



東邦大学

いのち
生命の科学で未来をつなぐ

MOAI: Multiple Origin ASes Identification BGPの広告元特徴を取り入れた IP Prefix Hijacking検出を実装してみた

○東邦大学 今井 宏謙
日本ネットワークインフォメーションセンター 岡田 雅之
東邦大学 金岡 晃

目次

1. はじめに
2. 背景
3. 概要
4. 手法
5. 検証
6. 評価
7. 課題
8. まとめ

1. はじめに

- **氏名**：今井 宏謙
- **所属**：東邦大学 大学院
- **研究内容**：BGPのハイジャック検知について
- **出没場所**：技術系カンファレンスで時々NOCに参加
- **JANOG初参加**：JANOG38@金沢
 - 若者支援プログラム有難うございます
- **JANOG発表のきっかけ**：
 - 大学院でBGPハイジャック検知について研究しており、それを元に実際にネットワーク運用をしている方々と色々な話をしてみたかった

2. 背景

- インターネット

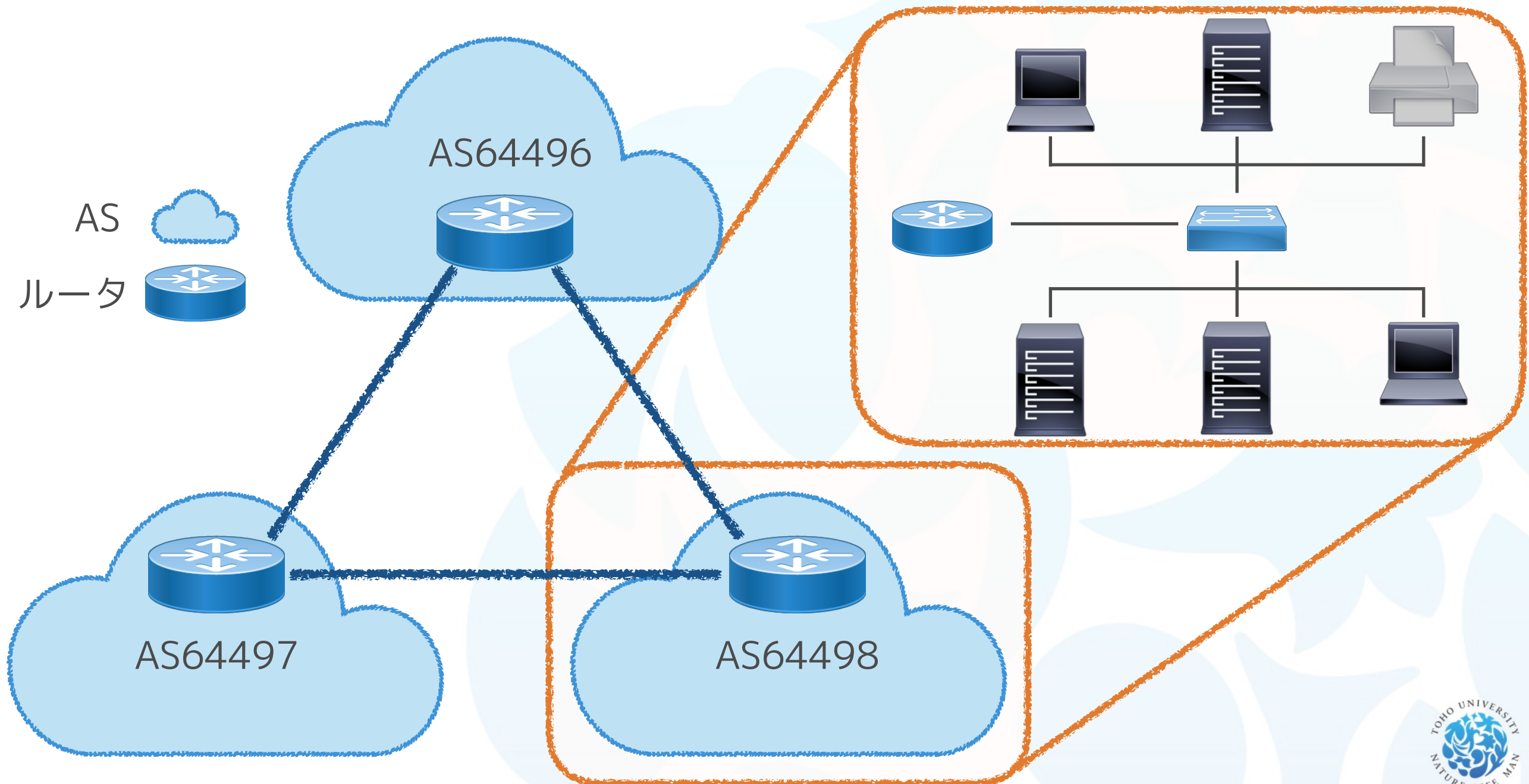
- 自律・分散・協調を基本的な考えとし、相互信頼の前提の上に成り立っているネットワーク

- BGP (Border Gateway Protocol)

- インターネット全体における経路制御に必要
- AS (Autonomous System) 単位で経路情報の交換を行う
- BGPの経路情報：AS番号+IPアドレス
- 経路情報をインターネット上に通知すること：「広告」と呼ぶ

• AS (Autonomous System)

- 共通のポリシーや同じ管理下で運用されているネットワークの集合
 - インターネットはこのネットワークの集合
- 各ASには識別するためのAS番号が割り当てられている



背景 - 不適切広告 (IP Prefix Hijacking)

10.1.1.10
にアクセス

エンドユーザ



AS 64496

ルーティングテーブル

IP Prefix	AS
10.1.1.0/22	64497
⋮	⋮

インターネット

正常

正規の接続先



背景 - 不適切広告 (IP Prefix Hijacking)

10.1.1.10
にアクセス

エンドユーザ



AS 64496

ルーティングテーブル

IP Prefix	AS
10.1.1.0/22	64497
⋮	⋮

インターネット

ハイジャック発生

不適切経路広告

(AS64498, 10.1.1.0/24)

正規の接続先

AS 64497 10.1.1.10

10.1.1.0/22
本物の経路情報

不適切な接続先

AS 64498

10.1.1.0/24
不適切な経路情報

背景 - 不適切広告 (IP Prefix Hijacking)

10.1.1.10
にアクセス

エンドユーザ



AS 64496

ルーティングテーブル

IP Prefix	AS
10.1.1.0/24	<u>64498</u>
⋮	⋮

インターネット

ハイジャック発生

不適切経路広告

(AS64498, 10.1.1.0/24)

- プリフィックス長が長い
 - 経由ASが少ない
- 経路情報が優先される

正規の接続先

AS 64497 10.1.1.10

10.1.1.0/22
本物の経路情報

不適切な接続先

AS 64498

10.1.1.0/24
不適切な経路情報

背景 - 不適切広告 (IP Prefix Hijacking)

10.1.1.10
にアクセス

エンドユーザ



AS 64496

ルーティングテーブル

IP Prefix	AS
10.1.1.0/24	64498
⋮	⋮

インターネット

ハイジャック発生

不適切経路広告

正規の接続先

AS 64497 10.1.1.10

10.1.1.0/22
本物の経路情報

不適切な接続先

AS 64498

10.1.1.0/24
不適切な経路情報

- プリフィックス長が長い
 - 経由ASが少ない
- 経路情報が優先される

不適切経路広告によるインシデントケース

- **YouTubeハイジャック（2008）**

- YouTubeへのアクセス不可
- コンテンツサービスへの損害

<https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study>



- **Bitcoinハイジャック（2014）**

- Bitcoinのマイニング結果が奪われる
- 攻撃者が\$83,000以上の利益を得る

<https://bgpmon.net/the-canadian-bitcoin-hijack/>



- **Amazon Route53ハイジャック（2018）**

- Amazon AWSのDNSサーバがハイジャックされる
- myetherwallet.comのDNS応答が改竄

<https://www.internetsociety.org/blog/2018/04/amazons-route-53-bgp-hijack/>



既存アプローチ

特定のASに関するハイジャック検知

Zhengら (2007), iSpy (2008)

pingやトラフィックのプローブを利用したハイジャックの検出手法

ARTEMIS (2018)

ASが主体となり, 自ASに対するハイジャックを検知・抑制

任意のASに関するハイジャック検知

PHAS (2006), pgBGP (2006)

Huら (2007)

IPプリフィックスの衝突する経路広告の検出手法

経路奉行

ICT-ISACの運営する, JPIRRを活用した日本国内のハイジャック検出

本研究の位置づけ

特定のASに関するハイジャック検知

Zhengら (2007), iSpy (2008)

pingやトラフィックのプローブを利用したハイジャックの検出手法

ARTEMIS (2018)

ASが主体となり，自ASに対するハイジャックを検知・抑制

広告元特徴：

ASの国割当情報やwhoisデータベースなど，OriginASに関する広く公開されているデータ

任意のASに関するハイジャック検知

PHAS (2006), pgBGP (2006)

Huら (2007)

