金沢大学
KANAZAWA UNIVERSITY

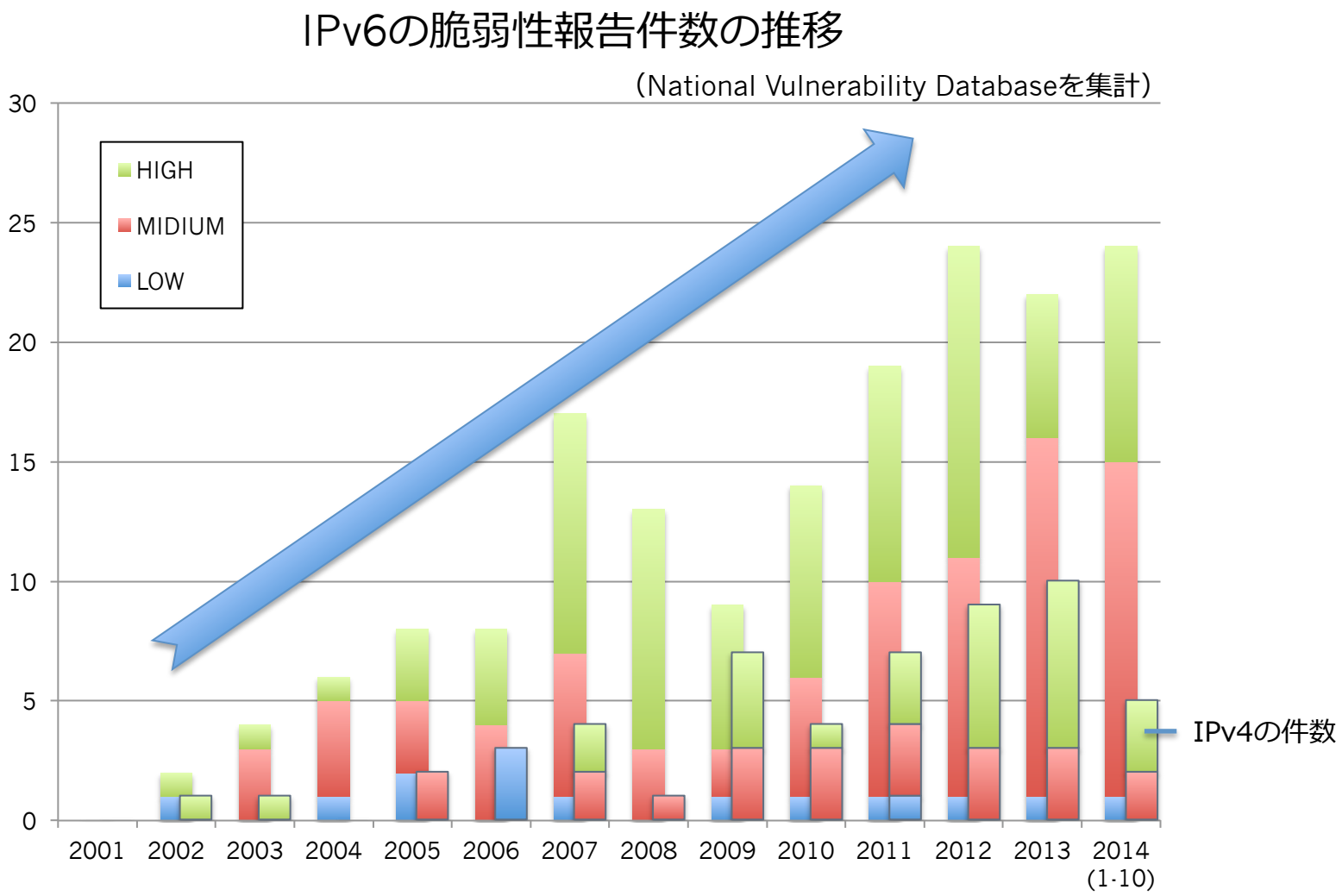
T3 必修！IPv6セキュリティ

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

November 19, 2014

IPv6における脆弱性報告



脆弱性報告が増加傾向から横ばい傾向に（報告件数は多い）

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

IPv6の仕様に因るセキュリティ課題

① 仕様が変更され解決した課題
② 実装面で注意が必要な課題
③ 運用面での対策が必要な課題

デュアルスタック運用における観点

④ IPv4仕様との違いの理解
⑤ IPv6機能有効時の動作の理解

IPv6対応時のセキュリティ観点の整理

金沢大学 KANAZAWA UNIVERSITY

IPv6の仕様に因るセキュリティ課題

① 仕様が変更され解決した課題

② • ソースルートオプション（RH0）

③ • IPv6アドレス短縮表記のゆれ
• 不正RAとNDPフラグメント

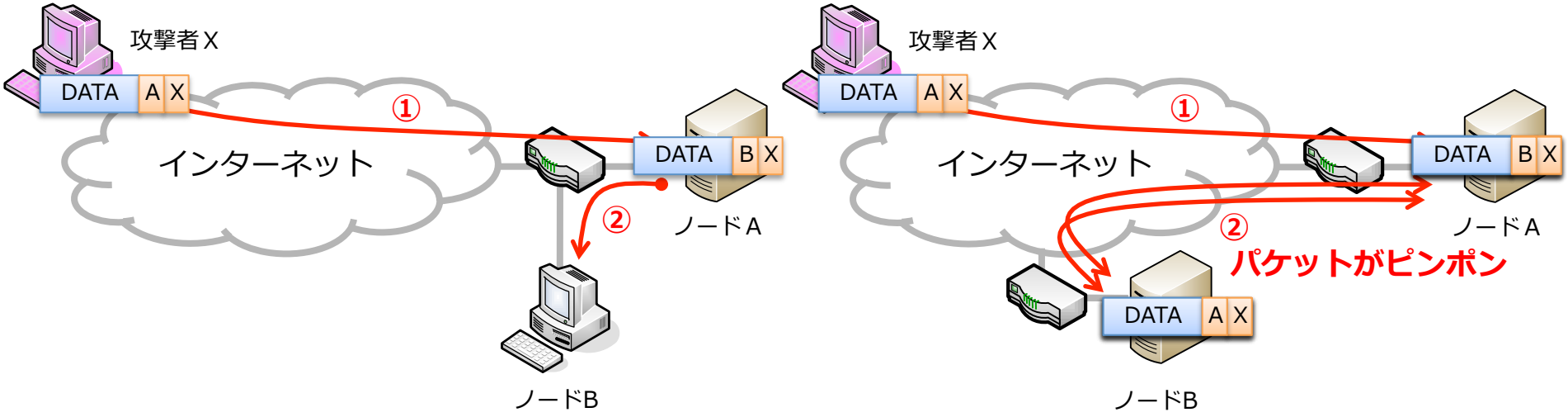
デュアルスタック運用における観点

④ IPv4仕様との違いの理解

⑤ IPv6機能有効時の動作の理解

ソースルートオプション（RH0）の課題

- 概要
  - タイプ0ルーティングヘッダ（RH0）を利用した攻撃
  - 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フィルタリング回避
  - 指定する二台のノード間でのパケット増幅攻撃



