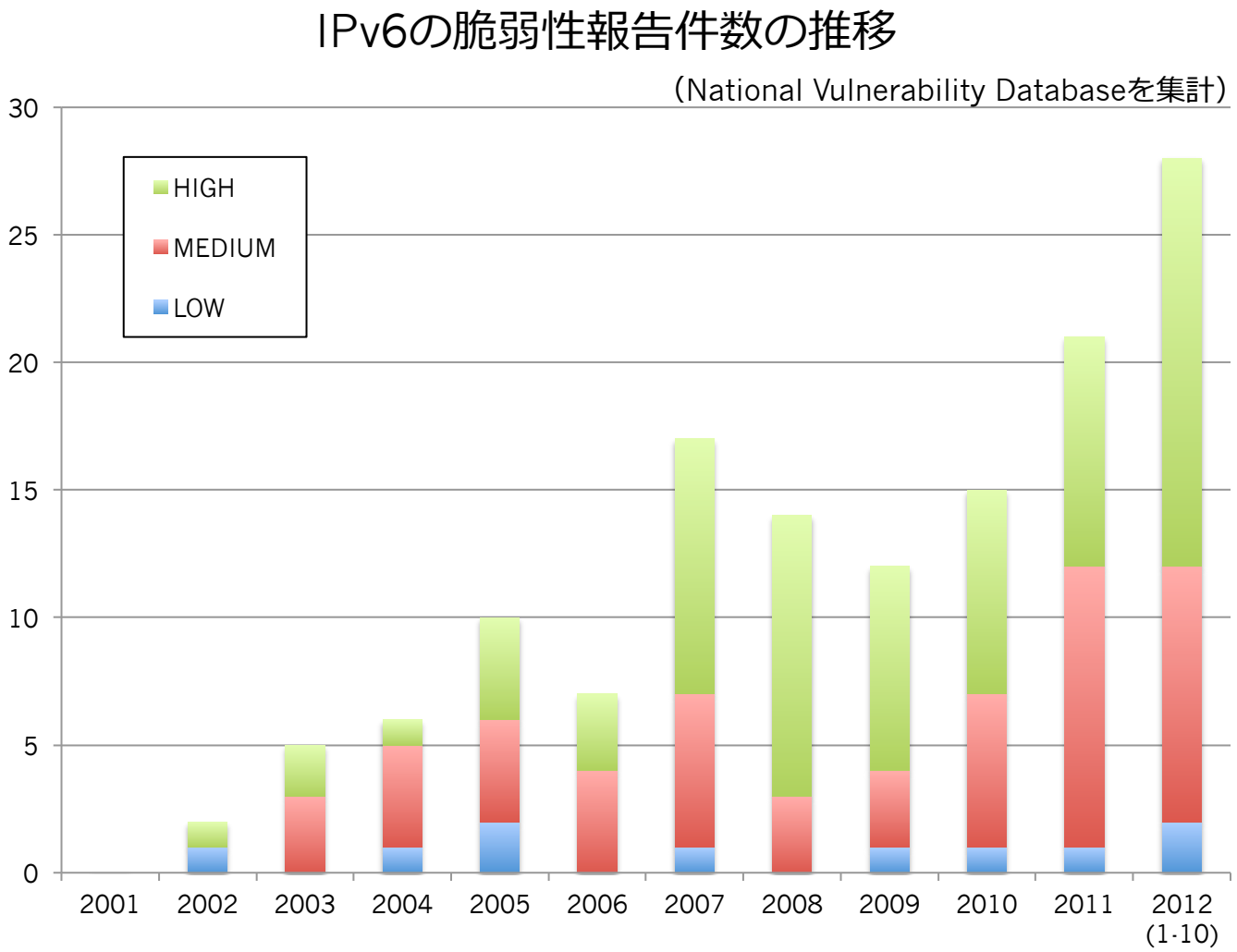
金沢大学
KANAZAWA UNIVERSITY

IPv6実践講座
～トラブルシューティング，セキュリティ対応からアプリケーション構築まで～
IPv6セキュリティ

IPv6とセキュリティ（概要）

金沢大学 総合メディア基盤センター
北口 善明

IPv6における脆弱性報告



脆弱性報告が増加傾向 → IPv6の本格導入の増加が原因が？

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

IPv6対応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

① IPv4から引き継いだ課題
② IPv6にて顕著になる課題
③ IPv6にて新たに登場する課題

実装上における課題

④ 仕様上の明示的でない処理の実装
⑤ 実装における検証が不十分な点

運用上における課題

⑥ デュアルスタック時の動作の理解
⑦ IPv6機能有効時の動作の理解

①仕様上の課題　～IPv4から引き継いだ課題～

金沢大学 KANAZAWA UNIVERSITY

- IPv6はIPv4の仕組みを（良くも悪くも）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
  - 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問題点と供に継承

近隣探索プロトコル：NDP

Neighbor Discovery Protocol

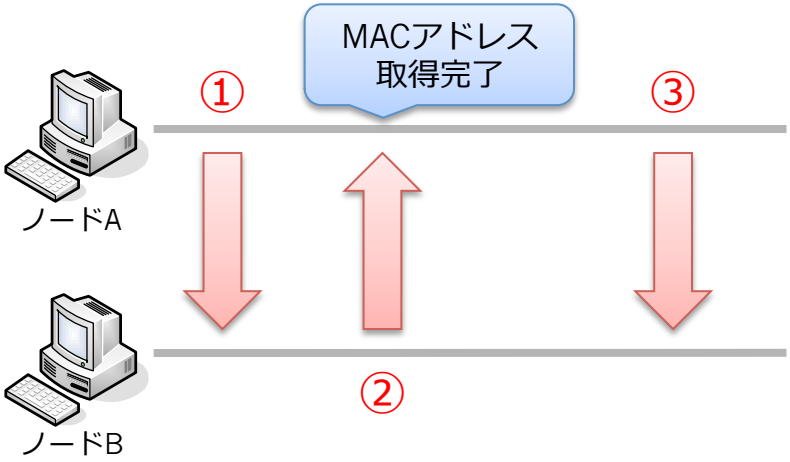
処理	機能	説明
リンクレイヤアドレスの解決（ARP相当）	近隣キャッシュ	IPアドレスとリンクレイヤアドレス（MACアドレス）対応を保持
	不到達検出機能	近隣キャッシュ内のリストを最新に保つ機能
自動アドレス設定（SLAAC）	重複アドレス検出機能（DAD）	設定IPアドレスの重複がないか検出する機能（RFC5227にてIPv4の仕様に逆輸入された）
	デフォルトルートの設定	ルータ広告の送信元IPアドレスを利用
	グローバルアドレスの生成	ルータ広告に含まれるプレフィックス情報を利用

