

# RPKI チュートリアル & ハンズオン ～ ROA 発行からルータでの参照まで～

2013年4月26日(金)  
ENOG20 Meeting

# はじめに

---

- ご紹介
  - 岡田雅之（おかだまさゆき）
    - 技術部
  - 木村泰司（きむらたいじ）
    - 技術部／インターネット推進部

# 内容

---

- RPKIチュートリアル
- ハンズオン

# RPKIチュートリアル

---

- RPKIとは
- RPKIは何に使えるのか
- 国際・国内の動向

# RPKIとは

# ことば

---

RPKI (リソースPKI)

⇒ Resource Public-Key Infrastructure

公開鍵 = パブリックキー？

PKI？

リソース？

なぜ”基盤”？

# ことば

---

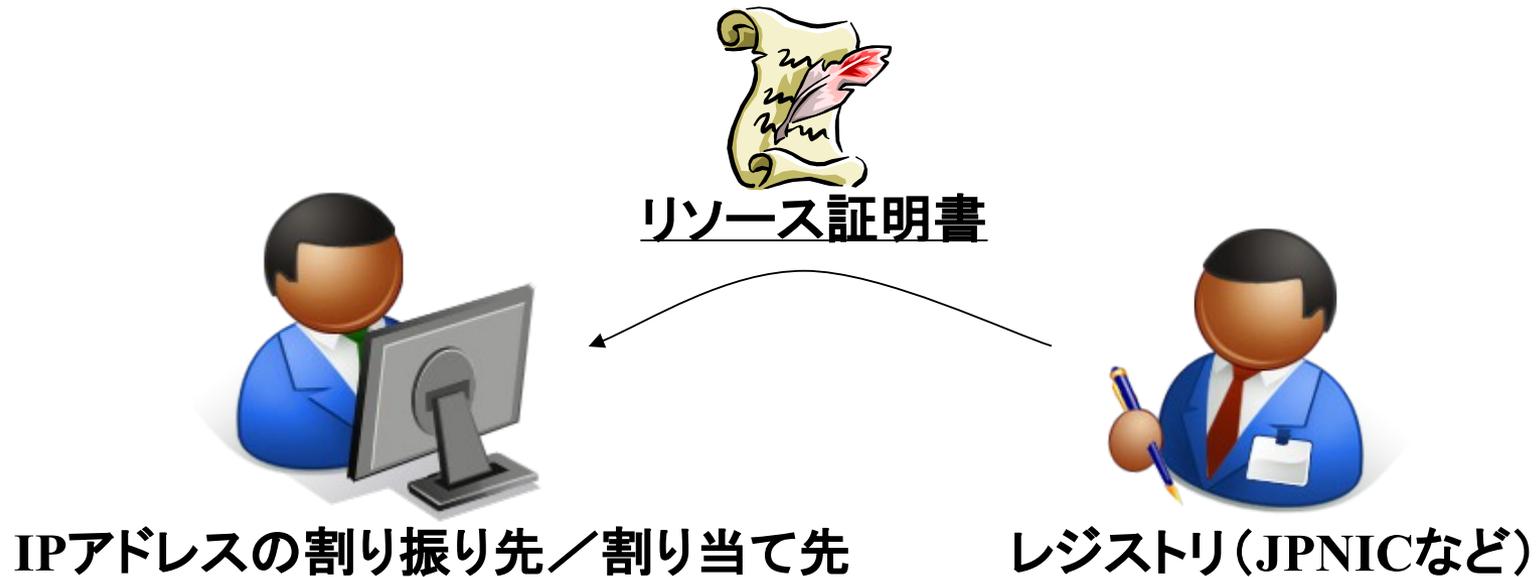
**リソース証明書**

**⇒ Resource Certificate**

サーバ証明書とどう違う？

またまたリソース？

# リソース証明書



リソース証明書=IPアドレスやAS番号が書かれている電子証明書

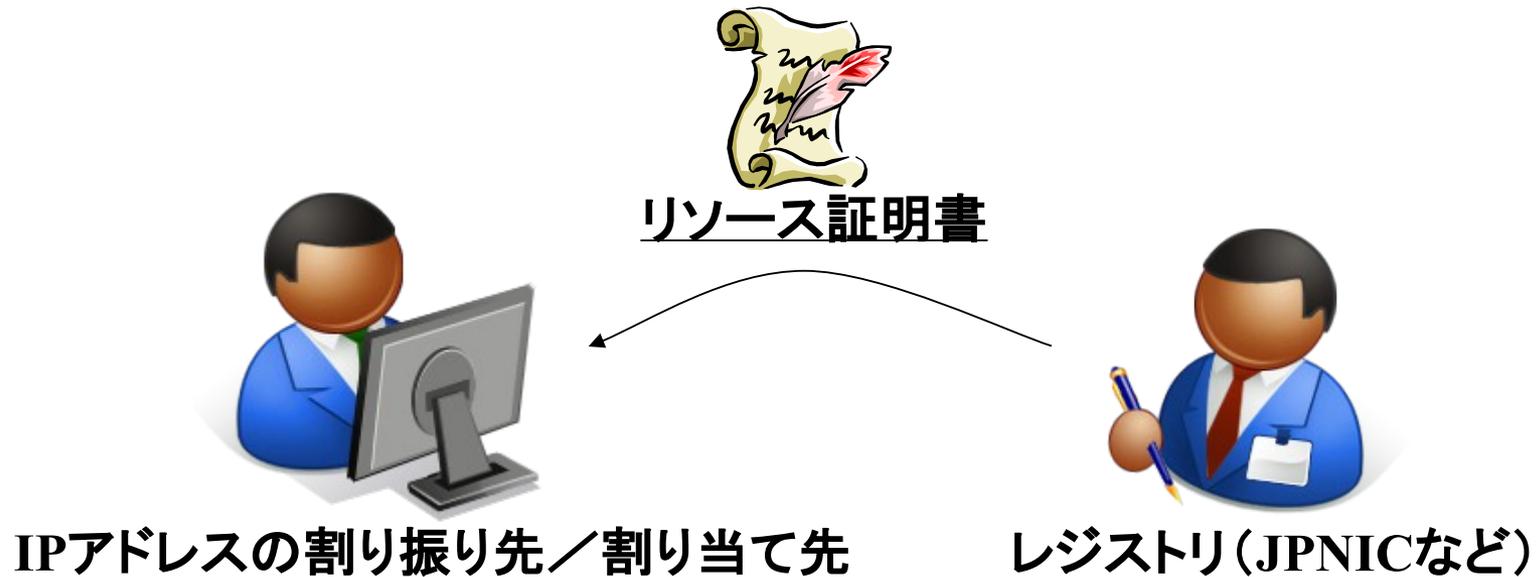
# JPNICとリソース証明書

---

- JPNICには。。
  - WHOISデータベース
  - ↓
  - 割り振り情報や割り当て情報  
(IPアドレスやAS番号が入っている)
  - ↓
  - 電子証明書を発行すれば「リソース証明書」!

