

C7 見落とされがちなネットワーク監視 ～ IPv6見ていますか？

ー プロトコル視点での整理 ー

東京科学大学 情報基盤センター

北口 善明

November 25, 2025

- 氏名：北口 善明（きたぐち よしあき）
- 所属：東京科学大学 情報基盤センター
- 経歴：
 - 2009年まで民間企業でSIer兼研究者
 - ネットワーク運用技術/IPv6の研究開発・普及啓発活動（1998～）
 - 2009年10月 金沢大学 総合メディア基盤センター
 - 2017年05月 東京工業大学 学術国際情報センター
 - 2024年10月 大学統合に伴い現職
- 主な業務：
 - キャンパスネットワークの設計・構築・運用・管理
 - IPv6運用技術およびセキュリティの研究
 - ネットワーク通信品質計測の研究 など



「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
- デュアルスタック環境では**IPv6通信が優先される**認識も必要

● 基本的なコンセプトは同じ

- アドレス長が 32 vs. 128 であるためヘッダサイズ等はもちろん異なる

	IPv4	IPv6
①自動アドレス設定	DHCPを別途利用	SLAACによりIPv6のみで可能
②プライベートアドレス	NAPTと組み合わせで必須	基本的にグローバルアドレス
③ユーザセグメントサイズ	CIDRによる可変長	プレフィックス長 = 64
④リンク層アドレス解決	ARPを別途利用	NDPがIPv6の機能として存在

SLAAC (Stateless Address Auto-Configuration)

NAPT (Network Address Port Translation)

CIDR (Classless Inter-Domain Routing)

ARP (Address Resolution Protocol)

NDP (Neighbor Discovery Protocol)

- 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
 - RA (ルータ広告) を用いたアドレス設定
 - 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(v4)
デフォルト経路	○	× (1)	○
アドレス	○ (2)	○	○
プレフィックス長	○	× (1)	○ * 正確にはネットマスク
サーバ情報 (RDNSSなど)	○ (3)	○	○
ルータ優先度 (RFC 4191)	○	× (1)	—

(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**)
- 配布プレフィックスを割り当てるDHCPv6-PD (**RFC 8415**) も存在

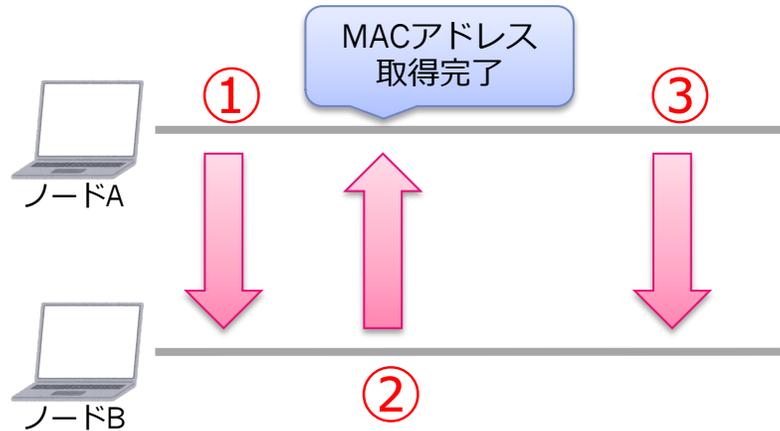
● NDPが果たす役割（RFC 4861）

処理	機能	説明
リンク層アドレスの解決（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（ARPにない機能）
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
	プレフィックスの発見	セグメントのプレフィックス情報を取得
	アドレスの自動生成	ルータ広告に含まれるプレフィックス情報から生成