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）

NDPの動作概要

リンクローカルアドレス解決の流れ

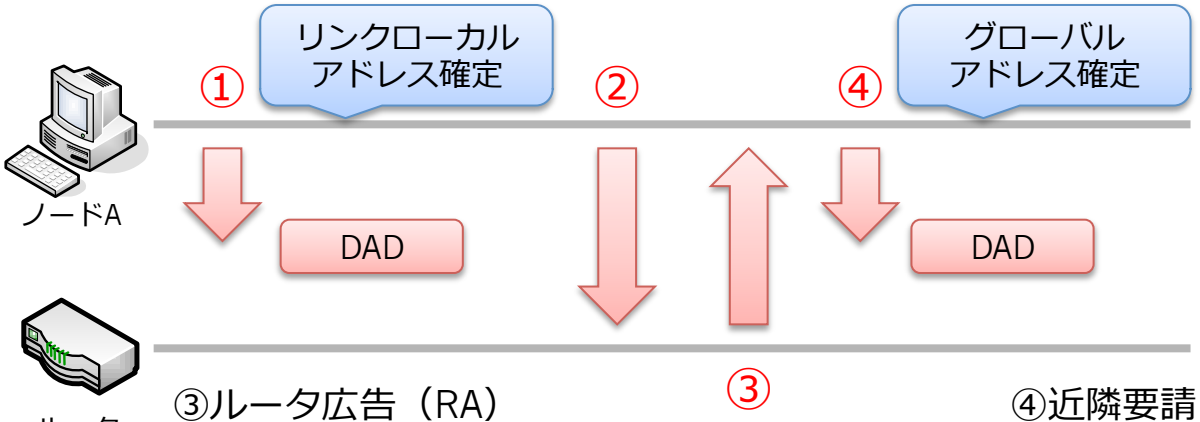


①近隣要請（NS）
通信相手のMACアドレスを探索
（宛先はマルチキャスト）
近隣広告がない場合はオンリンクでないと判断

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

自動アドレス設定（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

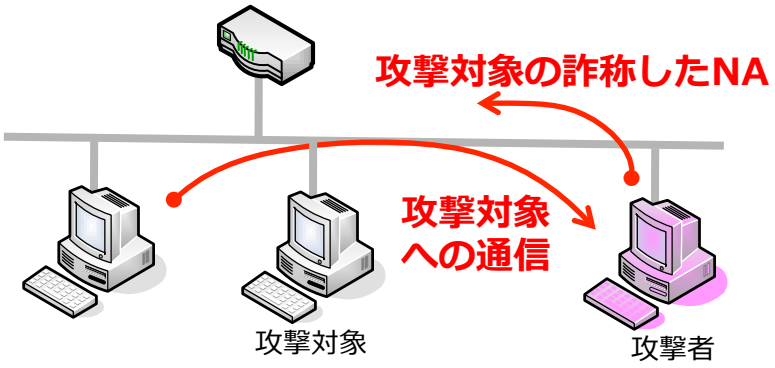
②ルータ要請（RS）
全ルータマルチキャスト
（ff02::2）宛に送信

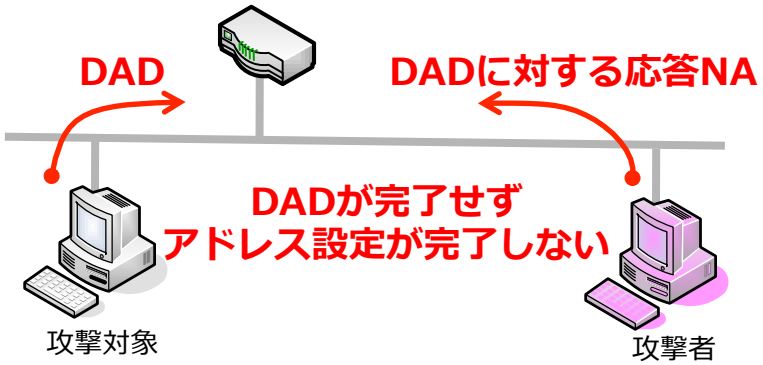
③ルータ広告（RA）
全ノードマルチキャス（ff02::1）宛に送信
取得プレフィックスからグローバルアドレス
を生成

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）

具体例(1)：NA詐称

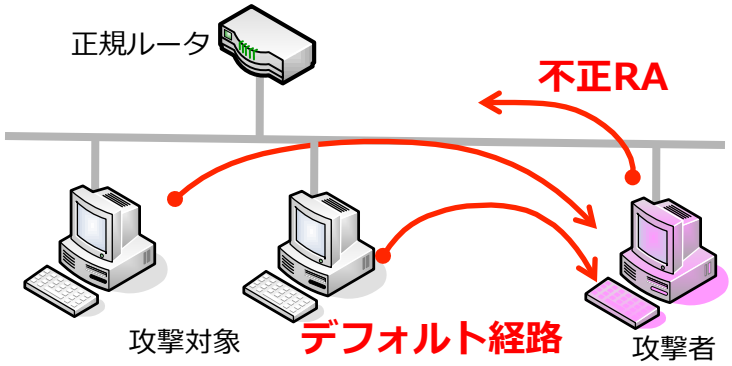
- 概要
  - 近隣広告（NA）の詐称により近隣キャッシュを汚染
    - ARPと異なり”override flag”の設定で強制的な変更可
  - 攻撃対象のIPアドレスへの通信を誘導可能
  - DADにおける応答を返すことでIPアドレス設定を妨害
- 想定される問題
  - IPv4のARPにおける問題と同様の脅威
  - 通信断、盗聴、サービス妨害、意図せぬ通信





