明治大学総合数理学部

2022 年度

卒　業　研　究

IP ブラックリストを用いた Residential IP Proxy ホスト検知手法の提案

学位請求者　先端メディアサイエンス学科

北原 拓海

目次

第 1 章

はじめに

近年，住宅用の IP アドレスを使用したプロキシアプリである Residential IP Proxy(RESIP) の利用が盛んになってきている．主な用途としては，IP アドレスに基づく検閲や，データスクレイピングによるアクセス制限を回避する場合などが挙げられる．

しかし RESIP はそのような用途の他にも，自身の身元を秘匿することを利用した不正アクセスや攻撃の踏み台としても悪用が疑われている．Mi らは 2017 年に RESIP ホストの 95% が住宅用の IP アドレスであり，その内の 43% が IoT 機器のものであることを報告している [2]．半沢らは国内のダークネットを観測し，所有する機器が意図せずに RESIP ホストとなり悪意を持った第三者に利用されている可能性があることを指摘している [3]．そのためユーザーは所有する機器が悪用されていることを検知して防ぐことが重要である．Tosun らは端末で取得したパケットの特徴を分析してホストで稼働している RESIP アプリを検知するアルゴリズム [4] を提案している．しかし，誤検知の頻度が高く，精度に問題があった．

そこで本稿では，RESIP について，従来の方法とは異なる IP アドレスのブラックリストを作成することで主要な RESIP アプリの検知を提案する．また，実験に基づく検出精度を報告する．

第 2 章

準備

本研究では Hola VPN[5], Proxyrack[6], Honeygain[7] の 3 つの RESIP アプリについての調査を行った.

2.1 Hola VPN

Hola VPN は 2008 年頃にイスラエルで開発された RESIP アプリである．無料でクライアントとなる場合には利用者のネットワークのリソースを提供して Brightdata の RESIP ホストになる旨がソフトウェアの利用時に表示される.

2.2 Proxyrack アプリ

Proxyrack は 2014 年に創設された有料の RESIP アプリである．Proxyrack の RESIP ホストとなることで報酬を受け取る事 Proxyrack アプリを配布をしている.

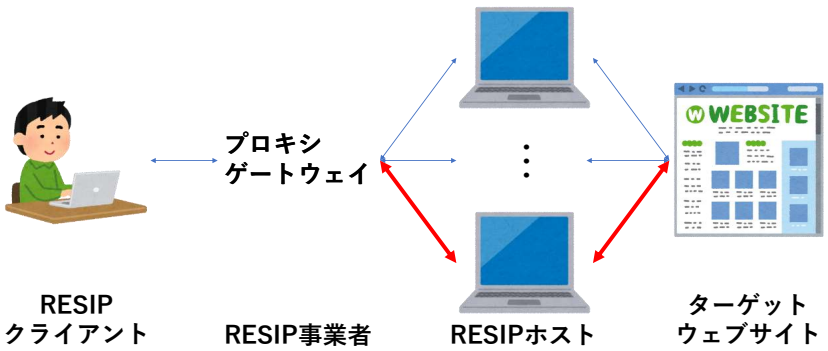

図 2.1 実験環境

表 2.1　調査した RESIP の開始年，対応プラットフォームと使用している SDK

名称	開発年	対応プラットフォーム	RESIP プロバイダ
Hola VPN	2008 頃	Windows, Android, iOS, Mac	Brightdata
Proxyrack	2014	Windows	Proxyrack
Honeygain	2018	Windows, Android, iOS, Mac	Oxylab

2.3　Honeygain

Honeygain は 2018 年に開発された，RESIP ホストとなることで仮想通貨などの報酬を受け取ることが可能なアプリである．Honeygain は RESIP アプリの Oxylab との独占契約を締結しており，Honeygain を使用して RESIP ホストになったユーザのネットワークリソースは Oxylab を利用する RESIP 利用者に提供される．

第 3 章

提案手法

3.1　予備調査

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，RESIP 事業者のゲートウェイとの定期的な通信が行われる．

そこで本調査では 3 つの RESIP アプリのホストとなって各アプリについて 5 分× 100 回の通信を観測して IP アドレスを収集し，各 RESIP アプリの通信の特徴を定量化する．

3.2　観測方法

パケットの観測と通信先 IP アドレスを収集する．Python で作成した観測手順を図 3.1 に示す．本観測では RESIP 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 RESIP 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．

表 3.1 に本ツールを動作させた時のログを示す．通信の観測を開始した時刻と，5 分間で観測したパケットの数で降順に並べられた IP アドレスリストを出力し，次の 5 分間の観測結果を下に追加する．図 3.1 の例は RESIP アプリを起動しない状態で取得したログの一部が表示されている．この 5 分間で一番通信が多く観測された IP アドレスは 20.190.141.32 であり，その量は 73 個であったことを示している．

また第 1 オクテットが 20 または 52 の IP アドレスが多く観測されているが，これらはいずれも Microsoft のアドレスである．

入力 調査対象 PC で取得した通信先 IP アドレス *ip*，IP アドレスのリスト *list*

1. RESIP アプリを起動して 100 秒待機する
2. 5 分間パケット *ip* を取得する
3. *ip* がプライベート IP アドレスではなければリスト *list* に記録する
4. RESIP アプリを終了する
5. 1. から 5. を 100 回繰り返す

