インターネット経路制御の信頼性向上に向けて

～RPKIの普及と課題～

2014/12/5
インターネットマルチフィード（株）
JPNIC IRR/RPKI動向調査専門家チーム Chair
吉田友哉 (yoshida@mfeed.ad.jp)

Agenda

- インターネット経路制御を脅かす脅威
- RPKIの現状と課題
- 今後の展望

インターネット経路制御を脅かす脅威

- 機器等の故障による物理的なもの
  - ルータがreloadを繰り返し、経路情報が不安定な状態が継続するetc..
- 制御機器（ルータ等）の解釈の違いやBug
  - Malformed AS_PATH attributeがついた経路情報をneighborから受信し、flapし続けるetc..

- 人為的な問題で経路制御に不具合が発生
  - ポリシーとは異なる経路広報
  - 経路ハイジャック、mis-origination

インターネット経路制御を脅かす脅威

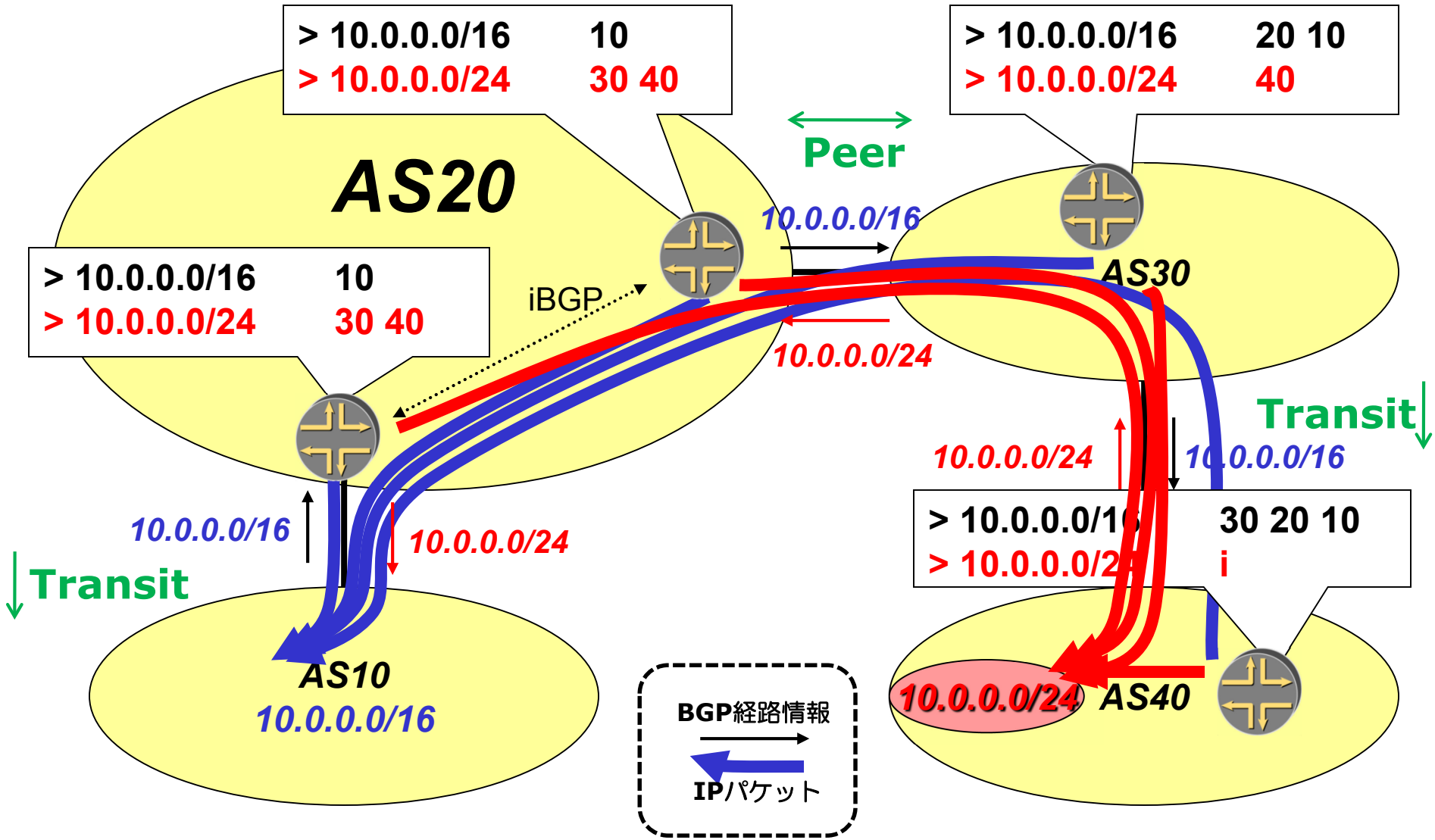
- 機器等の故障による物理的なもの
  - ルータがreloadを繰り返し、経路情報が不安定な状態が継続するetc..

- 制御機器（ルータ等）の解釈の違いやBug
  - Malformed AS_PATH attributeがついた経路情報をneighborから受信し、flapし続けるetc..

