明治大学総合数理学部

2022 年度

卒　業　研　究

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

学位請求者　先端メディアサイエンス学科

守屋 龍一

目次

第 1 章　はじめに 2

第 2 章　事前準備 3

2.1　利用ツール 3

2.2　先行研究 3

第 3 章　Windows プロキシアプリの調査 5

3.1　調査目的 5

3.2　RESIP プロバイダの予備調査 5

第 4 章　実験 8

4.1　実験目的 8

4.2　実験環境 8

4.3　実験方法 8

4.4　実験結果 9

4.5　考察 14

第 5 章　本研究の適法性と倫理考慮 16

第 6 章　おわりに 17

参考文献 18

付録 A　Fiddler Script による位置情報スプーフィング攻撃の調査研究 20

A.1　はじめに 20

A.2　提案手法 21

A.3　実験 23

A.4　おわりに 31

参考文献 32

第 1 章

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 1.1 に示す．

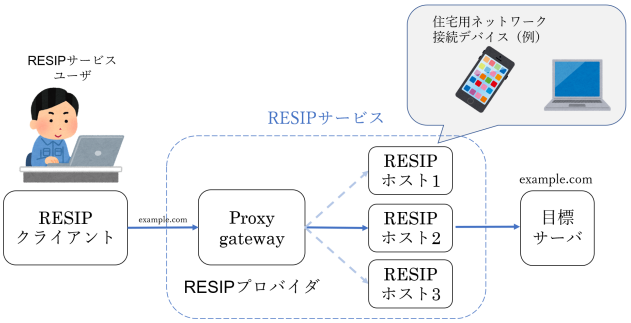

図 1.1　RESIP サービス概要図

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．

第 2 章

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 2.1 に使用したツールの説明と利用目的を示す．

表 2.1　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

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 2.2 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．

表 2.2　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

第 3 章

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 3.1 に示す．

表 3.1　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

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 に関連する文字列を持つドメインのサブドメイン数は表 3.2 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 3.2　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 3.3 に示す．

表 3.3　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 3.1 のような同意画面が表示されることから確認できた．

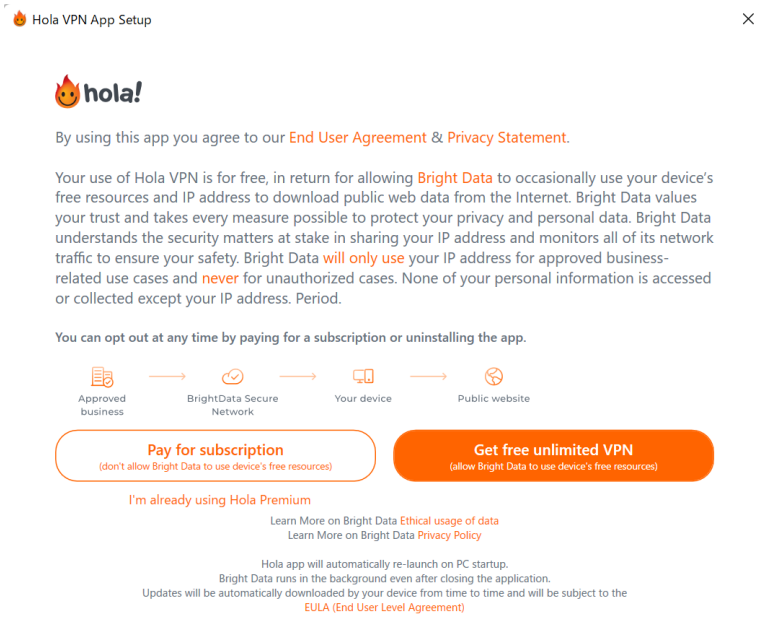

図 3.1　Hola の同意画面

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．

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．

第 4 章

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 4.1 に示す．

表 4.1 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

subsection 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．

subsection 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

subsection 実験 1：RESIP ホスト比較実験

表 4.2 と表 4.3 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 4.2　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 4.3　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 4.4 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 4.2 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 4.4　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 4.5 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 4.6 と図 4.1 に示す.