IPプリフィックスの衝突する経路広告の検出手法

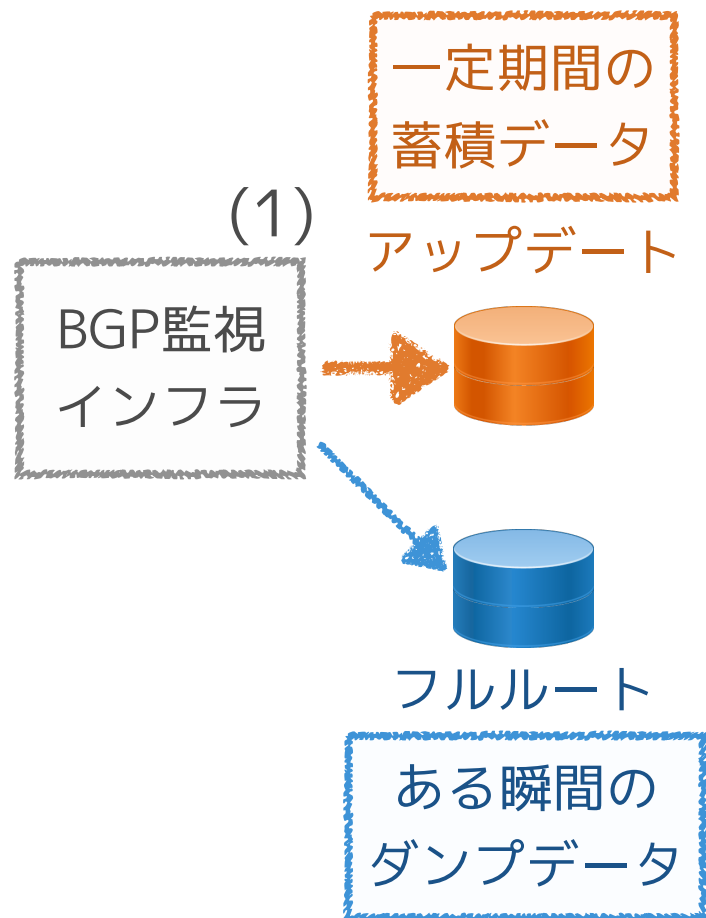
経路奉行

ICT-ISACの運営する，JPIRRを活用した日本国内のハイジャック検出

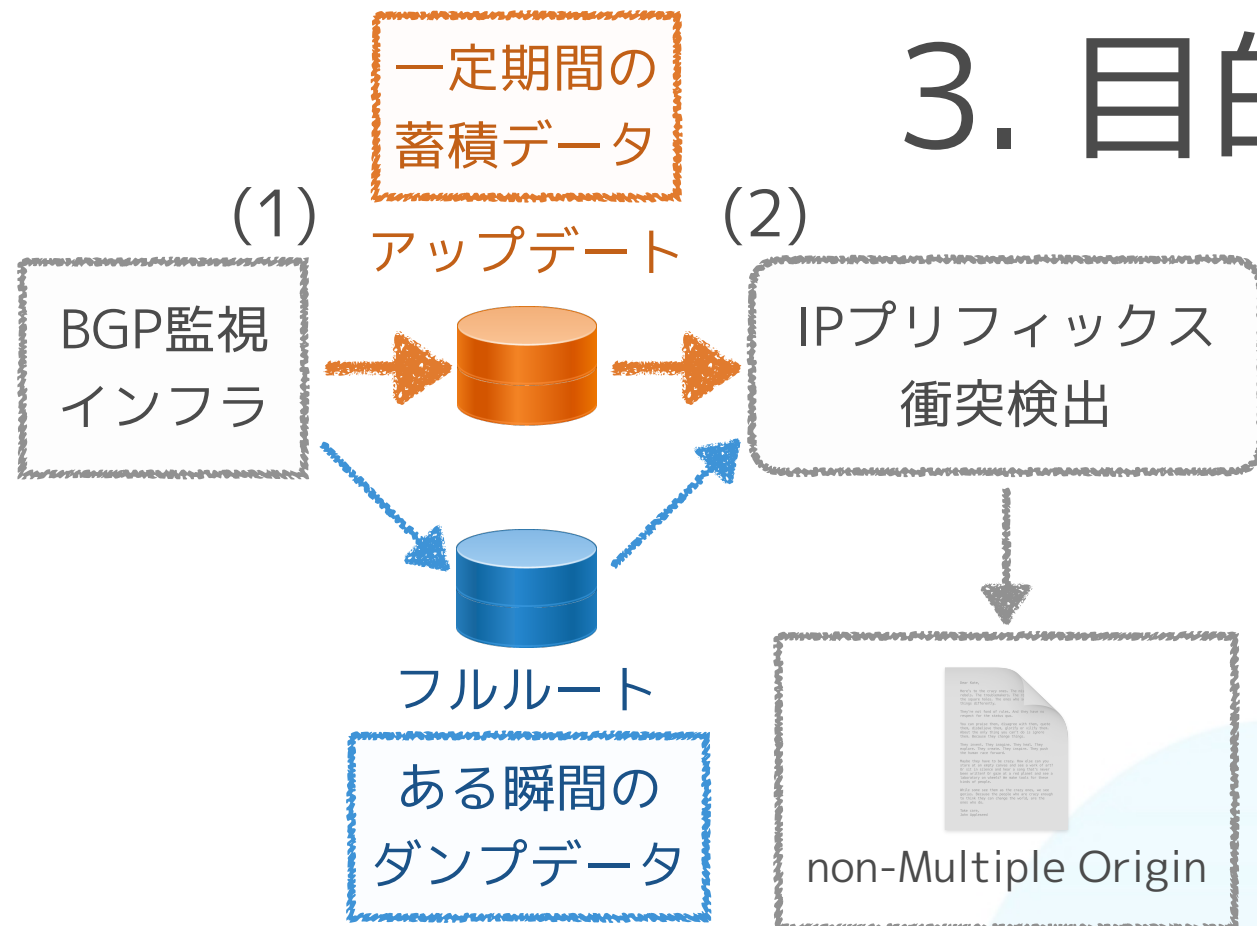
本研究：MOAI (Multiple Origin ASes Identification)

