明治大学総合数理学部

2022 年度

卒　業　研　究

ホームネットワークにおける全ホストを管理する Simple Home Security の開発

学位請求者　先端メディアサイエンス学科

井窪竜矢

目次

第 1 章

はじめに

2020 年以降流行している COVID-19 により，オンライン学習や在宅勤務の利用が増えた．今後もオンラインを用いる作業への需要は残ると考えられる．

しかしながら，専門知識を持つ管理者がいないホームネットワークにおいては気づかないうちに個人情報を盗まれたり，自身の所有する機器が乗っ取られることもある．特に，専用のファイアウォールがないため，知識のない家族が勝手に導入したスマートフォンのアクセス制限ができない．

そこで，本研究は，ホームネットワークにおいて家族が危険なサイトにアクセスしないように，Wi-Fi に接続している全ての機器を自動検出し，特定サイトへのアクセス制御を施すことを目的とする．しかし，ホームネットワークには通常専用のファイアウォールがなく，危険なサイトへのアクセスを遮断するのが困難である．そこで，本研究では，IP アドレスと mac アドレスを対応付ける ARP（Address Resolution Protocol）[3] に注目する．ARP を代理で送信する良性の ARP スプーフィングを応用することで，ファイアウォールを代用することを提案する．本稿では，システム開発と各家庭で行った実証実験の結果を報告する．

第 2 章

提案システム構成

2.1　ホームネットワークの危険性

家庭内で運用するネットワークにおいて注意すべき事項について３つ挙げる．

１つは専用ファイアウォールの有無だ．ファイアウォールはインターネットを通してローカルネットワークに侵入する不正なアクセスを防止するためのセキュリティシステムである．企業ではセキュリティ対策として専用のファイアウォールを設けているが，ホームネットワークにおいては高度なセキュリティ対策はなされていない．

次に，利用する人の知識不足が挙げられる．セキュリティやネットワークに対し，知識や関心が無い場合，不正なアクセスに気づかない場合も多い．

最後は，家族がアプリを勝手にアプリをインストールできることだ．ホームネットワーク内において，接続端末が不用意にインストールし，ウイルスに感染した場合，ホームネットワーク全体が危機に晒られる．

これらの問題を解消するため，ローカルネットワーク内のアクセスを制御するシステムを提案する．

2.2　ローカルネットワーク内のアクセス制御

図 2.1 に，ローカルネットワーク内で行われている通信と，本研究で実現するアクセス制御を示す．通常，家庭内にある各機器 A，B，C はルータ R を通し外部と通信するのに対し，Simple Home Security（SHS）設置では，A，B，C から R への通信を全て獲得し，SHS 経由で中継する．これを設置し，SHS の内部で各ホス

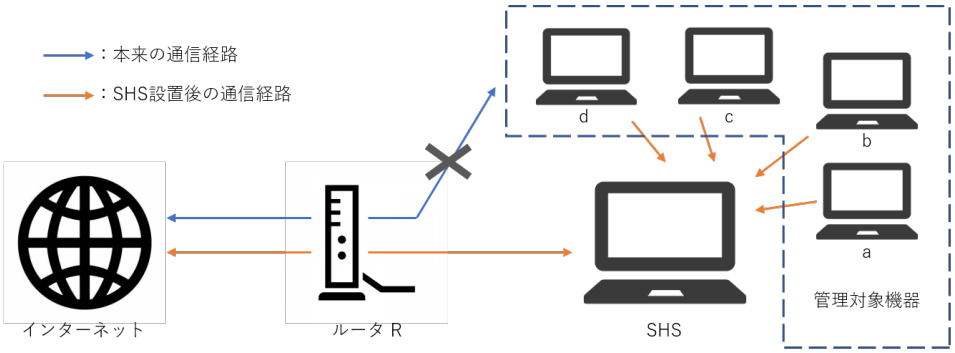

図 2.1　SHS 設置後のシステム構成図

トからの特定のサイトへの通信を遮断することができる．

2.3　目標とするセキュリティ対策

以下のセキュリティ対策を目的とする．

- Wi-Fi に接続している全ての機器の自動検出
- 各機器が所有する以下の情報の自動検出
  - IP アドレス
  - mac アドレス
  - ベンダー情報
- サイトのアクセス制限

2.4　ARP スプーフィング

ARP テーブルは IP アドレスと mac アドレスの対応表であり，通信に必要な mac アドレスを IP アドレスからスムーズに変換する役割を担っている．ARP スプーフィングは，ARP テーブルを書き換え本来の通信経路を強制的に変更することである．

表 2.1 に図 2.1 におけるルータ R，SHS，機器 a，機器 b の ARP テーブル，表 2.2 に，R が持つ ARP テーブル，表 2.3 に書き換えられた ARP テーブルを示す．ARP テーブルの書き換えによる影響は図 2.1 の通信経路の変化に該当する．

