明治大学大学院　先端数理科学研究科

2020 年度

修士学位請求論文

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

学位請求者　先端メディアサイエンス専攻

半澤　映拓

目 次

第1章　序論

1.1　本研究の背景

近年，Fingerprinting 技術 [1] の普及により，サーバ側からユーザの識別やブロッキングが容易になってきた．Fingerprinting とは，ユーザがブラウザから Web サーバへアクセスした際に，Web サーバ側が通信元 IP アドレスや使用ブラウザ，使用端末に関する情報を取得し，ユーザを識別する技術である．Web サイトの運営者や Web 広告企業は Fingerprinting の結果から得られたユーザの居場所や興味の対象を広告のターゲッティングに利用している．また通信を検閲し，ユーザのインターネットアクセスを制限している地域が存在することが知られている．例として，中国，イラン，オマーン，カタール，クウェートでは I2P Project の Web ページ [2] へのアクセスがブロックされている [3].

Fingerprinting や検閲の回避に対する需要から，住宅用の IP アドレスを利用したプロキシである Residential IP Proxy(以下 RESIP とする) をサービスする企業が出現した．RESIP サービスの主要な顧客は，データスクレイピング等を目的とした膨大なアクセスを行うユーザや自国内のネットワークの利用が制約されているユーザである．RESIP サービスは住宅用ネットワークにあるホストをプロキシとして提供している．サービスプロバイダは住宅用 IP アドレスを保有する人々が「自発的に」ホストを提供していると主張している．RESIP は従来のプロキシや匿名ネットワークと同様の匿名通信を提供するのに加え，接続先サーバからの検出やブロッキングに耐性を持つ.

しかしながら，RESIP サービスはアクセス制限の回避だけに使われる訳ではない.

匿名通信路 Tor と同様に送信元を秘匿することができる上に，RESIP サービスでプロキシとして提供されている住宅用ホストの大半はブラックリストに登録されていない．これらの特徴から，身元を秘匿したままでの，SPAM の送信，不正アクセスのための脆弱なホストを探索するポートスキャン，DoS 攻撃などにも悪用されている．RESIP プロバイダは不正利用について言及していないが，悪意のあるクライアントに中継 IP アドレスの短時間での変更を提供しており，トレースされにくくしているため，問題となっている.

Mi らは 2017 年に RESIP サービスで提供されるホストの IP アドレスを収集し，RESIP サービスの基盤・規模を明らかにした [4]．95%の RESIP ホストが住宅用に割り当てられた IP であり，その 43%が IoT 機器であると報告している．これらを根拠に，RESIP が不正行為を担う傾向にあると結論付けた.

1.2　本研究の目的

RESIP サービスはプロバイダや中継点を提供しているホストについて，現在もその実態が不明な点が多い．Mi らの研究では RESIP ホストとなっているのは IoT 機器であること，日本にも RESIP

ホストが設置されていることが報告されている．

これらのことから RESIP サービスに対して次の疑問がわく．

1. 日本にある RESIP ホストはどんなネットワーク環境のホストが利用されているのか?住宅のみか，企業や大学にはないか?
2. どのインターネットサービスプロバイダやどの県のユーザが RESIP ホストになっているのか?地域やプロバイダに差はあるのか?
3. 日本のネットワークは RESIP を利用した不正通信の脅威にさらされているのか?
4. RESIP サービスが不正利用されている場合，その実態はどうなっているのか?
5. 現在の RESIP サービスを取り巻く環境はどうなっているのか?Mi らが RESIP ホストの情報を収集した 2017 年から変化しているのか?
6. Mi らはデバイスへのポートスキャンに対する応答からデバイスタイプとベンダを推測していたが，IoT 機器の Web インターフェイスからデバイスベンダを明らかにすることはできないのか?

これらの問に答えることが本研究の目標である．

1.3 研究方法

1，2 を明らかにするには，RESIP として用いられている IP アドレスを調べる必要がある．本研究では，Mi らが収集した RESIP ホストのデータセット [7] について，Maxmind 社の提供する GeoLite2 city データベース [8] と Asia-Pacific Network Information Centre(APNIC) の提供する Registration Data Access Protocol(RDAP) サービス [9] を用いて，2017 年に日本に存在していた RESIP ホストが所属する都道府県・機関・プロバイダについて明らかにする．

3，4 を明らかにするには，RESIP の IP アドレスによる不正行為を検出しなくてはならない．本研究では，情報通信研究機構の提供する分析基盤 Nicter Open Network Security Test-Out Platform (NONSTOP)[11] を用いて，先行研究が実施された 2017 年に RESIP ホストから日本のネットワークに送信されたパケットについて調査を行う．その結果から RESIP を利用するクライアントがどのようなサービスを標的とする傾向があるのかを明らかにすることを試みる．

5，6 を明らかにするには，RESIP サービスを契約し RESIP ホストの情報を収集する必要がある．本研究では 2020 年 2 月から 11 月の 9ヶ月間，RESIP サービスを契約して RESIP ホストの IP アドレスと Web インターフェイスで提供される HTML ソースコードを収集し，分析を行った．その結果から RESIP サービスを取り巻く環境の現状と RESIP ホストとなっている機器のデバイスベンダを明らかにすることを試みる．

1.4 本研究の新規性

本研究の新規性は以下の 3 つである．

- 日本国内に存在する RESIP ホストの詳細な所在と管理団体を明らかにしたこと．
- RESIP サービスを利用した実際の攻撃から RESIP の不正利用の事態を明らかにしたこと．
- RESIP サービスを契約し，RESIP ホストとなっている機器の Web インターフェイスからデバイスベンダを明らかにしたこと．

1.5 本稿の構成

本稿は 8 章で構成される．

1 章では本研究の背景と目的を述べた．

2 章では本稿の基本定義と先行研究について述べる．

3 章では本研究で使用したデータセット・データベースを説明する．

4 章では Mi らの研究で観測された RESIP ホストのうち，日本国内に存在するホストに対する調査について結果を述べる．

5 章では NICTER のダークネット上で観測された RESIP ホストが行っている不正通信の調査について結果を述べる．

6 章では RESIP サービスを利用した内部からの RESIP ホストの調査について結果を述べる．

7 章では RESIP ホスト上で展開されている Web ページの調査について結果を述べる．

8 章では本研究の結論を述べる．

第2章　基本定義と従来研究

2.1　基本定義

2.1.1　Residential IP Proxy

表 2.1: RESIP サービスの価格推移

RESIP プロバイダ	料金 (2017 年)	料金 (2020 年)
Proxies Online(アメリカ)	$25/Gb	証明書切れ
Geosurf(オランダ)	$300/月	$450/月
ProxyRack（アメリカ）	$40/月	$80/月
Luminati(アメリカ)	$500/月	$12.5/GB+$500/月
IAPS Security	$500/月	サービス停止

RESIP サービスは住宅用 IP による通信の中継を提供するサービスである．

RESIP サービスのモデルを図 2.1 に示す．RESIP サービスの主要部分はクライアント，プロキシゲートウェイ，住宅用ホストの 3 つで構成される．RESIP ユーザはサービスの利用登録をしたのち，RESIP クライアントからプロキシゲートウェイへ接続するための IP アドレス，または URL を受け取る．ゲートウェイはクライアントからの通信を定期的に異なる住宅用 IP へと割当て，通信する．接続先サーバからの応答は住宅用 IP アドレスを経由してクライアントへと返される．中継に使用されるホストの変更頻度はオプションで調整できるようになっている．RESIP サービスによってはリゾルバ DNS を変更するオプションを有しているものもある．

RESIP サービスは動的な IP アドレスによる通信の中継への需要の高まりとともにその市場規模を拡大している．その現状を示す価格の推移を表 2.1 に示す．Mi らの研究 [4] で調査が行われた 2017 年と現在の Residential IP Proxy プロバイダの利用価格を比較すると，Geosurf，Proxyrack，Luminati の 3 つのプロバイダで価格が上昇していることがわかる．一方で Proxies Online，IAPS Security はすでにサービスが終了している．このことから市場の競争が激しいことが伺える．

2.1.2　ダークネット観測

ダークネットはインターネット上で到達可能かつ未使用の IP アドレス空間である．

本来であれば未使用の IP アドレスに対する通信は存在しないはずだが，実際は膨大な数の通信が到達しており，その多くはマルウェア感染機器による次の標的のスキャンや送信元 IP アドレスを詐称した攻撃者に DDoS 攻撃を受けたサーバの応答であるバックスキャッタなどの，攻撃者による不正

