RPKI試してみませんか
JANOG35

２０１５年1月１６日

一般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

JPNIC 一般社団法人 日本ネットワークインフォメーションセンター

RPKIに至る前

- **ルーティングは相互信頼が基本**
  - あて先の情報は基本的に信頼
- **たまにおかしくなっても仕組みが単純**
  - 普及ハードルが下がる
- **たまにおかしくなる**
  - Mis-Origination/ハイジャックによる吸い込み
  - 気づいた人が不正確な経路を遮断し数時間で回復
- **経路フィルタをかけて防止しよう**
  - IXでのメールベースの経路フィルタ
  - IRRを参照した経路フィルタ

数時間おかしくなるリスクはあるが単純で普及が容易

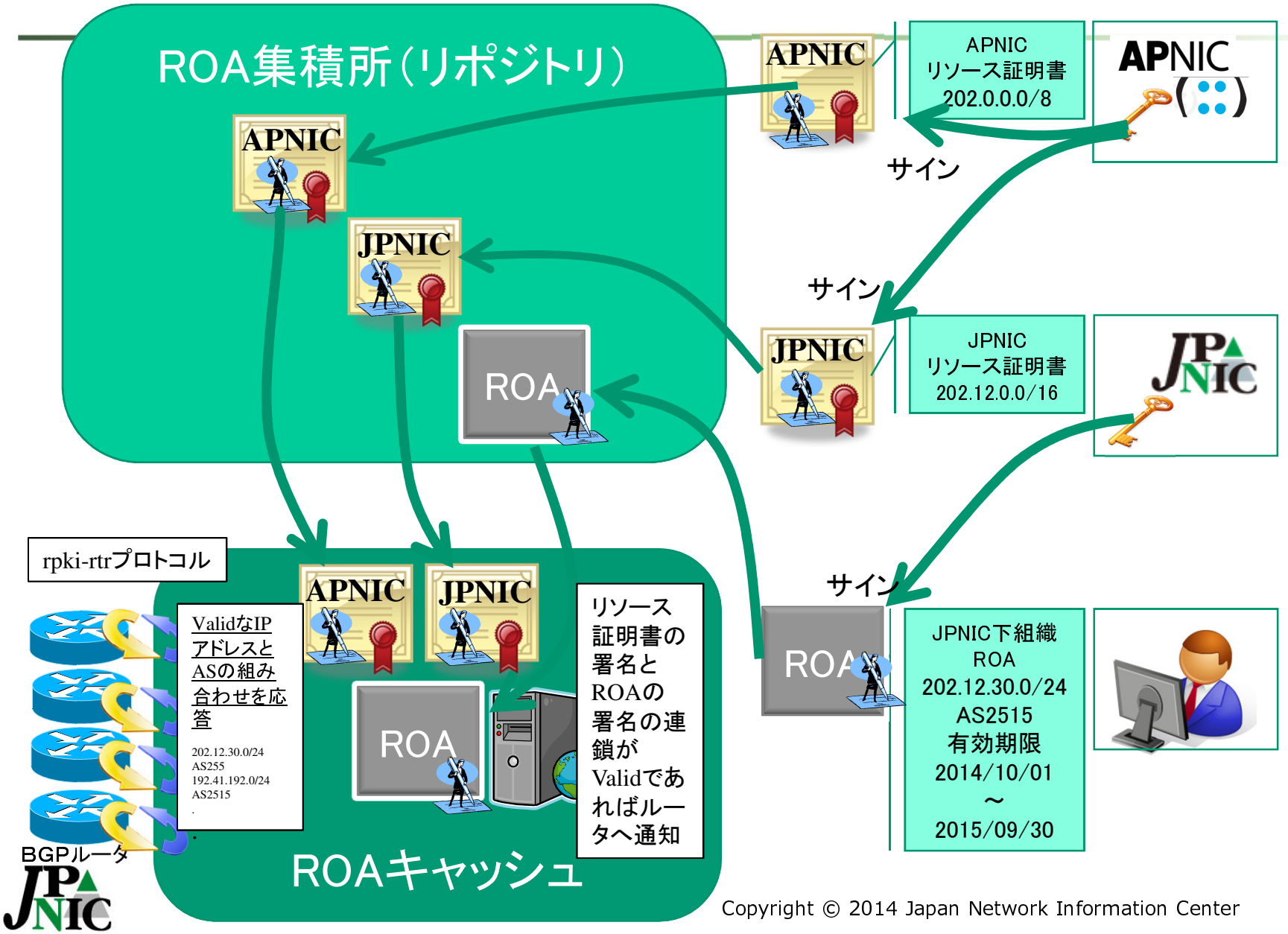
インターネットの普及・発展

- **Mis-Origination/経路ハイジャックの実害**
- **対策データベースのIRRの限界**
  - 自己申告データをどこまで信じるのか？
  - 検索結果の改ざんの対策は？

    →まったくなし
