NTT

NTT Information Sharing Platform Laboratories
NTT 情報流通プラットフォーム研究所

IPv6再入門
IPv6ネットワーク構築基礎

NTT情報流通プラットフォーム研究所
セキュアコミュニケーション基盤プロジェクト
加藤 淳也

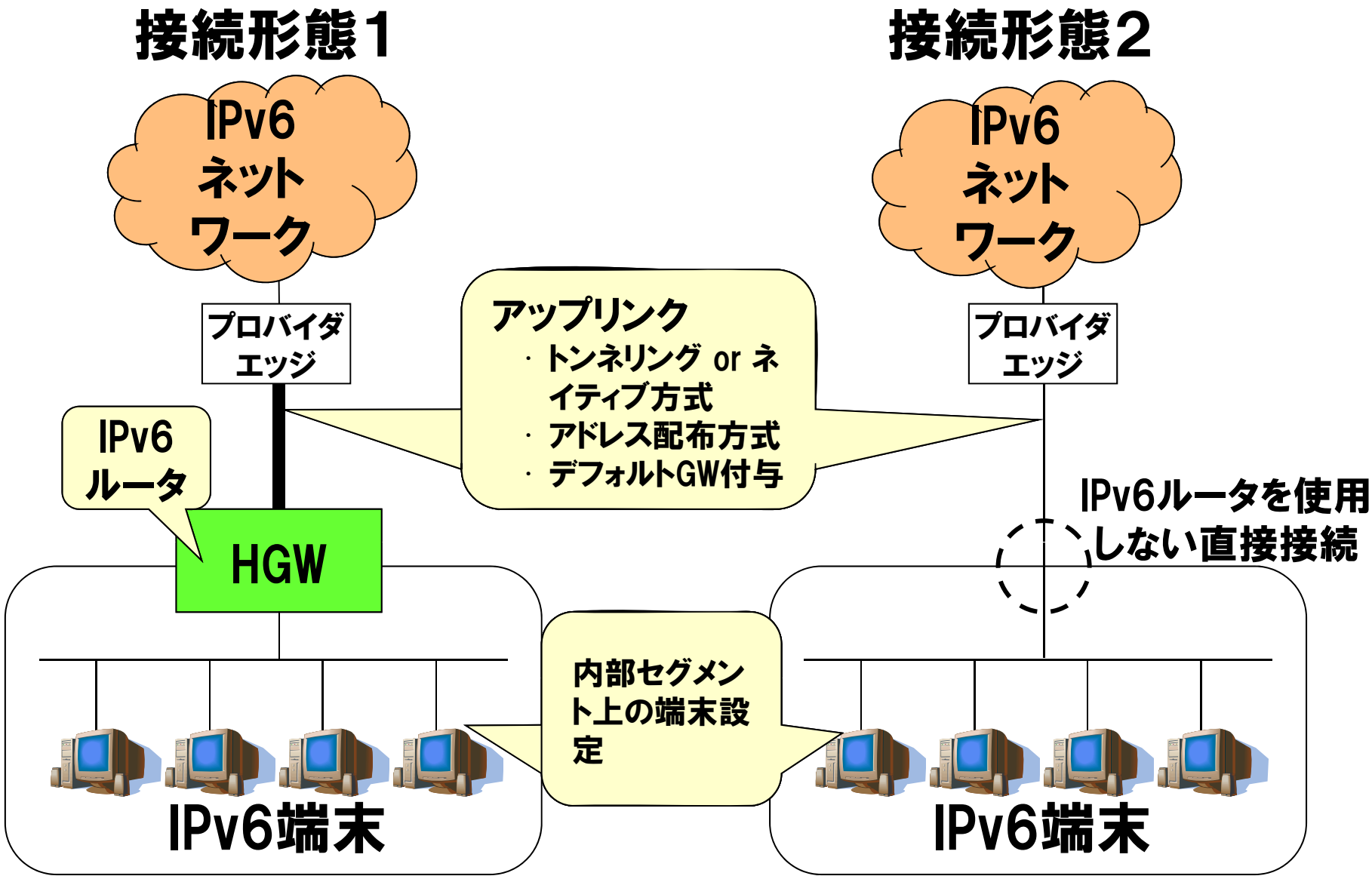
本セッションの目的とアウトライン

- 目的
  - 家庭・SOHO環境を対象としたIPv6ネットワーク構築法の解説

- 主なトピック
  - IPv6インターネットへの対外接続の確保
  - IPv6アドレス割り当てとデフォルトルータの配布方式
  - LAN内部での端末設定について
  - 家庭・SOHO環境でのセキュリティ
  - NGN上で提供予定のIPv6インターネット接続機能

  [付録]
    - ヤマハ製ブロードバンドルータRT58iでの設定例
    - ステートレスDHCPv6サーバの設定例

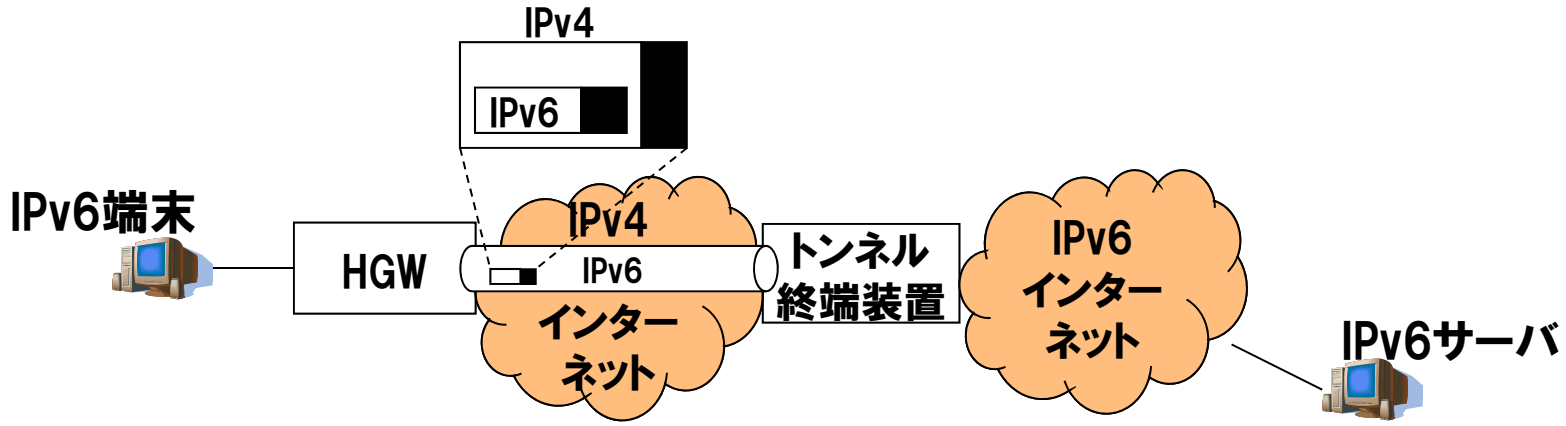
NTT 本セッションの想定SOHOネットワーク



IPv6インターネットへの対外接続の確保

スタティック（IPv6 over IPv4）トンネル

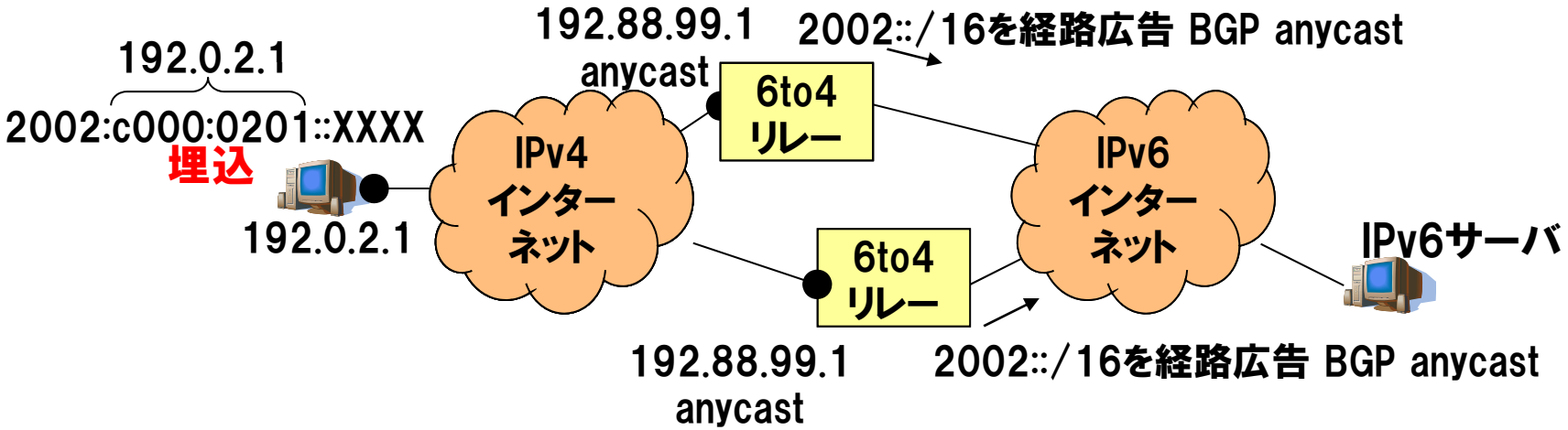
- IPv4インターネット上で IPv6パケットをカプセル化して転送する方式



- 主要ISPの多くが固定IPv4アドレスユーザ向けに提供
  - 代表例
    - OCN ： OCN IPv6トンネル接続サービス
    - IIJ　 ： IPv6トンネリングサービス
- HGW, 終端装置の双方にIPv4アドレスを指定する設定が必要
- NATを越えるためにはプロトコル番号41を通す必要がある