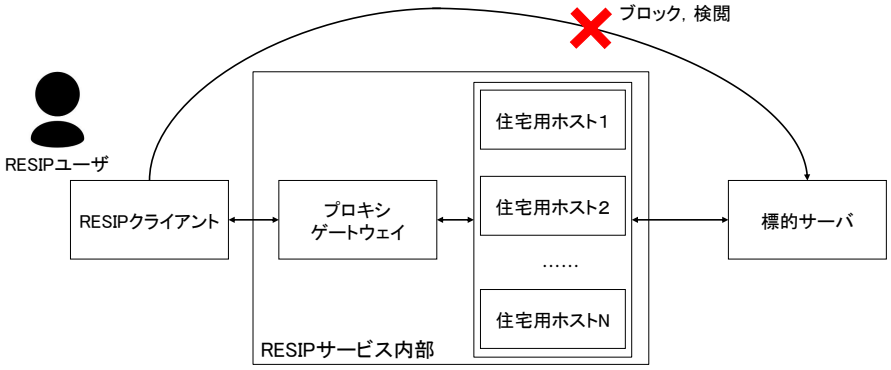

図 2.1: RESIP サービスのシステム概要図

な通信に起因するものである．ダークネットに到達する通信の分析を行うことで，攻撃者の特徴や標的とするサービス，流行しているマルウェアの種類といった情報を探ることができる．

ダークネット観測を行うにあたって，センサと呼ばれるパケット収集・応答用マシンを未使用 IP アドレスに設置する．センサには送信元に対する応答により種類がわけられる．ブラックホールセンサは到達するパケットに対して応答を返さない．低インタラクションセンサは攻撃の詳細な情報を得るために，既知の脆弱性を有するデバイスの擬態をする設定や特定の通信に対してあらかじめ決まった応答を返す設定がなされている．高インタラクションセンサは実際のマシンかそれと同等の応答を返すセンサで，マルウェア感染時の挙動や攻撃者が不正アクセスに成功した後の動きといった情報まで取得することができる．ただし，センサのインタラクションが高度になるほど運用の難易度やコストが上昇するため，設置規模とのバランスを考慮する必要がある．

2.2 従来研究

2.2.1 Residential IP Proxy

Mi らは RESIP サービスに使用される住宅用 IP を収集するフレームワークを構築し，6,183,876 個の RESIP のアドレスを収集した [4]．収集した RESIP アドレスに対して住宅用 IP であるかの識別を行う分類器と RESIP アドレスに接続されている機器や生存時間の情報を収集するプロファイラを構築し，RESIP で使用される IP アドレスの分析を行った．その結果を図 2.2 に示す．収集した IP アドレスの 95.22%が住宅用の IP アドレスであると判定された．収集したアドレスのうち 547,497 個の IP アドレスについて接続されているデバイスとベンダ情報を調査し，237,029 個 (43.2%) の IP アドレスに IoT 機器が接続されていると結論付けた．

RESIP サービスのプロバイダは住宅用 IP が保有者によって「自発的に」提供されていると主張している．Mi らの研究ではプロバイダがどのようにして住宅用 IP アドレス提供者を募っているのか調

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

図 2.2: 先行研究の調査結果 [4]

査を行った．Luminati[1]では住宅用 IP アドレスを提供することで他の住宅用 IP アドレスをプロキシとして利用できるサービスを得られるプランを提供することで住宅用 IP アドレス提供者を募っていたことが明らかになった．しかし，その他の RESIP プロバイダが提供者を募る方法に関しては解明されなかった．

2.2.2 NICTER Darknet

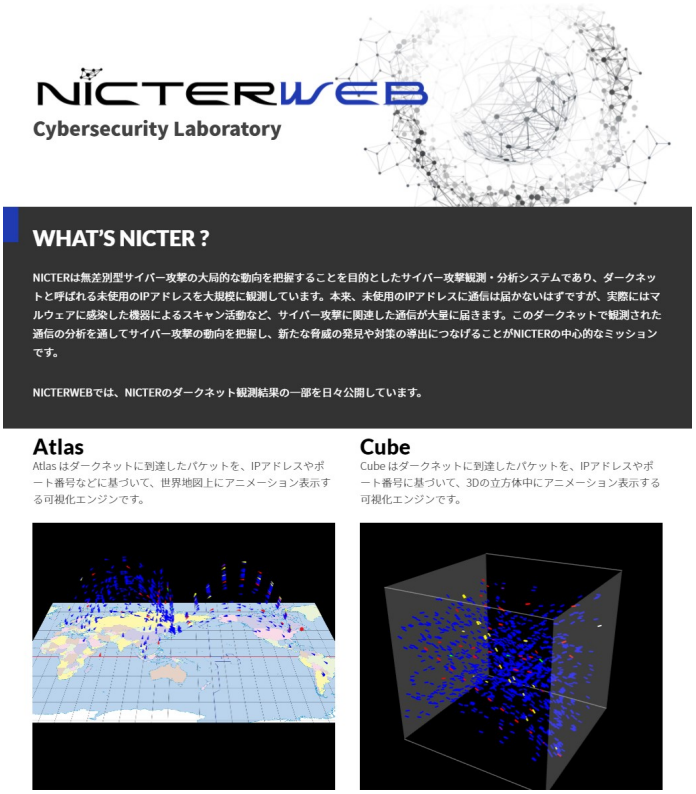

図 2.3: NICTER の Web ページ

[1]Luminati: largest business proxy service., http://luminati.io/，2021.02.13 参照.

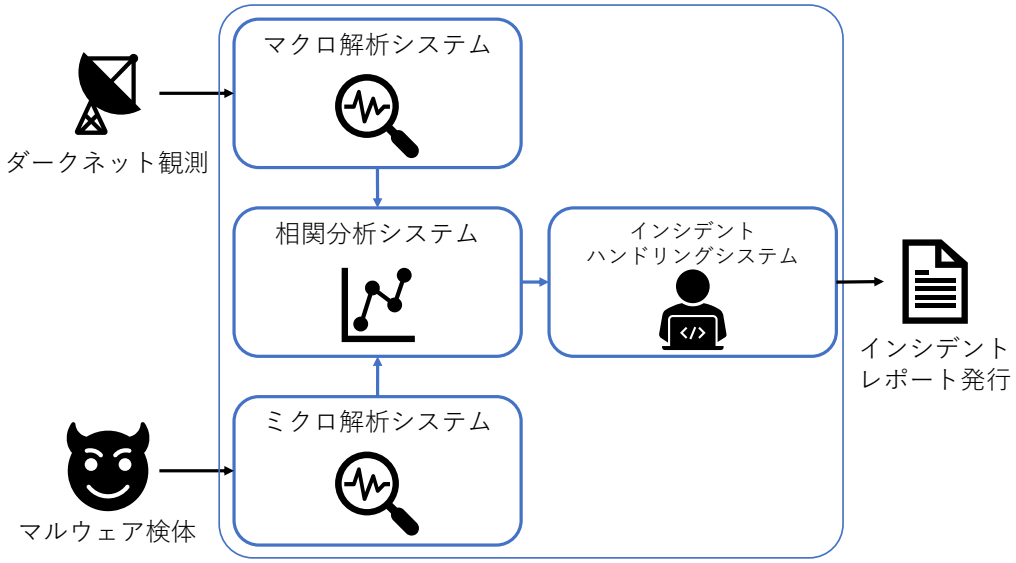

図 2.4: NICTER のシステム概要図

中尾らはネットワークに大規模な悪影響を及ぼすインシデントの早期な検出と対策の確立を目指したインシデント分析センター nicter を開発した [10]．nicter はダークネット観測によるマクロ解析システム，マルウェア解析によるミクロ解析システム，これらの 2 つのシステムから導き出された解析結果の相関関係を分析する相関分析システムを融合させたシステムである．

マクロ解析システムとして/20 の規模の連続したダークネットに設置したブラックホールセンサでのトラフィックの観測を行っている．2019 年には年間を通じて約 3,279 億のパケットが観測されている [5]．観測されたパケットの送信元アドレスや送信先ポートの情報は Atlas と Cube の 2 つの可視化エンジンにより可視化され，Web ページ上で公開されている [6]．

