ICT-ISAC JAPAN

ICT-ISAC JAPAN
ICT Information Sharing And Analysis Center Japan

S10
2019年のルーティングインシデントとその観測・検知の現状と展望

2019/11/27

ICT-ISAC Japan BGP-WG主査/NTTコミュニケーションズ
渡辺　英一郎

私のパートで話すこと

「経路監視」の観点から以下のAgendaでお話します。

1. BGP経路監視の必要性について
2. BGP経路監視システム「経路奉行」について
3. 2019年に発生した大きなルーティングインシデント
   （と、その時経路奉行ではどのように見えていたか？）
4. 世界で利用されているBGP経路監視システムについて
5. BGP経路監視の現状と展望

1．BGP経路監視の必要性について

インターネットにおいては

自身が広報した経路は、世界のどこかで

受け取ってもらえていないかもしれない

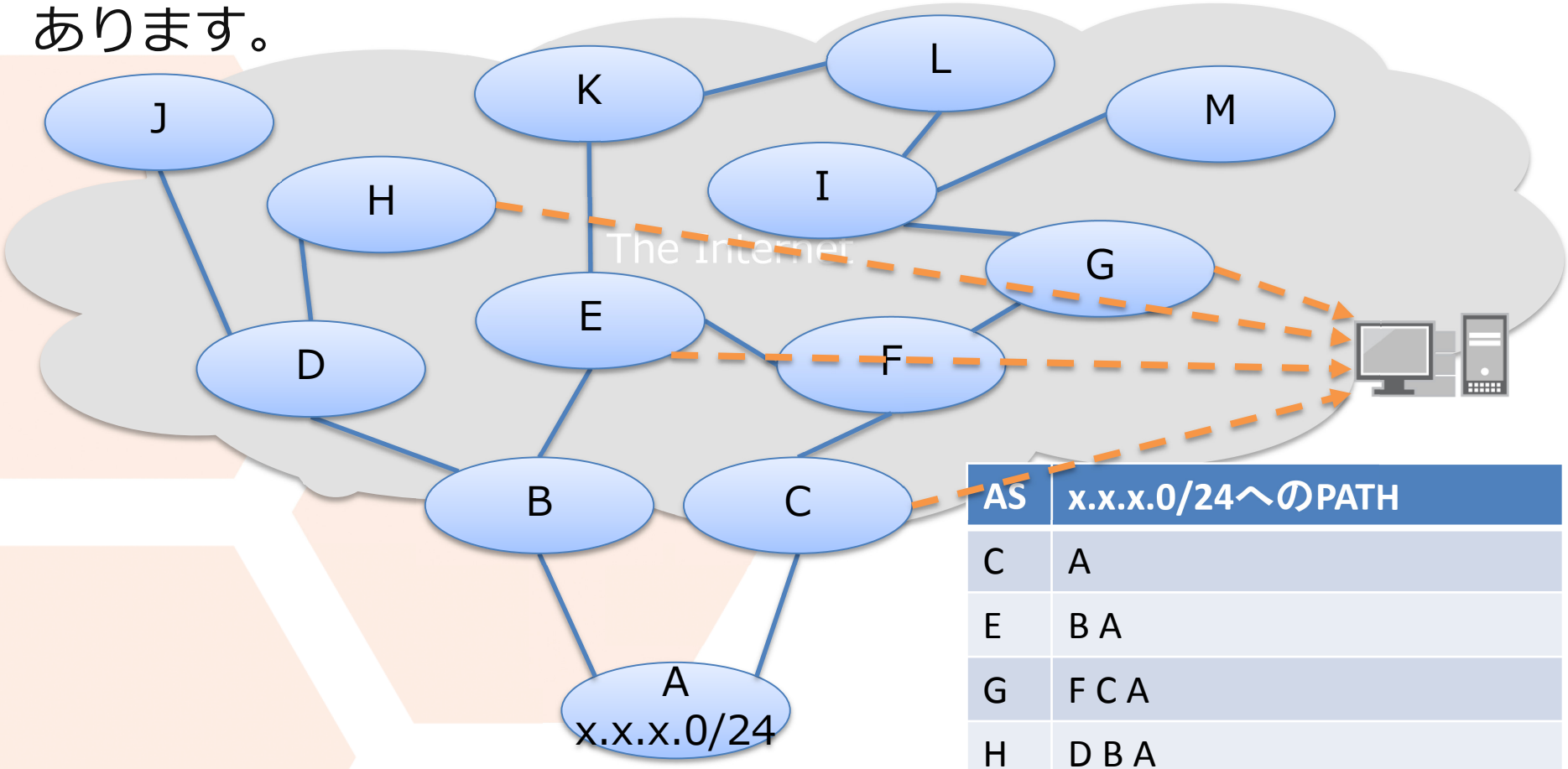
遠回りになっているかもしれない

だれかに勝手に使われているかもしれない

正しく経路を広報したとしても、インターネット上のさまざまなイベントにより、広報元の思い通りにならないことがしばしばあります。

BGP経路監視

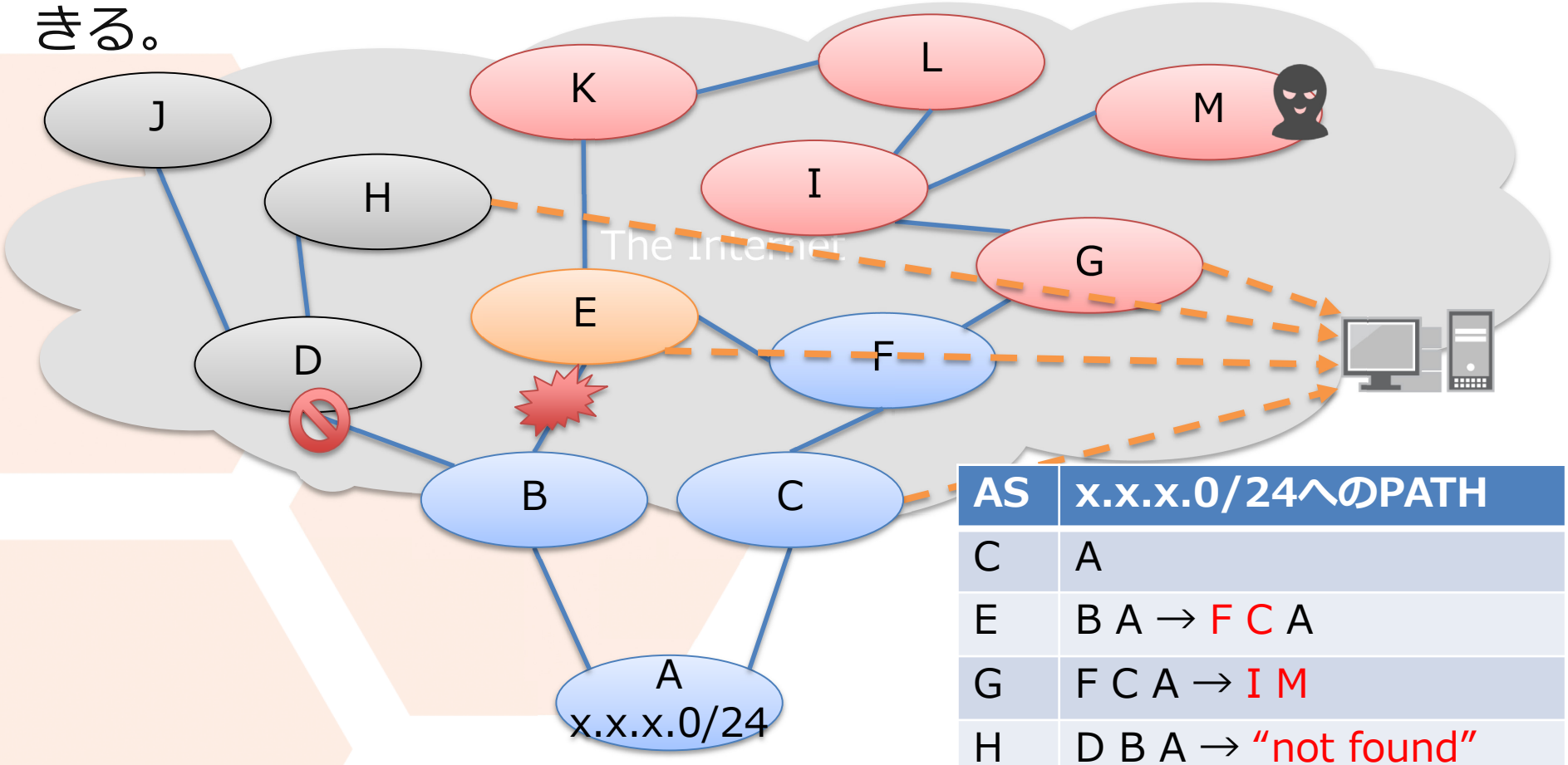
インターネット上には、BGP経路をモニタリングし、
そのデータを蓄積・公開・共有などをしているプロジェクトがあります。



AS	x.x.x.0/24へのPATH
C	A
E	B A
G	F C A
H	D B A

BGP経路監視(Cont')

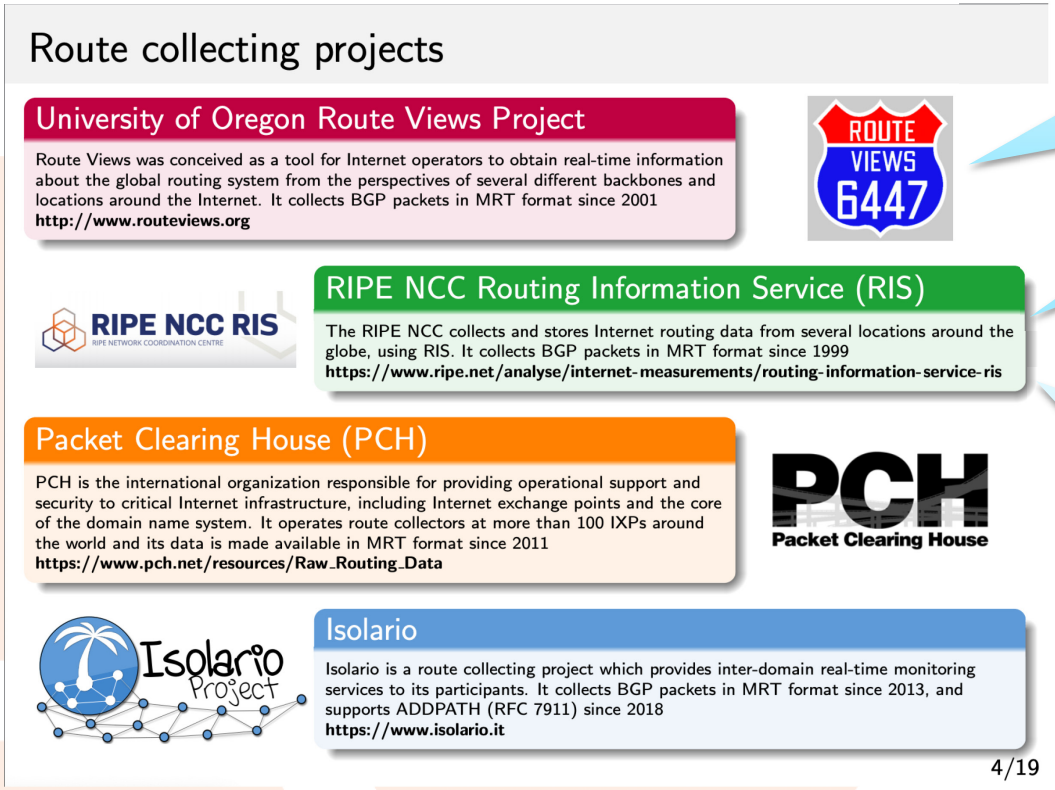
これらの情報を利用して、自身が広報した経路が外でどのように見えているのか？何が発生していたのかをある程度推測ができる。



