AS運用と
ルーティングセキュリティ

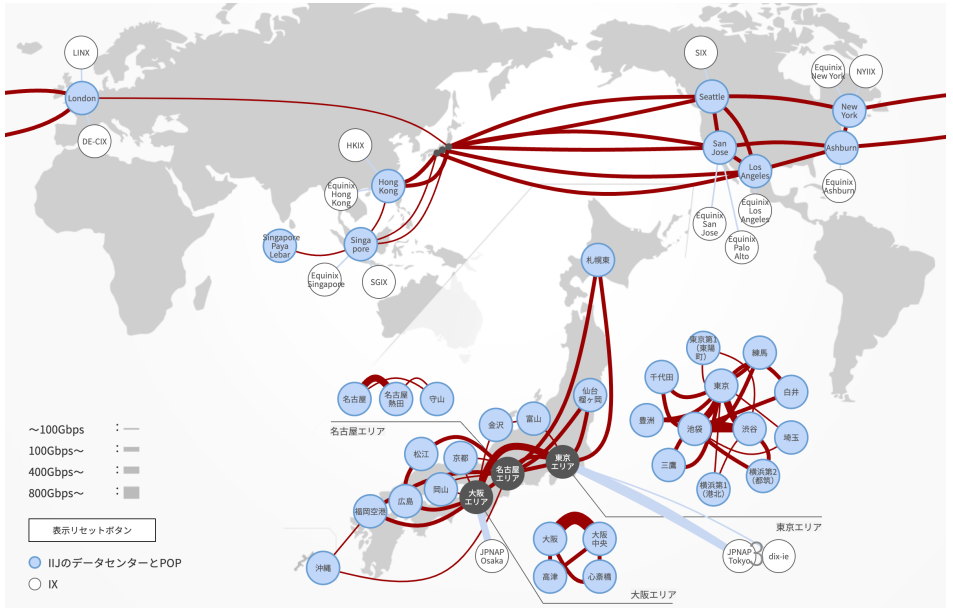
IIJ/AS2497 hori@iij.ad.jp

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
- お仕事: 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)およびインフラ全般の企画

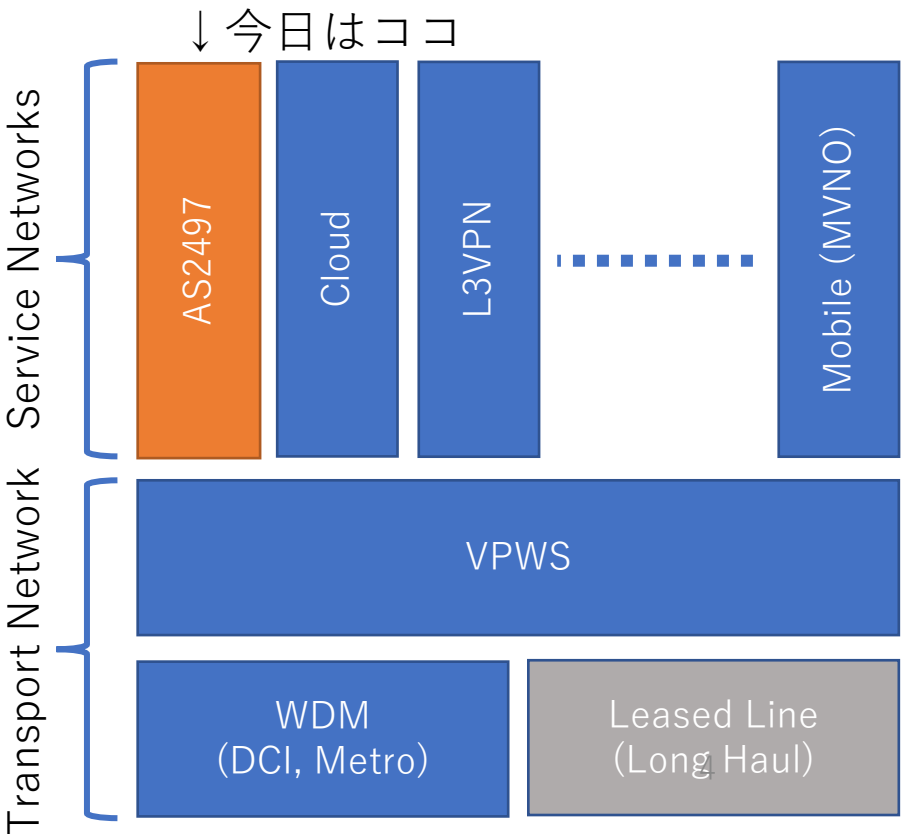
About IIJ

- 古参の商用ISP、今では手広く事業を展開
  - モバイル、クラウド、IoT、ヘルスケア、デジタル通貨など
  - 今年で創業30周年
- 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 + 海外現法のASいくつかを運用



