IPv6 家庭用ルータ
ガイドライン

【第 2.0 版】

2010 年 7 月 29 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
0.9	2009 年 5 月 22 日	パブリックコメント版
1.0	2009 年 6 月 22 日	第 1 版 若干の修正、未検討項目の作成
2.0	2010 年 7 月 29 日	第 2 版 アドレス利用の考察追加、ユーザインターフェース追加、 検討機能への連番付与

目次

1 はじめに

1.1 当該文書の背景と目的

IPv6 普及･高度化推進協議会[1]（以下､v6 協議会）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 2009 年 6 月 22 日に公開した「IPv6 家庭用ルータガイドライン 第 1 版」の検討開始から既に一ヶ年が経過しようとしている。

第 1 版作成後の振り返りの中で国際的貢献、議論の反映、視点が不十分等大きく３つの課題が挙げられたことから、第２版作成と同時進行で第 1 版の英語化を実施し、2010 年 4 月 27 日に v6 協議会のウェブページ[3]にて公開した。また、国際的議論／視点を補足するために Broadband Forum[4]（以下、BBF）と本 SWG が主体となり v6 協議会がリエゾン（連携）を締結し相互協力できる体制も構築している最中である。

第 1 版では、パブリックコメントとして幅広いご意見を収集し反映させることでより使いやすいガイドラインとしたが、ご意見の一部について、検討に時間を要するものがあったことから、それらを今回の検討課題とし、完成と同時にそれらを第 2 版に反映させることにした。第 2 版は第 1 版とほぼ同じ章構成としているが各章の内容について追加・変更等見直しを実施し、また、幾つかの新規項目追加を行いながら議論を行った。

議論を行う過程において、IPv4 アドレス枯渇、IPv6 に関連する公開資料等も更新され、その一つとして IPv4 アドレス枯渇対応タスクフォースが 2009 年 2 月に公開したアクションプラン 2009.2 版は 2009.10 版を経て 2010.06 版として改版され、NTT フレッツ光ネクスト IPv6 サービス提供開始時期をターゲットにした推奨スケジュールと共に各種最新状況に合わせた見直しと修正を反映させたものとなっている（図 1-1）。

[1] IPv6 普及・高度化推進協議会：http://www.v6pc.jp/
[2] IPv6 家庭用ルータ SWG：http://www.v6pc.jp/jp/wg/coexistenceWG/v6hgw-swg.phtml
[3] 第 1 版ガイドラインの英語版：http:// www.v6pc.jp/en/wg/coexistenceWG/v6hgw-swg.phtml
[4] Broadband Forum：http://www.broadband-forum.org/

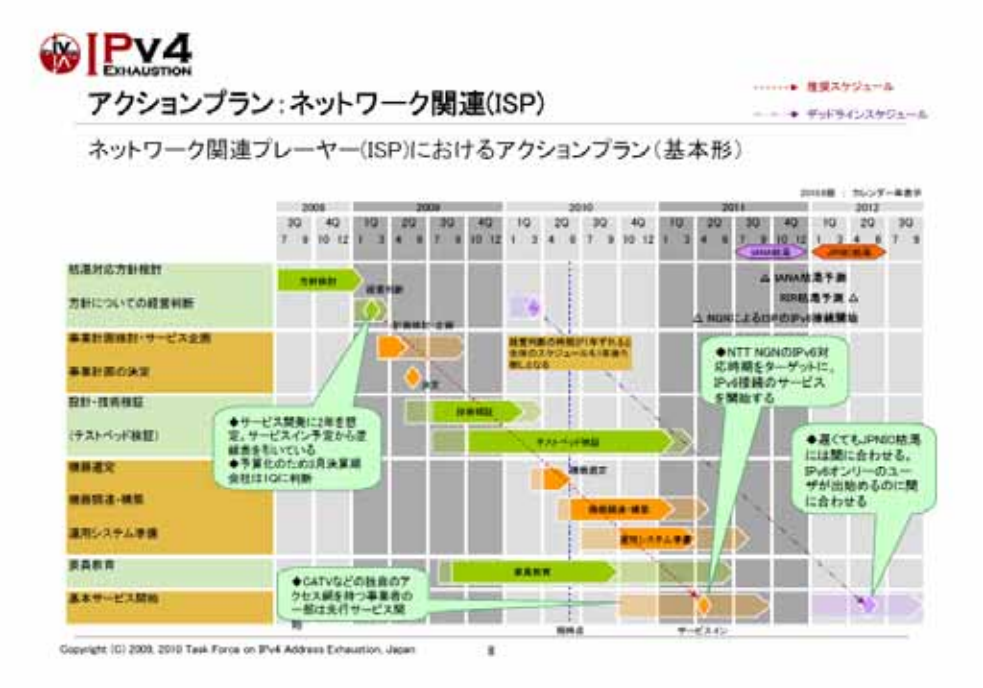

図 1-1　IPv4 アドレス枯渇タスクフォースによるアクションプラン[5]

また、総務省「IPv6 によるインターネットの利用高度化に関する研究会」にて検討された「ISP の IPv4 アドレス在庫枯渇対応に関する情報公開ガイドライン」[6]、IPv4 アドレス枯渇対応タスクフォース「IPv6 サービスリスト」[7]等の公開により、各事業者の IPv6 導入検討／対応状況が明らかとなってきた。このような中、通信事業者ごとの IPv6 サービス提供形態等に差異があり、それにより提供される機能等が異なる可能性があると考えられたことから本資料を補完する目的で「日本におけるブロードバンドアクセス回線の種類」について検討を実施した（付録として別資料とした）。ここでは 2010 年 5 月時点におけるブロードバンド回線として FTTH、ADSL、CATV、BWA の 4 種類に大別し、各通信事業者の IPv6 に関するサービス提供概要を簡素にまとめ、まずは NTT 東西が提供する「フレッツ光ネクスト」の IPv6 サービス概要、及び CATV サービス概要をまとめている。

なお、IPv4 アドレス在庫枯渇に関する各種情報は随時更新され、現在の予測[8]では IANA（Internet Assigned Numbers Authority）から RIR（Regional Internet Registry）への IPv4 アドレスの最終割り振りは 2011 年中盤から後半と予測されている。

---

[5] 出展:IPv4アドレス枯渇対応タスクフォース「IPv4アドレス枯渇対応アクションプラン　2010.06版　アクションプラン：ネットワーク関連(ISP)」から
参照 URL：http://www.kokatsu.jp/blog/ipv4/news/ActionPlan_20100607.pdf

[6] 総務省 ISP の IPv4 アドレス在庫枯渇対応に関する情報公開ガイドライン」：
http://www.soumu.go.jp/menu_news/s-news/02kiban04_000022.html

[7] IPv4 アドレス枯渇対応タスクフォース IPv6 サービスリスト：
http://www.kokatsu.jp/blog/ipv4/data/ipv6service-list.html

[8] Geoff Huston 氏の IPv4 アドレス枯渇時期公開サイト：http://ipv4.potaroo.net/

本ガイドラインは、第 1 版に引き続き「IPv6 家庭用ルータ SWG」にて検討を進めてきた内容を、具体的なアウトプット「IPv6 家庭用ルータガイドライン 第 2 版」としてまとめたものである。本ガイドラインが、家庭用ルータの実装者及びサービス提供者（本ガイドラインでは ISP を含めた IPv6 接続事業を提供する事業者をサービス提供者という表現で統一して扱う）における IPv6 接続サービスの仕様策定等に対して参考になれば幸いである。

＜参考情報＞　v6 協議会「サーティフィケーション WG」の活動紹介

v6 協議会では、IPv4/IPv6 共存 WG の他にも様々な WG が活動している。その中の一つであるサーティフィケーション WG（主査：江崎浩東大院教授）では、「IPv6 Ready Logo Program」[9]を推進している。このプログラムは、IPv6 実装が、IETF の RFC に基づき運用可能な事を実証し、ユーザへの信頼性向上を図ることを目的とした国際 NPO 法人 IPv6Forum により運用されているテストプログラムである。このプログラムでは、RFC に準拠している事を確認する手段として、試験仕様（test specification）とそれに基づく Self-test tool を無償で公開している。IPv6 実装におけるプロトコルとしての動作検証を行う際には、大変有用なプログラムであり、IPv6 家庭用ルータの動作検証にも有効である。

[9] IPv6 Ready Logo Program：
http://www.ipv6ready.org/（英文サイト）
http://ipv6.jate.jp/ready（JATE による日本語翻訳サイト）

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（ユーザ宅内に設置される小型ルータ）を介して家庭内ネットワークをサービス提供者に接続する環境を想定している。IPv6 接続サービスはデュアルスタック環境を想定しており、IPv4 機器の通信は IPv4 で行うことを前提として検討する。IPv4 アドレス枯渇による環境の変化に伴い必要となる LSN（Large Scale NAT）等の機能に関しては対象外としている。

下記に、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
- ホットスポット等の公共のネットワーク
- クライアント端末が直接接続するネットワーク
- 多段 NAT 等のミドルボックスを併用したネットワーク

また、想定する IPv6 家庭用ルータは、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となる。

本ガイドラインは、特に、下記の方々に読まれることを旨として記述している。

- 家庭用ルータを設計・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に関して

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」[10]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。上記に記述されていない用語に関して以下に解説する。

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、いわゆる 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（ACS：Auto Configuration Server）との間の通信を定義している[44]。
UPnP	Universal Plug and Play。UPnP Forum の定める技術仕様の総称であり、機器を接続しただけでネットワークに参加することを可能とすることを目的としている。具体的には、機器の持つ機能の記述や動作の制御等の情報を XML で記述し、それを SOAP/HTTP 等の既存プロトコルにより送信する[45]。

IPv4 アドレスと IPv6 アドレス双方を持つ表現として、「IPv4/IPv6」という表現方法を用いている。また、IPv6 アドレスのプレフィックスサイズを比較する表現には「（プレフィックス長が）短い／長い」を用いており、その定義を以下に明示する。

・/35 より短い：プレフィックス長が 35 ビットより短いことを意味する　　例）/32
　　プレフィックスサイズとしてはその空間が広いことを示す
・/35 より長い：プレフィックス長が 35 ビットより長いことを意味する　　例）/64
　　プレフィックスサイズとしてはその空間が狭いことを示す

[10] IPv6 関連用語集（IAJapan）：http://www.iajapan.org/ipv6/v6term/glossary_01.html

1.4　ガイドライン作成にあたり

本節では、本ガイドラインにて取り上げる家庭用ルータの機能に関する概要をまとめ、本ガイドラインの構成を解説する。

1.4.1 サービス提供者が提供する基本機能

本ガイドラインが想定するサービス提供者による IPv6 接続サービスは、図 1-2 に示すように大きく 4 つの機能に分けることができる。

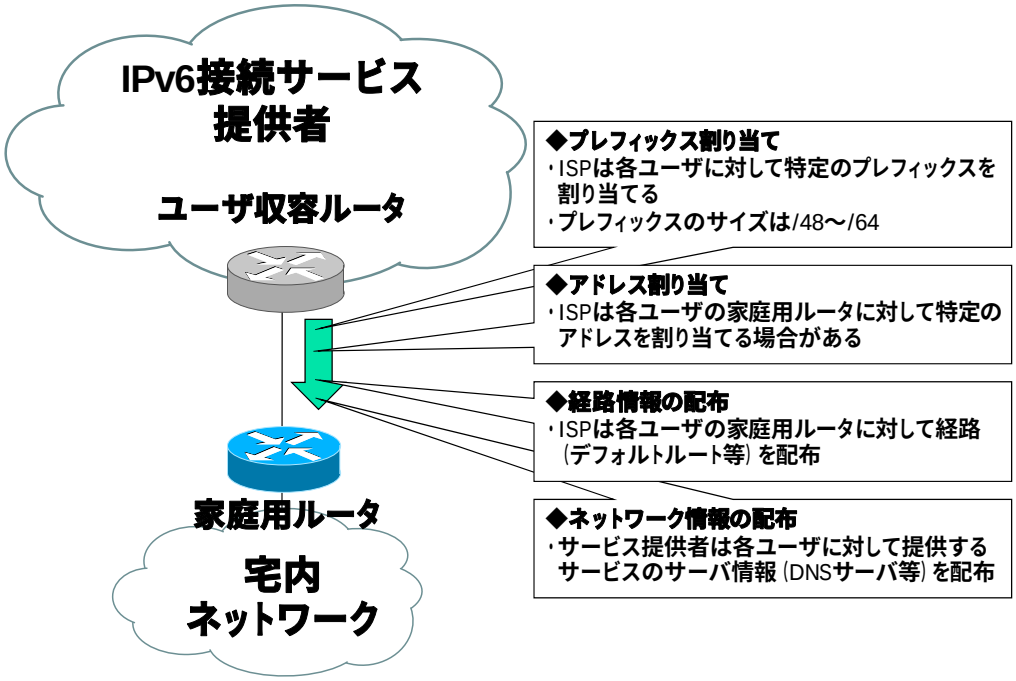

図 1-2　サービス提供者のサービス形態概略

・プレフィックス割り当て

IPv6 では、IPv4 における接続サービスと異なり、プレフィックス単位でのアドレス割り当てが必要となる。割り当てプレフィックスサイズはサービスにより異なるが、概ねプレフィックス長が/64 から/48 の間と想定される[8]。

・アドレス割り当て

IPv6 の家庭用ルータの WAN 側インターフェースに対して、サービス提供者側から回線の死活監視等の目的でアドレスを付与する場合が考えられる。

・経路情報の配布

基本的に IPv4 の場合と同様に、サービス提供者からはデフォルトルートがユーザ側に設定される。

・ネットワーク情報の配布
サービス提供者がユーザに対して提供するサーバ情報は、静的な文字情報として伝えられるだけではなく、DHCP 等によって配布されることが一般的である。

上記のような仕組みが想定される環境を前提に、家庭用ルータが実装する必要がある機能の整理に努めた。

1.4.2 宅内ネットワークの概略

家庭用ルータでは、前述したサービス提供者側から付与される各ネットワーク情報を宅内ネットワークに再配布及び割り当てる必要がある。本ガイドラインでは、宅内ネットワークの設定に関して次のルータ機能を取り上げている。

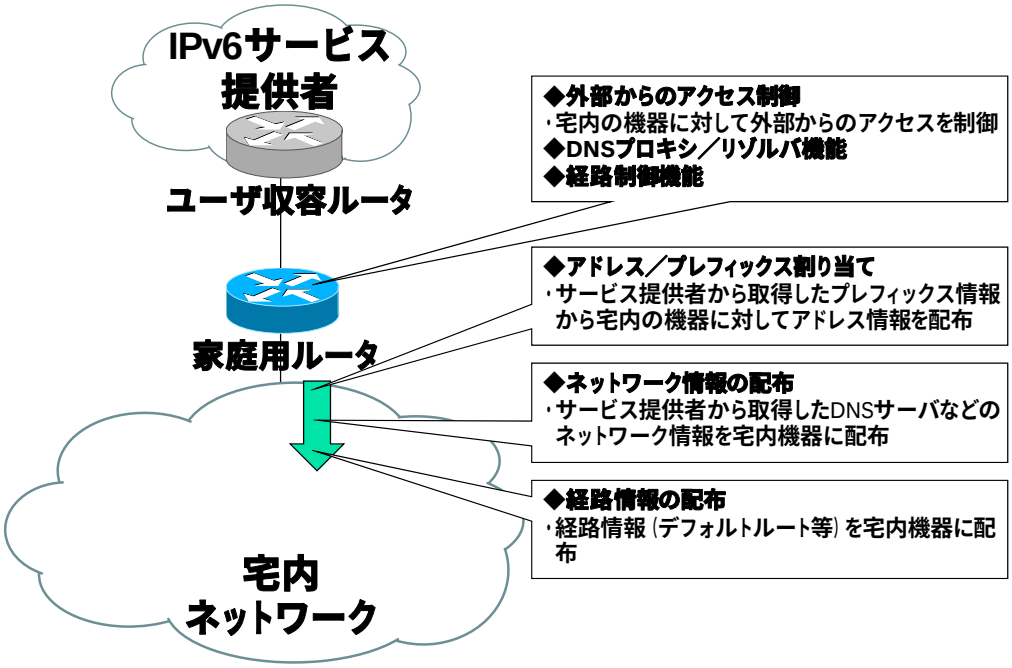

図 1-3　宅内ネットワークの設定概要

・アドレス／プレフィックスの割り当て
サービス提供者側から割り当てられたアドレス空間を用い、宅内の LAN に対してプレフィックスやアドレスをクライアント端末に割り当てる機能。動的・静的等様々な手法が考えられる。

・ネットワーク情報の配布
DNS サーバ等の情報をクライアント端末に配布する機能。標準化されているいくつかの手法が存在する。

・経路情報の配布
クライアント端末に対する経路情報としてはデフォルトルートのみを配布する形が一般的と考えられる。

・外部からのアクセス制御
IPv6 でも、IPv4 の場合と同様に宅内への通信制御が必要とされる。特に、IPv6 ではグローバルアドレスで宅内ネットワークが構成される可能性が高いため、外部からのアクセス制御は重要と考えられる。
・DNS プロキシ／リゾルバ機能
クライアント端末から直接サービス提供者の提供する DNS サーバを利用することも可能であるが、IPv4 の場合と同じように DNS プロキシ機能を有する場合が想定される。
・経路制御
IPv4 の場合と異なり、割り当てアドレス空間が広く、未使用空間が出現することへの対応が求められる。また、提供サービスに依存するが、マルチキャストに対する実装が必要になるケースも想定される。

1.4.3 アドレス／プレフィックスに関する考察

IPv6 接続サービスにおける接続形態に関して、一般的な手法は明確になっておらず、サービス提供者により異なることが想定される。本節において、サービス提供者が取りうるアドレス／プレフィックスの割り当て手法の整理と、宅内通信で利用するアドレスに関しての整理を行う。

