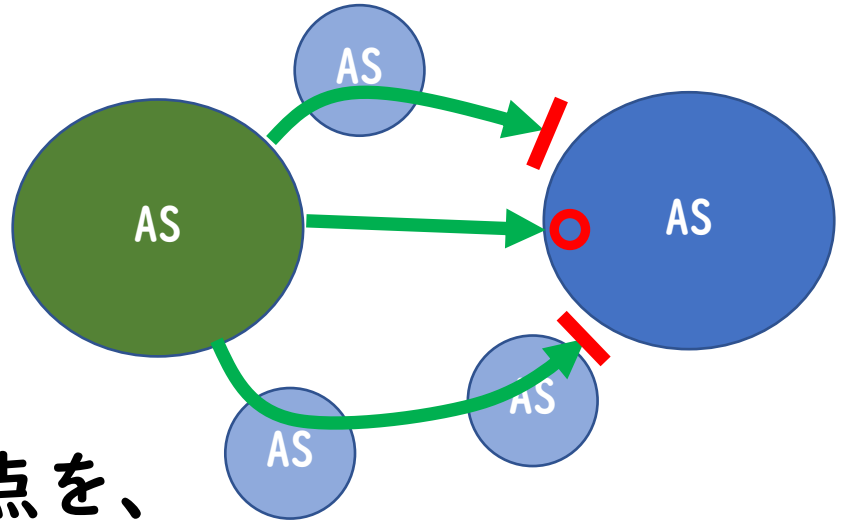
peerlock導入検討ワーキンググループ報告

peerlock導入検討ワーキンググループ
Matsuzaki ‘maz’ Yoshinobu
<maz@iij.ad.jp>

それはJANOG45で始まった・・・

peerlock導入検討WG



peerlockとは

保護対象ASからの経路が流入するBGP接続点を、
経路フィルタで制限することにより、
経路リーク等の影響を軽減する経路制御手法

(Job Snijders氏が考案)

このワーキンググループでは、peerlock機能を提供する際の考慮点などを議論、検討した。

BGPの接続モデル

- 接続先カテゴリ毎に経路制御ポリシーが異なる
- 接続先に任せるしかない制御(3.のところ)もある

接続先	1.受信を期待する経路	2.広報する経路	3.期待する経路の流通先
ピア	相手とそのカスタマ	自身とカスタマからの経路	相手とそのカスタマ
上流	フルルート/デフォルト	自身とカスタマからの経路	相手とその全接続先
カスタマ	相手とそのカスタマ	フルルート/デフォルト	相手とそのカスタマ

経路リーク（RFC7908）

- 経路が意図や期待を超えて伝播してしまうこと
  - 例：ピアから受信した経路を他のピア/上流に広報した
  - 例：上流から受信した経路を他のピア/上流に広報した

- 意図せぬ経路状態になったり、遅延やパケットロスが発生して通信品質が劣化するなどの影響も発生する
  - 影響はAS間の経路制御状態やリークした経路内容によって異なる

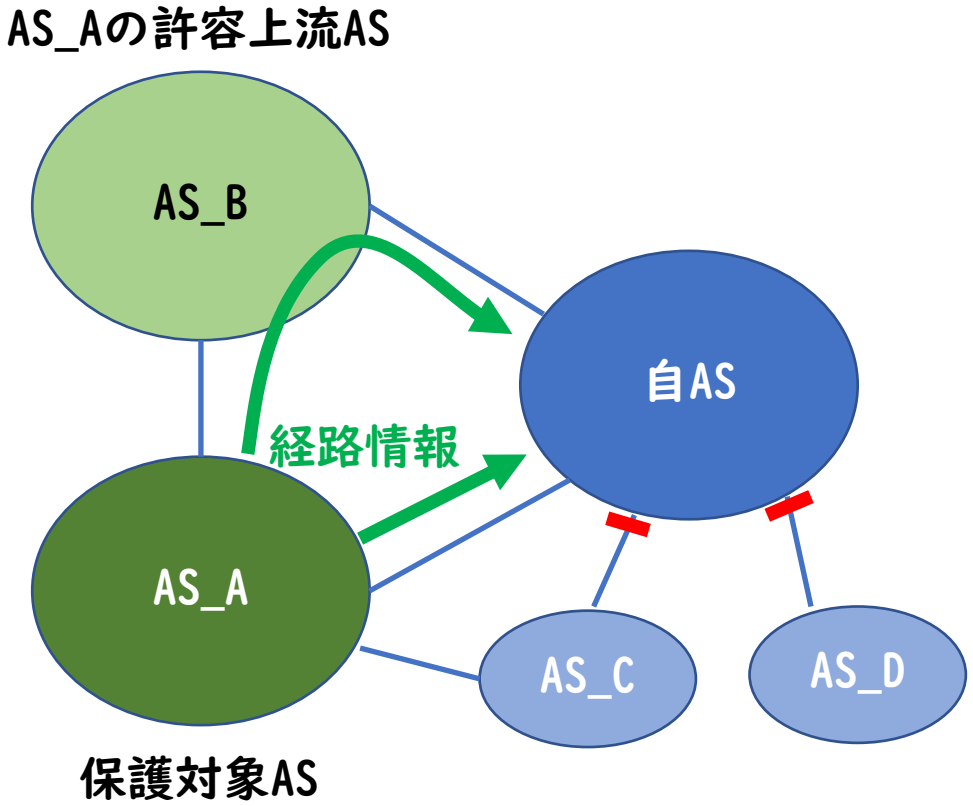
経路リークへの対策

- 厳密な受信経路フィルタの適用
  - しかしピアに対しては厳密な経路フィルタが適用しにくい
  - IRRを用いた自動化にも限界がある
- Down Only (DO) Community
  - ピアや上流から受信した経路にBGP Large Communityで共通的なタグを付加しておいて、経路種別を識別しようという提案
- AS Provider Authorization (ASPA) + BGPSec
  - 予めASの上流を宣言しておき、それに基づいてAS_PATHを評価する提案

