RPKIとインターネット ルーティングセキュリティ

Internet Week 2009

NECビッグローブ株式会社
川村　聖一

RPKI到来の背景

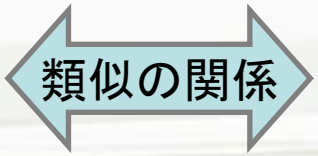
- 続発するルーティング事件、インシデント
  - YouTubeハイジャック事件、など
- インターネットのインフラとしての信頼性への期待
- アドレス枯渇時期の到来
  - アドレス移転ポリシーの成立
    - 分割して他社への移転ができる
    - 202.247.0.0/16の内202.247.128.0/17を他社へ移転、など
  - 細切れ経路の増加、不正経路（勝手なアドレス利用）の増加

アドレス・経路の信頼性が今までに増して重要

RPKIって何？

Resource Public Key Infrastructure

- SSLのX.509証明書などでお馴染みの公開鍵管理方式
- アドレスリソース、AS番号リソースを指す

ドメインと「SSL証明書」  アドレス(Prefix)と「リソース証明書」

※但し、リソース証明書はどちらかというと「許可書」。

アドレス、AS番号などのナンバーリソースに証明書を付け、
それを使ってインターネットルーティングをセキュアにするための管理・運用の仕組み

＜参考＞証明書の種類と機能

証明書の種類

1. CA Certificate：割り振り・割り当て業務を行う組織

2. Resource Certificate:リソース証明書
   - ■ IPアドレスを証明
   - ■ AS番号を証明

上記証明書を利用した応用機能

1. Route Origin Authorization (ROA)
   - ■ IPアドレスにルーティング権を付与する(Origin ASを指定する)

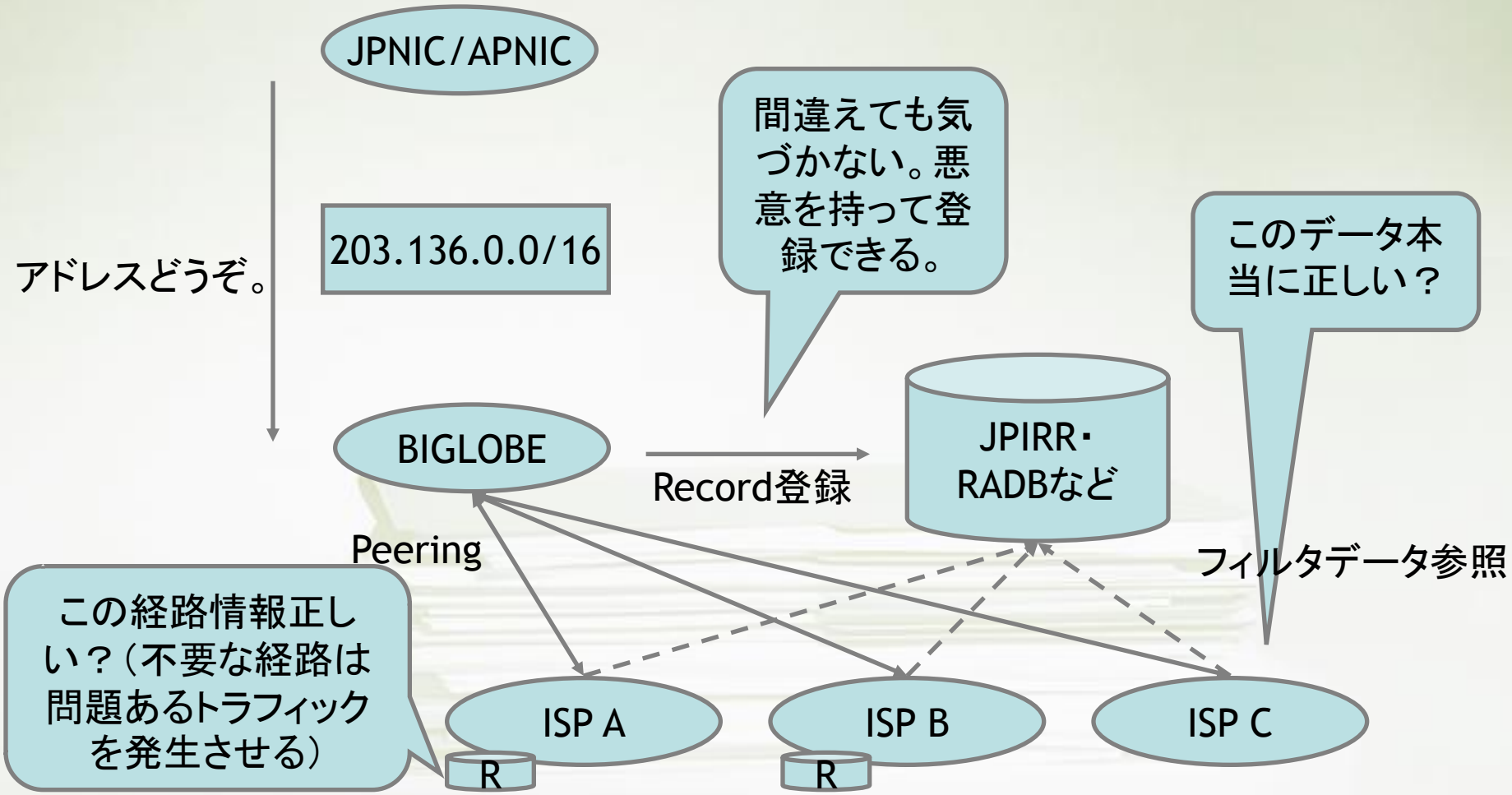
現時点でIETFで検討されているものの一部。

証明書がもたらす未来のイメージ

- 続発するルーティング事件、インシデント
  - 理想1：ハイジャックしようとしても証明書がなければできない
- インターネットのインフラとしての信頼性への期待
  - 理想2：「証明」が付くだけで信頼Up。(SSL的な感覚)
- アドレス枯渇時期の到来
  - 理想3：アドレスを勝手に移転しても、わかってしまう
  - 理想4：勝手に未割り振りアドレスを使おうとしても、わかってしまう