RH0問題の対策

- RH0は非推奨扱いに（**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

    ※すべてのルーティングヘッダが禁止ではない
- 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

（参考）主な定義済みルーティングヘッダのタイプ

Routing Type	説明
0	ソースルーティングで利用（非推奨） [RFC2460][RFC5095]
1	Nimrod routing system用（非推奨）
2	MIPv6で利用（中継ノードは1つだけ指定可能） [RFC6275]
3	RPL（Routing Protocol for Low-Power and Lossy Networks）で利用するソースルーティング用 [RFC6554]

IPv6アドレス表記法のおさらい

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」は省略してもよい

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

・省略表記②：連続した「0」は1回に限り「::」に省略してもよい

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アドレスに課題

◆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

近隣探索プロトコル：NDPのおさらい

Neighbor Discovery Protocol

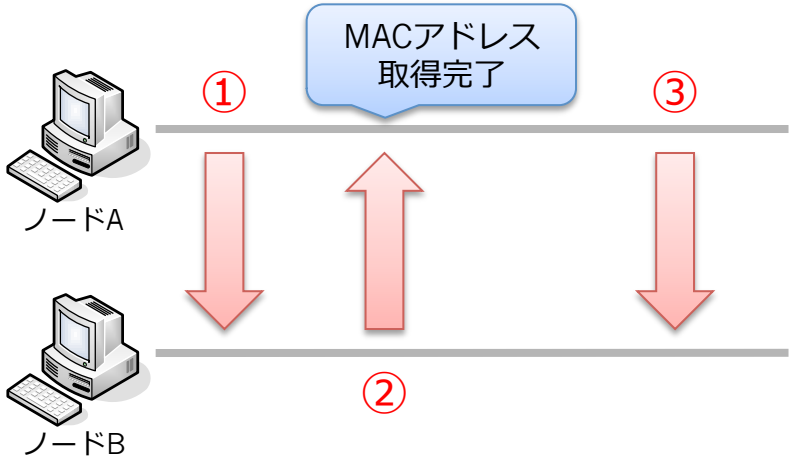
処理	機能	説明
リンクレイヤアドレスの解決（ARP相当）	近隣キャッシュ	IPアドレスとリンクレイヤアドレス（MACアドレス）対応を保持
	不到達検出機能	近隣キャッシュ内のリストを最新に保つ機能
自動アドレス設定（SLAAC）	重複アドレス検出機能（DAD）	設定IPアドレスの重複がないか検出する機能（RFC5227にてIPv4の仕様に逆輸入された）
	デフォルトルートの設定	ルータ広告の送信元IPアドレスを利用
	グローバルアドレスの生成	ルータ広告に含まれるプレフィックス情報を利用

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

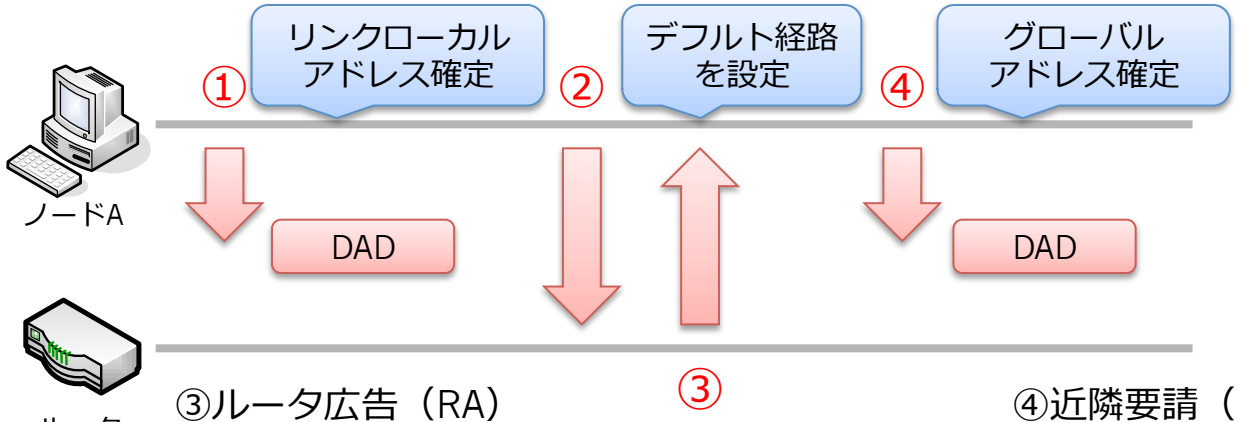


①近隣要請（NS）
通信相手のMACアドレスを探索
（宛先はマルチキャスト）
近隣広告がない場合はオンリンクでないと判断

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

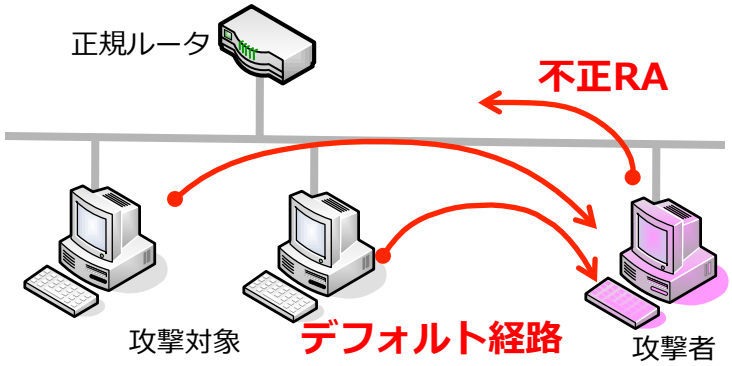
②ルータ要請（RS）
全ルータマルチキャスト
（ff02::2）宛に送信

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）

不正RAによる課題

- 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



不正RAからサブネットを守る方法（1）

- 認証技術による防御
  - SEND（SEcure Neighbor Discovery）の導入
    - NDPが認証機能を持つので詐称が困難に
    - 証明書DoS攻撃の危険性は残る
      - 証明書検証はノードに取って重い処理
    - 実装が少ない点や全てのノードに設定が必要な点も課題
  - IEEE802.1X認証の利用
    - 攻撃者をサブネットに接続させない発想
    - 運用ミスでルータ広告が流れる可能性あり

