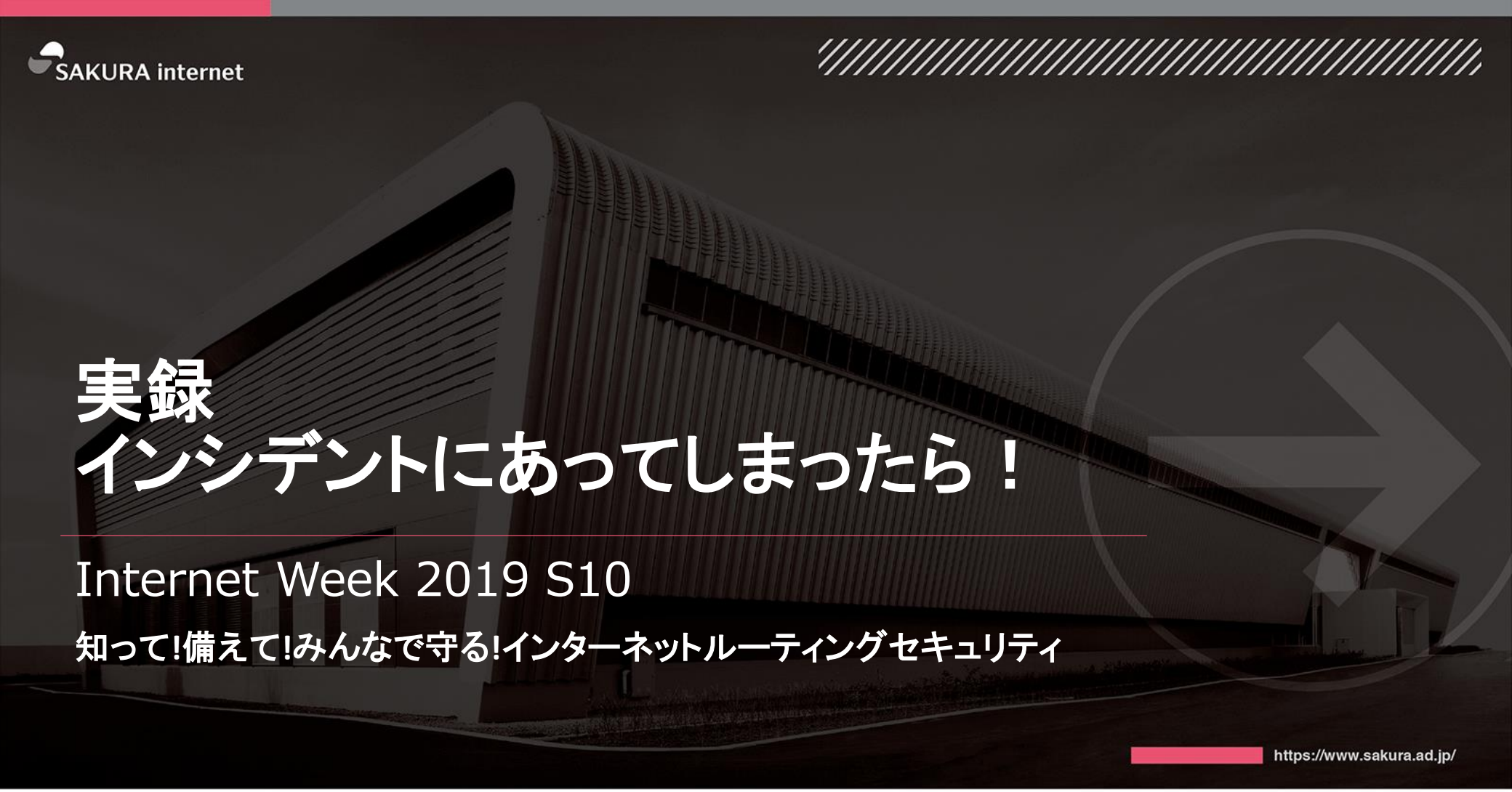


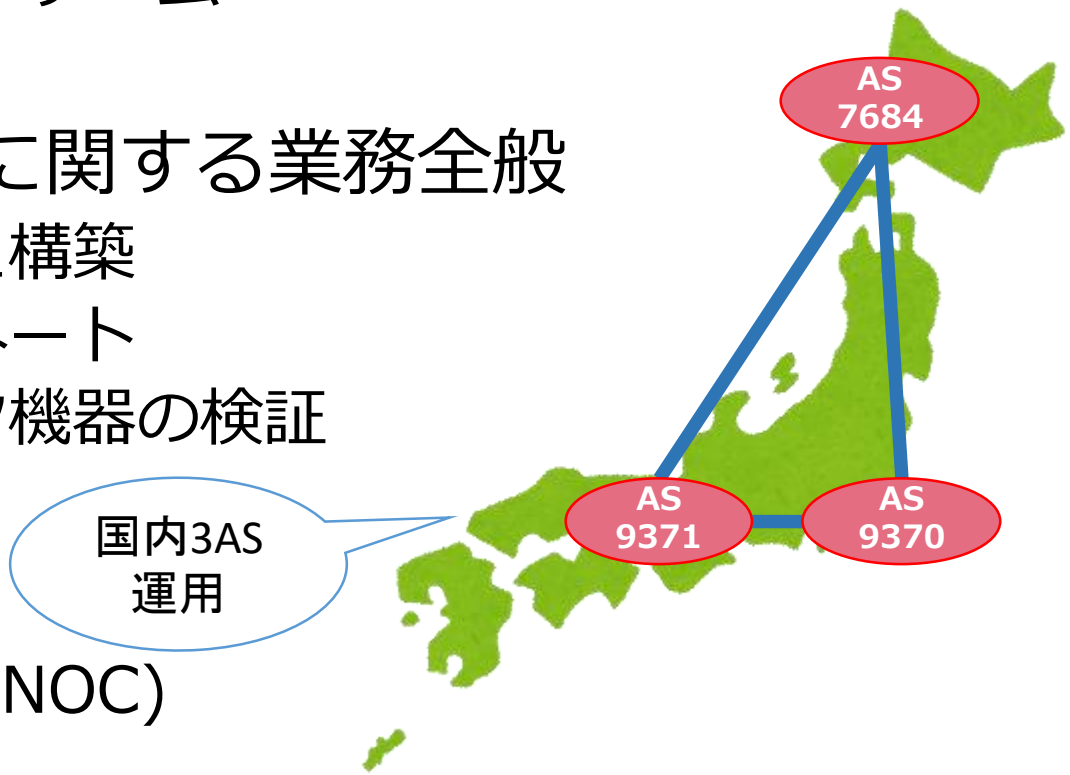
DAY	COMPANY	DEPARTMENT	NAME
2019/11/26	さくらインターネット株式会社	技術本部	山口　勝司

- 名前：山口　勝司（やまぐち　かつし）

- 所属：さくらインターネット株式会社
  - 2016年入社（BGPに関わって6年程）
  - 技術本部 バックボーンチーム

- 業務：自社ASの運用に関する業務全般
  - ネットワークの設計と構築
