# S3
# 経路制御とセキュリティの最新動向

木村泰司

2018年11月27日(火)

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

- **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)
- **業務分野**
  - 電子証明書 / RPKI / DNSSEC (DPS/鍵管理/HSM他)
  - 国際動向 IETF

# 経路制御とセキュリティの最新動向

- 2018年に起きたインシデント
- 技術利用の動向/国際動向
- RPKI/オリジン検証のリスク要素と対応策

# 2018年に起きたインシデント

- DNSサーバのprefixに対する不正経路
  - 重要なDNSサーバは、ROAやIRRの登録を通じて不正経路をするなど対策も
- 経路広告を止める”インターネット・シャットダウン”も発生

# 2018年4月24日 - 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**

- BGP Hijack of Amazon DNS to Steal Crypto Currency
  https://dyn.com/blog/bgp-hijack-of-amazon-dns-to-steal-crypto-currency/
- 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/

# 2018年7月6日 - 決済サービス

- **手法**
  - 決済サービスのDNSサーバのアドレスが含まれるprefixが、インドネシアとマレーシアにあるASによって経路広告される
    - Datawire社のトランザクションシステムらしきホスト名に対して本来と異なるAレコードが返される。
    - Vantiv社・Mercury Payment Systems社のネームサーバが経路広告されたprefixに含まれていた。
- **影響**
  - 不正送金されたかどうかは不明

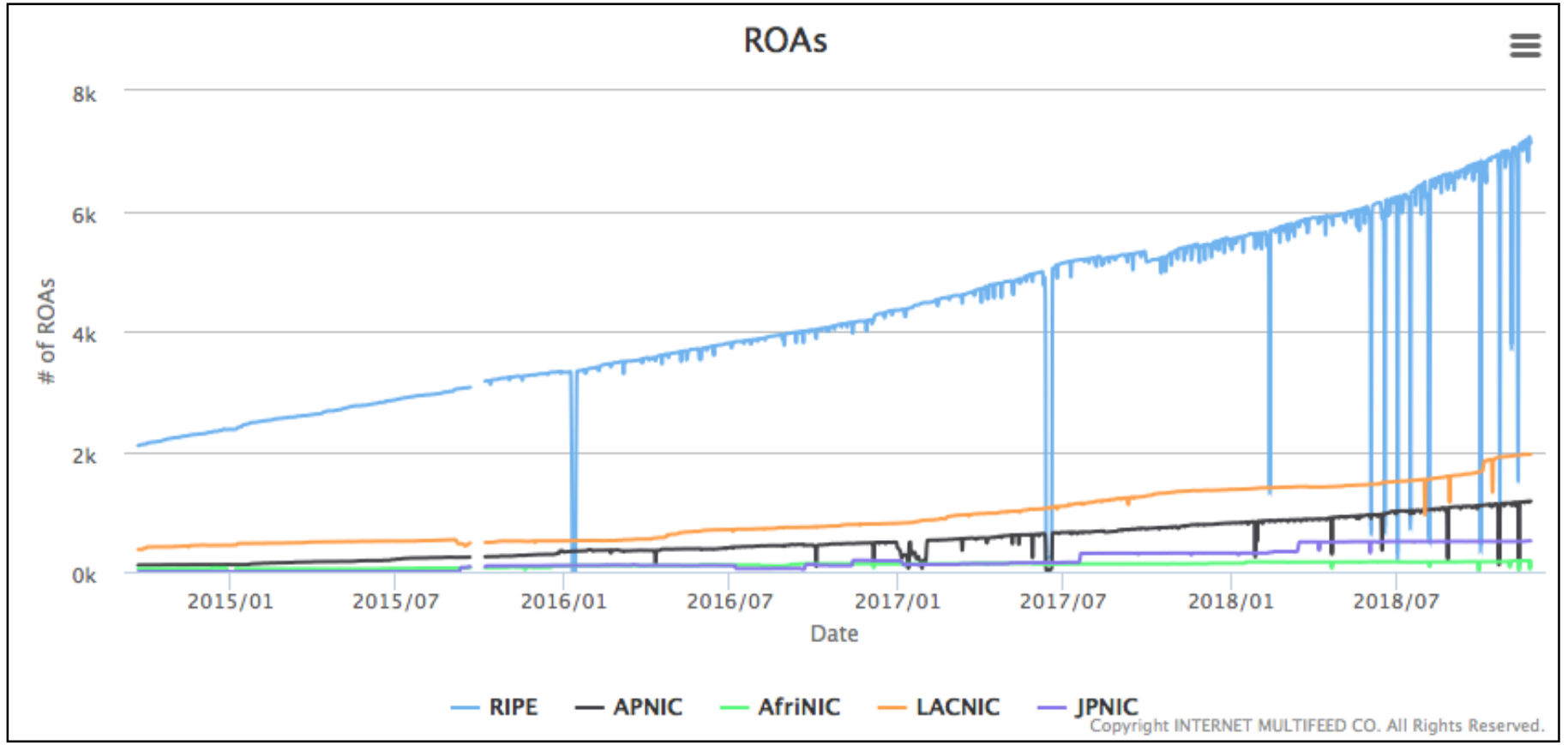
**不正な経路広告によって偽のDNS応答を返し、偽のサーバにアクセスさせる手法**

- BGP/DNS Hijacks Target Payment Systems
  https://dyn.com/blog/bgp-dns-hijacks-target-payment-systems/

