# 国内IPv6対応サービス状況チェックで発見された事例について

2014/7/11

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

# 目次

# はじめに

IPv4のアドレス在庫が枯渇し，IPv6の導入が世界的に進んでいる．日本国内においても，コンシューマ向けのIPv6サービスが始まるなど，一般ユーザがIPv6インターネットに接続できる環境が整い始めている．また，省庁のWebサービスを始め，サーバサービスのIPv6対応も進み始めた．

IPv6普及・高度化推進協議会 IPv4/IPv6共存WG IPv6導入時に起因する問題検討SWGでは，これらサービスの対応状況について，調査を実施してきた．本文書では，調査時に発見された事例を元に，サーバサービス等，外部公開サービスをIPv6に対応させる際に注意すべき点について報告する．

# IPv6普及状況とサービス実装の必要性

2011年4月頃より，コンシューマ向けのIPv6サービスが開始されており，ISPによる対応（新規ユーザに対するIPv6ディフォルト化，既存ユーザのIPv6化）が進行している．2013年後半の普及状況は以下の通りである．今後，ユーザサイド，サーバサイドともにIPv6対応が進展し，IPv6によるアクセスが急増することが想定される．

## ISPによる対応状況

■ フレッツ光ネクストのIPv6普及率

| | NGN IPv6普及率 | NGN契約数 |
|---|---|---|
| 2012.12 | 0.8% | 8,127,000 |
| 2013.03 | 1.4% | 8,595,000 |
| 2013.06 | 2.0% | 9,094,000 |
| 2013.09 | 2.5% | 9,506,000 |
| 2013.12 | 2.7% | 10,741,000 |
| 2014.03 | 3.2% | 11,301,000 |

注：実際の普及率よりも値が低く出る（算出方法（2）参照）

参考）フレッツ光ネクスト以外のネットワークのIPv6普及率

| | KDDI au ひかり | ctcコミュファ光 |
|---|---|---|
| 2012.12 | 55% | 24% |
| 2013.03 | 61% | 29% |
| 2013.06 | 63% | 36% |
| 2013.09 | 65% | 40% |
| 2013.12 | 66% | 44% |
| 2014.03 | 67% | 48% |

http://v6pc.jp/jp/spread/ipv6spread2013_03.phtml

## Google サーバへのトラフィック状況（国内）

| 順位 | ISP | IPv6率 |
|---|---|---|
| 1 | KDDI | 13.90% |
| 2 | SoftBank BB | 2.54% |
| 3 | ctc | 35.96% |
| 4 | So-net | 2.84% |
| 5 | Sony Global Solutions | 99.36% |
| 6 | IIJ | 2.02% |
| 7 | iTSCOM | 4.74% |
| 8 | bit-drive | 8.39% |
| 9 | TDNC | 4.11% |
| 10 | BIGLOBE | 0.51% |

2014.4.23 Google提供

# 典型的な事例とその影響

IPv6対応サービスの増加に伴い，不具合も散見されるようになって来た．問題として，以下のようなものが観測されている．

- DNS設定の不具合
  - 場合によっては，DNSによる名前解決に失敗し，サービスにアクセスできない
- Web サービスの不具合
  - IPv6でのアクセスに失敗する場合がある

これらの不具合はIPv6に特化したものではないが，結果として，「IPv6を導入することにより不具合が発生した」，「IPv6普及時には，サービスへのアクセスが少ない等の理由で不具合の発見が遅れた」ということになる可能性がある．詳細については次頁以降で紹介する．

# 不具合事例の記述形式

- 不具合の事例は，以下の様式にて記述する.
  - 事例：発生していた事象の具体的内容について記述する.
  - 想定される影響：本事象が原因で起こり得る不具合について記述する.
  - 検証方法：事例が発生していることの確認方法の例を記述する.
  - その他：関連事項を記述する.

# 不具合の事例1

- 事例
  - ネームサーバのグルー(glue) AAAA のIPv6アドレスと，ゾーンファイル中のAAAAレコードのIPv6アドレスが違っている.
    - レジストリ等，上位ドメインの DNS への登録情報と，権威サーバでの設定情報が整合していない.
  - 本事例は，IPv4のみの環境でも同等のことが発生しうる.
- 想定される影響
  - ネームサーバ のグルーに書かれているDNSサーバにアクセスできない場合，当該ドメインと通信できない可能性がある（実装に依存）.
  - ドメイン乗っ取りの原因になる可能性がある.
- 検証方法（例）
  - http://dnscheck.jp/ によりチェックする .
- その他
  - IPv6導入時，グルーレコードや，権威サーバの情報にAAAAアドレス記述が追加されることがある. この場合，整合性を取るべき情報が増えること，IPv6普及段階では，追加した情報に対するアクセスが少なく，結果として不具合の発見が遅れることなどが想定される.

