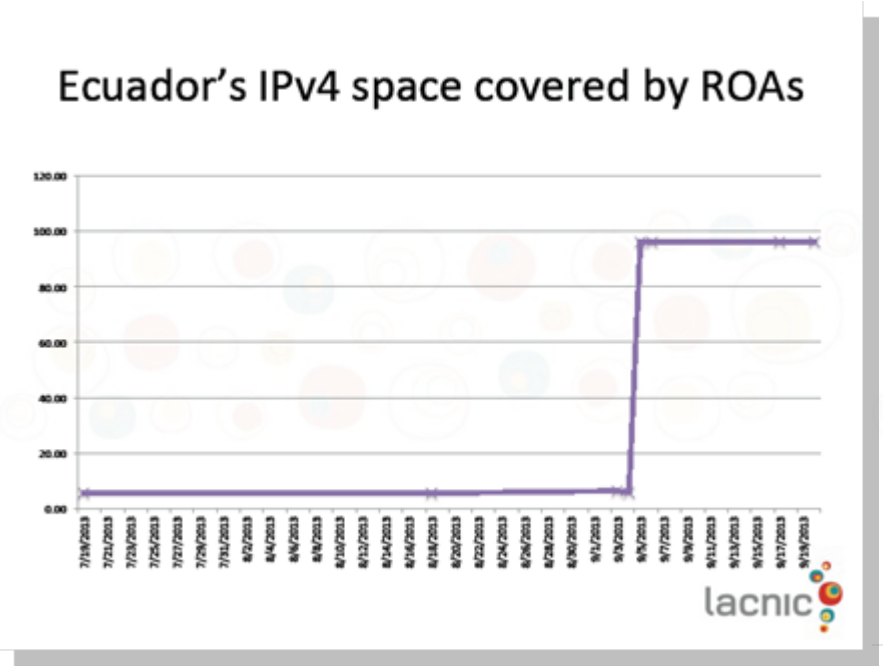
ルーティングの国際動向とRPKIの将来
～2013年の国際動向と今後の課題～

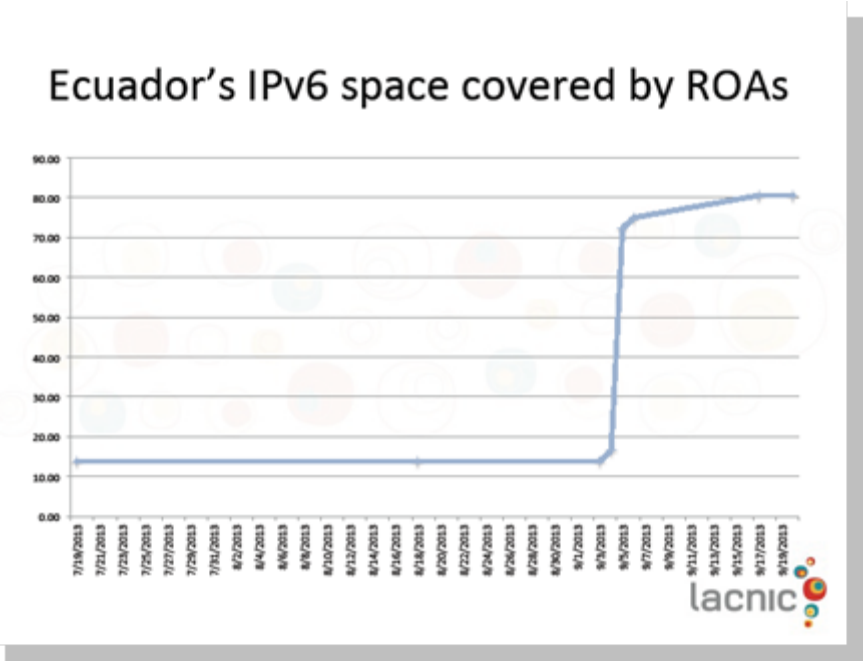
木村泰司

JPNIC 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

エクアドル（1/2）

- 2013年9月4日～5日にROAの発行数が激増
- IPv4、IPv6共にカバー率が90%ほどに上昇





http://www.iepg.org/2013-11-ietf88/RPKI-Ecuador-Experience-v2b-1.pdf

エクアドル(2/2)

