JPOPM43

割り当て後のIPアドレスを運用してみた

2022/11/22

株式会社インターネットイニシアティブ
蓬田 裕一 Yuichi Yomogita
y-yomogita@iij.ad.jp

経歴

- 蓬田 裕一 (よもぎた ゆういち)
- 2008-2014 IIJ
  - トランジットサービス運用
  - バックボーン運用
- 2015-2019 JPNAP
  - IXサービスの運営・設計・構築・運用
- 2019- IIJ
  - バックボーン企画・設計・構築・運用
  - Peeringマネージャー

本日の発表

- IPアドレスの割り当てから実際に利用するまでの手順、インターネットへ経路広告する際のポリシーや気をつけているポイント、IPアドレスの管理手法等を共有します
- IIJバックボーンネットワークでの運用の状況と合わせてご紹介します

バックボーン

- 日々の構築・運用業務
  - 機器オペレーションや障害対応
  - 運用フローの構築
- バックボーンネットワーク
  - 新機種選定、検証、新機能導入
  - インターネット接続系サービス設備の運営
  - SDN基盤の立ち上げとサービス設備の運営

対外対応

- Peering戦略検討と交渉
  - 顧客、ニーズを意識した戦略を検討
- 社外交渉
  - Peering以外にも、海外回線調達、海外機器の保守事業者選定
- 社外コラボレーション
  - 他社とのサービス協業の検討

- **私のIPアドレスへの関わり方**
  - IIJのバックボーン部門
    - IIJに割り振りを受けたアドレスをインフラ利用で割り当ててもらう
    - IIJのサービスで利用するIPアドレスをインターネットへ広告する
    - IIJバックボーン内のIPアドレスやルーティングを設定、管理する

- **IIJはJPNICのIPアドレス管理指定事業者です**
  - IIJではLIR(Local Internet Registry)の役割を果たすチームがあります
    - アサインメントウィンドウサイズ: 32C(/19)
    - IIJ保有のIPアドレス管理
    - IIJのサービスインフラや顧客へIPアドレスの割り当てを実施
      - IPアドレス利用申請に応じて割り当てを実施する

    - IIJに割り振られた新規のIPアドレスをIIJで利用するために経路の広告をバックボーン部門へ依頼

- **新規IPアドレス利用の流れ (主にIIJバックボーン運用者視点)**
  1. IPアドレスの申請(必要な部署 ⇔ LIR ⇔ RIR/NIR)
  2. 割り当てられたIPアドレスの管理
  3. RADB,JPIRRなどのIRRへrouteオブジェクトを追加/ RPKI ROAを追加
  4. 対外組織の経路フィルタ更新
  5. 各種prefix-list(inbound/outbound)の更新
  6. インターネットへIPアドレスを広告

