IPv6 マルチプレフィックス環境の構築に関する考察

【第１版】

2007 年 6 月 22 日

IPv6 普及・高度化推進協議会

移行 WG マルチプレフィックス検討 SWG

目次

1　はじめに

1.1　背景

昨今、日本国内で提供されるIPv6サービスが増えはじめている。サービス内容としては、ISPによるインターネット接続サービスに加え、映像配信やビルオートメーションなど、アプリケーションに特化したものもある。

こうしたサービス事情のもと、ユーザは複数のISPの利用によるマルチホーム環境の構築や、ISPとアプリケーションに特化したIPv6サービスの利用などを目的として、複数のIPv6サービスを契約する可能性がある。この場合、それぞれのIPv6サービスがユーザサイトにプレフィックスを割り当てる構成も考えられる。

しかし、このような「マルチプレフィックス環境」では、いくつか解決すべき課題が残されていることが分かっている。

こうした背景のもと、2006年6月にIPv6普及・高度化推進協議会の移行ワーキンググループにおいて、マルチプレフィックス検討サブワーキンググループを発足した。本サブワーキンググループは、マルチプレフィックス環境の構築に関する課題の整理と、それぞれの課題に対して想定される解決手法についての検討を行うことを目的としている。

本文書は、本サブワーキンググループをベースとして実施した検討内容をまとめる。

1.2 本文書における用語定義

本文書における用語定義を表 1.2-1 に示す。

表 1.2-1 用語定義

用語	定義
ISP	ISP（Internet Service Provider）とは、インターネット接続業者である。ユーザである企業や家庭のコンピュータなどをインターネットに接続するサービスを提供する。 本文書における ISP とは、ユーザサイトに対してプレフィックスを払い出し、インターネットリーチャビリティを提供するものと定義する。
閉域 ASP	ASP（Application Service Provider）とは、アプリケーションサービスを提供する業者である。ASP には様々な形態がある。 本文書における閉域 ASP とは、ユーザサイトに対してプレフィックスを払い出すがインターネットリーチャビリティを提供しないものと定義する。
xSP	ISP や ASP など、ネットワークを介してサービスを提供する各種サービスプロバイダの総称。本文書では、ISP と閉域 ASP の総称とする。
ISP マルチホーム	本文書では、ユーザサイトが複数の ISP に接続する形態とする。
プレフィックス	IPv6 アドレスのプレフィックス（Prefix）には、次の意味がある。 1. 連続するアドレスブロックを指す、アドレスの上位部分 2. アドレスの前半の/64 部分 本文書では、1.の意味とする。
サービスネットワーク	本文書では、ユーザに対してプレフィックスを割り当て、インターネットや閉域 ASP へのコネクティビティを提供するネットワークとする。
ユーザサイト	本文書では、ユーザ宅内やユーザ拠点内など地理的なロケーションとする。（図 1.2-1 参照）
ユーザ端末	本文書では、ユーザサイト内にある端末とする。（図 1.2-1 参照）
ユーザルータ	本文書では、ユーザサイト内にあるルータとする。（図 1.2-1 参照）

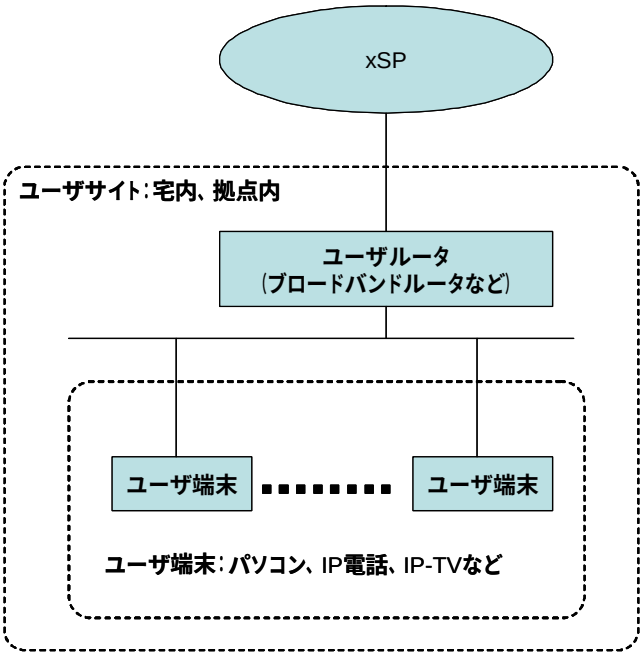


図 1.2-1 ユーザサイト等用語定義補足

1.3 検討対象

本文書の検討対象を以下に示す。

1.3.1 マルチプレフィックス環境の定義

本文書では図 1.3-1 に示すように、ユーザサイトが複数のサービスネットワークに接続し、それぞれからプレフィックスを払い出されている環境を、マルチプレフィックス環境とする。なお、本定義は、端末に複数のアドレスが付与されるかどうかといったユーザサイト内のネットワーク構成や、サービスネットワークとユーザサイト間の回線種別には依らないものとする。

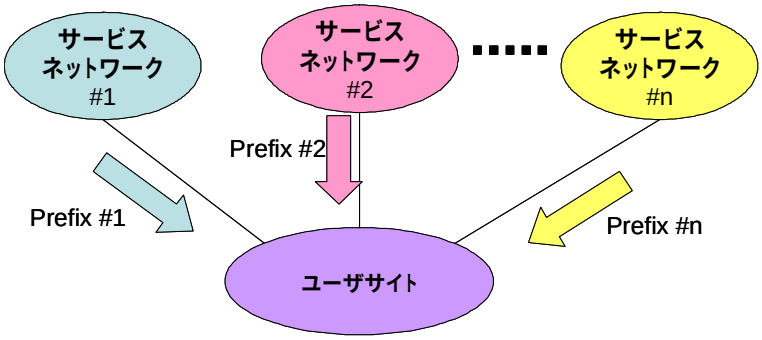


図 1.3-1 マルチプレフィックス環境

1.3.2 ユーザサイト内の構成

マルチプレフィックス環境は、ユーザサイト内において、サービスネットワークと複数の機器（ユーザルータおよびユーザ端末）が接続するか否かという観点、また、ユーザ端末に複数のアドレスが設定されるか否かという観点で分類が可能である。（表 1.3-1 参照）

表 1.3-1 マルチプレフィックス環境の分類

		1 つのユーザ端末に設定されるアドレスの数	
		複数	1 つ
サービスネットワークと接続する機器の数	複数	パターン 1	パターン 3
	1 つ	パターン 2	パターン 4

以下に、表 1.3-1 での分類をもとにユーザサイトの構成例を示す。

[パターン 1]　サービスネットワークとユーザサイト内の複数の機器が接続し、ユーザ端末に複数のアドレスが設定される構成を想定している。構成例を図 1.3-2 に示す。

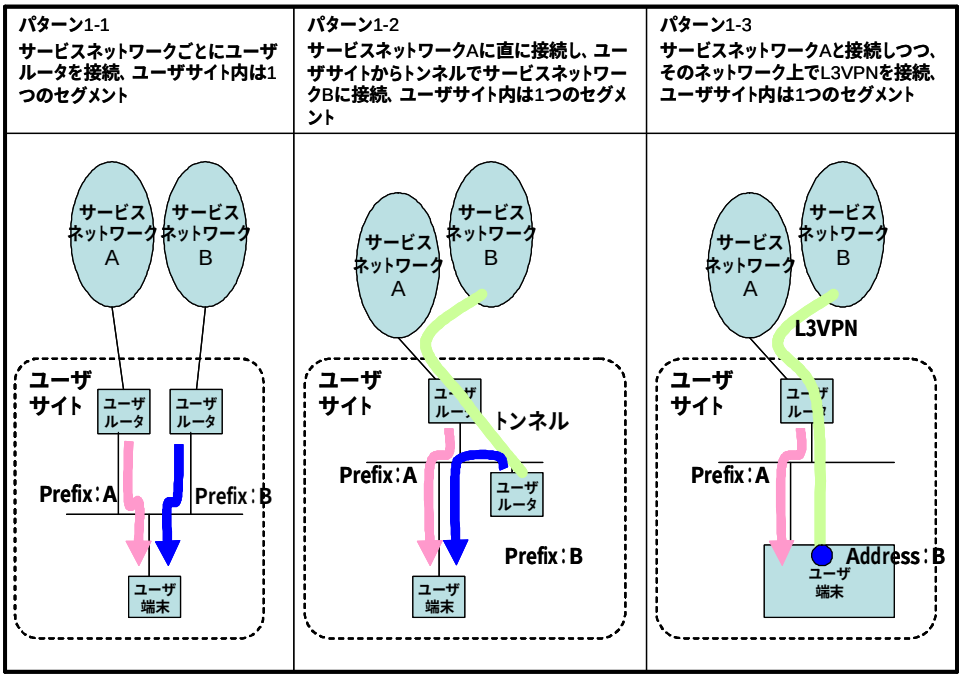


図 1.3-2 パターン 1 のユーザサイト構成例

[パターン 2] サービスネットワークとユーザサイト内の 1 つの機器が接続し、ユーザ端末に複数のアドレスが設定される構成を想定している。構成例を図 1.3-3 に示す。

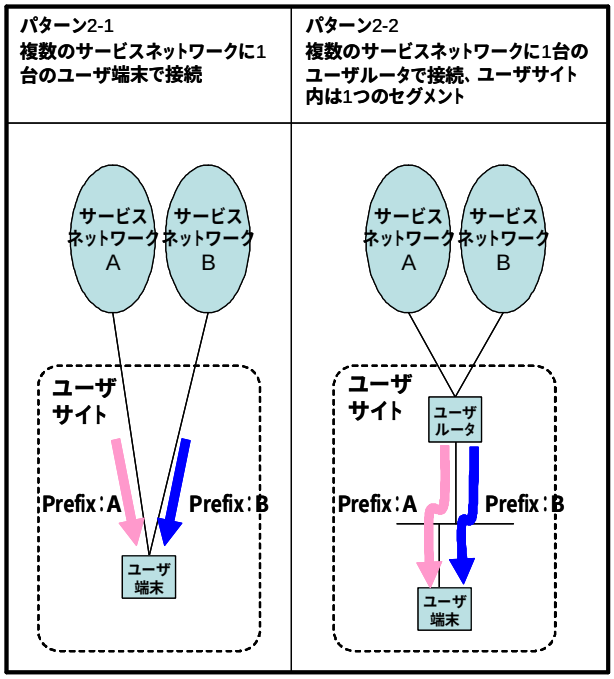


図 1.3-3 パターン 2 のユーザサイト構成例

[パターン 3] サービスネットワークとユーザサイト内の複数の機器が接続し、ユーザ端末に 1 つのアドレスが設定される構成を想定している。構成例を図 1.3-4 に示す。

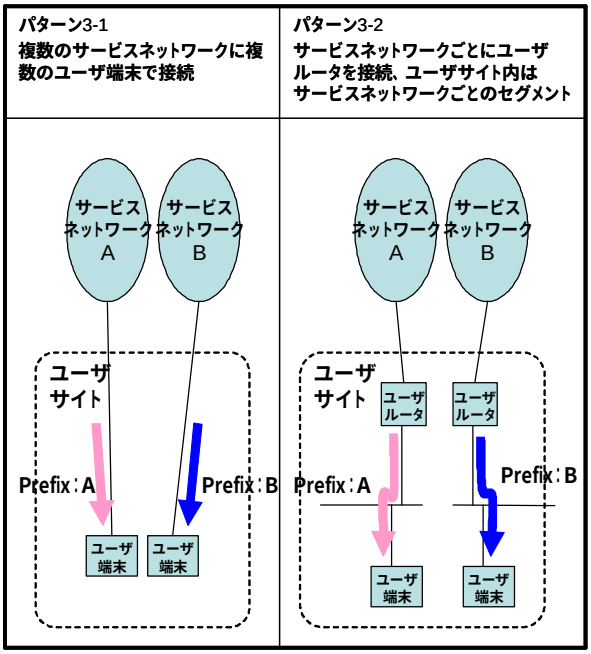


図 1.3-4 パターン 3 のユーザサイト構成例

[パターン 4] サービスネットワークとユーザサイト内の 1 つの機器が接続し、ユーザ端末に 1 つのアドレスが設定される構成を想定している。構成例を図 1.3-5 に示す。

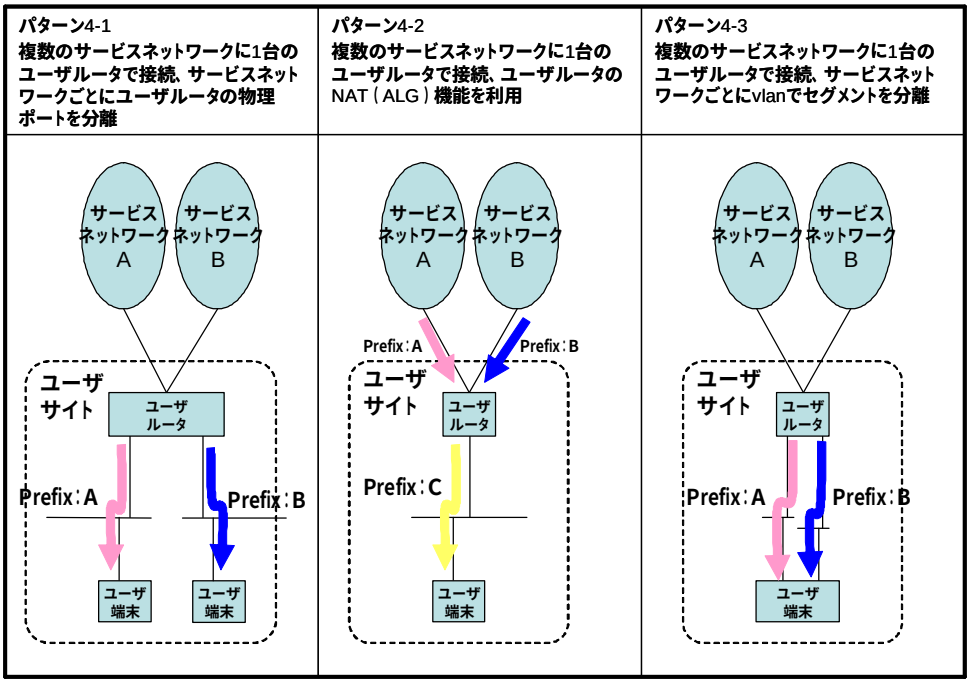
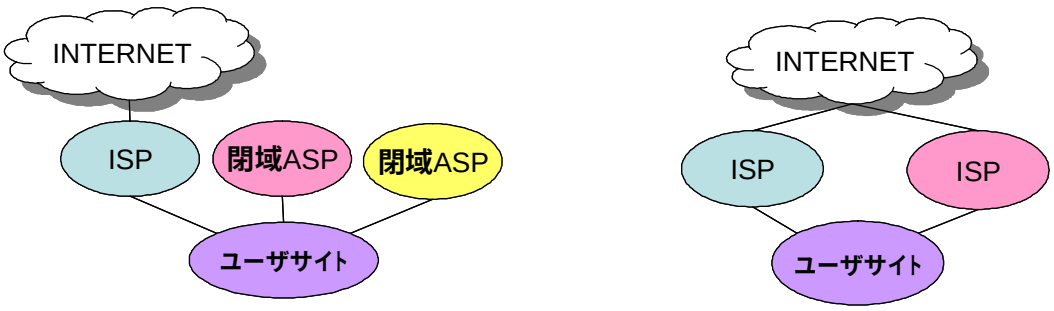


図 1.3-5 パターン 4 のユーザサイト構成例

本文書では、経路選択問題または送信元アドレス選択問題の発生するパターン 1、パターン 2、パターン 4 を検討対象とする。なお、問題の解説については 2 章以降で行う。

1.3.3 サービスネットワークとユーザサイトの接続構成

- サービスネットワークとユーザサイトとの接続構成については、さまざまなバリエーションがあるが、代表的な例として本文書では次の 2 つの構成（図 1.3-6 参照）をモデルとして検討する。
  - ① 単一 ISP と複数閉域 ASP 構成
    - ユーザサイトが 1 つの ISP と複数の閉域 ASP に接続する構成。
    - 本検討では、1 つの ISP と 2 つの閉域 ASP に単純化し、検討を実施する。
  - ② ISP マルチホーム構成
    - 複数の ISP とユーザサイトがマルチホームで接続する構成。
    - 本検討では、2 つの ISP に単純化し、検討を実施する。



