IIJ/AS2497でRPKIはじめました

Let's start RPKI with IIJ/AS2497

Internet Initiative Japan

2021年1月29日

IIJ/AS2497 hori, y-yomogita

- **蓬田 裕一 YOMOGITA Yuichi (y-yomogita@iij.ad.jp)**
  - 2008年　IIJ入社
  - 2008-2009年　接続サービス導入・保守・サポート
  - 2010-2014年　バックボーン構築・運用
  - 2015-2019年　JPNAPサービス全般
  - 2019年-　バックボーン企画・設計・対外接続関連

- **堀 高房 HORI Takafusa (hori@iij.ad.jp)**
  - 2002年　IIJ入社
  - 2002-2013年　接続サービスやバックボーンなど
  - 2013-2017年　徐々にモバイルへ浮気。浮気が本気に…
  - 2018年-　正気を取り戻しバックボーンへ出戻り

はじめに

- **(今更なので) 省略!**

- **標準化**
  - IETF SIDR WG
  - RFC 3779, 6811, 6810, 7115, 8210, and more
- **過去のJANOGセッション**
  - JANOG30 どこまで動く? RPKI/Router
  - JANOG31 RPKI ハッカソン
  - JANOG32 RPKI セッション、RPKI routing WG報告
  - JANOG35 RPKIやってみませんか?
  - and more
  - (最近はない… すでに旬は過ぎた?)
- **有益なドキュメント**
  - NLnet Labs RPKI Documentation (https://rpki.readthedocs.io/)
  - and more

MANRS

- **MANRS知ってますか?**
  - https://www.manrs.org/
  - インターネットに参加する各組織(AS)が守るべき”マナー”
    - Network Operator, IXP, CDN & Cloud Operatorの3業態向け
  - 日本からは20組織程度が参加。IIJは2015年から

- **3業態ともRPKIが求められている**

(MANRS for Network Operator)

Action 4: Facilitate routing information on a global scale – RPKI

A network operator should create a valid Route Origination Authorization (ROA) for each IP prefix or set of prefixes it is legitimately authorised and intends to originate.

Discussion:

The most secure method of facilitating validation on a global scale is through the RPKI system which allows their routing announcements to be cryptographically verified. Network operators can obtain RPKI certificates for their own IP prefixes from the RIRs that allocated them, and then generate, publish, and maintain Route of Origin Authorizations (ROAs) corresponding to the IP prefixes they announce. Network operators must also encourage their Customer Network operators to do so as well.

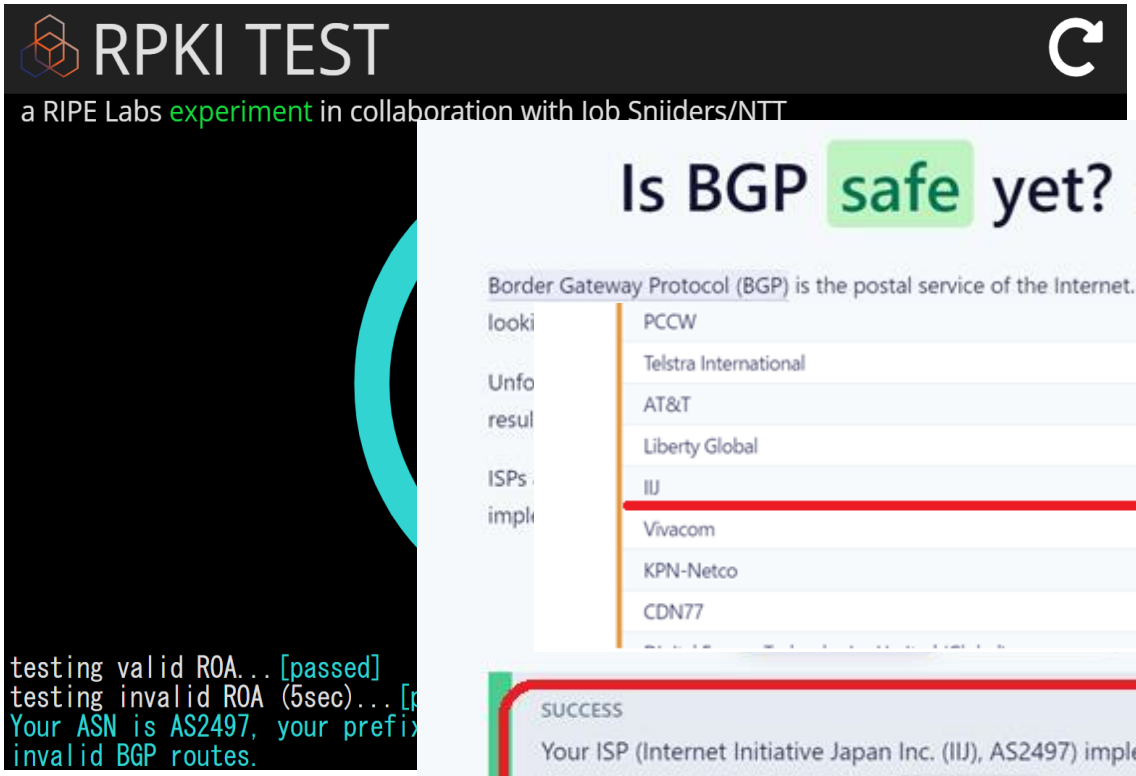
References:

