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[1,a)]　菊池 浩明[1,b)]

概要：Residential IP Proxy は，住宅用ネットワークのホストを利用したトラフィック中継を提供するプロキシサービスである．サービスを提供している事業者はホストが自発的にサービスに参加して良質な各種応用に利用されていると主張しているが，実際のところは，良性なユーザとして振る舞うことで検出やブロッキングを回避し，DoS 攻撃などの不正行為に悪用されているのが明らかになっていた．Mi らは 2019 年に Residential IP Proxy サービスに参加するホストによる不正行為を指摘し，ホストの探索とプロファイルを行い，Residential IP Proxy サービスの基盤，規模，悪性を明らかにした．本研究では，Mi らが収集した Residential IP Proxy に参加するホストのデータセットを解析し，情報通信研究機構の提供する分析基盤 NONSTOP を用いて，Residential IP Proxy が国内のインターネットで行っている通信についての調査結果を報告する．解析結果に基づき， Residential IP Proxy が日本のネットワークにもたらす脅威について明らかにする．

キーワード：ネットワーク観測, ダークネット, Residential IP Proxy

Study on Residential Hosts Exploited by Residential IP Proxy Services

Akihiro Hanzawa[1,a)]　Hiroaki Kikuchi[1,b)]

Abstract: Residential IP Proxy is a proxy service that provides traffic relay using hosts on residential networks. Although the service providers claim that the hosts voluntarily participates in the service and are used for various high-quality applications, in fact, the service provides avoiding detection and blocking by pretending as benign users, they exploited the residential hosts to perform malicious acts such as DoS attacks. In 2019, Xianghang Mi et al. Pointed out malicious hosts participating in the Residential IP Proxy service, searched hosts and profiled them, and clarified the infrastructure, scale, and malignancy of the Residential IP Proxy service. In this paper, we analyze datasets of hosts participating in Residential IP Proxy collected by Mi and report the analysis on the communication that Residential IP Proxies perform in Japan, using NONSTOP, the analysis platform, provided by Information Technology Research Organization.

Keywords: CSS 2019, LaTeX, style files

1. はじめに

近年，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その市場規模を拡大している．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が，アクセス制限を回避するために住宅用ネットワークにあるホストをプロキシとしてアクセスに利用している．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

[1] 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
Frontier Media Science Program, Graduate School of Advanced Mathematical Sciences, Meiji University
[a)] cs192013@meiji.ac.jp
[b)] kikn@meiji.ac.jp

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．表 1 に確認できている主要な RESIP サービス事業者の一覧を示す．

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ので，SPAM の送信，脆弱性のポートスキャン，DoS 攻撃などにも悪用されている．RESIP プロバイダは，その様を不正利用については明示しないが，認知済と考えられる．表 1 の高額な利用料金や RESIP サービスは悪意のあるクライアントに中継 IP アドレスの変更を短い間隔で更新して提供しているため，トレースされにくくしていることなどがその根拠である．

Mi らは 2017 年に RESIP サービスで提供される 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 [1]．RESIP が不正行為を担う傾向にあると結論付けた．Mi らは，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．

RESIP サービスに関して，次の疑問がわく．

(1) どんなネットワーク環境のホストが RESIP として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 ISP やどの県のユーザが RESIP のホストになっているのか?地域差はあるのか?
(3) どの RESIP サービスが主流か?
(4) 日本のネットワークは RESIP の脅威にさらされているのか?
(5) RESIP サービスは何に使われているのか?本当に不正利用されているのか?利用の実態はどうか?

