

IPv6とセキュリティ

～家庭ネットワーク/SOHO編～

NTTコミュニケーションズ株式会社
ソリューションサービス部
山形育平

2012/11/20

AGENDA

1. 現在のIPv6対応状況
2. 家庭・SOHOネットワークのIPv6セキュリティについて
 - NW構築時に気をつける点
 - IPv6の仕様による課題
 - Dualstackによる影響
- まとめ

家庭・SOHO向けIPv6対応製品

端末

Windows

Mac OS

PC

BSD

Linux

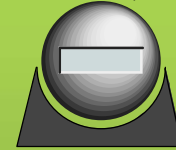
Windows Phone

Mobile/タブレット

iOS

Android

ネットワークカメラ



その他



TV

家庭・SOHO向けルータ(CPE)

NTTCommunicationsをはじめ、NEC、Yamahaなど
各社から提供済み

IPv6対応サイト

Google

検索

gmail

youtube

OCN Topページ



IPv6でのアクセスを表示



World IPv6 Launchでは

Facebook

Wikipedia

などを代表に約3000以上の企業・サイトが参加

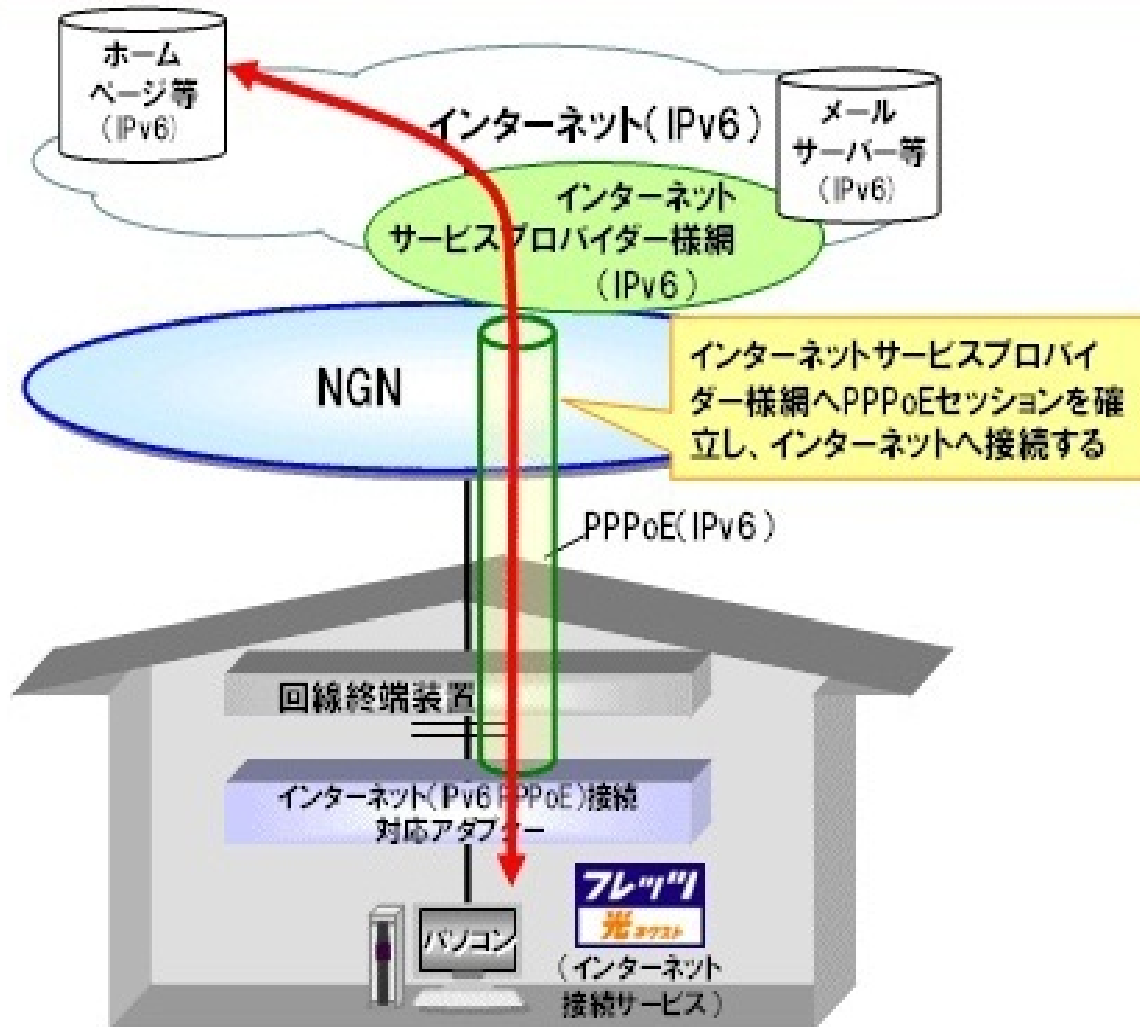
<http://www.worldipv6launch.org/participants/>参照

