Global ICT Partner
Innovative. Reliable. Seamless.

NTT Communications

IPv6セキュリティの勘どころ
家庭・SOHOネットワークでのIPv6セキュリティ

NTTコミュニケーションズ株式会社
先端IPアーキテクチャセンタ
IPコアテックTU
山形育平

2011/12/01

AGENDA

Global ICT Partner
Innovative. Reliable. Seamless.
NTT Communications

1. 来場の皆さまへ質問
2. 現在のIPv6対応状況
3. 家庭・SOHOネットワークの
   IPv6セキュリティについて
   - ネットワーク構築において気をつける点
   - IPv6の仕様による課題
   - デュアルスタックによる影響
   - ホストの実装
4. まとめ

来場されている方々へ質問

Global ICT Partner
Innovative. Reliable. Seamless.
NTT Communications

- あなたのご自宅の環境はどれにあてはまりますか？

1. ネットワークはIPv6に対応しているし，機器もすべてがIPv6対応です
2. ネットワークはIPv6に対応しているが，一部の機器がIPv6未対応です
3. ネットワークがまだIPv6に対応していないですが，近いうちに対応する予定です
4. ネットワークがIPv6に対応するのはまだまだ先の予定です
5. そもそも気にしていません

家庭・SOHO向けIPv6対応製品

Global ICT Partner
Innovative. Reliable. Seamless.
NTT Communications

端末

PC
- Windows
- Mac OS
- BSD
- Linux

Mobile/タブレット
- Windows Phone
- iOS
- Android

その他
ネットワークカメラ

- HDTV
- TV

家庭・SOHO向けルータ(CPE)

- OCN提供 DS-RA01
- NEC製 AtermWR8371N
- Yamaha製 NVR500

IPv6対応サイト

Global ICT Partner
Innovative. Reliable. Seamless.
NTT Communications

Google

検索

gmail

youtube

OCN

OCN Topページ

IPv6でのアクセスを表示

World IPv6 Dayでは

Facebook

Yahoo!

などを中心に420社以上が参加

http://www.attn.jp/worldipv6day/participant.html参照

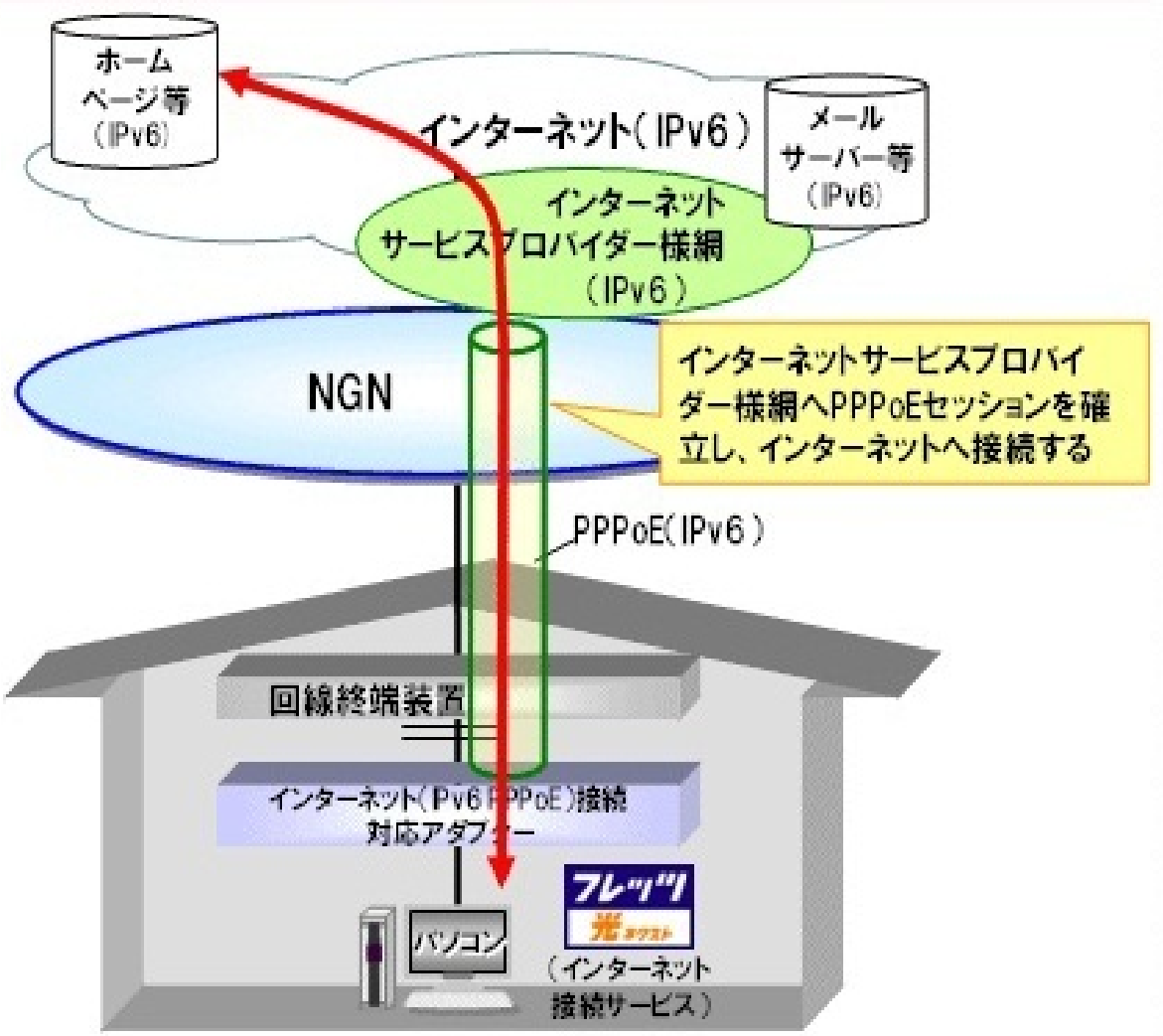
家庭向けIPv6接続サービス

Global ICT Partner
Innovative. Reliable. Seamless.
NTT Communications

フレッツ光ネクストを使用したIPv6接続サービス

IPv6 PPPoE (トンネル方式/案2)

- ISPとユーザ宅内をPPPoEにて接続
  - IPv4と同じ
  - マルチプレフィックス問題解決のためNPT(NAT66)が必要
- ISPを経由したのちInternetへ接続



http://www.ntt-west.co.jp/news/1105/110526d_2.htmlより抜粋

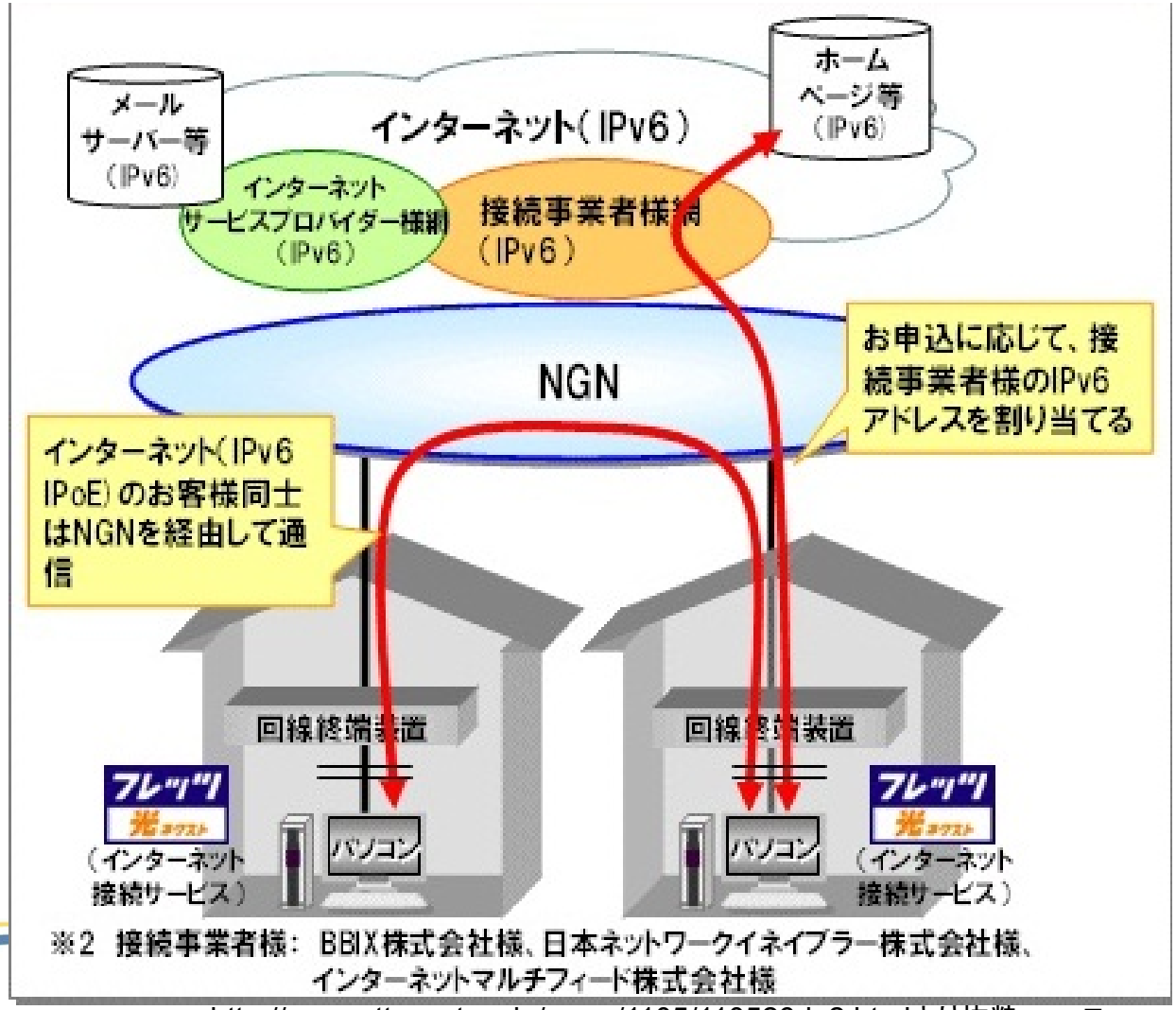
家庭向けIPv6接続サービス

Global ICT Partner
Innovative. Reliable. Seamless.
NTT Communications

フレッツ光ネクストを使用したIPv6接続サービス

IPv6 IPoE (ネイティブ方式/案4)