- Origin Validation Operation based on the Resource Public Key Infrastructure (RPKI) – http://www.rfc-editor.org/bcp/bcp185.txt

- **いまや各ASが当然取り組むべきこと**

2016	社内でRPKI導入の気運が高まる
|	(散発的に検証は進めるも停滞)
2019末	導入の気運が再燃。本気出し始める
2020/3	ROV: 機能検証開始@Lab
2020/x	ROV: 機能検証開始@実網
2020/7	手応えを掴み実導入に向けてプロジェクト化
2020/10	ROA: 試験登録、検証
	ROV: キャッシュとRTR接続
2020/11	ROA: (現時点で可能な自社保有IP) 本番登録開始
	ROV: (Peer,Upstream) invalid経路のreject開始
2020/12	ROV: (Peer,Upstream) invalid経路のreject完了
	ROA: (現時点で可能な自社保有IP) 本番登録完了
2021(予定)	ROV: (Transit Customer) invalid経路のreject完了
	ROA: (自社保有IP全て) 登録完了
	(可能な限りの顧客PI) 登録完了

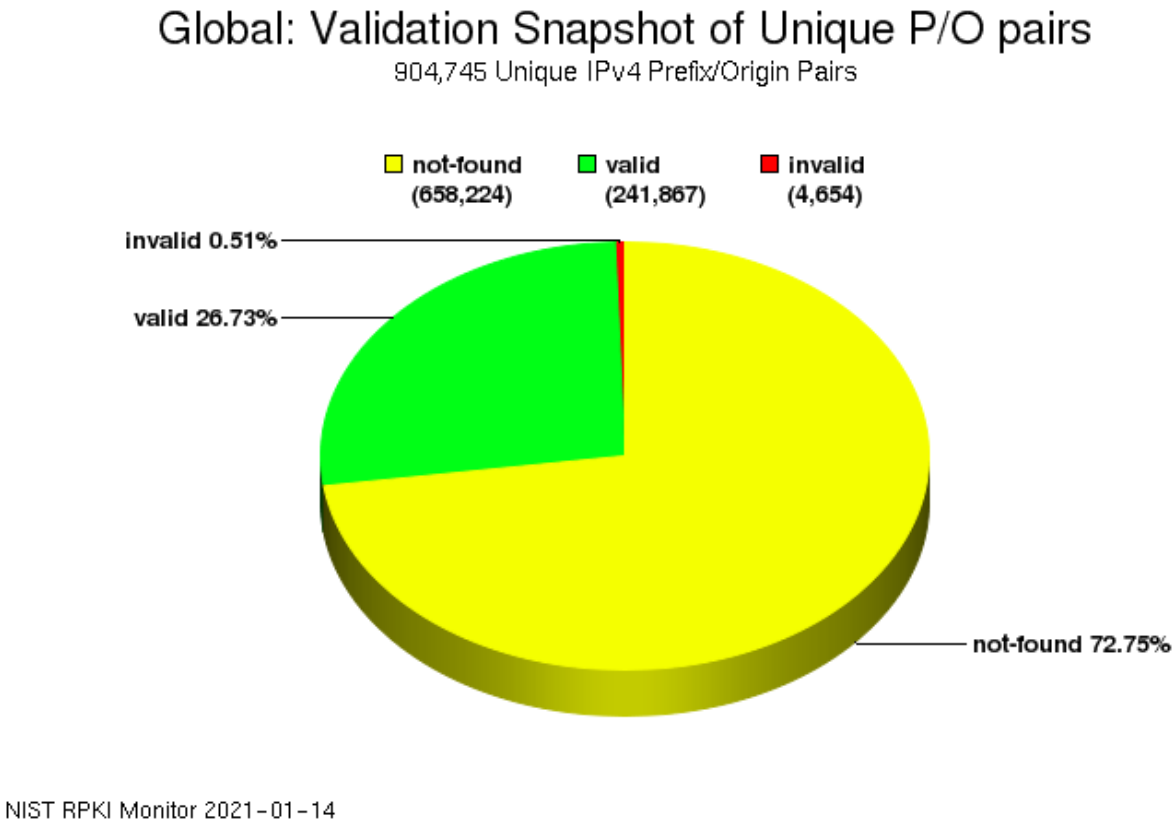
- **はい、IIJ/AS2497のBGPは安全です。**



出典: RIPE RPKI Test: https://labs.ripe.net/Members/nathalie_nathalie/rpki-webtest　CloudFlare: https://isbgpsafeyet.com/

- **RPKIを始めるために(最低限)やるべきこと**
  1. ROAを作る (作ってもらう) → 自Origin経路を守る
     - 自社に割り振られたアドレス (自社AS Origin, 顧客AS Origin)
     - Customerが持ち込むPIアドレス (自社AS Origin)
  2. ROVを入れる → 不正経路を伝搬させない
     - Upstream
     - Peer
     - Customer

