
RPKIの普及と課題

インターネットマルチフィード

吉田友哉

-
- 世界中で実装もはじまり具体化してきた
 - ハッカソンも充実

-
- 何を備えておく必要があるのか
 - 従来の経路制御と何が異なるのか
 - 具体的効果は？

3つのやること

1.ROAを作って

2.ルータにくわせて

3.Validation(marking)する

1. ROAをつくる

- 作る人
 - AS管理者
 - アドレス管理者（指定事業者）
- APNICやRIPE等では、アドレス管理者が、自分が広告して欲しいAS情報を書いてROAをつくる
- 日本ではこれから検討
 - 従来のIRRと異なってくる可能性がある

1. ROAをつくる

rpki.net

Home

Logged in as YOSHIDA

Log Out

YOSHIDA

[dashboard](#)
[routes](#)

[export identity](#)

Resources

Resource	Valid Until	Parent
AS4713	June 26, 2014, 7:13 a.m.	JPNIC02
AS9598	June 26, 2014, 7:13 a.m.	JPNIC02
AS18131	June 26, 2014, 7:13 a.m.	JPNIC02
133.93.0.0/16	June 26, 2014, 7:13 a.m.	JPNIC02

[refresh](#)

ROA Requests

Prefix	Max Length	AS	
133.93.0.0/16-17	17	131155	info delete
133.93.0.0/16-17	17	18131	info delete
133.93.0.0/16-33	33	38639	info delete

[Create](#)

Children

Handle
Import

Unallocated Resources

The following resources have not been allocated to a child, nor appear in a ROA.

ASNs

- AS4713
- AS9598

Ghostbuster Requests

Full Name	Organization	Email	Telephone
Create			

Parents

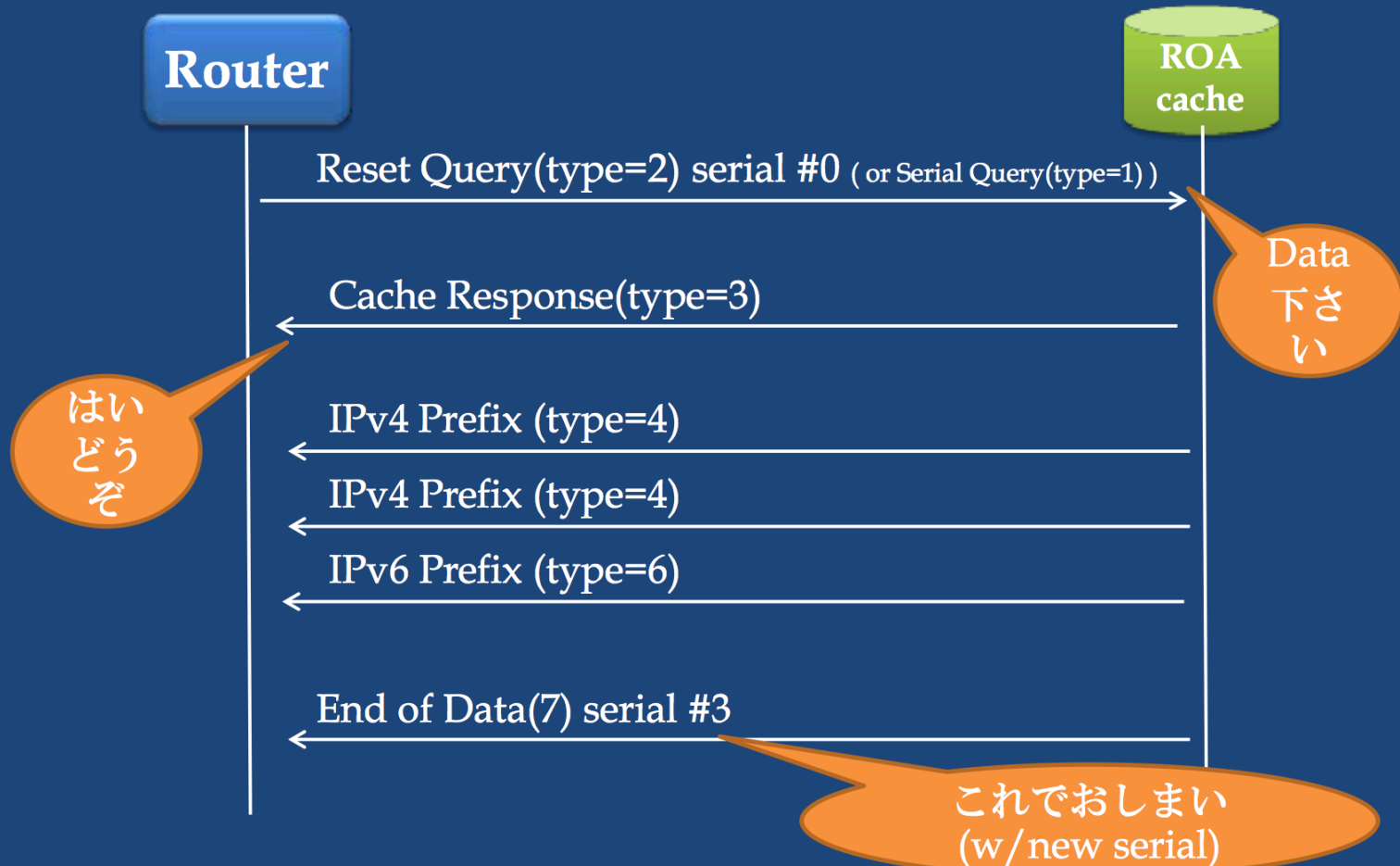
Handle
JPNIC02 delete

1. ROAをつくる

- 今は1つ1つ作っていく必要がある
 - 一気につつこめるIFがあると便利
- IRRへのexport “ROA to IRR”が検討されている (incremental deployment)
 - Max-lengthの概念をどうするか
 - /16/-24まで全部さすがに書くのはやりすぎ
 - 最もshorterな/16のみを作る？
 - とはいっても、いまのIRRはexact match…
 - Description等で補足するぐらい？ (RPKI valid)

2. ルータにくわせる

1. RTR(RPKI/Router) Protocol Start or Restart



2. ルータにくわせる

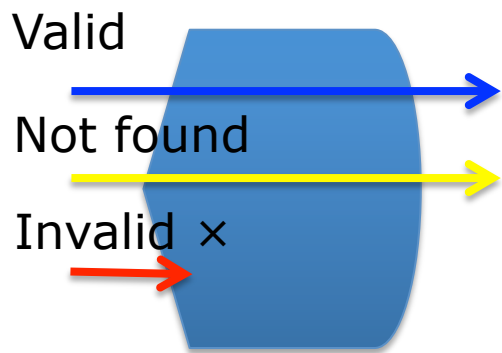
- 外部のcacheDBに依存
 - RTR Protocolがきちんと動く必要がある
 - DBの中身に依存
- 従来
 - 静的にin/outのフィルタ
- 全BGPスピーカーで動かす必要はない（後述）

3. Validation(marking)する

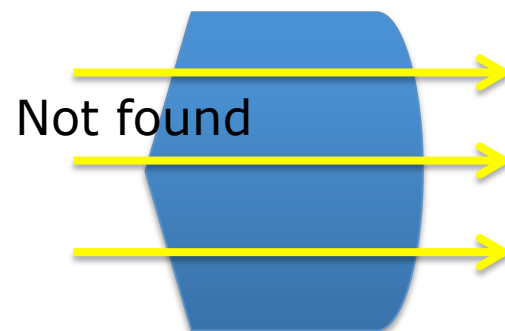
- 異なる様々なポリシー
 - 例) Validのみをpermitしそれ以外はたたきおとす。。
 - 例) Invalidは全部たたきおとし、それ以外は寛容に。。
 - 例) まずはmarkingするところから。。

従来の経路制御との違い

- RTRセッションが切れると、validation結果が“not found” (cacheが無い状態)になる可能性がある。
 - セッション確立時に“Invalid”でrejectされていた経路や、“Valid”でpriorityがあがっていた経路がのきなみ“not found”になる。。
 - 出ちゃいけない経路が出てしまう



