IPv6 端末 OS における
IPv6 対応・IPv6 機能活用ガイドライン

【第 1 版】

2007 年 3 月 30 日

IPv6 普及・高度化推進協議会

移行 WG　　IPv6 端末 OS 評価 SWG

目次

1 組織・背景・目的

1.1 当該文書の背景と目的

近年、一般ユーザの使う主要な端末 OS にて IPv6 が利用可能になり、ユーザが気づかないうちに IPv6 を使う状況が起こりつつある。特に日本は世界に先駆けて IPv6 が普及している環境であるからこそ、一般ユーザにとって IPv6 利用による問題が発生する可能性があり、この起こりうる問題について検討を行う必要がある。

この様な状況に鑑み、IPv6 普及・高度化推進協議会[1]の移行ワーキンググループ（WG）では、一般ユーザが利用するであろう端末 OS が IPv6 化した際に発生しうる問題をピックアップし、現状の課題整理などを行うためのサブワーキンググループ（SWG）として、2006 年 4 月に IPv6 端末 OS 評価 SWG[2]を設置した。当該文章は、本 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 端末 OS の IPv6 対応・機能活用ガイドライン」としてまとめたものである。

本ガイドラインでは、IPv6 に対応した端末 OS の利用について、下記の事柄について説明している。

- IPv6 対応端末 OS を利用する際、どのような課題が発生しうるか
- その課題を解決する方針、手段（ユーザや管理者はどのようにすべきか）

これらの事柄について本ガイドラインでは、Microsoft 社の Windows Vista™（以下 Windows Vista）を中心に検証・検討を行っている。ただし、これらの事柄は Windows Vista のみに留まらず、他の端末 OS および各種アプリケーションや各種ネットワークデバイスの実装の際にも、参考となることを目指している。

[1] IPv6 普及・高度化推進協議会: http://www.v6pc.jp/
[2] IPv6 端末 OS 評価 SWG: http://www.v6pc.jp/jp/wg/transWG/osSWG.phtml

1.2　本ガイドラインの対象者と検証 OS について

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。

- IPv6 に対応した機器や OS を含めたソフトウェアを設計・製作する方々に、IPv6 に対応した製品が解決すべき課題やそのための機能仕様を提供し、問題の発生を予防し、問題への対処速度を向上する。
- 企業等の組織内や家庭内で、個人が使用する PC が接続されているネットワークを設計・構築・管理する方々に、設計・構築・管理の際に解決すべき課題を提供し、問題の発生を予防し、問題への対処速度を向上する。
- ISP など、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に、IPv6 に対応した端末で発生しうる課題を提供し、自社やお客様へのサポートを強化する。
- その他、IPv6 技術に関わる方に情報を提供し、エンジニアの能力向上や扱っている課題の解決を目指す。

前節でも述べたように、今回の検証は Windows Vista を中心に実施している。検証に用いた Windows Vista は Ultimate Edition であるが、他の Edition と挙動が大きく変わるものではないと思われる。

また、本ガイドラインにおいて記載されている内容は、再現される事象を述べたものであり、Windows Vista および他の端末 OS の挙動に関しても、提供元の Microsoft 社等による公式見解ではないことを予めお断りしておく。

1.3　記述用語に関して

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」[3]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。また、上記に記述されていない用語について、以下に説明する。

用語	説明
NXDOMAIN	DNS の通信におけるエラーメッセージの一種。NXDOMAIN とは、クエリで要求されたドメイン名に対してあらゆるリソースレコードが存在しないことを示すメッセージである。 AAAA レコードのクエリに対して A レコードが存在しているにも関わらず NXDOMAIN を返答するバグが顕在化し IPv6 通信を阻害する原因の一つとして問題になりつつある。

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

Teredo （RFC4380）	NAT を越える IPv6 over IPv4 トンネル接続技術。UDP の 3544 番を利用して Teredo サーバとのトンネル接続を行い、IPv6 インターネットへの到達性を確保する。Teredo リレーを介して IPv6 ネットワークとも接続できる。
ULA （RFC4193）	Unique Local IPv6 Unicast Addresses。IPv4 のプライベートアドレスや、廃止された IPv6 サイトローカルアドレスと似ており、インターネットでは使用しない、ローカルでのみ使用する IP アドレスである。ULA には利用者にユニークに割り当てられる空間と、プレフィックス部分をランダムに生成して使用する二種類のアドレス空間が定義されている。
ポリシーテーブル （RFC3484）	終点アドレスと始点アドレスの組み合わせを選択する際に用いられる、最長一致プレフィックス検索テーブル。優先度（Precedence）とラベル（Label）を比較して利用するアドレスを決定する。優先度は終点アドレスの順位付けに、ラベルは終点アドレスに対する始点アドレスの決定にそれぞれ用いられる。

1.4　表記方法に関して

本ガイドラインでは、IPv6 対応端末 OS における設定方法を提示する際に、各端末 OS における設定コマンドを明記している。入力するコマンドは太字で示している部分となり、"%"、"#"、"C:¥>"等はプロンプトを表している。なお、Windows Vista における「netsh」コマンドの利用方法は A.1 節にて付録として説明する。

また、IPv6 アドレスと IPv4 アドレス双方を持つ表現として、「IPv6/IPv4」という表現方法を用いている。

1.5　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。

姓名	所属
大平 浩貴【共同チェア】	株式会社リコー
北口 善明【共同チェア】	株式会社インテック・ネットコア
荒野 高志	株式会社インテック・ネットコア
河野 義広	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
川村 大輔	東日本電信電話株式会社
廣瀬 和則	東日本電信電話株式会社
常川 聡	東日本電信電話株式会社 - 神奈川
植松 高史【オブザーバ】	西日本電信電話株式会社
槇林 康雄【オブザーバ】	西日本電信電話株式会社
加藤 淳也	日本電信電話株式会社 PF 研
藤崎 智宏【オブザーバ】	日本電信電話株式会社 PF 研
太田 善之	NTT コミュニケーションズ株式会社
島村 潤	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
神明 達哉【オブザーバ】	株式会社 東芝
瀬川 卓見	パナソニック コミュニケーションズ株式会社
酒井 淳一	パナソニック コミュニケーションズ株式会社
猪俣 彰浩	富士通株式会社
横田 徹也	富士通株式会社
楠正 憲【検討フォロー】	マイクロソフト株式会社
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
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
清水 友晴【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

2 ネットワーク（既存の IPv4 網）への影響に関する課題と検討結果

本章では、IPv6 対応したデュアルスタック端末が登場することにより、既存の IPv4 によるインターネットが受ける影響に関して議論する。これらの課題は、ネットワークが IPv6 対応とならなくても発生するもので、IPv4 しか利用しない環境下においても理解が必要である。

2.1 DNS のクエリ量の増加による DNS キャッシュサーバへの影響

2.1.1 問題の背景と概要

標準で IPv6 機能が有効となっている端末 OS が普及した場合、DNS キャッシュサーバへのクエリ処理要求が増加することが予測される。本節では DNS キャッシュサーバに対するインパクトを考察し、DNS キャッシュサーバを運用するサービス提供事業者および、ネットワークアプリケーションの開発者らが考慮すべき点を提示する。

これまでの IPv4 ネットワーク上で動作する標準的なアプリケーションは、ホスト名から、IPv4 アドレスのみを解決していた。しかしアプリケーションを IPv6 対応とすることで、ホスト名から IPv4 アドレスと、IPv6 アドレスの両者の解決を試みる。ほとんどの場合において、IPv6 対応の端末 OS 上で稼動する IPv6 対応アプリケーションとは、IPv6/IPv4 のデュアルプロトコルに対応するものである。

したがって、仮に現在利用されているすべてのネットワークアプリケーションが IPv6 対応となった場合、DNS クエリが現在の 2 倍に増加する可能性がある。

また端末 OS やアプリケーションが自動的に補完するドメインサフィックスも DNS クエリを増加させる一因である。端末 OS の設定によっては、ひとつの DNS クエリに対して、ドメインサフィックスを自動的に補完してホスト名の解決を試みる。さらに Web ブラウザなどのネットワークアプリケーションは、独自にドメインサフィックスの補完を行ったり、ホスト名をキーワードとみなして検索を行ったりするためサーチエンジンなどの関連するホスト名の名前解決を行うことがある。ユーザから見た単一の動作（例えば Web ブラウザ上のワンクリック）が、複数の DNS クエリに展開される可能性を秘めている。

したがって、端末 OS のリゾルバ機能やアプリケーションの挙動とあいまって、今後端末 OS の IPv6 対応が進むと DNS クエリが増加し、DNS キャッシュサーバの負荷が高まる可能性がある。図 2-1 に、ある ISP において計測された DNS クエリの推移と今後の予測に関するグラフを示す。

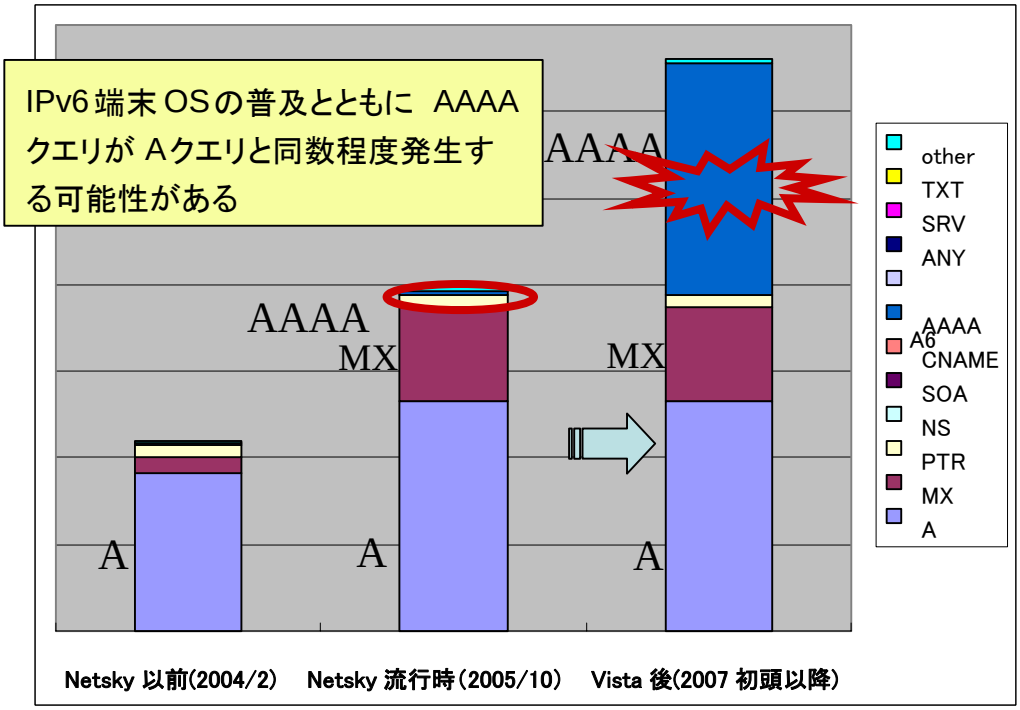

図 2-1　DNS クエリ増加の予測

2.1.2 DNS キャッシュサーバの高負荷による影響

アプリケーションを操作するユーザの立場からみて DNS クエリの応答時間は、アプリケーションの応答性に直接影響を及ぼす。特に DNS キャッシュサーバが高負荷となり、クエリに対する応答に大きな遅延が発生する場合は、ユーザはアプリケーションの操作性に不満を感じる。ネットワークサービスやアプリケーションサービスを提供する事業者にとってユーザの不満は、顧客クレームに直結する恐れがあるため、DNS キャッシュサーバの応答時間はサービス全体のクオリティを保つためにも重要である。

特に、多数のユーザを抱え DNS キャッシュサーバの処理クエリ数が膨大であるサービス事業者は注意が必要である。

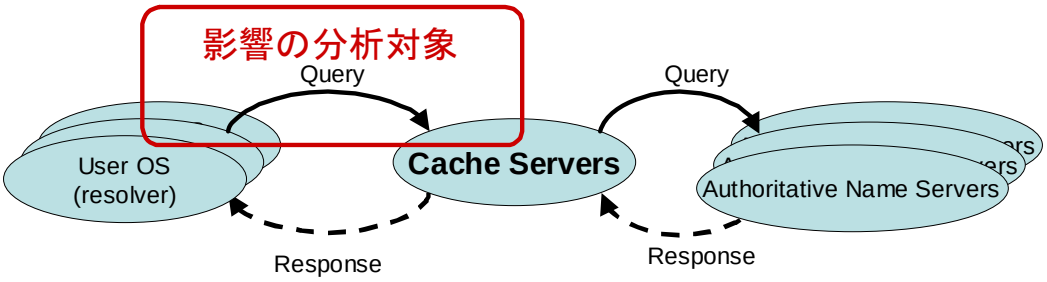

図 2-2　DNS 負荷に関する検討の分析範囲

2.1.3 問題のスコープと端末 OS の動作分析対象

本節では、DNS クエリのうち、端末 OS が発するクエリを直接受ける DNS キャッシュサーバのトラフィックについて考慮する。図 2-2 に分析範囲を示すように、キャッシュサーバからルート DNS やオーソリティ DNS サーバへのトラフィックは考慮しないものとする。

本スコープに対して端末 OS の動作分析を行い、以下の挙動による DNS キャッシュサーバへのクエリ増大を検討する。

- 挙動 A： 端末 OS の IPv6 対応による IPv6 アドレスの解決追加
- 挙動 B： 端末 OS によるドメインサフィックスの補完機能
- 挙動 C： アプリケーションの挙動に依存したホスト名の解決
- 挙動 A＋挙動 B： IPv6/IPv4 アドレスの解決とドメインサフィックス補完

2.1.4 端末 OS の IPv6 対応による IPv6 アドレスの解決追加の検証

IPv4 のみに対応した端末 OS に付属するアプリケーションは、ホスト名の名前解決を実施する際に、IPv4 アドレス（A レコード）のみを検索していた（以下 A クエリ）。しかし、IPv6 を有効化した端末 OS では、IPv4 アドレスに加えて IPv6 アドレス（AAAA レコード）の解決（以下 AAAA クエリ）も行われる。一般に、IPv6/IPv4 両者に対応したアプリケーションは、ユーザが IP アドレスファミリを明示的に指定しない限り IPv4 および IPv6 の両者アドレスの解決を試みる。したがって IPv4 のみに対応した端末 OS と比べて、発生する DNS クエリが 2 倍となる可能性がある。

- FreeBSD 6.2-RELEASEの挙動

ネットワークインターフェイスに IPv6 グローバルアドレスを持たない場合でも IPv6 アドレスの解決を試みる。アドレスファミリを指定しないホスト名の解決について、A クエリと同様に AAAA クエリも試みられ、ひとつのホスト名の解決に対して、2 つの DNS クエリが発生する。解決順序は A クエリに先行して AAAA クエリが試みられる。もし先行する A クエリに対する返答として NXDOMAIN（no exist domain name）を受信した場合でも、AAAA クエリは抑止されない。

- Windows XP SP2の挙動

ネットワークインターフェイスに IPv6 グローバルアドレスを持たない場合でも、IPv6 スタックの機能が有効になっていれば AAAA クエリが試みられ、ひとつのホスト名に対して 2 つの DNS クエリが発生する。解決順序は A クエリに先行して AAAA クエリを試みる。もし AAAA クエリに対する返答として NXDOMAIN（no exist domain name）を受信した場合、A クエリは抑止される。なお Service Pack 1 + Advanced Network Pack（817778）以前の Windows XP では、NXDOMAIN を受信しても A クエリは抑止されず、IPv4 アドレスの解決結果と IPv6 アドレスの解決結果に依存性はない。

- Windows Vistaの挙動

Windows Vista では、ネットワークインターフェイスに IPv6 グローバルアドレスを持たない場合は AAAA クエリが抑止される（この IPv6 グローバルアドレスには 6to4 アドレスも含まれる（3.1.3 節表 3-1 参照））。また、クエリの送信順序は、A クエリが AAAA クエリに対して先行して行われる。もし A クエリに対する返答として NXDOMAIN を受信した場合、AAAA クエリが抑制される。IPv6/IPv4 アドレスの解決順序が Windows XP SP2 の挙動とは異なる[4]。

表 2-1 に、上記の挙動をより詳細にまとめる。縦軸に端末 OS 側のインターフェイスにおけるアドレス、横軸に DNS サーバが持つアドレスの種類を示している。両者がデュアルスタックの場合には、利用トランスポートのフォールバックも発生する可能性がある。

表 2-1　Windows Vista における DNS クエリの挙動

		DNS サーバ		
		IPv4 のみ	IPv6 のみ	デュアルスタック
端末 OS	IPv4 プライベート	①	―	①
	IPv6	―	②	②
	デュアルスタック	③	④	⑤

① IPv4 で A クエリを実行
② IPv6 で AAAA クエリを実行
③ IPv4 で A クエリを実行し NXDOMAIN でなければ AAAA クエリを実行
④ IPv6 で A クエリを実行し NXDOMAIN でなければ AAAA クエリを実行
⑤ IPv6 で A クエリを実行し NXDOMAIN でなければ AAAA クエリを実行
A クエリで NXDOMAIN が返ってきた場合には IPv4 でのクエリ（①）に以降する

※IPv4 グローバルのみの場合は、6to4 アドレスが付与され、デュアルスタックの場合と同様になる。

2.1.5 端末 OS によるドメインサフィックスの補完機能の検証

端末 OS の実装によっては名前解決が失敗した場合、自動的にドメインサフィックスを補完して再度問い合わせを試みる。例えば "host" の解決が失敗した場合、"host.com" → "host.net" → "host.org" → ... のようにドメインサフィックスを補って名前解決を行う。

端末 OS が補完する代表的なドメインサフィックスは次の設定である。

[4] Windows Vista IPv6 実装はどう変わる？（JANOG18）：
http://www.janog.gr.jp/meeting/janog18/files/IPv6_Oikawa.pdf

1. DHCP、PPP 接続時にサーバから配布されたドメインサフィックス
2. 端末 OS への設定項目
    - FreeBSD など: /etc/resolv.conf への設定項目（domain, search）
    - Windows: マイコンピュータ名およびネットワークインターフェイスの TCP/IP のプロパティ設定

もし補完すべきドメインサフィックスが複数あれば、名前解決が成功するまで補完が試みられる。したがってユーザ（アプリケーション）の単一の名前解決を、端末 OS が自動的に数倍の DNS クエリに展開する可能性がある。

例えば、Windows Vista では次の設定項目に補完するドメインサフィックスが記入可能である。

1. マイコンピュータのプロパティで指定するドメイン名
   ⇒ ".example1.jp"
2. DHCP でサーバから自動的に配布されたドメイン名
   ⇒ ".example2.jp"
3. 各ネットワークインターフェイスの TCP/IP のプロパティで指定したドメイン名
   ⇒ ".example3.jp"

1.～3.の設定項目に上記のドメインサフィックスを設定し、ホスト名 "host" の名前解決を試みた場合、名前解決が成功するまで、次のように順次ドメインサフィックスの補完と展開が行われる。

- 上記 3.に相当する項目が設定されていない場合
    - host.example1.jp
    - host.example2.jp
    - host.example3.jp
- 上記 3.に相当する項目が設定されている場合
    - host.example3.jp
      この場合 example1.jp, example2.jp は補完の対象とならない。

ただしホスト名に "." （ピリオド）が含まれている場合（例えばホスト名 "host.subdomain"）は、1.～3. の設定項目に補完対象のドメインサフィックスを設定しても補完は行われない。

2.1.6 アプリケーションの挙動に依存したホスト名の解決の検証

端末 OS がドメインサフィックスの補完を行っても名前解決に失敗する場合、アプリケーションが関連する他のホスト名を解決することがある。下記の代表的な Web ブラウザでは本来 URL（ホスト名）を入力すべきアドレスバーにキーワードが入力されると、サーチエンジンへの問い合わせが行われる。このときサーチエンジンのホスト名を解決するための DNS クエリが発生する。

- Internet Explorer 7（Windows Vista）
  - case 1: 単純なキーワードの入力

    アドレスバーに、http:// など URL の接頭辞で始まらない単語を入力した場合：
    OS に設定されたドメインサフィックスの補完を試みる。それでも名前解決ができない場合は MSN Live Search へキーワードを転送し検索結果を表示する。
  - case 2: URL の入力

    http://XXXX/ のように URI の接頭辞から始まる語を入力した場合：
    OS によるドメイン名の補完が行われるが、名前解決が失敗しても語は検索エンジンへ転送されずブラウザ上にエラー出力が行われる。

- Firefox 2.0.0.3 (Windows向け日本語版)
  - case 1: 単純なキーワードの入力

    アドレスバーに、http:// など URL の接頭辞で始まらない単語を入力した場合：
    OS に設定されたドメインサフィックスの補完を試みる。それでも名前解決ができない場合は Google, Yahoo!などの検索エンジンへキーワードを転送し検索結果を表示する。
  - case 2: URL の入力

    http://XXXX/ のように URI の接頭辞から始まる語を入力した場合：
    FireFox（アプリケーション）自身が、XXXX の前後に www と.com を補って（www.XXXX.com）名前解決を試みる。名前解決が失敗しても、語は検索エンジンへ転送されずブラウザ上にエラー出力がされる。

上記に挙げたアプリケーションのように、特定のアプリケーションによっては、.com などのドメイン名を自動的に補完したり、誤ったホスト名が与えられても即座にエラーとして処理したりするのではなく、関連する情報を検索してユーザに提示する機能を持つ。ユーザにとっては利便性の向上が図れるが、特に DNS クエリを多く発生させるような仕組みの場合は、ユーザ利便性とサーバ・ネットワーク負荷のトレードオフになる。特にアプリケーションの開発者はこの点を留意する必要がある。

2.1.7 IPv6/IPv4 アドレスの解決とドメインサフィックス補完の検証

FreeBSD 6.2-RELEASE、 Windows XP SP2、 Windows Vista の各端末 OS において、ホスト名

“hostname”

を解決する。ここで各 OS が補完するドメインサフィックスとして次の 3 つのサフィックスを設定しているものとする。

- .co.jp
- .example.jp
- .com

このときホスト名 "hostname" の名前解決に対して各端末 OS が発生する DNS クエリは次のとおりである。

- FreeBSD 6.2-RELEASE

IPv6 アドレス、IPv4 アドレスのいずれかが名前解決できるまで、最大で補完対象のドメインサフィックスの数だけ繰り返す。繰り返しのパタンは図 2-3 に示すようにホスト名を示す文字列ごとに、A クエリ→AAAA クエリの順で、IPv4 アドレスから先行して名前解決が行われる。

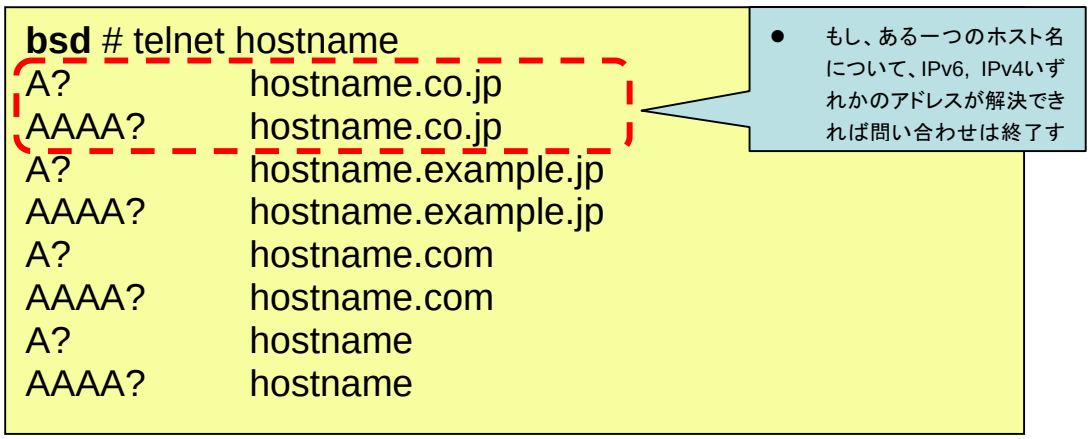

図 2-3 サブドメイン補完の例（FreeBSD 6.2-RELEASE）

- Windows XP SP2

IPv6 アドレスの解決を優先して補完対象のドメイン名の数だけ繰り返す。繰り返しのパタンは図 2-4 に示すように全ての AAAA クエリを実行した後に A クエリを開始する動きとなる。はじめの 3 つのクエリで IPv6 アドレスの解決が行われるため、IPv4 アドレスの解決が開始されるまで、補完対象のドメインサフィックス分だけ AAAA クエリを行う必要が生じる。本文書を作成する 2007 年 3 月現在のインターネットの現状では、多くのホスト名

は IPv4 アドレスのみをもち、IPv6 アドレスを持ったホストは少ない。そのため IPv6 アドレスの解決にために発生する大多数のクエリに対して、有効な返答が得られない。

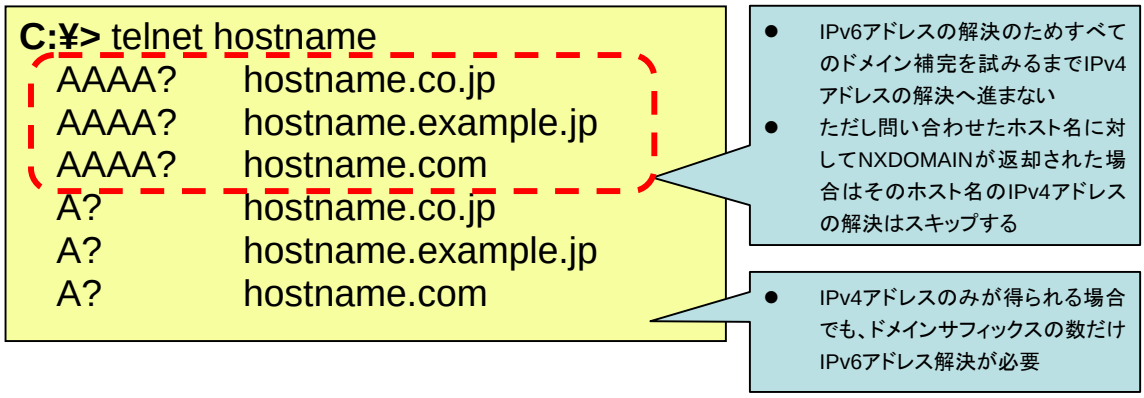

図 2-4　サブドメイン補完の例（Windows XP SP2）

- Windows Vista

図 2-5 に示すように、ホスト名を示す文字列ごとに、IPv4 アドレスから先行して名前解決が行われる。A クエリの段階で NXDOMAIN が応答された場合は、それに続く AAAA クエリはスキップする。多くのインターネット上のホストに IPv4 アドレスが付与され、IPv6 アドレスが付与されたホストが少ない現状では、不要な DNS クエリを抑制する上でも効率的な動作となっている。しかしながら、今後 IPv6 が普及して多くのホスト名に IPv6 アドレスが付与される場合は、IPv6 アドレスを優先して解決する挙動のほうが効率的となる。IPv6 の普及状況によって問い合わせ順序は見直されるべきである。

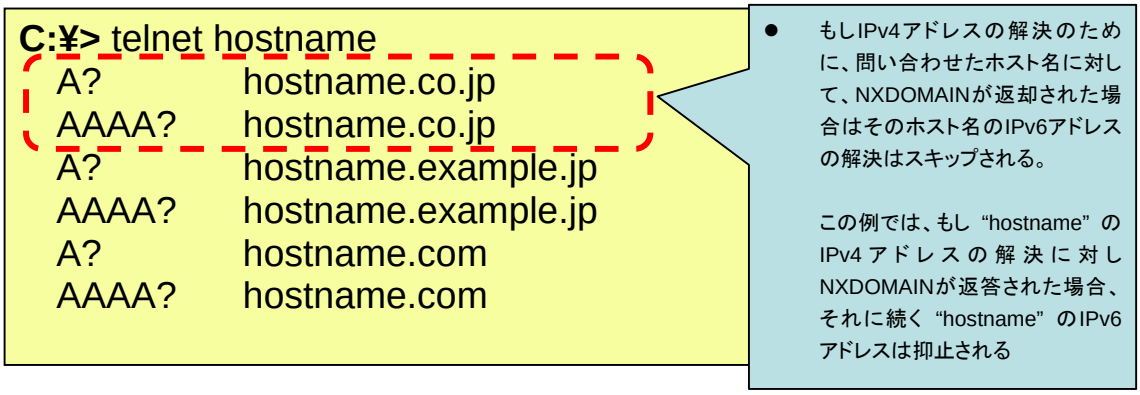

図 2-5　サブドメイン補完の例（Windows Vista）

2.1.8 まとめ

IPv6 対応の端末 OS が普及すると、IPv6 アドレスの解決のため DNS キャッシュサーバへの DNS クエリが増加することが予測される。また端末 OS やネットワークアプリケーションのドメインサフィックスの補完機能を用いられており、DNS クエリの増加に拍車をかけている。

したがって、DNS キャッシュサーバを運用するサービス事業者の方々には、DNS キャッシュサーバのリソースについて現状のキャパシティの確認と、今後の DNS トラフィック増加に対応するための検討をお勧めしたい。またネットワークアプリケーションの開発者は、DNS クエリの抑制を意識した開発を行っていただきたい。

