Residential IP Proxyサービスを悪用した不正行為の調査

明治大学 総合数理学部

住友孝彰 菊池浩明

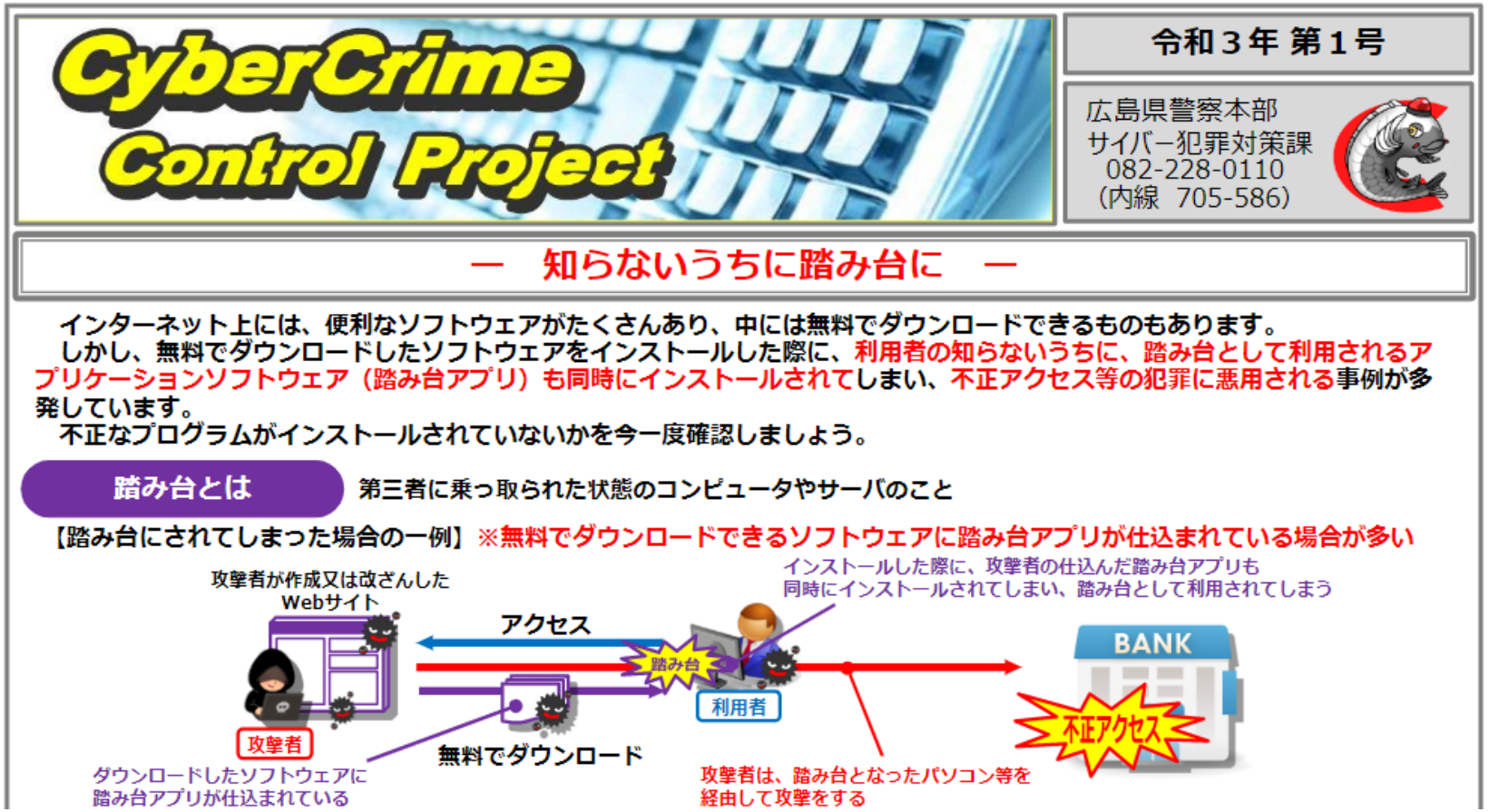
背景

- Residential IP Proxy(以下RESIPとする)をサービスとして提供する企業の出現

- Residential IP Proxyサービス
  - 家庭用の機器をproxyとして提供しているサービス
  - サーバ側からブラウザ側の秘匿、通信の検閲の回避(ex, 中国)に対して需要がある

