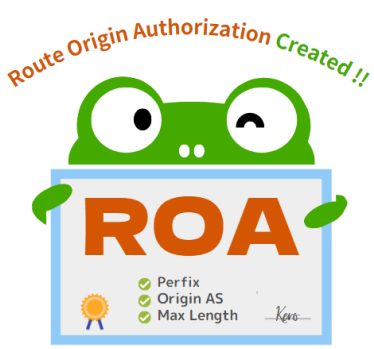
ROAキャン▲ 地域事業者がRPKIはじめてみて
～みんなの半歩が大きな一歩に～
@JANOG51

JPNIC　塩沢　啓

自己紹介

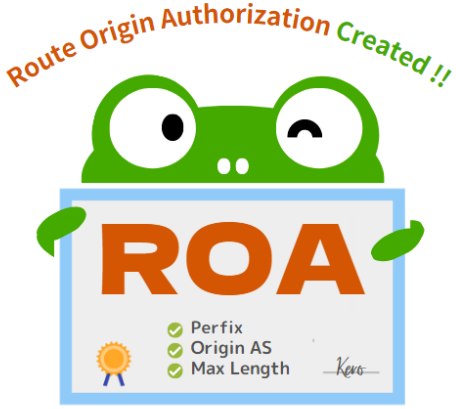
- **名前：塩沢　啓**
- **所属：JPNIC**
- **普段の業務：技術部・インターネット推進部**
  - BGP、DNS運用
  - セミナー/イベントの企画運営
    - 最近はオンライン開催の配信もやったり
- **JANOG歴**
  - J39@金沢で初参加、J45@札幌で初スタッフ/初登壇、今回は2回目の登壇
- **ROAキャン▲でもっとRPKIを広めたい**
  - 今回はケーロちゃん（JPNICのRPKIキャラクター）も ROAとROVに対応しました ☺ →



※JPNICのRPKIキャラクター：ケーロちゃん

第一部　RPKI動き出す、一歩
「動き出すまでの、歩み」

ROA発行の流れ



ROA発行の流れ

準備

- **資源管理者証明書を準備（資源管理カード／ブラウザ内）**
- **資源申請者証明書を担当者に発行（ブラウザ内）**

発行

- **JPNICのRPKIシステムでROAを発行 *https://rpki.nic.ad.jp/***

  ※ 自社でCA(Certificate Authority)を運用することも可能(BPKI: Business PKI)

確認

- **登録前後でROA発行状況を確認**
  - RIPE https://rpki-validator.ripe.net/ui/ , APNIC https://netox.apnic.net/ , JPNIC http://roa2.nic.ad.jp:8080/roas Cloudflare https://rpki.cloudflare.com/?view=validator , NLNOG https://irrexplorer.nlnog.net/ https://console.rpki-client.org/ などなど
- **登録前後のトラフィックの確認**
- **発行後は ROAと経路情報が乖離しないように！**

参考　JPNIC　ROAの作成と管理の方法 *https://nic.ad.jp/ja/rpki/howto-create-roa.html*
IRS33 ROA登録チートシート（長県大 岡田さん） *http://irs.ietf.to/wiki.cgi?page=IRS33*