  - ピアリングコーディネート
  - 新技術やネットワーク機器の検証

- その他
  - AS59105 (AS-HOMENOC)



1. はじめに

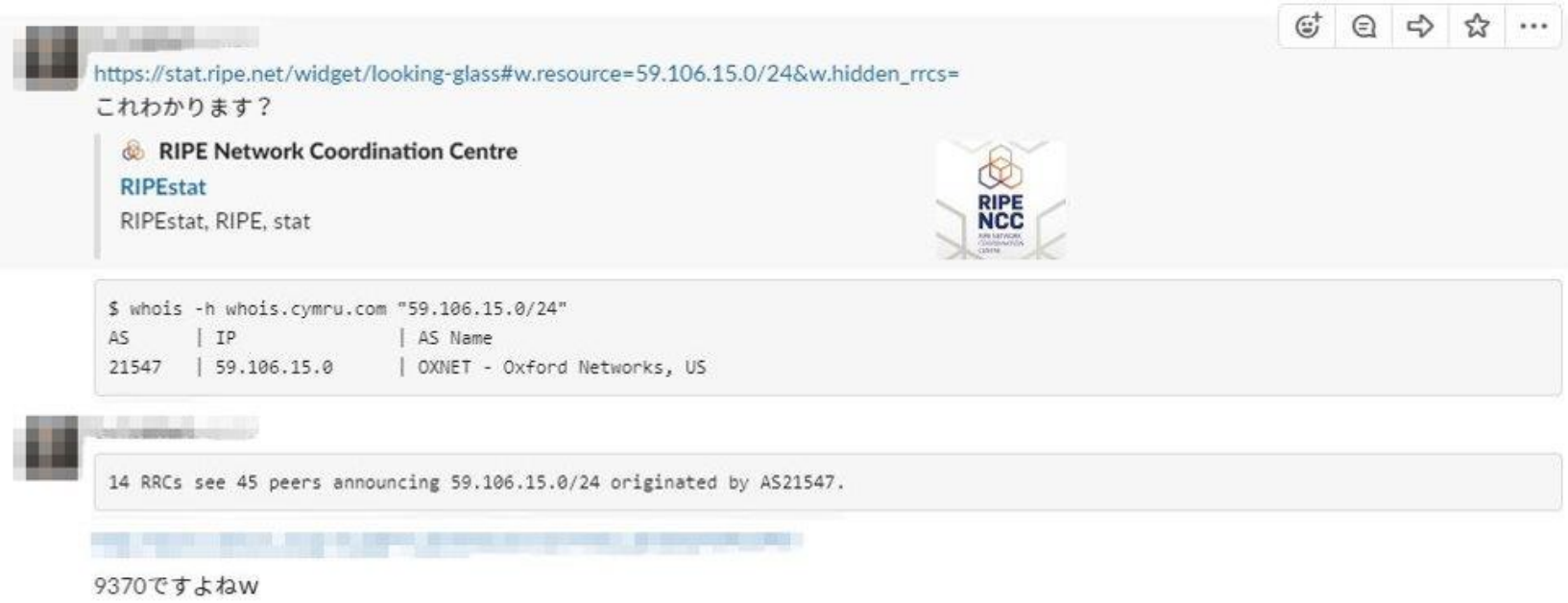
- BGPでの経路広報
  - プロトコルの仕様上どんなIPアドレスでも広報できる
    - 設定ミスや悪意による不正な経路が広報される事故が毎年発生
  - 自分が広報した経路がどう使われるかは相手次第
    - 意図せず遠回りになったり、品質の悪いルートを通っていたり

