

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

守屋龍一, 北原拓海, 福田ひかり, 菊池浩明

明治大学 総合数理学部

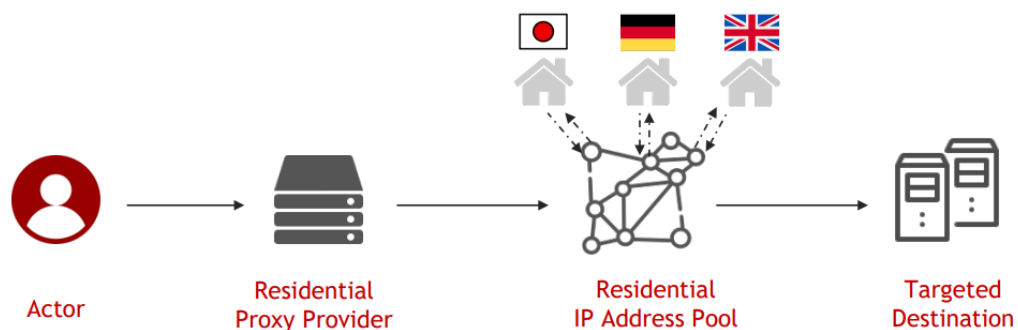
# 背景

## ◆ 本来の目的以外でResidential IP Proxy (以下RESIPとする)サービスが

違法行為に不正利用されていることを指摘 [1] (Miら)

- 例：違法な広告プロモーション、フィッシング、マルウェアホスティングなど

Residential proxy covers actor identity and fakes card holder location



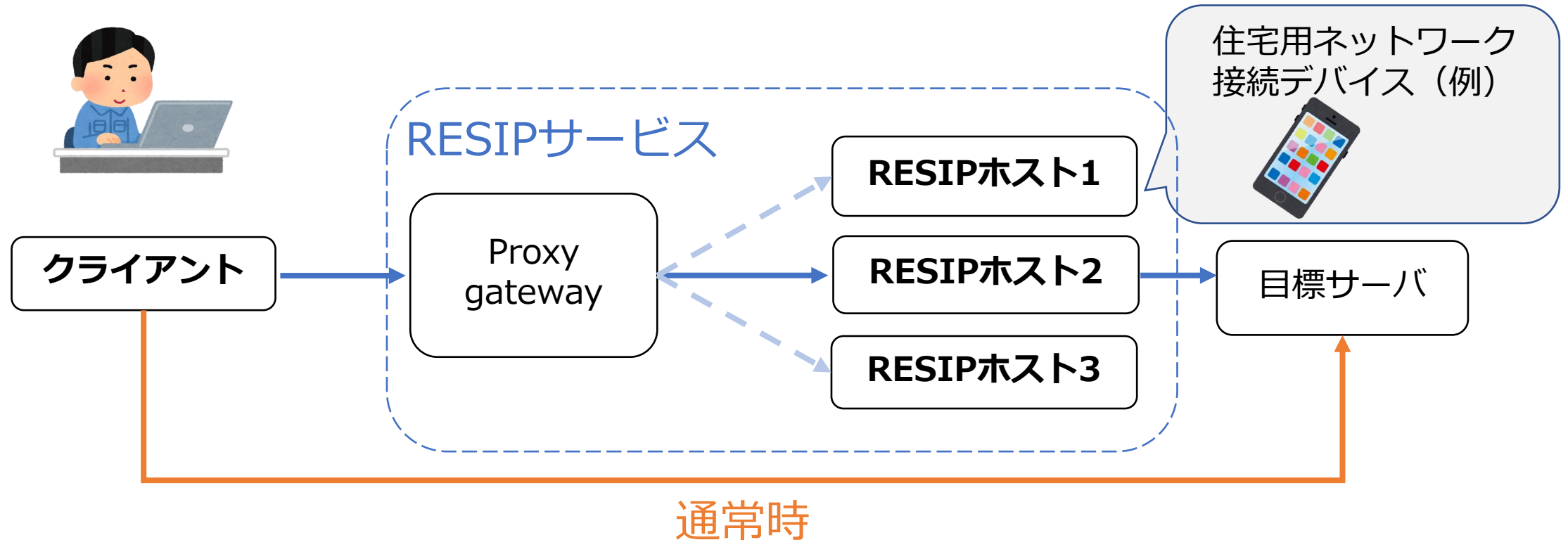
フィッシング等で集めた  
クレジットカード使用時、  
身元の秘匿、場所の偽装が可能