JPNIC ROA Web

Web操作でROAの発行が可能

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

通常利用のRPKIシステムに加えて、
国内テスト用のRPKIシステムもあり

JPNIC ROA Web

- **ROAの管理**
  - 発行済みのROAが表示
- **ROA発行のできるリソース一覧**
  - **「ROAを作成」**をクリック

JPNIC ROA Web

ROAの発行に必要な情報を入力

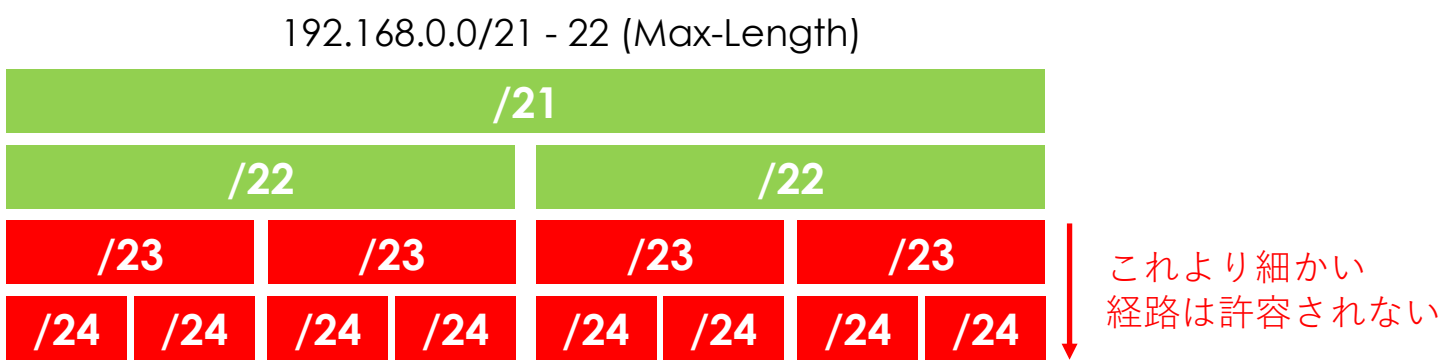
- Prefix
- Origin AS
- 最大prefix長（max prefix length）

JPNIC ROA Web

- **Prefix**
- **Origin AS**
  - 異なるOring ASのROAを複数発行することも可能
    - 自社の複数のASから経路広告する場合
    - クラウドサービスなど他ASから経路広告する可能性がある場合 など
- **最大prefix長（max prefix length/max length）**
  - ROAで許容される最大のプレフィックス長
  - Max-Length を不必要に長くする事は推奨されない (ref RFC9319)
    - 原則、経路情報と一致させるような設定が推奨
    - Origin詐称による経路ハイジャックのリスクを低減

(ex) 192.168.0.0/21のROA

✓ Prefix	192.168.0.0/21
✓ Origin AS	64500
✓ Max Length	/22

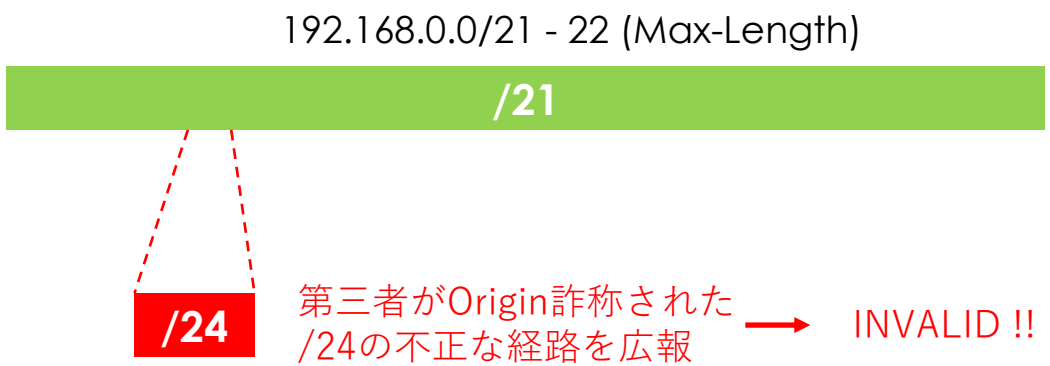


JPNIC ROA Web

- **Prefix**
- **Origin AS**
  - 異なるOring ASのROAを複数発行することも可能
    - 自社の複数のASから経路広告する場合
    - クラウドサービスなど他ASから経路広告する可能性がある場合 など
- **最大prefix長（max prefix length/max length）**
  - ROAで許容される最大のプレフィックス長
  - Max-Length を不必要に長くする事は推奨されない (ref RFC9319)
    - 原則、経路情報と一致させるような設定が推奨
    - Origin詐称による経路ハイジャックのリスクを低減