図 3.1　観測手順

表 3.1　観測ログの例

Time	IP	Count
2022/11/23_5:21:56	20.190.141.32	73
	20.54.89.15	59
	20.205.248.73	28
	20.54.89.106	24
	52.191.219.104	24
	52.148.82.138	17
	20.72.205.209	12
	52.109.8.44	12

第 4 章

RESIP 検知プログラムの開発

4.1　概要

本ツールは前述の観測ツールで収集された IP アドレスを元に作成されたブラックリストを使用し，RESIP アプリとの関係が疑われる通信先との通信を検知する．Python で作成したこの提案方式のアルゴリズムを図 4.1 に示す．

4.2　実験方法

本実験では調査対象の RESIP 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 RESIP 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．実験で使用したアプリを起動する OS は Windows 10 である．調査した RESIP アプリは Hola VPN, Proxyrack, Honeygain の 3 つである．

(1) 表 2.1 の 3 つの RESIP アプリついて，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．

4.3　実験 1 結果 (通信先)

4.3.1　通常時

RESIP を起動しない状態での端末の通信先と通信量を図 4.2 に，100 回の観測で継続的に通信を行っていることが確認できた通信先を表 4.2 に示す．観測は 2022 年 11 月 24 日 5:53-14:06 に東京都の自宅から，家庭内 LAN に接続した Windows 10 端末で行った．

入力 調査対象 PC で取得したパケット p，通信先 IP アドレスのリスト a

1. 5 分間パケット p を取得する
2. プライベート IP アドレス以外の通信先 IP アドレスをリスト a に記録する
3. a をブラックリストと照合する

図 4.1　提案プログラムのアルゴリズム

表 4.1　実験で使用した RESIP アプリ及び収集した IP アドレスとパケット数

使用した RESIP	IP	パケット
なし (通常時)	48	1786
Hola VPN	141	11192
Proxyrack	325	89416
Honeygain	703	208820

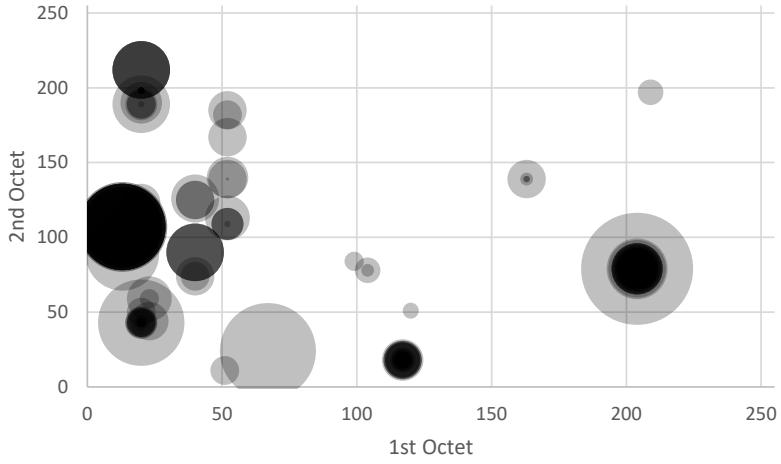

図 4.2　RESIP ホストではない状態での通信先と通信量

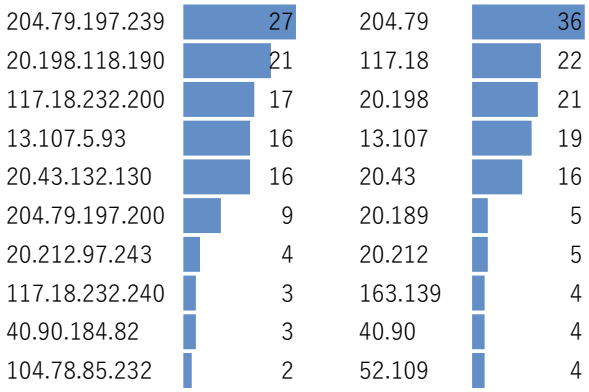

図 4.3　RESIP ホストではない状態での通信先と 100 回の観測頻度 (上位 10)

通常時の通信では 5 分 x100 回の観測で 48 のアドレスから 1786 のパケットを観測した．

継続的に通信を行っていた IP アドレスは，100 回中 27 回観測した 204.79.197.239 が最多だった．また通信先 IP アドレスを第 2 オクテットまででまとめた結果も同様に 204.79.x.x が最多であった．表 4.2 の上位の IP アドレスは Microsoft と CDN の EdgeCast(旧 Verizon) である．

表 4.2　通常時の通信先 IP アドレスと whois 情報 (上位 10)

IP アドレス	whois
204.79.197.239	Microsoft Corporation (MSFT)
20.198.118.190	Microsoft Corporation (MSFT)
117.18.232.200	EdgeCast Networks Asia Pacific Network
13.107.5.93	Microsoft Corporation (MSFT)
20.43.132.130	Microsoft Corporation (MSFT)
204.79.197.200	Microsoft Corporation (MSFT)
20.212.97.243	Microsoft Corporation (MSFT)
117.18.232.240	EdgeCast Networks Asia Pacific Network
40.90.184.82	Microsoft Corporation (MSFT)
104.78.85.232	Akamai Technologies, Inc.

