

JANOG57 in Osaka Day 2

なぜBGPルートリークはなくならないのか、 RFC 9234が目指す「最後の防波堤」

日本ヒューレット・パッカード合同会社

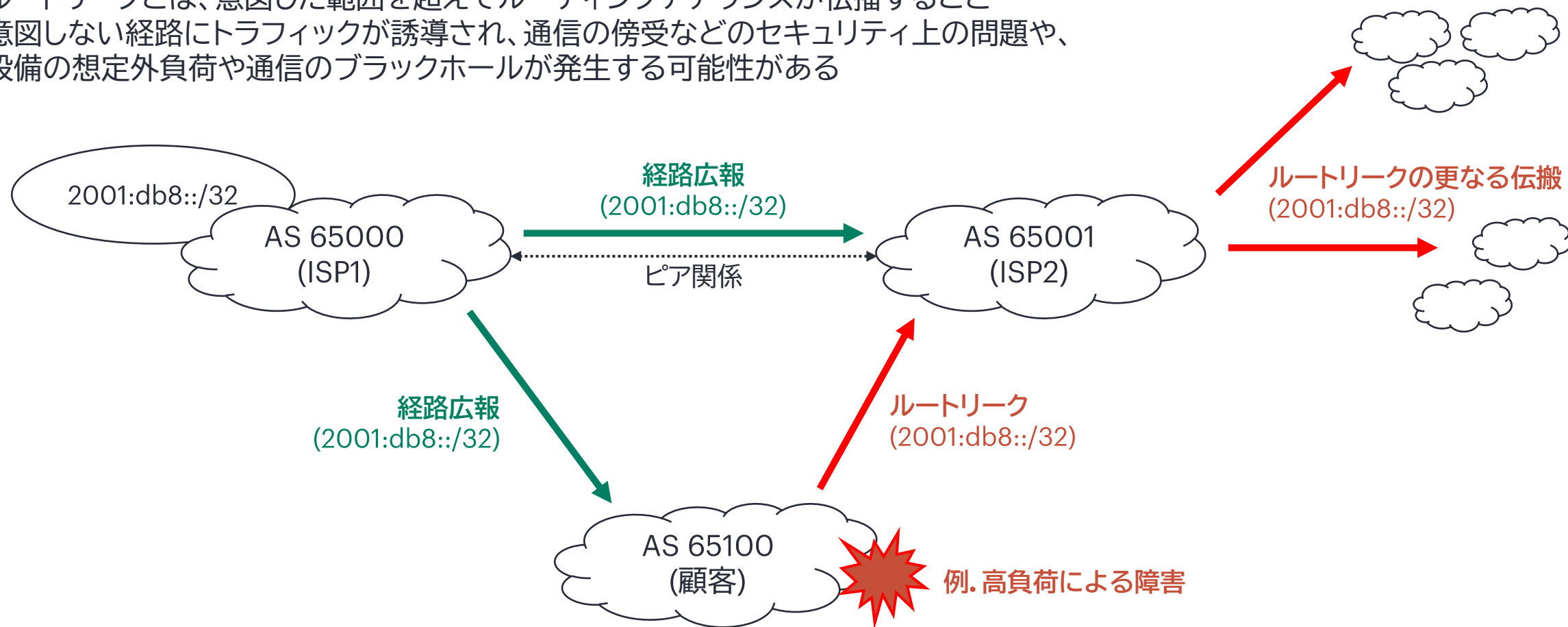
山岸 祐大

BGPルートリークとは？

RFC7908にて、BGPルートリークは以下のように定義されている:

RFC 7908: Problem Definition and Classification of BGP Route Leaks

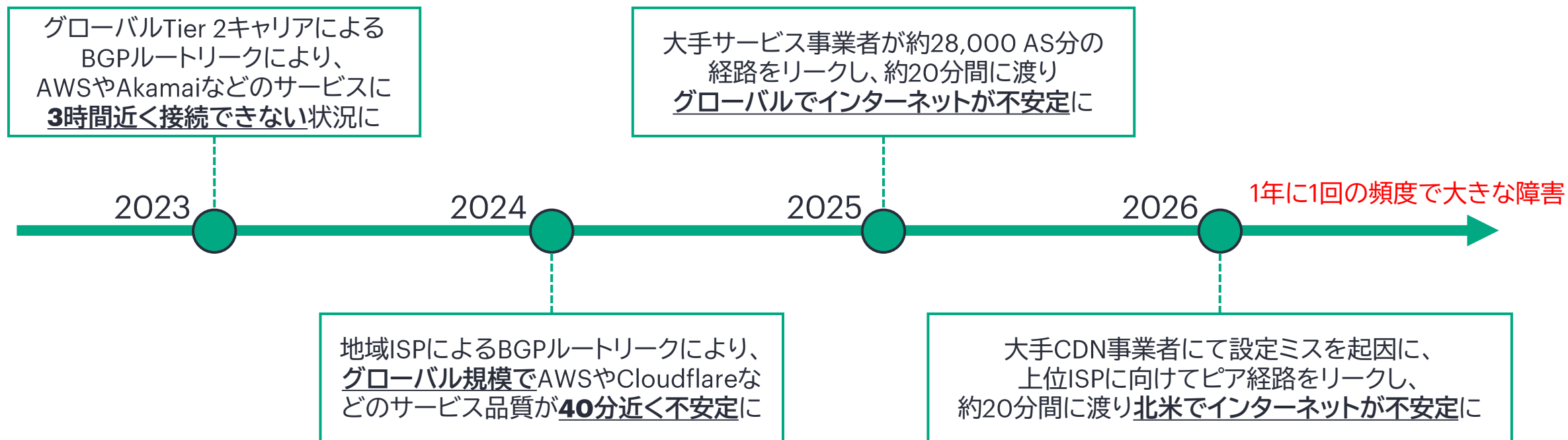
- ルートリークとは、意図した範囲を超えてルーティングアナウンスが伝播すること
- 意図しない経路にトラフィックが誘導され、通信の傍受などのセキュリティ上の問題や、設備の想定外負荷や通信のブラックホールが発生する可能性がある



BGPルートリークは身近で起きている

“ In 2025, ... On average, **1,966 ASes per month were involved in route leaks**, compared to 1,977 in 2024. The dynamics of global BGP incidents differed from those observed for ordinary incidents. In 2025, **the number of global route leaks** decreased by roughly one third compared to 2024, **falling from 33 to 25**. ”

2025 DDoS, bad bots, and BGP incidents statistics and overview ^{*1}
Qrator Labs

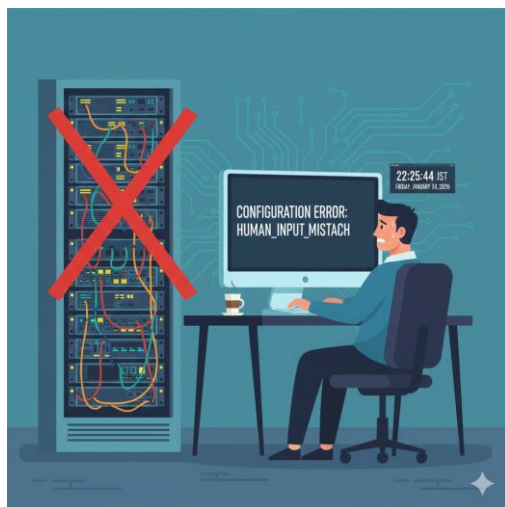


*1. 出典: 2025 DDoS, bad bots, and BGP incidents statistics and overview, Qrator Labs,
<https://qrator.net/blog/details/2025-DDoS-bad-bots-and-BGP-incidents-statistics-and-overview/>

なぜBGPルートリークは起きるのか？

BGPルートリークが発生する原因の例として以下の4つが挙げられる:

1. 設定エラー



2. 故意的



3. コミュニケーションミス



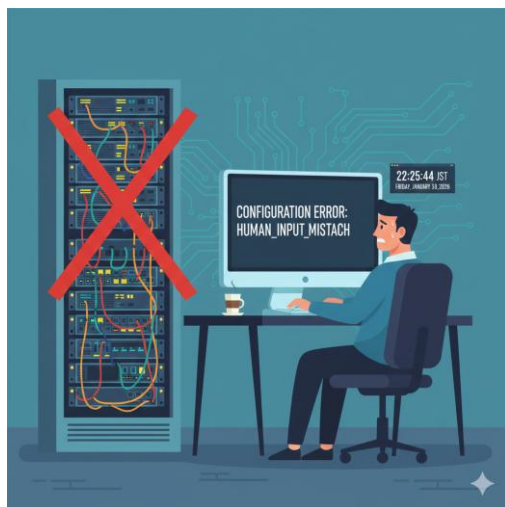
4. 機器不具合



なぜBGPルートリークは起きるのか？

BGPルートリークが発生する原因の例として以下の4つが挙げられる:

1. 設定エラー



2. 故意的



3. コミュニケーションミス



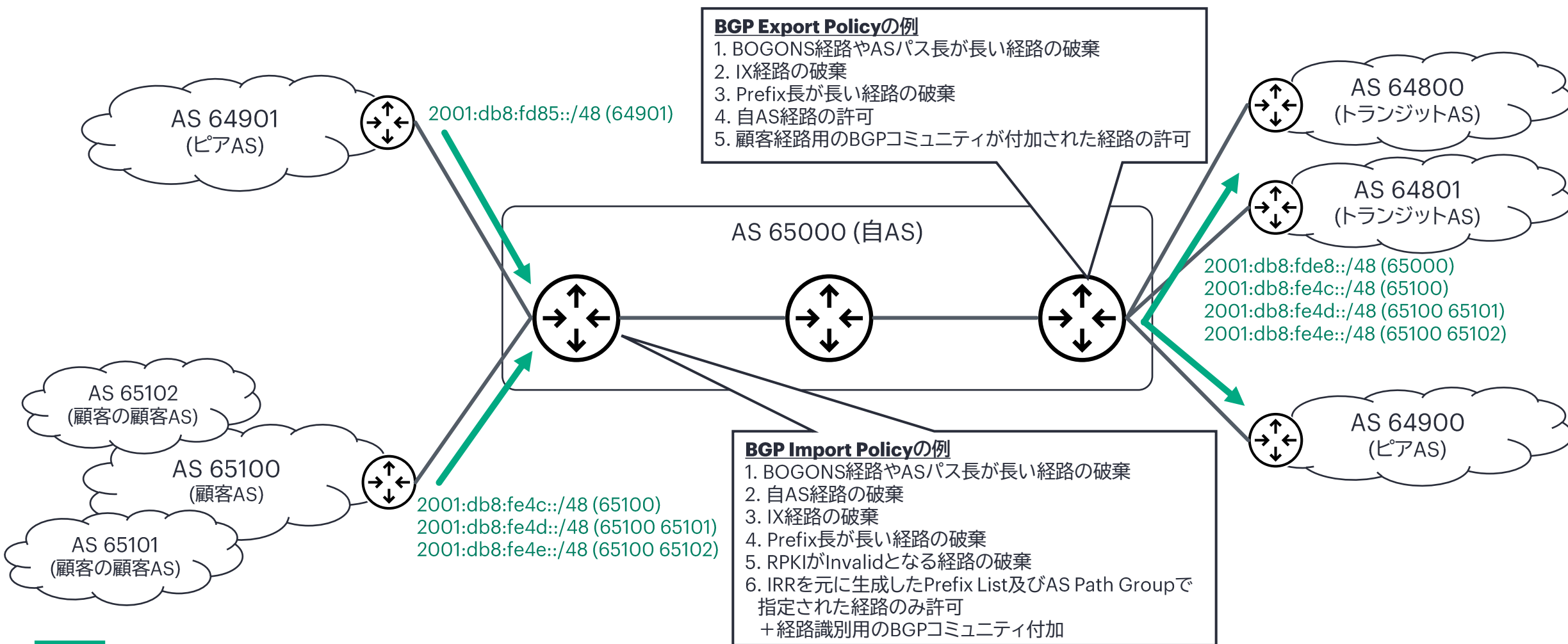
4. 機器不具合



“Route leaks can be accidental or malicious but **most often arise from accidental misconfigurations.**”
RFC7908より

