ルーティングにおける認証

木村泰司

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

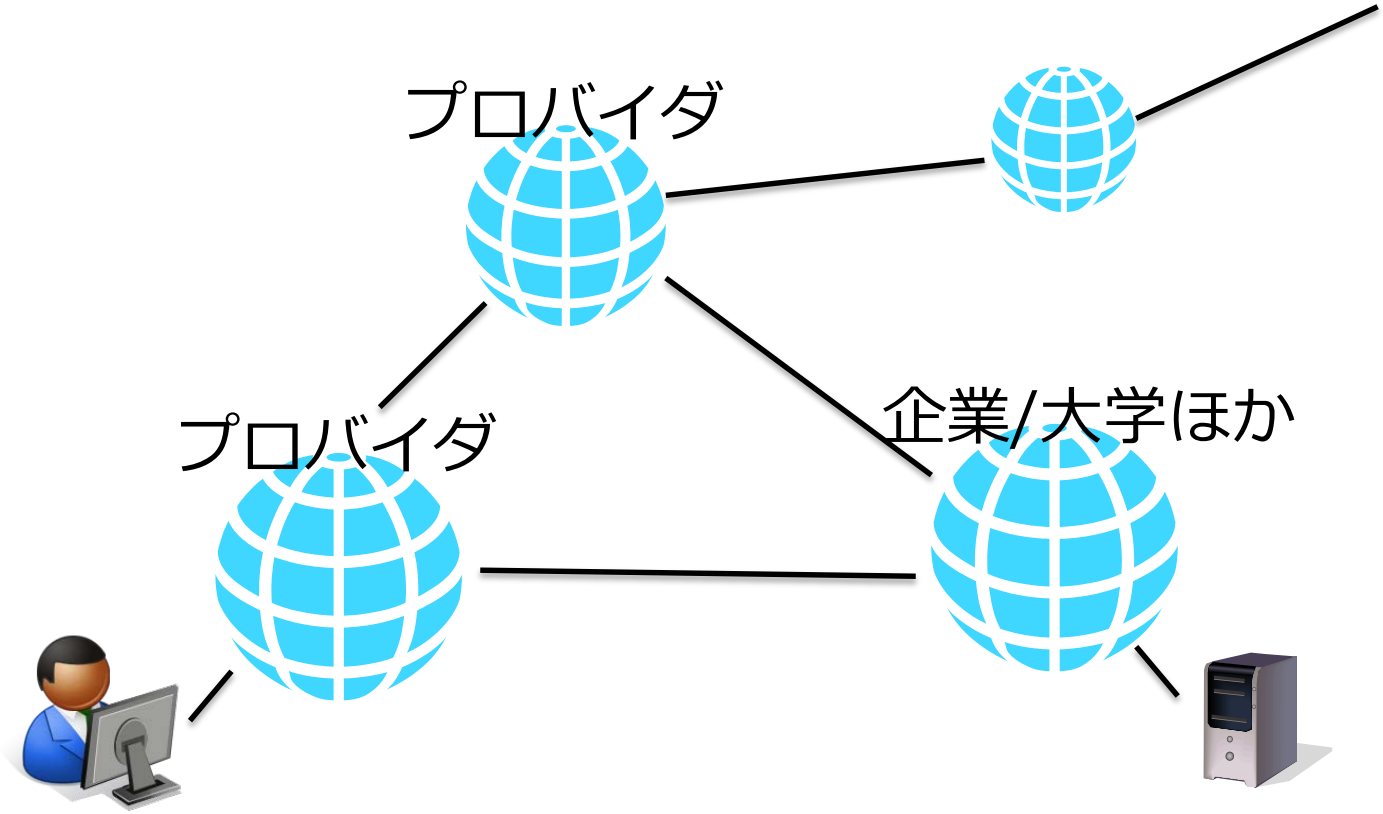
発表者について

- 名前
  - 木村泰司（きむらたいじ）
- 所属
  - 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 (JPNIC)
    - JPNICの認証局・RPKI・DNSSEC鍵管理・セキュリティ関連：開発/運用/ユーザサポート/解説/セミナー/連携/企画
- 参加活動
  - JNSA PKI WG/フィッシング対策協議会/WIDE
- IETF参加
  - MLは1997年頃、ミーティングは2002年頃より

