

Residential IP Proxyサービスを 悪用した不正行為の調査

総合数理学部 先端メディアサイエンス学科
菊池研究室4年

住友孝彰

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



デモ

The image shows a web browser window displaying the 'What Is My IP Address' website. The browser's address bar shows the URL `https://whatismyipaddress.com`. The website's main content displays the user's IP address information: 'My IP Address is: IPv4: ? **133.26.40.10** IPv6: ? **Not detected**'. Below this is a map of Japan with a location pin and a tooltip that says 'Click for more about 133.26'. At the bottom of the page, there is a notification 'Location not accurate?' and a button 'Update My IP Location'.

A settings menu is open on the left side of the browser window, listing various system settings: 設定 (Settings), ホーム (Home), ネットワークとインターネット (Network and Internet), 状態 (Status), Wi-Fi, ダイヤルアップ (Dial-up), VPN, 機内モード (Airplane Mode), モバイル ホットスポット (Mobile Hotspot), and プロキシ (Proxy). The 'Proxy' option is selected.

A 'プロキシ' (Proxy) settings dialog box is overlaid on the right side of the browser window. The dialog contains the following text and controls:

- プロキシ** (Proxy)
- イーサネットまたは Wi-Fi 接続にプロキシ サーバーを使います。これらの設定は、VPN 接続には適用されません。
- プロキシ サーバーを使う (Toggle switch): オフ (Off)
- アドレス (Address): `http://zproxy.lum-superp`
- ポート (Port): `22225`
- 次のエントリで始まるアドレス以外にプロキシ サーバーを使います。エントリを区切るにはセミコロン (;) を使います。
- Input field: `<-loopback>`
- ローカル (イントラネット) のアドレスにはプロキシ サーバーを使わない
- 保存 (Save) button

At the bottom of the dialog box, there is a 'StreetMap Terms' link.

先行研究

- 2017年、Miら
 - RESIPサービスで使用されるIPアドレスを収集し分析を行った
 - 分析の結果、RESIPサービスが悪用されていると報告した
- 2021年、半澤ら
 - RESIPホストから継続的に国内のダークネットに通信が行われていることを明らかにした

