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

【第0版】

2006 年 12 月 15 日

IPv6 普及・高度化推進協議会

移行 WG　　IPv6 端末 OS 評価 SWG

1 組織・背景・目的

1.1 当該文書の背景と目的

当該文書は、IPv6 普及・高度化推進協議会(http://www.v6pc.jp/)における IPv6 端末 OS 評価 SWG のアウトプットである。

現在、一般ユーザの使う主要 OS で 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、一般ユーザの IPv6 利用による問題が起こる可能性があり、この発生しうる問題について検討を行う必要がある。

IPv6 端末 OS 評価 SWG はこの様な状況に鑑み、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、課題の整理などを行うものである。当該 SWG の具体的なアウトプットとして、下記の事柄を検討し、最終アウトプットとして、IPv6 端末 OS の IPv6 対応・機能活用ガイドラインである当該文書を作成した。

当該文書では、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）

本アウトプット文書ではこれらの事柄について、Microsoft 社の 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 のみに留まらず、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。

特に、当該文書は、下記の方々に読まれることを旨として記述した。

- 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、Internet 接続性を提供するサービスをご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。

1.2 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 ソフトウェア研究開発本部
北口善明【共同チェア】	株式会社インテック・ネットコア IPv6 研究開発グループ
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 IPv6 研究開発グループ
川島正伸	ＮＥＣアクセステクニカ株式会社 アクセスネットワーク技術部
島村潤	NTT コミュニケーションズ株式会社 ブロードバンド IP 事業部 サービスクリエーション部
鈴木聡介	NTT コミュニケーションズ株式会社 ネットビジネス事業本部 OCN サービス部
太田善之	NTT コミュニケーションズ株式会社 第三法人営業本部 ビジネスソリューション部
川村大輔	株式会社 NTT 東日本 ブロードバンドサービス部 フレッツネットワークセンタ
廣瀬和則	株式会社 NTT 東日本 ブロードバンドサービス部 フレッツネットワークセンタ
常川聡	株式会社ＮＴＴ東日本-神奈川 法人営業部 ブロードバンドビジネスソリューション部門
高村信【調査参加】	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【調査参加】	総務省 総合通信基盤局 電気通信事業部 データ通信課
神明達哉【オブザーバ】	株式会社 東芝 研究開発センター 通信プラットホームラボラトリー
加藤淳也	日本電信電話株式会社 情報流通プラットフォーム研究所
瀬川卓見	パナソニック コミュニケーションズ株式会社 開発研究所
酒井淳一	パナソニック コミュニケーションズ株式会社 開発研究所
猪俣彰浩	富士通株式会社　ネットワークサービス事業本部 FENICS システム統括部 サービス企画部

横田徹也	富士通株式会社　ネットワークサービス事業本部 FENICS システム統括部 サービス企画部
楠正憲【検討フォロー】	マイクロソフト株式会社 最高技術責任者補佐
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

1.3　第 0 版ガイドラインにおける注意事項

本ガイドラインは、代表的な商用 OS である Windows Vista の正式リリース前に公開し、IPv6 対応された OS の登場による影響を広く認知して頂く事を目的としています。そのため、検証内容は Windows Vista のβリリース版が中心となっており、この検証結果は商用版と異なる場合があることを認識しておく必要があります。

IPv6 端末 OS 評価 SWG では、この版は広く識者方から意見を戴くための版と位置づけており、誤りに対する修正やコメントなどを積極的取入れることで、2007 年 1 月下旬に予定している改訂版に反映して公開したいと考えています。

また、本ガイドラインにて取り上げていない検討項目もまだ多く存在しています。ULA（Unique Local IPv6 Unicast Addresses）の利用に関する課題やアドホックネットワークに関する課題など、今後の改訂版には追記してより有用な資料とする努力も引き続き実施したいと考えており、広く意見などを求めたいと考えています。

訂正やコメントなどの御意見がありましたら、下記のアドレスまでお送りください。2007 年 1 月下旬のラストコールまでに戴いた内容を検討し、ガイドラインとして発行したいと考えています。

お問い合わせ先：　v6os-info@v6pc.jp

2 ネットワークへの影響（既存 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置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の提示を目的とする。

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。しかしながら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、IPv4/IPv6 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、アプリケーションの挙動とあいまって、今後端末 OS の IPv6 対応が進むことで 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 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。

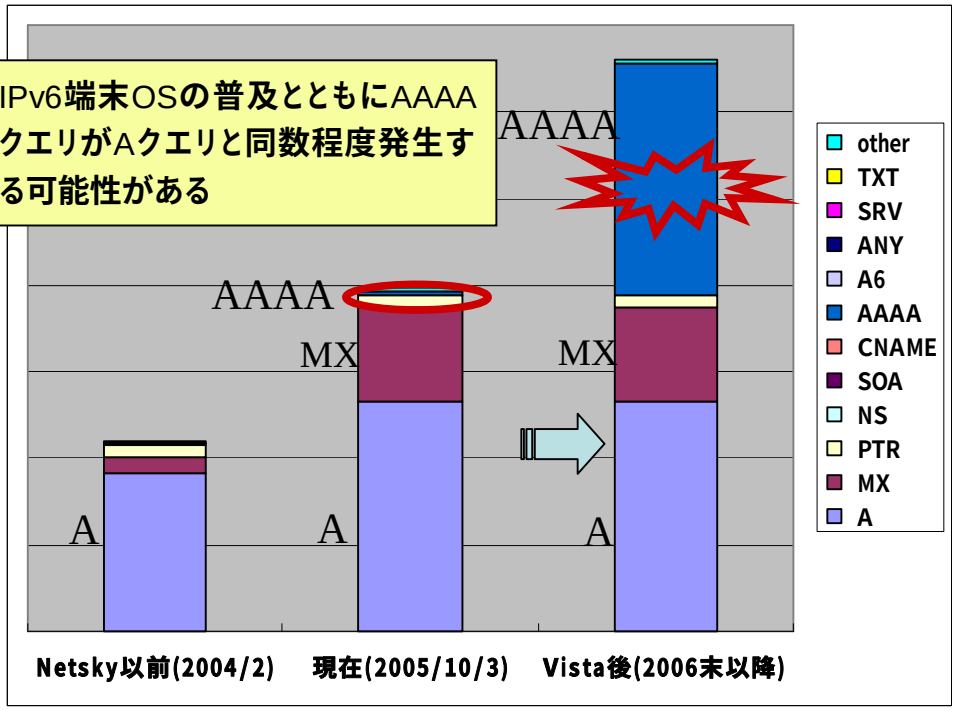


図 1　　DNS クエリ増加の予測

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。

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 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。

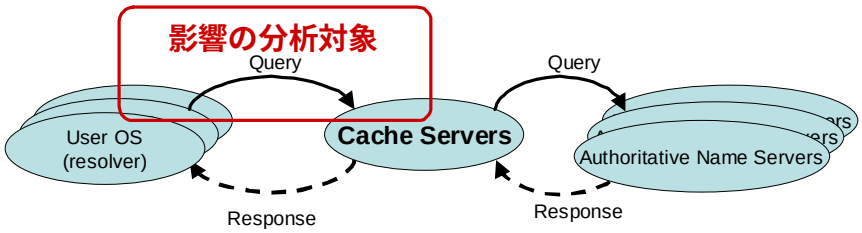


図 2　　DNS 負荷に関する検討の分析範囲

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推測する。

挙動 A. 端末 OS の IPv6 対応による IPv6 アドレスの解決機能の追加
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

2.1.4 DNS クエリの増加問題の検討と端末 OS の挙動

2.1.4.1　　挙動 A:　端末 OS の IPv6 対応による IPv6 アドレスの解決機能

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。しかし、IPv6 を有効化した端末 OS では、IPv6 アドレス（AAAA レコード）の解決も行われる。一般に、IPv4/IPv6 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 5.5-RELEASE、 Windows XP SP2 の挙動

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、IPv4 アドレス（A レコード）のクエリと同様に IPv6 アドレス（AAAA レコード）の解決も試みる。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。IPv4 アドレスの解決の結果が IPv6 アドレスの解決結果に依存することもない。

FreeBSD 5.5-RELEASE、Windows XP SP2 ではネットワークインターフェースに 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、IPv6 アドレスの解決を試みる。

- Windows Vista RC1 (Build 5600) の挙動

Windows Vista RC1 (Build 5600)ではネットワークインターフェースにIPv6グローバルアドレスを持たない場合はIPv6アドレスの解決が抑止される。またIPv6グローバルアドレスを持つ場合でも、IPv4アドレスの解決がIPv6アドレスの解決に対して先行して行われる。もしIPv4アドレスの解決に対する返答としてNXDOMAIN (no exist domain name)を受信した場合、IPv6アドレスの解決が抑制される。

なおNXDOMAINとはDNS応答コード３で表現されるメッセージであり、当該のホスト名に関するどのタイプのリソースレコードも存在しないことを示している。AAAAレコードの解決に対して、NXDOMAINが返却応答された場合はAレコードも存在しない。

2.1.4.2 挙動 B: 端末 OS によるドメインサフィックスの補完機能

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、FreeBSD 5.5-RELEASE、 Windows XP SP2/Vista RC1の場合、補完されるドメインサフィックスは下記の設定から決定される。

1. DHCP、 PPP接続時に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: /etc/resolv.conf への設定項目（domain, search）
   - Windows: マイコンピュータ名、ネットワークインターフェースのTCP/IPのプロパティ設定など

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 XP SP2/Vista RC1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ースの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ようなドメインサフィックスが設定した場合、ホスト名 "host" の名前解決を試みたとき、名前解決が成功するまで、下記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。

- host
- host.example1.jp
- host.example2.jp
- host.example3.jp

2.1.4.3 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

OS によって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 6 （Windows XP SP2）

  MSN Live Search へキーワードを転送し検索結果を表示

- Firefox 1.5.0.7 (Windows 向け日本語版）

  Google、 はてなダイアリーへキーワードを転送。検索結果の URI を開いて表示

上記に挙げたアプリケーションにように、特定のアプリケーションによっては、.com, .org, .net, .co.jp, .jp, … 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。

2.1.4.4 挙動 A と挙動 B の複合: IPv4/IPv6 アドレスの解決とドメインサフィックス補完

FreeBSD 5.5-RELEASE、 Windows XP SP2、 Windows Vista RC1 (Build 5600)の各端末 OS において、ホスト名

“q.example.jp”

を解決する。このときに、各 OS が補完するドメインサフィックスとして

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

上記の 3 つのサフィックスを設定しているものとする。

このとき "q.example.jp" 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 5.5-RELEASE