● NDPの5つのメッセージタイプ

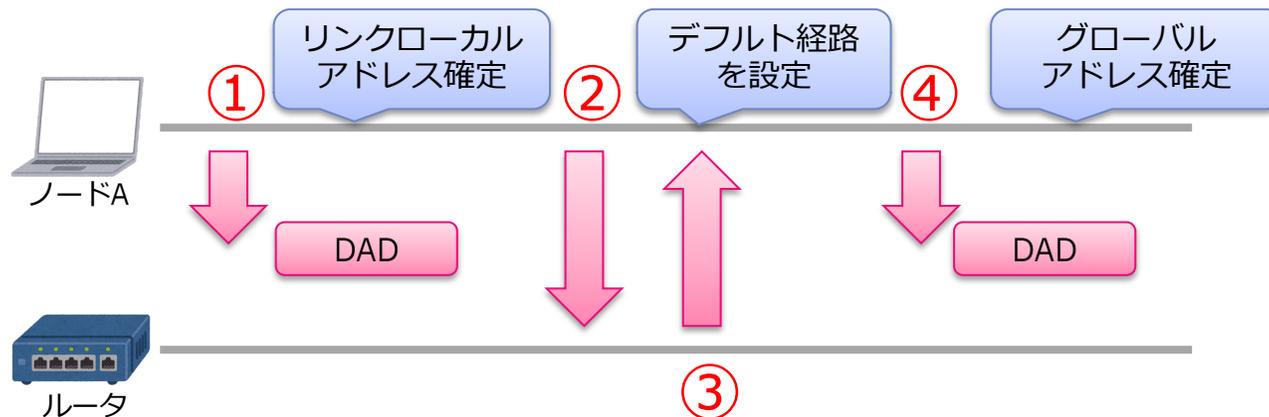
機能	ICMPv6 type	説明
ルータ要請（RS : Router Solicitation）	133	セグメント内のルータ発見に利用、ルータ広告を即座に取得する場合に送出
ルータ広告（RA : router Advertisement）	134	ルータによるデフォルト経路の通知、プレフィックス情報配布で自動アドレス設定が可能
近隣要請（NS : Neighbor Solicitation）	135	重複アドレス検出や到達性／不到達性の確認、リンクレイヤアドレスの解決
近隣広告（NA : Neighbor Advertisement）	136	近隣要請に対する応答、自身のIPアドレス変更の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

● リンク層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)

● RAフラグから見た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サーバ配布可能
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 (PIO) 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 (サーバ情報のみ配布)
- 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)

① 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クライアント非実装の問題

- IPv6におけるステートフルアドレス設定が不可能

● Googleの主張 (**RFC 7934**) *Best Current Practice*

- DHCPv6利用 = インタフェースにIPv6アドレスが1つのみ

- 1インタフェースに複数のアドレスを持つIPv6の拡張性を阻害
- 1つにするとIPアドレスをシェアするNAPT利用を助長



**DHCPv6クライアント
非実装**

● 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

● 端末毎のプレフィックス配布

- 端末に/64を割り当てる手法
- GoogleはAndroidにDHCPv6-PDクライアント搭載を表明*

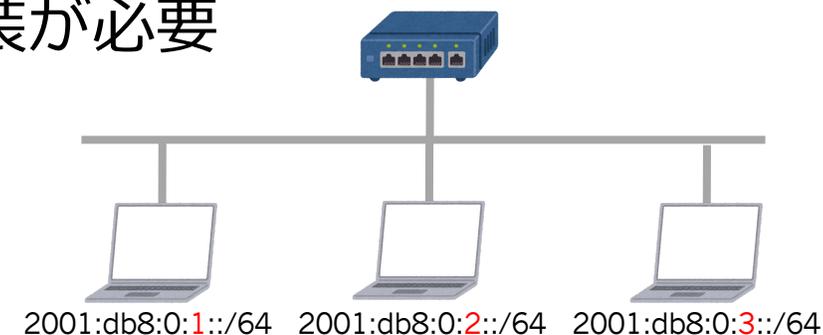
* <https://android-developers.googleblog.com/2025/09/simplifying-advanced-networking-with.html>: "Simplifying advanced networking with DHCPv6 Prefix Delegation", Sep. 2025