表 2.1　各機器の IP アドレスと mac アドレス

	IP アドレス	mac アドレス
ルータ R	10.1	01
SHS	10.2	02
機器 a	10.101	11
機器 b	10.102	12
機器 c	10.103	13
機器 d	10.104	14

表 2.2　R が所有する ARP テーブル

	IP アドレス	mac アドレス
SHS	10.2	02
a	10.101	11
b	10.102	12
c	10.103	13
d	10.104	14

表 2.3　R が所有する ARP テーブル：変化後

	IP アドレス	mac アドレス
SHS	10.2	02
a	10.101	02
b	10.102	02
c	10.103	02
d	10.104	02

2.5 先行研究

北原が報告 [1] した単独ツールでの ARP スプーフィングの実験結果をまとめた表 3.1 では，パケットの送信間隔に関わらず，高い割合で ARP スプーフィングが成功したことが分かる．2 台同時で実験を行った表 3.2 によると，2 種類のツールを用いて同時に ARP スプーフィングを実行する場合，パケットの送信間隔が短いツールが，より長く ARP テーブルを占有している．

村上らが報告 [2] したセキュリティ設定の不備に対する注意喚起の検証では，注意喚起を行わない場合に比べ 5 週間で 3 倍以上のポート開放状況の改善が確認された．

第 3 章

SHS の開発

3.1 ローカル Web サーバ

SHS はホームネットワークに接続する機器を管理するために，ローカル Web サーバを起動する．図 3.1 に作成した web サイト，表 3.1 に図 3.1 における各項目の説明を示す．

表 3.1 設定画面の機能

ipv4	IP アドレスの確認
access	Wi-Fi への接続権限の設定
control	管理対象の設定
mac	mac アドレスの確認
vendor	ベンダー情報の確認
name	ホスト名の確認
filter	制限されている IP アドレスの確認
config	制限するサイトを追加（URL を入力）
	ホストネームの変更
submit	config の送信
initialize	登録されている機器の初期化

3.2 主要な機能の仕組み

SHS のデバイス検知と ARP スプーフィング，閲覧制限について説明する．

家族が無許可で接続したデバイスを検知するには，デバイスがルータに向けてブロードキャストした ARP リクエストを検知することで実現できる．しかしこの方法では，図 3.2 のように初回のブロードキャストしか検知できない．

そこで，新たなデバイスの検知は，ローカルアドレス全てに ARP リクエストを送信し，返答される ARP テーブルから IP アドレスと mac アドレスを取得している．これにより，勝手にルータに接続している機器を検知することができる．

ARP スプーフィングは，Python にて scapy[4] を用いて 2 秒おきに ARP リプライを送信することで実現

している．40 秒に一回 ARP リクエストを送信し，応答がなかった場合，ARP スプーフィングを停止する．

閲覧制限については，nftables[5] を利用している．nftables はファイアウォールで，特定の通信を遮断する．図 3.3 に nftables に記載した内容を示す．図 3.3 において，1 に作成した遮断する IP アドレスのリストを 2 で宣言し，読み込む．最後に 3 で IP アドレスのリスト全てに対し，通信を遮断する．

