Residential IP Proxyサービスに悪用される住宅用ホストの調査

半澤 映拓，菊池 浩明

明治大学大学院先端数理科学研究科

背景

- Fingerprinting技術の普及[1]によりサーバ側からのユーザの識別が容易になった
  - サービス利用者のユーザ層特定
  - Torブラウザ利用者の識別
  - 通信の検閲
  - スクレイピングのブロック

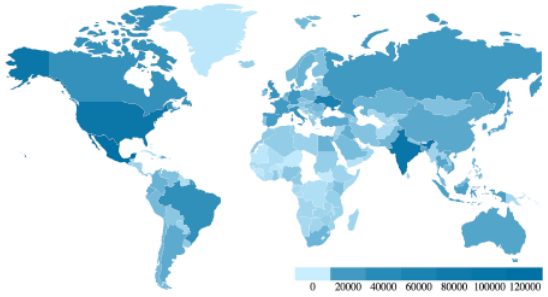
[1] 齋藤孝道,高須航,山田智隆,武居直樹,石川貴之,細井理央,安田昂樹,高橋和司,”Web Browser Fingerprint 技術の現状と課題”, コンピュータセキュリティシンポジウム2015, pp. 663-670, 2015

背景

- Fingerprintingの回避に対する需要からResidential IP Proxy（以下RESIPとする）をサービスする企業が出現
- 住宅用IPアドレスを利用したプロキシである
- RESIPはデータスクレイピングや複数アカウントの登録，ブロッキング回避を目的とするユーザが利用する
- 検閲により通信が制限される国でも利用される

問題点

- Miら[2]はRESIPサービスで提供されるIPアドレスを収集し，RESIPが不正行為を担う傾向にあると結論付けた



(b) RESIPs responded to our probings.

Top 1-5	# RESIPs	%
Spam	8,299	36.55%
Malicious URL	7,305	32.17%
Bruteforce	3,325	14.64%
Suspicious	629	2.77%
Dionaea	618	2.72%

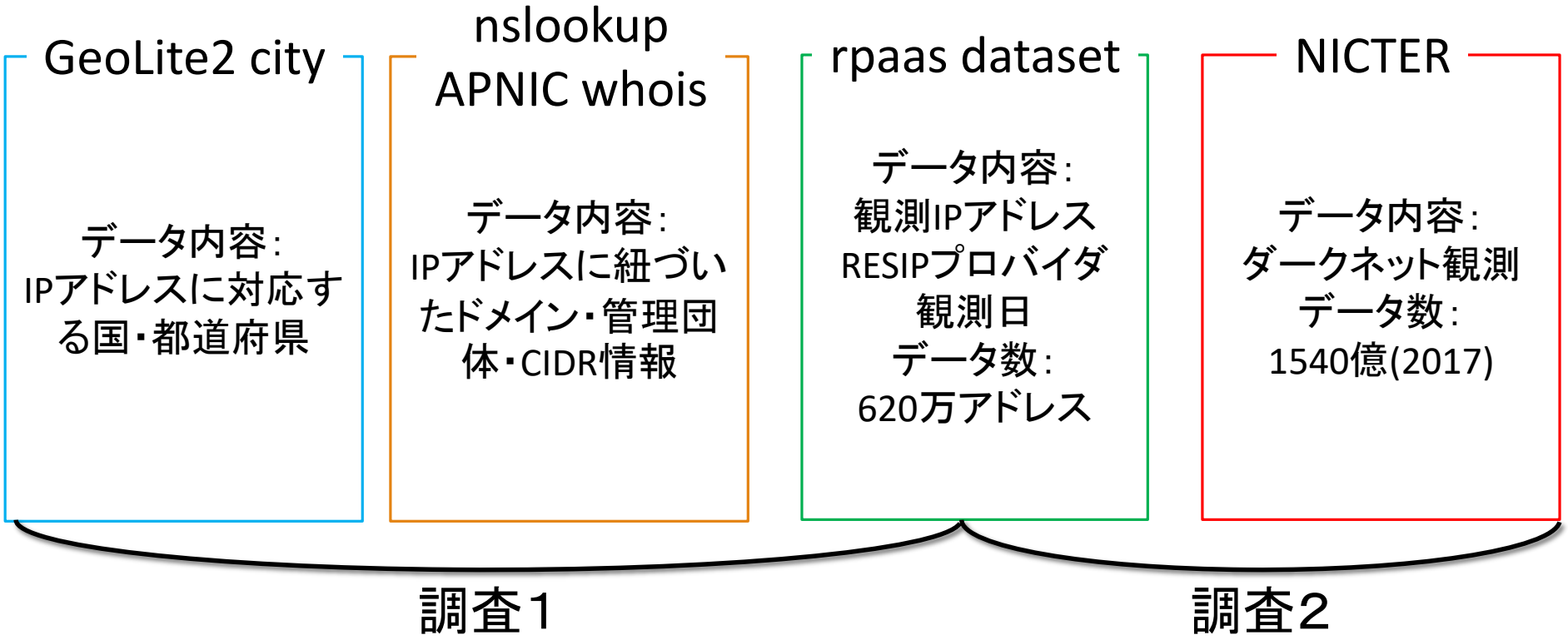
Device Type	Num	(%)
router	114,768	48.42
firewall	25,088	10.58
WAP	24,470	10.32
gateway	22,003	9.28
broadband router	17,358	7.32
webcam	13,024	5.49
security-misc	10,608	4.48
DVR	4,249	1.79
media device	2,589	1.09
storage-misc	1,988	0.84