- **どうやってIPアドレスとASの正しい組み合わせを判別しよう？？？**

RPKIの長い道のり

Resource PKIの（ほぼ）全部



必要な仕組み

（ほぼ）レジストリがやる

- **“僕のIPアドレスだ！”(注意)を証明する仕組み**
  - IPアドレス＋電子証明書＝リソース証明書
- **僕のIPアドレスがどのAS番号で広報されるのか意思表示する仕組み**
  - IPアドレス＋AS番号＋電子署名＝RouteOriginAuthorization（ROA　ﾛｫｳｱｰと発音）
- **これらの証明書・を公開・収集する仕組み**
- ~~**証明書・ROAの正しさを検証する仕組み**~~

運用者

- **Origin Validation**
  - ルータがROAを参照して制御する仕組み

いよいよネットワーク運用者に鍛えてもらいたい時期


白山岳
3776
剣ヶ峰
頂上浅間大社奥宮
頂上富士館
成就ヶ岳
富士宮ルート頂上
九合九勺
胸突山荘
九合目
万年雪山荘
八合目
池田館
衛生センター
（夏期臨時診療所）
山口山荘
七合目
新七合目
御来光山荘
宝永山荘
宝永火山
雲海荘
六合目
レストセンター
新六合目
2390
富士宮口新五合目
公衆トイレ
富士山総合指導センター

