WHOISを地域拠点とconnectして冗長化してみた話
～ 君の名(前解決)は ～

一般社団法人日本ネットワークインフォメーションセンター
塩沢　啓

JANOG 45@札幌 (2020/1/24)

目次

- はじめに
  - WHOISの地域拠点を作って冗長化してみた
- 地域拠点のWHOISに切り替えて、試験提供してみた
  - 切り替え方法の検討
  - DNSラウンドロビン＋Aレコード、AAAAレコードの切り替え
- 試験提供の結果と、ディスカッション

目次

- はじめに
  - WHOISの地域拠点を作って冗長化してみた
- 地域拠点のWHOISに切り替えて、試験提供してみた
  - 切り替え方法の検討
  - DNSラウンドロビン＋Aレコード、AAAAレコードの切り替え
- 試験提供の結果と、ディスカッション

WHOISの地域拠点で冗長化？

- 2019年以前

```
$ dig @8.8.8.8 whois.nic.ad.jp A
....
;; ANSWER SECTION:
whois.nic.ad.jp.        18      IN      A       192.41.192.40
....
```

- 2019年某日

```
$ dig @8.8.8.8 whois.nic.ad.jp A
....
;; ANSWER SECTION:
whois.nic.ad.jp.        18      IN      A       192.41.192.40
whois.nic.ad.jp.        18      IN      A       58.84.254.30
```

WHOISの地域冗長化にむけた取り組み

- 今までIPレジストシステムは東京複数拠点＋APNICで運用
- 以前から地域冗長化に向けて検討してきた
- 2019年、 ENOG(Echigo Network Operators' Group)さんにご協力いただき、 Echigo IXに地域拠点の新潟WHOISを構築
- 東京WHOISから新潟WHOISに切り替えて、 WHOISサービスを試験提供してみた

今回の発表について

- 新潟に地域拠点のWHOISを作って冗長化した話

- 東京WHOISから新潟WHOISへ切り替えて、試験提供した
  → DNSラウンドロビン＆A/AAAAレコードを切り替え
  →うまく切り替わったが、わずかにアクセスが残った

