C13 ルーティングセキュリティ インターネット運用の羅針盤

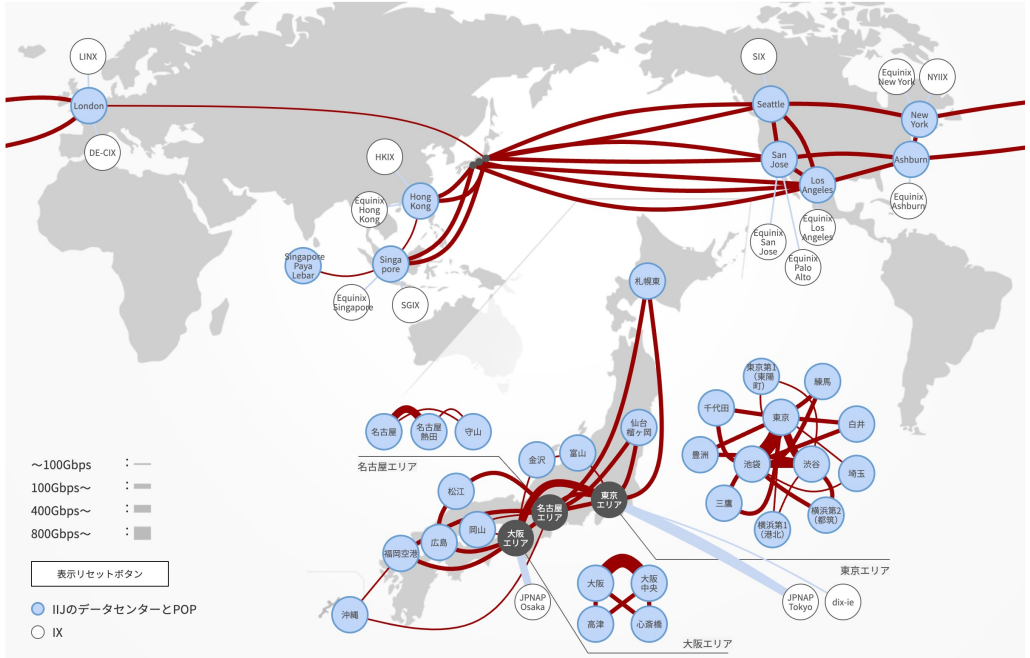
IIJ/AS2497 hori@iij.ad.jp

About Me

- 氏名: 堀 高房
- 所属: 株式会社インターネットイニシアティブ
  基盤エンジニアリング本部
- 主務: ネットワークやDC、サーバなどインフラ全般の企画
- 趣味: AS2497の中の人
  (バックボーンネットワークの企画、開発、運用等全般)

