経路奉行の取り組み

(財)日本データ通信協会

Telecom-ISAC Japan

経路情報共有ワーキンググループ

渡辺　英一郎(watanabe@mfeed.ad.jp)

Telecom-ISAC Japan
Telecom Information Sharing and Analysis Center Japan

本発表の内容

- 経路奉行概要
  - 経路奉行とは？をざっくり説明します。
- 経路ハイジャック検出状況
  - JPNICさんとの連携実験で得られた検出結果を報告します。
- 経路ハイジャック検出事例
  - 過去に発生した経路ハイジャック事例のなかでよくある事例を紹介します。
- 検出側からみる経路ハイジャック
  - 経路ハイジャック検出側からみた問題点をふまえ、BGPオペレータのみなさんにも考えていただきたいことについて言及します。

経路奉行概要

経路奉行概要

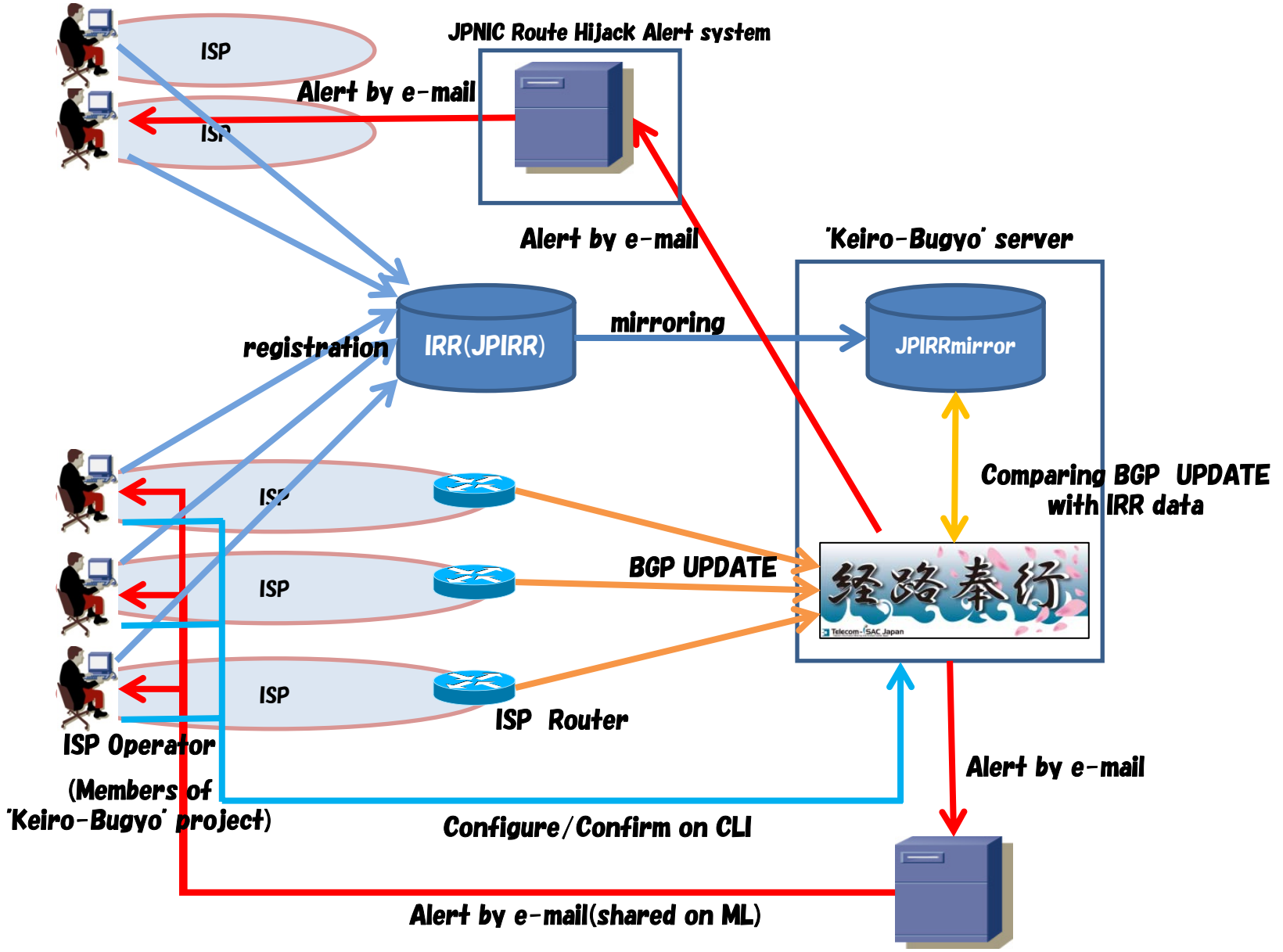
- （財）日本データ通信協会　Telecom-ISAC Japanで運用。

- 経路奉行メンバ（2009/11/25時点。順不同）
  - IIJ(AS2497)
  - KDDI(AS2516/AS4716)
  - KDDI研究所(AS7667)
  - SoftBankBB(AS17676)
  - SoftbankTelecom(AS4725)
  - Biglobe(AS2518)
  - 富士通(AS2510)