- NGNのアドレスではなく接続事業者のアドレスを付与
  - マルチプレイフィックス問題は発生せず
- 接続事業者を通してインターネットへ接続
  - ISPはNW設備を持たなくともサービス提供が可能



http://www.ntt-west.co.jp/news/1105/110526d_2.htmlより抜粋

家庭向けIPv6接続サービス

Global ICT Partner
Innovative. Reliable. Seamless.
NTT Communications

ISPによってはdefaultでIPv6を
自動的に付与するサービスも

au ひかり

- ISP側装置とユーザ宅内装置のversionUPにより提供開始
- ユーザは何もすることなくIPv6アドレスが付与される状態に
- 追加料金なし

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

Xi(moperaU)

- XiでかつmoperaUに申し込むことにより提供開始
- ユーザはIPv6を使用するための追加の申し込みを行う必要はなし
- 追加料金なし

http://www.mopera.net/service/option/internet/ipv6/index.html参照

- 他にも既にIPv6でサービス開始しているものや検討しているものもあり

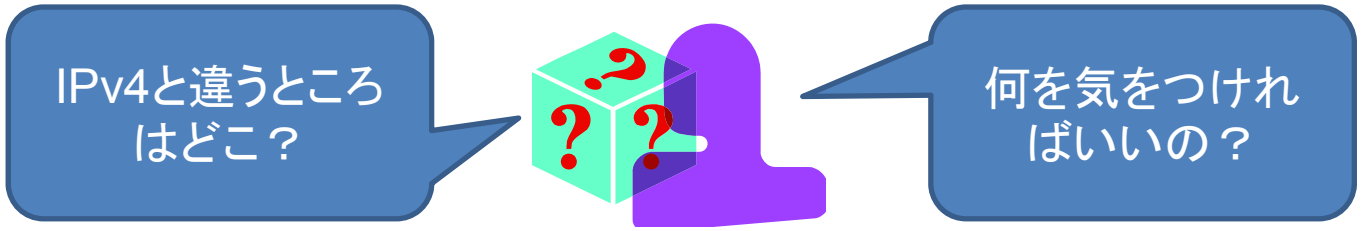
装置・端末・サービスともにIPv6 ready

Global ICT Partner
Innovative. Reliable. Seamless.
NTT Communications

家庭・SOHO向けの通信もIPv6 ready!!

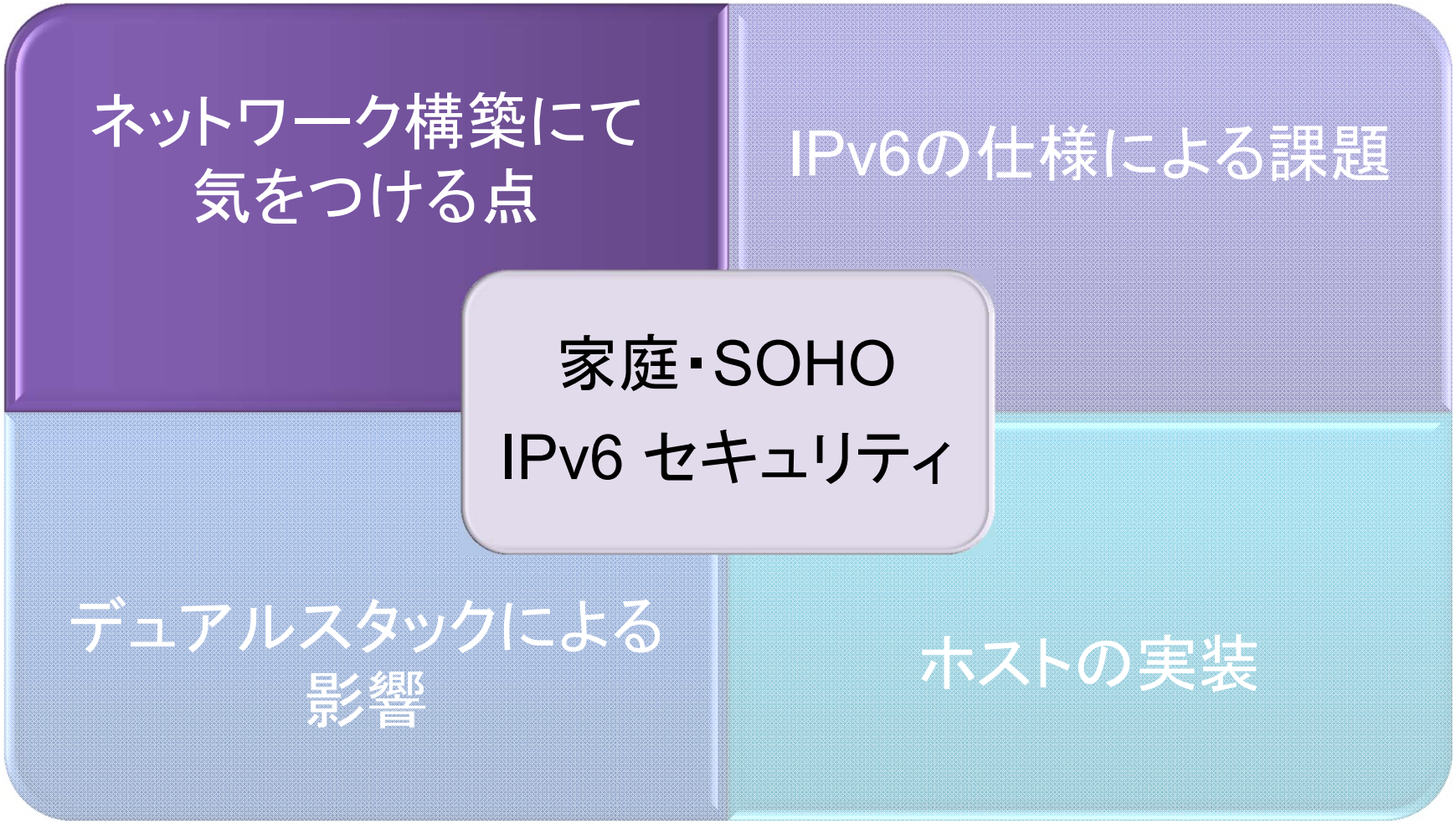
知らないうちにIPv6を使っているかも

ネットワークを構築する上でのセキュリティは？

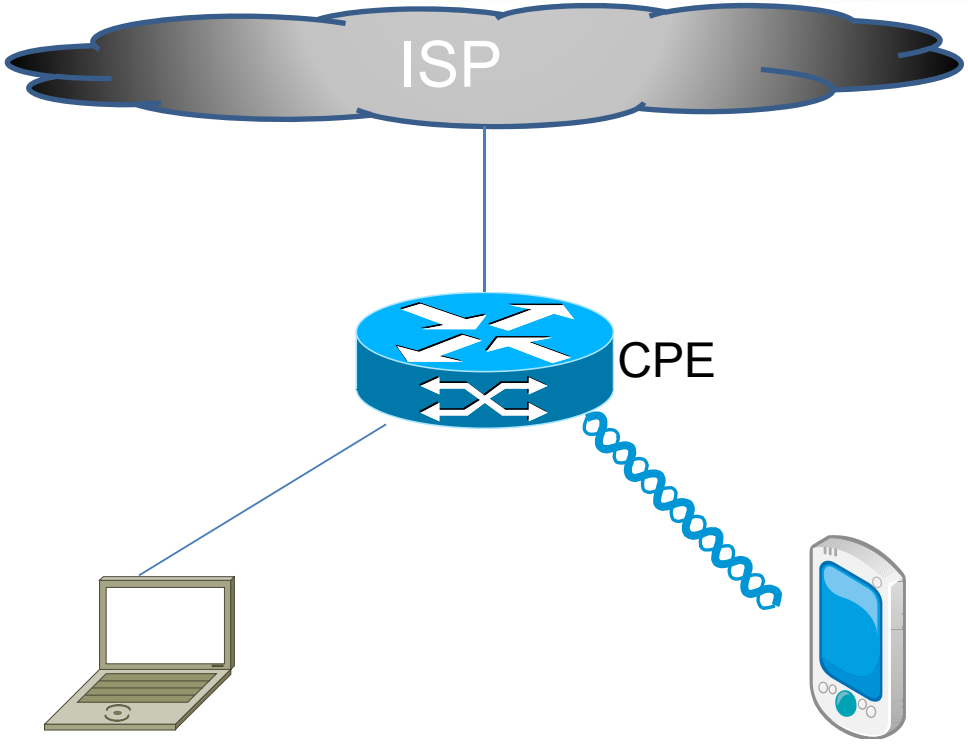


- ここでは家庭・SOHOネットワークのIPv6に関するセキュリティについて述べさせていただきます
  - ネットワークを構築・利用する際に気をつける点
  - ISPや企業が個人向けサービスを行ううえで気をつける点