2.2　閉域 IPv6 網混在環境での IPv6 から IPv4 へのフォールバック

2.2.1 問題の背景と概要

IPv6 に対応した端末 OS では、IPv4 通信のみを利用していた端末では発生しなかった問題が起きる可能性がある。その問題の 1 つとして、本節では TCP 通信開始時において、IPv6 での接続から IPv4 での接続へのフォールバックに時間がかかる場合があることを取り扱う。具体例としては、インターネットへの到達性を持たない IPv6 ネットワーク（以下、閉域 IPv6 網）が混在する環境において、インターネットへの TCP 通信が遅く感じる場合があるというものである。TCP プロトコルを使う通信の代表例には、我々に馴染み深いアプリケーションである WWW や電子メールがある。

ここで閉域 IPv6 網が既存 IPv4 インターネット環境と混在した環境を考えてみる。今後の IPv6 の普及にともなって、企業ネットワークのイントラネット環境や、検証や開発のための実験ネットワーク、通信事業者が提供するサービスなどの閉域 IPv6 網が出てくるかもしれない。この環境において、インターネット上のデュアルスタックサイトへアクセスするケースでは、IPv6 通信を優先するように動作するホストは、インターネット到達性が無い場合にも IPv6 通信で接続を試みてしまうため、IPv4 通信へフォールバックするまで時間がかかる。このように、特定の環境下ではインターネットアクセスが遅いと感じるケースが起きる場合がある。

IPv6 と IPv4 のデュアルスタック OS である Windows Vista では、ユーザが主体的に IPv6 通信を利用することを選択せずとも、初期状態で IPv6 通信機能が有効になっている。さらに多くの IPv6 対応端末 OS の実装と同様、IPv6 での通信が優先される。したがって、Windows Vista からデュアルスタックサイトへ接続する場合、前述したように、まず IPv6 で通信を試み、その試みが失敗すると、IPv4 での通信へフォールバックするように動作する。

本節ではホームユーザネットワークでの既存 IPv4 ネットワーク環境への影響の観点で、Windows Vista を利用した WWW 通信の挙動の確認をすると伴に、Windows Vista 利用者側で取り得る問題回避方法について述べる。

2.2.2 想定するネットワーク環境

ユーザ LAN 内に、IPv4 ネットワークと閉域 IPv6 網が共存する環境での、Windows Vista ノードの挙動を確認する。本節の調査は典型的なホームユーザネットワーク環境を模擬するものとして、図 2-6 に示す環境でおこなった。

また、閉域 IPv6 網環境は、図 2-6 の環境において IPv6 ネットワークのルータから先のインターネットへの到達性を失わせるよう状態を作ることで模擬した（図 2-7）。ネットワークの構成情報は次の通り。

- IPv4 ネットワークはプライベートアドレスで構成。
- IPv4 ネットワークではルータが有する DHCP 機能を利用し、テスト PC は IPv4 ネットワーク情報（DNS サーバアドレス情報を含む）の通知を受ける。
- IPv6 ネットワークはインターネットへの到達性は持たせない。
- IPv6 ネットワークではルータがルータ広告（RA：Router Advertisement）を送信する。

この環境で TCP 通信開始時における IPv6 通信から IPv4 通信へのフォールバック問題についての調査を実施した。

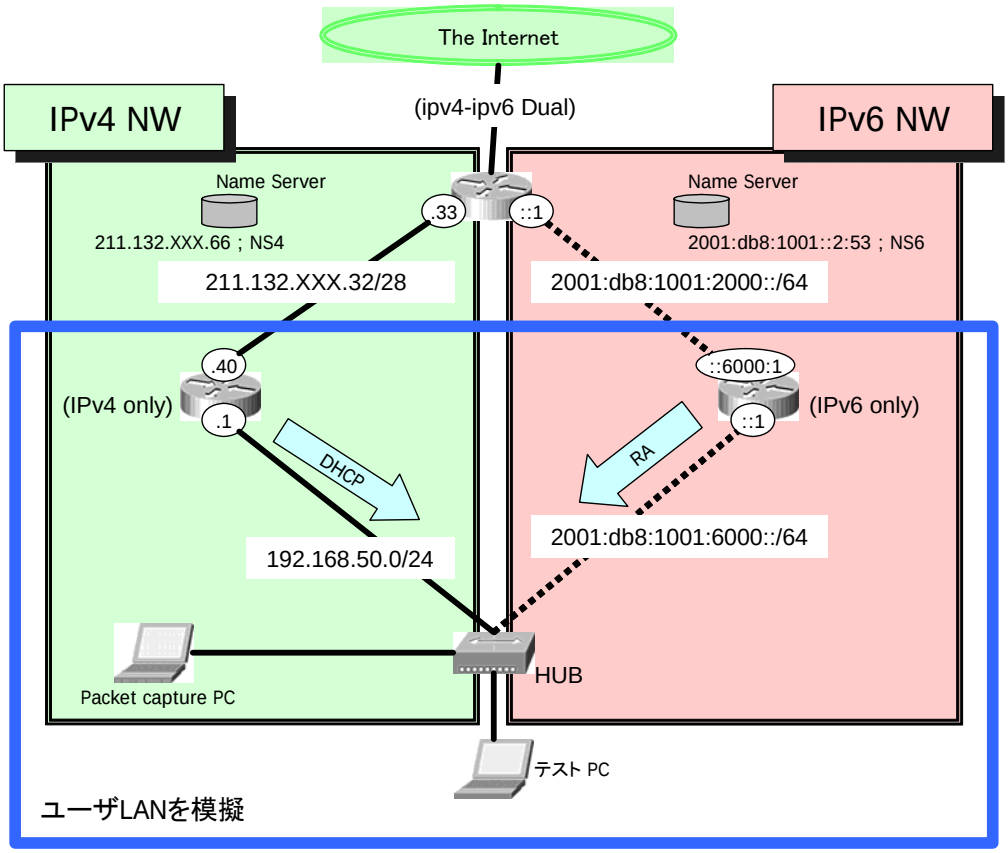

図 2-6　ホームユーザネットワーク環境を模擬した検証環境図

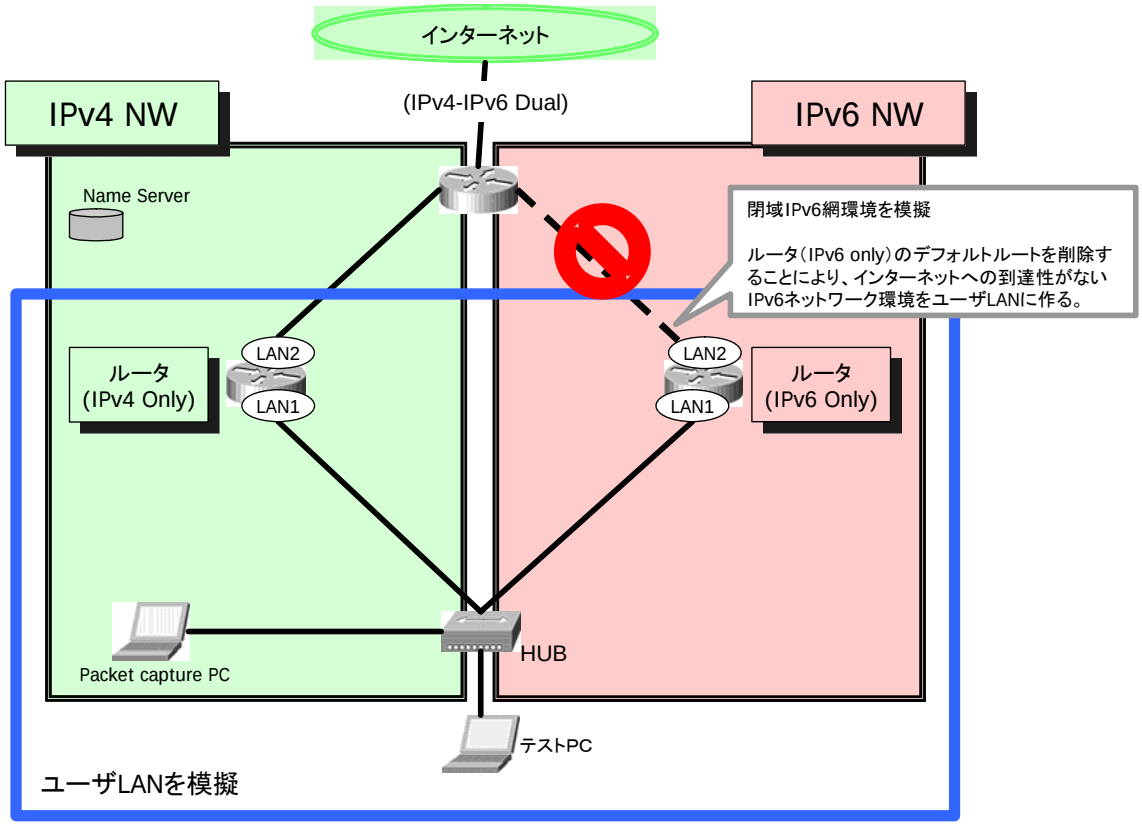

図 2-7　既存 IPv4 ネットワークに閉域 IPv6 ネットワークが加わった状況を模擬する環境

2.2.3 ICMPv6 による不到達通知とフォールバック挙動の検証

Windows Vista が、IPv4 ネットワークと閉域 IPv6 網が共存している環境に接続された場合の動作を調査するため、ICMPv6 の不到達通知[5]（以下、不到達通知）に関する下記の 3 項目の検証を行う。

1. Windows ファイアウォール（【セキュリティが強化された Windows ファイアウォール】）の ICMPv6 フィルタ設定の有無の確認。
2. Windows Vista が不到達通知を受信しない場合のフォールバック挙動確認。
3. Windows Vista が不到達通知を受信する場合のフォールバック挙動確認。

検証を実施するための前提条件を下記に示す。

- Windows Vista の Windows ファイアウォールはインストール後の初期状態で実施。フィルタのルールを新たに作成することをせずに、Windows ファイアウォールが初期状態で持っているフィルタルールについて、許可/ブロックの操作をすることとした。なお、【セキュリティが強化された Windows ファイアウォール】の設定画面の利用方法は A.2 節を参照のこと。

[5] ICMPv6 不到達通知：ICMPv6 の Type1 Code0（Route Unreachable）

- 不到達通知の送信の有無はユーザ LAN 内の IPv6 ルータで制御。
- 不到達通知の送信はユーザ LAN 内の IPv6 ルータでデフォルトゲートウェイ設定を削除することで実施。
- 検証に用いる Web ブラウザは Internet Explorer 7（以下 IE7）とする。

- **検証項目1**
  1. IPv6 対応 OS 端末をユーザ LAN 内に接続する。
  2. Windows Vista の初期状態での Windows ファイアウォールの設定を確認する。

- **検証項目2**
  1. ユーザ LAN 内の IPv6 ルータが不到達通知を送信しないに設定する。
  2. IPv6 対応 OS 端末から、AAAA RR と A RR を持つインターネット上の WWW サーバへ IE7 ブラウザで接続する。
  3. IPv6 対応 OS 端末と WWW サーバ間の通信をキャプチャして解析する。

- **検証項目3**
  1. ユーザ LAN 内の IPv6 ルータが不到達通知を送信するように設定する。
  2. IPv6 対応 OS 端末から、AAAA RR と A RR を持つインターネット上の WWW サーバへ IE7 ブラウザで接続する。
  3. IPv6 対応 OS 端末と WWW サーバ間の通信をキャプチャして解析する。

2.2.4 検証結果

- **検証項目1**

Windows Vista の Windows ファイアウォールは初期状態で不到達通知（ICMPv6 Type1）は受信許可されている（4.2.2 節参照）。

- **検証項目2**

WWW サーバへの接続に際し、多くの人はたいていの場合、URI（Uniform Resource Identifier）を指定するのに「http://www.example.jp/example/index.html」のように WWW サービスを提供しているホスト名を使っている。テスト PC からWWWサーバへ接続リクエストが送信されると、ホスト名から IP アドレスを検索するために、DNS サーバへの名前解決の DNS クエリ（問い合わせ）が起きる。

2.1.4 節で述べたように、Windows Vista はネットワークインターフェイスに IPv4 アドレスと IPv6 アドレス（グローバルユニキャストアドレス）を割り当てている場合、DNS サーバに対して A RR および AAAA RR 両方の回答を得ようとする。A RR および AAAA RR 両方の回答を得た上で、まずは AAAA RR に対して TCP/IPv6 での接続要求を開始する。

テスト PC からの TCP 接続要求の様子は次の通りであった。WWW サーバへの IPv6 通

信での到達性が無い環境であるので TCP/IPv6 での接続の試みは失敗するのだが、初回の失敗を含めて 3 回の試行失敗の後、TCP/IPv4 へフォールバックした。接続のリトライ間隔は等間隔ではなかった。1 度目の TCP/IPv6 接続要求が失敗した約 3 秒後に、2 度目の TCP/IPv6 接続要求を WWW サーバ宛てに送信した。2 度目の TCP/IPv6 接続要求に失敗した約 6 秒後に、3 度目の TCP/IPv6 接続要求を WWW サーバ宛てに送信した。3 度目の TCP/IPv6 接続要求が失敗した約 12 秒後に、IPv6 での TCP 接続をあきらめて、WWW サーバに対して TCP/IPv4 接続要求を送信した。このように IPv6 通信から IPv4 通信へのフォールバックが起きて、WWW サーバとの通信が開始された。

Windows Vista での TCP 通信開始時における IPv6 から IPv4 へのフォールバック時間の内訳は以下の通りであった。

TCP 通信開始時における IPv6 から IPv4 へのフォールバック時間
= 約 21 秒
= 約 3 秒（2 回目までの TCP/IPv6 再送待ち時間）
+ 約 6 秒（3 回目までの TCP/IPv6 再送待ち時間）
+ 約 12 秒（TCP/IPv4 フォールバック接続までの待ち時間）

- **検証項目3**

検証項目 2 との違いとして、ユーザ LAN 内の IPv6 ルータからテスト PC へ不到達通知を送信することによって、WWW サーバへの IPv6 通信での到達性が無い環境であると通知するようにしたことである。不到達通知を受信しても TCP/IPv6 から TCP/IPv4 のフォールバックにかかる時間に、検証項目②での結果と違いは現れなかった。テスト PC は TCP/IPv6 での WWW サーバへの接続要求後、すぐにユーザ LAN 内の IPv6 ルータから不到達通知を受信した。1 度目の TCP/IPv6 接続要求が失敗した約 3 秒後に、2 度目の TCP/IPv6 接続要求を WWW サーバ宛てに送信した。2 度目の TCP/IPv6 接続要求後も、1 度目の TCP/IPv6 接続要求送信後同様に、すぐにユーザ LAN 内の IPv6 ルータから不到達通知を受信した。2 度目の TCP/IPv6 接続要求に失敗した約 6 秒後に、3 度目の TCP/IPv6 接続要求を AAAA RR 宛てに送信した。3 度目の TCP/IPv6 接続要求送信後も、すぐにユーザ LAN 内の IPv6 ルータから不到達通知を受信した。3 度目の IPv6 での TCP 接続要求に失敗した約 12 秒後に、TCP/IPv6 接続をあきらめて、WWW サーバへ TCP/IPv4 接続要求を送信した。このように TCP/IPv6 通信から TCP/IPv4 通信へのフォールバックが起きて、WWW サーバとの通信が開始された。

TCP 通信開始時における IPv6 から IPv4 へのフォールバック時間
= 約 21 秒
= 約 3 秒（2 回目までの TCP/IPv6 再送待ち時間）
+ 約 6 秒（3 回目までの TCP/IPv6 再送待ち時間）
+ 約 12 秒（TCP/IPv4 フォールバック接続までの待ち時間）

2.2.5 検証データ

- 検証項目1

擬似ネットワークへ Windows Vista を接続したときの環境は以下の通り。

```
----------------------------------------------------------------------------
C:¥>ipconfig /all
:
イーサネット アダプタ ローカル エリア接続:

   接続固有の DNS サフィックス . . :
   説明. . . . . . . . . . . . . . : ********
   物理アドレス. . . . . . . . . . : **-**-**-2E-E1-71
   DHCP 有効 . . . . . . . . . . . : はい
   自動構成有効. . . . . . . . . . : はい
   IPv6 アドレス . . . . . . . . . : 2001:db8:1001:6000:894f:f69f:2813:7b16(優先)
   一時 IPv6 アドレス. . . . . . . : 2001:db8:1001:6000:dca3:5848:6c2b:79cd(優先)
   リンクローカル IPv6 アドレス. . : fe80::894f:f69f:2813:7b16%12(優先)
   IPv4 アドレス . . . . . . . . . : 192.168.50.12(優先)
   サブネット マスク . . . . . . . : 255.255.255.0
   リース取得. . . . . . . . . . . : 2006 年 2 月 12 日 13:56:32
   リースの有効期限. . . . . . . . : 2006 年 2 月 15 日 13:56:32
   デフォルト ゲートウェイ . . . . : fe80::2a0:deff:fe0f:406d%12
                                      192.168.50.1
   DHCP サーバー . . . . . . . . . : 192.168.50.1
   DHCPv6 IAID . . . . . . . . . . : 285215460
   DNS サーバー. . . . . . . . . . : 211.132.XXX.66
   NetBIOS over TCP/IP . . . . . . : 有効
----------------------------------------------------------------------------
```

Windows Vista の Windows ファイアウォールの ICMPv6 に関する初期設定を図 2-8 に示す。

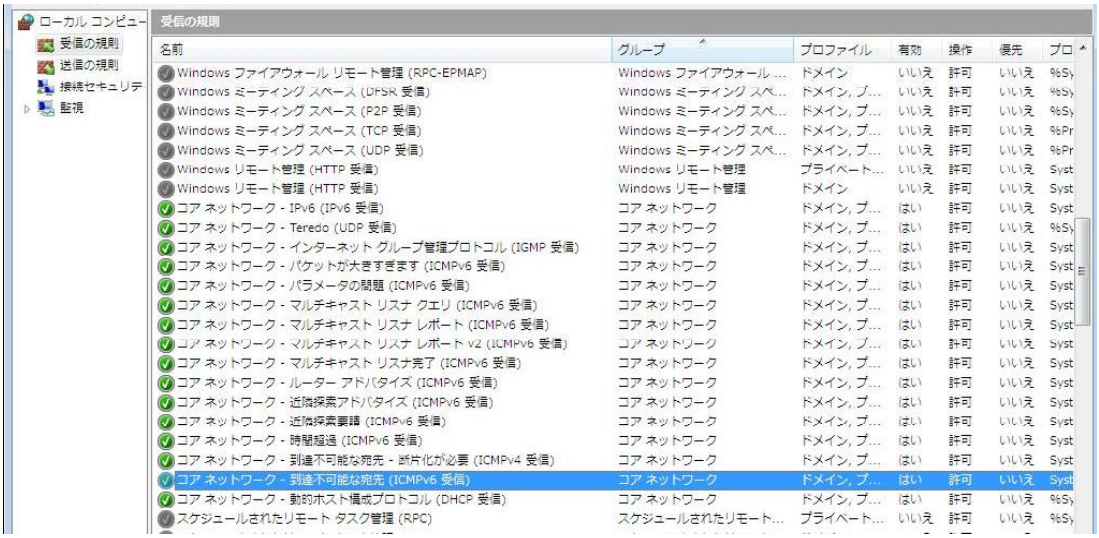

図 2-8　Windows ファイアウォールの初期設定

- **検証項目2**

ユーザ LAN 内の IPv6 ルータの config は以下の通り。

```
------------------------------------------------------------------------------
ipv6 lan1 address 2001:db8:1001:6000::1/64
ipv6 lan1 rtadv send 1
ipv6 lan2 address 2001:db8:1001:2000::6000:1/64
ipv6 prefix 1 2001:db8:1001:6000::/64
ipv6 icmp unreachable send off
------------------------------------------------------------------------------
```

IE7 ブラウザで WWW サーバへ接続を実施したときのパケットキャプチャデータを図 2-9 に、TCP シーケンス図を図 2-10 にそれぞれ示す。

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.50.12	211.132.[redacted].66	DNS	Standard query A www.kame.net
2	0.002249	211.132.[redacted].66	192.168.50.12	DNS	Standard query response A 203.178.141.194
3	0.002733	192.168.50.12	211.132.[redacted].66	DNS	Standard query AAAA www.kame.net
4	0.004726	211.132.[redacted].66	192.168.50.12	DNS	Standard query response AAAA 2001:200:0:80(
5	0.005628	2001:[redacted]:1001:6000:2065:f	2001:200:0:8002:203:47ff:'	TCP	49221 > http [SYN] Seq=0 Ack=0 Win=8192 Ler
6	2.992564	2001:[redacted]:1001:6000:2065:f	2001:200:0:8002:203:47ff:'	TCP	49221 > http [SYN] Seq=0 Ack=0 Win=2097152
9	8.992521	2001:[redacted]:1001:6000:2065:f	2001:200:0:8002:203:47ff:'	TCP	49221 > http [SYN] Seq=0 Ack=0 Win=2097152
14	20.994404	192.168.50.12	203.178.141.194	TCP	49222 > http [SYN] Seq=0 Ack=0 Win=8192 Ler
15	20.997771	203.178.141.194	192.168.50.12	TCP	http > 49222 [SYN, ACK] Seq=0 Ack=1 Win=65(
16	20.997887	192.168.50.12	203.178.141.194	TCP	49222 > http [ACK] Seq=1 Ack=1 Win=65536 Le

図 2-9　不到達通知を受信しない場合のパケットキャプチャデータ

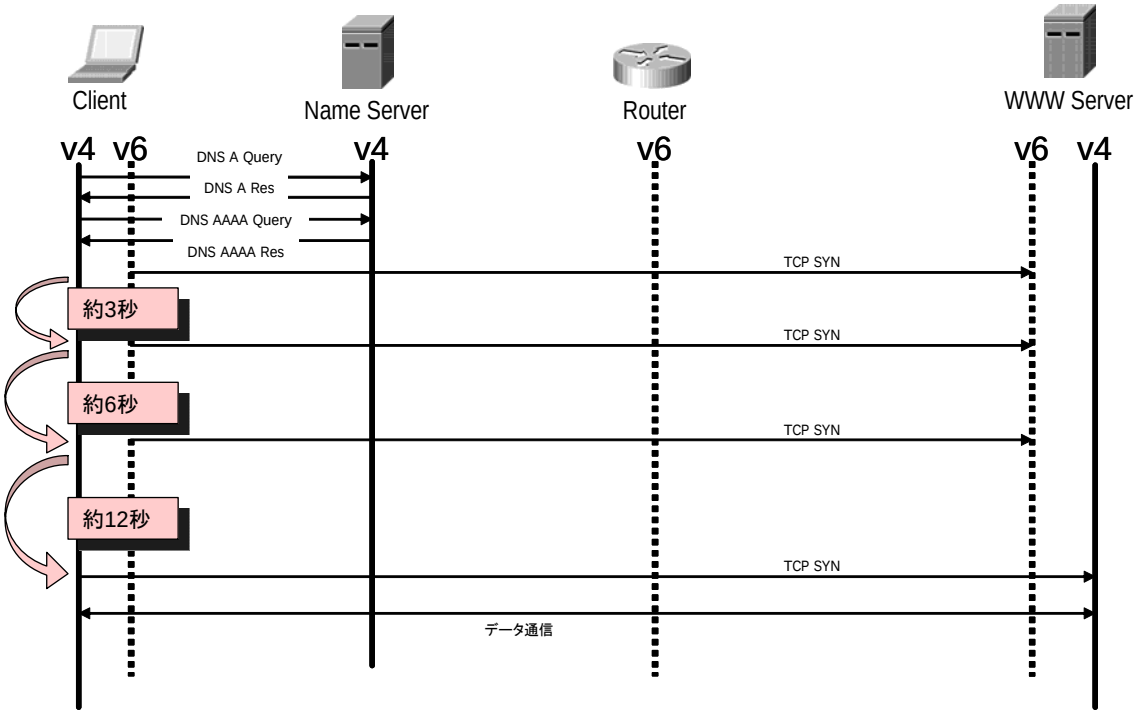

図 2-10　不到達通知を受信しない場合のシーケンス図

- **検証項目3**

ユーザ LAN 内の IPv6 ルータの config は以下の通り。

```
------------------------------------------------------------------------------
ipv6 lan1 address 2001:db8:1001:6000::1/64
ipv6 lan1 rtadv send 1
ipv6 lan2 address 2001:db8:1001:2000::6000:1/64
ipv6 prefix 1 2001:db8:1001:6000::/64
------------------------------------------------------------------------------
```

IE7 ブラウザにて WWW サーバへ接続を実施したときのパケットキャプチャデータを図 2-11 に、TCP シーケンス図を図 2-12 にそれぞれ示す。

No.	Time	Source	Destination	Protocol	Info
3	0.000357	192.168.50.12	211.132.[redacted].66	DNS	Standard query A www.kame.net
4	0.002521	211.132.[redacted].66	192.168.50.12	DNS	Standard query response A 203.178.141.194
5	0.004439	192.168.50.12	211.132.[redacted]66	DNS	Standard query AAAA www.kame.net
6	0.010957	211.132.[redacted]66	192.168.50.12	DNS	Standard query response AAAA 2001:200:0:8002:203:4
7	0.023335	2001:[redacted]:1001:6000:2065:	ff02::1:ff0f:406d	ICMPv6	Neighbor solicitation
8	0.024013	2001:[redacted]:1001:6000::1	2001:[redacted]:1001:6000:20(	ICMPv6	Neighbor advertisement
9	0.024078	2001:[redacted]:1001:6000:2065:	2001:200:0:8002:203:47	TCP	49178 > http [SYN] Seq=0 Ack=0 Win=8192 Len=0 MSS=
10	0.024742	2001:[redacted]:1001:6000::1	2001:[redacted]:1001:6000:20(	ICMPv6	Unreachable (Route unreachable)
11	3.008875	2001:[redacted]:1001:6000:2065:	2001:200:0:8002:203:47	TCP	49178 > http [SYN] Seq=0 Ack=0 Win=2097152 Len=0 M
12	3.009432	2001:[redacted]:1001:6000::1	2001:[redacted]:1001:6000:20(	ICMPv6	Unreachable (Route unreachable)
13	4.691434	2001:[redacted]:1001:6000::1	2001:[redacted]:1001:6000:20(	ICMPv6	Neighbor solicitation
14	4.691657	2001:[redacted]:1001:6000:2065:	2001:[redacted]:1001:6000::1	ICMPv6	Neighbor advertisement
15	9.008839	2001:[redacted]:1001:6000:2065:	2001:200:0:8002:203:47	TCP	49178 > http [SYN] Seq=0 Ack=0 Win=2097152 Len=0 M
16	9.009425	2001:[redacted]:1001:6000::1	2001:[redacted]:1001:6000:20(	ICMPv6	Unreachable (Route unreachable)
17	9.274379	2001:[redacted]:1001:6000:2065:	2001:[redacted]:1001:6000::1	ICMPv6	Neighbor solicitation
18	9.274963	2001:[redacted]:1001:6000::1	2001:[redacted]:1001:6000:20(	ICMPv6	Neighbor advertisement
19	21.034070	192.168.50.12	203.178.141.194	TCP	49179 > http [SYN] Seq=0 Ack=0 Win=8192 Len=0 MSS=
20	21.037528	203.178.141.194	192.168.50.12	TCP	http > 49179 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=
21	21.037640	192.168.50.12	203.178.141.194	TCP	49179 > http [ACK] Seq=1 Ack=1 Win=65536 Len=0
22	21.037895	192.168.50.12	203.178.141.194	HTTP	GET / HTTP/1.1

図 2-11　不到達通知受信時のパケットキャプチャ結果

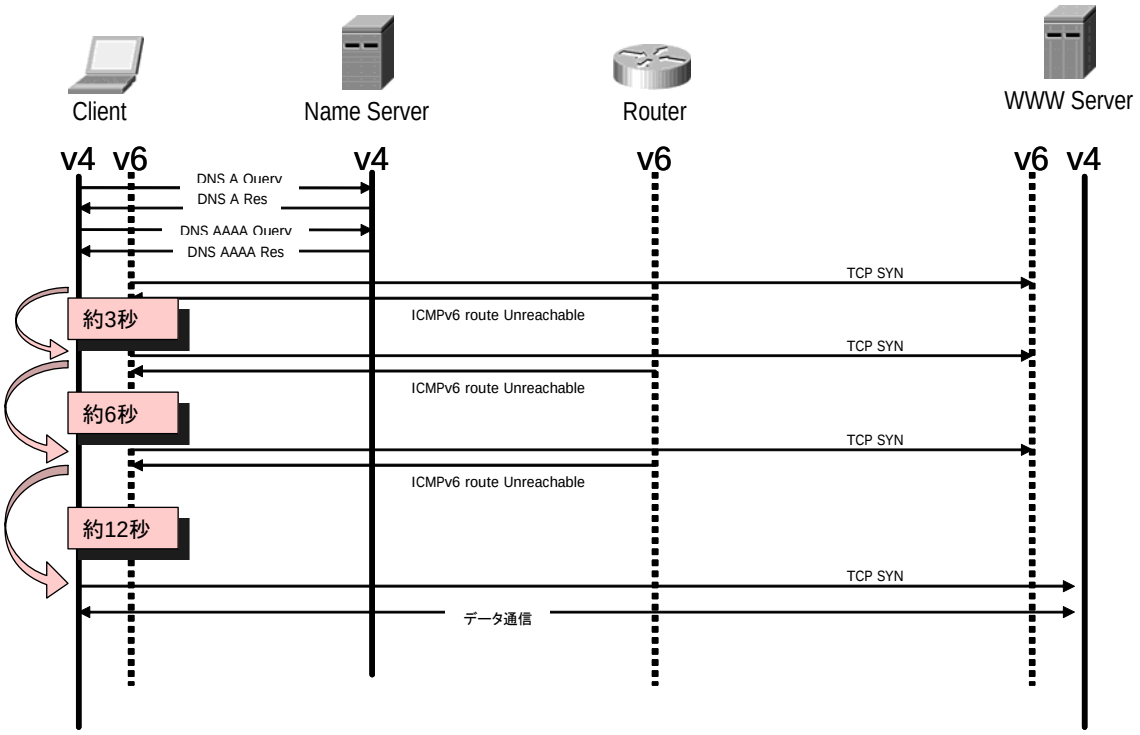

図 2-12　不到達通知受信時のシーケンス図

2.2.6 複数の AAAA RR が登録された WWW サーバへのアクセス検証

IPv6 では 1 つのホストに対して、複数のグローバルユニキャスト IPv6 アドレスを設定して運用することが可能である。閉域 IPv6 網に接続する IPv6 対応 OS 端末が、複数のグローバルユニキャスト IPv6 アドレスを割り当てられた WWW サーバに接続を試みた場合、どのような挙動を示すか確認を行った。