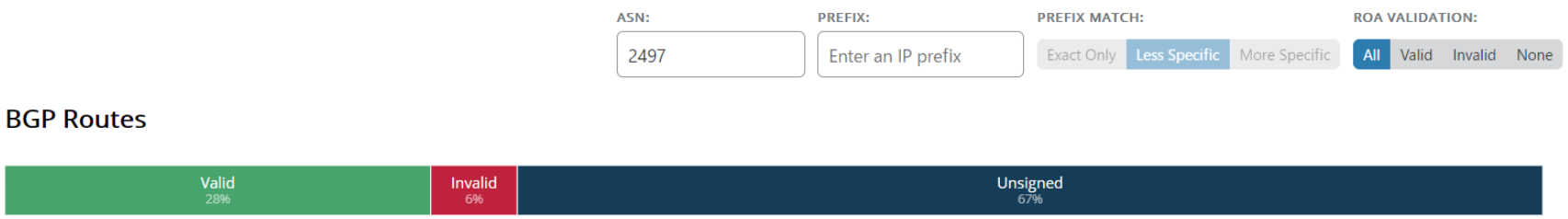
ROA



出典: https://rpki-monitor.antd.nist.gov/

- **JPNIC保有アドレスのROA状況** ※旧ROA Webの登録数
  - IPv4: 44.2%
  - IPv6: 57.2%

- **自社保有アドレスにおけるROA登録状況 (JPNIC割振)**
  - IPv4: 81.6%
  - IPv6: 100%
- **のはすが、Origin AS2497で見ると…**



出典: https://rpki.cloudflare.com/?view=bgp&validateRoute=2497_&asn=2497

- validはわずか28%
- invalid 6%はテスト
- unsigned 67%の大半は顧客が持ち込みAS2497でOriginateするPIアドレス

- **自社保有IPのうちROA登録できてないIPv4 18.4%の内訳**
  - 133.x.x.x/16
    - 歴史的PIアドレス
    - JPNIC RPKIシステムの対応待ち
  - 203.180.0.0/16
    - JPNIC ROA Webでリソース証明書がないと言われる
    - JPNIC RPKIシステムの対応待ち
  - 割り振りアドレスの全てを顧客へ割り当てている
    - Origin ASが顧客
    - パンチングホールでないが、顧客と調整が必要
  - 割り振りアドレスの一部を顧客に割り当てている
    - 一部のアドレスのOrigin ASが顧客
    - パンチングホール。顧客と調整が必要

ROAと広告経路の状態一覧

BGP Prefix	Origin AS	ROA Prefix	ROA Origin AS	ROA Maximum length	状況説明	ROV状況
172.122.0.0/15	2497	なし	なし	なし	ROAなし	unknown
172.122.0.0/22	2497	172.122.0.0/22	2497	22	完全一致ROAあり	valid
172.122.16.0/22	2497	172.122.16.0/22	2497	24	これを包含するROAあり	valid
172.122.32.0/22	2497	172.122.32.0/20	2497	20	SuperNetのROAしかない	invalid length
172.122.48.0/22	2497	172.122.48.0/20	2497	24	これを包含するROAあり	valid
172.122.64.0/22	2497	172.122.64.0/22	61215	22	Origin違いで完全一致ROAあり	invalid ASN
172.122.80.0/22	2497	172.122.80.0/22	61215	24	Origin違いでこれを包含するROAあり	invalid ASN
172.122.96.0/22	2497	172.122.96.0/20	61215	20	Origin違いでSuperNetのROAしかない	invalid ASN
172.122.112.0/22	2497	172.122.112.0/20	61215	24	Origin違いでこれを包含するROAあり	invalid ASN
172.122.128.0/22	2497	172.122.128.0/22	0	22	Origin0で完全一致ROAあり	invalid ASN
172.122.144.0/22	2497	172.122.144.0/22	0	24	Origin0でこれを包含するROAあり	invalid ASN
172.122.160.0/22	2497	172.122.160.0/20	0	20	Origin0でSuperNetのROAしかない	invalid ASN
172.122.176.0/22	2497	172.122.176.0/20	0	24	Origin0でこれを包含するROAあり	invalid ASN
202.16.104.0/21	2497	202.16.104.0/21	2497	21	Exact Match	valid
202.16.104.0/24	61215	202.16.104.0/24	61215	24	パンチングホール	valid
202.48.108.0/23	2497	202.48.108.0/23	2497	23	Exact Match	valid
202.48.108.0/24	61215	202.48.108.0/23	2497	23	経路ハイジャック	invalid ASN

