

RPKI deployment experience in Japan

Hiroki Kawabata

Agenda

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

Key message

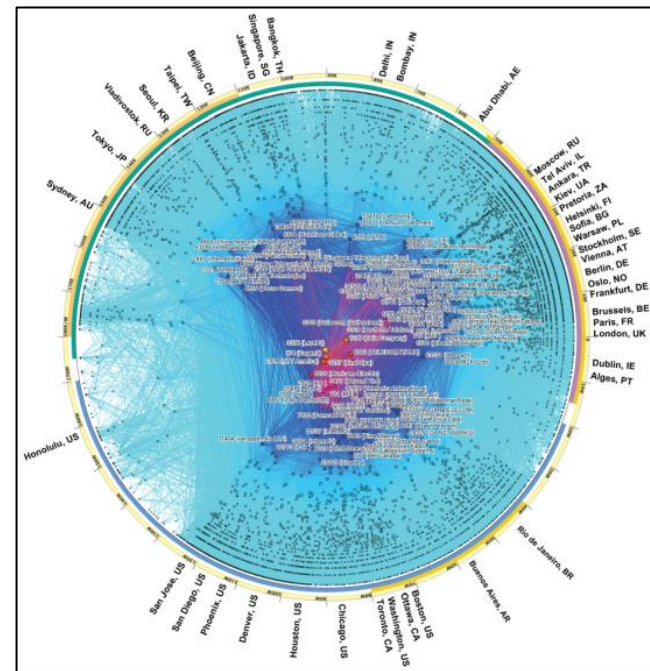
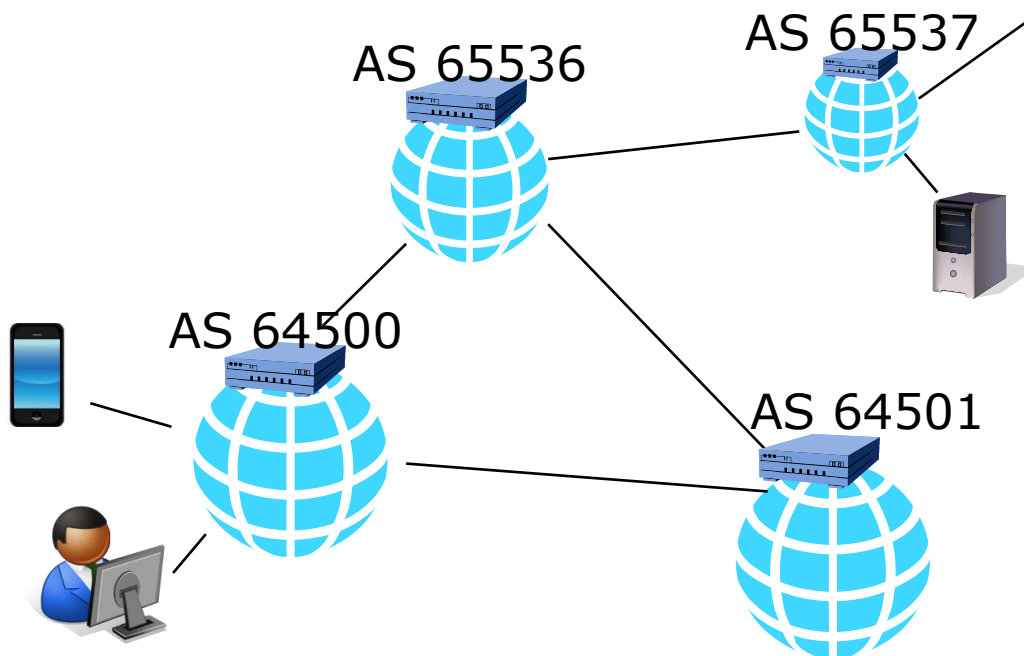
- **The era to know actual state of things**
 - The global routing system has been looked complicated. And it was seemed difficult to know it's whole figure.
- **For opening eyes on un-visualized things**
 - Build a tool to know actual use of address
 - Make more colleagues to go forward
 - Make standard to deploy for making our sight wider

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.

