Residential IP Proxy サービスのホストを介した潜在的不正行為の調査

守屋 龍一[1]　北原 拓海[1]　福田 ひかり[1]　菊池 浩明[1]

概要：Residential IP Proxy (RESIP) は，住宅用ネットワークのホスト上で動作するプロキシサーバを提供するサービスである．しかし，不正利用が疑われ，Mi らが行った 2019 年の先行研究では本来の目的以外で RESIP サービスが違法行為に不正利用されていると報告された．この研究を契機に，国内外で RESIP サービスの不正利用に関する調査が行われた．しかしながら、これらの研究では自ら RESIP クライアントになった際の通信情報の調査などに留まっており，一般の RESIP クライアントの行動の詳細は不明であった．そこで本研究では，主要な RESIP である Bright Data, ProxyRack, Oxylabs の 3 つを調査して，RESIP ホストが行う通信を観測した．通信先などのメタ情報から RESIP サービスを介した潜在的な不正行為の考察を行う．

Investigating Potential Malicious Activities via Residential IP Proxy Services

Abstract: Residential IP Proxy (RESIP) is a service that provides a proxy server running on hosts in residential networks. However, RESIP service is suspected of being used illegally. Mi et al. reported in 2019 that RESIP service was illegally used for purposes other than its original purpose. Triggered by this research, many investigations on malicious use of RESIP services have been done so far. Most of these studies were limited to investigating communication that were initiated from sample RESIP clients, and the details of general RESIP clients' behavior were unknown. In this paper, we investigate three major RESIPs, Bright Data, ProxyRack, and Oxylabs, and observe the communication performed by the general RESIP hosts. We discuss some potential malicious behavior through RESIP service based on the meta data of communication.

1. はじめに

近年，住宅用ネットワークを中継するプロキシサービスである Residential IP Proxy（以下 RESIP とする）サービスの市場規模拡大が著しい．検閲や Web スクレイピングに対するアクセス制限の回避を必要とする顧客をターゲットにして，多くのプロバイダが RESIP サービスを提供している．RESIP サービスの概要図を**図 1** に示す．

しかしながら，Mi らによって本来の目的以外で RESIP サービスが違法行為に不正利用されているという指摘 [1] や，RESIP サービスで用いられる住宅用ネットワークの提供者が意図せずに RESIP サービスに参加している可能性の報告 [2] がなされ問題になっている．

Strawberry Donut（仮名）は，フィッシングで集めたクレジットカード情報から現金化をする際に，RESIP サービスで身元を秘匿することが中国の不正フィッシング教室において勧められていることを報告している [3]．半澤らは，RESIP サービスが中継に利用する RESIP ホストに着目して，日本国内に影響を及ぼす RESIP サービスを調査した [4]．住友らは，RESIP サービス不正利用の最新状況を

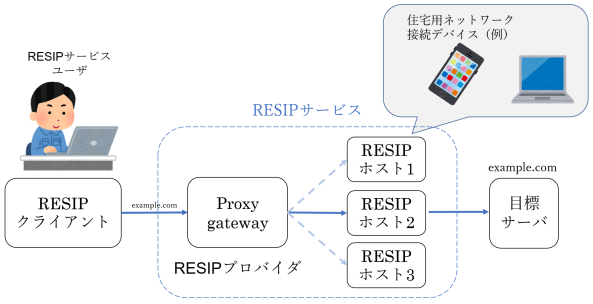

図 1　RESIP サービス概要図
Fig. 1　Overview of RESIP Service.

[1] 明治大学総合数理学部
School of Interdisciplinary Mathematical Sciences, Meiji University

調査している [5]．Mi らは，住宅用ネットワークを RESIP ホストとしてサービスに組み込む機能をもつ Android プロキシアプリを調査している [2]．しかしながら，これらの研究では自ら RESIP クライアントになった際の通信情報の調査などに留まっており，一般の RESIP クライアントの行動の詳細は不明であった．

そこで，本研究は RESIP サービスの不正利用を調査し，その実態を検討することを目的とする．この目的のために，実際に RESIP ホストになり，利用規約の範囲内で利用内容の推測を試みる．RESIP サービスが自身の所有するのネットワークを中継するようになる Windows プロキシアプリについて調査する．そのプロキシアプリを実際に動かすことで得られる RESIP ホストの通信から RESIP サービスに関する不正行為の考察を行う．

2. RESIP サービス

2.1 先行研究

Mi らのモバイルプロキシの調査 [2] では，判明した Android プロキシアプリの総数は 963 個であり，そのうちの 86.60 %がプロキシアプリの悪質性から Google Play 上から削除されていた．一方で，広島県警察本部の報告 [6] によると，無料でダウンロードしたソフトウェアに仕込まれていた MaskVPN や ProxyGate といった Windows 踏み台アプリが不正アクセス等の犯罪に悪用される事例が多発している．