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

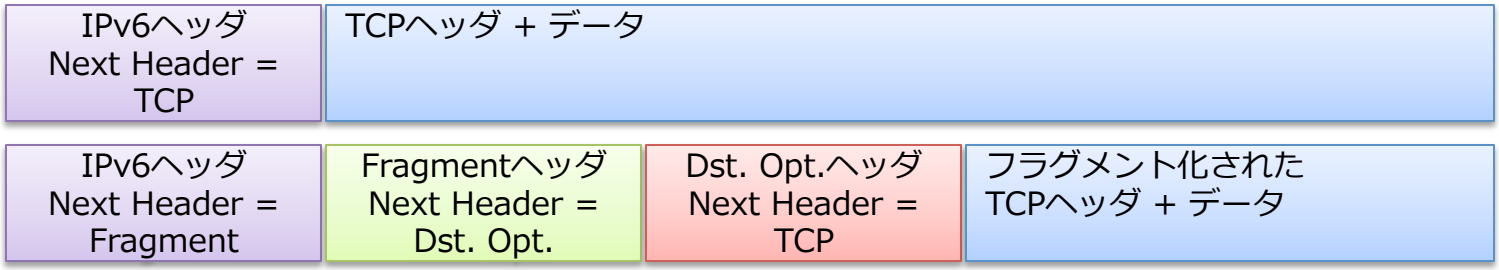


NA詐称や不正RAへの対策

- 双方に有効な対策
  - SEND（Secure Neighbor Discovery）の導入
    - 認証DoS攻撃の危険性は残る
  - NDPのモニタリング（NDPMonなど）
    - 攻撃の早期確認が可能
- NA詐称の対策
  - L2スイッチにおけるノード間通信を禁止する運用
- 不正RAの対策
  - L2スイッチによるRAのフィルタリング（RA-Guard）
    - 対応機器は現状ハイエンド機器が主流
  - Router Preference（RFC4191）の利用
    - 意図的なものは排除不能

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

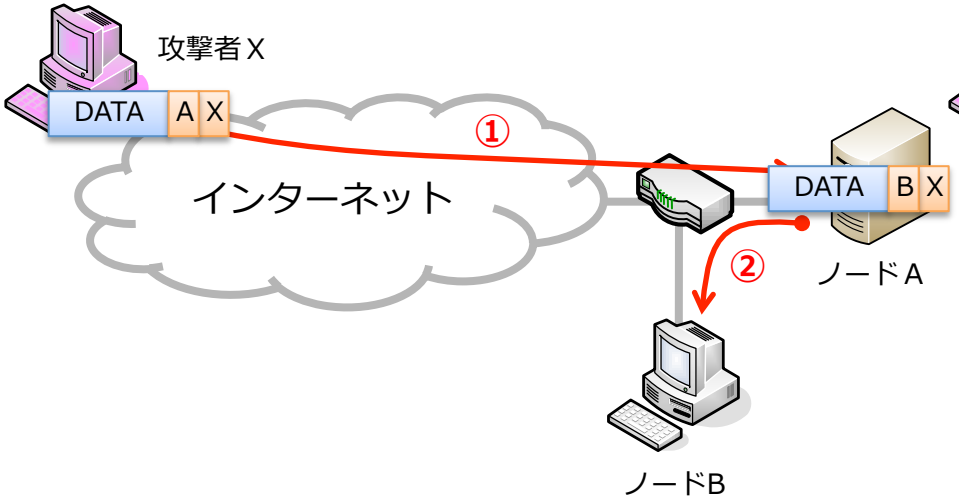


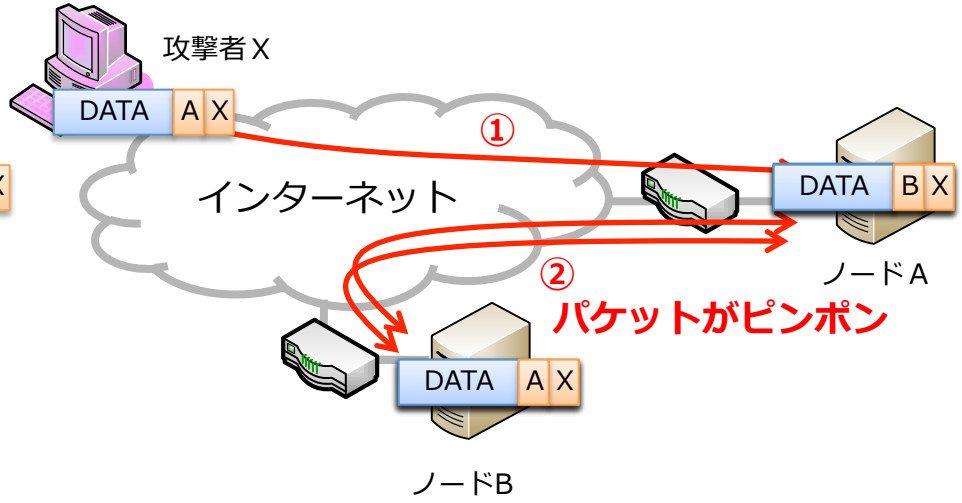
- 拡張ヘッダの種類

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 [RFC 5095]
44	Fragment header	パケット分割時に利用する
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
60	Destination Options header	エンドノードにて実行する内容を記述する
135	Mobility header [RFC 6275]	MIPv6におけるモバイルノードの情報交換で利用

具体例(3)：ソースルートオプション（RH0）

- 概要
  - タイプ0ルーティングヘッダ（RH0）を利用した攻撃
    - 現在は利用が禁止されている仕様
  - ソースルートオプションはIPv4においても問題あり
    - 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





