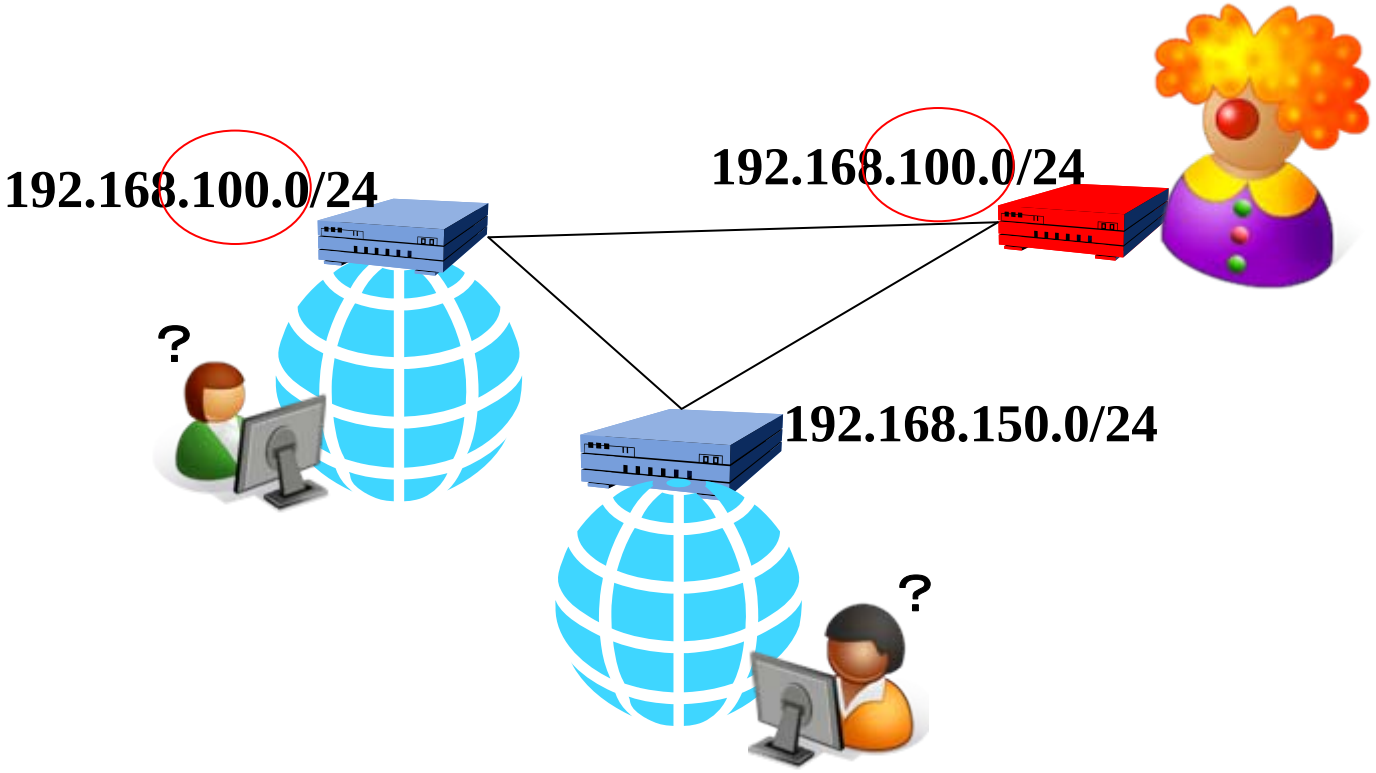
ルーティングセキュリティ関連状況
～Secure Inter-Domain Routing (SIDR)～