2.2 RESIP クライアントへ与える影響の調査

Google アカウントなどにログインして RESIP サービスを利用した際に RESIP ホストの影響を受けるか，位置情報とターゲット広告を用いて調査を行う．

本調査で利用した RESIP プロバイダは**表 1** の Bright Data[7], ProxyRack[8], Oxylabs[9], Proxy-Seller[10] の 4 社である．Bright Data，ProxyRack，Oxylabs の 3 社は先行研究 [1][2][4][11] にて調査されており，RESIP の所在国とホスト数が多いことから選定した．Proxy-Seller は他の 3 社がアクセスごとに任意にプロキシホストを割り当てることに対して，契約時に指定した地域のアドレスが固定して提供されることから選定した．

表 1 に RESIP プロバイダの主要な機能や特徴を示す．ここで提供しているプロキシの種類は，図 1 の Proxy gateway を介して接続するサービスであり，Bright Data は 4 種類に対して ProxyRack は 2 種類，Oxylabs と Proxy-Seller は 3 種類ある．Proxy-Seller は契約時のみ利用する REIP ホストの所在国を指定することができるが，他の 3 社は利用時に指定が可能である．また，Proxy-Seller の特徴は 3 社よりも RESIP の所在国数は少ないが 1 ヶ月分の料金が安いことである．

行った調査実験の概要を**表 2** に示す．

2.2.1 調査実験 1：位置情報の調査結果

表 3 の◯は全ての RESIP 利用時にプロキシの影響を受け表示結果が変化したものを示す．×は全ての RESIP 利用時にエラーとなり結果が表示されなかったことや結果が RESIP の所在国ではなかったことを示す．

現在地検索では Bright Data と Proxy-Seller の韓国とインドに所在する RESIP ホスト利用時には変化が見られなかった．現在地特定では Firefox 利用時において，どのプロキシプロバイダを利用しても現在地特定が成功した．

2.2.2 調査実験 2，3：ターゲット広告の調査結果

表 4 に結果を示す．列が観測方法, 行が訪れたサイト, 値は表示された広告のうち影響を受けた広告の割合，Oxylabs の“×”は広告が表示されなかったことを示す．

yahoo は日本以外からのアクセスを制限しているため他のサイトに比べて低い．Bright Data で rocket の 0.12 が最も低く，Proxy-Seller で smart の 0.70 が最も高い．プロバイダの比較をすると Bright Data が 0.42 で他の 2 社に比べて影響を受けていない．また，Proxy-Seller が rocket を除いた 3 つのサイトにおいて影響を受けた割合が最も高い．

2.2.3 考察

自動で全広告数が減ったことの原因として一部の広告が取得できていないこと，広告が短時間の表示であること，広告が表示されるまでに時間がかかることが考えられる．

Proxy-Seller のインドと韓国に所在する RESIP については，一部の IP アドレスの所在地などを確認できる web サイト [13] にて指定した国とは異なる国が表示された．web サイト [13] で調査した RESIP ホストの所在地と現在地検索結果が同じ地域であったため，RESIP に紐づいている地域が実際の所在地と異なることが RESIP 原因だと考える．

2.2.4 まとめ

調査実験より，アカウント利用時においても RESIP サービスの影響を受けることがわかった．RESIP を用いることで通常時とは異なる結果が表示されるため，位置情報とターゲット広告の偽装が可能であることが判明した．

3. RESIP ホスト

3.1 Windows プロキシアプリの調査

RESIP ホストの立場で RESIP サービスに参加するため，Windows プロキシアプリを調査した．Windows を調査対象にした理由は，デスクトップ OS の中で最もシェア率が高く，Android プロキシアプリのように Google Play による削除も期待できないため，報告 [6] にもあるような踏み台アプリケーションが無数に存在し，誤ってインストールする確率が高いと考えたためである．

代表的な RESIP サービスである Bright Data の Windows プロキシアプリを調査した結果を**表 5** に示す．

2022 年 6 月時点で，Hola VPN と SunsetScreen，EarnApp は Bright Data の Windows プロキシアプリであり，それは

表 1　RESIP プロバイダ比較
Table 1　RESIP Provider Comparison.

プロバイダ名	Bright Data	ProxyRack	Oxylabs	Proxy-Seller
本社所在地	イスラエル	香港	リトアニア	キプロス共和国
プロトコル	HTTP/HTTPS, Socks4, Socks5	HTTP/HTTPS, Socks4, Socks5	HTTP, HTTPS	Socks5, HTTPS
1 ヶ月分の料金	USD15.00~/GB	USD49.95~/10GB	USD15.00~/GB	USD1.64~/IP
RESIP の所在国数	195 か国	195 か国	195 か国	50 か国
用いたプラン名	Residential Proxies	25 Private Unmetered Residential Ports	Residential Proxies	Proxy IPv4
RESIP 所在地指定	○	○	○	契約時に指定
リクエストごとに RESIP を変更	○	×	○	×

表 2　調査実験の目的と日数，方法
Table 2　Objectives, methodologies, and specifications of experiments.

