブネットID

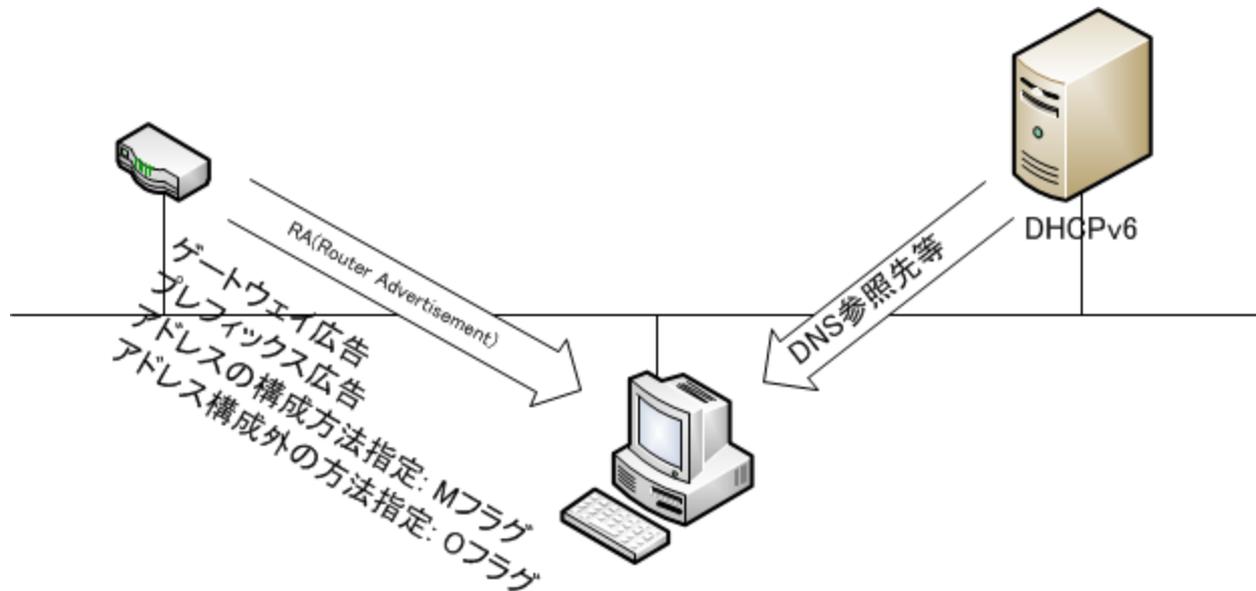
インターフェイスID

スコープ



IPアドレスの自動構成

RA(Router Advertisement)



RAとDHCPv6の関係

M flag	O flag	意味
ON	ON	アドレスとそれ以外の情報を DHCPv6 で構成する (ステートフル) IPv4 の DHCP と同じ動作
ON	OFF	アドレス構成は DHCPv6 を使用するが、それ以外の情報は手動等の別の手段で設定する
OFF	ON	アドレス構成には RA を使用するが、それ以外の情報は DHCPv6 を使用する (ステートレス) アドレス構成は RA が主体
OFF	OFF	DHCPv6 を使用しない

DHCPv6の動作モード

▶ ステートレス

- ▶ DNSディスカバリー情報等のアナウンス
- ▶ IPv6アドレスの振り出しをしない

▶ ステートフル

- ▶ DNSディスカバリー情報等のアナウンス
- ▶ IPv6アドレスの振り出しをする

IPアドレスの構成

- ▶ 手動設定
- ▶ プレフィックス+EUI-64
 - ▶ MACアドレスから算出したインターフェイスID
- ▶ プレフィックス+ランダム
 - ▶ Windows Server OS
 - ▶ ランダム構成されたインターフェイスID
 - ▶ 静的割当て
 - ▶ DDNSに登録される
- ▶ プレフィックス+匿名アドレス(ランダム)
 - ▶ Windows Client OS
 - ▶ ランダム構成されたインターフェイスID
 - ▶ 一定時間 or 再起動で再構成
 - ▶ DDNSに**登録されない**

Windows Server 2008 の自動構成

```
コマンド プロンプト
C:\>ipconfig

Windows IP 構成

イーサネット アダプター HOST:

  接続固有の DNS サフィックス . . . . : vwnet.jp
  IPv6 アドレス . . . . . : 2001:278:101d:0:8c7f:a140:d9b2:1192
  IPv6 アドレス . . . . . : fd75:f582:7ae3:0:8c7f:a140:d9b2:1192
  リンクローカル IPv6 アドレス . . . . : fe00::8c7f:a140:d9b2:1192%11
  IPv4 アドレス . . . . . : 192.168.33.198
  サブネット マスク . . . . . : 255.255.255.0
  デフォルト ゲートウェイ . . . . . : fe80::209:fff:fe16:3a24%11
                                       192.168.33.254

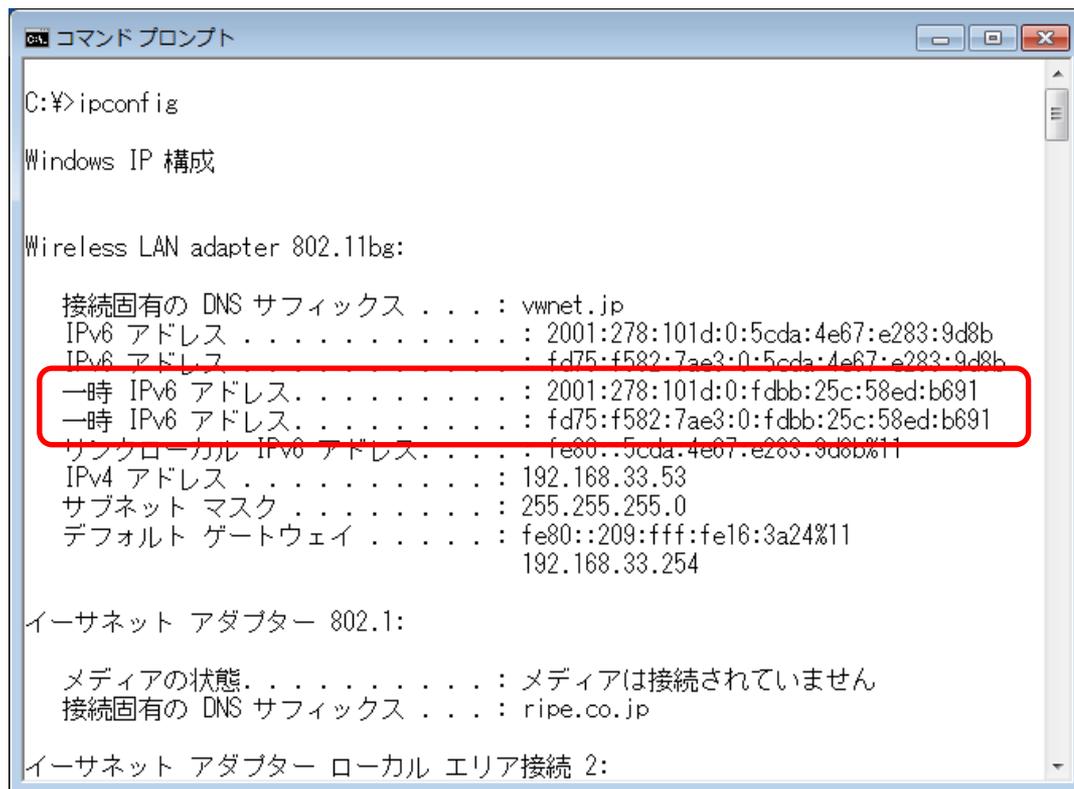
Tunnel adapter isatap.{23EA202D-86F3-4C03-A4E8-8A96E754051D}:

  メディアの状態. . . . . : メディアは接続されていません
  接続固有の DNS サフィックス . . . . : vwnet.jp

Tunnel adapter Teredo Tunneling Pseudo-Interface:

  メディアの状態. . . . . : メディアは接続されていません
```

Windows7の自動構成



```
コマンドプロンプト
C:\¥>ipconfig

Windows IP 構成

Wireless LAN adapter 802.11bg:

    接続固有の DNS サフィックス . . . . : vwnet.jp
    IPv6 アドレス . . . . . : 2001:278:101d:0:5cda:4e67:e283:9d8b
    IPv6 アドレス . . . . . : fd75:f582:7ae3:0:5cda:4e67:e283:9d8b
    一時 IPv6 アドレス . . . . . : 2001:278:101d:0:fd8b:25c:58ed:b691
    一時 IPv6 アドレス . . . . . : fd75:f582:7ae3:0:fd8b:25c:58ed:b691
    リンクローカル IPv6 アドレス . . . . : fe80::5cda:4e67:e283:9d8b%11
    IPv4 アドレス . . . . . : 192.168.33.53
    サブネット マスク . . . . . : 255.255.255.0
    デフォルト ゲートウェイ . . . . . : fe80::209:fff:fe16:3a24%11
                                     192.168.33.254

イーサネット アダプター 802.1:

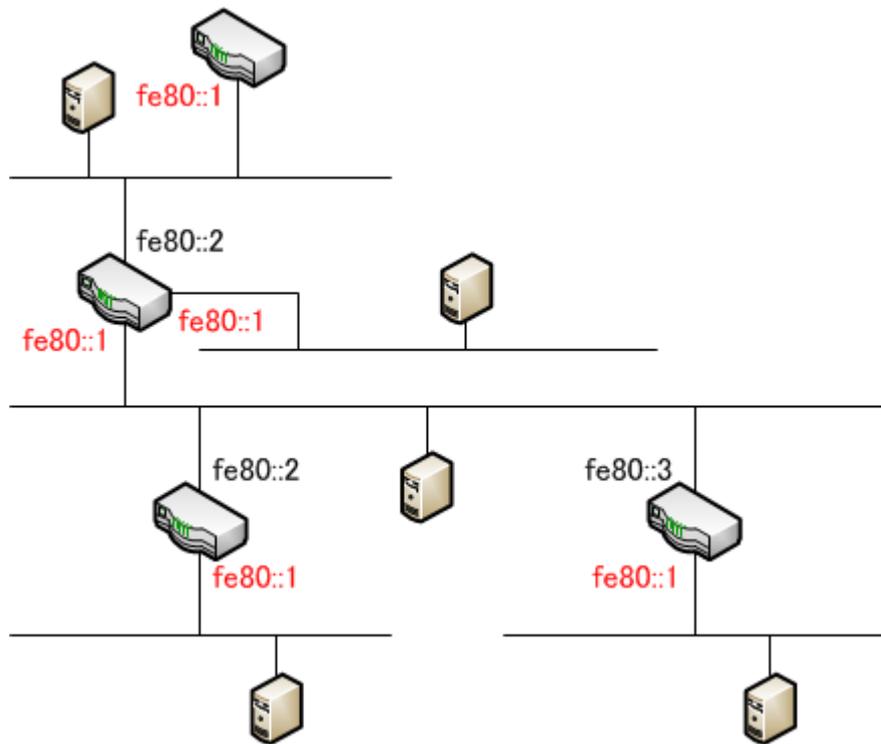
    メディアの状態 . . . . . : メディアは接続されていません
    接続固有の DNS サフィックス . . . . : ripe.co.jp

イーサネット アダプター ローカル エリア接続 2:
```

ゲートウェイアドレス

- ▶ ゲートウェイはリンクローカルアドレス指定が出来る
- ▶ デフォルトゲートウェイにfe80::1を割り当てると、手動設定の時にミスが起きにくい

ゲートウェイアドレスの割当て例



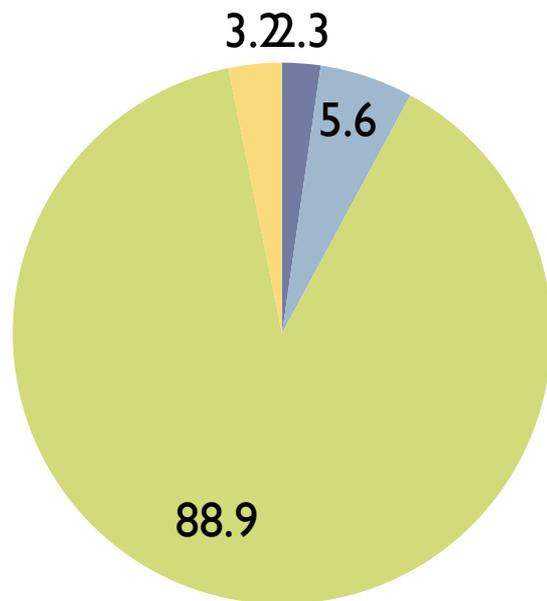
IPv4 とIPv6の共存

- ▶ IPv4/IPv6 **デュアルスタック**が基本
- ▶ IPv4とIPv6の互換性は無い
- ▶ IPv4/IPv6トランスレーターは高価
- ▶ IPv4は当分生き残る
- ▶ LANへのIPv6展開は簡単(RA設定だけ)