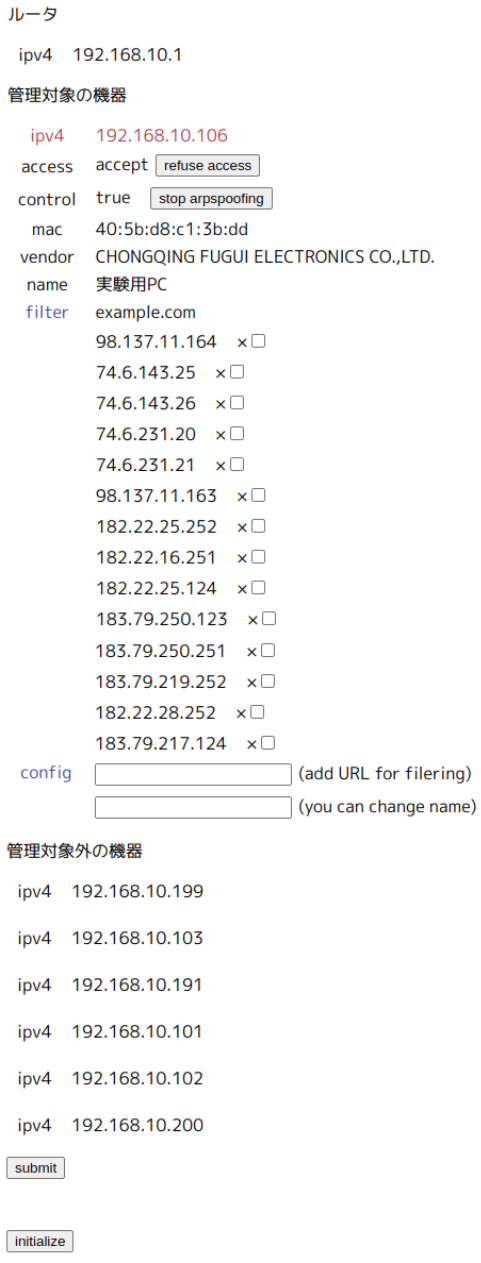

図 3.1　設定画面（Web サイト）

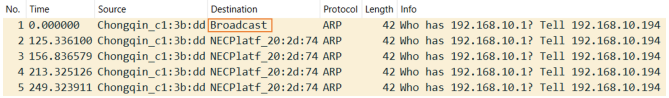

図 3.2　ARP リクエスト

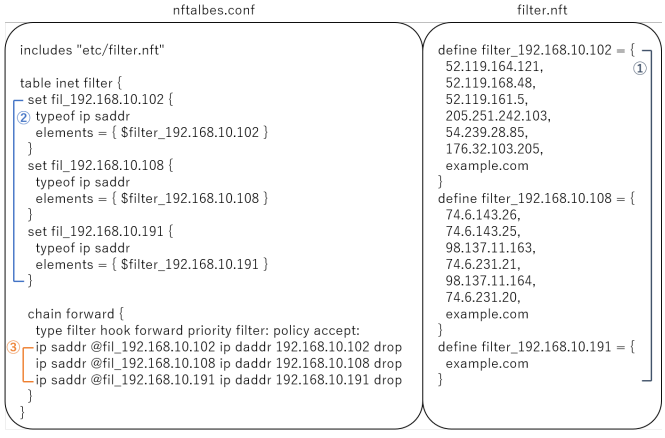

図 3.3　nftables

表 3.2　実行画面の説明

t(s)	意味	実行画面
0 〜 30	① ARP テーブルを 30 秒毎に取得	count: 0 192.168.10.106: 40:5b:d8:c1:3b:dd 192.168.10.199: 76:f0:98:c9:27:fc 192.168.10.200: 48:a5:e7:4e:07:56 192.168.10.101: 7a:93:2d:b9:62:b3 192.168.10.102: f0:67:28:6b:20:73 192.168.10.103: ca:3f:7f:58:78:f8 192.168.10.1: 08:10:86:20:2d:74
	名前の変更	name_192.168.10.106: 実験用 pc
	ARP スプーフィング の対象に設定	run arpspoofing on 192.168.10.106
30 〜 60	①と同様	count: 1 （省略）
	ARP スプーフィング実行	192.168.10.106 Start ARPspoofing...
60 〜 90	①と同様	count:2 （省略）
	url（yahoo.co.jp）の IP アドレスの取得, ブラックリストへの追加	filter_192.168.10.106: yahoo.co.jp 182.22.25.252 stored success 182.22.16.251 stored success 182.22.25.124 stored success 183.79.250.123 stored success 183.79.250.251 stored success 183.79.219.252 stored success 182.22.28.252 stored success 183.79.217.124 stored success refer:25-33

3.3　SHS の実行

表 3.2 に実行画面と説明を示す．通常は 30 秒毎に ARP テーブルを取得しており，その際に管理対象に設定された機器にのみ ARP スプーフィングを実行する．

3.4　課題

実際にルータに接続している全てのデバイスが検知できない．計測した結果，10 の機器に対し，SHS では 8 つしか検出できなかった．検知できなかった IP アドレスに ping を送信したところ「Destination host unreachable.」と出力されたため，宛先ホストに到達できていないことが分かる．このメッセージには宛先ホストがそもそもない，ルータが宛先を知らない等の意味がある．

第 4 章

SHS の利用方法

4.1 SHS の起動方法

SHS には Node.js と Python のプログラム言語を使用している．SHS 起動に向けた事前準備として以下のライブラリのインストールが必要となる．

- Node.js
  - python-shell
  - body-parser
  - express
- Python
  - scapy

SHS は配布したフォルダ内にある「nd.js」を実行するため，カレントディレクトリの移動後，ターミナルで「node nd.js」を入力すると起動する．

4.2 サイトへのアクセス制限

SHS の起動後，任意のブラウザで「http://127.0.0.1:8000/」と入力すると図 3.1 のサイトにアクセスする．表 3.1 に記載したように，config の入力欄に制限するサイトの URL を入力し，「control」を true の状態にすると，アクセス制限が完了する．