# RPKI/ROA普及の動向

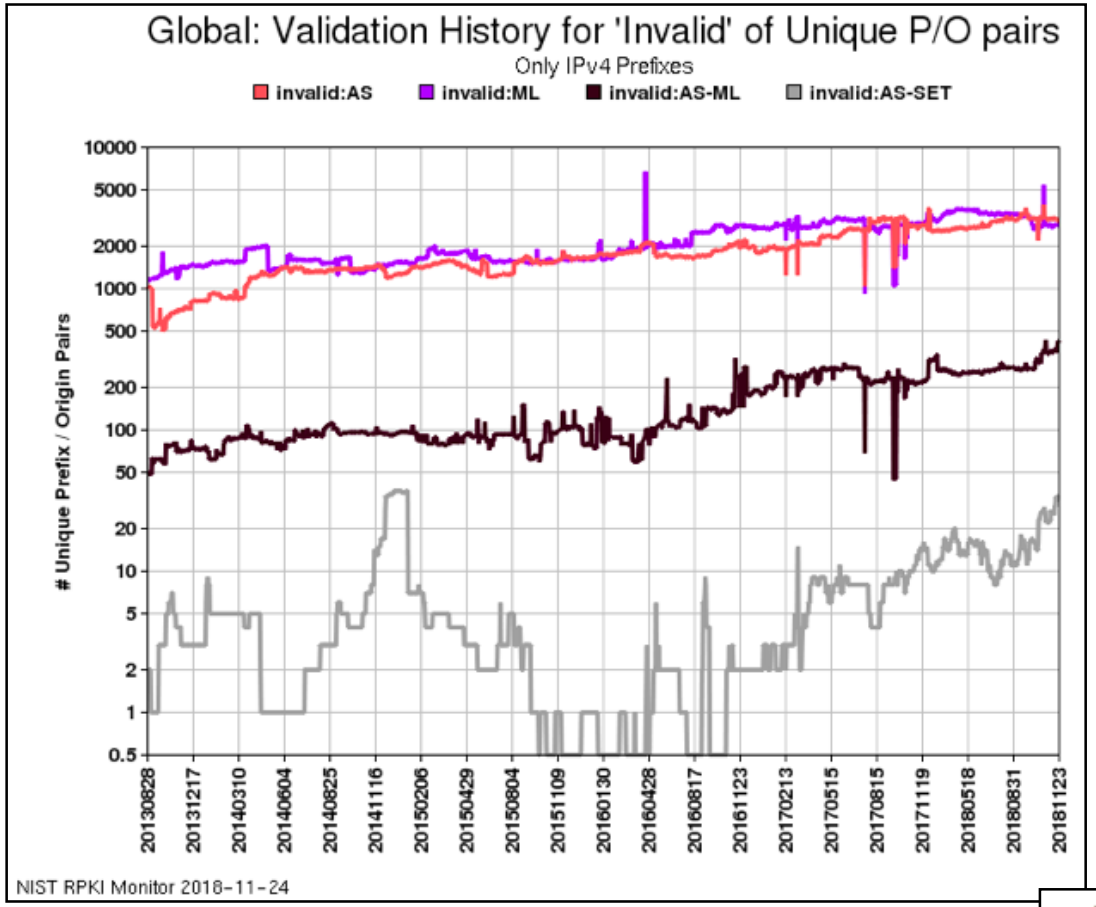
# RIRごとのROAの数

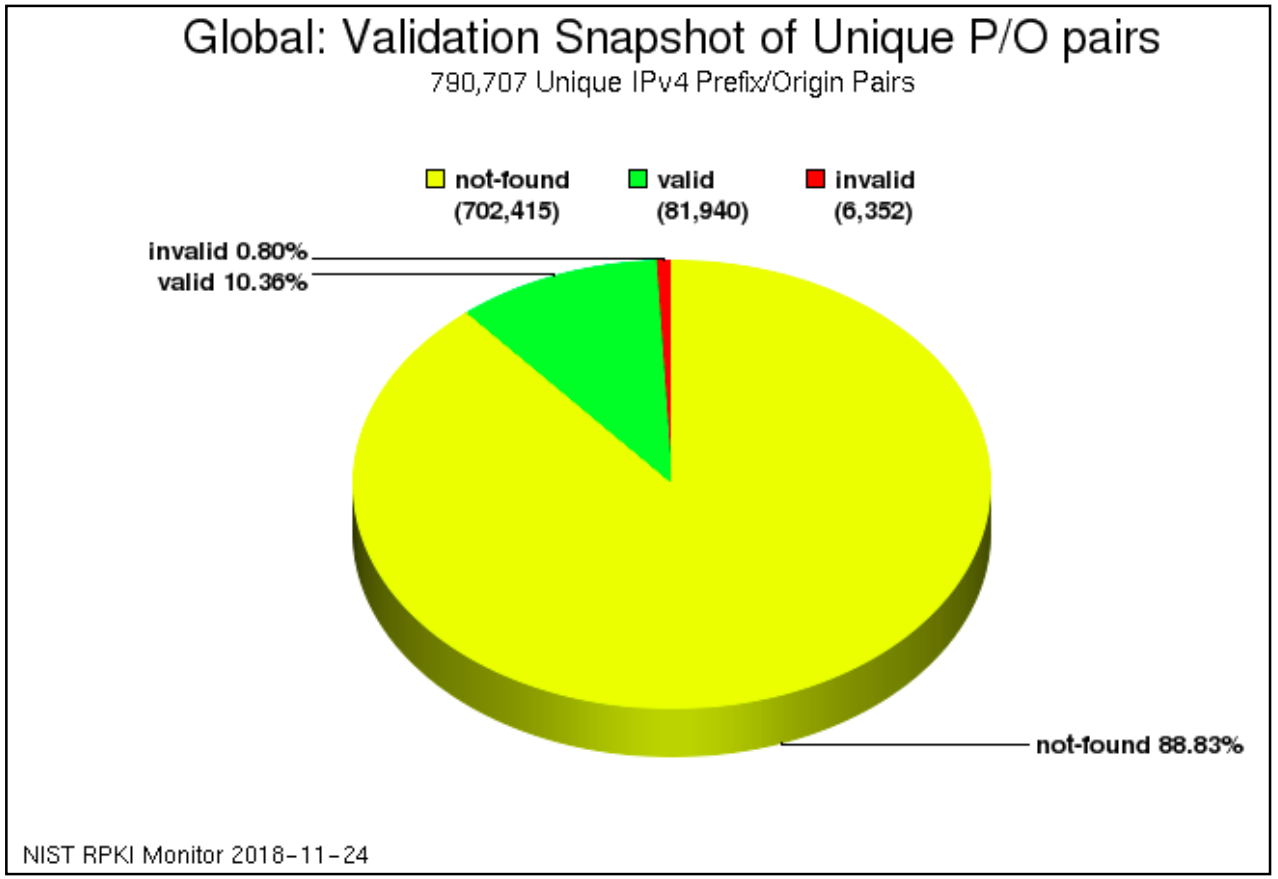
ROA数, MF RPKI Project, 2018/11/25
http://www.mfeed.co.jp/rpki/roa_cache/statistics.html#roas




**RIPE地域のROA数がダントツで引き続き純増中。(RIPE NCCの申請システムにログインすると登録を促すダイアログボックスが表示される模様)**

# NIST RPKI Monitorより




- RPKI Deployment Monitor
  https://rpki-monitor.antd.nist.gov

- **Invalid:AS** Covering ROA Prefix, maxLength Satisfied, and AS Mismatch.
- **Invalid:ML** Covering ROA Prefix, maxLength Exceeded, and AS Match.
- **Invalid:ML-AS** Covering ROA Prefix, maxLength Exceeded, and AS Mismatch.
- **Invalid:AS-SET** The origin AS could not be determined from the BGP update used to announce the prefix (i.e., because it contains an AS-SET), and a ROA covering the prefix exists.

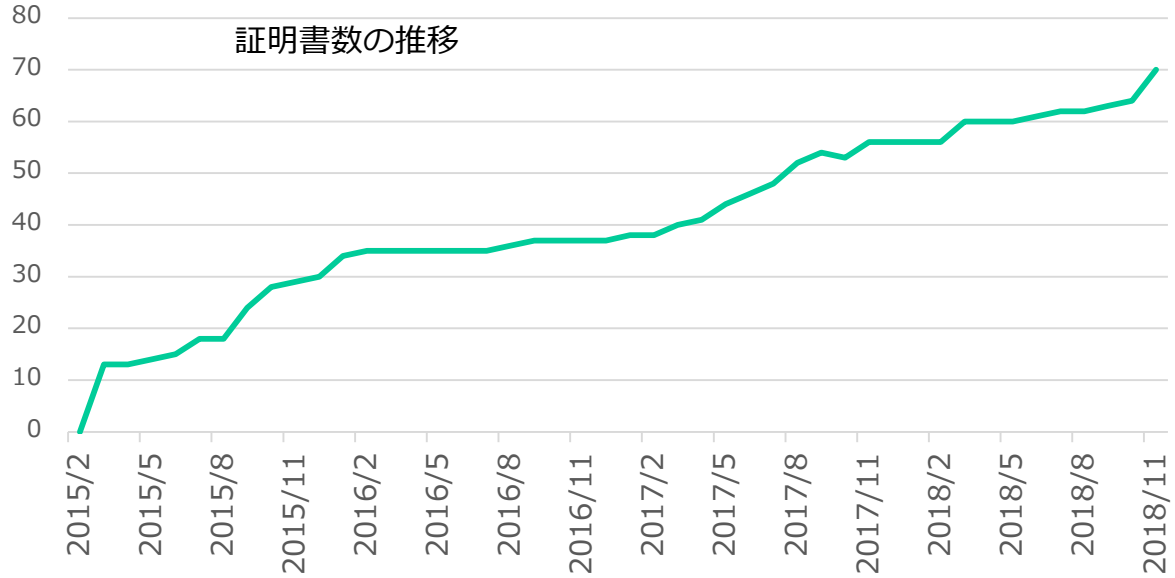
# アジア太平洋地域の状況

- **APNIC**
  - 五つのトラストアンカーを一つに移行（2018年2月）
  - 発行先のリソース証明書に発行元のリソース証明書にはないリソースが入っていても、重なっている範囲については有効とみなす「Validation Reconsidered」方式に切り替えるフラッグデーを模索中。リソース証明書中のOIDが変更。
- **CNNIC**
  - RPKIシステムを提供開始（2017年6月）
  - APNICと連携した後、運用再開（2018年11月）
- **TWNIC**
  - RPKIシステムを提供開始（2018年10月）
- **VNNIC**
  - RPKIについて積極的にヒアリング