第三者視点のBGP観測データを用いた
広告元特徴を取り入れた分析による
ハイジャックの検出

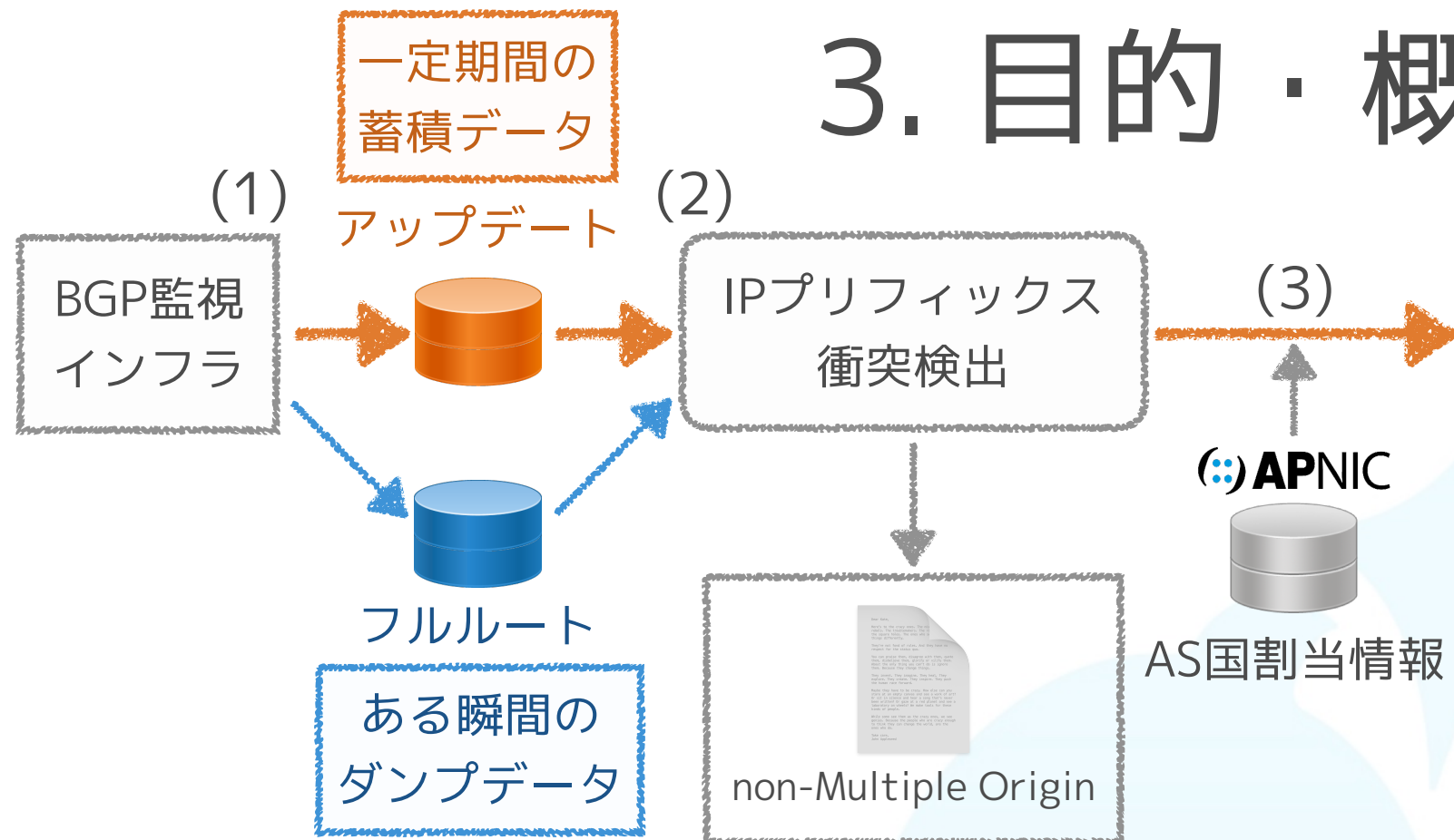
3. 目的・概要



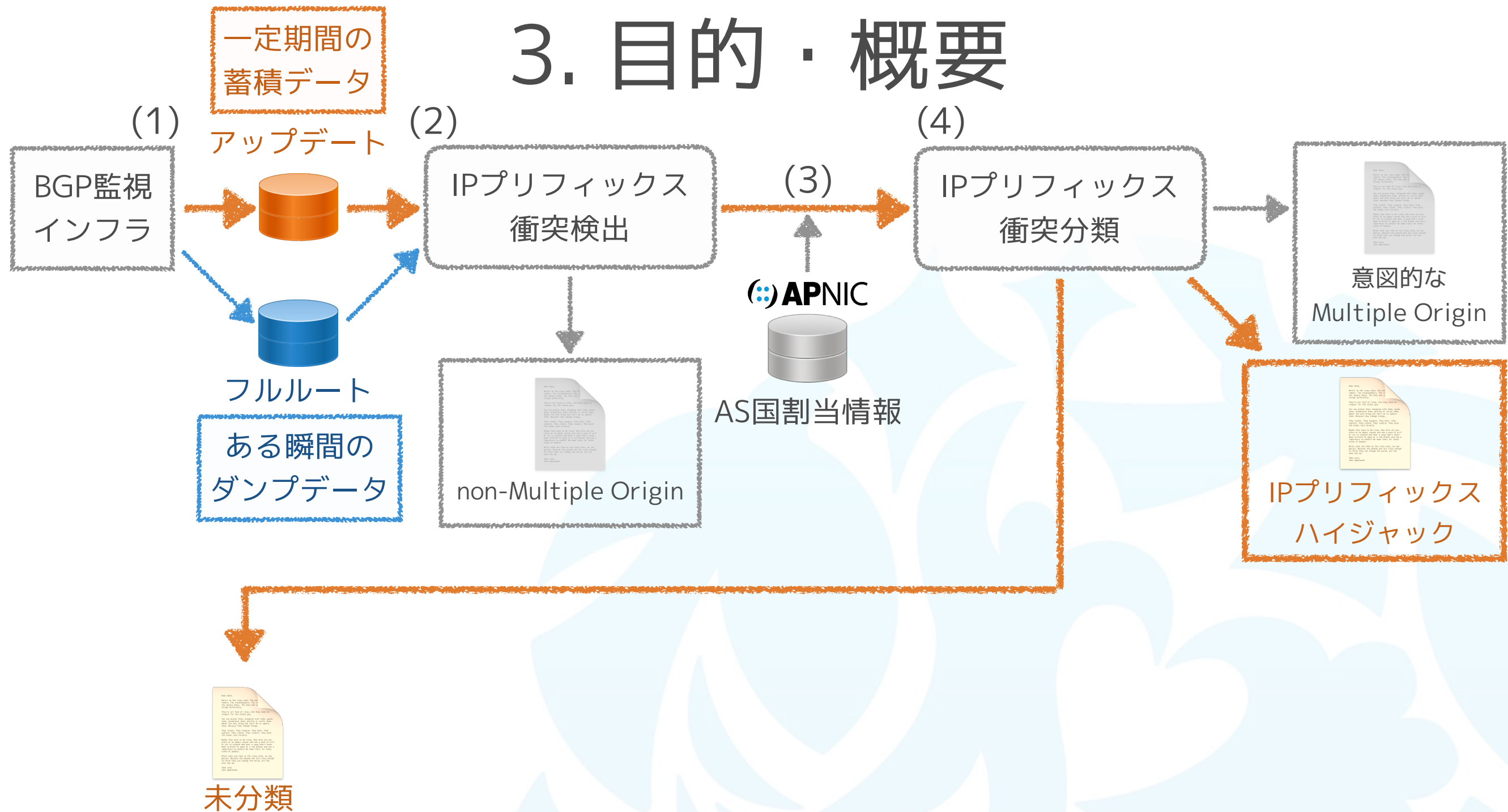
3. 目的・概要



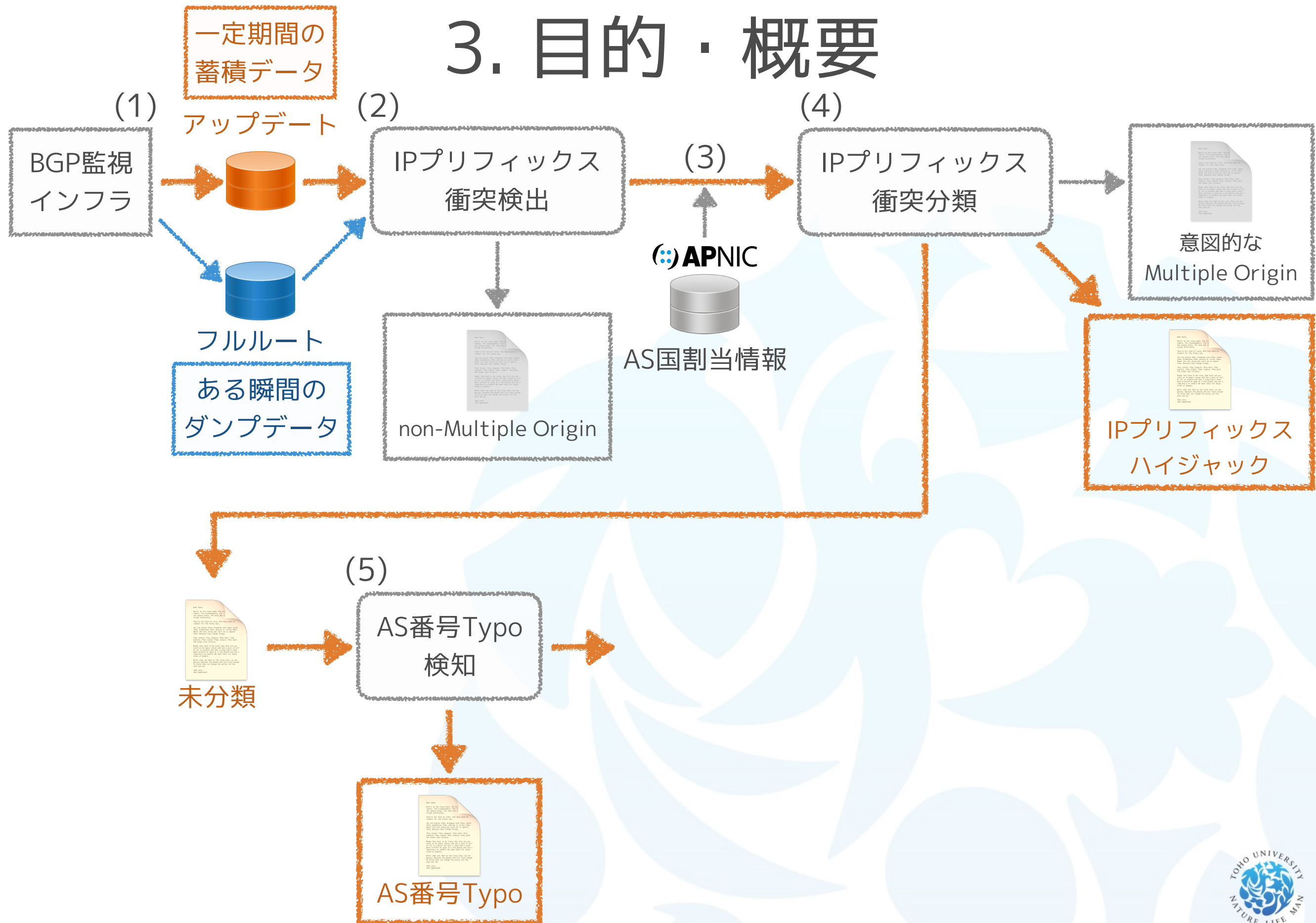
3. 目的・概要



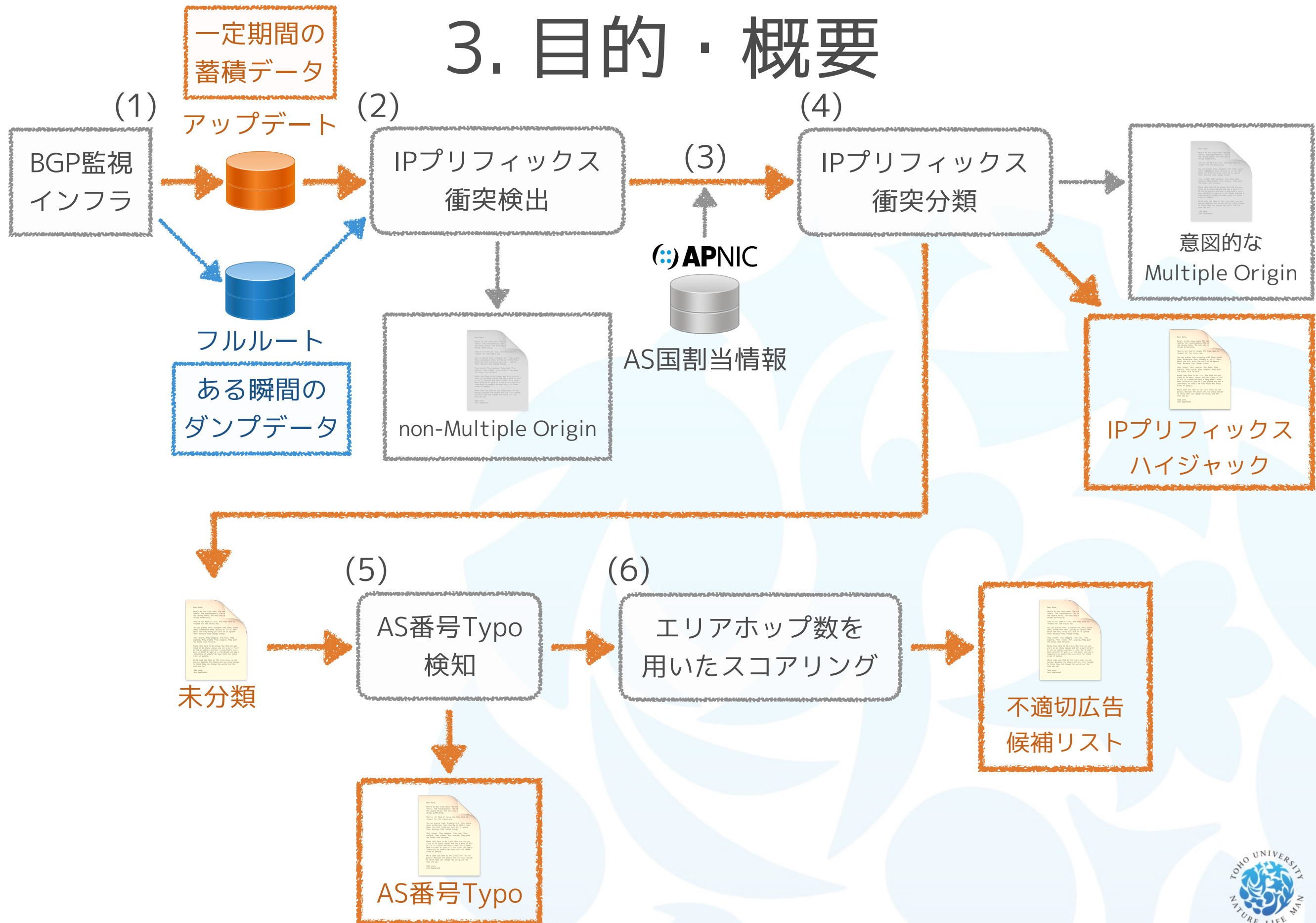
3. 目的・概要



3. 目的・概要



3. 目的・概要



4. 手法

- 経路情報の取得

- RIPE RIS

