【今さら聞けないQ&Aコーナー：応用編】

企業ネットの対策：どこからどう手を付ける？

2011年10月13日

IPv4アドレス枯渇対応タスクフォース

パネリスト紹介

荒野　高志（あらの　たかし）

IPv6普及・高度化推進協議会　常務理事

日本ネットワークインフォメーションセンター　理事（IPv6担当）

ITホールディングス　執行役員　事業推進本部長

今井　恵一（いまい　けいいち）

社団法人　テレコムサービス協会　政策委員会委員長

NEC　プラットフォームマーケティング戦略本部　エグゼクティブエキスパート

企業ネットの対策：どこからどう手を付ける？

Q1: IPv4アドレス枯渇後、これからのインターネットはどうなる？

Q2: IPv4アドレス枯渇が、企業ネットワークに与える直接の影響は？

Q3:企業の公開サーバ、DMZをIPv6対応しないと何が困る？

Q4:企業の公開サーバ、DMZのIPv6対応はいつまでに必要か？

Q5:企業のDMZのIPv6対応って具体的にはどうすればいい？

Q6: IPv6対応した場合、セキュリティ面の問題はないの？

Q7: 企業網のイントラネット内部はIPv6対応しなくていいの？

Q8: 企業網にIPv6を導入するとどういうメリットがあるの？

Q9: 現在調達できる機器やソフトウェアはIPv6対応してるの？

Q10: 企業の場合、IPv6アドレスはどこから調達すればいいの？

