金沢大学
KANAZAWA UNIVERSITY

IPv6セキュリティの勘どころ

IPv6とセキュリティ

金沢大学 総合メディア基盤センター
北口 善明

0. 本日のセッションの概要

金沢大学 KANAZAWA UNIVERSITY

- IPv6におけるセキュリティ概要
  - IPv6導入時におけるセキュリティ課題の整理
  - 簡単なIPv6の仕様も含めた解説
- 企業ネットワークの観点からの整理
  - 企業ネットワークでの注意点とセグメント毎の対策
  - IPv6の市場動向やIPv6の導入事例紹介
- 家庭ネットワークの観点からの整理
  - 家庭などの小規模ネットワークにおける注意点と対策
  - 端末やISPのIPv6対応状況やプライバシ

1.1. IPv6対応時のキーワード

金沢大学 KANAZAWA UNIVERSITY

「IPv6対応」 ≠ 「IPv6への移行」

- IPv4ネットワークがなくなるのではない
- IPv6ネットワークの追加運用

二重のネットワーク運用

- 三つの視点での考慮が必要
  - IPv4ネットワーク
  - IPv6ネットワーク
  - デュアルスタックネットワーク
- IPv4だけのネットワーク運用との相違点の把握が重要

1.2. IPv6移行時のセキュリティ観点の整理

金沢大学 KANAZAWA UNIVERSITY

仕様上における課題

- IPv4にも存在する同様の課題
- IPv6にて顕著になる課題
- IPv6にて新たに登場する課題

実装上における課題

- 仕様上で明示的な記述がない処理
- 実装における検証が不十分である点
- 新しい仕様の実装が遅れている点

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

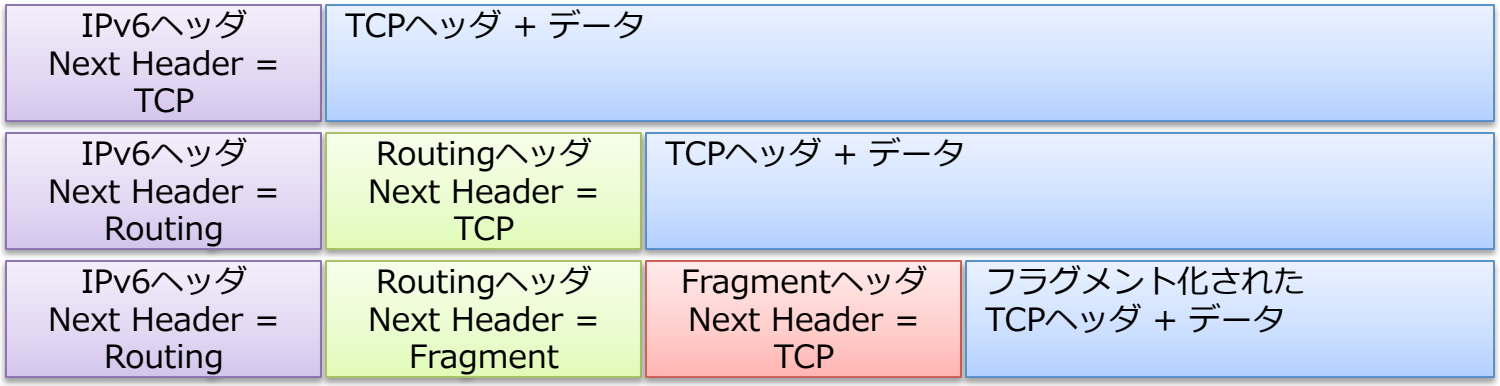
2.1. 仕様上の課題　～IPv4と同様の課題～

金沢大学 KANAZAWA UNIVERSITY

- 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
    - 攻撃例
      - ルータ探索における攻撃
      - アドレス設定における攻撃
      - アドレス解決における攻撃
      - リダイレクトによる攻撃　　等