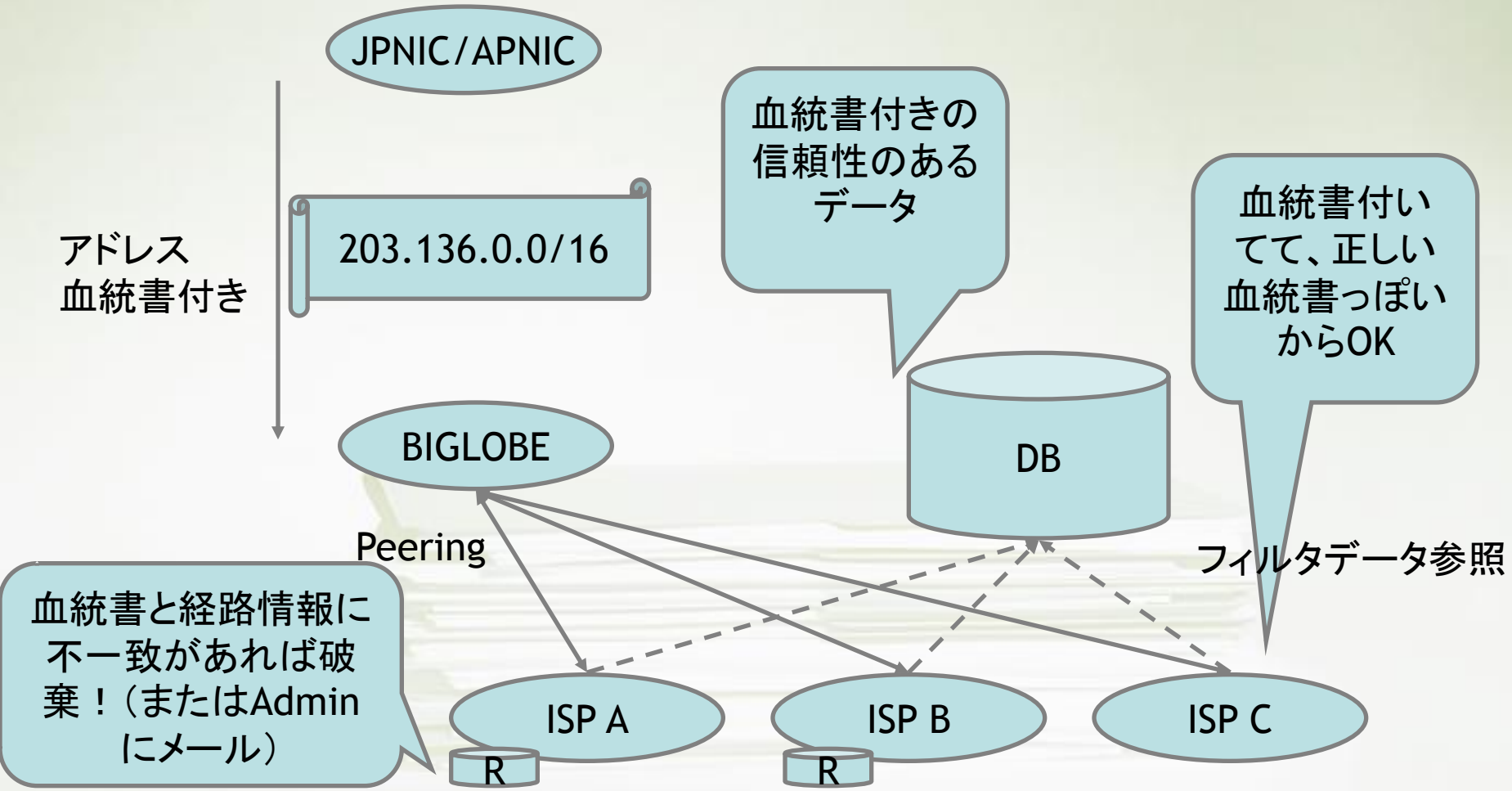
今見えている問題は、改善される

今までのアドレス、ルーティングの扱い



証明書を利用したイメージ(期待)

【イメージ把握しやすさのため、厳密に正しい説明ではありません。】



RPKIアーキテクチャのポイント

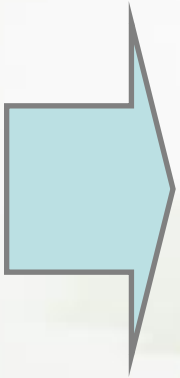
- NICがアドレスを割り振る時に、「血統書」をつける
  - 他人に勝手に譲る、委譲する、などしてもすぐ分かる
  - 証明書の仕組みで明示的に禁止する事もできる

- リソース証明書を元に、OriginとPrefixの関連付けができる。（Prefix所有者の権利）
  - かってにPrefixが使われない

- 経路の検証ができる
  - あやしいPrefixがすぐわかる。
    - Origin Validation：BGPで受け取るPrefixが、正しいOrigin ASを持っているか検証
  - 調査の結果、適切かもしれないが、少なくとも異常を検知する仕組みとなる

おまけ

- SPAM対策、Malware対策にも実は有効
  - Active経路をHijackし、SPAM・Botに活用
  - ゴースト経路(割り振られた組織がアドレス放棄)をのっとってSPAM・Botに活用
  - 未使用、不正アドレスをSPAM・Botに活用



