IPv6 家庭用ルータ
ガイドライン

【第 3.0 版】

2024 年 2 月 13 日

IPv6 普及･高度化推進協議会

IPv4/IPv6 共存 WG　IPv6 家庭用ルータ SWG

変更履歴

版	改版日	摘要
1.0	2009 年 6 月 22 日	若干の修正、未検討項目の作成
2.0	2010 年 7 月 29 日	アドレス利用の考察追加、ユーザーインターフェース追加、検討機能への連番付与
3.0	2024年 2月 13 日	IETF や Broadband Forum 等の国際標準化動向を反映して各技術要件を最新情報に更新

目次

1. はじめに

1.1 本ガイドラインの背景と目的

IPv6 普及・高度化推進協議会[1]IPv4/IPv6 共存ワーキンググループ(WG)IPv6 家庭用ルータサブワーキンググループ(SWG)[2]が 2010 年 7 月 29 日に公開した「IPv6 家庭用ルータガイドライン 第2版」の公開から既に 13 年が経過している。

第2版の公開後、多くの家庭用ルーター実装者及びサービス提供者(IPv6 接続サービスを提供する事業者)に本ガイドラインは参照され、IPv6 普及の一助となった。

一方、日本を含めた世界各国における IPv6 の実利用が進んでおり、IPv6 が普及することで得られた知見が国際標準文書に反映される、といったサイクルがまわっており、本 SWG においては、この間に関連ドキュメントの調査活動を行うと共に国際標準文書と IPv6 家庭用ルータガイドラインとの比較文書の発行を行ってきた。具体的には Internet Engineering Task Force[3](以降、IETF), Broadband Forum[4]等が発行したドキュメントを対象としている。この活動は、調査対象ドキュメントとガイドラインの差異を明確にするとともに、将来的なガイドラインの改版において、対象ドキュメントの内容を IPv6 家庭用ルータガイドラインに取り込むことを目的とした。

本ガイドラインは、上記国際標準および国内で得られた知見をふまえ、「IPv6 家庭用ルータガイドライン 第2版」を抜本的に見直し、「IPv6 家庭用ルータガイドライン 第3版」としてまとめたものである。本ガイドラインが家庭用ルーターの実装者における仕様検討およびサービス提供者における IPv6 接続サービス検討の一助となれば幸いである。

[1] IPv6 普及・高度化推進協議会:https://v6pc.jp/jp/
[2] IPv6 家庭用ルータ SWG:https://v6pc.jp/jp/wg/coexistenceWG/v6hgw-swg.phtml
[3] Internet Engineering Task Force:https://www.ietf.org/
[4] Broadband Forum:https://www.broadband-forum.org/

1.2 本ガイドラインの想定環境と対象とする読者

本ガイドラインで扱うインターネット接続形態は、家庭用ルーター（ユーザー宅内に設置される小型ルーター）を介して家庭内ネットワークを IPv6 接続サービス提供者と接続する環境を想定している。インターネット接続サービスは、IPv4 と IPv6 をそれぞれ提供するデュアルスタック環境のみならず、IPv6 インターネット接続サービスを基本として、その上で IPv4 接続サービスを提供する MAP-E や DS-Lite に代表される IPv6 移行技術についても想定している。

下記に検討の対象外としたネットワーク例を列挙する。

＜対象外のネットワーク環境＞
- 企業ネットワーク
- 公衆無線 LAN 等のパブリックネットワーク
- ルーターを使用せず、クライアント端末が直接接続する形態
- 複数の IPv6 サービスを契約している環境（マルチプレフィックス・マルチホーム）

また、想定する IPv6 家庭用ルーターは、汎用性を十分に考慮した上で、最低限必要とされる機能を有するものである。

尚、本ガイドラインでは、特に下記の方々を読者として想定して記述している。
- 家庭用ルーターを設計・開発する方々
- ISP 等、インターネット接続性を提供するサービスを提供されている方々

1.3 記述用語と表記方法

本ガイドラインにて記述されている用語は、IAjapan(財団法人日本インターネット協会)においてまとめている、「IPv6 関連用語集」[5]に従っている。各用語に関する解説は用語集を参照して頂きたい。用語集に記述されていない用語は下記に解説する。

表 1-1 本ガイドラインで扱う用語解説

用語	説明
ULA (RFC 4193)	Unique Local IPv6 Unicast Addresses。サイト内等、ローカル通信で利用するために制定された IPv6 ユニキャストアドレス。IPv4 のプライベートアドレス(RFC 1918)に相当するが、プレフィックスの一部をランダムに生成することが規定されており、アドレスの一意性を高めている。
TR-069	Technical Report 069。Broadband Forum の定める技術仕様の1つであり、CPE 機器を遠隔管理するためのアプリケーション層のプロトコルを定義している。具体的には、SOAP/HTTP により CPE と自動設定サーバー(ACS:Auto Configuration Server)との間の通信を定義している。
TR-124	Technical Report 124。Broadband Forum の定める技術仕様の1つであり、CPE 機器に関する機能要件をまとめたものである。
フィルターステート	RFC6092 REC-12 の ”filter state record” や REC 14 ”state record for a UDP flow” に対応する語句。(静的フィルターではなく) SPI フィルターの、TCP/UDP フロー1つに対応するフィルターの状態のこと。
ルーター	「CPE」「HGW」「家庭用ルーター」など、本文書が対象とする機器のこと。 ※内閣告示, 内閣訓令における外来語の表記に従い、本文中の表記は「ルーター」(長音符号表記)としているが、ガイドライン名称およびワーキンググループ名称は従来通り「ルータ」のままとしている。
DNS スタブリゾルバー	DNS クライアントとも呼ばれる。家庭用ルーター上で動作するリゾルバー。フルサービスリゾルバー(キャッシュ DNS サーバー)に対して名前解決を要求する機能。
DNS プロキシ	DNS フォワーダーとも呼ばれる。LAN 上のクライアントからの DNS の名前解決要求に対して代理で応答を行い、別のフルサービスリゾルバー(キャッシュ DNS サーバー)に名前解決を要求する機能のこと。

[5] IPv6 関連用語集(IAjapan):https://www.iajapan.org/ipv6/v6termwg.html

RA	IPv6 NDP の ”Router Advertisement” メッセージのこと。

1.4 ガイドライン作成にあたり

本節では、ガイドラインの構成および技術要件の記載項目について解説する。
本ガイドラインでは、以下の章立てでまとめている。
第2章は、IPv6 接続サービスを提供するサービス提供者への接続モデルについて記載。
第3章は、General Requirements(一般事項に関する要求項目)について記載。
第4章は、WAN Requirements(WAN 側機能に関する要求項目)について記載。
第5章は、LAN Requirements(LAN 側機能に関する要求項目)について記載。
第6章は、Security Requirements(セキュリティに関する要求項目)について記載。
第7章では、第3章から第6章までに定義した技術要件を一覧表としてまとめている。

以上の内容でガイドラインを構成し、技術要件の記載項目については表 1-2 に挙げる項目に整理してまとめている。

表 1-2 技術要件の記載項目説明

項目	意味
要件番号:	要件を識別するカテゴリ(以下)と番号を記載 (例. GEN-1) カテゴリ:GEN(General)／WAN／LAN／SEC(Security)
前提条件:	要件に対する前提条件を記載
要件:	要件の概要を記載
要件詳細:	要件内容の詳細や補足的な事項を記載
理由:	当該要件を必要とする事由を記載
必要度:	技術要件の必要性を、「必須／推奨／オプション」のいずれかで記載 必須(MUST):必ず必要とされる機能 推奨(SHOULD):実装されていることが推奨される機能 オプション(MAY):実装はルーターとしての付加価値的なもの(サービス依存な機能等)であるため任意でよい機能 ※前提条件がある場合の必要度は、前提条件となる技術要件の必要度が上位の必要度となっている。 (例) 前提条件となる技術要件の必要度が MAY で、当該技術要件の必要度が MUST の場合、前提となる技術要件を実装しない場合は、当該技術要件を満たす必要はない。

出典：	技術要件の参考情報を記載 ※出典の多い「IPv6 家庭用ルータガイドライン」第 2 版、IETF RFC 文書 　および Broadband Forum TR-124 Issue 5 文書のリンクは以下 「第 2 版」: IPv6 家庭用ルータガイドライン 第 2 版 https://www.v6pc.jp/jp/upload/pdf/v6hgw Guideline 2.0.pdf IETF RFC https://www.rfc-editor.org/rfc-index.html Broadband Forum TR-124 Issue 5 https://www.broadband-forum.org/pdfs/tr-124-5-0-0.pdf
備考：	要件を実装するにあたって参考となる情報を記載

2. サービス提供者への接続モデル

この章では、サービス提供者が提供するインターネット接続サービスを利用する際に、家庭用ルーターが必要とされる接続モデルに関してまとめる。

2.1 IPv6 接続モデル

この節では、エンドユーザーがインターネットで IPv6 通信するための、家庭用ルーターとサービス提供者の接続モデルを提示する。

2.1.1 ネイティブ接続

家庭用ルーターで PPP 等によるトンネルを終端することなく、IPv6 インターネットへのリーチャビリティを提供するモデルである。

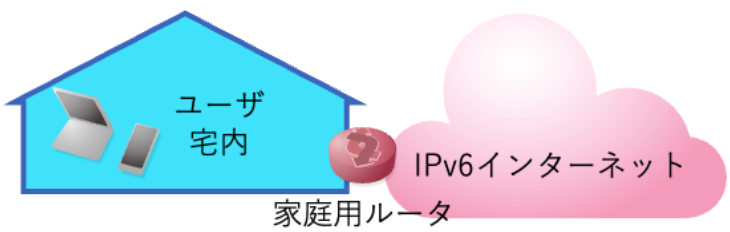

図 2. 1 ネイティブ接続

2024年2月時点、ネイティブ接続が行えるサービスとしては、NTT 東西のフレッツ光(インターネット接続には別途 VNE を経由)、KDDI の au ひかり(KDDI の独自回線あるいはダークファイバー利用の場合)、ソニーネットワークコミュニケーションズ株式会社の NURO 光、J:COM 等の CATV 網を利用するサービス、各 MNO(株式会社 NTT ドコモ、KDDI 株式会社、ソフトバンク株式会社、楽天モバイル株式会社)が提供する移動通信網を利用するサービス等がある。

2.1.2 PPPoE

PPP によるトンネルを利用して、ユーザー宅内へ IPv6 インターネットへのリーチャビリティを提供するモデルである。

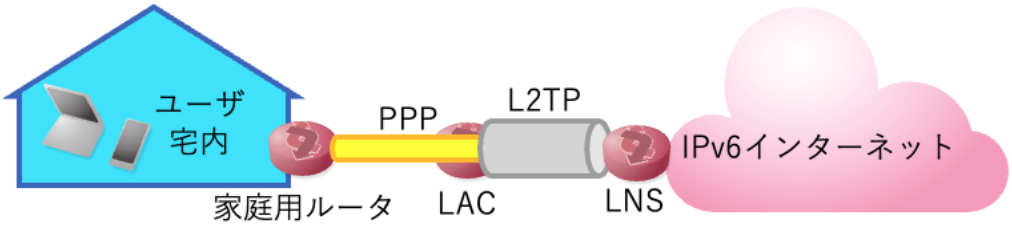

図 2. 2 PPPoE 接続

2024 年2月現在、PPPoE を利用するサービスとしては、NTT 東西のフレッツ光(インターネット接続には別途 ISP を経由)、株式会社オプテージの eo 光ネット、中部テレコミュニケーション株式会社(ctc)のコミュファ光がある。

2.2 IPv4 インターネットへの接続性提供技術

この節では、インターネットのプロトコルとして IPv6 が普及する中で、エンドユーザーが IPv4 通信を継続するためのネットワークモデルを紹介する。

2.2.1 DS-Lite

サービス提供者が IPv4 NAT 機能と IPv4 over IPv6 トンネル終端機能を備えた装置 AFTR (DS-Lite Address Family Transition Router element)を IPv4 Internet と CPE の間に新たに設置し、さらに、CPE を B4 (DS-Lite Basic Bridging BroadBand element) として IPv4 over IPv6 トンネル終端機能を備え、CPE の NAPT 機能を不要とする方式である。[6]

これまでは通常、CPE の WAN 側インターフェースに1つグローバルアドレスを付与しインターネットとの IPv4 での通信をしてきたが、DS-Lite 方式においては、CPE(B4)から AFTR を介し、複数のユーザーで1つのグローバル IPv4 アドレスを共有する(NAT444 モデルと同様)。さらに、B4 と AFTR の間では、IPv4 パケットを IPv4 over IPv6 カプセル化した上で IPv6 を用いてパケット転送する。

ユーザー端末から IPv4 Internet に向けて送信されたパケットは B4 において IPv6 でカプセル化され、AFTR に転送される。AFTR では、IPv6 カプセル化を解いて IPv4 パケットに戻し、さらに IPv4 NAT を実施しインターネットに転送する。