番号	日数	目的	方法
調査実験 1	2022 年 8 月 27 日〜9 月 11 日（16 日間）	位置情報が実験地から変化することを調査	gmap，ymap，mapfan にて現在地検索と現在地特定を行う
調査実験 2	2022 年 8 月 27 日〜9 月 11 日（16 日間）	ターゲット広告の表示言語やターゲットへの影響を調査	ターゲット広告の表示言語やターゲットへの影響を調査
調査実験 3	2022 年 11 月 24 日〜12 月 1 日（7 日間）	調査実験 2 の自動化による調査件数の増加と調査実験 2 との比較を調査	青山 [12] の自動観測プログラムを用いて広告を取得し条件に合致するか確認を行う

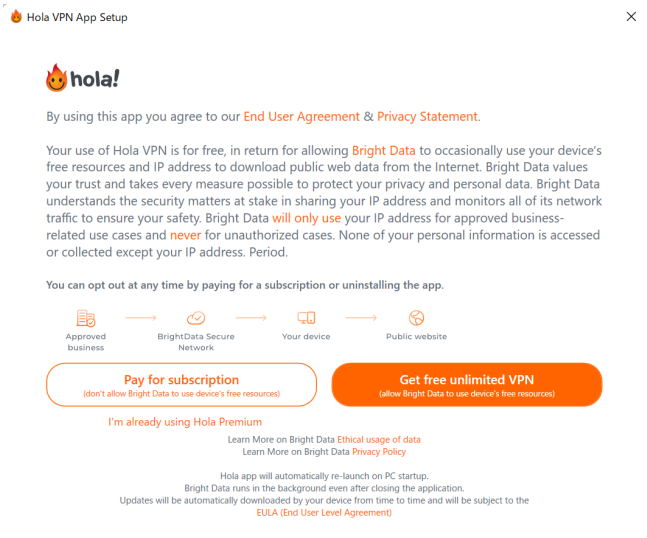

図 2　Hola の同意画面
Fig. 2　A user consent window in Hola.

セットアップ時に**図 2** のような同意画面が表示されることから確認できた．

また，Bright Data と並んで代表的な RESIP プロバイダである ProxyRack と Oxylabs の Windows プロキシアプリについても調査を行った．

RESIP サービスの通信を中継する機能をもつ Windows プロキシアプリ関して，ProxyRack では Web サイト内 [14] で，Oxylabs では住宅用プロキシネットワークに関する独占契約を結んだ Honeygain[15][16] で Windows プロキシアプリの存在を確認できた．Oxylabs は RESIP ホスト収集をアウトソーシングする点で異なっていたが，ProxyRack と Oxylabs の Windows プロキシアプリは Bright Data が提供する EarnApp と同様の機能を有しており，インターネット接続しているデバイスのリソースを提供することで受動的収入を得るアプリケーションだった．

3.2　RESIP 検知

自身が RESIP ホストになっていることを判断するには，ホストでパケットを観測してその通信路の情報を調査する方法 [17] がある．RESIP ホストとなって様々なアドレスにアクセスする際，プロキシアプリの Proxy gateway との定期的な通信が行われる．

4.　実験

4.1　実験目的

本実験は，以下の 3 点を目的とする．

(1) RESIP 検知プログラムの開発と評価を行う．
(2) 不正通信に関する 3 つの RESIP ホストの差を明らかにする．
(3) RESIP ホスト経由での潜在的不正行為を明らかにする．

4.2　実験環境

ノート PC（Lenovo ThinkPad X1 Carbon 5th Signature Edition, Windows10 Education）と，b-mobileSIM を日本国内で使用した．RESIP ホスト環境を用意するのに用いた Windows プロキシアプリを**表 6** に示す．

4.3　実験方法

4.3.1　実験 1：RESIP 検知プログラムの開発と評価

2022 年 11 月 24 日から 11 月 28 日までの期間に，家庭内 LAN（東京都）に接続した Windows 10 端末で本実験を行った．通常時と表 6 の 3 つのプロキシアプリのホストとなり，各アプリについて 5 分× 100 回の通信を観測して

表 3 位置情報の調査結果
Table 3 Experimental results on location estimation.

RESIP	Microsoft Edge		Google Chrome		firefox	
プロバイダ	現在地検索	現在地特定	現在地検索	現在地特定	現在地検索	現在地特定
Bright Data	×	○	×	○	×	○
ProxyRack	○	×	○	×	○	○
Oxylabs	○	×	○	×	○	○
Proxy-Seller	○（US，JP） ×（KR，IN）	×	○（US，JP） ×（KR，IN）	×	○（US，JP） ×（KR，IN）	○
通常	○	○	○	○	○	○

表 4 広告調査結果
Table 4 Ad Survey Results.

観測サイト	Bright Data	ProxyRack	Oxylabs	Proxy-Seller
yahoo	0.00	0.00	×	0.00
game	0.39	0.29	×	0.50
folk	0.53	0.35	×	0.32
rocket	**0.04**	0.38	×	0.10
smart	0.70	0.57	×	**0.70**
平均	0.41	0.40	×	0.40

表 5 Bright Data の Windows プロキシアプリ例
Table 5 Windows Proxy Apps Used by Bright Data.

