IPv6導入時に注意すべき課題

IPv6 普及・高度化推進協議会
IPv4/IPv6共存WG
IPv6導入に起因する問題検討SWG

2011年11月24日

目 次

1　はじめに

IPv4 アドレス在庫枯渇を期に、IPv6 の重要性がより高まり、世界的にも徐々に導入が進んでいます。この IPv6 の普及に伴い、新たな課題が発生する可能性があります。オペレータコミュニティや標準化団体などでも、それぞれに IPv6 導入時に発生する可能性のある問題についての情報共有や対応を実施していますが、これらをさらに広く共有することが重要になってきています。

2005 年、WIDE プロジェクトにて IPv6 を実装した製品の動作、技術的課題確認、整理を行うことで IPv6 実装/導入/運用の改善を図る「IPv6 Fix(v6fix)」と呼ばれる活動が実施されました (http://v6fix.net/)。この活動の後、IPv6 に関する RFC など技術情報は大きく追加/更新され、また、IPv6 を実装している機器も増えてきました。

このような状況のもと、2010 年 11 月、IPv6 普及・高度化推進協議会 IPv4/IPv6 共存 WG 内に新たに「IPv6 導入に起因する問題検討 SWG (v6fix swg)」を立ち上げ、これらの技術課題の整理と共に「IPv6 Fix(v6fix)」の意思を引き継ぎ新たな IPv6Fix として活動をはじめました。

本文書では、v6fix swg 参加メンバにより検討した技術課題をリストアップし、課題の内容を紹介しています。課題の解決方法や対処方法は、導入環境により変わってくるため、課題自体の共有に主を置いています。IPv6 を導入する際や、IPv6 サービス提供の際の参考になれば幸いです。

2　IPv6 から IPv4 へのフォールバックに関する課題

2.1　課題の解説

IPv4/IPv6 が同時に使える環境では、デュアルスタックノードは IPv4/IPv6 アドレス両方を持つ相手と通信する場合に、IPv6 を優先して利用することが多い。この場合 IPv6 の接続性に問題があると、IPv6 から IPv4 に切り換えて通信をしようとする。この動作をフォールバックと呼ぶ。この切り換えに時間がかかる、もしくは切り換わらないことがあり、ユーザの利便性を損なう (IPv4 から IPv6 への切り換えにも同様の事象が発生するが、ここでは取り扱わない)。

2.2　発生原因

1. ノードは TCP 通信において通信先とセッションがはれない場合に何度かセッションの確立を試みる。この動作により最終的に通信先と通信ができないと判断し、次のセッションへと切り換わるまでに多くの時間を要する場合がある。この動作は宛先アドレス一つ毎に対して行われるため、通信先が DNS に複数の IPv6 アドレスを登録しているようなサーバで、IPv6 接続性に問題

がある場合、フォールバックが成功するまでにより多くの時間がかかる可能性がある。

2. 通信先がDNSに複数のIPv6アドレスを登録している場合、その全てのアドレスに対し通信を試みた後にIPv4アドレスへの通信に切り替わるが、その際の試行回数の上限が決まっている実装があり、登録されているIPv6アドレスがその上限数以上の場合IPv4へとフォールバックせずに通信を終了してしまう。

3. フォールバック動作自体をしない実装や、特定のプロトコルのみフォールバックを行わない実装などがある。

(問題が確認された実装例)

1. 多くのOS(Windows XP/Vista/7, MacOS X, Linux, UNIX)で、IPv6の接続性に問題がありかつネットワーク側からも応答が何もない場合、そのアドレスに対するTCPのセッション確立を諦める(タイムアウトする)までに20秒以上時間がかかる。

2. Microsoft Internet Explorer (IE7, IE8)ではフォールバックの回数の上限が決まっており、これを超える数のIPv6アドレスが名前解決の際に得られた場合、IPv4へフォールバックせずに通信が終了してしまう。回数はレジストリで制御可能となっており、ディフォルト値が5回となっている。

3. iOS 4.2.1ではネットワーク側から何も応答がない場合、フォールバックを行わずに通信を終了してしまう。

4. Android 2.3.2の一部製品ではHTTPではフォールバックするが、HTTPSではフォールバックしない。

2.3 Security Consideration

パスワードの送付など、ユーザ認証系ではHTTPSが利用されているため、上記4のような実装には注意する必要がある。

2.4 IPv6特有の課題であるか?

IPv4でも起こりえる。デュアルスタックノードがIPv4通信を優先して利用する場合は、IPv4の接続性に問題が発生するとIPv6通信へと切り換える。

2.5 課題状況の確認方法

1. 通信完了に時間がかかる (Web ページが表示されない)、通信に失敗する等で発見できることがある。

2. `http://test-ipv6.jp/` または、`http://test-ipv6.com/` につないで確認する。

2.6 対処方法

1. サイトの出口等で、TCP 通信ならクライアントに TCP-RST を返すことで、迅速にフォールバックさせることが可能な実装が多い。

2. 上記実装例 2 の場合、サーバ側で DNS レコードの登録数を少なくする。Windows 端末で、レジストリの値を変更し、フォールバック回数を増やす等で回避可能（参考文献 2.8)。

3. 課題 3 の対処方法も参照。

4. Windows や UNIX 系システムでは、RFC3484 に従ったポリシテーブルの設定で、特定の通信相手との通信の際に IPv4 を優先する等の設定が可能であり、フォールバック問題を回避できる。

2.7 現象

- サイトの表示までに時間がかかる。
- サイトが表示されない。

2.8 参考文献

- Microsoft サポートページ `http://support.microsoft.com/kb/2293762/ja`

3 DNS の問い合わせに関する課題

3.1 課題の解説

1. IPv6 で通信したい場合に、DNS による名前解決において AAAA RR を正常に取得できないことがある。「IPv6 only で通信したい」 状況として以下のようなパターンが想定される。

- IPv6 only の通信相手との通信
- IPv4 の方が通信品質が悪い場合 (CGN が入っている場合等) で IPv6 を利用した方が良好な場合

2. キャッシュDNS サーバへのアクセスに、IPv4/IPv6 のどちらを使うかは現状、実装依存であり、どちらで通信してもおなじ結果が得られることが期待されているが、そうでない場合に、意図したサイト以外へのアクセスになる、通信できない、といった問題が発生する。

3.2 発生原因

- DNS サーバの実装によっては、AAAA, A のみの登録の場合、登録されていない RR を聞かれたときに NX_DOMAIN を返してしまう。このため、場合によって、IPv6 でも IPv4 でも通信ができないことがある (1)。
  - OS やアプリケーションによる実装の違い。AAAA, A の優先順位や解決の順番が異なる。
  - ロードバランサの DNS 実装で、AAAA に返答しないものが存在する (参考文献参照)。
  - OS 毎の挙動の違いに加え、同じ OS でもバージョンが異なるとレゾルバの挙動が変わる場合がある。ex) Windows
- キャッシュDNS サーバの設定によっては、AAAA RR を返答しないことがある (BIND の設定等)。その場合、ユーザが IPv6 を使いたくても使えない (1)。
  - DNS サーバが query のトランスポートに合わせる (IPv6 で聞かれたら AAAA を返す) 実装をしている。デュアルスタックで通信可能だが DNS サーバとして IPv4 アドレスしか通知されていないと IPv4 でしか通信しない。
  - DNS のトランスポートに IPv4 しか扱えないクライアント OS も存在する (WindowsXP など)。
- DNS サーバへの到達性がない場合、DNS の名前解決が原因でアクセスが遅くなったり、不可能になったりすることがある (1)(2)。
  - OS によっては、キャッシュDNS サーバとして IPv4、IPv6 アドレス両方を持っている場合には、IPv6 を優先する。この場合、IPv6 DNS サーバへの通信ができないと、名前解決に時間がかかる。

- DNS proxy, キャッシュDNS サーバなどが AAAA RR を透過できずに IPv6 アドレスを解決できない。家庭用ルータには簡易な DNS proxy 機能が実装されていることが多い。解決できない原因として以下のようなケースが存在する。
  - AAAA RR を正常にハンドリングできず無応答のまま、ないしはエラーを返す (1)。
  - AAAA RR を透過できない。原因として、以下のような理由が考えられる (1)。
    * 実装が古く AAAA RR を正常に取り扱うことができない。
    * 512 バイト以上の DNS パケットを正しく取り扱えずに解決不能。AAAA RR は A RR より 12 バイト大きいため発生しやすい。
    * IPv6 が閉域網になっているなどの事情から IPv6 アドレスを通知したくないという理由で意図的に AAAA RR を返さない。※ IPv6 家庭用ルータガイドライン (2.0 版) では 「リソースレコード (RR) の種別に関わらず全て透過的に処理すること」 を必須としている。