- 2019年に起きた主なトラブル
  - VerizonとBGPオプティマイザを原因とする経路障害
    - https://blog.cloudflare.com/jp/how-verizon-and-a-bgp-optimizer-knocked-large-parts-of-the-internet-offline-today-jp/
  - スイスの事業者が経路をリークし中国経由で伝搬
    - https://www.gizmodo.jp/2019/06/china-telecom-swallows-huge-amount-of-european-traffic.html

経路ハイジャックだけではなく「経路リーク」の事例が目立った

2. 実際にあった経路ハイジャックの話

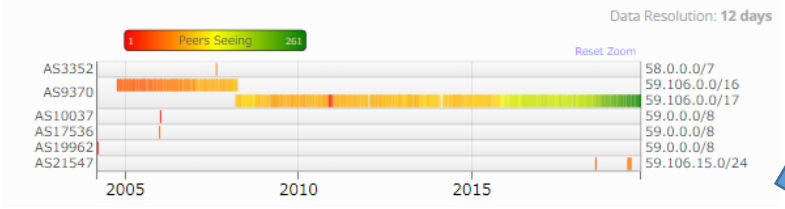
- はじまりはSlackメッセージ
  - 2019年7月末日Slackでダイレクトメッセージが届いた



59.106.0.0/17（弊社AS9370広報）に含まれる
59.106.15.0/24 が AS21547 から広報されているみたい？？

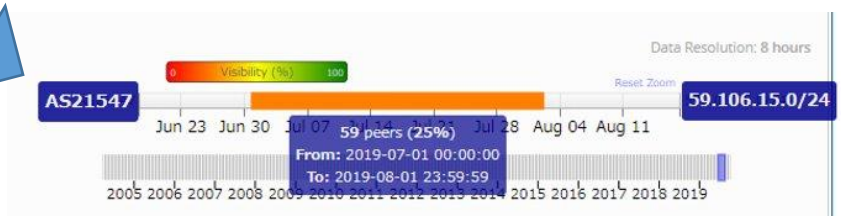
- 59.106.15.0/24
  - 弊社サービス提供用として利用していたアドレス
  - 経路ハイジャックされた時点では利用していなかった
    - 結果として**お客様に影響はなかった**
  - 東京地区ネットワーク（AS9370）で分割利用
    - JPNICから59.106.0.0/16として割り振りを受ける
    - 59.106.0.0/17としてインターネットに広報
    - JPIRR・RADBにOrigin AS9370として登録
  - 1年前も**同経路の同ASからの経路ハイジャック**が発生
    - その際は問い合わせに返信も無かったが自然収束していた