About IIJ Backbone

- VPWSをベース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

- 機器故障、回線障害はどのネットワークでも日常的に発生、
  インターネットの場合はこれに加えて…
- DDoS
  - 以前は顧客宛のDoSが目立っていたが、ここ1,2年は顧客発インターネット宛が多発、Botnetに組み込まれた脆弱な端末発のDoSが数100G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
  - 根本的には顧客に端末の対処をしてもらうしかなく、対応には苦慮
  - ここにいるみなさんも是非お手元の端末の確認を! ISPの方は自社E/Uに責任を!
- Network OS(NOS)の脆弱性
  - 端末とは異なり侵入される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
  - 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…
- 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 (1/2)

- ルーティングインシデントも様々
- 「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の問い合わせは主にこれ
  - 行きと戻りで非対称経路を通ることはよくあるため対向からのtracerouteも欲しいが手に入らないことも
  - 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
- 「国内にあるサイトBへpingすると100ms超えて遅いんです」
  - 国内で外資のTier 1からtransitを買うと起こりがち
  - Tier 1のM単価は魅力だが使い分けは大事
  - 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
  - 実は今話題のSTARLINKからwww.iij.ad.jpにtracerouteすると…

ルーティングインシデント (2/2)

- 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。
    極稀にOrigin ASを自分に変える輩も
  - 正規の経路とは異なるAS経由となり多くは輻輳し通信断に至る。新聞沙汰になることも
  - 多くはmis configurationによるもの
  - 現状実装されている技術では防ぐことが難しい
    - AS-PATHのValidationやASPA(Autonomous System Provider Authorization)は発展途上、現時点では実用的とはいい難い状況
    - 特定AS間ではPeer Lockも
- 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)
  - mis configurationや何からの意図を感じるものまで
    - 数ヶ月前にはロシアのASがAppleの経路をハイジャックしていた
  - 対策: RPKIによるOrigin Validation

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は若干集めづらいが今はBGP-LSの利用も)
  - 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
  - bgpdの情報を用いて経路変動をグラフ化、アノマリを検出
  - JPNIC経路奉行 (経路ハイジャックの検知)
  - ISAC bgp-wg slack (経路ハイジャックやルートリークの検知、情報交換)
  - 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監視は重要
- トラブルシュートで使えるツール
  - RIPE RIS、route-views、各ASのlooking glass

監視で検知した実例

- 2022/4 ドイツのとあるAS yがIIJのアドレス 20弱を不正に広告したことをISAC bgp-wg slack等で検知
  - 見えた経路のAS-PATHは”AS x, AS y”、”経路上”のOriginはAS y
  - AS yの別アップストリームとIIJはPNIしていて、そこでは当該経路は見えていない
  - その他、主要Tier 1のlooking glassでも当該経路は見えていない
  - RIPEのamsterdamノードでだけ経路が見える状況
- OriginではないAS xの挙動が不審だったため問い合わせたところ、すぐに修正したと応答あり
  - 何を間違えたのか、意図した変更だったのか、誰がOriginateしたのか等の詳細に関しては一切言及なし (海外にありがち。顧客への説明に苦慮する)
- 結果的に被害は軽微(もしくはなかった)
  - 今回は不正経路自体が極めて限定的に広告されたようだが、IIJは以前からROAを作っており、仮に広く全世界へ広告されても主要Tier 1が停めてくれと期待できる
  - 教訓: RPKI大事 (後述)

