RPKI deployment experience in Japan

Hiroki Kawabata

Agenda

- How RPKI is explained in Japan
- Deployment status
- FAQ and a hot issue

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

Key message

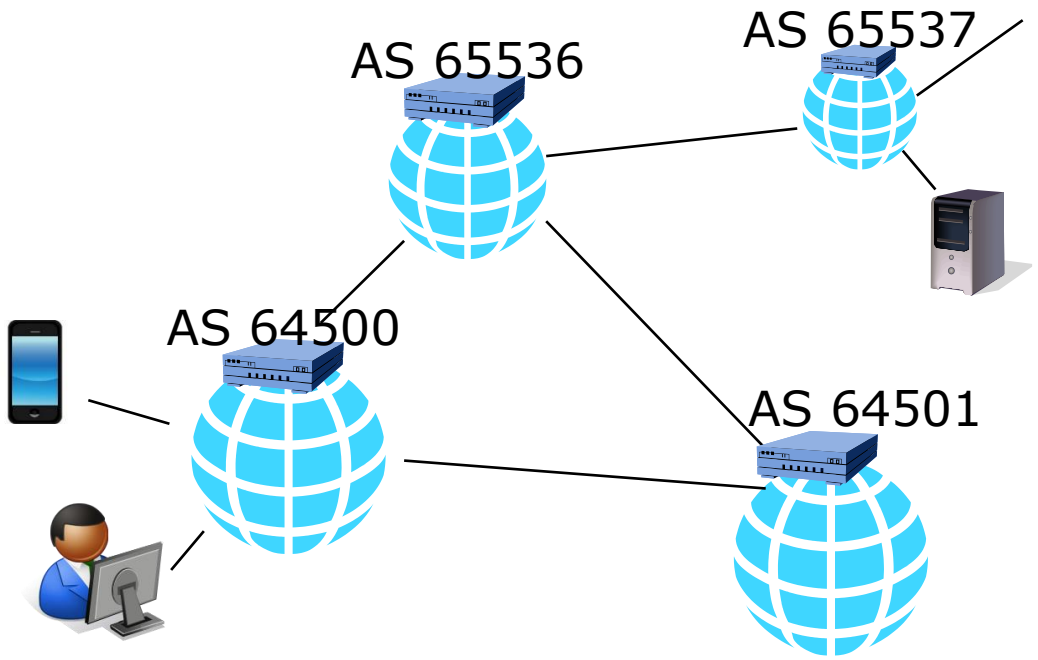
- **The era to know actual state of things**
  - The global routing system has been looked complicated. And it was seemed difficult to know it’s whole figure.

- **For opening eyes on un-visualized things**
  - Build a tool to know actual use of address
  - Make more colleagues to go forward
  - Make standard to deploy for making our sight wider

JPNIC

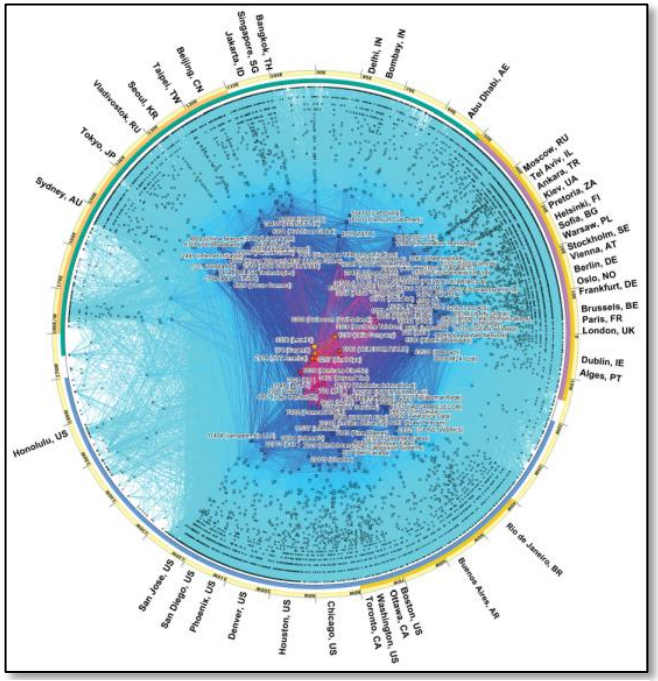
How RPKI is explained in Japan(1)

