# RPKI 101

JANOG47

IXのルートサーバーにおけるRPKIの取り組み 事前資料

インターネットマルチフィード 後藤 / 萩原

Copyright © 2020

# はじめに

- 背景
  - 昨今RPKIがますます話題に挙がるようになった
  - 世界では商用サービスにおいてRPKIで不正と判定した経路を破棄する事業者も増えている
  - 一方で日本国内では未だ導入実績は多くない

- おことわり
  - 本資料は2020/05に作成されました
  - 一部情報が古くなっている箇所がありましたらご容赦ください

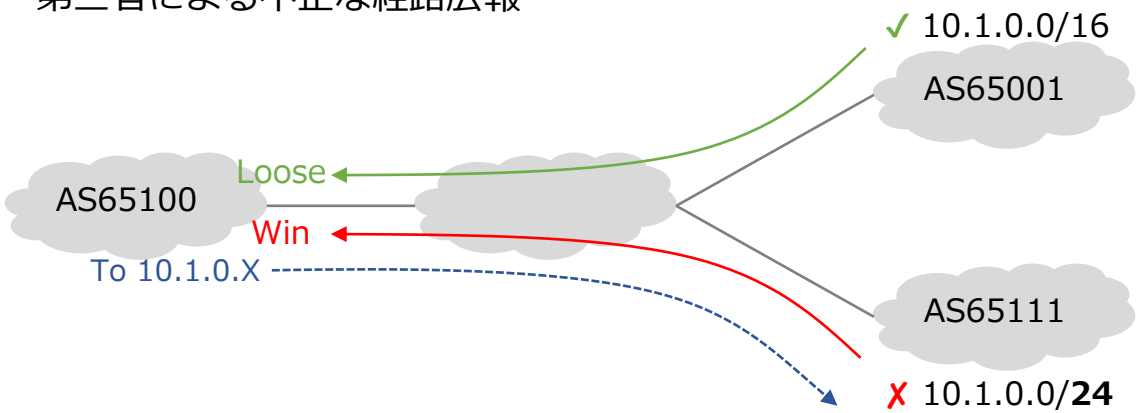
Copyright © 2020

# Why RPKI?

# ルーティングインシデント

## 経路ハイジャック

第三者による不正な経路広報




Examples:

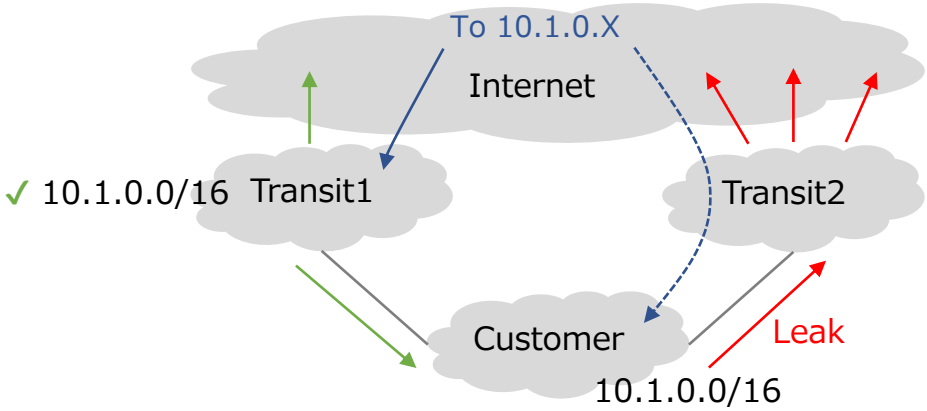
- TWNICが運営するPublic DNSの経路をブラジルのISPが広報, (MANRSより)
- さくらインターネットの経路をアメリカのISP?が広報, (Internet Week 2019より, PDF)

FYI:

- ICT-ISAC経路奉行では月に数十～百数十件を検知, (Internet Week 2019より, PDF)