[6] RFC 6333: Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion

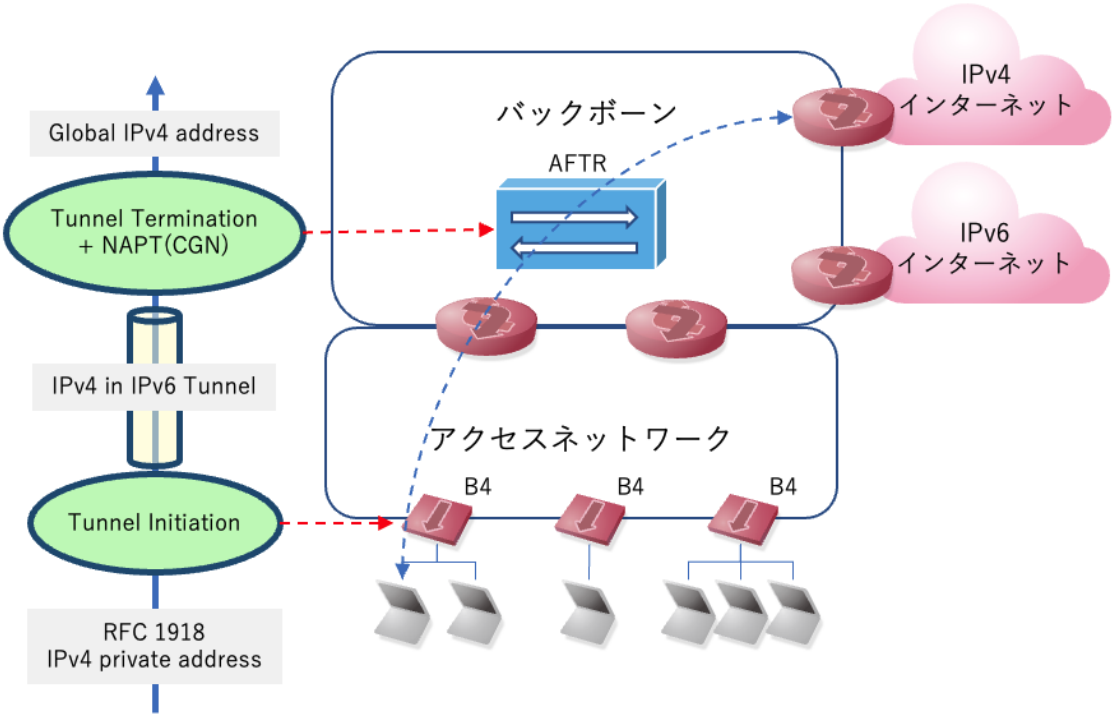

図 2. 3 DS-Lite のネットワーク構成図

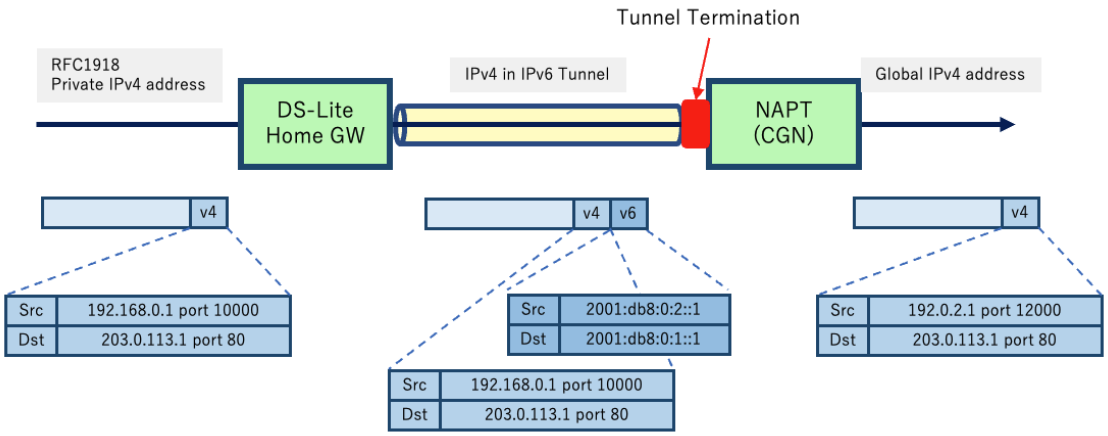

図 2. 4 DS-Lite のパケットフロー

このモデルの特徴は以下の通りである。

- CPEにB4機能が必要となる
- NATはAFTRで行われる一段のみである

- アクセスネットワークはIPv6 onlyでよい
- AFTRでセッション状態を保持する必要があり、スケーラビリティに懸念がある（B4とAFTR間はトンネリングのため、AFTRの配置に自由度が高く、AFTRの増強によるスケーラビリティ拡大はある程度可能である）
- AFTRとB4においてトンネル処理が必要である
- NAT越えが必要なアプリケーションや、膨大なセッションを必要とするアプリケーションに影響が出る可能性がある
- AFTRでのNATの処理は既存のNATとは異なる

2024 年2月現在、DS-Lite を利用するサービスは、インターネットマルチフィード株式会社の transix、アルテリア・ネットワークス株式会社のクロスパス、株式会社朝日ネットの v6 コネクト等が提供している。

2.2.2 MAP-E

これまでサービス提供者は、CPE に対して IPv4 アドレス 1 個を割り当て、TCP や UDP のポート番号は特に制限をしていなかった。このモデルでは、サービス提供者は複数のユーザーにグローバル IPv4 アドレス 1 個と、それらのユーザー毎に異なるポート番号の範囲（例えば、あるユーザーに対し 4096～8191、別のユーザーに対し 8192～12287 でそれぞれ 4096 個）を指定し割り当てることで、複数の CPE（ユーザー）間で1つのグローバル IPv4 アドレスを共有する。[7]

サービス提供者は IPv4 インターネットから CPE に向けて転送するパケットを、終点ポート番号に基づいて CPE に振り分ける機能を備えた MAP-E BR（Border Relay）を設置する。振り分けた後のパケットは、IPv4 over IPv6 カプセル化された上で MAP-E CE に転送される。

NAT 444 の CGN[8]や、DS-Lite の AFTR と違い、MAP-E BR では IPv4 NAT の機能なしで、グローバル IPv4 アドレスを同一サービス提供者の複数のユーザーで共有することができる。そのため、NAT444 モデルにおける LSN 等、個々の TCP セッション等に対する NAPT の状態を管理する必要があるモデルと比べて、管理情報が少なくなる。

MAP-E の導入には、CPE の置き換えが必要なこと、サービス提供者網内に MAP-E BR ルーターの設置が必要なこと、ICMP 等ポート番号に依存していないプロトコルが使用できなくなること、特定ポート使用のアプリケーションに対策が必要なこと等課題が多い。

[7] RFC 7597: Mapping of Address and Port with Encapsulation（MAP-E）

[8] CGN: Carrier Grade NAT。RFC 6598 で定めるシェアードアドレスを用い、通信事業者で実施される大規模な NAPT。

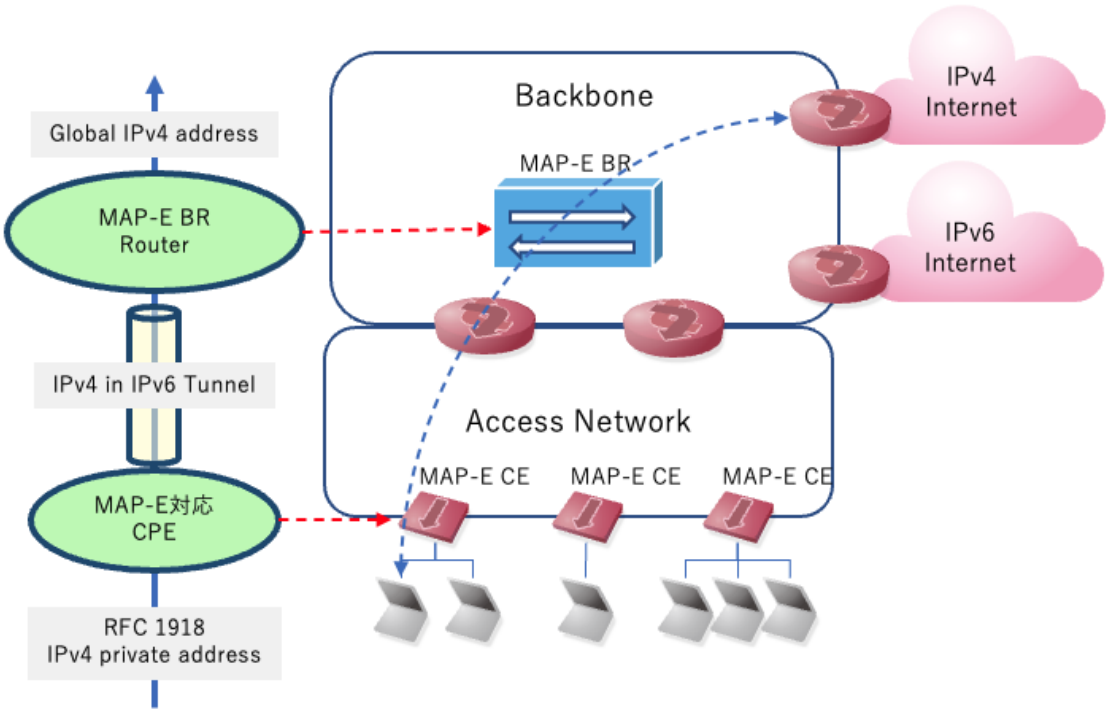

図 2. 5 MAP-E のネットワーク構成図

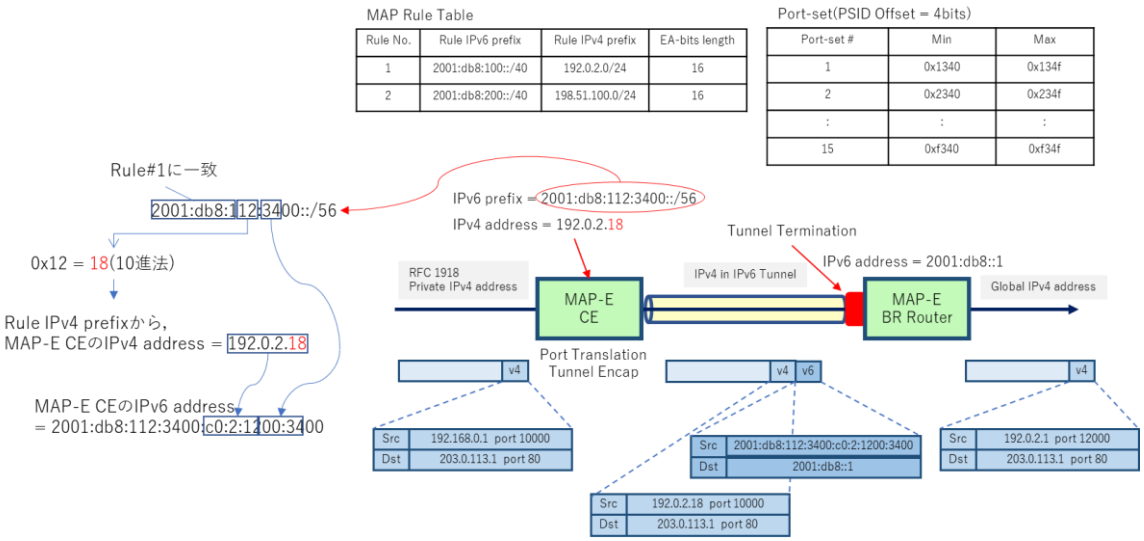

図 2. 6 MAP-E のパケットフロー

2024 年2月現在、株式会社 JPIX の v6 プラス、ビッグローブ株式会社の IPv6 オプションで MAP-E を採用している。

2.2.3 NAT64

NAT64 と DNS64 を利用して、IPv6 only のクライアントから IPv4 サーバーへのアクセスを実現するモデルである。[9]

図 2.7 においてまず、IPv6 only のクライアントから DNS64 サーバーに、www.example.jp の IPv6 アドレスを問合わせる。DNS64 サーバーでは www.example.jp を名前解決し、その解決された IPv4 アドレスを含める形で、Translator にルーティングされる IPv6 アドレスを作成し、それを IPv6 only クライアントからの問合わせの返答として答える(DNS64)。それを受け取った IPv6 only クライアントはその IPv6 アドレスへ通信しようとするが、その IPv6 パケットは NAT64 装置にルーティングされる。NAT64 装置では IPv6 パケットから IPv4 パケットに変換し、終点アドレスを実際の www.example.jp のアドレスである IPv4 アドレスに変換し、通信を行う。