今回の検証では WWW サーバの 1 つのホスト名に対して 5 つの AAAA RR と 1 つの A RR を設定し、Web ブラウザアプリケーションに IE7 を利用して IPv6 対応 OS 端末での閲覧を実施した。

検証の手順は下記の通りである。

1. WWW サーバのホスト名にたいして、5 つの AAAA RR と 1 つの A RR を設定する
2. IPv6 対応 OS 端末から WWW サーバに対して接続する
3. IPv6 対応 OS 端末と WWW サーバ間の通信をパケットキャプチャし解析する

2.2.7 検証結果

WWW サーバへのアクセスは、下記の順番で TCP 接続が行われた。

1. AAAA RR の 1 つ目
2. AAAA RR の 2 つ目
3. AAAA RR の 3 つ目
4. AAAA RR の 4 つ目
5. AAAA RR の 5 つ目
6. A RR の 1 つ目

WWW サーバの IPv6 アドレスそれぞれに対し、TCP/IPv6 での接続開始要求を、3 回ずつおこなう。1 つ目の AAAA RR へ TCP/IPv6 での接続開始要求を連続で 3 回試行し、すべてが失敗すると、次の AAAA RR へ TCP/IPv6 で接続開始要求を送信し始めるという具合に振舞う。1 つの AAAA RR につき、TCP/IPv6 による接続開始要求の通信タイムアウト時間は Windows Vista では約 21 秒（2.2.4 節で確認）である。すなわち、複数の AAAA RR が登録されている IPv6/IPv4 デュアルスタック構成の WWW サーバへアクセスする場合、TCP/IPv4 へのフォールバック時間は（AAAA RR 登録個数）×21 秒となる。

IPv6 対応 OS 端末の中には、IPv4 へのフォールバック時間まで待ち切れずに Web ブラウザアプリケーションでタイムアウトが発生するものもあった。Windows Vista における IE7 は、約 105 秒でタイムアウトが発生した。タイムアウトが発生した場合、Web ブラウザアプリケーションを終了せずに「更新」ボタンを押下すると、タイムアウト発生前までに接続を試みた RR へ再度接続することはせず、次点の RR から順に接続を開始する。本検証の構成の場合、ブラウザアプリケーションの「更新」ボタン押下後は TCP/IPv4 への接続が直ちに行われ WWW サーバと通信が確立された。

2.2.8 検証データ

DNS に設定した AAAA RR および A RR は以下の通り。

www	A	211.132.XXX.5
	AAAA	2001:db8:1001:1001::80
	AAAA	2001:db8:1001:1001::a:80
	AAAA	2001:db8:1001:1001::b:80
	AAAA	2001:db8:1001:1001::c:80
	AAAA	2001:db8:1001:1001::d:80

IE7 ブラウザにて WWW サーバへ接続を実施したときのパケットキャプチャデータを図 2-13 に、TCP シーケンス図を図 2-14 にそれぞれ示す。

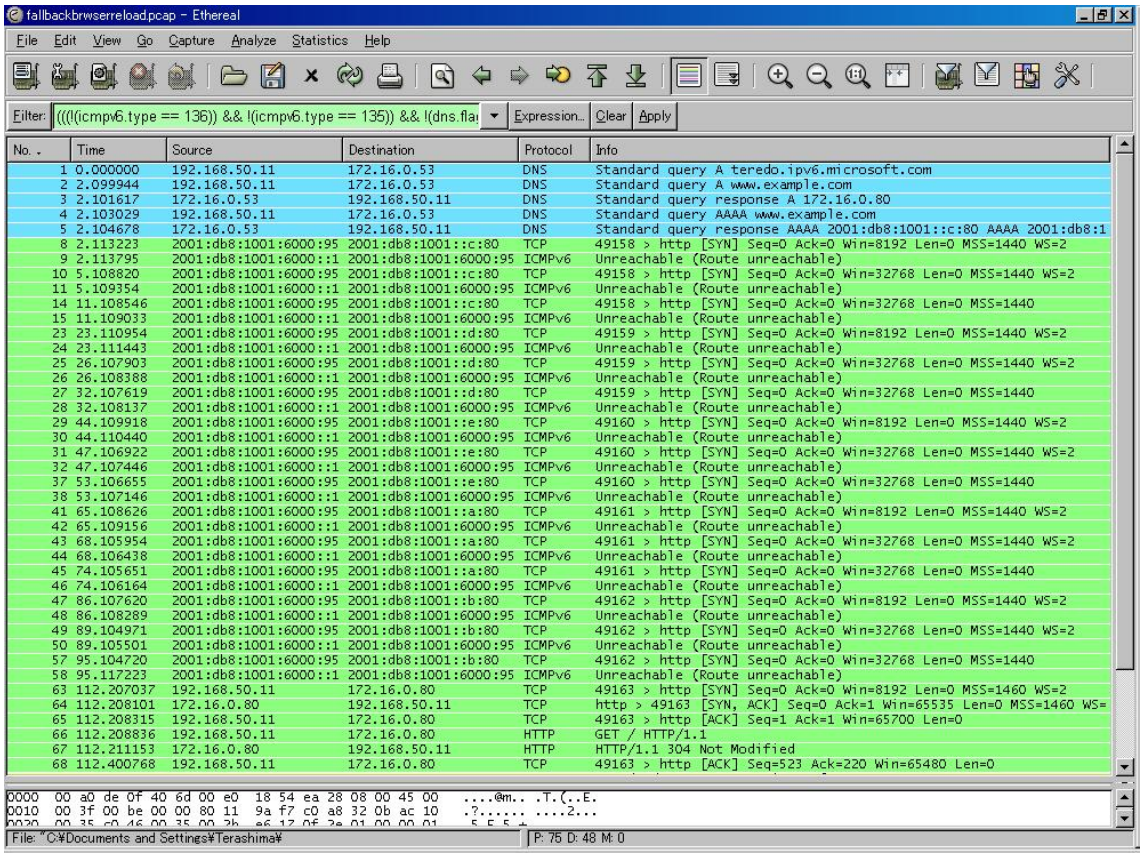

図 2-13　AAAA RR が 5 つ設定された場合のパケットキャプチャデータ

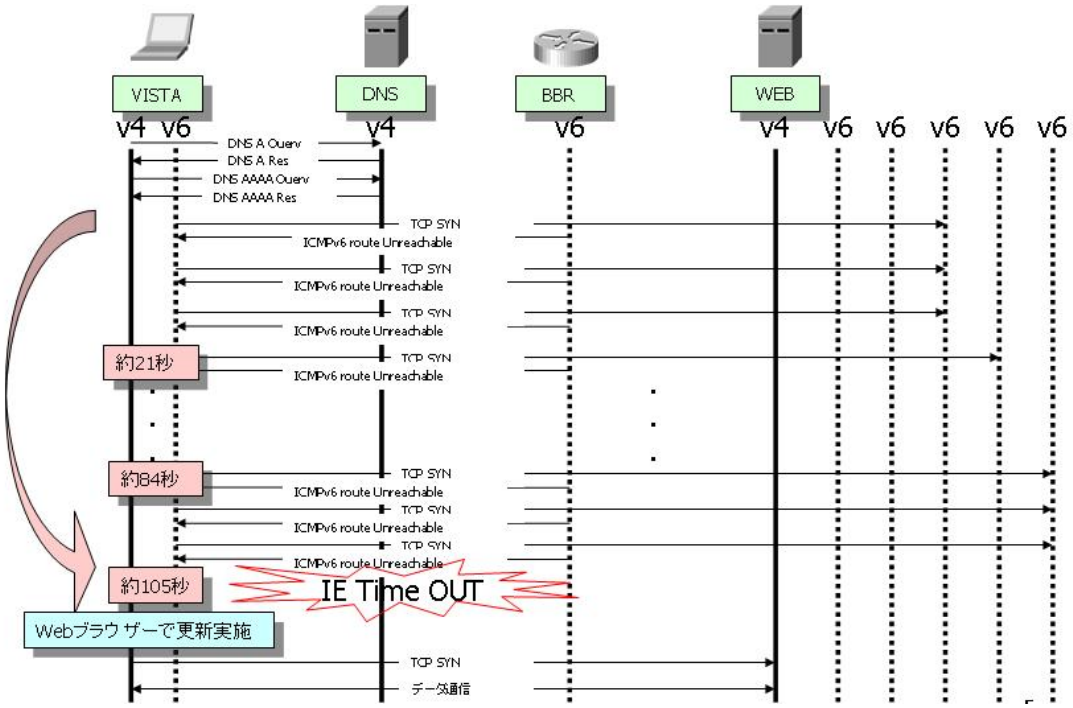

図 2-14　AAAA RR が 5 つ設定された場合のシーケンス図

2.2.9 Windows Vista での PPPoE 接続時の検証

ここではホームユーザにとってシンプルなインターネット接続環境として、PC での PPPoE 接続のケースを取り上げる。

Windows Vista の PPPoE インターフェイスを利用し、インターネット接続サービスを享受しているところに、閉域 IPv6 網が追加される環境を想定する。閉域 IPv6 網が追加されるケースの典型例としては、ホームユーザネットワークに閉域の IPv6 ローカル LAN 環境を作ることや、品質やセキュリティの確保の観点から閉域 IPv6 網を利用して提供されるブロードバンドサービスを受けること等がある。この環境下において、IPv6 対応 OS 端末（Windows Vista）がインターネット上のデュアルスタック構成の WWW サーバに接続を試みた際の挙動について検証した。検証時に利用する Web ブラウザアプリケーションとして IE7 を用いている。

本検証の環境は図 2-15 のようなホームネットワークを想定し、実施した。

- 接続ノードの OS は Windows Vista
- 既存 IPv4 環境は PPPoE 接続で構成
- 共存する閉域 IPv6 環境は、閉域 IPv6 網接続サービスを提供する通信サービス事業者網から広告される RA メッセージを受信することで構成

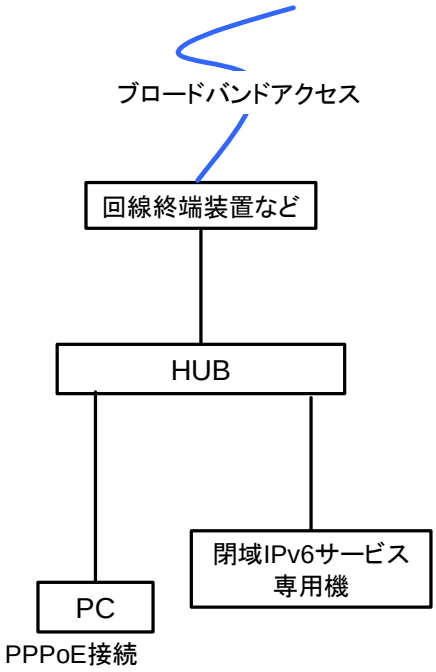

図 2-15　Windows Vista における PPPoE 接続で想定する環境

検証の手順は下記の通りである。

1. IPv6 対応 OS 端末にて、PPPoE を利用してインターネットに接続する。PPPoE では IPv4 のみを設定する。
2. IPv6 対応 OS 端末から AAAA RR と A RR を持つインターネット上の WWW サーバへ接続する。
3. IPv6 対応 OS 端末と WWW サーバ間の通信をキャプチャして解析する。

2.2.10 検証結果

インターネット上のデュアルスタック構成の Web サーバへの接続において、TCP/IPv4 通信だけが発生した。すなわち、このケースでは TCP/IPv6 通信から TCP/IPv4 通信へのフォールバックに待ち時間が発生してしまう現象は起こらなかった。2.2.4 節および 2.2.7 節の結果と異なり、IPv6 通信が発生しなかった理由に関して以下に考察する。

このような挙動となった原因として、ネットワークインターフェイスに付与されたメトリック値の差異が考えられる。PPPoE 接続が確立した状態で、システム上のネットワークインターフェイス情報を「netsh」コマンドで確認（2.2.11 節の検証データの項を参照）すると、PPPoE 接続のネットワークインターフェイスに設定されているメトリック値（検証データ中の Met）が小さくなっていることがわかる。Windows Vista では、このメトリック値が小さいインターフェイスが優先的に利用される実装になっているようで、優先的に利用されるインターフェイスが IPv4 のみであることから A クエリのみ実施（2.1.4 節参照）されたのだと予想される。ただし、これは仮説であり、どのような基準によって PPPoE イ

ンターフェイスが優先的に使用されているのかについては今後のさらなる調査と、それによる断定が必要である。

2.2.11 検証データ

本検証環境の Windows Vista のネットワーク情報を以下に示す。比較のために、PPPoE 接続確立の前後の情報を示す。

- PPPoE接続確立前

インターフェイス情報

```
------------------------------------------------------------------------------
C:¥>ipconfig /all
:
イーサネット アダプタ ローカル エリア接続:

   接続固有の DNS サフィックス . . :
   説明. . . . . . . . . . . . . . : ********
   物理アドレス. . . . . . . . . . : **-**-**-54-EA-28
   DHCP 有効 . . . . . . . . . . . : はい
   自動構成有効. . . . . . . . . . : はい
   IPv6 アドレス . . . . . . . . . : 2001:db8:1234:5678:ad91:da6a:77bc:d648(優先)
   一時 IPv6 アドレス. . . . . . . : 2001:db8:1234:5678:e972:13db:29e4:9f64(優先)
   リンクローカル IPv6 アドレス. . : fe80::ad91:da6a:77bc:d648%8(優先)
   IPv4 アドレス . . . . . . . . . : 169.254.214.72(優先)
   サブネット マスク . . . . . . . : 255.255.0.0
   デフォルト ゲートウェイ . . . . : fe80::*:*:fe61:bc1a%8
   DHCPv6 IAID . . . . . . . . . . : 201383960
   DNS サーバー. . . . . . . . . . : fec0:0:0:ffff::1%1
                                     fec0:0:0:ffff::2%1
                                     fec0:0:0:ffff::3%1
   NetBIOS over TCP/IP . . . . . . : 有効
------------------------------------------------------------------------------
```

◆インターフェイスの確認コマンドの実行結果

```
------------------------------------------------------------------------------
C:¥>netsh interface ipv4 show interface

Idx     Met         MTU          状態                名前
---------------------------------------------------------------------------
1       50          4294967295   connected           Loopback Pseudo-Interface 1
8       20          1500         connected           ローカル エリア接続
------------------------------------------------------------------------------
```

- PPPoE接続確立後

インターフェイス情報

```
C:¥>ipconfig /all
:
PPP アダプタ ブロードバンド接続:

   接続固有の DNS サフィックス . . :
   説明. . . . . . . . . . . . . . : ブロードバンド接続
   物理アドレス. . . . . . . . . . :
   DHCP 有効 . . . . . . . . . . . : いいえ
   自動構成有効. . . . . . . . . . : はい
   IPv4 アドレス . . . . . . . . . : 221.XXX.XXX.248(優先)
   サブネット マスク . . . . . . . : 255.255.255.255
   デフォルト ゲートウェイ . . . . : 0.0.0.0
   DNS サーバー. . . . . . . . . . : XXX.XXX.XXX.XXX
   NetBIOS over TCP/IP . . . . . . : 無効

イーサネット アダプタ ローカル エリア接続:

   接続固有の DNS サフィックス . . :
   説明. . . . . . . . . . . . . . : ********
   物理アドレス. . . . . . . . . . : **-**-**-54-EA-28
   DHCP 有効 . . . . . . . . . . . : はい
   自動構成有効. . . . . . . . . . : はい
   IPv6 アドレス . . . . . . . . . : 2001:db8:1234:5678:ad91:da6a:77bc:d648(優先)
   一時 IPv6 アドレス. . . . . . . : 2001:db8:1234:5678:e972:13db:29e4:9f64(優先)
   リンクローカル IPv6 アドレス. . : fe80::ad91:da6a:77bc:d648%8(優先)
   自動構成 IPv4 アドレス. . . . . : 169.254.214.72(優先)
   サブネット マスク . . . . . . . : 255.255.0.0
   デフォルト ゲートウェイ . . . . : fe80::*:*:fe61:bc1a%8
   DHCPv6 IAID . . . . . . . . . . : 201383960
   DNS サーバー. . . . . . . . . . : fec0:0:0:ffff::1%1
                                     fec0:0:0:ffff::2%1
                                     fec0:0:0:ffff::3%1
   NetBIOS over TCP/IP . . . . . . : 有効
```

◆インターフェイスの確認コマンドの実行結果

```
C:¥>netsh interface ipv4 show interface

Idx     Met         MTU          状態                名前
---------------------------------------------------------------------------
1       4275  4294967295  connected     Loopback Pseudo-Interface 1
16      20          1454  connected     ブロードバンド接続
8       4245        1500  connected     ローカル エリア接続
```

IE7 ブラウザにて WWW サーバへの接続を実施したパケットキャプチャデータを図 2-16 に、TCP シーケンス図を図 2-17 にそれぞれ示す。

No.	Time	Source	Destination	Protocol	Info
1	0.000000	221.[redacted].248	61.[redacted]156	DNS	Standard query A www.kame.net
2	0.001479	61.[redacted]156	221.[redacted].248	DNS	Standard query response A 203.178.141.194
3	0.009029	221.[redacted]248	203.178.141.194	TCP	49275 > http [SYN] Seq=0 Len=0 MSS=1414 WS=8
4	0.011694	203.178.141.194	221.[redacted].248	TCP	http > 49275 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1
5	0.018082	221.[redacted].248	203.178.141.194	TCP	49275 > http [ACK] Seq=1 Ack=1 Win=66304 Len=0
6	0.018672	221.[redacted].248	203.178.141.194	HTTP	GET / HTTP/1.1
7	0.022696	203.178.141.194	221.[redacted]248	HTTP	HTTP/1.1 304 Not Modified
8	0.179918	221.[redacted].248	203.178.141.194	HTTP	GET /style.css HTTP/1.1
9	0.182994	221.[redacted].248	203.178.141.194	TCP	49276 > http [SYN] Seq=0 Len=0 MSS=1414 WS=8

図 2-16　PPPoE 接続を実施した場合のパケットキャプチャ

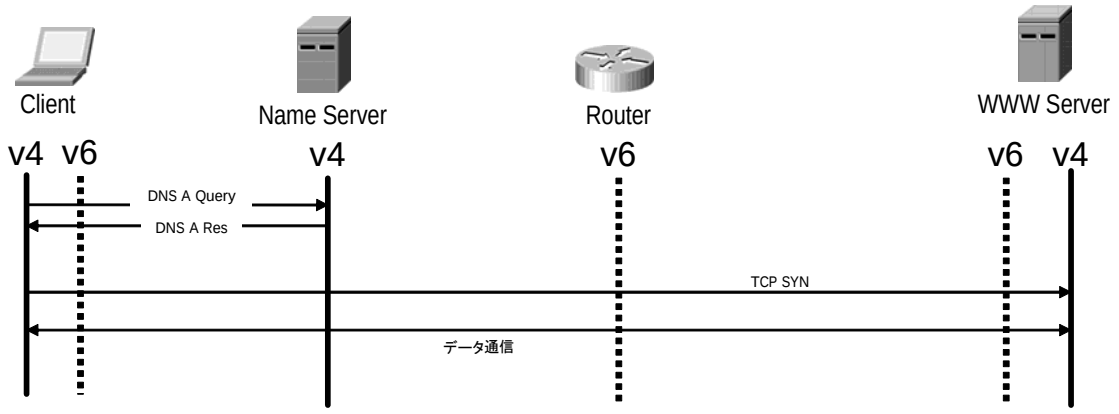

図 2-17　PPPoE 接続を実施した場合のシーケンス図

2.2.12 考察

検証項目 1 の結果より Windows Vista の Windows ファイアウォールには不到達通知に関するフィルタ制限は行われていないため、不到達通知がネットワーク側から送信された場合でも受信することが可能である。

検証項目 2・3 の結果より、Windows Vista では不到達通知を受けることによる挙動の違いは見られなかった。TCP/IPv6 から TCP/IPv4 へのフォールバックが発生するまでの時間は、一律で 21 秒前後となり、内訳は以下の通りである。

TCP/IPv6 再送は 2 回起こり、初回を含めると合計 3 回の TCP/IPv6 通信を試行していた。
1 回目の TCP/IPv6 通信失敗後、2 回目の TCP/IPv6 通信開始までの時間間隔が約 3 秒。
2 回目の TCP/IPv6 通信失敗後、3 回目の TCP/IPv6 通信開始までの時間間隔が約 6 秒。
3 回目の TCP/IPv6 通信失敗の後に、TCP/IPv6 通信をあきらめて TCP/IPv4 通信へフォールバックすることになるが、この IPv4 通信開始までの時間間隔は約 12 秒であった。

約 21 秒　＝　約 3 秒　＋　約 6 秒　＋　約 12 秒

なお、いったん TCP/IPv4 通信へのフォールバックが起きると、IE7 ブラウザでは、それ

以降のアクセスでは Web ブラウザアプリケーションを終了するまではローカルに DNS キャッシュを保持し、すぐに IPv4 通信を開始することを確認した。

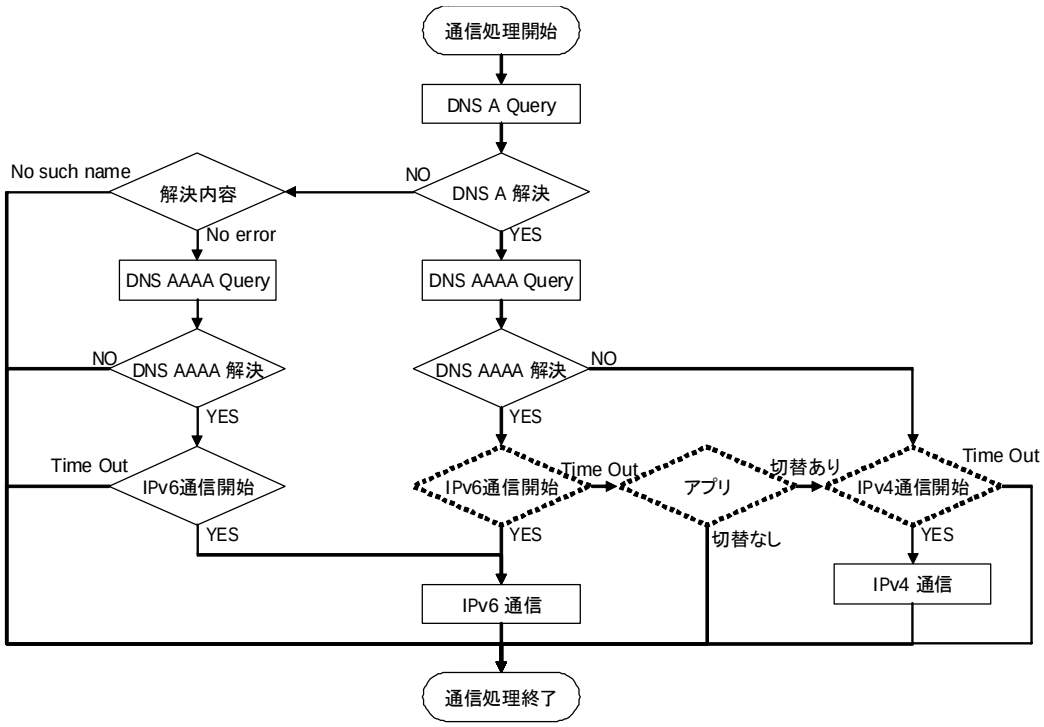

図 2-18　Windows Vista における IPv6 通信フローチャート図

図 2-18 に本検証で利用した Windows Vista での名前解決を伴うアプリケーションの動作について、フローチャート図で示す。ただし、グローバルユニキャスト IPv6 アドレスと IPv4 アドレスの両方がアサインされた物理インターフェイスが、優先的に利用されるネットワークインターフェイスである場合について示した図である。

図 2-18 における破線部分での待ち時間によって、ユーザによっては不快感を示す可能性がある。

この問題について、Windows Vista 利用者側で取り得る問題回避方法例を 2 つ挙げる。

- **対策例1**

RFC3484 のアドレス選択ポリシーテーブル（以下ポリシーテーブル）を利用することで問題回避することが可能である。ポリシーテーブルにおいて、閉域 IPv6 網の IPv6 アドレスプレフィックスの優先度を高く設定し、次点で IPv4 アドレスを意味する IPv4-mapped address（IPv4 射影アドレス　::ffff:0:0/96）を設定する。IPv6 デフォルトゲートウェイへは、これらに続く優先度を設定する。

Windows Vista での具体例を示す。以下に Windows Vista における初期設定のポリシーテーブルを示す。Teredo アドレス以外は、RFC3484 にて初期設定として推奨されているポリシーテーブルとなっている。

```
---------------------------------------------------------------------------
C:¥>netsh interface ipv6 show prefixpolicies
アクティブ状態を照会しています...

優先順位    ラベル  プレフィックス                          （説明）
---------  -----  ----------------------------------
        50      0  ::1/128                       ←      IPv6 localhost Address
        40      1  ::/0                          ←      IPv6 Address
        30      2  2002::/16                     ←      6to4 Address
        20      3  ::/96                        ←      IPv4-compatible Address
        10      4  ::ffff:0:0/96                ←      IPv4-mapped Address
         5      5  2001::/32                     ←      Teredo Address
---------------------------------------------------------------------------
```

ポリシーテーブルでは、送信元アドレスおよび宛先アドレスの両方ともユーザが優先したいアドレスを明示的に指定することが可能である。宛先アドレスの選択では優先度の高いものから選択される。また、送信元アドレスの選択には宛先アドレスと同じラベルのものが選択される。ポリシーテーブルを利用した場合、送信元アドレスの選択の処理は次の順序でおこなわれる。まず、宛先アドレスのラベルを求める。次に送信元アドレスのラベルを求める。宛先アドレス、送信元アドレスそれぞれのラベルを比較して同じラベルの送信元アドレスを選択する。

Windows Vista での初期設定では、IPv6 での通信が優先されるように設定されている。閉域 IPv6 網の次点で、IPv4 通信を優先するためには以下の方法を実施する。(2001:db8::/32 が閉域 IPv6 網のアドレス空間であり、ホームネットワーク環境で広告を受けている RA メッセージに含まれる IPv6 アドレスプレフィックス情報が 2001:db8:1234:5678::/64 であるとする。)

◆アドレス選択ポリシーテーブルの変更

```
C:¥>netsh interface ipv6 <set | add> prefixpolicy <prefix> <precedence> <label>  ☆
---------------------------------------------------------------------------
C:¥>netsh interface ipv6 set prefixpolicy ::1/128 50 0                        ☆
C:¥>netsh interface ipv6 add prefixpolicy 2001:db8::/32 45 1                  ☆
C:¥>netsh interface ipv6 add prefixpolicy 2001:db8:1234:5678::/64 45 1        ☆
C:¥>netsh interface ipv6 add prefixpolicy ::ffff:0:0/96 40 2                  ☆
C:¥>netsh interface ipv6 add prefixpolicy ::/0 30 3                           ☆
C:¥>netsh interface ipv6 add prefixpolicy 2002::/16 20 4                      ☆
C:¥>netsh interface ipv6 add prefixpolicy ::/96 10 5                          ☆
C:¥>netsh interface ipv6 add prefixpolicy 2001::/32 5 6                       ☆
---------------------------------------------------------------------------
```

上記コマンドを実行することにより、アドレス選択ポリシーテーブルは次のように変更される。

```
---------------------------------------------------------------------------
C:¥>netsh interface ipv6 show prefixpolicies
アクティブ状態を照会しています...

優先順位    ラベル  プレフィックス                          （説明）
---------  -----  ------------------------------
        50      0  ::1/128                        ←      IPv6 localhost Address
        45      1  2001:db8::/32                  ←      Closed IPv6 Address
        45      1  2001:db8:1234:5678::/64       ←      Home NW IPv6 Address
        40      2  ::ffff:0:0/96                 ←      IPv4-mapped Address
        30      3  ::/0                           ←      IPv6 Address
        20      4  2002::/16                      ←      6to4 Address
        10      5  ::/96                         ←      IPv4-compatible Address
         5      6  2001::/32                     ←      Teredo Address
---------------------------------------------------------------------------
```

ポリシーテーブルに、この設定を施したWindows Vistaが通信を開始する場合、閉域IPv6通信→IPv4通信→IPv6通信の順番で通信が行われる。この対策例で示したアドレス選択ポリシーテーブルでは、いずれIPv6が普及し、インターネット接続可能なIPv6サービスに加入した際にも、インターネット上のIPv6/IPv4デュアルスタックサイトへの接続にIPv4通信を優先的に利用することになってしまう点に注意が必要である。ネットワーク利用のそれぞれの場面で、自らが望む通信が可能になるようにポリシーテーブルを設定していかなくてはならない。