## 経路リーク [RFC7908]

意図した範囲を超えた経路広報

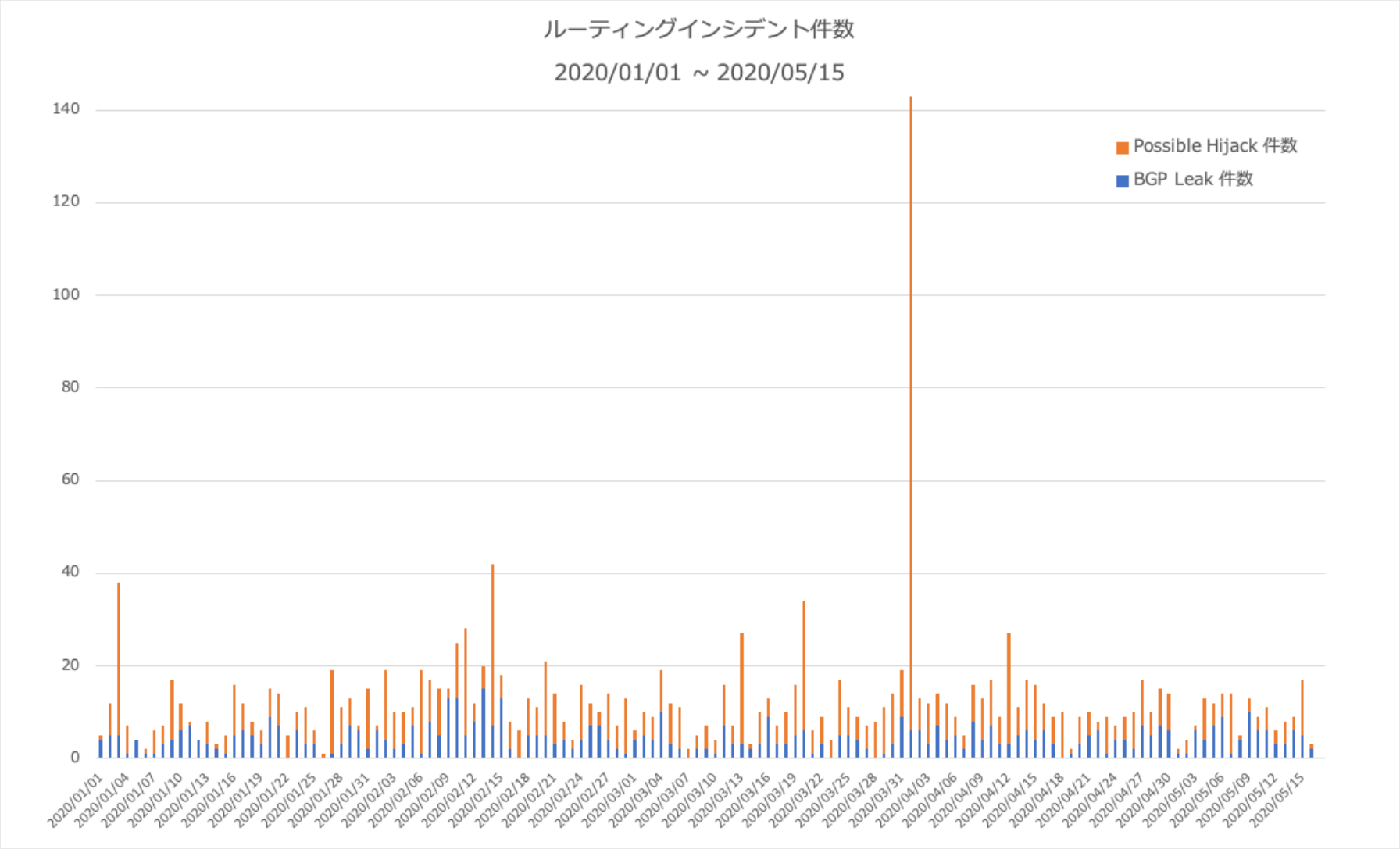



Examples:

- 2 AS間で交換された通常より細かい経路がVerizonにリークしそこからインターネット全体に伝搬, (The Cloudflare Blogより)

Copyright © 2020

# ルーティングインシデント件数

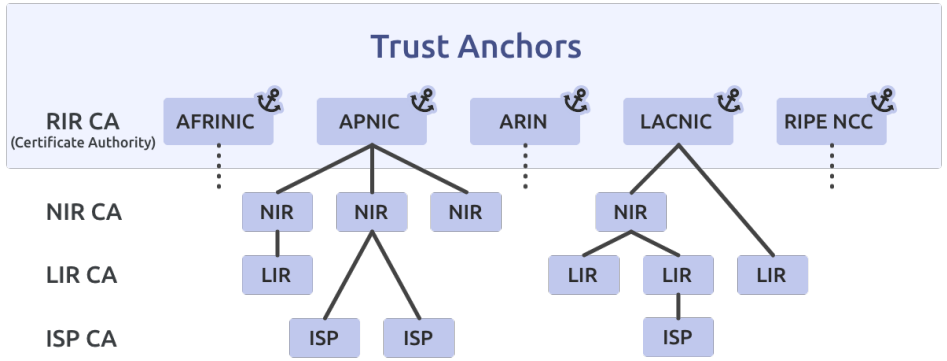



https://bgpstream.com/ より

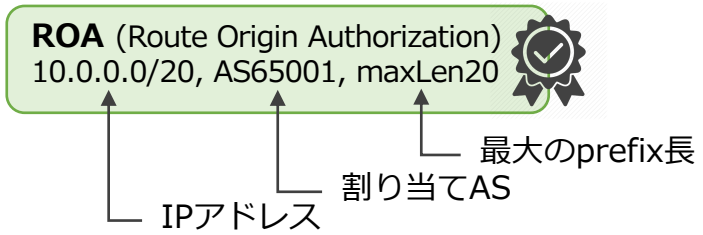
# RPKI

# RPKI

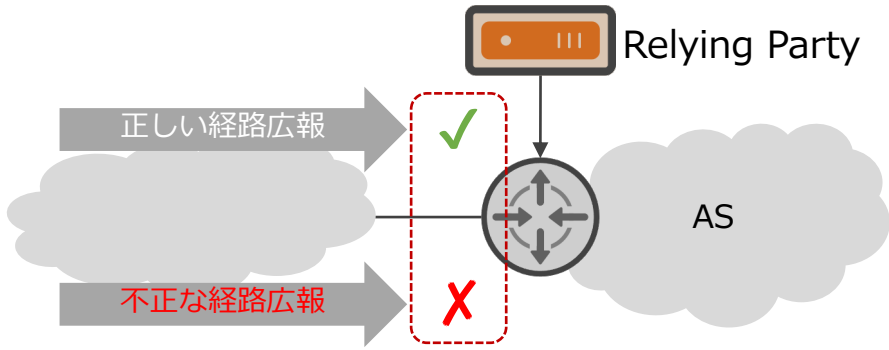
- RPKI (Resource Public Key Infrastructure)
  - インターネット資源情報 (IPアドレス, AS番号) の割り当ての正当性を証明するための公開鍵基盤
  - インターネットレジストリと同じ形の証明書ツリーに基づき資源情報に対しリソース証明書を発行する




- ROA (Route Origination Authorization)
  - “IPアドレスとそれを広報するAS番号の正しい組み合わせ” に、RPKIで発行したリソース証明書で署名を施したデータ