- 新しいサービスへの切り替えはどうすればいいか、
  みなさんの知見やアドバイスを聞きたい！

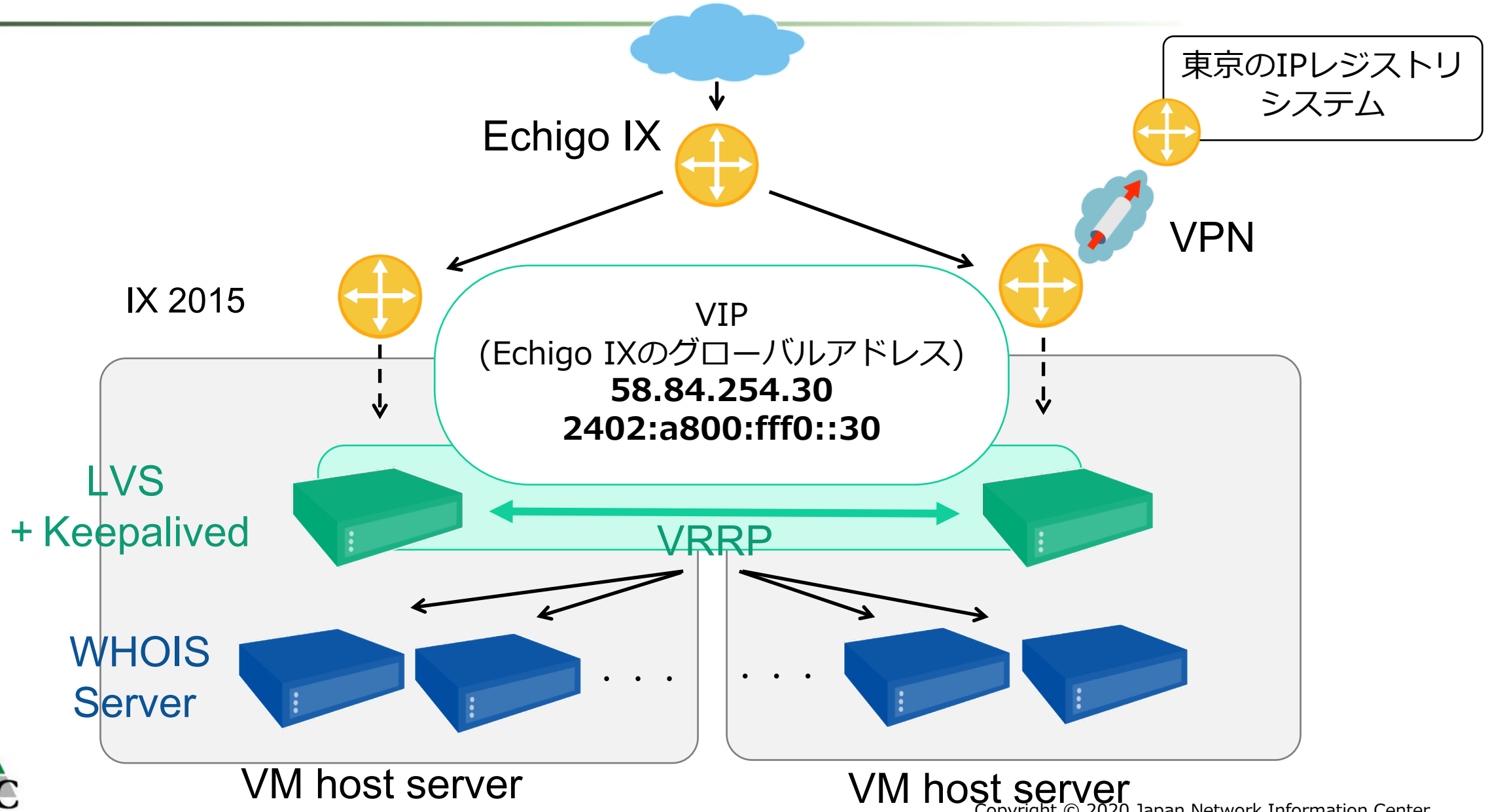
目次

- はじめに
  - WHOISの地域拠点を作って冗長化してみた

- 地域拠点のWHOISに切り替えて、試験提供してみた
  - 切り替え方法の検討
  - DNSラウンドロビン＋Aレコード、AAAAレコードの切り替え

- 試験提供の結果と、ディスカッション

地域拠点の新潟WHOISを作ってみた



新潟WHOISで試験提供してみよう！

2019年7月31日

各位

一般社団法人日本ネットワークインフォメーションセンター(JPNIC)

【重要】8月のシステムメンテナンスに伴うサービス停止のお知らせ

JPNICでは、 下記の日程でIPアドレス・AS番号に関する申請処理システムおよびJPNIC資源管理認証局システムのメンテナンスを行います。

メンテナンス期間中は、IPアドレスに関する申請システム、 逆引きDNSに関する情報の更新およびWHOISサービスが停止いたします。

この期間の前後で、申請等を予定されている方は、 下記の内容をいまいちどご確認くださいますようお願いいたします。 皆様にはご迷惑をおかけいたしますが、ご理解とご協力をお願い申し上げます。

記

メンテナンス日時

2019年8月9日(金) 18:00 ～ 13日(火) 10:00

昨年のお盆にDCの引越しで、東京WHOISが停止。
この間、新潟WHOISを試験提供してみることに！

東京WHOISから新潟WHOISへ切り替えるには？

- どうやって切り替えるか…
  - 今回の条件 → 新潟WHOISのIPアドレスは、Echigo IXのグローバルアドレス
- ルーティングで切り替え
  - BGP Anycastは無理か。。JPNICに吸い込んで新潟にトンネル？
- DNSで切り替え
  - 別のURLで提供か
  - DNSラウンドロビンとAレコードの切り替えか
    - DNSを引かずにIPアドレス直打ちのクエリが一定数存在する？
    - TTLを無視するフルリゾルバサーバがある？

切り替え方法の比較

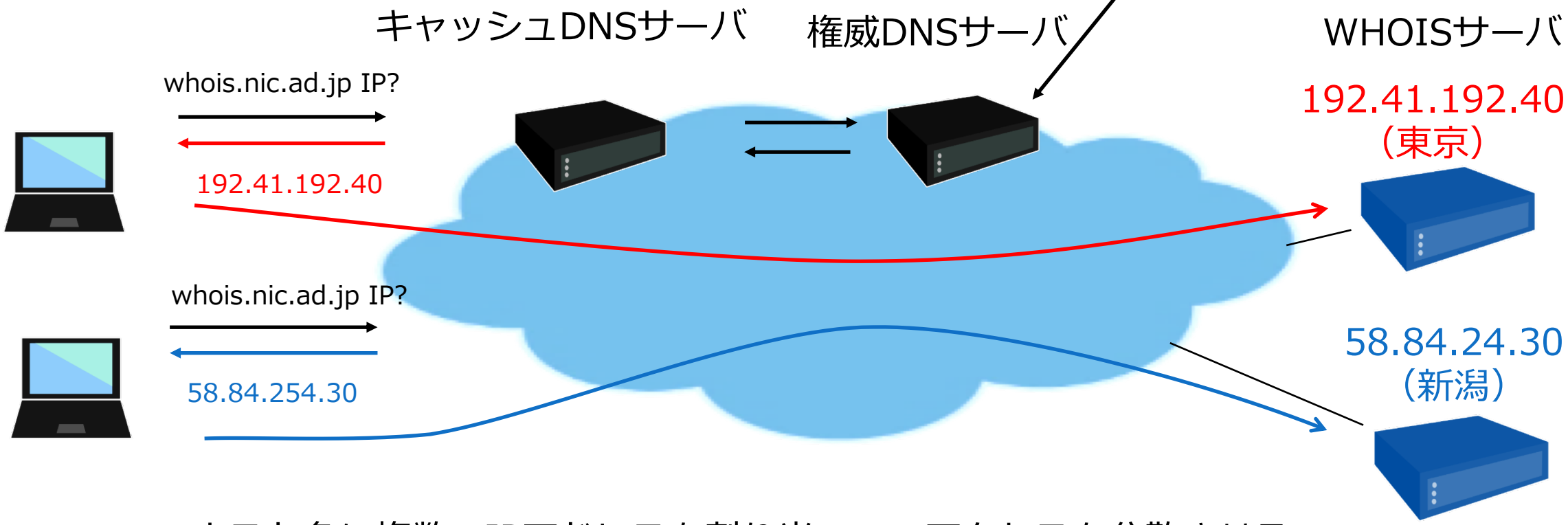
No.	切り替え方法	導入は簡単か	冗長性	DNSを引かずにIPアドレス直打ちのクエリ
1	BGP Anycast	× 新潟WHOISはEchigo IXのIPアドレス	○	○ 救える
2	JPNICへ吸い込み、新潟へトンネル	○	× JPNICのASが死んだらアクセスできなくなる	○ 救える
3	別URLでの提供	△ 既存のURLを引き続ける人には影響が発生	○	△ 救えない
4	DNSラウンドロビン＋Aレコードの切り替え	○ ゾーンファイルの設定変更のみ。ただし、キャッシュDNSサーバのTTLによる待ち時間あり	○	△ 救えない