AS	x.x.x.0/24へのPATH
C	A
E	B A → F C A
G	F C A → I M
H	D B A → “not found”

パブリックな経路観測プロジェクト

MRTファイル形式で情報提供しているプロジェクト



BGPstream(by CAIDA)
https://bgpstream.caida.org/
via kafka

RIS Live(by RIPE labs.)
https://labs.ripe.net/tools/ris-live
via websocket

https://www.itnog.it/itnog4/files/10-bgpscannerpres.pdf

静的ファイル(MRT)からstream(websocket, kafka)提供へ
よりリアルタイムに情報を取得できるように。

BGP経路監視の必要性

外部監視の手法として

✓ pingなどによる疎通監視

✓ 利用しているサービス監視

などに加え、「BGP経路監視」も加えることで、

より、迅速に何が起きているのかを把握し、回復や対処にむけてのアクションをとることができます。

2. BGP経路監視システム「経路奉行」について

「経路奉行」のご紹介

「経路奉行」ってご存知ですか？

ICT-ISAC Japan(https://www.ict-isac.jp/)とJPNICで運用している「BGP経路監視システム」です。

2004年　国内最強looking glassを作る！

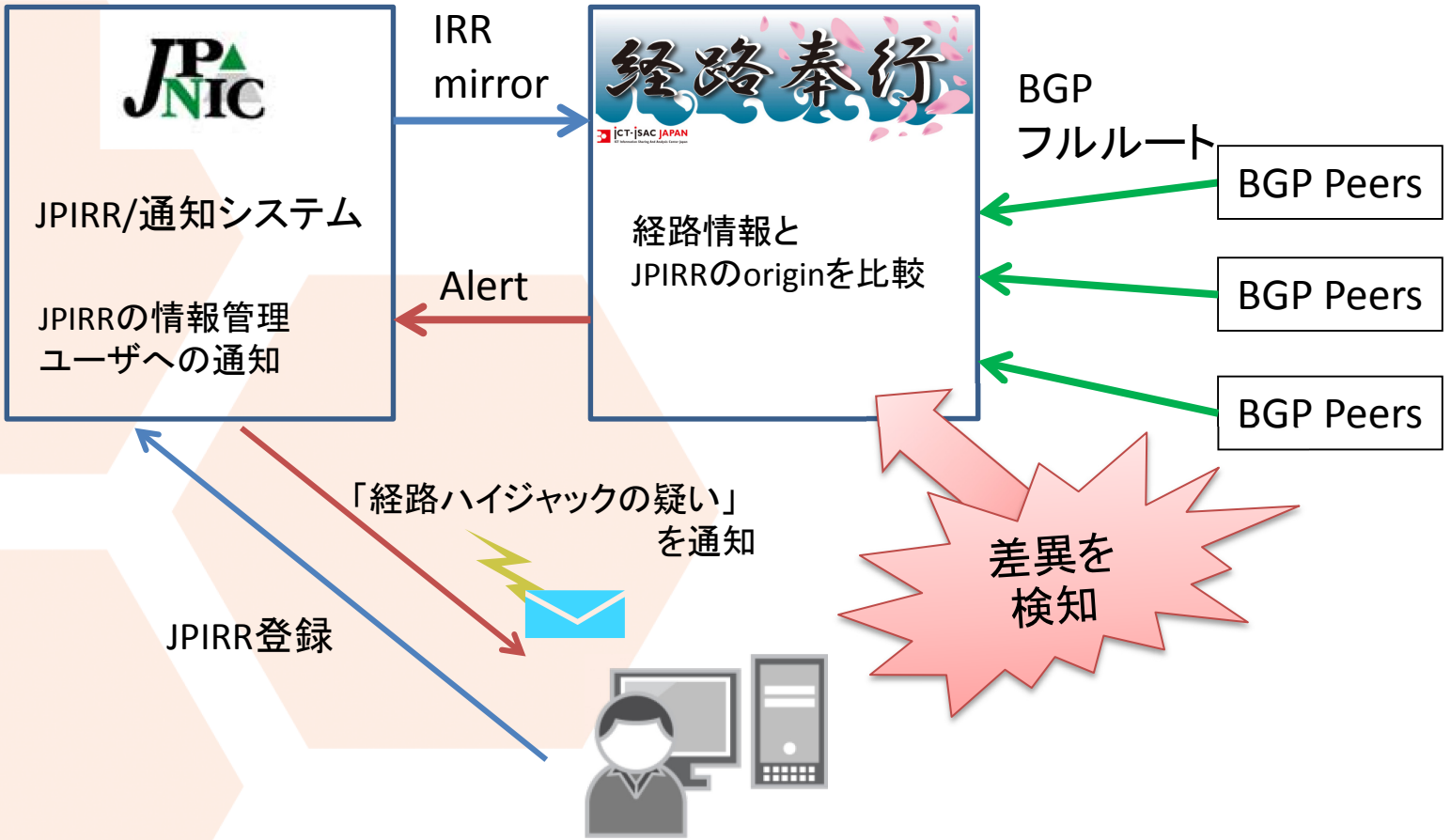
2005年　経路ハイジャック監視開始
=>「経路奉行」と名付けよう！

2008年　JPNICと連携
・正しい経路台帳(JPIRR)の構築に貢献できれば！
・検知情報を可能な限り、ISACメンバではない方にも！

2019年　現在に至る…。!?15年経ってるw

「経路奉行」システム

みなさんがJPIRRに登録した経路と、日本国内の複数のASから受信したBGPフルルートを（ほぼ）リアルタイムで比較し、差異を検知した場合、希望者に通知するシステムです。



現在、「経路奉行」にご協力いただいている組織/AS

2019/11/27時点

企業名	通称	経路奉行接続AS
（株）インターネットイニシアティブ	IIJ	AS2497
インターネットマルチフィード（株）	MF/JPNAP	AS7521
エヌ・ティ・ティ・コミュニケーションズ（株）	NTTCom/GIN/OCN	AS2914/AS4713
（株）オプテージ	K-Opticom/OPTAGE	AS17511(準備中)
KDDI(株)	KDDI	AS2516
（株）KDDI総合研究所	KDDI lab.	AS7667/AS131078
ソニーネットワークコミュニケーションズ(株)	So-net	AS2527
ソフトバンク（株）	ODN/SBB	AS4725/AS17676
ビッグローブ（株）	Biglobe	AS2518
（株）NTTドコモ	NTTDoCoMo	AS9605
アルテリア・ネットワークス（株）	ALTERIA/UCOM	AS2519/AS17506(準備中)
さくらインターネット（株）	SAKURA	AS9370/AS9371
（株）IDCフロンティア	IDCF	AS4694
エヌ・ティ・ティ・スマートコネクト（株）	NTT-SMC	AS7671
（株）エヌ・ティ・ティピー・シーコミュニケーションズ	NTT-PC	AS2514
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	JPNIC	AS2515
日本インターネットエクスチェンジ（株）	JPIX	（検討中）

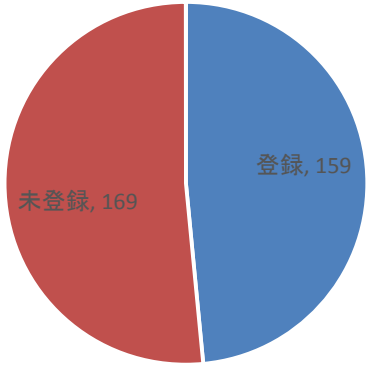
ご協力ありがとうございます。
特にMF様、JPNIC様には設備の提供含め
多大なるご協力をいただいております。

うちのAS、まだやっていない…という方は、ぜひ！

- JPIRRで監視してほしいrouteオブジェクトまたはmntnerオブジェクトのdescrフィールドに魔法のコトバを追加するだけ。

```
mntner:     MAINT-AS7521
descr:      People authorized to make changes for AS7521
            X-Keiro: noc@mfeed.ad.jp
admin-c:    JP00001394
tech-c:     JP00001394
upd-to:     tech-c@mfeed.ad.jp
mnt-nfy:    tech-c@mfeed.ad.jp
notify:     tech-c@mfeed.ad.jp
auth:       CRYPT-PW HIDDENCRYPTPW
mnt-by:     MAINT-AS7521
changed:    tech-c@mfeed.ad.jp 20190717
source:     JPIRR
```

参考)2019/11/19現在のX-Keiro利用mntner数



約48%の方々にご利用いただいております。
ご利用ありがとうございます。

- 詳しくはJPNIC経路奉行のページ

https://www.nic.ad.jp/ja/ip/irr/jpnic-keirobugyou.html

登録に関して困ったことがあれば、JPNICの方々がヘルプしてくれますので安心です。

経路奉行での検知仕様①

基本的にRPKIにおけるRoute Origin Validation(ROV)と（ほぼ）同じ動作。

判定結果が”INVALID”でかつ”Origin ASが異なる”場合、
“経路ハイジャックが疑われる状態(Invalid Origin)”
の発生として検知。

```
result = BGP_PFXV_STATE_NOT_FOUND;

//Iterate through all the Covering entries in the local VRP
//database, pfx_validate_table.
entry = next_lookup_result(pfx_validate_table, route_prefix);

while (entry != NULL) {
  prefix_exists = TRUE;
    if (route_prefix_length <= entry->max_length) {
      if (route_origin_as != NONE
          && entry->origin_as != 0
          && route_origin_as == entry->origin_as) {
        result = BGP_PFXV_STATE_VALID; return (result);
      }
    }
    entry = next_lookup_result(pfx_validate_table, input.prefix);
  }

  //If one or more VRP entries Covered the route prefix, but
  //none Matched, return "Invalid" validation state.
  if (prefix_exists == TRUE) {
    result = BGP_PFXV_STATE_INVALID;
  }
  return (result);
```

経路奉行では以下を拡張実装

Invalid Originの場合：
(route_origin_as != entry->origin_as)
=>”経路ハイジャックが疑われる状態”
として検出

それ以外の場合(eg. Invalid Length)：
=>ログのみ

RFC6811) 2.1 Pseudo Code

経路奉行での検知仕様②

- 現時点ではRPKIのROAは利用していない
  日本のROA登録率少ない…涙。
  普及が進めば、RPKI利用を検討しますので、みなさんご協力を！

- JPIRRのRoute(6)オブジェクトから
  ROA相当の情報を生成して利用。

```
route:      203.139.160.0/19
descr:      OCN (AS4713) CIDR BLOCK 1
            -- snip --
origin:     AS4713
mnt-by:     MAINT-AS4713
changed:    admin@ocn.ad.jp 20190301
source:     JPIRR
```