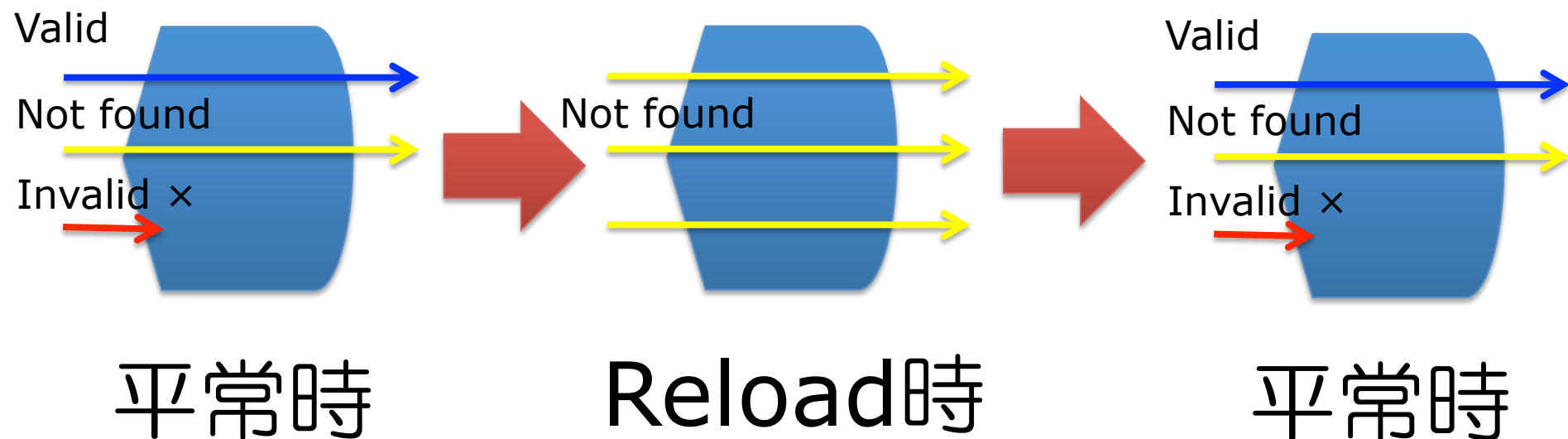
平常時



RTR down

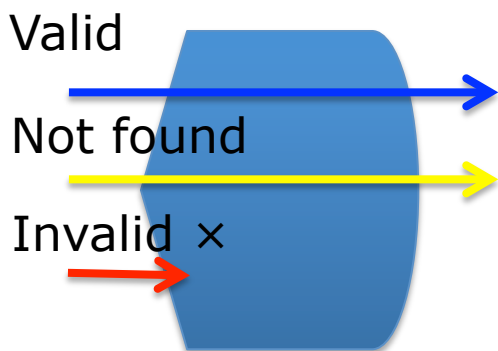
従来の経路制御との違い

- (不用意に)ルータがreloadした場合、RIB/FIBのconvergenceとcache installのconvergenceの時間差で経路選択が異なってくる可能性あり
 - 従来の多くは、Filterが静的に設定されているため、rejectする経路、permitする経路が状況に応じて異なる事はない。

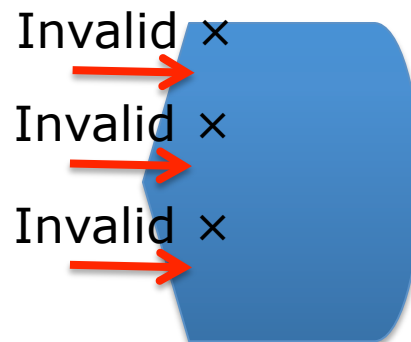


従来の経路制御との違い

- もしcacheDBの中身が何らか不正な状態となったら、validation結果が(全て) “Invalid”になってしまう可能性もある
 - RIRの運用が厳格に行われる必要がある、かつ何かおきても大丈夫な状態にしておく必要がある