第 5 章

被験者実験

自作したプログラムが正確に動作することの確認するため，2022 年 11 月 16 日から 12 月 18 日に菊池研究室に所属する大学院生，学部生を対象として実験を行った．本実験は参加対象者へのプログラムの配布，各家庭においてプログラムの実行，機器の情報が登録された json ファイルの提出という手順を踏んでいる．表 5 に実験で明らかにされた各世帯におけるデバイスベンダ―の統計を示す．ルータや PC の他にゲーム，映像出力，プリンターを販売している Nintendo，Amazon，Epson 等の機器を検出した．

mac アドレスからベンダー情報が判明しなかったものを「不明」と表記している．ベンダー情報が取得できない原因として mac アドレスのランダム化 [6] が考えられる．これにより，企業ごとに決まっていた mac アドレスに統一性がなくなり，プライバシー保護が期待できる．

表 5.1　被験者実験の結果：ベンダー情報

	A	B	C	D	E	F	G	H	I	J	K	合計
BUFFALO	1				2	1	1				1	6
ELECOM			1			1						2
NEC Platforms		1		1						1		3
AlliedTelesis								1				1
HonHai Precision Ind	1								1			2
Nintendo	1	1				2						4
AmazonTechnologies.	1				1		1			1	1	5
Apple	1			1		1					1	4
TP-LINK TECHNOLOGIES			1	1					1			3
Liteon Technology			1									1
INNONET			1	1								2
Seiko Epson		1		1								2
OkiElectric Industry					1							1
HUAWEITECHNOLOGIES					1							1
SonyCorporation						1						1
ASRockIncorporation								1				1
GUANGDONGOPPO[a]		1										1
不明	2	2	1	4	2	6			4			21
合計	7	6	5	9	7	12	2	2	6	2	3	61

[a] GUANGDONGOPPO MOBILE TELECOMMUNICATIONS の略

第 6 章

おわりに

本研究では，ARP スプーフィングを応用することで，子供が危険なサイトにアクセスしないよう，ホームネットワークを安全に管理するシステム SHS を開発した．しかし，本プログラムは Ubuntu でしか実行を想定しており，windows で実装できている機能はデバイスの検出のみのため，今後は windows でのアクセス制御の実装を課題とする

参考文献

[1] 北原，“ARP テーブルスプーフィング攻撃のリスク評価”，2021 年度明治大学卒業論文，2021.

[2] 村上ら：セキュリティ設定に不備のある IoT 機器の所有者に対する専用アプリを介した注意喚起の効果検証，コンピュータセキュリティシンポジウム 2021，pp.183-190, 2021

[3] IT 用語辞典 e-Words，“ARP【Address Resolution Protocol】アドレス解決プロトコル”（https://e-words.jp/w/ARP.html，2022 年 4 月参照）

[4] Scapy，“Packet crafting for Python2 and Python3”(https://scapy.net/，2022 年 6 月参照)

[5] wiki-nftables，“Main Page”(https://wiki.nftables.org/wiki-nftables/，2022 年 6 月参照)

[6] Wi-Fi Column，“進む MAC アドレスのランダム化。影響や切り替え方法をご紹介”（https://www.ntt-bp.net/column/blog/2021/12/post-64.html，2023 年 1 月参照）

付録 A

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

A.1　はじめに

近年，プロキシサービスの中でも住宅用ネットワークを利用したトラフィック中継を提供する Residential IP Proxy（以下 RESIP とする）が人気を博している．RESIP に利用されている住宅用 IP アドレスは，住宅用 IP アドレスの保有者が各プロキシサービスのネットワークに自主的に参加することで収集されているとしている．また，プロキシサービスプロバイダではアプリの開発者を対象に収益の手段として SDK（Software Development Kit）を提供している [1][2]．これによりプロキシサービスプロバイダは，RESIP ホストの承諾を得，アプリ開発者は承諾したホスト数に応じてプロキシサービスから収益を受け取ることが可能となった．

しかし，Mi らの調査 [3] によると，，ユーザが RESIP ホストへの参加を承諾する際の SDK の同意書の文章はトラフィックの中継動作について曖昧であり，図 A.1 のようなユーザに誤解を与えやすい内容であること