3.3 Security Consideration

- IPv4/IPv6 双方で提供するデータやサービスの内容は DNS やアプリケーションで一致させる必要がある。
  - 整合性がとれないと XSS 同様のセキュリティ問題になる。
  - 同じくフィッシングと判定されるかもしれない。

3.4 IPv6 特有の課題であるか?

- デュアルスタック環境下で起こりうる問題
- 特に閉域網では注意が必要

3.5 対処方法

- IPv4 と IPv6 両方のトランスポートで解決できるようキャッシュDNS サーバを維持し、ユーザ端末には IPv4 アドレスと IPv6 アドレスの両方を通知する (2)。
- UDP フラグメントが転送できることが前提となる。

  - エンドノードのファイアウォールで転送を許可する。
  - 家庭用ブロードバンドルータではフラグメントに対応していないものも存在するため、注意。
- TCP での問合せも送受信できるようにしておく。
  - ファイアウォールで TCP での DNS 通信を許可する。
- 8.8.8.8 などの public DNS サーバを利用する。

3.6 参考文献

- RFC3596: DNS Extensions to Support IP Version 6
- RFC4294: IPv6 Node Requirements
- draft-ietf-6man-node-req-bis
- RFC3901: DNS IPv6 Transport Operational Guidelines
- JPRS IPv4 アドレス枯渇と DNS〜DNS の IPv6 対応について〜 http://www.kokatsu.jp/blog/ipv4/data/interop2009/11_JPRS_TAKASHIMA.pdf
- RFC4472: Operational Considerations and Issues with IPv6 DNS
- RFC4942: IPv6 Transition/Coexistence Security Considerations
- IPv6 普及・高度化推進協議会 IPv6 家庭用ルータガイドライン (2.0 版) http://www.v6pc.jp/jp/upload/pdf/v6hgw_Guideline_2.0.pdf

3.7 検索キーワード

IPv6 DNS 問題, パケットサイズ 512(バイト以上), UDP フラグメント, TCP DNS フィルター, 逆引き

4 キャプティブポータルと DNS に関する課題 (ホテルでの IPv6 uninstall 問題)

4.1 課題の解説

- 公衆のインターネット接続を利用する際に、一旦特定のウェブページへアクセスして認証 (ブラウザ認証) する方法が動作しないため、解決策として、

「IPv6 をアンインストールすべし」というインストラクションがホテル等に常置されている。

- (ホテル等の) キャプティブポータルのキャッシュDNS サーバで、AAAA 問い合わせに A を返すものがある。
- Windows XP では、AAAA 問い合わせに対して返ってきた A 応答を利用するために、リダイレクト表示される URL の A 応答によりフォールバックすることなく通信不能となる。
- Windows Vista 以降、Linux、MacOSX、FreeBSD では AAAA 問い合わせに対して返ってきた A 応答を利用せずに、A 問い合わせに対して返ってきた A 応答のみを利用するため問題なく動作する。

4.2 発生原因

- クライアント OS による DNS 実装の違い。
- 認証システムに実装されている DNS 機能が問い合わせのレコードに正しく応答していない。

4.3 IPv6 特有の課題であるか?

- デュアルスタック環境で発生

4.4 対処方法

- ホテルなどのネットワーク設備による問題であり根本的な対処は困難。
- 応急処置として、クライアントの IPv6 通信機能を一時的に解除。

4.5 検索キーワード

ホテル, 接続, IPv6

4.6 現象

- インターネット接続認証画面が表示されず、インターネット接続が利用できない。

5 品質の悪いトンネルに関する課題 – 移行技術関連 (6to4, Teredo)

5.1 課題の解説

- 無保証なリレールータ、通信品質の悪い経路を使用しての通信となる可能性があるため、通信品質が悪い、つながらない、という場合がある。
- 十分に管理されていないリレールータを利用する場合があり、通信ができなくなる可能性がある。

5.2 発生原因

- ユーザが 6to4 や Teredo のアドレスを使用して通信をした場合に、速度が遅いと感じる。
- Windows XP/Vista/7 の場合、デュアルスタックサーバに対してのアクセスに関しては、ポリシテーブルにより、トンネルよりも IPv4 の方が優先される。6to4 に関しては、IPv6 グローバルユニキャストアドレスが付与された場合にはトンネルアドレスは付与されないため、特に問題になることはないはず。
  - 昔の MacOS X(10.6.4 まで) では、6to4 を含め、IPv6 を優先する。

5.3 Security Consideration

- Teredo アドレスにはユーザが使用している NAT ルータの IPv4 グローバルアドレスや L4 ポート番号が使われているため注意が必要。
  - NAT ルータによっては、外部からの使用アドレス/ポート向けのパケットを通してしまう。
- 6to4 アドレスには、端末の IPv4 アドレスが埋め込まれいるので、注意が必要。
- リレールータが信用できない場合、パケットの盗聴等の懸念がある。

5.4 IPv6 特有の課題であるか?

- 6to4, Teredo 等の移行技術利用時の問題

5.5 課題状況の確認方法

- トンネルインタフェースが利用されているかの確認
  - ipconfig + パケットキャプチャ、ipconfig + netstat

5.6 対処方法

- 品質のよい IPv6 サービスを利用する (商用サービス等)。
- MacOS X では、6to4 を disable するか、最新バージョンにアップデートする。

5.7 参考文献

- RFC3056: Connection of IPv6 Domains via IPv4 Clouds
- RFC3068: An Anycast Prefix for 6to4 Relay Routers
- RFC3964: Security Considerations for 6to4
- RFC4380: Teredo: Tunneling IPv6 over UDP through Network Address Translations
- RFC6081: Teredo Extensions
- RFC6343: Advisory Guidelines for 6to4 Deployment
- draft-ietf-v6ops-6to4-to-historic

5.8 検索キーワード

6to4, Teredo

5.9 現象

通信が遅いとユーザが感じる。

6　不正ルータ広告に関する課題

6.1　課題の解説

想定していない機器がルータ広告 (RA) を送出し、同一リンク上の機器にディフォルト経路、（プレフィックス）が追加付与され、

- 通信経路が混乱する。
- プレフィックスが複数付与され、OS がアドレス選択動作により、場合によって通信ができなくなる。
- プレフィックスが多数付与されることで、OS が異常動作を起こす。

という課題。

6.2　発生原因

- Windows の Internet Connection Sharing (ICS:インターネット接続の共有) 機能が on になっている場合、IPv6 接続性も共有しようとして RA を送出する場合がある。特に、IPv4 グローバルアドレスが付与されている場合、6to4 プレフィックスを RA で広告する。
- 通信妨害や、通信盗聴のために、故意に RA を流すことも想定される。

6.3　Security Consideration

同一リンク上のノードに対する、

- 攻撃（プレフィックスを多数付与しリソースを消費させる、等）
- 通信の妨害や盗聴

に利用される可能性がある。

6.4　IPv6 特有の課題であるか?

- IPv4 の DHCP でも同等の事象は発生するが、RA はマルチキャストを利用しているため、より簡単に、広範囲のホストに影響が生じる可能性がある。

6.5 課題状況の確認方法

- 付与されているアドレスの確認
- ディフォルト経路の確認、等

6.6 対処方法

- スイッチなどによる RA のフィルタリング
- Router Preference(RFC4191) の利用
  意図的なものは排除できない
- モニタリングによる対策
  - NDPMon : セグメント内の NDP パケットの異常を検知
  - rafixd(KAME) : 不正 RA と同じ RA を Router Lifetime=0 で広告、不正 RA による機器内容をリセット
  - SEND(Secure Neighbor Discovery) の導入
- 設定アドレスの上限設定
  無制限に RA を受け付けず上限を実装において設ける

6.7 参考文献

- 情報処理推進機構：情報セキュリティ技術動向調査（2009 年下期）タスクグループ報告書
  http://www.ipa.go.jp/security/fy21/reports/tech1-tg/documents/tech-1-2009b-00.pdf
- JNSA Network Security Forum 2009：北口善明/金沢大学 総合メディア基盤センター
  http://www.jnsa.org/seminar/2009/0127nsf2009/data/A4_3Kitaguchi.pdf
- インターネット協会 IPv6 Summit 2010：佐々木良一/東京電機大学 未来科学部 教授, 内閣官房情報セキュリティセンター 情報セキュリティ補佐官
  http://www.iajapan.org/ipv6/summit/2010/pdf/04/01_sasaki.pdf
- InternetWeek? 2009：鈴木 伸介/アラクサラネットワークス株式会社
  http://www.nic.ad.jp/ja/materials/iw/2009/proceedings/h5/iw2009-h5-02.pdf

