NTT

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

IPv6 とセキュリティ

NTT情報流通プラットフォーム研究所
藤崎 智宏
fujisaki@nttv6.net

IPv6のセキュリティ

- IPv6のセキュリティは,
  - IPv6自体のセキュリティ課題
  - IPv6実装のセキュリティ問題
  - IPv6/IPv4共存時に発生する問題
  - IPv6時代のセキュリティモデル

等について考える必要があります.

IPv6のセキュリティ：標準化（1／2）

- 標準化の領域でも，IPv6プロトコル（関連）のセキュリティ議論は多い．

IPv6プロトコル自体のセキュリティ

- RFC5722: Handling of Overlapping IPv6 Fragments
- RFC5095: Deprecation of Type 0 Routing Headers in IPv6

IPv6利用時のセキュリティ

- RFC5157: IPv6 Implications for Network Scanning
- RFC4942: IPv6 Transition/Co-existence Security Considerations
- RFC4896: Recommendations for Filtering ICMPv6 Messages in Firewalls
- RFC4864: Local Network Protection for IPv6

IPv6移行プロトコルに関するセキュリティ

- RFC5991: Teredo Security Updates
- RFC3964: Security Considerations for 6to4

IPv6のセキュリティ：標準化（2／2）

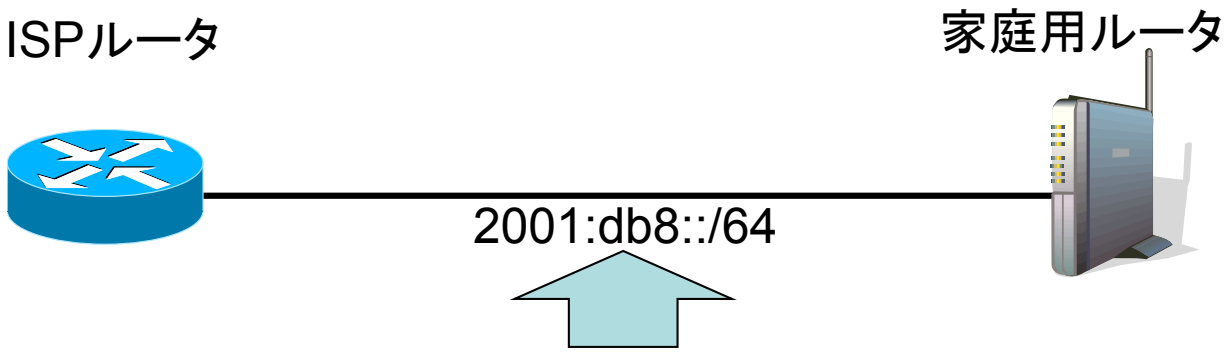
- 標準化の領域でも，IPv6プロトコル（関連）のセキュリティ議論は多い．

  議論中のもの

  – Recommended Simple Security Capabilities in Customer Premises Equipment for Providing Residential IPv6 Internet Service: draft-ietf-v6ops-cpe-simple-security
  – Rogue IPv6 Router Advertisement Problem Statement: draft-ietf-v6ops-rogue-ra
  – IPv6 Router Advertisement Guard: draft-ietf-v6ops-ra-guard
  – Security Concerns With IP Tunneling: draft-ietf-v6ops-tunnel-security-concerns

標準化以前の問題

- 近隣探索にまつわる問題
  - 標準化の舞台でも指摘，解決方法の提案はあったが，今後の課題となっている.
- IPv6の近隣探索 ≒ IPv4のARP
  - （ユーザ側でなく）ISP側で大きな問題になりうる.



  - 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？

IPv6とプライバシー

- 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

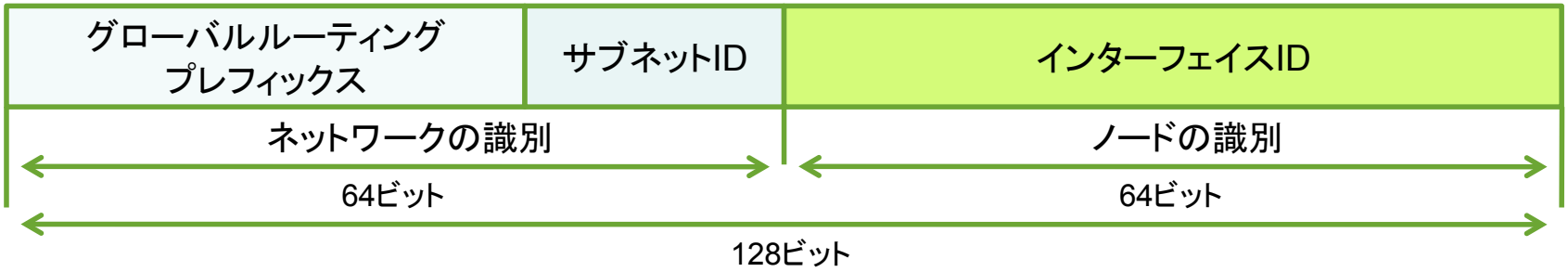
- 固定の場合，IPアドレスが認識されると，攻撃の対象になりやすいことから，セキュリティ問題とも考えられる．
  - 特定のホストに対する攻撃
  - ユーザ宅の対外リンクを埋めるような攻撃　等