実行ファイル名	概要
Hola VPN[18]	ピアツーピアネットワークを介した VPN アプリケーション
SunsetScreen	ディィスプレイの明るさを自動調整するフリーソフト
EarnApp[19]	Bright Data が提供しているインターネット接続している未使用のデバイスのリソースを利用して受動的収入を得るアプリケーション

表 6 使用する Windows プロキシアプリ
Table 6 Windows Proxy Apps.

RESIP プロバイダ	Windows プロキシアプリ
Bright Data	Hola VPN [18]
ProxyRack	ProxyRack アプリ [14]
Oxylabs	Honeygain [15]

図 1 における Proxy gateway と目標サーバの通信先 IP アドレスを収集した．本観測ではプロキシアプリを起動した後 100 秒待機してからホストの通信を 5 分間観測し，その後プロキシアプリを再起動することで，確立された接続をリセットするようにした．

調査対象のプロキシアプリの通信を観測して定期的にアクセスを行う IP アドレスを記録することで，各プロキシアプリの通信の特徴と RESIP 検知プログラムのブラックリストに登録すべきアドレスについて調査を行う．

(1) 表 6 の 3 つの RESIP アプリについて，5 分のパケット収集を 100 回行う．

(2) 実験 1 で収集した IP アドレスについて，継続的に通信が行われていたものを IP ブラックリストに記録し，作成した RESIP 検知プログラムの精度を調査する．

表 7 実験で使用したプロキシアプリ及び収集した IP アドレスとパケット数
Table 7 IP addresses and packets counts collected from Proxy apps.

使用したプロキシアプリ	IP	パケット
なし (通常時)	48	1786
Hola VPN	141	11192
ProxyrRack アプリ	325	89416
Honeygain	703	208820

4.3.2 実験 2：RESIP ホスト比較実験

2022 年 7 月 13 日から 7 月 17 日までの 5 日間で，Bright Data，ProxyRack 及び Oxylabs それぞれの RESIP ホスト環境と RESIP ホストではない環境で実験を行う．RESIP ホストでない環境は，Wireshark 以外のアプリを自発的に起動していない状態である．4 つの環境でそれぞれ 5 時間 Wireshark を用いて通信を観測する．パケットから観測日時，通信 IP アドレス，通信ドメイン，通信ポート及びパケット長を抽出する．

ドメインの分析に VirusTotal による悪性判定とカテゴリ分類を行う．ドメインの悪性判定に関して，VirusTotal で “malicious” もしくは “suspicious” と 1 つでも判定されたドメインを悪性と定める．

4.3.3 実験 3：RESIP ホスト 24 時間観測

2022 年 10 月 15 日から 10 月 17 日の 3 日間で，Bright Data 及び ProxyRack の RESIP ホスト環境で実験を行う．継続的に 24 時間以上 RESIP ホスト環境で通信を観測するとパケットキャプチャファイルのデータ量が膨大になると考えた．そこで，pyshark でパケットのリアルタイム分析を行うシステムを実装し，宛先 IP アドレスと通信ドメインのみを自動取得する．

RESIP ホストのグローバル IP アドレスを 60 秒ごとに記録し，NICTER Darknet[20] を用いて国内のダークネットで観測された不正通信の IP アドレスと突合する．

4.4 実験結果

4.4.1 実験 1：RESIP 検知プログラムの開発と評価

通常時と 3 つのプロキシアプリについて収集した IP アドレスの数とパケットの数を**表 7** に示す．

収集した IP アドレスを元に RESIP ホスト検知プログラムに使用するブラックリストを作成した．登録した IP アド

表 8 ブラックリストに登録した IP アドレスの割当国
Table 8 Blacklisted IP addresses and its countries .

IP アドレス	割当国	whois
3.228.x.x	アメリカ	Amazon Technologies Inc.
3.94.x.x	アメリカ	Amazon Technologies Inc.
162.125.x.x	アメリカ	Dropbox, Inc.
81.31.x.x	ドイツ	JAGEX
23.227.x.x	アメリカ	Leaf Group Ltd.
38.84.x.x	アメリカ	PSINet, Inc.
104.16.x.x	アメリカ	Cloudflare, Inc.
104.26.x.x	アメリカ	Cloudflare, Inc.
18.65.x.x	アメリカ	Amazon Technologies Inc.
34.237.x.x	アメリカ	Amazon Technologies Inc.

表 9 RESIP 検知プログラムの精度 [%]
Table 9 Accuracy of RESIP detection program.

	Hola VPN	ProxyRack アプリ	Honeygain
従来手法 [17] TP	100	99	100
従来手法 [17] TN	88	88	88
提案手法 TP	99	98	100
提案手法 TN	100	100	100

表 10 単位時間（30 分）あたりの観測された IP アドレス数とドメイン数
Table 10 Number of IP addresses and domains observed per unit time (30 minutes).