- IPv6 Secure Neighbor Discovery: Protecting Your IPv6 Layer 2 Access Network
  http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6553/white_paper_c11-563156.html
- RFC6104: Rogue IPv6 Router Advertisement Problem Statement
- RFC6105: IPv6 Router Advertisement Guard

6.8 検索キーワード

不正ルータ広告, rogue RA

6.9 現象

IPv6 での通信ができない，不安定

7 デュアルスタックサイトのプロトコル別品質

7.1 課題の解説

- 回線品質やサーバの処理能力は IPv4 と IPv6 では異なる場合があり、A と AAAA 両方が付与されたサイトにアクセスする際に IPv4 と IPv6 でレスポンスタイムが異なったり、片方でアクセスが出来ないという事象が発生する可能性がある。
- 現在は、IPv6 だと遅くなるという場合が目立つと思われるが、IPv4 と IPv6 で別サーバにしている場合に IPv4 のサーバが過負荷状態でも IPv6 のサーバが空いていて IPv4 の方が遅くなるといった事例も起こりうる。

7.2 発生原因

- サーバ側の回線が
  - IPv4 と IPv6 で回線速度が異なる。
  - IPv4 と IPv6 の RTT が異なる (IPv6 が海外周りになる場合がある)。
- ファイアウォール, サーバ OS, アプリケーションなどが IPv6 の場合にパフォーマンスが劣化する場合がある。

- そもそも IPv6 が有効になっていないのに AAAA を書いている (接続できない)。
- ルーティング、途中経路
- ラストワンマイル (トンネル含む)
- クライアント OS の実装の問題
- (サーバを分けている場合) サーバの処理能力とアクセス数の違い

7.3 IPv6 特有の課題であるか?

- デュアルスタック環境下での問題

7.4 課題状況の確認方法

- IPv4 と IPv6、両方でアクセスをし速度・疎通を比較 (ただし、「品質の悪いトンネル問題」の場合もあるため、それとの切り分けも必要)

7.5 対処方法

- エンドユーザ側
  - 品質のよいプロトコルを利用する (IPv6 の優先度を下げ、IPv4 でアクセスをする等)。
  - サービス提供者に苦情を入れる。
- サービス提供者
  - IPv4 と IPv6 で、サービスの提供品質に差が出ないようにする (今後、デュアルスタックのユーザ端末が増加すること、そのようなユーザ端末では IPv6 通信が優先されるであろうことを考えると、IPv6 でのサービス提供品質に特に気をつかう必要がある)。
    * IPv6 の回線品質の向上。
    * ファイアウォール, サーバ機器などの増強。

8 アドレス選択に関する課題 (マルチプレフィックスに関する課題)

8.1 課題の解説

- 複数の IP プレフィックスを持つユーザが通信を行う際に、選択する送信元 IP アドレスによっては通信ができない場合があるという問題。

8.2 発生原因

- 端末が複数の IPv6 プレフィックスを持つ場合の、送信元 IP アドレスの選択誤りによる。
  - プレフィックスを払い出したサービス提供者に、そのサービス提供者が払い出した IPv6 アドレス以外を始点アドレスとするパケットを送信した場合、uRPF 等でフィルタされることがあり、通信が成立しないことがある。片方が閉域網サービスの場合、始点 IP アドレス選択を誤ると、フィルタされなかったとしても通信パケットが届かない。
- ユーザが複数の IPv6 プレフィックスを持つ例としては、以下のような場合がある。
  - フレッツサービスと ISP の IPv6 サービスの併用
  - 6to4 等に対応した IPv6 ルータ (AirMac 等) と、ISP IPv6 サービスの同時利用

8.3 IPv6 特有の課題であるか?

- IPv4 でも起こりうるが、IPv6 ではユーザが複数の IP プレフィックスを容易に設定可能なため、顕著に発生する。

8.4 課題状況の確認方法

- パケットのソースアドレスが正しいことを確認する。

8.5 対処方法

- 正しいアドレスを選択する (RFC3484 の利用)。
- 利用する IPv6 アドレスを一つにする。

8.6 参考文献

- RFC3484: Default Address Selection for Internet Protocol version 6 (IPv6)
- RFC5220: Problem Statement for Default Address Selection in Multi-Prefix Environments: Operational Issues of RFC 3484 Default Rules
- draft-ietf-6man-rfc3484-revise

8.7 検索キーワード

マルチプレフィックス

8.8 現象

- IPv6 での通信ができない。

9 IPv6 ブリッジ機能 (IPv6 パススルー機能) サポートのみで「IPv6 対応ルータ」であると誤認識されていることに関する課題

9.1 課題の解説

- IPv6 インターネット接続サービスを利用したいユーザが、IPv6 をブリッジする機能のみを有したルータを「IPv6 対応ルータ」として販売しているベンダの製品を購入してしまい、IPv6 インターネット接続サービスを利用できないという問題。

9.2 発生原因

- 「IPv6 対応」の認識の違いにより、表記方法が統一されていないことが原因。

9.3 課題の分析

- IPv6 対応ルータだと思って購入しても、IPv6 ブリッジ機能では対応できないサービスの場合に、IPv6 接続サービスを利用することができない。

9.4 Security Consideration

課題 10 を参照

9.5 IPv6 特有の課題であるか?

- IPv6 特有

9.6 対処方法

- IPv6 対応ルータであっても全 IPv6 接続サービスに対応可能ではないことを周知する。
- 「IPv6 対応ルータ」の定義を明確にすると共に、ベンダは各製品が対応している IPv6 接続サービスのリストを、ユーザにわかりやすい形で公開することで問題の低減が可能。

9.7 参考文献

- IPv6 ブリッジ機能: `http://bb.watch.impress.co.jp/cda/koko_osa/18406.html`
- Google 等で「IPv6 対応ルータ」を検索した場合、検索結果には IPv6 ブリッジ機能を有するルータも多く含まれることに注意。
- フレッツ 光ネクスト対応状況一覧表 (他社ブロードバンドルータ) `http://flets.com/next/list_router.html`

9.8 現象

- IPv6 対応ルータだと思って購入しても、IPv6 接続サービスを利用することができない。

10 「IPv6 対応ルータ」におけるブリッジ・フィルタに関する課題

10.1 課題の解説

- 「IPv6 パススルー機能」を持つホームルータにて、IPv6 フィルタが対応されておらず、セキュリティ的に問題がある場合がある。

10.2 発生原因

- IPv6 パススルー機能にて、フィルタリング機能が想定されていないため。

10.3 課題の分析

- 「IPv6 パススルー機能」が有効になっているホームルータは、IPv4 を NAT 等でアクセス制限する一方で、IPv6 は単純にブリッジするだけでフィルタリング機能を持っていない。IPv4 と IPv6 で同じセキュリティレベルを提供できない点が問題。

10.4 Security Consideration

- IPv6 においてセキュリティレベルが確保できない可能性がある。

10.5 IPv6 特有の課題であるか?

- 原理的には、IPv4 でも起こりうるが、製品として「IPv6 パススルー」機能付きルータが多く市販されているため、IPv6 環境にて影響が大きい。

10.6 課題状況の確認方法

- ホームルータの「IPv6 パススルー」機能の調査。

10.7 対処方法

- IPv6 フィルタリング機能を具備した「IPv6 パススルー機能」を持つホームルータを導入する (現状、安価なルータでは皆無)。
- 「IPv6 ブリッジ機能」は、フィルタ機能を持たない、ということを認識して利用する (別なセキュリティ対策手法を用意する)。

10.8 参考文献

ブリッジ機能のセキュリティ問題 : http://121ware.com/product/atermstation/product/function/33.html

10.9 検索キーワード

IPv6 パススルー機能

10.10 現象

- IPv4 で守られていたものが IPv6 では守れなくなる。

11 DNS への登録に関する課題

11.1 課題の解説

- アドレス自動設定を使ったときの DNS 正引き、逆引き登録問題。
  1. DHCPv6 を使った場合には、IPv4 と同等
  2. SLAAC を使った場合の、登録方法
  3. 一時アドレスを使った場合の登録方法
- そもそも、逆引きを登録すべきか否か。
  - IPv6 又はデュアルスタック環境下でのホストへの DNS 正引き・逆引きの登録方法について一般化されておらず、各事業者が個別の対応を取る事で事業者間・ユーザが共通の技術として利用しにくくなるという問題。