Major residential proxy used by fraudsters:  
911 (China), oxylabs (Lithuania), BrightData (Israel)

CODE BLUE 2022, Strawberry Donut, Understanding the Chinese underground card shop ecosystem and becoming a phishing master

# RESIPサービスとは

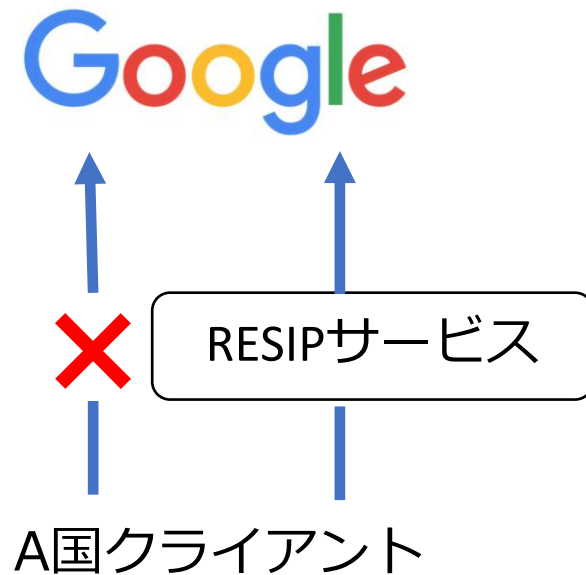
- ◆ 通信を中継するプロキシサービスの一つ
- ◆ 中継機が実際に使用されているデバイスのため通常時と**区別されにくい**



# RESIPの利用目的

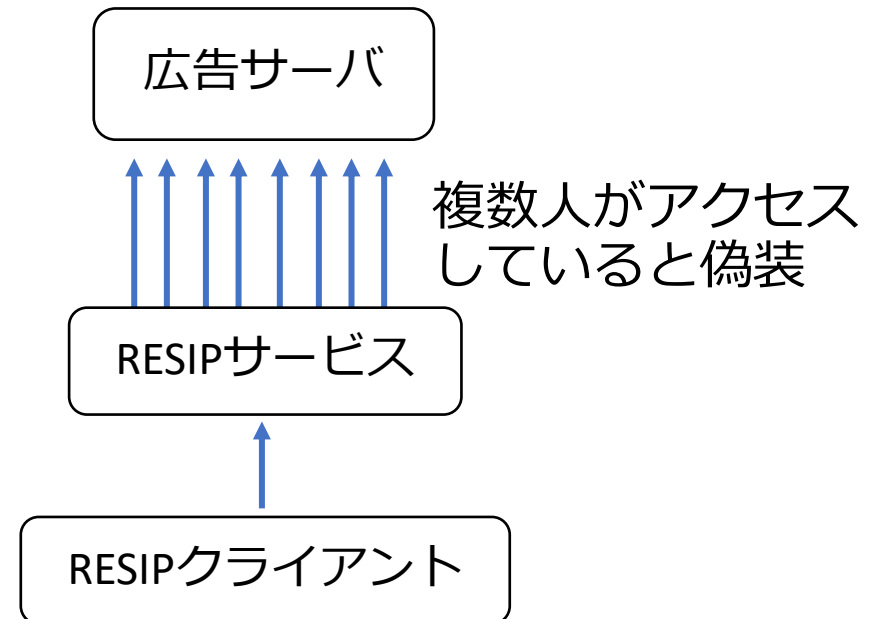
◆ ネット検閲の回避

◆ 身元の秘匿







◆ クローリング

◆ 広告アクセス数の水増し



# RESIPプロバイダ比較

プロバイダ	 bright data	 Proxyrack	 oxylabs®	 PROXYSELLER
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	<b>50か国</b>
RESIPが交換される 間隔の指定	× (IPを交換しない ことは可能)	○ (5, 10, 15, 30, 60分)	○	×
RESIP所在地指定	○	○	○	<b>契約時に指定 変更不可</b>
リクエストごとに RESIPを変更	○	プランによる	○	×