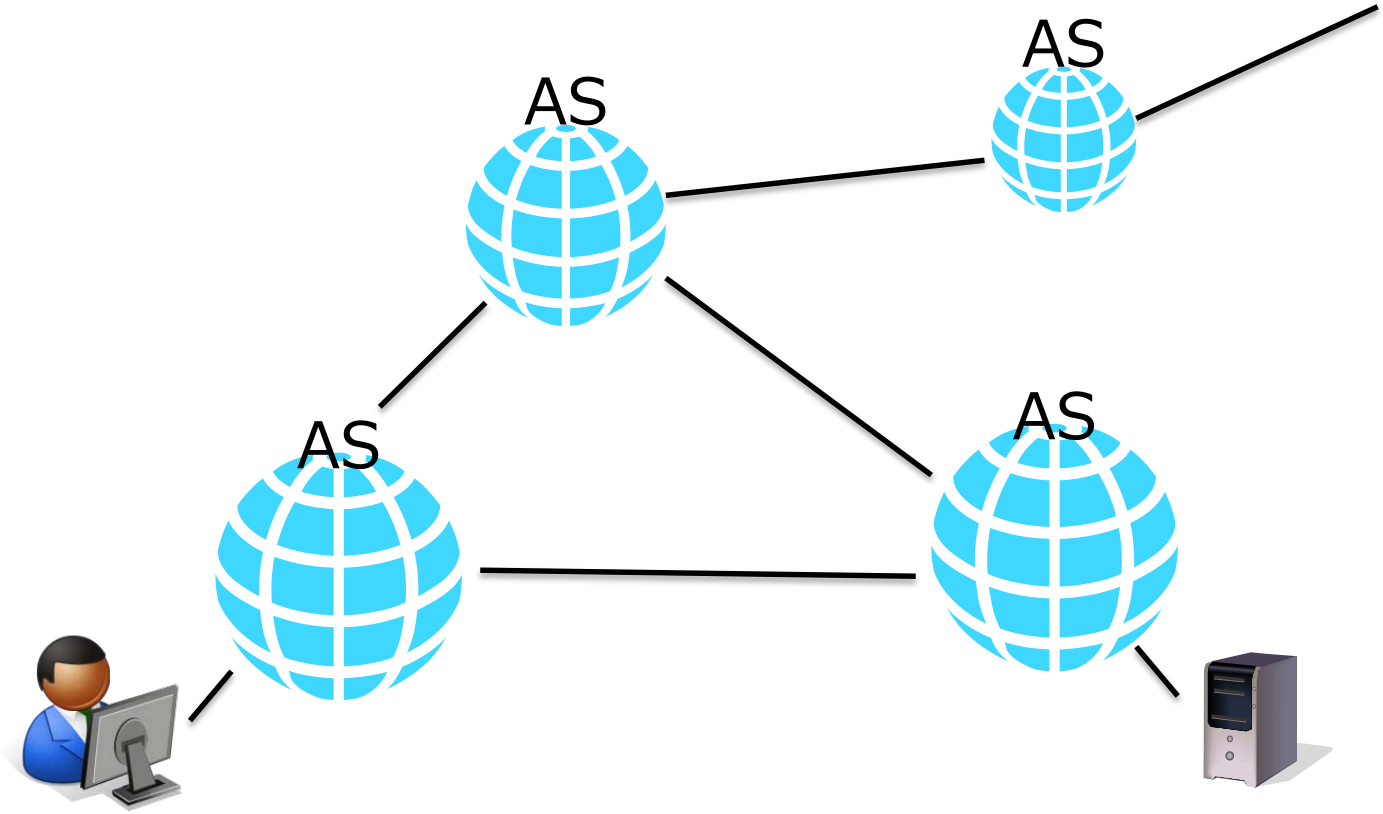
ここで
RPKI入門

インターネットの姿（１）

インターネットの姿（２）

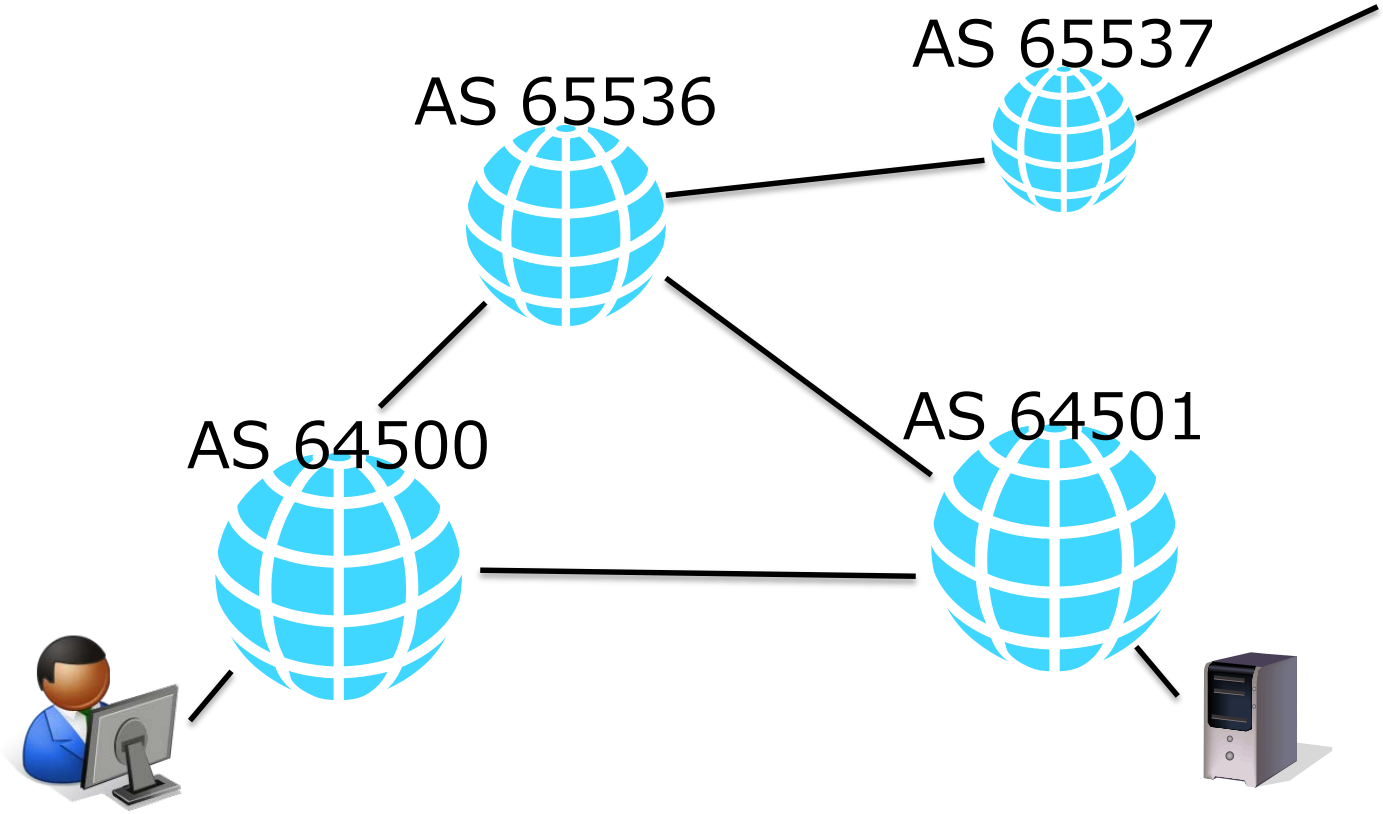


AS(Autonomous System) – 自律システム



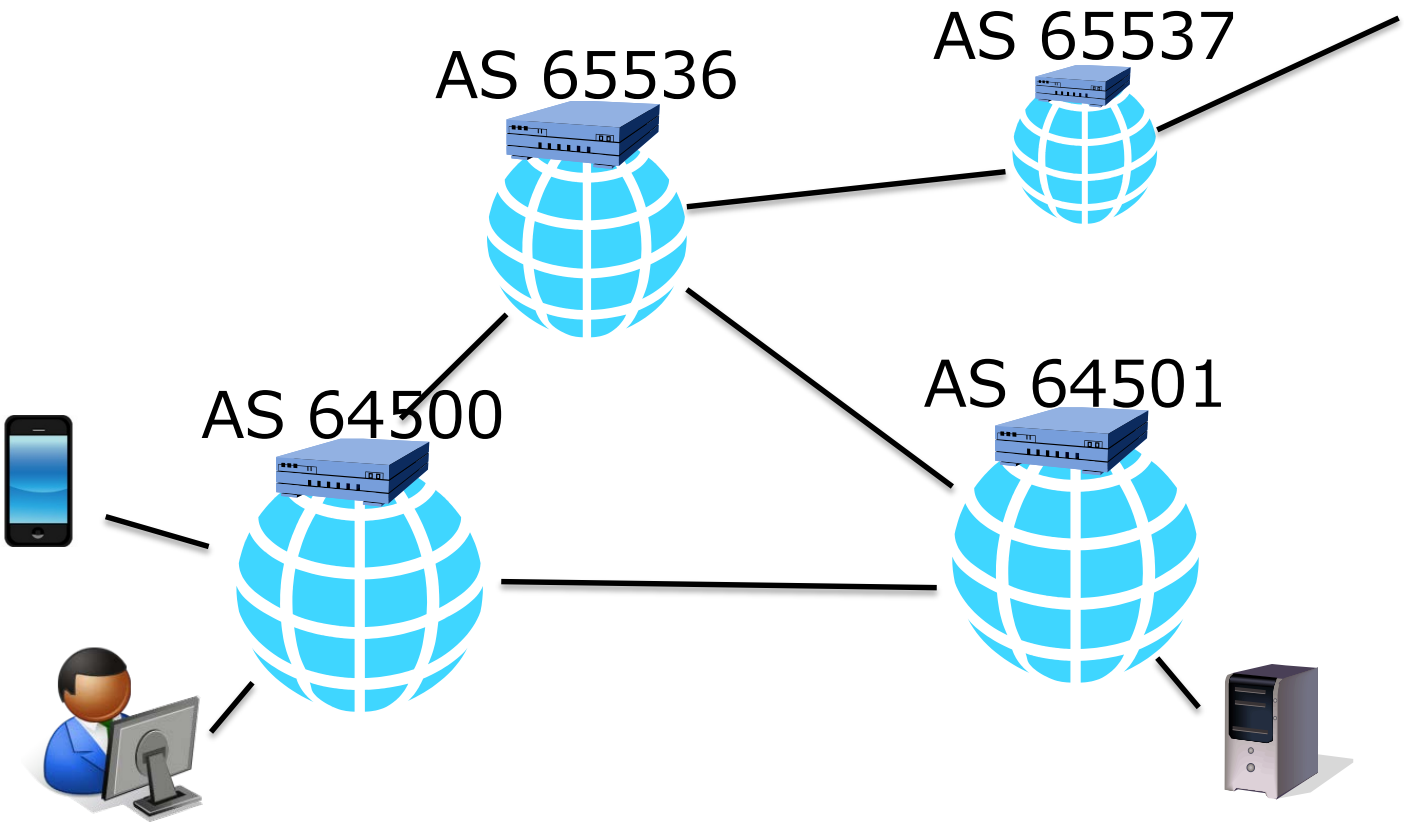
インターネットは、自律的なネットワークである「AS」のつながりによって構成されている。