→ No.4 が有効な方法か検証！

DNSラウンドロビンとは…

ゾーンファイル

```
whois.nic.ad.jp   60  IN  A  192.41.192.40    # 東京
whois.nic.ad.jp   60  IN  A  58.84.24.30      # 新潟
```



ホスト名に複数のIPアドレスを割り当てて、アクセスを分散させる。
導入は比較的簡単だけど、厳密に制御すると難しい

試験提供にむけたゾーンファイルの変更

- 8月1日　TTL 900 → 60 に変更

```
whois.nic.ad.jp   60  IN  A  192.41.192.40
```

- 8月5日　新潟WHOISのＡレコードを追加

```
whois.nic.ad.jp   60  IN  A  192.41.192.40
whois.nic.ad.jp   60  IN  A  58.84.254.30
```

- 8月7日　東京WHOISのＡレコードを削除
  → 新潟WHOISのみで試験提供

```
whois.nic.ad.jp   60  IN  A  58.84.254.30
```

- 8月9日-10日　DCの引越しで東京WHOIS停止
- 8月19日　東京WHOISのAレコード復活

```
whois.nic.ad.jp   60  IN  A  192.41.192.40
whois.nic.ad.jp   60  IN  A  58.84.254.30
```

- 8月21日　新潟WHOISのＡレコード削除→試験提供終了！

```
whois.nic.ad.jp   60  IN  A  192.41.192.40
```

試験提供期間

試験提供にむけたゾーンファイルの変更

```
$ dig @8.8.8.8 whois.nic.ad.jp A

; <<>> DiG 9.9.5-3ubuntu0.18-Ubuntu <<>> @8.8.8.8 whois.nic.ad.jp A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6863
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;whois.nic.ad.jp.               IN      A

;; ANSWER SECTION:
whois.nic.ad.jp.        18      IN      A       192.41.192.40
whois.nic.ad.jp.        18      IN      A       58.84.254.30

;; Query time: 4 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Mon Aug 05 19:01:14 JST 2019
;; MSG SIZE  rcvd: 60
```


