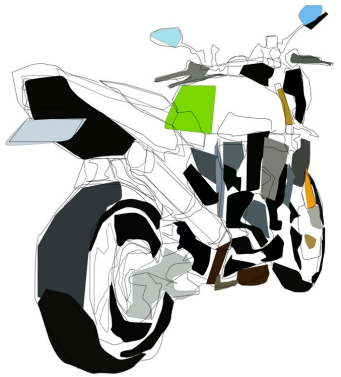
ASPA導入・運用における問題点に関する考察

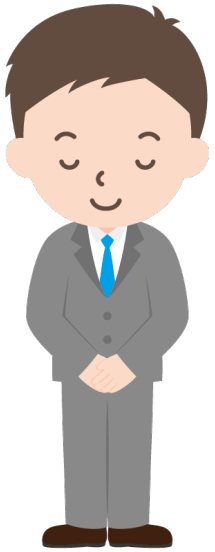
~ROAの一歩先の未来~

大阪大学情報科学研究科M2
山口 雄翔
y-yamaguchi@ist.osaka-u.ac.jp

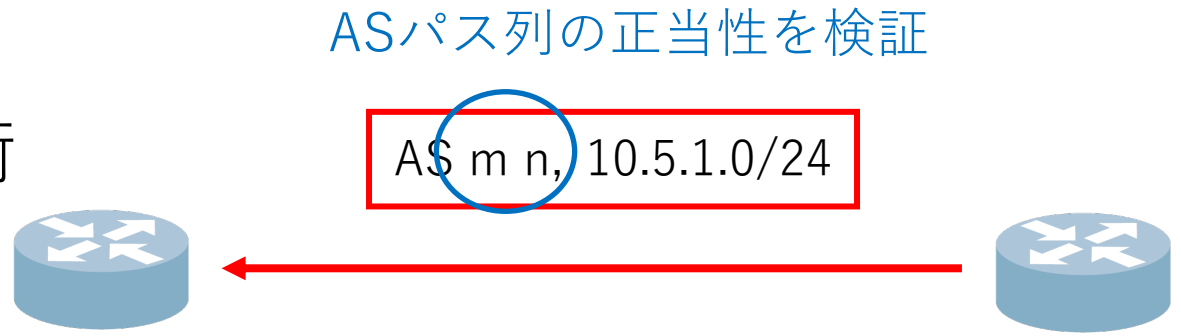


はじめに

- 私はAS運用をしたことがない人間です
- AS運用の現場の感覚とズレた話をしていましたら、遠慮なくご指摘いただけると嬉しいです



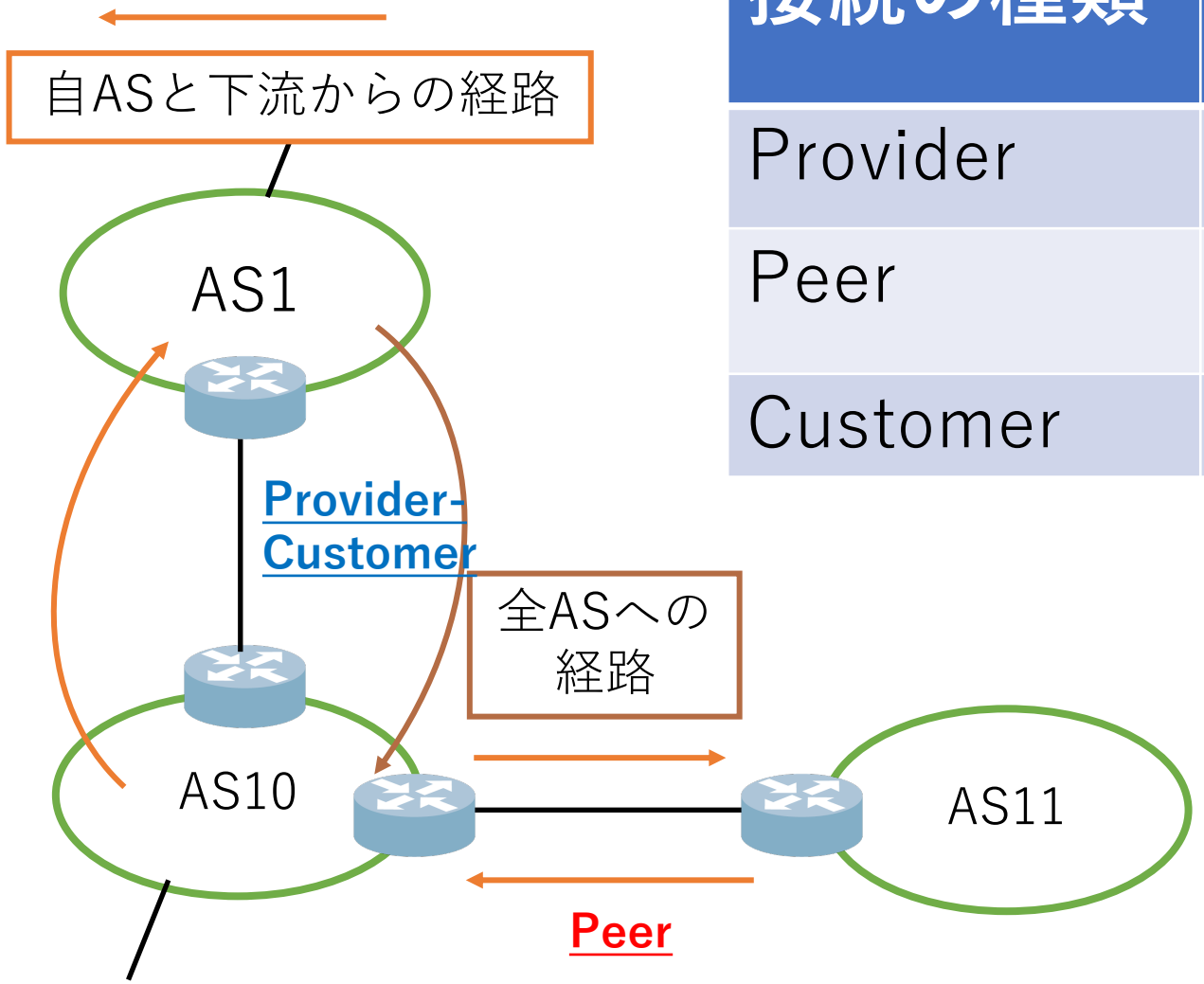
ASPAとは



- RPKIを用いたBGP経路検証技術
  - 構成はROAと同じ
- Path列の正当性を検証
  - ROAではできないルートリークの検知をすることができる
- 検証のしくみ
  - 各ASが自身のProvider ASを宣言しておく
  - BGPで広告された経路が、それらと矛盾していないかを検証
- 現状
  - ROAの次に導入を進めていくことが想定される
  - 現在標準化の途中

参考資料:
https://www.janog.gr.jp/meeting/janog51/wp-content/uploads/2022/12/janog51-bgp-pub.pdf

