IPv6のセキュリティ

北口　善明
金沢大学 総合メディア基盤センター

IPv6導入時のセキュリティ観点

- 仕様上における課題
  - IPv4と同様のもの
  - IPv6で顕著になるもの
  - IPv6で登場するもの
- 運用上における課題
  - デュアルスタック時の動作の認識
  - IPv6機能が有効であることの認識

IPv4と同様の課題

- IPv6はIPv4の仕組みを（良くも悪くも）継承
  - ソースルーティングなどのオプション機能
    - IPv4で実質利用されないものも継承
  - 信頼モデルを基にしたリンク内プロトコル
    - ARPと同様に認証機構がないNDP
    - マルチキャストでのMLDも同様
    - 便利さと実装の容易さを優先したモデル
  - ⇒ 便利さを残しつつのセキュリティ対策が求められる

IPv6で顕著になる課題

- エンドまで到達可能になる点
  - セキュリティ対策の重要性がIPv4と比較して増加
  - エンドノードのセキュリティ担保が必要
- アドレス量が増える点
  - スキャニングに強くなる半面、攻撃元の特定が困難
    - 遠隔からの無差別攻撃は実質不可能
  - 機器におけるリソース消費の増大
    - 同一セグメントに最大で2^{64}台の端末が接続可能
    - 複数のプレフィックス、デフォルト経路を設定可能

IPv6で登場する課題

- 拡張ヘッダ処理に伴うリソース消費の増大
  - 仕様上設定数の上限がないものもある
  - IPヘッダと上位ヘッダの間にあるので走査が必要
    - フィルタリング実装がIPv4よりも複雑化
- IPv4と仕様が異なる点
  - 落とせなくなったICMP
    - PMTUD、NDP、フォールバックなどに必須
  - 自動アドレス設定の違い
    - DHCPv6ではデフォルト経路は配れない
    - RAはpushで機器の設定を変更できる
  - P2Pセグメントの扱い
    - /127は仕様上使えない

デュアルスタックでの課題（1）

- IPv6優先利用の認識
  - 基本的にデュアルスタックではIPv6を優先
  - OSにより挙動が少々異なる
- DNSの挙動の認識
  - 名前解決と利用プロトコルは独立
    - IPv4アドレスのDNSサーバに対してIPv6の名前解決が可能

    ⇒ DHCPv6による設定はIPv4通信にも影響
  - DNSクエリが二倍
    - AクエリとAAAAクエリを出す必要がある

デュアルスタックでの課題（2）

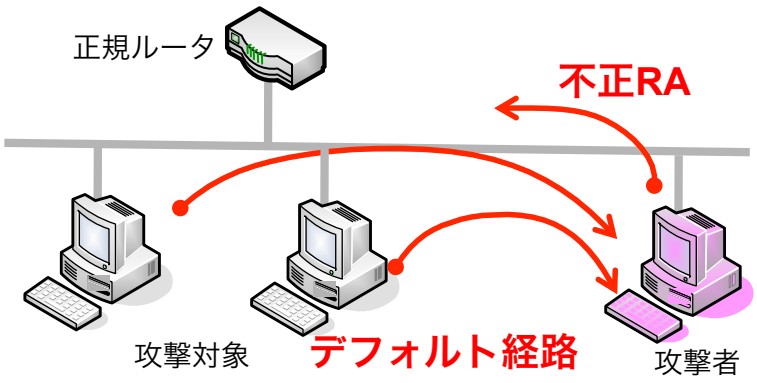
- IPv6が有効になっている認識
  - デフォルトでIPv6機能が有効になっている
  - 自動トンネリング機能でIPv6到達性がある場合も

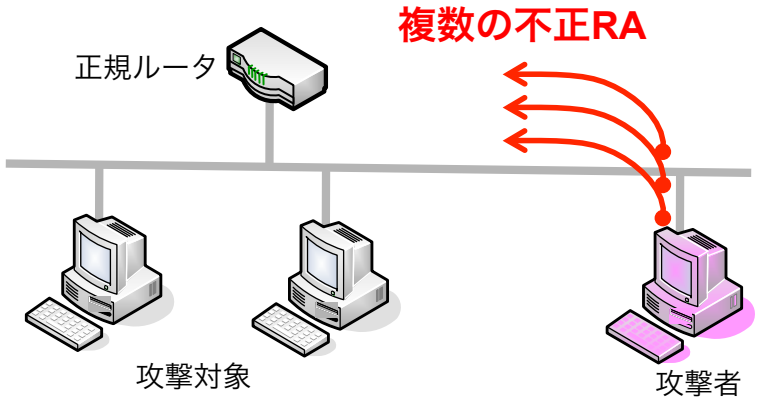
  ⇒ 知らずにIPv6通信となることが危険
- IPv4射影アドレスの認識
  - IPv6アプリでIPv4通信も扱える