試験提供で確認したいこと

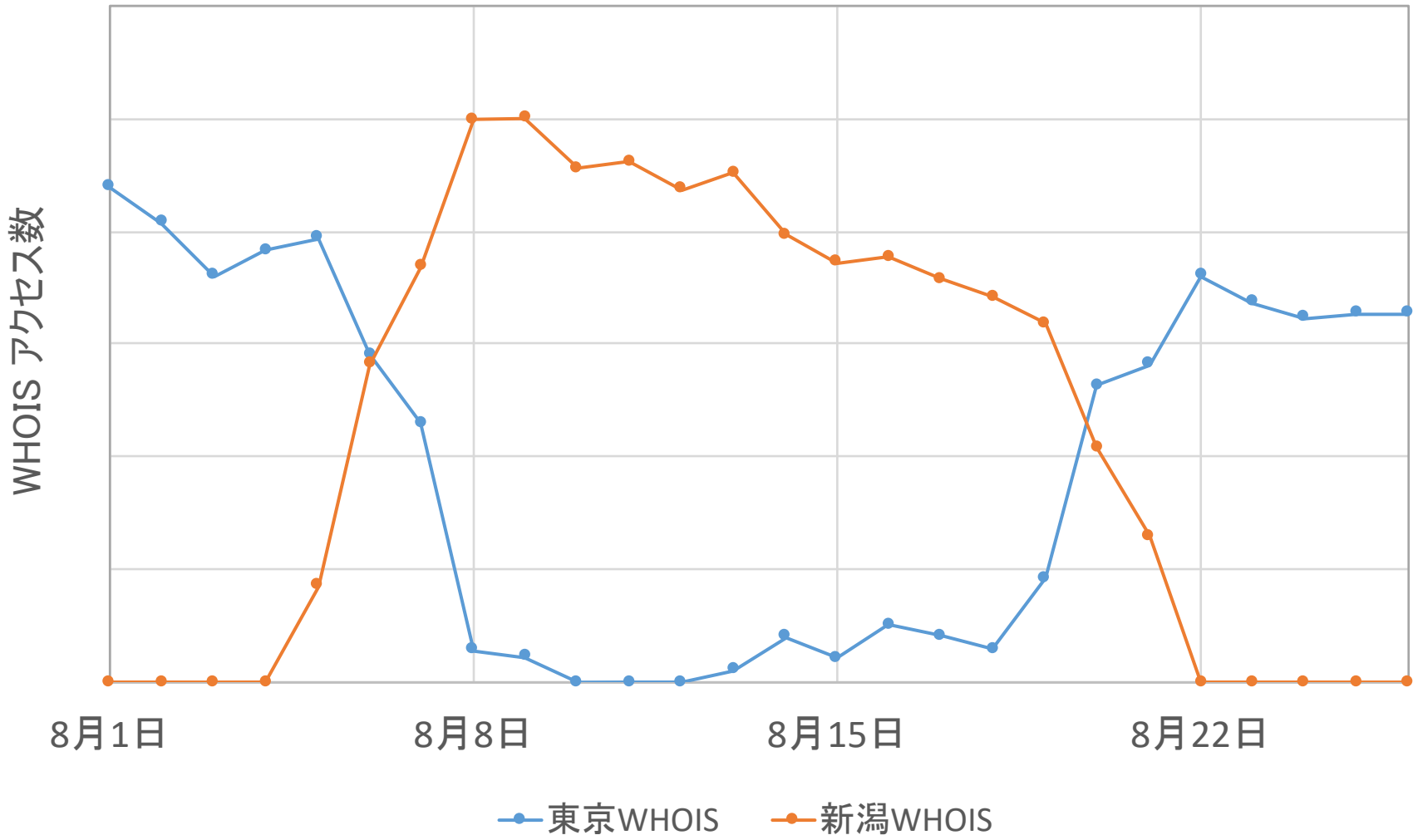
DNSラウンドロビン＋Aレコード切り替えは有効な方法？

Aレコード切り替え前後のアクセス傾向から以下を確認する！

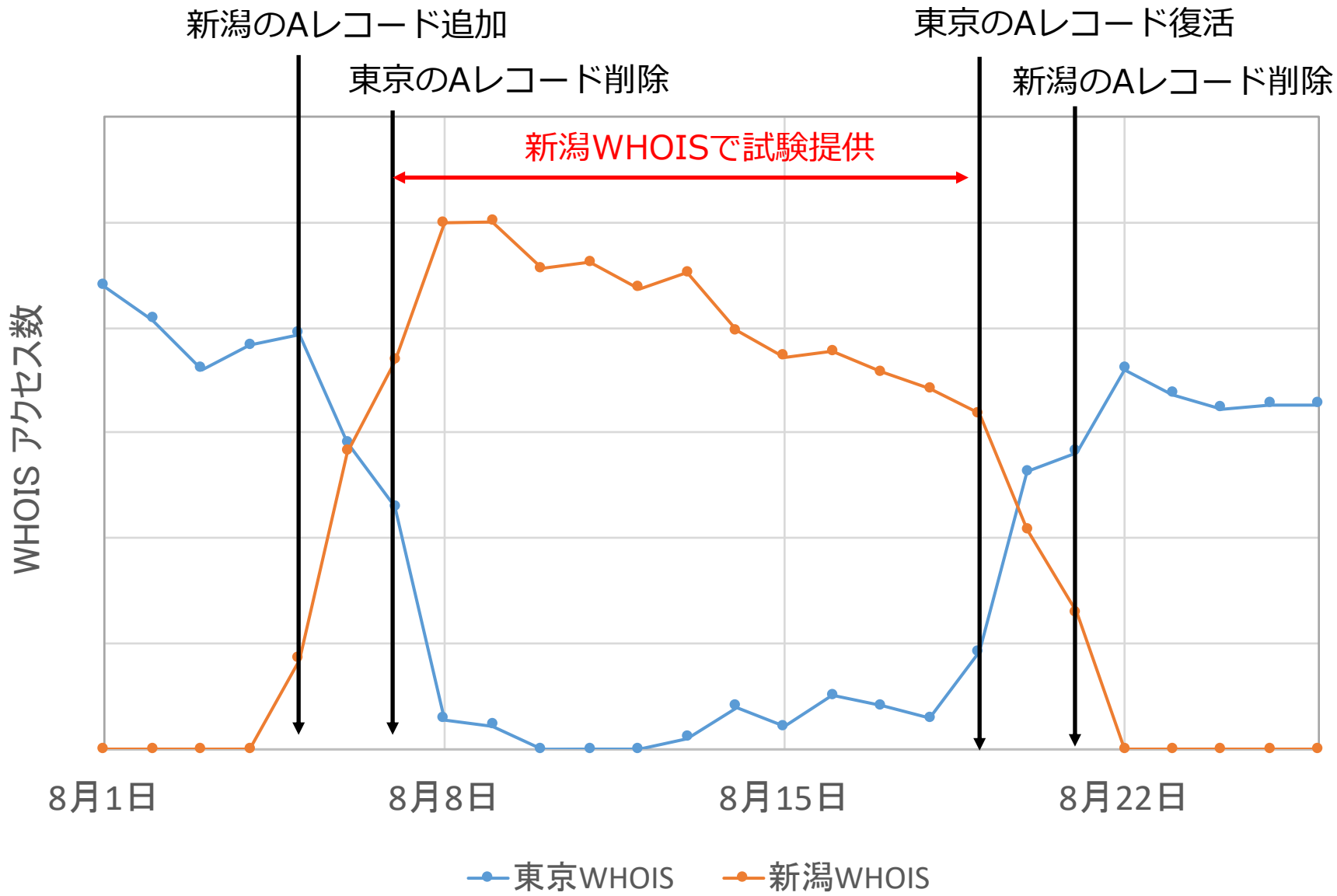
1. DNSを引かずIPアドレス直打ちのアクセスがどの程度存在するか

2. TTL を短くしてもフルリゾルバサーバでTTLを曲げてアクセスする人がどの程度存在するか

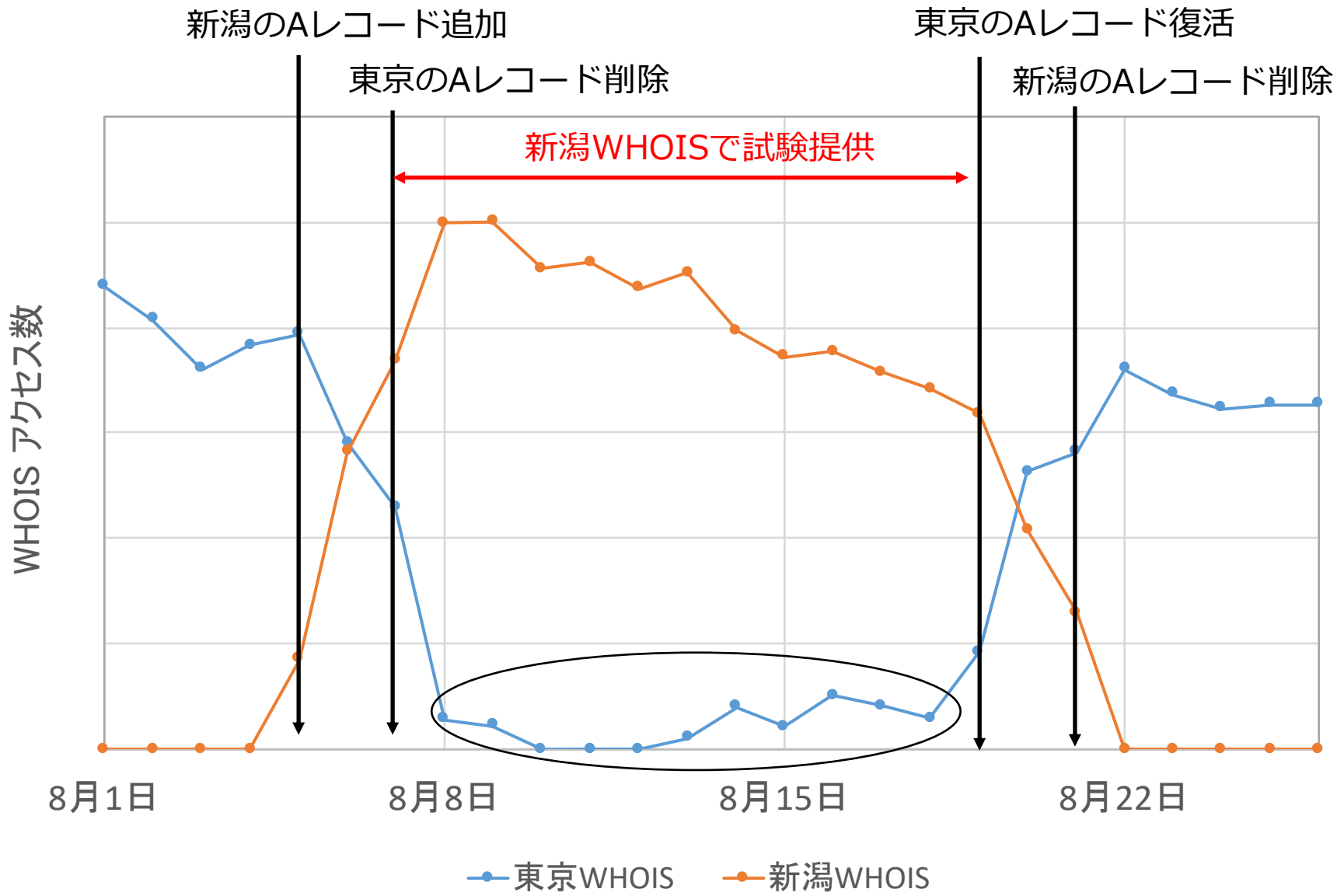
WHOISアクセス数の推移



WHOISアクセス数の推移



WHOISアクセス数の推移



東京のWHOISへアクセスが一定数残る

- IPアドレス直打ちのアクセス or TTLを無視したアクセスか???
- アクセスログを見てみると、、、

```
・・・・
2001:xxxx: xxxx::1    ext    [07/Aug/2019 21:30:03]  none ...
2001:xxxx: xxxx::1     ext    [07/Aug/2019 21:30:12]  none  ...
2001:xxxx: xxxx::1     ext    [07/Aug/2019 21:30:16]  none ...
・・・・
```

- ほとんどがIPv6からのアクセスだった
- 今回の試験提供で、新潟WHOISはIPv4のみでしたorz

→つまり、　Aレコード：新潟WHOIS

AAAAレコード：東京WHOISのまま

→その結果、IPv6のアクセスは全て東京WHOISへ…

試験提供　再チャレンジ

- 期間　10月7日～10月30日
- 今度は新潟WHOISもIPv4とIPv6も対応済み！
- 切り替え方法　DNSラウンドロビン+A/AAAAレコード切り替え
- スケジュール

