

ほっといたらIPv4運用に影響する IPv6の話

アンカーテクノロジー株式会社
國武 功一

そろそろIPv6の足音が (いや、まじで)

- IPv6アドレス取得国は100カ国を超えた。
- GoogleもIPv6アドレスを取得済
- IPv6アドレスの取得率からいうと日本は一位の座からとっくに滑り落ちてる
- そろそろ本当にIPv4アドレスがやばいらしい
- IETFではすでにIPv6を特別扱いしてない (なにとも言わなくても、IPv4/IPv6共に考慮される)

IPv6というかVistaが来ますよ？

- 最初からIPv6対応 (らしい)
- IPv6をuninstallできない (らしい)
- IPv4 onlyでは動かせない (らしい)
- むしろIPv6 onlyで動く (らしい)
- IPv4/IPv6どちらもモウマンタイ (らしい) ？

ほんとうのところはどうなの？

いやーでもおれ関係ないし.....

- エンジニアは、ユーザにとってはラストリゾルト、デフォルトルート
- ユーザは、みなさんに「知らん」といわれたら、それまで (涙)
- IPv6を使うことになる可能性が残っている限り、それに備えるのがエンジニア
- じゃあなにをどう備えるべきなの？

今回の主題

やっぱり俺には関係ないんじゃない？

- ユーザがIPv6ノードを利用したと、IPv4運用にも影響を及ぼす可能性があるかも
- 今日の議論でその点を確認し、備えておこう。

本発表では、いかに現状のサービスに影響を与えないようにするか、にフォーカスする。

~~あのひとは今~~IPv6問題点おさらい

- TCPコネクション確立問題
- DNSリゾルバ問題
- DNSサーバ問題
- IPv6仕様不備問題(onlink assumption)
- パケットフィルタリング問題
- Webベース認証システム問題