(ex) 192.168.0.0/21のROA

✓ Prefix	192.168.0.0/21
✓ Origin AS	64500
✓ Max Length	/22



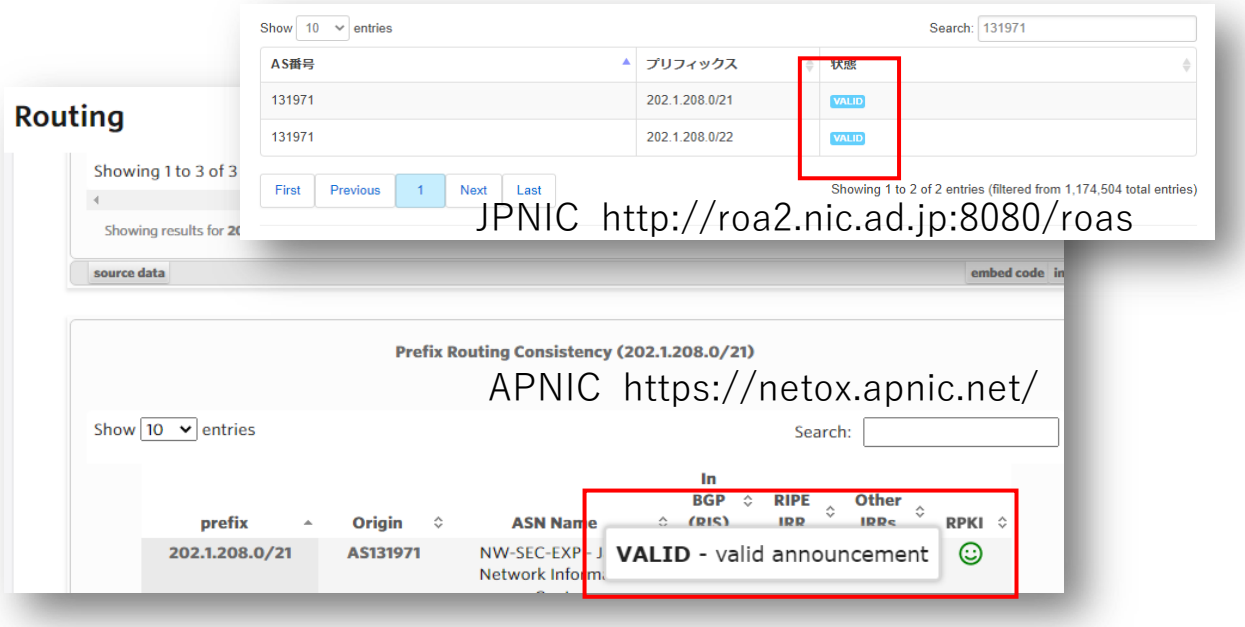
JPNIC ROA Web

ROAのプレビュー画面

- 観測されている経路情報とROVの状況が表示
- Invalidの場合は注意！

JPNIC ROA Web

- ROAが発行済になりました



外部からもVALIDになっているか確認！

第一部　RPKI動き出す、一歩
「動き出すまでの、歩み」

RPKIの動向と、普及に向けたこれまでの活動実績や課題感

RPKIとROAのこれまで

(*) Secure Inter-Domain Routing WG

IETF動向

sidr(*) WG started

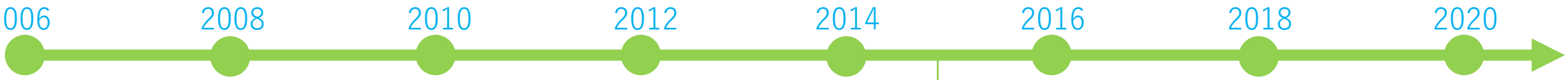
ROAとROVに関するRFC
RFC 6482 ROA profile
RFC 6486 Resource cert. profile
RFC 6810 RTR
RFC 6490 TAL
RFC 6811 Origin Validation

