

LANや端末でIPv6を 利用する際の問題

IPv6普及高度化推進協議会
移行WG IPv6端末OS評価SWG
(株)リコー ソフトウェア研究開発本部
大平浩貴



当該セッションの予定

第1部

-  IPv6普及高度化推進協議会 移行WG v6端末OS評価SWGの検討成果を発表
-  PCのOSがIPv6化する際の問題
 - ❖ 特にWindows Vistaでの実験結果を交えて説明

第2部

-  3名のエッジ技術者の方々にご登場頂きます
-  KAME、USAGI、MacOSX各処理系におけるIPv6化の問題、課題、経験則など何でも

IPv6端末の増加

❁ 一般消費者が使うPCのOSがIPv6化

- Windows VISTAのリリース
- その他のOSもv6化が一般的になりつつある
 - ❖ MacOS X、Linux、*BSD、Solaris、etc...

❁ 買ってきたPCに電源を入れて、ネットワークにつないただけで...

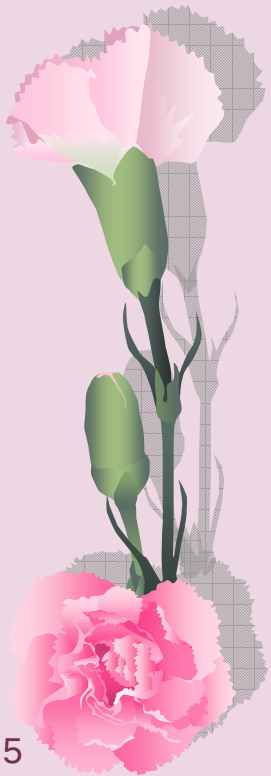
- RSを送り、RAを受け、DADして、設定されたIPv6アドレスでDHCPv6を使いDNSサーバを知り、AAAAレコードの名前引きを行い、PMTUDをしてサーバにアクセスする
- ほとんどの人がやったことないはずだけど、大丈夫？

IPv6の通信はできる。だけど...

- ❁ ほとんどの環境でIPv6の通信はできるでしょう
- ❁ だけど正常に、便利に使うことはできる？
 - ❏ お客様にv6対応ソリューションをお売りすることはできる？
 - ❏ クリティカルな環境でv6を使うことはできる？
 - ❏ セキュリティ的な穴がないと言える？

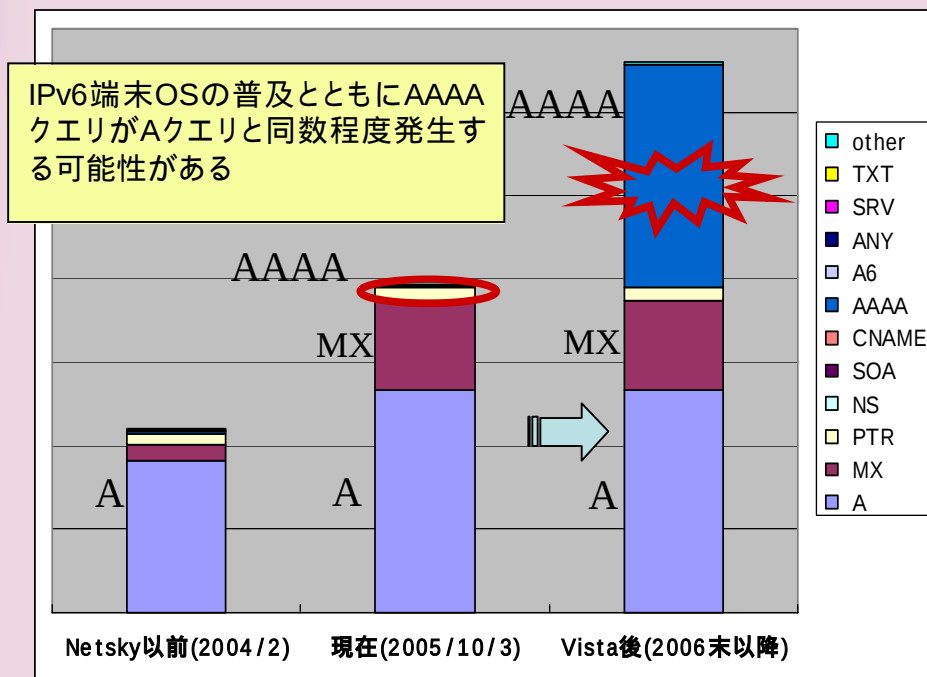
起こり得る問題を棚卸しして、備えましょう

IPv6端末の浸透によって 発生しうる問題



DNSのクエリ量の増加(1/4)

- IPv6に対応すると、Aレコードだけでなく、AAAAレコードの名前引きも必要になる



DNSのクエリ量の増加(2/4)

❁ 現在既に、1回のWebアクセスで、数回の名前引きが発生しうる

q.example.jpへのアクセス

A? q.example.jp
AAAA? q.example.jp
A? q.example.jp.co.jp
AAAA? q.example.jp.co.jp
A? q.example.jp.example.jp
AAAA? q.example.jp.example.jp
A? q.example.jp.com
AAAA? q.example.jp.com

●もしq.example.jp のIPv4, IPv6いずれかのアドレスが解決できれば問い合わせは終了する

DNSのクエリ量の増加(3/4)

```
C:\> telnet q.example.jp
AAAA?q.example.jp
AAAA?q.example.jp.co.jp
AAAA?q.example.jp.example.jp
AAAA?q.example.jp.com
A? q.example.jp
A? q.example.jp.co.jp
A? q.example.jp.example.jp
A? q.example.jp.com
```

- IPv6アドレスの解決のためすべてのドメイン補完を試みるまでIPv4アドレスの解決へ進まない
- 問い合わせしたホスト名に対してNXDOMAINが返却されてもIPv4アドレスの解決を試みる

