（I）RPKIの動向 ～実装状況とIPアドレス利用や移転に関するRIPEでの議論 ～

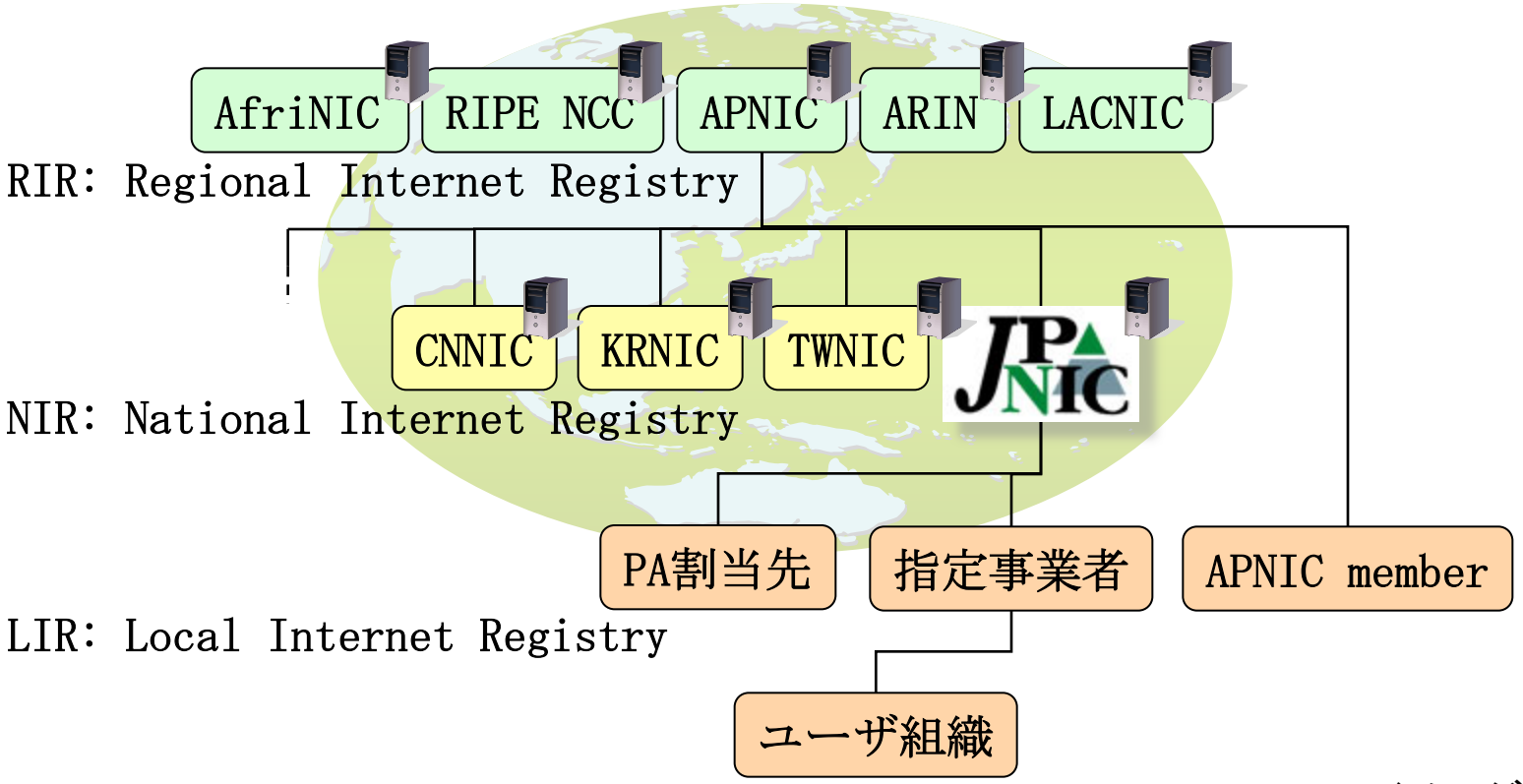
社団法人日本ネットワークインフォメーションセンター
木村泰司

内容

- RPKIについてRIRの中で最も先行するRIPE地域の動向
  - 第64回RIPEミーティング（RIPE64）での話題
  - どういう状況で何が課題となっているのか
- 日本におけるRPKIの展望と課題