自動トンネル接続技術 6to4

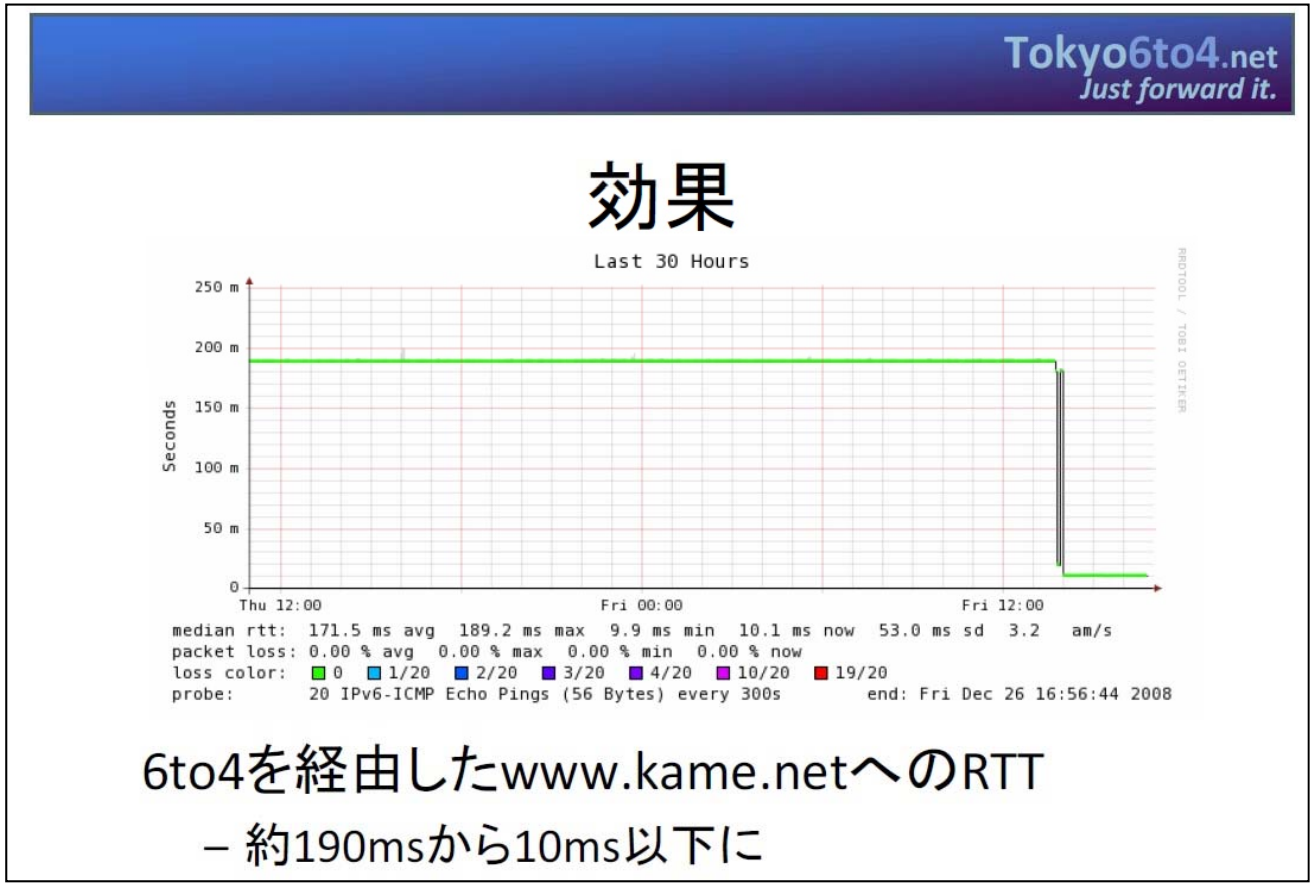
トンネル設定が不要なIPv6インターネット接続性確保技術



- メリット
  - 接続契約や登録は不要。IPv6アドレスはIPv4アドレスから自動生成する
  - RFC3056にて仕様が規定されており、実装が豊富（Win, Mac, UNIX, ブロードバンドルータも存在）
    - Windows Vista, 7 ではデフォルトで有効化されている
- デメリット
  - 経路制御が難しい（行きと帰りが非対称）
  - IPv4グローバルアドレスを必要とする（NAT越えが難しい）
  - リレールータの信頼性に課題

Tokyo6to4 プロジェクト

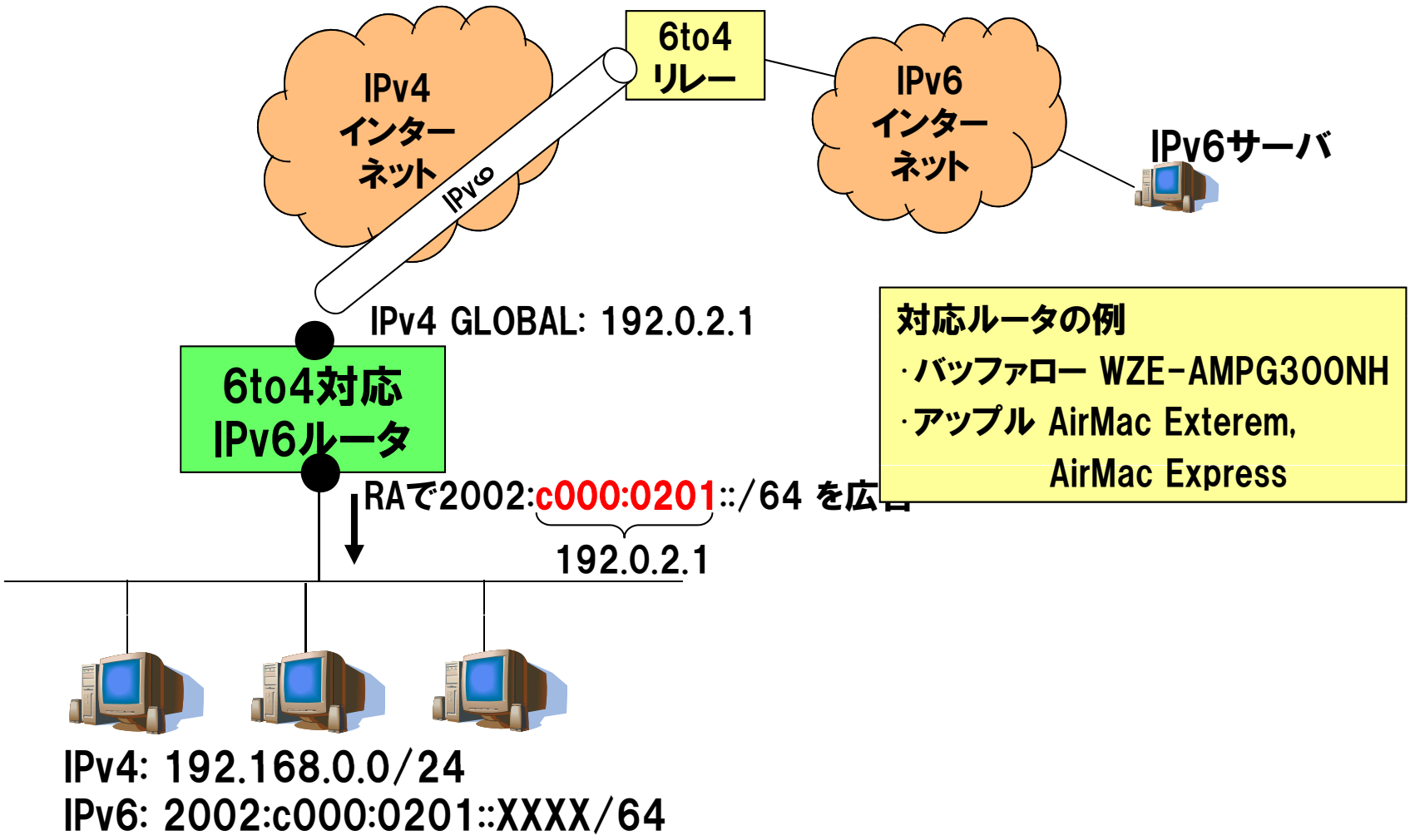
- 日本国内(JPIX)で、6to4リレールータが実験運用されている
- IPv6インターネットへの接続性が改善



(出典) http://www.tokyo6to4.net/

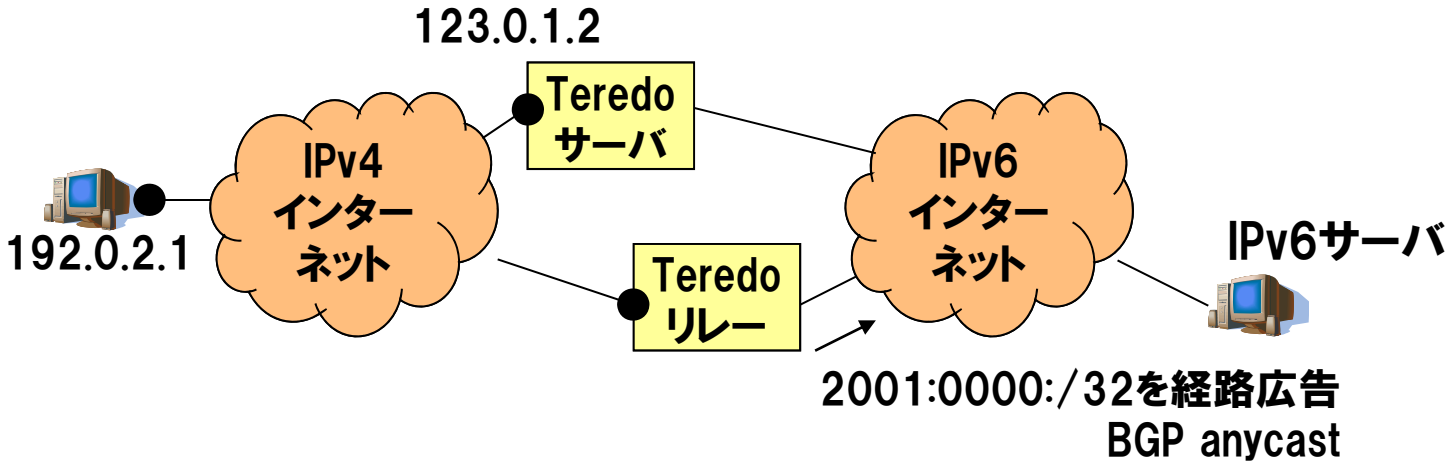
NTT 6to4対応ブロードバンドルータを使った外部接続

プライベートIPv4アドレスをもつデュアルスタック端末でもIPv6外部接続が可能



NTT NAT越えが可能な自動トンネル技術 Teredo（1）

- 6to4と同様にトンネル設定や契約行為は不要
- RFC4380にて標準が規定されている

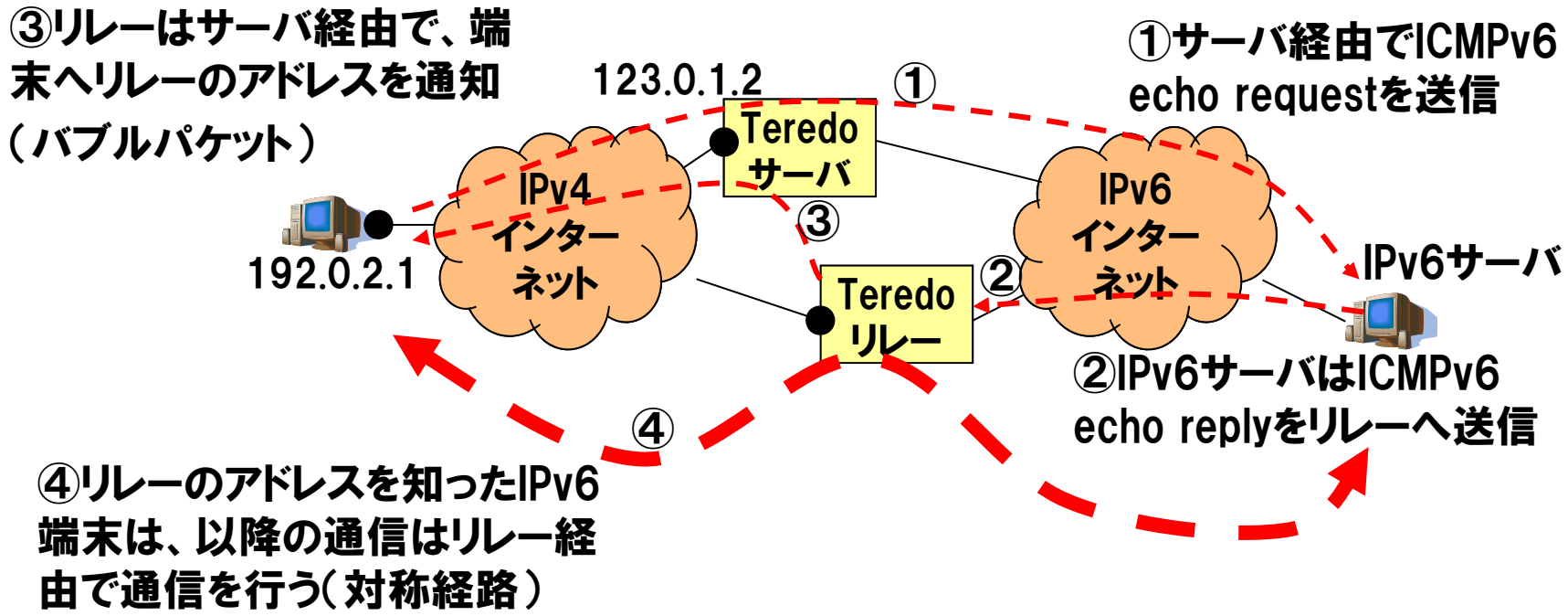


32ビット　16ビット　16ビット　32ビット

2001:0000:[サーバのIPv4アドレス]:[フラグ]:[ポート]:[端末のIPv4アドレス]