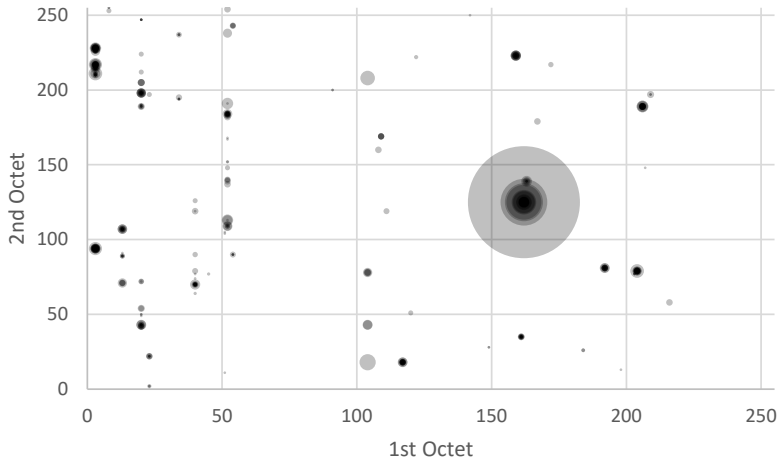

図 4.4　Hola VPN の通信先と通信量

4.3.2　Hola VPN

Hola VPN を起動した時の通信先と通信量を図 4.4 に，100 回の観測で継続的に通信を行っていることが確認できた通信先を表 4.3 に示す．2022 年 11 月 23 日 5:28-16:29 に観測した Hola VPN の通信は通常時の通信と比較すると通信先は 2.9 倍，パケットは 6 倍であり，通信先には通常時には見られなかった Dropbox, Amazon, DigitalOcean などのアドレスが多く見られた．

4.3.3　Proxyrack

Proxyrack を起動した時の通信先と通信量を図 4.6 に，100 回の観測で継続的に通信を行っていることが確認できた通信先を表 4.4 に示す．2022 年 11 月 24 日 7:49-18:52 に観測した Proxyrack アプリの通信は通常時の通信と比較すると通信先は 6.8 倍，パケットは 50 倍であった．最も観測された回数が多かった IP アドレス

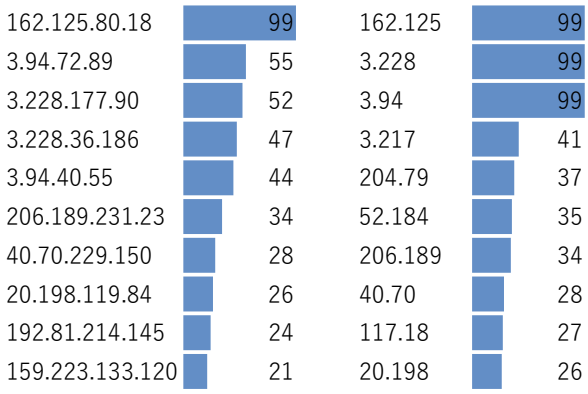

図 4.5　Hola VPN の通信先と 100 回の観測での観測回数 (上位 10)

表 4.3　Hola VPN の通信先 IP アドレスと whois 情報 (上位 10)

IP アドレス	whois
162.125.80.18	Dropbox, Inc. (DROPB)
3.94.72.89	Amazon Technologies Inc.
3.228.177.90	Amazon Technologies Inc.
3.228.36.186	Amazon Technologies Inc.
3.94.40.55	Amazon Technologies Inc.
206.189.231.23	DigitalOcean, LLC (DO-13)
40.70.229.150	Microsoft Corporation (MSFT)
20.198.119.84	Microsoft Corporation (MSFT)
192.81.214.145	DigitalOcean, LLC (DO-13)
159.223.133.120	DigitalOcean, LLC (DO-13)

は 100 回中 98 回観測された 38.84.x.x(PSINet) であり，その他には 24 SHELLS, VeriSign のアドレスが上位 10 アドレス中 6 つを占めた．

4.3.4　Honeygain

Honeygain を起動した時の通信先と通信量を図 4.8 に，100 回の観測で継続的に通信を行っていることが確認できた通信先を表 4.5 に示す．2022 年 11 月 28 日 1:30-13:22 に観測した Honeygain の通信は通常時の通信と比較すると通信先は 14.6 倍，パケットは 116 倍であった．最も観測された回数が多かった IP アドレスは 100 回中 89 回観測された 34.237.x.x(Amazon) であり，その他には Cloudflare のアドレスが上位 10 アドレスの半分を占めた．

4.4　実験 2 結果 (ブラックリストの作成)

調査 1 で収集した 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 アドレスの割当国と whois 情報を表 4.6 に示す．登録した IP アドレスは，実験 1 での 100 回の観

