

RPKIやROA登録ってなんで必要なの？ 初歩からひも解いていったお話(仮)

2021/11/30

長崎県立大学情報システム学部 真崎かれん

自己紹介

名前: 真崎 かれん

所属: 長崎県立大学情報システム学部情報セキュリティ学科4年



情報セキュリティ産学
共同研究センターが建
設中

研究テーマ

「BGPにおけるAS番号とそのIPアドレスの組を蓄積するIRR(既存のDB)とROA(PKIベースの電子署名付き)を比較し、IRRのデータの正確性を検証する」 → IRRの登録状況の調査

```
IRR>ROA|158.247.0.0/16|AS8159|158.247.192.0/18|AS20473|JP
IRR=ROA|210.188.192.0/19|AS9371|210.188.222.0/24|AS10013|JP
IRR=ROA|210.188.192.0/19|AS9371|210.188.201.0/24|AS131965|JP
IRR=ROA|210.188.192.0/19|AS9371|210.188.210.0/24|AS10013|JP
IRR=ROA|210.224.160.0/19|AS9371|210.224.183.0/24|AS10013|JP
IRR<ROA|218.216.96.0/23|AS17954|218.216.96.0/20|AS17675|JP
IRR>ROA|150.35.0.0/16|AS4713|150.35.240.0/24|AS14418|JP
IRR>ROA|150.35.0.0/16|AS4713|150.35.240.0/24|AS16509|JP
IRR<ROA|202.249.24.0/22|AS4717|202.249.0.0/17|AS2500|JP
IRR<ROA|202.249.47.0/24|AS4717|202.249.0.0/17|AS2500|JP
IRR<ROA|203.9.176.0/23|AS4648|203.9.176.0/21|AS22822|JP
```

	AS	件数
IRR==ROA	○	-
	×	137
IRR⊃ROA	○	-
	×	228
IRR⊂ROA	○	-
	×	815

BGP(Border Gateway Protocol)

192.0.2.0/24はAS2515
にあるよ

BGP:ASどうしをつなげるルーティングプロトコル

ASどうしがBGPルーターにIPアドレスをAS番号のセットを飛ばしあって情報を共有しています。

このとき、受け取った情報(オリジン)が本当に正しい内容なのか証明されていません。

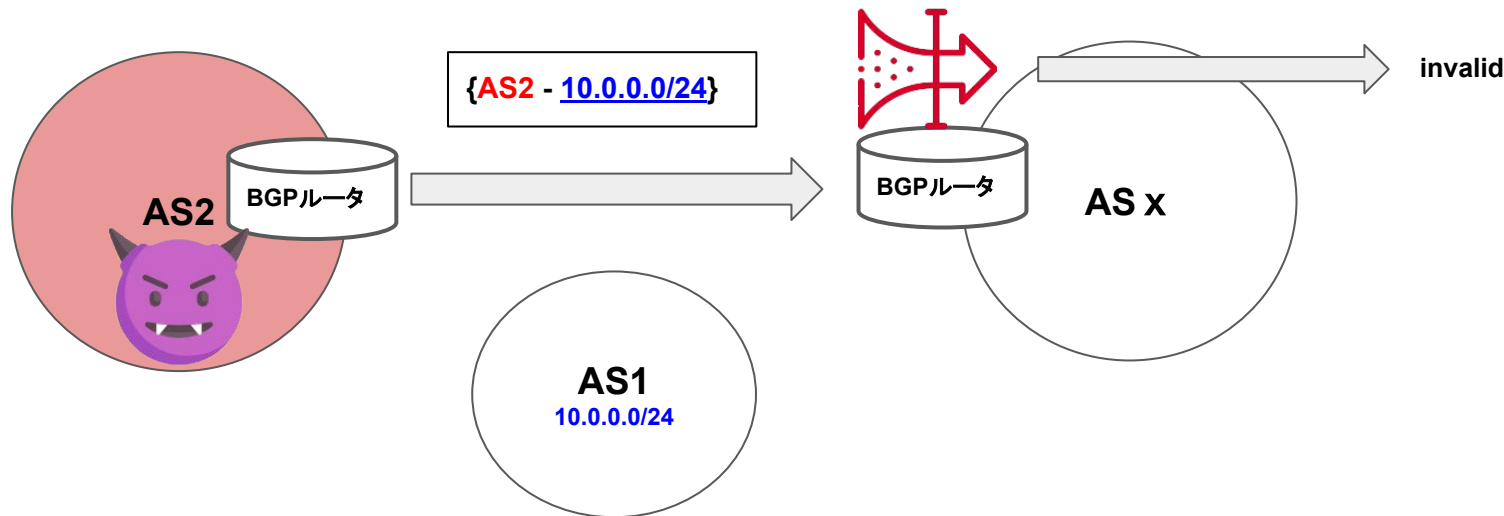
正しい内容かどうかを判断するために、IRRまたはROAを用いた**オリジン検証**をしています。



なぜオリジン検証が必要なのか...

