

# WHOIS登録情報 正確性向上を取り巻く議論

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  
インターネット推進部・IP事業部 奥谷泉

# WHOISと法執行機関を取り巻く現状

- WHOISは主にNW上の問題解決の為の利用想定
- **法執行機関もサイバー犯罪捜査に利用**
  - NW上の問題解決の一環
  - JPNIC・RIRも、情報開示について定義・公開している手続きの範囲内で登録情報の情報開示に協力
  - RIRは法執行機関との協力関係の構築・維持を重視
- **現在ドメイン名の gTLD WHOISの抜本的改定  
→ 法執行機関による利用も考慮**
  - ICANN 「Next-Generation gTLD Registration Directory Services to Replace Whois」 PDP WG

# WHOIS登録情報の正確性向上検討

- 2016年秋、法執行機関が、全RIR地域での提案意向を発表
- **APNIC42**
  - スリランカ警察 + FBI(リモート)が発表
  - Public Safety and Accuracy of IP Address WHOIS
    - <https://conference.apnic.net/42/program#/schedule/day/7>
- **JPOPM31**
  - FBIより発表・課題共有
    - <http://jpopf.net/JPOPM31Program>



FBI Jesse Schibilia氏

# JPOPM31でのFBIによる説明

- **WHOISの公安目的利用：サイバー犯罪対応**
  - その他ツールも利用しているが第一ステップとしてはまずをWHOISで確認
- **登録情報の正確性**
  - 特にLIR(IP指定事業者)を介した、二次ISPへの分配に関する登録情報の正確性が課題
  - エンドユーザを特定できる必要はなく、上流ISPが正確に特定できればよい
- **不正確な登録情報による捜査活動への影響**
  - 正しい上流ISPを特定できないと情報開示請求・捜査令状の取り直し等、捜査活動に遅延を及ぼす
  - 人命に関わり、迅速な対応が必要な事件での不正確なWHOIS登録情報の影響は深刻

# JPOPM31・ip-usersでの議論

- **登録のあり方の見直しを促す案**
  - 法執行機関対応に特化した連絡先情報登録案
  - 公開情報と法執行機関向けに提供する連絡先情報を分けることを検討するべき
  - IRRやPeering DB等、情報更新を行うインセンティブのある情報とセットで検討するべきではないか
- **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**
  - その上で一定の割合以上にマークのついている割り当て情報を管理している組織への通知や、ペナルティ等の対応も検討できるのでは

# その後の動向

---

- **ARIN39(2017年4月)、RIPE74(2017年5月)で議論**
- **ARIN39: Draft Policy ARIN-2017-3: Update to NRPM 3.6: Annual Whois POC Validation**
  - [https://www.arin.net/vault/participate/meetings/reports/ARIN\\_39/ppm.html](https://www.arin.net/vault/participate/meetings/reports/ARIN_39/ppm.html)
- **RIPE74: WHOIS Accuracy and Public Safety - Update**
  - <https://ripe74.ripe.net/archives/#thu>



# ARIN会議での提案

## • 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)

# ARIN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**



# RIPE会議での発表

## • 問題提起

- RIPE NCCとLIRは契約関係にあり、LIRに関する情報更新は担保できる仕組み
- 一方、二次ISPに関する登録情報の正確性を維持を遵守する仕組みが充分ではない
  - RIPE NCCはLIRに正確な登録情報維持を求めている
  - しかし、二次ISPは情報変更をLIRに通知せずとも困らない
- 捜査協力を求める国を特定するうえで、登録情報の「国」はどう登録するべきか
  - NW運用者、分配先、委託先
- 他、基本的背景は、JPOPMで紹介した内容と共通

## • 今後



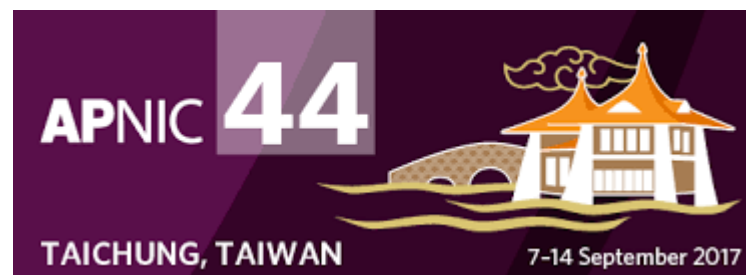
具体的な提案はなく、今後対策をコミュニティと共に検討したいと呼びかけ

# RIPE参加者の反応

- **法執行機関の需要に応じてWHOISの改定を求められることへの疑問**
  - WHOISの利用対象に法執行機関は想定していない
  - 技術者向けでも正確性維持に苦勞している中、法執行機関の需要に応えるのはさらに敷居が高い
  - 二次ISPの登録情報の正確性の問題は認識しているが、対応のモチベーションがなく解決策がない
- **WHOISに頼る対策が現実的ではないとの姿勢**
  - より適切な検索方法があるのでは(Traceroute、BGP)
  - 誰もが利用できる方法の必要性を発表者は反論
- **一方、法執行機関vs技術コミュニティのような態度はよくないとの意見もあった (少数派)**

# APNIC地域の今後

- **次回APNIC会議での提案は未定**
  - コミュニティから提案が提出されることが理想
  - 状況によってはポリシー提案ではなく、APNIC事務局でなんらかの取り組み案を出す可能性
- **対策が完璧ではなくてもよいので、協力的な姿勢、対策を進めている方向性を出せることが大事と思われる**



# ディスカッション

## 1. 目的と意義は支持できるか？

- 支持できる
- 支持しない
- 目的・意義は支持できるがWHOIS以外の方法で対応すべき → その場合、どういう方法か？

## 2. 今後、提案または対策が行われた場合、絶対賛成できない対応はあるか？その理由は？

- 年に一度の情報更新の要請
- 一定期間以上更新されない情報はその旨表示
- 逆引きの削除 \*レジストリ内で情報は残し、逆引きゾーンから外す
- WHOIS登録情報の削除 \*レジストリ内で情報は残す
- 情報更新しない場合の罰金

## 3. 「こういう対応のほうが受け入れやすい」等 JPNICの案があればおきかせください