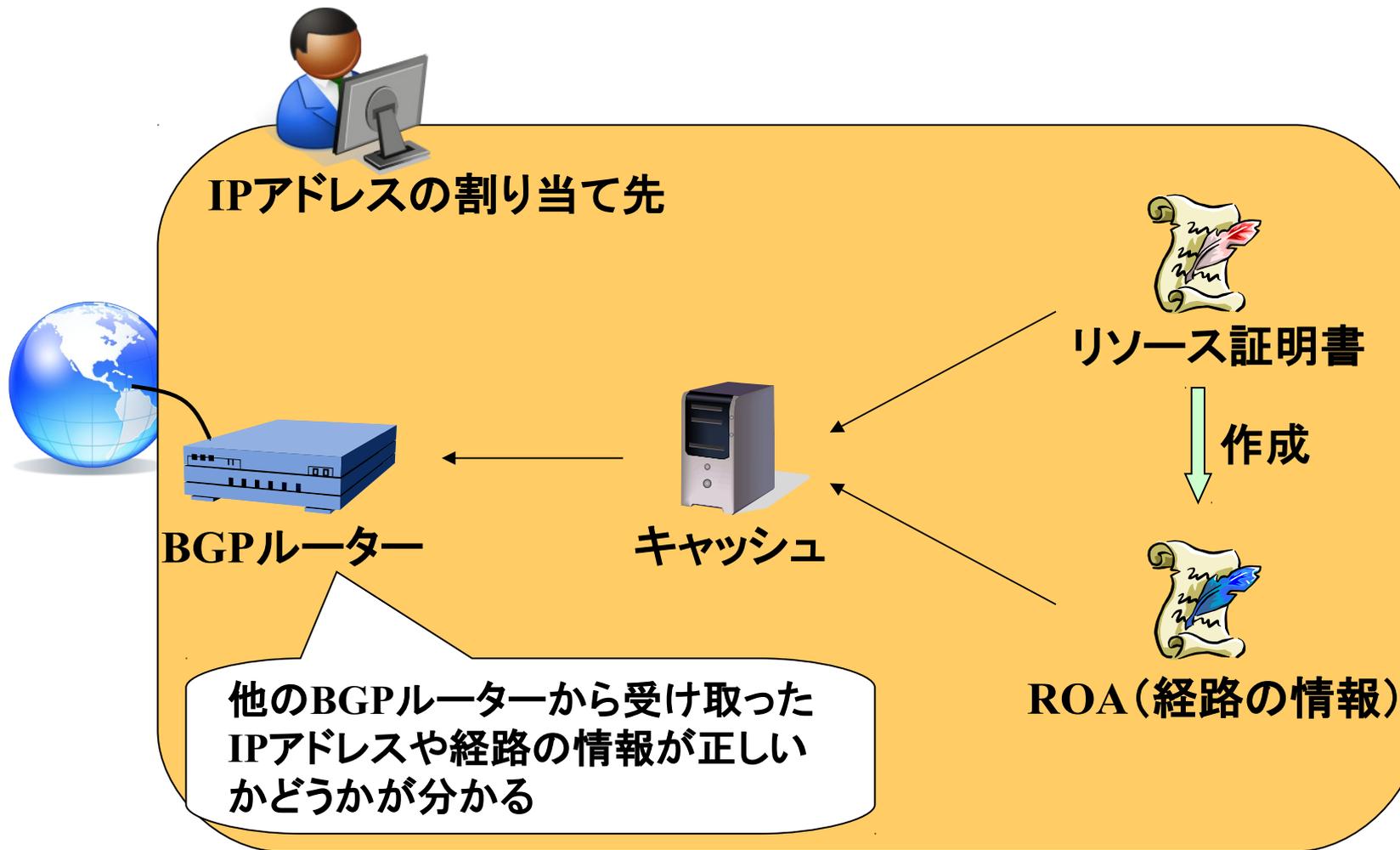
# RPKIは何に使えるのか

# リソース証明書



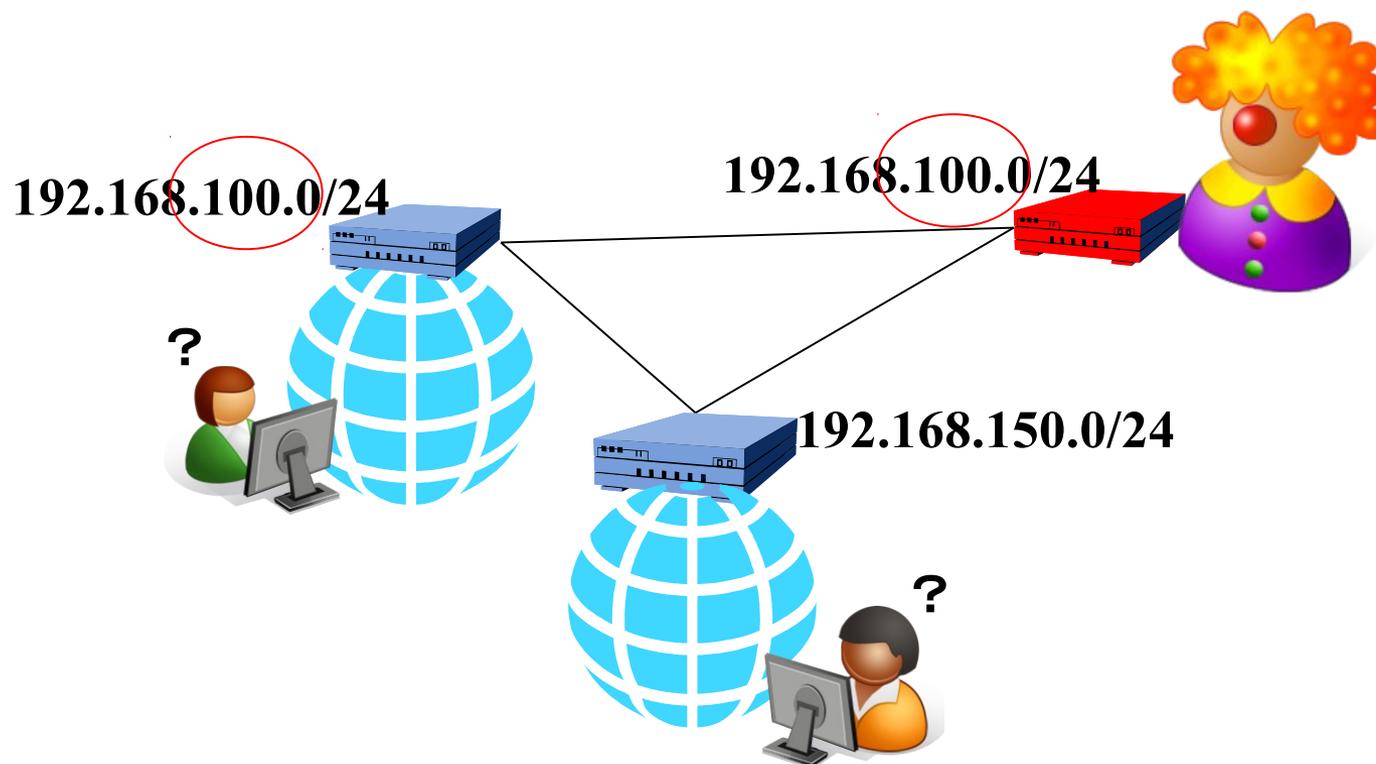