2.2. IPv6拡張ヘッダ

- 数珠つなぎで拡張機能を付加
  - IPv6ヘッダが固定長化されたために導入された機能

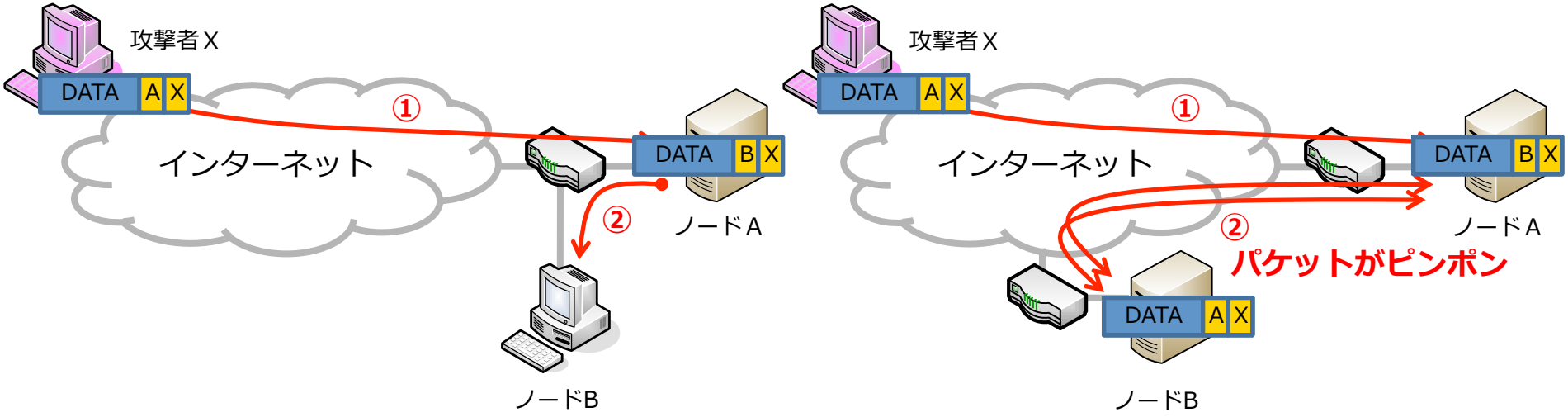


- 拡張ヘッダの種類

Protocol番号	拡張ヘッダ名称	説明
0	Hop-by-Hop Options header	中継ノードの処理を記述する
43	Routing header	送信元がルーティング経路を指定する Type 0は利用禁止に（RFC5095）
44	Fragment header	パケット分割時に利用する
60	Destination Options header	エンドノードにて実行する内容を記述する
51	Authentication header	エンドツーエンドにて完全性と認証を提供する
50	Encapsrational Security Payload header	IPsecにてペイロードを暗号化する際に利用する

2.3. 具体例(1)：ソースルートオプション

- 概要
  - タイプ0ルーティングヘッダを利用した攻撃
    - 現在は利用が禁止されている仕様
  - ソースルートプションはIPv4においても問題があった
    - そのままの機能をIPv4から引き継いだもの
- 想定される問題
  - 中継ノードを指定することによるアクセス制御回避
  - 指定する二台のノード間でのパケット増幅攻撃



2.4. 近隣探索プロトコル：NDP

金沢大学 KANAZAWA UNIVERSITY

Neighbor Discovery Protocol

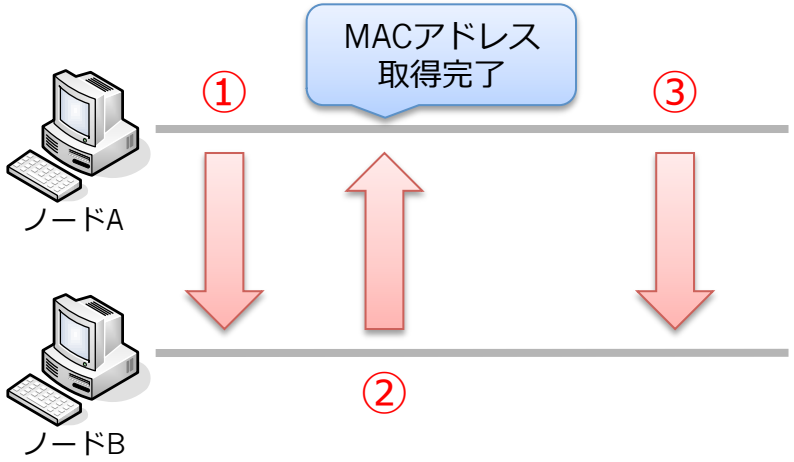
処理	機能	説明
リンクレイヤアドレスの解決（ARP相当）	近隣キャッシュ	IPアドレスとリンクレイヤアドレス（MACアドレス）対応を保持
	不到達検出機能	近隣キャッシュ内のリストを最新に保つ機能
自動アドレス設定（SLAAC）	重複アドレス検出機能（DAD）	設定IPアドレスの重複がないか検出する機能（RFC5227にてIPv4の仕様に逆輸入された）
	デフォルトルートの設定	ルータ広告の送信元IPアドレスを利用
	グローバルアドレスの生成	ルータ広告に含まれるプレフィックス情報を利用

5つのメッセージタイプ

機能	説明
ルータ要請（ICMPv6 type 133） RS：Router Solicitation	セグメント内のルータ発見に利用 ルータ広告を即座に取得する場合に送出
ルータ広告（ICMPv6 type 134） RA：router Advertisement	ルータによるデフォルト経路の通知 プレフィックス情報配布で自動アドレス設定が可能
近隣要請（ICMPv6 type 135） NS：Neighbor Solicitation	重複アドレス検出や到達性／不到達性の確認 リンクレイヤアドレスの解決
近隣広告（ICMPv6 type 136） NA：Neighbor Advertisement	近隣要請に対する応答、自身のIPアドレス変更の通知
リダイレクト（ICMPv6 type 137）	最適なデフォルト経路を通知（IPv4のリダイレクトと同様）