# リサーチクエスチョン

---

- ◆ Q1. RESIPホストは悪性サイトと通信している？
- ◆ Q2. 広告不正をしている？
- ◆ Q3. マネタイズに使われている？

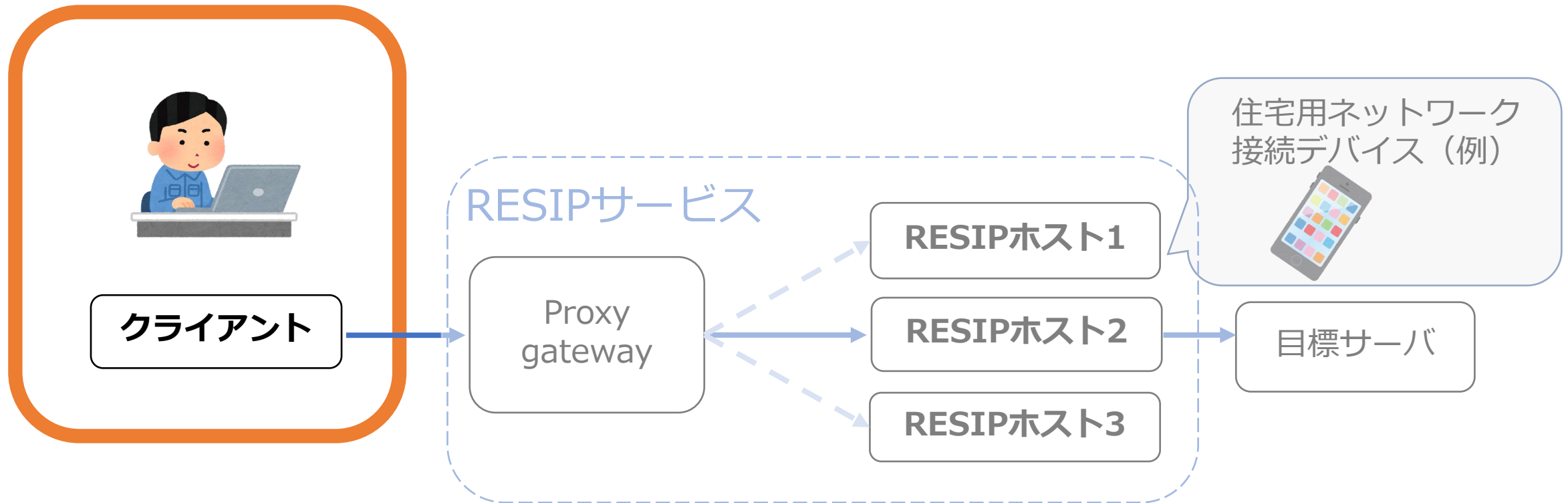
# リサーチクエスチョン

---

- ◆ Q1. RESIPホストは悪性サイトと通信している？
- ◆ Q2. 広告不正をしている？
- ◆ Q3. マネタイズに使われている？

# RESIPクライアントへ与える影響の調査

- ◆ RESIPサービスが不正が行える環境であるのかを調査



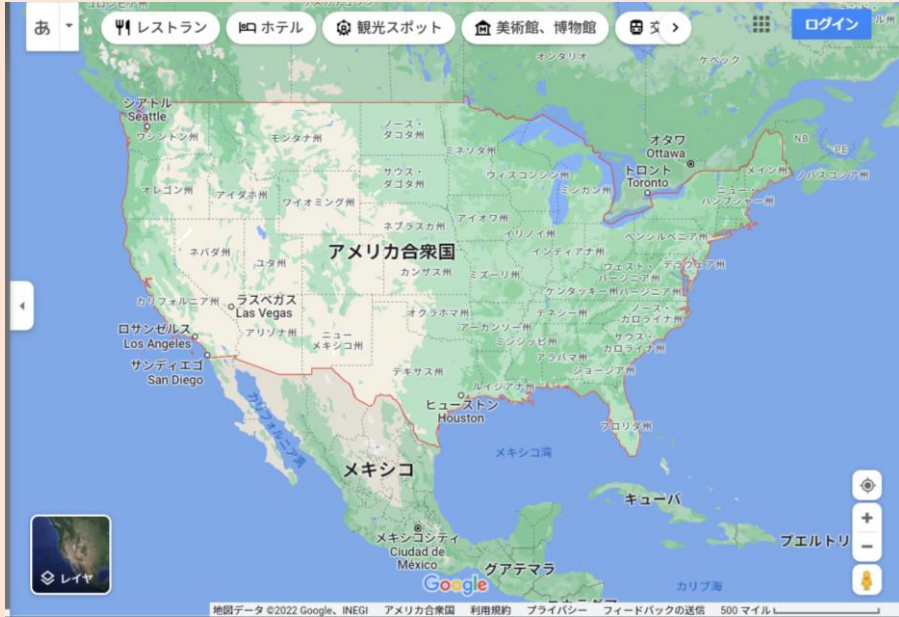
通常時



# 調査 1 : 位置情報



通常時  
明治大学中野キャンパス