ミクロ解析システムではマルウェアの動的解析エンジンと静的解析エンジンにより，マルウェア解析の自動化と並列化がされている．静的解析エンジンはハニーポットや Web クローラで採取したマルウェアの実行コードを逆アセンブルし，マルウェアの機能を詳細を明らかにする．逆アセンブルを阻害するコード難読化が施された近年のマルウェアに対しては，マルウェアをマシン上で実行させてメモリに復号されたコードを逆アセンブルすることにより，難読化の無効化を可能にしている．動的解析エンジンはマルウェアを実行させることにより，使用した API やネットワークアクセスの挙動を明らかにする．解析環境ではマルウェアを実行するサンドボックスのほかに，DNS などの多数のダミーサーバを実装されている．これにより疑似的なインターネットを再現され，マルウェアにサンドボックス環境下にあることを検知させず，かつ安全に動的解析ができる環境を実現している．

相関分析システムはマクロ解析システムで観測されたスキャンをプロトコル，TCP フラグ，送信元ポート番号とその変化，宛先ポートのセット，宛先 IP アドレスの遷移といった特徴からプロファイルし，ミクロ解析システムで明らかにしたマルウェアのプロファイルと照合を行う．その結果から発生しているインシデントの原因や流行しているマルウェアを特定する．

第3章　本研究で使用したデータセット・データベース

3.1　RPaaS データセット

RPaaS データセットは Mi らが収集した RESIP のアドレスと実験期間，RESIP プロバイダの情報である．観測を行った RESIP プロバイダは Proxies Online[1]，Geosurf[2]，Proxyrack[3]，Luminati[1]，IAPS Security[4]の 5 つである．RPaaS データセットはフレームワークと IP プロファイリングツールのソースコードとともに公開されている [7].

表 3.1: RpaaS データセットのデータ例

IP アドレス	RESIP プロバイダ	観測開始日	観測終了日
1.0.100.107	Proxyrack	2017/9/19	2017/9/29
106.161.254.128	Proxies Online	2017/12/1	2017/12/1

3.2　NICTER Darknet と NONSTOP

NICTER Darknet は国立研究法人 情報通信研究機構が開発しているインシデント分析システム NICTER（Network Incident analysis for Tactical Emergency Response） [10] プロジェクトで観測を行っている/20 の連続したダークネットである．NONSTOP（NICTER Open Network Security Test-Out Platform）は NICTER の保有するサイバーセキュリティ情報を外部から利用するための分析基盤である [11].

NICTER Darknet に到達したパケットは PCAP サーバに日ごとにダンプファイルとして保存される．パケットの IP ヘッダ，TCP ヘッダ，UDP ヘッダ，ICMP ヘッダ，それら以外のプロトコルを使用するパケットのヘッダ，ペイロード情報，オプション情報は DB サーバに保存される．観測されたパケットの情報は情報通信研究機構が提供する分析基盤 NONSTOP からアクセスできる．NONSTOP からはパケットの到着時刻，送信元・送信先のアドレス・ポート，送信元国などの情報を取得できる．

[1]Proxies Online. http://proxies.online, 2021.02.13 参照.
[2]Geosurf: Residential and data center proxy network. https://www.geosurf.com/，2021.02.13 参照.
[3]Proxyrack. https://www.proxyrack.com/, 2021.02.13 参照.
[4]Iaps security. https://www/intl-alliance.com/.

3.3 GeoLite2 City データベース

GeoLite2 City データベースは MaxMind 社が提供している無償のデータベースである [8]．ユーザは MAXMIND のアカウント作成後，データベースファイルをダウンロードし利用できる．Python や Ruby，PHP など複数の言語で API が用意されており，IP アドレスから国・地域・緯度・経度の情報を検索し，JSON 形式で取得できる．

3.4 APNIC whois データベース

APNIC whois データベースはアジア・太平洋地域の IP アドレスの管理を行う APNIC が提供するドメイン・IP アドレス・AS 番号の登録情報の検索サービスである [12]．RDAP(Registration Data Access Protocol) は地域レジストリに登録された IP アドレスに関する情報にアクセスするためのプロトコルである．クエリを HTTP，または HTTPS で送信することで登録されている情報を JSON 形式で取得できる．

3.5 VirusTotal

VirusTotal は Google 社の運営する脅威情報検索プラットフォームである [13]．Web サイト上でマルウェアやファイルのスキャン，URL や IP アドレスの悪性判定を行うことができる．API を利用した情報検索も提供されており，リクエストを HTTPS で送信することで IP アドレスのブラックリスト登録状況が取得できる．

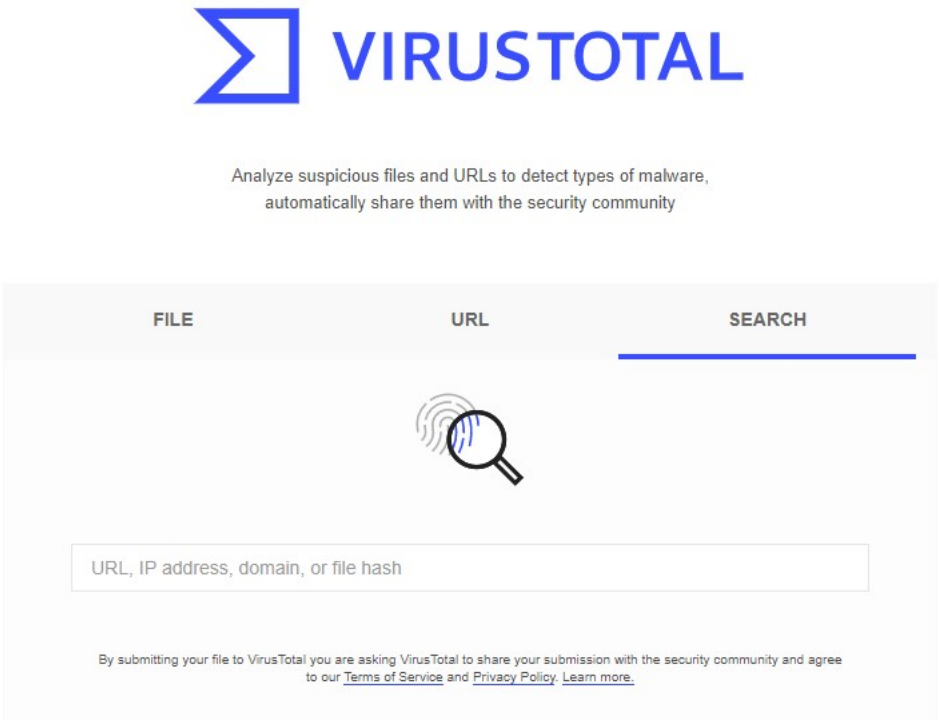

図 3.1: VirusTotal の Web ページ

3.6 Shodan

Shodan はインターネットに接続されたデバイスに関する情報の検索を目的とした検索エンジンである [14]．インターネット全体をクロールし，開放しているポート番号，位置情報，応答から得られたバナー情報を収集してデータベース化している．ユーザは Web サイトからの検索と API を利用したデータの取得が利用できる．

