BGPセキュリティの動向と日本の現状 ～RPKI時代のルーティング～

社団法人日本ネットワークインフォメーションセンター
岡田 雅之
（木村 泰司）
インターネットマルチフィード株式会社
吉田友哉
（渡辺 英一郎）
株式会社インターネットイニシアティブ
Randy Bush
逐次通訳　川村　聖一
（松崎 吉伸）

JPNIC 社団法人 日本ネットワークインフォメーションセンター

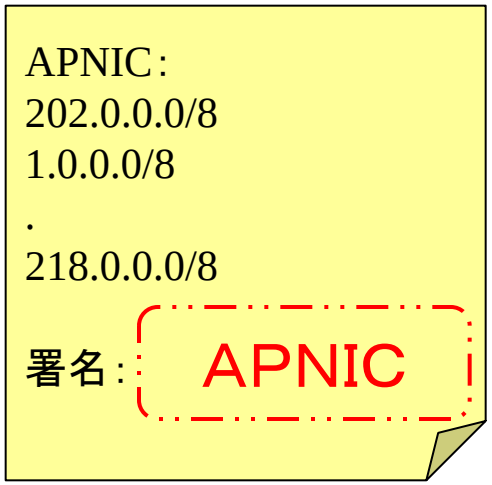
このプログラムでお話する内容

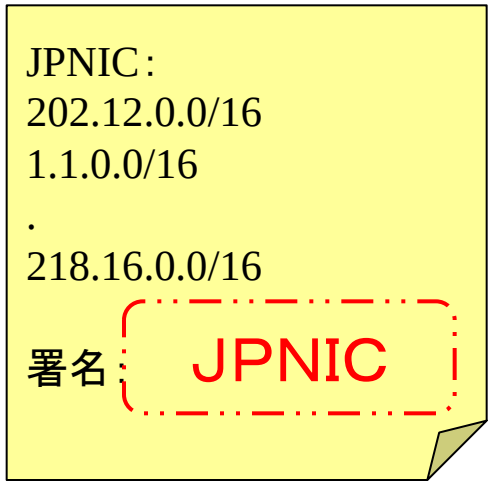
- **いまさら聞けないRPKI（岡田）**
  - RPKIの簡単なおさらい
  - 最新動向の共有
- **バックボーンルータにおけるRPKI（吉田）**
  - RPKI（ROA OriginAS Valiadtion）実装状況
  - ルータでの検証結果の共有
- **RPKI利用動向の計測（Randy）**
  - RPKIの普及度の計測
  - RPKIリポジトリ運営者の体験談（rpki.net)

いまさら聞けないRPKI

RPKIとは何か

- **IPアドレスとAS　＝　アドレス資源、の証明書**
  - Resource PKI（＝RPKI)
- **現在RIRが5つのroot認証局になる想定**
- **一般の電子証明書へIPアドレス・AS番号が記載**





（イメージ）

RPKIとは何か　－　その実態　－

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            eb:d2:0f:f6:fa:a8:22:14
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=Testbed root RPKI certificate
        Validity
            Not Before: May 17 00:27:38 2012 GMT
            Not After : Jun 16 00:27:38 2012 GMT
        Subject: CN=Testbed root RPKI certificate
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:ea:db:7e:7f:dc:82:0e:62:e3:dd:41:06:de:66:
                    e8:93:45:c3:84:35:50:b1:00:d0:32:ad:d3:55:18:
                    ae:1b:c7:b6:91:c5:78:4e:4f:5b:34:d3:ce:7d:be:
                    e2:0a:b7:47:6b:de:da:98:fe:0a:df:5d:c6:a9:8d:
                    45:ad:d0:05:39:be:ab:b0:59:50:bb:e9:31:e6:20:
                    c9:98:f6:cd:5d:15:e9:97:80:e7:a9:ed:50:de:62:
                    82:08:5e:ec:43:bc:7f:fe:de:25:0b:db:a4:4c:2a:
                    99:5f:40:4d:a7:8f:3e:ae:6d:0b:be:f2:6b:d3:71:
                    97:ad:3b:be:e5:06:09:bb:6e:cb:22:01:6c:68:a6:
                    db:93:d2:ca:40:81:24:64:9e:e3:85:82:b4:5a:2a:
                    26:f9:36:b5:fd:bb:06:fb:96:fd:16:01:db:61:19:
                    3b:13:f4:a3:98:a3:7b:75:c6:ea:40:c2:11:41:e8:
                    3c:a5:f4:a2:44:b4:68:4f:5e:5e:c4:54:53:05:08:

                    8d:20:01:3c:71:bc:56:87:2b:6a:c4:84:60:fc:3c:
                    3f:41:72:2d:2b:f8:91:7c:b3:d3:c6:78:82:7e:02:
                    36:15:18:7a:fa:e0:63:d3:9c:c4:5e:e7:d9:2e:94:
                    dc:8c:85:d7:42:b0:53:34:d6:95:e6:e7:9d:81:7c:
                    bb:7f
```

```
Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Subject Key Identifier:

1D:19:E8:25:53:AF:13:45:45:1B:00:56:44:96:17:E4:11:
88:7D:4E
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            Subject Information Access:
                CA Repository -
URI:rsync://dhcp203.nic.ad.jp/rpki/
                1.3.6.1.5.5.7.48.10 -
URI:rsync://dhcp203.nic.ad.jp/rpki/root.mft

            X509v3 Certificate Policies: critical
                Policy: 1.3.6.1.5.5.7.14.2

            sbgp-autonomousSysNum: critical
                Autonomous System Numbers:
                  0-65535

            sbgp-ipAddrBlock: critical
                IPv4:
                  0.0.0.0/0
                IPv6:
                  ::/0
```

RPKIを規定する文書群

- RFC3779:X.509 Extensions for IP Address…
- RFC5280:Internet X.509 Public Key Infra….
- RFC6480:An Infrastructure to Support Secure..
- RFC6481:A Profile for Resource Certificate…
- RFC6482:A Profile for Route Origin Autho…
- RFC6486:Manifests for the Resource Public…
- I-D:The RPKI/Router Protocol draft-ietf…
- I-D:ietf-sidr-pfx-validate…

今日は一切説明しません

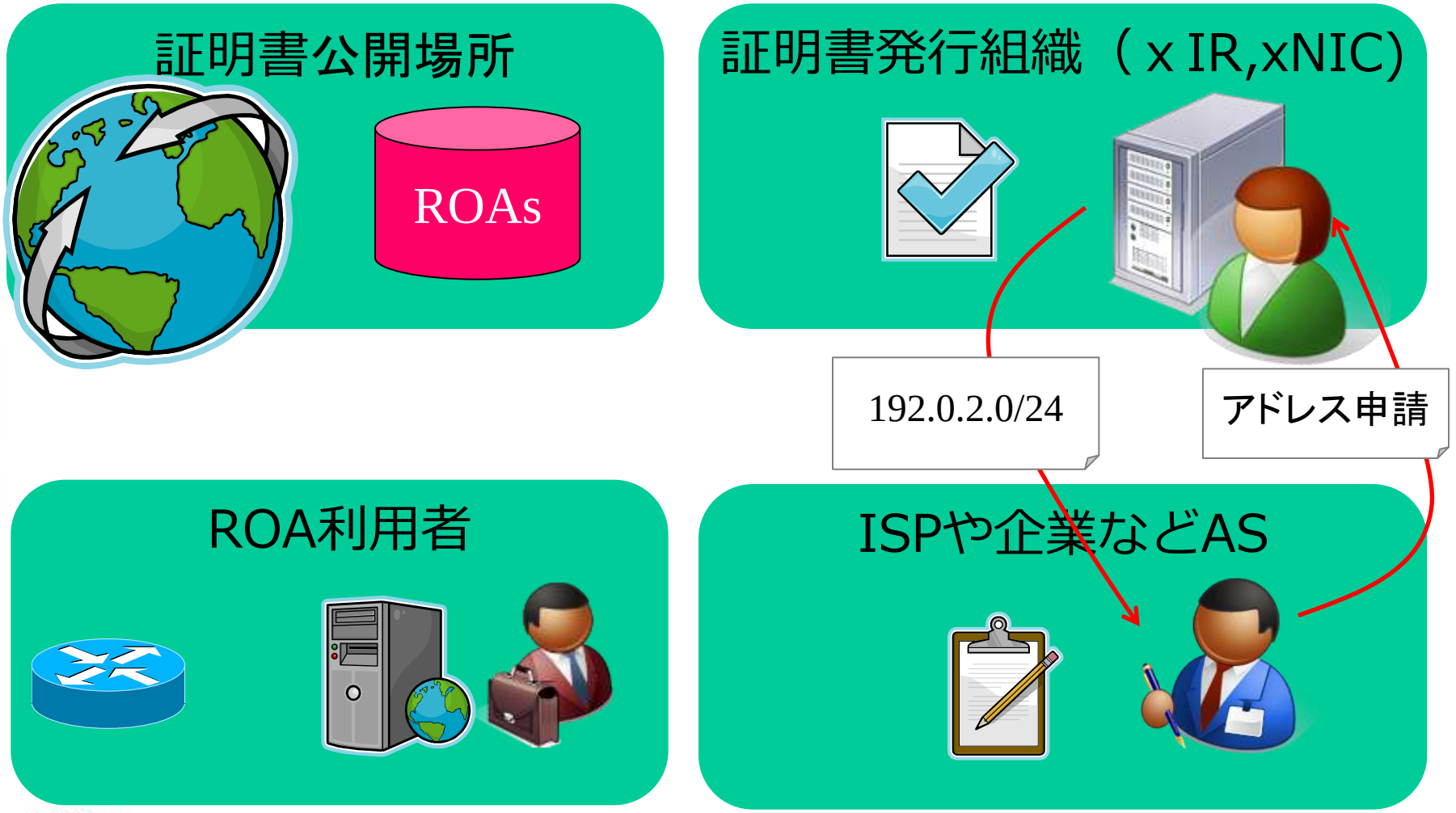
（※ＲＦＣは３０個位あります）

RPKIとROAを理解するために　登場人物

- **証明書を発行する組織（レジストリや企業）**
  - 証明書からROAの妥当性を確認
- **ROA（Route　Origin Authorization）**
  - IPアドレスのOrigin　ASを主張するためのもの
