DNS逆引き登録は必要か?

藤崎 智宏
NTT情報流通プラットフォーム研究所

本発表の趣旨

(特に) IPv6インターネットにおいて，DNSの逆引き登録が必要かどうかに関し，議論したい

本発表の流れ

1. 逆引きDNSに関する議論の経緯
2. 準備
   - DNSの正引きと逆引き
   - IPv4インターネットでの逆引き利用
3. 逆引きDNSに関する規約の現状
4. IPv6における逆引きの問題点
5. 逆引きDNS WGにおける議論の紹介
6. IPv6オペレーション研究会での意見
7. 御意見募集

逆引きDNS議論の経緯

第2回JPNICオープンポリシミーティング
IPv6 での逆引きの必要性に関して問題提起

JPNICよりIPv6オペレーション研究会に，「IPv6インターネットにおいて，DNSの逆引き登録の必要性」について検討依頼

IPv6オペレーション研究会 ＤＮＳ逆引きWG※にて議論

IPv6オペレーション研究会にて議論

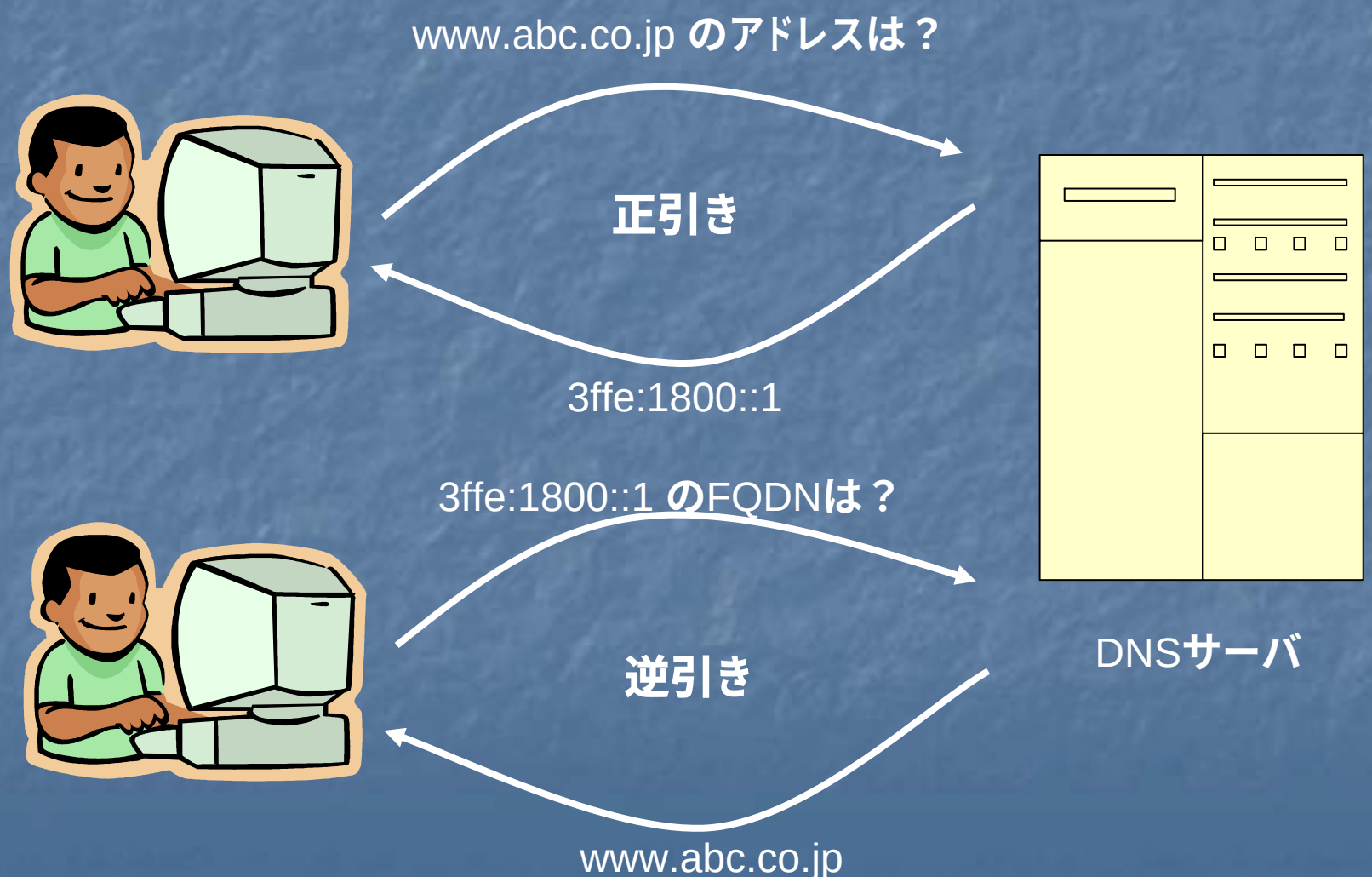
JPNICへ答申

ＪＡＮＯＧで議論（本日）

ＲＩＲポリシ等への反映

※　http://www.bugest.net/ipv6-ops/rdns/

DNSの正引きと逆引き



IPv4における逆引きの利用

- 簡易な認証として利用
  - 逆引き登録のないホストへのアクセス制限
  - Double reverse (正引き，逆引き一致)チェック
- 逆引きした情報の利用
  - アドレスの，地理的な場所の推定に利用
- IPアドレス情報の見やすさ向上
  - 各種log，traceroute 等
- アクセスリスト等の記述
  - DNSを利用したIPアドレス群のグルーピング
    - ISP等で，不連続CIDRブロックを一括

逆引きに関する規約の現状 その1

- 逆引きに関連する規約（IPv4）
  - RFC2050

    5. In-ADDR.ARPAドメインの管理
       - 地域レジストリは、ISPに対して発行したアドレスの上位ブロック、あるいは/16以下のプリフィックス長のCIDRブロックについてのみ、INADDR.ARPAレコードを管理する責任を負う。ローカルIRやISPで/16以下のプリフィックスを有するものは、顧客のIN-ADDR.ARPA資源レコードをすべて管理する責任を負う。特定のISPと関係のないネットワークに関するIN-ADDR.ARPA資源レコードは、引き続き地域レジストリが管理する。

  - JPNIC IPアドレス割り当て等に関する規則

    第21条 (IP指定事業者の義務)

    3 IP指定事業者は、別に定める手続にしたがい逆引きのためのネームサーバの設定、管理および運用を行わなければならない。

逆引きに関する規約の現状その2

- JPNICにおけるアドレス空間ポリシ
  - 7.18. in-addr.arpa資源レコード維持の責任

    /24よりも小さな割り当てに関しては、IP指定事業者は顧客のネットワークに関するin-addr.arpa資源レコードを維持しなければならない。

- 逆引きに関する規約（IPv6）
  - IPv6 Address Allocation and Assignment Policy
