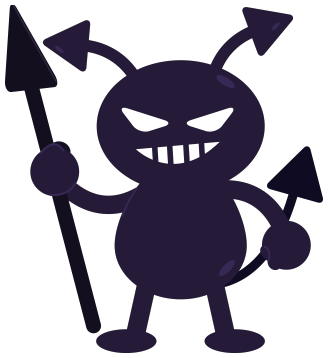
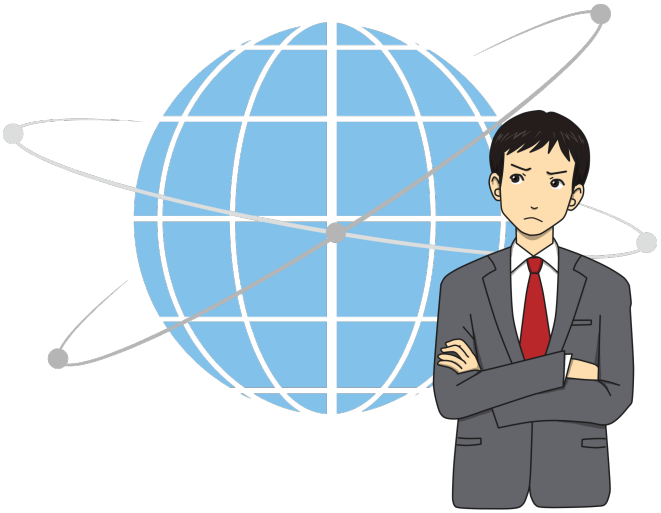
ルーティングセキュリティ技術ASPAの普及の重点をシミュレーションしてみた
- どこで検証すると経路を守れるの？ -

大阪大学 大学院情報科学研究科 M2
梅田 直希





目次

- 自己紹介
- これまでの研究
- 不正経路伝搬と ASPA
- 実験
- 結論

自己紹介

<名前> 梅田 直希

<所属> 大阪大学 大学院情報科学研究科 セキュリティ工学講座 (藤原研究室)

<研究テーマキーワード>

BGP, RPKI, ROA, ROV, BGPsec, ASPA

<その他>

研究室内ネットワーク管理・読書

<これまでの JANOG 発表>

JANOG 47 (初心者) LT

「BGP実験用ネットワークが自動生成できる軽量なプラットフォーム SQUAB」

https://github.com/han9umeda/SQUAB

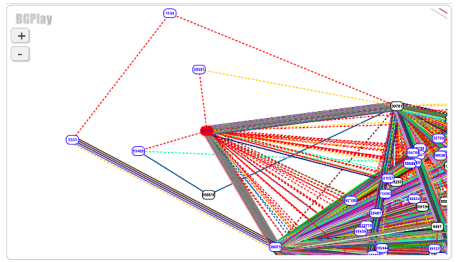
(今見返すと、あの書きぶりでよく採用されたなと感じます。

発表の際は Slack の方で大変盛り上がっていただき、とても嬉しかったです。)