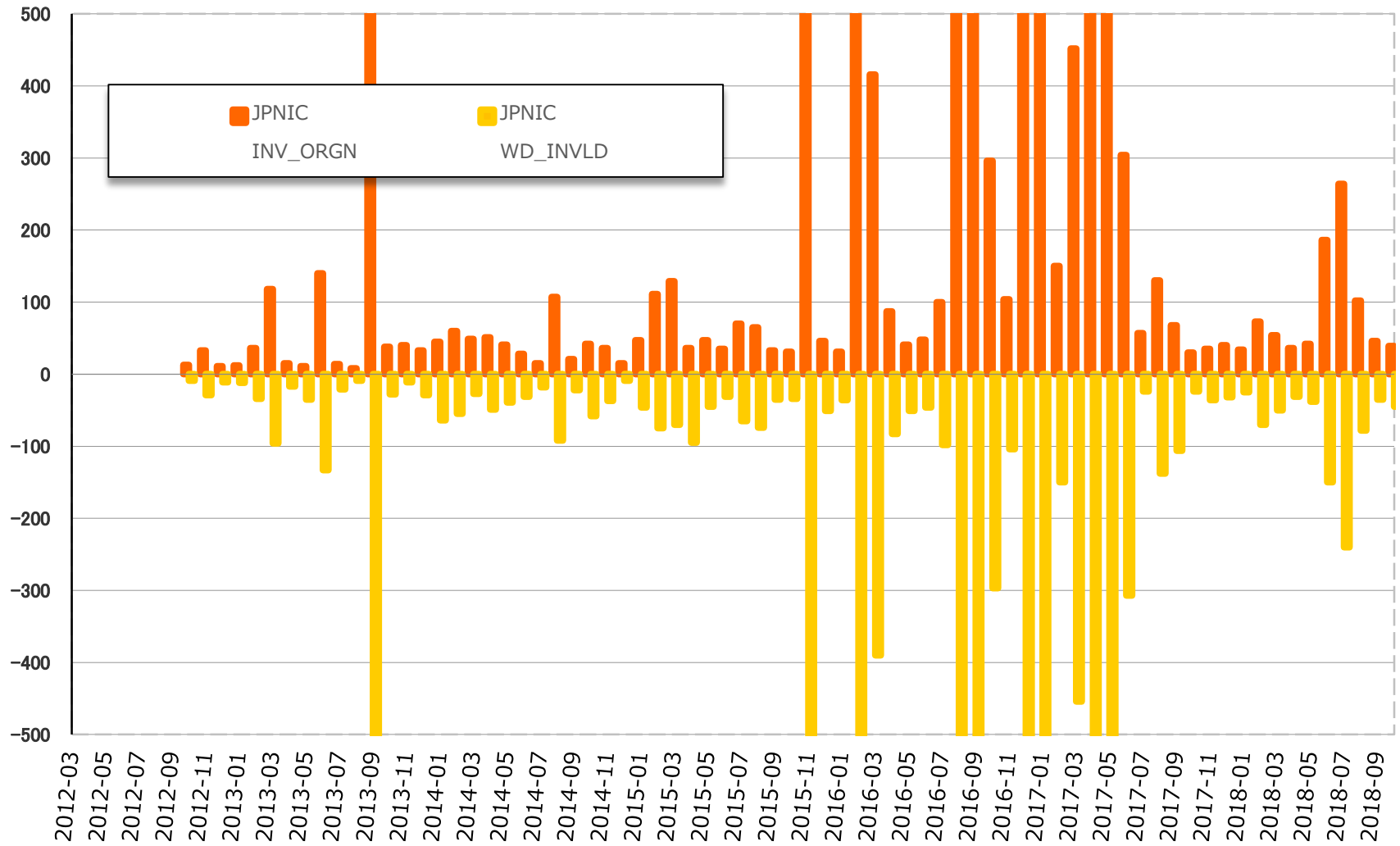
**CNNICとTWNICがRPKIシステムの提供を開始。CNでは13LIRがROAを作成。TWでは6LIRがROAを作成。**

# JPNICのRPKI試験提供（2015年3月～） (更新)

- **アドレスホルダ毎に発行される証明書数**
  - 70
- **発行されているROA**
  - 256
- **割り振られているIPアドレスに対してROAがカバーする割合**
  - 3.5% IPv4
  - 38.1% IPv6



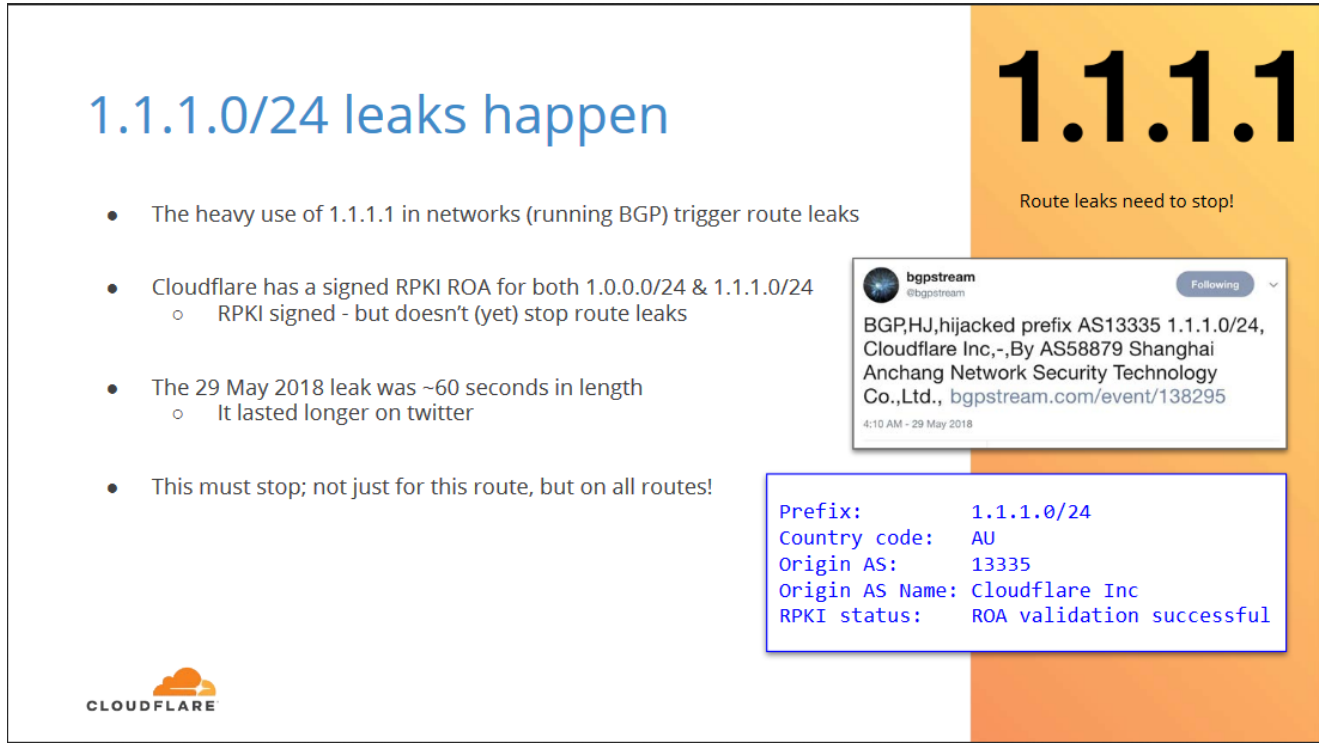
# JPNIC経路奉行 検知の状況



# CloudFlare (1/2)

- **BGP経路を守るために1.1.1.0/24と1.0.0.0/24のROAを発行**
  - ミスオリジネーションは発生している
  - "ルートリークを止めるには至っていない。"