AS番号



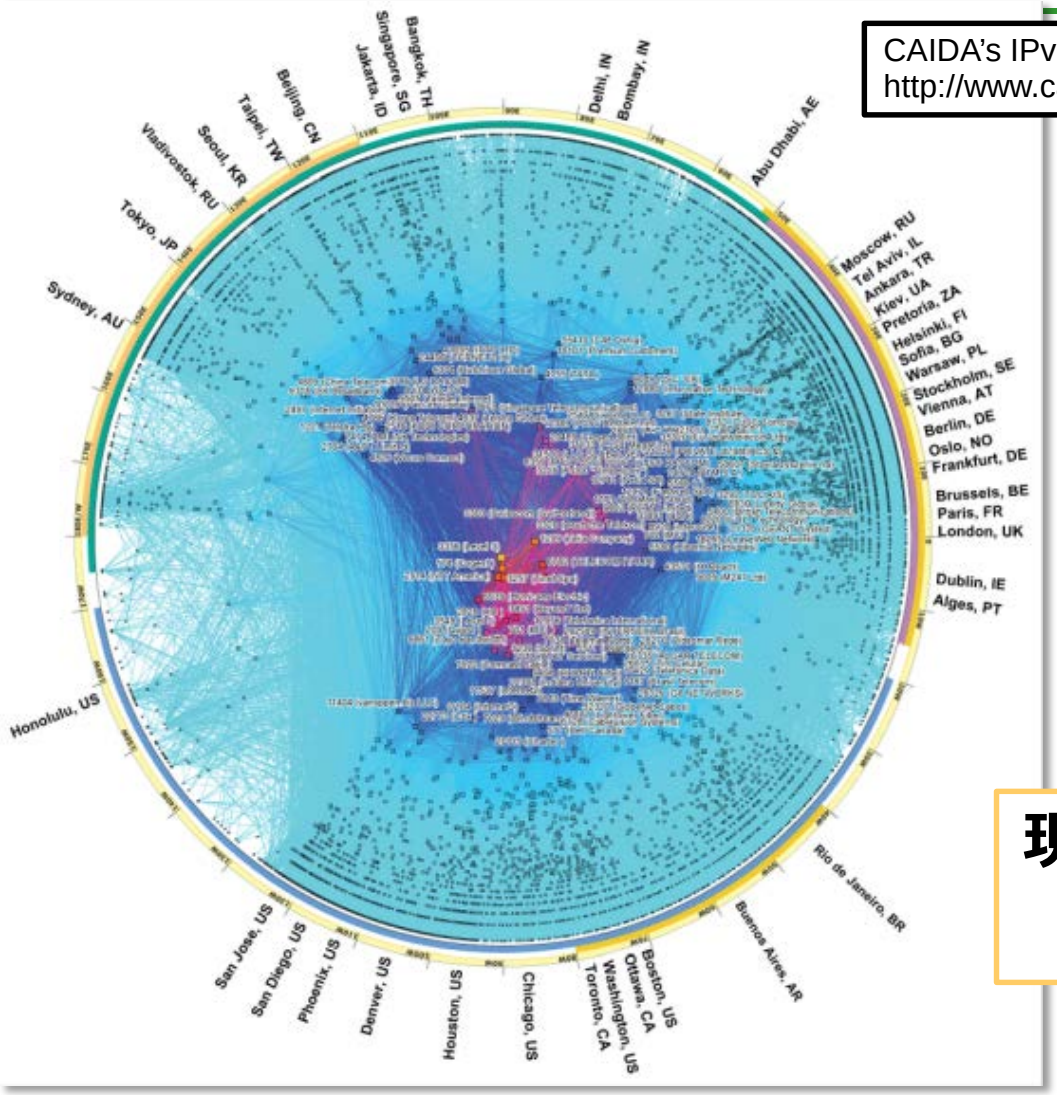
ASを識別する番号の「AS番号」は、JPNICのような「レジストリ」によって割り当てられる。

AS間ルーティングとBGP



ASで収容されているIPアドレスは「経路情報」と呼ばれ「BGP」を使って伝播される。

インターネットとASのつながり



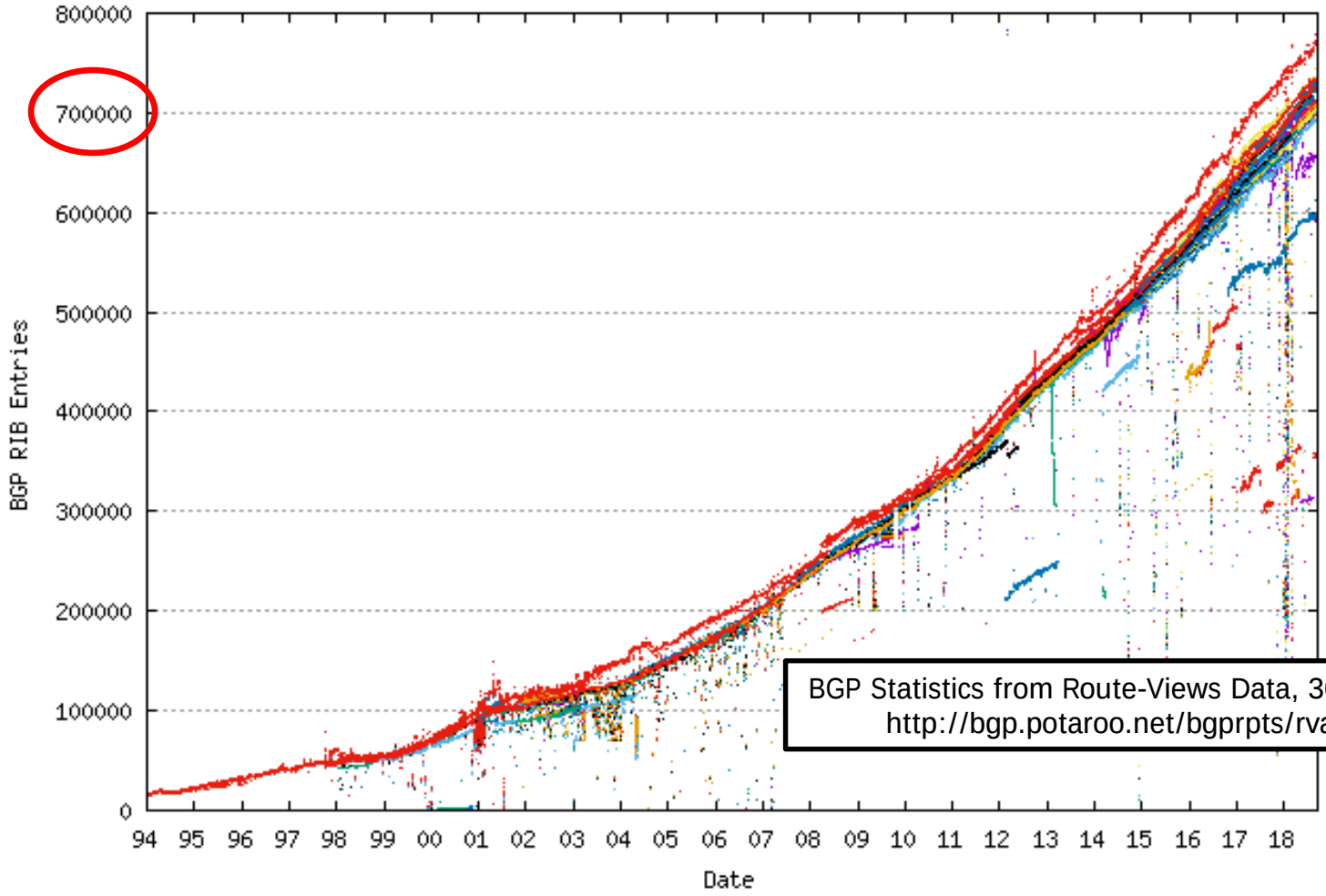
CAIDA's IPv6 AS Core AS-Level Internet Graph
http://www.caida.org/research/topology/as_core_network/