2 IPv6導入状況

IPv6の導入状況

IPv6導入状況



- 導入/運用している
- まだ導入していないが、具体的に導入、運用を始める予定がある
- 導入しておらず、具体的な導入予定もない
- わからない

N=216 日経コミュニケーション 2011/8 より抜粋

導入した主な理由

- ▶ いずれは導入が必要になると考えたから
- ▶ まずは試験的に導入し、評価を行いたいから
- ▶ IPv6に対応したサービスや製品などの開発のため
- ▶ VPNの足回り回線として導入
- ▶ 一部サービスでIPv6でしか対応が出来なかったため

日経コミュニケーション 2011/8 より抜粋

導入予定が無い理由

- ▶ いずれは導入が必要と漠然と考えているが、まだその時期ではないと考えているから
- ▶ いずれは導入が必要と漠然と考えているが、どこから手を付けてよいかわからないから
- ▶ 現時点でIPv6導入は必要ないと判断したから
- ▶ 外部に公開しているサーバーなどが無く、社内でも必要ないから
- ▶ IPv6導入のために調査、検証、評価などを進めているが、導入予定のメドが立っていないから
- ▶ 会社の上層部の許可が得られず、IPv6導入に必要な予算がつかないから
- ▶ その他
- ▶ わからない

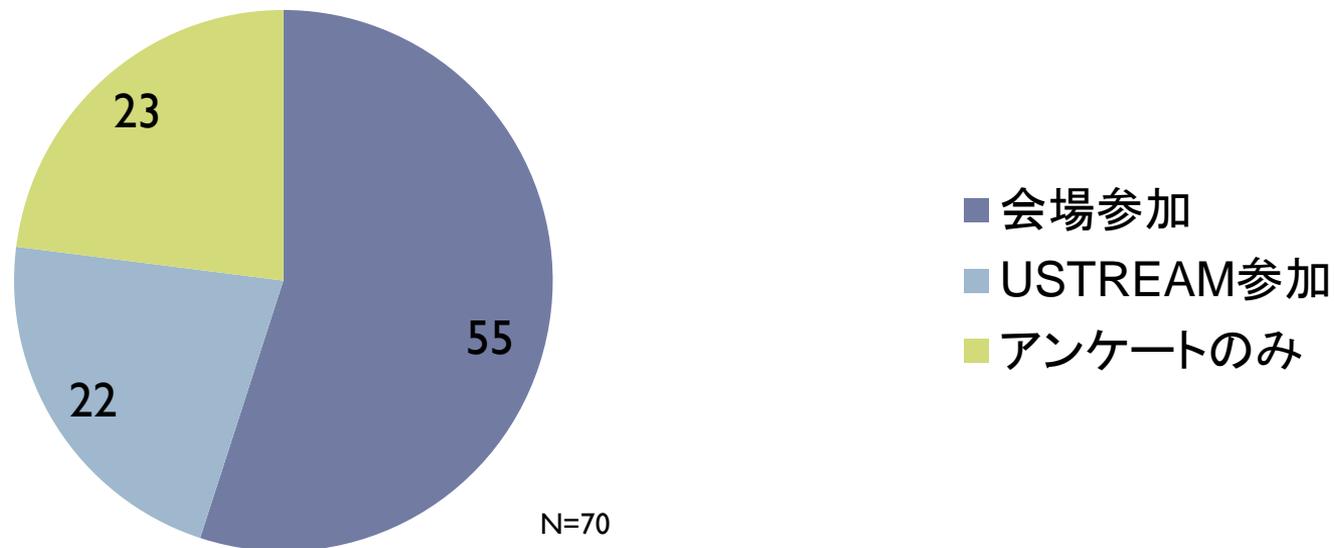
日経コミュニケーション 2011/8 より抜粋

アンケート結果発表

多くのご回答ありがとうございました

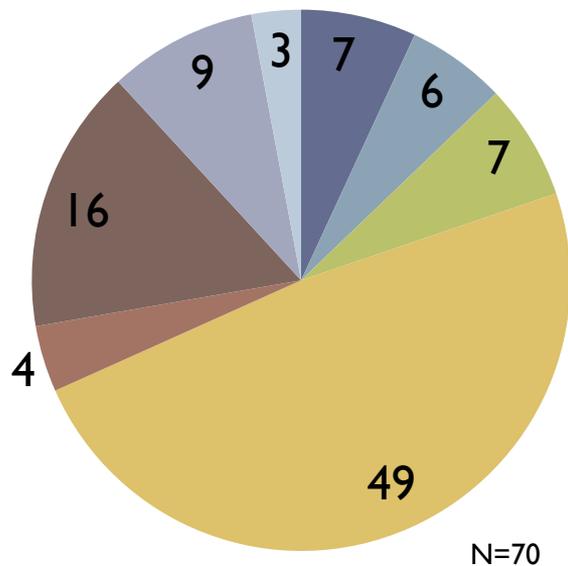
Q-1 勉強会への参加

Q-1 勉強会への参加



Q-2 IPv6の理解

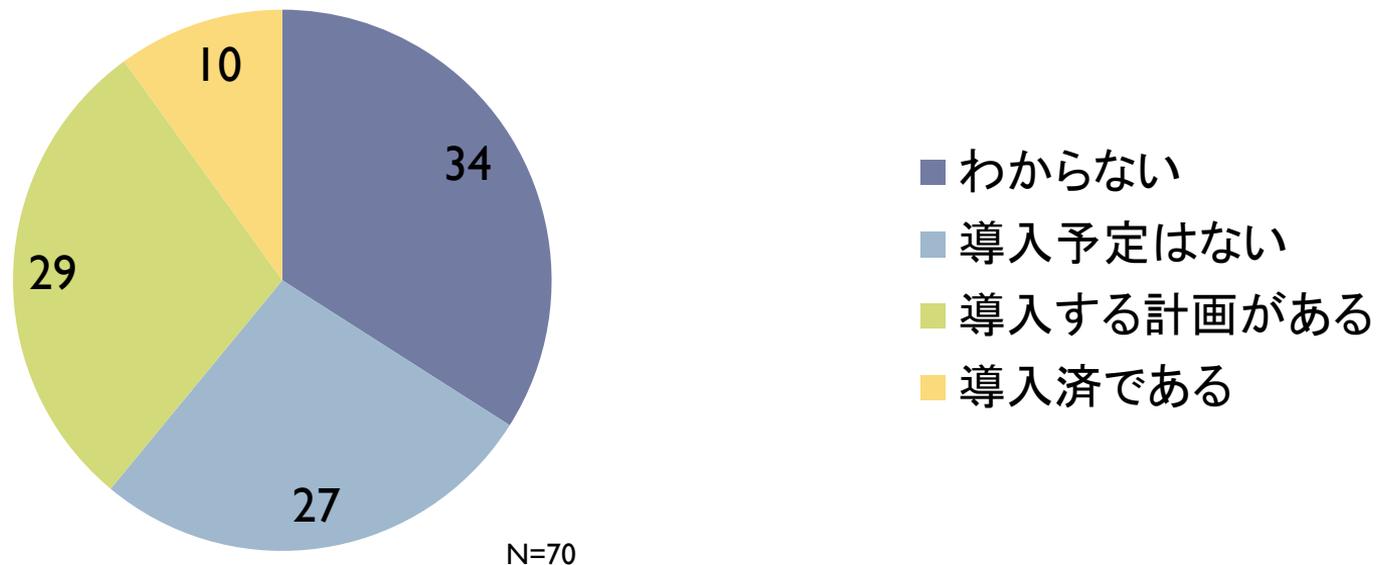
Q-2 IPv6 の理解



- わからない
- 128ビットで構成されていることは知っている
- IPv6アドレスの表記方法を知っている
- IPv6にもローカルアドレスとグローバルアドレスがある事を知っている
- RAとDHCPv6について説明が出来る
- IPv6の設定をしたことがある
- 2セグメント以上を持つネットワークの設計/構築経験がある
- DMZの設計/構築経験がある

Q-3 所属組織へのIPv6導入状況

Q-3 所属組織へのIPv6導入状況

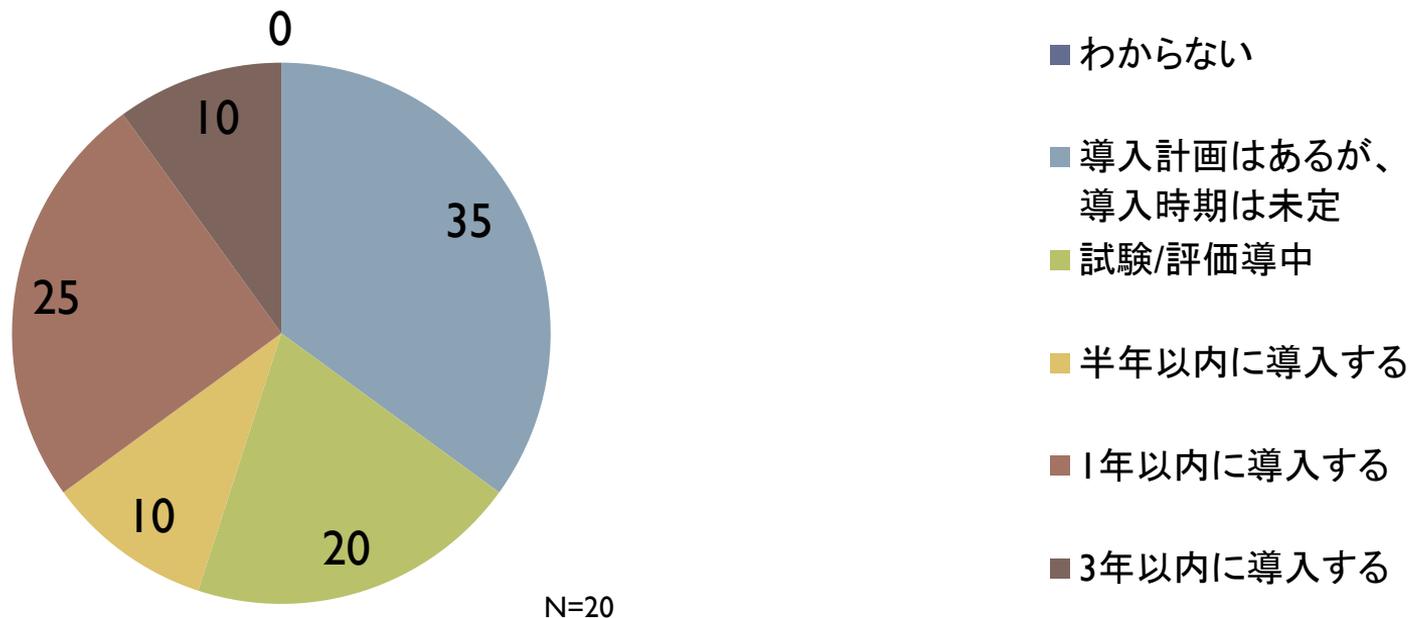


Q-4 導入しない理由はなんですか？

- ▶ 必要性を感じない/必要性がわからない
 - ▶ 13件
- ▶ ノウハウ不足
 - ▶ 8件
- ▶ コスト
 - ▶ 3件
- ▶ 環境など(外部がIPv4/古いOSが健在)
 - ▶ 3件