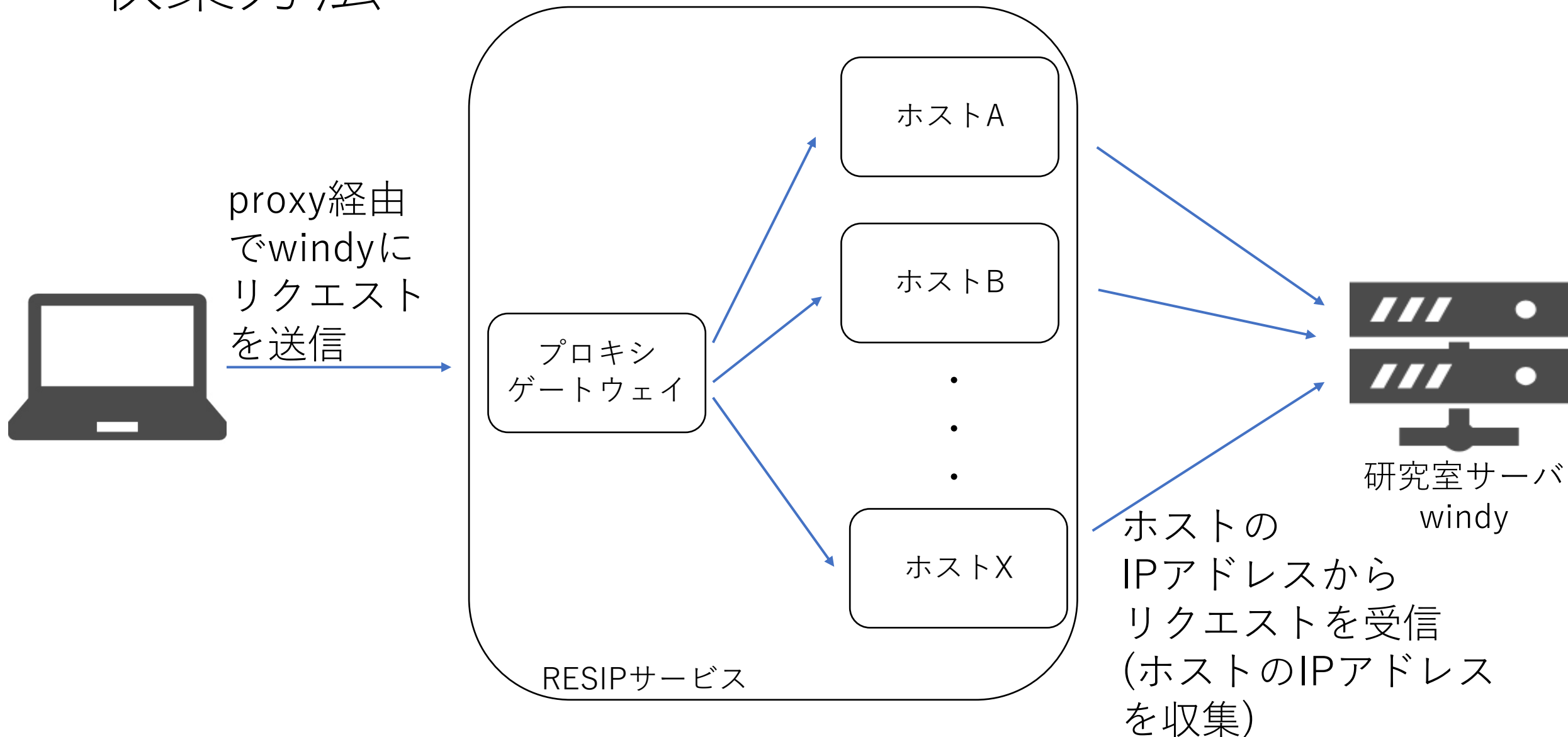
[Mi, 2017] “Resident Evil: Understanding Residential IP Proxy as a Dark Service”

[半澤, 2021] “Residential IP Proxyサービスに悪用される住宅用ホストの調査”