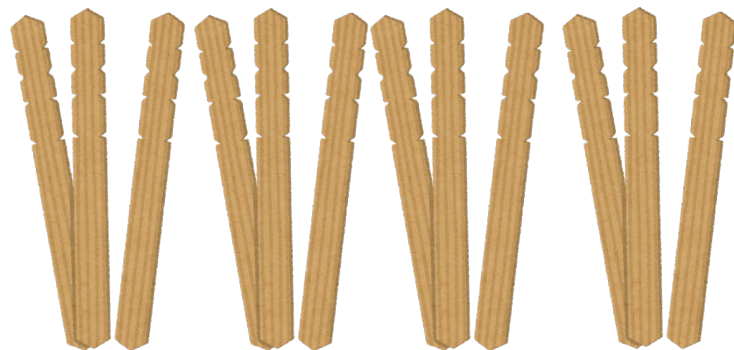
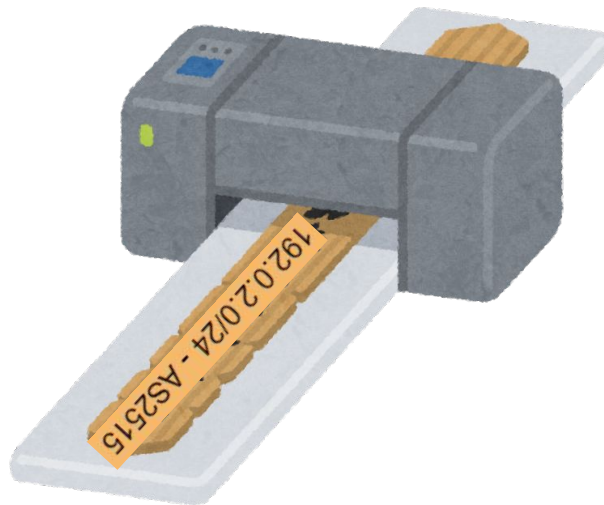
- 悪意に対して(うっかりミス含む)
 - 経路の乗っ取りを見分けるため
 - 経路情報とASの対応関係が正しいかどうか
 - 悪意: 迷惑メール送信などの悪意のもとをたつ
 - うっかり: 運用ミスを素早く検知して知らせるため
- 必要な経路制御に対して
 - 一見乗っ取りにみえる経路を自らの意思でやっていると言
 - DDoS救済サービス
 - エニーキャスト
 - GSLB
- 悪意を見つけたり、経路制御上必要な状態かを見分けたりするためにオリジン検証が必要

オリジン検証



IRR(Internet Routing Registry)

立て看板、卒塔婆。あるIPアドレスがこのAS番号にあると宣言しています。
卒塔婆によって受け取った広告が正しい内容かを判断できます。



お寺によってはろくに管理されず、ぼろぼろ(古い情報)だったり他人のIPアドレスやAS番号を宣言することもできます。

203.151.73.0/24

```
route: 203.151.73.0/24
descr: CMI (Customer Route)
origin: AS38082
mnt-by: MAINT-AS58453
changed: qas_support@cmi.chinamobile.com 20180906
source: RADB
```

```
route: 203.151.73.0/24
descr: CAT route object for CS Communication
origin: AS7568
mnt-by: MAINT-THIX-CAT-TH
changed: ktanus@cat.net.th 19991125
source: RADB
```

```
route: 203.151.73.0/24
descr: Proxy-registered route object
origin: AS4618
notify: radb@hutchcity.com
mnt-by: MAINT-AS9304
changed: radb@hutchcity.com 20120325
source: RADB
```

```
route: 203.151.73.0/24
descr: Ad Venture
origin: AS4741
mnt-by: MAINT-SAMART-TH
changed: yut@samart.co.th 19991102
source: RADB
```

RADBでは、全く同じIPアドレスが複数登録されていることも。。。

検索した側が判断するしかない、、、

ROAなら重複することもない

AS4618, 203.151.64.0/19, 20

いろいろな宗派がある

IRRを運営する団体を宗派とすると様々な宗派があります。

最も多いのは、MERIT山のRADbです。

ここでは、お布施さえ払えば自由に IPアドレスとAS番号を宣言できます。

List of Routing Registries

This list was designed for the Internet community. It enables users to coordinate their Routing Registry efforts by providing mirroring and contact information.