RH0への対策

- RH0は仕様から削除（RFC5095）
  - 古い実装の場合注意が必要
  - モバイルIPではルーティングヘッダを用いるが新たにタイプ2が用意された
- 対外接続箇所におけるフィルタリング
  - 利用禁止と合わせて転送も禁止
  - FW機器でのルーティングヘッダのタイプ識別が必要

②仕様上の課題　～IPv6にて顕著になる課題～

金沢大学 KANAZAWA UNIVERSITY

- 多数のアドレスが利用できる点がIPv4と異なる
  - グローバルアドレス利用が基本となる
    - セキュリティ対策の重要性がIPv4と比較して増加
    - プライバシーの課題
  - 複数のインターフェースアドレスとマルチキャスト
    - IPv4と異なりI/Fに複数のアドレス設定が基本
    - マルチキャストとダイナミックVLANの課題
  - 利用アドレス量が増加する
    - 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

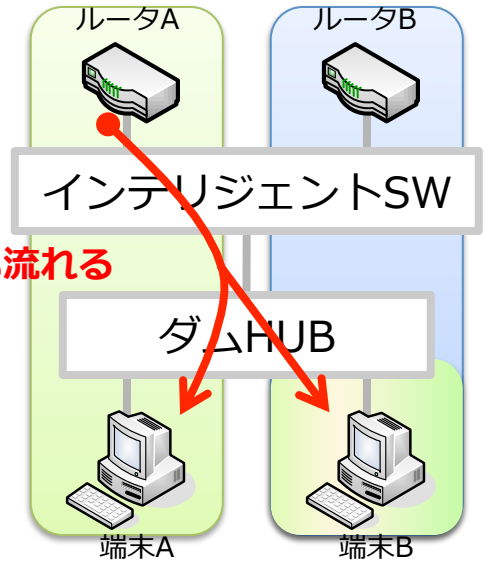
        ⇒ 実装上の課題

グローバルアドレスとNAT

- NATなしでセキュリティが低下？
  - 適切なフィルタリングでセキュリティは確保可能
  - NATの通信中は外部からの到達性がある
    NATでセキュリティ担保されている判断は誤り
- IPv6でNATは不要か？
  - マルチホーム環境などで有用性がある
- プライバシーに関する議論
  - 下位64ビットにMACアドレスを用いる仕様
    - ノードを一意に特定可能でプライバシー問題がある
  - 一時アドレスの仕様化で下位64ビットがランダム生成
    - 上位64ビットはISPで固定なので完全な解決には至っていない
    - 利用アドレス量の増加にもつながる

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化しなかった
    - 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



② マルチキャストとVLANへの対策

- 機器や構成による対策
  - L2製品であってもIPv6対応が必要
    - MACアドレス学習時にVLANポートにのみフラッドする実装
      - MACアドレスVLAN（ダイナミックVLAN）も同様
    - 単に全ポートにフラッドするのはそもそも正しい実装ではない
    - 実装上の課題と言える
  - ネットワーク構成をユニキャストのみにする
    - IPv6 over IPv4によるPtoP接続構成など
- IPv6の仕様の理解
  - IPv6では1ノード1IPアドレスが成り立たない
  - IPアドレスによる端末制御もIPv4と同様にはできない

② 利用アドレス量増加による課題

金沢大学 KANAZAWA UNIVERSITY

- 利点
  - アドレススキャンに強くなる
    - IPv4のようにアドレスを単純に総当たりするのは不可能
- 欠点（課題）
  - 管理上のスキャニングもできない
  - 攻撃者の潜伏が用意に
    - 一時アドレスなどを利用し攻撃元の特定を困難に
- 対策
  - NDPのモニタリングが重要

③仕様上の課題　～IPv6にて新たに登場する課題～

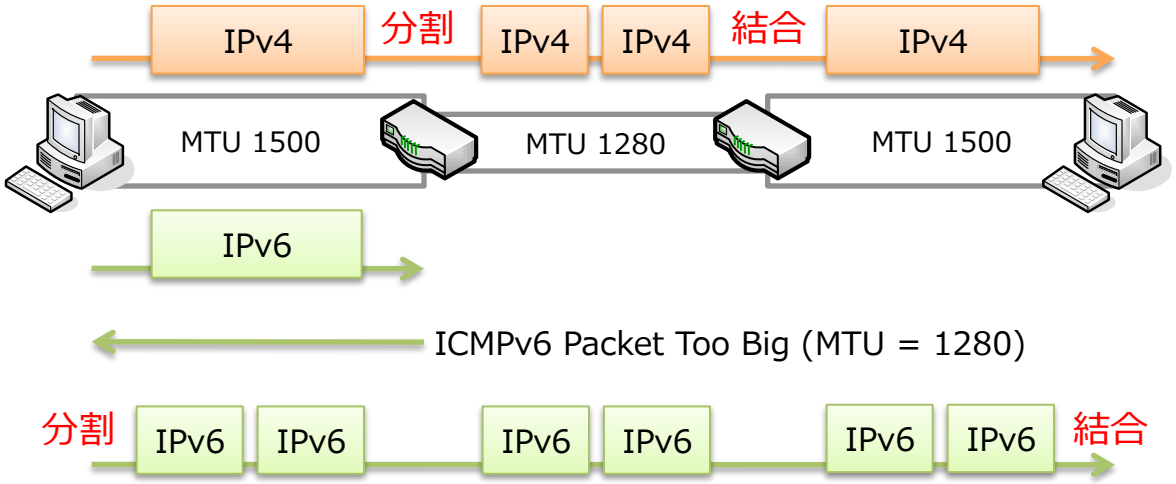
金沢大学 KANAZAWA UNIVERSITY

- 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
    - 多段に拡張ヘッダを挿入可能
  - フィルタリング実装がIPv4よりも複雑化

    ⇒ 実装上の課題につながる
- IPv4と仕様が異なる点の注意
  - 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