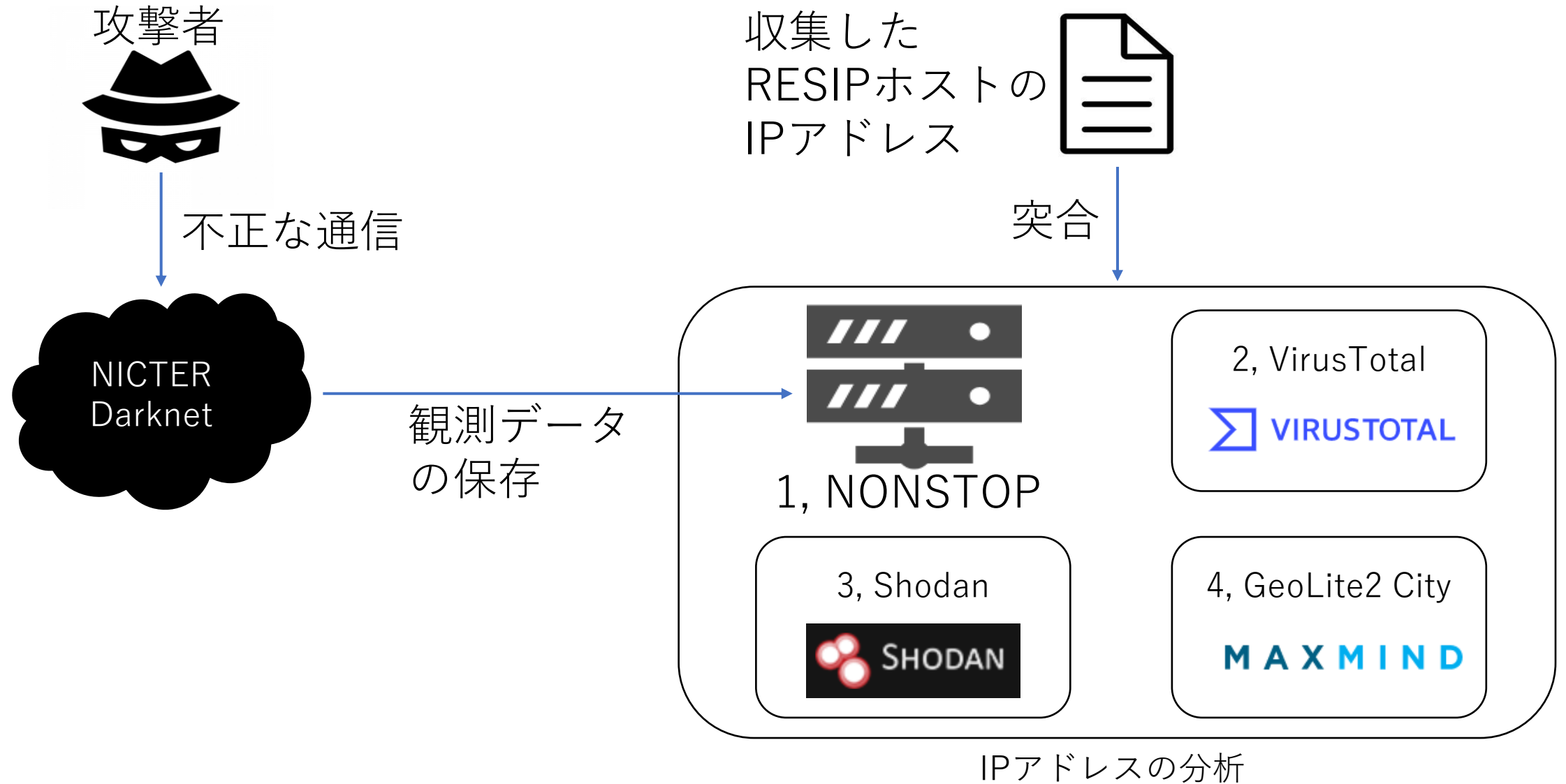
研究目的

- 本研究はRESIPサービスの不正利用の最新状況を明らかにすることを目的とする
- 実験目的は以下の3点である
 1. 代表的な2つのRESIPサービスのホストの差を明らかにする
 2. proxy経由の通信が国内のダークネットに到達しているか調査する
 3. 悪性利用のポートと用途, RESIPホストの分布を明らかにする

