IPv6 Summit in SAPPORO 2018

～IPv6セキュリティチュートリアル～

IPv6セキュリティ概説 -プロトコル編-

一般財団法人インターネット協会IPv6デプロイメント委員会
東京工業大学 学術国際情報センター
北口 善明

March 12, 2018

IPv6対応時のキーワード

「IPv6対応」≠「IPv6への移行」

- IPv4ネットワークからIPv6ネットワークに置き換わるのではない
- IPv6ネットワークがIPv4ネットワークに**追加**される

二重のネットワーク運用

- 三つの視点での考慮が求められる
  - 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を理解することが重要

IPv6対応時のセキュリティ観点の整理

① IPv6の仕様変更で解決した問題

- ルーティングヘッダにおけるDoS攻撃問題
- 不完全なフラグメントヘッダによる問題
- IPv6におけるプライベートアドレス問題
- IPv6アドレスの運用管理とプライバシの問題
- IPv6アドレスの短縮表記と厳密性不足の問題
- ポイントツーポイントのアドレッシング問題
- リンクローカルセグメントにおける脆弱性

② IPv6移行の進捗に伴う仕様の追加変更

- トンネリング手法における問題と変遷
- トンランスレータ技術における問題
- 複雑な自動アドレス設定による運用面の課題

IPv6対応時のセキュリティ観点の整理

東京工業大学
Tokyo Institute of Technology

① IPv6の仕様変更で解決した問題

- ルーティングヘッダにおけるDoS攻撃問題
- 不完全なフラグメントヘッダによる問題
- IPv6におけるプライベートアドレス問題
- IPv6アドレスの運用管理とプライバシの問題
- IPv6アドレスの短縮表記と厳密性不足の問題
- ポイントツーポイントのアドレッシング問題
- リンクローカルセグメントにおける脆弱性

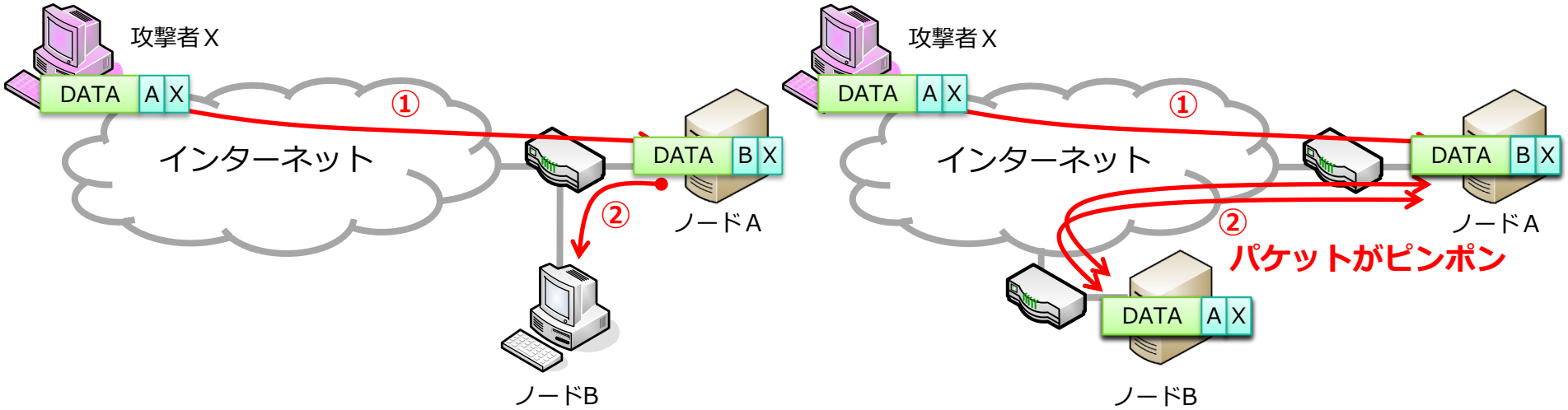
② IPv6移行の進捗に伴う仕様の追加変更

- トンネリング手法における問題と変遷
- トンランスレータ技術における問題
- 複雑な自動アドレス設定による運用面の課題

ルーティングヘッダにおけるDoS攻撃問題

東京工業大学 Tokyo Institute of Technology

- ルーティングヘッダ
  - IPv6の拡張ヘッダの一つでIPv4におけるソースルーティングを実現
    - IPv4においてもすでに問題が指摘されていて利用されていなかったが
  - Type 0で複数の経由地（IPアドレス）を指定可能
- タイプ0ルーティングヘッダ（RH0）による攻撃（2007年）
  - 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



ルーティングヘッダにおけるDoS攻撃問題

- 仕様変更点
  - **RFC 5095**でRH0が廃止（**RFC 8200**からも削除されている）
  - ルーティングヘッダはタイプ毎に制御が必要
- ルーティングタイプの種類
  - 廃止となったのは Type 0 のみ なのでRouting Typeでの制御が必要
  - Type 2はモバイルIPで利用

（参考）現在割当されているRouting Type一覧（2017.11現在）

Routing Type	説明
0	ソースルーティングで利用（非推奨）　[RFC 5095][RFC 8200]
1	Nimrod routing system用（非推奨 2009-05-06）
2	Type 2 Routing Header: MIPv6で利用（中継ノードは1つだけ指定可能）　[RFC 6275]
3	RPL (Routing Protocol for Low-Power and Lossy Networks) Source Route Header　[RFC6554]
4-252	未割当
253	RFC3639-style Experiment 1　[RFC 4727]
254	RFC3639-style Experiment 1　[RFC 4727]
255	私用しない

https://www.iana.org/assignments/ipv6-parameters/ipv6-parameters.xhtml#ipv6-parameters-3