不正RAからサブネットを守る方法（2）

- 運用における対策
  - NDPのモニタリング（NDPMonなど）
    - 攻撃の早期確認が可能
  - Router Preference（**RFC4191**）の利用
    - 正規ルータの優先度を”high”に設定
    - 意図的なもの（攻撃）は排除不能
  - パーソナルファイアウォールの利用
    - 正規ルータのアドレスからのみルータ広告を許可
    - 全てのノードに設定が必要な点が課題
  - 不正RAの浄化（rafixdなど）
    - 不正RAと同じRAを「Router Lifetime=0」で広告
    - 不正RAによるノードの学習をリセット

最低限必要な対策

最低限必要な対策

不正RAからサブネットを守る方法（3）

- L2スイッチによる防御
  - RA-Guard（**RFC6105**）機能の利用
    - 対応機器は現状ハイエンド機器が主流
  - フラグメント利用によるRA-Guard回避問題
    - L2スイッチにてパケット再構成が必要で問題
  - フラグメント化されたNDPパケットの破棄が必要に
    ⇒**RFC6980**にて仕様化
    RFC6980実装の機器＋RA-Guard機能で防御可能

完全抑制可能な対策

IPv6対応時のセキュリティ観点の整理

金沢大学 KANAZAWA UNIVERSITY

IPv6の仕様に因るセキュリティ課題

① 仕様が変更され解決した課題

② 実装面で注意が必要な課題

③
- 拡張ヘッダDoS攻撃
- 大量アドレスDoS攻撃
- フラグメント処理

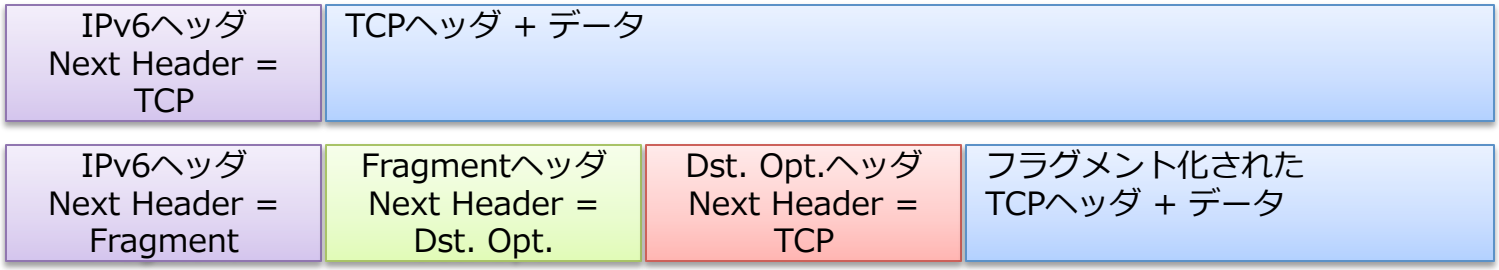
デュアルスタック運用における観点

④ IPv4仕様との違いの理解

⑤ IPv6機能有効時の動作の理解

IPv6拡張ヘッダのおさらい

- 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

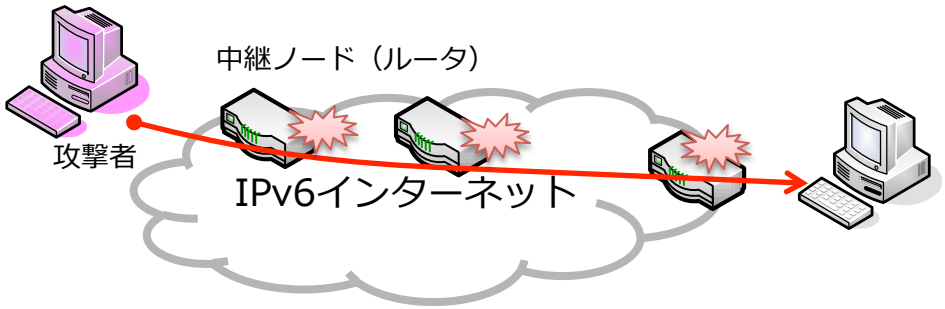


- 拡張ヘッダの種類

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は廃止 [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
140	Shim6 Protocol [RFC 5533]	Shim6で利用される

拡張ヘッダDoS攻撃の課題

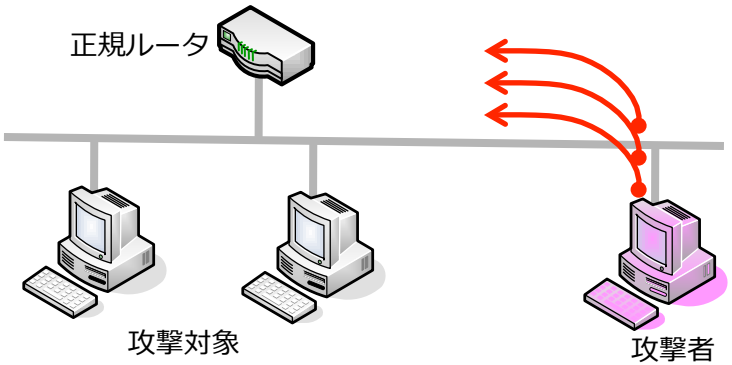
- 概要
  - ホップバイホップ・オプション ヘッダの悪用
    - 中継ノード（ルータ）にて唯一処理が必須な拡張ヘッダ
    - Jambo Payloadオプションで巨大な値を指定
  - 多数の拡張ヘッダ利用による負荷
    - ファイアウォール機器など走査を必要とする機器が影響
- 想定される問題
  - ルータやファイアウォールの過負荷による動作不良