Resource PKI（RPKI）

- RIRで準備が進められている、「リソース証明書」を提供する仕組み



RPKIのイメージ

RIPE64におけるRPKIの話題

- RPKIチュートリアル
  - 初のチュートリアル
- ポリシーWGでの議論
  - 「移転するアドレスの正当性を確認するためにリソース証明書とROAを使う」という考え方がWG内にある
  - 一時検討されたが、ポリシー提案に至っていない
- プレナリーでの議論
  - RPKIのインターネット運用への影響

RPKIチュートリアル

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

チュートリアルの概要

- 管理モデルは、(1)メンバーで各自立ち上げてRIPE NCCを上位認証局（トラストアンカー）とするか(2)RIPE NCCにホストしてもらうモデルの2つ
- ROAの管理とルータにおける解釈
  - VALID: ROA found, authorised announcement
  - INVALID: ROA found, unauthorised announcement
  - UNKNOWN: No ROA found (resource not yet signed)
- RPKI テストルーター
  - Cisco
  - Juniper

RPKIテストルーター

- Cisco
  - rpki-rtr.ripe.net
  - telnet username: ripe, no password
  - “sh ip bgp 93.175.146.0/24 (or your prefix)”, “sh ip bgp rpki table”,
  - “sh ip bgp ipv6 unicast rpki table”, “sh ip bgp rpki server”
- Juniper
  - 193.34.50.25, 193.34.50.26
  - telnet username: rpki, password: testbed
  - “show validation session detail”, “show validation statistics”, “show validation database”, “show route protocol bgp validation-state valid”

チュートリアルでの質疑応答（主なもの）

- **失効によって起こることは何か？**
  - originの検証に失敗するが、BGPルーターでそれをどう扱うかはやり方による。Looseモードでおこなうと失敗したことがわかるだけ。
- 秘密鍵をRIPE NCCに持たせることは不安ではないのか？短期間ではWebのツールはいいが、長期的にはよくないのでは。
  - その通りであるが、いずれはユーザのチョイスであると思う。

プレナリーでの議論

RPKIに関する発表

- プレナリー（4/17第二部）
  - ROAの検証と発行について, Randy Bush氏（IIJ）
    - ルータにおけるROAのチェック方式の説明。prefixが長過ぎるものは無効とする。
    - プライベートアドレスのような、経路広告されないIPアドレスへの対応方法：AS0などの紹介
  - リソース証明（RPKI）のセキュリティ ～耐性、自律性～ Alex Band氏（RIPE NCC）
    - ROAに入れるprefixをまとめて管理できるUIの紹介。**前回の第63回RIPEミーティングで指摘されたことへの対応**として。

前回のRIPE63ミーティングで挙げられ今回議論された3つの懸案事項

- 1. AS運用の自律性が失われる可能性
  - 法執行機関によりRIRがリソース証明書の操作(失効等)を行う可能性があること
- 2. RPKIシステムのセキュリティ
  - RPKIのシステムが不正に侵入されたり、エラーが起きたりする可能性があること。（経路制御に影響する可能性があるため、セキュリティ対策が重要になる）
- 3. RPKIシステムの耐性
  - RPKIシステムの動作不良が起きうること。リソース証明書等のデータが取得できなくなることで経路制御に影響する可能性があること。

会場での議論（1／2）

- 1. AS運用の自律性が失われる可能性
  - インターネット経路制御が依存するところ（すなわち政府（法執行機関）がインターネットの経路制御に関与できるポイント）をいかになくすか
    - 「RIPE NCCがあるオランダの法律は、実際にルーターがあるオランダ外では関係なく、この提供者と運用者の状況の違いも考慮する必要がある」
  - ルーターにおけるトラストアンカーの設定が、ルーティングオペレーターに委ねられていることで独立性を担保できると言えるか
    - そこまでは言えない。。