    - 5.6. 逆引き

      RIR/NIRは、IPv6アドレス空間を組織に委譲するとき、割り振られたIPv6アドレス空間に対応する逆引きルックアップゾーンを管理する責務も委譲する。各組織はその逆引きルックアップゾーンを適切に管理する。アドレスの割り当てを行なう際、組織は、割り当てられたアドレスに対応する逆引きルックアップゾーンを管理する責務を、要求に応じて割り当て先の組織に委譲しなければならない。

以上，http://www.nic.ad.jp の資料より抜粋

IPv6における逆引きの問題点 その1

- ネットワークに繋がる機器が膨大な数になる
  - 手動管理はスケール的に困難
  - ISPでの代行コストが高くなる
    - とにかくアドレスが長い．．．

例：IPv6の逆引きゾーンファイル

```
;
; Example PTR Record File
;
$ORIGIN e.f.f.3.ip6.int.
9.6.e.5.9.7.e.f.f.f.7.2.0.9.2.0.1.0.0.0.0.0.0.0.1.1.8.1   IN   PTR     pisces.nttv6.net.
d.0.2.1.c.d.e.f.f.f.9.c.0.a.2.0.0.0.0.0.0.0.0.0.1.8.1     IN   PTR     aries.nttv6.net.
9.2.2.1.c.d.e.f.f.f.9.c.0.a.2.0.0.0.0.0.0.0.0.0.1.8.1     IN   PTR     cancer.nttv6.net.
6.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f.f.f.0.0.0.0.1.8.1   IN   PTR     virgo.nttv6.net.
9.7.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.5.0.0.0.0.0.0.0.1.8.1   IN   PTR     virgo.nttv6.net.
7.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f.f.f.0.0.0.0.1.8.1   IN   PTR     paix.nttv6.net.
5.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f.f.f.0.0.0.0.1.8.1   IN   PTR     cancer.nttv6.net.
2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f.f.f.0.1.8.1   IN   PTR     cancer.nttv6.net.
```

間違えない方がおかしい？

IPv6における逆引きの問題点 その1

- ネットワークに繋がる機器が膨大な数になる
  - 手動管理はスケール的に困難
  - ISPでの代行コストが高くなる
    - とにかくアドレスが長い．．．
- Unmanaged network が増える
  - そもそもDNSサーバをどこに置いて誰が管理するのか
  - データが信頼できるのか