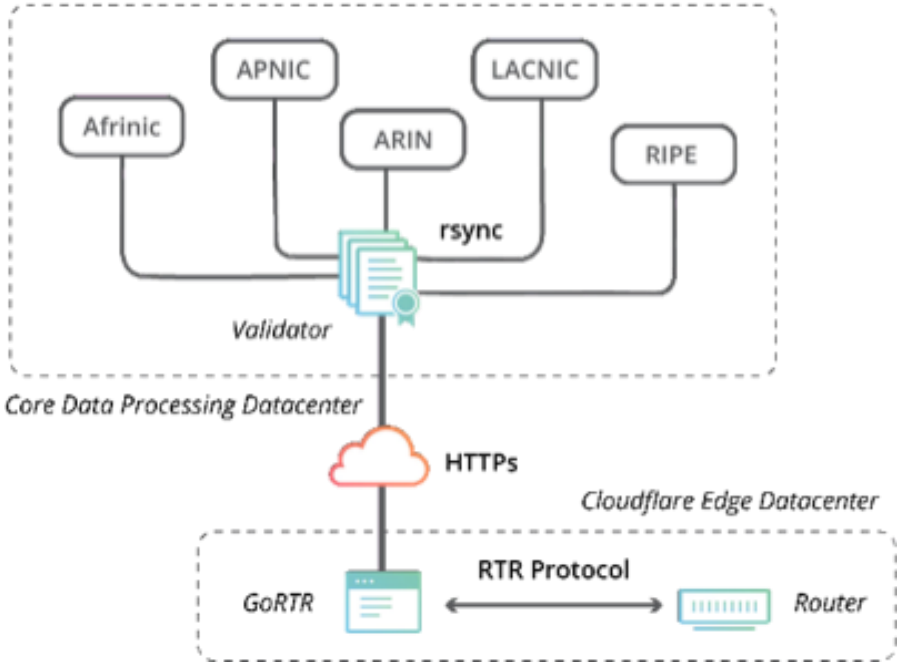
**経路情報が正常かどうかのチェックには使えているが、多くのASでROVを行ってInvalidな経路情報を除かない限り防止には至らないと考えられる。**




DNS resolver 1.1.1.1
https://conference.apnic.net/46/assets/files/APNC402/DNS-resolver-1.1.1.1-from-Cloudflare.pdf

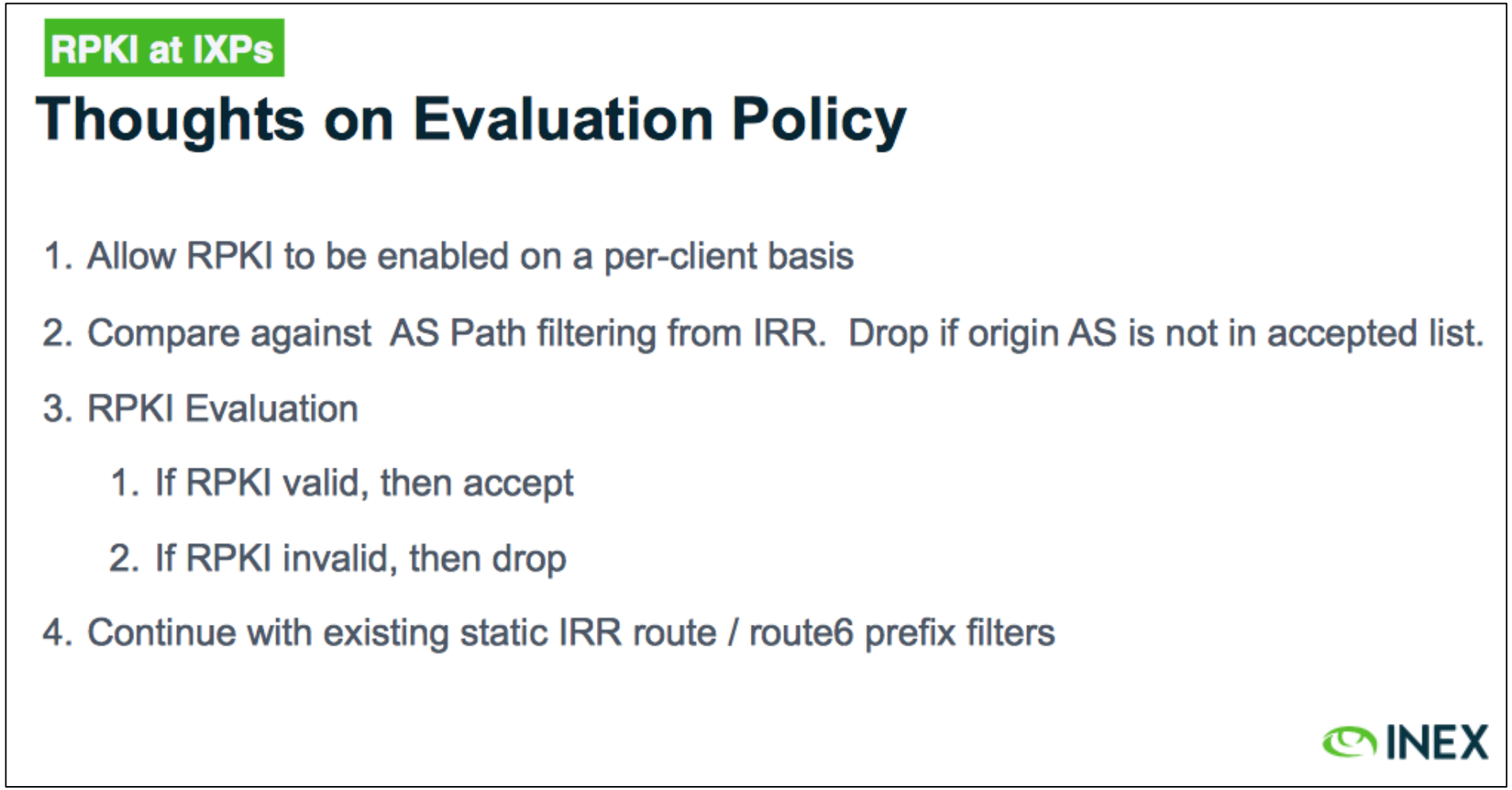
# CloudFlare (2/2)

- **5つのRIRの地域で合計150以上のPOPを運用中**
- **スケーラブルなローカルROAキャッシュ**
  - すべてのPOPでROAキャッシュを運用
    - JSON形式の検証結果をCDNで配布
      https://rpki.cloudflare.com/rpki.json
  - ROAキャッシュをauthorityと位置づけ、開発したカスタムRTRサーバでルータに伝達
    - GoRTR
      https://github.com/cloudflare/gortr




RPKI: our approach for deploying at scale
https://ripe77.ripe.net/wp-content/uploads/presentations/149-RPKI-deployment-at-scale-RIPE.pdf

# IXPのルートサーバにおける利用




- RPKI on IXP Route Servers
https://ripe77.ripe.net/wp-content/uploads/presentations/81-inex-ripe-amsterdam-connect-2018-10-17.pdf

# 最新技術動向

# IETF103より

- **GROW WG - Route leak対策技術の提案**
  - Solution for Route Leaks Using BGP Communities https://tools.ietf.org/html/draft-ietf-idr-route-leak-detection-mitigation-10
    - BGPコミュニティに特定の値を入れ検出する
- **SIDROPS WG**
  - **Drop Invalid if Still Routable(DISR)** = ROAのValidな、もしくはROAがNot Foundのless specific経路があるときに、more specific経路をドロップする提案
  - BGPSECのパス検証に代わる**Autonomous System Provider Authorization(ASPA)**の提案。

