NTT

NTT Information Sharing Platform Laboratories

NTT 情報流通プラットフォーム研究所

点検！IPv6のセキュリティ
～点検！ホームネットワーク～

藤崎 智宏

日本電信電話(株)／慶應義塾大学大学院

Agenda

- はじめに
- ISP接続リンクに関する問題
- 家庭内ネットワークに関する問題
- おわりに

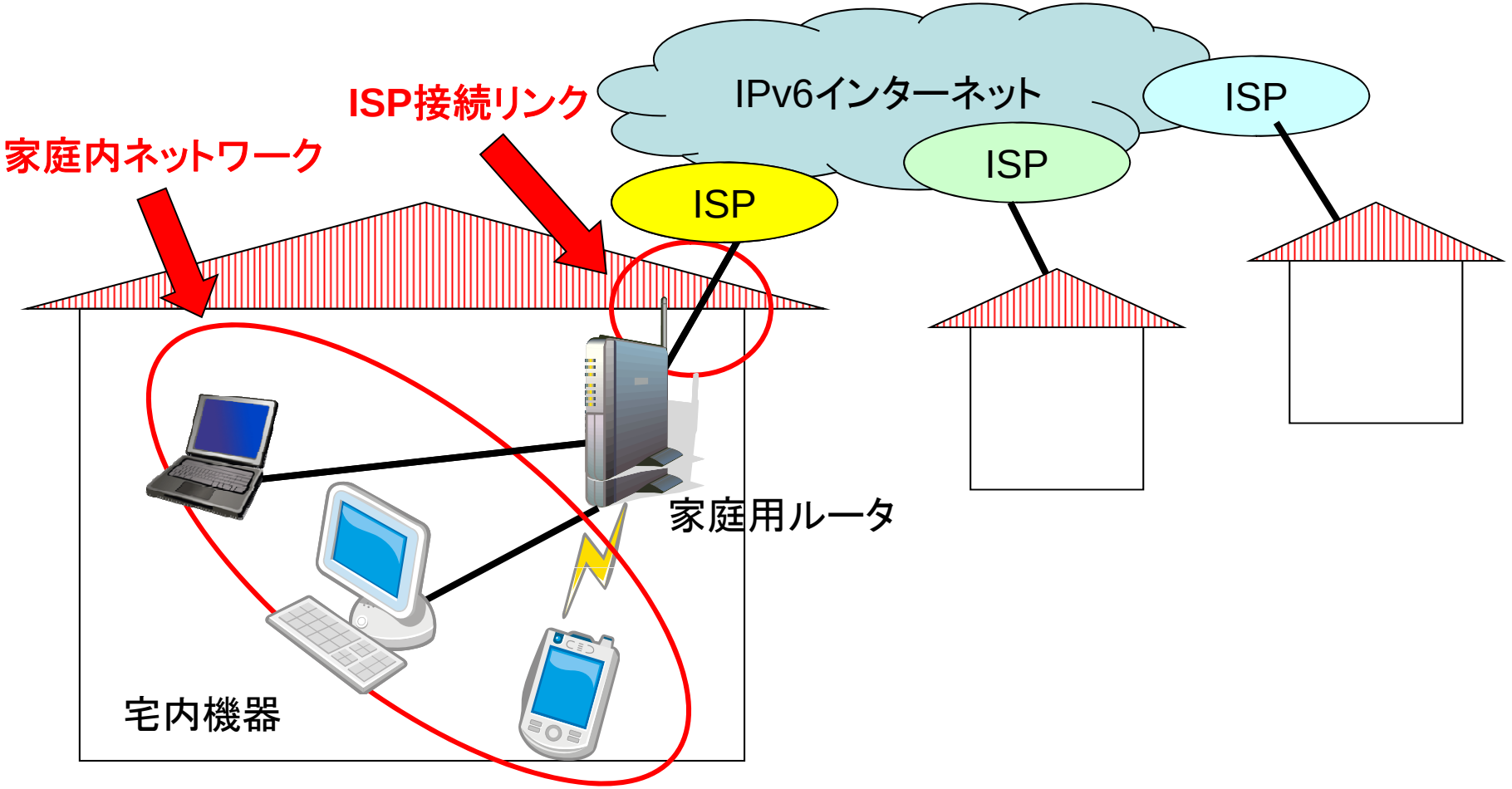
2

NTT

はじめに

本発表での分析対象

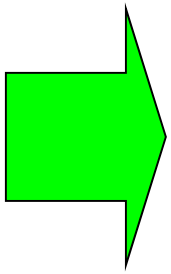