- **IPアドレスの全社管理はLIRチーム**
  - 割当や管理、NIR/RIRとの窓口
- **ROAの作成・削除・変更**
  - AS運用ポリシーに従って作成したいが、ネットワーク運用部隊(NOC)とLIRが密に連携を行うのはしんどい
  - というわけで、NOCへ権限を付与
    - ROAの他にも**返却やDNS変更が可能な非常に強力な権限**
    - (近い将来JPNICではROAに限った権限を付与可能になる?)
- **LIR/NOCの役割分担**
  - LIR: 新規にアドレスが割り振られたらOrigin AS0でROA作成(未広告アドレスのフリーライド防止)
  - NOC: 実利用開始時(= AS2497広告時)にOrigin AS2497へ変更
  - NOC: 実利用終了時にOrigin AS0へ変更しLIRに返上
  - LIR: Origin AS0なアドレスを返却 (ミス防止)

- **IIJへ割振済み、AS2497 Originで経路未広告**
  - Prefix: 割振アドレス、Origin AS: 0、Max Length: 割振サイズ
- **IIJへ割当済み、AS2497 Originで経路広告**
  - Prefix: 割振アドレス、Origin AS: 2497、Max Length: 広告サイズ
- **IIJへ割当済み、一部を顧客Originで経路広告**
  - パンチングホール
  - Prefix: 割振アドレス、Origin AS: 2497、Max Length: 広告サイズ
  - Prefix: 割当アドレス、Origin AS: 顧客、Max Length: 顧客と相談

- **Max Lengthはどうあるべき?**
  - 原則広告経路と一致させ、Max Lengthを大きくするべきではない
  - Origin AS詐称による経路ハイジャックのリスクを低減
    - ref. RFC7115
  - RTBHやBGPを使ったDDoS mitigation等には注意
    - draft-ietf-sidrops-rpkimaxlen

- **手段は2つ**
  - NIR/RIRのRPKIシステムを使う
  - 自社でCAを運用する (BPKI: Business RPKI)

- **BPKI**
  - 自社でCAを独自運用
  - NIR/RIRからPublication Pointを向けてもらう
  - オープンなソフトウェアもある
    - Krill、rpkid
  - メリット
    - 自社アドレス管理システムとの統合、自動反映など?
  - デメリット
    - 運用コスト
    - 実際、運用が適当なCAも散見される

- **IIJはJPNICのRPKIを利用**
  - 現状では運用コストに見合ったメリットが見出せない

- **JPNIC ROA Web**
  - https://www.nic.ad.jp/ja/rpki/
  - 2020/10に新システムリリースされ、JPNIC/APNICの連携が早くなった (それまでは小人さんが夜な夜な頑張ってた!?)

- **オペレーション**
  - 危険。一瞬で到達性を失わせることも可能性
  - Web UIゆえ自動化は困難。作業は必ず2人体制
    - 操作履歴はTeamsを利用し画面録画
  - JPNIC ROA WebはROA登録直前に想定されるROV状態を表示してくれるため安心
  - 変更はなく、削除 + 再作成

- **各ASへの反映には時間が掛かる**
  - DNS浸透警察のほうから来た人に怒られかねないが…
  - DNSのようなROA作成者が指定可能なTTLはない
  - 各ASのROA/VRP取得タイミングはまちまち。反映時間は読めない

1. NIR/RIRのRPKIシステムに登録
2. NIR/RIRがROA作成
3. (場合によっては?) RIR CAからNIR CAにPublication Pointが向く?

(以下、世界の各ASで)

4. TALを辿り各CAからROA取得・検証、VRP作成
5. キャッシュがVRPロード
6. キャッシュがルータにSerial Notify送信 or
   ルータがキャッシュにSerial Query送信
7. ルータがキャッシュからVRP取得
8. ルータがAdj-RIBs-Inを再評価、RIB/FIB更新
9. AS内にベストパスが伝搬

- **何を監視するか?**
  - 他ASで正しくvalid扱いされているか?
  - ROAがないまま広告していないか?
  - ROAに反する経路を漏らしていないか?
  - パンチングホールは大丈夫か?
  - 経路ハイジャックされていないか?

- **どうやって?**
  - bgpalerter
  - RIPE RIS
  - 経路奉行

- **ROAあるある**
  - 把握してないROAが存在
    - ROAは勝手に生えない
    - (前任が)なんとなく登録した?
  - ROAを考慮せず広告サイズを変更 or パンチングホール実施
  - ROV普及により到達性が徐々に失われ発覚
    - 到達性にムラがあるため発覚しづらい、調査しづらい