1.4.3.1 WAN 側アドレスに関して

IPv4 接続サービスでは、一般的に 1 つのアドレスをユーザに割り当てる手法が取られていたが、IPv6 では次の 3 つの形態が考えられる。

1. WAN 側のアドレスをユーザ割り当てプレフィックスと別に割り当てる
   サービス提供者のネットワーク範囲を家庭用ルータの WAN 側インターフェースまでとするモデルで、次の点に注意が必要となる。
   - サービス提供者は、家庭用ルータのインターフェースまでのネットワーク設計が必要で、アクセス回線セグメントのアドレス管理が求められる。
   - ユーザに対して割り当てられたアドレス空間以外のアドレスが家庭用ルータに設定されていることを知らせておく必要がある。これはセキュリティの観点から重要である。
2. WAN 側のアドレスをユーザ割り当てプレフィックス内から割り当てる
   サービス提供者のネットワーク範囲を顧客収容ルータまでとするモデルで、次の点に注意が必要となる。
   - ユーザに割り当てるアドレス空間の中から、WAN 側に割り当てるアドレスを選ぶルール策定が必要である。最も若番のプレフィックスを WAN 側に割り当て、ホスト ID は若番をサービス提供者側のルータに設定する等が考えられるが、一般的なルールは存在していない。

- ユーザの利便性を考えると、WAN 側のアドレスを自動的に設定する仕組みを家庭用ルータに用意する必要があるが、標準的な手法は確立されていない。

備考：上述した割り当てルールの一例を示す。

ユーザ割り当てプレフィックス：　2001:db8:2000::/48
WAN 側プレフィックス：　2001:db8:2000::/64
サービス提供者側ルータアドレス：　2001:db8:2000::1/64
家庭用ルータアドレス：　2001:db8:2000::2/64
LAN 側プレフィックス：　2001:db8:2000:1::/64

3. WAN 側のアドレスを割り当てない Weak Host Model で運用する
WAN 側はリンクローカルアドレスだけの運用となり、ルータ自信が外部と通信する際には LAN 側、もしくは仮想的なインターフェース（ループバックインターフェース等）のアドレスを始点アドレスとして利用するモデル。このモデルでは、次の点に注意が必要である。

- WAN 側にはリンクローカルアドレスのみとなるため、サービス提供者側からの導通確認ができない場合に、アクセス回線側の問題なのか家庭用ルータ内の問題なのかを切り分けることが難しくなる。切り分けのためにはアクセス回線上のリンクローカルアドレスでの通信確認が必要になる。

1.4.3.2　割り当てプレフィックスに関して

サービス提供者がユーザに配布するプレフィックスについては、固定的に割り当てるか、時間経過により変更するかの 2 つの形態が考えられる。

1. 固定プレフィックスによる割り当て
ユーザ情報に基づき、固定プレフィックスを割り当てるモデル。ユーザネットワークの安定動作や運用面を考えると、毎回同じプレフィックスを割り当てるほうが無難と言えるが、次の課題がある。

- 固定プレフィックスと MAC アドレスによるホスト ID の利用では、常に同じ IP アドレスを利用することとなるため、アドレス収集に因る攻撃対象になりやすい。
- 常に同じプレフィックスであるため、プライバシー拡張[64]による対応を行ったとしても、プレフィックスからユーザが同定できる可能性がある。

2. 非固定プレフィックスによる割り当て
時間の経過等によりユーザに割り当てるプレフィックスを変更するモデル。現状の IPv4 接続サービスではアドレスを非固定で割り当てる形態が多い。また、ユーザの通信プライバシーを担保するために必要という観点から利用が求められる可能性があるが、次の課題がある。

- プレフィックスが変更になった際のリナンバリング等、接続端末に対する要件に対して多くの制限がある。
- 家庭用ルータとしては、プレフィックス変更を検知できること（以前割り当てられたプレフィックスを記憶しておき、変更があった場合には適切に動作すること）や、通信中のセッションの扱い、変更時にユーザ宅内機器のリナンバリングに対応すること等の考慮が必要となる（3.3.3 節も参照）。

以上の概要を表 1-2 に整理する。

表 1-2　割り当てプレフィックスが固定／非固定による影響

	カテゴリ	具体的なイメージ	対象	セキュリティ/プライバシー
固定 ▲	サービス提供者との契約を解除する都度アドレスが変わる	ユーザが ISP-A から ISP-B に契約を変更する場合	運用管理が容易	攻撃の対象になっていないユーザは固定アドレスのメリットを享受
	場所が変わる都度アドレスが変わる	ユーザが引っ越しをする場合		プライバシー問題あり
	オペレーション都合の都度アドレスが変わる	ISP バックボーンの設計変更等数年に一回程度		
	ユーザの申告の都度アドレスが変わる	DoS 攻撃を受けたのでアドレスを変更したい場合	宅内すべてのアドレスが変わってしまう可能性がある	攻撃の対象になっているユーザは攻撃を回避できる
▼ 非固定	接続の都度アドレスが変わる	家庭用ルータもしくは PC を起動する度にアドレスが変わる（ユーザは気付かない程度）	・リンクダウン時 ・家庭用ルータ交換時	

1.4.3.3　宅内通信で利用するアドレスについて

宅内通信で利用可能なアドレスを大別すると 4 種類になる。IPv6 グローバルアドレス、IPv6 リンクローカルアドレス、IPv6 ULA、IPv4 プライベートアドレスである。宅内機器がインターネット上の機器と通信する際には、IPv6 グローバルアドレス又は当面 IPv4 グローバルアドレス（始点アドレスは IPv4 プライベートアドレス）の 2 種類の内の 1 つを利用することになると考えられるが、宅内通信に使うアドレスについては、上述 4 種類全てが考えられる。以下、それぞれの特徴について整理する。

1. IPv6 グローバルアドレス

   宅内ネットワークがサービス提供者との契約がある場合、宅内機器間通信において IPv6 グローバルアドレスを利用することが可能である。しかし、次のケースにおいて、通信が瞬間的又は長時間に渡り途切れる可能性があることを考慮しておく必要がある。

   - 宅内に払い出されているプレフィックスが変わる場合、宅内各端末が新アドレスに一斉に切り替わる際に一時的に宅内通信が切れる可能性がある。また、マルチプレフィックス環境となり、正しく始点アドレスが選択されない可能性がある。
   - 宅内に払い出されているプレフィックスが変わる場合、新アドレスへの切り替えに時間を要する端末が仮に存在する場合に、新アドレスの端末と旧アドレスの端末間で通信できなくなる可能性がある。
   - WAN 側回線の障害時や、ISP 等の上位サービス提供者との契約を解除する場合に、宅内ネットワークがインターネットから孤立するために、家庭用ルータへのプレフィックス払い出しが止まってしまう。その後、一定の時間が経過すると宅内の端末から IPv6 アドレスが自動削除されてしまい、IPv6 グローバルアドレスによる宅内通信が不可能となることが考えられる。

2. IPv6 リンクローカルアドレス

   IPv6 の仕様上、宅内における全ての機器がリンクローカルアドレスによる通信に対応していることを前提とすることが可能である。従って、宅内通信でリンクローカルアドレスを使うことは妥当であると考えることができるが、次の課題がある。

   - 宅内にネットワークセグメントを複数設置する場合、ルータを跨ぐ別の宅内セグメントとの機器間で通信ができなくなる。

   備考：本ガイドラインでは、家庭用ルータは上位から/48 から/64 の範囲内のプレフィックスを受け取り、そのうち /64 を 1 ブロックずつ切り出して LAN 側に再分配することを前提としている。従って、宅内には複数のセグメントが存在することを前提とすることが合理的である。

3. IPv6 ULA

   ULA は、宅内通信等の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である。宅内通信で ULA を使う場合、IPv6 グローバルアドレスや IPv6 リンクローカルアドレスの項に記述した課題は生じないが、次の課題がある。

   - 将来、IPv6 アドレス利用者が増え 2 進数表記で“1”から始まるアドレスがグローバルユニキャストアドレスとして使われることになった場合、始点アドレスのアドレス選択の面で問題が起きる可能性がある。現在使われているグローバルユニキャストアドレスは 2000::/3 であり、2 進数表記では”0010 0000 0000 0000 ….”と表記され”0”から始まっているため、現在この問題は発生しない（コラム参照）。

4. IPv4 プライベートアドレス
   全ての宅内機器に IPv4 プライベートアドレスが割り当てられている環境においては、宅内通信で IPv4 プライベートアドレスを利用することは可能であり、大きな問題は発生しない。
   しかし、将来、機器のコストダウン等のために IPv4 を実装せずに IPv6 のみに対応する機器が出現することが想定でき、その際、宅内通信のために IPv4 プライベートアドレスが使えなくなる。中長期的に設計を行う場合には IPv4 プライベートアドレスに頼るべきではない。

以上より、宅内通信用に使うアドレスには完璧なものは存在しない。本ガイドラインではどのアドレスについても推奨することができないため、引き続き幅広く有識者との情報交換等を行い、方向性を示したい。また、以上の概要を表 1-3 に整理する。

表 1-3　宅内通信で使用するアドレスの比較

アドレス種別	利用の条件	課題
IPv6 グローバルアドレス	・ BB 回線の契約があり正常に接続できること	・ BB 回線障害時には利用不可 ・ BB 回線解約時には利用不可
リンクローカルアドレス	・ 常時利用可能	・ 宅内をルータでセグメント分けした場合に利用不可（例：無線を別セグメントにする場合）
ULA	・ 家庭用ルータが ULA プレフィックスを生成できること ・ 常時利用可能	・ BB 回線を契約する場合は宅内に IPv6 グローバルアドレスと ULA が共存する ・ インターネット接続の場合はアドレスを使い分ける必要がある
IPv4 プライベートアドレス	・ 常時利用可能	・ 現在の宅内 IPv4 通信と同様 ・ 将来 IPv6 のみをサポートする端末が出てきた場合に対応不可となる

[コラム] アドレス選択の仕組み

機能概要

IPv6 では１つのインターフェースに複数のアドレスを付与できるため複数の始点アドレスを持つことになる。そのために、利用するアドレスを選択する手法を定義する必要があり、RFC3484[15]にて規定された。この RFC3484 では、以下のアルゴリズムを規定している。

- 始点アドレスが複数ある場合にどれを選択するかのアルゴリズム（8 ルール）
- 終点アドレスが複数ある場合にどれを選択するかのアルゴリズム（10 ルール）

アドレス選択のためのポリシーテーブル

始点アドレスや終点アドレスの選択において、ユーザが優先させるアドレスを明示的に指定可能にする仕組みとして”ポリシーテーブル”が定義されている。Precedence により終点アドレスの利用順序が決定され、Label により始点アドレスが終点アドレスの Label 値を元に決定される。表 1-1 は RFC3484 にて定義されているデフォルトのポリシーテーブルで、この定義から、終点アドレスとしては IPv4 アドレスよりも IPv6 アドレスを優先することや、6to4 アドレスと IPv6 アドレスの Label が異なるためこの組み合わせでのアドレスは選ばれにくいことなどが分かる。

表 1-4　RFC3484 におけるポリシーテーブルのデフォルト値

Prefix	Precedence	Label	Prefix の意味
::1/128	50	0	ループバックアドレス
::/0	40	1	IPv6 アドレス
2002::/16	30	2	6to4 アドレス
::/96	20	3	IPv4 互換アドレス
::ffff:0:0/96	10	4	IPv4 アドレス

スコープの概念

IPv6 ではアドレスの適用範囲を示すスコープの概念が導入されており、グローバル、サイトローカル、リンクローカルの三種類が定義されている。アドレス選択においては、このスコープが一致するものを優先する仕様となっている。なお、IPv4 アドレスに対するスコープに関してもこの RFC3484 にて規定されている。

Longest prefix match による始点アドレスの選択

Longest prefix match は、特にポリシーを設定しないときの最終手段として定義されており、IP アドレスのビット情報を左からより長く一致するもの（ネットワーク的に近しいもの）を選択する仕組みである。したがって、将来グローバルユニキャストアドレスとして 8000::/3 の範囲が割り振りされた場合、現状の仕様であれば ULA が始点アドレスとして選択されてしまうため問題が生じる。

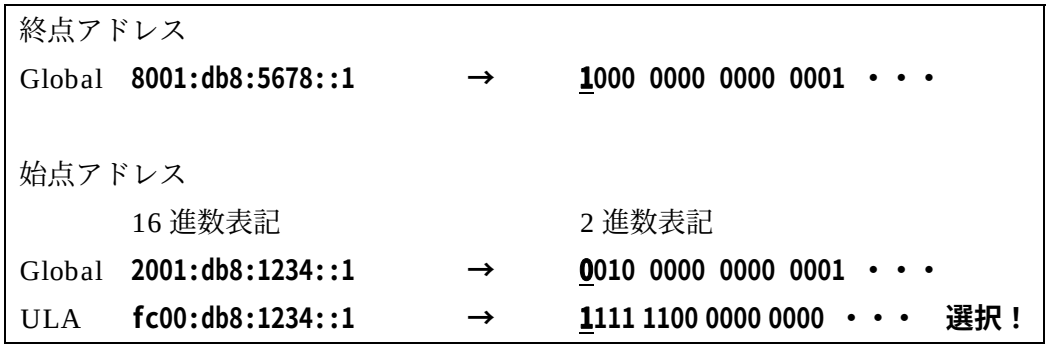

図 1-4　Longest prefix match によるアドレス選択

アドレス選択例

表 1-2 に、デフォルト設定により選ばれるアドレスの組み合わせ例を示す。このように複数の終点および始点アドレスが合った場合に、どのアドレスから利用するのかを必ず決定できる仕組みが規定されている。

表 1-5　デフォルトのルールにより選ばれるアドレスの組み合わせ例

始点アドレス	終点アドレス	選択される組	理由
s1: 192.0.2.1 s2: 2001:db8:1234::1	d1: 198.51.100.1 d2: 2001:db8:2:2::2	s2 - d2	Precedence の大きいものを優先
s1: 192.0.2.1 s2: 2001:db8:1234::1	d1: 198.51.100.1 d2: 2002: 836b:4179::1	s1 - d1	Label が一致する組を優先
s1: fe80::1 s2: 2001:db8:1234::1	d1: 2001:db8:2:2::2	s2 - d1	スコープが一致する組を優先
s1: 2001:db8:1234::1 s2: fc00:db8:1234::1	d1: 2001:db8:2:2::2	s1 - d1	最長一致のルールより

1.4.4 家庭用ルータに求められる機能

1.4.1 節及び 1.4.2 節で挙げた各サービス・機能を前提として、本ガイドラインで取り上げる家庭用ルータに求められる機能を表 1-6 のように整理した。

表 1-6　家庭用ルータに求められる機能概要と掲載章番号一覧

大項目	中項目	章番号
アドレス／プレフィックス設定機能	プレフィックス情報の受信	3.1
	アドレス／プレフィックス情報の配布	3.3, 5.2, 6.1
	WAN 側アドレス設定	3.2, 8.1.1
経路制御機能	経路設定	7.2
	不到達アドレス／プレフィックス制御	7.1
	マルチキャスト機能	7.3
アクセス制御機能	ルータ自身へのアクセス制御	4.1.4
	宅内ネットワークへのアクセス制御	4.1, 7.2.3
	制御ルール設定	4.1(4.1.2)
サーバ機能	DNS プロキシ機能	5.1, 5.2, 5.3, 5.4
	DNS リゾルバ機能	5.4.1
	ネットワーク情報の取得と配布	6.2, 8.2.4.2
	ルータ自身の設定機能	8.1, 8.2, 9.1, 9.2
その他	アドレス表記	9.3, 9.4

本ガイドラインでは、これらの機能を以下の章立てでまとめている。

第 2 章では、IPv6 接続サービスを提供するサービス提供者に対して接続する際に必要となる機能の整理を行う。ただし、2009 年度時点において、サービス提供者が提供する IPv6 接続サービスの形態が不明確であることから、この版では、IPv6 接続サービス形態の整理のみとしている。また合わせて、IPv4 アドレス枯渇時代における IPv4 接続サービス形態に関しても記載する。

第 3 章では、サービス提供者から割り当てられるアドレス空間の利用に焦点を当てて機能を整理する。具体的に利用するプロトコルに関しては第 6 章及び第 8 章にて記載する。

第 4 章では、外部からのアクセス制御に関して必要となる機能をまとめる。IPv6 ではエンドツーエンド接続が可能になるため、本機能の重要性も増すと考えられる。

第 5 章では、DNS サービス関連の機能をまとめる。IPv4 の場合と同様に DNS プロキシ等を実装する際に注意が必要な点等を整理する。

第 6 章では、宅内ネットワーク設定の視点から整理を行う。

第 7 章では、経路制御に関する機能をまとめており、マルチキャスト利用についても触れる。

第 8 章では、IPv6 接続サービスを提供するサービス提供者側から必要となる機能としての整理を行う。大半の機能がここまでにまとめた機能となるためポインタを記載している。

第 9 章では、ユーザインターフェースに関する機能をまとめる。

以上のように家庭用ルータに求められる機能を整理し、詳細機能を表 1-7 に挙げる項目に整理して必要性をまとめている。

表 1-7　詳細機能（小項目）の記載項目説明

項目	意味
前提：	本要件に対する前提条件を記載
要件：	家庭用ルータに必要な詳細機能の概要を記載
必要度：	取りあげた要件の必要性を"必須/推奨/オプション"で表現 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
理由：	要件として挙げた機能の必要度を導き出した事由を記載
備考：	必要度を決める際に議論された経過情報等を記載

第 10 章では、第 3 章から第 9 章までに定義した要件とその必要度を一覧表としてまとめ、また、ガイドライン第 1 版からの差分を追記している。なお、最後に掲載する参考文献は、本文内で参照した時点におけるものとしているため、インターネットドラフトなどは旧版を参照している場合がある。