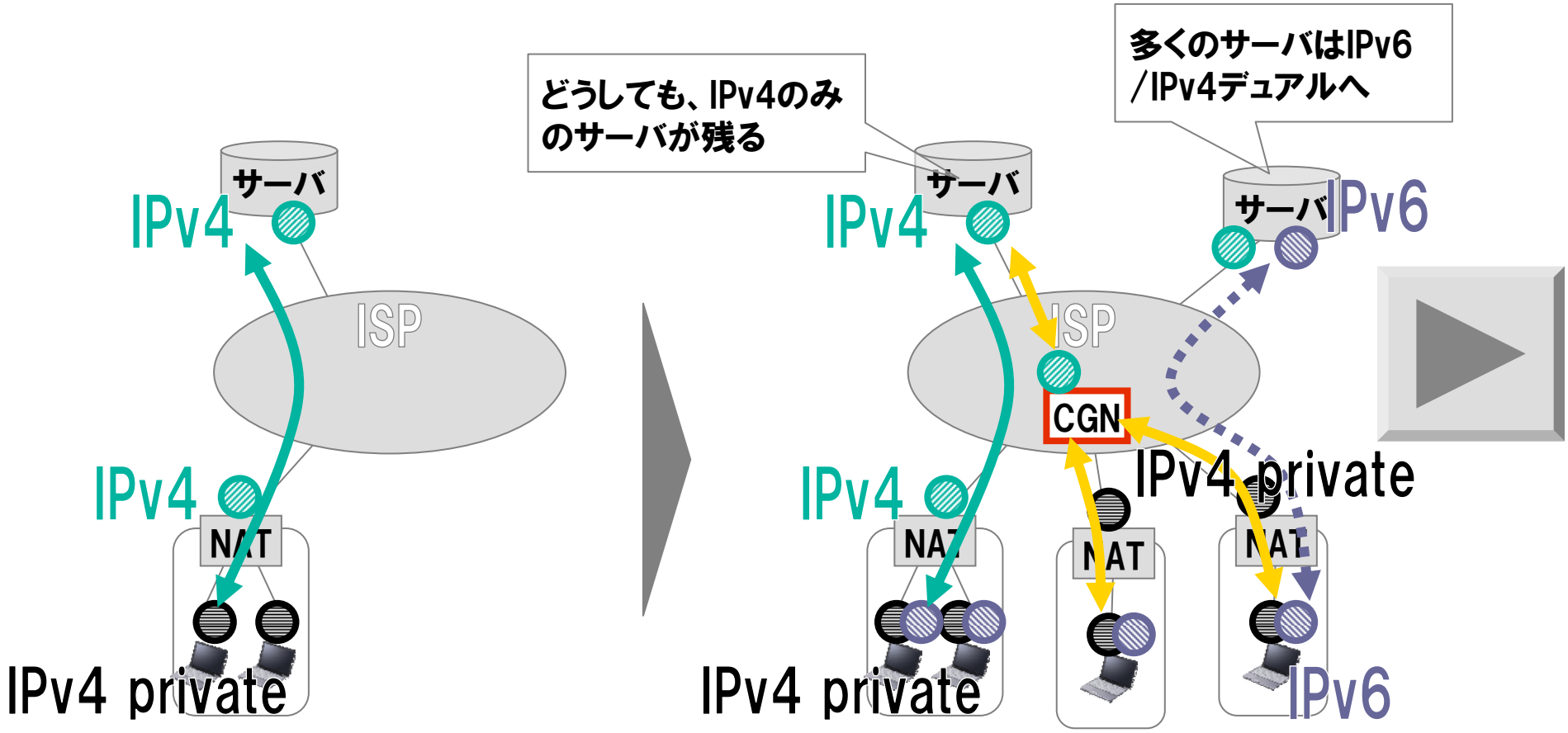
Q1

Q1: IPv4アドレス枯渇後、これからのインターネットはどうなる?

- ISPは新規ユーザにIPv4（グローバル）アドレスを配れなくなる。
- IPv6アドレスとIPv4プライベートアドレスを配り、インターネット上のIPv4のサーバにはCGN経由で接続することになる。
- このCGN経由の接続は結構制約が多いので、次第にIPv6での接続の方が多くなりそう。

IPv4アドレスが枯渇すると ISPは・・・

- **ISPはIPv6/IPv4デュアルのサービスへ移行**
  - **➔在庫枯渇後は、IPv6アドレス＋IPv4プライベートアドレスを割り当てる**



CGN: Carrier Grade NAT (Network Address Translator)

しかし、制約があるCGN経由のアクセス

- 以下のような制約あり

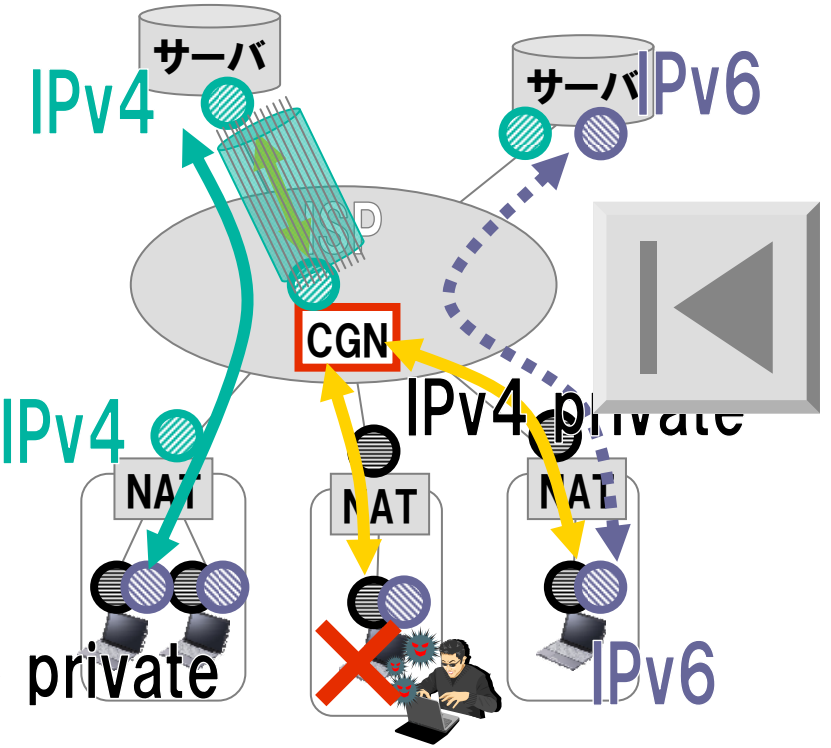
→IPv4アドレスを共有するユーザ間で
同時接続セッション数に制限

→サーバ側では、IPアドレスだけでは
通信相手を識別できない

→通信ログにIPアドレス＋ポート番号
を格納する必要あり

⇒ 正常にWeb画面が
表示されないケースあり

⇒ 悪意のあるユーザの
特定に手間がかかる



CGN: Carrier Grade NAT (Network Address Translator)