[2]Xianghang Mi, Xuan Feng, Xiaojing Liao, Baojun Liu, XiaoFeng Wang, Feng Qian, Zhou Li, Sumayah Alrwais, Limin Sun, and Ying Liu. “Residential Evil: Understanding Residential IP Proxy as a Dark Service”, 2019 IEEE Symposium on Security and Privacy (SP), volume: 1, pp. 170-186, 2019.

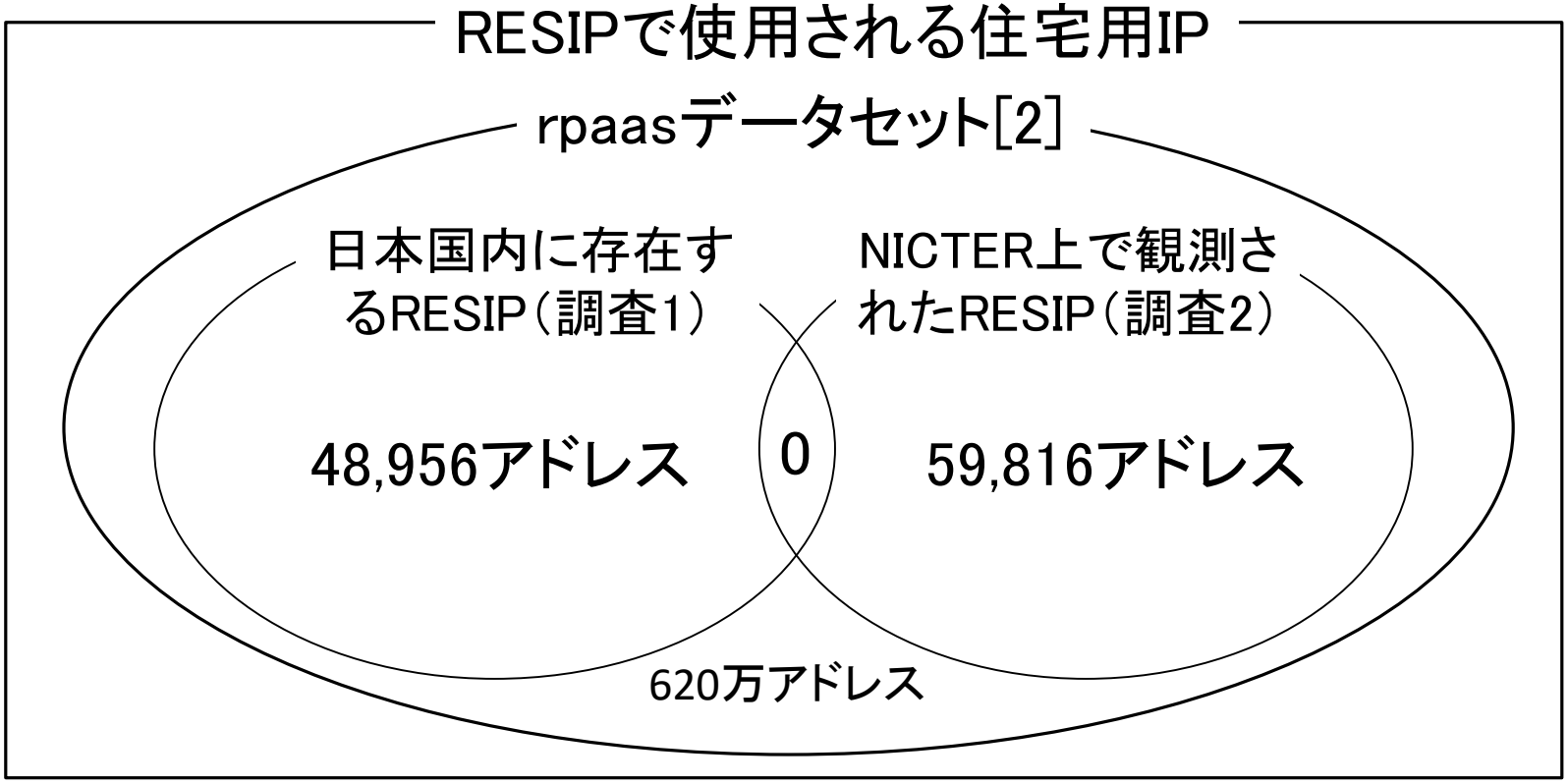
リサーチクエスチョン

- 課題
  1. RESIPホストとなっているのは本当にIoTデバイスなのか?
  2. RESIPホストが多い都道府県やISPはどこか?
  3. RESIPサービスの不正利用の目的は何なのか?

調査方法


GeoLite2 city
データ内容:
IPアドレスに対応する国・都道府県
nslookup
APNIC whois
データ内容:
IPアドレスに紐づいたドメイン・管理団体・CIDR情報
rpaas dataset
データ内容:
観測IPアドレス
RESIPプロバイダ
観測日
データ数:
620万アドレス
NICTER
データ内容:
ダークネット観測
データ数:
1540億(2017)
調査1
調査2