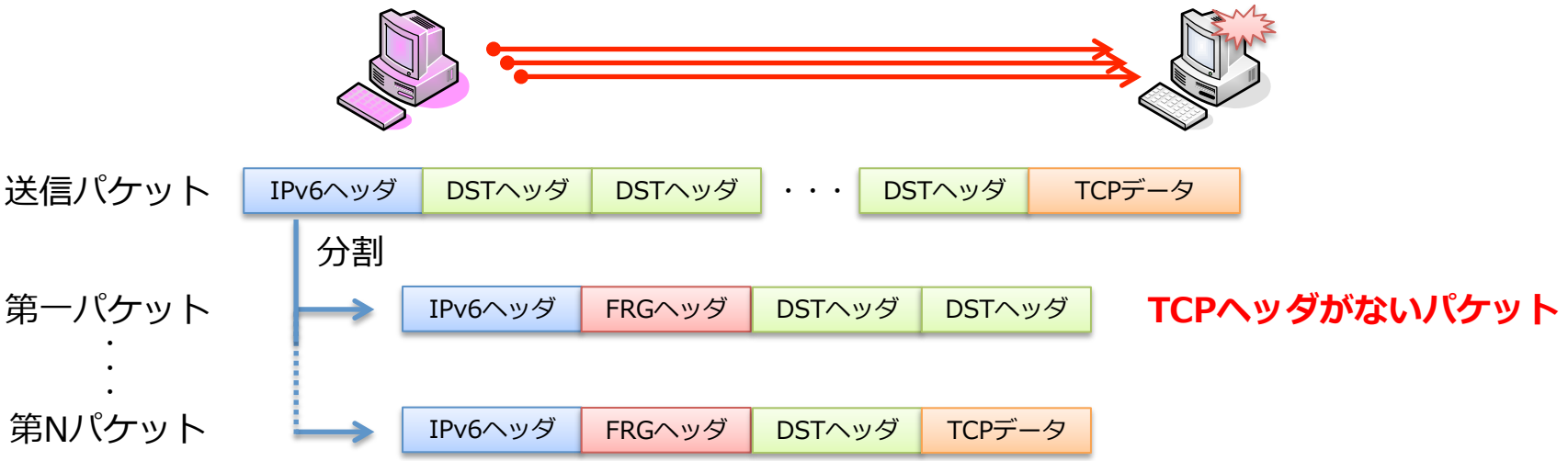
パケットフラグメント処理の違い

- 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



具体例(5)：細かいフラグメントパケット

- 概要
  - フラグメントサイズを小さくしTCPヘッダを持たない第一パケットを作成
  - 拡張ヘッダを利用することで比較的容易に実現
- 想定される問題
  - パケット再構成できない機器のアクセス制御回避
  - 処理負荷による動作不良



③ 細かいフラグメントパケットへの対策

- 仕様の修正および実装での対応
  - 最小パケットサイズを大きく設定（640バイトなど）
  - 利用可能な拡張ヘッダ数を制限
    - 多くの通信では拡張ヘッダは不要
- パケット再構成を必ず実施
  - IPv4にも存在する課題でありIPv4同様に対処が必要
  - 再構成用のバッファを確保する必要あり

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 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
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 3 （Time Exceed）	Code0がホップ数超過時に送られるものでエラー処理が必要
Type 4 （Parameter Probrem）	ネクストヘッダタイプ異常（Code1）とIPv6オプション異常（Code2）を受け取れないと障害解析ができない

自動アドレス設定手法の差異

- 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	（参考）DHCP
デフォルト経路	○	× (1)	○
アドレス	○ (2)	○	○
プレフィックス長	○	× (1)	○
サーバ情報（DNSなど）	○	○	○
ルータ優先度	○	× (1)	ー

(1) IETFにて仕様化の議論中
(2) プレフィックス情報からアドレスを生成

- （参考）OS毎の対応

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

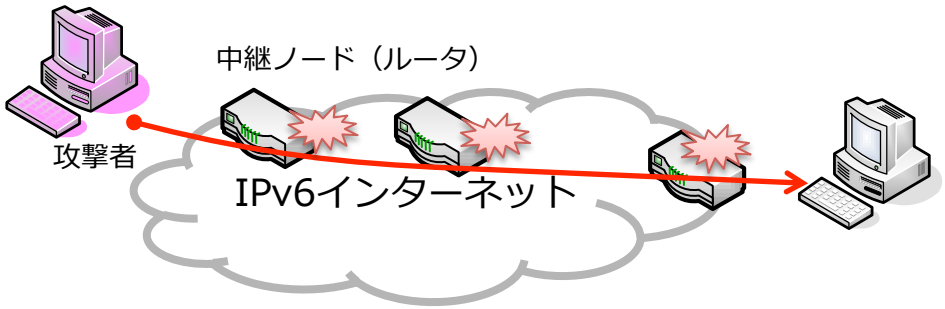
※ http://en.wikipedia.org/wiki/Comparison_of_IPv6_support_in_operating_systems より

④実装上の課題　～仕様上の明示的でない処理の実装～

- 拡張ヘッダ処理の課題
  - 拡張ヘッダの付加数に制限がない
  - オプションフィールド値が広大なものがある
- 同一セグメントにおける課題
  - 2^{64}もの広大な同一セグメント
  - 複数のプレフィックス、デフォルト経路
- 機器で扱うリソースの上限値は実装依存