①. 単一ISPと複数閉域ASP構成　　②. ISPマルチホーム構成

図 1.3-6 検討するサービスネットワークとユーザサイトの接続構成

- 本サブワーキンググループでは、①を重点的に検討した。また、マルチプレフィックス環境となる構成として ISP マルチホームも考えられるため、②の検討を行った。①と②は独立して検討したため、本文書におけるそれぞれの解決案について必ずしも整合が図られているわけではない。なお、複数の ISP と複数の閉域 ASP にユーザサイトが接続する構成については、①と②の組み合わせであると考えられるが、本文書では検討できていない。
- ユーザサイト内のネットワークについては、原則として、1 サブネット程度のシンプルなネットワークを想定する。

1.4 想定読者

本文書は、IPv6 サービスに関係する下記の方々を想定読者とする。

・IPv6 サービス提供者（xSP 事業者）

本文書は、ユーザサイトが IPv6 サービスを複数同時利用する場合に、ユーザサイト内で発生する可能性のある課題についてまとめている。また、現在検討されている課題解決手法についてもまとめている。

・IPv6 サービス接続用機器の提供者

本文書は、ユーザサイトが IPv6 サービスを複数同時利用する場合に、ユーザルータ等、現在の一般的な接続用機器が、どのような挙動を示すかについて課題を含めてまとめている。また、現在検討されている課題解決手法についてもまとめている。

・IPv6 端末/端末用ソフトウェアの提供者

本文書は、ユーザサイトが IPv6 サービスを複数同時利用する場合に、現在の一般的なユーザ端末が、どのような挙動を示すかについて課題を含めてまとめている。また、現在検討されている課題解決手法についてもまとめている。

1.5 本文書の構成

本文書の構成を次の表 1.5-1 に示す。

表 1.5-1 本文書の構成

章番号	タイトル	主な内容
1	はじめに	・背景 ・本文書におけるマルチプレフィックス環境の定義 ・本文書が検討範囲とするマルチプレフィックス環境の構成
2	単一 ISP と複数閉域 ASP 構成の課題検討	・課題の整理 ・各課題に関して想定される解決手法
3	ISP マルチホーム構成の課題検討	・課題の整理 ・各課題に関して想定される解決手法
4	セキュリティ考察	・マルチプレフィックス環境に特有のセキュリティ上の注意事項についての考察結果
5	マルチプレフィックス環境の事例紹介	・マルチプレフィックス環境を活用したサービス構築への取り組みの紹介 ・マルチプレフィックス環境の構築事例の紹介
6	まとめ	・今回検討しきれなかった事項について ・本文書のまとめ

1.6 検討メンバー

本文書の検討メンバーを次表に示す。記載順は会務担当者を除き、所属の 50 音順に従っている。

表 1.6-1 本文書作成の検討メンバー

姓名	所属
松本 存史【主査】	日本電信電話株式会社 PF 研
金山 健一【副査】	株式会社インテック・ネットコア
鈴木 伸介	アラクサラネットワークス株式会社
荒野 高志	株式会社インテック・ネットコア
廣海 緑里	株式会社インテック・ネットコア
川島 正伸	NEC アクセステクニカ株式会社
常川 聡	東日本電信電話株式会社
植松 高史	西日本電信電話株式会社
槇林 康雄	西日本電信電話株式会社
藤崎 智宏	日本電信電話株式会社 PF 研
上水流 由香	NTT コミュニケーションズ株式会社
鈴木 聡介	NTT コミュニケーションズ株式会社
瀬川 卓見	パナソニックコミュニケーションズ株式会社
池田 伸一	松下電器産業株式会社
金本 秀勝	松下電器産業株式会社
高村 信【オブザーバ】	総務省 総合通信基盤局 電気通信事業部 データ通信課
能登 治【オブザーバ】	総務省 総合通信基盤局 電気通信事業部 データ通信課
中村 秀治【事務局】	IPv6 普及・高度化推進協議会事務局 株式会社三菱総合研究所
澤部 直太【事務局】	IPv6 普及・高度化推進協議会事務局 株式会社三菱総合研究所
佐藤 明男【事務局】	IPv6 普及・高度化推進協議会事務局 株式会社三菱総合研究所
神保 至【事務局】	IPv6 普及・高度化推進協議会事務局 株式会社三菱総合研究所
津国 剛【事務局】	IPv6 普及・高度化推進協議会事務局 株式会社三菱総合研究所
福島 直央【事務局】	IPv6 普及・高度化推進協議会事務局 株式会社三菱総合研究所
黒坂 達也【事務局】	IPv6 普及・高度化推進協議会事務局

2　単一 ISP と複数閉域 ASP 構成の課題検討

2.1　課題

2.1.1　送信元アドレス選択問題

端末の１つのネットワークインターフェースに複数のアドレスが付いた場合、期待されるアドレスとは別の送信元アドレスが選択されることがある。

送信元アドレスが誤って選択された場合、上流回線を提供するネットワーク事業者においては、セキュリティ確保等の観点から、事業者が払い出したアドレス以外を送信元アドレスとしたパケットを廃棄することが一般的に実施されている。このような ISP に入ってくるパケットに対するフィルタは Ingress Filter と呼ばれる。また閉域 ASP の場合、閉域 ASP のアドレスを用いてインターネット上のホストにパケットを送信すると、インターネットから閉域 ASP のアドレスに対する経路が存在しないために、相手ホストからの応答パケットが届かず、通信が正常に行えない。これは ISP が Ingress Filter を実施していない場合でも発生する問題である。

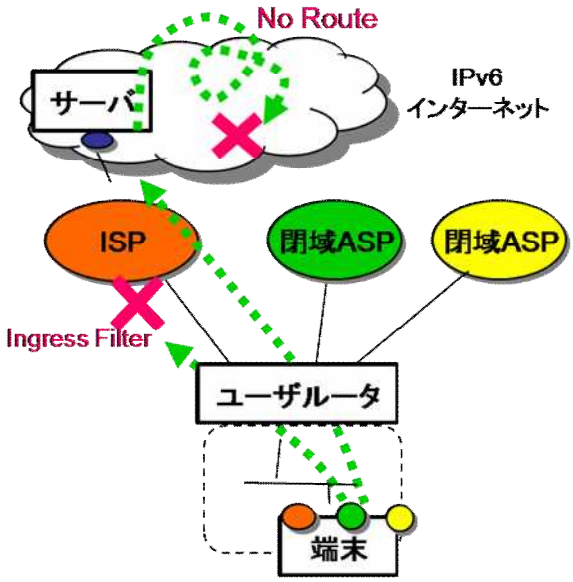


図 2.1-1 送信元アドレス選択問題

送信元アドレス選択のルールは RFC 3484 で定められており、送信先アドレスと送信元アドレスに関する様々な状況を考慮してアドレス選択が行われることが規定されているが、一般的に 1 つのインターフェースに複数の IPv6 グローバルアドレスが付いている場合は、送信先アドレスと送信元アドレスの上位ビットからの一致ビット数によって決定されることが多く（ロンゲストマッチアルゴリズム）、送信先アドレスによっては、送信元アドレスが誤って選択される。

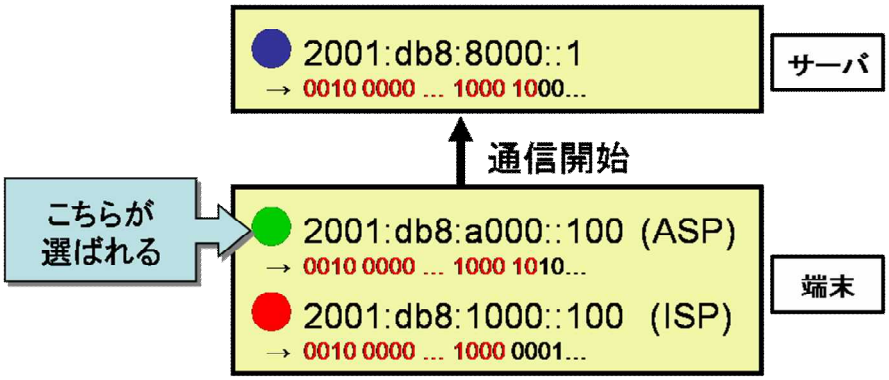


図 2.1-2 ロンゲストマッチアルゴリズムによるアドレス選択の例

[解説] 例えば図 2.1-2 のように、通信を開始する端末が ISP から 2001:db8:1000::100 というアドレスを付与され、同時に閉域 ASP の 1 つから 2001:db8:a000::100 というアドレスを付与されており、通信相手が 2001:db8:8000::1 というアドレスを持っていた場合、このロンゲストマッチアルゴリズムにより、送信元アドレスは 2001:db8:a000::100 となる。これは閉域 ASP から付与されたアドレスであり、前述のようにこのアドレスに対するインターネットからの戻り経路がないため通信が失敗する。

2.1.2 経路選択問題

ユーザサイトが複数のサービスネットワークと接続している場合、端末またはユーザルータにおいて、送信するパケットを次に転送するルータ（ネクストホップ）を適切に選択しなければ、通信できないことがある。これを経路選択問題と呼ぶ。

[解説] 例えば、同一リンク上で IPv6 の RA が複数のルータから送信されるような環境では、デフォルトルートをどちらに設定するかは実装依存であり、例えば先に受信した RA を優先するようになっている実装では、RA を受信するタイミングに依って、また通信相手に依って、通信ができなくなる可能性がある。図 2.1-3 のように、インターネットと閉域 ASP という 2 つの上流回線を持つ場合、閉域 ASP 側のルータにデフォルトルートを向けてしまうと、閉域 ASP からインターネットへ抜ける経路は存在しないため、インターネット上に通信相手がいる場合、通信不能に陥る。

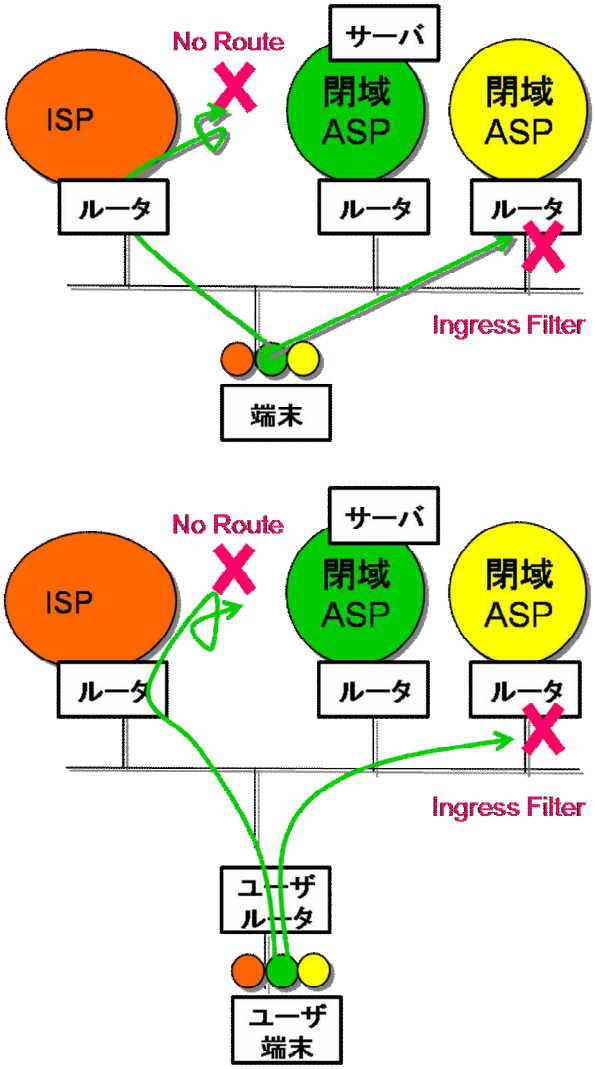


図 2.1-3 経路選択問題

また、逆に ISP 側のルータにデフォルトルートを向けてしまうと、インターネットから ASP へ到達する経路が存在しないため、通信相手からの応答パケットが届かないという状況に陥る。

このようなネクストホップの誤選択については、ICMP リダイレクトを用いてホストに正しいルータをネクストホップとして選択するよう通知することが可能である。しかし、そのためにはホストのネクストホップとなる複数のルータが同一リンク上に存在し、かつそのルータ間で経路情報の交換が行われていなければならず、ICMP リダイレクトを利用できる環境は限られる。

2.1.3 DNS サーバ選択問題

ISP や閉域 ASP 等のサービスネットワークでは各々異なるポリシにて DNS サーバ運用を行っていることがあり、その場合、マルチプレフィックス環境となるユーザサイトにおいて、DNS サーバをサービスネットワーク毎に使い分ける必要がある。

このような環境では、DNS サーバの選択を誤ると名前解決に要する通信遅延の発生や、場合によっては通信できない事象の発生が懸念される。

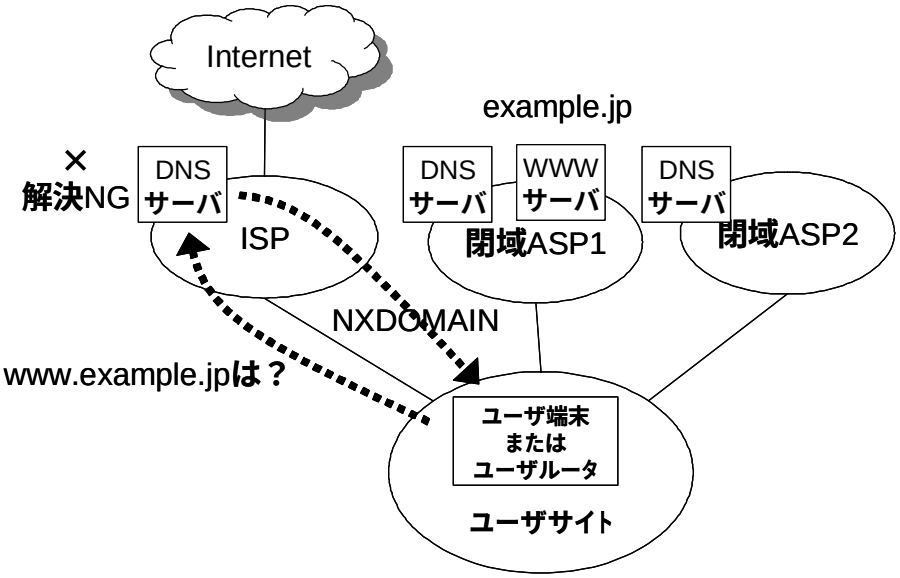


図 2.1-4 DNS サーバ選択問題

[解説] 例えば図 2.1-4 では、閉域 ASP1 内の DNS サーバが example.jp のドメイン管理を行っている。ユーザ端末またはユーザルータが www.example.jp との通信を行う目的で ISP 内の DNS サーバに対して DNS クエリ送出した場合、ドメインが存在しないことを示す NXDOMAIN が応答されることがある。このような場合に名前解決が失敗する可能性がある。

2.1.4 今回の活動では検討しきれなかった事項について

今回、マルチプレフィックス環境で発生しうるいくつかの問題について検討を行った。しかしながら、今回検討した問題以外にも DNS ドメインサフィックスの選択問題、Web プロキシの選択問題などが指摘されている。実際のマルチプレフィックス環境の構築にあたってはこれらの問題に対する検討も必要である。

2.2 解決手法

2.2.1 送信元アドレス選択問題に対する解決案

以下に送信元アドレス選択問題を解決するための方式について述べる。

・ポリシテーブルの活用

Windows や Solaris 等の多くの OS には、RFC 3484[1]で定められたポリシテーブルというアドレス選択を制御するための機構が実装されている。このポリシテーブルを適切に設定することによって、大抵の環境では送信元アドレス選択問題を回避することができる。ただ、一般のユーザにこのポリシテーブルを手動で設定させることは、その設定操作が難しいことや、設定情報を通知する仕組みが必要なることから困難である。

そこで、ポリシテーブル情報を自動的に配布する方法や、ツールを利用することによってポリシテーブルを設定する方法が必要である。ポリシテーブルを自動配布する方式としては、DHCPv6 オプションを利用する方法が IETF にて提案されている が、市中の製品への実装も行われておらず、今すぐに利用することはできない。また、ポリシテーブルを設定するツールとしては付録・III が存在するが、これは IPv4 と IPv6 の優先度を切り替えることのみを目的としたツールである。

