2021年2月12日
修士論文発表会

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

菊池研究室

背景

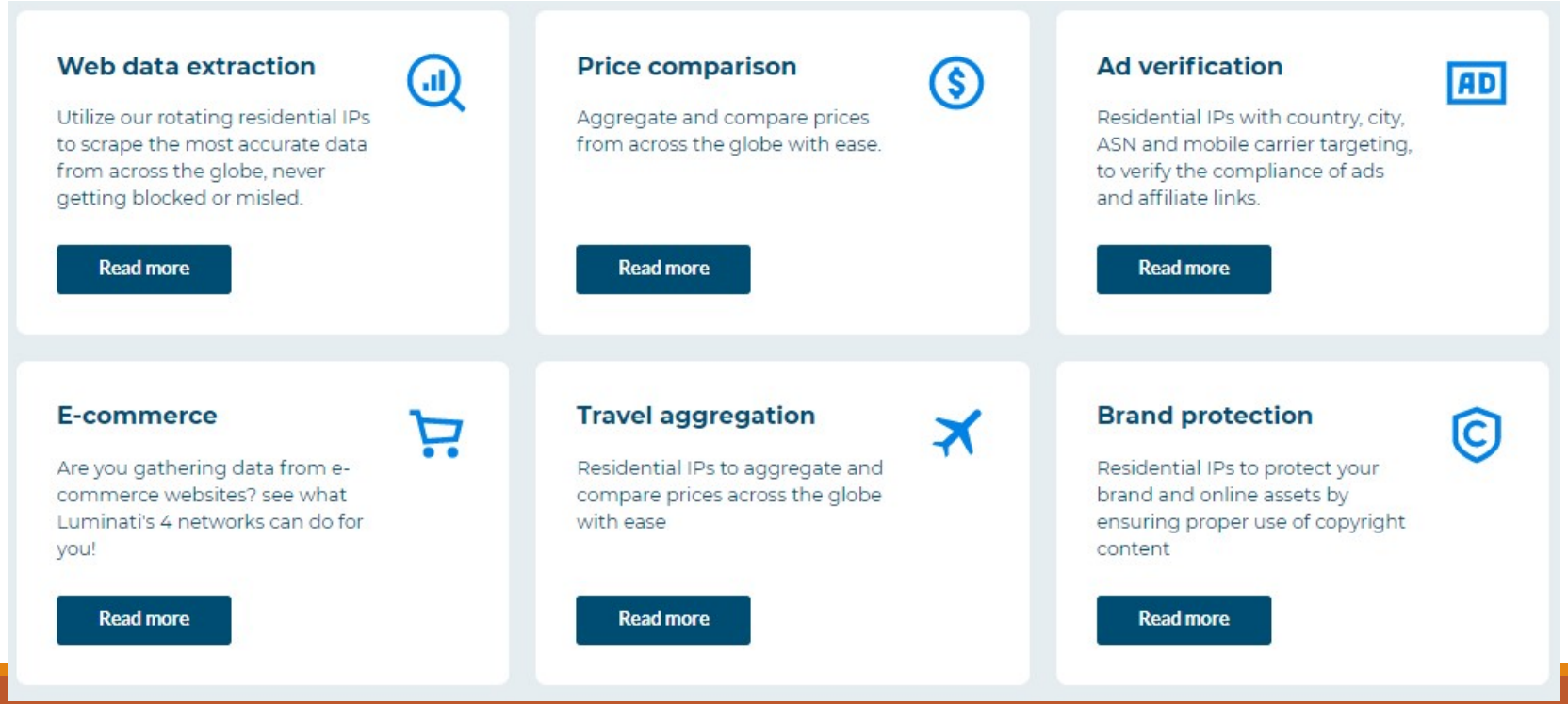
Residential IP Proxy（以下RESIPとする）をサービスする企業の出現