- **対策例2**

IPv6対応OS端末が起動時に同一リンク上にあるIPv6ルータとの間で交わすRSメッセージ/RAメッセージのやりとりによって、端末が自身に設定するネットワーク情報を削除すると伴に、閉域IPv6網のIPv6アドレスプレフィックスをルーティングテーブルに追加することで問題回避することが可能である。

Windows Vistaでの具体例を示す。コマンドプロンプトから次のnetshコマンドを実行する。

◆ルーティングテーブルからIPv6デフォルトゲートウェイを削除
C:¥>netsh interface ipv6 delete route ::/0 <interface> <nexthop> ☆
◆ルーティングテーブルに閉域IPv6網のIPアドレスプレフィックスを追加
C:¥>netsh interface ipv6 add route <prefix> <interface> <nexthop> ☆

ただし、IPv6ルータから定期的にRAメッセージが送信される場合は、その都度デフォルトゲートウェイの削除が必要となる。定期的に送信されるRAメッセージを受信しない方法としては次の2つの方法がある（5.1.6節参照）。

この対策例を実施した場合、いずれIPv6が普及し、インターネット接続可能なIPv6サ

ービスに加入した際にも、インターネット上の IPv6/IPv4 デュアルスタックサイトへの接続に IPv4 通信を優先的に利用してしまうことに注意が必要である。

なお、RFC4191 にて規定されている RA の経路情報通知オプションを利用することで、前述した netsh コマンドと同様の設定をルータから付与することができる。この経路情報通知オプションの挙動検証は 5.5.2 節以降で詳しく述べる。

2.2.13 関連する検討

下記にこのフォールバック問題について関連する検討を示す。

http://v6fix.net/docs/v6fix.html.ja#sec4
http://www.janog.gr.jp/meeting/janog17/abstract.html#p04
http://www.janog.gr.jp/meeting/janog18/program-abstract.html#P1
UNIX magazine 2006 年 10 月号 [P.128～P.130]

3 周辺アプリ・機器との連携に関する課題と検討結果

本章では、周辺アプリケーションとネットワーク機器への影響を中心に、IPv6 対応した端末 OS が既存のサービスを利用する際の注意点について議論する。

3.1 キャプティブポータル接続環境での利用

3.1.1 問題の背景と概要

キャプティブポータルとは、Web ブラウザで最初に外部サイトへのアクセスを行う際に強制的に認証ページが表示され、そこで認証・課金を行う仕組みである（図 3-1 参照）。ホテルのインターネット接続サービス、無線 LAN サービスなどでしばしば採用されており、ほとんどの場合 IPv4 サービスに限定されていて、IPv6 では利用できない。

このキャプティブポータルを、IPv6 をインストールしたデュアルスタックの端末を用いて利用した場合、一部の環境では Web ページにアクセスできないケースがあった。つまりキャプティブポータルにおいては、端末がデュアルスタックな状態で、IPv4 サービスが使えないといった問題が生じるケースがある。例えば、キャプティブポータルサーバが提供する DNS 機能が、存在しない DNS リソースレコードに対して、常に特定の A 応答を返す実装になっている際には問題が生じていた。これには、IPv6 端末 OS が、DNS に問い合わせたリソースレコード（AAAA）の種類と、その応答として返ってきた種類（A）が合致していなくても受理するということも影響している[6]。

3.1.2 検証手順

IPv6 端末を使用してキャプティブポータルサービス利用時に問題が生じるのは、端末が AAAA クエリを送出し、利用しているキャプティブポータルサーバがその AAAA クエリに A 応答を返す仕様になっていて、かつ端末がその不正応答（クエリの種類（AAAA）と応答の種類（A）が異なっている）を受理する時である。そのため端末が AAAA クエリを行わなければ問題が生じることはない。このことを踏まえ Windows Vista においてキャプティブポータルサービス問題が解決されているかどうかを調査するため、具体的に以下の 2 項目の検証を行う。

1. Windows Vista がどのような IP アドレス付与状況下で AAAA クエリを出すかを調査する。また調査結果からキャプティブポータルサービス利用に問題が生じる可能性がある IP アドレス付与状況を抽出する。
2. AAAA クエリに対する A 応答を Windows Vista が受理するかどうかを検証する。

[6] ホテル接続環境に関する調査報告（WIDE v6fix WG）：http://v6fix.net/docs/hotel.html.ja

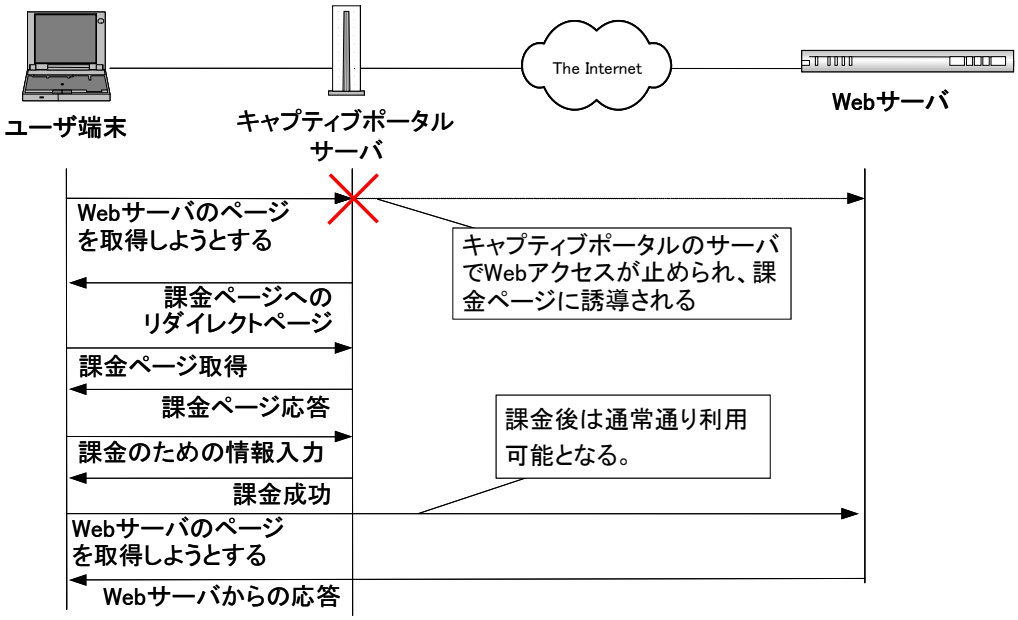

図 3-1　キャプティブポータル概要

各項目の検証手順は以下の通りである。

- **検証項目1**

1. 初期設定の Windows Vista を準備する。
2. IPv4 回線に Windows Vista を接続し、下記 2 通りの環境を構築する。
   ① 端末に IPv4 プライベートアドレスが付与される環境（PPPoE を BB ルータ等の上位ネットワーク装置で終端する NAT 配下環境）
   ② 端末に IPv4 グローバルアドレスが付与される環境（Windows Vista 自身で PPPoE を終端し、"PPP アダプタ"に IPv4 グローバルアドレスが付与され優先的なインターフェイスとして振舞う環境（2.2 章参照））

   続いて、①，②それぞれの環境で、“特に何もしない（初期設定）”、“手動で IPv6 アドレスを設定”、“IPv6-RA を上位 NW から流し自動構成によって IPv6 アドレスを設定” を実施した環境を構築する。以上の作業により全部で 6 通りの環境が構築されることになる。
3. パケットアナライザを配置する。
4. IE7 ブラウザで、どこかの Web ページを表示する。
5. DNS とのパケットのやり取りをアナライザでキャプチャし、解析する。
6. AAAA クエリが発生しているかどうかを確認する。

- **検証項目2**

1. AAAA クエリに対して特定の A レコード（172.31.0.1）を返す DNS を立てる（Perl module の Net::DNS::Server を使用）。
2. パケットアナライザを配置する。
3. IPv6/IPv4 デュアル回線に Windows Vista を接続する。
4. Windows Vista で IPv4 の DNS 指定欄に 1.で構築した DNS サーバアドレスを手動指定する。
5. IE7，Firefox，Opera 等の Web ブラウザで、どこかの Web ページを表示する。
6. DNS とのパケットのやり取りをアナライザでキャプチャし、解析する。

検証項目 2 の検証構成図を図 3-2 に示す。

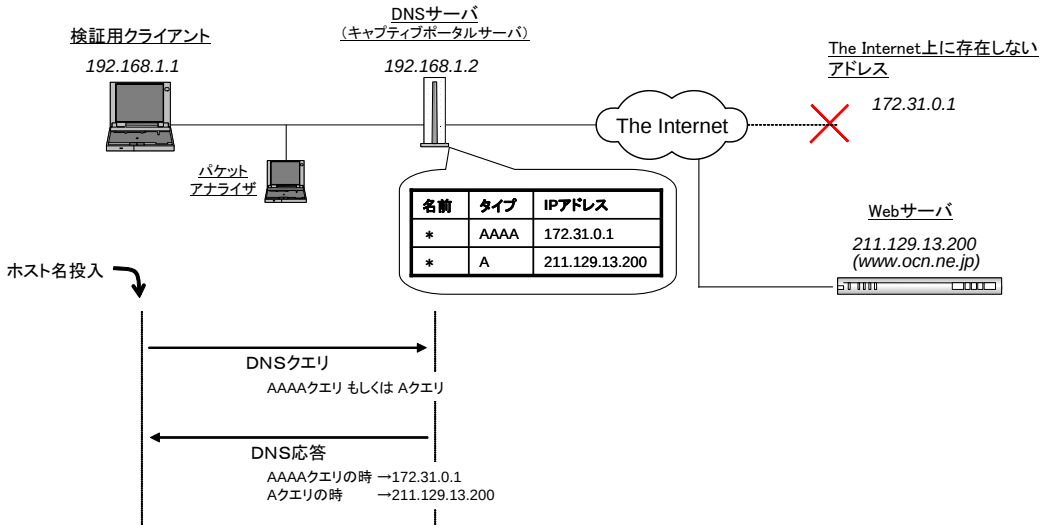

図 3-2　検証項目 2 の検証構成図

3.1.3 検証結果

- **検証項目1**

表 3-1 に構築した 6 通りの環境下での、Windows Vista に付与される IPv6 アドレス状況と、その状況下での各 DNS クエリ（AAAA，A）有無の関係を示す。表中 Teredo や 6to4 は“特に何もしない（初期設定)”の時に Windows Vista 端末に自動で設定される IPv6 アドレスである（4.1 節参照)。

6 通りの状況において AAAA クエリを送出するのは次の場合となる（表 3-1 中に黄色で示した)。

① 端末に IPv4 プライベートアドレスが付与される環境で、かつ IPv6 アドレスを手動設定している Windows Vista

② 端末に IPv4 プライベートアドレスが付与される環境で、かつ上位ネットワークから RA を受信している Windows Vista

③ 端末に IPv4 グローバルアドレスが付与される環境で、かつ初期設定により 6to4 アドレスが付与された Windows Vista

表 3-1　端末に付与された IPv6 アドレス状況と DNS クエリ送出の関係

クエリ送出	IPv4 プライベートアドレス環境 (注 1)			IPv4 グローバルアドレス環境 (注 2)		
	初期設定（teredo）	IPv6 アドレス手動設定 (注 3)	RA (注 3)	初期設定（6to4）	IPv6 アドレス手動設定 (注 3)	RA (注 3)
AAAA	×	○	○	○	×	×
A	○	○	○	○	○	○

（注 1）　ブロードバンドルータ等で PPP を終端し、配下端末には NAT で IPv4 プライベートアドレスが配布される環境

（注 2）　Windows Vista で PPPoE を終端し、”PPP アダプタ”に IPv4 グローバルアドレスが付与され優先的なインターフェイスとして振舞う環境（2.2.9 節参照）

（注 3）　”ローカルエリア接続”に IPv6 アドレスが設定されるものとした場合

- **検証項目2**

以下に、検証項目 2 の環境下での Windows Vista において、どこかの Web ページを表示した時のパケットキャプチャ結果とブラウザのスクリーンキャプチャ結果を、検証に用いた Web ブラウザ毎に示す。また、参考として Windows XP SP2 を利用した時の検証データも示す（図 3-9)。なお下記データでは 192.168.1.1 のアドレスを持つ端末は検証用クライアント（Windows Vista or Windows XP SP2）を、同様に 192.168.1.2 は AAAA クエリに対して存在しないアドレスを含む不正な A 応答を出す DNS サーバを表している。

◆Internet Explorer

検証データから、AAAA クエリに対する A 応答（172.31.0.1）を不正として検知し、無効なアドレスへのクエリであると判定し、検索サイトへと移行しようとしているものと思われる。つまり IE7 を利用した場合 DNS に問い合わせたリソースレコードの種類と、その応答として返ってきた種類が合致していない場合はこれを受理しないと言える。ただし、検索サイトへ移行するのみで、正常な DNS 応答（検証データでは A クエリ（www.ocn.ne.jp）に対する A 応答（211.129.13.200））のアドレスを使った接続へのフォールバックはしない。図 3-3 と図 3-4 に検証結果を示す。

◆Firefox

検証データから、AAAA クエリに対する応答 A,172.31.0.1 を受理し、そのアドレスへ接続しようとしている。つまり Firefox を利用した場合、DNS に問い合わせたリソースレコードの種類と、その応答として返ってきた種類が合致していない場合でも、これを受理する。ここでは 172.31.0.1 はインターネット上に存在しないアドレスのため、接続に失敗する。図 3-5 と図 3-6 に検証結果を示す。

◆Opera

Firefox と同様。図 3-7 と図 3-8 に検証結果を示す。

以上の結果から OS のリゾルバ機能としては、DNS クエリに応答を全て受理し、その応答を利用するか否かは各アプリケーション（ここでは Web ブラウザ）に委ねているものと思われる。

3.1.3.1 検証データ

以下に検証データをまとめる。

```
#No, Source IP, Destination IP, Protocol, Infomation
1, 192.168.1.1, 192.168.1.2, DNS, Standard query A www.ocn.ne.jp
2, 192.168.1.2, 192.168.1.1, DNS, Standard query response A 211.129.13.200
3, 192.168.1.1, 192.168.1.2, DNS, Standard query AAAA www.ocn.ne.jp
4, 192.168.1.2, 192.168.1.1, DNS, Standard query response A 172.31.0.1
5, 192.168.1.1, 192.168.1.2, DNS, Standard query A www.google.co.jp
6, 192.168.1.2, 192.168.1.1, DNS, Standard query response A 211.129.13.200
7, 192.168.1.1, 192.168.1.2, DNS, Standard query AAAA www.google.co.jp
8, 192.168.1.2, 192.168.1.1, DNS, Standard query response A 172.31.0.1
 :
```

AAAA クエリに対する A 応答を無視

図 3-3 Windows Vista（Internet Explorer 7.0）でのキャプチャデータ

図 3-4　Internet Explorer7.0 での検証結果

```
#No, Source IP, Destination IP, Protocol, Infomation
1, 192.168.1.1, 192.168.1.2, DNS, Standard query A www.ocn.ne.jp
1, 192.168.1.1, 192.168.1.2, DNS, Standard query A www.ocn.ne.jp
2, 192.168.1.2, 192.168.1.1, DNS, Standard query response A 211.129.13.200
3, 192.168.1.1, 192.168.1.2, DNS, Standard query AAAA www.ocn.ne.jp
4, 192.168.1.2, 192.168.1.1, DNS, Standard query response A 172.31.0.1
5, 192.168.1.1, 172.31.0.1, TCP 1141 > http, [SYN] Seq=0 Len=0 MSS=1460
 :
```

AAAA クエリに対する A 応答を受理

図 3-5　Windows Vista（Firefox 2.0.0.1）でのキャプチャデータ

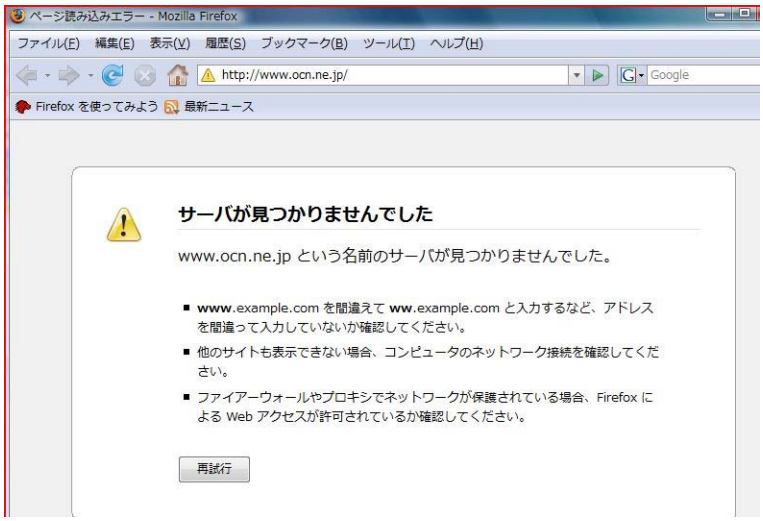

図 3-6　Firefox 2.0.0.1 での検証結果

```
#No, Source IP, Destination IP, Protocol, Infomation
1, 192.168.1.1, 192.168.1.2, DNS, Standard query A www.ocn.ne.jp
2, 192.168.1.2, 192.168.1.1, DNS, Standard query response A 211.129.13.200
3, 192.168.1.1, 192.168.1.2, DNS, Standard query AAAA www.ocn.ne.jp
4, 192.168.1.2, 192.168.1.1, DNS, Standard query response A 172.31.0.1
5, 192.168.1.1, 172.31.0.1, TCP 1141 > http, [SYN] Seq=0 Len=0 MSS=1460
 :
```

AAAA クエリに対する A 応答を受理

図 3-7　Windows Vista（Opera 9.10）でのキャプチャデータ

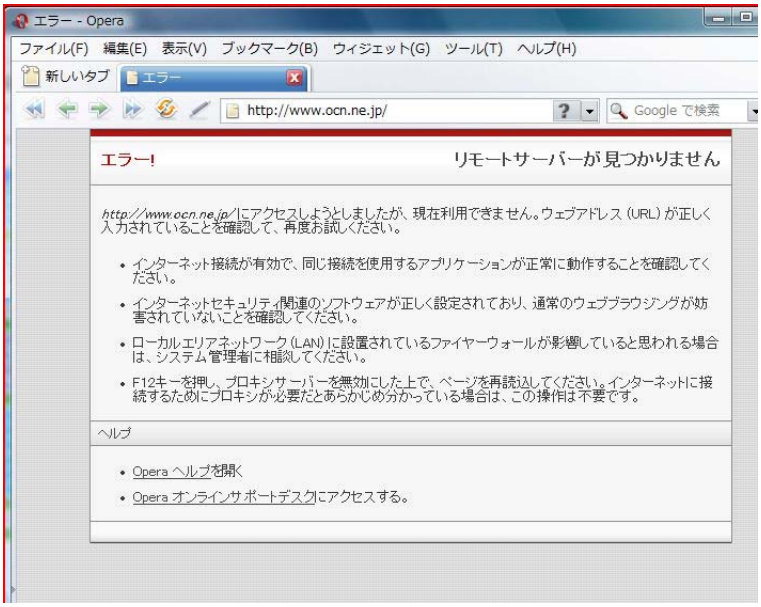

図 3-8　Opera 9.10 での検証結果

```
#No, Source IP, Destination IP, Protocol, Infomation
1, 192.168.1.1, 192.168.1.2, DNS, Standard query A www.ocn.ne.jp
1, 192.168.1.1, 192.168.1.2, DNS, Standard query AAAA www.ocn.ne.jp
2, 192.168.1.2, 192.168.1.1, DNS, Standard query response A 172.31.0.1
3, 192.168.1.1, 172.31.0.1, TCP 1141 > http, [SYN] Seq=0 Len=0 MSS=1460
4, 192.168.1.1, 172.31.0.1, TCP 1141 > http, [SYN] Seq=0 Len=0 MSS=1460
 :
```

AAAA クエリに対する A 応答を受理

図 3-9　Windows XP SP2（Internet Explorer 6.0）

3.1.4 考察

検証項目 1 の結果から、Windows Vista のリゾルバは自端末に IPv4 プライベートアドレスのみ付与されている時（Teredo アドレスを除く）には AAAA クエリを行わないため（2.1 節参照）、「DNS に問い合わせたリソースレコードの種類と、その応答として返ってきた種類が合致していなくても、端末の DNS リゾルバが受理する」という状況自体が発生しない。したがって、一般的に IPv4 サービスに限定され IPv4 プライベートアドレスを付与するキ

ャプティブポータルサービス下では、ユーザは Windows Vista を利用してサービスに問題なく接続できると言える。

ただし、次のような環境下では Windows Vista のリゾルバは AAAA クエリを行う。

① 手動で IPv6 グローバルアドレスを端末に設定している場合

② IPv6 対応のキャプティブポータルサービスを利用する場合

③ IPv4 グローバルアドレスを端末に割り振るキャプティブポータルサービスを利用する場合

これらの場合において、かつ利用するキャプティブポータルサービスのサーバが提供している DNS 機能で AAAA RR が存在しない時に適当な A 応答を返す実装になっている時には、各 Web ブラウザは、不正応答を拒絶するが正常応答のアドレスを使った接続へ移行しない、もしくは不正応答のアドレスを受理するため、キャプティブポータルサービスに接続できないといった問題が生じる可能性がある。

この点についてはキャプティブポータルサービス側の DNS 機能の改善が求められるが、IPv6 端末についても OS もしくは Web ブラウザとしての改善の余地がある。それまでの暫定的な対処策は以下の通りである。

A) IPv6 アドレス手動設定時に問題に遭遇した時の対策（以下のいずれかの方法を端末で実施）

a) 手動設定 IPv6 アドレスの消去

"ローカル エリア接続のプロパティ"の"インターネット プロトコル バージョン 6 (TCP/IPv6)のプロパティ"で「IPv6 アドレスを自動的に取得する」に変更

b) IPv6 機能の停止

"ローカル エリア接続のプロパティ"で"インターネット プロトコル バージョン 6(TCP/IPv6)"のチェックを外す

B) IPv6 を提供するキャプティブポータルサービスに接続した際に問題に遭遇した時の対策（以下のいずれかの方法を端末で実施）

a) RA 受信機能を無効化

コマンドプロンプトで、下記コマンドを実施

```
C:¥>netsh interface ipv6 set interface <id> routerdiscovery=disabled      ☆
```

※ <id>には利用しているインターフェイス ID を指定する

b) IPv6 機能の停止

"ローカル エリア接続のプロパティ"で"インターネット プロトコル バージョン 6（TCP/IPv6）"のチェックを外す

C) IPv4 グローバルアドレスを割り振るキャプティブポータルサービスに接続した際に問題に遭遇した時の対策（以下の方法を端末で実施）

a) 6to4 機能を無効化

コマンドプロンプトで、下記コマンドを実施

```
C:¥>netsh interface ipv6 6to4 set state disable                           ☆
```

3.2 Proxy サーバへの HTTP クエリの IPv6 対応状況

3.2.1 問題の背景と概要

IPv6、IPv4 の両者に対応する Proxy が提供されつつある。Windows Vista に標準搭載された Web ブラウザである IE7 が、

- IPv6 対応の Proxy を指定できるか
- Proxy サーバへの HTTP クエリとして IPv6 を用いるか

を検証する。

3.2.2 検証手順

下記の手順に従って検証を行った。

1. デュアルスタック Proxy サーバ（例：Apache）を立てる。
2. IPv6/IPv4 デュアル回線に Proxy サーバ、Windows Vista を接続する。
3. IE7 の Proxy 設定欄に 1.のマシンの IPv6 アドレスを設定する。
4. Windows Vista から送出されるパケットを監視できるようにパケットアナライザを配置し、キャプチャする。
5. IE7 で IPv6 対応 Web ページを閲覧する。
6. 5.の時のパケットが IPv6 かどうかをアナライザで知る。

3.2.3 検証結果

IE7 の Proxy 設定欄では Proxy サーバの IPv6 アドレスを[ ]で括ることによって設定できた。またサイト閲覧時の Proxy サーバへの HTTP クエリには IPv6 を用いていることがパケットキャプチャ結果から確認できた。

3.2.4 考察

Windows Vista では Windows XP SP2 同様、Proxy サーバへの HTTP クエリに IPv6 を用いる。これは所望の動作であり、Windows Vista を使用することよって何らかの問題が生じるということはないと思われる。

4 IPv6 端末 OS 実装上の課題と検討結果

本章では、IPv6 端末 OS における実装上の特にセキュリティに関する課題を中心に議論する。IPv4 しか利用しないネットワーク環境下においても、本章で取り上げる項目の理解がないと管理者および利用者が意図していない IPv6 通信が可能となってしまうため十分な注意が必要である。

4.1 自動トンネル機能

4.1.1 問題の背景と概要

IPv6 端末 OS においては、IPv4 接続のみが提供されている回線に接続している時でも IPv6 接続を可能とするサービスが提供されていることがある。例えば 6to4 というサービスを使うとグローバル IPv4 アドレスから生成される特別な IPv6 アドレスを使うことで、IPv6 インターネットへのアクセスが可能となる。端末 OS の実装によっては、インターネットに接続すると何の追加設定もなく 6to4 サービスが起動するものもあり、IPv6 を意識して利用する者にとっては非常に便利なものである。

例えば Windows Vista には Teredo と 6to4 という自動トンネル機能が実装されている。以下に各機能に関して簡単にまとめる。

4.1.2 自動トンネル機能の解説

- Teredo（RFC4380）

Teredo は、NAT の内側から IPv4 UDP カプセリングによって IPv6 インターネットへの到達を実現するプロトコルで、設定されるトンネルインターフェイスには、Teredo 用の IPv6 アドレス空間（2001:0000::/32）から/128 のアドレスが 1 つだけ付与される。Teredo を実現する構成要素として Teredo クライアント、Teredo サーバ、Teredo リレーがある。

Teredo クライアントは、Windows Vista に標準実装されており、Teredo サーバと通信して Teredo ベースの IPv6 アドレスの構成元となるアドレスプレフィックスを取得する。Teredo サーバは、Teredo クライアントのアドレス構成支援、および Teredo クライアントと他の Teredo クライアント間の通信転送を行う。また、IPv4 インターネット上の Teredo クライアントと IPv6 ホスト間でパケットを転送する Teredo リレー機能も有する場合には、Teredo クライアントと IPv6 ホスト間の初期通信支援を行う。

なお、Windows Vista に実装されている Teredo では、Teredo サーバとして初期設定で”teredo.ipv6.microsoft.com”が指定されている。

- 6to4（RFC3056）

6to4 は、IPv4 グローバルアドレスが付与された場合に設定されるトンネル接続プロトコルで、設定されるトンネルインターフェイスには IPv4 グローバルアドレスを基にしたプレフィックス（2002:<IPv4 address>::/48）が付与される。したがって、6to4 トンネルが作られた端末は、自身の配下に/48 のアドレス空間を持つことが可能となる。また、IPv6 ネットワークとの相互接続には 6to4 リレーが用いられる。

なお、Windows に実装されている 6to4 では 6to4 用の IPv6 アドレス空間（2002::/16）から/128 のアドレス（2002:<IPv4 address>::<IPv4 address>/128）が 1 つだけ付与される。また、6to4 リレーとして初期設定で”6to4.ipv6.microsoft.com”が指定されている。

4.1.3 検証内容

本節では、Windows Vista の自動トンネル機能を調査するため、初期設定の Windows Vista において、以下の 2 項目の検証を行う。

1. Teredo アドレス、6to4 アドレスが自動的に付与される挙動の確認。
2. Teredo アドレス、6to4 アドレスを使った通信の確認。

検証項目 2 の検証通信経路としては、Teredo については図 4-1 の 3 通りを、6to4 については図 4-2 の 2 通りをそれぞれ確認する。

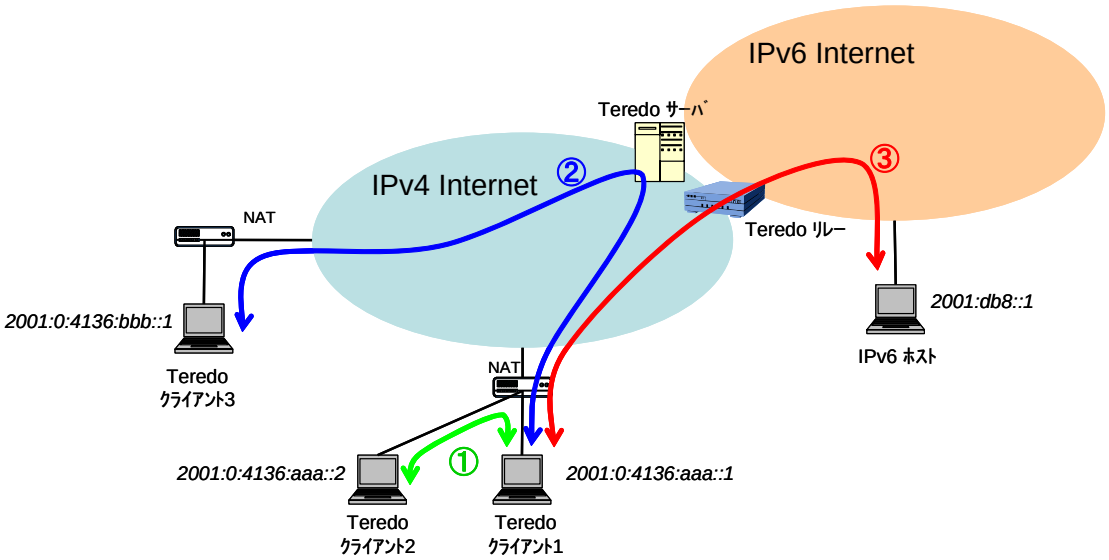

図 4-1　検証した通信経路（Teredo）

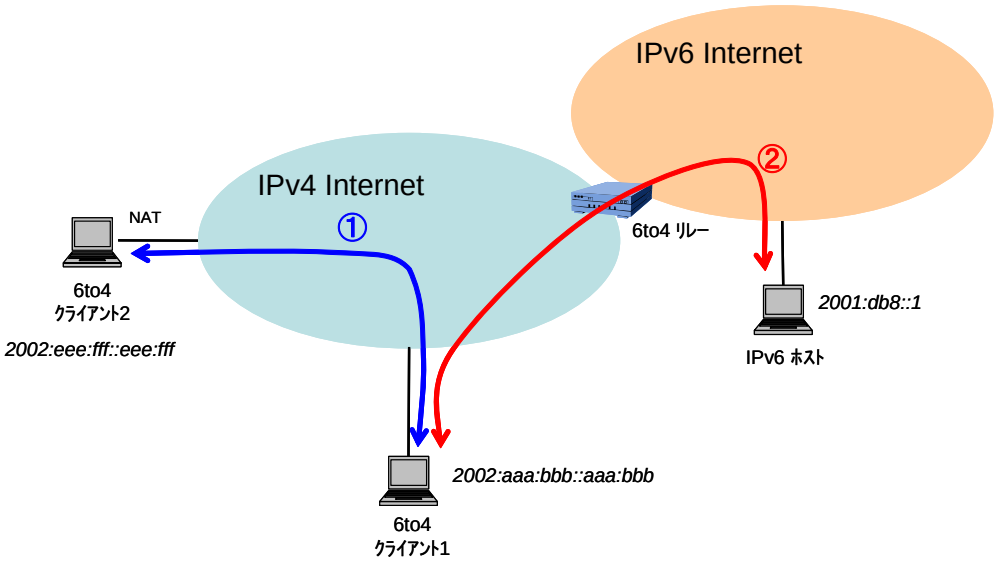

図 4-2　検証した通信経路（6to4）

4.1.4 検証手順

- 検証項目1

【Teredo】

1. IPv4 プライベートアドレスが付与されるネットワーク（NAT 配下）に Windows Vista を接続。
2. ipconfig /all で " Tunnel adapter ローカル エリア接続(説明：Teredo Tunneling Pseudo-Interface)"に IPv6 アドレスが付与されているかどうかを確認