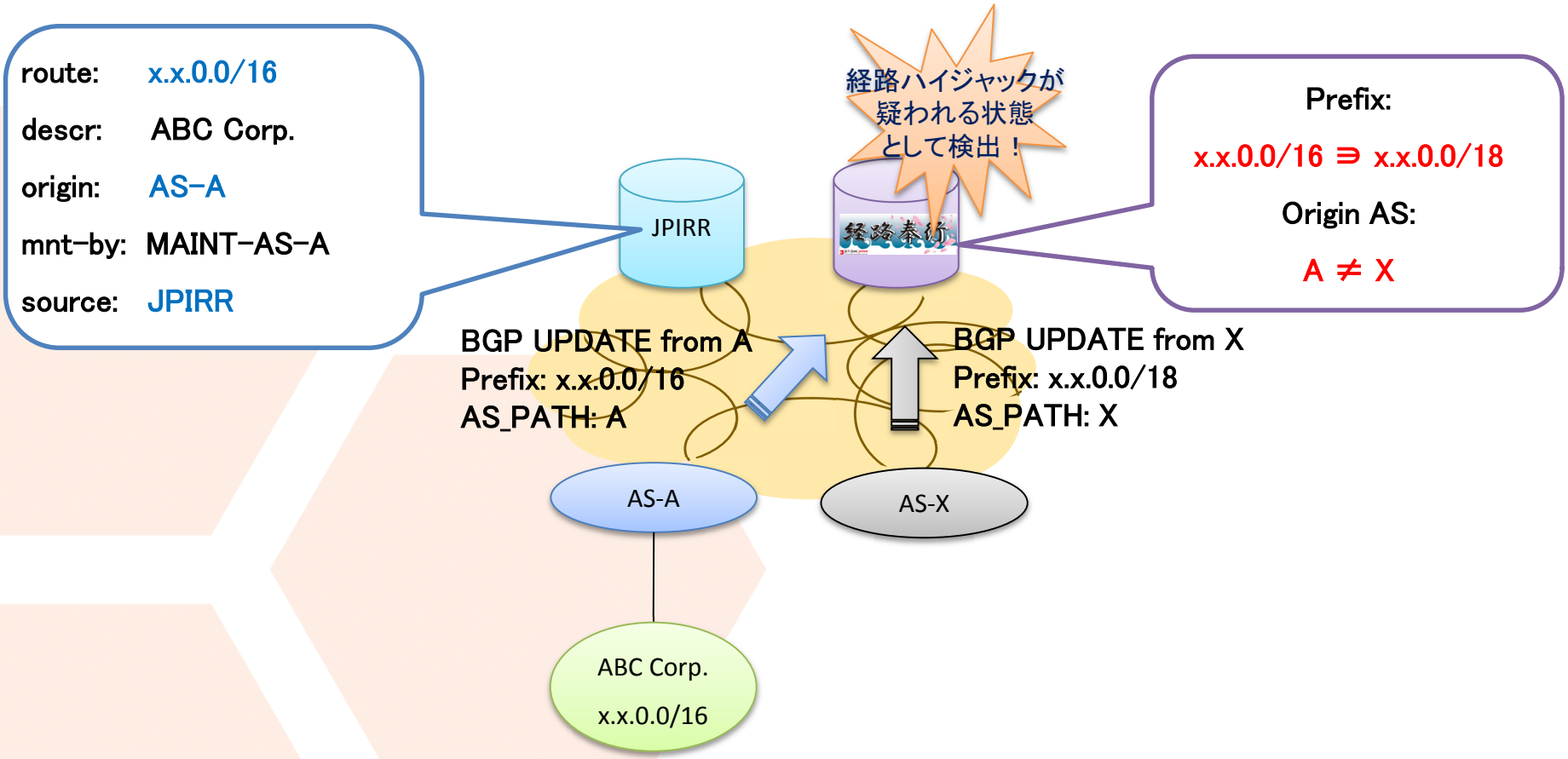
ROA(相当)の情報を生成して正しい経路として利用

Prefix: 203.139.160.0/19
MaxLen: 19
AS: 4713

注１）exact-match
注２）sourceはJPIRRのみ（RADBミラーなどは参照しません）

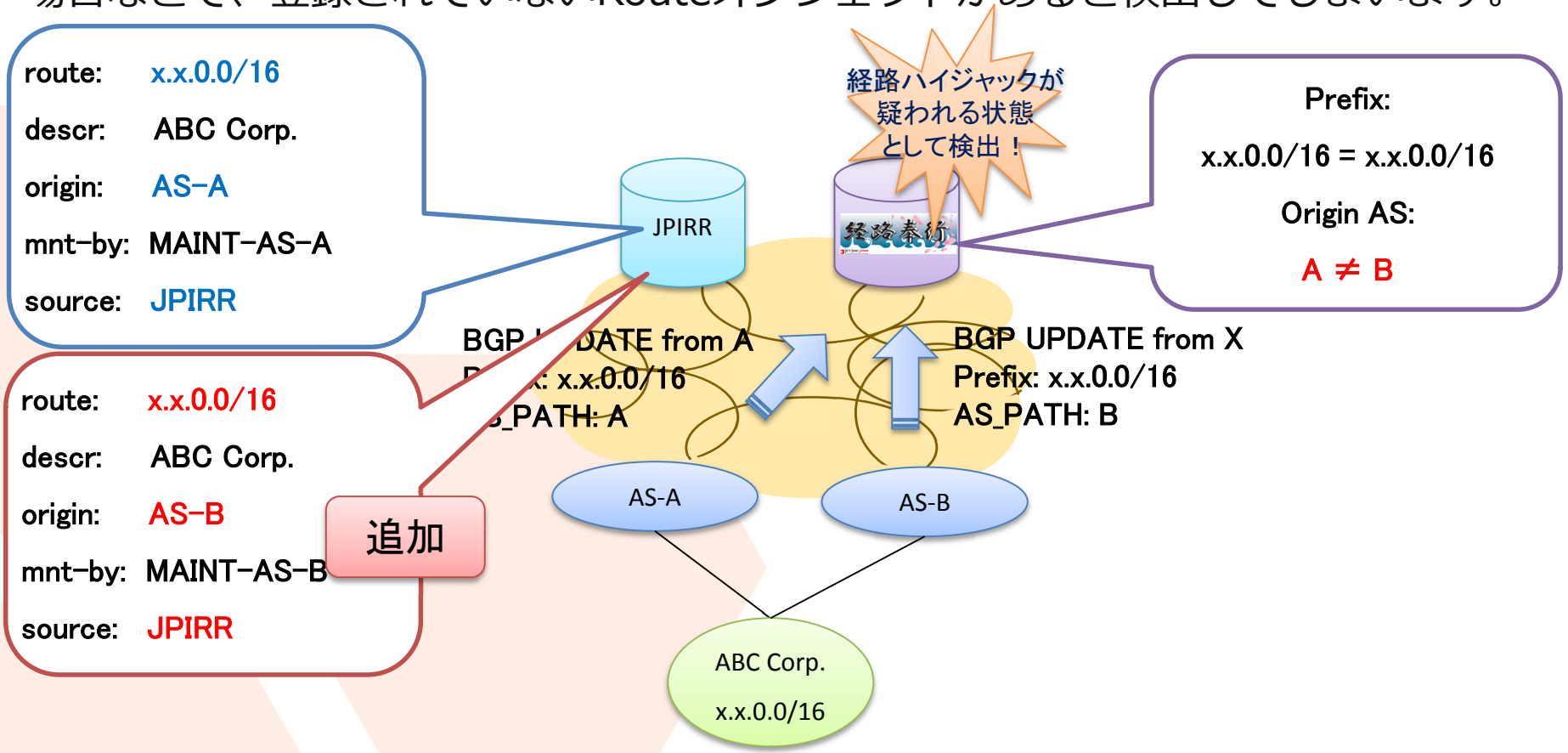
経路奉行での検知例（正しく検出）

JPIRRに登録されていないASから経路を受信すると検出します。



経路奉行での検知例（誤検出①）

同一Prefixを複数のASをOrigin ASとして広報する(MOAS/Multiple Origin AS)の場合などで、登録されていないRouteオブジェクトがあると検出してしまいます。



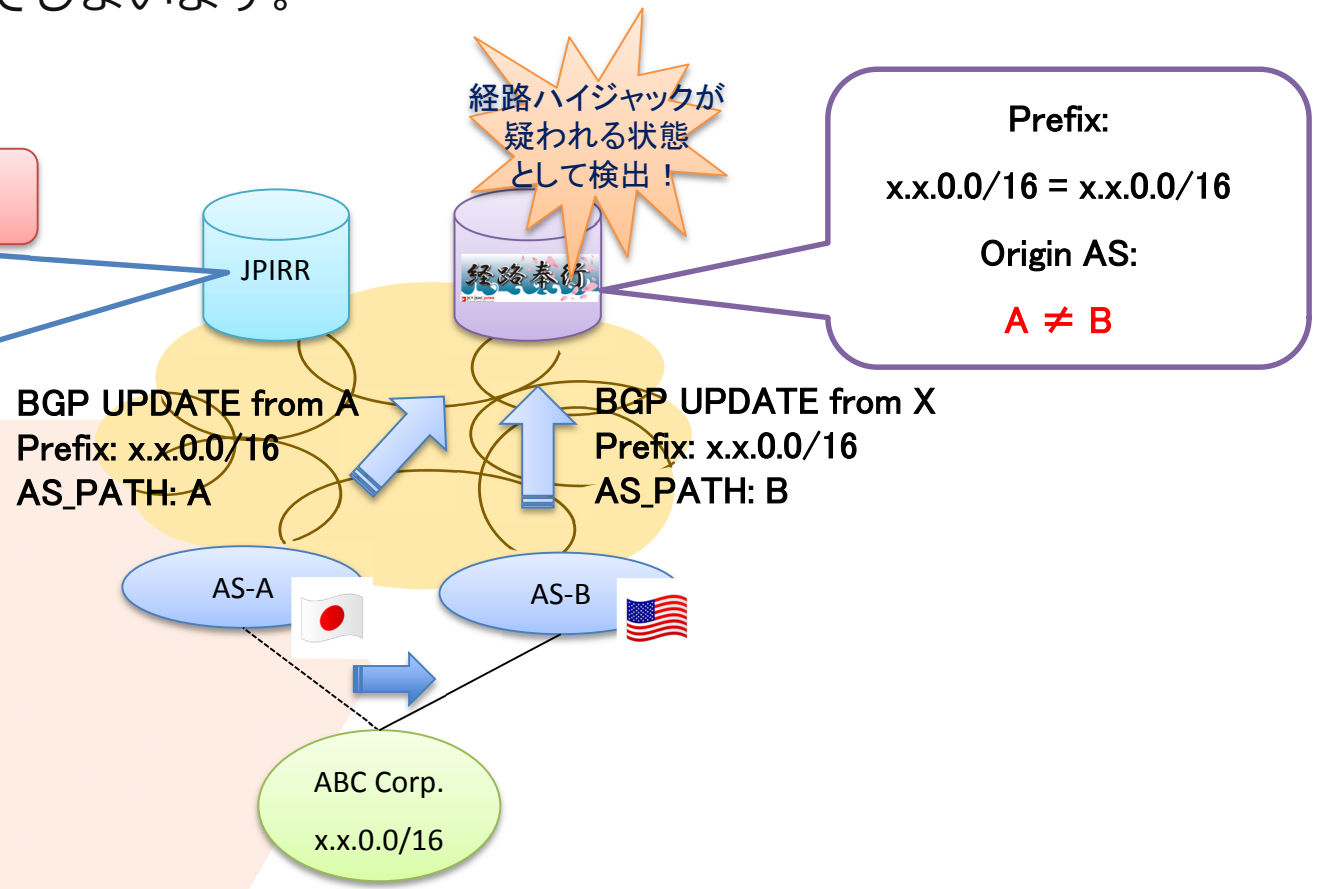
広報元となるOrigin ASのRouteオブジェクトもきちんと登録しましょう。