10月8日　新潟WHOISのA/AAAAレコードを追加

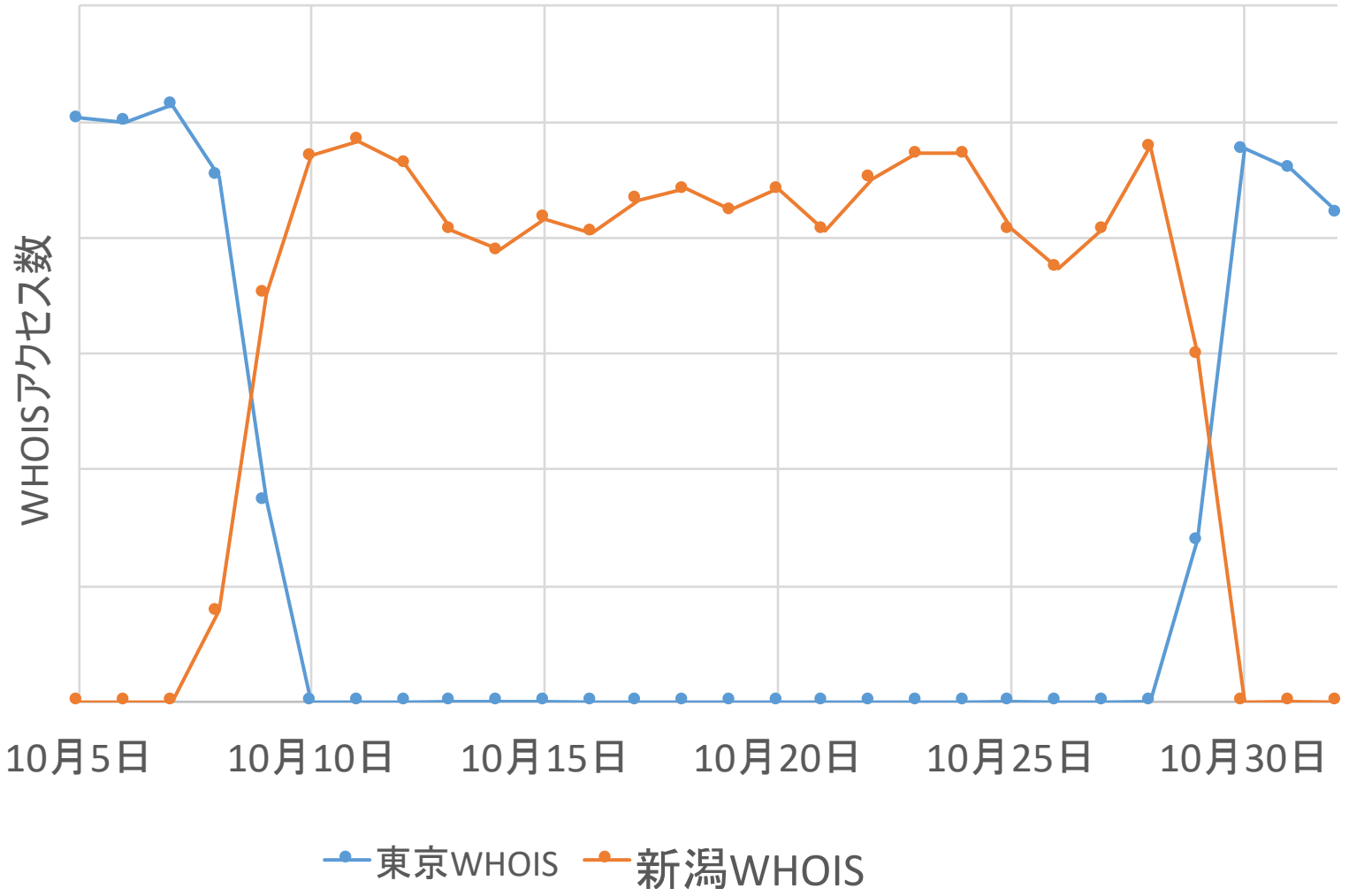
```
whois.nic.ad.jp   60  IN  A     192.41.192.40
whois.nic.ad.jp   60  IN  A     58.84.254.30
whois.nic.ad.jp   60  IN  AAAA  2001:dc2:1000:6000::43
whois.nic.ad.jp   60  IN  AAAA  2402:a800:fff0::30
```

10月9日　東京WHOISのA/AAAAレコードを削除

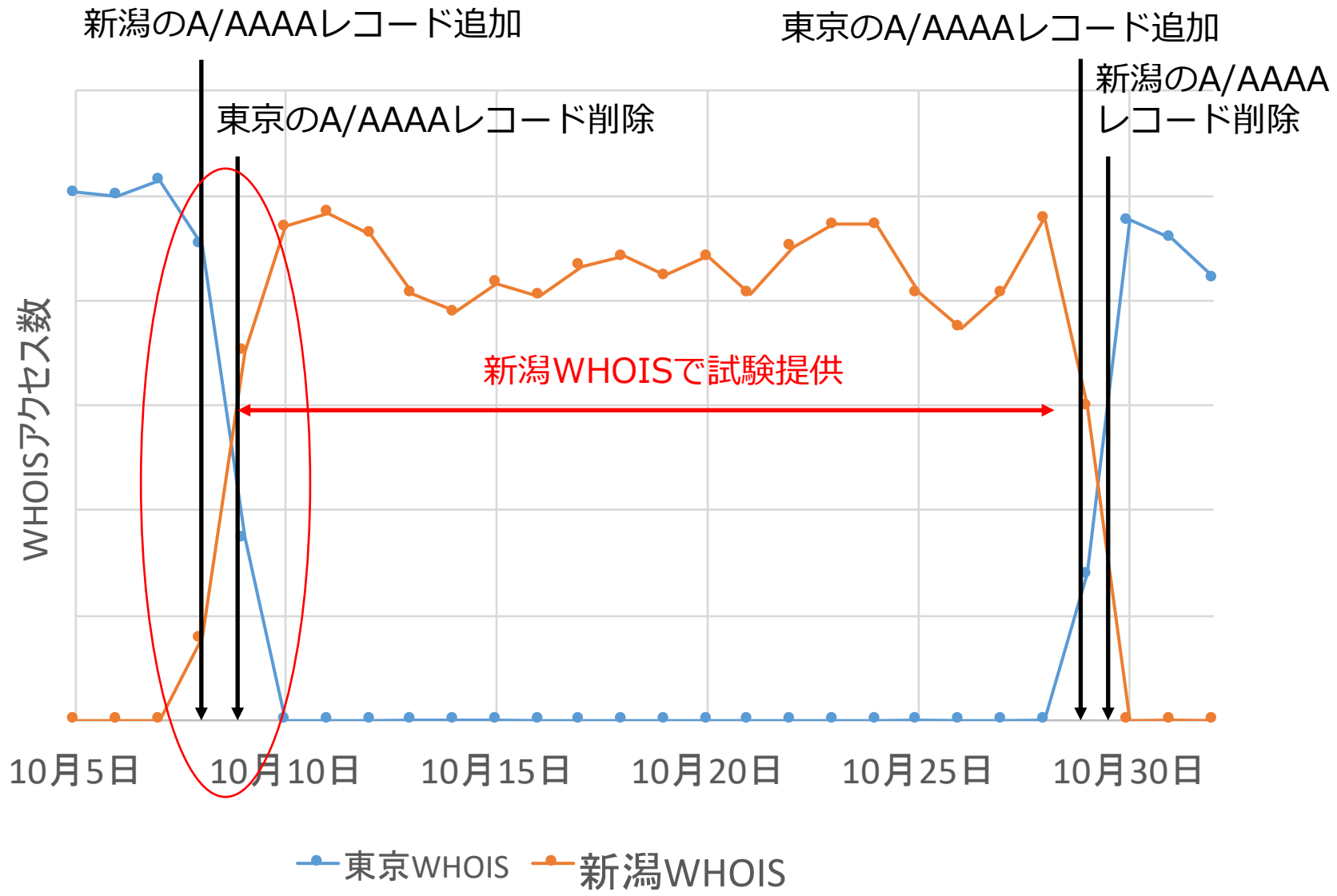
→ 新潟WHOISのみで試験提供

```
whois.nic.ad.jp   60  IN  A     58.84.254.30
whois.nic.ad.jp   60  IN  AAAA  2402:a800:fff0::30
```