- IPv6インターネット接続サービス利用時の家庭ネットワーク環境



ISP接続リンクに関する問題

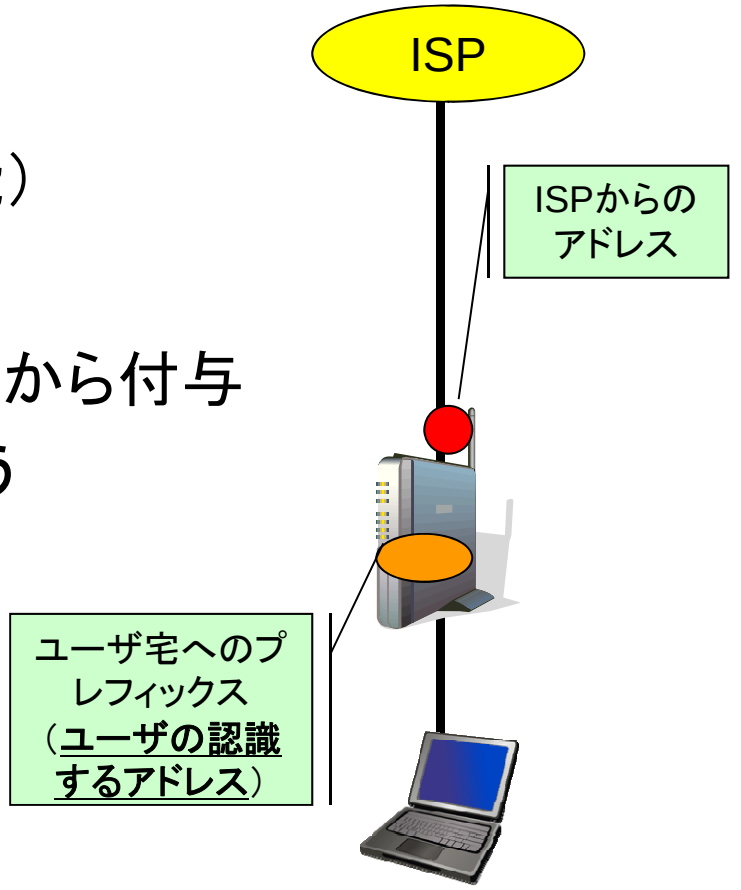
ISP接続インタフェースとアドレス問題

- ISPとユーザ宅の間のリンクのインタフェースにグローバルアドレスを付与する場合のセキュリティ問題.
  - –付与を希望するISPは多い.
  - –(リンクローカルアドレスのみ
    でもサービス提供は可能)
- 付与するアドレス
  - –ユーザに割り当てるプレフィックス外から付与
  - –ユーザの認識しているアドレスと違う