不完全なフラグメントヘッダによる問題

- 第二フラグメントパケットによる上書き攻撃（**RFC 5722**）
  - オフセット値を操作して最初のパケット情報を上書き
  - アクセス制御を回避可能な課題（IPv4でも存在した課題）
- 単独フラグメント（atomic fragment）パケット問題（**RFC 6946**）
  - Mフラグ=0 かつ オフセット値=0 のパケット（次がない断片）
  - 仕様が不明確であったため実装によって予期せぬ動作
- 拡張ヘッダチェーンのフラグメント問題（**RFC 7112**）
  - IPv6ヘッダ情報を含まない第一フラグメントパケットを作成可能
  - アクセス制御に対するリソース消費攻撃

いずれも仕様に禁止・破棄可能という記載はない

不完全なフラグメントヘッダによる問題

- 仕様変更点
  - 第二フラグメントパケットでの上書きは破棄
    - ICMPエラーも送信しなくてよい
  - 単独フラグメント時のパケット再構成処理を定義
    - 単独フラグメントの生成自体を禁止
  - 第一フラグメントパケットが拡張ヘッダで埋まるものは破棄
  - **RFC 8200**にすべて反映

IPv6におけるプライベートアドレス問題

- サイトローカルアドレス（fec0::/10）は廃止されました
  - IPv4でも発生していたVPN接続時などにおけるアドレス重複問題
  - NAPTを助長することにつながる → **RFC 3879**で廃止に
- 微妙に残っている点に注意
  - RDNSS のための well-known エニーキャストアドレス
    - draft-ietf-ipv6-dns-discovery での提案（Expired）
    - Windows 8.1 までの実装に残っている（fec0:0:0:ffff::1, 2, 3）
    - IPv6 RDNSSが別途設定されると利用されない実装
- ULA（Unique Local IPv6 Unicast Address）の登場（**RFC 4193**）
  - グローバルユニークなプライベートアドレス（fc00::/7）
  - 外部との通信のためにはアドレス変換（NAPT等）が必要
  - ULAの外部漏洩を防ぐACLが必ず必要（ルータでのbogonフィルタなど）

IPv6におけるプライベートアドレス問題

- IPv6におけるNAT/NAPTの存在
  - IPv4のNAPTに相当するNAT66は標準化されていないが実装がある状態
    - Linux（ip6tablesで実現）、VMware
  - プレフィックス変換のNPTv6が標準化（**RFC 6296**）
    - ステートレスなアドレス変換：アドレスを1対1変換
    - 仮想化環境やテザリングで有用との意見
    - ただしIETFとしてはNPTv6利用も推奨していない立場
- グローバルアドレス利用だとセキュリティ的に弱い？
  - 適切なフィルタリングでセキュリティ確保可能
    - Ingressフィルタ＋動的フィルタ（SPI）
  - NATは一方通行のように見えているだけでセキュリティデバイスではない

IPv6アドレスの運用管理とプライバシの問題

- IPv6アドレスフォーマット

※IPv6自動アドレス設定時にはIID = 64 bitが前提（n = 64）

- IPv6自動アドレス設定時のIID生成方法の変遷
  - 最初の仕様はMACアドレスからの生成：Modified EUI-64（**RFC 4861**）
    - プレフィックスが変化しても一意に特定可能（プライバシ問題）
    - MACアドレスによる特定機器を狙った攻撃（セキュリティ問題）
  - プライバシ拡張アドレスによるランダム生成の登場（**RFC 4941**）
    - 定期的に変化するためトレーサビリティ確保が困難（管理者視点）
    - 攻撃者にアドレスの匿名性を利用されてしまう問題
  - プライバシを確保しつつ管理性の確保：Semantically Opaque（**RFC 7217**）
    - プレフィックスをIID生成キーの一つとして定義
    - プレフィックス変化でIIDが変わるが同じ環境下では変化しない
      - macOSやLinuxにて実装を確認

※ **RFC 8064**：IID生成手法の仕様を網羅的に解説

IPv6アドレスの短縮表記と厳密性不足の問題

- IPv6アドレスの省略表記
  - 先頭の”0”は省略しても良い（MAY）
    - 2001:0db8:cafe:0000:0000:0000:0000:0101 ➡ 2001:db8:cafe:0:0:0:0:101
  - 連続した”0”は1回に限り”::”で省略してもよい（MAY）
    - 2001:db8:cafe:0:0:0:0:101 ➡ 2001:db8:cafe::101
- ゆるい仕様によるアドレス表記における<u>ゆれ</u>が発生

◆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判定にて誤りが発生
  - ログチェックなど運用面で問題

IPv6アドレスの短縮表記と厳密性不足の問題

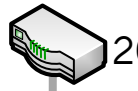
- 仕様変更点
  - 省略表記を実施する際に以下を遵守する（MUST）と修正（**RFC 5952**）
    - 先頭の”0”はすべて省略すること
    - “::”の省略はもっとも長い部分に適用すること
    - 同じ長さの場合には前半に適用すること
    - 1フィールド（hextet）だけの”::”利用は禁止
      - 2001:db8::1:1:1:1:1はNG ➡ 2001:db8:0:1:1:1:1:1