根本解決ではないが、少なくとも証明書を
使えばこういう事はやりにくくなる

～オペレーション観点で見るRPKI～

経路広告とアドレスの関係

- 忘れがちな大原則：

  【IPアドレスの割り振りを受けた組織が、どのASをOriginとするか、判断する権利がある】

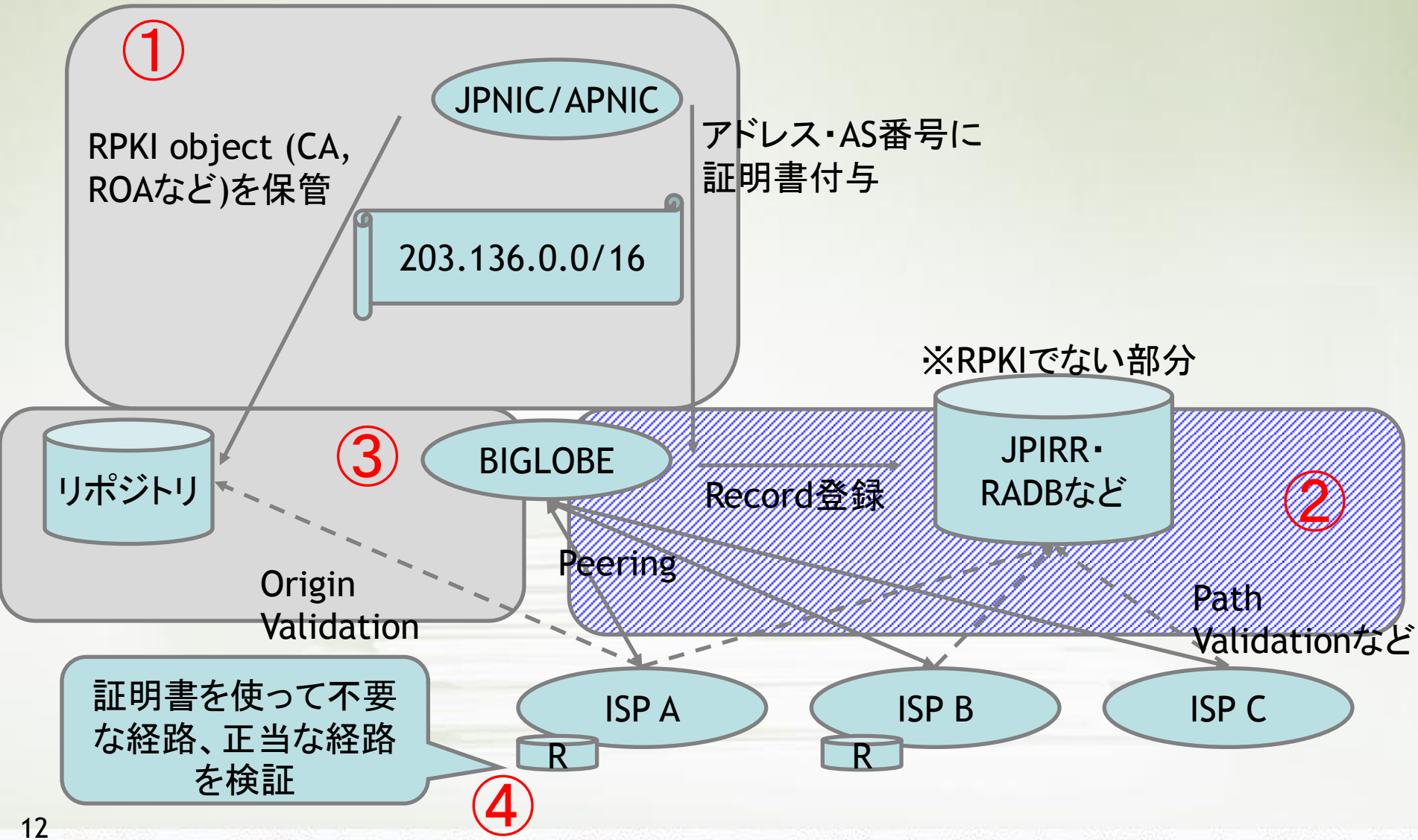
  つまり、BIGLOBEが割り振りを受けたアドレスをAS2518から出すか、AS45674から出すかは、BIGLOBEの自由。