Q-5 組織へのIPv6導入計画について

Q-5 組織へのIPv6導入計画について

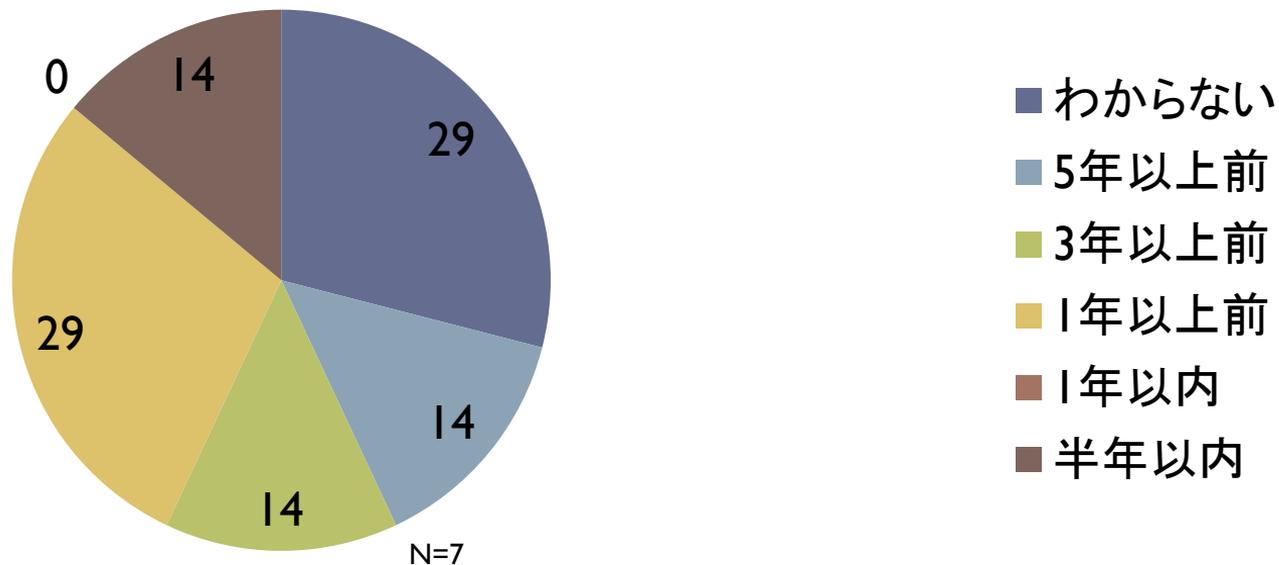


Q-5A 導入時期未定の理由はなんですか？

- ▶ 上流/ISPの対応が未定
- ▶ 社内からIPv6についての必要との声が上がってこない
- ▶ 予算が無い
- ▶ 導入に対しての知識不足
- ▶ 具体的な話が出てこない

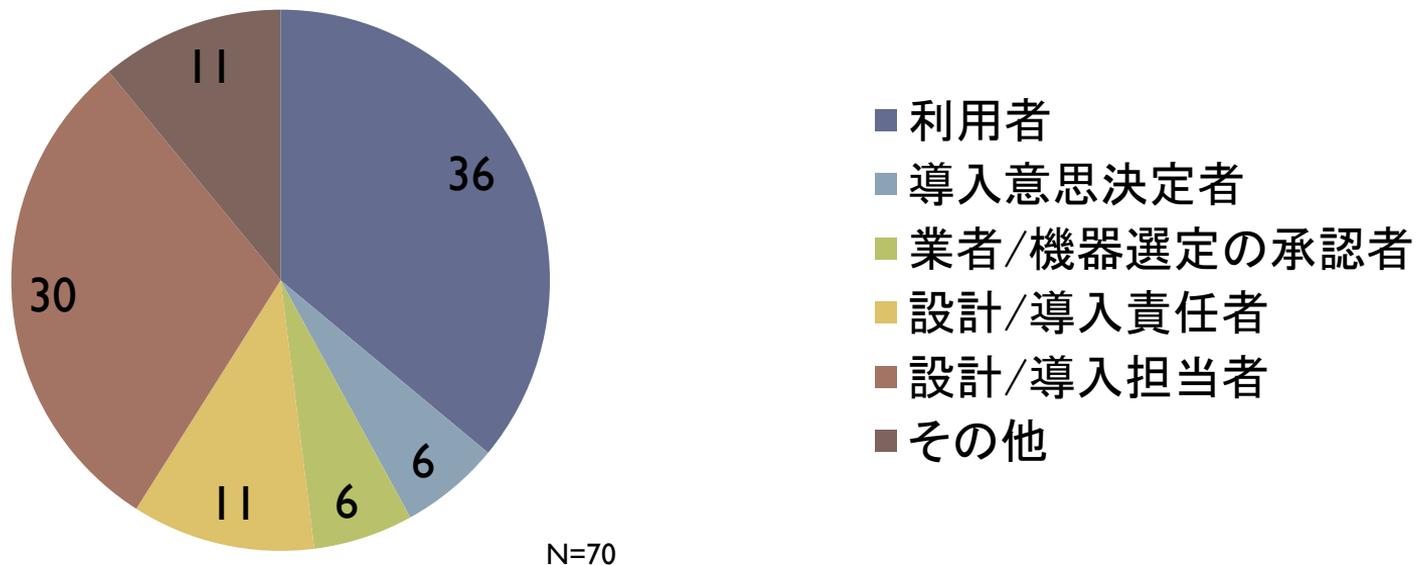
Q-6 組織へのIPv6導入したのはいつごろですか？

Q-6 組織へのIPv6導入したのはいつごろですか



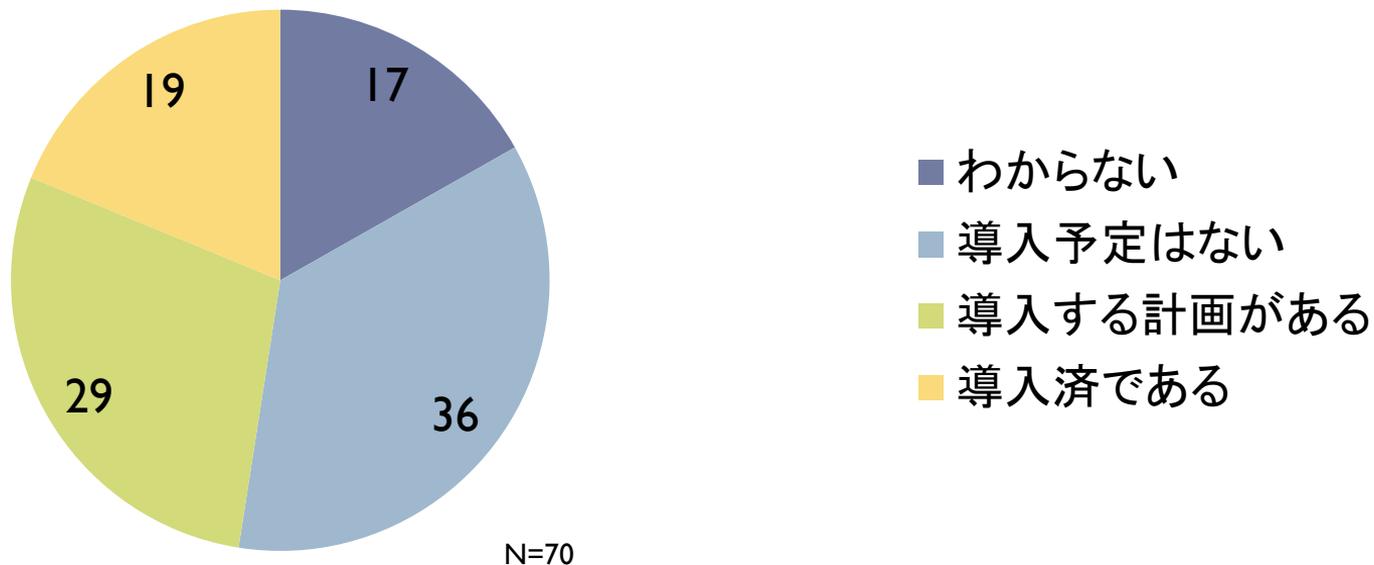
Q-7 組織に IPv6 導入する際の立場

Q-7 組織に IPv6 導入する際の立場



Q-8 自宅へのIPv6導入状況

Q-8 自宅へのIPv6導入状況



Q-9 IPv6 導入に関して思う事(その1)

- ▶ **不安/情報不足**
 - ▶ IPv4が取得できなくなった時にどうすれば良いのかわからない
 - ▶ IPv4との違いが多く理解が難しい
 - ▶ IPv4との併存はどうすれば良いのかわからない
 - ▶ こうすれば出来ると言うハウツー情報がほとんどない
 - ▶ IPv6の導入メリットが見えてこない
 - ▶ 導入実績が少ない
 - ▶ IPv4の枯渇対応以外で、IPv6でしか出来ない事がよくわからない
- ▶ **環境/機器のIPv6対応遅れ**
 - ▶ IPv6未対応のホスト/ネットワーク機器/アプリがある
 - ▶ IPv6対応機器であってもでも、部分的にIPv6未対応の部分がある
 - ▶ 上位ISPが対応しない
 - ▶ IPv6対応サイトが少ない
- ▶ **コストの問題**
 - ▶ ネットワーク機器の追加ライセンス等でコスト高になる
 - ▶ 個人導入にはコストが高い
 - ▶ 経営層の理解が得られない

Q-9 IPv6 導入に関して思う事(その2)

- ▶ 期待する/勉強したい
 - ▶ 基礎から勉強したい
 - ▶ エンジニアとして遅かれ早かれ避けては通れない道
 - ▶ これからIPv6対応は増えてくるのでスキルを習得したい
 - ▶ 早い段階で知識・経験を積んでおきたい
 - ▶ ISP/ASPが対応すれば、普及は早いと思う
 - ▶ 普及は必須なので、早期に技術習得したい
 - ▶ 具体的なネットワーク構成、コンフィグ、ドキュメントの書き方などについてもっと情報が欲しい
 - ▶ ネットワーク・DMZ設計などの知識を習得したい
- ▶ 雑感
 - ▶ アドレスが長くて覚えられない
 - ▶ IPv6じゃないとダメと言う案件が無い
 - ▶ 管理が難しそうに感じる
 - ▶ 待ったなしの筈なのに...
 - ▶ これからが楽しみ

Q-10 IPv6導入で一番の障壁は何だと思いますか?(1)

▶ 環境

- ▶ ISP/IDCの対応
- ▶ 安価にIPv6を提供しようとする姿勢が国内ISPに見られない
- ▶ 各ベンダーのIPv6対応/BBルーターの対応
- ▶ 監視/運用ツールがデュアルスタックに耐えられないように感じる
- ▶ 対応できるエンジニアの絶対数が足りない

▶ コスト/メリット

- ▶ 導入/運用に手間がかかる
- ▶ 導入コストを説明できない/予算が付かない/費用対効果が見えない
- ▶ インセンティブが無い
- ▶ ネットワーク機器のリプレイス、ソフトウェアのアップデート

▶ 情報/知識不足

- ▶ 導入/移行/運用/トラブル対応などの情報が少ない
- ▶ アドレス範囲拡張以外のメリットがアピールされていない
- ▶ 何が起こるか皆無であるため、リスクと考えている?
- ▶ IPv6の導入メリットの明確化

Q-10 IPv6導入で一番の障壁は何だと思いますか?(2)

▶ 意識

- ▶ 導入に対する理解が得られない/危機感が薄い
- ▶ 他人事になっている
- ▶ 普通の人には困っていません
- ▶ NAPTで事が足りるのではないか
- ▶ 検討すらされていない

▶ 仕様/規格

- ▶ ISPとの接続方法が多種あるので混乱が生じる
- ▶ ISP、NGN、低価格ルーターメーカーの表記が甘い
- ▶ 利用する機材によっては接続できないなどの問題が出ると予想される
- ▶ RFCの動きが激しく安定した規格とは思えない

▶ 他

- ▶ きっかけ
- ▶ いつまで現行環境が利用できるのか、本当の期限の見極めが必要

3 IPv6を導入しないとどうなるか

真綿で首を絞めるように

- ▶ 今すぐ問題が顕在化するわけではない
- ▶ LSNでWebサービスが劣化
- ▶ 新規IPアドレス取得時にグローバルIPv4アドレスが取得できない
- ▶ IPアドレスリナンバー発生時にIPv4アドレスが取得できない

- ▶ IPv6しか割り当てられなかった拠点とインターネットVPNが張れない
- ▶ モバイル環境がLSN+IPv6環境になった場合、IPv4でのリモートアクセスが出来なくなるかもしれない
- ▶ IPv6しか取得できなかった客先とメール交換などのB2B取引が出来ない
- ▶ IPv4アドレスの供給が受けられず IPv6 Only となってしまった公開サーバーに対してIPv4 Onlyユーザーがアクセスできない
- ▶ IPv6しか割り当てられなかったユーザーがWebサイトをアクセスできない
- ▶ IPv6を導入していないと、IPv6前提の未知のサービスが出てきた時に対応が出来ない

- ▶ これからのインターネットスタンダードはIPv6!!!