- エクアドル国内のIXPであるNAP.ECでRPKIを導入するイベントが開催される
- IPアドレスの割り振り先組織の担当者が集まってリソース証明書とROAを発行
- ルートサーバにおけるOrigin Validationが実装されるなどツールも用意

エクアドルでRPKIが動き始めた！

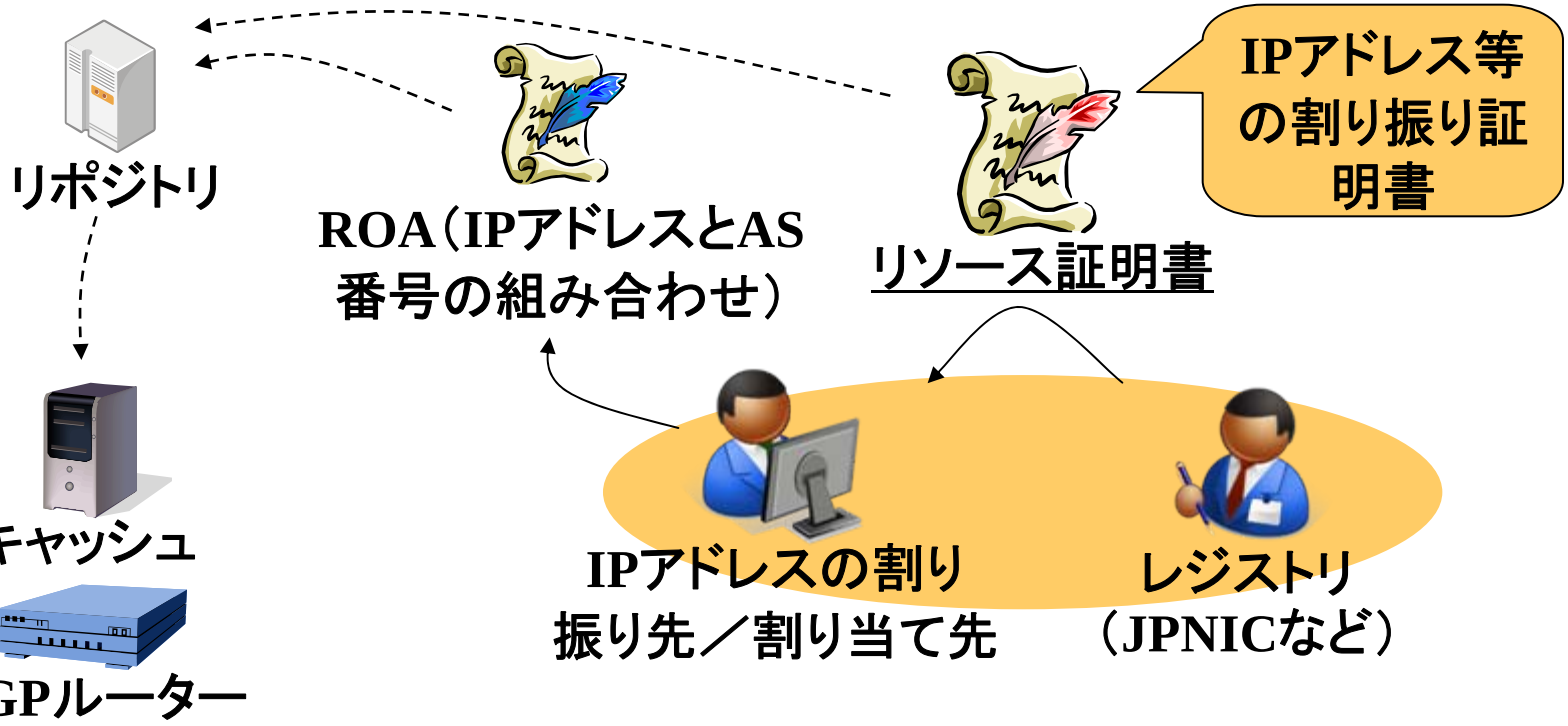
この発表の内容

- RPKIとは