	IP アドレス数			ドメイン数		
	総数	平均	最大	総数	平均	最大
Bright Data	**654**	**128.3**	**205**	**430**	**90.1**	**152**
ProxyRack	172	66.7	97	68	29.7	54
Oxylabs	306	62.1	120	173	34.0	87
通常時	45	13.0	19	27	5.6	13

レスの割当国と whois 情報を**表 8** に示す．登録した IP アドレスは，実験 1 での 100 回の観測のうち 80 回以上観測したアドレスの上位 16 ビットに限定した．ただし Honeygain のパケットの観測でのべ 190 回観測した 20.198.x.x は通常時でも観測されるアドレスのため，最終的にはその 1 つを除いた計 10 個の IP アドレスをブラックリストに登録した．

作成したブラックリストを用いて，収集したパケットを判定した結果を**表 9** に示す．

RESIP ホストである偽陽性は 100 回の実験では起こらなかった．

4.4.2 実験 2：RESIP ホスト比較実験

表 10 に収集した宛先 IP アドレスとドメインの総数を示す．Bright Data の RESIP ホストが IP アドレスとドメイン共に高い値を示した．3 つの RESIP ホストの中で最も低い値を示した ProxyRack の RESIP ホストも，通常時と比較して IP アドレスは 3.8 倍，ドメインは 2.5 倍になっていた．RESIP ホスト環境では通常時の通信に加えて，RESIP サービスによる通信の中継作業があるため，多くの IP アドレスとドメインとの通信を行っていると考えられる．

表 11 ドメインの悪性判定結果
Table 11 Number of malicious domains.

	Bright Data	ProxyRack	Oxylabs
悪性総数	24	4	7
悪性割合 [%]	5.6	5.9	4.0

表 12 ドメインのカテゴリ分類結果
Table 12 Domain categories.

	Bright Data	ProxyRack	Oxylabs
Travel	23(5%)	1(1%)	2(1%)
Shopping	**57**(**13**%)	5(7%)	4(2%)
Advertisements	46(11%)	0(0%)	**64**(**37**%)
Social Networking	13(3%)	**10**(**15**%)	11(6%)
Web Analytics	18(4%)	0(0%)	12(7%)
Finance	9(2%)	1(1%)	1(1%)
Search Engine	18(4%)	3(4%)	27(16%)
News	1(0%)	1(1%)	9(5%)

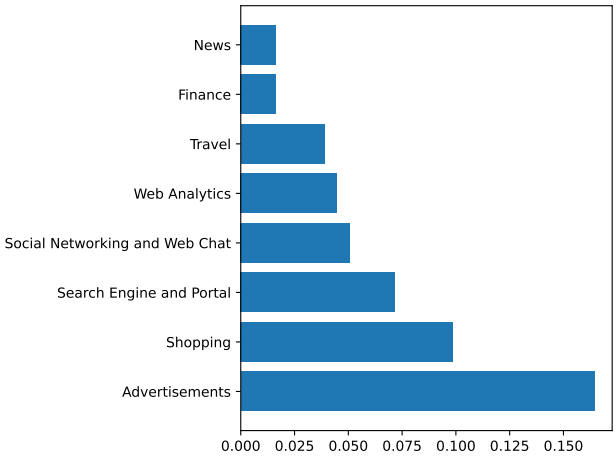

図 3 全通信のドメインカテゴリ割合
Fig. 3 Domain Category Percentage of All Communications.

表 13 悪性ドメイン例（2022 年 10 月 9 日時点）
Table 13 Sample malicious domains (as of October 9, 2022)

ドメイン	RESIP プロバイダ
cpi-offers.com	Bright Data
api.bdisl.com	Bright Data
ariesbee.com	Oxylabs

2022 年 10 月 8 日と 10 月 9 日時点で，ドメインの悪性判定結果を**表 11** に示し，VirusTotal の分類タグを用いてドメインのカテゴリ分類をした結果を**表 12** と**図 3** に示す．

表 11 から，どの RESIP ホストも一定の割合で悪性サイトに接続していることが分かった．RESIP ホストが通信を行った悪性サイトの多くはフィッシングやマルウェア攻撃に関わっているサイトである．その一例を，**表 13** に示す．ここで api.bdisl.com は，IPA の 2020 年度の報告書 [21] において述べられている不正プログラムへの感染や実行，フィッシング詐欺被害等の脅威がある不正サイトである．

表 12 に，VirusTotal で判定した通信先のカテゴリーを示

表 14　PUP のトラフィック分析結果 [1]
Table 14　PUP Traffic Analysis Results[1].

Category	割合 [1]	本調査	順位
ad	75%	16.4%	1
search engines	8%	7.2%	3
shopping	7%	9.9%	2
malicious websites	5%	5.2%	4
social networks	2%	5.1%	5

表 15　1 日観測データの総数
Table 15　Total number of daily observation data.