<https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris/ris-raw-data>

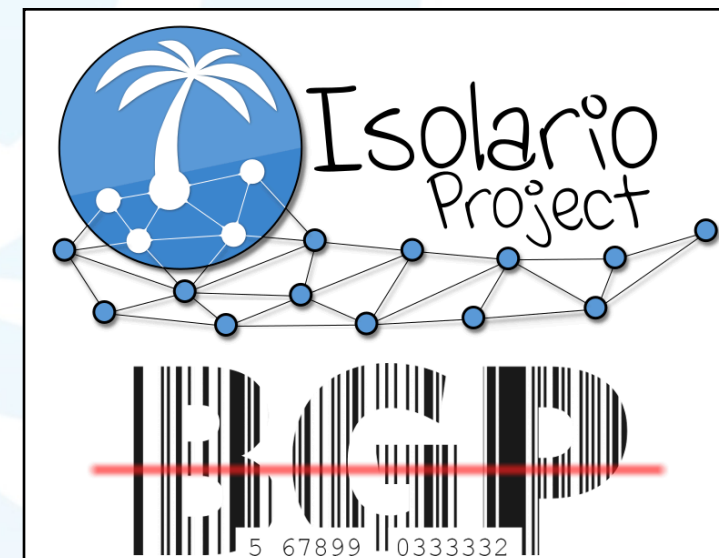
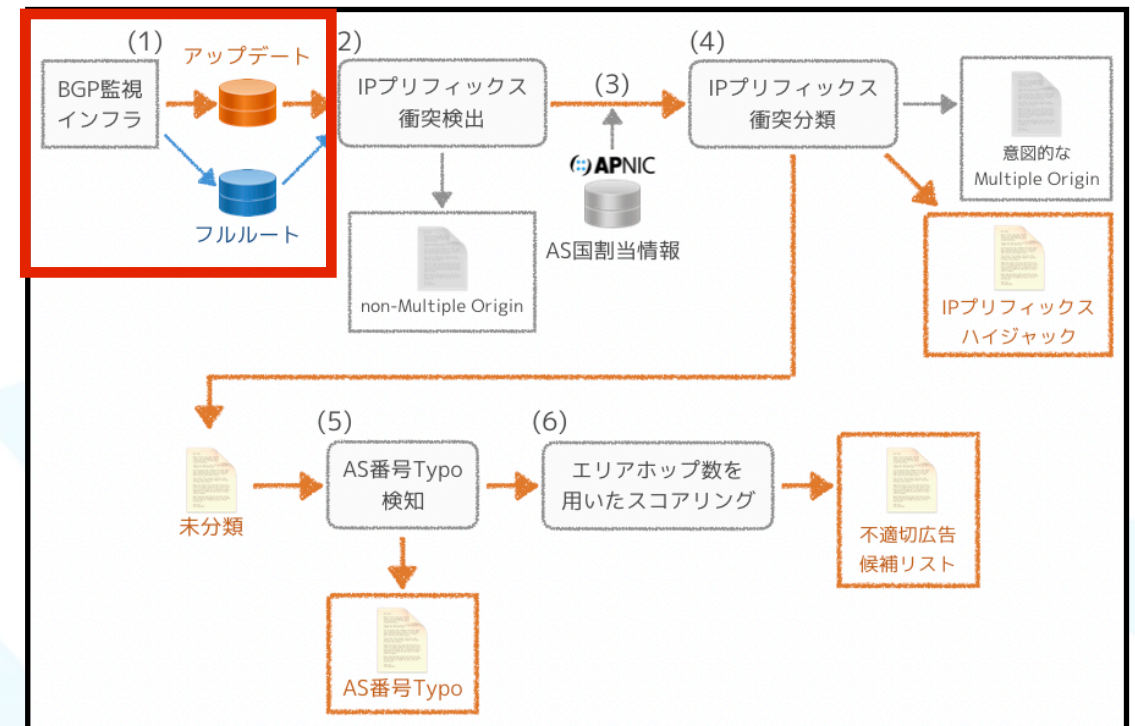
- Route Views

<http://archive.routeviews.org>

- 経路情報の変換

- bgpscannerを利用

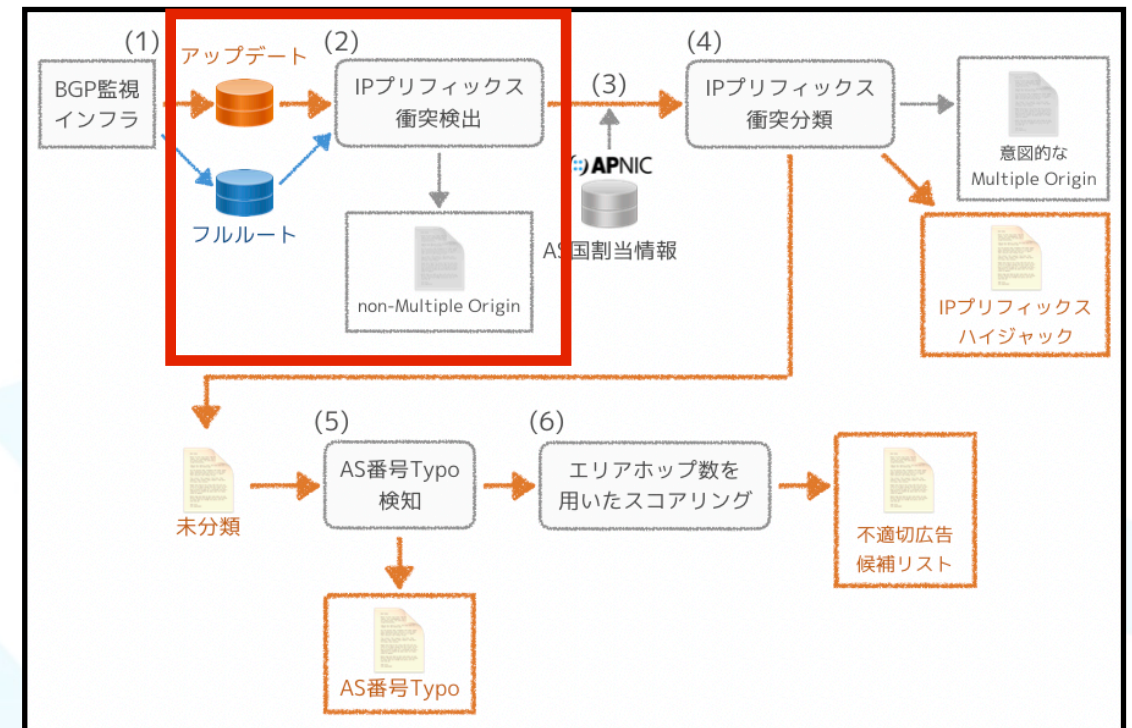
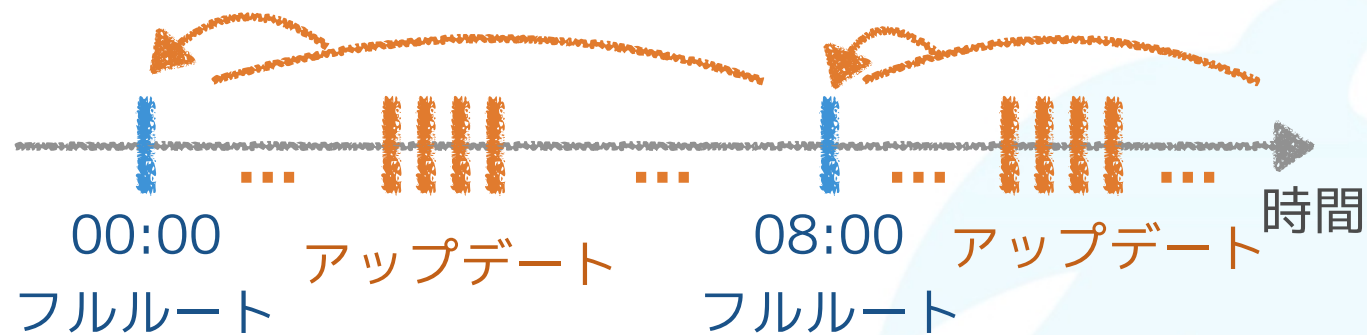
<https://gitlab.com/Isolario/bgpscanner>