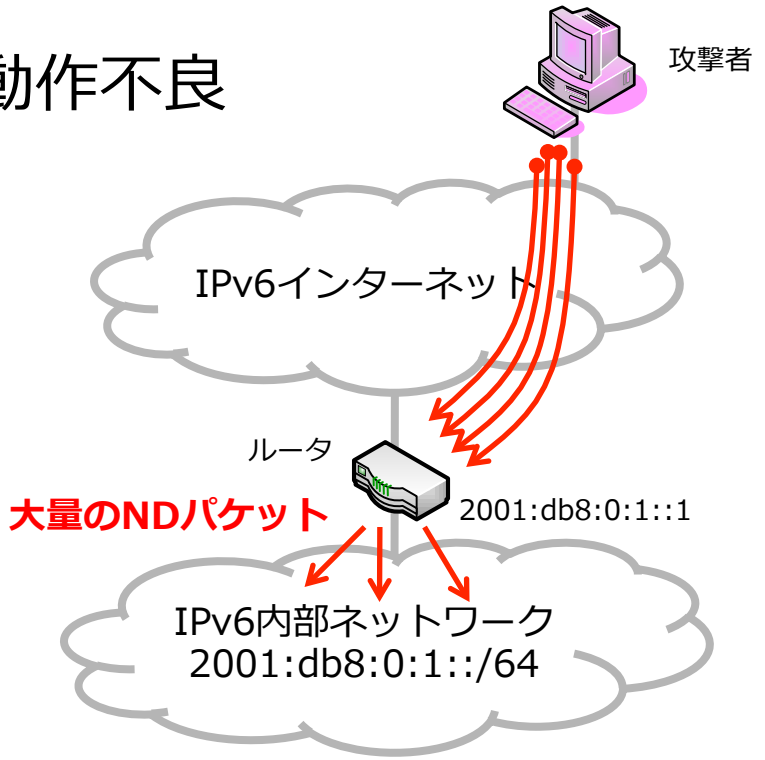
多数のホプバイホップ・オプション ヘッダを付加したパケット

大量アドレスDoS攻撃の課題

- 概要
  - アドレスの異なる大量の通信（近隣キャッシュの肥大）
    - セグメント内のノード許容数は/64だと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



①近隣キャッシュの肥大化
②多数のアドレス／デフォルト経路



② 拡張ヘッダ／大量アドレスDoS攻撃への対策

金沢大学 KANAZAWA UNIVERSITY

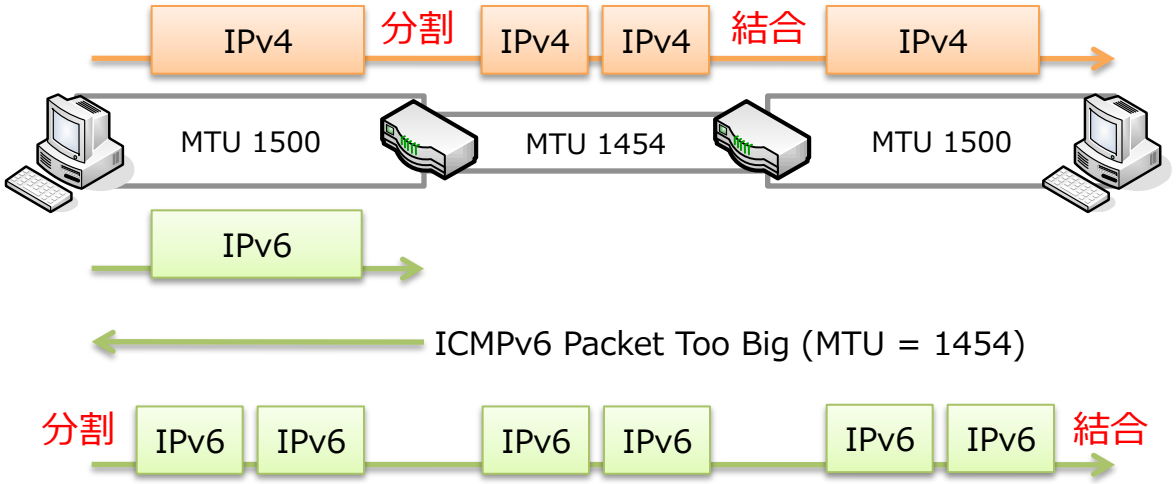
- 実装面での対策
  - 仕様上明確でない上限値を実装で設ける
    - 利用可能な拡張ヘッダ数、オプション値、近隣キャッシュ数、利用プレフィックス数、デフォルト経路数
  - スキャンにはSYNフラッド攻撃対策同様の処理を実装
    - DDoS攻撃となると難しい
  - 現時点の端末OSの実装では
    - 利用プレフィックス数の上限があるものは限定的
      - Linux、Mac OS Xなど
    - 多数のプレフィックス設定で再起動が発生する実装も
    - 同一サブネット上の攻撃なので改修しない実装もある
- 運用面での対策
  - サブネットサイズを小さくした運用（/120 など）
    - SLAACは利用できなくなる

② 拡張ヘッダに関する議論

- 未知の拡張ヘッダ
  - フォーマットが規定（**RFC6564**）
  - TLV形式に
- 拡張ヘッダ仕様の更新
  - 拡張ヘッダ処理に関する整理：**RFC7045**
    - 中間転送ノード（FW機器など）での制限事項を明記
      - デフォルト設定で標準拡張ヘッダは許可するべき
      - 実験的な拡張ヘッダを扱える必要あり
      - ルーティングヘッダもTypeにより許可されるべき
  - 拡張ヘッダチェーンのフラグメント禁止：**RFC7112**
    - 第一フラグメントが全ての拡張ヘッダを持つことが必須に
    - 再構成不要でパケット検査が可能

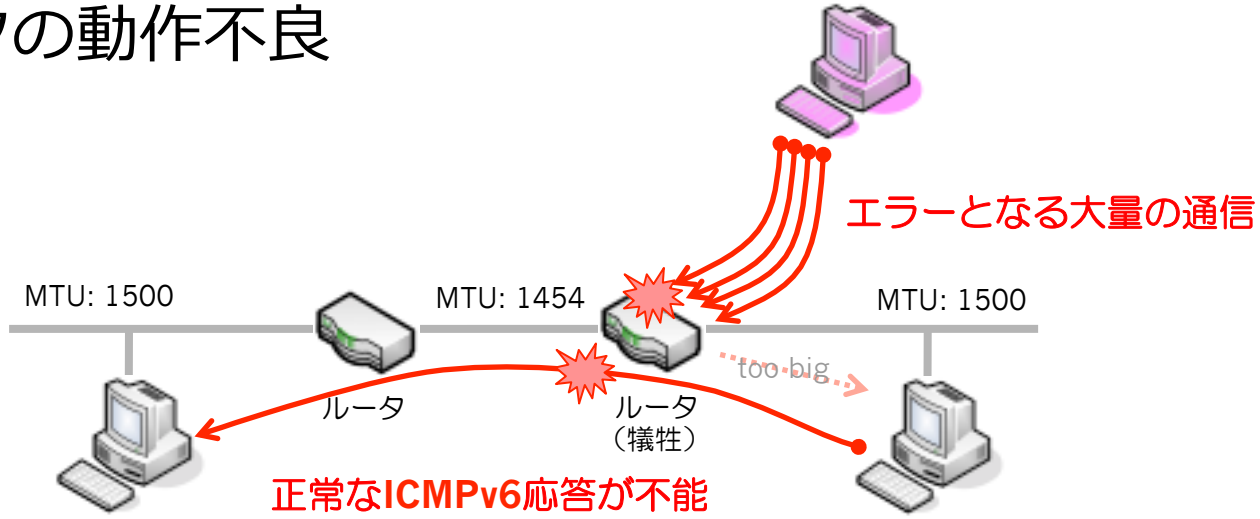
パケットフラグメント処理の違い

- 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



ルータにおけるICMPv6処理の必須化と課題

- 概要
  - PMTUDでIPv6ルータはICMPv6処理が必須
    - MTUより大きなパケットに対してPacket too bigを返答
  - パラメータ異常となるパケットをルータ宛てに多数送信することで正常な通信を阻害するDoS攻撃が可能
- 想定される問題
  - ルータのICMPv6処理不能による通信障害
  - ルータの動作不良