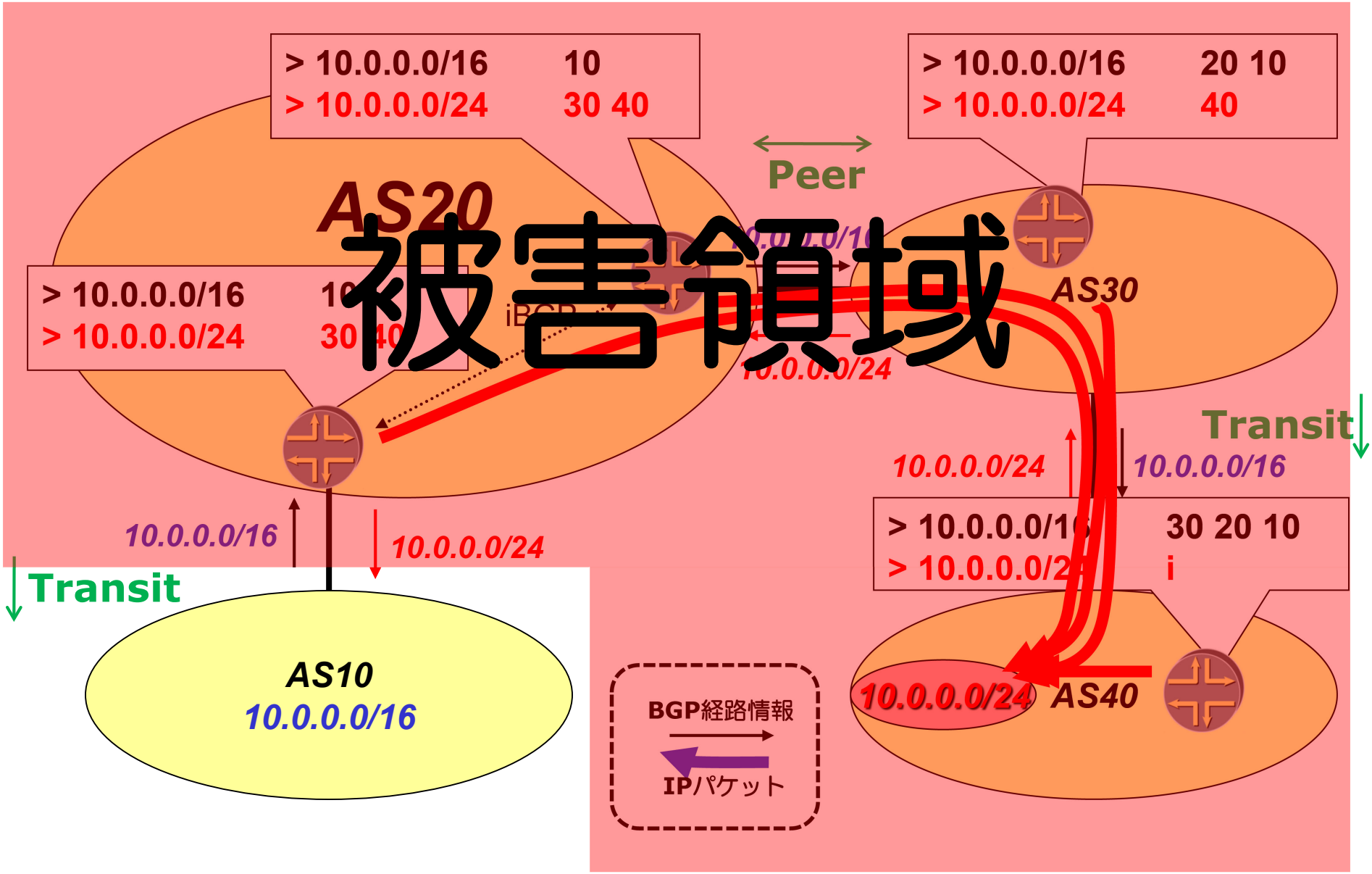
- 人為的な問題で経路制御に不具合が発生
  - ポリシーとは異なる経路広報

経路ハイジャック、mis-origination

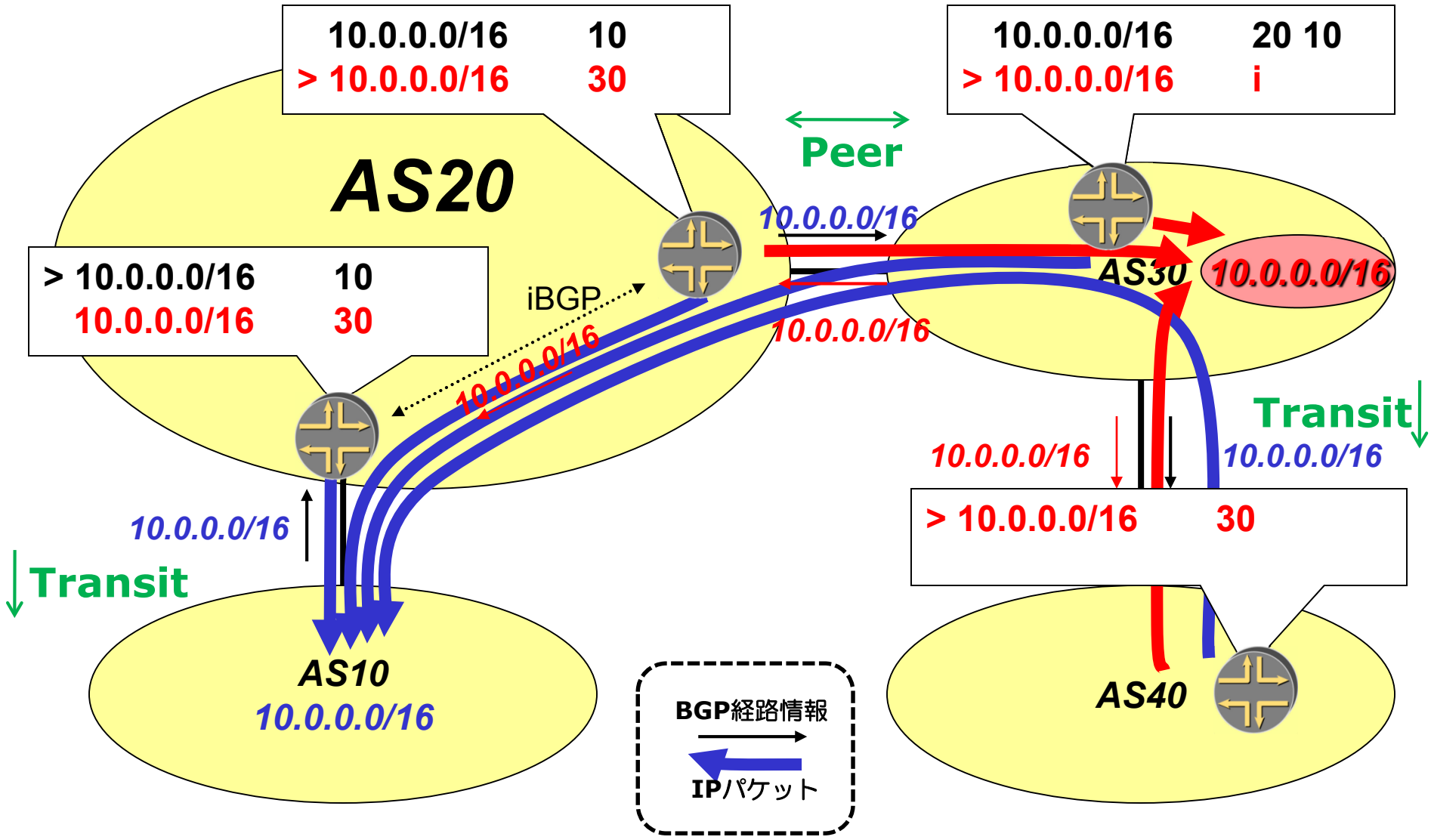
事例１：グローバルに影響が及ぶ場合



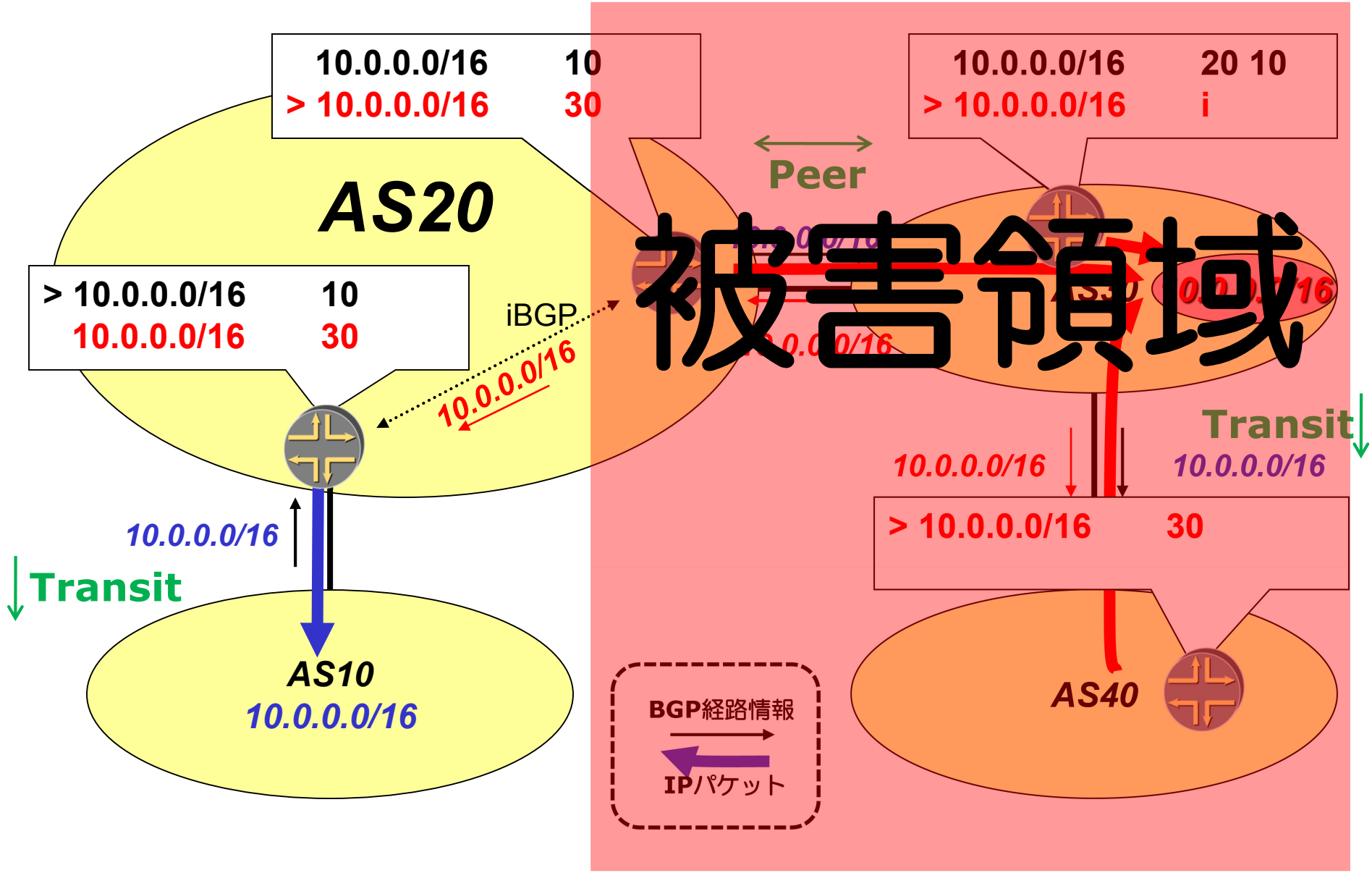
事例１：グローバルに影響が及ぶ場合



事例２：一部のエリアに影響が及ぶ場合



事例２：一部のエリアに影響が及ぶ場合



経路ハイジャック, mis-origination

- ２つの要因
  - Operational fault (Fat finger)
  - Intentional fault

- ちなみに、2008年に発生した “youtube incident”は、Fat finger, Intentional fault両方に該当する
  - パキスタンテレコムが自国に経路をまげるために内部からyoutubeのprefixを広告
  - それを上流のtransitISPがneighborに誤って経路広告してしまった

数年前の日本での事例

	事例１	事例２	事例３
時期	2004/6	2004/9	2006/11
不正経路広告元	日本国内ISP	アジアISP	アジアISP
Prefix	Longer, Invalid /24x2, /25x1, /29x1	Longer, Invalid /24x2	Same, Invalid /14x2, /17x2
Action	広告元に連絡 のち経路広報停止	PeerISPに連絡し 対処をうながす のち経路広報停止	NO Action (のちwithdrawn)
Impact	約150分	約2日	約5分
備考			のちの解析により、他の経路も含め広範囲にわたって経路を誤って広告していた模様

全てオペレーションミスによるものと推察

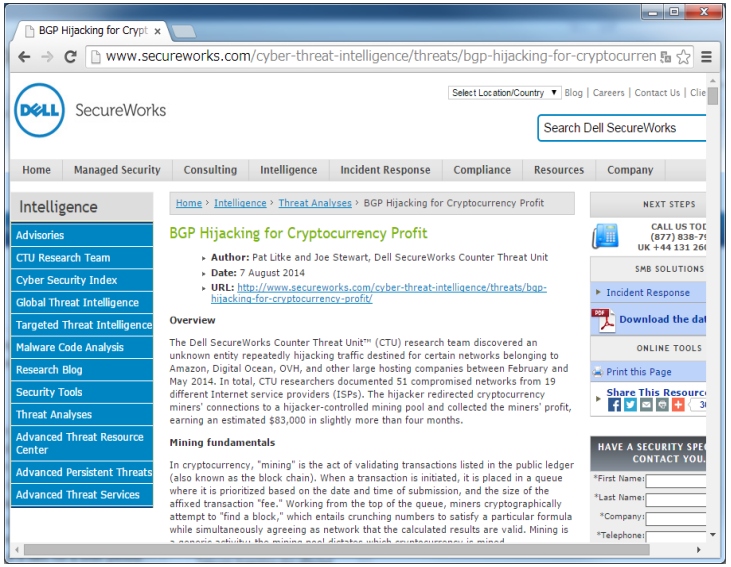
2014年の経路ハイジャック事情

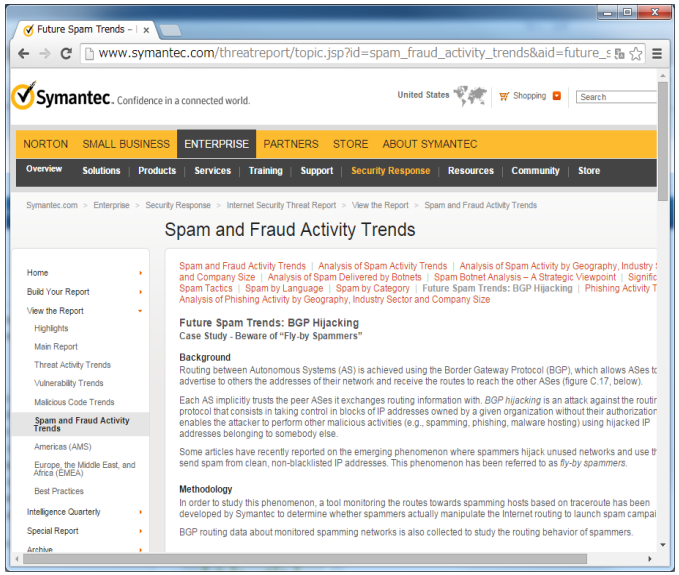
- 以前の愉快犯的な状況ではない。金銭目的の意図的なものも多い
  - BGP経路ハイジャックでBitcoin(8万ドル)を稼ぐ

    http://www.secureworks.com/cyber-threat-intelligence/threats/bgp-hijacking-for-cryptocurrency-profit/
    http://www.bgpmon.net/the-canadian-bitcoin-hijack/

  - BGP経路ハイジャックを使ったSPAM

    http://www.symantec.com/threatreport/topic.jsp?id=spam_fraud_activity_trends&aid=future_spam_trends
    https://www.usenix.org/conference/lisa-07/homeless-vikings-bgp-prefix-hijacking-and-spam-wars





Spamcopさんから…

(一時的な) 経路ハイジャック + SPAM

2014年2月、 弊社JPNAPのセグメント(/24)で“経路ハイジャックを使ったSPAM”を、ロ●アのASにやられた模様

時系列(JST)

2/11 23:47 経路奉行で経路ハイジャック発生検知
(218.100.45.0/24)

2/12 13:22 SPAM送信
(218.100.45.34, JPNAP未割当IP)

2/12 13:27 spamcopがSPAM検出

2/12 14:40 経路奉行で経路ハイジャック回復検知

2/12 PM spamcopからのメールに気づき対応
=> SPAMメールヘッダのMXレコードはすでに存在せず。

未利用IPを勝手に使う
組織的な犯罪との見方が強い

spamcopからのアラートメール

[SpamCop (218.100.45.34) id:6074690948]A sweet deal! Moto X. No contract. No down payment..

[SpamCop V4.8.1.007]

This message is brief for your comfort. Please use links below for details.

Email from 218.100.45.34 / Tue, 11 Feb 2014 22:27:49 -0600

http://www.spamcop.net/w3m?i=z6074690948z4d537a65b10c84041666fb2664f998cez

[Offending message]

Return-path: <Motorola@wappextil.com>

Received: from wappextil.com ([unknown] [218.100.45.34])
by vms172083.mailsrvcs.net
(Sun Java(tm) System Messaging Server 7u2-7.02 32bit (built Apr 16 2009))
with ESMTP id <0N0V004K08E3TI20@vms172083.mailsrvcs.net> for x; Tue, 11 Feb 2014 22:27:49 -0600 (CST)

Received: by wappextil.com id hvbsaa1hvj41 for <x>; Tue, 11 Feb 2014 23:22:31 -0500 (envelope-from <Motorola@wappextil.com>)

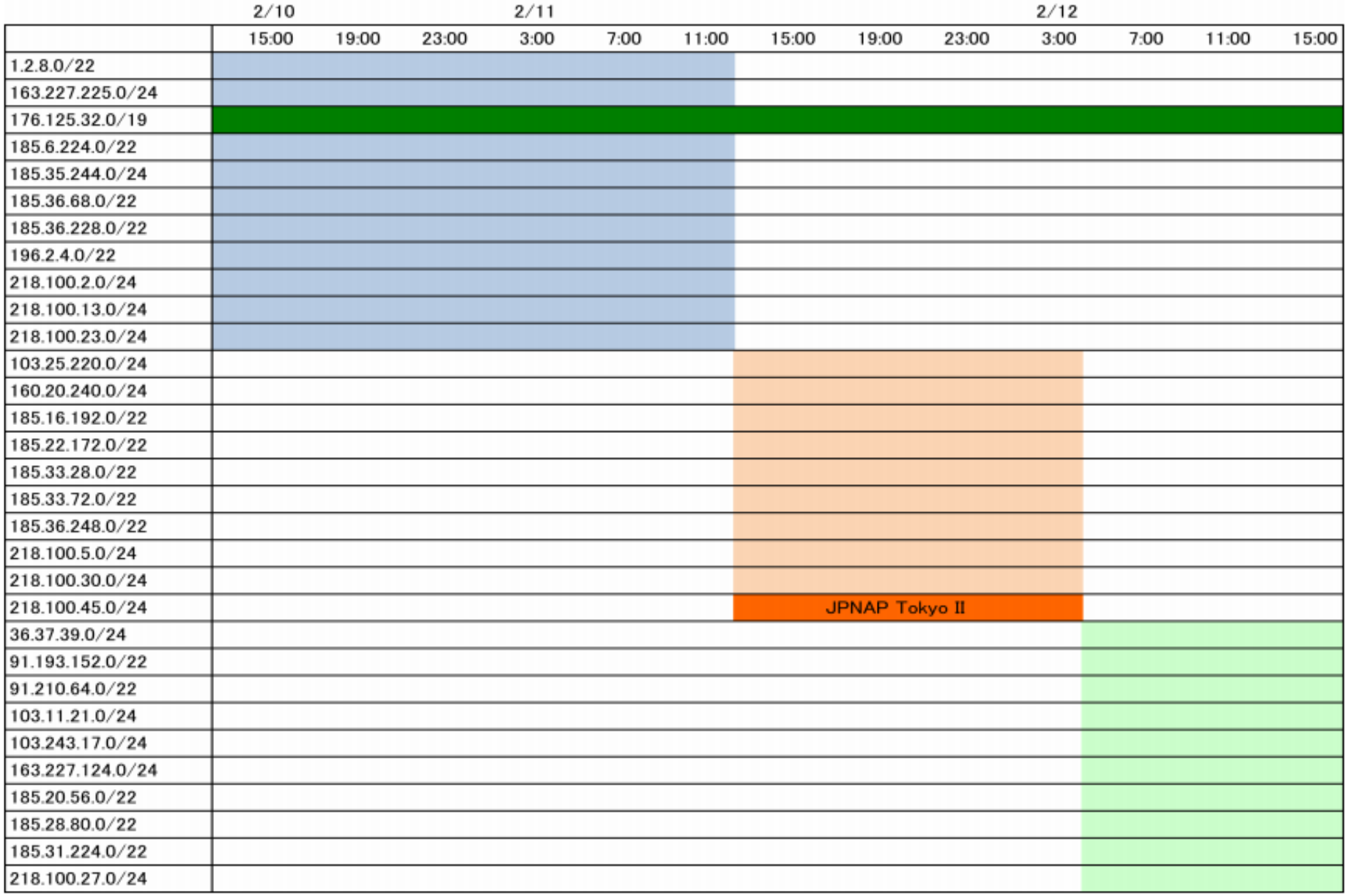
Date: Wed, 12 Feb 2014 04:22:30 +0000

From: "Motorola 7214186" <possible@wappextil.com>

Subject: A sweet deal! Moto X. No contract. No down payment. No hassles.