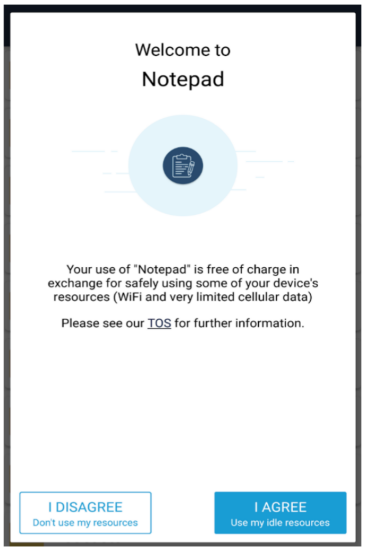

図 A.1　SDK の同意書

[5]fig4 より引用

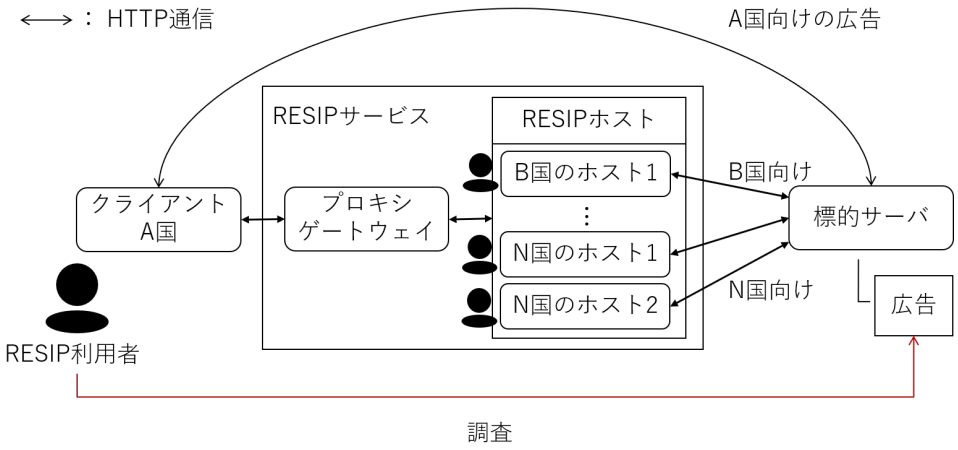

図 A.2　RESIP サービスのシステム構成図

がわかった．さらに，プロキシ SDK がユーザの同意なしに，ネットワークを中継する RESIP ホストに登録されていることも判明した．

しかし，意図せず登録された RESIP ホストが RESIP に登録されたことに気づくための RESIP ホストに対する調査が不足している．RESIP 利用者から RESIP ホストへの影響は RESIP 事業者によって秘匿されているため，利用されているか判断することが難しい．そこで本研究では，RESIP 利用者に注目して，サービスをを用いることによる影響を明らかにすることを目的とする．調査対象の RESIP プロバイダは規模の大きさや先行研究 [3][4][5] での調査状況をふまえ，Bright Data(https://brightdata.com/) と ProxyRack(https://www.proxyrack.com/) とした．本稿では，RESIP がユーザに与える影響に着目し，RESIP 利用時に RESIP ホスト，プロキシプロバイダによって位置情報，ターゲット広告に与える影響に差があるかの調査を報告する．

A.2　システム構成

A.2.1　RESIP

図 A.2 は RESIP サービスを用いた広告調査の構成図である．RESIP サービスは住宅用 IP によって通信を中継するサービスであり，クライアント，プロキシゲートウェイ，住宅用ホストから構成されている．RESIP 利用者がプロキシを利用する場合，ゲートウェイは RESIP 利用者から来た通信を設定に応じて異なる RESIP ホストへと割り当てる．標的サーバからの応答は割り当てられたホストを経由して RESIP 利用者へ中断される．

A.2.2　ターゲット広告

ターゲット広告とは，ユーザの web ページ閲覧履歴などを基に配信されるユーザを標的にした広告である．図 A.3 のターゲット広告はプロキシを経由すると図 A.4 になった．広告の内容だけでなく，広告に使用されている言語も異なっている．ターゲット広告のうち，RESIP ホストによって内容が変化するものを標的と呼び，全ターゲット広告数に対する割合を標的率と定義する．

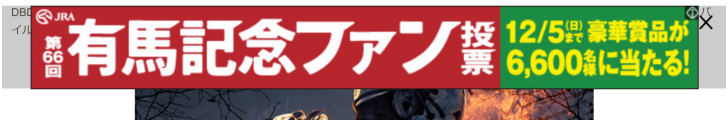

図 A.3　プロキシなしのターゲット広告の例

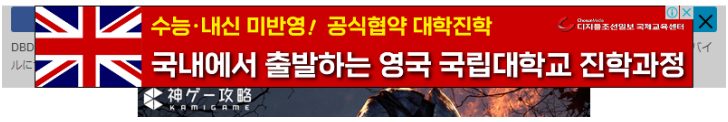

図 A.4　プロキシありのターゲット広告の例

表 A.1　調査対象の web サイト

web サイト	本実験での名称	URL
Yahoo！ JAPAN	yahoo	https://www.yahoo.co.jp/
神ゲー攻略	game	https://kamigame.jp/
folk	folk	https://folk-media.com
ロケットニュース 24	rocket	https://rocketnews24.com/
Smartlog	smart	https://smartlog.jp/