123.0.1.2　NATタイプ判定　端末の待受ポート　192.0.2.1

Teredoの動作例



32ビット　16ビット　16ビット　32ビット

2001:0000:[サーバのIPv4アドレス]:[フラグ]:[ポート]:[端末のIPv4アドレス]

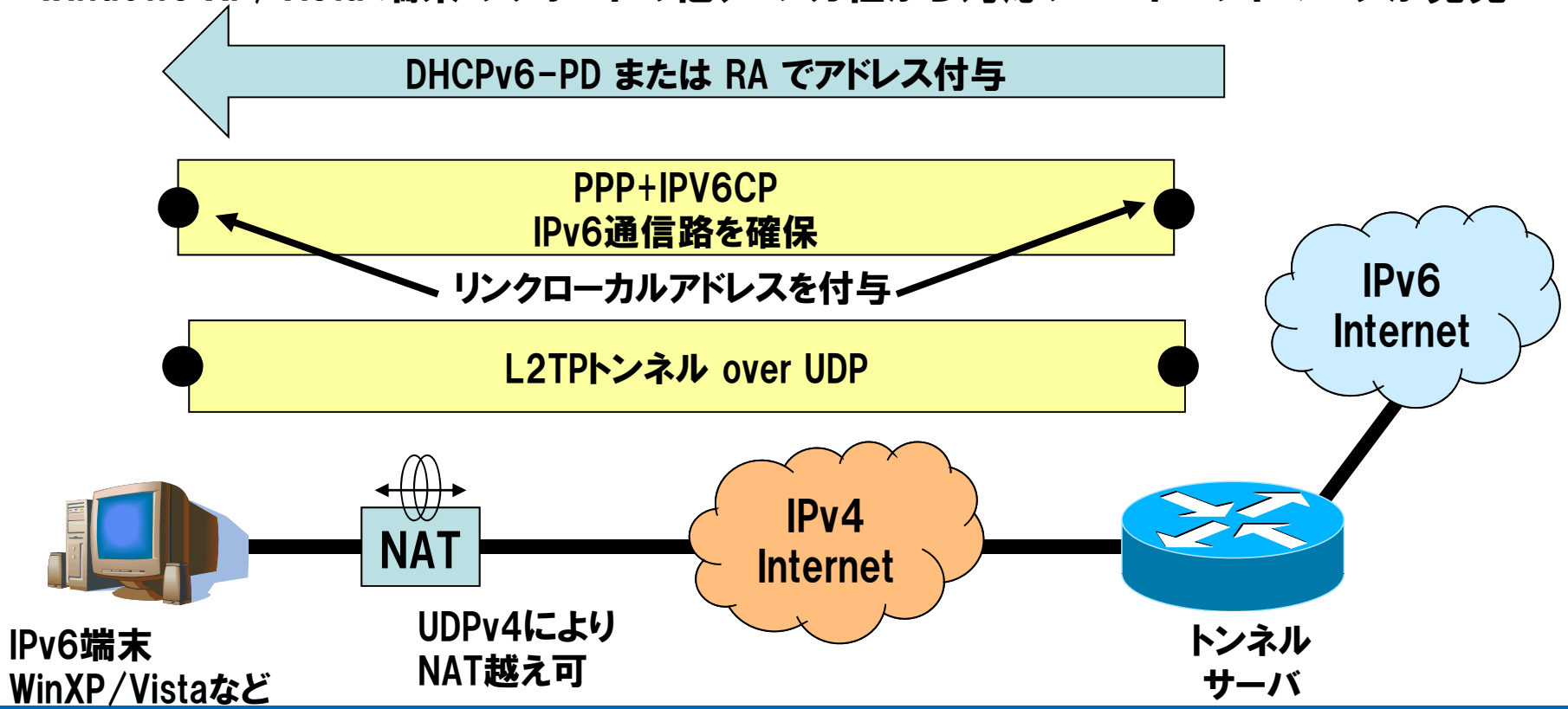
123.0.1.2　端末の待受ポート　192.0.2.1

NTT NAT越えが可能な自動トンネル技術 Teredo（3）

- メリット
  - 6to4と同様に接続契約や登録は不要。IPv6アドレスをIPv4アドレスから自動生成する
  - NATに対応。プライベートIPv4アドレスの端末でも使用可能
    - Symatric NAT は対応が難しい
  - Windows Vista, 7 では標準機能として提供される
  - 一定の経路最適化がおこなわれる（バブルパケット）
- デメリット
  - パブリックに利用可能なサーバー・リレールータが少ない
    - Euro6IX deploys Teredo Servers (11-01-2005).
      teredo.autotrans.consulintel.com
    - Miredo – Linux/FreeBSD 向け実装
      teredo.remlab.net
  - IPv6アドレスが端末情報を多く含む セキュリティ面の懸念
    - 待受（開放済み）ポートなどの情報が含まれるため

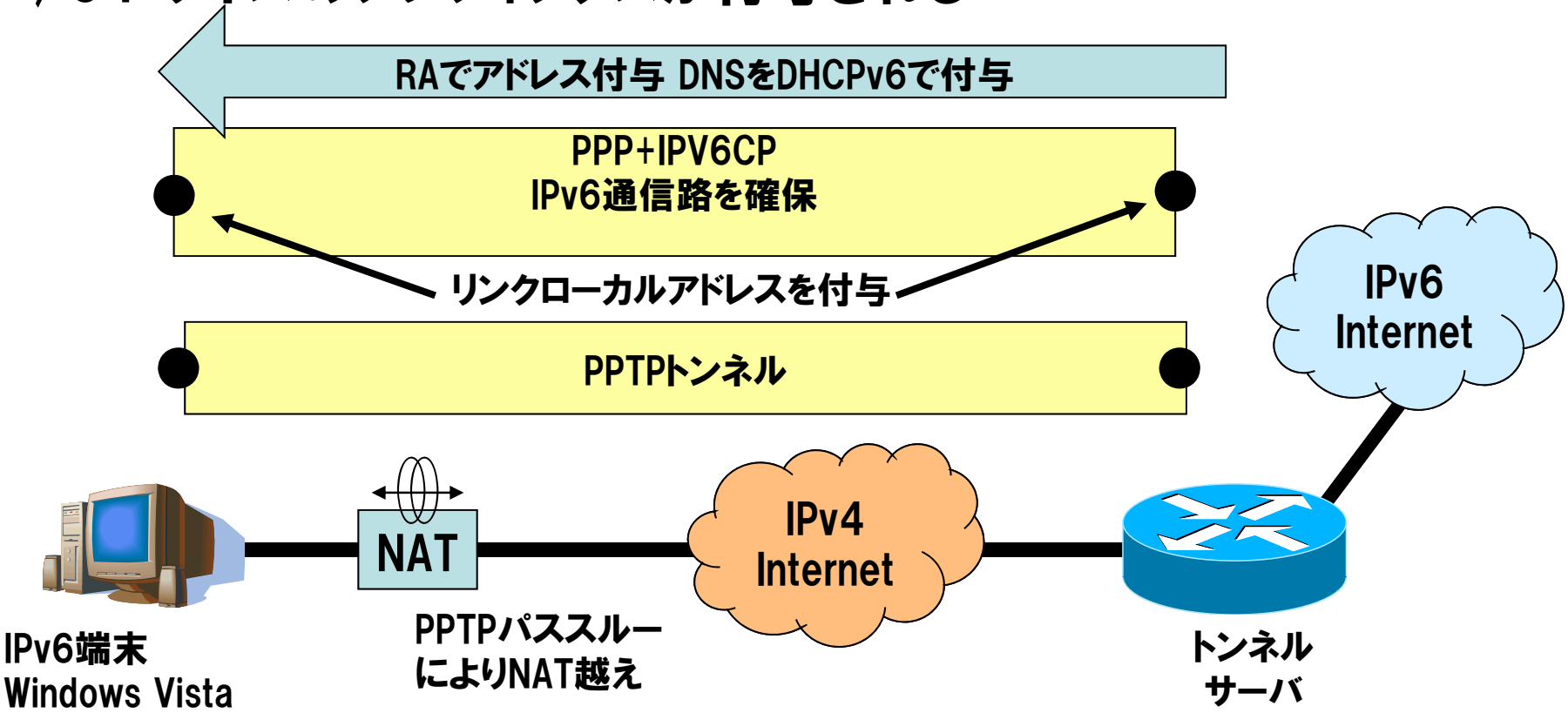
NTT OCNによる個人向けIPv6インターネット接続サービス

- OCNが有償で提供するオプションサービス（300円/月）
- 固定IPv4アドレスは不要
- プライバシーに配慮し 二つのプレフィックスを選択可
  - 固定プレフィックス（/64ひとつ）
  - 動的プレフィックス（接続のたびに値が変わる /64をひとつ）両者を使用可能
- Windows XP, Vista 端末のサポートの他、コレガ社から対応ブロードバンドルータが発売



IIJによるマス向けIPv6インターネット接続サービス

- IIJが自社の顧客向けに無償で提供するオプションサービス
- 固定IPv4アドレスは不要
- Windows Vista向けに接続ソフトを提供している
- /64 サイズのプレフィックスが付与される



その他のトンネルブローカー

- フリービット feel6（DTCP） - http://www.feel6.jp/
  - /48サイズのプレフィックスを委譲（サイト内で再委譲が可能）
  - フリー! 固定/48 が無料で使用可能
  - Windows, Mac OS, Linux など広範なOSのサポート
  - ヤマハ製のブロードバンドルータ（RTシリーズ）がサポート
  - NAT越えには工夫（プロトコル番号41のマッピング）が必要

- Hexago freenet6（TSP） – http://www.gogo6.com/
  - フリーで利用可能
  - ソフトウェアGPLで公開されており、多くの機種で動作可能
  - NAT越えに対応している
  - トンネル終端サーバが北米にあるため国内からの接続はやや不利