調査結果

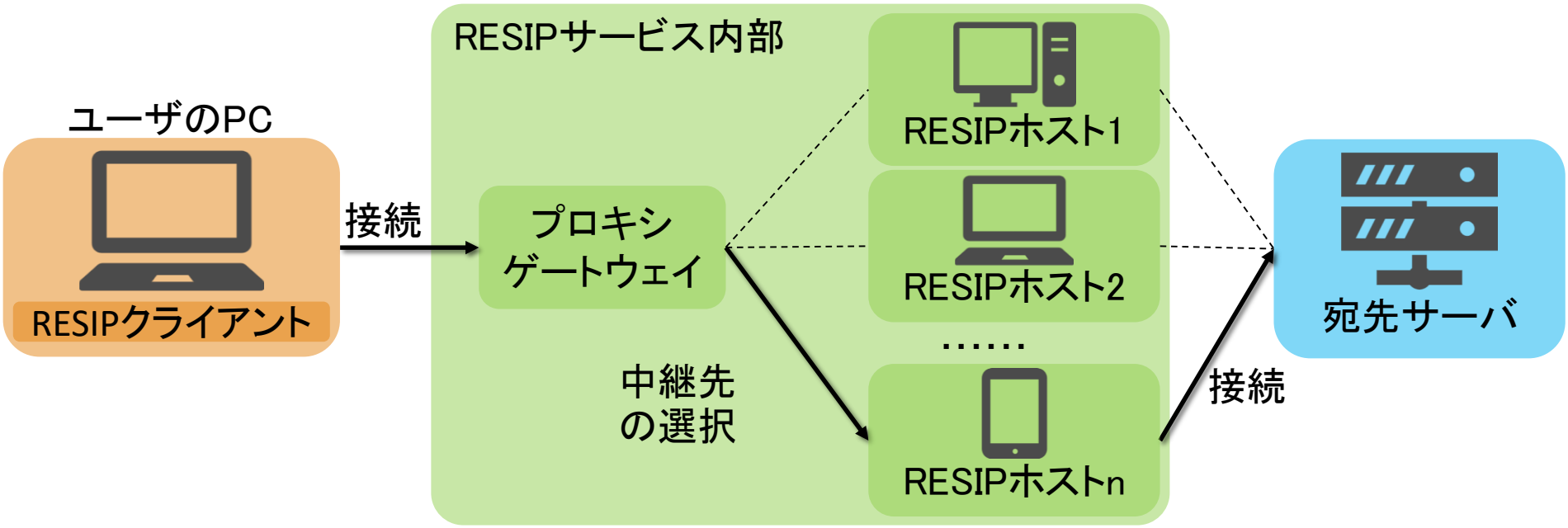

RESIPで使用される住宅用IP
rpaasデータセット[2]
日本国内に存在するRESIP（調査1）
NICTER上で観測されたRESIP（調査2）
48,956アドレス
0
59,816アドレス
620万アドレス

リサーチクエスチョンに対する結論

1. RESIPホストとなっているのは本当にIoTデバイスなのか?
   A.IoT機器ではなくモバイル機器ではないか
2. RESIPホストが多い都道府県やISPはどこか?
   A.47都道府県で観測され東京が最も多かった，ISPはNTT・KDDI・Softbankの順にRESIPホストが多かった
3. RESIPサービスの不正利用の目的は何なのか?
   A.168万件近くのスキャン行為が確認され，Telnetを標的としたものが最も多かった

133.26.240.58	2017/10/20	Luminati	ocha-mobile58-240.mind.meiji.ac.jp
133.11.114.249	2017/11/1	Luminati	g.h.u-Tokyo.ac.jp
133.70.80.19	2017/11/6	proxies	gw19.shizuoka.ac.jp