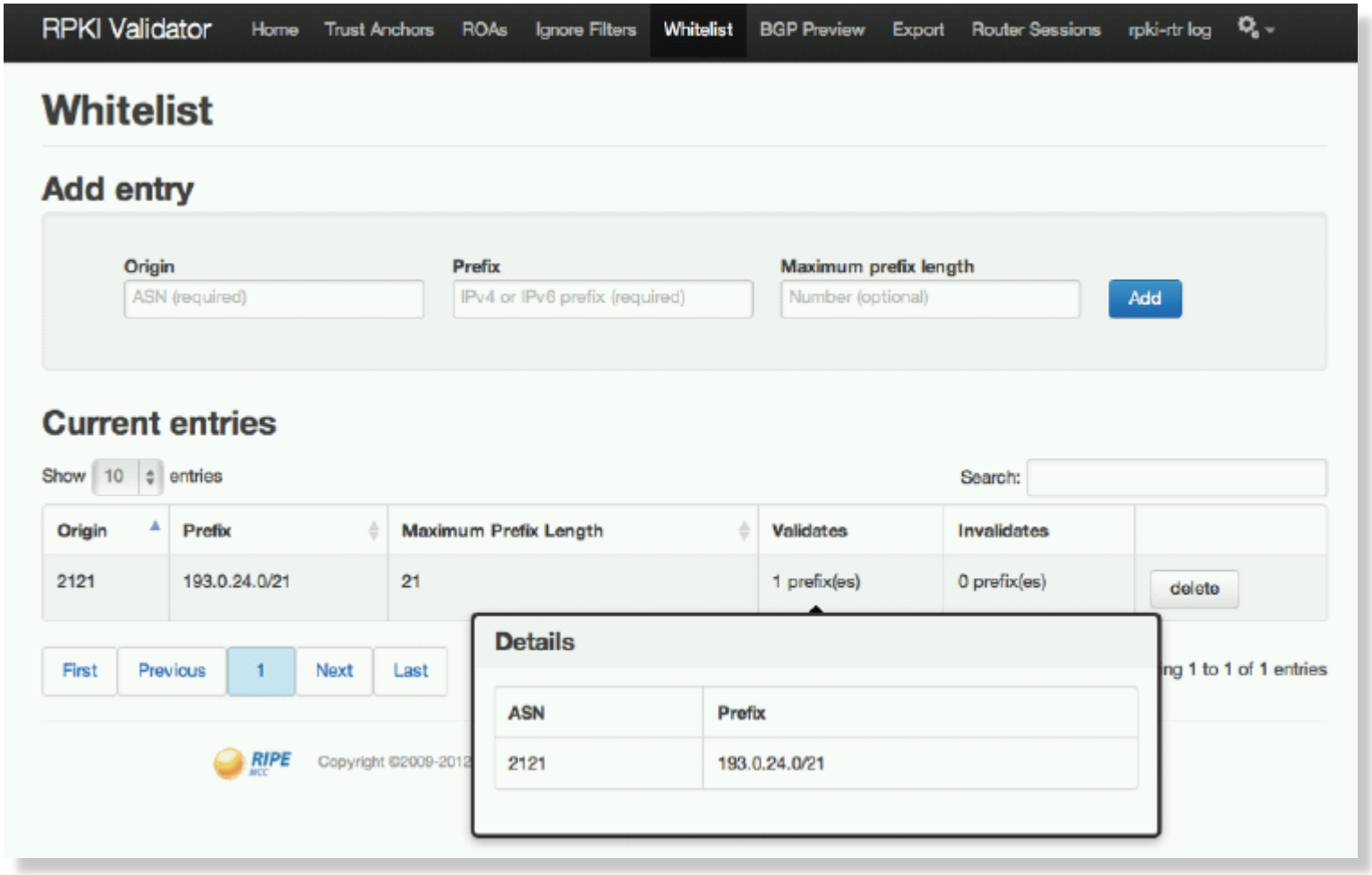
会場での議論（2／2）

- ホワイトリストとブラックリストの方式でうまくいくか
  - スパムフィルターと同じで、他人に登録されたらそれを直すのは結局人手で行わなければならない。
  - ルーターや他の実装でもRIPE NCCのように行われるとは限らない。
- **結論のような意見：アドレス管理が階層的に行われていることはもはや変えられないし、インターネット経路制御に対するASの独自性に影響するようなことは避けるように考えていこう**