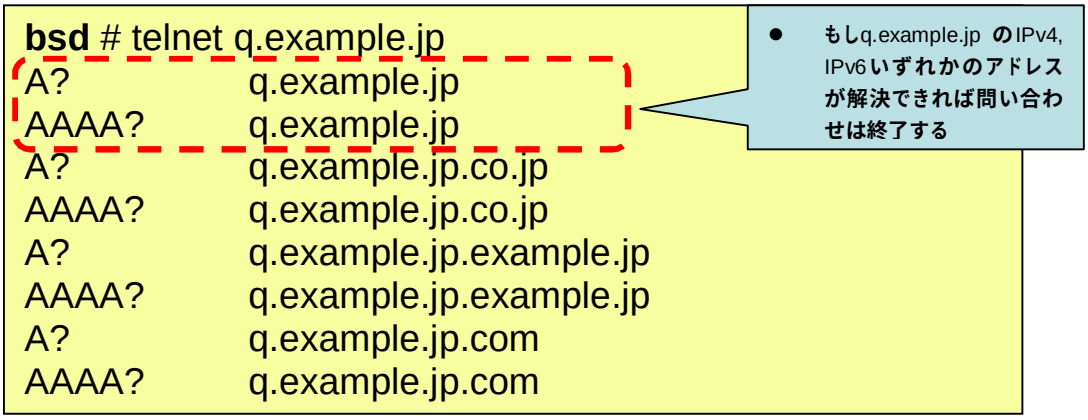


図 3 サブドメイン補完の例（FreeBSD 5.5-RELEASE）

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（IPv4、IPv6）→（IPv4、IPv6）→（IPv4、IPv6）→（IPv4、IPv6）となる。

- Windows XP SP2

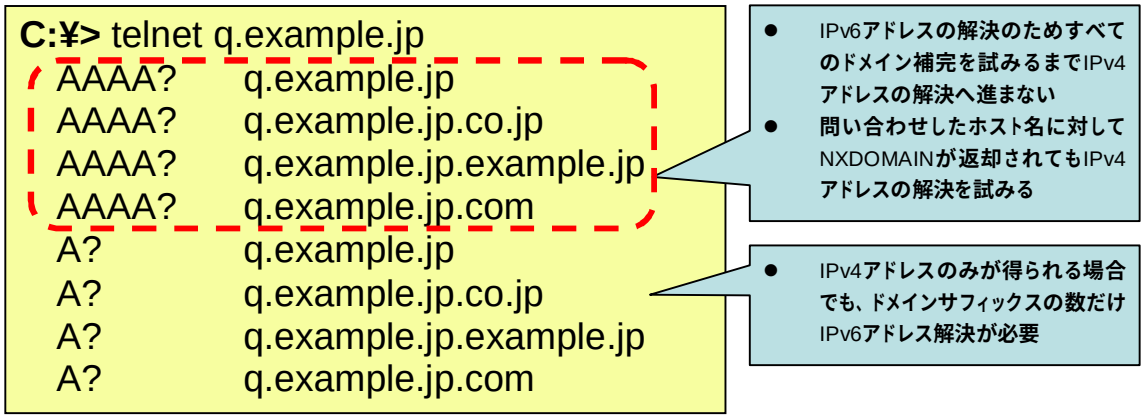


図 4　　サブドメイン補完の例（Windows XP SP2）

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（IPv6、IPv6、IPv6、IPv6）→（IPv4、IPv4、IPv4、IPv4）となる。はじめの 4 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 IPv6 アドレスの解決を行う必要が生じる。本文書を作成する 2006 年 11 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。

さらに、第 2.1.4.1 節で述べたように、IPv6 アドレスの解決の段階で NXDOMAIN が返却されても IPv4 アドレスの解決を試みる。NXDOMAIN の応答が正しいものであれば、A レコードは存在せず IPv4 アドレスの解決は失敗する。

- Windows Vista RC1 (Build 5600)

IPv4 アドレスの解決が優先して行われる。IPv4 アドレスの解決の段階で NXDOMAIN が応答された場合は IPv6 アドレスの解決が抑制される。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。

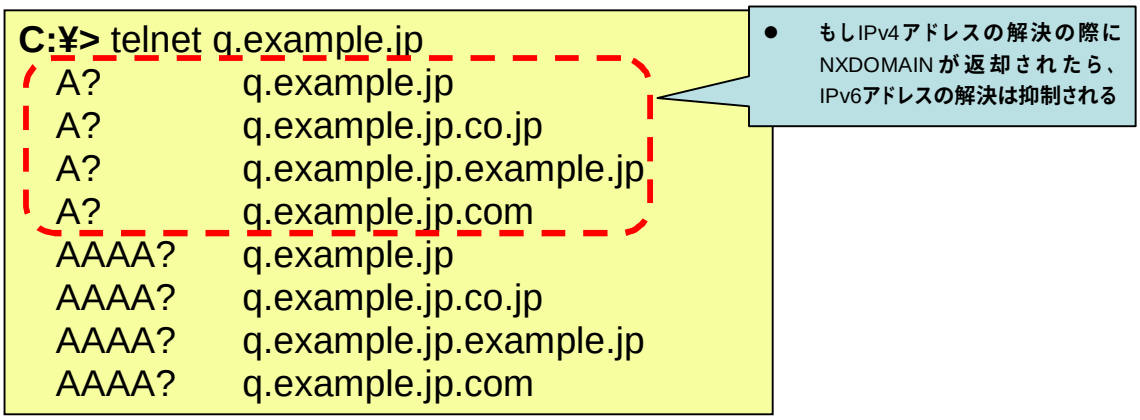


図 5　　サブドメイン補完の例（Windows Vista RC1）

2.1.5 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 アドレス利用時の TCP フォールバック

2.2.1 問題の解説

Microsoft Windows Vista は Microsoft Windows XP と異なり、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。

この状況によって、Microsoft Windows Vista 端末利用時に、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。ユーザネットワーク内のみで利用している IPv6 ネットワークや、閉域 ASP サービスへ接続された IPv6 ネットワークなどが存在する場合、The Internet への接続する際にアクセスが遅いと感じることが起きる。これは IPv6 通信を優先しているために起きるのである。インターネット到達性がないにもかかわらず IPv6 通信で接続を試み、IPv4 通信へフォールバックするまで時間がかかっているために起きる事象である。このような場合には、The Internet への接続では IPv4 通信を優先させることが必要となる。

Microsoft Windows Vista がネットワーク側から終点となるルートが存在しない事(ICMPv6 type1)を通知された場合の動作検証と、起こりえる不具合の回避方法について検証を行った。

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 The Internet への到達性を持たない IPv6 ネットワークが並存した環境での、Microsoft Windows Vista ノードの挙動を確認する。本セクションの調査は、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 6 に示す環境でおこなった。

また、閉域 IPv6 ネットワーク環境の模擬は、図 6 の環境において IPv6 ネットワークのルータから先の The Internet への到達性を失わせるようリンクを切断した（図 7)。この状態で、以下の環境を模擬した。

- 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 ネットワークはグローバル・ルーティング・プレフィックス (global routing prefix) で構成するが、The Internet 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。