- **リポジトリ（証明書公開所）**
  - リソースの証明書やROAを溜め込み公開
- **ROAのキャッシュと道具**
  - ROAを溜め込みルータへ送るキャッシュサーバ
  - プロトコル

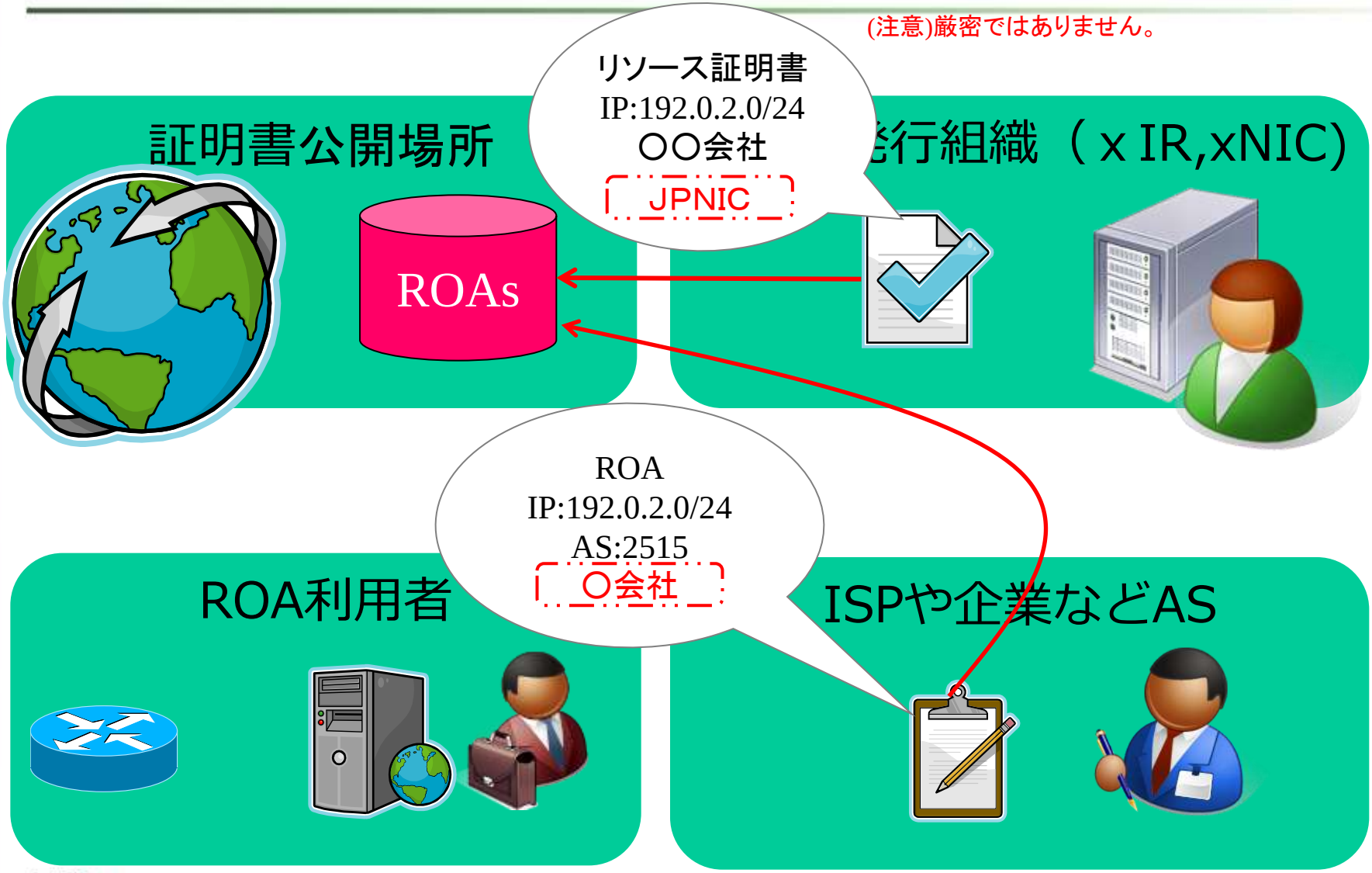
RPKIとROAを理解するために　利用の流れ

(注意)厳密ではありません。



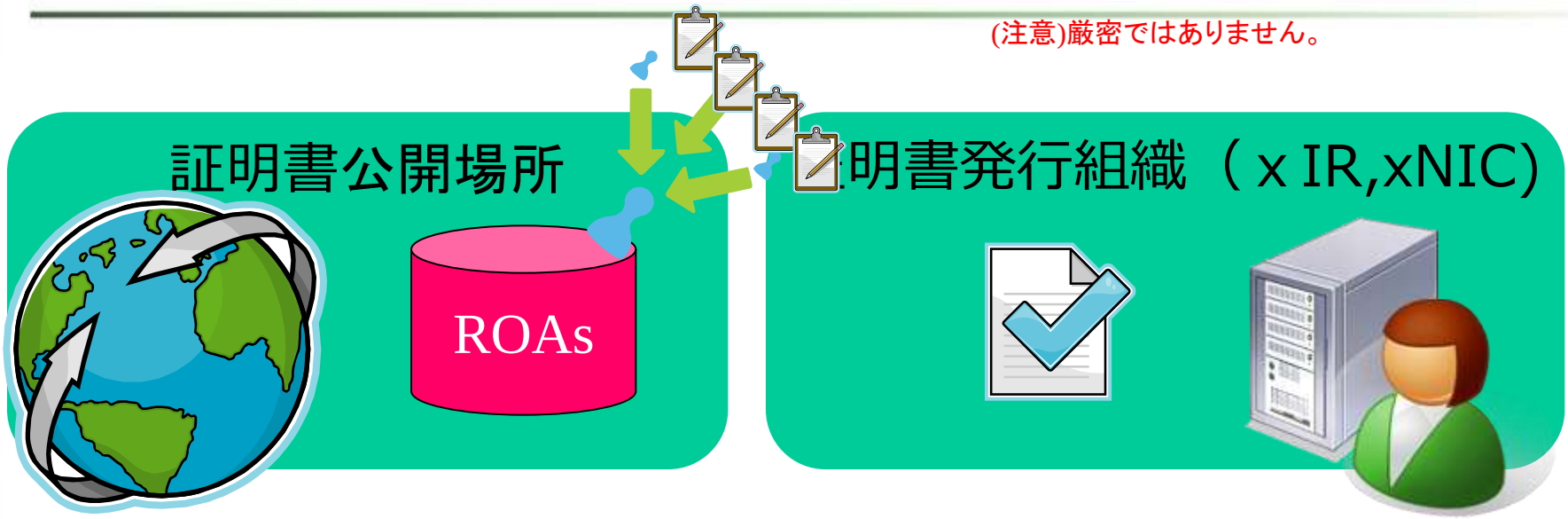
RPKIとROAを理解するために　利用の流れ

(注意)厳密ではありません。

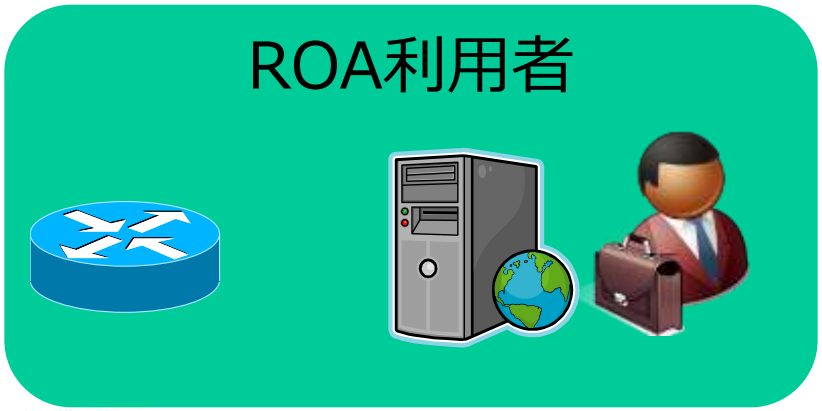


RPKIとROAを理解するために　利用の流れ

(注意)厳密ではありません。

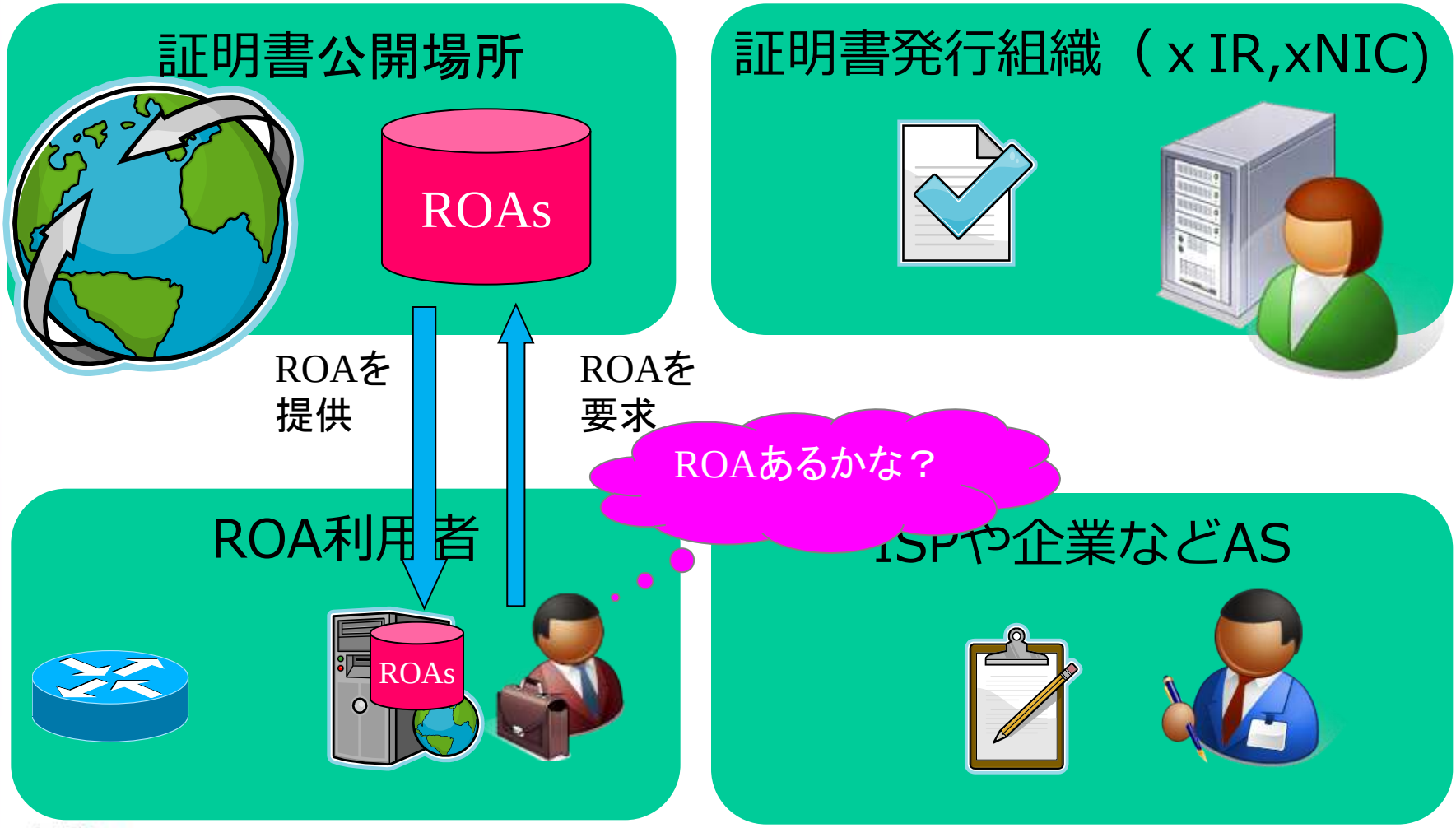


ROAをみんなが登録



RPKIとROAを理解するために　利用の流れ

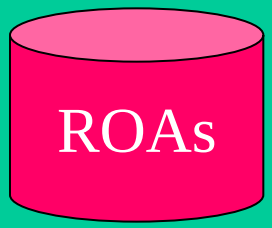
(注意)厳密ではありません。



RPKIとROAを理解するために　利用の流れ

(注意)厳密ではありません。