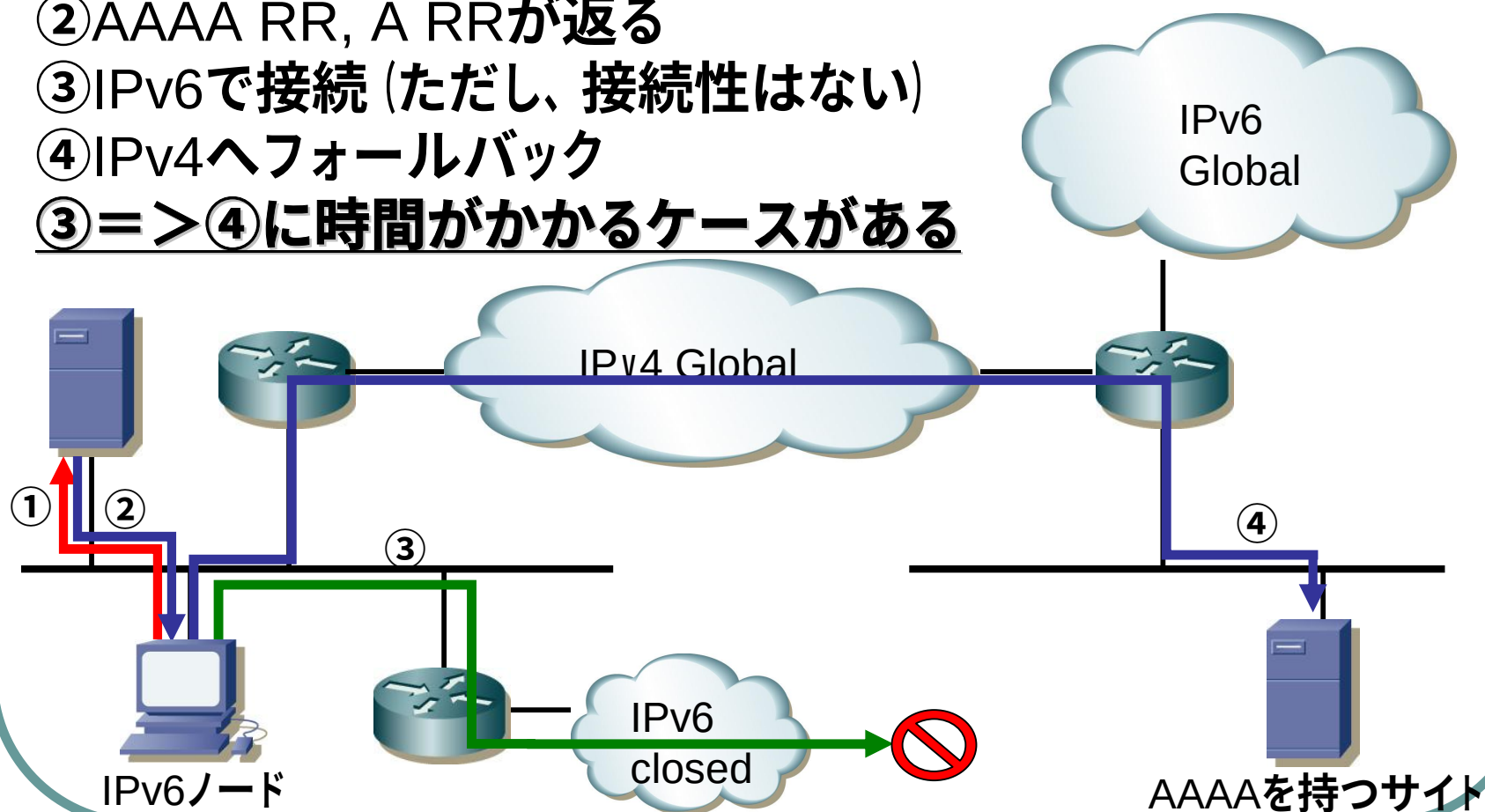
TCPコネクション確立問題

● 概要

- 通常の利用では問題ないが、顧客が某フレッツドットネットや光プレミアムなど、IPv6のグローバルアドレス空間を閉鎖網として利用している場合、AAAAを登録しているサイトへの到達性がないため、IPv4へフォールバックするまで、時間がかかる場合がある。
- 本議論とは話がずれるが、同様にIPv6を閉鎖網として使おうと思っている場合には注意（この点は、IPv4を閉鎖網として使う場合と同様）

TCPコネクション確立問題 (Cont)

- ①アドレスを引く
 - ②AAAA RR, A RRが返る
 - ③IPv6で接続 (ただし、接続性はない)
 - ④IPv4へフォールバック
- ③=>④に時間がかかるケースがある



ちょっとまで

- AAAAってなに？
 - DNSのレコードのひとつで、IPv6アドレスが格納される。

www.example.com.	IN	A	192.0.2.1
mail.example.com.	IN	A	192.0.2.1
	IN	AAAA	2001:db8::1

TCPコネクション確立問題 (Cont)

- **なにが問題か？**
 - 閉鎖網からICMPv6 Destination Unreachableが返らない環境がある
 - Personal Firewall に阻まれるなどして、クライアントがICMPv6 Destination Unreachableを受け取らない
 - ICMPv6エラーのハンドリングに関するクライアント側の実装、挙動などが統一されておらず、あまりよくない。
- **影響を受ける人**
 - フレッツドットネットや光プレミアムなどを、IPv4のサービスと平行して使おうとしているユーザ

詳細は、JANOG17 IPv4/IPv6フォールバックの現状を参照

TCPコネクション確立問題 (Cont)

- 閉鎖網からのICMPv6 Destination Unreachable 応答に関して検証してみた。
但し、幅広く検証するのは大変なので
以下のように限定的な環境のみで実施。😊
- フレッツドットネット
 - 東京のとあるドットネット回線にて、7月に実施。
- フレッツ光プレミアム
 - 静岡のとある光プレミアム回線にて、7月に実施。

TCPコネクション確立問題 (Cont)

- フレッツドットネットは
ICMPv6 Destination Unreachableを返した。
 - 技術参考資料には、
“ICMPv6をサポートする”と記載されている
 - NTT東日本 IP通信網サービスのインタフェース
フレッツシリーズ <付加サービス編> (第9版) P.102 [2.1.3]
http://flets.com/pdf/flets_add.pdf

TCPコネクション確立問題 (Cont)

- **フレッツ光プレミアムは
ICMPv6 Destination Unreachableを
返さなかった。**
 - 技術参考資料には、
“IP通信網内に存在しない宛先に送信されるパケット
については、IP通信網内において応答なくパケット破棄
される場合があります”と記載されている。
 - NTT西日本 IP通信網サービスのインタフェース
フレッツシリーズ (第24版) P.63 [4.5.4]
http://www.ntt-west.co.jp/flets/siryou/gijyutsu_sankou.pdf