- **今一度、保有IPのROA登録状況確認を!**

ROV

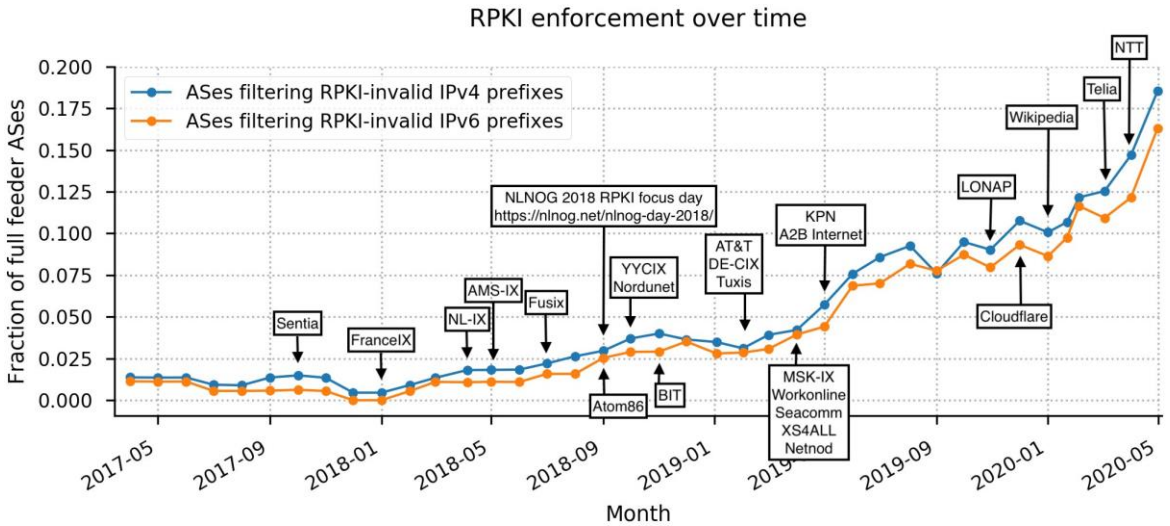
- **IX/Tier 1中心にだったが、2020年はさらに多くのASで導入が進んでいる模様**
- **しかし、日本ではGINくらい?**
  - 導入済みの人は挙手!
- **やるなら今でしょ!**

Status

Displaying 29 major operators　　+ Show all　+ Show ASN column

NAME	TYPE	DETAILS	STATUS
Telia	transit	signed + filtering	safe
Cogent	transit	signed + filtering	safe
GTT	transit	signed + filtering	safe
NTT	transit	signed + filtering	safe
Hurricane Electric	transit	signed + filtering	safe
TATA	transit	signed + filtering	safe
PCCW	transit	signed + filtering	safe
RETN	transit	partially signed + filtering	safe
Cloudflare	cloud	signed + filtering	safe
Amazon	cloud	signed + filtering	safe
Netflix	cloud	signed + filtering	safe
…on	cloud	signed + filtering	safe
	cloud	signed + filtering	safe
	transit	signed	partially safe
	ISP	signed + filtering peers only	partially safe
	cloud	signed	partially safe
	transit	started	unsafe
	transit	started	unsafe

https://isbgpsafeyet.com/



https://twitter.com/JobSnijders/status/1256326712347881473

- **どこで? → AS境界でROVする**
  - 対Peer、対Upstreamが対象
  - 初期導入においてはTransit Customerは対象外
  - 内部のeBGP(Private AS等)は対象外

- **何をどうする? → invalid経路を一律破棄**
  - 悪意のある不正な経路、設定ミスかは不問
  - あくまでRPKI的にinvalidかどうかだけ。当たり前だが案外大事
  - valid, not found, unverifiedは等価に扱う

- **誰に伝える? → 顧客への公式アナウンスはしない**
  - サポート部門と相談し決定

- **基本的な動作**
  - ルータ: RTR、Validation、Policy/Best Path Selection
  - Relying Party(キャッシュ): RTR、Rync/RRDP、ROA Validation
- **負荷**
  - ルータ: メモリ使用量、Routing Process負荷
  - Relying Party: RTRセッション数、メモリ使用量、CPU負荷
- **様々なケース**
  - RFC6907 7.1 Prefix-Origin Validation Use Cases
  - AS_SETの扱い
  - 実ROA + 試験用ROA(SLRUMで作成)

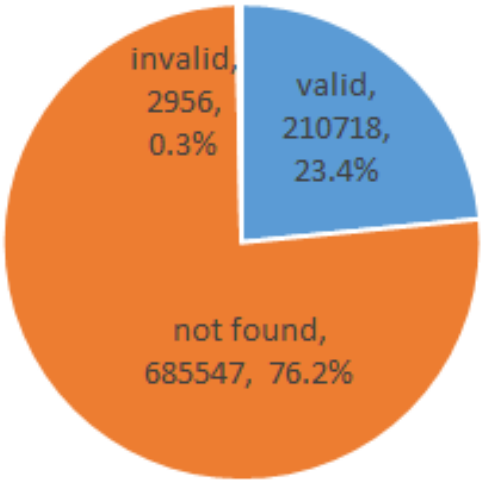
- **ルータ**
  - OS/Version
    - JUNOS、IOS-XR。ここでは言えないほど古いものも…
    - DampeningしているならJuniper PR1483097も注意が必要かも
  - RTRパラメータ
    - Serial Query送信間隔、RTRが落ちてからVRP消すまでの時間など
      - JUNOSはrecord-lifetimeを短くすると不定期にVRPが消えた
    - OS間の挙動差異はなくしたいが、設定可能パラメータが異なる
  - ROVする(しない)ピアの選定
    - 組織内のeBGPなど意図しないピアでROVすると大障害
    - IOS-XRは無効にするピアを明示するので忘れやすい
  - Policy
    - validation自体とその結果に基づく経路制御は別物
    - validation結果に対してどう制御するか (local pref. 0 → reject)
    - IOS-XRはさらにbest path selectionへの反映も指定
    - community(RFC8097)をつけてiBGPに流す