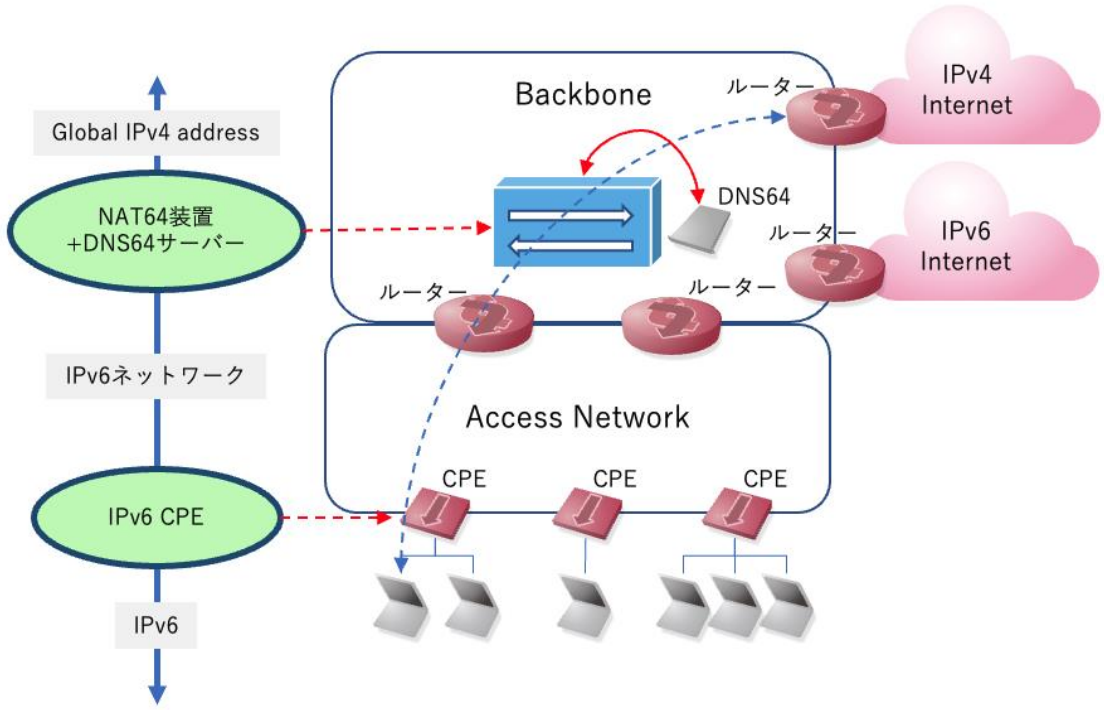

図 2. 7 NAT64 のネットワーク構成図

[9] RFC 6146: Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers

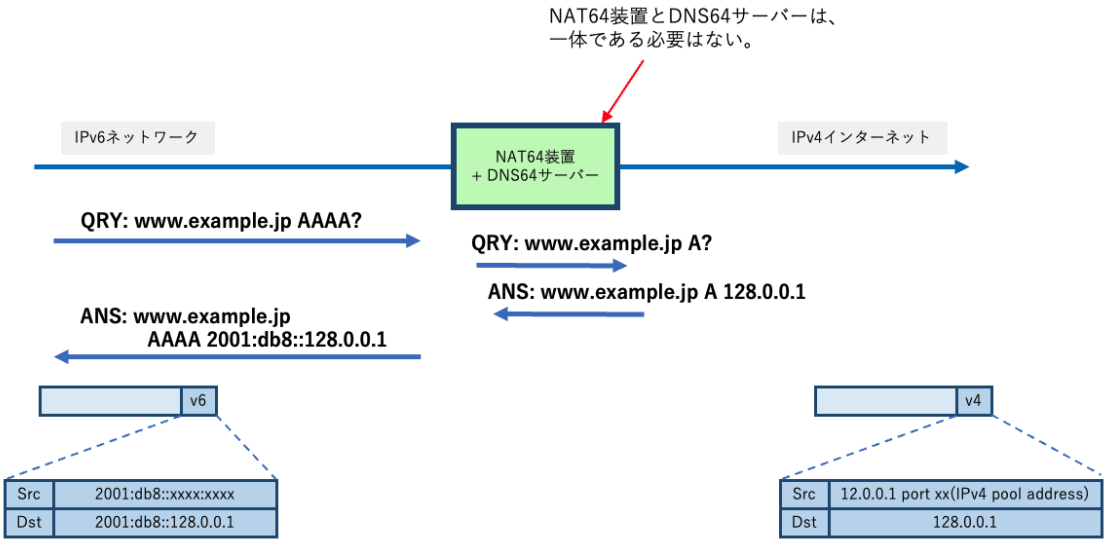

図 2. 8 NAT64 のパケットフロー

2024 年2月現在、株式会社 NTT ドコモが IPv6 シングルスタック方式で、ビッグローブ株式会社等が NAT64/DNS64 サービスで NAT64 を採用している。

2.2.4 464XLAT

NAT64 と SIIT(Stateless IP/ICMP Translation algorithm)を利用して、ステートレストランスレーションとステートフルトランスレーションの組み合わせにより、IPv6 ネットワーク経由で IPv4 インターネット接続を実現するモデルである。[10]

図 2.9 における IPv4 クライアントからインターネットを経由した IPv4 通信では、まず IPv4 クライアントから CLAT[11] を介し IPv6 アドレスへの変換が行われ、IPv6 インターネットを経由して PLAT[12] によりアドレスが IPv4 へ再変換され、通信先の IPv4 ホストにアクセスする。

[10] RFC 6877: Combination of Stateful and Stateless Translation

[11] CLAT: Customer side translator。RFC 7915 に準拠したステートレスで、プライベート IPv4 アドレスとグローバル IPv6 アドレスの変換を行う。

[12] PLAT: Provider side translator。RFC 6146 に準拠したステートフルトランスレーターで、グローバル IPv6 アドレスとグローバル IPv4 アドレスの 1:n 変換を行う。

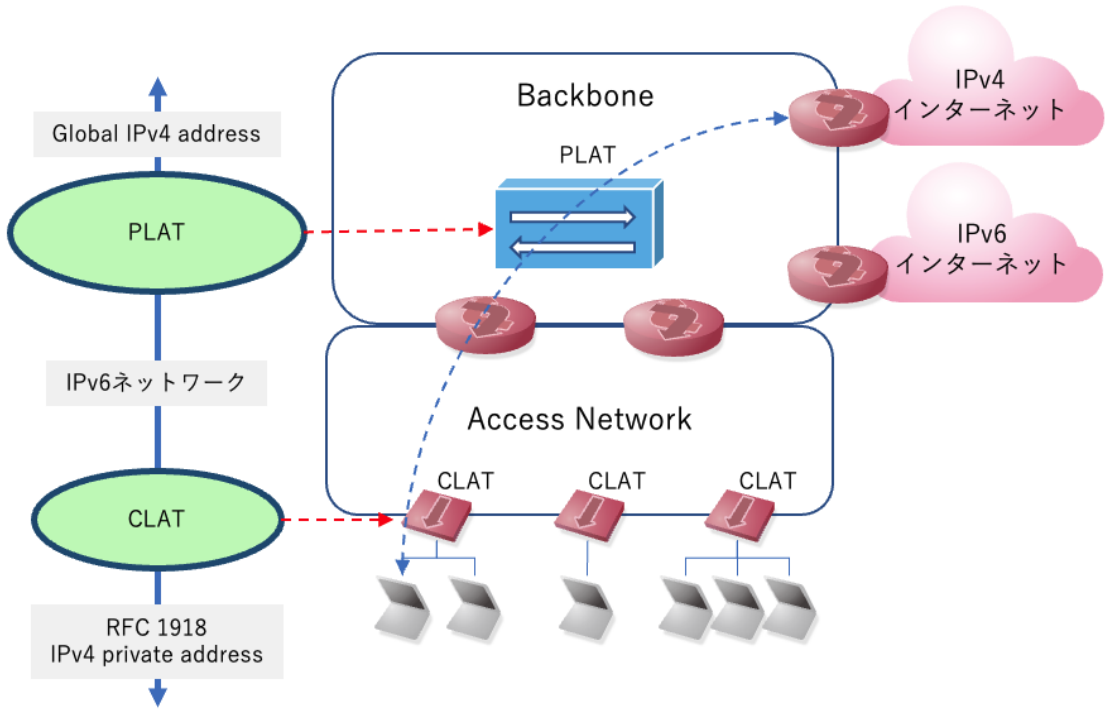

図 2. 9 464XLAT のネットワーク構成図

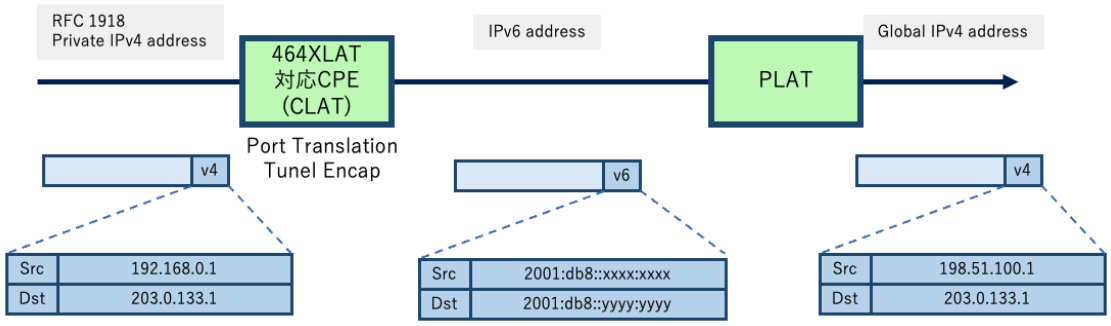

図 2. 10 464XLAT のパケットフロー

2024 年2月現在、464XLAT は、NTT ドコモが IPv6 シングルスタック方式で採用している。[13]

[13] アドレス利用拡大に向けたドコモの取り組み
https://www.janog.gr.jp/meeting/janog48/wp-content/uploads/2021/05/janog48-ipv6-minakuchi-kunitomo-aikawa.pdf

2.2.5 HB46PP（HTTP-Based IPv4 over IPv6 Provisioning Protocol）

2020 年 8 月に日本国内において、IPv4 over IPv6 のプロビジョニング方式の標準化を図ったものとして HB46PP が作成された。[14]

2024 年2月現在、HB46PP に準拠する機器は NEC プラットフォームズ株式会社、株式会社アイ・オー・データ機器、株式会社バッファロー、エレコム株式会社、アライドテレシス株式会社、日本電気株式会社、古河電気工業株式会社等から、サービスは株式会社朝日ネット、ビッグローブ株式会社から提供されている。

[14] IPv6 マイグレーション技術の国内標準プロビジョニング方式【第 1.1 版】
https://github.com/v6pc/v6mig-prov/blob/1.1/spec.md

3. 一般の要求事項（GEN）

要件番号：GEN-1

要件：DNS プロキシもしくは DNS スタブリゾルバーは、DNS サーバーに問合せを行う際に IPv4 トランスポートと IPv6 トランスポートのいずれも利用可能であること。

理由：サービス提供者から指定される DNS サーバーアドレスが IPv4、IPv6 いずれの場合であっても対応可能とするため。

必要度：必須（MUST）

出典：第2版 要件 18

要件番号：GEN-2

要件：DNS プロキシは、端末からの問合せをトランスポートに関わらずサービス提供者の要求するトランスポートに変換できること。

理由：サービス提供者から指定される DNS サーバーアドレスが IPv4、IPv6 いずれの場合であっても対応可能とするため。

必要度：必須（MUST）

出典：第2版 要件 19

要件番号：GEN-3

要件：DNS プロキシは、IPv4 および IPv6 の DNS サーバーが共に利用可能な場合は、端末からの DNS 問合せが IPv4 であるか IPv6 であるかに関わらず、IPv6 の DNS サーバーに対して IPv6 トランスポートを使用してプロキシ動作を行うこと。

理由：多くの実装において IPv6 を優先する実装となっているため。

必要度：推奨（SHOULD）

出典：第2版 要件 20, TR124i5 LAN.DNSv6.6

要件番号：GEN-4

要件：DNS プロキシとして待ち受けるアドレスの種類は、ユニキャストアドレス（グローバルアドレス、ULA、リンクローカルアドレスの内いずれか）で待ち受け可能であること。

理由：少なくともいずれかのユニキャストアドレスで待ち受ける必要があるため。

必要度：必須（MUST）

出典：第2版 要件 21

備考：DNS プロキシがグローバルアドレスで待ち受ける場合、上位回線の切断時あるいはセットアップ未完了時等、DNS プロキシにグローバルアドレスが付与されていない状態が存在することが考えられる。この時、DNS プロキシには問合せのパケットが到達しないため注意が必要である。
DNS プロキシが ULA で待ち受ける場合、DNS プロキシにはあらかじめ使用する ULA を定義しておく必要がある。
DNS プロキシがリンクローカルアドレスで待ち受ける場合、他のセグメントからの問合せは DNS プロキシに到達しない。また、リンクローカルアドレスが指定できない端末リゾルバーが存在する可能性があるため注意が必要である。

要件番号：GEN-5

要件：DNS サーバー情報を手動設定できること。

理由：サービス提供者から自動取得できない場合も想定されるため。

必要度：推奨（SHOULD）

出典：第2版 要件 61

要件番号：GEN-6

要件：各種サーバーアドレスを手動設定できること。

理由：サービス提供者から自動取得できない場合も想定されるため。

必要度：推奨（SHOULD）

出典：第2版 要件 63

要件番号：GEN-7

要件：ユーザーからの設定を受け付けるために HTTP（80/tcp）もしくは HTTPS（443/tcp）による WebUI の設定インターフェースは IPv6 トランスポートに対応すること。

理由：IPv6 トランスポートに対応することで、ユーザー設定の利便性を高めることができるため。ただし、IPv4 トランスポートのみの場合でも最低限の機能提供が可能であるため、必要度は推奨とする。

必要度：推奨（SHOULD）

出典：第2版 要件 64

備考：セキュリティの観点からは HTTPS を使用することが望ましい。

要件番号：GEN-8

要件：ユーザーからの設定を受け付けるために SSH（22/tcp）による CLI（Command Line Interface）の設定インターフェースは IPv6 トランスポートに対応すること。

理由：IPv6 トランスポートに対応することで、ユーザー設定の利便性を高めることができるため。ただし、IPv4 トランスポートの場合においても家庭用ルーターでは必須機能でない為、必要度はオプションとする。

必要度：オプション（MAY）

出典：第2版 要件 65

備考：セキュリティの観点からは TELNET は除外している。

要件番号：GEN-9

要件：設定インターフェースにおいて、IPv6 アドレス/プレフィックスの入力を求める場合は、RFC4291 に規定されている表記が入力可能なこと。

理由：省略表記での入力または省略しない表記での入力いずれについても入力可能とすることでユーザー設定の利便性を高めることができるため。

必要度：推奨（SHOULD）

出典：第2版 要件 66, RFC4291

要件番号：GEN-10

要件：IPv6 アドレス／プレフィックスの出力表記は、RFC5952 に規定されている推奨表記に対応すること。

理由：IPv6 アドレス表記は省略表記が可能となっているため、同じアドレスであっても異なるアドレスに見えてしまうなど、エンドユーザーやカスタマサポート等にて誤認する可能性があるため。

必要度：推奨（SHOULD）

出典：第2版 要件 67, RFC5952

要件番号：GEN-11

要件：IPv6 トランスポートでのファームウェアのアップデートが可能であること。

理由：新機能が追加された場合や、新たに発見された脆弱性を解消する必要があるため。

必要度：必須（MUST）

出典：第2版 要件 59

要件番号：GEN-12

要件：ファームウェアを安全に更新する方法を提供すること。

要件詳細：ルーターは、セキュリティアップデートやその他ベンダーが推奨する更新を適用するために、ファームウェアを更新する手段を提供することが推奨される。なお、不正なファームウェアを排除する仕組みや、自動的に更新を適用する仕組みを備えることが望ましい。