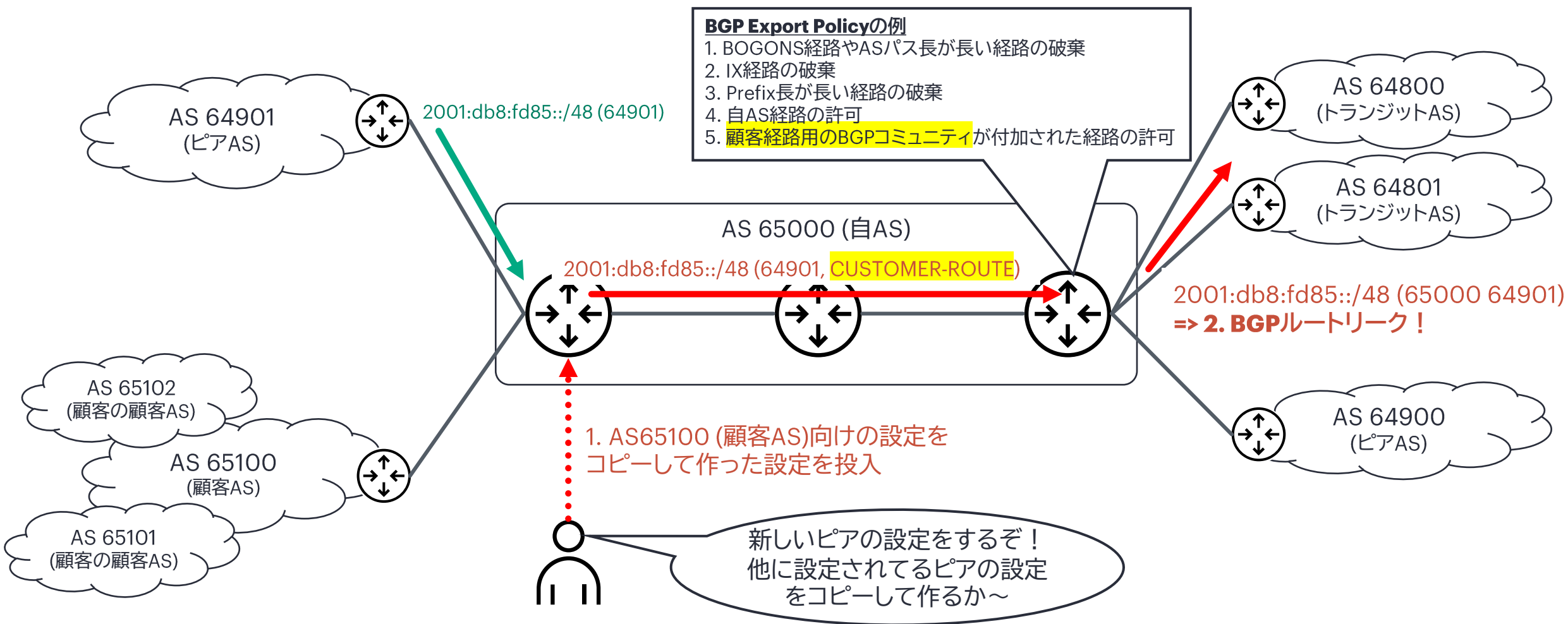
外接ルータの設定は複雑 #1

近年推奨されているベストプラクティスなBGPポリシーを全て導入するとコンフィグが比較的複雑に



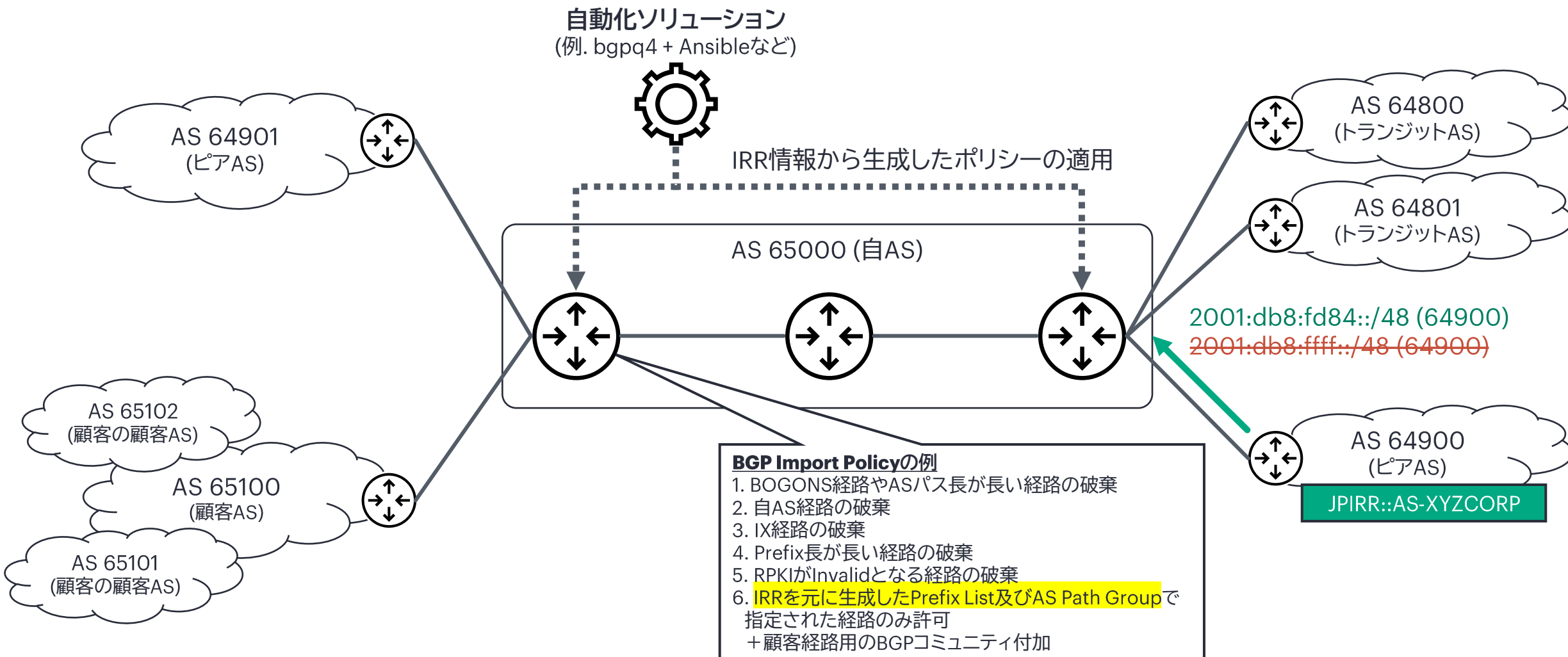
複雑が故にヒューマンエラーの温床に

設定変更時に考慮するポイントが多く、細かい部分での見落としが発生しやすい



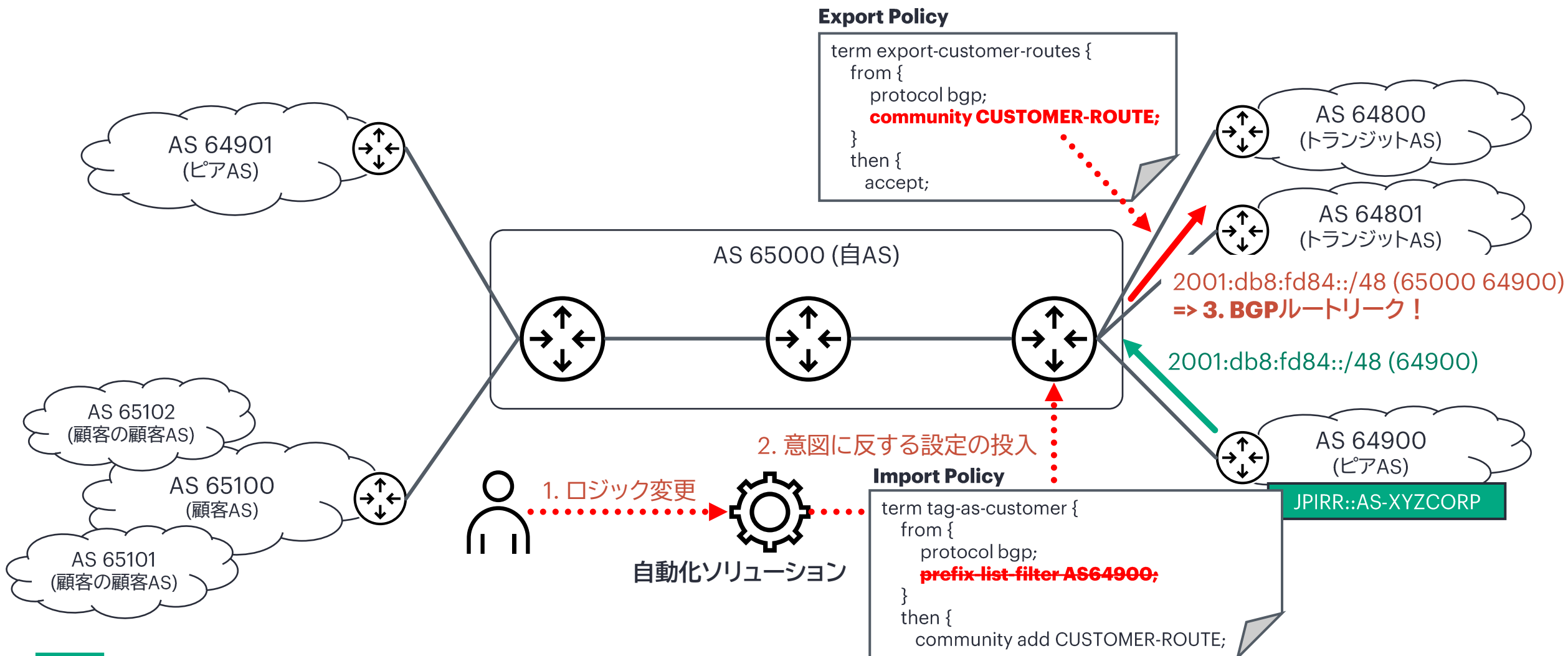
外接ルータの設定は複雑 #2

IRRの情報に追従させるためなど、BGPポリシー制御を自動化しているケースも多い



自動化によるトラブル

BGPポリシーが複雑な故に、自動化するためのソフトウェアロジックも複雑になりがち



BGPルートリークを防止する仕組みの必要性

DevOpsやSREの考え方では「ミスが障害につながることを許したシステム側の不備に責任がある」

“ A “Bad Apple” problem, to the extent that you can prove its existence, “
is a system problem and a system responsibility.”

Sidney Dekker, The Field Guide to Understanding ‘Human Error’, Routledge, 2014

“ it is not acceptable to have a countermeasure to merely “be more careful” or “be less stupid” — instead, **we must design real countermeasures to prevent these errors from happening again.**”

Kim, Gene, et al. The DevOps handbook: How to create world-class agility, reliability, & security in technology organizations, It Revolution, 2021



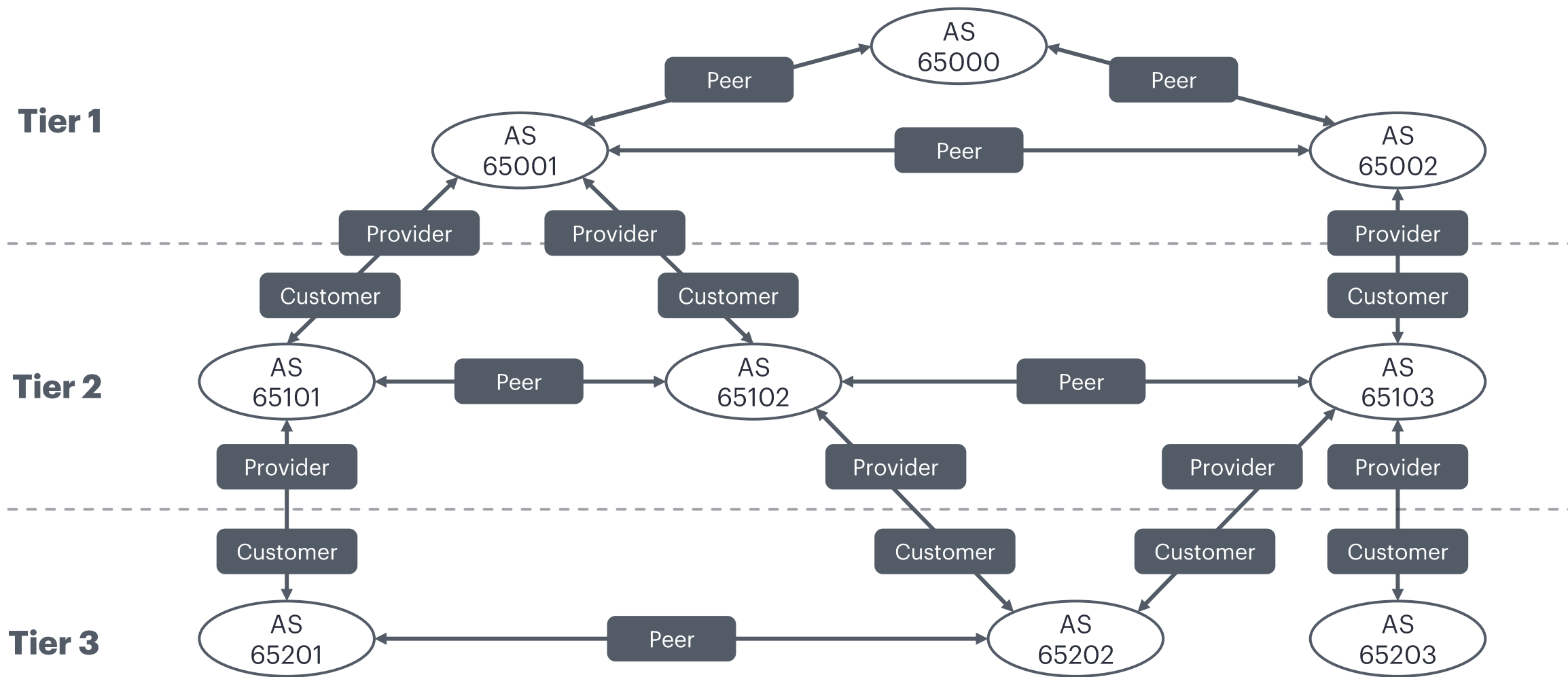
ヒューマンエラーは起きるものとして考え、
万が一の際にBGPルートリークによる障害を防ぐ「防波堤」が必要



RFC 9234: Route Leak Prevention and Detection Using Roles in UPDATE and OPEN Messages

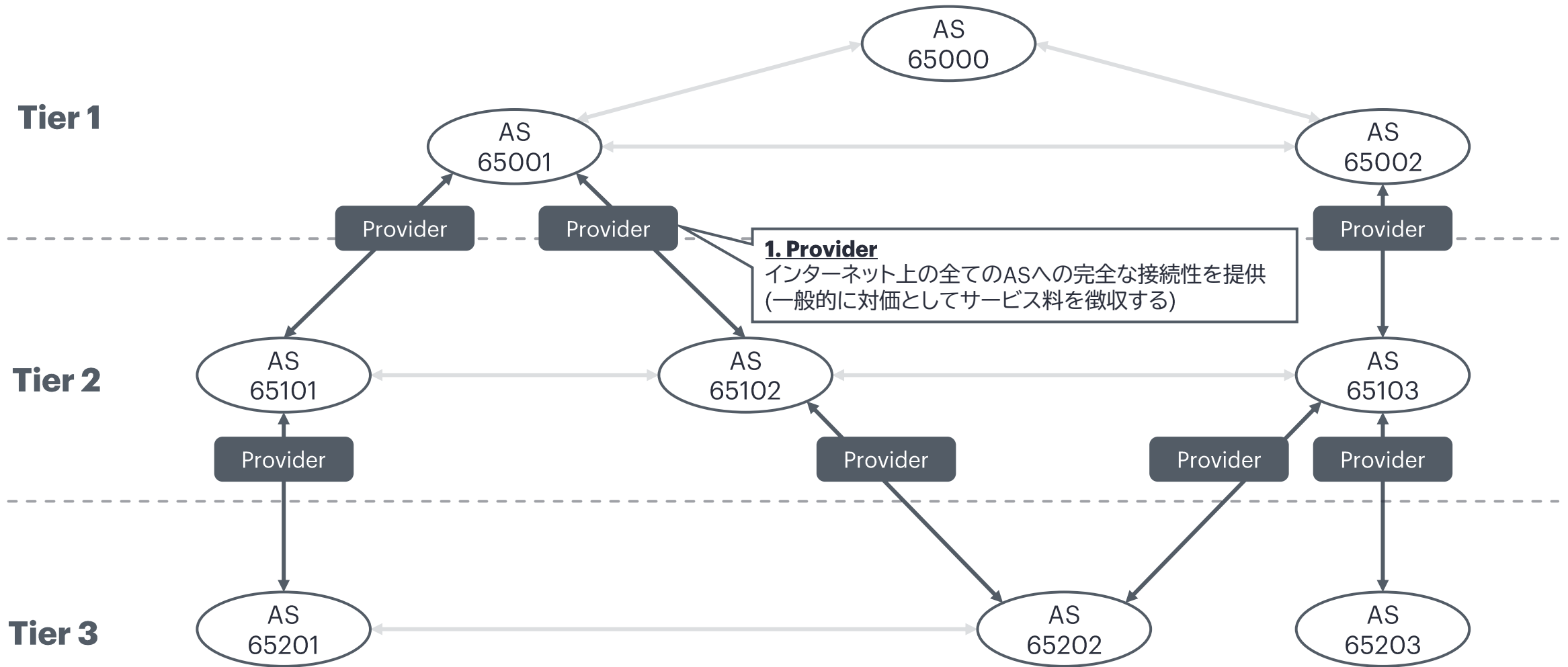
インターネットの構造

インターネットには、接続組織間 (=AS間)の「関係性 (Role*)」が存在する



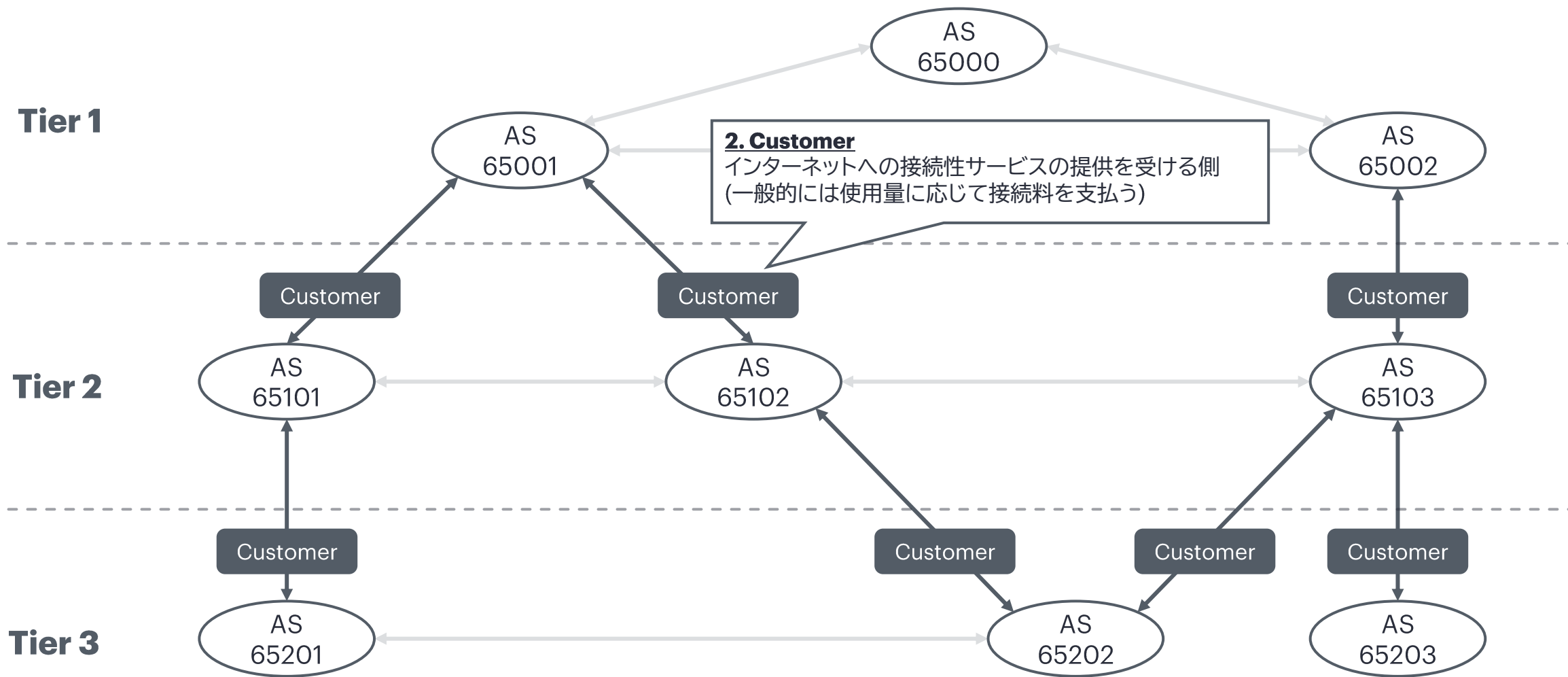
インターネットの構造

インターネットには、接続組織間 (=AS間)の「関係性 (Role*)」が存在する



インターネットの構造

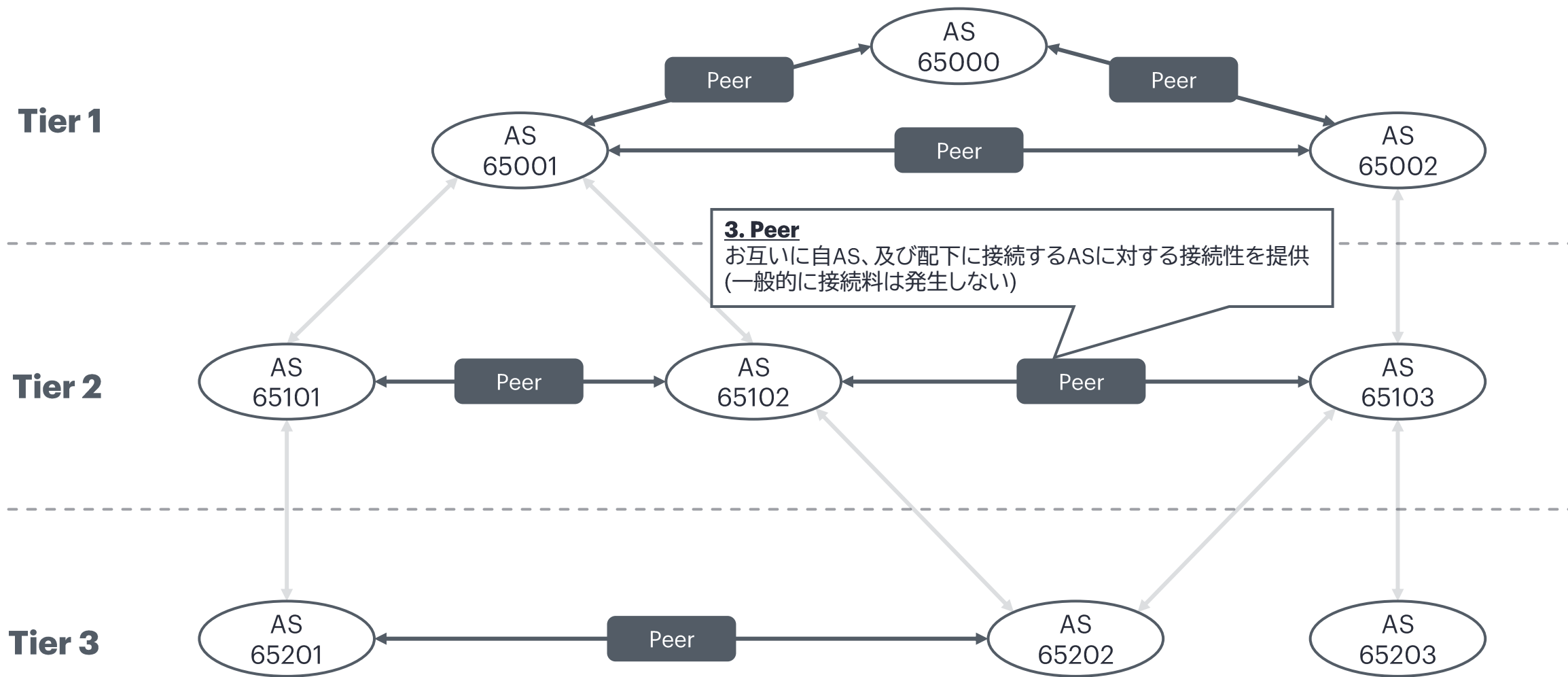
インターネットには、接続組織間 (=AS間)の「関係性 (Role*)」が存在する