家庭向けIPv6接続サービス

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



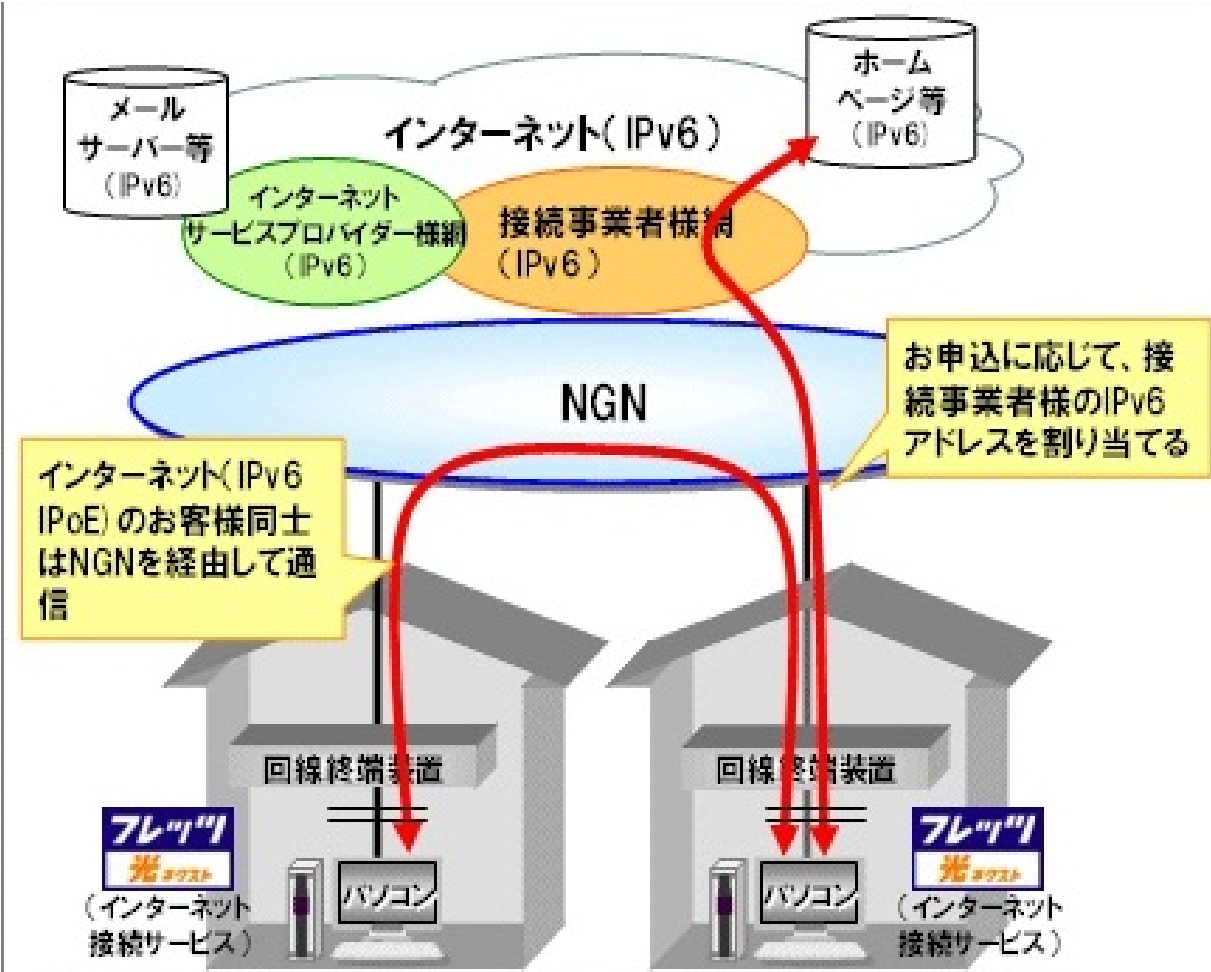
http://www.ntt-west.co.jp/news/1105/110526d_2.htmlより抜粋

家庭向けIPv6接続サービス

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



※2 接続事業者様: BBIX株式会社様、日本ネットワークイネイブラー株式会社様、インターネットマルチフィード株式会社様

家庭向けIPv6接続サービス

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

法人・SOHO向けIPv6 VPNサービス

Global ICT Partner
Innovative. Reliable. Seamless.