11.2 発生原因

- DNS の登録運用方法の不一致

11.3 Security Consideration

- フィルタ漏れによるオーバーブロッキング

11.4 IPv6 特有の課題であるか?

- IPv4 でも起こりうる。
- IPv6 及びデュアルスタック環境下で起こる。

11.5 課題状況の確認方法

- 一般ユーザでは発見することは難しい。

11.6 対処方法

- 対処方法としては下記 4 つが可能性としてあり、業界内での十分な検討が必要。
  - 登録しない
  - レコードの自動生成
  - ワイルドカードレコードの利用
  - DynamicDNS(DDNS) の利用

11.7 参考文献

- IPv6 端末 OS における IPv6 対応・IPv6 機能活用ガイドライン
  - http://www.v6pc.jp/pdf/v6TermOs_Guideline_1.pdf
- Reverse DNS in IPv6 for Internet Service Providers
  - http://datatracker.ietf.org/doc/draft-howard-isp-ip6rdns/
- DNS の v6 対応
  - http://v6ops-f.jp/index.php?plugin=attach&refer=meeting%2F%C2%E81%B2%F3IPv6%A5%AA%A5%DA%A5%EC%A1%BC%A5%B7%A5%E7%A5%F3%A5%BA%A5%D5%A5%A9%A1%BC%A5%E9%A5%E0&openfile=v6ops-f-dns-ito.pdf
- IPv6 時代の DNS 設定を考える
  - http://v6ops-f.jp/index.php?plugin=attach&refer=meeting%2F%C2%E81%B2%F3IPv6%A5%AA%A5%DA%A5%EC%A1%BC%A5%B7%A5%E7%A5%F3%A5%BA%A5%D5%A5%A9%A1%BC%A5%E9%A5%E0&openfile=v6ops-f-dns-shin.pdf
- IPv6 逆引き自動生成 DNS サーバ
  - http://v6ops-f.jp/index.php?plugin=attach&refer=meeting%2F%C2%E82%B2%F3IPv6%A5%AA%A5%DA%A5%EC%A1%BC%A5%B7%A5%E7%A5%F3%A5%BA%A5%D5%A5%A9%A1%BC%A5%E9%A5%E0&openfile=2_06_v6rev.pdf

- One implementation of IPv6 reverse DNS server
  - `http://member.wide.ad.jp/~fujiwara/v6rev.html`
- IPv6 Reverse Zone Maker
  - `http://negi.ipv6labs.jp/shared/ipv6_reverse-zone-maker.html`

11.8 現象

- ログ解析が難しくなる。
- アクセス制御がしづらくなる。
- 逆正一致が困難になる。

12 セキュリティ：フィルタリングに関する課題

12.1 課題の解説

- インターネットとの接続ルータにおけるフィルタ設定において、IPv4 と同じポリシと同じポリシを IPv6 に適用した場合、阻害してはいけない IPv6 通信を意図せず阻害してしまい、結果として IPv6 環境においてインターネット通信ができなくなるという問題

12.2 発生原因

- IPv6 の通信特性を理解していないフィルタ設定

12.3 課題の分析

- ICMPv6 フィルタ (Path MTU Discovery 対応)
  - DoS 攻撃の対策として近年 IPv4 接続においては、外部からの ICMP パケットをフィルタしている場合が多く見受けられる。しかしながら IPv6 接続においても、IPv4 接続と同様に ICMPv6 パケットをフィルタした状態が見受けられる。この場合、Path MTU discovery 動作における ICMP エラーパケット (Too-Big-Message) を破棄してしまうことになり、配下の端末が、MTU 探索に失敗してしまう状態となっている。

12.4 IPv6 特有の課題であるか?

- IPv6 特有

12.5 課題状況の確認方法

- ICMPv6 フィルタ
  - インターネット通信ができない。

12.6 対処方法

- インターネット接続ルータにおけるフィルタを変更する。

12.7 現象

- IPv6 のインターネット通信ができない。

13 メールシステムの対応状況

13.1 課題の解説

メールシステムを IPv6 対応にした場合に、メールの送受信ができなくなることがある。

13.2 課題の分析

MX レコードに、AAAA と A のホストが併記されており、AAAA のみのホストが優先されている場合、MTA によっては、メールの送受信に問題が発生することがある。

13.3 発生原因

MTA の不具合。

13.4 IPv6 特有の課題であるか?

IPv6 と IPv4 の混在環境で発生。

13.5 課題状況の確認方法

IPv6 対応後、メールが正しく送受信できない。

13.6 対処方法

受信側では、MX に登録されているホストを確認し、AAAA のみのホスト登録を避ける。ソフトウェアを変更する。送信側では、通信相手に交渉する、特定サイト向けを IPv4 通信とするような設定をする。

13.7 現象

メールシステムを IPv6 対応にした場合に、メールの送受信ができなくなることがある。

14 迷惑メール対策：MTA の逆引きとの関連

14.1 課題の解説

メールシステムを IPv6 対応にした場合に、受信先によってはメールを送信できなくなるケースが想定される。

14.2 課題の分析

受信側 MTA の迷惑メール対策として、送信元 MTA に逆引きが設定されていない場合、メール受信を拒否する手法が用いられている。

14.3 発生原因

ボットネットからの迷惑メール送信に代表されるように、逆引き設定のない MTA から送信されるメールの大半が迷惑メールであるという事実が存在する。この事実を利用し、IPv4 でのメール運用において、逆引きを設定していない送信側 MTA を迷惑メール送信者として扱い、受信側 MTA で受信拒否する設定が採用されてきた。

14.4 Security Consideration

逆引きによる迷惑メール判定は、誤判定の可能性もある (逆引きできない MTA のすべてが迷惑メール送信者とは言えない) ため、通信事業者で採用しているケースは少ない。が、一般企業などでは導入しやすいために、採用している事例も多い。また、メールアプライアンスのディフォルト設定となっているケースも想定される。このため、IPv6 では一般的には逆引き設定不要と言われているが、MTA に関しては逆引き設定が必須であると考えるべきである。

14.5 IPv6 特有の課題であるか?

IPv4 においても、逆引きを設定していない MTA からは、メールを送信できないことがあるため、IPv6 特有の問題ではない。

14.6 課題状況の確認方法

IPv6 対応後、メールが正しく送信できているかを確認する。送信できる相手と、送信できない相手がある場合には、逆引き設定が間違っている可能性がある。

14.7 対処方法

MTA の逆引きが正しく設定されているかどうかを確認し、されていない場合には適切に登録する。

14.8 検索キーワード

迷惑メール, spam

14.9 現象

メールシステムを IPv6 対応にした場合に、宛先によってはメールの送信ができなくなる。

15 迷惑メール対策 : グレイリスティング

15.1 課題の解説

メールシステムを IPv6 対応にした場合に、グレイリスティングの有効性が不明。

15.2 課題の分析

グレイリスティングは、IP アドレスをベースとした一時拒否フィルタリング手法である。既存のフィルタリングプログラムでは、IPv4 アドレスを前提として処理しているため、IPv6 アドレス対応が必要となる。しかし、IPv6 アドレス空間は広大であるため運用上の困難が想定される。

15.3 発生原因

既存プログラムの処理が IPv4 アドレスを前提としているものがある。

15.4 Security Consideration

IPv6 アドレス空間が広大なため、迷惑メール送信元が IP アドレスを次々と変えながら送信し続ける可能性があり、IPv4 同等の効果が発揮できるか不明。

15.5 IPv6 特有の課題であるか?

IPv6 アドレスの長さや形式やアドレス空間のサイズに起因する問題であるため、IPv6 特有の問題である。

15.6 課題状況の確認方法

既存 IPv4 運用時に、グレイリスティングを使用しているかどうか、設定を確認する。

15.7 対処方法

- 下記参考文献に挙げた IPv6 対応のグレイリスティングプログラムを使用して効果を測定する。
- IP アドレスベースではなく、送信ドメイン認証技術の認証結果とそのドメイン名によるレピュテーションに基づいた迷惑メール判定を検討する。

15.8 参考文献

- `http://gurubert.de/greylisting`
- `http://hcpnet.free.fr/milter-greylist/`

15.9 検索キーワード

迷惑メール, spam

15.10 現象

メールシステムを IPv6 対応にした場合に、グレイリスティングの有効性が不明。

16 迷惑メール対策：ブラックリストデータベースサービス (DNSBL)

16.1 課題の解説

メールシステムを IPv6 対応にした場合に、DNSBL を利用できない。

16.2 課題の分析

- DNSBL は、IP アドレスを利用したブラックリストデータベースを利用して、迷惑メール送信元からのメール受信を拒否する技術である。IPv4 アドレスを前提としているため、IPv6 アドレス対応が必要となる。