- 今までRIR・NIRは、ルーティングに＊基本的には＊関与していない

  アドレスを誰がどう広告するかは、割り振りうけた人の勝手。

RPKIの原点でもある（はず）

RPKIアーキテクチャ：実際の姿とオペレーション



RPKIアーキテクチャ：実際の姿とオペレーション

① アドレス・AS番号の証明書発行はすでに始まっている。

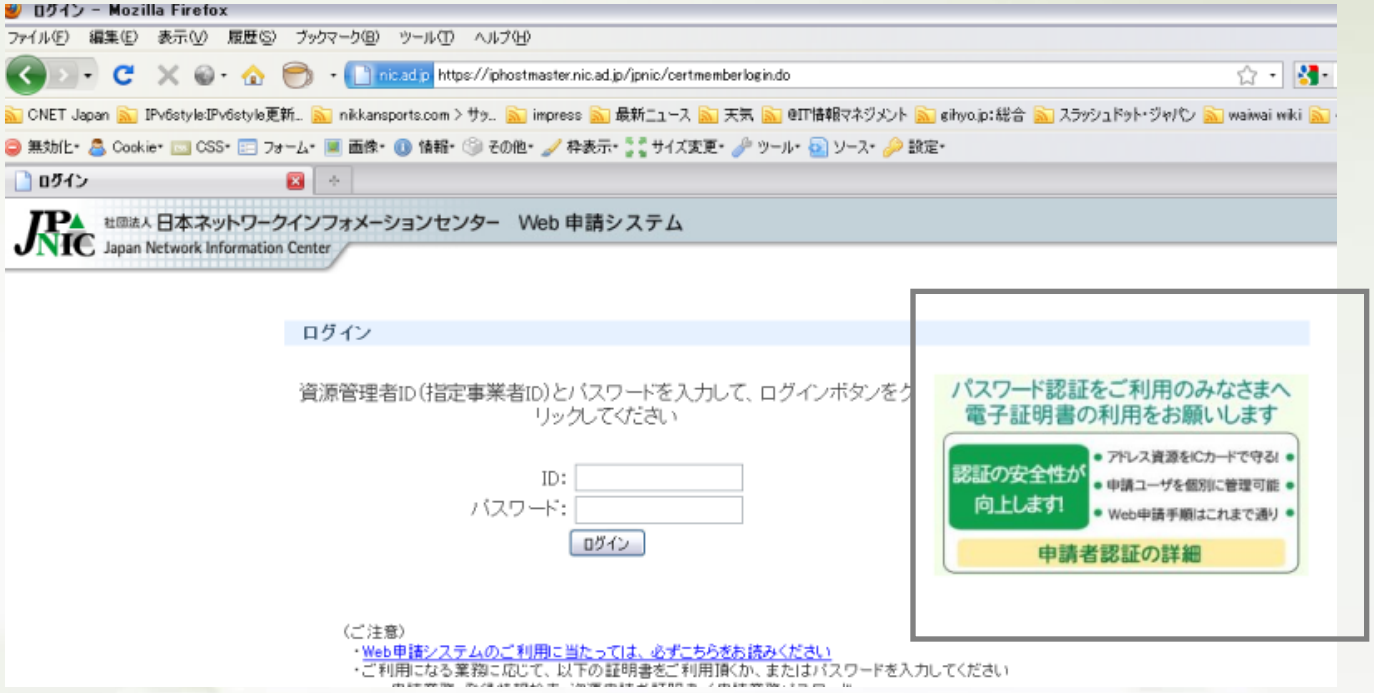
② 今まで参照していたJPIRR・RADBなどの信頼性があがるのかは不明。RPKIアーキテクチャには、現状登場しない（securing RPSL objects with RPKIというのはある）

