How to ease deploying a security mechanism - ROV

Taiji Kimura
taiji-k@nic.ad.jp

JPNIC and RPKI

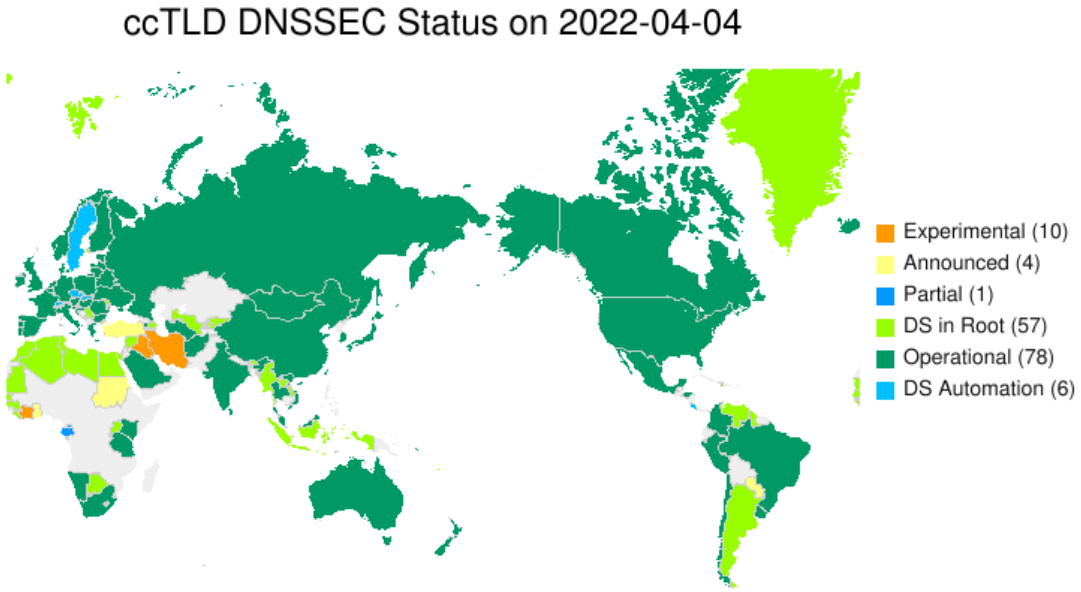
- **JPNIC is a NIR(National Internet Registry) in Japan.**
  - Number of LIR is 2,500 approximately.
- **RPKI**
  - Current ROA adoption rates IPv4 47.1%, IPv6 62%
  - History
    - 2000's Workshops
    - 2013 RPKI Hackathons
    - 2014 Trials using RPKI Tools
    - 2015 An experimental RPKI service (without BPKI with APNIC) - ROAWeb
    - 2017 BPKI with APNIC - ROAWeb

Contents

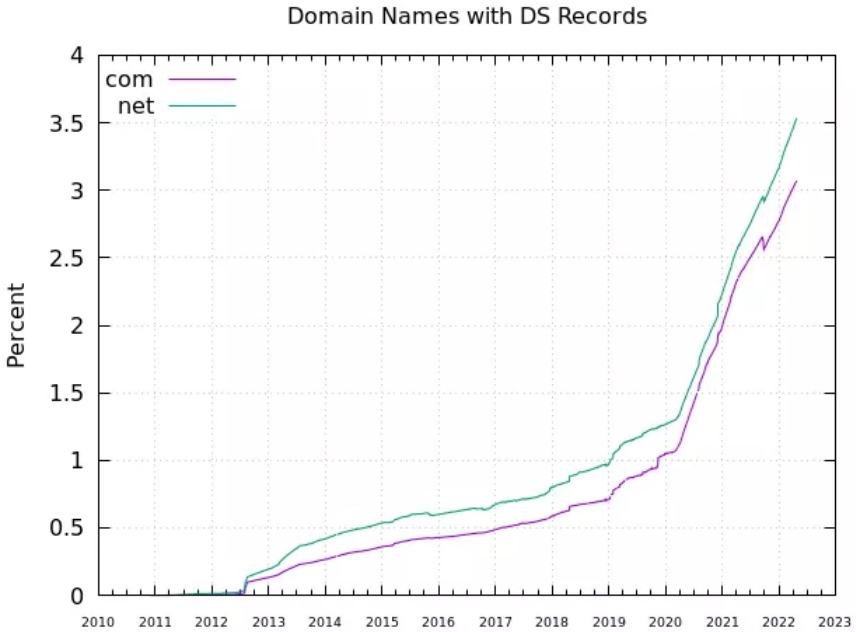
- Deploying a security mechanism is not easy
- WHAT
- WHO and WHERE
- WHEN
- WHY
- How to ease deploying a security mechanism - ROV