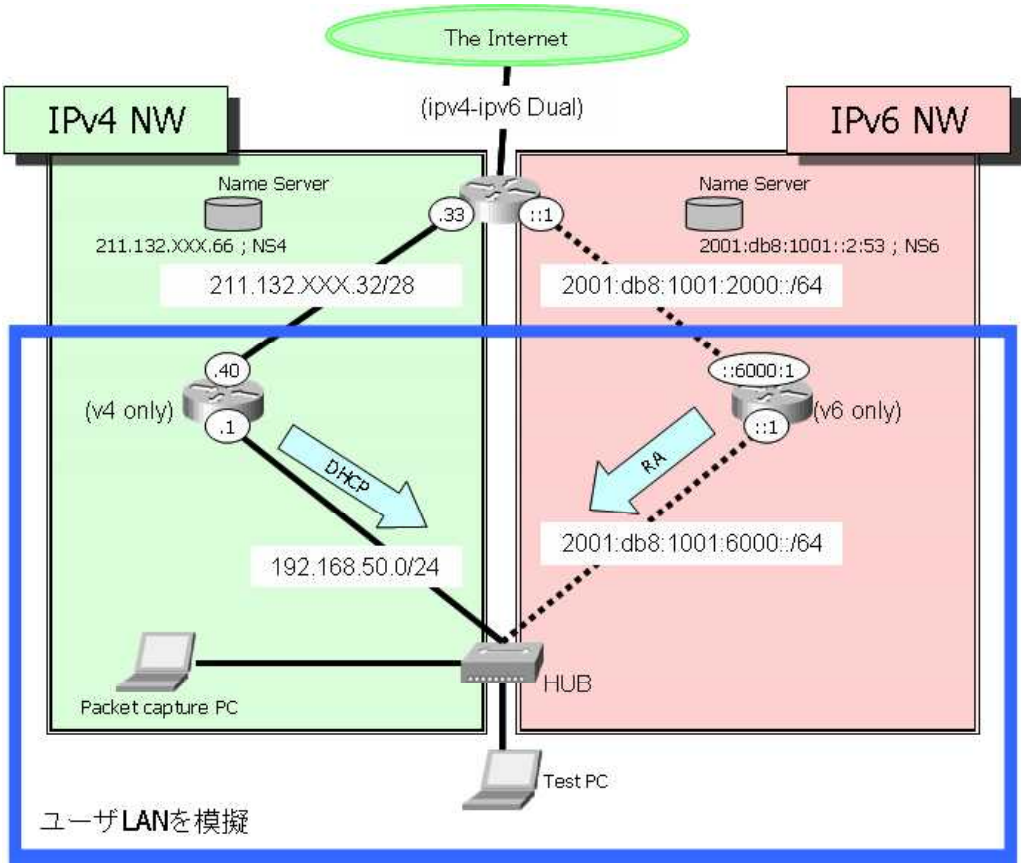


図 6　　ホームユーザネットワーク環境を模擬した検証環境図

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

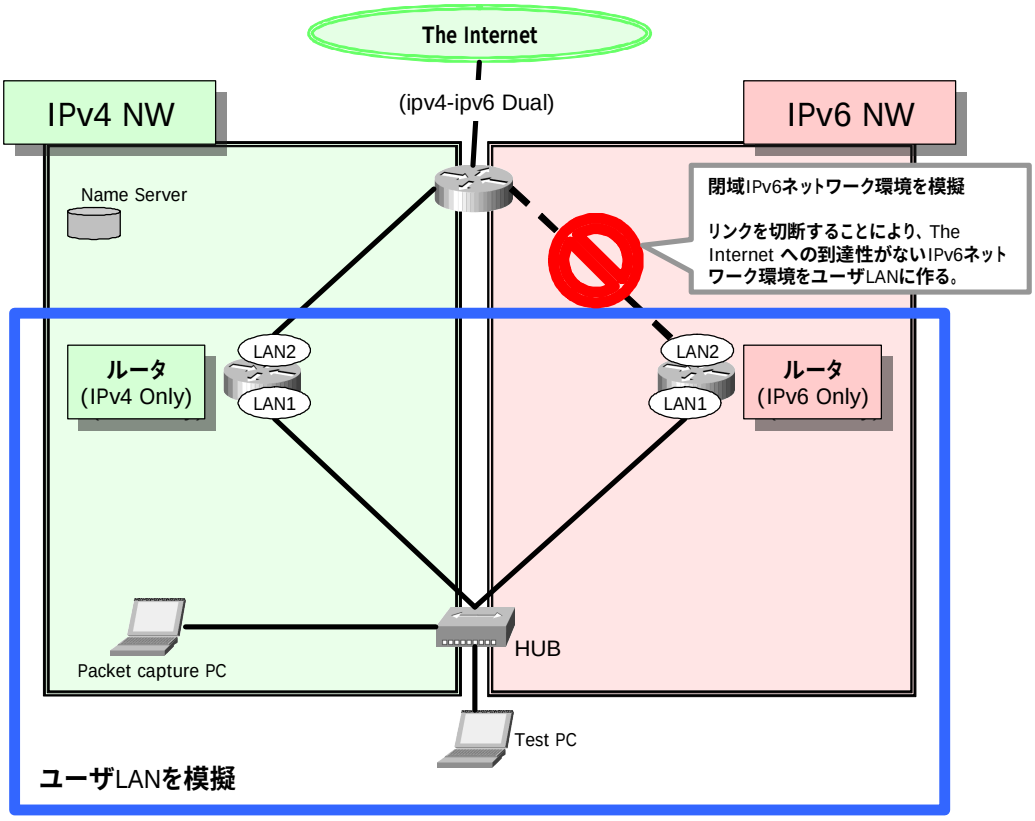


図 7　　ホームネットワークで IPv4 ネットワークに閉域 IPv6 ネットワークが加わった状況

2.2.3 検証手順

Microsoft Windows Vista が IPv4 ネットワークと、インターネットへの接続性を持たない IPv6 ネットワーク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、下記の 3 項目の検証を行う。

1. Windows Firewall （「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. Microsoft Windows Vista が ICMPv6 type1 を受信した場合のフォールバック挙動確認
3. Microsoft Windows Vista が ICMPv6 type1 を受信しない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。

- Microsoft Windows Vista の Windows Firewall はインストール後のデフォルト状態で実施。 フィルタのルールを新たに作成することをせずに、Windows Firewall がデフォルト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」の設定画面には、コントロールパネル→システムとメンテナンス→管理ツールと辿っていくことでアクセスできる。
- ICMPv6 type1 の送信の有無はユーザ LAN 内の IPv6 ルータで制御。
- ICMPv6 type1 はコード 0 (route unreachable)を送信。これはユーザ 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。

- 検証項目①

1. IPv6 対応 OS 端末をユーザ LAN 内に接続。
2. Microsoft Windows Vista の初期状態での Windows Firewall 設定の確認。

- 検証項目②

1. ユーザ LAN 内の IPv6 ルータが ICMPv6 type1 を送信するように設定する。
   (当該ルータのデフォルトゲートウェイを削除)
2. IPv6 対応 OS 端末から、AAAA RR と A RR を持つ WWW サーバへ接続する。
3. IPv6 対応 OS 端末と WWW サーバ間の通信をパケット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 ICMPv6 type1 を送信しないように設定する。
   (当該ルータに ICMPv6 送信 OFF 設定投入)
2. IPv6 対応 OS 端末から、AAAA RR と A RR を持つ 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。

2.2.4 検証結果

- 検証項目①

Microsoft Windows Vista の Windows Firewall は初期状態で ICMPv6 type1 は許可されている。

- **検証項目②**

Microsoft Windows Vista は WWW サーバへの接続要求が発生すると、DNS リゾルバに対して A RR のクエリ（query）を送信する。A RR の回答を得た後、AAAA RR クエリを送信する。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 の接続要求を開始する。

TCP の接続要求後すぐに、ユーザ LAN 内の IPv6 ルータから ICMPv6 type1 を受信する。1 度目の TCP 接続要求の 3 秒後に 2 度目の TCP 接続要求を AAAA RR 宛てに送信する。２度目のＴＣＰ接続要求後も、１度目の TCP 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 ICMPv6 type1 を受信する。2 度目の TCP 接続要求の 6 秒後に、3 度目の TCP 接続要求を AAAA RR 宛てに送信する。３度目の TCP 接続要求送信後、すぐに LAN 内の IPv6 ルータから ICMPv6 type1 を受信する。３度目の TCP 接続要求の 12 秒後に、IPv6 での TCP 接続をあきらめて、A RR に対して TCP 接続要求を送信する。このようにＴＣＰ接続において、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る。

つまり、Microsoft Windows Vista での TCP フォールバック時間の内訳は以下の通り。

TCP フォールバック時間 = 21 秒 = 3 秒（２回目までの再送待ち時間） + 6 秒（３回目までの再送待ち時間） + 12 秒（IPv4 フォールバック接続までの待ち時間）

- **検証項目③**

Microsoft Windows Vista は WWW サーバへの接続要求が発生すると、DNS リゾルバに対して A RR のクエリ（query）を送信する。A RR の回答を得た後、AAAA RR クエリを送信する。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 の接続要求を開始する。1 度目の TCP 接続要求を試み、失敗するとその 3 秒後に 2 度目の TCP 接続要求を AAAA RR 宛てに送信する。2 度目の TCP 接続要求に失敗すると、6 秒後に 3 度目の TCP 接続要求を AAAA RR 宛てに送信する。３度目の TCP 接続要求にも失敗すると、その失敗から 12 秒後に A RR に対して TCP 接続要求を送信する。このようにＴＣＰ接続において、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る。

TCP フォールバック時間 = 21 秒 = 3 秒（２回目までの再送待ち時間） + 6 秒（３回目までの再送待ち時間） + 12 秒（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 IPv6 対応 OS 端末を接続したときの環境は以下の通り。

```
---------------------------------------------------------------------
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. . . . . . . . . . . . . . : Intel(R) PRO/1000 MT Mobile Connection
   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 9 月 12 日 13:56:32
   リースの有効期限. . . . . . . . . : 2006 年 9 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
---------------------------------------------------------------------
```

Microsoft Windows Vista の Windows Firewall の ICMPv6 type1 に関する初期設定を図 8 に示す。

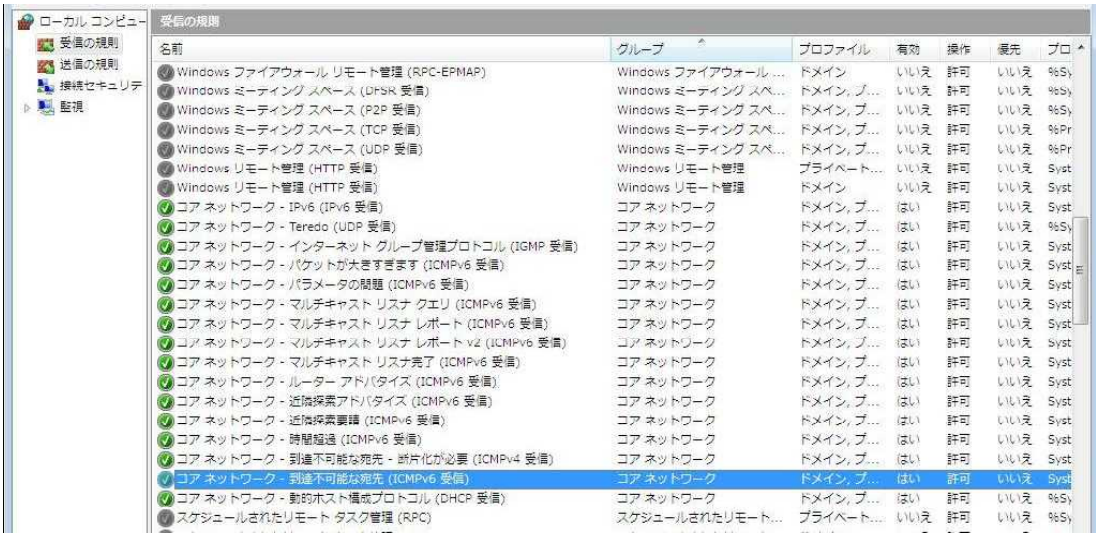


図 8　　Windows Firewall の初期設定

- **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

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 9 に、TCP シーケンス図を図 10 にそれぞれ示す。