2.5. NDPの動作概要

リンクローカルアドレス解決の流れ

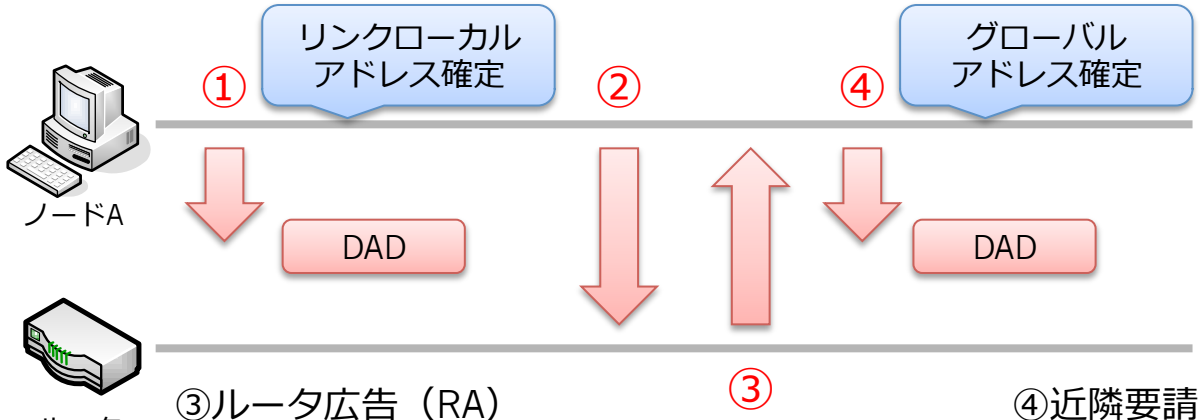


①近隣要請（NS）
通信相手のMACアドレスを探索
（宛先はマルチキャスト）
近隣広告がない場合はオンリンクでないと判断

②近隣広告（NA）
ターゲットアドレスを持つノードが回答
ただし誰でもこの応答は可能

③通信開始

SLAACの流れ



①近隣要請（NS）
近隣広告がなければ
アドレスの利用が可能

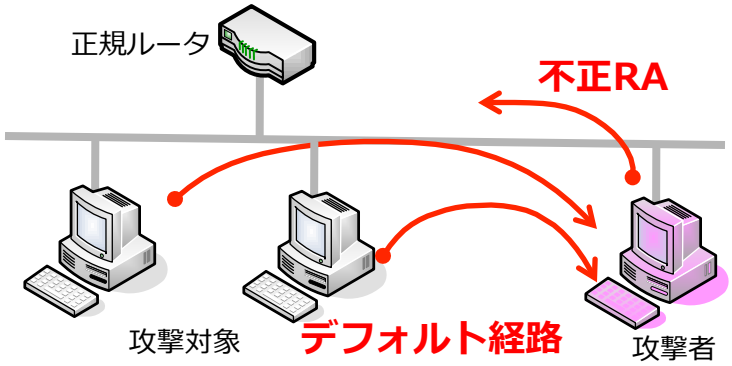
②ルータ要請（RS）
全ルータマルチキャスト
（ff02::2）宛に送信

③ルータ広告（RA）
全ノードマルチキャス（ff02::1）宛に送信
取得プレフィックスからグローバルアドレス
を生成

④近隣要請（NS）
近隣広告がなければアドレスの利用が
可能（応答があるとアドレスを再構成）

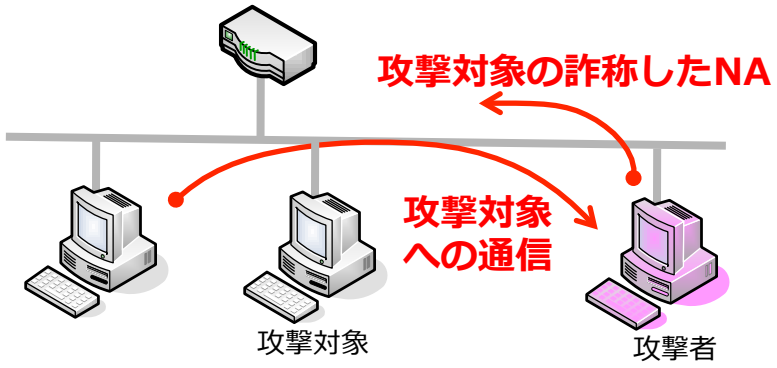
2.6. 具体例(2)：不正RA

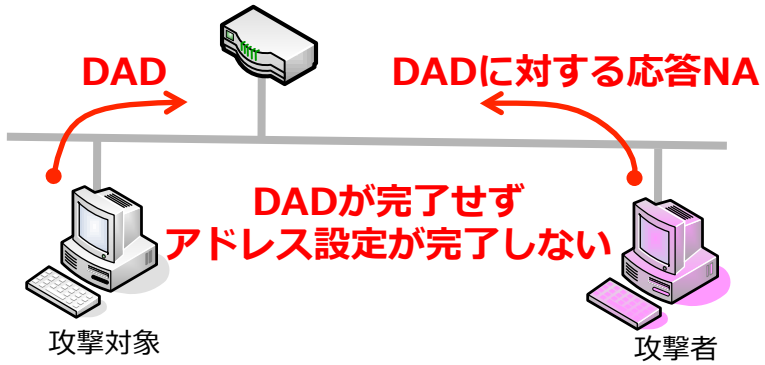
- 概要
  - 意図しないアドレス／デフォルト経路の生成
  - RAは1つのパケットでセグメント内全体に影響を与える
  - DHCPと異なりアドレスの追加設定が可能
- 想定される問題
  - IPv4の偽DHCPサーバ設置と同様の脅威
  - 通信断、盗聴、機器のリソース消費、意図せぬ通信



2.7. 具体例(3)：NA詐称

- 概要
  - 近隣広告（NA）の詐称により近隣キャッシュを汚染
    - ARPと異なり”override flag”の設定で強制的な変更可
  - 攻撃対象のIPアドレスへの通信を誘導可能
  - DADにおける応答を返すことでIPアドレス設定を妨害
- 想定される問題
  - IPv4のARPにおける問題と同様の脅威