Master'sONE® セキュア・インターネットVPN-HighSpeed

フレッツ光ネクストを使用したVPN接続サービス

<http://www.nttpc.co.jp/press/2012/03/201203221500.html>より抜粋



- フレッツ光ネクストをVPNバックボーンNWとして使用し、IPv6でVPNを確立
- 拠点間ではIPv4が使用可能

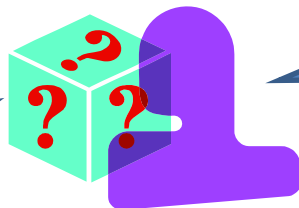
装置・端末・サービスともにIPv6 ready

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？

IPv4と違うところ
はどこ？



何を気をつけ
ばいいの？

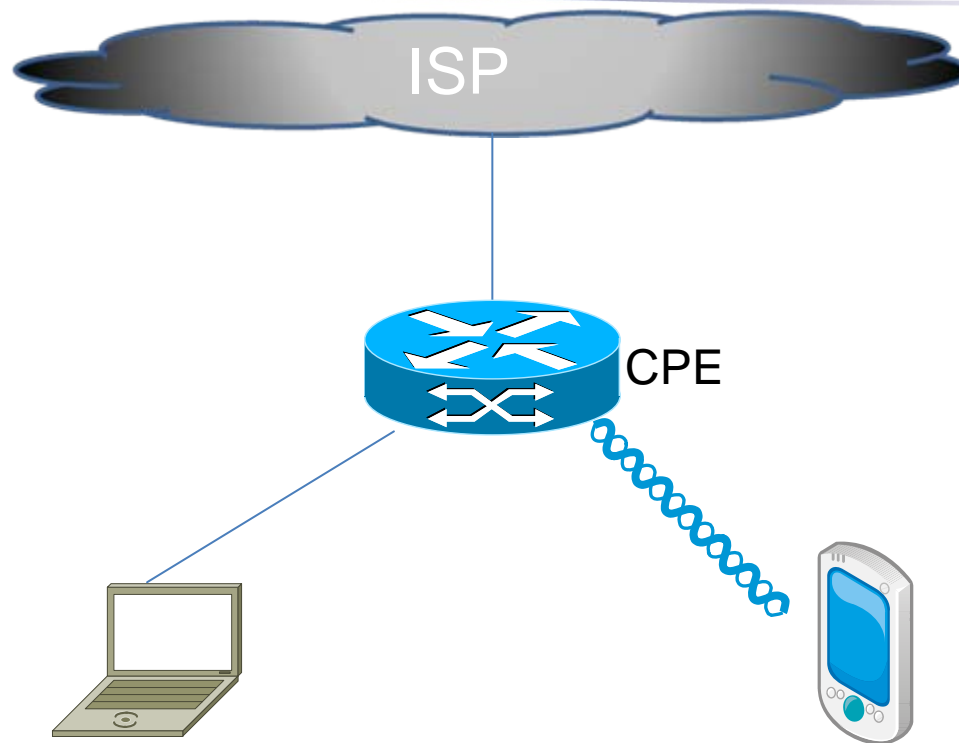
- ここでは家庭・SOHOネットワークのIPv6に関するセキュリティについて述べさせていただきます
 - ネットワークを構築・利用する際に気をつける点
 - ISPや企業が個人向けサービスを行ううえで気をつける点