Deploying a security mechanism is not easy

DNSSEC signers --- ccTLD, .com and .net



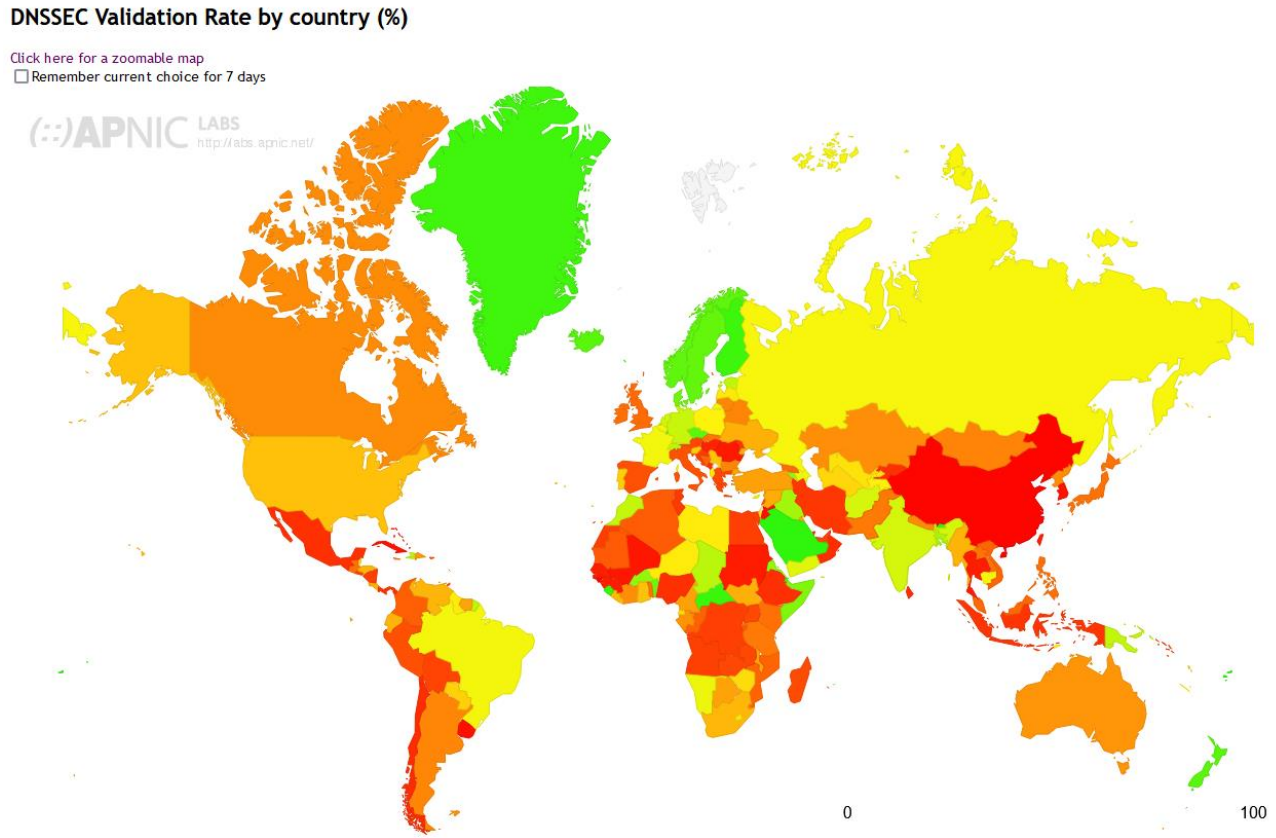
TLD DNSSEC deployment maps, ISOC, deploy360
You can subscribe mail-list from
https://www.internetsociety.org/deploy360/dnssec/maps/