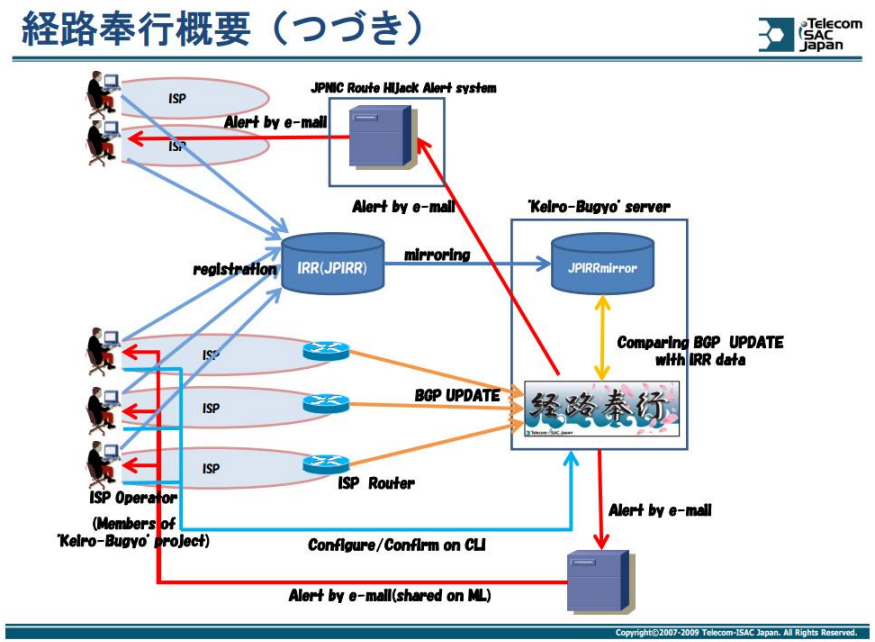
- **IIJ社内でのIPアドレスの割り当て申請**
  - 先程のKDDI森川さんのお話はLIR/NIRからのアドレス割り振り/割り当ての話でした
  - サービス設備でIPアドレスを利用したい、お客様へIPアドレスを割り当てたいときはIIJのLIRへ申請を実施する
    - JPNICのポリシーに従った運営: https://www.nic.ad.jp/ja/ip/application-procedure/
    - 申請者からLIRへIPアドレス申請を実施、承認の後にIPアドレス割り当て
      - お客様のアドレスもサービス契約時にIPアドレス申請書を取得して申請
      - ネットワーク利用計画も厳密に記載する
      - IIJのアサインメントウィンドウを超えたサイズはJPNIC審議
  - 割り当て完了後はwhoisへ登録される

```
Network Information: [ネットワーク情報]
a. [IPネットワークアドレス]     58.138.97.0/24
b. [ネットワーク名]              IIJNET
f. [組織名]                      IIJ インターネット
g. [Organization]                IIJ Internet
m. [管理者連絡窓口]              JP00010080
n. [技術連絡担当者]              JP00010080
o. [Abuse]
p. [ネームサーバ]                dns0.iij.ad.jp
p. [ネームサーバ]                dns1.iij.ad.jp
[割当年月日]                     2008/05/19
[返却年月日]
[最終更新]                       2008/05/19 14:05:06(JST)

上位情報
----------
株式会社インターネットイニシアティブ (Internet Initiative Japan Inc.)
                    [割り振り]                                  58.138.0.0/17

下位情報
----------
該当するデータがありません。
```

- **みなさん、IPアドレスはどうやって管理していますか？**
- **IIJのCIDR管理はテキストです**
  - iij-cidr.txt
    - 各種システムと連携されている重要なファイル
    - 参照用DNSのフィルタが開放されたり、顧客の構成管理ツールと連携したり、・・・
    - もっと使いやすくしたいお気持ちはあり
      - 最近だとROAの発行有無とか管理したい、が…
- **バックボーンインフラでのアドレス管理**
  - 各サービス設備の利用形態毎に確保されたIPアドレス空間を事前準備
  - こちらも管理はテキスト (あくまでIIJバックボーンインフラのお話)
    - 過去から脈々と受け継がれており、version管理は… RCS!
  - 担当者が要望に応じて取得し、利用
    - 管理ファイル(ここがMaster)、現状のconfigで利用していない(重複チェック)、DNSが登録されていない(利用中は必ずDNS登録する)
    - もちろん最大限の完全性で管理される
      - 利用開始/利用変更/利用終了、頑張りましょう。みんなの努力

- **IRR(Internet Routing Registry)への登録**
  - 割り当て済みなのでwhoisの情報を正にしてIPアドレス情報を確認
    - 間違ったIPアドレスを登録しないように気をつける
  - IIJではRADbとJPIRRへ登録
    - IRR登録の意義はIPアドレス/ルーティング情報の正当性の確保
    - IRRを利用して受信経路フィルタを実施しているASへの対応
    - IRR冗長と参照範囲を期待して、日本国内と世界的に利用されているIRRへ登録を実施
    - 登録作業はバックボーン運用者で実施する
    - 顧客の持ち込みPIアドレス(IIJ/AS2497 Originated route)も代行登録する
  - IRRでのミラーリング
    - IRR間でRouteオブジェクトの登録情報は共有されている
    - JPIRRもRADBも複数のIRRとミラーリングを実施
      - RADb: Mirrors the data of more than 30 other IRR databases
      - JPIRR: https://www.nic.ad.jp/doc/jpnic-01234.html
    - RADb/JPIRRを参照していないASでも正しくデータベース情報が利用できる