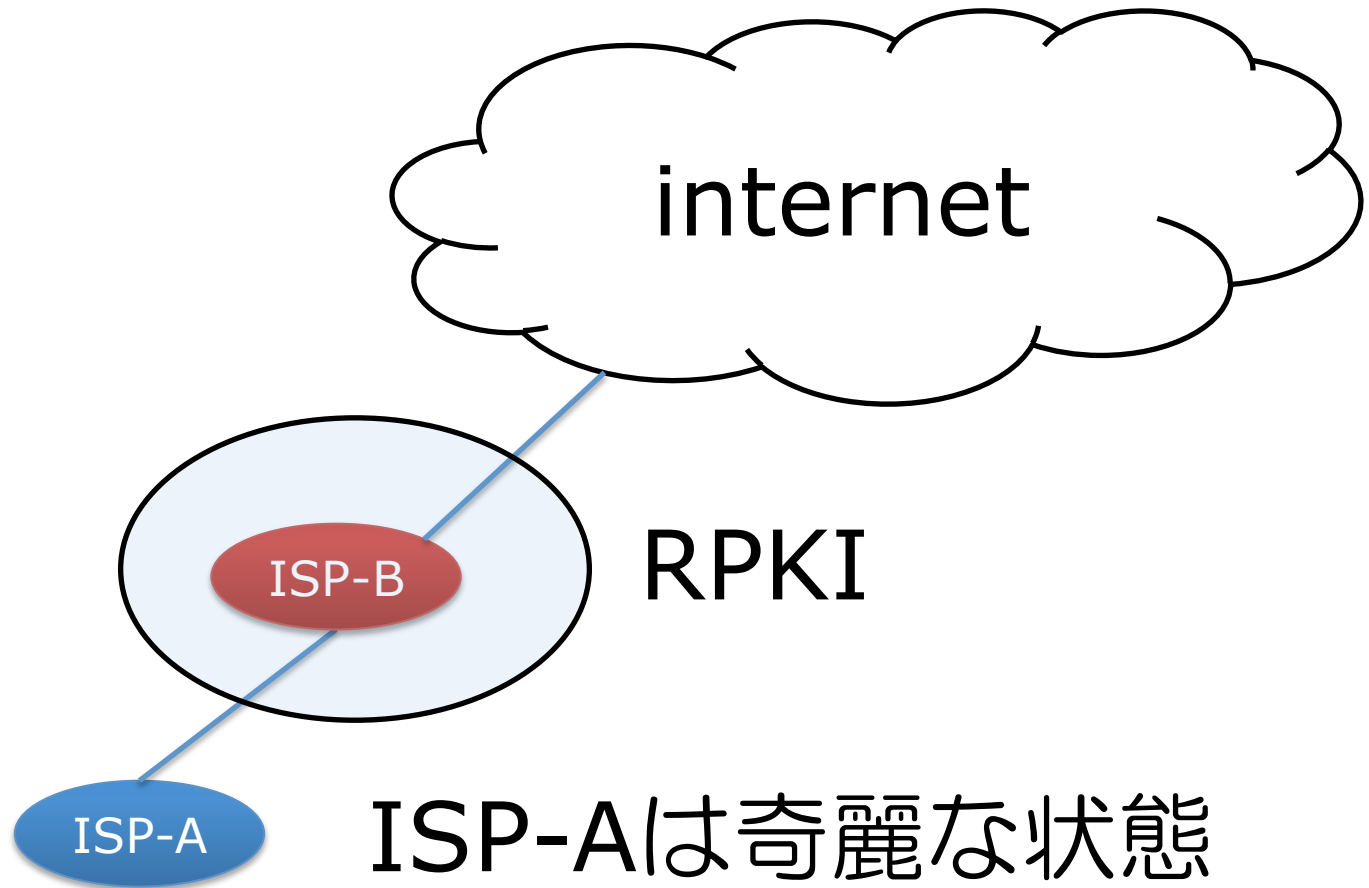
平常時

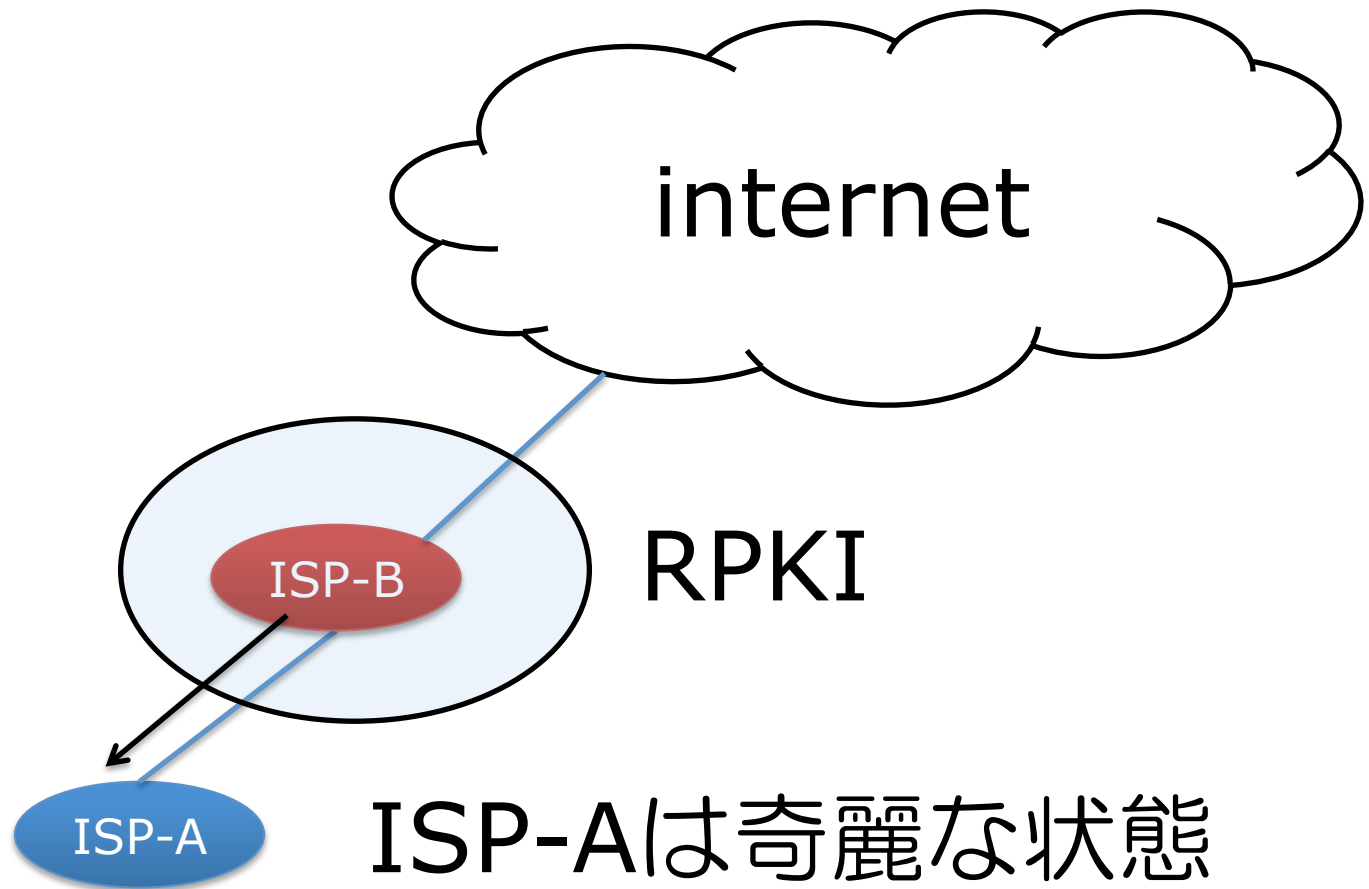


DBが...