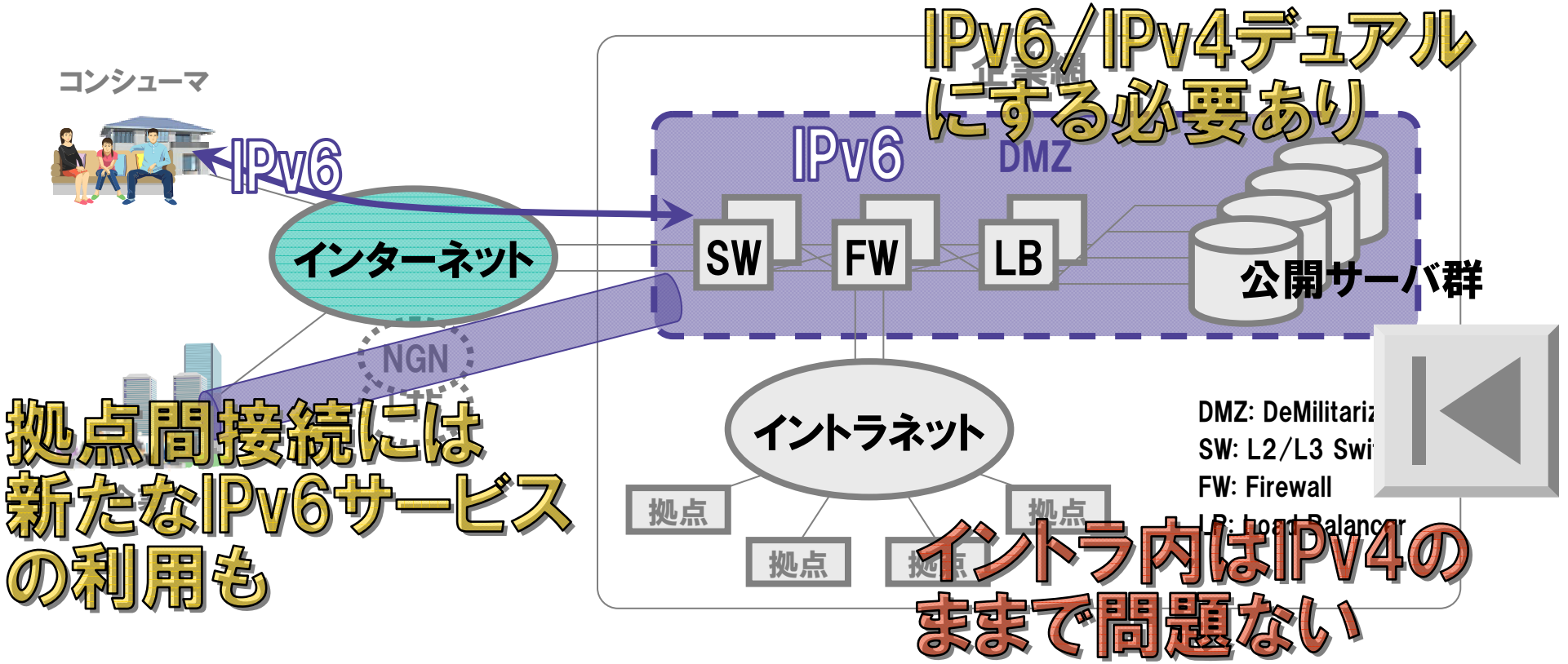
Q2

Q2: IPv4アドレス枯渇が、企業ネットワークに与える直接の影響は?