  - NTTCom(AS4713/AS2914)
  - インターネットマルチフィード(AS7521)
  - So-net(AS2527)
  - さくらインターネット(AS9370/AS9371)
  - YAHOO! Japan(AS4694)
  - NTTスマートコネクト(AS7671)
  - NTT-PCコミュニケーションズ(AS2514)

- 経路奉行は自ISPだけで解決できないルーティング障害について情報共有するためのシステム。経路奉行メンバにとっては、経路ハイジャック通知だけでなく、経路情報の過去検索や（自称）日本国内最強のlooking glassとして利用。

- JPNIC 「経路ハイジャック通知実験」の検出エンジンとして情報提供も行う。

経路奉行概要（つづき）



経路奉行検出範囲

JPIRRにRouteオブジェクトとして登録されたprefix/originの組み合わせと経路奉行メンバから提供されたBGP UPDATEを比較。

受信したprefixがequal or longerでoriginが異なる場合、NG。

IPv4経路のみ（IPv6経路は検討中）。

JPIRRにミラーされたRouteオブジェクトは対象外。

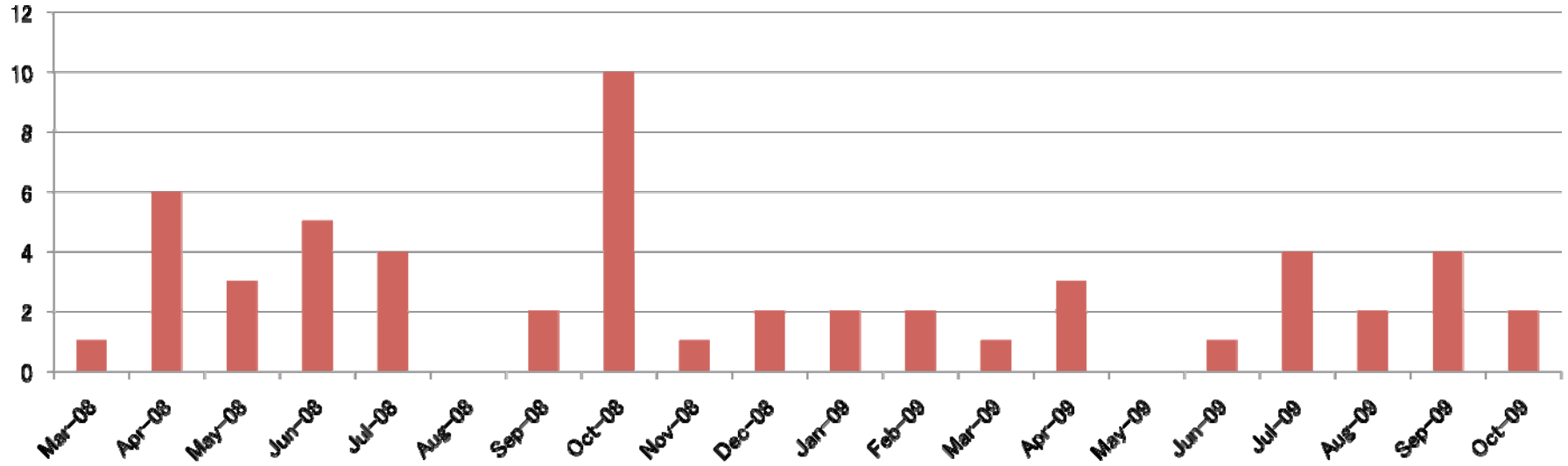
※本資料では上記の条件で発生したものを経路ハイジャックと呼んでいます。

経路ハイジャック検出状況

経路ハイジャック検出状況

インシデント別検出状況(2008/03/01-2009/10/31)