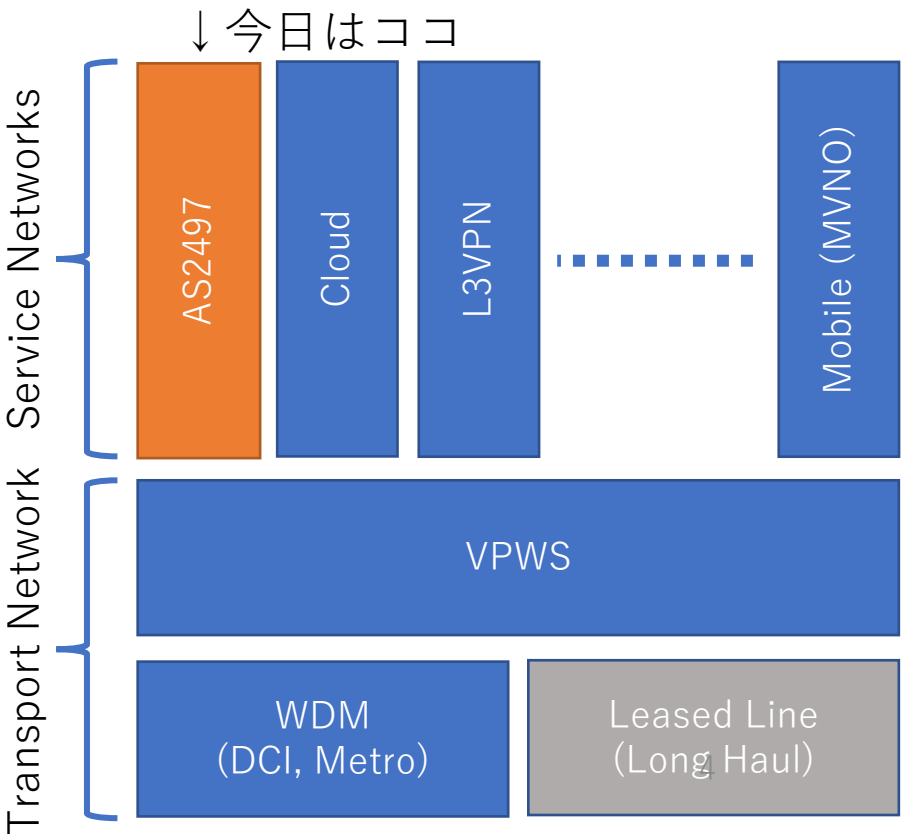
About IIJ

- 古参の商用ISP、今では手広く事業を展開
  - 創業30年+
  - クラウド、モバイル、IoT、ヘルスケア、デジタル通貨など
- 日本を中心に海外各地にネットワークを展開 (50 POP程度)
- AS2497 + 海外現法ASいくつかを運用



About IIJ Backbone

- VPWSを基盤として、その上位に各サービスネットワークを構成
  - Internet Backbone(AS2497)もサービスネットワークの1つ
  - VPWSはtraditionalなMPLS-RSVP
- シンプルで運用性の良いネットワークをコンセプトに設計
  - 昨今のニーズにそぐわないところも出てきているため、刷新に向け企画中
- サービスネットワークも含め、数1,000台のネットワークノードを運用



AS運用はインシデントとの戦い (1/3)

- 機器故障、回線障害は日常的
  - 1-2台/週はルータが故障している感覚
  - 国際線は数本/日、特にアジア周辺は一度切れると数ヶ月復旧しないことも
    - 国家規模のイベントや国際情勢でケーブル修理に係る当局許可がもらえない?
    - IIJでも実は昨年末から一向に復旧しない回線が😭
- Network OS(NOS)のバグ
  - つい先月も特定のBGP attributeに起因するインシデントが世界的に発生
    - https://labs.ripe.net/author/emileaben/unknown-attribute-28-a-source-of-entropy-in-interdomain-routing/
  - バグを全て回避するのは不可能であり、1つの要因で全滅しない考慮が大事
    - ベンダー、プラットフォーム、OS versionの分散によるSPoF軽減
    - 昨年IIJでもとあるAS起因のBGP updateにより多数のルータでプロセスクラッシュが発生したが、全滅には至らず (大変ご迷惑をお掛けしました🙇 > お客様各位)

AS運用はインシデントとの戦い (2/3)

- DDoS
  - ~100Gbps程度の顧客宛DDoSはありふれたもの
    - scrubbing center + 手動flowspecで対処
  - ここ数年は顧客発インターネット宛が多発、脆弱な端末がBot化し数100Gbps規模にまで激化
    - ウクライナ等、国際情勢に関連すると思われるものも多数
    - upstreamからAUP違反による利用停止をチラつかされる羽目に
  - 根本的には顧客に端末の対処をしてもらうしかなく、受け身な対応に終始
    - もう少しプロアクティブに対応したいが現状の法制度・ガイドラインでは困難
    - 総務省サイバーセキュリティタスクフォースに期待
  - エンドユーザな方は自分の端末に、ISPの方は自社の顧客に責任を!