経路奉行での検知例（誤検出②）

対象PrefixがJPIRR管轄外に引っ越しした場合などで、JPIRRにRouteオブジェクトが残っていると検知してしまいます。

route: x.x.0.0/16
descr: ABC Corp.
origin: AS-A
mnt-by: MAINT-AS-A
source: JPIRR

削除

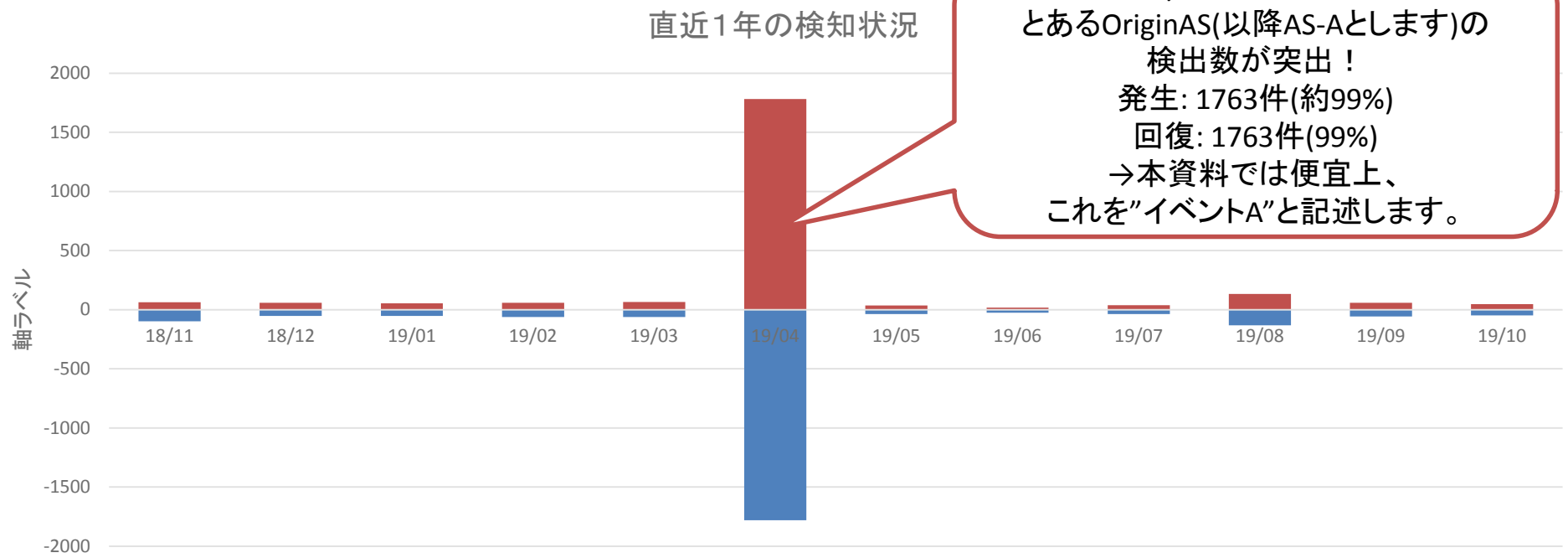


Prefix:
x.x.0.0/16 = x.x.0.0/16
Origin AS:
A ≠ B

広報しなくなったRouteオブジェクトは削除しましょう。
（一定期間経過後、JPIRRのガベージコレクタにより削除されますが、何も考えず更新しちゃっているケースも見受けられます。）

直近1年(2018/11-2019/10)における経路奉行の検知状況

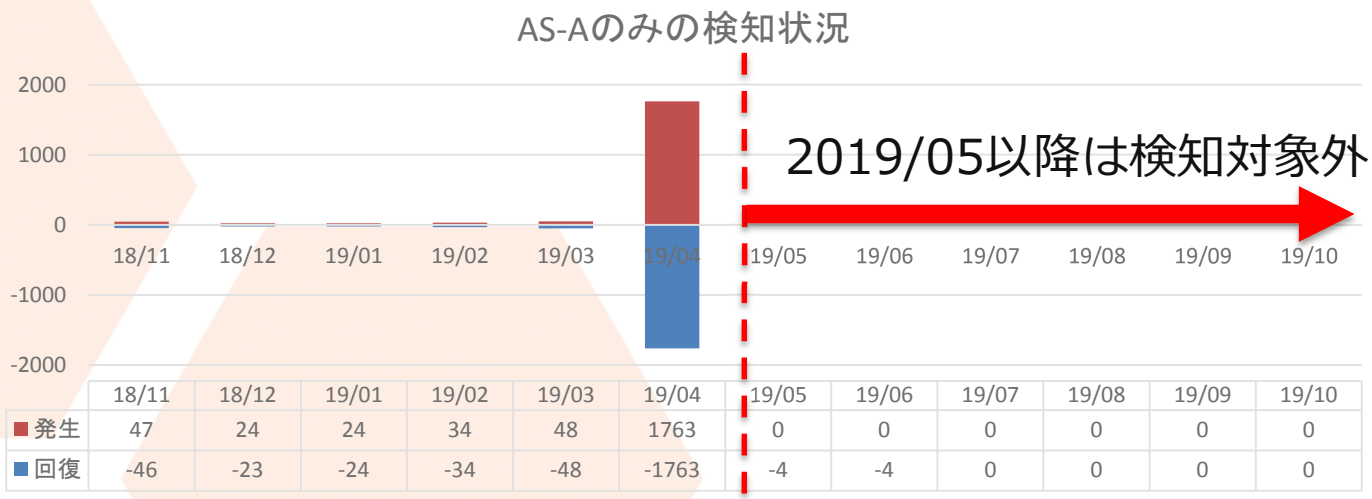
- 2019/04に突出した検知数(発生1782件/回復1781件)
- それ以外は例月通りの検知数(数十～百数十件/月ペース)



	18/11	18/12	19/01	19/02	19/03	19/04	19/05	19/06	19/07	19/08	19/09	19/10
発生	62	58	55	58	65	1782	36	18	37	133	58	47
回復	-97	-52	-52	-61	-62	-1781	-37	-26	-37	-132	-58	-49

イベントAについての経路奉行の検知状況

- イベントAに関する検知は2018/04だけでなく、以前(2016/03ごろ)から発生していた。



	18/11	18/12	19/01	19/02	19/03	19/04	19/05	19/06	19/07	19/08	19/09	19/10
発生	47	24	24	34	48	1763	0	0	0	0	0	0
回復	-46	-23	-24	-34	-48	-1763	-4	-4	0	0	0	0

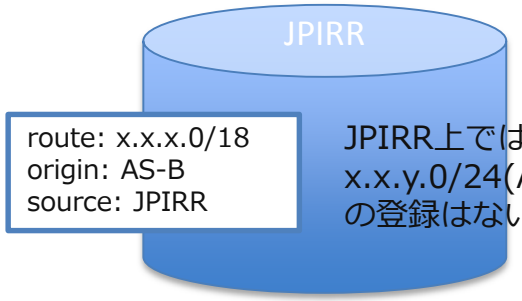
- このまま続くとシステム的には困る（狼警報化して、大事なものを見逃す可能性がある）のでやむをえず、イベントAを監視対象から外すこととしました。

イベントAについて、状況から見える発生原因を推定してみる

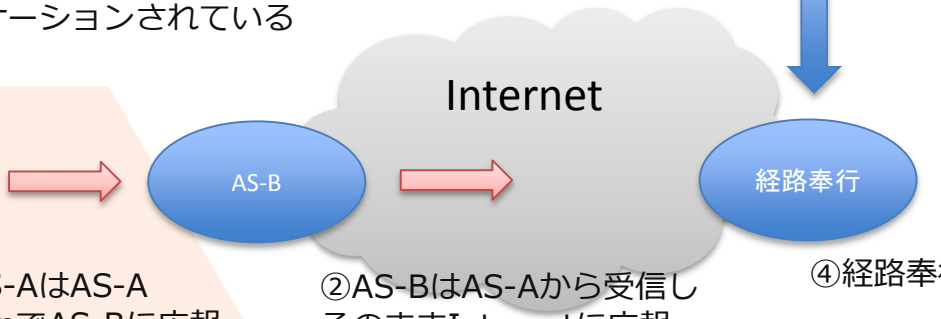
Mask長	経路数
/26	x 1
/27	x 3
/28	x 4
/29	x 4

JPNIC whois
x.x.x.0/18(B社/Allocation)
x.x.y.0/24(A社/SubAllocation)

whois上では該当network範囲で
サブアロケーションされている



JPIRR上では
x.x.y.0/24(AS-A)
の登録はない



①AS-AはAS-A
originでAS-Bに広報
(prepend x 1)
AS_PATH: A A

②AS-BはAS-Aから受信し
そのままInternetに広報
AS_PATH: B A A

④経路奉行で大量に検知

③この区間のどこかで頻繁にflap
(おそらくAS-A網内でredistribute connected的な設定がされ該当subnetのdown/upで発生していると思われる)

※Prefix、AS、Org情報はマスクしています。

イベントAについてのコメント

◘ 経路監視の観点

検知除外しているので、（悪意のあるハイジャックが発生したとしても）今後検知できない場合がある。

検知除外は静的に設定するので、もしAS-Aが状況を改善したとしても、（教えてもらわないと）監視側は気づけない。

◘ BGPオペレータとしての観点

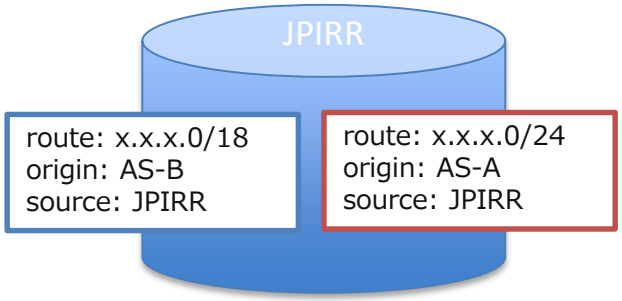
インターネットの経路数をむやみに増やさないために、できるだけ経路集約すべき。（いくら少なくても積り積もれば...)

経路フラップは他のASのルータの処理にも影響を与えるので、できるかぎり安定的に広報すべき。

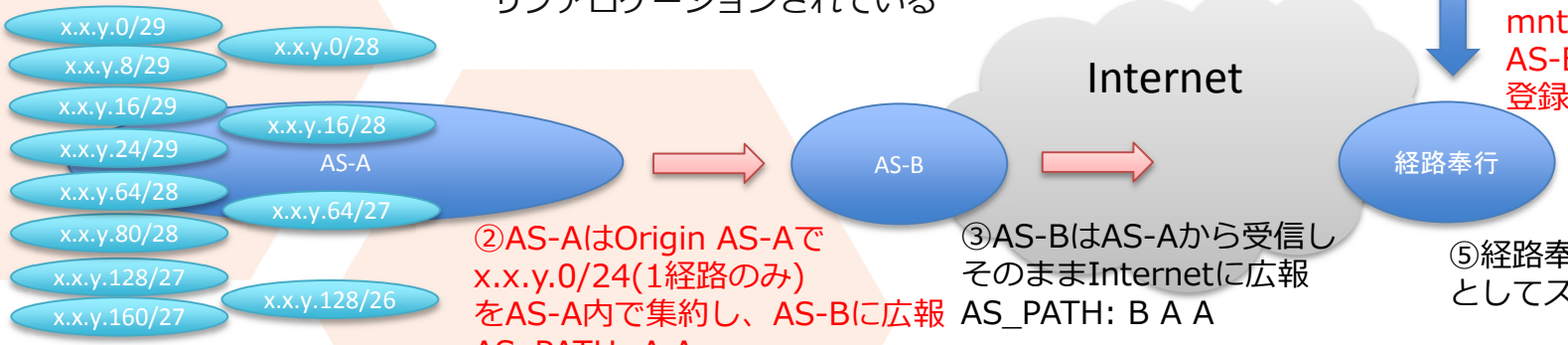
改善提案①PunchingHoleとしてちゃんと(!?)広報

Mask長	経路数
/26	x 1
/27	x 3
/28	x 4
/29	x 4

whois上では該当network範囲で
サブアロケーションされている



①JPIRRに
x.x.y.0/24(AS-A)
を登録
mntnerがなければ、
AS-Bと協議の上
登録してもらう



②AS-AはOrigin AS-Aで
x.x.y.0/24(1経路のみ)
をAS-A内で集約し、AS-Bに広報
AS_PATH: A A

③AS-BはAS-Aから受信し
そのままInternetに広報
AS_PATH: B A A

⑤経路奉行では正常な経路
としてスルー

④
AS-A網内でのdown/up => AS-Aは安定的にx.x.y.0/24のみを広報するため、外部には影響を与えない。
AS-A～AS-B間でのdown/up => Internet全体でflapは発生するがまぁ許容範囲(w)

※Prefix、AS、Org情報はマスクしています。

AS-Aの設定変更だけで解決可能。

改善提案②x.x.y.0/24をInternetには広報しない

Mask長	経路数
/26	x 1
/27	x 3
/28	x 4
/29	x 4

JPNIC whois
x.x.x.0/18(B社/Allocation)
x.x.y.0/24(A社/SubAllocation)

whois上では該当network範囲で
サブアロケーションされている

JPIRR

route: x.x.x.0/18
origin: AS-B
source: JPIRR

Internet

AS-B

経路奉行

①AS-AはOrigin AS-Aで
x.x.y.0/24(1経路のみ)
をAS-A内で集約し、AS-Bに広報
AS_PATH: A A

②AS-BはAS-Aから受信した
経路はInternetに広報せず、
AS-B網内のみに留める。
x.x.x.0/18が広報されていれば
問題なくルーティングされる。

④経路奉行では正常な経路
としてスルー
x.x.x.0/24を受信した場合
は経路リークとして検知で
きる(?)