RESIPに不正利用

- 猪野、2022年JSAC
  - カード利用(不正)
  - なりすましログイン
  - 投資詐欺



https://www.pref.hiroshima.lg.jp/uploaded/attachment/417114.pdf

[猪野, 2022] “国内悪性プロキシサービスとの闘争”, JSAC2022

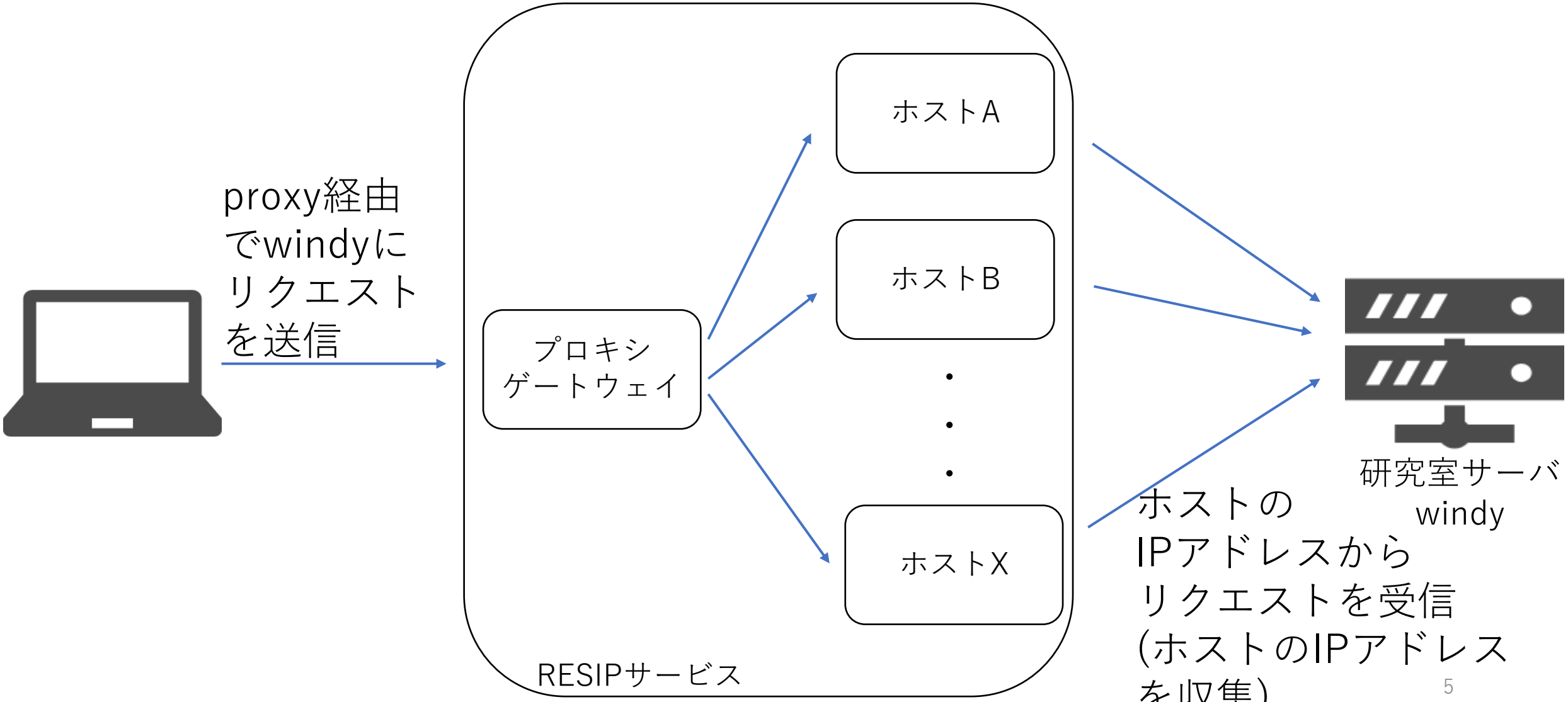
研究目的

- RESIPサービスの不正利用の最新状況を明らかにすること

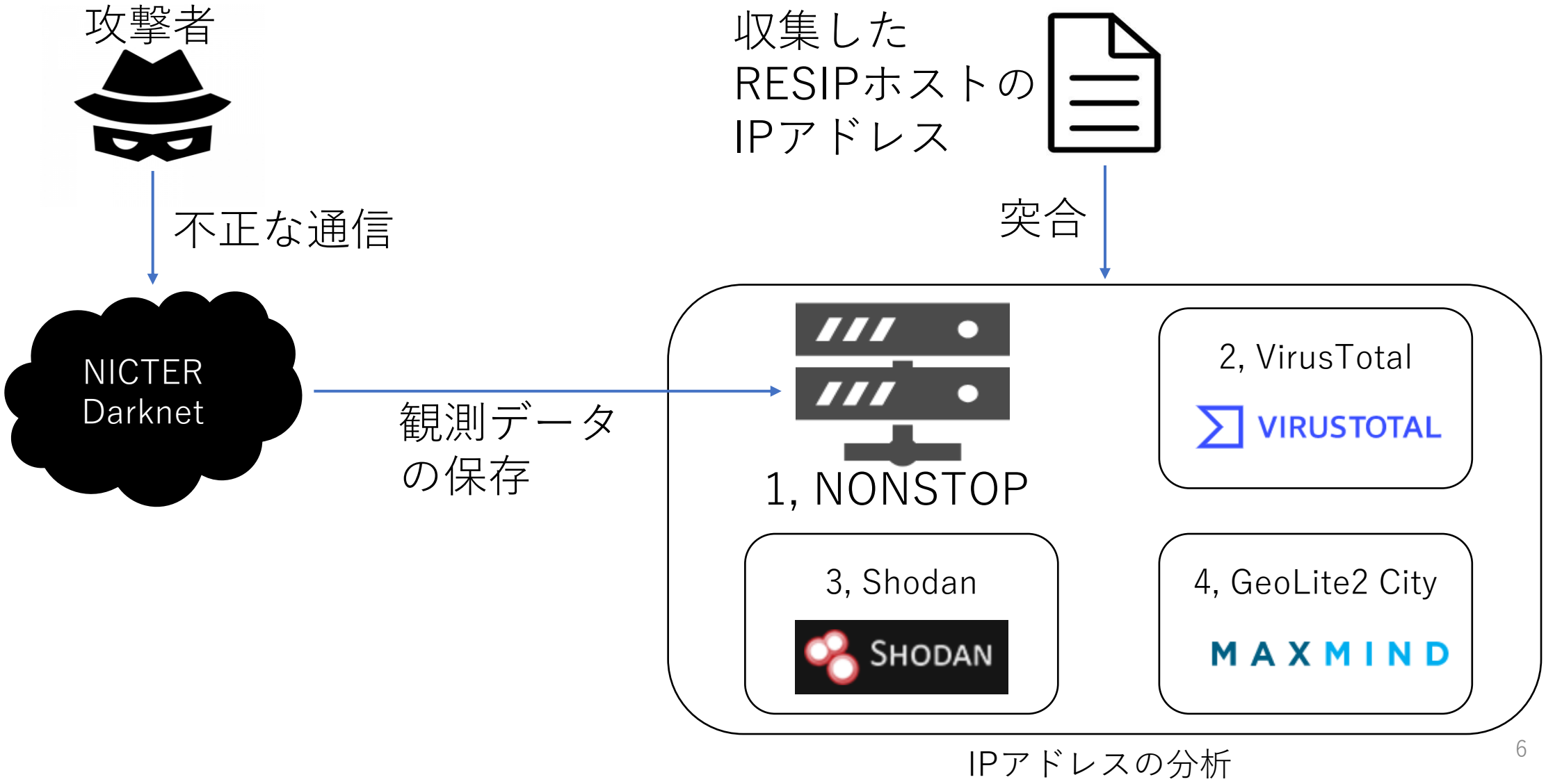