リソース証明書=IPアドレスやAS番号が書かれている電子証明書

# リソース証明書 の用途の一つ



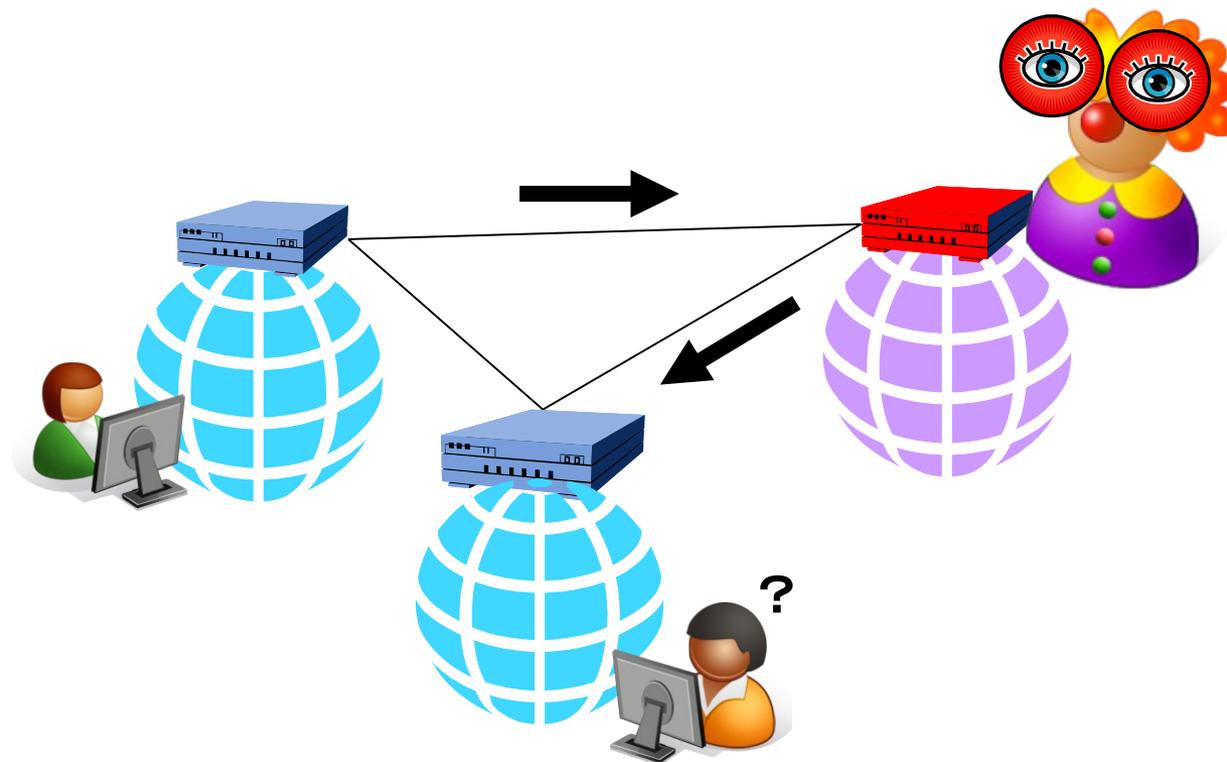
# インターネットへのつなぎ方 良くない例(1)