- 企業内のネットワークは、普通IPv4プライベートアドレスを使うので、イントラネット内についてはすぐに直接的な影響はない。
- ただし、インターネット自体は今後IPv6/IPv4デュアルの構成になるので、企業網のインターネット接続部分については影響を受ける。

IPv4アドレスが枯渇すると 企業網は・・・

- 企業の公開サーバとDMZのIPv6対応は必要
  - →コンシューマを中心にインターネットからIPv6でアクセスするユーザが出現



Q3

Q3: 企業の公開サーバ、 DMZをIPv6対応しないと何が困る?

- 公開サーバをIPv4のままにしておくと、CGN経由で接続するユーザが出てくる。その場合、ユーザにも制約があるし、サーバ側でもいくつか問題が出てくる。
- 単純なWebサーバはともかく、ECサイトのようなサーバは早めの対処が必要。

しかし、制約があるCGN経由のアクセス

- 以下のような制約あり

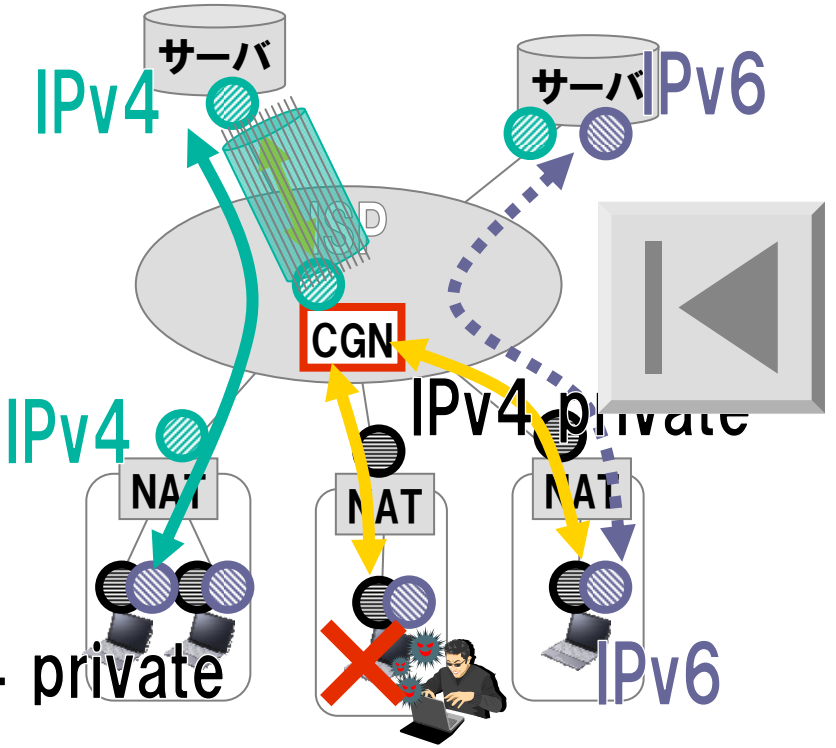
→IPv4アドレスを共有するユーザ間で同時接続セッション数に制限

→サーバ側では、IPアドレスだけでは通信相手を識別できない

→通信ログにIPアドレス＋ポート番号を格納する必要あり

⇒ 悪意のあるユーザの特定に手間がかかる

⇒ 正常にWeb画面が表示されないケースあり



CGN: Carrier Grade NAT (Network Address Translator)

Q4

Q4: 企業の公開サーバ、 DMZのIPv6対応はいつまでに必要か？

- ISPのIPv4アドレス在庫がなくなる時（≒CGN経由のアクセスが発生する時）までに必要。
- 在庫に余裕の少ないISPの場合、APNIC枯渇（2011年5月）の1年後とも言われている。日本より、アジアで先になくなりそう。
- 今後、ISPが節約しながら使っても、2012年はともかく2013年にはなくなるかも・・・