  - 通信断、盗聴、サービス妨害、意図せぬ通信





3.1. 仕様上の課題　～IPv6で顕著になる課題～

金沢大学 KANAZAWA UNIVERSITY

- 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
- ノードが複数のアドレスを持てる点
  - IPv4と異なりI/Fに複数のアドレス設定が基本
- 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

※実装上の課題でもある

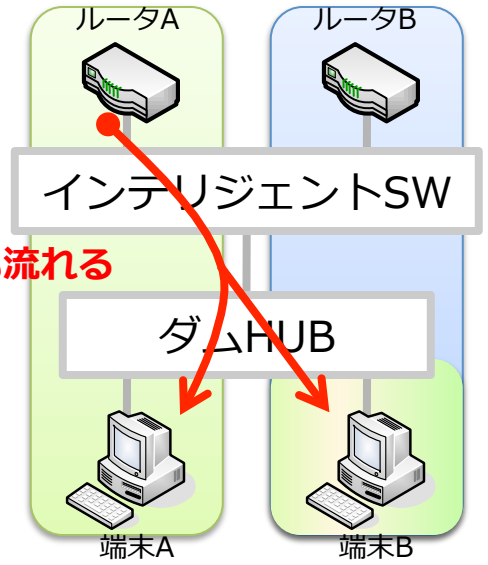
3.2. ノードやルータが持つIPv6アドレス

金沢大学 KANAZAWA UNIVERSITY

- ノードが持つアドレス（最低6こ）
  - インターフェース毎のリンクローカルアドレス
  - インターフェース毎のユニキャストアドレス
  - ループバックアドレス
  - 全ノードマルチキャストアドレス
  - 要請ノードマルチキャストアドレス
  - 所属するマルチキャストアドレス
- ルータが持つアドレス（最低8こ）
  - ノードが持つアドレス
  - サブネットルータエニーキャストアドレス
  - 全ルータマルチキャストアドレス

3.3. 具体例(4)：マルチキャストとVLAN

- 概要
  - IPv6はRAなどで積極的にマルチキャストを利用
  - ノードは複数のIPv6アドレスを持つ点がIPv4と異なる
  - IPv4で問題が出なかった構成でもIPv6で問題の可能性
    - IPv4ではIPアドレスは1つであったから顕在しなかった
    - IPv6では1ノード1IPアドレスが成り立たない認識が重要
- 想定される問題
  - 異なるVLANのアドレスを取得することに因る意図しない通信の発生
    - 異なるVLAN間の短絡通信など
  - 情報漏えい