図 2.2-1 のように、ISP が 2001:db8:1::/48 というアドレスブロックを、ASP1 が 2001:db8:2::/48 を保持し、それぞれから 2001:db8:1::/56、2001:db8:2::/56 というアドレスプレフィックスをユーザネットワークに付与した場合、このユーザネットワーク内の端末に図 2.2-1 のようにポリシテーブルを設定することにより[2]、前述の通信障害を回避することができる。Prec とは Precedence の意で、送信先アドレス選択を決める際に用いられるため、本文書では説明を割愛する。送信元アドレス選択については、図 2.2-1 の状況ではポリシテーブルの Label フィールドを用いて、どのアドレスを用いるかが決定される。例えば閉域 ASP1 内の 2001:db8:2:ffff::1 というアドレスを持つサーバと通信を行う場合、送信先アドレスはポリシテーブルの 3 行目のアドレスブロックにマッチすることから、Label は 2 となる。このとき、同様に Label が 2 となるアドレスが送信元アドレスとして優先され、2001:db8:2::という ASP1 から付与されたプレフィックスを持つアドレスが選択される。一方、インターネット上のホスト 2001:db8:4::1 というサーバに接続する際にも同様の方法でアドレスの優先順位が決まり、送信先アドレスがマッチするのは 2 行目となり Label は 1 となる。このとき、Label が 1 となる ISP から付与されたプレフィックス 2001:db8:1::を持つアドレスが選択される。

通常端末が保持できるポリシテーブルは 1 つであり、図 2.2-1 のように xSP がそれぞれ

[1] RFC 3484, “Default Address Selection for Internet Protocol version 6 (IPv6)”

[2] 実際には、インターネットに接続しているホストのポリシテーブルには、上記以外に IPv4 アドレスに関するポリシや、6to4 と呼ばれるトンネルを用いた IPv6 接続のためのアドレスに関するポリシも含めるべきであるが、ここでは簡単のために ISP と閉域 ASP に関するポリシのみ記述した。

ポリシテーブルを配布する環境では、ユーザルータまたは端末においてポリシテーブルを結合し、端末は１つのポリシテーブルとして格納する必要がある。ポリシテーブルでは同一プレフィックスに対するポリシは１つしか保持できないため、同一プレフィックスに対するポリシが複数配布されるような環境では、１つを選択して格納しなければならない。しかし、xSP 内のネットワーク構成について深い知識を持たない一般ユーザに、適切なポリシを選択させることは困難である。対策としては、ユーザに xSP 間の優先度設定をユーザルータや端末に対して設定させ、その優先度に基づきユーザルータや端末が自動的にポリシテーブルの結合を行う等の方法が考えられる。

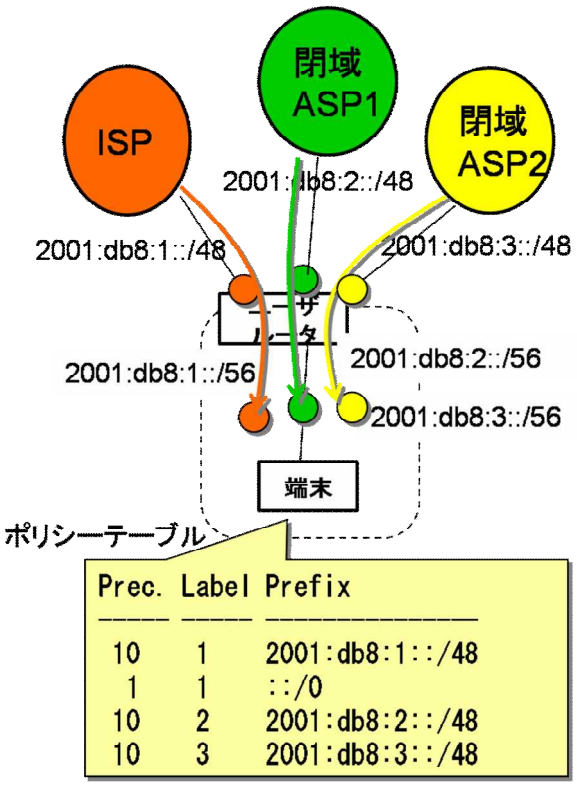


図 2.2-1 ポリシテーブルの配布

・ULA （Unique Local IPv6 Unicast Address）[3]の利用

端末に複数の IPv6 グローバルアドレスを付与することにより、送信元アドレス選択問題が生じることは前述の通りであるが、閉域 ASP で用いるアドレスを ULA と呼ばれるものに変えることにより、アドレス選択問題を回避できる場合がある。ULA とは、IPv6 インターネットに接続していない小規模なサイトで用いることを想定して策定されたものである。このアドレスの特徴は、/48 単位で利用すること、ユーザが申請など不要で自由に利用できること、そして fd00::/8 というアドレスブロックを用いることなどがある。また、ULA には、Centrally Managed と呼ばれる管理組織が利用者からの申請に基づいてアドレスを固

[3] RFC 4193, “Unique Local IPv6 Unicast Addresses”

定的に割り当てるタイプのものが提案されていたが、この標準化は現在停止状態にあるため、ここでは標準化が完了しているもののみを検討の対象とする。

図 2.2-2 のように、インターネットへの接続性を提供していない閉域 ASP において、この ULA を用いることにより、ホストでの送信元アドレス選択問題による通信障害を回避することができる。なぜなら、インターネット上で現在用いられている IPv6 のアドレス空間と、ULA で用いられるアドレス空間がかけ離れている、すなわち両アドレスが共有している上位ビット数が 0 であり、ロンゲストマッチアルゴリズムによって正しい送信元アドレス選択が行われるからである。

ただし、現在は IPv4 から IPv6 への過渡期であり、IPv6 アドレスの利用者数も多くないが、今後 IPv6 が普及し IPv6 アドレス空間の多くがグローバルアドレスとして割り振られ、現在グローバルアドレス空間として定義されている 2000::/3 （/32 の経路が 2^29 個相当）が消費され、将来的に 8000::/1 の空間が使われるようになると、このロンゲストマッチアルゴリズムによる問題解決も有効ではなくなってしまう。

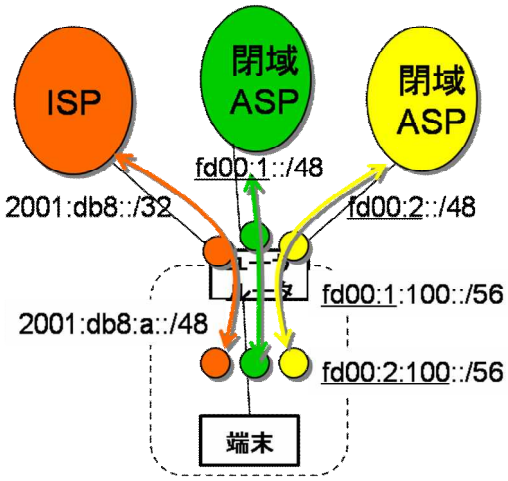


図 2.2-2 ASP での ULA の利用

また、ULA は/48 単位での使用が原則であり、/48 の連続ブロックでの使用は原則として認められていないため、大規模 ISP・閉域 ASP の運営者は非常に多くの ULA ブロックを用いてサイトを運営せねばならず、ネットワークが複雑化するということが挙げられる。特にユーザに/64 よりも大きい/56 などのアドレスブロックを割り当てる場合は、１つの ULA で 256 個までしかアドレスブロックを確保できず、xSP はより多くの ULA を使ってサービスを提供しなければならない。

さらに、ULA では IPv4 のプライベートアドレス同様、他の xSP やユーザが利用しているアドレスブロックと同一になってしまう可能性がある。ただし、ULA ではプレフィックスを乱数によって生成することが定められており、その可能性は極めて低い。前述の Centrally Managed ULA を用いることができれば、/48 よりも大きいアドレスブロックが利用できるようになる可能性があり、またアドレスブロックの衝突も確実に回避すること

ができる。

・ICMP エラーメッセージの利用

本方式では、ユーザ端末が不適切な送信元アドレスを選択したパケットを送信した際に、経路上のルータ等の装置が送信元アドレスの誤選択を検出し、パケット送信元のユーザ端末に ICMP エラーメッセージを送信する。そして、エラーメッセージを受信したユーザ端末は、送信元アドレスを別のものに付け替えて再度通信を試みる。

図 2.2-3 に示すように、端末が単一のユーザルータを介して xSP に接続している環境では、ユーザ端末はサービスネットワークの構成についての情報は不要であり、ルータだけがサービスネットワークの経路を把握しておけば、本方式によって適切な送信元アドレス選択を促すことが可能である。

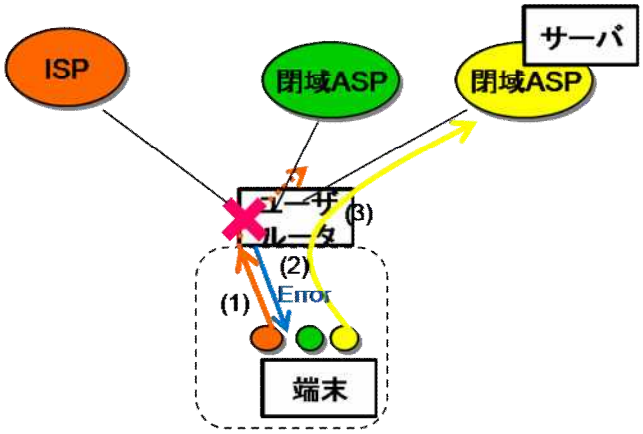


図 2.2-3 ICMP エラーの利用

ただし、現在の TCP/IP プロトコルスタックでは本方式のような、一度選択した送信元アドレスを選択しなおす機能はサポートされておらず、またこの機能を実現するためには、プロトコルスタックの大規模な変更を伴う。IETF の Shim6 ワーキンググループ[4]ではこの通信開始時の障害回避や、通信開始後の障害を回避する機能を実現するための、新しいアーキテクチャの標準化が行われている。

想定される課題として、通信開始時に様々なアドレスを試すことから、アドレスが多数端末に付与される環境では、通信開始時に時間がかかり、ユーザビリティを損ねるといったことが挙げられる。また、ユーザルータに対して xSP に関する経路情報を設定しておく必要があり、このための手段は別途必要である。

・ユーザルータで NAT を用いる

端末に複数の IPv6 アドレスを付与せず、端末のマルチプレフィックス状態を作らないよ

[4] Shim6 WG http://www.ietf.org/html.charters/shim6-charter.html

うにするという方式の１つが、この NAT を用いた方式である。図 2.2-4 に示すように、ユーザサイト内では、ULA（Unique Local IPv6 Unicast Address）もしくはサービスネットワークから割り振られたプレフィックス１つを用い、ユーザルータにおいて出口インターフェースのアドレス（プレフィックス）に NAT を行うことで、ホストでの送信元アドレスの誤選択を防ぐことが可能である。ただし、ユーザルータには、サービスネットワークに対する適切な経路情報が設定され、ユーザルータが出口インターフェースに付与されたアドレスを送信元アドレスとして選択できる必要がある。

本方式は、IPv4 ではしばしば用いられる方式であるが、本来の IPv6 のメリットである End-to-End での IP 通信ができなくなってしまう可能性があることから、その利用は推奨されない。

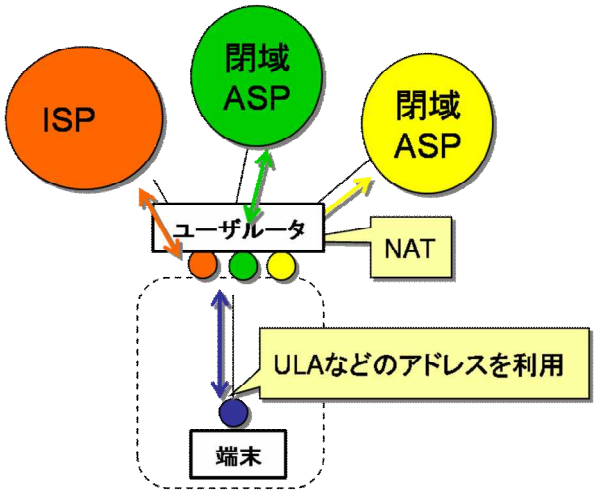


図 2.2-4 NAT の利用

・ALG（Application Level Gateway）を用いる

NAT 方式とは、IP 層のアドレスを書き換えることによって、端末とサーバ間の通信を介在する NAT 装置によって IP 層で終端する方式であった。ALG 方式では IP 層ではなく、アプリケーション層において、ALG 装置が通信を終端するものである。ウェブプロキシーを例にとると、端末はウェブプロキシーに対してウェブページの取得要求を行い、ウェブプロキシーは端末からの要求を受けて、ウェブサーバに対して当該ウェブページの取得要求を行う。このとき、端末-ALG 装置間と ALG-サーバ間の HTTP 通信は全く別の通信であり、HTTP 通信を ALG 装置が終端しているといえる。

本方式により、NAT を用いることなく、NAT と同様に端末でのアドレス選択問題の発生を回避することができる。しかし、端末とサーバとの End-to-End 通信ができなくなるということや、利用できるサービスが ALG の機能によって制限されたり、アプリケーションにおいても ALG のサポートが必要になったりすることが留意点として挙げられる。

・ユーザルータのポート毎にネットワークセグメントを分割する（物理 NW 分割）

NAT 方式と同様に、端末をマルチプレフィックス状態にしない方法として、ポート分割方式が挙げられる。ユーザルータが複数のポートを持ち、ポート毎にセグメントを分けることで、１つのポートからは１つのプレフィックスしか利用できない環境を作る、という方式である。この場合、図 2.2-5 に示すように、例えば PC 端末はインターネットへつながる ISP 専用ポート、一方テレビ（セットトップボックス）や電話はその ASP へつながる専用ポートへつなげる、といった利用方法になる。

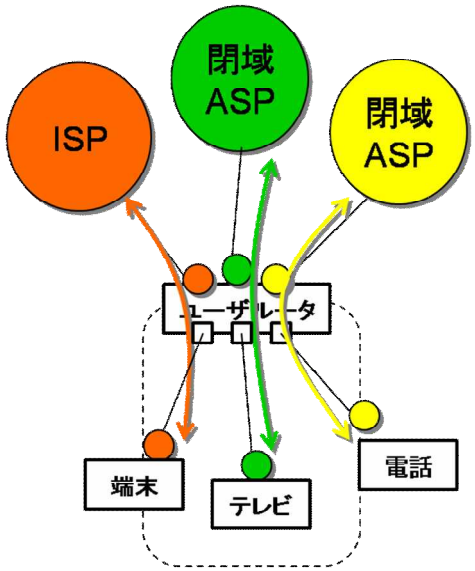


図 2.2-5 ポート毎にネットワークセグメントを分割する

本方式は、新たな通信プロトコル・端末実装の改変などを必要としないというメリットがある反面、1 つの端末が複数インターフェースを用いない限り、複数のサービスを同時に利用できず、使用するサービスを切り替える場合には、接続するポートのつなぎかえが必要になるということや、ユーザネットワーク内の端末同士が別々のセグメントであれば通信できない、という制約がある。またユーザが複数のネットワークの存在とその使い分けを意識する必要があることから、ユーザビリティが低下につながる可能性があり、サービス提供者にとってはトラブルシューティングの稼働が増える恐れがある。

・VLAN（論理 NW 分割）

上に述べた方式は、物理的にポート単位でネットワークを分割するという方式であったが、VLAN や各種トンネルプロトコルを用いて、論理的にネットワークを分割することによって、1 つの論理ネットワークインターフェースに 1 つのアドレスを付与し、送信元アドレス選択問題を回避する、という方式も考えられる。例えば IEEE802.1q にて定められる tagged VLAN を用いれば、端末の 1 つの物理インターフェースで、複数の NW を利用できる。

この方式では、1 つの端末が 1 つの NW しか同時に利用できないというデメリットは無く

なるが、ユーザルータと端末への VLAN ID 等の設定を自動で行う方式は存在しないため、これをユーザが手動で行うことになる。

先に述べたアドレス選択問題を解決する手法の評価を下記の表にまとめた。この表では、これまでに行った各送信元アドレス選択手法の評価を xSP、ベンダ、ユーザという 3 つの視点から分類した。