家庭・SOHO向けIPv6セキュリティ



一般的なIPv4 ネットワーク



ISPとの接続点はCPEが存在

CPEでNAT

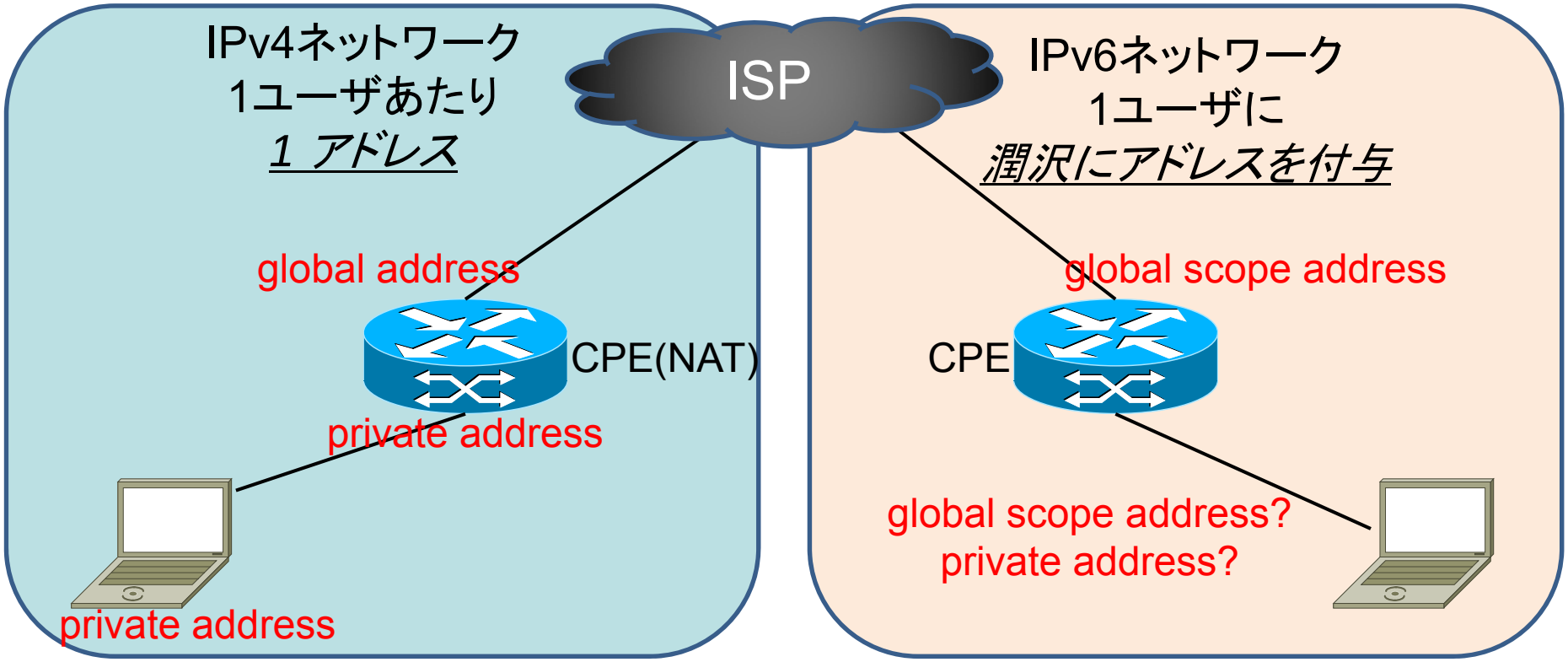
IPv6ネットワークでは
一般的にはどうするべきか？

一般的な？IPv6 ネットワーク

Global ICT Partner
Innovative. Reliable. Seamless.
NTT Communications

IPv6でのネットワーク構築時の大きな変更点

global scope addressを端末にも付与可能



端末にglobal scope addressで大丈夫？

Global ICT Partner
Innovative. Reliable. Seamless.
NTT Communications

- 端末へのglobal scope addressの付与

→NATが不要になる

  - メリット
    - 高い透過性
  - デメリット
    - セキュリティの低下？

IPv4時代のNATによるセキュリティへの恩恵

外部からの通信
の遮断

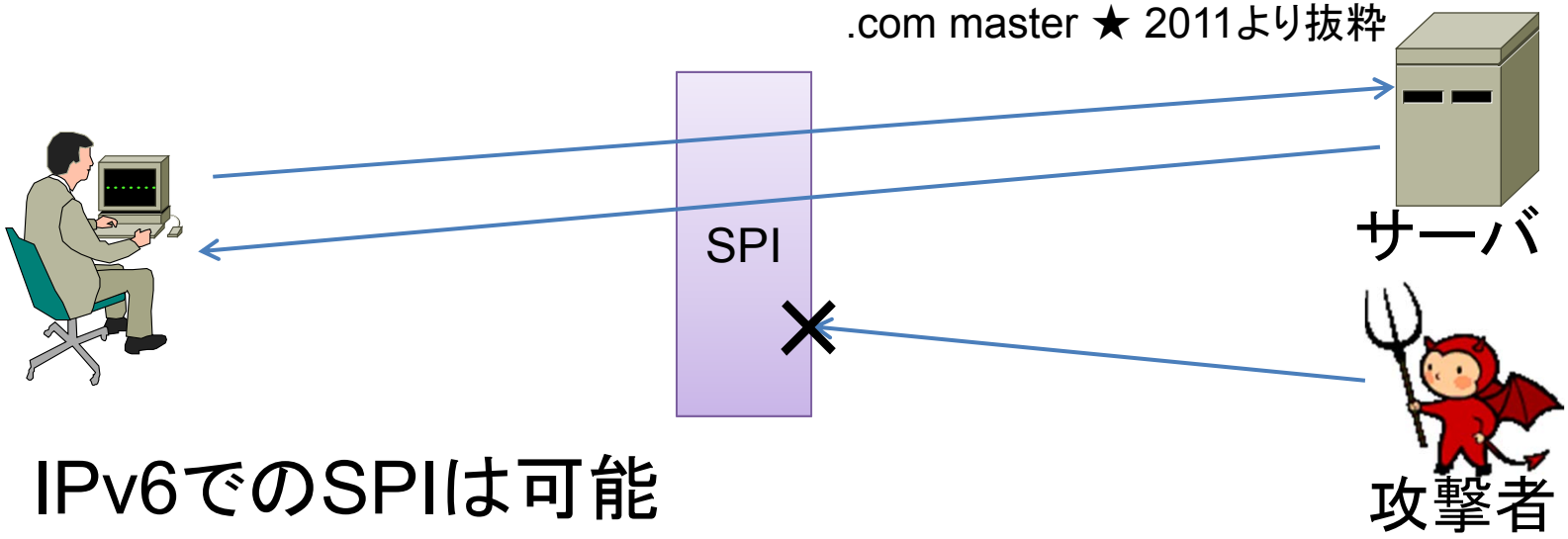
Stateful Packet Inspection(SPI)によるもの

端末にglobal scope addressで大丈夫？

Global ICT Partner
Innovative. Reliable. Seamless.
NTT Communications

SPIとは．．．

内部コンピュータが外部ネットワークに対して実施している
通信状態を記録しておき，その通信に対する応答パケットと
推定できるものだけ内部に通過させる機能



- IPv6でのSPIは可能
  - 一般的なIPv6対応CPEには搭載済み

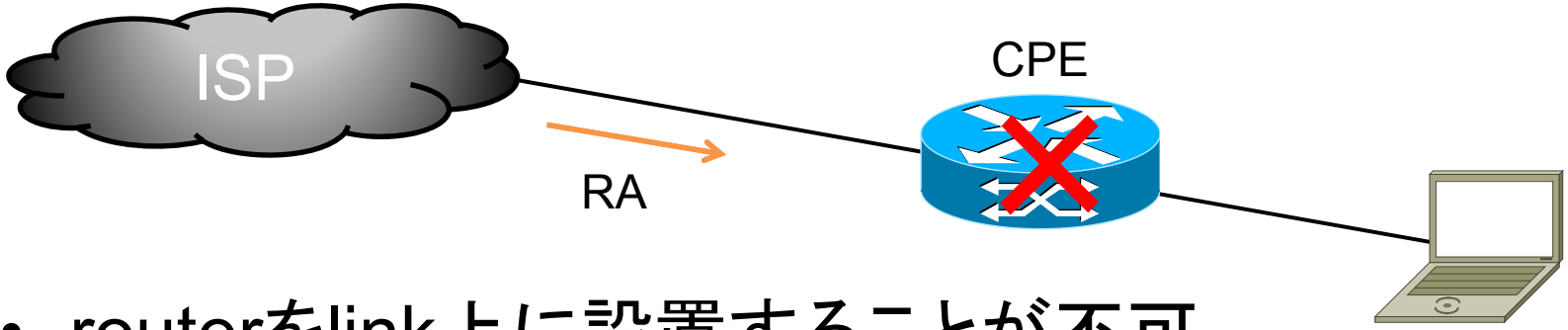
→IPv4と同レベルの防御が可能

端末へのglobal scope addressの付与
+ CPEでのSPIを推奨

【注意】CPEを置けないケース

Global ICT Partner
Innovative. Reliable. Seamless.
NTT Communications

RAでのみアドレスが付与されるサービス
e.g. IPoEでのHGWなし(ひかり電話契約なし)の場合



- routerをlink上に設置することが不可
  - CPEでのSPIが不可能
- 代替としてはL2FW
  - 家庭用(廉価なもの)は存在していない
- 端末での対処(personal FWなど)が必要
  - e.g.. Windows:public networkを選択