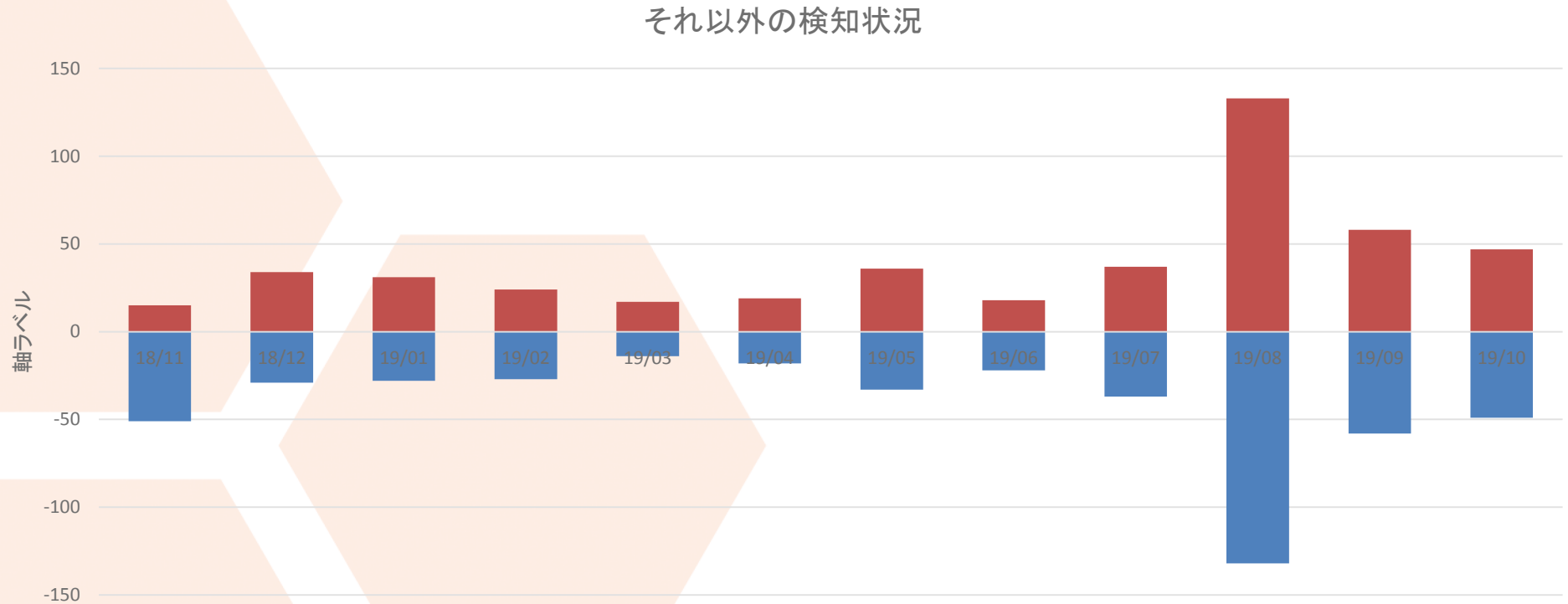
③
AS-A網内でのdown/up => AS-Aは安定的にx.x.y.0/24のみを広報するため、外部には影響を与えない。
AS-A～AS-B間でのdown/up => Internet全体には波及しない。

※Prefix、AS、Org情報はマスクしています。

AS-A, AS-Bの設定変更が必要。

イベントAを除いた検知状況

まぁ、ぼちぼちです。

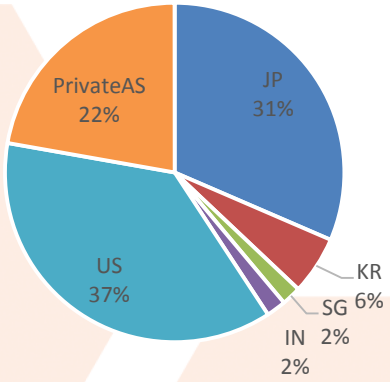


	18/11	18/12	19/01	19/02	19/03	19/04	19/05	19/06	19/07	19/08	19/09	19/10
発生	15	34	31	24	17	19	36	18	37	133	58	47
回復	-51	-29	-28	-27	-14	-18	-33	-22	-37	-132	-58	-49

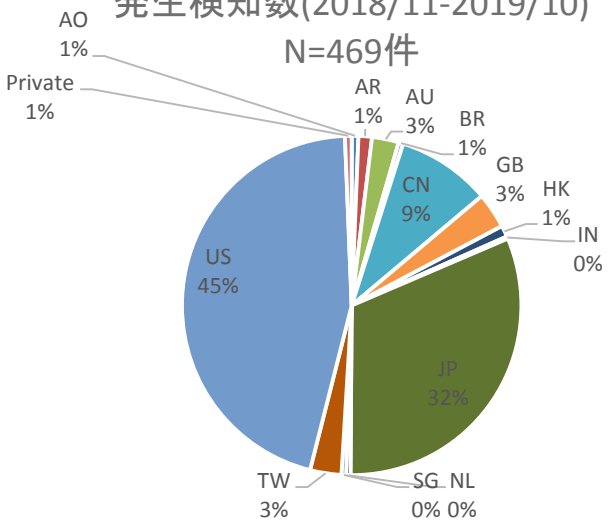
それ以外の検知状況の分析

- 発生検知のOrigin ASの国別割合を10年前のデータと比較

発生検知数(2008/03-2009/10)
N=54件



発生検知数(2018/11-2019/10)
N=469件



- 検知数Nの増加
  経路数の増加
  JPIRRの登録普及に伴う、検知対象prefixの増加
- 国種別がバラエティに富んできている
  10年前はAP/USリージョンに限定されていた。
  現在はその他のリージョンのOrigin ASからも。
- PrivateASは減った
  remove-private-asや経路フィルタが普及した?

ヒアリングベースで「やられた！」件

ICT-ISAC JAPAN

■ 実際に経路ハイジャックされた例は４件（あくまでヒアリングできた限りで）

2019/05 アンゴラ方面から

- 1prefix広報(/24)
- 発生・回復を3回繰り返す。
- ３回目発生後、/24を広報して応戦し、経路奉行では回復。

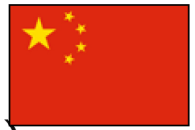
2019/05 アルゼンチン方面から

- 2prefix広報(/23, /24)
- 発生・回復を3回繰り返す。
- ３回目発生後、/24および/25x2を広報して応戦し、経路奉行では回復。
- 広報元にメールしたところ、「設定を間違えた」と返答を受ける。

2019/07 ブラジル方面から

- 1prefix広報(/24)
- 6分後回復したため、特に対応しなかった。

2019/09 中国方面から



- 1prefix広報(/24)
- 発生後、中国方面の知り合いに片っ端からメール。その後回復。＾＾)

３．2019年に発生した大きなルーティングインシデント（と、その時経路奉行ではどのように見えていたか？）

2019年に発生した主なルーティングインシデント

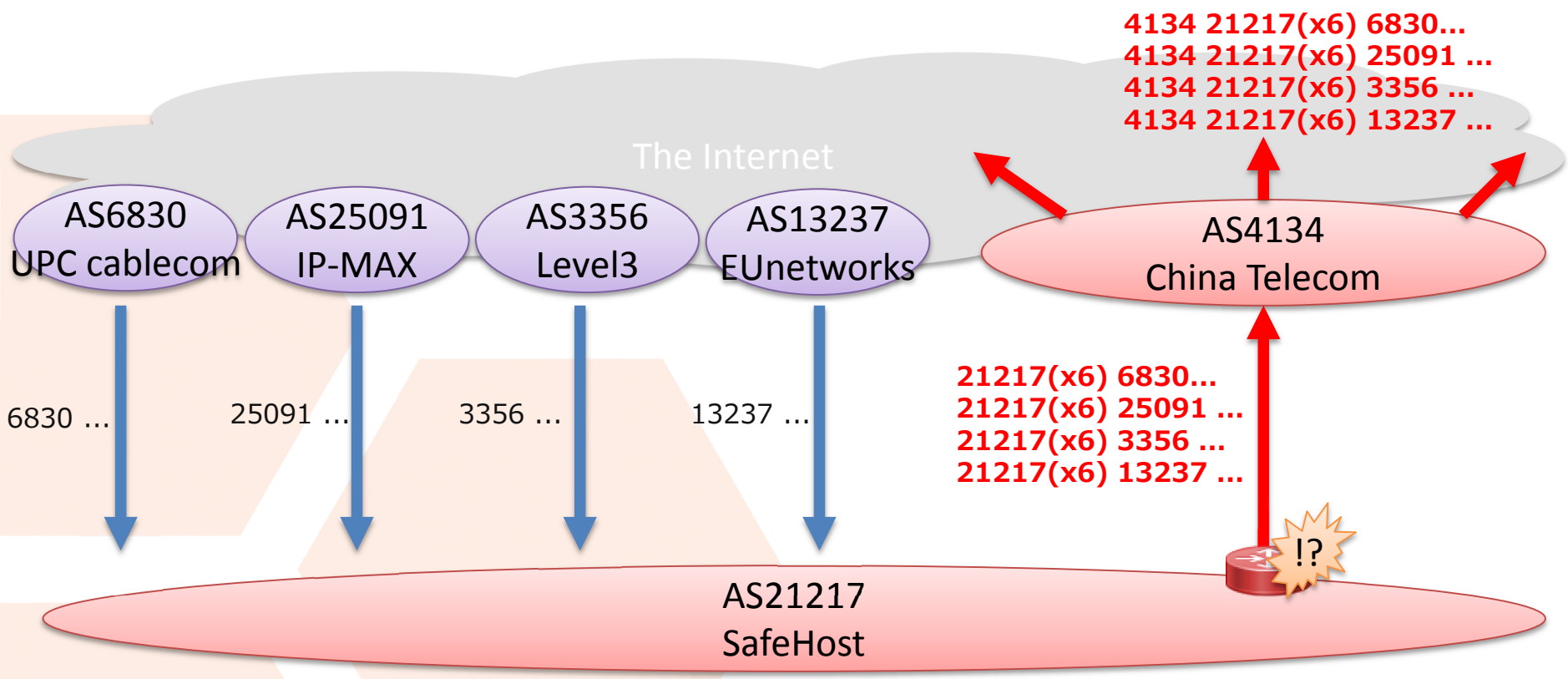
事例１）CTの大量経路リーク

事例２）BGPオプティマイザとVerizonの経路リーク

事例１）
CTの大量経路リーク（サマリ）

- 事象　：6/6 09:43(UTC)ごろ、スイスのDC事業者であるSafeHost(AS21217)が、大量の経路をChina Telecom(AS4134)にリークし、さらにInternet全体に伝播した。
- 広報時間　：約2時間以上？
  さみだれにリークが発生しており、
  影響時間はそれぞれ異なっている。
- 影響Prefix数　：7万経路以上
- 参照元　：
  - ORACLE
    “Large European Routing Leak Sends Traffic Through China Telecom”
    https://blogs.oracle.com/internetintelligence/large-european-routing-leak-sends-traffic-through-china-telecom
  - arstechnica
    “BGP events sends European mobile traffic through China Telecom for 2 hours”
    https://arstechnica.com/information-technology/2019/06/bgp-mishap-sends-european-mobile-traffic-through-china-telecom-for-2-hours