* 意訳

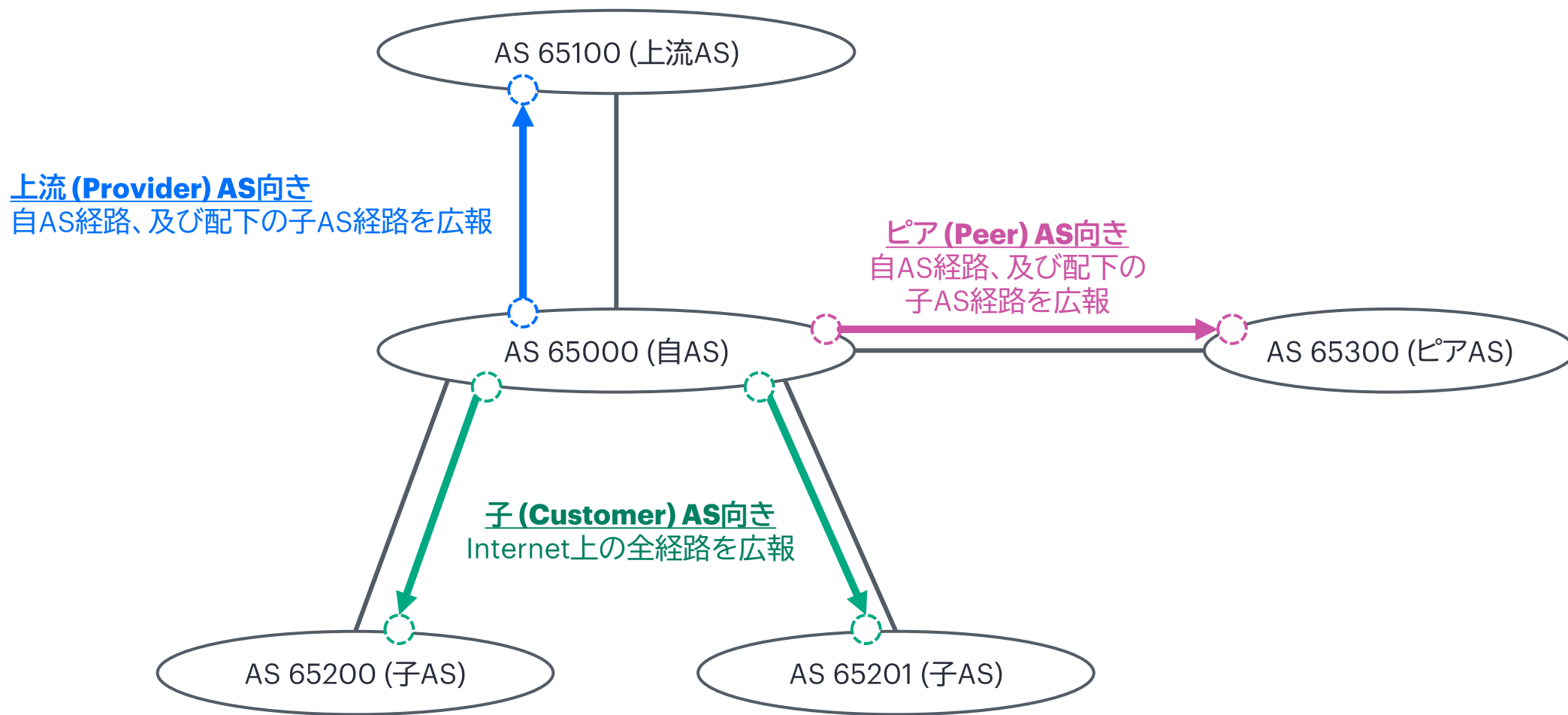
インターネットの構造

インターネットには、接続組織間 (=AS間)の「関係性 (Role*)」が存在する



組織間で交換される経路

組織間の関係性が対向組織に広報する経路、及び対向組織から受信する経路を大きく左右する

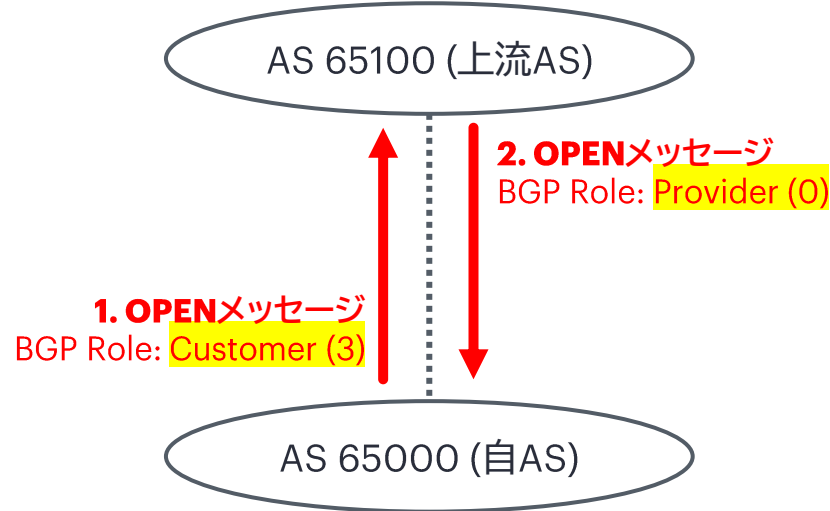


RFC 9234: 関係性の概念をBGPへ

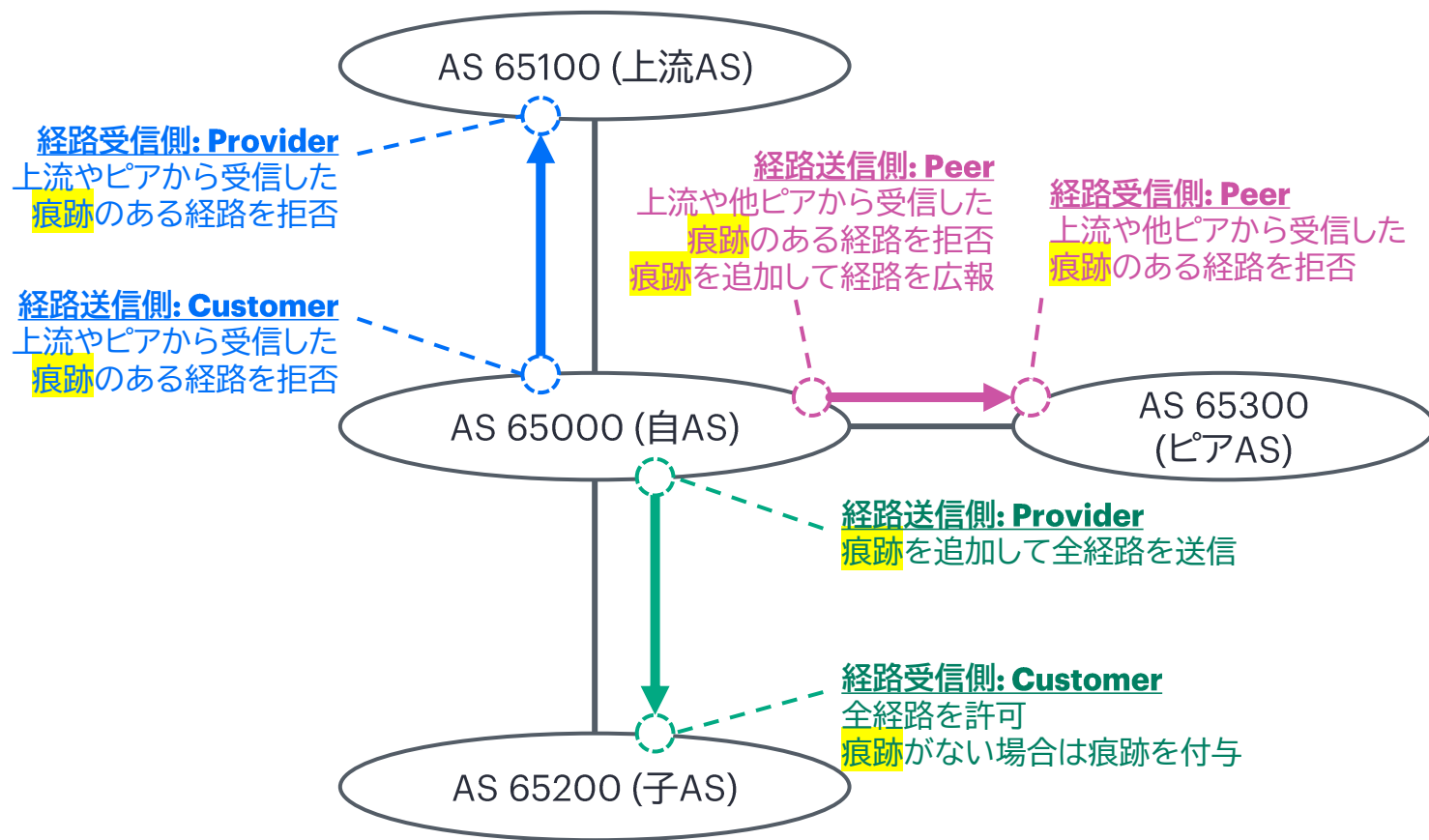
BGP上でお互いの「関係性 (Role)」を合意し、「関係性 (Role)」に応じて交換できる経路を制限する

RFC 9234: Route Leak Prevention and Detection Using Roles in UPDATE and OPEN Messages

1. 関係性 (Role)の合意



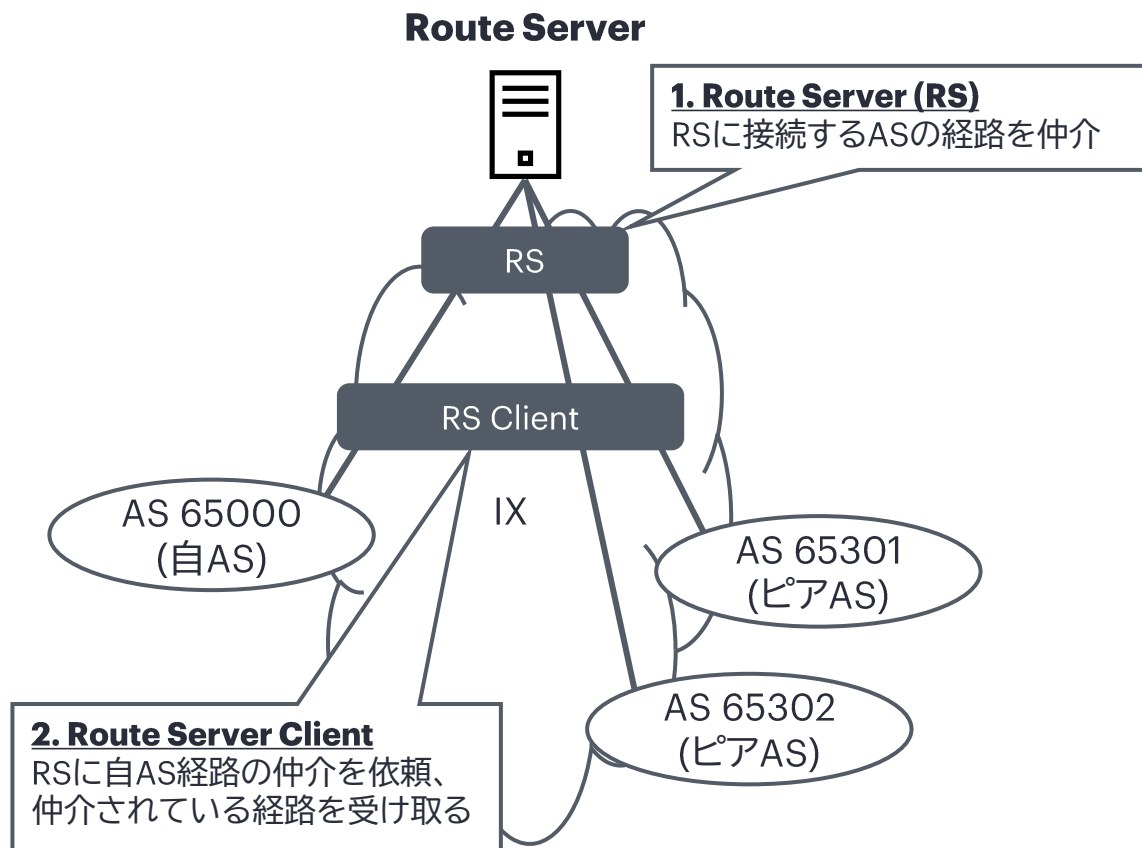
2. 交換できる経路の制限



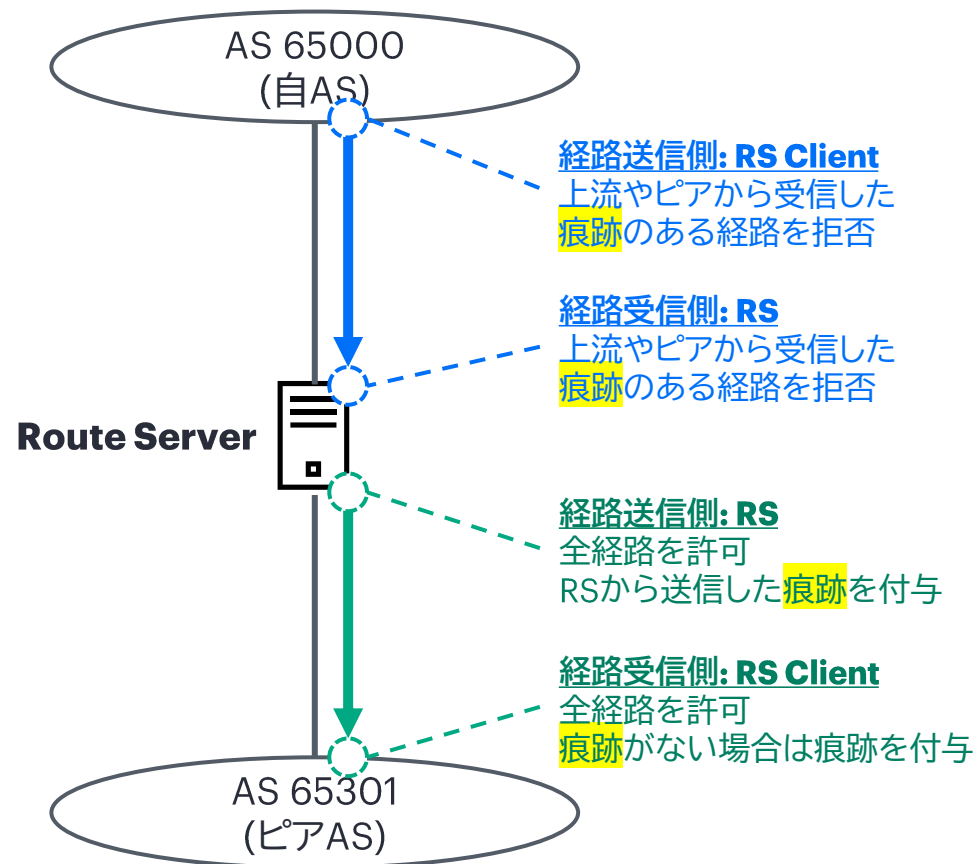
IX Route Serverへの対応

Route Serverとの接続におけるRoleも定義されており、交換できる経路の制限も行われる

Route Serverとの関係性



Route Serverと交換できる経路



RFC 9234の設定はシンプル

基本的にはBGPピアとの「関係性 (Role)」を指定するだけ

Junos/Junos EVO (>= 25.2R1)

```
protocols {
  bgp {
    group AS65000-CUSTOMER-V4 {
      type external;
      import [ ... ];
      family inet {
        unicast;
      }
      export [ ... ];
      peer-as 65000;
      otc-local-role {
        provider;
      }
      neighbor 100.64.1.1;
    }
    log-updown;
  }
}
```

FRRouting (FRR)