- **BGP**



Assigned ASN 95,230

The 32-bit AS Number Report
http://www.potaroo.net/tools/asn32/



CAIDA's IPv6 AS Core AS-Level Internet Graph
http://www.caida.org/research/topology/as_core_network/

IP address prefix accommodated in a AS is announced to other AS via BGP.

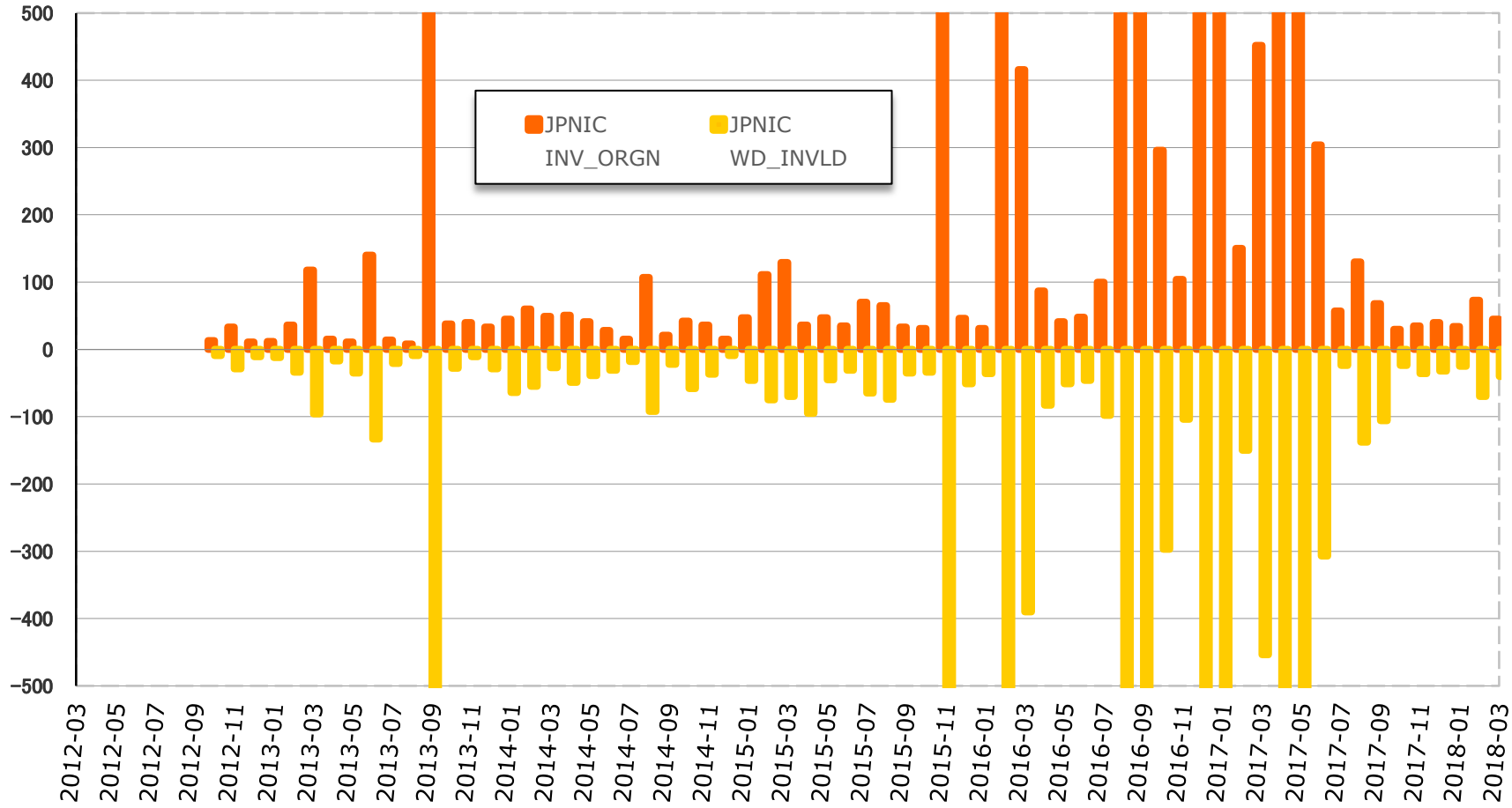
How RPKI is explained in Japan(2)