- IPv4アドレスのみが得られる場合でも、ドメインサフィックスの数だけIPv6アドレス解決が必要

Windows XP SP2

```
C:\> telnet q.example.jp
A? q.example.jp
A? q.example.jp.co.jp
A? q.example.jp.example.jp
A? q.example.jp.com
```

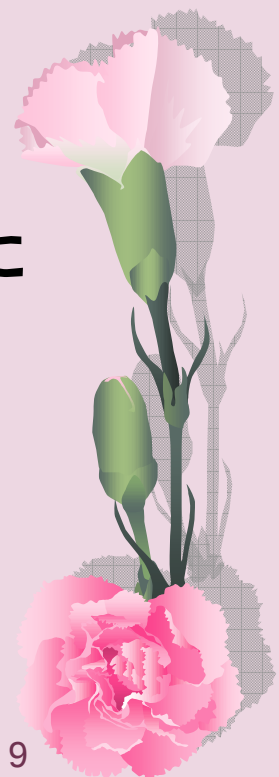
- もしIPv4アドレスの解決の際にNXDOMAINが返却されたら、IPv6アドレスの解決は抑制される

Windows
Vista Build
5600

```
AAAA?q.example.jp
AAAA?q.example.jp.co.jp
AAAA?q.example.jp.example.jp
AAAA?q.example.jp.com
```

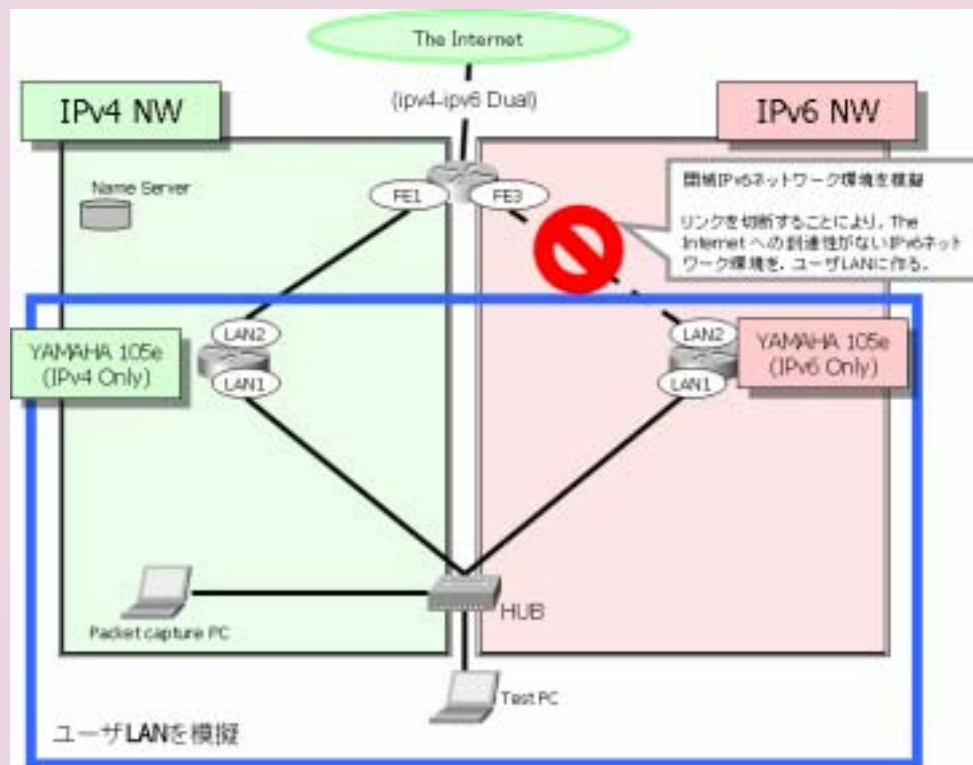
DNSのクエリ量の増加(4/4 まとめ)

- ❁ NXDOMAINが得られたら、即座に解決を止めてしまうという実装が、BCPと考えられる
 - ➡ Windows Vista Build 5600が採用
- ❁ DNSキャッシュサーバを運用するサービス事業者の方々には、DNSキャッシュサーバの計算機資源について、ご注意&増強の検討をお勧めしたい
- ❁ またネットワークアプリケーションの開発者は、DNSクエリの抑制を意識してほしい