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

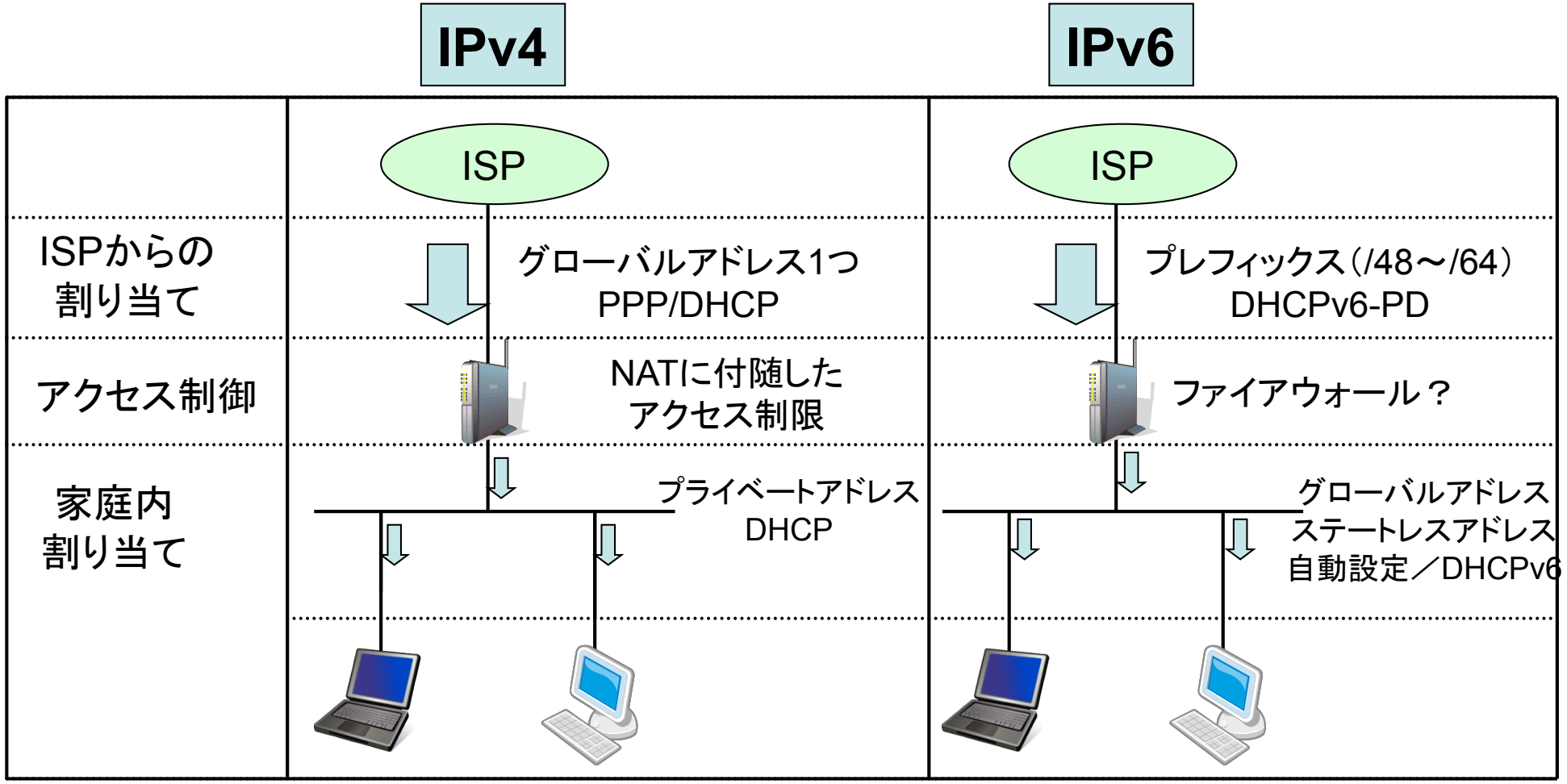
- RFC4941: Privacy Extensions for Stateless Address Autoconfiguration in IPv6
  - IPv6アドレスの下位64ビット(インターフェイスID)にランダムな値を用いる.
    - 一定時間(最大7日間)で更新しノードの特定を困難にする



  - 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.
    - 割り振りアドレスを自動的に変更することも，プロトコル的には可能.