【6to4】

1. IPv4 グローバルアドレスが付与されるネットワークに Windows Vista を接続。
   （実験では Windows Vista にイーサケーブルを直接接続した状態で OCN に PPPoE 接続して IPv4 グローバルアドレスを付与）
2. ipconfig /all で "Tunnel adapter ローカル エリア接続（説明：Microsoft 6to4 Adapter）"に IPv6 アドレスが付与されているかどうかを確認

- 検証項目2

【Teredo】

1. 基準となる Windows Vista を Teredo クライアント 1 として、IPv4 プライベートアドレスが付与されるネットワーク（NAT 配下）に接続する。
2. 疎通確認先として、Teredo クライアント 1 と同じルータ配下に設置した Windows Vista（Teredo クライアント 2)、クライアント 1 と異なるルータ配下に設置した Windows Vista （Teredo クライアント 3)、IPv6 ネットワーク上に IPv6 ホストをそれぞれ構築する（図 4-1 参照)。

3. 図 4-1 中の 3 通りの通信経路について、相手の Teredo アドレスもしくは IPv6 アドレスを指定して ping によりそれぞれ疎通確認を行なう。

【6to4】

1. 基準となる Windows Vista を 6to4 クライアント 1 として、IPv4 グローバルアドレスが付与されるネットワークに接続する。
2. 疎通確認先として、クライアント 1 と異なるルータ配下に設置した Windows Vista（6to4 クライアント 2)、IPv6 ネットワーク上に IPv6 ホストをそれぞれ構築する（図 4-2 参照)。
3. 図 4-2 中の 2 通りの通信経路について、相手の 6to4 アドレスもしくは IPv6 アドレスを指定して ping によりそれぞれ疎通確認を行なう。

4.1.5 検証結果

- **検証項目1**

IPv4 プライベートアドレスが付与された Windows Vista には、初期設定で Teredo 自動トンネルが張られる。IPv4 だけのネットワーク環境で IPv4 グローバルアドレスが付与された Windows Vista には、初期設定で 6to4 自動トンネルが張られる。ただし Teredo の起動には、【パーソナルファイアウォール】をオンにしておく必要がある (A.2 節参照)。また、RA により IPv6 アドレスが設定される環境下では 6to4 が機能することはない。

- **検証項目2**

【Teredo】

起動後しばらく経った後に以下のように Teredo 接続可能状態となった端末を使用して各経路間の接続確認を行った。

```
------------------------------------------------------------------------------
C:¥>netsh interface ipv6 show teredo
Teredo パラメータ
------------------------------------------
種類                    : default
サーバー名              : teredo.ipv6.microsoft.com
クライアント更新間隔    : 30 秒
クライアント ポート     : unspecified
状態                    : qualified
クライアントの種類      : teredo client
ネットワーク            : managed
NAT                     : restricted
------------------------------------------
------------------------------------------------------------------------------
```

その結果、経路間の疎通は以下の通りの結果となった。

- 通信経路①
  ping 疎通可
- 通信経路②
  ping 疎通可
- 通信経路③
  ping 疎通不可

通信経路①の疎通は、パケットキャプチャ結果からルータでの折返し通信となっていることが確認された。このことから、Teredo クライアントが ping 通信時に宛先の Teredo アドレスを見て同一セグメント内かどうかを判定し、同一セグメント配下であれば IPv6 パケットをカプセル化している IPv4 の宛先アドレスを同一セグメント用に変更しているものと思われる。

通信経路②については、Windows 端末間で IPv6 を用いた P2P 通信を促進するといったマイクロソフト社の Teredo に対するコンセプトから、つながることが期待され、本検証でも疎通を確認できた。

また、初期設定の Windows Vista では Teredo サーバとして"teredo.ipv6.microsoft.com"が設定されているが、通信経路③の結果から、このサーバはリレー機能を提供していないものと思われる（2007 年 3 月現在)。そのため通信経路③の通信を実現するにはリレー機能を提供しているサーバへ、以下のコマンドにより手動変更する必要がある。

◆Teredo サーバの変更

```
C:¥>netsh interface ipv6 set teredo client <teredo ｻｰﾊﾞの IPv4 ｱﾄﾞﾚｽ or FQDN 名>  ☆
```

なお、サーバを変更しても Teredo 通信が確立されない時がある。検証を通じて得た Teredo での通信条件に関する知見を以下にまとめておく。

【Teredo 通信条件】

1. Windows Vista 端末で【パーソナルファイアウォール】設定をオンにしておく
2. 上位ルータでのフィルタリング設定で UDP 通信は許可にしておく
3. 他の IPv6-RA は切り、Windows Vista 端末を IPv4 ネイティブな状態にする
   （初期設定では Teredo アドレスが付与されていても、他の IPv6 アドレスが付与されていると、Teredo アドレスの利用を明示的に指定しない限り通信時に利用されないため）
4. 通信先として FQDN は指定しない（IPv6 アドレスを直接指定）

以上の条件を満たしていても Teredo 通信が確立されない時がある。Teredo での疎通可否は経路中で使用する機器の実装に依存するため、この点が影響して失敗する可能性も有り、今後対応機器の洗い出し等更なる調査、検証が必要である。

【6to4】

経路間の疎通は以下の通りの結果となった。

- 通信経路①

  ping 疎通可

- 通信経路②

  ping 疎通可

通信経路①の疎通時のパケットキャプチャ結果データを図 4-3 に示す。パケットキャプチャデータから、通信経路①の時は IPv6 パケットをカプセル化している IPv4 の宛先アドレスが 6to4 クライアント 2 の IPv4 グローバルアドレスになっていることが確認された。これは通信の開始元である 6to4 クライアント 1 が ping 通信時に宛先の IPv6 アドレスを見て 2002::/16 から始まるかどうかをチェックし、2002::/16 から始まるのであれば 6to4 クライアントであると判定し、6to4 クライアントであれば IPv6 パケットをカプセル化している IPv4 の宛先アドレスを宛先 6to4 クライアントの IPv4 グローバルアドレスに変更することによって実現されているものと思われる。

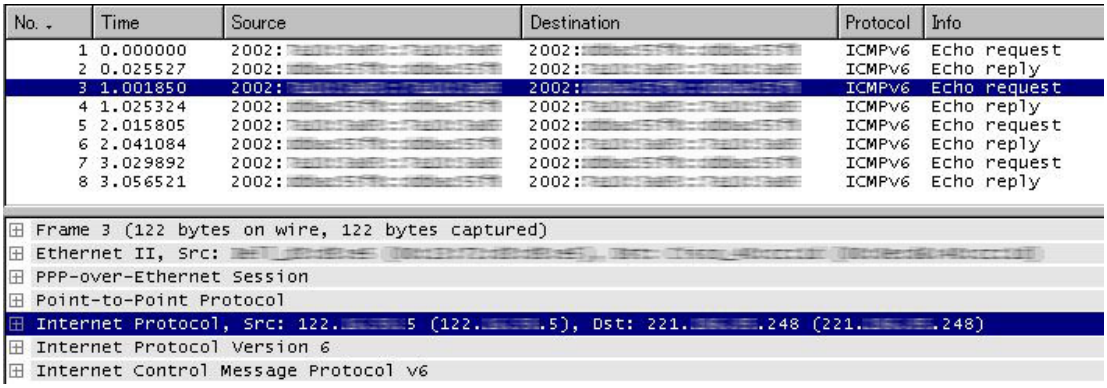

図 4-3　6to4 通信経路①疎通時のパケットキャプチャデータ

通信経路②の疎通時のパケットキャプチャ結果データを図 4-4 に示す。パケットキャプチャデータから、通信経路②の時は IPv6 パケットをカプセル化している IPv4 の宛先アドレスが常に一意の IPv4 グローバルアドレス(192.88.99.1)になっていることが確認された。この IPv4 アドレスは 6to4 リレー用のエニーキャストアドレスで、これを指定することによって経路的に最も近いリレールータが選択される。通信経路①の時同様に通信開始元の

6to4 クライアントが宛先の IPv6 アドレスをチェックして、宛先が IPv6 ホストであればカプセル化している IPv4 の宛先アドレスを 6to4 リレーとし、6to4 リレーを経由することによって IPv6 ホストとの通信を実現している。6to4 アドレスを使って Web ブラウザを用いた IPv6 サイトの閲覧も特に問題なく実施できた（図 4-5）。なお Teredo 同様に、通信先として IPv6 アドレスを直接指定しないと 6to4 は使われないことに注意すべきである。

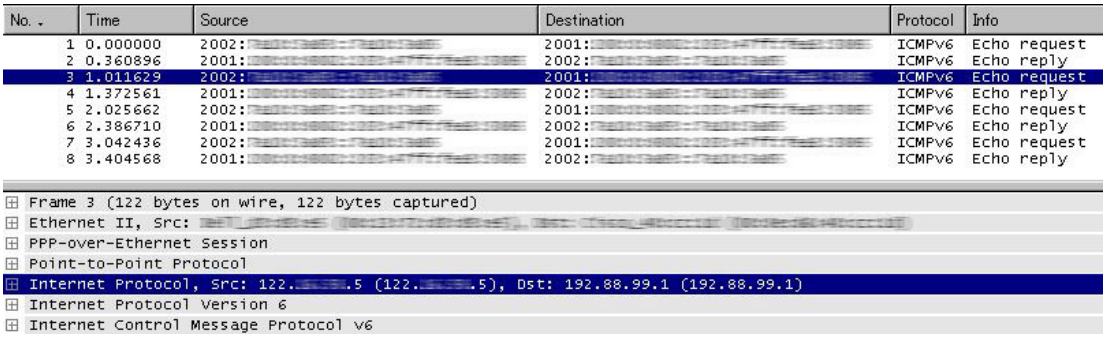

図 4-4　6to4 通信経路②疎通時のパケットキャプチャデータ

図 4-5　6to4 アドレスによる IPv6 サイトの閲覧

4.1.6 考察

Windows Vista では、プライベートの IPv4 アドレスが付与された時には、初期設定で Teredo 自動トンネルが張られる。また、IPv4 だけのネットワーク環境でグローバル IPv4 アドレスが付与された Windows Vista には、初期設定で 6to4 自動トンネルが張られる。両機能は IPv6 を利用したくても IPv6 ネットワーク環境がない場合には、IPv6 を利用したいエンドユーザにとっては非常に便利なものである。

しかしながら、これらのサービスはサービス提供者が用意するサーバへ自動でトンネル接続を行うものがほとんどであり、IPv6 を利用しない者にとっては無意識のうちに意図しない経路ができるためセキュリティのバックドアとなりかねない。そのため、IPv6 端末 OS 利用者やネットワーク管理者は、これらの経路が自動生成されることについて十分注意しておかなければならない。例えば、ネットワーク管理者がこれらの自動トンネルの発生を良しと思わない場合は、Windows Vista ユーザに以下のコマンドをエンドユーザ端末にて実施してもらう等の対処を啓蒙・実施する必要がある。

◆Teredo クライアント機能の停止

```
C:¥>netsh interface teredo set state disable                    ☆
```

◆6to4 クライアント機能の停止

```
C:¥>netsh interface 6to4 set state disable                      ☆
```

4.2　初期状態でオープンしているポート・サービスの認識

4.2.1 問題の背景と概要

IPv6 では、End-End の通信形態が基本となり、IP 端末側の自己防衛がより一層重要となる。Windows Vista は初期設定で IPv6 に対応しているため、初期状態のセキュリティレベルを把握しておく必要がある。一方で、Windows Vista では、セキュリティが強化されたと言われており、IPv6 の基本的な通信までが遮断され、IPv6 通信に影響を及ぼす可能性も考えられる。

そこで、本節では、Windows Vista の初期状態において、Windows ファイアウォールの設定によるパケットフィルタ規則と、オープンしている TCP および UDP ポート番号の調査を行う。

ここで Windows Vista の初期状態とは、「何もインストールされていない PC に、Windows Vista の CDROM から OS をインストールし、ユーザ登録など OS にログインするための必要最低限の項目のみを設定し、LAN ケーブルだけを接続した状態」としている。

4.2.2 パケットフィルタ規則の確認

Windows Vista の初期状態における【セキュリティが強化された Windows ファイアウォール】のルールを調査した。操作方法は A.2 節を参照のこと。

Windows ファイアウォールのパケットフィルタの基本原則は、

- 受信：初期設定で遮断、規則に一致したパケットを許可
- 送信：初期設定で許可、規則に一致したパケットを遮断

となっている。

Windows Vista の初期状態にて許可する ICMPv6 パケットの受信規則一覧を表 4-1 に示す。【セキュリティが強化された Windows ファイアウォール】で有効になっているパケット受信規則のうち、ICMPv6 に関する規則を抜き出した。

表 4-1　Windows Vista の初期状態における ICMPv6 パケットの受信規則

プロトコル	タイプ	許可 or 遮断	プロトコルの説明
ICMPv6	1	許可	Destination Unreachable
	2	許可	Packet Too Big
	3	許可	Time Exceeded
	4	許可	Parameter Problem
	128	遮断	Echo Request
	129	遮断	Echo Reply
	130	許可	Multicast Listener Query

プロトコル	タイプ	許可 or 遮断	プロトコルの説明
ICMPv6	131	許可	Multicast Listener Report
	132	許可	Multicast Listener Done
	133	遮断	Router Solicitation
	134	許可	Router Advertisement
	135	許可	Neighbor Solicitation
	136	許可	Neighbor Advertisement
	137	遮断	Redirect
	143	許可	Multicast Listener Report Version2

次に、Windows Vista の初期状態で許可している TCP および UDP パケットの受信規則の一覧を表 4-2 に示す。【セキュリティが強化された Windows ファイアウォール】で有効になっているパケット受信規則のうち、TCP および UDP に関する規則を抜き出した。

表 4-2　Windows Vista の初期状態における TCP および UDP パケットの受信規則

プロトコル	ポート番号	プロトコルの説明	規則の説明
TCP	135	epmap（RPC）	・リモートアシスタンス（DCOM 受信）
	2869	LCSLAP	・ネットワーク探索（UPnP 受信） ・リモートアシスタンス（UPnP 受信）
	5357	Web Service for Devices	・ネットワーク探索（WSD イベント受信）
	5358	WS for Devices Secured	・ネットワーク探索（WSD EventsSecure 受信）
	任意		・リモートアシスタンス（TCP 受信） ・リモートアシスタンス（RA-サーバ TCP 受信）
UDP	エッジトラバーサル	Teredo	・コアネットワーク-Teredo（UDP 受信）
	68	Bootpc	・コアネットワーク-動的ホスト構成プロトコル（DHCP 受信）
	137	NETBIOS Name Service	・ネットワーク探索（NB 名受信）

プロトコル	ポート	プロトコルの説明	規則の説明
UDP	138	NETBIOS Datagram Service	・ネットワーク探索（NB データグラム受信）
	1900	SSDP	・ネットワーク探索（SSDP 受信） ・リモートアシスタンス（SSDP 受信）
	3702	UPnP v2 Discovery	・ネットワーク探索（pub WSD 受信） ・ネットワーク探索（WSD 受信）
	5355	LLMNR（Linklocal Multicast Name Resolution）	・ネットワーク探索（LLMNR UDP 受信）

4.2.3 初期状態オープンしているポート番号の確認

Windows Vista のコマンドプロンプトから、”**netstat -an**”コマンド実行し、ネットワーク接続時に、初期状態でオープンしている TCP および UDP ポート番号を調査した。その結果の一覧を表 4-3 に示す。参考に Windows XP の情報も併記する。

表 4-3 Windows Vista の初期状態においてオープンしている TCP および UDP ポート番号

プロトコル	ポート番号	Windows XP (IPv4)	Windows Vista (IPv4)	Windows Vista (IPv6)	プロトコルの説明
TCP	135	○	○	○	epmap（RPC）
	139	○	○	×	NETBIOS Session Service
	445	○	×	○	Microsoft-DS (プリンタ/ファイル共有)
UDP	123	○	○	○	NTP
	137	○	○	×	NETBIOS Name Service
	138	○	○	×	NETBIOS Datagram Service
	445	○	×	×	Microsoft-DS (プリンタ/ファイル共有)
	500	○	○	○	ISAKMP(IKE)

プロトコル	ポート番号	Windows XP (IPv4)	Windows Vista (IPv4)	Windows Vista (IPv6)	プロトコルの説明
UDP	1900	○	○	○	SSDP
	3702	×	○	○	UPnP v2 Discovery
	4500	○	○	×	IPsec NAT Traversal
	5355	×	○	○	LLMNR (Linklocal Multicast Name Resolution)

4.2.4 考察

Windows Vista では、受信パケットは初期設定で遮断となっており、必要最低限のパケットのみを受信するようになっているため、適切な自己防衛がなされていると考えられる。一方で、ICMPv6、TCP、UDP とも、必要最小限の受信許可規則が設定されており、IPv6 の基本的な通信に影響はないと思われる。Windows XP のときと同様に、初期状態では、IPv6、IPv4 とも、ping には応答しない設定となっている。

また、TCP および UDP ポート番号の調査からも、必要最小限のポート番号のみオープンしており、適切な自己防衛がなされていると考えられる。

ところで、初期状態でオープンしていたとしても、Windows ファイアウォールで遮断されたり、ローカルホスト向けにしかオープンしていなかったりという理由から、外部からは接続できないポートがある。初期状態でオープンしていて、かつ外部から接続可能なポートを表 4-4 に示す。初期状態でオープンしている TCP および UDP ポートのうち、【セキュリティが強化された Windows ファイアウォール】で有効になっているパケット受信規則を抜き出した。

表 4-4　Windows Vista の初期状態において外部から接続可能なポート番号

プロトコル	ポート番号	Windows Vista (IPv4)	Windows Vista (IPv6)	プロトコルの説明
TCP	135	○	○	epmap（RPC）
UDP	137	○	×	NETBIOS Name Service
	138	○	×	NETBIOS Datagram Service
	1900	○	×	SSDP
	3702	○	○	UPnP v2 Discovery
	5355	○	○	LLMNR（Linklocal Multicast Name Resolution）

4.3　IPsec と ND/NA およびﾏﾙﾁｷｬｽﾄ通信取り扱いに関する問題

4.3.1 問題の背景と概要

IPv4 で通信を行うためには ARP が欠かせない。しかし、ARP は IPv4 とは異なるプロトコルとして定義されていた。対して IPv6 では ARP に代わる Neighbor Discovery（以下 ND）を IPv6（ICMPv6）の一部として定義している。また、この通信にはマルチキャスト通信がよく使われている。この様な状況で、IPsec 通信機能が有効化された場合、IPv6 の ND やマルチキャスト通信がどのように扱われるのか確認した。

既存の処理系において、ND に IPsec を適用してしまう問題が知られている。従来の IPv4 では、ARP を IP とは異なるプロトコルとしていたため、ARP はそもそも IPsec の対象外であった（IPsec は IP をセキュア化するので、ARP は対象外だった）。対して、IPv6 の環境では ND は IPv6 に含まれるため、IPsec の対象となりえてしまうのである。

このような処理系ではうまく通信できないことがありえる。通常、IPsec を必須とされているホストと通信をしようとすると、要求されたホストとの IPsec 通信の開始に先立ち、鍵交換が行われる。この鍵交換を行うためには ND が必要となる。しかし、IPv6 通信の一種である ND を行うときに、IPsec が必要となってしまうことになる。つまり、IPsec を開始するために鍵交換を行うのにもかかわらず、その鍵交換にも IPsec が要求されてしまうということになる。結果として、このような処理系で、ND が必要になる場合（つまり相手の ND エントリが存在しないとき）に IPsec 通信を開始しようとすると通信不能に陥ることがわかっている。

このような障害を避ける最も簡便な解決法は、ND には IPsec が適用しないという手段である。この処理系では少なくとも ND を IPsec 対象から除外するという設定を明示的に指定しなければならない。このような手続きは WindowsVista において必要なのかどうか、について検証すべきである。

また、ND と同様に、マルチキャスト通信時についても IPsec 化が適用されるかどうかも確認した。

4.3.2 検証手順

Windows Vista において、【ローカルセキュリティポリシ】(【管理ツール】→【ローカルセキュリティポリシ】)によって、任意の IP アドレスから任意の IP アドレスに対して送信されるパケットには IPsec が要求されるもの（require）とする設定を行う。

平行して、【セキュリティが強化された Windows ファイアウォール】でも同様の IPsec 設定を行って下記の 2 処理を実行する（A.2 節参照）。

- **検証項目1**

事前に両者の ND エントリを削除して、集約可能グローバルユニキャストアドレスへの ping を行う。この検証により、IPsec が設定されている状況で、ND と ICMPv6 が行われる。このため、ND に IPsec が要求されるかどうかが判別できる。

- **検証項目2**

ff02::で始まる、IANA によって割り当てられるマルチキャストアドレスへの ping を行う。この検証により、一般的なマルチキャストに対して IPsec 化が適用されるかどうかの判断の指標となる。

4.3.3 検証結果

以下に、それぞれの検証項目による結果をまとめる。

- **検証項目1**

検証の結果、SA が張られていない状況で ND が動作すると、通信手順が中断することがわかった。

具体的には SA がない場合において、両者のホストの IPsec 設定を有効化し、両ホストで netsh コマンドを使い両者の ND エントリを削除し、その後一方からもう一方に ping を投げた。このとき ND が開始される。まずマルチキャスト通信である NS の送信は IPsec であることが要求されず、送信元ホストからネットワーク上に創出された。質問されたホストにそのパケットが到達して、そのホストが NA の応答を送った。これがネットワーク上でも観測されたものの、NS の送信者はそれを受信することが出来なかった様子であり、何度か NS のリトライを行っていた様子である。これは、無視されてしまった NA がユニキャストで送信されており、それには IPsec が必要となっていたためと推察される。つまり、次ホップノードのノードアドレスが ND キャッシュに記載されていない相手に対して、IPsec で通信を開始しようとすると、NA を受け取ることが出来ずに通信に失敗するということがわかる。

- **検証項目2**

ff02::12e に対して ping を行ったが、該当アドレスへの通信は IPsec 化されなかった。

以上の 2 検証において、どちらも IPv6 マルチキャストアドレスへのパケットは暗号化されなかった。全ての IP 機器との通信を IPsec 化すると設定しても、マルチキャスト通信に IPsec が適用されることはなかったということである。しかし、NA はユニキャストで返答されるため、NS 送信者はその応答である NA を受け取ることが出来なかった。

4.3.4 考察

検証項目 1 の結果から、前述の「ND を IPsec から除外するという動作を必要とした処理系」と同様の問題が発生しうることがわかった。これを避けるためには、ICMPv6 を IPsec 化しないという設定が必要になる。これは、【セキュリティが強化された Windows ファイアウォール】においては、【Windows ファイアウォールのプロパティ】における【IPsec の設定】タブ内で、ICMPv6 を常に除外するという設定を行うことになる。

ただし、これについて、既に SA が張られている場合、IPsec の開始が明示的に行われないため、このような問題は発生しない。なお、SA が存在するかどうかは【セキュリティが強化された Windows ファイアウォール】において、左ペインのツリーにある【監視】-【セキュリティアソシエーション】の下にある【メインモード】ないしは【クイックモード】のブランチの下にフォーカスを当てればよい。すると、中央ペインに現在存在する SA が表示される。

以上から、Windows Vista において IPv6 の IPsec を利用する場合、NS/NA ないしは ICMPv6 を IPsec 対象から除外する設定が必要だと思われる。ただし、IPv6 マルチキャスト通信に IPsec が適用されないように IPsec を設定する必要はないと思われる。

検証項目 2 の評価として、ff02::12e に対して ping を行ったが、該当アドレスへの通信は IPsec 化されなかった。検証項目 1 の NS が IPsec 化されなかったことも含めて、Windows Vista は少なくとも Well-known なマルチキャスト通信を IPsec 化しないということがわかった。このため、マルチキャスト通信に IPsec を適用品要に、事前に明示的に指定する必要はないものと考えられる。

5 IPv6 の仕様に関する問題とその検討

本章では、IPv6 の仕様上の問題を取り上げる。IPv6 が標準化されてから 10 年近く経ったが、運用上の課題として標準化が途上のものもいくつか存在する。これらの問題に対する対応策や IPv6 端末の実証状況の対応に関して以下に説明する。

5.1 RA の取り扱い問題

5.1.1 問題の背景と概要

Windows Vista は初期状態で IPv6 が有効である。そのため、ユーザがネットワークに接続した場合に、意図しない RA メッセージを受信することで不都合が発生する可能性が考えられる。

そこで、Windows Vista において RA メッセージを受信したことを確認する方法と、意図しない RA メッセージを受け入れないようにする方法を紹介する。

5.1.2 想定されるネットワーク環境

ユーザ LAN 内に IPv6 ネットワークを構築した。RA メッセージはユーザ LAN 内に設置している IPv6 ルータから受信する。図 5-1 に示す環境で動作検証を行った。

RA メッセージの lifetime は実験で使用したルータの初期値とした。

- valid_lifetime(有効寿命)・・・2,592,000 秒
- preferred_lifetime(推奨寿命)・・・604,800 秒

5.1.3 検証手順

Windows Vista が IPv6 ルータから RA メッセージを受信した場合の挙動の確認と、RA メッセージ受信の制御について確認するため以下の 2 項目について検証を行う。

1. RA メッセージを受信したときのネットワークインターフェイスの情報を確認する。
2. RA メッセージ受信の抑制に関して、Windows ファイアウォールによる操作を確認する。なお、確認方法は A.2 節を参考のこと。

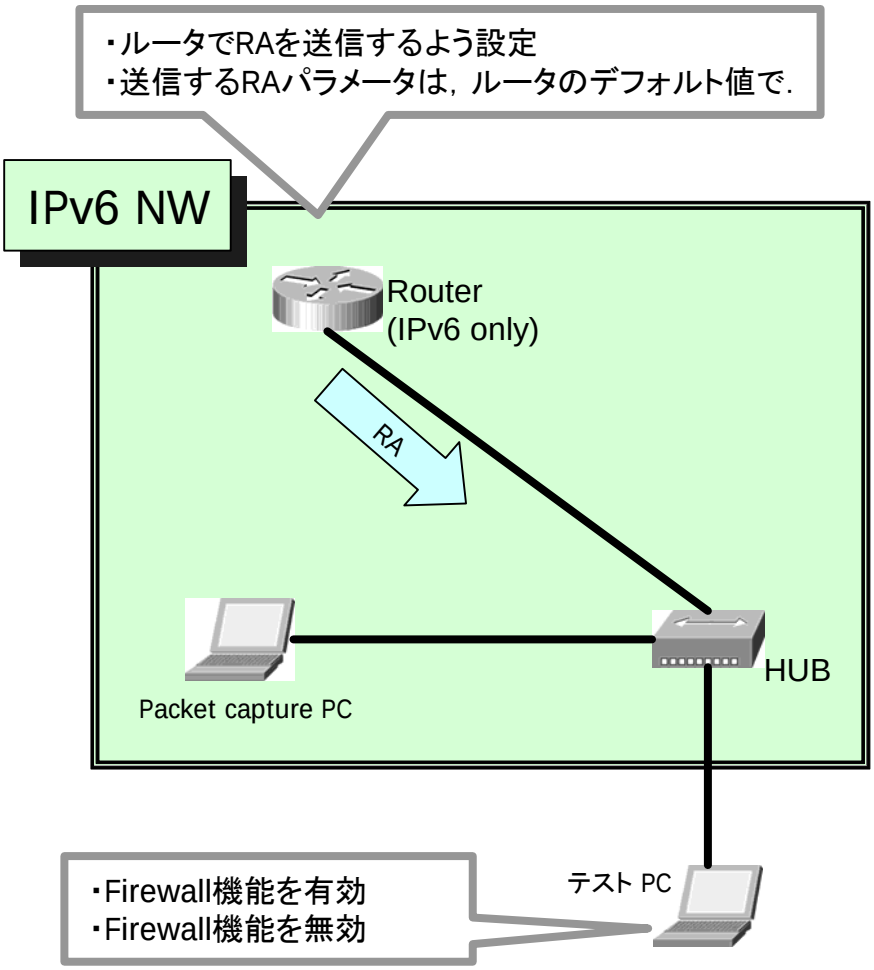

図 5-1　IPv6 ネットワーク環境例

- 検証項目1
  1. Windows Vista を IPv6 ネットワーク接続する。
  2. IPv6 ルータからの RA メッセージ受信後、各ネットワークインターフェイスのステータスを確認する。