具体例(6)：拡張ヘッダDoS攻撃

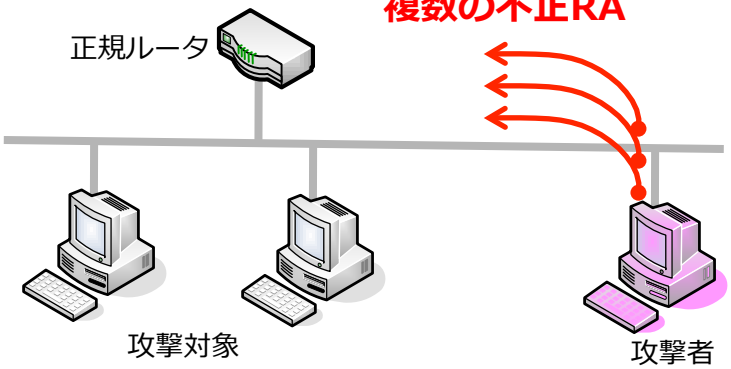
- 概要
  - ホップバイホップ・オプション ヘッダの悪用
    - 中継ノード（ルータ）にて唯一処理が必須な拡張ヘッダ
  - 多数の拡張ヘッダ利用による負荷
  - Jambo Payloadオプションで巨大な値を指定
- 想定される問題
  - ルータ過負荷による動作不良

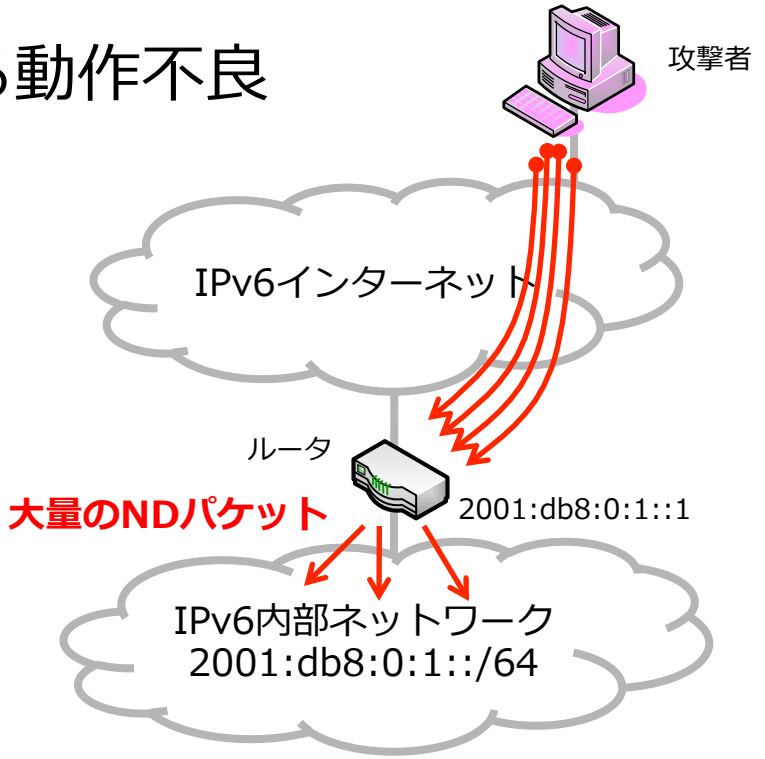


多数のホプバイホップ・オプション ヘッダを付加したパケット

具体例(7)：大量アドレスDoS攻撃

- 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





③ 拡張ヘッダ／大量アドレスDoS攻撃への対策

金沢大学 KANAZAWA UNIVERSITY

- 実装面での対策
  - 仕様上明確でない上限値を実装で必ず設定
    - 利用可能な拡張ヘッダ数、オプション値、NDPキャッシュ数、利用プレフィックス数、デフォルト経路数
    - 無制限にRAを受け付けず上限を実装において設ける
  - SYNフラッド攻撃対策と同様の処理を実装
    - DDoS攻撃となると難しい
- 現時点の端末OSの実装では
  - 利用プレフィックス数の上限があるものは限定的
    - Linux、Mac OS X 10.7など
  - 多数のプレフィックス設定で再起動が発生する実装も
    - 同一サブネット上の攻撃なので改修しない実装もある
    - 侵入をそもそも制御することで対処可能

⑤実装上の課題　～実装における検証が不十分な点～

- 不十分な実装の検証
  - 本格運用のためには実装の検証が必要
  - 検証⇒公開のスキームが今後必要

（参考）IPv6技術検証協議会からの最終報告書が公開されました

http://ipv6vc.jp/documents/20121023Report.pdf

- IPv6アドレス表記の課題
  - 省略法によりアドレスの誤判定が発生
  - 実装による表記の差異

IPv6アドレス表記法

IPv4のアドレス表記法

2進数表記（32ビット）

11000000 10101000 00000000 00000001

・8ビットに区切り10進数で表現　区切り文字はピリオド「.」

192.168.0.1

IPv6のアドレス表記法（省略法）

2進数表記（128ビット）

0010000000000001 0000110110111000 1011111011101111 1100101011111110
0000000000000000 0000000000000000 0000000000000000 0001001000110100

・**16ビット**に区切り**16進数**で表現　区切り文字は**コロン**「**:**」

2001:0db8:beef:cafe:0000:0000:0000:1234

・省略表記①：各ブロックの先頭の連続する「0」は省略可能

2001:db8:beef:cafe:0:0:0:1234

・省略表記②：連続した「0」は1回に限り「::」に省略可能

2001:db8:beef:cafe::1234

IPv6アドレス表記のゆれによる課題

- 柔軟な表記が可能なIPv6アドレス

◆省略形やアルファベットの大文字/小文字など複数の表記が可能
＜同じアドレスの例＞

① 2001:db8:0:0:1:0:0:1	::による省略がなくてもよい
② 2001:0db8:0:0:1:0:0:1	頭の0の省略があってもなくてもよい
③ 2001:db8::1:0:0:1 2001:db8:0:0:1::1	同じ長さの0なのでどちらの表記も可
④ 2001:db8::0:1:0:0:1	1ブロックだけを::に省略してもよい
⑤ 2001:DB8:0:0:1::1	アルファベットは大文字／小文字が可

  - 正規化しないとアドレスの差異を誤判定
  - RFC5952にて省略表記ルールが明確に
    - ②と④はNG、③は前半省略、⑤は小文字利用
    - 古い実装に注意が必要
- 運用面からの要求
  - 非省略表記と省略表記を設定で指定できる実装