課題

Max-lenの活用の現状（１）

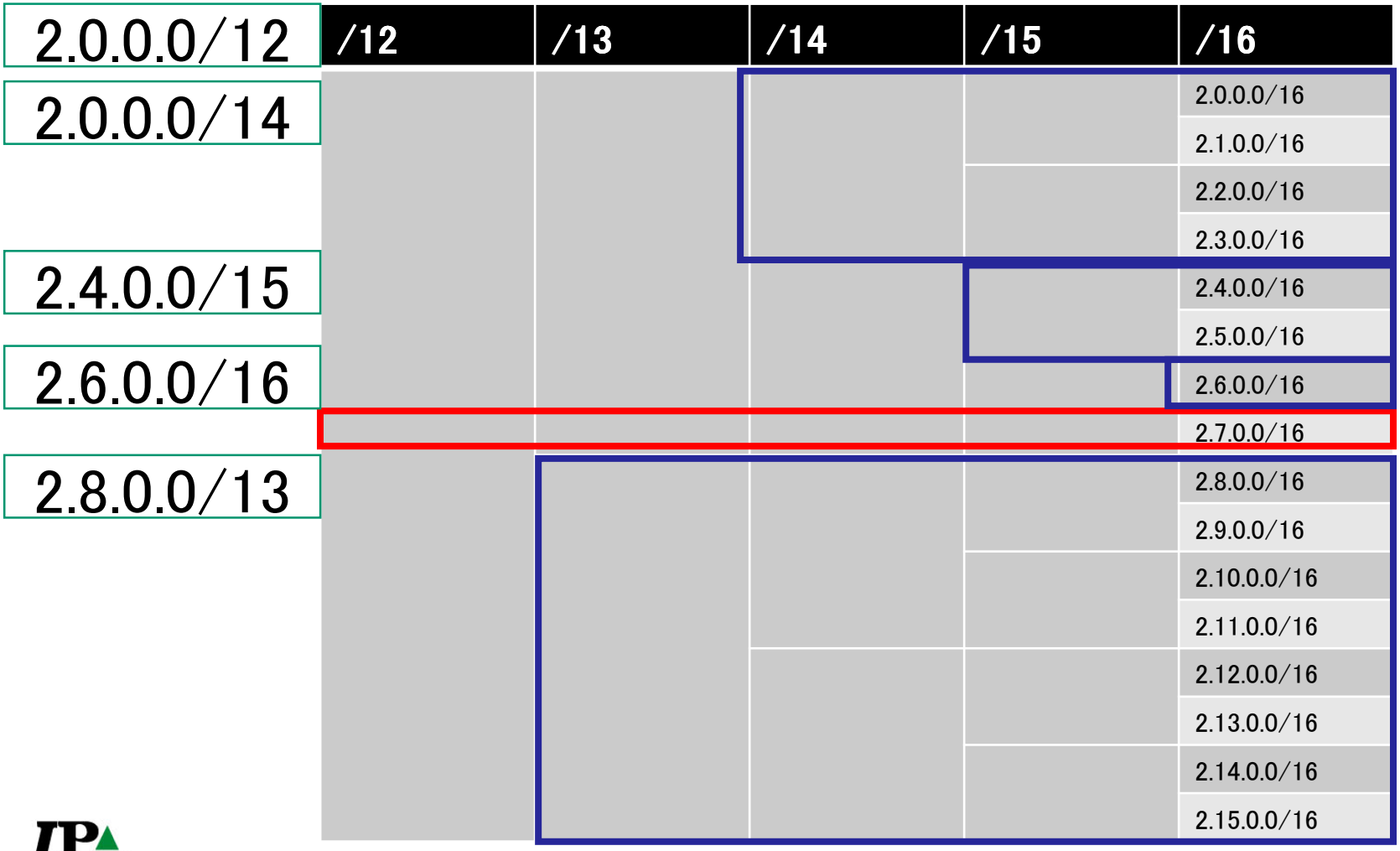
- **IRRにあわせてROAを細かくしている人が存在**
  - IRRにMax-lenの概念がない

ROA	IRR
2.0.0.0/12-16　ASXXX	2.0.0.0/12　ASXXX 2.0.0.0/13　ASXXX 2.0.0.0/14　ASXXX 2.0.0.0/15　ASXXX 2.0.0.0/16　ASXXX

IRR側にあわせるためROAが増大する

Max-lenの活用の現状（２）

- ROAから一部のアドレスを除きたい(のかな？)



ROAキャッシュをどこにおくべきか

- **rpki-rtrプロトコルはValidationに関連した署名情報をルータへ渡さない前提**
  - キャッシュにはIP/ASの情報しかない
- **IP/AS情報の改ざんを検出できない**
- **キャッシュは**
  - 信頼できる組織＋信頼できるトランスポート経由
- **ルータに近いところへキャッシュは置く必要**

これからキャッシュについては議論・改善される（はず）

まだまだ議論の余地があります

- ROAと異なる経路の取り扱い
- ルートリフレクタがある場合のValidation
- Anycastの証明書・ROA
- オレオレルート証明書RPKIの是非
- RPKI発行組織を狙ったソーシャル攻撃