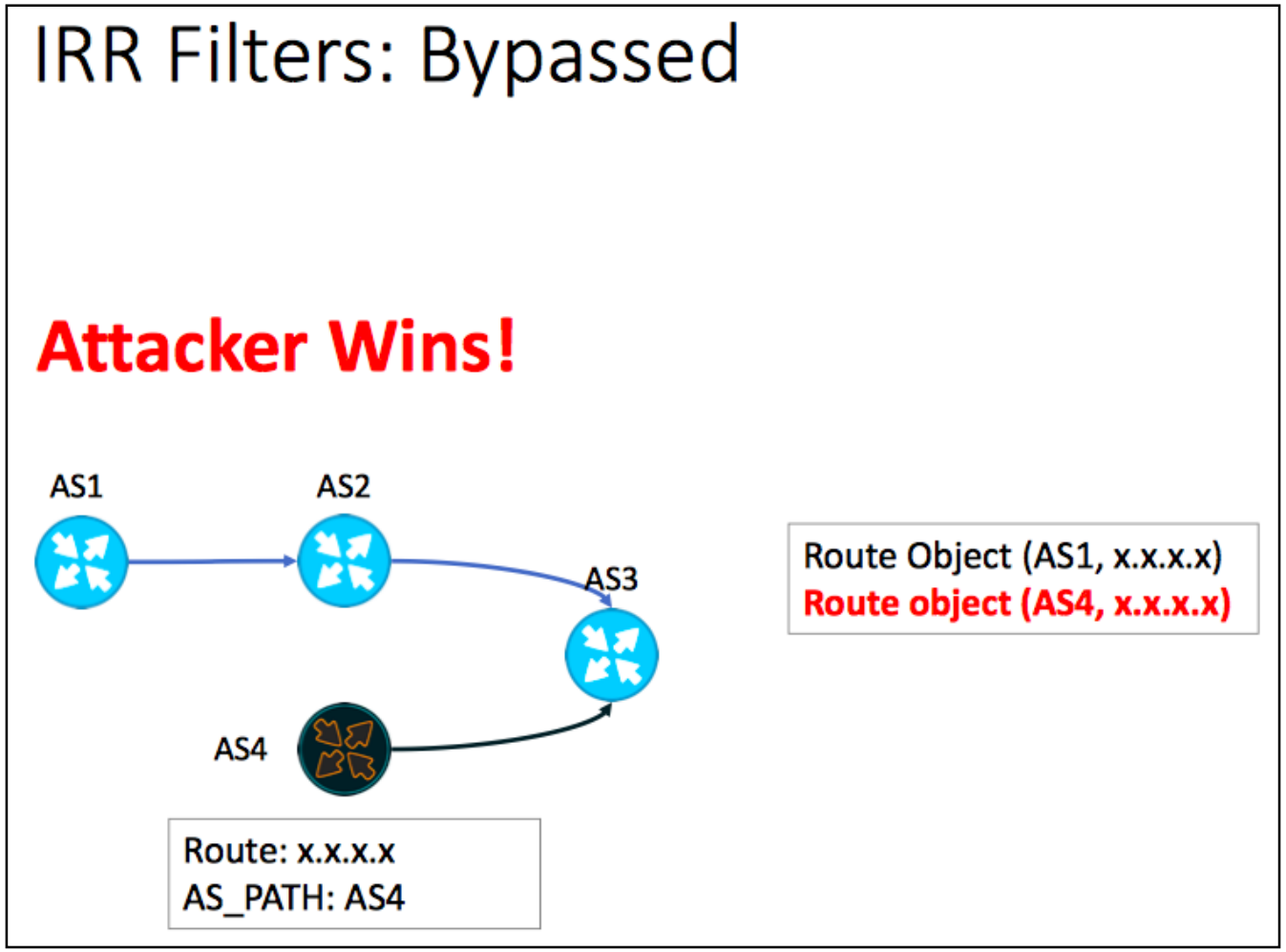
**いずれも提案の段階だが会場の反応からして、策定が進む可能性がある。**

# RIPEミーティングにおける不正経路の議論

- **現在の技術は故意の不正経路への対策になるのか**
  - IRRを使った経路フィルター、ROAを使ったオリジン検証、BGPSECのパス検証は、不正な経路を検知し対処できるようにするものだが、他の手段と組み合わせた*故意の*不正経路には有効ではないケースが考えられる。
  - これらを踏まえて、新たなASパスの検証を行う方式の提案(ASPA)につながっている。

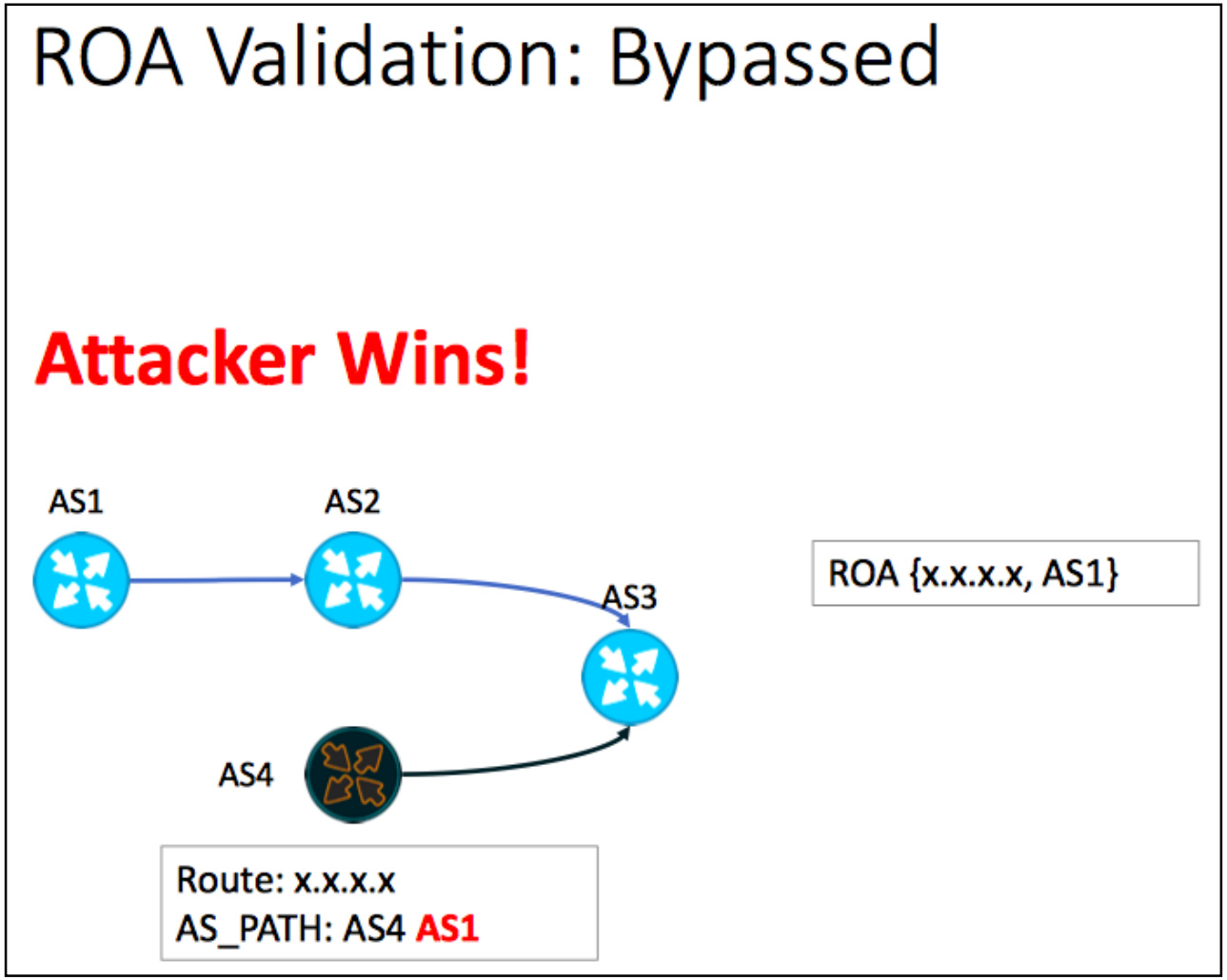
  - BGP Route Security Cycling to the Future!, Alexander Azimov Qrator Labs

