Peering Best Practices 2025
ピアリングベストプラクティス 2025

概要:

本ドキュメントは、インターネットピアリングにおいて2025年現時点で推奨される主なベストプラクティスを記述したドキュメントです。ベストプラクティスは、技術の発展や業界のトレンドなどによって変化するものであり、不変ではありません。そのため、2025年時点での推奨となっています。本ドキュメントは、技術事項だけでなく、接続構成、データベース、コミュニケーションなどのベストプラクティスについても記載しています。これからピアリングをしようと思っている組織や、既にピアリングを実施している組織の定期点検のガイダンスとなれば幸いです。

主な接続構成:

- PNI（プライベートピア）
    - 構成概要：PNIは2つのASが、専用のインターフェース（バーチャルインターフェース含め）を使い、専用のルーター間サブネットを割り当てて、1:1のピアリングを行うものです。2つのASは、構内配線を使って物理接続するのが一般的ですが、帯域サービスやダークファイバーなどを使ってリモートPNIの構成も珍しくありません。
    - ベストプラクティス：IPアドレスはどちらのASが付与するか特段決まりはないですが、構内配線を手配する側がアドレスも付与する、などの取り決めをすると管理がしやすくなります。ルーター間PrefixはIPv4の場合/31か/30が一般的で、IPv6の場合/127 (RFC6164) か/126が一般的です。これ以外のPrefix長になる場合は特殊構成であるケースか、ループのリスクを伴う事を許容しないといけません。構内配線コストは、折半する事が一般的ですが、AS間で協議して決めるものです。インターフェースが1本の場合でもSingle member LAGを設定する事が多く、インターフェーステストの際、LAGなしでテストした後にLAG設定を入れる事が一般的です。開通時や障害対応の際、回線トラブルシュートのため、Loopback試験を実施する事が多く、その場合は現地でのループ作成などでピアASとの綿密なやり取りが必要となります。
- IX接続
    - ベストプラクティス：原則各IXのガイダンスに従う必要があります。
- リモート接続についての注意点
    - リモート接続はPNIの場合もIX接続の場合も、トラブル時の切り分けなどの難しさがあります。冗長構成が保たれている状態がベストですが、そうでない場合はピアに長期断を許容するお願いをしないといけない場合があります。ピアによっては長期断を許容せず、ピアを削除してしまう事があり、それをリスクとして認識する必要があります。リモート接続している場合、ピアASにそれが伝わらない事により、予想外の遅延が発生したりする事もリスクとして考える必要があります（例：日本のISP AとISP Bが両方ロンドンのルートサーバーに接続していて、日本で直ピアはしておらず、共通で接続している国内ルートサーバに障害があった場合）。リモート接続は、回線テストのLoopback試験も複雑になります。これはIXに接続する場合はなおさら、自AS、リモート回線業者、IX事業者、構内配線事業者、など多数のプレイヤーとの連携が必要になります。
- 冗長構成について
    - PNIの場合、最低限2つの独立したセッションを、ルーター冗長で接続する事が望ましいです。複数POPでの接続が可能な場合はより冗長性が増します。これは自AS側の冗長だけでなく、ピアASのPeering POPも冗長を考慮して接続する必要があります。ただし、本当に冗長が取れているかは、リモート接続だとわかりにくくなるため、リモートなのかそうでないのかの確認が必要です。都市間（例えば東京で1PNI、大阪で1PNI）はあまり冗長構成とは言えませ

ん。一つの都市で冗長を取り、さらにその上でもう一つの都市でも冗長が最も望ましいですが、片方の都市がシングルという構成は何もないよりはマシとされています。
    - IXの場合、異なるIX上でのピアが望ましく、一つのIXに複数IPを持っている場合は、その全てのIPでピアする事が望ましいです。例えば、自ASがIP2つ、ピアASがIP2つの場合、プロトコル毎に合計4つのセッションを確立する事になります。
    - PNIのバックアップとしてIXでのピアは、どちらかで輻輳リスクを伴うためあまりお勧めではありませんが、ピアASと相談する必要があります。IXでのみピアしている場合でも通常トラフィック交換されているIXのバックアップとなるIXでお互い十分な帯域が確保できているかを考慮する事も望ましいです。ただし、大手コンテンツ事業者など、送信側で輻輳を検知して自動迂回してくれる場合は、自AS側の空帯域に留意していれば大きな問題には発生しにくいです（コンテンツ側の帯域不足によりトランジットにトラフィックが回る可能性はあります）。