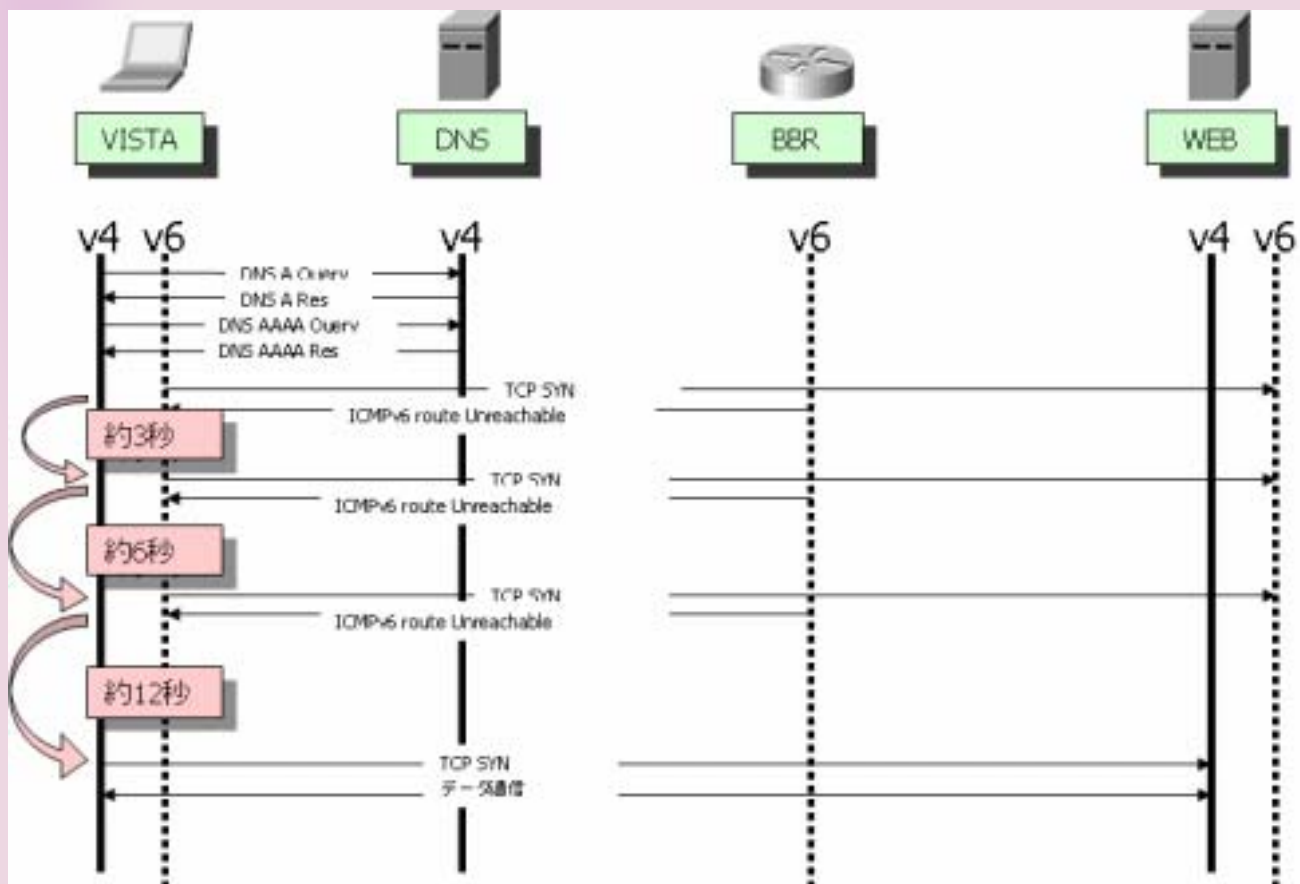
IPv6到達性がないときのTCP フォールバック(1/4)

- IPv6アドレスが割り振られているが社外へのIPv6到達性が無い場合、正常に通信できる？

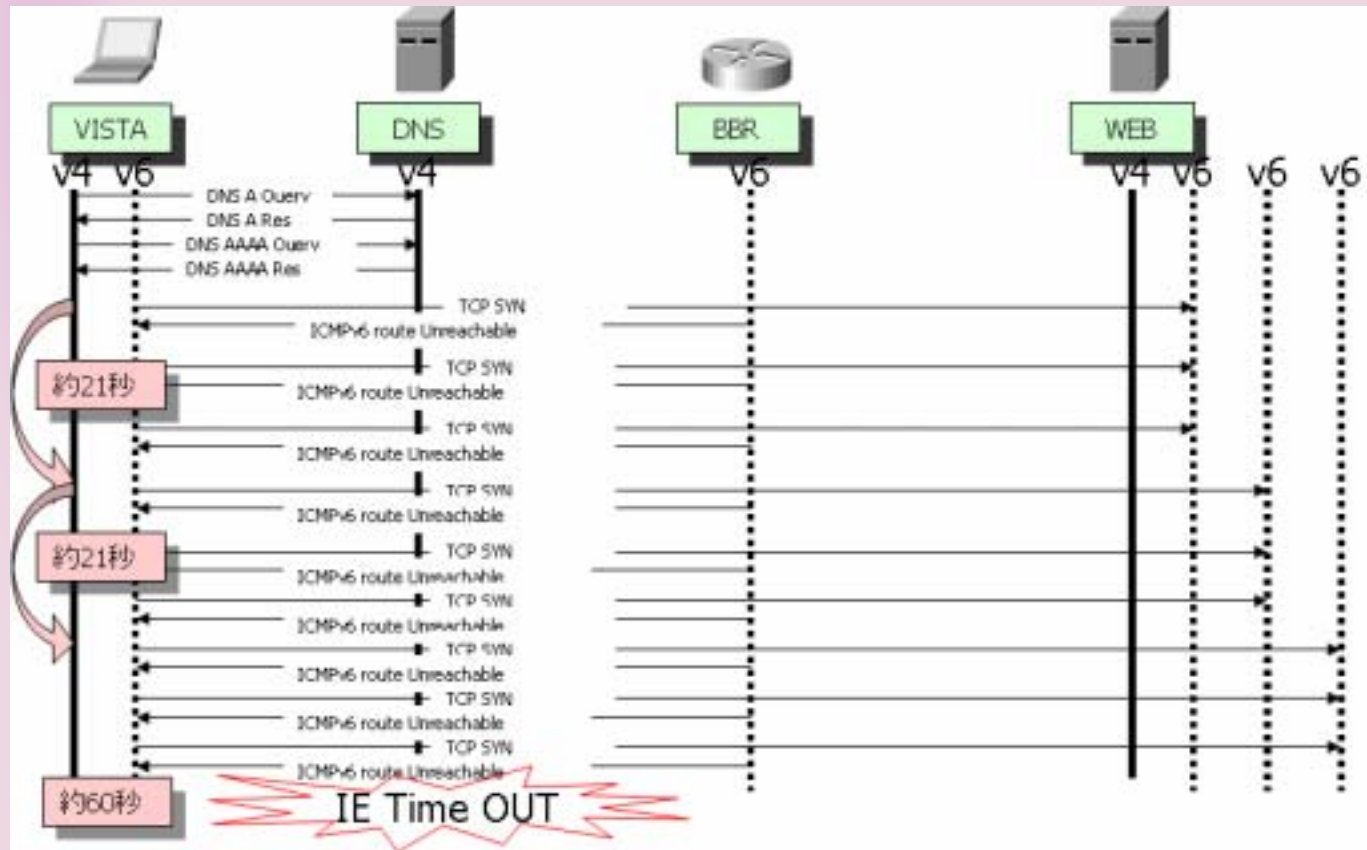


IPv6到達性がないときのTCP フォールバック(2/4)