- DDoS　mitigationとの共存?？？？

パブリックキャッシュサーバ

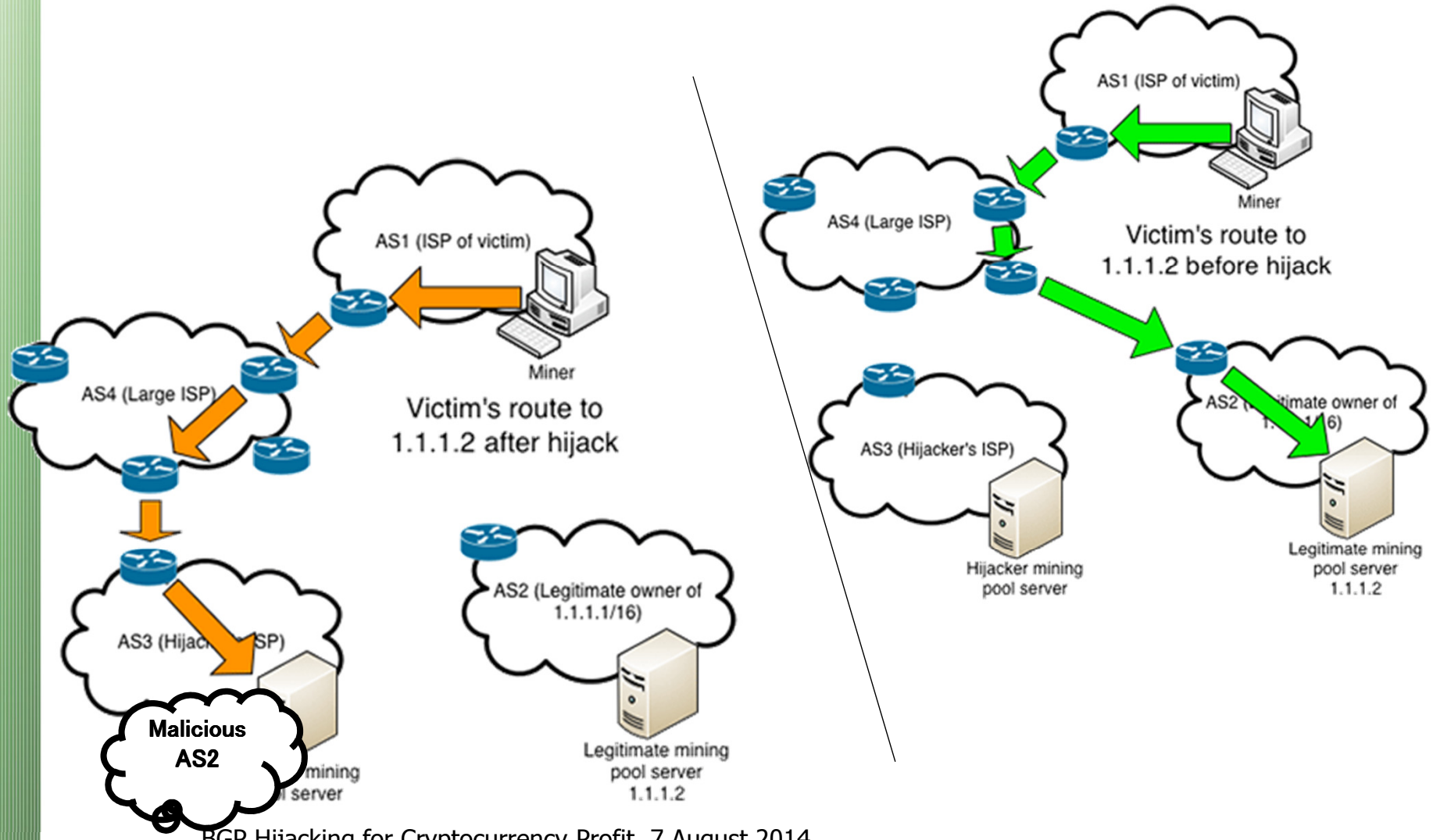
インターネットマルチフィード様Webより

Origin Validationがあれば防げた例

- **あるIPアドレスを別のASが僕のIPアドレスだ！と宣言してしまう例**
  - Mis-Origination
  - 経路ハイジャック
- **事例**
  - 古代の事例　　：AS7007
  - 有名な事例　　：Youtube
  - ここ数年の事例　　：大陸からの疑わしい事例
- **RPKIによるOrigin Validationが有効**

よくある誤解：RPKIが普及すればすべてOK→×
RPKIによるOrigin Validationの普及が必須

Origin Validationの効果が低い事例



BGP Hijacking for Cryptocurrency Profit, 7 August 2014
Pat Litke and Joe Stewart, Dell SecureWorks Counter Threat Unit
http://www.secureworks.com/cyber-threat-intelligence/threats/bgp-hijacking-for-cryptocurrency-profit/

僕たちのたたかいはまだまだ続く

- BGPSEC：Path Validationも必要
- ~~次回作に~~ さらなる進歩にご期待ください

皆様に使っていただくことが改善へ

- みんなでRPKI/ROAワールドに漕ぎ出そう