ICT-ISAC JAPAN

ICT-ISAC JAPAN
ICT Information Sharing And Analysis Center Japan

C8 明日のインターネットをみんなで守るルーティングセキュリティ

経路奉行での経路ハイジャック検知状況

2021/11/22
ICT-ISAC Japan/NTTコミュニケーションズ
渡辺　英一郎

はじめに

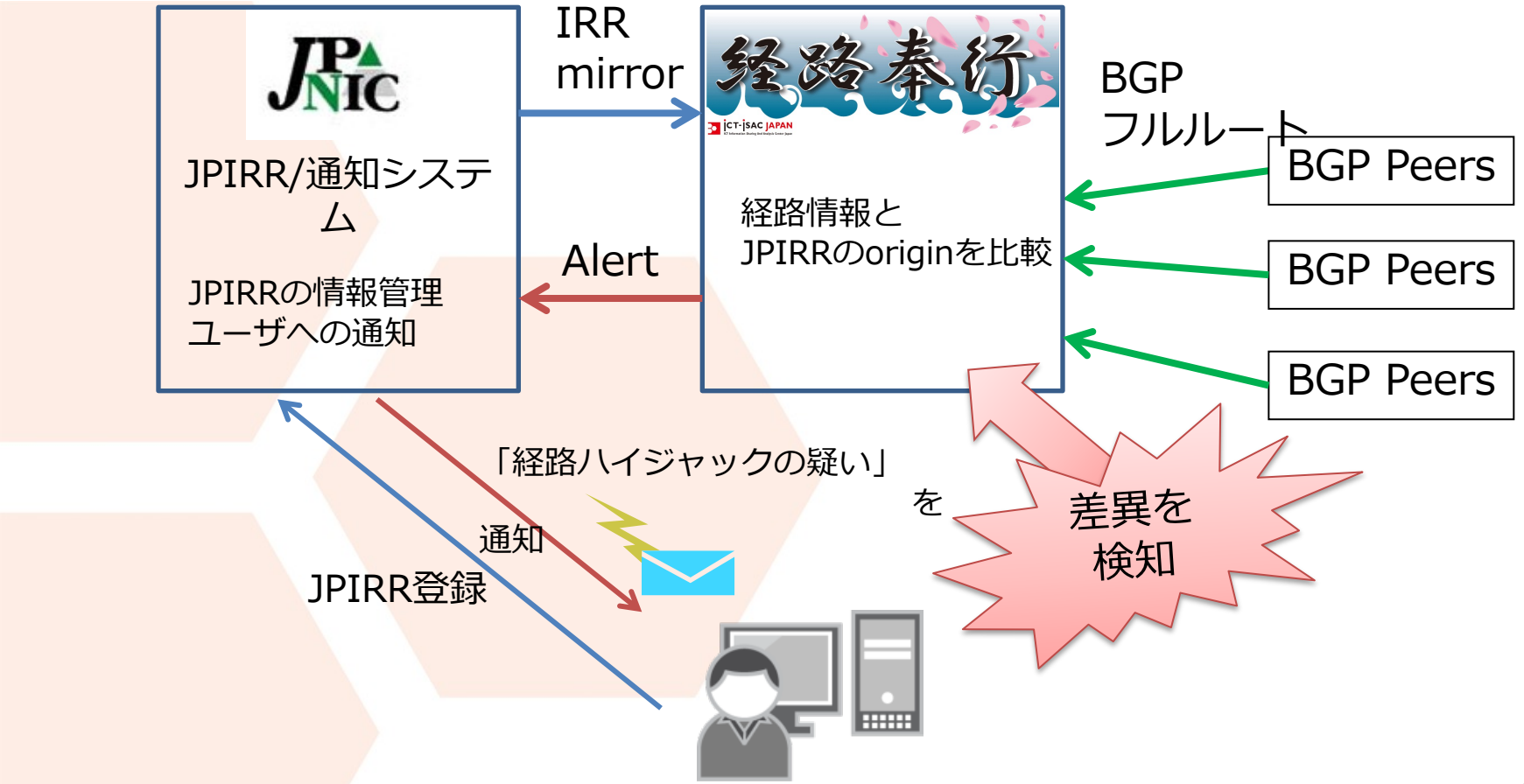
私のパートでは

ICT-ISAC Japanで運営している
経路ハイジャック検知システム「経路奉行」での
2021年の日本国内におけるアラート検知状況と検知事例