IE7で社外のWebサーバにアクセスするとどうなる？



IPv6到達性がないときのTCP フォールバック(3/4)



IPv6到達性がないときのTCP フォールバック(4/4 まとめ)

❁ フォールバック問題:タイムアウトを待ってしまう

❁ 解決法1

■ RFC3484のPolicy Tableを採用する

- ❖ 閉域IPv6prefixの優先度を高く設定、次点でIPv4 mapped address(::ffff:0:0/96)を設定、その次をIPv6 default routeとする

❁ 解決法2

■ 起動時のRS/RAで生成された情報の削除と、閉域IPv6ネットワークPrefixのルーティングテーブル追加

- ❖ IPv6デフォルトゲートウェイの削除
 - > netsh interface ipv6 delete route ::/0 [interface] [nexthop]
- ❖ 到着するRAをフィルタでドロップする
- ❖ 閉域IPv6ネットワークPrefixの追加
 - >netsh interface ipv6 add route [prefix] [interface] [nexthop]



キャプティブポータル接続環境 における問題

❁ キャプティブポータルとは

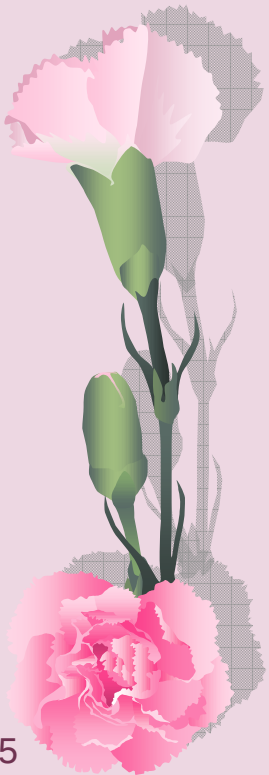
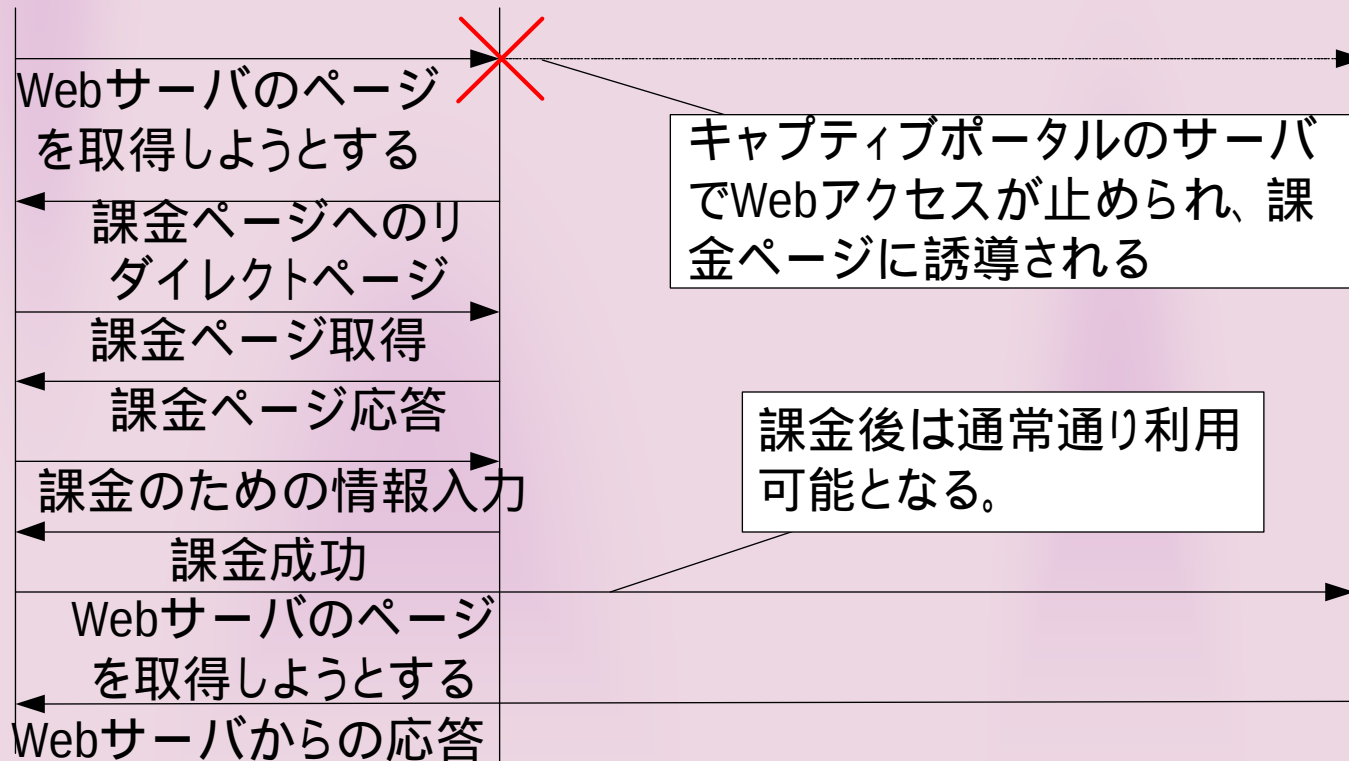
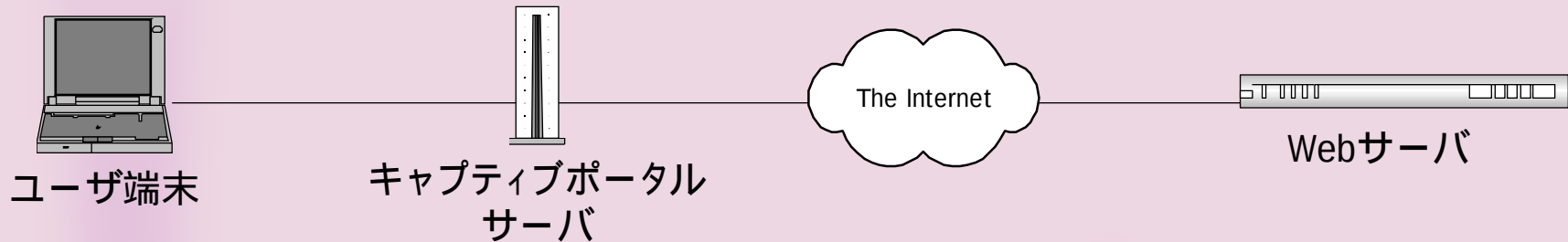
- ❏ 無線LANサービス、ホテルなどで採用しているインターネット接続時の認証、課金システム