16.3 発生原因

- 既存の DNSBL を利用した対策は IPv4 アドレスを前提としている。
- IPv6 アドレスは、データ長や表現形式などが IPv4 アドレスと異なるため、同様の処理を行うにはプログラムの改修とデータベースの拡張が必要である。

16.4 Security Consideration

- 現時点では、IPv6 アドレスに対応した DNSBL がほとんど存在していない。
- IPv6 対応可能な DNSBL において、広大な IPv6 アドレスを個別に登録するのか、プレフィックスでグループ化して対応するのかというような方法論が定まっていない。
  - IPv6 アドレスを個別登録する場合、迷惑メール送信側でアドレスを変えながら送信し続ける可能性があり、データベースとしての有効性に疑問がある。

– プレフィックスで対応する場合には、その中に迷惑メール送信者ではないアドレスを含んでしまう可能性もあるため、過剰なフィルタリングとなる危険性がある。

16.5 IPv6 特有の課題であるか?

IPv6 アドレスの長さや形式やアドレス空間のサイズに起因する問題であるため、IPv6 特有の問題である。

16.6 課題状況の確認方法

既存 IPv4 運用上、DNSBL を利用しているかどうかを確認する。メール・アプライアンスではディフォルトで設定されている可能性がある。

16.7 対処方法

- DNSBL の IPv6 上での実装に関しては、方法論が定まるまで待つ。
- 一部の DNSBL においては、ホワイトリストでの対処が検討されている。その有効性に関しては検証されていない。
- IP アドレスベースではなく、送信ドメイン認証技術の認証結果とそのドメイン名によるレピュテーションに基づいた迷惑メール判定を検討する。

16.8 検索キーワード

迷惑メール, spam

16.9 現象

メールシステムを IPv6 対応にした場合に、DNSBL を利用できない。

17 アクセス回線におけるトラブルの切り分け

17.1 課題の解説

- ユーザから通信が異常に見えた際に、契約先 (ISP, アクセス回線事業者) に連絡しても異常が発見されない場合がある (かもしれない)。

17.2 発生原因

- ユーザから見えるアクセス回線事業者と ISP のほかに、ユーザには見えない事業者がいる場合があり (VNE, ローミング)、故障がユーザから見えない事業者で発生した場合に、ユーザから見えているコールセンタだけでは解決できない場合がある。

17.3 課題の分析

- 大規模な故障の場合には、おそらく情報が共有される。
- レアケースなユーザ影響の場合には、解決できないかもしれない。

17.4 IPv6 特有の課題であるか?

- 特有ではない。
- バックボーンの大手事業者への委託やローミングというこれまであったビジネスと同等。

17.5 対処方法

- 関係する事業者が連携する。
- どんなロールが存在して成り立っているか啓蒙活動する。

17.6 参考文献

- http://www.soumu.go.jp/main_content/000009743.pdf

17.7 現象

- 問題の解決に時間がかかる (かもしれない)
- そもそも原因が特定されない (かもしれない)
- コールセンタにたらい回しにされる (かもしれない)

18　L2 マルチキャスト未対応機器の存在

18.1　課題の解説

- マルチキャスト機能に未対応もしくは実装に不具合がある L2 通信機器を使用した場合に、マルチキャスト機能を使用する NDP が失敗して IPv6 通信ができない。

18.2　発生原因

- LAN 内に、マルチキャスト機能に未対応もしくは実装に不具合がある L2 通信機器が存在している。以下が該当する L2 通信機器の例。
  - L2 スイッチ (ハードウェア/ファームウェア)
  - イーサネットカード (ハードウェア/ファームウェア/ドライバ)
  - PC 等 (OS ドライバ)
- LAN 上でマルチキャストパケットの送信に失敗するケース (L2 スイッチ等の問題) と、ノード上でマルチキャストパケットの受信に失敗するケース (イーサネットカードや OS ドライバの問題) がある。
- LAN 上で一部のノードのみがマルチキャスト受信に対応していない場合、そのノードから送信される IPv6 パケットは他のノードに届くが、他のノードからそのノードに IPv6 パケットが送信できないという非対称の障害になることがある。

18.3　Security Consideration

- Promiscuous モードに設定するワークアラウンドを採用する場合は、特権が必要。本来必要のないパケットへの対処が必要なため、別なセキュリティ問題を引き起こす可能性がある。また、ノードの過負荷といった問題も発生する。

18.4　IPv6 特有の課題であるか?

- IPv6 の問題というよりは、L2 におけるマルチキャスト機能の問題。
- IPv4 ではアドレス解決にブロードキャストを使用する ARP を用いるが、IPv6 ではマルチキャストを使用する NDP が必須である。
- IPv4 環境では L2 マルチキャストを使用する機会が多くないので、問題が顕在化しにくい。

18.5 課題状況の確認方法

- 一部もしくは全部の機器で IPv6 通信全般ができない状態になるため、原因がわかりにくい。
- 二台のノード間で、片方向だけパケットが疎通することがある。
- PC 等で問題の解析を行おうとしてパケットキャプチャを有効にすると、Promiscuous モードが設定されて通信が可能になることがある。

18.6 対処方法

- L2 通信機器のファームウェアやドライバを最新バージョンにアップデートする。
- L2 通信機器をマルチキャスト機能に対応したものに置き換える。
- ネットワークインタフェースを Promiscuous モードに設定し、マルチキャストか否かに関わらず LAN 上の全パケットを受信するようにする。
- マルチキャストに対応していないスイッチの場合、通信相手が特定できる場合には、特定のマルチキャストアドレスを透過する設定で対処が可能な場合がある。

18.7 参考文献

- RFC4861: Neighbor Discovery for IP version 6 (IPv6)

18.8 検索キーワード

NDP, NS, NA, 近隣探索, 近隣要請, 近隣通知マルチキャスト, L2, 通信不可

18.9 現象

- LAN 上で、ノード間の IPv6 通信に失敗する。
- 近隣探索 (NDP) による、MAC アドレス解決に失敗する。
- 特定のノードのみ IPv6 通信ができない。または特定のノード宛の IPv6 パケットのみが届かない。

19　IPv6 マルチキャストが宅内通信に悪影響を与えることに関する課題

19.1　課題の解説

- IPv6 マルチキャストによる配信サービス等を受けている環境等で、必要のない機器にまでマルチキャストが届き、高負荷のため正常な通信に影響が出ることがある。

19.2　発生原因

- 仕様上、マルチキャストは、同一セグメント上すべてのノードに配信されるため。

19.3　課題の分析

- 映像配信等トラフィックの多いマルチキャスト通信が存在する場合に、マルチキャスト通信に関係しないスイッチや、ノードがその通信に影響される。特に、無線アクセスポイント等をブリッジで設置している場合には、有線側の帯域に比べて無線の帯域が狭いことが多く、無線での通信に輻輳等の問題が発生する場合がある。

19.4　IPv6 特有の課題であるか?

- IPv4 でも、マルチキャストを利用した場合には発生する。

19.5　課題状況の確認方法

- スイッチの通信状態を示すランプの点滅等で確認可能な場合がある。
- パケットのキャプチャ、通信状態の確認等で確認可能。

19.6　対処方法

- マルチキャストサービスに加入している場合には、通信が必要な機器とそれ以外の機器でセグメントを分ける、MLD snooping 機能をもった機器や (必要なければ) 無線側にマルチキャストをフォワードしない機能をもった無線機器を利用する、等で対処可能。

19.7 参考文献

- RFC4541: ”Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches”

19.8 検索キーワード

IPv6, マルチキャスト, MLD Snooping

19.9 現象

- 影響を受けている機器の、通信品質に問題が発生する (遅延、パケットのドロップなど)

20 アドレス表記に起因する課題

20.1 課題の解説

- IPv6 では様々なアドレス表記が可能となっており、アドレス検索が容易に行えないという問題、ログ出力の不一致に関する問題、カスタマーサポート等における意思疎通が適切に行えないという問題などがある。

20.2 発生原因

- IPv6 では省略表記が認められており、アドレス表記に柔軟性があるため、様々なアドレス表記を行うことが可能となっている。

20.3 課題の分析

- RFC3513 前後でアドレス表記に関する仕様が変更されている (16bit 0 Field が 1 つだけの場合の解釈)。
- 推奨される統一的なアドレス表記が存在していなかった。

20.4 Security Consideration

- アクセス制御等の目的で X.509 証明書を用いているような場合に、証明書の検証時にテキストによる単純比較を行ってしまうと、有効/無効を誤判定してしまう可能性があり、セキュリティリスクとなる。