4. 手法

• IPプリフィックス衝突検出

- 任意のアップデートに対し、その直前のフルルートと比較



IPプリフィックスが異なる

新規経路広告

IPプリフィックスが一致し、AS番号が一致

non-Multiple Origin

IPプリフィックスが一致し、AS番号が異なる

IP Prefix Hijackingの可能性

IPプリフィックスが含まれ、AS番号が一致

non-Multiple Origin

IPプリフィックスが含まれ、AS番号が異なる

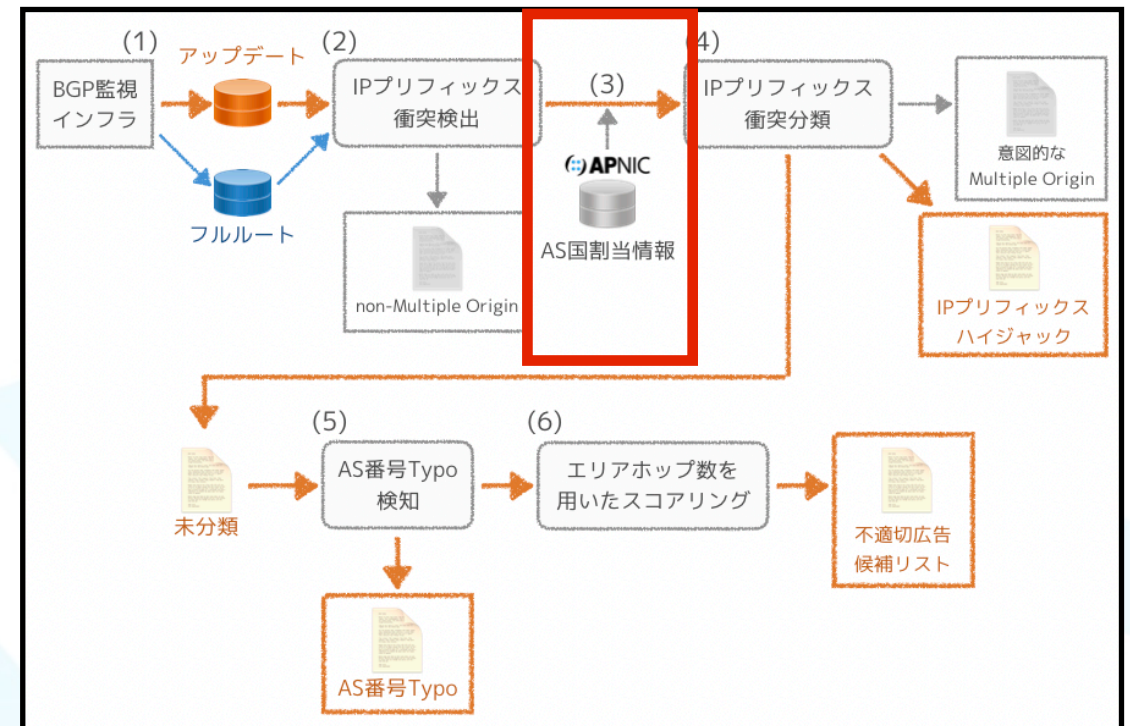
IP Prefix Hijackingの可能性

4. 手法

- 国情情報の付与

- APNICのWebページより
ASが属する国情情報を取得

<http://ftp.apnic.net/stats/>

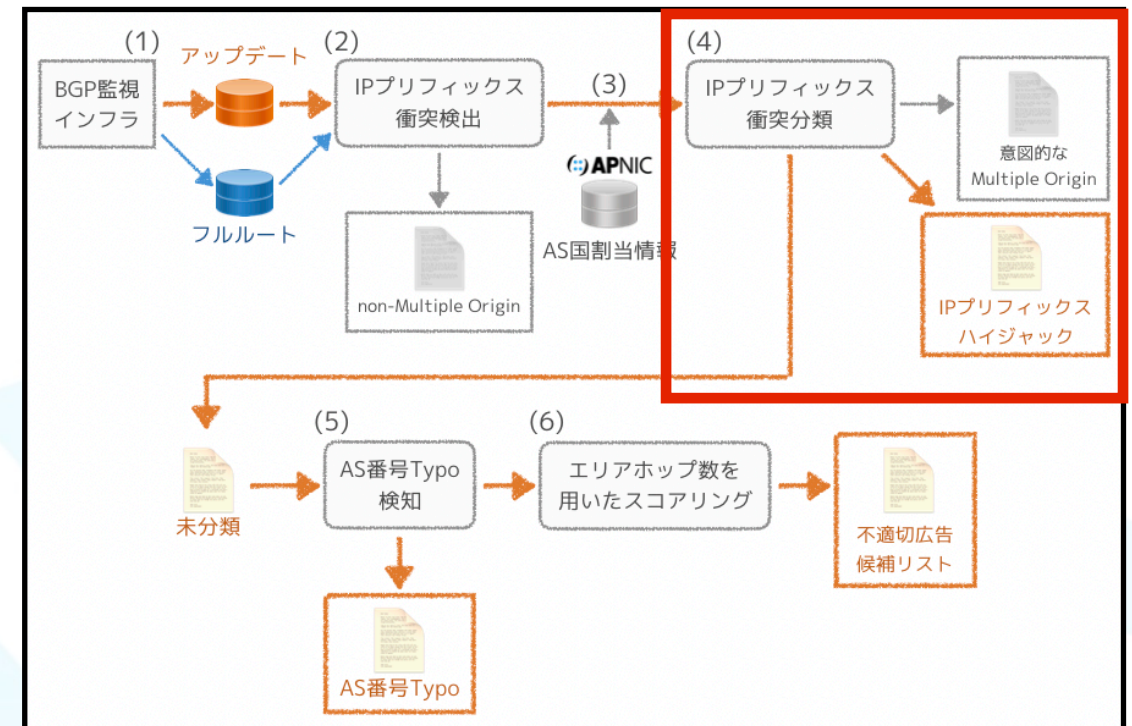


4. 手法

- 国情情報の付与

- APNICのWebページより
ASが属する国情情報を取得

<http://ftp.apnic.net/stats/>



- IPプリフィックス衝突分類

- AS番号と国コードに着目し，経路広告を18のConflict Type（CT）にヒューリスティックに分類
 - ・ 意図的なMultiple Originと思われる経路広告
 - ・ IPプリフィックスハイジャックと思われる経路広告

衝突タイプ（Conflict Type）分類

CT	説明	CT	説明
1	プライベートASN	10	DDoS軽減サービス（利用側）
2	同一国内の衝突	11	友好ASの衝突
3	地理的な隣接国	12	ハイジャックに対する防御
4	海底ケーブルでの隣接国	13	大学機関でのプロジェクト
5	MANRS参加AS	14	国によるブロッキング
6	同一組織の衝突	15	IPアドレスのリースサービス
7	CDNによる衝突	16	IANA予約済みASN
8	近隣国のAS	17	4bitASN（ASN：23456）
9	DDoS軽減サービス（提供側）	18	未割り当てASN

- **プライベートASN**
 - プライベートAS番号によりIPプリフィックスが衝突している経路
 - 不適切な経路だが，悪性はなく検出は不要
- **国内・隣接・近隣国での衝突**
 - 近い距離での衝突は顕在化しやすく，ハイジャックも発生しにくい
 - 検出の優先度は低い
- **MANRS参加AS・大学機関でのプロジェクト**
 - 信頼できるASによる衝突は意図的なものである可能性が高い
- **同一組織・友好ASによる衝突**
 - 同一組織間・友好AS間の衝突に悪性はないと考えられる
- **CDNによる衝突**
 - CDNの提供のための意図的な衝突と考えられる

- **DDoS軽減サービスに伴う衝突**

- DDoS軽減のためにサービス利用ASの持つIPプリフィックスを広告する
事があり, これに悪性は無い

- **ハイジャックに対する防御**

- ハイジャックへの防御のために衝突した経路広告をする事がある

- **国によるブロッキング**

- 国家機関によるブロッキングによる経路衝突は意図的なものである

- **IPアドレスのリースサービス**

- IPv4の枯渇に伴い, IPアドレスのリースサービスが登場している
- IPアドレスリースのための衝突は意図的なものである

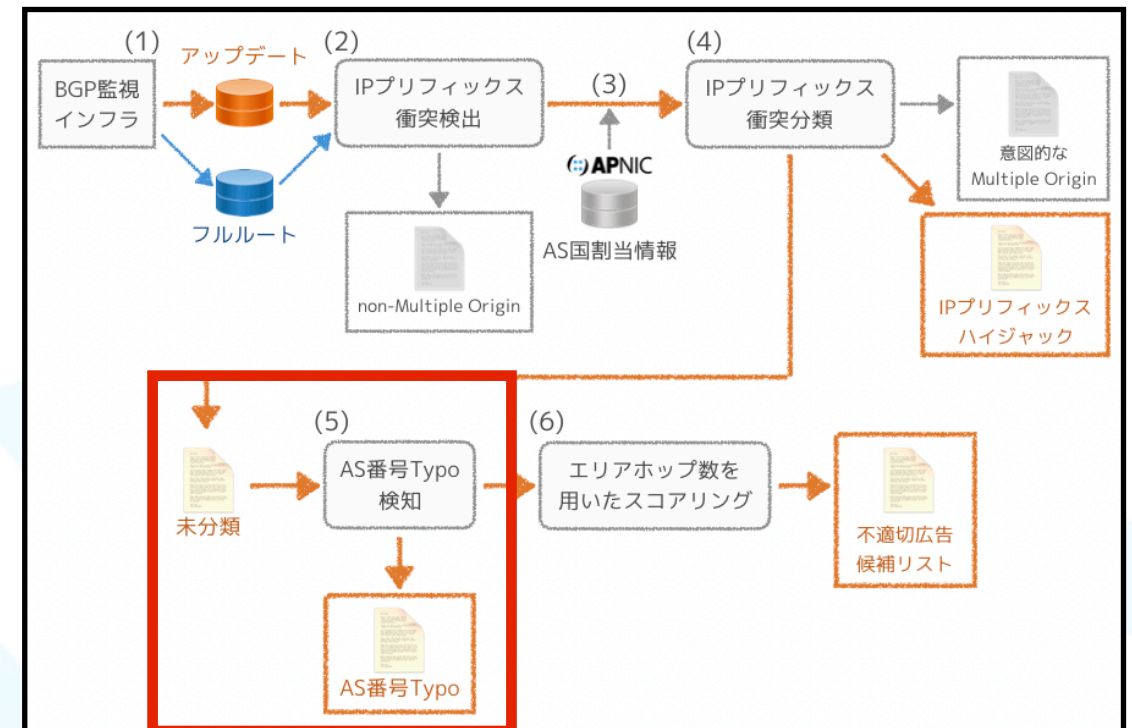
- **IANA予約済み・4bit ASN・未割り当てASN**

- これらのアドレスがOrigin ASとして広告されるのは不適切
- これらのアドレスによるIPプリフィックスの衝突はハイジャックである可能性が高い

4. 手法

- AS番号タイプミス検知

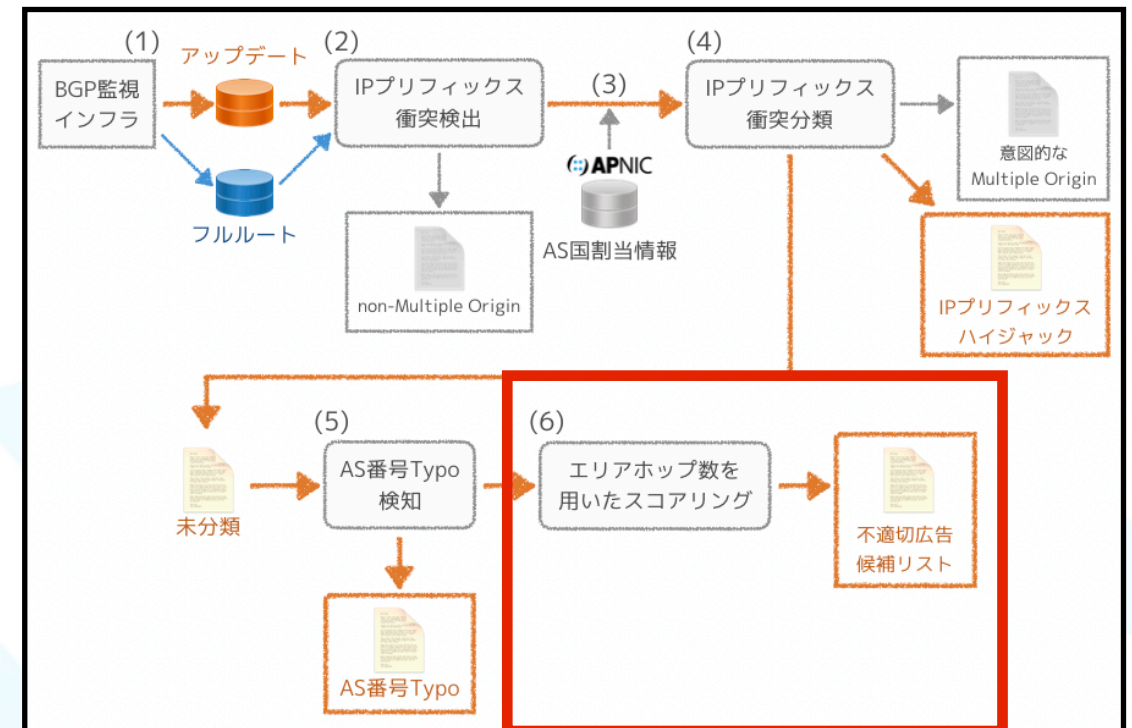
- レーベンシュタイン距離を元にしたタイプミスによる衝突を分類
 - ▶ キーボードでの隣接を閾値とする