各種データベース登録:

- PeeringDB
  ピアリングを申請する前に、PeeringDBに自ASの情報を登録する必要があります。登録の際にはいくつか注意点があります。まず最低限考慮するべき事として、PeeringDBのアカウントはAS運用で使っている業務用メールアドレスを使うこと、接続しているIXのIPアドレスも公開すること、PNIをするのであれば、ファシリティ情報も可能な限り公開すること、運用連絡先を公開することです。IRR(後述)のAS-SET情報の登録(IRR as-set/route-set)、経路数の登録(IPv4 Prefixes、IPv6 Prefixes)を正確に登録する事も強く推奨します。経路数は実際の経路数ではなく、最大これくらいになるかも、という数を登録しておく事が望ましいです。この情報登録が重要となるのは、大規模ネットワークを運用しているISPやコンテンツ事業者はPeeringDBの情報を参照して設定を自動化しているところが多く、情報に不足があるとピアリングできず、メールなどでは取り合ってもらえない事があるからです。

- IRR
  トランジット事業者やピアリング相手に経路を広報する前に、IRR (Internet Routing Registry)に広報する経路 (route/route6) オブジェクト、そして広報する経路のOrigin AS一覧となるas-setオブジェクトを最低限登録されている必要があります。IPトランジット事業者はこの情報を元に顧客とのBGPセッションに経路フィルターを設定する傾向にあります。また、有効性について疑問はあるものの、ピアに対してas-setの情報を元にAS pathフィルターを設定する事業者も少なくありません。IPトランジット事業者などにIRRに代理で登録してもらうproxy register方式という形もとれますが、適切な登録およびトランジット事業者を変更した際も安定して継続運用するため、自ASで登録管理する事を強く推奨します。IRRは、一般的にJPNICやAPNICなどのレジストリが提供しているものや、RADBなど独立機関が運用するものや、NTTなどのトランジット事業者が運用しているものなどがありますが、レジストリが提供しているものを利用するのが推奨です。複数併用する場合は、更新漏れの無いよう留意しましょう。

  参考：JPIRRでのオブジェクト登録について

- RPKI ROA
  IRR登録と同等のタイミングで、経路広報前にRPKIのROAを作成する事を強く推奨します。2025年現在、ROAの登録が無くても(Unknown状態)経路広報を受け入れてくれるピアが大半です。しかしROAを登録していない場合、経路ハイジャックなどにより到達性障害リスクが増大するだけでなく、自AS広報の正当性を主張していない事となるため、障害復旧やピアからの協力に遅れが出る可能性もあります。ROAを生成する場合、exactだけでなく、自身で運用する可能性のあるprefix length最大値まで設定する事が望ましいです。

ピアまたは顧客から受信する経路に対してROAなどを元に経路フィルターを作成する、またはROVを実施するASが増えています。特に、顧客から受け取ったInvalidな経路をそのままピアなどに流しているトランジット事業者は、Invalid経路が多すぎる場合ピアを敬遠されてしまう可能性があります。ROVでなくとも、相応のフィルターを実施している事が望ましいとされます。受取Prefix長は、ROAで主張されているPrefix lengthも受け入れる事が望ましいです。

RPKIについてまとめると以下です。
ROA：全員に登録を強く推奨。
ROV：トランジット事業者はROVまたは同等の効果の経路フィルターを強く推奨。なお、IXでルートサーバーを運用している事業者もROVを実装する事が望ましい一方、Unknownの取扱についても厳しく運用するか、Unknownを許容するかは2025年時点ではベストプラクティスが定まっていません。

参考：JPNIC　ROAの作成と管理の方法

接続機器の設定:

接続機器の設定については、原則JANOG Commentとして策定されている文章を参照する事が望ましいです。それに加え、最新のアップデートを以下に記載します。

- IXに接続する時のルーター設定 (JC1005)
    - IXセグメントをバックボーン内に経路注入し、NOCから監視できるようにしたいというニーズがあります。しかしこれをやってしまうと、たとえ対外ピアに対して経路広報しない場合であっても、そのネットワークのユーザー側からも到達できてしまうため、一般的にロバストに作られていないIXのルートサーバなどのリソースに対してのDDoSが成立しやすくなります。このため、監視は（トンネルネットワーク経由やSNMPなど）別の方法で実施する事が望ましいです。
    - 現状、特にIX上のBGPセッションにMD5を設定する事業者は多く見られます。後継とされるTCP-AOの採用は限定的ですが、今後の普及に注目していく必要があります。
    - IX上でBFDを設定する事業者は現状稀ですが、リモート接続であったり、BGPタイマー依存の切り替えでは問題のあるケースで設定される事もあります。ただし、現状設定に前向きな事業者は限定的です。
    - 特にルートサーバに接続している場合、大量の経路が流れてきてMax prefixを設定している場合セッションがダウンしてしまう事がある。対策として、discard extraなどの手法を用いる事もできるが、この運用はまだ一般的とは言えません。重要なピアは、ルートサーバに依存せず個別にピアを設定する事が現状ベストプラクティスと言えます。Max prefixは、各ピアASのPeeringDBの値を参照する事になりますが、その値よりも多く設定する、もしくは前ピアー律で高めの値を設定する、という形が一般的なようです。長期ピア断のお掃除などに合わせ、Max prefixは定期的な見直しを業務に組み込む事がお勧めです。
- PNIのルーター設定
    - 基本は上述JC1005のSection4-4とほぼ同等になります（ルートサーバの設定は不要）。
- 推奨フィルター
    - トランジットに対するフィルタは (JC1001) を参照。
    - ピアに対するフィルタ (JC1002)
        - ピアから受信する経路も、IRRやROAを元にフィルターを書く方が現在は望ましいとされています。IRRベースのフィルターの効果は限定的です。
    - 顧客に対するフィルタ (JC1003)
        - JC1003の2-2の部分で、「顧客側 AS から広告をすると通知があった Prefix のみを accept する」と記載されていますが、昨今は顧客が通知してきたPrefixの正当性をROAやIRRなどのデータを参照して正当性を確認する事が望ましいです。

    - JCに明確な記載は無いが推奨するフィルタ
        - BGP nexthopになっているセグメント、例えばIXのセグメントや、PNIのルータ間アドレス用に使っているセグメントを、外部から受信しない経路フィルターを設定する事が望ましいです。

経路広報および受信（フィルタ以外）

- バイラテラル
    - 推奨Prefix長はIPv4の場合最大/24までを広報、受信する設定が未だ一般的です。それ以上の経路を受け取らなければならないケースも他国では存在しますが、Transitから受け取る経路も/24までで問題ありません。IPv6の場合は/48まで受け取る設定が一般的ですが、/64まで受け取る設定の方もいます。経路広報は可能な限り/48までとした方が到達性のトラブルを避ける事ができます。
    - BGP Communityに、Roleという機能がRFC9234で定義されました。2025年時点でこの運用はまだ一般的ではありませんが、将来これを元に経路フィルターを実装する事が想定されます。Well-known Communityは受信時に削除しないようにしましょう。
    - ピアASから受け取るMEDを受け入れるかどうかは、ピアによって異なるため、ピアに確認するか、原則MEDに依存しない設定を想定しましょう。
    - 特定のピアASと設定する全てのBGPセッションで、地域的な要素を除き、可能な限り同一ポリシーを適用した経路を交換する事が望ましいです。
- マルチラテラルおよびそのリスク
    - ルートサーバ経由の経路交換（マルチラテラル）は、一つのBGPセッションで複数のASと経路交換ができるメリットがあります。一方で、以下のリスクが認められています。
        - 大量経路流入リスク：これは前述の通りMax prefixの問題です
        - Inbound輻輳リスク：経路を送信していると、DDoSも含め、想定外のピアASからトラフィックが到達してしまう可能性があります。この結果IXのスイッチ側での輻輳になる事があるため、RTBH対応もしくは経路送信を止めるなどの対応をする事があります。重要なピアは、バイラテラルで経路交換する事がベストプラクティスです。
        - 経路フィルター不可リスク：経路フィルターはルートサーバー運用社側に委ねられる事が多く、特にIRRをベースにした経路フィルターをルートサーバーとのBGPセッションに自ら設定する事は運用負荷がとても高くなり、あまり現実的ではありません。特に海外のIXに接続する場合、ルートサーバの経路フィルターを適切に対応しているIXとそうでないIXが混在します。