(参考) 光プレミアム よくあるご質問より

Q. 特定ホームページの表示が遅い。

A. インターネット上には、IPv6とIPv4の両方で公開されているホームページが一部存在しており、このようなホームページへアクセスする場合には、初回表示に数十秒かかる可能性がありますのでご了承ください。なお、初回表示以降は端末のキャッシュ機能により表示遅延はなくなると考えられます。

TCPコネクション確立問題

- 対応策（パーフェクトな対策ではない）
 - 上流ルータ側で、ICMPv6 Destination Unreachable を返し、IPv4へのフォールバックを促す。
 - またクライアントはそのICMPv6 Destination Unreachableを確実に受け取ること。
 - Firewallの設定、間違っていないよね？

TCPコネクション確立問題

Windows Vistaではどうなの？

TCPコネクション確立問題 (Cont)

- IPv6閉鎖網を利用したサービスを提供しているISPがICMPv6 Destination Unreachableを返しても、クライアントの実装がまずい場合も？
 - 本質は、TCP仕様に起因
 - 複数アドレス持つことを想定していなかった？
 - コネクション確立時に限り、素早くフォールバックする手法もあるが。。。
 - draft-gont-tcpm-tcp-soft-errors-02.txt (September 2005)

詳細は、JANOG17 IPv4/IPv6フォールバックの現状を参照

閉域IPv6網TIPS

- **TCP接続でIPv6のタイムアウト待ちをなくしたい=>IPv4接続を優先する**
 - IPv6対応OSでは通常IPv6接続が優先
 - RFC3484 (Default Address Selection) の仕組みを利用
 - IPv4 (IPv4射影IPv6アドレス) の優先度を上げる
 - getaddrinfoの戻り値がポリシの順にソートされる
 - 実装OS: Windows XP、Windows Vista、FreeBSD

Windows XP

- netshコマンドにてIPv4優先設定

```
> netsh interface ipv6 set prefixpolicy ::ffff:0:0/96 50 0  
> netsh interface ipv6 set prefixpolicy ::1/128 40 1  
> netsh interface ipv6 set prefixpolicy ::/0 30 2  
> netsh interface ipv6 set prefixpolicy 2002::/16 20 3  
> netsh interface ipv6 set prefixpolicy ::/96 10 4  
> netsh interface ipv6 set prefixpolicy 3ffe:831f::/32 5 5
```

Windows Vista

● netshコマンドにてIPv4優先設定

```
> netsh interface ipv6 set prefixpolicy ::ffff:0:0/96 50 0  
> netsh interface ipv6 add prefixpolicy ::1/128 40 1  
> netsh interface ipv6 add prefixpolicy ::/0 30 2  
> netsh interface ipv6 add prefixpolicy 2002::/16 20 3  
> netsh interface ipv6 add prefixpolicy ::/96 10 4  
> netsh interface ipv6 add prefixpolicy 3ffe:831f::/32 5 5
```

※Beta2 Build5384にて確認

FreeBSD (5.4R以降)

- **ip6addrctlコマンドによるIPv4優先設定**

```
# ip6addrctl flush  
# ip6addrctl add ::ffff:0:0/96 50 0  
# ip6addrctl add ::1/128 40 1  
# ip6addrctl add ::/0 30 2  
# ip6addrctl add 2002::/16 20 3  
# ip6addrctl add ::/96 10 4
```

- **/etc/rc.d/ip6addrctlの利用**

```
# /etc/rc.d/ip6addrctl prefer_ipv4
```

※/etc/rc.confに「ip6addrctl_enable=“YES”」を追加する必要あり

IPv4優先ポリシーテーブルの確認

Windows XP

```
> netsh interface ipv6 show prefixpolicy
```

Precedence	Label	Prefix
-----	-----	-----
5	5	3ffe:831f::/32
10	4	::/96
20	3	2002::/16
30	2	::/0
40	1	:::1/128
50	0	::ffff:0:0/96

Windows Vista

```
> netsh interface ipv6 show prefixpolicies
```

優先順位	ラベル	プレフィックス
-----	-----	-----
5	5	3ffe:831f::/32
10	4	::/96
20	3	2002::/16
30	2	::/0
40	1	:::1/128
50	0	::ffff:0:0/96

FreeBSD

```
% ip6addrctl show
```

Prefix	Prec	Label	Use
::ffff:0.0.0.0/96	50	0	0
:::1/128	40	1	0
::/0	30	2	0
2002::/16	20	3	0
::/96	10	4	0