- **Relying Party**
  - 冗長性
    - 物理サーバ/VM/Container、POP、ソフトウェア実装
  - ROA取得・検証/VRP生成とRTRを分離するか?
  - 自営 or パブリックキャッシュ利用

(IIJの場合)

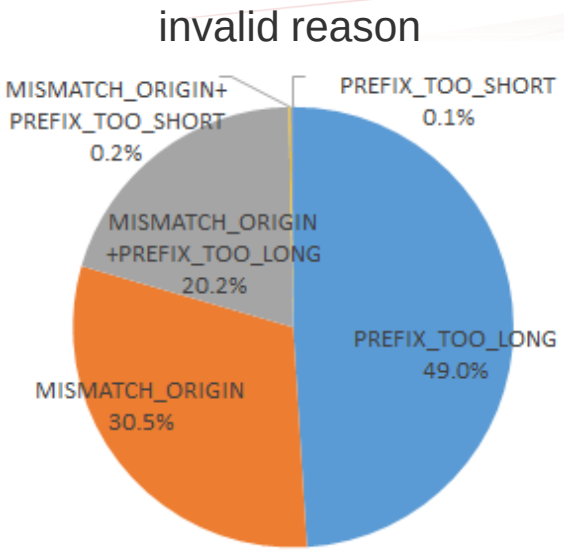
- 各ルータは2台のキャッシュと接続
  - 異なる国内POP、異なるソフトウェア実装
  - 海外ルータも国内を参照
  - キャッシュ1台が20台程度のルータを担当
- Routinator 0.8.2 + RIPE NCC RPKI Validator 3.1 (2021/1現在)
  - ROA取得からRTRまで同じインスタンスで完結
    - CAに負荷が掛かるので取得はまとめるべき…
  - Routinator: デプロイも日々の運用も容易
  - RPKI Validator: Java… Web UIは便利。2021/7開発終了☹

- **顧客フロント(サポート、営業)が気にすること**
  - 趣旨に対する反対意見は皆無だが… 導入時においては
    ROVによるメリット <<< ROVによる通信影響
  - 理由がなんであれ(本当の不正、mis-configuration)、
    ROVによりこれまでできていた通信ができなくなる不安
  - よく理解できるので、この不安を取り除いてあげる



- **ROVで破棄される経路** *2020/9頃
  - およそ3,000経路
  - フルルートの0.3%、多いような少ないような…
  - 当然、これらが本当の不正経路か、設定ミスかはわからない
  - 3,000経路/0.3%だけを見せるとさらに不安が募るので深掘り

invalid経路の分析 (1/3)



- PREFIX_TOO_LONG
  - Max Lengthより細かい
  - AS内の細かい経路を漏らしてる?
- MISMATCH_ORIGIN
  - Origin ASがおかしい。パンチングホールかも?
- MISMATCH_ORIGIN + PREFIX_TOO_LONG
  - 細かい経路 & Origin ASおかしい
  - パンチングホールでありがち
- PREFIX_TOO_SHORT
  - ROAより経路長が短い。なぞ
- MISMATCH_ORIGIN + PREFIX_TOO_SHORT
  - Origin ASのおかしい。なぞ

いずれも本当の不正経路の可能性はあるが
それなら対処して長期間は続かないはず…

設定ミスや考慮漏れの可能性が高いか?

invalid経路の分析 (2/3)

invalid経路のOrigin AS (TOP10)

#	ASN	Routes	%	CAIDA AS Rank
1	INDOSATM2-ID/AS4795	128	4.34	2597
2	UNKNOWN/AS54004	126	4.27	108
3	Clouvider/AS62240	104	3.53	711
4	VSNL-AS-AP/AS4755	93	3.15	38
5	OPENNET-COMM-AS-AP/AS131178	79	2.68	6951
6	AIRTELBROADBAND-AS-AP/AS24560	56	1.90	10593
7	TMVADS-AP/AS17971	40	1.36	13509
8	GLOBEINTERNET/AS6453	36	1.22	7
9	UNKNOWN/AS22368	36	1.22	11253
10	CNNIC-TENCENT-NET-AP/AS45090	34	1.15	10587

invalid経路に対応するROA Origin AS

#	ASN	Routes	%	CAIDA AS Rank
1	CV-INET/AS6128	292	9.90	100
2	INDOSATM2-ID/AS4795	135	4.58	2597
3	VSNL-AS-AP/AS4755	114	3.87	38
4	Clouvider/AS62240	106	3.59	711
5	FPT-AS-AP/AS18403	79	2.68	272
6	GBLX/AS3549	52	1.76	13
7	AIRTELBROADBAND-AS-AP/AS24560	51	1.73	10593
8	TMVADS-AP/AS17971	40	1.36	13509
9	UNIRED-TDATAPERU/AS6147	40	1.36	2593
10	GLOBEINTERNET/AS6453	39	1.32	7