- 検証項目2
  1. Windows ファイアウォールにて RA メッセージをドロップする設定に変更する。
  2. Windows Vista の再起動を実施し、IPv6 ルータとの通信をキャプチャして解析する。
  3. IPv6 ルータから定期的に送信される RA メッセージをキャプチャして解析する。
  4. IPv6 ルータから定期的に送信された RA メッセージ受信後の Windows Vista のステータスを確認。

5.1.4 検証結果

- **検証項目1**

Windows Vista では、IPv6 ルータからの RA メッセージを受信することによりグローバルユニキャスト IPv6 アドレスが自動生成される。「netsh interface ipv6 show address」コマンドを実行することで、自動生成されたものか、あるいは手動設定したものかを知ることが可能である。このコマンドの実行結果において、自動生成されたものは「Public および Temporary」で表示され、手動設定したものは「Manual」で表示される。ネットワークインターフェイスに手動で IPv6 アドレスを設定していたとしても、当該ネットワークインターフェイスが RA メッセージを受信すれば、自動生成するグローバルユニキャスト IPv6 アドレスが追加で割り当てられる。

Windows Vista でネットワークインターフェイスがどのような IPv6 アドレスプレフィックス情報を受信しているかを確認するには、「netsh interface ipv6 show siteprefixes」を実行する。RA メッセージを受信している場合、RA メッセージを受信しているネットワークインターフェイス名、IPv6 アドレスプレフィックス情報を確認できる。有効時間として（valid_lifetime）×2 秒が設定されていた。

Windows XP の場合も Windows Vista と同様のコマンドで確認することができるが、「netsh interface ipv6 show siteprefixes」を実行した場合は、/48 での表示であった。/49～/64 部分については切り捨てられていた。有効時間を示す valid_lifetime の値は RA メッセージで通知される値がそのまま設定されていた。

- **検証項目2**

Windows Vista の Windows ファイアウォールで RA メッセージ受信をドロップ（破棄）するルールを適用しても起動時に RA メッセージを受け取っていた。起動後は Windows ファイアウォールのルールが適用され、IPv6 ルータから定期的に通知される RA メッセージを期待通りにドロップできていた。

起動時に受信した RA メッセージの（valid_lifetime × 2）秒の時間経過後、有効時間が切れ、ネットワークインターフェイスに割り当てられていたグローバルユニキャスト IPv6 アドレスは消失した。

また、Windows Vista は「ipconfig /renew6」コマンドが実行されると、RS メッセージを送信する。送信した RS メッセージに対する応答 RA メッセージは Windows ファイアウォール でドロップされることなく通過し、グローバルユニキャスト IPv6 アドレスが自動生成された。この時の Windows ファイアウォールは検証項目②の手順 1 で設定した状態である。

5.1.5 検証データ

- 検証項目1

IPv6 ルータの設定（RA メッセージ送信に関係する部分の抜粋）は以下の通り。

```
-------------------------------------------------------------------------------
ipv6 lan1 address 2001:db8:1234:5678::1/64
ipv6 lan1 rtadv send 1
ipv6 prefix 1 2001:db8:1234:5678::/64
-------------------------------------------------------------------------------
```

Windows Vista での「netsh interface ipv6 show address」結果を以下に示す。

```
-------------------------------------------------------------------------------
C:¥>netsh interface ipv6 show address
アクティブ状態を参照しています...
インターフェイス 12: ローカル エリア接続
アドレス種類  DAD 状態  有効期間  優先有効期間  アドレス
---------  ----  ----------  ----------  ----------------------------------
Manual     設定      infinite    infinite  2001:db8:1234:5678::1111
Temporary  設定    6d22h1m20s  6d22h1m20s  2001:db8:1234:5678:3d06:b0c4:9b84:974a
Public     設定  29d23h59m54s  6d23h59m54s  2001:db8:1234:5678:894f:f69f:2813:7b16
その他     設定      infinite    infinite  fe80::894f:f69f:2813:7b16%12
:
-------------------------------------------------------------------------------
```

Windows Vista での「netsh interface ipv6 show siteprefixes」結果を以下に示す。

```
-------------------------------------------------------------------------------
C:¥>netsh interface ipv6 show siteprefixes
プレフィックス          有効期間        インターフェイス
----------------------------------  ----------------------  ----------------------------
2001:db8:1234:5678::/64     59d23h59m44s     ローカル エリア接続
-------------------------------------------------------------------------------
```

Windows XP での「netsh interface ipv6 show siteprefixes」結果を以下に示す。

```
-------------------------------------------------------------------------------
C:¥>netsh interface ipv6 show siteprefixes
Prefix                  Lifetime            Interface
--------------------------  ----------------------  ----------------------------
2001:db8:1234::/48      29d23h57m23s      ローカル エリア接続
-------------------------------------------------------------------------------
```

- 検証項目2

Windows ファイアウォールに RA メッセージ受信をドロップするルールを適用した様子を図 5-2 と図 5-3 にそれぞれ示す。

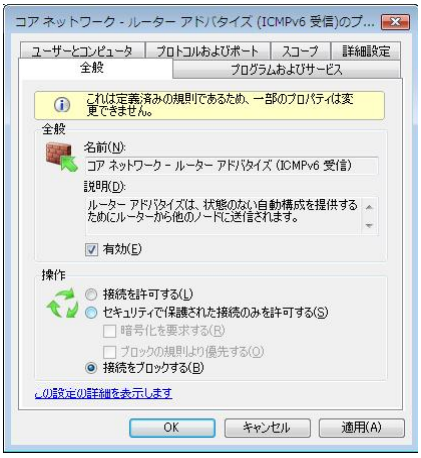

図 5-2　フィルタルール変更画面

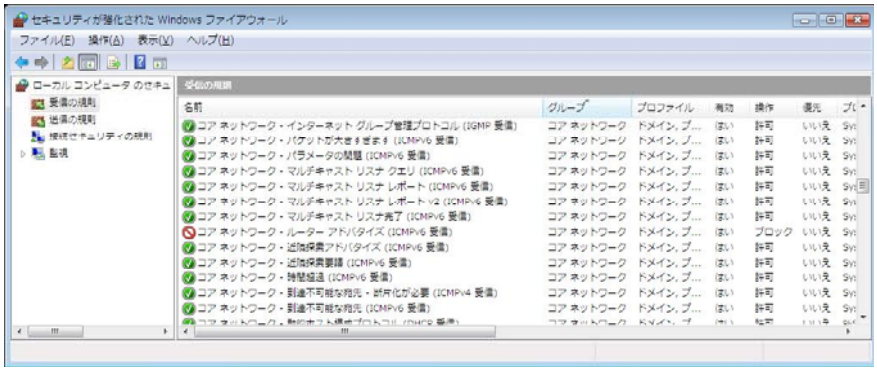

図 5-3　RA メッセージ受信ドロップルール適用完了

5.1.6 考察

検証 1 より、Windows Vista は初期状態において、RA メッセージを受信するとグローバルユニキャスト IPv6 アドレスを自動生成する。ネットワークインターフェイスに手動で IPv6 アドレスを設定していたとしても、当該ネットワークインターフェイスが RA メッセージを受信すれば、自動生成するグローバルユニキャスト IPv6 アドレスが追加で割当てられる。

検証 2 より、Windows ファイアウォール に RA メッセージをドロップするルールを適用した場合でも、システム起動時には RA メッセージを受け取るため、ネットワークインターフェイスにはグローバルユニキャスト IPv6 アドレスが自動生成される。IPv6 ルータから定期的に通知される RA メッセージは、システム起動後には Windows ファイアウォールでドロップされるが、「ipconfig /renew6」コマンド実行時に送信する RS メッセージに対する応答 RA メッセージは Windows ファイアウォール でドロップされない。

RA メッセージ受信によってネットワークインターフェイスに施される設定を無効にしたい場合の対処法の例を下記に記載する。

- **対策例1**

Windows Vista において、「netsh」コマンドを利用することで RA メッセージ受信による設定を無効にすることが可能である。下記に示したコマンドを実行した場合、RS メッセージ送信と RA メッセージ受信を抑制する。IPv6 の利用を無効化したいインターフェイスに対して実行する。

◆RS メッセージ送信および RA メッセージ受信を抑制するコマンド

```
C:¥>netsh interface ipv6 set interface [interface] routerdiscovery=disable      ☆
```

この対策例では、いかなる RA メッセージも受信しなくなることに注意が必要である。

- **対策例2**

Windows ファイアウォールを利用し RA メッセージを受信しない設定と RS メッセージを送信しない設定を実施する。システム起動時に受信してしまう RA メッセージによって生成される情報は以下に記載するコマンドにて削除を実施する。

◆グローバルユニキャスト IPv6 アドレスの削除

```
C:¥>netsh interface ipv6 delete address [interface] [ip address]                ☆
```

◆ルーティングテーブルから IPv6 デフォルトゲートウェイを削除

```
C:¥>netsh interface ipv6 delete route [prefix] [interface] [nexthop]            ☆
```

◆RA メッセージ受信拒否設定の実施

図 5-3 のウィンドウで実施

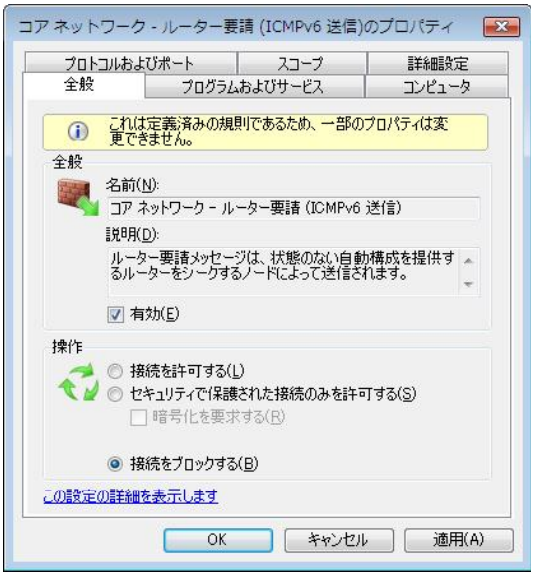

図 5-4　RS メッセージ送信フィルタルール変更画面

◆RS メッセージ送信拒否設定の実施

図 5-5 のウィンドウで実施

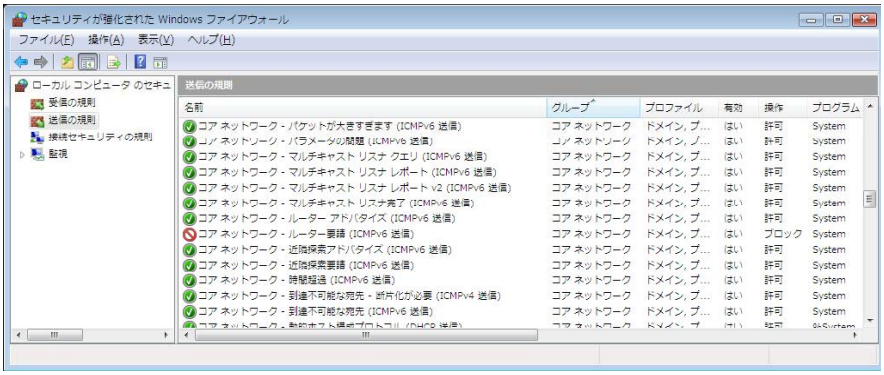

図 5-5　RS メッセージ送信フィルタルール変更完了画面

上記項目を実施することにより、システム起動時に受信してしまう RA メッセージによって自動生成するグローバルユニキャスト IPv6 アドレス情報と IPv6 デフォルトゲートウェイ情報の削除、および、以降の RA メッセージ受信ドロップと RS メッセージ送信抑制が可能となる。

この対策例はシステムを起動する度に、システム起動時に受信してしまう RA メッセージによって自動生成するグローバルユニキャスト IPv6 アドレス情報と IPv6 デフォルトゲートウェイ情報の削除を実施しなくてはならないことに注意が必要である。

5.2 IPv6 の Dynamic DNS について

5.2.1 問題の背景と概要

IPv6 アドレスは IPv4 アドレスと比較して長く複雑であり、一般的に記憶しにくいため DNS がより重要になる。一方 IPv6 環境では IPv6 アドレスは自動で設定されることが多く、この場合にはサーバ管理者が手動で DNS に登録するのは難しい。

IPv6 アドレスが自動設定されるような環境においては Dynamic DNS（以下 DDNS）を組み合わせることで IPv6 関連のネットワーク設定作業を削減し IPv6 ホストを利用しやすくすることができる。このため IPv6 環境では IPv4 環境以上に DDNS に対して期待がある。

ただし、単一のアドレスが単一のプロトコルで登録されるだけであった IPv4 の DDNS と比較して IPv6 対応端末 OS においては DDNS がより複雑になる。具体的には下記のような挙動について検討が必要である。

- IPv6 DNS サーバへ更新リクエストに失敗した場合の挙動
  - IPv4 DNS サーバへフォールバックするか
- 複数アドレスをもつ場合の挙動
  - IPv6/IPv4 アドレスをもつ場合、すべて登録するのか
  - 複数の IPv6 アドレスを持つ場合すべて登録するのか
  - 登録するアドレスを制限できるか

DDNS には外部パッケージによるもの、OS 標準機能によるもの等がある。Windows Vista は OS 標準機能として IPv6、IPv4 での DDNS をサポートしており、ここではその機能について検証を行う。

5.2.2 問題の検証環境

検証環境は下記の通りである。

- 対象端末: Windows Vista 日本語版
- DNS サーバ: Fedora Core 6 / bind 9.4.0 であり、dy.example.jp ゾーンに関して IPv6/IPv4 で dynamic 更新可能に構成している。

図 5-6 に DDNS Update の検証を行った環境を示す。

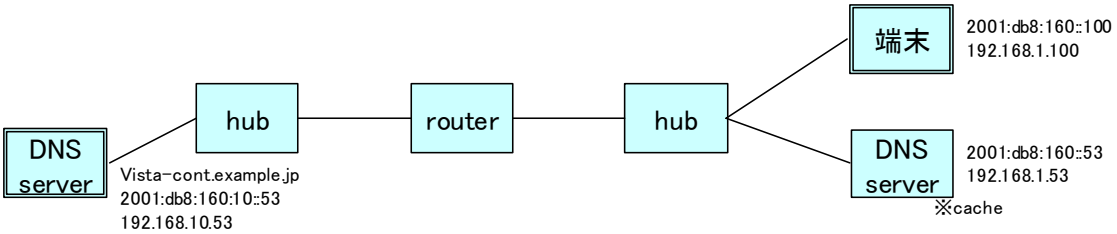

図 5-6　DDNS Update 検証構成

本環境において、

- 端末に設定されたアドレスが IPv6 のみ、IPv4 のみ、IPv6/IPv4 両方の場合
- 端末に設定された DNS サーバが IPv6 DNS サーバのみ、IPv4 DNS サーバのみ、IPv6/IPv4 DNS サーバ両方の場合
- 端末と DDNS を実行する対象の DNS サーバの間で通信可能なプロトコルが IPv6 のみ、IPv4 のみ、あるいは IPv6/IPv4 両方の場合

というケースについて DDNS update の挙動を確認した。

5.2.3 検証手順

検証手順を以下に示す。

1. dy.example.jp ゾーンに関して IPv6/IPv4 で dynamic 更新可能なように DNS サーバを構成、設置する。
2. 1.とは別に端末に設定する DNS キャッシュサーバを IPv6/IPv4 デュアルスタックで構成、設置する。
3. ルータにて検証条件（IPv6、IPv4、IPv6/IPv4）にあわせてルーティング情報を設定する。
4. 端末のアドレス、DNS サーバ設定を検証条件（IPv6、IPv4、IPv6/IPv4）にあわせて設定する。
5. パケットアナライザを接続しキャプチャを開始する。
6. 端末をネットワークに接続する。
7. DNS サーバのログ情報、ゾーン情報およびキャプチャデータを解析し、DDNS の実施内容を確認する。

※もし端末接続後一定時間経過しても DDNS の実行がみられない場合は、ipconfig /registerdns コマンドで明示的に DDNS を実行する。

5.2.4 検証結果

検証結果を以下の表 5-1 にまとめる。

表 5-1　DDNS Update 検証結果

		到達性	PC のアドレス設定		
			IPv6	IPv6/IPv4	IPv4
DNSサーバ設定	IPv6	IPv6	登録：IPv6 RR：AAAA	登録：IPv6 RR：AAAA、A	NG
		IPv6 IPv4	登録：IPv6 RR：AAAA	登録：IPv6 RR：AAAA、A	NG
		IPv4	NG	NG	NG
	IPv6/IPv4	IPv6	登録：IPv6 RR：AAAA	登録：IPv6 RR：AAAA、A	NG
		IPv6 IPv4	登録：IPv6 RR：AAAA	登録：IPv6 RR：AAAA、A	登録：IPv4 RR：A
		IPv4	NG	登録:IPv6 から IPv4 にフォールバック RR：AAAA、A	登録：IPv4 RR：A
	IPv4	IPv6	NG	NG	NG
		IPv6 IPv4	NG	登録：IPv4 RR：AAAA、A	登録：IPv4 RR：A
		IPv4	NG	登録：IPv4 RR：AAAA、A	登録：IPv4 RR：A

表 5-1 の横軸に端末に設定したアドレス条件（IPv6、IPv4、IPv6/IPv4）、縦軸に端末に設定した DNS サーバのアドレス条件（IPv6、IPv4、IPv6/IPv4）を配し、さらにそれぞれのケースにおいて端末と DDNS 対象 DNS サーバ間での通信可能プロトコル条件を変えた場合の DDNS 結果について以下の内容を記載している。

- 登録されたか否か（登録 or NG）
- 登録された場合、IPv6/IPv4 いずれのプロトコルで DDNS が行われたか（v6 or v4）
- 登録されたアドレス（レコード）は何か（AAAA or A）

5.2.5 検証データ

参考として一般的な DDNS のパケットキャプチャ結果を図 5-7 に示す。

```
#No, Source IPv6, Destination IPv6, Protocol, Infomation
1,  2001:db8:160::100, 2001:db8:160::53, DNS, Standard query SOA vista-PC.dy.example.jp
2,  2001:db8:160::53, 2001:db8:160::100, DNS, Standard query response
3,  2001:db8:160::100, 2001:db8:160::53, DNS, Standard query AAAA vista-cont.example.jp
4,  2001:db8:160::53, 2001:db8:160::100, DNS, Standard query response AAAA 2001:db8:160:10::53
5,  2001:db8:160::100, 2001:db8:160:10::53, DNS, Dynamic update SOA dy.example.jp
6,  2001:db8:160:10::53, 2001:db8:160::100, DNS, Dynamic update response
7,  2001:db8:160::100, 2001:db8:160::53, DNS, Standard query SOA ¥
                  0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.1.0.8.b.d.0.1.0.0.2.ip6.arpa
8,  2001:db8:160::53, 2001:db8:160::100, DNS, Standard query response
9,  2001:db8:160::100, 2001:db8:160::53, DNS, Standard query AAAA vista-cont.example.jp
10, 2001:db8:160::53, 2001:db8:160::100, DNS, Standard query response AAAA 2001:db8:160:10::53
11, 2001:db8:160::100, 2001:db8:160:10::53, DNS, Dynamic update SOA ¥
                                                  0.0.0.0.0.6.1.0.8.b.d.0.1.0.0.2.ip6.arpa
12, 2001:db8:160:10::53, 2001:db8:160::100, DNS, Dynamic update response
13, 2001:db8:160::100, 2001:db8:160::53, DNS, Standard query SOA ¥
                  0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.2.0.0.0.0.6.1.0.8.b.d.0.1.0.0.2.ip6.arpa
14, 2001:db8:160::53, 2001:db8:160::100, DNS, Standard query response, No such name
15, 2001:db8:160::100, 2001:db8:160::53, DNS, Standard query SOA 100.1.168.192.in-addr.arpa
16, 2001:db8:160::53, 2001:db8:160::100, DNS, Standard query response
17, 2001:db8:160::100, 2001:db8:160::53, DNS, Standard query AAAA vista-cont.example.jp
18, 2001:db8:160::53, 2001:db8:160::100, DNS, Standard query response AAAA 2001:db8:160:10::53
19, 2001:db8:160::100, 2001:db8:160:10::53, DNS, Dynamic update SOA 1.168.192.in-addr.arpa
20, 2001:db8:160:10::53, 2001:db8:160::100, DNS, Dynamic update response
```

図 5-7　一般的な DDNS のキャプチャデータ

dy.example.jp ゾーンへの update を実施している 5 番目のパケットをみてみると、複数の IPv6 アドレスおよび IPv4 アドレスについて update しようとしていることがわかる。以下にキャプチャデータの詳細を示す。

◆DDNS のゾーン update パケットの詳細

```
Ethernet II, Src: * (*:*:*:*:*:*), Dst: * (*:*:*:*:*:*)
Internet Protocol Version 6
User Datagram Protocol, Src Port: 50326 (50326), Dst Port: domain (53)
Domain Name System (query)
    [Response In: 135]
    Transaction ID: 0x51b4
    Flags: 0x2800 (Dynamic update)
        0... .... .... .... = Response: Message is a query
        .010 1... .... .... = Opcode: Dynamic update (5)
        .... ..0. .... .... = Truncated: Message is not truncated
        .... ...0 .... .... = Recursion desired: Don't do query recursively
        .... .... .0.. .... = Z: reserved (0)
        .... .... ...0 .... = Non-authenticated data OK: Non-authenticated data is unacceptable
```

```
    Zones: 1
    Prerequisites: 1
    Updates: 5
    Additional RRs: 0
    Zone
        dy.example.jp: type SOA, class IN
            Name: dy.example.jp
            Type: SOA (Start of zone of authority)
            Class: IN (0x0001)
    Prerequisites
        vista-PC.dy.example.jp: type CNAME, class NONE
            Name: vista-PC.dy.example.jp
            Type: CNAME (Canonical name for an alias)
            Class: NONE (0x00fe)
            Time to live: 0 time
            Data length: 0
    Updates
        vista-PC.dy.example.jp: type AAAA, class ANY
            Name: vista-PC.dy.example.jp
            Type: AAAA (IPv6 address)
            Class: ANY (0x00ff)
            Time to live: 0 time
            Data length: 0
        vista-PC.dy.example.jp: type A, class ANY
            Name: vista-PC.dy.example.jp
            Type: A (Host address)
            Class: ANY (0x00ff)
            Time to live: 0 time
            Data length: 0
        vista-PC.dy.example.jp: type AAAA, class IN, addr 2001:db8:160::100
            Name: vista-PC.dy.example.jp
            Type: AAAA (IPv6 address)
            Class: IN (0x0001)
            Time to live: 20 minutes
            Data length: 16
            Addr: 2001:db8:160::100
        vista-PC.dy.example.jp: type AAAA, class IN, addr 2001:db8:160:2::100
            Name: vista-PC.dy.example.jp
            Type: AAAA (IPv6 address)
            Class: IN (0x0001)
            Time to live: 20 minutes
            Data length: 16
            Addr: 2001:db8:160:2::100
        vista-PC.dy.example.jp: type A, class IN, addr 192.168.1.100
            Name: vista-PC.dy.example.jp
            Type: A (Host address)
            Class: IN (0x0001)
            Time to live: 20 minutes
            Data length: 4
            Addr: 192.168.1.100
-------------------------------------------------------------------------------
```

5.2.6 考察

検証結果についてまとめると、下記のことが確認できた。

- IPv6 DNS サーバへ更新リクエストに失敗した場合には、IPv4 DNS サーバへフォールバックを行う
- IPv6/IPv4 アドレスをもつ場合、IPv6/IPv4 トランスポートいずれであるか、また疎通があるかどうかに関わらず全てのアドレスを登録する。(ただし teredo、6to4、一時 IPv6 アドレスは登録されない)
- IPv6 のみ、IPv4 のみ、あるいは複数の IPv6 アドレスをもつ場合、一部のアドレスのみを登録するといった、登録制限を行うことはできない。

前記にまとめたように IPv6/IPv4 アドレスのどちらか一方が通信可能であれば、通信できないアドレスについても登録される。たとえばグローバル IPv6 アドレスとプライベート IPv4 アドレスを持つような場合、IPv4 アドレスについても登録されるので注意する必要がある。

5.3　DNS ディスカバリの現状について

5.3.1 問題の背景と概要

IPv6 環境において、IPv6 アドレスの自動設定方法はかなり以前に規格化され、現在ではほとんどの OS・環境で実装されており、実際に利用されている。一方で DNS サーバの自動設定（DNS ディスカバリ）については浸透が遅れている。現在 IETF で RFC（RFC4339）として提案されている DNS ディスカバリの方法は以下の 3 つである。

- RA による通知
- DHCPv6 による通知
- Well-known Anycast Addresses

IPv6 端末 OS で現在サポートしている、また将来サポートされうる DNS ディスカバリ手法について、調査を行う必要がある。

5.3.2 問題の検証と検討

Windows Vista における DNS ディスカバリ手法を検証したところ、DHCPv6 と well-known アドレスによる自動発見のサポートを確認することができた。

まず、DHCPv6 については、Managed-Flag が 1 であるような RA を受信することで Stateful な DHCPv6 により IPv6 アドレスと共に DNS サーバのアドレス取得を試みる。また、OtherConfig-Flag が 1 であるような RA を受信することで Stateless な DHCPv6 により DNS サーバアドレス取得を試みる。

各ケースにおけるパケットキャプチャの結果を図 5-8 と図 5-9 にそれぞれ示す。フラグを変更した RA を送信するルータは DHCPv6 サーバも兼ねている。

```
#No, Source IPv6, Destination IPv6, Protocol, Infomation
1,  "fe80::*:*:fe75:a2a4", "ff02::1", "ICMPv6", "Router advertisement"
2,  "fe80::*:*:cf26:da6a", "ff02::1:2", "DHCPv6", "Solicit"
       [elapsed-time]
       [client-identifier]
       [ia-na]
       [vendor-class]
       [domain-search-list]
       [dns-recursive-name-server]
       [vendor-specific-information]
3,  "fe80::*:*:fe75:a2a4", "fe80::*:*:cf26:da6a", "DHCPv6", "Advertise"
4,  "fe80::*:*:cf26:da6a", "ff02::1:2", "DHCPv6", "Request"
5,  "fe80::*:*:fe75:a2a4", "fe80::*:*:cf26:da6a", "DHCPv6", "Reply"
```

図 5-8　Managed-Flag が 1 である場合のキャプチャデータ

```
#No, Source IPv6, Destination IPv6, Protocol, Infomation
1,  "fe80::*:*:fe75:a2a4", "ff02::1", "ICMPv6", "Router advertisement"
2,  "fe80:: *:*:cf26:da6a", "ff02::1:2", "DHCPv6", "Information-request"
       [elapsed-time]
       [client-identifier]
       [vendor-class]
       [domain-search-list]
       [dns-recursive-name-server]
       [vendor-specific-information]
3,  "fe80:: *:*:fe75:a2a4", "fe80::*:*:cf26:da6a", "DHCPv6", "Reply"
```

図 5-9　OtherConfig-Flag が 1 である場合のキャプチャデータ

Managed-Flag が 1 の場合は、RA を受信した Windows Vista にて DHCPv6 クライアントが起動され、DHCPv6 Solicit の送信が実施される。その後、DHCPv6 Request を送信して DNS サーバの取得を行う。OtherConfig-Flag が 1 の場合には、DHCPv6 クライアントが起動されるが、DHCPv6 Solicit ではなく DHCPv6 Information-request を送信して DNS サーバの取得を行うため手順が少ないことが分かる。

DNS サーバが自動・手動いずれにおいても設定されない場合 fec0:0:0:ffff::1～fec0:0:0:ffff::3 という Well-known Site Local アドレスの DNS サーバが自動設定される。以下に ipconfig を実行した結果を示す（有効な物理インターフェイスのみ抜粋)。

```
------------------------------------------------------------------------------
C:¥>ipconfig /all
 :
イーサネット アダプタ ローカル エリア接続:

   接続固有の DNS サフィックス . . . :
   説明. . . . . . . . . . . . . . . : Fast Ethernet
   物理アドレス. . . . . . . . . . . : *-*-*-*-*-*
   DHCP 有効 . . . . . . . . . . . . : はい
   自動構成有効. . . . . . . . . . . : はい
   IPv6 アドレス . . . . . . . . . . . : 2001:db8:160::100(優先)
   リンクローカル IPv6 アドレス. . . . : fe80::*:*:*:*%8(優先)
   自動構成 IPv4 アドレス. . . . . . : 169.254.165.212(優先)
   サブネット マスク . . . . . . . . : 255.255.0.0
   デフォルト ゲートウェイ . . . . . : 2001:db8:160::1
   DHCPv6 IAID . . . . . . . . . . . : *
   DNS サーバー. . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over TCP/IP . . . . . . . : 有効
------------------------------------------------------------------------------
```