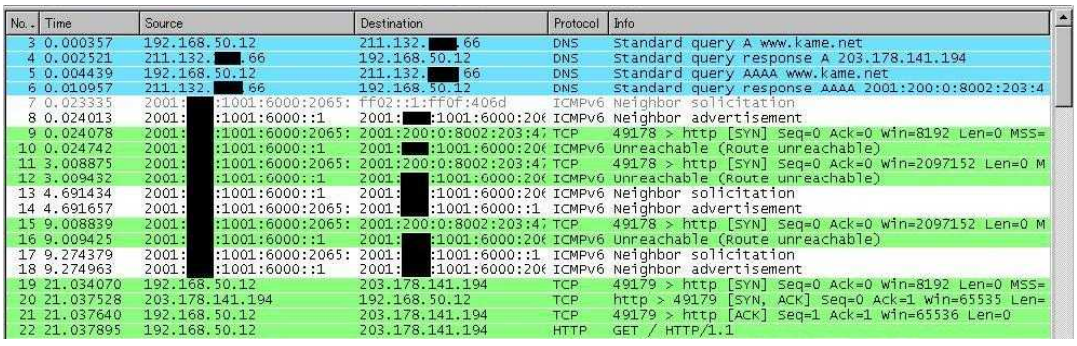


図 9　　ICMPv6 type1 受信時のパケットキャプチャ結果

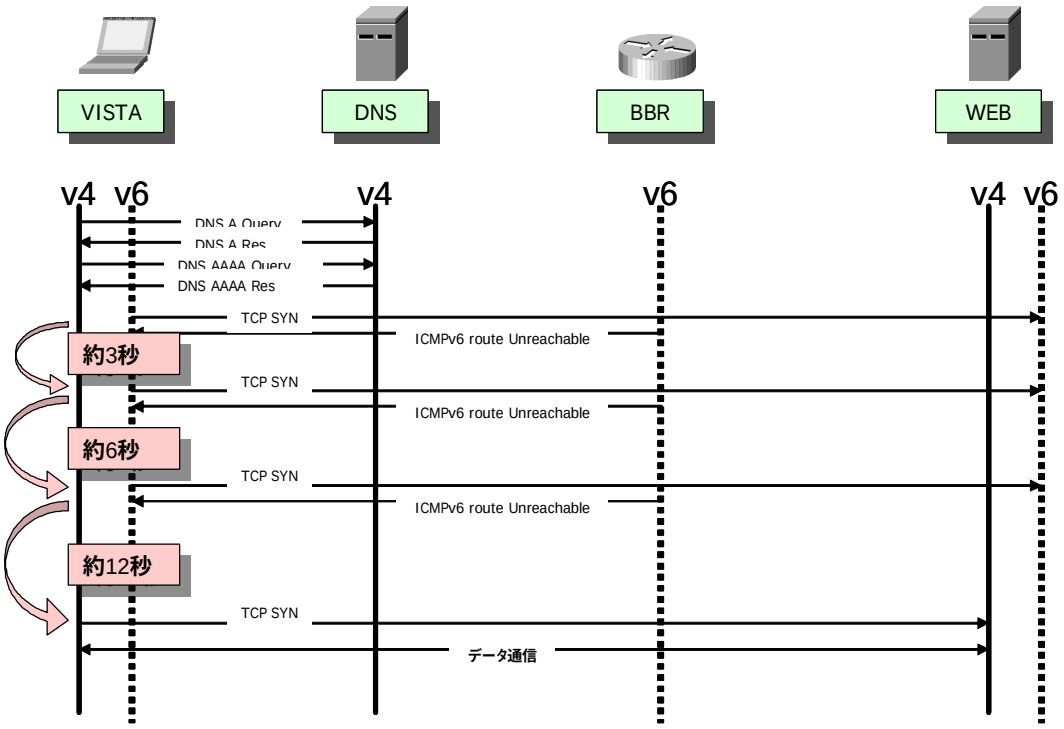


図 10　ICMPv6 type1 受信時のシーケンス図

- **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
ipv6 icmp unreachable send off
----------------------------------------------------------------------
```

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 11 に、TCP シーケンス図を図 12 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 2001:200:0:800
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 Len
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 Len
15	20.997771	203.178.141.194	192.168.50.12	TCP	http > 49222 [SYN, ACK] Seq=0 Ack=1 Win=655
16	20.997887	192.168.50.12	203.178.141.194	TCP	49222 > http [ACK] Seq=1 Ack=1 Win=65536 Le

図 11　ICMPv6 type1 を受信しない場合のパケットキャプチャデータ

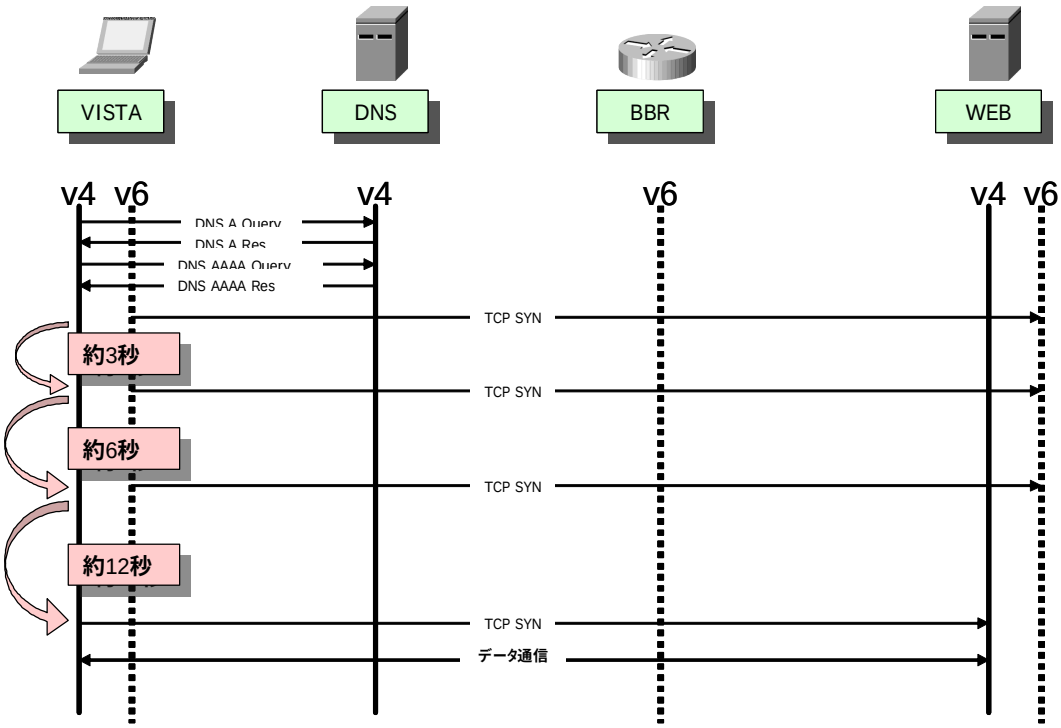


図 12　ICMPv6 type1 を受信しない場合のシーケンス図

2.2.6 追加検証

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 アドレスを設定し運用することが想定される。この場合、閉域 IPv6 ネットワークに接続された IPv6 対応 OS 端末が、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 AAAA RR を 3 つ設定し、IPv6 対応 OS 端末での閲覧を実施した。

2.2.7 検証手順

検証の手順は下記の通りである。

1. Name Server に AAAA RR を 3 つ記述したホストを設定する
2. IPv6 対応 OS 端末から該 WWW サーバに対して接続する
3. IPv6 対応 OS 端末と該 WWW サーバ間の通信をパケットキャプチャし解析する

2.2.8 検証結果

1 つのホスト名に対して複数の AAAA RR を記載していた場合、下記の順番で TCP 接続を行っている。

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

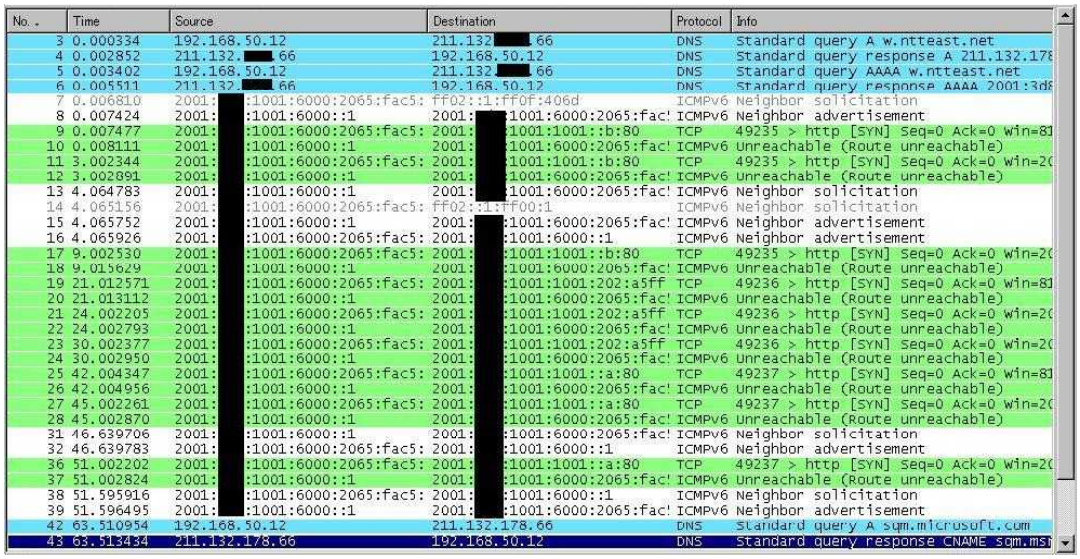
IPv6 対応 OS 端末の中には、IPv4 へのフォールバックを待たずに WEB ブラウザで Timeout が発生してしまい表示することができなくなるものもあった。Windows Vista 上の IE7 が、このケースに該当する。

2.2.9 検証データ

DNS に対して設定した AAAA RR および A RR は以下の通り。

```
-------------------------------------------------------------------------
www             A       211.132.XXX.5
                AAAA    2001:db8:1001:1001:202:a5ff:fe8c:e2ff
                AAAA    2001:db8:1001:1001::a:80
                AAAA    2001:db8:1001:1001::b: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 13 に、TCP シーケンス図を図 14 にそれぞれ示す。



No.	Time	Source	Destination	Protocol	Info
3	0.000334	192.168.50.12	211.132.[redacted].66	DNS	Standard query A w.ntteast.net
4	0.002852	211.132.[redacted].66	192.168.50.12	DNS	Standard query response A 211.132.178
5	0.003402	192.168.50.12	211.132.[redacted].66	DNS	Standard query AAAA w.ntteast.net
6	0.005511	211.132.[redacted].66	192.168.50.12	DNS	Standard query response AAAA 2001:3d8
7	0.006810	2001:[redacted]:1001:6000:2065:fac5:	ff02::1:ff0f:406d	ICMPv6	Neighbor solicitation
8	0.007424	2001:[redacted]:1001:6000::1	2001:[redacted]:1001:6000:2065:fac	ICMPv6	Neighbor advertisement
9	0.007477	2001:[redacted]:1001:6000:2065:fac5:	2001:[redacted]:1001:1001::b:80	TCP	49235 > http [SYN] Seq=0 Ack=0 Win=81
10	0.008111	2001:[redacted]:1001:6000::1	2001:[redacted]:1001:6000:2065:fac	ICMPv6	Unreachable (Route unreachable)
11	3.002344	2001:[redacted]:1001:6000:2065:fac5:	2001:[redacted]:1001:1001::b:80	TCP	49235 > http [SYN] Seq=0 Ack=0 Win=20
12	3.002891	2001:[redacted]:1001:6000::1	2001:[redacted]:1001:6000:2065:fac	ICMPv6	Unreachable (Route unreachable)
13	4.064783	2001:[redacted]:1001:6000::1	2001:[redacted]:1001:6000:2065:fac	ICMPv6	Neighbor solicitation
14	4.065156	2001:[redacted]:1001:6000:2065:fac5:	ff02::1:ff00:1	ICMPv6	Neighbor solicitation
15	4.065752	2001:[redacted]:1001:6000::1	2001:[redacted]:1001:6000:2065:fac	ICMPv6	Neighbor advertisement
16	4.065926	2001:[redacted]:1001:6000:2065:fac5:	2001:[redacted]:1001:6000::1	ICMPv6	Neighbor advertisement
17	9.002530	2001:[redacted]:1001:6000:2065:fac5:	2001:[redacted]:1001:1001::b:80	TCP	49235 > http [SYN] Seq=0 Ack=0 Win=20
18	9.015629	2001:[redacted]:1001:6000::1	2001:[redacted]:1001:6000:2065:fac	ICMPv6	Unreachable (Route unreachable)
19	21.012571	2001:[redacted]:1001:6000:2065:fac5:	2001:[redacted]:1001:1001:202:a5ff	TCP	49236 > http [SYN] Seq=0 Ack=0 Win=81
20	21.013112	2001:[redacted]:1001:6000::1	2001:[redacted]:1001:6000:2065:fac	ICMPv6	Unreachable (Route unreachable)
21	24.002205	2001:[redacted]:1001:6000:2065:fac5:	2001:[redacted]:1001:1001:202:a5ff	TCP	49236 > http [SYN] Seq=0 Ack=0 Win=20
22	24.002793	2001:[redacted]:1001:6000::1	2001:[redacted]:1001:6000:2065:fac	ICMPv6	Unreachable (Route unreachable)
23	30.002377	2001:[redacted]:1001:6000:2065:fac5:	2001:[redacted]:1001:1001:202:a5ff	TCP	49236 > http [SYN] Seq=0 Ack=0 Win=20
24	30.002950	2001:[redacted]:1001:6000::1	2001:[redacted]:1001:6000:2065:fac	ICMPv6	Unreachable (Route unreachable)
25	42.004347	2001:[redacted]:1001:6000:2065:fac5:	2001:[redacted]:1001:1001::a:80	TCP	49237 > http [SYN] Seq=0 Ack=0 Win=81
26	42.004956	2001:[redacted]:1001:6000::1	2001:[redacted]:1001:6000:2065:fac	ICMPv6	Unreachable (Route unreachable)
27	45.002261	2001:[redacted]:1001:6000:2065:fac5:	2001:[redacted]:1001:1001::a:80	TCP	49237 > http [SYN] Seq=0 Ack=0 Win=20
28	45.002870	2001:[redacted]:1001:6000::1	2001:[redacted]:1001:6000:2065:fac	ICMPv6	Unreachable (Route unreachable)
31	46.639706	2001:[redacted]:1001:6000::1	2001:[redacted]:1001:6000:2065:fac	ICMPv6	Neighbor solicitation
32	46.639783	2001:[redacted]:1001:6000:2065:fac5:	2001:[redacted]:1001:6000::1	ICMPv6	Neighbor advertisement
36	51.002202	2001:[redacted]:1001:6000:2065:fac5:	2001:[redacted]:1001:1001::a:80	TCP	49237 > http [SYN] Seq=0 Ack=0 Win=20
37	51.002824	2001:[redacted]:1001:6000::1	2001:[redacted]:1001:6000:2065:fac	ICMPv6	Unreachable (Route unreachable)
38	51.595916	2001:[redacted]:1001:6000:2065:fac5:	2001:[redacted]:1001:6000::1	ICMPv6	Neighbor solicitation
39	51.596495	2001:[redacted]:1001:6000::1	2001:[redacted]:1001:6000:2065:fac	ICMPv6	Neighbor advertisement
42	63.510954	192.168.50.12	211.132.178.66	DNS	Standard query A sqm.microsoft.com
43	63.513434	211.132.178.66	192.168.50.12	DNS	Standard query response CNAME sqm.msf