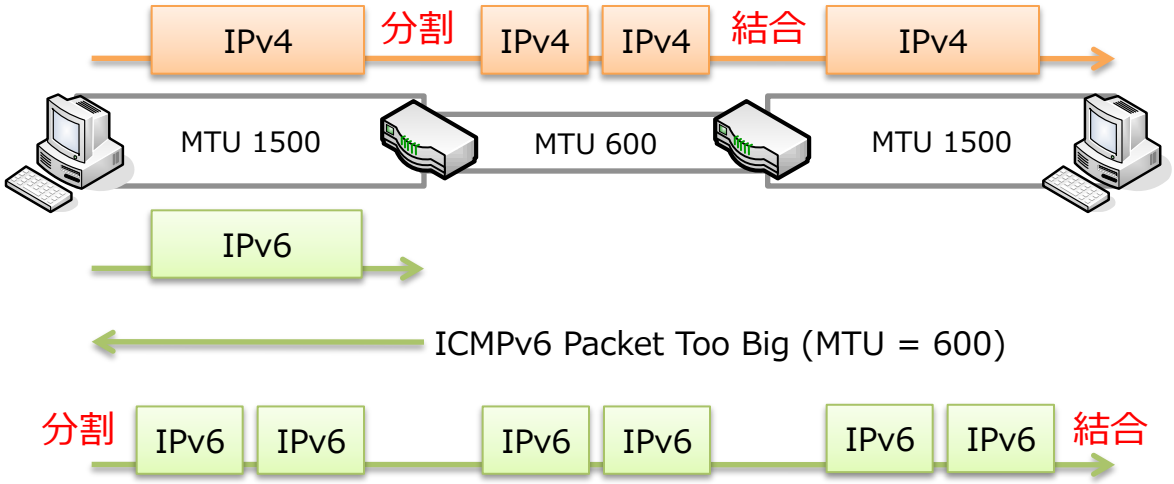


4.1. 仕様上の課題　～IPv6で登場する課題～

- 拡張ヘッダ処理に伴うリソース消費の増大
  - 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は仕様上使えないものであった
    - RFC6164でIPv4の/30と同様の運用が可能に

4.2. パケットフラグメント処理の違い

- Path MTU Discovery（PMTUD）が必須に
  - 通信経路の最小MTUサイズを求める手順
  - 中継ノードでのフラグメントをしないIPv6では必須
    - IPv4では中継ノードで適宜フラグメントしている
  - ICMPv6を利用して調整
    - 転送先リンクのMTUサイズを超えるパケットが来た場合
      ルータは送信元にICMPv6 Packet Too Bigを送信
    - 送信元はメッセージ内のMTUサイズにフラグメントして再送信



4.3. フィルタリング設定時の注意点

- IPv6ではICMPv6の扱いが重要
  - IPv4と異なりICMPを全て落とすと通信不能に

ICMPv6タイプ	説明
type 2 （Packet Too Big）	ルータでのフラグメントができないため通信経路のMTUサイズを調べるPath MTU Discovery（PMTUD）で必要となるため必須
type 135 （Neighbor Solicitation） type 136 （Neighbor Advertisement）	同一セグメント内の通信のためにはNDPによるリンクレイヤアドレス解決が必要 この処理に二つのタイプが必須
type 1 （Destination Unreachable）	IPv4からIPv6への迅速なTCPフォールバックのためにはエラー通知が必要

4.4. 自動アドレス設定手法

- 設定項目の差異の認識が必要
  - 二種類の方式で設定できる項目に違いがある

	RA	DHCPv6
デフォルト経路	○	ー　※1
アドレス／プレフィックス	プレフィックス割り当て	アドレス割り当て
プレフィックス長	○	RAから学習
サーバ情報（DNSなど）	△　※2	○

※1 標準化されておらずIETFにて議論中のステータス

※2 RFC6106にてDNSサーバの配布（RDNSSオプション）が仕様化された

【参考情報】
各端末OSにおけるDHCPv6とRAのRDNSSオプションの実装状況
http://en.wikipedia.org/wiki/Comparison_of_IPv6_support_in_operating_systems より

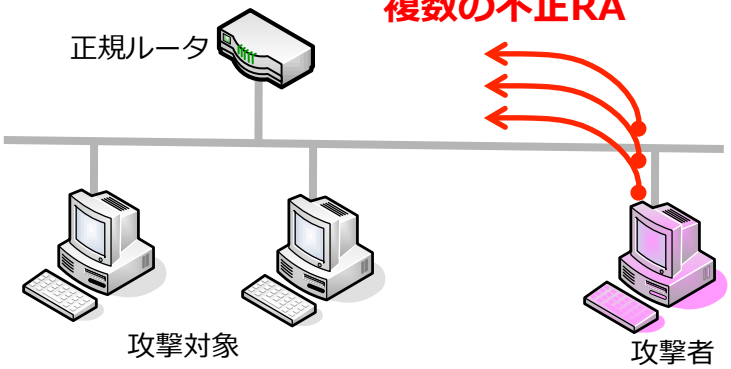
OS	DHCPv6	RDNSS
Windows XP	×	×
Windows Vista	○	×
Windows 7	○	×
Mac OS X 10.6	×	×
Mac OS X 10.7	○	○
RHEL 6	○	○
Ubuntu 10.10	○	○
Android 2.3.4	×	×
iOS 4.1	○	○
Windows Phone 6.5	△	×