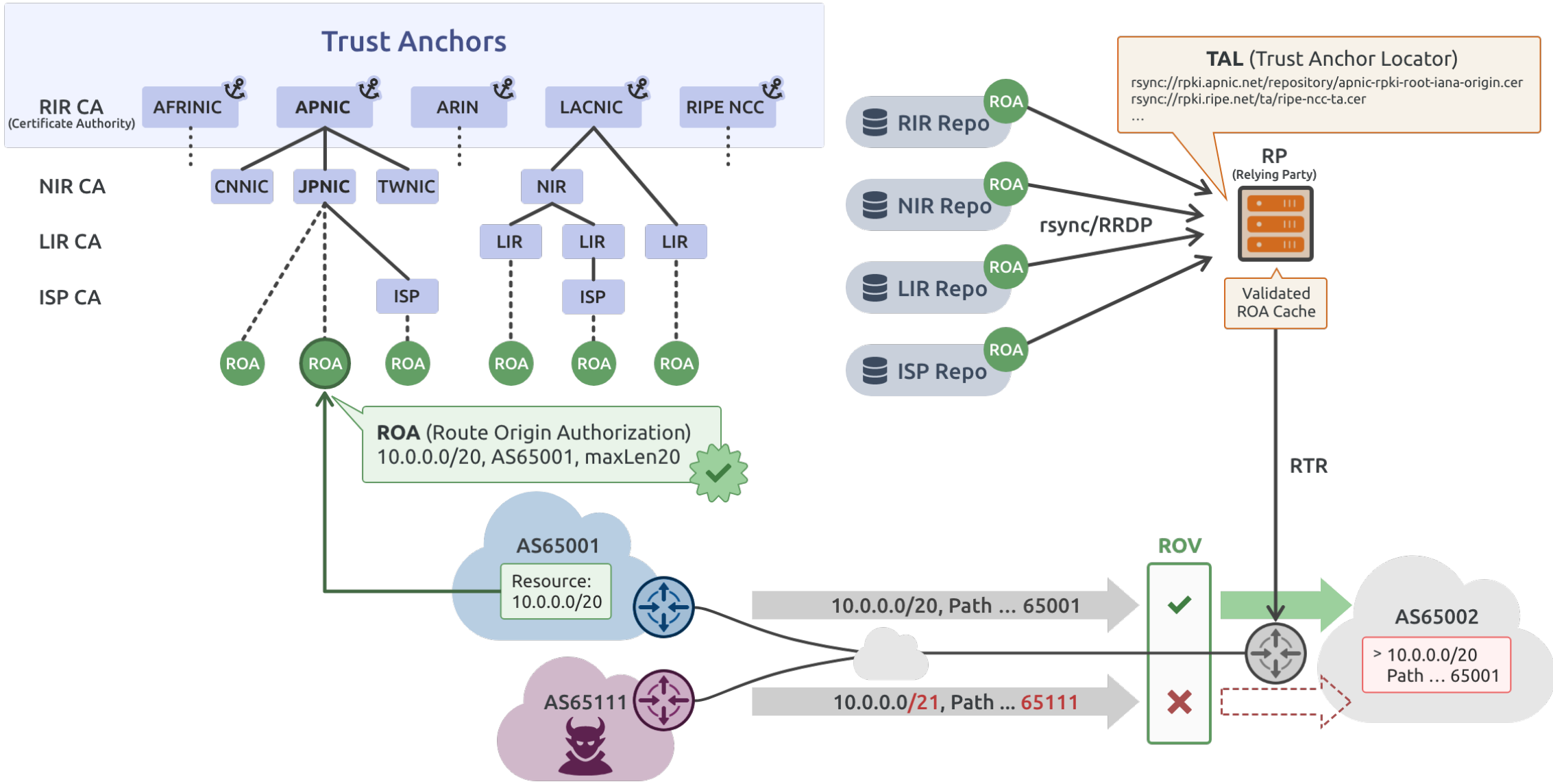



- ROV (Route Origin Validation)
  - ROAとBGPで受信したの経路情報とを照合し、“IPアドレスが正当なOrigin ASから広報されているか” を判定する
    → 経路ハイジャックを検知することが可能
  - ルーター等でROVを行うためにはROAに付与された署名を事前に検証するRelying Partyが別途必要となる