表 4.5　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 4.6　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%)

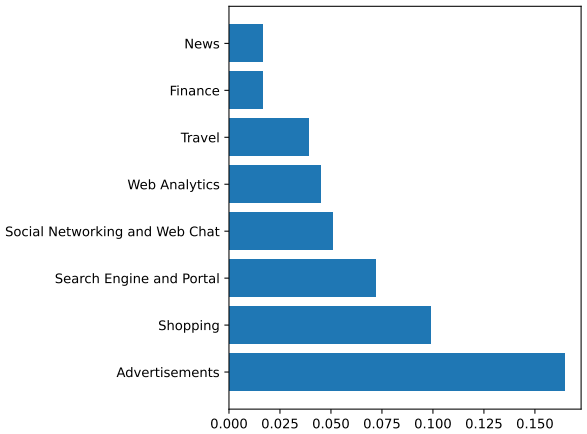

図 4.1　全通信のドメインカテゴリ割合

表 4.5 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 4.7 に示す．

表 4.7　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 4.6 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 4.1 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 4.8 に示す．

表 4.8　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 4.1 と表 4.8 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．

subsection 実験 2：RESIP ホスト 24 時間観測実験表 4.9 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 4.9　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 4.2 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 4.3（Bright Data）と図 4.4（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．

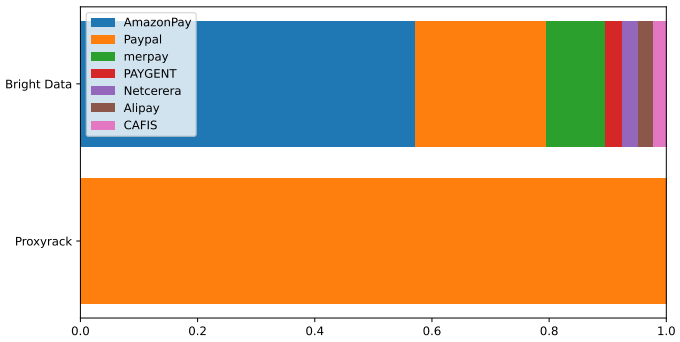

図 4.2　RESIP ホストと決済サービスとの通信

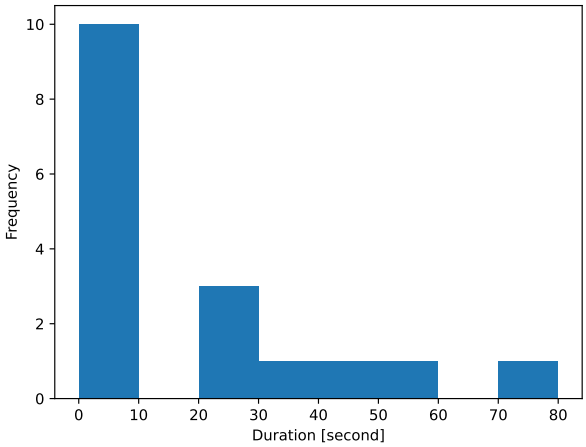

図 4.3　Bright Data の RESIP ホストと決済サービスとの通信時間分布
(2022 年 10 月 15 日 17 時 15 分から 24 時間)

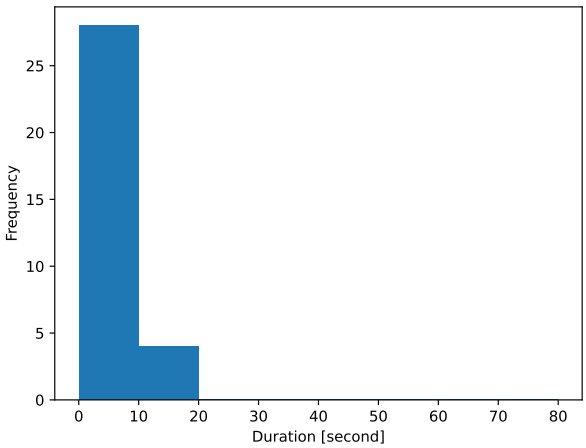

図 4.4 ProxyRack の RESIP ホストと決済サービスとの通信時間分布 (2022 年 10 月 16 日 18 時 30 分から 24 時間)

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 4.10 に示す.

表 4.10 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 4.6 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 4.5 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 4.8 の malicious websites が 5% であったことと，本調査の表 4.5 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 4.1 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 4.3 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 4.10 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．

第 5 章

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 3.1），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．

第 6 章

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）.