家庭・SOHO向けIPv6ルータの現状

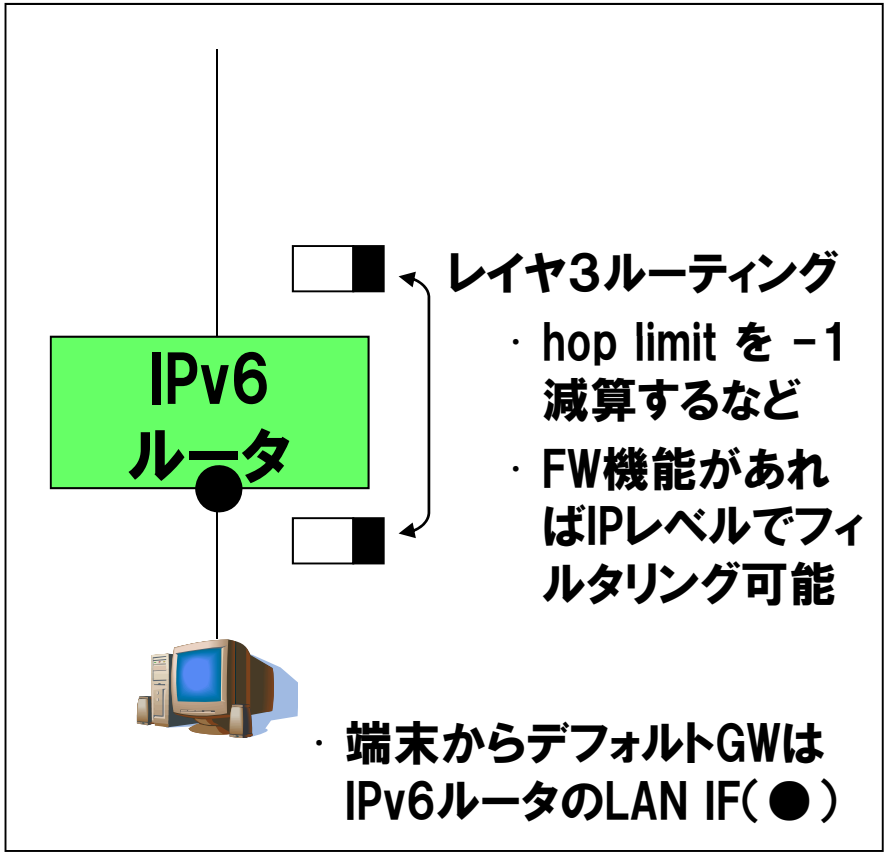
家庭・SOHO向け市販IPv6ルータのラインナップ

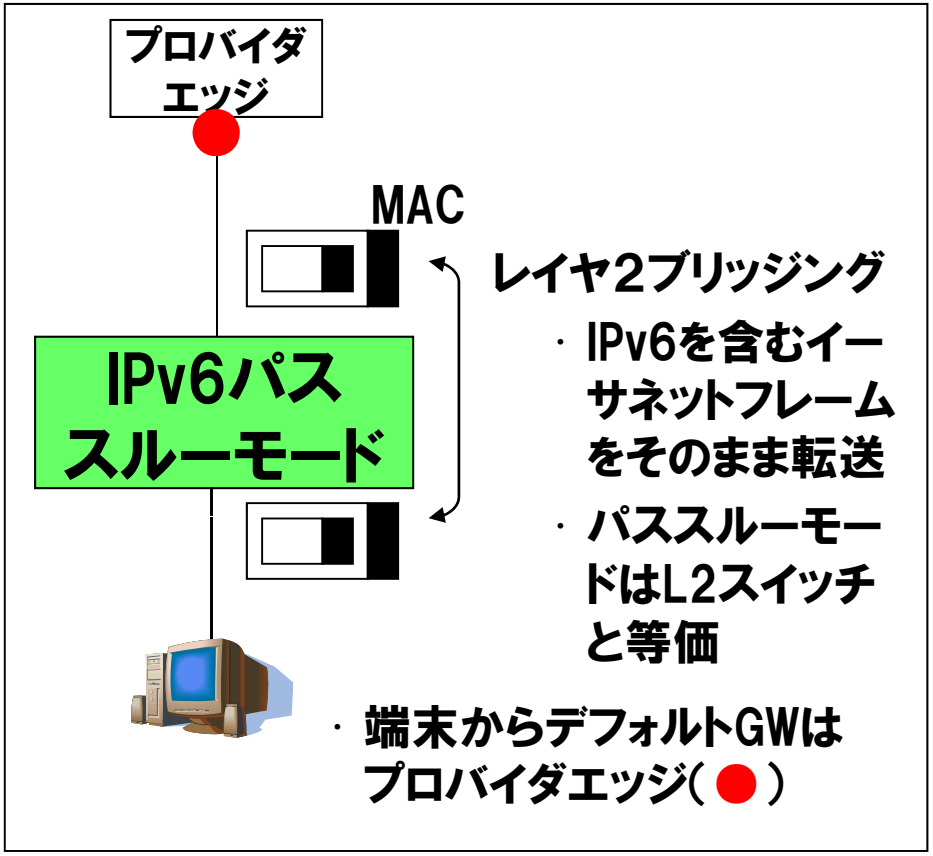
家庭・SOHO向けのIPv6ルータ製品群も選択肢が広がりつつある

メーカ 機種名	主な特徴	参考 価格
NEC UNIVERGE IX2005 	IPv6ルーティングのほか、IPsec, VRRP, QoSなど高度な機能に対応した企業向け	6万円 程度
アライドテレシス CentreCOM AR415S 	IPsec, VRRP, IEEE802.1x など、高度な機能に対応した企業向けVPNアクセスルータ	6万円 程度
ヤマハ NetVolante RT58i 	IPv6ルーティング, SPIファイヤウォールを搭載 DTCP, RA proxy（NTTフレッツ向け機能）	3万円 程度
バッファロー WZR-AMPG300NH 	Win Vista Premiumロゴ取得。6to4でのIPv6インターネットアクセスをサポートしている	1～2万 円程度
アップル AirMac Extreme, AirMac Express 	6to4によるIPv6インターネットアクセスをサポート。Extremeはファイヤウォール機能を装備	16,800円 9,800円
コレガ CG-BARPRO6 	OCN IPv6への接続機能をサポート 現在は販売終了	1万円 未満

IPv6対応（パススルーモード）の注意点

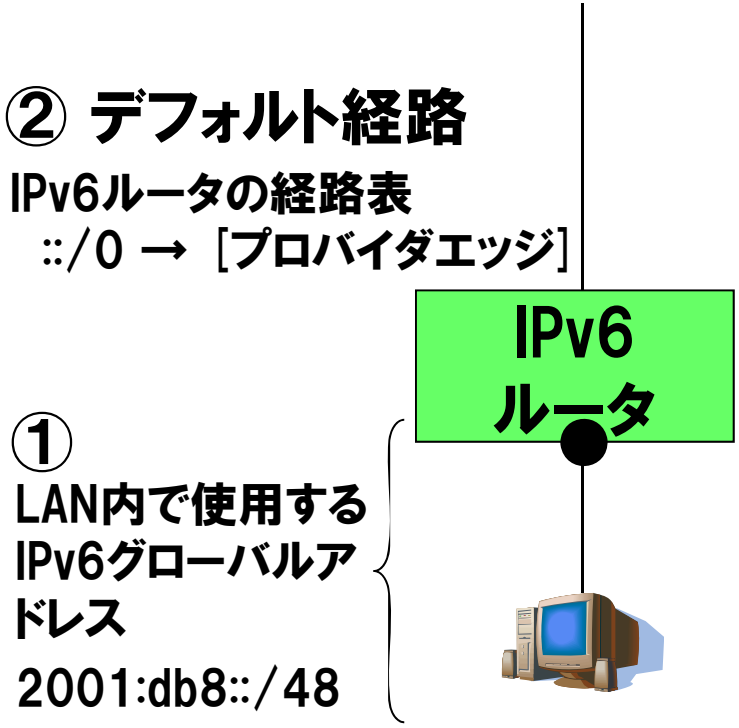
IPv6パススルーモードはレイヤ3ルーティング機能ではない
ブロードバンドルータ購入時の「IPv6対応」の表記には注意





IPv6アドレス割り当てと
デフォルトルータの配布方式

IPv6アドレスの配布とデフォルト経路の設定



① IPv6アドレスの割り当て方法

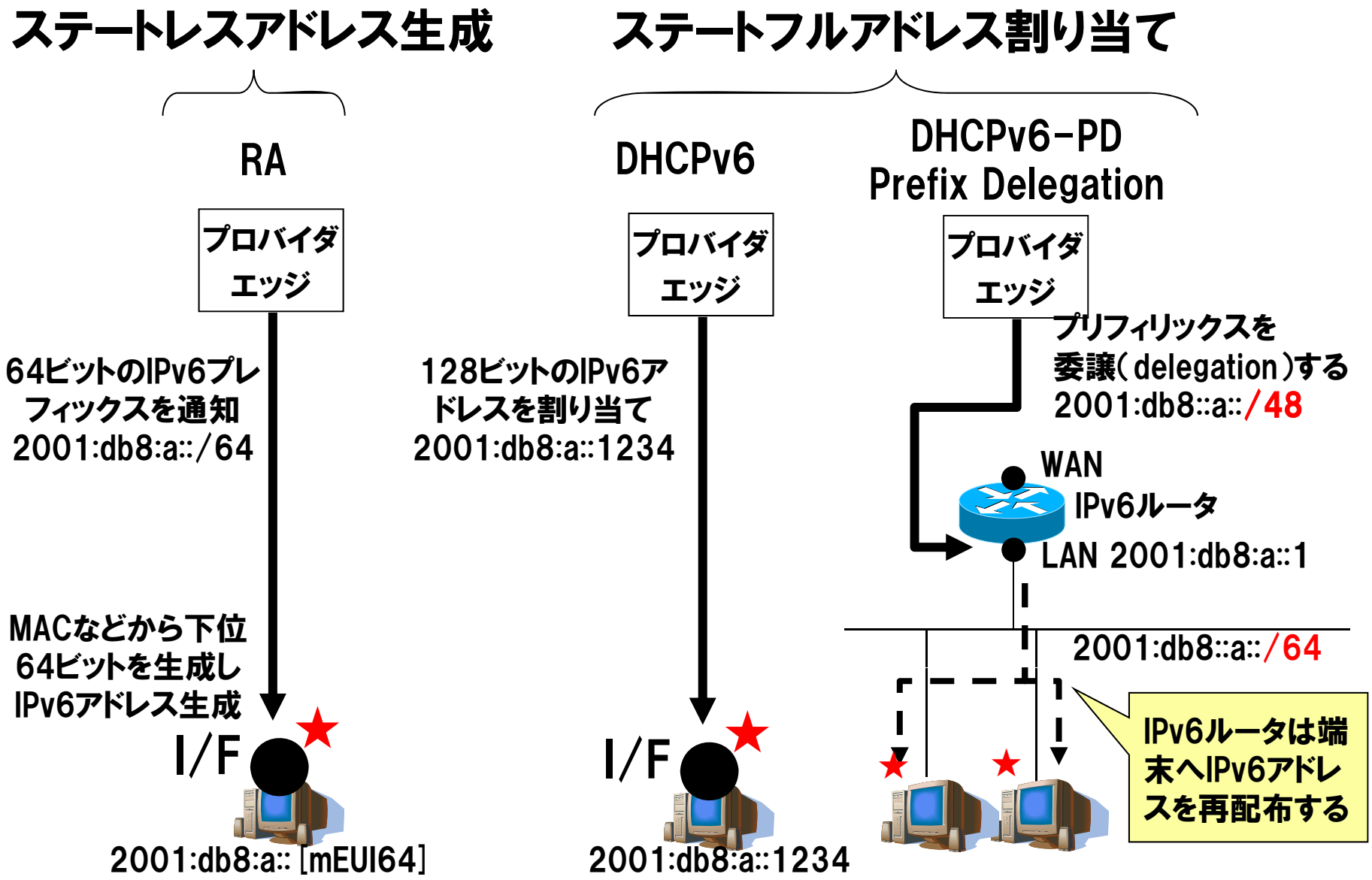
（1）手動割り当て

- IPv6ルータにアドレス情報をあらかじめ手動設定しておく方法
- IPv6アドレス情報は書面等で通知
- 外部接続がスタティックトンネルの形態で使われることが多い

