長崎県立大学
UNIVERSITY OF NAGASAKI

# C8 明日のインターネットをみんなで守る ルーティングセキュリティ 運用に向けた課題

2021年11月22日

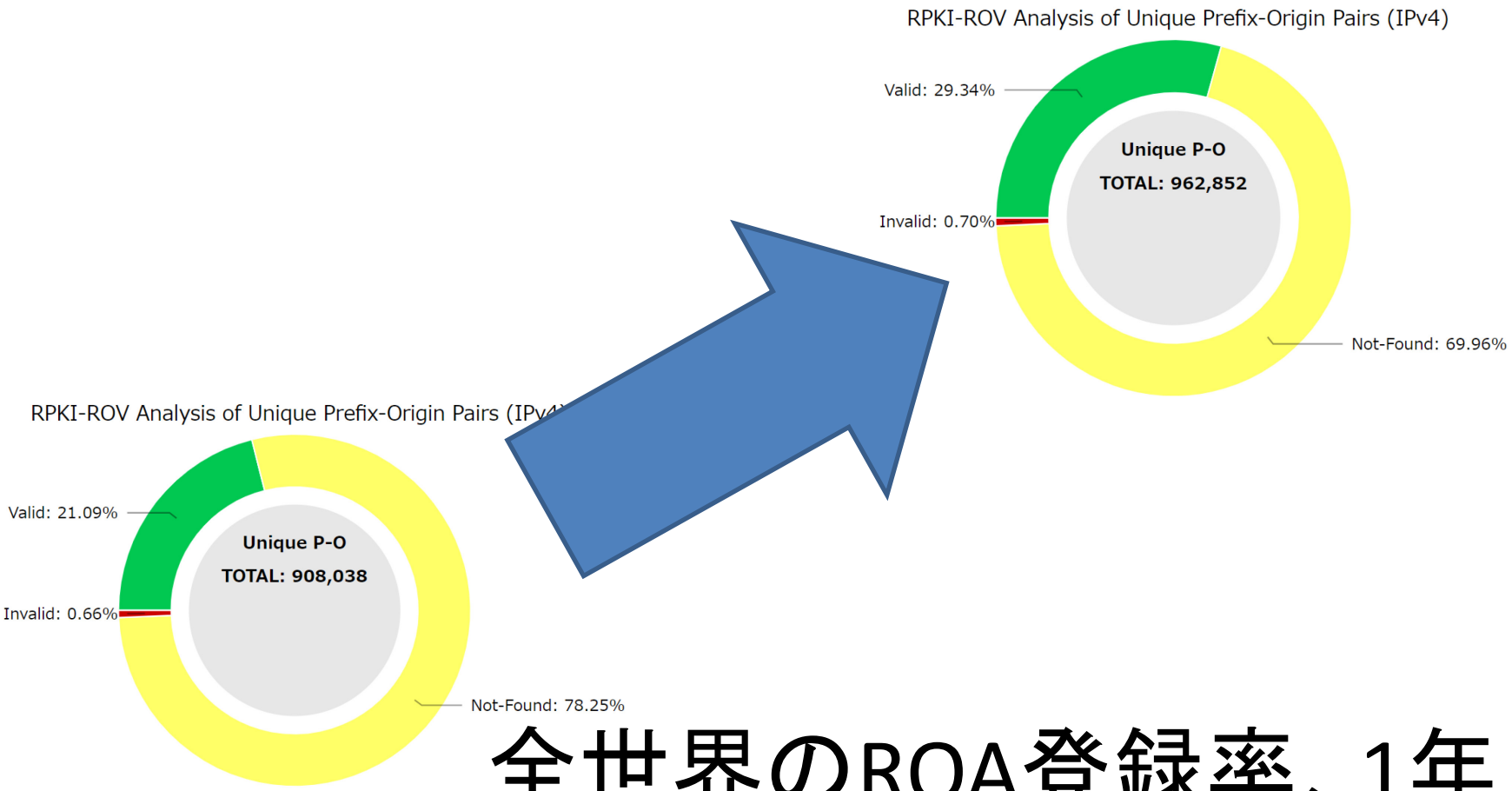
長崎県立大学 岡田 雅之

# RPKIとOrigin Validation普及状況

長崎県立大学
UNIVERSITY OF NAGASAKI

- 2000年よりRPKIの準備がインターネット配布組織にて開始
- 2008年より実際のRPKIシステムが提供開始
  - 日本では、2016年から開始
- 参照ソフトウェアのリリース
  - RPKI情報を収集し、ルータへ中継するRPKI-RouterProtocolの実装と改善
- ルータの実装
  - 初期の実装は重大事故に結びつくRPKI機能拡張があり、改善が継続した