付録 A

Fiddler Script による位置情報スプーフィング攻撃の調査研究

A.1　はじめに

近年，SNS や位置情報ゲームをはじめ様々な場所で現在地情報を利用したサービス [1] が提供されている．しかしながら，現在地情報を利用したサービスには正しく利用できない状況が存在し，偽の GPS 信号による位置情報への攻撃であるサイバーセキュリティの危険性が指摘されている [2]．また，江藤らは，MAC アドレスを偽装した複数台の Wi-Fi アクセスポイントを周囲に設置することで本来と異なる現在地を表示する位置情報スプーフィング攻撃の脅威を指摘して，成功する条件の一部を明らかにした [3][4]．位置情報スプーフィング攻撃により，利用者は正しく現在地情報を利用できず，またサービス提供者にとっては不正利用による不利益が生じる可能性がある．しかしながら，[3] ではスプーフィングを実行するのに多くの偽装ルータを用意する必要があった．そのため，信号強度による条件も正確に定めることができなかった．

そこで，本研究では先行研究で明らかになっていなかった位置情報スプーフィング攻撃が成功する条件について詳細に求めることを目的とする．従来，複数台必要だった攻撃を 1 台で実行する新たな攻撃手法を提案する．実機の代わりに，Proxy サービス Fiddler を活用し，信号強度の正確な条件を明らかにする．以上の新規性を表 A.1 に整理する．本研究の新規性は次の通りである．

- MAC アドレスが Geolocation API サーバ内のデータベースに登録されているか判断する方法を提案する．
- 信号強度が位置情報スプーフィング攻撃にどのように関わるかを明らかにする．
- PC1 台で行う新規のスプーフィング攻撃を提案する．
- 一定距離ある 2 か所でそれぞれ収集した MAC アドレス同士を組み合わせて，収集した場所とは別の場所を合成する．

表 A.1　先行研究と本研究の比較

内容	先行研究 [3][4]	本研究
攻撃時に使用する PC の最低台数	5 台	1 台
MAC アドレスの組み合わせ	なし	あり
分析方法	偽装 Wi-Fi を設置して実験	Fiddler Script を用いて自動化
攻撃と信号強度との関係	不明	明らかになった
データベースへの所属検査方法	3 日間連続観測の可否	“accuracy” の値で判断

A.2　提案手法

A.2.1　位置情報スプーフィング

先行研究 [3][4] の位置情報スプーフィング攻撃の概要図を図 A.1 に示す．Linux のパッケージである macchanger を用いて現在地とは別の場所にある AP の MAC アドレスに偽装して，偽装 AP を作ることができる [3]．現在地の周囲にあって検出できる既存 AP の数より多い偽装 AP を設置することで偽装 Wi-Fi アクセスポイントによる位置情報スプーフィング攻撃が可能であることが明らかになっている [4]．

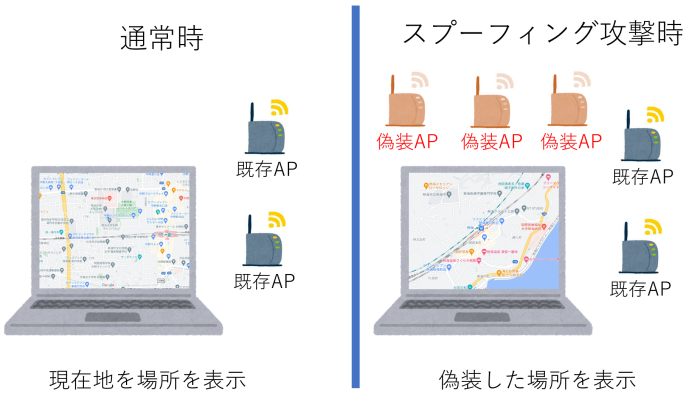

図 A.1　位置情報スプーフィング攻撃手法概要図

A.2.2　Fiddler Script

Fiddler は，http の proxy サーバとして作用しパケットをキャプチャするツールである [5]．Google Chrome で Google Maps を開くときの送信パケットは，Fiddler を用いて観測すると図 A.3 のように得ている．図 A.3 は json 形式で “age” は AP が検知されてからの時間 (ミリ秒)，“macadress” は位置推定時の周囲の AP が有する MAC アドレス，“signalStrength” はその MAC アドレスの信号強度をそれぞれ表している．

Fiddler の拡張 UI である Fiddler Script の例を図 A.4 に示す．パケットのリクエスト送信時やレスポンス受信時にパケット内容を変更し，デバックをすることを可能にしている．Fiddler Script によりパケット送信内容を書き換える例を図 A.4 に示す．OnBeforeRequest 関数内に記述することで Google Geolocation API のパケット送信時に本来のパケットの一部を指定テキストファイル記載の図 A.3 の形式の内容に書き換えてデバックすることができる．この機能は，Google Geolocation API 使用時に位置情報スプーフィング攻撃が成功する条件を明らかにする目的で使用する．