sidrops WG started

sidr WG concluded

RFC8182 RRDP

ASPAの議論



RIR/NIR動向

RPKI in MyAPNIC

RIPE NCC's beta testing

RPKI.NET

JANOG
RPKIルーティングを試す会

JPNIC RPKI Started

JPNIC/APNICで
RPKIの連携開始

ROA/ROV 標準化

徐々に普及期

ROAのこれから

OBSERVATORY | ROUTING SECURITY

Will 2023 be the Year Half of the Internet is RPKI-Enabled?

By Aftab Siddiqui • 16 Jan 2023

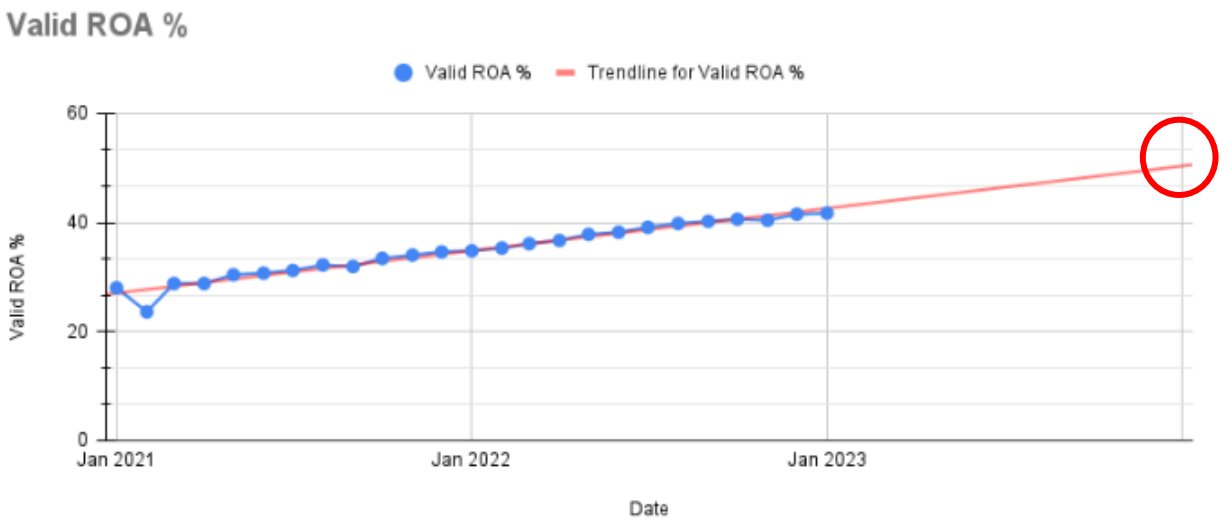


Figure 11 – Percentage of valid RPKI-enabled resources (IPv4 and IPv6) based on RIPE Stat and NIST RPKI monitor.

- 前年よりもルーティングインシデントの発生件数は多かったが、**RPKIの利用が普及したため深刻な被害には至らなかった**
- 2023年末には、**ValidなROAの割合が50%以上**になると予測

Will 2023 be the Year Half of the Internet is RPKI-Enabled ?, Aftab Siddiqui, MANRS
https://www.manrs.org/2023/01/will-2023-be-the-year-half-of-the-internet-is-rpki-enabled/