      ※ hextet (ヘクテット/ヘクステット) : 16ビットのグループを指す言葉（I-Dで議論があったがRFCにならず）
  - アルファベットは小文字を用いること（MUST）と修正
- 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も必要
  - プログラミングではIPアドレス型を利用
    - PostgreSQLにおけるネットワークアドレス型　など

ポイントツーポイントリンクのアドレッシング問題

東京工業大学 Tokyo Institute of Technology

- ポイントツーポイントリンクへのDoS攻撃
  - パケットのピンポンが発生することによるリソース消費
  - NDPの近隣キャッシュを肥大化させるDoS攻撃
  - IPv4でも同様の問題があり/30を利用することで回避可能
  - IPv6では/127利用に問題（**RFC 3627**）
    - 若番がサブネットルータエニーキャストアドレスのため使えない



2001:db8::3
～ 2001:db8::ffff:ffff:ffff:ffff
宛の対策が必要

※サブネットルータエニーキャストアドレス：リンク内の全ルータに到達できるアドレス

◇IPv4の/30		◇IPv6の/127	
192.168.0.0	ネットワークアドレス	2001:db8::0	サブネットルータエニーキャスト
192.168.0.1	ルータ１	2001:db8::1	ルータ１
192.168.0.2	ルータ２	※ルータ２にアドレス設定できない	
192.168.0.3	ブロードキャストアドレス		

- 仕様変更点
  - /127の場合サブネットルータエニーキャストアドレスは無効（**RFC 6164**）
    - ポイントツーポイントでは/127を利用することを推奨

NDPのおさらい：役割とメッセージタイプ

- NDPが果たす役割

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（RFC 5227にてIPv4の仕様に逆輸入）
	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

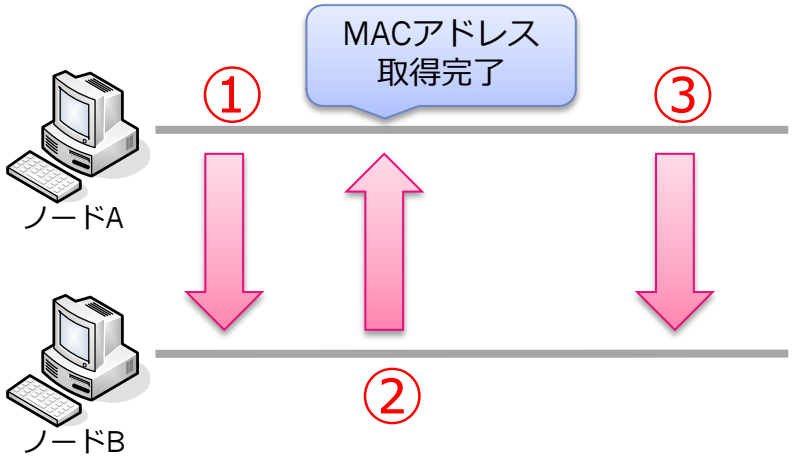
- NDPの5つのメッセージタイプ

機能	ICMPv6 type	説明
ルータ要請（RS：Router Solicitation）	133	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（RA：router Advertisement）	134	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（NS：Neighbor Solicitation）	135	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（NA：Neighbor Advertisement）	136	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	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のおさらい：動作概要