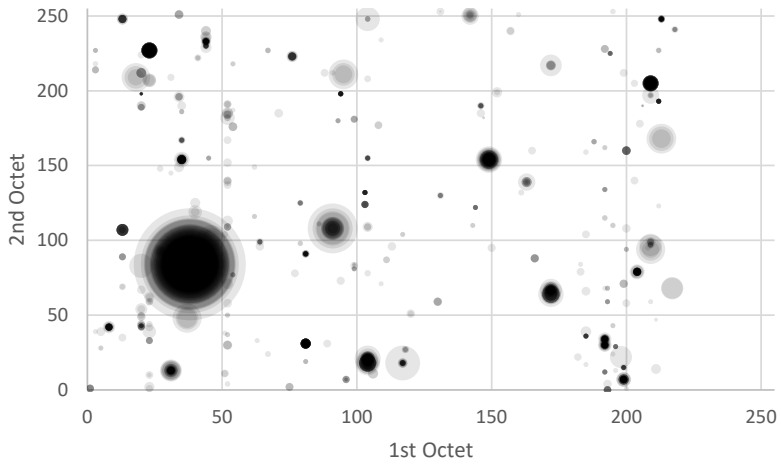

図 4.6　Proxyrack の通信先と通信量

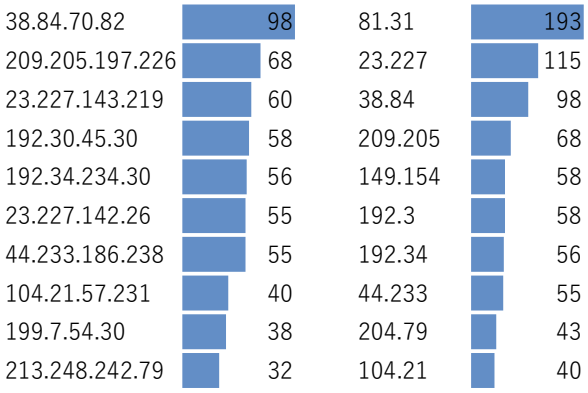

図 4.7　Proxyrack の通信先と 100 回の観測での観測回数 (上位 10)

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 4.7 に示す．

RESIP ホストでない通常時のパケットで RESIP ホストであると誤判定される偽陽性は 100 回の実験では起こらなかった．

表 4.4　Proxyrack の通信先 IP アドレスと whois 情報 (上位 10)

IP アドレス	whois
38.84.70.82	PSINet, Inc. (PSI)
209.205.197.226	24 SHELLS (TS-74)
23.227.143.219	24 SHELLS (TS-74)
192.30.45.30	VeriSign Global Registry Services
192.34.234.30	VeriSign Global Registry Services
23.227.142.26	24 SHELLS (TS-74)
44.233.186.238	Amazon.com, Inc. (AMAZO-4)
104.21.57.231	Cloudflare, Inc. (CLOUD14)
199.7.54.30	VeriSign Global Registry Services
213.248.242.79	Nominet UK

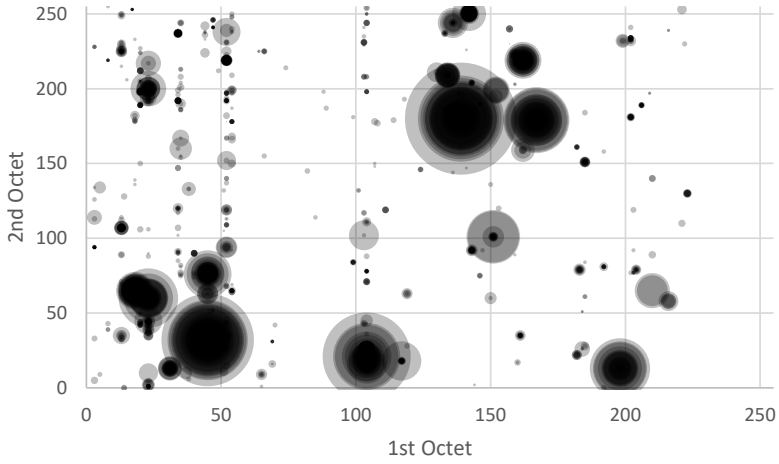

図 4.8　Honeygain の通信先と通信量

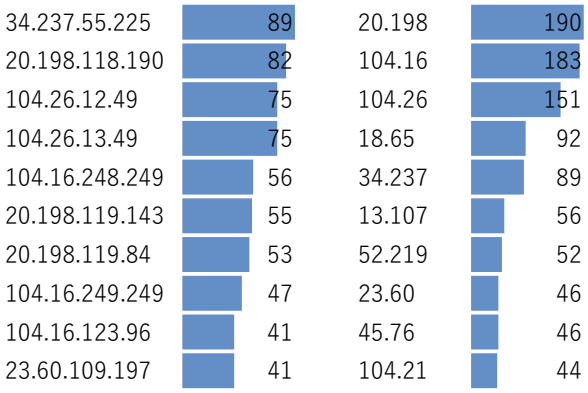

図 4.9　Honeygain の通信先と 100 回の観測での観測回数 (上位 10)

表 4.5　Honeygain の通信先 IP アドレスと whois 情報 (上位 10)

IP アドレス	whois
34.237.55.225	Amazon Technologies Inc.
20.198.118.190	Microsoft Corporation(MSFT)
104.26.12.49	Cloudflare, Inc.(CLOUD14)
104.26.13.49	Cloudflare, Inc.(CLOUD14)
104.16.248.249	Cloudflare, Inc.(CLOUD14)
20.198.119.143	Microsoft Corporation(MSFT)
20.198.119.84	Microsoft Corporation(MSFT)
104.16.249.249	Cloudflare, Inc.(CLOUD14)
104.16.123.96	Cloudflare, Inc.(CLOUD14)
23.60.109.197	Akamai Technologies, Inc.