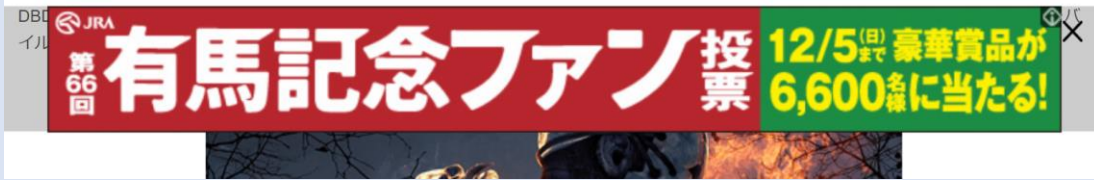
RESIPサービス利用時  
アメリカ合衆国

位置情報の調査結果 (RESIPホストの位置が推定された件数/総数)

Bright Data	ProxyRack	Oxylabs	Proxy-Seller
0/20	20/20	20/20	10/20

位置の偽装は可能

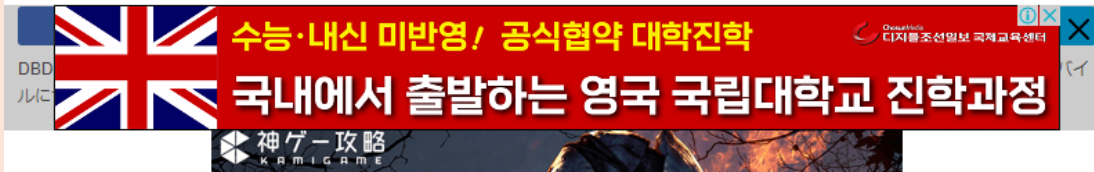
# 調査 2 : ターゲット広告



通常時



条件 2 : 日本語表記で**海外在住者向け**の内容



条件 1 : **言語**が変化



条件 3 : **RESIP所在地の地名**が入っている

RESIPサービス利用時

広告調査結果 (影響を受けた広告数/全広告数)