4. 手法

• AS番号タイプミス検知

- レーベンシュタイン距離を元にしたタイプミスによる衝突を分類
 - ▶ キーボードでの隣接を閾値とする



• エリアホップ数を用いたスコアリング

- 不適切経路広告の候補リストに対し，エリアホップ数に基づくハイジャック可能性 $P(n)$ のスコアリングを行う

エリアホップ数	2	3	4	>5
ハイジャック可能性 $P(n)$	0.3	0.5	0.5	1

エリアホップ数による分類

エリアホップ数が2, 3, 4かつ未分類の経路情報50件をランダムに抽出し, 手動でConflictType分類を実施

※エリアホップ数>5の経路広告は十分な数のサンプルがなかった

エリアホップ数	2ホップ	%	3ホップ	%	4ホップ	%
ハイジャック可能性	15	<u>30.0</u>	25	<u>50.0</u>	25	<u>50.0</u>
ホワイトリスト	35	70.0	25	50.0	25	50.0

エリアホップ数が3以上の経路はホップ数が2の経路に比べ
ハイジャックの可能性が高い経路である傾向にある

5. フィルタリング効果の検証

- 検証のために取得したデータ

- 2018/01/01～2018/12/31
- ripe_rc00, ripe_rc01, routeviews_oregonのルートコレクタ
 - ▶ 3,284件のフルルート
 - ▶ 245,182件のアップデート

	ripe_rc00	ripe_rc01	routeviews	total
フルルート	1,095	1,095	1,094	3,284
アップデート	105,109	105,107	34,966	245,182
経路広告	2,460,825,619	924,620,092	1,769,249,121	5,154,694,834

のべ50億超の経路広告を取得

● 衝突検出

- アップデートに含まれる経路広告を，直前のフルルートと比較
- IPプリフィックスとAS番号に着目して5種類に分類

	ripe_rc00	%	ripe_rc01	%	routeviews	%	Total	%
新規経路	3,310,083	0.13	316,491	0.03	1,172,877	0.07	4,799,451	0.09
IP一致, AS一致	2,451,057,018	99.60	918,760,368	99.37	1,763,117,349	99.65	5,132,934,735	99.78
IP一致, AS相違	1,137,208	<u>0.05</u>	870,895	<u>0.09</u>	937,852	<u>0.05</u>	2,945,955	<u>0.06</u>
IP包含, AS一致	4,319,553	0.18	3,615,373	0.39	3,023,418	0.17	10,958,344	0.21
IP包含, AS相違	1,001,757	<u>0.04</u>	1,056,965	<u>0.11</u>	997,625	<u>0.06</u>	3,056,347	<u>0.06</u>

IPプリフィックスの衝突する（MultipleOrigin
である）経路広告は6,002,302 0.12%

• IPプリフィックス衝突分類 / AS番号Typo

- AS番号に着目して衝突経路広告を18のConflictTypeに分類
- レーベンシュタイン距離を元にしたAS番号のTypoを検知

	ripe_rc00	%	ripe_rc01	%	routeviews	%	total	%
CT1~15 ホワイトリスト	2,081,362	97.31	1,887,328	97.90	1,878,213	97.04	5,846,903	91.67
CT16~18 ブラックリスト	12,487	<u>0.58</u>	6,780	<u>0.35</u>	10,922	<u>0.56</u>	30,189	<u>0.50</u>
AS番号Typo	2,652	<u>0.12</u>	2,143	<u>0.11</u>	2,475	<u>0.13</u>	7,270	<u>0.12</u>
未分類	42,464	<u>1.99</u>	31,609	<u>1.64</u>	43,867	<u>2.27</u>	117,940	<u>1.96</u>

Multiple Originな経路広告6,002,302に対し

- ハイジャックである広告は37,459 (0.62% 全体の0.00073%)
- ハイジャックの可能性のある広告は117,940 (1.96% 全体の0.0023%)
- AS番号タイプミスによるMultipleOriginは7,270 (0.12% 全体の0.00014%)

CT		ripe_rc00	%	ripe_rc01	%	routeviews	%	total	%
1	プライベートASN	159,233	7.44	40,922	2.12	79,371	4.10	279,526	4.66
2	同一国内の衝突	1,672,844	78.21	1,657,946	86.00	1,293,414	66.8	4,624,204	77.04
3	地理的な隣接国	55,798	2.61	33,964	1.76	147,110	7.60	236,872	3.95
4	海底ケーブル隣接国	102,852	4.81	84,337	4.38	98,350	5.08	285,539	4.76
5	MANRS参加AS	11,622	0.54	3,880	0.20	6,053	0.31	21,555	0.36
6	同一組織の衝突	15,476	0.72	13,938	0.72	10,541	0.55	39,955	0.67
7	CDNによる衝突	11,785	0.55	8,127	0.42	16,787	0.87	36,699	0.61
8	近隣AS	20,918	0.98	15,539	0.81	17,924	0.93	54,381	0.91
9	DDoS軽減サービス（提供）	19,133	0.89	19,971	1.04	197,379	10.20	236,483	3.94
10	DDoS軽減サービス（利用）	3,671	0.17	2,791	0.15	3,148	0.16	9,610	0.16
11	友好AS	4	0.00	0	0	4	0.00	8	0.00
12	ハイジャック防御	106	0.01	273	0.01	75	0.00	454	0.01
13	大学機関でのプロジェクト	4,605	0.22	3,420	0.18	4,570	0.24	12,595	0.21
14	国によるブロッキング	162	0.01	33	0.00	1,041	0.05	1,236	0.02
15	IPアドレスリース	3,153	0.15	2,187	0.11	2,446	0.13	7,786	0.13
16	IANA予約済みASN	5,503	<u>0.26</u>	1,940	<u>0.10</u>	3,626	<u>0.19</u>	11,069	<u>0.18</u>
17	4bit ASN	189	<u>0.01</u>	4	<u>0.00</u>	38	<u>0.00</u>	231	<u>0.00</u>
18	未割り当てASN	6,795	<u>0.32</u>	4,836	<u>0.25</u>	7,258	<u>0.38</u>	18,889	<u>0.31</u>
-	AS番号Typo	2,652	<u>0.12</u>	2,143	<u>0.11</u>	2,475	<u>0.13</u>	7,270	<u>0.12</u>
-	未分類	42,464	<u>1.99</u>	31,609	<u>1.64</u>	43,867	<u>2.27</u>	117,940	<u>1.96</u>

• エリアホップ数を用いたスコアリング

- ConflictTypeが未分類・AS番号Typoでない経路広告に対し、
エリアホップ数を用いてハイジャック可能性 $P(n)$ をスコアリング

エリアホップ数	ripe_rc00	%	ripe_rc01	%	routeviews	%	total	%
2 ($P(2) = 0.3$)	25,455	59.94	19,033	61.30	27,809	63.39	72,297	61.30
3 ($P(3) = 0.5$)	10,692	25.18	6,783	21.40	7,770	17.71	25,245	21.40
4 ($P(4) = 0.5$)	850	2.00	643	1.91	758	1.73	2,251	1.91
>5 ($P(n) = 1$)	0	0	0	0	0	0	0	0
不明	2,204	7.68	1,876	10.23	2,006	12.59	6,086	5.16
EU	3,263	5.19	3,274	5.16	5,524	4.57	12,061	10.23

EU：AS割当国が“EU”であり，エリアホップ数の算出ができないもの

実例：同一国・隣接国

asn	conf_asn	asn_cc	conflict_asn_cc	date_detection	prefix_set_count	update_count
47331	9121	TR	TR	2019-04-01 05:38:07	46133	355178
12357	12430	ES	ES	2019-04-08 01:20:04	22105	63813
9121	47331	TR	TR	2019-04-08 01:32:07	20025	213188
12479	12715	ES	ES	2019-04-01 05:32:52	8292	259955
7713	17974	ID	ID	2019-04-01 05:31:59	6149	47571
7470	17552	TH	TH	2019-04-01 07:43:30	5777	18729
13979	4152	US	US	2019-04-01 16:41:43	5230	5230
33650	7922	US	US	2019-04-05 10:52:15	5074	5195
16625	35994	US	US	2019-04-01 05:31:57	4550	117369
33387	32097	US	US	2019-04-01 05:39:40	3938	4405
134705	134548	HK	HK	2019-04-04 16:23:16	3130	19690
4323	3549	US	US	2019-04-01 05:34:37	3117	10476
327693	37611	ZA	ZA	2019-04-01 05:31:59	2963	19342
1536	4010	US	US	2019-04-01 05:45:56	2885	30849
12357	6739	ES	ES	2019-04-01 05:32:52	2793	8597
58224	12880	IR	IR	2019-03-31 21:19:46	2714	56592
38733	18403	VN	VN	2019-04-06 10:28:23	2706	3807
10620	14080	CO	CO	2019-04-01 05:31:58	2654	8723
22884	17072	MX	MX	2019-04-01 05:32:52	2382	6435
14080	10620	CO	CO	2019-04-01 05:32:41	2287	11240
5972	721	US	US	2019-04-01 05:31:57	2254	18264
38733	45899	VN	VN	2019-04-06 10:28:23	2177	2735
10036	9943	KR	KR	2019-07-04 14:45:17	2163	8865
1541	721	US	US	2019-03-31 21:19:46	2056	59422
38370	9394	CN	CN	2019-04-02 13:30:16	1929	25083
32708	35916	US	US	2019-04-02 02:52:04	1895	7528
3549	3356	US	US	2019-04-01 05:32:41	1886	7564
11664	19037	AR	AR	2019-04-01 05:31:57	1801	9623
10429	18881	BR	BR	2019-04-07 04:55:50	1773	14135
26484	35916	US	US	2019-04-01 16:36:53	1682	7110
28118	12066	DO	DO	2019-03-31 21:19:46	1661	11629
4538	23910	CN	CN	2019-04-01 05:46:21	1657	11236
15557	8228	FR	FR	2019-04-06 10:40:34	1635	7625
12741	8374	PL	PL	2019-06-05 09:40:08	1591	2034
27046	721	US	US	2019-04-01 05:31:57	1528	21734
22394	6167	US	US	2019-04-01 05:31:58	1506	12766
3269	20959	IT	IT	2019-04-01 16:38:23	1487	5867
9808	9394	CN	CN	2019-07-05 03:09:45	1455	19028
10318	10481	AR	AR	2019-04-02 02:46:40	1443	18124
385	721	US	US	2019-04-01 05:31:58	1342	12697