表 2.2-1 送信元アドレス選択問題の解決手法の評価のまとめ

方式	xSP 視点	ベンダ視点	ユーザ視点	実装状況
ポリシテーブル配布(手動設定)	×xSP 間のポリシ衝突の可能性有り ×ユーザに対する設定情報の通知が別途必要	○機器への変更不要	×設定が煩雑(ツールにより簡単化可能)	○ Windows, *BSD, Solaris 等に実装済み
ポリシテーブル配布(自動設定)	×xSP での装置導入が必要 ×xSP 間のポリシ衝突の可能性有り	×標準無し	×ポリシ結合設定が必要になる可能性有り ×ユーザルータ, 端末への実装が必要	×対応実装無し
ULA	×xSP 間のアドレス衝突の可能性有り ×大規模 xSP では運用が複雑化	○機器への変更不要	×ユーザが利用するアドレスと衝突の可能性有り	×将来的に効果消滅の可能性有り
ICMP エラー	×ユーザルータへの経路情報通知手段が別途必要	×標準無し	×通信開始までに時間がかかる恐れあり ×ユーザルータ、端末での実装必要	×実装無し ×既存のプロトコルスタックに大幅な変更必要

方式	xSP 視点	ベンダ視点	ユーザ視点	実装状況
NAT	×ユーザ端末との End-to-End での IP 通信ができない	×IPv6 の設計思想と不一致(標準無し)	×ユーザルータへの機能付加が必要 ×アプリケーションへの変更が必要となる可能性あり	×実装無し
ALG	×ユーザ端末との End-to-End 通信ができない	○標準化技術と競合しない	×利用できるアプリケーションが制限される可能性有り ×ALG の設置が必要(またはユーザルータへの変更必要)	○ALG ソフトウェア実装は多数存在 ×DNS-ALG 以外のユーザルータでの実装は非一般的
物理 NW 分割(ポート分割)	○xSP 間の競合が発生しにくい ×ユーザサポート稼働が高くなる恐れあり	○標準化技術と競合しない	×複数ネットワークの使い分けを意識する必要あり ×単一端末の同時複数 NW 接続困難 ×ユーザルータへの機能実装必要 ×ユーザサイト内通信不可	×ユーザルータでの実装は無い ○高機能ルータでのポート VLAN の実装は一般的
論理 NW 分割(VLAN)	○xSP 間の競合が発生しにくい	○Tagged VLAN は標準あり	×ルータ及び端末への設定が必要 ×ユーザルータ、ユーザ端末への機能実装必要	×ユーザルータ、での実装は非一般的 ○ TaggedVLAN の高機能ルータでの実装は一般的

2.2.2　経路選択問題に対する解決案

・経路情報の配布：ルーティングプロトコル

ユーザルータや端末に経路情報を配布する方法として、RIPng や OSPFv3 などのルーティングプロトコルがある。本方式は以前から存在し、多くのバックボーンルータで実装され、現在でも多くのネットワークで用いられており、実装・仕様の両面で安定した運用が期待できる。しかし、廉価な家庭用ユーザルータや、ユーザ向け端末などには実装されていない場合がほとんどであり、xSP 側のユーザ収容ルータにおいても、ユーザサイトとの間でルーティングプロトコルを用いる運用はほぼ実施されていない。

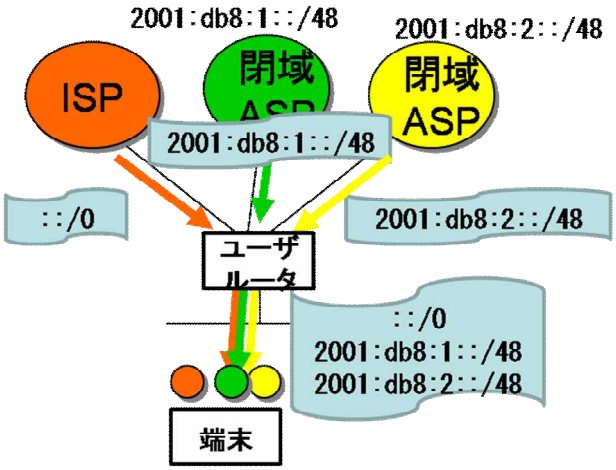


図 2.2-6 ルーティングプロトコルによる経路情報の配布

・経路情報の配布：RA + More Specific Routes

経路情報を配布する別の手段として、RFC4191 にて定義される、More Specific Routes というオプションを用いる方法がある。RA はルータがサブネット内の端末に対して、そのサブネットで用いるプレフィックスとデフォルトルートを広告するためのものであるが、このオプションを用いることにより、デフォルトルート以外の特定の経路情報も併せて広告することができる。またこのオプションでは、デフォルトルートを広告せず、特定の経路のみを広告することも可能である。

RFC4191 はそもそも複数インターフェースを持つ端末が、複数のネットワークにつながっている際の経路選択問題を解決することを目的として策定されたものであるが、図 2.1-3 のような単一リンク上に複数のルータが存在する場合の経路選択にも適用可能である。

RFC は存在するものの、More Specific Routes の実装は現時点では広く普及しているとは言えない。ユーザ端末では Windows Vista での実装が確認されているが、ルータでの実装はまだ多くはない。

RFC4191 では、Router Preference と呼ばれる、ルータの優先度情報を同時に広告することができ、これを用いることで端末が複数の RA を受信した場合にどちらの RA を優先す

るか、という設定を行うことができる。

・経路情報の配布：手動設定
上述の 2 つの手法以外に、端末またはルータの経路表を手動設定する方法がある。この手法では、xSP のルータやユーザルータ・ユーザの端末に新たな実装は必要とされないが、ユーザに設定すべき経路情報を通知する別の手段が必要であり、また煩雑な設定作業をユーザに強いることによりユーザビリティを低下させる、というデメリットがある。このようなユーザビリティの低下を緩和するために、ユーザサイトの環境に応じて経路情報を自動設定するツールを利用するという方法も考えられる。

・ICMP リダイレクトによる経路制御
端末に経路情報をあらかじめ配布することなく、パケットを中継するルータからのメッセージによって、動的に端末に経路情報を配布する方式が本方式である。図 2.2-7 のように、端末がネクストホップを誤ってパケットを送信したとき、パケットを受信したユーザルータがその送信先アドレスに対する適切なネクストホップ情報を保持していれば、端末に対して ICMP リダイレクトと呼ばれるメッセージを送信することができる。ICMP リダイレクトを受信した端末は、ルーティングテーブルに送信先に対するネクストホップ情報を記録し、エラーとなったパケットを指示されたネクストホップに対して送信する。以上により、端末への事前設定の必要なく、適切な経路選択を行うことができる。

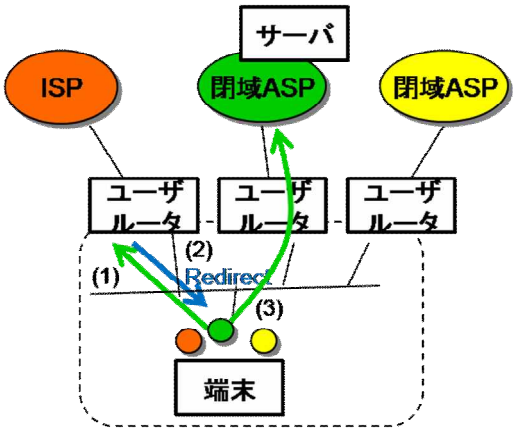


図 2.2-7 ICMP リダイレクトを用いた経路選択

本方式は IPv4 や IPv6 の基本機能であり、ほぼ全ての端末やルータにおいて実装されていると考えられる。ただし、本方式ではルータが同一リンク上に存在し、かつそのルータ間で経路情報を交換しておく必要がある。通常、xSP 間の経路情報をユーザサイトを介して交換することは考えにくい。そこで本文書では、図 2.2-7 のように、ユーザがそれぞれの xSP との接続のためにユーザルータを設置し、それらを同一リンクに接続した環境を本

方式の適用対象とする。

・送信元アドレスに基づくポリシルーティング

経路情報を必要とすることなく、経路選択問題を解決する方法が、この送信元アドレスに基づくポリシルーティングである。ユーザルータはサービスネットワークから、DHCP-PD などによりアドレスブロックを割り当てられ、その全てまたは一部をユーザサイトに対して広告する。そしてユーザルータはユーザサイト内の端末から送信されたパケットの送信元アドレスを見て、そのパケットをどのサービスネットワークに対して送信するかを決定する。つまり、パケットの送信元アドレスを含むアドレスブロックを割り当てたサービスネットワークにパケットを転送する。

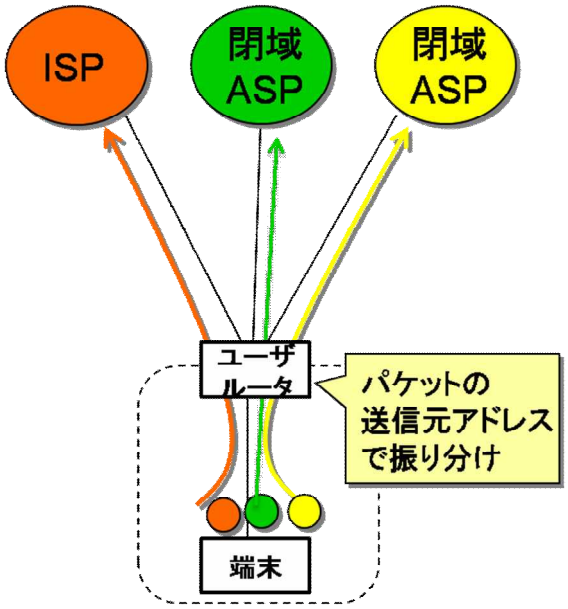


図 2.2-8 送信元アドレスによるポリシルーティング

これにより、ユーザサイト内の端末が適切な送信元アドレスを選びさえすれば、ユーザルータは経路情報を必要とせずに、正しい経路制御を行うことができる。また、近年ブロードバンドルータ等の機器自体も、ファームウェアのバージョンアップなどの理由により、インターネット上に設置されたサーバと通信する必要のある場合があり、その場合はルータ機器においても、経路選択や送信元アドレス選択のための機構が必要となる。

経路選択手法についても同様の項目について評価をまとめた。経路選択手法は、まず経路選択を行う箇所によって、大きくユーザルータとユーザ端末という２つの分類を行い、それぞれに対する各手法の評価を行った。

また、物理 NW 分割（ポート分割）方式は、ポート毎の上流回線の関連付けを行うこと

で、ユーザルータでの経路選択問題の解決も行うことができると考えられるが、この機能は送信元アドレスを用いるポリシルーティング方式と同一であると考えられるため、この表には掲載していない。

この表では、これまでに行った各経路選択手法の評価を xSP、ベンダ、ユーザという 3 つの視点から評価をまとめた。

表 2.2-2 ユーザルータにおける経路選択問題の解決手法の評価のまとめ

方式	xSP 視点	ベンダ視点	ユーザ視点	実装状況
ルーティングプロトコル	×xSP ルータへの(設定)変更が必要 ×マスユーザ向けの運用経験が乏しい	○標準有り	×ユーザルータへの変更必要	○高機能ルータでは既存実装多数 ×全ユーザルータが実装しているわけではない
RA (More Specific Routes)	×xSP のルータへの変更必要	○標準化技術 ×ルータでの RA 受信は非一般的	×ユーザルータへの変更必要	×ユーザルータへの実装は非一般的
経路表手動設定	×ユーザへの経路情報通知が別途必要 ○既存設備への変更不要	○既存実装への変更不要	×設定作業が煩雑(ツール利用により簡単化可能)	○ユーザルータでの実装は標準的
ポリシルーティング	○既存設備への変更不要	○標準技術との競合無し	×ユーザルータへのポリシ設定が必要 ×ユーザルータへの実装が必要 ×ユーザルータ自身からの通信には注意が必要	○高機能ルータでは既存実装多数 ×ユーザルータでの実装は非一般的

表 2.2-3 ユーザ端末における経路選択問題の解決手法の評価のまとめ

方式	xSP 視点	ベンダ視点	ユーザ視点	実装状況
ルーティングプロトコル	×xSP ルータへの(設定)変更が必要	○標準有り ○実装経験が豊富	×端末への変更必要	×端末での実装は非一般的 ○高機能ルータでは既存実装多数
RA (More Specific Routes)	×xSP ルータへの変更必要	○標準化技術	×端末への変更必要	×WindowsXP 以前は非対応
経路表手動設定	×ユーザへの経路情報通知が別途必要 ○既存設備への変更不要	○既存実装への変更不要	×設定作業が煩雑(ツール利用により簡単化可能)	○ユーザ端末での実装は標準的
ICMP リダイレクト	○対応の必要なし	○標準化技術	×適用環境が限られる(同一リンク＋経路情報交換) ×ユーザルータへの経路情報設定が必要	○実装は一般的

2.2.3 DNS サーバ選択問題に対する解決案

以下に DNS サーバ選択問題を解決するための方式について述べる。

・順次サーチ方式

複数の DNS サーバのリストを使用して、順番に DNS クエリ送出を行う方式である。ユーザ端末またはユーザルータへの実装で実現可能である。

非常にシンプルな実装となるが、名前解決に要する通信遅延が発生する可能性がある。遅延発生を抑制するために一斉に DNS クエリ送出することも可能であるが、ネットワークに対して不必要なトラフィックを送出する為、DNS サーバへの負荷が懸念される。

なお、もし複数の xSP の DNS サーバが、同じホスト名への DNS クエリに対してそれぞれ異なる IP アドレスを応答する場合、そのホスト名への通信の際にユーザの期待する通信経路が選択されない可能性がある点には注意が必要である。

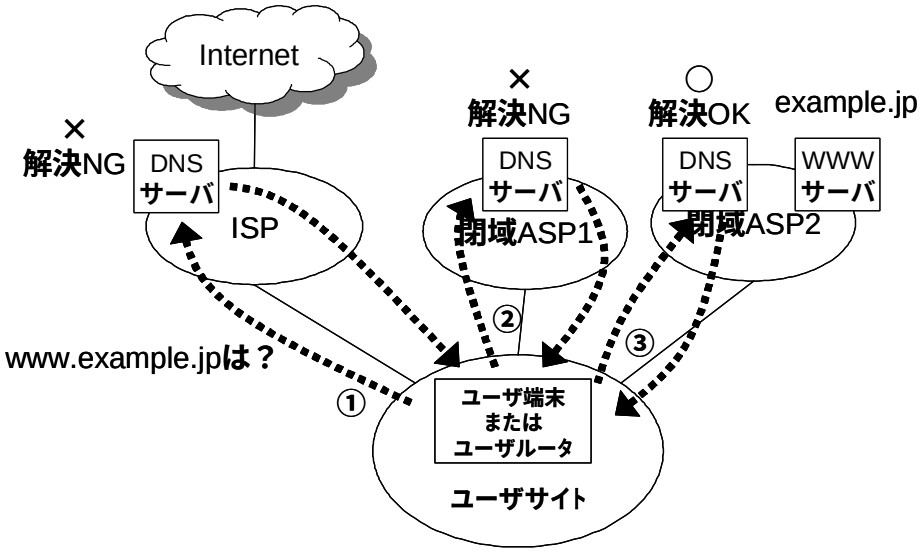


図 2.2-9 順次サーチ方式

[解説] 図 2.2-9 では、閉域 ASP2 内の DNS サーバが example.jp のドメイン管理を行っている。ユーザ端末またはユーザルータは www.example.jp との通信を行う為に、DNS サーバのリストから ISP→閉域 ASP1→閉域 ASP2 の DNS サーバの順で DNS クエリ送出を行うが、ISP や閉域 ASP1 の DNS サーバでは example.jp のドメイン管理を行っていない為、①や②では名前解決に失敗し、③の DNS クエリ送出でようやく名前解決が実現する。

・ドメイン識別方式

名前解決の対象となるドメイン名と DNS サーバの組を管理し、名前解決を行うドメイン名に応じて DNS サーバを選択する方式である。ユーザ端末またはユーザルータへの実装が必要であり、設定を自動化する場合には網設備への機能追加も必要となる。