- リサーチクエスチョン

  RQ1. 代表的な2つのRESIPサービスのホストで不正利用の差はあるのか
  RQ2. 何の目的にRESIPホストがよく用いられているのか
  RQ3. どの国に不正なproxyが多いのか

実験方法1：収集


proxy経由でwindyにリクエストを送信
プロキシゲートウェイ
ホストA
ホストB
ホストX
RESIPサービス
研究室サーバ windy
ホストのIPアドレスからリクエストを受信(ホストのIPアドレスを収集)

実験方法2：分析


攻撃者
不正な通信
NICTER
Darknet
観測データ
の保存
収集した
RESIPホストの
IPアドレス
突合
1, NONSTOP
2, VirusTotal
VIRUSTOTAL
3, Shodan
SHODAN
4, GeoLite2 City
MAXMIND
IPアドレスの分析

実験結果：データ概要

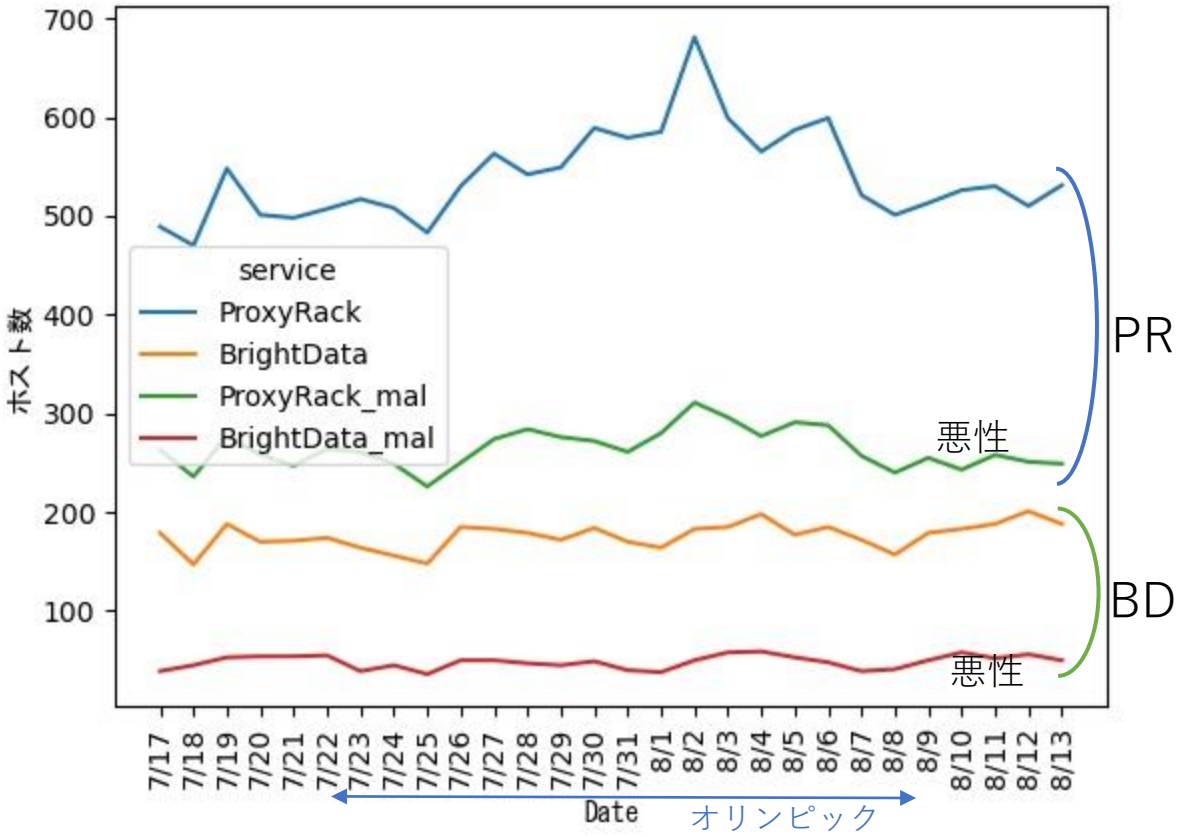
ProxyRackはBright Dataより
不正IPアドレスの割合は2.04倍
不正IP中、悪性IPアドレスの割合は1.76倍
不正パケット数は16.09倍
高いことが分かった