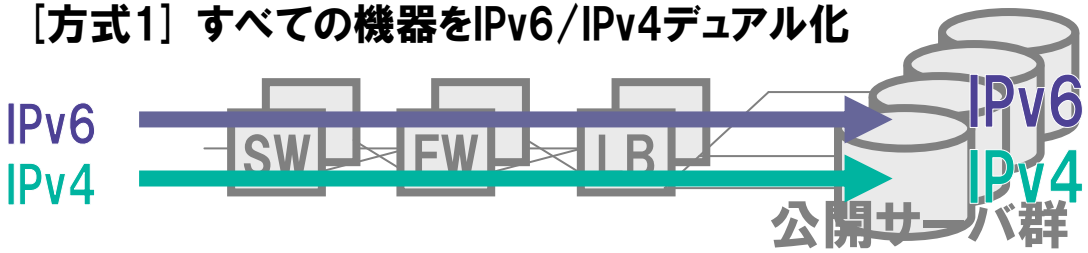
Q5

Q5: 企業のDMZのIPv6対応って具体的にはどうすればいい?

- 究極的にはDMZ内のすべての機器（ルータ/スイッチ、ファイアウォール、ロードバランサー、各種のセキュリティ機器、Webサーバなど）をIPv6/IPv4デュアルにすべき。
- ロードバランサーでIPv6/IPv4変換し、公開サーバ自身はIPv4のままという構成もありうる。
- 暫定対処ならReverse Proxyという手も・・・

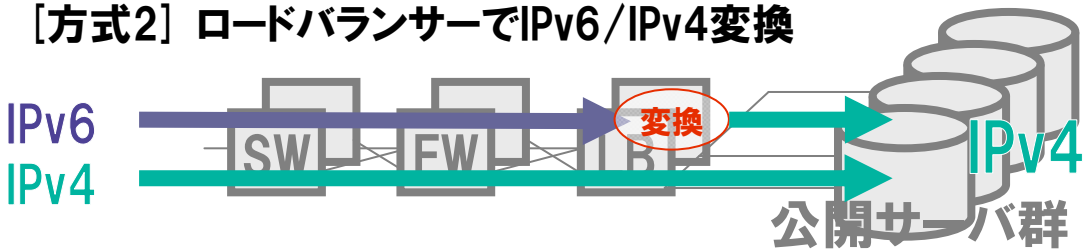
公開サーバおよびDMZのIPv6対応の実現方式

[方式1] すべての機器をIPv6/IPv4デュアル化



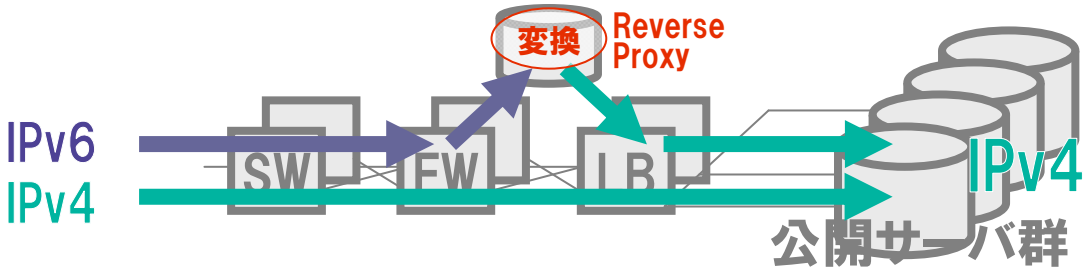
○最もシンプルな構成であり、究極的にはこの方式にすべき
×新規のサーバであればよいが、稼働中のサーバをIPv6/IPv4デュアル化するのはリスクも伴う

[方式2] ロードバランサーでIPv6/IPv4変換



○公開サーバはIPv4のままでよい
×サーバ上のAPLで通信相手をIPアドレスで識別している場合はAPLの改造が必要となる
×LBの変換機能に不具合があった場合、IPv4のトラヒックに影響を与える恐れがある