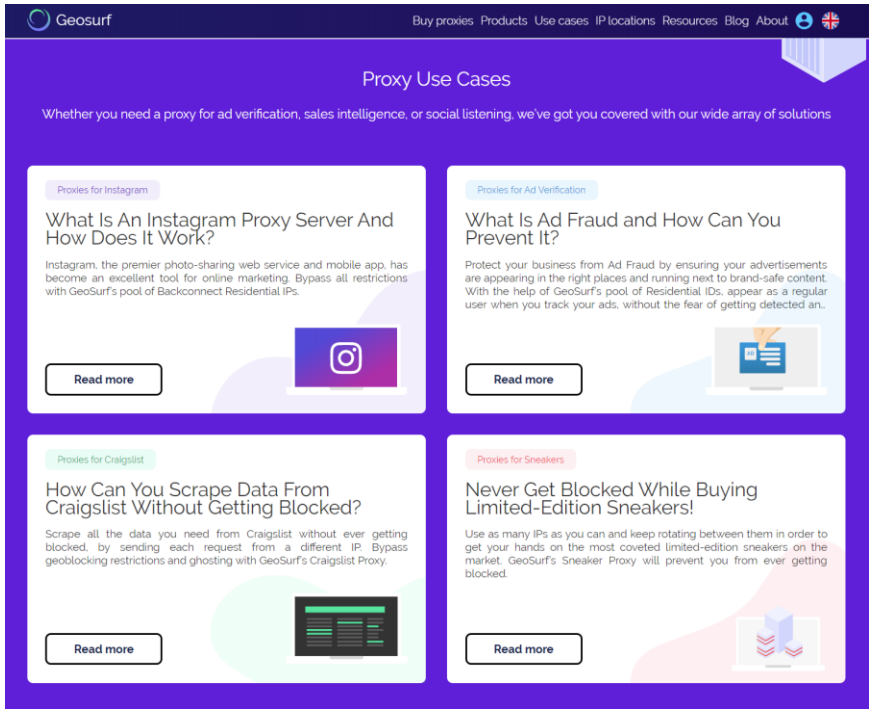
Residential IP Proxyサービス

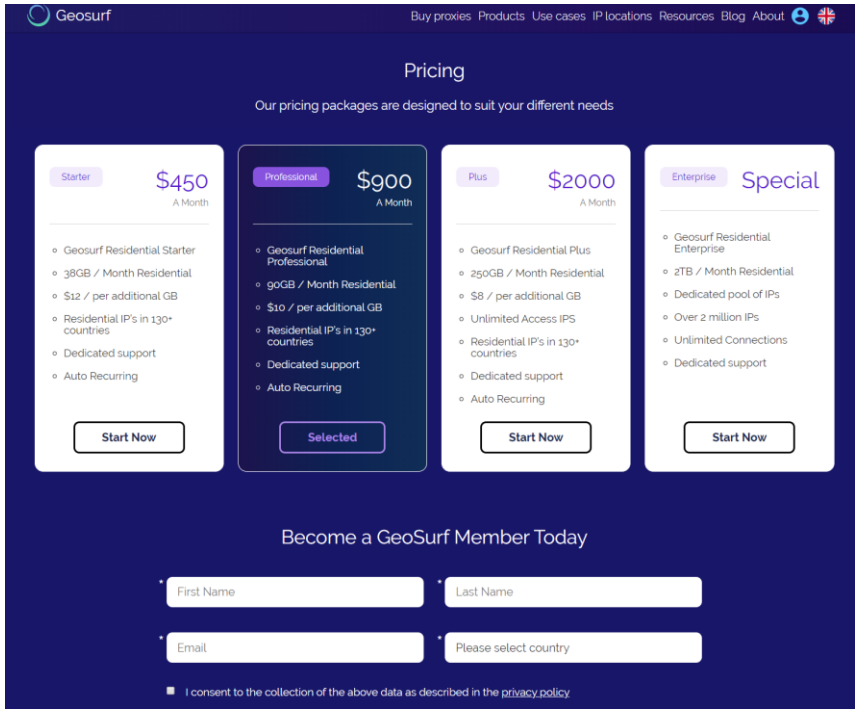


Residential IP Proxyサービス

- SOCKS4・5、HTTP/HTTPSに対応
- サインアップするとゲートウェイのIPアドレスかURLが渡される
- 中継に使用するIPアドレスの変更頻度はオプションで調整できる
- リゾルバDNSを変更するオプションもある

Residential IP Proxyサービス