（2）自動割り当て

- ISPからRA, DHCPv6などの自動設定プロトコルを使ってアドレスを通知する
- 固定アドレス割り当てが一般的だが動的な割り当て行う運用も可能

NTT ①-（2） 動的なIPv6アドレス割り当て方式

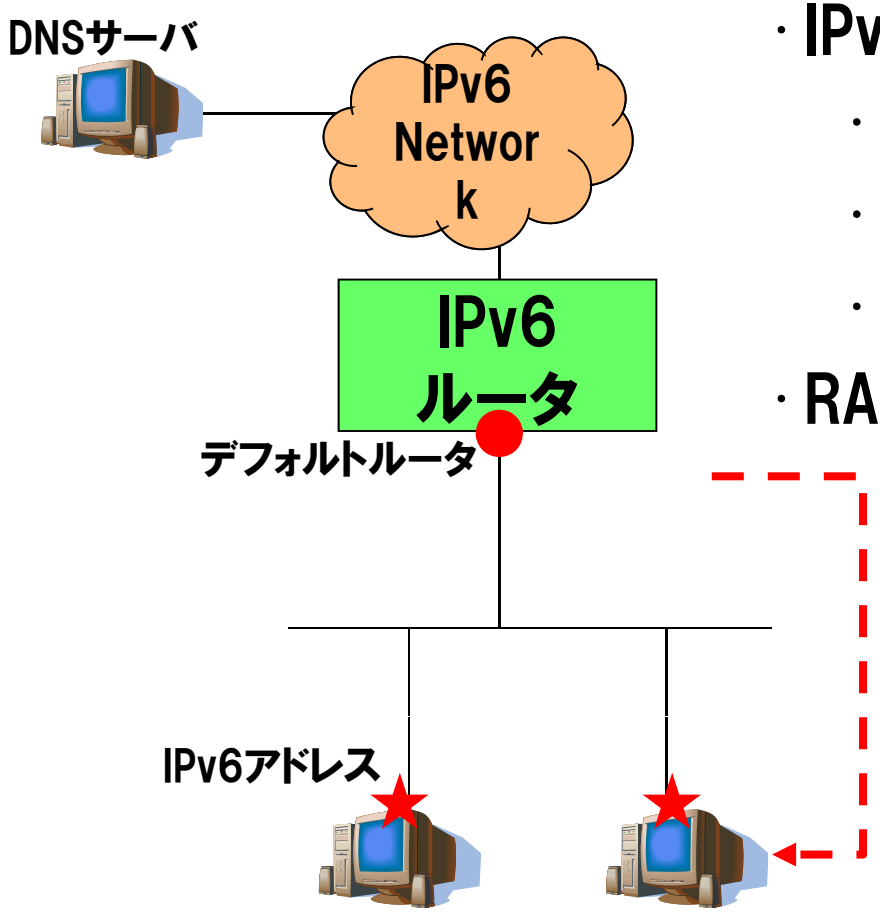


主要なIPv6接続サービスの接続方式

サービス名	外部接続	アドレスサイズ	アドレス割り当て手法	②デフォルトルータ付与手法	その他
OCN IPv6トンネル接続サービス	IPv6 over IPv4 スタティックトンネル	/48	手動設定	手動設定	
IIJ IPv6トンネルサービス	IPv6 over IPv4 スタティックトンネル	/48	手動設定	手動設定(RIPngでの経路広告が必要)	
OCN IPv6	PPP/L2TPトンネル	/64×2	RA	DHCPv6-PC	
IIJ仮想アクセス	PPP/PPTP	/64	RA	RA	DNSをステートレスDHCPv6で通知
フリービット feel6	DTCP	/48	DTCP	DTCP	
Hexago Freenet6	TSP	/64	TSP	TSP	
フレッツ光ネクスト(NGN)	Ethernet IPv6ネイティブ	/48	RA	DHCPv6-PDまたはRA	

LAN内部の端末設定

家庭・SOHOのLAN内部の端末設定



- IPv6ルータから端末へ付与する情報
  - IPv6アドレス
  - デフォルトルータ
  - DNSサーバ
- RA, DHCPv6の利用が一般的

端末OSは Windows Vista, 7 を想定

DHCPv4とDHCPv6の違い

DHCPv4	DHCPv6
・IPv4アドレス	・IPv6アドレス
・サブネットマスク	・~~サブネットマスク~~ なし！
・デフォルトゲートウェイ	・~~デフォルトゲートウェイ~~ なし！
・DNS情報	・DNS情報
・その他付加的情報（NTP, SIP など）	・その他付加的情報（NTP, SIP など）
・端末識別はMACアドレス	・端末識別はDUID

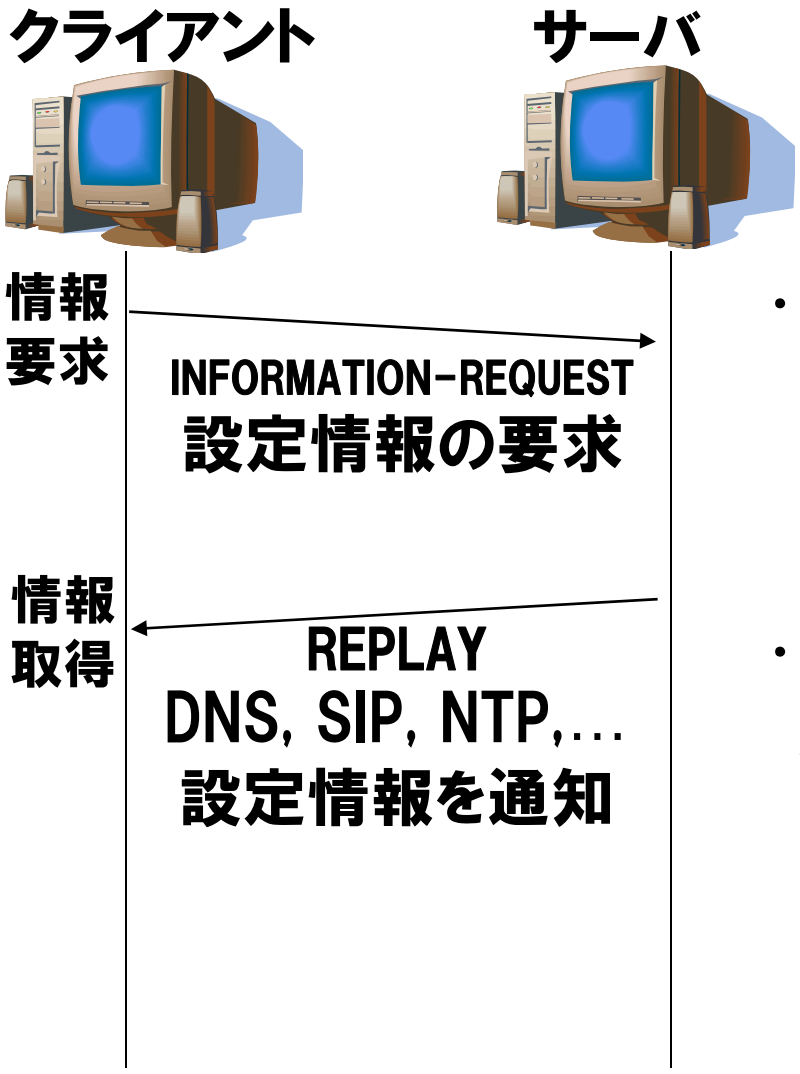
DHCPv6はデフォルトゲートウェイ付与不可
Router Advertisement（RA）の併用が必要

DHCPv6とRAの連携によるアドレス付与

- Router Advertisement（RA）
  - 本来の役目は「ルータの存在」を「広告」するもの
    - ⇒ 端末はRAの送信元をデフォルトゲートウェイに設定
  - アドレス情報（prefix information option）はオプション
    - ⇒ アドレス情報なしのRAもありえる
- RAがもつ2つのフラグ：m/o flags

Managedフラグ	Otherconfigフラグ
・RA: デフォルトGW ・DHCPv6: アドレス, DNS	・RA: アドレス, デフォルトGW ・DHCPv6: DNS