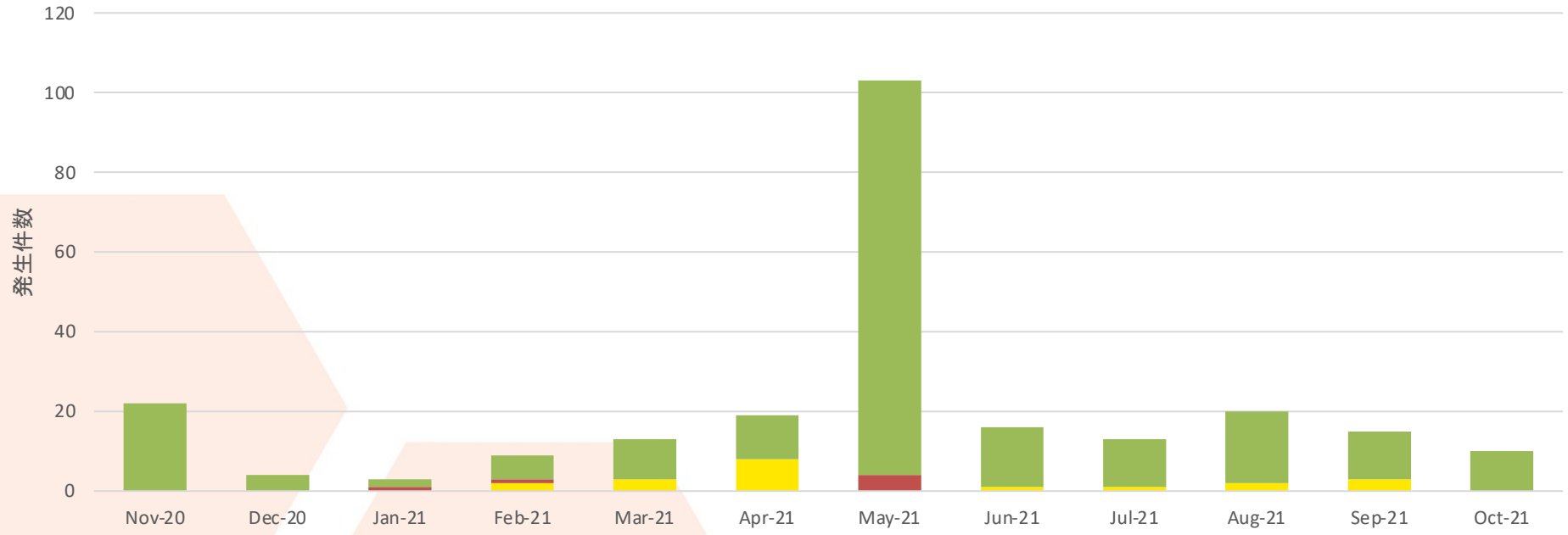
を話します。

経路奉行とは

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。



2021年の経路奉行でのアラート検知状況



	Nov-20	Dec-20	Jan-21	Feb-21	Mar-21	Apr-21	May-21	Jun-21	Jul-21	Aug-21	Sep-21	Oct-21
分類1	22	4	2	6	10	11	99	15	12	18	12	10
分類2	0	0	1	1	0	0	4	0	0	0	0	0
分類3	0	0	0	2	3	8	0	1	1	2	3	0