対応案

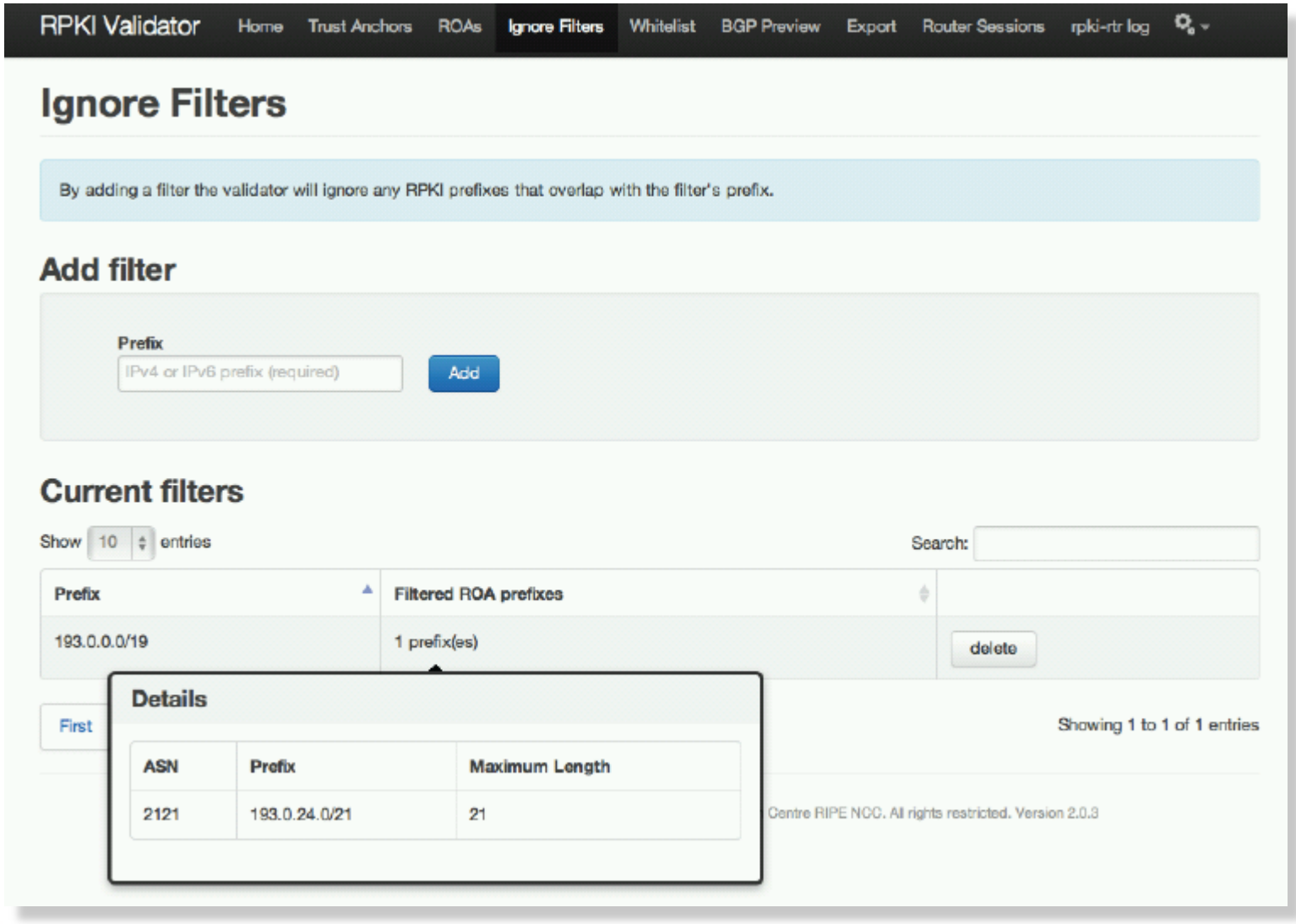
- トラストアンカーを設定するのはルーターのオペレーターであるという点を踏まえた上で...
- RIPE NCCのツール「RPKI Validator」の機能の改良（案）
  - RPKIの検証結果を無視する設定
    - White List (Apply RPKI status ‘Valid’)
    - Ignore Filter (Apply RPKI status ‘Unknown’)