	IP アドレス	ドメイン	国数
Bright Data	2315	1319	29
ProxyRack	572	524	72

す．Bright Data と Oxylabs の RESIP ホストでは高かった広告やウェブアナリティクスの割合が，ProxyRack では極めて低い．一方，ProxyRack では SNS への通信の頻度が高く，RESIP プロバイダによる通信用途の差異を確認できる．

図 3 に，3 つのプロバイダーを合わせた全通信先のカテゴリー分布を示す．RESIP ホスト全体で広告に関するドメインへの通信の割合が多いことが分かる．また，ファイナンスに関するドメインにも通信が行われていた．

Mi らが調査した 2017 年時点で RESIP サービスをプロキシする PUP（不審なプログラム）のトラフィックログからトラフィック量が多い上位 1,000 の宛先 [1] を**表 14**[*1]に示す．広告やショッピング，検索エンジンに関するドメインが多い点で共通していた．また，本調査では SNS に関するドメインの割合の増加が確認できた．

4.4.3　実験 3：RESIP ホスト 24 時間観測実験

表 15 に pyshark で収集した宛先 IP アドレスとドメイン総数，IP アドレスから判定された国の数を示す．

ファイナンス関連のドメインについて調査したところ，本実験で共通して決済サービスである Paypal のドメインが観測できた．Bright Data の RESIP ホストは Paypal 以外にも，Amazon アカウントを使った決済サービスである Amazon Pay やメルカリアプリでのスマホ決済サービスである merpay，三菱 UFJ ニコスと NTT データによる決済代行サービスである PAYGENT，グローバル決済ソリューション企業の Netcerera，中国のモバイル決済サービスの Alipay，NTT データのキャッシュレス決済総合プラットフォームである CAFIS のような決済サービスやクレジットカード決済で使用されるサービスとの通信が行われていることが確認できた．RESIP ホストを送信元としたそれぞれの宛先パケット数の割合を**図 4** に示す．

RESIP ホストと決済サービスとの通信時間の分布を**図 5**（Bright Data）と**図 6**（ProxyRack）に示す．パケットの送信間隔が 60 秒以内のものを一連のセッションと判断する．

RESIP ホストの IP アドレスと NICTER Darknet を用いて国内のダークネットで観測された不正通信の送信元 IP アドレスとの突合結果を**表 16** に示す．

[*1] 本調査では VirusTotal の分類タグを用いて分類したため，未分類のドメインが存在する．本調査の malicious websites についてのみ，表 11 の結果に準ずる．

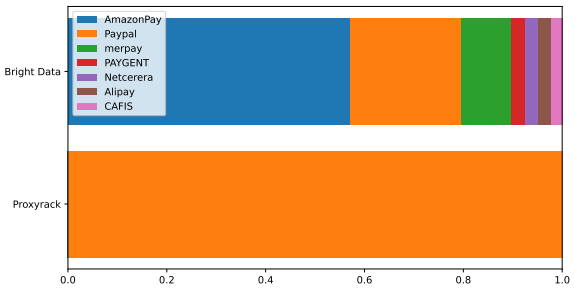

図 4　RESIP ホストと決済サービスとの通信
Fig. 4　Communication between RESIP host and payment service.

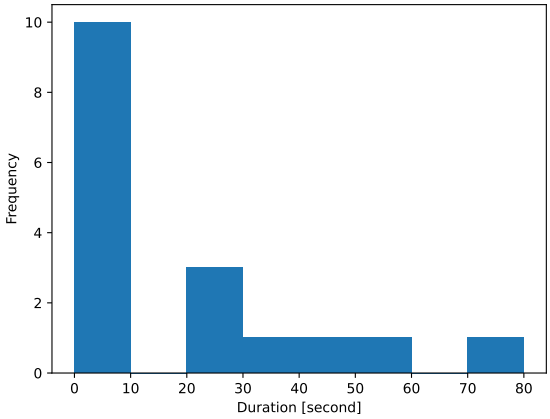

図 5　Bright Data の RESIP ホストと決済サービスとの通信時間分布
(2022 年 10 月 15 日 17 時 15 分から 24 時間)
Fig. 5　Distribution of communication time between Bright Data's RESIP hosts and payment services (24 hours from 5:15 p.m. on 10/15/2022)

表 16　RESIP ホストと NICTER 上の IP アドレスの突合
Table 16　IP addresses of RESIP hosts mached in NICTER.