表 4.6　ブラックリストに登録した IP アドレスの割当国

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 4.7　RESIP 検知プログラムの精度

	提案手法			従来手法 [4]		
	Hola VPN	Proxyrack	Honeygain	Hola VPN	Proxyrack	Honeygain
TP	99	98	100	100	99	100
TN	100	100	100	88	88	88
Accuracy	0.995	0.99	1	0.94	0.935	0.94
F-score	0.994	0.989	1	0.943	0.938	0.943

第 5 章

おわりに

本研究では RESIP アプリのホストとなる 3 つのアプリについて通信先 IP アドレスを観測することで，各 RESIP アプリが高頻度で定期的に通信する IP アドレスを確認した．またそれらの IP アドレスに基づいて，対象の端末が RESIP ホストとなっているかを高い精度で判別する方法を提案した．

謝辞

本研究を進めるにあたり、多くの方々にご指導いただきました．指導教官である明治大学総合数理学部先端メディアサイエンス学科の菊池浩明教授に感謝いたします．また，メンターとして指導していただいた梶間大地さんをはじめ研究室の方々には様々な意見を頂き感謝の念に堪えません．本当にありがとうございました．

参考文献

[1] Mirai ボットネットとは？ Cloudflare，(閲覧日：2022/11/29，https://www.cloudflare.com/ja-jp/learning/ddos/glossary/mirai-botnet/)

[2] Xianghang Mi, et al., “Resident Evil: Understanding Residential IP Proxy as a Dark Service”，2019 IEEE Symposium on Security and Privacy，2019，pp. 1185-1201.

[3] 半澤 映拓， 菊池 浩明， Residential IP Proxy サービスに悪用される住宅用ホストの調査，CSS2019，pp.918-925，2019.

[4] Altug Tosun, et al., “RESIP Host Detection: Identification of Malicious Residential IP Proxy Flows”，2021 IEEE International Conference on Consumer Electronics，2021.

[5] Get The Free and Premium Hola Online — Proxy Unblocker，(閲覧日 2022/11/15，https://hola.org/)

[6] Proxyrack: Buy Proxies HTTP, UDP, SOCKS Proxy，(閲覧日：2022/11/15，https://www.proxyrack.com/)

[7] Passive Income – Effortlessly — Honeygain，(閲覧日：2022/11/15，https://www.honeygain.com/)

付録 A

ARP テーブルスプーフィング攻撃のリスク評価

A.1　はじめに

近年はテレワークの普及に伴い，家庭内 LAN におけるセキュリティ対策が問題になっている．通信内容の盗聴や，スプーフィングを利用してフィッシングサイトに誘導するといった脅威にさらされている．中でも，IP アドレス導出プロトコル ARP には認証機能がなく，容易に偽造される脅威が潜在しており，ettercap, dsniff, scapy などの多くの攻撃ツールが入手容易な状態にある．

そこで，本研究ではルータへの通信を盗聴する中間者攻撃を実現する ARP スプーフィングを行うツールに対する，ARP を用いて家庭内ネットワークの構築を管理している商用セキュリティ機器ウィルスバスター for Home Network の耐性と，ARP 偽装の強度を明らかにすることを目的とする．ARP テーブルの時系列変化を観測する実験を行い，ARP パケットの送信間隔などの要因を調査する．

A.2　準備

A.2.1　ARP

ARP(Address Resolution Protocol) は LAN 内のホストの IP アドレスと MAC アドレスを紐付けるための 2 層のプロトコルである．Ethernet フレームを送信に必要な宛先の MAC アドレスが必要な場合に，ネットワークに ARP リクエストをブロードキャストして相手の MAC アドレスを得る．得られた IP アドレスと MAC アドレスの関係は各ホストの ARP テーブルに格納される．

A.2.2　ARP スプーフィング

ARP では ARP パケットの内容が正しいことを仮定し，正しさを検証する方法が備わっていない．悪意を持った攻撃者が偽りの ARP パケットを送信することで，本来のルータとホストの間の経路 1 を攻撃者 IP3 を経由する偽の経路 2 に変更する攻撃を ARP スプーフィングという．

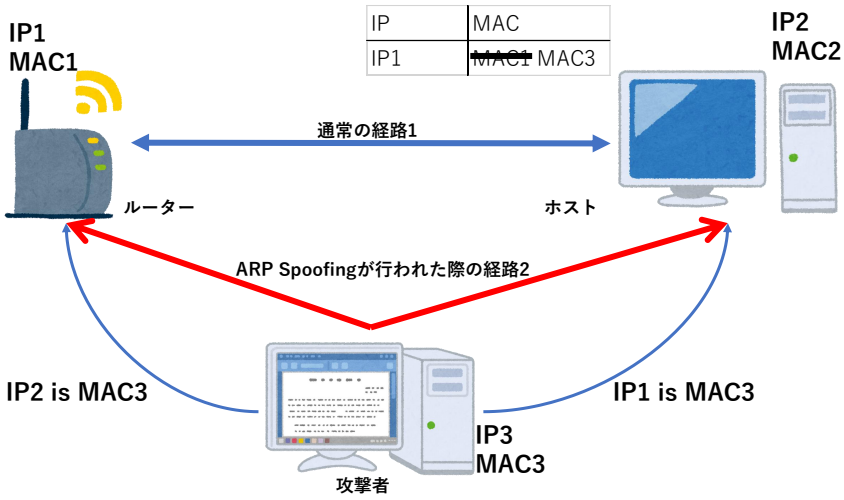

図 A.1　ARP スプーフィング

表 A.1　4 つのツールの名称，開発者と開発目的

使用ツール	開発者	開発目的
VBHN	トレンドマイクロ社	セキュリティ対策 [4]
scapy	Philippe Biondi	パケットの操作 [5]
ettercap	Ettercap Dev. Team	ネットワーク及びホストの解析 [6]
dsniff	Dug Song	ネットワークの監査及びペネトレーションテスト [7]

A.2.3　ウイルスバスター for Home Network(VBHN)