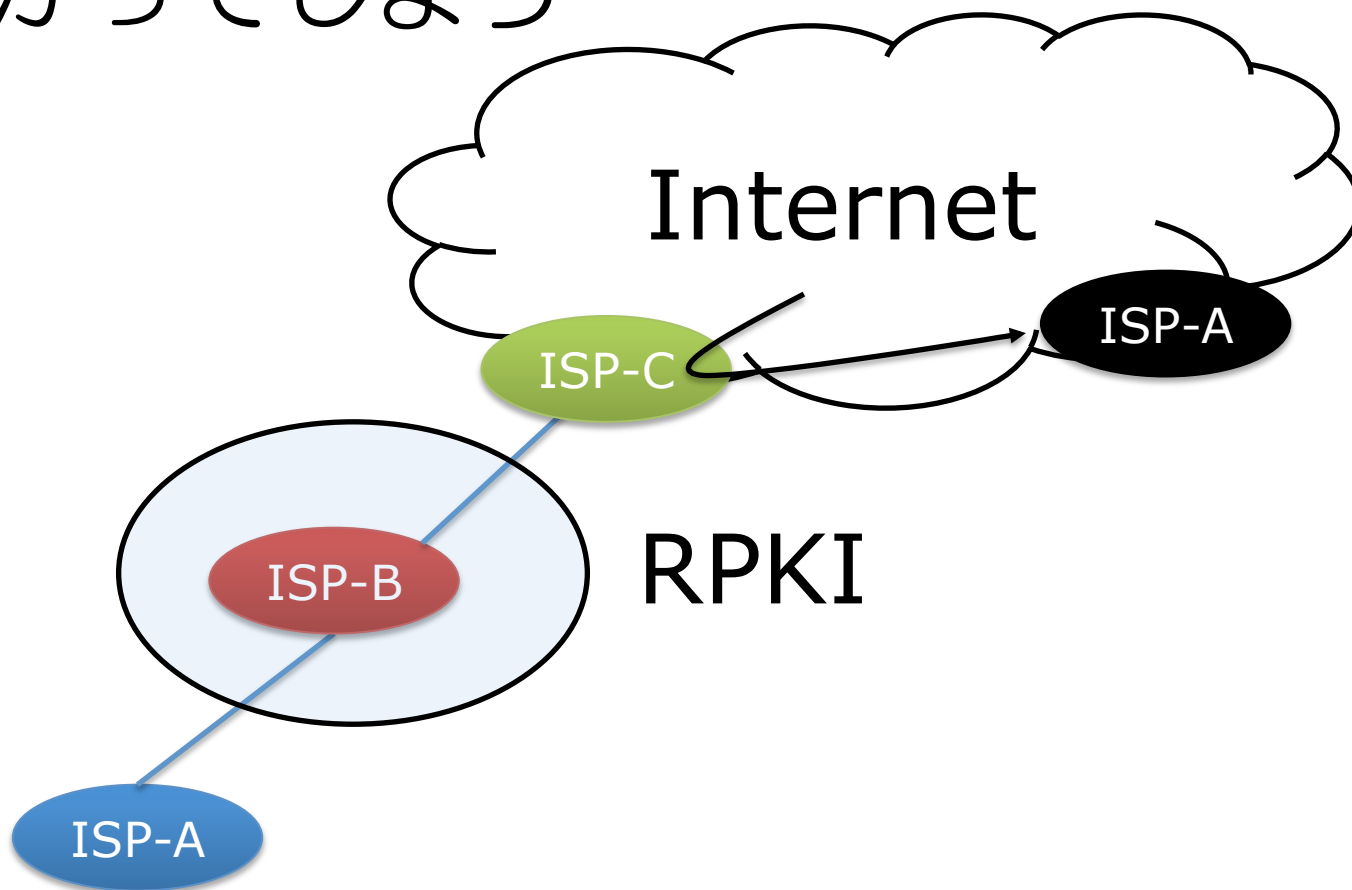
様々な疑問

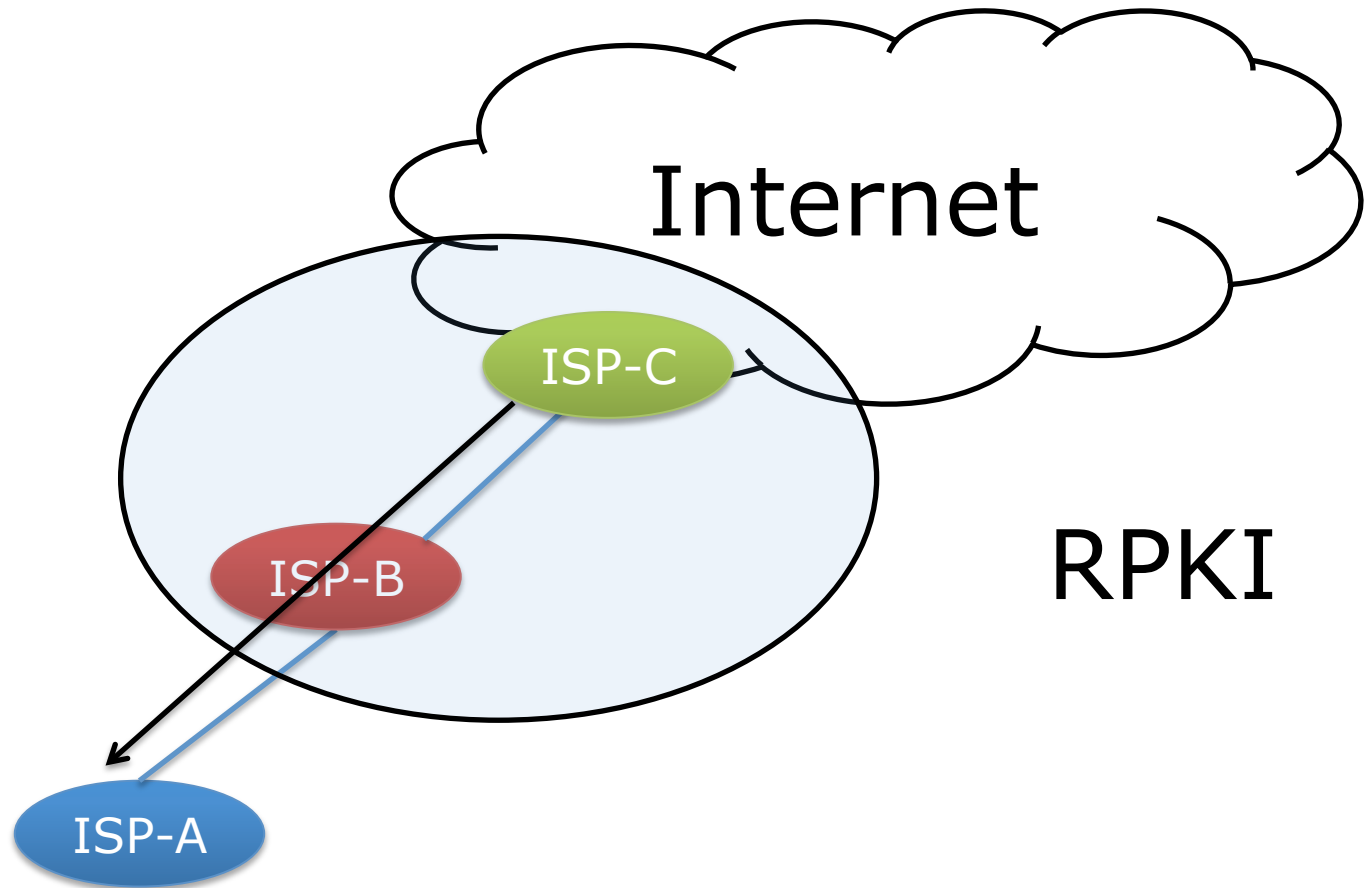
- ROAを作るところはなんとかかなりそうだけど…
- ルータでどうすれば良い？
- IGPのどのルータに適応すれば良い？
 - 全てのエッジルータにも適応する必要がある？
- 上流ISPさんでなんとかならない？
- いろいろなリスクはどう回避すれば良い？
- Filterはいらない？
- ほんとに効果あるの？