現在のAS番号割り当て数
96,495

The 32-bit AS Number Report
http://www.potaroo.net/tools/asn32/

BGPにおける経路情報の数

2014年前後に古いBGPルータで扱えない可能性があった50万を超え、継続して増加傾向にある。



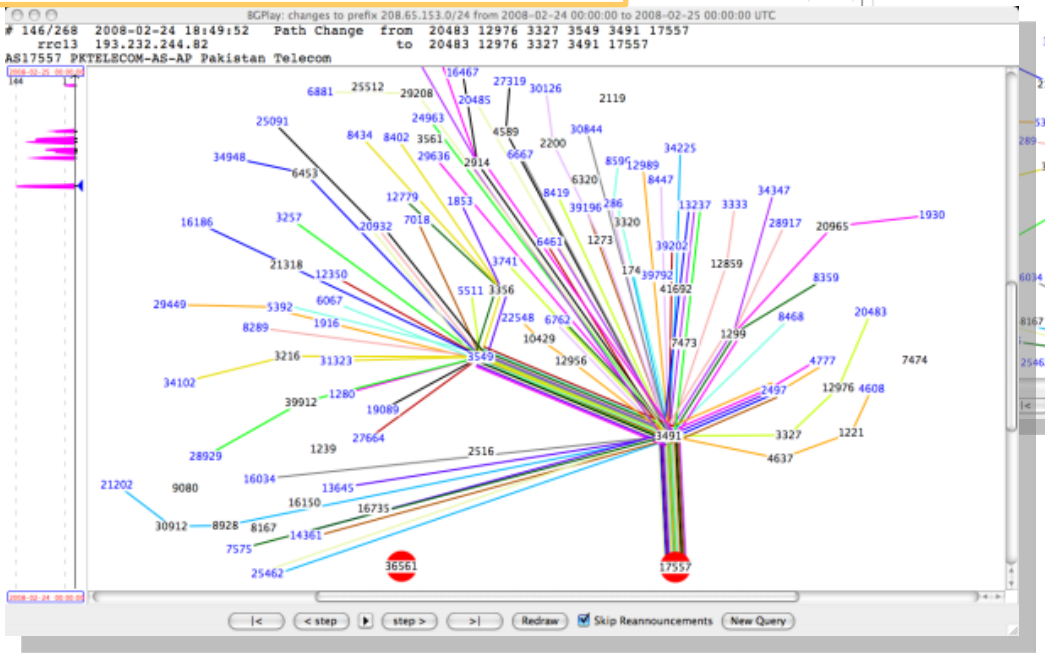
BGP Statistics from Route-Views Data, 30 Aug, 2017
http://bgp.potaroo.net/bgprpts/rva-index.html

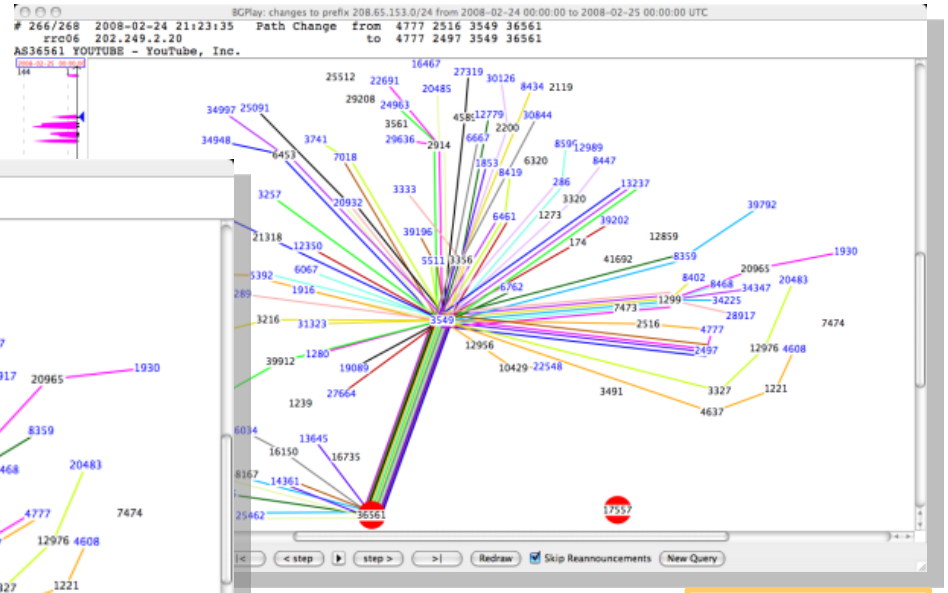
AS間ルーティングにおけるインシデント

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

2008年のYouTubeインシデント

インシデント発生時





平常時

YouTube Hijacking: A RIPE NCC RIS case study, 17 Mar 2008, RIPE NCC,
http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study

YouTubeの経路情報が別のASによって広告され、約2時間半の間、アクセスできなくなった。

MyEtherWallet.com

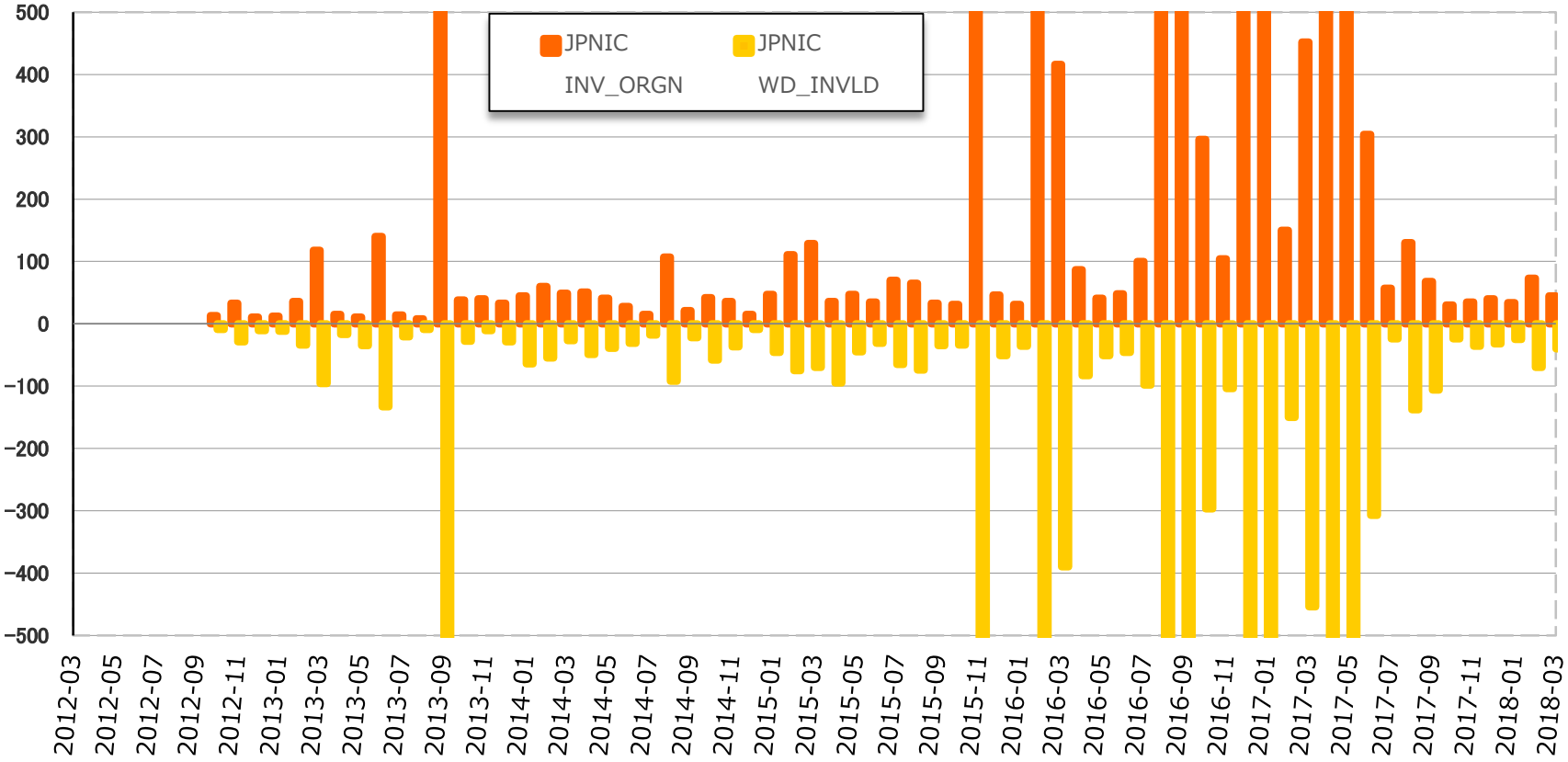
- 手法
  - AWS Route 53の経路(/23など)を/24で経路広告
  - MyEtherWallet.comの問い合わせに対して偽のAレコードを応答
  - サーバ証明書は自己署名証明書だった模様（本来EV SSL証明書"MyEtherWallet Inc"）
- 影響
  - 総額15万ドル（約1630万円）相当が不正送金される
    - サーバ証明書のエラーを無視して接続したユーザは他のウォレットに送金させられた