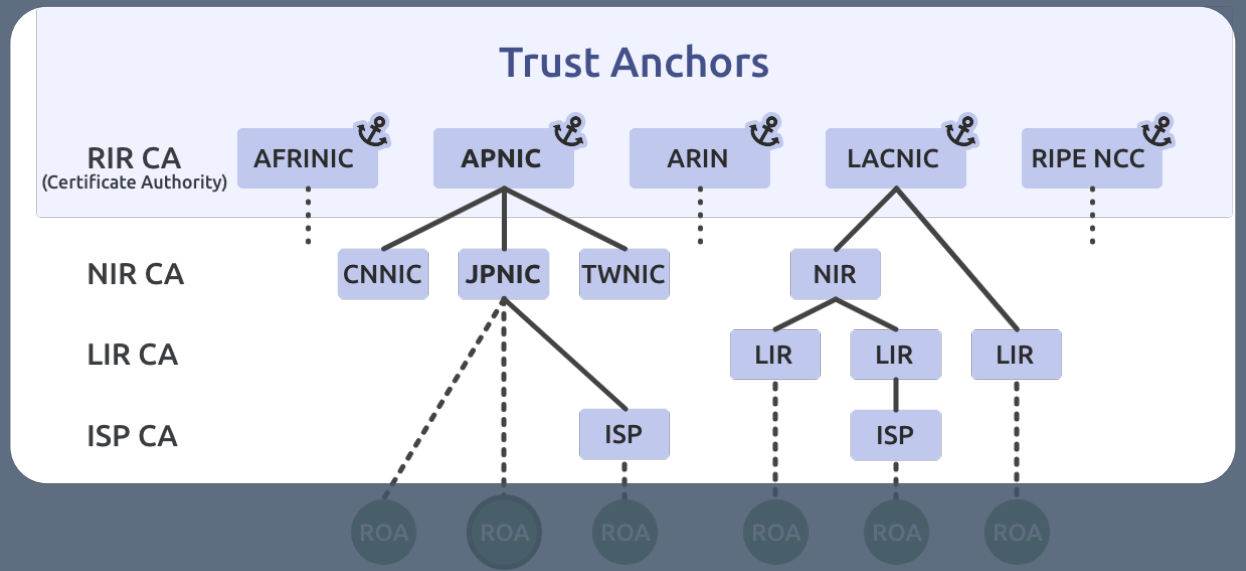

Copyright © 2020

# RPKI ROV Overview

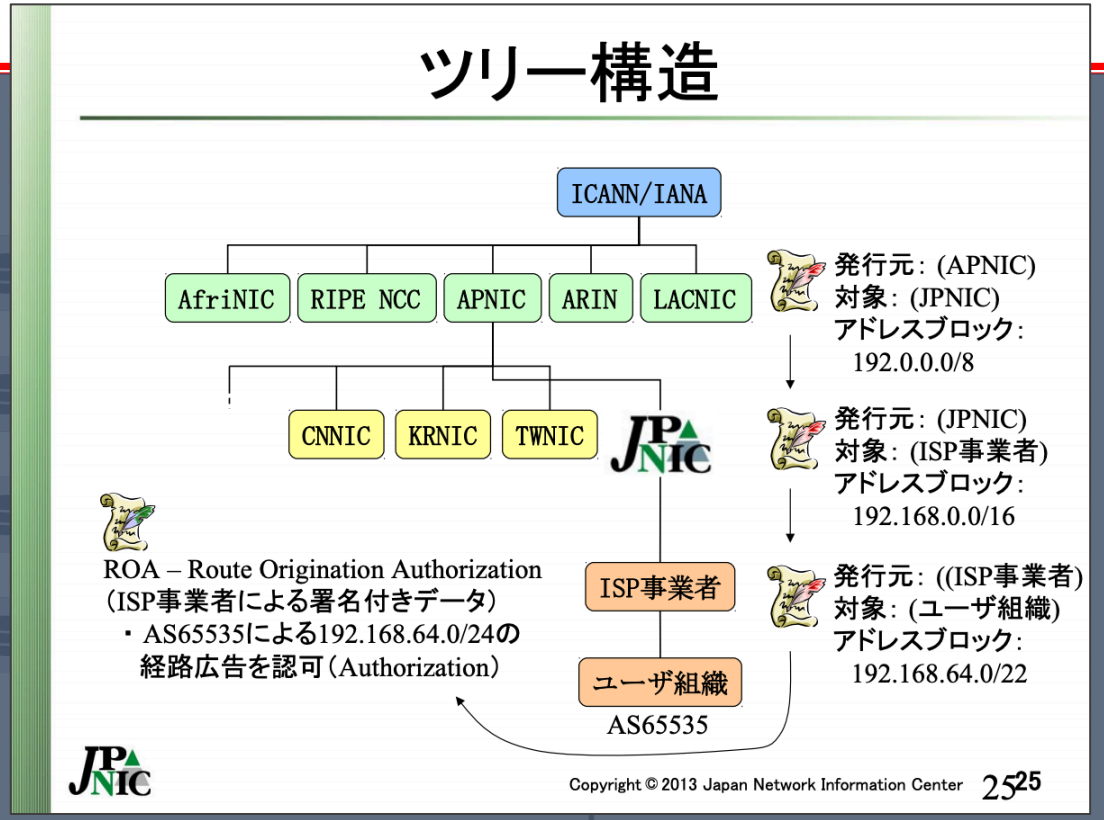



Copyright © 2020

# RPKI ROV Overview



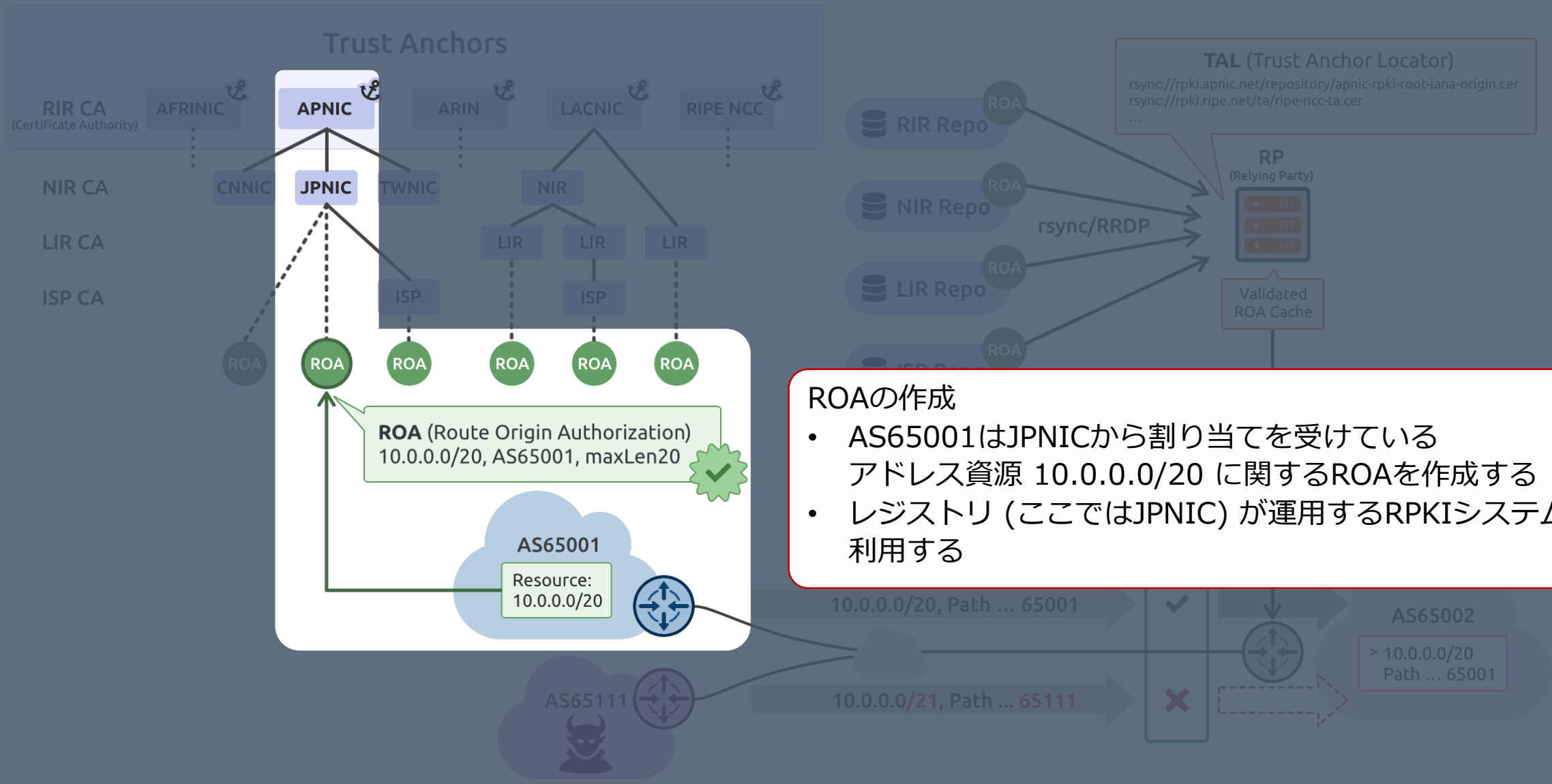

RPKI チュートリアル & ハンズオン ～ ROA 発行からルータでの参照まで～
http://enog.jp/wp-content/uploads/2013/05/2013-0426_enog20-rpki-04.pdf