必要度：推奨（SHOULD）

出典：第 2 版 要件 59, RFC6092

コラム：IPv6 対応 UPnP の最新状況

本ガイドラインにおいては、国内/海外における IPv6 対応 UPnP の普及が十分に進んでいない状況を鑑み、技術要件として記述していない。

尚、本ガイドラインにて多くの参照を行っている Broadband Forum 発行の TR124i5 においては、UPnP の IGD version 2 仕様のサポートが MUST 要件となっている。

Universal Plug and Play(UPnP) [15]は、コントロールポイント(制御する側)とデバイス(制御される側)を構成要素として、機器をネットワークに接続した際に複雑な設定作業などを行わなくても、即座に他の機器と通信、あるいは機器が持つ機能またはサービスを利用可能とするプロトコルである。

2024 年2月現在、Open Connectivity Foundation(OCF)が UPnP および UPnP+ の技術仕様に関する標準化および認証取得のための審査機関として活動を行っている。家庭用ルーターは一般的に UPnP のデバイスとして用いられる。その観点から見ると、Device Control Protocol(DCP)の1つとして定義されている Internet Gateway Device(IGD)仕様をサポートすることと同義であり、UPnP の IPv6 対応を行うためには、IGDversion 2 仕様のサポートが必要となる。

OCF では、UPnP 認証および UPnP+認証を取得した製品のリストを公開[16]しているが、2021 年 9 月以降、IPv6 対応の UPnP 認証を取得するルーターベンダが増加傾向にある。(当該リストは、認証取得を非公開としているルーターベンダは含まれていないことに注意)

また、国内においては、株式会社コナミデジタルエンタテインメントとNECプラットフォームズ株式会社が IPv6 対応 UPnP の相互接続検証を行い、IPv6 UPnP 対応製品がリリース[17]されている状況であり、ゲーム機器をはじめとする宅内機器の IPv6 利用時の接続性改善に向けた取り組みが始まっている。

UPnP の IPv6 対応を行う際には、OCF が公開している UPnP 技術仕様および TR124 を参照すること。尚、UPnP のセキュリティ懸念については、UPnP 技術仕様に記載の Device Protection の実装要否の検討およびセキュリティリスクへの対処方法について適切な実装を行うべきである。

---

[15] UPnP Standards & Architecture
https://openconnectivity.org/developer/specifications/upnp-resources/upnp/

[16] Announced Certified Product Registry
https://openconnectivity.org/certified-products/

[17] Aterm が IPv6 による新世代 UPnP に対応！ KONAMI との共同検証で実現したピンホール制御で、ゲームも IoT も IPv6 直接接続へ
https://internet.watch.impress.co.jp/docs/column/shimizu/1538789.html

4. WAN の要求事項（WAN）

要件番号：WAN-1

要件：ND プロキシもしくは、IPv6 ブリッジ機能をサポートすること。

要件詳細：WAN 側より割り当てられたプレフィックス長が/64 であった場合、ND プロキシ、もしくは、IPv6 ブリッジとして動作し内部（LAN）と外部（WAN）の双方向に IPv6 パケット（EtherType：0x86DD に相当するパケット）を透過させる機能を有すること

理由：DHCPv6-PD によるプレフィックス割り当てが行われず、GUA の割り当てのみが行われるネットワークであっても、ルーターの内部（LAN）から外部（WAN）との通信を可能とするため。

必要度：必須（MUST）

出典：TR124i5 WAN.BRIDGE.4

要件番号：WAN-2

要件：ND プロキシもしくは、IPv6 ブリッジ機能は IPv4 の動作状態・設定に依存せず、独立した設定が用意されていること。

理由：IPv4 の接続モデルと IPv6 の接続モデルは独立したネットワークで構成される為、それぞれの接続モデルに依存しない設定が可能である必要がある。

必要度：必須（MUST）

出典：TR124i5 WAN.BRIDGE.5

要件番号：WAN-3

要件：複数の WAN インターフェースを有する場合、家庭用ルーターは、WAN インターフェース毎に独立した ND プロキシ、または IPv6 ブリッジいずれかの設定が行えること。

理由：複数の回線への接続を可能とする場合、それぞれの回線毎に接続形態が異なる可能性があり、回線毎に独立した動作・設定が必要である。

必要度：必須（MUST）

出典：TR124i5 WAN.BRIDGE.6

要件番号：WAN-4

要件：ND プロキシまたは、IPv6 ブリッジ動作する場合、家庭用ルーターは WAN 側インターフェースにおいて、IPv6 ルーターとして動作せず、IPv6 ホストとしてふるまうこと。

要件詳細：IPv6 ホストとして SLAAC や DHCPv6 IA_NA を利用し、IPv6 ルーター機能である DHCPv6 IA_PD は利用しないこと。

必要度：必須（MUST）

出典：TR124i5 WAN.BRIDGE.7

要件番号：WAN-5

要件：TR124i5 Annex A.2 のフローに従った IPv6 接続の自動確立機能を有すること。

必要度：推奨（SHOULD）

出典：TR124i5 WAN.IPv6.1

要件番号：WAN-6

要件：RFC 8415 に準拠した DHCPv6 クライアント機能を有すること。

必要度：必須（MUST）

出典：TR124i5 WAN.IPv6. Item 4,5

要件番号：WAN-7

要件：SLAAC（StateLess Address AutoConfiguration）により WAN 側インターフェースへのグローバルアドレスを自動的に付与できる機能を有すること。

必要度：必須（MUST）

出典：RFC4862, TR124i5 WAN.IPv6.9

要件番号：WAN-8

前提条件：WAN-6

要件：DHCPv6 による RFC3646 に準拠した DNS Search List オプションに対応すること。

理由：国内では、ISP 毎に固有の本オプションが配布されているため。

必要度：必須（MUST）

出典：RFC3646, TR124i5 WAN.IPv6.14

要件番号：WAN-9

要件：PPP セッションに利用するパスワードは全て保存できること。また、保存されたパスワードは他の目的（他インターフェースへの表示、照合、通知など）に利用しないこと。

理由：不慮の事態により PPP セッションが切断された等の場合においても、事前に入力されたパスワードを用いてセッションを復旧するため。

必要度：推奨（SHOULD）

出典：TR124i5 WAN.PPP.6

備考：TR-124i5 において同項目は MUST となっているが、本書においてはパスワード等の扱いについては利便性を鑑み、SHOULD とする。

要件番号：WAN-10

要件：PPP セッションが接続されているインターフェースが物理的に切断された場合でも、2 分間はセッションを維持し、その間にインターフェースの接続が回復した場合、セッションの維持を試みること。それが拒否、もしくは時間が経過した場合、元のセッションを切断し、新規にセッションの接続を試みること。

理由：複数の PPP セッションの同時利用が許容されない場合等において、物理的な切断は上流の PPP サーバー側に通知されず、新規セッションの接続ができない場合を考慮し、短時間の切断においては PPP セッションを維持する必要があるため。

必要度：推奨（SHOULD）

出典：TR124i5 WAN.PPP.7

備考：TR-124i5 においては本項は MUST となっているが、接続先や接続目的によって異なるケースもあることから、本項は SHOULD とする。

要件番号：WAN-11

要件：起動後、各IP通信及びPPPセッションを開始する前に、ランダムな遅延処理を組み込むこと。

理由：不特定多数のユーザーが一斉に機器を再起動するような何らかの要因（停電による一斉復旧など）が発生した際、ランダムな開始遅延を組み込むことで、負荷集中による接続障害の発生を軽減するため

必要度：推奨（SHOULD）

出典：TR124i5 WAN.PPP.8

要件番号：WAN-12

要件：PPP 接続時、認証エラーとなった場合、試行回数に応じて間隔を延長すること。

理由：ユーザーの入力ミスなどによって発生する可能性の高い認証エラーについては、再試行による回復の見込みが低く、回線への負荷とならないよう早期に再試行間隔を延長する必要があるため。

必要度：推奨（SHOULD）

出典：TR124i5 WAN.PPP.9

要件番号：WAN-13

要件：LAN 側機器から出された PPPoE セッションを確立できるよう WAN インターフェースに双方向転送できること。（PPPoE パススルー機能）

理由：複数の PPPoE セッションを許容するサービスを利用している場合でも、物理的にWAN側ネットワークに複数台接続できないケースが多く、LAN 側からの PPPoE セッション要求をWAN 側に通すことで複数の PPPoE セッションをユーザーに提供できるため。

必要度：必須（MUST）

出典：TR124i5 WAN.PPP.10

備考：ルーター自身が PPPoE セッションを確立している場合でも、本要件を満たすことが望ましい。

要件番号：WAN-14

要件：IPv6 over PPPoE をサポートするルーターは RFC 5072 に則した IPv6 over PPP をサポートすること。

必要度：必須（MUST）

出典：TR124i5 WAN.PPP.IPv6.1

要件番号：WAN-15

要件：PPP 接続に対して、IPv4 通信、IPv6 通信、IPv4/IPv6 両方の通信、のいずれにおいても選択できること。

必要度：推奨（SHOULD）

出典：TR124i5 WAN.PPP.IPv6.3

要件番号：WAN-16

要件：ルーターに複数の PPPoE 接続先が設定できる場合、すべての接続先のユーザー/パスワード設定を同一にし、ドメインのみ異なるように設定できること。

必要度：オプション（MAY）

出典：TR124i5 WAN.PPP.IPv6.4

要件番号：WAN-17

要件：想定した事業者サービスに応じた IPv4 over IPv6 接続（DS-Lite かつ MAP-E）の実装を行うこと。

理由：国内の各 VNE 事業者が提供する IPv4 over IPv6 接続の普及に伴い、IPv4 接続を行うために必要であるため。

必要度：推奨（SHOULD）

出典：RFC 8585

備考：2024 年2月現在、国内で一般的に利用されている上記2つの方式を記述している。

要件番号：WAN-18

前提条件：WAN-17

要件：RFC6333 に準拠した DS-Lite 方式による IPv4 接続に対応した機能を有すること。

理由：必要度は前提条件に合わせて、推奨（SHOULD）とする。

必要度：推奨（SHOULD）

出典：RFC6333, TR124i5 WAN.TRANS.DS-LITE.1

要件番号：WAN-19

前提条件：WAN-18

要件：DS-Lite 方式 の設定手法を用意すること。

要件詳細：
想定した事業者サービスに応じて実装を行うこと。
国内標準
・IPv6 マイグレーション技術の国内標準プロビジョニング方式による設定（自動）

国内独自
・AFTR 情報配信サーバーより AFTR 情報受信による設定
国際標準
・AFTR に FQDN を指定し、DHCPv6 により名前解決を行う設定（手動）
・AFTR にグローバルアドレスを指定する設定（手動）
・Broadband Forum TR-069 による設定（自動）
・DHCPv6 オプションによる設定（自動）

必要度：必須（MUST）

出典：RFC2473, RFC6333, RFC6334, TR124i5 WAN.TRANS.DS-LITE.6-8

要件番号：WAN-20

前提条件：WAN-17

要件：RFC7597 に準拠した MAP-E 方式による IPv4 接続に対応した機能を有すること。

要件詳細：国内サービスでは、RFC7597 ではなく draft-ietf-softwire-map-03 が使用されている。

理由：必要度は前提条件に合わせて、推奨（SHOULD）とする。

必要度：推奨（SHOULD）

出典：RFC7597, draft-ietf-softwire-map-03, TR124i5 WAN.TRANS.MAP-E.1

要件番号：WAN-21

前提条件：WAN-20

要件：MAP-E 方式の設定手法を用意すること。

要件詳細：
想定した事業者サービスに応じて実装を行うこと。

国内標準
・IPv6 マイグレーション技術の国内標準プロビジョニング方式による設定（自動）
国内独自
・MAP ルール配信サーバーより MAP ルールの受信による設定（自動）
国際標準
・Broadband Forum TR-069 による設定（自動）
・DHCPv6 オプションによる設定（自動）

理由：
必要度は本実装方法の中での選択を必須とするため必須（MUST）。

必要度：必須（MUST）

出典：RFC7597, RFC7598, TR069, TR124i5 WAN.TRANS.MAP-E.2

要件番号：WAN-22

前提条件：WAN-20, WAN-21

要件：MAP-E 方式において、RFC7597 に準拠したメッシュモードおよびハブアンドスポークモードに対応すること。

理由：サービス事業者がどちらのモードを採用するかわからないため、両モードを対応する。

必要度：必須（MUST）

出典：RFC7597, TR124i5 WAN.TRANS.MAP-E.6

備考：
メッシュモードでは IPv6 網内での P2P 通信により、より効率的な通信が行える。
ハブアンドスポークモードでは障害発生時の原因が確認しやすい。

要件番号：WAN-23

要件：宅内用 IPv6 プレフィックス情報を接続サービス提供者から DHCPv6-PD にて取得できること。

理由：DHCPv6-PD は IPv6 プレフィックス割り当てを自動に実施するための標準プロトコルであり、ユーザー手入力による設定ミスをなくすため。

必要度：必須（MUST）

出典：第2版要件 1

要件番号：WAN-24

要件：/48～/64 の幅でサービス提供者が割り当てたプレフィックスを受信できること。

必要度：必須（MUST）

出典：第2版要件 3

備考：割り当てプレフィックスサイズは無線セグメント／有線セグメントの分離や
DMZ の設置等も考えられるので、複数セグメント（/64 より短いプレフィックス
長）の分配が望ましいと考えるが、サービス提供者が決定する部分である。
IPv6 アドレス割り当てポリシーについては、以下のドキュメントを参考とする。
Broadband Forum TR-177
RFC6177
JPNIC におけるIPv6 アドレス割り振りおよび割り当てポリシー