stateless-DHCPv6（RFC3736）



- サーバがクライアントの状態を管理しない
- 端末の設定情報（DNS, SIP, NTP）のみを渡す
- １往復（２メッセージ）だけで情報を取得

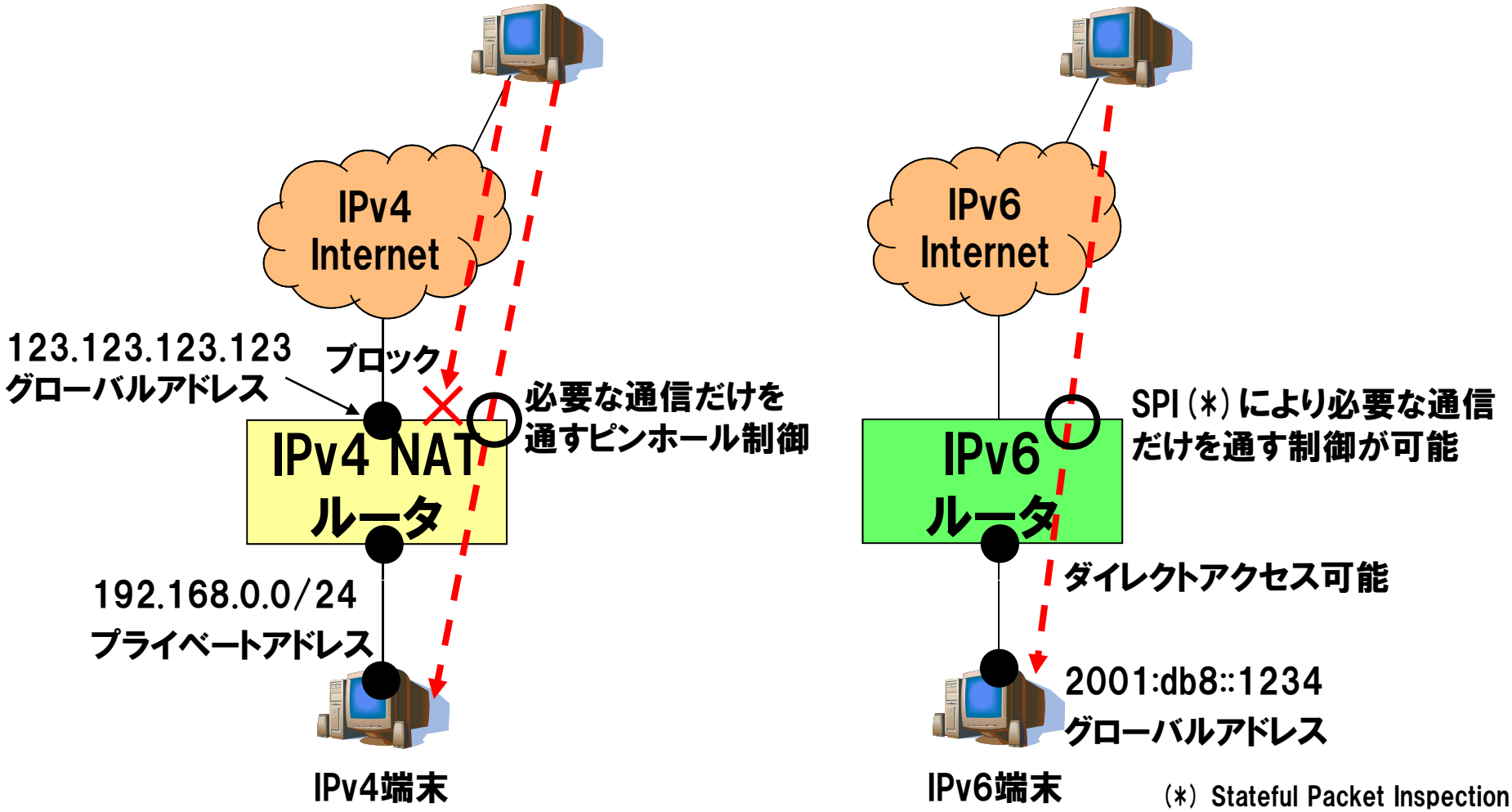
NTT

家庭・SOHO環境でのセキュリティ

IPv4プライベートアドレス＋NAT と IPv6の比較

適切なパケットフィルタリングでIPv4 NATと同等なセキュリティを確保

RFC4864（Local Network Protection for IPv6）は安全性担保の方法を記述



(*) Stateful Packet Inspection

NTT デュアル環境でのセキュリティ上の注意点

- ファイヤウォールポリシの不整合に注意
  - IPv4は適切なポリシーが設定されていても
  - IPv6は一切の制御なし、全通信が許可では意味がない

  ⇒ 基本的にIPv4/IPv6同一ポリシで運用するのが望ましい

- 自動トンネルによる意図しない外部接続
  - 6to4, Teredo

    Windows Vista/7 ではデフォルトでON

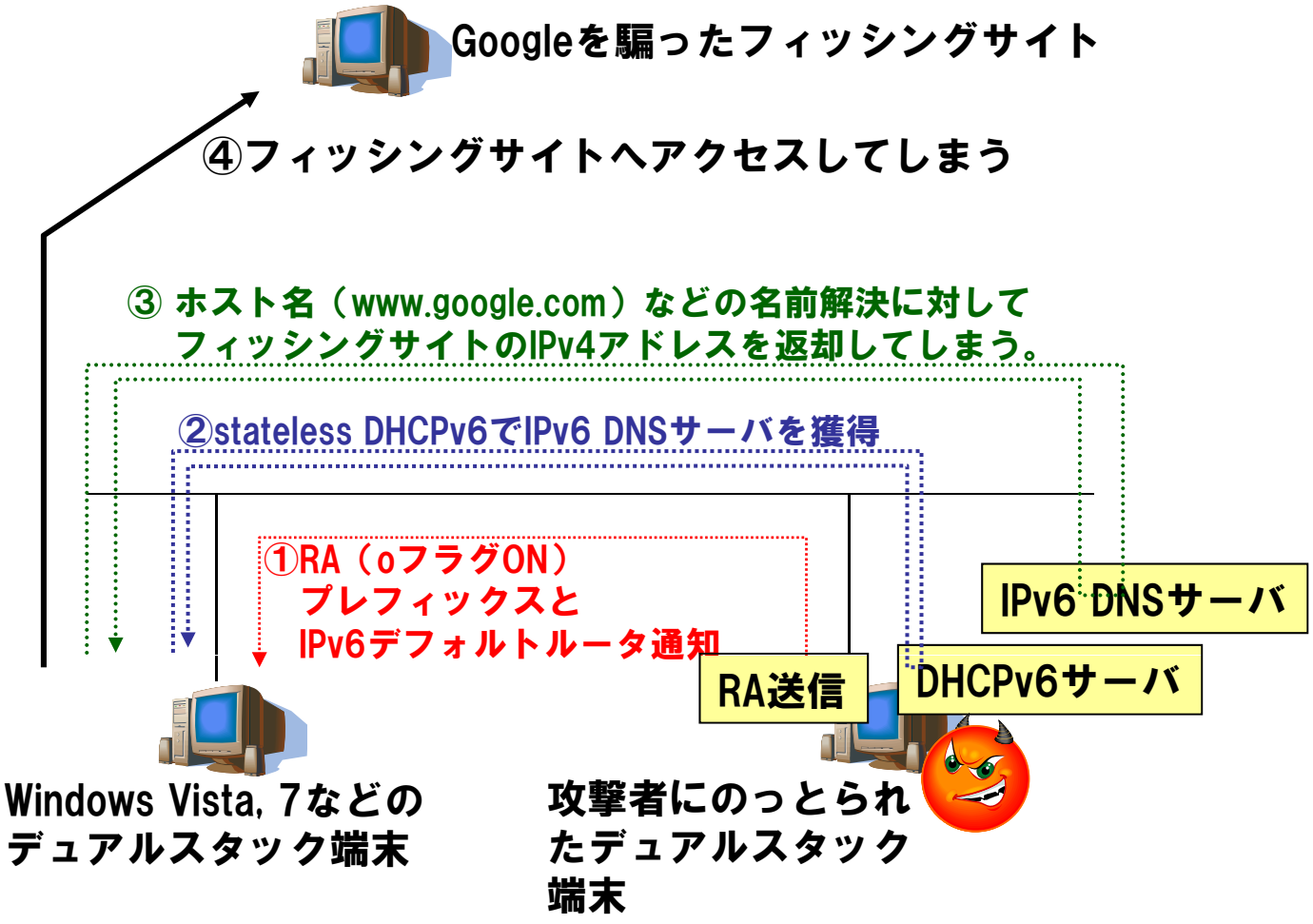
  ⇒ 意図しない外部接続性を放置しないこと

  [対処法] LAN内部からのIPv4パケットを遮断する
    - プロトコル番号41（IPv6 over IPv4トンネル, 6to4）
    - UDP ポート 3544（Teredo）

デュアル環境に対する攻撃例

デュアルスタック環境ではIPv4, IPv6が相互に影響しあう場面がある

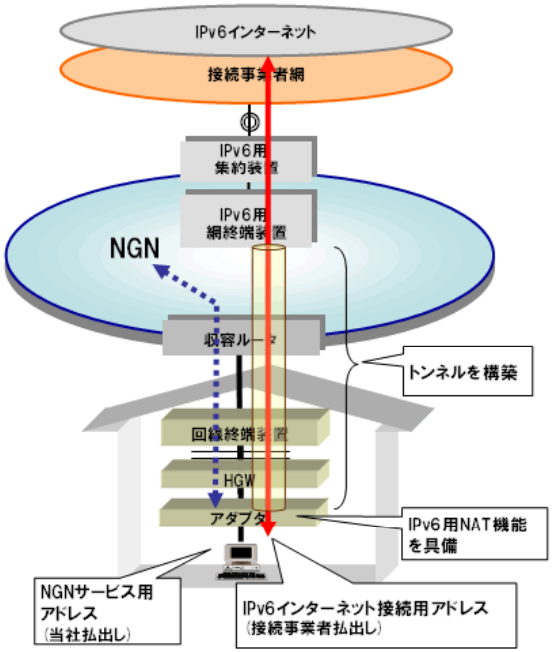
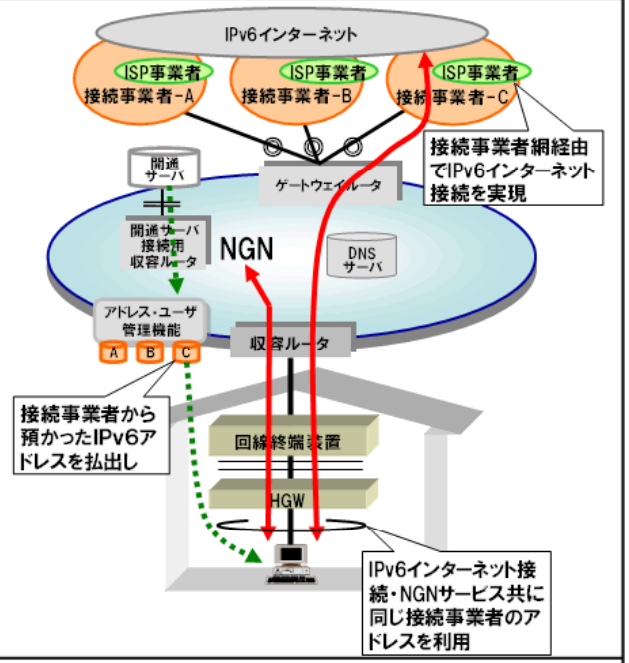
■ DHCPv6とDNSを使った攻撃例 – 多くのIPv6/IPv4デュアル端末はIPv6を優先して使用



NGN上で提供予定の
IPv6インターネット接続機能

NGNが提供予定のIPv6インターネットアクセス

NTT東西のニュースリリースより

接続機能	トンネル方式	ネイティブ方式
概　要	アダプタからIPv6用網終端装置までの間に新たにトンネルを構築してIPv6インターネット接続を実現する機能	接続事業者様※1から預かったIPv6アドレスを当社が払い出し、IPv6インターネット接続を実現する機能 ※1 NGNと直接接続する接続事業者様の最大数は当面3社。
		
接続事業者様にご負担いただく費用範囲※2	IPv6用集約装置、およびIPv6用網終端装置のうち一部（インタフェースパッケージ相当）に係る費用※3 ※3　現行のIPv4インターネット接続と同様。	ゲートウェイルータ、DNSサーバ※4およびNGNへの追加開発※4に係る費用 ※4　接続事業者様と当社との間で利用割合に応じて負担。

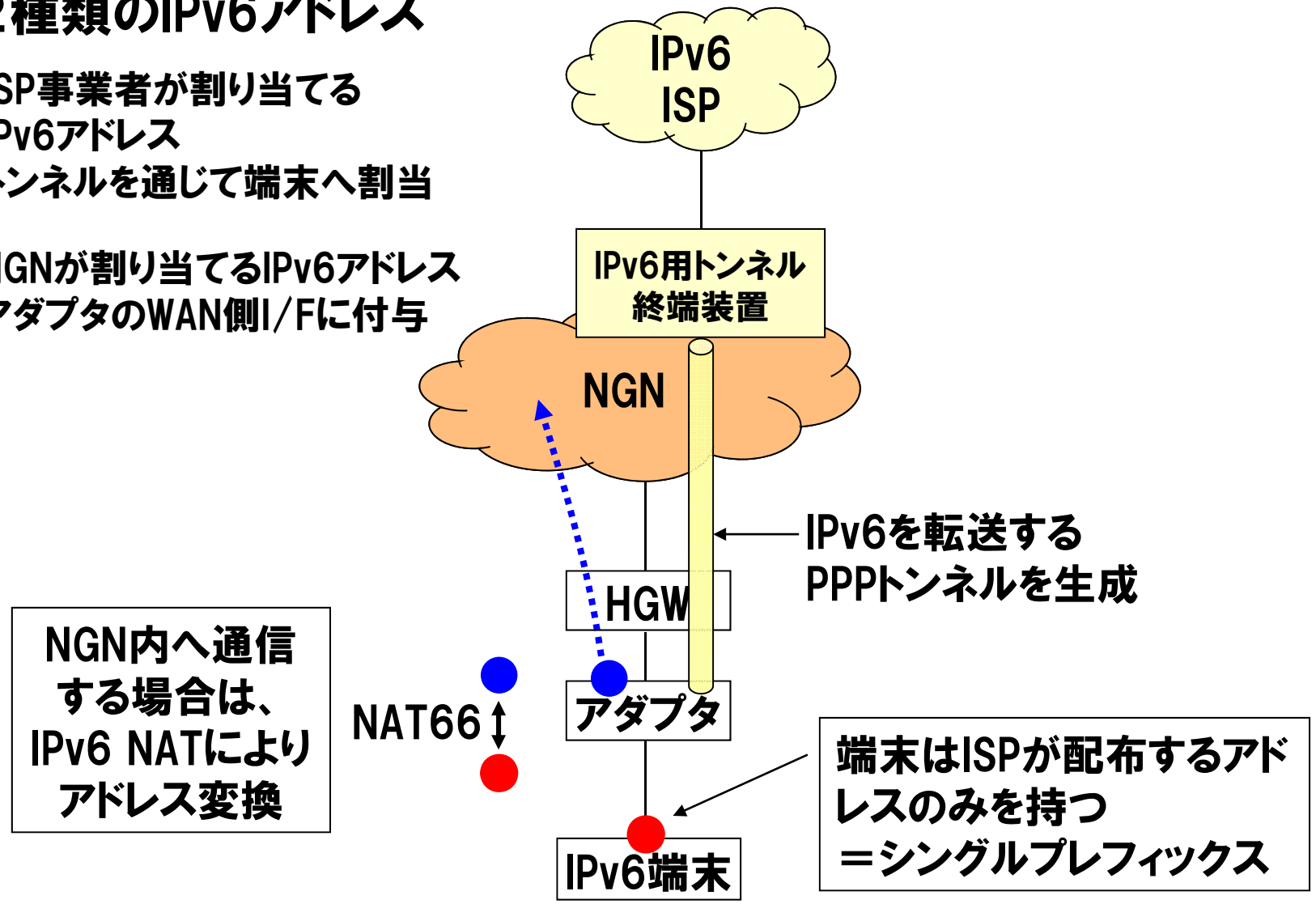
※2　費用については、接続約款に規定する網改造料の算出式に基づき算定。

（参考）次世代ネットワーク（NGN）におけるIPv6インターネット接続機能の提供に係る接続約款変更の認可申請について
http://www.ntt-east.co.jp/release/0905/090519b.html
http://www.ntt-west.co.jp/news/0905/090519a.html