A.3　実験

A.3.1　目的

本実験は RESIP サービスを用いることで位置情報とターゲット広告に影響を与えるのかを調査し，RESIP サービスの影響を判明させることが目的である．

A.3.2　方法

実験 1：位置情報の調査

現在地を取得したとき実際の現在地から変化するか Google Maps(https://www.google.co.jp/maps) を使用し調査する．調査は各プロキシプロバイダにおいて 40 個の RESIP ホストを利用し，合計 80 個の RESIP ホストに対して 2021 年 9 月 9 日から 11 日にかけて行った．Bright Data で利用した RESIP ホストはアメリカ合衆国，カナダ，ウクライナの 3 か国に位置するものを各 10 個，日本，韓国の 2 か国に位置するものを各 5 個である．ProxyRack は地域を指定せず 40 個の RESIP ホストを利用した．

実験 2：ターゲット広告の調査

ターゲット広告へプロキシの影響があるか，5 つの web サイトを対象として 2 つのプロキシプロバイダを用いて調査する．対象とした 5 つの web サイトを表 A.1 に示す．Bright Data の RESIP ホストは実験 1 と同じ条件で行った．一方，ProxyRack は実験 1 と全く同一の RESIP ホストを用いて調査を行う．

プロキシの影響を受けているターゲット広告は，次の 3 つの条件のいずれかが満たされている広告と定義す

表 A.2　位置情報の変化数

	Bright Data	ProxyRack
現在地の変化	0/40	38/40

る．判断が難しいものについてはプロキシの影響がないものとする．

1. 日本語以外の言語で書かれている
2. 日本語表記であり，海外在住者向けの広告である（日本商品の通信販売や日本在住と同様のインターネット環境の構築など）
3. 日本語表記であり，現在地と異なる地名が入っている

以下に調査の手順について示す．調査は 2021 年 8 月 22 日から 9 月 11 日にかけて手動で行った．

1. RESIP を経由し表 A.1 のサイトにアクセスして，ターゲット広告の個数，RESIP 利用により表示内容が変化したターゲット広告の数を記録する．
2. 1 を各 RESIP アドレスに対して 5 つの web サイトで行い，繰り返す

実験 3：自動プログラムによる自動化

実験 2 をプログラムにより自動化した調査を 2021 年 11 月 12 日から 11 月 16 日までの 4 日間で行った．

本プログラムは node.js のライブラリである puppeteer[6] によって RESIP の設定，ブラウザ操作，画像取得を自動化し，ターゲット広告を含む web サイトの画像を取得する．puppeteer の選定理由はヘッドレスブラウザによりブラウザ操作を自動化できるためである．以下の手順で広告の変化を調査する．

1. プログラムを用いてプロキシを経由し，ヘッドレスブラウザを立ち上げる．
2. 対象の web サイトの画像を取得する．
3. 取得した画像を目視で確認し，表示された広告のうち，ターゲット広告の個数，RESIP 利用により表示内容が変化したターゲット広告の数を記録する．
4. 全てのサイトについて 1 から 3 を繰り返す．

A.3.3　結果

実験 1：位置情報の調査結果

位置情報についての実験 1 の結果を表 A.2 に示す．位置情報が現在地と異なっていたサイト数を示す．

表 A.2 より，Microsoft Edge，Google Chrome 共に Bright Data では全ての RESIP ホストにおいて現在地の取得がでなかった．ProxyRack では 403 Forbitten のエラーメッセージが返されるサイトが 4 個あるが，それ以外の RESIP ホストにおいて現在地が異なった．Bright Data では，「現在地を特定できませんでした」という Google Maps のエラーが返される．

実験 2：手動でのターゲット広告の調査

実験 2 の広告調査結果を表 A.3 に示す．

表 A.3　手動での広告調査結果

		Bright Data	ProxyRack	平均
yahoo	標的数	0.10	0.00	0.10
	総数	2.00	2.00	4.00
	標的率	0.05	0.00	0.03
game	標的数	6.76	2.15	8.91
	総数	9.11	4.51	13.62
	標的率	0.74	0.48	0.65
folk	標的数	3.93	5.06	8.99
	総数	4.79	7.41	12.20
	標的率	0.82	0.68	0.74
rocket	標的数	2.75	3.08	5.83
	総数	5.08	4.42	9.50
	標的率	0.54	0.70	0.61
smart	標的数	3.95	2.29	6.24
	総数	4.78	4.38	9.16
	標的率	0.83	0.52	0.68
平均	標的率	0.68	0.55	0.62