これらの問に答えることが本研究の目標である．

(1)，(2) を明らかにするには，Proxy として用いられている IP アドレスを調べる必要がある．

そこで本研究では Mi らが収集した RESIP ホストのデータセット [2] について，Maxmind 社の提供する GeoLite2 city データベース [3] と APNIC の提供する RDAP サービス [4] 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) や (5) 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．そこで本研究では，情報通信研究機構の提供する分析基盤 NONSTOP[6] 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．

2. Residential IP Proxy

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 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 を経由してクライアントへと返される．

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．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，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．先行研究 [1] ではプロバイダがどのようにして住宅用 IP 提供者を募っているのか調査を行った．Luminati[1]では住宅用 IP を提供することで他の住宅用 IP 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 提供者を募っていた．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．

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 1 に示す．先行研究 [1] 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，複数のプロバイダで価格が大きく上昇していることがわかる．一方ですでにサービスが終了しているサービスや更新が停止しているサービスも出てきている．

表 1 RESIP サービスの概要

RESIP プロバイダ	料金 (2017 年)	料金 (2019 年)	ホスト数 [1]
Proxies Online(アメリカ)	$25/Gb	証明書切れ	1,257,418
Geosurf(オランダ)	$300/月	$450～2000/月	432,975
ProxyRack（アメリカ）	$40/月	$60～120/月	857,178
Luminati(アメリカ)	$500/月	$12.5/GB+$500/月	4,033,418
IAPS Security	$500/月	サービス停止	

表 2　本研究で使用したデータセット・データベース

	rpaas データセット	NICTER Darknet データセット	GeoLite2 City データベース	APNIC whois データベース
時期	2017 年	2017 年	2019 年	2019 年
内容	Mi らが調査で収集した RESIP に参加している IP アドレスのリスト	情報通信研究機構が/20 のダークネットで観測したパケットの送信元，送信先の情報	MaxMind 社が提供している無償の IP アドレスと地理情報のデータベース	アジア・太平洋地域の IP アドレスの管理を行う APNIC が提供するアドレス・ドメイン検索データベース
レコード数	6,183,876	約 1,504 億		
収集方法	公開されている	NICTER NONSTOP から利用	Python による データベース利用	Python による RDAP リクエスト

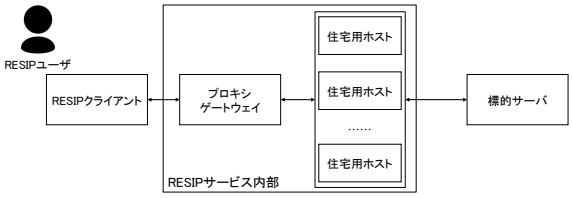

図 1　RESIP サービスのシステム概要

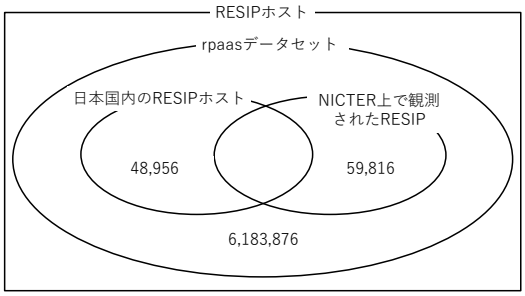

図 2　各データセットの IP アドレス集合の関係

3. 調査方法

3.1 データセット・データベース

本研究で使用したデータセットとデータベースについて説明する．使用した 4 つのデータセットの情報を表 2 に示す．

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．先行研究で観測を行った RESIP プロバイダは Proxies Online[2], Geosurf[3], ProxyRack[4], Luminati[1], IAPS Security[5]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 [2].

NICTER Darknet データセットは情報通信研究機構が保有する/20 のダークネットで観測された通信の情報である [5]．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．

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 [6]．IP アドレスから国・地域・緯度・経度の情報を取得できる．

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．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 [7].

3.2 日本国内に存在する RESIP ホストの調査

先行研究 [1] で収集された rpaas データセットは日本の IP アドレスが含まれていることが示されている．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．

(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

[1] Luminati: largest business proxy service. http://luminati.io/.
[2] Proxies Online. http://proxies.online.
[3] Geosurf: Residential and data center proxy network. https://www.geosurf.com/.
[4] Proxyrack. https://www.proxyrack.com/.
[5] Iaps security. https://www/intl-alliance.com/.