[方式3] リバースプロキシを導入



○公開サーバはIPv4のままでよい
×サーバ上のAPLで通信相手をIPアドレスで識別している場合はAPLの改造が必要となる
○Reverse Proxyに不具合が生じても、IPv4のトラヒックには影響を与えない
×IPv6のトラヒックが増えるとReverse Proxyも増設が必要になる

- 究極的には[方式1]にすべきだが、単純なWebサーバ(通信相手のIPアドレスを管理しない)であれば、簡易的な[方式2]または[方式3]でも実現可能

Q6

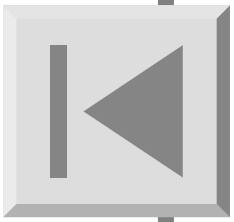
Q6: IPv6対応した場合、セキュリティ面の問題はないの？

- 基本的にはIPv4と同じようなセキュリティ対策をIPv6にも施せばよく、ことさらIPv6が危険というわけではない。
- ただし、現状ではIPv6でのセキュリティ面の運用ノウハウが必ずしも十分でない面はある。
- これは、今後習熟させていくしかない。

Q7

Q7: 企業網のイントラネット内部はIPv6対応しなくていいの?

- IPv4のみの時よりメンテナンスのコストは上がるので、それを上回るメリットがあるかどうかという話になる。
- 今は、メリットがあるケースは少ないかも・・・
- ただし、今後調達する機器、ソフトはIPv6対応のものにするべき。



Q8

Q8: 企業網にIPv6を導入するとどういうメリットがあるの?