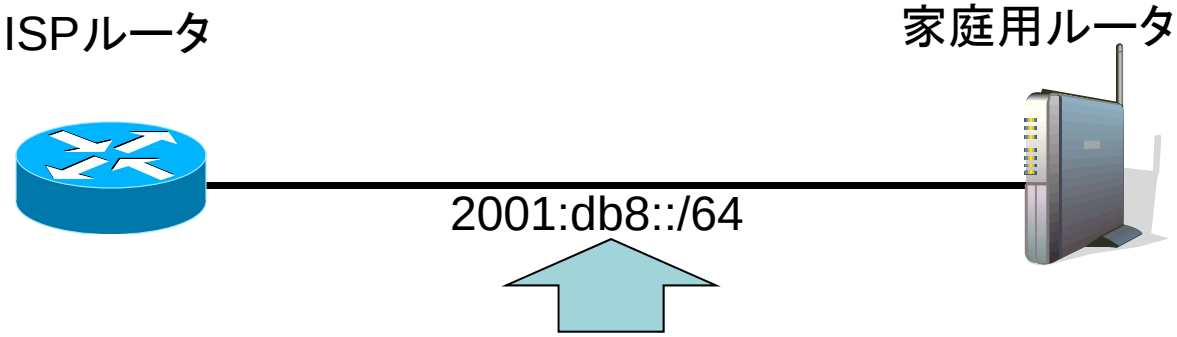
このアドレスが攻撃対象になる可能性がある.

IPv4でも同様だが, 誰(ISP or ユーザ?)がどこを気にしなければいけないかがまだ曖昧.