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

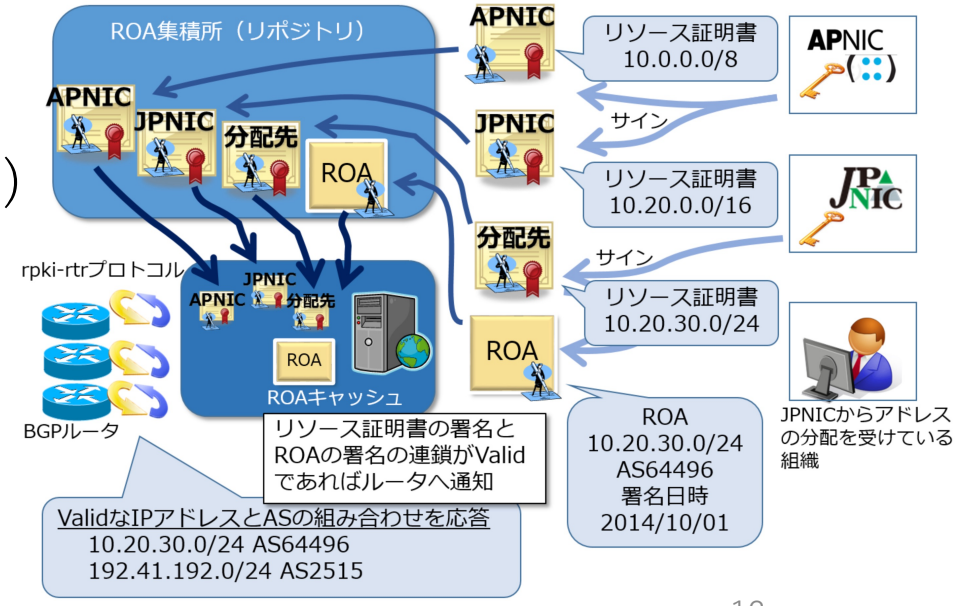
Organization Name	Areas Served	ASNs	Action 1 Filtering	Action 2 Anti-Spoofing	Action 3 Coordination	Action 4 Global Validation
IIJ	JP	2497	✓	✓	✓	✓
Organization Name	Areas Served	ASNs	Action 1 Filtering	Action 2 Anti-Spoofing	Action 3 Coordination	Action 4 Global Validation

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

- 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/ より引用

RPKI: ROA

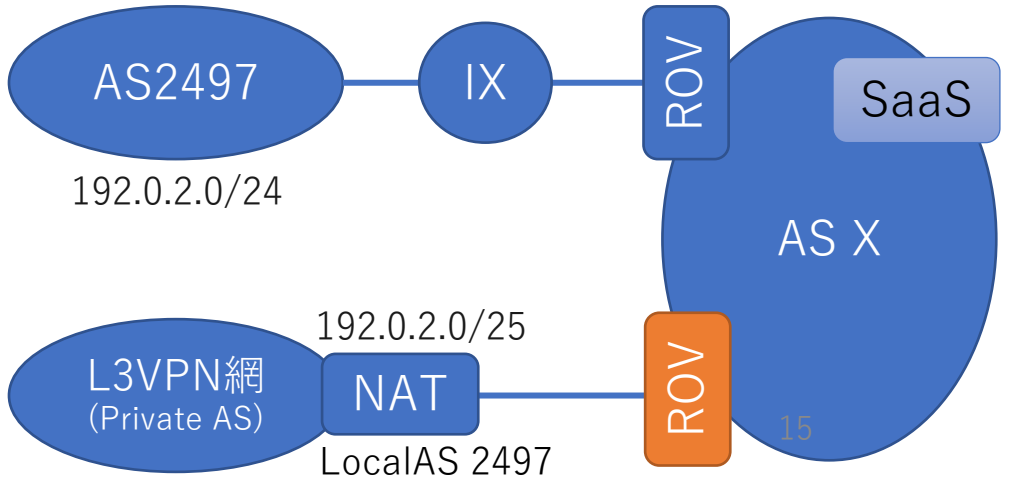
- 自社でCAは建てず、JPNICを利用
  - 現状のIIJでは自社でCA建てるメリットなし
- 登録開始当初はRIR/NIR要因で一部作成できないレンジがあったが徐々に解消
- 顧客がPIアドレスを持ち込みAS2497 originで広告するアドレスはこれから顧客へ依頼
  - IIJでは作成できない
  - AS運用しない人には実感のない話、どこまで理解が得られるかは未知数
- Max Lengthは使わない or 広告経路のPrefix Lengthと同じ
  - 他ASではハイジャックされたときのcountermeasureとしてか、やたらと長くしているケースを散見 (ハイジャックされたらmore specificで奪い返す)
  - 今のROVはoriginとprefixの組み合わせでしかvalidationしていない
  - むやみにMax Lengthを伸ばすと逆にorigin詐称されたsubnetでハイジャックを許すことに (ref. RFC9319)

RPKI: ROV

- 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に関連する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)



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
- **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!**