本方式では、ドメイン名と DNS サーバの組をどのように取得するかが重要となるが、手動設定または DHCPv6 を使用した自動設定が想定される。手動設定については、ユーザに設定スキルを要求する点が大きな課題である。DHCPv6 における自動設定においては、RFC3646[5]の DNS Recursive Name Server Option と Domain Search List Option の適用が可能と考えられるが、どちらも本方式のような使用方法を意図して定義されていないことに注意が必要である。上記 Option を同時に受信して組として解釈するか、組を識別するためのフラグを定義する必要がある。尚、IPv4 のブロードバンドルータにおいては、手動設定の実装が多く存在している。

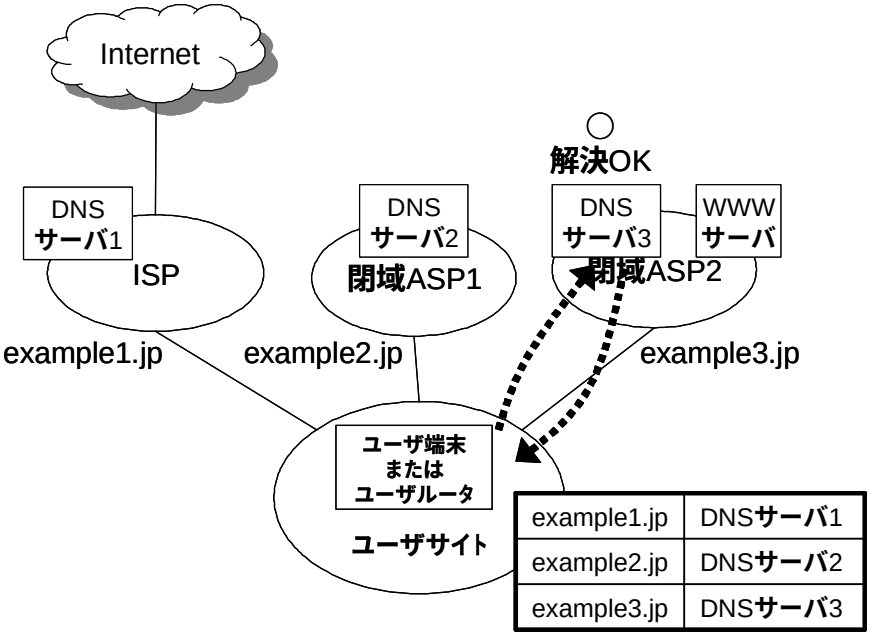


図 2.2-10 ドメイン識別方式

[解説] 図 2.2-10 では、DNS サーバ 1／2／3 は example1.jp／example2.jp／example3.jp のドメイン管理を行っている。ユーザ端末またはユーザルータは www.example3.jp との通信を行う為にドメイン名と DNS サーバの組を管理しているテーブル上から DNS サーバ 3 を選択し DNS クエリ送出を行い、名前解決が実現する。

[5] RFC 3646, DNS Configuration Option for DHCPv6

先に述べた DNS サーバ選択問題に対する解決案の評価を表 2.2-4 にまとめた。この表では、xSP 始点、ベンダ視点、ユーザ視点の 3 つの視点から評価を分類した。

表 2.2-4 DNS サーバ選択問題の解決手法の評価のまとめ

方式			xSP 視点	ベンダ視点	ユーザ視点	実装状況
ユーザ端末	順次サーチ		×不要なトラフィックの発生	×標準化されてない ○実装が容易	×通信遅延発生（一斉送信した場合は遅延なし） ×期待しない通信経路となる可能性あり	×実装なし
	ドメイン識別	手動設定	○対応の必要なし	×標準化されてない	×設定スキルを要求される	×実装なし
		自動設定 (DHCPv6)	×網設備への機能追加が必要	×標準化されてない	○対応の必要なし	×実装なし
ユーザルータ	順次サーチ		×不要なトラフィックの発生	×標準化されてない ○実装が容易	×通信遅延発生（一斉送信した場合は遅延なし） ×期待しない通信経路となる可能性あり	×実装なし ○IPv4 での実装は一般的
	ドメイン識別	手動設定	○対応の必要なし	×標準化されてない	×設定スキルを要求される	×実装なし ○IPv4 での実装は一般的
		自動設定 (DHCPv6)	×網設備への機能追加が必要	×標準化されてない	○対応の必要なし	×実装なし

3　ISP マルチホーム構成の課題検討

本節では ISP マルチホーム構成時のマルチプレフィックス環境の課題の整理、および、現在検討されている解決手法の紹介を行う。

3.1　課題

ISP マルチホーム構成では、ユーザサイトは複数の ISP と同時接続する。さらに、各 ISP はユーザサイトへそれぞれのプレフィックスを配布し、そのいずれもユーザサイト内でそのまま利用されるため、ユーザサイト内はマルチプレフィックス環境となる。

この際のユーザサイト内の IP 機器構成は、次の図 3.1-1 に示すシングルユーザルータ構成とマルチユーザルータ構成の 2 種類が想定される。なお、本文書では主な検討範囲をコンシューマのユーザサイトとするため、ユーザルータとユーザ端末の間にまた別のルータが置かれる構成は、考察の対象外とした。

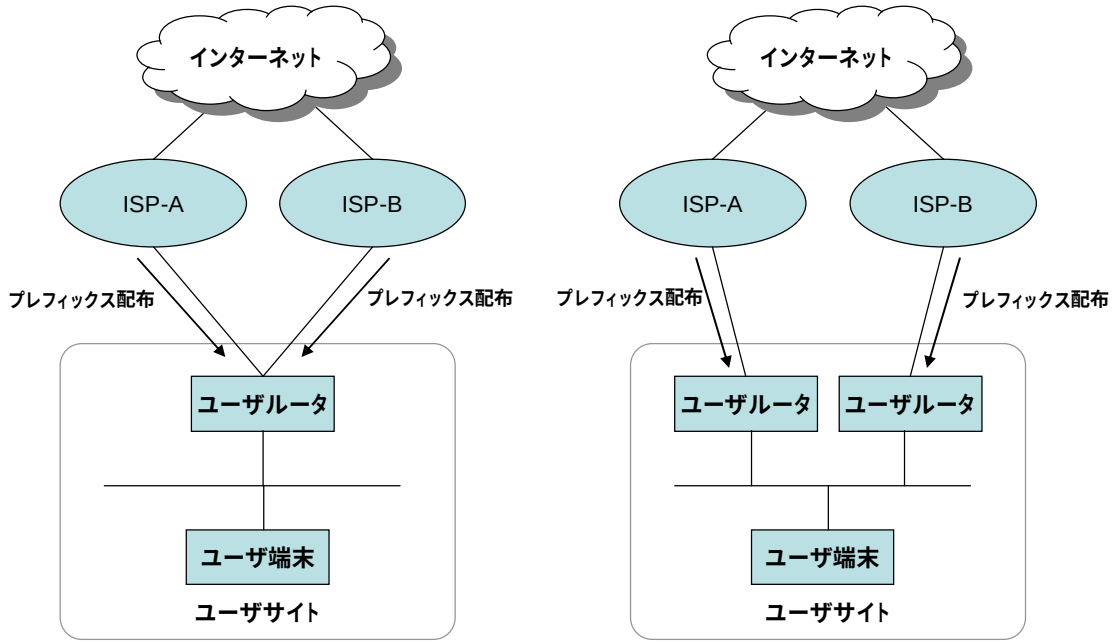


図 3.1-1 ISP マルチホーム構成時のユーザサイト内の IP 機器構成

このような構成のもと、ISP マルチホーム構成により発生するマルチプレフィックス環境には、主にパケット送信時の端末の経路選択問題と送信元アドレス選択問題の 2 つの課題がある。それぞれの課題を以下で整理する。

3.1.1　経路選択問題

ユーザ端末からの送信パケットの転送は、ISP マルチホームの利用目的に応じて、適切な

ISP を経由するように振り分けられることが求められる。この実現のためには、ユーザ端末からの送信パケットの転送途中で複数 ISP へと経路が分岐するポイントで実施されるネクストホップ選択が重要なポイントとなる。

これは、シングルユーザルータ構成では、ユーザサイト内のユーザルータのネクストホップ選択機能が該当する。また、マルチユーザルータ構成ではユーザサイト内の端末のネクストホップ選択機能が該当する。

ISP マルチホームの利用目的が、従来からあるインターネットへの通信路の冗長化、通信トラフィックの負荷分散、およびサービスに応じた ISP の使い分け等の場合は、各構成で目的に応じたネクストホップ選択機能が必要となる。ただし、これらの目的実現のためにパケット転送時の送信元アドレスの判定を積極的に行う場合以外は、基本的にはそれらの機能にマルチプレフィックス環境特有のものが必要なわけではない。

ユーザサイトからインターネットへの単純な通信到達性の確保の観点では、端末の送信元アドレス選択問題がネクストホップ選択の機能にも関係する。本件については、次節で述べる。

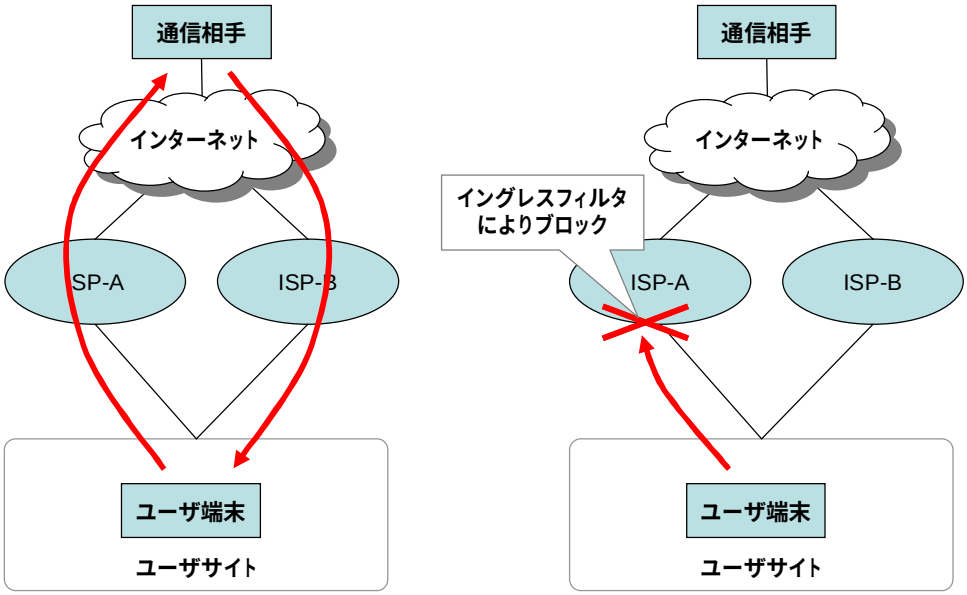
3.1.2 送信元アドレス選択問題

現在の IPv6 の標準仕様では、ユーザ端末の送信パケットの送信元アドレスとして、転送時に経由する ISP からのプレフィックスとは異なるものが選択される可能性がある。

まず、シングルユーザルータ構成の場合、ユーザ端末の送信パケットの転送先の ISP はユーザサイト内のユーザルータが選択する。その際、ユーザルータはパケットを送信元アドレスに応じた ISP 以外へ転送する可能性がある。これを回避するためには、ユーザルータがパケットの送信元アドレスに応じたネクストホップ選択を行うソースアドレスルーティングがあるが、現在のユーザルータ実装においてはそれほど一般的な機能ではない。

また、マルチユーザルータ構成の場合、端末はパケット送信時に不適切な組み合わせの送信元アドレスとネクストホップとしてのユーザルータを選択する可能性がある。これは、現在の IPv6 端末には自身の保持するプレフィックスとネクストホップとなるユーザルータとのマッチングルールを持つ機能が存在しないためである。

このようにユーザ端末の送信パケットの送信元アドレスに不適切なプレフィックスが選択された場合、次の図 3.1-2 に示す非対称経路による通信、または ISP のイングレスフィルタによる通信ブロックが発生する可能性がある。



非対称経路による通信　　**ISPのイングレスフィルタによる転送ブロック**

図 3.1-2 端末の送信元アドレス選択の誤りにより発生する問題

誤った送信元アドレスを選択したパケットが通信相手まで届いた場合、その通信相手は受信したパケットの送信元アドレスを送信先アドレスとしてパケットを生成して送信するため、非対称経路による通信が発生する。

また、ユーザ端末からの同様のパケットがイングレスフィルタを実施している ISP を経由しようとする場合、そのパケットはその ISP により途中で破棄される可能性がある。この場合は、ユーザサイト内の端末から通信相手への通信到達性が失われることになる。

3.2 IETF でのインターネットマルチホーム問題検討状況

インターネットマルチホームは昨今のIPv4インターネットの経路エントリ数増大の大きな原因である。従来 IPv6 では「階層的アドレッシングを用いた経路集約により、IPv4 のような経路エントリ数増大を防止できる」とされてきたが、2007 年からの PI アドレス配布開始（後述）により、この理論が成り立たなくなることが予測される。そのためオペレータコミュニティやベンダは、IETF に IPv4/v6 両方を考慮したマルチホーム問題解決方法の検討を強く期待している。

これを受けて、IETF では同課題解決のために 2006 年 10 月に RAW（IAB Workshop on Routing and Addressing）[6]を開催した。

RAW ではインターネットマルチホームに対する明確な解答は出なかったものの、問題点の洗い出しを行い今後の継続議論の方向性を定めた[7]。本節では RAW で指摘された課題を踏まえつつ、これまでに IETF で議論された解決案を簡単に紹介する。

IETF では前節で述べた課題のうち、送信元アドレス選択問題のみが課題とされている。経路選択問題については、ICMPv6 Redirect により解決済と見なされているためである。（ルータが ICMPv6 Redirect を送るためにはしかるべき経路制御設定が必要だが、インターネットマルチホームを行うようなネットワークならば通常そうした設定は行われているため）

- GSE （Global, Site and End-System Designator）[8]

1997 年に提案されたが、標準化完了に至らなかった提案である。

パケットがサイト外に入出力されるときにサイト境界ルータでパケット内の送信元アドレスのネットワーク ID 部（前半 64 ビットの一部=Routing Goop）を適切に書き換えることにより、送信元アドレス選択問題を解決する技術である（図 3.2-1 参照）。

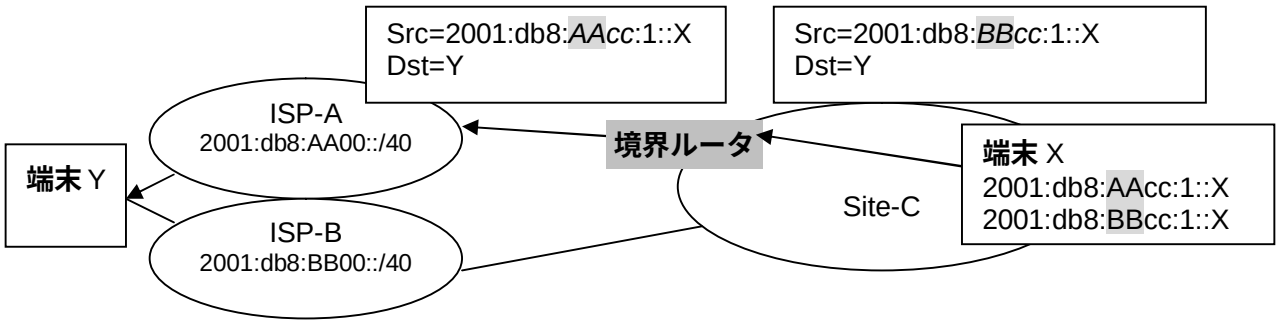


図 3.2-1 GSE の動作例

[6] http://www.iab.org/about/workshops/routingandaddressing/index.html
[7] draft-iab-raws-report-00.txt
[8] draft-ietf-ipngwg-gseaddr-00.txt (既に Expire 済)

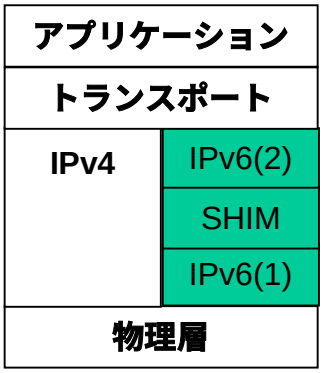
GSE は、NAT とは異なりサイト内のトポロジー情報を完全に隠さないものの、本質的に NAT と等価な技術である。そのため NAT と同様な技術課題を有する （e.g. ペイロード内に埋め込まれた IP アドレスの変換が困難、IPsec への対応）。

・ SHIM6[9]