ISP接続インタフェースと近隣探索

- IPv6の近隣探索 ≒ IPv4のARP
- (ユーザでなく)ISP側に大きな問題



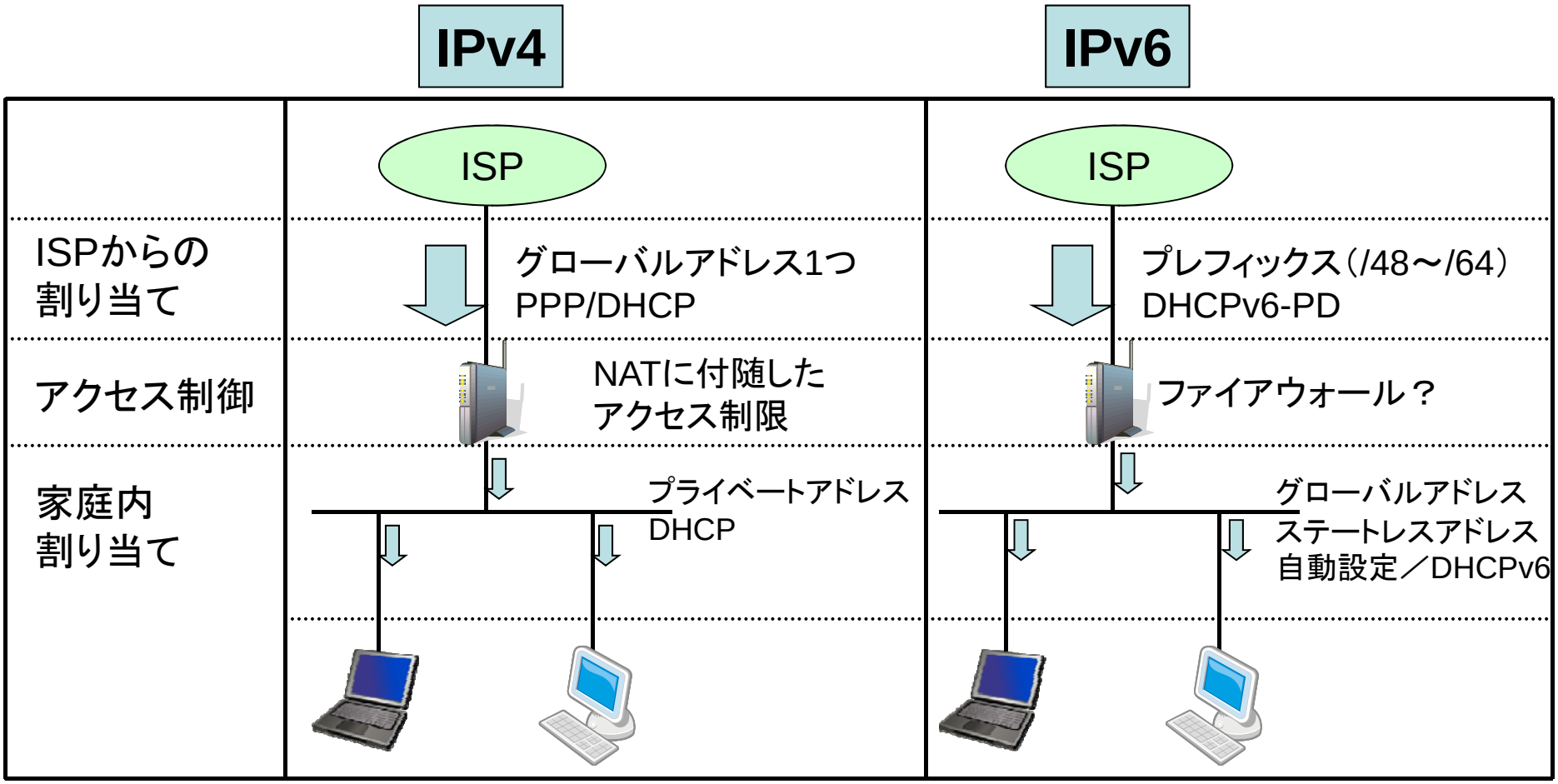
ここが Point-to-point **でない「ネットワーク」の場合**

- ISPとの接続リンクに，“複数のノード”を接続可能
  - IPネットワーク的には，IPv4の場合には /30，IPv6は /64 の場合が多い．
    - NDキャッシュ(≒ARPテーブル)どのくらい必要？

家庭内ネットワークに関する問題

全てのノードにグローバルアドレス

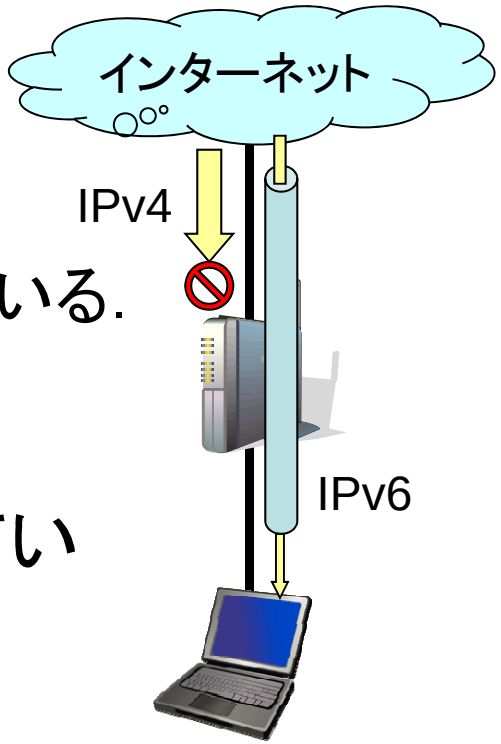
- 家庭内の**全ての機器にグローバルアドレス**が付与される.



外部から直接ノードのアドレスが指定される可能性があることに注意！

宅内機器の自動トンネル問題

- 宅内機器（特に，PC）が，自動的にIPv4トンネルを利用したIPv6接続をする場合がある.
  - 6to4 (グローバルアドレスを持つ機器での利用を想定)
    - Windows OS, Airmac Extreme 等で実装されている
  - Teredo (NAT配下での利用を想定)
    - Windows OS 等に実装されている
- これらのトンネルが動作すると，ユーザは気がつかないうちにIPv6 reachable になっている.



ユーザが想定しているファイアウォールをバイパスしてしまっている可能性がある.

自動トンネル

- 6to4 トンネルの例

NAT配下でも，Teredo アドレスがついて，外部から導通性があることがある.