# RPKI導入の現状




全世界のROA登録率、1年で20%→30%へ増加中

# RPKI参照組織の増加

長崎県立大学
UNIVERSITY OF NAGASAKI

- IIJ
- NTTCOM-GIN
- Level3
- Orange（France-Telecom）
- CloudFlare
- Akamai
- AMS-IX
- DeCIX
- COMCAST
- LINX
- JPNAP
- ○○IX
- その他、EU地域AS複数

# 普及のハードル

長崎県立大学
UNIVERSITY OF NAGASAKI

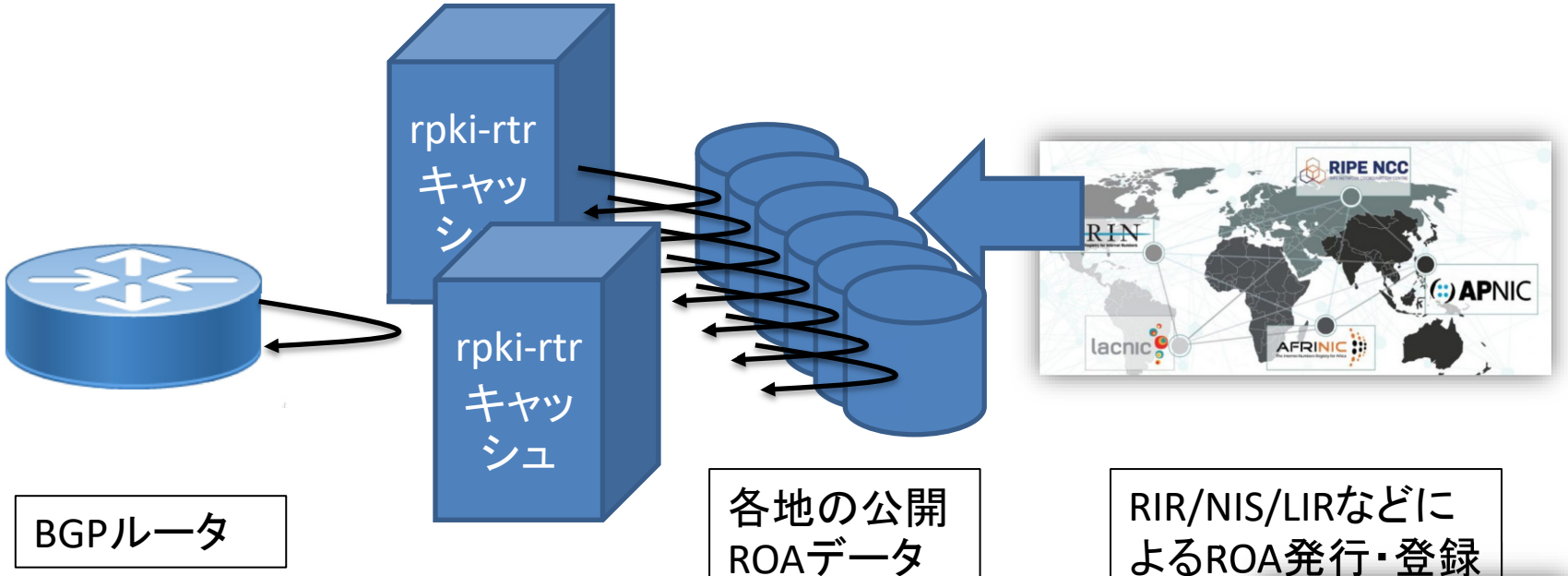
- BGPルーティングが上位プロトコル併存
  - RPKI、ROA収集に**DNSや転送プロトコル**を利用
- インターネット停止ボタンにつながりかねない
  - 政府や悪意のある組織により、証明書を失効
    - これにより経路が停止する
- インターネット運用者の習熟
  - RPKI/ROA参照ルーティングの経験がほぼ0
- RPKI-RTRプロトコルキャッシュの信頼性
- ROA登録の習熟
  - IPアドレス担当者から登録が必要
  - とはいえまずは登録から始めましょう。登録登録登録