- サーバ側からのユーザの識別，通信の検閲への回避に対する需要
- RESIP：住宅用ネットワークのホストを利用したプロキシ

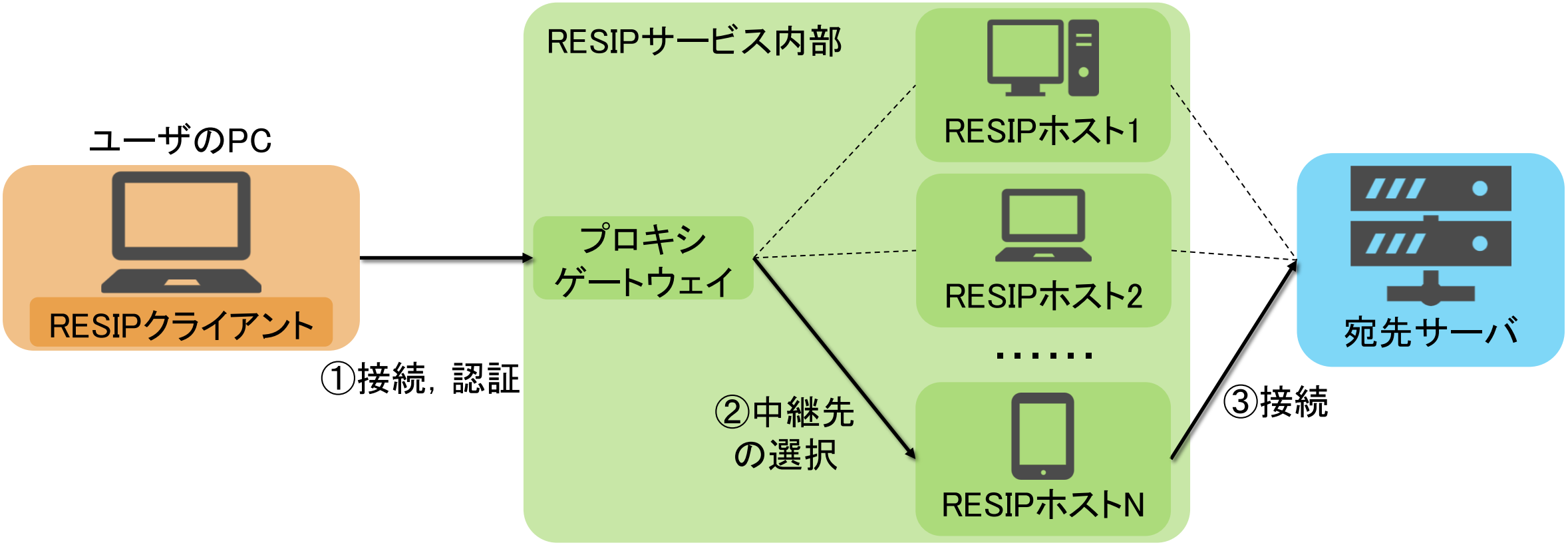
Geosurf

Luminati

proxyrack



Residential IP Proxyのサービスモデル



RESIPサービスの問題点

Miら[1]はRESIPサービスで提供される全世界のRESIPホストの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

Top 1-5	# RESIPs	%	Top 6-10	# RESIPs	%
Spam	8,299	36.55%	Malicious Sample	438	1.93%
Malicious URL	7,305	32.17%	Zombie	277	1.22%
Bruteforce	3,325	14.64%	Telnet	249	1.10%
Suspicious	629	2.77%	Trojan	171	0.75%
Dionaea	618	2.72%	EDROP	164	0.72%

TABLE III: Malicious activities related to RESIPs.

Device Type	Num	(%)	Device Vendor	Num	(%)
router	114,768	48.42	MikroTik	86,593	36.53
firewall	25,088	10.58	Huawei	37,545	15.84
WAP	24,470	10.32	BusyBox	18,337	7.74
gateway	22,003	9.28	Technicolor	16,866	7.12
broadband router	17,358	7.32	SonicWALL	14,122	5.96
webcam	13,024	5.49	Fortinet	9,190	3.88
security-misc	10,608	4.48	Dahua	6,258	2.64
DVR	4,249	1.79	ZyXEL	5,601	2.36
media device	2,589	1.09	AVM	5,272	2.22
storage-misc	1,988	0.84	Cyberoam	4,558	1.92

TABLE IV: List of the top 10 device vendors and device types.