③ リポジトリなるものが見えてきているが今後の運用形態が見えていない。

④ 証明書検証の仕組みとルータコンフィグの連携はプロトタイプレベルのものしかない。BGP外部での動き。
※近々でBGPへ機能追加される事は考えにくい

＜参考＞RPKIとJPNICの「電子証明書を用いた認証方式 」の関係

- JPNICにアドレス申請する際電子証明を使ってます。

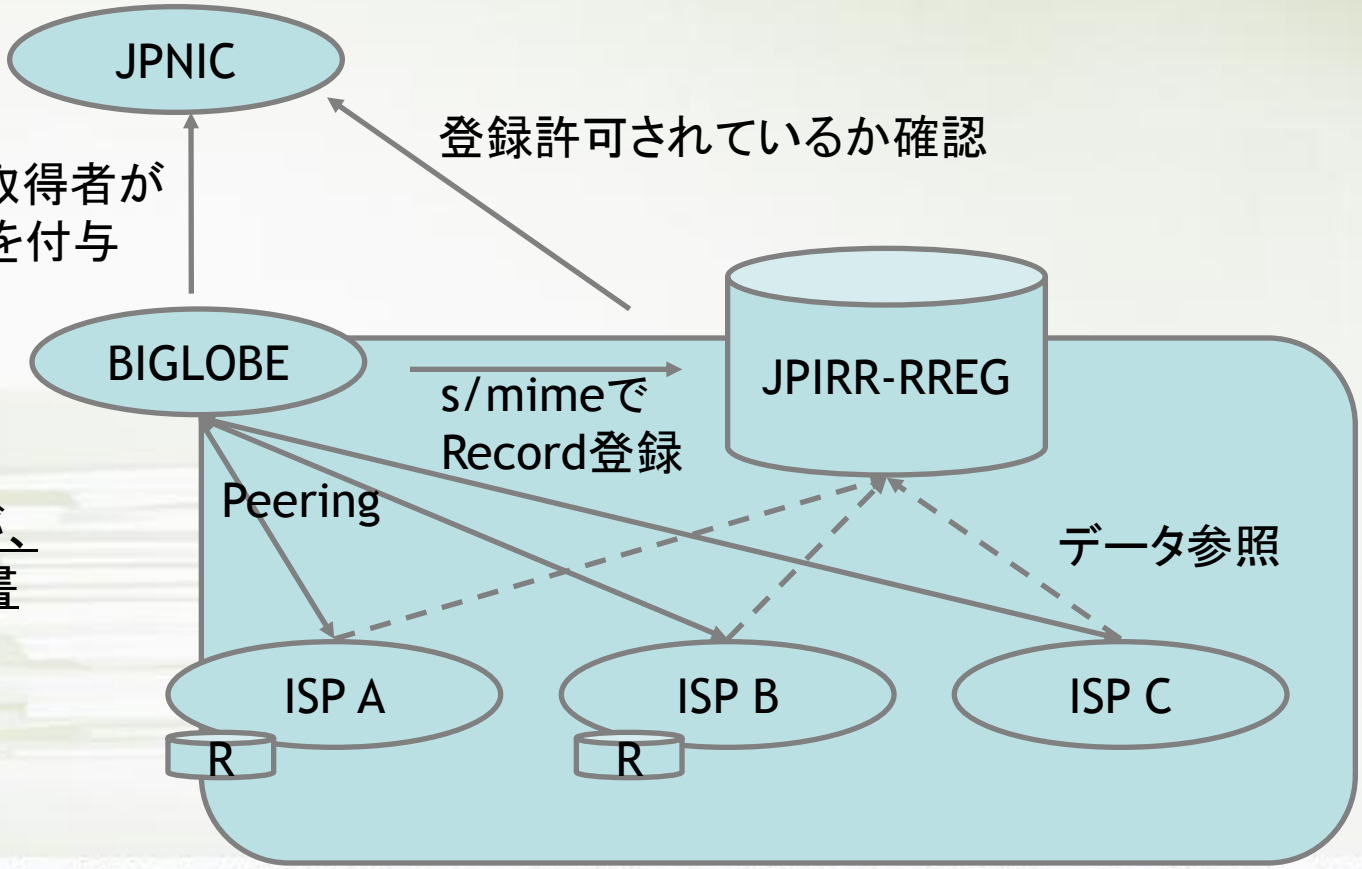


ここ

関係ありません。WEBへのログイン用証明書と、リソースの証明書は別です。

＜参考＞RPKIとJPNICの「経路情報の登録認可機構」の関係

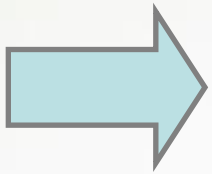
- RPKIアーキテクチャの目指している考え方の一部分を実装しているが、**RPKIではありません**