図 13　AAAA RR が 3 つ設定された場合のパケットキャプチャデータ

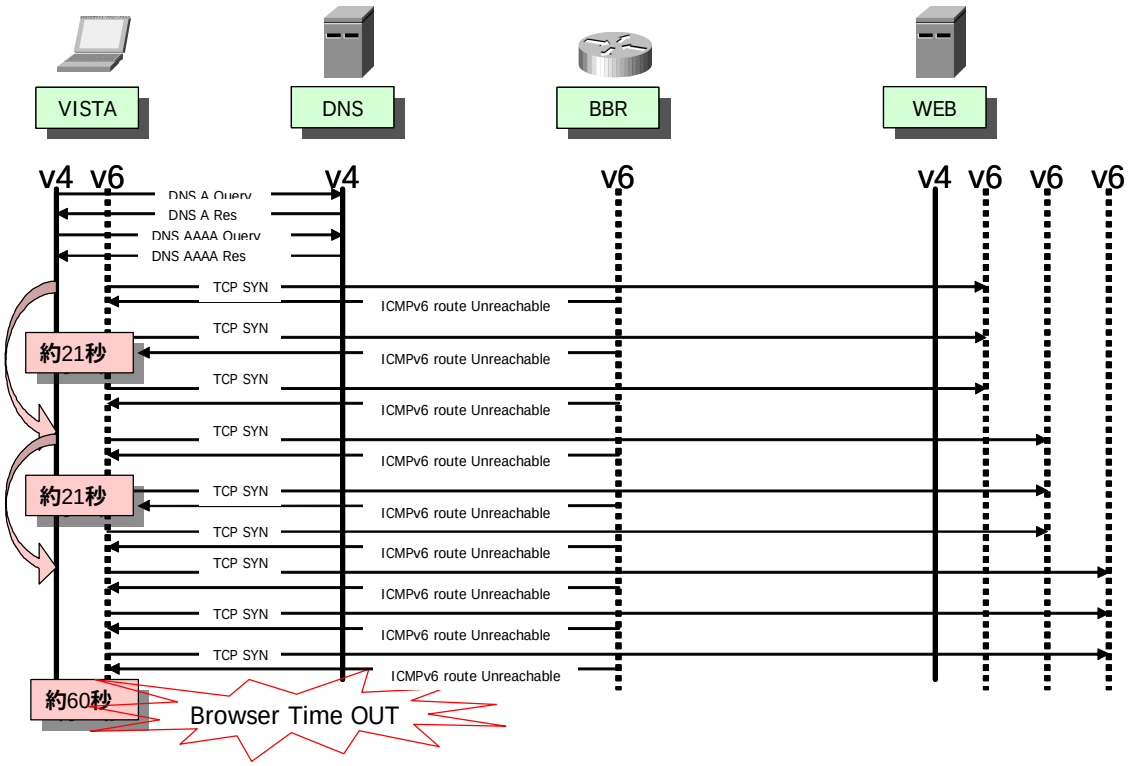


図 14　AAAA RR が 3 つ記載された場合のシーケンス図

2.2.10 検証まとめ

検証項目①の結果より Microsoft Windows Vista の Windows Firewall には ICMPv6 type1 に関するフィルタ制限は行われていないため、ICMPv6 type1 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、Microsoft Windows Vista では ICMPv6 type1 を受けることによる挙動の違いは見られなかった。TCP 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 再送回数は２回おこなわれ、初回を含めると合計３回の IPv6 通信を試行していた。１回目の IPv6 通信失敗後、２回目の IPv6 通信開始までの時間間隔が３秒。２回目の IPv6 通信失敗後、３回目の IPv6 通信開始までの時間間隔が 6 秒。３回目の IPv6 通信失敗の後に、IPv6 通信をあきらめて 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 12 秒である。

２１秒 ＝ ３秒 ＋ ６秒 ＋ １２秒

なお、いったん IPv4 通信へのフォールバックが起きると、それ以降のアクセスではローカルに 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。

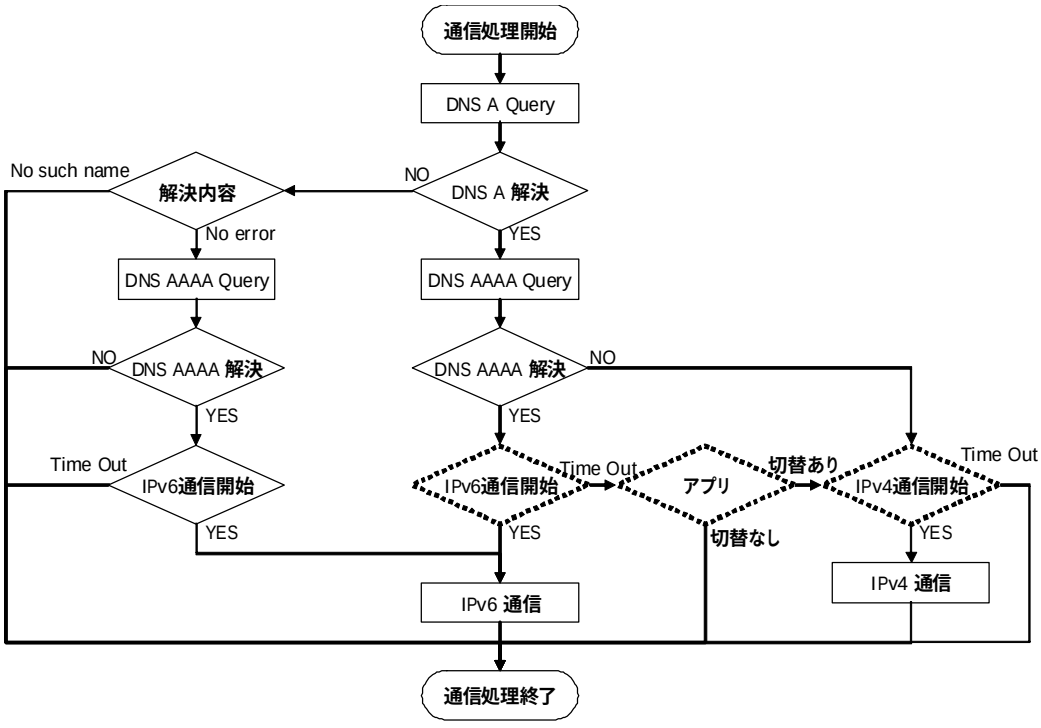


図 15 Microsoft Windows Vista における IPv6 通信フローチャート図

図 15 に本検証で利用した Microsoft 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。図 15 における破線部分での待ち時間により利用するユーザにて不快感が出る可能性がある。
この問題の解決方法について、下記に 2 つ挙げる。

- 対策例 1

検討ベースであるが、RFC3484 の Policy Table を採用するのが妥当ではないかと思われる。Policy Table において、閉域 IPv6 アドレスの prefix の優先度を高く設定しておき、次点で IPv4 mapped address(::ffff:0:0/96)を設定する。IPv6 default gateway をそのあとに設定することで、この様な問題を回避できると考えられる。

- 対策例 2

IPv6 対応 OS 端末側が起動時の RS/RA で生成された情報の削除と、閉域 IPv6 ネットワーク Prefix のルーティングテーブル追加を実施することでも問題の回避が可能である。

IPv6 デフォルトゲートウェイの削除
>netsh interface ipv6 delete route ::/0 [interface] [nexthop]
閉域 IPv6 ネットワーク Prefix の追加
>netsh interface ipv6 add route [prefix] [interface] [nexthop]

ただし、IPv6 ルータから定期的に RA 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。起動後に受信する RA は、Windows Firewall 機能を利用してドロップ可能である（5.1 節参照）。

2.2.11 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における問題

3.1.1 問題の解説

キャプティブポータルとは、無線 LAN サービス、ホテルなどで採用しているインターネット接続時の認証、課金システムで、ブラウザで任意のウェブページにアクセスすると、強制的にサービス提供者のページにリダイレクトされ、そこで認証や課金処理が行われる。その処理の後に、ユーザは自由にウェブページにアクセスできるようになる。これらの接続サービスはほとんどの場合 IPv4 サービスに限定されており、IPv6 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、一部の環境ではウェブ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提供者が利用している DNS 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。

参考： http://v6fix.net/docs/hotel.html.ja

3.1.2 問題の検証と検討

3.1.2.1 検証内容・手順

キャプティブポータル問題の原因の１つである端末側の問題「DNS に問い合わせたリソースレコードの種類（AAAA）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、端末の DNS リゾルバが受理する」がデフォルト設定の Windows Vista において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. 一般的に IPv4 サービスに限定される（端末に IPv6 アドレスが付与されない）キャプティブポータルサービスに接続した Windows Vista が AAAA 問合せを行うかどうか。
2. AAAA 問合せに対する A 応答を Windows Vista が受理するかどうか。