不正な経路広告によって偽のDNS応答を返し、偽のサーバにアクセスさせ不正送金したという報告

- MyEtherWallet、DNSサーバーにハッキング、15万ドル分のETH盗難か
  https://jp.cointelegraph.com/news/myetherwallet-warns-that-a-couple-of-its-dns-servers-have-been-hacked
- AWS DNS network hijack turns MyEtherWallet into ThievesEtherWallet - The Register, 2018/4/24
  https://www.theregister.co.uk/2018/04/24/myetherwallet_dns_hijack/

国内における観測

検出状況



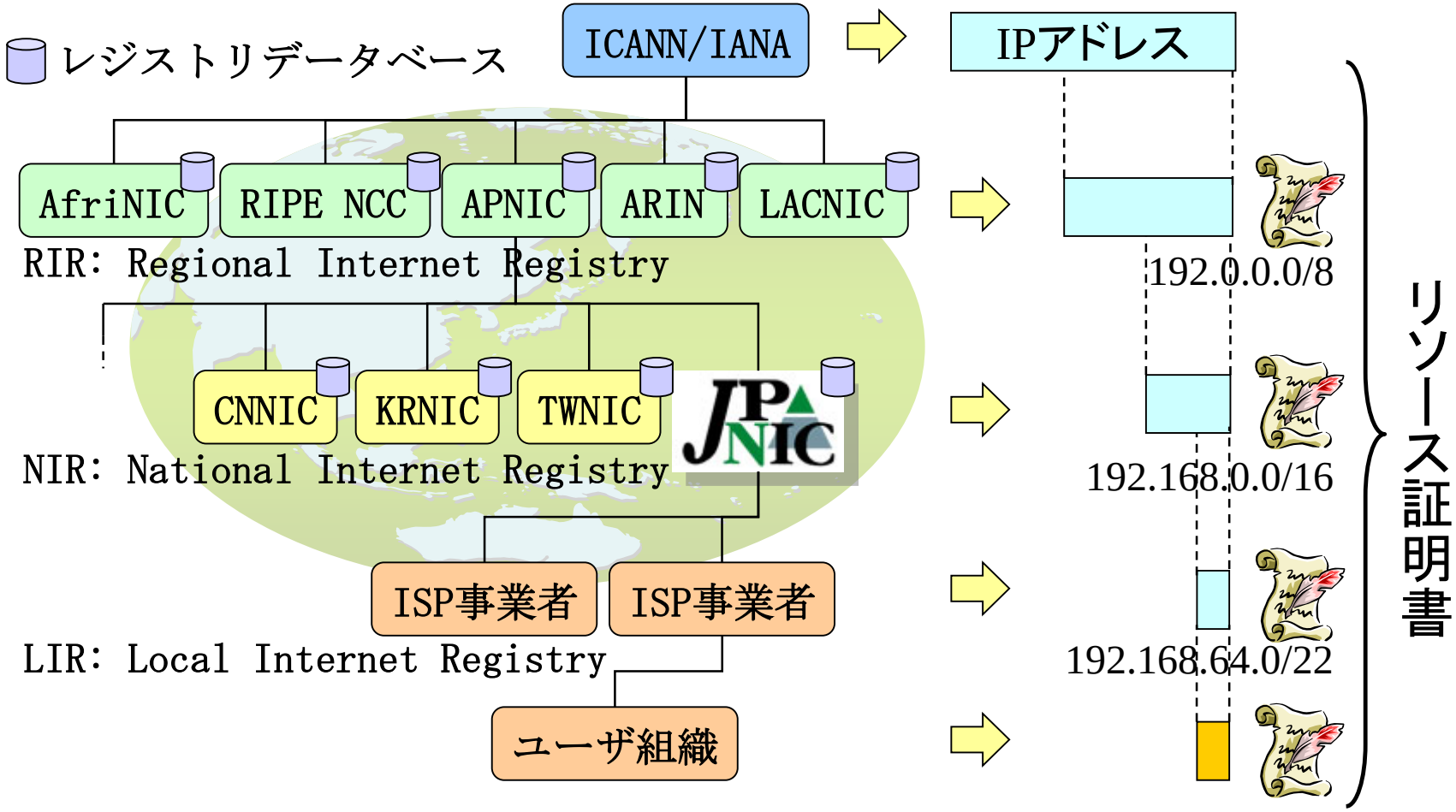
AS番号が本来とは異なる疑いのある経路情報が観測されている。 (JPIRRの登録情報との比較)

対策の考え方

- 経路情報における正しさ
  - IPアドレスの分配を軸に判断 ⇒ RPKI
- 経路の情報は膨大
  - スケーラビリティのある判別の仕組み
    ⇒ オブジェクトセキュリティ/署名技術
  - 運用者が人手で対応するのはほぼ不可能
    ⇒ 機械可読・ルーターで判別

RPKIとは

リソース証明書

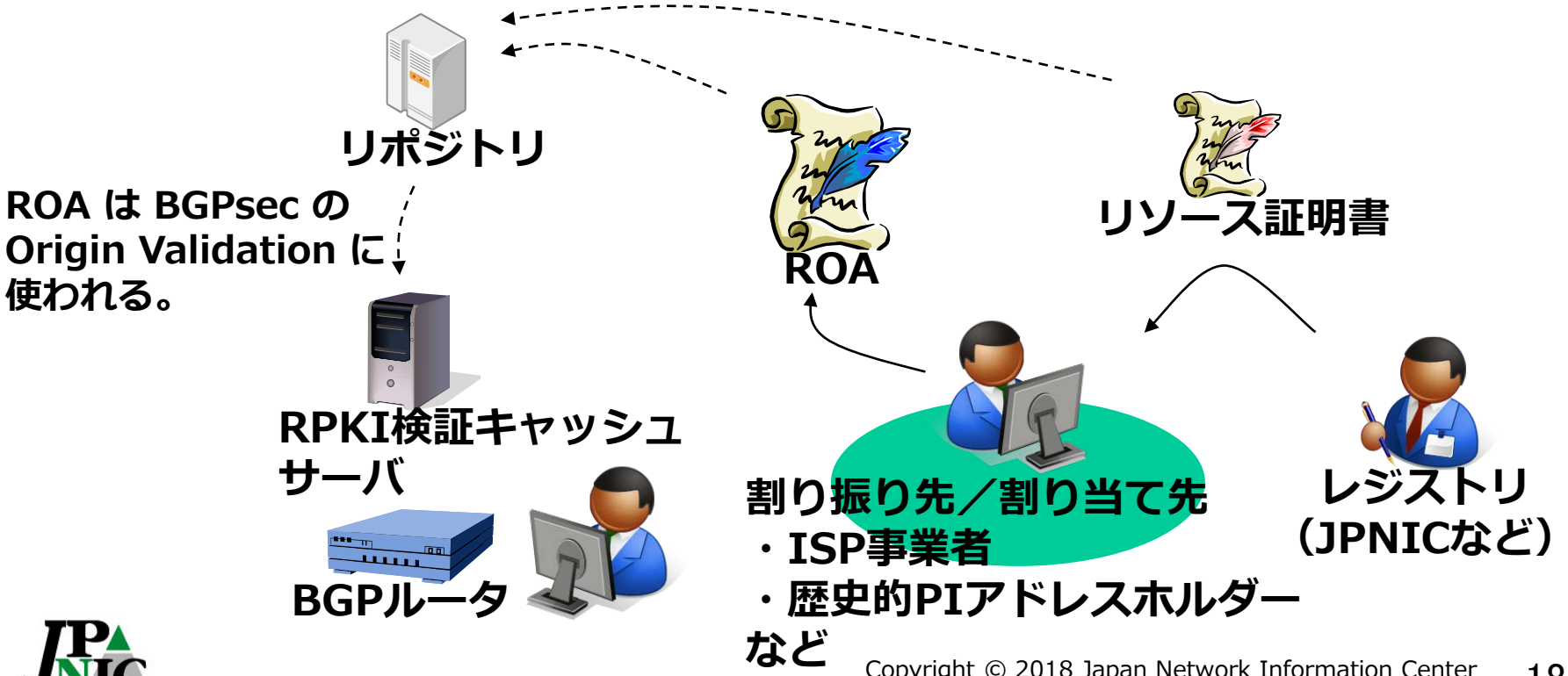


リソース証明書は、下に行くほど小さなprefixが記載される。

Copyright © 2018 Japan Network Information Center

リソース証明書とROA

- **Route Origination Authorization**
  - IPアドレスのホルダーによる署名付きデータで、割り当てられたIPアドレスの経路広告を特定のASから経路広告することを認可したことを示す。



