発表概要

発表タイトル

- IXにRTBHフィルタリングを導入してみた ～L2網上での設計と運用の課題～

概要

- IX利用者の間でもDDoS攻撃対策への需要が高まる中、JPNAPでは2022年9月にRTBHフィルタリングサービスの提供を開始しました。サービスの実現に当たり、IXというL2の環境ではトラフィックの破棄について自網ルーターでのnull0へのルーティングという手法が使えず、RTBH用の経路を顧客ルーターで受け入れてもらう必要があるなど、ISPのようなL3網での一般的な実装とは異なる制約や課題があります。

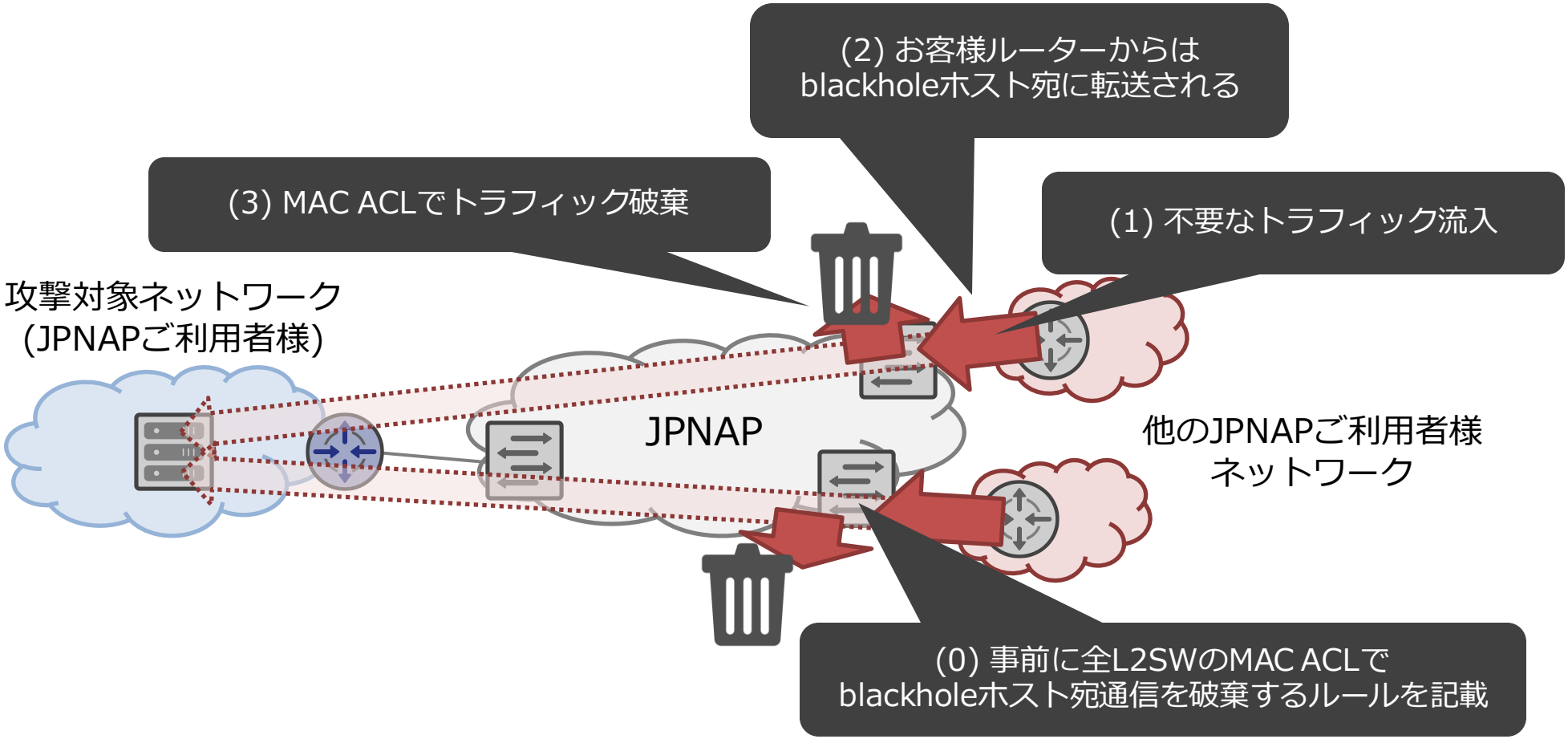
  今回はJPNAPでの設計やサービス仕様をご紹介しつつ、この仕様・実装方式についての率直な感想やIXでのRTBHについてどうあるべきか・どうあってほしいか、IX利用者およびサービス提供者双方の視点で、皆さまと議論できればと考えております。