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サービスを利用する際に、家庭用ルータが必要とされる接続モデルに関してまとめる。ただし、本ガイドライン検討時点において、サービス提供者による IPv6 ネットワークのリーチャビリティの提供手法が不明確であることから、どのような接続形態が存在し得るのかについての整理のみとしている。したがって、この章では、ルータに必要とされる機能定義は行っていない。また、各接続形態におけるユーザ認証に関連する機能に関しても対象外としている。

2.1 IPv6 接続モデル

この節では、エンドユーザがインターネットと IPv6 通信をするための、家庭用ルータ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

家庭用ルータでトンネル等を終端しない接続方式で 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。

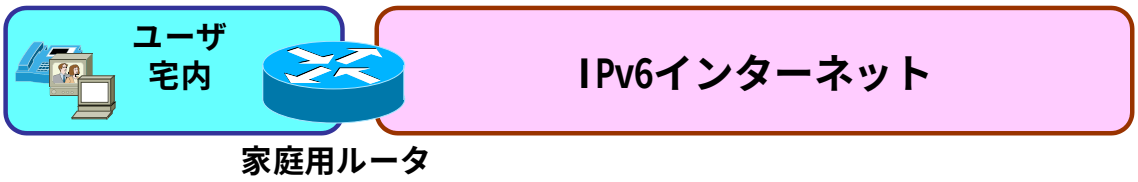

図 2-1　ネイティブ接続

2.1.2 PPPoE/PPPoA

PPP を利用して、ユーザ宅内へ 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[1][2][3]。

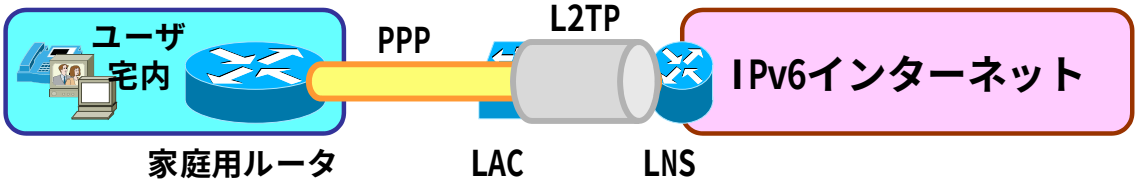

図 2-2　PPPoE/PPPoA 接続

2.1.3 IP ベースのトンネル（IPv6 over IPv4 等）

2.1.3.1　接続形態

IP でのカプセリングを利用し、ユーザ宅内へ 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[4][5][6][7]。

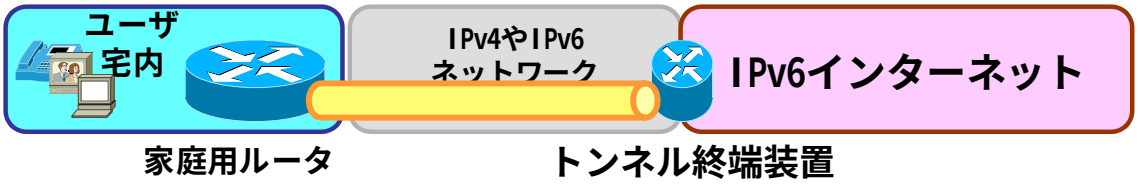

図 2-3　IP ベースのトンネル接続

2.1.3.2　6to4

IPv4 Internet の中に点在する IPv6（6to4）サイト間を、IPv6 パケットを IPv4 ヘッダでカプセル化して転送する方式である[4]。IPv4 グローバルアドレス x.y.z.w が割り当てられているホストを、IPv6 プレフィックス（2002:x.y.z.w::/48）のサイトへの入り口として１対１に紐付ける。2002:x.y.z.w::/48 のアドレス形式を持つ 6to4 サイト間では、IPv6 over IPv4 カプセル化する際に、x.y.z.w 部分を解釈し、あて先 IPv6 アドレスに紐付けられた IPv4 ホストアドレスに向けて、直接 IPv4 パケットを送信する。6to4 サイトと 2002::/16 以外の IPv6 端末との通信には、6to4 ゲートウェイを経由する。

6to4 ゲートウェイが IPv6 インターネットへ広告する経路は 2002::/16 であり、後述する 6rd と比較してサービス提供者での経路制御等に制限がある。

2.1.3.3　6rd

6to4 と同じく IPv6 over IPv4 モデルであり、ユーザに付与した IPv4 アドレスの一部を IPv6 prefix の一部に埋め込む点では 6to4 と同様である。しかし、6to4 は 2002:で始まるプレフィックスしか使えなかったところを、ユーザあたりのネットワークを 6to4 の/48 よりも小さくすることにより、提供事業者の prefix を使用できるようにした方式である[53]。

例えば、サービス提供者に割り振られた prefix が 2001:db8::/32 であり、ユーザの CPE に付与された IPv4 アドレス x.y.z.w の下位 24bit のみをマッピングに使用する場合、2001:db8:y.z.w::/56 のプレフィックス宛パケットが当該 6rd ルータの配下にあると想定されて転送される。

6to4 と比較すると、サービス提供者に割り振られた prefix で経路広告できるため、サービス提供者での経路制御の自由度が高まる。

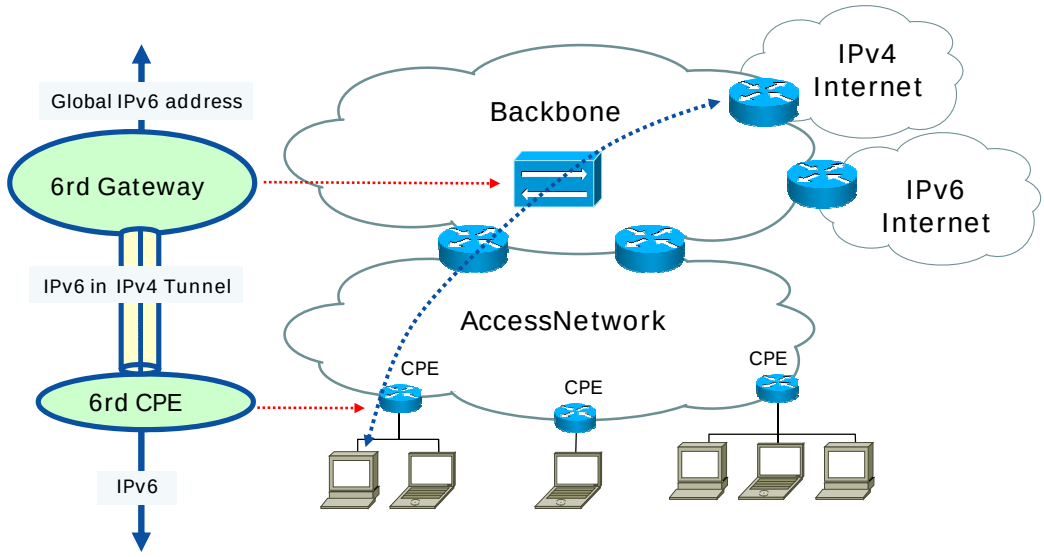

図 2-4　6rd のネットワーク構成図[11]

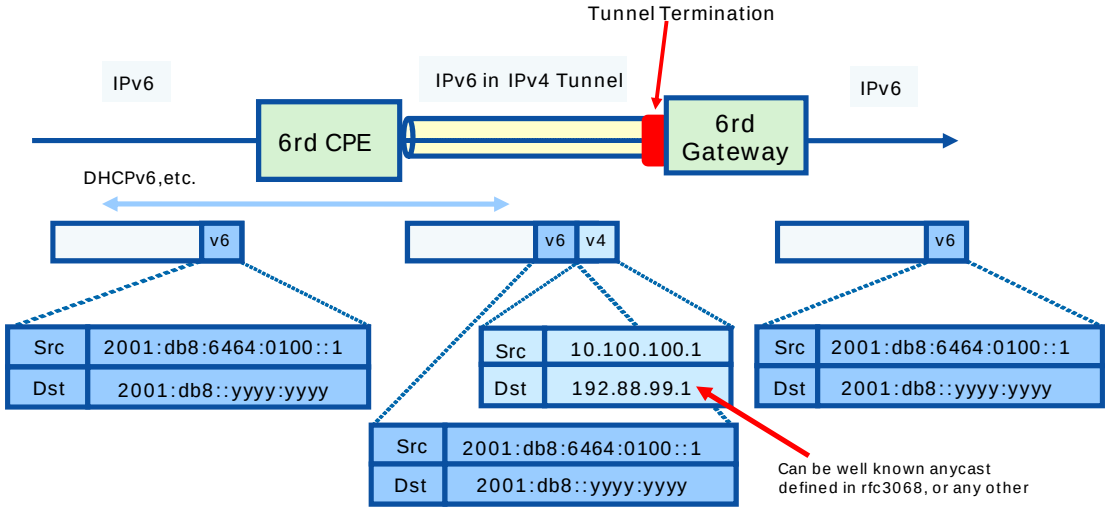

図 2-5　6rd のパケットフロー

2.1.3.4　Softwire with L2TPv2

上記 2 モデルと同様に IPv6 over IPv4 モデルであるが、本モデルではユーザ宅内の端末と ISP 側ゲートウェイを L2TP トンネルにより接続することにより、CPE 及び ISP 側中継網での IPv6 対応を必要とせず、エンドユーザへ IPv6 インターネットへの接続性が提供できることが特徴となる[62]。

[11] 図 2-4～図 2-13 は第 2 回 IPv6 Operation Forum 資料を基に作成

2.2　IPv4 接続モデル

この節では、IPv4 アドレスが枯渇し始めた際にエンドユーザがインターネットと 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 NAT444

サービス提供者が IPv4 NAT 機能を備えた装置（Large Scale NAT または LSN、もしくは、Carrier Grade NAT または CGN）を用意し、複数のエンドユーザが 1 つの IPv4 アドレスを共有するモデルである[54]。

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、NAT444 モデルにおいては CPE から LSN を介して通信する。

ユーザ端末からインターネットに向けて送信された IPv4 パケットは CPE において IPv4 NAT を行い LSN に転送される。LSN でも IPv4 NAT を行ってインターネット側に転送する。CPE と LSN のそれぞれで IPv4 NAT（NAT44）を行うため、NAT44+NAT44 で NAT444 と呼ぶ。

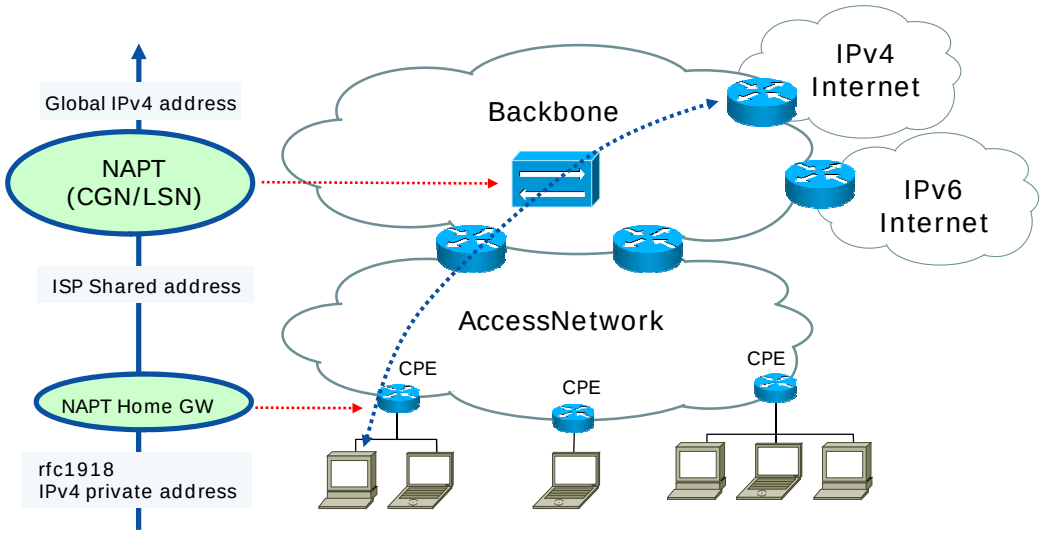

図 2-6　NAT444 のネットワーク構成図

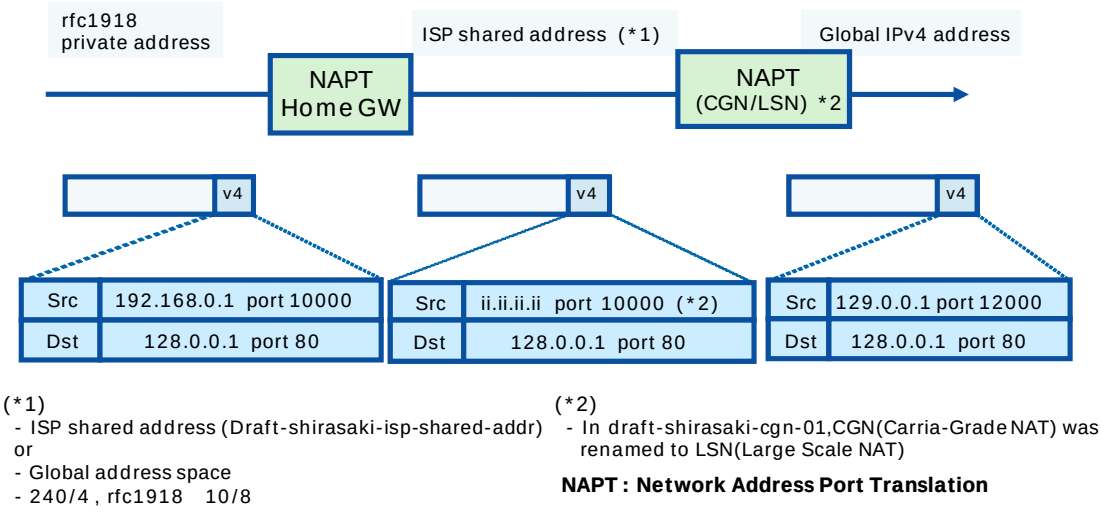

図 2-7　NAT444 のパケットフロー

このモデルの特徴は以下の通りである。

- 現在の CPE を変更する必要がない
- NAPT は既に普及しており実績のある機能である（LSN の実装は既存の NAT とは多少異なる）
- LSN でセッション状態を保持する必要があり、LSN のスケーラビリティに懸念がある
- 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

2.2.2 DS-Lite（Dual-Stack 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 機能を不使用とする方式である[55]。

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 から AFTR を介し、複数のサービス提供者加入者で 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。

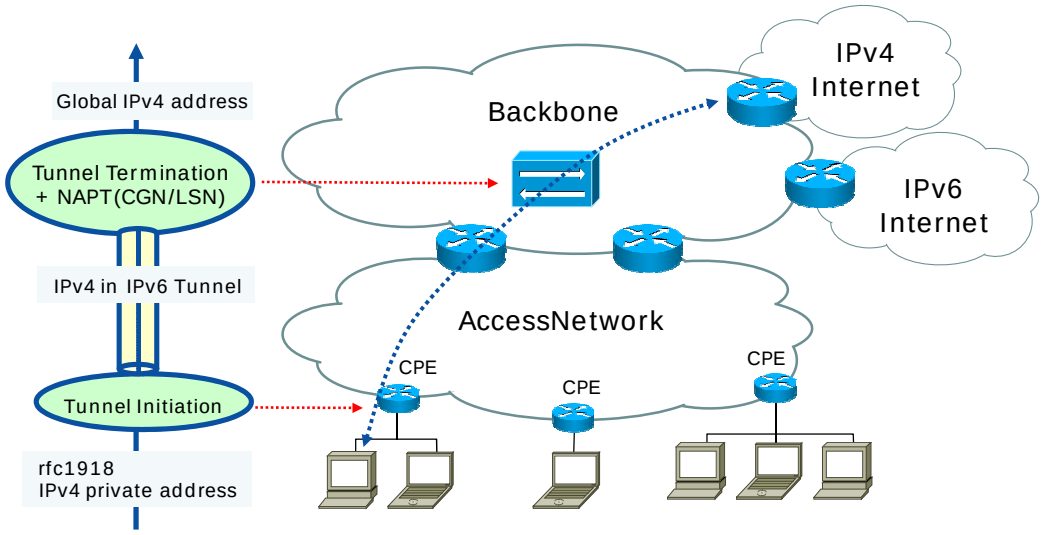

図 2-8　DS-lite のネットワーク構成図

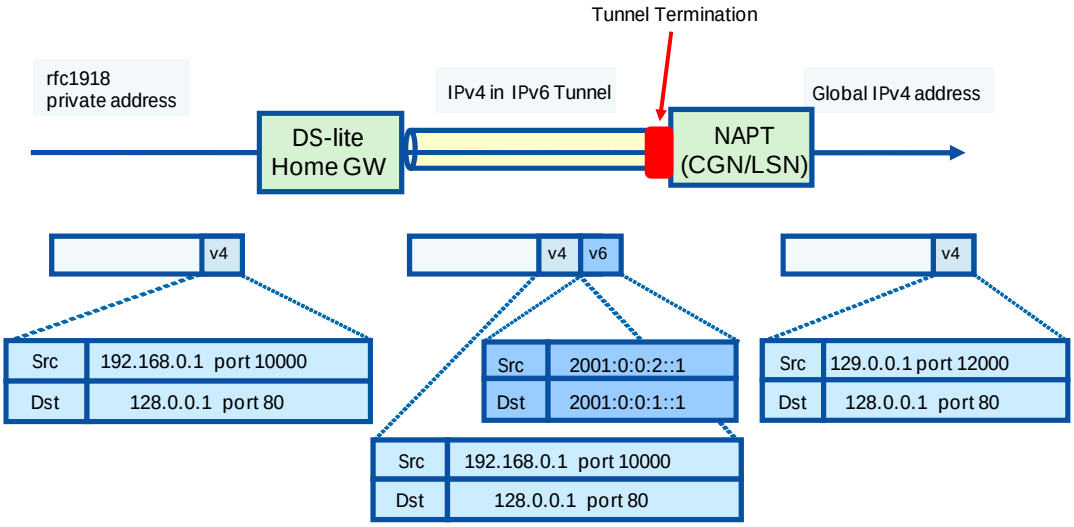

図 2-9　　DS-lite のパケットフロー

このモデルの特徴は以下の通りである。

- CPE の変更が必要
- 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 間はトンネルリンクのため、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
- DS-Lite LSN の実装は既存の NAT とは異なる