“IPv6対応ルータ”の定義について

Global ICT Partner
Innovative. Reliable. Seamless.
NTT Communications

“IPv6対応ルータ”として現在家庭向けに販売されているものにはおおよそ2つに分類

IPv6 ルーティング対応ルータ	IPv6パススルー対応ルータ
• SPI搭載 • IPv6 PPPoEやIPv6 パススルーも付加されている場合もあり	• SPI未搭載 • パススルー機能のみ

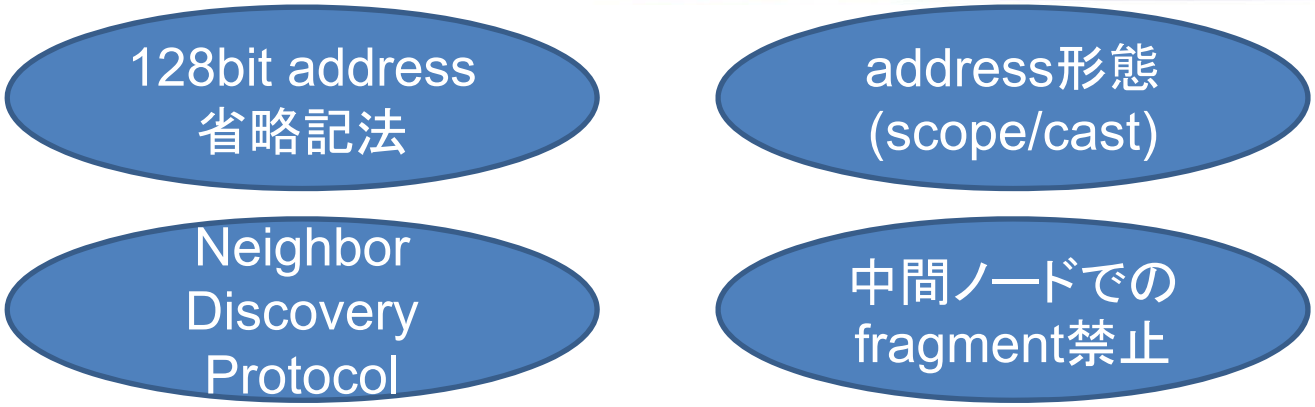
- 最近新しく出ているものは“ IPv6 ルーティング対応ルータ”のことが多い
- 一部のルータは“IPv6パススルー対応ルータ”のため購入する際は注意が必要

まとめ

- IPv6ではSPI機能を利用することでIPv4のNATと同レベルのセキュリティを担保可能
- 端末にはglobal scope addressを付与することでIPv4と比べて透過性を高めることが可能
- SPI機能のあるCPEが設置できない場合は端末側での対応が必要

家庭・SOHO向けIPv6セキュリティ

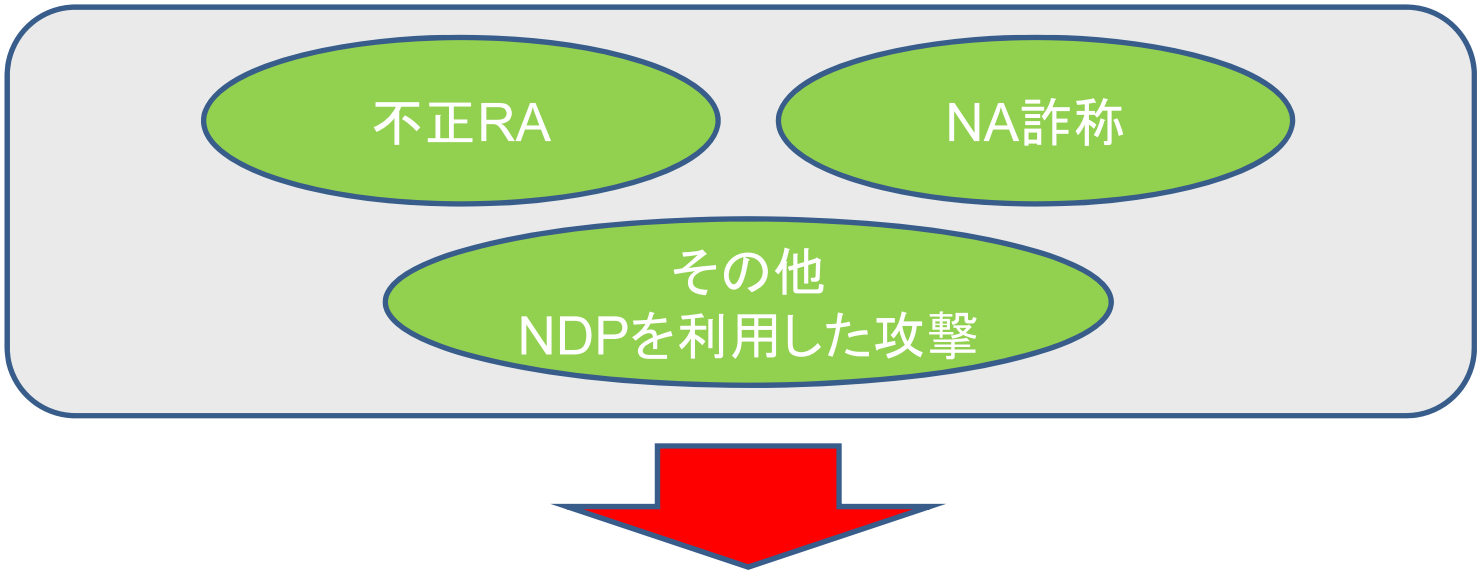
IPv6の仕様



- NDPはIPv6の中核のプロトコル
  - Router Solicitation(RS)
  - Router Advertisement(RA)
  - Neighbor Solicitation(NS)
  - Neighbor Advertisement(NA)
  - ICMP redirect