証明書を使いますが、
アドレス・ASの証明書
ではないです。
「人（メンテナ）」の
証明書です。

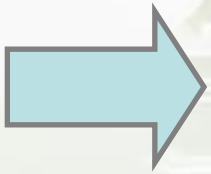
RPKIとアドレス業務

- アドレスの割り振り、割り当て業務に拡張する形と捉えるとわかりやすい。
  - 割り振りを受けると、アドレスと一緒に証明書をもらう
  - ASをもらうと、番号といっしょに証明書をもらう



楽そう

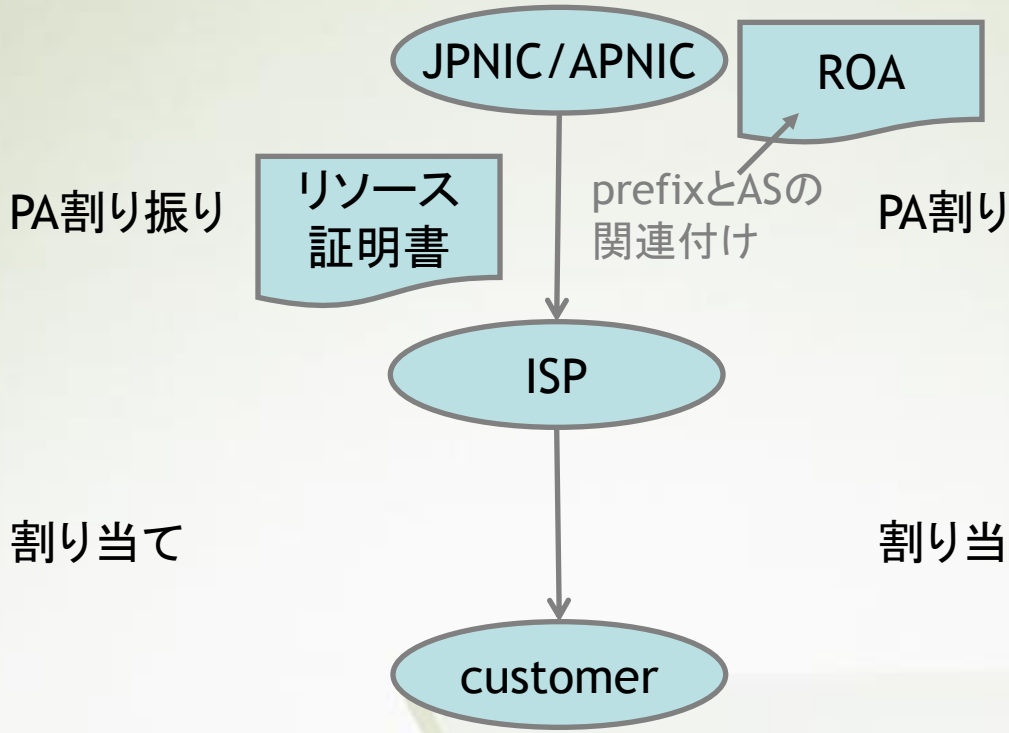
- 再割り振り、割り当てとともに、証明書を発行する

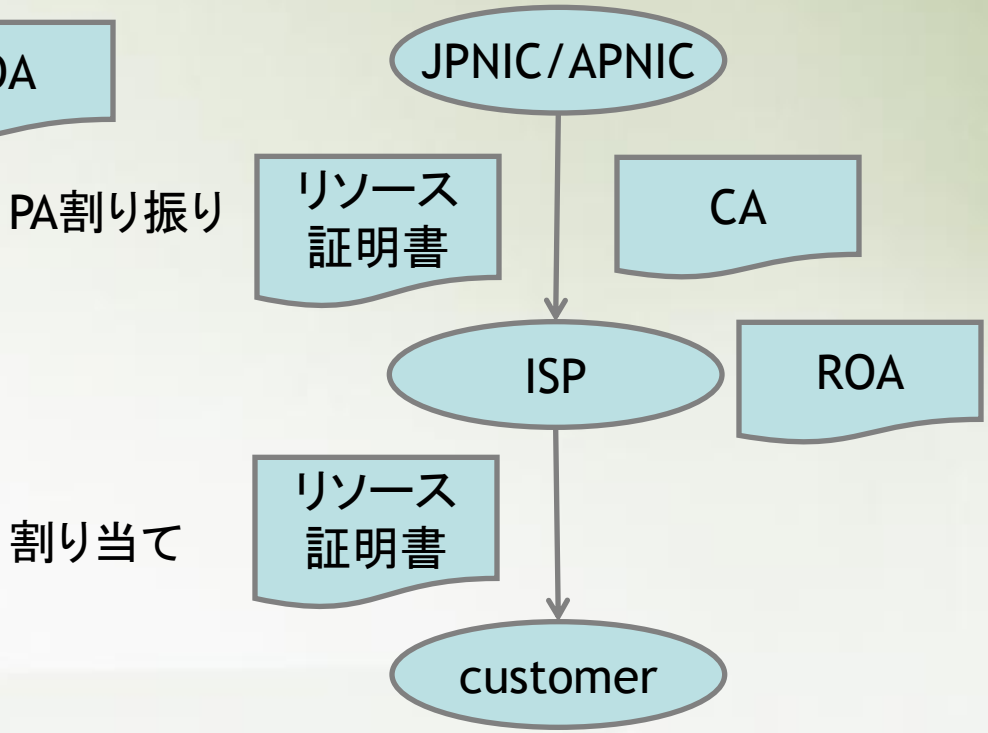


面倒そう

- 部分的な導入が考慮されているため、まずはRIRや、上位ISPの動向を見よう

RPKI導入イメージ





【パターン1:初期導入】
・JPNIC/APNICが認証局を運用
・ISPはJPNIC/APNICのWebなどから
証明書取得、ROAの署名を行う。
ISPは認証局を運用しない。
・customerはRPKIに参加できない
※トライアル的イメージ

【パターン2: full RPKI】
・ISPが認証局を運用する。
・CustomerはRPKIに参加できる。
・ISPはユーザ向けインタフェースと
機能が必要(ROA署名など)。
・ISPには証明書運用の知識が必要。

RPKIとルーティング業務

RPKIが導入されると、現状のルーティング業務は
どのように変化すると推測されるのか

- IRRベース/メールベースのAS-PATHフィルタは、しばらくそのまま。ただしこのままだと今後増える脅威には対応できない。