収集方法



分析方法

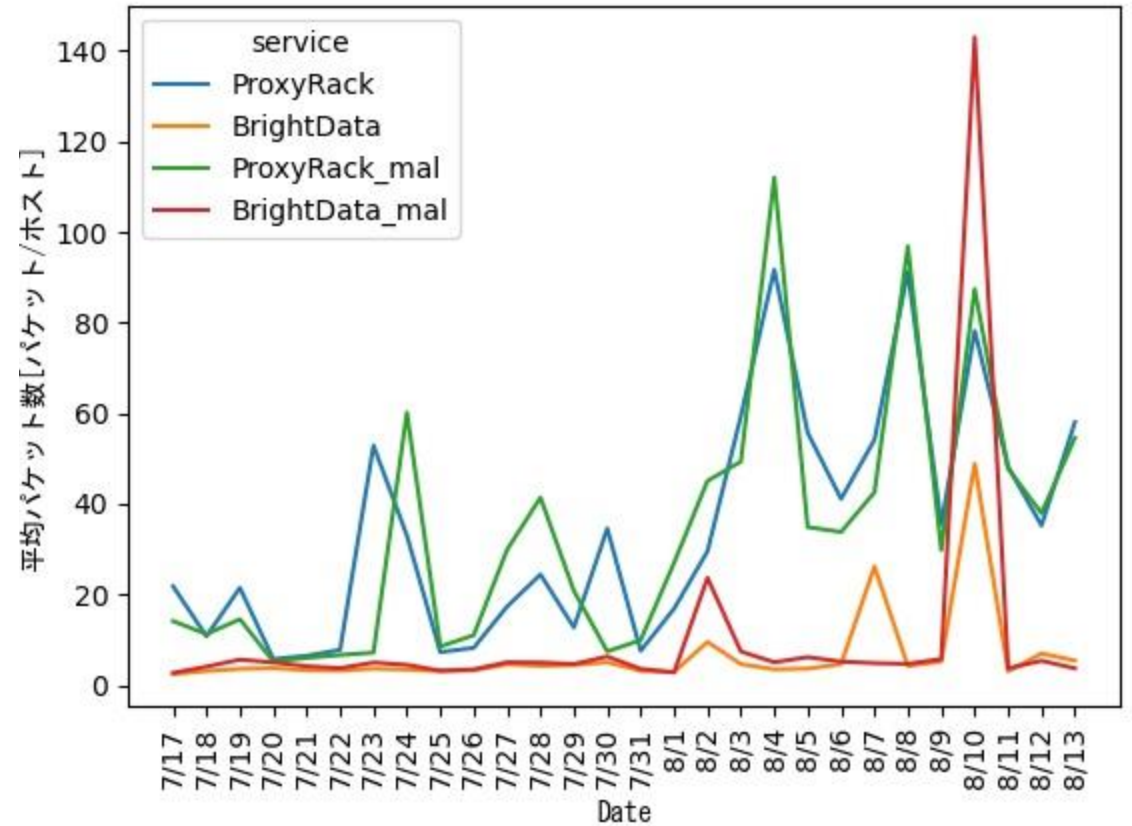
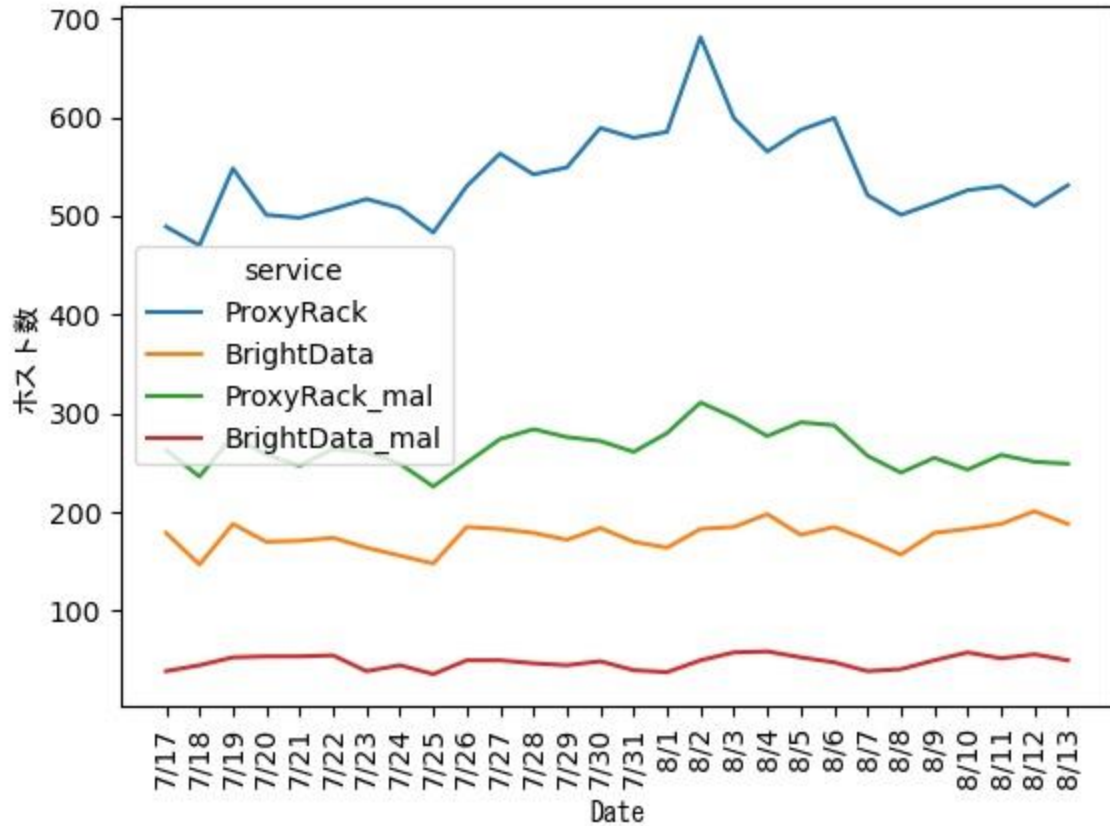