2005 年から検討されている技術である。

端末の IP アドレスには、端末の識別子（Identifier）、端末の所属する場所の識別子（Locator）という 2 つの意味が重畳されている。SHIM6 はこの意味の重畳に注目し、両者の意味を明確に区別して IP アドレスを使い分けることにより、送信元アドレス選択問題を解決する技術である。

具体的には端末内 Layer3 の処理を IP 中継処理部と自宛処理部とに分解し、両者の間に SHIM 層を挟み込む。アプリケーション層は ULID（Upper-Layer ID, 実際には端末の IP アドレスのうちどれか適当なもの。Identifier 相当）を送信元アドレスとして用いて通信し、SHIM 層で ULID を適切な IP アドレス（Locator）に変換してネットワークへ出力する（図 3.2-2 参照）。



IPv6(2) = IP end-point sub-layer
- IPsec, Fragment, Destination Option処理

SHIM
- Locator/Identifier対応付け
- Locator/IdentifierのIPv6アドレス付替

IPv6(1) = IP routing sub-layer
- NDP, IPv6パケット送受信処理

図 3.2-2 IP パケットにおける SHIM6 の位置づけ

アプリケーション層には送信元アドレス選択の結果にかかわらず ULID が見えるため、NAT と同様な技術課題（e.g. ペイロード内の IP アドレスの変換が困難、IPsec への対応）を有さない。

しかしながら ULID と Locator の適切な対応付けがが SHIM6 の課題である。SHIM6 では Locator アドレスの疎通状況に基づき対応付けを決定するが、ISP 主導のトラフィックエンジニアリングを考えるとこの方法は非実用的、との批判もある[10]。

[9] draft-ietf-shim6-proto-07.txt
[10] http://www.nanog.org/mtg-0510/schiller.html

・　PI Address （Provider-Independent Address）

現在 IPv4 で行われているマルチホームと同様なインターネットマルチホーム実現方法である。

マルチホームしているサイトに RIR から上流 ISP とは独立なプレフィックス（Provider-Independent Address=PI Address）を割り当て、上流 ISP 間で同プレフィックスの経路制御を行う。この場合端末が有するアドレスは、グローバルアドレスとリンクローカルアドレスのみなので、サイト外への通信で送信元アドレス選択を誤ることはありえない。

こうした目的での PI Address 配布は既に 2006 年に ARIN で許可され[11]、2007 年 3 月には APNIC で許可された[12]他、RIPE[13]でも実施に向け検討が行われている（2007 年 4 月現在）。IPv4 インターネットマルチホーム技術をそのまま用いるだけなので適用は容易だが、経路エントリ数増大に伴うパケット中継装置の負荷（RIB エントリ用のメモリ量、FIB エントリ用の高速メモリ量、経路計算収束に要する CPU 負荷など）が課題である。

11 http://www.arin.net/policy/proposals/2005_1.html
12 http://www.apnic.org/docs/policy/ipv6-address-policy.html
13 http://www.ripe.net/ripe/policies/proposals/2006-01.html

4　セキュリティ考察

本章では、マルチプレフィックス環境に特有のセキュリティ上の注意事項について、考察を行う。

4.1　想定されるセキュリティリスク

・ネットワーク複雑化によるユーザの設定ミス・操作ミスの誘発

「2005 年 IPv6 移行ガイドラインセキュリティ編」[14]でも指摘されているように、マルチプレフィックス環境では複数の IPv6 アドレスプレフィックスを取り扱うため、シングルプレフィックス環境に比べて、ユーザサイトのネットワーク構成や端末の通信制御・セキュリティ設定が複雑で難しいものとなり、ユーザの設定ミスや操作ミスを誘発する可能性が高くなる。設定ミス・操作ミスの結果、端末にセキュリティホールが生じると、各種の不正アクセス攻撃（不正経路情報注入、パケット盗聴、改ざん、侵入・攻撃準備、セッションジャック、DoS 攻撃）の被害にあう恐れがある。

2 章・3 章の送信元アドレス選択問題に対する解決案の中では、ポリシテーブル配布（手動設定）と VLAN（論理 NW 分割）、経路選択問題に対する解決案の中では、経路表手動設定とポリシルーティングの方式で、ユーザの手動設定を必要とするため、新たな設定ミスが生じる可能性がある。また、ポート分割方式（物理 NW 分割）でのポートの挿し間違いによる端末とプレフィックスの対応付けの誤りも考えられる。これらによって、通信障害が生じたり、目的とは異なるネットワークにつながったりしてしまうと、セキュリティリスクが増加する。

・他のネットワークへのセキュリティ被害の拡大

複数のサービスネットワークを利用している端末が、不正アクセスやウイルスによる攻撃で乗っ取られたり踏み台にされたりした場合に、セキュリティ被害が他のサービスネットワークに拡大してしまうことが懸念される。

これは 2 章・3 章で列挙したどの解決方式にも限らず起こりうる。ただし、ポート分割方式では、端末の 1 インターフェースごとに 1 サービスネットワークを利用することとしているため、端末が 2 つ以上のインターフェースを利用している場合や、1 つのインターフェースの接続ポートをサービスネットワークごとに挿し替えて利用する場合のリスクとなる。

・保持する複数のプレフィックスアドレスの特定

複数のプレフィックスアドレスを保持する端末が送信元アドレス選択を誤った場合、通信障害が生じるだけでなく、選択した他のプレフィックスアドレスが別のサービスネットワーク上の端末に漏れ、加入サービスの特定などプライバシーを探られる可能性がある。

送信元アドレス選択の機構が適切に実装できている場合には、パケット送信時のアドレ

[14] http://www.v6pc.jp/pdf/ja-09-v6trans-security-050722.pdf

ス選択誤りによる保持アドレス群の漏れは防ぐことができる（ポート分割方式、PI Address の方式に関しては端末がグローバルアドレスを一つしか持たないため、そもそもこのリスクはあてはまらない）。

しかし、送信元アドレス選択の実装およびポリシの設定などが不十分である場合、RFC3484[15]では、攻撃元がターゲットにわざとアドレス選択を実行させるようなパケットを送り、その応答によってターゲットが保持するアドレス群を把握・関連付けすることができれば、加入サービスの特定などプライバシーを探られる可能性があるとの指摘がされている。一般的にユニキャストでは、宛先として送られてきたアドレスを自身の送信元アドレスとして応答するため、このような攻撃へのリスクは低いと思われるが、エニキャストやマルチキャストによるパケットや、OS の送信元アドレス選択の機構に依存せず独自にアドレス選択を行うようなアプリケーションへのパケットによって、この種の攻撃が実行される可能性はある。

・リダイレクト攻撃

ISP マルチホーム構成におけるセキュリティリスク（RFC4218[16]）として、3 章で述べた SHIM6 などで通信を行っている場合に、Locator アドレスと Identifier アドレスのマッピング誤りや偽装による第三者へのリダイレクトによって、パケット盗聴やセッションジャックといった攻撃にさらされる恐れがある。

4.2 必要と思われる対策案

先で述べた各種のセキュリティリスクにはまだ顕在化していないものや、あくまで可能性としての見解も含まれているが、今後マルチプレフィックス環境をユーザに安全に提供していくためには、ネットワーク提供側・端末提供側にて以下のような対策の実現が望まれる。

・ネットワーク管理、端末管理におけるユーザへのサポート

マルチプレフィックス環境ではシングルプレフィックス環境に比べて、ユーザの利用する IP アドレスが増え、ネットワーク構成やセキュリティ設定項目の複雑化が予想されるため、各端末とプレフィックスの対応付けの把握や、ユーザサイト出口のユーザルータで送信元アドレスによるフィルタを実施するなど、従来以上に統合的・網羅的なネットワーク管理、端末管理が必要となってくる。

しかし、ユーザへの作業負担はできる限り小さくなることが望ましく、ネットワーク側で接続端末の認証やセキュリティの管理といった対処の実施、端末側でセキュリティなど

[15] RFC3484, Default Address Selection for Internet Protocol version 6 (IPv6)
[16] RFC4218, Threats to IPv6 Multihoming Solutions

の設定の簡便化や設定誤りの検出といったユーザをサポートする機能の実装が行われるとよい。

・マルチプレフィックス環境におけるアプリケーションの評価

特に高いセキュリティが求められるアプリケーションでは、送信元アドレス選択の動作をはじめとして、あらかじめマルチプレフィックス環境下での動作を十分に評価しておくことが望ましい。

・ISP マルチホーム環境の SHIM6 におけるリダイレクト攻撃への対策

3 章でも述べられているように ISP マルチホーム構成における SHIM6 の通信では、Identifier アドレス（ULID）と Locator アドレスの適切な対応付けが課題であり、対応付けの誤りやアドレスの偽装によるリダイレクト攻撃を防ぐためのセキュアな機構が必要となる。SHIM6 にはハッシュを用いてアドレス情報を安全に交換する HBA（Hash Based Addresses）というセッションジャック防止の機能が試みられているが、現時点では、プロトコル仕様の標準化が進行中の段階である。

本章で挙げたセキュリティリスクのほかにも、マルチプレフィックス環境になることによって、これまでに想定していない新しいタイプの攻撃が登場する可能性があり、各種最新動向には常に注意しておきたい。

5　マルチプレフィックス環境の事例紹介

5.1　MPMH（Multi-prefix Multi-home）

5.1.1　背景

ブロードバンド環境とユビキタスネットワーク環境の急速な普及によりインターネットの利用シーンも多様化し、またインターネットを介したサービス提供事業者により多数のサービスが提供され始めている。

このような背景の中、NTT 東日本のように IPv6 の利用拡大を狙いとし、IPv6 普及期に於いて、これまでインターネット接続事業者経由で提供してきた ASP サービスとは異なる、同時接続性や独立性など ASP 個々の自由度やユーザ利便性の向上を図る新たなサービスモデルの可能性について検討を行う通信事業者も現れている。

MPMH モデルは IP 技術の応用で、オープンなインターネット接続による ISP 経由の ASP サービスに加え、サービス提供のための IP アドレス空間を閉域 ASP が直接割り当てを受けてエンドユーザに対してダイレクトに複数同時に異なる閉域 ASP サービスを提供することを想定し、1 つのプレフィックス単位に論理的にクローズドネットワークグループを構成し、基盤網上に複数のサービス空間をオーバーレイすることで構成・制御するネットワーク環境の総称であり、IPv6 の本格的普及時代のサービスの１つとしてモデル化したものである。

5.1.2　MPMH モデルの考え方

ユーザサイトにおけるネットワーク環境に求められる要件として、

- 多種多様な機器が多数接続してきても混乱を生じないネットワーク
- 機器群毎に適切なサービス事業者と接続でき、所望のサービスを受けることが出来る
- 性質の異なるネットワークを同時に利用可能で、各々必要なセキュリティや品質等を確保出来るネットワーク

これらを満たすモデル環境として以下のようなモデル環境を定義した。

- マルチプレフィックス（MP）：ユーザサイト内に複数のネットワークが存在
- マルチホーム（MH）：ユーザサイトから同時に複数の接続先（閉域 ASP）に接続

5.1.3　MPMH モデル環境の概要

- ユーザサイト内でマルチプレフィックス環境をサポート
- ユーザダイレクトなマルチサービスを提供（複数の事業者拠点を同時に接続）

・ サービス毎にポリシを設定（セキュリティ、QoS 等）
・ オープン・プラットホーム（特定の ASP に非依存であり、NW インフラを持たない仮想サービス事業者に対応）
※図 5.1-1 参照

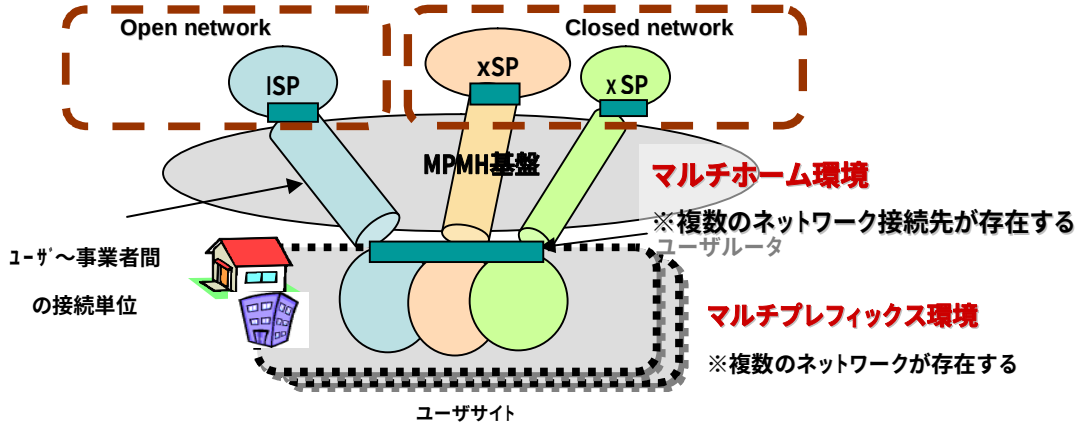


図 5.1-1 MPMH モデル（単一 ISP と複数閉域 ASP 構成の場合）

MPMH モデルにおける IPv6 利用のメリット

・ IPv4 に比べより多くの組織・事業者、ユーザがアドレスを豊富に利用できる
  ✓ 拠点毎の複数ネットワークへの対応
  ✓ 独自の IPv6 アドレスを持つサービス提供事業者が直接ユーザに対しプレフィックスを配布しサービス提供が可能
  ✓ 異なる複数の組織・事業者が提供するサービスを同時に利用可能
・ IPv6 では QoS や IPsec などの機能が標準装備してある
  ✓ IP で繋がるすべての機器に対して優先制御やセキュリティの確保が可能であり、ネットワーク毎にポリシ制御が容易
・ IPv6 ではプラグアンドプレイでネットワークに簡単に接続できる
  ✓ PC 以外の機器でも比較的容易にネットワークへ接続が可能

5.1.4 MPMH モデルの構成例

MPMH を構成する実現機能として、以下の 3 つの機能をネットワークに配備し実証を行った（図 5.1-2）。

・ トンネリング機構
  ✓ ユーザサイト内のネットワークとサービスネットワークの両空間を GRE 等の

トンネル技術を利用して仮想的に結合

- マルチホーム機構
  - ✓ ユーザサイトからサービスネットワーク空間毎にパケットを振り分け転送
- サービスネットワーク配布機構
  - ✓ ユーザサイト内のネットワークに対して自サービスネットワーク空間の一部を割り当てる

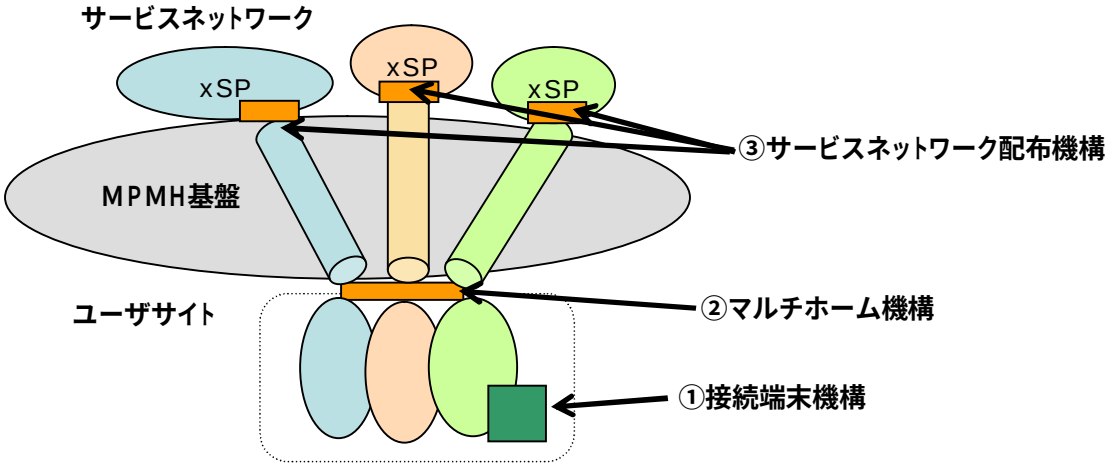


図 5.1-2 MPMH 実現機能

なお、この MPMH モデルは平成 16 年度及び平成 17 年度の総務省 IPv6 移行実証実験を通じて技術的確認とフィールドにおける有効性の確認を行っている。