これまでの研究

BGP 実験用プラットフォーム SQUAB の開発・BGPsec の調査

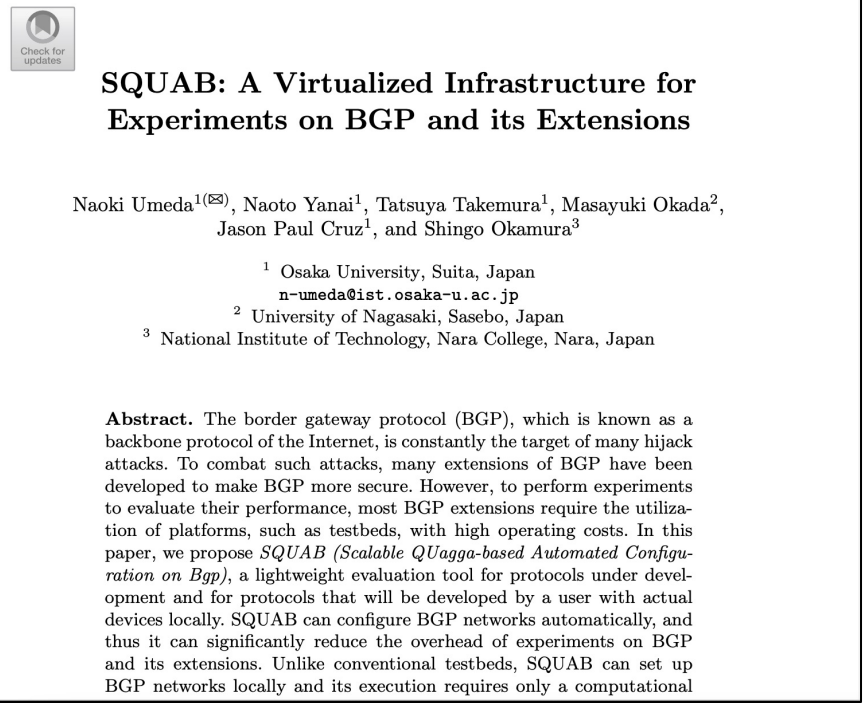
GitHub https://github.com/han9umeda/SQUAB




```
AS_Setting:
  1103:
    image: quagga
  3333:
    image: quagga
  29075:
    image: quagga
  30781:
    image: quagga
  39351:
    image: quagga
  51405:
    image: quagga
  57119:
    image: quagga
  206610:
    image: quagga
Peer_info:
  - [3333, 1103]
  - [1103, 30781]
  - [30781, 39351]
  - [30781, 57119]
  - [30781, 206610]
  - [57119, 51405]
  - [206610, 51405]
  - [30781, 29075]
  - [57119, 29075]
  - [29075, 3333]
```

```
(squab) han9umeda@umedanoMacBook-Pro SQUAB % docker ps
CONTAINER ID   IMAGE     COMMAND       CREATED          STATUS          PORTS     NAMES
40468320b2f7   quagga    "/bin/bash"   30 seconds ago   Up 21 seconds             naitway_router_1103_for_3333_1
6995fe10101b   quagga    "/bin/bash"   30 seconds ago   Up 23 seconds             naitway_router_51405_for_206610_1
2b4614961329   quagga    "/bin/bash"   30 seconds ago   Up 21 seconds             naitway_router_30781_for_39351_1
4e3ed1a4fb29   srx       "/bin/bash"   30 seconds ago   Up 23 seconds             naitway_rpki_1
c57e1a0d6e72   quagga    "/bin/bash"   30 seconds ago   Up 21 seconds             naitway_router_57119_for_51405_1
c2fe250850f3   quagga    "/bin/bash"   30 seconds ago   Up 21 seconds             naitway_router_29075_for_3333_1
11f14f6f042f   quagga    "/bin/bash"   30 seconds ago   Up 21 seconds             naitway_router_3333_for_1103_1
182cbd4fe568   quagga    "/bin/bash"   30 seconds ago   Up 23 seconds             naitway_router_29075_for_30781_1
7bb85e6de395   quagga    "/bin/bash"   30 seconds ago   Up 22 seconds             naitway_router_39351_for_30781_1
d38b70c142ca   quagga    "/bin/bash"   30 seconds ago   Up 21 seconds             naitway_router_30781_for_206610_1
785a1c769e56   quagga    "/bin/bash"   30 seconds ago   Up 21 seconds             naitway_router_57119_for_29075_1
9f4b0d70b947   quagga    "/bin/bash"   30 seconds ago   Up 21 seconds             naitway_router_3333_for_29075_1
8001a35c4f76   quagga    "/bin/bash"   30 seconds ago   Up 22 seconds             naitway_router_206610_for_30781_1
884e9bd05a8e   quagga    "/bin/bash"   30 seconds ago   Up 22 seconds             naitway_router_206610_for_51405_1
71529c5aa1ae   quagga    "/bin/bash"   30 seconds ago   Up 22 seconds             naitway_router_30781_for_57119_1
98916adaba8e   quagga    "/bin/bash"   30 seconds ago   Up 21 seconds             naitway_router_57119_for_30781_1
636b8bd62dfc   quagga    "/bin/bash"   30 seconds ago   Up 21 seconds             naitway_router_30781_for_1103_1
7d4c36cadde5   quagga    "/bin/bash"   30 seconds ago   Up 22 seconds             naitway_router_51405_for_57119_1
9a8120fef2ac   quagga    "/bin/bash"   30 seconds ago   Up 21 seconds             naitway_router_1103_for_30781_1
a525f0913641   quagga    "/bin/bash"   30 seconds ago   Up 21 seconds             naitway_router_30781_for_29075_1
9cb660e932a4   quagga    "/bin/bash"   30 seconds ago   Up 21 seconds             naitway_router_29075_for_57119_1
```

```
bgpd> naitway_router_30781_for_29075_1
spawn telnet localhost 2605
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.

Hello, this is Quagga (version 0.99.22.4).
Copyright 1996-2005 Kunihiro Ishiguro, et al.


User Access Verification

Password:
bgpd> show ip bgp summary
BGP router identifier 10.10.10.12, local AS number 30781
RIB entries 15, using 1680 bytes of memory
Peers 5, using 22 KiB of memory

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.23.158.2    4 30781       7      10        0    0    0 00:03:31        3
172.23.158.3    4 30781       8       9        0    0    0 00:03:32        3
172.23.158.5    4 30781       7       9        0    0    0 00:03:31        2
172.23.158.6    4 30781       8       9        0    0    0 00:03:30        3
172.25.112.2    4 29075      11      14        0    0    0 00:03:29        4

Total number of neighbors 5
bgpd> show ip bgp
BGP table version is 0, local router ID is 10.10.10.12
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  172.18.86.0/24   172.25.112.2                             0 29075 57119 51405 i
* i                 172.18.99.2                    100      0 206610 51405 i
*>i                 172.21.39.3                    100      0 57119 51405 i
*> 172.20.21.0/24  172.25.112.2             0               0 29075 i
*  172.22.132.0/24 172.25.112.2                             0 29075 57119 i
*>i                 172.21.39.3             0      100      0 57119 i
*>i172.22.199.0/24 172.24.113.2             0      100      0 1103 i
*>i172.22.254.0/24 172.18.99.2              0      100      0 206610 i
* i172.23.158.0/24 172.23.158.6             0      100      0 i
* i                 172.23.158.2             0      100      0 i
* i                 172.23.158.5             0      100      0 i
* i                 172.23.158.3             0      100      0 i
*>                  0.0.0.0                  0         32768 i
*> 172.26.217.0/24 172.25.112.2                             0 29075 3333 i
* i                 172.24.113.2                   100      0 1103 3333 i
*>i172.27.167.0/24 172.24.98.2              0      100      0 39351 i

Total number of prefixes 8
```



Check for updates

SQUAB: A Virtualized Infrastructure for Experiments on BGP and its Extensions

Naoki Umeda[1(✉)], Naoto Yanai[1], Tatsuya Takemura[1], Masayuki Okada[2], Jason Paul Cruz[1], and Shingo Okamura[3]

[1] Osaka University, Suita, Japan
n-umeda@ist.osaka-u.ac.jp
[2] University of Nagasaki, Sasebo, Japan
[3] National Institute of Technology, Nara College, Nara, Japan

Abstract. The border gateway protocol (BGP), which is known as a backbone protocol of the Internet, is constantly the target of many hijack attacks. To combat such attacks, many extensions of BGP have been developed to make BGP more secure. However, to perform experiments to evaluate their performance, most BGP extensions require the utilization of platforms, such as testbeds, with high operating costs. In this paper, we propose *SQUAB (Scalable QUagga-based Automated Configuration on Bgp)*, a lightweight evaluation tool for protocols under development and for protocols that will be developed by a user with actual devices locally. SQUAB can configure BGP networks automatically, and thus it can significantly reduce the overhead of experiments on BGP and its extensions. Unlike conventional testbeds, SQUAB can set up BGP networks locally and its execution requires only a computational