Bright Data 全体における標的率より，yahoo を除いた 4 つのサイトにおいては広告の半分以上がプロキシの影響を受けたターゲット広告の条件を満たしている．特に標的率が高いのが smart の 0.83，folk の 0.81 であり表示されたターゲット広告の 0.8 以上が変化したことがわかる．

表 A.3 より，ProxyRack 全体における標的率が最も低い値が 0.49 である．特に標的率が高いのが smart の 0.71 であり．最も低い値である rocket とは約 0.2 差があることがわかる．また，ブラウザを比較すると，総数は game，smart においては Google Chrome のほうが値が上回っており，標的率は値が等しいか上回っている結果となった．

また，ブラウザを比較すると，総数は rocket を除いて Microsoft Edge のほうが値が約 0.3 上回っており，標的率も game を除いて値が約 0.03 上回っている結果となった．

実験 3：自動でのターゲット広告の調査

実験 3 の広告調査結果について表 A.4 に示す．表 A.4 より標的率で最も高い値が ProxyRack の 0.43 であり，表 A.5 より，手動の方が値が良いことがわかる．

A.4　評価

A.4.1　ホストの所在国への依存

ProxyRack を用いて調査した際に使用した RESIP の所在国と広告について考察する．

表 A.6 は取得した 40 個の RESIP ホストの Google Maps における所在国を示している．代表的な game のターゲット広告数である．所在国が同一のホストが 3 個以上あるものを降順で示す．表 A.6 より，韓国が

表 A.4　プログラム使用時における広告調査結果

		Bright Data	ProxyRack	平均
yahoo	標的数	0.00	0.00	0.00
	総数	0.00	0.00	0.00
	標的率	0.00	0.00	0.00
game	標的数	0.90	0.07	0.97
	総数	4.33	5.69	10.02
	標的率	0.21	0.01	0.10
folk	標的数	1.05	0.03	1.08
	総数	2.47	3.24	5.71
	標的率	0.43	0.01	0.19
rocket	標的数	0.28	0.16	0.44
	総数	2.35	2.82	5.17
	標的率	0.12	0.06	0.09
smart	標的数	0.77	0.06	0.83
	総数	1.93	2.16	4.09
	標的率	0.40	0.03	0.20
平均	標的率	0.27	0.02	0.13

最も多い．日本の標的率は相対的に小さい．

表 A.7 は geo ロケーションサービスを用いて推定した 100 個のプロキシホストの国別の game のターゲット広告率である．所在国が同一のホストが 2 個以上あるものを降順で示す．

表 A.7 から ProxyRack の RESIP ホストは日本からアクセスする場合，韓国が最も多い．香港の RESIP ホストが他の国と比べて 2 倍以上ある．

国ごとで標的数に差があるのか明らかにするため，有意水準を 5% とし独立性の χ 二乗検定を表 A.8 に示す．最も多く調査できた韓国と調査件数が 3 件以上の国で行った検定の結果を示している．表 A.8 から，韓国と差があった国は日本とウクライナのみであった．すなわち，RESIP ホスト国と標的率に相関はない．

A.4.2　Residential IP Proxy プロバイダの比較

本実験で使用した Bright Data と ProxyRack の比較を行う．

位置情報の変化に関しては，Bright Data では現在地が表示されなかったことから，プロバイダにより位置情報が変化することがわかった．

ターゲット広告の調査について，Bright Data を対象にした調査が最も標的率が高くなった

A.4.3　自動観測プログラムの精度

実験 3 で使用した自動観測プログラムについて，実験 2 にて得られた結果に対して相対誤差を求め，表 A.10 に示す．

表 A.10 より，Bright Data と ProxyRack 共に誤差が 50% 以上あり，自動観測プログラムの精度は低い．

表 A.5　広告調査結果

		Bright Data		ProxyRack		平均	
		手動	自動	手動	自動	手動	自動
yahoo	標的数	0.10	0.00	0.00	0.00		
	総数	2.00	0.00	2.00	0.00		
	標的率	0.05	0.00	0.00	0.00	0.03	0.00
game	標的数	6.76	0.07	2.15	0.90		
	総数	9.11	5.69	4.51	4.33		
	標的率	0.74	0.02	0.48	0.21	0.65	0.10
folk	標的数	3.93	0.03	5.06	1.05		
	総数	4.79	3.24	7.41	2.47		
	標的率	0.82	0.02	0.68	**0.43**	**0.74**	0.19
rocket	標的数	2.75	0.16	3.08	0.28		
	総数	5.08	2.82	4.42	2.35		
	標的率	0.54	**0.05**	**0.70**	0.12	0.61	0.09
smart	標的数	3.95	0.06	2.29	0.77		
	総数	4.78	2.16	4.38	1.93		
	標的率	**0.83**	0.02	0.52	0.40	0.68	**0.20**
平均	標的率	0.68	0.02	0.55	0.27	0.62	0.13