IETF報告会（86thオーランド）

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
木村泰司

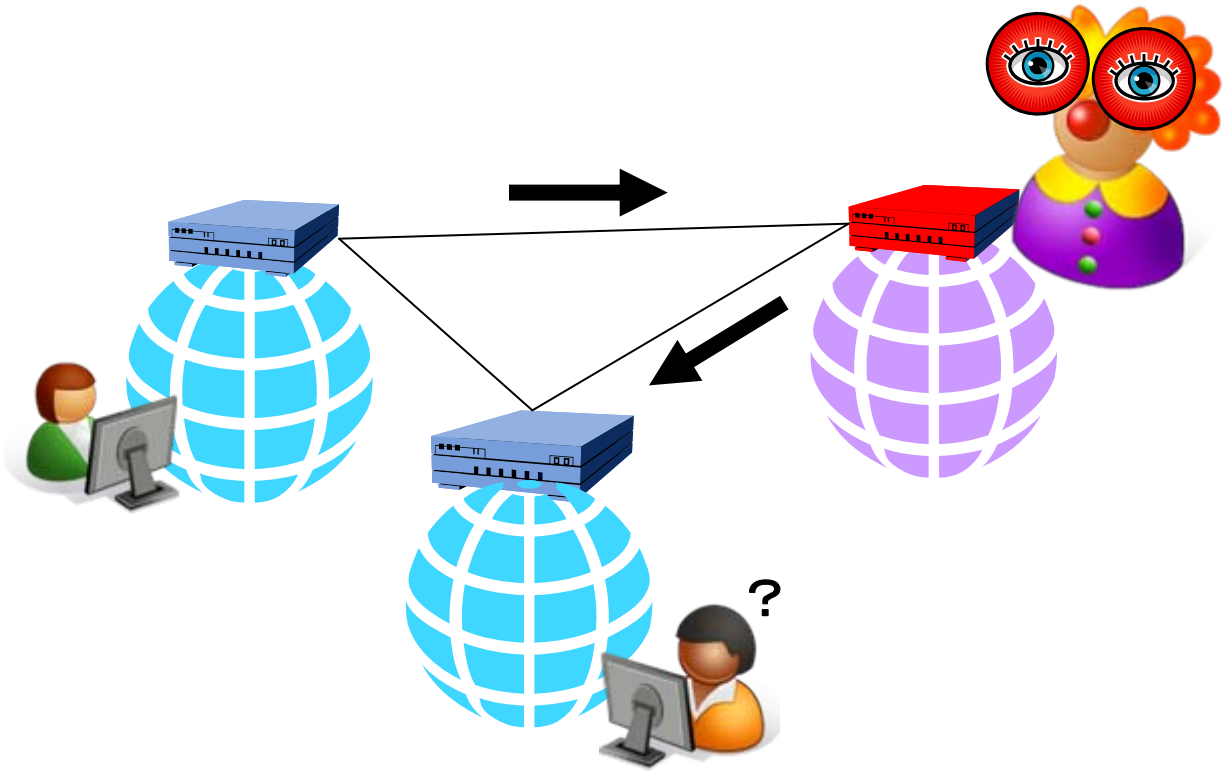
インターネットへのつなぎ方　良くない例（1）

- インターネットに接続したBGPルーターで、他人のIPアドレスを設定する。