不正RAやNA詐称などの上記の仕組みを悪用した
攻撃手法が存在

IPv6の仕様によるセキュリティ



同一リンク内に攻撃者がいることが条件

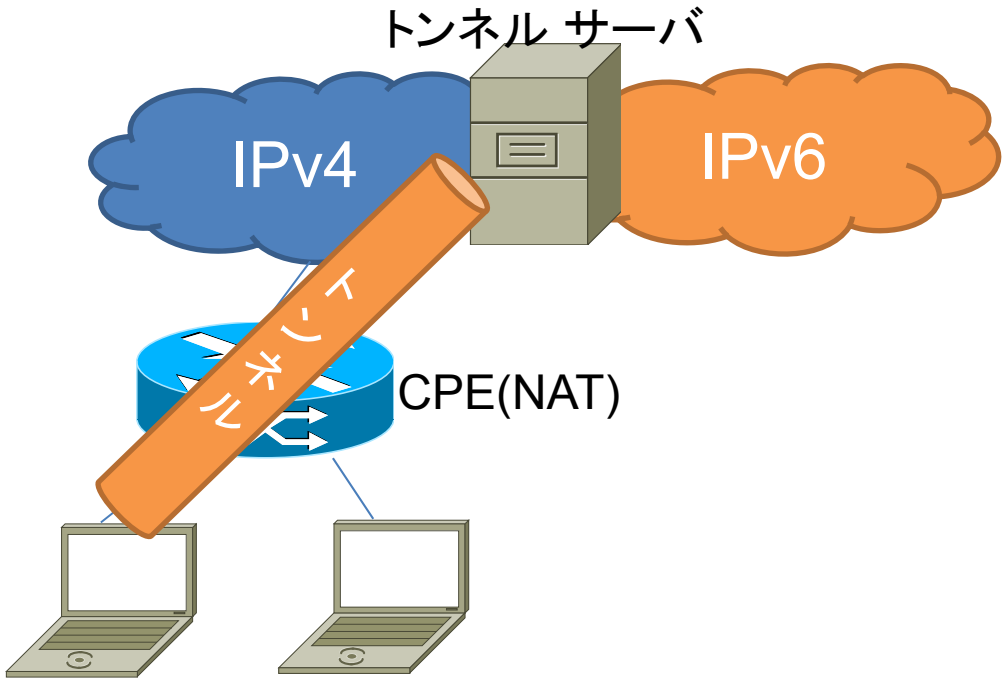
- 家族で使っていたり，一人で使っている場合には気にしなくてよい？

トンネルによるバックドア形成の危険性あり

トンネルによる外部からの到達性

Global ICT Partner
Innovative. Reliable. Seamless.
NTT Communications

- IPv6 over IPv4 トンネル技術により，内部ネットワークに直接アクセス可能
  →端末で終端する場合CPEをバイパス可能



- CPEのFWでは検知不可
  - CPEにとっては正常なIPv4通信
- 外部からの到達性あり

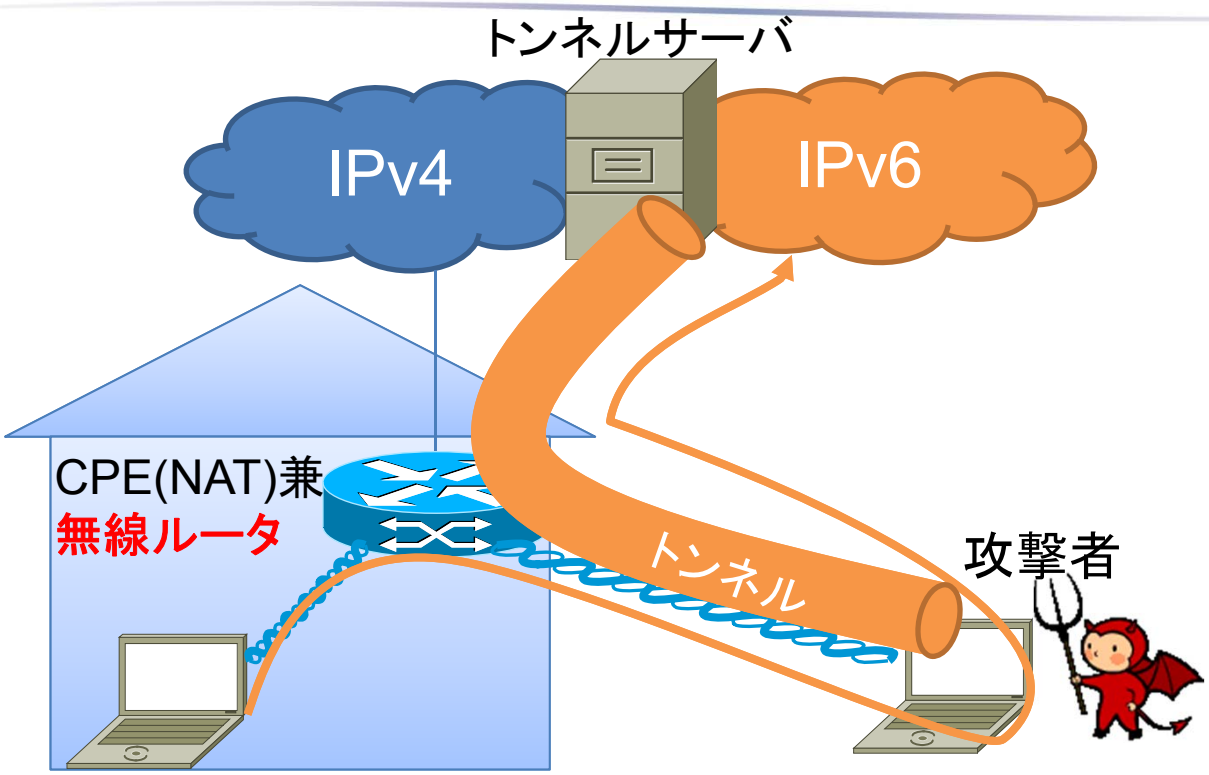
“さらされている”状態

バックドア形成の危険性

不必要なtunnelは使用しない/CPEでのFilter

使用する場合は端末でFWなどの防御策を実施

無線使用時には特に要注意



- 無線のセキュリティが甘いとバックドアの作成がより容易に
  - 攻撃者を経由して通信することで Man-in-the-middle attackになる場合も

無線使用時にはWPAなどの強固な暗号方式を使用

IPv6での端末へのアドレス付与方法

Global ICT Partner
Innovative. Reliable. Seamless.
NTT Communications

- IPv4では．．．
  - CPEがDHCPで付与
  - global addressはPPPoEを張りなおす度に変化

➡ DHCP + アドレス非固定

IPv6ではどうなのか

- DHCPv6
  - ✓ OSでのclient実装がされていないものあり
    - e.g. Windows XP, Mac OS X 10.6
  - ✓ CPEでのserver機能も未実装なものが多い
- SLAAC→現状では一般的

SLAACでのアドレスの付与

Global ICT Partner
Innovative. Reliable. Seamless.
NTT Communications

Prefix(64bit) ＋ Interface ID(64bit)

- ISPやサービス仕様によって決定
  - ユーザは指定することができない
- サービスによって固定・非固定が決定

- 一般的にはEUI-64にて決定
  - MACアドレスにより一意に決まる
- Interface IDをランダムに生成し，適宜変更するPrivacy Extensionが存在
  - OSによってはデフォルトでは未使用のものも

Prefix固定かつPrivacy Extension不使用だと
アドレスが半永久的に固定

アドレス固定のPros and Cons

Global ICT Partner
Innovative. Reliable. Seamless.
NTT Communications

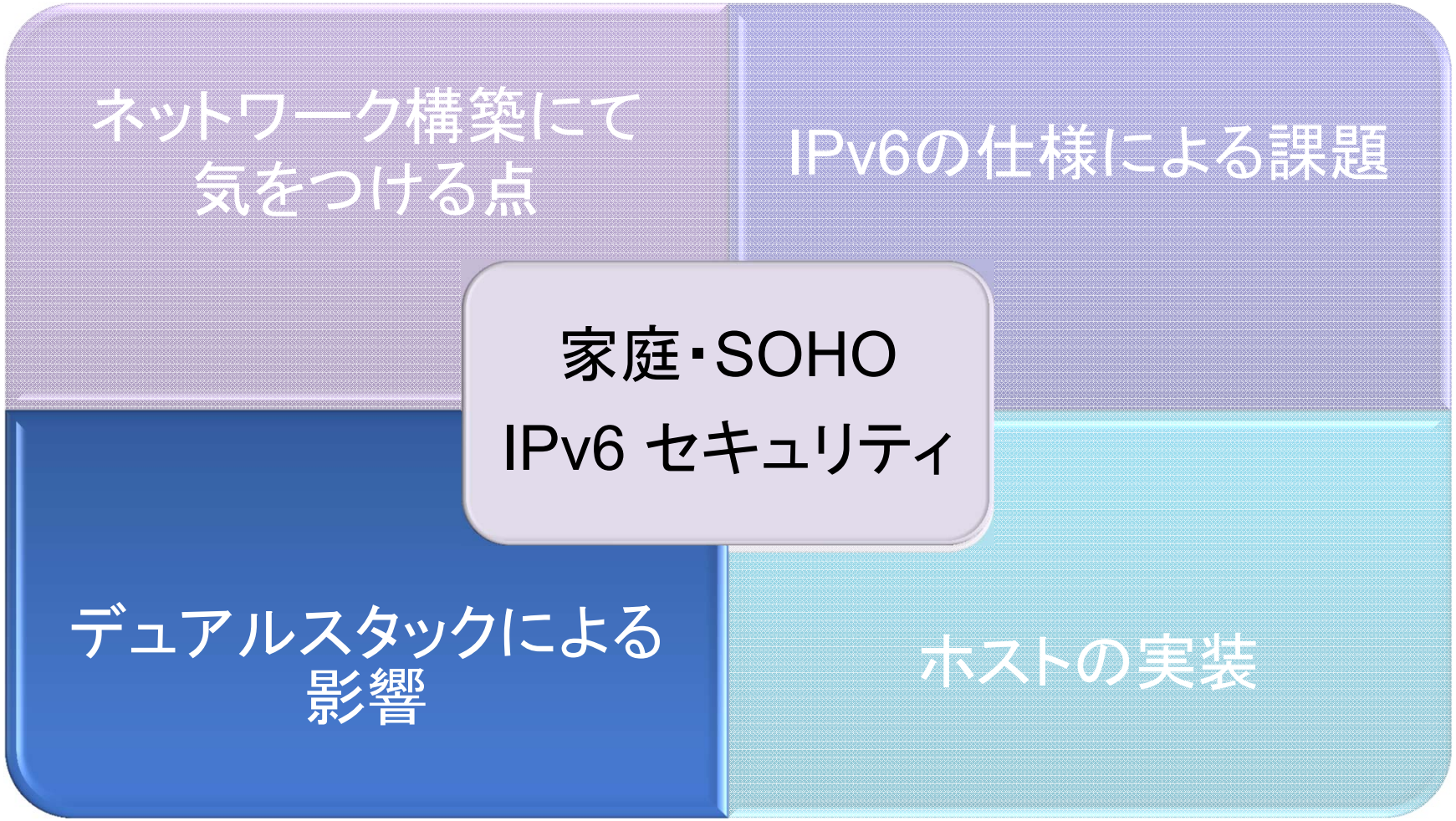
Pros	外部からの通信が容易 (サーバ構築時は望ましい)
Cons	同一ユーザかどうかの特定が容易 Prefix →**同一ID(家庭)**からの通信かを判別可能 InterfaceID→**同一端末**からの通信かを判別可能