-- 以下、spamメールの内容添付 --

被害の状況（2/10-2/12）



実は多くのIXが被害を受けていた

Prefix	Desc
218.100.2.0/24	Sydney IX Lan
218.100.5.0/24	OBIS-IX,Internet Exchange Point,Okayama,Japan
218.100.13.0/24	Melbourne IX Lan
218.100.23.0/24	Dunedin Peering Exchange
218.100.27.0/24	OpenIXP, Internet Exchange Point, Indonesia
218.100.30.0/24	APJII Indonesia Internet eXchange
218.100.45.0/24	JPNAP Tokyo II IX

重要インフラのIPアドレスが脅威にさらされている

取り得る対応策

検知
detection
起きている状況にまずは気づく

回復
Recover
なるべく元の状態に回復させる

予防
Prevention
そもそも事象が起きないようにする

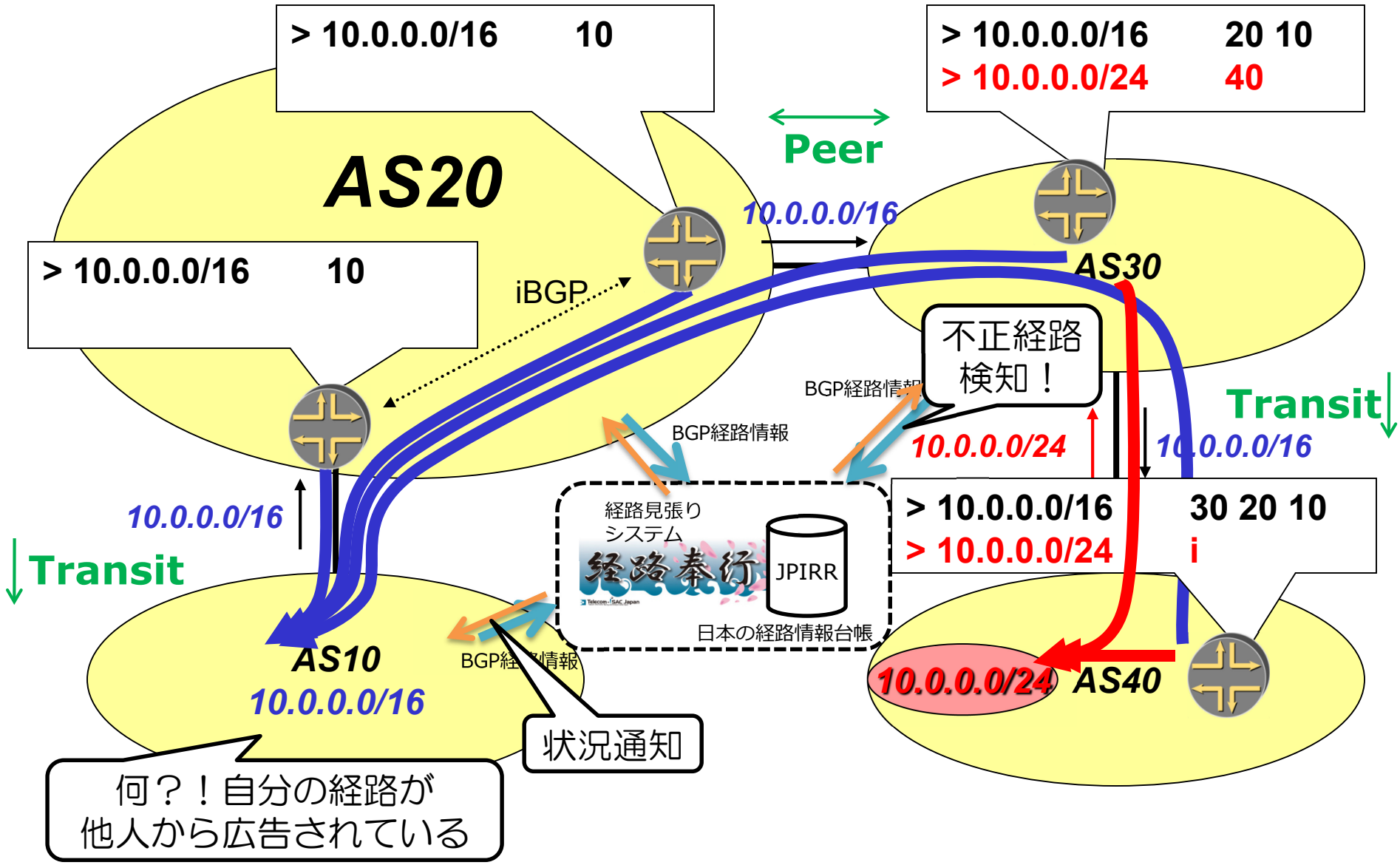
取り得る対応策

検知
detection
起きている状況にまずは気づく

回復
Recover
なるべく元の状態に回復させる

予防
Prevention
そもそも事象が起きないようにする

検知：Detection



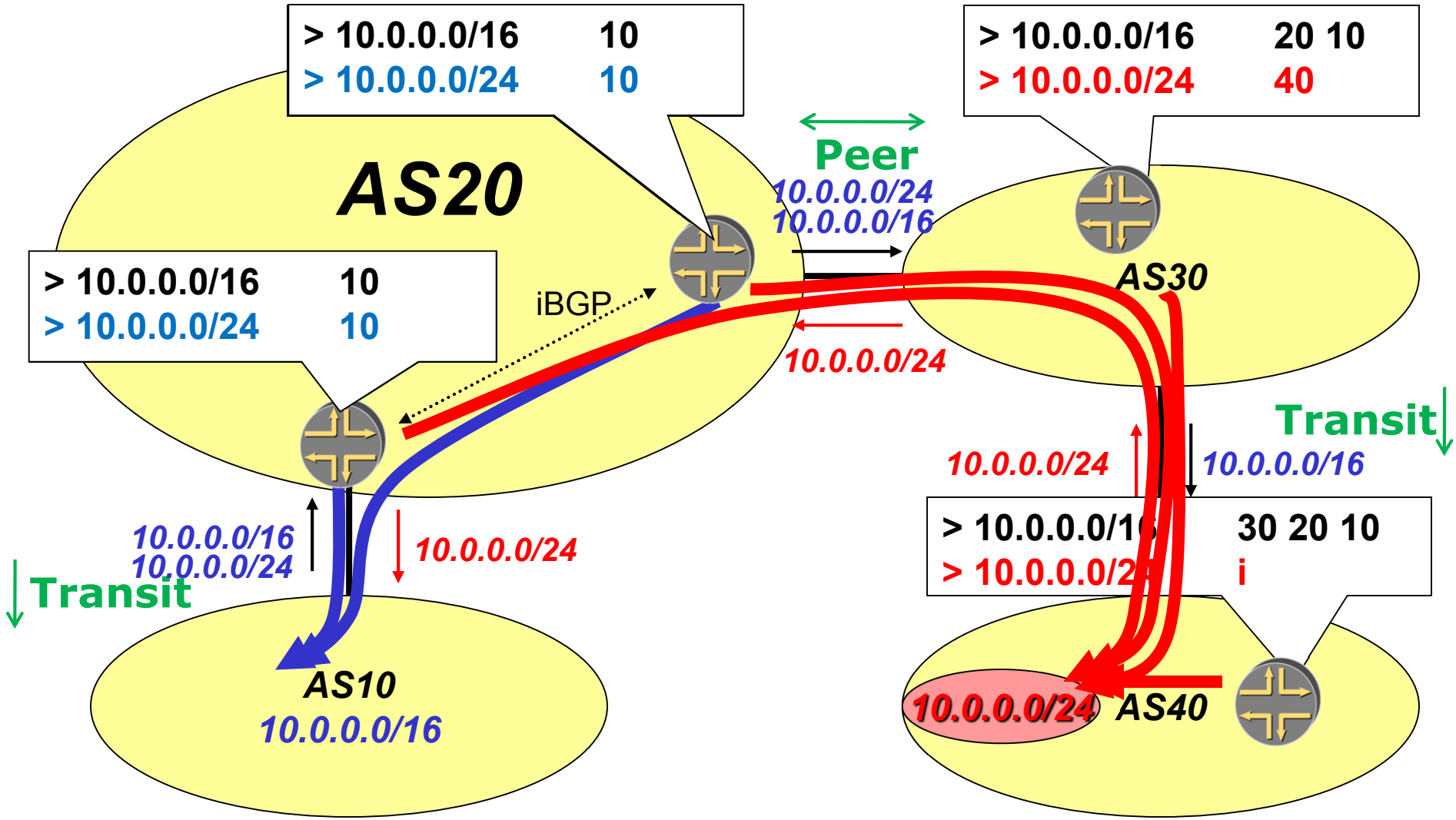
取り得る対応策

検知
detection
起きている状況にまずは気づく

回復
Recover
なるべく元の状態に回復させる

予防
Prevention
そもそも事象が起きないようにする

回復：Recover



一部の通信経路が回復

取り得る対応策

検知
detection

起きている状況にまずは気づく

回復
Recover

なるべく元の状態に回復させる

予防
Prevention

そもそも事象が起きないようにする

Resource Public Key Infrastructure

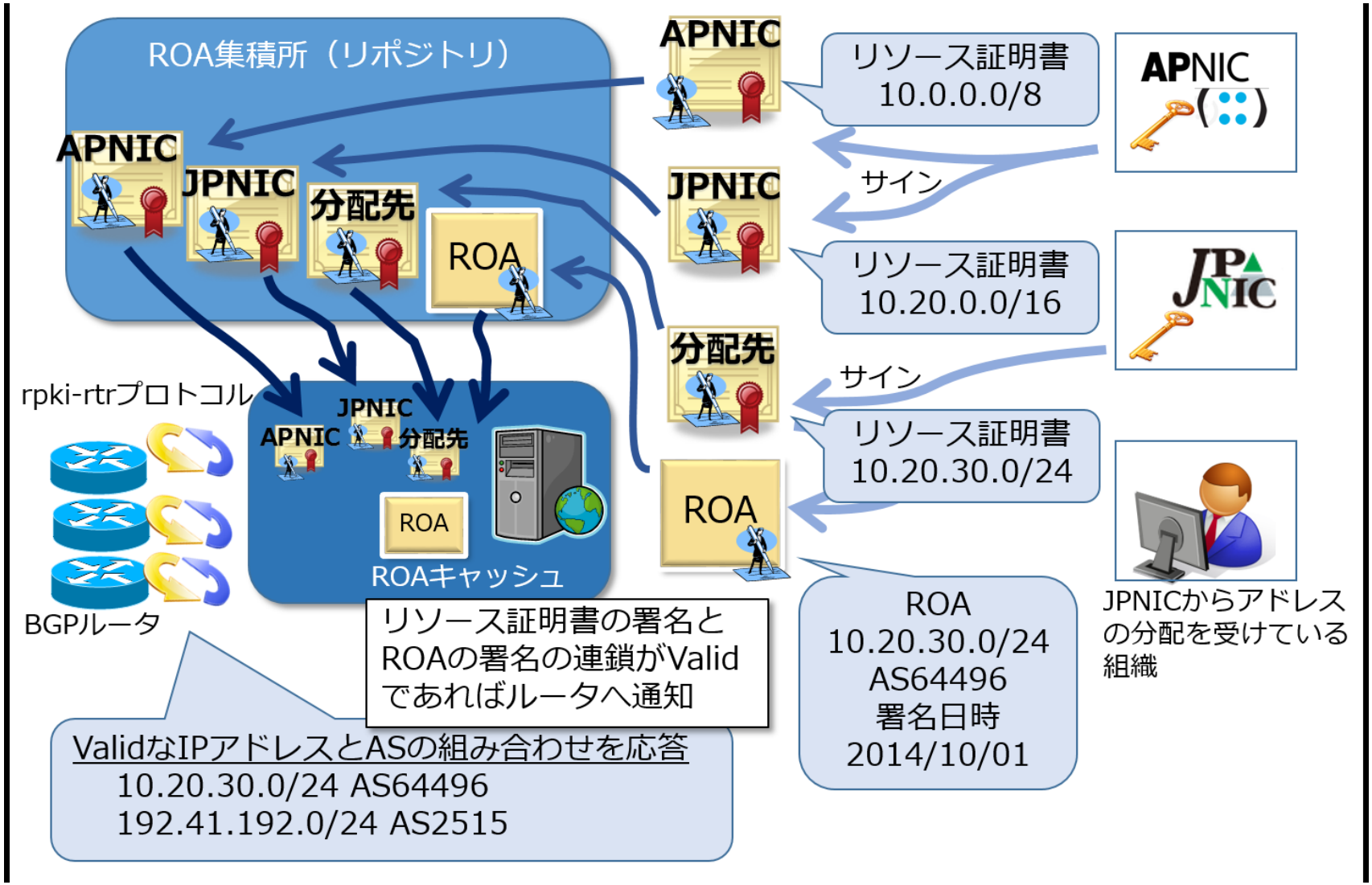
RPKI

RPKI

- Resource Public Key Infrastructureの略で、IPアドレスやAS番号リソースに関して、正しい所有者が誰なのかを証明するための認証基盤
- あるIPアドレスリソースが不正利用された場合でも、証明書により正しい保有者が誰なのかを証明することが可能となります
- RPKIは各地域のインターネットレジストリによって運用されています。アジア太平洋地域では現在APNICが正式に運用を行っており、日本ではJPNICが実験的にRPKIの運用を2013年より行っています。