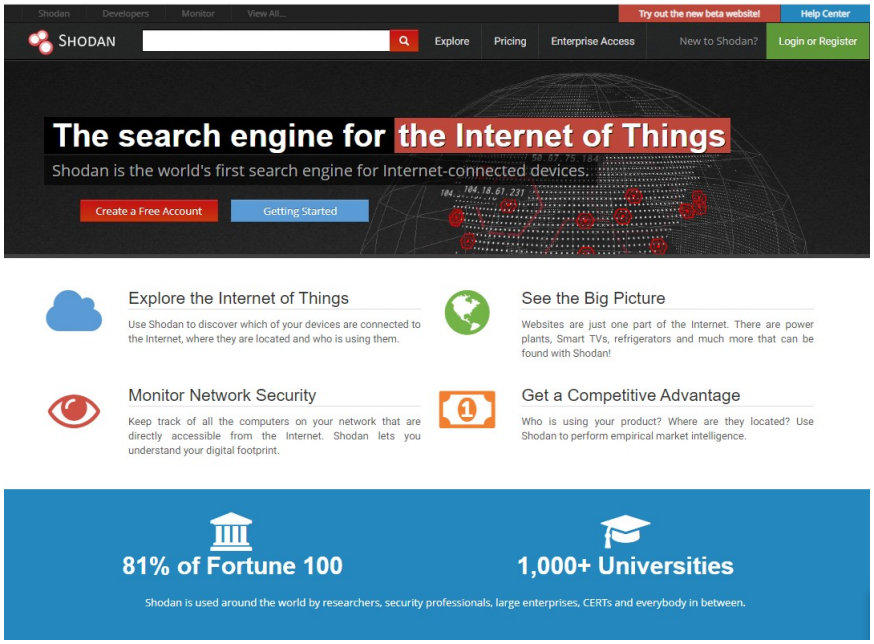

図 3.2: Shodan の Web ページ

3.7 まとめ

表 3.2 に本研究で使用したデータセット，データベースについてその内容をまとめる．

表 3.2: 使用したデータセット・データベースの概要

データセット データベース	内容	Web サイト	使用した調査
RPaaS Dataset	Mi らが収集した RESIP ホストの IP アドレス，RESIP プロバイダ，観測日	[7]	4，5，6，7 章
NICTER Darknet	情報研究通信機構が/20 のダークネットで 観測したパケット本体とそのヘッダー情報	[6]	5 章
GeoLite2 City	MaxMind 社が提供している IP Geolocation データベース	[8]	4，6 章
APNIC whois	アジア・太平洋地域の IP アドレス を管理する APNIC が提供する アドレス・ドメイン検索データベース	[12]	4 章
VirusTotal	Google 社の脅威情報検索プラットフォーム	[13]	6 章
Shodan	インターネット全体のクロールにより収集 されたデバイス情報検索データベース	[14]	6 章

第4章　日本国内に存在するRESIPホストの調査

4.1　目的

Mi らが収集した RPaaS データセットは日本の IP アドレスを含んでいる．本研究では，2017 年に収集された RESIP の中の日本の IP アドレスに着目し，それらの IP アドレスが所属する都道府県，管理団体，アドレスブロック情報，紐づいているドメインについて次の手順で調査を行い，日本から RESIP ホストに参加する IP アドレスがどのような特徴を持つのかを明らかにする．

4.2　方法

図 4.1 に調査の概要を示す．

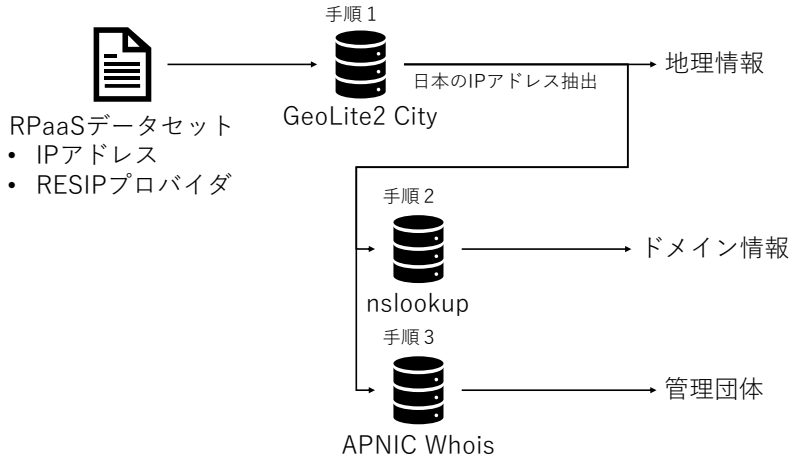

図 4.1: 日本国内に存在する RESIP ホストの調査

1. RPaaS データセットからの日本の IP アドレスの抽出には GeoLite2 City データベースを用いる．RPaaS データセット内の IP アドレスに対して GeoLite2 City データベースで検索を行い，所属する国が日本と判定されたものに所属する都道府県の情報を付加する．

2. 抽出した IP アドレス群に対して nslookup を行い，日本の RESIP に紐づいているドメイン（FQDN）の調査する．

3. 抽出した IP アドレスから APNIC whois への RDAP リクエストを作成し，取得した JSON からアドレスブロック (CIDR) 情報と管理団体を取得する．

4.3 結果

表 4.1: 都道府県別の RESIP アドレス数，RESIP プロバイダ PO: Proxies Online，GS: Geosurf，PR: Proxyrack，LU: Luminati，IS: IAPS Security

都道府県	RESIP アドレス数	割合 (%)	PO	GS	PR	LU	IS	携帯電話・PHS 契約数の割合 (%)[15]	ISDN 契約者数の割合 (%)[15]
東京	12,766	26.1	2,709	84	4,442	5,027	4	26.0	17.8
神奈川	3,094	6.3	721	17	1,145	1,087	0	6.4	6.2
愛知	2,940	6.0	715	15	1,163	942	0	5.2	5.7
大阪	2,917	5.9	769	17	1,148	880	1	6.7	8.6
埼玉	2,544	5.1	605	14	1,082	754	0	4.7	4.3
千葉	1,912	3.9	484	32	726	557	0	4.0	3.7
兵庫	1,722	3.5	460	21	693	493	0	3.5	3.2
福岡	1,266	2.5	426	9	436	320	0	4.0	4.0
静岡	1,083	2.2	251	7	484	308	0	2.2	2.7
not found	6,619	13.5	1,741	52	2,108	2,507	8		
総計	48,956	100	11,918	304	18,502	16,325	13	100	100

表 4.2: RESIP ホストの分布に対する携帯電話・PHS 契約者数の割合と ISDN 契約者数の割合のユークリッド距離

	ユークリッド距離
携帯電話・PHS	1.9287
ISDN	8.9190

調査の結果，RPaaS データセット内の IP アドレスのうち 48,956 アドレスが日本国内の IP アドレスだった．これは RPaaS データセットに情報のある RESIP ホストのうちの 0.79%である．

表 4.1 に，RESIP ホストアドレスが属する上位 10 都道府県と各県の RESIP プロバイダごとの RESIP アドレス数を示す．ここで，*not found* は GeoLite2 City データベースで都道府県が参照できなかった IP アドレスを示している．これは GeoLite2 City データベースが無償版のデータベースであり，精度が良くないことや欠損データが存在することが原因であると考えられる．最も RESIP 保有数が多かった都道府県は東京都で，12,766 アドレスが存在していた．日本国内で最も多い RESIP プロバイダは Proxyrack で 18,502 アドレスだった．

表 4.2 に，上位 10 都道府県における RESIP ホストの分布と携帯電話・PHS 契約者数の割合と ISDN 契約者数の割合のユークリッド距離を示す．この結果から，ISDN 契約者数の割合よりも携帯電話・PHS 契約者数の割合の方が RESIP ホストの分布とユークリッド距離が近いことがわかった．

nslookup で取得できたドメインから第 3 レベルまでのドメインを抽出した．表 4.3 に，ドメインごとの RESIP アドレス数の上位 10 ドメインの結果を示す．ここで，*not found* は nslookup でドメイ

表 4.3: ドメインごとの RESIP アドレス数

ドメイン	アドレス数	%
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

ンが検索できなかった IP アドレスを示している．ocn.ne.jp が最も多く 7,468 アドレスが観測されていた．

RDAP で取得した管理団体のデータと第 3 レベルまでのドメインの情報から，管理団体ごとの主なドメインと観測された RESIP アドレス数の上位 10 団体の結果を表 4.4 に示す．最も多く観測されていたのは NTT Communincation Corporation が管理するアドレスで 10,941 アドレスが観測されていた．

日本国内に存在する RESIP ホストでトップレベルドメインが jp のアドレスは 38,946 件あった．その中で一般的なドメインの属性を示す第 2 レベルのドメインについてのアドレス数を表 4.5 に示す．最も多かったのは住宅用インターネットプロバイダでも使われる ne だった．しかし，大学向けのドメインである ac や会社組織で使われる co，政府機関や独立行政法人で使われる go ドメインも観測されている．

表 4.6 に RESIP プロバイダごとの家庭用 2LD と公共機関用 2LD の数を示す．全ての RESIP プロバイダで家庭用 2LD が多く観測され，公共機関用 2LD の割合が 1%を超える RESIP プロバイダはなかった．公共機関用 2LD が最も多く観測された RESIP プロバイダは Luminati だった．IAPS Security では家庭用 2LD が 1 つだけ観測され，公共機関用 2LD は観測されなかった．

GeoLite2 City データベースでは東京に存在すると判定された IP アドレスでトップレベルドメインが.ru のものが 43 件観測された．この 43 件のドメインはすべて pinspb.ru というドメインで，全てのアドレスが 46.161.57.0/24 の範囲内だった．このドメインからアクセスできる Web サイト内ではロシア語が使われていた．これらの IP アドレスについて GeoLite2 City 以外のデータベース [17][18] で検索したところ，ロシアやイスラエルに属する IP アドレスであった．

