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 †
明治大学総合数理学部 先端メディアサイエンス学科 菊池研究室 †

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．

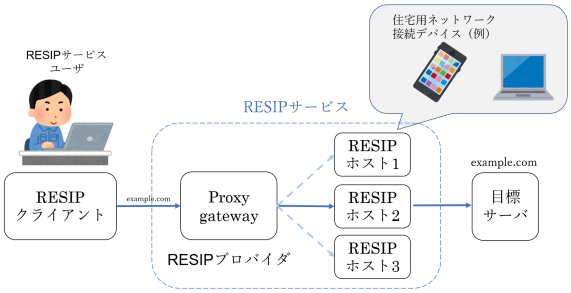

図 1 RESIP サービス概要図

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．

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 [3]．住友らは，RESIP サービス不正利用の最新状況を調査している [4]．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．

†Kikuchi Laboratory, Department of Frontier Media Science, School of Interdisciplinary Mathematical Science, Meiji University.

2 事前準備

2.1 利用ツール

本研究では，ViruTotal，Wireshark，pyshark，GeoLite2 Free Geolocation Data 及び NICTER Darknet を利用した．表 1 に使用したツールの説明と利用目的を示す．

2.2 先行研究

福田らが報告 [10] した RESIP プロバイダを比較した表 2 によると，モバイルプロキシに対応しているプロバイダが多いことが分かる．モバイルプロキシを調査した [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ると報告した．

一方で，広島県警察本部の報告 [11] 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．

3 Windows プロキシアプリの調査

3.1 調査目的

本調査では，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する．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 [11] 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．

3.2 RESIP プロバイダの予備調査

代表的な RESIP サービスである Bright Data[12] の Windows プロキシアプリを調査を行った．

2022 年 6 月 8 日に，Bright Data の RESIP クライアント側から Proxy Gateway に接続し，Bright Data の Proxy Gateway IP アドレスを収集した．収集した IP アドレスを VirusTotal を用いて調査した結果を表 3 に示す．

悪性だと判定された 6 個の IP アドレスの判定結果を詳しく見たところ，過去に brd-cdn.com や luminatinet.com，lum-sdk.io などのサブドメインから名前解決された IP アドレスだったことが分かった．brd-cdn.com，luminatinet.com 及び lum-sdk.io は Bright Data や Luminati（Bright Data の旧名）に関連する文字列を持つドメインであることから，3 つのドメインとそれらのサブドメインに対して通信を行った Windows 実行ファイルが Bright Data の Windows プロキシアプリであると推測できる．なお，2022 年 10 月 28 日時点で，VirusTotal に記録されている Bright Data に関連する文

表 1　利用ツールの概要と用途

ツール名	概要	用途
VirusTotal[5]	ファイルやウェブサイトの マルウェア検査を行う脅威判定プラットフォーム	RESIP ホストが通信したドメインの 悪性判定，カテゴリ分類など
Wireshark[6]	ネットワークを流れるパケットを 観測できるパケットキャプチャツール	RESIP ホストが行う通信の観測
pyshark[7]	Python でリアルタイムパケット分析を 可能にするパッケージ	RESIP ホストが行う通信の観測
GeoLite2 Free Geolocation Data[8]	IP アドレスから地理情報を判定できるデータベース	RESIP ホストが通信した IP アドレスの国判定
NICTER Darknet[9]	分析基盤 NONSTOP によって遠隔で使用できる 情報通信研究機構（NICT）の国内ダークネット宛ての トラフィックデータ観測情報	RESIP ホストが国内ダークネットに 対して通信を行ったか調査

表 2　RESIP プロバイダ比較（[10] より引用し一部改変）

プロバイダ	Bright Data	ProxyRack	Oxylabs	Proxy-Seller
提供しているプロキシの種類	Residential proxies, ISP proxies, Datacenter proxies, Mobile proxies	Residential proxies, Datacenter proxies	Datacenter Proxies, Residential Proxies, Next-Gen Residential Proxies	Proxy IPv4, Proxy IPv6, Mobile Proxy LTE

表 3　Bright Data の Proxy Gateway IP アドレス

IP アドレス総数	悪性 IP アドレス数
60	6

字列を持つドメインのサブドメイン数は表 4 の通りであり，膨大な数のサブドメインを使い回しているしていることが分かる．

表 4　Bright Data に関連するドメインのサブドメイン数

ドメイン	サブドメインの数
brd-cdn.com	2070
luminatinet.com	2480
lum-sdk.io	1130

VirusTotal を用いて，これらのドメインと通信を行った Windows 実行ファイル名を調査した結果を表 5 に示す．

表 5　Bright Data に関連するドメインと通信を行った Windows 実行ファイル例

実行ファイル名	概要
Hola VPN[13]	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	ディスプレイの明るさを 自動調整するフリーソフト
EarnApp[14]	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