http://www.mfeed.ad.jp/rpki/misc/whatisrpki.html

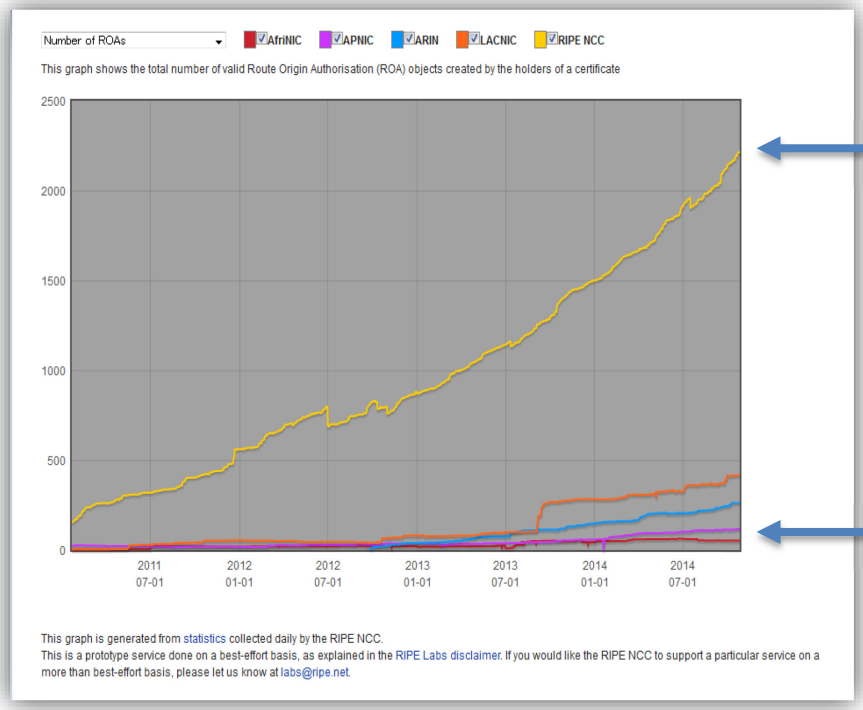
RPKIとROAの概要



https://www.nic.ad.jp/ja/rpki/

RPKIの普及状況

- 日本を含むアジア太平洋地域では、RPKIの普及がヨーロッパ地域等に比べて乏しい状況



RIPE

APNIC

登録されているROA数の推移
http://certification-stats.ripe.net/

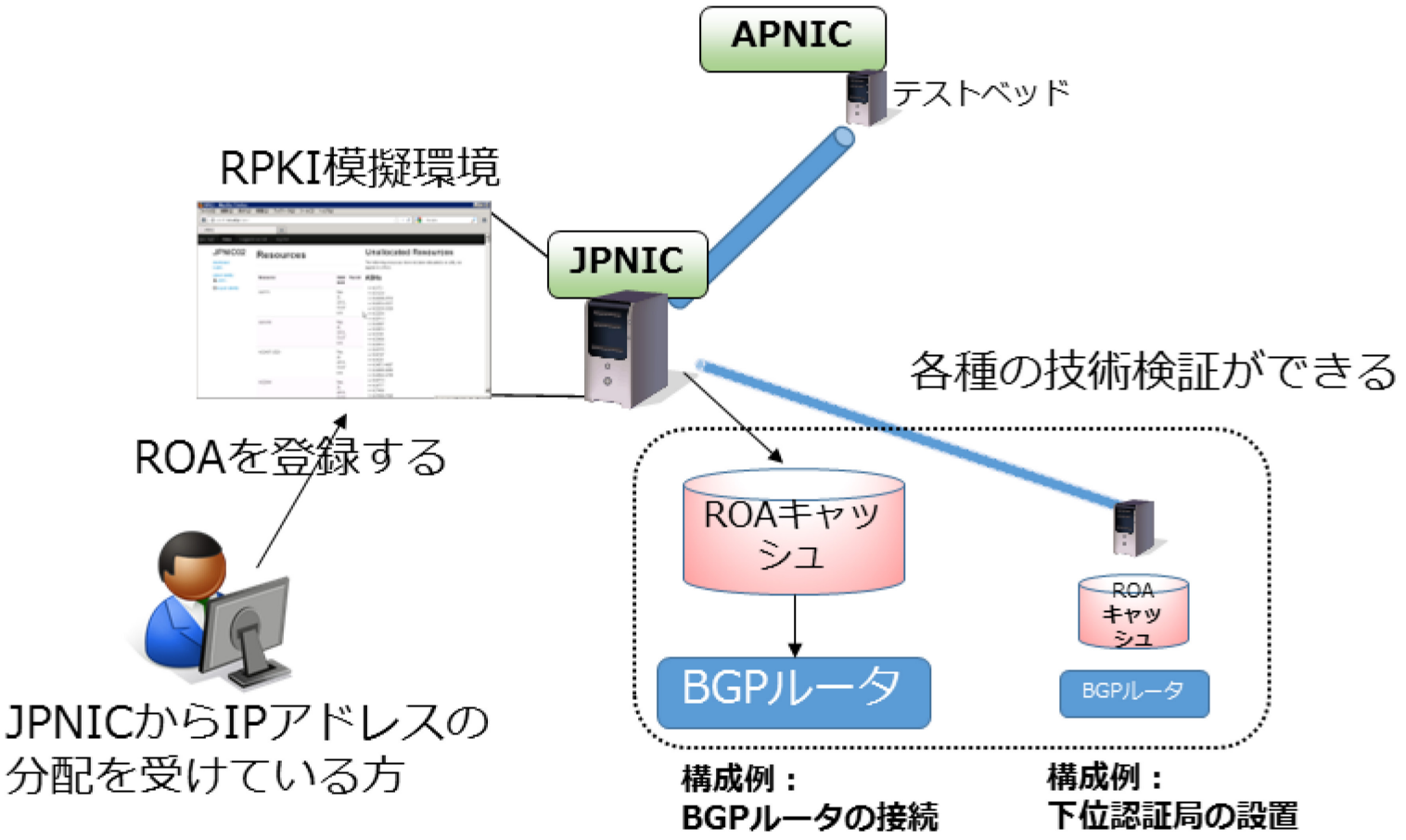
- 日本やアジア地域での普及促進が必要

日本でのRPKI本格利用に向けて

- 2014/10/1
  - 日本国内初「RPKI ROAパブリックキャッシュ情報配信」の試験提供をインターネットマルチフィード社とJPNICで開始
    - 世界中のROA情報（正しいPrefixとOriginAS情報）を気軽に取得することができ、AS内のBGP経路制御に活用
    - BGPルータが動作するインターネット環境からアクセス可能
  - RPKIに関するポータルサイト
    - IMF -> http://www.mfeed.ad.jp/rpki/
    - JPNIC -> https://www.nic.ad.jp/ja/rpki/

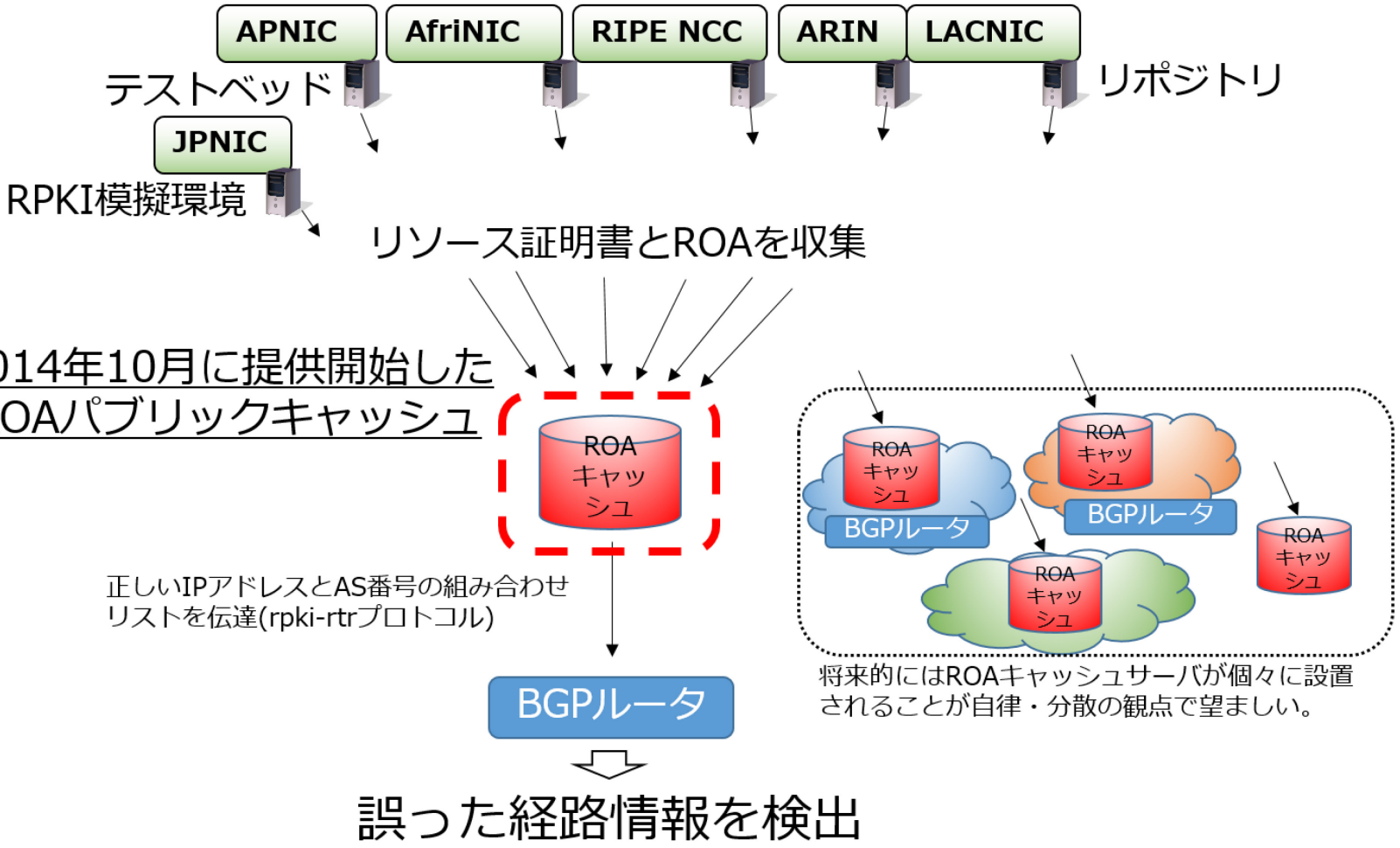
ROA: Route Origin Authentication

現在提供されているJPNIC模擬環境



https://www.nic.ad.jp/ja/rpki/

ROAパブリックキャッシュ情報提供



https://www.nic.ad.jp/ja/rpki/

JPNIC RPKI Project Page

JPNICはインターネットの円滑な運営を支えるための組織です

Top Q&A サイトマップ 文字サイズ：小 中 大

一般社団法人 日本ネットワークインフォメーションセンター
Japan Network Information Center

English(英語) RSS

サイト内検索… 検索

トップページ > インターネットの技術

プリント用ページの表示 ツイート いいね！ 34

リソースPKI(RPKI)

リソースPKI(RPKI)とは

リソースPKI(RPKI)は、 アドレス資源の割り振りや割り当てを証明するためのPKI(Public-Key Infrastructure: 公開鍵基盤)で、 IPアドレスが正しく割り振られたものであるかどうかを確認できるほか、 BGPルータにおける誤ったインターネットの経路情報(Mis-Origination)を見つけるために使えます。 IPアドレスの割り振りや割り当てを証明するリソース証明書(Resource Certificate)と呼ばれる電子証明書はRPKIを使って発行されます。

BGPを使ったインターネットの経路制御では、 「IPアドレス」と「インターネット上のネットワークを識別する番号(Autonomous System Number: AS番号)」が情報交換されます。 リソース証明書は、 IPアドレスとAS番号の正しい組み合わせを示すデータ「Route Origin Authorization(ROA)」を生成するために使えます。

- リソースPKIとは(インターネット用語1分解説)
- ROAとは(インターネット用語1分解説)
- BGPルータにおける誤ったインターネットの経路情報(Mis-Origination)

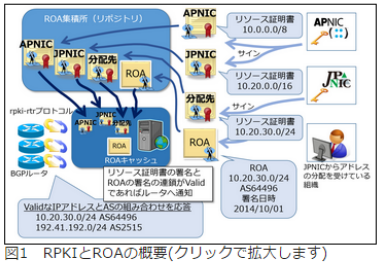


図1 RPKIとROAの概要(クリックで拡大します)

JPNICが提供するRPKI関連の仕組み

RPKI模擬環境

JPNICではRPKIを簡単に試す環境として、 RPKI模擬環境を提供しています。 模擬環境は、RPKIの使い方を体験できるシステムで、 APNICのRPKIテスト環境(APNICテストベッド)と連携しています。

RPKIを本格的に利用してゆくには、 リソース証明書に記載されるIPアドレスがIPレジストリシステムのデータベースに基づいたものである必要があると考えられます。 模擬環境では、RPKIの体験や技術検証のための環境であるため、 JPNICのRPKI担当者が、 模擬環境利用者の希望や状況に応じてIPアドレスの分配情報を入力しています。 利用者はROAの発行をWebから実行できます。 模擬環境で発行したROAは、 ROAパブリックキャッシュサーバ等へいくつかの処理を経た上で転送され、 BGPルータで検証が可能となっています。

RPKI模擬環境は、 IPアドレスの分配を受けている方がWebインタフェースを利用してROAを発行したり、利用者側で立ち上げられたROAキャッシュでそれを処理したり、 といった技術的な操作を確認するために使えます。

またRPKIのリソース証明書を自組織で発行できるRPKIのプログラム(例：RPKI Tools)の設定をして、JPNICの模擬環境と接続し、 動作検証をすることも可能です。

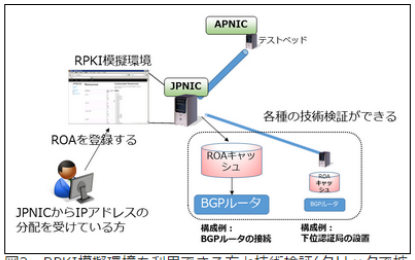


図2 RPKI模擬環境を利用できる方と技術検証(クリックで拡大します)

- JPNICとは
- IPアドレス
- インターネットの基礎
- ドメイン名
- インターネットガバナンス
- インターネットの技術
  - IETFとRFC
  - IRR
  - DNS
  - RPKI
  - ENUM
  - ドメイン名の国際化
- インターネットの歴史・統計
- ライブラリ
- JPNICトピックス一覧
- Web更新履歴一覧
- Q&A
- イベントカレンダー
- WHOIS

IMF RPKI Project Page

MF RPKI Project English

- ROAキャッシュ
- 技術情報
- 統計情報
- その他
- RPKIとは
- メンテナンス・障害情報
- 関連リンク
- 免責事項
- お問い合わせ

MF RPKIプロジェクト

インターネットにおけるBGP経路情報の交換では、AS運用者の設定ミスや悪意のある不正な経路広告によって、正しい宛先ネットワークに到達出来なくなる可能性があります。2008年に発生した、YouTubeが世界中から参照できなくなった事例のように、不正な経路情報がインターネット全体に蔓延し、世界中の通信に悪影響が及ぼされる事例も多く発生しています。

このような状況の中、インターネットマルチフィード社(MF)では、これまでJPNICや大手ルータベンダ各社等と連携し、インターネットの経路制御の信頼性向上を目指し、将来ISPの皆様が利用されるRPKI技術に関して、2012年よりROAキャッシュサーバの構築およびそれを参照するルータの動作検証を実施し、業界へフィードバックして参りました。

2014年10月1日より、日本のISPの皆様が今後RPKIの運用を本格化することを念頭に、ROAキャッシュサーバの運用を開始し、本格的にRPKI運用技術の習得およびインターネット全体の信頼性向上を目指し、より安心・安全なネットワーク環境を提供できるよう、インターネットの発展に貢献して参ります。

トピックス

2014/10/27 NEW!!