- インターネットに接続したBGPルーターで、他人のIPアドレスを設定する。

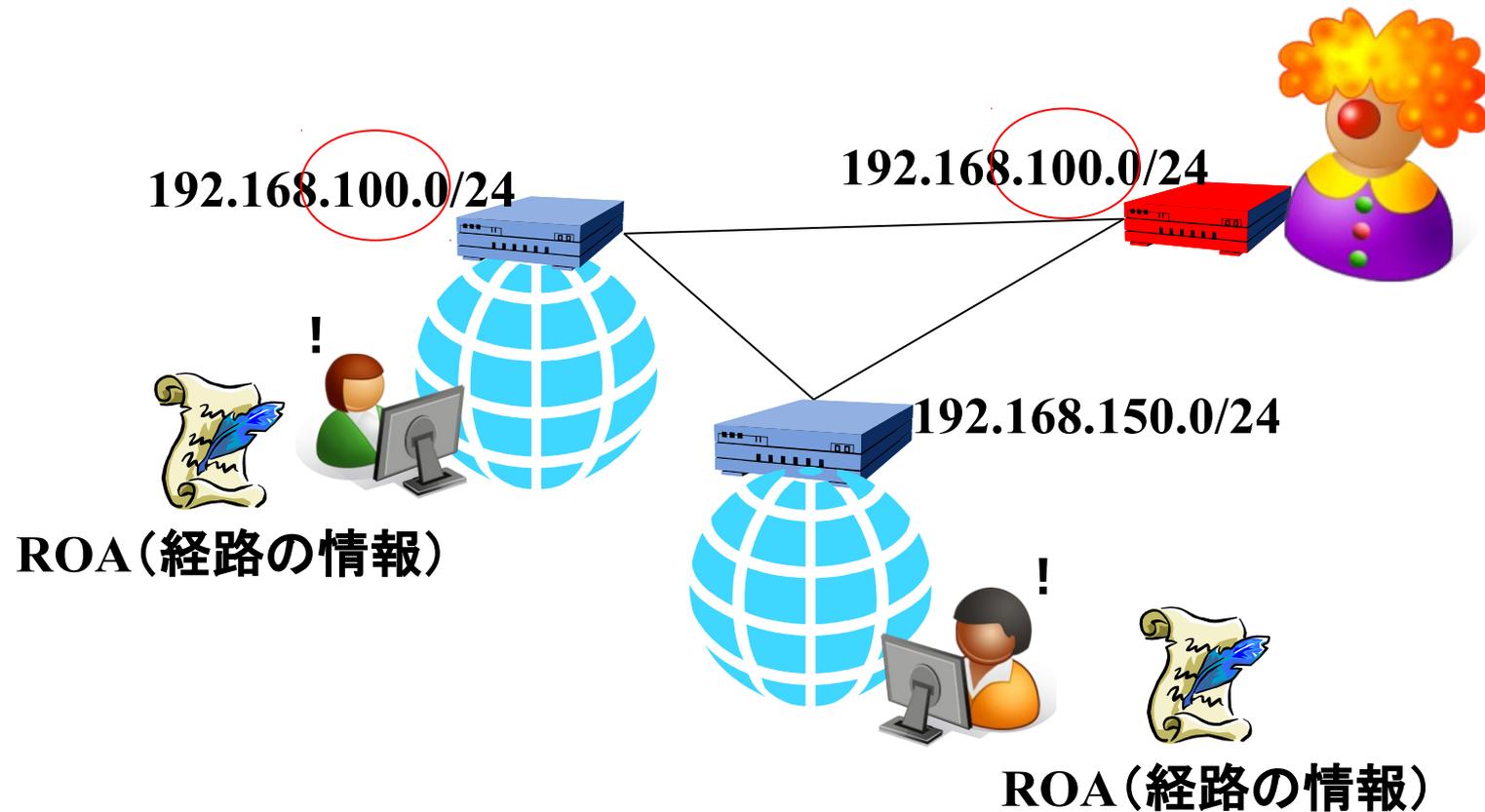


# インターネットへのつなぎ方 良くない例(2)

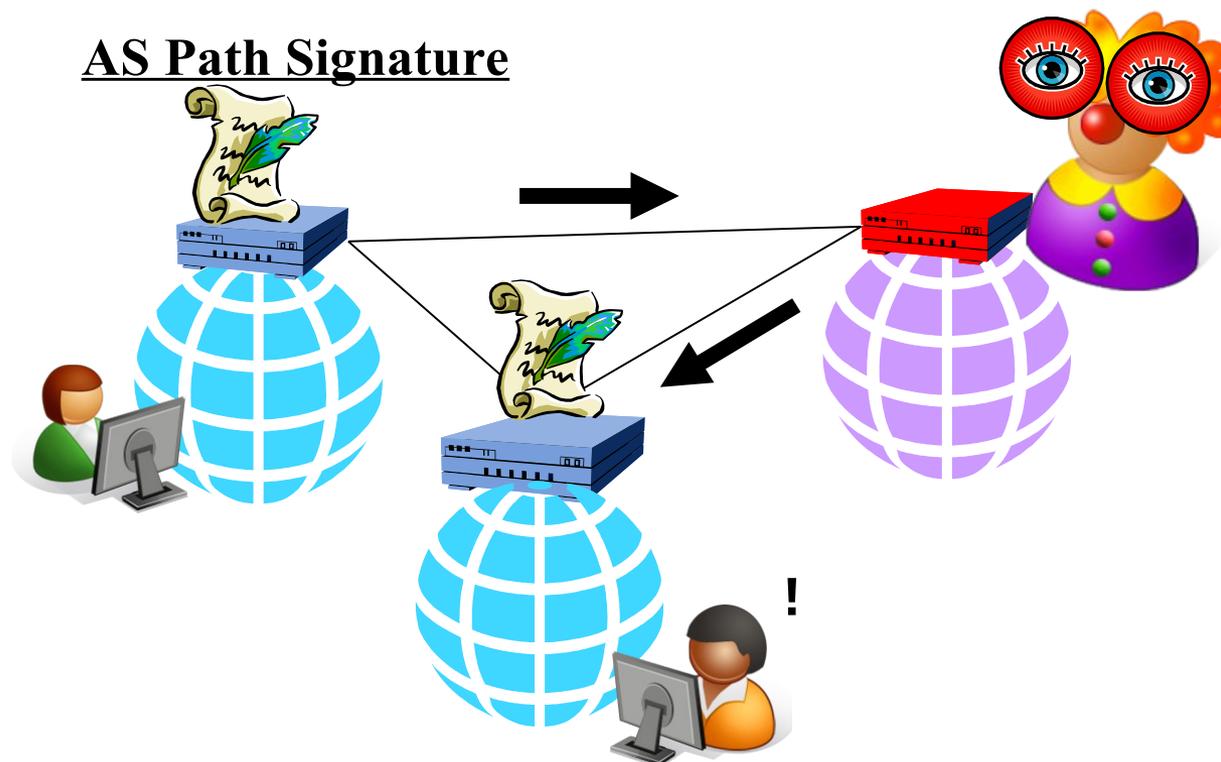
- 本来とは異なる経路(ASパス)を設定する。



# (1) Origin Validation



# (2) Path Validation



# RPKIによって

- IPアドレスの設定ミスや不正な設定を、BGPルータで検知できる可能性が出てくる。
  - Origin Validation
    - 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