# 現在も考えられる課題

長崎県立大学
UNIVERSITY OF NAGASAKI

- ARINのルート証明書問題
  - 北米地域のROA活用には北米地域のレジストリが提供する頂点の証明書が必要
  - しかしながら、その証明書には非常に利用者側に不利な同意が必要なことにより、北米だけ参照が欠落している
- Origin AS偽装問題
  - 悪意を持つASにとって、AS-PATHを偽装し、Origin-ASを偽装された場合Origin-Validationでの防衛は困難
    - BGPSEC PATH Validationが研究中

# rpki-rtr キャッシュの重要性

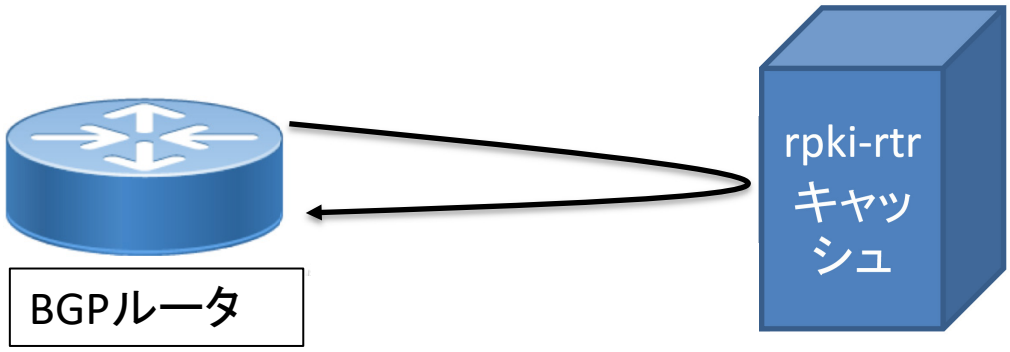



動作の流れ

1. rpki-rtrキャッシュに設定されたRPKIツリーの頂点からROAを収穫してゆく
2. ROAの収穫は、現状、最短5分～状況によっては30分程度
3. 収穫したROAのうち、電子署名の署名検証がOKなものだけをBGPルータへ出荷
4. BGPルータからのrpki-rtrの要求により、正しいIPアドレス/AS番号/Maxlenの組み合わせをお知らせ

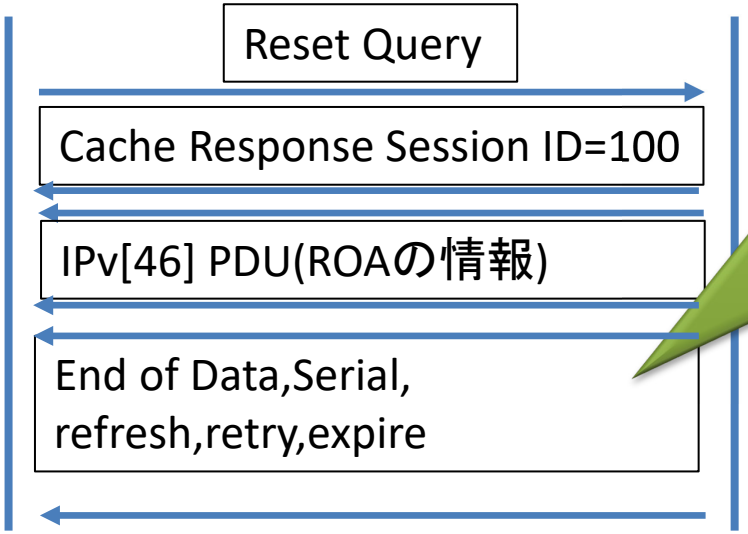
# rpki-rtr protocolと接続初期化

- RFC8210（Updated RFC6810）
  - rpki-rtr protocol version 0 = RFC6810
  - version 1 = RFC8210