- **MyEtherWallet.com**
  - What observed
    - AWS Route 53's prefix originally /23 was announced as /24
    - A DNS server in the prefix made forged DNS response for MyEtherWallet.com
    - The web server has self-signed certificate (EV SSL certificate is used on the original server)
  - What happened
    - $150,000 in Ethereum was sent abnormally

Mis-originated BGP prefix was used to redirect to a phishing site.

- MyEtherWallet、DNSサーバーにハッキング、15万ドル分のETH盗難か https://jp.cointelegraph.com/news/myetherwallet-warns-that-a-couple-of-its-dns-servers-have-been-hacked
- AWS DNS network hijack turns MyEtherWallet into ThievesEtherWallet - The Register, 2018/4/24 https://www.theregister.co.uk/2018/04/24/myetherwallet_dns_hijack/

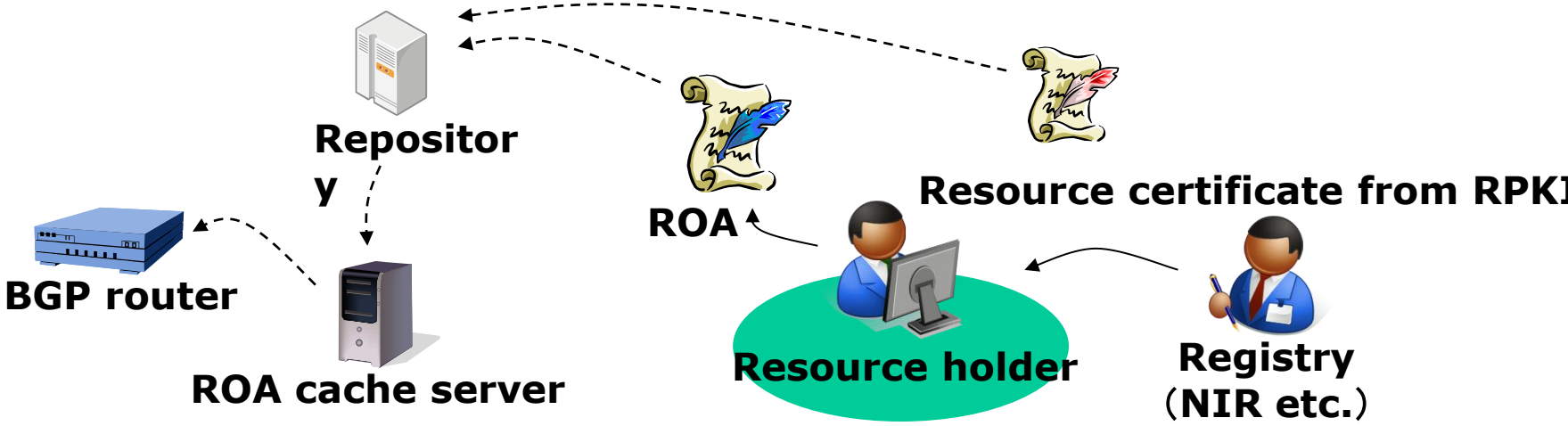
How RPKI is explained in Japan(3)



Mis-originated route (compared with route object registered in JPIRR) is detected regularly.

