WHOIS

DNS Summer Day 2017
～DNS気になる話

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)
技術部 澁谷 晃

お話したいこと

レジストリが管理する資源情報を公開するサービスであるWHOISについて、技術的・政策的な観点から抜本的な見直しが進行しています。

本発表にて、次世代WHOISプロトコルと言われるRDAPの規格や実装状況、およびICANNや各インターネットレジストリにおける政策議論の最新動向を紹介させていただきます。

目次

- RDAP
- WHOWAS
- ICANNにおけるWHOISの見直し
- WHOIS登録情報の正確性向上
- (最後に)お知らせ

RDAP(1/5)-イントロダクション

- **RDAPとは**
  - Registration Data Access Protocol
  - RFC7480-7485(2015年)
- **従来使われているWHOIS**
  - 最初の仕様はRFC812 (1982年)
  - port43
  - データのフォーマット無し
  - 登録レジストリがどこかは人手で探索

RDAP(2/5)-特徴

- **HTTP(s)**
- **RESTful**
  - http://[rdap-server]/ip/192.0.2.0/24
  - http://[rdap-server]/autnum/64496
  - http://[rdap-server]/domain/domain.example
- **JSON(後述)**
- **bootstrap(後述)**

RDAP(3/5)-JSON

- **機械可読**
  - 例： https://rdap.apnic.net/ip/202.12.30.0/24 の応答


```
{
 "handle" : "202.12.30.0 - 202.12.30.255",
 "startAddress" : "202.12.30.0",
 "endAddress" : "202.12.30.255",
 "ipVersion" : "v4",
 "name" : "JPNIC-NET-JP",
 "type" : "ASSIGNED PORTABLE",
 "country" : "JP",
 "objectClassName" : "ip network",
 "entities" : [ {
 (以下略)
```

RDAP(4/5)-boot strap service

- **Authoritativeであるリソースの参照場所を示す**
  - 例： http://data.iana.org/rdap/ipv4.json


```
{
   "description": "RDAP bootstrap file for IPv4 address
allocations",
   "publication": "2015-08-11T00:09:31Z",
   "services": [
          (略)
             "202.0.0.0/8",
          (略)
          ],
          [
             "https://rdap.apnic.net/"
          ]
}
```


仮にARINのRDAPサーバー(*)に問い合わせてもAPNICにリダイレクトされて応答

*https://rdap.arin.net/registry/ip/202.12.30.0/24

RDAP(5/5)-サービス状況

- **RIR(地域レジストリ)はサービス提供中**
  - https://rdap.apnic.net/
  - https://rdap.arin.net/
  - https://rdap.db.ripe.net/
  - https://rdap.lacnic.net/rdap/
  - https://rdap.afrinic.net/rdap/
- **APNIC地域のNIR(国別レジストリ)は対応検討中**

WHOWAS(1/3)-概観

- **WHOIS登録情報の過去のデータを閲覧**
- **RIR**
  - ARIN：所定の申請手続を経て閲覧する
    - https://www.arin.net/resources/whowas/
  - RIPE：公開
    - WHOISコマンドで所定のオプションを付ける
      - 例：
      - whois -h whois.ripe.net -- "--list-versions 192.0.2.0 – 192.0.2.255"
      - whois -h whois.ripe.net -- "--show-version rev# 192.0.2.0 – 192.0.2.255"
      - 参考：https://labs.ripe.net/Members/kranjbar/proposal-to-display-history-of-objects-in-ripe-database