東京工業大学 Tokyo Institute of Technology

- リンクローカルアドレス解決の流れ

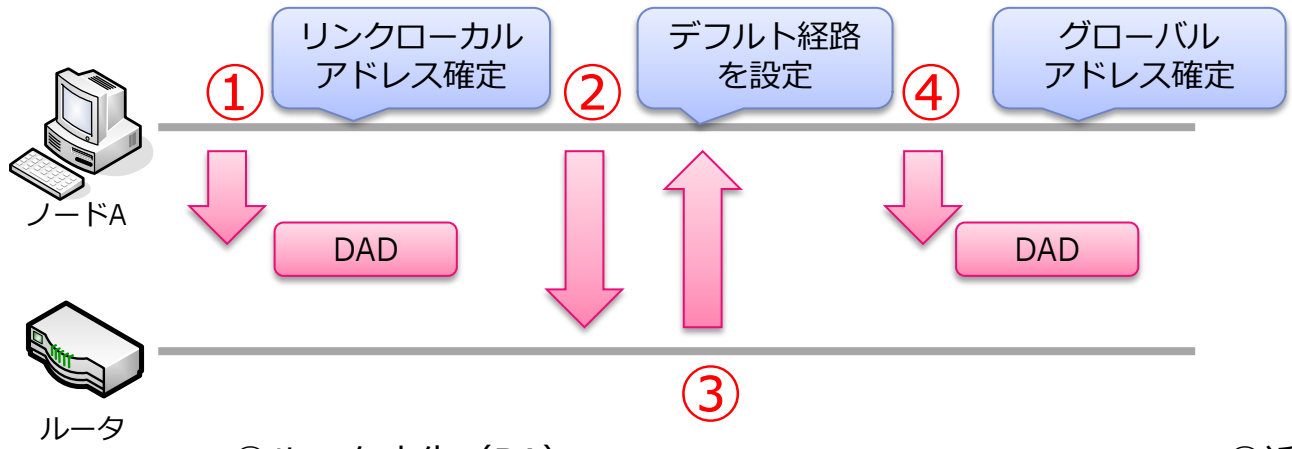


①近隣要請（NS）
通信相手のMACアドレスを探索（宛先はマルチキャスト）
近隣広告がない場合はオンリンクでないと判断

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

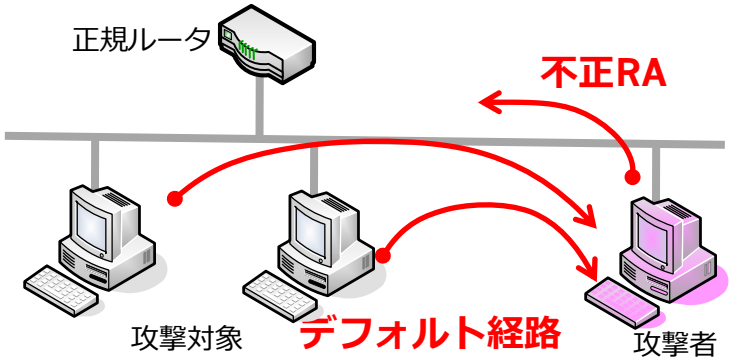
②ルータ要請（RS）
全ルータマルチキャスト（ff02::2）宛に送信

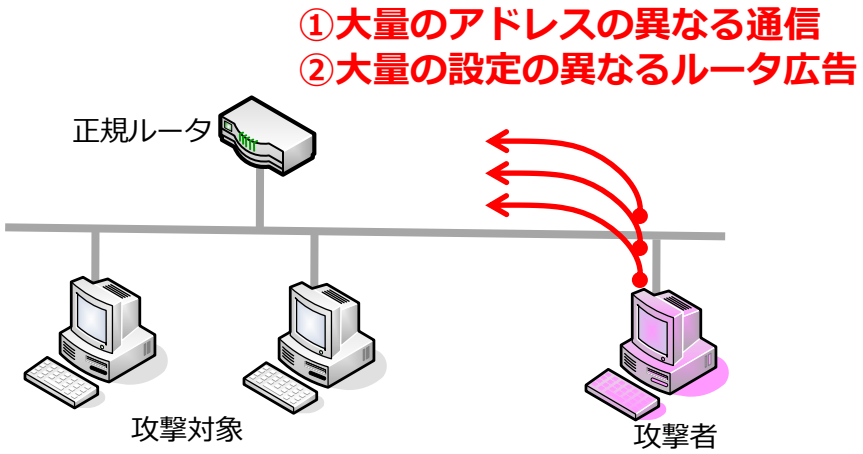
③ルータ広告（RA）
全ノードマルチキャスト（ff02::1）宛に送信
取得プレフィックスからグローバルアドレスを生成

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）

リンクローカルセグメントにおける脆弱性（不正RA）

- 認証スキームのない近隣探索プロトコル（NDP）
  - 同一リンクの端末に悪意のある端末はいないモデルで脆弱（デメリット）
  - 実装が容易であるため普及・展開が迅速に可能（メリット）
  - IPv4におけるARPと同じメリット・デメリットを持つ
- 不正なRAによる課題（**RFC 6104**）
  - 意図しないアドレス／デフォルト経路を設定し盗聴・通信障害が可能
  - 大量のRAを送信することで機器のリソース大量消費が可能





リンクローカルセグメントにおける脆弱性（不正RA）

- 不正RAからサブネットを守る方法：認証技術の利用／運用面の対策
  - SEND（SEcure Neighbor Discovery）の導入
    - NDPに認証機能を持たせるので詐称防御が可能
    - 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）
    - 全てのノードに設定が必要な点が課題で普及に至っていない
  - 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
  - NDPのモニタリング（NDPMonなど）
    - 攻撃の早期確認が可能
  - 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」で広告しノードの学習をリセット

最低限必要な対策

リンクローカルセグメントにおける脆弱性（不正RA）

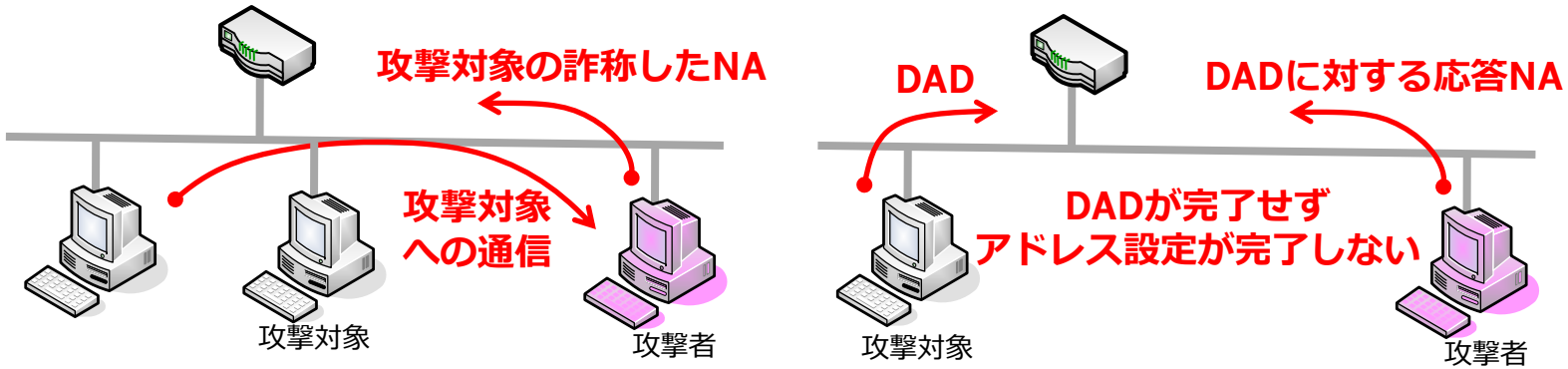
- 追加された新しい仕様を利用した防御手法
  - ルータ優先度（**RFC 4191**）の利用
    - 正規ルータの優先度を”high”に設定
    - 意図的なもの（攻撃）は排除不能
  - RA-Guard（**RFC 6105**）機能の利用
    - L2スイッチにおけるRAのIngressフィルタ
    - フラグメント利用によるRA-Guard回避問題の指摘
- 仕様変更点
  - フラグメント化されたNDPパケットの利用禁止（**RFC 6980**）
  - RD-Guardの実装手法の整理（**RFC 7113**）