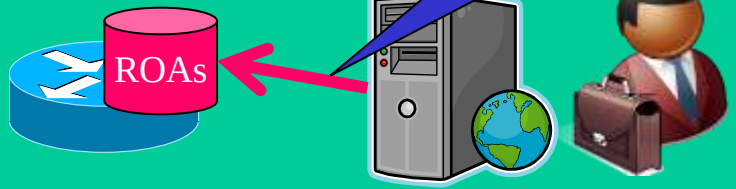
証明書公開場所



証明書発行組織（ｘIR,xNIC)

ROAとリソースが一致したら
RPKI-RouterプロトコルでRouterへ

ROA利用者



ISPや企業などAS

RPKIとROAを理解するために　利用の流れ

(注意)厳密ではありません。

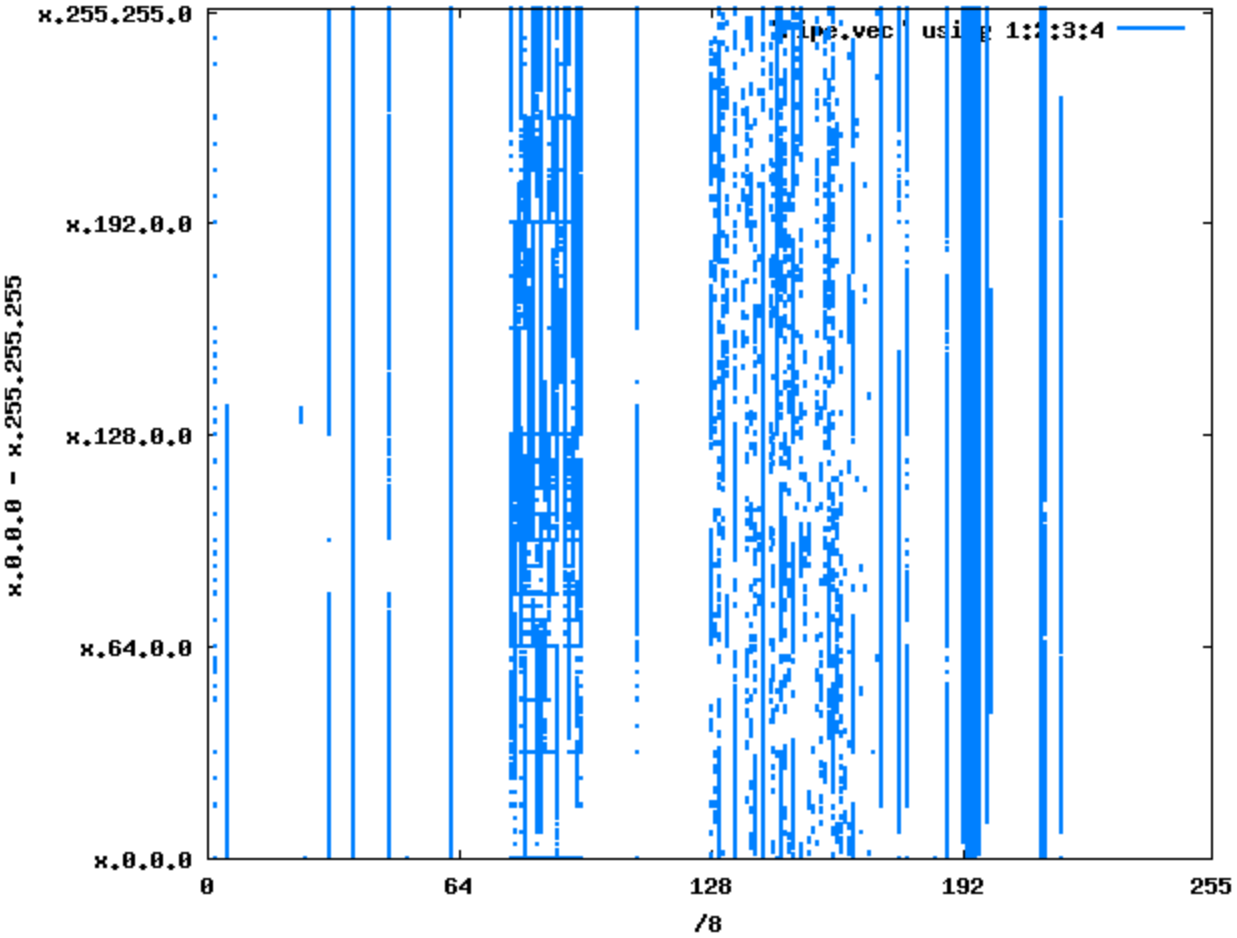
RPKIの動向（１）　　現状はどうか？

- **道具の観点**
  - 証明書作成～ルータ投入まで問題なく可能
  - 発行～ルータ投入までオープンソース
- **ルータの対応状況**
  - 一部のBGPルータが対応
    - 経路のOrigin　AS検証が可能
- **人の関心度合いは？**
  - 地域によって温度差
  - RIPE地域では3800ROAが登録公開
    - RIPE地域　IPアドレス数換算で30%

RPKIの動向（２）　　RIRのROA登録状況

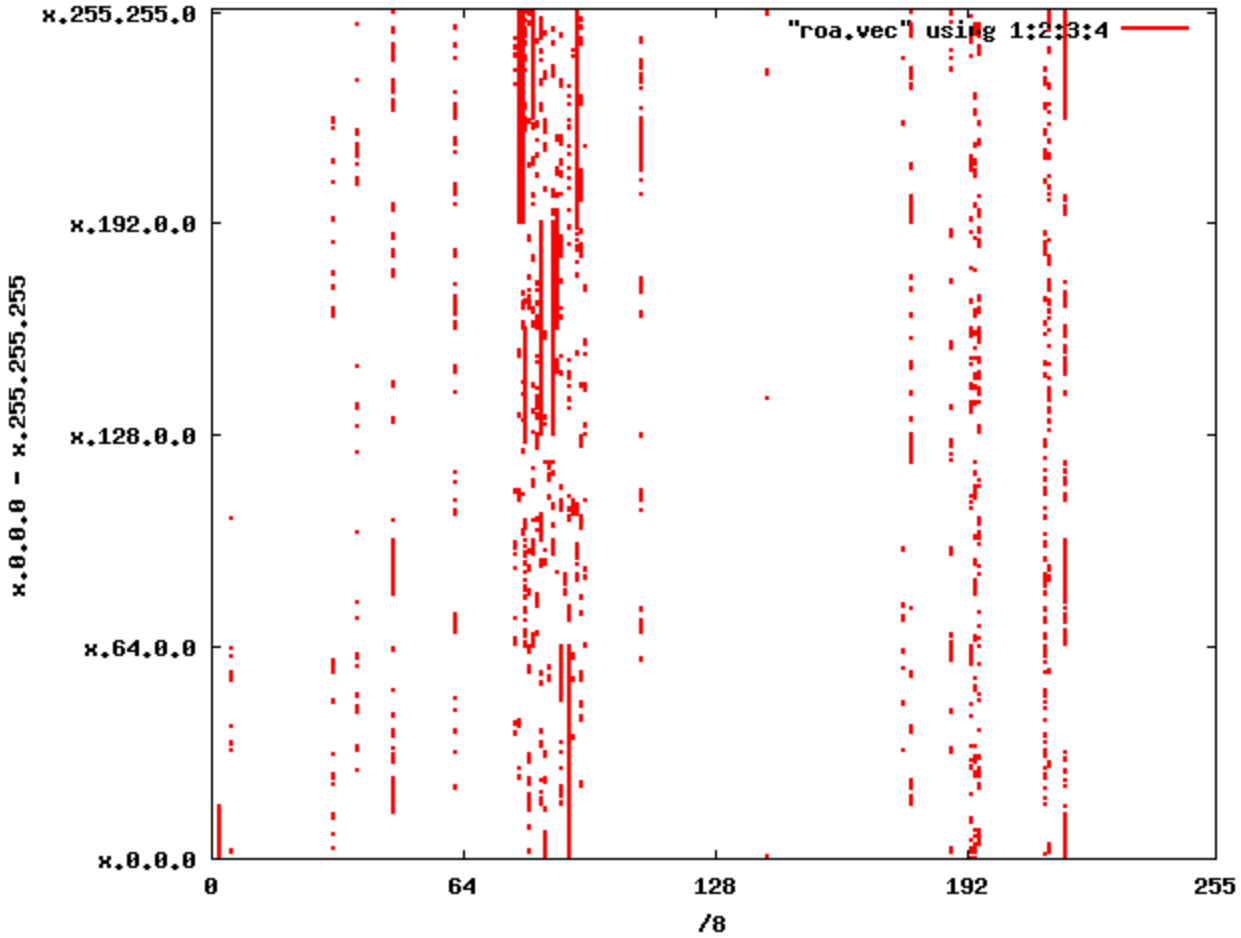
- **どのRIRも基本ROA作成可能**

RPKIの動向（２’）　　特にRIPEの状況