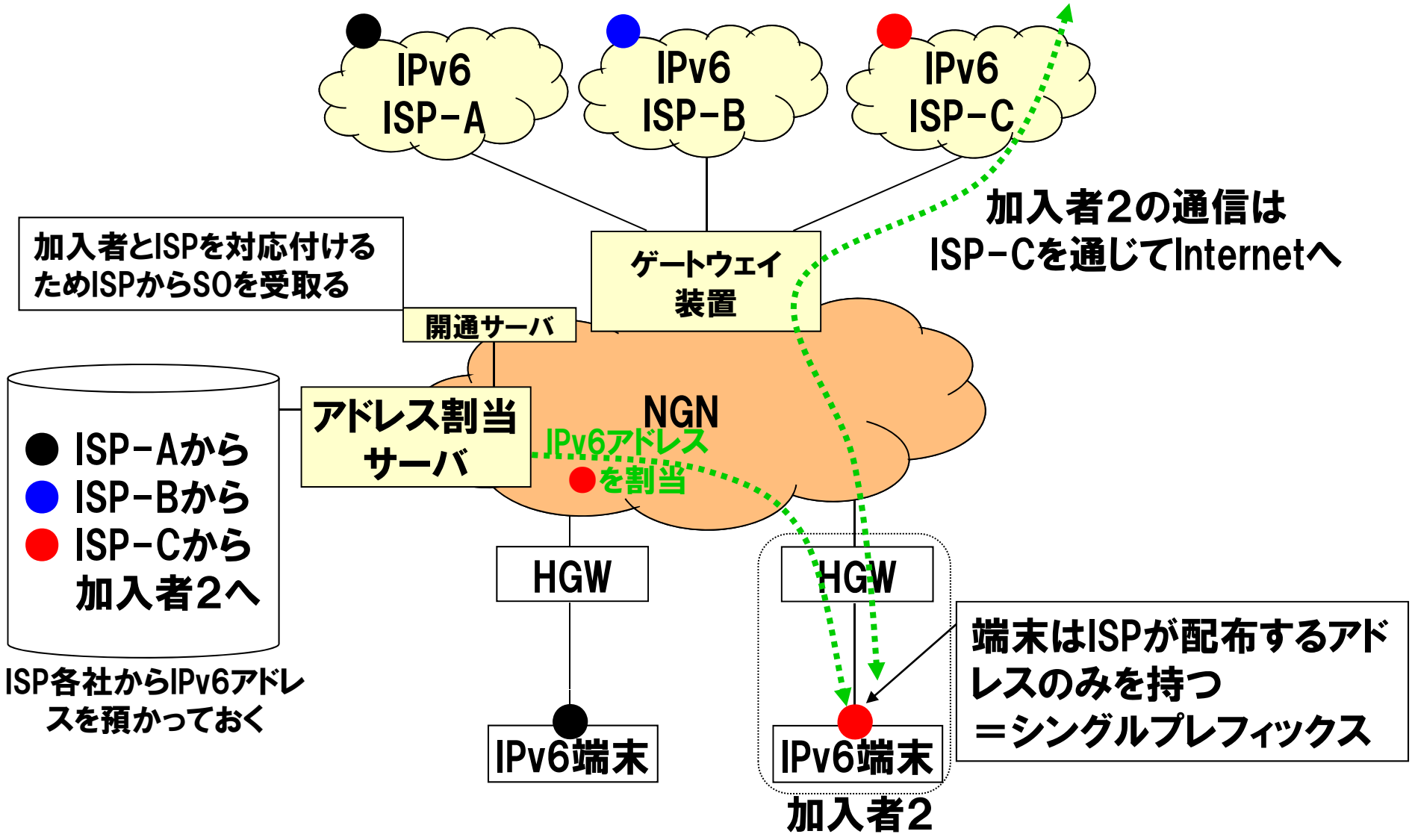
IPv6アドレスの扱いに注目したトンネル方式の詳細

■2種類のIPv6アドレス

- ISP事業者が割り当てる
  IPv6アドレス
  トンネルを通じて端末へ割当
- NGNが割り当てるIPv6アドレス
  アダプタのWAN側I/Fに付与



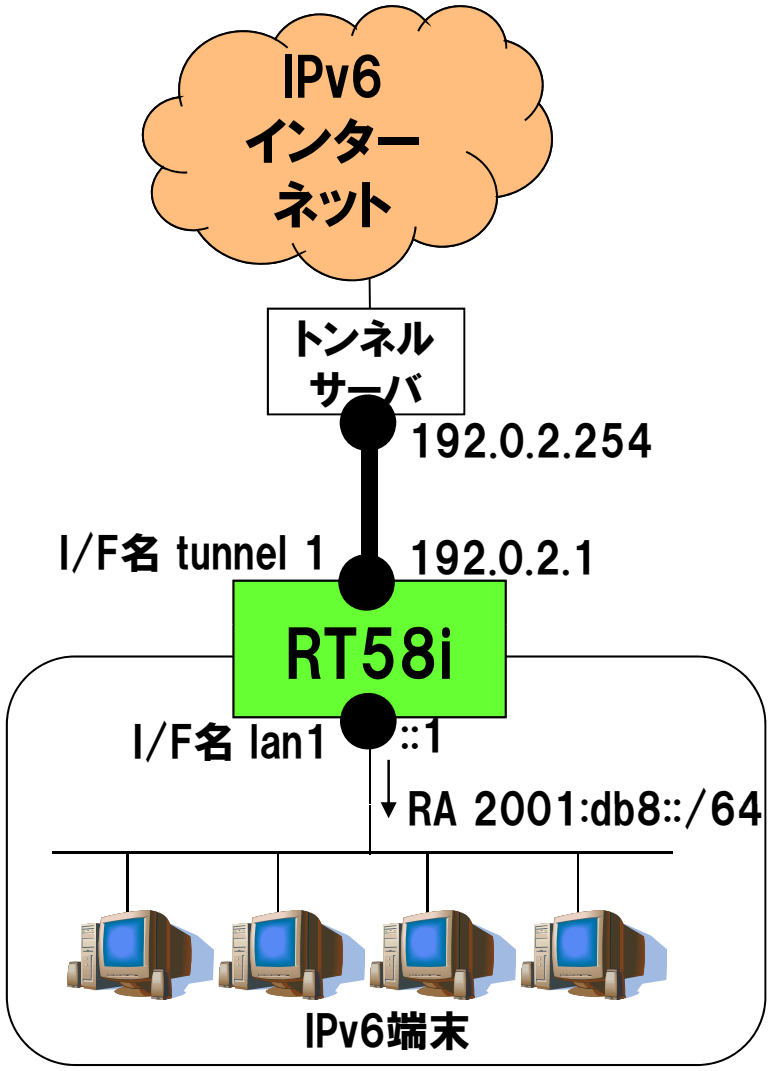
IPv6アドレスの扱いに注目したネイティブ方式の詳細



ヤマハ製ブロードバンドルータ
RT58iでの設定例

ヤマハRT58iによる設定例(１)

IPv6 over IPv4 トンネルによる接続

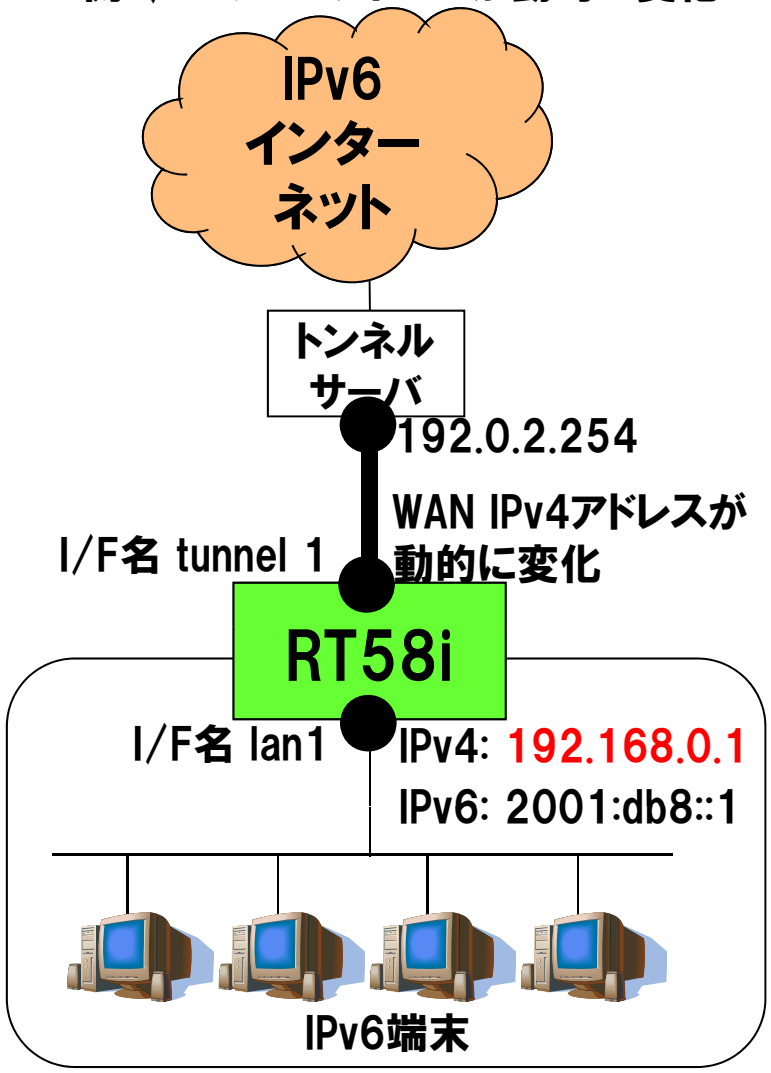


- 外部接続
  - 接続方式 IPv6 over IPv4 スタティックトンネル
    - 192.0.2.1 ⇔ 192.0.2.254
  - プレフィックス 2001:db8::/48 を通知されている
- 内部設定
  - プレフィックス 2001:db8::/64 を端末へ割当て

```
# IPv6ルーティングをON
ipv6 routing on

# トンネルデバイスを作成
tunnel select 1
  encapsulation ipip
  endpoint address 192.0.2.1 192.0.2.254
  tunnel enable 1

# デフォルトゲートウェイをトンネルに向ける
ipv6 route default gateway tunnel 1

# LAN内の設定
ipv6 lan1 address 2001:db8::1/64
ipv6 prefix 1 2001:db8::/64
ipv6 lan1 rtadv send 1 o_flag=on
```