NW構築時に
気をつける点

IPv6の仕様
による課題

Dualstackに
よる影響

一般的なIPv4 ネットワーク



ISPとの接続点はCPEが存在

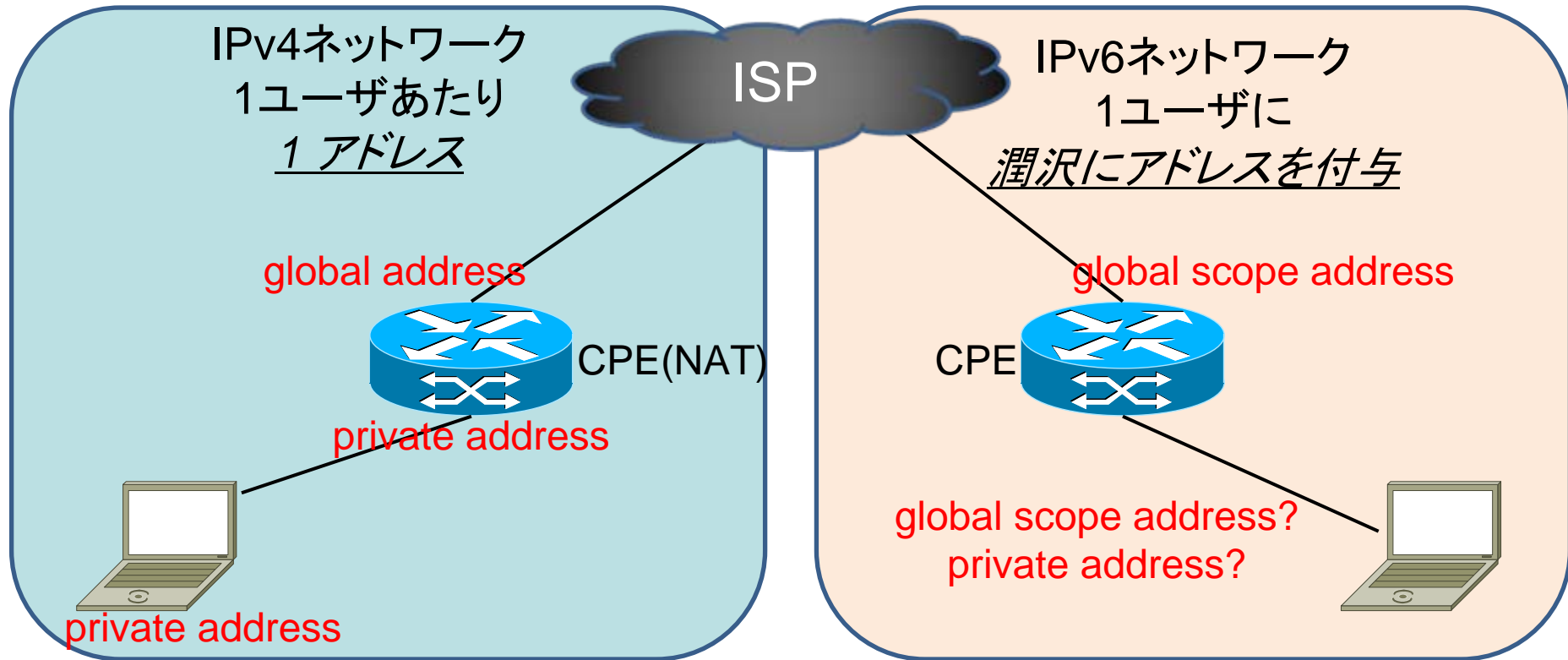
CPEでNAT

IPv6ネットワークでは
一般的にはどうすべきか？

一般的な？ IPv6 ネットワーク

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？

- 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



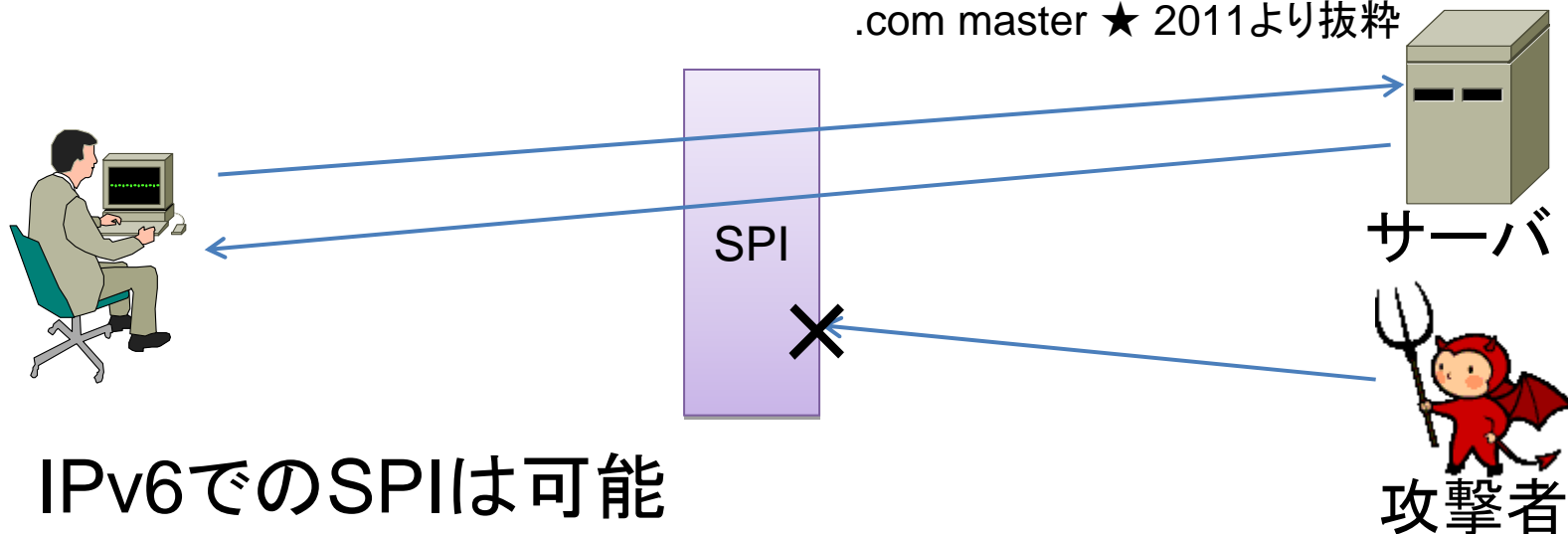
Stateful Packet Inspection(SPI)によるもの

端末にglobal scope addressで大丈夫？

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

.com master ★ 2011より抜粋