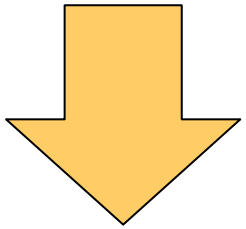
インターネットへのつなぎ方　良くない例（2）

- 本来とは異なる経路（ASパス）を設定する。



良くない例の良くない所

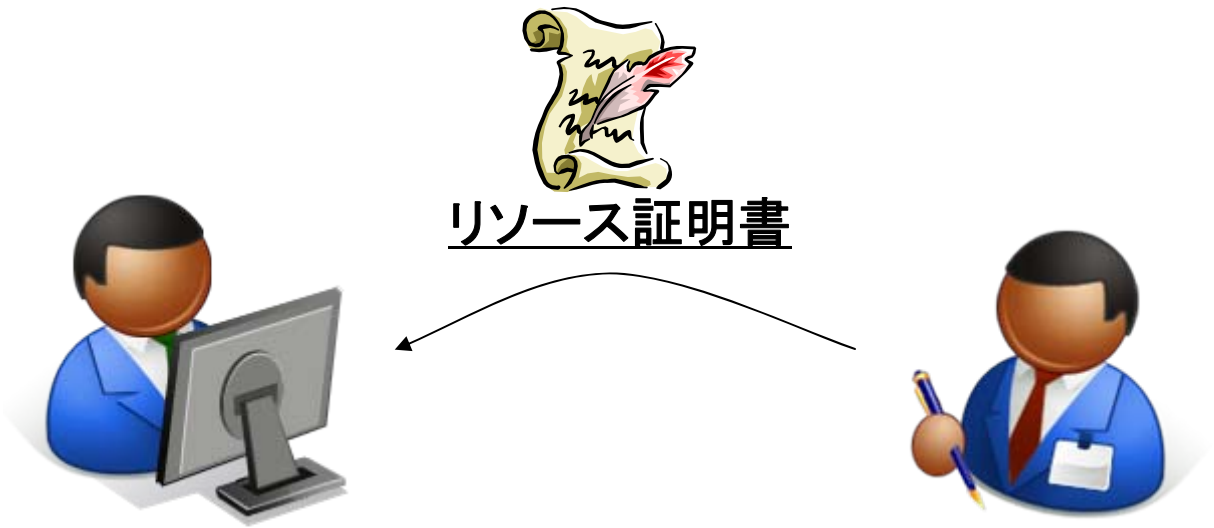
- 何が正しいのかわかりにくい。
  - 被害にあって初めて気づく。



分かるようにする仕組みを考える

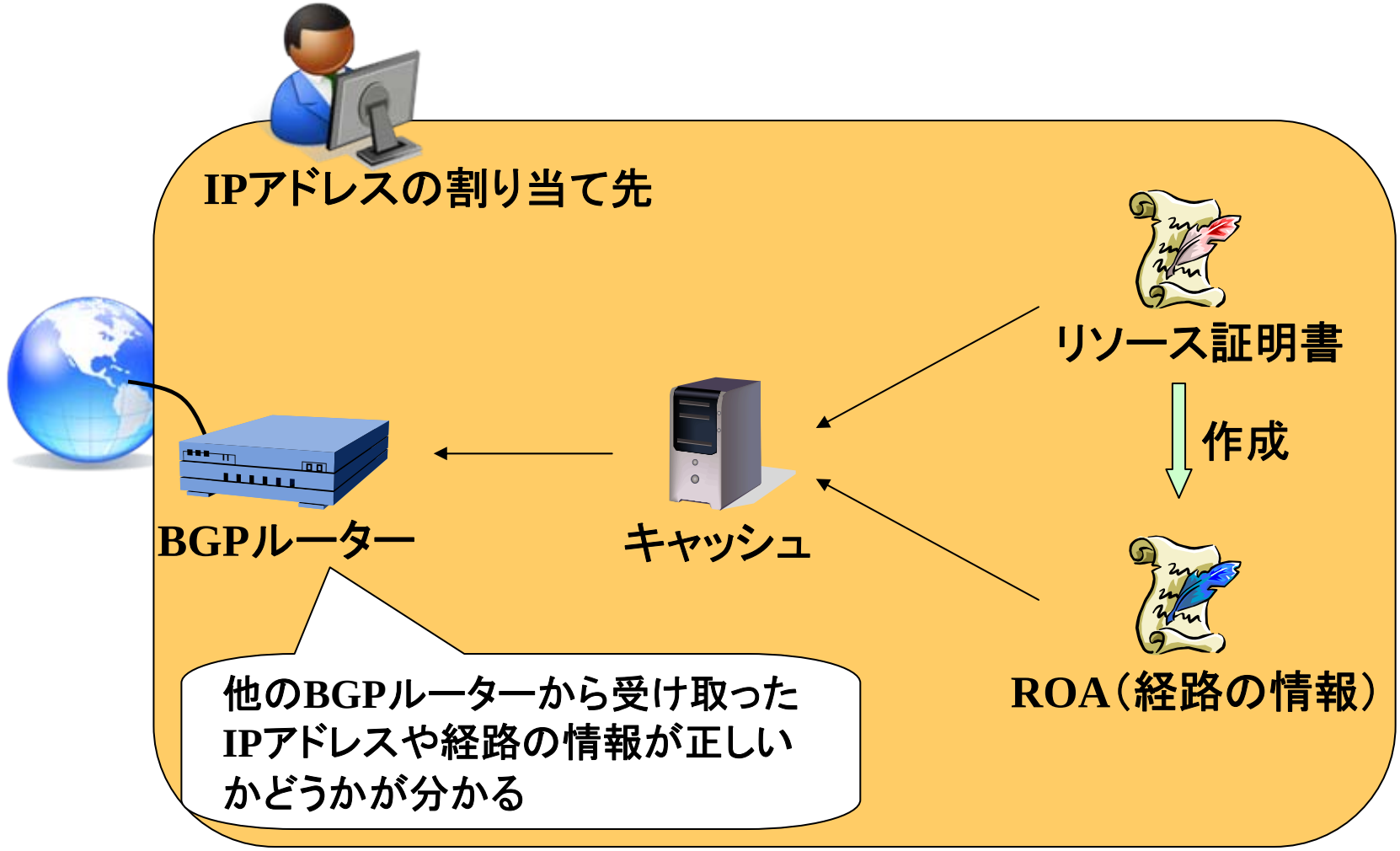