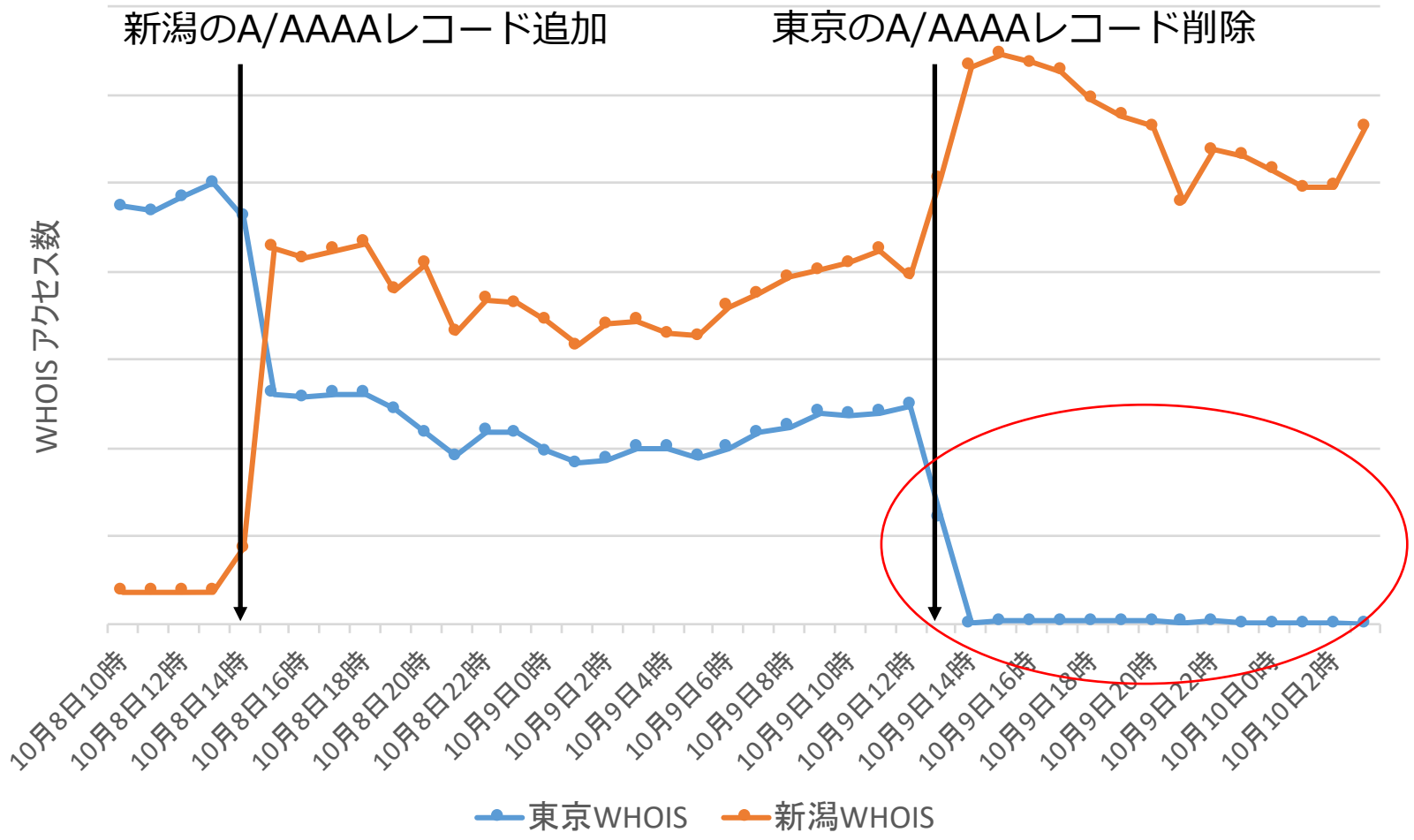

WHOISアクセス数の推移



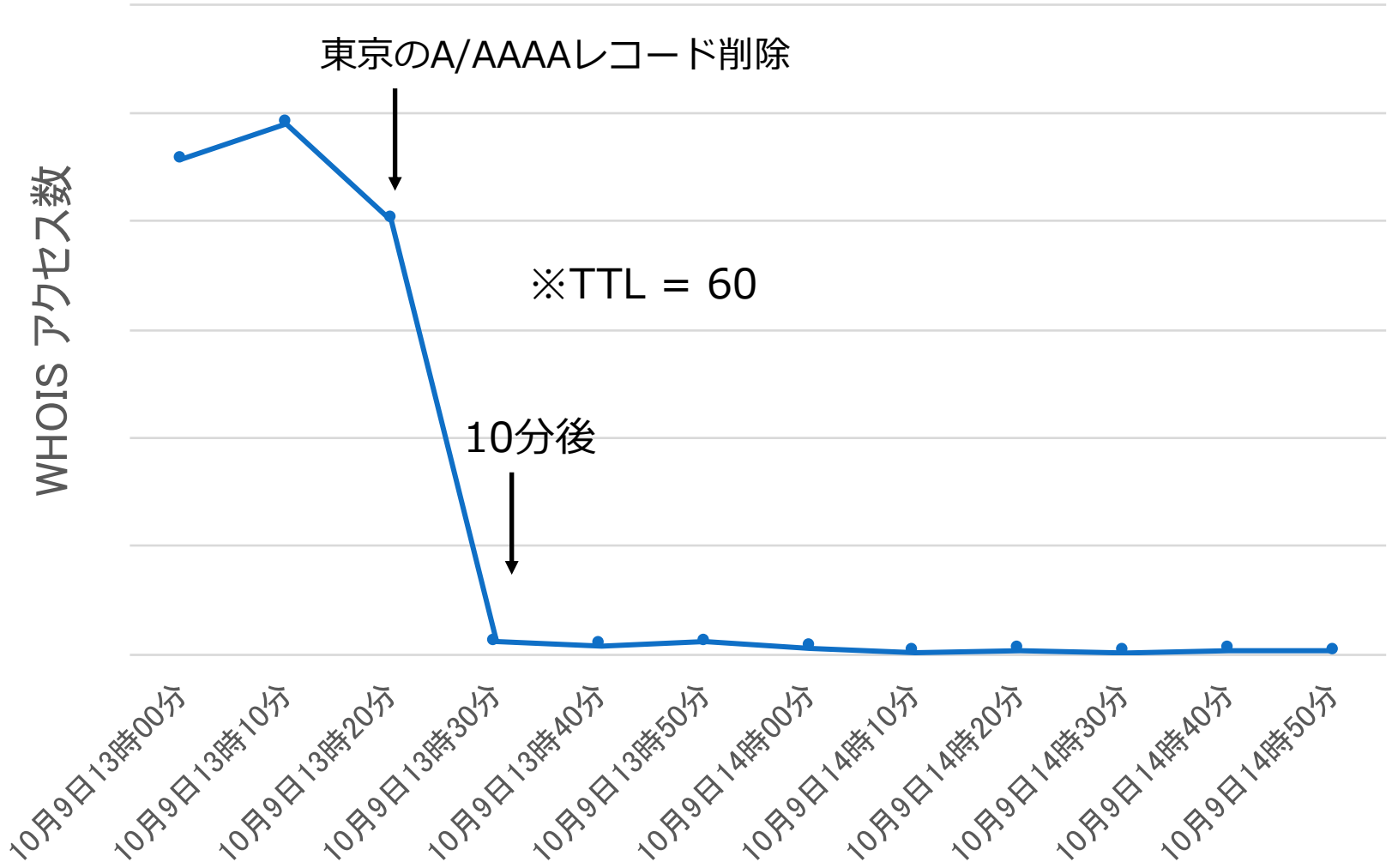
WHOISアクセス数の推移



WHOISアクセス数の推移（1時間毎）



WHOISアクセス数の推移（10分毎）



試験提供の結果

- 確認したかったこと

DNSラウンドロビン＋A/AAAAレコード切り替え後も、IPアドレスの直打ち or TTLの無視で東京WHOISにアクセスする人が存在するかどうか

- TTL=60で切り替えたところ、10分後にはほとんどのクエリが新潟WHOISに向かった

DNSラウンドロビン＋A/AAAAレコード切り替えは、
有効な手段ということがわかった！

東京WHOISへのわずかなアクセス…

- 一方で、切り替え後も、東京WHOISへ最大数10クエリ/時のアクセスが残った…

- 残ったアクセスの傾向
  - ➢ コマンドラインではなく、WEBからのアクセスが多かった
    - WEBブラウザがA/AAAAレコードをTTLを無視してキャッシュ?
  - ➢ ソースIPアドレスは、外資系のクラウド事業者からが多いようだった
    - クラウドのVMからのクエリ？
    - スクリプト次第では切り替え後もアクセスが残ることも考えられる

東京WHOISへのわずかなアクセス…

- 残ったアクセスの傾向（続き）

➢アクセスが残らないスクリプト例

```
#!/bin/sh