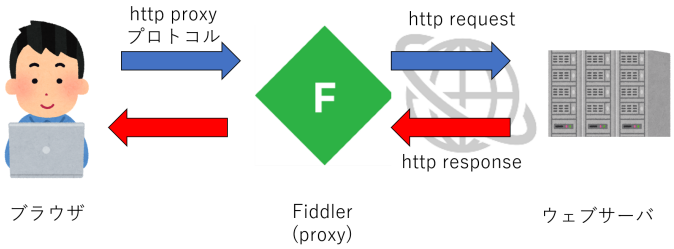

図 A.2　Fiddler 概要図


```
{"wifiAccessPoints":[
{"age":0,"macAddress":"00-1a-eb-82-e0-**","signalStrength":-34},
{"age":0,"macAddress":"98-f1-99-8c-04-**","signalStrength":-56},
{"age":0,"macAddress":"98-f1-99-a4-7d-**","signalStrength":-57},
{"age":0,"macAddress":"18-c2-bf-8b-08-**","signalStrength":-81},
{"age":0,"macAddress":"18-c2-bf-8b-08-**","signalStrength":-83}]}
```


図 A.3　API の送信パケットの一部

```
static function OnBeforeRequest(oSession: Session) {

        if (oSession.HostnameIs("www.googleapis.com")
                && oSession.uriContains("/geolocation/v1/")) {
            var oBody = oSession.GetRequestBodyAsString();
            var oBody = File.ReadAllText("C://aos//file_request.txt")
            oSession.utilSetRequestBody(oBody);
        }
```

図 A.4　FiddlerScript ソースコード例

A.2.3　MAC アドレスの収集

位置情報スプーフィングを行うには，偽装したい場所の周囲にあるアクセスポイントの MAC アドレスを事前に知る必要がある．そこで，Android Studio を用いて周囲の MAC アドレスを取得するアプリを開発した．実行例を図 A.5 に示す．緯度経度も同時に観測している．2021 年 8 月 2 日，9 月 2 日に本 MAC アドレス収集アプリを用いて各所で MAC アドレス収集した．

図 A.5　MAC アドレス収集アプリ実行画面

A.2.4　タイムシェアリングを用いたスプーフィング攻撃

偽装アクセスポイントとなる PC を何台も用意せずに，PC1 台で定期的に短時間で複数の MAC アドレスの変更を行うことで位置情報スプーフィング攻撃をする方式を提案する．これにより攻撃側のコストを削減する．

A.3　実験

A.3.1　実験目的

本実験は，以下の 4 点を目的とする．

1. MAC アドレスが Geolocation API のサーバ内のデータベースに登録されているか判断する方法を明らかにする．
2. 位置情報スプーフィング攻撃が成功する条件について先行研究よりさらに明らかにする．
3. PC1 台で行う新規のスプーフィング攻撃を検証する．
4. 一定距離ある 2 か所でそれぞれ収集した MAC アドレス同士を組み合わせて，収集した場所とは別の場所を合成する攻撃を検証する．

A.3.2　実験環境

GPS を有さないノート PC(Lenovo 80Y1, Windows10 19043) を利用する．Google Chrome を用いて Google Maps で現在地を推定する．現在地推定に成功するとその場所を青い点で示し，失敗すると過去の位置推定の情報からおおよその場所を示す．

偽装 Wi-Fi アクセスポイントを用いる実験を行う場所は，東京都立和田堀公園 A.2 である．

表 A.2　実験場所アクセスポイントの数

場所	緯度, 経度	平均
和田堀公園	35.685476, 139.638313	1.2

A.3.3　実験目的と方法

表 A.3　実験一覧

実験	目的	方法
1	MAC アドレスが DB に登録されているか判断する	“accuracy” の値の確認
2	信号強度と位置情報スプーフィング攻撃の関係を明らかにする	偽装 Wi-Fi によるアクセスポイント
3	位置情報スプーフィング攻撃が成功する信号強度の条件を明らかにする	Fiddler Script
4	DB に属さない MAC アドレスを用いた位置情報スプーフィング攻撃が成功する条件を明らかにする	Fiddler Script
5	タイムシェアリングスプーフィング攻撃の検証	タイムシェアリングスプーフィング攻撃
6	MAC アドレスの組み合わせによる偽装場所の合成の検証	タイムシェアリングスプーフィング攻撃

実験 1：MAC アドレスのデータベース所属検査

Google Geolocation API サーバ内のデータベースに調べたい MAC アドレスが登録されているかを識別することを目的とする．

Google Geolocation API のリクエストボディには 2 つ以上の MAC アドレスが必要である [7]．そのため，データベースに登録されている MAC アドレスがリクエストボディに 2 つ以上ある場合と，それ以外の場合で “accuracy” の値が異なると考えられる．収集した 2 つの MAC アドレスをサーバに送信して，返ってきたレスポンスボディの “accuracy” の値の大きさでデータベースに登録されているかを識別する．