あえて差異発生時のアラートを分類してみる
分類１：おそらく通信影響がないと思われるもの→経路ハイジャックの可能性低
分類２：IXセグメントの誤広報→経路ハイジャックの可能性高
分類３：上記以外→経路ハイジャックの可能性中

分類１の事例

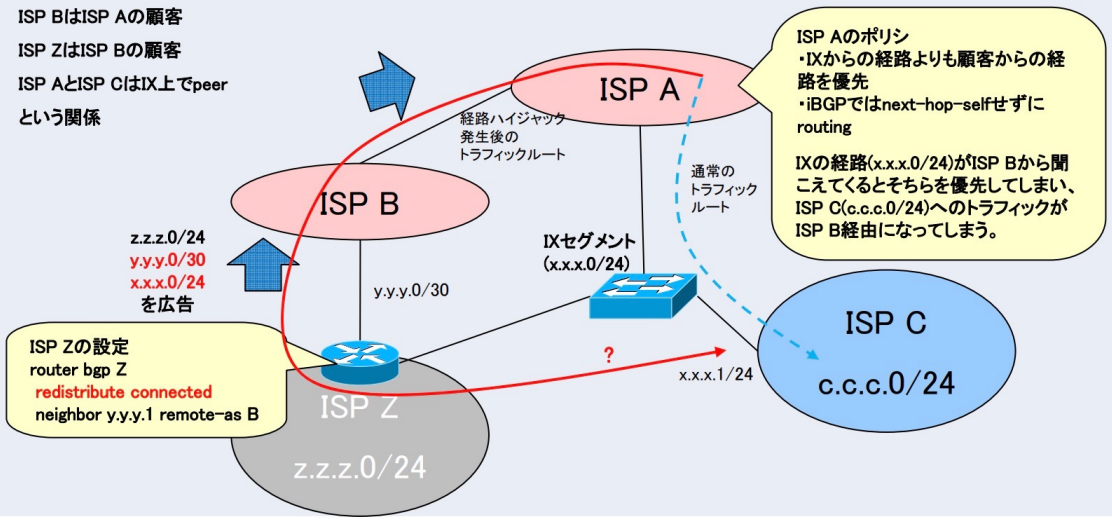
JPIRRの情報、受信したBGP情報、その他の情報(JPIRR以外のIRR、whoisなど)から、JPIRRには正しく登録されていないけれども、合意の上の経路広報である可能性が高いと考えられ、経路ハイジャックの可能性は低い。

- 複数のASから同一Prefixを広報するケースで一部のASの情報がJPIRRには登録されていない
  - ・JPIRRには登録せず、RADBにのみ登録されているなど
- 古い情報がJPIRRに残ったままになっている
  - ・PIアドレスの引っ越し
  - ・CDN事業者からレンタルされたアドレスの解約など
- BGPで広報されたOriginASとJPIRRのOriginASに何らかの関係性がある
  - ・同一会社の別AS
  - ・隣接AS(Transit-Customer関係)
- DDoS ProtectionサービスのASによる広報

JPIRRに正しく登録されれば、アラートは発生しませんので正しく管理しましょう！

分類２の事例

IX(インターネットエクスチェンジ）のユーザが、誤ってIXセグメントを、自オリジンとして他ASに再配信してしまうケース。
IXセグメントはIX事業者以外がグローバルに配信すべきものではないため確実に経路ハイジャック。
他社ASに影響を与える可能性もあるので注意！

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	

https://www.nic.ad.jp/ja/materials/iw/2009/proceedings/h10/iw2009-h10-02.pdf

分類２の対策

加害者にならないために

- 送信経路のフィルタリング
  - AS_PATH filter
  - Prefix filter
- IX接続ルータでredistribute connectedする場合は注意

被害者にならないために

- IXでPeer先から受信した経路はnexthop-selfして自AS内に配信する
  →nexthop-selfしていればIX経路が他から聞こえてきても影響は受けない
- nexthop-selfができないNW構成ならIX接続ルータ以外のeBGPルータでIXセグメントをrejectする
- IXセグメントがROAに登録されていれば、ROVの導入も有効