内容 (案)

- **一般的なRTBHについて**
  - ISP等の構成例：ルートリフレクタ (RR) から自AS内にRTBH経路を広告し、null0に向けて破棄させる
- **IXのNW構成上の制約・課題**
  - IXでは経路の受け入れ先となるルーターはお客様の管理下なので、コントロールが効かない
- **JPNAPで採用した、RTBHサービス仕様・実装方式説明**
  - RTBHサービス仕様
    - ルートサーバーではRTBH経路として/32 (IPv4), /128 (IPv6) のprefix長の経路のみ受け入れ
  - 実装方式
    - IXセグメント上に通信破棄用の宛先となるblackholeホストを用意
    - ルートサーバーで、 blackhole communityが付与された経路のNEXT_HOPを blackholeホストに書き換えて、他の利用者ルーターに広報
    - L2スイッチのMAC ACLで、blackholeホスト宛通信を破棄することでRTBHを実現
    - ※ルートサーバーを介さない直接のピアリング (バイラテラルピアリング) の場合は、 利用者側でNEXT_HOPをあらかじめblackholeホストにした経路を広報することで、トラフィックの破棄は可能
- **議論** (詳細はp.4,5)
  - 利用者視点での仕様に対するご意見、この構成・設計についてのコメント等

JPNAP RTBH 略図

- 不要なトラフィックの宛先をblackhole用ホストに向けることで、
  エッジのL2スイッチのMAC ACLで破棄させる



議論したいポイント案 (1/2)

- **本方式でのRTBHについて、利用者視点での率直な感触をお伺いしたい**
  - RTBHの利用に際し、ルートサーバーに求める仕様はあるか？
    - 現時点の仕様では、RTBH経路として /32 (IPv4), /128 (IPv6) のみ許可としている
      - ✓ 利用者ルータでこの長さの経路が許可されないと、blackholeホストに経路が向かない
      - ✓ 一般的には長い経路はフィルタされている認識のため、お客様にJPNAP上では受け入れをお願いをする方向で考えているが、感触をお聞きしたい
        - » /32, /128 の受け入れはやはり抵抗がある？
        - » RTBH用経路は所定のBGP communityが付いているなど、目印があればまだ受け入れやすい？
    - NEXT_HOPがネイバーのIPアドレスでない場合はルートサーバーではrejectする仕様だが、blackhole community付与時に限り、NEXT_HOPがblackholeホストならacceptすることを検討中
      - ✓ IX用の設定としてルートサーバー経由/直接ピアリング (バイラテラルピアリング) 用でポリシーを共用している場合、ルートサーバーに対しても、バイラテラルピアの設定と揃えてNEXT_HOPを利用者側で予めblackholeホストに向けて広告した方がconfig的に楽というケースがあった

議論したいポイント案 (2/2)

- **本方式でのRTBHについて、利用者視点での率直な感触をお伺いしたい (続き)**
  - RTBH経路を広告するときの想定運用について
    - いざRTBHを利用したい時に、blackhole communityを付与して経路広報するハードルは高い？
      - ✓ ポータルサイト上のGUI操作で適用できると嬉しい？ (現状の構成だと反映までタイムラグが生じる)
    - RTBHの特性上、攻撃が止まったかどうかの判断がお客様側でできないことについて
      - ✓ IX側でMAC ACLのdenyカウンターを見る程度しか取れる手がないと考えている
  - RTBHの経路に対してはRPKI ROVを実施できないことへの感想

- **サービス提供者視点で、この仕組みがより効果的に機能する環境をどう作っていくか**
  - お客様向けに地道にRTBH用経路の受け入れを依頼？
  - 馴染みのないお客様向けに、RTBHの勉強会などを開催？