(注)インシデント=同時刻に発生した経路ハイジャックを1件とする。
全発生件数から誤検知の可能性が高いものを除く。

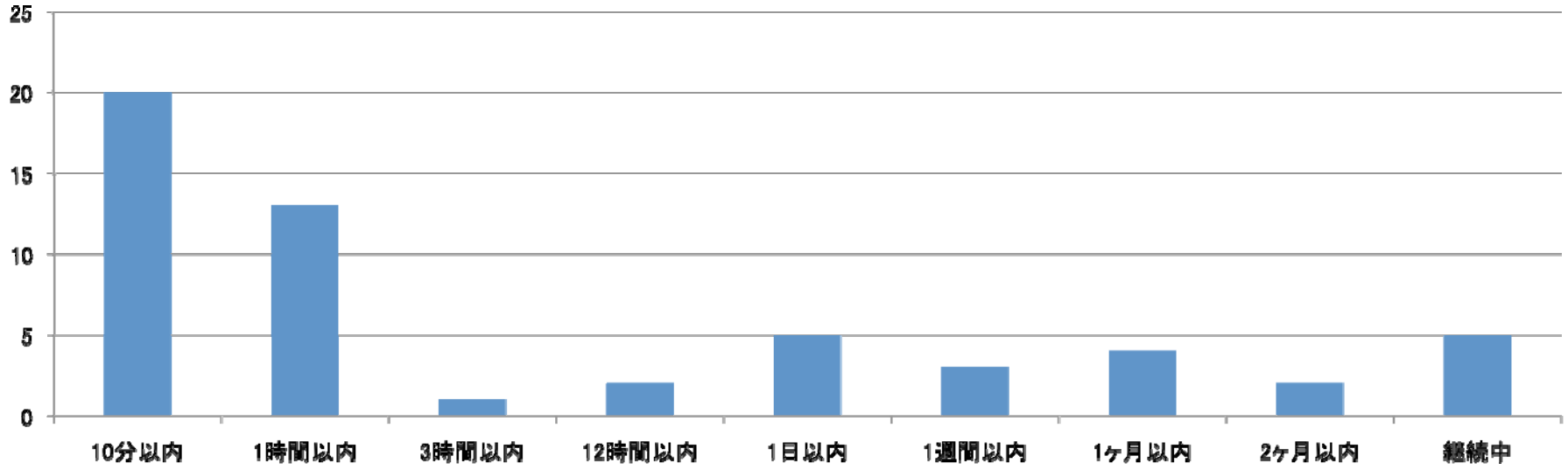


- 期間内総数=55件
- 毎月ぼちぼち発生(月平均2.75件)

経路ハイジャック回復状況

経路ハイジャック回復時間統計(2008/03/01-2009/10/31)