5.1.5 MPMH の適用分野

MPMH の適用分野として以下が考えられる。

① 家庭内ネットワーク（図 5.1-3）
② ビル設備管理・制御（図 5.1-4）
③ エリア管理・制御（図 5.1-5）

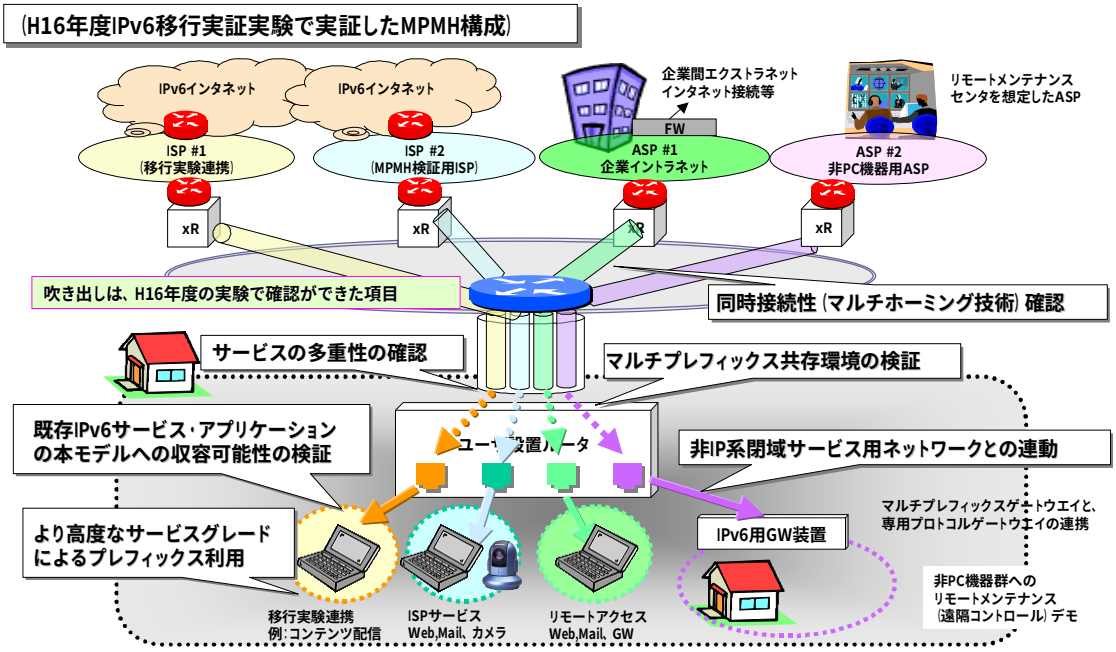


図 5.1-3 ①家庭内ネットワークへの応用

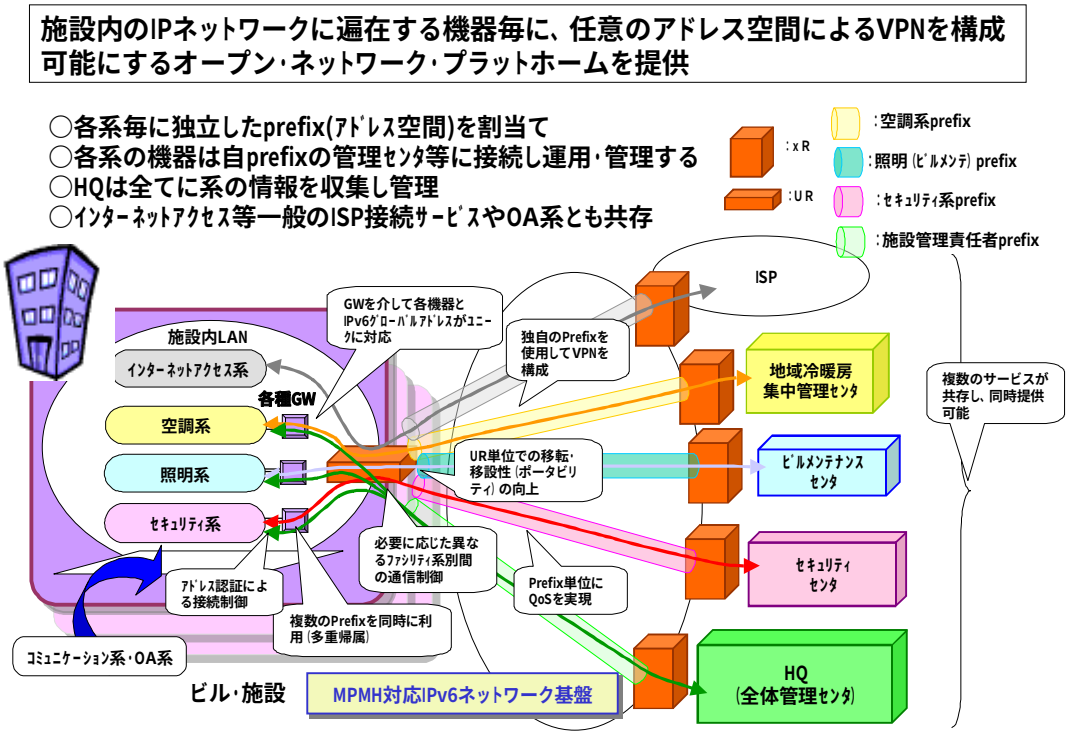


図 5.1-4 ②ビル施設管理・制御への応用

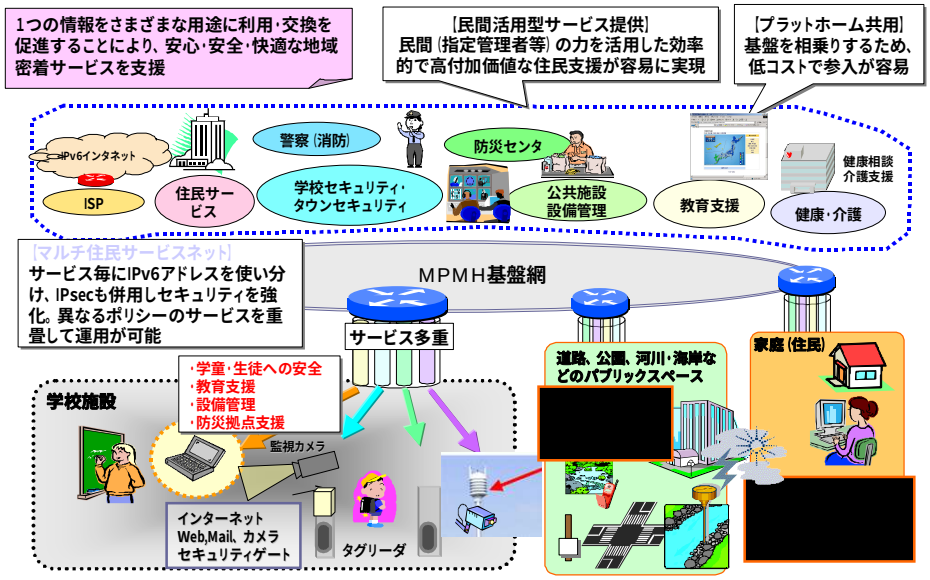


図 5.1-5 ③安心・安全住民サポート基盤ネットワークへの応用

5.1.6 MPMH モデル適用に際しての課題と今後の展開

マルチプレフィックス環境を利用した MPMH モデルでは、3 章で既に示されている課題に対し、その課題を解決もしくは実現環境において影響を及ぼさないように配慮を行う必要があるが、現状は以下の条件の下で適用検討を行っている。

- 1ISP＋複数閉域 ASP もしくは、複数閉域 ASP モデルに限定
- 個々の閉域 ASP が払い出すプレフィックスは空間的に互いに充分離れており、送信元アドレス選択機構利用時の選択誤りが発生しないよう設計段階での配慮を行う。
- センサノードのような非インテリジェント端末の接続においてはプレフィックス混在を回避するために、ユーザサイト内のネットワークに複数物理ポートを用意してプレフィックス毎の物理的なネットワークの分離を実施する、あるいは MAC アドレス等の情報を利用した機器選択を行う等の手当てを行う。

MPMH モデルの適用について、現状では別章で示される課題を回避するために幾つかの制約条件の下に置かれているものの、そのメリットを享受できる適用シーンは多数存在すると考えられる。

また、MPMH モデルのようにマルチサービスに関わる機能をネットワーク層である IP 層で実現することで以下の示す効果も将来的には期待できる。

- **IP 層に集約することで、設計・管理・運用の負荷低減**
- **IP 層に集約することで、他のレイヤの機能と共存や棲み分けが比較的容易になり、より高度なサービスが提供可能**
- **転送に係る細かな制御や高度な制御が容易に実現可能**
- **サービス事業者とネットワーク事業者が共に関与できる IP 層で観測・制御可能なオーバーレイ・ネットワークが構成可能**

5.2 コンシューマ向け IPv6 接続サービスの同時利用

コンシューマユーザが、2 つの異なる事業者が提供する IPv6 ネットワークサービスを利用する際にマルチプレフィックスに起因する課題の発生事例について解説する。はじめにモデルを使った説明を行い、次に実機による動作例をつける。

5.2.1 マルチプレフィックスに起因する問題事例

マルチプレフィックスの典型的な事例を取り挙げ、どのように問題が生じるかを説明する。

・ 終端端末の状況

端末は、市中製品として普及している OS のもつ IPv6 の機能を、特別な設定なしに利用していることを前提とする。つまり、本文の「2.2 解決手法」で示されたような、RA の More Specific Route やポリシテーブル、端末でのダイナミックルーティングを利用していない。

・ ネットワーク環境

現在、IPv6 接続を提供するコンシューマユーザ向けサービスとしては、以下の 2 種類の形態のサービスが同時利用可能である。

- アクセス回線に付帯して提供される IPv6 閉域網サービス
- トンネル技術を利用した IPv6 インターネットサービス

IPv6 閉域網サービスと、IPv6 インターネットサービスは、それぞれ別の事業者からそれぞれが別の IPv6 プレフィックスで、それぞれ異なるルータから提供される。また、インターネット IPv6 サービスについてはトンネル技術を利用しているため、ブロードバンドルータではなく、ユーザが所有する PC で終端機能が提供される場合がある。ここでは、いずれの場合も、IPv6 としては“ルータ”機能と位置付けられるため、ルータと呼ぶ。このとき、ルータ間での経路情報の交換や互いに経路制御を行うような設定は行われない。
ユーザのネットワーク構成を図 5.2-1 のように想定する。R1 と R2 はそれぞれのネットワークへの接続を提供し、両方のルータが RA（Router Advertise）で、端末が利用するプレフィックスを通知する。

この例は、R1 から IPv6 ISP-X のプレフィックスである 2001:db8:1::/64 が、R2 から IPv6 閉域 ASP-Y のプレフィックスである 2001:db8:2::/64 というプレフィックスが通知されるものとする。また、ルータ R1、R2 はそれぞれ別の事業者から機能提供されているため、R1、R2 間で経路情報の交換や設定などをおこなっていない。

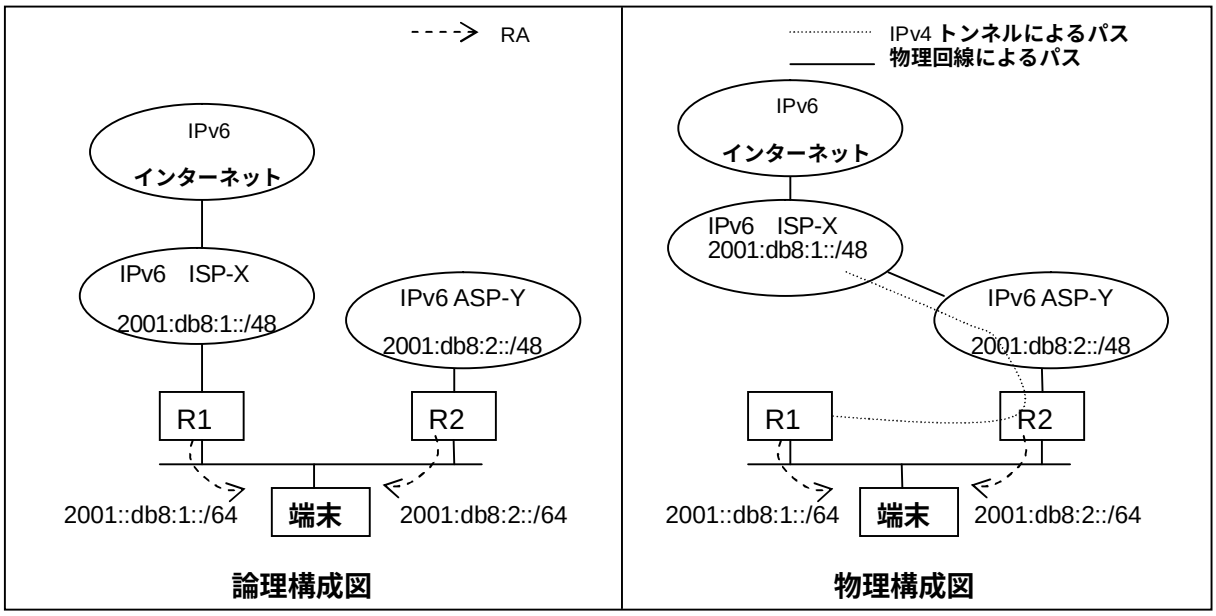


図 5.2-1 ネットワーク構成

・ 端末の動作

端末は、R1 **と** R2 **それぞれからプレフィックス情報つきの** RA **を受けとり、以下のような状態になる。**

A) **インターフェースに** 2 **種類のプレフィックスを付与される**

インターフェースには 2001:db8:1::/64 **と** 2001:db8:2::/64 **という** 2 **種類のプレフィックスが付与される。パケット送信時には、**2 **つのプレフィックスのうちいずれかを始点プレフィックスとして選択する。始点プレフィックスは終点アドレスのプレフィックスとのロンゲストマッチアルゴリズムにより決められるため、送信パケットの終点アドレスに応じたプレフィックス選択を行うことになる。**

B) **デフォルトルートのネクストホップとして** R1 **と** R2 **を学習**

ネクストホップの異なる２つのデフォルトルート（::/0**）を学習する。ただし、パケット送信時に利用されるのは片方のデフォルトルートのみである。広告された** RA **に含まれる優先度情報に差があれば優先度の高い** RA **で学習したデフォルトルートを常にネクストホップとして選択する。**RA **の優先度に差がない場合には、任意の方法でいずれかのデフォルトルートを選択する。このとき、送信パケットの送信先アドレスに応じてデフォルトルートを変更するといった処理は行われない。**

ここで注目すべきは、A) **始点プレフィックスの選択と、**B) **ネクストホップの選択には相関関係がないということである。パケットの終点アドレスとしてどちらを選択したとしても、パケットは特定のルータを常に経由し、始点プレフィックスに応じた切り替えがな**

いため、パケットが始点プレフィックスを RA として広告したルータを必ずしも経由するとは限らない。

・ 送信先アドレスによる 2 つの事例

送信元アドレスと、ネクストホップルータ選択の組み合わせによる通信への影響を、端末の通信相手が ISP-X もしくは閉域 ASP-Y 内の場合と、ISP-X や閉域 ASP-Y 以外のネットワークに属する場合の 2 つのケースに分けて説明する。

- ケース 1：ISP-X 内の端末と通信する場合

  ISP-X 内の 2001:db8:1:0:1::/64 というプレフィックスをもつ端末へパケットを送信する場合、以下のようになる。

1. 送信元アドレス選択

   ロンゲストマッチアルゴリズムにより、インターフェースに付与された 2 つのプレフィックスのうち、2001:db8:1:0:1::/64 と先頭ビットからの一致部分の長い 2001:db8:1::/64 を始点プレフィックスとして選択する。

2. ネクストホップ選択

   ネクストホップの異なる 2 つのデフォルトルート（::/0）を学習する。ただし、パケット送信時に利用されるのは片方のデフォルトルートのみである。広告された RA に含まれる優先度情報に差があれば優先度の高い RA によるデフォルトルートを、RA の優先度に差がない場合には、任意の方法でいずれかのデフォルトルートを選択する。