AS運用はインシデントとの戦い (2/2)

- NOSの脆弱性
  - PCとは異なりRCEのような脆弱性はあまりないが、ルーティングプロセスのクラッシュや過負荷などは日常的
    - 前述の6月の事例もメーカからSecuriry Advisoryが公開された
  - バグや短くなる傾向にあるNOSのEOL含め、真面目に対処していると常に最新OSへアップデートする羽目に
    - 数台/週ペースでやらないと追いつかず、検証とメンテナンスに明け暮れる日々
    - 皆さんはどのくらい真面目にやってます?
- ルーティングインシデント
  - 今日のお題

ルーティングインシデント (1/3)

- 一口にルーティングインシデントと言っても様々
- 「サイトAに到達性がないんです」
  - 顧客やサポートチームからよくある問い合わせはこれ
  - 行きと戻りで異なる経路を通ることはよくあり対向からのtracerouteも欲しいが手に入らないことも多く、looking glassがあると助かる
    - （そういえばIIJは公開してない…）
  - 相手のNOCに問い合わせてもガン無視されることも多い
    - 特に復旧したあとに問い合せても相手にしてくれない。お国柄?
- 「国内にあるサイトBへpingすると100ms超えて遅いんです」
  - 実は太平洋往復してました、とか
  - 国内で外資Tier 1からtransitを買うと起こりがち。Tier 1のM単価は魅力だが…
  - peering policyやコストの問題から必ずしも解決できるとは限らない

ルーティングインシデント (2/3)

- ルートリーク
  - 外部ASからもらった経路(主にインターネットフルルート)を他のASに広告する
    - 稀にOrigin ASを自分に変える輩も
    - 大半はmis configurationによるものと思われる
  - 正規経路とは異なるAS経由となり、多くは輻輳し通信断に至る
    - Google宛のトラフィックが自社に流れ込むことを想像してみてください
    - 影響範囲が広く、新聞沙汰になることも
  - 現状実装されている技術では根本対応が困難
    - AS-PATHのValidationやASPA(Autonomous System Provider Authorization)は発展途上、特定AS間に限ればPeer Lockも考えられるが誰でも使える手段ではない
    - 各ASがミスせず、Transit ISPは顧客の広告経路に責任を持つのが大事

ルーティングインシデント (3/3)

- 経路ハイジャック
  - あるASが持つ経路のsubnetを別AS Originで広告する
    - longest matchの原則により別ASに通信を奪われる(= ハイジャック)
  - ルートリーク同様、mis configurationが多いが意図を感じるものも…
    - 昨年はロシアのASがAppleの経路をハイジャックしていた
  - ルートリークと異なり影響範囲は限定的だが、それが自社となると当然被害甚大
    - 局所的故、顧客から厳しい指摘に受けることに
  - 対策: RPKIによるOrigin Validation (後述)

ルーティングの監視、トラブルシュート

- トラブルシュート用の情報は常時収集
  - 網内のBGP,IGP経路の記録 (IGPは集めづらいが今はBGP-LSが便利)
  - 商用アプリおよびOSSのbgpdを利用
- ルーティング異常の監視
  - iBGP Full Mesh監視 (SLA計測兼ねてFull Meshでping)
  - bgpdの情報を用いて経路updateをグラフ化しアノマリ検出
  - JPNIC経路奉行、ICT-ISAC BGP-WG Slack (経路ハイジャック等の検知)
  - bgpalerter等のOSS (経路ハイジャックや想定外の経路広報、ROAの監視)
  - 外部で自ASの経路がどう見えているかの把握は重要
- トラブルシュートで使えるツール
  - RIPE RIS、route-views、各ASのlooking glass

ルーティングセキュリティのBCP: MANRS

- Mutually Agreed Norms for Routing Security
- 業態ごとに取るべきアクションが記載されている
  - ISP、CDN/Cloud、IXP、Device Vendor
- ISPの場合
  - 必須: Prevent propagation of incorrect routing information
  - 必須: Facilitate global operational communication and coordination
  - 必須: Facilitate routing information on a global scale – IRR
  - 推奨: Prevent traffic with spoofed source IP addresses – Filtering
  - 推奨: Facilitate routing information on a global scale – RPKI
- IIJは全て対応済み
  - 2015年にJoin