2.2.3 A+P

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、サービス提供者はユーザに IPv4 アドレス 1 個と、(例えば、あるユーザには 4096～8191 の 4096 個与える、のように) ポート番号の範囲を指定し割り当てることで、複数の CPE（ユーザ）間で１つの IPv4 グローバルアドレスを共有する[56]。

サービス提供者は IPv4 Internet 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装置(A+P ルータ装置)を設置する。振り分けた後のパケットを A+P 装置と CPE の間で転送する手段については特に規定していないため、PPP、IPv4 over IPv6、L2TP 等の技術と組み合わせて使用する。

NAT 444 の LSN や、DS-Lite の AFTR と違い、A+P 装置では IPv4 NAT の機能無しで、IPv4 グローバルアドレスをサービス提供者の複数のユーザ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。

課題としては、CPE の置き換えが必要なこと、サービス提供者網内に A+P ルータ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私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[57]。

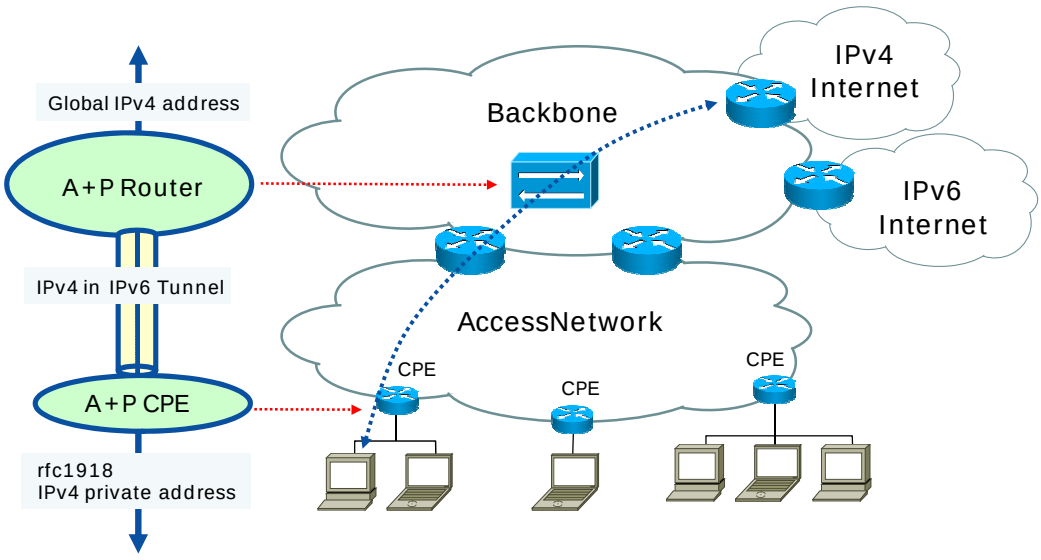

図 2-10　A+P のネットワーク構成図

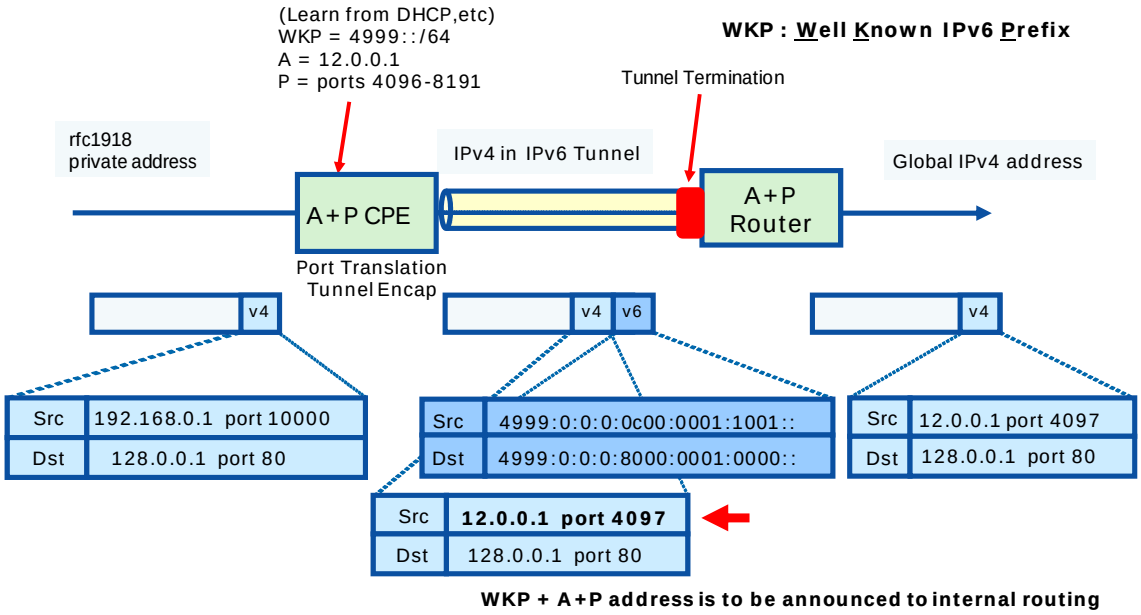

図 2-11　A+P のパケットフロー

2.3　IPv6-IPv4 相互通信モデル

この節では、IPv6 端末と IPv4 端末を相互に通信させるために利用可能と思われるネットワークモデルを紹介する。

2.3.1 NAT64（IPv6→IPv4 Translator）

NAT64 と DNS64 を利用して、IPv6 only のクライアントから IPv4 サーバへのアクセスを実現するモデルである[58]。

図 2-13 において、まず、IPv6 only のクライアントから DNS ALG に、www.example.com の IPv6 アドレスを問合わせる。DNS ALG では www.example.com 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 Translator にルーティングされる。Translator 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.com のアドレスである IPv4 アドレスに変換し、通信を行う。

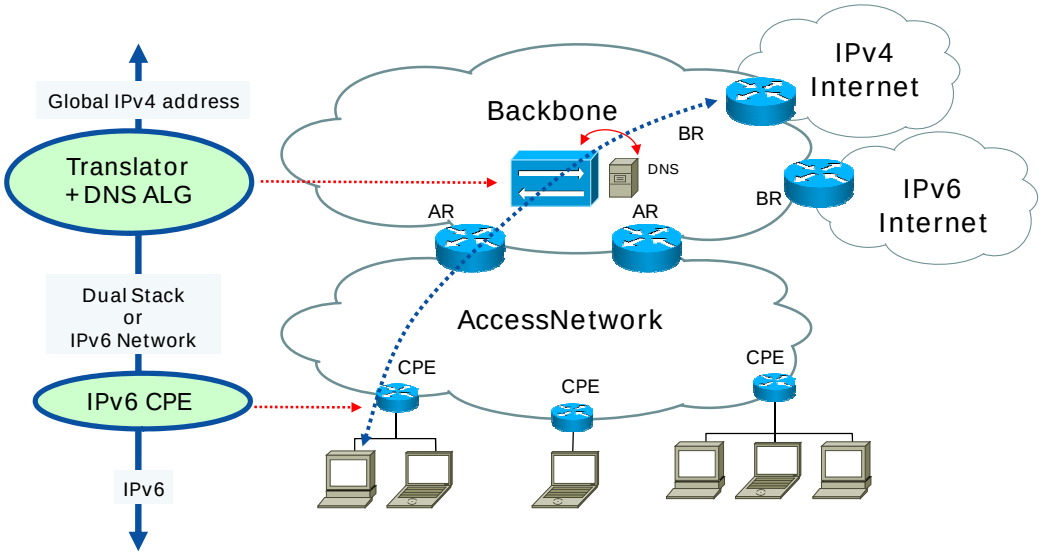

図 2-12　NAT64 のネットワーク構成図

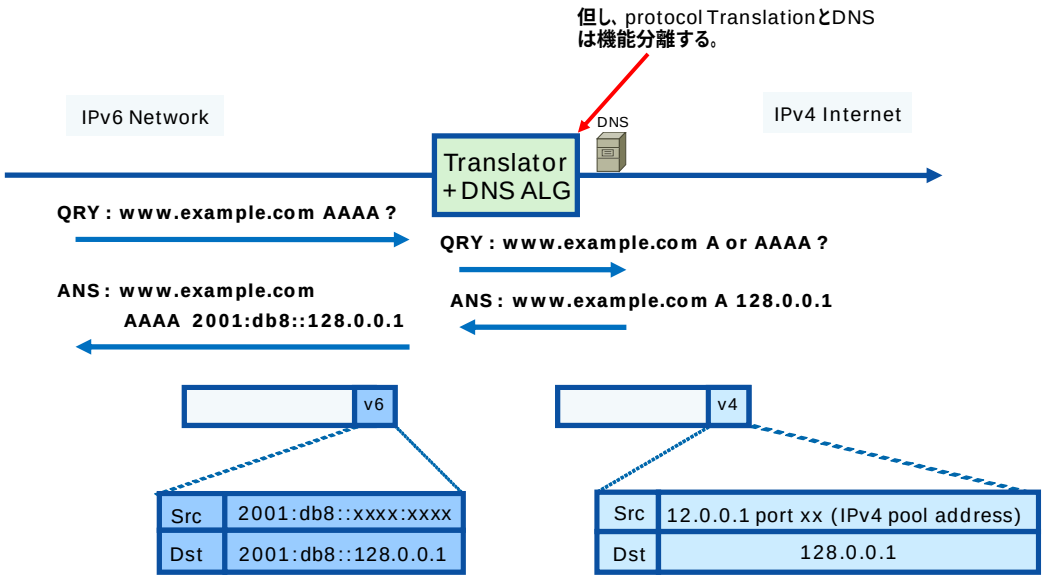

図 2-13　NAT64 のパケットフロー

2.4　IPv6 利用時課題解決モデル

この節では、IPv6 利用時の課題解決モデルについて紹介する。

2.4.1 NAT66

インターフェース ID を変化させずにプレフィックスのみを変換するステートレスな（マッピングを覚えない）NAT 装置により、IPv6 アドレス同士で NAT を行うモデルである[12]。

3 アドレス割り当て機能

この章では、ルータの WAN 側、LAN 側及び LAN 側セグメントに接続される端末への各種アドレスの割り当て手法について述べる。

3.1 プレフィックス割り当て

本節では、サービス提供者がユーザにプレフィックスを割り当てる際に、ルータに求められる要求条件について記述する。

3.1.1 宅内ネットワークへ配布するプレフィックス情報

要件1： 宅内用プレフィックス情報を接続先サービス提供者から DHCPv6-PD にて取得できること。

必要度：必須（MUST）

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

要件2： 宅内用プレフィックス情報を手動設定できること。

必要度：必須（MUST）

理由：接続先サービス提供者が DHCPv6-PD によるプレフィックス配布に対応していない場合の対処のため。

3.1.2 宅内ネットワークへの割り当てプレフィックスサイズ

要件3： /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）

理由：「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」[8]において、エンドサイトには基本的に/48～/64 の割り当てを実施することが求められているため。

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。
企業網を考えた場合、/48 より短いプレフィックス長が割り当てられる可能性もあるが、本文書では企業網は検討の対象外とする。

3.2 WAN 側アドレス

本節では、1.4.3.1 節で述べたサービスモデルにおける家庭用ルータの WAN 側（サービス提供者との間のリンク）におけるアドレス付与について述べる。

3.2.1 グローバルアドレスの付与方法（自動）

要件4： 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こと。

必要度：必須（MUST）

理由：ユーザの手を介さない自動設定を実現するため。方式として、下記の両方式を必須とする。

[a] SLAAC（Stateless Address Auto Configuration）

[b] DHCPv6

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に設定させず自動判別させることも可能と考えられる[59]。

SLAAC を利用する際には、設定されたアドレスをサービス提供者へ通知する仕組み（DDNS 等）と併用しないと、サービス提供者が付与されたアドレスを知ることができない。

方式選択にあたっては、技術動向（2010 年 7 月現在、DHCPv6 ではプレフィックス長配布に別途ルータ広告／プレフィックスオプションとの併用が必要であること等）、IPv6 のグローバルユニキャストアドレスにおいては、インターフェース識別子が 64 ビット長であると規定されていること[46]、及び他要件（WAN 側に割り当てるアドレスプレフィックスサイズと、発生しうる問題（7.1 節））との兼ね合いも考慮が必要。

3.2.2 グローバルアドレスの付与方式（手動）

要件5： 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。

必要度：必須（MUST）

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。

3.2.3 グローバルアドレスが付与されない場合の対応

要件6： 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。

必要度：必須（MUST）

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、ルータ自身がパケットを送受信する必要があるため。

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。

3.3 LAN 側アドレス

本節では、家庭用ルータの LAN 側（ユーザ宅内ネットワークとの間のリンク）に対するアドレス付与について述べる。

3.3.1 プレフィックスの再配布

要件7： 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）

理由：サービス提供者がユーザ宅に配布したプレフィックスを、自動的に宅内の機器に再配布する手段が必要であるため。

備考：再配布するプロトコルは 6.1 節を参照。
/64 より広いプレフィックスを DHCPv6-PD で受け取った場合に、そこから一つの /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。

3.3.2 複数プレフィックスの受信

要件8： 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。

必要度：オプション（MAY）

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。

備考：固定プレフィックスと非固定プレフィックスをそれぞれ 1 つずつ配布するような接続サービスが考えられる。

固定プレフィックスと非固定プレフィックスにはそれぞれの利点があり、ユーザが選択できることが望ましい。

片方のプレフィックスを選択した場合に、特定のネットワークにアクセスできなくなるようなケースも考えられるため注意が必要である。

複数のサービス提供者から複数のプレフィックスを割り当てられている状態（マルチプレフィックス）では端末の挙動に問題が発生する場合がある[17]。

3.3.3 配布プレフィックスの変更

要件9： 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。

必要度：必須（MUST）

理由：時間の経過によりユーザ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。

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。

配布プレフィックスを変化させた際の家庭内端末のリナンバリングについては 6.1.2 節を参照。

3.3.4 ULA プレフィックスの生成及び配布

要件10：サービス提供者からプレフィックス情報を取得していない場合、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。

必要度：推奨（SHOULD）

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。

備考：ULA の仕様は RFC4193 に準拠すること。

参考文献[59]では ULA の使用が必須（MUST）となっている。

ULA プレフィックスの配布後にサービス提供者からプレフィックス情報を取得した場合、リナンバリングが必要。

4 セキュリティ機能

本章では、ユーザ宅内ネットワークを保護するために最低限必要と考えるセキュリティ機能について述べる。ここで取り上げる機能は、完全性（データ改ざん防止・検知・復旧等）機密性（暗号化等）、可用性（設定等を含む利便性等）を実現するための最低限必要な要素である。ユーザ側のセキュリティに対する意識とともに、これらを組み合わせた形での柔軟な対応を行なっていく必要がある[60][61]。

4.1 アクセス制御機能

4.1.1 外部からのアクセスの制限

前提条件として、IPv6 の家庭用ルータにおいても、IPv4 の場合に取られていたセキュリティ機能（NAT/NAPT により外部ネットワークから直接宅内ネットワークへの到達性が失われていた点も含む）は必要とする。

4.1.1.1 アクセス制限の基本設定

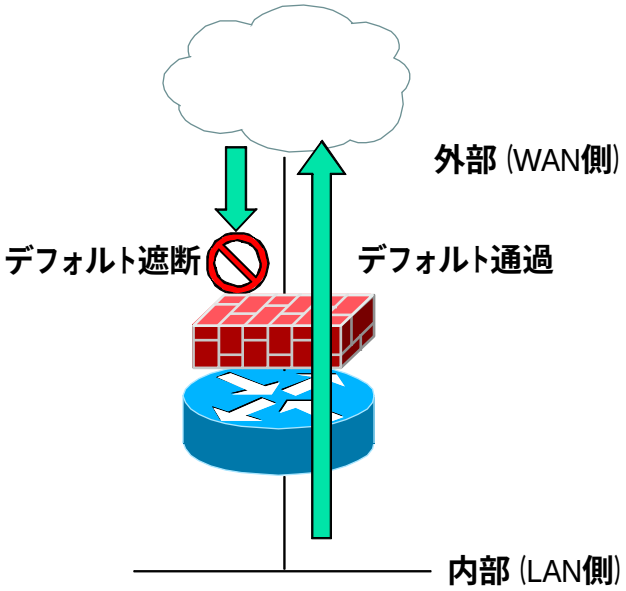

図 4-1 外部からのアクセス制御機能

要件11：内部（LAN 側）から外部（WAN 側）への通信は通過させ、外部から内部への通信は遮断するアクセス制限が行えること。

必要度：必須（MUST）

理由：現在の IPv4 家庭用ルータの初期動作と同等のアクセス制御が必要であるため。

備考：デフォルトの挙動では外部から内部への通信を遮断としているが、設定により通信可能にできることも同時に必要である（4.1.2 節も参照のこと）。

4.1.1.2　静的フィルタによるアクセス制限

要件12：静的フィルタによりアクセスを制限できること。

- 内部から外部へは、デフォルトで通過させる。
- TCP は外部から内部への SYN をデフォルトで遮断する。
- UDP は外部から内部への通信はデフォルトで遮断する。
  ※ただし、DNS やその他サービス（電話、TV 等）依存で必須となるプロトコルは通過させる必要がある。
- ICMPv6 は外部から内部へ必須なメッセージ[9]のみ通過させ、その他はデフォルトで遮断する。