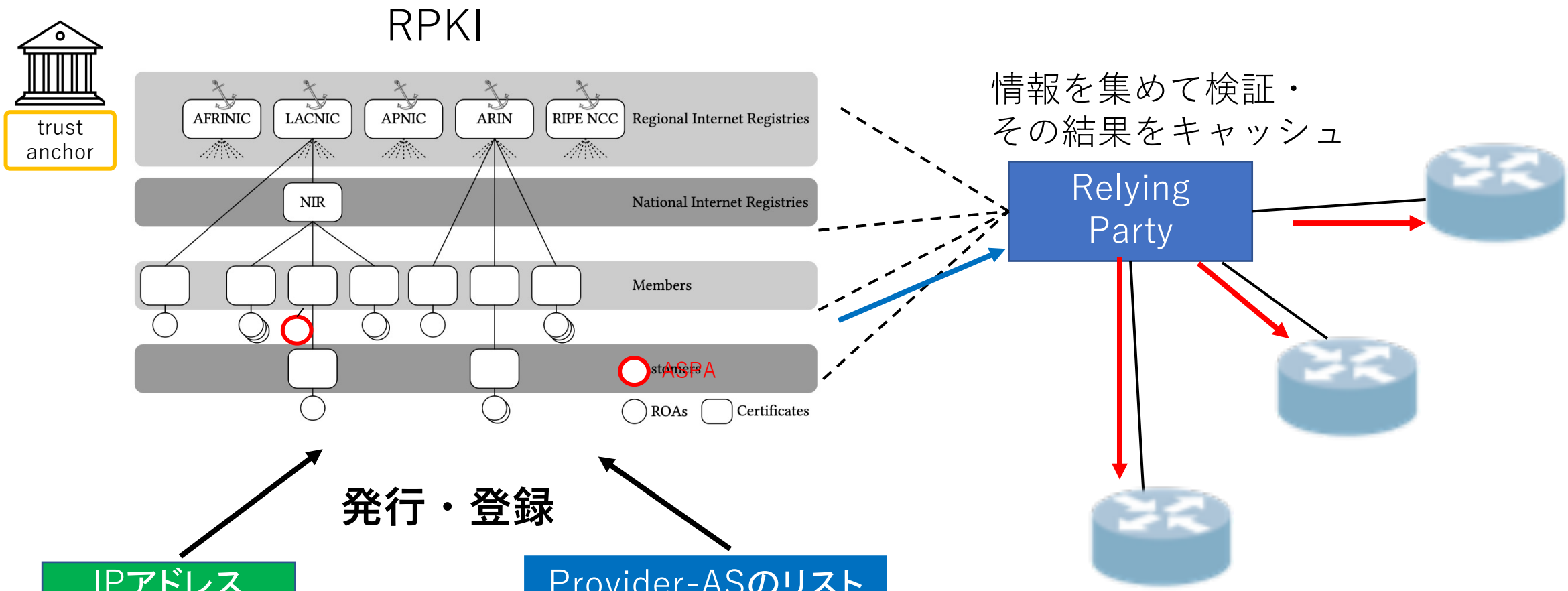
参考スライド: AS 間の接続の種類と流す経路



接続の種類	広告する経路
Provider	自ASとCustomer(下流)からの経路
Peer	自ASとCustomer(下流)からの経路
Customer	(基本的には)全ASへの経路