② 不完全なフラグメントパケットによる問題

金沢大学 KANAZAWA UNIVERSITY

- 概要
  - 第一フラグメントパケットのみを大量に送信
    - パケットの再構成処理に必要なリソースを無駄に消費
  - 原子フラグメント（atomic fragment）処理が未定義で実装依存
    - 実装によってはパケット再構成ができない
    - 原子フラグメント: fragment offset値とMフラグの値が共に”0”となる単一のフラグメントパケット
- 想定される問題
  - フラグメント再構成における動作不良
  - 機器のリソース消費による動作不良

② フラグメント関連の課題における対策

- 実装面における対策
  - パラメータ異常処理とPMTUD処理を分離する実装
    - 有効な対策は存在しないため実装での工夫が必要
  - フラグメントパケットを再構成するまでに保持する時間の調整が機器のリソースに合わせて必要
    - DoS攻撃の判断ができるかが鍵
  - 原子フラグメントを受け取った場合にも再構成処理を
    - **RFC6946**で明確に定義された
- フラグメントに関する議論
  - IPv6でフラグメント機能を廃止する案が浮上
    - draft-bonica-6man-frag-deprecate
    - 今年に入ってから議論はなく進展なし

IPv6対応時のセキュリティ観点の整理

IPv6の仕様に因るセキュリティ課題

① 仕様が変更され解決した課題
② 実装面で注意が必要な課題
③ 運用面での対策が必要な課題

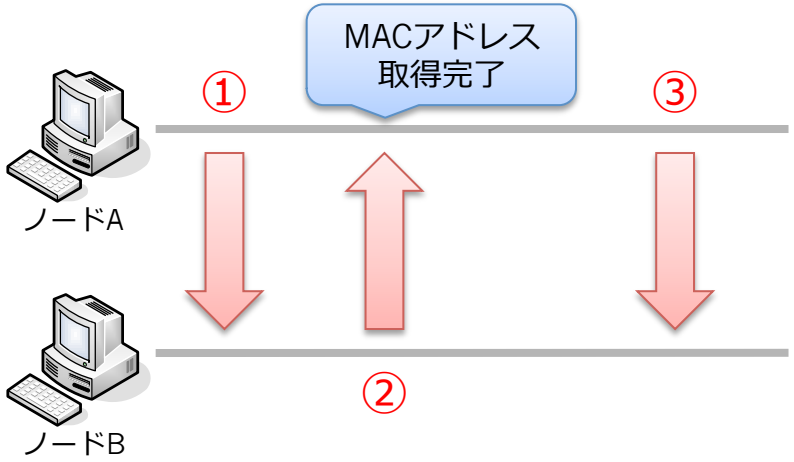
- NA詐称
- マルチキャストとVLAN
- グローバルアドレスの利用

デュアルスタック運用における観点

④ IPv4仕様との違いの理解
⑤ IPv6機能有効時の動作の理解

NDPの動作概要（再掲）

リンクローカルアドレス解決の流れ

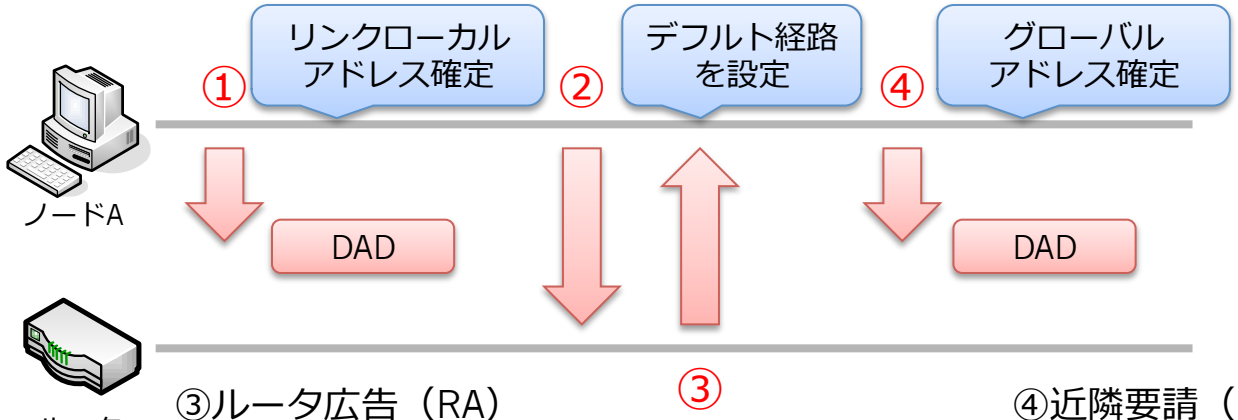


①近隣要請（NS）
通信相手のMACアドレスを探索
（宛先はマルチキャスト）
近隣広告がない場合はオンリンクでないと判断

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

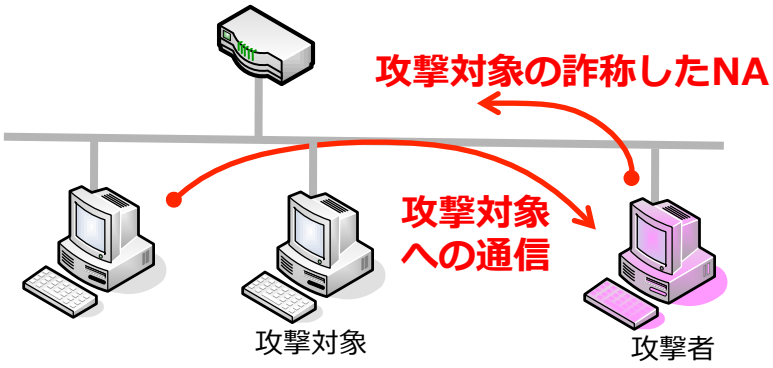
②ルータ要請（RS）
全ルータマルチキャスト
（ff02::2）宛に送信

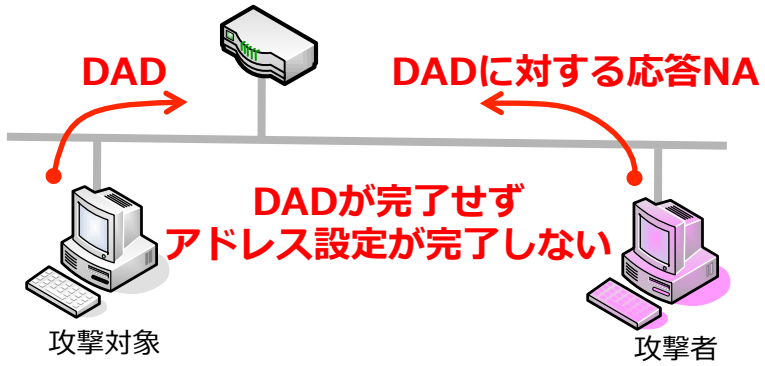
③ルータ広告（RA）
全ノードマルチキャス（ff02::1）宛に送信
取得プレフィックスからグローバルアドレス
を生成

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）

NA詐称による課題

- 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





③NA詐称からサブネットを守る方法

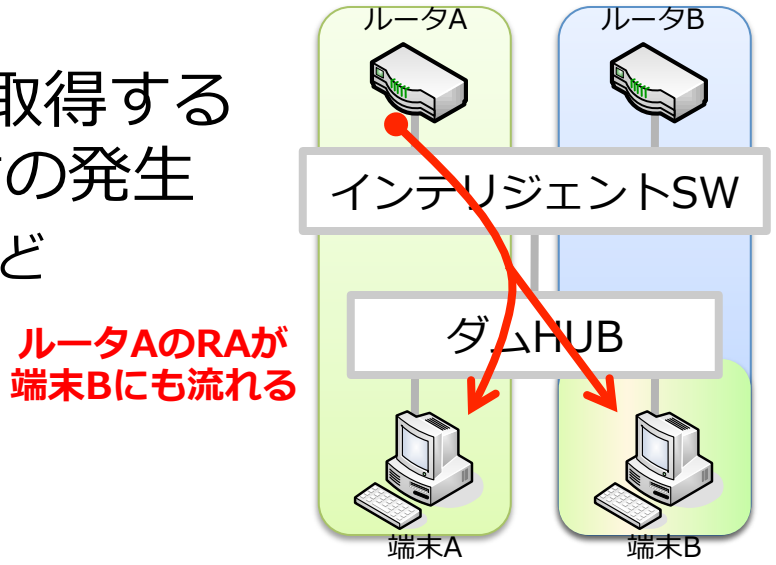
- 認証技術による防御
  - SEND（SEcure Neighbor Discovery）の導入
  - IEEE802.1X認証の利用
- 運用における対策
  - NDPのモニタリング（NDPMonなど）
  - L2スイッチにおけるノード間通信を禁止する運用
    - ルータが全てのリンクレイヤ内通信を中継
  - L2スイッチのポートに複数ノードを接続しない運用
    - MACアドレスが頻繁に異なるポートを遮断

※不正RAほど深刻な問題ではない

⇒L2スイッチでの対策は費用対効果が見合わない

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
    - マルチキャストを全ポートに流す実装で問題
  - 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



マルチキャストとVLANへの対策

- 機器や構成による対策
  - L2スイッチもIPv6利用で問題が出ないものを選択