Site Local アドレスは既に利用しないことに決まっているが、ここで設定された Well-known Site Local アドレスの DNS サーバは実際に DNS 問い合わせに利用される。

その様子をパケットキャプチャに示す。

```
#No, Source IPv6, Destination IPv6, Protocol, Infomation
1,  2001:db8:160::100, fec0:0:0:ffff::3, DNS, Standard query AAAA ns.example.com
2,  2001:db8:160::1, 2001:db8:160:1::100, ICMPv6, Unreachable (Route unreachable)
3,  2001:db8:160::100, fec0:0:0:ffff::2, DNS, Standard query AAAA ns.example.com
4,  2001:db8:160::1, 2001:db8:160:1::100, ICMPv6, Unreachable (Route unreachable)
5,  2001:db8:160::100, fec0:0:0:ffff::1, DNS, Standard query AAAA ns.example.com
6,  2001:db8:160::1, 2001:db8:160::100, ICMPv6, Unreachable (Route unreachable)
7,  2001:db8:160::100, fec0:0:0:ffff::1, DNS, Standard query AAAA ns.example.com
8,  2001:db8:160::100, fec0:0:0:ffff::2, DNS, Standard query AAAA ns.example.com
9,  2001:db8:160::100, fec0:0:0:ffff::3, DNS, Standard query AAAA ns.example.com
10, 2001:db8:160::1, 2001:db8:160::100, ICMPv6, Unreachable (Route unreachable)
11, 2001:db8:160::1, 2001:db8:160::100, ICMPv6, Unreachable (Route unreachable)
12, 2001:db8:160::1, 2001:db8:160::100, ICMPv6, Unreachable (Route unreachable)
13, 2001:db8:160::100, fec0:0:0:ffff::1, DNS, Standard query AAAA root1.example.com
14, 2001:db8:160::100, fec0:0:0:ffff::2, DNS, Standard query AAAA root1.example.com
15, 2001:db8:160::100, fec0:0:0:ffff::3, DNS, Standard query AAAA root1.example.com
16, 2001:db8:160::1, 2001:db8:160::100, ICMPv6, Unreachable (Route unreachable)
17, 2001:db8:160::1, 2001:db8:160::100, ICMPv6, Unreachable (Route unreachable)
18, 2001:db8:160::1, 2001:db8:160::100, ICMPv6, Unreachable (Route unreachable)
```

図 5-10　Well-known Site Local アドレスの DNS サーバへの通信のキャプチャデータ

この例では Site-local アドレスをもつネットワークや DNS サーバが存在しないためルータでエラーになっているが、もしも域内に Site-local アドレスをもつ DNS サーバを適切に設置した場合は DNS キャッシュサーバとして利用可能である。

5.3.3 考察

以上のように Windows Vista では DNS ディスカバリとして、

- Stateful DHCPv6
- Stateless DHCPv6
- well-known Site-local アドレス

を利用することができる。Well-known Site local アドレスについては現状 DNS サーバが他の手段で設定されない場合に自動的に設定されるとはいえ、既に Site local アドレス自体が廃止と決まっていることから IPv6 における DNS ディスカバリとしては主に DHCPv6 を利用することになると考えられる（DHCPv6 サーバ機能は Windows Longhorn server に搭載予定である）。

ただし DHCP サーバだけが必要な IPv4 の場合とは異なり IPv6 においては DHCPv6 サーバの他に RA を送信する機器が必要となることから、アドレス自動割当てとあわせて端末向けネットワークインフラの設計においてはその構成について十分留意する必要がある。

5.4　マルチプレフィックス環境下での送信元アドレス選択の問題

5.4.1 問題の背景と概要

IPv6 では、1 つのインターフェイスに対して複数のアドレスを利用することが可能であり、通常の利用においてもリンクローカルアドレスとグローバルアドレスの双方を利用することになる。複数のアドレスを利用する環境において、特にグローバルアドレスを複数扱う環境をマルチプレフィックス環境と呼ぶ。このマルチプレフィックス環境では、通信開始時に端末 OS 自身が利用する送信元アドレスの選択に関して問題が発生する場合がある。図 5-11 にこの問題が発生する想定環境を示し、以下に解説する。

図中におけるケース 1、ケース 2 における対象組織（ユーザサイトなど）は、どちらも、ISP や ASP（Application Service Provider）など複数の他ネットワークへの接続を持ち、複数のプレフィックスの割り当てを受けている。

特に、この想定環境では、対象組織が 1 つの ISP と 2 つの ASP に接続性を持っているとしており、組織内のホストがインターネット向けパケットを送ると、ISP を通って外部ホストに到達することになる。この ISP から供給されるプレフィックスを A（2001:db8:a:1::/64）とする。また、この組織は、二つの ASP（ASP-1 と ASP-2）からサービス利用のために、B（2001:db8:10b:1::/64）および C（2001:db8:c:1::/64）のプレフィックスが端末 OS に設定されていて、さらにプレフィックス D（2001:db8:10d::/48）を持つ ASP-3 が ASP-2 のサービス内に含まれる環境とする。

ケース 1 は、この状況で組織内の端末が、組織外の端末にパケットを送るとき、A、B、C のどの送信元アドレスを選ぶべきかの問題を示している。組織内の端末が、組織外に向けたパケットを作成して送信する際、その送信元アドレスには A、B、C のいずれかのプレフィックスによる自身のアドレスを使用しなければならない。もしこの時 C のプレフィックスによるアドレスが利用されたとすると、通信パケットは組織外にルーティングされるが、組織外の端末からの応答パケットが到達することはなく、通信は成立しない。なぜなら、利用した C の送信元アドレスは ISP より広告されているアドレスでなく、ルーティング不能であるためである。ケース 1 はこの様子を示したものである。

また、ケース 2 では、ASP-2 のサービスの範囲に存在する ASP-3 への通信を行う際に、ASP-1 の送信元アドレス B を利用した場合を示している。ケース 1 と同じく戻りの経路が存在しないためパケットが到達しない状態を示している。

これらの様な場合は、送信時に適切なアドレスを選択できるような機構が必要となる。

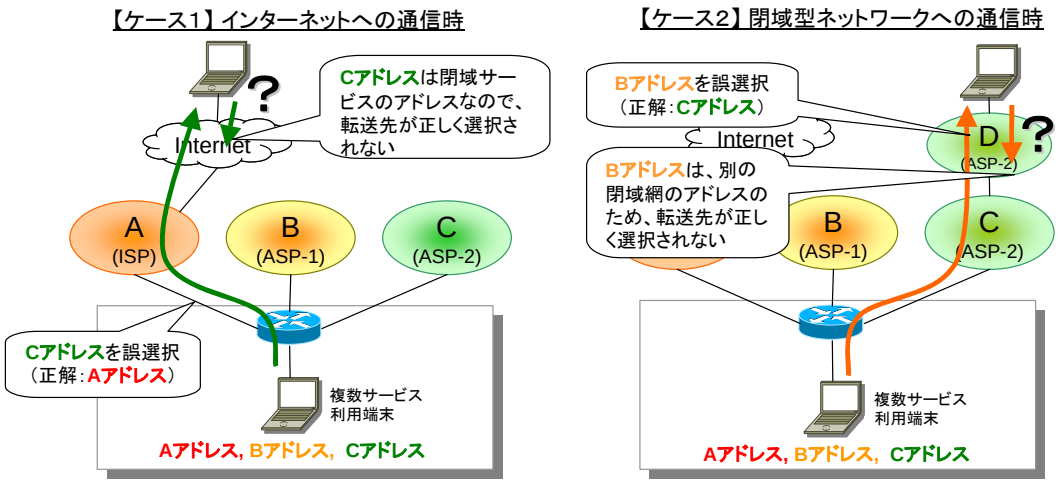

図 5-11　送信元アドレス選択にて問題が発生しうる想定環境

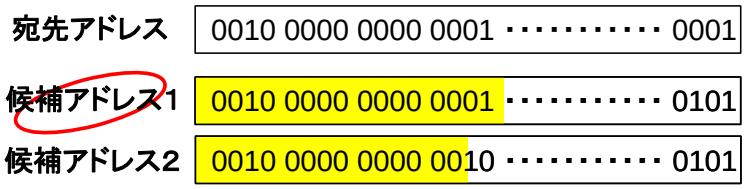

図 5-12　最長一致による送信元アドレスの選択

5.4.2 現状の実装の確認

IETF では、アドレス選択に関する標準仕様を RFC 3484 “Default address selection for IPv6”にて規定している。この RFC では、宛先アドレスに対して送信元アドレスを選択するアルゴリズムが明記されており、基本的には同じアドレススコープのものを選択し、最終的には先頭ビットから最長一致するアドレスが選ばれることになる。以上の動作が、複数のアドレスを持つ端末において一般的に実装されているアドレス選択機構になる。

この実装によって、複数の候補アドレスの中から、始点アドレスとして採用すべきアドレスを選ぶ様子を図 5-12 に示す。

この最長一致によって大概の場合において問題は発生しない。しかしながら、宛先アドレスに最も近い候補アドレスが、常に送信元アドレスとして選択されることが最も適しているとは限らない場合も存在する。5.4.1 節における想定環境においても、ISP の先にあるインターネット上の通信相手のアドレスが、ASP-1 や ASP-2 のプレフィックスに近かった場合などにおいて、謝った送信元アドレスが選択されるからである。したがって、この手法だけでは、問題を完全に解決することはできないと言える。

5.4.3 検証内容

本節にて取り上げた問題の解決手法の 1 つとして考えられるものに、RFC3484 中で規定されている「アドレス選択ポリシーテーブル（以下ポリシーテーブル)」がある。このポリシーテーブルの挙動を検証するため、以下の 2 項目の検証を行う。

1. 初期設定のポリシーテーブルにおける挙動の確認
2. アドレス選択問題を解決する設定実施したポリシーテーブルでの挙動の確認

RFC3484 を実装している場合においても、このポリシーテーブルを操作することができない端末 OS も存在している。本節では FreeBSD 5.5 Release、Windows XP SP2、Windows Vista を動作検証の対象端末 OS として用いる。なお、ポリシーテーブルの解説は 2.2.12 節を参照のこと。

5.4.4 検証手順

検証環境には図 5-11 に示した想定環境を用いる。表 5-2 に利用するサービスプロバイダとプレフィックスの関係をまとめておく。それぞれのプレフィックスは 1 台のルータからの RA にて端末 OS に配布されるものとする。

表 5-2　想定環境におけるプレフィックス一覧

サービスプロバイダ	プレフィックス空間	割り当てられるプレフィックス
ISP　（A）	2001:db8:a::/48	2001:db8:a:1::/64
ASP-1　（B）	2001:db8:10b::/48	2001:db8:10b:1::/64
ASP-2　（C）	2001:db8:c::/48	2001:db8:c:1::/64
ASP-3　（D）	2001:db8:10d::/48	－

以下に実施する検証項目をまとめる。

- **検証項目1**

初期設定のポリシーテーブルにて以下の挙動の確認をそれぞれの端末 OS にて実施する。

② ISP の先にあるとする端末（2001:db8:e:1::1）への通信

③ ASP-3 にある端末（2001:db8:10d:1::1）への通信

- **検証項目2**

想定環境下において、アドレス選択問題を解決する挙動を期待できるアドレス選択ポリシーを設定した状態で、以下の挙動の確認をそれぞれの端末 OS にて実施する。

① ISP の先にあるとする端末（2001:db8:e:1::1）への通信

② ASP-3 にある端末（2001:db8:10d:1::1）への通信

検証項目 2 で設定するポリシーテーブルを表 5-3 に示す。ISP からのプレフィックスに IPv6 アドレスを表す「::/0」と同じラベルを設定し、その他のプレフィックスは ASP 毎に独立したラベルとしている。

表 5-3　検証項目 2 で利用するポリシーテーブル設定

プレフィックス	優先順位	ラベル
::1/128	50	0
2001:db8:a::/48	40	1
2001:db8:10b::/48	40	11
2001:db8:c::/48	40	12
2001:db8:10d::/48	40	12
::/0	40	1
2002::/16	30	2
::/96	20	3
::ffff:0:0/96	10	4

以上の各検証に用いる通信には ping6（Windows Vista の場合は ping –6）を利用し、送信元アドレスの確認を行う。

5.4.5 検証結果

- **検証項目1**

アドレスの最長一致により、第 2 ヘクサデシット[7]目まで同じ 3 つのプレフィックス（A、B、C）によるアドレスが送信元アドレスの候補となり、第 3 ヘクサデシット目の一致量で送信元アドレスが選択された。

通信①では 2001:db8:c:1::/64 のプレフィックスによるアドレスが、通信②では 2001:db8:10b:1::/64 のプレフィックスによるアドレスがそれぞれ選択され通信が開始されることを確認した。これらの双方において、対象とした 3 つの端末 OS は共に同じ挙動を示すことを確認している。

参考として、図 5-13 と図 5-14 に最長一致で選択される様子を示す。

[7] ヘクサデシット（hexadecet）：16 ビットを表す情報量のことで、ここでは「:」で区切られた IPv6 アドレスの数値を指す

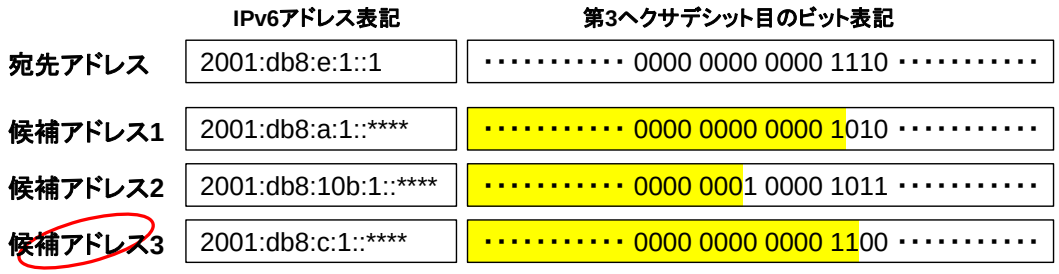

図 5-13　通信①における最長一致での送信元アドレス選択

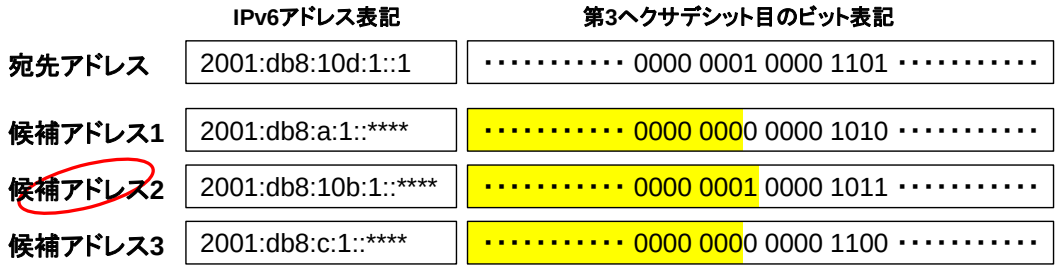

図 5-14　通信②における最長一致での送信元アドレス選択

- 検証項目2

表 5-3 のポリシーテーブルの設定により、同じラベルのプレフィックスによるアドレスが選択された。

通信①では宛先アドレスが::/0 に含まれるため、ラベル値 1 を持つ 2001:db8:a:1::/64 のプレフィックスによるアドレスが、通信②では 2002:db8:10d::/32 と同じラベル値 12 を持つ 2001:db8:c:1::/64 のプレフィックスによるアドレスがそれぞれ選択され通信が開始されることを確認した。検証項目 1 と同様に、これらの双方において、対象とした 3 つの端末 OS は共に同じ挙動を示すことを確認している。

5.4.6 検証データ

- **検証項目1**

検証時のインターフェイス情報と初期設定のポリシーテーブル、ping6/ping -6 を検証アドレスに実行した結果を各端末 OS 毎にまとめる。

[FreeBSD 5.5 Release]

インターフェイス情報

```
% ifconfig
 :
fxp0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=b<RXCSUM,TXCSUM,VLAN_MTU>
        inet6 fe80::***:****:fe53:1c24%fxp0 prefixlen 64 scopeid 0x1
        inet 192.168.1.28 netmask 0xffffff00 broadcast 192.168.1.255
        inet6 2001:db8:a:1:***:****:fe53:1c24 prefixlen 64 autoconf
        inet6 2001:db8:10b:1:***:****:fe53:1c24 prefixlen 64 autoconf
        inet6 2001:db8:c:1:***:****:fe53:1c24 prefixlen 64 autoconf
        ether **:**:**:53:1c:24
        media: Ethernet autoselect (10baseT/UTP)
        status: active
```

ポリシーテーブル

```
% ip6addrctl
Prefix                    Prec Label    Use
::1/128                     50     0      0
::/0                        40     1     93
2002::/16                   30     2      0
::/96                       20     3      0
::ffff:0.0.0.0/96           10     4      0
```

Ping の実行結果

```
% ping6 2001:db8:e:1::1
PING6(56=40+8+8 bytes) 2001:db8:c:1:***:****:fe53:1c24 --> 2001:db8:e:1::1
 :
% ping6 2001:db8:10d:1::1
PING6(56=40+8+8 bytes) 2001:db8:10b:1:***:****:fe53:1c24 --> 2001:db8:10d:1::1
 :
```

[Windows XP SP2]

インターフェイス情報

```
--------------------------------------------------------------------------------
C:¥>ipconfig
 :
Ethernet adapter ローカル エリア接続:

      Connection-specific DNS Suffix  . :
      IP Address. . . . . . . . . . . . : 192.168.1.40
      Subnet Mask . . . . . . . . . . . : 255.255.255.0
      IP Address. . . . . . . . . . . . : 2001:db8:a:1:ddda:9b7d:a44d:9548
      IP Address. . . . . . . . . . . . : 2001:db8:a:1:***:****:fe48:8d04
      IP Address. . . . . . . . . . . . : 2001:db8:10b:1:ddda:9b7d:a44d:9548
      IP Address. . . . . . . . . . . . : 2001:db8:10b:1: ***:****:fe48:8d04
      IP Address. . . . . . . . . . . . : 2001:db8:c:1:ddda:9b7d:a44d:9548
      IP Address. . . . . . . . . . . . : 2001:db8:c:1: ***:****:fe48:8d04
      IP Address. . . . . . . . . . . . : fe80:: ***:****:fe48:8d04%5
      Default Gateway . . . . . . . . . : 192.168.1.254
                                          fe80:: ***:****:fe51:e7fe%5
--------------------------------------------------------------------------------
```

ポリシーテーブル

```
--------------------------------------------------------------------------------
C:¥>netsh interface ipv6 show prefixpolicy
アクティブ状態を照会しています...

Precedence  Label  Prefix
----------  -----  ------------------------------
         5      5  2001::/32
        10      4  ::ffff:0:0/96
        20      3  ::/96
        30      2  2002::/16
        40      1  ::/0
        50      0  ::1/128
--------------------------------------------------------------------------------
```

Ping の実行結果

```
--------------------------------------------------------------------------------
C:¥>ping6 2001:db8:e:1::1
Pinging 2001:db8:e:1::1
from 2001:db8:c:1:ddda:9b7d:a44d:9548 with 32 bytes of data:

要求はタイム アウトしました。
 :
C:¥>ping6 2001:db8:10d:1::1
Pinging 2001:db8:10d:1::1
from 2001:db8:10b:1:ddda:9b7d:a44d:9548 with 32 bytes of data:

要求はタイム アウトしました。
 :
--------------------------------------------------------------------------------
```

[Windows Vista]

インターフェイス情報

```
---------------------------------------------------------------------------
C:¥>ipconfig
 :
イーサネット アダプタ ローカル エリア接続:

   接続固有の DNS サフィックス . . :
   IPv6 アドレス . . . . . . . . . . : 2001:db8:a:1:25d6:3d69:bbef:c800
   IPv6 アドレス . . . . . . . . . . : 2001:db8:c:1:25d6:3d69:bbef:c800
   IPv6 アドレス . . . . . . . . . . : 2001:db8:10b:1:25d6:3d69:bbef:c800
   一時 IPv6 アドレス. . . . . . . . : 2001:db8:a:1:a4af:e581:a323:ce7e
   一時 IPv6 アドレス. . . . . . . . : 2001:db8:c:1:a4af:e581:a323:ce7e
   一時 IPv6 アドレス. . . . . . . . : 2001:db8:10b:1:a4af:e581:a323:ce7e
   リンクローカル IPv6 アドレス. . . : fe80::25d6:3d69:bbef:c800%8
   IPv4 アドレス . . . . . . . . . . : 192.168.1.38
   サブネット マスク . . . . . . . . : 255.255.255.0
   デフォルト ゲートウェイ . . . . . : fe80::*:*:fe51:e7fe%8
                                       192.168.1.254
---------------------------------------------------------------------------
```

ポリシーテーブル

```
---------------------------------------------------------------------------
C:¥>netsh interface ipv6 show prefixpolicies
アクティブ状態を照会しています...

優先順位    ラベル  プレフィックス
----------  -----  --------------------------------
        50      0  ::1/128
        40      1  ::/0
        30      2  2002::/16
        20      3  ::/96
        10      4  ::ffff:0:0/96
         5      5  2001::/32
---------------------------------------------------------------------------
```

Ping の実行結果

```
---------------------------------------------------------------------------
C:¥>ping -6 2001:db8:e:1::1
2001:db8:e:1::1 に ping を送信しています 2001:db8:c:1:a4af:e581:a323:ce7e から
32 バイトのデータ:

要求はタイム アウトしました。
 :
C:¥>ping -6 2001:db8:10d:1::1
2001:db8:10d:1::1 に ping を送信しています 2001:db8:10b:1:a4af:e581:a323:ce7e
から 32 バイトのデータ:

要求はタイム アウトしました。
 :
---------------------------------------------------------------------------
```

- **検証項目2**

検証時のポリシーテーブル、Ping を検証アドレスに実行した結果を各端末 OS 毎にまとめる（インターフェイス情報は検証項目 1 に同じなので割愛する）。

[FreeBSD 5.5 Release]

ポリシーテーブル

```
% ip6addrctl
Prefix                          Prec Label       Use
::1/128                           50     0         0
::/0                              40     1       103
2002::/16                         30     2         0
::/96                             20     3         0
::ffff:0.0.0.0/96                 10     4         0
2001:db8:a::/48                   40     1         0
2001:db8:10b::/48                 40    11         0
2001:db8:c::/48                   40    12         0
2001:db8:10d::/48                 40    12         0
```

Ping の実行結果

```
% ping6 2001:db8:e:1::1
PING6(56=40+8+8 bytes) 2001:db8:a:1:***:****:fe53:1c24 --> 2001:db8:e:1::1
16 bytes from 2001:db8:e:1::1, icmp_seq=0 hlim=64 time=0.335 ms
 :
% ping6 2001:db8:10d:1::1
PING6(56=40+8+8 bytes) 2001:db8:c:1:***:****:fe53:1c24 --> 2001:db8:10d:1::1
16 bytes from 2001:db8:10d:1::1, icmp_seq=0 hlim=64 time=0.300 ms
 :
```

[Windows XP SP2]

ポリシーテーブル

```
C:¥>netsh interface ipv6 show prefixpolicy
アクティブ状態を照会しています...

Precedence  Label  Prefix
----------  -----  ------------------------------
        50      0  ::1/128
        40      1  2001:db8:a::/48
        40     11  2001:db8:10b::/48
        40     12  2001:db8:c::/48
        40     12  2001:db8:10d::/48
        40      1  ::/0
        30      2  2002::/16
        20      3  ::/96
        10      4  ::ffff:0:0/96
```

Ping の実行結果

```
--------------------------------------------------------------------------------
C:¥>ping6 2001:db8:e:1::1
Pinging 2001:db8:e:1::1
from 2001:db8:a:1:ddda:9b7d:a44d:9548 with 32 bytes of data:

Reply from 2001:db8:e:1::1: bytes=32 time=5ms
 :
C:¥>ping6 2001:db8:10d:1::1
Pinging 2001:db8:10d:1::1
from 2001:db8:c:1:ddda:9b7d:a44d:9548 with 32 bytes of data:

Reply from 2001:db8:10d:1::1: bytes=32 time=5ms
 :
--------------------------------------------------------------------------------
```

[Windows Vista]

ポリシーテーブル

```
--------------------------------------------------------------------------------
C:¥>netsh interface ipv6 show prefixpolicies
アクティブ状態を照会しています...

優先順位    ラベル  プレフィックス
----------  -----  --------------------------------
        50      0  ::1/128
        40      1  2001:db8:a::/48
        40     11  2001:db8:10b::/48
        40     12  2001:db8:c::/48
        40     12  2001:db8:10d::/48
        40      1  ::/0
        30      2  2002::/16
        20      3  ::/96
        10      4  ::ffff:0:0/96
--------------------------------------------------------------------------------
```

Ping の実行結果

```
--------------------------------------------------------------------------------
C:¥>ping -6 2001:db8:e:1::1
2001:db8:e:1::1 に ping を送信しています 2001:db8:a:1:a4af:e581:a323:ce7e から
32 バイトのデータ:

2001:db8:e:1::1 からの応答: 時間 =533ms
 :
C:¥>ping -6 2001:db8:10d:1::1
2001:db8:10d:1::1 に ping を送信しています 2001:db8:c:1:a4af:e581:a323:ce7e
から 32 バイトのデータ:

2001:db8:10d:1::1 からの応答: 時間 =504ms
 :
--------------------------------------------------------------------------------
```

5.4.7 考察

本節では、インターフェイスに複数のアドレスが付与されるマルチプレフィックス環境において発生する送信元アドレス選択問題を取り上げた。この問題の解決手法の 1 つとして、RFC3484 に提案されているアドレス選択ポリシーテーブルの検証を実施し、ポリシーテーブル操作で問題解決が可能であると確認した。この検証には用いた IPv6 端末 OS は FreeBSD、Windows XP SP2、Windows Vista であり、それぞれにおいて動作検証することができた。

しかしながら、現在の仕様を基にして利用者が端末に対して手動で設定を行うことは、サービス提供として現実的ではない。そのためとして、ポリシーテーブルの自動設定機能が有効であるとする議論もあり、IPv6 における標準的なネットワーク自動設定技術（RA や DHCP）の拡張により行う技術の標準化なども進められている。また、その他の対応手法も含め、本節の問題に関するより詳しい議論は、IPv6 普及・高度化推進協議会におけるマルチプレフィックス SWG にて実施されているので参考にしていただきたい。

最後に、今回検証に用いた各端末 OS におけるポリシーテーブルの操作方法を、検証用の設定を実施する場合を例に取り上げて以下にまとめる。

◆アドレス選択ポリシーテーブル設定コマンド

[FreeBSD 5.5 Release]

```
ip6addrctl add <prefix> <precedence> <label>                                    ☆
```

※root 権限で実行。/etc/rc.conf にて ip6addrctl_enable="YES"としておく必要がある。

```
-------------------------------------------------------------------------------
# ip6addrctl add 2001:db8:a::/48 40 0                                           ☆
# ip6addrctl add 2001:db8:10b::/48 40 11                                        ☆
# ip6addrctl add 2001:db8:c::/48 40 12                                          ☆
# ip6addrctl add 2001:db8:10d::/48 40 12                                        ☆
-------------------------------------------------------------------------------
```

[Windows XP SP2]

```
netsh interface ipv6 set prefixpolicy <prefix> <precedence> <label>             ☆
```

※管理者権限で実行。初めての実行時には全てのエントリを設定する必要がある。

```
-------------------------------------------------------------------------------
C:¥>netsh interfave ipv6 set prefixpolicy ::1/128 50 0                          ☆
C:¥>netsh interfave ipv6 set prefixpolicy 2001:db8:a::/48 40 1                  ☆
C:¥>netsh interfave ipv6 set prefixpolicy 2001:db8:10b::/48 40 11               ☆
C:¥>netsh interfave ipv6 set prefixpolicy 2001:db8:c::/48 40 12                 ☆
C:¥>netsh interfave ipv6 set prefixpolicy 2001:db8:10d::/48 40 12               ☆
C:¥>netsh interfave ipv6 set prefixpolicy ::/0 40 1                             ☆
C:¥>netsh interfave ipv6 set prefixpolicy 2002::/16 30 2                        ☆
C:¥>netsh interfave ipv6 set prefixpolicy ::/96 20 3                            ☆
C:¥>netsh interfave ipv6 set prefixpolicy ::ffff:0:0/96 10 4                    ☆
-------------------------------------------------------------------------------
```

[Windows Vista]

netsh interface ipv6 <set | add> prefixpolicy <prefix> <precedence> <label>　　☆

※管理者権限で実行。初めての実行時には最初のエントリのみ set を指定し、以後は add を用いる。また、全てのエントリを設定する必要がある。

```
C:¥>netsh interfave ipv6 set prefixpolicy ::1/128 50 0                    ☆
C:¥>netsh interfave ipv6 add prefixpolicy 2001:db8:a::/48 40 1            ☆
C:¥>netsh interfave ipv6 add prefixpolicy 2001:db8:10b::/48 40 11         ☆
C:¥>netsh interfave ipv6 add prefixpolicy 2001:db8:c::/48 40 12           ☆
C:¥>netsh interfave ipv6 add prefixpolicy 2001:db8:10d::/48 40 12         ☆
C:¥>netsh interfave ipv6 add prefixpolicy ::/0 40 1                       ☆
C:¥>netsh interfave ipv6 add prefixpolicy 2002::/16 30 2                  ☆
C:¥>netsh interfave ipv6 add prefixpolicy ::/96 20 3                      ☆
C:¥>netsh interfave ipv6 add prefixpolicy ::ffff:0:0/96 10 4              ☆
```