- **経路奉行での監視登録**
  - JPIRRにRouteオブジェクトとして登録されたprefix/originの組み合わせと経路奉行メンバから提供されたBGP UPDATE を比較
    - オブジェクトの‘descr:’属性へ X-Keiro: メールアドレスを登録
    - ルートオブジェクト毎に登録する or メンテナーオブジェクトに登録
    - 既にメンテナーオブジェクトに登録されていれば個別対応は不要
    - https://www.nic.ad.jp/ja/ip/irr/jpnic-keirobugyou.html




```
y-yomogita@y-yomogita-ice:~$ whois -h jpirr.nic.ad.jp MAINT-AS2497
mntner:      MAINT-AS2497
descr:       People authorized to make changes for AS2497
             X-Keiro: noc@iij.ad.jp
admin-c:     Junichi Shimagami
tech-c:      Junichi Shi
upd-to:      noc@iij.ad.j
mnt-nfy:     noc@iij.ad.j
auth:        PGPKEY-8AB6A
auth:        PGPKEY-4A928
auth:        PGPKEY-5D02F
auth:        PGPKEY-6B8FF
auth:        PGPKEY-08FDF
auth:        PGPKEY-DB111
auth:        PGPKEY-49CAE
auth:        PGPKEY-A51FA
auth:        PGPKEY-F0471
mnt-by:      MAINT-AS2497
changed:     shuhei-o@iij
source:      JPIRR
```

差出人: jpirrhj@nic.ad.jp　宛先: noc@iij.ad.jp Cc: jpirrhj@nic.ad.jp
件名: [NOC 492033] JPIRR Route Hijack alert　日時: Wed, 18 May 2022 01:15:50 +0900 (JST)

ご担当者様

以下の通り、経路ハイジャックが疑われる状態を検知しました。

```
検知日時                  :  Wed 18 May 2022 01:15:48 +0900 (JST)
Routeオブジェクト         :  202.232.0.0/16
RouteオブジェクトのOrigin :  AS2497
検知したPrefix            :  202.232.1.76/30
検知したOrigin            :  [redacted]
ROAに関する情報           :  2021-11-01T01:28:42Z 2497 202.232.0.0/16
```

このお知らせについてご不明の点は、jpirrhj@nic.ad.jp までお問い合わせください。

経路ハイジャック検出システムは一般社団法人ICT-ISACから提供を受けています。

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)
事務局 JPIRR担当
E-mail: jpirrhj@nic.ad.jp

出典: https://www.nic.ad.jp/ja/materials/iw/2009/proceedings/h10/iw2009-h10-02.pdf

- **ROA(Route Origin Authorization)登録**
  - IPアドレスと広告元であるOrigin ASNの組み合わせが正しいことを証明する電子署名データ
  - 登録するべき情報は以下
    - Origin ASN : 広告元AS
    - Prefix : 広告するPrefix
    - Maximum length : 最大広告サイズ
  - ROAの登録データをBGP経路のValidationに利用して経路ハイジャックの影響を軽減する (ROV: Route Origin Validation)
  - IIJの場合はRIR/NIRが用意するシステムを使って発行。自前(BPKI)でCAを用意することもできるがやっていない
    - IPアドレスは複数のNIR/RIRから割り振り/割り当てを受けており、それぞれ対応する
    - JPNIC / ARIN / APNIC / RIPE
  - 証明書なので期限があるが、RIR/NIRによっては自動で管理・更新しており発行されていれば半永久的に有効となっている場合もあり