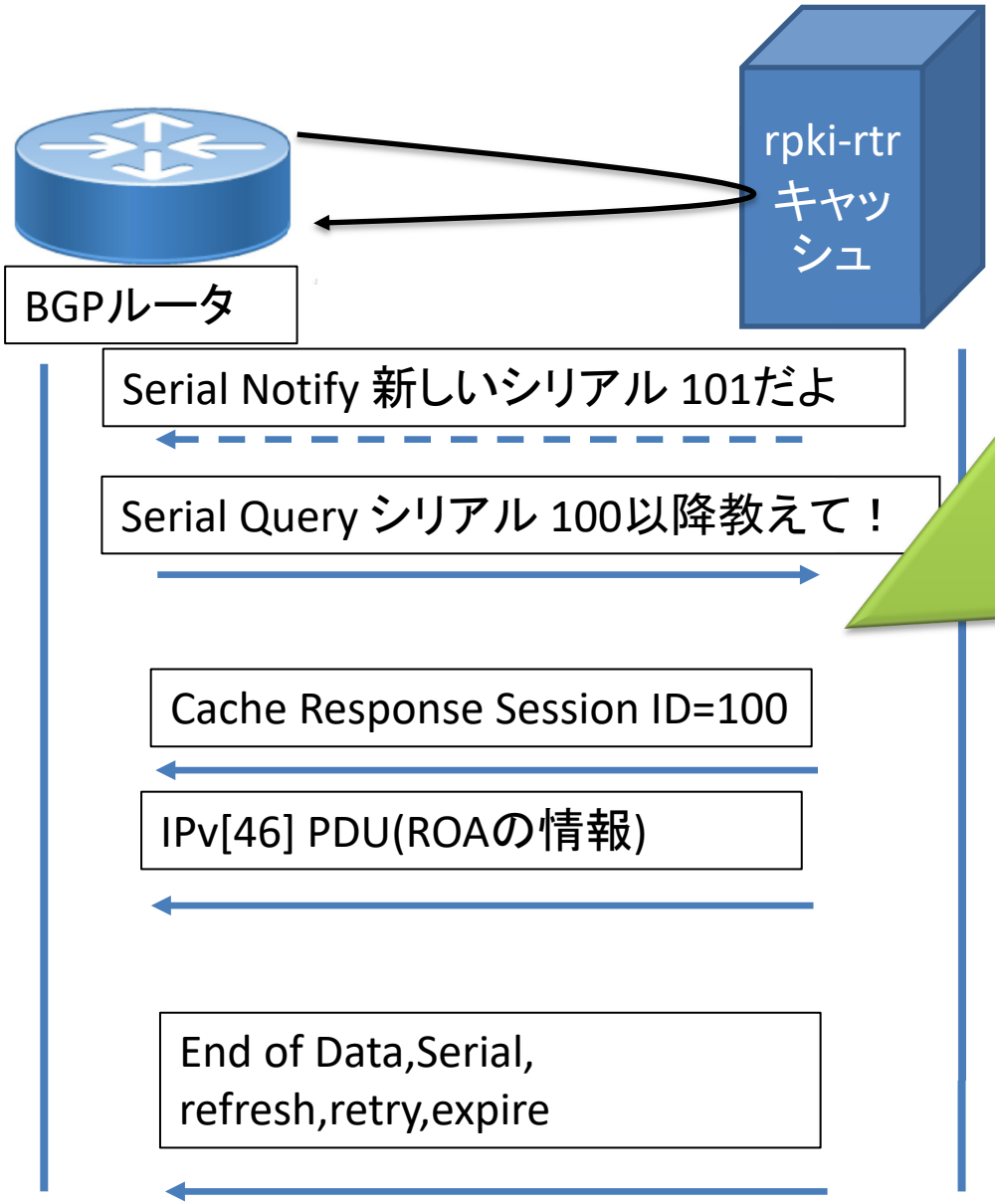



Serial:ROAデータの現状のバージョン(これが上がると差分がある)
Refresh:シリアルを確認する頻度
Retry:エラーの際の再訪問時間
Expire:接続トラブル時のキャッシュデータの破棄時間