DNSリゾルバ問題

- 概要

- OS,アプリケーションによるドメイン自動補完 & AAAA 問い合わせによるコンボアタック
- これにより、DNSサーバへのクエリが増加することが懸念されている。

- 想定される影響

- 増大するクエリに耐え切れなくなったDNSサーバが発生した場合、エンドユーザ側で、新規接続に対して、レスポンスが低下する。

DNSリゾルバ問題 (Cont)

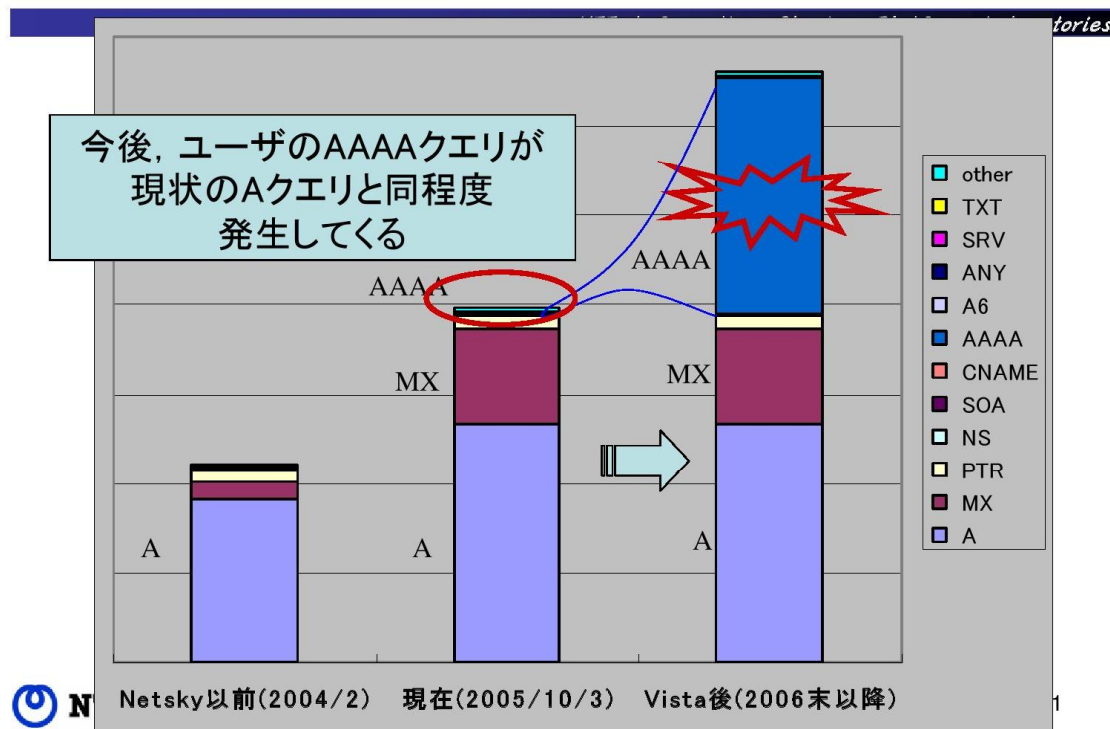
- **対処方法**

- **DNSサーバの増強 (実はしなくても余裕?)**
- **もし可能なら、OS・アプリのドメイン自動補完機能の停止**

DNSリゾルバ問題 (Cont)

2006 JANOG17@sendai

DNSキャッシュサーバへのクエリ推測



ドメインサーチオーダとIPv6

NTT情報流通プラットフォーム研究所さま JANOG17 公開資料より引用

DNSリゾルバ問題

Windows Vistaではどうなの？

DNSサーバ問題

- **概要**

- AAAAクエリに対して不正な応答を返す、イリーガルな実装のDNSサーバ、もしくはDNSのクエリを加工してしまうFirewall等が存在する。

- **現象**

- あるホストのA RRが存在し、AAAA RRが存在しない場合、AAAA RRの問い合わせに対しては、DNSサーバは以下の返答を返す必要がある。
 - Response code(RCODE)が0
 - Answer sectionは空

DNSサーバ問題 (Cont)

● 事例

- AAAA RRの問い合わせを無視する
- RCODE 3(NXDOMAIN) を返す
- NODOMAIN以外のRCODEを返す
- 壊れた返答を返す (IPv4アドレスを返すなど)
- Lame Delegationになる

DNSサーバ問題 (Cont)