- CAIDA AS Rankを添えて、気にするようなASでないことを主張…
- いずれにも出てくるASはおそらく設定ミス。自業自得

- **invalid経路を破棄した場合、実際に到達性がなくなるのはどのくらい?**
  - あるinvalid経路を破棄しても、代わりの経路があれば到達性は保たれる
  - 何を持って「代わりの経路がある」とするかにより異なる
  - invalidでない && invalid経路より短い && invalid経路と同じOrigin AS
    - 到達性を失うのはフルルートの0.152%
  - invalidでない && invalid経路より短い
    - 到達性を失うのはフルルートの0.097%

- **これら宛先との通信量を推定**
  - samplingした経路との通信量をNetFlowで調査
  - 散発的に少量が流れているのみ

→ **3,000経路を破棄しても大きな通信影響はない!**
  - もちろん全くないとは言い切れないが個別対応可能なレベル

- **Transit Customerへの影響**
  - 当然、IIJからのinvalid経路広告がなくなる
  - ROV導入済みのASとIIJからTransitを調達していたら、IIJが導入したタイミングで経路を失う… (先にやればよかった)

- **どうしてもそのinvalid経路が今必要だ! と言われたら**
  - 各ソフトウェアともSLRUM(RFC8416)が使えるので、強引にvalidにして通す (オレオレROA)
  - 用意はしたが、未来永劫使われないことを願う
    - 本当の経路ハイジャックを許すことになるかも。乱用禁止
    - 各ASでROV導入が進む中、IIJだけ通しても意味は薄い

- **サポートからの要望**
  - 顧客問い合わせ時にROVの影響かどうか確認できるようにして
    - Looking Glass、 RPKI ValidatorのWeb UI、invalid経路ダンプ
  - invalid経路をなくす取り組み、RPKIの啓蒙をして
    - IIJ単独でどうにかなる話ではないので、業界全体で

- **公式アナウンスするか?**
  - (前提) 今回の導入時点ではTransit Customerに対してROVはしない
  - 当然、影響はIPバックボーンを経由するあらゆるサービス

- **類似事例**
  - Source Address Validation、OP25B、児ポ/マルウェアブロッキング
  - それぞれ事情は異なるが…アナウンスは実施
  - 了承を得られた顧客から(にだけ)導入したケースも

- **今回は、公式アナウンスはしない**
  - 趣旨は理解いただけるだろうが、各顧客の実通信に影響がないことを説明/証明するのは困難 (弱気)
  - ASとしてのポリシーであり、サービスの話ではない (強気)
  - RPKI的にinvalidなんだから落として何が悪い (暴言)
  - 代わりに、ルーティングセキュリティ向上への取り組みとして各所で紹介、RPKIが当たり前であると(緩やかに)理解してもらう

聞いてないよ!というお客様がいればこの場を借りてお詫びします

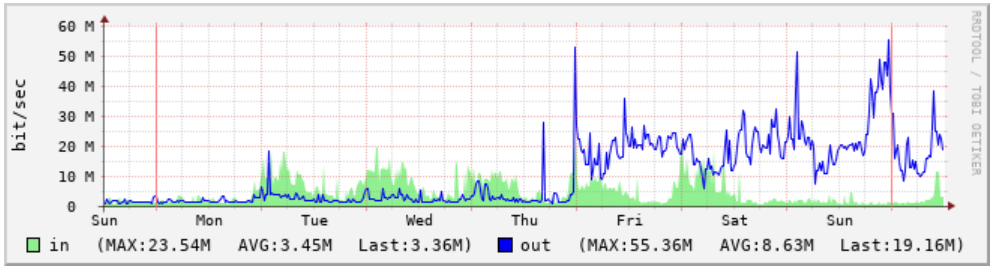
- **Relying Party**
  - 各ソフトウエアともにMetricは充実
  - GrafanaやPrometheus等との連携は容易
  - アラームをあげるMetricの選定、閾値調整が難しく未設定
  - フルルートの監視に近い命題?
    - パブリックなキャッシュと比べるとVRP数に差異が…
  - CAからの取得失敗も日常茶飯事

```
> show validation session
Session                State    Flaps          Uptime     #IPv4/IPv6 records
(CloudFlare)            Up          0 2w5d  02:06:10      177519/29164
(JPNIC)                 Up          0 11w6d 19:47:46      161601/27836
(IIJ#1)                 Up          0 11w6d 19:48:15      178784/29839
(IIJ#2)                 Up          0 11w6d 19:48:15      178784/29839
(IIJ#3)                 Up          0 11w6d 19:48:15      178785/29839
(IIJ#4)                 Up          0 11w6d 19:48:15      178785/29839
(IIJ#5)                 Up          0 11w6d 19:48:15      178780/29837
(IIJ#6)                 Up          2 1w2d  02:44:05      178767/29836
(MFEED)                 Up          0 11w6d 19:47:56      161540/27813
```

- **ルータ**
  - RTRセッションは当然として
  - 最低限、VRP数や各validation state数は欲しいが外部から取得できるMetricが少ない
    - MIBはなさそう。Telemetryは未確認
    - 実装お願いします > 各ルータメーカーさん
  - Rejectした経路の記録
    - サポートからの要望。顧客の問い合わせに備える
    - このためだけにBMPするのは重い…
    - 定期的に”show …”の結果をダンプする力技
- **外形監視**
  - RIPE Beaconの経路が定義どおりvalidationできているか
  - 他にアイデアがあればぜひ共有を!