① 端末毎のプレフィックス配布に関する議論

* 後述

- IPアドレス共有とローカルセグメントの脆弱性* を回避
 - RA PIOのL (on-link) flag = 0とし全ての通信をルータ経由に
 - NDPによるリンク層アドレス解決を実施しない
- ユニキャストRAによる配布手法 (**RFC 8273**) *Informational*
 - クライアント毎にプレフィックス情報を変更 (配布管理の実装が必要)
 - クライアントの追加実装は不要だがクライアント離脱をルータが把握不能
- DHCPv6-PDにて配布する手法 (**RFC 9663**) *Informational*
 - DHCPv6によるステートを保持した運用が可能
 - RA PIO P (DHCPv6-PD preferred) flag でクライアントに可用性を通知 (**RFC 9762**)
 - クライアントにDHCPv6-PDクライアントの実装が必要

手法	クライアント実装	離脱検知
RFC 8273	不要 (SLAACで動作)	追加実装が必要
RFC 9663	追加が必要	DHCPv6で管理



② 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) の廃止
 - 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
- ULA (Unique Local IPv6 Unicast Address) の登場 (**RFC 4193**)
 - グローバルユニークなローカルアドレス (fc00::/7)
 - 外部との通信のためには別途グローバルアドレスが必要
 - ULAの外部漏洩を防ぐACLが必須 (ルータでのbogonフィルタなど)
- 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等の仮想化基盤：いずれもアドレス共有のNAPT
 - プレフィックス変換のNPTv6が標準化 (**RFC 6296**) *Experimental*
 - ステートレスなアドレス変換でアドレス共有しない

● デフォルトアドレス選択機構 (RFC 6724) における優先順位

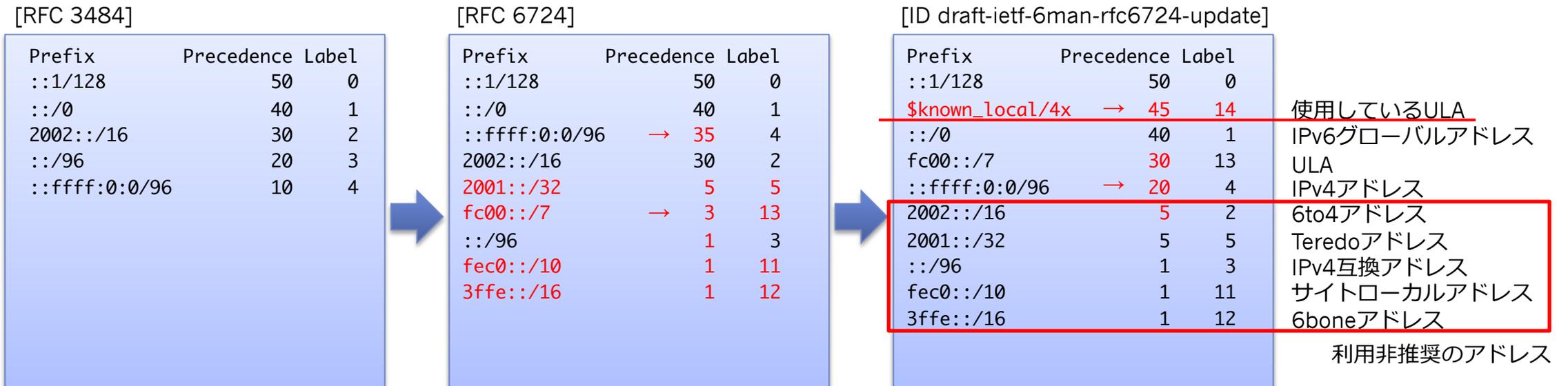
● IPv4プライベートアドレスがULAより優先度高い

➡ デュアルスタック環境でIPv6 (ULA) が利用されない問題

● IETFでの議論 (draft-ietf-6man-rfc6724-update)