- RIPE Statを使った調査
  - IPアドレスを入力して「Routing」>「RoutingHistory」

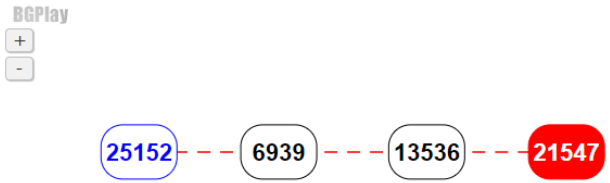


1年前にもハイジャックされている
（この時は連絡するも返信がなく自然終息）

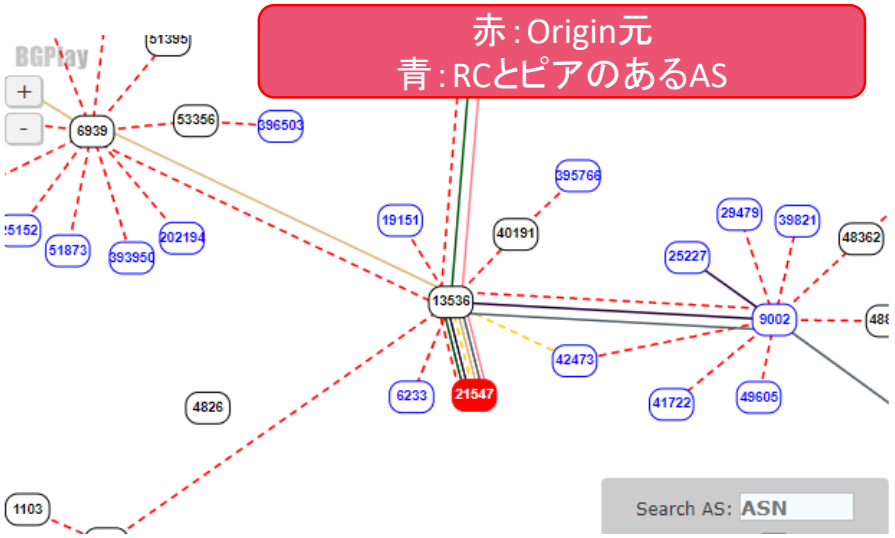
約一カ月間ハイジャックされていた



- 「Routing」 > 「BGPlay」で期間とRCを指定
  - AS21547からAS13536を経由して伝搬している
  - 参照するRCを変えると色々分かる

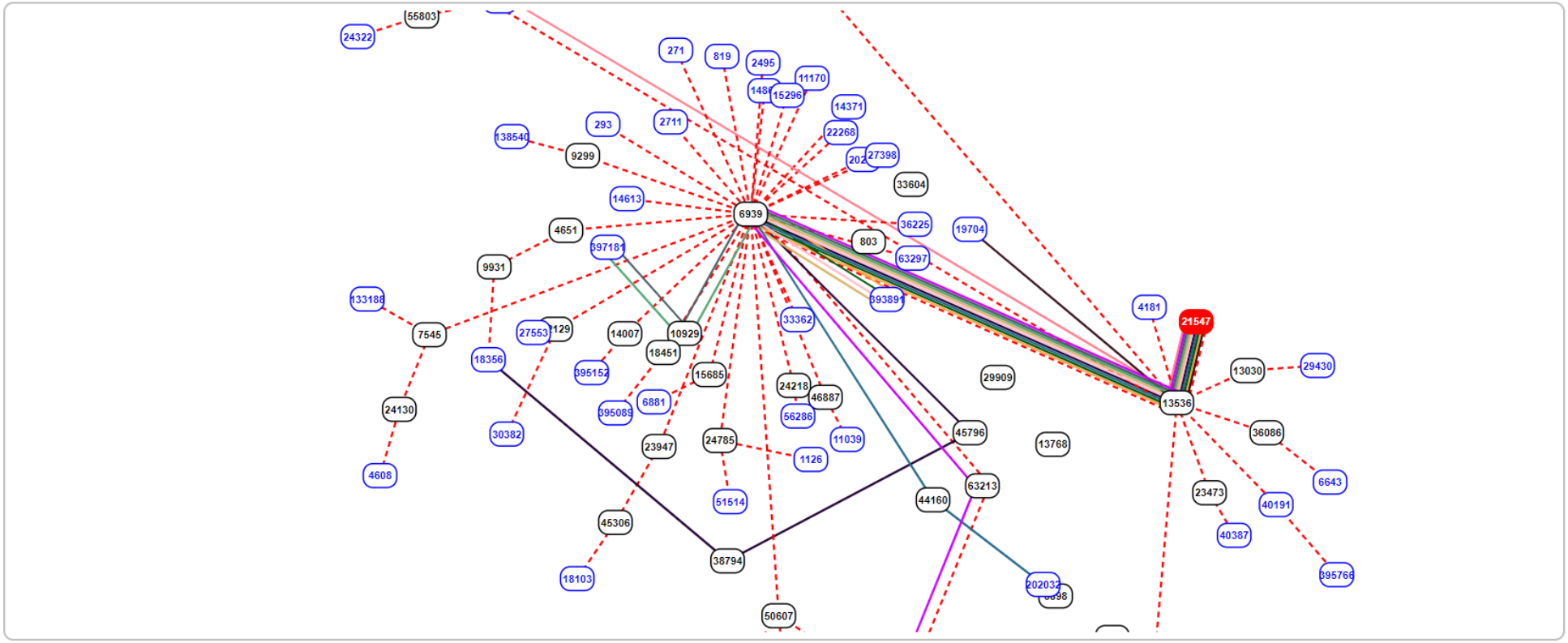


赤：Origin元
青：RCとピアのあるAS



日本（大手町）RCではAS25152で観測

- BGPMon（bgpstream.com）
  - https://bgpstream.com/event/210236
  - BGPMonにもPossible BGP hijackとして掲載されていた
  - RIPEと同様に**経路変動を可視化された情報**が提供される