トラフィックコントロール手法

- ピアリング
    - 送信側によるコントロールが強いため、受信側で取れる手段は限られています。送信が多いコンテンツ側の設定としては、トラフィックの大小に関係なく、一般的にはAct/Sby構成でなく、全リンクActとして設定する方が好まれがちです。Inboundトラフィックが大きいISP事業者の場合、Outboundを一本のリンクに集約するケースが見られますが、なるべく通常状態でも複数リンクにMultipathなどの設計や技術で分散させる事が望ましいです。難しい場合は、ピアと相談しLAGにより帯域を均一に増強していく事が望ましいです。
    - 受信側でコントロールできる最も一般的手法はPrependです。前述のとおり、MEDを受け付けない事業者は少なくありません。経路広報は、バックボーンでつながっていない経路があるなどの場合を除き、なるべく特定のPeerに対しては全BGPセッションで同じ経路を送信する事で、トランジットなどの高コストパスの利用を避ける事ができます。一時的にトラフィック分散の

ために経路が同一でなくなる事は許容されるが、それを通常状態とするとトラブルシュートが長引かせる問題につながります。
    - ローカルにあるIXでピアリングしていて、remote peeringなどの手段で遠方のIX（遠く離れた国や地域）のIXでもピアリングした場合、同じ経路を受けるとトラフィックが遠い場所を経由してしまう形になりかねない。遠方のルートサーバ利用の場合得にリスクになりやすく、設定に配慮する必要があります。
- トランジットのトラフィックコントロールは、トランジット事業者やそのTier構造での位置付けによって異なるため、一概に良い方法というのは存在しません。ピアリングと大きく変わらないが、全てのトラフィックが課金トラフィックとなるため、ピアリングと比べて無理やりな方法で対処せざるをえない状況もあるが、事業者選定の時からなるべくこうならないように選定するのが望ましいです。

ピアとのコミュニケーション

- NOC問い合わせ
    - NOC間の問い合わせは、適切な連絡先をPeeringDBに掲載する事で連絡を取りやすくする事が望ましいです。大量のピアを設定している国際的な事業者の場合、独自のデータベースに連絡先を入力するよう求める事業者もいます。単一国家で運用している事業者はこの方式は避けるべきで、可能な限りPeeringDBへの適切な情報掲載をするべきでしょう。
- ピアへの障害通知
    - IX上でのピア断を伴う障害通知は、長期にわたる断でない限りあまり求められる事はありません。メンテナンスのピア断も事前通知しない事業者が多いです。トランジット含め別経路に迂回していれば問題ありませんが、ピアASから説明を求められた場合は可能な限りの対応をする事が望ましいです。
    - PNIはIXと異なり、専用の回線であるためメンテナンス通知や障害通知は出す事が望ましいです。特に専用線などの障害で長期にわたる断が発生する場合、ピアASにその旨を通知する方が良いです。

参考文献

https://www.rfc-editor.org/rfc/rfc7454.html

貢献いただいたみなさま

川村（Editor）、馬渡さん、Tomochaさん、松崎さん、外山さん、小山さん、饗庭さん、熊本さん、大日方さん、生野さん、福智さん

Version 1.0 2025年12月3日