ヤマハRT58iによる設定例(２)

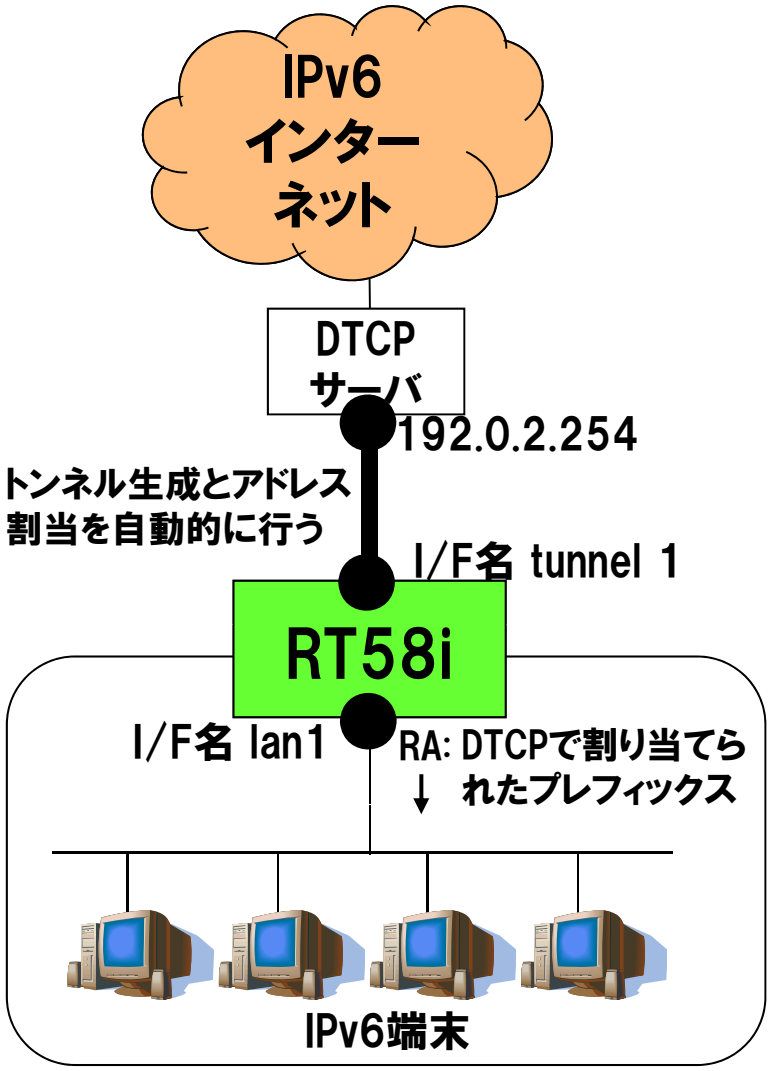
IPv6 over IPv4 トンネルによる接続
WAN側 I/F のIPv4アドレスが動的に変化




```
# IPv6ルーティングをON
ipv6 routing on

# トンネルデバイスを作成
# エンドポイントを（LANプライベートアドレス）-（トンネルサーバ）
tunnel select 1
  encapsulation ipip
  endpoint address 192.168.0.1 192.0.2.254
  tunnel enable 1

# デフォルトゲートウェイをトンネルに向ける
ipv6 route default gateway tunnel 1

# LAN内の設定
ipv6 lan1 address 2001:db8::1/64
ipv6 prefix 1 2001:db8::/64
ipv6 lan1 rtadv send 1 o_flag=on

# NAT設定
nat descriptor type 1 masquerade
nat descriptor masquerade static 1 1
                              192.168.0.1 ipv6 *
pp select 1
  ip pp nat descriptor 1
```

ヤマハRT58iによる設定例(３)

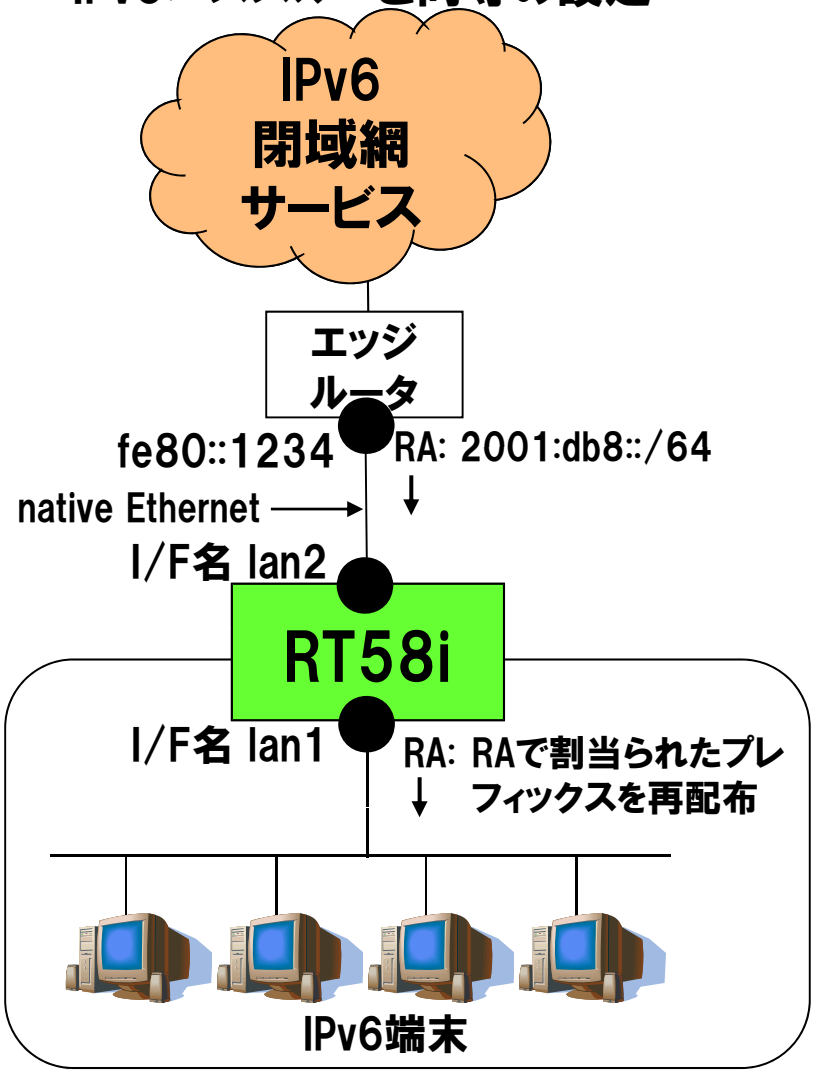
DTCPによるトンネル接続




```
# IPv6ルーティングをON
ipv6 routing on

# DTCPトンネルを作成 - feel6サービスへの接続例
tunnel select 1
  tunnel dtcp dtcp.feel6.jp
              myname USERID PASSWORD
  tunnel enable 1

# デフォルトゲートウェイをトンネルに向ける
ipv6 route default gateway tunnel 1

# LAN内の設定
ipv6 lan1 address dtcp-prefix@tunnel1::1/64
ipv6 prefix 1 dtcp-prefix@tunnel1::/64
ipv6 lan1 rtadv send 1 o_flag=on

# 必要に応じてフィルタリング設定も可
ipv6 filter 1 reject
           dtcp-prefix@tunnel1::/64 *
ipv6 filter 2 pass
           * dtcp-prefix@lan2::1 * tcp * www
```

ヤマハRT58iによる設定例(４)

RA-proxy による接続例
IPv6パススルーと同等の設定

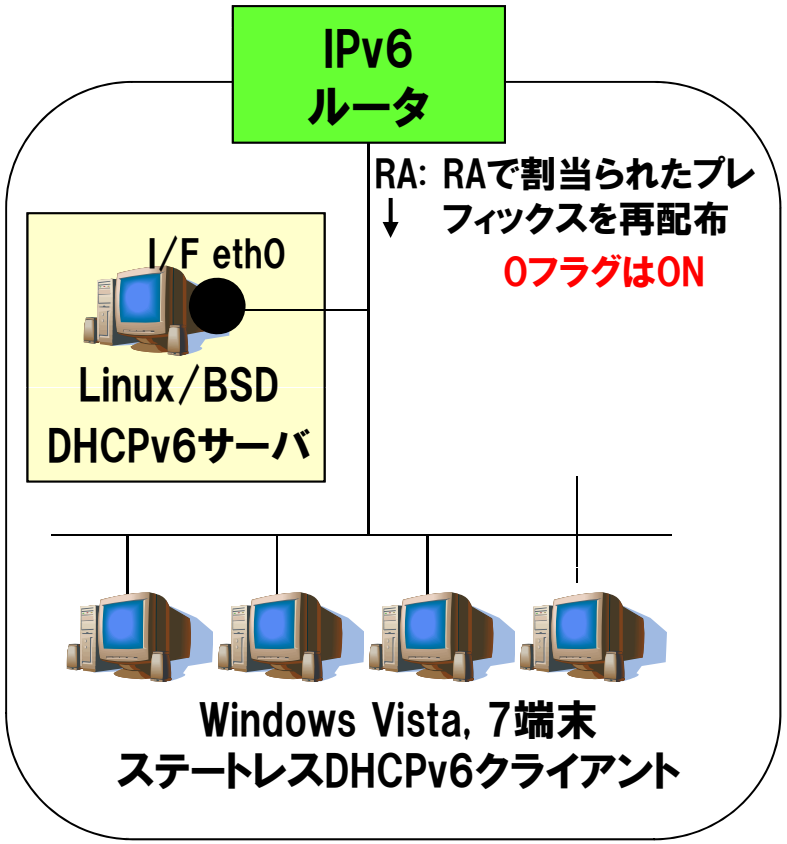



```
# IPv6ルーティングをON
ipv6 routing on

# デフォルトゲートウェイをトンネルに向ける
ipv6 route default gateway tunnel 1

# LAN内の設定
ipv6 lan1 address ra-prefix@lan2::1/64
ipv6 prefix 1 ra-prefix@lan2::/64
ipv6 lan1 rtadv send 1

# RA-Proxyでも必要に応じてフィルタリング設定も可
# IPv6パススルーに対応したルータでも、フィルタリングは
# ほとんど実装されていない
ipv6 filter 1 reject
            ra-prefix@tunnel1::/64 *
ipv6 filter 2 pass
            * ra-prefix@lan2::1 * tcp * www
```

ステートレスDHCPv6サーバの設定例

ステートレスDHCPv6サーバの設定例

WIDE-DHCPv6サーバによる設定例



■ステートレスDHCPv6サーバの設定と起動

dhcp6s.conf への記述内容

```
option domain-name-servers 2001:db8::53;
option domain-name “example.jp";
```

ステートレスDHCPv6サーバの起動

```
# dhcp6s -c dhcp6s.conf eth0
```

■Windows Vista 端末での情報取得の様子

```
C:¥> ipconfig /renew6
C:¥> ipconfig /all
イーサネット アダプタ ローカル エリア接続:
   接続固有の DNS サフィックス. : example.jp
   DHCP 有効 ..... : はい
   自動構成有効 ..... : はい
   IPv6 アドレス ..... : 2001:db8::XXXX(優先)
   デフォルト ゲートウェイ ..... : fe80::XXXX%1
   DHCPv6 IAID ..... : 268869872
   DHCPv6 クライアント DUID . : 00-01-00-01-11-62-4C
                                -59-00-1C-25-9F-8A-36
   DNS サーバー ..... : 2001:db8::53
```

http://sourceforge.jp/projects/sfnet_wide-dhcpv6/