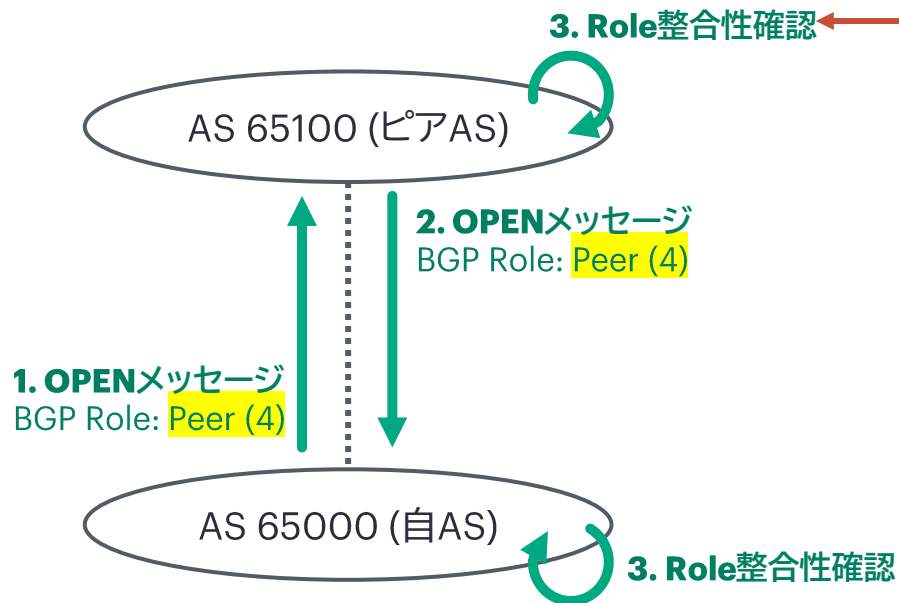
```
router bgp 65100
  bgp router-id 192.168.2.1
  network 192.0.2.0/24
  neighbor AS65000 peer-group
  neighbor AS65000 remote-as 65000
  neighbor AS65000 local-role provider
  neighbor 100.64.1.1 peer-group AS65000
  address-family ipv4 unicast
    neighbor AS65000 route-map AS65000-ROUTE-MAP in
  exit-address-family
```

* 他にもBIRD, OpenBGPDなどでサポート

OPENメッセージを通じてBGP Roleを通知し、組み合わせの整合性をお互いが確認する

OPENメッセージ例

```
> Internet Protocol Version 4, Src: 100.64.0.1, Dst: 100.64.0.2
> Transmission Control Protocol, Src Port: 59323, Dst Port: 179, Seq: 1, Ack: 1, Len: 68
√ Border Gateway Protocol – OPEN Message
  Marker: ffffffffffffffffffffffffffffffffffff
  Length: 68
  Type: OPEN Message (1)
  Version: 4
  My AS: 65000
  Hold Time: 90
  BGP Identifier: 192.0.2.1
  Optional Parameters Length: 39
  √ Optional Parameters
    > Optional Parameter: Capability
    > Optional Parameter: Capability
    > Optional Parameter: Capability
    > Optional Parameter: Capability
    > Optional Parameter: Capability
    > Optional Parameter: Capability
    > Optional Parameter: Capability
    √ Optional Parameter: Capability
      Parameter Type: Capability (2)
      Parameter Length: 3
      √ Capability: BGP Role
        Type: BGP Role (9)
        Length: 1
        BGP Role: Peer (4)
```

許容される**Role**の組み合わせ

Local AS Role	Remote AS Role
Provider (0)	Customer (3)
Customer (3)	Provider (0)
RS (1)	RS-Client (2)
RS-Client (2)	RS (1)
Peer (4)	Peer (4)

組み合わせに不整合がある場合

```
> Internet Protocol Version 4, Src: 100.64.0.2, Dst: 100.64.0.1
> Transmission Control Protocol, Src Port: 179, Dst Port: 59323, Seq: 69, Ack: 69, Len: 21
> Border Gateway Protocol - NOTIFICATION Message
  Marker: ffffffffffffffffffffffffffffffffff
  Length: 21
  Type: NOTIFICATION Message (3)
  Major error Code: OPEN Message Error (2)
  Minor error Code (Open Message): Role Mismatch (11)
```

対向がRFC 9234をサポートしていない場合

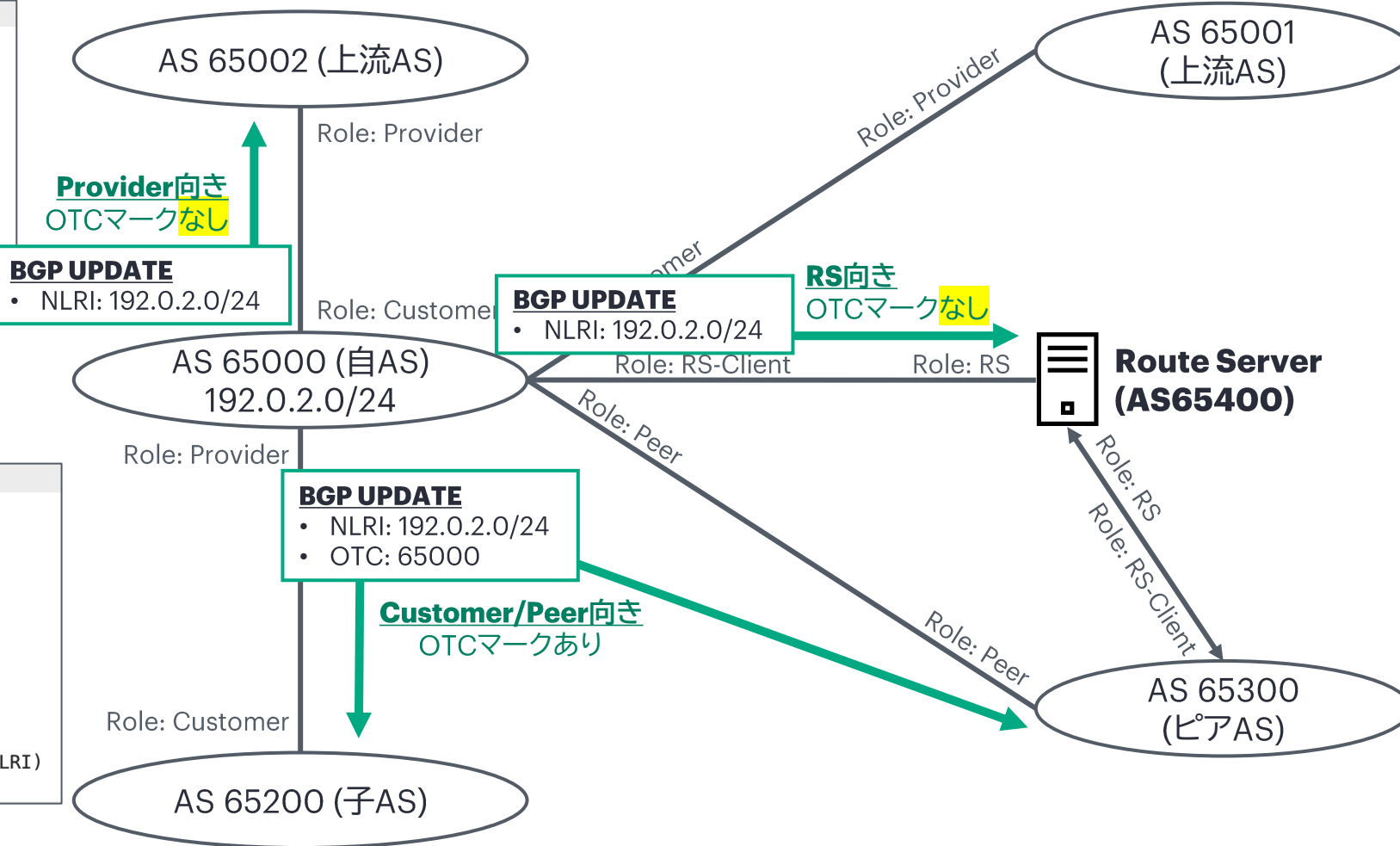
- デフォルトでは、BGPセッションは通常通り上がる
(自AS側だけでOTCの動作を行う)
- Strict Mode”を設定すると対向でのRFC 9234サポートを強制

経路のマーキング: Only To Customer (OTC) Attribute

上流、またはピアから受信した経路である「痕跡」としてOTC Attributeを経路にマーキングする

UPDATEメッセージ例 (OTCなし)

```
Border Gateway Protocol - UPDATE Message
Marker: ffffffffffffffffffffffffffffffff
Length: 47
Type: UPDATE Message (2)
Withdrawn Routes Length: 0
Total Path Attribute Length: 20
Path attributes
> Path Attribute - ORIGIN: IGP
> Path Attribute - AS_PATH: 65000
> Path Attribute - NEXT_HOP: 100.64.1.1
Network Layer Reachability Information (NLRI)
> 192.0.2.0/24
```

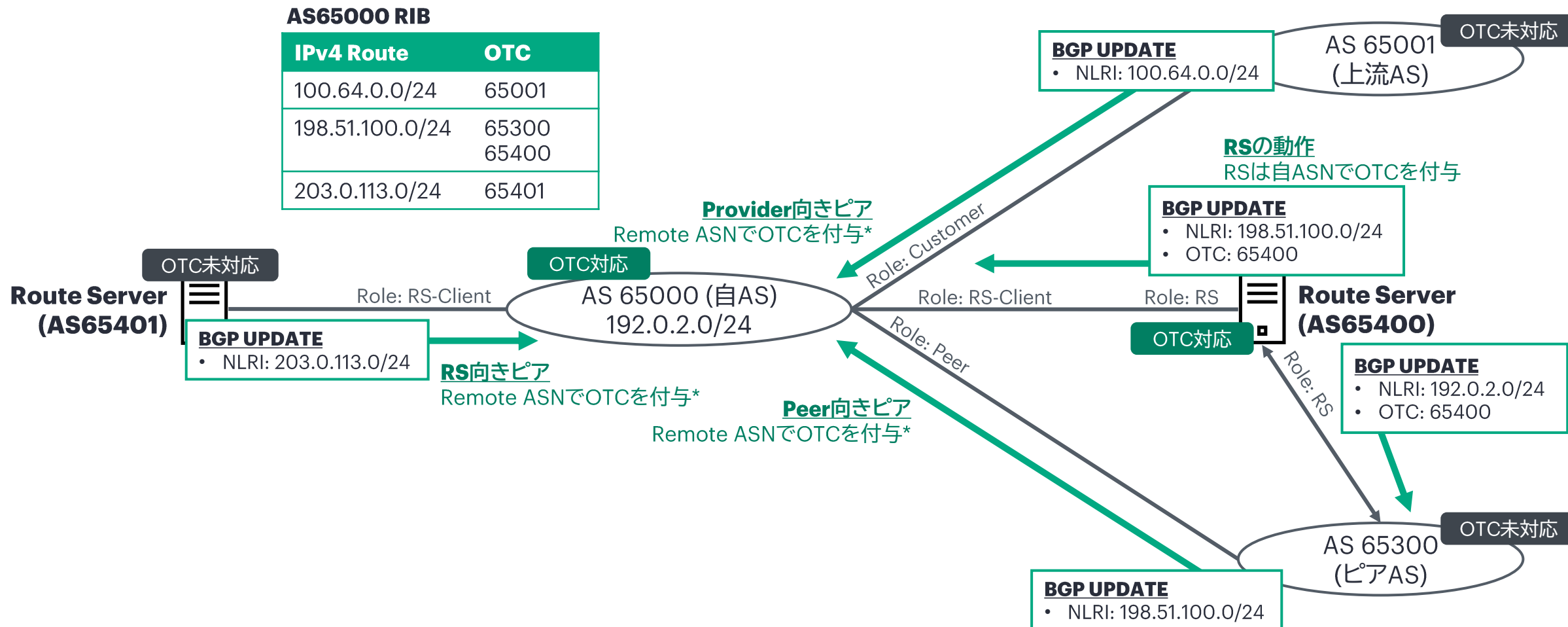


UPDATEメッセージ例 (OTCあり)

```
Border Gateway Protocol - UPDATE Message
Marker: ffffffffffffffffffffffffffffffff
Length: 54
Type: UPDATE Message (2)
Withdrawn Routes Length: 0
Total Path Attribute Length: 27
Path attributes
> Path Attribute - ORIGIN: IGP
> Path Attribute - AS_PATH: 65000
> Path Attribute - NEXT_HOP: 100.64.0.1
> Path Attribute - OTC: 65000
Network Layer Reachability Information (NLRI)
> 192.0.2.0/24
```


受信経路に対するOTCマーキング

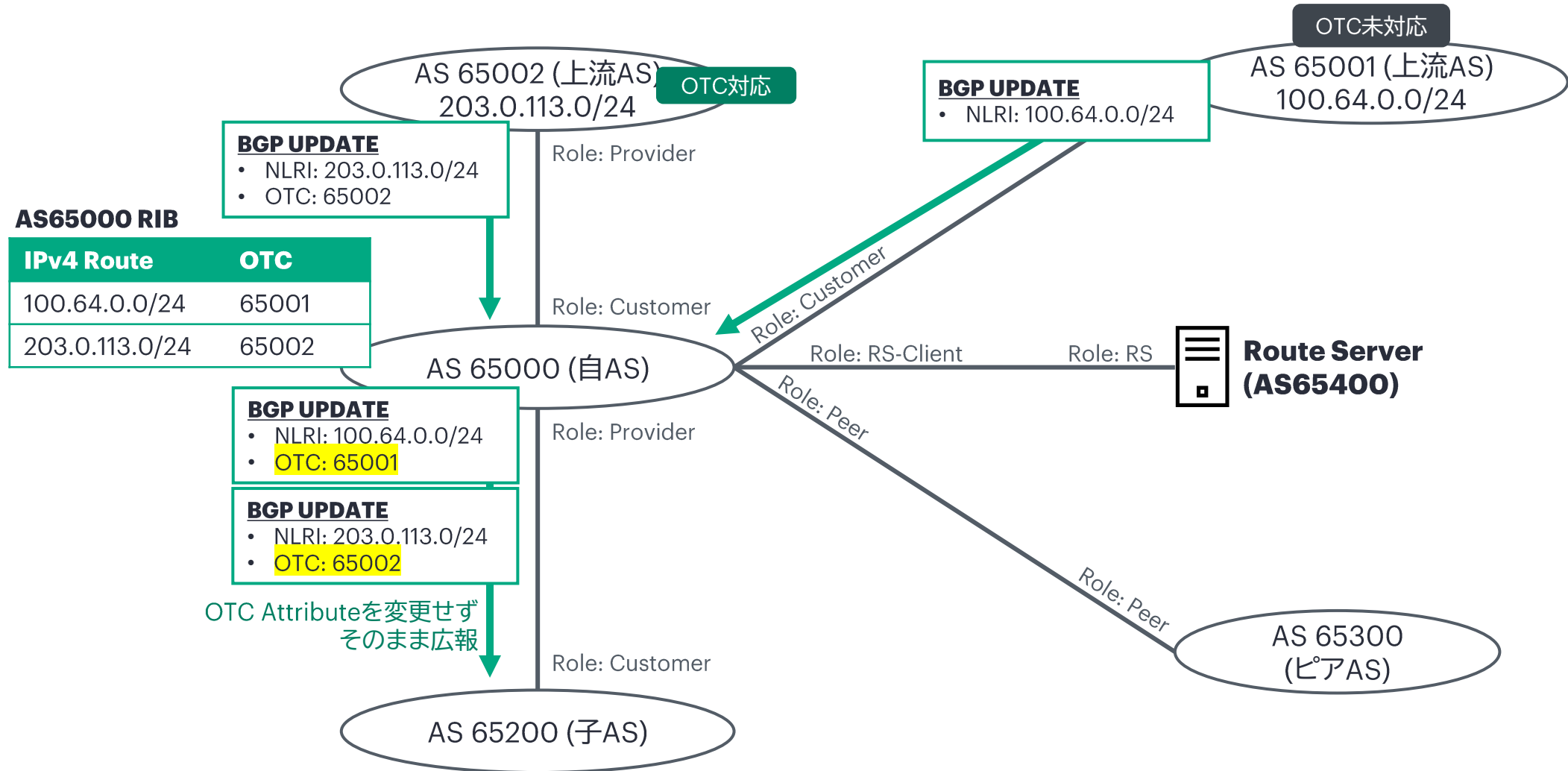
OTC未対応のASから経路を受信した際や、RSが経路を広報する際にもOTCが付与されるケースがある