RPKI証明書ツリー

- 各レジストリが認証局 (Certificate Authority, CA) としてリソース証明書を発行する
- 上位のレジストリの秘密鍵で下位のレジストリの証明書を署名する
- 署名の検証時は Trust Anchor (5つのRIR) から対象のオブジェクト (ROA) に向けてツリーを辿る
- CAとして Dragon Research Labs RPKI Toolkit, Krill といったソフトウェアがある

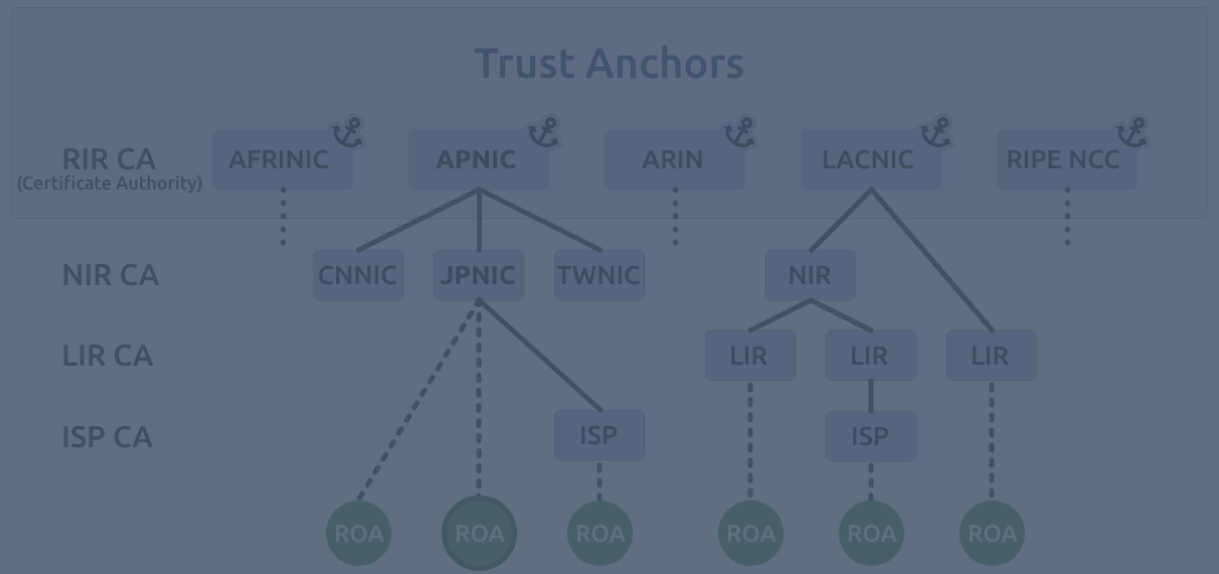
# RPKI ROV Overview

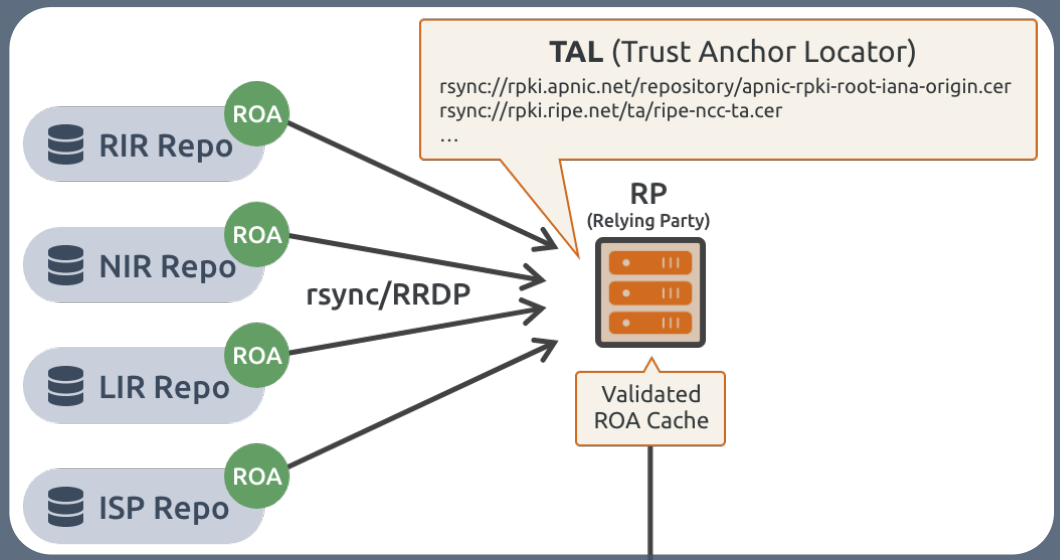



ROAの作成

- AS65001はJPNICから割り当てを受けている
  アドレス資源 10.0.0.0/20 に関するROAを作成する
- レジストリ (ここではJPNIC) が運用するRPKIシステムを利用する