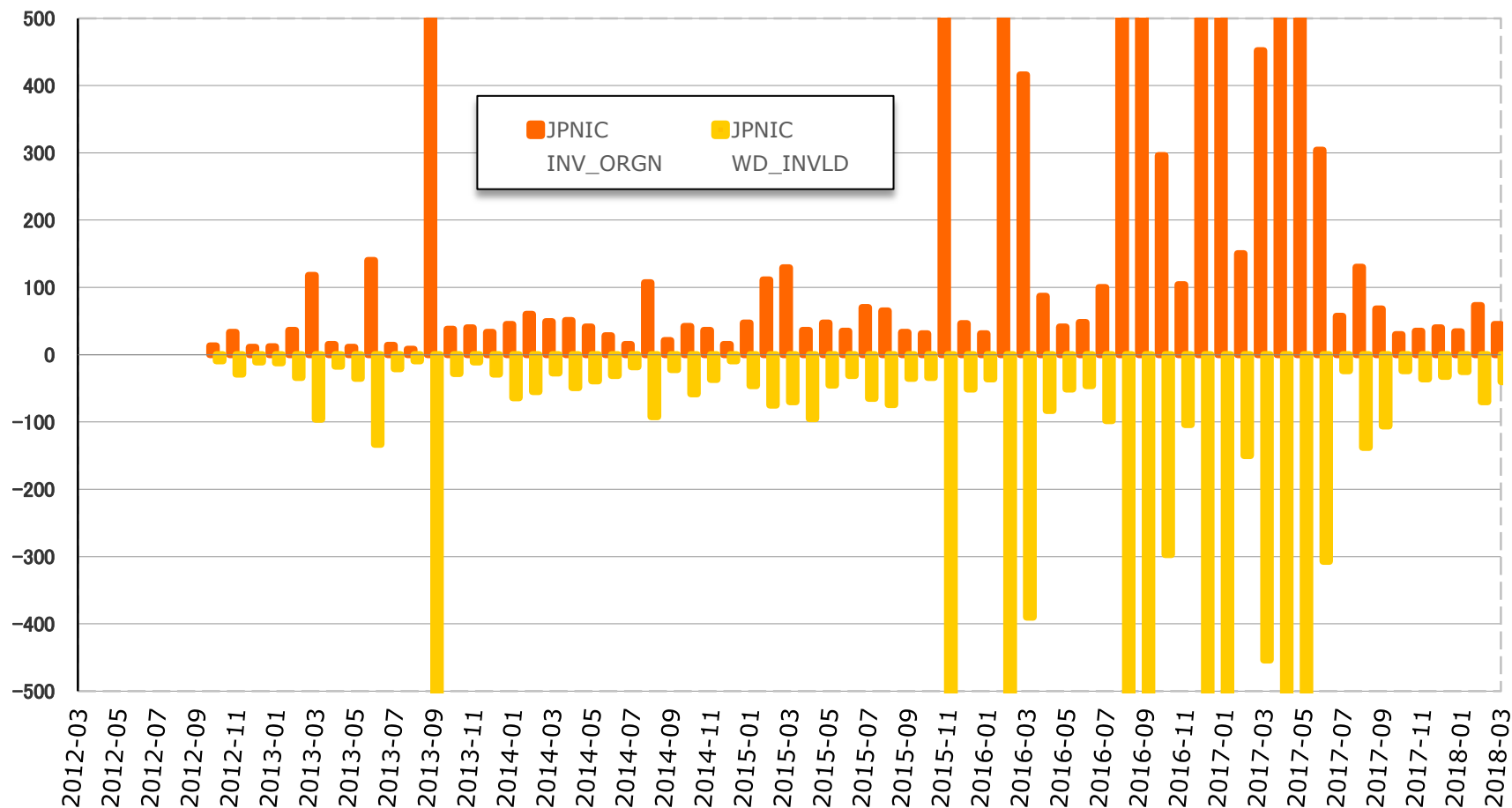
How RPKI is explained in Japan(2)

- **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/

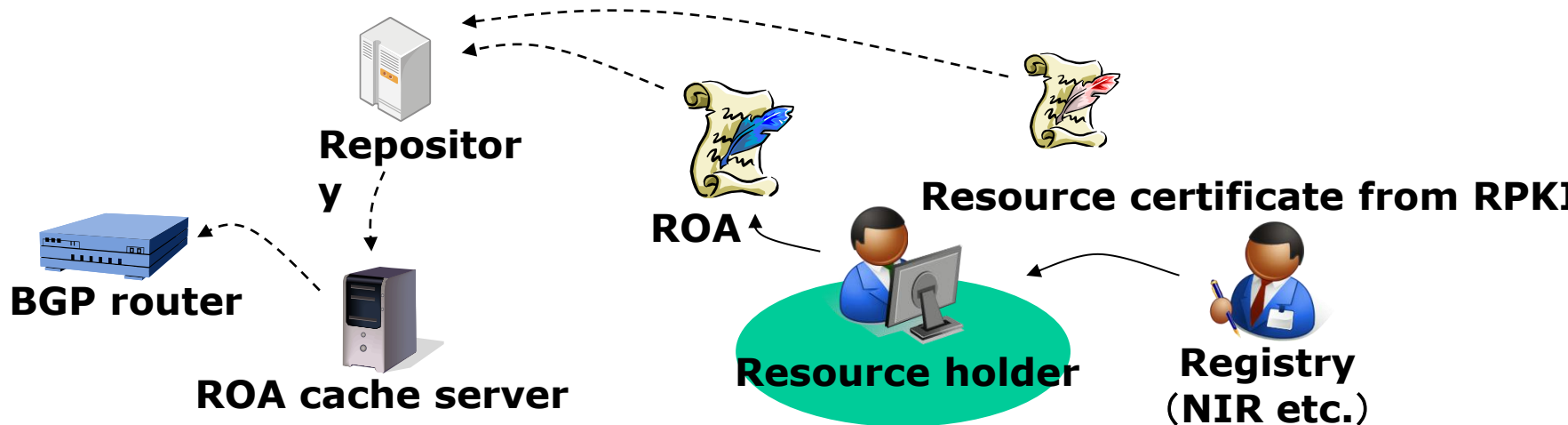
How RPKI is explained in Japan(3)