Copyright © 2018 Japan Network Information Center

```
# telnet localhost bgpd
Escape character is '^]'.

Hello, this is QuaggaSrx (version 0.99.16-0.3.0.0).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

User Access Verification
Password:
bgpd> en
bgpd# sh ip bgp

BGP table version is 0, local router ID is 192.41.192.249
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, R Removed

Validation:    v - valid, n - notfound, i - invalid, ? - undefined
SRx Status:    I - route ignored, D - SRx evaluation deactivated
SRxVal Format: validation result (origin validation, path validation)
Origin codes: i - IGP, e - EGP, ? - incomplete

   Ident    SRxVal SRxLP Status Network          Next Hop            Metric  LocPrf Weight Path
*> DE8368 1B v(v,-) + 200,       202.12.30.0      192.41.192.226                200s      0 65001 2515 i
*> FBF4BE57 n(n,-) + 100,       202.12.31.0      192.41.192.226                100s      0 65001 2515

bgpd#
```

Origin Validation - IPアドレスを使っている(経路広告元)ASが正しいかどうかを確認する仕組み

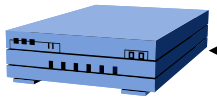
Copyright © 2018 Japan Network Information Center

オリジン検証の内容(1)

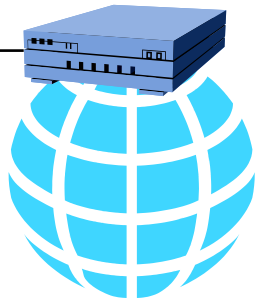
(1)AS2515が勝手にIPアドレスを使っていないかな？

202.12.30.0 AS2515
202.12.31.0 AS2515

AS65001



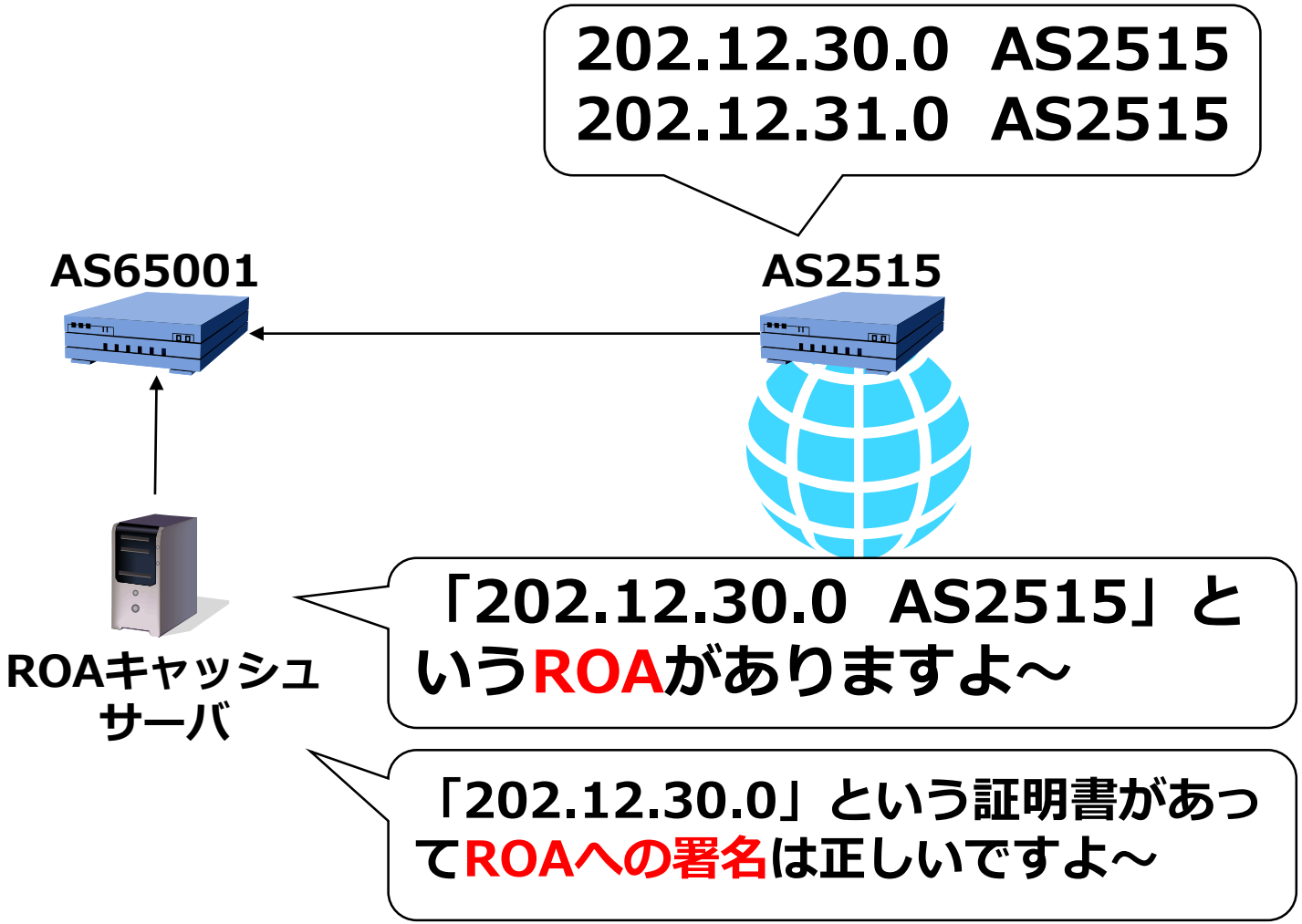
AS2515



(2)そもそも2つのprefixはレジストリから割り振られたものかな？

Copyright © 2018 Japan Network Information Center

オリジン検証の内容(2)