WHOWAS(2/3)-APNIC

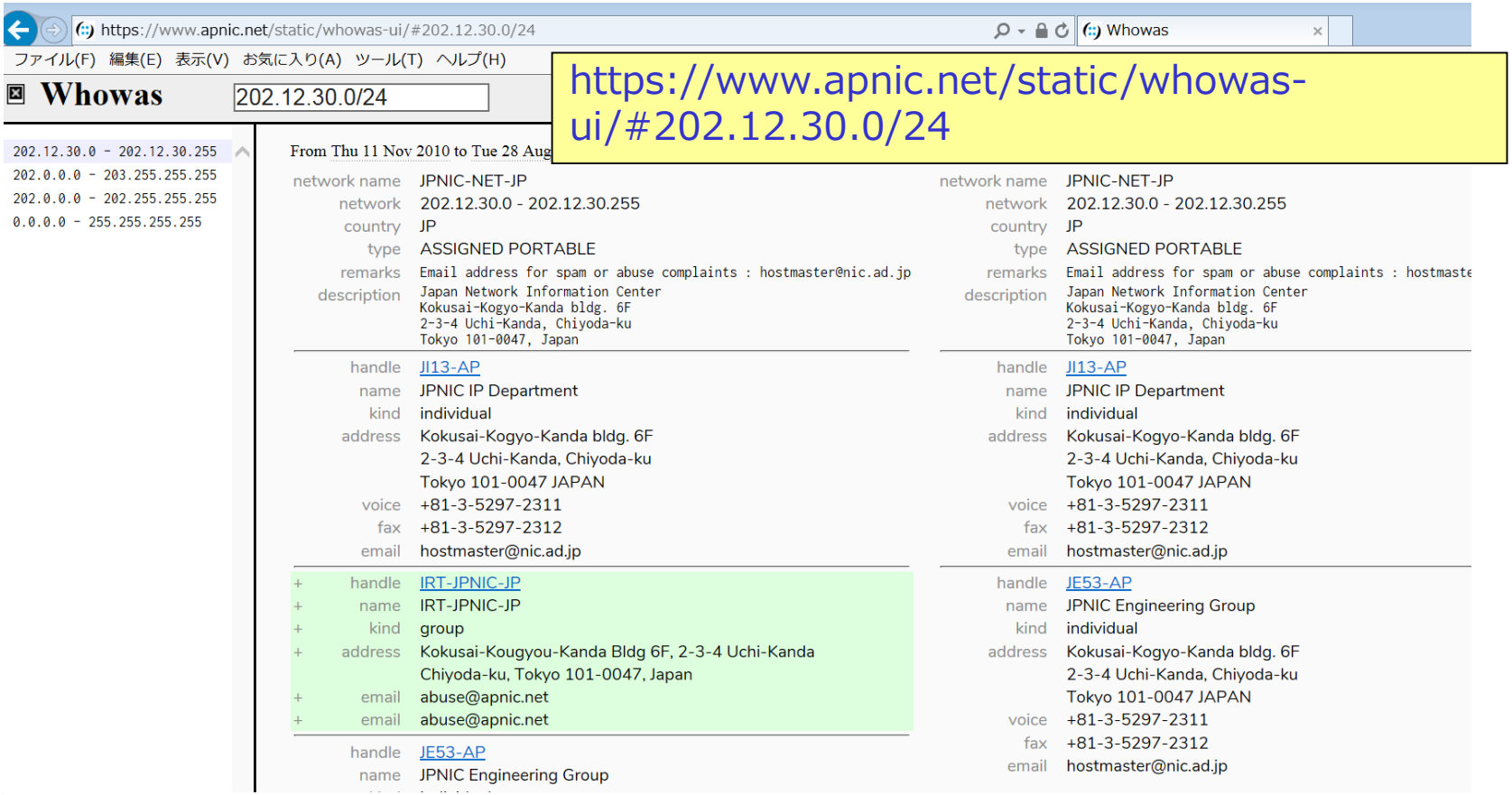
- APNIC：RDAPを応用したサービスとして開発・試験公開中
- historyを付けたURLでアクセス
- 例:
  - http://rdap.apnic.net/history/ip/202.12.30.0/24


```
{
"applicableFrom": "2010-11-11T07:00:02Z",
"applicableUntil": "2012-08-28T08:00:01Z",
{
    "label": "Kokusai-Kogyo-Kanda bldg. 6F¥n2-3-4
Uchi-Kanda, Chiyoda-ku¥nTokyo 101-0047
JAPAN"
}
}
```


JPNICオフィス移転(2012年)より前の住所

WHOWAS(3/3)-APNIC(続き)

- **APNIC WHOWASのWeb UI**
  - https://www.apnic.net/static/whowas-ui/



ICANNにおける(ドメイン名)WHOISの見直し(1/3)-タイムライン

- **WHOISの抜本的見直し(タイムライン)**
  - 2009年10月：AoC(責務の確認)中の重要責務の１つ　にWhoisポリシーが掲げられる
  - 2010年9月：Whoisポリシーレビューチーム(RT)が発足
  - 2012年5月：WhoisポリシーRTが最終報告書を公表
  - 2012年12月：gTLDディレクトリサービス専門家作業部会(EWG)設立
  - 2014年6月：EWGが最終報告書提出
  - 2015年5月：理事会発議によりPDP(Policy Development Process)が開始
  - 2016年1月：GNSO RDS PDP作業部会(WG)設立

ICANNにおける(ドメイン名)WHOISの見直し(2/3)-現在のPDP検討状況

- **PDP作業部会の検討**
  - フェーズ1：ポリシー要件の策定
    - 今はこのフェーズにあり、以下の2つの問いに関するコンセンサスを得ようと試みている
    - gTLD登録データに関する基本的な要件は何か
      - 少なくとも次の点を検討：利用者および目的および付随するアクセス、正確性、データ要素、プライバシー要求
      - データ要素については、まずは「最小限の公開データ集合」について検討中(後述)
    - 基本的要件を満たすために新たなポリシーの枠組みが必要かどうか
      - 必要な場合、何の分野横断的な要件を扱うのか
      - 不要な場合、現在のWHOISポリシーに関する枠組みは効率的に基本的要件を扱っているか
  - フェーズ2：策定されたポリシーの基本設計
  - フェーズ3：設計されたポリシーの実装検討

ICANNにおける(ドメイン名)WHOISの見直し(3/3)-PDP検討状況補足

- **当初は「最小限の公開データ集合」に絞り検討**
  - 最小限の公開データ集合＝Thinレジストリ(.com, .netなどの登録者情報を持たないレジストリ)がWHOISで表示する情報