公開サーバーがIPv6に

- ▶ IPv4アドレスは枯渇したので、ISP/iDC手持ちIPv4アドレスが無くなった時点で**公開サーバー用のIPv4アドレスが取得できなくなる**
- ▶ IPv6 Only サーバーは IPv4 Only のユーザーからアクセスできない
- ▶ 利用者へのIPv6普及が進まないとインターネットサービスに影が出る!!
 - ▶ でもISPのIPv6サービスは現状有償(涙)

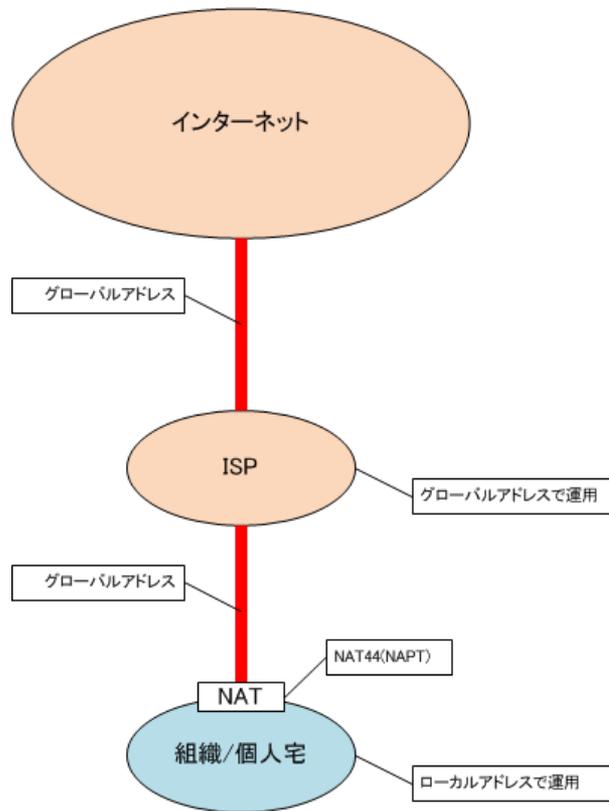
インターネットVPN

- ▶ 固定IP運用でも拠点移動/新拠点/**品目変更**で**IPv4アドレス**が**取得できなくなる**
- ▶ LSNに收容された拠点やモバイルとのIPsec/PPTPが維持できるか現状不透明
 - ▶ パススルー可否が現状不明
- ▶ センター側のIPv6対応が必須となる

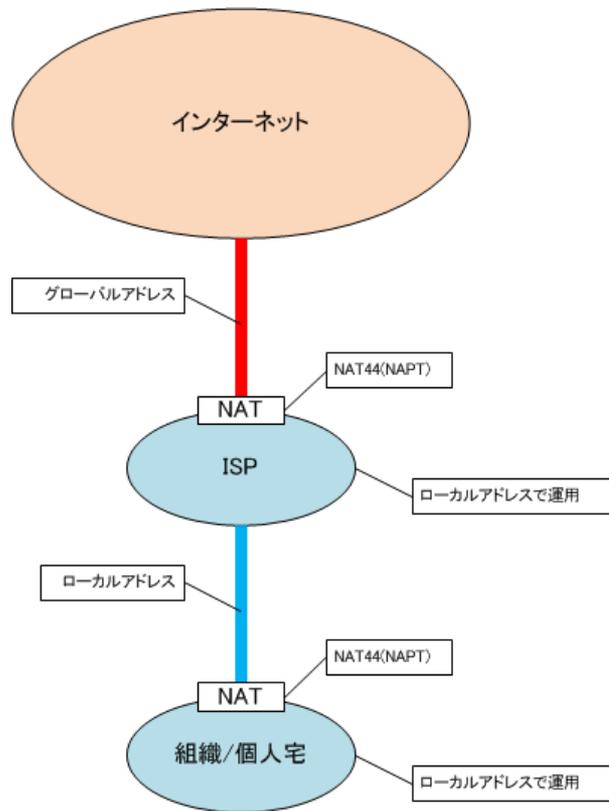
未知のIPv6サービス

- ▶ 未知のIPv6サービスが提供された時にサービスが利用できない

従来のIPv4サービス



LSNのイメージ



LSNの宿命

- ▶ IPv4は枯渇したので、ISPが持っている現有IPv4アドレスの使い回し
- ▶ 固定IPv4アドレス要求ユーザーのために動的IPv4割り当て用のアドレスを圧縮
- ▶ 公開サーバー増加、利用者増加、利用機器増加、ISP内部機器増設などでIPv4アドレス消費は増える一方
- ▶ 動的IPv4利用者をNAT44(NAPT)に押し込んでIPv4アドレスを確保
↑これがLSN
- ▶ Webブラウザ1画面で10-20(物によってはそれ以上)セッション × 同時に開く画面数 × 利用デバイス × 利用者数 × 収容世帯数 < 65,535
- ▶ 動的IPv4利用環境では一部通信が出来ない等の劣化が発生
- ▶ 非TCP/UDP通信(IPsec/PPTP等)が通るかは現状不透明

リナンバーの落とし穴

- ▶ IPv6導入や回線増強で回線品目やISP変更は通常事象
- ▶ 回線品目変更をすると取得済みのIPアドレスがリナンバーされる可能性が高い
 - ▶ 例) Bフレッツ→フレッツ光NEXT
- ▶ リナンバーが発生した時にISP/IDCが割り当て可能なIPv4アドレスを持っているとは限らない
- ▶ 固定IPv4を持つ前提で回線品目変更するのであれば、出来るだけ早く回線の引き込みをしておくのが賢明
- ▶ 現在持っているIPv4アドレスを維持するのであれば、IPv6対応時に回線増設になる事も

リスク分析だけは早急に

- ▶ IPv6導入は今すぐでなくても良いが、**リスク分析**だけは早急にしておかないと後で泣きを見る!!! (かもしれない)

IPv6導入のメリット/デメリット

▶ メリット

- ▶ IPv6を導入しない場合の問題回避
- ▶ NAT不要

▶ デメリット

- ▶ 導入コストがかかる

▶ 現状IPv6導入推進する決め手に欠ける

- ▶ ウイルス対策導入初期と同じ道を歩んでいる?

4 IPv6の導入シナリオ

実装のまとめ

- ▶ 基本はデュアルスタック
- ▶ IPv6アドレスはGUA/ULAの両方を割り当てる
- ▶ RA+DHCPv6でIPv6を展開
- ▶ 固定IPv6アドレスが必要なサーバー以外は自動構成で運用可能
- ▶ IPv6対応が難しい、必要が無い物はIPv4のまま運用
- ▶ 特殊事情が無い限りNAT-PTは考えない
- ▶ デフォルトゲートウェイに fe80::1 を設定しておくともミスが少なくて済む
- ▶ DMZから手を付ける
- ▶ DMZポリシーはセグメント単位で設計
- ▶ IPv6アドレスからホストを特定する必要があるのなら、匿名IPv6アドレスは使用しない
- ▶ IPv6アドレスを生で使うのはミスの原因。DDNS必須

導入のステップ

1. 準備段階
2. 実現方法検討
3. 稟議
4. 回線開通/テスト導入
5. 設計
6. 展開

1 準備段階

事前準備は入念に

トレーニングと検証

- ▶ IPv6そのものの勉強
- ▶ IPv6実装試験
- ▶ デュアルスタックの動作確認
- ▶ RAとDHCPv6の実装試験
- ▶ 自動構成の動作確認
- ▶ ダイナミック/スタティックルーティングの動作確認
- ▶ サーバーとクライアントの動作確認

環境調査

- ▶ セグメントごとにIPアドレスを持つノードを全て洗い出す
- ▶ ノードごとにIPv6対応の要否判定
- ▶ 現状の問題点を再確認

IPv6対応が必要な機器

- ▶ L3以上で動作している
- ▶ インターネットと通信している
- ▶ インターネット通信する経路になっている

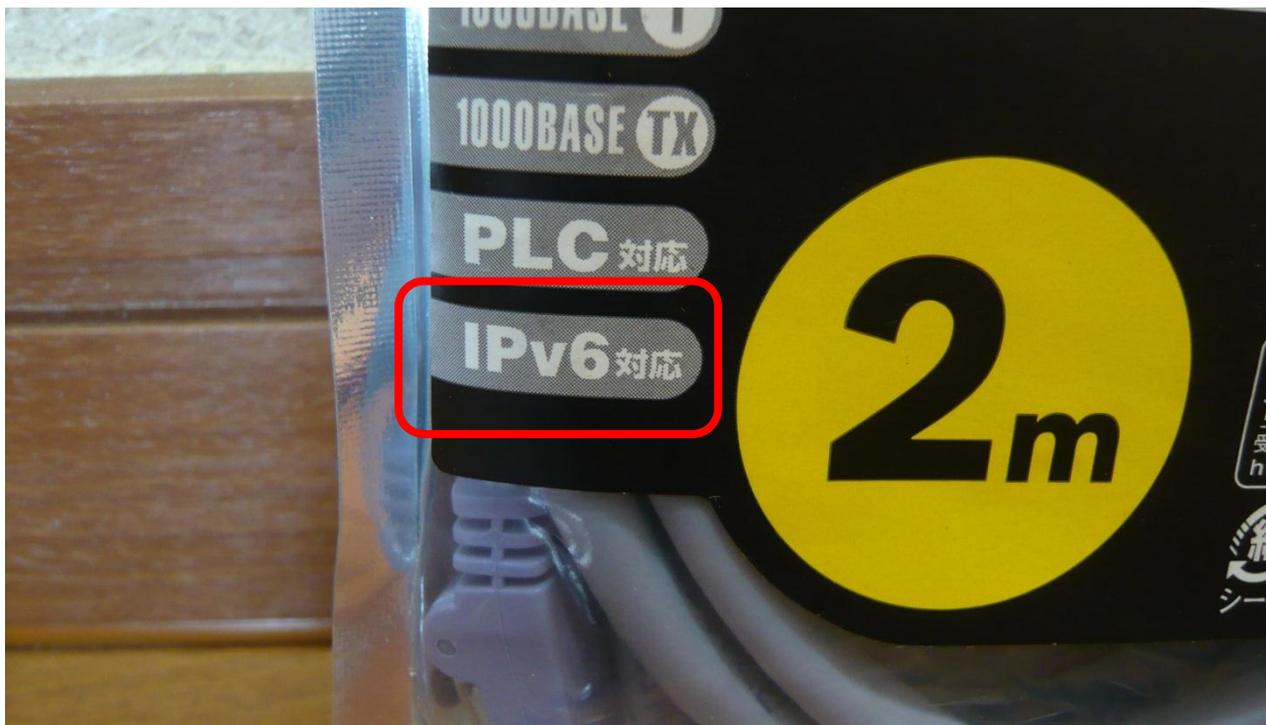
IPv6対応が不要な機器

- ▶ **L2以下**で動作している
 - ▶ L2-SW
 - ▶ LANケーブル
 - ▶ 無線LAN
- ▶ **LANに閉じた**通信しかしない
 - ▶ プリンタ/複合機
 - ▶ 管理インターフェイス
 - ▶ 業務システム
- ▶ インターネット通信する**経路から外れている**
 - ▶ 公衆回線とだけ接続しているIP電話(VoIP)
 - ▶ 外界から隔離されたネットワークに使用している機器

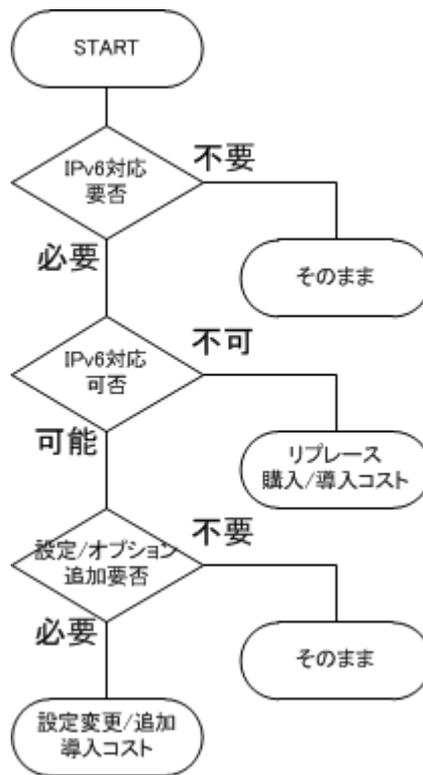
LANケーブル買ってきました



IPv6対応?