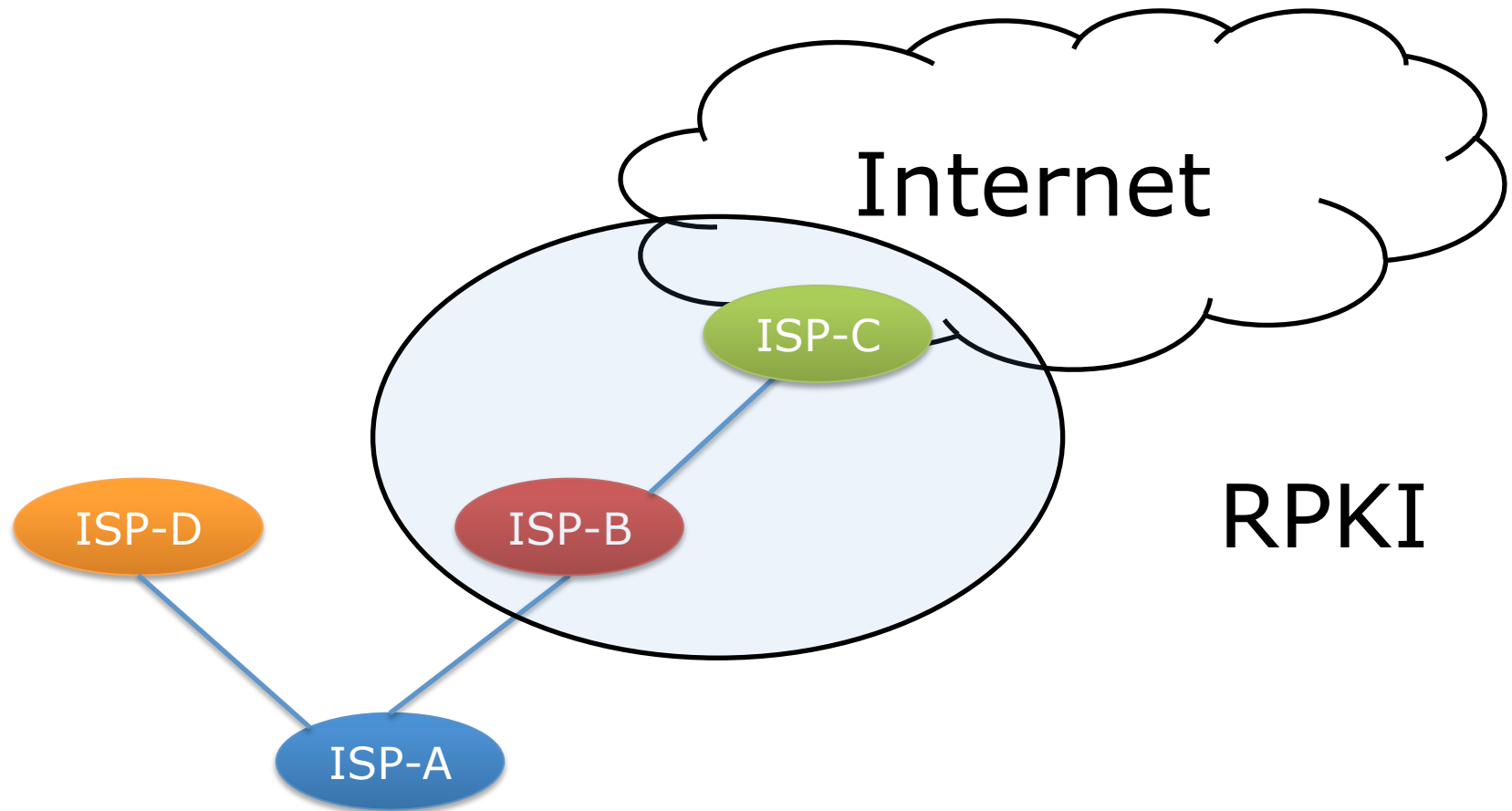


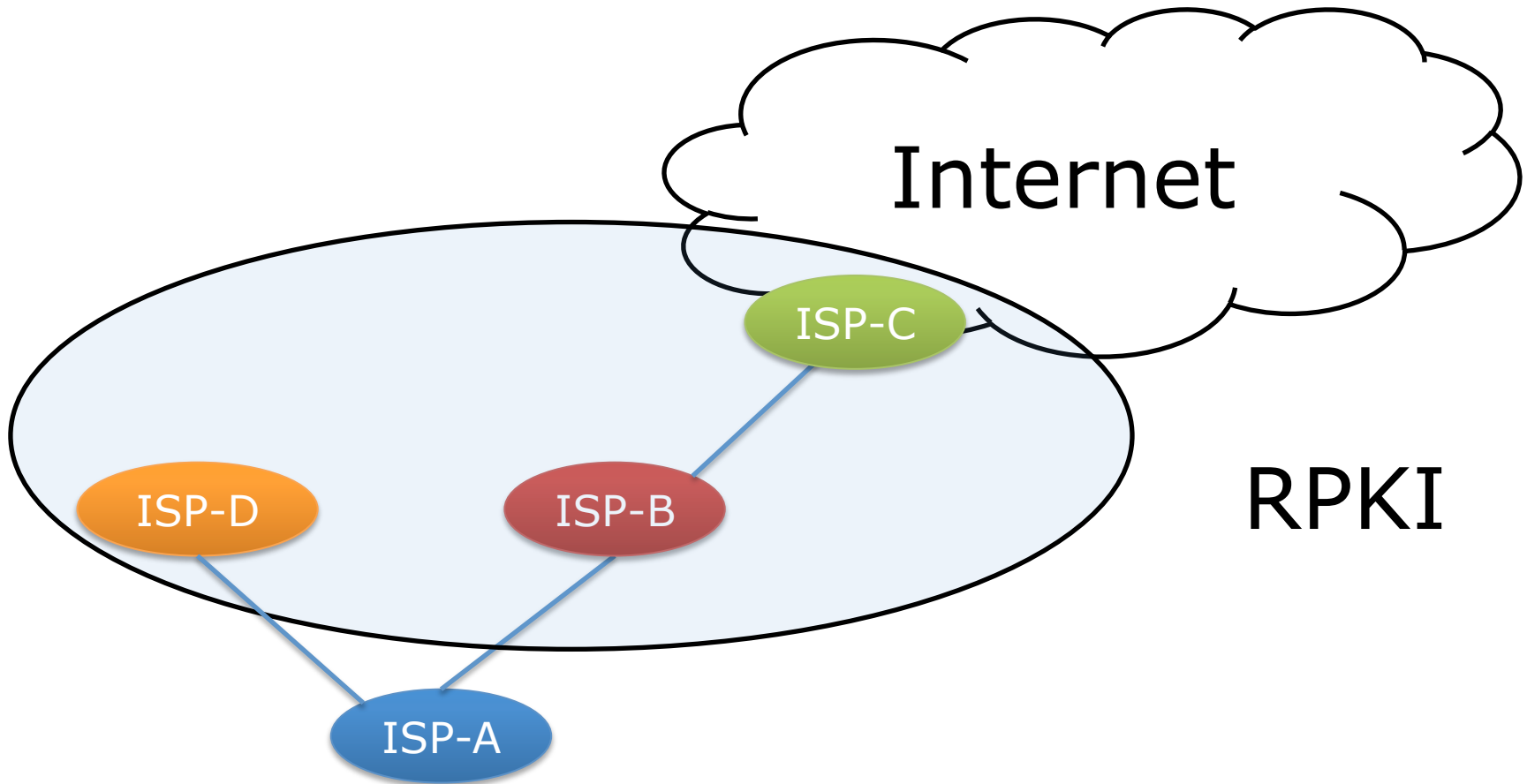


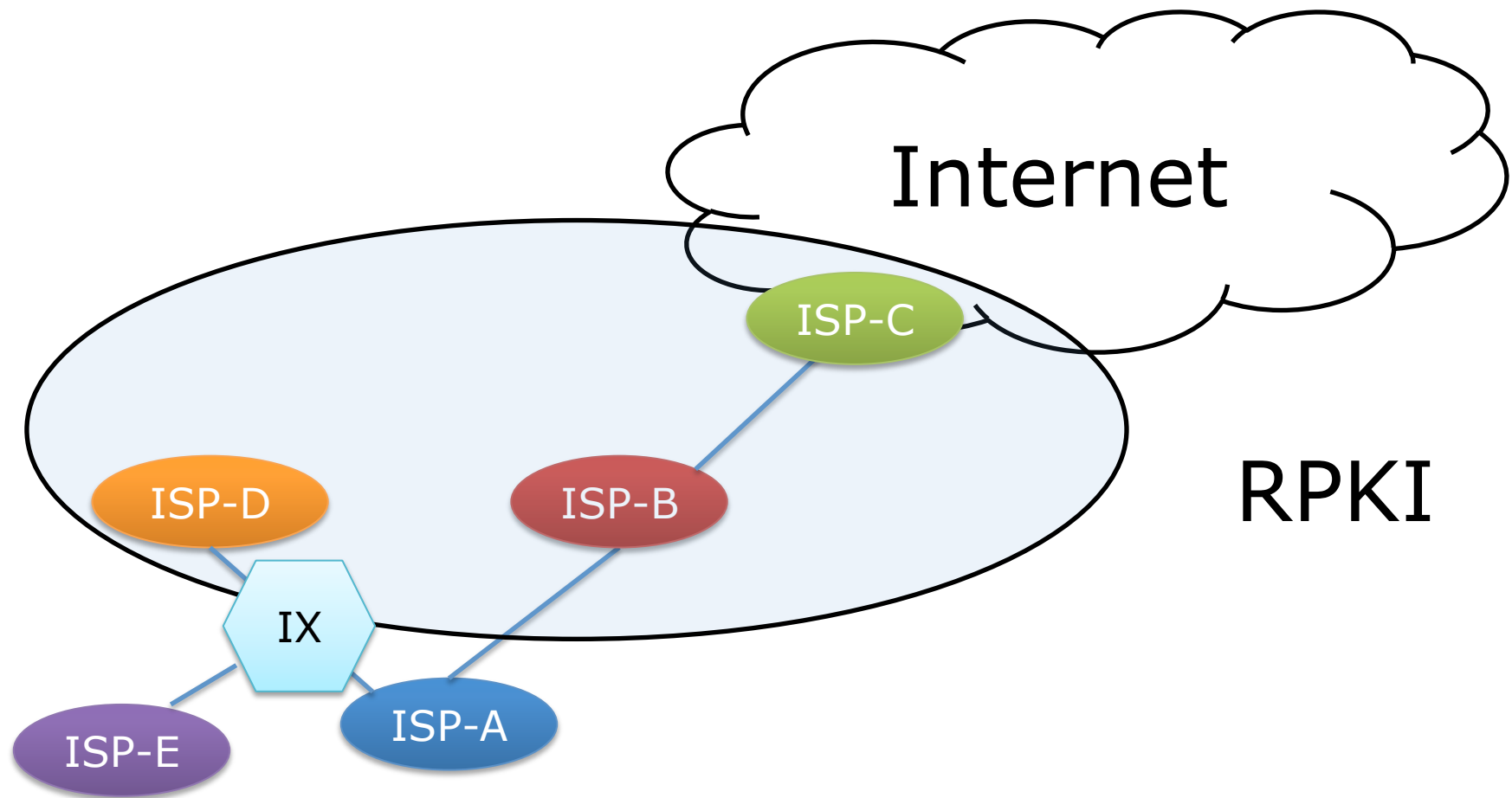
ISP-C次第で
他に曲がってしまう