❁ PCから最初の1回目のWebへアクセスを検出したら、そのアクセスを途中で取出し、課金ページにリダイレクトする応答を戻す

❁ 課金ページで登録したら、それ以降のアクセスは通常通り利用可能になる。



キャプティブポータル環境の概観



キャプティブポータル環境での 問題

❁ 症状

- Windows XP で、IPv6 installしたPCは通信
ができなくなる

❁ 原因

- 最初の名前引きで、XPのPCがAAAAレコード
のクエリを出すと、キャプティブポータルサー
バが何故かAレコードの応答を返す
- その応答をXPのPCが受理してしまう

キャプティブポータル問題への対策(Vistaによる対策)

🌸 Vistaが行なった対策

- 🍃 ISPなどから提供されるIPv6アドレスが付与されていない時はAAAA問合せを行わない
 - ❖ (Teredoアドレスを除く)

🌸 効果

- 🍃 名前引き処理で、自身にv6アドレスが割り振られているかどうかに応じて処理を変える手続きを追加した
- 🍃 これにより、IPv6の使えない環境ではAAAA名前引きが発生せず、キャプティブポータル問題を回避できるようになった



自動トンネル機能によって意図しない経路が生成されうる

🌸 Windows は高度な自動トンネル機能を実装している

🌿 6to4、teredo

🌸 上記の機能は、勝手にアクティベートされてしまうのか？

🌿 その場合、IPv6のInternet到達性が勝手にできあがってしまうことになる



自動トンネルの調査結果



調査手順



[6to4]

1. v4グローバルアドレスが付与されるNWにVistaを接続 .
 - ❖ (実験ではVistaにイーサケーブルを直接接続した状態でOCNにPPPoE接続してv4グローバルアドレスを付与)
2. ipconfig /allで "Tunnel adapter(6to4 Tunneling Pseudo-Interface)"のv6アドレスを確認



[Teredo]

1. v4プライベートアドレスが付与されるNW (NAT配下) にVistaを接続 .
2. ipconfig /allで "Tunnel adapter(Teredo Tunneling Pseudo-Interface)"のv6アドレスを確認



調査結果と考察

調査結果

-  IPv4グローバルアドレスが割り当てられる
 - ❖ 6to4が自動的に設定される
-  IPv4プライベートアドレスが割り振られる
 - ❖ Terodoが有効化する

結論

-  自動的にトンネルが構築されてしまう
 - ❖ ただし、IPv6はサブネット内の利用可能アドレスに対する実際のホスト数が非常に希薄であるため、ポートスキャンなどには利用されないと思われる。

初期状態でのファイアウォール 設定とオープンポート

- 🌸 Vistaでは、IPv6関連はどのようなポート、ICMPが空いている？
- 🌸 Vistaでは、どのようなサービスが初期状態で起動している？



初期状態でのファイアウォール 設定(ICMP)

プロトコル	タイプ	許可 or 遮断	プロトコルの説明
ICMPv6	1	許可	Destination Unreachable
	2	許可	Packet Too Big
	3	許可	Time Exceeded
	4	許可	Parameter Problem
	128	遮断	Echo Request
	129	遮断	Echo Reply
	130	許可	Multicast Listener Query
	131	許可	Multicast Listener Report
	132	許可	Multicast Listener Done
	133	遮断	Router Solicitation
	134	許可	Router Advertisement
	135	許可	Neighbor Solicitation
	136	許可	Neighbor Advertisement
	137	遮断	Redirect
	143	許可	Multicast Listener Report Version2

初期状態でのファイアウォール 設定(TCP/UDP)

プロトコル	ポート番号	プロトコルの説明	規則の説明
TCP	2869	LCSLAP	- ネットワーク探索(UPnP受信) - リモートアシスタンス(UPnP受信)
	5355	LLMNR (Linklocal Multicast Name Resolution)	ネットワーク探索(LLMNR TCP受信)
	5357	Web Service for Devices	ネットワーク探索(WSDイベント受信)
	5358	WS for Devices Secured	ネットワーク探索(WSD EventsSecure受信)
	任意		リモートアシスタンス(TCP受信)
UDP	エッジトラ バーサル 68	Teredo	コアネットワーク-Teredo(UDP受信)
		Bootpc	コアネットワーク-動的ホスト構成プロトコル(DHCP受信)
	137	NETBIOS Name Service	ネットワーク探索(NB名受信)
	138	NETBIOS Datagram Service	ネットワーク探索(NBデータグラム受信)
	1900	SSDP	- ネットワーク探索(SSDP受信) - リモートアシスタンス(SSDP受信)
	3702	UPnP v2 Discovery	- ネットワーク探索(pub WSD受信) - ネットワーク探索(WSD受信)
	5355	LLMNR (Linklocal Multicast Name Resolution)	ネットワーク探索(LLMNR UDP受信)