IPv6対応の切り分け



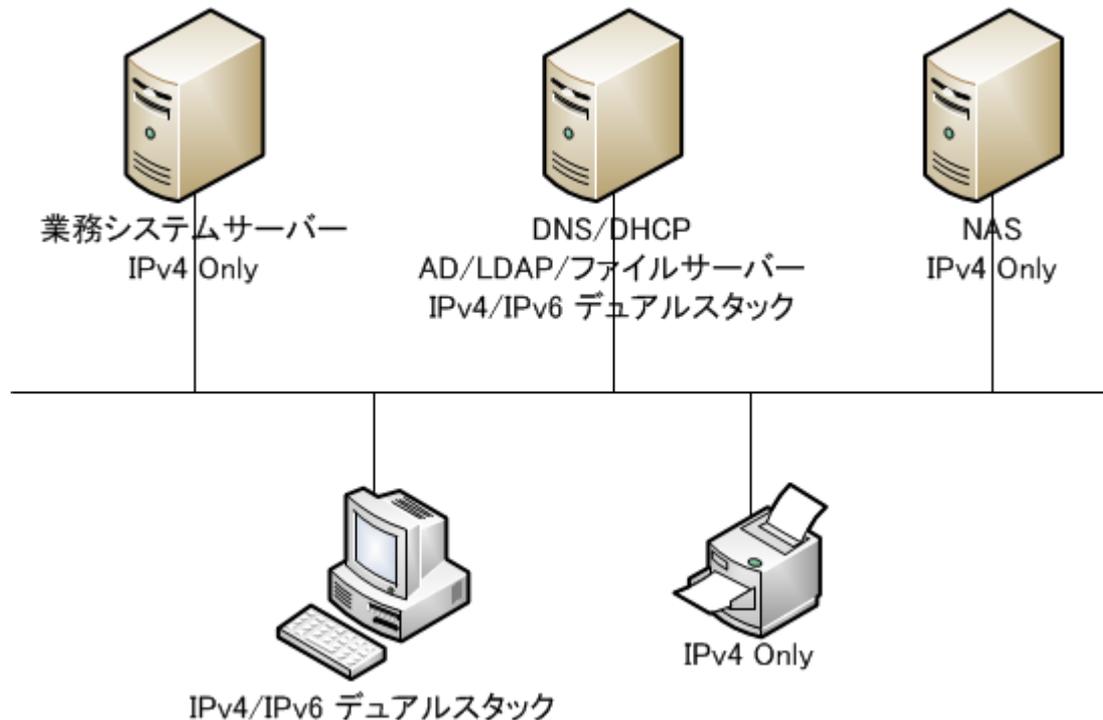
コスト見積

- ▶ ベンダーに機器/導入見積依頼
- ▶ 自力で設定するのなら工数見積
- ▶ 運用コスト見積もお忘れなく

導入の方向性検討

- ▶ どこから手を付けるか
 - ▶ 回線 > 評価環境 > DMZ > LAN/サーバー > 拠点/モバイル
- ▶ どこまで導入するか
 - ▶ 基本的にはIPv6対応が必要な範囲全て
 - ▶ IPv6実装が難しい物は**無理にIPv6対応する必要なし**
 - ▶ 部分的導入にとどめるのならDMZだけ
- ▶ 回線はどうするか
 - ▶ 品目/ISP変更なら新設廃止がお勧め
 - ▶ 所有しているIPv4アドレスを維持するのならIPv6回線増設

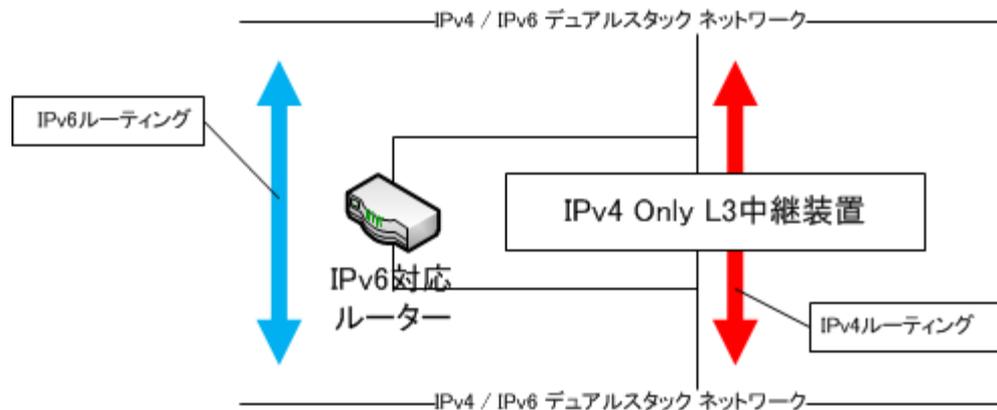
全てをIPv6対応にする必要はない



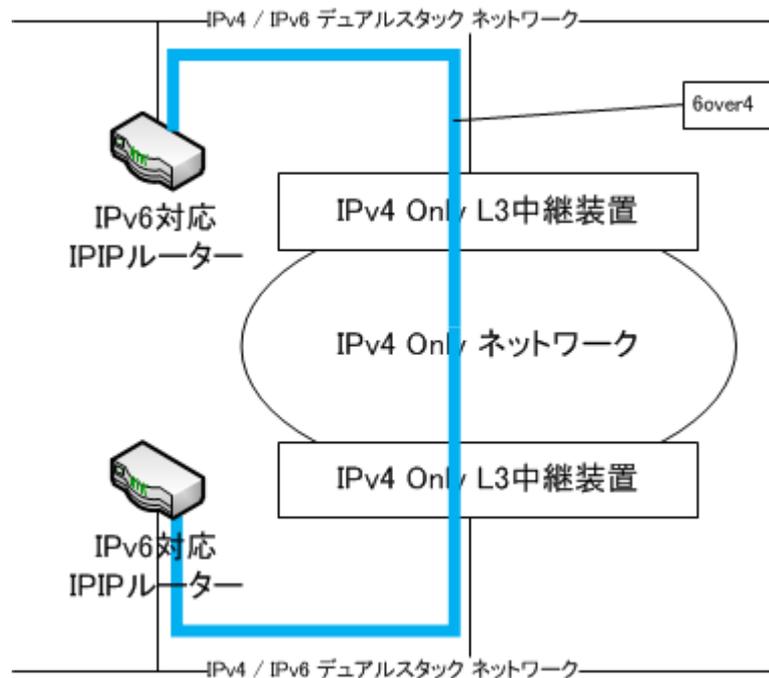
L3中継装置のIPv6対応が難しい時

- ▶ DMZまでIPv6対応にして、LANはそのまま
- ▶ IPv6ルーティング専用に安価なIPv6対応ルーターで迂回路を作る
- ▶ IPIPトンネルが張れる安価なルーターで、内部6over4ネットワークを作る

ルーターで迂回



内部6over4



回線検討

- ▶ 専用線タイプ
 - ▶ 高いがSLAが効く
- ▶ フレッツ光NEXT
 - ▶ 企業で使うのならIPv6 PPPoE 一択
 - ▶ IPv6 IPoE は半固定なので内部使用のGUAには一抹の不安が残る
- ▶ 6over4
 - ▶ 現有IPv4回線の中に通すのでパフォーマンスは落ちるがコストは低い

2 実現方法検討

回線接続方法

- ▶ デュアルスタック専用回線
 - ▶ コストは高いが安定
- ▶ フレッツ光NEXT
 - ▶ PPPoEの実装場所
 - ▶ NAT44の実装場所
- ▶ 6over4
 - ▶ 現有のIPv4を生かせる
 - ▶ コストは低いが、パフォーマンスに劣る
 - ▶ IPIトンネルの実装場所
- ▶ IPv6専用回線を増設する
 - ▶ 現有のIPv4を生かせる
 - ▶ 収容場所

DMZ

- ▶ グローバルIPv4/GUA手動割当てなので**RA不要**
- ▶ NATにするか、ブリッジにするか
- ▶ DNSはどこを参照するか
 - ▶ キャッシュ毒盛りを避けて内部用のDNSを参照?
- ▶ この際だから、**クラウド**に全部持っていくってのもアリ

サーバーセグメント

- ▶ ローカルIPv4アドレス手動設定
- ▶ **固定IPv6が必要なサーバーはGUA/ULAを手動設定**
- ▶ 内部がAD等のDDNSなら、固定IPv6が必要なサーバー以外のGUA/ULAは**自動構成でOK**
- ▶ DHCPv6設置

クライアント

- ▶ IPv4: DHCPv4
- ▶ IPv6: GUA/ULA **自動構成**
- ▶ DNSディスカバリー: DHCPv6リレーまたは **IPv4 で賄う**

3 「稟議」と言う名の鬼門

予算をどうやって通すか

稟議を書く前にIPv6導入の必要性を再考

- ▶ リスク分析
 - ▶ IPv6普及が自組織にどのような影響を与えるか
 - ▶ IPv4枯渇の影響が自組織にどのような影響を与えるか
 - ▶ 自社用IPv4が取得できなかった場合にどのようなインパクトがあるか
 - ▶ 機会損失も十分考慮
- ▶ コスト/リスクを総合して、現実的な対応案を決める
 - ▶ 導入する
 - ▶ → 稟議書と大日程作成
 - ▶ 先送り
 - ▶ リプレース時には IPv6 Ready製品をチョイス
 - ▶ ライフサイクルから再検討開始時期を決めておく

正攻法で攻める

- ▶ 危機感に訴える
- ▶ 機会損失に訴える

- ▶ 正攻法は**リスク分析**が物をいう

別の論点で攻める

- ▶ コストメリットに訴える
 - ▶ 別のキャリアや、同等の新品目を調査
 - ▶ キャリアのキャンペーンをチェック
- ▶ 制限緩和に訴える
 - ▶ フレッツ光NEXTは**接続端末台数制限**が外れている
 - ▶ 増速してより快適に
- ▶ 問題解消に訴える
 - ▶ グローバルIPv4アドレスが足りない
 - ▶ キャリアのトラブルが多い
 - ▶ 帯域不足

- ▶ 別の論点で攻める場合は、事前に**入念な調査**が物を言う

Bフレッツ vs フレッツ光NEXT(1)

比較項目	Bフレッツ	フレッツ光NEXT	備考
収容ネットワーク	フレッツ網	NGN網	フレッツ網(地域IP網)とNGN網は別収容となる
品質保証(QoS)	なし	あり	
通信方式	ベストエフォード	ベストエフォード+帯域確保(通信種類による)	
サービス品目	<ul style="list-style-type: none">・ハイパーファミリータイプ・マンションタイプ・ベーシックタイプ・ビジネスタイプ・エンタープライズタイプ・ワイヤレスアクセスタイプ(アドバンスドサポート)	<ul style="list-style-type: none">・ファミリータイプ・マンションタイプ・ビジネスタイプ	3タイプでの提供 ベーシック、ワイヤレスタイプはなし

NTT | フレッツ光ネクスト[Bフレッツとの比較] <http://www.isdn-info.co.jp/next/hikaku.html> より引用

Bフレッツ vs フレッツ光NEXT(2)

比較項目	Bフレッツ	フレッツ光NEXT	備考
マンション品目	<ul style="list-style-type: none">・ミニ(VDSL、LAN)・プラン1、2(VDSL、LAN)・ミニハイパー(光配線)・プラン1ハイパー(光配線)・プラン2ハイパー(VDSL、LAN、光配線)	プラン1、2、ミニ(VDSL、LAN、光配線)	
ユーザー通信速度	100Mbps	100Mbps ビジネスのみ概ね 1Gbps	
セッション数	ビジネスタイプ:4セッション その他の品目:2セッション	全品目2セッション	セッションの追加はオプション(有料)で提供
IPv6対応	フレッツドットネット経由で対応 ※H20.3よりBフレッツみ標準対応	標準対応	利用OS及び接続端末もIPv6に対応している必要あり