※注意

発表内容は、BGP を研究テーマに据えている学生の視点で組み立てています。

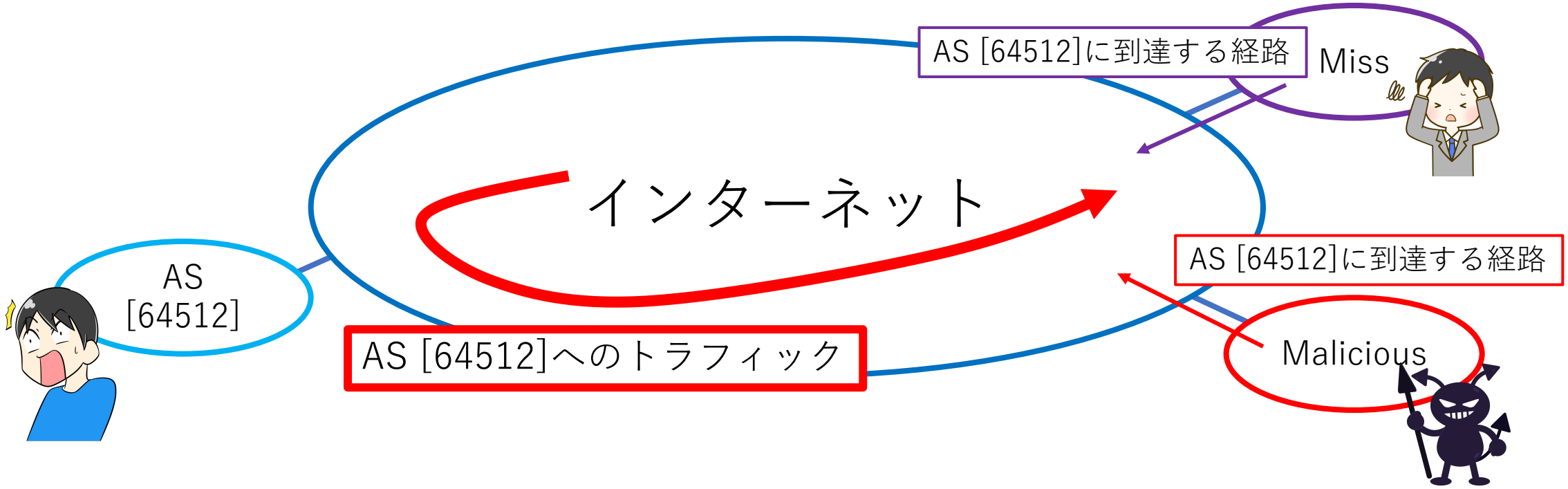
ネットワーク運用経験も研究室 LAN やその境界に留まります。

AS 運用者の観点からは暴論を含んでいる可能性もありますので、

ご了承ください。

発表後の議論でコメントをいただけると嬉しいです。

AS 運用における懸念: 不正経路伝搬



グローバルに共有されてほしくない経路が出回ってしまうことがある

- ルートリーク
- 悪意を持った不正経路広告 (経路ハイジャック)

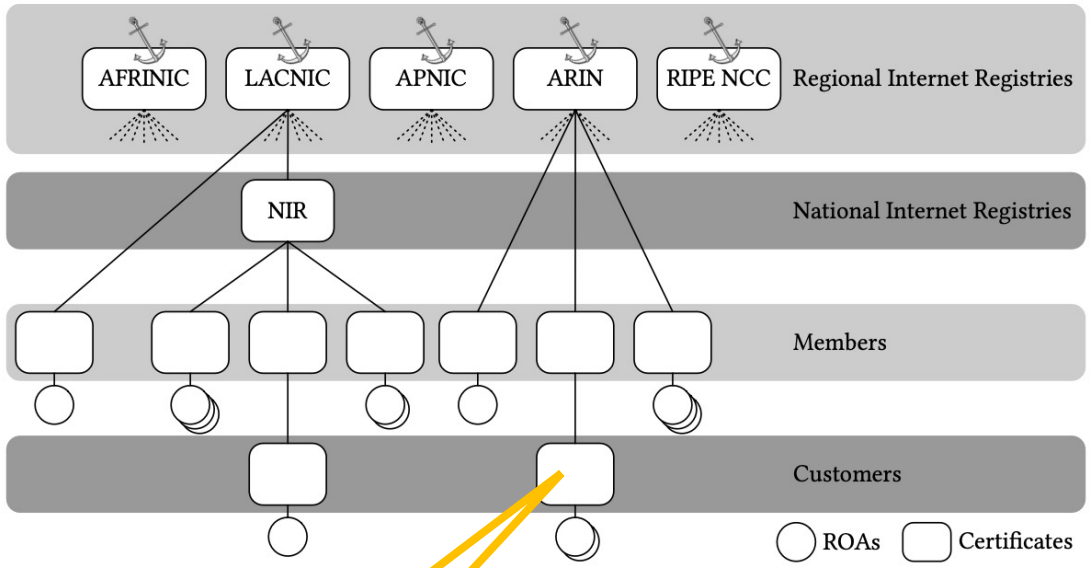
-> 対策としてRPKI, ROA, ROV, BGPsec, ASPA

ROA, BGPsec, ASPA

	保護対象	普及	備考
ROA (ROV)	Origin	うまくいっている	JPNIC 管轄 AS ROA 発行率 プレフィックスベースで 2 割から 3 割 (2021年6月時点) *[JPOPM40]*
BGPsec PV	Path	見込みなし	国際的な普及率数% 利用率が低ければ、むしろ弊害がある
ASPA	Path	これから	ROA と似たような構成の技術 普及の見込みあり