この方法を用いて，調査対象の MAC アドレスがデータベースに存在しているかを 2021 年 11 月 10 日に調査した．

実験 2：信号強度と位置情報スプーフィング攻撃成功の相関

位置情報スプーフィング攻撃を行う際に信号強度がどのように関わっているか明らかにすることをも目的とする．

本実験は，2021 年 10 月 15 日に東京都杉並区和田堀公園で行った．偽装 Wi-Fi によるアクセスポイントで，明治大学中野キャンパスで収集した MAC アドレス 3 つを偽装した PC を 3 台用いる．3 台の偽装 AP から使用デバイスの距離を 0, 2, 4, 6m で変化させる．

実験 3：Fiddler を用いた位置情報スプーフィング攻撃と信号強度の関係の調査

位置情報スプーフィング攻撃に関わる信号強度の条件の詳細を明らかにすること目的とする．

2021 年 12 月 7 日に実験を行い，Fiddler Script を実験環境として用いる．和田堀公園で収集した MAC アドレス 1 つと，偽装したい場所で収集した MAC アドレス 1 つの信号強度を −1dBm から −100dBm まで 1dBm ずつ変化させて送信する．本実験は 3 か所の異なる場所を偽装させて 3 回試行した．和田堀公園で収集した MAC アドレスの信号強度は，−80dBm と −50dBm について調査する．

実験 4：データベースに登録されていない MAC アドレスを有する AP と位置情報スプーフィングの関係の調査

Google Geolocation API サーバのデータベースに登録されていない MAC アドレスを有する AP が多い時，位置情報スプーフィング攻撃が成功する条件を明らかにすることを目的とする．

2021 年 10 月 26 日に実験を行い，Fiddler Script を実験環境として用いて，データベースに登録されていない架空の MAC アドレス 7 個と登録されている明治大学中野キャンパスで収集した MAC アドレス 2 個で位置推定を行う．

表 A.4　実験 4 で使用する MAC アドレス

使用した MAC アドレス	収集場所	信号強度 [dBm]
e8-26-89-0e-9c-**	明治大学中野キャンパス	−50
18-c2-bf-73-95-**	明治大学中野キャンパス	−50
aa-aa-aa-aa-aa-aa	架空の MAC アドレス	−50
aa-aa-aa-aa-aa-bb	架空の MAC アドレス	−50
aa-aa-aa-aa-bb-bb	架空の MAC アドレス	−50
aa-aa-aa-bb-bb-bb	架空の MAC アドレス	−50
aa-aa-bb-bb-bb-bb	架空の MAC アドレス	−50
aa-bb-bb-bb-bb-bb	架空の MAC アドレス	−50
bb-bb-bb-bb-bb-bb	架空の MAC アドレス	−50

実験 5：タイムシェアリングスプーフィング攻撃の検証

PC1 台で複数の偽装 AP の代わりに位置情報スプーフィング攻撃をすることが可能であるかを明らかにすることを目的とする．

図 A.6 は本実験の概要図である．1 台の PC で，A，B，C，D，E の 5 台の AP を偽装する．本実験は，2021 年 10 月 15 日に東京都杉並区和田堀公園で行った．Ubuntu18.04 の PC1 台で macchanger コマンドにより明治大学中野キャンパスで収集した MAC アドレス 5 つの MAC アドレスを時分割で割り当てる．図 A.7 に本実験を行うシェルスクリプトを示す．この場合，MAC アドレスは図 A.8 のように変化する．MAC アドレスの更新を 0.5 秒の間隔で行うことで，攻撃対象のデバイスに検知させる時間を与える．偽装 AP の信号強度が −35dBm を上回らないように偽装 AP との距離は 4m とする．