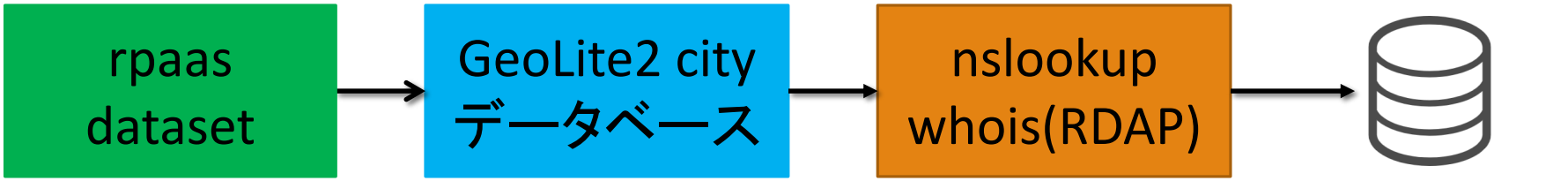


RESIPサービスの価格推移

- 価格が上昇している
- サービスやサイトの更新が終了している

RESIPプロバイダ	料金(2017)[2]	料金(現在)
Proxies Online(アメリカ)	$25/Gb	サイトの証明書切れ
Geosurf(オランダ)	$300/month	$450/month
ProxyRack(アメリカ)	$40/month	$80/month
Luminati(アメリカ)	$500/month	$12.5/GB+$500/month
IAPS Security(アメリカ)	$500/month	サービス停止