ASPAではこの原則に反する経路広告→ルートリーク
とみなす

参考スライド: RPKIのエコシステム



ASPAの課題

- 経路検証自体のメカニズムやエコシステムが複雑

→ 今までになかった問題がASPAの導入によって生じる可能性

- **本格的な導入・運用が始まる前に、詳細を明らかにする必要がある！**

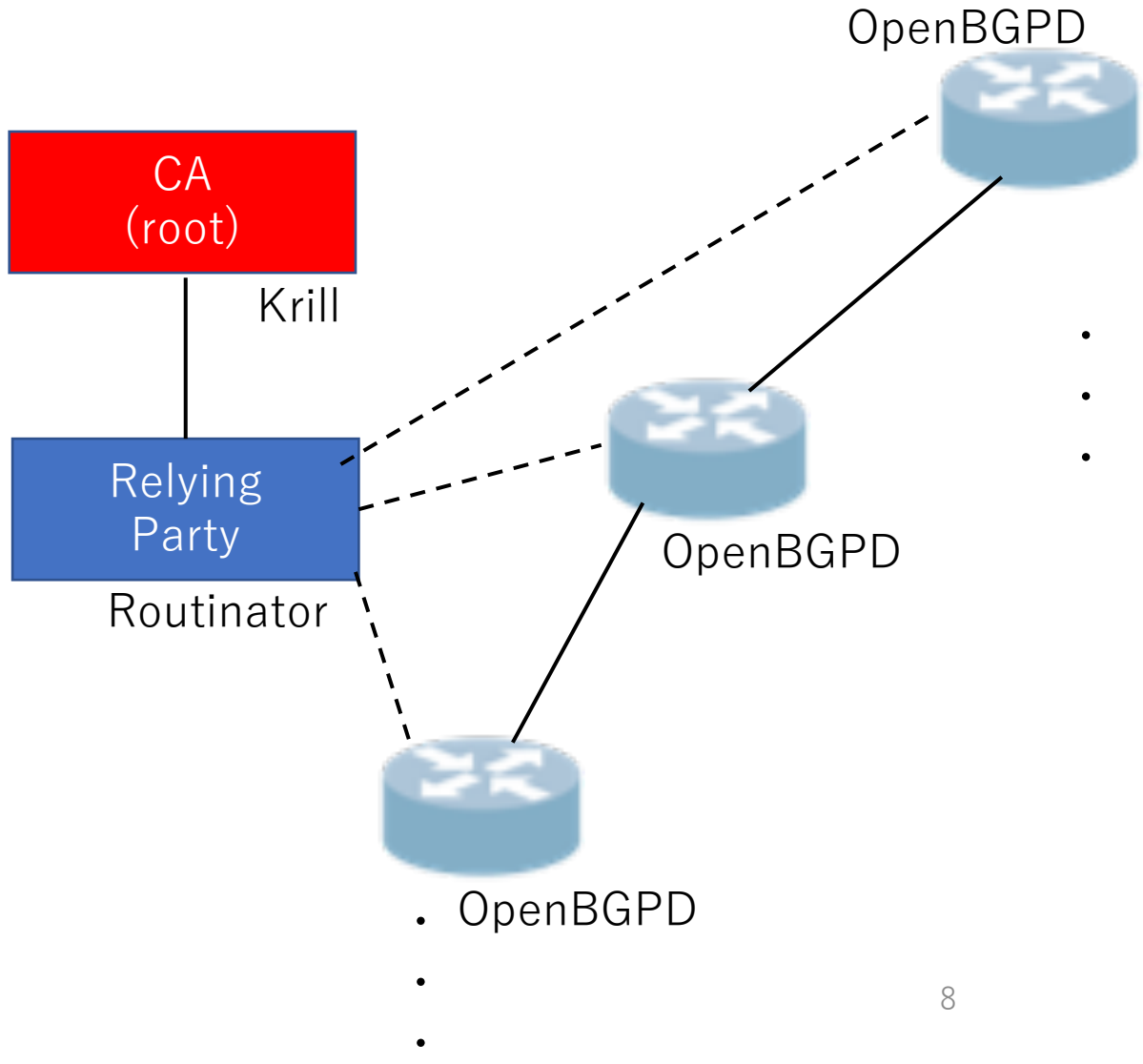
扱った問題

- ASPAの導入・運用に際して起こりうる不具合の具体例
  1. 期待に反してASPAで不適切経路の伝播を防げないケース
  2. 関連コンポーネントの障害や運用ミスに起因する不具合

  - BGP運用上避けるべき事象(不具合)
    - 不適切な経路を受理してしまう
    - 受理すべき経路をドロップしてしまう
    - 経路ループの原因になる

検証環境の構成図

構成要素	ソフトウェア
認証局	Krill
キャッシュサーバ (Relying Party)	Routinator