一致数	0
[4] で報告された一致数	59,816

4.5　考察

4.5.1　RESIP プロバイダの差

観測できた IP アドレスとドメインの数，通信ドメインのカテゴリや通信 IP アドレスから，Bright Data，ProxyRack 及び Oxylabs の 3 つの RESIP ホストの差について明らかにすることができた．

表 12 のようにドメインカテゴリが RESIP サービスごと

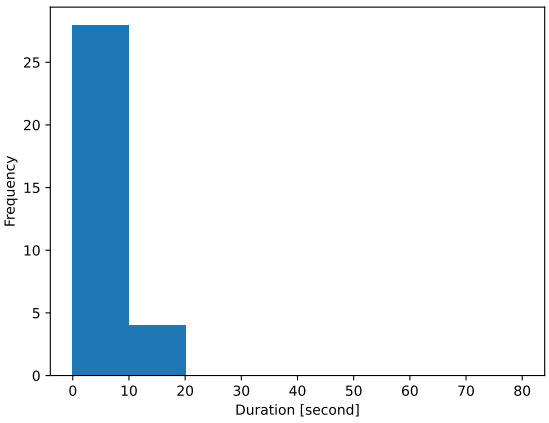

図 6 ProxyRack の RESIP ホストと決済サービスとの通信時間分布
(2022 年 10 月 16 日 18 時 30 分から 24 時間)

Fig. 6 Distribution of communication time between ProxyRack's RESIP hosts and payment services (24 hours from 18:30 on October 16, 2022)

に異なっていたことから，RESIP サービスは利用用途に差があると考えられる．

4.5.2 悪性サイトとの通信

表 11 で RESIP ホストが悪性サイトと通信を行っていた理由として，フィッシング運営などの作業に RESIP サービスを利用しているためだと考える．RESIP サービスは匿名で通信を行うことができるため，身元を追跡されるのを防いでいる．

2017 年に Mi らによって調査された結果である表 14 の malicious websites が 5%であったことと，本調査の表 11 で各 RESIP サービスで 5%前後の値を示したことから，悪性サイトとの通信の割合は大きく変化していないと考える．

4.5.3 広告不正

図 3 のように広告に関するドメインとの通信が多い結果となった理由として，RESIP サービスを悪用したクリックボットを利用した広告クリック詐欺の可能性がある．例えば，不正 Web サイト運営者は，自分の Web サイト対して RESIP ホストを介してアクセスを偽装することで，広告ネットワーク事業者から不正に収益を得ることができる．リクエスト毎に IP アドレスを変更できる RESIP サービスを用いれば，クリックボットの検出が困難になるためである．

[22] によると，PPC 広告の支出のうち 14%が無効なクリックであり，2020 年末までに世界のマーケティング担当者に 237 億ドルの年間損失をもたらしたと試算されている．このことから，RESIP サービスを用いた広告に関する不正行為が行われているという仮定は支持できる．

実験 1 で広告関連のドメインは 110 個観測され，15 時間で 347 回の通信が行われていた．この通信がすべてクリックであり，Google ディスプレイ広告の平均 CPM である 3.12 ドル [23] を参考にして 1000 クリックのインプレッション広告単価が 3.12 ドルとした場合，1 ヵ月あたり 1 つの RESIP ホストは 51.97 ドルの被害を生むことになる．

住友ら [5] は，RESIP サービスによって 1 ヵ月以内でおよそ 7 万の IP アドレスを中継することに成功していることから，RESIP サービス全体では 3,637,670 ドル以上の被害を生んでいると見積もられる．

4.5.4 マネタイズ

RESIP ホストが Paypal やファイナンス関連のドメインと通信を行っていたことに関して，フィッシングで不正に入手したアカウントを用いたマネタイズ（現金化）の際に，決済サービスやクレジットカードを用いた不正行為が行われていたと考える．図 5 のように 20 秒以上の継続した通信が観測されていることから，手動による通信の可能性が高い．RESIP サービスの使用料は最低 15 ドル必要な高価なものなので，ただ買い物をするために使っている可能性が低いとため，マネタイズが行われていると考える．Paypal を始めとしたオンライン決済サービスは，登録時の国からのみログインできる設定であることが少なくないため，地理的制限を回避し海外からの不正ログインできる点で RESIP サービスが悪用される可能性がある．

4.5.5 ダークネット

半澤らの研究 [4] では RESIP ホストの IP アドレスから国内ダークネットへの通信が観測されていたが，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，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が明らかになっていなかった．[5] によると，RESIP ホストの開放ポートに注目することで，RESIP ホストは脆弱性を利用されたデバイスの割合が高いと推測されていた．

本実験では，Windows プロキシアプリ以外の疑わしいプロセスが起動していない状態で，RESIP サービスの通信を中継していた．表 16 に示すとおり，本実験では RESIP ホストから国内ダークネットへの通信が観測できなかった．従って，[4] で RESIP ホストの IP アドレスから国内ダークネットへの通信が観測された原因は，RESIP サービスのクライアントユーザが RESIP ホストを介して送信したからではなく，プロキシアプリと同時に感染していたマルウェアによるデバイスから国内ダークネットへのポートスキャンが行われた可能性が高いと考える．

5. 本研究の適法性と倫理考慮

[18][14][15] を用いた研究を行うにあたって，Hola VPN のセットアップの同意（図 2），ProxyRack のライセンス契約書や Honeygain の利用規約を確認し，定められた規約の範囲での本研究を行った．