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の調査する．

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

3.3 RESIP ホストから日本に宛てる不正通信の調査

先行研究 [1] で収集された rpaas データセットは RESIP のアドレス，観測期間，RESIP プロバイダの情報が含まれている．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 サービスの依頼人か 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仮定する．

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分析基盤 NONSTOP を用いて，先行研究の 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調査する．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，NONSTOP のデータベースから該当する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する．

4. 調査結果

4.1 日本国内の RESIP

全 RESIP ホストと rpaas データセット，本研究で調査を行った RESIP ホストと各集合の交わりの大きさを図 2 に示す．

調査の結果，rpaas データセット内の IP アドレスの内 48,956 アドレスが日本国内の IP アドレスだった．

表 3 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．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．

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 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 5 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．

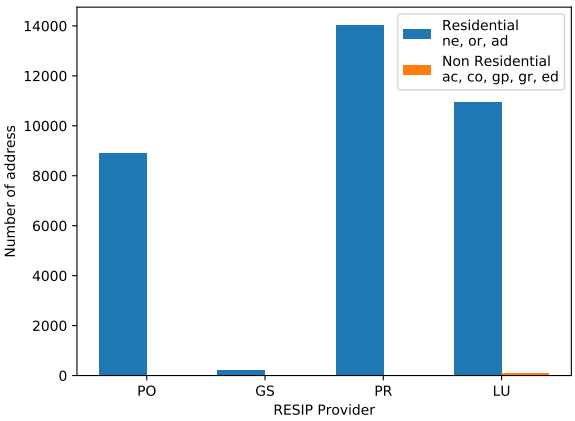

図 3 RESIP プロバイダごとの第 2 レベルドメイン数

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．その中で一般的な第 2 レベルのドメインのものについてのアドレス数を表 6 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．

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 pinpb.ru というドメインだった．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 [10][11] 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．

4.2 RESIP から日本への通信

NICTER 上で RESIP からの通信が観測されているのかを明らかにする．NICTER 上での日ごとの RESIP 観測数を図 4 に示す．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．図 4 から，先行研究 [1] 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．

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 7 に示す．単一の RESIP アドレスからは最大で 62,669 パケットがダークネットに到達していた．

表 7 の 10 個の IP アドレスについて観測されている時期を図 5 に示す．

送信先ポート番号別のパケット観測件数の上位 10 ポー

表 3　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 (%)[8]
東京	12,766	26.1	2,709	84	4,442	5,027	4	26.0
神奈川	3,094	6.3	721	17	1,145	1,087	0	6.4
愛知	2,940	6.0	715	15	1,163	942	0	5.2
大阪	2,917	5.9	769	17	1,148	880	1	6.7
埼玉	2,544	5.1	605	14	1,082	754	0	4.7
千葉	1,912	3.9	484	32	726	557	0	4.0
兵庫	1,722	3.5	460	21	693	493	0	3.5
福岡	1,266	2.5	426	9	436	320	0	4.0
静岡	1,083	2.2	251	7	484	308	0	2.2
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