各項目の検証手順は以下の通りである。

- 検証項目①

1. IPv4 回線に Windows Vista を接続する。
2. IPv6 アドレスが付与されていないことを確認する。
3. Windows Vista の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。
4. IE7 ブラウザで、どこかのウェブページを表示する。
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 問合せ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 レコードを返す DNS を立てる（Perl module の Net::DNS::Server を使用）。
2. Windows Vista の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。
3. IPv4/IPv6 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 ブラウザで、どこかのウェブページを表示する。
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。

3.1.2.2 検証結果と検討

- 検証項目①

Windows Vista は ISP などから提供される IPv6 アドレスが付与されていない時(Teredo アドレスを除く）は AAAA 問合せを行わない。しかし、Windows XP SP2 は IPv6 アドレスが付与されていなくても AAAA 問合せを行うことを確認している。

- 検証項目②

Windows Vista の DNS リゾルバでは、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。しかし、Windows XP SP2 ではこれを受理してしまい、キャプティブポータル問題に陥る可能性がある。

各 OS を用いたケースでの検証結果データは以下の通り。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 問合せ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。なお、検証用に用いた Windows Vista のビルドは RC2 Build5744 Japanese である。

- Windows Vista

```
-----------------------------------------------------------------------
No. Source        Destination Protocol Info
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 61.208.134.143
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, 61.208.134.143, TCP 50652 > http [SYN] Seq=0 Len=0 MSS=1460 WS=8
6 61.208.134.143, 192.168.1.1, TCP http > 50652 [SYN, ACK] Seq=0 Ack=1 Win=1460 Len=0 MSS=1412
-----------------------------------------------------------------------
```

AAAA クエリに対する A 応答を無視

- Windows XP SP2

---

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

3.1.3 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 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 問合せを行わないため、「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。**このため一般的に IPv4 サービスに限定されるキャプティブポータルサービス下では、ユーザは Windows Vista を利用してキャプティブポータルサービス(IPv4)に問題なく接続できると言える。**なお、Teredo アドレスが付与されているのに AAAA 問合せを行わないのは Windows Vista の仕様と思われる。

仮に IPv6 サービスも利用できるキャプティブポータルサービスが存在して Windows Vista のリゾルバが AAAA 問合せを行い、かつキャプティブポータルサービスが提供している DNS サーバが、AAAA リソースレコードが存在しない時に A 応答を返す実装になっている時も、検証項目②の結果から **Windows Vista ではこの応答を受理しないため問題が生じることは無い。**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も Windows Vista のリゾルバは AAAA 問合せを行うが、同様に問題が生じることは無い。

3.2 Proxy サーバへの HTTP クエリの IPv6 対応状況

3.2.1 問題の解説

IPv6、IPv4 の両者に対応する Proxy が提供されつつある。Windows Vista に搭載された Web ブラウザが、このようなデュアルスタック Proxy サーバへの HTTP クエリに IPv6 を用いるのかが判然としない。

3.2.2 問題の検証と検討

3.2.2.1 検証内容・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 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 HP 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。

3.2.2.2 検証結果と検討

Windows Vista と IE7 の組み合わせでは Proxy サーバへの HTTP クエリに IPv6 を用いる。Windows XP SP2 も同様であった。なお、IE7 の Proxy 設定欄には[]で IPv6 アドレスを括って指定した。

3.2.3 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 端末実装上の課題と検討結果

本章では、IPv6 端末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 自動トンネル機能による意図しない IPv6 経路の問題

4.1.1 問題の解説

IPv6 対応 OS 端末においては、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。IPv6 対応 OS 端末によっては、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。

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リレールータ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 対応 OS 端末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 Windows Vista（RC2 Build5744 Japanese）では IPv4 接続のみが提供されている回線でグローバルの IPv4 アドレスが付与された時には既定の設定で 6to4 自動トンネルが張られる。また、プライベートの IPv4 アドレスが付与された Windows Vista には既定の設定で Teredo 自動トンネルが張られる（IPv6 アドレスを指定した通信の開始時にトンネル確立を行う）。このため、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

```
netsh interface ipv6 6to4 set state disable        （6to4 サービスの停止）
netsh interface teredo set state disable           （Teredo サービスの停止）
```

をコマンドプロンプトで実施してもらう等の対処を啓蒙・実施する必要がある。

4.1.2 自動トンネル機能の解説

本節で対象とする自動トンネル機能の各プロトコルは、RA による IPv6 アドレスが付与される環境下では自動的に設定されることはない。以下に各機能に関して簡単にまとめる。

- 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フェースには 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。

- Teredo（RFC4380）

Teredo は、NAT の内側から 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フェースには、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。

4.1.3 検証手順

- 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 Vista を接続。
   （実験では 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(6to4 Tunneling Pseudo-Interface)"に IPv6 アドレスが付与されているかどうかを確認

- 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 Vista を接続。
2. ipconfig /all で "Tunnel adapter(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

4.1.4 検証結果

IPv4 だけのネットワーク環境でグローバルの IPv4 アドレスが付与された Vista には、デフォルトの設定で 6to4 自動トンネルが張られる。プライベートの IPv4 アドレスが付与された Vista には、デフォルトの設定で Teredo 自動トンネルが張られる。

ただし、前述したように、RA により IPv6 アドレスが設定される環境下では 6to4 および Teredo の両自動トンネルが機能することはない。

4.2 初期状態でのファイアウォール設定

4.2.1 この確認項目の解説

Windows Vista では、セキュリティが強化されたと言われている。そのため、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がある。そこで、Windows ファイアウォールのデフォルト設定における、パケットフィルタ規則を確認した。

4.2.2 この確認項目の検証と検討

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：デフォルトで遮断、規則に一致したパケットを許可
- 送信：デフォルトで許可、規則に一致したパケットを遮断

となっている。

デフォルトで許可する ICMPv6 パケットの受信規則一覧を表 1 に、デフォルトで許可している TCP および UDP パケットの受信規則の一覧を表 2 にそれぞれ示す。

表 1　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
	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

表 2　TCP/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	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**)
	5355	LLMNR (Linklocal Multicast Name Resolution)	・ **ネットワーク探索** (LLMNR TCP **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**)
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**)
	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 考察

Windows Vista では、受信パケットはデフォルト遮断であるが、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、デフォルトでは、IPv4、IPv6 とも、ping や traceroute には応答しない設定となっている。

4.3　初期状態でオープンしているポート・サービスの認識

4.3.1 この確認項目の解説

セキュリティ上、デフォルトで稼動しているサービスを把握しておく必要がある。また、必要のないサービスは無効にしておく必要がある。

そこで、ネットワークに接続したときに、初期状態でオープンしている TCP および UDP のポート番号を確認した。

4.3.2 この確認項目の検証と検討

Windows Vista において、ネットワーク接続時に、初期状態でオープンしていた TCP および UDP ポート番号の一覧を表 3 示す。

表 3　　初期設定でオープンになっている TCP/UDP ポート番号一覧

プロトコル	ポート番号	XP (IPv4)	Vista (IPv4)	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)
	1900	○	○	○	SSDP
	3702	×	○	○	UPnP v2 Discovery
	4500	○	○	×	IPsec NAT Traversal

	5355	×	○	○	LLMNR (Linklocal Multicast Name Resolution)

4.3.3 考察

検証結果からは、必要最小限のポート番号のみがオープンしていると考えられる。

初期状態でオープンしていたとしても、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い理由から、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 に示す。

表 4　初期設定でオープンかつ外部から接続可能なポート番号一覧

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

4.4　IPsec 対応とマルチキャストアドレス取り扱いに関する問題

4.4.1 この確認項目の解説

IPv6 で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、OS の IPsec 通信機能が有効化された場合、マルチキャスト通信はどのように扱われるのか確認した。

4.4.2 この確認項目の検証と検討

IPsec 設定ツール([管理ツール]→[ローカルセキュリティポリシ])によって、全てのホストとの通信に IPsec が使われるものとして設定した。
この状況で下記の通信を行った。

- ND/NA を使った通信
- well-known なマルチキャストアドレスを通信相手とした場合

いずれの場合も、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。
IPv6 マルチキャストを行う際には、コネクションの一種である SA を構築するのが難しいため、この様な実装となっていると思われる。
つまり IPsec の設定を行う上で、ICMPv6 やその他のマルチキャスト通信に SA を使用しないように、IPsec 設定をする必要はない。全ての IP 機器との通信を IPsec 化するとしても、SA の必要のない ND などのプロトコルでは IPsec 化されず、問題が発生しないことになる。

5 IPv6 の仕様に関する問題とその検討

本章では、IPv6 の使用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 問題の解説

Microsoft 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 を受信することで不具合が発生する可能性が考えられる。そこで、Microsoft Windows Vista において RA 受信することによる動作検証と、意図しない RA については受け入れないようにすることができるかを検証した。

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 はユーザ LAN 内に設置している IPv6 ルータから受信する。図 16 に示す環境で動作検証を行った。

RA の lifetime は実験で使用した YAMAHA RT105e のデフォルト値としている。

- 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

Microsoft Windows Vista が IPv6 ルータから RA を受信した場合の挙動の確認と、RA 受信に関する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. Microsoft Windows Vista のネットワークインターフェースにどのような Prefix が付与されているかを確認
2. Windows Firewall による RA フィルタリングに関する動作確認

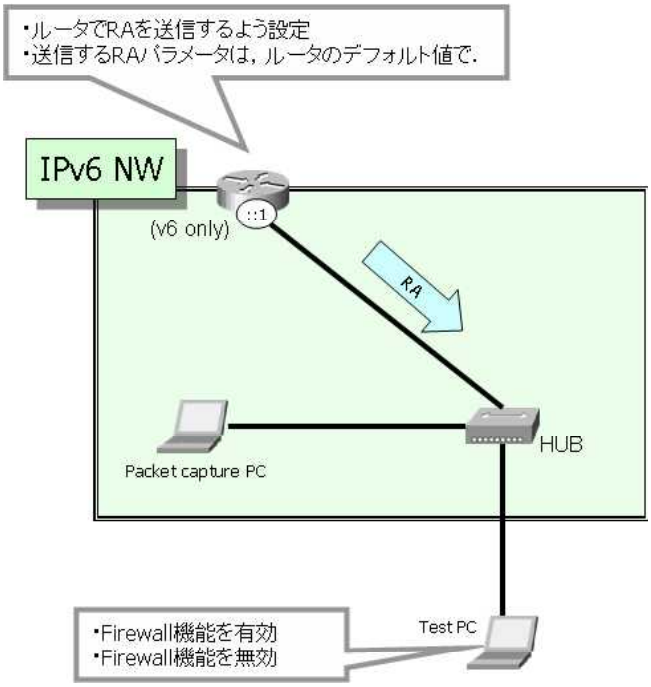


図 16　IPv6 ネットワーク環境例

- **検証項目①**

1. Microsoft Windows Vista　を IPv6 ネットワーク接続
2. IPv6 ルータからの RA 受信後、各ネットワークインターフェースのステータスを確認する

- **検証項目②**

1. Windows Firewall にて RA をドロップする設定に変更
2. Microsoft Windows Vista の再起動を実施し、IPv6 ルータとの通信をパケットキャプチャし解析
3. IPv6 ルータから定期的に送信される RA 情報をパケットキャプチャし解析
4. IPv6 ルータから定期的に送信された RA 受信後の Microsoft Windows Vista のステータスを確認する