BGPルータ	OpenBGPD



OSSを使ってこれらのコンポーネントを全てコンテナ上で動かす検証環境を構築(tinetを利用)

評価したケース

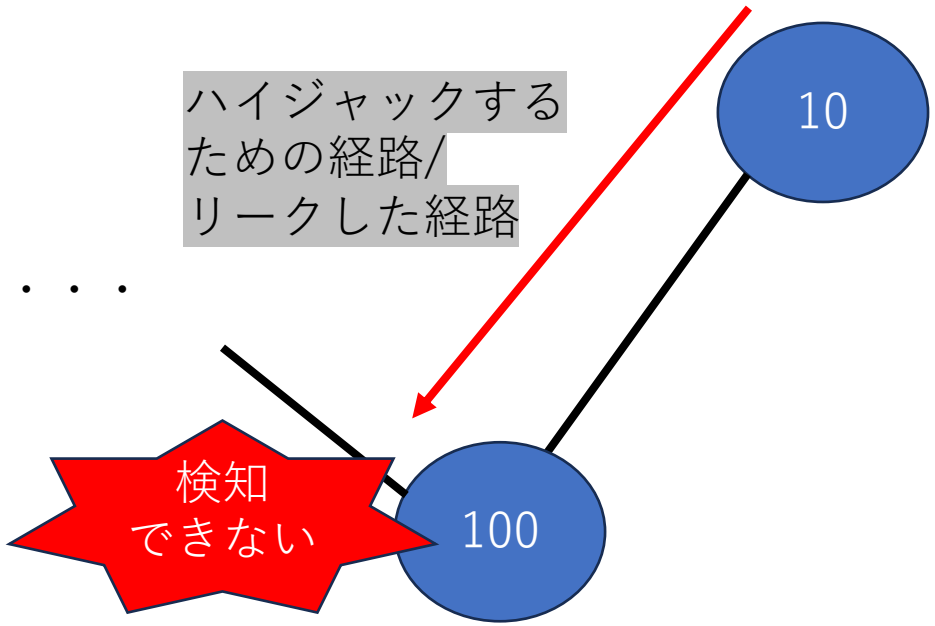
- 1.期待に反してASPAで不適切経路の伝播を防げないケース
  - 1-1) Providerからのリーク/ハイジャック
  - 1-2) ASPA未発行プロバイダを持つことによる脆弱性
  - 1-3) ASPA未発行プロバイダ群からの経路をCustomerがリークしても、それを検知できない
- 2.関連コンポーネントの障害や運用ミスが接続性に影響を与えるケース
  - 2-1) Peerから受け取った経路をPeerに流す運用をしている場合
  - 2-2) ASPAを発行しているが、特定のProviderを登録し損ねている場合
  - 2-3) キャッシュサーバとの通信に起因する障害

  - (※ケース(2-3)以外、検証環境で不具合が起きることを確認)