DNSSEC Scoreboard: .com and .net Domain Names with DS Records - Verisign
https://www.verisign.com/en_US/company-information/verisign-labs/internet-security-tools/dnssec-scoreboard/index.xhtml

"Signing" is getting adopted. ccTLD has better adoption rate. For gTLD - .com and .net have higher adoption rate than before 2019.

DNSSEC validators



DNSSEC World Map
https://stats.labs.apnic.net/dnssec

"Validation" adopted sparsely. Except high-rate countries, many of them has low adoption rates.

Deploying a security mechanism is not easy

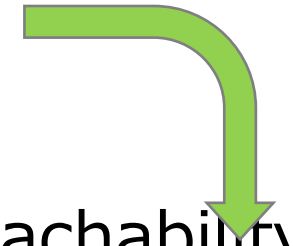
- **Scalable for worldwide: digital signature**
- **Digital signature-based mechanism requires two parties: “signers” and “validators”.**
  - Signing is designed not to have much risks.
  - Validating will have actual effects (and some risks!).
- **Deployment is always partial.**

Let’s look into ROV as partial deployed security mechanism.

5W

WHAT deploying ROV means

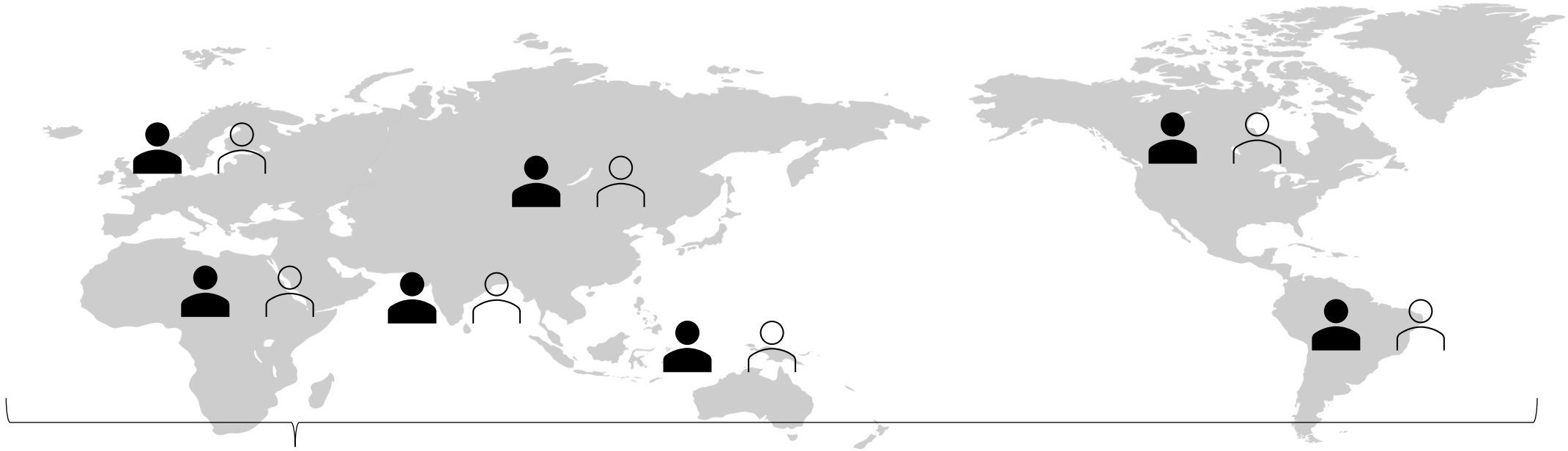
- **It is a matter of changing what is working.**
- **It will have good effects.**
  - Malicious BGP routes can have lower priority automatically.
- **It will have risks, but they are uncertain.**
  - “Invalid” prefix may have been used.
  - If your ROAs make “invalid”, it’s prefix can lose reachability.