20.5 IPv6 特有の課題であるか?

- IPv6 特有の問題である。IPv4 アドレスは省略表記やアルファベットがなく、唯一 Leading zeros(先行する 0) に関して柔軟性を持つが、一般知識として誰でも Leading zeros を理解できるため問題とならない。

20.6 課題状況の確認方法

- IPv6 アドレス検索に失敗した場合、ログ出力が一致しない場合など。

20.7 対処方法

- RFC5952 に準拠した製品、システム等の使用 (恒久対処)。
- RFC5952 に未対応の製品、システム等に関しては、提供元に対して改善依頼を行うと共に、RFC5952 に準拠したアドレス表記への正規化処理を行うことで回避する (暫定対処)。
- エンジニアやカスタマサポート要員に対して、RFC5952 に準拠したアドレス表記の教育、啓蒙を行う。
- TEL 等で IPv6 アドレスを伝える際には RFC5952 に準拠した省略表記を用いる。アルファベットに関しては Phonetic code(A : Alfa, B : Bravo, C : Charlie …) 等の円滑なコミュニケーションのための手段を用いることも有効である。

20.8 参考文献

- RFC5952: A Recommendation for IPv6 Address Text Representation

21 実装としてのミニマムスペックがないことに関する課題

21.1 課題の解説

- 家電やセンサー機器を IPv6 ネットワークに接続する際の最低限必要なスペックが共通化・共有されていない。

21.2 課題の分析

- IPv6 接続環境下においてIPv6 アドレスやDNS その他オプション値の取得など接続する為の端末実装についてミニマムスペックが無い。

21.3 IPv6 特有の課題であるか?

- IPv4 環境でも発生しうるが、技術的に枯れており発生しにくい。

21.4 対処方法

- IPv6 端末ミニマムスペックの定義

21.5 課題状況の確認方法

- ネットワークに接続できない・正常に通信できない。

21.6 参考文献

- IPv6 端末OS における IPv6 対応・IPv6 機能活用ガイドライン
  - http://www.v6pc.jp/pdf/v6TermOs_Guideline_1.pdf
- IPv6 家庭用ルータガイドライン
  - http://www.v6pc.jp/jp/upload/pdf/v6hgw_Guideline_2.0.pdf
- RFC4294: IPv6 node requirements
- ripe-501: Requirements For IPv6 in ICT Equipment
  - http://www.ripe.net/ripe/docs/ripe-501

21.7 現象

- IPv6 接続について様々な実装が出てくる。

22　一時アドレス (RFC4941) の利用

22.1　課題の解説

1. RFC4941 が、想定通りの利用がされていない。
    - サーバでの待ち受けアドレスとしての利用等
2. 「IP アドレスは固定」を前提としているネットワーク (企業網等) で利用された場合に、ホストの管理がしにくくなる。

22.2　発生原因

IPv6 アドレスの下位 64bit をランダムに変更させる RFC4941 が、どのようなケースで推奨できるのか、何を解決できて何を解決できないのかが理解されていない。また、意図せずに利用されているケースがある。

22.3　課題の分析

- IPv6 アドレスの下位 64bit は、当初デバイスの MAC アドレスを元に設計する方向 (EUI64) であったが、デバイスを変更しない限り、付与される IPv6 アドレスの下位 64bit が変更されずホストが特定され、個人や利用機器の特定と利用状況の追跡が可能となる懸念があるため、プライバシ保護の観点から、匿名アドレス生成方法として RFC3041 が作成され、後に RFC4941 と改訂された。

- RFC4941 は実サービス上、推奨されるものか否か。
  「IPv6 アドレスは固定アドレスである」ことを前提として、IPv6 アドレスを認証キーとしたアプリケーション検討、もしくは Push 型サービス検討がなされている場合があるが、匿名アドレス利用だと通常は利用できなくなるので注意が必要である (DDNS や MobileIPv6 等の対応が必要)。Push 型サービスの利用に制限が出てしまうと、IPv6 のメリットが薄れてしまう可能性がある。必要に応じて、関係者への周知徹底が必要である。

- RFC4941 によって、何が解決されるか。
  下位 64bit がランダムに変化するため、使用するホストの MAC アドレスを外部から隠ぺいすることができ、通信の記録や追跡に伴うプライバシの懸念を低減させる。ただし、上位 64bit が不変である場合には、トレーサビリティに伴うプライバシ懸念を必ずしも低減させることはできない。

22.4 Security Consideration

- RFC4941 の一義的な想定は、MAC アドレスの流出を防止するものであり、従来の EUI64 ベースのアドレス生成以上にセキュリティ問題を発生させることはない (RFC4941 の 7 章)。

22.5 IPv6 特有の課題であるか?

IPv4 においてもブロードバンド接続サービスにおいて、固定の IPv4 アドレスを付与しているケースでは、何らかの手段でこのアドレスと個人情報を紐付けられれば、同じ懸念は存在していた。

22.6 対処方法

1. RFC4941 が、どのような場合に有効に使えるかを啓蒙する。
    - OS ごとの挙動の違いにも注意する必要がある (Windows ではディフォルトで on になっている、等)。
2. 管理下のホストで、RFC4941 を利用しない設定をする。

22.7 参考文献

- draft-iesg-serno-privacy (Exipred)
- RFC4941 : 「Privacy Extensions for Address Configuration in IPv6」
- 総務省 : 「電子政府システムの IPv6 対応に向けたガイドライン, P22, 平成 19 年 3 月 30 日」

22.8 現象

- MAC アドレスを隠ぺいし、IPv6 アドレスを可変にすることで、通信の追跡を困難にし、プライバシの懸念を低減することができる。
- 固定アドレス前提でサービスが作られている場合、RFC4941 適用者は利用できなくなる。

23　IPv6アドレスのトレーサビリティ

23.1　課題の解説

- IPv6 の使用により、IPv4 とは異なるレベルのトレーサビリティが生じることがある。対処は難しいが影響は限定的。

23.2　発生原因

- ISP の IPv6 プレフィックスの割り当てが IPv4 グローバルアドレスの割り当てに比べてスタティック性が高い運用が多くなることが予想されるため。
- IPv6 のインターフェース ID(後ろ 64bit) がスタティックである運用が (しかも MAC アドレスを用いて) なされることがあるため。 (⇒ 21. を参照)

23.3　課題の分析

- ここでは IP アドレスのトレーサビリティとは、ユーザとインターネット経由でつながる接続先において、同じ接続元 IP アドレスからの複数の接続に関して、これらは同じユーザからの接続であると推測できることをいう。接続先は同一ホストである必要はない。
- 同じ IP アドレスが長期間運用されていると、長期間トレーサビリティを提供していることになる。
- 従来 IPv4 の運用においては、家庭用ルータに ISP が割り振るグローバルアドレスは動的なものが多かった。ユーザはサービスオプションとして静的な運用を選択できるものもあった。静的アドレスを保証しない場合でも実際にはめったに異なるアドレスが割り振られない運用のものもあれば、家庭用ルータの電源再投入で異なるアドレスを得られる運用もあるなど、様々であった。よって、ユーザは ISP 選択も含めれば、自分の家庭用ルータのトレーサビリティをある程度制御することもできた。
- なお、IPv4 運用時には、家庭用ルータに長期のトレーサビリティを提供する ISP が大きな問題となっていたわけではない。
- 一方、IPv6 においては家庭用ルータに割り振られるプレフィックス部分を見ることによって、IPv4 同様に家庭用ルータのトレーサビリティを得ることができる。しかし、本格運用前ではあるが、このプレフィックスは IPv4 グローバルアドレスの運用ほど動的には運用されない可能性が高いと予測されている。

- なぜなら、IPv4 グローバルアドレスは節約目的で動的運用されていた側面もあるが、IPv6 プレフィックスにはその必要性が少ないからである。また、IPv4 グローバルアドレスの変更は家庭用ルータの WAN アドレスにしか影響しないが、IPv6 プレフィックスの変更は家庭用ルータ以下の全機器の IPv6 アドレスの変更を呼び起こすためである (ただし数日単位ならば、あまり問題はないだろう)。
- よって、ユーザは家庭用ルータのトレーサビリティを制御する方法が大幅に制約される (ISP 変更レベル) ことになる。
- ほぼすべての家庭で長期トレーサビリティが提供されるとすると、それを前提にしたサービスが開発されるかもしれず、そうしたサービスが広まると、それらに障害があるという理由でプレフィックスを変更することが困難になってしまうことすら考えられる。

23.4 Security Consideration

- プライバシ (深刻度低)