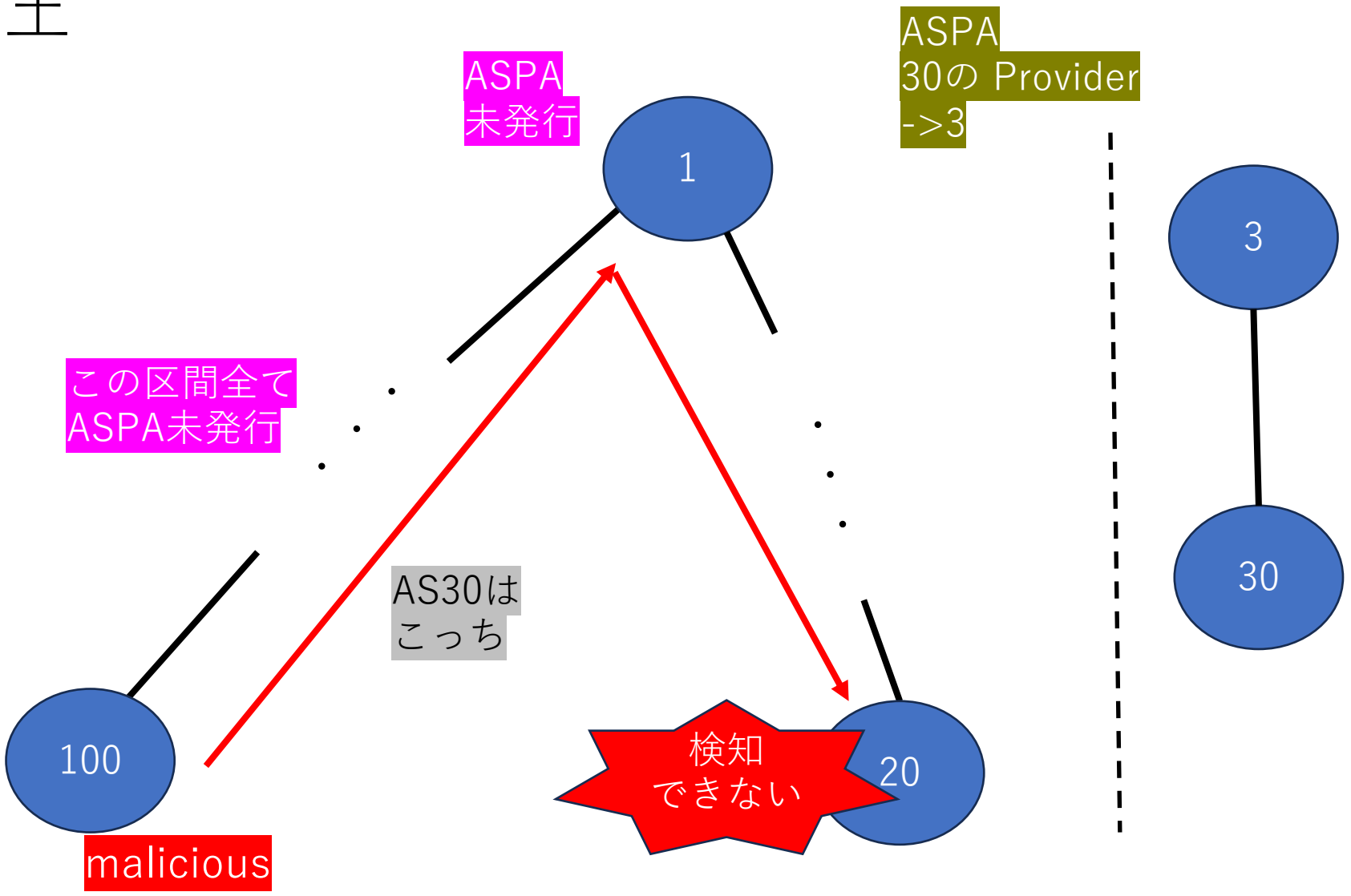
プロトコル仕様は現時点で最新のdraftを参照: https://datatracker.ietf.org/doc/draft-ietf-sidrops-aspa-verification/