[JPOPM40] JPOPM40 "ROA登録促進の提案に向けた事前のご相談" 吉田 友哉, 渡辺 英一郎
https://jpopf.net/JPOPM40Program?action=AttachFile&do=view&target=jpopm40_rpki_20210625.pdf

ROA と ASPA



- AS 番号
- ネットワークアドレス
- 鍵

RPKI

[CT+19]

<RPKI>

AS 番号と鍵の対応関係が公開されたデータベース

<ROA>

AS 番号とネットワークプレフィックスの対応関係を示すデータ

ROA = (AS number, Network Prefix, Sign by Key)

<ASPA>

AS 番号とその Provider AS の対応関係を示すデータ

ASPA

= (AS number, Provider AS number, Sign by Key)

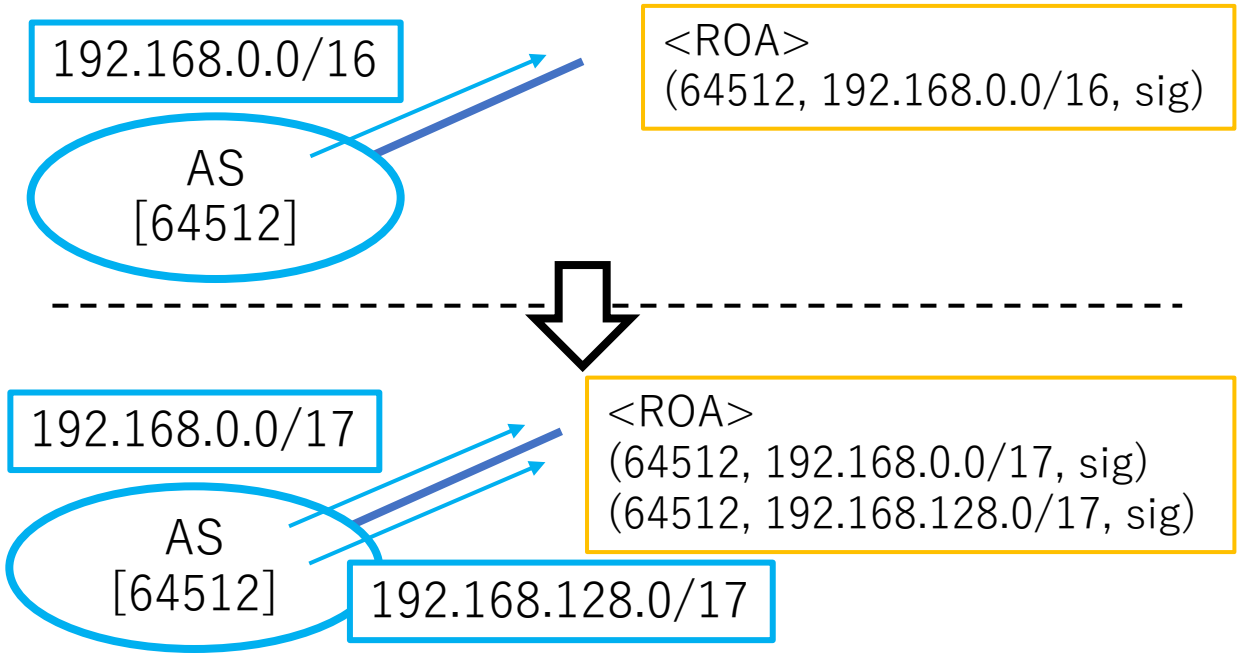
[CT+19] Chung, Taejoong, et al. "RPKI is coming of age: A longitudinal study of RPKI deployment and invalid route origins." Proceedings of the Internet Measurement Conference. 2019.