◆アドレス選択ポリシーテーブル確認コマンド

[FreeBSD 5.5 Release]

```
% ip6addrctl [show]
```

※/etc/rc.conf にて ip6addrctl_enable="YES"としておく必要がある。

[Windows XP SP2]

```
C:¥>netsh interfave ipv6 show preficpolicy
```

[Windows Vista]

```
C:¥>netsh interfave ipv6 show preficpolicies
```

※Windows XP の場合と最後の文字が若干異なる点に注意。

5.5　複数のルータ配下における経路選択の問題

5.5.1 問題の背景と概要

インターネットへの接続に冗長性を持たせるためのマルチホーム環境など、端末 OS が複数のネクストホップ（パケットを転送するルータ）を持ち、通信時にパケットの転送先を決定する必要がある環境がある。この時、端末 OS ではネクストホップを適切に選択する必要があり、選択手法の実装が必要となる。

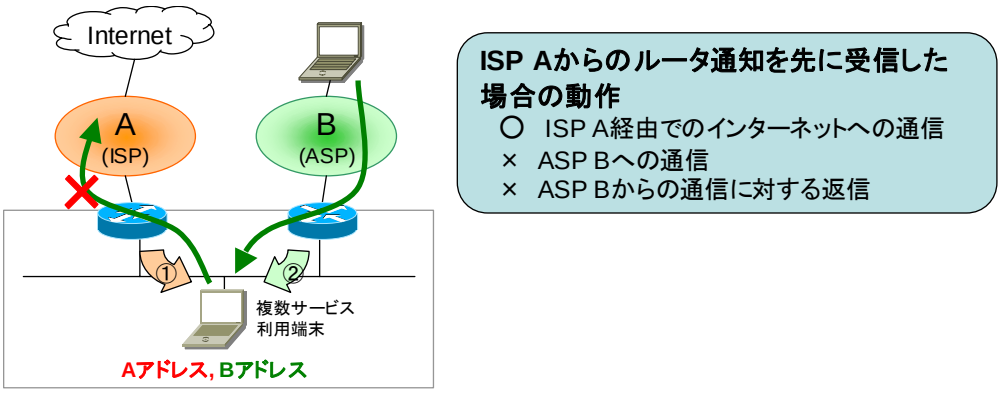

図 5-15　経路選択問題が発生しうる想定環境

一例として、同一リンク上に複数のルータが配置され、経路選択問題が発生するネットワーク構成を図 5-15 に示す。この図のように、複数のルータへの接続性を持つホストは、どちらのルータをデフォルトルータにして良いのか判断できなくなる。これは、複数のルータ通知（RA）が流されたとき、どちらのルータをデフォルトルータにするべきか、判断基準がないために発生する問題である。

多くの IPv6 端末の実装では、先に受信した RA の情報を優先するようになっており、複数のデフォルトルートを想定通りに扱うことができない。また、ルータから出される RA にも優先順位を指定して端末に情報を伝える必要があると考えられる。

5.5.2 検証内容

この経路選択問題を解決する手法として、RFC4191 にて定義されている RA の拡張機能が考えられる。RFC4191 では、RA の追加知能として、ルータ優先度フラグが定義されている。ルータ通知のフラグフィールドに 3 段階（01 : high、00:medium（初期値）、11:low）で優先度を指定でき、端末 OS では受信したデフォルトルートに優先順位を付けられる。また、対応していない RA ではこの RFC にて定義されているフラグフィールドは初期値の

medium 設定となる。

また、RFC4191 では、経路情報通知オプション機能（more-specific route）も定義されている。これによって、デフォルトルートだけでなく、特定の経路情報をルータから通知することができ、IPv6 端末 OS に対して経路制御プロトコルのように経路を柔軟に配布することが可能となる。

本節では、RFC4191 における RA の拡張機能に関する動作を確認するため、以下の 3 項目の検証を行う。

1. RA 拡張機能なしの場合における挙動の確確認
2. ルータ優先度フラグを利用した場合の挙動
3. 経路情報通知オプションを利用した場合の挙動

対象とする端末 OS には Windows XP SP2、Windows Vista を用い、RA の実装として Linux の radvd を利用する。なお、FreeBSD の rtadvd においても RFC4191 の機能は実装されている。

5.5.3 検証手順

検証に用いたネットワーク環境を図 5-16 に示す。

ルータ A からプレフィックス（2001:db8:a:1::/64）を含めた RA を流しておき、RA の拡張機能は利用しない。ルータ B からは、端末が接続された後で RA を送信する。ルータ B からの RA において検証項目における拡張機能を付加して検証を行う。

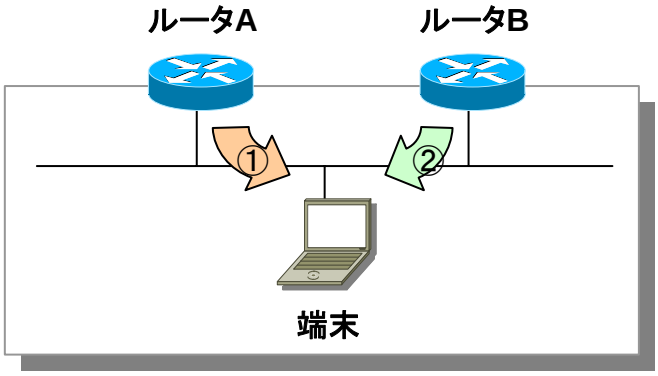

図 5-16　経路選択問題の検証環境

- **検証項目1**

1. ルータ A から拡張機能を利用しない RA を送信し、検証端末を接続する。
2. Ping により、ルータ A の向うの端末（2001:db8:a::1）への通信を確認する。
3. ルータ B から拡張機能を利用しない RA を送信し、2.の確認を実施する。

- **検証項目2**

  1. ルータ A から拡張機能を利用しない RA を送信し、検証端末を接続する。
  2. Ping により、ルータ A の向うの端末（2001:db8:a::1）への通信を確認する。
  3. ルータ B からルータ優先度フラグを high にした RA を送信し、2.の確認を実施する。

- **検証項目3**

  1. ルータ A から拡張機能を利用しない RA を送信し、検証端末を接続する。
  2. Ping により、ルータ A の向うの端末（2001:db8:a::1）への通信を確認する。
  3. ルータ B からルータ経路情報通知オプションに 2001:db8:b::/48 を設定した RA を送信する。
  4. 2001:db8:a::1 と 2001:db8:b::1 への通信を確認する。

5.5.4 検証結果

- **検証項目1**

Windows XP SP2 では、ルータ B の RA によるデフォルトルートが同じメトリック値で追加され、追加されたデフォルトルートが利用される。

Windows Vista では、ルータ B の RA によるデフォルトルートが同じメトリック値で追加されるが、Windows XP SP2 とは異なり、追加されたデフォルトルートは利用されない。

- **検証項目2**

Windows XP SP2 と Windows Vista では、ルータ B の RA によるデフォルトルートが低いメトリック値で追加され、追加されたデフォルトルートが利用される。両端末 OS 伴に、ルータ優先度を low にすると高いメトリックで追加され、ルータ A のデフォルトルートがそのまま利用される。

- **検証項目3**

Windows Vista では、ルータ B の RA による経路情報が追加され、両方の検証ターゲットに通信することが可能であった。

以上の検証結果を表 5-4 にまとめる。表中の A および B は、本検証にて A→B の順で RA を付与した際に、優先的に利用されるものを示している。

表 5-4　RFC4191 の動作検証結果

	ルータ優先度			経路情報通知
	low	medium	high	
Windows XP	B	B	A	未対応
Windows Vista	B	A	A	対応

5.5.5 検証データ

- **検証項目1**

ルータ A からのみ RA を受信していた場合のルーティングテーブルと ping6/ping -6 の実行結果、ルータ B からの RA を追加した場合のルーティングテーブルと ping6/ping -6 の実行結果を各端末 OS 毎にまとめる。

[Windows XP SP2]

ルータ A の RA のみ受信時のルーティングテーブルと Ping の実行結果

```
-------------------------------------------------------------------------------
C:¥>netsh interface ipv6 show route
アクティブ状態を照会しています...

Publish  Type       Met  Prefix                    Idx  Gateway/Interface Name
-------  --------  ----  ------------------------  ---  --------------------
no       Autoconf   256  ::/0                        5  fe80::***:****:fefe:8c1b
no       Autoconf     8  2001:c90:780:1011::/64      5  ローカル エリア接続

C:¥>ping6 2001:db8:a::1
Pinging 2001:db8:a::1
from 2001:db8:a:1:ddda:9b7d:a44d:9548 with 32 bytes of data:

Reply from 2001:db8:a::1: bytes=32 time=5ms
 :
-------------------------------------------------------------------------------
```

ルータ B の RA を追加した時のルーティングテーブルと Ping の実行結果

```
-------------------------------------------------------------------------------
C:¥>netsh interface ipv6 show route
アクティブ状態を照会しています...

Publish  Type       Met  Prefix                    Idx  Gateway/Interface Name
-------  --------  ----  ------------------------  ---  --------------------
no       Autoconf   256  ::/0                        5  fe80::***:****:fe51:e7fe
no       Autoconf   256  ::/0                        5  fe80::***:****:fefe:8c1b
no       Autoconf     8  2001:c90:780:1011::/64      5  ローカル エリア接続

C:¥>ping6 2001:db8:a::1
Pinging 2001:db8:a::1
from 2001:db8:a:1:ddda:9b7d:a44d:9548 with 32 bytes of data:

要求はタイム アウトしました。
 :
-------------------------------------------------------------------------------
```

[Windows Vista]

ルータ A の RA のみ受信時のルーティングテーブルと Ping の実行結果

```
-------------------------------------------------------------------------------
C:¥>netsh interface ipv6 show route

発行     種類     Met  プレフィックス          Idx ゲートウェイ/インターフェイス名
-------  -------  ---  --------------------  ---  -------------------------
いいえ   Manual   286  ::/0                    8   fe80::***:****:fefe:8c1b
いいえ   Manual   306  ::1/128                 1   Loopback Pseudo-Interface 1
いいえ   Manual    38  2001:db8:a:1::/64       8   ローカル エリア接続
いいえ   Manual   286  2001:db8:a:1:25d6:3d69:bbef:c800/128 10 ローカル エリア接続
 :
C:¥>ping -6 2001:db8:a::1
2001:db8:a::1 に ping を送信しています 2001:db8:a:1:a4af:e581:a323:ce7e から
32 バイトのデータ:

2001:db8:a::1 からの応答: 時間 =533ms
 :
-------------------------------------------------------------------------------
```

ルータ B の RA を追加した時のルーティングテーブルと Ping の実行結果

```
-------------------------------------------------------------------------------
C:¥>netsh interface ipv6 show route

発行     種類     Met  プレフィックス          Idx ゲートウェイ/インターフェイス名
-------  -------  ---  --------------------  ---  -------------------------
いいえ   Manual   286  ::/0                    8   fe80::***:****:fefe:8c1b
いいえ   Manual   286  ::/0                    8   fe80::***:****:fe51:e7fe
いいえ   Manual   306  ::1/128                 1   Loopback Pseudo-Interface 1
いいえ   Manual    38  2001:db8:a:1::/64       8   ローカル エリア接続
いいえ   Manual   286  2001:db8:a:1:25d6:3d69:bbef:c800/128 10 ローカル エリア接続
 :
C:¥>ping -6 2001:db8:a::1
2001:db8:a::1 に ping を送信しています 2001:db8:a:1:a4af:e581:a323:ce7e から
32 バイトのデータ:

2001:db8:a::1 からの応答: 時間 =533ms
 :
-------------------------------------------------------------------------------
```

- **検証項目2**

ルータ B からの RA を追加した場合のルーティングテーブルと ping6/ping -6 の実行結果を各端末 OS 毎にまとめる（ルータ A のみの場合は検証項目 1 に同じ）。

[Windows XP SP2]

ルータ B の RA を追加した時のルーティングテーブルと Ping の実行結果

```
------------------------------------------------------------------------------
C:¥>netsh interface ipv6 show route
アクティブ状態を照会しています...

Publish  Type       Met  Prefix                    Idx  Gateway/Interface Name
-------  ---------  ---  ------------------------  ---  ---------------------
no       Autoconf    16  ::/0                        5  fe80::***:****:fe51:e7fe
no       Autoconf   256  ::/0                        5  fe80::***:****:fefe:8c1b
no       Autoconf     8  2001:c90:780:1011::/64      5  ローカル エリア接続

C:¥>ping6 2001:db8:a::1
Pinging 2001:db8:a::1
from 2001:db8:a:1:ddda:9b7d:a44d:9548 with 32 bytes of data:

要求はタイム アウトしました。
 :
------------------------------------------------------------------------------
```

[Windows Vista]

ルータ B の RA を追加した時のルーティングテーブルと Ping の実行結果

```
------------------------------------------------------------------------------
C:¥>netsh interface ipv6 show route

発行      種類      Met  プレフィックス                Idx ゲートウェイ/インターフェイス名
------    -------   ---  --------------------  ---  ------------------------
いいえ    Manual    286  ::/0                    8   fe80::***:****:fefe:8c1b
いいえ    Manual     46  ::/0                    8   fe80::***:****:fe51:e7fe
いいえ    Manual    306  ::1/128                 1   Loopback Pseudo-Interface 1
いいえ    Manual     38  2001:db8:a:1::/64       8   ローカル エリア接続
いいえ    Manual    286  2001:db8:a:1:25d6:3d69:bbef:c800/128 10 ローカル エリア接続
 :
C:¥>ping -6 2001:db8:a::1
2001:db8:a::1 に ping を送信しています 2001:db8:a:1:a4af:e581:a323:ce7e から
32 バイトのデータ:

要求はタイム アウトしました。
 :
------------------------------------------------------------------------------
```

- **検証項目3**

ルータ B からの RA を追加した場合のルーティングテーブルと ping6/ping –6 の実行結果を各端末 OS 毎にまとめる（ルータ A のみの場合は検証項目 1 に同じ）。

[Windows XP SP2]

ルータ B の RA を追加した時のルーティングテーブルと Ping の実行結果

```
------------------------------------------------------------------------------
C:¥>netsh interface ipv6 show route
アクティブ状態を照会しています...

Publish  Type       Met  Prefix                    Idx  Gateway/Interface Name
-------  ---------  ---  ------------------------  ---  ---------------------
no       Autoconf   256  ::/0                        5  fe80::***:****:fe51:e7fe
no       Autoconf   256  ::/0                        5  fe80::***:****:fefe:8c1b
no       Autoconf     8  2001:c90:780:1011::/64      5  ローカル エリア接続

C:¥>ping6 2001:db8:a::1
Pinging 2001:db8:a::1
from 2001:db8:a:1:ddda:9b7d:a44d:9548 with 32 bytes of data:

要求はタイム アウトしました。
 :
C:¥>ping6 2001:db8:b::1
Pinging 2001:db8:b::1
from 2001:db8:a:1:ddda:9b7d:a44d:9548 with 32 bytes of data:

要求はタイム アウトしました。
 :
------------------------------------------------------------------------------
```

[Windows Vista]

ルータ B の RA を追加した時のルーティングテーブルと Ping の実行結果

```
------------------------------------------------------------------------------
C:¥>netsh interface ipv6 show route

発行     種類     Met  プレフィックス                  Idx ゲートウェイ/インターフェイス名
-------  -------  ---  ---------------------  ---  ------------------------
いいえ   Manual   286  ::/0                     8   fe80::***:****:fefe:8c1b
いいえ   Manual   286  ::/0                     8   fe80::***:****:fe51:e7fe
いいえ   Manual   306  ::1/128                  1   Loopback Pseudo-Interface 1
いいえ   Manual    38  2001:db8:a:1::/64        8   ローカル エリア接続
いいえ   Manual   286  2001:db8:a:1:25d6:3d69:bbef:c800/128 10 ローカル エリア接続
いいえ   Manual   286  2001:db8:a:1:a4af:e581:a323:ce7e/128 10 ローカル エリア接続
いいえ   Manual   286  2001:db8:b:1::/64        8   fe80::***:****:fe51:e7fe
 :
C:¥>ping -6 2001:db8:a::1
2001:db8:a::1 に ping を送信しています 2001:db8:a:1:a4af:e581:a323:ce7e から
32 バイトのデータ:
```

```
2001:db8:a::1 からの応答: 時間 =533ms
:
C:¥>ping -6 2001:db8:b::1
2001:db8:b::1 に ping を送信しています 2001:db8:a:1:a4af:e581:a323:ce7e から
32 バイトのデータ:

2001:db8:b::1 からの応答: 時間 =533ms
:
--------------------------------------------------------------------------------
```

5.5.6 考察

本節では、同一リンク上に複数のルータが配置された際に発生する経路選択問題に関して取り上げた。この中で、1 つの解決方法である RFC4191 について調査し、Windows XP SP2 と Windows Vista を用いて動作検証を行った。

ルータ優先度に関しては、デフォルト値（medium）の場合の挙動に違いが見られ、Windows XP SP2 では後で認識したもの、Windows Vista では先に認識したものがそれぞれ優先される結果であった。また、優先度を low および high で指定することで、意図した挙動を示すことが確認でき、経路選択問題の解決手段として利用できると考えられる。

経路情報通知オプションに関しては、Windows Vista にて実装を確認することができ、意図する動作を実現できることを検証した。これによって、デフォルトルートだけでなく、通信可能な経路情報を通知可能となり、IPv6 端末 OS に対して経路制御プロトコルのように経路を柔軟に配布することが可能となる。

なお、今回の検証で用いなかった端末 OS の実装としては FreeBSD 6.1 Release があるが、経路情報通知オプションには対応していない。また、RA 実装に関しては、Linux の radvd を利用して検証したが、FreeBSD で使われている rtadvd での実装されている。
今回の検証にて取り上げた RFC4191 による解決手法以外にも、本節の問題を解決する手段は存在しており、より詳しい情報に関しては、IPv6 普及・高度化推進協議会におけるマルチプレフィックス SWG による考察文章を参考にしていただきたい。

6 まとめ

6.1 今回の活動では検討しきれなかった事項について

今回、IPv6 端末 OS のリリースに応じて発生しうる多数の問題をピックアップして、それら一つ一つについて検討を行った。しかしながら、今回挙げた問題で、全ての発生しうる問題をカバーできたわけではない。

現在既に上がっている検討すべき事柄として、下記がある。

- ユニークローカル IPv6 ユニキャストアドレス（Unique Local IPv6 Unicast Address/ULA）を利用した実運用形態
- アドホックネットワークの構築形態・取り扱い
- IPsec を利用する際の鍵交換プロトコルの選定について

これらについては、今後ウォッチしていくべき検討事項である。当該 SWG として、今後も取り扱うことができれば幸いである。

6.2 当該ガイドラインの最後として

従来、Mac OS X や Solaris、*BSD、Linux などの OS が IPv6 Ready となっていた。そして、今、たくさんのユーザを抱える Microsoft 社により IPv6 に初期設定で対応している Windows Vista がリリースされた。

これまで、業務用ルータが活発に IPv6 に対応してきたが、今後はさらに個人の端末も IPv6 化が進むと思われる。これによって、多数のアプリケーションソフトウェアや周辺機器、ISP のサービスなども IPv6 化するようになるだろう。

日本ではこれまでに、一部の環境では既に IPv6 対応が始まっており、また対応する機器も存在している。これらの機器や環境と、新しい IPv6 対応端末 OS が組み合わさることによって、また、新たなアプリケーションがリリースされることによって、ビジネスチャンスが生まれると思われる。それと同時に、新しい環境は比較的問題が発生しがちであることも理解しなければならない。

IPv6 に対応した新しい端末 OS と従来からの IPv6 環境が正常に通信できるのか、また IPv4 ばかりを扱ってきた環境は、IPv6 とともに動作するという新たな使用方法に充分に対応できるのか。

IPv6 がインターネット業界の成長をよりスムーズにさせるだけの技術的ポテンシャルを

持っていることは誰の目にも明らかであろう。このような技術を実運用で損傷させないように、発生しうる問題をできる限り事前に予測し、対処することが、IPv6 のスムーズな浸透、ひいては、インターネット業界の健全な成長に繋がると考えられる。

当該の活動はそれを目的として進めているものであり、この文章がその役に立つことを望んでいる。

A 付録

A.1 netsh コマンドについて

「netsh」コマンドは、コマンドラインにて Windows のネットワーク設定の参照や変更を実施するコマンドで、様々なネットワークプロトコルの設定に利用される。本節では、IPv6 に関連する機能に焦点を当てて利用方法をまとめる。また、扱う「netsh」コマンドは Windows Vista のものであり、他のバージョン（Windows XP や Windows 2000 等）とは挙動が異なる場合があるため注意が必要になる。

本ガイドラインにおけるコマンドラインの表記方法を以下に示す。

- 全て小文字で表記
- <>で囲まれた部分は適宜パラメータ値を設定する必要がある項目
- []で囲まれた部分は省略が可能な項目
- ☆が最後に付加されたコマンドは管理者権限が必要

「netsh」コマンドは、二種類の入力方法が存在する。引数をすべて記述して実行する方法と netsh シェルの状態にして対話式に入力する方法である。本節では前者の方法で全て解説する。なお、対話式モードへは netsh のみを入力することで移行することができ、コマンドプロンプトが「**netsh>**」に変化する。この状態で「**?**」を入力することで、利用可能なパラメータの一覧を得ることができる（図 A-1 参照）。

図 A-1　netsh シェル状態での利用方法例

- **管理者権限でのコマンドプロンプトの起動方法**

Windows Vista では、セキュリティ機能としてユーザアカウント制御（UAC：User Account Control）機能が初期設定で有効になっている。この UAC では、管理者権限が必要な処理を実行する度に確認を行うことで、許可されていないコンピュータへの変更を防止する機能を提供している。この動作は、管理者権限を有するユーザであっても、同様に確認が求められるため、セキュリティ向上のために有効な機能となっている。

本ガイドラインで紹介した設定コマンドのほとんどが管理者権限を必要とするコマンドで、コマンドプロンプトで実行する際にはあらかじめ管理者権限での起動が必要になる。管理者権限で起動する場合は、図 A-2 に示すように、コマンドプロンプト選択する際に右クリックして[管理者として実行(A)]を選択する。その後、確認を経て起動されたコマンドプロンプト上では、管理者権限が必要なコマンドも実行することが可能になる。

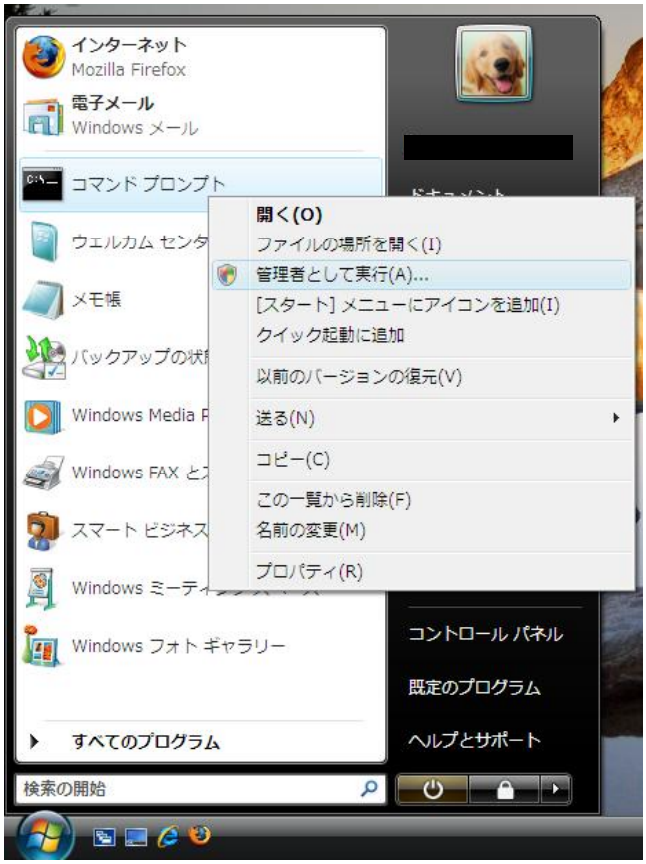

図 A-2　コマンドプロンプトを管理者として実行する方法

A.2　Windows ファイアウォールについて

- **WindowsファイアウォールとセキュリティがWindowsファイアウォール**

従来の Windows XP から Windows Vista に進化するにあたり、Windows ファイアウォールは大きな機能拡張が加えられた。そのため、Windows Vista では、

- 【コントロールパネル】→【Windows ファイアウォール】
- 【管理ツール】→【セキュリティが強化された Windows ファイアウォール】

という二つの、ファイアウォール制御用ユーザインターフェイス（以下 UI）を持っている。前者は Windows XP からの互換性を継承している UI で、後者はより詳細で柔軟な操作を可能にする UI となっている。たとえば、従来 IPsec の UI が netsh とローカルセキュリティポリシだけであった事に対して、Windows Vista では後者の【セキュリティが強化された Windows ファイアウォール】においても IPsec 制御のための UI が提供されている。

本文書の検証では、2.2 節、4.2 節、4.3 節における検証において後者の UI 操作を前提としており、また、5.1 節の検証については互換性を考慮して、前者の UI を利用している。

- **【セキュリティが強化されたWindowsファイアウォール】の起動方法**

起動の手順：
【スタート】から【コントロールパネル】を選択することで【コントロールパネル】が表示される（図 A-3）。このウィンドウの中の【システムとメンテナンス】をダブルクリック、表示される【システムとメンテナンス】ウィンドウ（図 A-4）内で【管理ツール】を選択する。その後表示されるウィンドウ内で【セキュリティが強化された Windows ファイアウォール】（図 A-5）を選択すれば起動する。

図 A-3　【コントロールパネル】ウィンドウの様子

図 A-4　【システムとメンテナンス】ウィンドウの様子

図 A-5　【管理ツール】ウィンドウの様子

以上の手順により、【セキュリティが強化された Windows ファイアウォール】が起動される。

- **IPsecにおけるSAの表示方法**

SA の表示方法：
上記図 A-6 の状況で、左ペインにある【監視】→【セキュリティアソシエーション】を選ぶことによって、中央のペインに現在張られている SA が記載される。
このとき、メインモードとクイックモードのどちらで構築されたのかを選択すれば、SA の最新状況が表示される。

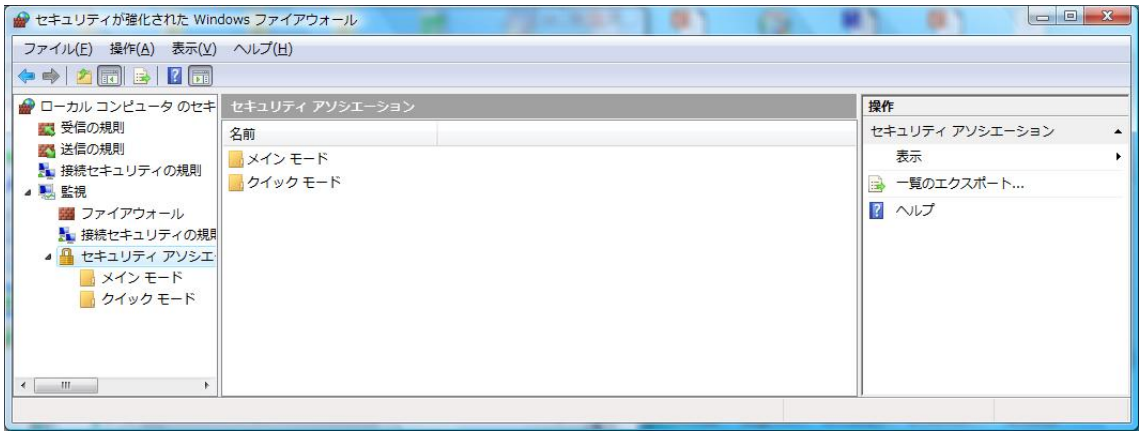

図 A-6　【セキュリティが強化された Windows ファイアウォール】ウィンドウの様子

図 A-5【管理ツール】ウィンドウの下のほうには、従来からあるローカルセキュリティポリシが存在しており、この UI でも IPsec の管理ができる。ただし、SA のリアルタイムの状況を得るのであれば、こちらの【セキュリティが強化された Windows ファイアウォール】の方が適している。【セキュリティが強化された Windows ファイアウォール】の UI を図 A-6 に示す。

A.3　IPv6 対応アプリケーション

参考情報として、Windows Vista において利用可能な IPv6 対応アプリケーション情報を以下にまとめる。いずれのアプリケーションに関しても 2007 年 3 月現在での対応状況となっている。

アプリケーション名	IPv6 対応状況	備考
リモートデスクトップ接続	○	
Windows リモートアシスタンス	○	
Windows ミーティングスペース	○	
Windows Media Player 11	○	
Internet Explorer 7.0	○	
パーソナル Firewall	○	
Windows メール	○	
共有フォルダ	○	
IIS 7.0	△	細かい設定は不可（IPv6 のみでリッスンの指定など）
Telnet Server	○	
Telnet Client	○	
FTP Server	×	
FTP Client	○	
Windows Live Messenger 8.1	△	レジストリの変更が必要
Microsoft Network Monitor 3.0	○	
Windows Media エンコーダ	○	
Microsoft Office Groove	×	
Microsoft Outlook 2007	○	
GUI によるネットワーク設定	○	
IPsec	○	機能のフルサポート
MLDv2	○	
LLMNR	○	
PPPv6	○	
DHCPv6	○	
WPAD（Web Proxy Auto-Discovery）	○	

参考 URL :

http://www.microsoft.com/japan/technet/community/columns/cableguy/cg1005.mspx