Let’s clearly see what could happen.

And feedback loops for operators on ROA and ROV will be needed.

WHO and WHERE will be affected by ROV



Things happens anywhere:
- Invalid routes propagated
- ROA different from BGP routes

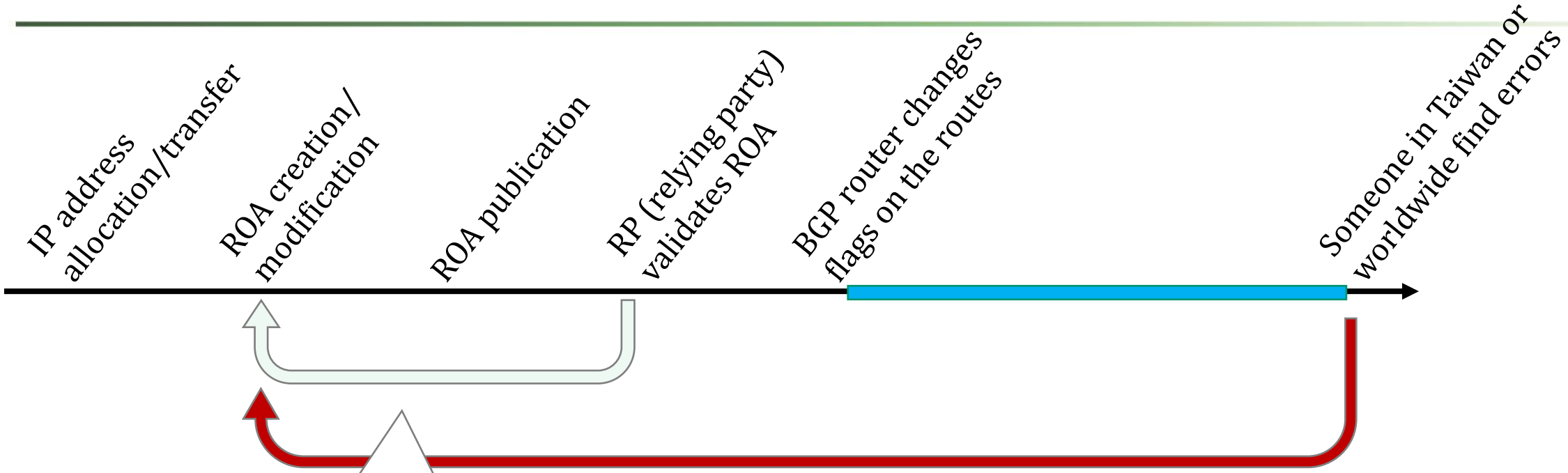
ROA operators (signer)

ROV operators (validator)

Mis-originated BGP routes can be coming from other networks and outgoing to them.

It is important to keep contacting not only among people within a community, but also among people from different communities.

WHEN ROV affects



Registry (TWNIC) or community can make this feedback loop to prevent errors for IP address in Taiwan.

To shorten the duration of the error (sky blue line), the red line feedback loop will be crucial.

WHY we deploy ROV and why didn’t do yet

- **ROV will make a protection on use of IP address in AS from mis-originated routes. They could happen in other networks or in your customer networks.**
- **But incidents do not happen often. Or we did not experience yet.**

Let’s find out clearly why we didn’t deploy ROV yet.
If we can know what will happen and can have confidence to manage them.

Summary: How to ease deploying a security mechanism - ROV

- **We know the mechanism is worthy to adopt but it has uncertainty because of its property.**

From 5W:

- If the reason not to deploy is uncertain-ness, let's clearly see what could happen when deployed partially.
- Needed feedback loops for invalid routes: In TWNIC, in Taiwan community and in other communities. They are also important as communication channels when error occurs.
- Let's make uncertain things into "confidence".

Confidence items (example):

- ROV can protect specific BGP routes
- Which routes will be invalid?
- Are there any users using it?
- How do we know errors and manage them?