ROA と ASPA 個人的な思い

メンテナンスは ASPA のほうがラク？

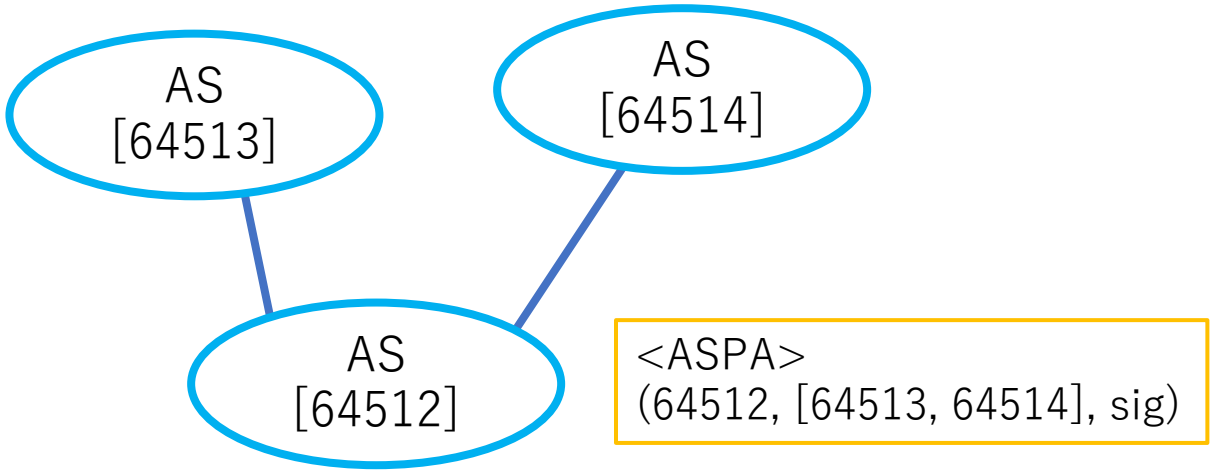
ROA

ネットワークアドレスのやりとりごと
に更新が必要

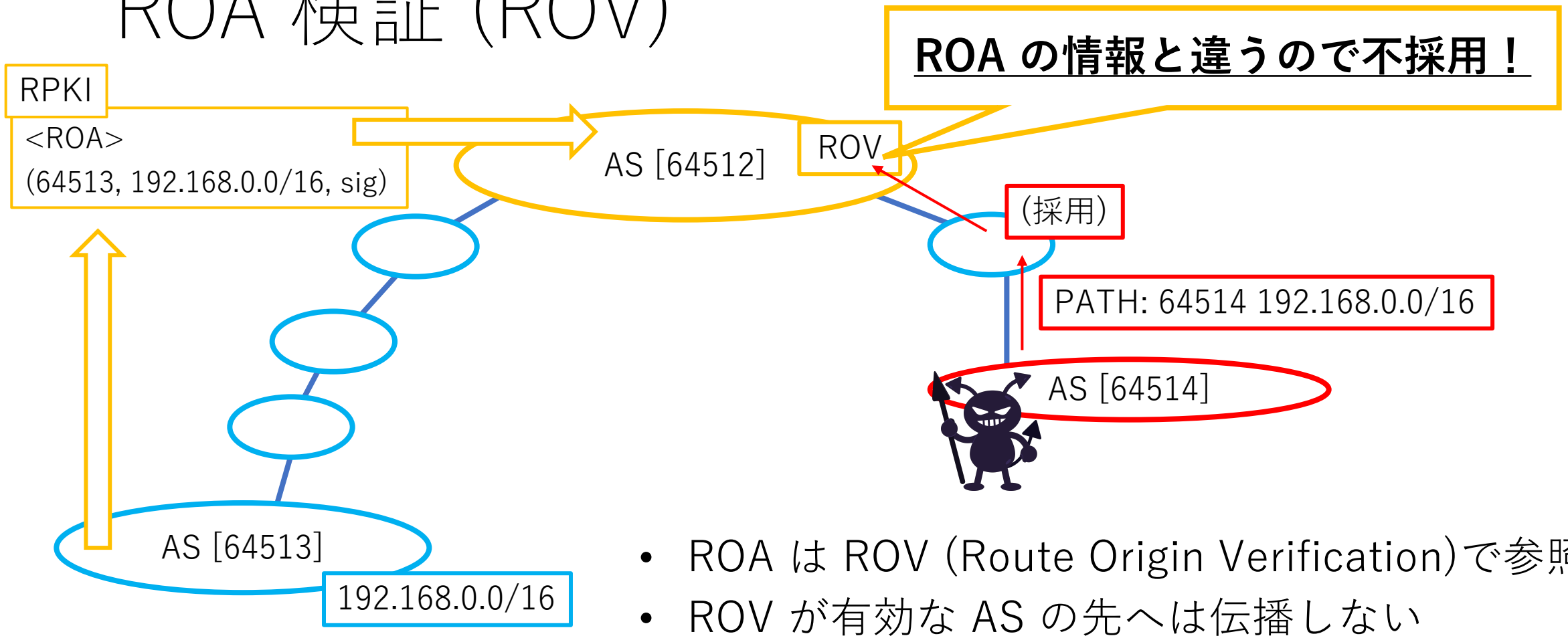


ASPA

Provider との接続関係が変わらない限り
更新不要

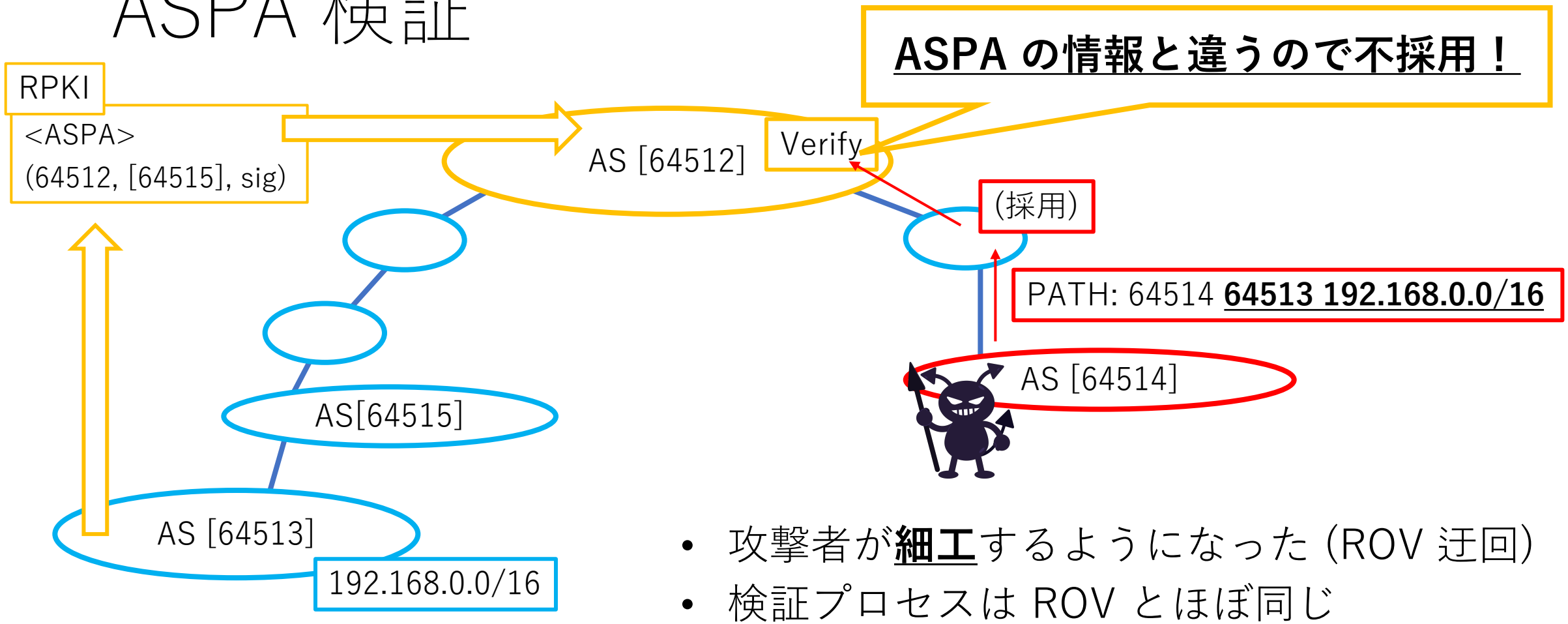


ROA 検証 (ROV)