- 2013年の国際動向 ～IETFを中心に～
- Origin Validationの導入課題

RPKIとは

RPKI （リソースPKI）

⇒ Resource Public-Key Infrastructure

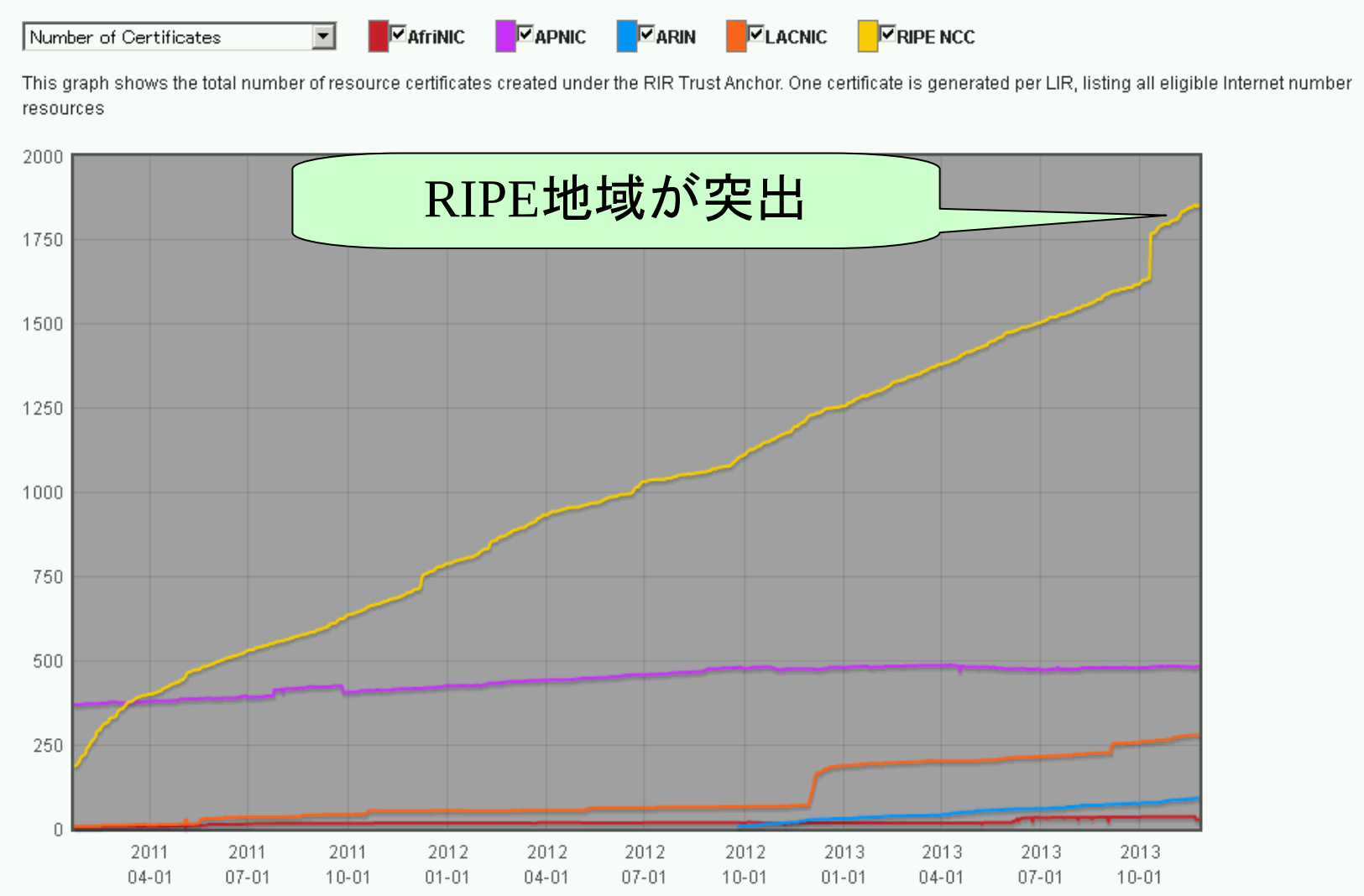


2013年の国際動向
～IETFを中心に～

2013年のRPKIの国際動向