# IRRを使った経路フィルターの回避



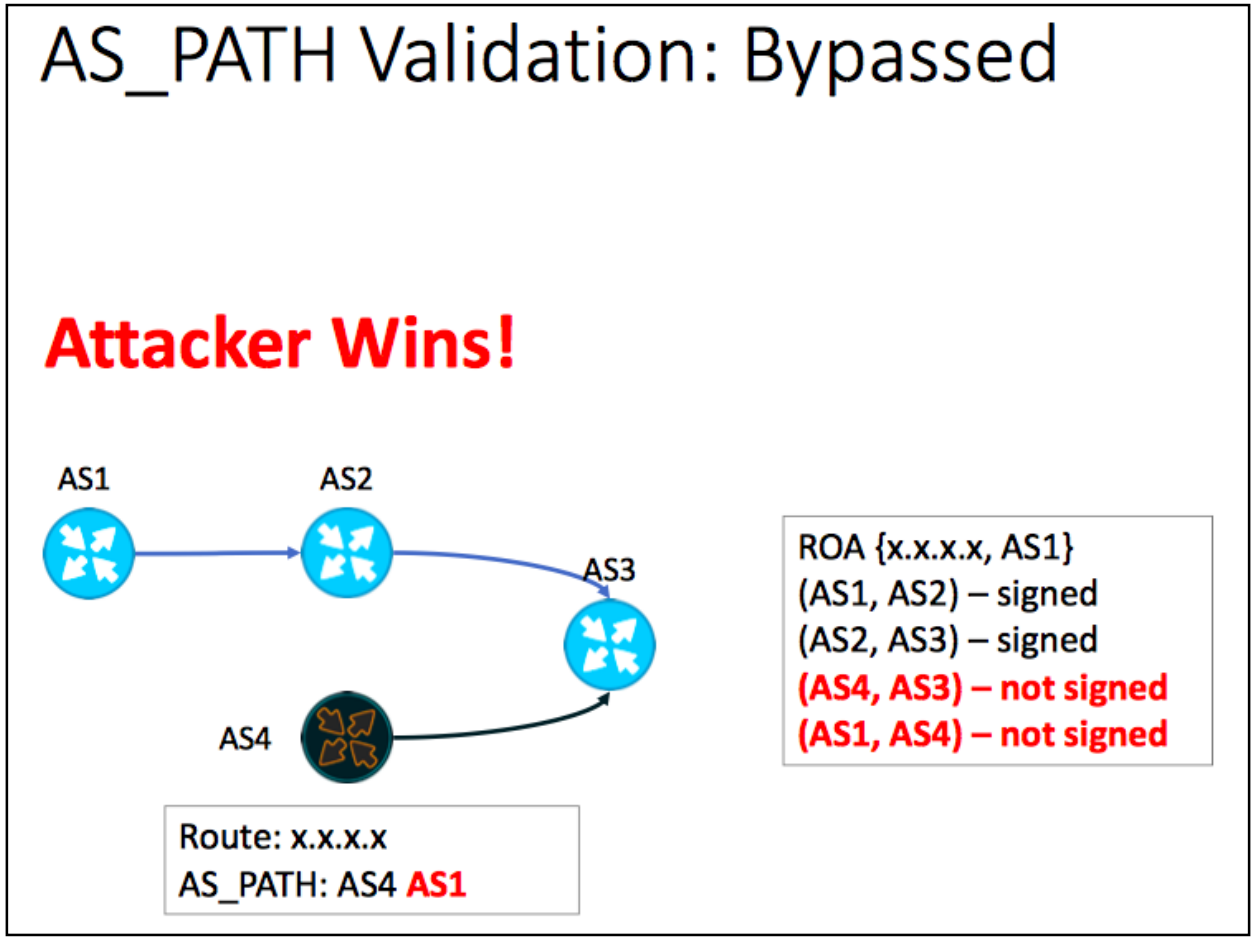

- BGP Route Security Cycling to the Future!
  https://ripe77.ripe.net/wp-content/uploads/presentations/118-ripe77.azimov_v2.pdf

# オリジン検証の回避




- BGP Route Security Cycling to the Future!
  https://ripe77.ripe.net/wp-content/uploads/presentations/118-ripe77.azimov_v2.pdf

# BGPsecのパス検証の回避

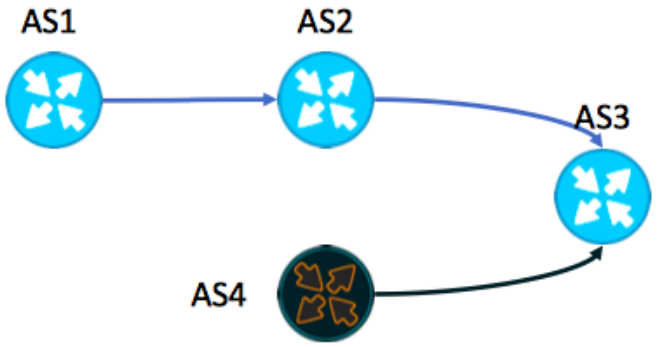



- BGP Route Security Cycling to the Future!
  https://ripe77.ripe.net/wp-content/uploads/presentations/118-ripe77.azimov_v2.pdf

# ASPAを使った検知の方法

## AS_PATH Verification

1. If the closest AS in the AS_PATH is not the receiver's neighbor ASN then procedure halts with the outcome "invalid";
2. If in one of AS_SEQ segments there is a pair (AS(I-1), AS(I)) is "invalid" then the procedure also halts with the outcome "invalid";