⇒ Secure Inter-Domain Routing WG

リソース証明書

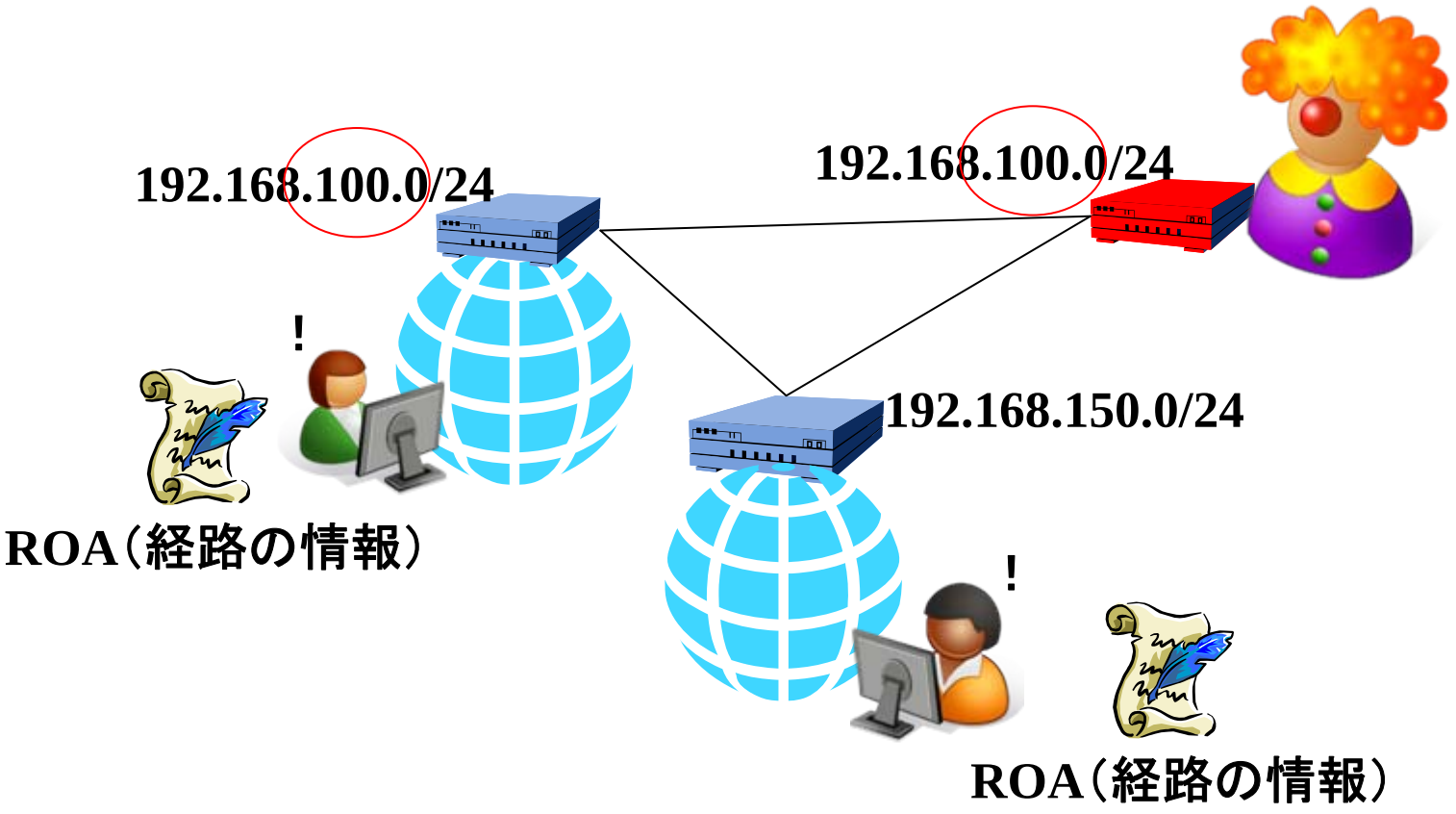


リソース証明書＝IPアドレスやAS番号が書かれている電子証明書

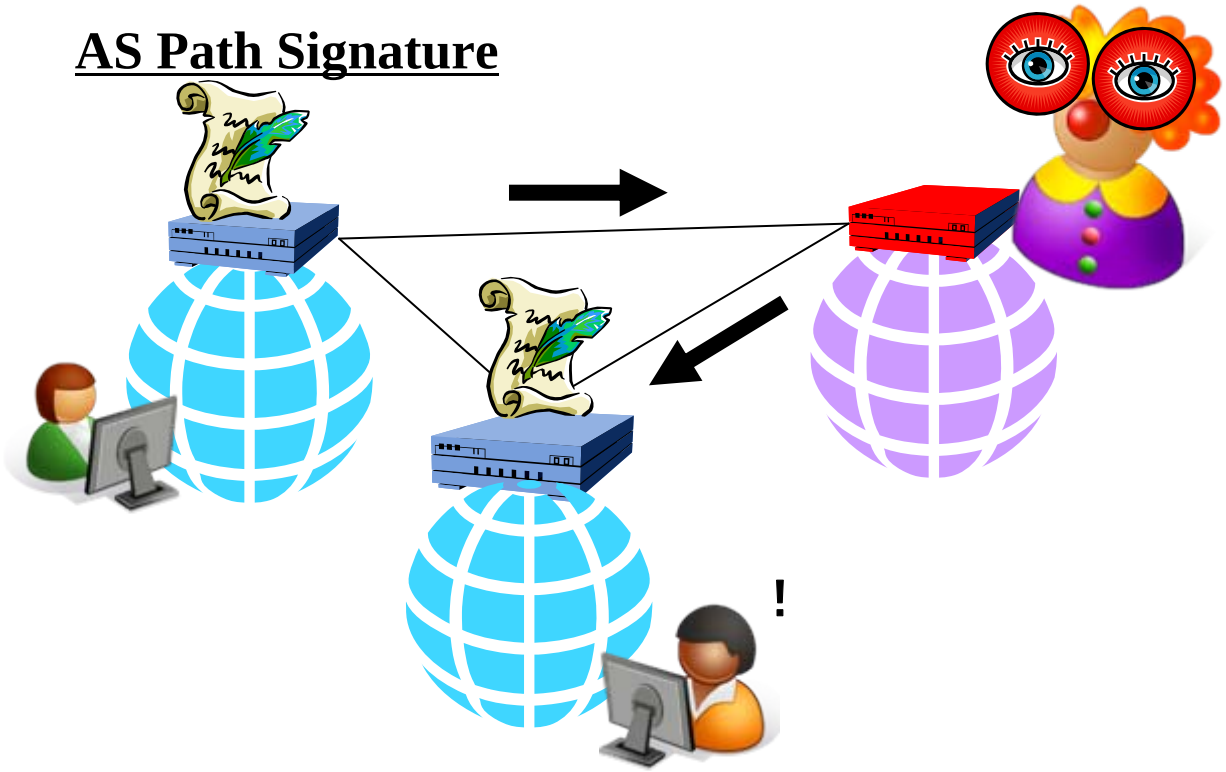
リソース証明書の用途の一つ



Origin Validation