同一ユーザかの特定を防ぎたい場合は
Privacy Extensionを有効に

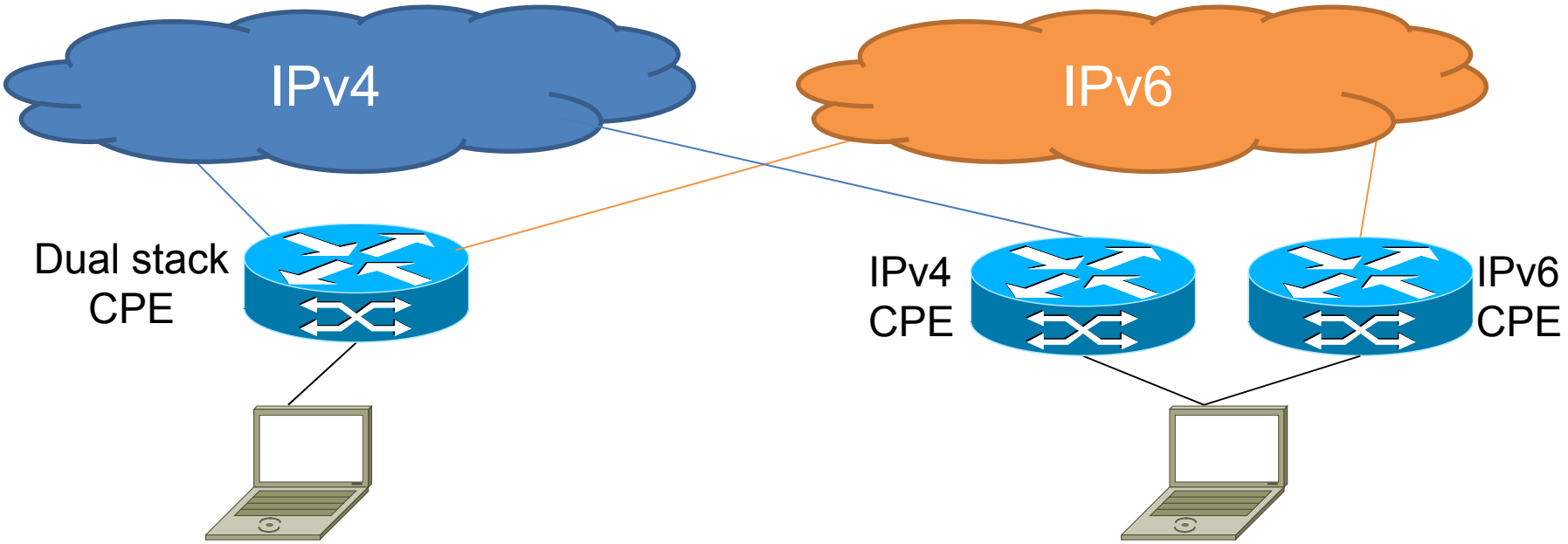
まとめ

- IPv6の仕様によるセキュリティに関して致命的なものはなし
  - トンネルについては不要なものを無効化する
  - トンネルを使用するときにはクライアント側のFW(SPI)を使用する
  - 無線使用時には強固な暗号(WPAなど)を使用
  - 同一ユーザかどうかの特定を防ぎたい場合には，まずはPrivacy Extensionの積極的な利用を

家庭・SOHO向けIPv6セキュリティ



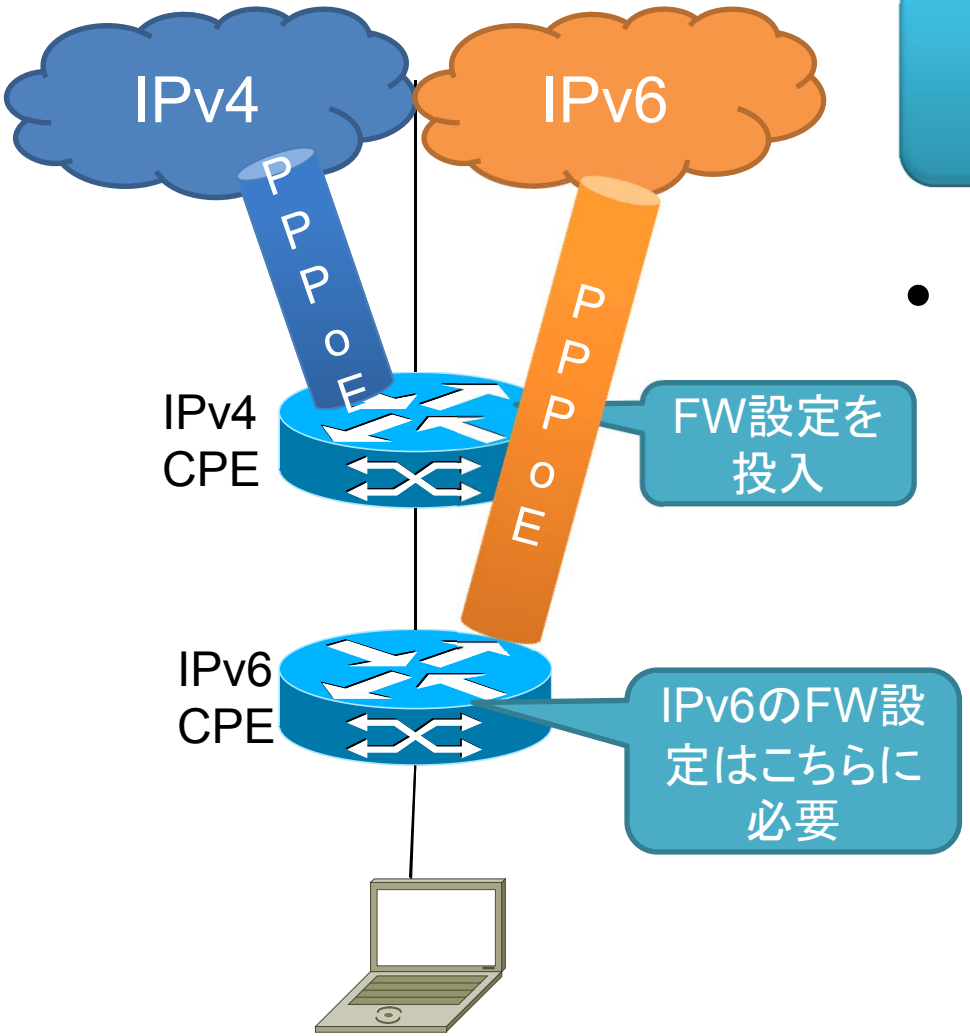
デュアルスタックによる影響



- IPv4/IPv6ともにCPEがGWの役割
  - FilterなどのFW機能もIPv4/IPv6どちらにも設定が必要
  - CPEが分かれている場合にはそれぞれにログインが必要