➔メリットとして考えられるのは、

- イントラ内でのIPマルチキャストの利用
- グループ会社間のNAT経由しない(TV会議などの)PtoP通信
- 会社のM&Aなどによるネットワークの統合

などか・・・

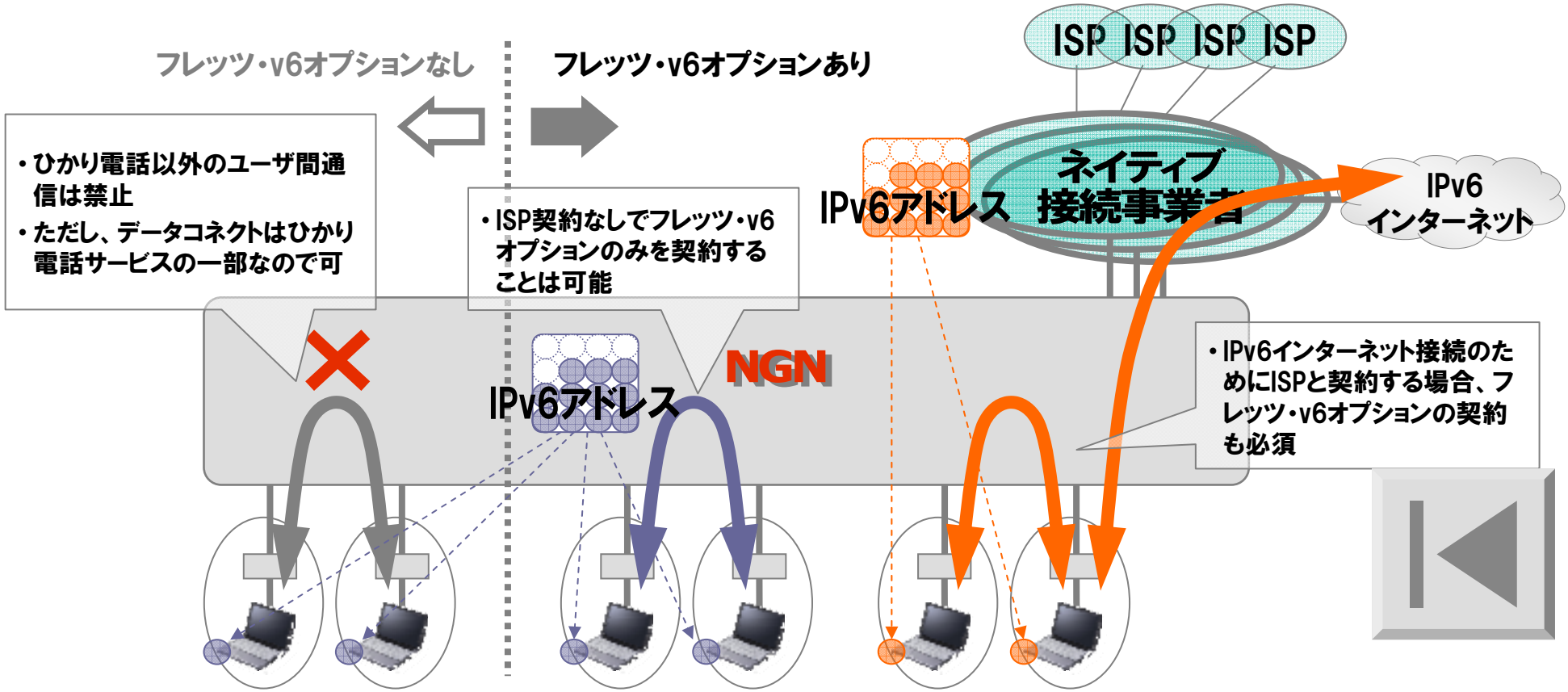
➔IPv6だけで提供される新たなサービスもある・・・

NGN内の折り返し通信機能（フレッツ・v6オプション）

NTT東西は、IPv6 IPoE接続と共に「フレッツ・v6オプション」サービスを開始

- 網内でのUNI-UNI間折り返し通信が可能
- ベストエフォートだが、100Mbps以上の通信速度を期待

工事費：2,000円が必要だが、月額利用料は不要



Q9

Q9: 現在調達できる機器やソフトウェアはIPv6対応してるの?

- 企業網に入れるルータ、スイッチなどのネットワーク機器、およびサーバのOSなどは、ほとんどのものがIPv6対応している。
- 最近では、ファイアウォールやロードバランサーなどの機器もIPv6対応しているものが多い。
- アプリケーションソフトについては、本来IPアドレスに依存しないものが多いが・・・

Q10

Q10: 企業の場合、IPv6アドレスはどこから調達すればいいの?

- ISPから調達するのが最も簡単。
- ただし、ISPを変更するとIPv6アドレスも変わってしまうことになる。
- 企業が自らAPNIC/JPNICにIPv6アドレスを申請することも可能。その場合は、接続するISPとの間でルーチングプロトコル等のやり取りが必要。

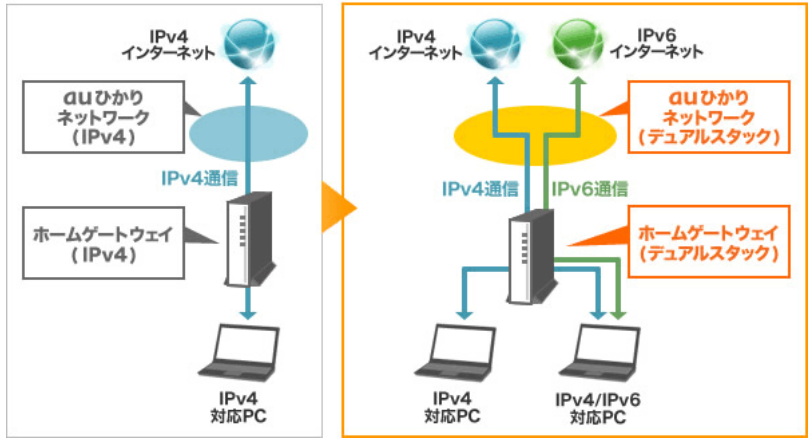
既に始まっているIPv6サービス　KDDIでは

- KDDI、『auひかり』でIPv6アドレス配布を開始
  - ➔関東エリアで2011年4月以降にIPv6アドレスの配布を開始し、既に完了

加入者の申し込み不要で、追加料金もなし!!

ユーザが気づかないうちにIPv6へ!!

■IPv4/IPv6デュアルスタック方式イメージ図



http://www.auhikari.jp/news/110418.html