*ただし、OTCを付与するのはOTCが既に付与されていない場合に限る

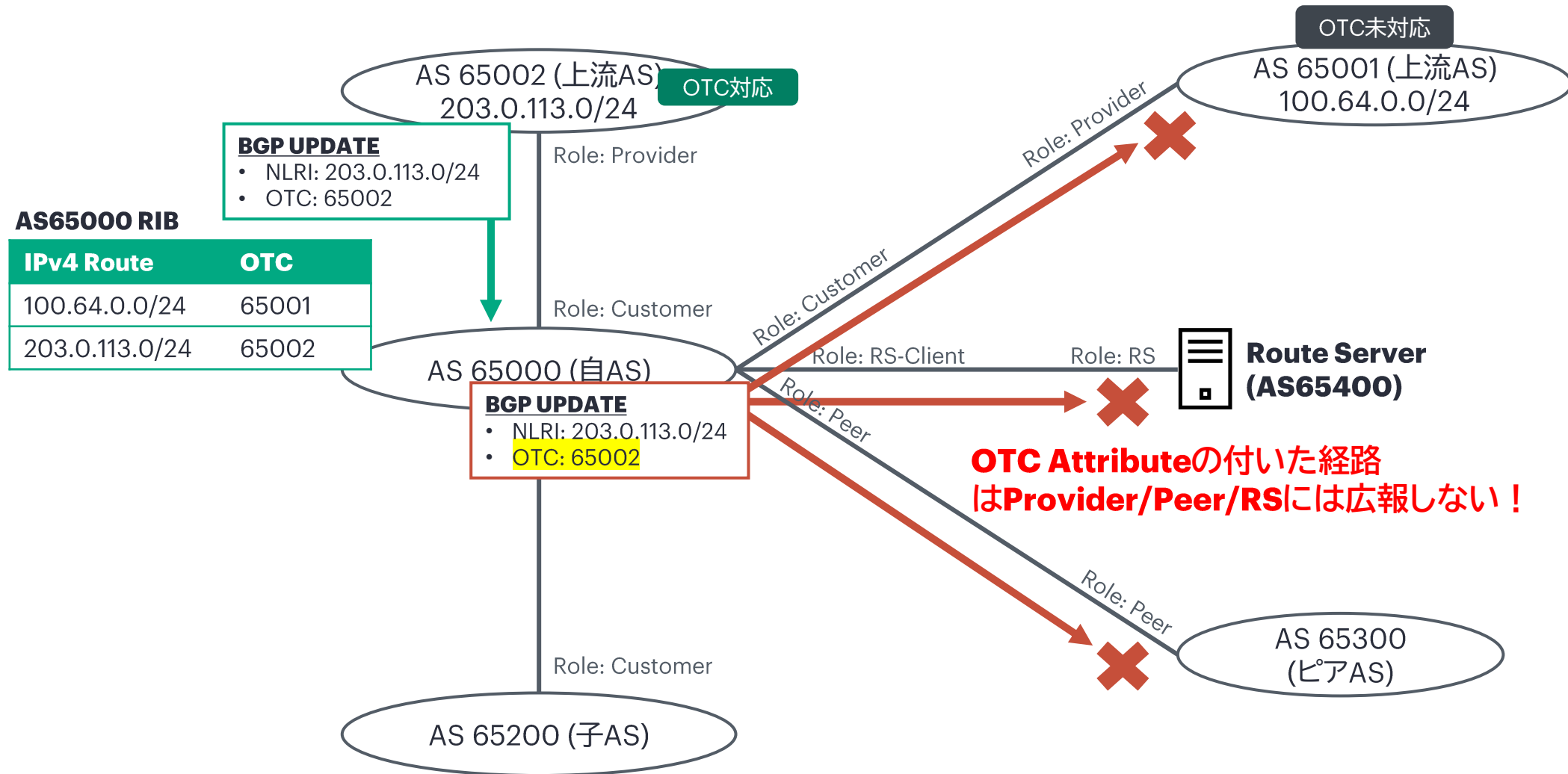
OTCが付与された経路の広報: Customer

経路をOTCの値を維持したまま広報する



OTCが付与された経路の広報: Provider/RS/Peer

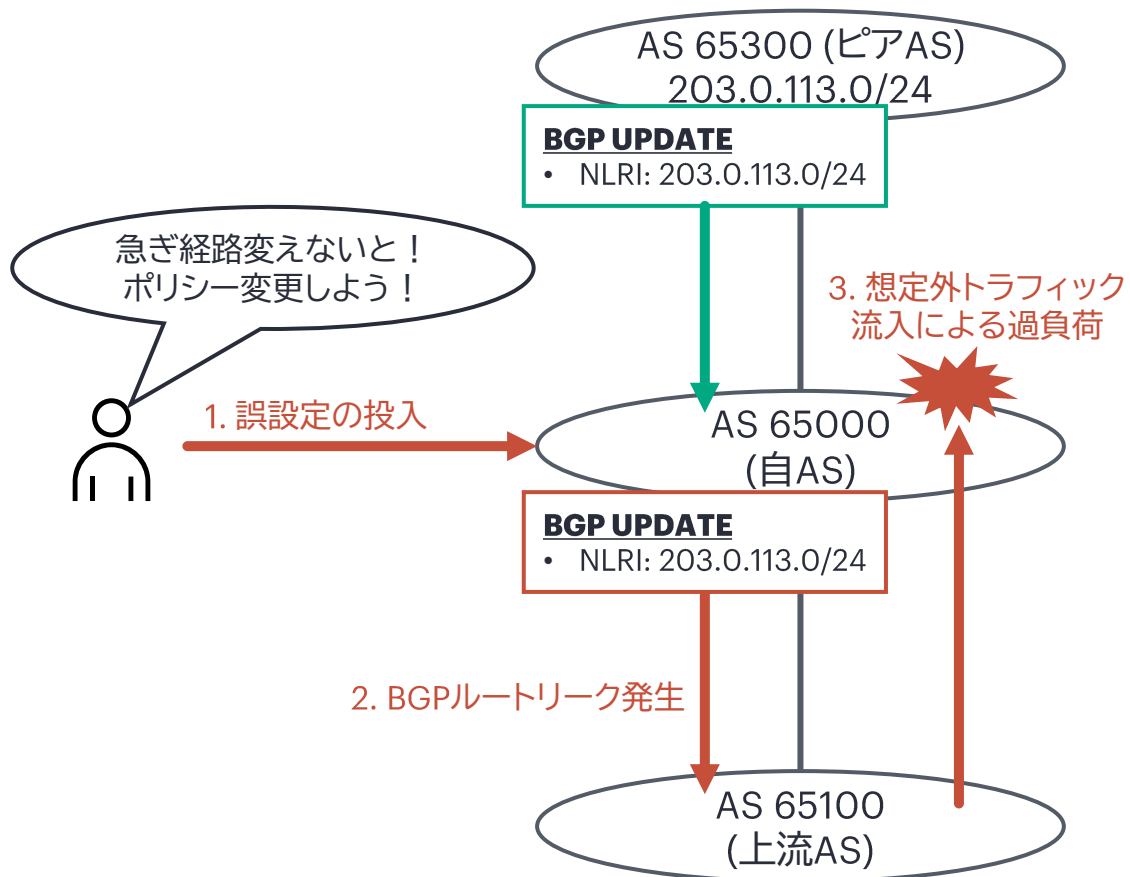
OTCでマークされた経路はRoleが“Provider”, “RS”, “Peer”のピアに対しては広報しない



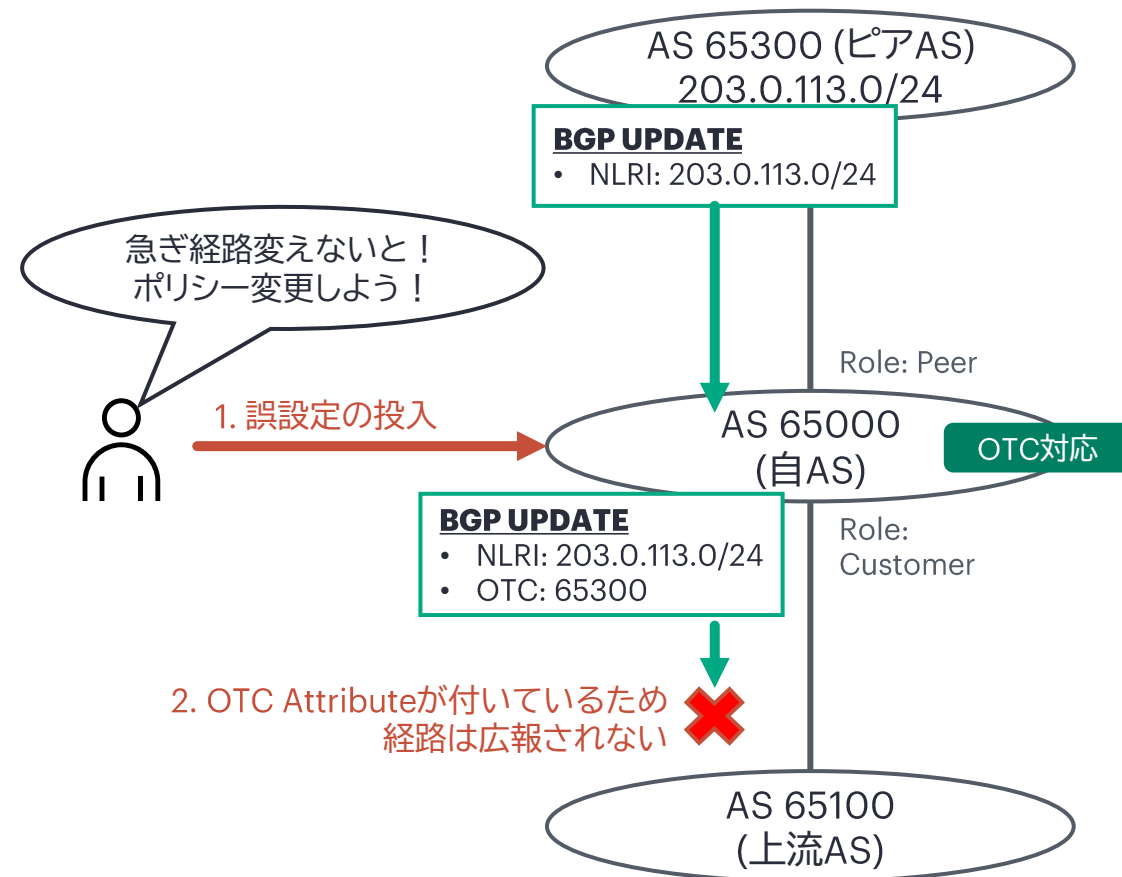
RFC 9234を入れることによるBefore/After

自AS内だけでもRFC 9234対応を行うことで、万が一の設定ミスによるトラブルを防止できる

RFC 9234を導入していない場合

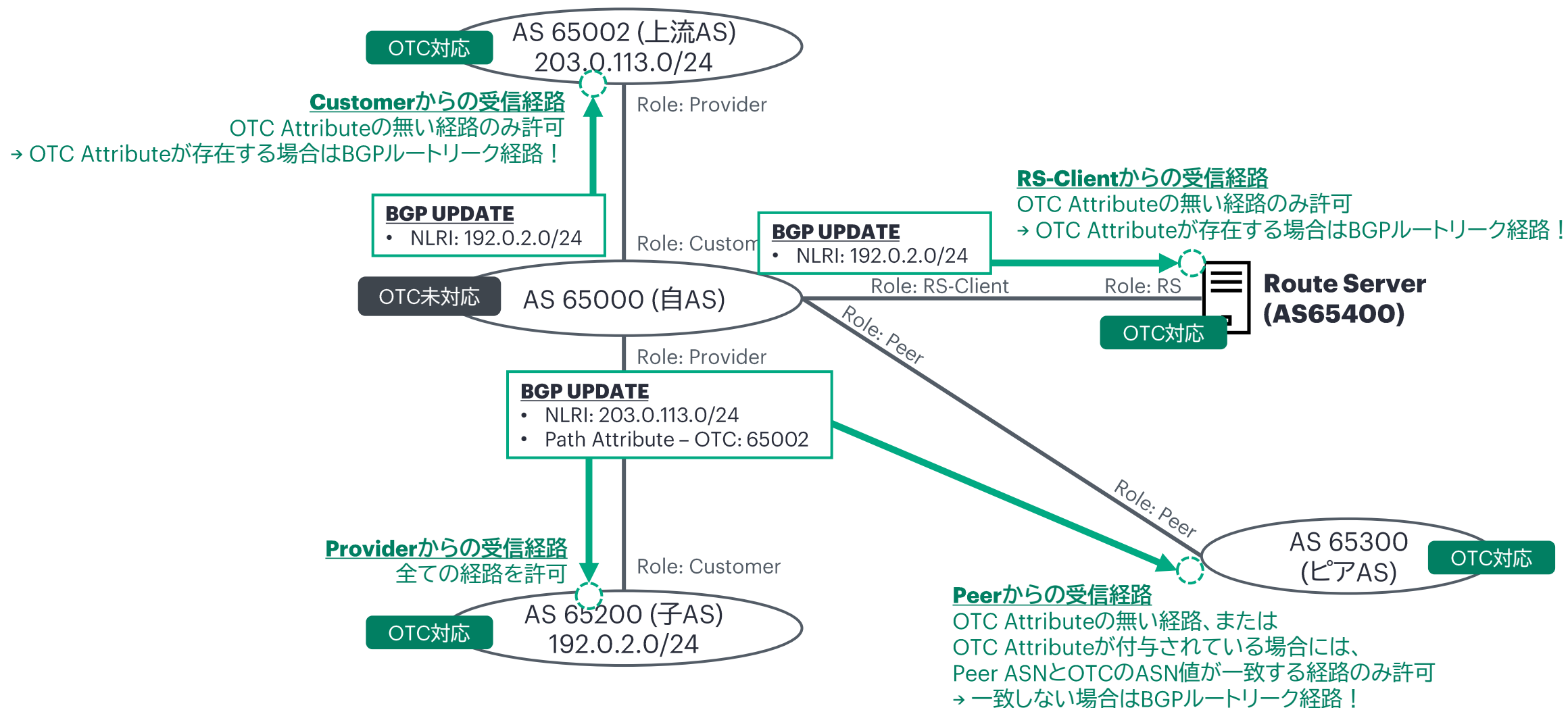


RFC 9234を導入した場合



経路受信側におけるOTCの評価

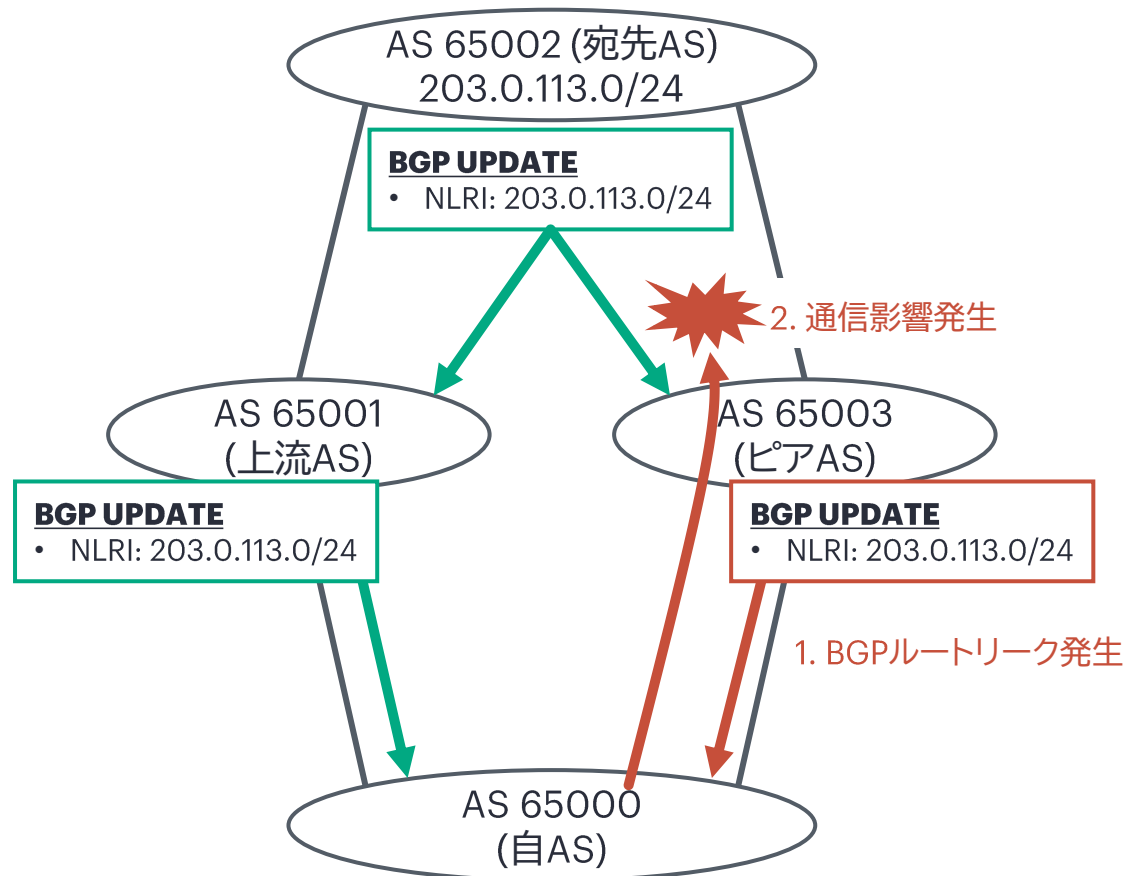
OTCが付与された経路を受信した場合は、受信側でも送信側と同様の評価を行っている