  ⇒ 意図しないIPv4通信となる可能性
  - IPV6_V6ONLYソケットオプションで無効可能

具体例（1）：不正RA

- 概要
  - 意図しないアドレス／デフォルト経路の生成
  - RAは1つのパケットでセグメント内全体に影響を与える
  - DHCPと異なりアドレスの追加設定が可能
- 想定される問題
  - IPv4の偽DHCPサーバ設置と同様の脅威
  - 通信断、盗聴、機器のリソース消費、意図せぬ通信





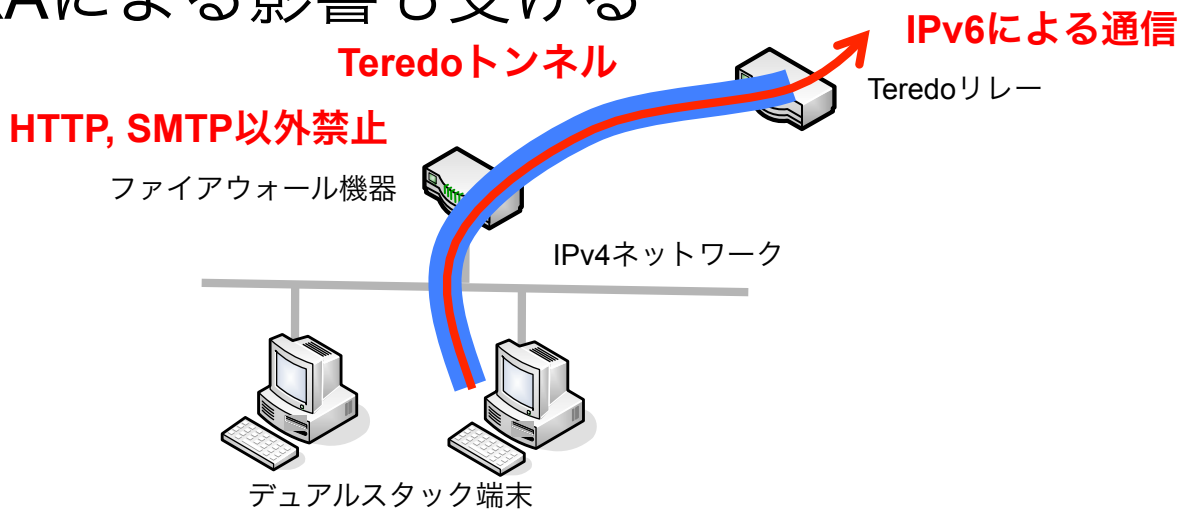
多数のアドレス／デフォルト経路

具体例（1）：不正RA

- 対策
  - スイッチによるRAのフィルタリング
  - Router Preference（RFC4191）の利用
    - 意図的なものは排除できない
  - モニタリングによる対策
    - NDPMon：セグメント内のNDPパケットの異常を検知
    - rafixd（KAME）：不正RAと同じRAをRouter Lifetime=0で広告
      不正RAによる機器の学習内容をリセット
  - SEND（Secure Neighbor Discovery）の導入
    - 実装機器は少ない
  - 設定アドレスの上限設定
    - 無制限にRAを受け付けず上限を実装において設ける

具体例（2）：意図しないIPv6通信

- 概要
  - IPv4しかないネットワークからのIPv6通信
  - デフォルトでIPv6機能が有効
    - Windows Vista/7では自動トンネル機能が有効
- 想定される問題
  - アクセス制御を回避した通信がIPv6で可能
  - 不正RAによる影響も受ける



具体例（2）：意図しないIPv6通信

- 対策
  - IPv4ネットワークでもデュアルスタック端末の存在を認識することが重要
  - Teredoを禁止するルールを追加
    - 3544/udpのフィルタ
  - 正しい動作の理解が肝要
    - 6to4トンネル：インターフェイスにIPv4グローバルアドレスが付与されると設定されるが、IPv6のみの通信相手でない限りIPv4通信が優先される（RFC3484ルール）
    - Teredoトンネル：インターフェイスにIPv4アドレスが付与されると設定されるが、利用優先度は一番低く、自信からの発信がない限りパケットを受信しない
    - 名前解決：IPv6グローバルアドレスがインターフェイスに付与されないと実施しない実装がある（Windows Vista/7）

まとめ

- 基本的にIPv4と同様の課題をIPv6は持つ
  - IPv4との違いの認識が必要
- IPv6機能が有効である認識を持つことが重要
  - IPv4ネットワークでの対策も必要
- デュアルスタック時の挙動把握も必要
  - IPv6優先挙動やIPv6ソケットの理解
- IPv6で良くなること
  - アドレス空間増大によるアドレススキャンの不可
  - IPsec標準実装のアドバンテージ