VBHN はトレンドマイクロ株式会社が発売しているセキュリティ対策機器である，家庭内ネットワーク内の通信を監視してネットワーク内の端末に対しての攻撃のブロックやインターネットへのアクセス管理を行う．VBHN は通信を監視するためにネットワーク内の全端末にプロキシ ARP を行い，パケットが VBHN を経由するようにすることでこれらのセキュリティ対策を実現している．

A.2.4　ARP スプーフィングツール

本実験で使用するプロキシ ARP 及び ARP スプーフィングを行うツールについて表 A.1 に示す．本稿では VBHN の行うプロキシ ARP に着目し，その他 3 つの ARP スプーフィングを行うツール，scapy，ettercap，dsniff との比較を行う．

入力 調査対象 IP アドレス x, 競合する MAC アドレス m_1,m_2

1. ARP テーブルを確認する
2. x に対応している MAC アドレスが m_1 か m_2 か記録する
3. 1. から 2. を決められた時間繰り返す
4. ホスト別の ARP テーブル保有累積時間を求めて出力する

図 A.2　プログラムのアルゴリズム

```
2021-11-14 21:54:00.989563: Current 192.168.10.1 is d0-c6-37-a5-24-63
2021-11-14 21:54:05.793870: 192.168.10.1 changed to 00-28-f8-41-80-2f
2021-11-14 21:54:06.228602: 192.168.10.1 changed to d0-c6-37-a5-24-63
2021-11-14 21:54:15.731611: 192.168.10.1 changed to 00-28-f8-41-80-2f
2021-11-14 21:54:16.167987: 192.168.10.1 changed to d0-c6-37-a5-24-63
2021-11-14 21:54:25.763313: 192.168.10.1 changed to 00-28-f8-41-80-2f
2021-11-14 21:54:26.193277: 192.168.10.1 changed to d0-c6-37-a5-24-63
2021-11-14 21:54:35.790487: 192.168.10.1 changed to 00-28-f8-41-80-2f
2021-11-14 21:54:36.228958: 192.168.10.1 changed to d0-c6-37-a5-24-63
2021-11-14 21:54:45.761540: 192.168.10.1 changed to 00-28-f8-41-80-2f
2021-11-14 21:54:46.181296: 192.168.10.1 changed to d0-c6-37-a5-24-63
2021-11-14 21:54:55.904047: 192.168.10.1 changed to 00-28-f8-41-80-2f
2021-11-14 21:54:56.178663: 192.168.10.1 changed to d0-c6-37-a5-24-63
router=0:00:00, b=0:00:07.279810, c=0:00:52.755185
```

図 A.3　観測ログの例

A.3　実験

A.3.1　実験目的

ARP スプーフィングが行われるとホストの ARP テーブルでルータの IP アドレスに対応した MAC アドレスが変化する．しかし，複数のツールが混在する環境では，パケットの一部のみ中継されて，通信品質が不確定である．従って，ARP スプーフィングツールに対するネットワーク管理の安全性を正確に評価するためには，各ホストの ARP テーブルの変化をミクロに観測する必要がある．そこで，ARP テーブルの時系列変化を観測して，各種ツールのリスクを定量化することを本研究の目的とする．

A.3.2　観測ツールの開発

本ツールは ARP テーブルの変化の検知を行う．Python で作成した観測ツールのアルゴリズムを図 A.2 に示す．ではホストの ARP テーブルを 0.1 秒毎に観測し，ルータの IP アドレスに対応した MAC アドレスの変化を表示する．ホストが ARP テーブルを保有していた累積時間を集計し，計測終了後に表示する．

図 A.3 に本ツールを動作させた時のログを示す．ARP テーブルを調べて表示し，それ以降は ARP テーブルが変更された時のみ通知する．また 60 秒の観測が終了したあと，各ホストの ARP テーブルを保有累積時間を表示する．図 A.3 の例では ettercap と dsniff を使ってホストに ARP スプーフィングを行っている．観測を開始した 2021-11-14 21:54:00 の時点では A の ARP テーブルは MAC アドレス d0-c6-37-a5-24-63 の攻撃ホスト 1 で動いている dsniff が支配しているがその後は MAC アドレス 00-28-f8-41-80-2f の攻撃ホスト 2 で動