# RPKI ROV Overview




RP (Relying Party) によるROAの収集/検証

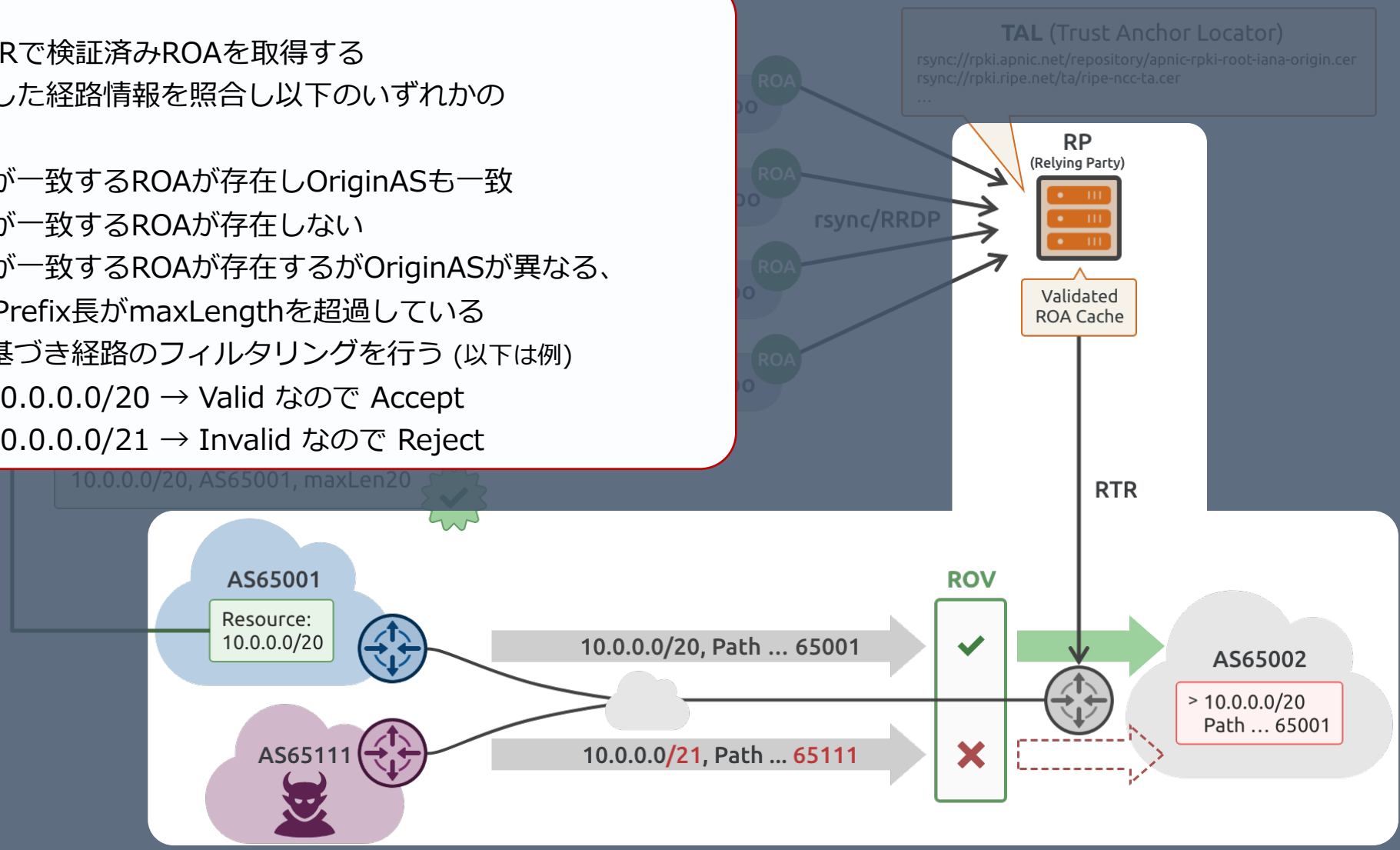
- 各レジストリのリポジトリからrsync/RRDPプロトコルでROAを収集する
- ROAの電子署名を暗号的に検証し、検証に成功したデータをキャッシュとして保有する
- キャッシュはRTR (RPKI to Router Protocol) で公開することができる
- RPとして RIPE NCC RPKI Validator 3, Routinator 3000 などのソフトウェアがある