asn	conf_asn	asn_cc	conflict_asn_cc	date_detection	prefix_set_count	update_count
55649	4134	HK	CN	2019-05-30 21:47:20	20534	63859
133731	55933	CN	HK	2019-04-01 05:38:21	2321	16286
38001	131297	SG	MY	2019-04-02 02:52:04	1993	10186
137443	58879	HK	CN	2019-04-04 16:09:00	1555	5114
58879	137443	CN	HK	2019-04-05 11:06:51	1369	3447
5511	12479	FR	ES	2019-07-29 05:40:02	1160	1160
19905	15128	US	CA	2019-04-03 00:45:09	900	11423
55649	4837	HK	CN	2019-05-30 21:47:35	784	4456
262589	18678	BR	CO	2019-04-01 05:40:23	576	5327
55933	133731	HK	CN	2019-04-01 07:41:41	555	2748
56082	9535	HK	CN	2019-04-02 13:31:25	410	2330
3257	5580	DE	NL	2019-04-01 05:47:17	366	602
9535	56082	CN	HK	2019-04-03 00:37:06	356	1202
64021	132422	CN	HK	2019-07-04 14:36:27	347	3042
133731	55933, 134196	CN	HK, HK	2019-07-28 16:37:43	304	1342
135357	134548	CN	HK	2019-04-07 04:55:58	287	995
48666	51150	RU	NO	2019-07-05 16:29:19	251	4106
36352	55286	US	CA	2019-04-01 05:40:42	248	602
133731	134196, 55933	CN	HK, HK	2019-07-25 20:11:56	244	1066
12389	202053	RU	FI	2019-06-05 10:12:24	242	21343
135377	59077	HK	CN	2019-04-03 12:29:38	219	765
15399	37027	KE	TZ	2019-04-01 16:38:16	205	2210
397796	393504	US	CA	2019-08-04 02:23:01	192	288
37440	37133	MW	TZ	2019-04-01 05:45:22	178	998
6830	29562	AT	DE	2019-07-05 16:27:34	176	522
137280	59019	HK	CN	2019-04-01 07:44:31	167	633
55649	4538	HK	CN	2019-05-30 21:47:11	163	760
17488	4134	IN	CN	2019-04-01 05:34:22	153	309
37440	37287	MW	ZM	2019-04-01 05:32:42	147	1813
55649	4809	HK	CN	2019-05-30 21:47:20	145	467
135663	55933	CN	HK	2019-04-02 02:46:25	139	370
52340	53240	BO	BR	2019-04-01 07:40:09	135	1506
5580	3257	NL	DE	2019-06-03 14:45:56	134	472
12552	50608	SE	NO	2019-04-01 16:45:07	125	241
134196	133731	HK	CN	2019-07-06 10:51:09	120	992
2119	39651	NO	SE	2019-07-05 16:32:11	117	146
58879	132839	CN	HK	2019-04-06 10:31:22	114	551
57101	61153	PL	DE	2019-04-02 13:31:30	114	207
12127	13682	SV	GT	2019-04-01 16:38:23	110	354
38001	9542	SG	MY	2019-04-03 12:25:00	105	105

実例：同一組織・大学機関

asn	conf_asn	asn_cc	conflict_asn_cc	asn_whois	conflict_asn_whois	date_detection	prefix_set_count	update_count
61317	61440	GB	CL	Digital Energy Technologies Ltd.	Digital Energy Technologies Chile SpA	2019-04-01 16:39:46	1013	7529
20940	34164	EU	GB	Akamai International B.V.	Akamai International B.V.	2019-04-01 05:31:57	709	4398
781	2200	EU	FR	Renater	Renater	2019-04-01 16:44:39	245	271
136162	206819	HK	GB	ANSON NETWORK LIMITED	ANSON NETWORK LIMITED	2019-04-01 07:44:40	203	2878
41264	36384	CH	US	Google Switzerland GmbH	Google LLC	2019-04-01 05:38:07	202	2007
198148	3491	BE	US	Gateway Communications	PCCW Global, Inc.	2019-04-03 12:35:54	193	2015
38226	38266	HK	IN	Hutchison GlobalCenter Limited	Hutchison Max Telecom Limited	2019-04-04 16:23:46	192	2116
61440	61317	CL	GB	Digital Energy Technologies Chile SpA	Digital Energy Technologies Ltd.	2019-04-01 16:41:45	181	930
61317	37692	GB	ZA	Digital Energy Technologies Ltd.	NetStack Ltd	2019-04-03 00:45:03	107	227
133296	33480	IN	US	WEBWERKS-AS-IN	Web Werks	2019-04-01 16:36:31	100	287
132721	64013	NL	HK	PING GLOBAL LIMITED	PING GLOBAL LIMITED	2019-04-06 10:41:33	99	1750
58272	56495	NL	RU	LeaderTelecom B.V.	LeaderTelecom Ltd.	2019-04-02 02:51:51	96	369
37553	62135	SC	NL	Inspiring Networks LTD	Inspiring Networks BV	2019-04-07 04:56:30	96	128
206819	136162	GB	HK	ANSON NETWORK LIMITED	ANSON NETWORK LIMITED	2019-04-03 00:45:43	79	233
35900	33576	BB	JM	Digicel Barbados Ltd	Digicel Jamaica	2019-04-01 16:39:46	78	207
44828	52055	DE	BG	Mayak Smart Services Ltd.	Mayak Smart Services Ltd.	2019-04-02 13:32:00	67	96

asn	conf_asn	asn_cc	conflict_asn_cc	asn_whois	conflict_asn_whois	date_detection	prefix_set_count	update_count
2	6697	US	BY	-	-	2019-06-04 17:31:22	281	281
3	23682	US	IN	Massachusetts Institute of Technology	PACENET-AS	2019-03-31 21:19:46	195	322
3	17488	US	IN	-	-	2019-07-06 23:26:17	181	1530
2	21412	US	LT	University of Delaware	UAB "Cgates"	2019-04-05 10:51:19	112	193
4	18196	US	IN	University of Southern California	7 STAR DOT COM Pvt. Ltd	2019-04-01 05:38:21	81	259
2	134884	US	IN	University of Delaware	AISPL-AS	2019-04-04 16:23:16	34	170
3	57248	US	SK	Massachusetts Institute of Technology	Wisper s.r.o.	2019-04-02 02:46:32	32	175
3	134294	US	IN	-	-	2019-07-05 16:19:15	30	98
2	204213	US	IR	-	-	2019-07-04 14:40:16	30	64
3	134884	US	IN	Massachusetts Institute of Technology	AISPL-AS	2019-04-04 16:23:16	29	75
3	133676	US	IN	Massachusetts Institute of Technology	PNPL-AS	2019-04-01 16:36:57	29	178
4	43391	US	TR	University of Southern California	Netdirekt A.S.	2019-04-06 10:33:02	27	27
2	43391	US	TR	University of Delaware	Netdirekt A.S.	2019-04-06 10:33:02	27	27
2	37140	US	GH	-	-	2019-07-05 03:14:46	27	905
3	44208	US	IR	-	-	2019-07-05 03:18:27	24	24
3	135125	US	BD	Massachusetts Institute of Technology	Talmuri Computer System	2019-04-01 05:40:42	24	366
3	135341	US	BD	Massachusetts Institute of Technology	Brosis Communications	2019-04-03 00:38:03	24	147
2	135853	US	IN	University of Delaware	CRAZYNET-AS	2019-04-02 02:46:34	24	374
3	134552	US	BD	Massachusetts Institute of Technology	Geotel Bangladesh IT Ltd.	2019-04-01 05:32:42	23	218

実例：同一組織・大学機関

asn	conf_asn	asn_cc	conflict_asn_cc	asn_whois	conflict_asn_whois	date_detection	prefix_set_count	update_count
61317	61440	GB		Digital Energy Technologies Ltd.	Digital Energy Technologies Ltd.	2019-04-01 16:39:46	1013	7529
20940	34164	EU		Akamai International B.V.	Akamai International B.V.	2019-04-01 05:31:57	709	4398
781	2200	EU		Renater	Renater	2019-04-01 16:44:39	245	271
136162	206819	HK	GB	ANSON NETWORK LIMITED	ANSON NETWORK LIMITED	2019-04-01 07:44:40	203	2878
41264	36384			Digital Energy Technologies Ltd.	Digital Energy Technologies Chile SpA	2019-04-01 05:38:07	202	2007
198148	3491			Akamai International B.V.	Akamai International B.V.	2019-04-03 12:35:54	193	2015
38226	38266			Renater	Renater	2019-04-04 16:23:46	192	2116
61440	61317			ANSON NETWORK LIMITED	ANSON NETWORK LIMITED	2019-04-01 16:41:45	181	930
61317	37692			Google Switzerland GmbH	Google LLC	2019-04-03 00:45:03	107	227
133296	33480					2019-04-01 16:36:31	100	287
132721	64013					2019-04-06 10:41:33	99	1750
58272	56495					2019-04-02 02:51:51	96	369
37553	62135					2019-04-07 04:56:30	96	128
206819	136162					2019-04-03 00:45:43	79	233
35900	33576	BB	JM	Digicel Barbados Ltd	Digicel Jamaica	2019-04-01 16:39:46	78	207
44828	52055	DE	BG	Mayak Smart Services Ltd.	Mayak Smart Services Ltd.	2019-04-02 13:32:00	67	96