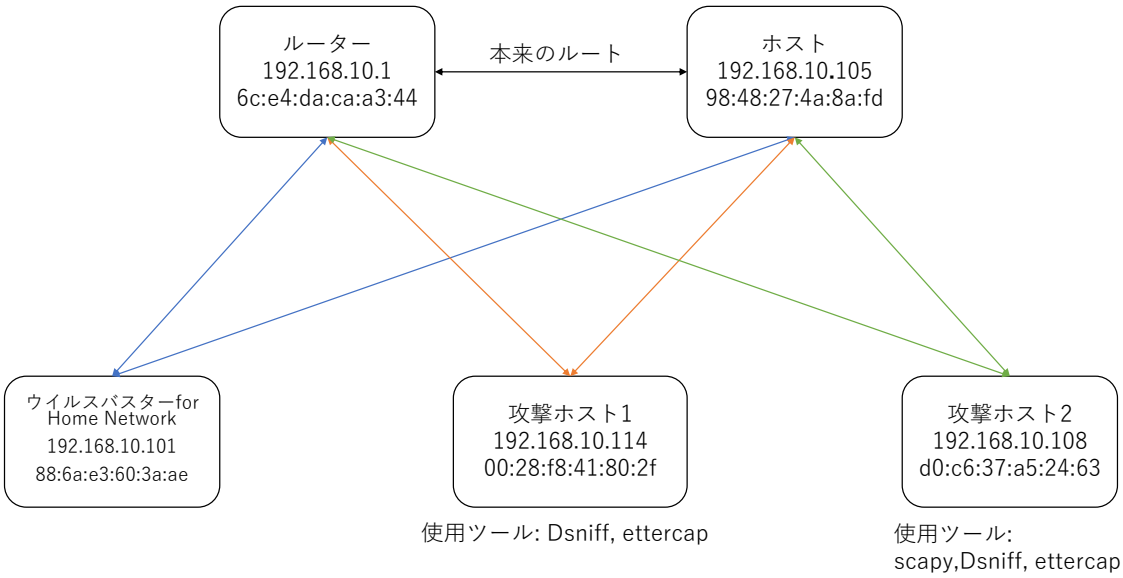

図 A.4　実験環境

いている ettercap と交互に支配している．60 秒の観測の結果，dsniff が 52.7 秒間，ettercap が 7.2 秒間 A の ARP テーブルを保有していたことがわかる．

A.3.3　実験方法

本実験では複数の攻撃者が同時に一つのホストに ARP スプーフィング攻撃を行った際にその攻撃を受けたホストの ARP テーブルの変化の違いを観測することで ARP スプーフィング攻撃のリスクの調査を行う．実験環境は図 A.4 で示される家庭内のネットワークでである．ホスト *A* は Windows 10 である．ARP スプーフィングを行う機器は，VBHN，Windows 11，Ubuntu 20.04，Kali Linux 2021.2 の 4 台である．また Windows，Ubuntu，Kali については IP フォワーディングの設定を行っている．

実験 1 では表 A.1 の 4 つのツールについて，はじめに 1 つずつ ARP スプーフィングを行い *A* の ARP テーブルの変化の仕方を調査する．次の実験 2 では 4 つのツールのうち 2 つを選び同時に ARP スプーフィングを行った際の *A* の ARP テーブルの変化の違いを調査する．

開発したツールを用いて測定を行い，得られた 60 秒間の ARP テーブルの変化と，どの機器がどの期間 ARP テーブルを支配していたか記録する．

A.3.4　実験結果

実験 1

一つのツールで ARP スプーフィングを行った際の ARP テーブルを支配していた時間と割合を表 A.2 に示す．VBHN と ettercap は計測中は常に ARP スプーフィングが成功している状態であり，ARP テーブルにルータの MAC アドレスが存在する状態は観測できなかった．一方，scapy は 1.15 秒間，dsniff は 1.95 秒間ルータ

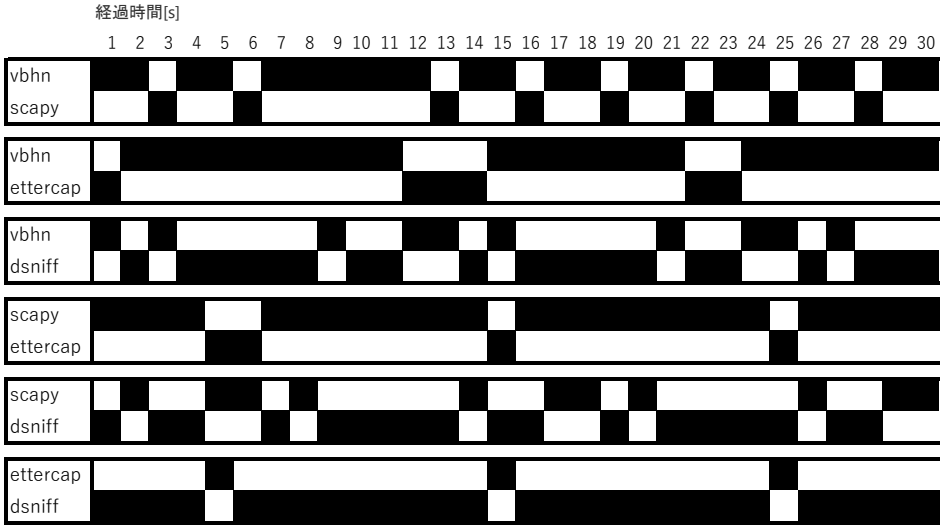

図 A.5　ARP テーブルを支配していたホストを示すタイムチャート

表 A.2　単独ツールで ARP スプーフィングを行った際の ARP テーブルの変化

ツール	送信間隔 [s]	計測時間 [s]	テーブルを支配した累積時間 [s]	割合 [%]
VBHN	3	60.24	60.24	100.00
scapy	3	60.51	59.36	97.93
ettercap	10	60.89	60.89	100.00
dsniff	2	59.29	57.34	96.71

表 A.3　2 台同時に ARP スプーフィングを行った際の ARP テーブルの保持期間

	VBHN[s]	scapy[s]	ettercap[s]	dsniff[s]	平均 [%]
VBHN		25.55(42.64%)	46.83(84.06%)	18.19(31.47%)	52.72
scapy	34.26(57.35%)		50.85(84.44%)	21.69(36.01%)	59.26
ettercap	8.88(15.93%)	9.37(15.55%)		7.27(12.11%)	14.53
dsniff	39.61(68.52%)	37.59(62.41%)	52.75(87.88%)		72.93

に ARP テーブルを書き換えられたが，4 つのツールで一番支配時間が短かった dsniff の場合でも 96.71% の時間で ARP スプーフィングが成功していた．