⑥運用上の課題　～デュアルスタック時の動作～

金沢大学 KANAZAWA UNIVERSITY

- IPv6優先利用の理解
  - 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ため動作の理解が必要
    - TCPフォールバック時の動作
    - アドレス選択機構の実装の差異
- DNSの挙動の理解
  - 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

TCPフォールバックの課題

- TCPフォールバック
  - IPv6通信が確立できない場合にIPv4通信へ移行
- 実装による差異が大きい
  - 通信試行回数が実装により異なる
  - TCPフォールバックを実施しない実装もある
- 課題
  - 挙動が実装により異なるためデバッグが困難
  - 通信できる端末とできない端末が存在
- 対策
  - 各実装の改善が進んでいる
  - 挙動の確認が必要
    - http://test-ipv6.jp/などで挙動確認が可能

アドレス選択機構（RFC3484）の課題

- IPv6では複数のアドレスを使い分ける必要がある
  - リンクローカルアドレスとグローバルアドレス
  - IPv4アドレスとIPv6アドレス　など
- ポリシーテーブル
  - アドレス選択時に利用するラベルや優先度を定義
  - 優先度：終点アドレス選択時に利用、高い値ほど優先
  - ラベル：始点/終点アドレス選択時に利用、一致するものを優先
- 課題点
  - RFC3484の後に追加された仕様に非対応
    - ULAやTeredoアドレスの優先度が実装依存
  - longest matching rule（Rule 9）の弊害
    - 現在の仕様ではロードバランスなどが機能しない
    - 同じプレフィックスの負荷分散で片方のアドレスに偏る

新しいアドレス選択機構（RFC6724）

- デフォルトポリシテーブルの変更
  - ULAやTeredoアドレス、利用不可アドレスの明示的な追加
  - 6to4アドレスやIPv4アドレスの優先度変更

Prefix	Precedence	Label
::1/128	50	0
::/0	40	1
2002::/16	30	2
::/96	20	3
::ffff:0:0/96	10	4

Prefix	Precedence	Label	
::1/128	50	0	
::/0	40	1	
::ffff:0:0/96	35	4	IPv4アドレス
2002::/16	30	2	
2001::/32	5	5	Teredoアドレス
fc00::/7	3	13	ULA
::/96	1	3	IPv4互換アドレス
fec0::/10	1	11	サイトローカルアドレス
3ffe::/16	1	12	6boneアドレス

- ルールの変更
  - DNSラウンドロビン利用のためRule 9を変更
    - プレフィックス部分までを評価
  - 複数の出口とプレフィックス対応のためのRule 5.5を追加
    - ネクストホップと広告アドレスの一致を優先
  - IPv4プライベートアドレスをグローバルスコープに（Rule 2）
    - 6to4よりもIPv4通信を優先させるため
  - プライバシ対応のため一時アドレスを優先にRule 7を変更

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（現在の主流）
    - 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運用上の課題　～IPv6機能有効時の動作～

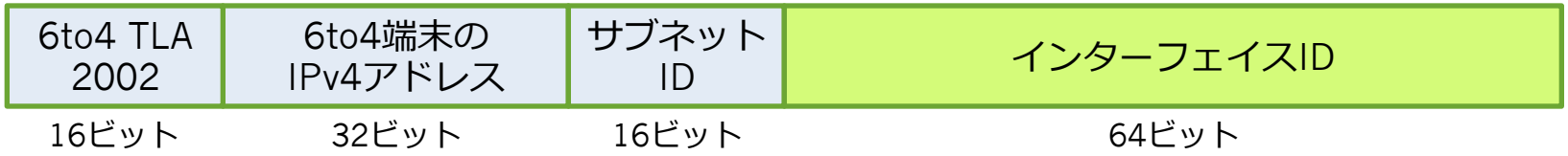
金沢大学 KANAZAWA UNIVERSITY

- 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ネットワーク上のIPv6対応機器の存在
  - RAなどでIPv6アドレスが付与されれば通信を実施
  - IPv6通信が優先されるため問題
  - IPv6対策のないIPv4ネットワークが最も危険