表 4　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

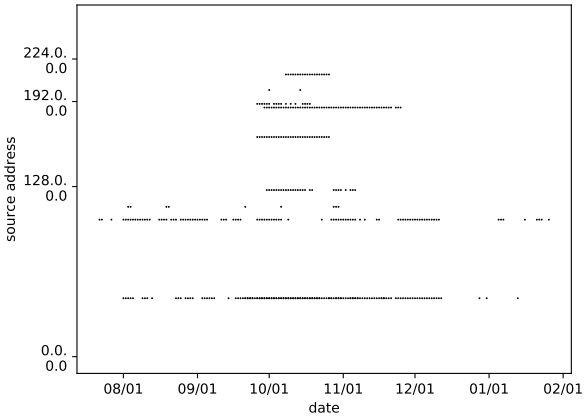

図 5　観測されたアドレスと観測期間

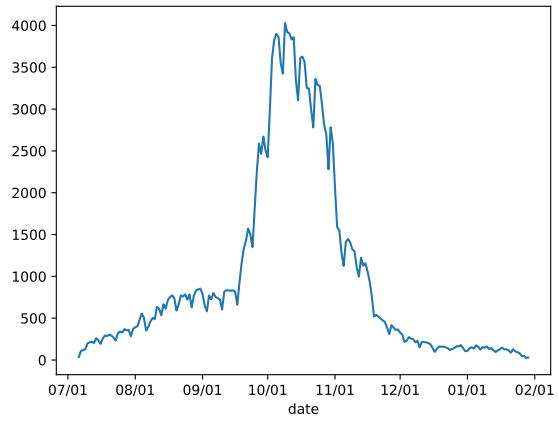

図 4　日別の NICTER で観測された RESIP 数

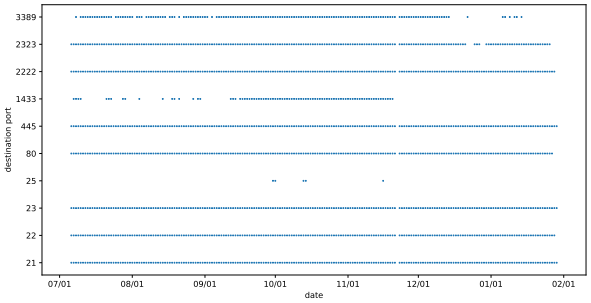

図 6　観測されたポートと時期

トと各ポートを使用するサービスを表 8 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 8 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 6 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．

4.3　考察

1 章で掲げた 5 つの疑問に対して調査結果から考察を行っていく．

表 5　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 の契約数におけるシェア (%)[9]
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	

表 6　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 7　ダークネット上で観測された上位 10 の RESIP アドレス

アドレス	観測日数	RESIP 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

表 8　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

(1) に関して，表 6，図 3 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．

(2)，(3) に関して，表 3 や表 4，表 5 の結果から，RESIP ホストは携帯電話，PHS の契約数の割合とほぼ一致している．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 5 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，今回は付録に記載しているが，47 都道府県全てで RESIP ホストが観測されており，日本全体での対策の必要性があることを示している．

(4) に関して，表 7，図 4，図 5 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．2017 年度の NICTER 観測レポート [12] の宛先ポート番号別の年間観測パケット数割合と比較すると，RESIP ホストから日本のネットワークに対する攻撃が発生していることが明らかである．

(5) に関して，表 8 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．先行研究 [1] 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 6 からは SMTP での通信が行われる期間も短い．

本研究で観測されたパケットが RESIP である住宅用ホストに接続されている機器から送られたものなのか，あるいは RESIP サービス利用者が RESIP ホストを経由して送信したものなのかは，本調査からは明らかになっていない．

5. 結論

本調査から明らかになった結論を報告する．

日本の RESIP ホストは 48,956 個で，先行研究 [1] で観測された全世界の RESIP ホストの 0.79%を占めていた．90.8%が住宅用ホストである．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．

RESIP ホストからの不正な通信は日本のダークネットで観測されており，その数は 1,683,550 件に上った．Mi らは，RESIP サービスを利用した悪性行動の 36.55%がスパムであると報告していたが，本調査による RESIP ホストからの不正な通信の 91%はスキャンを目的とした通信が占めていた．

これらの結果から日本のネットワークが RESIP による脅威に晒されていると結論付ける．RESIP に関する悪性行動への対策が必要である．

先行研究 [1] で収集された RESIP ホストのデータは 2017 年のものであり，表 1 での各 RESIP プロバイダの現状を鑑みると RESIP サービスを取り巻く環境が大きく変化している可能性もある．継続的，多角的な RESIP ホストに関する調査が今後も必要であると考える．

参考文献

[1] 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.

[2] RPaaS: Characterizing Residential IP Proxy as a Service. https://rpaas.site/.

[3] MAXMIND: GeoLite2 Free Downloadable Databases. https://dev.maxmind.com/geoip/geoip2/geolite2/.

[4] APNIC: Whois search. https://www.apnic.net/about-apnic/whois_search/.

[5] 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.

[6] 竹久，神薗，笠間，中里，衛藤，井上，中尾，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.

[7] APNIC: Registration Data Access Protocol. https://www.apnic.net/about-apnic/whois_search/about/rdap/.

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

[9] , http://www.soumu.go.jp/main_content/000523384.pdf.

[10] IPInfoDB. https://ipinfodb.com/.

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

[12] 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.

付　　録

A.1 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