必要度：必須（MUST）

理由：現行の IPv4 ネットワークにおける NAT により制限されていた最低限必要なネットワークセキュリティレベルを IPv6 でも維持するため。

備考：外部（WAN 側）のインターフェースに対しての IPv6 アドレスの設定を行うか否かは、サービス提供上の必要性とセキュリティを考慮する必要がある。
アクセス制御を実施する際には、フラグメントされたパケットの再構成を考慮して実装する必要がある（4.1.3 節も参照のこと）。
内側からのトラフィックにおいても始点が下記のアドレスである場合は遮断することを推奨する。

・サービス提供者が割り当てたアドレス以外のグローバルアドレス
・リンクローカルアドレス（fe80::/10）
・サイトローカルアドレス（fec0::/10、RFC3879 にて廃止）
・ULA（fc00::/7）
・マルチキャストアドレス（ff00::/8）
・ウェルノウンエニーキャストアドレス
　サブネットルータエニーキャストアドレス　等
・IANA リザーブアドレス（::/8）
　ループバックアドレス、未指定アドレス、IPv4 互換アドレス、
　IPv4 射影アドレス等
・ドキュメント用アドレス（2001:db8::/32）

4.1.1.3　動的フィルタ（SPI）によるアクセス制限

要件13：動的フィルタ（SPI）によりアクセスを制限できること。

- 内部から外部へは、デフォルトで通過させる。
- 内部から外部への通信があったコネクションを記憶し、このコネクションについては外部から内部へ通過させる。

必要度：推奨（SHOULD）

理由：現行の IPv4 動的フィルタ（SPI）相当のセキュリティレベルを IPv6 でも維持するため。ただし、静的フィルタ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推奨とする。

IPv6 でもセキュリティレベルを維持するために重要な機能であるため、推奨とする。

SPI に関しては、RFC 4787 の記述も参照のこと[47]。

SPI のステート管理において、タイマ設定による管理を考慮した実装を推奨とする。

4.1.2 アクセス制御のために設定できる機能及びその必要度

要件14：表 4-1 で示した機能についてアクセス制御を設定できること。

必要度：必須（MUST）

表 4-1　アクセス制御のために設定できる機能及びその必要度

機能	必要度
IPv6 始点/終点アドレスでアクセスを制限できること	必須（MUST）
次ヘッダを認識できること（7.2.3 節の参照）	必須（MUST）
プロトコル種別でアクセスを制限できること	推奨（SHOULD）
次ヘッダチェーンを辿ること	必須（MUST）
ICMP の Type と Code でアクセスを制限できること[9]	推奨（SHOULD）
TCP/UDP の始点/終点ポート番号でアクセスを制限できること	必須（MUST）

理由：現行の IPv4 ネットワークのセキュリティレベルを IPv6 でも維持するため[10]。

備考：次ヘッダチェーンを辿る際に、どの程度の深さまで辿る必要があるかは、規定しない。

トンネルを利用した通信を実現する場合、トンネルの内側アドレスに対応したアクセス制御の実装（DPI：Deep Packet Inspection 等）を考慮する必要がある。

4.1.3 フラグメントパケットのアクセス制御

要件15：フラグメントパケットを再構成し、外部からのアクセス制限の条件設定に基づき、アクセス制御可能であること。

必要度：オプション (MAY)

理由：フラグメントパケットにおいてもアクセス制御を行う必要があるため。ただし、フラグメントパケットの再構成や保持には、装置資源を消費するため、オプションとする。

備考：DNS の通信は UDP の 1 パケットで行われる場合が多く、今後は DNSSEC の普及等で応答サイズが増大し、パケットのサイズが大きくなることが見込まれる。パケットが経路 MTU サイズを超えた場合、元パケットはフラグメントとして分割送信される。この場合、フラグメント化不可能部分（Unfragmentable Part）については各フラグメントパケットに現れるが、フラグメント化可能部分（Fragmentable Part）については当該のフラグメントパケットにのみ存在する。このため、本機能を実装しない場合、アクセス制御対象の上位層プロトコルヘッダ等が、フラグメント化可能部分にのみ存在する場合は、フラグメントの先頭パケットでのみアクセス制御が可能で、他のフラグメントパケットについてはアクセス制御が不可能となる。

4.1.4 装置自身に対するアクセス制限

要件16：装置自身への通信に対するアクセス制御が可能であること。また、装置自身の管理機能へのアクセスについても同様にアクセス制御が可能であること。

必要度：必須（MUST）

理由：装置自身が IPv6 ホストとして提供するサービス機能について、セキュリティ確保が必要なため。

4.2 その他のセキュリティ機能

要件17：設定変更に対する警告等のセキュリティ機能を備えること。

- ルータ自身に対する内部外部からのセキュリティリスクを保護するために安全な初期設定を備え、脆弱な設定変更が行われる場合は警告を行うこと。
- ウイルス・改ざん等の対策機能を備えること。
- ログ・通知、障害復旧に対応するための機能等を有すること。
- ルータを経由する通信に対する安全な初期設定を備えること。
- セキュリティリスクを伴う変更に対する警告・通知を行えること。
- アドレス変換等の設定が行なえること。
- 無線 LAN を利用する場合は、強固な暗号機能を有すること。

必要度：オプション（MAY）

理由：セキュリティに詳しくないユーザに対して設定内容の安全性やそのリスクを示したりサポートしたりするため。ただし、ここで示す機能は幅が広く、最低限の機能として定義することが困難であることからオプションとする。

5 DNS プロキシ／リゾルバ機能

本節では、既存 IPv4 対応家庭用ルータの多くに具備されている DNS プロキシ機能及び、リゾルバ機能等その他の DNS 関連機能について述べる。[14]も参照のこと。

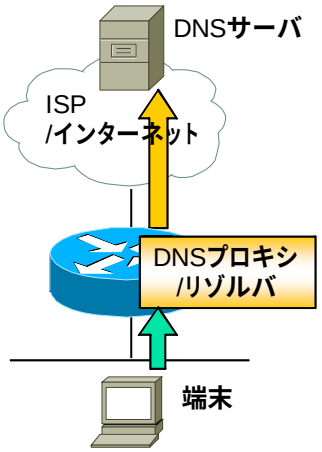

図 5-1　DNS プロキシ／リゾルバ機能の概念図

家庭用ルータでの DNS プロキシ／リゾルバ機能の要否は意見が分かれるところであるが、実装しキャッシュを使用した場合には DNS サーバの負荷を軽減させることができる。

また、実装しなかった場合には端末側における DNS サーバの誤選択により、遅延や通信不可等の問題が発生する可能性がある。さらに、家庭用ルータの Web-GUI へのアクセスに FQDN ではなく IP アドレスを直接入力する必要があり、IPv6 アドレスの直接入力は困難であるためユーザの利便性が低下する。

http://setup.example.jp/ → http://[2001:db8:1234:5678::1]/

本ガイドラインでは以下を前提条件として DNS プロキシ／リゾルバ機能を実装する場合の要件をまとめる。

- 端末からの問合せや DNS サーバからの応答に対して、フラグやデータを変更せず、可能な限り透過的に扱うこと。
- トランスレータや ALG（アプリケーションレベルゲートウェイ）等の変換処理が入る場合、この機能はトランスレータや ALG の機能領域となるため、今回は検討対象外とした。
  上記の変換処理が入る場合、端末が意図しない応答を得ることになるリスクがあるため、個別検討が必要である。
- DNS リゾルバ部分は IPv4 及び IPv6 に関わらず考慮すべき事項として記述している。

5.1　トランスポート

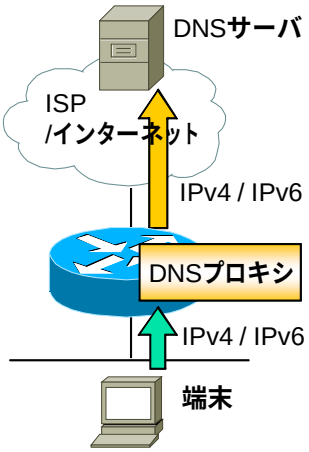

図 5-2　利用トランスポートの選択

5.1.1 利用可能なトランスポート

要件18：DNS サーバに問合せを行うトランスポートは、IPv6 トランスポートと IPv4 トランスポートの両方が利用可能であること。

必要度：必須（MUST）

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

5.1.2 トランスポート変換機能

要件19：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。

必要度：必須（MUST）

理由：IPv6 移行期においても DNS 通信ができる必要があるため。

5.1.3 優先するトランスポート

要件20：端末から問合せを行うトランスポートがサービス提供者から指定される DNS サーバのトランスポートと同じ場合には、端末から問合せを行うトランスポートと同じトランスポートでプロキシ動作を行うこと。

必要度：オプション（MAY）

理由：トランスポートを変更しないことで、要求端末にて期待する結果が得られる可能性が高くなるため[15]。ただし、家庭用ルータ（DNS プロキシ）から先の DNS サーバにてトランスポートが同一である保証がないためオプションとする。

備考：端末から DNS プロキシへの問合せが IPv6 トランスポートであるにもかかわらず、DNS サーバが IPv4 トランスポートのみの対応である場合には、DNS プロキシにはトランスポート変更機能が必要である。また、端末がトランスポートを意識した問合せをしていない限り DNS プロキシがトランスポートを合わせても意味がない。

同一トランスポートでのプロキシ動作を行う場合、DNS プロキシには端末から問合せを行ったトランスポートを記憶しておく機能が必要である。

IPv4 インターネットにおいては、始点アドレスによって DNS サーバからの応答が異なる運用があるので、トランスポートを合わせても必ずしも同じ回答を得られるわけではないが、トランスポートを合わせておくことがより適切な応答を得られる可能性がある。また、端末がトランスポートを意識した問合せを行っている場合もあり得るので、トランスポートを合わせておく方がより適切な応答を得られる可能性がある。

将来、トランスポートを合わせる必要が出てきた時には必要度を再検討する。

5.2　DNS プロキシとして待ち受けるアドレスの種類

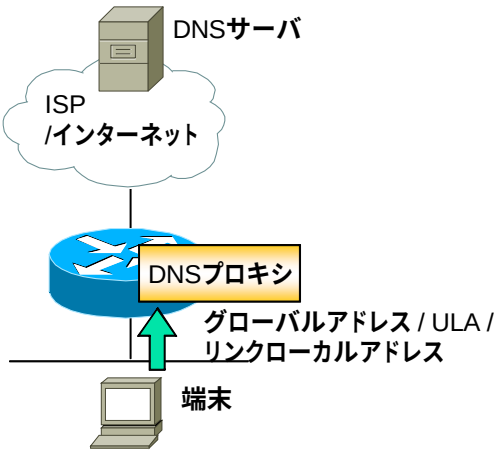

図 5-3　待ち受けるアドレスの種類

5.2.1 DNS プロキシとして待ち受けるアドレスの種類

要件21：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。

必要度：必須（MUST）

理由：最低限ユニキャストアドレスで待ち受けることができる必要があるため。

備考：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。尚、ULA が LAN 上で既に使用されていた場合は衝突しない別の ULA を生成する仕組みが必要である。

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。また、DNS の増幅攻撃の要因となる DNS オープンリゾルバとならないように、WAN 側からの問合せを受け付けない等の配慮が必要である。

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が存在する可能性があるため注意が必要である。

5.3　DNS サーバが複数存在する場合の選択方法

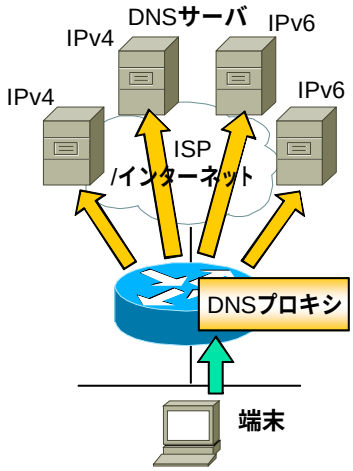

図 5-4　DNS サーバの選択

5.3.1 順次サーチによる選択

要件22：複数の DNS サーバを利用することができ、順次サーチにより DNS の選択を行うこと。

必要度：必須（MUST）

理由：通信先への到達可能性を高めるため。

5.3.2 任意選択機能

要件23：特定のポリシーに応じて DNS サーバを任意に選択するドメイン識別方式等の機能がある場合はその機能で設定されたルールに従うこと。

必要度：オプション（MAY）

理由：ユーザもしくはサービス提供者の意図を優先するため。ただし、本機能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。

備考：順次サーチ方式とドメイン識別方式のいずれも、マルチプレフィックス環境におけるサービスネットワークごとの DNS サーバ選択問題の解決策にもなり得るが、万能ではないため、その得失を考慮した上で実装すべきである[16][17]。

IPv6 トランスポートと IPv4 トランスポートの DNS サーバがそれぞれある場合の優先順位に関する規定はない。

現状では IPv6 の DNS サーバに不安があるので IPv4 にしたいという意見や、近い将来の IPv6 への移行を考慮するのであれば IPv6 にすべきという意見等見解の分かれるところであり、今後の検討課題である。

各種 OS のリゾルバでは IPv6 を優先しているものが多い。

DNS では、トランスポートに関わらず同じ応答が返って来る前提となっている。

5.4　キャッシュ

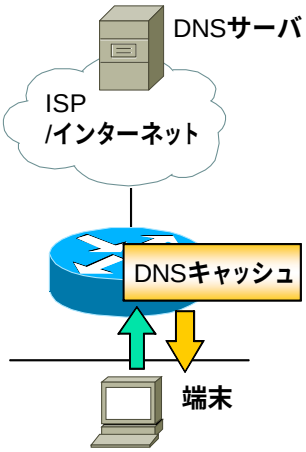

図 5-5　DNS キャッシュ機能

5.4.1 キャッシュ機能

要件24：端末からの問合せにより得られた応答をキャッシュしておき、以降同様の問合せがあった場合は、キャッシュ情報を応答すること。

必要度：オプション（MAY）

理由：サービス提供者の DNS サーバの負荷軽減（問合せ／応答パケットの抑制）が可能であるため。ただし、実装において考慮事項が多いためオプションとする。

備考：カミンスキーアタック[18]等DNS に関する脆弱性が見つかった場合は、迅速な対応が求められることからその得失を判断した上で実装する必要がある。
DNSSEC 対応のためにサイズの大きな RRSIG 等のキャッシュを行う必要がある点に注意すべきである。

5.5　リゾルバ機能

リゾルバで必要な以下の機能は必ずしも IPv6 特有のものではないが、IPv4 よりも IPv6 に密接に関係しているため、家庭用ルータへ実装するスペックとして考慮しておくことを推奨する。

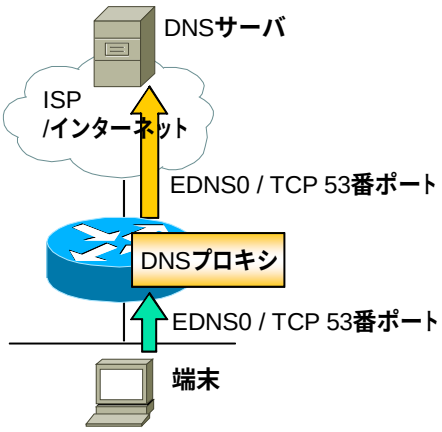

図 5-6　DNS リゾルバ機能

5.5.1 対応リソースレコード

要件25：端末からの問合せに対して、リソースレコード（RR）の種別に関わらず全て透過的に処理すること。

必要度：必須（MUST）

理由：RR 種別を限定すると、要求端末にて期待する応答が得られないため。

備考：但し、ULA の逆引き問合せを行わないこと（サービス提供者内にて ULA を使用する場合を除く）。

5.5.2予期しないフラグとデータ

要件26：解釈できないフラグやデータを受信しても変更や削除を行わないこと。

必要度：必須（MUST）

理由：端末と DNS サーバ間の透過性を保つため。

5.5.3 EDNS0

要件27：EDNS0[19]に対応した問合せ（OPT RR を含む）パケットを透過的に処理し、512byte を超える応答を端末に送信可能なこと。さらに、フラグメントされた応答パケットもそのまま転送もしくは再構成して転送すること。

必要度：必須（MUST）

理由：AAAA や PTR、SPF、SRV、TXT、DNSSEC 等の使用により、DNS 応答パケットが 512byte を超える状況が発生しているため。

5.5.4 TCP 53 番ポート対応

要件28：端末が（DNS Header TC=1 受信により[20][21]）TCP 接続にフォールバックして問合せを行った場合においても透過的に処理を行うこと（UDP 53 番ポートだけでなく、TCP 53 番ポートにおいても待ち受けること）。

必要度：必須（MUST）

理由：端末からの問合せに関する振る舞いに影響を与えないため。

5.5.5 DNSSEC

要件29：DNSSEC に対応したパケットを透過的に処理可能なこと[22][23][24]。

- EDNS0（OPT RR）DO bit がセットされている。
- RRSIG、DNSKEY、DS、NSEC、NSEC3、NSEC3PARAM の RR が使用される。
- DNS Header Bit に CD（checking disabled）や AD（authentic data）が使用される。

必要度：必須（MUST）

理由：端末からの問合せに関する振る舞いに影響を与えないため。

要件30：DNS プロキシ／リゾルバ機能として、署名検証を含む DNSSEC の再帰処理（バリデータ）を実装すること[22][23][24]。

必要度：オプション（MAY）

理由：端末からの問合せを適切に処理するため。ただし、IP アドレスの変換のみの単機能プロキシとしての実現も可能であるためオプションとする。

備考：現状、Windows XP や Windows Vista には実装されていないが、Windows 7 では DNSSEC に対応しているため検討する必要がある。