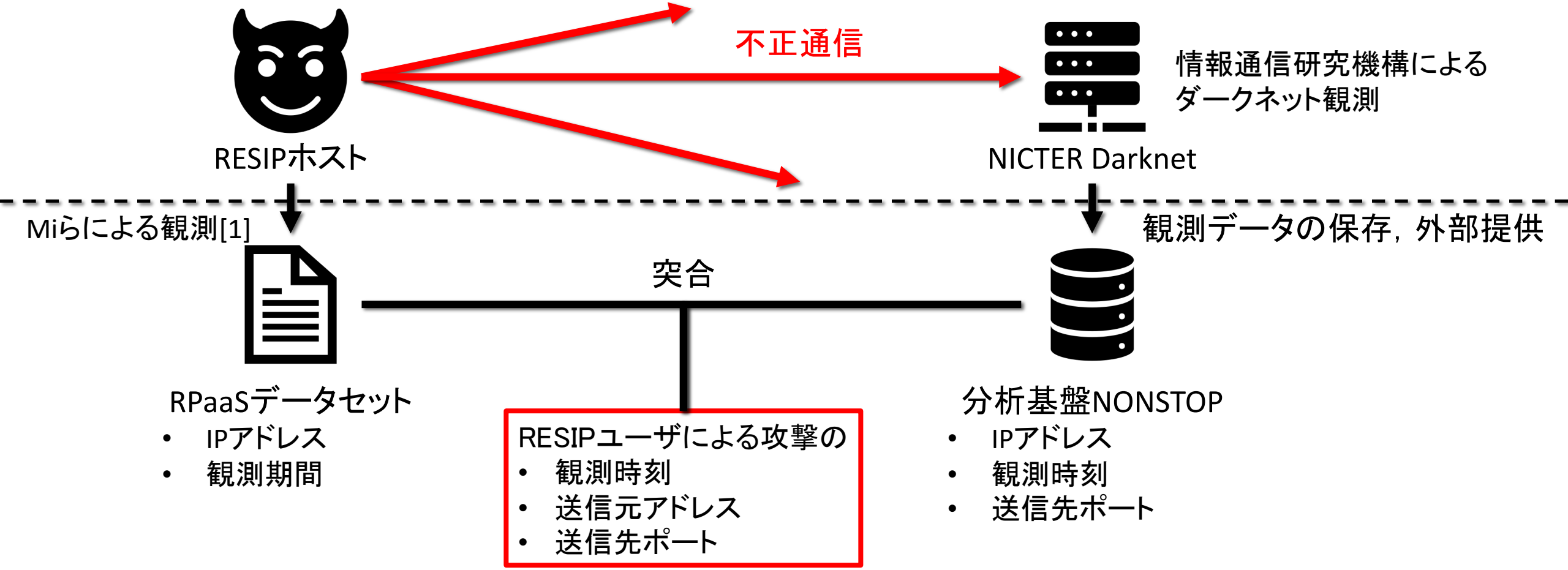
[1]Xianghang Mi, Xuan Feng, Xiaojing Liao, Baojun Liu, XiaoFeng Wang, Feng Qian, Zhou Li, Sumayah Alrwais, Limin Sun, and Ying Liu. “Residential Evil: Understanding Residential IP Proxy as a Dark Service”, 2019 IEEE Symposium on Security and Privacy (SP), volume: 1, pp. 170-186, 2019.