表 4.4: 管理団体ごとの RESIP アドレス数

管理団体	主なドメイン	アドレス数	割合 (%)	FTTH 契約数におけるシェア (%)[16]
NTT Communication Corporation	ocn.ne.jp, plala.or.jp	10,941	22.3	34.2
KDDI CORPORATION	au-net.ne.jp, dion.ne.jp	8,301	16.9	12.8
Japan Nation-wide Network of Softbank Corp.	bbtec.net, access-internet.ne.jp	7,781	15.8	
Japan Network Information Center	nttpc.ne.jp, mesh.ad.jp	4,756	9.7	
Sony Network Communicatoins Inc.	so-net.ne.jp, ap.nuro.jp	2,544	5.1	
OPTAGE Inc.	eonet.ne.jp	1,274	2.6	5.4
BIGLOBE Inc.	mesh.ad.jp	1,230	2.5	
Jupiter Telecommunication Co.,Ltd	home.ne.jp	1,209	2.4	
Chubu Telecommunicatons Co.,Inc.	commufa.jp	1,125	2.2	
ARTERIA Networks Corporation	ucom.ne.jp, vectant.ne.jp	965	1.9	2.3
計		48,956	100	

4.4 考察

表 4.5，表 4.6 の結果から，90.8%の RESIP ホストは，個人用に使われる ne, ad, or ドメインであった．従って，日本の RESIP ホストは主に住宅用ホストであると結論付けられる．一方，非住宅用の ac, co ドメインのアドレスも，その多くはモバイル用のドメインであり，住宅でマルウェアに感染した端末を企業や大学に持ち込んだものと考えられる．

表 4.1 や表 4.2，表 4.3，表 4.4 の結果から，RESIP ホストの割合は ISDN 契約数の割合よりも携帯電話，PHS の契約数の割合と近いと考えられる．従って，地域による差はなく，モバイルユーザ数に比例している．家庭用 ISP やモバイル用 ISP が主に RESIP ホストとなっていると考える．

表 4.4 より，ISP の契約者数のシェアと RESIP ホストの割合は一致しており，ISP 間の差も認められない．各 ISP が RESIP となっている住宅用ホストについて注視する必要があると言える．都道府県ごとの RESIP プロバイダ別ホスト数を見ると，東京では Luminati の RESIP ホストが多いが，それ以外の大都市では ProxyRack の RESIP ホストが最も多くなっており，日本全体で見ると ProxyRack が最も多くの RESIP ホストを有している．また，本研究付録に記載している様に 47 都道府県全てで RESIP ホストが観測されており，都市部に限らず日本全国での RESIP ホスト提供者の実態を探る必要があることを示している．

表 4.5: 第 2 レベルドメインごとの RESIP アドレス数

2LD	アドレス数	%
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

表 4.6: RESIP プロバイダごとの第 2 レベルドメイン数

RESIP プロバイダ	家庭用 2LD 数 (ne, or, ad)	公共機関用 2LD 数 (ac, co, gp, gr, ed)
Proxies Online	9,431	9
Geosurf	1,167	0
Proxyrack	14,862	11
Luminati	11,228	82
IAPS Security	1	0
計	36,689	102

表 4.7: 東京に存在する ru ドメインの例

IP アドレス	観測開始日	観測終了日	都道府県	FQDN	RESIP プロバイダ
46.161.57.***	2017/10/23	2017/11/19	Tokyo	pinspb.ru	Proxyrack

第5章　RESIPホストから国内ネットワークを標的とする不正通信の調査

5.1　目的

Mi らの研究で収集された RPaaS データセット [7] は RESIP のアドレス，観測期間，RESIP プロバイダの情報を含んでいる．観測期間中に RESIP ホストの IP アドレスが日本のダークネットで観測された場合，RESIP ホストに接続されている機器が不正な通信を送っていたと考えられる．本研究では RPaaS データセットと情報通信研究機構が提供する NONSTOP[11] を用いて，Mi らの研究が行われた 2017 年の調査期間中に RESIP から日本のダークネットにパケットが送信されているのか，送信されていた場合にどのサービスに対する攻撃が行われていたのかを明らかにする．

5.2　方法

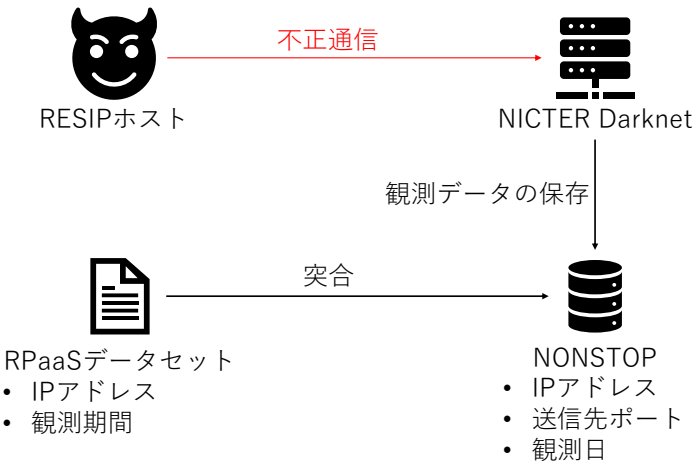

図 5.1: RESIP ホストから国内ネットワークに到達する不正通信の調査

図 5.1 に調査の概要を示す．RPaaS データセットの IP アドレス，観測開始日，観測終了日の情報をもとに，Mi らの研究での観測期間内に NICTER Darknet で観測された RESIP ホストからの不正通信を NONSTOP のデータベースから検索する．該当したパケットの受信時刻，送信元アドレス，送信先アドレス，送信先ポート，送信元国の情報を取得し調査を行う．

5.3 結果

表 5.1: 調査結果の概要

観測通信件数	1683,440
観測アドレス数	59,816

NICTER 上で RESIP からの通信が観測されているのかについて結果を述べる．表 5.1 に調査結果の概要を示す．59,816 個の RESIP ホストがダークネット上で観測されており，観測されたパケットは合計で 1,683,440 件だった．NICTER 上での日ごとの RESIP 観測数を図 5.2 に示す．図 5.2 から，Mi らの研究での RESIP 観測期間中に継続して NICTER へパケットが到達していることがわかる．

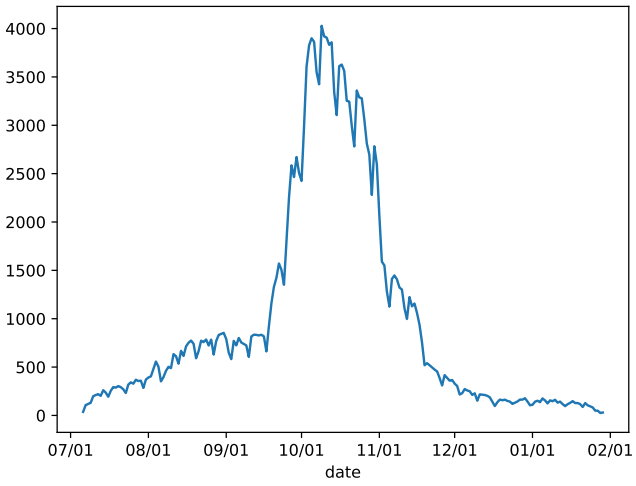

図 5.2: NICTER で 2017 年に観測された 1 日あたりの RESIP ホスト数の変化

送信元の RESIP アドレスごとのパケット観測件数の上位 10 アドレスを表 5.2 に示す．単一の RESIP アドレスからは最大で 8 日間に 62,669 パケットがダークネットに到達しており，1 日当たり約 7800 パケットを送信していることになる．

送信先ポート番号別のパケット観測件数の上位 10 ポートと各ポートを使用するサービスを表 5.3 に示す．RESIP に最も狙われていたサービスは Telnet で 613,606 パケットが観測されていた．

標的とするポートが時期で異なるのかを明らかにする．表 5.3 で取り上げたポートに関してパケット観測時期と観測されたポートの散布図を図 5.3 に示す．大半のポートは時期に関わらず標的とされていることがわかる．一方で，MSSQL や SMTP を標的とする通信は特定の期間で多く観測されている．