- 国内には問題の経路は殆ど入ってこなかった
  - 国内主要トランジッターでは経路を観測できなかった
    - IIJとGINのLookingGlassで確認
  - 経路奉行からもアラートメールは発信されていない
  - 北米では他の地域より多くのASで観測できていた
    - NewYork(RC11),PaloAlto(RC14),Maiami(RC16)

- このような観測結果になった原因は分からない
  - 日本は厳格なPrefixフィルタをしているASが多いから？
  - さらに詳しく調べることもできそうだが実施していない

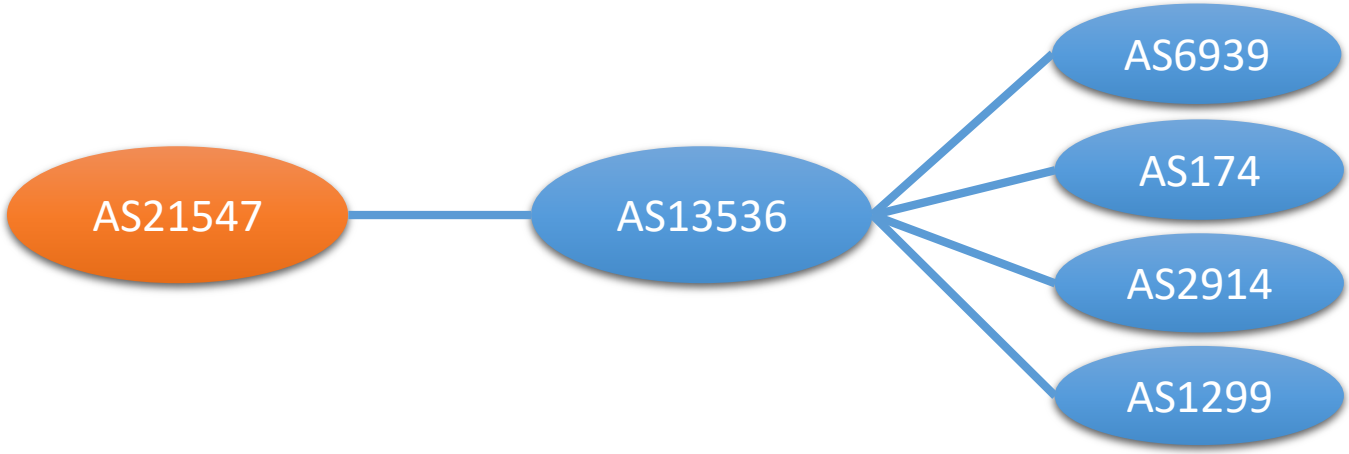
運用者として重要なことは経路の広報停止とお客様への回答（の材料）にできること

- 広報元の**AS21547**に連絡する
  - PeeringDB
    - 連絡先の記載がなかった（連絡先以外も多くが非公開）
    - 昨年ハイジャックの被害を受けたときは記載があった
  - IRR（aut-num Object）
    - notify,changedには他組織（Upstream AS13536）の連絡先
    - AS13536のサービス名と企業名と思われるドメインのアドレス
  - Whois
    - tech,noc,abuseには他組織（Upstream AS13536 ）の連絡先

Upstream AS （SIer？）に運用まで委託しているようなケース？？
昨年のアドレス＋上流のAbuseとNOC(サービス名と思われるドメイン)宛にメール
同日はこれで様子見することに

- 約24時間経過後も返信は無かった
  - JPNICの岡田さんに相談してアドバイスを貰う

- 連絡先を変えて**AS13536**に連絡
  - PeeringDBのnoc,peering+IPアドレスの管理者の連絡先
    - 色々なメールアドレスを巻き込んでメールを送った
  - 少し厳しめの表現でメールしてみた
    - その広報は許可していないから直ぐに止めるように！
    - 昨年も発生しているので原因と対応を報告して！



- 迅速に対応してもらえた
  - 2019/08/01 15:30 広報停止を依頼
  - 2019/08/01 21:00 謝罪のメールを受信
  - 2019/08/02 出勤時 経路広報停止を確認

- 原因は回答してくれなかった
  - 意図的？設定ミス？
  - なぜ過去に同一の経路ハイジャックが起きたのか？
  - 再発しないように対策したのか？

3. 運用者から見た経路ハイジャック対応

- 経路ハイジャックの発生に気付けなかった
  - 経路奉行のアラートメールで対応を行う社内手順はあった
  - 国内経路を元にしているサービスのため検知しなかった
  - 国内での経路情報のコレクタは経路奉行の方が多い