NTT | フレッツ光ネクスト[Bフレッツとの比較] <http://www.isdn-info.co.jp/next/hikaku.html> より引用

Bフレッツ vs フレッツ光NEXT(3)

比較項目	Bフレッツ	フレッツ光NEXT	備考
端末台数	<ul style="list-style-type: none">・ハイパーファミリー:5台・マンション:5台・ベーシック:10台・ビジネス:50台	制限なし	品目ごとの端末制限を撤廃
対応OS	<ul style="list-style-type: none">・Windows95以上・MacOS7~9	<ul style="list-style-type: none">・Windows2000以上・MacOS7~9	
契約料	800円(1契約ごと)	800円(1契約ごと)	Bフレッツからフレッツ光ネクストへの移行際の契約料は不要
月額利用料金	<ul style="list-style-type: none">・ハイパーファミリー:4,100円・マンション:2,500円~・ベーシック:9,000円・ビジネス:40,000円	現行Bフレッツと同等 ※ただし現行ベーシック品目はなし	
工事費用	<ul style="list-style-type: none">・基本工事費・交換機工事費等	Bフレッツと同じ	Bフレッツからフレッツ光ネクストへの移行工事費は有料 (工事費無料キャンペーンにより移転扱いの場合は無料)

NTT | フレッツ光ネクスト[Bフレッツとの比較] <http://www.isdn-info.co.jp/next/hikaku.html> より引用

Bフレッツ vs フレッツ光NEXT(4)

比較項目	Bフレッツ	フレッツ光NEXT	備考
オプション	・ひかり電話 ・フレッツ・ウイルスクリア	現行フレッツサービスをキャッチアップ及びNGN新サービスを提供	
利用接続端末	ONU、VDSL	NGN対応のONU、VDSL等で接続	

NTT | フレッツ光ネクスト[Bフレッツとの比較] <http://www.isdn-info.co.jp/next/hikaku.html> より引用

力技で押し切る

- ▶ これも時代の流れ
 - ▶ IPv4アドレス枯渇報道はあった
 - ▶ World IPv6 Dayも少し報道された
 - ▶ その他IPv6に関する報道は以前より増えている
 - ▶ IPv6対応製品の増加
- ▶ 先進性を内外へアピール
- ▶ 押切系は、押し切れるだけの**理論武装**が必要

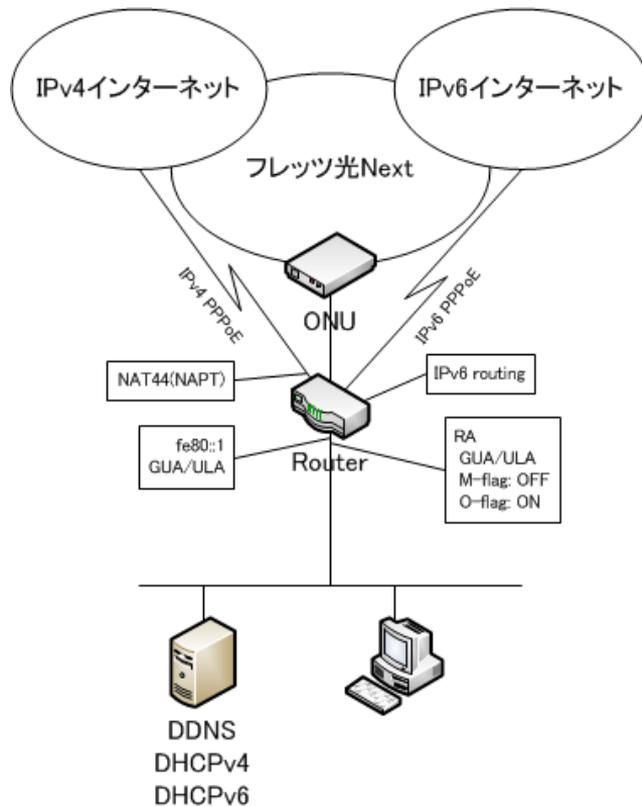
予算取り

- ▶ 予算/日程を稟議書にまとめて、いざ勝負!!
 - ▶ 根回し、寝技も大切かも?
 - ▶ 一度負けても、ここでくじけない!

4 回線開通/テスト導入

実環境でIPv6を実感する

テスト導入環境設計



回線開通/テスト導入

- ▶ 予算が取れたらまずは回線開通着手
- ▶ 回線が開いても、いきなり本番展開は危険
 - ▶ テスト導入で必ず評価
 - ▶ テスト導入環境でしばらくテスト運用をしてノウハウチャージ

5 設計

プレフィックス設計

- ▶ 基本的にIPv4の設計と同じ
 - ▶ IPなので考え方は一緒
 - ▶ 台帳を作っておかないと後で必ず泣きを見る
- ▶ 単純スター/リニア型
 - ▶ 必要に応じて/64を順番に振り出す
- ▶ ツリー型
 - ▶ 末端から必要セグメント数を積み上げる
 - ▶ ツリー元に対してプレフィックスを割当て
 - ▶ 枝に進むごとに設計したプレフィックスを割当て
 - ▶ 末端に/64を割当て

インターフェイスIDの割り当てルール例

- ▶ IPv4アドレスを流用する
 - ▶ 192.168.0.1 → プレフィックス:192:168:0:1
- ▶ プロトコル番号を使う
 - ▶ Webサーバー: プレフィックス::80
- ▶ 意味付けする
 - ▶ 16進なのでa~fが使える
 - ▶ ドメインコントローラー: プレフィックス::ad01
- ▶ 一定のルールを決める
 - ▶ プリンタ: プレフィックス::ff01
 - ▶ 中継装置: プレフィックス::1
- ▶ 奇をてらって?
 - ▶ プレフィックス::beef
 - ▶ プレフィックス::cafe

インターフェイスID体系例

ノード	インターフェイスID
中継装置	プレフィックス::1~
ドメインコントローラ	プレフィックス::ad01
Webサーバー	プレフィックス::cafe
DNSサーバー	プレフィックス::53
メールサーバー	プレフィックス::25
プリンタ	プレフィックス::f001
クライアント	自動構成

GUA/ULAの割り当て

- ▶ DMZ: GUA
- ▶ サーバーセグメント: GUA+ULA
- ▶ クライアントセグメント: GUA+ULA

RAの要否

- ▶ DMZ: 不要
- ▶ サーバーセグメント: 必要
- ▶ クライアントセグメント: 必要

セキュリティが必要なセグメント

- セグメント単位にポリシーを設計
- **ICMP**を止める場合は、**タイプ**を見極めて!!!

DMZポリシー例

- ▶ インターネット側からのインバウンド
 - ▶ 公開サービスとICMPをPass
- ▶ インターネット側へのアウトバウンド
 - ▶ 必要サービスとICMPをPass
- ▶ 内部セグメントからのインバウンド
 - ▶ 必要サービスとICMPのみPass
- ▶ 内部セグメントへのアウトバウンド
 - ▶ 必要サービスとICMPをPass

セキュアセグメントポリシー例

- ▶ アクセス許可セグメントからインバウンド
 - ▶ 許可サービスとICMPをPass
- ▶ アクセス許可セグメントへのアウトバウンド
 - ▶ 許可サービスとICMPをPass

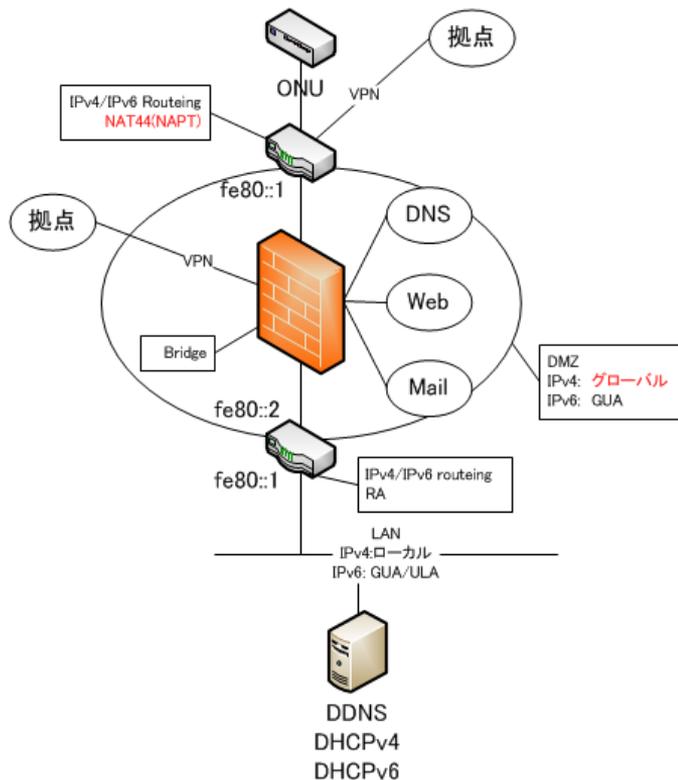
クライアントセグメントポリシー例

- ▶ インターネットへのアウトバウンド
 - ▶ 許可サービスとICMPをPass
- ▶ インターネットからのインバウンド
 - ▶ ICMPのみPass

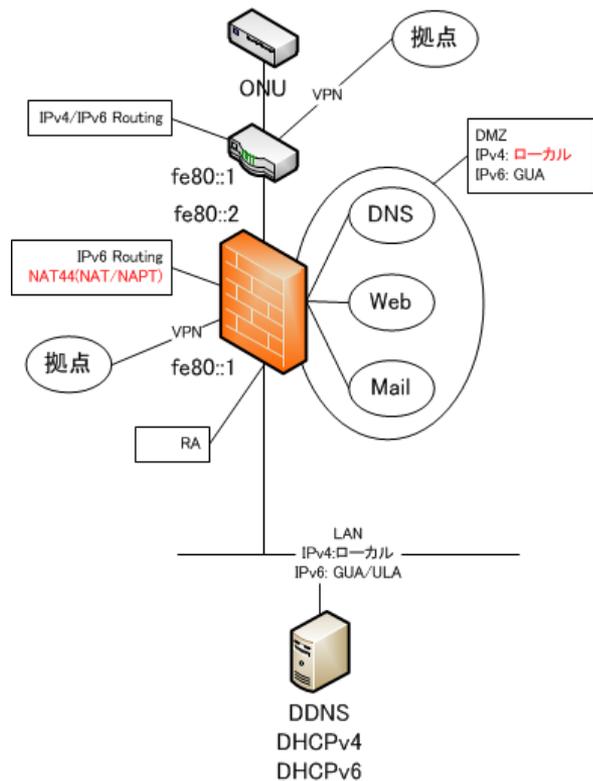
インターネット境界とDMZ設計

- ▶ **PPPoEの実装位置**
 - ▶ インターネット境界
- ▶ **NAT44の実装位置**
 - ▶ DMZが**NAT**方式なら**ファイアウォール**
 - ▶ DMZが**ブリッジ**方式なら**インターネット境界**
- ▶ **インターネット境界**
 - ▶ テスト設計がそのまま使えるはず
- ▶ **NGN内部をアクセスするか?**
 - ▶ 個人的には不要論者
- ▶ **DMZの方針**
 - ▶ NAT方式にするかブリッジ方式にするか
- ▶ **LAN境界**
 - ▶ DMZを**ブリッジ**方式にするのなら**LAN境界が必要**

ブリッジ方式の設計例



NAT方式の設計例



名前解決

- ▶ DHCPv6リレーでDNSを指定
- ▶ IPv4で名前解決
 - ▶ IPv4でAAAAを引いても問題なし
- ▶ 手動でDNSのIPv6アドレスを指定するのはトラブルの元
- ▶ 512オクテットを超える事があるので、DNSのEDNS0をONに
 - ▶ ファイアウォール等もEDNS0対応が必要