- **影響が想定される人**
 - 企業、個人などのエンドユーザ
 - 苦情を受け取るDNSサーバ管理者
- **自分が該当するか不安なら、以下のサイトでチェック可能(単一ドメインのみ)**

http://www.cnri.dit.ie/cgi-bin/check_aaaa.pl

DNSサーバ問題 (Cont)

- **解決策**

- **DNSサーバ側での解決**

- 正しい挙動をするDNSサーバ、Firewall等を使う

- **リゾルバによる解決(クライアント側での解決)**

- AAAA RRの問い合わせを、それが必要な場合に限定する (IPv6の到達性がない場合は引かないなど)
- AAAA RRの問い合わせ待ち時間がある条件の下で短縮する。
 - A RRを先に引き、その返答に掛かった時間を参考にAAAA RRの返答待ち時間を設定する。

DNSサーバ問題(Cont)

- リゾルバ実装例

- KAME(BSD)におけるgetaddrinfo()

A RRの問い合わせに要した時間を T とし

AAAA RRへの待ち時間を $\max(1\text{秒}, T*2)$ とする。

これにより、Aには答えるけど、AAAAを無視するようなサーバに聞いてもあまり待たずに済む。

DNSサーバ問題

Windows Vistaではどうなの？

パケットフィルタリング問題

- 概要

- Firewallなどパケットを遮断することのできる機器で、TCP 53番ポートやEDNS0を遮断することで発生する問題（ある意味IPv6の問題じゃないけど。）

- 影響を受ける人

- そのFirewall内にいるエンドユーザ
- DNS 512 bytes超過なレコードを持つサイト (AAAA, ENUM, DNSSEC, etc)

パケットフィルタ問題

- 対処方法

- 正しいフィルタに直す

- DNSはTCP 53番ポートも使うよ！
 - EDNS0も通そう！

- Workaround

- レコードが 512bytesを超えないようにする。

パケットフィルタ問題

Windows Vistaではどうなの？

キャプティブポータル問題

- 概要

- ホテル問題といえは思い出してもらえるでしょうか？
- 客室に提供されているインターネット接続サービスを利用しようとしたら、うまく動かず、フロントに苦情を入れたら

“ipv6 uninstall”と打ち込んでください、とかいわれた

キャプティブポータル問題(Cont)

- **概要**

- Windows SP2では以下の理由により IPv6が有効になっていると、インターネット接続システムが利用できなかった。

キャプティブポータル問題(Cont)

1. ホテルのLANへPCを接続
2. DHCPでプライベートアドレス & DNSサーバのアドレス(例: 172.31.0.1)をゲット
3. ブラウザでとりあえず適当なサイトへアクセス (たとえば<http://v6fix.net/>)
4. DNSサーバ(172.31.0.1)へ v6fix.netのAAAA RRを問い合わせる

キャプティブポータル問題(Cont)

5. IPv6の接続性はないので、すぐに IPv4へフォールバックする
6. v6fix.netのA RRは203.178.140.19なので、そこへ HTTP GETを発効
7. 6.のリクエストは横取りされ、サービス規約確認画面を表示するためのHTTP OKが返る

キャプティブポータル問題(Cont)

8. 応答内のJavascriptにより、
<http://registration.example.jp/>
にリダイレクトされる。
9. リダイレクト先のAAAAをDNSサーバへ問い合わせる。
10. 問題のシステムのDNSサーバは、存在しないRRの問い合わせに対して、常にあるIPv4アドレスを返す。

キャプティブポータル問題(Cont)

11. WindowsXP SP2は AAAA RRの問い合わせに対して返信されたA RRを受理し、問い合わせをやめてしまう。
12. 得られたA RRへHTTP GETする
13. 6. へ戻り、ループ。

キャプティブポータル問題(Cont)

- **実装について**

- Linux
- Mac OS X
- BSD

**上記実装では、AAAA問い合わせに対して返って来たA RRは受け取らず、常にA問い合わせに対して返ってきたA応答のみを利用する。
このため、影響を受けない。**

キャプティブポータル問題 (Cont)