Path Validation



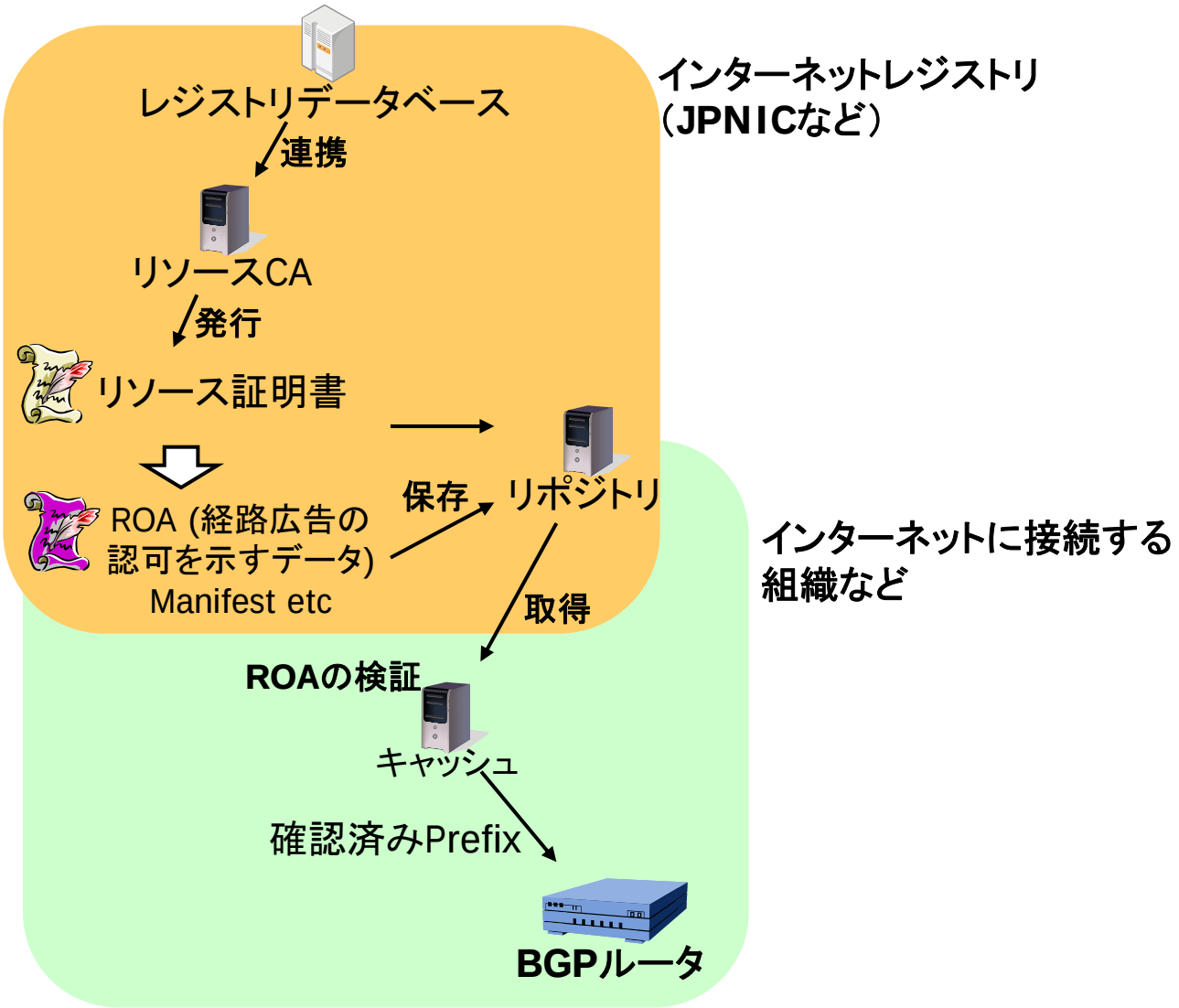
SIDR WGの概要

- Secure Inter-Domain Routing WGミーティング
  - 第一回
    - 2013年3月11日 9:00-11:45 (60名ほど)
  - 第二回
    - 2013年3月12日 10:30-11:23 (40名ほど)