調査方法1:日本にあるRESIPホスト



- 都道府県

- ドメイン
- CIDR情報
- 管理団体

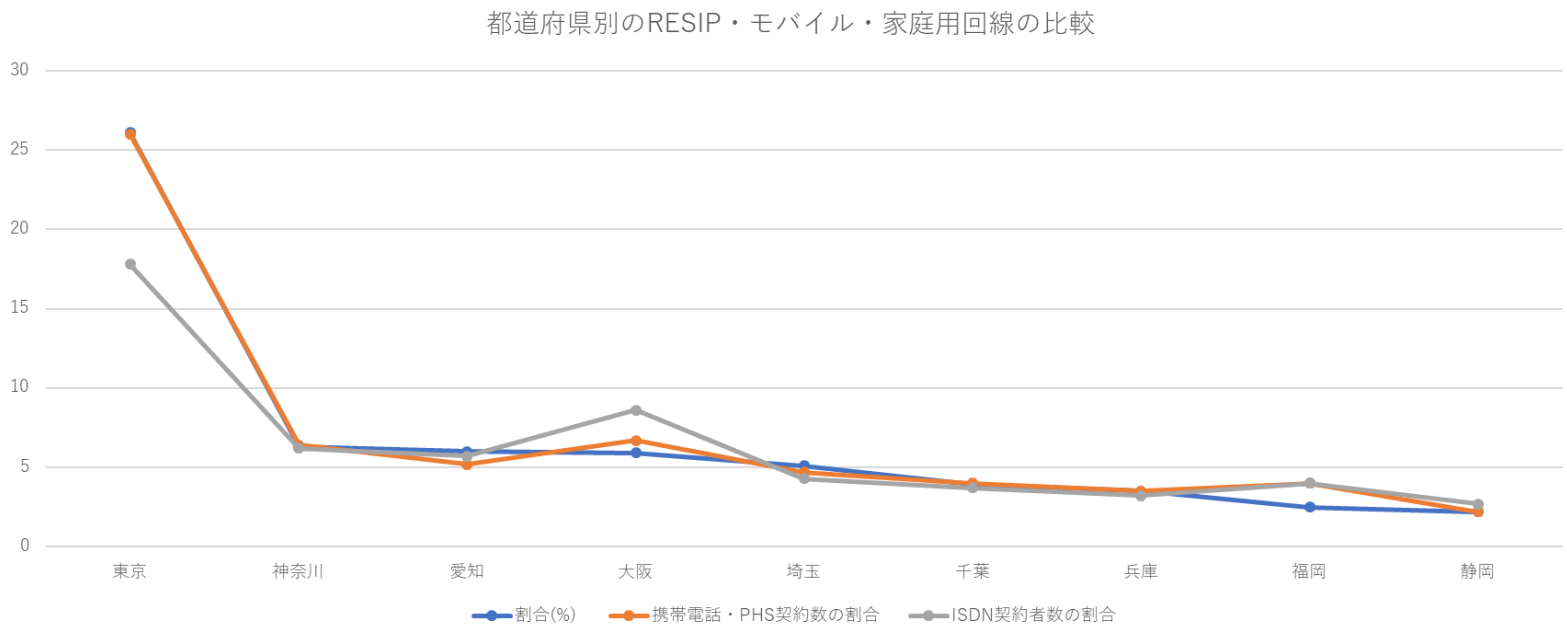
resip_jp.csv

調査結果1.1　都道府県別アドレス数

都道府県	RESIP ホスト数	割合(%)	携帯電話・PHS契約数の割合[3]	ISDN契約者数の割合[3]
東京	12,766	26.1	26.0	17.8
神奈川	3,094	6.3	6.4	6.2
愛知	2,940	6.0	5.2	5.7
大阪	2,917	5.9	6.7	8.6
埼玉	2,544	5.1	4.7	4.3
千葉	1,912	3.9	4.0	3.7
兵庫	1,722	3.5	3.5	3.2
福岡	1,266	2.5	4.0	4.0
静岡	1,083	2.2	2.2	2.7
not found	6,619	13.5		
計	48956	100	100	100