IPv6における逆引きの問題点 その2

- 一時アドレス（temporaryアドレス）の存在
- アドレスブロックが大きく，決まっているためグルーピングが楽
- draft-itojun-jinmei-ipv6-issues-00.txt

1.1. Reverse mapping of IPv6 addresses

前述のいくつかの内容，及びip6.int. と ip6.arpa.移行問題等逆引きが不整合を起こす等より，逆引きを前提とすることをやめるようにすべき　（藤崎 意訳）

IPv6オペレーション研究会
～逆引きDNS検討WGでの議論～

- *Reverse DNS WG メンバ*

斎藤和典	*ニフティ*
中原一彦	*日本電気*
長島朋英	*日本テレコム*
山崎俊之	*NTTコミュニケーションズ*
猪俣 彰浩	*富士通*
荒野 高志	*インテックネットコア*
近藤 邦昭	*インテックネットコア*
藤崎 智宏	*日本電信電話*

逆引きDNS検討WGでの議論

逆引き必要派

- どこから通信が来ているか，ということを知りたいのは自然．数字の羅列を意味のある文字(所属を示す文字列)に直せた方が直せないよりはよい．
- 将来的に，逆引きを利用したアプリケーションが出てこないとも限らない．
- 仕組み/プラットフォームとしては残すべき
- 実際問題として，逆引き出来ないとアクセスを許さないサーバが存在する．
- 管理の時等，オペレーションの簡略化(アクセスリストなど)、見易さ　(Traceroute など)

