

IPv6 Fix WGの検討内容紹介

InternetWeek 2013 T3: IPv6トラブルシューティング 2013
2013/11/27 (水) 9:15~11:45

NTTコミュニケーションズ株式会社 高田美紀

自己紹介

- 1993～ 株式会社NTTPCコミュニケーションズ
 - ISP (InfoSphere) サーバの運用
 - ホスティング (WebARENA) 立ち上げ～開発～運用
 - 主にDNS、メールシステム担当
- 2013/4～ NTTコミュニケーションズ株式会社
 - 先端IPアーキテクチャセンタ
 - ✓ R&D部門
 - ✓ DDoS対策技術、DNSまわりでの事業部サポート、対外活動
- 対外活動
 - dnsops.jp 幹事
 - ときどき JANOG meeting スタッフ、などなど
- エンジニア+母親業の両輪で活動中

Agenda

- IPv6普及・高度化推進協議会、v6fix swgの紹介
- ガイドライン: 追加する課題
 - DNS関連の課題
 - 新しいglibc問題
 - ULAのリーク
 - IPv4アドレス生表記
- ガイドライン: 更新する課題
 - SMTP関連
 - LL言語でのIPv6アドレスの扱い
 - 無線アクセスポイントの使い方
 - 機器の挙動 (IPv6の優先に関して)
- まとめ、参考資料

「IPv4/IPv6共存WG」配下SWG

■ サービス移行SWG (v6app)

- IPv4アドレスでビジネスをしているxSP事業者やデータセンター、中小ISP等の事業者が問題なくIPv6サービスの導入ができる環境やリスクの分析
- ネットワークやサーバのデュアルスタック化の検証
- IPv6における運用ノウハウの洗い出し

■ IPv6家庭用ルータSWG (hgw)

- IPv6家庭用ルータの仕様に係る各種技術的検討
- 「IPv6家庭用ルータガイドライン第1版」ブラッシュアップ
- BroadbandForum等、海外標準化組織との連携

■ IPv6導入に起因する問題検討SWG (v6fix)

- 情報収集 (As-ISの状態の)
- 既存のIPv6/IPv4混在環境での問題の再チェック
 - ✓ <http://www.v6fix.net/> など
- 想定されるIPv6/IPv4混在環境で発生する問題の洗い出し、解法の検討
- 検討結果の公開 (FAQ集等)

v6fix: チャーター

■ 趣旨

2011年4月以降、コンシューマ向けIPv6サービスが順次提供開始されると想定される。提供後、ユーザネットワークはIPv6/IPv4混在環境となり、それに伴い数々の問題の発生が想定される。本WGでは、IPv6導入後に発生すると考えられる問題を洗い出し、問題に対する解法を検討、共有することで、IPv6サービスの円滑な導入を支援することを目的とする。

■ 体制

- 部会長 藤崎智宏 (日本電信電話株式会社)
- 部会長 新善文 (アラクサラネットワークス株式会社)
- 部会長 北口善明 (金沢大学)

v6fix: 活動内容

■ これまでの活動

- 2011/9/30 「IPv6導入時に注意すべき課題」 公開
 - ✓ http://www.v6pc.jp/jp/entry/wg/2011/09/ipv6_2.phtml
 - ✓ http://www.v6pc.jp/jp/pdf/20111124_v6fix.pdf
 - ✓ 2011/11/24 更新版

■ 今後の活動予定

- 2013年内
 - ✓ 公開サーバにおけるIPv6対応状況の調査及びフィードバック
- ~2014/3
 - ✓ ドキュメント更新作業
- 2014/5頃
 - ✓ パブコメ募集

■ ドキュメントへのご意見募集中

- <https://www.v6pc.jp/jp/wg/coexistenceWG/comment2.phtml>

DNSの課題

- 中途半端な(?)IPv6導入

どんな問題か: web, mail

- ホスト名に対するAAAAレコードのIPv6アドレスへの接続性
 - 複数サーバのうち1つだけ or 全部
 - 一度目は接続できないが、繰り返すと可能になる
 - ✓ 別マシンから or 何日か後に再接続すると、同様の事象
- ドメインに対するMXレコードの参照先への接続性
- Webサイト、メールシステム等のIPv6導入が中途半端(?)
 - Dual Stack環境、IPv6環境からの接続に問題
 - 繋がらない、繋がるのに時間がかかる、もっさり、
 - メールが送信できない、などなど