英語版ページをリリースしました。
Alcatelのルータ設定例を追加しました。

2014/10/01

MF RPKIプロジェクトページ(本サイト)を開設しました。
ROAキャッシュサーバの試験提供を開始しました。

いいね! シェア 66 +1 2
ツイート 2

ツイート フォローする

rpki_project @rpki_project 10月27日
English page has been released!
mfeed.ad.jp/rpki/en/index....
And added sample config for alcatel.

rpki_project @rpki_project 10月1日
インターネットルーティングにおけるRPKIの普及を目的として、ROAキャッシュサーバの提供を開始しました！
mfeed.ad.jp/rpki/index.html
開く

rpki_project @rpki_project 10月1日
URLは
mfeed.ad.jp/rpki/
です。

rpki_project @rpki_project 10月1日
インターネットルーティングにおけるRPKIの普及を目的として、ROAキャッシュサーバの提供を開始しました！
開く

さらに読み込む

@rpki_projectさん宛にツイートする

IMF RPKI Project Page

MF RPKI Project

ルータ設定例

下記の例では、AS65000のBGPルータがROAキャッシュサーバ(210.173.170.254)にRPKI-RTRプロトコルで接続するための基本的な設定例とコマンド例です。 対応するVersionやその他のオプションについては各ルータベンダにお問い合わせください。

Cisco IOS-XE

RPKI-RTR基本設定例

```
!
router bgp 65000
  bgp rpki server tcp 210.173.170.254 port 323 refresh 60
!
```

※ 上記設定では'RPKI State'が'valid'または'not found'のBGP経路のみ がルーティングテーブルにインストールされます。 invalidのBGP経路も追加したい場合は下記を参考にしてください。

BGP Origin Validation設定例('invalid'と判定された経路もルーティングテーブルにインストールする場合)

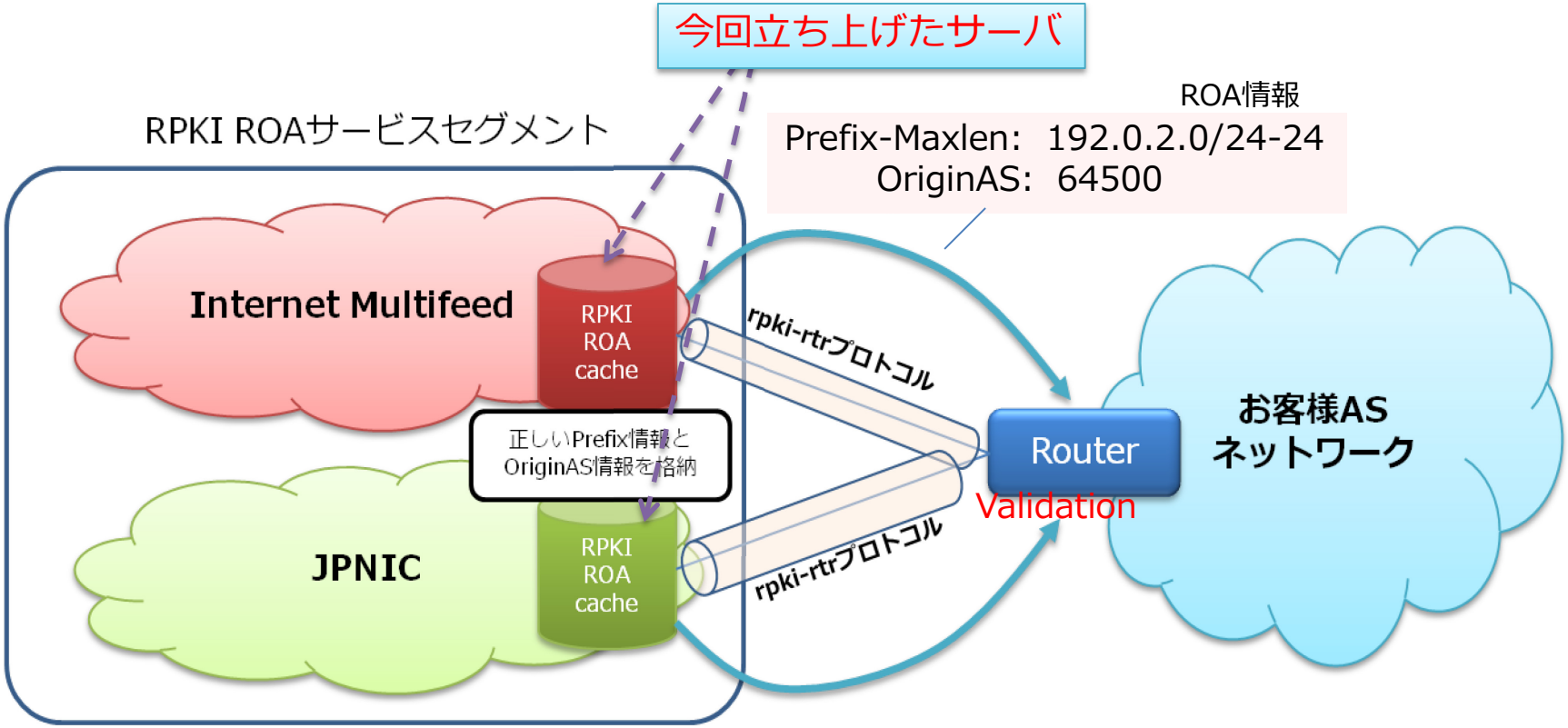
```
!
router bgp 65000
  address-family ipv4
    bgp bestpath prefix-validate allow-invalid
  exit-address-family
  !
  address-family ipv6
    bgp bestpath prefix-validate allow-invalid
  exit-address-family
!
```

※ その他のアクションを行いたい場合はroute-mapを書く必要があります。

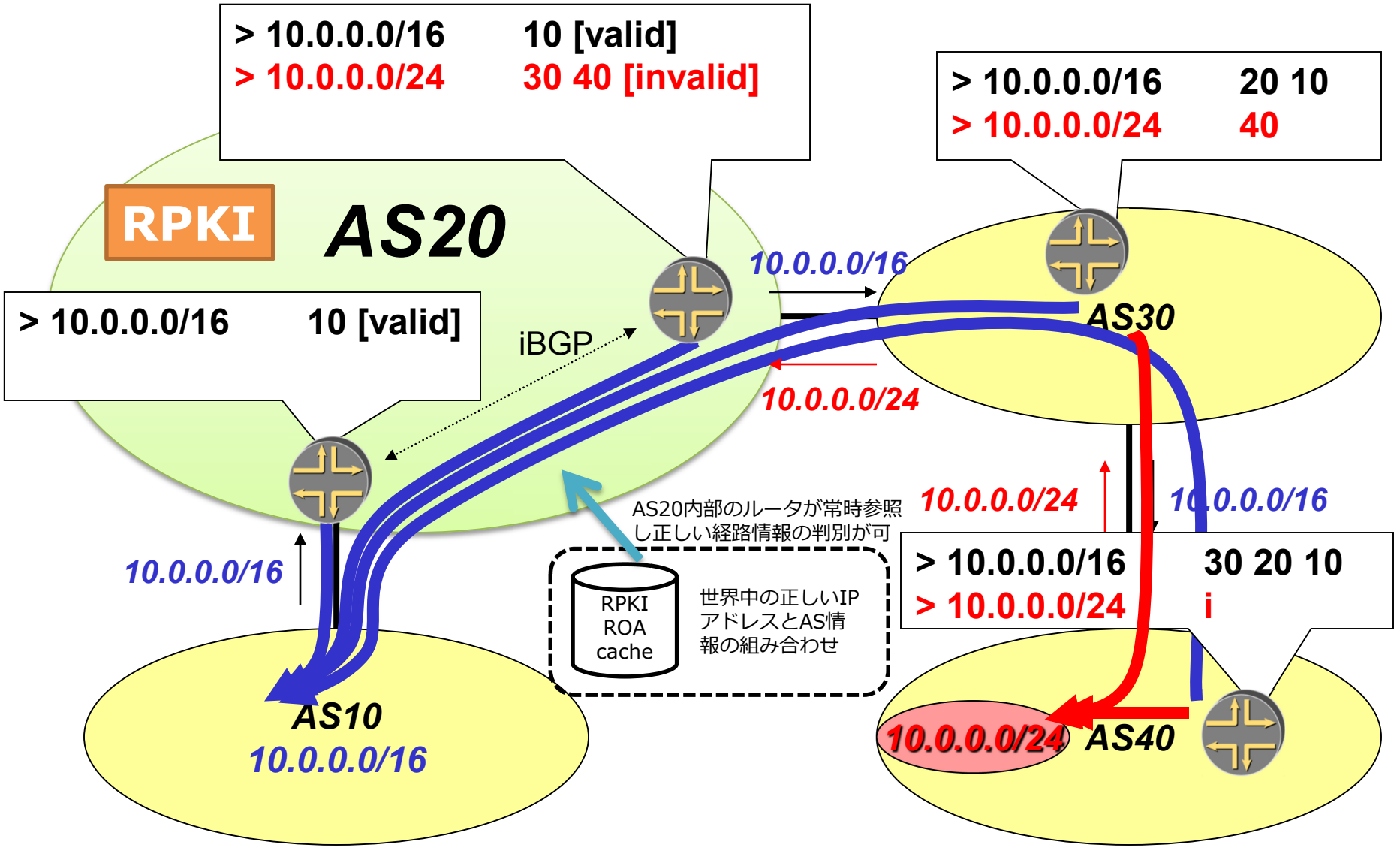
RPKI-RTRセッション確認コマンド

```
Cisco> show ip bgp rpki servers
```

サービス提供概念図


今回立ち上げたサーバ
ROA情報
Prefix-Maxlen: 192.0.2.0/24-24
OriginAS: 64500
RPKI ROAサービスセグメント
Internet Multifeed
RPKI
ROA
cache
正しいPrefix情報と
OriginAS情報を格納
JPNIC
RPKI
ROA
cache
rpki-rtrプロトコル
rpki-rtrプロトコル
Router
Validation
お客様AS
ネットワーク

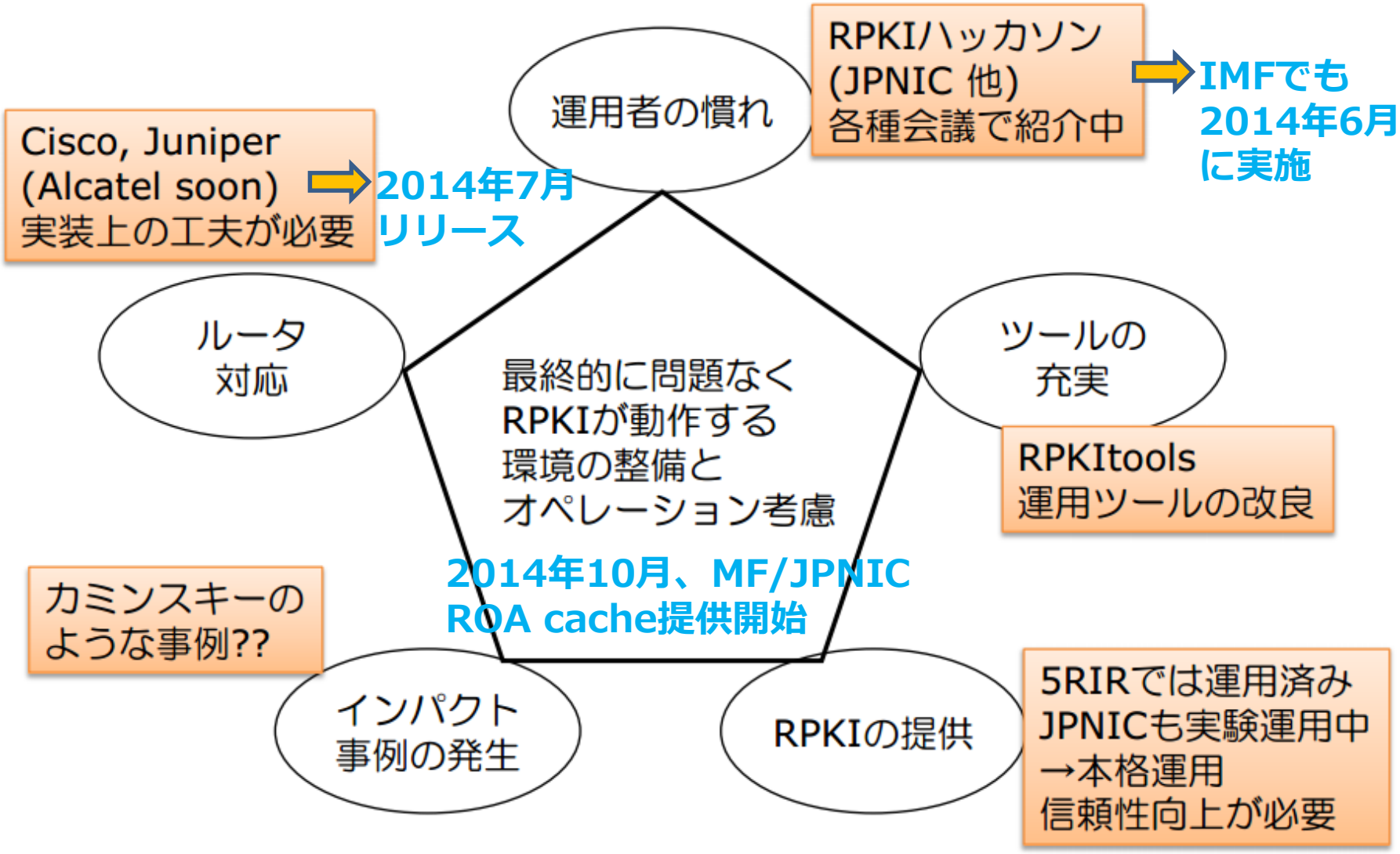
予防：Prevention w/RPKI



RPKI普及に向けた課題

- ROAの情報がまだまだ不足
  - RPKIを活用して経路制御できるレベルではない
- ISPでのROAキャッシュ運用のハードルが高い
  - X509等の証明書関連技術知識が必要
  - 提供ツールがまだ発展途上の段階
- ARINのROA情報の取得／提供に制限がある
  - ARINは、RPA(Relying Party Agreement)によって第三者への情報提供を禁止している
- RPKI-RTR(tcp:323) プロトコルのTLS encryptionが未サポート
  - ROAのような重要な情報に関するデータ転送には必須
  - CiscoやJuniperなどの大手ルータベンダも未サポート
- RPKIの重要性は理解できるが、社内で導入するにあたり、メリットを上司に説明できない。。
  - 世界中の人が登録しないと意味がない？？
  - 実際に経路制御にどう適応したらよいの？？