1. 期待に反してASPAで不適切経路の伝播を防げないケース

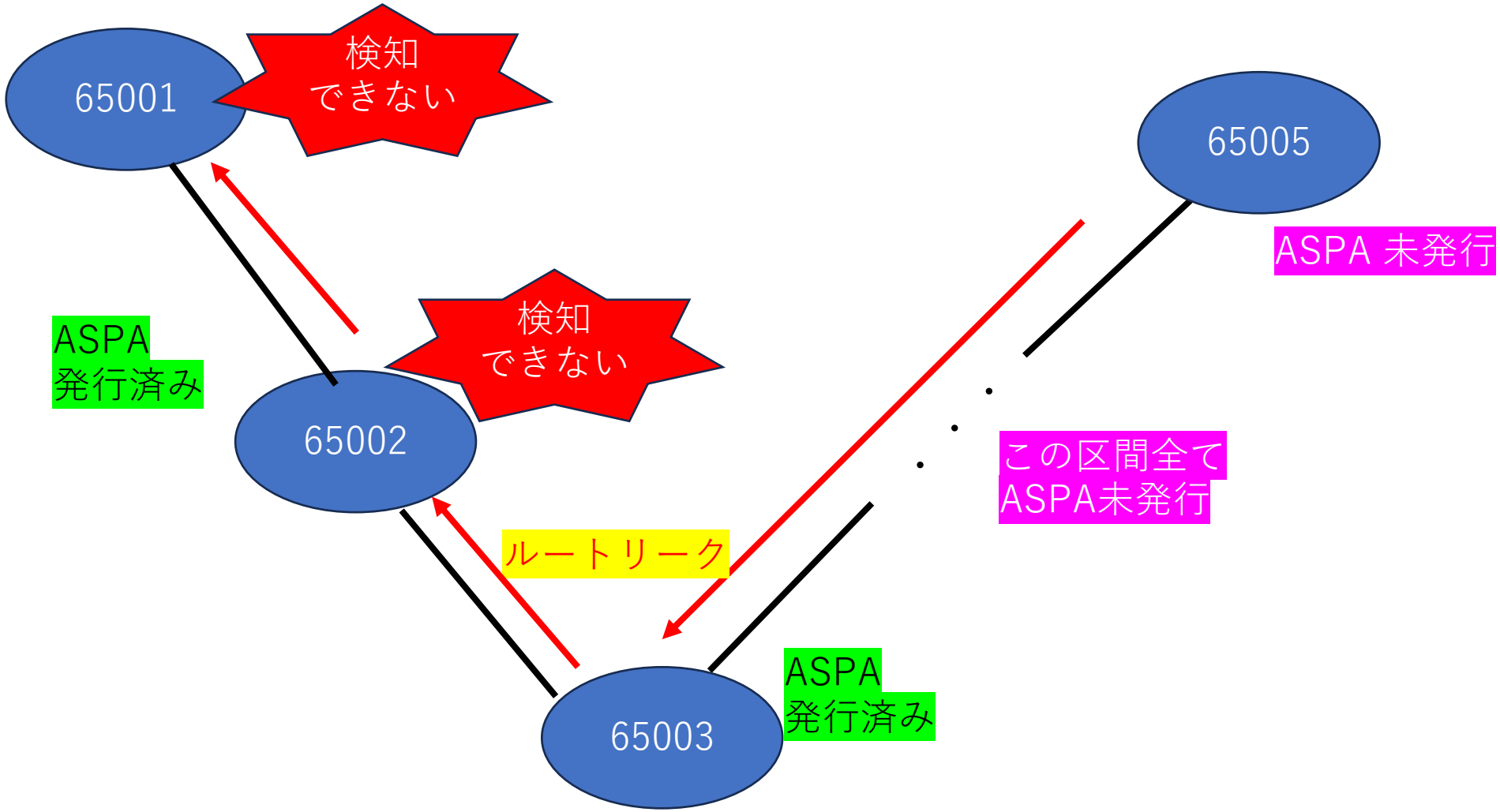
1-1) Providerからのリーク/ハイジャック



1-2) ASPA未発行Providerを持つことによる脆弱性



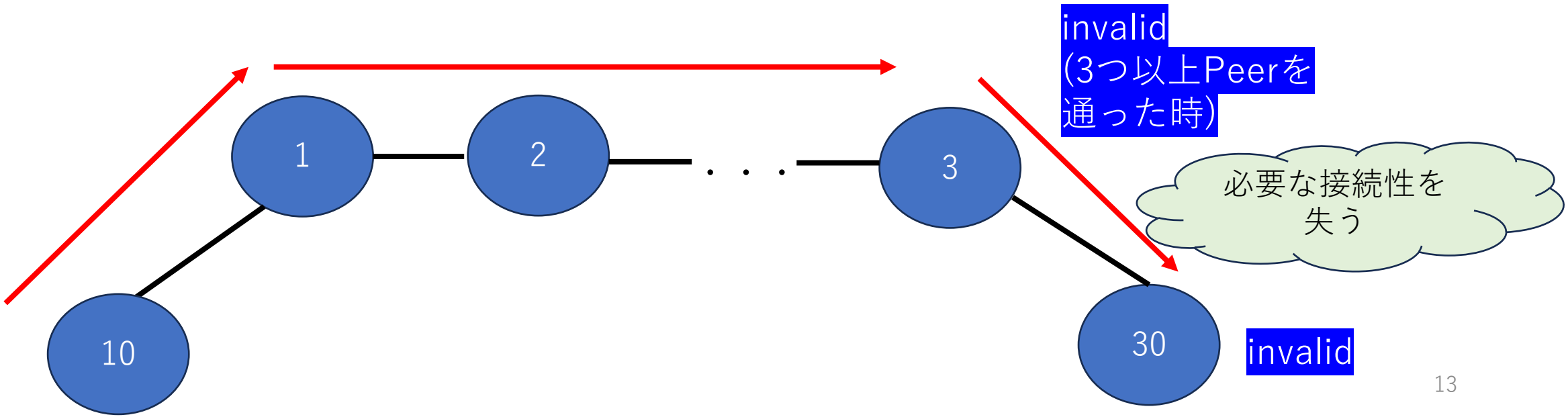
1-3) ASPA未発行Providerからのリークを検知できない問題



2. 関連コンポーネントの障害や運用ミスが接続性に影響を与えるケース

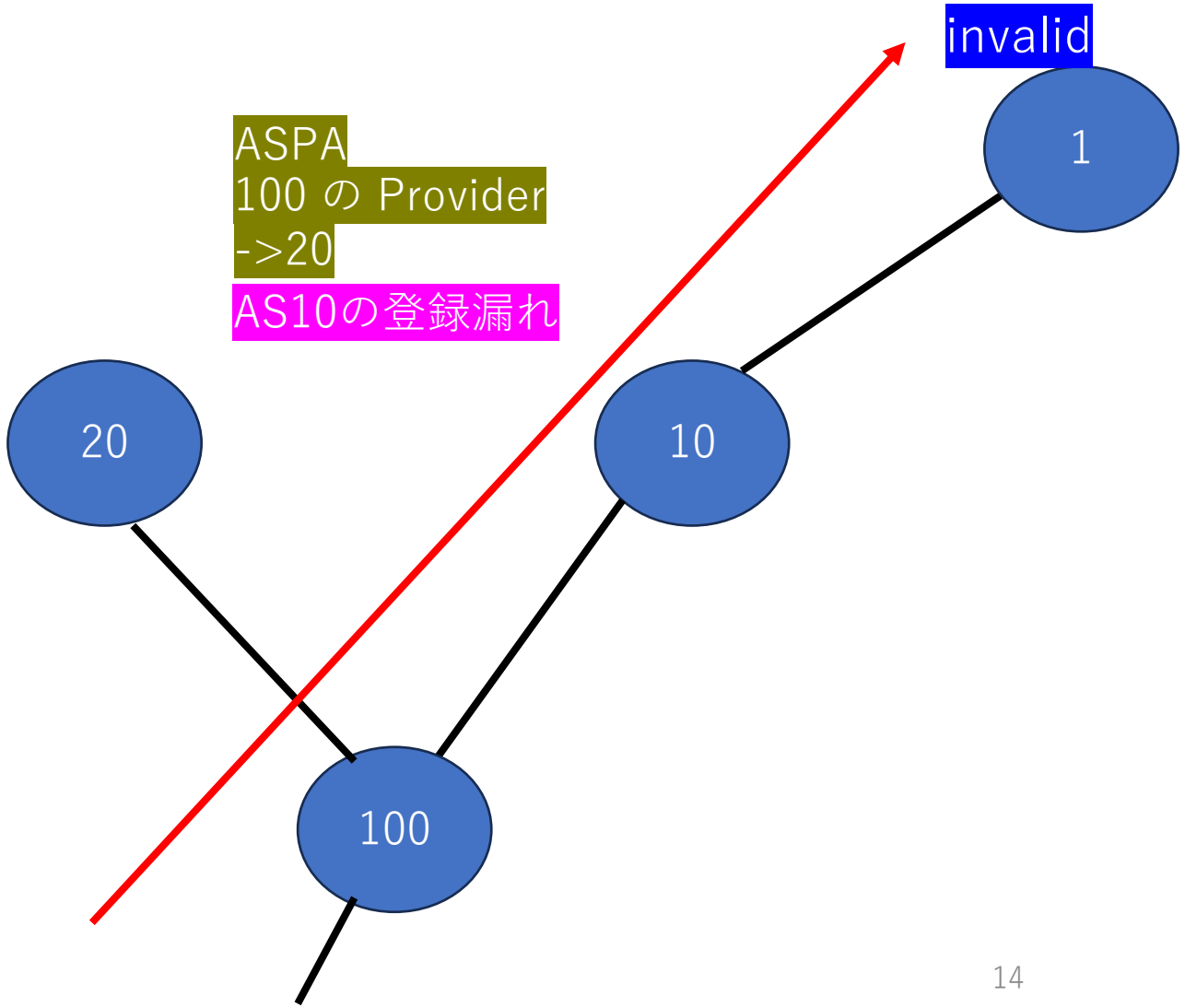