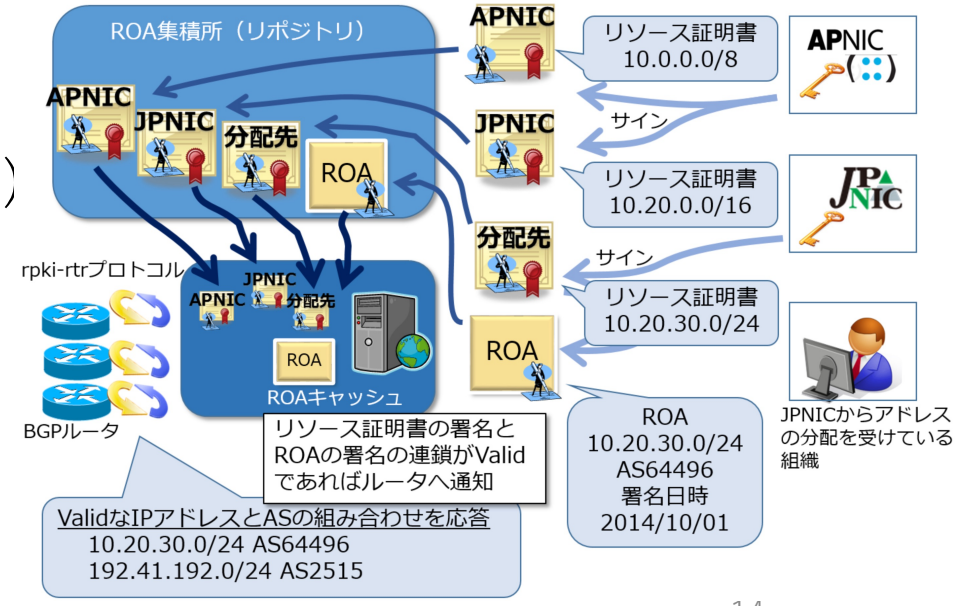
Organization Name	Areas Served	ASNs	Action 1 Filtering	Action 2 Anti-Spoofing	Action 3 Coordination	Action 4 Global Validation
IIJ	JP	2497	✓	✓	✓	✓
Organization Name	Areas Served	ASNs	Action 1 Filtering	Action 2 Anti-Spoofing	Action 3 Coordination	Action 4 Global Validation

IIJの取り組み

- Prevent propagation of incorrect routing information
  - transit customerにはstrictなprefix,as-path filterを実装
- Facilitate global operational communication and coordination
  - peering db他にnocへのcontact pointを記載
- Facilitate routing information on a global scale – IRR
  - 自社アドレスは当然、transit customerにもIRR登録を依頼
- Prevent traffic with spoofed source IP addresses – Filtering
  - customer edgeにSAV(Souce Address Validation)を実装済み (2010年頃?)
  - uRPF or ACL
- Facilitate routing information on a global scale – RPKI
  - 自社アドレスのROA作成済み (2020年)
  - peeringにROVを実装済み (2020年)
  - transit customerへのROVは準備中

RPKI (1/2)

- Resource Public-Key Infrastructure
  - アドレス資源の割り当て、割り振りを証明するための公開鍵基盤
- これをBGP Routingに応用
  - アドレス保有者は事前にアドレスとOrigin ASの組をROA(Route Origin Authorization)としてLIR等のRPKIに登録
  - 外部から経路を受信したBGPルータはROAを参照、経路とOrigin ASの組み合わせが正しいかチェックし不正であれば受信拒否 (ROV:Route Origin Validation)
  - 経路ハイジャックへの効果が期待される技術
- RFC6810として2013年頃に標準化
  - 徐々に各NOSの実装が進み、2010年代後半から各ASが対応 (ref. https://isbgpsafeyet.com/)
  - IIJも2020年に対応



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

RPKI (2/2)

- AS運用者、アドレス保有者がすべきことはたった2つ

1. ROAを作る
   - 難易度低
   - 自社のアドレスを他社のROVで守ってもらう
2. ROVを実装する
   - チョットタイヘン?
   - 自社ネットワークに不正な経路が混入するのを防ぐ
     - → 自社の顧客の通信を守る
   - 自社を経由して不正な経路が伝搬するのを防ぐ
     - → 他社ASの経路を守ってあげる、つまりインターネットの平和を守る

ROAを作る (1/2)