Copyright © 2020

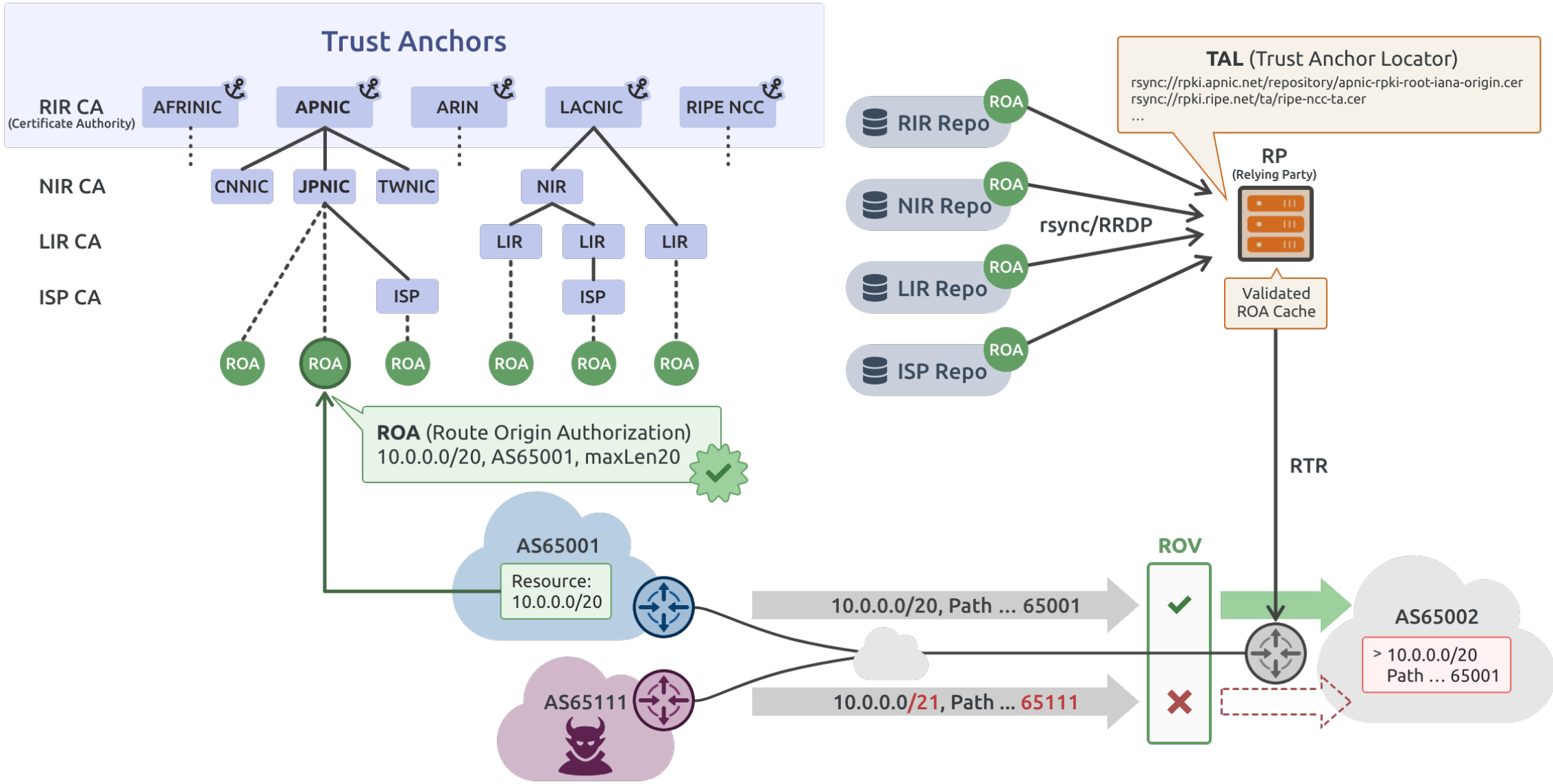
# RPKI ROV Overview

ROVの実行

- ルーターはValidatorからRTRで検証済みROAを取得する
- ROVではROAとBGPで受信した経路情報を照合し以下のいずれかの検証結果を得る
  - Valid　：Prefixが一致するROAが存在しOriginASも一致
  - NotFound　：Prefixが一致するROAが存在しない
  - Invalid　：Prefixが一致するROAが存在するがOriginASが異なる、またはPrefix長がmaxLengthを超過している
- ルーターはROV検証結果に基づき経路のフィルタリングを行う (以下は例)
  - AS65001が広報した10.0.0.0/20 → Valid なので Accept
  - AS65111が広報した10.0.0.0/21 → Invalid なので Reject



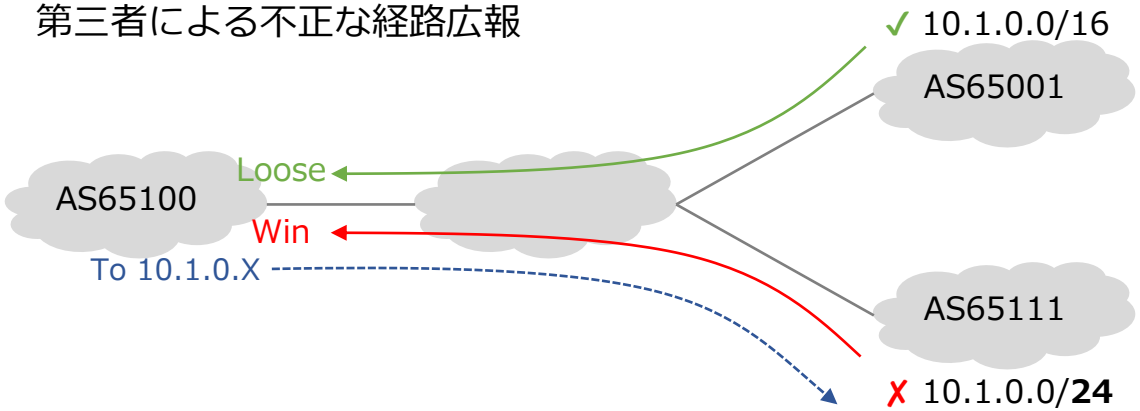
# (再掲) RPKI ROV Overview



# RPKI ROVで何を防ぐことができるのか？

## ✓ 経路ハイジャック

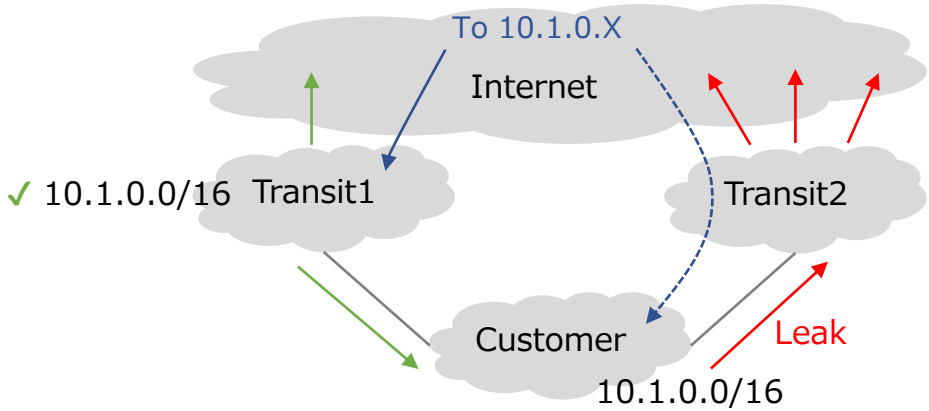
第三者による不正な経路広報




※原因は設定/オペレーションミスが多い

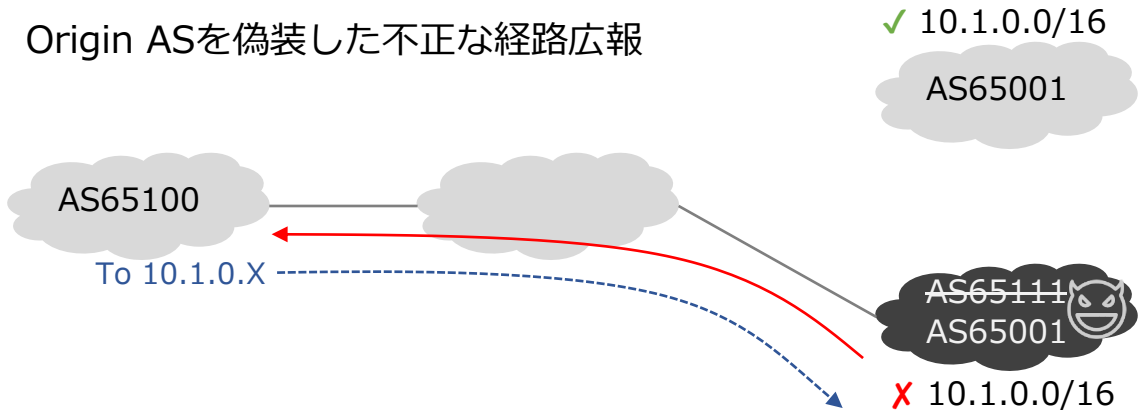
## ✗ 経路リーク [RFC7908]