データ概要

	サービス	ProxyRack		Bright Data	
	期間	2021/7/22-8/7, 8/16-23 計:25日		2021/9/30-10/13, 10/15-23, 11/19-21 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%

不正は国内のダークネットに通信を行ったこと、悪性はVirusTotalで1つでも悪性と判定されたものを指す

1、ホスト数と不正通信数の変化



*_malは悪性IPアドレスの数である

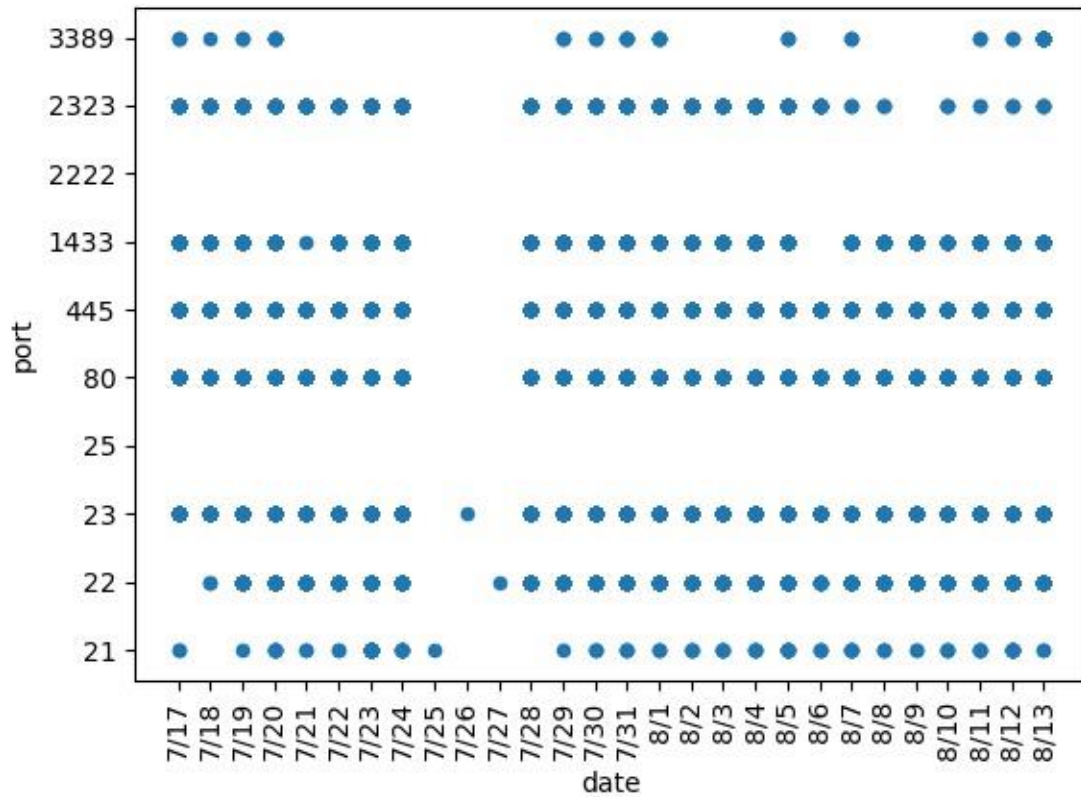
ホスト数, 1ホスト当たりの通信数ともに全ての日数においてProxyRackの方が多い