- **自身で発行できる範囲**
  - 自身が保有するIPアドレスのみ
  - 2022/11月現時点ではIRRような代行登録はできない

- **現状のアドレス利用、広告状況の把握**
  - 利用形態に応じたROA発行が必要
    - 広告元のOrigin AS / Prefixと広告(予定)サイズ
  - 広告予定の経路の使い方を把握する
    - 経路の広告サイズや分割ポリシー、Origin AS
    - パンチングホールや他のASからの経路広告はあるか？
      - 自社AS利用 or 他社AS利用
      - 自社のIPアドレスを他社へ持ち込んでいる可能性
      - クラウド型DDoS対策サービスの契約等はないか
      - IPアドレスの貸出をしていないか

- **対外接続先の経路フィルタ開放**
  - 申告されたIPアドレスベースで厳密に制御されている場合は対外接続先に更新を依頼
  - IRR登録されていれば自動で更新される場合もあり
    - TransitやPeerでもIRRベースのフィルタが多い印象
    - どうやって開放されるかを事前に確認しておくと吉
    - 設定変更されるまでリードタイムがある場合もあるので前もって実施しておく

- **経路フィルタは結構気を使う**
  - お客様向けの経路フィルタはお客様からの申告で開放
  - 一部試験的にIRRベースでのフィルタ生成を導入 (not 自動反映)

- **IIJのUpstreamはIRRベースが多い**
- **Peerで厳密な経路フィルタを実施しているところは少ない？？**

- **経路の広告制御**
  - outbound (from IIJ to the Internet)
    - 生成されたCIDR経路の経路長でインターネットへ広告
    - IIJ内部では細かな経路を利用しているため、CIDR経路のサブネット経路が外部へ広告されないように経路フィルタで制御
      - CIDR経路よりも細かな経路は明示的にdeny
  - inbound (from the Internet to IIJ)
    - IIJの外部組織からIIJのCIDR経路を受け取らないフィルタを設定
    - 外部からの不要な経路を削って経路ハイジャックを防ぐ
      - IIJ外部からIIJが生成している経路が来ることはおかしい

- **経路の生成**
  - IIJの場合はdiscard/null 経路で生成しiBGPで経路広報
  - 日本(東京/大阪)に経路生成用ルータが存在
    - 複数ルータ、複数リージョンでの経路生成により冗長性を確保
    - bug等の不具合での経路消失リスクを排除すべく機種やOSも分けている
    - 昔はIIJ America経路はUSで生成していたが、日本へ経路生成ルータを集約

- **経路広告後はAS外部での経路確認**
  - 各社提供のlooking glassなどを利用
  - 経路フィルタが開放されているか、なども再チェック
  - ROVのstatusが想定通りvalidになっているかのチェックも最近では重要

- **ここまで準備できてIIJでIPアドレスがサービスで利用可能となる**

- **(特に対外組織との) IPアドレス利用状況の多様化**
  - AS内のルーティング管理の難しさ
    - インターネットを介さないSaaSとの直接接続
    - サービスのオンデマンド化やネットワーク設定の自動化の拡大
      - いままではAS2497のインターネット運用部隊が外部へ経路広告を管理・監督してきた
      - 誤入力や誤設定ありうるかも？
      - IRR/ROAではさまざまな想定パターンを考慮しなくてはいけない事情が出てきた
  - AS内ルーティング状況やIPアドレスの利用状況が正しい、正しくない、直ぐに判別/判断できますか？

- **組織内のIPアドレス管理**
  - 外部へ広告する際はそれなりに厳密に対処
  - ではAS内部でのIPアドレスは適正に利用されているのか
    - どのIPアドレスがどのサービス設備/どのインタフェース/どの顧客へ割り当てられていて、その情報は適宜更新されているのか…結構あやしい!?
    - お客様へ割り当てた後のwhoisのOganizationとか適宜更新されていますか
    - 組織内whoisとか、IPAMとか、みなさんお持ちでしょうか？

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。