初期状態でオープンしている ポート・サービス

プロトコル	ポート	XP(IPv4)	Vista(IPv4)	Vista(IPv6)	プロトコルの説明
TCP	135	○	○	○	epmap(RPC)
	139	○	○	×	NETBIOS Session Service
	445	○	×	○	Microsoft-DS (プリンタ/ファイル共有)
UDP	123	○	○	○	NTP
	137	○	○	×	NETBIOS Name Service
	138	○	○	×	NETBIOS Datagram Service
	445	○	×	×	Microsoft-DS (プリンタ/ファイル共有)
	500	○	○	○	ISAKMP(IKE)
	1900	○	○	○	SSDP
	3702	×	○	○	UPnP v2 Discovery
	4500	○	○	×	IPsec NAT Traversal
	5355	×	○	○	LLMNR (Linklocal Multicast Name Resolution)

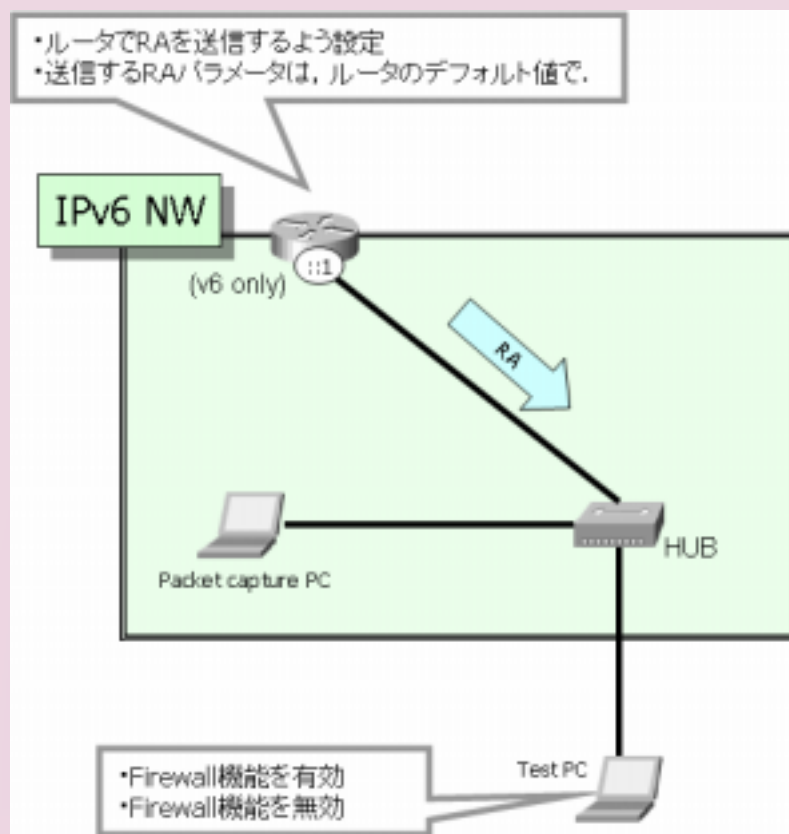
初期状態のオープンポート考察

- ❁ FirewallはICMPv6、TCP、UDPとも、必要最小限の受信許可規則が設定されており、IPv6の基本的な通信には問題ない
- ❁ Windows XPのときと同様に、デフォルトではpingや traceroute には応答しない設定
- ❁ 必要最小限のポート番号のみがオープンしていると考えられる
- ❁ サービスが起動していても、ファイアウォールで遮断されているものがある
 - これらはPCローカルで利用するためにこうなっていると考えられる

RAの取り扱い

❁ サーバなどで誤ったRAを受信できないようにすべきである

🍃 この運用が実現できるか検証をした



RAを排除する処理の確認

確認手順

1. Windows FirewallにてRAをドロップする設定に変更
2. Vista の再起動を実施し, IPv6ルータとの通信をパケットキャプチャし解析
3. IPv6ルータから定期的に送信されるRA情報をパケットキャプチャし解析
4. IPv6ルータから定期的に送信されたRA受信後の Windows Vista のステータスを確認する

確認結果

- Vista のWindows Firewall でRA受信をドロップするルールを適用しても起動時にRAを受信する。
- 起動後は Windows Firewall のルールが適用され, IPv6ルータから定期的に送信されるRAについてはドロップする。
- 起動時に受信したRAの ($\text{valid_lifetime} \times 2$) 秒の時間経過後、Prefix有効時間が切れてグローバルユニキャストIPv6アドレスは消失する。

RAを排除する処理の考察

🌸 Firewallで排除しようとしても、起動時にはIPアドレスが割り振られてしまう

🌸 対策

- Windows FirewallにRAを排除するように登録する
- Windows起動時にはそれでもRAを受信してしまうので、起動直後に下記の機能を持つスクリプトを走行させる
 - ❖ グローバルユニキャストアドレスの削除
 - ❖ デフォルトゲートウェイ情報の削除