このケースでは送信元アドレスは適切に選択されるが、ネクストホップについては ISP-X 側が選択されない場合もあるため、ルータ R2 を選択した場合、R2 から閉域 ASP-Y へ送られたパケットは ISP-X 内へ到達できないため通信が失敗する。通信の成功を○、失敗を×として、送信元アドレス選択とネクストホップ選択との関係を表 5.2-1 にまとめる。

表 5.2-1 ケース 2 での通信の可否

ネクストホップ選択 / 送信元アドレス選択	R1 (ISP-X)	R2 (閉域 ASP-Y)
2001:db8:1::/64 (ISP-X)	○	×

逆に、閉域 ASP-Y 内の端末に通信を行う場合についても、ISP-X 内の端末との通信の場合と同様な組み合わせで通信の成功、失敗が決まる。

- ケース 2：ISP-X、閉域 ASP-Y 以外のインターネット上の端末との通信の場合

ISP-X 以外の IPv6 インターネット上にあり、2001:db8:8000::/64　というプレフィックスをもつ端末との通信する場合、以下の状態になる。

1. 送信元アドレス選択
   宛先プレフィックス 2001:db8:8000::/64 は、端末のもつ 2 つのプレフィックス（2001:db8:1::/64, 2001:db8:2::/64）と先頭ビットからの一致するビット長が同じであるため、ロンゲストマッチアルゴリズムによりどちらかに決めることができず、任意の方法でそのいずれかが選択されることになる。
2. ネクストホップ選択
   ネクストホップの異なる 2 つのデフォルトルート（::/0）を学習する。ただし、パケット送信時に利用されるのは片方のデフォルトルートのみである。広告された RA に含まれる優先度情報に差があれば優先度の高い RA によるデフォルトルートを、RA の優先度に差がない場合には、任意の方法でいずれかのデフォルトルートを選択する。

送信元アドレスとして、閉域網である閉域 ASP-Y のプレフィックス 2001:db8:2::/64 を選択した場合、通信相手がインターネット上にあるため、応答パケットが届かなくなる。また、ケース 1 と同様ネクストホップ選択については、通信が成功または失敗となる。通信の成功を○、失敗を×として、送信元アドレス選択とネクストホップ選択との関係を表 5.2-2 にまとめる。

表 5.2-2　ケース 2 での通信の可否

ネクストホップ選択 / 送信元アドレス選択	R1 (ISP-X)	R2 (閉域 ASP-Y)
2001:db8:1::/64 (ISP-X)	○	×
2001:db8:2::/64 (閉域 ASP-Y)	×	×

表 5.2-2 の通り、送信元アドレス選択とネクストホップ選択の両方が正しく行われないかぎり、通信が成功しない。

5.2.2 実機での動作例

実際に図 5.2-1 のようなマルチプレフィックス状態を構成した動作例を示す。ISP-X 側から RA で広告されるプレフィックスを 2001:db8:1::/64、閉域 ASP-Y 側から広告されるプレフィックスを 2001:db8:2::/64 に置き換えて結果を表示する。

```
C:¥>ipconfig
Windows IP Configuration
Ethernet adapter ローカルエリア接続:
        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.102
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        IP Address. . . . . . . . . . . . : 2001:db8:2::20e:a6ff:fe24:6d81    ←“閉域 ASP-Y 側ルータ(R2)”
        IP Address. . . . . . . . . . . . : 2001:db8:1::20e:a6ff:fe24:6d81    ←“ISP-X 側ルータ(R1)”
        IP Address. . . . . . . . . . . . : fe80::20e:a6ff:fe24:6d81%4
        Default Gateway . . . . . . . . . : 192.168.1.1
                                            fe80::20b:45ff:feed:5ca8%4
                                            fe80::202:2dff:fe70:a7e2%4
```

このとき端末のもつルーティングテーブルは以下のように 2 つのデフォルト経路（::/0）を持つ。この事例では、ISP-X 側からの RA の preference が高く設定されているため常に優先される。

```
C:¥>ipv6 rt
2001:db8:2::/64 -> 4 pref 8 life 29d23h59m56s (autoconf)
::/0 -> 4/fe80::20b:45ff:feed:5ca8 pref 256 life 29m56s (autoconf)      ←“閉域 ASP-Y 側(R2）”
2001:db8:1::/64 -> 4 pref 8 life 2m55s (autoconf)
::/0 -> 4/fe80::202:2dff:fe70:a7e2 pref 16 life 69s (autoconf)          ←“ISP-X 側(R1)”
```

・ 閉域 ASP-Y 内の端末への通信で適切なネクストホップが選択されなかった事例

この状態では、ISP-X 側（R1）を常にネクストホップとして選択するため、この端末から送信されるパケットは常に R1 側（ISP-X）へ送られ、閉域 ASP-Y 内への通信は常に失敗する。実際に、閉域 ASP-Y 内の端末 2001:db8:2:0:1::1 に向けた通信確認の結果は以下の通り失敗した。

```
C:¥>tracert foo.net

Tracing route to foo.net [2001:db8:2:1::1]

over a maximum of 30 hops:


  1     *        *        *     Request timed out.

  2     *        *        *     Request timed out.

  3     *        *        *     Request timed out.
```

- **ISP-X、閉域 ASP-Y 以外のインターネット上の端末との通信事例**

  送信先がインターネットにある場合には、ネクストホップ選択として ISP-X が選択されているため、パケット送信時は成功する。しかし、送信元アドレス選択で、ISP-X ではなく閉域 ASP-Y 側のプレフィックスを選択する場合は、戻りパケットが IPv6 インターネットから閉域 ASP-Y に到達できないため、失敗となる。

- **適切な送信元アドレスが選択された場合（ISP-X からのプレフィックスを選択）**

  この例では、送信元アドレスとして 2001:db8:1::/64 が選択されたため[17]、IPv6 インターネット経由での通信が成功している。

```
C:¥> ping www.v6pc.jp


Pinging www.v6pc.jp [2001:218:2001:3000::11] with 32 bytes of data:


Reply from 2001:218:2001:3000::11: time=23ms

Reply from 2001:218:2001:3000::11: time=23ms

Reply from 2001:218:2001:3000::11: time=23ms


Ping statistics for 2001:218:2001:3000::11:

    Packets: Sent = 23, Received = 23, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

    Minimum = 23ms, Maximum = 23ms, Average = 23ms
```

[17] **ここでは実際のプレフィックスを 2001:db8:1 に置き換えているが、実際には宛先プレフィックス (2001:218:2001:3000::/64) とのロンゲストマッチにより選択された。**

- **適切な送信元アドレスが選択されなかった場合（閉域 ASP-Y からのプレフィックスを選択）**

  この例では、送信元アドレスとして 2001:db8:2::/64 が選択されたため[18]、IPv6 インターネット側からの戻りのパケットが到達できず、通信が失敗となった。

```
C:¥>tracert www.apnic.net

Tracing route to www.apnic.net [2001:dc0:2001:0:4608:20::]
over a maximum of 30 hops:

  1     *        *        *     Request timed out.
  2     *        *        *     Request timed out.
  3     *        *        *     Request timed out.
  4     *        *        *     Request timed out.
```

5.2.3 マルチプレフィックスに起因する課題の回避策

ケース 1、ケース 2 についての解決方法としては、3 章にいくつかの方法が示されている。ただし、端末やルータの機能に手を加えられないという条件の下では、図 5.2-2 のように、2 つの IPv6 ネットワークへ接続ごとにセグメントを分離する、という方法が現実的であり、すぐに実行できる方法である。

[18] **ここでは実際のプレフィックスを 2001:db8:2 に置き換えているが、実際にはあて先プレフィックス（2001:dc0:2001:0::/64）とのロンゲストマッチにより、2001:db8:2::/64 が選択された。**

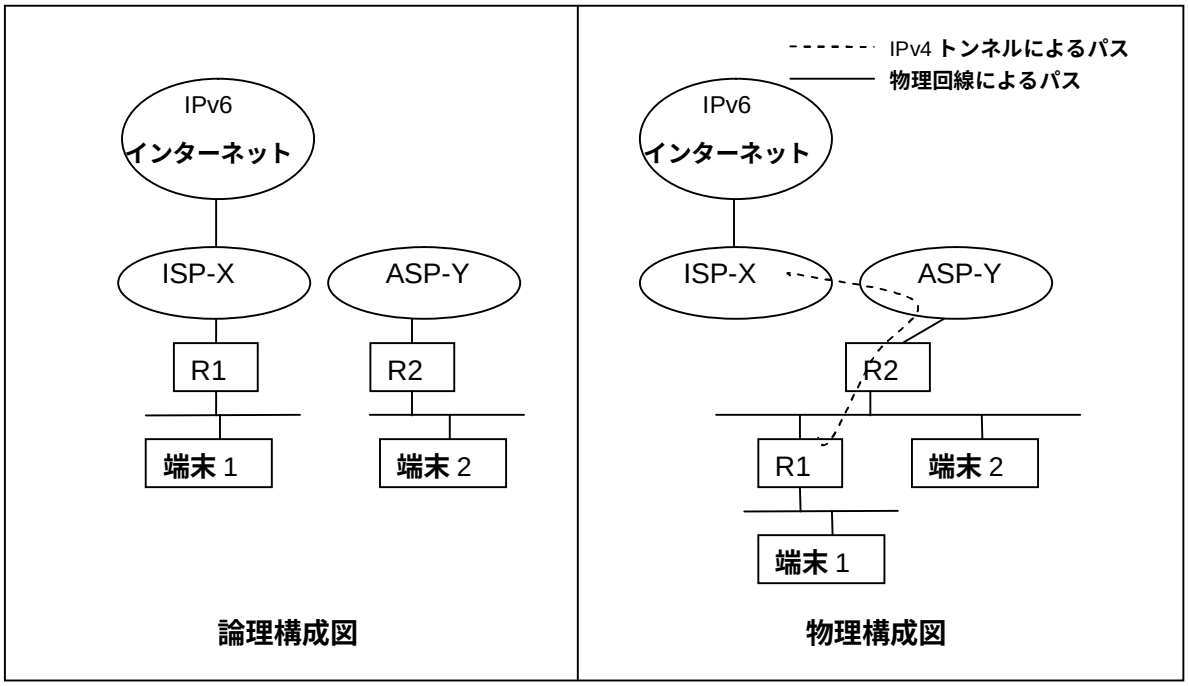


図 5.2-2 セグメントを分離する問題

この場合、利用目的に応じて端末を端末 1 の位置または端末 2 の位置に接続や、それぞれ別の端末を準備するといった対応が必要となるため、ユーザにとって設定が煩雑になるという欠点がある。しかし、確実に問題を回避できるという意味では、現実的な方法であるといえる。

6　まとめ

6.1　今回の活動では検討しきれなかった事項

今回の活動において、マルチプレフィックス環境の課題として挙げられたものの、検討しきれなかった事項について以下にまとめる。

- 単一 ISP と複数閉域 ASP 構成において検討しきれなかった事項（本文 2.1.4 節参照）
  - DNS ドメインサフィックスの選択問題
  - Web プロキシの選択問題

実際の IPv6 サービスの構築にあたってはこれらの問題に対する検討も必要である。

6.2　おわりに

現在、既に複数のコンシューマ向けの IPv6 サービスが提供されており、ユーザがこれらのサービスを複数利用する際には、それぞれが適切に利用できることが望まれる。

しかし、その際にユーザサイトがマルチプレフィックス環境となる場合、いくつかの課題が残されており、そのうちの主要なものは、ユーザ端末、およびユーザルータの挙動に関するものである。そのため、本文書ではユーザサイト内の既存の機器実装に対して現在適用可能な解決手法と、IETF で標準化の提案段階にある解決手法の両方について述べた。

現在適用可能な解決手法は、今すぐ適用できる反面、利用者に専門的な知識と端末への煩雑な設定作業を要求する傾向がある。これは、端末実装ごとに設定簡易化ツールを用意することなどで軽減可能であり、特定の IPv6 サービス、および特定の端末実装を対象として課題解決を行うことには有効である。

本文書ではマルチプレフィックス環境の構築に関する現状の課題と整理、セキュリティの考察、および、いくつかの事例紹介を行った。本文書が、今後の IPv6 サービスの環境の構築に関わる方々の一助となれば幸いである。

付録

Ⅰ. 参考文献

本文書に掲載した参考文献を次の表にまとめる。

表（付録-Ⅰ） 参考文献

本文中の関係箇所	参考文献
送信元アドレス選択問題に対する解決案（2.2.1 節）	RFC 3484, “Default Address Selection for Internet Protocol version 6 (IPv6)”
	Internet-Draft, “Distributing Default Address Selection Policy using DHCPv6”, draft-fujisaki-dhc-addr-select-opt-03.txt
	RFC 4193, “Unique Local IPv6 Unicast Addresses”
	Shim6 WG http://www.ietf.org/html.charters/shim6-charter.html
経路選択問題に対する解決案（2.2.2 節）	RFC 4191, “Default Router Preferences and More-Specific Routes ”
DNS サーバ選択問題に対する解決案（2.1.3 節）	RFC 3646, “DNS Configuration Options for DHCPv6”
IETF でのインターネットマルチホーム問題検討状況（3.2 節）	RAW (IAB Workshop on Routing and Addressing) http://www.iab.org/about/workshops/routingandaddressing/index.html ・RAW report: draft-iab-raws-report-00.txt
	Internet-Draft, “GSE – An Alternate Addressing Architecture for IPv6”, draft-ietf-ipngwg-gseaddr-00.txt (既に Expire 済)
	SHIM6 WG Internet-Draft, “Level 3 multihoming shim protocol”, draft-ietf-shim6-proto-07.txt
	Shim6: Network Operator Concerns http://www.nanog.org/mtg-0510/schiller.html
	RIR の PI(Provider-Independent)アドレス割り当てポリシ ・ARIN http://www.arin.net/policy/proposals/2005_1.html ・APNIC http://www.apnic.org/meetings/22/archive/minutes/policy.html ・RIPE NCC http://www.ripe.net/ripe/policies/proposals/2006-01.html
想定されるセキュリティリスク（4.1 節）	2005 年 IPv6 移行ガイドラインセキュリティ編 http://www.v6pc.jp/pdf/ja-09-v6trans-security-050722.pdf

本文中の関係箇所	参考文献
必要と思われる対策案（4.2 節）	RFC 3484, “Default Address Selection for Internet Protocol version 6 (IPv6)”
	RFC 4218, Threats to IPv6 Multihoming Solutions”

Ⅱ. 標準機能の実装状況

本文中で取り上げた課題解決手法のうち、標準化されている主要なものの実装状況の調査を行った。調査は、機能が実装されていることまでを確認し、動作検証までは実施していない。結果を次の表にまとめる。

表（付録-Ⅱ） 標準機能の実装状況（2007 年 4 月現在）

標準機能	機能対応する実装	
	ユーザ端末	ユーザルータ
RFC 3484, “Default Address Selection for IPv6”のポリシテーブル機能	• Windows XP SP2 • Windows Vista • FreeBSD（5.2-RELEASE 以降） • Linux（カーネルレベルでの対応は送信元アドレス選択に関するデフォルト設定のみで、ユーザによる設定変更には未対応）	
RFC 4191, “Default Router Preferences and More-Specific Routes ”の ”More-Specific Routes”機能	• Windows Vista • Linux（実験的・デフォルト無効）	• FreeBSD（rtadvd） • NetBSD（rtadvd） • OpenBSD（rtadvd） • Linux（radvd）

III. 関連ツールの紹介

IPv6 サービスを利用するユーザ端末の IPv6 関連の設定を簡易化するツールを以下の表に紹介する。

表（付録-III） 関連ツール

名称	説明
Windows XP/Vista 兼用 IPv4/IPv6 優先切り替えツール（コードネーム：Beagle）	RFC3484 default address policy table の IPv6 と IPv4 の優先度を変更するツール。以下の URL から無償でダウンロードできる。 http://entne.jp/tool/toollist/index.php
Windows Vista 用 IPv6/IPv4 TCP フォールバック問題回避ツール（コードネーム：Greyhound）	IPv6 に準拠した Microsoft Windows Vista と NTT 東日本「フレッツ・ドットネット」サービス、または NTT 西日本「フレッツ・光プレミアム」サービス等を同時利用時に、インターネット上に存在する IPv6 対応 Web サイトにアクセスしようとした場合、遅延が発生する問題を回避するため RFC3484 default address policy table を変更するツール。以下の URL から無償でダウンロードできる。 http://entne.jp/tool/toollist/index.php