2-1) Peerからの経路をPeerに流す運用

- mutual-transitの関係で接続すれば回避可能

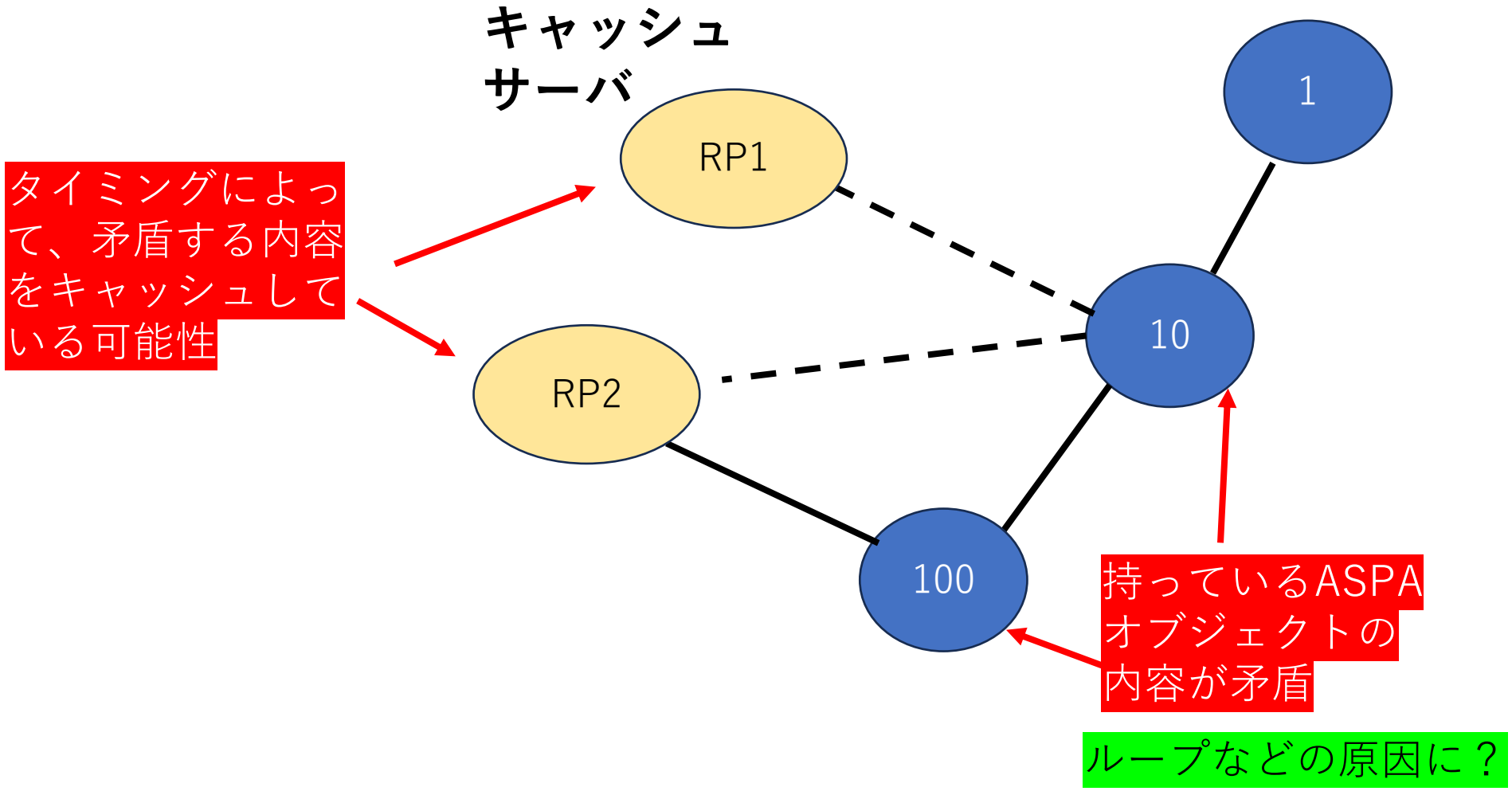


2-2) Providerの登録漏れ

必要な接続性を
失う



2-3) キャッシュサーバとの通信に起因する障害



考察

- 見えてきたプロトコルの特徴
  - 上流ASがASPAオブジェクトを発行するのが圧倒的に効果大
  - 上流からの経路をInvalidにする基準が厳しい
    →信頼できるProviderと接続する必要あり

- 関連コンポーネントに関して
  - プロトコル仕様の外の部分を詰めてから運用を始める必要性
    - 認証局-キャッシュサーバ の同期間隔をどうするか
    - 通信が落ちた時どうするか.　など

この結果をどう活かすか

- 導入・運用のフェーズの前に、注意点を広く共有
  - ASPAは、到達性がある経路をドロップしうる技術

- 結果を踏まえて、議論を深める
  - プロトコル作成をしている方々
  - ASPAの導入を検討されているISPの方々

IA研での研究発表:https://ken.ieice.org/ken/paper/20231122RCYm/