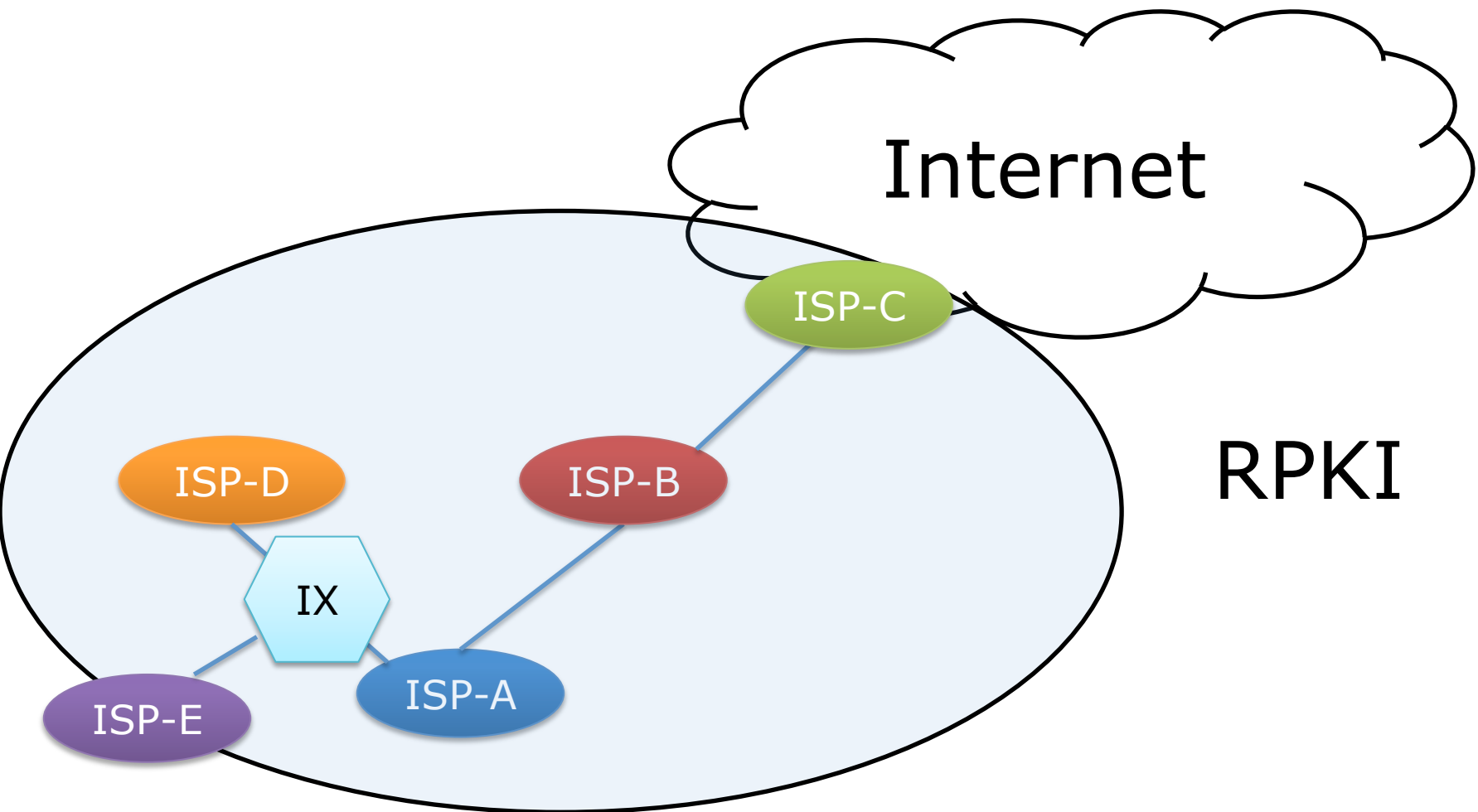






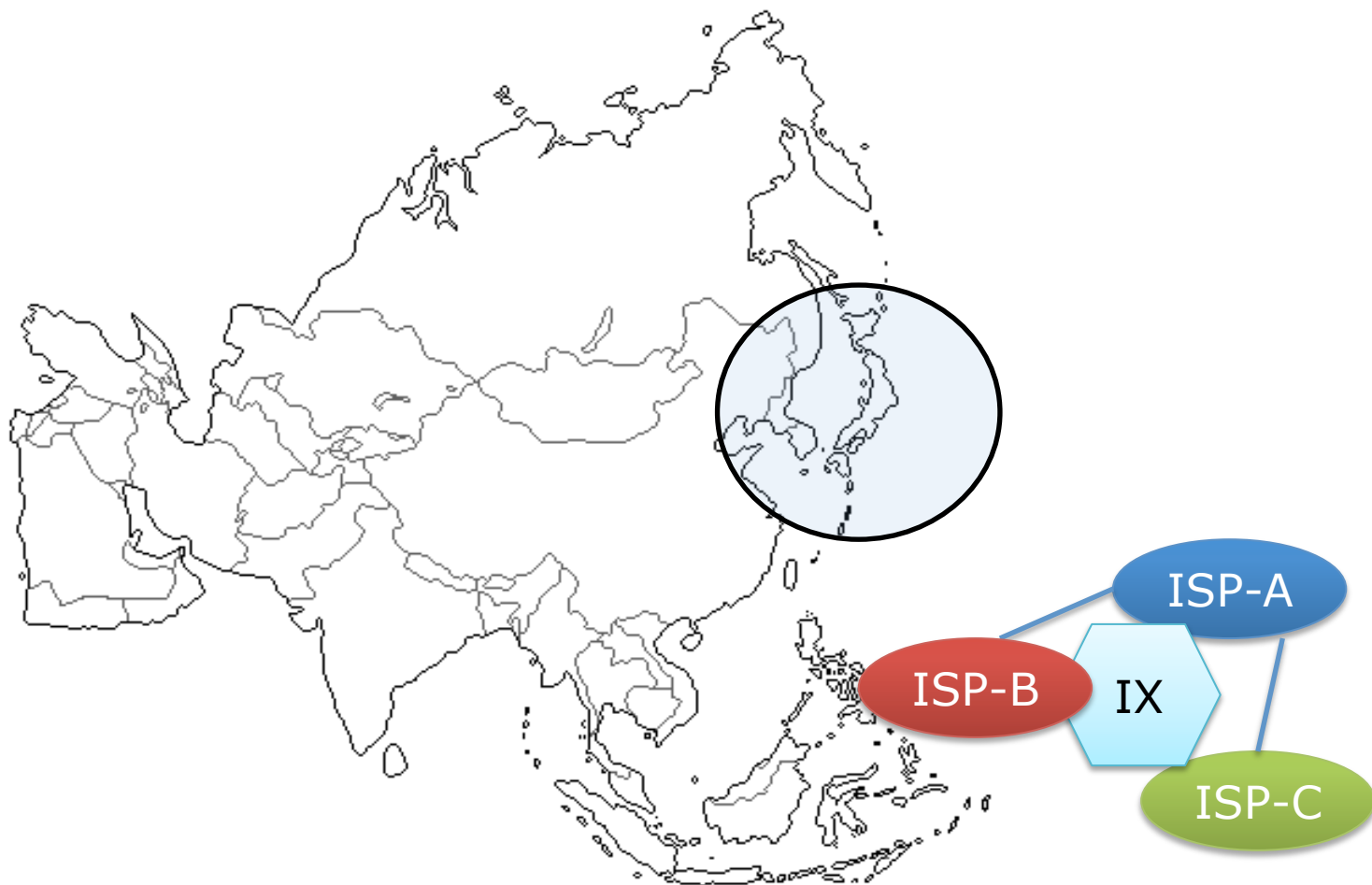






局所的でも効果はある

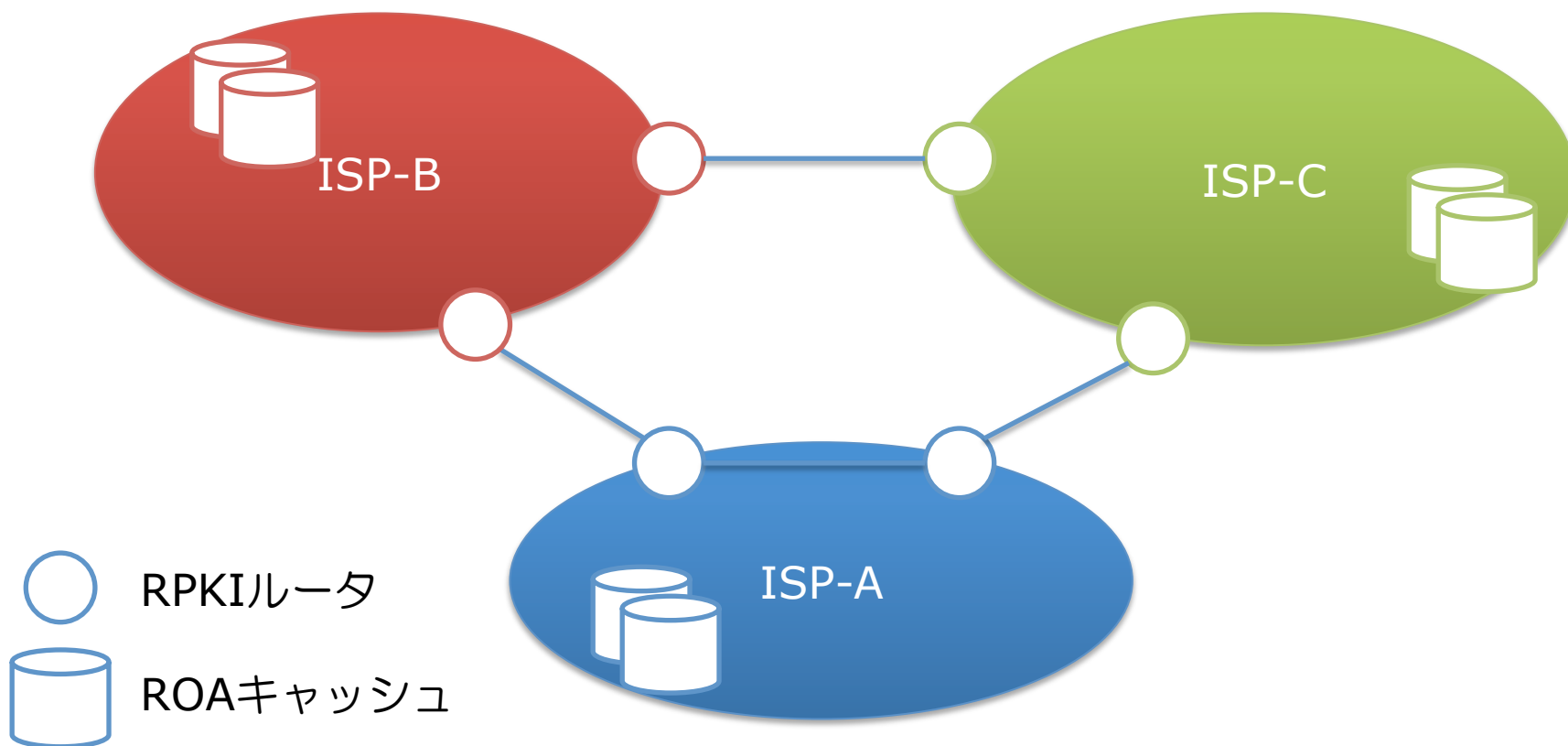
日本内の通信は影響を受けないですむ(etc)