- AFRINIC
- ALTDB
- AOLTW
- APNIC
- ARIN
- ARIN-NONAUTH
- BELL
- BBOI
- CANARIE
- EPOCH
- HOST
- IDNIC
- JPIRR
- LACNIC
- LEVEL3
- NESTEGG
- NTTCOM
- OPENFACE
- PANIX
- RADB
- REACH
- RGNET
- RIPE
- ROGERS
- TC

IRRの問題

最も信者の多いRADbでは管理が行き届いていないため、ぼろぼろな卒塔婆や他人の情報を勝手に宣言している卒塔婆も乱立しています。

卒塔婆 = ルートオブジェクト

ルートオブジェクトの例

この卒塔婆を用いてオリジン検証をできますが、信頼度は低いです。

203.151.73.0/24

```
route:      203.151.73.0/24
descr:      CMI (Customer Route)
origin:      AS38082
mnt-by:      MAINT-AS58453
changed:     qas_support@cmi.chinamobile.com 20180906
source:      RADB
```

```
route:      203.151.73.0/24
descr:      CAT route object for CS Communication
origin:      AS7568
mnt-by:      MAINT-THIX-CAT-TH
changed:     ktanus@cat.net.th 19991125
source:      RADB
```

```
route:      203.151.73.0/24
descr:      Proxy-registered route object
origin:      AS4618
notify:      radb@hutchcity.com
mnt-by:      MAINT-AS9304
changed:     radb@hutchcity.com 20120325
source:      RADB
```

```
route: 203.151.73.0/24
descr: Ad Venture
origin: AS4741
```

IRRの問題点

- IPアドレスの保有者の意思(=AS番号)が登録されてるかわからない
- 情報の改ざんなどの検出ができない

そこで、PKIの仕組みをつかって、電子的に解決しようとした

RPKI(Resource Public-Key Infrastructure)

RPKIとは、アドレス資源の割り当てや割り振りを証明するための PKI

PKI

公開鍵とその所有者を結びつける



RPKI

リソース資源とその割り当てを受けた人を結びつける

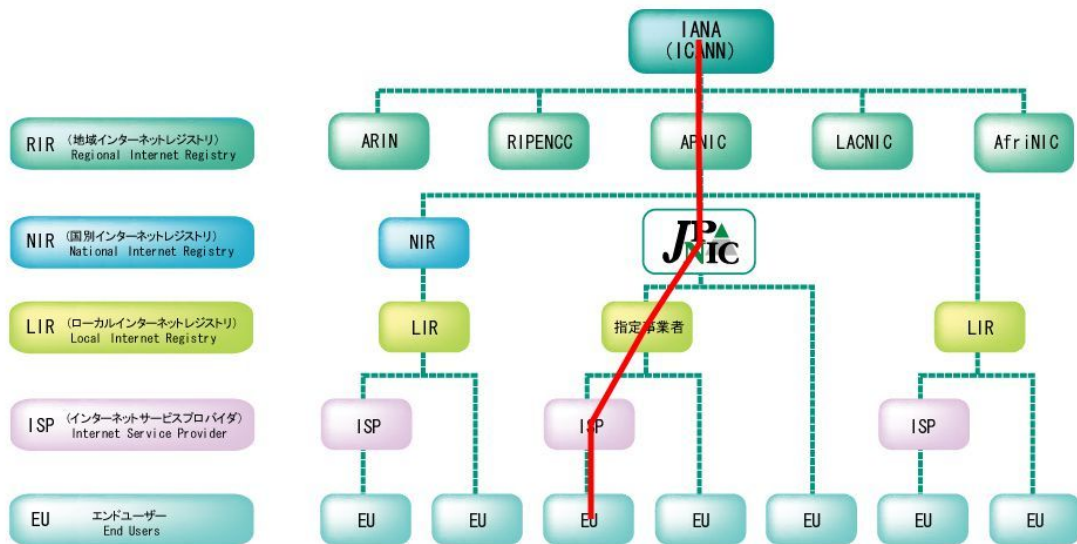
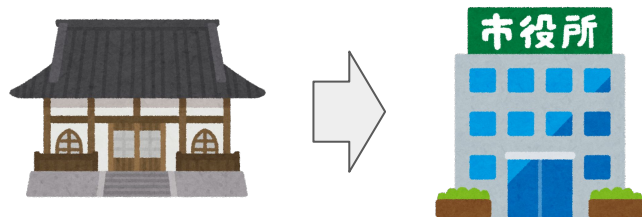


IPアドレス
AS番号...