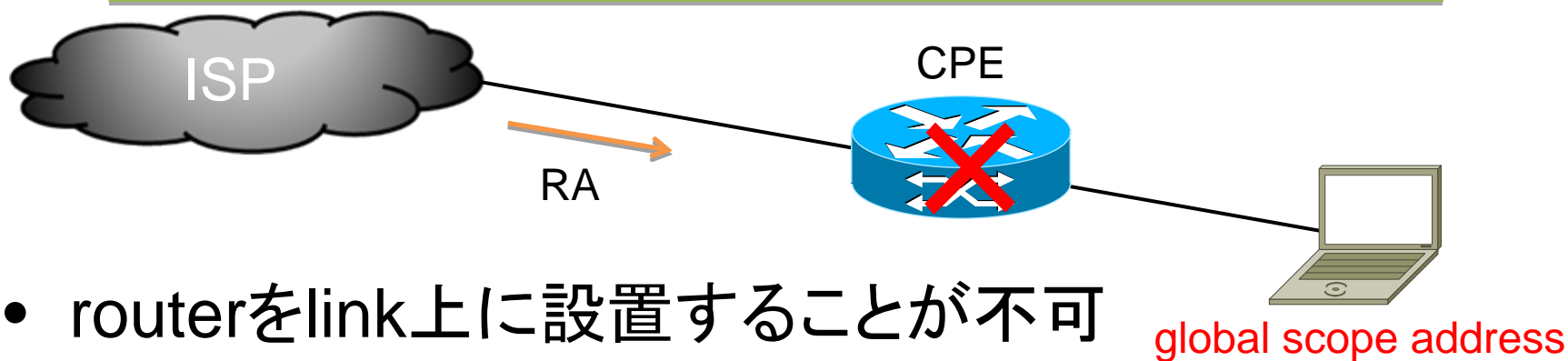
- IPv6でのSPIは可能
 - 一般的なIPv6対応CPEには搭載済み

→ 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

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

“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

- 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

IPv6パススルー対応ルータ

- 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

NW構築時に
気をつける点

IPv6の仕様
による課題

Dualstackに
よる影響

IPv6の仕様

128bit address
省略記法

address形態
(scope/cast)