SIDR WG – 概要

- ドラフトドキュメントの議論
- RPKIの性能に関連する話題
  - RPKIを使って発行されたリソース証明書とROAの配布（rsyncを利用）の性能に関する話題
- RPKIに関連した新しい話題
  - WGのドキュメントではないRPKIの話題
- RPKIの実装に関する話題

Origin Validationのための RPKIとBGPルーター連携の図



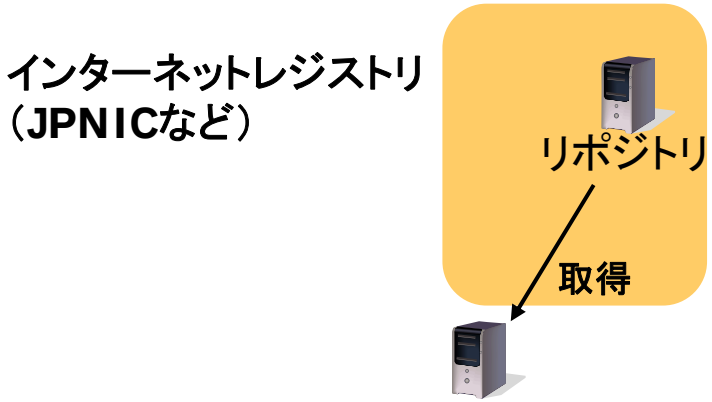
ドラフトドキュメントの議論(1/2)

- BGPSEC Protocol Specification
  - BGP Updateに含まれるASパスへの電子署名と検証方式
- Router Keying for BGPsec
  - BGPルーターにおける鍵とその運用のための鍵の定義（”鍵管理”の議論には至っていない）

インターネットに接続する
組織など

ドラフトドキュメントの議論(2/2)

- Multiple Repository Publication Points support in the Resource Public Key Infrastructure
  - リソース証明書とROAの配布サーバであるPublication Pointに冗長性を持たせる提案
- Policy Qualifiers in RPKI Certificates
  - （WGのドラフトではまだない）
  - Policy Qualifierを入れる提案（RFC6487のUpdate）

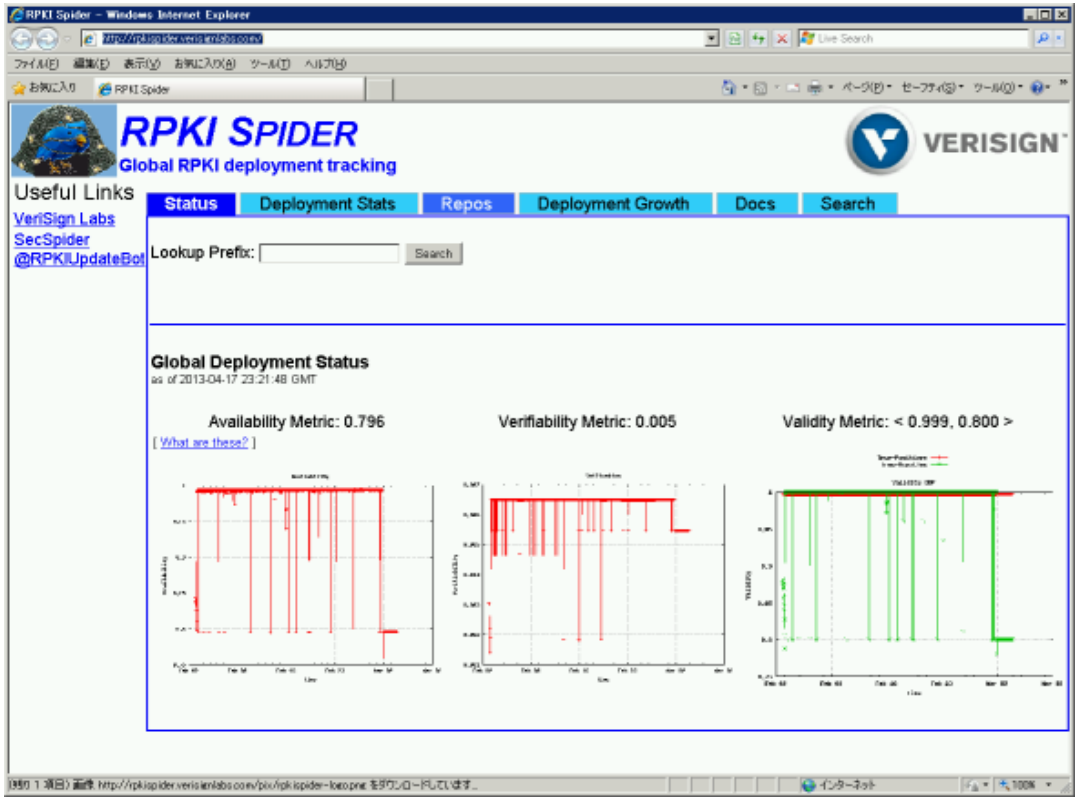


性能に関連する話題（１／２）

- RPKI Repository Analysis and Delta Protocol, Oleg Muravski, RIPE NCC
  - リポジトリのrsyncによる転送性能のスケーラビリティに対する指摘と差分転送のための通知提案
- RPKI rsync Download Delay Modeling, Steve Kent, Kotikalapudi Sriram
  - リポジトリにおけるファイルの変更とネットワーク遅延を考慮したときのシミュレーション