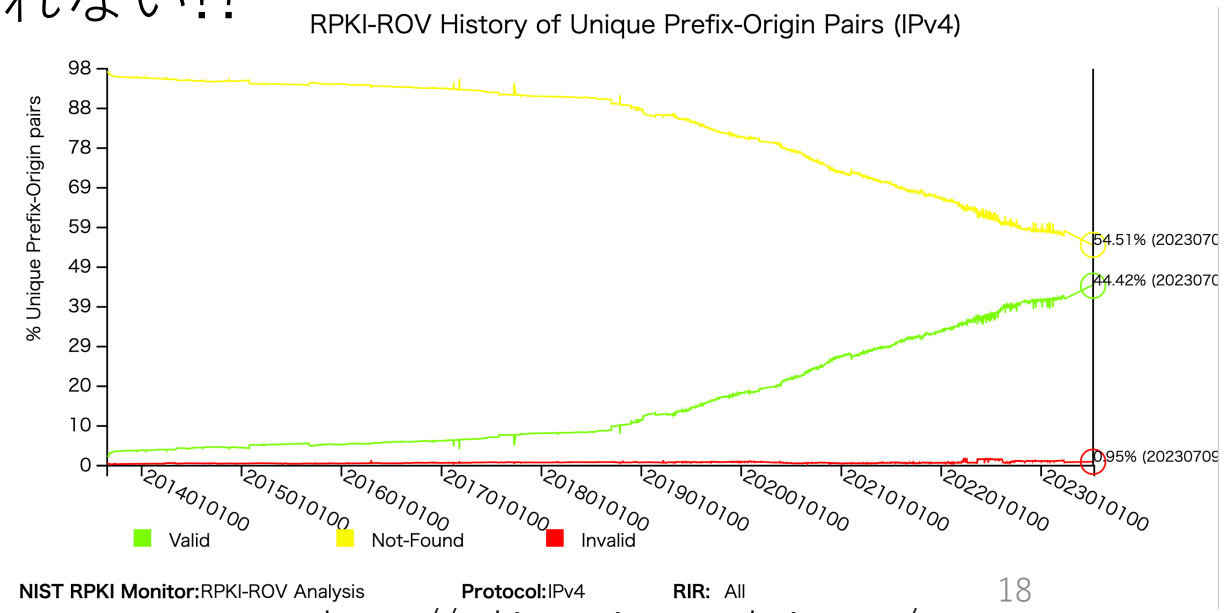
- まずは、自社アドレスの把握
  - 普通はできている?
  - どのアドレスをどの経路長でどのOrigin ASから広告するか(しているか)
  - パンチングホールやsubnetなどの管理がROA作成で唯一のハマりポイント
  - + AS-SETになるケース(confederationやaggregate)
- あとは作るだけ!
  - JPNICがイケてるWebを用意してくれているので簡単かつ安全
  - 自社CAは建てることも可能だが、通常はJPNICシステムで十分 (IIJも利用)
- AS2497 Origin経路も一部を除き登録済み
  - 一部 = パンチングホールおよび顧客がPIアドレスを持ち込みAS2497 originで広告するアドレス
  - 特に後者はROA作成自体顧客でしかできず、かつAS運用していない場合は実感が湧かない話でどこまで理解が得られるか不安

ROAを作る (2/2)

- Max Lengthは使わない or 広告経路のPrefix Lengthと同じがオススメ
  - 他ASではやたらと長くしているケースを散見
    - ハイジャックされたらmore specificで奪い返す想定?
    - もしくは管理をサボりたいから?
  - 今のROVはoriginとprefixの組み合わせでしかvalidationしておらず、むやみにMax Lengthを伸ばすとorigin詐称されハイジャックを許すことに (ref. RFC9319)

ROAの普及状況

- 2019年頃から普及が進み、現在はBGP経路の44%をカバー
- 日本でも導入が盛ん
  - 総務省もサイバーセキュリティの一貫として注視
    (ref. https://www.soumu.go.jp/main_content/000805821.pdf)
- 作ってませんでした、ではもう済まされない!?
  - あなたのネットワークで事が起きてからでは遅い
  - デメリットは皆無。今すぐ作成を!



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

ROVを実装する (1/3)

- やることは主に2つ
  1. キャッシュを建てる
  2. ルータでROVをenableにする

- キャッシュを建てる
  - RIRなどのRPKIリポジトリからROAを取得し内容を検証、VRP(Validate ROA Payload)を作成しルータに提供するのが仕事
  - RoutinatorやFORTなどOSSが充実、品質も十分
    - メンテが停まるものもあるが…
    - IIJではSPoF回避のため異なる実装を複数利用
  - IX等がpublicに公開しているが、自社でも運用自体は十分可能
    - 動作検証をどこまでやるかでハードルが異なる (DNSサーバと同じ感覚?)