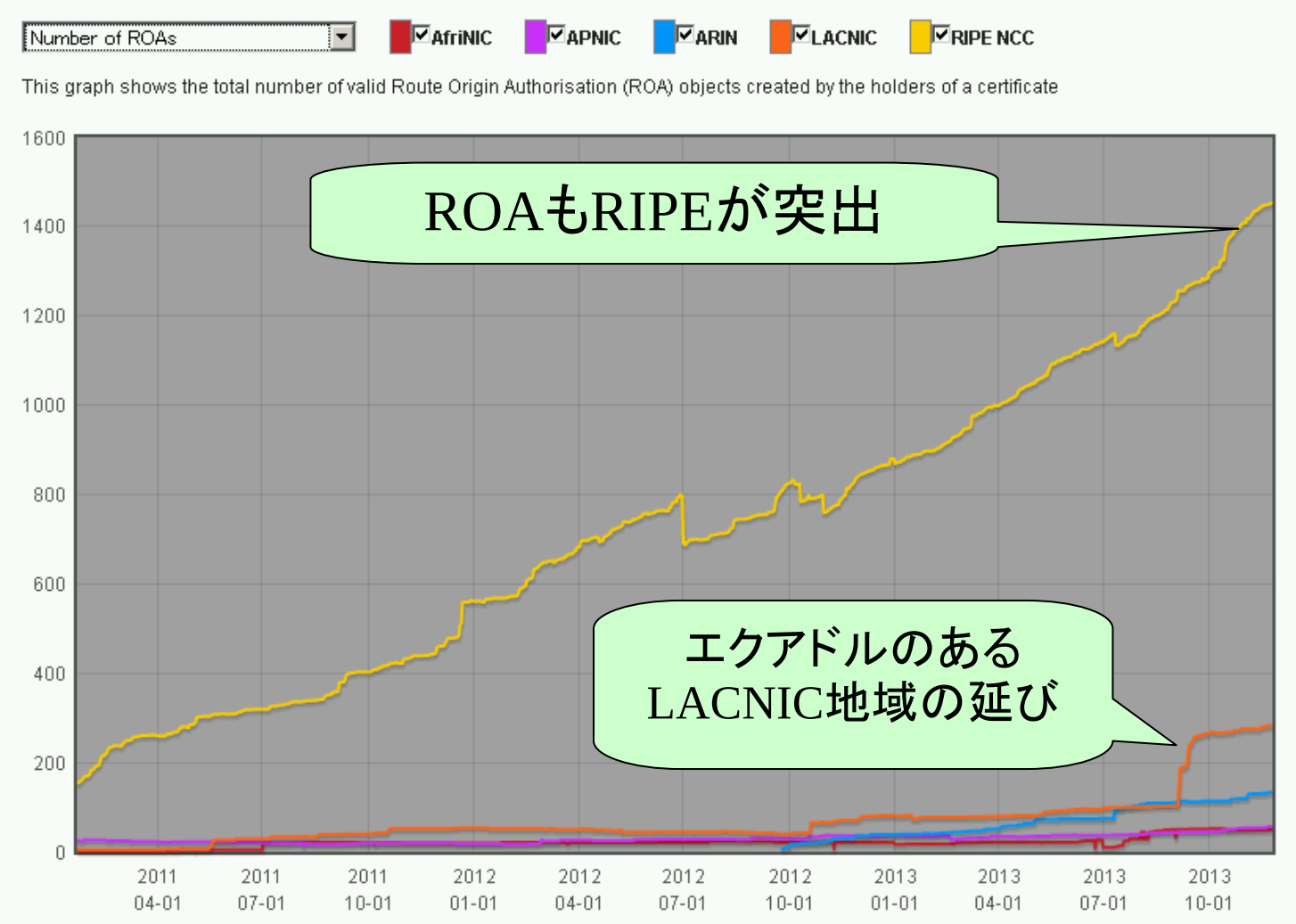
- リソース証明書とROAの増加
  - RIPE地域
  - エクアドルのIXP
- RPKIの実装や利用環境も徐々にできてきた
  - 統計・可視化のWebサイトの登場
  - BGPルータの対応
- ディスカッションが進む
  - RPKIワークショップ（2013年7月）
  - RPKIオペレーショナルパネル（2013年8月）