ROAの名産地



RIPE地域のIPアドレスのプロット

RPKIの動向（２’）　　特にRIPEの状況



RIPE地域のROA登録があるIPアドレスのプロット

RPKIに関する議論・疑問

- **そもそもRPKI/ROAへ依存することの是非？**
  - RPKI/ROAの問題発生時、経路交換が停止
  - システム障害、そのほかPoliticalな懸案
- **IPアドレス・ASの割り当て情報との紐付けは？**
  - 現状、ROAは考慮しない
  - あくまで、「IPアドレスの利用者が自分のASを主張」
    - 過去JPNICで実験は実施
- **どのようにRPKI/ROAを配布するのか？**
  - 経路交換を上位レイヤに依存すること
    - ー あ、証明書のURLにDNS名ががが

現状との比較 特に、RPKIとIRR

- **IRRを参照するモデルと何が異なるのか**
  - 今のところ、RPKI/ROAはOrigin AS　Validationまで
    - みんながROAを参照すれば経路ハイジャック対策有効
      - IRRでもみんながやればできる（気がする）
  - ROA　≒　署名つきRouteオブジェクト
    - IPアドレスの利用者が、AS番号を主張する点はIRRと同
    - ただし、正しいIPアドレス利用者の主張であることは担保

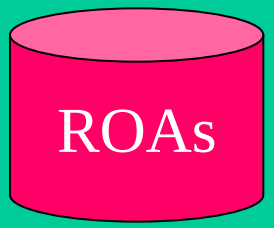
    →　IRR情報ののっとりは困難化
- **より強固なIRRシステムとしてのROAか？**
  - これからも利用法が変化する可能性があります

RPKIの現状のまとめ

- **ルーティングをお手伝いするRPKIの基盤**
  - ほぼ完成
- **地域によってはRPKI/ROAの発行が開始**
  - 地域の温度差あり
- **ルータの実装状況**
  - 対応ルータが出てきた（状況は吉田さん）
- **さて、どのように活用するのか？**
  - どこまで依存できるのか？
  - これから議論・検討が必要
  - IRR登録参照モデルと変わらないかもしれない

吉田さん、Ｒａｎｄｙの発表内容

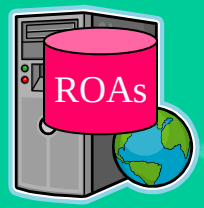
証明書公開場所



証明書発行組織（ｘIR,xNIC)

Randyの発表の対象

ROA利用者



ISPや企業などAS

吉田さんの発表の対象