Bright Data	ProxyRack	Oxylabs	Proxy-Seller	平均
0.42	0.55	×	0.54	0.50

Oxylabsの“ × ”は広告が表示されなかったことを示す

**広告業者を偽ることが可能**

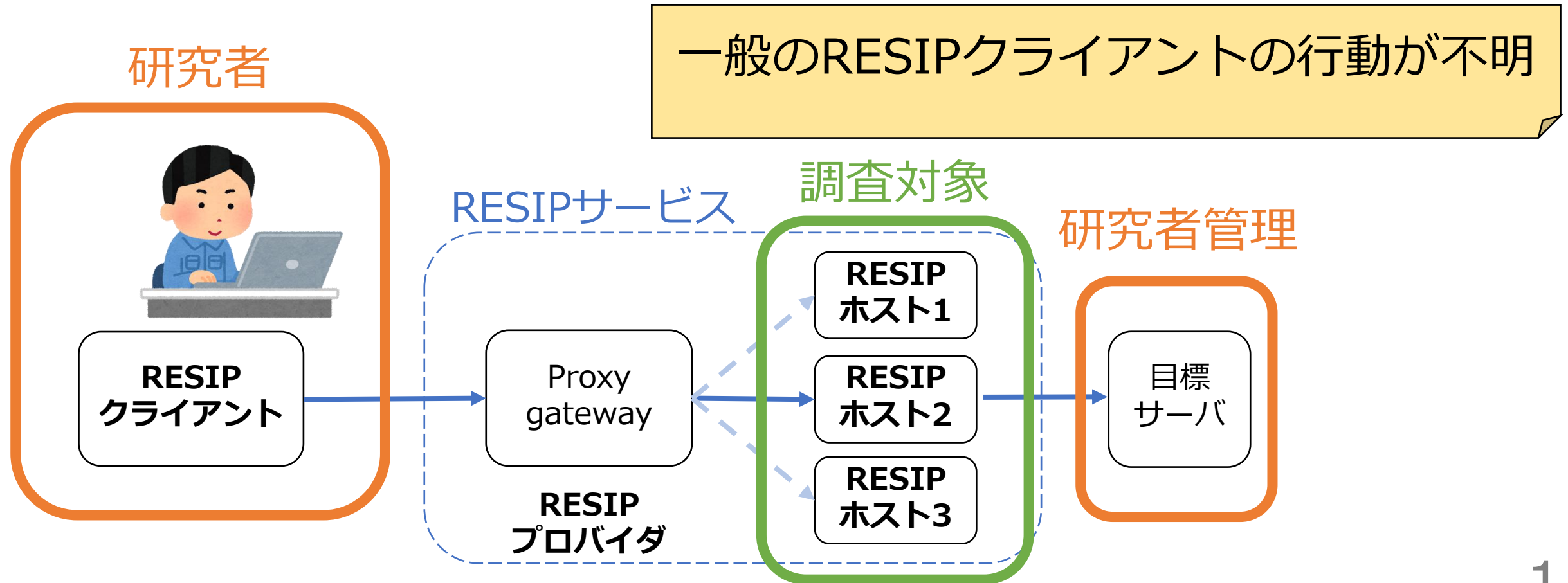
# RESIP不正利用の報告に対してプロバイダ側の主張

## ◆ RESIPプロバイダは適切に使用されていると主張

The image shows a screenshot of the Bright Data website. At the top, the 'bright data' logo is on the left, and navigation links for 'Proxy', 'Web Data', 'Resources', 'Pricing', 'Contact sales', and 'Sign i' are on the right. Below the navigation, there are several icons representing different use cases: 'FULL CONSENT', 'MONITOR AND PROTECT', 'IMPROVED UX', 'USER COMPLIANCE EVALUATION & COMPLIANCE', 'NO USER DATA COLLECTING', 'COMPLIANCE OFFICER', 'VERIFIED USE CASES', 'USAGE MONITORING', and 'NC RESEL'. A large orange text overlay on the right side of the screenshot reads: 'ウェブサイトのテスト、価格比較、旅行データの集計 など'. In the center, a section titled 'Verified use cases only' contains a text box with the following text: 'Approved use of the Bright Data network includes gathering data for website testing, price comparison, travel data aggregation, brand protection, and actions of a similar nature for business intelligence. We do not accept any use of our network that aims to emulate a real user in return for direct payment, misleading purposes or fraudulent activity. For more information, see our [Acceptable Use Policy](#).' Below this, two icons are shown: one for 'Ad fraud or click fraud' and another for 'Adding any-kindof reviews'. The text '広告詐欺' is written in large black characters at the bottom left of the screenshot.