5.4 考察

表 5.2，図 5.2 の結果から，RESIP ホストから日本のネットワークに不正な通信が継続的に到達していると結論付けることができる．

表 5.2: ダークネット上で観測された上位 10 の RESIP アドレス

順位	アドレス	観測日数	RESIP プロバイダ	観測件数
1	43.249.57.255	8	ProxyRack	62,669
2	187.120.17.2	34	Proxies Online Geosurf	35,353
3	200.170.223.50	7	Luminati	21,676
4	103.29.97.2	8	Proxies Online Geosurf Luminati	17,004
5	165.73.122.29	14	Luminati	16,127
6	212.90.62.209	5	Luminati	15,142
7	43.248.73.6	90	Proxies Online Geosurf Luminati	13,425
8	190.57.236.230	18	Luminati	13,388
9	112.196.77.202	27	Proxies Online Geosurf	13,061
9	125.99.100.22	10	Proxies Online Luminati	12,952

表 5.3 の結果から，RESIP が行う通信のほとんどがスキャンを目的とした通信であった．Mi らの研究では RESIP に関する悪性行動で最も多かったのはスパムで 36.55%だったが，本研究の結果ではスパムに用いられる SMTP での通信は全体の 1.3%にとどまっており，図 5.3 からは SMTP での通信が行われる期間も短いことがわかる．

表 5.3: 送信先ポート別のパケット観測件数

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	0.1
3389	RDP	9,782	0.5

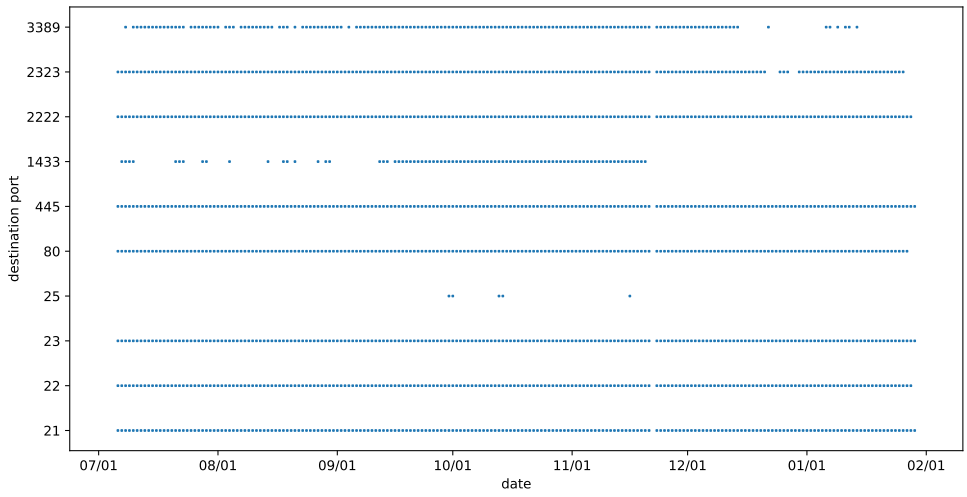

図 5.3: 観測されたポートと時期

第6章　Proxyrackを利用した内部からのRESIPホストの調査

6.1　目的

Miらの研究でRESIPサービスを利用したホスト情報の収集が行われたのは2017年であった．2020年となった現状では当時とRESIPプロバイダの振る舞いやそれを取り巻く状況が異なってきている可能性がある．そこで新たに，代表的なRESIPサービスであるProxyrackを購入して内部からの調査を行い，2020年のRESIPホストの特徴を明らかにする．

6.2　方法

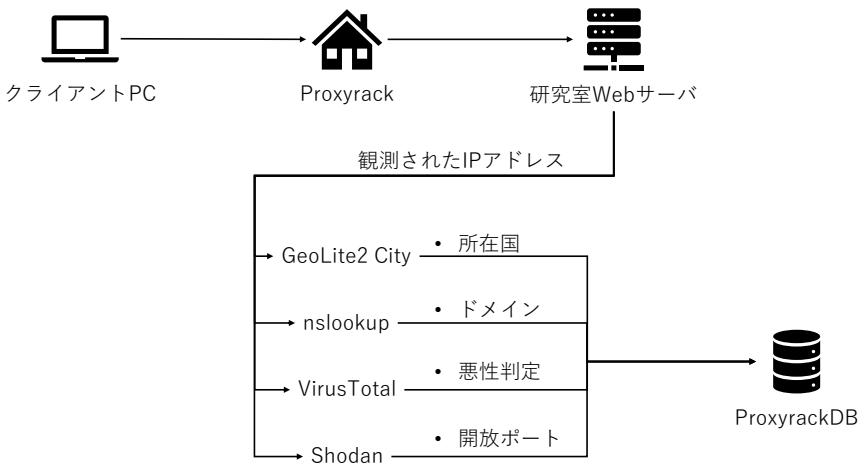

図 6.1: Proxyrackを利用したRESIPホストの調査

図6.1に調査の概要を示す．2020年2月20日から11月6日の261日間で，Miらの研究で調査が行われたRESIPサービスの1つであるProxyrack[3]を利用し，RESIPホストとなっているIPアドレスの調査を行った．クライアントPCからProxyrack経由で研究室Webサーバにアクセスし，通信ログに記録されたIPアドレスを収集した．クライアントPCからのWebアクセスの際，User-Agent属性に特徴的な文字列を挿入することにより通常のWebアクセスと実験でのWebアクセスを判別した．収集されたWebアクセスのログはProxyrackDBの表6.1のlogテーブルに格納されている．表6.2にlogテーブルのデータ例を示す．観測されたIPアドレスは，GeoLite2 City，nslookup，VirusTotal，Shodanの４つのデータベースを用いて，所在国，ドメイン，IPブラックリストでの良性判定数，悪

表 6.1: log テーブルの概要

属性	内容
Unixtime	観測時刻の UNIX 時刻表記
Datetime	観測時刻
Address_deci	観測された IP アドレスの十進表記
Address	観測された IP アドレス

表 6.2: log テーブルの例

Unixtime	Datetime	Address_deci	Address
1582179528	2020-02-20 15:18:48	249733641	14.226.162.9
1582179692	2020-02-20 15:21:32	1963368705	117.6.161.1

性判定数，外部に対する開放ポートを明らかにし，表 6.3 の ProxyrackDB の ip_info テーブルに格納した．表 6.4 に ip_info テーブルのデータ例を示す．

6.3 結果

収集期間と観測件数，観測アドレス数の結果を表 6.5 に示す．71,647 件の RESIP を経由した通信を観測し，得られた RESIP ホストの IP アドレス数は 52,081 個だった．複数回観測されたアドレスは 10,721 個で，最大で 863 回観測されているアドレスがあった．

表 6.6 に国別の RESIP ホスト観測数上位 10 国を示す．最も RESIP ホストが多く観測されたのは韓国で 8,585 アドレスが観測された．

表 6.7 に国別の VirusTotal に悪性判定された RESIP ホスト数上位 10 国を示す．VirusTotal に悪性判定された RESIP ホストは全体で 2,025 個あった．悪性判定された RESIP ホストを最も有しているのはベトナムだった．

表 6.8 に開放しているポート別の RESIP ホスト数を示す．外部にポートを開放している RESIP ホストは 11,686 個であり，全体の 16.3%であった．RESIP となっているホストが開放しているポートとして最も多かったのは 7547TCP(CPE WAN Management Protocol) だった．

6.4 考察

表 6.6 より Proxyrack で観測された国は韓国，ベトナム，日本の順で多かった．Mi らの研究ではアメリカ，ブラジル，ロシア，インド，トルコなどの国が多く観測されていた．

Mi らの研究では 6,183,876 の RESIP のホスト情報を収集し，その中でブラックリストに登録されていた IP アドレスは 2.2%だった．表 6.7 より，本研究で行った調査で収集した RESIP ホストがブ

表 6.3: ip_info テーブルの概要

属性	内容
Address_deci	観測された IP アドレスの十進表記
Address	観測された IP アドレス
Country	所属国
ASN	AS 番号
Organization	管理団体
Domain	ドメイン
VT_harmless	VirusTotal での良性判定数
VT_malicious	VirusTotal での悪性判定数
shodan	Shodan による外部開放ポート情報

表 6.4: ip_info テーブルの例

Address_deci	Address	Country	ASN	Organization	Domain	VT_harmless	VT_malicious	shodan
249733641	14.226.162.9	VN	45899	VNPT Corp	static.vnpt.vn	78	1	80, 443
1198091265	71.105.108.1	US	701	UUNET	o0-100.NYCMNY-VFTTP-316.verizon-gni.net	79	0	close