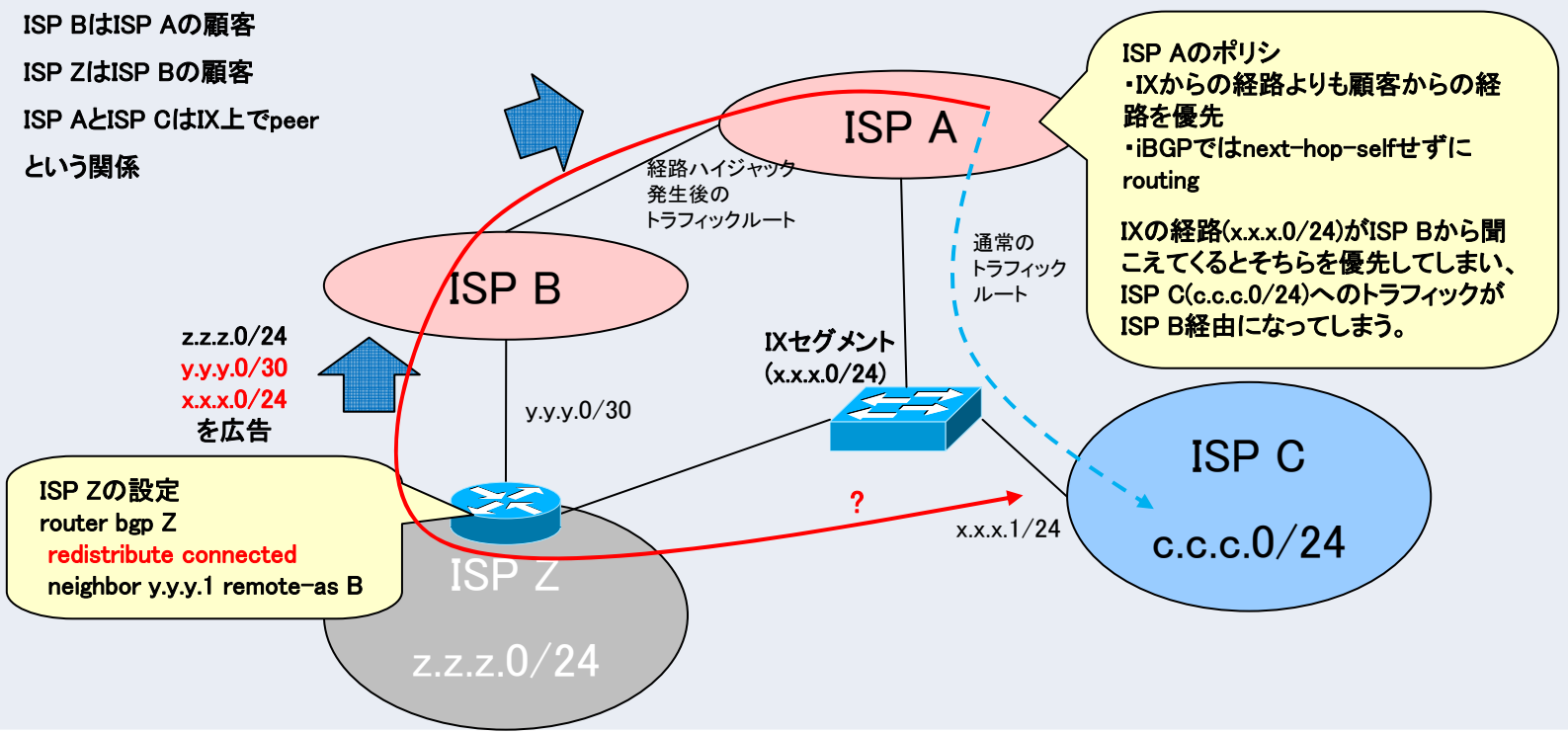
(注)回復時間＝WITHDRAW時間-UPDATE時間



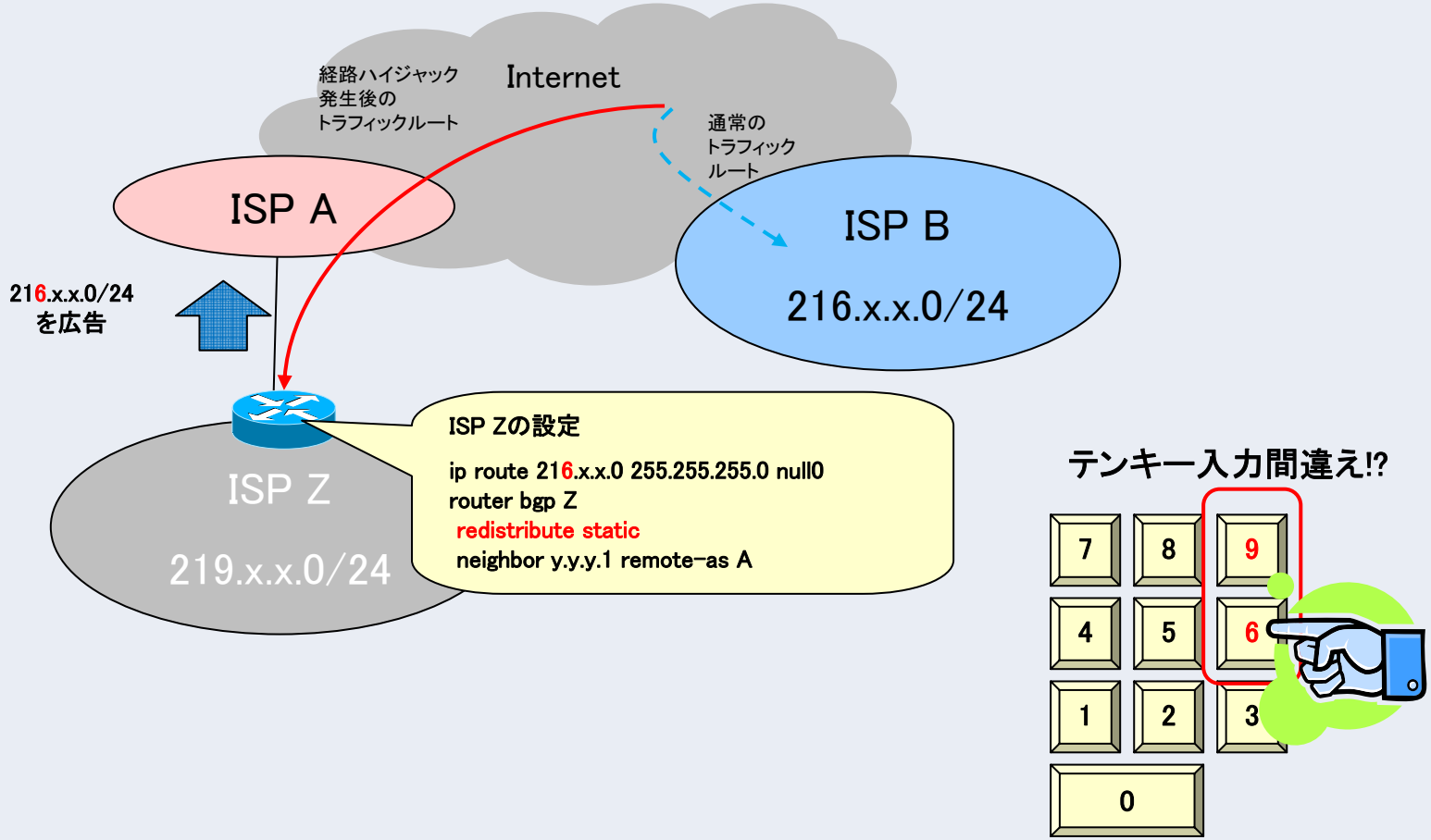
- 約60%は1時間以内に回復。