（http://www.nic.ad.jp/doc/jpnic-01272.html）

要件番号：WAN-25

要件：SLAAC、DHCPv6 の両方式をサポートし、いずれかの方法で WAN 側インターフェースにグローバルアドレスを付与できること。

理由：ユーザーの手を介さない自動設定を実現するため。

必要度：必須（MUST）

出典：第2版要件4, RFC7084

備考：アドレスを付与する際に SLAAC と DHCPv6 のどちらの方式が利用されるかはサービス提供者に依存する。しかしながら、アドレスの自動付与方式としては両方式のどちらかを利用することになるため、両方式を必須とすることで WAN 側にアドレスを割り当てないサービスにも対応可能となる。SLAAC と DHCPv6 のどちらを利用するかをユーザーに設定させず自動判別させることも可能と考えられる。

要件番号：WAN-26

要件：WAN 側インターフェースへのグローバルアドレスを手動で付与できること。

理由：自動設定が前提であるが、手動設定も必要であるため。

必要度：必須（MUST）

出典：第2版要件 5

要件番号：WAN-27

要件：WAN 側インターフェースにグローバルアドレスが付与されていない場合に、ユーザーに割り当てられたプレフィックス内のアドレスを使って通信できること。

理由：WAN 側にグローバルアドレスが付与されないサービスモデルの場合でも、ルーター自身がパケットを送受信する必要があるため。

必要度：必須（MUST）

出典：第2版要件6

備考：DNS プロキシ等として動作する際には本機能が必要となる。
LAN 側のアドレスを使用する仮想インターフェースにアドレスを付与する等が
考えられるが、使用するアドレスをどのように生成するかは、本文書では規定しない。

要件番号：WAN-28

要件：割り当てられたプレフィックス宛てのトラフィックを上流にフォワードしない機能を持つこと。

理由：Hop Limit が 0 になるまでパケットが家庭用ルーターとサービス提供者ルーター間でピンポンすることを防ぐため。

必要度：必須（MUST）

出典：第2版要件 43

要件番号：WAN-29

要件：Point-to-Point リンクのルーターにて、自インターフェース以外のユニキャストアドレス宛のパケットを受け取った際には ICMPv6 Destination Unreachable messages, Code 3（Address unreachable）を送出し、パケットを転送しないこと。

理由：Hop Limit が 0 になるまでパケットが家庭用ルーターとサービス提供者ルーター間で ピンポンすることを防ぐため。

必要度：必須（MUST）

出典：第 2 版 要件 44, RFC4443

要件番号：WAN-30

要件：WAN 向けのスタティックルートが設定できること。

理由：デフォルトルート等ルーターにて明示的に設定をする機能が最低限必要なため。

必要度：推奨（SHOULD）

出典：第 2 版 要件 45

要件番号：WAN-31

要件：RA を利用してのデフォルトルートが自動設定できること。

必要度：必須（MUST）

出典：第 2 版 要件 46, RFC 4862

備考：複数の WAN インターフェースが存在し、複数の RA を受信する場合にはどちらのデフォルトルートを優先するか判断する必要がある。

要件番号：WAN-32

要件：家庭用ルーターを通過する TCP 通信に対して、MSS（Maximum Segment Size）オプションを適切に調整する機能を有すること。

理由：アクセス回線の MTU 値が宅内ネットワークの MTU 値より小さい場合に、新規 TCP 通信が開始される度にパス MTU 探索が実行され通信効率が低下するため。

必要度：オプション（MAY）

出典：第 2 版 要件 55

要件番号：WAN-33

前提条件：WAN-6

要件：DNS サーバーアドレスを接続先サービス提供者から DHCPv6 にて取得できること。

理由：ルーターへ配布される各種サーバー情報は、提供するサービスに応じて異なることが一般的であり、必要な情報を選択的に配布できる方式が望ましいため。

必要度：必須（MUST）

出典：第 2 版 要件 62

要件番号：WAN-34

前提条件：WAN-6

要件：各種サーバーアドレス（NTP、SIP 等）を接続先サービス提供者から DHCPv6 にて取得できること。

必要度：オプション（MAY）

出典：第 2 版 要件 62

---

5. LAN の要求事項（LAN）

要件番号：LAN-1

要件：LAN インターフェースにリンクローカルアドレスを作成すること。

要件詳細：LAN インターフェースにリンクローカルアドレスを作成すること。RFC4862 に基づき、DAD（重複アドレス検出）が機能すること。リブートや停電後にも同じリンクローカルアドレスが使われること。

理由：IPv6 ルーターでの IPv6 通信にはリンクローカルアドレスが必須であるため。

必要度：必須（MUST）

出典：RFC4291, RFC4862, TR124i5 LAN.ADDRESS.v6.1

要件番号：LAN-2

要件：重複アドレスが検出された場合、かわりのリンクローカルアドレスを付与すること。

要件詳細：ベンダーはこのケースで利用するアルゴリズムを定義することができる。

理由：IPv6 通信には一意のリンクローカルアドレスが必須であるため。

必要度：推奨（SHOULD）

出典：RFC4291, TR124i5 LAN.ADDRESS.v6.2

要件番号：LAN-3

要件：RFC4861 6.2 Router Specification をサポートすること。

理由：IPv6 ルーターに必須の機能であるため。

必要度：必須（MUST）

出典：RFC4861, TR124i5 LAN.ADDRESS.v6.6

要件番号：LAN-4

要件：キャプティブポータルを実装する場合は、IPv4 だけではなく IPv6 も実装すること。

理由：DNS でのキャプティブポータルでは動作の不確実性や、セキュリティ的な懸念点があるため、RA、DHCPv6、DHCP を使用したキャプティブポータルの利用を勧める。

必要度：オプション（MAY）

出典：RFC8910, TR124i5 LAN.CAPTIVE

要件番号：LAN-5

要件： ULA プレフィックスを生成しそれを LAN 側に配布できること。

理由：IPv6 のみの環境でグローバルアドレスが割り当てられていない時にも宅内通信を担保するため。ただし、実際の宅内ネットワークは IPv4/IPv6 のデュアルスタックとなることが想定されるため推奨とする。

必要度：推奨（SHOULD）

出典：第 2 版 要件 10, RFC4193, RFC7084

備考：ULA の仕様は RFC4193 に準拠すること。TR124i5 LAN.ADDRESSv6 では、ULA プリフィックスの生成は必須（MUST）、配布は推奨（SHOULD）となっており、RFC7084 では ULA プレフィックスの生成、配布が推奨（SHOULD）とされている。

要件番号：LAN-6

前提条件：LAN-5

要件：ULA を使用できる場合、ULA プレフィックスを設定変更する機能を持つこと。

理由：ユーザーが既定のものではない ULA プレフィックスを利用したい場合があるため。

必要度：オプション（MAY）

出典：TR124i5 LAN.ADDRESS.v6.4

要件番号：LAN-7

前提条件：LAN-5

要件：ULA プレフィックスを利用する場合、ULA プレフィックス広告を有効化・無効化する機能を持つこと。

要件詳細：RA により ULA プレフィックスからの/64 の広告を有効または無効とする機能をサポートする必要がある。

理由：ULA プレフィックスを利用する場合、RA の機能の設定変更が必要なため

必要度：必須（MUST）

出典：TR124i5 LAN.ADDRESS.v6.5

要件番号：LAN-8

要件：RFC8415 に準拠し、DHCPv6 サーバーメッセージと動作をサポートすること。

理由：
・IA_NA を使用した IPv6 アドレスの管理が行いやすい
・新しい実装が行われていない端末において、RA による DNS サーバーの配布に対応していない
・IA_PD での IPv6 プレフィックスの再委譲

必要度：推奨（SHOULD）

出典：RFC8415, TR124i5 LAN.DHCPv6S.1

要件番号：LAN-9

前提条件：LAN-8

要件：DHCPv6 Information-Request メッセージをサポートすること。

理由：DHCPv6 によるアドレス割り当て機能が無効化されている場合でも、SIP サーバー、DNS サーバー、SNTP サーバー等の情報を端末に通知可能にするため

必要度：必須（MUST）

出典：RFC8415, TR124i5 LAN.DHCPv6S.8

備考：DHCPv6 Information-Request メッセージを用いて各種サーバー等の情報を端末に通知する場合には、O フラグを 1 とした RA を LAN セグメントに広告すること。

要件番号：LAN-10

前提条件：LAN-9

要件：LAN セグメントに対して、DHCPv6 DNS Recursive Name Server（オプション 23）にて DNS サーバーアドレスを配布する機能を持つこと。

理由：DHCPv6 により DNS サーバー情報を取得する端末が存在しているため。

必要度：必須（MUST）

出典：第 2 版 要件 39, RFC3646, TR124i5 LAN.DNSv6.9

要件番号：LAN-11

前提条件：WAN-22

要件：接続先サービス提供者から DHCPv6-PD で受け取ったプレフィックスを基に/64 のプレフィックスを生成しそれを LAN 側に再配布できること。

必要度：必須（MUST）

出典：第 2 版 要件 7

備考：/64 より広いプレフィックスを DHCPv6-PD で受け取った場合に、そこから1つの /64 プレフィックスを切り出す方法は規定しない。例えば、DHCPv6-PD で/48 のプレフィックスを受け取った場合、LAN 側に再配布する際は 49～64 ビットの範囲の値を決める必要がある。その決め方については、本文書では規定しない。

要件番号：LAN-12

前提条件：LAN-11

要件：1つのもしくは複数のサービス提供者から複数のプレフィックスを DHCPv6-PD で受け取った場合、どのプレフィックスを LAN 側に再配布するか選択できること。

理由：上流サービス提供者が複数存在する環境や、サービス提供者が複数の別々のプレフィックスを配布する環境に対応するため。ただし、複数の上流がある環境は家庭用ルーターとしては特殊であると考えられるためオプションとする。

必要度：オプション（MAY）

出典：第 2 版 要件 8

要件番号：LAN-13

前提条件：LAN-11

要件：WAN 側回線の再接続等でサービス提供者が DHCPv6-PD にて配布するプレフィックスが変化した場合に、LAN 側に配布するプレフィックスを適切に変更できること。

理由：時間の経過によりユーザーに割り当てられたプレフィックスが変化するサービスを利用する場合等により、ユーザーネットワークの通信に与える影響を最小限に抑える必要があるため。

必要度：必須（MUST）

出典：第 2 版 要件 9

備考： 配布プレフィックスを変化させる具体的な方式は規定しない。

要件番号：LAN-14

前提条件：LAN-8

要件：宅内の端末に IPv6 アドレスを DHCPv6 IA_NA（オプション 3）で通知する機能を持つこと。

理由：宅内ネットワークの端末に特定の IPv6 アドレスを割り当てたい場合に有効であるため。ただし、現状、端末側では SLAAC による IPv6 アドレス設定が一般的であるためオプションとする。

必要度：オプション（MAY）

出典：第 2 版 要件 35, RFC8415

備考：本機能を有効とした場合、M フラグを 1 とした RA を LAN セグメントに広告すること。

要件番号：LAN-15

前提条件：LAN-14

要件：DHCPv6 による IPv6 アドレス割り当て機能の有効化・無効化を設定できること。

理由：ユーザーの利用環境に応じて、DHCPv6 による IPv6 アドレス配布を無効に設定できる必要があるため。

必要度：推奨（SHOULD）

出典：TR124i5 LAN.DHCPv6S.2

要件番号：LAN-16

前提条件：LAN-14

要件：Reconfigure Message Option の msg-type を 5（Renew message の要求）とした Reconfigure message を送信する機能を持つこと。

理由：アドレス変更時に、端末に対して迅速に DHCPv6 によるアドレスの再取得を促すために有効であるため。ただし、本機能を動作させるタイミングも考慮した実装とする必要あるため推奨とする。

必要度：推奨（SHOULD）

出典：第 2 版 要件 36

備考：本機能を動作させるタイミングとして、サービス提供者の切り替え等により、サービス提供者から割り当てられるプレフィックスの変更を検出した時等が考えられる。

要件番号：LAN-17

前提条件：LAN-14, LAN-16

要件：Reconfigure Accept をサポートすること。

理由：DHCPv6 クライアントから Reconfigure Accept を受けた場合、Reconfigure メッセージを送付すべきであるため

必要度：推奨（SHOULD）

出典：RFC8415, TR124i5 LAN.DHCPv6S.10

要件番号：LAN-18

前提条件：LAN-8

要件：DHCPv6 IA_PD（オプション 29）[30]により宅内機器（ルーター等）にプレフィックスを配布する機能（DHCPv6-PD サーバー機能）を持つこと。

理由：宅内に複数のルーターが存在する場合、当該ルーターに接続された端末に割り当てるプレフィックスを配布する場合に有効であるため。ただし、宅内に複数のルーターを設置するユーザーはあまり多くないと考えられるためオプションとする。

必要度：オプション（MAY）

出典：第 2 版 要件 37, RFC8415, TR124i5 LAN.DHCPv6S.5/6/9

要件番号：LAN-19

要件：WAN から受信したプレフィックスまたは ULA プレフィックスから、DHCPv6 IA_NA によるアドレス割り当てに使用する/64 のプレフィックスを自動設定または手動設定できること。

必要度：必須（MUST）

出典：TR124i5 LAN.DHCPv6S.3

備考：WAN 側のプレフィックスの受信状態によって、配布するプレフィックスの生成に関して、複数プレフィックスの受信（行 100）、ULA プレフィックスの生成及び配布（行 102）を参照。IP アドレスの再配布に関して、配布プレフィックスの変更（行 101）を参照。