ちなみに

**BGPSEC**

**= Origin Validation + Path Validation**

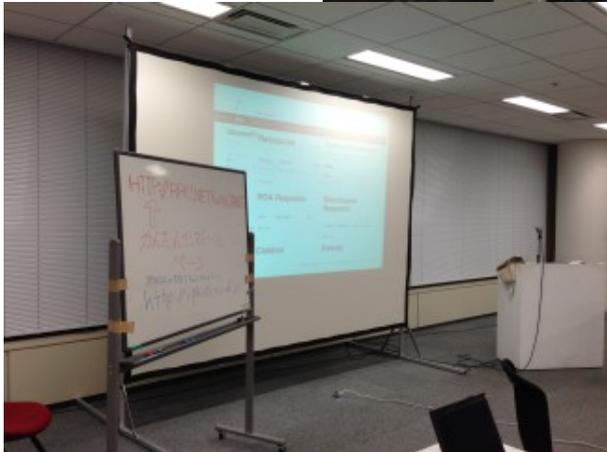
# 国際・国内の動向

# 国内

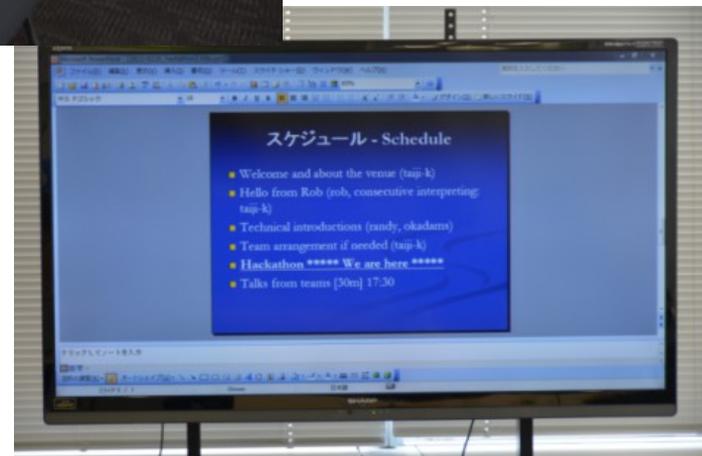
---

- JANOG RPKIルーティングを試す会  
– RPKIハッカソン
  - 2013年1月23日@IIJ
  - 2013年2月20日@JPNIC

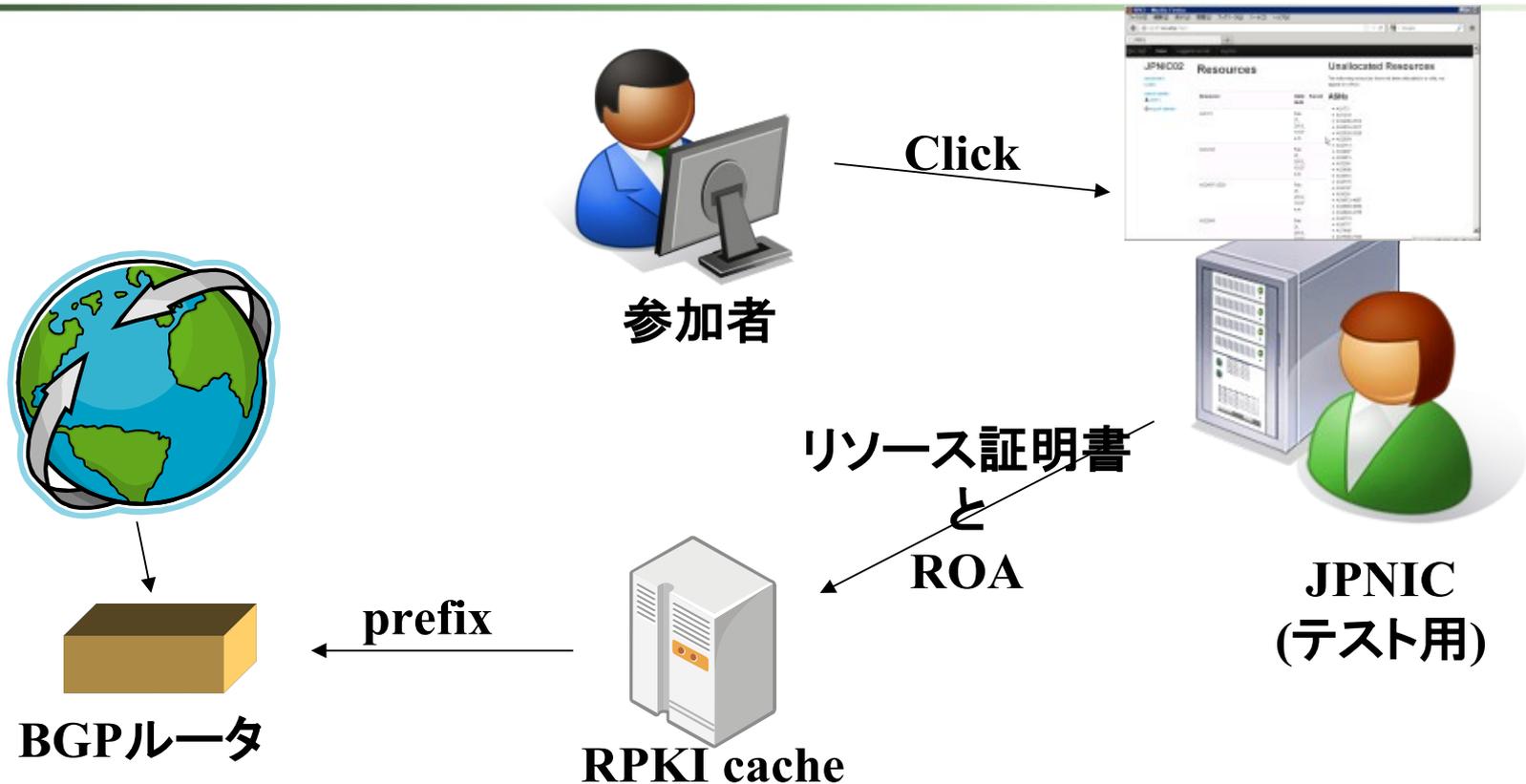
# RPKI ハッカソン@IIJ



# RPKIハッカソン2@JPNIC

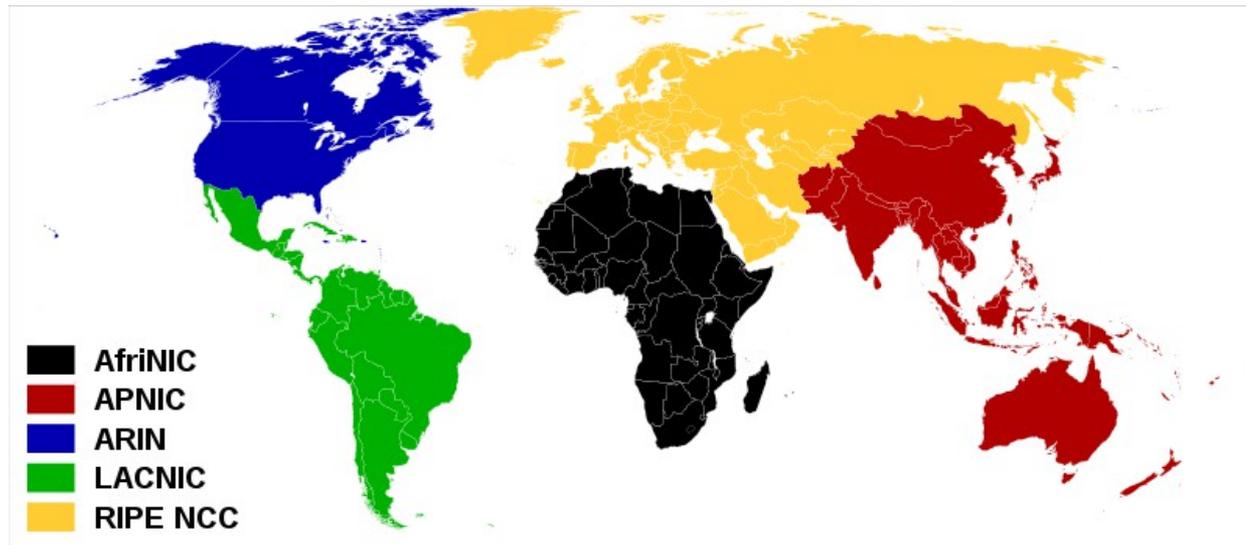


# RPKIハッカソン 実施内容



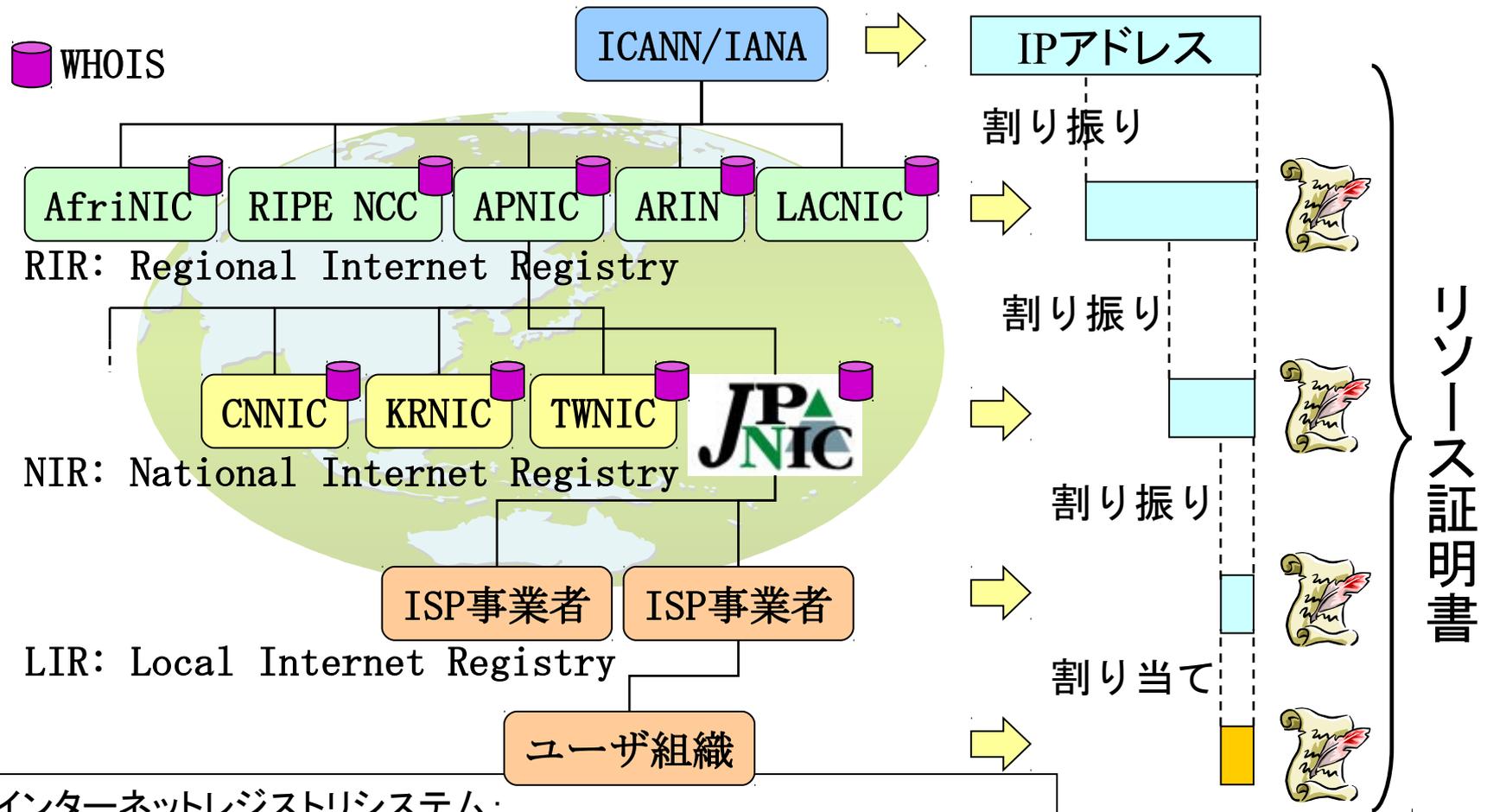
- JPNICの割り振り情報にもとづいてリソース証明書とROAを発行
- 参加者がROAを発行してリポジトリに格納(自動)
- リソース証明書とROAをキャッシュに転送
- BGPルータで正しい経路かどうかを確認!