どんな問題か: DNS

■ 権威DNSサーバ設定、委任の問題

- 上位DNSに登録されているglue AAAAに問い合わせを送っても返答がない
- glue AAAAと、権威DNSに登録したAAAAに違いがある
- IPv4の方でカバーしている場合が多い
 - ✓ IPv6 onlyの環境だと??
 - ✓ 参照先キャッシュDNSサーバのトランスポートによる

■ 権威DNSサーバ実装の問題

- AAAAを問い合わせると沈黙する権威DNSサーバ
 - ✓ キャッシュDNSサーバは返事をタイムアウトまで待つ
 - ✓ リゾルバへはSERVFAILを返す
 - ✓ IPv4へフォールバック (端末OS,アプリケーションの実装次第)
- GSLB機器の問題?

中途半端なIPv6対応: 問題の解決

- どのサービスをどうIPv6対応するのか?
- 計画通り設定されたかチェック
 - DNS (委任、ゾーン内のコンテンツ、キャッシュ)
 - web (http, https)
 - ✓ 想定通りのコンテンツを取得できるか
 - メール (smtp, smtps, pop, pops, imap, imaps)
 - ✓ 宛先に届いたかどうか
 - ✓ メールボックスからの取得
 - 大事なこと
 - ✓ telnet, openssl, dig コマンド等、プロトコルの動きのわかるもの
 - ✓ 「全ての」「IPアドレス」に対して!!
- サービス監視
 - IPv4でのサービスと同レベルで

どんな通信を
しているか
隠蔽されない

DNSとの
切り分け

中途半端なIPv6対応: 問題の解決: DNS

■ 委任関係

- DNS設定チェック (JPRS)
 - ✓ <http://dnscheck.jp/>
- 委任関係のチェックのみ
- ゾーン内のレコードについてはノーケア
 - ✓ 正しいIPアドレスを設定してあるか、など
 - ✓ dig, nslookup で

■ digコマンド, nslookupコマンド

- 権威DNSサーバのIPv6対応
 - ✓ 権威DNSサーバのIPv6アドレスに対して検索要求
- ゾーン内コンテンツのIPv6対応
 - ✓ AAAAレコードを検索
- 初心者のためのDNS運用入門 -トラブルとその解決のポイント-
 - ✓ <http://dnsops.jp/event/20130719/20130719-dns-beginners-guide-mizuno-2.pdf>

中途半端なIPv6対応: 問題の解決: DNS

```
% dig www.example.jp aaaa @2001:db8::53 +norec
; <<>> DiG 9.9.3-P2 <<>> www.example.jp aaaa @2001:db8::53 +norec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERR
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 4
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:;, udp: 4096
;; QUESTION SECTION:
;www.example.jp.                IN      AAAA
;; ANSWER SECTION:
www.example.jp.                86400  IN      AAAA   2001:db8:7::80
;; AUTHORITY SECTION:
example.jp.                    86400  IN      NS     ns1.example.jp.
example.jp.                    86400  IN      NS     ns2.example.jp.
;; ADDITIONAL SECTION:
ns1.example.jp.               86400  IN      A      192.0.2.53
ns1.example.jp.               86400  IN      AAAA   2001:db8::53
ns2.example.jp.               86400  IN      A      192.0.2.153
ns2.example.jp.               86400  IN      AAAA   2001:db8::153
;; Query time: 4 msec
;; SERVER: 2001:db8::53#53(2001:db8::53)
;; WHEN: Sun Nov 10 07:49:43 JST 2013
;; MSG SIZE rcvd: 226
```

チェックしたい
権威DNSサーバの
IPv6アドレス

中途半端なIPv6対応: 問題の解決: 他サービス

```
% telnet 2001:db8::25 25
Trying 2001:db8::25...
Connected to 2001:db8::25.
Escape character is '^]'.
220 mail.example.jp ESMTP Postfix
helo example.jp
250 mail.example.jp
mail from: test@example.com
250 2.1.0 Ok
rcpt to: test@example.jp
250 2.1.5 Ok
2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
Subject: test mail

test

.
250 2.0.0 Ok: queued as 051B22F5CAB
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

```
% telnet 2001:db8::80 80
Trying 2001:db8::80...
Connected to 2001:db8::80.
Escape character is '^]'.
GET / HTTP/1.1
host: www.example.jp