5.1.4 検証結果

- **検証項目①**

Microsoft Windows Vista では、IPv6 ルータからの RA を受信することにより IP アドレスが自動生成される。「netsh interface ipv6 show address」を実行することで、自動生成（Public、Temporary）されたものか、あるいは手動設定(Manual)されているものかを確認することが可能である。ネットワークインターフェースに手動で IPv6 アドレスを設定しても RA を受信すると、IPv6 アドレスを自動生成する。

Microsoft Windows Vista でネットワークインターフェースがどのような Prefix を受信しているかを確認するためには、「netsh interface ipv6 show siteprefixes」を実行する。RA を受信している場合は、プレフィックス部分に受信 Prefix と、有効期間として（vaild_lifetime）×2 秒が設定される。また、RA を受信しているネットワークインターフェース名も確認することが可能。

Microsoft Windows XP の場合も Microsoft 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 での表示となる。/49～/64 部分については切り捨てられる。有効期間は Vaild_lifetime の値がそのまま設定される。

- **検証項目②**

Microsoft Windows Vista の Windows Firewall で RA 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 を受信する。起動後は Windows Firewall のルールが適用され、IPv6 ルータから定期的に送信される RA についてはドロップする。

起動時に受信した RA の（valid_lifetime × 2）秒の時間経過後、Prefix 有効時間が切れ、ネットワークインターフェースについていたグローバルユニキャスト IPv6 アドレスは消失する。

Microsoft Windows Vista に実装されている「ipconfig /renew6」を実行することで RS を送信する。この際に送信した RS の応答 RA は Windows Firewall を通過し、グローバルユニキャスト IPv6 アドレスを自動生成する。（Windows Firewall がデフォルトで持っているルールによる制御の場合）

5.1.5 検証データ

- **検証項目①**

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 route default gateway 2001:db8:1001:2000::1%2
ipv6 prefix 1 2001:db8:1001:6000::/64
-------------------------------------------------------------------------
```

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

```
-------------------------------------------------------------------------
インターフェース 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:db8:1001:6000::1111
Temporary       設定      6d22h1m20s  6d22h1m20s  2001:db8:1001:6000:3d06:b0c4:9b84:974a
Public          設定      29d23h59m54s 6d23h59m54s 2001:db8:1001:6000:894f:f69f:2813:7b16
その他          設定      infinite    infinite    fe80::894f:f69f:2813:7b16%12
-------------------------------------------------------------------------
```

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

```
-------------------------------------------------------------------------
プレフィックス          有効期間      インターフェース
----------------------------------  ----------------------  ---------------------------
2001:3d8:1001:6000::/64 59d23h59m44s  ローカル エリア接続
2001:0:4136:e37c::/64   infinite      ローカル エリア接続* 2
-------------------------------------------------------------------------
```

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

```
---------------------------------------------------------------------------
Prefix                  Lifetime          Interface
------------------------ ---------------- ---------------------------------
2001:db8:1001::/48      29d23h57m23s      onboard1
---------------------------------------------------------------------------
```

- **検証項目②**

Windows Firewall に RA 受信をドロップするルールを適用した様子を図 17 と図 18 にそれぞれ示す。

図 17　フィルタルール変更画面

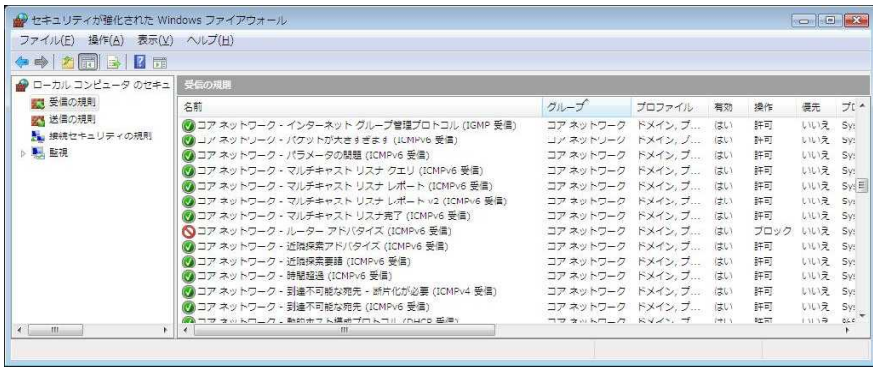


図 18　RA フィルタリングルール変更完了

5.1.6 検証まとめ

検証①より、Microsoft Windows Vista にて RA を受信した場合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。ネットワークインターフェースに対して IPv6 アドレスを手動で設定した場合であっても、RA を受信した場合は IPv6 アドレスの自動生成が行われる。

検証②より、Windows Firewall にて RA 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 を受信するため、グローバルユニキャスト IPv6 アドレスを自動生成してネットワークインターフェースに設定する。ルータから定期的に通知される RA については Windows Firewall によりドロップされ受信しないが、ipconfig などによる RS 送信後の RA については受信する。

RA 受信による動作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

Microsoft Windows Vista において受信した RA 情報を無効にしたい場合は、システム起動時に受信してしまう RA によって生成される情報を削除するとともに、以降の RA を受信しない設定と RS を送信しない設定を実施する。

- グローバルユニキャスト IPv6 アドレスの削除
  >netsh interface ipv6 delete address [interface] [ip address]
- デフォルトゲートウェイ情報の削除
  >netsh interface ipv6 delete route [prefix] [interface] [nexthop]
- RA 受信拒否設定の実施(図 19、図 20 参照)
- RS 送信拒否設定の実施

図 19　RS 送信フィルタルール変更画面

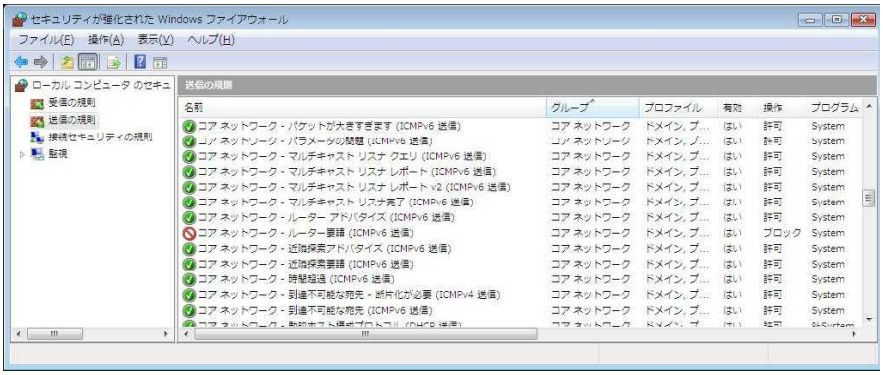


図 20　RS 送信フィルタルール変更完了画面

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 によって生成する IPv6 アドレス情報の削除、および、以降の RA 受信ドロップが可能となる。

5.2 IPv6 の Dynamic DNS について

5.2.1 問題の解説

IPv6 環境では、多くの場合、IPv6 アドレス自動設定が行なわれる。これと DDNS を組み合わせることによって、IPv6 関連のネットワーク設定作業が削減され、IPv6 ホストを利用しやすくなる。このため、IPv6 環境では DDNS に対して期待がある。

ただし、IPv6 対応端末 OS は DDNS 関連の下記の挙動について、検討が必要となる。

- IPv6 DNS server へ更新リクエストに失敗した場合の挙動
  - IPv4 DNS server へ fall back するか
- 複数アドレスをもつ場合の挙動
  - IPv4、IPv6 address をもつ場合、すべて登録するのか
  - 複数の IPv6 address を持つ場合すべて登録するのか
  - 登録する address を制限できるか

5.2.2 問題の検証と検討

検証環境は下記の通りである。

- 対象端末: Windows Vista β2 日本語版(Build 5384)
- DNS サーバ: Fedora Core 4 / bind 9.3.2 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 21 に DDNS Update の検証を行った環境を示す。

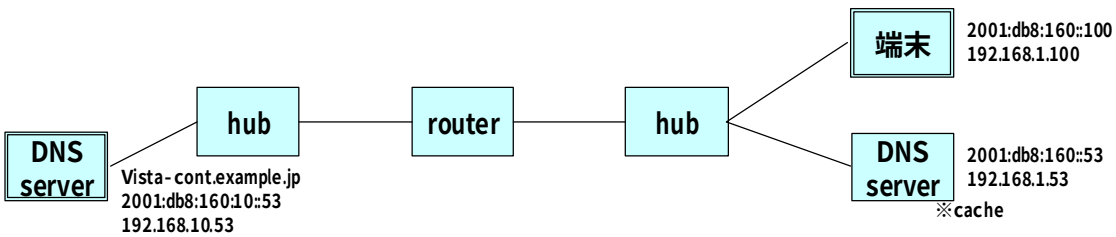


図 21　DDNS Update 検証構成

表 5　DDNS Update 検証結果

		DNS Server 設定								
		IPv6			IPv6/IPv4			IPv4		
到達性		IPv6	IPv6/IPv4	IPv4	IPv6	IPv6/IPv4	IPv4	IPv6	IPv6/IPv4	IPv6
PC のアドレス設定	IPv6	・v6 で更新 ・AAAA	・v6 で更新 ・AAAA	NG	・v6 で更新 ・AAAA	・v6 で更新 ・AAAA	NG	NG	NG	NG
	IPv6/IPv4	・v6 で更新 ・AAAA,A	・v6 で更新 ・AAAA,A	NG	・v6 で更新 ・AAAA,A	・v6 で更新 ・AAAA,A	・ v6 → v4 と fallback して更新 ・AAAA,A	・v4 で更新 ・AAAA,A	・v4 で更新 ・AAAA,A	・v4 で更新 ・AAAA,A
	IPv4	NG	NG	NG	NG	NG	・v4 で更新 ・A	NG	・v4 で更新 ・A	・v4 で更新 ・A

表 5 に示す内容が検証結果である。まとめると、下記の特徴がある。

- IPv6 DNS server へ更新リクエストに失敗した場合には、IPv4 DNS server へ fall back を行う
- IPv4、IPv6 address をもつ場合、IPv6/IPv4 transport いずれであるか、また疎通があるかどうかに関わらずすべての address を登録する。(ただし teredo、6to4、一時 IPv6 address は登録されない)
- IPv6 のみ、IPv4 のみ、あるいは複数の IPv6 address をもつ場合、一部の address 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

5.3 DNS ディスカバリの現状について

5.3.1 問題の解説

IPv6 環境における自身の IP アドレスが自動設定方法はかなり以前に規格化され、現在に至ってほとんどの環境で実装されており、利用されることが多い。しかしながら、この規格策定の時期に比べ、DNS サーバの自動発見の浸透は遅れている。現在 RFC4339 で提案されている自動発見手法は下記の通りである。

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

IPv6 端末 OS でサポートしている、またサポートされうる自動発見手法について、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 Discovery 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。

DHCPv6 については、ManagedFlag 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、OtherConfigFlag 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。

- Managed-Flag が 1 である場合