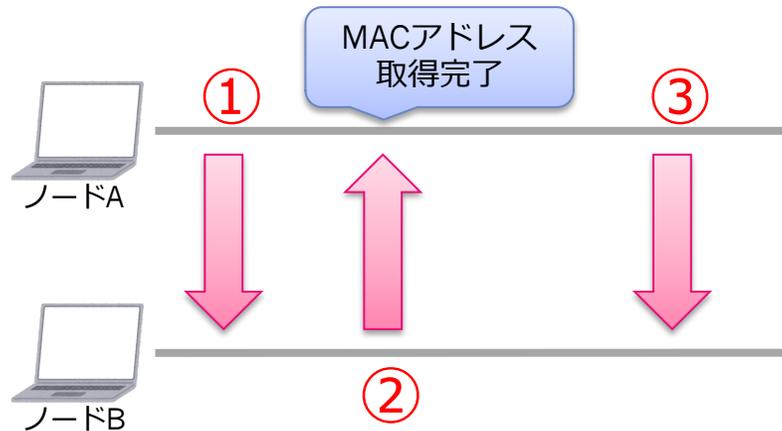
● 利用しているULAを定義し最優先に

● 実装による挙動の差異がしばらく発生する可能性



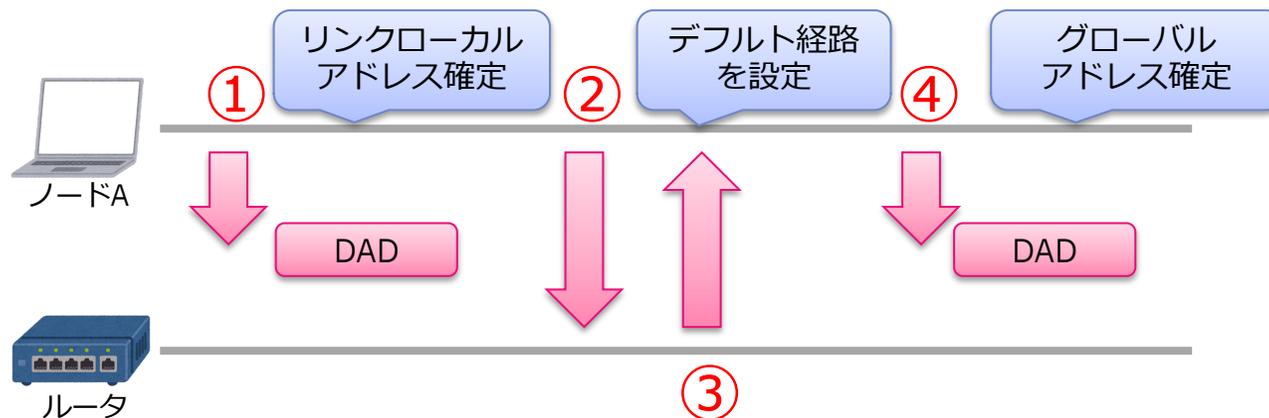
* 赤字が変更点

● リンク層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

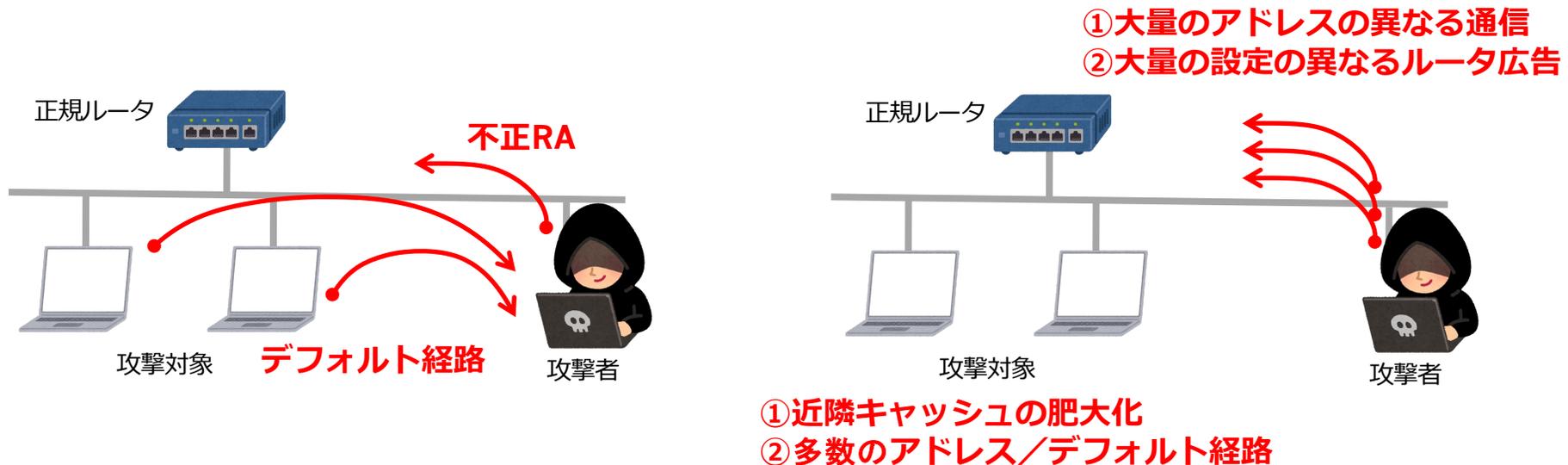


- ①近隣要請 (NS)
近隣広告がなければアドレスの利用が可能
- ②ルータ要請 (RS)
全ルータマルチキャスト (ff02::2) 宛に送信
- ③ルータ広告 (RA)
全ノードマルチキャスト (ff02::1) 宛に送信
取得プレフィックスからグローバルアドレスを生成
- ④近隣要請 (NS)
近隣広告がなければアドレスの利用が可能
(応答があるとアドレスを再構成)

④ 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**） *Informational*
 - 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

IPv4の偽DHCPサーバ問題と似た問題
追加できる点がより強力！



③ ユーザセグメント空間の拡大

- CIDRによる節約運用のIPv4
 - 接続端末数に合わせたネットマスクの変更
- SLAACにおけるプレフィックス長 = 64
 - SLAACで利用するインターフェイスID (IID) の初期仕様がModified EUI-64
 - EUI-64: MACアドレスから64ビットIIDを自動生成する手法
 - $2^{64} = 1.8 \times 10^{19}$ という広大な空間での運用が必要
 - 上限を設けないとリソース枯渇に
 - (参考) P2Pセグメントでは/127を利用可能 (**RFC 6164**)
 - Subnetwork Router Anycastを利用不可とし最小空間を定義
 - (参考) 長いプレフィックス長 (e.g. 80) 利用の議論も
 - draft-mishra-6man-variable-iids
 - draft-mishra-v6ops-variable-iids-problem-statement

● IPv6アドレスフォーマット

プレフィックス (n bits)

IID: インタフェース識別子 (128 - n bits)

※SLAACではIID = 64 bitが前提 (n = 64)