# 国際動向



[http://en.wikipedia.org/wiki/File:Regional\\_Internet\\_Registries\\_world\\_map.svg](http://en.wikipedia.org/wiki/File:Regional_Internet_Registries_world_map.svg)

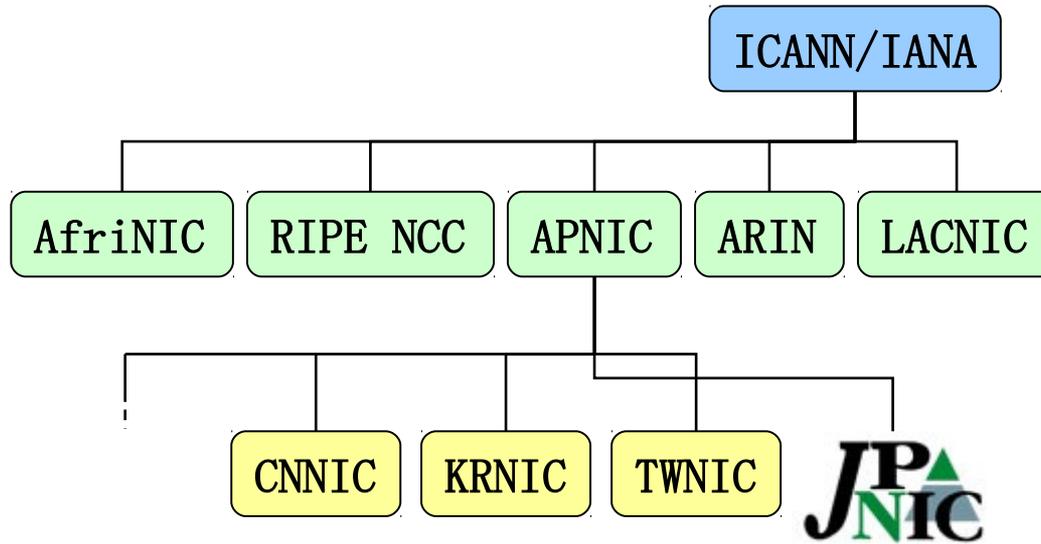
# インターネットレジストリとリソース証明書



インターネットレジストリシステム:  
IPアドレスの一意性を保証し経路制御の適応性を向上させる仕組み



# ツリー構造



発行元: (APNIC)  
対象: (JPNIC)  
アドレスブロック:  
192.0.0.0/8



発行元: (JPNIC)  
対象: (ISP事業者)  
アドレスブロック:  
192.168.0.0/16



発行元: ((ISP事業者))  
対象: (ユーザ組織)  
アドレスブロック:  
192.168.64.0/22



ROA – Route Origination Authorization  
(ISP事業者による署名付きデータ)

- AS65535による192.168.64.0/24の  
経路広告を認可 (Authorization)