	サービス				
	期間	計		計:26日	
IPアドレス	IPアドレスの総数	69,369		70,253	
	不正IPアドレス数	3,092	**4.5%**	1,545	**2.2%**
	同アドレス中 悪性IPアドレス数	1,087	**35.2%**	307	**19.9%**
パケット	不正パケット数	526,674		32,724	
	悪性IPアドレスから 到達したパケット数	252,454	**47.9%**	15,379	**47.0%**

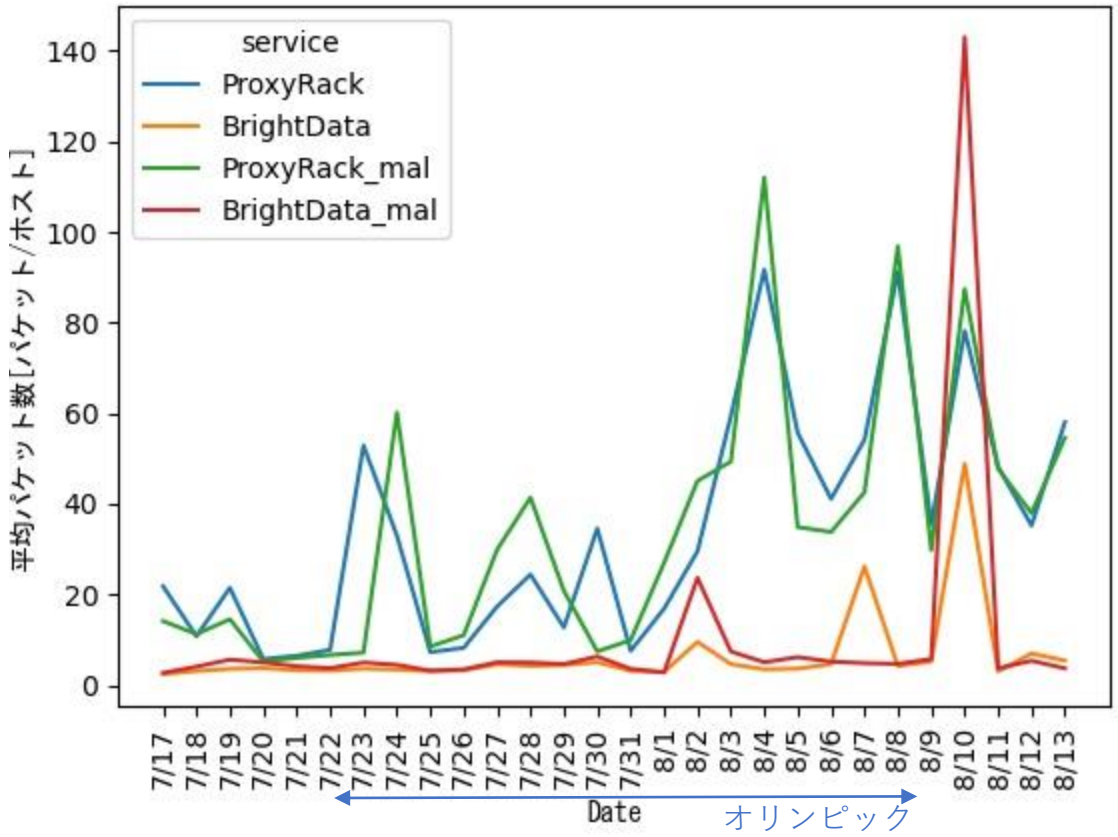
不正：未使用のIPアドレス空間にスキャンを行った
悪性：VirusTotalで悪性と判定された