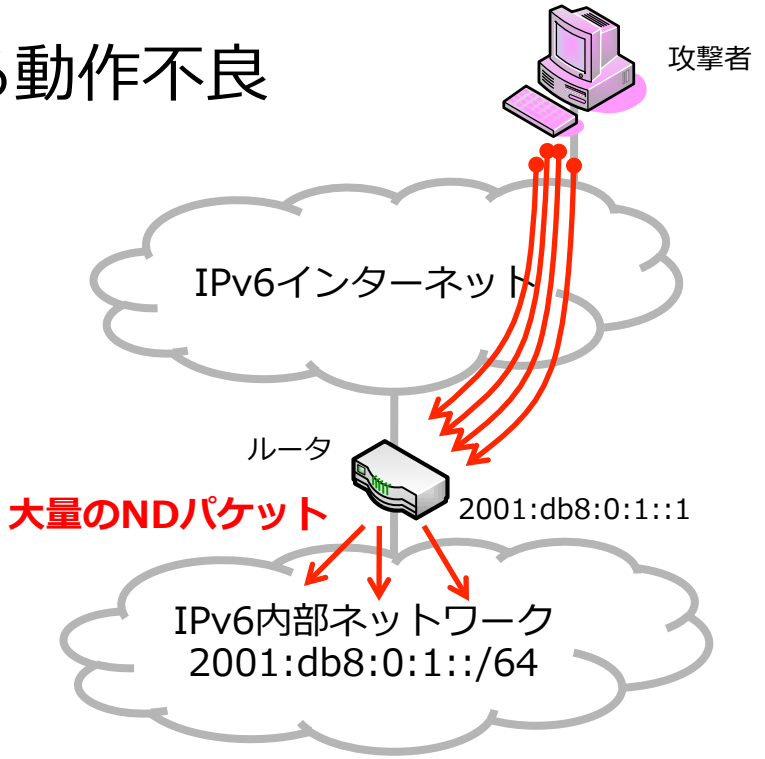
5.1. 実装上の課題

- 機器で扱うリソースの上限値は実装依存
  - 拡張ヘッダの処理数の上限
  - インターフェースに設定するアドレスの上限
  - デフォルト経路の設定数の上限
  - NDPキャッシュの登録数の上限
- デュアルスタック時の挙動は実装依存
  - IPv6とIPv4のどちらを優先するか
  - 機器（OS）毎の挙動の違いを把握する必要あり
- 「IPv6対応」は実装依存
  - どの仕様（RFC）を実装しているかで挙動が異なる

5.2. 具体例(5)：大量アドレス利用

- 概要
  - アドレスの異なる大量の通信（DoS攻撃）
    - セグメント内のノード許容数は2^{64}個
  - 大量のリンクレイヤアドレス解決におけるリソース消費
- 想定される問題
  - 機器のリソース消費による動作不良
  - サービス不能





6.1. 運用上の課題　～デュアルスタックの挙動～

金沢大学 KANAZAWA UNIVERSITY

- 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

6.2. OS毎のDNSリゾルバ実装の差異

- クエリ順序はOSで異なる
  - AAAAクエリを先に実施するOS
    - Windows XP、Linux
  - Aクエリを先に実施するOS
    - Windows Vista、Windows 7、FreeBSD、Mac OS X
- 利用プロトコルの優先順位
  - IPv6を優先的に利用するOS
    - Windows Vista、Windows 7
  - IPv4しか利用できないOS
    - Windows XP
  - 設定ファイルに依存するOS（/etc/resolv.confの順序）
    - Mac OS X、FreeBSD、Linux

7.1. 運用上の課題　～IPv6機能有効時の挙動～

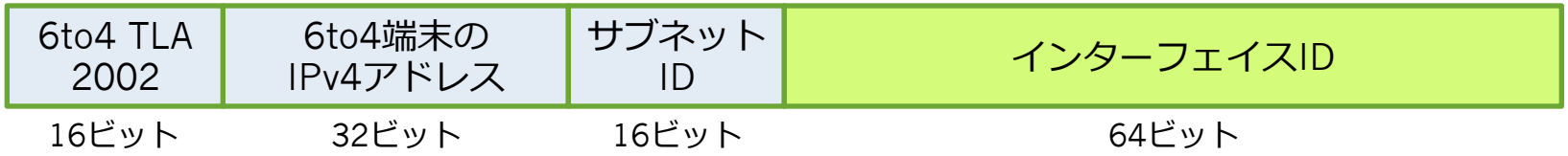
金沢大学 KANAZAWA UNIVERSITY

- 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通信を扱うためのアドレス
  - 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