IPv6のDDNSについて

❁ IPv6アドレス割り振り後、DDNS処理はどうなるかが不明

■ IPv6 DNS serverへ更新リクエストに失敗した場合の挙動

❖ IPv4 DNS serverへ fall backする？

■ 複数アドレスをもつ場合の挙動

❖ IPv4、IPv6アドレスを持つ場合、全て登録する？

❖ 複数のIPv6 addressを持つ場合すべて登録する？

❖ 登録するaddressを制限できる？

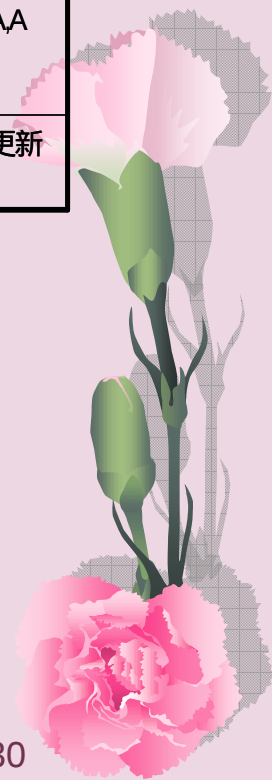
IPv6のDDNS検証結果

		DNS server 設定								
		IPv6			IPv6/IPv4			IPv4		
到達性		IPv6	IPv6/IPv4	IPv4	IPv6	IPv6/IPv4	IPv4	IPv6	IPv6/IPv4	IPv4
PCの アドレス 設定	IPv6	・v6で更新 ・AAAA	・v6で更新 ・AAAA	NG	・v6で更新 ・AAAA	・v6で更新 ・AAAA	NG	NG	NG	NG
	IPv6/ IPv4	・v6で更新 ・AAAA,A	・v6で更新 ・AAAA,A	NG	・v6で更新 ・AAAA,A	・v6で更新 ・AAAA,A	・v6→v4 とfallback して更新 ・AAAA,A	・v4で更新 ・AAAA,A	・v4で更新 ・AAAA,A	・v4で更新 ・AAAA,A
	IPv4	NG	NG	NG	NG	・v4で更新 ・A	・v4で更新 ・A	NG	・v4で更新 ・A	・v4で更新 ・A

🌸 Vistaはβ 2のBuild 5384 を使用

🌸 まとめ

- IPv6 DNS serverのupdateで失敗した場合にはIPv4 DNS serverへfall backする
- IPv4,IPv6 両方のグローバルアドレスを複数もつ場合、それらを全て登録する
- IPv6のみ,IPv4のみ,あるいは複数のIPv6 addressをもつ場合、一部のaddressのみを登録するといった、登録制限を行なうことはできない



DNSディスカバリについて

DNSサーバ発見が必要

-  ホスト自身のIPアドレス自動設定は規格化されているが、DNSサーバ設定の自動化(DNSサーバ発見)は遅れている
-  RFC4433で定義されている発見手法
 - ❖ RAによる通知
 - ❖ DHCPv6による通知
 - ❖ Well-known Anycast Addresses

IPv6端末OSでサポートしている、またサポートされうる自動発見手法について、調査を行なう

VistaにおけるDNSディスカバリ

❁ DHCPv6とWell-knownアドレスの2種による

❁ [DHCPv6]

- ❏ ManagedFlagが1となっているRAを受けたら、DHCPv6によるSolicitとRequestにより、DNSサーバ取得を試みる
- ❏ OtherConfigFlagが1となっているRAを受けたら、DHCPv6によるInformation-requestによってサーバ取得を試みる

❁ [Well-known]

- ❏ 上記のいずれでも取得できなかった場合、fec0:0:0:ffff::1 ~ fec0:0:0:ffff::3のwell-knownアドレスを利用する
- ❏ サイトローカルアドレスはobsoleteであるため、この使用は避けるべきと考えられる

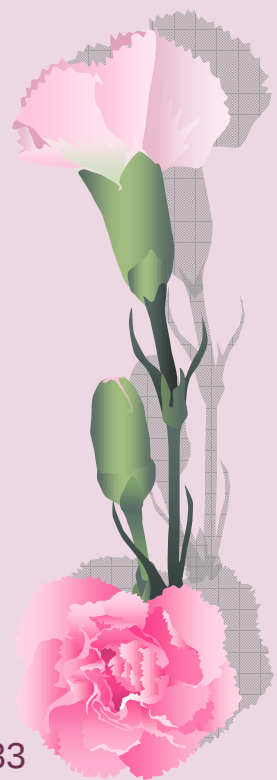
マルチプレフィクス/マルチホーミング

❁ MH(マルチホーミング)とは

- ❏ ある一つのネットワークが、外部ネットワークへの接続口を持つことをホーミングと呼ぶ
 - ❖ 例:Internetに繋ぐため、ISPにホーミングする
- ❏ 二つ以上の外部ネットワークへの接続口を持つ状態をマルチホーミングと呼ぶ
 - ❖ 例:Internetと、動画配信用のマルチキャストネットの両方に
つなぐなど

❁ 各ホーミング先のサービスを使うため、ホーミングの数のぶんだけ、IPアドレスが割り当てられる

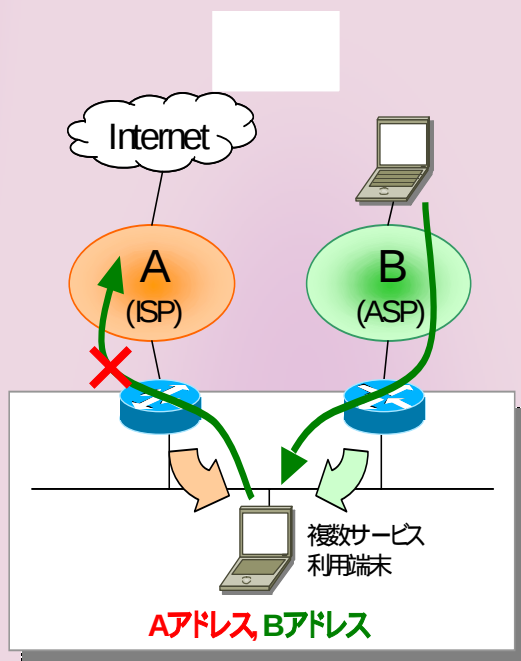
- ❏ 例:2つのホーミングを行なうと、組織内の全端末が2つのIPアドレスを持つ
- ❏ 一つのサブネットに複数のプレフィクスが来るのでMP(マルチプレフィクス)と呼ぶ