- 【新規】IRRに経路登録するように、ROA（PrefixとASの関連付けに署名）を作成する必要がある。
- 【新規】ROAを元に、他社から受け取る経路を検証。

ポイント

現状のRPKIの仕組みでは、AS-PATHフィルタ相当のものは無いため
既存の運用をすぐに辞めることにはならない。

RPKIで不安な要素

【全体的に見えていないもの】
- 認証局を運用するコスト、運用負荷
- インシデントリスク（証明書に関するトラブル）
- 信用チェーンの運用モデル(trust anchor)

【ISP(アドレス運用者)に必要となりそうな投資・開発】
- 認証局用サーバ（バックエンドシステム）
- 顧客への提供Interface

【オペレータに必要となりそうなツール】
- リソース証明書収集・検証ツール
- ROA検証ツール（フィルタの仕組み）

事業者としてフォローすべき情報、タイムスケジュール

- 現状様子見でも問題ない
  - まだJPNICからリソース証明書をもらう事はできない
  - リソース証明書だけでは何もできない

- 何がキーなのか
  - IETFの標準化
  - RIR/NIRからの案内

- 今やるべきこと
  - 現状の仕組みでできる範囲をしっかりやる
  - DB参照、ハイジャック検知に慣れておかないとRPKI運用も大変

おまけ：ネットワークエンジニアがやれること

- 現状IETF（sidr-wg）で議論されているRPKIで問題が全て解決されるわけではない。

- 運用しにくい実装はルータファームを重くしてコスト増になるだけ。

- IRRの検証とRPKIを両方運用するのも負荷。オペレーションモデルが、まだあまり考慮されていない。

IETF、NICのMeetingなどでの積極的な議論がRPKIをより良くします