ラックリストに登録されている割合は 3.9%だった．2017 年と比較してブラックリストに登録されている IP アドレスの割合は増えているものの，ブラックリストによる対策が現在も効果的ではないという点は変わっていないといえる．

表 6.8 より，外部にポートを開放している RESIP ホストは 11,686 個であり，全体の 16.3%であった．Mi らの調査では外部にポートを開放していた RESIP ホストは全体の 11.8%であり，2017 年よりも現在の方が外部にポートを開放している RESIP ホストが増加しているといえる．RESIP ホストとなっている機器が外部に開放しているポートで最も多かったのは 7547/TCP であった．このポートは 5 章で述べた RESIP ユーザの攻撃先ポートの上位には入っていなかったが，IoT 機器を標的とするマルウェアである「Mirai」の亜種が標的とするポートとして TrendMicro 社に報告されている [21]．このことから RESIP ホストとなっているのは「Mirai」などの IoT 機器を標的とするマルウェアに狙われうる脆弱性を抱えたデバイスでないかと考えられる．

表 6.5: 調査結果の概要

観測期間	2020/02/20 - 2020/11/06
観測件数	71,647
観測アドレス数	52,081

表 6.6: 国別 RESIP ホスト観測数

国	観測数	%
KR(韓国)	8,585	16.5
VN(ベトナム)	6,812	13.1
JP(日本)	4,648	8.9
US(アメリカ)	3,777	7.3
TH(タイ)	2,459	4.7
IN(インド)	2,125	4.1
BR(ブラジル)	2,090	4.0
ID(インドネシア)	1,698	3.3
RU(ロシア)	1,560	3.0
EG(エジプト)	1,515	2.9
計	52,081	100

表 6.7: 国別の VirusTotal 悪性判定数

国	観測数	国別 RESIP ホスト観測数に対する割合 (%)
VN(ベトナム)	367	5.4
TH(タイ)	221	9.0
IN(インド)	156	7.3
BR(ブラジル)	143	7.0
ID(インドネシア)	135	8.0
US(アメリカ)	78	2.0
PK(パキスタン)	56	7.0
KR(韓国)	55	0.6
IT(イタリア)	52	14.2
RU(ロシア)	49	3.1
計	2,025	3.9

表 6.8: 開放ポート別 RESIP 数

ポート	観測数	RESIP ホスト観測数に対する割合 (%)
7547(CWMP)	2,763	5.3
80(HTTP)	1,660	3.1
179(BGP)	1,393	2.6
443(HTTPS)	1,306	2.5
123(NTP)	979	1.8
2000	809	1.5
22(SSH)	749	1.4
53(DNS)	701	1.3
1723(PPTP)	612	1.1
23(Telnet)	578	1.1

第7章　RESIPホスト上で展開されているWebページの調査

7.1　目的

Miらの研究でRESIPホストの開放しているポートとバナー応答からNmap service detecton list[20]を用いてデバイスの推定を行い，547,497のRESIPホストのデバイスタイプとベンダ情報を明らかにした．その結果，237,029のRESIPホストがルータ，Webカメラ，プリンターなどのIoT機器であり，デバイスベンダがMikroTikが最も多かったという結論に至っている．

RESIPホストに接続されているデバイスがIoT機器である場合，機器設定用のWebインターフェイスがRESIPホスト上で展開されており，Webブラウザを用いてアクセスした際にルータのコンフィグ画面が観測できる可能性が考えられる．そこで本章では，RESIPホストに対してHTTPリクエストを送信し，取得したHTMLソースコードの情報からデバイスのベンダや型番の特定が可能か調査を行った．

7.2　方法

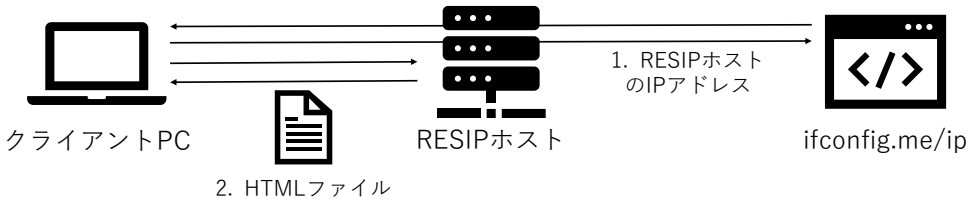

図 7.1: Proxyrackを利用したRESIPホストで展開されているWebページの調査

図7.1に調査の概要を示す．2020年11月12日から11月27日の16日間で，Proxyrackを利用してRESIPホスト上で展開されているWebページの調査を行った．

```
<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
```

図 7.2: デバイスベンダが HTML ソースコードに記載されている例

```
<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>
```

図 7.3: 機器の型番が HTML ソースコードに記載されている例

1. クライアント PC から RESIP ホスト経由で ifconfig.me/ip にアクセスし，RESIP ホストの IP アドレスを取得する．
2. RESIP に接続した状態で RESIP ホストの IP アドレスに HTTP リクエストを送信し，応答の HTML ファイルを取得する．

取得した HTML ソースコードを解析し，RESIP ホストのデバイスベンダや機器を判別する．図 7.2，7.3 に HTML ソースコード内にデバイスベンダと機器の型番が記載されている例を示す．

7.3 結果

表 7.1 に実験結果の概要を示す．2020 年 11 月 12 日から 27 日の期間で，9,316 の RESIP ホストにアクセスし，1,097 の HTML ソースコードを取得した．ソースコード内の情報からデバイスベンダが明らかになった RESIP ホストの数は 333 だった．

表 7.1: 調査結果の概要

調査項目	内容
観測期間	2020/11/12 - 2020/11/27
観測件数	9,316
取得した HTML ソースコード数	1,097
ベンダの明らかになった RESIP ホスト数	333

図 7.4: RESIP ホストとなっているデバイスにアクセスした際の Web ページ

図 7.4 に RESIP ホストとして稼働しているデバイスに，ブラウザからアクセスした際の表示される Web ページの例を示す．この例では Fortinet 社のアラート画面が表示されている．

表 7.2 に観測されたデバイスベンダと観測件数について示す．最も多く観測されたデバイスベンダは Cambium Networks で 86 件だった．Mi らの研究でも観測された上位 10 のデバイスベンダの中で，Zyxel Networks，Huawei Technologies が本実験でも観測数上位に入っている．

7.4 考察

表 7.1 より，本研究で観測された RESIP ホストのうち，デバイスベンダが明らかになったのは 3.6% だった．Mi らの研究では 6,183,876 の RESIP ホストの情報を収集し，そのうちの 8.9%である 547,497 のデバイスのベンダを明らかにした．先行研究と比較して本実験で明らかになった RESIP のデバイスベンダの割合は減少した．この点から本実験の手法は先行研究と比較して，適用できるホストの数は限られると考えられる．

表 7.2 より，本実験の手法により観測されたデバイスベンダのうち，最も多かったのは Cambium Networks 社だった．これは Mi らの研究では観測数の上位に入らなかったデバイスベンダである．先行研究で用いられたバナー応答のリスト [20] は Cambium Networks 社の製品に対応していなかった．この点から本実験の手法が先行研究と比較して，より正確に RESIP ホストのデバイスベンダを特定できるといえる．

表 7.2: 観測されたデバイスベンダ

デバイスベンダ	観測件数
Cambium Networks	93
Parks Comunicações	52
Zyxel Networks	35
TP-Link Technologies	30
KT	26
Huawei Technologies	16
Mercury	14
Belkin (Linksys)	10
Comcast (Xfinity)	7
Buffalo	6
計	333

第8章　結論

本稿では Mi らの収集した Residential IP Proxy に参加する住宅用ホストのデータセットと情報通信研究機構の提供する分析基盤 NONSTOP，その他データベースを用いて，日本国内の Residential IP Proxy ホストと Residential IP Proxy が国内のインターネットで行っている不正通信の調査を行った．さらに実際に RESIP サービスの１つである Proxyrack を利用して，ネットワークの内部から RESIP となっているホストの特徴を調査し，2020 年現在の RESIP サービスを取り巻く状況を明らかにした．

1. 4 章の日本国内に存在する RESIP の調査では，日本の RESIP ホストは 48,956 個で，Mi らの研究で観測された全世界の RESIP ホストの 0.79%を占めていること，90.8%が住宅用ホストであることが明らかになった．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，ISP ごとのシェアと比例しており，都道府県間，ISP 間での差異は認められなかった．