DHCPv6リレーの要否

- ▶ DMZ: 不要
- ▶ クライアントセグメント
 - ▶ DHCPv6でDNSを指定: 必要
 - ▶ IPv4で名前解決: 不要

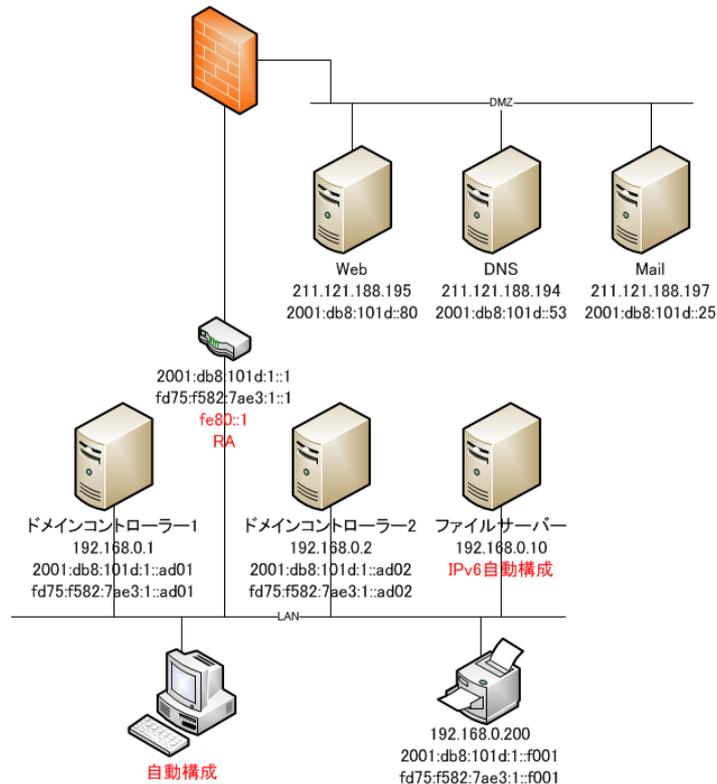
DHCPv6か固定IPアドレスか

- ▶ 基本は**自動構成**
- ▶ 固定アドレスが必要なノードは手動設定
- ▶ DDNSに自動登録されないノードは手動設定

匿名アドレスの注意点

- ▶ 匿名アドレスは**DDNSに登録されない**
- ▶ IPv6アドレスから**ホスト名の逆引き**が必要な時は匿名アドレスをOFF
 - ▶ netsh で匿名アドレス(一時IPv6アドレス)を止める
 - ▶ ステートフル DHCPv6 で自動構成(未検証 ^^;)

セグメント設計例



VPN

- ▶ 接続先セキュリティゲートウェイは名前で指定
- ▶ IPv6アドレス指定しないといけない場合はTypoに注意

拠点

- ▶ WAN自体をデュアルスタック対応にする
- ▶ 拠点内をデュアルスタックにする

- ▶ WAN自体がデュアルスタック対応になっていなくても工夫次第で何とかなる
 - ▶ 6over4とかIPsecでトンネルの内側をデュアルスタック化

モバイル

- ▶ 使用している回線がLSNなのか確認
- ▶ IPv6が提供されている環境ならIPv6で接続を優先に
- ▶ IPv6が供給されておらず、IPv4でVPNプロトコルが通らないのならキャリア変更

6 展開

DMZ移行を乗り切ればあとは簡単
展開は計画的に

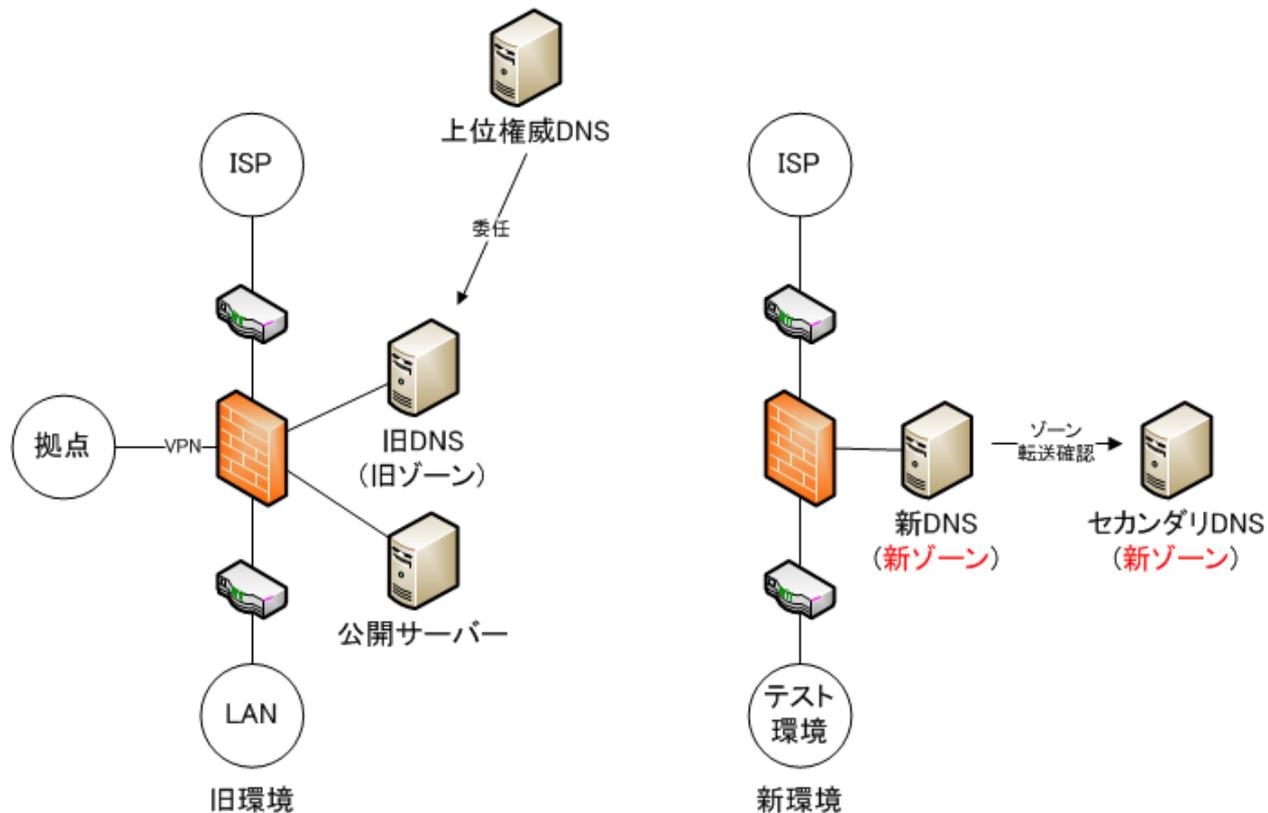
DMZ移行計画

- ▶ 新設廃止の方がトラブルは少ない
 - ▶ ただし、IPv4アドレスが必要数取得できるのなら
- ▶ 名前解決空白時間対策はTTL値を小さくして対応
- ▶ リスクを極力回避するのなら、IPv4アドレスのリナンバーが発生しないようにする
 - ▶ 6over4
 - ▶ IPv6回線追加

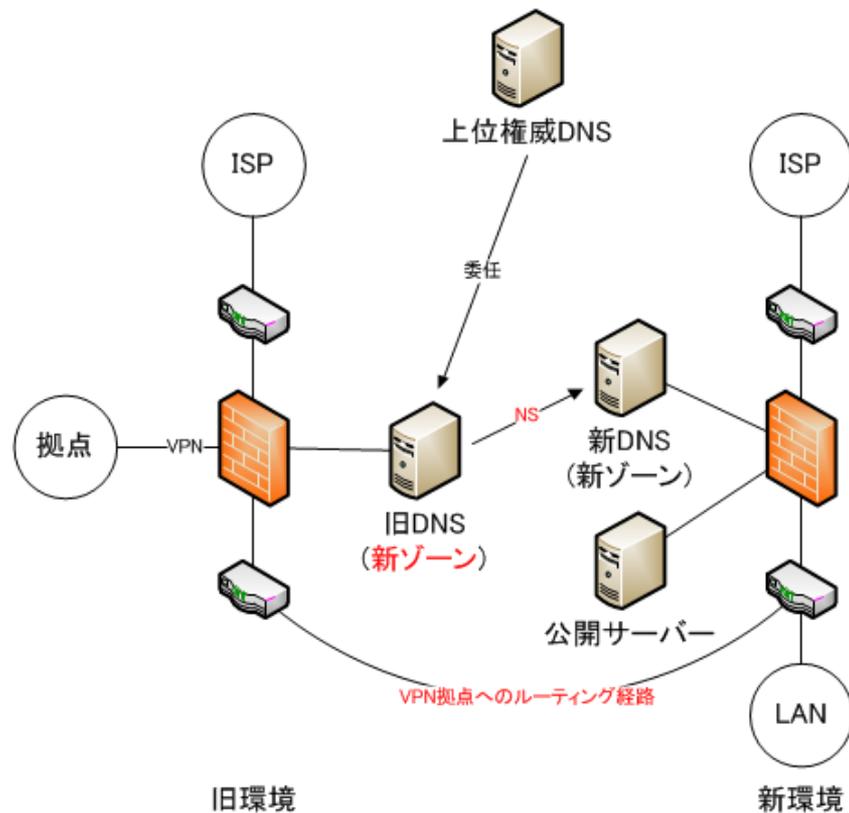
回線新設廃止 / ISP変更のDNZ移行例

- ▶ 新回線開通
 - ▶ 通信機器設置
 - ▶ 通信確認
 - ▶ 新回線側にDNS設置(新ゾーン情報)
 - ▶ セカンダリDNSゾーン転送確認
- ▶ DMZ 移行
 - ▶ DMZ 機器を新回線側に移設
 - ▶ 旧DNSゾーン情報を新ゾーン情報に書き換え、NSを新DNSに向ける
- ▶ レジストラトランスファー
 - ▶ 上位権威DNSの委譲を新回線側のDNSへ変更
- ▶ VPN移行
 - ▶ VPN拠点を新回線側に収容替え
- ▶ 旧回線廃止
 - ▶ 旧契約解除
 - ▶ 旧回線廃止