- ROA は ROV (Route Origin Verification)で参照
- ROV が有効な AS の先へは伝播しない
- ROV 導入を公言している大規模事業者もあり
- ROA を発行しないと、恩恵を受けられない

ASPA 検証



- 攻撃者が**細工**するようになった (ROV 迂回)
- 検証プロセスは ROV とほぼ同じ
- Provider も ASPA を発行すればより強固に
- ROA との組み合わせで効果を発揮

実験 (ASPA 検証はどこでやればいい？)

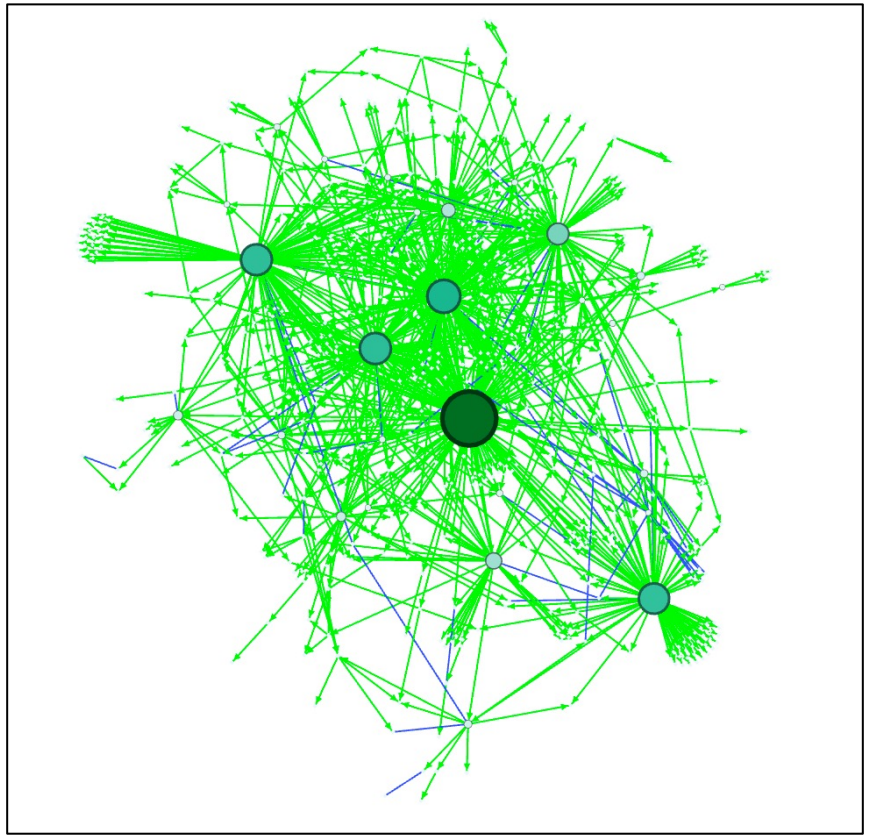
実験目的

JPNIC 管轄 AS で構成されるネットワークにおいて、

どの程度の ASPA 検証の導入が必要かを明らかにする

(大きな AS で導入すればよい気がするが、どれくらい

導入すればどの程度の効果があるかを調べたい)



実験方法

シミュレータ作りました

GitHub
https://github.com/han9umeda/LOTUS

LOTUS (Lightweight rOuTing simUlator with aSpa)

- AS, その接続関係, ASPA 発行状況, ASPA 検証実施の有無を設定
- Customer から来た経路は全ての AS へ流し、それ以外の経路は Customer へしか流さない

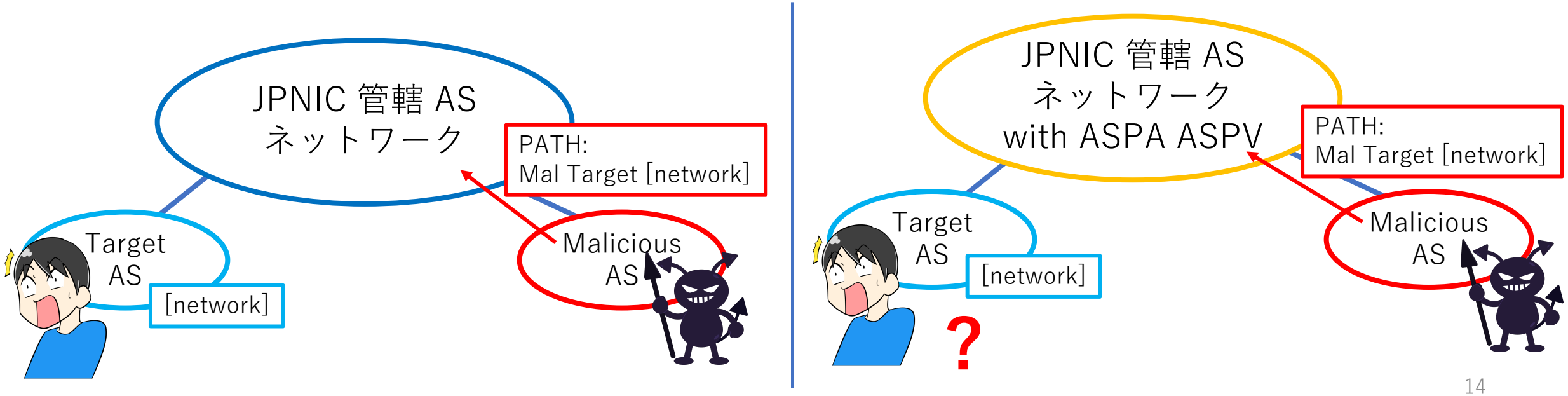
モデルの制限

- 経路のアグリゲーションなし
- IXポリシー無し
- 固定 Local Preference (複数 Provider は同じ値)
- Peer かつ Customer-Provider の関係は Customer-Provider に統一
- 観測できていない Peer が (きっと) ある