# リソース証明書発行数

Number of Certificates



AfriNIC



APNIC



ARIN

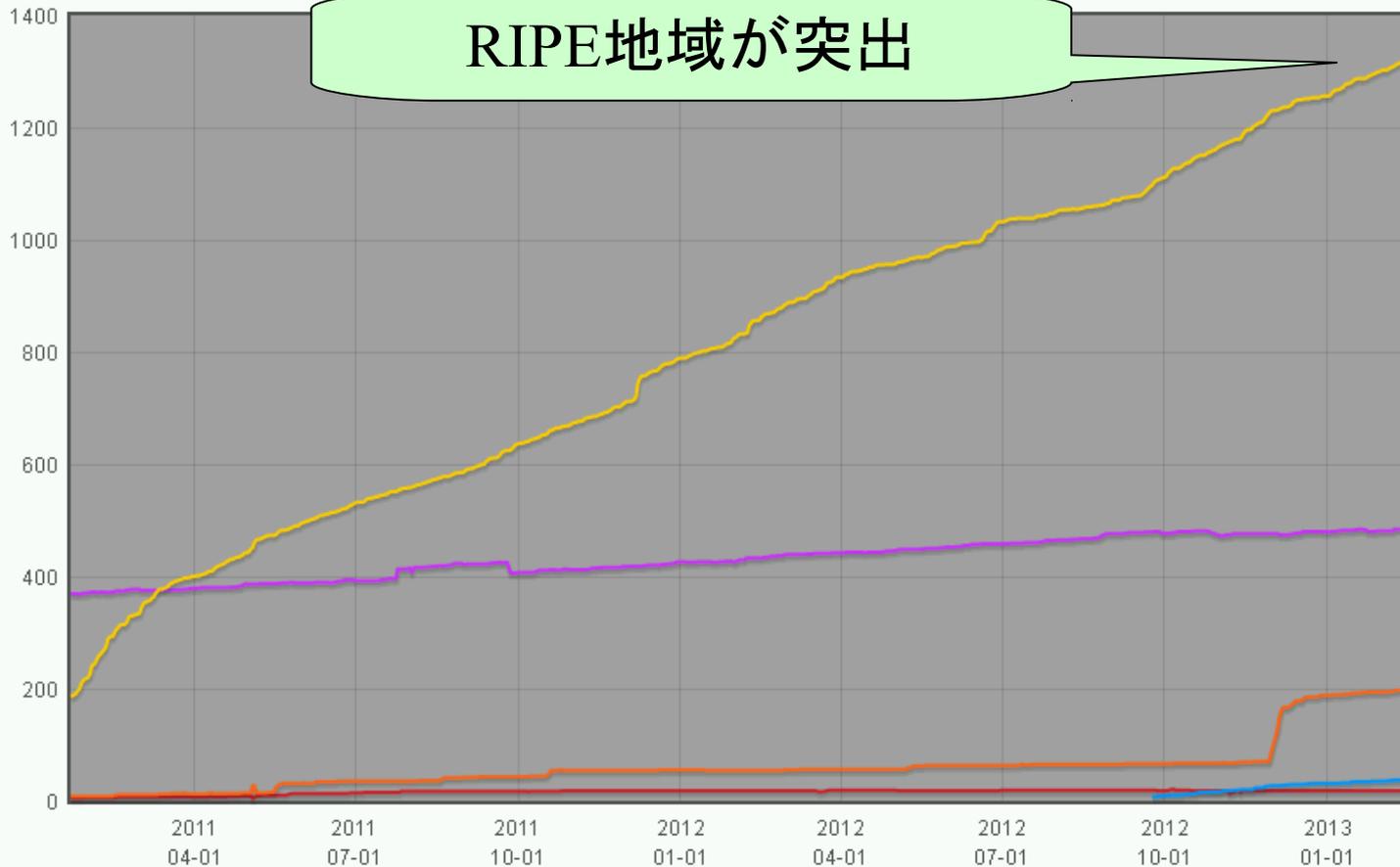


LACNIC

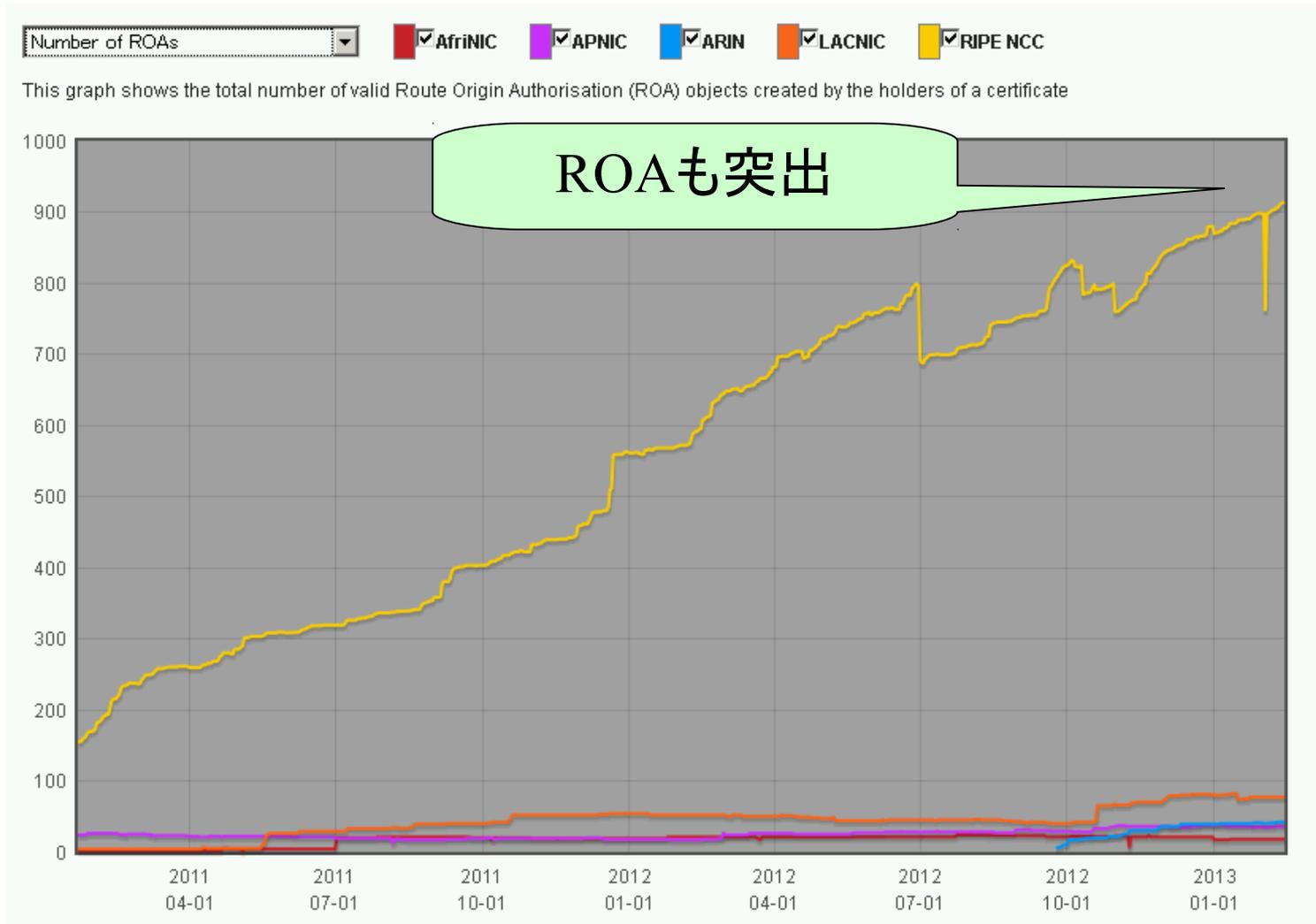


RIPE NCC

This graph shows the total number of resource certificates created under the RIR Trust Anchor. One certificate is generated per LIR, listing all eligible Internet number resources