Neighbor
Discovery
Protocol

中間ノードでの
fragment禁止

- NDPはIPv6の中核の^o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



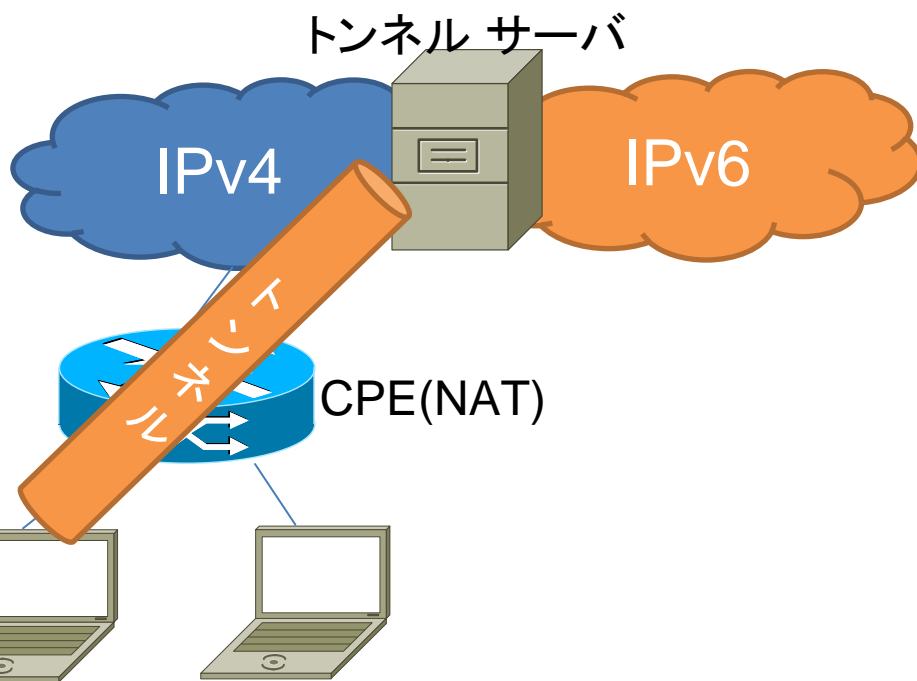
同一リンク内に攻撃者がいることが条件

- 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

- 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

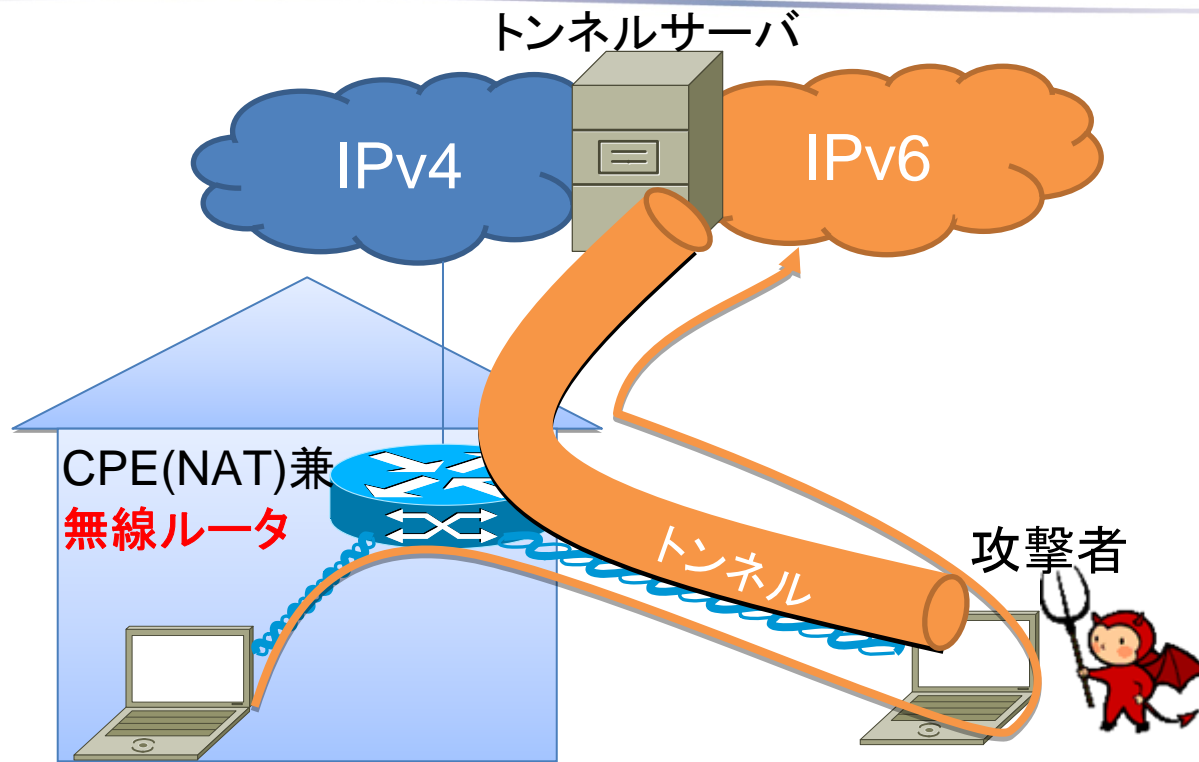


“さらされている”状態

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
 - 攻撃者を經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