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[15] と Oxylabs[16] の Windows プロキシアプリについても調査を行った．

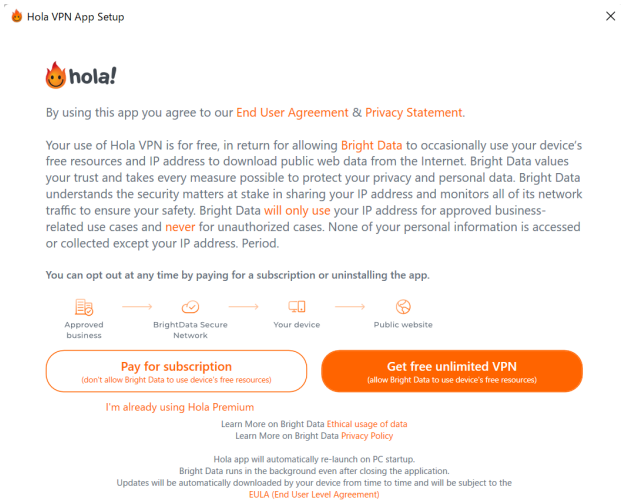

図 2　Hola の同意画面

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 [17] 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[18][19] 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．

4　実験

4.1　実験目的

本実験は，以下の 2 点を目的とする．

1. 不正通信に関する 3 つの RESIP ホストの差を明らかにする．
2. 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．

表 6　使用する Windows プロキシアプリ

RESIP プロバイダ	Windows プロキシアプリ
Bright Data	Hola VPN [13]
ProxyRack	ProxyRack Point of Presence [17]
Oxylabs	Honeygain [18]

4.3 実験方法

4.3.1 実験 1：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．

GeoLite2 Free Geolocation Data による国判定，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．

4.3.2 実験 2：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 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 ホスト比較実験

表 7 と表 8 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 7　単位時間（30 分）あたりの観測された IP アドレス数

	総数	平均	最大
Bright Data	**654**	**128.3**	**205**
ProxyRack	172	66.7	97
Oxylabs	306	62.1	120
通常時	45	13.0	19

表 8　単位時間（30 分）あたりの観測されたドメイン数

	総数	平均	最大
Bright Data	**430**	**90.1**	**152**
ProxyRack	68	29.7	54
Oxylabs	173	34.0	87
通常時	27	5.6	13

宛先 IP アドレスの上位 3 国を表 9 に示す．宛先 IP アドレスの国判定の結果，アメリカと日本が上位であることが共通していた．また，表 7 で IP アドレス数が RESIP サービスの中で最も低かった ProxyRack が国数では Bright Data の 1.7 倍と最も高い値を示していたことから，ProxyRack では多くの国と通信を行っていることが分かった．

表 9　宛先 IP アドレスの上位 3 国

	1 位	2 位	3 位	国総数
Bright Data	アメリカ	日本	シンガポール	18
ProxyRack	アメリカ	日本	イギリス	**31**
Oxylabs	アメリカ	日本	シンガポール	12
通常時	アメリカ	日本	シンガポール	8

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 10 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 11 と図 3 に示す．

表 10　ドメインの悪性判定結果

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

表 11　ドメインのカテゴリ分類結果

	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%)

表 10 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 12 に示す．

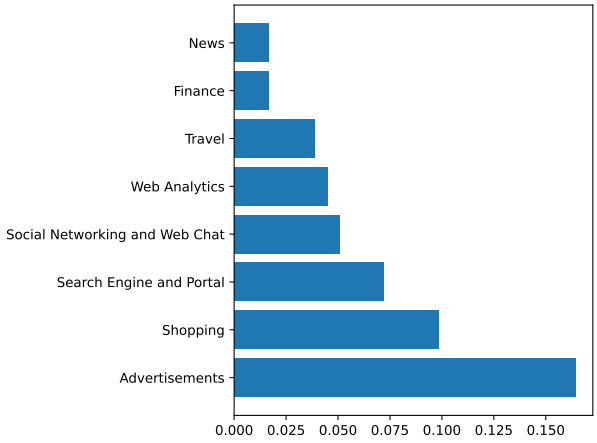

図 3　全通信のドメインカテゴリ割合

表 12　悪性ドメイン例（2022 年 10 月 9 日時点）

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

ここで api.bdisl.com は，IPA の 2020 年度の報告書 [20] 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 11 を見ると，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 からは，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 13 に示す．

表 13　PUP のトラフィック分析結果 [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%	-	-
social networks	2%	5.1%	4