IX事業者の方へ

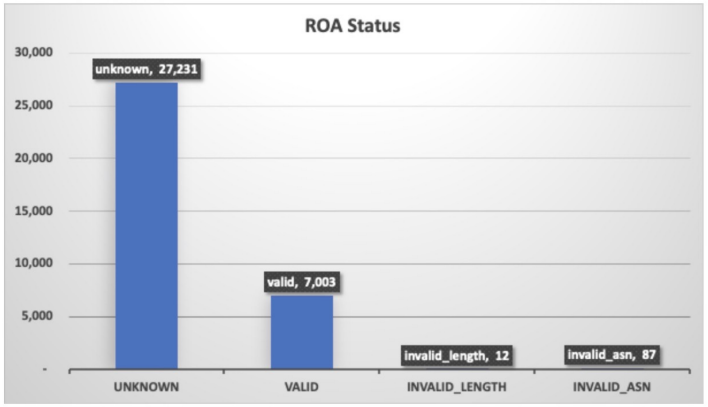
- IXセグメントを含む経路のROAを登録する（自ASまたはAS0で登録）
  一部のIX(MSK-IX, DE-CIX, Equinix, MegaIXなど)はAS0で登録している模様。
  ぜひ日本のIXでも導入を検討していただきたい。

分類３の事例（その１）

4/16 インドのAS(Vodafone Idea/AS55410)による大量経路の誤配信。

MANRSのブログ
https://www.manrs.org/2021/04/a-major-bgp-hijack-by-as55410-vodafone-idea-ltd/
によると、30,000超の他社AS経路(日本:409経路)が広報された模様。

Around 80% of the hijacked routes had no ROAs (unknown) hence those routes must have propagated globally, whereas little more than 7000 had valid ROAs means anyone else originating those routes made them invalid and must have been filtered out by many network operators. That's why it's key to create ROAs as it protects your prefixes from such hijack attempts, even if most are unintentional.



(意訳)
被害を受けた経路の約80%はROAが存在しなかったため、グローバルに伝搬したと思われるが、**7,000超についてはなROAが存在し、これらについては多くのネットワークオペレータによって除外されたはず。**