ROVの実装

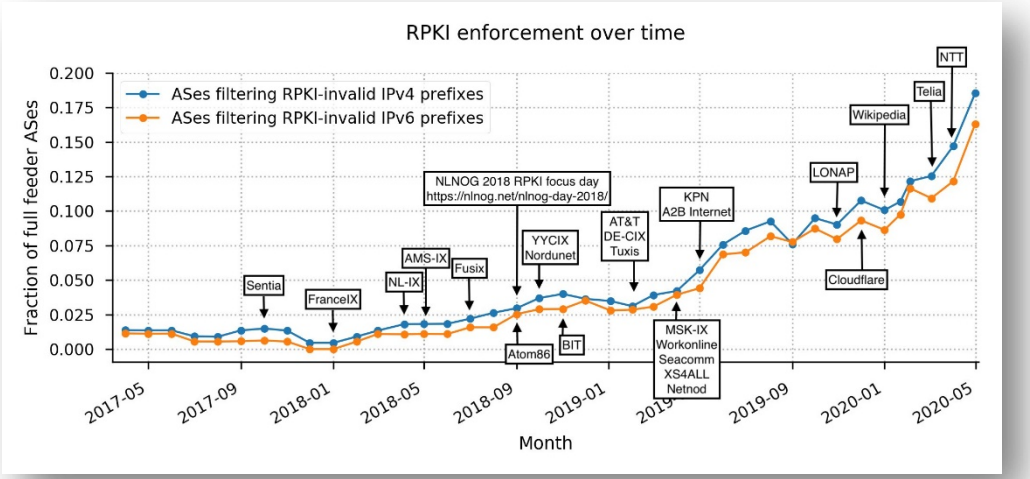
RoVista

Overview of ROV Filtering Ratio

Show: 10 Search:

Rank ▲	ASN	Country	Organization	ROV-Ratio
1	3356	United States	Level 3 Parent, LLC	1
2	1299	Sweden	Telia Company AB	1
3	174	United States	Cogent Communications	1
4	3257	United States	GTT Communications Inc.	1
6	2914	United States	NTT America, Inc.	1
7	6939	United States	Hurricane Electric LLC	1
8	6461	United States	Zayo Bandwidth	0
9	6453	United States	TATA COMMUNICATIONS (AMERICA) INC	1
10	3491	United States	PCCW Global, Inc.	1
11	1273	European Union	Vodafone Group PLC	0

https://rovista.netsecurelab.org/



https://twitter.com/JobSnijders/status/1256326712347881473

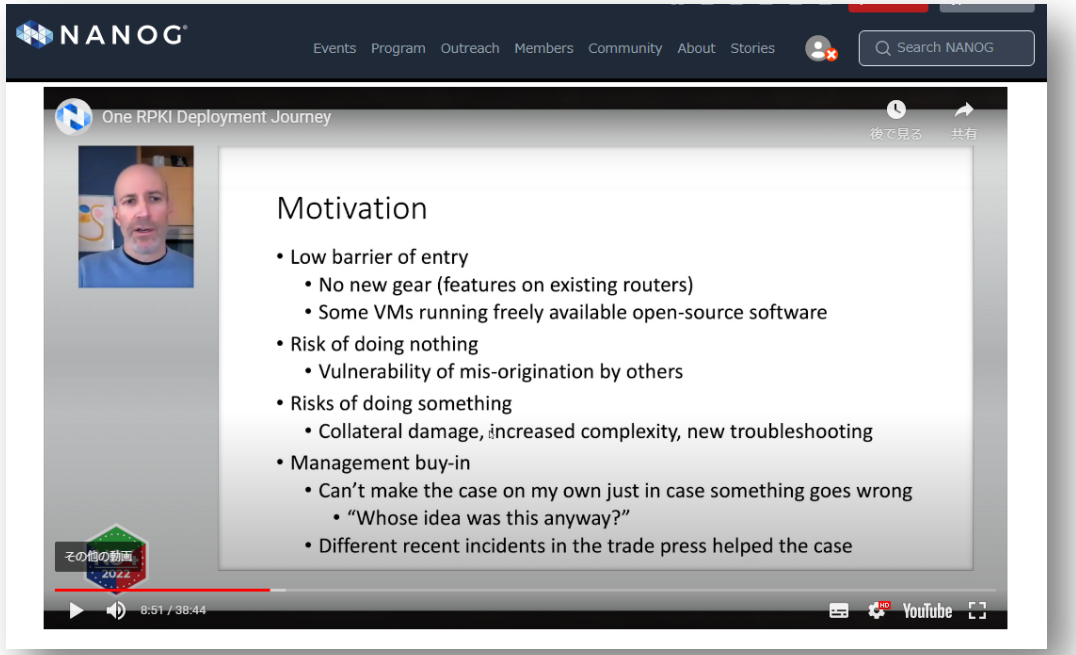
- **RoVista**：27,000以上のASのROV実装状況を測定
- **Tier 1を中心にROVを実装**していることが判明
  - Level 3 (AS 3356), Telia (AS 1299), GTT (AS 3257), NTT America (AS 2914), TATA Communications (AS 6453), PCCW Global (AS 3491), Orange (AS 5511), AT&T (AS 7018), Liberty Global (AS 6830), Sprint (AS 1239), and CenturyLink (AS 209)