図 3 と表 13 を比較すると，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．

4.4.2　実験 2：RESIP ホスト 24 時間観測実験

表 14 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．

表 14　1 日観測データの総数

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

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．

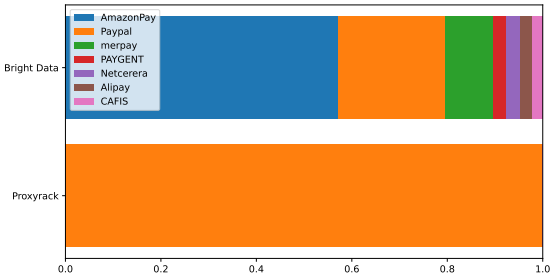

図 4　RESIP ホストと決済サービスとの通信

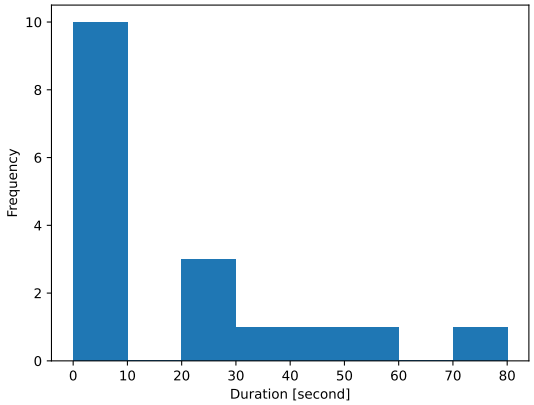

図 5　Bright Data の RESIP ホストと決済サービスとの通信時間分布
(2022 年 10 月 15 日 17 時 15 分から 24 時間)

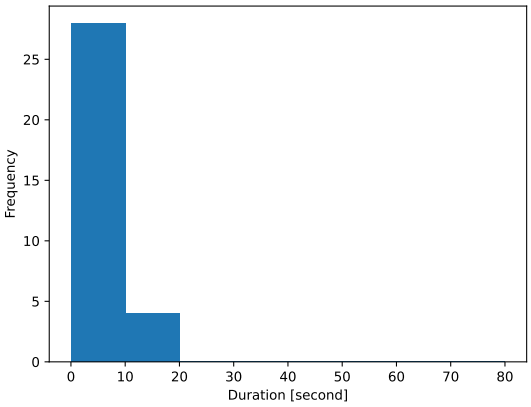

図 6　ProxyRack の RESIP ホストと決済サービスとの通信時間分布
(2022 年 10 月 16 日 18 時 30 分から 24 時間)

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 15 に示す.

表 15　RESIP ホストと NICTER 上の IP アドレスの突合

一致数	0
[3] 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 アドレスからの国判定などから，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 11 のようにドメインカテゴリが RESIP サービスごと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 10 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 13 の malicious websites が 5% であったことと，本調査の表 10 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.

[21] 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 [22] 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 [4] 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

研究 [3] 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．[4] 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 15 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，[3] 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

[13][17][18] 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．

利用規約で禁じられている

- 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うこと．
- 他のユーザに関する個人情報を追跡，保存，送信，または記録すること．

に該当する行為はない．

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 [4] 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．

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] 半澤映拓，“Residential IP Proxy サービスに悪用される住宅用ホストの調査”，2020 年度明治大学大学院修士論文，2021.

[4] 住友孝彰，“Residential IP Proxy サービスを悪用した不正行為の調査”，2021 年度明治大学卒業論文，2022.

[5] VirusTotal（https://www.virustotal.com/, 2022 年 10 月参照）.

[6] Wireshark（https://www.wireshark.org/，2022 年 10 月参照）.

[7] pyshark（https://github.com/KimiNewt/pyshark/，2022 年 10 月参照）.

[8] MAXMIND，“GeoLite2 Free Geolocation Data”（https://dev.maxmind.com/geoip/geolite2-free-geolocation-data，2022 年 10 月参照）.

[9] 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.

[10] 福田ひかり，“Residential IP Proxy サービスを用いた位置情報とターゲット広告の調査”，2022 年度菊池研究室卒業論文，2023.

[11] 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）.

[12] Bright Data（https://brightdata.com/, 2022 年 10 月参照）.

[13] Hola VPN（https://hola.org，2022 年 10 月参照）.

[14] EarnApp（https://earnapp.com/, 2022 年 10 月参照）.

[15] ProxyRack（https://www.proxyrack.com/, 2022 年 10 月参照）.

[16] Oxylabs（https://oxylabs.io/，2022 年 10 月参照）.

[17] ProxyRack, “Become A Peer Earn passsive income”（https://www.proxyrack.com/become-a-peer/，2022 年 10 月参照）.

[18] Honeygain（https://www.honeygain.com/, 2022 年 10 月参照）.

[19] Oxylabs, “Oxylabs Signs Exclusive Contract with Honeygain” （https://oxylabs.io/blog/oxylabs-signs-exclusive-contract-with-honeygain, 2022 年 10 月参照）.

[20] 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）.

[21] 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）.

[22] TOPDRAW, “ONLINE ADVERTISING COSTS IN 2021”（https://www.topdraw.com/insights/is-online-advertising-expensive/，2022 年 12 月参照）.