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

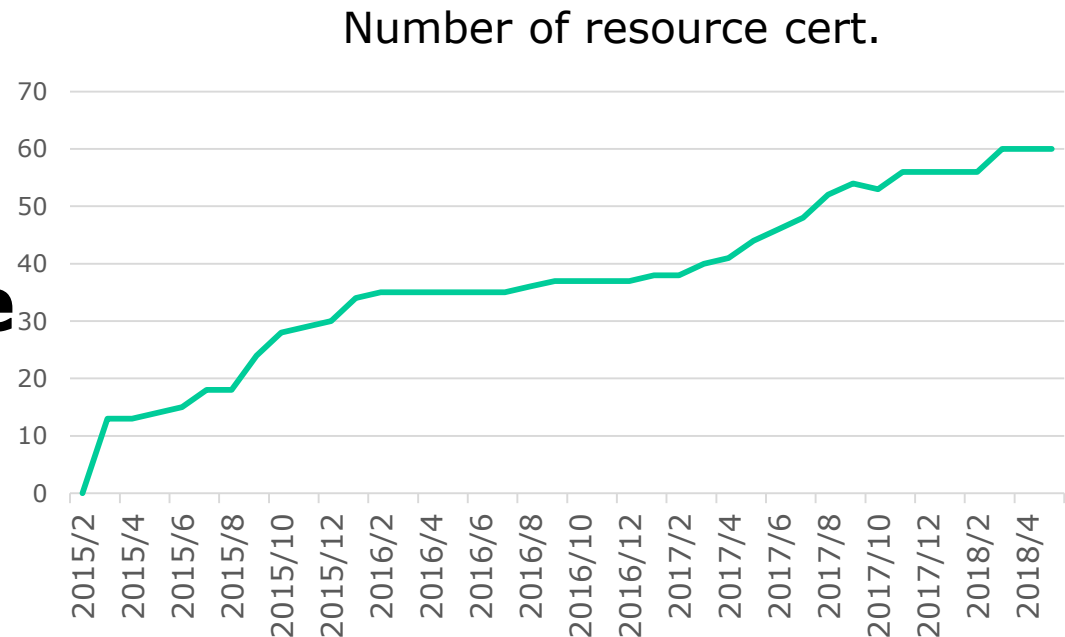
- **ROA**

- 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/>

JPNICはインターネットの円滑な運営を支えるための組織です

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
Japan Network Information Center

トップページ > インターネットの技術

リソースPKI(RPKI)

2015年2月25日

リソースPKI(RPKI)とは

リソースPKI(RPKI)は、アドレス資源の割り振りや割り当てを証明するためのPKI(Public-Key Infrastructure:公開鍵基盤)で、IPアドレスが正しく割り振られたものであるかどうかを確認できるほか、[BGPルータにおける誤ったインターネットの経路情報\(Mis-Origination\)](#)を見つけるために使えます。IPアドレスの割り振りや割り当てを証明するリソース証明書(Resource Certificate)と呼ばれる電子証明書はRPKIを使って発行されます。

BGPを使ったインターネットの経路制御では、「IPアドレス」と「インターネット上のネットワークを識別する番号(Autonomous System Number: AS番号)」が情報交換されます。リソース証明書は、IPアドレスとAS番号の正しい組み合わせを示すデータ「Route Origin Authorization(ROA)」を生成するために使えます。

- [リソースPKIとは\(インターネット用語1分解説\)](#)
- [ROAとは\(インターネット用語1分解説\)](#)
- [BGPルータにおける誤ったインターネットの経路情報\(Mis-Origination\)](#)

JPNICが提供するRPKI関連の仕組み

RPKIシステム

JPNICのRPKIシステムは、IPアドレスやAS番号のデータベースに基づいて、リソース証明書を発行するシステムです。APNICのRPKIシステムと連携しており、IPアドレスやAS番号の分配に応じてリソース証明書が発行されます。発行されたリソース証明書を使ってROA(Route Origin Authorization)を発行することとなります。

図1 RPKIとROAの概要(クリックで拡大します)

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 are used internally and not announced 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)



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
secretariat

Copyright © 2018 Japan Network Information
Center