2、通信の宛先ポート

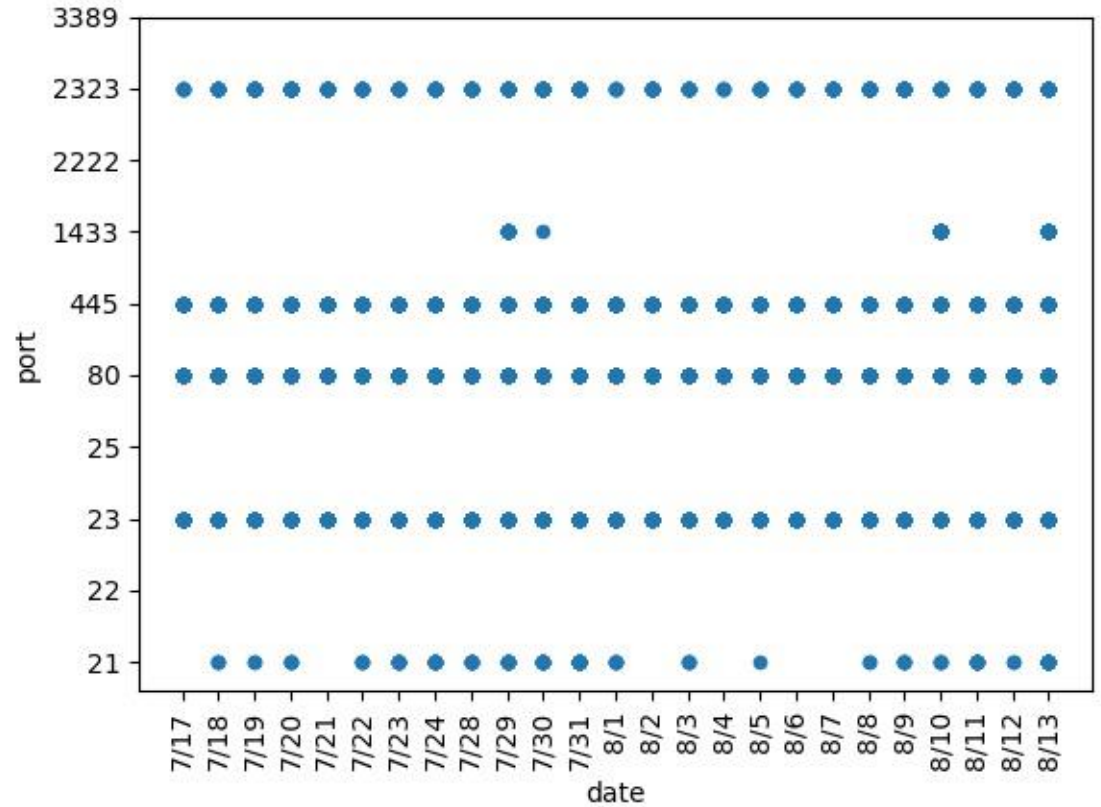
宛先ポート番号 (サービス)	ProxyRack		Bright Data		[半澤, 2021]	
	観測件数	[%]	観測件数	[%]	観測件数	[%]
21(FTP)	112	0	125	0.4	193,917	11.5
22(SSH)	38592	7.3	0	0	49,767	2.9
23(Telnet)	32300	6.1	4051	12.4	613,606	36.4
25(SMTP)	0	0	0	0	21,732	1.3
80(HTTP)	15150	2.9	2044	6.2	97,780	5.8
445(SMB)	19682	3.7	11284	34.5	399,250	23.7
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のホストはスキャン活動を、Bright Dataのホストは意図的な行動を行っている可能性がある