海外の局所的なハイジャックにも対応できるシステムと経路奉行の併用が必要

- 他の経路状態の監視サービス
  - 無償のものは機能や検知速度が不十分だったり…
  - 有償のものは利用料が高価だったり…

検知ツールを自前で用意することにした

• 主な経路監視サービス（有償サービス）

	ThousandEyes	BGPMon	Radar by Qrator
概要	統合監視システム 一機能として経路監視の仕組みを持っておりBGPの監視にも力を入れている。 自社内に監視VMを置いて品質監視もで、ルートリークの検出も可能。	Ciscoに買収され 「CrossworkNetwork Insights」の一部となった。	ロシア企業のサービス 一部機能が無料で利用可能 eBGP接続することで詳細な解析可能 ルートリークやDDoSなどのセキュリティ監視の機能もある
経路ソース	独自	RIPE RIS	独自？
価格	有償	有償（一部無料）	有償（一部無料）
通知	メール/Web	Web/メール	Web/メール

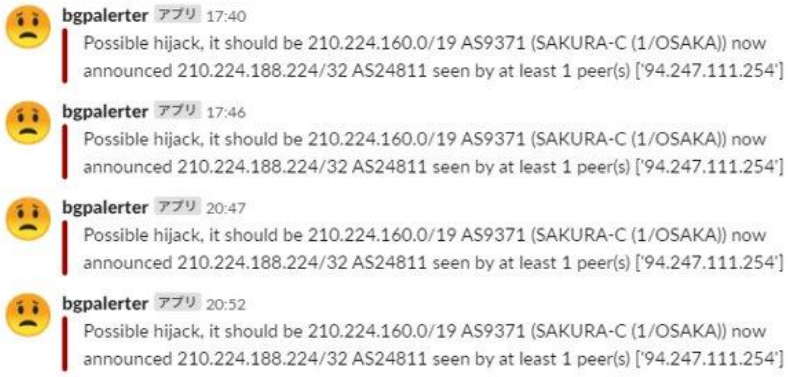
有償のものを含めると選択肢は比較的多いと思われる

- RIS Live (RIPE NCC)
  - https://ris-live.ripe.net/
  - BGPアップデートのライブフィード
  - 世界中25ヶ所にあるRIPEのRoute Collectorから情報収集
  - WebSocket JSON APIでストリーム配信

- Bgpalerter (NLNOG)
  - https://github.com/NLNOG/bgpalerter
  - PrefixとASの組合わせをリアルタイムで監視するスクリプト
  - 弊社にて不具合修正と機能をカスタマイズしたものを利用
    - https://github.com/tamihiro/bgpalerter/tree/br01
  - NLNOGのコミッタらしき人がNTTに移籍したようで書き直されたものが最新版として提供されている
    - https://github.com/nttgin/BGPalerter

- 監視対象
  - RADBに登録された弊社OriginのRoute Objectが対象
    - 将来的にはRPKI（ROA）ベースの監視を検討
  - CronjobでRADBから毎日1回取得する

- Slackへの通知
  - 経路ハイジャックのアップデートを受信した場合
    - RIPEのRCの最低1RC以上、最低1ピアからの受信
  - 同一経路についてwithdrawnを受信した場合
    - RIPEのRCの最低1RC以上、最低10ピアからの受信
  - 事象が継続した際は2分間隔で5回アラート発報



• 監視ツールの効果（ハイジャックと思われる事象）

発生日	広報元	国	被ハイジャック経路	継続時間	検知RC
2019/9/8	AS24811	RU	1経路	約60分	RC00（Amsterdam, Netherlands）
2019/9/13	AS24811	RU	1経路	約60分	RC00（Amsterdam, Netherlands）
2019/10/5	AS24811	RU	1経路	約60分	RC00（Amsterdam, Netherlands）
2019/10/8	AS24811	RU	1経路	約60分	RC00（Amsterdam, Netherlands）
2019/10/16	AS41497	IT	34経路	約80分	RC10（Milan, Italy）
2019/11/12	AS24811	RU	1経路	約60分	RC00（Amsterdam, Netherlands）
2019/11/11	AS24811	RU	1経路	約60分	RC00（Amsterdam, Netherlands）
2019/11/19	AS24811	RU	1経路	-	RC00（Amsterdam, Netherlands）