現在のWhite List操作画面



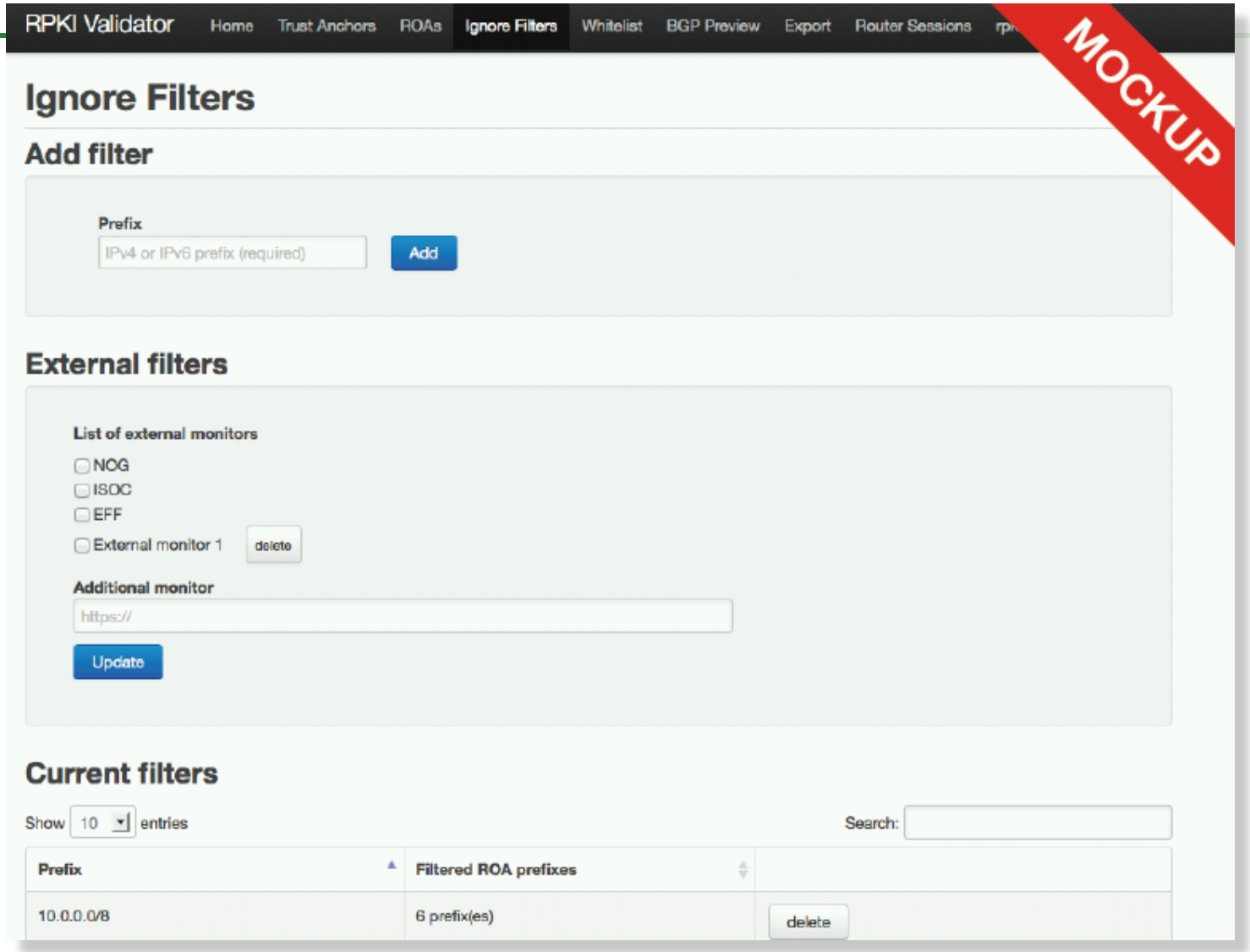
Alex Band氏の発表資料より

現在のIgnore Filter操作画面



Alex Band氏の発表資料より

改良案



Alex Band氏の発表資料より

2, 3.RPKIシステムのセキュリティと耐性

- ユーザ認証の強化
  - SMSを併用した二要素認証
  - 8,000名以上（72ヶ国）で使える方式として
- 独立した人員による認証局のコード評価
- 障害と攻撃への対応
  - Hosted Certificate and ROA management
    - LIR Portal
  - Non-hosted Parent Certificate system
    - up/down
  - Data retrieval
    - RIPE NCC ROA Repository

第63回RIPEミーティング（前回）の議論

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

RIPE63のRIPE NCC総会における決議事項

- RIPE NCCはRPKIの取り組み(以下2点)を続ける
  - リソース証明書はオプトインで提供
  - BGPの Origin Validation に関するプラットホームを提供

RIPE NCCとしてRIPEメンバーが賛同していると認識している事項(3点)

- アドレス資源の検証可能な証拠(リソース証明書)を提供するサービスを行うこと

- BGP Origin Validation に期待される活用方法(以下2点)
  - 経路ハイジャック(意図的でないものを含む)を防ぐこと
  - BGPのパス検証を行うBGPSECへの布石になること