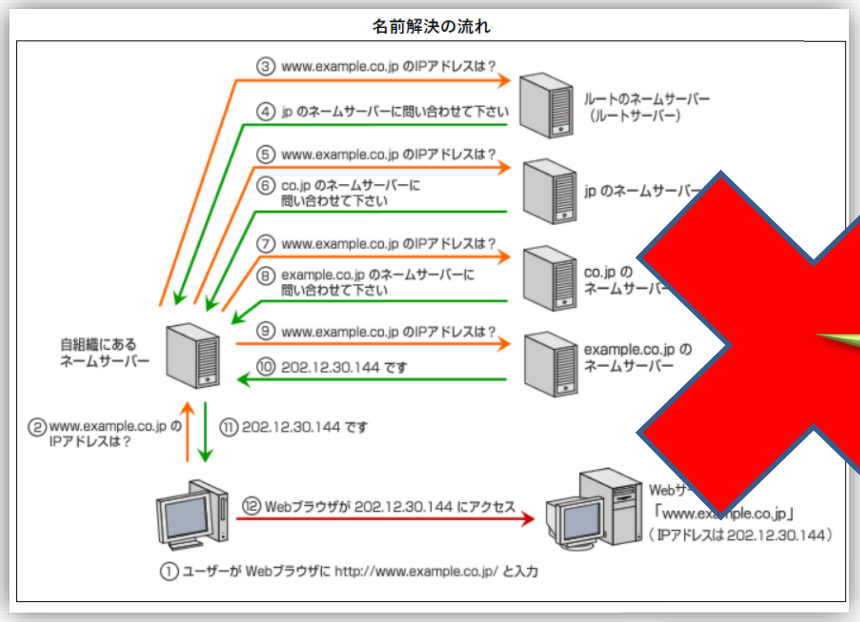
Version 0/1の主な差異
End of Data パケットに各種タイマーが実装された