ROVを実装する (2/3)

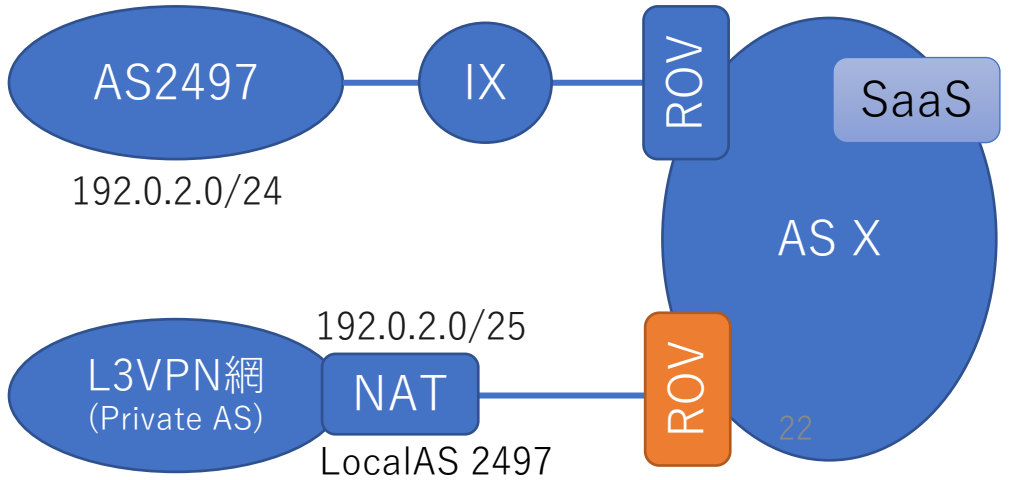
- ルータでROVをenableにする
  - キャッシュとRTRセッションを確立
    - それなりにCPUやメモリへのインパクトがあるので事前検証をオススメ
  - BGP peerやinbound policyにROVを追加する
    - 設定方法自体は難しくはない
    - NOSによってはいくつか手段がある場合も (IOS-XRなど)
    - BGP Origin Validation State Extended Community (RFC8097)の利用で思わぬbest path selectionが発生するので注意
    - 不具合も少なからずあるので当然検証は必要、あとは覚悟と勇気と熱意
  - Metricはあまり充実しておらず監視は難しい
    - ROVによりrejectした経路数をモニタできない場合あり

ROVを実装する (3/3)

- 導入には細心の注意を払った
  - ROV導入当時、rejectすることになるinvalid経路は約3,000経路
    - インターネットフルルート100万経路に対して多いような少ないような…
    - これをこのままサポートチーム等に説明するといたずらに不安を煽るため、これらのアドレスとの通信量を調べるなど、影響は軽微であることを丁寧に説明
  - まずはlocal pref. 0にしてしばらく様子見てからreject
  - 導入後の問い合わせに備えてreject経路を記録
- 導入時、導入後の不具合
  - 特定条件でrouting processがcrash (2つのNOSで引いた😂)
  - AS-SETの扱い (AS-SETの利用は辞めよう! ref. RFC6472)
  - ROAが更新されてもadj-rib-in内の経路が再評価されない
  - BGP Origin Validation State Extended Community (RFC8097)の利用で思わぬbest path selectionが発生