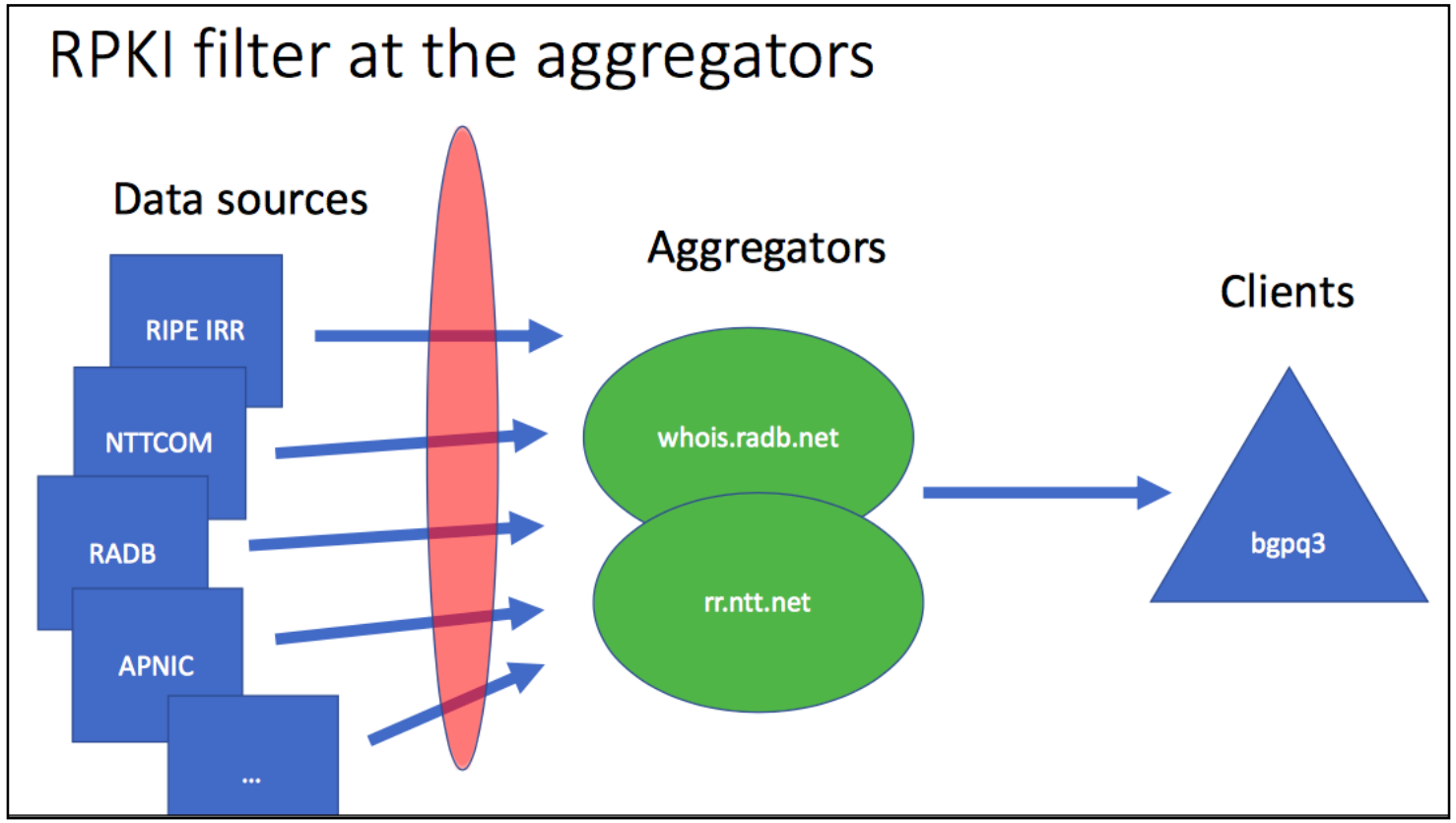

ROA {x.x.x.x, AS1}
ASPA {AS1, AS2}
ASPA {AS2, AS3}
ASPA {AS3, 0}

Route: x.x.x.x
AS_PATH: **AS2 AS1**

- BGP Route Security Cycling to the Future!
  https://ripe77.ripe.net/wp-content/uploads/presentations/118-ripe77.azimov_v2.pdf

# IEPGミーティングより

- ROAとコンフリクトするIRRのrouteオブジェクトをフィルタリングしてIRRの情報を集約




- Routing Security Roadmap
  http://iepg.org/2018-11-04-ietf103/IETF103_Snijders_Routing_security_roadmap-v2.pdf

# RPKI/オリジン検証のリスク要素と対応策

オリジン検証の導入検討のために

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

# オリジン検証が使えなくなる要素と対策(1/4)

- **有効期限/nextUpdate**
  - リソース証明書(1年)、ROA(約1年)、CRL(10日)、マニフェスト(10日)に設定されている。RPKIシステムでは自動的に更新するようになっているが、これらを過ぎるとROAキャッシュにおいてROA検証の結果が無効となり、RTRを通じてそのプレフィックスがルータに伝わらなくなる。有効なROAが見つからないとROVの結果は「Not found」の状態になる。
    - ROV = Route Origin Validation
  - RPソフトウェアでマニフェスト等を無視する設定はあるが、各々によって守られるものがあるため、無視することは非推奨。Validなプレフィックスを監視しておき「Not found」になったときにアラートをあげる等の対策が考えられる。Not foundの経路をドロップする設定にしてしまうと上記の理由で不必要にドロップしてしまう恐れあり。

# オリジン検証が使えなくなる要素と対策(2/4)

- **発行システム**
  - リソースPKIのC発行システムが使えない場合、新たなリソース証明書の発行と失効、ROAの発行、ROAの削除ができなくなる。ただしリポジトリのサーバにアクセスできれば、発行済のオブジェクトを参照することはできる。
  - 発行システムのメンテナンスなどのアナウンスは要注意。予め必要なROAを発行しておきたい。(JPNICでは発行システムの通年稼働のための構成を検討中)

# オリジン検証が使えなくなる要素と対策(3/4)

- **リソース**
  - APNICやJPNICのリソースCAの証明書が何らかの原因で有効にならない時、ユーザのリソース証明書やROAが有効にならなくなる。またAPNICやJPNICでは、レジストリデータベースを元に分配の正当性を確認しているため、返却などの状態に合わせてそのアドレスが記載されたリソース証明書やROAは無効になる。
  - ROVの結果は「Not found」になる。対策は「有効期限/nextUpdate」と同じ。(証明書が原因である場合は、その切り分けのためにJPNICのTALとAPNICのTALを使える)
    アドレス移転の手続きは返却→再割り振りという流れになるため基本的に有効性は維持されない事に要注意。

# オリジン検証が使えなくなる要素と対策(4/4)

- **オブジェクト取得**
  - リソース証明書・ROA・CRL・マニフェストを配布しているサーバ(リポジトリ)は、発行システムとは別になっており、リソース証明書の新規発行や失効の操作ができなくても、発行済みのリソース証明書・ROA・CRL・マニフェストにはアクセスできる。
  - 試験提供である現在はJPNICがリポジトリを運用しているが、ミラーリング等によってリポジトリの可用性を高めることができる。転送時間の削減にもなるためご検討を推奨。

# おわり

# RPKIのはじめ方

資源管理者証明書を準備（資源管理カード／ブラウザ内）

申請における認証について
https://www.nic.ad.jp/ja/ip/id-procedure.html

↓

資源申請者証明書を担当者に発行（ブラウザ内）

資源申請者証明書発行マニュアル
https://www.nic.ad.jp/doc/issue-manual-02.pdf

↓

リソース証明書とROAの発行開始

https://rpki.nic.ad.jp/

↓

発行完了！

お問合せ窓口： ip-service@nir.nic.ad.jp
（または rpki-query@nic.ad.jp）

# JPNICのRPKIまとめ

- **試験提供サービス**

  https://www.nic.ad.jp/ja/rpki/

  https://rpki.nic.ad.jp/

  - IPアドレスの割り振りを受けている方がROAを登録したりRPKIのCAを立ち上げてつなげたりできる。
- **ROAキャッシュサーバ**

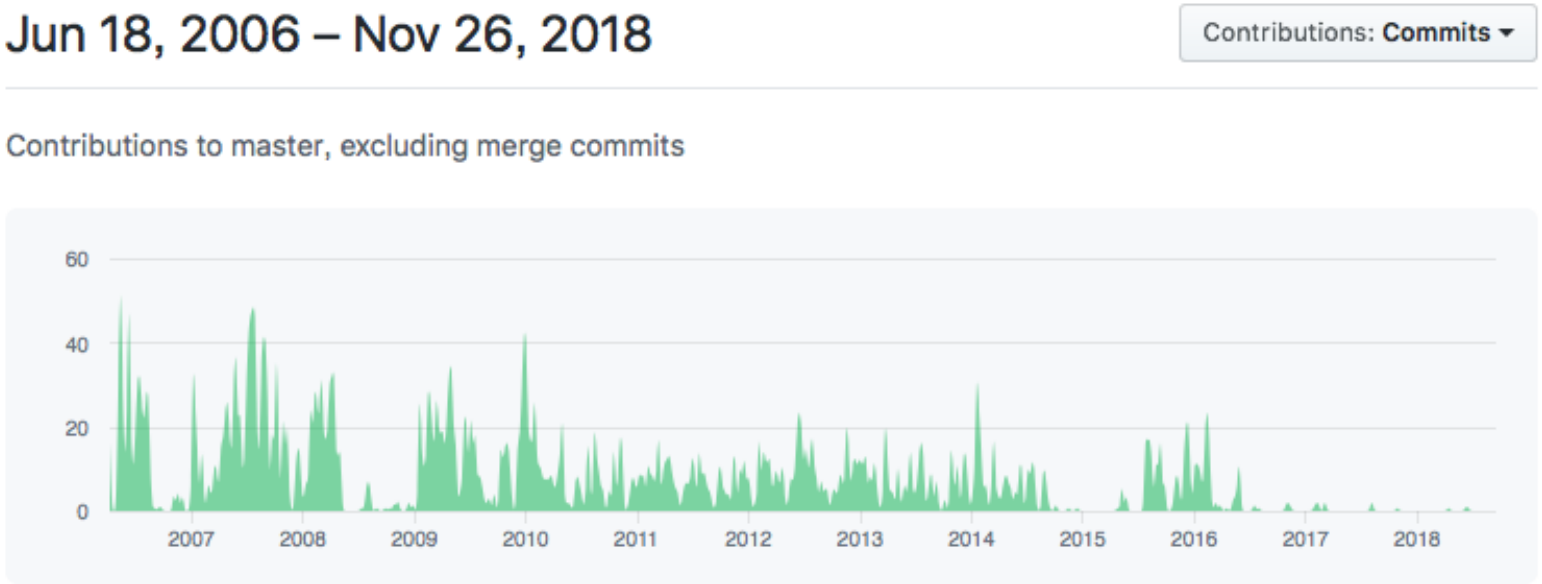
  192.41.192.218　port　323
- **日本語版RPKI Validator**

  http://roa2.nic.ad.jp:8080/
- **JPNICのTrust Anchor**

  https://serv.nic.ad.jp/rpki/jpnic-preliminary-ca-s1.tal

# リソースCAの実装

- **RPKI Tools**
  - https://github.com/dragonresearch/rpki.net




https://github.com/dragonresearch/rpki.net/graphs/contributors
© 2018 GitHub, Inc.