リソース証明書の発行数

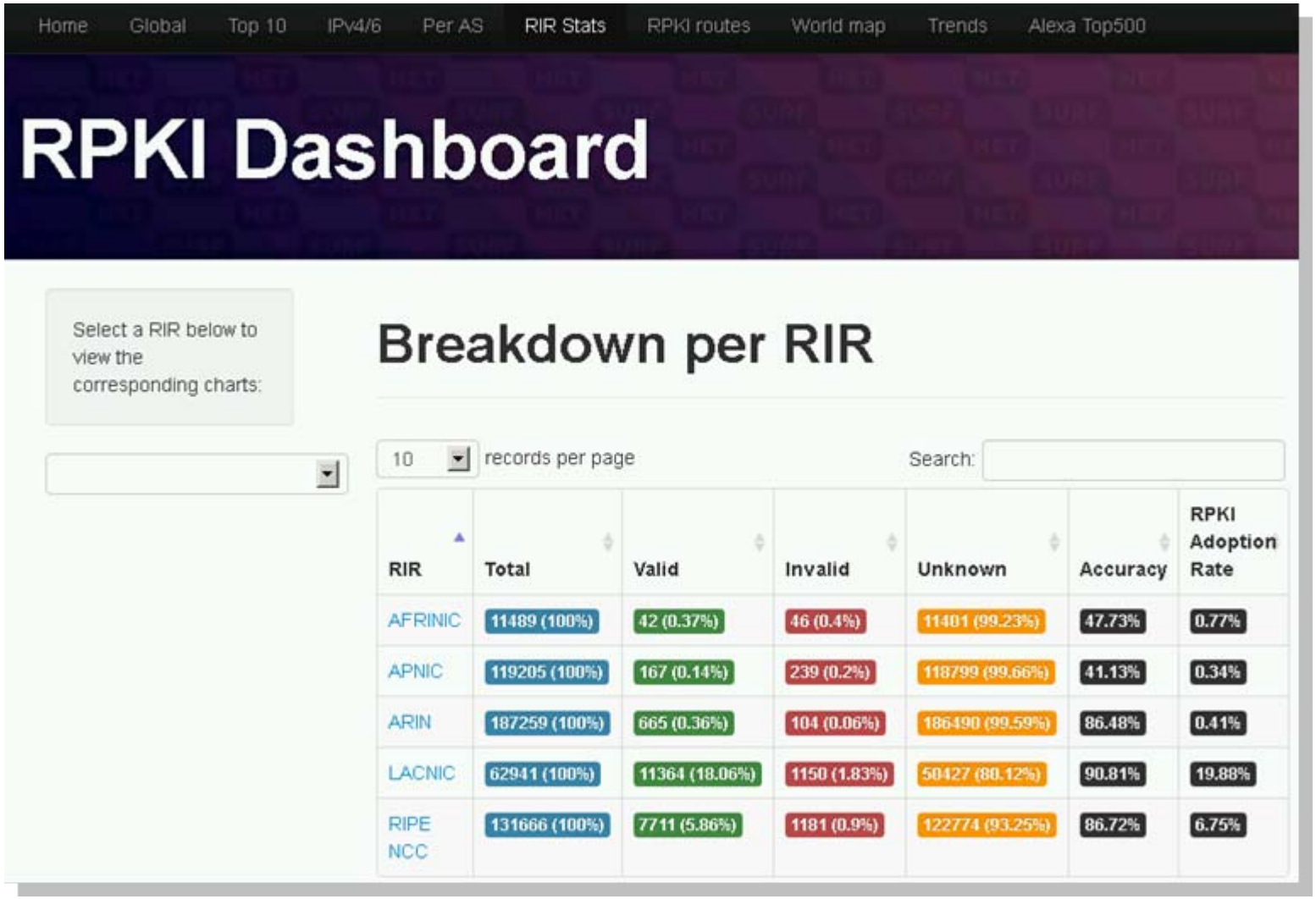


http://certification-stats.ripe.net/

ROAの発行数



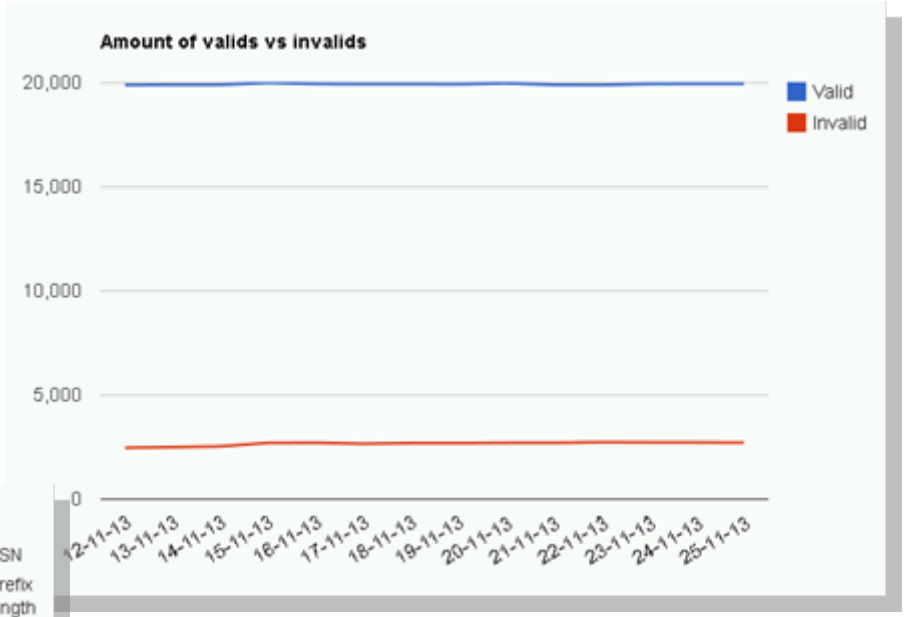
統計・可視化のWebサイト

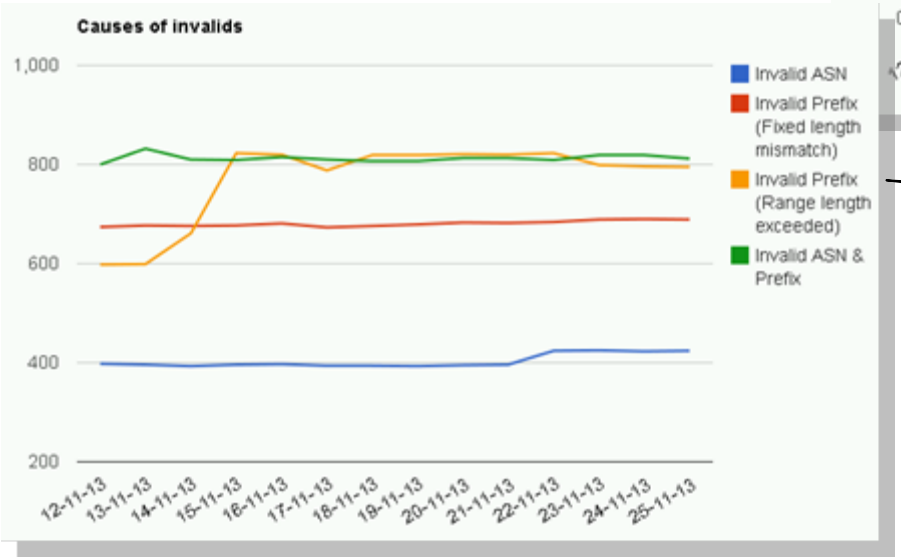


http://rpki.surfnet.nl/

統計・可視化のWebサイト