Copyright © 2018 Japan Network Information Center

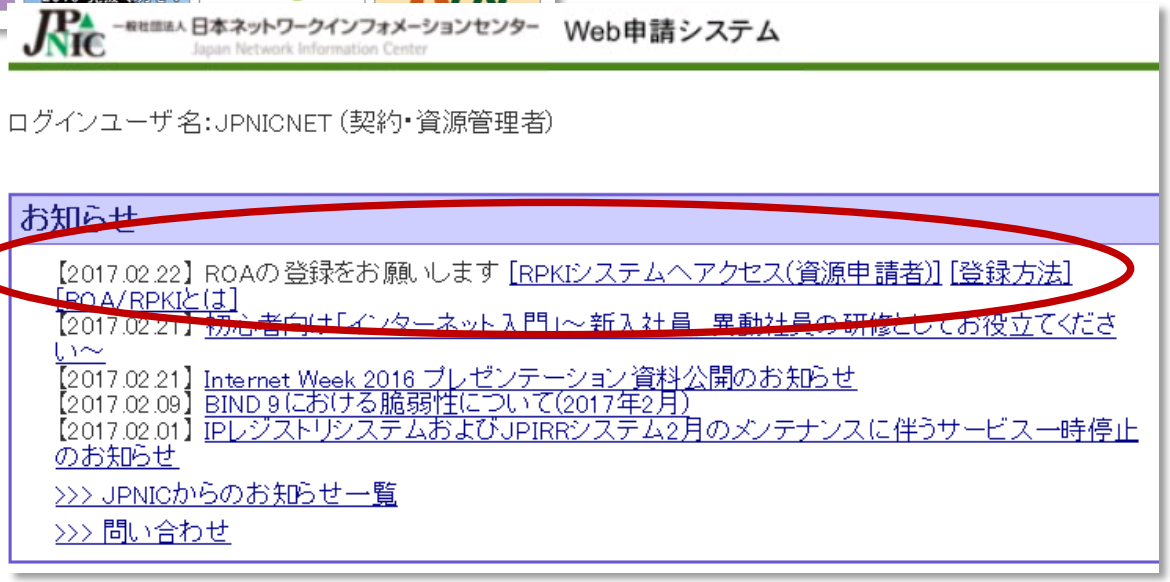
Origin Validationの仕組み

- **RPKIキャッシュ**
  - リソース証明書の署名検証を通じて、IPアドレスが正式に割り当てられたものであることを確認
  - ROAの署名検証を通じて、経路広告元のAS番号が正式なIPアドレスの割り当て先によって指定されたものであることを確認
- **BGPルータ**
  - BGP Updateメッセージとして伝播してきたIPアドレスprefixと経路広告元のAS番号を確認

BGPルータにおいて、BGP経路情報の中の不適切なIPアドレスや本来とは異なる経路広告元が検出できる。

Copyright © 2018 Japan Network Information Center

ROAの登録と管理の方法 (ガイド)



Copyright © 2018 Japan Network Information Center

ルーティングにおける認証

- **オブジェクトセキュリティ**
  - インターネットにおける経路情報のセキュリティのため、認証対象の規模拡張性が重要。
- **認証の意味**
  - ROA - 正しいIPアドレスのホルダーがASに対してそのIPアドレスを経路広告する事を認可(予め登録された情報の正しさとの照合)

Copyright © 2018 Japan Network Information Center

RPKIのIETFにおける動向
sidrops WG

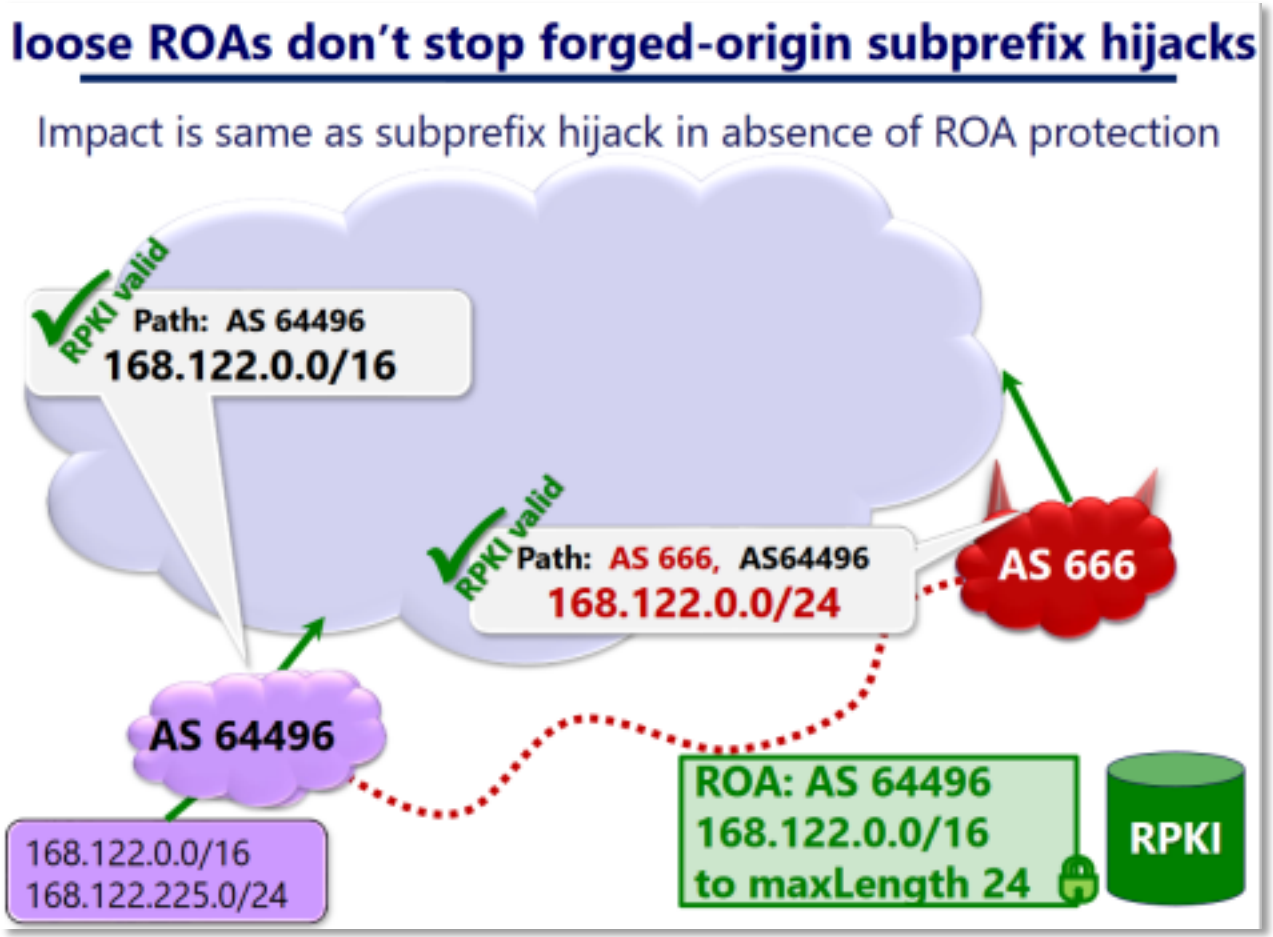
Copyright © 2018 Japan Network Information Center

sidrops - アジェンダ

- **7/16(月) 13:30-15:17 60名程**
- **アジェンダ**
  - The Use of Maxlength in the RPKI, Sharon Goldberg
  - Origin Validation Signaling, Randy Bush
  - A Profile for Autonomous System Provider Authorization, Alexander Azimov
  - Modified Validation deployment planning, George Michaelson
  - RPKI signed object for TAL, Tim Bruijnzeels

Copyright © 2018 Japan Network Information Center

The Use of Maxlength in the RPKI(1/2)



Use of MaxLength in the RPKIより
https://datatracker.ietf.org/meeting/102/materials/slides-102-sidrops-draft-ieft-sidrops-rpkimaxlen-00