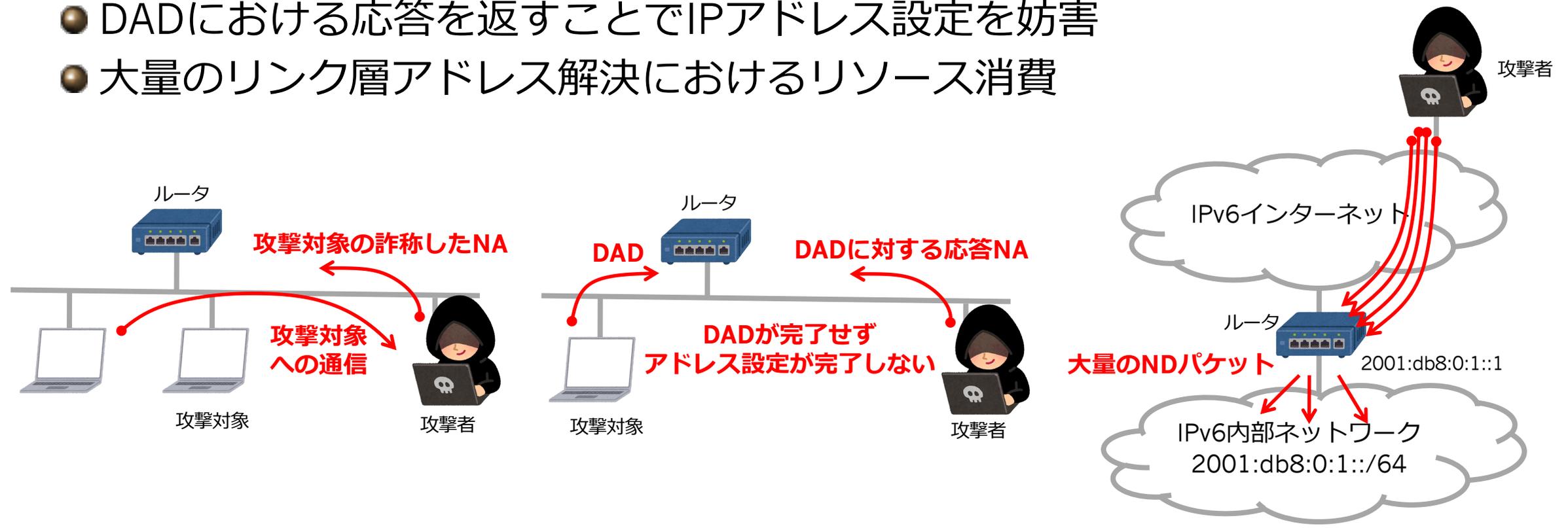
● SLAACにおけるIID生成方法の変遷

- 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 (**プライバシー問題**)
 - 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

※ **RFC 8064**: IID生成手法の仕様を網羅的に解説

● 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にも似た問題）
- 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
- 大量のリンク層アドレス解決におけるリソース消費



- IPv6の仕様は問題発生と共に改修
 - IPv4と同様の”性善説”仕様から発生したものが多い
 - インターネット標準定義により見通しは改善
 - **RFC 8200**、**RFC 8201**に多くの改修RFCがマージ
 - セキュリティ議論の整理 (**RFC 6583**, **RFC 9099**)
 - NDP問題・解決策の整理は進行中 (**draft-ietf-v6ops-nd-considerations**)
 - 最新の仕様を実装しているかの確認が重要
- ネットワーク機器はIPv6 Ready
 - IPv6はネットワーク利用していなくとも動作中！
 - IPv4との挙動差、OS毎のIPv6挙動差に注意！