要件番号：LAN-20

前提条件：LAN-18

要件：DHCPv6-PD によるプレフィックス委譲の有効・無効を設定できること。

必要度：必須（MUST）

出典：RFC8415, TR124i5 LAN.DHCPv6S.5

要件番号：LAN-21

前提条件：LAN-18

要件： WAN 側から受信したプレフィックスあるいは独自の ULA プレフィックスが/64 より短い場合に LAN 側の機器に対するプレフィックス委譲をサポートすること。

理由：DHCPv6 によるプレフィックス委譲は家庭用ルーターには必須ではないと考えられる。宅内に複数のルーターを設置するユーザーはあまり多くないが、ネットワークの分割を行いたい場合に本機能が有効なためオプションとする。

必要度：オプション（MAY）

出典：RFC8415, TR124i5 LAN.DHCPv6S.6

要件番号：LAN-22

前提条件：LAN-18

要件：WAN 側から受信したプレフィックスあるいは独自の ULA プレフィックスの中から LAN 側への委譲を行うプレフィックスが設定可能であること。

理由：DHCPv6-PD によるプレフィックス配布はユーザー環境によってはユーザーの任意のプレフィックスを設定したい場合があるため。

必要度：オプション（MAY）

出典：TR124i5 LAN.DHCPv6S.7

要件番号：LAN-23

前提条件：LAN-10

要件：上位ネットワークから取得した DNS 再帰ネームサーバーアドレス、ユーザーが指定したアドレス、ルーターのアドレス（DNS プロキシとして動作する場合）のいずれかを設定できること。

必要度：推奨（SHOULD）

出典：TR124i5 LAN.DNSv6.8

要件番号：LAN-24

前提条件：LAN-8

要件：LANセグメントに対して、DHCPv6 にてその他のサーバーアドレス（SIP、NTP 等）を配布する機能を持つこと。

理由：ユーザーの手入力による設定誤りを避けるため。ただし、その他のサーバーを利用するかどうかはサービス提供者のサービスに大きく依存するためオプションとする。

必要度：オプション（MAY）

出典：第 2 版 要件 40, RFC3319, RFC3646, RFC3898, RFC4075

備考：どのサーバーアドレスを配布するかはサービス提供者のサービス仕様に依存する。DHCPv6 で配布可能なサーバーアドレスは、DHCPv6 のパラメーター一覧を参照。
https://www.iana.org/assignments/dhcpv6-parameters/

要件番号：LAN-25

前提条件：LAN-8

要件：Reconfigure Message option の msg-type を 11（Information-request message の要求）とした Reconfigure message を送信する機能を持つこと。

理由：サービス提供者の切り替え等により配布するサーバーアドレスが変更された場合に、端末に対して迅速に DHCPv6 によるサーバー情報の再取得を促すため。ただし、サーバー情報の変更はサービス提供者のサービスに依存するため推奨とする。

必要度：推奨（SHOULD）

出典：第 2 版 要件 41

要件番号：LAN-26

要件：LAN セグメントに対して、RA で MTU 値を広告する機能を持つこと。また広告する MTU の値を設定可能とすること。

理由：宅内ネットワークの MTU 値を一括して変更したい場合に有効であるため。ただし、小さい MTU 値にする設定は LAN 内通信のパフォーマンスを落とす可能性があるため推奨とする。

必要度：推奨（SHOULD）

出典：第 2 版 要件 42, TR124i5 LAN.ADDRESS.v6.8

要件番号：LAN-27

要件：宅内ネットワークの端末に割り当てるプレフィックスを RA で通知する機能を持つこと。

要件詳細：広告される RA は、L=1, A=1, WAN から受信した委譲のライフタイムを持つこと。

理由：IPv6 ルーターに必須の機能であるため。

必要度：必須（MUST）

出典：第 2 版 要件 31, RFC8504, TR124i5 LAN.ADDRESS.v6.9

備考：複数プレフィックスをサービス提供者から取得した場合の LAN 内への配布ポリシー等については、3.3.2 節を参照。

要件番号：LAN-28

前提条件：LAN-27

要件：RA の RDNSS オプションで DNS サーバーを広告すること。

理由：DHCPv6 未対応のクライアントでも RA の RDNSS オプションで DNS サーバー情報を取得可能とするため

必要度：必須（MUST）

出典：RFC8106, TR124i5 LAN.ADDRESS.v6.10

要件番号：LAN-29

前提条件：LAN-27

要件：RA で通知するプレフィックス長は、デフォルトを/64 とすること。

理由：端末における SLAAC では、多くの実装がアドレスの下位 64 ビットをインターフェース ID とするため。

必要度：必須（MUST）

出典：第 2 版 要件 32, RFC4862

備考：/64 以外のプレフィックス長で配布した場合、LAN 内機器にアドレスが正しく設定されない場合がある点に留意すること。SLAAC の仕様では、RA の Prefix Information Option 中の prefix length と、端末自身の持つ interface ID の長さの合計が 128 で無い場合には、その Prefix Information Option を無視することとなっている。（MUST）

要件番号：LAN-30

前提条件：LAN-27

要件：Prefix Information Option 中の Preferred Lifetime を 0 とした RA を広告する機能を持つこと。

理由：サービス提供者を切り替えた場合等において、端末の通信への影響を最小限に抑えるために必要な機能であるため。ただし、本機能を動作させるタイミングも考慮した実装とする必要があるため推奨とする。

必要度：推奨（SHOULD）

出典：第 2 版 要件 33, RFC7084

備考：端末に Preferred Lifetime が 0 であるアドレス（A）と Preferred Lifetime が 0 でないアドレス（B）が割り当てられている場合、その端末が新たに通信を行う際の始点アドレスとして（B）を使用することが優先される。本機能を動作させるタイミングとして、例えばサービス提供者の切り替え等により、サービス提供者から割り当てられるプレフィックスの変更を検出した時が考えられる。この場合、古いプレフィックスについて Preferred Lifetime = 0 とした RA を広告すれば、その RA を受信した端末は以降の通信において古いプレフィックスを持つアドレスを使用しなくなるため、宅内端末のアドレス変更（リナンバリング）をスムーズに行うことができる。Preferred Lifetime = 0 の RA を広告しない場合、端末において旧プレフィックスの Preferred Lifetime が 0 となるまでは、新規通信における始点アドレスとして旧プレフィックスから生成されたアドレスが選択される可能性があるため、その結果通信に問題が発生する場合も考えられる。
その他のタイミングとして、WAN 側リンクの切断を検出した時が考えられる（宅内ネットワークに割り当てられたグローバルプレフィックスへの到達性がなくなるため、そのプレフィックスを無効とする）。しかしこの場合宅内のグローバルアドレスが無効になった時点（Valid Lifetime が 0 となった時点）で、特にルーターを越える宅内通信ができなくなる可能性があるため、ULA プレフィックスを広告して宅内通信を担保する等の対応をとる必要がある。

要件番号：LAN-31

前提条件：LAN-27

要件：Router Lifetime を 0 とした RA を広告する機能を持つこと。

理由：端末に対して、自身をデフォルトルートとして選択させたくない場合に有効である。ただし、本機能を動作させるタイミングも考慮した実装とする必要があるため推奨とする。

必要度：推奨（SHOULD）

出典：第 2 版 要件 34, RFC7084

備考：Router Lifetime = 0 の RA を受信した端末は、その RA の送信元ルーターをデフォルトルートとして選択しない。

要件番号：LAN-32

要件：MLD（v1/v2）プロキシ機能を有すること。

理由：サービス事業者側がマルチキャストサービスを提供する場合、MLD でサービス提供者側へマルチキャストグループへの参加／離脱を通知する機能はマルチキャスト利用には最低限必要であるため。

必要度：オプション（MAY）

出典：第 2 版 要件 53, RFC4605

要件番号：LAN-33

前提条件：LAN-32

要件：MLD（v1/v2）スヌーピング機能を有すること。

理由：スイッチング機能を有する場合、不要なマルチキャストトラフィックを制限するため。

必要度：必須（MUST）

出典：第 2 版 要件 54, RFC4541

要件番号：LAN-34

要件：DNS プロキシを実装する場合は、DHCPv6 等の手段にて取得した DNS サーバー情報を使用できること。

必要度：必須（MUST）

出典：第 2 版 要件 60

要件番号：LAN-35

要件：Wi-Fi インターフェースを実装する場合、L2 レイヤのマルチキャストアドレスをユニキャストアドレスに変換し通信ができること。

理由：IPv6 のマルチキャストパケットでの映像配信サービスを受ける Wi-Fi 端末が映像の品質を維持するのに有効なため。

必要度：推奨（SHOULD）

出典：RFC9119

備考：Wi-Fi 部分のマルチキャストパケットは、昨今の映像配信では不十分なパフォーマンスとなり、本問題点を解決するための手法となる。
Wi-Fi 部分のマルチキャストパケットからユニキャストパケットへ変換を行う条件において、ICMPv6、UPnP やプライベートなマルチキャスト通信を透過させる等の実装の注意点がある。

---

6. セキュリティの要求事項(SEC)

要件番号:SEC-1

要件:始点アドレスもしくは終点アドレスがインターネット上で利用すべきではないアドレスであるようなパケットを外部(WAN 側)に転送しないこと。

要件詳細:インターネット上で利用すべきではないアドレスの例としては、以下のものがある。
- IPv4 互換(compatible)アドレス(::/96)
- IPv4 射影(mapped)アドレス(::ffff:0:0/96)
- ドキュメンテーションアドレス(2001:db8::/32)
- サイトローカルアドレス(fec0::/10, RFC3879 にて廃止済み)

必要度:必須(MUST)

出典:第2版 要件 12, RFC6092, RFC6890

備考:インターネット上で利用すべきではないアドレスについては、RFC6890 に記載されているものなど他にも考えられるが、多数に及ぶため、本文書では代表的な上記の 4 種類のアドレスのみを例示する。

要件番号:SEC-2

要件:ULA アドレスを始点アドレスもしくは終点アドレスとして持つパケットは、WAN 側インターフェースでは転送せず破棄すること。

要件詳細:外部から当該パケットが入ってきた時と、内部から当該パケットが出て行こうとする時の、いずれの場合にも破棄すること。なおデフォルトの動作は破棄することが望ましいが、ユーザーの設定によって変更できても良い。また、ユーザーが LAN 内で ULA アドレスを利用する場合があるため、LAN 側インターフェースの間では当該パケットを適切に転送すること(たとえばイーサネットインターフェースから入ってきたパケットを無線 LAN インターフェースに出力する場合)。

必要度:推奨(SHOULD)

出典：RFC6092

要件番号：SEC-3

要件：始点アドレスがマルチキャストアドレスであるパケットを送信もしくは転送しないこと。

理由：そのようなパケットは RFC4291 で禁止されているため。

必要度：必須（MUST）

出典：RFC4291, RFC6092

要件番号：SEC-4

要件：事業者から割り当てられたプレフィックスに含まれるアドレスを始点アドレスとして持つパケットを WAN インターフェースで受信した場合は、それを転送せずに破棄すること。

理由：そのようなパケットを受信した場合は、そのパケットの始点アドレスが詐称されているか、あるいはネットワーク上でループが発生して戻ってきたパケットであると考えられるため、破棄すべきである。

必要度：必須（MUST）

出典：RFC6092, TR124i5 WAN.DoS.2

要件番号：SEC-5

要件：事業者から割り当てられたプレフィックスに含まれないアドレスを始点アドレスとして持つパケットを外部（WAN 側）に転送しないこと。

必要度：必須（MUST）

出典：RFC6092, TR124i5 WAN.DoS.4

要件番号：SEC-6

要件：事業者から割り当てられたプレフィックスに含まれるアドレスを終点アドレスとして持つパケットは、外部（WAN 側）に転送しないこと。

理由：そのようなパケットを転送すると、Hop Limit が 0 になるまで家庭用ルーターとサービス提供者ルーターの間でパケットがピンポンする可能性があるため。

必要度：必須（MUST）

出典：第 2 版 要件 43

備考：事業者から割り当てられたものの利用していないプレフィックスへのパケットは破棄専用のインターフェースに転送するようなルーティングを設定する、といった実装が考えられる。

要件番号：SEC-7

要件：事業者からのプレフィックスの取得処理が完了するまでは、パケットを外部（WAN 側）に転送しないこと。

理由：前項（行 180）の目的を達成するためには、事業者から割り当てられたプレフィックスを家庭用ルーターが認識していなければならないため。

必要度：推奨（SHOULD）

出典：TR124i5 WAN.DoS.5

要件番号：SEC-8

要件：IPv6 パケットを選択的に破棄する静的パケットフィルター機能を有すること。

必要度：必須（MUST）

出典：第2版 要件 12

要件番号：SEC-9

要件：IPv6 通信フローの状態を認識しつつパケットの転送や破棄を行う動的パケットフィルター機能（SPI）を有すること。

理由：IPv4 で一般に利用される動的パケットフィルター機能（あるいは SPI = Stateful Packet Inspection や Stateful Filtering とも呼ばれる）を IPv6 でも実現するため。ただし、静的フィルターにより必要最低限のセキュリティを確保することが可能であることから必要度は推奨とする。

必要度：推奨（SHOULD）

出典：第2版 要件 13

備考：ESP のパケットは、送信元 IP アドレス、宛先 IP アドレス、プロトコル番号（=50）を通信フローの識別子とすることが望ましい。

要件番号：SEC-10

前提条件：SEC-9

要件：SPI フィルターのフィルターステートの有効期間は 2 分以上とすること。

要件詳細：ステートフルフィルターの状態は、設定された時間の間パケットが通過しなければ削除される。その有効期間は 2 分より短くしてはならない。但し、フィルターの実装が DNS などの特定のプロトコルに固有の処理を行う場合は、必ずしもこの制限に従わなくても良い。