    - 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
    - 運用負荷が大きい課題
- 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

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？
  - マルチプレフィックス環境などで有用性あり
    - NPTv6（RFC6296）によるステートレス変換
- プライバシーとセキュリティに関する議論
  - IID※にMACアドレスを用いる仕様 ※IID（Interface ID）：下位64ビット部分
    - ノードを一意に特定可能でプライバシー問題がある
    - MACアドレスによる特定機器を狙った攻撃が可能との指摘
  - 対策
    - 一次アドレス（RFC4941）にてIIDのランダム生成
    - 新たな固定IID生成方法（RFC7217）やその整理が進行中

IPv6対応時のセキュリティ観点の整理

金沢大学 KANAZAWA UNIVERSITY

IPv6の仕様に因るセキュリティ課題

① 仕様が変更され解決した課題
② 実装面で注意が必要な課題
③ 運用面での対策が必要な課題

デュアルスタック運用における観点

④ IPv4仕様との違いの理解

⑤
- 全て落とせなくなったICMPv6
- 複雑な自動アドレス設定

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

	SLAAC※	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）	○ (3)	○	○
ルータ優先度	○	× (1)	ー

(1) IETFにて過去に議論があったが標準化の見通しなし（draft-ietf-mif-dhcpv6-route-option (expired)）
(2) プレフィックス情報からアドレスを生成　　(3) RDNSSオプション（RFC6106）

※SLAAC（StateLess Address Auto Configuration）

- （参考）OS毎の対応

OS	DHCPv6	RDNSS	OS	DHCPv6	RDNSS
Windows Vista	○	addon	RHEL 6	○	○
Windows 7	○	addon	Ubuntu 11.04 以降	○	○
Windows 8	○	addon	Android 4.4.4	×	×
Mac OS X 10.6	×	×	iOS 4.3.1 以降	○	○
Mac OS X 10.7 以降	○	○	Windows Phone 8	○	×

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

SLAACとDHCPv6の関係

- ルータ広告中のフラグにより挙動を制御
  - A (autonomous address-configuration) flag
    - プレフィックス情報オプション中のフラグ
    - =1でプレフィックス情報を利用したSLAACを促す
  - O (Other configuration) flag
    - アドレス以外の設定情報（DNSサーバなど）を示すフラグ
    - =1でステートレスDHCPv6を促す
  - M (Managed address configuration) flag
    - ルータ広告以外のアドレス設定を示すフラグ
    - =1でステートフルDHCPv6を促す
- ステートフル/ステートレスDHCPv6
  - ステートレス：DNSサーバなどの情報配布のみ
  - ステートフル：IPv6アドレスの配布と状態管理

複雑な仕様ゆえ異なる実装

- 共通の動作

	A flag	O flag	M flag	備考
SLAAC	1	0	0	RDNSSオプションでDNSサーバ
SLAAC+ステートレスDHCPv6	1	1	0	ほとんどのOSで利用可能
ステートフルDHCPv6	0	1	1	割当アドレス管理を実施する形態
SLAAC+ステートフルDHCPv6	1	1	1	SLAACによるアドレスとDHCPv6による双方のアドレスが付く