RPKI普及に関する要素と現状

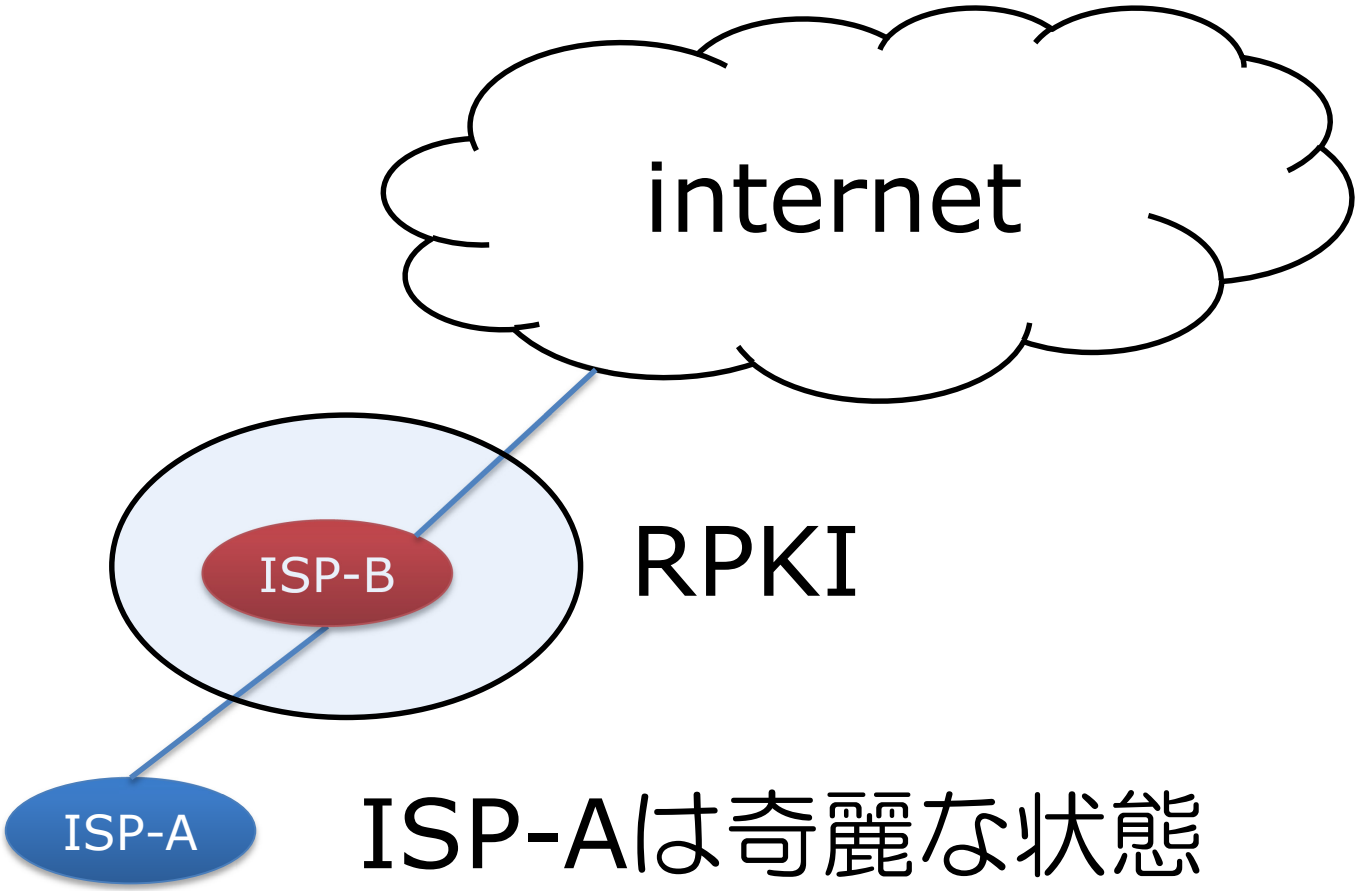


Source: JPNIC岡田氏の講演資料を元に作成

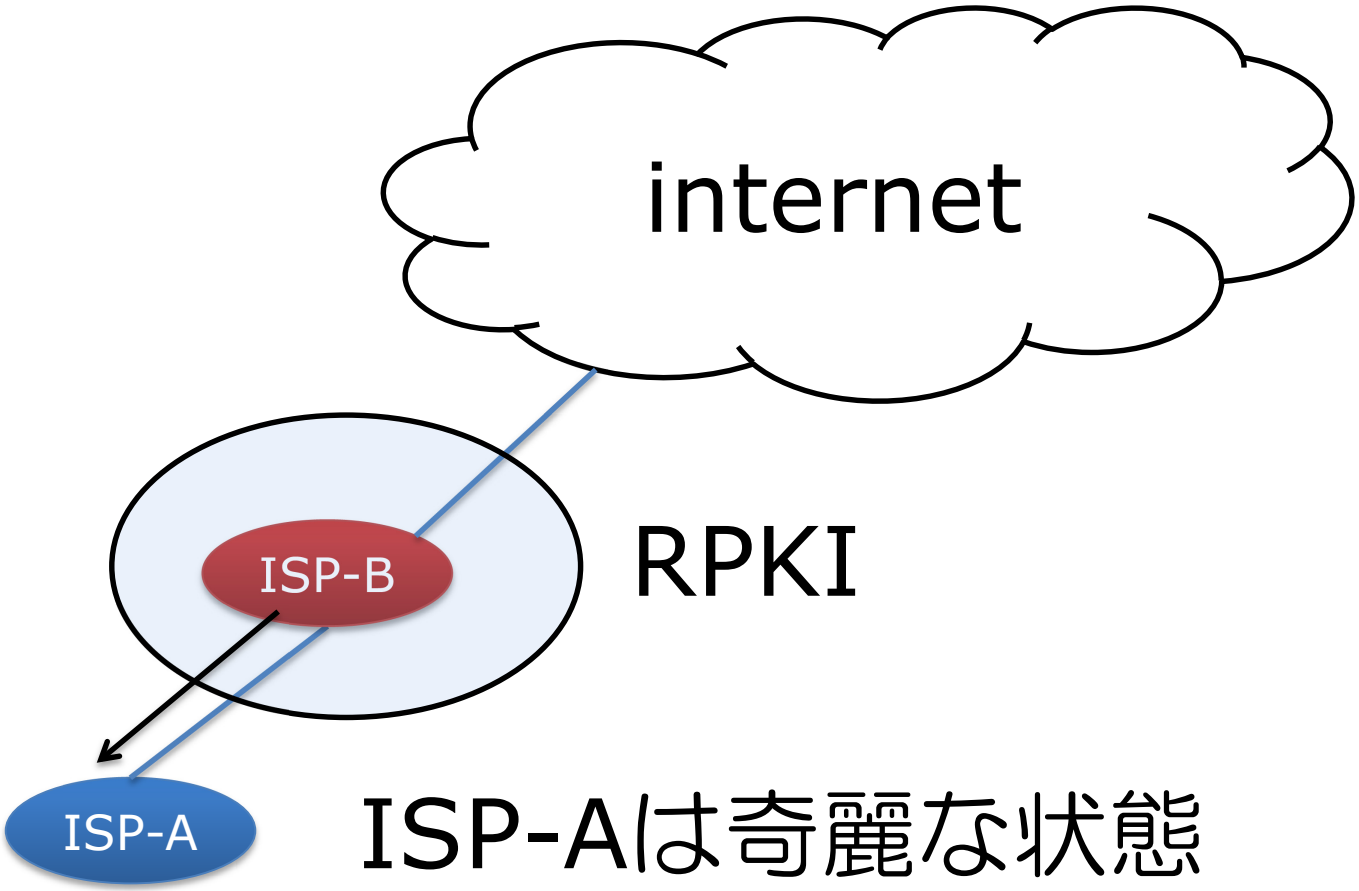
RPKI活用モデル

- 経路情報の不整合検知
- 顧客経路のフィルタ情報としての活用
- Peer/上流ISPからの受信経路制御
- IXのroute-serverでの信憑性向上
- IRRへの自動オブジェクト登録(rpki2irr)
- 持ち込みアドレスの認証
- リソース保持の証明