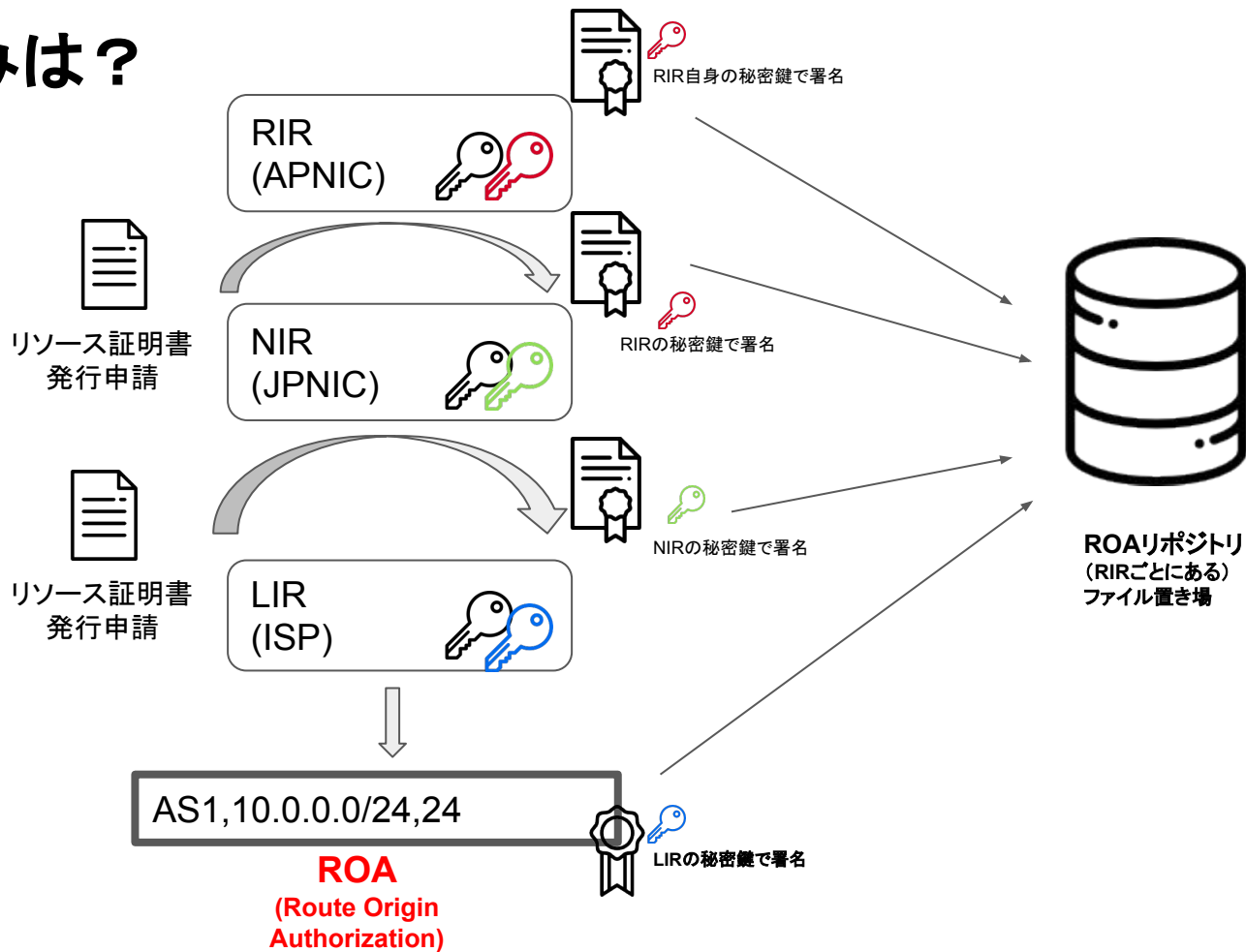
RPKI(Resource Public-Key Infrastructure)