- 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

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

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

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

まとめ

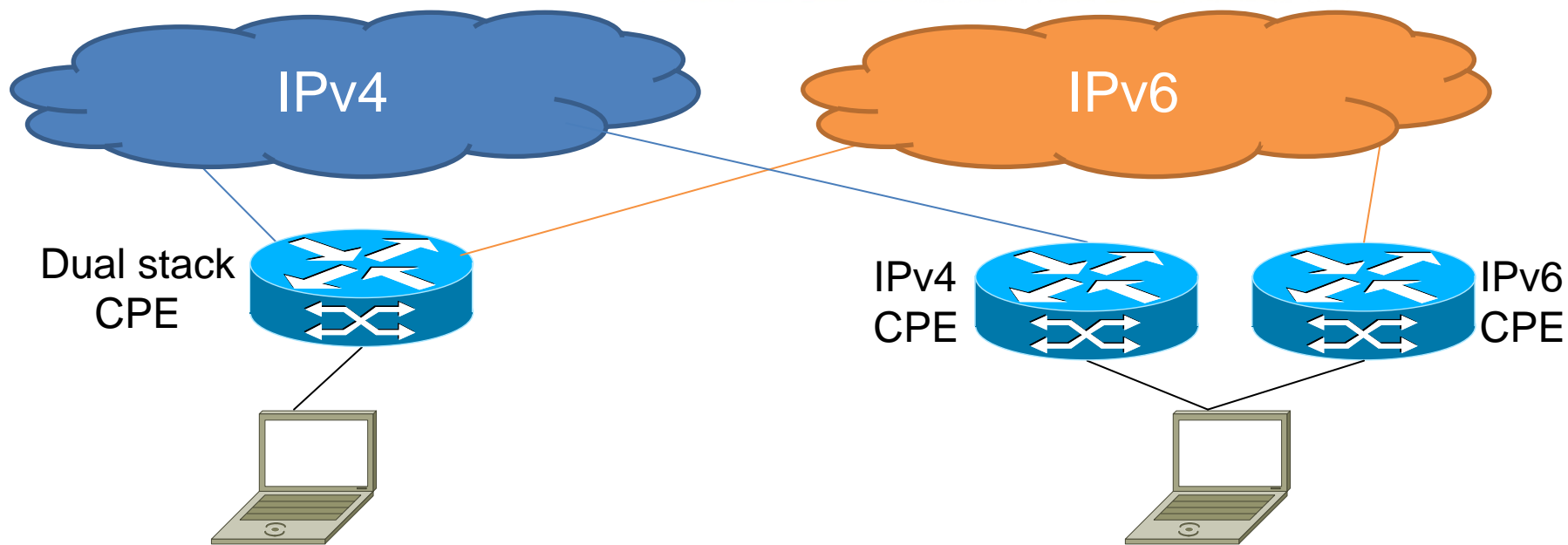
- IPv6の仕様によるセキュリティに関して致命的なものはなし
 - トンネルについては不要なものを無効化する
 - トンネルを使用するときにはクライアント側のFW(SPI)を使用する
 - 無線使用時には強固な暗号(WPAなど)を使用
 - 同一ユーザかどうかの特定を防ぎたい場合には、まずはPrivacy Extensionの積極的な利用を