23.5 IPv6 特有の課題であるか?

- IPv4 でもあった問題が、IPv6 だと影響が大きくなる

23.6 課題状況の確認方法

- ISP の運用ポリシを確認する
- 実際に長期間、プレフィックス値を観察する

23.7 現象

- 悪意のあるサービスによるトレーサビリティの濫用の可能性
  - ログイン等の仕組みがない複数のサイトでのアクセスを IP 寄せしてターゲッティングなど
- ルータの IP を変更すればなんとかなったタイプの Workaround が困難に

24 CGN, トランスレーションに関する課題

24.1 課題の解説

- CGN, トランスレータの影響で、一部のアプリケーション/サービスがユーザの期待通りに動作しないという問題が起こる。
  - IPv4/IPv6 トランスレータが、以下の目的で導入される。
    - IPv4 only 機器からの IPv6 インターネットへの reachability を確保するため
    - IPv6 only 機器からの IPv4 インターネットへの reachability を確保するため
  - CGN の導入も同様の影響があると考えられている (IPv4 ⇒ IPv4 通信で問題)

24.2 発生原因

CGN, トランスレータが導入されたため。

24.3 課題の分析

- 性能・運用や、アプリケーション毎の事情もあるので一概にはいえない。
- アプリケーション/サービスもユーザ環境もデュアル対応している場合は、IPv6 が優先されることが多いため、問題は発生しない。つまり移行時期のみの問題である。
- 同時セッション数制限による問題
  - 参考文献 1 によれば、99%のユーザに影響を及ぼさないようにするためには同時セッション数の上限を 1,000 にしなければいけないが、これでは Global IPv4 消費のペースをたかだか 1/64 にするにすぎない (90%までのユーザで良いとする場合は上限 100 本)。
- サービス側で利用者を IP アドレスで特定できないことによる問題
  - CGN や、IPv4/IPv6 トランスレータの外からは同じ Global IPv4 アドレスにみえてしまう。
  - IP ベースでアクセス管理を行っているサービスと相性が悪い。

  - 掲示板のアクセス制限や、並列ダウンロードを禁止するサイトなど。ログの解析の難易度も上がる。

- CGN が導入された場合、一部の NAT Traversal 技術が動作しないという問題
  - UPnP など、double NAT 下では機能しないものがある。
- 一部のアプリケーションプロトコルに含まれる IP アドレスの問題
  - CGN/トランスレータの ALG も対応していないようなプロトコルでは IP アドレスを正しく変換できないと思われる。
- NAT4:4:4 で、ISP レベルと家庭内で同じサブネットアドレスを用いた場合
  - 同じ CGN 内のユーザ宛の通信は CGN を経由しないで直接できるようになっている場合、サブネットアドレスがかぶると家庭内と CGN 内でうまく経路選択できない実装のホームルータがあると思われる。

24.4 IPv6 特有の課題であるか?

IPv6 に IPv4 との互換性がないために導入される、既存機器との接続互換性を確保するための別技術 (トランスレーション) が引き起こす問題。

24.5 課題状況の確認方法

アプリケーションが期待通りに動作しないという現象は発見しやすい。一方で、問題の原因がトランスレータであることを特定することはユーザにはほぼ不可能である。

24.6 対処方法

- ユーザができること
  - (CGN/トランスレータ) 同時セッション数を減らす (同時に使うアプリケーション・機器を減らす)。
  - (CGN) ホームネットワークのサブネットアドレスを変えてみる。
  - (CGN/トランスレータ) 諦めて違うアプリケーション・サービスを試す。
- 開発者ができること

- (CGN/トランスレータ) 同時セッション数を減らすことができるようにする (ユーザ設定や、ダイナミック本数コントロールなど)。
- (CGN/トランスレータ)source IP 以外の情報を考慮したアクセス分析をする。
- (CGN)double NAT を考慮した NAT Traversal 技術を利用する。
- (CGN/トランスレータ) 自前プロトコルの場合には IP アドレスを埋め込まないようにする。
- (トランスレータ)IPv6 ではまともに動くようにして、IPv4 でのユーザ体験が悪くてもしょうがないと割り切る。

24.7 参考文献

1. 「ISP への NAT 導入によるユーザ影響評価」
   - http://www.ieice.org/jpn/books/kaishikiji/2010/201006.pdf
2. 「NAT のご利用は計画的に」
   - http://www.janog.gr.jp/meeting/janog24/program/d2p5.html
3. 「消費者の理解を得にくい, ネット家電の IPv6 問題」
   - http://itpro.nikkeibp.co.jp/article/Watcher/20091015/338865/

24.8 検索キーワード

LSN, CGN, トランスレータ, ALG

24.9 現象

アプリケーションが期待通りに動作しない、地図に穴が開くなど。

25 誤解されそうな表現、古い情報の共有

25.1 課題の解説

- IPv6 環境では IPsec が必ず実装されている。
  - 必ず使用していると誤解してしまう

- グローバルアドレスを使うとセキュリティが低下すると過剰に警戒してしまう。
- マルチキャストに対応しているということの意味。
- 「IPv6 対応」の意味 (8 項も参照)。
- IPv6 を uninstall, 無効化すると機器が速くなる (無効化推奨) といった情報。

25.2 発生原因

新情報の周知不徹底。

25.3 課題の分析

利用者の知識の問題である。

25.4 Security Consideration

IPsec に対する誤解とグローバルアドレスへの過剰な警戒はセキュリティに関連する。

25.5 IPv6 特有の課題であるか?

特有の問題である。

25.6 課題状況の確認方法

知識の問題であるため難しい。対象者に対する設問などで確認をとるほかない。

25.7 対処方法

知識の周知。なんらかの設問形式の資料などで敷居を下げて周知することが考えられる。

25.8 現象

現在の標準ではない環境を作ってしまう。

26 IPv4で複数サブネットを利用している環境へのIPv6導入

26.1 課題の解説

IPv4 で複数サブネットを利用しているネットワークに、IPv6 を導入する場合、以下の項目について検討する必要がある。

- ISP から割り当てられるプレフィックス長。
  - IPv6 では、/64〜/48 の間でアドレスが割り当てられる。各サブネットに、手動、または DHCP-PD でアドレスを割り当てる。
- IPv4 で複数のサブネットを利用している場合には、IPv6 も同じトポロジにする、IPv6 パススルー機能を利用して、別トポロジで構成する、等の選択肢があるが、IPv4 でサブネットを分けている理由がある場合には、IPv6 パススルー機能の利用に関しては考慮が必要。

26.2 Security Consideration

IPv4 と IPv6 でトポロジが異なる場合に、IPv4 でのネットワークアクセスポリシと IPv6 でのポリシが合致しない可能性がある。

26.3 IPv6 特有の課題であるか?

IPv4/IPv6 混在の問題。

27 L2 ネットワークと IPv6

27.1 課題の解説

IPv4 で動作した環境に IPv6 を導入しても正しく動作しない、また IPv4 では分かれていたセグメントが IPv6 では繋がって見えてしまうといった問題。

27.2 発生原因

- L2 の設計を誤っていた場合
- VLAN の実装が IPv4 に依存している機能となっている L2 機器

27.3 課題の分析

- IPv4 では L2 のネットワーク設計が雑でも、インターフェースに設定されるネットワーク情報が一種類しかなかったため動作できていたが、IPv6 になると複数のネットワーク情報が付与されるので問題となる。
- IPv4 では認証とダイナミック VLAN の組み合わせで問題なかったものが、IPv6 ではルータ広告のようなマルチキャスト通信が全てのポートに流れる実装があり問題となる。

27.4 Security Consideration

想定外のセグメントを設定してしまう場合がある。

27.5 IPv6 特有の課題であるか?

IPv4 では顕著に問題とならなかったが、IPv6 では問題となる。

27.6 課題状況の確認方法

想定外のセグメントに IPv6 のルータ広告が届いているか調査する。

27.7 対処方法

- L2 のネットワーク設計を正しく (マルチキャストを意識して) 実施する。
- VLAN なども含み、マルチキャストを正しく扱える L2 機器を導入する。

27.8 検索キーワード

VLAN, マルチキャスト

27.9 現象

セグメントが混ざった状態となるので正しく通信ができなくなる。

28 PMTUD BlackHoleに関する課題

28.1 課題の解説

ICMPv6 が経路の途中でフィルタリングされていることで、通信ができなくなるという問題

28.2 発生原因

- ICMPv6 がすべてフィルタリングで落とされている場合や、トランスペアレントなファイアウォール機器にて ICMPv6 がフィルタされている。

28.3 課題の分析

- IPv6 では PMTU を調査することが必須である。そのため、ICMPv6 がフィルタで落とされていた場合には”Packet Too Big”の ICMPv6 パケットも落ちてしまい、途中経路の MTU を通知できないため。