家庭用ルータの DNS プロキシ／リゾルバ機能として、署名検証を含む再帰処理（バリデータ）を実装するか、あるいは IP アドレスの変換のみの単機能プロキシとして動作するかは実装依存である。

6 宅内ネットワークへの情報配布機能

本章では、家庭用ルータが宅内端末に対して配布するアドレス／プレフィックス情報及びサーバ情報の配布方式について述べる。

6.1 アドレス／プレフィックス情報の配布

6.1.1 RA による配布

要件31：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。

必要度：必須（MUST）

理由：IPv6 ルータに必須の機能であるため[28]。

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。

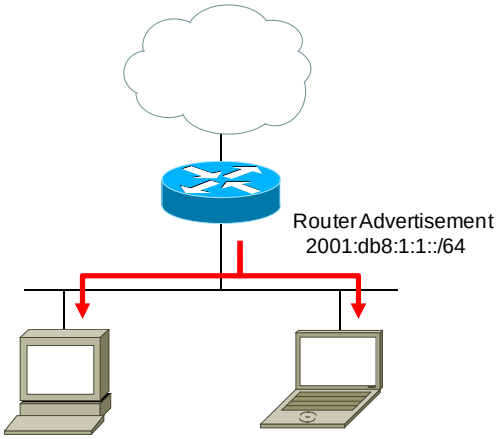

図 6-1 RA によるプレフィックス情報の配布

要件32：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。

必要度：必須（MUST）

理由：端末におけるステートレスアドレス自動設定では、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。

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。例えば、Windows Vista SP1 では/64 以外のプレフィックスからアドレス生成できない。

SLAAC（RFC 4862）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（MUST）となっている[29][48]。

要件33：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。

必要度：推奨（SHOULD）

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。

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[15]。

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（3.3.4 節を参照）。

要件34：Router Lifetime を 0 とした RA を広告する機能を持つこと。

必要度：推奨（SHOULD）

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。

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

本機能を動作させるタイミングとして、例えば WAN 側リンクの切断を検出した時が考えられる。この場合、Router Lifetime = 0 の RA を広告することで、それを受信した端末は、その RA の送信元ルータをデフォルトルートとして選択しなくなるため、端末からそのルータに、自 LAN セグメント外へのパケット(インターネット向けのパケット)が送信されなくなる。

ルータに複数の LAN セグメントが接続されている場合には注意が必要である。この場合 Router Lifetime = 0 の RA のみ広告すると、一方の LAN セグメントから他方の LAN セグメントへの通信もできなくなるため、More-Specific Routes[35]による経路配布等の対策が必要となる。

6.1.2 DHCPv6 による配布

要件35：宅内の端末にアドレスを DHCPv6[27]で通知する機能を持つこと。

必要度：オプション（MAY）

理由：宅内ネットワークの端末に特定の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 によるアドレス設定が一般的であるためオプションとする。

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。

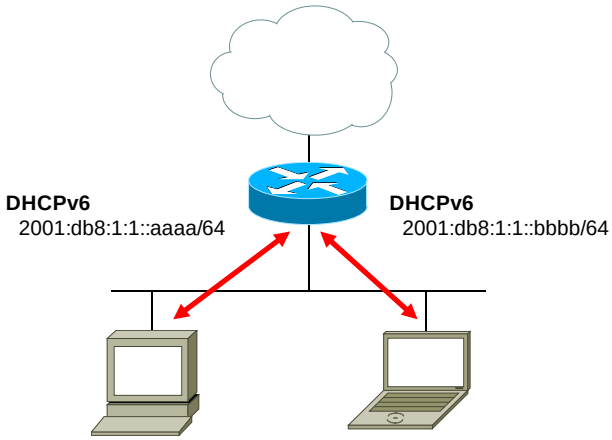

図 6-2　DHCPv6 によるアドレス情報の配布

要件36：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。
前提：要件 35 を実装している場合。
必要度：推奨（SHOULD）
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。
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37：DHCPv6-PD[30]により宅内機器（ルータ）にプレフィックスを配布する機能を持つこと。機器ごとに配布するプレフィックスを指定できる機能を持つこと。
必要度：オプション（MAY）
理由：宅内に複数のルータが存在する場合、当該ルータ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を設置するユーザはあまり多くないと考えられるためオプションとする。

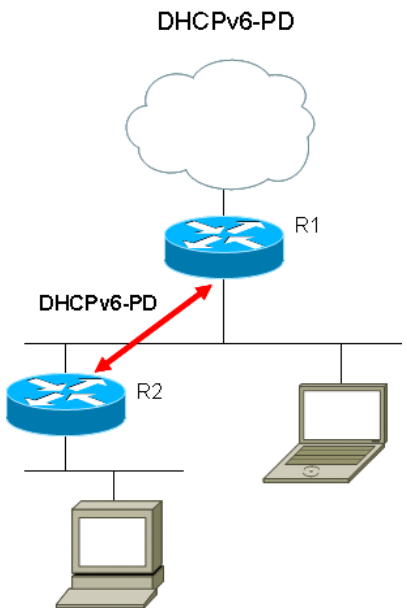

図 6-3　DHCPv6-PD によるプレフィックス情報の配布

6.2　サーバ情報の配布

6.2.1 RA による配布

要件38：LAN セグメントに対して、RA にて DNS サーバアドレスを配布する機能を持つこと。

必要度：オプション（MAY）

理由：端末において、RA から DNS サーバ情報を取得する実装が想定されるため（RA による DNS 配布の Standard Track 化による[31]）。ただし、現状、Windows XP/Vista/7 や Mac OS には標準で実装されていないためオプションとする。

備考：サービス提供者の切り替え等により DNS サーバアドレスが変更となった場合は、端末が保持する DNS サーバリストから旧 DNS サーバアドレスを削除させるため、旧 DNS サーバアドレスについて RDNSS オプション中の Lifetime を 0 とした RA を広告することが望ましい。

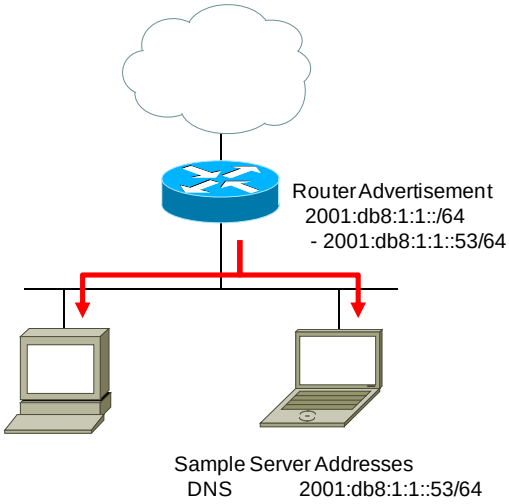

図 6-4　RA によるサーバ情報の配布

6.2.2 DHCPv6 による配布

要件39：LAN セグメントに対して、DHCPv6 にて DNS サーバアドレスを配布する機能を持つこと。

必要度：必須（MUST）

理由：端末側の実装として、DHCPv6 により DNS サーバ情報を取得する方法が一般的であるため。

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

標準化としては、DHCPv6 が Standard Track（RFC 3646）であるのに対し、RA

の方は Experimental（RFC 5006）である[32]が、現在 IETF にて RFC5006 を Standard Track とする方向で検討されている。

要件40：LAN セグメントに対して、DHCPv6 にてその他のサーバアドレス(SIP、NTP 等）を配布する機能を持つこと。

必要度：オプション（MAY）

理由：ユーザ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。

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

どのサーバ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アドレス：

SIP サーバ[49]、DNS サーバ[50]、NIS サーバ[51]、SNTP サーバ[52]等

DHCPv6 のパラメータ一覧：

http://www.iana.org/assignments/dhcpv6-parameters/

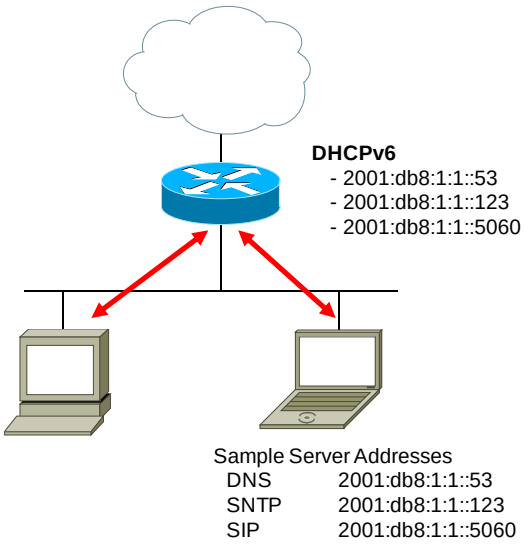

図 6-5　DHCPv6 によるサーバ情報の配布

要件41：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。

前提：要件 40 を実装している場合。

必要度：推奨（SHOULD）

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 によるサーバ情報の再取得を促すため。ただし、サーバ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。

6.3 その他の情報の配布

6.3.1 MTU 情報の配布

要件42：LAN セグメントに対して、RA でアクセス回線の MTU 値を広告する機能を持つこと。また広告するアクセス回線の MTU の値を設定可能とすること。

必要度：推奨（SHOULD）

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。

備考：ICMPv6 Packet Too Big メッセージがフィルタリングされる等により、端末がパス MTU 探索での最適な MTU を発見できず、その結果通信断が発生する場合がある（7.4 節参照）。この場合、端末のインターフェースの MTU を小さくすると通信が回復する。

端末のインターフェース MTU を手動で変更する方法もあるが、LAN に複数の端末が接続している場合は設定に手間がかかる。ルータが LAN セグメントにリンク MTU を広告すれば、LAN に接続する全ての端末にその MTU が反映されるため、端末での設定の手間を省くことができる。

7 ルーティング／マルチキャスト機能

本章では家庭用ルータに IPv6 をサービスに接続するために最低限必要なルーティング機能/マルチキャスト機能に関して記述する。

7.1 使用していないアドレス／ネットワークへの通信

要件43：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。

必要度：必須（MUST）

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

備考：利用されていないアドレス空間宛てのパケットをデフォルトルートにフォワードせずに処理する必要がある。

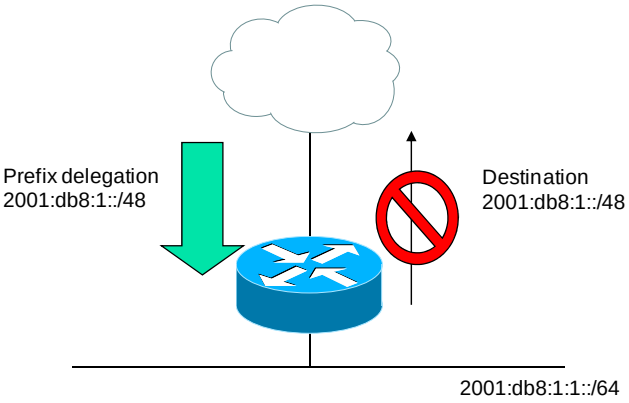

図 7-1 DHCPv6-PD によるアドレス割り当てを行うサービス

要件44：Point-to-Point リンクのルータにて、自インターフェース以外の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[33]。

必要度：必須（MUST）

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

備考：RFC2463 では未定義であったが、RFC4443 で仕様として定義された。

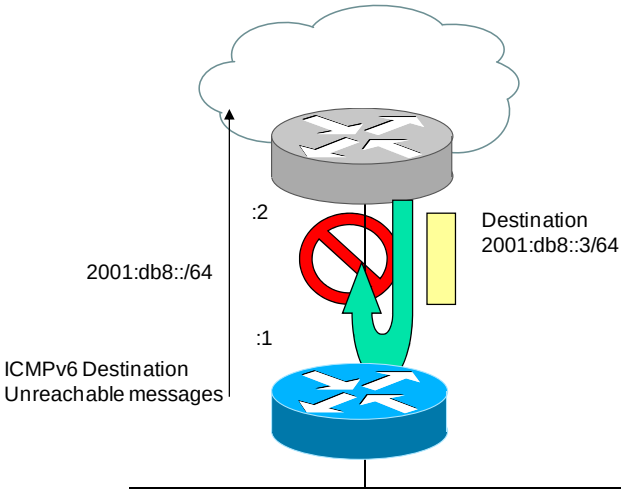

図 7-2　WAN 側を Point-to-point リンクとして接続するサービス

7.2　経路情報・拡張ヘッダ

7.2.1 WAN 側における経路制御

要件45：WAN 向けのスタティックルートが設定できること。

必要度：必須（MUST）

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

備考：ネクストホップアドレスにリンクローカルアドレスを指定できないと ICMPv6 のリダイレクト機能が有効に働かなくなるため、リンクローカルアドレスも指定できる必要がある。

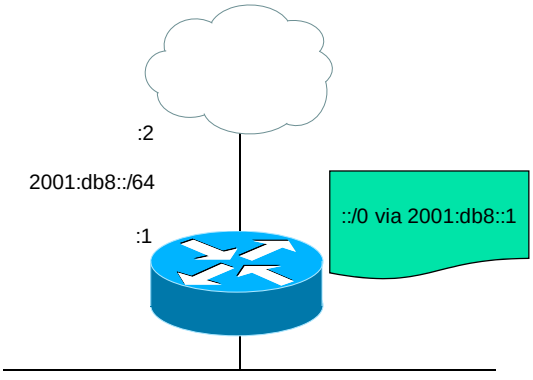

図 7-3　WAN 向けのスタティック経路設定

要件46：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）
理由：RA による IPv6 アドレス設定を行うサービスへの考慮が必要であるため。
備考：ルータは一般的に RA による経路の自動設定をサポートしないが、家庭用ルータにおいては、ユーザの手を介さないサービス提供者への設定を実施することが重要である[48]。なお、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ため注意が必要である。今後検討が必要な項目としている（10.2 節参照）。

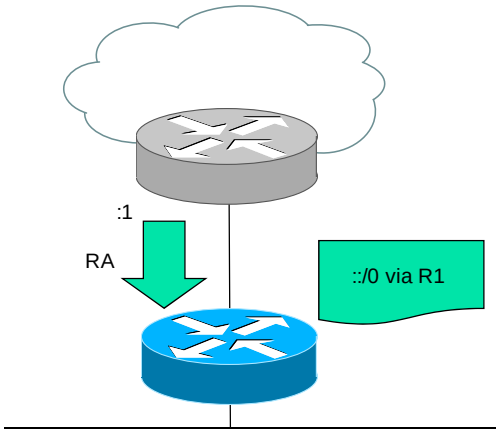

図 7-4　RA を利用したデフォルトルートの自動設定

7.2.2 LAN 側への経路制御

要件47：RIPng[34]により LAN 側に経路配布ができること。
必要度：オプション（MAY）
理由：ルータの LAN 側に接続されたネットワークへの経路制御に対する使用が想定されるため。ただし、宅内に複数のルータを設置するユーザはあまり多くないと考えられるためオプションとする。

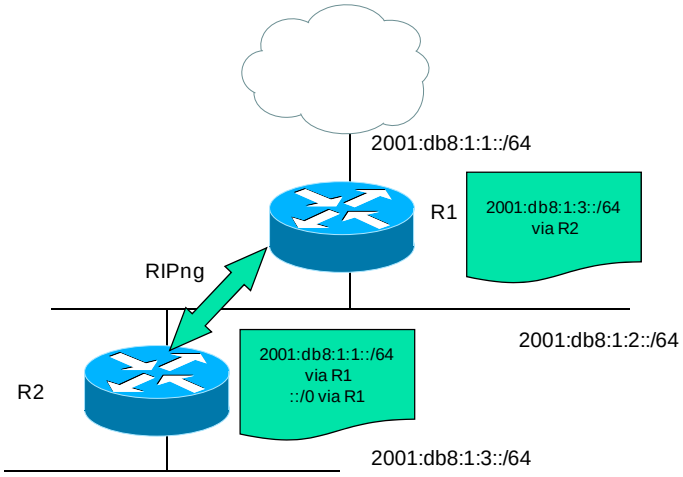

図 7-5　RIPng による経路制御

要件48：More-Specific Routes[35]により LAN 側に経路を配布できること。

必要度：オプション（MAY）

理由：ルータの LAN 側に接続されたネットワークへの経路制御に対する使用が想定されるため。ただし、本機能はサービス提供者のサービスに依存するためオプションとする。

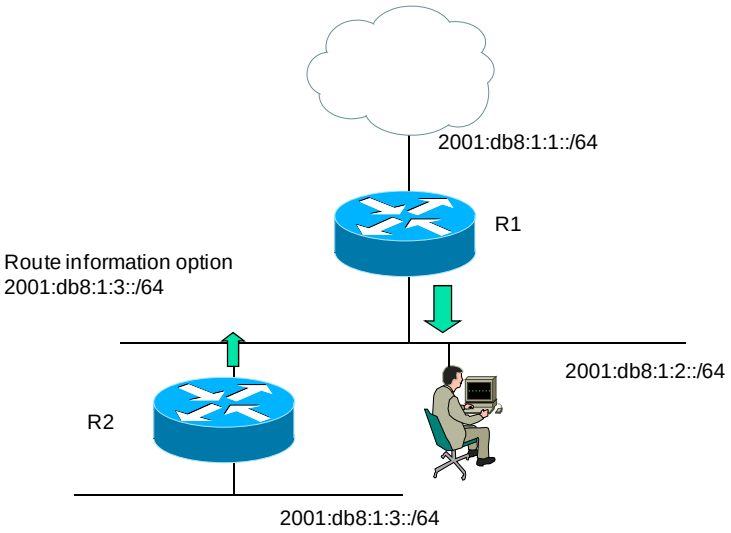

図 7-6　More-Specific Route の利用

7.2.3 拡張ヘッダ

要件49：RH0（Type 0 ルーティングヘッダ）のパケット転送を禁止できること。
必要度：必須（MUST）
理由：IPv6 ソースルーティングによる DoS 攻撃への考慮[11]が必要であり、現仕様において利用が禁止されているため。
備考：ルーティングヘッダ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 のみ禁止できる必要がある。