次の倫理的配慮を行って研究を進めた．

- 利用規定で禁じられている逆コンパイル，逆アセンブ

ルやリバースエンジニアリングを行わない．

- 特定のクライアントの通信を追跡，保存せず，十分な長さの期間内の複数のクライアントが混在した通信先を観測した．
- パケットのペイロードはアクセスせず，ヘッダーのみを観測した．

これらの取組が，サービスの透明性を高めて，ネットワークの健全な利用が進むことを目指している．

6. おわりに

本研究では，RESIP ホストとなる複数の Windows プロキシアプリを用いて，RESIP ホストがどのような通信を行うのかを明らかにした．

RESIP サービスに関する不正行為については，広告や決済サービスに関する不正の可能性を示すことができた．RESIP ホストから国内ダークネットへの通信が観測できなかったことから，先行研究 [5] で述べられた脆弱性を利用されたデバイスが RESIP ホストになっている可能性を支持する結果を示すことができた．

RESIP サービスを悪用した不正行為の詳細について明らかにし，RESIP ホストの通信観測をさらに長期間行える環境をつくることが今後の課題である．

謝辞

本研究を進めるにあたって有益な助言を頂いた，NTT 社会情報研究所の秋山 満昭氏に感謝いたします．

参考文献

[1] Xianghang Mi et al. , “Resident Evil: Understanding Residential IP Proxy as a Dark Service”，IEEE Symposium on Security and Privacy (SP), volume: 1, pp. 170-186, 2019.
[2] Xianghang Mi，et al. , “Your Phone is My Proxy: Detecting and Understanding Mobile Proxy Networks”，NDSS Symposium 2021，pp.1-18，2021.
[3] Strawberry Donut,“Understanding the Chinese underground card shop ecosystem and becoming a phishing master by Strawberry Donut”（ 入手先 ⟨https://www.slideshare.net/codeblue_jp/cb22-understanding-the-chinese-underground-card-shop-ecosystem-and-becoming-a-phishing-master⟩，2023 年 1 月参照)，CODE BLUE 2022.
[4] 半澤，菊池,“Residential IP Proxy サービスに悪用される住宅用ホストの調査”，コンピュータセキュリティシンポジウム 2019 論文集，pp. 918-925，2019.
[5] 住友，菊池,“Residential IP Proxy サービスを悪用した不正行為の調査”，第 84 回全国大会講演論文集，pp. 555-556，2022.
[6] 広島県警察本部サイバー犯罪対策課，“Cyber Crime Control Project 令和 3 年 第 1 号 ―知らないうちに踏み台に―”，(https://www.pref.hiroshima.lg.jp/uploaded/attachment/417114.pdf，2022 年 10 月参照)．
[7] Bright Data（https://brightdata.com/，2022 年 10 月参照)．
[8] ProxyRack（https://www.proxyrack.com/, 2022 年 10 月参照)．
[9] Oxylabs（https://oxylabs.io/，2022 年 10 月参照)．
[10] Proxy-Seller, (https://proxy-seller.com/, 2022 年 12 月参照)．
[11] 福田，井窪，菊池,“Residential IP Proxy サービスを用いた位置情報・ターゲット広告の調査”，第 84 回情報処理学会全国大会，pp. 557-558，2022.
[12] 青山，菊池,“ターゲット広告はどのペルソナで最も多いのか？”，第 100 回 CSEC 研究会，2023.
[13] WhatIsMyIPAddress.com,（https://whatismyip-address.com/，2022 年 12 月参照)．
[14] ProxyRack,“Become A Peer Earn passsive income”（https://www.proxyrack.com/become-a-peer/，2022 年 10 月参照)．
[15] Honeygain（https://www.honeygain.com/，2022 年 10 月参照)．
[16] Oxylabs,“Oxylabs Signs Exclusive Contract with Honeygain”（https://oxylabs.io/blog/oxylabs-signs-exclusive-contract-with-honeygain, 2022 年 10 月参照)．
[17] A. Tosun，M. De Donno，N. Dragoni and X. Fafoutis,“RESIP Host Detection: Identification of Malicious Residential IP Proxy Flows”，2021 IEEE International Conference on Consumer Electronics (ICCE)，pp. 1-6，2021.
[18] Hola VPN（https://hola.org，2022 年 10 月参照)．
[19] EarnApp（https://earnapp.com/，2022 年 10 月参照)．
[20] 竹久他,“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.
[21] IPA・東日本電信電話株式会社,“令和 2 年度中小企業サイバーセキュリティ対策支援体制構築事業（実証対象：北海道）成果報告書”（https://www.ipa.go.jp/files/000091309.pdf，2022 年 12 月参照)．
[22] Roberto Cavazos,“The Economic Cost of Invalid Clicks in Paid Search and Paid Social Campaigns”（https://irp-cdn.multiscreensite.com/9d8f1a2e/files/uploaded/UniBaltimore%20PPC%20Fraud%20%281%29.pdf，2022 年 12 月参照)．
[23] TOPDRAW, “ONLINE ADVERTISING COSTS IN 2021”（https://www.topdraw.com/insights/is-online-advertising-expensive/，2022 年 12 月参照)．