- 数ヶ月以上回復していないものもある。

経路ハイジャック検出事例

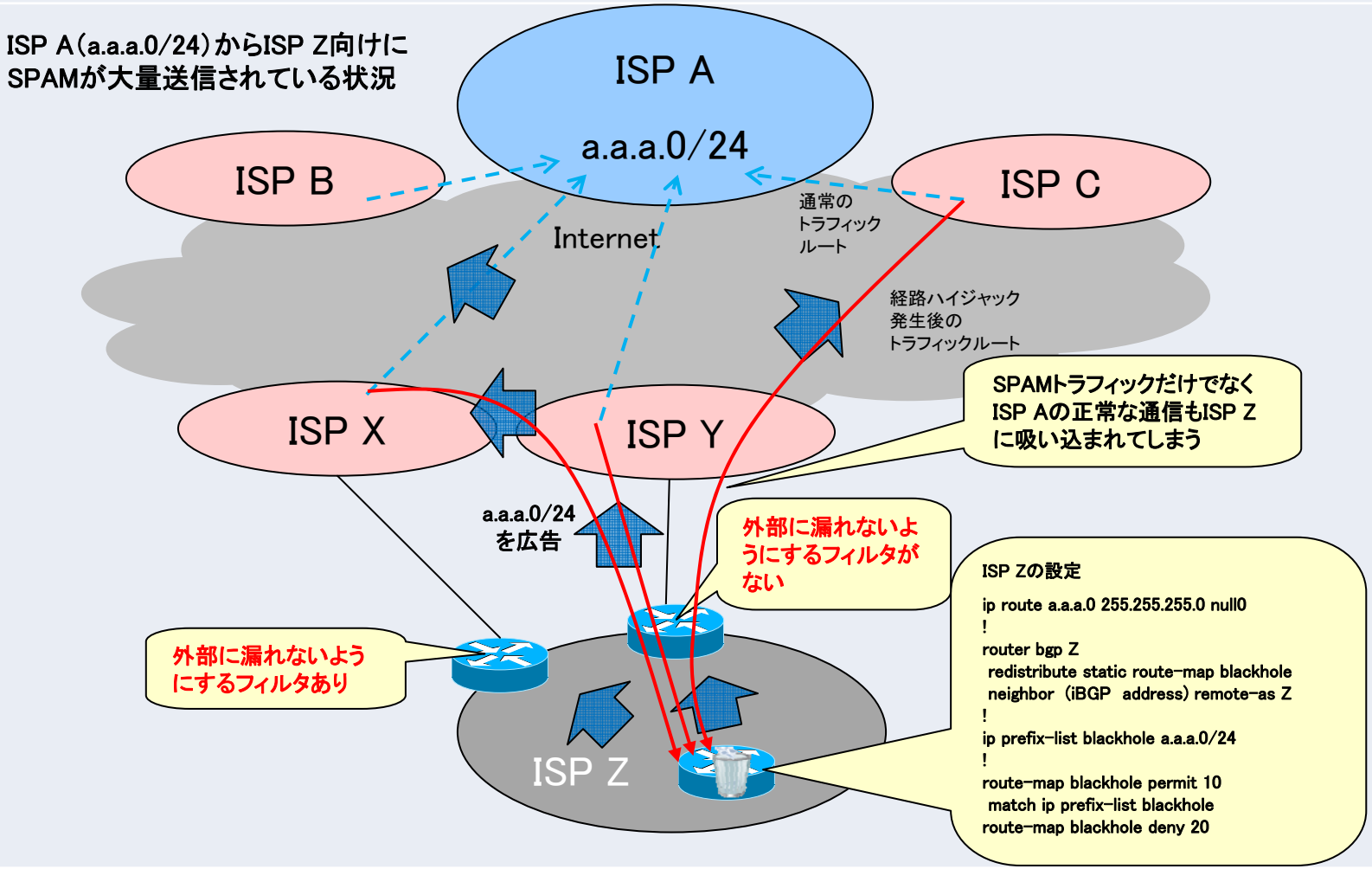
検出事例その１(redistribute connected to bgp)