[3] テレコムデータブック2018(TCA編), https://www.tca.or.jp/databook/pdf/2018chapter_2j.pdf

調査結果1.1　都道府県別アドレス数



各都道府県の占めるRESIPの割合は携帯電話・PHS契約者数の割合と近い
→モバイル用ISPがRESIPホストとなっているのではないか

調査結果1.2　ドメイン別アドレス数

ドメイン	アドレス数	割合
ocn.ne.jp	7,468	15.2
au-net.ne.jp	5,616	11.4
plala.or.jp	2,900	5.9
dion.ne.jp	2,528	5.1
not found	2,441	4.9
so-net.ne.jp	1,966	4.0
mesh.ad.jp	1,935	3.9
eonet.ne.jp	1,305	2.6
home.ne.jp	1,209	2.4
nttpc.ne.jp	1,116	2.2
計	48,956	100

2LD	アドレス数	割合
ne	28,824	74.1
or	4,340	11.1
ad	2,208	5.6
ac	91	0.2
co	9	
go	1	
gr	1	
ed	1	
計（.jp）	38,946	100

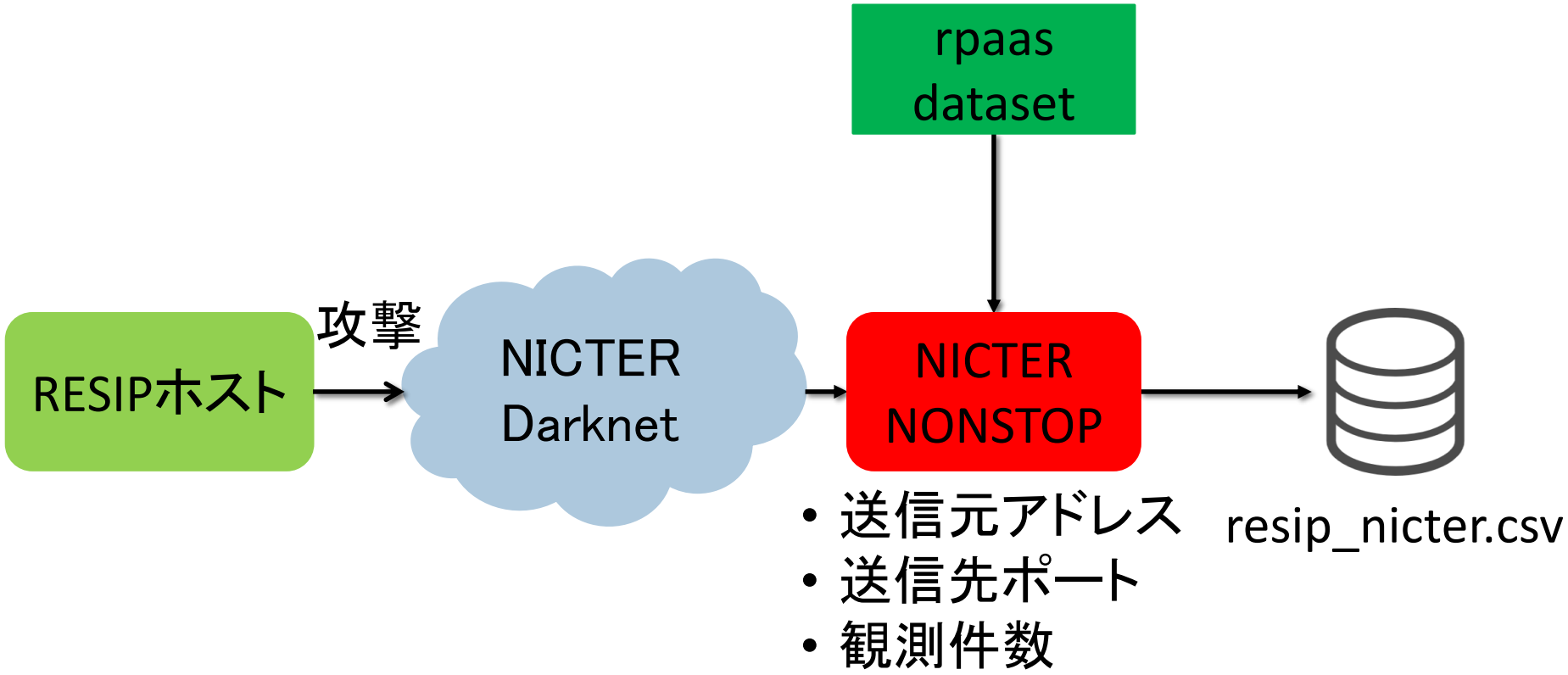
90.8%

90.8%が個人用ドメインである

調査結果1.3　管理団体別アドレス数

管理団体	アドレス数	割合(%)	FTTH契約数のシェア
NTT Communications Corporation	10941	22.3	34.2
KDDI CORPORATION	8301	16.9	12.8
Japan Nation-wide Network of Softbank Corp.	7781	15.8	
Japan Network Information Center	4756	9.7	
Sony Network Communications Inc.	2544	5.1	
OPTAGE Inc.	1274	2.6	5.4
BIGLOBE Inc.	1230	2.5	
Jupiter Telecommunication Co. Ltd	1209	2.4	
Chubu Telecommunications Co.,Inc.	1125	2.2	
ARTERIA Networks Corporation	965	1.9	2.3
計	48956	100	

調査方法2:NICTERでのRESIP観測