- 異なる動作 ⇒ 課題の整理をIETFで実施中
  - Windows 7は忠実な動作
    - A=0, O=1, M=0 でステートレスDHCPv6の動作
    - 状態変化で設定をリリース
  - Linux/Mac OSX/iOSは状態変化に弱い
    - M=1からM=0になってもDHCPv6のアドレスを解放しない
    - A=1, M=0からA=0, M=1になってもSLAACのみのまま　など

dtaft-ietf-v6ops-dhcpv6-slaac-problem

IPv6対応時のセキュリティ観点の整理

金沢大学 KANAZAWA UNIVERSITY

IPv6の仕様に因るセキュリティ課題

① 仕様が変更され解決した課題
② 実装面で注意が必要な課題
③ 運用面での対策が必要な課題

デュアルスタック運用における観点

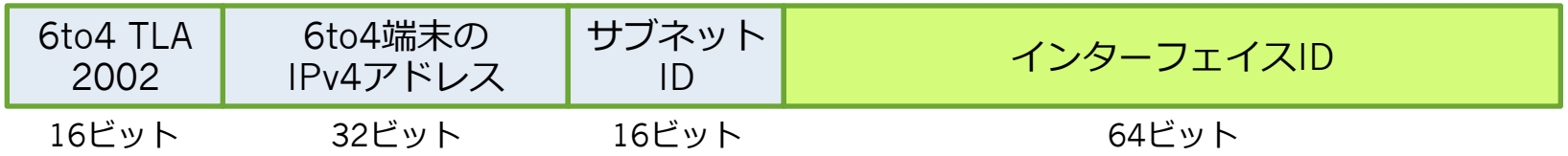
④ IPv4仕様との違いの理解
⑤ IPv6機能有効時の動作の理解

- 意図しないトンネル通信
- IPv6通信優先の理解

自動トンネリングのおさらい

- 6to4（RFC3056）※IETFでは廃止に向けた議論が進行中
  - 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

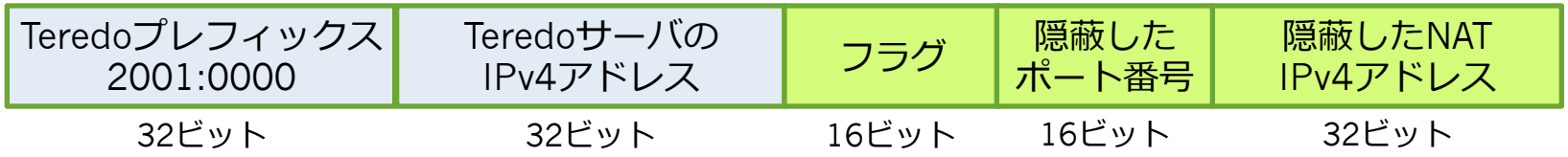
◆6to4のアドレス形式



・/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

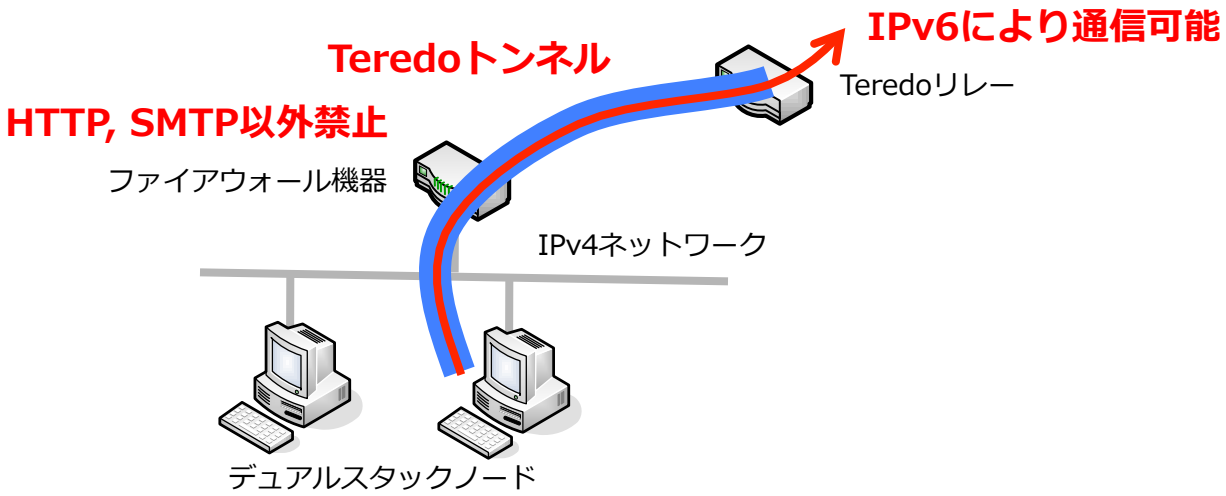
◆Teredoのアドレス形式



・/128のアドレスが一つ割り当てられる

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/7/8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



⑤ 意図しないIPv6通信への対策

- 運用面での対策
  - 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
- 認識と理解が重要
  - 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、自身からの発信がない限りパケットを受信しない

⑤ IPv4ネットワークのデュアルスタック端末

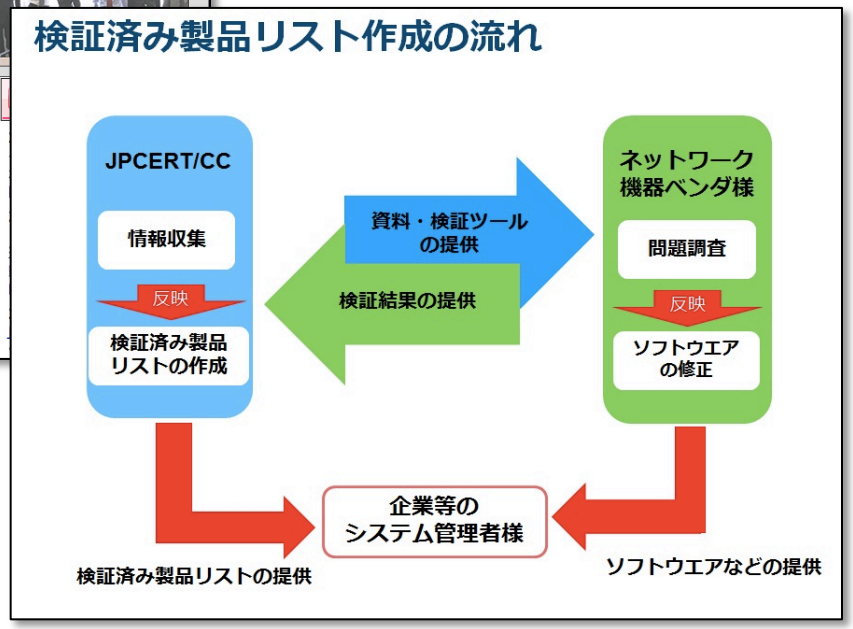
金沢大学 KANAZAWA UNIVERSITY

- 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
  - Windows 8などは定期的な通信で優先を決定
- IPv6が有効になっている認識が重要
  - デフォルトでIPv6機能が有効になっている！
  - RAなどでIPv6アドレスが付与されれば通信を実施
    - IPv6通信が優先されると問題が大きい
  - **IPv6対策のないIPv4ネットワークが最も危険**
- 対策
  - IPv4のみのネットワークでもIPv6通信の監視を実施