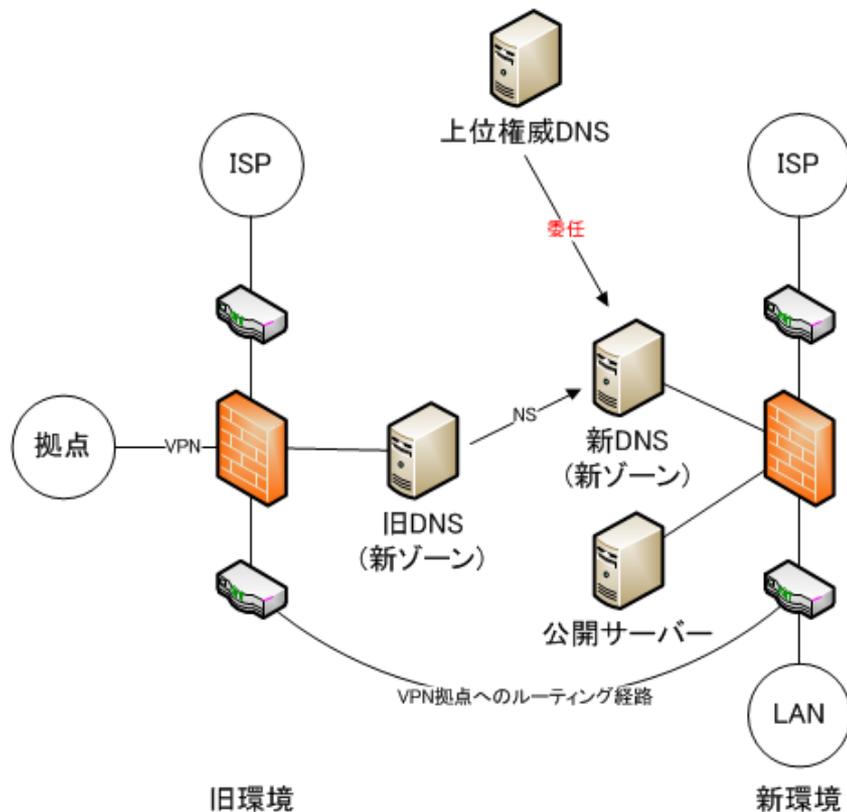
新回線開通



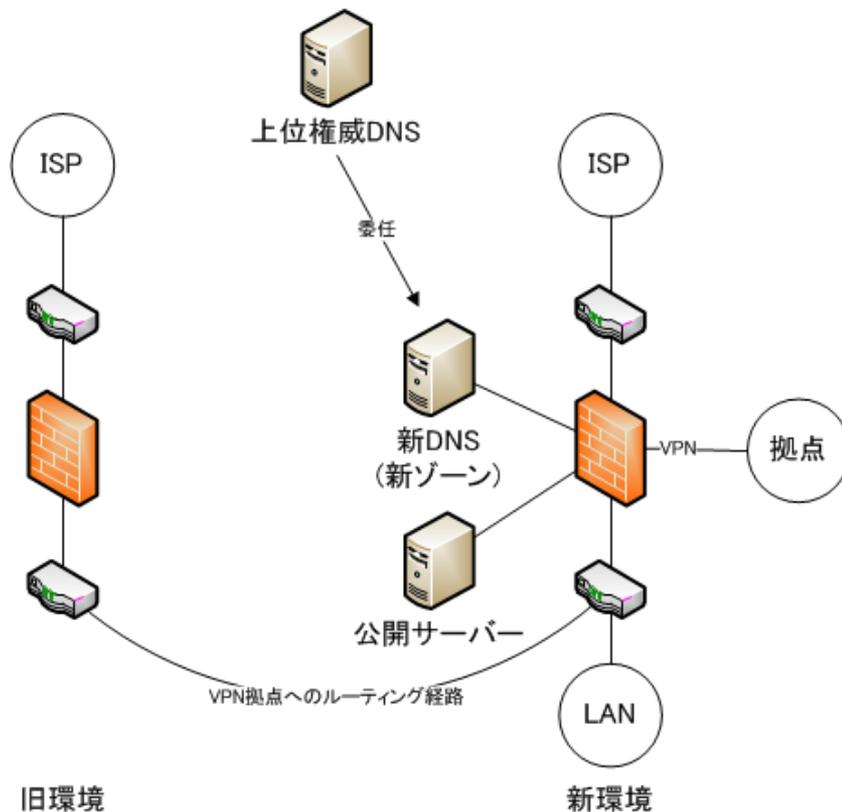
DMZ移行



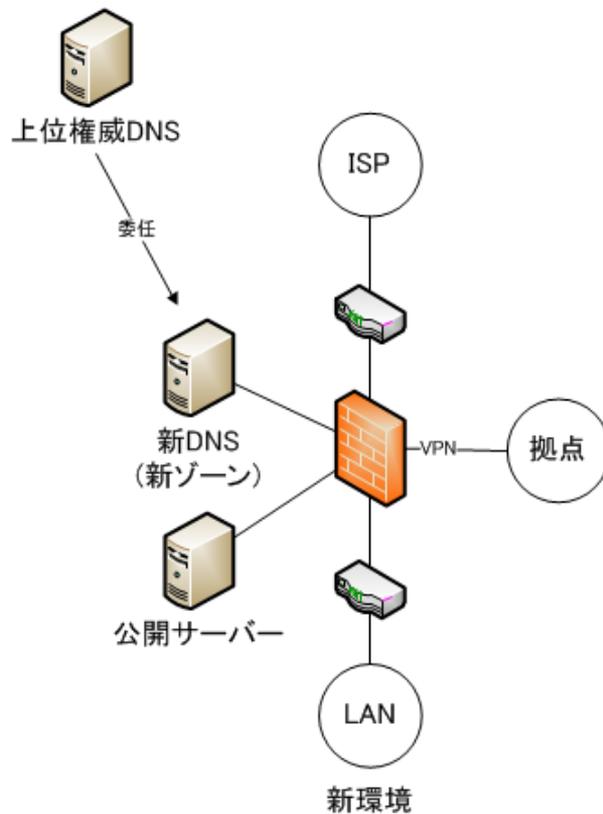
レジストラトランスファー



旧DNS撤去とVPN收容替え



旧回線廃止



展開実施

- ▶ 計画に基づいて順次展開
- ▶ 展開の都度問題が起きていないかしばらく見守る
- ▶ パフォーマンスがちゃんと出ているか確認

- ▶ 一気に展開するのではなく、段階的に

評価

- ▶ 使い勝手やパフォーマンスについてヒヤリング実施
 - ▶ 利用者がIPv6導入に気が付かないのがベスト
- ▶ 障害が起きていないか、しばらく注視
- ▶ 各ノードの状態監視

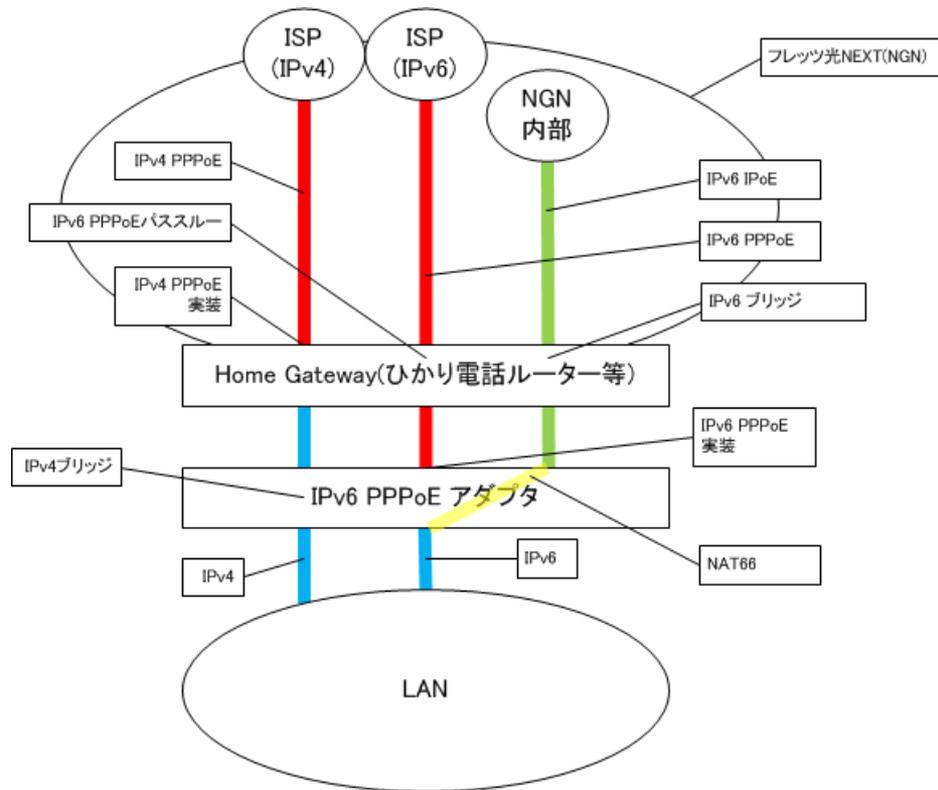
運用

- ▶ アドレス/プレフィックス管理台帳更新を確実に実施
- ▶ トラブルが発生したら、症状/原因/対応の詳細を記録し、
ノウハウを残す

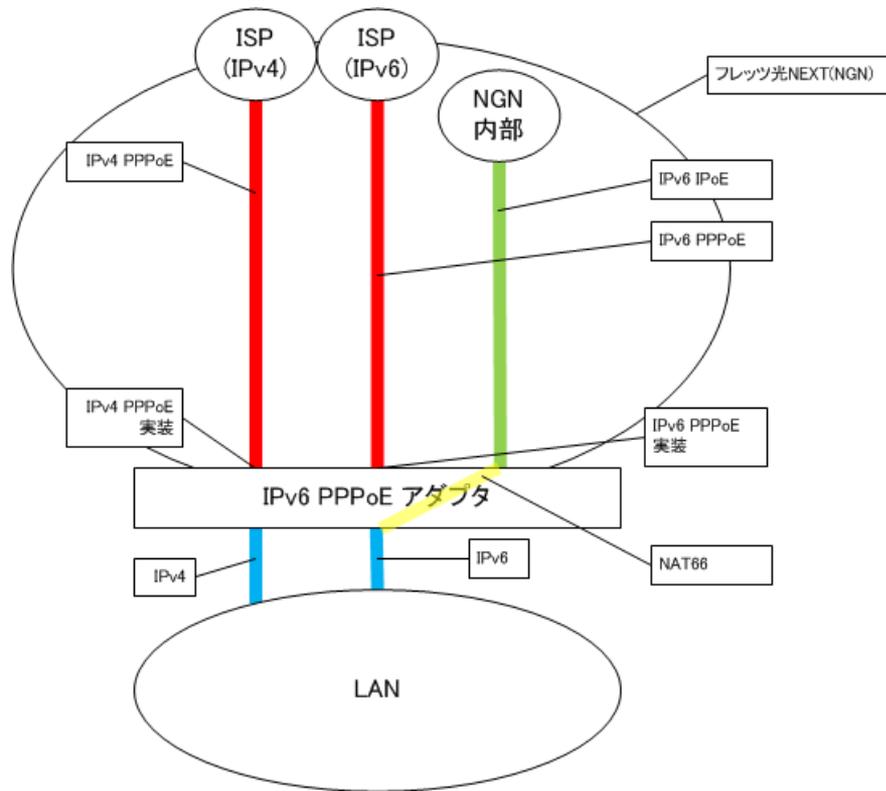
台帳サンプル

SOHO / 個人宅への IPv6 導入

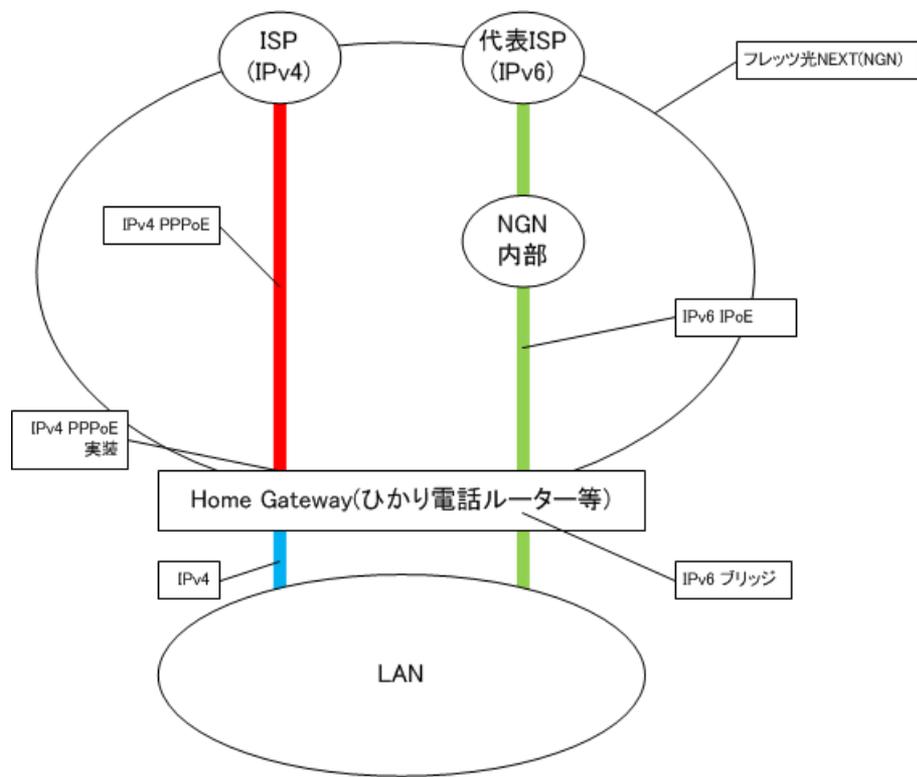
IPv6 PPPoE(HGW+IPv6 PPPoEアダプタ)



IPv6 PPPoE(IPv6 PPPoEアダプタ)



IPv6 IPoE(HGW)



まとめ

IPv6の実装

- ▶ 基本はデュアルスタック
- ▶ ノードにはGUAとULAの両方を割り当てる
- ▶ ICMPは止めない
- ▶ IPv6のDHCPはRAとセット
- ▶ デフォルトゲートウェイにはfe80::1
- ▶ DMZポリシーはセグメント単位で考える
- ▶ 全てのノードをIPv6対応にする必要は無い

導入の流れ

1. 回線開通
2. 試験運用
3. DMZへの導入
4. LANへの導入
5. 拠点展開/モバイル対応

MURAからの提言

- ▶ グローバルIPv4アドレスが入手不能になるのは**時間の問題**
- ▶ 漠然と考えるのではなく、グローバルIPv4アドレスが入手できない場合や、IPv6を導入しない場合の**リスク分析を早々に済ませ、その結論に基づいた導入時期や方針を見定めて下さい!!**

Q&A