調査結果2.1:観測数上位10件のRESIPホスト

送信元アドレス	先行研究での観測日数	プロバイダ	観測件数
43.249.57.255	8	ProxyRack	62,669
187.120.17.2	34	Proxies Online, Geosurf	35,353
200.170.223.50	7	Luminati	21,676
103.29.97.2	8	Proxies Online, Geosurf, Luminati	17,004
165.73.122.29	14	Luminati	16,127
212.90.62.209	5	Luminati	15,142
43.248.73.6	90	Proxies Online, Geosurf, Luminati	13,425
190.57.236.230	18	Luminati	13,388
112.196.77.202	27	Proxies Online, Geosurf	13,061
125.99.100.22	10	Proxies Online, Luminati	12,952

調査結果2.2:不正利用の目的

送信先ポート番号	サービス	観測件数	割合(%)
23	Telnet	613,606	36.4
445	SMB	399,250	23.7
21	FTP	193,917	11.5
1433	MSSQL	144,928	8.6
80	HTTP	97,780	5.8
22	SSH	49,767	2.9
2323	(Telnet)	43,310	2.5
25	SMTP	21,732	1.3
2222	(SSH)	16,838	1.0
3389	RDP	9,782	0.5

IoT機器を標的とした攻撃

spamメール

結論

- 日本に存在したRESIPホストは48,956個　そのうち90.8%が住宅用ホスト
- 日本においてRESIPホストとなっているのはモバイルデバイスである可能性が高い
- 47都道府県全てにRESIPが存在していた
- 都道府県別，ISP別のRESIPの分布は各都道府県でのモバイルデバイスの割合やISPごとのシェアの順位と一致していた
- NICTER Darknet上で1,683,550件のスキャン行為が観測された

不審な.ruドメインが43件 RIPE whoisではイスラエル

46.161.57.130	2017/10/23	proxyrack	pinspb.ru
46.161.57.189	2017/9/20	proxyrack_geosurf	pinspb.ru