# ROAキャッシュの実装

- **RPKI Tools**
  - 情報と入手元　1つ前のスライドと同じ
- **RPKI Validator**
  - https://github.com/RIPE-NCC/rpki-validator
- **RPSTIR**
  - https://github.com/bgpsecurity/rpstir
- **ROUTINATOR**
  - NLnetLabs/routinator
    https://github.com/NLnetLabs/routinator

# BGPルータ

- **Cisco “BGP - Origin AS validation”**
  - Cisco Feature Navigatorより
    IOS XE - ISR 4451-X, ASR1002-Xほか
    IOX - ME3800, 7201ほか
- **Juniper “Origin Validation for BGP”**
  - Juniper Feature Explorerより
    EX9200 - Junos OS 12.3R2, M7i - Junos OS 13.2R2, vMX - Junos OS 14.1R5ほか
- **Nokia(旧Alcatel-Lucent)**
  - SR OS 12.0.4R以降

# BGPルータ

- **NIST BGP Secure Routing Extension (BGP-SRx / BGPSEC-IO)**

  https://www-x.antd.nist.gov/bgpsrx/
  - ASパス検証に対応
- **BIRD BGPsec**

  http://bird.network.cz/
  http://www.securerouting.net/tools/bird/
  - ASパス検証に対応
- **FRRouting**

  https://github.com/FRRouting/frr
  - オリジン検証に対応

# BGPルータ

- **GoBGP**

  https://osrg.github.io/gobgp/

  https://github.com/osrg/gobgp/

  - オリジン検証に対応

# その他 - Webブラウザ

- **機能**
  - WebサーバのIPアドレスがROAに入っているかどうかを確認し、オリジン検証の結果を表示する。

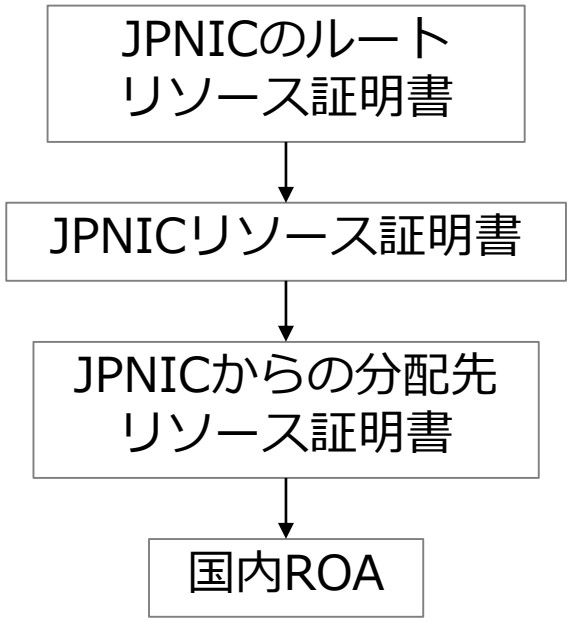
- **Firefox addon**
  - rtrlib/firefox-addon
    https://github.com/rtrlib/firefox-addon
- **Chrome 拡張**
  - rtrlib/chrome-extension
    https://github.com/rtrlib/chrome-extension

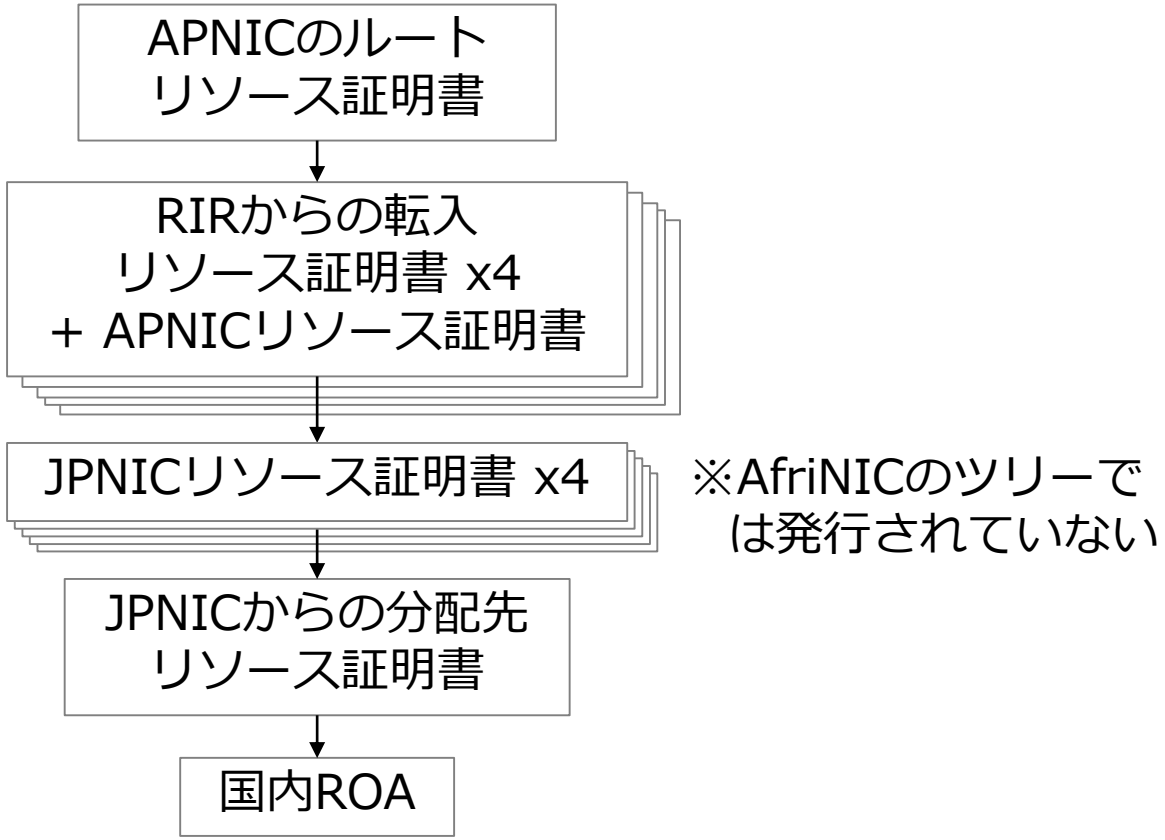
# JPNICが運営する経路奉行への経路提供組織

- 株式会社インターネットイニシアティブ
- インターネットマルチフィード株式会社
- エヌ・ティ・ティ・コミュニケーションズ株式会社
- エヌ・ティ・ティ・スマートコネクト株式会社
- KDDI株式会社
- 株式会社KDDI研究所
- さくらインターネット株式会社
- ソネットエンタテインメント株式会社

**JPNICで収集した経路情報も利用**

# JPとAPのリソース証明書のツリー構造




※AfriNICのツリーでは発行されていない

**APNICのTALとJPNICのTALの両方を使うと、国内のprefixを持つROAが二つ見える。ツリーが異なるため、片方にエラーが起きてももう片方に影響はでにくい(署名の系としての二重化)。**