51万経路中ROAに照らし合わせてvalidだったprefix数約20,000



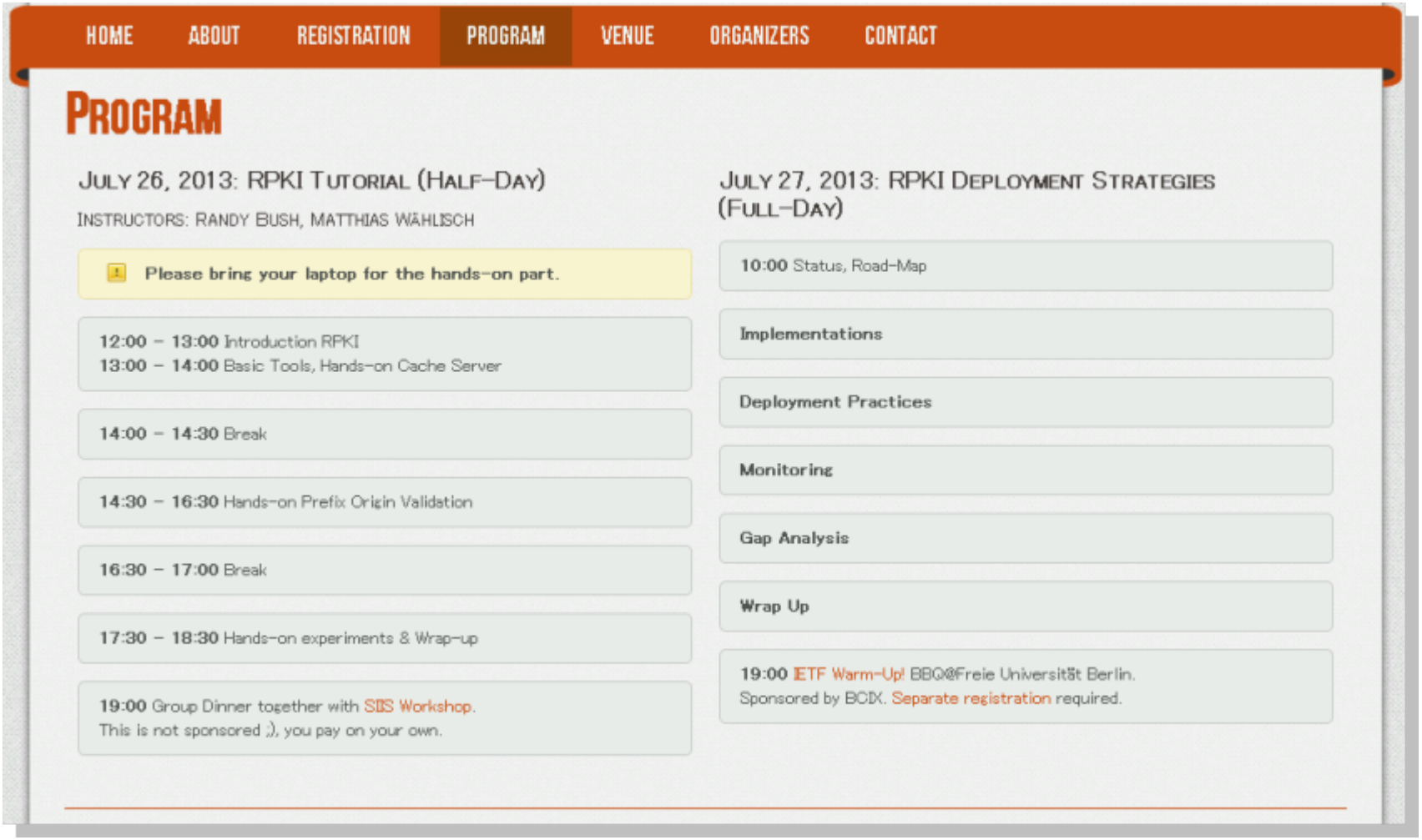


invalidだった2720 prefixの内訳。AS番号が異なる「Invalid ASN」は1,200近くある。

RPKIワークショップ（2013年7月）

http://rpkiws.realmv6.org/

プログラム



http://rpkiws.realmv6.org/#program

RPKIワークショップ Day2のまとめ

- RPKIの今後の課題 – Deployment Strategy

黒板	Policy&Regal	Tools&Infrastructure	**How To**
	• Value / Risk • Legacy / PI • Control (Gov)	• Monitoring • Route (support) • Stability • **Reliability (includes implementation.)**	• BCP / Deployment