- そんなわけで今すぐ実装できそうなpeerlockの登場

自ASでpeerlockをAS_Aに提供する

- 保護対象ASからの経路が流入する接続点を明確化
  - AS_Aとの直接接続経由
  - AS_Aの上流AS(AS_B)経由
  - (自ASの上流AS経由)
- 他の全てのBGP接続でAS_Aを AP_PATHに含む経路をフィルタ
  - 例えばAS_CやAS_DとのBGP接続



peerlockが機能しやすい環境

- 保護対象ASと直接接続している
- 保護対象ASは、ピアや上流に全ての接続点で同一のprefixを広報している
- 保護対象ASとの相互接続が十分冗長で、他のAS_PATHに迂回することを想定しなくて良い
- 迂回するとしても、ごく少数の代替AS_PATHに限られる

- これらが満たされてないと、あれこれ追加の検討が必要

問題が発生しそうな条件

- 保護対象ASがピアや上流毎に異なるprefixを広報している
  - peerlockで意図せず経路がフィルタされる危険性があるので要注意
- 保護対象ASとの相互接続が十分冗長でない
  - 直接接続が断すると許容上流AS経由の通信になるため、許容上流ASの設定が常に正しいかを確認しておく
- 迂回時のAS_PATHが多様
  - 許容上流ASのさらに上流など、流入を許可しなければならないBGP接続が増えたり、不明確になったりして厳密なpeerlockを提供できない

  →特にTier 1以外で発生しそうな条件

条件付き適用の検討

- 強い心で他のAS_PATHには迂回させない
  - 保護対象ASをAS_PATHに含む経路は、直接接続だけで受信
  - 保護対象ASとの相互接続が十分冗長なら検討に値する

- 代替経路として使いたくないBGP接続に経路フィルタを適用
  - 例：帯域が細い他ASとの接続
  - 例：地域が異なる他ASとの接続
  - 継続的な設定見直しと保護対象ASとの意識合わせが重要
  - ちょっと複雑なのでお勧めしない

AS間での確認事項

- 連絡先
- 運用ポリシー
- 設定変更に要する目安時間

確認事項：連絡先

- お互いの連絡の窓口
  - メールアドレスの他にも手段があるとなお良い
  - 依頼受付窓口として顧客向けポータル等を利用しても良い

- 連絡時に厳密な連絡元の認証は必要ないと考えられる
  - 変更がすぐさま到達性に影響しないため
- メールで連絡する場合、確認と履歴が取れるようNOCやピアリング窓口などを含めることが望ましい

確認事項：適用ポリシー

- どのような適用を行う明確にしておくこと
  - 万が一の障害切り分け時に参考になる
- できれば文章等で参照できるようにしておくことが望ましい
- 保護対象ASが何らかASを跨いだ特殊な経路制御を実施する場合にはpeerlock適用下で問題が発生しないことを確認しておくことが望ましい

確認事項：設定変更に要する目安時間

- 設定変更に要する目安時間を示しておくこと
- 保護対象ASが設定変更を依頼しようとする場合には余裕を持った連絡を行うことが望ましい
- peerlockの性質上、設定変更の依頼はそれほど発生しないものと想定される

peerlock提供側での迂回範囲検討

- 直接接続が全断した時の備え
  - 保護対象ASとの相互接続が冗長なら必要ないかもしれない
- 許容上流ASとの関係
  - 許容上流ASのさらに上流からの経路流入は許容する？
  - 許容上流ASと直接接続がなかったらどうする？
- 自ASの上流ASとの関係
  - 自ASの上流からの経路流入は許容する？
- 運用を簡素化するため、事前に提供条件をまとめておく

peerlock提供側でのフィルタ適用手法

- フィルタでは必ず経路を破棄すること
  - 優先度を落とす設定では、細かい経路が採用される危険性を残す
- 1）保護対象ASをもとに生成したAS_PATHフィルタを適用する
  - 保護対象ASがAS_PATHに含まれていた場合、該当経路を破棄
- 2）その接続から受信しても良いAS_PATHフィルタを適用する
  - 許可リスト以外の経路を破棄
    - 保護対象ASが許可リストに入っていないため、破棄されるはず
  - 完全なAS_PATHを記述した場合、1)と同等の挙動になる
  - 広報元ASのみを指定した場合、AS_PATHの途中に保護対象ASが含まれていても許可するため、1)と微妙に挙動が異なるので注意が必要

peerlock提供側でのフィルタ運用

- より高頻度な設定変更が必要になる
  - 具体的には経路フィルタの適用、更新
  - 保護対象ASの追加削除、許容上流ASの変更やその他ポリシーの変更、新たな相互接続の追加などなど、様々な変化に追従する必要
- 接続先AS毎に異なるAS_PATHフィルタを都度生成
  - これを適切に実施するため、必要に応じて設定や設定確認の自動化なども検討することが望ましい