IPv6は利用しない場合でも”ほぼ全てのネットワーク機器”でIPv6機能は有効
IPv4との違いを理解した上でIPv6を”見る”ことが現状必須

- RFC 3971 SEcure Neighbor Discovery (SEND)
 - RFC 3879 Deprecating Site Local Addresses
 - RFC 4191 Default Router Preferences and More-Specific Routes
 - RFC 4193 Unique Local IPv6 Unicast Addresses
 - RFC 4861 Neighbor Discovery for IP version 6 (IPv6)
 - RFC 4941 Privacy Extensions for Stateless Address Autoconfiguration in IPv6
 - RFC 6104 Rogue IPv6 Router Advertisement Problem Statement
 - RFC 6105 IPv6 Router Advertisement Guard
 - RFC 6164 Using 127-Bit IPv6 Prefixes on Inter-Router Links
 - RFC 6286 [Experimental]
 - RFC 6583 Operational Neighbor Discovery Problems
 - RFC 6724 Default Address Selection for Internet Protocol Version 6 (IPv6)
 - RFC 7113 Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard)
 - RFC 7217 A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)
 - RFC 7610 DHCPv6-Shield: Protecting against Rogue DHCPv6 Servers
 - RFC 7707 Network Reconnaissance in IPv6 Networks
 - RFC 7934 Host Address Availability Recommendations
 - RFC 8064 Recommendation on Stable IPv6 Interface Identifiers
 - RFC 8106 IPv6 Router Advertisement Options for DNS Configuration
 - RFC 8200 Internet Protocol, Version 6 (IPv6) Specification
 - RFC 8201 Path MTU Discovery for IP version 6
 - RFC 8273 Unique IPv6 Prefix per Host
 - RFC 8415 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
 - RFC 9099 Operational Security Considerations for IPv6 Networks
 - RFC 9663 Using DHCPv6 Prefix Delegation (DHCPv6-PD) to Allocate Unique IPv6 Prefixes per Client in Large Broadcast Networks
 - RFC 9762 Using Router Advertisements to Signal the Availability of DHCPv6 Prefix Delegation to Clients
- [Internet Draft]**
- draft-ietf-v6ops-dhcpv6-slaac-problem: DHCPv6/SLAAC Interaction Problems on Address and DNS Configuration (**expired**)
 - draft-ietf-dhc-sedhcpv6: Secure DHCPv6 (**expired**)
 - draft-ietf-6man-rfc6724-update: Prioritizing known-local IPv6 ULAs through address selection policy (ver. 25)
 - draft-ietf-v6ops-nd-considerations: Neighbor Discovery Considerations in IPv6 Deployments (ver. 14)
 - draft-mishra-6man-variable-iids: SLAAC Prefixes with Variable Interface ID (IID)
 - draft-mishra-v6ops-variable-iids-problem-statement: SLAAC Prefixes with Variable Interface ID (IID) Problem Statement
- [Proposed Standard] 安全な近隣探索プロトコル
- [Proposed Standard] サイトローカルアドレス非推奨へ
- [Proposed Standard] RAにおけるルータ優先度
- [Proposed Standard] グローバルユニークなローカルアドレス (ULA)
- [Draft Standard] 近隣探索プロトコル (NDP)
- [Draft Standard] プライバシ拡張アドレス
- [Informational] 不正RAによる問題
- [Informational] RA-Guardによる不正RA防御
- [Proposed Standard] /127利用時のサブネットルータエニーキャストの無効化
- [Informational] NDPの問題点と対処方法
- [Proposed Standard] 送信元および宛先アドレスの選択アルゴリズム
- [Informational] RA-Guardを実装する際の注意点
- [Proposed Standard] Semantically Opaque IIDの定義
- [Best Current Practice] 不正DHCPv6サーバ対策のためのDHCPv6-Shield
- [Informational] IPv6ネットワークにおけるアドレススキャン手法
- [Best Current Practice] 端末へのIPv6アドレス割当に関する議論
- [Proposed Standard] インタフェースID生成手法のまとめ
- [Proposed Standard] RAにおけるRDNSSオプションとその必須化
- [Internet Standard] IPv6の基本仕様 (Internet Standards)
- [Internet Standard] IPv6におけるパスMTU探索 (Internet Standards)
- [Informational] 端末毎に異なるIPv6プレフィックスを配布する手法
- [Proposed Standard] DHCPv6の仕様
- [Informational] IPv6ネットワーク運用のためのセキュリティ考慮事項
- [Informational] DHCPv6-PDを利用した端末毎に異なるIPv6プレフィックス割り当て手法
- [Proposed Standard] RAにおけるDHCPv6-PDの可用性通知オプション
- SLAACとDHCPv6によるアドレス自動設定の問題
- 安全性を高めたDHCPv6
- アドレス選択機構の更新 (ULAの優先度向上)
- NDP問題の整理と解決手法
- SLAACにおける可変長IIDの議論 (**WG Documentではない点に注意**)
- SLAACにおける可変長IIDの議論 (**WG Documentではない点に注意**)