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

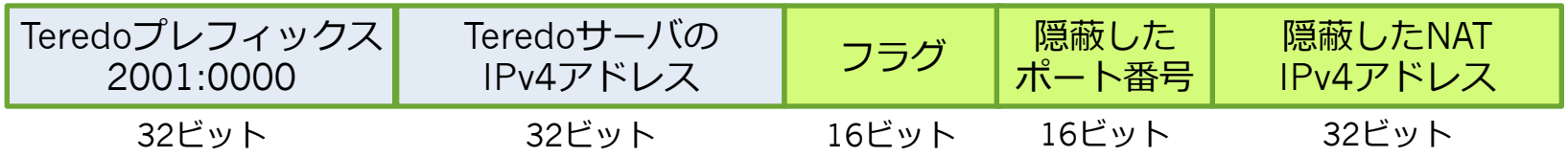
◆6to4のアドレス形式



・/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

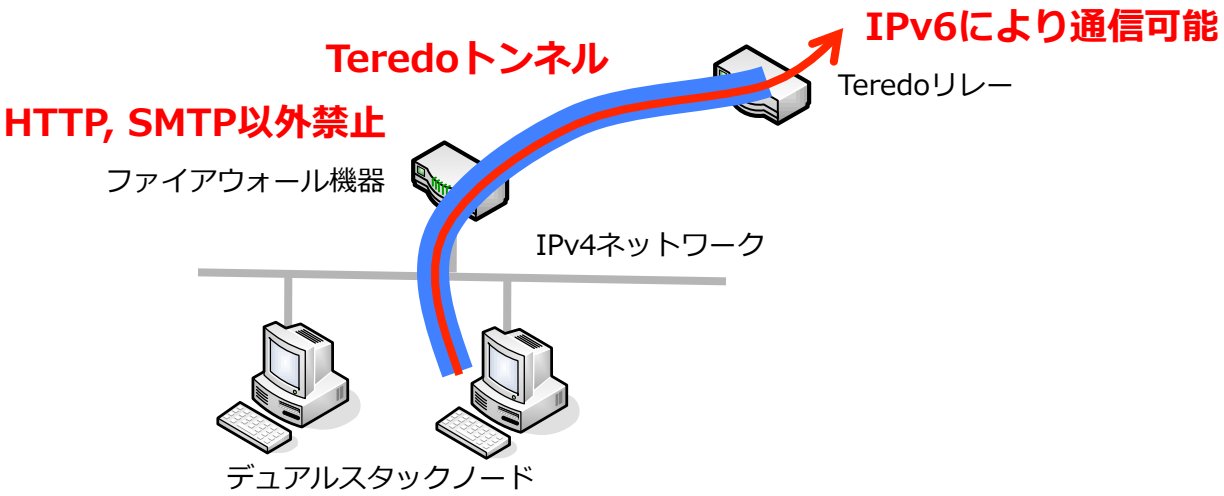
◆Teredoのアドレス形式



・/128のアドレスが一つ割り当てられる

具体例(8)：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
  - バックドアの危険、通信傍受
  - 不正RAによる影響も受ける



⑦ 意図しないIPv6通信への対策

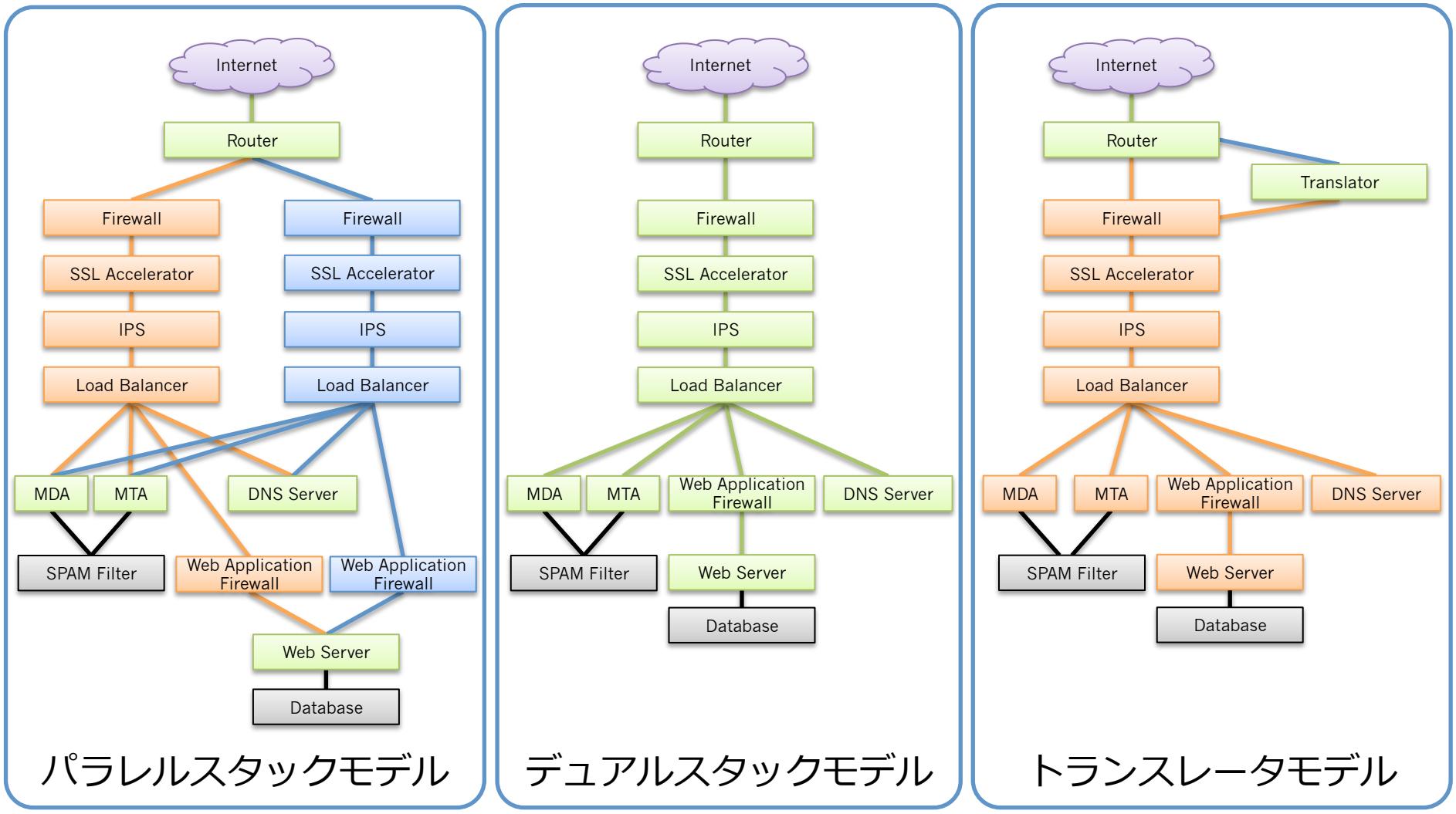
金沢大学 KANAZAWA UNIVERSITY

- 対策
  - Teredoを禁止するルールを追加
    - 3544/udpのフィルタ
  - IPv6通信のモニタリング
- 認識と理解
  - IPv4のみでもデュアルスタック端末の存在認識が重要
  - 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
    - 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（Windows Vista/7）
    - 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）

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
- DMZにおける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

3つの導入モデルの比較（DMZの例）



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

まとめ

- 仕様面
  - IPv4と同様である同一リンク上の脆弱性
  - 情報の追加が可能である点で脅威が増す
    - ただしオンリンクに侵入された場合に限定的
  - IPv6導入に関してセグメントの構成確認が必要
- 実装面
  - 仕様上明確でない上限値の実装が重要
  - 可用性を損なわない制限に関して議論が必要
- 運用面
  - IPv6対応機器が多く存在してることの認識が重要
  - デュアルスタックにおける挙動の理解が必要
  - IPv4ネットワークでのIPv6通信監視が必須