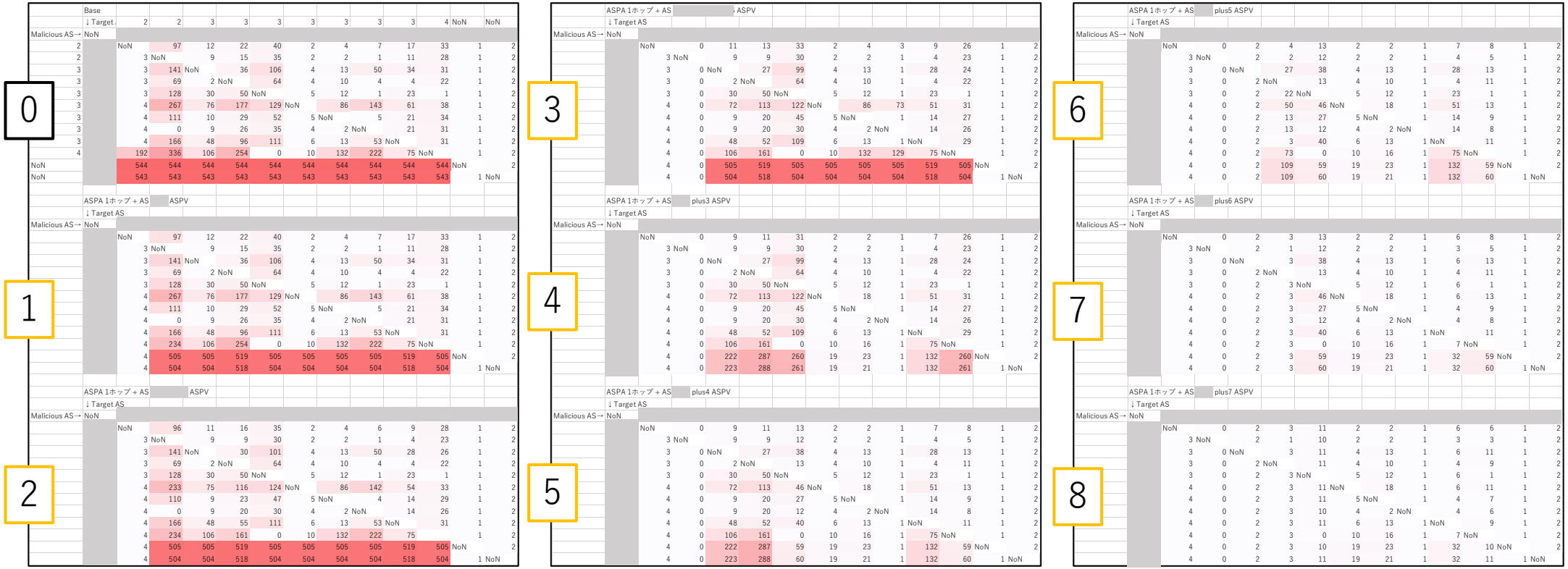
実験設定

- ASPA, ASPV が展開されていないネットワーク
- 被害者 AS が ASPA を発行しており、いくつかの AS が ASPA 検証の導入をおこなっているネットワーク

それぞれに経路を奪取する攻撃を行う



結果



- JPNIC 管轄 AS ネットワークで末端に存在する AS を適当に 12 個選択し、互いに攻撃
- 数字は Top N AS が ASPA 検証導入
- 上位 7 AS が導入したところで、大方の攻撃が防げている

結果 (海外からの攻撃)

0

	Base																																	
Distance from 2497	↓ Target AS	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	NoN
Outside AS with→	NoN																																	
2		0	95	75	98	79	22	21	22	55	30	11	18	11	21	4	4	7	11	3	2	0	2	41	18	14	14	42	20	9	17	13	7	5
2		0	7	0	0	32	14	14	9	22	12	8	14	8	12	4	1	5	5	1	2	4	1	36	8	8	8	33	1	1	12	10	5	3
3		282	171	207	142	0	59	59	64	70	35	7	14	7	18	27	6	5	11	1	6	4	2	107	61	57	57	45	57	52	50	12	5	5
3		141	0	96	70	0	7	7	10	0	22	1	7	1	15	3	5	5	10	1	6	4	1	65	9	5	4	28	10	6	5	3	5	4
3		192	156	130	129	107	35	35	8	74	24	2	9	1	17	20	7	5	11	1	7	4	2	0	6	2	2	7	14	2	4	6	5	6
3		516	353	380	268	224	209	209	202	104	165	150	100	143	92	58	77	79	0	75	1	5	2	130	196	196	196	61	108	145	68	19	5	6
3		157	129	0	112	95	19	19	19	60	27	9	15	8	1	13	7	5	10	1	7	5	2	53	16	12	12	40	17	7	29	16	5	6
3		113	81	0	0	67	16	16	16	45	19	9	16	8	14	13	6	5	10	1	6	5	2	36	13	9	9	37	12	3	12	10	5	5
3		268	206	195	167	100	134	134	132	0	77	60	62	54	22	3	8	5	17	1	8	5	2	112	105	101	100	39	66	55	39	12	5	6
4		261	343	282	337	321	384	384	349	232	330	324	280	323	265	221	264	262	196	262	194	193	193	0	303	303	303	31	137	224	26	8	5	6
NoN		545	545	545	545	545	545	545	545	545	545	545	545	545	545	545	545	545	545	545	545	545	545	545	545	545	545	545	545	545	545	545	545	6
NoN		544	544	544	544	544	544	544	544	544	544	544	544	544	544	544	544	544	544	544	544	544	544	544	544	544	544	544	544	544	544	544	544	6
		3019	2630	2454	2412	2114	1988	1987	1920	1751	1830	1670	1624	1653	1566	1455	1474	1472	1370	1436	1328	1318	1298	1669	1824	1796	1794	1452	1531	1593	1351	1198	1141	