7.2. 自動トンネリング

- 6to4（RFC3056）
  - トンネル接続とIPv6アドレス割り当てを同時に実現
  - IPv4グローバルアドレスを利用したIPv6アドレス

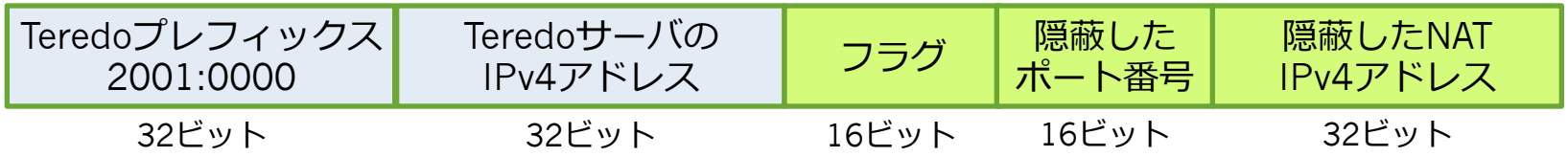
◆6to4のアドレス形式



・/48のアドレス空間が割り当てられる

- Teredo（RFC4380）
  - NATトラバーサルをIPv6で実現する技術
  - NATの内側からIPv6トンネル接続が可能

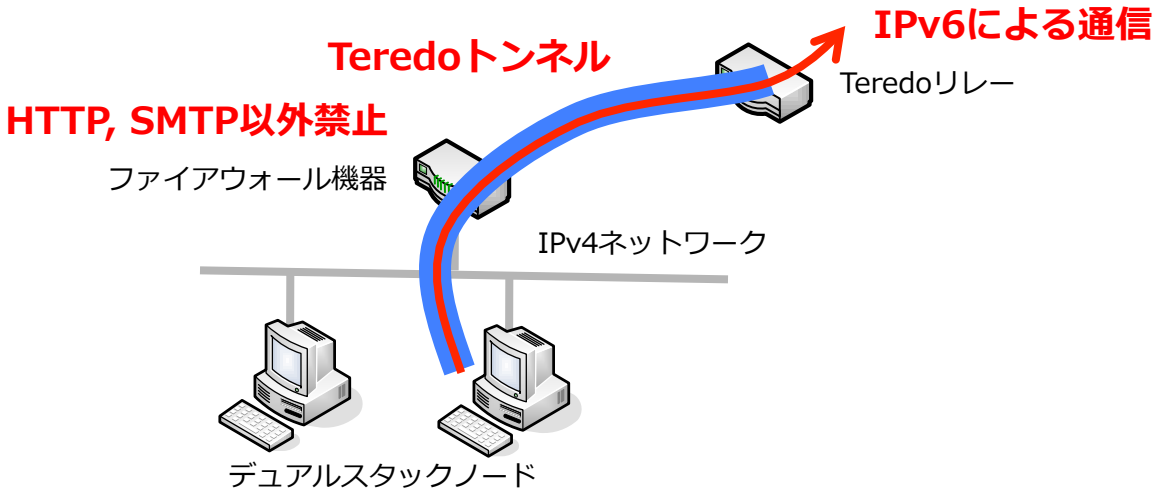
◆Teredoのアドレス形式



・/128のアドレスが一つ割り当てられる

7.3. 具体例(6)：意図しないIPv6通信

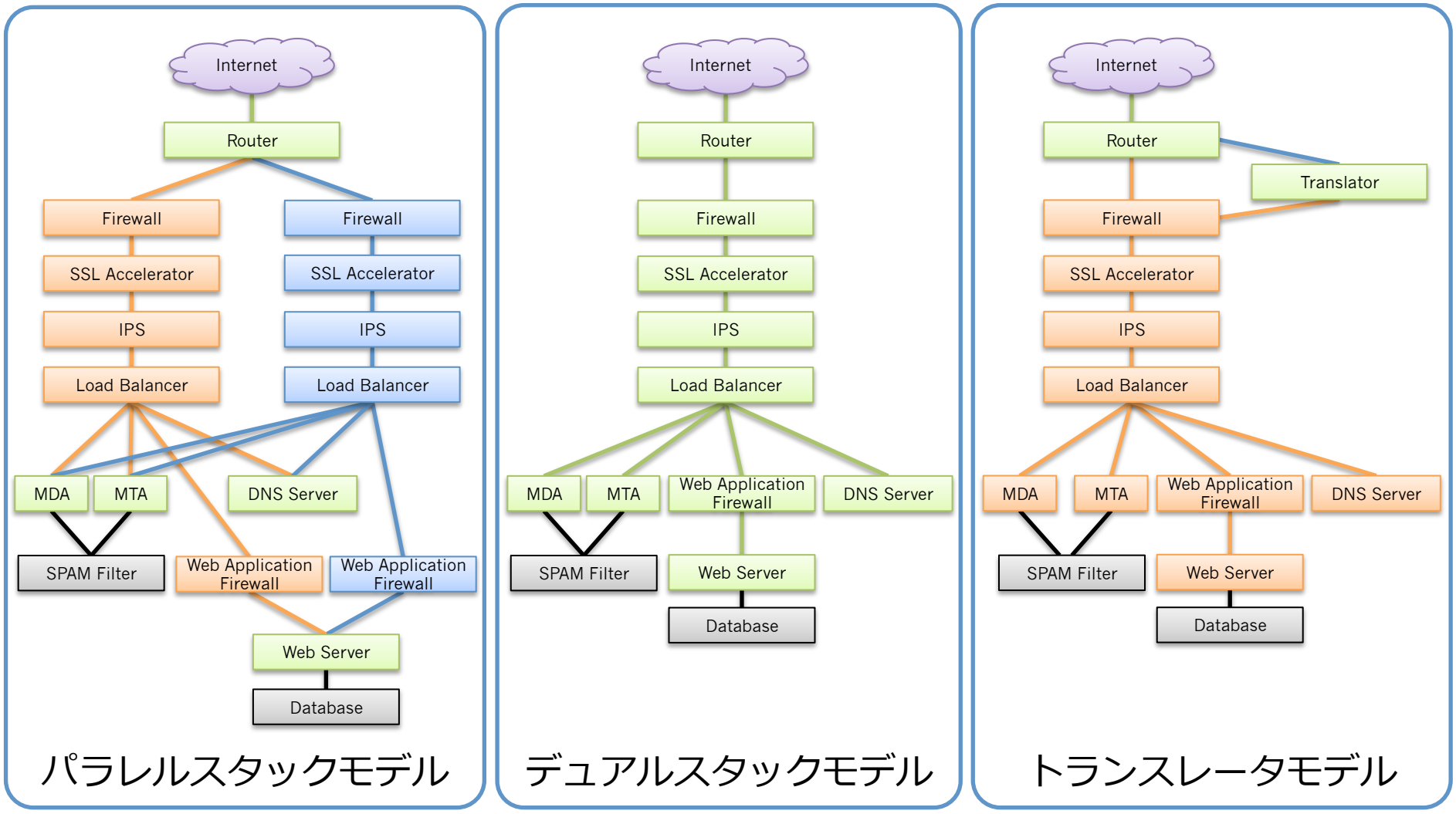
- 概要
  - IPv4しかないネットワークからのIPv6通信
  - デフォルトでIPv6機能が有効
    - Windows Vista/7では自動トンネル機能が有効
- 想定される問題
  - アクセス制御を回避した通信がIPv6で可能
  - 不正RAによる影響も受ける



8.1. IPv6導入モデルの整理

- 二重のネットワーク運用における分類
  - IPv6対応はデュアルスタックだけではない
  - 導入セグメントの性質に注意して検討が必要
- 3つの導入モデル
  - パラレルスタックモデル
    - IPv6ネットワークをIPv4と独立して導入するモデル