性能に関連する話題（2／2）

- RPKI monitoring system RPKI Spider
  - リソース証明書とROAの可視化（グラフ化）



新しい話題

- APNIC RPKI Report
  - APNICで他のRIRからの移転を受け入れたときのリソース証明書を発行するための実験（？）レポート
- A Look at Classification for Origin Validation
  - ROAの検証結果の扱いに関する考察

RPKIの実装に関する話題

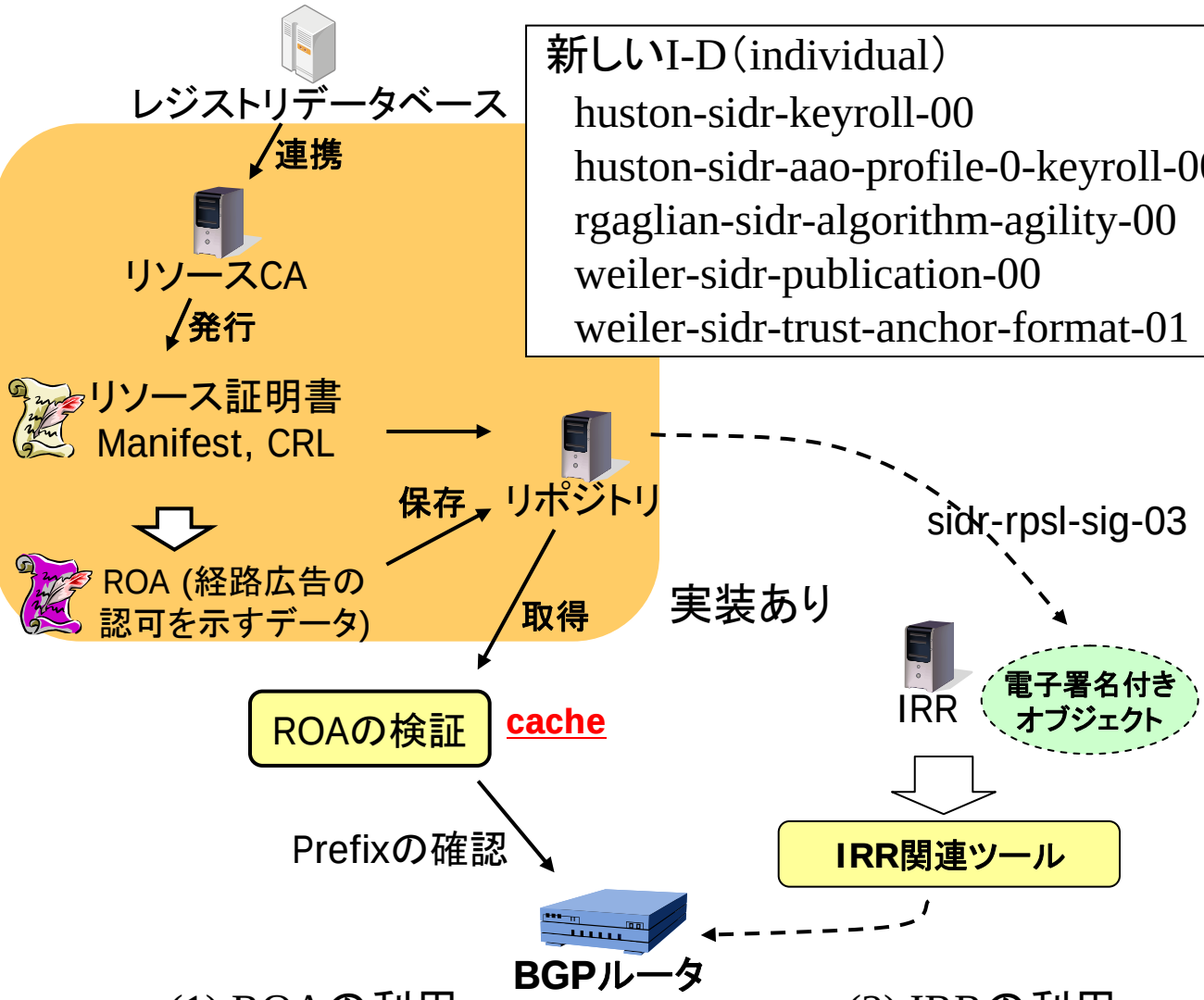
- RPSTIR Validator Testing
  - BBNスタッフによって実装されている検証実験の報告