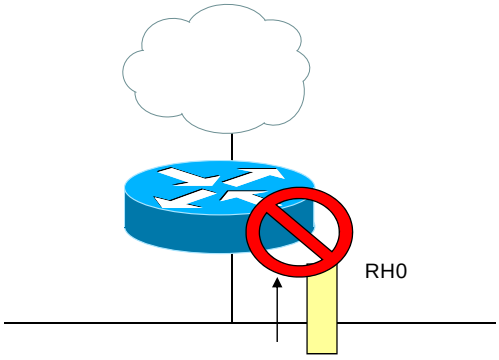

図 7-7　RH0 のパケット転送禁止

7.3　IPv6 マルチキャスト

IPv6 では NDP 等のコントロールパケットで多くのマルチキャストメッセージを利用する。IPv6 機器でのマルチキャストサポートは必須機能である。本章で記載のマルチキャストとはマルチキャストルーティング機能に関する記載である。

要件50：マルチキャストルーティング機能
必要度：オプション（MAY）
理由：マルチキャストによるサービスに対応するため。ただし、本機能はサービス提供者によるサービスに大きく依存する機能であるため、機能全体をオプションとする。

7.3.1 IPv6 マルチキャスト接続形態ごとの機能

IPv6 マルチキャストサービスへの接続では、家庭用ルータから上位（WAN 側）で使用するプロトコルにより 2 つの接続パターンが考えられる。それぞれの接続形態ごとに必要となる機能を以下に示す。

7.3.2 PIM による接続

PIM を使用してサービス提供者へマルチキャストグループへの参加／離脱を通知する。

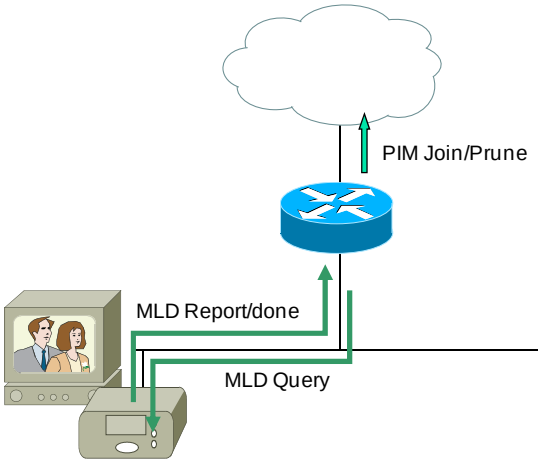

図 7-8　PIM を用いたマルチキャスト接続

要件51：PIM[36][37][38]によるマルチキャストルーティング機能を持つこと。
前提：要件 50 を実装している場合。
必要度：オプション（MAY）
理由：WAN 側のプロトコルとして PIM を使用するサービスへ対応するため。ただし、本機能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。
備考：PIM-SM/SSM の仕様には多くのオプション機能が存在しており、接続性を確保するために必要となるオプションについてはサービス提供者側のサービス仕様に大きく依存する。また、家庭用ルータでサポートが必要となるシンプルなツリー構造においては MLD プロキシでの実装の方が、複雑な PIM プロトコルよりも実装コストが低くなり、より簡易な導入が可能となると考えられる。

要件52：MLD（v1/v2）ルータ機能[39][40][41]を有すること。
前提：要件 50 を実装している場合。
必要度：オプション（MAY）
理由：PIM 接続の際に、端末がマルチキャストネットワークへ参加するためにはルータでの MLD ルータ機能のサポートが必要であるため。ただし、接続性を確保するために必要となるオプションについては、サービス提供者側のサービスに大きく依存するためオプションとする。
備考：PIM-SM/SSM の仕様には多くのオプション機能が存在している。また、家庭用ルータでサポートが必要となるシンプルなツリー構造においては MLD プロキシでの実装の方が、複雑な PIM プロトコルよりも実装コストが低くなり、より簡易な導入が可能となると考えられる。

7.3.3 MLD プロキシによる接続

MLD を使用してサービス提供者へマルチキャストグループへの参加／離脱を通知する。

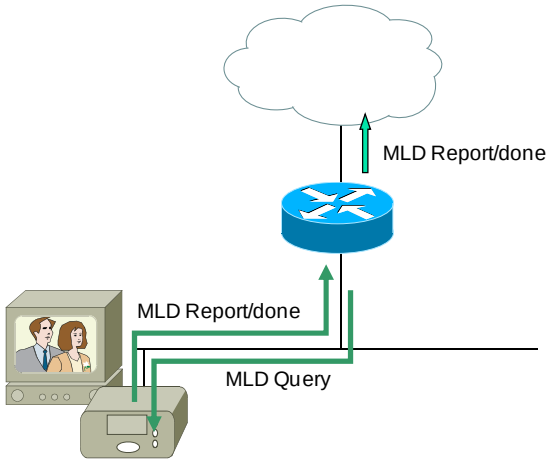

図 7-9　MLD プロキシを用いたマルチキャスト接続

要件53：MLD（v1/v2）プロキシ[42]機能を有すること。
前提：要件 50 を実装している場合。
必要度：必須（MUST）
理由：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。

7.3.4 MLD スヌーピング

7.3.1 節のいずれの接続形式においても、家庭用ルータがスイッチ機能を有する場合には下記の MLD スヌーピング[43]機能も実装する事が望ましい。

要件54：MLD（v1/v2）スヌーピング[43]機能を有すること。
前提：要件 50 を実装している場合。
必要度：オプション（MAY）
理由：不要なマルチキャストトラフィックを制限する必要があるため。ただし、ルータがスイッチング機能を持つ際にのみ使用が想定されるためオプションとする。
備考：家庭用ルータが無線 LAN 機能を有する場合、本機能を持つことが望ましい。

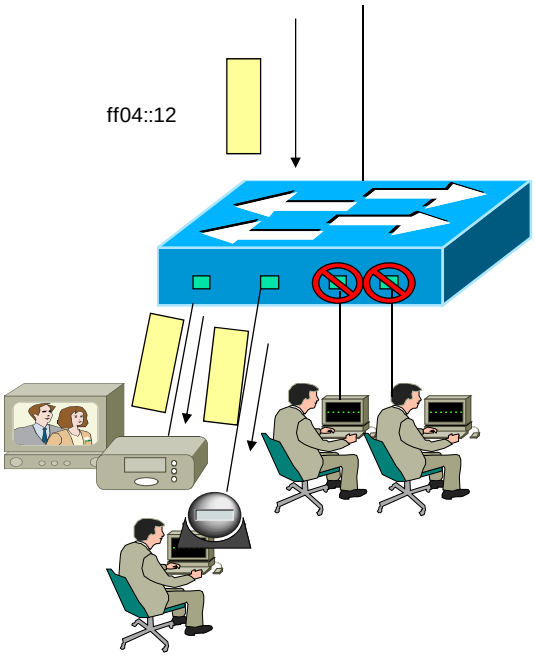

図 7-10　MLD スヌーピング機能

7.4 特殊なフォワーディング

要件55：家庭用ルータを通過する 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

必要度：オプション（MAY）

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。ただし、本機能は、6.3.1 節に規定される MTU 情報の配布機能によって代替可能であるためオプションとする。

備考：宅内の機器が送信する TCP SYN パケットに含まれる MSS オプションの MSS 値は、宅内ネットワークの MTU 値から決定される。したがってアクセス回線の MTU 値が宅内ネットワークの MTU 値より小さい場合、TCP の接続先ホストから宅内の機器に対して送信される TCP セグメントのサイズがアクセス回線の MTU 値より大きくなり、パス MTU 探索が発生する。

頻繁にパス MTU 探索を実行することによりアクセス網内のルータに負荷を与え、その結果としてパス MTU 探索に支障が生じる状況を避けるためにも、本機能の実装が望ましい。

適切な MSS 値はアクセス回線の MTU/MRU 値から算出可能である。

8 サービス側の設定機能

本章では、家庭用ルータに対する設定方式及び設定項目について述べる。なお、設定主体はサービス提供者である。

8.1 設定方式

要件56：サービス提供者から家庭用ルータに対して必要な設定の投入を行なうための機能を、家庭用ルータが具備すること（サービス提供者により提供される家庭用ルータが対象）。

必要度：推奨（SHOULD）

理由：宅内機器がサービス提供者によるサービスを利用する上で必要となる情報を、家庭用ルータが何らかの手段により取得する必要があるため。ただし、どの方式を使用するかはサービス提供者のサービスに依存しており、設定済みの家庭用ルータを配布する場合も想定されることから推奨とする。

備考：サービス提供者以外からの設定投入を禁止し、サービス提供者の使用する方式以外の方式は無効としておくことが必要である。（4.1.4 節参照）
具体的な設定方式については、以下に例示列挙する。

8.1.1 自動設定

本節では、サービス提供者から直接家庭用ルータを操作することなく、家庭用ルータが自律的に必要な設定情報を取得するための方式として、以下に例示列挙する。

- SLAAC 機能を有すること。

  DHCPv6 サーバを用いず RA によって IPv6 アドレスを設定する方法。

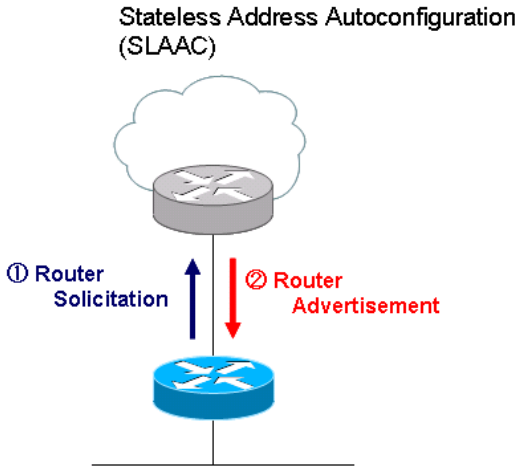

図 8-1　SLAAC による自動設定

- DHCPv6 クライアント機能を有すること。
  DHCPv6 のクライアント機能とは IPv6 アドレス等の情報を DHCPv6 サーバに対して要求し、取得した情報をホスト自身に設定する機能を指す。

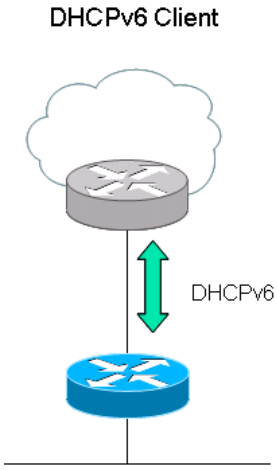

図 8-2　DHCPv6 によるアドレス設定

- TR-069 による設定ができること。
  Broadband Forum により定義された CPE 機器を遠隔管理するためのプロトコル：TR-069 を用いて設定する方法。

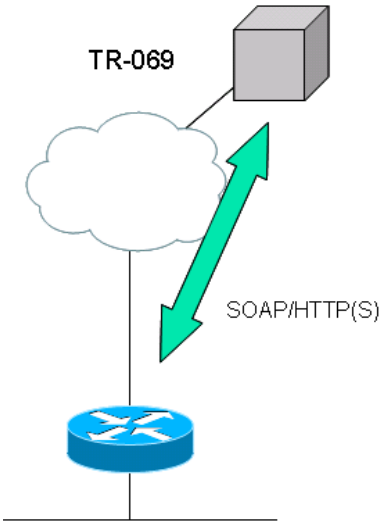

図 8-3　TR-069 によるアドレス設定

- UPnP による設定ができること。
  UPnP Forum により定義された自動機器登録の仕組み：UPnP によりアドレスを設定する方法。

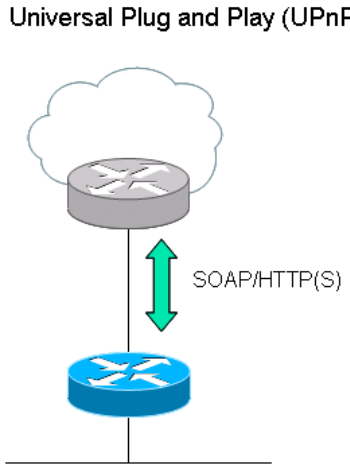

図 8-4　UPnP によるアドレス設定

8.1.2 手動設定

サービス提供者は家庭用ルータに対して手動で直接設定する場合も想定されるため、そのためのインターフェースを具備しておく必要がある。具体的には Web インターフェースや Telnet、SSH 等が該当する。

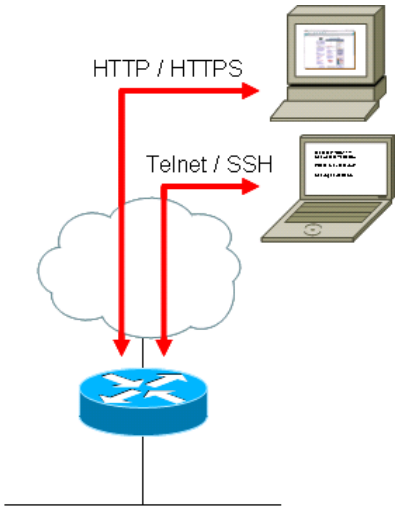

図 8-5　手動設定の概念図

8.2 設定項目

本節では、8.1 節にて述べた設定方式により家庭用ルータに設定される具体的な項目について述べる。

8.2.1 アドレス設定

3 章を参照のこと。

8.2.2 セキュリティ関連設定

8.2.2.1 外部からのアクセス制限機能

要件57：装置のアクセス制限機能を設定可能であること。
必要度：推奨（SHOULD）
理由：セキュリティ設定に不慣れなユーザでもサービスを受ける際に必要なセキュリティレベルを維持できるようなサービス提供を可能にするため。ただし、本機能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。
備考：利用しない場合等ユーザの設定で機能を無効にできる必要がある。

要件58：WAN インターフェース側にあるサービス提供者の管理セグメントから、家庭用ルータの管理用インターフェースへアクセスする手段を持つこと。
必要度：オプション（MAY）
理由：グローバルアドレスが付与されて監視する場合に、外部からの不正なアクセスから防御するため。ただし、本機能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。

8.2.2.2 ファームウェアのアップデート機能

要件59：ファームウェアのアップデートが可能であること。
必要度：推奨（SHOULD）
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。ただし、本機能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。
備考：基本的にはサービス提供者により使用されるが、家庭用ルータの利用者自身により使用されることもある。

8.2.3 DNS 設定

本節では、家庭用ルータにて DNS プロキシ機能を使用する場合の、家庭用ルータへの DNS サーバアドレスの設定方式について述べる。その他の項目については 5 章参照のこと。

8.2.3.1 DNS プロキシ機能のための DNS サーバアドレス

要件60：DHCPv6 等の手段にて取得した DNS サーバ情報を使用できること。
必要度：必須（MUST）
理由：自動化により設定ミスをなくすため。

要件61：DNS サーバ情報を手動設定できること。
必要度：必須（MUST）
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。

8.2.4 宅内ネットワーク設定

本節では、家庭用ルータが宅内機器に対する設定を行なうにあたり必要となる情報の設定手法について述べる。

8.2.4.1 LAN 側へ配布するプレフィックス

3 章を参照のこと。

8.2.4.2 LAN 側へ配布する各種サーバアドレス

要件62：各種サーバ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。
必要度：必須（MUST）
理由：ルータへ配布される各種サーバ情報は、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。

要件63：各種サーバアドレスを手動設定できること。
必要度：必須（MUST）
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。

8.2.5 ルーティング・マルチキャスト設定

7 章を参照のこと。

9 ユーザインターフェース機能

本章では、家庭用ルータの利用者に対して提供されるユーザインターフェースに関して述べる。ユーザインターフェースに用いるプロトコルの IPv6 対応に関しては、IPv4 にてその機能が提供されている場合に対する必要度として記載する。

9.1 Web-GUI（Graphical User Interface）

要件64：ユーザからの設定を受け付けるために表 9-1 で示すプロトコルによる Web-GUI を IPv6 対応すること。

必要度：推奨（SHOULD）

表 9-1 Web-GUI で用いるプロトコル

プロトコル	必要度
HTTP（80/tcp）	推奨（SHOULD）
HTTPS（443/tcp）	オプション（MAY）

理由：IPv6 トランスポートに対応することで、ユーザ設定の利便性を高めることができるため。ただし、IPv4 トランスポートの実装でも最低限の機能提供が可能であるため推奨とする。

備考：家庭用ルータの設定は、PC 等の Web ブラウザから家庭用ルータの Web-GUI にアクセスして設定することが一般的である。
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。

9.2 CLI（Command Line Interface）

要件65：ユーザからの設定を受け付けるために表 9-2 で示すプロトコルによる CLI を IPv6 対応すること。

必要度：オプション（MAY）

表 9-2 CLI で用いるプロトコル

プロトコル	必要度
TELNET（23/tcp）	オプション（MAY）
SSH（22/tcp）	オプション（MAY）

理由：IPv6 トランスポートに対応することでユーザ設定の利便性を高めることができるため。ただし、IPv4 トランスポートによる実装も必須機能でもないためオプションとする。

備考：セキュリティの観点からは ssh を使用することが望ましい。

9.3 IPv6 アドレス／プレフィックスの入力

要件66：ユーザに 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。

必要度：推奨（SHOULD）

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設定の利便性を高めることができるため。ただし、本機能は実装されていなくても IPv6 通信には影響しないため推奨とする。

9.4 IPv6 アドレス／プレフィックスの表記

要件67：IPv6 アドレス／プレフィックスの出力表記は、IETF による推奨表記[63] を用いること。

必要度：推奨（SHOULD）

理由：IPv6 アドレス表記は様々な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みえてしまう等、誤認する可能性があるため。ただし、本機能は実装されていなくても IPv6 通信には影響しないため推奨とする。

備考：ユーザが目にする部分の表記（Web-GUI、ログ等）を推奨表記とすることで統一的な表記となるため、ユーザサポート等において誤認の問題を避けることが可能となる。