アドレス固定・非固定問題

- IPアドレスを固定で割り当てるか，時間等で変化するように非固定で割り当てるか．

- 主に，プライバシーの問題として議論される．
  - ユーザのトレーサビリティ

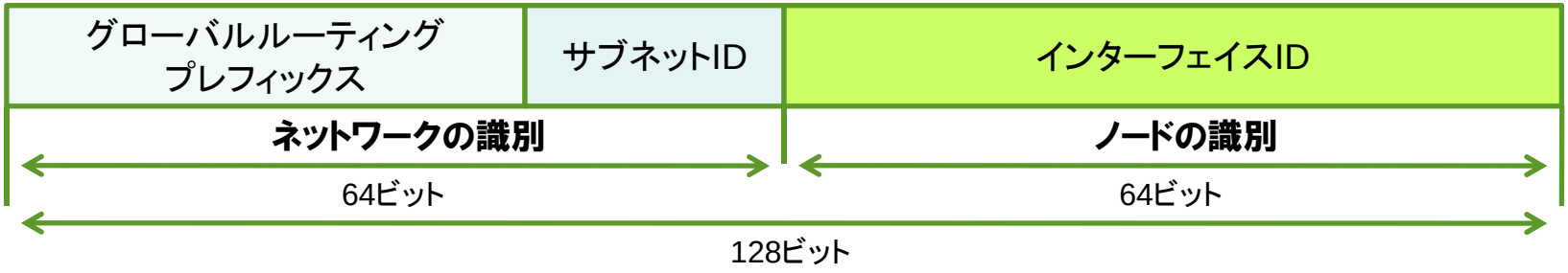
- 固定の場合，IPアドレスが認識されると，攻撃の対象になりやすいことから，セキュリティ問題として扱う．
  - 特定のホストに対する攻撃
  - ユーザ宅の対外リンクを埋めるような攻撃　等

ユーザ宅に対するアドレス割当問題

- IPv4ではユーザ宅へのアドレスは非固定が主流
  - –ダイアルアップでのアドレス使い回しの名残
  - –固定アドレスは有料☺
- IPv6ではどうなるか.
  - –固定アドレスが主流？
    - プライバシーの問題や，外部からのアタックがしやすくなる可能性
  - –可変にする？
    - 宅内機器のアドレス変更が必要になる
      - –ビデオレコーダ，冷蔵庫など，長時間（常時？）電源が入っている機器も増えてくる.
    - 各機器はアドレスを使い分けられるか？
    - 機器のトレースがしにくくなることにより，各種問題が把握しづらくなる

プロトコル的な対処：IPv6 Privacy Extension

- RFC4941: Privacy Extensions for Stateless Address Autoconfiguration in IPv6
  - **IPv6アドレスの下位64ビット（インターフェイスID）にランダムな値を用いる．**
    - **一定時間（最大7日間）で更新しノードの特定を困難にする**



  - **ホストアドレスの隠蔽は可能だが，ネットワーク部は隠蔽されない．**

アドレスは固定か，非固定か．

	カテゴリ	具体的なイメージ	対象	セキュリティ/プライバシー
固定	ISPとの契約を解除する都度アドレスが変わる	ユーザがISP-AからISP-Bに契約を変更する場合	運用管理が容易	攻撃の対象になっていないユーザは固定アドレスのメリットを享受
固定	場所が変わる都度アドレスが変わる	ユーザが引っ越しをする場合		プライバシー問題あり
固定	オペレーション都合の都度アドレスが変わる	ISPバックボーンの設計変更等数年に一回程度		
非固定	ユーザの申告の都度アドレスが変わる	DoS攻撃を受けたのでアドレスを変更したい場合	宅内すべてのアドレスが変わってしまう可能性がある	攻撃の対象になっているユーザは攻撃を回避できる
非固定	接続の都度アドレスが変わる	家庭用ルータもしくはPCを起動する度にアドレスが変わる（ユーザは気付かない程度)	・リンクダウン時 ・家庭用ルータ交換時	

IPv6普及・推進高度化協議会 共存WG 家庭用ルータSWG ガイドラインより抜粋

おわりに

IPv6時代のホームネットワーク

- IPv4との「違い」に注意する必要がある
  - 端末一つひとつがグローバルアドレスで外から reachable になる
  - デュアルスタック端末は，出入り口（プロトコル）が二つある
  - アドレスは固定が主流（？）
- ユーザに「違い」は認識させたくはない
  - トンネルなど，移行期はしかたない？
  - ISPなどの事業者がどこまでカバーできるか．