Copyright © 2018 Japan Network Information Center

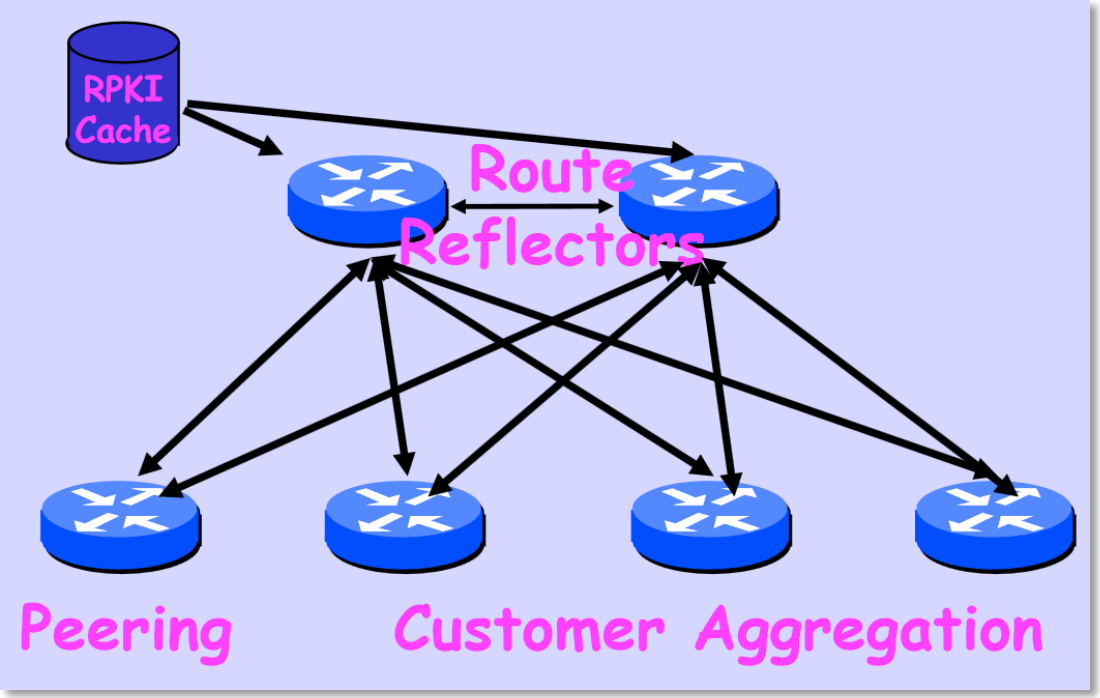
The Use of Maxlength in the RPKI(2/2)

- **このI-Dにおける提案**
  - 最大プレフィックス長の記載をやめて、経路広告するプレフィックスのみを入れる。
- **議論**
  - /32や/128のようなホスト経路はどうすればいいのか。→ それはこの問題を避ける対象ではない。(別の人の回答) MaxLenだけでマッチしたものは受け付けたくない。
  - ROAの最大プレフィックス長そのものを名sくしたいわけでもない。

Copyright © 2018 Japan Network Information Center

Origin Validation Signaling(1/2)

- "Evaluator"がBGP拡張コミュニティを使ってROAを使ったオリジン検証のInvalidの結果を返す。



Origin Validation Signalingより
https://datatracker.ietf.org/meeting/102/materials/slides-102-sidrops-draft-ymbk-sidrops-ov-signal-00

Copyright © 2018 Japan Network Information Center

Origin Validation Signaling(2/2)

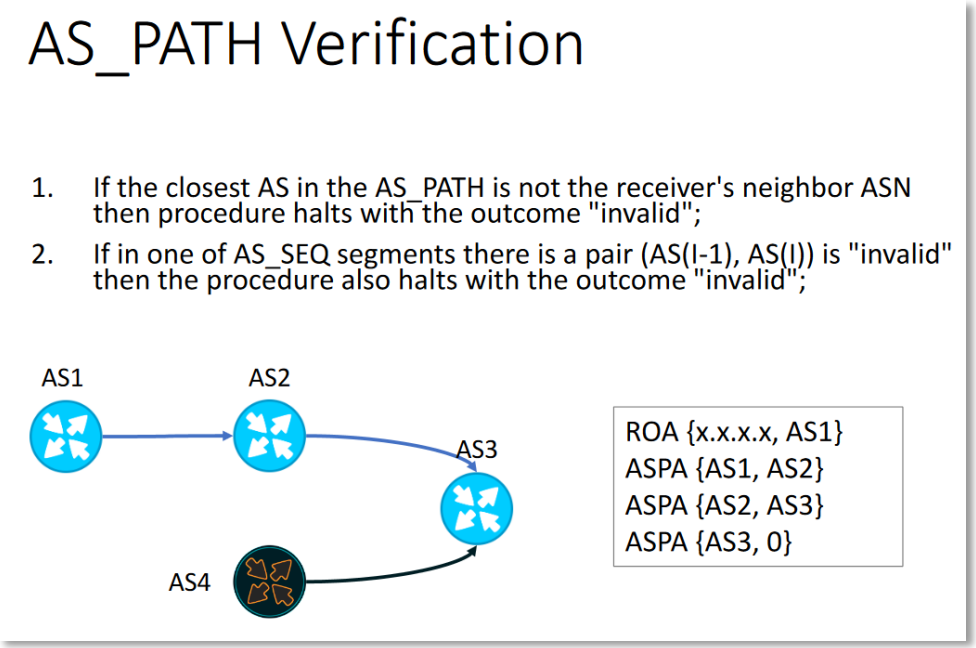
- **議論**
  - デバイスによってはルーティングトラストバウンダリーの中で行う必要はないかも知れない。route reflector は良いユースケース。(randy)
  - (経路は)Inboundかoutboundか。Inboundならいいが… → inboundの話。

Route reflectorは
IBGP?で接続？

Copyright © 2018 Japan Network Information Center

A Profile for Autonomous System Provider Authorization

- **このドラフトにおける提案**
  - 「BGPsecに対応していない」と言うことによってBGPsecのパス検証を回避する不正なルータへの対策＝意図的なASパスの操作への対策



AS_PATH Verifcation Using ASPAより
https://datatracker.ietf.org/meeting/102/materials/slides-102-sidrops-as-path-verifcation-using-aspa-00

Copyright © 2018 Japan Network Information Center

Modified Validation deployment planning

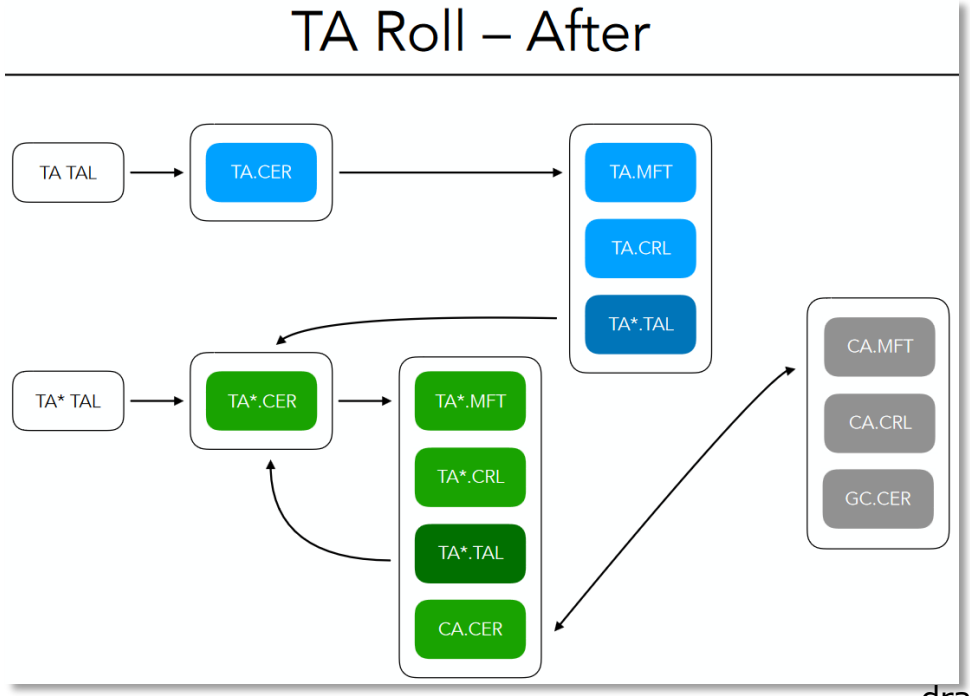
- **内容**
  - リソース証明書に記載されたプレフィックスのセットのうち、一部を内包していれば有効とみなす形式（OIDで指定）に移行することについての考察
    - 2018年7月を「フラッグディ」として移行する事を検討中
    - コードなし。利用者(RP)・中間認証局であるNIR共に対応していない。

まずはNIRやRPKI Tools開発者と相談しては？

Copyright © 2018 Japan Network Information Center

RPKI signed object for TAL

- 平文のTAL(Trust Anchor Locator)を署名付きのオブジェクトで鍵の世代交代ができるように改良する提案



draft-ietf-sidrops-signed-talより
https://datatracker.ietf.org/meeting/102/materials/slides-102-sidrops-draft-ietf-sidrops-signed-tal-00

Copyright © 2018 Japan Network Information Center

おわり