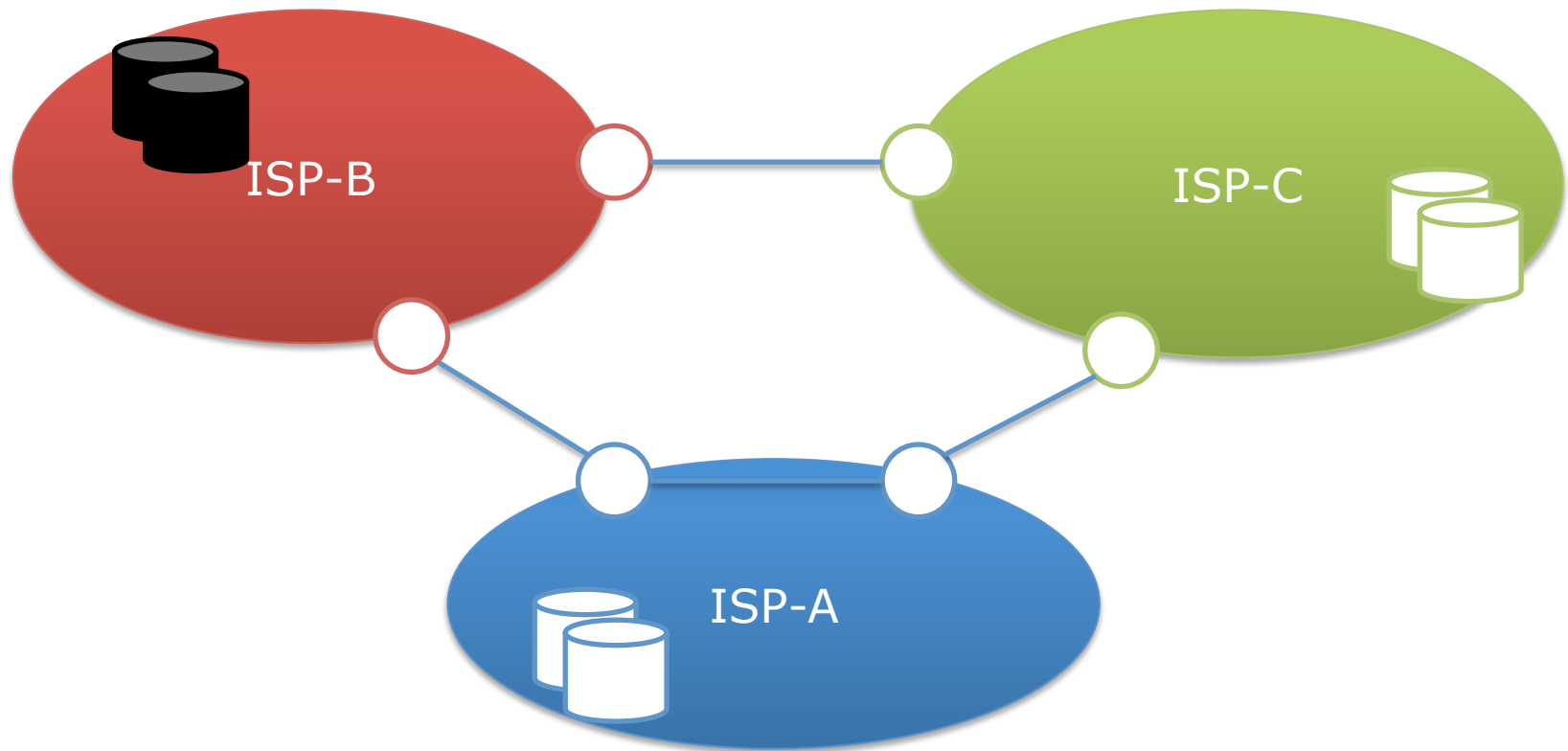
RPKIの適応例

各ISPにキャッシュを設置

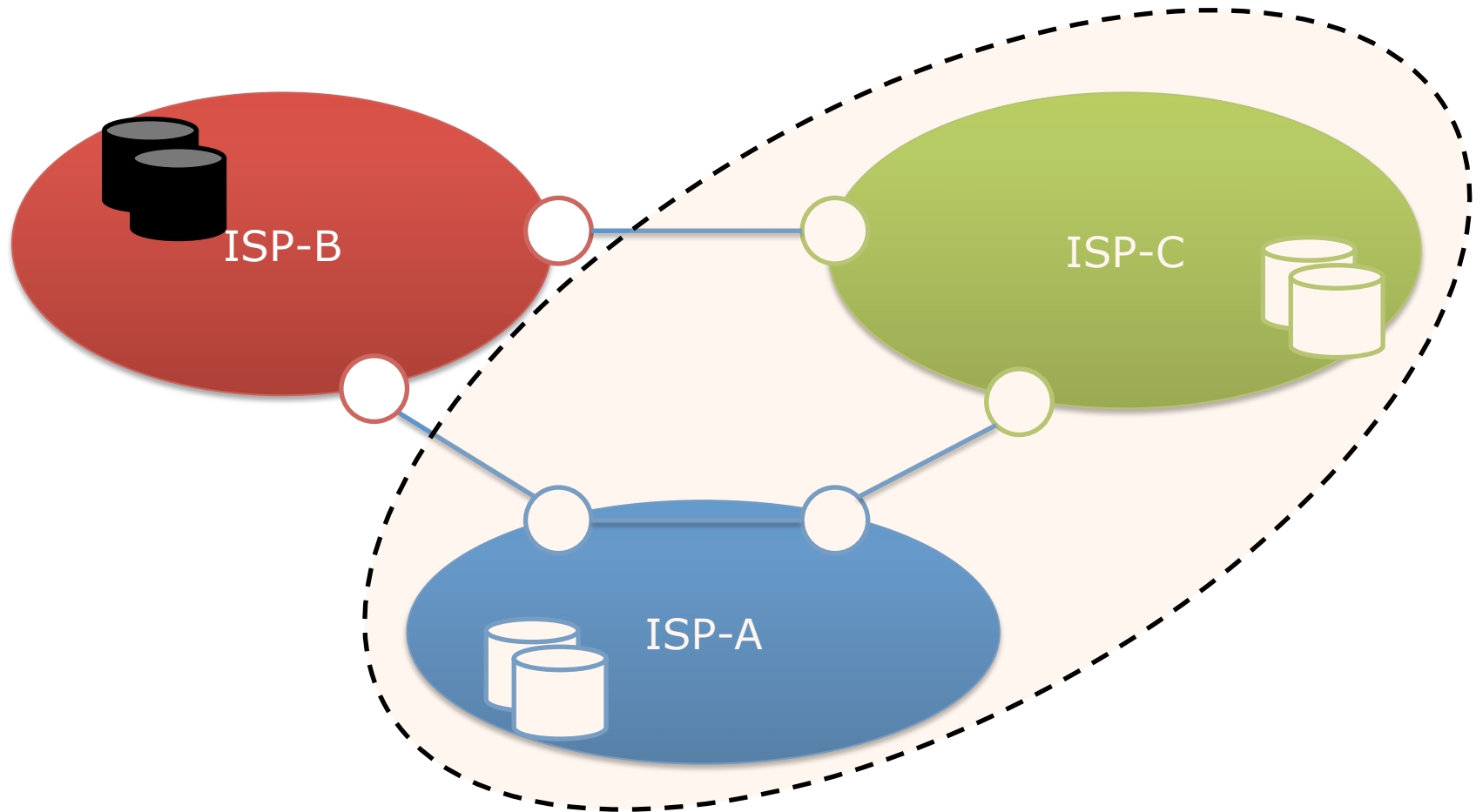
RPKIを動作させるルータは他ISPとの接続GWで



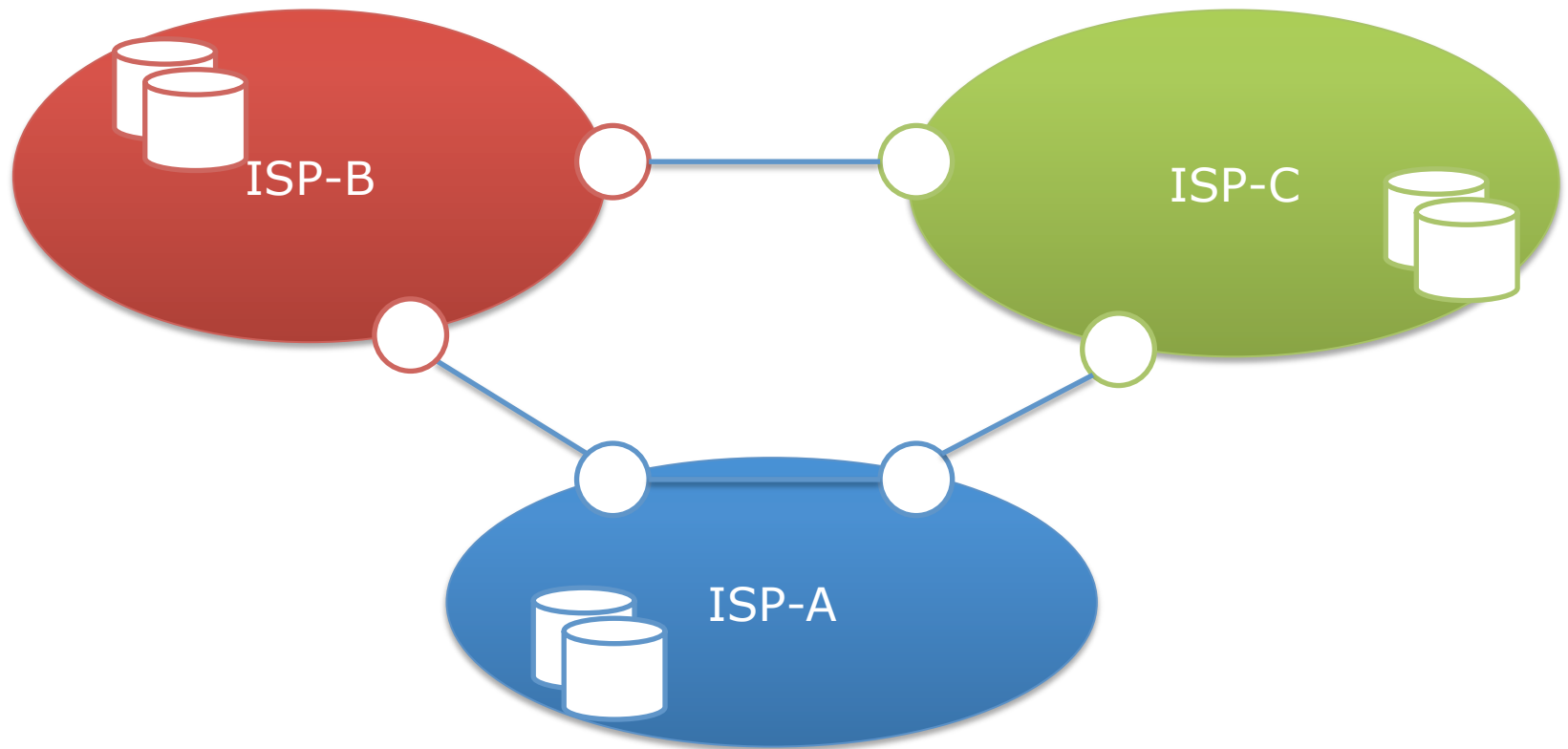
Cacheに毒が入った場合



一定の範囲は守られる

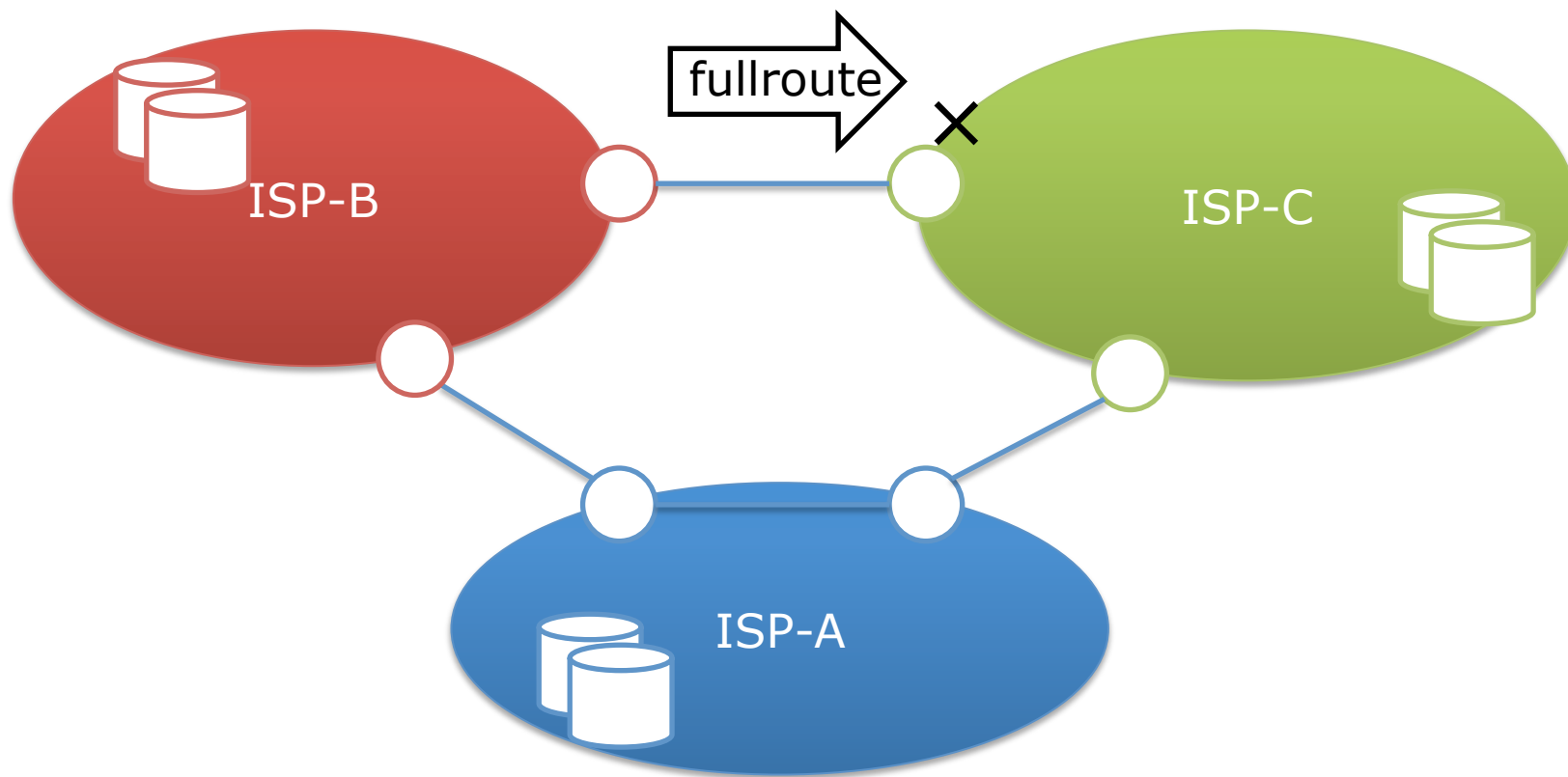


Filterはいらない？



Filterは必要

Validな経路だとしても、受け取っていいかとは別問題



ルータのpolicy

- 最終的にInvalidを皆がたたき落とさないという意味が無い
 - 局所的に適応してもYoutubeの事件はは防げない
- Validとnot foundに実際差をつける？
 - Valid : 64500 64501 64502 64503 7521
 - Not Found : 64500 7521
- Valid, Invalidと判定して欲しい人は、自分がROAをPublishするのと合わせ技

今後の展開

- Markingできるところを増やして、Monitoringしていく
- Transit ISPが適応していく
- Regional -> Global

ディスカッション

- その他に想定外のリスクは？
- RIRの運用は大丈夫？
 - 全部Invalidになったら？（想像したくない…）
- 共通のconfigポリシーをつくる？
- BGP Communityでうまく出来ない？
- 日本で出来るうまいやり方は？
- こんな実験をやってみると良いのでは？
- その他
 - IXのRouteServerからValidationした結果を送ったら嬉しいですね？