国際的な通信事業者やIXを中心にROVの実装も進む

Take Survey to Help Validate ROV Adoption Measurements, Taejoong Chung, MANRS
https://www.manrs.org/2023/01/take-survey-to-help-validate-rov-adoption-measurements/

ROVの実装

Comcast のROVを導入したモチベーション



- **すでに一部の大手ISPではROVが行われている**
  - Invalidなプレフィックスはすでに落とされている
- **参入障壁が低い**
  - 新しい機材が不要（既存のルータに搭載可能）
  - 自由に利用できるオープンソースソフトウェアを実行するVMもある
- **何もしない場合のリスク**
  - 他者による誤った広報の可能性がある
- **何かした場合のリスク**
  - 巻き添え被害、複雑性の増大、新たなトラブルシューティングの発生

Tony Tauber, One RPKI Deployment Journey, NANOG 84
https://www.nanog.org/news-stories/nanog-tv/nanog-84/one-rpki-deployment-journey/

RPKI普及に向けた活動とこれまでの課題感

- **RPKI普及状況：海外、日本国内でも徐々に普及**
  - ROA：カバー率は年々上昇している
    - まずはROAの発行から！
    - 過去に発行したことがあったなという方は今一度確認を。現在の経路情報と乖離がないような運用も。
  - ROVは国際的な通信事業者やIXを中心に実装されてはじめている
- **JPNICにおける普及活動**
  - コミュニティの場などで最新動向発表、ハンズオンセミナー開催
    - JANOG、地域NOG、Internet Week、IRS etc…
    - ROA Webの使い方や、ROVを体験するハンズオン
      - オンライン開催で場所を問わず今までより気軽に参加
- **日本国内の登録数も増えるが、一方で地域の事業者との取り組みが課題に…**
  - オンラインセミナーなど気軽に参加いただけるが、密なコミュニケーションは取りづらい。
  - RPKI/ROAの普及に向けて、みんなが「一歩、動き出す」にはどうすればいいか？

第二部　新技術 普及する、一歩

第二部　新技術 普及する、一歩

- **RPKIに限らず、インターネットをより安全にするための技術**
  - ルーティング
  - DNS
  - アプリケーション
    - メール、Web　etc...

第71回JPNIC総会 座談会「インターネットを守るための技術普及を官民で考える」より
https://youtu.be/ijP6QSQxfA0

第二部　新技術 普及する、一歩

「一歩、動き出す」ためのオモテとウラの取り組み…

- **オモテ**
  - 継続的な情報発信
  - 先駆者達のknow-howを共有
  - コミュニティのbest practiceを議論
  - 産学官の連携

- **ウラ**
  - コミュニティの活用
    - みんなでやっていこう
    - 何かあったら助けられる環境
  - 一緒に悩める仲間作り！

新技術の普及について、うまくいった経験や取り組んでいる事例、
こうしたらもっとうまくいくという事があったら教えてください！