  - デュアルスタックモデル
    - 機器をIPv6対応し両プロトコルで運用するモデル
  - トランスレータ
    - IPv4ネットワークを変更せずトランスレータによりIPv6対応をするモデル

8.2. 3つの導入モデルの比較（DMZの例）



8.3. 導入モデルにおける注意事項

金沢大学 KANAZAWA UNIVERSITY

- 3つの導入モデルにおけるメリット／デメリット

	メリット	デメリット
パラレル スタック	• 分岐点が明確 • 概念が単純 • 実績の少ないネットワークの分離が可能 • 導入・移行が容易	• 初期投資が多い • 管理対象が増す
デュアル スタック	• 新規投資が少ない	• セキュリティ機器の実績が乏しい • ネットワーク構造を変更する必要がある • 分析・管理工数が増加 • 障害時の影響範囲が広い
トランスレータ	• 新規投資が少ない • ネットワークの構造変更が少ない	• 実績が非常に少ない • 障害発生時の対応が比較的難しい • セキュリティ機器の通信制御が難しい

9. まとめ

IPv6関連の現状認識として

◆IPv6対応機器はクライアントOSなど多く存在

IPv6の技術習得が本格的に必要な段階

セキュリティ対策の考慮が必要

◆基本的にIPv4と同様の課題をIPv6は持っている

◆IPv6の仕様の理解とIPv4との違いを把握することが重要

◆デュアルスタックでの挙動の理解が肝要

◆IPv4のみのネットワークでもIPv6対応OSが存在

IPv6利用の有無に関わらず対策が必要