2. 5 章の RESIP ホストから国内ネットワークを標的とする不正通信の調査では，日本のダークネットで観測された RESIP ホストからの不正な通信が 1,683,550 件に上ることが明らかになった．Mi らは，RESIP サービスを利用した悪性行動の 36.55%がスパムメールであると報告していたが，本調査では RESIP ホストからの不正な通信の 54%はブルートフォースを目的とした通信が占めていた．

3. 6 章の Proxyrack で利用される RESIP ホストの調査では，52,081 件のホスト情報を収集した．RESIP ホストがブラックリストに登録されている割合は 3.9%で，2017 年と比較して割合は増加しているものの，対策としては今だ不十分であるとわかった．RESIP ホストが外部に開放しているポートとして最も多かったのは 7547/TCP だった．このことから世界中で RESIP ホストとなっているのは IoT 機器を標的とするマルウェアに脆弱なデバイスであると考えられる．

4. 7 章の Proxyrack を利用した RESIP ホストで展開されている Web ページの調査では，1,097 のホスト上で展開されている Web ページの HTML ソースコードを収集し，その中で 333 のデバイスのベンダを特定した．RESIP ホストとなっているデバイスのベンダは Cambium Networks 社のものが最も多く，93 件観測された．

これらの結果から今後の RESIP ホストに対するさらなる調査と RESIP サービスの悪用による脅威への対策が必要であると考える．

参考文献

[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.

[2] I2P 匿名ネットワーク，https://geti2p.net/ja/，2021.02.13 参照.

[3] Nguyen Phong Hoang, Sadie Doreen, and Michalis Polychronakis, Measuring I2P Consorship at a Global Scale, 9th USENIX Workshop on Free and Open Communications on the Internet (FOCI '19), 2019.

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

[5] NICTER 観測レポート 2019 の公開，https://www.nict.go.jp/press/2020/02/10-1.html, 2021.02.13 参照.

[6] NICTERWEB - ダークネット観測，https://www.nicter.jp/，2021.02.13 参照.

[7] RPaaS: Characterizing Residential IP Proxy as a Service. https://rpaas.site/，2019.06.13 参照.

[8] MAXMIND: GeoLite2 Free Downloadable Databases. https://dev.maxmind.com/geoip/geoip2/geolite2/，2021.02.13 参照.

[9] APNIC: Whois search. https://www.apnic.net/about-apnic/whois_search/，2021.02.13 参照.

[10] D Inoue, et al., nicter: An incident analysis system toward binding network monitoring with malware analysis. In Information Security Threats Data Collection and Sharaing, 2008. WISTDCS'08. WOMBAT Workshop on, pp. 58-66. IEEE, 2008.

[11] 竹久達也，神薗雅紀，笠間貴弘，中里純二，衛藤将史，井上大介，中尾康二，サイバーセキュリティ情報遠隔分析基盤 NONSTOP の利活用について，コンピュータセキュリティシンポジウム 2014 論文集，volume: 2，pp. 207-214, 2014.

[12] APNIC: Registration Data Access Protocol. https://www.apnic.net/about-apnic/whois_search/about/rdap/，2021.02.13 参照.

[13] Virustotal, https://www.virustotal.com/, 2021.02.13 参照.

[14] Shodan, https://www.shodan.io/, 2021.02.13 参照.

[15] テレコムデータブック 2018(TCA 編), https://www.tca.or.jp/databook/pdf/2018chapter_2j.pdf, 2021.02.13 参照.

[16] 電気通信サービスの契約数及びシェアに関する四半期データの公表 別紙（平成 29 年度第 2 四半期（9 月末））, https://www.soumu.go.jp/main_content/000523384.pdf, 2021.02.13 参照.

[17] IPInfoDB. https://ipinfodb.com/，2021.02.13 参照.

[18] RIPE NCC: whois Database, https://www.ripe.net/manage-ips-and-asns/db/support/documentation/glossary/whois-database，2021.02.13 参照.

[19] 情報通信研究機構 NICTER 観測レポート 2017, https://www.nict.go.jp/cyber/report/NICTER_report_2017.pdf，2021.02.13 参照.

[20] Nmap service detection list, https://svn.nmap.org/nmap/nmap-service-probes，2021.02.13 参照.

[21] TrendMicro: 「Mirai」亜種か？ 海外製ルータを狙うアクセスが急増 (https://www.trendmicro.com/jp/iot-security/news/3086, 2020.01.12 参照)，2021.02.13 参照.

謝辞

本論文は筆者が明治大学大学院先端数理科学研究科先端メディアサイエンス専攻白紙前期課程に在学中の研究成果をまとめたものである．本研究を遂行するに当たり多くの方々から多大なるご指導とご援助を賜りました．

特に，明治大学総合数理学部先端メディアサイエンス学科の菊池浩明教授には，コロナ禍で思うように研究活動が進まないような状況に陥った著者に対して格別のご助力をいただきました．深く感謝申し上げます．

合同ゼミにおいて何度も有益なご討論，ご助言をいただいた静岡大学想像科学技術大学院 西垣正勝教授，静岡大学情報学部情報科学科講師 大木哲史先生に心から感謝いたします．

さらに，２年間共に切磋琢磨し，ときには研究に限らない貴重な助言を与えてくれた明治大学菊池研究室の皆様に感謝を申し上げます．

最後に，大学４年間だけでなく博士前期課程まで進学する機会を与えてくださった家族に深く感謝します．ありがとうございました．

業績

国際会議論文（査読あり）

1. Akihiro Hanzawa, Hiroaki Kikuchi, Analysis on Malicious Residential Hosts Activities Exploited by Residential IP Proxy, Lecture Notes in Computer Science, proceedings of WISA2020, Springer, Jeju Island, South Korea, pp. 406-417, 2020.

国内研究会

1. 半澤 映拓, 菊池 浩明, Residential IP Proxy サービスに悪用される住宅用ホストの調査，Computer Security Symposium2019(CSS-2019), pp.918-925, 2019.

付 録A　47都道府県のRESIP数

ここでは，日本の 47 都道府県全ての RESIP ホスト数と RESIP プロバイダ別ホスト数を表 A.1 に示す.

表 A.1: 都道府県別の RESIP アドレス数，RESIP プロバイダ数 PO: Proxies Online，GS: Geosurf，PR: Proxyrack，LU: Luminati，IS: IAPS Security

都道府県	RESIP アドレス数	PO	GS	PR	LU	IS
東京	12,766	2,709	84	4,442	5,027	4
神奈川	3,094	721	17	1,145	1,087	0
愛知	2,940	715	15	1,163	942	0
大阪	2,917	769	17	1,148	880	1
埼玉	2,544	605	14	1,082	754	0
千葉	1,912	484	32	726	557	0
兵庫	1,722	460	21	693	493	0
福岡	1,266	426	9	436	320	0
静岡	1,083	251	7	484	308	0
北海道	1,061	324	9	448	225	0
京都	997	213	0	438	310	0
三重	638	115	1	300	208	0
広島	589	168	2	257	138	0
岐阜	584	118	1	299	139	0
茨城	568	107	1	264	179	0
沖縄	543	89	3	153	284	0
栃木	473	125	1	186	134	0
群馬	432	112	1	144	158	0
長野	418	80	0	172	144	0
新潟	409	95	0	200	100	0
滋賀	380	99	1	131	135	0
宮城	372	104	5	150	97	0
岡山	316	89	0	129	97	0

奈良	302	74	1	121	85	0
熊本	297	98	1	108	82	0
愛媛	271	94	0	97	68	0
山口	242	79	0	97	57	0
福島	241	72	0	113	42	0
香川	227	60	2	128	27	0
富山	216	57	0	92	56	0
石川	210	61	0	65	73	0
山梨	201	54	0	81	62	0
大分	186	48	1	77	52	0
和歌山	177	51	0	88	34	0
青森	168	34	0	85	46	0
福井	159	36	1	57	61	0
鹿児島	157	41	1	72	38	0
高知	154	53	0	67	27	0
山形	148	31	1	68	38	0
岩手	139	36	0	61	32	0
秋田	131	36	0	60	31	0
長崎	128	25	0	49	52	0
佐賀	126	38	0	54	28	0
徳島	125	37	0	46	33	0
宮崎	124	33	0	51	36	0
鳥取	94	38	0	37	14	0
島根	90	13	0	30	43	0
not found	6,619	1,741	52	2,108	2,507	8
総計	48,956	11,918	304	18,502	16,325	13