よくある事例	ルータの接続IFを経路フィルタなしでBGPにredistributeし外部に広報してしまうケース。そのルータ上でUPしているconnected routeがすべてアナ
影響度	特にIXセグメントの広報が危険。IX上の他ASのルータの設定によっては通信に影響を及ぼす。
構成例	

検出事例その２（広告prefixのtypo）

よくある事例	自ASの経路を広報する際に、prefixをtypoした状態でstatic routeを設定し、BGPにredistributeしてしまうケース。
影響度	typoしたprefixが他ASで使用しているアドレス空間であった場合影響大。
構成例	

検出事例その３（経路漏れ）

よくある事例	AS内部でのみ利用すべき経路をAS外部にも漏らしてしまうケース SPAMをredistribute static to bgpでblackholeしたりする場合に発生。
影響度	影響大な場合が多い。
構成例	

検出事例その４（こんなのアリ？）

とあるASが、日本の複数のISPのprefixを同時に広告。

経路ハイジャック事象自体は広報元で気づいたのか約5分後には回復。（なので大問題にはならなかった。）

しかし、後に、被害を受けたISPのオペレータが、「なんでこんなことしたの？」と聞いたら、広報元からこんな返事が…

うちの顧客がプライベートアドレスとしてこのprefixを
使っていて間違って広報しちゃったようです。

(!￣Д￣)えぇぇぇ……

検出側からみる経路ハイジャック

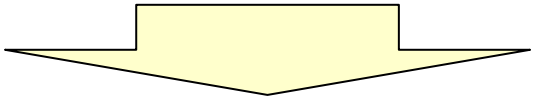
検出側で見えること

実は誤検出(false positive)が多い…。（p.8グラフの約３倍検出）

誤検出の原因

- IRR情報の未登録
- IRR情報の一部誤り
- IRR情報の削除漏れ

IRR情報が正確に保たれていないと、誤検出(false positive)をひきおこすだけでなく、経路ハイジャックを検出できない状態(false negative)もひきおこす。



AS運用をする上ではうれしくない

BGPオペレータのみなさんへ

- 自分の運用するネットワークの正常性を監視するために経路ハイジャック監視も取り入れてみてください。

- 自分が経路ハイジャックの加害者にならないために、経路広報時には細心の注意を払いましょう！

- みなさんが経路情報をIRR上で正確に保つことにより、経路ハイジャック検知の精度が向上します。ご協力お願いいたします。