# 不具合の事例2

- 事例
  - NSとして9つのFQDNが設定されており，そのうちの2つに対し，設定されているIPv6アドレスへのクエリに対して返答がない．
  - 9つのFQDNのうち，1つにはIPv4でのクエリにも返答無し
  - その他にも，DNSの設定的に，以下の問題があるように見受けられた．
    - 特定のDNSサーバに AAAAレコード を問い合わせると Authority section に NS として 別のサーバが返ってくる。この サーバ に対して問い合わせると A は値を返し、HINFO, TXT, MX, NS などは REFUSED となり、AAAA, A6 はNOERRORとなる．
- 想定される影響
  - DNSのクエリに時間がかかる．
  - DNSが引けない可能性がある．
- 検証方法（例）:
  - （DNSへの疎通性確認）ping6/ping コマンド による確認
  - (DNSチェック) http://dnscheck.jp による確認, DNS 関連コマンド (nslookup, host, dig等) を利用したチェック

# 不具合の事例3-1

- 事例
  - レジストリに登録されているグルーにはAAAAレコードがあるが，ゾーンデータには，AAAAレコードが登録されていない.
- 想定される影響
  - ネームサーバのグルーに書かれているDNSサーバにアクセスできない場合，当該ドメインと通信できない可能性がある（実装に依存）.
  - ドメイン乗っ取りの原因になる可能性がある.
- 検証方法（例）:
  - (DNSチェック) http://dnscheck.jp による確認

# 不具合の事例3-2

- 事例
  - ICMPv6パケット過大メッセージをサーバが受け取れず，パスMTU探索が動作しないため，クライアント側で，IPv6トランスポートによりコンテンツが受信できない．
    パスMTU探索が動作しないケースとして，以下が存在する．
    - 経路上のファイアウォールにて，ICMPv6がフィルタされている．
    - 経路途中のルータが，レートリミットにより，ICMPv6を生成できない．
    - IPS,UTMの設定により，ICMPv6パケットが破棄される*1.
- 想定される影響
  - IPv6にて，web サーバに接続はできるが，ブラウザに依っては，IPv4にフォールバックせず，コンテンツが表示できない場合や，表示完了まで多大な時間がかかることがある．
- 検証方法（例）:
  - クライアント側のMTU値を 1,280 オクテットに変更し，コンテンツが正常に取得できれば，パスMTUが動作していない可能性があることが確認できる．
  - ping6 等で，パケット長を調整し，返答の有無をチェックする．
  - tracepath6 等のツールを利用し，途中経路のMTU値を確認する．
- その他
  - パスMTU探索が必要となるのは，すべてのユーザとは限らないため，影響をうけるユーザと影響を受けないユーザが混在することに注意する必要がある．
  - パスMTU探索には，方向性が存在する．Web等の場合と，メール等の場合には，方向が逆なので注意が必要である．

*1: 以下のような事例が報告されている．
[ScreenOS] Large Size ICMP Packet (size > 1024) in IPv6 environment.
http://kb.juniper.net/InfoCenter/index?page=content&id=KB26473&actp=RSS

# 不具合の具体例4

- 事例
  - 複数のDNS権威サーバ間で応答が整合していない*1.
    - IPv6でアクセス可能なサーバとIPv4でアクセス可能なサーバでゾーンファイルが異なっており，NSレコードや，SOAレコードが一致していない.
    - IPv6アドレス（AAAAレコード）の問い合わせ（IPv4/IPv6トランスポートどちらでも）に対して返答するものと返答しないものが混在している
- 想定される影響
  - 本事象は，IPv6でのDNSクエリにはAAAAレコードを，IPv4でのDNSクエリにはAレコードを返答することを目的として設定されている環境かと想定される. しかしながら，一般的に，A，AAAAレコードのクエリと，クエリのトランスポートは一致しない. また，キャッシュサーバが，IPv4/IPv6どちらでクエリを出すか制御できない. このため，クライアント側がIPv6環境でも，IPv6サーバにアクセスできない可能性がある.
- 検証方法（例）
  - (DNSチェック) http://dnscheck.jp による確認，DNS 関連コマンド (nslookup, host, dig等)を利用したチェック

*1 JANOG32 LT: http://www.janog.gr.jp/meeting/janog32/program/hennav6.html

# 不具合の具体例5

- 事例
  - DNSサーバやWebサーバにて，IPv4 でアクセスした際とIPv6 でアクセスした際に，得られるコンテンツが違う.
- 想定される影響
  - DNSの場合には，本事象は，IPv6でのDNSクエリにはAAAAレコードを，IPv4でのDNSクエリにはAレコードを返答することを目的として設定されている環境かと想定される．しかしながら，一般的に，A，AAAAレコードのクエリと，クエリのトランスポートは一致しない．また，キャッシュサーバが，IPv4/IPv6どちらでクエリを出すか制御できない．このため，クライアント側がIPv6環境でも，IPv6サーバにアクセスできない可能性がある.
  - Webコンテンツの場合，IPv4サーバとIPv6サーバでコンテンツを別々に管理している際，片方のコンテンツ更新を失念し，意図しないコンテンツが表示される，ということがある.
- 検証方法（例）
  - コンテンツの確認の際，両方のプロトコルでチェックを実施する.
    - DNSの場合には，権威サーバ（セカンダリサーバを含む）に対し，直接両プロトコルでアクセスして検証する必要がある.

# 最後に

- 観測された事象は，IPv6における問題というよりは，DNS の設定不具合が多く見られた.
- IPv6を導入する際に，既存システムとの整合性を考えた設計，導入後の統合的な試験が必要だと思われる.

# 参考1:有用なURL

DNSの設定不具合をチェックできるサイト

- http://dnscheck.jp/

# 参考2： telnet コマンドを利用した動作確認の例

サービスごとの動作確認例を示す. アンダーラインの行が入力行となる.

SMTP（port 25/tcp)

```
% 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.
```

http（port 80/tcp)

```
% 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
         :       :
```

Pop（port 110/tcp)

```
% 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.
```

# 参考3： openssl コマンドを利用した動作確認の例

アンダーラインの行が入力行となる.

■ 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
```