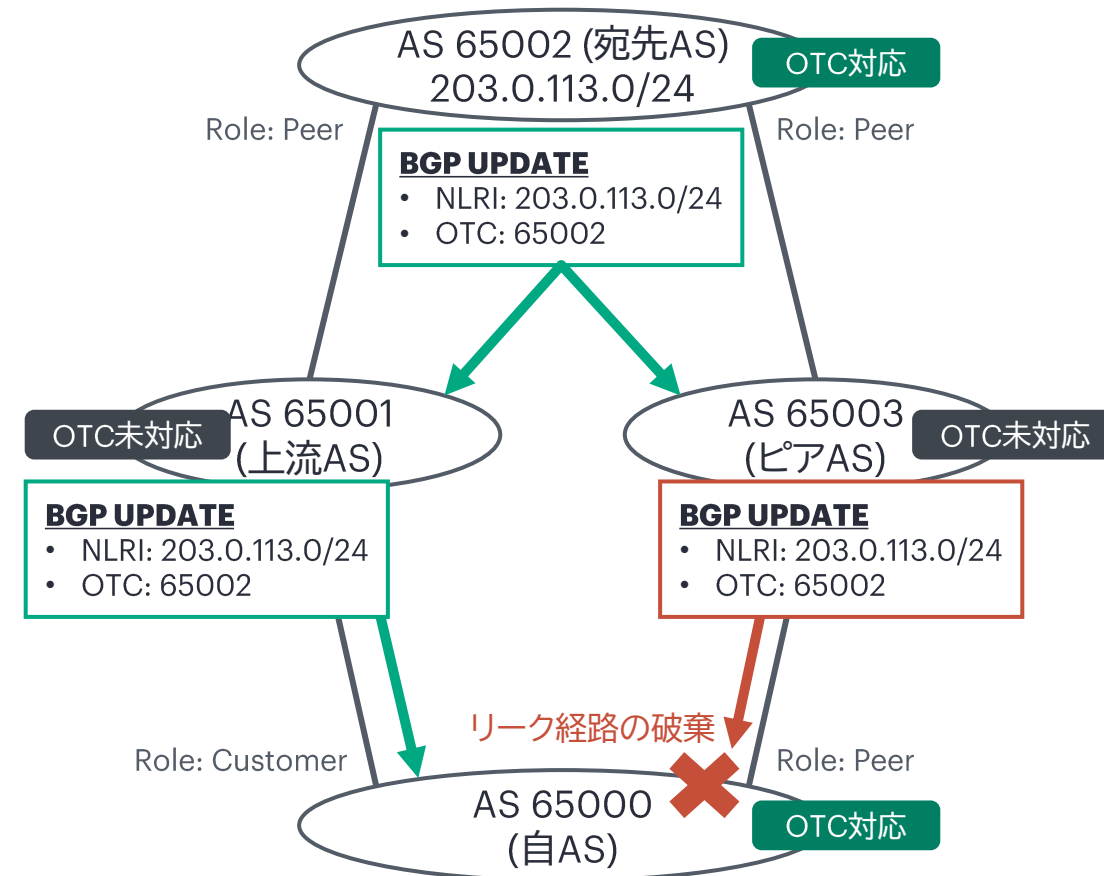
受信側での評価が役立つ例 #1

中継区間がRFC 9234に対応していない場合でもBGPルートリークの影響を阻止できるケースがある

RFC 9234を導入していない場合



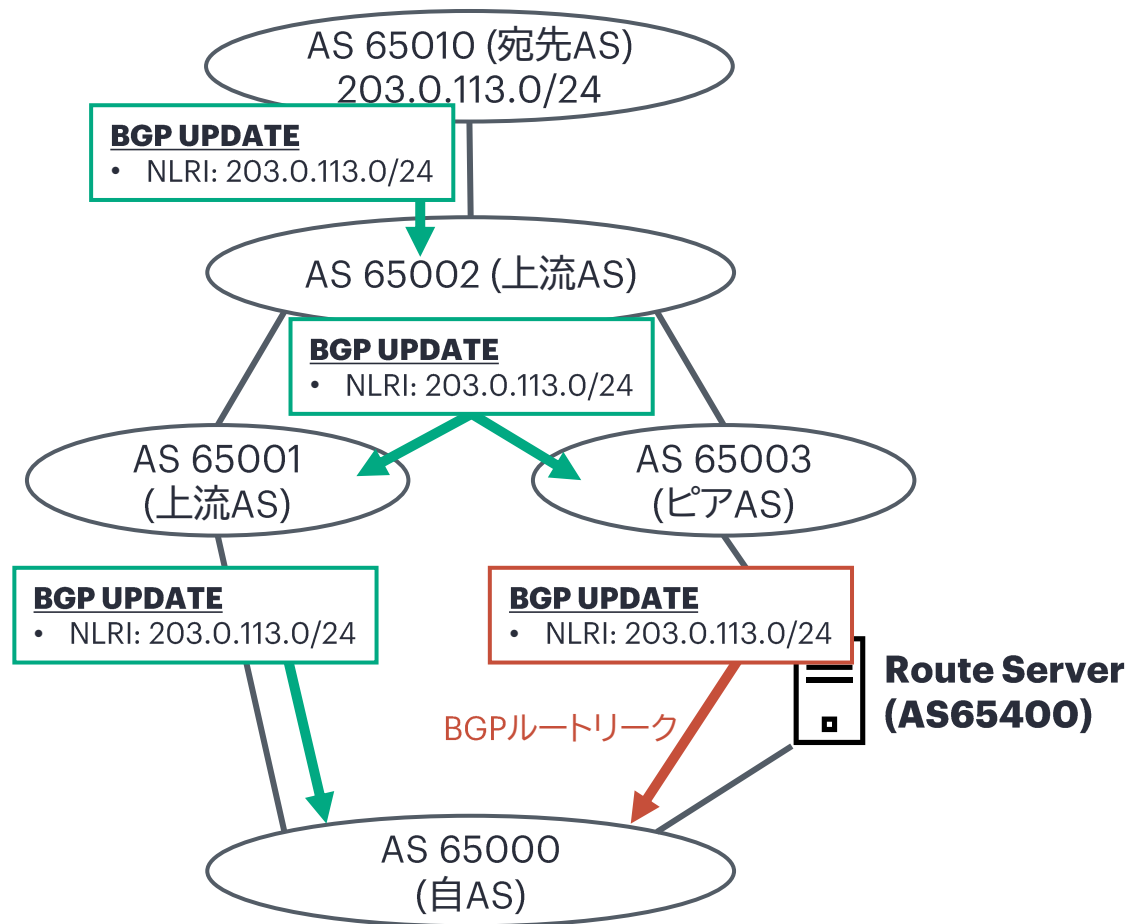
RFC 9234を導入した場合



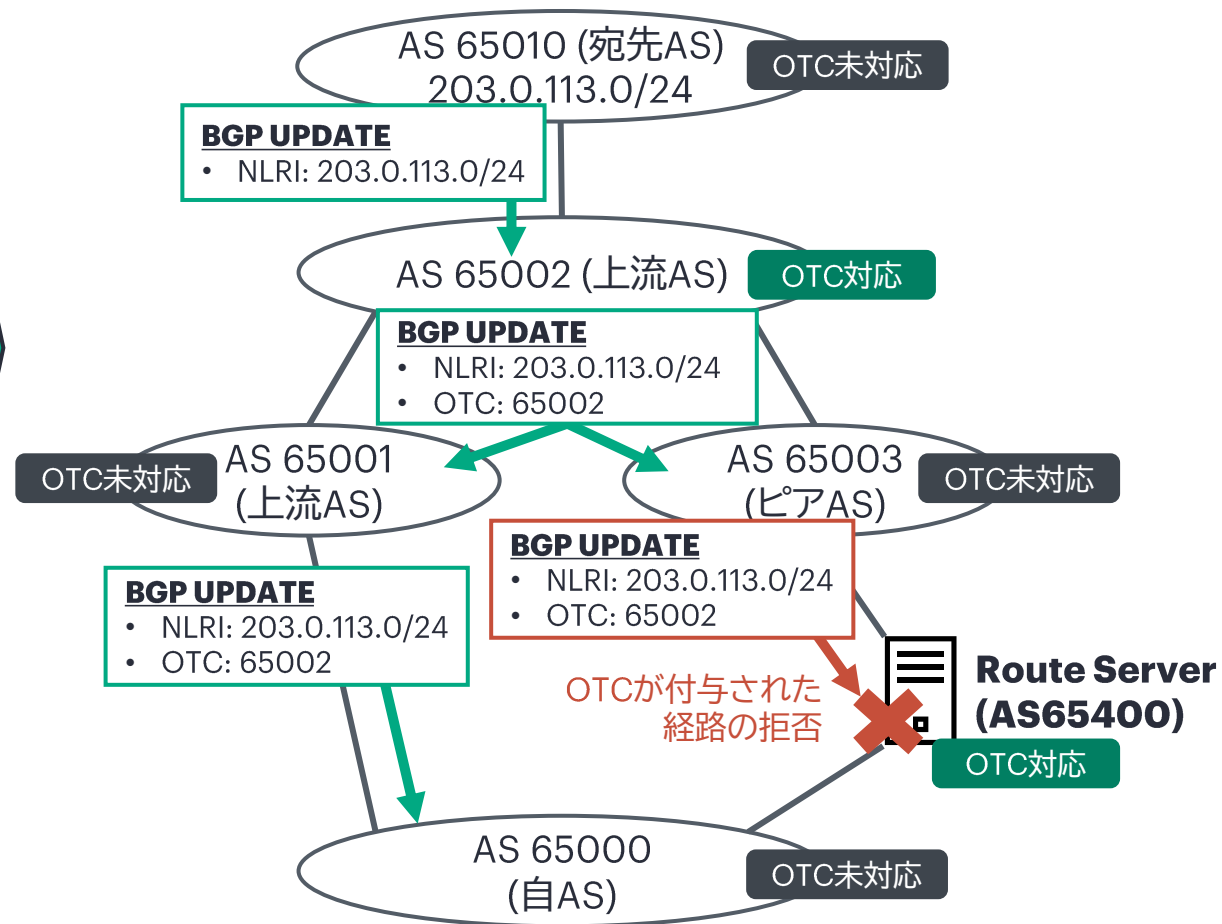
受信側での評価が役立つ例 #2

Route Serverや中継区間がRFC 9234に対応している場合にルートリークから守られるシナリオもある

RFC 9234を導入していない場合

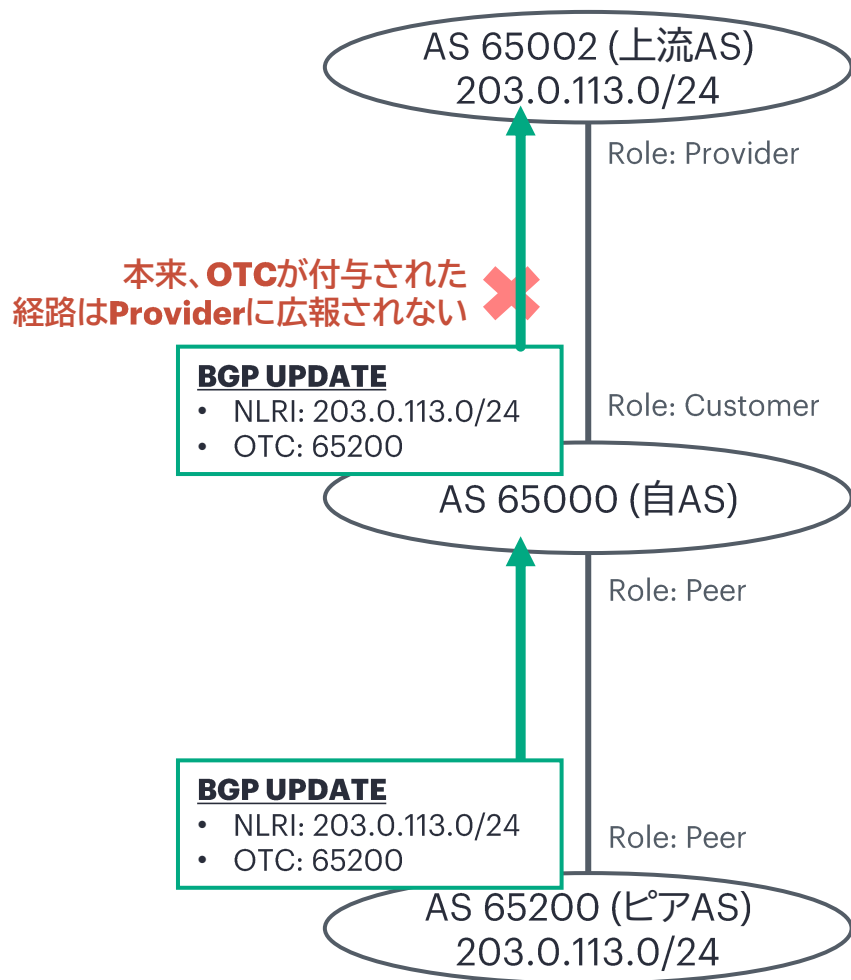


RFC 9234を導入した場合



Route Leakをしたい特殊ケース

RFC 9234では推奨されていないが、特殊ケースに対応できるように柔軟性を持たせてる実装もある



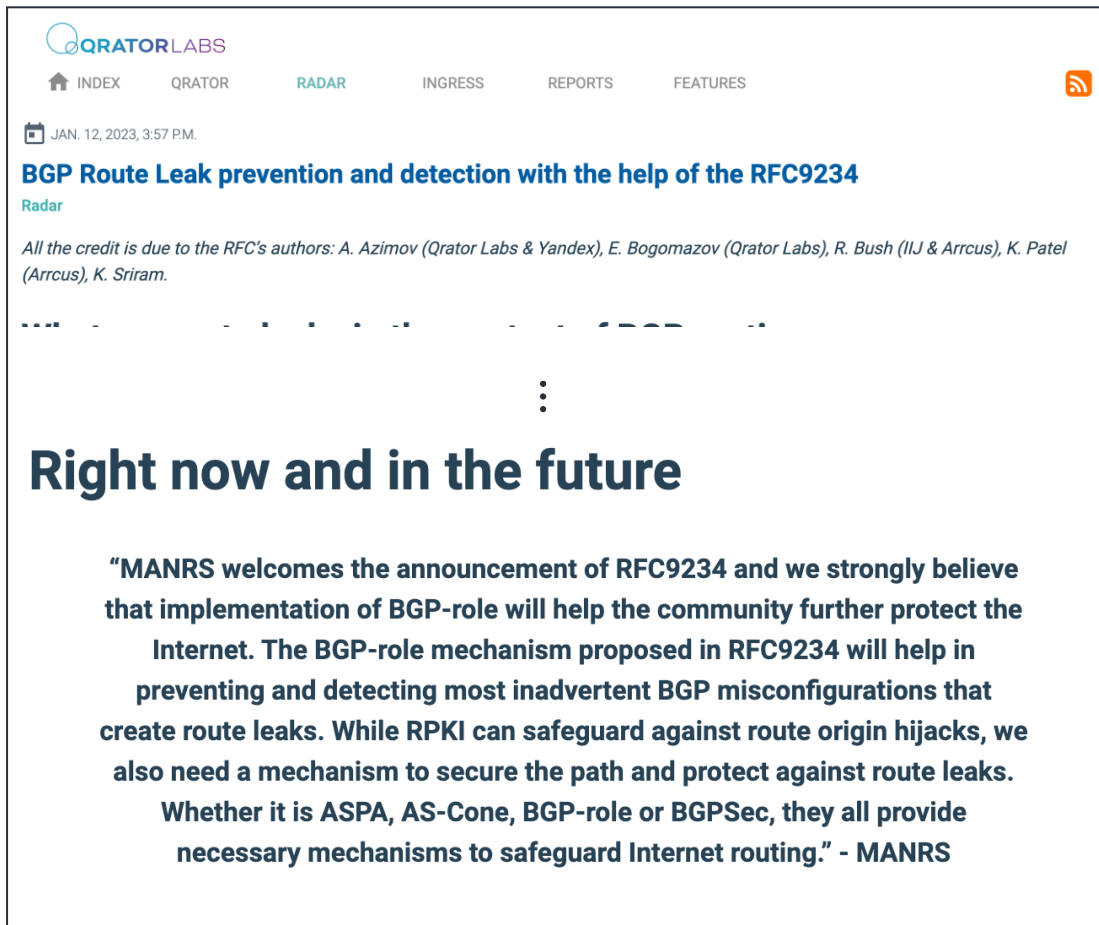
Junosでの例

```
policy-options {
  policy-statement EXPORT-AS65002 {
    term PARTIAL-TRANSIT-OVERRIDE {
      from {
        protocol bgp;
        route-filter 203.0.113.0/24 exact;
      }
      then {
        accept;
        otc-local-role provider;
      }
    }
    term CUSTOMER {
      from {
        protocol bgp;
        community CUSTOMER;
      }
      then accept;
    }
  }
}
```

acceptだけでは広報されない！
特定経路における**OTCのRole**を
変更する必要がある

RFC 9234への期待

BGPルートリークの対策としてRFC 9234に期待している事業者が増えている

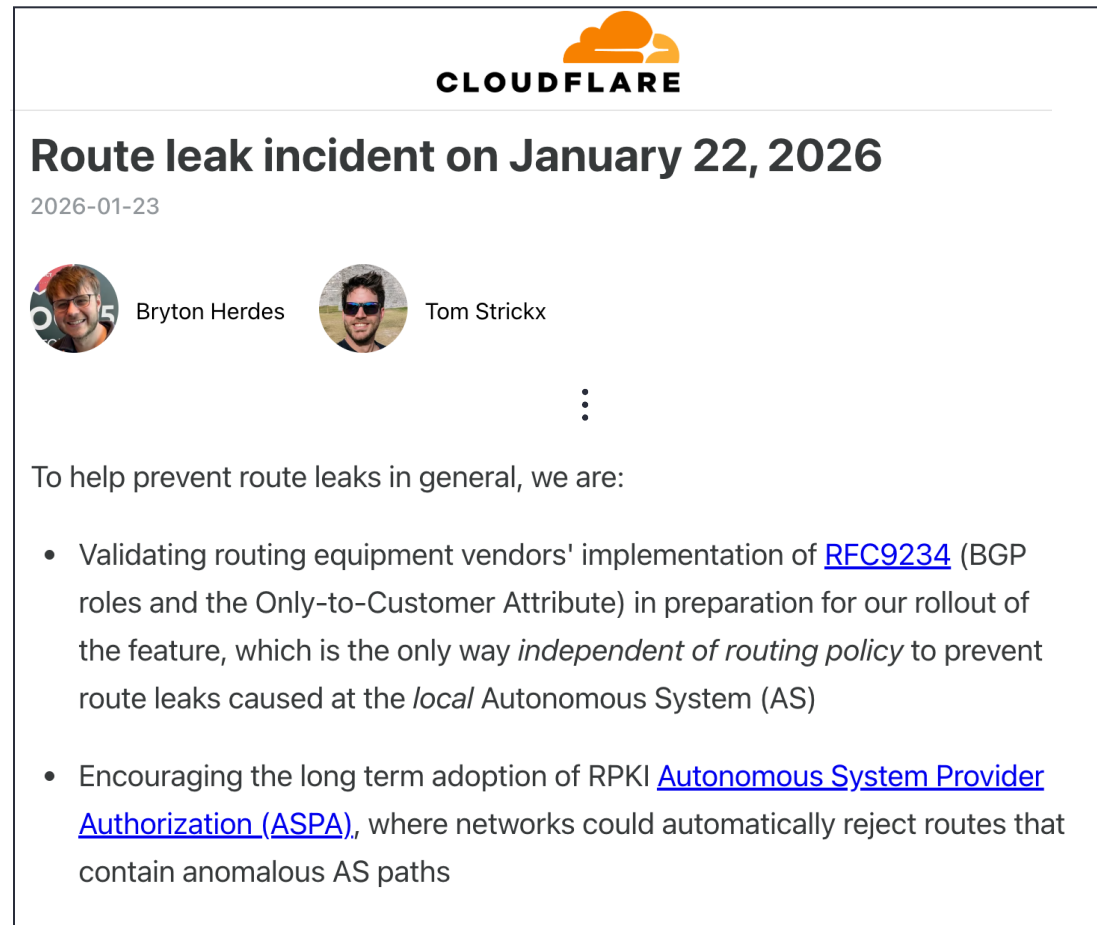


The screenshot shows the top of a blog post from QRATOR LABS. The navigation bar includes links for INDEX, QRATOR, RADAR, INGRESS, REPORTS, and FEATURES. The post title is "BGP Route Leak prevention and detection with the help of the RFC9234" and it is categorized under "Radar". A date stamp indicates it was published on JAN. 12, 2023, at 3:57 P.M. The text credits the RFC authors: A. Azimov (Qrator Labs & Yandex), E. Bogomazov (Qrator Labs), R. Bush (IJJ & Arrcus), K. Patel (Arrcus), and K. Sriram. Below the text, there is a large vertical ellipsis (three dots) and the heading "Right now and in the future".