# rpki-rtr protocol 差分の受け渡し

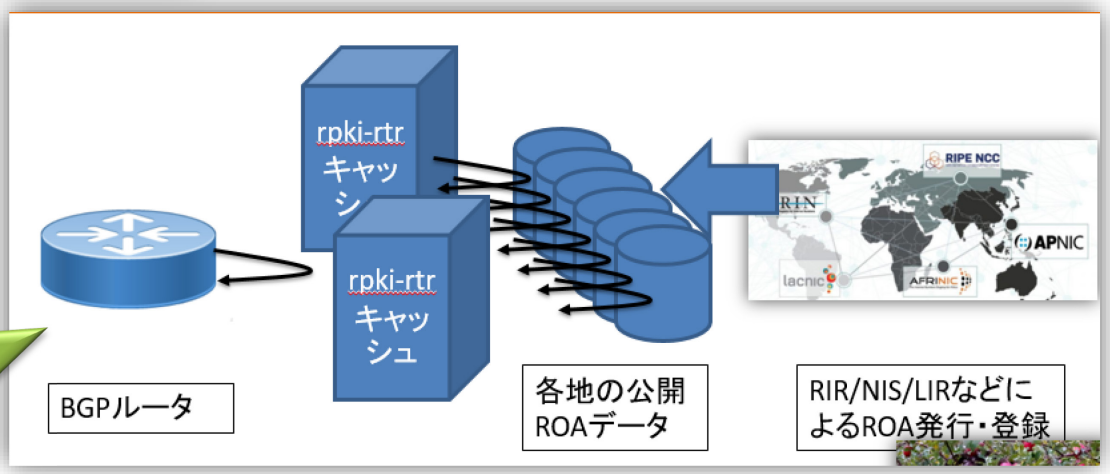


# rpki-rtr protocol 誤解




DNSフルリゾルバ型クエリ発生時にrootやTLDへ都度問い合わせる。キャッシュがあればその値を応答

キャッシュの起動時に地球上の全RPKI/ROAデータを取得、その時の全データをルータへPush 起動時に時間が要



# rpki-rtrの運用

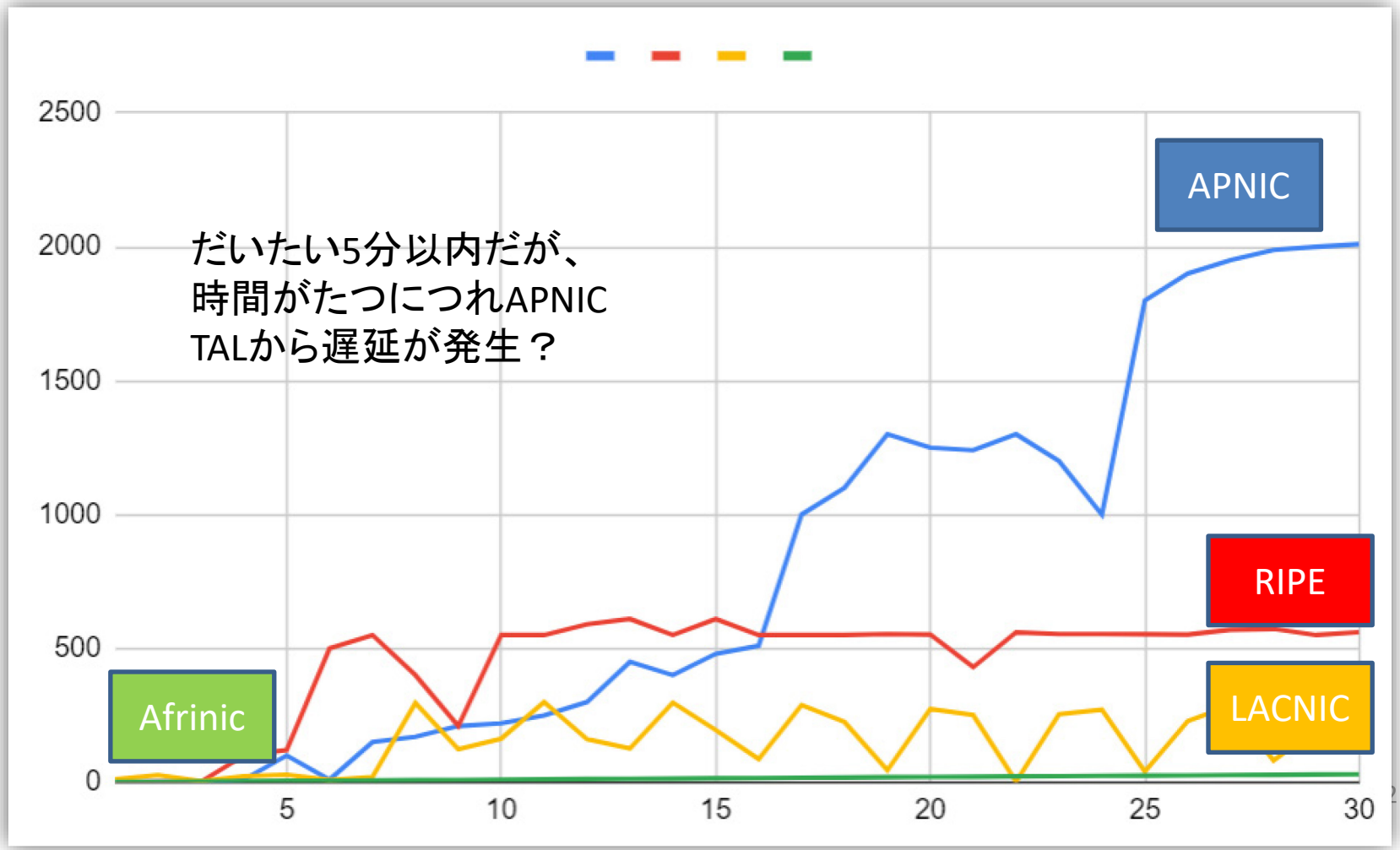
長崎県立大学
UNIVERSITY OF NAGASAKI

- 相互運用性

| | Cisco | | | Juniper | BIRD | FRR | 備考 |
|---|---|---|---|---|---|---|---|
| | IOS-XRv | CSR1000v IOS-XE17.3 | Cat8000v IOS-XE17.5 | vMX JUNOS21.3 | 2.0.6 | 8.1.0 | |
| routinator | ○ | ○ | ○ | ○ | ○ | ○ | |
| FORT | △ | △ | △ | ○ | △ | n/a | 接続後のqueryに難 |
| GoRTR/Octo RPKI | ○(v0) | ○(v0) | ○(v0) | ○(v0) | ○(v0) | ○(v0) | v1がうまく動かず |
| rpki-validator v3 | ○(v0) | ○(v0) | ○(v0) | ○(v0) | ○(v0) | n/a | v1非対応 |
| OpenBGPd | rpki-rtrの対応せず、ConfigのROAを手書きする必要性あり | | | | | | |