事例１）
CTの大量経路リーク（イメージ）



事例１）
CTの大量経路リーク（補足①）

SafeHost(AS21217)のtwitterによると、
当時彼らは何もオペレーションしてなかった模様。
その後の彼らの調査では、ルータのFIB使用率が高負荷となりoutフィルタに影響を与え、経路をリークした
とPOSTしている。

https://twitter.com/swisscolo

事例１）
CTの大量経路リーク（補足②）

China Telecom経由になったといっても、中国経由になったわけではなく、
China TelecomのヨーロッパエリアのPOPを経由になった模様。

traceroute from Google (Ashburn, VA) to ACOnet (Vienna, Austria) at 09:57 Jun 06, 2019

1	*				0.0
2	195.219.50.2	if-ae-7-2.tcore1.fnm-frankfurt.as6453.net	Frankfurt	Germany	86.451
3	*				0.0
4	*				0.0
5	118.85.205.233	CHINANET BACKBONE NETWORK	Amsterdam	Netherlands	265.544
6	*				0.0
7	202.97.52.65	CHINANET backbone network	Frankfurt am Main	Germany	387.218
8	118.85.205.90	CHINANET BACKBONE NETWORK		China	340.859
9	80.80.225.142	vlan24.cs2.gva.safehost.net	Genève	Switzerland	297.579
10	80.80.225.211	Safe Host Network Geneva	Genève	Switzerland	309.027
11	80.80.225.193	ge-3-1.ds4.gva.safehost.net	Genève	Switzerland	308.962
12	83.137.83.1	euNetworks GmbH	Vevey	Switzerland	222.019
13	80.86.163.17	Loopbacks and PtP links Switzerl	Braunschweig	Germany	219.624
14	217.71.96.37	ae6.irt1.fra44.de.as13237.net	Frankfurt am Main	Germany	218.007
15	217.71.96.6	ae4.irt1.mun02.de.as13237.net	Munich	Germany	213.565
16	217.71.96.110	ae1.400.irt1.vie08.at.as13237.net	Vienna	Austria	222.668
17	193.171.255.33	ACOnet Services Network	Vienna	Austria	221.573

インシデント発生中のtraceroute結果（前述のarstechnica記事より）
→5～8Hop目がChinaNetのネットワーク。
(8Hop目の国表示は”China”となっているがおそらくこれはアドレッシングによるものと思われる。）

事例１）
CTの大量経路リーク（経路奉行ではどう見えた？）

ICT-ISAC JAPAN

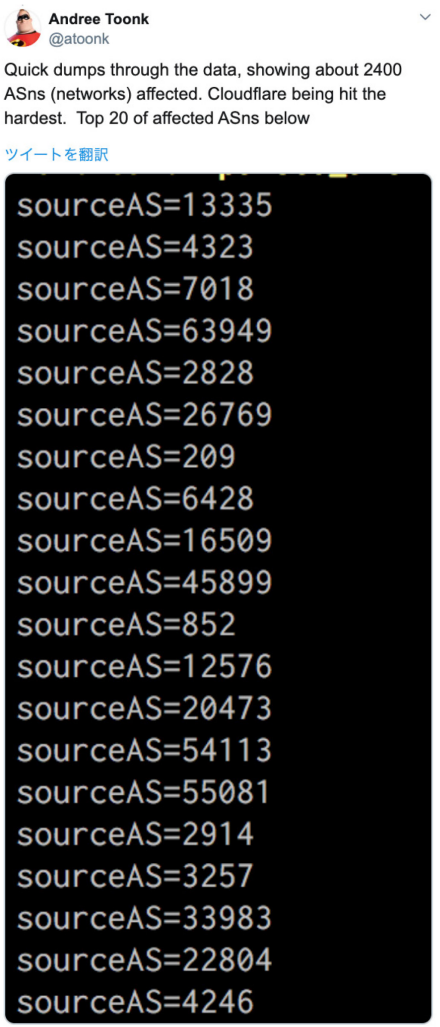
- 経路奉行ではどう見えていたか？
  - 該当時間近辺で、AS_PATHが
    ”4134 21217”
    を含む経路を探索。

	ORACLEによるレポート	経路奉行での観測
影響時間(UTC)	約2時間以上 09:43-13時過ぎ(グラフより)	3時間43分 09:43-13:26
影響Prefix数	7万経路以上	24,682経路(経路奉行合計)

  - すべてのAS(17AS)で観測しているが、受信した経路（および経路数）は各ASごとにさまざまだった。(1,243～20,185経路)
    これは、各ASごとのピア形態によるものであると思われる。

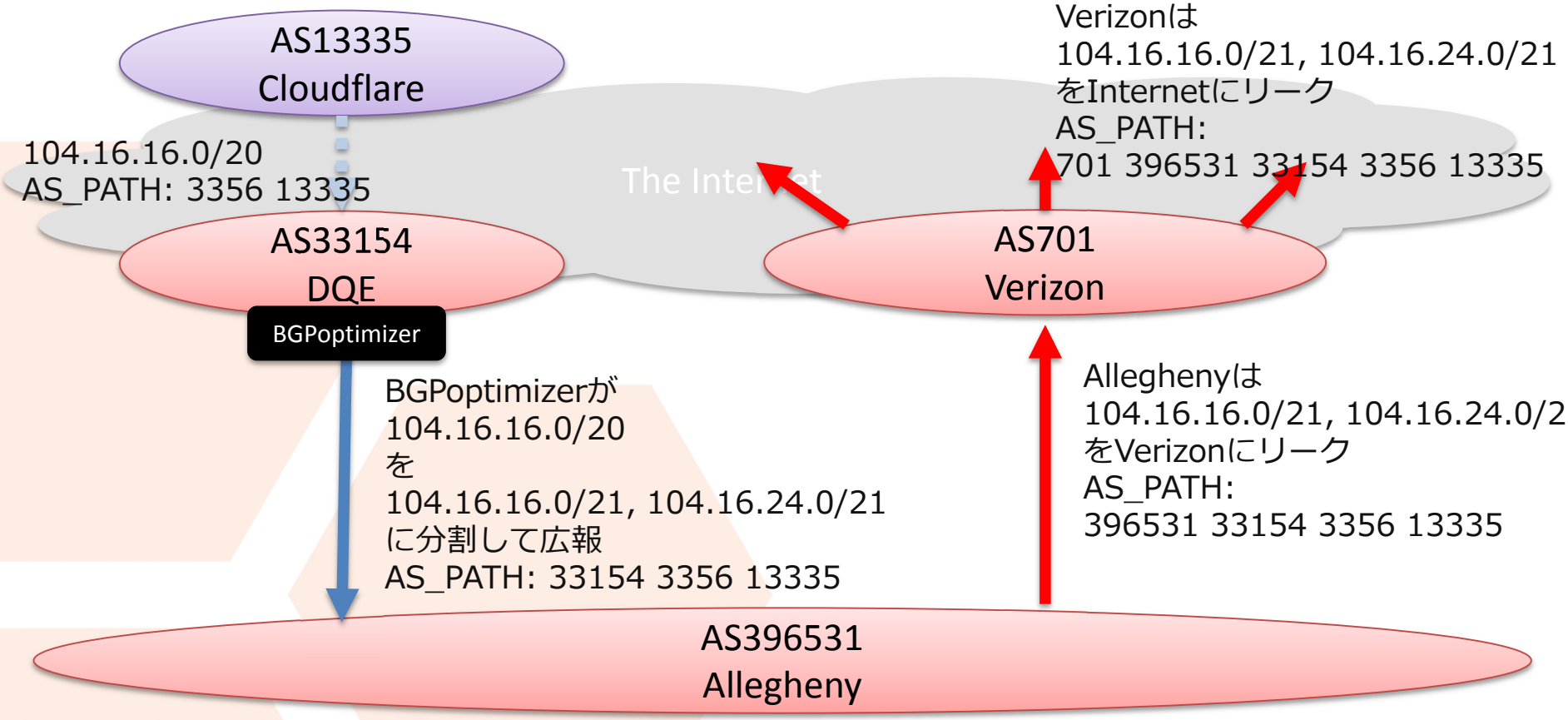
事例２）
BGPオプティマイザとVerizonの経路リーク（サマリ）

- 事象　：06/24 10:30(UTC)ごろ、Allegheny(AS396531) がDQE(AS33154)との間でのみ交換されていたCloudflare, Linode, Amazonなどの経路を分割した経路を、Verizon(AS703)にリークし、さらにInternet全体に伝播した。
- 広報時間　：約2時間？10:30-12:30(UTC)ごろ?
- 影響AS数　：約2,400AS
- 参照元　：
  - Cloudflare
    “How Verizon and a BGP optimizer Knocked Large Parts of the Internet Offline Today”
    https://blog.cloudflare.com/how-verizon-and-a-bgp-optimizer-knocked-large-parts-of-the-internet-offline-today/amp/
  - Twitter @atoonk
    https://twitter.com/atoonk/status/1143143943531454464



事例２）
BGPオプティマイザとVerizonの経路リーク（イメージ）

Cloudflare記事内に記述されているPrefixを例にしています



<u>BGP optimizerって何?</u>

受信したBGP経路を２分割して広報することでトラフィックを制御する装置。
Noctionという製品が使われていたようです。

事例２)BGPオプティマイザとVerizonの経路リーク（経路奉行ではどう見えた？）

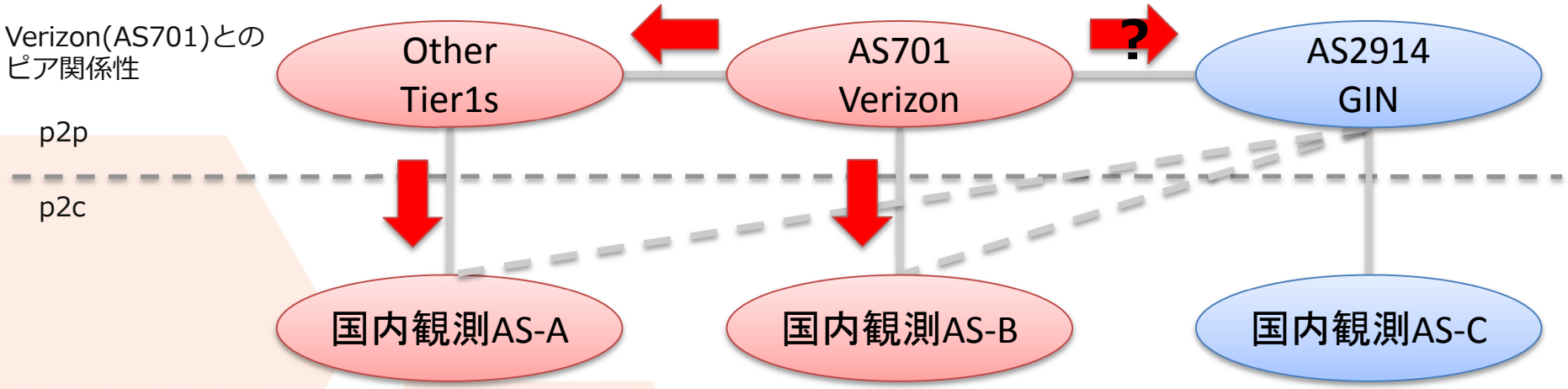
- 経路奉行ではどう見えていたか？
  - 該当時間近辺で、AS_PATHが”701 396531 33154”を含む経路を探索。