実験結果1：ホスト数と不正通信数の変化

ホスト数



平均パケット数



ホスト数は常にProxyRackの方が多い

平均パケット数の変化とオリンピック期間に相関は見つからず

実験結果2：通信の宛先ポート

	ProxyRack		Bright Data		[半澤, 2021]	
宛先ポート番号(サービス)	観測件数	[%]	観測件数	[%]	観測件数	[%]
21(FTP)	112	0	125	0.4	193,917	11.5
22(SSH)	38592	7.3	**0**	0	49,767	2.9
23(Telnet)	32300	6.1	4051	**12.4**	613,606	36.4
25(SMTP)	**0**	0	**0**	0	**21,732**	1.3
80(HTTP)	15150	2.9	2044	6.2	97,780	5.8
445(SMB)	19682	3.7	11284	**34.5**	399,250	23.7
1433 (MSSQL)	4671	0.9	524	1.6	144,928	8.6
2222(SSH)	**0**	0	**0**	0	**16,838**	0.1
2323(Telnet)	754	0.1	363	1.1	43,310	2.5
3389(RDP)	64	0	**0**	0	9,782	0.5
宛先総ポート数	**748個**		**365個**			

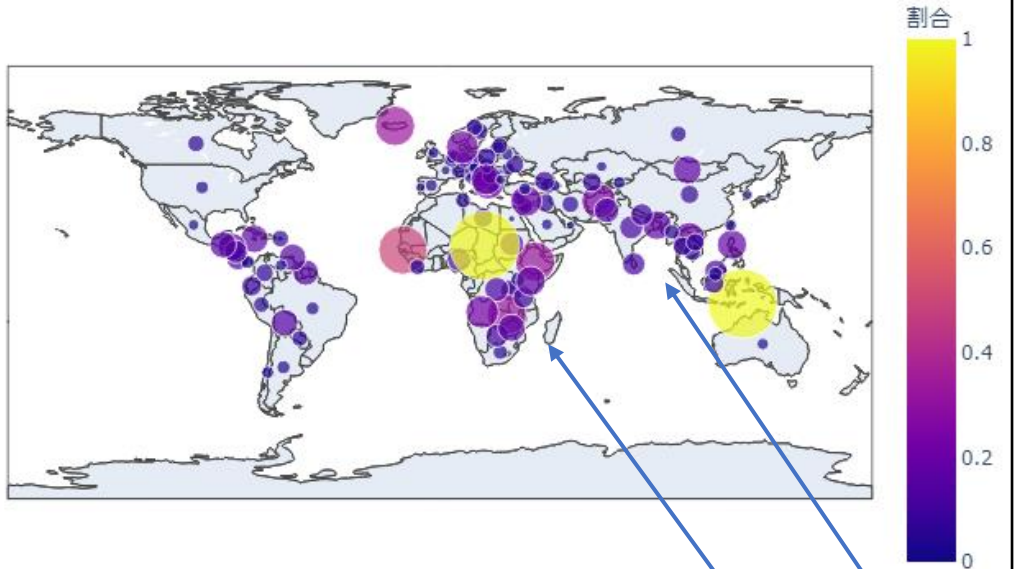
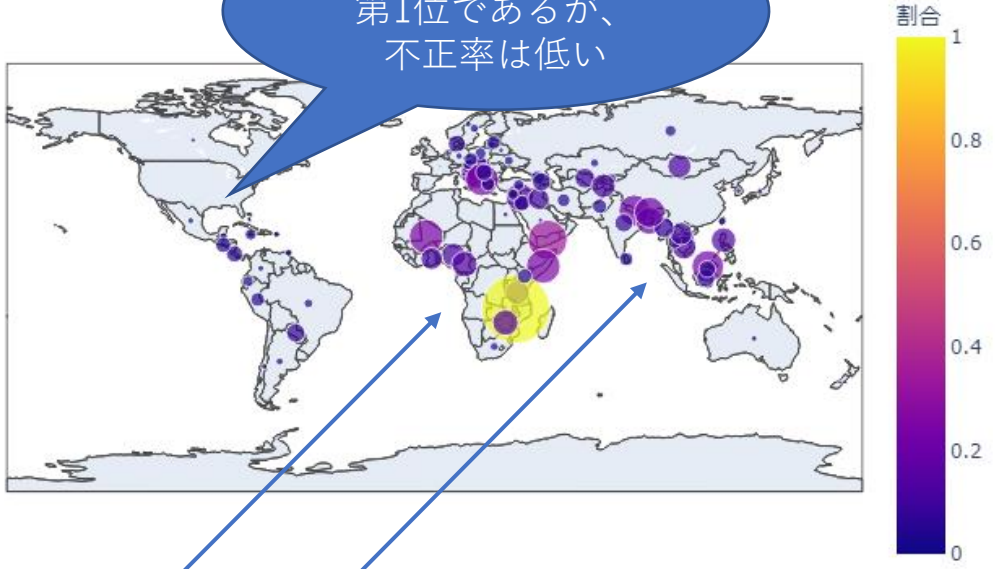
- **ProxyRackのは広域なスキャン**
- **Bright Data集中したスキャン**
- **半澤らが観測したポートは見られず**