NW構築時に
気をつける点

IPv6の仕様
による課題

Dualstackに
よる影響

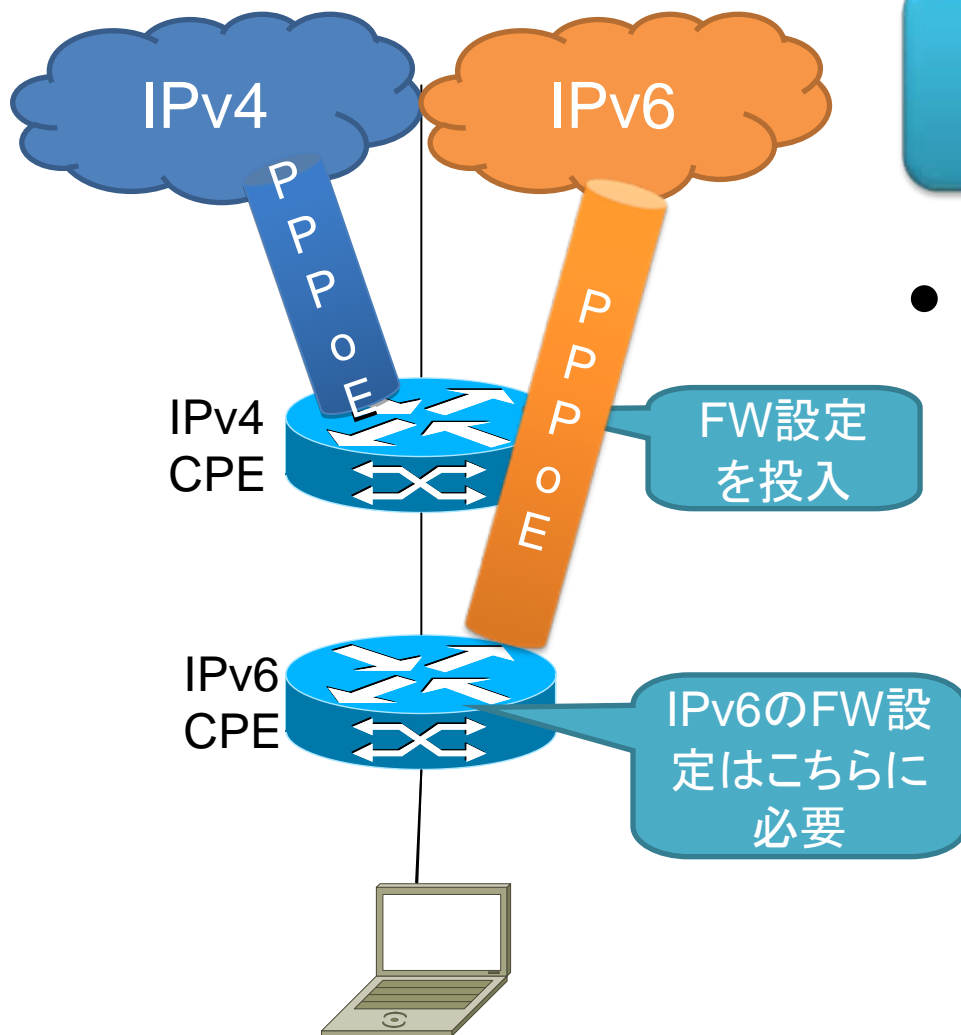
Dualstackによる影響



- 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

Dualstackによる影響

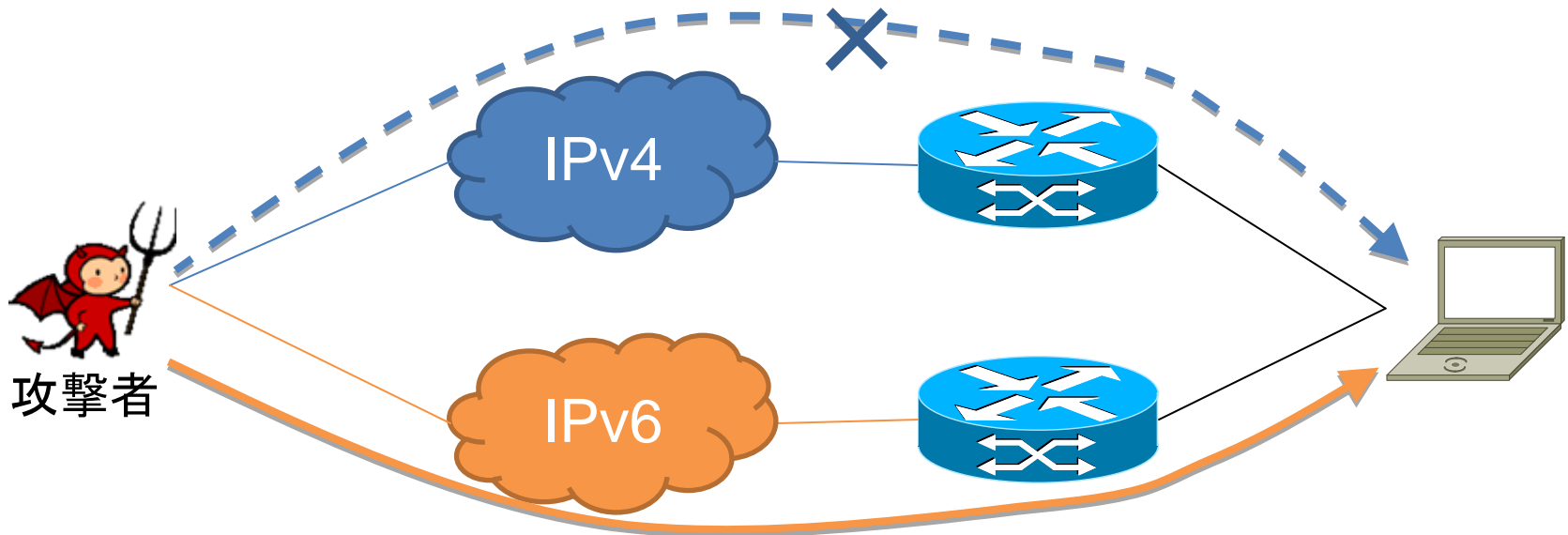


IPv4とIPv6の終端装置が異なる場合は特に要注意

- 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

Dualstackによる影響実例

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

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

最後に

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Dualstack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