- 番外編

- これからキャプティブポータルを構築する人は、WindowsXP SP2 + IPv6 install でチェックしておけば、ほぼ間違いない。

キャプティブポータル問題

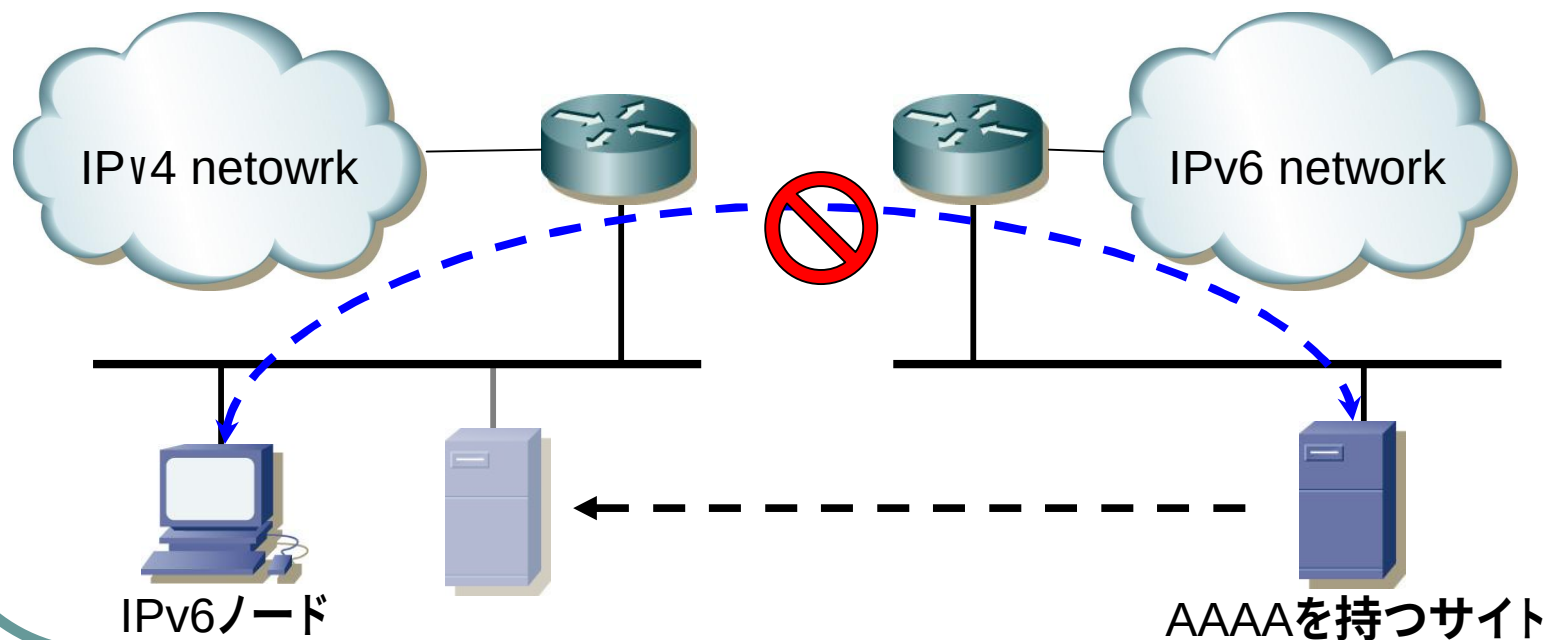
Windows Vistaではどうなの？

IPv6の仕様不備

onlink-assumption問題

● 概要

- Default routeがない場合、すべての宛先は同一リンクにあると仮定するという仕様



IPv6の仕様不備

onlink-assumption問題 (Cont)

● 問題点

- IPv6ノードをクライアントとして利用
- そのクライアントがOnlink-assumptionをサポートしている。
- IPv6のdefault routeが存在しない
- AAAAを持つサイトへアクセス

これらの条件がすべて満たされた場合、IPv4へのフォールバックまで数十秒～数分待たされる
(※1)

※1 待ち時間は実装に依存する。

IPv6の仕様不備

onlink-assumption問題(Cont)

- 影響を受けると想定されるユーザ
 - 企業および個人などのエンドユーザ
- 対処方法
 - RFC 2461が改訂され、onlink assumptionは無効化へ (draft-ietf-ipv6-2461bis-07.txt)

IPv6の仕様不備

onlink-assumption問題(Cont)

- **各実装の対応状況**

- Linux-2.6.9以前のカーネルでは影響を受ける。
Workaroundはあり。またディストリビューションによっては該当バージョンであっても独自にpatchが当てられている場合もある
- BSD
 - 問題なし
- MacOS X
 - 問題なし
- Solaris 9
 - 問題あり
- WindowsXP SP1およびSP2
 - 実装はされているが、問題は発生しない。

IPv6の仕様不備

onlink-assumption問題(Cont)

Windows Vistaではどうなの？