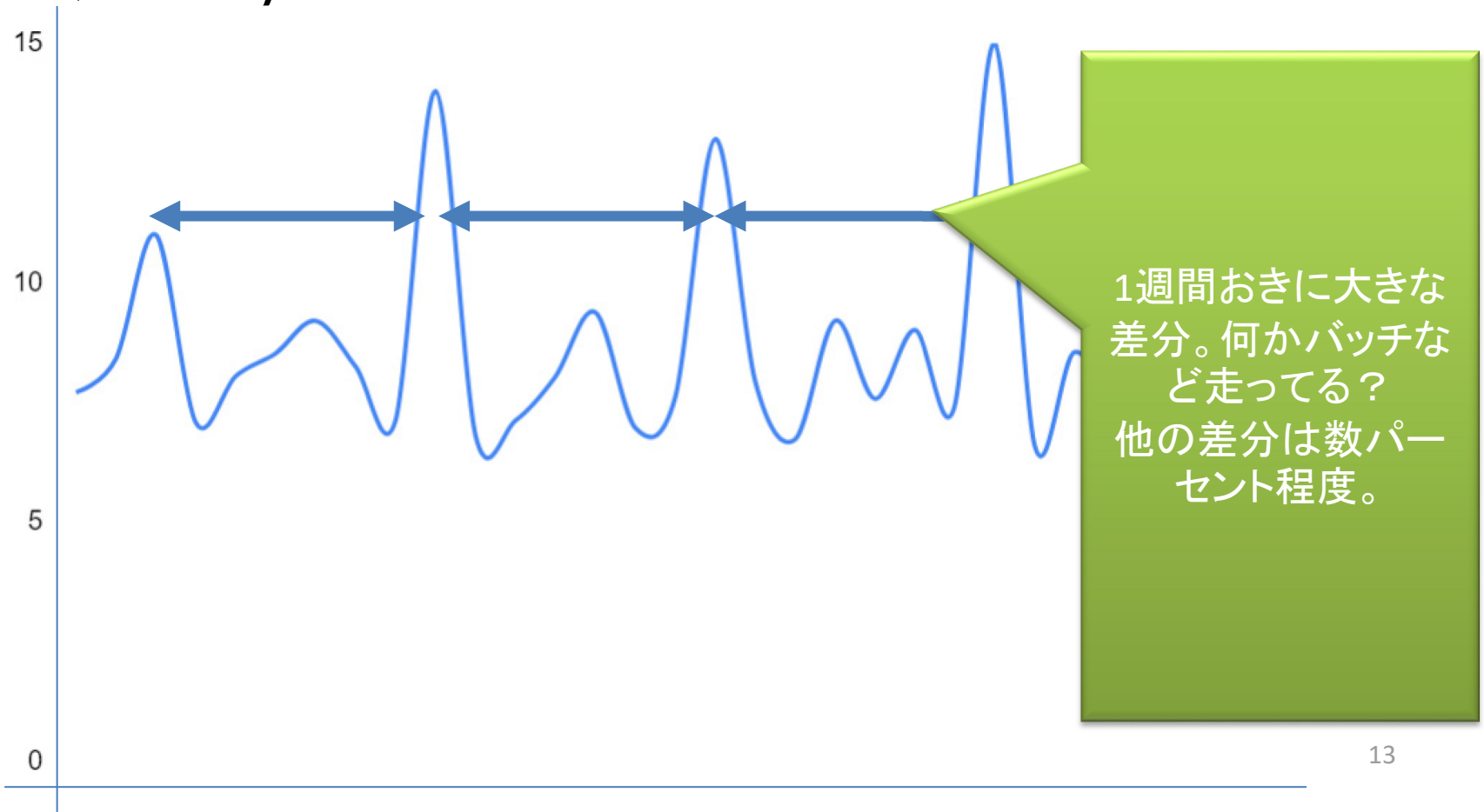
# rpki-rtrの運用

- ROA収穫時間の揺らぎ
- 2021年10月～11月のFORTによるROA収穫時間



# rpki-rtrの運用

- 収穫したROAの毎回の差異
- 30分おきにROA収穫をした際の差分(パーセンテージ)



# rpki-rtr 運用 うぅと思ったこと

長崎県立大学
UNIVERSITY OF NAGASAKI

- 複数キャッシュ運用時の優先順位
  - Valid/Invalid状態が混在した場合の挙動
  - CSR1000v IOS-XEの場合
    - 今のところ、両者をRoute-Mapなどで評価したっけとなる
    - しかし、Route-Mapで複数キャッシュを指定することは不可
- キャッシュ切断・Expire時の経路再計算
  - すべてのキャッシュが切断された場合、CPUが100%に張り付く
  - 30秒程度

# 期待

長崎県立大学
UNIVERSITY OF NAGASAKI

- 来年の本セッションでは「やってみた」例が複数あがることを期待

- まずは、ルーティングやOrigin Validationのまえに、「**ROAの登録**」をお願いします。