HTTP/1.1 200 OK
      :      :
```

```
% telnet 2001:db8::25 110
Trying 2001:db8::25...
Connected to 2001:db8::25.
Escape character is '^]'.
+OK Dovecot ready.
user test
+OK
pass testpass
+OK Logged in.
```

中途半端なIPv6対応: 問題の解決: 他サービス

■ SSL/TLS通信のチェック

- https

```
% openssl s_client -connect "[2001:db8::80]:443"  
:  
GET / HTTP/1.1  
host: www.example.jp  
  
HTTP/1.1 200 OK  
:
```

- smtp, pop, imap等は2種類のハンドシェーク

- ✓ いきなりSSL/TLS開始
- ✓ plaintextで接続し、STARTTLSコマンド開始

```
% openssl s_client -connect "[2001:db8::25]:25"  
  
% openssl s_client -connect "[2001:db8::25]:25" -starttls smtp  
  
% openssl s_client -connect "[2001:db8::25]:110"  
  
% openssl s_client -connect "[2001:db8::25]:110" -starttls pop3
```

新しいglibcに起因する問題

新しいglibcに起因する問題

3) データセンタ、サーバ構築における IPv6トラブルシューティング

株式会社ビーコンエヌシー 國武功一さんのコマ
で!

ULAのリーク問題

ULAのリーク問題

- ULA: ユニークローカルIPv6ユニキャストアドレス
 - RFC 4193
 - ローカルで自由に利用できるアドレス帯
 - 識別子をランダムな値とし、異組織間での重複を低減
 - fd80::/8, fc00::/8 (予約)
- ローカルアドレス
 - RFC 1918と同様に、インターネット上での到達性がない
 - グローバルに経路広告してはいけない
 - ✓ 実際にはULAアドレスの経路が観測されている
 - ✓ ULA in the wild / IEPG Meeting – July 2013 @ IETF 87
 - ✓ <http://www.iepg.org/2013-07-ietf87/1%20-%20ULA%20in%20the%20wild.pdf>
 - インターネット上に公開している権威DNSサーバでホストするゾーン内のRRとして書いてはいけない

IPv4アドレス生表記

IPv4アドレス生表記

- URLにIPv4アドレス入れたものをハードコードしている場合
 - ex. <http://192.0.2.10:8080/>
- IPv6 onlyの環境では何らかの問題が出る
- 解決方法: I-Dでの提案
 - <http://tools.ietf.org/html/draft-osamu-v6ops-ipv4-literal-in-url-00>
 - 生IPv4 URLには、ブラウザでMagic Wordを補完
 - ✓ ex. <http://192.0.2.10.TLD:8080/>
 - ✓ ex. <http://192.0.2.10.host:8080/>
 - ✓ ex. <http://192.0.2.10.dns64:8080/>
 - DNS検索させて解決

SMTP関連の問題

Gmail 逆引き

- GmailへのIPv6でのSMTP接続時、DNSチェックされるように
 - 2013/8末頃～
 - チェック内容
 - ✓ 接続元のIPv6アドレスにPTRを要求
 - ✓ PTRで得られたドメインを再度正引き
 - ✓ 接続元IPアドレスが得られるかどうか?
 - チェックに通らないとメールを受信してくれない
 - <https://support.google.com/mail/answer/81126>
- 解決策
 - メールサーバのIPアドレスについて、逆引きを設定する
 - メール送信トランスポートにはIPv4を優先する
 - 逆引き設定されているメールサーバに送信してもらう
 - ✓ Submission等

まとめ

- IPv6もIPv4と同じレベルで計画、運用しましょう
 - おかしな設定は他山の石として
 - IPv6を使う人達は増えてきてます

- 「あるある」ネタを見つけたら教えてください
 - みんなで幸せになりましょう

Q & A

- ご清聴ありがとうございました。

参考資料

参考資料

- IW2013 他にもIPv6関連のセッションが数多くあります
- 過去のInternet Weekページ
 - <https://www.nic.ad.jp/ja/materials/iw/>
 - 資料等豊富にあります
- 日本政府組織のIPv6対応状況調査
 - <http://www.attn.jp/ipv6status/jp/go/>
- IPv6 Deployment Status
 - <http://www.vyncke.org/ipv6status/detailed.php?country=jp>