7

	ASPA 1ホップ + AS 2497 plus6 ASPV																																	
	↓ Target AS																																	
Outside AS with→	NoN																																	
		0	0	0	0	0	4	3	10	0	20	2	9	1	19	3	2	5	9	1	2	0	2	14	6	2	2	15	14	3	5	3	5	5
		0	0	0	0	0	1	1	2	0	5	2	7	1	12	3	1	5	5	1	2	4	1	13	1	1	1	10	1	1	5	3	5	3
		0	0	0	0	0	4	4	9	0	29	2	8	1	18	3	6	5	11	1	6	4	2	39	6	2	2	27	12	3	41	3	5	5
		0	0	0	0	0	4	4	7	0	22	1	7	1	15	3	5	5	10	1	6	4	1	14	6	2	1	17	7	3	5	3	5	4
		0	0	0	0	0	4	4	8	0	24	2	9	1	17	1	7	5	11	1	7	4	2	0	6	2	2	7	14	2	4	6	5	6
		0	0	0	0	0	4	4	9	0	32	9	10	1	24	3	3	5	0	1	1	5	2	47	6	2	2	36	18	3	58	9	5	6
		0	0	0	0	0	3	3	9	0	20	3	8	1	1	3	7	5	10	1	7	5	2	28	6	2	2	15	13	3	19	6	5	6
		0	0	0	0	0	3	3	9	0	12	3	9	1	14	3	6	5	10	1	6	5	2	13	6	2	2	14	12	3	5	3	5	5
		0	0	0	0	0	4	4	9	0	24	8	9	1	22	3	8	5	17	1	8	5	2	41	6	2	2	19	18	3	36	8	5	6
		0	0	0	0	0	4	4	9	0	29	2	10	1	18	3	13	5	13	1	11	5	2	0	6	2	2	31	16	3	26	8	5	6
		0	0	0	0	0	4	4	10	0	33	97	10	1	24	3	20	5	20	1	20	5	2	60	6	2	2	90	18	3	85	10	5	6
		0	0	0	0	0	4	4	10	0	33	98	10	1	22	3	20	5	20	1	20	5	2	61	6	2	2	91	18	3	86	10	5	6

8

	ASPA 1ホップ + AS 2497 plus7 ASPV																																	
	↓ Target AS																																	
Outside AS with→	NoN																																	
		0	0	0	0	0	4	3	10	0	20	2	9	1	19	3	2	5	9	1	2	0	2	12	6	2	2	13	14	3	3	3	5	5
		0	0	0	0	0	1	1	2	0	5	2	7	1	12	3	1	5	5	1	2	4	1	11	1	1	1	8	1	1	3	3	5	3
		0	0	0	0	0	4	4	9	0	29	2	8	1	18	3	6	5	11	1	6	4	2	12	6	2	2	25	12	3	12	3	5	5
		0	0	0	0	0	4	4	7	0	22	1	7	1	15	3	5	5	10	1	6	4	1	12	6	2	1	15	7	3	3	3	5	4
		0	0	0	0	0	4	4	8	0	24	2	9	1	17	1	7	5	11	1	7	4	2	0	6	2	2	7	14	2	4	6	5	6
		0	0	0	0	0	4	4	9	0	32	9	10	1	24	3	3	5	0	1	1	5	2	12	6	2	2	34	18	3	21	9	5	6
		0	0	0	0	0	3	3	9	0	20	3	8	1	1	3	7	5	10	1	7	5	2	12	6	2	2	13	13	3	3	6	5	6
		0	0	0	0	0	3	3	9	0	12	3	9	1	14	3	6	5	10	1	6	5	2	11	6	2	2	12	12	3	3	3	5	5
		0	0	0	0	0	4	4	9	0	24	8	9	1	22	3	8	5	17	1	8	5	2	12	6	2	2	17	18	3	2	8	5	6
		0	0	0	0	0	4	4	9	0	29	2	10	1	18	3	13	5	13	1	11	5	2	0	6	2	2	31	16	3	26	8	5	6
		0	0	0	0	0	4	4	10	0	33	97	10	1	24	3	20	5	20	1	20	5	2	11	6	2	2	45	18	3	34	10	5	6
		0	0	0	0	0	4	4	10	0	33	98	10	1	22	3	20	5	20	1	20	5	2	12	6	2	2	46	18	3	34	10	5	6

- JPNIC 管轄でない AS を Customer に持つ AS から不正経路が流入する場合
- 末端ではない場所からの攻撃注入だが、必ずしも強力な攻撃になっているというわけではない
- こちらでも上位 7 AS で導入されていると、多くの攻撃が防げている

結論

- まず ROA の発行から
- ASPA は ROA よりも管理コストは少ない (と思う)
- ROV で Reject はつらいかもしれないが、ASPV は強い気持ちで Invalid を Reject すると良い (と思う)
- 上位 7 AS くらいの方々に ASPA 検証の導入を強くお願いしたい
  -> これでかなりの攻撃やルートリークが緩和できる

議論したいこと

- 現状の運用で、十分だと感じているか (到達性が揺らいだ経験は？)
- ROA, ROV, ASPA の導入に対する印象は？ (大変そう？)
- 実際に運用されている方、導入後に気になることは？

GitHub https://github.com/han9umeda/LOTUS

n-umeda@ist.osaka-u.ac.jp