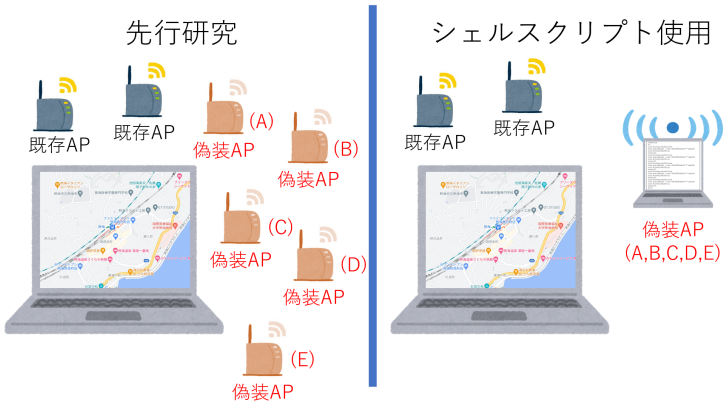

図 A.6　PC1 台での位置情報スプーフィング実験概要図

```
while true
do
sudo ifconfig wlp2s0 down
sudo macchanger --mac=e8:26:89:0e:9c:** wlp2s0  #A
sudo ifconfig wlp2s0 up
sleep 0.5
sudo ifconfig wlp2s0 down
sudo macchanger --mac=e8:26:89:0d:2e:** wlp2s0 #B
sudo ifconfig wlp2s0 up
sleep 0.5
sudo ifconfig wlp2s0 down
sudo macchanger --mac=e8:26:89:0e:9c:** wlp2s0 #C
sudo ifconfig wlp2s0 up
sleep 0.5
sudo ifconfig wlp2s0 down
sudo macchanger --mac=e8:26:89:0d:2e:** wlp2s0 #D
sudo ifconfig wlp2s0 up
sleep 0.5
sudo ifconfig wlp2s0 down
sudo macchanger --mac=e8:26:89:0d:2e:** wlp2s0 #E
sudo ifconfig wlp2s0 up
sleep 0.5
done
```

図 A.7　シェルスクリプトの例

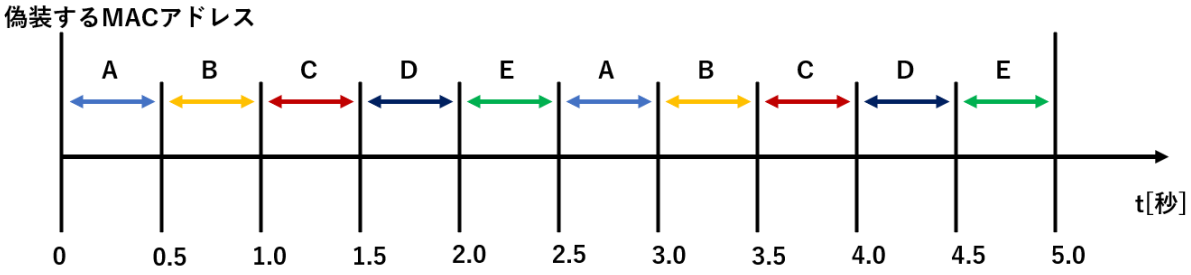

図 A.8　MAC アドレスの変化の例

実験 6：MAC アドレスの組み合わせによるスプーフィング攻撃の検証

別の場所で収集した MAC アドレスを組み合わせて与え，収集したいずれの場所とも異なる場所に偽装する位置情報スプーフィングが成功するかを明らかにする．

図 A.9 は本実験の概要図を示す．本実験は，2021 年 10 月 15 日に東京都杉並区和田堀公園で行った．Ubuntu18.04 の PC2 台を用意し， PC1 台で複数の偽 AP の代わりをする方法を用いて，1 台目の PC に浜田山駅で収集した MAC アドレス 5 個，2 台目の PC に明治大学駿河台キャンパスで収集した MAC アドレス 5 個を偽装させる．偽装 AP の信号強度が −35dBm を上回らないように偽装 AP との距離は 4m とする．

図 A.9　MAC アドレス組み合わせ実験概要図

A.3.4　実験結果

実験 1：MAC アドレスのデータベース所属検査

図 A.10 と表 A.5 に結果を示す．“accuracy” の値が 200 未満と 3500 以上で大きく分かれた．“accuracy” の値が 3500 以上の場合，レスポンスの緯度経度は常に自宅から 2km ほど離れた場所だった．これは，1 つ以下の調査対象である MAC アドレスをサーバに送信したときにも常に結果になる．また，MAC アドレスの収集場所と DB に登録されていた場所の距離を計算した [8]．その結果，“accuracy” の値が 200 未満である MAC アドレスの内，4 つを除く全ての距離が 200m 以内であった．