意図した範囲を超えた経路広報



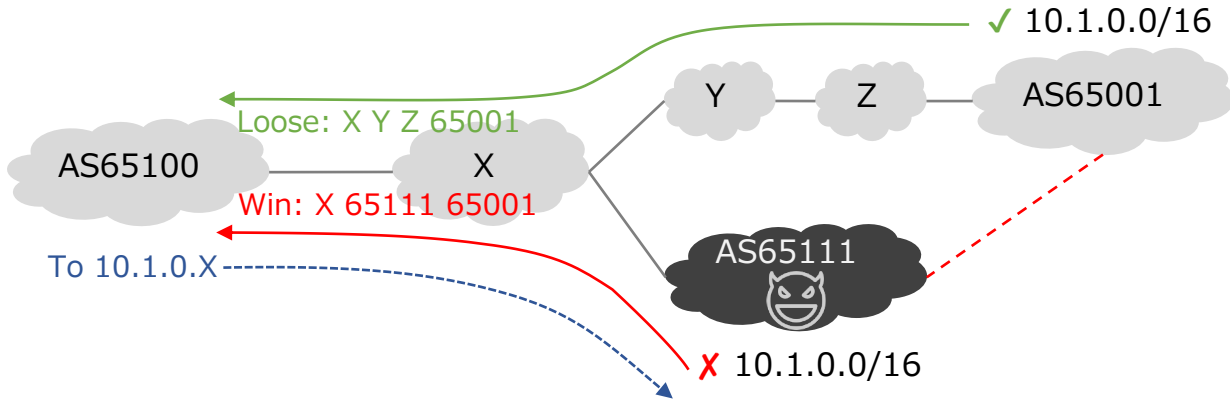

## ✗ 悪意のある経路ハイジャック (1)

Origin ASを偽装した不正な経路広報




## ✗ 悪意のある経路ハイジャック (1)

AS_PATHを不正に操作した経路広報




Copyright © 2020

# JPNAP vs 悪意のある経路ハイジャック/経路リーク

- 悪意のある経路ハイジャックや経路リークから身を守るためには AS_PATHフィルタリングの強化 が必要

(ライトな手法)

- Peer Locking
  - AS_PATHに “bignetwork” (= Tier1) のASが含まれている経路をrejectすることで経路リークを防止する
  - JANOGでWGが設立
    - [janog:14869] proposal: peerlock working group
    - JANOG47でWGの報告あり ※2021/01追記
  - 参考) Practical everyday BGP filtering with AS_PATH filters: Peer Locking (NANOG67より, PDF)

(ヘビーな手法)

- Path Validation
  - 電子署名を用いてAS_PATHの正当性を検証する
  - BGPsec, ASPA といった技術が検討されている (後述)

Copyright © 2020

# 参考) Path Validation

- BGPsec [RFC8205]
  - AS_PATHに電子署名 (BGPsec_PATH属性) を施し、AS_PATHが偽装されていないことを証明する
  - ✓ AS_PATHを偽装した経路広報 (4つのインシデント図における右下) に対して有効
  - ✗ 経路リークに対する効力はない
  - ✗ 署名検証に伴うルーターの負荷増
  - ✗ インターネット全体で高い導入率が必要
  - ✗ ダウングレード攻撃 (CapabilityのネゴシエーションでPath Validationを回避) が可能

- ASPA (Autonomous System Provider Authorization)
  - 経路広報の隣接関係に電子署名を施したASPAオブジェクトを用いてAS_PATHを検証し経路リークを防止する
    - AS_PATH Verifcation Using ASPA, (IETFより)
    - ASPAオブジェクト: {customerAS, providerASes, AFI}
  - ✓ ポリシー/ロールを考慮した検証を行うことができる
  - ✓ シンプル/軽量/スケーラブル

- (soBGP)

Copyright © 2020

# RPKI導入に向けた課題

- ROAの設計/運用どうする？
  - ネットワークの設計や運用に起因する “ROA設計のむずかしさ” は確かにある
    - 経路ハイジャックとROAの話 (IRS31より)
  - 正しく運用しないとインターネットからの疎通が失われるリスクがある
    - ほんとにあったRPKIの話 (InternetWeek2018より, PDF)
  - maxLengthはどう設定すべきか
    - RFC7115 では「実際に広報する経路のprefix長をmaxLengthにする」ことを推奨している
    - 一方でROVの普及率が低い現状では経路ハイジャックに対しlonger prefixで取り返すオペレーションもある

- ROVはまだ早い？
  - ルーター実装は進んでいる: IOS, IOS-XR, Junos, EOS, SR OS
    - 一部バグも報告されている
      - RPKI Deployment: 2020 SEACOM Update (APRICOT2020より, PDF)
  - 今後先導者 (Tier1等) からの情報共有が増えれば...

- Relying Partyソフトウエアはどれを使えばいい？
  - Relying Partyによって検証に成功するROA数が異なるという報告
    - Testing the validators and routers, (APNIC Blogより)

Copyright © 2020

# RPKI導入に向けた課題

- ROAの設計/運用どうする？
  - ネットワークの設計や運用に起因する “ROA設計のむずかしさ” は確かにある
    - 経路ハイジャックとROAの話 (IRS31より)
  - 正しく運用しないとインターネットからの疎通が失われるリスクがある
  - maxLengthはどう設定するべきか
    - RFC7115 では「実際に広報する経路のprefix長をmaxLengthにする」ことを推奨している
    - 一方でROVの普及率が低い現状では経路ハイジャックに対しlonger prefixで取り返すオペレーションもある
- ROVはまだ早い？
  - ルーター実装は進んでい…
    - 一部バグも報告されている
      - RPKI Deployment: 2020 SEACOM Update (APRICOT2020より, PDF)
  - 今後先導者 (Tier1等) からの情報共有が増えれば…
- Relying Partyソフトウエアはどれを使えばいい？
  - Relying Partyによって検証に成功するROA数が異なるという報告
    - Testing the validators and routers, (APNIC Blogより)

2021年になりこれらの状況は少し変わってきたように思います。
詳しくはJANOG47当日、議論しましょう！

Day3 2021年1月29日(金) 11:15～12:00 @HAKATA
IXのルートサーバーにおけるRPKIの取り組み

Day3 2021年1月29日(金) 13:30～14:30 @HAKATA
IIJ/AS2497でRPKIはじめました

※2021/01追記

# おわりに

インターネット/自分のネットワークの双方を守るため、
できるところから一歩ずつ！

Copyright © 2020