推奨表記に関する提案は、2010 年 6 月 1 日現在 RFC Editor Queue のステータスとなっており、Standards Track カテゴリの RFC として発行される予定である。

10 おわりに

10.1 IPv6 家庭用ルータが必要とする機能のまとめ

前章までにまとめた「IPv6 家庭用ルータにおける最小限の共通機能」を表 10-1 にまとめる。本ガイドラインは、IPv6 家庭用ルータに対する機能をすべて網羅していないが、ここに挙げた機能に関して最低限考慮した実装が IPv6 の家庭用ルータに求められる。

表 10-1　IPv6 家庭用ルータに必要とされる機能一覧

要件 前提	内容	必要度	節	1.0 版からの差分
要件 1：	宅内用プレフィックス情報を接続先サービス提供者から DHCPv6-PD にて取得できること。	必須	3.1.1	―
要件 2：	宅内用プレフィックス情報を手動設定できること。	必須	3.1.1	―
要件 3：	/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	3.1.2	―
要件 4：	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こと。	必須	3.2.1	―
要件 5：	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	3.2.2	―
要件 6：	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	3.2.3	新規
要件 7：	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	3.3.1	―
要件 8：	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	3.3.2	―
要件 9：	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	3.3.4	推奨から必須へ

要件 10：	サービス提供者からプレフィックス情報を取得していない場合、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	3.3.4	新規
要件 11：	内部（LAN 側）から外部（WAN 側）への通信は通過させ、外部から内部への通信は遮断するアクセス制限が行えること。	必須	4.1.1.1	―
要件 12：	静的フィルタによりアクセスを制限できること。	必須	4.1.1.2	―
要件 13：	動的フィルタ（SPI）によりアクセスを制限できること。	推奨	4.1.1.3	―
要件 14：	表 4-1 で示した機能についてアクセス制御を設定できること。	必須	4.1.2	表 4-1 内の文言変更
要件 15：	フラグメントパケットを再構成し、外部からのアクセス制限の条件設定に基づき、アクセス制御可能であること。	オプション	4.1.3	新規
要件 16：	装置自身への通信に対するアクセス制御が可能であること。また、装置自身の管理機能へのアクセスについても同様にアクセス制御が可能であること。	必須	4.1.4	―
要件 17：	設定変更に対する警告等のセキュリティ機能を備えること。	オプション	4.2	新規
要件 18：	DNS サーバに問合せを行うトランスポートは、IPv6 トランスポートと IPv4 トランスポートの両方が利用可能であること。	必須	5.1.1	―
要件 19：	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	5.1.2	新規
要件 20：	端末から問合せを行うトランスポートがサービス提供者から指定される DNS サーバのトランスポートと同じ場合には、端末から問合せを行うトランスポートと同じトランスポートでプロキシ動作を行うこと。	オプション	5.1.3	要件の文言修正
要件 21：	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	5.2.1	―
要件 22：	複数の DNS サーバを利用することができ、順次サーチにより DNS の選択を行うこと。	必須	5.3.1	要件の文言修正

要件 23：	特定のポリシーに応じて DNS サーバを任意に選択するドメイン識別方式等の機能がある場合はその機能で設定されたルールに従うこと。	オプション	5.3.2	―
要件 24：	端末からの問合せにより得られた応答をキャッシュしておき、以降同様の問合せがあった場合は、キャッシュ情報を応答すること。	オプション	5.4.1	―
要件 25：	端末からの問合せに対して、リソースレコード（RR）の種別に関わらず全て透過的に処理すること。	必須	5.5.1	―
要件 26：	解釈できないフラグやデータを受信しても変更や削除を行わないこと。	必須	5.5.2	新規
要件 27：	EDNS0[19]に対応した問合せ（OPT RR を含む）パケットを透過的に処理し、512byte を超える応答を端末に送信可能なこと。さらに、フラグメントされた応答パケットもそのまま転送もしくは再構成して転送すること。	必須	5.5.3	―
要件 28：	端末が（DNS Header TC=1 受信により[20][21]）TCP 接続にフォールバックして問合せを行った場合においても透過的に処理を行うこと（UDP 53 番ポートだけでなく、TCP 53 番ポートにおいても待ち受けること）。	必須	5.5.4	―
要件 29：	DNSSEC に対応したパケットを透過的に処理可能なこと[22][23][24]。	オプション	5.5.5	要件を分離
要件 30：	DNS プロキシ／リゾルバ機能として、署名検証を含む DNSSEC の再帰処理（バリデータ）を実装すること[22][23][24]。	オプション	5.5.5	要件を分離
要件 31：	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	6.1.1	―
要件 32： 前提 31	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	6.1.1	―
要件 33： 前提 31	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	6.1.1	新規
要件 34： 前提 31	Router Lifetime を 0 とした RA を広告する機能を持つこと。	推奨	6.1.1	新規
要件 35：	宅内の端末にアドレスを DHCPv6[27]で通知する機能を持つこと。	オプション	6.1.2	―

要件 36： 前提 35	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	6.1.2	新規
要件 37：	DHCPv6-PD[30]により宅内機器（ルータ）にプレフィックスを配布する機能を持つこと。機器ごとに配布するプレフィックスを指定できる機能を持つこと。	オプション	6.1.2	新規
要件 38：	LAN セグメントに対して、RA にて DNS サーバアドレスを配布する機能を持つこと。	オプション	6.2.1	―
要件 39：	LAN セグメントに対して、DHCPv6 にて DNS サーバアドレスを配布する機能を持つこと。	必須	6.2.2	―
要件 40：	LAN セグメントに対して、DHCPv6 にてその他のサーバアドレス（SIP、NTP 等）を配布する機能を持つこと。	オプション	6.2.2	―
要件 41：	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	6.2.2	新規
要件 42：	LAN セグメントに対して、RA でアクセス回線の MTU 値を広告する機能を持つこと。また広告するアクセス回線の MTU の値を設定可能とすること。	推奨	6.3.1	新規
要件 43：	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	7.1	―
要件 44：	Point-to-Point リンクのルータにて、自インターフェース以外の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[33]。	必須	7.1	―
要件 45：	WAN 向けのスタティックルートが設定できること。	必須	7.2.1	―
要件 46：	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	7.2.1	―
要件 47：	RIPng[34]により LAN 側に経路配布ができること。	オプション	7.2.2	―
要件 48：	More-Specific Routes[35]により LAN 側に経路を配布できること。	オプション	7.2.2	―
要件 49：	RH0（Type 0 ルーティングヘッダ）のパケット転送を禁止できること。	必須	7.2.3	―
要件 50：	マルチキャストルーティング機能	オプション	7.3	前提条件の整理

要件 51： 前提 50	PIM[36][37][38]によるマルチキャストルーティング機能を持つこと。	オプション	7.3.2	―
要件 52： 前提 50	MLD（v1/v2）ルータ機能[39][40][41]を有すること。	オプション	7.3.2	必須からオプションへ
要件 53： 前提 50	MLD（v1/v2）プロキシ[42]機能を有すること。	必須	7.3.3	―
要件 54： 前提 50	MLD（v1/v2）スヌーピング[43]機能を有すること。	オプション	7.3.4	―
要件 55：	家庭用ルータを通過する 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	7.4	新規
要件 56：	サービス提供者から家庭用ルータに対して必要な設定の投入を行なうための機能を、家庭用ルータが具備すること（サービス提供者により提供される家庭用ルータが対象）。	推奨	8.1	―
要件 57：	装置のアクセス制限機能を設定可能であること。	推奨	8.2.2.1	―
要件 58：	WAN インターフェース側にあるサービス提供者の管理セグメントから、家庭用ルータの管理用インターフェースへアクセスする手段を持つこと。	オプション	8.2.2.1	―
要件 59：	ファームウェアのアップデートが可能であること。	推奨	8.2.2.2	新規
要件 60：	DHCPv6 等の手段にて取得した DNS サーバ情報を使用できること。	必須	8.2.3.1	―
要件 61：	DNS サーバ情報を手動設定できること。	必須	8.2.3.1	―
要件 62：	各種サーバ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	8.2.4.2	―
要件 63：	各種サーバアドレスを手動設定できること。	必須	8.2.4.2	―
要件 64：	ユーザからの設定を受け付けるために表 9-1 で示すプロトコルによる Web-GUI を IPv6 対応すること。	推奨	9.1	新規
要件 65：	ユーザからの設定を受け付けるために表 9-2 で示すプロトコルによる CLI を IPv6 対応すること。	オプション	9.2	新規
要件 66：	ユーザに 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	9.3	新規
要件 67：	IPv6 アドレス／プレフィックスの出力表記は、IETF	推奨	9.4	新規

	による推奨表記[63] を用いること。			
—	ユーザに配布するプレフィックスを固定とすること。	—	—	削除
—	ユーザに配布するプレフィックスが時間の経過により変更すること。	—	—	削除
—	家庭用ルータの WAN 側にもグローバルアドレスを付与できること。付与するアドレスは、ユーザに割り当てたアドレス空間からではなく、サービス提供者が保有する別空間からとする。	—	—	削除
—	DHCPv6 リレー機能を持つこと。	—	—	削除

10.2 次版に向けた検討項目

本ガイドラインでは、家庭用ルータにおける全ての機能を網羅して機能定義をできておらず、今後引き続き検討を重ねる必要がある。以下に今後検討が必要と考えている項目をまとめる。

10.2.1 未検討項目

- 拡張ヘッダチェーンの対応ヘッダ数
- TCP,UDP 以外のトランスポートプロトコルへの対応
- フィルタリングの推奨値
  - 利用可能アプリケーション一覧等
- DNS サービス時の課題
  - ソースポートランダマイゼーション，DNSSEC 対応等
- プロバイダ接続機能（プロバイダごとのサービス対応）
  - Point-to-Multipoint 接続，ISP サービスの自動判別機能等
- マルチプレフィックス対応（複数の ISP 接続）
  - マルチセッション，デフォルトルートの扱い，66NAT 等
- サブネット・ルーター・エニーキャストの扱い
- IPv4/IPv6 相互変換機能
- ローカル名前解決／ノードディスカバリ／サービスディスカバリ機能
  - mDNS（zeroconf），LLMNR，UPnP 等
- その他の未検討ルータ機能（参考）

  QoS 機能, ダイナミック DNS 登録, 静的 NAT, ブリッジ機能, 機器のアクセス制御（MAC アドレス認証等），ホームゲートウェイの個体認証（個体識別），802.1x 認証，無線機能（802.11，Bluetooth），セットアップに関する機能（初期設定機能，Web での設定），各種メディア対応（無線，イーサ，USB,IEEE1394，電話，ISDN）等

10.3 検討メンバー

下記に検討メンバーを示す。会務担当者以外のメンバーは、所属の 50 音順に従っている。

氏名	所属
荒野 高志（WG 主査）	IT ホールディングス株式会社
北口 善明（chair）	国立大学法人金沢大学
藤崎 智宏（co-chair）	日本電信電話株式会社
中川 あきら（co-chair）	日本インターネットエクスチェンジ株式会社
印南 鉄也（co-chair）	ソフトバンク BB 株式会社
島田 康晴	株式会社アイ・オー・データ機器
新 善文	アラクサラネットワークス株式会社
鹿志村 康生	アルカテル・ルーセント
芦田 宏之	イッツ・コミュニケーションズ株式会社
佐原 具幸	株式会社インターネットイニシアティブ
川島 正伸	ＮＥＣアクセステクニカ株式会社
鈴木 聡介	NTT コミュニケーションズ株式会社
友近 剛史	NTT コミュニケーションズ株式会社
水越 一郎	東日本電信電話株式会社
岡田 真悟	日本電信電話株式会社
屏 雄一郎	株式会社 KDDI 研究所
土屋 師子生	シスコシステムズ合同会社
河野 美也	Juniper Networks
辻 晃	センチュリー・システムズ株式会社
中田 宗宏	センチュリー・システムズ株式会社
上根 義昭	ソネットエンタテインメント株式会社
村上 誠	ソフトバンクテレコム株式会社
菅沼 真	株式会社 電算
花山 寛	ネットワンシステムズ株式会社
伊田 吉宏	パナソニックシステムネットワークス株式会社
本橋 篤	富士通株式会社
小野田 充宏	ヤマハ株式会社
津国 剛（事務局）	株式会社三菱総合研究所
福島 直央（事務局）	株式会社三菱総合研究所

10.4 リファレンス一覧

[1] RFC 5072: IP Version6 over PPP
[2] RFC 5172: Negotiation for IPv6 Datagram Compression Using IPv6 Control Protocol
[3] RFC 1994: PPP Challenge Handshake Authentication Protocol (CHAP)
[4] RFC 3056: Connection of IPv6 Domains via IPv4 Clouds (6to4)
[5] RFC 4380: Tunneling IPv6 over UDP through Network Address Translations (Teredo)
[6] RFC 2784: Generic Routing Encapsulation (GRE)
[7] draft-kuwabara-softwire-ipv6-via-l2tpv2-00: A Model of IPv6 Internet Access Service via L2TPv2 Tunnel
[8] 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-01078.html
[9] RFC 4890: Recommendations for Filtering ICMPv6 Messages in Firewalls
[10] RFC 4864: Local Network Protection for IPv6
[11] RFC 5095 Deprecation of Type 0 Routing Headers in IPv6
[12] draft-mrw-behave-nat66-02: IPv6-to-IPv6 Network Address Translation (NAT66)
[13] DOCSIS 3.0 specification http://www.cablelabs.com/specifications/doc30.html
[14] RFC 5625: DNS Proxy Implementation Guidelines
[15] RFC 3484: Default Address Selection for Internet Protocol version 6 (IPv6)
[16] RFC 4477: Dynamic Host Configuration Protocol (DHCP) : IPv4 and IPv6 Dual-Stack Issues
[17] IPv6 マルチプレフィックス環境の構築に関する考察 http://www.v6pc.jp/pdf/v6pc-mp-1.0.pdf
[18] Kaminsky Attack に関する情報 http://jprs.jp/tech/security/multiple-dns-vuln-cache-poisoning.html
[19] RFC 2671: Extension Mechanisms for DNS (EDNS0)
[20] RFC 1035: DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION
[21] RFC 1123: Requirements for Internet Hosts -- Application and Support
[22] RFC 4033: DNS Security Introduction and Requirements
[23] RFC 4034: Resource Records for the DNS Security Extensions
[24] RFC 4035: Protocol Modifications for the DNS Security Extensions
[25] DNSSEC on Windows 7 DNS client http://blogs.technet.com/sseshad/archive/2008/11/11/dnssec-on-windows-7-dns-clien

t.aspx
[26] RFC 4294: IPv6 Node Requirements
[27] RFC 3315: Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
[28] RFC 4294: IPv6 Node Requirements
[29] RFC 4861: Neighbor Discovery for IP version 6 (IPv6)
[30] RFC 3633: IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6
[31] RFC 5006: IPv6 Router Advertisement Option for DNS Configuration
[32] RFC 4339: IPv6 Host Configuration of DNS Server Information Approaches
[33] RFC 4443: Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
[34] RFC 2080: RIPng for IPv6
[35] RFC 4191: Default Router Preferences and More-Specific Routes
[36] RFC 4601: Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)
[37] RFC 2362: Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification
[38] RFC 4607: Source-Specific Multicast for IP
[39] RFC 2710: Multicast Listener Discovery (MLD) for IPv6
[40] RFC 3810: Multicast Listener Discovery Version 2 (MLDv2) for IPv6
[41] RFC 4604: Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast
[42] RFC 4605: Internet Group Management Protocol (IGMP) / Multicast Listener Discovery (MLD)-Based Multicast Forwarding ("IGMP/MLD Proxying")
[43] RFC 4541: Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches
[44] TR-069 http://www.broadband-forum.org/technical/download/TR-069Amendment2.pdf
[45] UPnP http://www.upnp.org/specs/arch/UPnP-arch-DeviceArchitecture-v1.1.pdf
[46] RFC 4291: IP Version 6 Addressing Architecture
[47] RFC 4787: Network Address Translation (NAT) Behavioral Requirements for Unicast UDP
[48] RFC 4862: IPv6 Stateless Address Autoconfiguration
[49] RFC 3319: Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers

[50] RFC 3646: DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
[51] RFC 3898: Network Information Service (NIS) Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
[52] RFC 4075: Simple Network Time Protocol (SNTP) Configuration Option for DHCPv6
[53] draft-ietf-softwire-ipv6-6rd-08: IPv6 via IPv4 Service Provider Networks "6rd"
[54] draft-shirasaki-nat444-isp-shared-addr-03: NAT444 with ISP Shared Address
[55] draft-ietf-softwire-dual-stack-lite-04: Dual-stack lite broadband deployments post IPv4 exhaustion
[56] draft-ymbk-aplusp-05: The A+P Approach to the IPv4 Address Shortage
[57] Issues with Port-Restricted IPs
http://www.ietf.org/proceedings/09nov/slides/aplusp-3.pdf
[58] draft-ietf-behave-v6v4-xlate-stateful-11: Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers
[59] draft-ietf-v6ops-ipv6-cpe-router-04: Basic Requirements for IPv6 Customer Edge Routers
[60] IPv6 移行ガイドライン（2005 年版）・セキュリティセグメント
http://www.v6pc.jp/jp/archive/index.phtml
[61] draft-ietf-v6ops-cpe-simple-security-11: Recommended Simple Security Capabilities in Customer Premises Equipment for Providing Residential IPv6 Internet Service
[62] RFC 5571: Softwire Hub and Spoke Deployment Framework with Layer Two Tunneling Protocol Version 2 (L2TPv2)
[63] draft-ietf-6man-text-addr-representation-07: A Recommendation for IPv6 Address Text Representation
[64] RFC 3041: Privacy Extensions for Stateless Address Autoconfiguration in IPv6