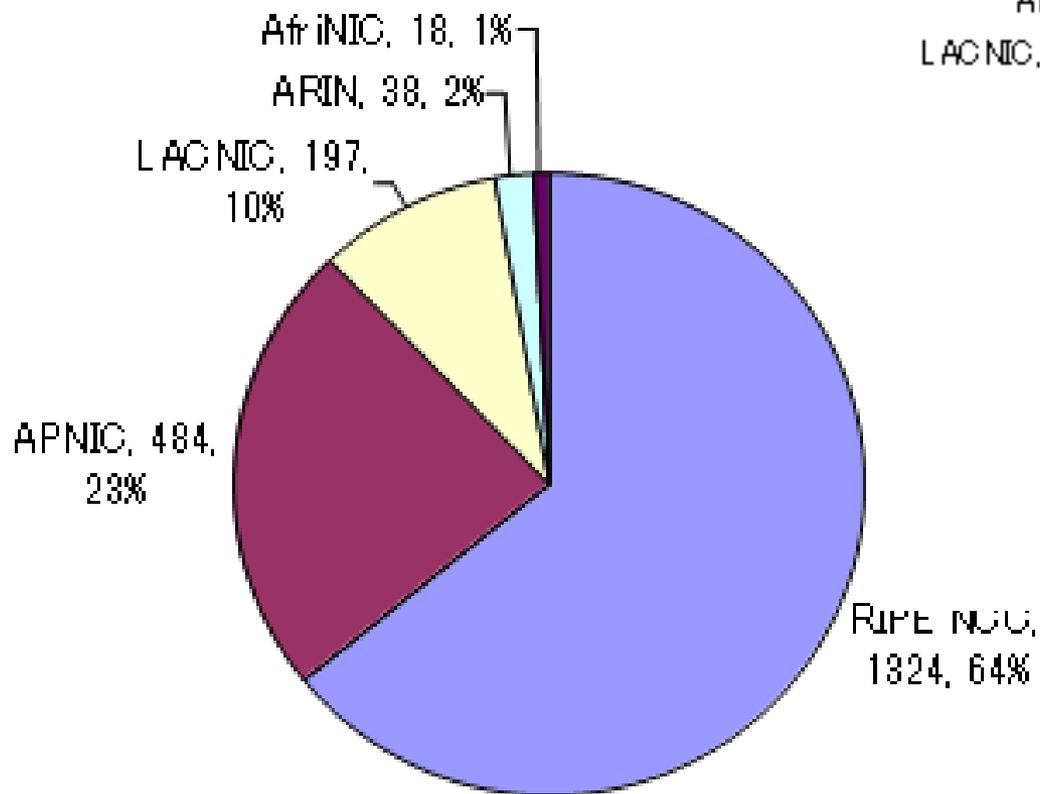


# ROAの発行数

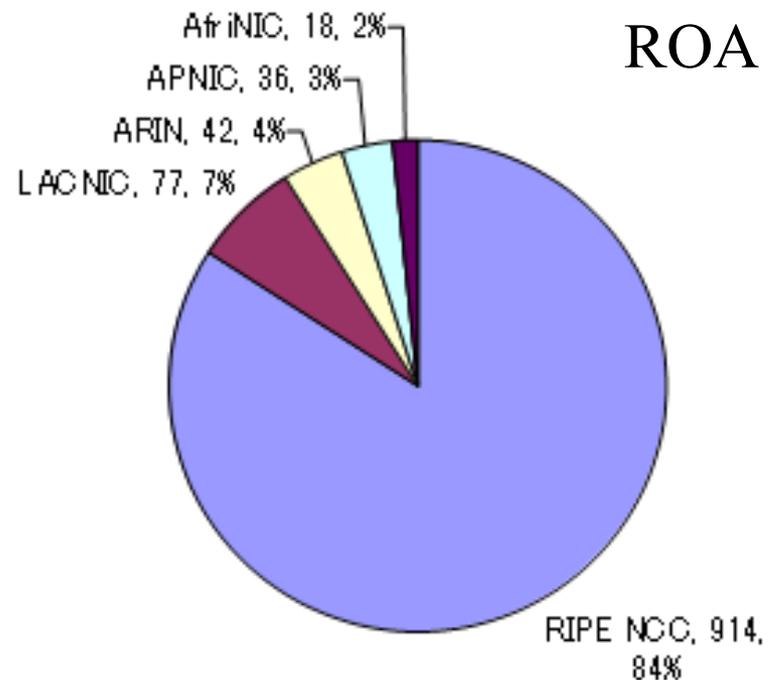


# 地域ごとの割合

## リソース証明書



## ROA



# グラフから読み取れること

- RIPE地域はリソース証明書とROの数が突出
  - いち早く「検証を体験できる」ツールの提供
  - や、RIPEミーティングでの活発な議論が要因か

- LACNICが2012年末に急な伸び
  - LACNIC XVIII(2012年11月)

ツールやその  
情報が鍵とも  
考えられる

⇒事業者にもメール連絡した(LACNIC担当者)(2013年4月加筆)

- APNICは伸びが緩やかでROAが比較的少ない
  - 最も早く提供を開始したが。。

# Validationツール

- Public RIPE NCC Validator

**RPKI Validator** Home Trust Anchors **ROAs** Ignore Filters Whitelist BGP Preview Export Router Sessions

## Validated ROAs

Validated ROAs from APNIC from AFRINIC RPKI Root, APNIC from ARIN RPKI Root, APNIC from IANA RPKI Root, APNIC from LACNIC RPKI Root, APNIC from RIPE RPKI Root, ARIN RPKI Root, AfriNIC RPKI Root, LACNIC RPKI Root, RIPE NCC RPKI Root, ripe-pilot ×

Show  entries Search:

ASN	Prefix	Maximum Length	Trust Anchor
42	194.0.17.0/24	24	RIPE NCC RPKI Root
42	2001:678:3::/48	48	RIPE NCC RPKI Root
42	194.0.42.0/24	24	RIPE NCC RPKI Root
42	2001:678:60::/48	48	RIPE NCC RPKI Root
42	192.30.152.0/21	32	ARIN RPKI Root
174	89.207.56.0/21	21	RIPE NCC RPKI Root
174	2a00:1ed8::/32	32	RIPE NCC RPKI Root

# Validationツール

- RPKI Origin Validation Looking Glass

The screenshot shows the web interface for the RPKI Origin Validation Looking Glass tool. At the top, there is a header with the 'lacniclabs' logo on the left, the text 'Origin Validation looking glass' in the center, and a green circular icon with a flask on the right. Below the header, the interface is divided into two main sections. On the left is a 'Search form:' containing several input fields: 'Query current RPKI Dataset:' with an empty text box, 'Select your query type:' with a dropdown menu set to 'Prefix CIDR query (v4 and v6)', 'Refine your search scope:' with a dropdown menu set to 'Search All Routes', and 'Time frame:' with a dropdown menu set to 'Last 24 hours'. A 'Search' button is located at the bottom of this form. On the right is a pie chart titled 'Valid and invalids as of today'. The chart shows three segments: a large blue segment for 'Valid Routes : 87.73%', a small red segment for 'Invalid / Bad OriginAS : 5.35%', and a small green segment for 'Invalid / Bad Max Len : 6.92%'. The source 'Highcharts.com' is noted at the bottom right of the chart area. Below the search form and chart, there is a section titled 'Origin Validation Looking Glass' with a descriptive paragraph: 'This tool allows performing different queries on a dataset composed of BGP routes currently covered by ROAs (Route Origin Authorizations) hosted on any of the five RIRs (Regional Internet Registries)'. A second paragraph states: 'BGP Route and path data are periodically fetched from RIPE NCC's RIS Project.' At the bottom of this section, it says 'Route counts for the last 24 hours'.

# RPKI CAハッカソン 実施内容

- リソース証明書を発行する側(NIR)のハッカソン



JPNIC  
(テスト用)

- NIRのテスト環境を作成開始
- NIRにおける運用やAP地域の進め方などを検討

# まとめ

- RPKI (Resource Public-Key Infrastructure)
  - リソース証明書 (IPアドレスやAS番号が書かれている電子証明書)
- RPKIの応用としてBGPを使ったインターネット経路制御のセキュリティの仕組みが実装されつつある。
- 国際・国内の動向
  - 国際的にはリソース証明書やROAの発行が実験的に行われている。インターネットの経路情報と比較して経路が正しいかどうかを見るために使う動きがある。