while true do;
  whois -h whois.nic.ad.jp 192.0.2.0/e
done
```

➢残る可能性があるスクリプト例

```
#!/bin/sh
HOST=`dig +short whois.nic.ad.jp`

while true do;
    whois -h $HOST 192.0.2.0/e
done
```

➢ ISPのフルリゾルバでTTLを曲げているケースもある？

- 切り替え後も残った人たちを救うべきかどうか….

まとめ

- 新潟WHOISで試験提供を8月、10月に実施
- 切り替えにはDNSラウンドロビン＋A/AAAAレコードの切り替えを採用
  - IP直打ち/TTL無視などによる切り替え後のアクセスはほとんど無く、有効な切り替え方法ということがわかった
  - わずかに残るアクセスをどうするか…

※なお、JPNICはWHOISのログを第三者には一切提供していません。
また、運用上必要なログの管理以上の行為は行っておりません。

みなさん、どうしていますか？

1. 新しいサービスへの切り替え方法
   - どんな方法で切り替えましたか
   - どんなところに気をつけましたか

2. Aレコード、AAAAレコードで切り替えについて
   - レコードを書き換えて、うまく切り替えられる？
     - IPアドレス直打ちする人は最近いない？
     - DNSのお作法を守っている人は多そう
   - 残ったアクセスはどうしていますか