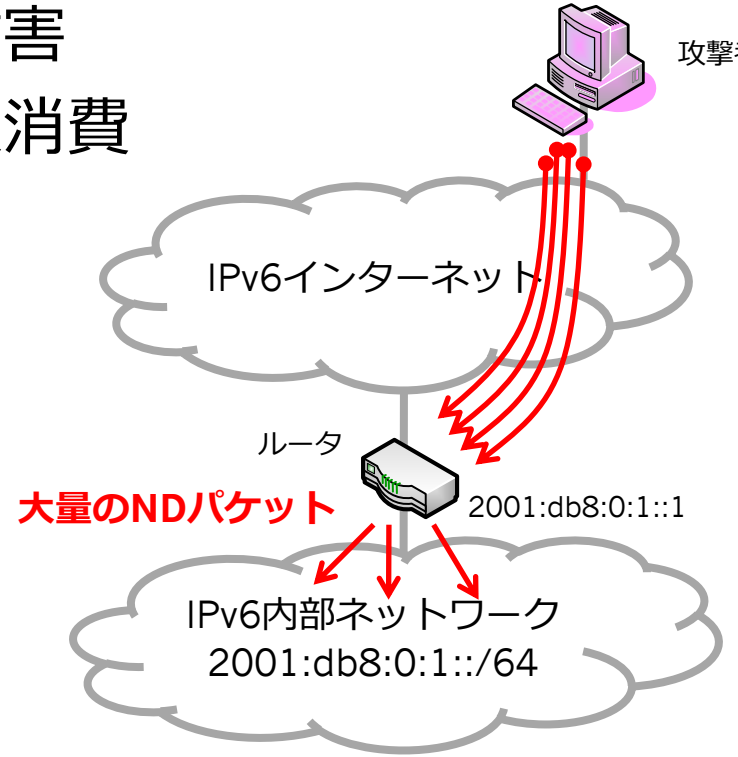
最低限必要な対策

RFC 6980対応＋RA-Guard機能利用が有効な防御手法

リンクローカルセグメントにおける脆弱性（その他）

- NDPにおけるDoS攻撃
  - 近隣広告（NA）の詐称により近隣キャッシュを汚染（ARPと同様）
  - 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
  - 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





- 不正なDHCPサーバによる課題
  - 認証機能がない点でNDPと同様の課題を持つ

リンクローカルセグメントにおける脆弱性（その他）

- 不正なNAを排除する手法（不正RA対策と同様）
  - 認証技術の導入
  - NDPのモニタリング

最低限必要な対策

- 追加された新しい仕様の導入
  - DHCPv6-shield（**RFC 7610**）
    - 不正なDHCPv6サーバから端末を保護する仕組み
    - RA-Guardと同様にL2スイッチによる防御手法

最低限必要な対策

- 実装におけるND/RAのレート制限の必要性（**RFC 6583**）
  - リソースを明確に管理する
    - IPv6のサブネットは非常に大きな空間であるため必要に応じて上限設定が必要
  - NDP近隣キャッシュ制御における優先順位の導入
    - 新エントリ追加より自身のアドレス解決応答を優先
    - 未知のアドレス探索は最低の優先度に　など

IPv6対応時のセキュリティ観点の整理

東京工業大学
Tokyo Institute of Technology

① IPv6の仕様変更で解決した問題

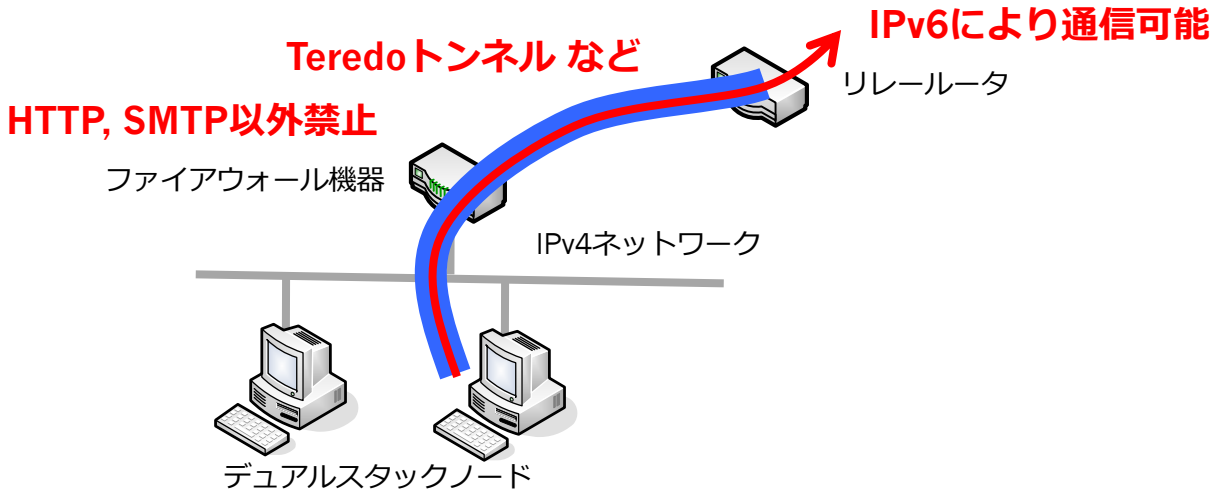
- ルーティングヘッダにおけるDoS攻撃問題
- 不完全なフラグメントヘッダによる問題
- IPv6におけるプライベートアドレス問題
- IPv6アドレスの運用管理とプライバシの問題
- IPv6アドレスの短縮表記と厳密性不足の問題
- ポイントツーポイントのアドレッシング問題
- リンクローカルセグメントにおける脆弱性