2、宛先ポートの変化



ProxyRack



Bright Data

ProxyRackのホストは継続的に各ポートに通信を行っており、ここからもスキャン活動を行っていると考えられる

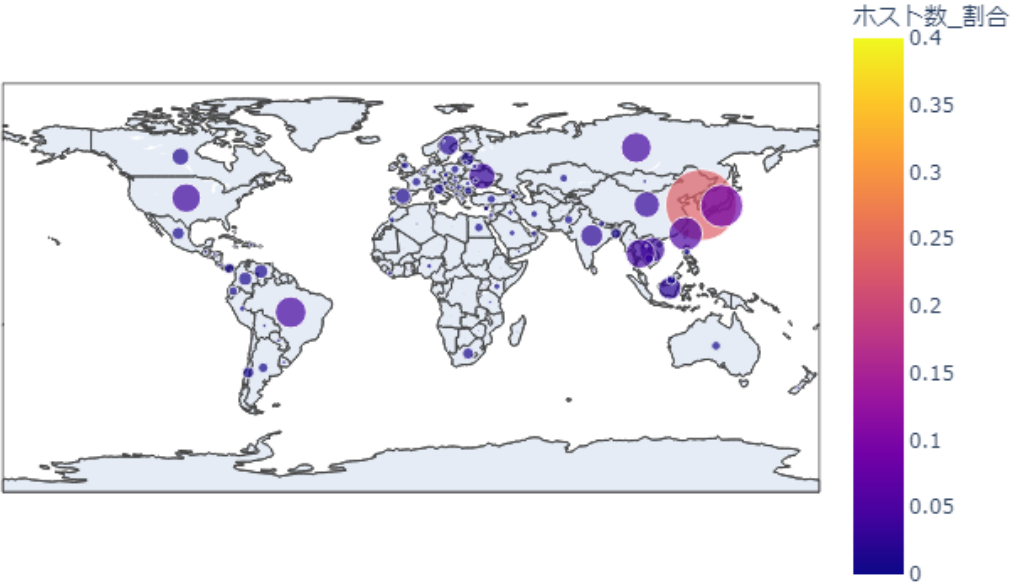
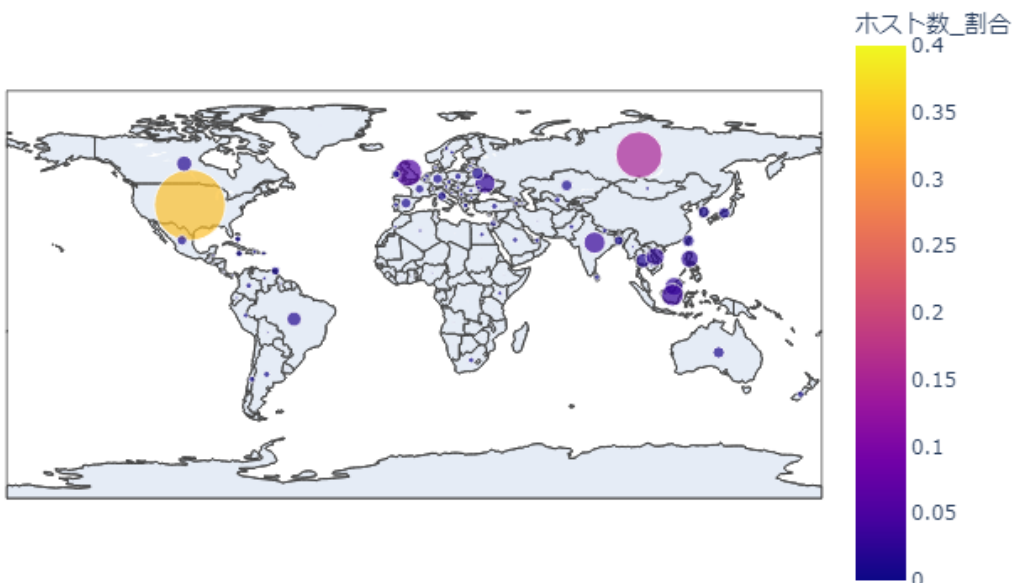
3、解放ポート

ポート番号	ProxyRack				Bright Data			
	不正IP数	[%]	悪質な不正IP数	[%]	不正IP数	[%]	悪質な不正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