28.4 IPv6 特有の課題であるか?

IPv4 において DF ビットが設定された場合と同様。

28.5 課題状況の確認方法

- MTU の値を小さく (IPv6 の最小値 1280 バイトなど) にして通信が可能であった場合にこの問題が原因と考えることができる。
- tracepath 等の経路 MTU を表示するツールを利用する。

28.6 対処方法

- 始点ホストが、MTU の値を小さく (IPv6 の最小値 1280 バイトなど) して通信を行う。
- TCP 通信の場合には、ホームゲートウェイ等で MSS の調整を実施する。
- ICMPv6 に対するフィルタを見直す。

28.7 検索キーワード

PMTUD(Path MTU Discovery)

28.8 現象

通信不可

29 CPE の独自ドメインを解決できないことに関する課題

29.1 課題の解説

CPE の設定画面へのアクセスができない場合がある。

29.2 発生原因

*「.setup 」のようなブロードバンドルータ固有のドメインが解決できない場合がある。

- IPv6 パススルー機能を持ったルータ下にいるホストで、IPv6 の DNS サーバアドレスが設定されている場合に、IPv6 での DNS クエリ送信が優先されると、問題の事象が発生する。
  - CPE が、IPv4 の DNS へのクエリが来る事を期待して固有ドメインを利用する場合、CPE は、v6 で DNS クエリが来るとスルーしてしまう。グローバルな DNS に問い合わせて NXDOMAIN が返り名前解決できず、ホストにてネガティブキャッシュされてしまう。

29.3 課題の分析

固有ドメインを使う事。IPv4/IPv6 混在環境を想定してない事。

29.4 IPv6 特有の課題であるか?

IPv4/IPv6 混在の問題。

29.5 課題状況の確認方法

- ホストの DNS 設定を確認する。

29.6 対処方法

- IP アドレスを直接入力する。
- ポリシテーブルをカスタマイズしてみる。

29.7 現象

CPE の設定ができない。

30 IRR への登録に関する課題

30.1 課題の解説

経路情報の登録が行われていないことによって、経路広告が遮断され、通信ができないことがある。

30.2 発生原因

- (上流)ISP 間の経路交換にあたっては、経路広告のポリシを IRR(Internet Routing Registry) と呼ばれるデータベースに登録することが求められる。
- IRR と並行して、アドレス割り当て管理機関が管理するレジストリデータベース (whois) で参照可能なことも条件とされる場合が多い。
- IRR への登録がされていない、登録に間違いがある場合に、経路広告が意図通りに行われないことがある。
- これにより、端末同士の通信が確立しなくなる。

30.3 課題の分析

- 設定ミス、登録忘れなど人災による。
- まれに、支払い問題など経済的理由でフィルタされたり、ピア切断する場合もある。

30.4 IPv6 特有の課題であるか?

IPv4 と同様の運用

30.5 課題状況の確認方法

ping や traceroute でのターゲットへの到達性がないことを確認後、以下の手順で確認できる。

- 公的な IRR の登録確認。
  - http://www.irr.net/docs/list.html
- 商用 IRR については、管理を行っている ISP へ問い合わせる必要がある (カスタマならば参照できる場合もある？)。
- レジストリデータベースでの登録確認。
- Looking Glass による確認。
  - http://www.bgp4.as/looking-glasses
  - http://neptune.dti.ad.jp/
  - http://lg.he.net/
  - http://www.ipv6tf.org/index.php?page=using/connectivity/looking_glass
  - http://www.switch.ch/network/tools/ipv6lookingglass/
- IX などでは、広告する経路情報をメールや専用ツールでお知らせして、フィルタ解除を求めることもある。

30.6 対処方法

- IPv6 導入時に、登録確認を行う。
- IPv6 導入時に、地理的な分散を考慮していくつかのサイトへの接続確認を行う。

30.7 参考文献

- RFC4012: Routing Policy Specification Language Next Generation (RPSLng), RFC2725 と RFC2622 の update
- RFC1786/RIPE-181: Representation of IP Routing Policies in a Routing Registry
- RFC2650: Using RPSL in Practice
- RFC2726: PGP Authentication for RIPE Database Updates
- RFC2769: Routing Policy System Replication
- RFC5943: A Dedicated Routing Policy Specification Language Interface Identifier for Operational Testing
- IPv6 BGP filter recommendations, RIPE31(1998/9/23), `http://www.space.net/~gert/RIPE/ipv6-filters.html`
- JANOG Comment, `http://www.janog.gr.jp/doc/janog-comment/jc1006.txt`: 「xSP のルータにおいて設定を推奨するフィルタの項目について (IPv6 版)」
- Reference for IPv6 Router settings, `http://www.team-cymru.org/ReadingRoom/Templates/IPv6Routers/`
- JPIRR, `http://www.nic.ad.jp/ja/ip/irr/`

30.8 現象

- 利用者が意図する、あるいは期待するとおりに通信が行われない。
- IPv6 通信可能にも関わらず IPv4 にフォールバックしたり通信不能となる。

31 DNS レコードの登録数と OS の動作に関する課題

31.1 課題の解説

Microsoft の Internet Explorer では、サーバに対する接続試行回数をレジストリで制御可能となっており、ディフォルトでは 5 回となっている。このため、AAAA が 5 つ以上ついている場合に、IPv6 接続性に問題があると IPv4 までフォールバックしない。

31.2 発生原因

接続回数制御パラメータ（ConnectRetries）のディフォルト値の問題。

31.3 課題の分析

現状、A レコードを多数登録している例があり、この場合、AAAA も同数登録される可能性が高い。

31.4 IPv6 特有の課題であるか?

IPv4 でも発生する。

31.5 課題状況の確認方法

IPv4/IPv6 デュアルスタック環境で、通信できない場合に、通信経路の状態を調べるとともに、AAAA, A の登録数も調べる。

31.6 対処方法

- DNS レコードの登録数を少なくする。
- レジストリの値を変更し、接続試行回数を増やす。

31.7 参考文献

`http://support.microsoft.com/kb/2293762/ja`

31.8 現象

サイトにアクセスできなくなる。

32　サイトの見え方に関する課題

32.1　課題の解説

- IPv6 でアクセスした場合と、IPv4 でアクセスした場合に、サイトの見え方や得られるデータが違うという問題 (故意に見え方を変えている場合は除く)。IPv6 でアクセスしたとき、古いコンテンツが見えていたり、データ的に、IPv4 でアクセスした場合と IPv6 でアクセスした場合に得られる結果が違った、などが報告されている。
- コンテンツの参照先が IPv4/IPv6 デュアルスタックで、参照先への IPv6 接続性がない。

32.2　発生原因

- IPv6 と IPv4 でコンテンツサーバを分けている場合で、データの同期がうまくいっていない場合に発生する。
- CMS の IPv6 対応。
  - リンク切れのチェック等を IPv6 で実施できない。

32.3　Security Consideration

サーバが複数ある場合に、管理レベルが違うとセキュリティ的な懸念がある。

32.4　IPv6 特有の課題であるか?

IPv4 でも、サーバ・データを分散している場合に起こる場合がある。

32.5　課題状況の確認方法

サイトの見栄え、得られたデータの違いから発見できる。

32.6　対処方法

構成に応じた、データの管理をしっかりする。発見した場合には、サイト管理者に通知。

32.7　現象

サイトの見え方、手に入る情報が違う。

A　検討メンバ

以下に検討メンバを示す。会務担当者以外のメンバーは、組織の 50 音順に従っている。

氏名	所属
新 善文 (部会長)	アラクサラネットワークス株式会社
北口 善明 (部会長)	金沢大学
藤崎 智宏 (部会長)	日本電信電話株式会社
島村 充	株式会社インターネットイニシアティブ
廣海 緑里	株式会社インテック
川島 正伸	ＮＥＣアクセステクニカ株式会社
高田 美紀	株式会社 NTTPC コミュニケーションズ
樋口 貴章	株式会社オープンテクノロジーズ 財団法人インターネット協会迷惑メール対策委員会
印南 鉄也	シスコシステムズ合同会社
吉川 典史	ソニー株式会社
上根 義昭	ソネットエンタテインメント株式会社
宮崎 純生	西日本電信電話株式会社
岩井 孝法	日本電気株式会社
北村 浩	日本電気株式会社
岡田 真悟	日本電信電話株式会社
花山 寛	ネットワンシステムズ株式会社
辰巳 智	

B　本文書内の情報について

本文書に記載されている情報については、IPv6 普及・高度化推進協議会のサイトポリシ (`http://www.v6pc.jp/jp/site_policy.phtml`) に従います。