プロトコル策定の状況(2011年11月)

SIDR WG関連の
ドキュメント

- sidr-arch-11
- sidr-res-cert-20
- sidr-cp-15
- sidr-ta-06
- sidr-repos-struct-06
- sidr-rescerts-provisioning-09
- sidr-rpki-manifest-09
- sidr-rpki-rtr-03
- sidr-roa-format-09
- sidr-roa-validation-10
- sidr-pfx-validate-00
- sidr-usecases-00

新しいI-D(individual)
- huston-sidr-keyroll-00
- huston-sidr-aao-profile-0-keyroll-00
- rgaglian-sidr-algorithm-agility-00
- weiler-sidr-publication-00
- weiler-sidr-trust-anchor-format-01



プロトコル策定の状況（2013年3月）

SIDR WG関連のドラフト
ドキュメント

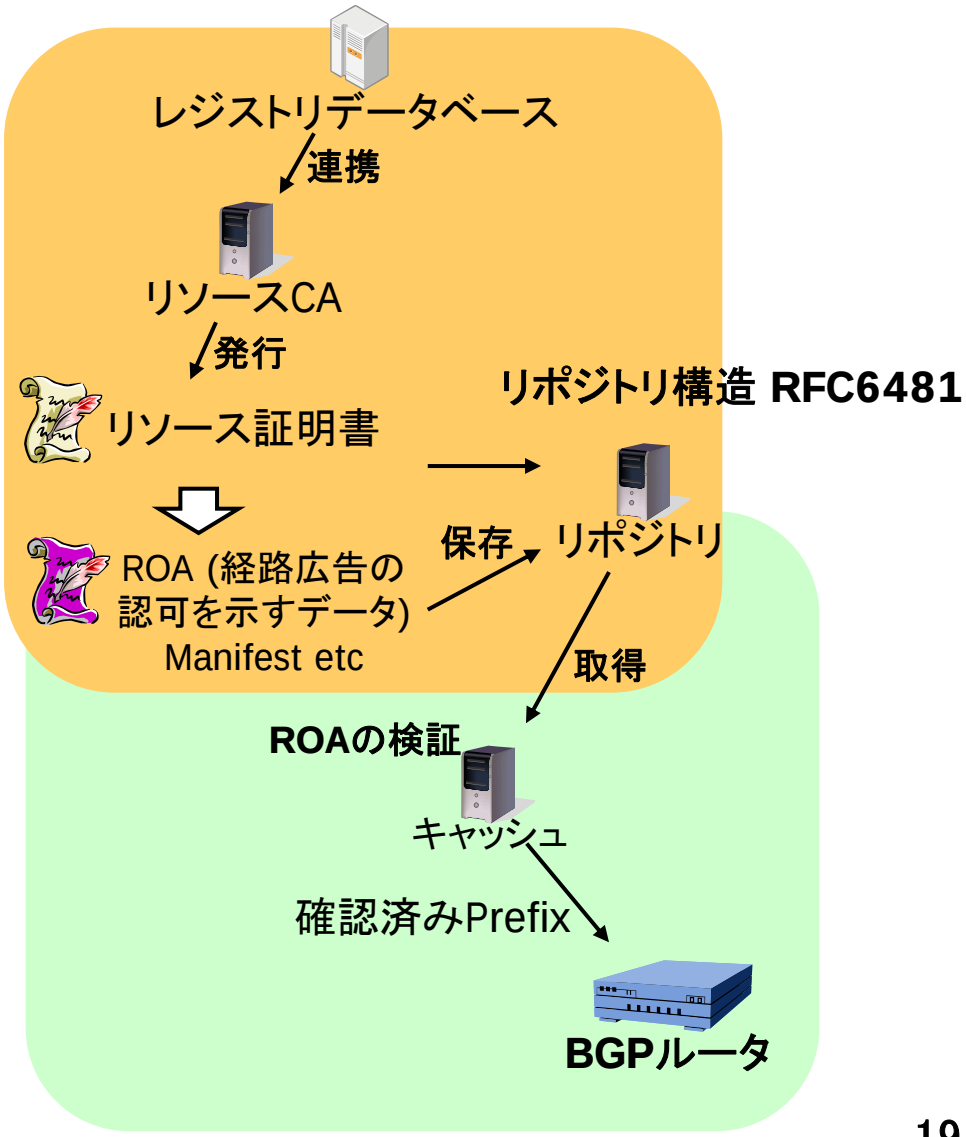
アーキテクチャ RFC6480

証明書プロファイル RFC6487
証明書ポリシー RFC6484
アルゴリズム RFC6485
発行処理 RFC6492

Manifest RFC6486
Ghostbusters RFC6493
ROA書式 RFC6482

トラストアンカー RFC6490
ROA検証 RFC6483
prefix検証 RFC6811

RPKI-to-Router RFC6810



おわり