表 A.6　Google maps によるプロキシホストの所在国とターゲット広告の変化率

国	RESIP 数	標的数	総数	標的率
South Korea	13	3.8	5.5	0.7
Japan	7	3.7	10.7	0.4
United States	4	4.3	6.3	**0.8**
Russia	3	4.7	5.3	**0.8**
Canada	2	8.5	8.5	**1.0**
Indonesia	2	2.5	4.0	0.6

実験 2

A.4.4　考察

ターゲット広告の調査において yahoo の変化の割合が著しく低い理由は，yahoo が日本の IP アドレスからの通信にのみターゲット広告を表示することが原因であると考えられる．

表 A.7　プログラム使用時の RESIP ホストの所在国とターゲット広告の変化率

country	RESIP 数	標的数	総数	標的率
South Korea	39	1.05	5.13	0.21
Japan	18	0.11	5.06	0.02
Hong Kong	6	1.00	3.00	0.33
Russia	3	1.33	4.00	0.33
Spain	3	1.00	2.33	0.43
Ukraine	3	2.33	4.33	0.54
United States	3	1.33	3.67	0.36
Vietnam	3	1.67	5.67	0.29
Brazil	2	2.50	2.50	**1.00**
Bulgaria	2	0.50	2.00	0.25
Canada	2	1.50	2.50	**0.60**
Portugal	2	0.50	1.50	0.33
Sweden	2	2.00	2.00	**1.00**

表 A.8　韓国とその他 7 か国間での χ 二乗検定

	韓国	
	p 値	有意差
日本	0.00	あり
香港	0.172	
ロシア	0.216	
スペイン	0.102	
ウクライナ	0.003	あり
アメリカ	0.146	
ベトナム	0.318	

A.5　おわりに

表 A.2 より，ProxyRack では 80 個のうち 76 個の RESIP ホストで位置情報が変化し，Bright Data においては位置情報サービスが機能していなかった．ターゲット広告に関しては表 A.3 より，BrightData と ProxyRack のいずれの調査においても標的が確認された．本調査では，上記 2 点において位置情報とターゲット広告の変化が確認されたことを明らかにした．

本稿では RESIP サービスが RESIP 利用者へ与える影響を調査した．今後は RESIP 利用者が RESIP ホストへ与える影響を調査することを課題とする．

表 A.9　プログラム使用時の 2 か国における調査結果

			Bright Data		ProxyRack	
			韓国	日本	韓国	日本
	RESIP 数		25	25	39	18
game	標的数	平均	0.04	0.09	1.05	0.11
		標準偏差	0.20	0.27	1.22	0.46
	総数	平均	5.60	5.52	5.13	5.06
		標準偏差	2.28	2.73	2.78	2.68
	標的率	平均	0.01	0.02	0.21	0.02
folk	標的数	平均	0.00	0.11	1.00	0.44
		標準偏差	0.00	0.27	1.18	0.96
	総数	平均	3.17	3.33	2.41	2.61
		標準偏差	1.08	2.06	1.61	1.67
	標的率	平均	0.00	**0.03**	0.41	0.17
rocket	標的数	平均	0.40	0.05	0.32	0.17
		標準偏差	0.64	0.20	0.51	0.37
	総数	平均	2.92	2.87	2.30	2.39
		標準偏差	0.74	1.00	1.36	1.21
	標的率	平均	**0.14**	0.02	0.14	0.07
smart	標的数	平均	0.00	0.04	0.95	0.47
		標準偏差	0.00	0.20	1.01	0.76
	総数	平均	2.12	2.30	1.97	2.12
		標準偏差	0.43	0.84	1.09	1.11
	標的率	平均	0.00	0.02	**0.48**	**0.22**

表 A.10　自動プログラムの精度

	Bright Data	ProxyRack
相対誤差	0.97	0.51

参考文献

[1] Bright Data, “Monetize inactive app users” (https://brightdata.com/sdk, 2021 年 11 月参照).

[2] ProxyRack, “Android Monetization SDK - ProxyRack” (https://www.proxyrack.com/android-sdk/, 2021 年 11 月参照).

[3] Xianghang Mi, et al. , Your Phone is My Proxy: Detecting and Understanding Mobile Proxy Networks NDSS Symposium 2021, pp.1-18, 2021.

[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] 半澤, “Residential IP Proxy サービスに悪用される住宅用ホストの調査”, 2020 年度菊池研究室修士論文, 2021.

[6] Alex Rudenko, “GitHub - puppeteer/puppeteer at v13.0.0”(https://github.com/puppeteer/puppeteer/tree/v13.0.0, 2021 年 12 月参照)