JPCERT/CCの取り組み（1）

- IPv6プロトコルのセキュリティ課題に関する取り組み
  - 検証リスト（15項目）を作成しテスト手順書を公開
  - 機器ベンダにテストを実施してもらい機器リストを公開

https://www.jpcert.or.jp/pr/2013/ipv6project.html



テストツールにはOSSを利用
- IPv6 Toolkit（SI6 Networks）
- THC-IPv6（The Hackers Choise）
- nmap

JPCERT/CCの取り組み（2）

金沢大学 KANAZAWA UNIVERSITY

検証項目一覧

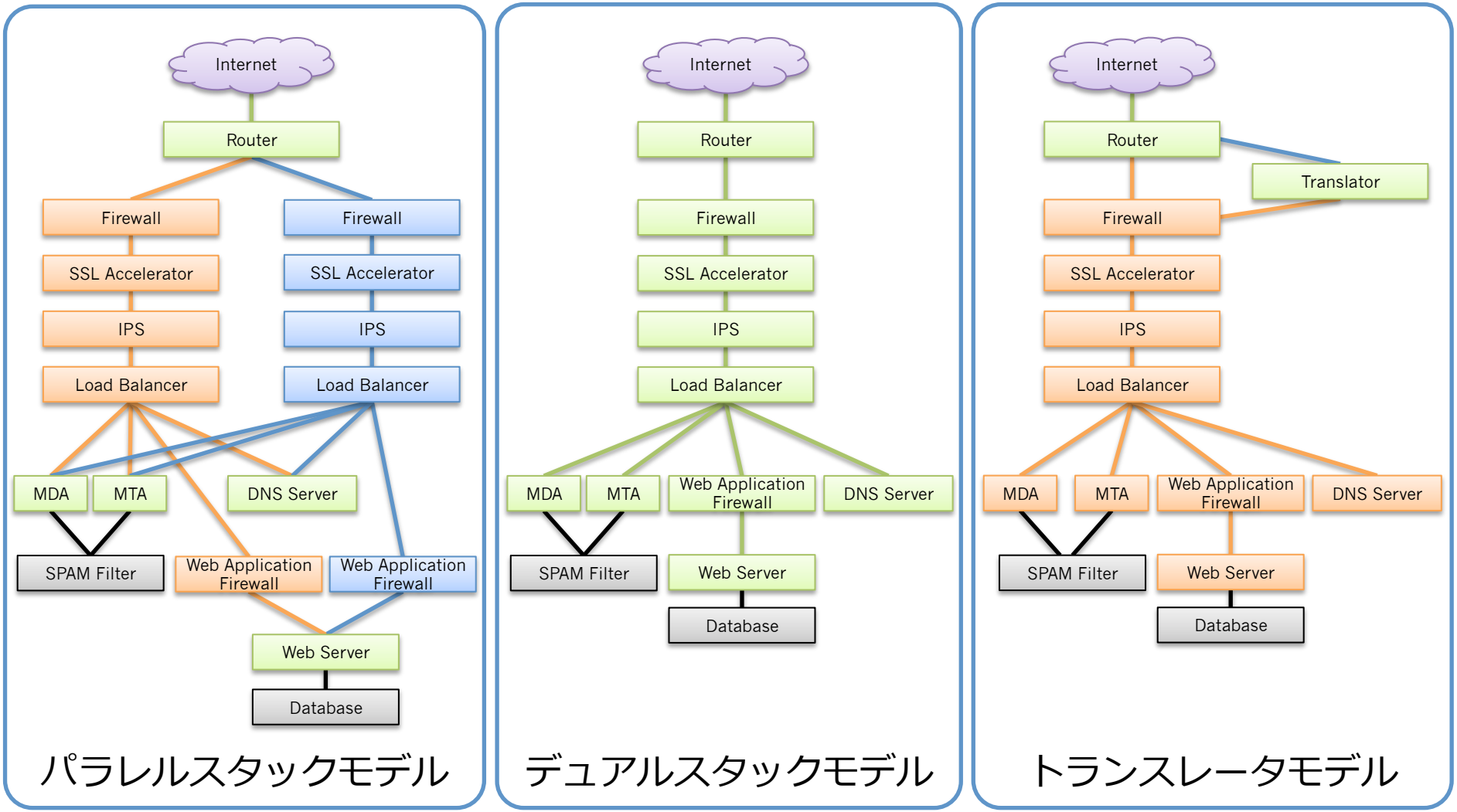
項番	項目名
1	タイプ0ルーティングヘッダ処理の無効化
2	ホップバイホップオプションヘッダによるルータへのDoS攻撃
3	特大ペイロードオプション利用における実装上の課題
4	不正なフラグメントヘッダによるパケット情報の上書きの対応　完全上書き（前）
5	不正なフラグメントヘッダによるパケット情報の上書きの対応　完全上書き（後）
6	不正なフラグメントヘッダによるパケット情報の上書きの対応　部分上書き（前）
7	不正なフラグメントヘッダによるパケット情報の上書きの対応　部分上書き（後）
8	細かいフラグメントヘッダを利用したDoS攻撃　tiny fragmentの実装確認
9	細かいフラグメントヘッダを利用したDoS攻撃　大量のtiny fragment
10	第一フラグメントパケットのみを送信することによるDoS攻撃
11	第一フラグメントヘッダを利用したDoS攻撃　atomic fragmentの実装確認
12	第一フラグメントヘッダを利用したDoS攻撃　大量のatomic fragment
13	フラグメントID予測による経路外攻撃者からの攻撃
14	近隣探索サービスを利用したルータへのDoS攻撃
15	ルータに対する大量の不正パケット送信によるDoS攻撃

参考：https://www.jpcert.or.jp/research/ipv6product_list.html
検証済み製品リストも順次公開

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
  - 課題があるものは改善されている
  - 新しいRFCに準拠しているか実装の確認が必要
  - 最近も改変の議論が盛ん
    - 基本仕様における曖昧さの解消が中心
- 実装面
  - 仕様上明確でない上限値の実装が求められる
  - 拡張ヘッダやPMTUDなどルータ処理が難しい点も
- 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