IPv6時代のセキュリティ

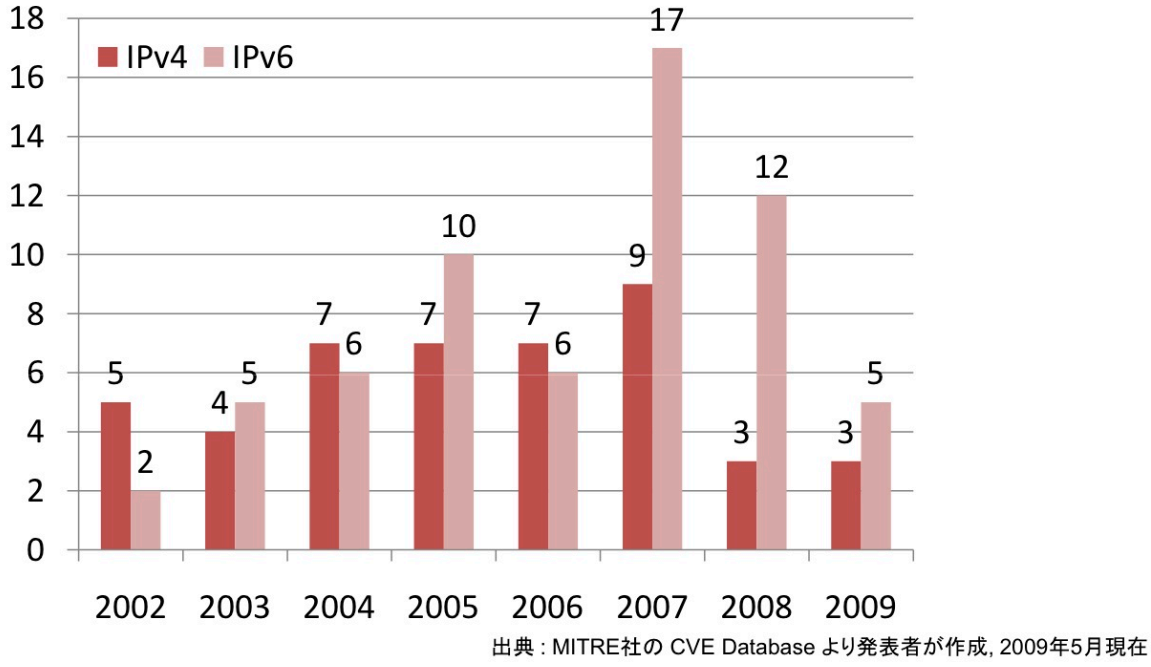
- 家庭内の全ての機器にグローバルアドレスが付与される.



さらなる議論が必要

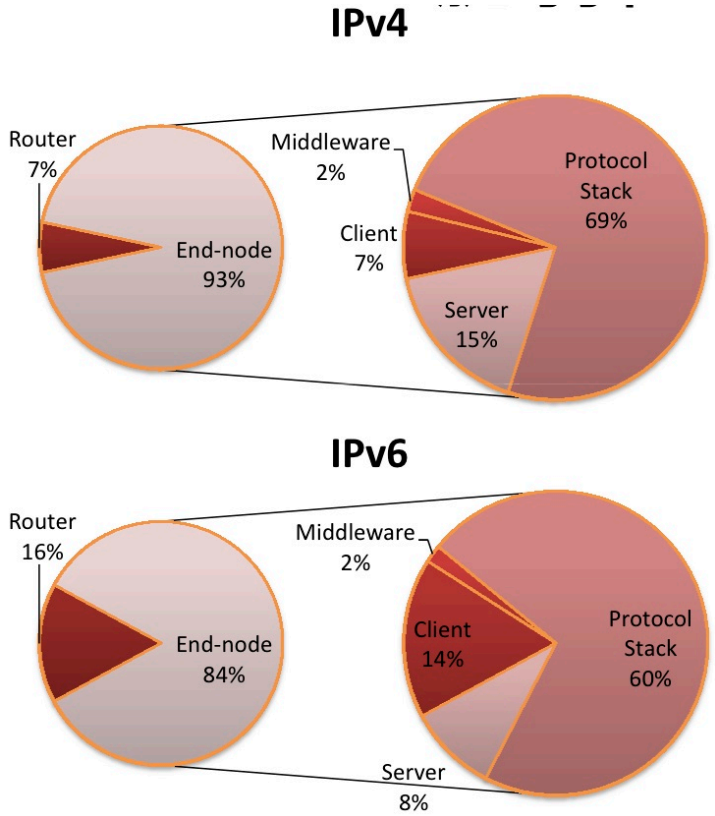
IPv6のセキュリティ：報告

- IPv6は，IPv4ほど枯れていない



出典：MITRE社の CVE Database より発表者が作成，2009年5月現在

IPv4/IPv6 プロトコル特有の脆弱性の推移



IPv4/IPv6に関連した脆弱性の傾向

両グラフとも，白畑 真/株式会社クララオンライン さん，「点検！サービスのセキュリティ」，InternetWeek 2009，
http://www.nic.ad.jp/ja/materials/iw/2009/proceedings/h5/iw2009-h5-04.pdf より

- 最近のIPv6に関する脆弱性の登録数はIPv4よりかなり多い．
- 脆弱性のIPv4，IPv6とも，多くは，プロトコルスタックに関係するもの．

終わりに

- IPv6のセキュリティを考える際に，
  - IPv6自体のセキュリティ課題
  - IPv6実装のセキュリティ問題

  を分けて考える必要があります．また，
  - IPv6/IPv4共存時のセキュリティ課題

  さらに，
  - IPv6時代のセキュリティモデル

  についても，今後，検討をすすめる必要があります．