# 先行研究の問題点

- ◆ RESIPクライアントになった際の通信情報の調査[4][5] (半澤ら、住友ら)

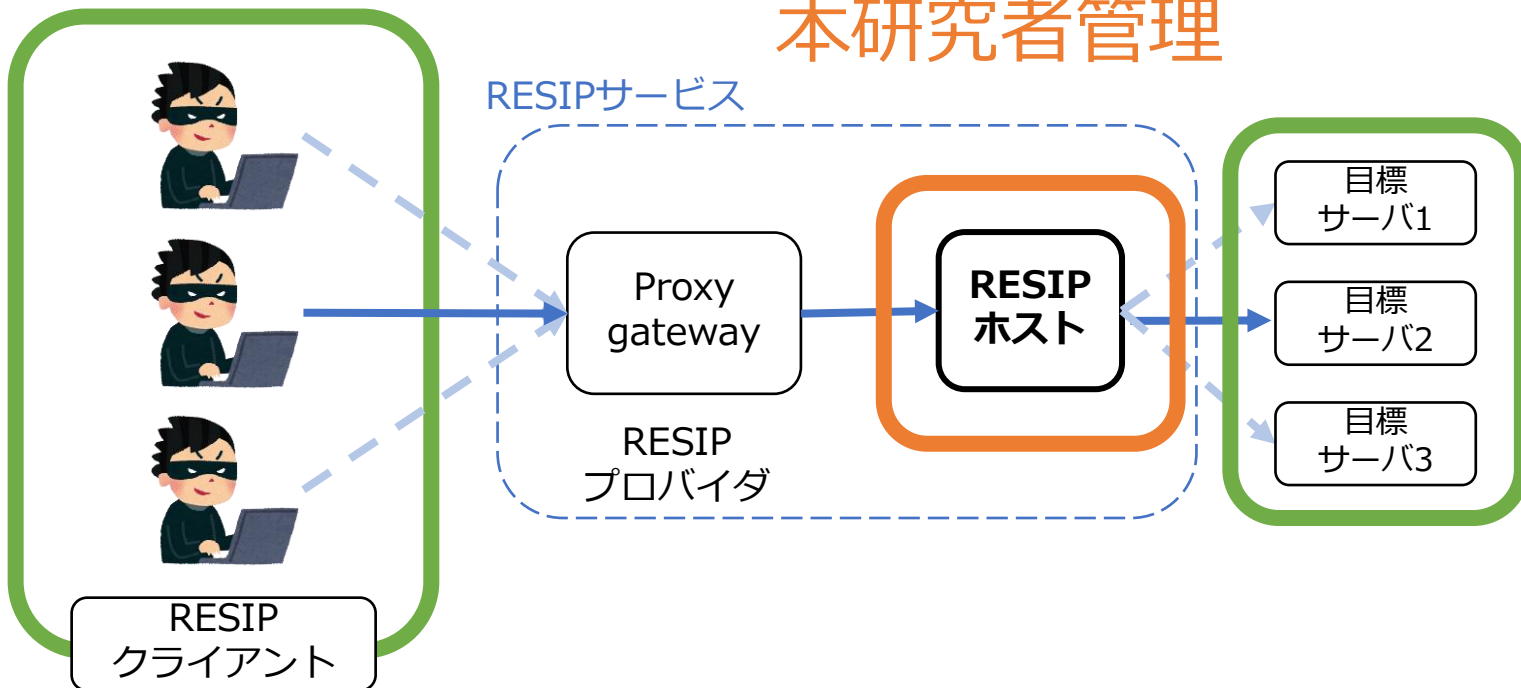


# 解決策

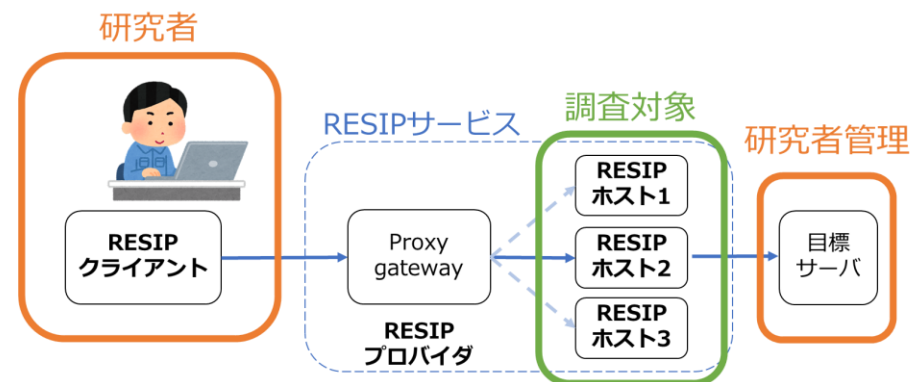
## ◆ RESIPサービスの不正利用の実態を調査

- 実際に**RESIPホスト**になり、RESIPクライアントの利用内容を推測

本調査対象



先行研究[4][5]