- これらのメリットが潜在的なリスク(以下2点)よりも重みを持つこと
  - BGPによる経路制御においてオペレーターのコントロール範囲を狭める
  - RPKIのなんらかの障害によってネットワークが到達しなくなることがある

日本におけるRPKIの展望と課題

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

日本における現状と今後の見通し

- 現状
  - RPKI testbedなどの実装があり日本国内でも、ローカルでRPKIを試すことができる
  - ルーターにおける実装は進みつつあるが、低価格のルーターで稼動させるには至っていない
  - JPNICでも検証環境を準備中
- 今後の見通し
  - 実効性を持って導入される状況ではないが、実装が増えていく見通し
  - RPKIが運用可能であり効果を持つのかの検証がより重要になってくる

RPKIに関する課題

- RPKIの運用と実効性
  - リソース証明書を発行する認証局、証明書などを配布するリポジトリ・証明書を検証するルーターなどがRPKI導入の効果を発揮できるように運用可能なのかの検証など
- ルーティングの自律性やRPKIシステム耐性
  - リソース証明書がある状況で自律性をどう担保するかの検証と整理
  - RPKIシステム（発行サイドと検証サイド）に耐性をどう持たせるか、枠組みの検討

⇒国内で検証を行っていく時期になってきたと考えられる

まとめ

- RPKIに関する論点
  - 1. AS運用の自律性
  - 2. システムセキュリティ
  - 3. RPKIの耐性
- RIPE地域では整理と対策の議論が進められている
- 日本でも技術的な検証と共に上記の論点を踏まえた検討を行っていく必要がある

おわり