実験結果3：解放されたポート(Shodan)

	ProxyRack				Bright Data			
ポート番号	不正IP数	[%]	悪性な不正IP数	[%]	不正IP数	[%]	悪性な不正IP数	[%]
2000	169	5.47	33	19.53	48	3.11	4	8.33
80(HTTP)	119	3.85	15	12.61	28	1.81	2	7.14
1723 (PPTP)	100	3.23	21	21	32	2.07	2	6.25
8291	75	2.43	11	14.67	18	1.17	2	11.11
53(DNS)	66	2.13	13	19.7	25	1.62	2	8
21(FTP)	53	1.71	10	18.87	6	0.39	0	0
22(SSH)	49	1.58	5	10.2	10	0.65	1	10
443(SMB)	48	1.55	8	16.67	28	1.81	2	7.14
7547 (CWMP)	41	1.33	4	9.76	4	0.26	0	0
8080 (HTTP)	29	0.94	7	24.14	5	0.32	1	20
5555	20	0.65	3	15	1	0.06	0	0
23(Telnet)	20	0.65	3	15	7	0.45	0	0

- 2000, 8291はMikroTik製ルータを標的とする攻撃の標的ポート
- 7545, 5555はMiraiが探索対象とするポート

実験結果4：不正IP数の割合

	ProxyRack	Bright Data
不正IP数の割合		

アメリカはホスト数
第1位であるが、
不正率は低い

アフリカ、東南アジア
に不正率が高い国が
集まっている

まとめ

RQ1. 差はある
Bright Dataと比べてProxyRackは
不正IPアドレスが約2倍
不正パケット数は約16倍

- RESIPホストのIPアドレスの不正利用の最新状況を明らかにした

RQ2. ポートスキャンが主目的
期間中ProxyRackのホストから748個
のポート宛のスキャンが確認された

RQ3.
東南アジアとアフリカに不正率が高い
国が集まっている

RQ2. [illegible]ホストがよく用いら[illegible]
RQ3. どの国に不正なproxyが多いのか

- IPアドレスを収集した期間に差があるため、今後、同一の期間で条件を揃えて再実験する予定である