	Cloudflare/@atoonk氏によるレポート	経路奉行での観測
影響時間(UTC)	約2時間 10:30-13時過ぎ	1時間45分 10:34-12:19
影響Prefix数	20,297	9,315経路(経路奉行合計)
影響Origin AS数	約2,400	約1,248(@atook氏のtwitterでのtop20はすべて含まれていた。)

  - 17AS中、14ASでリーク経路を受信。
→AS2914およびAS2914からのみトランジットを購入していると推定される2ASは、まったくリーク経路を受信していなかった。

事例２)BGPオプティマイザとVerizonの経路リーク（経路奉行からみる国内状況）

リーク経路受信状況からパターンわけするとこんな感じ



国内観測AS-A：(Verizon, GINではない）他のTier1からトランジットを購入している（と思われるAS）
=>影響あり

国内観測AS-B：Verizonからトランジットを購入している（と思われるAS）
=>影響あり

国内観測AS-C：GINから**のみ**購入している（と思われるAS）
=>影響なし

※AS-A, AS-Bパターンにおいて、GINからもトランジットを購入しているパターンがありますが、More specific経路を他から受信した場合はそちらを優先するため、影響を受けてしまう。

事例２)BGPオプティマイザとVerizonの経路リーク（なぜGINだけ？）

なぜ、GINだけリーク経路を受信しなかったのか？
考えられる要因は

１．Verizon(AS701)はGIN(AS2914)にだけリークしなかった？

そんな、バカな...。

２．Verizon(AS701)はGIN(AS2914)にリークしたが、GINのルータでMaximum prefix limitが働いた？

ありえるけど、しきい値を超えるまではリーク経路を受信するはずで、経路奉行にも記録が残るはず！
でも無い。

３．その他？

...Peer Lock！？

事例２）
BGPオプティマイザとVerizonの経路リーク（Peer Lock）

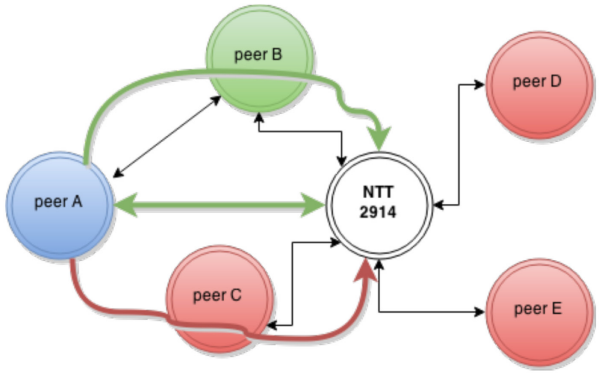
“Peer Lock” route leak prevention

https://archive.nanog.org/sites/default/files/Snijders_Everyday_Practical_Bgp.pdf
http://instituut.net/~job/peerlock_manual.pdf
http://peerlock.net/

BignetworksのAS

Peerlock schematic goal

Given ASNs A, B, C, D, and E as our peers. Peer A subscribes to the peerlock idea (`Protected ASN`) and indicates that peer B is an ”`Allowed Upstream`”



OK: ^A_
OK: ^B_A_
NOT OK: ^C_A_
NOT OK: ^D_A_
NOT OK: ^E_A_

Job Snijders - Peerlocking - NANOG67

```
RP/0/RSP0/CPU0:r04.miamfl02.us.bb#show run as-path-set lock-AS7018-in
as-path-set lock-AS7018-in
  ios-regex '_174_',
  ios-regex '_701_',
  ios-regex '_1239_',
  ios-regex '_1299_',
  ios-regex '_2828_',
  ios-regex '_3257_',
  ios-regex '_3356_',
  ios-regex '_3491_',
  ios-regex '_3549_',
  ios-regex '_6762_',
  ios-regex '_6830_',
  ios-regex '_6939_',
  ios-regex '_7922_',
  ios-regex '_8283_'
end-set
!
```

These are generated
- per peer
- per region

```
{master}
job@r27.tokyjp05.jp.bb-re0> show configuration policy-options as-path lock-AS3491-in
".* (174|701|1239|1299|2828|3257|3356|3549|6762|6830|6939|7018|7922|8283) .* ";

{master}
job@r27.tokyjp05.jp.bb-re0>
```

Job Snijders - Peerlocking - NANOG67

今回の事例では、AS701からリークされた経路のAS_PATHには、AS3356など”Bignetworks”が必ず含まれており、AS2914はすべてをrejectし流入を防ぐことができた。

事例２）
BGPオプティマイザとVerizonの経路リーク（Peer Lock）

- 前述の“Peer Lock”による対策は、すべての経路リークを防止できるわけではない。
しかし、今回のように大規模な経路リークの影響を最小限にできる効果がある。

- upstreamを持たないTier-1ならではの対策かもしれない。
ただし、提案者のJobさん曰く、
「相手のピアとちゃんと話し合えばやり方はある。
日本でもぜひ取り組んでほしい。」

> I think there are some ways to make the concept of peerlocking work of closely coordinating and cooperating ISPs. It would be good to cooperate between these organizations to increase the routing security pousure of Japanese internet routing. Thank you for kicking off.

ご参考までに。

4. 世界で利用されている BGP経路監視システムについて

6年前の経路監視システムはこんな感じでした

検知システム比較

	経路奉行	BGPmon	Cyclops	IS Alarms	Renesys
経路の情報源	国内ISPの経路情報	RIPE-RIS / Route views		RIPE-RIS	More than 360 sites
情報源との比較方法	JPIRR	ユーザ入力情報			
通知、確認方法	メール	Web/メール SMS	Web メール RSS	Web メール Syslog	Web
備考	JPIRRにObject登録で監視対象 X-keiro登録で通知対象	有料 (5prefixまでは無料) ROA対応らしい	事前登録要 ASNでPrefixも登録可 MITM検知	事前登録要 Prefix手入力 MITM検知	有料
その他	国内最強	遠回りする事例(MITMの可能性)やAS詐称も検知できた	動いてないかも	現在停止中	MITM検知できるとある

2013/11/26 KDDI株式会社 - All Rights Reserved 38

IW2013 D1 中野さん資料
https://www.nic.ad.jp/ja/materials/iw/2013/proceedings/d1/d1-nakano-IW2013_nakano_20131113.pdf

BGPmonはEnd of Lifeになるようです

BGPmonは来年春（2020/03/01）でEoLになるようです。

Question	Response
When is the BGPMon End of Sale and End of Live Announcement	January 31, 2019
When is the BGPMon End of Sale	March 1, 2019
When is the BGPMon End of Life	March 1, 2020
When is the BGPMon End of Existing Service / Support	For customers with active and valid BGPMon.net subscriptions, the service will be available until the termination date of the contracted subscription term, even if this date exceeds the End of Life. For all other customers the End of Life is the last date that the service will be accessible.
Who do I contact if I have further questions not answered in this FAQ	Please email eol@bgpmon.net, we will respond as quickly as possible.
What is the replacement product for BGPMon.net	Cisco have created a new product called Crosswork Network Insights
What do I do if my existing BGPmon.net Paid subscription falls after the End of Sale	You can continue to use BGPMon.net until End of Life at no charge, based on your existing level of subscription. You will be invited to a no obligation trial of Crosswork Network Insights during this time.
If I am a Paid customer of BGPMon.net do I automatically get a Trial	No, Trial request must be made via two methods 1) Via your Cisco Account representative or your Partner Channel representative.

https://bgpmon.net/wp-content/uploads/2019/01/BGPMon.net-EOL-EOS-faq.pdf

後継サービスとしては、買収先のCisco社の
「Cisco Crosswork Network Insights」
https://www.cisco.com/c/ja_jp/support/cloud-systems-management/crosswork-network-insights/model.html
の１機能として統合。（すでに一部は統合されている）

FAQを見る限り、（アカウント再作成は必要だが、）無料アカウントはありそう。

有償サービス系のBGP監視システム

詳しくは知らないので簡単な紹介にとどめます。

- ThousandEyes
  https://www.thousandeyes.com/
  ・もともとはサービス/エージェント監視システムで、BGP監視と組み合わせることで、より通信異常を検知できそう。
  ・GUIかっこいい
  ・ルーティングインシデント系のブログ更新頻度が多く、BGP経路監視にも力をいれていそう。
  ・15日間の評価ライセンスあり。

- Radar by Qrator
  https://radar.qrator.net/
  ・ロシアとチェコの会社。
  ・DDoS, DNSプロテクションなどがメインのサービスの模様。
  ・無料アカウントを作成し、監視対象のアドレス管理者に承認されることで、一部機能（経路異常の履歴閲覧および定期的なサマリレポート）を利用可能。

- BGProtect
  https://www.bgprotect.com/
  ・イスラエルの会社が運営
  ・詳細は全く不明 m(_)m

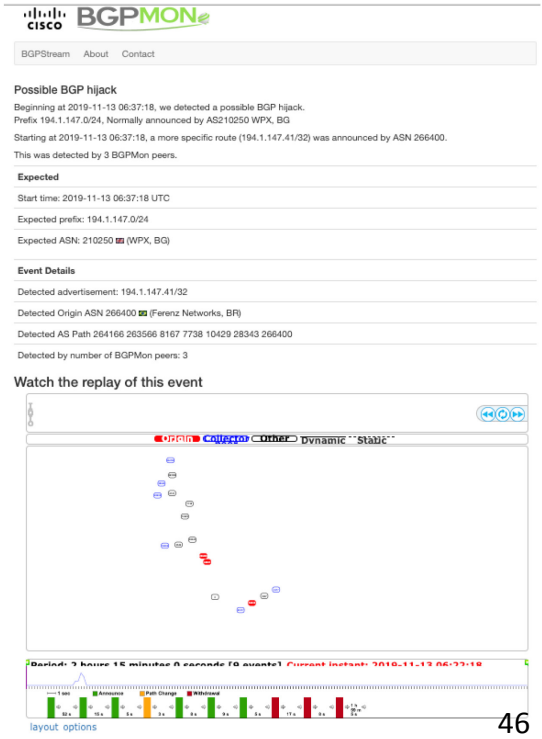
無償サービス（？）系のBGP監視システム

- BGPstream
  https://bgpstream.com/
  経路異常(Possible Hijack, Outage)が発生するとtwitterで配信
  - Possible Hijack(HJ): Origin ASが異なる経路を受けたとき(?)
  - Outage(OT): AS単位で経路が消失
  - BGP Leak: HPでのみ表示。

  発生イベントごとにリンクが設定され、BGPlayが起動。
  自分で監視対象の設定はできない。
  結構な頻度で流れてくる。
  最近、HPにCiscoの冠がついた。