Right now and in the future

"MANRS welcomes the announcement of RFC9234 and we strongly believe that implementation of BGP-role will help the community further protect the Internet. The BGP-role mechanism proposed in RFC9234 will help in preventing and detecting most inadvertent BGP misconfigurations that create route leaks. While RPKI can safeguard against route origin hijacks, we also need a mechanism to secure the path and protect against route leaks. Whether it is ASPA, AS-Cone, BGP-role or BGPSec, they all provide necessary mechanisms to safeguard Internet routing." - MANRS

出典: https://blog.qrator.net/en/route-leak-prevention-and-detection-rfc9234_162/



The screenshot shows the top of a blog post from CLOUDFLARE. The post title is "Route leak incident on January 22, 2026" and it is dated 2026-01-23. Below the title, there are two circular profile pictures of the authors, Bryton Herdes and Tom Strickx, with a vertical ellipsis (three dots) between them. The text states "To help prevent route leaks in general, we are:" followed by a bulleted list of two points.

Route leak incident on January 22, 2026

2026-01-23

Bryton Herdes Tom Strickx

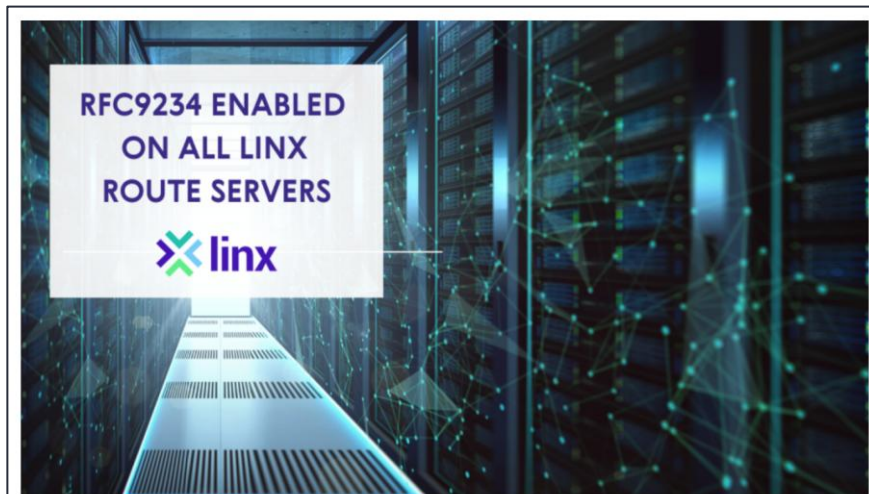
To help prevent route leaks in general, we are:

- Validating routing equipment vendors' implementation of [RFC9234](#) (BGP roles and the Only-to-Customer Attribute) in preparation for our rollout of the feature, which is the only way *independent of routing policy* to prevent route leaks caused at the *local* Autonomous System (AS)
- Encouraging the long term adoption of RPKI [Autonomous System Provider Authorization \(ASPA\)](#), where networks could automatically reject routes that contain anomalous AS paths

出典: <https://blog.cloudflare.com/route-leak-incident-january-22-2026/>

RFC 9234への期待: Internet Exchangeでの採用

RFC9234はLINXやAMS-IX、France IX、MSK-IX、YYCIXなどのRoute Serverで既に導入されている



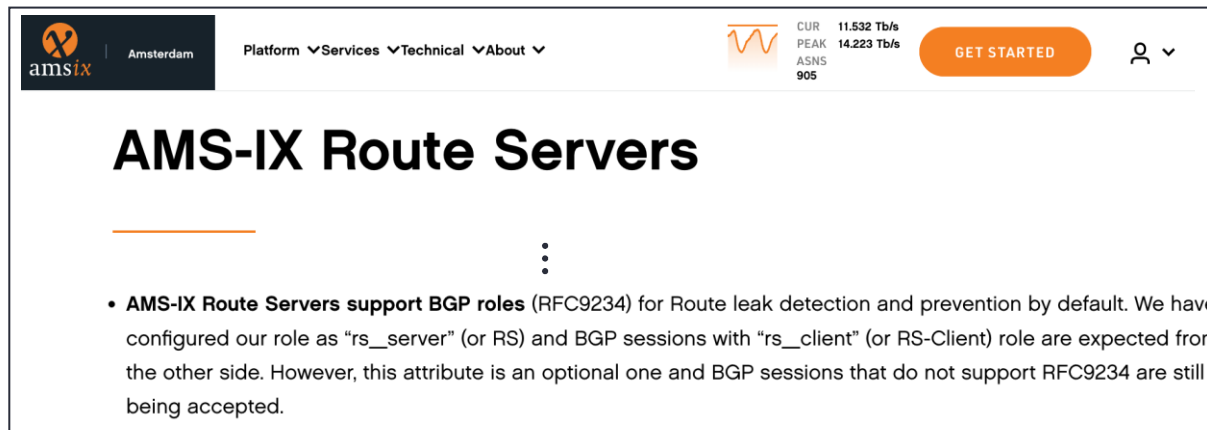
Written by Moyaze Shivji, Senior Network Engineer at LINX

The LINX engineering team has enabled RFC9234 on all LINX Route Servers for the detection and prevention of BGP route leaks, usually caused by errors and misconfigurations.

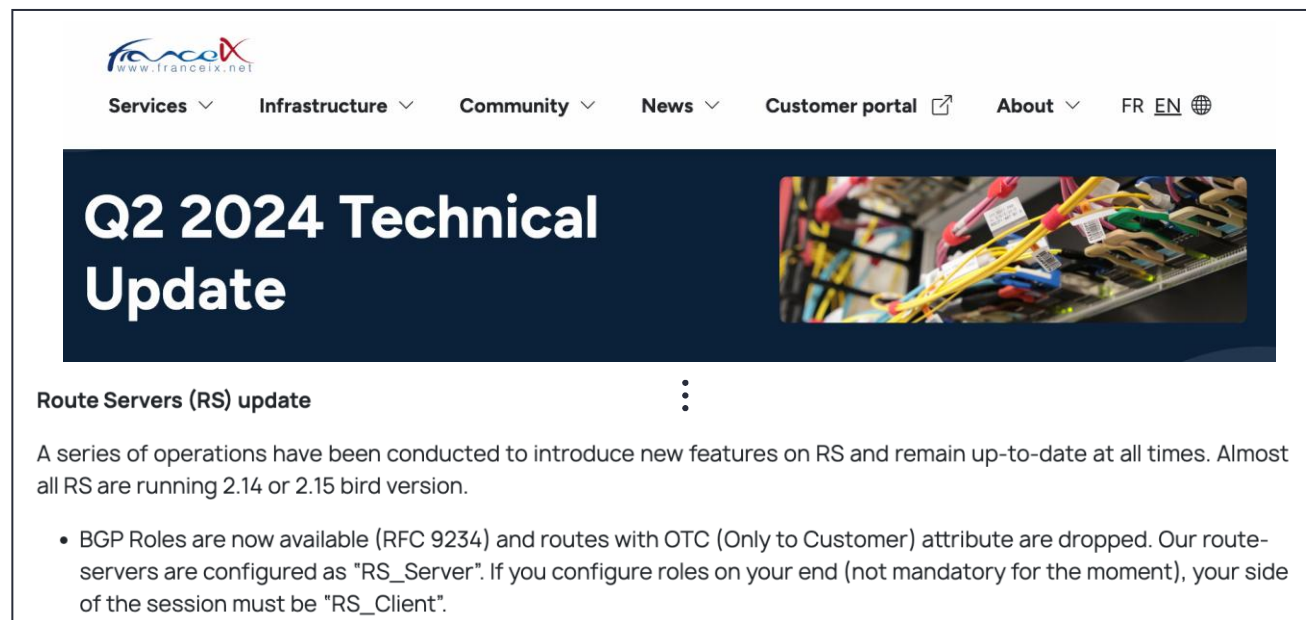
RFC (Request for Comments) – a formal document that can outline technical specs and protocols.

出典:

1. LINX: <https://www.linx.net/rfc9234-enabled-on-linx-route-servers/>
2. AMS-IX: <https://www.ams-ix.net/ams/documentation/ams-ix-route-servers>
3. France-IX: <https://www.franceix.net/en/infrastructure/techhub/rapport-technique-t2-2024/>



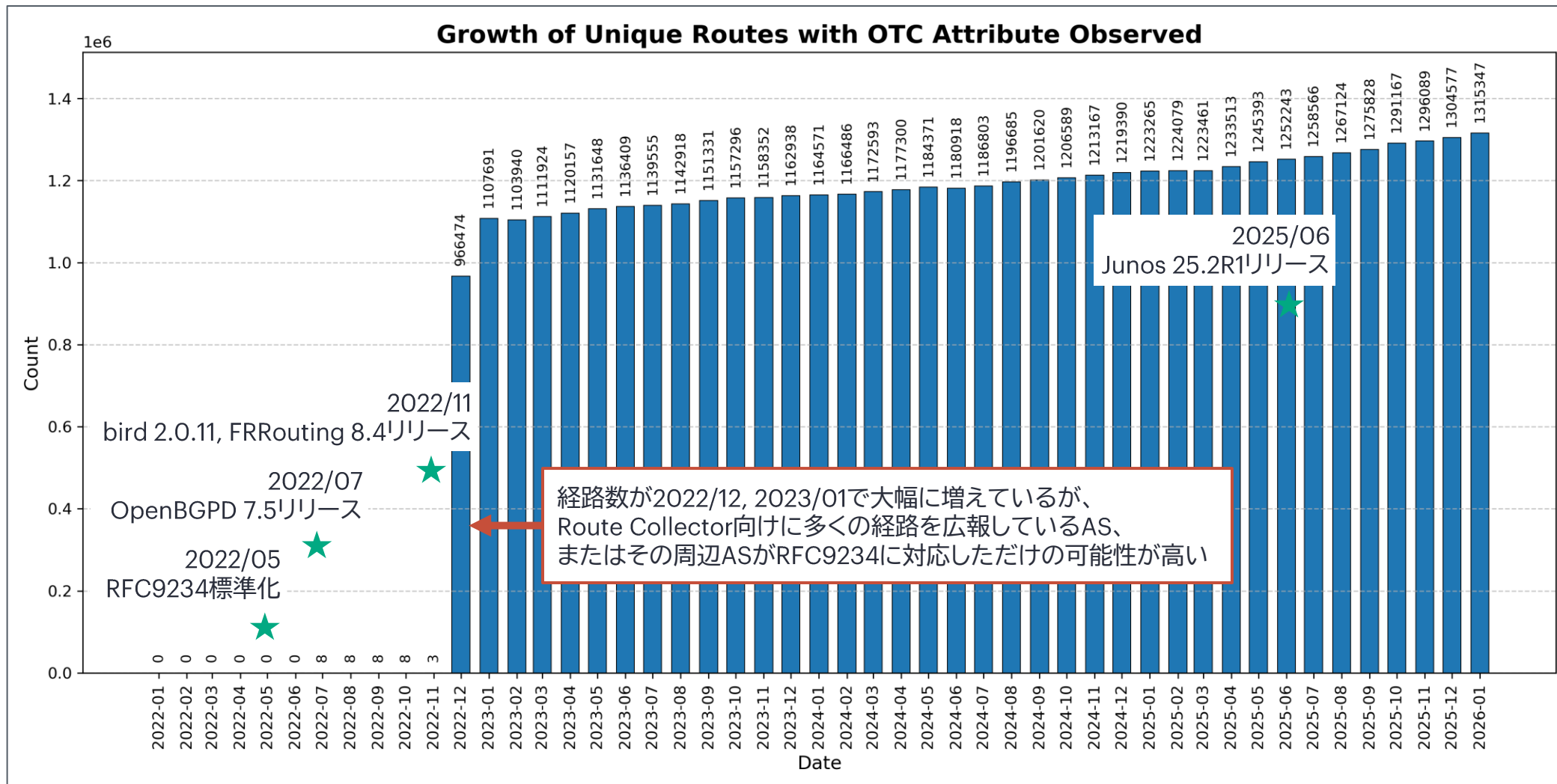
The screenshot shows the AMS-IX website header with navigation links (Platform, Services, Technical, About) and a status bar displaying current traffic (11.532 Tb/s) and peak traffic (14.223 Tb/s). The main heading is 'AMS-IX Route Servers'. Below it, a bulleted list states: 'AMS-IX Route Servers support BGP roles (RFC9234) for Route leak detection and prevention by default. We have configured our role as "rs_server" (or RS) and BGP sessions with "rs_client" (or RS-Client) role are expected from the other side. However, this attribute is an optional one and BGP sessions that do not support RFC9234 are still being accepted.'



The screenshot shows the FranceIX website header with navigation links (Services, Infrastructure, Community, News, Customer portal, About) and language options (FR, EN). The main heading is 'Q2 2024 Technical Update'. Below it, a section titled 'Route Servers (RS) update' contains the text: 'A series of operations have been conducted to introduce new features on RS and remain up-to-date at all times. Almost all RS are running 2.14 or 2.15 bird version.' A bulleted list follows: 'BGP Roles are now available (RFC 9234) and routes with OTC (Only to Customer) attribute are dropped. Our route-servers are configured as "RS_Server". If you configure roles on your end (not mandatory for the moment), your side of the session must be "RS_Client".'

RFC 9234への期待: OTC Attributeの付いた経路数の推移

IPv4/IPv6のBGP Full Route上にOTC Attribute付きの経路が存在し、増加傾向にあることが分かる



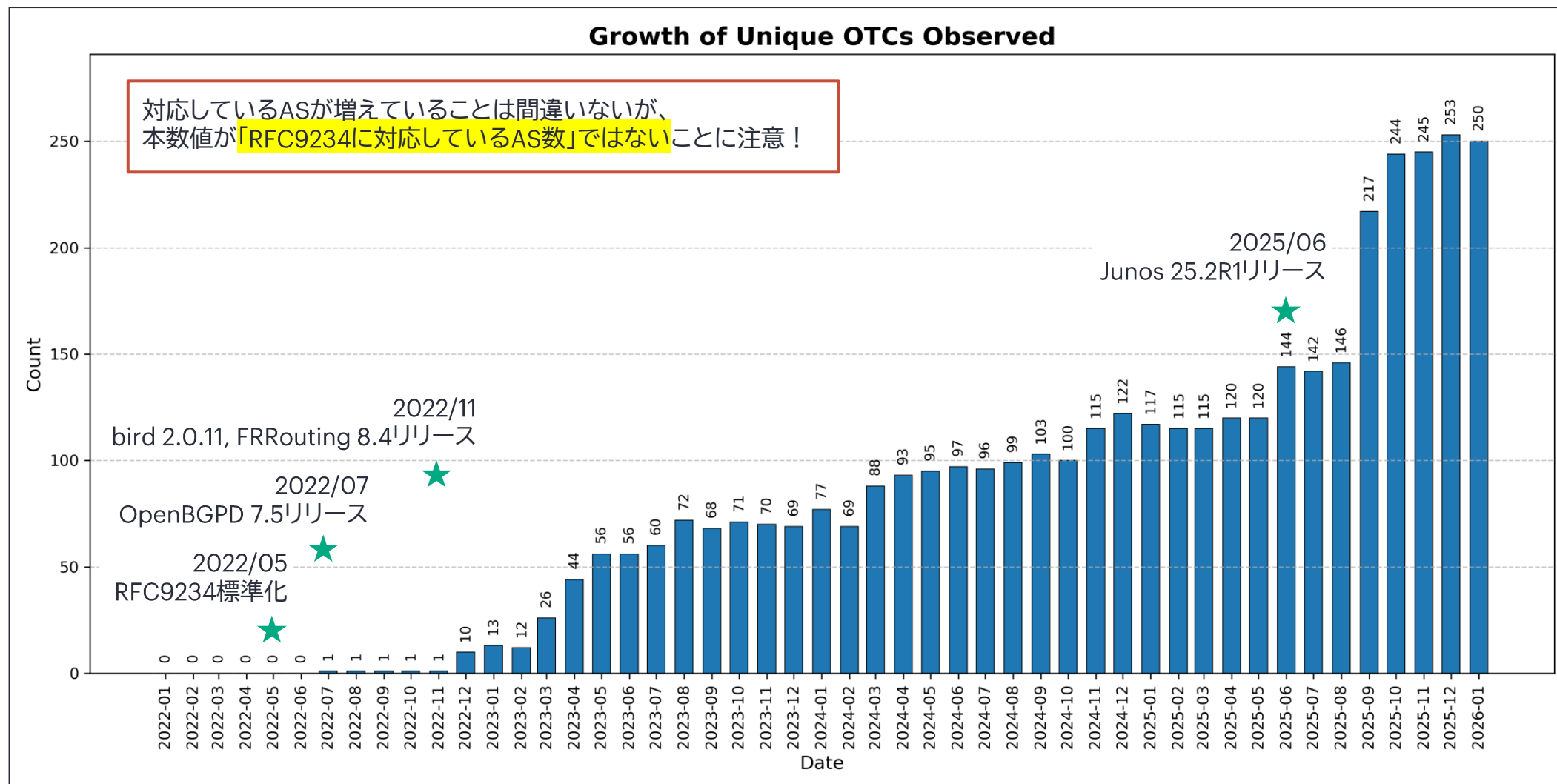
*1. 以下、合計23のRoute Collector上のデータより算出:

rrc00, rrc01, rrc03, rrc04, rrc05, rrc06, rrc07, rrc10, rrc11, rrc12, rrc13, rrc14, rrc15, rrc16, rrc18, rrc19, rrc20, rrc21, rrc22, rrc23, rrc24, rrc25, rrc26