その他の話題
〇Single Root
〇Monitoring (RPKI Dashboard)、Legacy Holder（RIPEで発行対象でない）
〇RPKIの導入価値：発行数の増加が価値なのではなく、運用者による不正な経路情報を検知し、復旧できることにこそ価値があるのではないか（木村）。
⇒RPKI Dashboardで変化を表示しては。

RPKIオペレーショナルパネル（2013年8月）in APNIC36

- 日時と場所
  - 2013年8月 西安・中国
- パネリスト
  - Geoff Huston氏(APNIC)、Randy Bush氏(IIJ)、吉田友哉氏(インターネットマルチフィード)、松崎吉伸氏(IIJ)、木村（JPNIC）
- 興味深い議論
  - **グローバルトラストアンカー（GTA）**
    - IANAに設置され、RIRの上位認証局すなわちルートの認証局となるGTAの必要性
  - トラストアンカーの考え方
    - GTA、RIR、NIRに各々認証局が設置される
  - レジストリにおける障害対応
    - 認証局やリポジトリにおける障害がBGPに影響する可能性（認証局・リポジトリ・キャッシュ各々の運用要件は異なる）

Origin Validationの導入課題

BGPSEC
＝ Origin Validation ＋ Path Validation

RPKIとBGPSEC

- **Origin Validation ← イマココ**
  - 他のネットワークが自ASのIPアドレスを使い始めたことが検知できる
- Path Validation
  - ASパスが途中で変えられてしまったことが検知できる

Origin Validationの導入課題

1. Multiple Originは扱えるのか

   – 重なっているprefixに対する複数のROAは発行できる。しかし、ISPにとっての顧客がIPアドレスを割り振られている場合やパンチングホールの場合は、ROAを管理/運用できるような形作りが必要になってくる。
   – RPKIにおけるROAの発行者はあくまでIPアドレスのホルダーであるため。

Origin Validationの導入課題

2. RPKIを使うためのキャッシュは自分で立ち上げる必要があるのか

- RPKIキャッシュを立ち上げることは（技術的には）難しくないが、安定運用には工夫が必要。
- 共有して使うためのRPKIキャッシュが立ち上がってくるとBGPルーターの設定のみでよく、新たなサーバを運用しなくて良くなる。
  ※リポジトリにアクセスできなくても、キャッシュにアクセスできれば、RPKIは利用できる。

Origin Validationの導入課題

3. RPKIに依存したルーティングになってしまわないか

- RPKIワークショップで指摘されているように、経路制御はBGPルータにおける設定による。ケーススタディが重要になってくると考えられる。
  ※おそらくInvalid prefixを全く取り入れないBGPルータは到達できるネットワークが少なすぎてしまう。
- レジストリの認証局にデータの正しさという意味で依存する形にはなるが、認証局が止まっても経路制御に影響がでにくく、かつ不適切な経路情報を検出して対応できる仕組みづくりが重要だと考えられる。

JPNICの模擬環境

- IPアドレス管理業務に関わる新技術のRPKIにご興味のある方に、その技術を体験していただくために、模擬環境を提供しています。
  - JPNICのIPレジストリシステムとは独立しており、模擬環境のご利用によって、IPアドレス等の登録情報に影響することはありません。
- ご利用方法
  - ca-query@nic.ad.jp
    「資源管理者」「資源管理者略称」と「氏名」「メールアドレス」をお書き添えの上、お申し込みください。Webインターフェースのアカウントを作成致します。

まとめ

- 2013年のRPKIの国際動向
  - リソース証明書とROAの増加
  - 統計・可視化のWebサイトやBGPルータの対応
  - RPKIワークショップなどが開催されディスカッションが進んだ
- Origin Validationの導入課題
  - AS運用の現状に合わせたROAの管理、RPKIという新たな仕組みを導入することという二種類に大別される課題がある。

JPNIC