② IPv6移行の進捗に伴う仕様の追加変更

- トンネリング手法における問題と変遷
- トンランスレータ技術における問題
- 複雑な自動アドレス設定による運用面の課題

トンネリング手法における問題と変遷

- IPv6 over IPv4トンネリング
  - IPv6対応の初期段階で必須の移行技術
  - IPv6島をIPv4インターネットを介して結合
- トンネリング手法における問題
  - IPv4におけるフィルタリングポリシの回避が可能
    - IPv6バックドア構築による通信傍受（不正RAとの連携で脅威拡大）
  - 自動トンネリング技術による意図しない通信の可能性
    - 6to4、Teredo など



トンネリング手法における問題と変遷

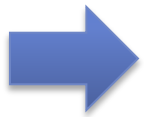
- 自動トンネリグ技術と現状
  - ISATAP：組織内におけるIPv6端末とネットワークの接続
    - トンネリングの両端を同じ組織が管理するため問題は小さい
  - 6to4：IPv4グローバルアドレスを利用したIPv6アドレス
    - 6to4リレールータのセキュリティ担保は困難で問題が存在
    - IPv4グローバルアドレスを持つと自動的にトンネルを設定する実装も存在
  - 6rd：6to4技術を用いたISP内のIPv6展開手法
    - 6to4リレーをISP内に設置するため問題は小さい
  - Teredo：IPv4 NATトラバーサルをIPv6で実現する技術
    - Windowsではデフォルトで設定されるが自身からの利用がないと受信しない仕様
    - Windows 10においてもインタフェースは存在
- 運用面における対策例（**RFC 7123**）
  - フィルタリング（Teredoの場合3544/udpを禁止　など）
  - IPv6通信のモニタリングが必要

トンネリング手法における問題と変遷

- 仕様の変遷
  - アドレス選択機構（**RFC 6724**）における優先度の変更
    - IPv4アドレスが6to4アドレスより優先されるように変更

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

（RFC 3484）



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

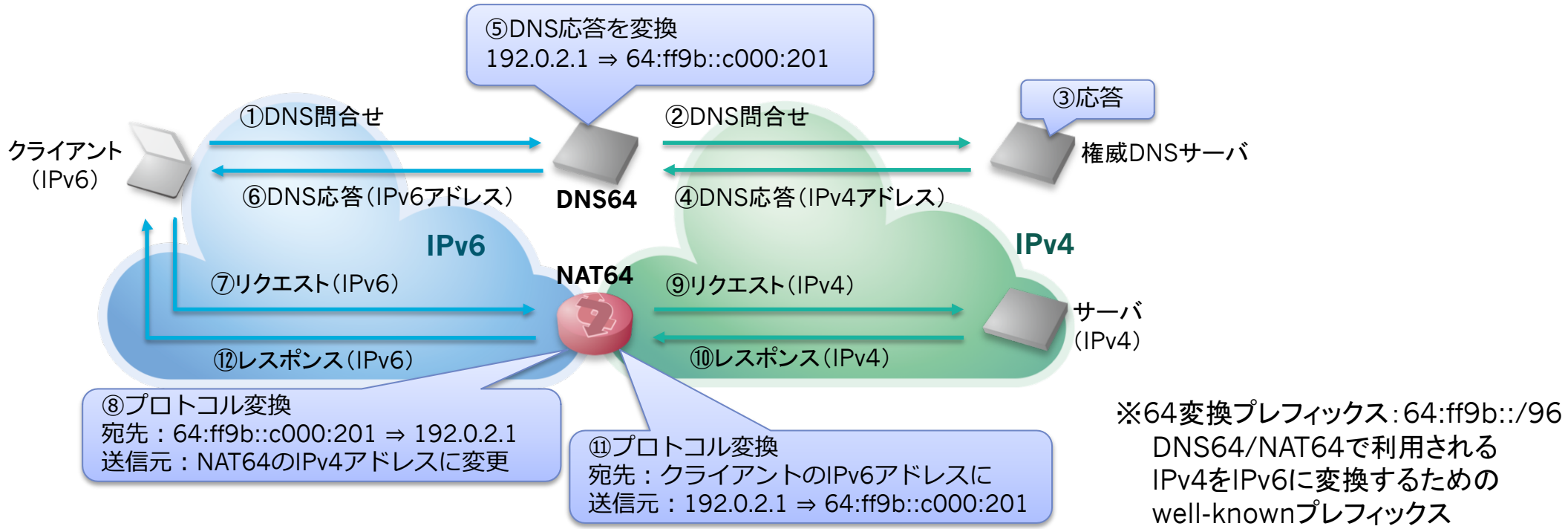
    - 現状は端末OS毎にRFC 6724＋αの実装となり異なっている
  - 6to4利用の非推奨（**RFC 7526**）
    - IPv6ネイティブ利用が進んだためトンネリングの必要性低下
    - 6to4リレールータでの問題は解決できないため非推奨に
  - UDPトンネリング時のチェックサム計算免除の例外追加（**RFC 6935**）
    - 処理の高速化のために仕様変更され例外処理を明確に定義