したがって，2 つの MAC アドレスをサーバに送信して，“accuracy” の値が 200 未満であればデータベースに登録されている識別できると考える．

調査対象である MAC アドレス 859 個のうち 624 個はデータベースに登録されていることが確認できた．

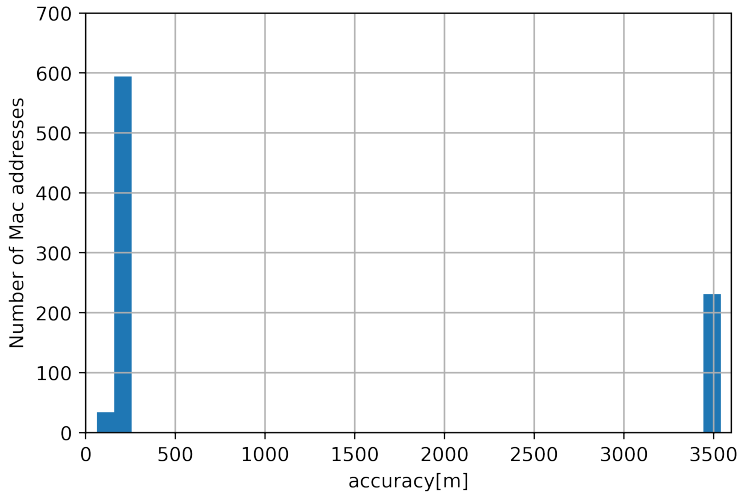

図 A.10　“accuracy” の値分布

表 A.5　“accuracy” によるデータベース所属検査の結果

	個数	“accuracy” の平均	収集場所と登録場所の距離の平均 [km]
登録済アドレス	624	173.917	0.080
未登録アドレス	235	3540.129	17.328

実験 2：信号強度と位置情報スプーフィング攻撃成功の相関

結果を表 A.6 に示す．〇は位置情報スプーフィング攻撃が成功し，明治大学中野キャンパスを現在地と誤って推定したことを表す．一方，×は位置推定が失敗したことを示す．使用デバイスと偽装 AP の距離が 0m のときに，位置情報スプーフィング攻撃が失敗している．

この結果から，位置情報スプーフィング攻撃に AP の信号強度が関わっていることが分かる．

表 A.6　位置情報スプーフィング攻撃と信号強度の関係実験の結果

距離 [m]	A’ 信号強度 [dBm]	B’ 信号強度 [dBm]	C’ 信号強度 [dBm]	結果
0	−30	−32	−33	×
2	−43	−40	−40	〇
4	−42	−54	−55	〇
6	−48	−54	−52	〇

実験 3：Fiddler を用いた位置情報スプーフィング攻撃と信号強度の関係の調査

実験 3 の結果を図 A.11 と図 A.12 に示す．成功率（Success Rate）は，変化させた偽装したい場所で収集した MAC アドレスの信号強度と現在地で偽装したい場所を表示し位置情報スプーフィング攻撃が成功した割合と定義する．偽装 AP の信号強度に応じて成功率が変化している．

図 A.11 から，偽装した場所で収集した MAC アドレスの信号強度が −79dBm から −35dBm の間のとき，100% の確からしさで，偽装したい場所で収集した MAC アドレスを表示し，位置情報スプーフィング攻撃が成功することが示された．−34dBm から −1dBm の間には位置推定に使用できず，−100dBm から −80dBm の間には和田堀公園を表示した．

図 A.11 と図 A.12 で共通して，信号強度が −34dBm 以上で強すぎる AP は位置推定に使用できないことが明らかになった．

また，図 A.11 と図 A.12 の比較から，AP が 2 つの場合は信号強度の値が高い MAC アドレスが登録されている場所を表示することが分かった．

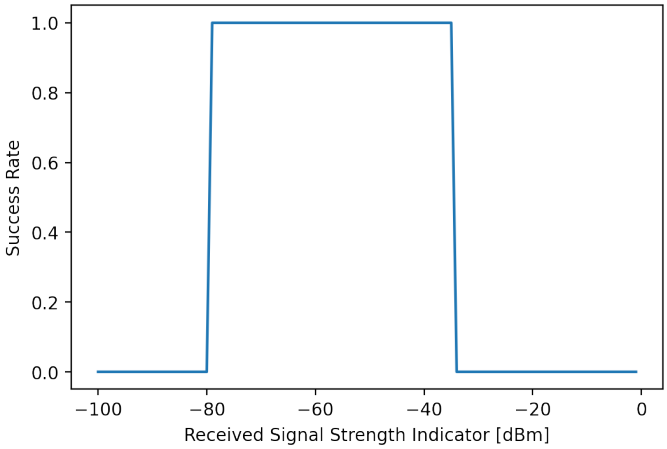

図 A.11　実験 3 結果 (和田堀公園の MCA アドレス −80dBm)