マルチホーミング時のデフォルトルート設定

❁ 複数のルータが存在する

- ❁ 両方からRAが到達する
- ❁ どちらをデフォルトルータにするべきか？



ISP Aからのルータ通知を先に受信した場合の動作

- ISP A経由でのインターネットへの通信
- × ASP Bへの通信
- × ASP Bからの通信に対する返信

マルチホーミング時のデフォルト ルート設定(考察)

- ❁ RFC4191にあるRAの拡張案を利用する
 - ❏ ルータ通知のフラグフィールドに、そのルータの優先度を3段階で指定できるようになっている
 - ❏ FreeBSDのrtadvd、Linuxのradvdにて実装済
- ❁ RFC4191では、経路情報通知オプション機能もある
 - ❏ ただし、ルーティング情報とRAは別物であり、これらの連携については今後の検討を待たなければならない
 - ❏ ルータを購入する際は、Router-Preference設定をサポートしている製品を採用すると良い

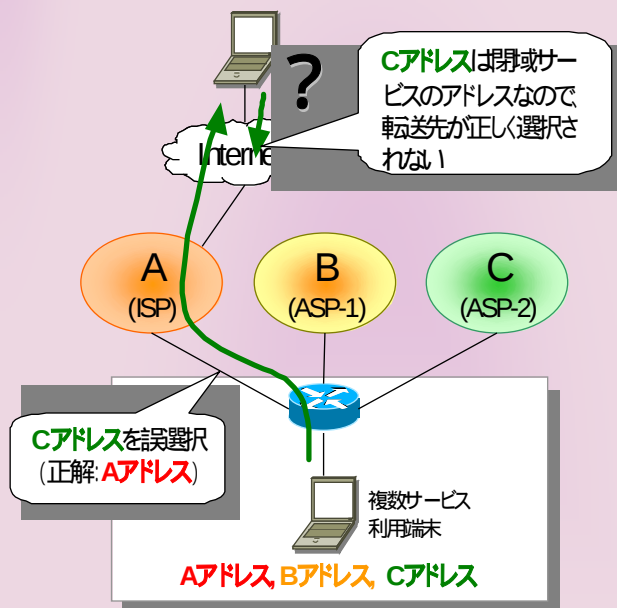


マルチプレフィックス時のソースアドレスセレクション

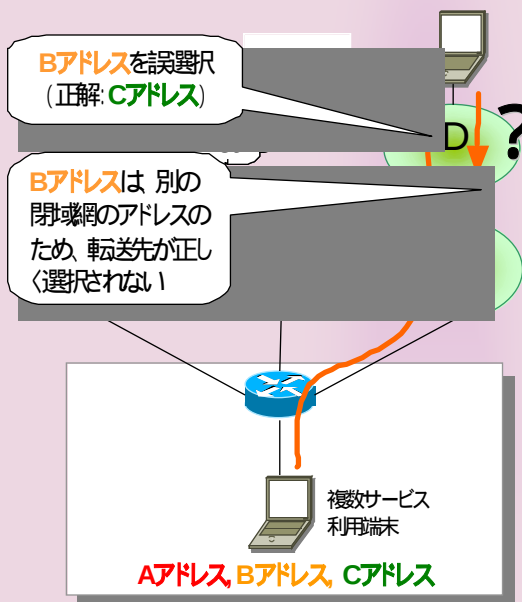
❁ 自分に複数のIPアドレスが割り振られた場合、どれをパケットのソースアドレスにしたら良いか？

- 間違えると、通信不能に陥ってしまう
- 例: Internetへの通信なのに、ローカルなIPアドレスをソースアドレスにすると、通信不能になる

【ケース1】インターネットへの通信時



【ケース2】閉域型ネットワークへの通信時

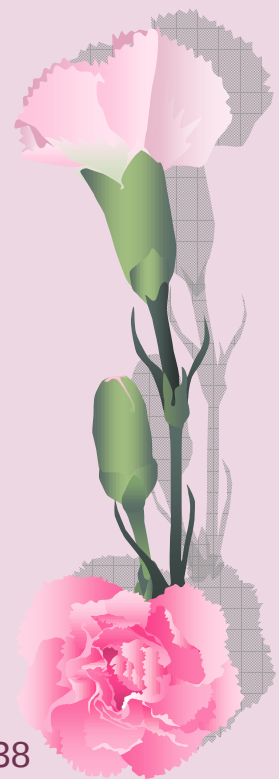


ソースアドレスセレクション(考察)

- ❁ RFC 3484 で定義されているLongest Matchという手法を使う
 - ➡ 宛先アドレスと最も似ているアドレスをソースアドレスとして選択する
- ❁ RFC3484で定義されているPolicy Table(宛先アドレスとソースアドレスの対応表)を利用する
 - ➡ テーブルの設定方式について今後の運用検討を待たなければならない



まとめ



Internetの発展から

- ❁ Internetが流行るとき、既にネットワーク技術は完成に近かった
 - IPv6も同様であり、IPv6が流入しようとしている今、既にIPv6の標準化は完成に近い状態
- ❁ 運用の完成度は、流行りだしてから進歩する
 - Firewall、ログ解析など、運用技術の向上は、大規模に利用され出してから本格化する
 - 使えば向上する=使うところにビジネスチャンスがある
- ❁ IPv6の大規模な実運用はこれから
 - たぶん、問題が発生して、我々の仕事が増える
 - それによって、IPv6が当たり前のように利用されるようになる



最後に

- ❁ IPv6の浸透は技術のイノベーション
- ❁ ここにいる技術者の皆さん(私含む)が活躍するチャンスがたくさんある
- ❁ 事前の勉強、問題の予測、大胆な解決を
- ❁ Internet 次の一步のために頑張りましょう