※1. AS24811：ピア？のAS49673を経由してRC00で検知

※2. AS41497：上流のAS6762を経由してRC10で検知

検知ツールは一定の効果を発揮

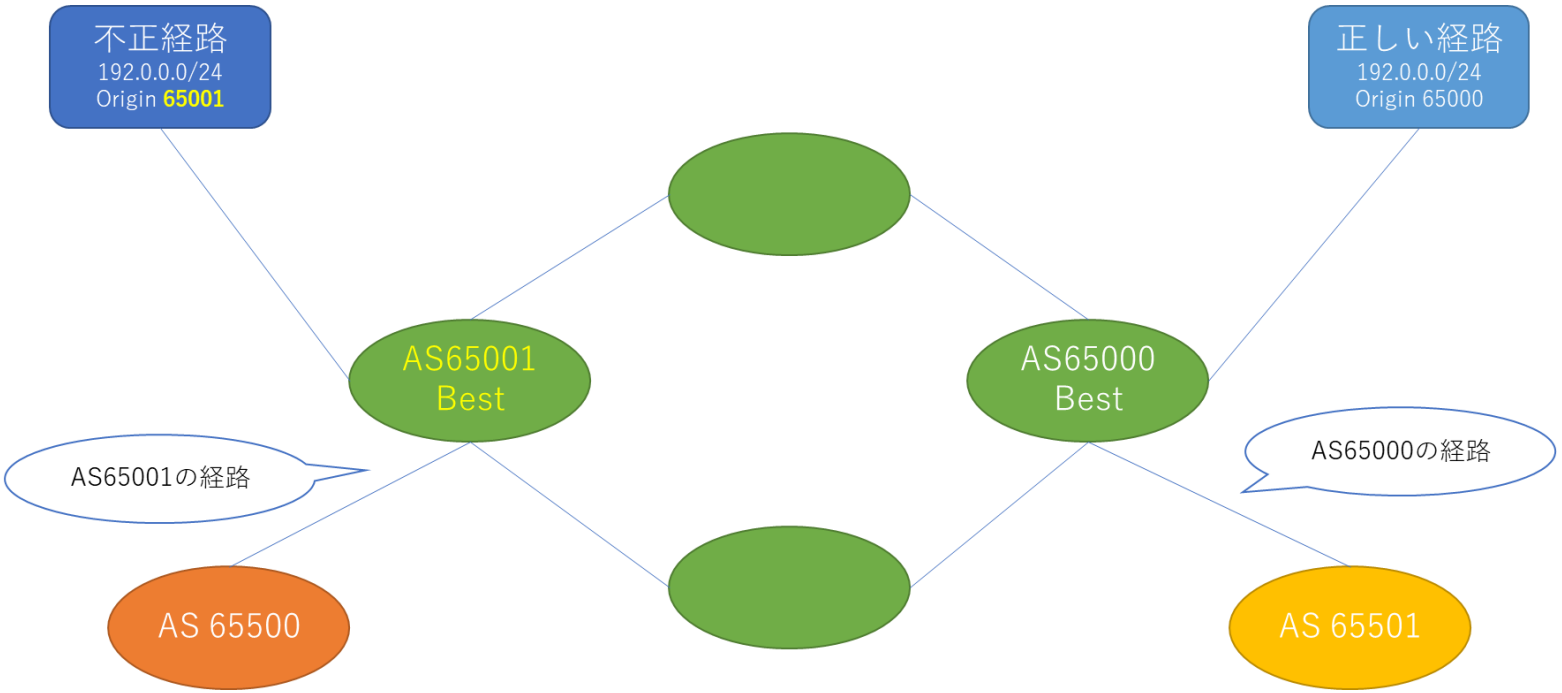
局所的な経路ハイジャックは比較的頻繁に発生している

- 同一のASによる被害が多い
  - 冒頭の事例のAS21547は2回目
  - AS24811は月に1-2回ペースで複数回発生
- 世界的には伝搬せず局所的な影響
  - 特定のピアに対して広報しているから？
  - IRRや申告ベースでPrefixフィルタが機能しているから？
  - no-exportがついているから？
- 故意なのか事故なのかは不明
  - ただし、同じPrefixの被害が繰り返される傾向はある

- RIPE Stat
  - https://stat.ripe.net/
  - 世界25ヶ所のRCが250ピアから経路情報
  - AS番号やIPアドレス情報をもとにWebから様々なデータが確認できる
- RIPE RIS
  - https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris
  - MRT形式でルーティングテーブルの情報を公開している
  - 初期調査というより詳細の解析向け
- bgpstream
  - https://bgpstream.com/　(Twitter：@bgpstream)
  - ルーティングトラブルについてWebやTwitterで情報発信
  - 情報が整理されてまとまっているがリアルタイム性は低い

この3つのツールを抑えておけば対応できそう

- 監視ツールの検知結果は絶対ではない
  - 経路コレクタのあるポイントでの情報にすぎない
  - 経路異常を検知した隣のASでは影響は無かったかも？
- 同じAS内でも影響の有無が異なることもある
  - 同一Prefix長でハイジャックされた場合などが一例
  - 地域によってBestPathと判断される経路が違うかも



- 広報元への問い合わせ
  - IRR、Whois、PeeringDB
  - 情報が古かったり見落とされる可能性がある
  - できるだけ多くの宛先を巻き込んでメールする

- 広報元ASからの反応が無ければ
  - 広報元の上流ASを探して聞いてみる
  - 契約関係がある場合が多いので対応してもらえるかも
  - ピア経由で広報されてる場合は隣のASやIXPなど