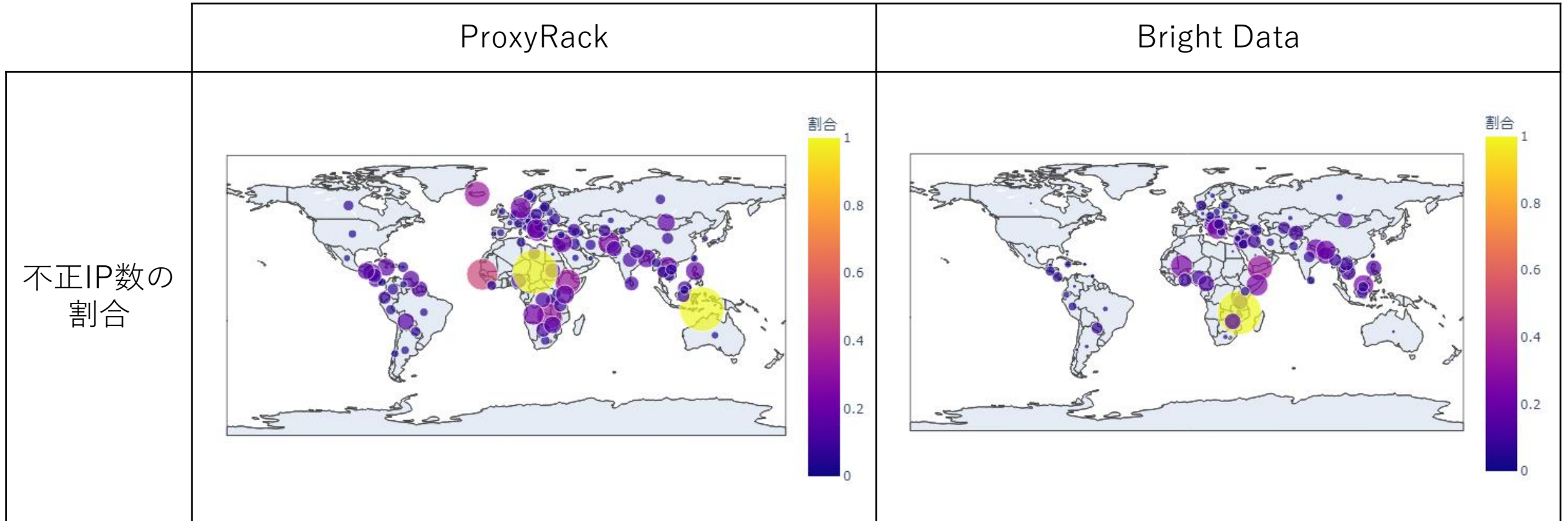
2000, 8291はMikroTik製ルータを標的とする攻撃の標的ポート、7545, 5555はMiraiが探索対象とするポートとして報告されている

→自発的でない外的な要因でホストにされている可能性がある

4、分布

	ProxyRack	Bright Data
RESIPホストの分布	 <p>ホスト数_割合 0.4 0.35 0.3 0.25 0.2 0.15 0.1 0.05 0</p>	 <p>ホスト数_割合 0.4 0.35 0.3 0.25 0.2 0.15 0.1 0.05 0</p>
	比較的アジア圏に集中している	比較的全世界に分布 アメリカ、ロシアなどに集中している

4、不正IP数の割合



両サービスともに全世界に不正なIPアドレスが分布しているが、ProxyRackの方が広く分布している

4、分布の比較

国名	ProxyRack		Bright Data	
	ホスト数	不正ホスト率 [%]	ホスト数	不正ホスト率 [%]
ブラジル	3151	3.9	1060	1.9
カナダ	1002	6.1	1214	0.6
インドネシア	1656	8.8	2415	7
インド	1647	11.8	2284	7.2
大韓民国	16114	1.9	695	0.7
ロシア連邦	2988	5.6	10578	3
タイ	2757	7.7	1058	3.9
台湾	3655	3.2	749	1.5
ウクライナ	2293	7	2104	2.1
アメリカ合衆国	2715	3.6	24258	0.05
ベトナム	2109	6.9	1677	4.2

両サービスの国別ホスト数TOP15に
共通して含まれている国

- 国別ホスト数TOP15か国中、11か国同じ国が含まれていた
- ホスト数、不正ホスト率には目立った共通点が見られなかった

まとめ

- RESIPホストのIPアドレスを収集し、RESIPサービスの不正利用の最新状況を明らかにした
 - 不正、悪性IPアドレスの割合
 - 不正通信を行っているホスト数、パケット数、宛先ポート
 - 不正IPアドレスでの解放ポート
 - 分布
- 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