トランスレータ技術における問題

- トランスレータ
  - IPv4とIPv6のプロトコル変換によりIPv6移行期間をサポートする技術
  - 現在の主流：DNS64/NAT64（**RFC 6146**, **RFC 6147**）
  - IPv6オンリーネットワーク運用の需要により利用拡大
- NAT64における問題点
  - IPv4 NAPTと同様にIPsecとの併用はできない
  - TCP SYNフラッド攻撃や不正フラグメント攻撃への対策が必要
  - 64変換プレフィックスを送信元に持つ外部からのパケットは破棄
    - IPv4ネットワークへの反射攻撃が可能になる
  - DNS64とNAT64間で同じ64変換プレフィックスを利用することが重要
    - 異なるとDoS攻撃、フィラッディング攻撃、盗聴攻撃の危険に晒される

参考：DNS64/NAT64

- IPv6をベースとしてIPv4へのアクセスをアドレス変換で提供
  - DNS64にてDNS応答におけるIPv4アドレスをIPv6アドレスに変換
  - NAT64にて特定のIPv6プレフィックス宛の通信をIPv4にアドレス変換
- DNS64/NAT64環境におけるIPv4サーバとの通信の流れ



※64変換プレフィックス：64:ff9b::/96
DNS64/NAT64で利用される
IPv4をIPv6に変換するための
well-knownプレフィックス

複雑な自動アドレス設定による運用面の課題

- 二種類のIPv6アドレス設定手法
  - SLAAC：ステートレスなIPv6アドレス設定
  - DHCPv6：ステートフルなIPv6アドレス設定
- 自動アドレス設定で設定される項目と手法

	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（RDNSSなど）	○ (3)	○	○
ルータ優先度（RFC 4191）	○	× (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（RFC 6106 -> 8106）

- RAのRDNSS（Recursive DNS Server）オプションの必須化（**RFC 8106**）

複雑な自動アドレス設定による運用面の課題

- SLAACとDHCPv6の関係（**RFC 4861**）

	A flag	O flag	M flag	備考
SLAAC	1	0	0	RDNSSオプションでDNSサーバ（**Windows 10 Creators Updateで対応**）
SLAAC+ステートレスDHCPv6	1	1	0	ほとんどのOSで利用可能（Androidは非対応）
ステートフルDHCPv6	0	N/A	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	N/A	1	SLAACによるアドレスとDHCPv6による双方のアドレスが付く

  - A (autonomous address-configuration) flag：
    - プレフィックス情報オプションのフラグ
    - =1 でプレフィックス情報を利用したSLAACによるアドレス設定を促す
  - O (other configuration) flag：
    - アドレス以外の設定をDHCPv6で実施するためのフラグ
    - =1 でステートレスDHCPv6処理を促す
  - M (managed address configuration) flag：
    - SLAAC以外でのアドレス設定をDHCPv6で実施するためのフラグ
    - =1 でステートフルDHCPv6処理を促す（O flagの値は無視される）

複雑な自動アドレス設定による運用面の課題

- 端末OS毎に異なる実装（**I-D ietf-v6ops-dhcpv6-slaac-problem**）
  - 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
  - Windows 8.1, 10は勝手にDHCPv6を利用
    - A=0, O=0, M=0 でもDHCPv6クライアントが動作
    - 2017年初頭のバージョンにはBUGがありIPv6オンリー環境で誤動作
      - Windows 10 Fall Creators Update (2017) にてBUGは改修
  - Linux/macOS/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

複雑な自動アドレス設定による運用面の課題

- AndroidにおけるDHCPv6非実装の問題
  - IPv6における統一的なステートフルアドレス設定が不可能
- Googleの主張（**RFC 7934**）
  - DHCPv6利用＝インタフェースのIPv6アドレスを1つに限定
    - 1インタフェースに複数のアドレスを持つIPv6の拡張性喪失
    - 1つのアドレスはNAPT利用を助長

    以上の理由からAndroidでDHCPv6を実装しないという判断
  - 複数アドレスのメリット
    - プライバシ拡張アドレスでトレース回避
    - アプリケーション毎にアドレスを使い分けることが可能
    - テザリングや仮想マシンに対して独立したアドレスを提供可能
- 端末毎の/64利用に関して
  - 端末にユニキャストRAにより/64を割り当てる手法（**RFC 8273**）