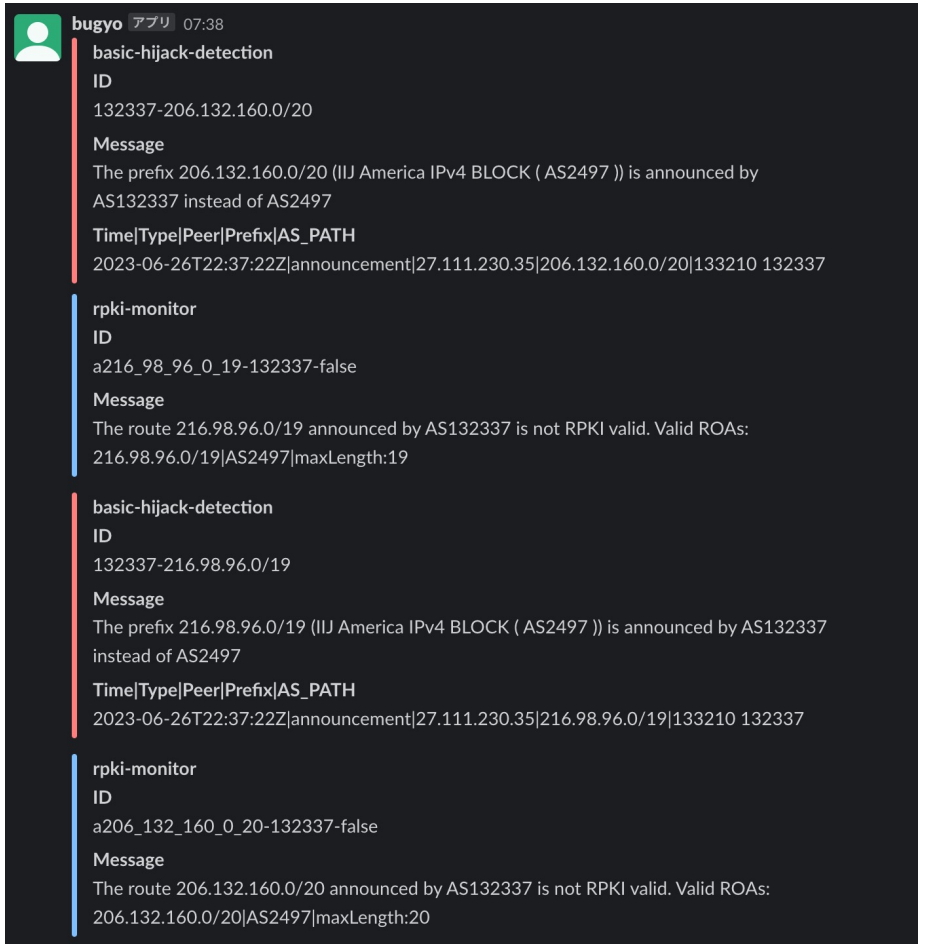
RPKIの思いがけないトラブル

- Public Clouldがインターネットで提供するサービスを専用接続から利用するオプションサービス
  - 特に日本で流行っている(?)
- ROAは192.0.2.0/24 (Origin 2497, MaxLength 24)で作成済み
- バックボーンチームが関与しないサービスネットワークからorigin AS2497でsubnetを広告していた
- ある日、AS Xがこの接続にROVを導入
  - ROAのMax Lengthに反しrejectされ障害に
- 教訓
  - 社外に広告する経路の把握、管理は(当然)大事
  - 旧来のインターネットとは異なる使い方も考慮
  - この場合でもMax Lengthは伸ばさず個別にROAを作るべき (数が多くなると自社CAが欲しくなる)



Don’t worry, I’m wearing… RPKI👍

- つい先日、IIJ US現地法人の2経路(Origin AS2497)をとあるASが勝手に広告したことを検知
  - RIPE RIS等を用いて世界での経路伝搬状況を調べたが限定的だった
  - RPKIが効果を発揮した実例
  - 同様の事象はここ1年だけでも数回発生
- ROVは兎も角、ROAは今すぐ作ろう!



ICT-ISAC Japan BGP-WGのSlack

まとめ

- AS運用においてルーティングインシデントはよくある事象
- 監視しないと気づくこともできない
  - サービス提供者にとって顧客から問い合わせで事象に気づくのは恥
  - 顧客に気づかれる前に察知して対処したい
  - 自網内だけで監視していてもインターネット上のインシデントは把握できない場合も
- ルーティングセキュリティは普段から備えを
  - 今の技術でもやれることは色々ある
  - 先駆者のknow-how、コミュニティのbest practiceを参考に
  - Transit ISPに聞いてみるのもあり (IIJはいつでもwelcome! 契約なくてもどうぞ)
- **各ASの取り組みがインターネットをより良いものにしていくと信じています!**