RPKI Deployment

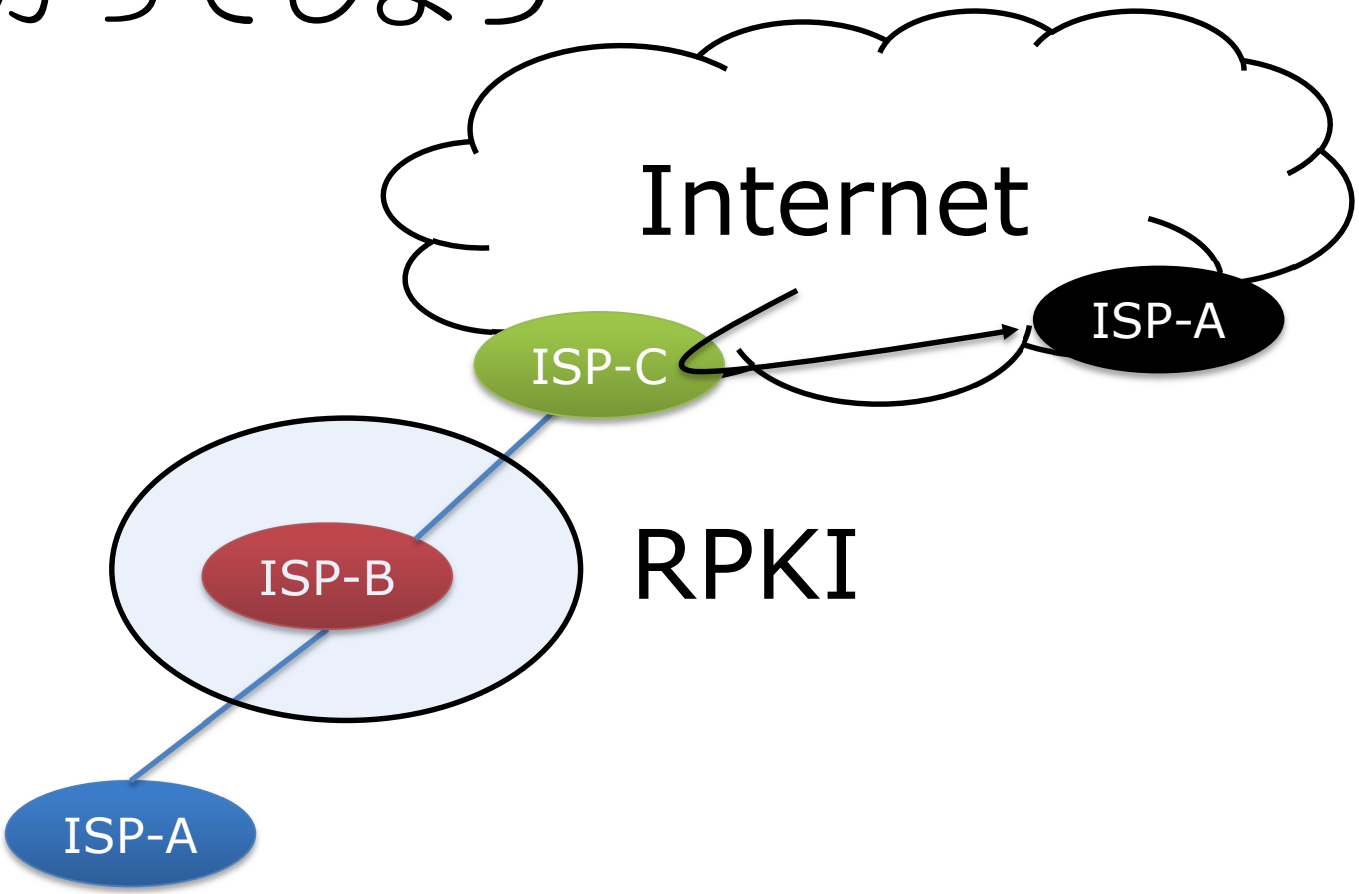


RPKI Deployment

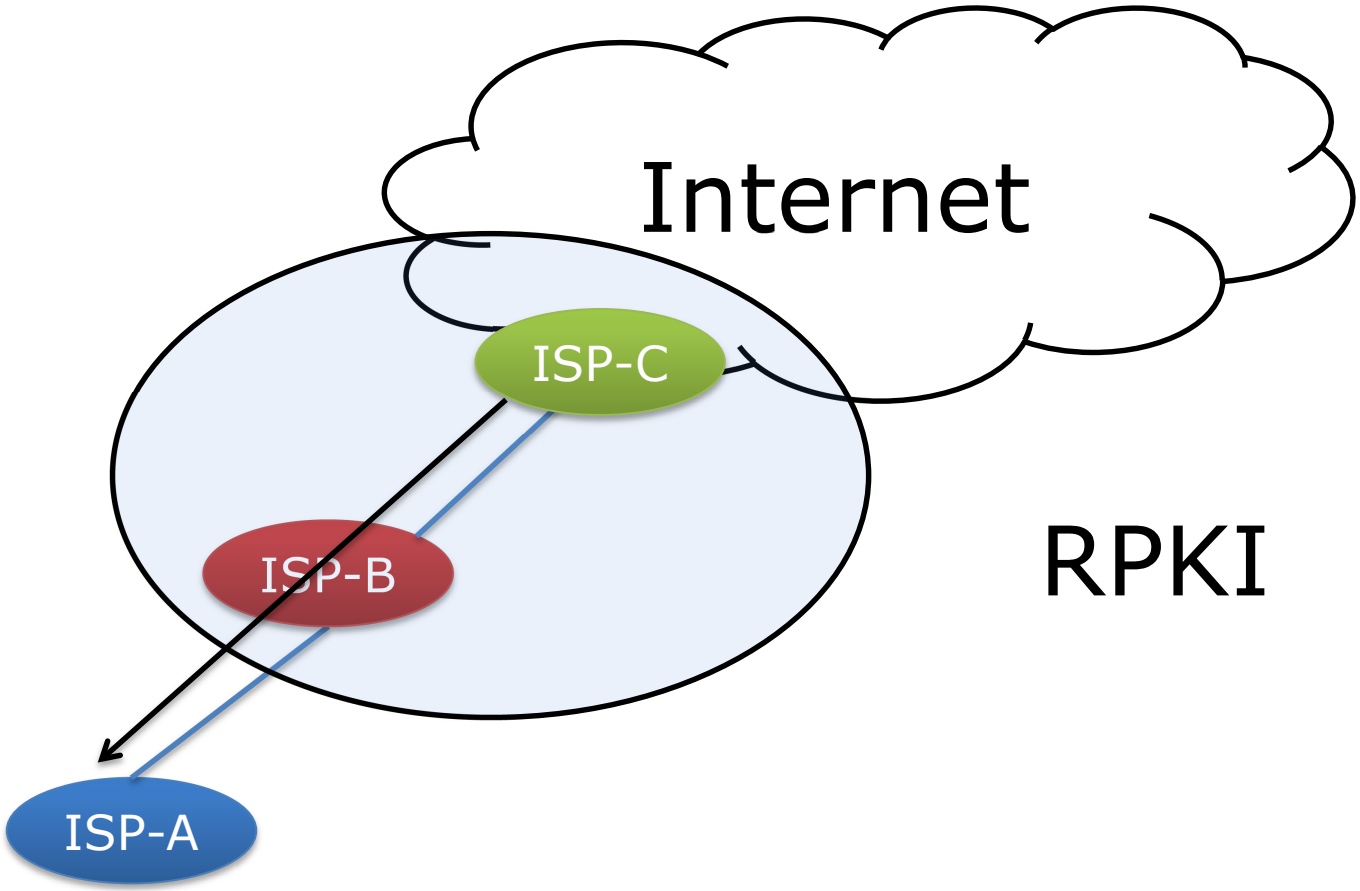


RPKI Deployment

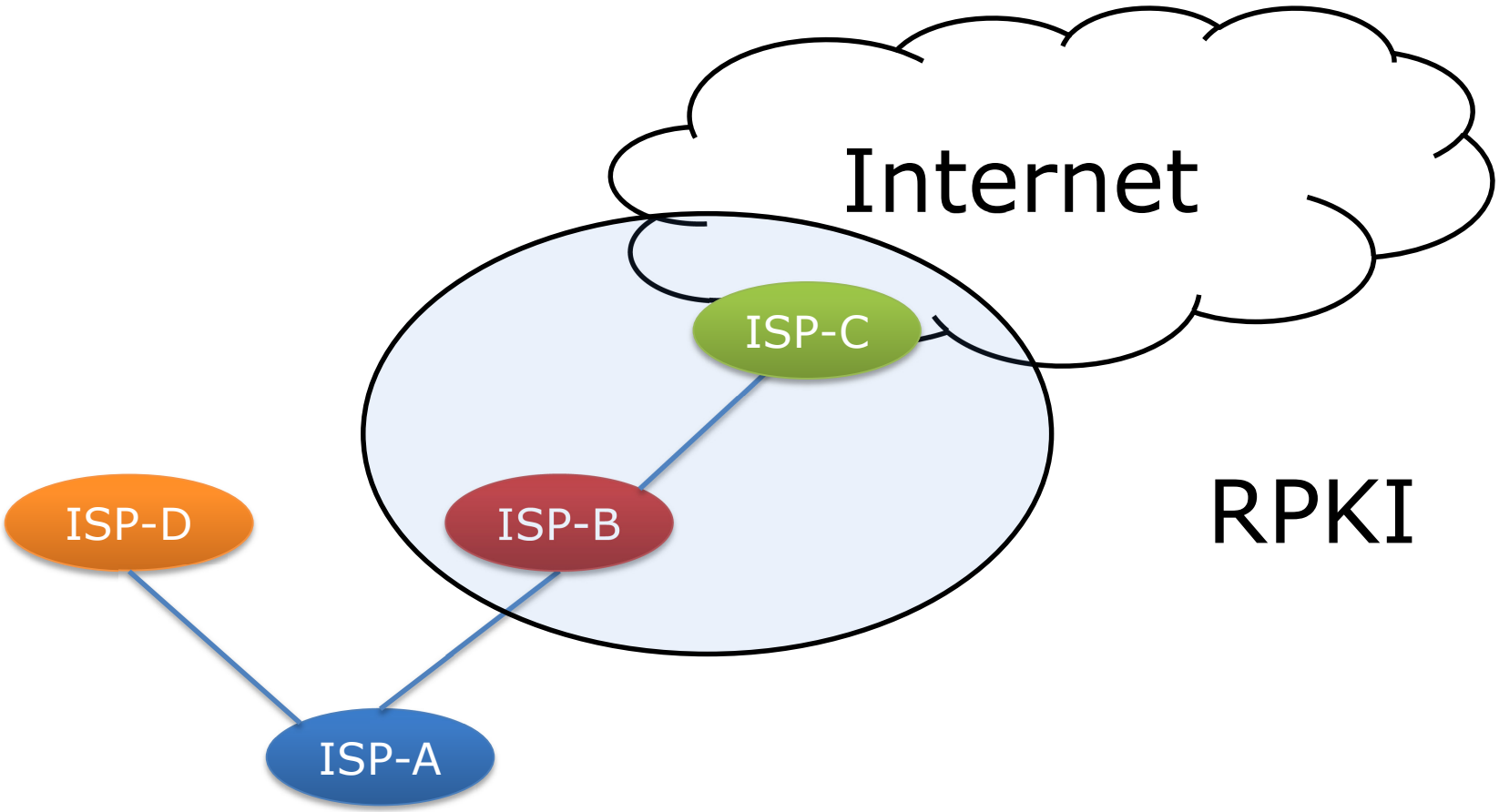
ISP-C次第で
他に曲がってしまう



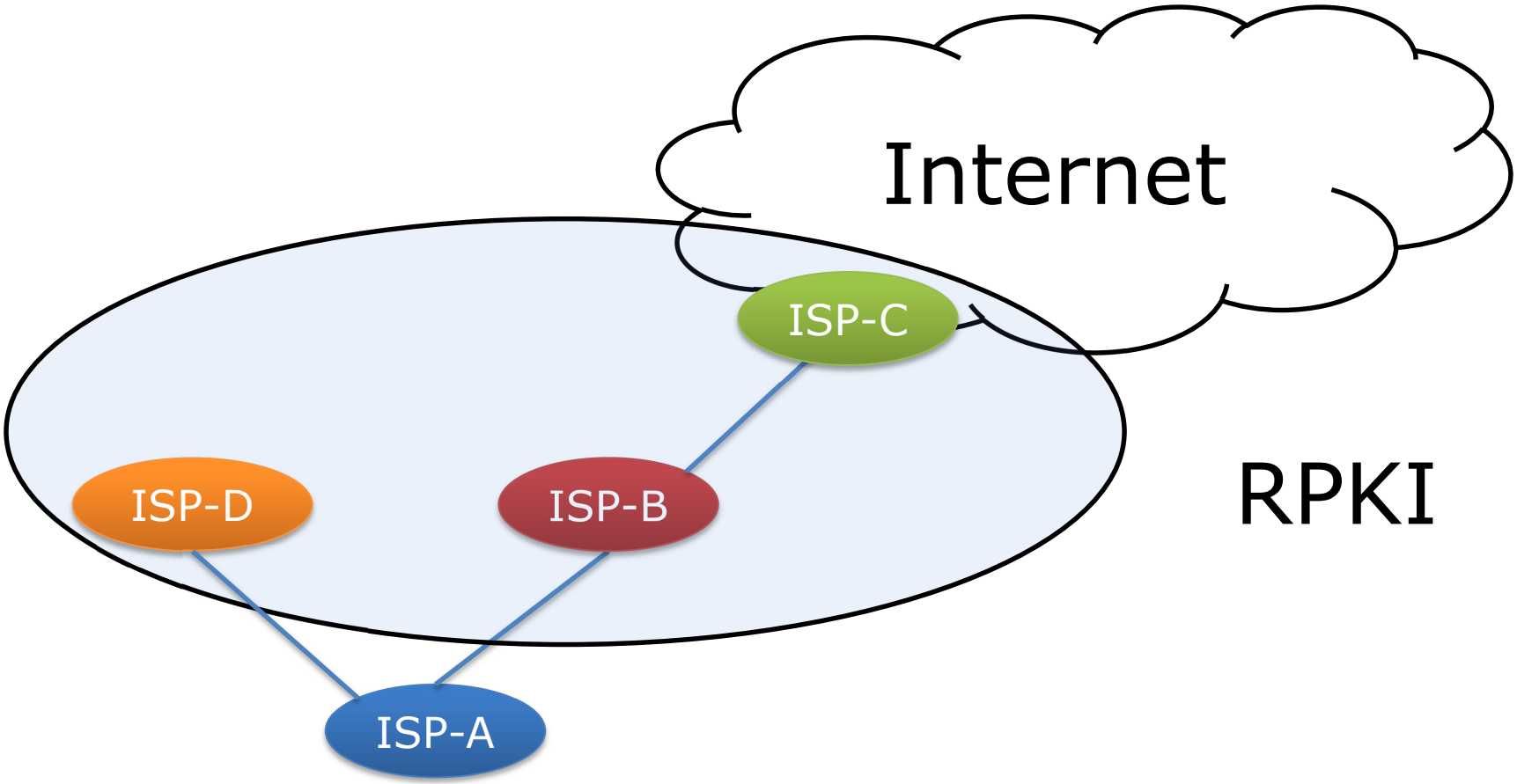
RPKI Deployment



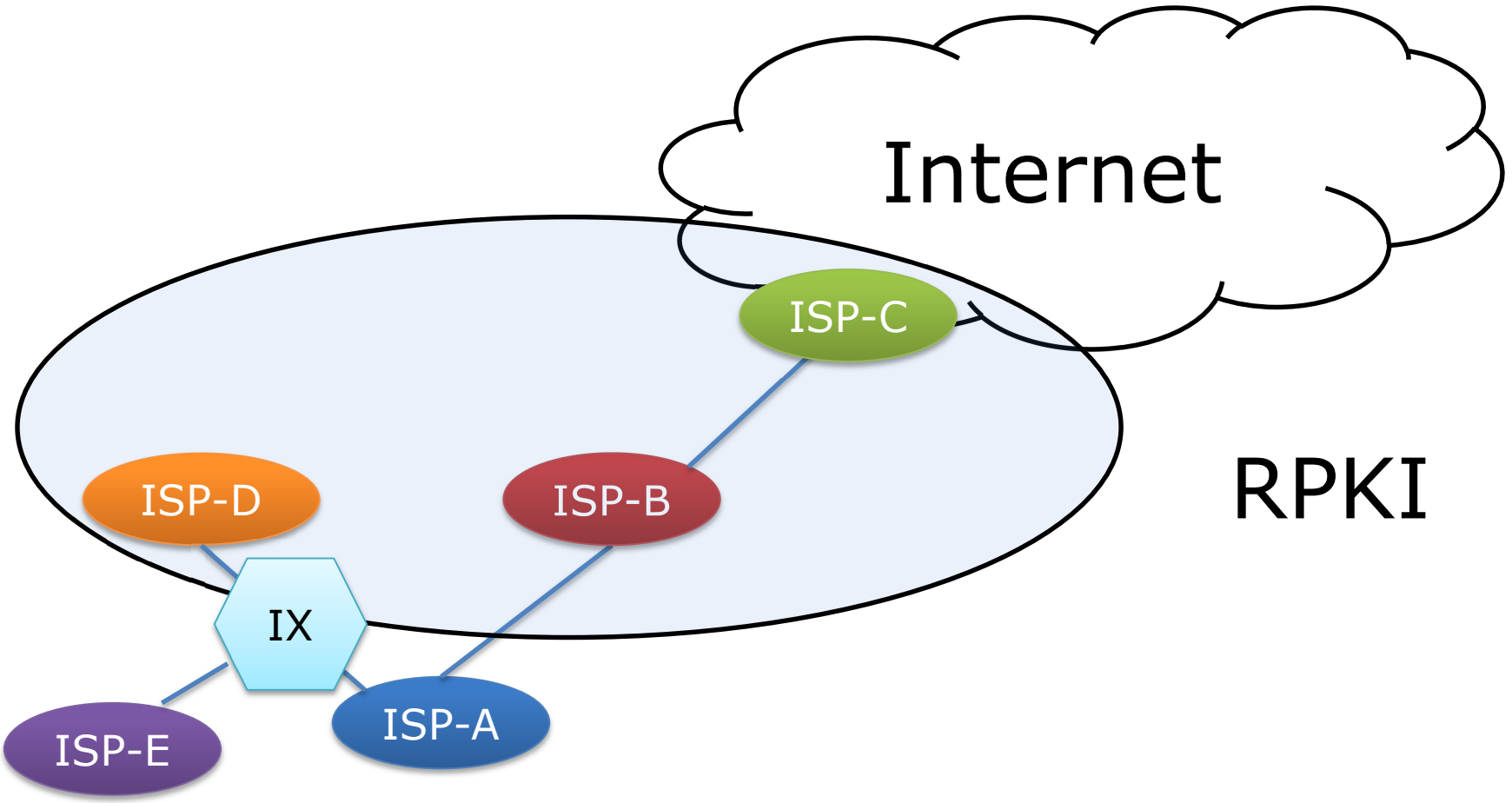
RPKI Deployment



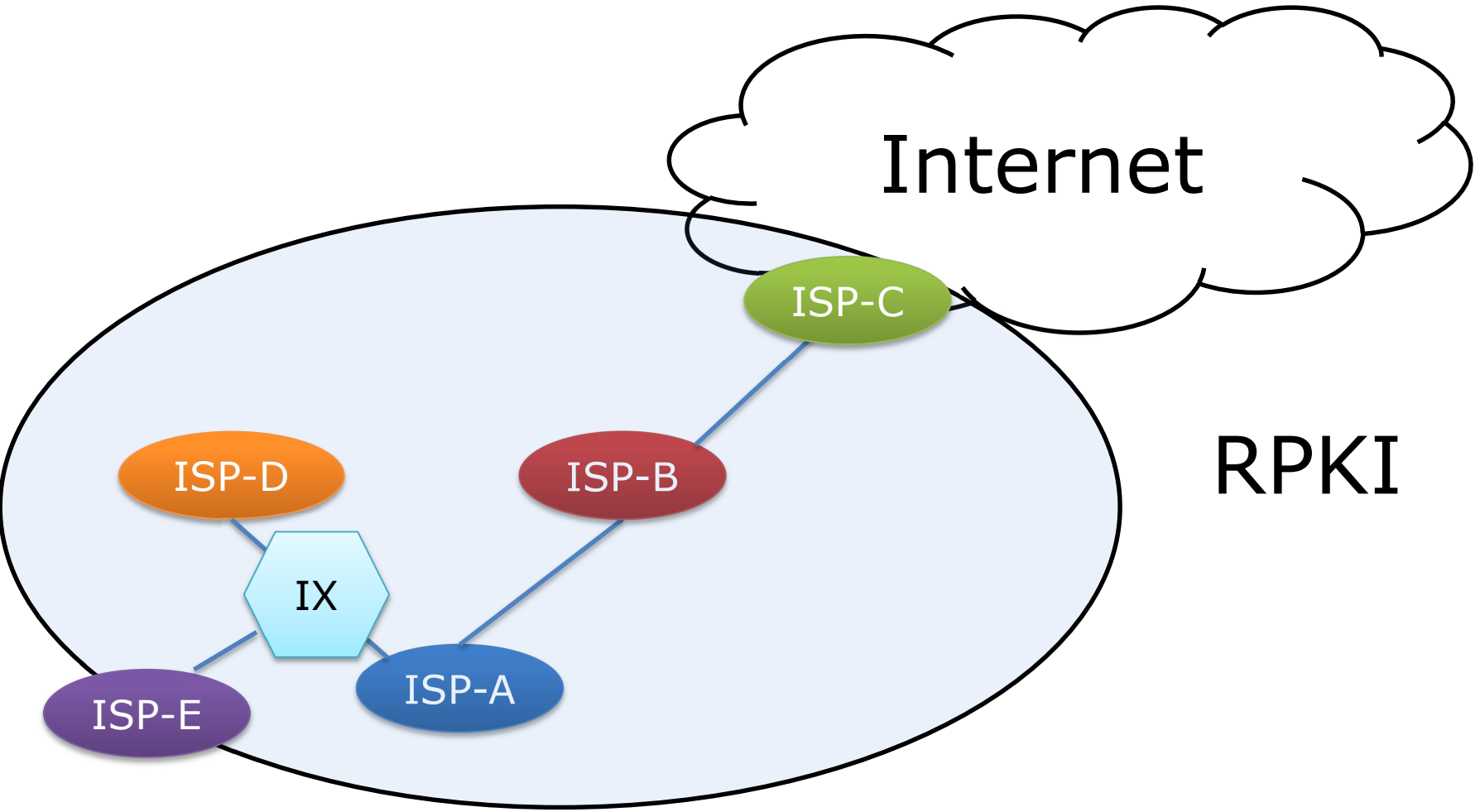
RPKI Deployment



RPKI Deployment

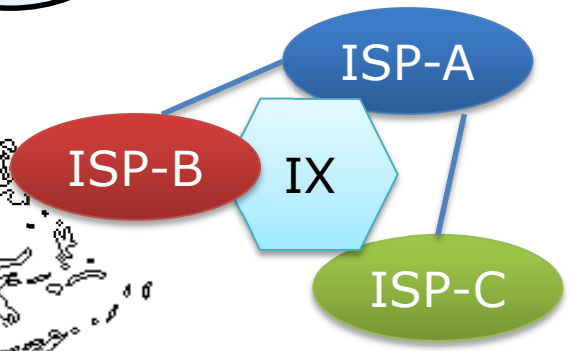


RPKI Deployment

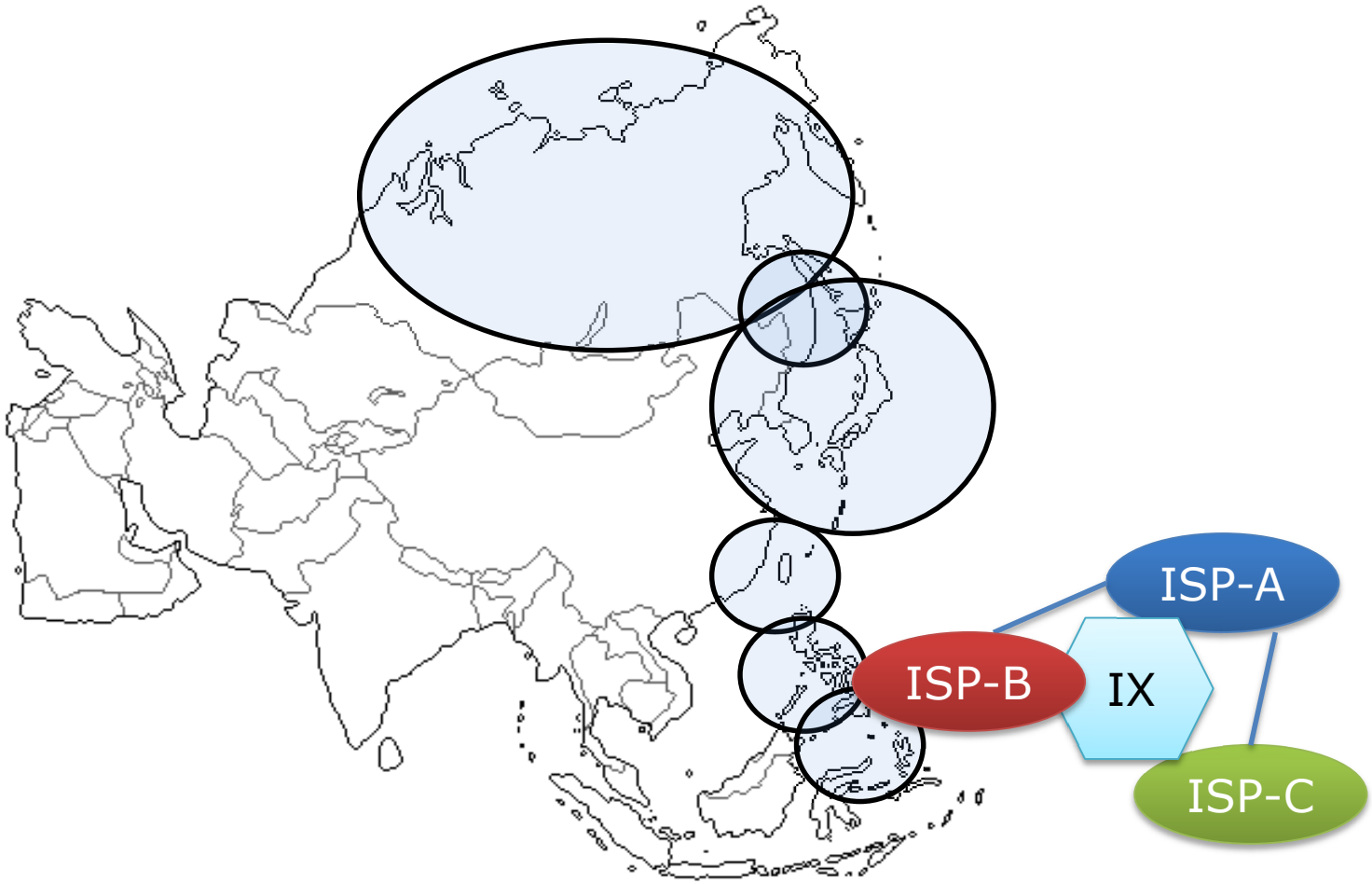


局所的でも効果はある

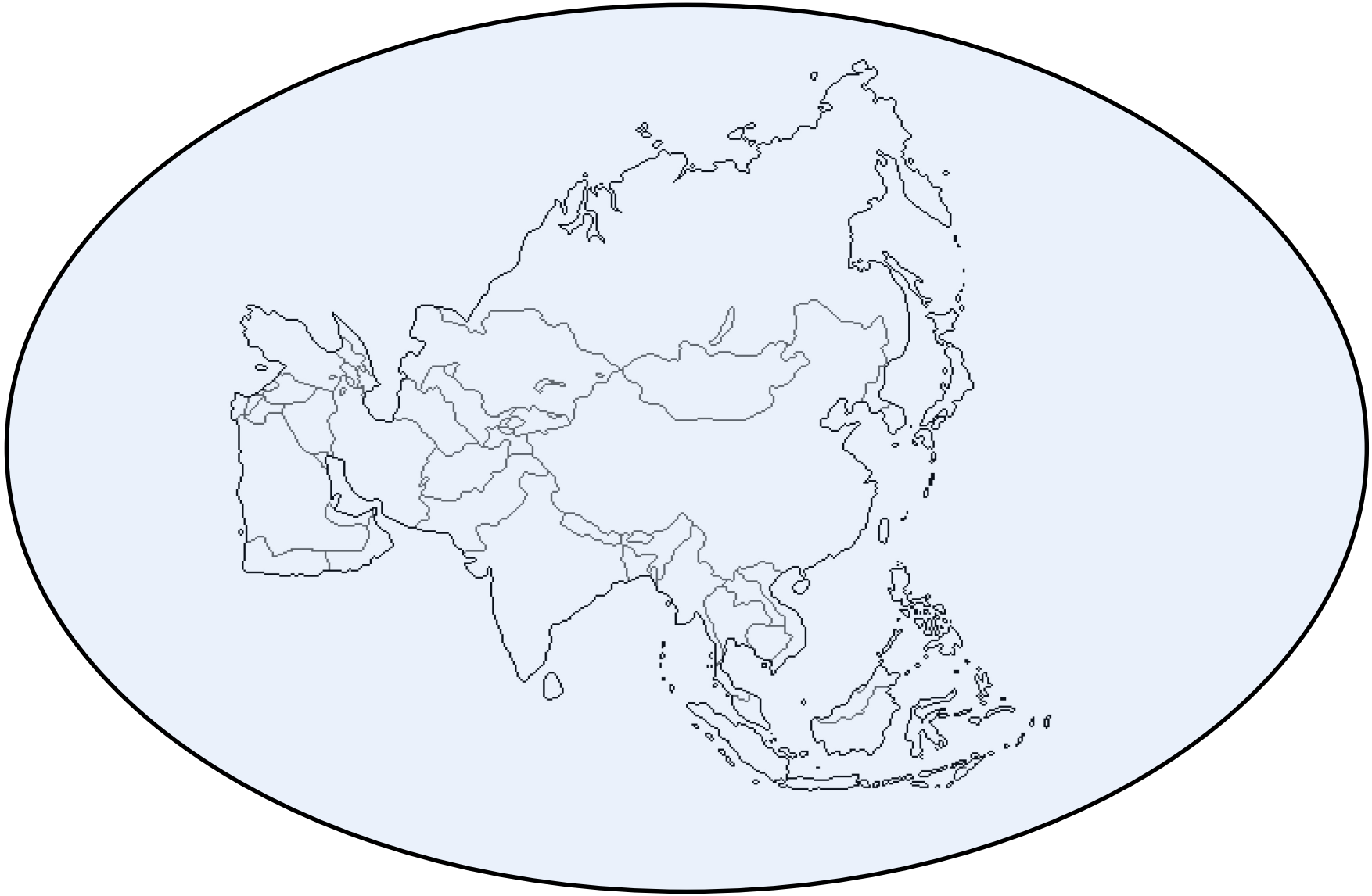
日本内の通信は影響を受けない



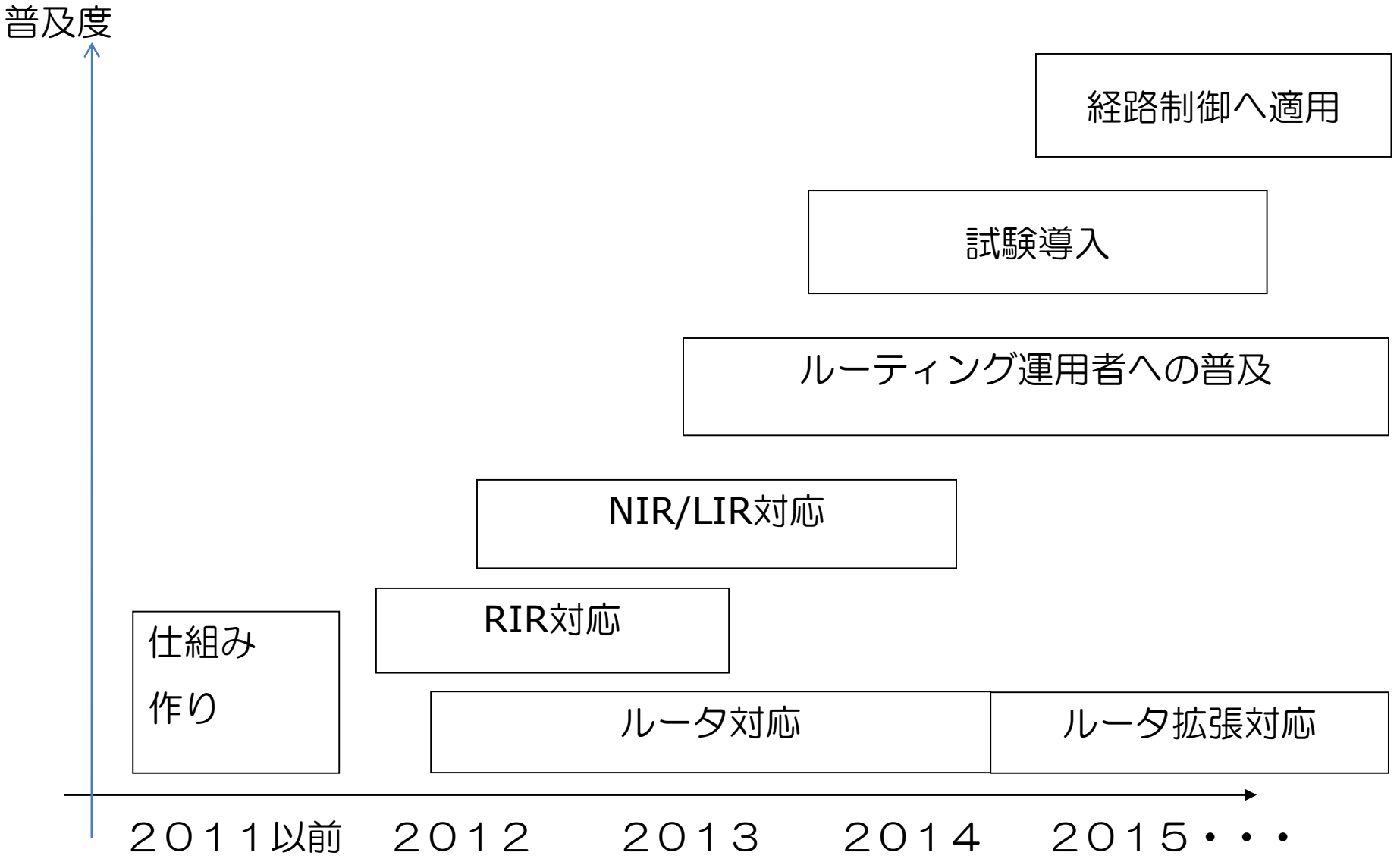
Worldwide RPKI Deployment



RPKI all over the world



RPKIを活用したルーティングの普及



最後に

- インターネットは、あらゆる社会インフラのインフラの役割を担っているということ。

- 2020年の東京オリンピックに向けて、より一層の安心・安全な通信インフラを皆さんで一緒に目指していきましょう！

（参考）旧IRR/RPKI動向調査専門家チーム

[メンバー(当時)]