# リサーチクエスチョン（再）

---

- ◆ Q1. RESIPホストは悪性サイトと通信している？
- ◆ Q2. 広告不正をしている？
- ◆ Q3. マネタイズに使われている？

# RESIPホストに関する実験

---

- ◆ 実験 1 : RESIP 検出プログラムの開発と評価 (4.3.1)
  - RESIPホストの通信の調査、RESIP検出プログラムの作成
- ◆ 実験 2 : RESIPホスト比較実験 (4.3.2)
  - Q1、Q2の回答
- ◆ 実験 3 : RESIPホスト24時間観測 (4.3.3)
  - Q3の回答

# 実験方法

---

## ◆ 実験 2 : RESIPホスト比較実験 (4.3.2)

- **Bright Data、ProxyRack、Oxylabs**のRESIP環境、**通常環境** (非RESIP環境)
- Wiresharkで上記環境の通信を5時間観測

- ドメイン
- IPアドレス
- 通信時間分布 など

## ◆ 実験 3 : RESIPホスト24時間観測 (4.3.3)

- Bright Data、ProxyRackのRESIP環境
- **pyshark**で上記環境の通信を**24時間観測**

### **pyshark**

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



# 実験結果 概要

観測したIPアドレスとドメイン総数

	IPアドレス総数	ドメイン総数
Bright Data	645	430
ProxyRack	177	68
Oxylabs	85	173
通常時	45	27

RESIPサービスの通信を  
中継しているため

宛先 IP アドレス の国判定結果

	国総数
Bright Data	18
ProxyRack	31
Oxylabs	12
通常時	8

GeoLite2 Free  
Geolocation  
Data  
で判定

VirusTotalの分類タグで分類

ドメインのカテゴリ分類結果

ドメインカテゴリ	Bright Data	ProxyRack	Oxylabs
Travel	5%	1%	2%
Shopping	13%	5%	4%
Advertisements	11%	0%	37%
Social Networking	3%	15%	6%
Web Analytics	4%	0%	7%
Finance	2%	1%	1%
Search Engine	4%	4%	16%
News	0%	1%	5%