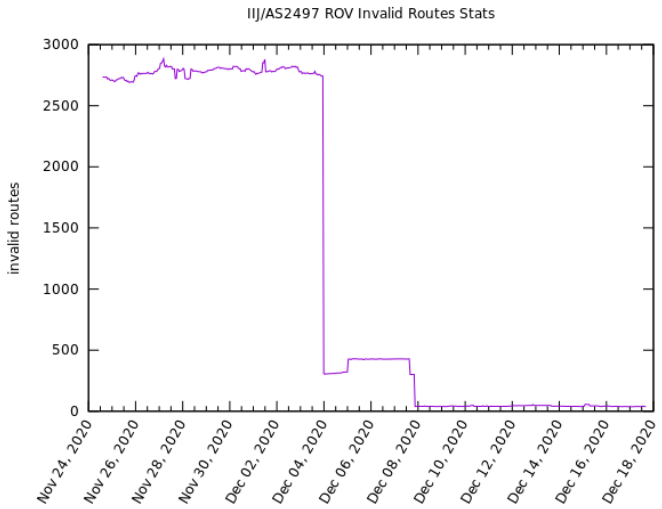
- **対象**
  - Peer/Upstreamと接続している数10ノード、2,000弱のBGPピア
  - これら全てにROVを入れて回る苦行
    - ついでにGSHUT(RFC8326)も入れた;-P

- **設定の流れ**
  - invalid 約3000経路の影響が未知数なのでケアする
  1. 全ノードでvalidationを開始、invalidはLocal Pref 0
     - トラフィックがすごーく遷移するかもしれないことは意識
  2. すこしづつinvalid経路をrejectするように変更
     - APAC/EAMA → JP → US → Upstream
     - 最終的にUpstreamの特定接続にinvalidが集中する状況を作ってみた
     - Upstreamは当然ROV導入済みなのでこの時点ですでにinvalid経路は少ない
  3. 満を持してすべてreject!



- **invalid経路の状況** *AS内のJUNOS 20.1で観測
  - Transit Customer(ROV未導入)からのinvalid経路はわずか数経路
  - Peer/Upstreamからのinvalid経路は30-40
    - すべてAS_SETを持つ経路
    - OS、バージョンにより扱いが異なる
    - RFC6907 7.1.9
      - Comment: In the spirit of [RFC6472], any route with an AS_SET in it should not be considered valid (by ROA-based validation). If the route contains an AS_SET and a covering ROA prefix exists for the route prefix, then the route should get an Invalid status. (Note: AS match or mismatch consideration does not apply.)

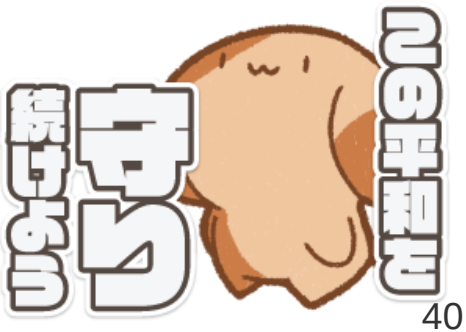
- **顧客/社内からの問い合わせ**
  - 現時点では皆無。よかった!



- **ROA**
  - AS2497 Originのカバレッジを100%に
  - Customer OriginもROA作成を啓蒙
- **ROV**
  - Transit CustomerへのROV導入
    - RTBHやprefix/as-path filterの考慮
  - Relying Party Softwareの更新
    - バージョンアップへの対応
    - RPKI-Validator3 2021/7 EoL
- **監視の充実**
- **さらにその先**
  - Peer Lock
  - AS-Path Validation

まとめ

- **IIJのRPKI導入事例を共有**
  - 腰は重かったが、本気でやれば1年でできた
- **みなさん、進捗どうですか?**
  - やってるなら、ノウハウを共有しましょう
    - ROA/ROVのポリシー・実装、監視
  - やっていないなら、ぜひはじめましょう!
    - 少なくともROAは作りましょう
    - ノウハウ共有は惜しみません。お気軽にご相談を
    - RPKI slack(rpki.slack.com)あります。 希望者は招待します
- **各ASの地道な努力がインターネットを支えています**
  - RPKIが当たり前の世界に
  - MANRSにも参加して、RPKI以外のアクションも



日本のインターネットは1992年、IIJとともにはじまりました。以来、IIJグループはネットワーク社会の基盤をつくり、技術力でその発展を支えてきました。インターネットの未来を想い、新たなイノベーションに挑戦し続けていく。それは、つねに先駆者としてインターネットの可能性を切り拓いてきたIIJの、これからも変わることのない姿勢です。IIJの真ん中のIはイニシアティブ――IIJはいつもはじまりであり、未来です。