チェア　吉田友哉　インターネットマルチフィード株式会社

有賀征爾　　NTTコミュニケーションズ株式会社
川村聖一　　ＮＥＣビッグローブ株式会社
中野達也　　KDDI株式会社
平井則輔　　ソフトバンクBB株式会社
松崎吉伸　　インターネットイニシアティブ株式会社
渡辺英一郎　Telecom-ISAC Japan

- インターネットにおける経路制御の現状
- IRRの動向
- RPKIの動向
- 今後の展望

報告書：https://www.nic.ad.jp/ja/materials/irr/report-201308.pdf

（参考）報告書より：骨子

- 現在のインターネットの経路制御は、不意の不正な経路広告によって複数の組織が甚大な被害を被った可能性があり、抜本的な予防策を講じる必要がある。
- 不正経路広告を防ぐための手段としてISPの経路フィルタが有効と言われている。経路フィルタを生成するための参照先データとしてIRRが最も活用されており、日本では経路奉行と連携した不正経路検知機能も提供されている。
- IRRは記述の自由度も高く様々な用途で活用されているが、登録情報の信憑性に問題があり、経路フィルタ生成の参照先データとして全世界で活用していくには新たな仕組みが求められている。
- 新たに、PKIを活用したIPアドレスの正当性を担保するResource PKI(RPKI)サービスが各RIR で開始され、正しい、IPアドレスとOrigin ASの組み合わせを記述したRoute Origin Authorization(ROA)の作成と活用が進んでいる。
- 今後 JPNICでは、RPKIサービスを日本国内で速やかに開始し、インターネットの経路制御基盤のセキュリティ向上に貢献する重要な役割を担っていく責任がある。
- 具体的には、日本国内の事業者に対するROAの発行、APNIC地域での安定したRPKIの提供を行っていく必要がある。