- 電話
  - 経路ハイジャックでは無いが疎通トラブルでは経験がある
  - チケット番号があるか聞いてあるなら貰っておく

- コミュニティの助けを借りる
  - Network Operators Group (NOG)
    - NANOG (North American Network Operators' Group)
    - ルーティングトラブルの質問メールが良く飛んでいる
    - 購読人数が多いMLなので必要なら予め上長に相談
  - 経路制御に詳しい人に聞いてみる
    - ICT-ISAC、BGPWG、JANOG
    - JPNIC、APNIC
    - コミュニティで良く名前を見かける詳しそうな人
    - 解決できたり有益な情報を提供してくれたりする

- 広報が止まらず影響が出ている時に有効
  - Longerな経路を広報してLongest Matchで奪い返す
  - IPv4は/23、IPv6は/47より短いPrefixで被害を受けた場合
- 上流ASがExact Matchでしか経路を受けない場合
  - フィルタ開放をしてもらう必要がある
  - 予め上流ASのフィルタの仕様を確認しておく
- 非広報にするアドレス
  - RPKIでOrigin0のROAを登録しておく
- 利用していないアドレス
  - IRRに登録し可能な限り経路広報をしておく

- 経路ハイジャックは珍しいことではない
  - 経路が局所的に伝搬するケースもある
  - 各ツールの特徴を把握し検出する仕組みの準備を
  - 発生したときの対応方法を理解しておく

- 広報停止依頼の宛先は多くのアドレスを巻き込んで
  - 広報元ASがダメなら上流に問い合わせ
  - コミュニティの力を借りることも検討する

- 運用者として取り組みたいこと
  - Whois,IRR などは最新の情報にアップデートしておく
  - RPKIなど新たな技術の導入の検討
  - 運用者間での情報の共有
  - 経路リークの検出方法の検討

これらをオペレータが対応できるように業務手順として整備しておきましょう

SAKURA internet

AS番号	プリフィックス	状態
9370	27.133.128.0/19	VALID
9370	27.133.247.0/24	VALID
9370	27.133.252.0/22	VALID
9370	27.134.240.0/20	VALID
9370	36.53.0.0/17	VALID
9370	36.53.128.0/18	VALID
9370	59.106.0.0/17	VALID
9370	59.106.128.0/18	VALID
9370	59.106.192.0/19	VALID
9370	59.106.224.0/20	VALID
9370	59.106.240.0/22	VALID
9370	61.211.224.0/20	VALID
9370	61.211.236.0/24	VALID
9370	103.57.4.0/22	UNKNOWN
9370	[illegible]	UNKNOWN
9370	110.44.128.0/20	VALID
9370	110.232.160.0/21	VALID
9370	110.232.168.0/21	VALID
9370	112.109.0.0/20	VALID
9370	113.20.160.0/19	VALID
9370	122.202.96.0/19	VALID
9370	153.121.0.0/19	VALID
9370	153.121.32.0/19	VALID
9370	153.121.64.0/19	VALID
9370	153.125.224.0/20	VALID

AS番号	プリフィックス	状態
7684	49.212.65.0/24	VALID
7684	49.212.66.0/24	VALID
7684	49.212.72.0/24	VALID
7684	49.212.73.0/24	VALID
7684	49.212.75.0/24	VALID
7684	49.212.78.0/24	VALID
7684	49.212.116.0/24	VALID
7684	49.212.120.0/24	VALID
7684	49.212.121.0/24	VALID
7684	49.212.168.0/24	VALID
7684	49.212.215.0/24	VALID
7684	[illegible]	VALID
7684	112.78.202.0/24	VALID
7684	112.78.203.0/24	VALID
7684	[illegible]	VALID
7684	112.78.212.0/24	VALID
7684	133.125.0.0/16	UNKNOWN
7684	133.242.0.0/16	UNKNOWN
7684	153.120.0.0/17	VALID
7684	153.120.128.0/18	VALID
7684	153.121.128.0/18	VALID
7684	153.125.128.0/18	VALID
7684	153.126.0.0/17	VALID
7684	153.126.128.0/17	VALID
7684	153.127.0.0/17	VALID

2019年9月末までに自社Originの殆どのPrefixでROAの作成を完了

- ROAの発行での弊社ならではの苦労話（IRS31発表）
  - https://speakerdeck.com/ktyamaguchi/jing-lu-haiziyatukutoroafalsehua

- 2019年8月にMANRSに参加
  - 最近はピアリング先にMANRS参加を推奨しているASも

SAKURA internet Inc. Website

https://www.sakura.ad.jp/

Areas Served: JP

ASNs

9370 9371 7684

Implementation of MANRS Actions

- ✓ **Action 1: Prevent propagation of incorrect routing information**
- ✓ **Action 3: Facilitate global operational communication and coordination between network operators**
- ✓ **Action 4: Facilitate validation of routing information on a global scale**