必要度：必須（MUST）

出典：RFC6092

備考：RFC6092 は、SPI フィルターのフィルターステートの有効期間のデフォルト値を 5 分と規定している。

要件番号：SEC-11

前提条件：SEC-9

要件：動的パケットフィルター機能は、デフォルトでは、内部（LAN 側）から外部（WAN 側）への通信と、その通信の応答である外部から内部への通信のみ通過させ、それ以外の不要な通信を遮断すること。

理由：一般的な家庭用ルーターが IPv4 通信に対して実現しているセキュリティと同等のセキュリティを IPv6 でも実現するため

必要度：必須（MUST）

出典：第2版 要件 11,12,13

備考：リモートアクセス利用等の VPN 通信を許可する場合は、IKE（UDP ポート 500）、ESP（プロトコル番号 50）、AH（プロトコル番号 51）の双方向の通信を許可すること。また NAT トラバーサル（UDP ポート 4500）通信も適切に通過させること。

要件番号：SEC-12

前提条件：SEC-11

要件：SEC-11 のパケットフィルターの動作を無効化する設定項目を有すること。

理由：複数の家庭用ルーターを組み合わせて利用する構成など、SEC-11 の機能を適用することが望ましくない場合があるため。

必要度：オプション（MAY）

出典：RFC6092

要件番号：SEC-13

前提条件：SEC-8, SEC-9

要件：フラグメントヘッダーを付与された IPv6 パケットに対してパケットフィルターを適用する場合は、擬似的に元の IPv6 パケットを再構成した上でルールを適用すること。

理由：フラグメントヘッダーを付与された IPv6 パケットは、TCP や UDP のヘッダーを含まないなど、そのままではパケットフィルターを適用できない場合がある。そのような IPv6 パケットに対してもパケットフィルターを適用するために、フラグメント化された IPv6 パケットをいったん保持しておき、擬似的に元の IPv6 パケットを再構成した上でパケットフィルターのルールを適用する必要がある。ただし、フラグメントパケットの保持や再構成には装置資源を消費するため、オプションとする。

必要度：オプション（MAY）

出典：第2版 要件 15

備考：IPv6 では中継ルーターによってフラグメントヘッダーを改変することは禁止されているため、IPv6 パケットの再構成はあくまで擬似的な処理に留めるべきであり、再構成後のパケットを転送（再送信）してはならない。

要件番号：SEC-14

前提条件：SEC-8, SEC-9

要件：ND プロキシ/IPv6 ブリッジ動作時にも静的/動的パケットフィルターを適用できること。

理由：ND プロキシ/IPv6 ブリッジのような通信を許可する場合、IPv6 ネットワークに接続されるホストはスキャンや攻撃の対象となる可能性がある。そのため、単純な通信の透過機能ではなく、それらの外部からの不正な通信をフィルターする機能を必要とする。

必要度：必須（MUST）

要件番号：SEC-15

前提条件：SEC-8, SEC-9

要件：パケットフィルター機能は、IPv6 始点/終点アドレス、プロトコル番号、TCP/UDP の始点/終点ポート番号等に基づいてルールを適用できること。

要件詳細：パケットフィルター機能は、送受信するパケットが一定のルールに合致した場合にそのパケットを通過あるいは破棄する機能である。そのルールとして、以下の条件を記述できることが望ましい。

- IPv6 始点/終点アドレスが特定のプレフィックスに含まれる。
- プロトコル番号（次ヘッダー値）が特定の値である。
  ※拡張ヘッダーが付加された IPv6 パケットの場合は、最後の拡張ヘッダーの次ヘッダー値で判断すること。なお拡張ヘッダーの段数については本文書では規定しない。
- TCP/UDP の始点/終点ポート番号が特定の値である。
- ICMP タイプが特定の値である。
- 特定の拡張ヘッダーが付加されている。
- IPv4 パケットフィルター機能を有する場合は、IPv6 パケットフィルター機能でもそれと同等のルールを記述できる。
- トンネリングもしくはトランスレーション技術を利用する場合は、外側と内側もしくは変換前と変換後の両方のプロトコルについてパケットフィルターを適用できる。

必要度：オプション（MAY）

出典：第2版 要件 14

要件番号：SEC-16

前提条件：SEC-9

要件：どのような ICMPv6 パケットを受信しても、TCP や UDP のフィルターステートを終了させないこと。

理由：ICMPv6 パケットは詐称が可能である。悪意のある第三者によって詐称された ICMPv6 パケットが送信され、そのパケットを受信したルーターが TCP や UDP の動的フィルターを終了させてしまうと、本来フィルターステートによって通過すべき TCP や UDP のパケットが通らなくなり、サービス妨害（DoS）攻撃が成立する可能性がある。

必要度：必須（MUST）

出典：RFC6092

要件番号：SEC-17

前提条件：SEC-9

要件：TCP のフィルターは、simultaneous open の場合を含め、RFC9293 で規定されているすべての正当なシーケンスをサポートすること。

必要度：必須（MUST）

出典：RFC6092

備考：simultaneous open における注意点は RFC5382 にまとまっている。

要件番号：SEC-18

前提条件：SEC-9

要件：UDP のフィルターステートは、内側から外側へのパケットが通過した時に有効期限を更新すること。

要件詳細：なお、外側から内側へのパケットが通過した場合には、有効期限を更新してもしなくてもどちらでも構わない。

必要度：必須（MUST）

出典：RFC6092

要件番号：SEC-19

前提条件：SEC-9

要件：始点ポートと終点ポートがともにウェルノウンポート（0-1023）ではない UDP のフィルターステートは、2 分未満で期限切れにしないこと。

要件詳細：なお、片方もしくは両方のポート番号がウェルノウンポートの場合は、IANA によってそのポート番号に割り宛てられたサービスを円滑に実行する目的のために、2 分より短い時間で期限切れとしても良い。また、UDP のフロー状態を維持する期間は、設定可能であっても良い。

必要度：必須（MUST）

出典：RFC6092

要件番号：SEC-20

前提条件：SEC-9

要件：UDP のフィルターステートが存在する場合には、そのフィルターステートに適合する UDP ヘッダーを含む ICMPv6 Destination Unreachable と ICMPv6 Packet Too Big メッセージも転送すること。

必要度：必須（MUST）

出典：RFC6092

備考：VPN 通信を許可する場合は、ESP の通信についても同様に対応する ICMPv6 パケットを転送することが望ましい。

コラム：IPv6 パケットに対する動的パケットフィルターの実現方式

IPv6 パケットに対する動的パケットフィルタリングでは、ある外向きの IPv6 パケットが通過した場合にそれに対応してどのような内向き IPv6 パケットを通すべきかについていくつかの方式が考えられる。

もっとも単純な方式としては、外向きパケットの送信先の IP アドレス/ポートから戻ってきた IPv6 パケットのみを通す方式が考えられ、これは Address and Port-Dependent Filtering と呼ばれる。この方式は単一のサーバーからなるシンプルなアプリケーションサービスでは問題なく動作するが、複数の IP アドレスを持つ複数台のサーバーからなるような複雑なサービスでは期待通りに動作しない場合がある。そのため外向きパケットの送信元アドレス/ポートに対して任意のサーバーから送信された IPv6 パケットを通すような方式もあり、これは Endpoint-Independent Filtering と呼ばれる。Endpoint-Independent Filtering では Address and Port-Dependent Filtering よりも多くのアプリケーションサービスが動作することが期待されるが、一方で不要なパケットも通過させてしまい、安全性が低下する懸念もある。

このように IPv6 パケットにおける動的パケットフィルタリングの方式にはそれぞれ利点欠点があるため、本ガイドラインでは方式を1つに定めていない。フィルタリングの方式については RFC4787 に詳細に述べられており、それらの方式を選択するための指針は RFC6092 に REC-11,REC-17,REC-33 として記載されている。家庭用ルーターの実装者は、これらの文書を参考に IPv6 パケットに対する動的パケットフィルターの方式を検討することが推奨される。

要件番号：SEC-21

要件：ルーティングヘッダー（Type 0）を持つパケットは転送しないこと。

理由：ルーティングヘッダー（Type 0）は、DoS 攻撃への懸念から RFC5095 にて廃止されたため。

必要度：必須（MUST）

出典：第2版 要件 49, RFC5095, RFC6092

備考：ルーティングヘッダーをすべて禁止する実装ではなく、タイプを正しく見て Type 0 のみ禁止すること。

要件番号：SEC-22

前提条件：GEN-4

要件：WAN 側インターフェースで受信した DNS や NTP の問い合わせは処理しないこと。

要件詳細：なお、ユーザーが明示的に許可した場合は、処理しても良い。

必要度：必須（MUST）

出典：RFC6092

備考：DNS と NTP に限らず、一般にルーターが WAN 側にサービスを公開する必要がある場合は、DoS 攻撃に脆弱にならないような手段を講じること。

要件番号：SEC-23

前提条件：LAN-8

要件：WAN 側インターフェースで受信した DHCPv6 の要求メッセージは処理しないこと。

要件詳細：本要件はルーター上で動作する DHCPv6 サーバー機能と DHCPv6 リレー機能の両方に適用される。

必要度：必須（MUST）

出典：RFC6092

要件番号：SEC-24

要件：WebUI 等の設定インターフェースは、デフォルト設定では WAN 側からはアクセスできないようにすること。

理由：利用者の意図に反して第三者により設定が変更されてしまうことを防ぐため。

必要度：必須（MUST）

出典：第2版 要件 16, RFC6092

備考：LAN 側からのアクセスについても、ゲスト用無線 LAN からの設定インターフェースへのアクセスを禁止する、特定の権限を持つユーザーにのみアクセスを許可するといった、柔軟なアクセス制御が実現できることが望ましい。

---

7. IPv6 家庭用ルーターに必要とされる機能一覧

前章までにまとめた「IPv6 家庭用ルーターに必要とされる機能」を表 7-1 に列挙しており、これらの機能に関して考慮した実装が IPv6 家庭用ルーターに求められる。

表 7-1 IPv6 家庭用ルーターに必要とされる機能一覧

要件番号	前提条件	要件	必要度
GEN-1		DNS プロキシもしくは DNS スタブリゾルバーは、DNS サーバーに問合せを行う際に IPv4 トランスポートと IPv6 トランスポートのいずれも利用可能であること。	必須(MUST)
GEN-2		DNS プロキシは、端末からの問合せをトランスポートに関わらずサービス提供者の要求するトランスポートに変換できること。	必須(MUST)
GEN-3		DNS プロキシは、IPv4 および IPv6 の DNS サーバーが共に利用可能な場合は、端末からの DNS 問合せが IPv4 であるか IPv6 であるかに関わらず、IPv6 の DNS サーバーに対して IPv6 トランスポートを使用してプロキシ動作を行うこと。	推奨(SHOULD)
GEN-4		DNS プロキシとして待ち受けるアドレスの種類は、ユニキャストアドレス(グローバルアドレス、ULA、リンクローカルアドレスの内いずれか)で待ち受け可能であること。	必須(MUST)
GEN-5		DNS サーバー情報を手動設定できること。	推奨(SHOULD)
GEN-6		各種サーバーアドレスを手動設定できること。	推奨(SHOULD)
GEN-7		ユーザーからの設定を受け付けるために HTTP(80/tcp)もしくは HTTPS (443/tcp)による WebUI の設定インターフェースは IPv6 トランスポートに対応すること。	推奨(SHOULD)
GEN-8		ユーザーからの設定を受け付けるために SSH(22/tcp)による CLI(Command Line Interface)の設定インターフェースは IPv6 トランスポートに対応すること。	オプション(MAY)
GEN-9		設定インターフェースにおいて、IPv6 アドレス/プレフィックスの入力を求める場合は、RFC4291 に規定されている表記が入力可能なこと。	推奨(SHOULD)
GEN-10		IPv6 アドレス／プレフィックスの出力表記は、RFC5952 に規定されている推奨表記に対応すること。	推奨(SHOULD)
GEN-11		IPv6 トランスポートでのファームウェアのアップデートが可能であること。	必須(MUST)
GEN-12		ファームウェアを安全に更新する方法を提供すること。	推奨(SHOULD)
WAN-1		ND プロキシもしくは、IPv6 ブリッジ機能をサポートすること。	必須(MUST)
WAN-2		ND プロキシもしくは、IPv6 ブリッジ機能は IPv4 の動作状態・設定に依存せず、独立した設定が用意されていること。	必須(MUST)
WAN-3		複数の WAN インターフェースを有する場合、家庭用ルーターは、WAN インターフェース毎に独立した ND プロキシ、または IPv6 ブリッジいずれかの設定が行えるこ	必須(MUST)