```
"fe80::20b:5dff:fe75:a2a4", "ff02::1", "ICMPv6", "Router advertisement"
"fe80::20bc:5f6a: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
"fe80::20b:5dff:fe75:a2a4", "fe80::20bc:5f6a:cf26:da6a", "DHCPv6", "Advertise"
"fe80::20bc:5f6a:cf26:da6a", "ff02::1:2", "DHCPv6", "Request"
"fe80::20b:5dff:fe75:a2a4", "fe80::20bc:5f6a:cf26:da6a", "DHCPv6", "Reply"
```

- OtherConfigFlag が 1 である場合

```
"fe80::20b:5dff:fe75:a2a4", "ff02::1", "ICMPv6", "Router advertisement"
"fe80::20bc:5f6a:cf26:da6a", "ff02::1:2", "DHCPv6", "Information-request"
                elapsed-time
                client-identifier
                vendor-class
                domain-search-list
                dns-recursive-name-server
                vendor-specific-information
"fe80::20b:5dff:fe75:a2a4", "fe80::20bc:5f6a:cf26:da6a", "DHCPv6", "Reply"
```

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。

Site Local アドレスは既に利用しないことになった、この機能の利用は一考すべきであり、特に理由がない場合は利用しないことをお勧めする。

5.4　マルチプレフィックス環境下での始点アドレス選択問題

5.4.1 問題の解説

IPv6 では、1 つのインターフェースに対して複数のアドレス利用を前提にして設計されている。特に IPv6 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び、このマルチプレフィクス環境では、通信開始時に始点アドレス選択の問題が発生する場合がある。図 22 に問題が発生する状況図を示し、以下に解説する。

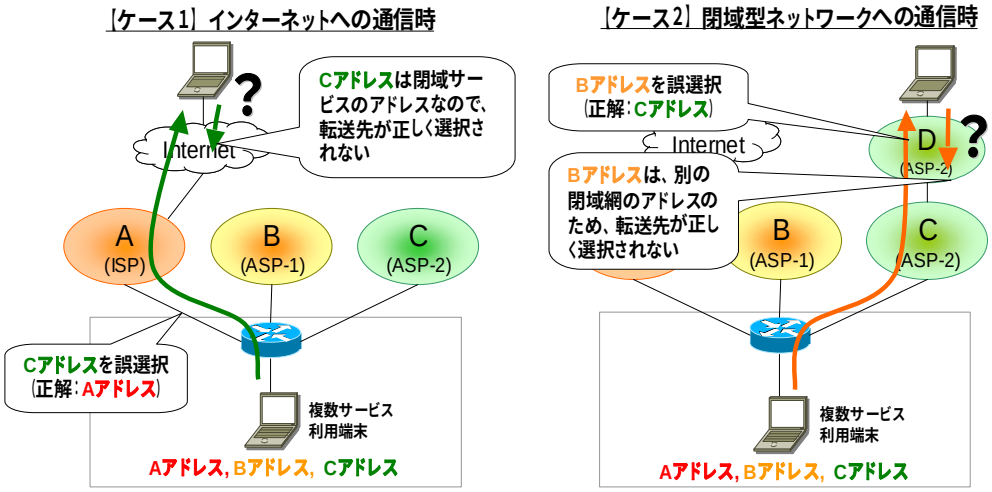


図 22　始点アドレス選択にて問題が発生するケース

ケース 1、ケース 2 はどちらも、ISP や ASP など複数の他ネットワークへの接続を持ち、複数のプレフィクスの割り当てを受けているユーザで発生しうる問題を示している。

特に、この例では、この組織が 1 つの ISP と 2 つの ASP に接続性を持っているとする。この時、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。この ISP が供給するプレフィクスが A だとする。この ISP の他にも、この組織は、ASP-1 や ASP-2 に接続性を持ち、これらの ASP を利用するため、B および C のプレフィクスを受けている。

ケース 1 は、この状況で組織内ホストが、組織外ホストにパケットを送るとき、A、B、C のどの始点アドレスを選ぶべきかの問題を示している。組織内のホストが、組織外に向けたパケットを作成して送信する際、その始点アドレスには A、B、C のいずれかのプレフィ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 のプレフィクスによるアドレスを使ったら、パケットは社外にルーティングされるが、その後社外側のホスト

から応答パケットを送る際に、その C のソースアドレスは社外からルーティング不能であるため、パケットが到達しないという事になり、通信が成立しない。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、同様の環境で、ASP-2 のサービスを利用するとき、ASP-1 の始点アドレス(B)を利用することで、ケース 1 と同じく戻りのパケットが到達しないことを示している。

この様な場合は、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。

5.4.2 現状の実装

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”で規定されており、複数のアドレスを持つ端末はデフォルト状態で、終点アドレスと先頭ビットから最長一致するものを始点アドレスとして選択するものとしている。
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 23 に示す。

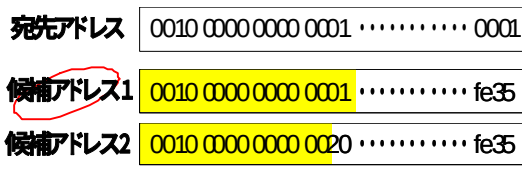


図 23　最長一致による始点アドレスの選択

実際、Windows XP や FreeBSD などでは、この仕様が実装されている。

しかしながら、この仕様から自明だが、終点アドレスに最も近い候補アドレスが、常に始点アドレスとして適しているというわけではない。特に、インターネットへのパケットの場合、終点アドレスは、候補アドレスとは無関係に、多彩な IP アドレスが終点となりうる。このため、この方法では、問題を完全に解決することはできない。

5.4.3 考えられる問題解決法

RFC3484 でも提案されている、終点アドレスブロック - 始点アドレス選択テーブルを実装することで、この問題は解決できる。この機構を採用することで、この問題は解決できる。実際、FreeBSD、Windows XP、Windows Vista（β版）において機能することを確認できた。

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。アドレス選択ポリシーの自動設定機能は、端末および端末直近のルータ全般への機能追加を必要とするため、実利用されるためには技術の標準化が必要となる。IPv6 で標準的なネットワーク自動設定技術（RA や DHCP）を拡張により行う技術が検討されており、今後この技術の動向を見守るべきである。

なお、本節の問題に関する議論は、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 にて詳細に議論されており、結果はガイドラインとして策定される予定である。

5.5　複数のルータ配下におけるデフォルトゲートウェイ選択問題

5.5.1 問題の解説

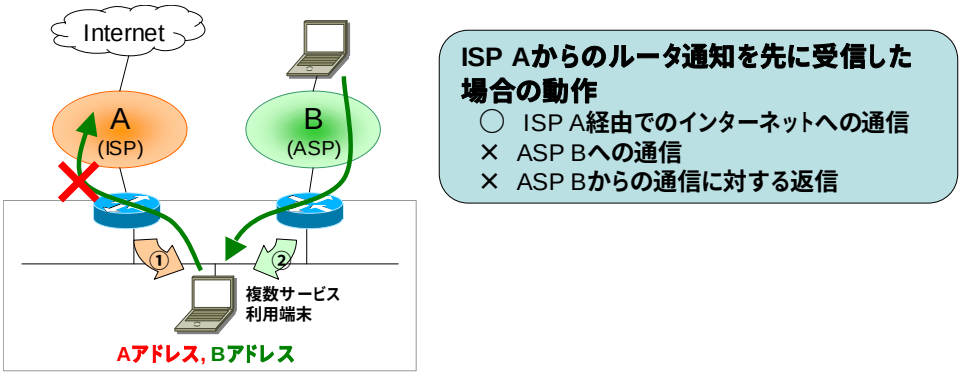


図 24　デフォルトゲートウェイ選択問題

図 24 にデフォルトゲートウェイ選択問題のネットワーク構成を示す。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 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うまく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 考えられる問題解決法

RFC4191 にて定義されている RA の拡張機能によって、この問題は解決することが可能である。RFC4191 において定義されている一つの追加機能としてルータ優先度フラグがあり、ルータ通知のフラグフィールドに 3 段階（01：high、00:medium（デフォルト）、11:low）で優先度を指定できる機能である。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デフォルトの medium 設定となる。この機能は、FreeBSD の rtadvd、Linux の radvd にて実装を確認することができた。

また、RFC4191 では、経路情報通知オプション機能もある。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。ただし、RA の優先度と経路情報の優先度は独立しているため、配布するプレフィックスと経路情報の関連についても検討する必要がある。

今後、この機能の実装・動向は、IPv6 端末 OS にとって影響が大きなものと考えられるため注目する必要があると思われる。

なお、本節の問題に関する議論は、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 にて詳細に議論されており、結果はガイドラインとして策定される予定である。

6 用語

当該文書で記述されている用語については、IAjapan(財団法人日本インターネット協会)様においてまとめられている、IPv6 関連用語集をご参照頂きたい。

http://www.iajapan.org/ipv6/v6term/glossary_01.html

上記に記述されていない用語について、下記で説明する。

用語	説明
ULA	Unique Local IPv6 Unicast Addresses の略であり、RFC4193 で定義されている。 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、Internet 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、プリフィックス部分をランダムに生成して使用する２種類の空間が定義されている。後者は取得の手続きは必要ないが完全な一意性が保証されない。ただし衝突が発生しにくいランダム値の計算方法が示されており、アドレス衝突の可能性を低減することは可能である。 これによって、組織の合併によるサイト境界の曖昧化やアドレスのリナンバリングを抑制することが期待されている。
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。 しかし、ドメイン名に対してなんらかのリソースレコードが存在するのに NXDOMAIN を返す不正な応答をする DNS サーバが存在する。 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。
Teredo	RFC4380 にて定義されている、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。ただし、シンメトリック NAT 配下では動作することができない。

7 まとめ

7.1 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。

7.2 当該ガイドラインの最後として

従来、Macintosh 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 社が IPv6 にデフォルトで対応している Windows Vista をリリースしようとしている。

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、Internet 業界の健全な成長に繋がると考えられる。

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