RPKI and ROA

- **Resource Public-Key Infrastructure**
  - A PKI for certify number resource allocations
- **Route Origin Authorization**
  - Signed object expressing an AS is authorized by resource holder to announce specific prefixes.
  - ROA can be used to compare BGP route to find mis-originated routes.



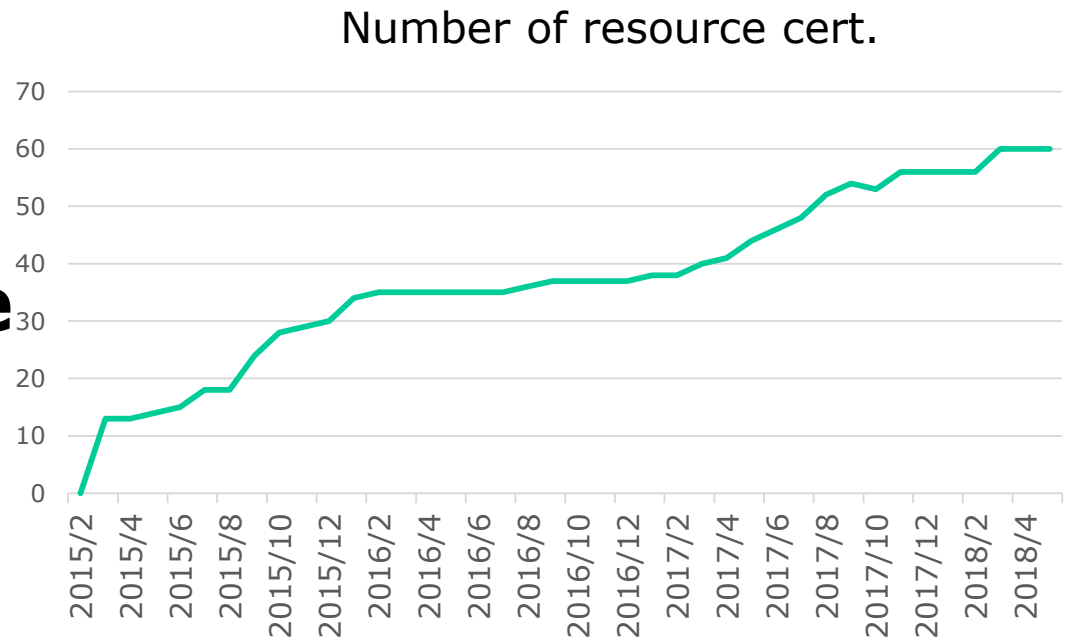
Origin validation using ROA

- **You can find mis-originated routes from Internet or customer.**
  - You may change priority of the route with preference value.

Only when resource holder issued ROA correctly.

Deployment status

- **Resource holder**
  - 60
- **ROA**
  - 248
- **Covering rate**
  - 3.3% IPv4
  - 38.1% IPv6



RPKI seminar in regular basis. The number of holders is increasing slowly.

Outreach Activities

- Tutorial course
  - Carries out regularly with hands-on seminar

- Provide information on our web page

https://www.nic.ad.jp/ja/rpki/

FAQ1

Q. I don't know which AS is announcing our IP address prefix…

A. Without ROA, mis-originated prefix cannot be found easily. Please consider to find correct AS this time.

FAQ2

Q. Some prefixes is used internally and not announce to the Internet.

A. ROA with AS "0" can express the prefix is not announced. It might help your historical address when other AS announced the prefix for sending spam or other malicious actions.

A hot issue

Q. An AS in Europe did not accept our prefix because ROA had shorter prefix length from announced prefix. What should we do?

A. It means that ROA management is getting more important than ever. And communication between customer support and network engineer also. (A customer reported this issue to ISP in this case.)

Thank you!

JPNIC Blog https://blog.nic.ad.jp/
(Sorry, All contents are written by Japanese)

JPNIC secretariat