configurationが(単純に考えると)2倍

デュアルスタックによる影響



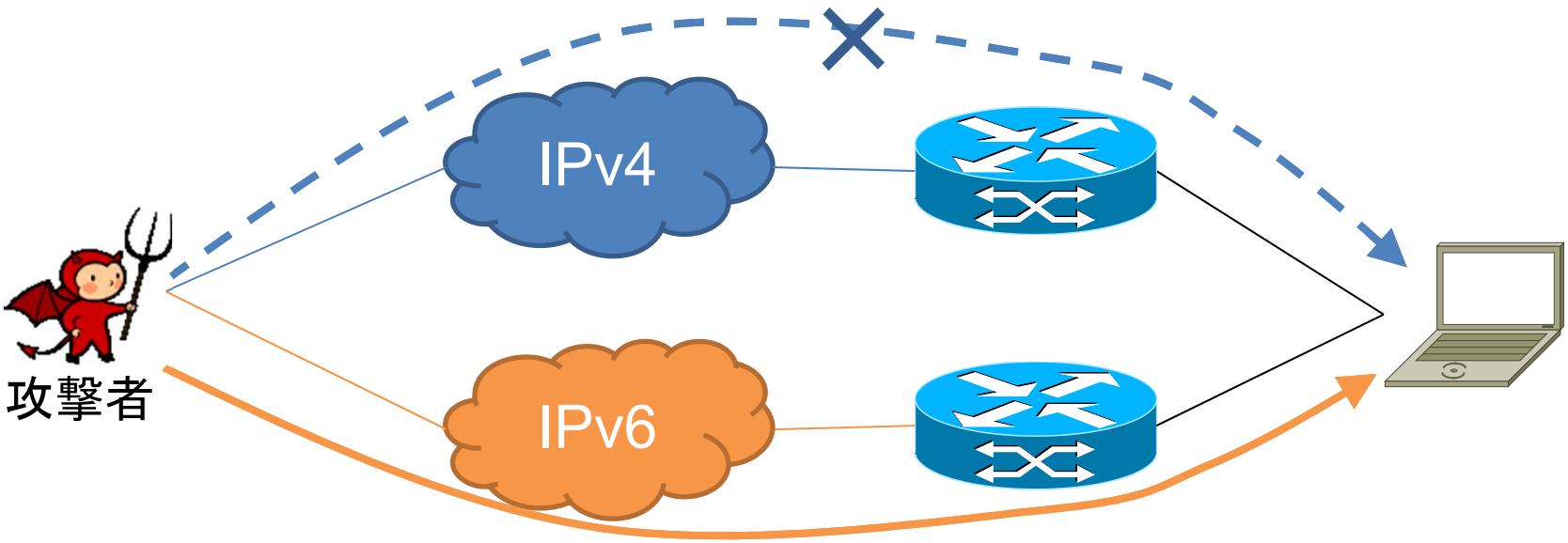
IPv4とIPv6の終端装置が異なる場合は特に要注意

- IPv6 PPPoEの場合
  - IPv4とIPv6の終端箇所が異なる装置の可能性あり
  - 物理的に上位ルータにのみFWを設置すればよいように見える

デュアルスタックによる影響実例

Global ICT Partner
Innovative. Reliable. Seamless.
NTT Communications

設定が不十分だと
Filterが十分に効かず想定外の通信が可能になることも



IPv4/IPv6両方でFilteringの設定が必要

IPv4/IPv6両方での確認が必要

FW機能について

- FW機能のIPv6対応が必要
  - 設定画面でIPv6アドレスが設定できること

- URL filtering
  - 通信させたくないサーバへのアクセスを制限
  - 一般的にはFQDNを指定
    - AAAA問い合わせ機能が必要
  - アドレス直打ちでのサイトに対応するためにアドレスでの設定も必要
    - IPv6アドレスで設定できること

Filteringなどの機能についてもIPv6対応を

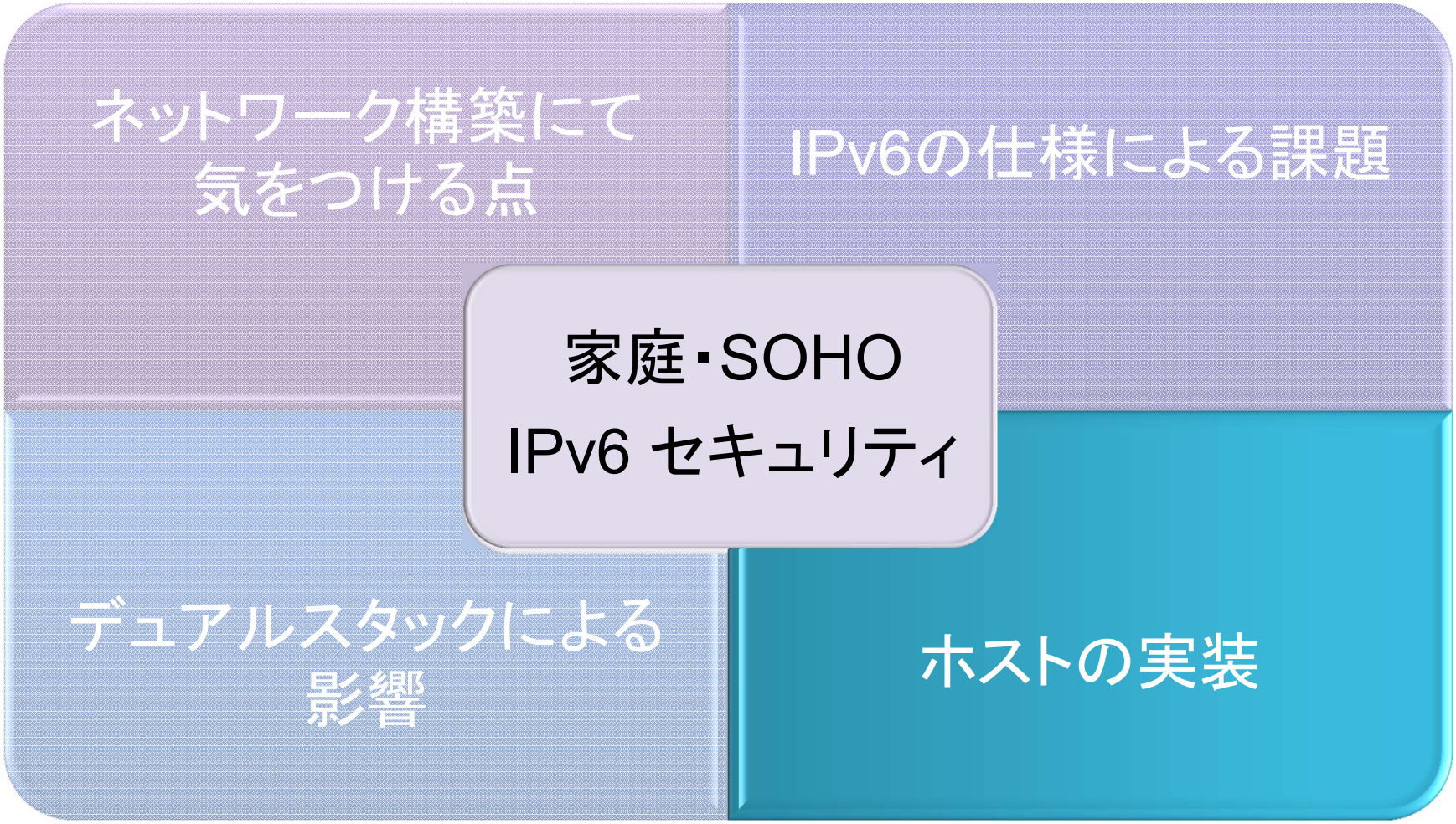
まとめ

- IPv4用とIPv6用の設定について各々に適切な対応を行うこと

- URL Filteringなど，Filtering機能のIPv6化を進め，購入の際はIPv6対応のものを選択すること

家庭・SOHO向けIPv6セキュリティ

Global ICT Partner
Innovative. Reliable. Seamless.
NTT Communications



ホストの実装

- 古いOSなどはIPv6に関する現在の仕様に準拠していなかったり，そもそも実装が不十分

Site Local DNS addressが
初期設定されているOS

- IPv6の仕様によりセキュリティの設計の見直しが必要

TCP Wrapperの逆引き設定

Site local DNS addressについて

- 古いOSではリゾルバにfec0:0:0:ffff::1などの Site local DNS anycast addressを初期設定しているものあり
- この場合Site local DNS addressをつけたPCを同一link内に置くことにより，DNS server詐称が可能