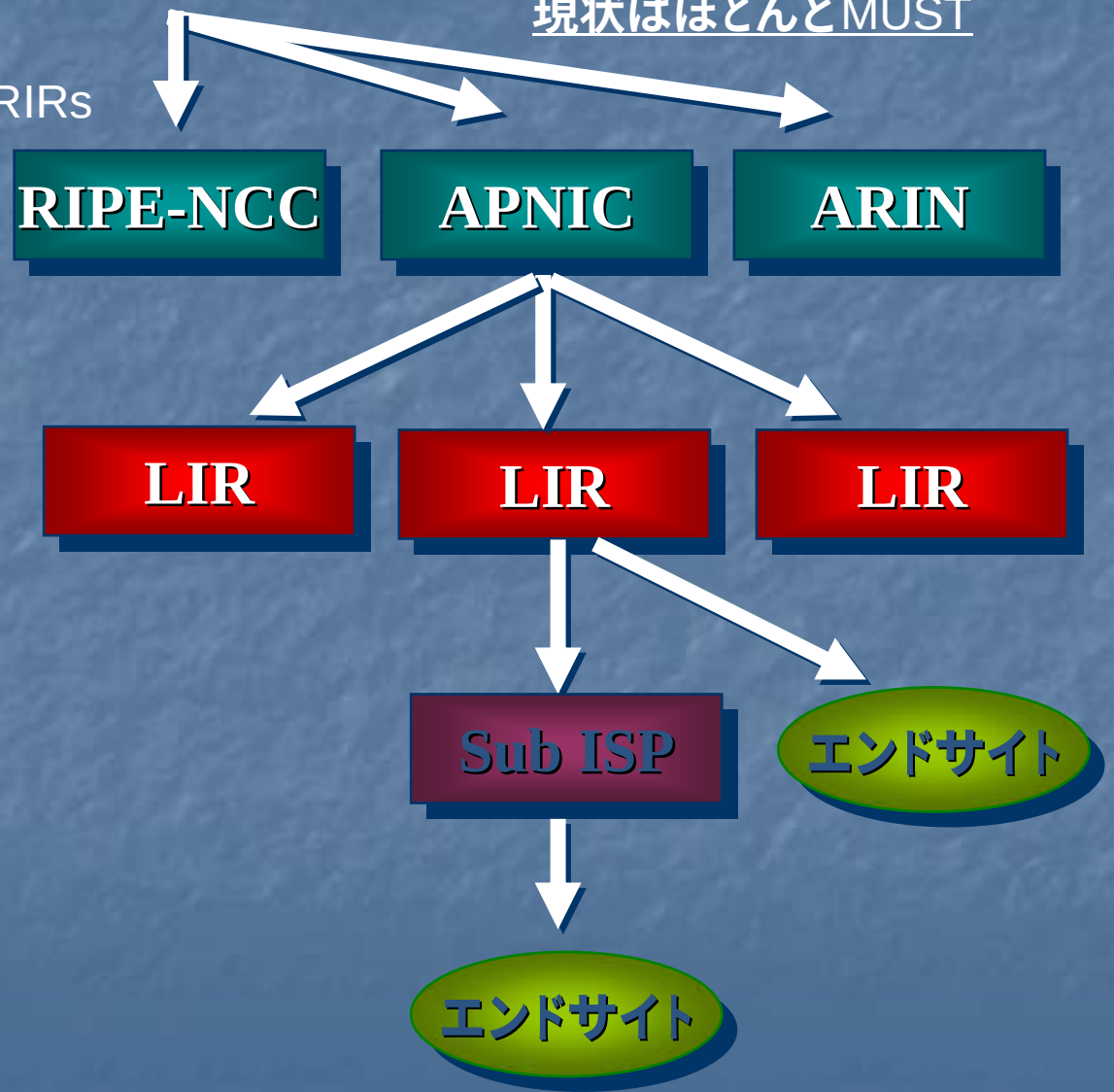
逆引き不必要派

- IPv6では，アドレスの階層構造が固定なので，アドレスの出元はある程度 はっきりする．Whois等もある．
- ホームネットワークなど，管理者のいないネットワークが増えてくることを考えると，逆引きを登録するのはほぼ不可能(一時アドレスなんてのもある)．
- 逆引きは，fake 出来るし，セキュリティを高めることにはならない．
- 現状，ISPとして「義務化」している．なければもっとサービスを安くできる．

必要性は低いが、必要でないともいいきれない．義務化ではないが、利用できる枠組みは残すべき．

DNS逆引きの現状改訂

現状はほとんどMUST



DNS逆引きWGでの改訂議論のポイント

① RIR からLIRへの委譲

② LIRからsub ISP／エンドサイトへの委譲

③ sub ISP からエンドサイトへの委譲

④ エンドサイトのレコード登録
（ISPインフラはエンドサイト相当

逆引きの必要性 その1

① RIRからLIRへの委譲
- MUST：RIRは選択できない

② LIRからsub ISP／エンドサイトへの委譲
- MUST派
  - SHOULDにするとなし崩し的に逆引き機構自体がなくなりそう
- SHOULD派
  - LIRは選択可能.
  - サービスとして逆引き無し（その分安い）とかもありでは？

③ Sub ISPからエンドサイトへの委譲
- LIRが責任をもって規定（約款等で規定）

逆引きの必要性 その2

④ エンドユーザでの逆引きレコード登録

- MUSTは事実上不可能だろう
  - Unmanaged networkが増えてくる
- SHOULD派
  - ここで推奨しないと誰も登録しない
- OPTIONAL派
  - 過去の経緯から，SHOULDはMUSTに近い意味合いがある．ISPが肩代わりすることになったら管理のコストが大きい．
  - プライバシの問題で，登録したくない場合もある．

IPv6オペレーション研究会
～IPv6 Opsミーティング (2002.9.27) での意見～

- 現状，既にIPv4でも認証に使われていない．ISPとしてはコスト面からもない方がよいと思う．ただ，traceroute 等では別に工夫が必要．ISPとしてはお客様から要求されたらやらなければならないというのは葛藤．結局，エンドユーザマター．

- 大学として，IPv4だとNATのアドレスで済むので登録はOKだが，これが学内全部，となると不可能．DDNS等の仕組みが必要．今は導入していない．

- 逆引きも，DNS Sec が普及すれば貴重な機能になる．ISPの仕組みとしてはないと困るのでは．

IPv6オペレーション研究会
～IPv6 Opsミーティング (2002.9.27) での意見～

- P2P通信の時には，相手をホスト名で指定．正引きは必要なので逆引きも 欲しい．VoIP 等のアプリケーションでは，発信元を表示するようなことを したい．必須ではないが，なくなると困る．
  - アドレス，というものをお客様に認識させたくないため，逆引きが欲しい．
  - リナンバリングを行なう際にも逆引きがあった方が便利．
  - ホームユーザに対してのアドレスの隠蔽は必要．
- アプリケーションとして必要な例はあるので仕組みは残しておくべき．P2Pの例等があがっているが，何らかの形でアドレスからFQDN等に変換出来ればいいのでそれがDNSである必要はないのでは．

- 来場者の投票:
  エンドユーザはDNS登録を
  - SHOULD: 3～4名
  - OPTIONAL: たくさん
  - なくてもいい: 0名
- ISPはDNSの委譲を
  - MUST: 15名
  - SHOULD: 20名

中・長期的な解として・・・

- DDNS関連技術
- Use of ICMPv6 node information query for reverse DNS lookup
  - draft-itojun-ipv6-nodeinfo-revlookup-00.txt
- DNSへの機能追加
  - プロバイダが容易に代行できるような機構

御意見をお願いします．