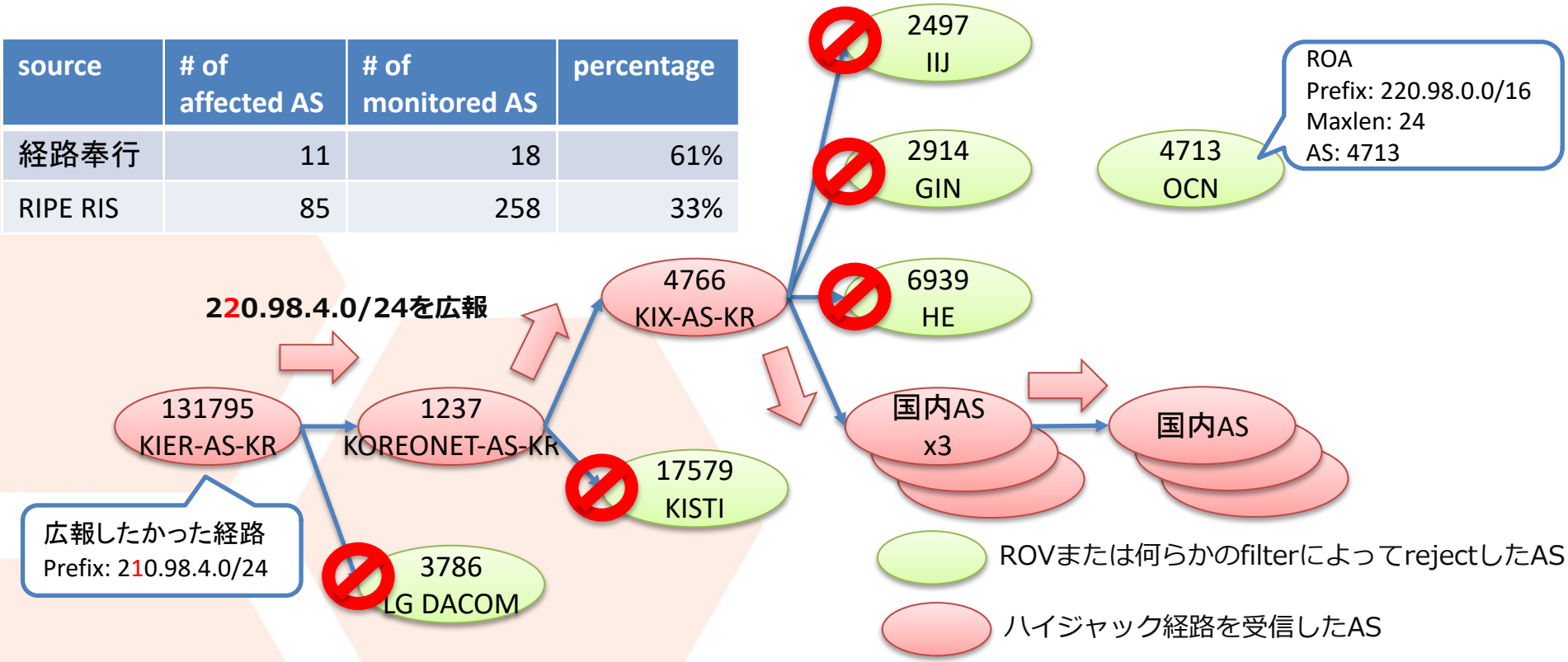
つまりROAを作成することは重要！

経路奉行においても、BGP情報提供元のASにより異なるが、約5,000～20,000経路受信。正しい経路と同一Prefixの広報だったため、AS_PATH長が短い正しい経路が選択され、国内通信には影響が少なかったと思われる。
経路奉行では、7経路(5AS)のアラートを検知。

分類３の事例（その２）

4/27 韓国のAS(KIER/AS131795)がOCN経路(220.98.0.0/16)の一部(220.98.4.0/24)を誤広報(fat finger)。約15分程度でwithdrawされて回復。

source	# of affected AS	# of monitored AS	percentage
経路奉行	11	18	61%
RIPE RIS	85	258	33%



Sub-prefix(more specific)ハイジャックであるため、通常であればグローバルインターネット全体(ほぼ100%)への到達性がなくなったと想定されるが、ROAを登録していたことにより、上流またはピアによって影響を低減できているといえる。

分類３の対策

加害者にならないために

- 送信経路のフィルタリング
  - AS_PATH filter
  - Prefix filter

被害者にならないために

- 大量経路の受信対策として受信経路制限の適用(max-prefix limit)
- 受信経路のフィルタリング
  - AS_PATH filter
  - Prefix filter
- 自ASオリジン経路の適切なROAおよびIRRの登録
- ROVの導入
  - 現時点で、自ASでのROV導入が困難なら、ROVを導入しているTransit ISPを選定するのもあり

最後に

ROAおよびIRRを正しく登録しましょう！

- 正しくIRRおよびROAを登録することで、不正な経路広報をした場合/された場合において、Internet上のセキュリティ意識の高いオペレータが検知または拒否することができ、Internet通信への影響を低減できます。今後、ROVの導入によってその範囲はより大きくなっていくことが予想されます。

- 日本において、JPIRRの登録率は比較的高いのに対し、特にROAの登録率はまだまだ低いです。ぜひ、ご協力を！

2021/09/03時点	IPv4	IPv6
ROA登録率	約37.8%	約32.0%
JPIRRのRoute Obj.登録率	約80.6%	約93.5%

現状、経路奉行では登録率の高いJPIRRベースで検知していますが、ROAの登録率が向上すればROAベースに変えていきたい。

明日のインターネットをみんなで守りましょう！