  – e.g. windows 2003 server

    ➢初期値で3つのSite local DNS anycast addressが登録

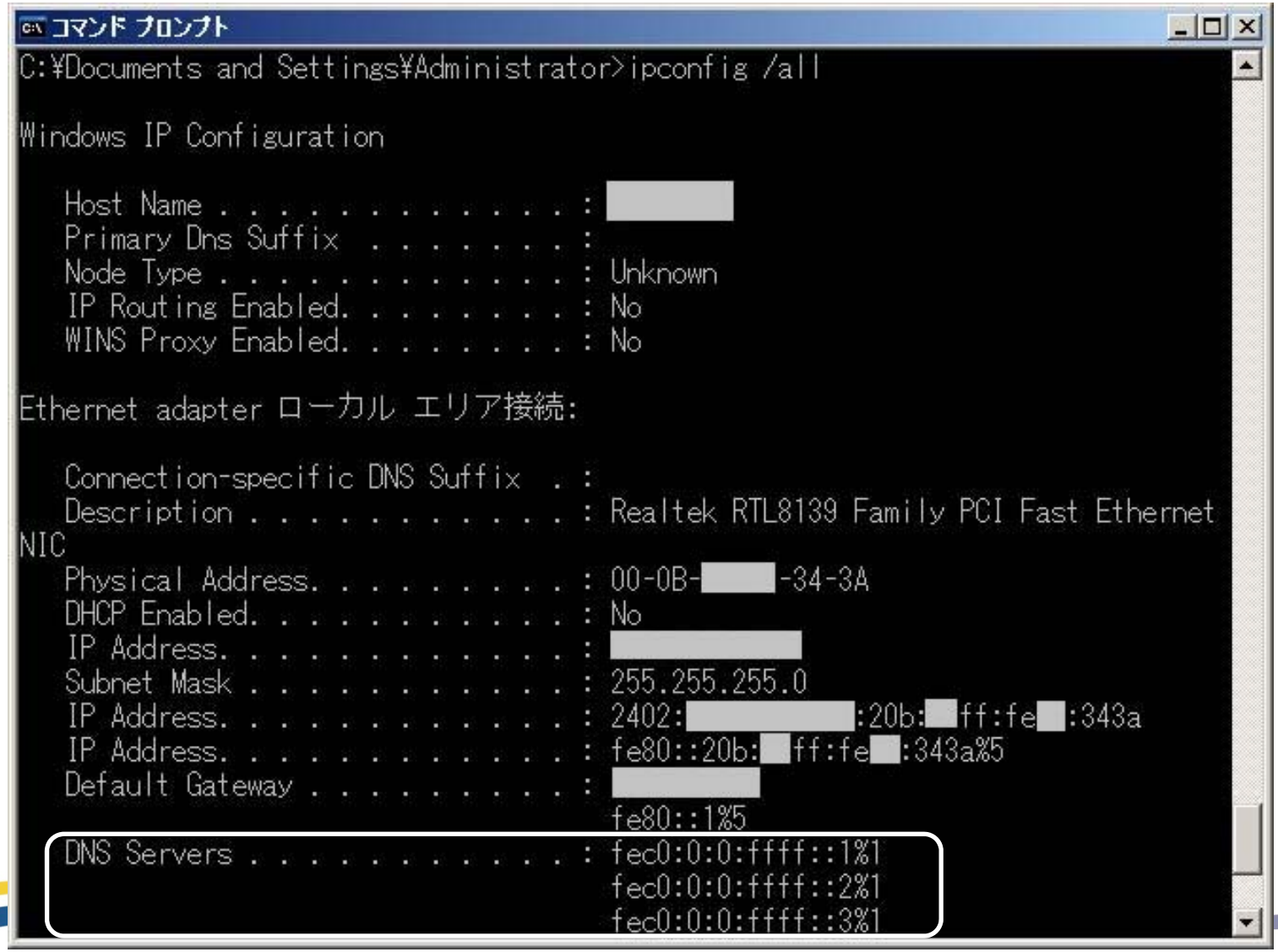
      ◆Netshを使用することで変更可能

    ➢IPv4のリゾルバに優先的に問い合わせを行うが，IPv4のリゾルバがない場合IPv6のリゾルバに問合わせ

Site local DNS addressについて

Global ICT Partner
Innovative. Reliable. Seamless.
NTT Communications

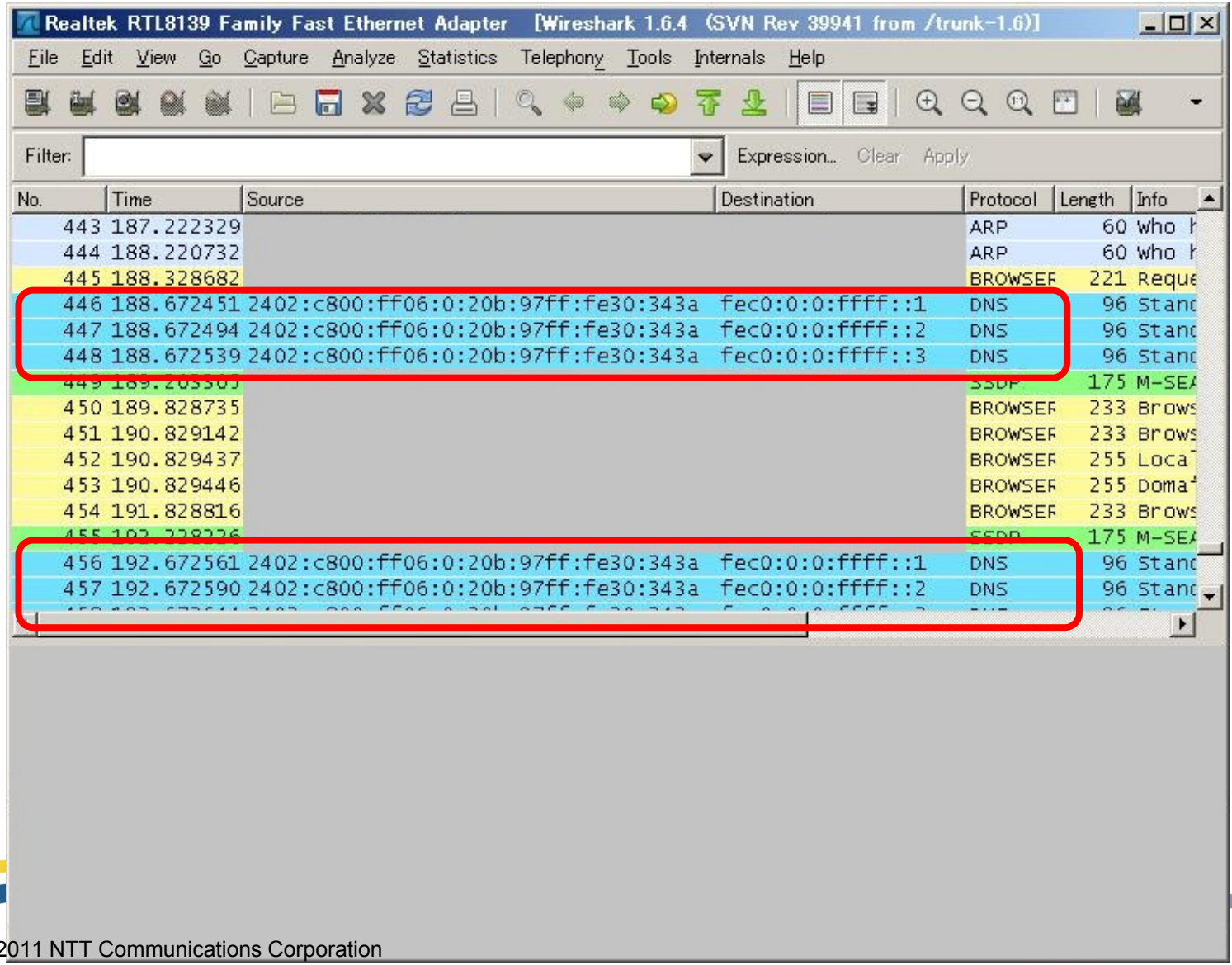
Windows 2003 serverのコマンドプロンプト(初期設定のまま)



Site local DNS addressについて

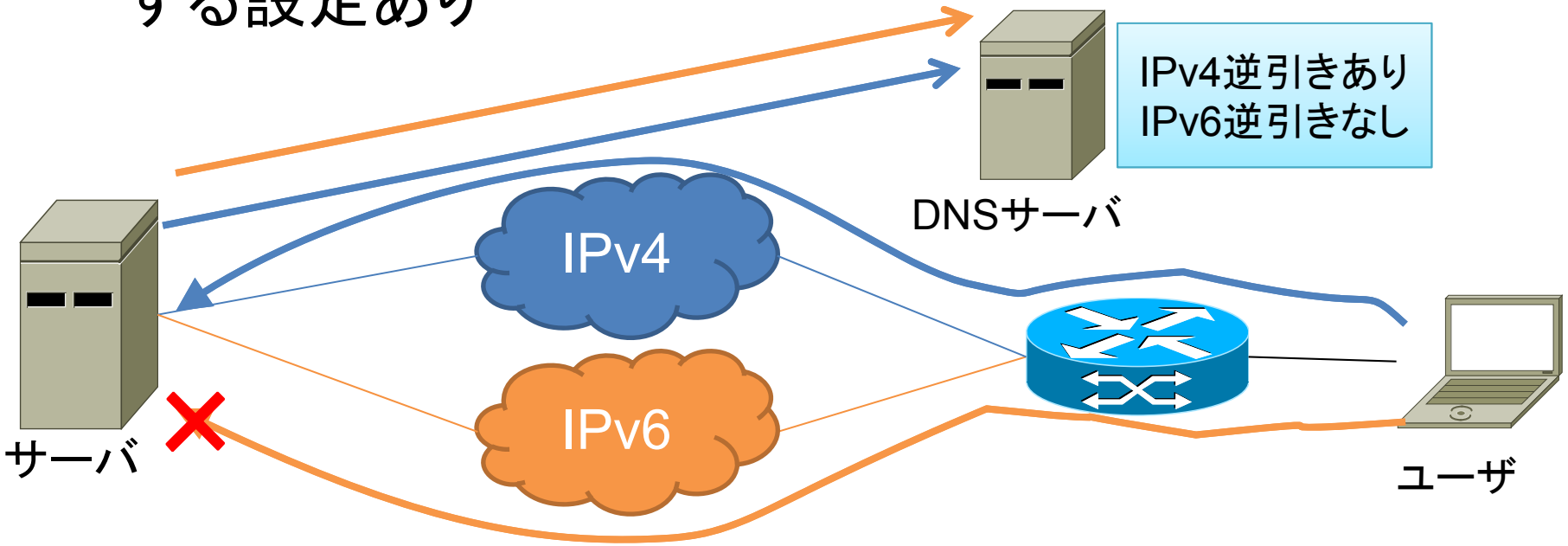
Global ICT Partner
Innovative. Reliable. Seamless.
NTT Communications

DNS問い合わせ時のパケットダンプ



TCP wrapperでの逆引き登録チェック

- IPv4では逆引きし登録があるものだけ通信を許可する設定あり



- IPv6では逆引き登録は今のところ一般的ではない
  - IPv4の設計のままだと通信できないユーザが多発

IPv6の現状に合わせたセキュリティの設計が必要なものも存在

まとめ

Global ICT Partner
Innovative. Reliable. Seamless.
NTT Communications

- 古いOSなどはIPv6に関する現在の仕様に準拠していなかったり，そもそも実装が不十分なものがあり，OSを最新のものにするのが望ましい

- IPv6特有の仕様により，IPv4と同じ設計では動作しない場合もあり

最後に

Global ICT Partner
Innovative. Reliable. Seamless.
NTT Communications

**セキュリティで気をつけるべき点は
IPv4とほとんど同じ**

例えば．．．

CPEにてSPIを実施

無線使用時は暗号化

一方で

- IPv6の仕様やデュアルスタックによる影響などにより，IPv4とは違う視点でのセキュリティの検討が必要になる場合も

**IPv6特有の仕様を理解し
それに沿ったネットワークの検討を**