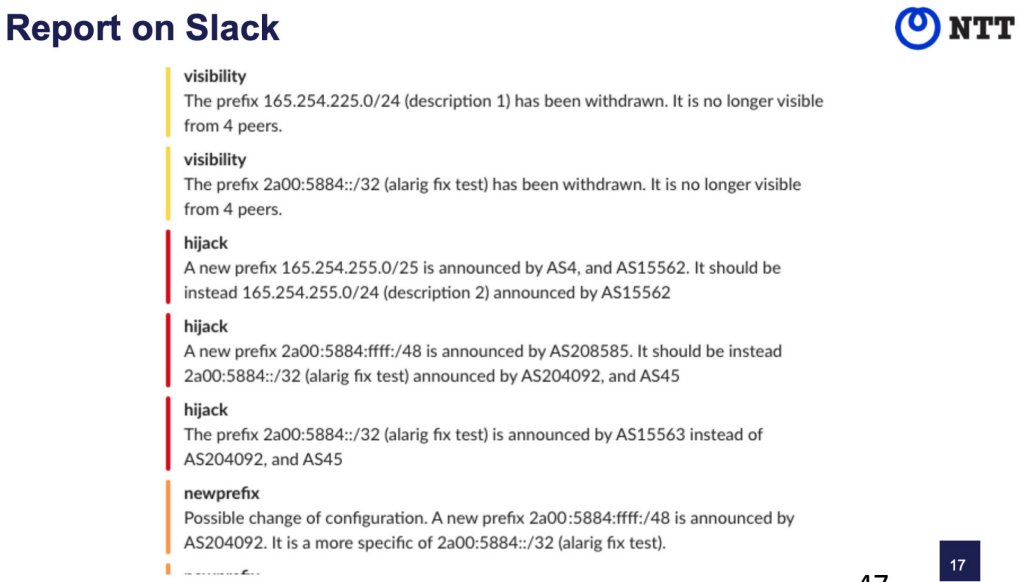
クリックすると

サイトに飛んで詳細な情報が確認できる。



オープンソース系のBGP監視システム①

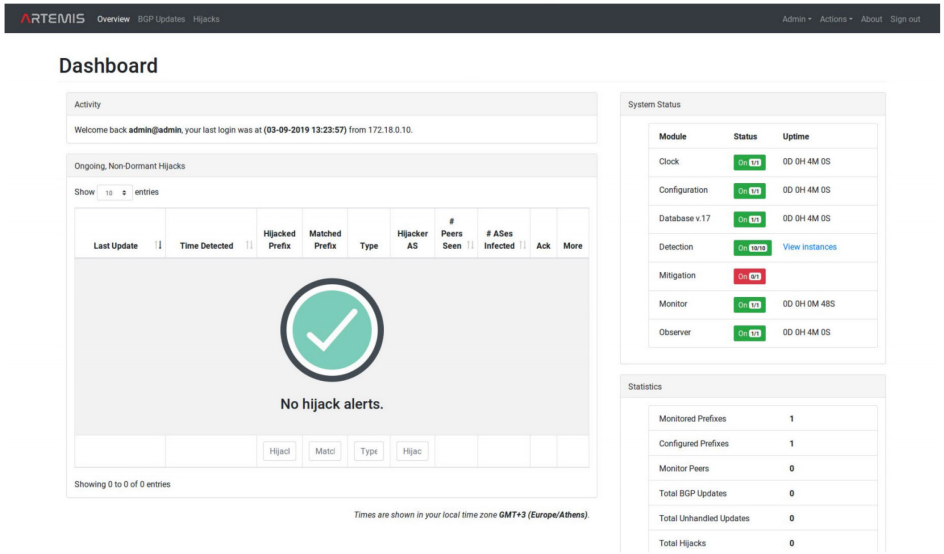
- BGPalerter
  - リポジトリ
    https://github.com/nttgin/BGPalerter
  - 先日のRIPE67での発表資料
    https://ripe79.ripe.net/presentations/111-BGPalerter_ripe79.pdf
  - インストールや設定が比較的簡単。
  - Node.jsで書かれており、依存するアプリケーションなどはない。
  - 情報ソースはRIPE RIS live(websocket)のみ。
  - ファイル、メールやslackなどに出力できる。
  - 検出種別
    - hijack
    - visibility
    - new prefix



オープンソース系のBGP監視システム②

- Artemis
  - リポジトリ
    https://github.com/FORTH-ICS-INSPIRE/artemis
  - 先日のRIPE67での発表資料
    https://ripe79.ripe.net/wp-content/uploads/presentations/11-KOTRONIS_ARTEMIS_LT_RIPE79.pdf
  - RabbitMQ, PostgreSQL, Redisなど多くのアプリケーションに依存している。
  - docker-composeまたはkuberneres(helm)でも起動可能。
  - 情報ソースは以下を利用可能。
    - RIPE RIS live
    - BGPstream
    - Local(exabgp)
  - ファイル、メールやslackなどに出力できる。
  - GUIでの設定変更・状況確認
  - 隣接関係を細かく設定すれば経路リークなども検出できる。
  - Mitigationも可能（未検証）

Demo: Start and configure ARTEMIS



5. BGP経路監視の現状と展望

経路奉行の現状

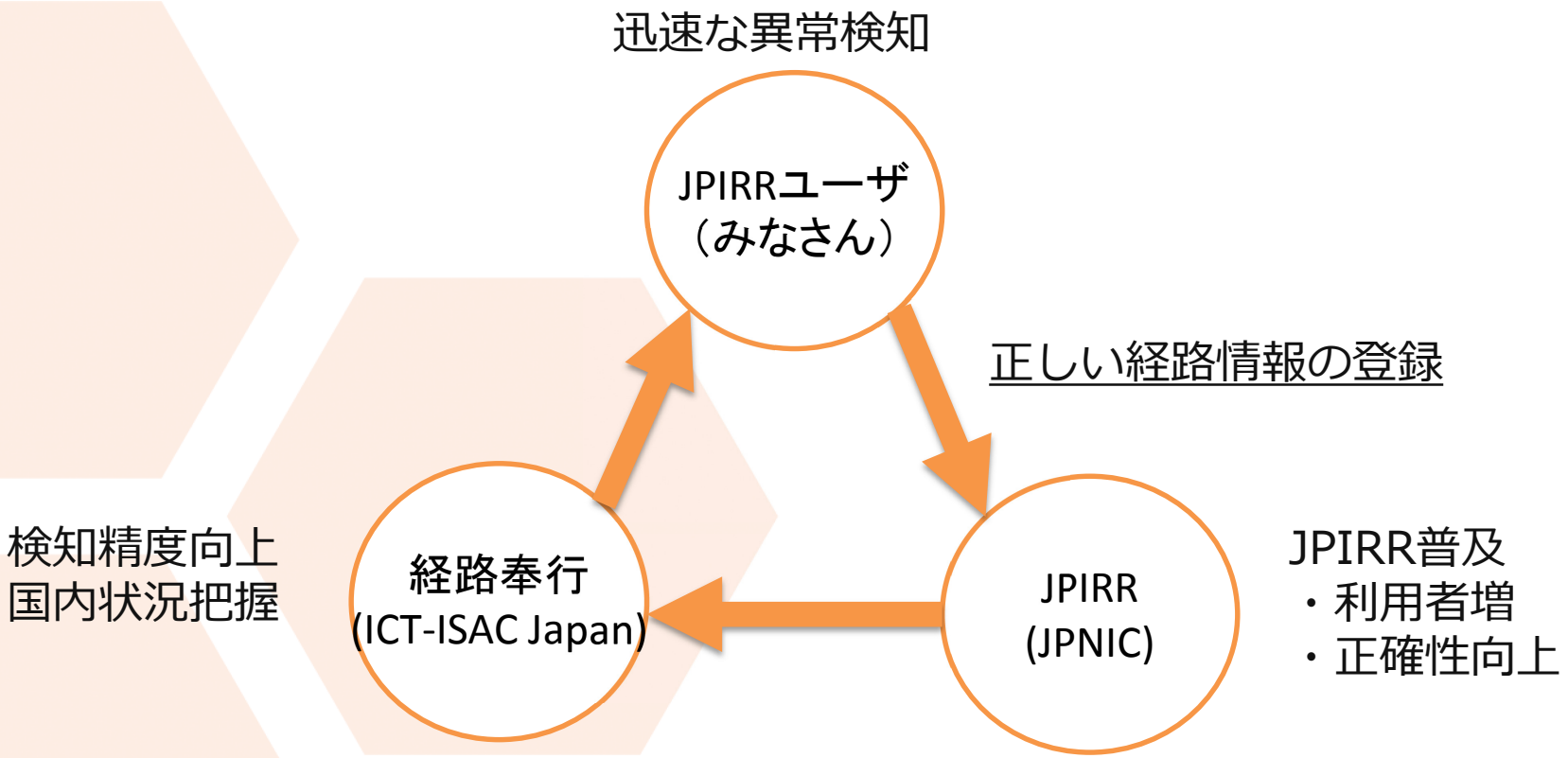
- いいところ
  - 日本国内の観測ASは他の監視システムよりも多い。
  - (JPNIC会員なら）無料
  - JPIRRと連動できる

- ダメなところ
  - 海外の観測ASがない
  - “経路ハイジャックが疑われる状態”しか検知できない
  - ポータルとかがない

ダメなところは改善できるよう検討していきます。

経路奉行（関係者）からの（いつもの）お願い

JPIRRユーザのみなさんが、正確に経路情報を登録いただくことで、良好なサイクルをまわすことができます。



ひきつづき、ご協力おねがいいたします。

BGP経路監視の現状（その１）

近年、Invalid Origin AS(いわゆる経路ハイジャック）だけでなく、経路リークも注目されている。

昔は「あー、遠回りで遅延してるね。」

今は、

- 大量のMore specific
  IPv4フルルート(80万弱) + 数万～十数万のリーク経路になり非力なNW機器は死亡…
- クラウドプロバイダやコンテンツへの影響
  破壊力抜群のトラフィック....迂回できるわけがない
- from 中国 or ロシア
  ・・・

でも、経路ハイジャックと違って、経路リークを検知するのは難しい。
Origin ASだけでなく、AS_PATH内のASの隣接関係をチェックする必要がある。

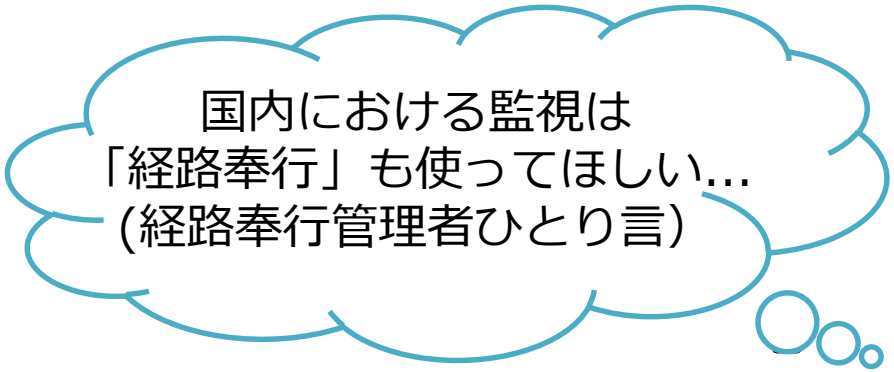
BGP経路監視の現状（その２）

さまざまな経路監視システムが存在し、さまざまな手法で
経路異常を検知する取り組みがなされている。
特に２極化されていきそう。

- 有償サービス(Cisco/aka BGPmon, ThousandEyes, etc)
  →リッチコンテンツ、サービス監視情報との連動、全てはお金で解決！

- Streamによる情報配信(RIS Live, BGPstream)
  + オープンソース(BGPalerter, Artemis, etc)
  →オペレータが自分でがんばる、カスタマイズできる。

など、世界中の経路監視ができ、かつ選択肢も増えてきている。



BGP経路監視の今後の展望

経路ハイジャックだけでなく、（今回紹介した）大量経路リークに
よっても大規模な障害が発生しており、迅速な状況把握といった意味で
BGP経路監視の重要度は増してきそう。

一方で、RPKIの普及や、PeerLockなどのworkaroundの導入など、
様々な実装や設定で経路制御をセキュアにしていく流れは続く。

では、セキュアな実装やその普及が進んだら、BGP経路監視は不要？

否！

BGP経路監視の今後の展望

BGP経路監視も、これらの動向と合わせて変化・進化していく必要がある。

- RPKI実装やフィルタ設定がちゃんと意図したとおりに動作しているのか？の検証
- OSやプロトコルのbugなど想定していない事象の原因解析

など検証・解析が可能な状態にしておくことに存在価値アリ！

線路は続くよどこまでも……