実運用に向けた検討

- IPv4と異なり様々なサブネット形態が存在
  - IPv4：プライベートアドレス、/24、DHCP
  - IPv6：ステートレス or ステートフル、アドレス割当 or プレフィックス割当
  - デュアルスタック or IPv6 only + NAT64/DNS64
- IPv6でのトレーサビリティ管理手法
  - DHCPv6リースファイル
    - IPv6アドレスとUDIDの組（DHCPv4と異なる点）
    - UDIDは3種類ありOSにより異なる
  - NDP近隣キャッシュ
    - IPv6アドレスとMACアドレスの組
    - ルータのNDP近隣キャッシュを定期的に収集 or NDPモニタ（MDPMonなど）
- セキュリティレベルと利用形態の整理が今後必要

まとめ

- IPv6の仕様は問題発生と共に改修
  - IPv4と同様の仕様から発生したものが多い
  - 多くの改修RFCが登場し全体が把握しづらくなっていた
    - IPv6ネットワーク運用におけるセキュリティ対策の整理（**I-D ietf-opsec-v6**）
  - インターネット標準により見通しの改善
    - RFC 8200、RFC 8201に多くの改修RFCがマージ
  - 最新の仕様を実装しているかの確認が重要
- これからも仕様変更・追加の議論に注意
  - アドレスアーキテクチャの標準化議論中
    - 大きな変更はないと想像されるが注意が必要
  - 実装毎の違いに注意
    - アドレス自動設定や追加仕様の実装状況
  - 本格的な運用に向けた実践的な議論が重要

（参考）参照RFC/I-D一覧

東京工業大学 Tokyo Institute of Technology

RFC 3627 Use of /127 Prefix Length Between Routers Considered Harmful	/127利用における問題点（→ RFC 6164）
RFC 3879 Deprecating Site Local Addresses	サイトローカルアドレス非推奨へ
RFC 4191 Default Router Preferences and More-Specific Routes	RAにおけるルータ優先度
RFC 4193 Unique Local IPv6 Unicast Addresses	グローバルユニークなローカルアドレス（ULA）
RFC 4861 Neighbor Discovery for IP version 6 (IPv6)	近隣探索プロトコル（NDP）
RFC 4941 Privacy Extensions for Stateless Address Autoconfiguration in IPv6	プライバシ拡張アドレス
RFC 5095 Deprecation of Type 0 Routing Headers in IPv6	Type 0 ルーティングヘッダの廃止（RFC 8200）
RFC 5722 Handling of Overlapping IPv6 Fragments	フラグメントヘッダの重複問題と対処方法（RFC 8200）
RFC 5952 A Recommendation for IPv6 Address Text Representation	IPv6アドレスの省略表記の厳密化
RFC 6104 Rogue IPv6 Router Advertisement Problem Statement	不正RAによる問題
RFC 6105 IPv6 Router Advertisement Guard	RA-Guardによる不正RA防御
RFC 6146 Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers	NAT64
RFC 6147 DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers	DNS64
RFC 6164 Using 127-Bit IPv6 Prefixes on Inter-Router Links	/127利用時のサブネットルータエニーキャストの無効化
RFC 6296 IPv6-to-IPv6 Network Prefix Translation	IPv6ネットワークアドレス変換（NPTv6）
RFC 6583 Operational Neighbor Discovery Problems	NDPの問題点と対処方法
RFC 6724 Default Address Selection for Internet Protocol Version 6 (IPv6)	送信元および宛先アドレスの選択アルゴリズム
RFC 6946 Processing of IPv6 “Atomic” Fragments	単独フラグメントパケットの問題（RFC 8200）
RFC 6935 IPv6 and UDP Checksums for Tunneled Packets	UDPトンネリングでのチェックサム計算の免除（RFC 8200）
RFC 6980 Security Implications of IPv6 Fragmentation with IPv6 Neighbor Discovery	NDPにおけるフラグメントパケットの破棄
RFC 7112 Implications of Oversized IPv6 Header Chains	拡張ヘッダチェーンのフラグメント制限（RFC 8200）
RFC 7113 Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard)	RA-Guardを実装する際の注意点
RFC 7123 Security Implications of IPv6 on IPv4 Networks	IPv4ネットワークにおけるIPv6を利用した攻撃手法
RFC 7217 A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration	Semantically Opaque IIDの定義
RFC 7526 Deprecating the Anycast Prefix for 6to4 Relay Routers	6to4利用が非推奨に
RFC 7610 DHCPv6-Shield: Protecting against Rogue DHCPv6 Servers	不正DHCPv6サーバ対策のためのDHCPv6-Shield
RFC 7934 Host Address Availability Recommendations	端末へのIPv6アドレス割当の議論
RFC 8064 Recommendation on Stable IPv6 Interface Identifiers	インタフェースID生成手法のまとめ
RFC 8106 IPv6 Router Advertisement Options for DNS Configuration	RAにおけるRDNSSオプションとその必須化
RFC 8200 Internet Protocol, Version 6 (IPv6) Specification	**IPv6の基本仕様（Internet Standards）**
RFC 8201 Path MTU Discovery for IP version 6	**IPv6におけるパスMTU探索（Internet Standards）**
RFC 8273 Unique IPv6 Prefix Per Host	端末に/64プレフィックスを割当する手法
I-D ietf-v6ops-dhcpv6-slaac-problem: DHCPv6/SLAAC Interaction Problems on Address and DNS Configuration (expired)	SLAACとDHCPv6によるアドレス自動設定の問題
I-D ietf-opsec-v6: Operational Security Considerations for IPv6 Networks (ver. 13)	IPv6ネットワーク運用におけるセキュリティ対策のまとめ