		と。	
WAN-4		ND プロキシまたは、IPv6 ブリッジ動作する場合、家庭用ルーターは WAN 側インターフェースにおいて、IPv6 ルーターとして動作せず、IPv6 ホストとしてふるまうこと。	必須(MUST)
WAN-5		TR124i5 Annex A.2 のフローに従った IPv6 接続の自動確立機能を有すること。	推奨(SHOULD)
WAN-6		RFC 8415 に準拠した DHCPv6 クライアント機能を有すること。	必須(MUST)
WAN-7		SLAAC(Stateless Address Auto Configuration)により WAN 側インターフェースへのグローバルアドレスを自動的に付与できる機能を有すること。	必須(MUST)
WAN-8	WAN-6	DHCPv6 による RFC3646 に準拠した DNS Search List オプションに対応すること。	必須(MUST)
WAN-9		PPP セッションに利用するパスワードは全て保存できること。また、保存されたパスワードは他の目的(他インターフェースへの表示、照合、通知など)に利用しないこと。	推奨(SHOULD)
WAN-10		PPP セッションが接続されているインターフェースが物理的に切断された場合でも、2 分間はセッションを維持し、その間にインターフェースの接続が回復した場合、セッションの維持を試みること。それが拒否、もしくは時間が経過した場合、元のセッションを切断し、新規にセッションの接続を試みること。	推奨(SHOULD)
WAN-11		起動後、各 IP 通信及び PPP セッションを開始する前に、ランダムな遅延処理を組み込むこと。	推奨(SHOULD)
WAN-12		PPP 接続時、認証エラーとなった場合、試行回数に応じて間隔を延長すること。	推奨(SHOULD)
WAN-13		LAN 側機器から出された PPPoE セッションを確立できるよう WAN インターフェースに双方向転送できること。(PPPoE パススルー機能)	必須(MUST)
WAN-14		IPv6 over PPPoE をサポートするルーターは RFC 5072 に則した IPv6 over PPP をサポートすること。	必須(MUST)
WAN-15		PPP 接続に対して、IPv4 通信、IPv6 通信、IPv4/IPv6 両方の通信、のいずれにおいても選択できること。	推奨(SHOULD)
WAN-16		ルーターに複数の PPPoE 接続先が設定できる場合、すべての接続先のユーザー/パスワード設定を同一にし、ドメインのみ異なるように設定できること。	オプション(MAY)
WAN-17		想定した事業者サービスに応じた IPv4 over IPv6 接続(DS-Lite かつ MAP-E)の実装を行うこと。	推奨(SHOULD)
WAN-18	WAN-17	RFC6333 に準拠した DS-Lite 方式による IPv4 接続に対応した機能を有すること。	推奨(SHOULD)
WAN-19	WAN-18	DS-Lite 方式 の設定手法を用意すること。	必須(MUST)
WAN-20	WAN-17	RFC7597 に準拠した MAP-E 方式による IPv4 接続に対応した機能を有すること。	推奨(SHOULD)

WAN-21	WAN-20	MAP-E 方式の設定手法を用意すること。	必須(MUST)
WAN-22	WAN-20, WAN-21	MAP-E 方式において、RFC7597 に準拠したメッシュモードおよびハブアンドスポークモードに対応すること。	必須(MUST)
WAN-23		宅内用 IPv6 プレフィックス情報を接続サービス提供者から DHCPv6-PD にて取得できること。	必須(MUST)
WAN-24		/48～/64 の幅でサービス提供者が割り当てたプレフィックスを受信できること。	必須(MUST)
WAN-25		SLAAC、DHCPv6 の両方式をサポートし、いずれかの方法で WAN 側インターフェースにグローバルアドレスを付与できること。	必須(MUST)
WAN-26		WAN 側インターフェースへのグローバルアドレスを手動で付与できること。	必須(MUST)
WAN-27		WAN 側インターフェースにグローバルアドレスが付与されていない場合に、ユーザーに割り当てられたプレフィックス内のアドレスを使って通信できること。	必須(MUST)
WAN-28		割り当てられたプレフィックス宛てのトラフィックを上流にフォワードしない機能を持つこと。	必須(MUST)
WAN-29		Point-to-Point リンクのルーターにて、自インターフェース以外のユニキャストアドレス宛のパケットを受け取った際には ICMPv6 Destination Unreachable messages, Code 3（Address unreachable）を送出し、パケットを転送しないこと。	必須(MUST)
WAN-30		WAN 向けのスタティックルートが設定できること。	推奨(SHOULD)
WAN-31		RA を利用してのデフォルトルートが自動設定できること。	必須(MUST)
WAN-32		家庭用ルーターを通過する TCP 通信に対して、MSS（Maximum Segment Size）オプションを適切に調整する機能を有すること。	オプション(MAY)
WAN-33	WAN-6	DNS サーバーアドレスを接続先サービス提供者から DHCPv6 にて取得できること。	必須(MUST)
WAN-34	WAN-6	各種サーバーアドレス（NTP、SIP 等）を接続先サービス提供者から DHCPv6 にて取得できること。	オプション(MAY)
LAN-1		LAN インターフェースにリンクローカルアドレスを作成すること。	必須(MUST)
LAN-2		重複アドレスが検出された場合、かわりのリンクローカルアドレスを付与すること。	推奨(SHOULD)
LAN-3		RFC4861 6.2 Router Specification をサポートすること。	必須(MUST)
LAN-4		キャプティブポータルを実装する場合は、IPv4 だけではなく IPv6 も実装すること。	オプション(MAY)
LAN-5		ULA プレフィックスを生成しそれを LAN 側に配布できること。	推奨(SHOULD)
LAN-6	LAN-5	ULA を使用できる場合、ULA プレフィックスを設定変更する機能を持つこと。	オプション(MAY)
LAN-7	LAN-5	ULA プレフィックスを利用する場合、ULA プレフィックス広告を有効化・無効化する機能を持つこと。	必須(MUST)
LAN-8		RFC8415 に準拠し、DHCPv6 サーバーメッセージと動作をサポートすること。	推奨(SHOULD)

LAN-9	LAN-8	DHCPv6 Information-Request メッセージをサポートすること。	必須(MUST)
LAN-10	LAN-9	DHCPv6 サーバーの DHCPv6 オプション 23(OPTION_DNS_SERVERS)をサポートすること。	必須(MUST)
LAN-11	WAN-22	接続先サービス提供者から DHCPv6-PD で受け取ったプレフィックスを基に/64 のプレフィックスを生成しそれを LAN 側に再配布できること。	必須(MUST)
LAN-12	LAN-11	ひとつのもしくは複数のサービス提供者から複数のプレフィックスを DHCPv6-PD で受け取った場合、どのプレフィックスを LAN 側に再配布するか選択できること。	オプション(MAY)
LAN-13	LAN-11	WAN 側回線の再接続等でサービス提供者が DHCPv6-PD にて配布するプレフィックスが変化した場合に、LAN 側に配布するプレフィックスを適切に変更できること。	必須(MUST)
LAN-14	LAN-8	宅内の端末に IPv6 アドレスを DHCPv6 IA_NA(オプション 3)で通知する機能を持つこと。	オプション(MAY)
LAN-15	LAN-14	DHCPv6 による IPv6 アドレス割り当て機能の有効化・無効化を設定できること。	推奨(SHOULD)
LAN-16	LAN-14	Reconfigure Message Option の msg-type を 5(Renew message の要求)とした Reconfigure message を送信する機能を持つこと。	推奨(SHOULD)
LAN-17	LAN-14、LAN-16	Reconfigure Accept をサポートすること。	推奨(SHOULD)
LAN-18	LAN-8	DHCPv6 IA_PD(オプション 29)[30]により宅内機器(ルータ等)にプレフィックスを配布する機能(DHCPv6-PD サーバー機能)を持つこと。	オプション(MAY)
LAN-19		WAN から受信したプレフィックスまたは ULA プレフィックスから、DHCPv6 IA_NA によるアドレス割り当てに使用する/64 のプレフィックスを自動設定または手動設定できること。	必須(MUST)
LAN-20	LAN-18	DHCPv6-PD によるプレフィックス委譲の有効・無効を設定できること。	必須(MUST)
LAN-21	LAN-18	WAN 側から受信したプレフィックスあるいは独自の ULA プレフィックスが/64 より短い場合に LAN 側の機器に対するプレフィックス委譲をサポートすること。	オプション(MAY)
LAN-22	LAN-18	WAN 側から受信したプレフィックスあるいは独自の ULA プレフィックスの中から LAN 側への委譲を行うプレフィックスが設定可能であること。	オプション(MAY)
LAN-23	LAN-10	上位ネットワークから取得した DNS 再帰ネームサーバーアドレス、ユーザーが指定したアドレス、ルーターのアドレス(DNS プロキシとして動作する場合)のいずれかを設定できること。	推奨(SHOULD)
LAN-24	LAN-8	LAN セグメントに対して、DHCPv6 にてその他のサーバーアドレス(SIP、NTP 等)を配布する機能を持つこと。	オプション(MAY)
LAN-25	LAN-8	Reconfigure Message option の msg-type を 11 (Information-request message の要求)とした Reconfigure message を送信する機能を持つこと。	推奨(SHOULD)

LAN-26		LAN セグメントに対して、RA で MTU 値を広告する機能を持つこと。また広告する MTU の値を設定可能とすること。	推奨(SHOULD)
LAN-27		宅内ネットワークの端末に割り当てるプレフィックスを RA で通知する機能を持つこと。	必須(MUST)
LAN-28	LAN-27	RA の RDNSS オプションで DNS サーバーを広告すること。	必須(MUST)
LAN-29	LAN-27	RA で通知するプレフィックス長は、デフォルトを/64 とすること。	必須(MUST)
LAN-30	LAN-27	Prefix Information Option 中の Preferred Lifetime を 0 とした RA を広告する機能を持つこと。	推奨(SHOULD)
LAN-31	LAN-27	Router Lifetime を 0 とした RA を広告する機能を持つこと。	推奨(SHOULD)
LAN-32		MLD(v1/v2)プロキシ機能を有すること。	オプション(MAY)
LAN-33	LAN-32	MLD(v1/v2)スヌーピング機能を有すること。	必須(MUST)
LAN-34		DNS プロキシを実装する場合は、DHCPv6 等の手段にて取得した DNS サーバー情報を使用できること。	必須(MUST)
LAN-35		Wi-Fi インターフェースを実装する場合、L2 レイヤのマルチキャストアドレスをユニキャストアドレスに変換し通信ができること。	推奨(SHOULD)
SEC-1		始点アドレスもしくは終点アドレスがインターネット上で利用すべきではないアドレスであるようなパケットを外部(WAN 側)に転送しないこと。	必須(MUST)
SEC-2		ULA アドレスを始点アドレスもしくは終点アドレスとして持つパケットは、WAN 側インターフェースでは転送せず破棄すること。	推奨(SHOULD)
SEC-3		始点アドレスがマルチキャストアドレスであるパケットを送信もしくは転送しないこと。	必須(MUST)
SEC-4		事業者から割り当てられたプレフィックスに含まれるアドレスを始点アドレスとして持つパケットを WAN インターフェースで受信した場合は、それを転送せずに破棄すること。	必須(MUST)
SEC-5		事業者から割り当てられたプレフィックスに含まれないアドレスを始点アドレスとして持つパケットを外部(WAN 側)に転送しないこと。	必須(MUST)
SEC-6		事業者から割り当てられたプレフィックスに含まれるアドレスを終点アドレスとして持つパケットは、外部(WAN 側)に転送しないこと。	必須(MUST)
SEC-7		事業者からのプレフィックスの取得処理が完了するまでは、パケットを外部(WAN 側)に転送しないこと。	推奨(SHOULD)
SEC-8		IPv6 パケットを選択的に破棄する静的パケットフィルター機能を有すること。	必須(MUST)
SEC-9		IPv6 通信フローの状態を認識しつつパケットの転送や破棄を行う動的パケットフィルター機能(SPI)を有すること。	推奨(SHOULD)
SEC-10	SEC-9	SPI フィルターのフィルターステートの有効期間は 2 分以上とすること。	必須(MUST)
SEC-11	SEC-9	動的パケットフィルター機能は、デフォルトでは、内部(LAN 側)から外部(WAN	必須(MUST)

		側)への通信と、その通信の応答である外部から内部への通信のみ通過させ、それ以外の不要な通信を遮断すること。	
SEC-12	SEC-11	SEC-11 のパケットフィルターの動作を無効化する設定項目を有すること。	オプション(MAY)
SEC-13	SEC-8, SEC-9	フラグメントヘッダーを付与された IPv6 パケットに対してパケットフィルターを適用する場合は、擬似的に元の IPv6 パケットを再構成した上でルールを適用すること。	オプション(MAY)
SEC-14	SEC-8, SEC-9	ND プロキシ/IPv6 ブリッジ動作時にも静的/動的パケットフィルターを適用できること。	必須(MUST)
SEC-15	SEC-8, SEC-9	パケットフィルター機能は、IPv6 始点/終点アドレス、プロトコル番号、TCP/UDP の始点/終点ポート番号等に基づいてルールを適用できること。	オプション(MAY)
SEC-16	SEC-9	どのような ICMPv6 パケットを受信しても、TCP や UDP のフィルターステートを終了させないこと。	必須(MUST)
SEC-17	SEC-9	TCPのフィルターは、simultaneous openの場合を含め、RFC9293で規定されているすべての正当なシーケンスをサポートすること。	必須(MUST)
SEC-18	SEC-9	UDP のフィルターステートは、内側から外側へのパケットが通過した時に有効期限を更新すること。	必須(MUST)
SEC-19	SEC-9	始点ポートと終点ポートがともにウェルノウンポート(0-1023)ではない UDP のフィルターステートは、2 分未満で期限切れにしないこと。	必須(MUST)
SEC-20	SEC-9	UDP のフィルターステートが存在する場合には、そのフィルターステートに適合する UDP ヘッダーを含む ICMPv6 Destination Unreachable と ICMPv6 Packet Too Big メッセージも転送すること。	必須(MUST)
SEC-21		ルーティングヘッダー(Type 0)を持つパケットは転送しないこと。	必須(MUST)
SEC-22	GEN-4	WAN 側インターフェースで受信した DNS や NTP の問い合わせは処理しないこと。	必須(MUST)
SEC-23	LAN-8	WAN 側インターフェースで受信した DHCPv6 の要求メッセージは処理しないこと。	必須(MUST)
SEC-24		WebUI 等の設定インターフェースは、デフォルト設定では WAN 側からはアクセスできないようにすること。	必須(MUST)

8. 検討メンバー

下記に検討メンバーを示す。順序は所属の 50 音順に従っている。

氏名	所属
川島 正伸(部会長)	NEC プラットフォームズ株式会社
藤崎 智宏(部会長)	NTT コミュニケーションズ株式会社
佐原 具幸(部会長)	株式会社インターネットイニシアティブ
鈴木 聡介	NTT コミュニケーションズ株式会社
田畑 敬司	株式会社アイ・オー・データ機器
高津戸 敦	株式会社ネクステック
稲田 哲也	株式会社バッファロー
太田 将博	ヤマハ株式会社