広告側

被広告側

asn	conf_asn	asn_cc	conflict_asn_cc	asn_whois	conflict_asn_whois	date_detection	prefix_set_count	update_count
2	6697	US		Massachusetts Institute of Technology	PACENET-AS	2019-06-04 17:31:22	281	281
3	23682	US		University of Delaware	UAB "Cgates"	2019-03-31 21:19:46	195	322
3	17488	US		University of Southern California	7 STAR DOT COM Pvt. Ltd	2019-07-06 23:26:17	181	1530
2	21412			University of Delaware	AISPL-AS	2019-04-05 10:51:19	112	193
4	18196			Massachusetts Institute of Technology	Wisper s.r.o.	2019-04-01 05:38:21	81	259
2	134884					2019-04-04 16:23:16	34	170
3	57248					2019-04-02 02:46:32	32	175
3	134294					2019-07-05 16:19:15	30	98
2	204213					2019-07-04 14:40:16	30	64
3	134884					2019-04-04 16:23:16	29	75
3	133676					2019-04-01 16:36:57	29	178
4	43391					2019-04-06 10:33:02	27	27
2	43391					2019-04-06 10:33:02	27	27
2	37140					2019-07-05 03:14:46	27	905
3	44208					2019-07-05 03:18:27	24	24
3	135125					2019-04-01 05:40:42	24	366
3	135341					2019-04-03 00:38:03	24	147
2	135853					2019-04-02 02:46:34	24	374
3	134552	US	BD	Geotek Bangladesh IT Ltd.		2019-04-01 05:32:42	23	218

広告側

被広告側

実例：typo

asn	conf_asn	asn_cc	conflict_asn_cc	asn_whois	conflict_asn_whois
136716	13716	IN	US	APPLEBB-AS	Alight Solutions LLC
3760	37605	US	NG	Texas Department of Agriculture	General Telecommunication Networks Limited
48900	48990	BG	ES	Info Data Center Ltd.	ATALAYA DE TELEVISION SL
261903	262903	unknown	BR	unknown	unknown
134552	13455	BD	US	Geotel Bangladesh IT Ltd.	Reach Marketing LLC
13455	134552	US	BD	Reach Marketing LLC	Geotel Bangladesh IT Ltd.
5563	55636	RU	KH	CJSC Ural WES	TPLC Holdings Ltd
37605	3760	NG	US	General Telecommunication Networks Limited	Texas Department of Agriculture
39334	393341	EE	US	EuroIir OU	Spokane County - Information Systems Department
410007	41007	unknown	KZ	unknown	CTC ASTANA LTD
6139	61390	US	RU	Washington Coordinating Center	Garant-G Ltd.
4596	45916	US	IN	Bank of America	GTPL-AS-AP
7981	17981	US	KH	DigiMark	Cambo Technology Company Ltd.
55636	5563	KH	RU	TPLC Holdings Ltd	CJSC Ural WES
242220	24220	unknown	AU	unknown	Illuminate Internet Services Pty Ltd
1234	12348	EU	DE	FORTUM-AS	ODN OnlineDienst Nordbayern GmbH & Co. KG
4247	42478	US	RU	CAPCON Library Network	"Yug-Link" Ltd.
3974729	394729	unknown	US	unknown	NeoPollard Interactive LLC
56699	55699	RU	ID	GUP NAO Neneckaya kompaniya electrosvyazi	STARNET-AS-ID
1007	10074	CA	SG	GONET	iBasis (Hong Kong) Ltd
135133	35133	IN	unknown	PI DATA CENTERS PRIVATE LIMITED	unknown
35133	135133	unknown	IN	unknown	PI DATA CENTERS PRIVATE LIMITED
1333301	133301	unknown	IN	unknown	DWANIRINN-AS
254589	264589	unknown	BR	unknown	E L DA SILVA SERVIÇOS DE REDES E COMUNICAÇÕES ME
60886	60885	IL	GB	Amit Net Telecom LTD	Zengenti Ltd.
5713	6713	ZA	MA	Telkom SA Ltd.	Office National des Postes et Telecommunications ONPT (Maroc Telecom) , IAM
227171	22717	unknown	US	unknown	Halliburton Company
205800	205801	IQ	FR	Steps Telecom For Internet Ltd.	Synalabs SARL
205801	205800	FR	IQ	Synalabs SARL	Steps Telecom For Internet Ltd.

実例：typo

広告側		被広告側	cc	asn_whois	conflict_asn_whois
3760	37605			APPLEBB-AS	Alight Solutions LLC
48900	48900	55636	5563	Texas Department of Agriculture	General Telecommunication Networks Limited
261903	261903			Info Data Center Ltd.	ATALAYA DE TELEVISION SL
134552	134552	242220	24220	unknown	unknown
13455	13455			Geotel Bangladesh IT Ltd.	Reach Marketing LLC
5563	5563	1234	12348	Reach Marketing LLC	Geotel Bangladesh IT Ltd.
37605	37605	4247	42478	CJSC Ural WES	TPLC Holdings Ltd
39334	39334	3974729	394729	General Telecommunication Networks Limited	Texas Department of Agriculture
410007	410007			Eurofir OU	Spokane County - Information Systems Department
6139	6139			unknown	CTC ASTANA LTD
4596	4596	56699	55699	Washington Coordinating Center	Garant-G Ltd.
7981	7981			Bank of America	GTPL-AS-AP
55636	55636	1007	10074	DigiMark	Cambo Technology Company Ltd.
242220	242220			TPLC Holdings Ltd	CJSC Ural WES
1234	1234	135133	35133	unknown	Illuminate Internet Services Pty Ltd
4247	4247	35133	135133	FORTUM-AS	ODN OnlineDienst Nordbayern GmbH & Co. KG
3974729	3974729			CAPCON Library Network	"Yug-Link" Ltd.
56699	56699	1333301	133301	unknown	NeoPollard Interactive LLC
1007	1007	254589	264589	GUP NAO Neneckaya kompaniya electrosvyazi	STARNET-AS-ID
135133	135133	60886	60885	GONET	iBasis (Hong Kong) Ltd
35133	35133			PI DATA CENTERS PRIVATE LIMITED	unknown
1333301	1333301			unknown	PI DATA CENTERS PRIVATE LIMITED
254589	254589	5713	6713	unknown	DWANIRINN-AS
60886	60886			unknown	E L DA SILVA SERVIÇOS DE REDES E COMUNICAÇÕES ME
5713	5713	227171	22717	Amit Net Telecom LTD	Zengenti Ltd.
227171	227171			Telkom SA Ltd.	Office National des Postes et Telecommunications ONPT (Maroc Telecom) , IAM
205800	205800	205800	205801	unknown	Halliburton Company
205801	205801			Steps Telecom For Internet Ltd.	Synalabs SARL
		205801	205800	Synalabs SARL	Steps Telecom For Internet Ltd.

フィルタリング効果の検証まとめ

2018/01/01～2018/12/31までのアップデートより、
のべ50億超の経路広告を取得

50億

経路広告に対するIPプリフィックス衝突検出の結果、
Multiple Originである経路広告は6,002,302 (0.12%)

0.12%

さらにIPプリフィックス衝突分類の結果、IPプリフィックス
ハイジャックの可能性のある経路広告は155,399 (2.59%)

2.59%

6. 評価

- フィルタリング効果

	MultipleOrigin である経路広告		ハイジャック可能性 のある経路広告
Huらの手法	7,065	→	483 (6.84%)
本手法	6,002,302	→	155,399 (<u>2.59%</u>)

- パフォーマンス

Ubuntu 18.04 / Intel Core i7-4770 / 32GB RAM / php7.2

- アップデートの取得から加工, 分類, 検知までおよそ3~10秒
- ルートコレクタごとに並列に処理できる
 - ▶ ルートコレクタの数を増加させても検知時間は変わらない

• 実インシデントによる評価

BitCanalによるハイジャック：～2018/07

AS3266/197426/200755が19種のIPプリフィックスをハイジャック

- CT2（同一国内）：1
- CT3（隣接エリア）：1
- CT4（海底ケーブルによる隣接エリア）：9
- 未分類（ハイジャック可能性）：8

ホワイトリスト

Taiwan Public DNSのハイジャック：2019/05/08

AS268869がAS36925の2種のIPプリフィックスをハイジャック

- 2種いずれも未分類（ハイジャック可能性）であり、
エリアホップ数は2であった

- 実インシデントによる評価

E

A

近隣国でのハイジャック：検知が困難

近隣国でのハイジャックは被害が顕在化
しやすく 検知の優先度は低い

ク

それ以外のハイジャック：検知可能

本手法では他の手法による

検出の難しいハイジャックの迅速な検知を実現

T

A

エリアホップ数は2であった

7. 今後の課題

隣接によるフィルタ

隣接地域のハイジャックに対応する，より詳細なフィルタリングが必要

ASハイジャックへの対応

本研究はIPプリフィックスハイジャックに焦点を当てているが，別種のASハイジャックというものも存在する

データソースの拡充

- ・ 対象ルートコレクタの増加による分析データの充実化
- ・ ヒューリスティックホワイトリスト作成の効率化

検出精度の評価・精度向上

第三者データでは，ハイジャック検出の正誤判定ができない
→被衝突経路広告ASにヒアリングを実施したいと考えている

ヒアリングへのご協力をよろしくお願いします！

8. まとめ

目的

第三者視点から任意の時間の任意の不適切広告を検出する

成果

延べ50億超の経路広告から、IP Prefix Hijackingの可能性のある経路広告を155,399件まで絞り込んだ

課題

隣接フィルタ, ASハイジャック対応, データソース拡充, 検出精度

総括

他の手法で検知することが難しいハイジャックの検知を実現できた一方, まだまだ精度改善の余地がある. 他の複数の手法と共に利用することで精度の高いハイジャックの検出ができるだろう

議論したいポイント

- **意図的なMultipleOriginの広告をする/される理由って他にどんなケースがある？**
 - 生データを眺めながら、ヒューリスティックに18種に分類した
 - 他にもホワイト・ブラックリストにできるものがあれば教えて欲しい
- **このシステムはどうすれば実運用に役立つと思う？**
 - インターフェースがまだできていない
 - WebやTwitterでのアラート, Slackチャンネルの作成などを検討
 - 他にも運用側の視点で改善点などあれば教えて欲しい
- **その他質問・意見等あれば何でも**

議論したいポイント

1	プライベートASN	10	DDoS軽減サービス（利用側）
2	同一国内の衝突	11	友好ASの衝突
3	地理的な隣接国	12	ハイジャックに対する防御
4	海底ケーブルでの隣接国	13	大学機関でのプロジェクト
5	MANRS参加AS	14	国によるブロッキング
6	同一組織の衝突	15	IPアドレスのリースサービス
7	CDNによる衝突	16	IANA予約済みASN
8	近隣国のAS	17	4bitASN（ASN：23456）
9	DDoS軽減サービス（提供側）	18	未割り当てASN

- 意図的なMultipleOriginの広告をする/される理由って他にどんなケースがある？
- このシステムはどうすれば実運用に役立つと思う？
- その他質問・意見等あれば何でも