実験 2

2 台同時に ARP スプーフィング攻撃を行った際の結果を表 A.3 に示す．複数ツール同士の実験では，ARP パケットの送信間隔が短いものの方が ARP テーブルの保持期間が長かった．一方 VBHN と scapy の様にパケット送信間隔が同じ 3 秒のツール同士の実験については，実験の度に ARP テーブルの支配時間が変化して安定していなかった．ARP テーブルの支配している時間を図 A.5 のタイムテーブルに示す．

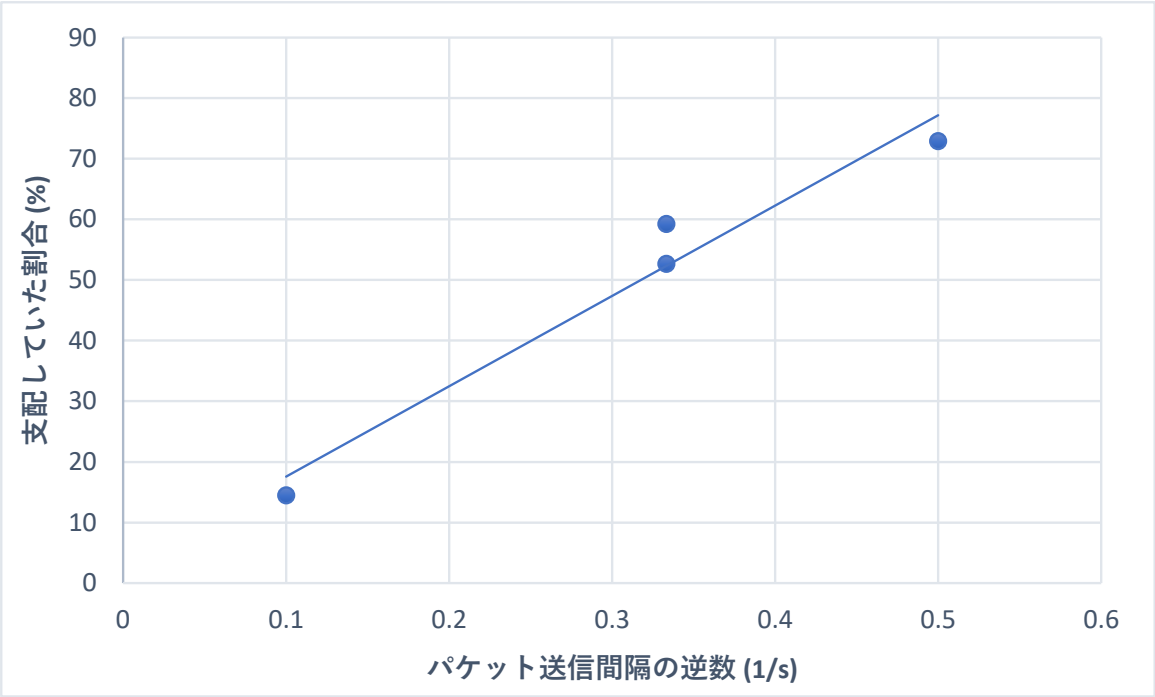

図 A.6　パケット送信間隔と支配率のグラフ

A.3.5　考察

単一のツールを用いて ARP スプーフィングを行った実験の結果で短い時間ルータの MAC アドレスがを回復した理由として，ARP パケットの送信先の違いが考えられる．ettercap はホスト *A* とルータ *R* の 2 方向に，scapy と dsniff はホスト *A* にのみ偽の ARP パケットを送っている．

また，ルータ等の通常の ARP パケットの送信間隔は 15〜45 秒であり，ツールの間隔と比較して非常に長いが，タイミングによってはスプーフィングされたテーブルを上書きする時間がある．

2 台のツールを同時に動かした実験 2 では，パケットの送信間隔が同じである VBHN と scapy の組を除く 5 つの組み合わせにおいて ARP パケットの送信間隔が短いツールの方が平均 74.11% の期間ホストの ARP テーブルを支配していた．前述の VBHN と scapy で結果にばらつきが見られたことについては 2 つのツールを開始させるタイミングに依る要素が大きいものと考える．

A.4　おわりに

本実験では ARP スプーフィングを行う 4 つのツールについて 2 つ同時に動作させた際の ARP テーブルの変化を観測した．ARP テーブルの保持期間には ARP パケットの送信間隔が関係しており，パケットの送信間隔の異なるツール同士が同時に ARP スプーフィングを行った場合にはパケットの送信間隔が短いツールのほうがより長い時間ホストの ARP テーブルを占有する．

参考文献

[1] 三宅猛ほか “ARP テーブルの集中管理による認証ネットワーク上の不正接続検出と排除方法の提案”，情報処理学会研究報告，2008-CSEC-40，2008.

[2] 住友 “ARP 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.

[3] 平山 “ウイルスバスター for Home Network の調査研究”，2020 年度菊池研究室卒業論文，2020.

[4] ウイルスバスター for Home Network ｜トレンドマイクロ，閲覧日 2022/1/4, https://www.trendmicro.com/ja_jp/forHome/products/vbhn.html

[5] Scapy，閲覧日 2022/1/4，https://scapy.net

[6] Ettercap Home Page，閲覧日 2022/1/4，https://www.ettercap-project.org

[7] dsniff，閲覧日 2022/1/4，https://www.monkey.org/~dugsong/dsniff/