例：

Domain Name:	EXAMPLE.TLD
WHOIS Server:	whois.example.tld
Referral URL:	http://www.example.tld
Updated Date:	2009-05-29T20:13:00Z
Creation Date:	2000-10-08T00:45:00Z
Registry Expiry Date:	2010-10-08T00:44:59Z
Sponsoring Registrar:	EXAMPLE REGISTRAR LLC
Sponsoring Registrar IANA ID:	5555555
Domain Status:	clientDeleteProhibited
Name Server:	NS01.EXAMPLEREGISTRAR.TLD
Name Server:	NS02.EXAMPLEREGISTRAR.TLD
DNSSEC:	signedDelegation

WHOIS登録情報の正確性向上(1/5)-法執行機関からの問題意識

- **2016年秋頃から、警察機構(例：EUROPOL/FBI)が世界各地域のコミュニティにて登壇・議論**
  - ARIN/RIPE/APNIC/JPOPM(後述)
- **発表内容**
  - WHOISは、公安・犯罪対応に利用
  - データが不正確（特に二次割り振り）

WHOIS登録情報の正確性向上 (2/5)-RIRにおける議論

- **ARIN：**
  - ARIN39 (2017年4月)
  - 具体的な提案が議論されている（後述）
- **RIPE：議論中**
  - RIPE74(2017年5月)
  - 具体的な提案は無く、今後対策をコミュニティと共に検討したいと呼びかけ
- **APNIC：議論予定？**
  - APNIC44(2017年9月)

WHOIS登録情報の正確性向上 (3/5)-ARIN会議のポリシー提案

- **現状**
  - 年に一度全POCに電子メールを送信し、登録情報の正確性確認を実施
  - 60日以内に確認がとれないもの、またはARIN職員が不正確と判断したものはその旨WHOISで表記
  - ただし、歴史PIの登録情報の正確性が特に課題
- **提案**
  - 確認日(毎年1月1日)と対象となるPOCを明記
  - Admin、Tech、NOC、Abuse
  - 90日を越えても反応がない情報は、十分な分析と調査のうえ、invalidとマーク
  - 当該情報から参照される資源のレンジを逆引きから外し、公開WHOISから外す(ARIN内では情報保持)

http://www.jpopf.net/JPOPM32Program?action=AttachFile&do=view&target=2-4-2_WHOIS_oktani_2.pdf　より

WHOIS登録情報の正確性向上(4/5)-ARIN会議参加者の反応

- **趣旨に大筋賛成で好意的**
  - 法執行機関もコミュニティの一員
  - 法執行機関が(規制ではなく)コミュニティでの提案プロセスへ参加していることを評価
  - FBI担当者(10年以上ARINに参加)によると実際、規制の話も内部で出ているとのこと
- **ただし、登録情報の削除は効果が薄いうえに問題を悪化させるとして反対意見多数**
  - 代案として課金による罰則案
  - 事業者への課金のタイミングで情報更新を促す案
- **歴史的PI、IPv4とIPv6を分けて考えた方がよく、長期的にはIPv6が重要になってくるだろう**

http://www.jpopf.net/JPOPM32Program?action=AttachFile&do=view&target=2-4-2_WHOIS_oktani_2.pdf　より

WHOIS登録情報の正確性向上 (5/5)-JPOPMでの議論

- **JPOPM31 (2016/11/30)**
  - FBIからの説明
    - WHOISの公安目的利用：サイバー犯罪対応
    - 登録情報の正確性
    - 不正確な登録情報による捜査活動への影響
  - 会場・ip-usersMLでの議論
    - 登録のあり方の見直しを促す案
    - 一定期間以上更新されていない情報にマークをつけ正しくない可能性があることを示す案
- **JPOPM32 (2017/06/21)**
  - Whois登録情報正確性向上に関するパネルディスカッション
    - 今後、継続して議論

(最後に)お知らせ

- **JPNICのlameチェック調査時の問い合わせ先アドレス変更について**
  - これまでの調査対象
    - 登録[IPネットワークアドレス](逆引きゾーン)が
      - IPv4アドレスであれば登録[ネームサーバ]のIPv4アドレス
      - IPv6アドレスであれば登録[ネームサーバ]のIPv6アドレス
  - 2017年7月13日以降
    - 調査対象の逆引きゾーンがIPv4アドレスかIPv6アドレスかのいずれに関わらず、登録 [ネームサーバ]に問い合わせた際に応答のあるIPv4/IPv6アドレス共に調査
  - 参考
    - https://www.nic.ad.jp/ja/topics/2017/20170627-01.html
    - https://www.nic.ad.jp/ja/dns/lame/transport.html

参考資料集

- **(本文中に掲げたものの他)**
- **JPNIC Blog :: RDAP ～次世代WHOISプロトコル～ の紹介**
  - https://blog.nic.ad.jp/blog/rdap-intro/
- **ICANN報告会資料**
  - https://www.nic.ad.jp/ja/materials/icann-report/

ご静聴ありがとうございました