リサーチクエスチョン

1. RESIPサービスを利用した不正通信は日本のネットワークに到達しているのか，どのようなサービスが標的となっているのか
   →RESIPユーザによる不正通信の調査

2. RESIPホスト上で展開されているWebページからホストとなっている機器の特徴を明らかにできないか
   →RESIPホスト上のWebページの調査

調査手法1 RESIPユーザによる不正通信



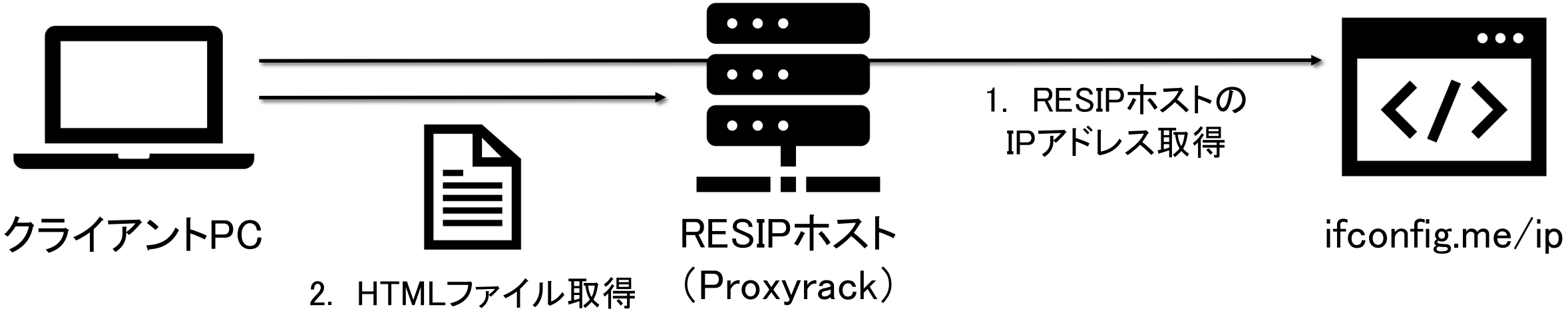
調査結果1 不正通信の送信先ポート

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
23	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)	16,836	1.0
3389	RDP	9,782	0.5
計		1,683,550	100

先行研究[1]での順位	悪性行動種別	割合(%)
1	Spam	36.55
2	Malicious URL	32.17
3	Bruteforce	14.64
4	Suspicious	2.77
5	Dionaea	2.72
6	Malicious Sample	1.93
7	Zombie	1.22
8	Telnet	1.10
9	Trojan	0.75
10	EDROP	0.72

- 59,816のホストからの168万の不正通信が観測された
- SpamよりもTelnetの方が多く観測された

調査手法2 RESIPホスト上のWebページ



観測期間	観測ホスト数	取得したHTMLソースコード数	ベンダが明らかになったホスト数
2020/11/12-2020/11/27	9,316	1,097	333

取得したHTMLソースコードの例

```
<div id="container">

  <div id="box">
  <a href="http://mikrotik.com"><img src="mikrotik_logo.
  <br style="clear: both;"/>
        <h1>RouterOS v6.45.9</h1>
    <p>You have connected to a router. Administrative acc
```

デバイスベンダが記載されている例

```
<html>
  <head>
  <title>RV-230SE</title>
  <meta http-equiv="content-type" content="text/html;cha
  <meta http-equiv="expires" content="0">
  <meta http-equiv="pragma" content="no-cache">
  <meta http-equiv="Content-Style-Type" content="text/cs
  <link rel="stylesheet" type="text/css" href="/css/commo
</head>
```

デバイスの型番が記載されている例

調査結果2　観測されたデバイスベンダ

順位	デバイスベンダ	観測件数	割合(%)
1	Cambium Networks	93	27.9
2	Parks Comunicações	52	15.6
3	Zyxel Networks	35	10.5
4	TP-Link Technologies	30	9.0
5	KT	26	7.8
6	Huawei Technologies	16	4.8
7	Mercury	14	4.2
8	Belkin(Linksys)	10	3.0
9	Comcast(Xfinity)	7	2.1
10	Buffalo	6	1.8
計		333	100

先行研究の手法[2]では明らかにならないデバイスベンダ

先行研究[1]での順位	デバイスベンダ	割合(%)
1	MikroTik	36.53
2	Huawei	15.84
3	BusyBox	7.74
4	Technicolor	7.12
5	SonicWALL	5.96
6	Fortinet	3.88
7	Dahua	2.64
8	ZyXEL	2.36
9	AVM	2.22
10	Cyberoam	1.92

[2]Nmap service detection probe list, https://svn.nmap.org/nmap/nmap-service-probes, 2020

まとめ

- 59,018のRESIPホストから日本のネットワークに168万件以上の不正通信が到達していることを明らかにした
- 不正通信の主な目的は先行研究と異なり，Telnet(36.4%)だった

- 9,316のRESIPホスト上で展開されているWebページを解析し，333のホストのデバイスベンダを明らかにした
- 先行研究の手法では観測されないデバイスベンダ(Cambium Networks, Parks Comunicações，KT)を観測した