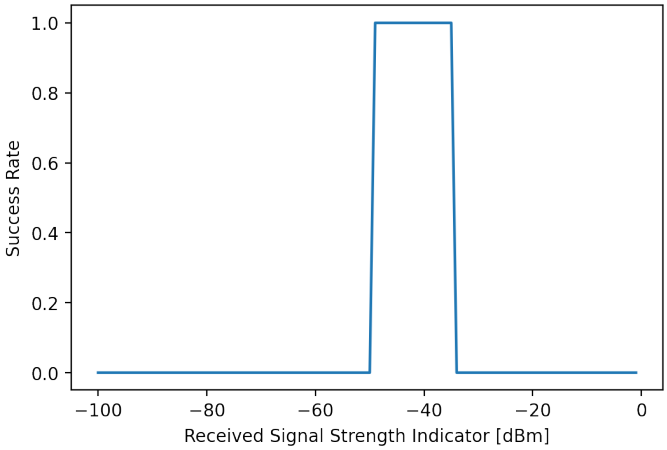

図 A.12　実験 3 結果 (和田堀公園の MCA アドレス −50dBm)

実験 4：データベースに登録されていない MAC アドレスを有する AP と位置情報スプーフィングの関係の調査

偽装 AP が示す明治大学中野キャンパスを現在地に誤って推定した．

この結果から，登録済のアドレスが 2 個あれば未登録の MAC アドレスを有する AP の数に無関係に位置情報スプーフィング攻撃が可能であることが分かった．

実験 5：タイムシェアリングスプーフィング攻撃の検証

偽装 AP として指定した明治大学中野キャンパスを現在地に誤って推定した．時分割で複数の MAC アドレスを割当てることで PC1 台で位置情報スプーフィング攻撃は可能であることが分かった．

実験 6：MAC アドレスの組み合わせによるスプーフィング攻撃の検証

偽装先として浜田山駅と明治大学駿河台キャンパスのの 2 つを与えた時，それらの間の場所を推定した．図 A.13 に結果を示す．一定距離ある 2 か所でそれぞれ収集した MAC アドレス同士を組み合わせて，収集した場所とは別の場所を合成することは可能であることが分かった．

ただし，想定のような偽装先 2 点の幾何学的な中間場所ではなかった．

図 A.13　MAC アドレス組み合わせ実験結果

A.3.5 考察

Google Geolocation API のサーバにデータベースに登録されていない MAC アドレスを 2 つ以下，または登録されている MAC アドレスを 1 つ以下送信したとき，常に同じ場所を示した．これは，周囲のアクセスポイントの数が不十分だった際に履歴からおおよその推定を行ったからだと考える．

強すぎる信号強度が位置推定に使用できない理由は，アクセスポイントが極めて近くにある状況が現実的でないからだと考える．したがって，偽装に適したアクセスポイントの信号強度は −35dBm 以下である．

タイムシェアリングスプーフィング攻撃は攻撃対象のデバイスの Wi-Fi 検知の仕様に依存しているので，他の OS では MAC アドレスの更新間隔や偽装可能な台数の変化が考えられる．

A.4 おわりに

実験の結果から，位置情報スプーフィング攻撃は偽装 AP の信号強度が −34dBm より弱いという条件で成功することが明らかになった．提案していた新しい方式である，シェルスクリプトを用いたタイムシェアリングスプーフィングや MAC アドレスを組み合わせたスプーフィングが可能であることが分かった．

実験 5 の手法が成功する詳しい条件を詳しくを調査すること，実験 6 の手法を使って自由な場所に偽装できる位置情報スプーフィング攻撃の方法を考えることを今後の課題とする．

参考文献

[1] 毎日新聞，“山口市全域で利用可に　運行３社でカバー　「乗車のきっかけに」”，2019 年 6 月 12 日

[2] 海老沼拓史，“GPS 信号の脆弱性と今そこにある危機”，中部大学工学部紀要 52 巻，2017.

[3] 江頭一樹，“偽造 Wi-Fi アクセスポイントによる現在地情報のスプーフィング攻撃の脅威”，2019 年度菊池研究室卒業論文，2019.

[4] 入沢響，“偽装 Wi-Fi アクセスポイントによる現在地情報のスプーフィング攻撃の調査”，2020 年度菊池研究室卒業論文，2020.

[5] Shinya Yamaguchi，“HTTPS パケット キャプチャ ツール Fiddler のインストールから使用開始まで。”（https://qiita.com/Shinya-Yamaguchi/items/37347ec532824c2dccad，2022 年 1 月参照）.

[6] Eric Lawrence，“Understanding FiddlerScript”（https://www.telerik.com/blogs/understanding-fiddlerscript，2022 年 1 月参照）.

[7] Google Maps Platform，“Web Services Geolocation API”（https://developers.google.com/maps/documentation/geolocation/overview，2022 年 1 月参照）．

[8] 国土地理院，“経緯度を用いた 2 地点間の測地線長、方位角を求める計算”，（https://vldb.gsi.go.jp/sokuchi/surveycalc/surveycalc/algorithm/bl2st/bl2st.htm，2022 年 1 月参照）.