IRRの管理者がお寺だったのに対し、
RPKIでは上下構造のある役所が管理しています。

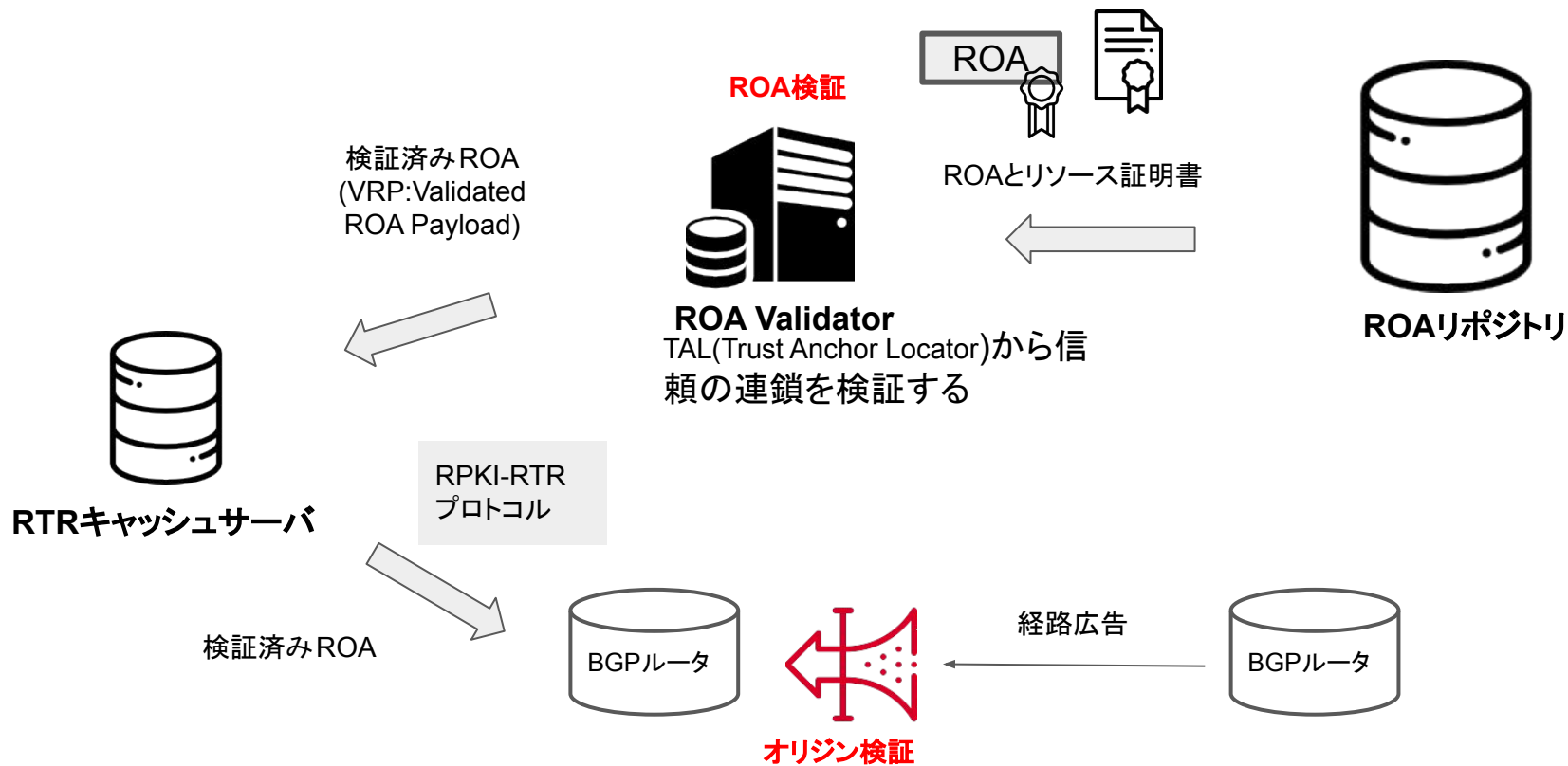


<https://www.nic.ad.jp/ja/ip/ipv4pool/img/admin.jpg>

RPKIの仕組みは？



オリジン検証の流れは？



RPKIって何？

- ✓ IPアドレスやAS番号の正しい利用者を証明する
- ✓ オリジン検証に利用されている
- ✓ IRRより信頼度が高い

RPKIがあればバラ色...？

- 相互運用性 → ルータとRPKIキャッシュサーバの相性
- リポジトリからROA収穫に要する時間 → まちまち
- そもそもAS番号を詐称したASはvalidになる → パス検証が必要

そのほかにもいろいろ。。。

事業者さんと共同研究にてこのあたりを調査中

IPアドレスとASの申請をしました！

お願い

IPアドレスの管理者が登録しないとROAは増えていかない

BGP運用者は自分のところで利用するかどうかは置いといて、とにかくROAの登録をしましょう。