*2. データは月末日 0:00 UTCのものを利用

RFC 9234への期待: OTCとして出現するAS数の推移

IPv4/IPv6のBGP Full Routeに存在するOTCとして出現するAS数も増加傾向にある



*1. 以下、合計23のRoute Collector上のデータより算出:

rrc00, rrc01, rrc03, rrc04, rrc05, rrc06, rrc07, rrc10, rrc11, rrc12, rrc13, rrc14, rrc15, rrc16, rrc18, rrc19, rrc20, rrc21, rrc22, rrc23, rrc24, rrc25, rrc26

*2. データは月末日 0:00 UTCのものを利用

RFC 9234を導入しているASを見つけるには

抜け漏れは発生する可能性はあるが、以下手法を使い、高確率でRFC 9234を導入しているASを検出
(より良い方法を思いついた方は教えてください・・・！ & メモリーが大量に必要にならない方法)

1. AS_PATH上にOTCの値が存在しないパターンを抽出 => Route ServerがRFC 9234対応の可能性
 1. 同じOTCの値が入っているAS Pathのパターンを全て抽出
 2. 同じASが全パターンに存在するか確認 => データセットが不十分のため判断不能
 3. 頻出するASの上位2つのASが全パターンに存在するか確認 => 恐らくRoute Server以外だがデータ不十分
 4. 上記にマッチしないもの => Route Serverが高確率で対応している
2. AS_PATHの最も左にいるASがOTCの値と一致しているパターンを抽出 => RFC 9234を高確率でサポート
3. Origin ASとOTCの値が一致している経路を抽出
=> Origin ASまたはOrigin ASのPeer/CustomerがOTCをサポート
 1. Origin AS (X)のTransit AS (P)を検出 (1つの経路に対してOrigin ASの次に来るASが複数のAS Pathに存在している)
 2. PがOrigin ASとなっている経路のAS Pathパターンを抽出
 1. PのTransit AS (P')を検出 -> AS PathパターンからP'が含まれるものを除外
 2. 残るAS Pathの全てがOTC == Pとなっているか確認 -> 正であれば、PはRFC 9234対応
 3. XがOrigin ASとなっている経路のAS Pathパターンを抽出
 1. AS PathパターンからPが含まれるものを除外
 2. 残るAS Pathの全てがOTC == Xとなっているか確認 -> 正であれば、XはRFC 9234対応

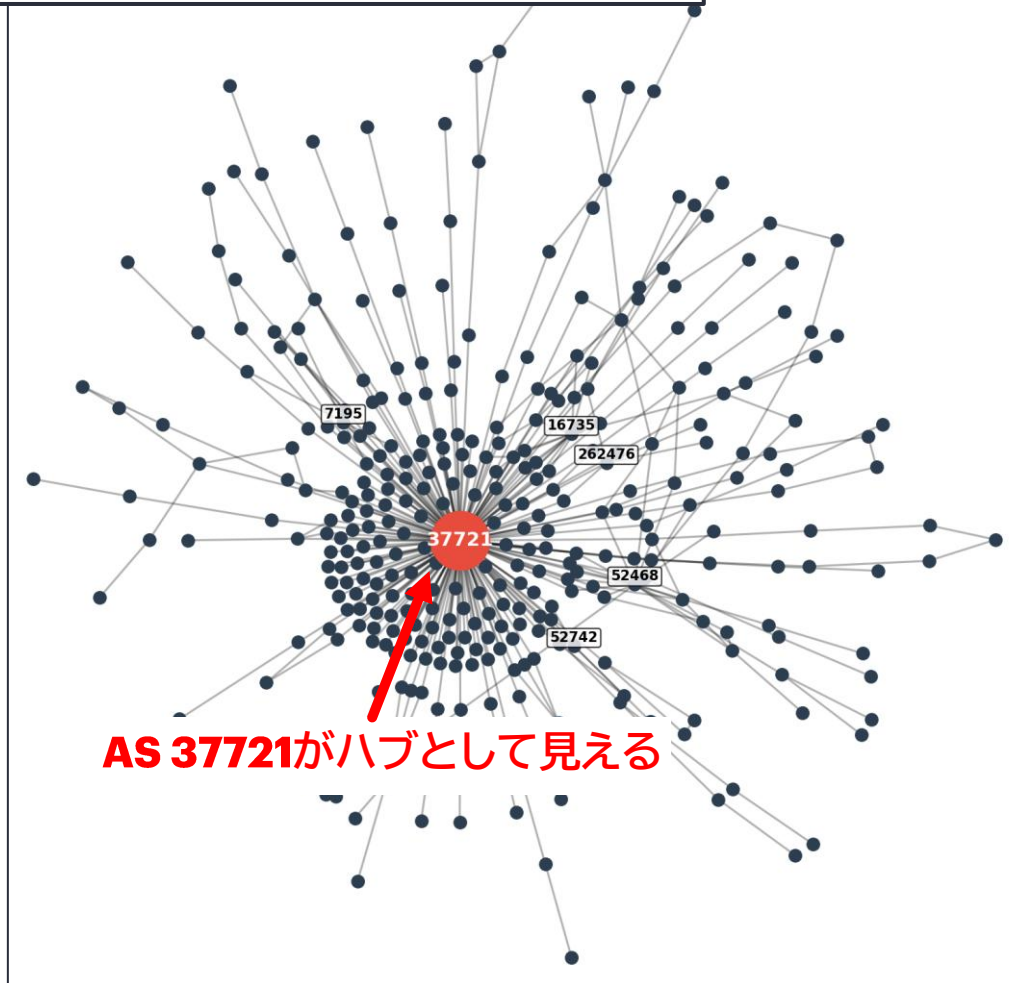


説明は割愛します

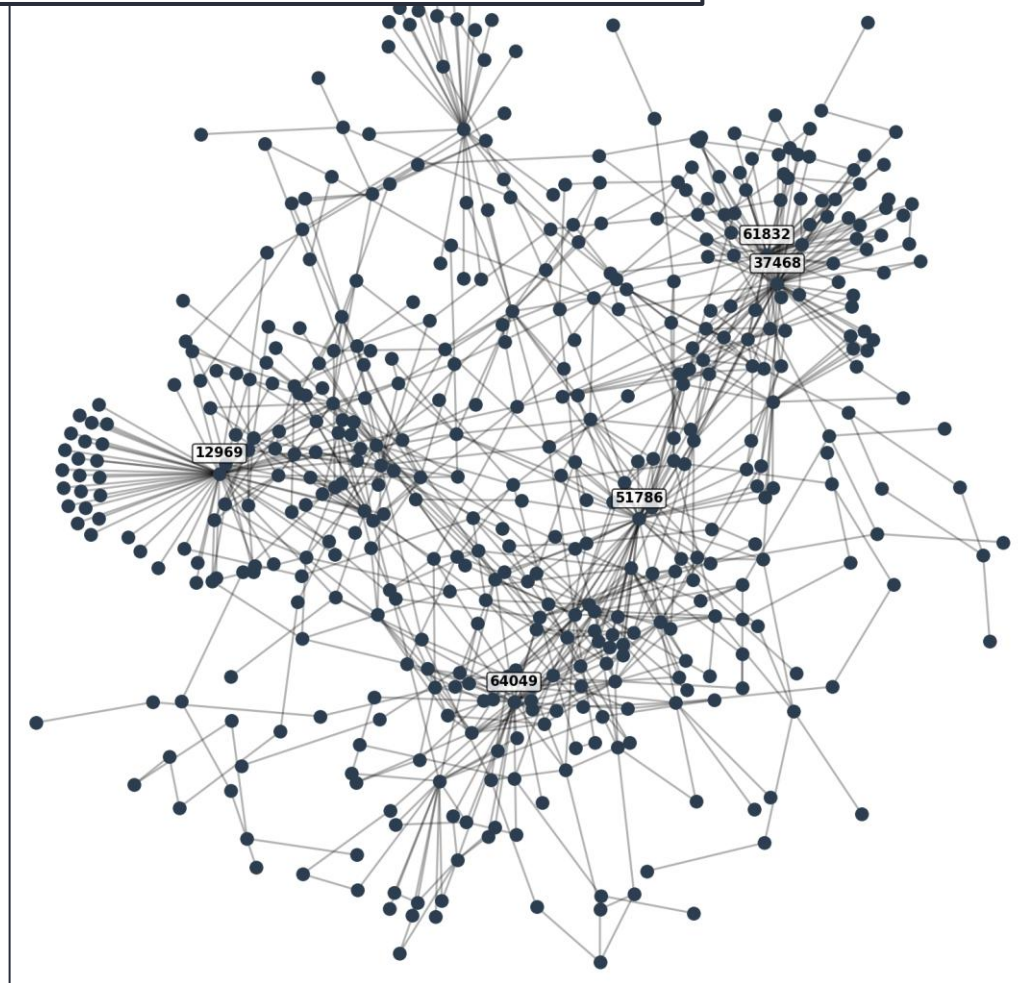
RFC9234に対応したIX Route Serverの検出

ハブとなるASが存在しない場合にはIXのRoute Server自体がRFC 9234に対応していると考えられる

“OTC==26162” で見える経路のAS_PATH

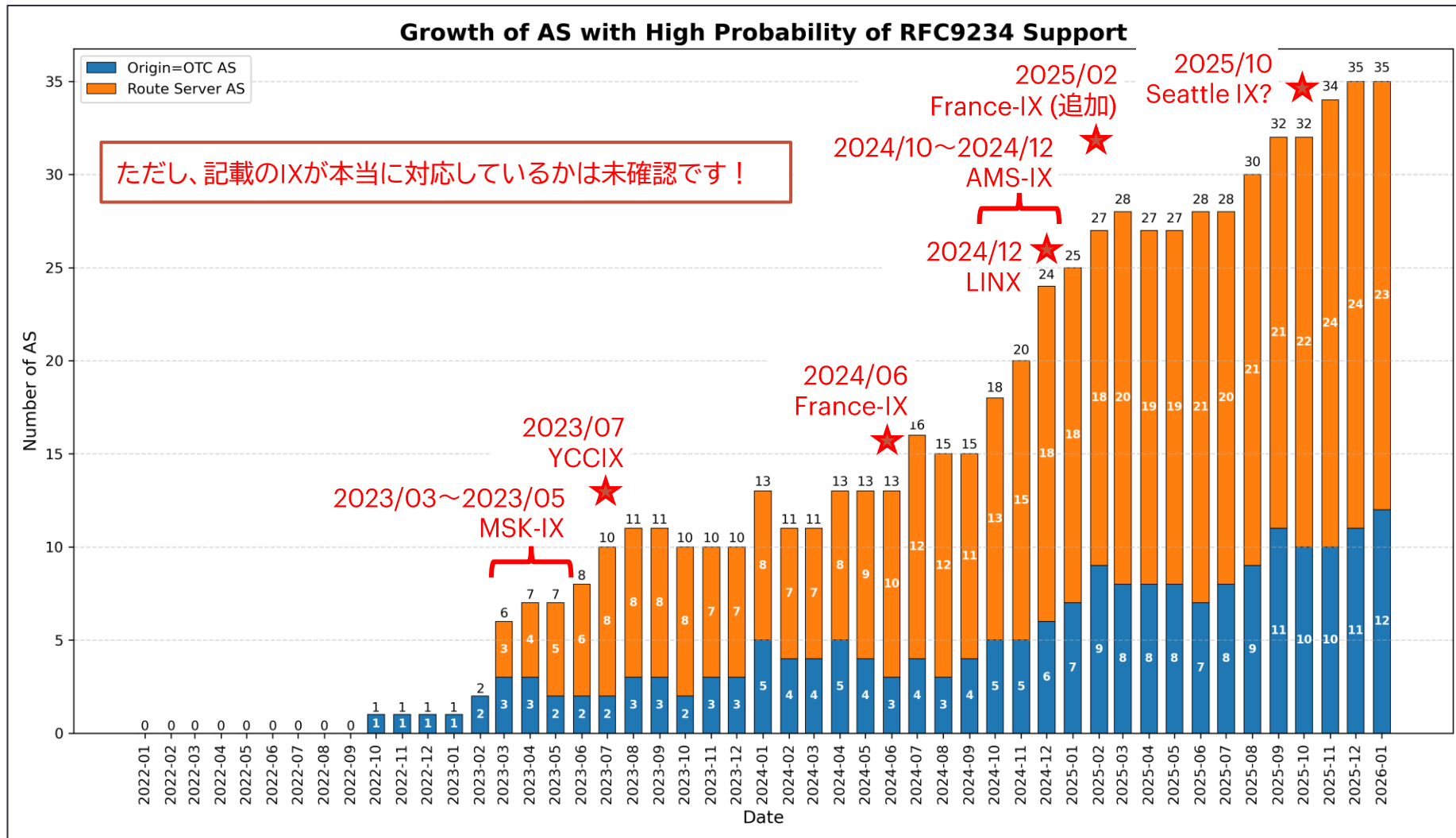


“OTC==8714” で見える経路のAS_PATH



RFC 9234への期待: RFC9234導入済みASの予測

RIPEのMRTデータから高い確率でRFC 9234に対応しているASを抽出 (多少の誤判定はある)



*1. 以下、合計23のRoute Collector上のデータより算出:

rrc00, rrc01, rrc03, rrc04, rrc05, rrc06, rrc07, rrc10, rrc11, rrc12, rrc13, rrc14, rrc15, rrc16, rrc18, rrc19, rrc20, rrc21, rrc22, rrc23, rrc24, rrc25, rrc26

*2. データは月末日 0:00 UTCのものを利用

RFC 9234は完璧か？

RFC 9234のデザイン思考

- シンプルなアプローチで大多数の設定ミスによるBGPルートリークを解決する
- 守る範囲は自ASと自ASと関係性の近いAS
- シンプルが故に複雑なピアリング関係で適用することは非推奨
“Roles MUST NOT be configured on an eBGP session with a Complex peering relationship.”

RFC9234が対象としていない問題

- BGPハイジャック (IP Prefixの不正広報) -> RPKI ROA
- 自ASから遠く離れた場所のBGPルートリーク, 悪意のある意図的なBGPルートリーク -> ASPA
- AS_PATHの改ざん -> BGPsec

RFC 9234の課題

- RFC 9234をサポートしており、OSが成熟状態のキャリアグレードルータが存在しない (調べた限りでは)
 - 例. Junos 25.2R1にてサポート、商用環境向けのR2は未リリース ☹
 - 現時点でRFC 9234を導入しているASの多くは恐らく「実験 (+ホビー) AS」または「Internet Exchange」
(つまり、BirdやOpenBGPDなどのソフトウェアベースのBGPデーモンで動いてそうなところ)



RPKI Route Origin Validation (ROV)

BGPルータがROA (Route Origin Authorization) を使って経路のOrigin ASが正しいことを検証

RIR/LIR/ISP



1. リソース証明書の発行

リソース証明書



Corp ABC
203.0.113.0/24

2. ROA署名

203.0.113.0/24
AS65200, maxLen /24

101
010

ROA

Relying Party



3. ROAの電子署名検証

4. 検証済みROAの取得
(RTRプロトコル)

AS 65000 (自AS)

BGP UPDATE

• NLRI: 203.0.113.0/24

AS_PATH: 65102 65101 65200

AS 65200
203.0.113.0/24

AS65101

AS65102

AS 65300
(不正AS)

BGP UPDATE

• NLRI: 203.0.113.0/24

AS_PATH: 65110 65300

AS65110

IPv4 Route	AS Path	Validation State
203.0.113.0/24	65102 65101 65200	Valid
	65110 65300	Invalid

5. ROA情報との整合性確認

Autonomous System Provider Authorization (ASPA)

BGPルータがRPKIで署名されたASPAオブジェクトを使って経路のAS Pathの正当性を検証

RIR/LIR/ISP



1. リソース証明書の発行

リソース証明書

Corp ABC
AS65200

2. ASPA署名

AS65200
Providers: 65101 (v4)

101
010

ASPA

Relying Party



3. ASPAの電子署名検証

4. 検証済みASPAの取得
(RTRプロトコル)

AS 65000 (自AS)



IPv4 Route	AS Path	Validation State
203.0.113.0/24	65102 65101 65200	Valid
203.0.113.0/24	65104 65103 65101 65200	Invalid

5. ROA情報との整合性確認

BGP UPDATE

• NLRI: 203.0.113.0/24

AS 65200
203.0.113.0/24

Transit

AS65101

Peer

AS65102

Peer

AS65103

Peer

AS65104

BGP UPDATE

• NLRI: 203.0.113.0/24

BGPルートリーク

→ “Valley-Free Routing”に違反するルート

まとめ

設定ミスによるBGPルートリークをRFC 9234で撲滅しましょう！

RFC 9234

- 昨今発生しているBGPルートリークの大多数は設定ミスによるもの
→システムとしてBGPルートリークが起きない「防波堤」のような仕組みが必要
- RFC 9234はシンプルなアプローチで大多数のBGPルートリークを防止する
 - BGPの仕組みにピア同士の「関係性」情報を入れ込む
 - BGPセッション確立時に関係性を確認
 - 経路交換時に、関係性の情報を元に交換して良い経路かシステムとして判断
- 既に一部のASやInternet Exchangeなどでは導入され始めている

ディスカッションポイント

- 現在、皆様が導入しているBGPルートリークに対する対策
- RFC 9234はBGPルートリークに有用だと思いますか？
- 各社ベンダーでの実装が進んだ後にRFC 9234を導入したいと思いますか？



Thank You

A photograph of two workers, a woman and a man, walking away from the camera on a dirt path in a field. They are both wearing white hard hats and high-visibility yellow safety vests over dark shirts. The woman is holding a tablet. The background shows a vast, open landscape with low-lying vegetation under a clear sky. A large green rectangular overlay covers the left side of the image, containing the text 'Thank You'.