各RESIPサービスの  
利用内容に差がある

# 悪性サイトとの通信

ドメインの悪性判定結果

	Bright Data	ProxyRack	Oxylabs	先行研究[1]
悪性総数	24	4	7	—
悪性割合 [%]	5.6	5.9	4.0	5

## 悪性ドメイン例

cpi-offers[.]com

api.bdisl[.]com

ariesbee[.]com

- ◆ どのRESIPホストも悪性サイトと通信
- ◆ RESIPサービスは匿名で通信を行うことができる

IPAの報告書[20]で、「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」

フィッシング運営などの作業に RESIPサービスを悪用している可能性

# 広告不正

広告に関するドメインが最も多い

◆ RESIPサービスは、

リクエストごとにIPアド

変更可能（ボットの検出が困難）

◆ 広告クリック詐欺の可能性

◆ RESIP サービス全体での被害額

3,637,670ドル(約5億円)が見積もられる（1か月間）

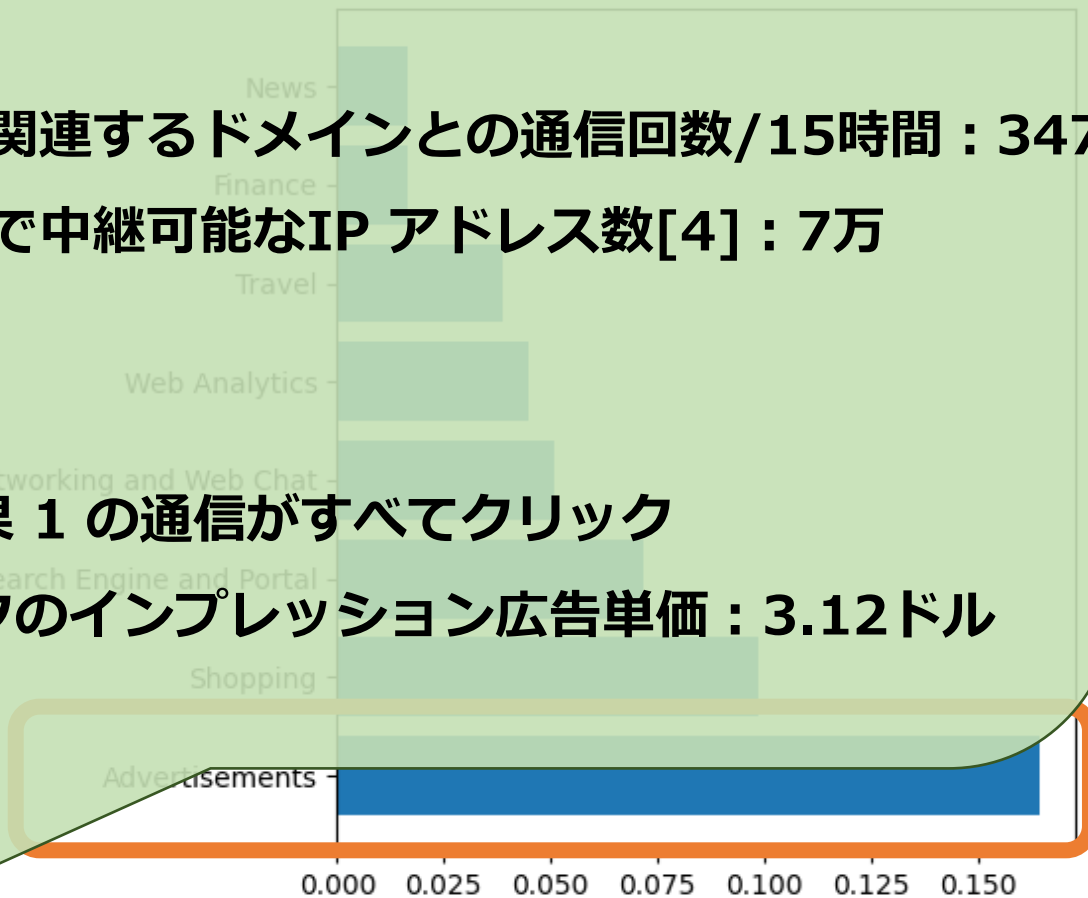
## 見積条件（1か月）

### ◆ 観測結果

1. 広告に関連するドメインとの通信回数/15時間：347
2. 1 ヶ月で中継可能なIP アドレス数[4]：7万

### ◆ 仮定条件

- 観測結果 1 の通信がすべてクリック
- クリックのインプレッション広告単価：3.12ドル



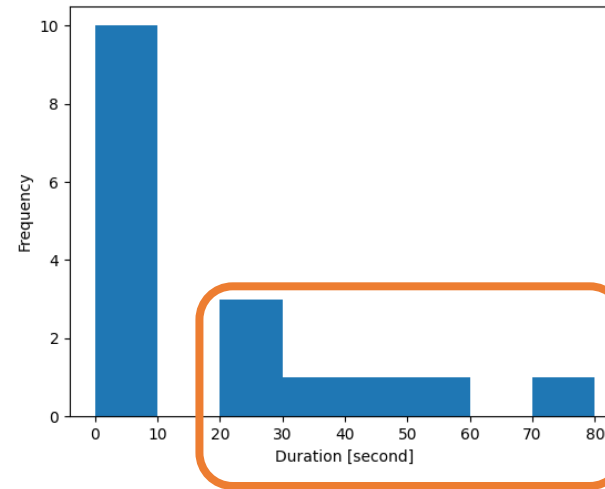
全通信のドメインカテゴリ割合

# マネタイズ

決済サービス（PaypalやAmazon Payなど）と通信を行っていた

- ◆ RESIPサービスは、
  - 使用料最低15ドルと高価
  - 地理的制限を回避し海外からの不正ログインが可能

## Bright Data



RESIP ホストと決済サービスとの通信時間分布

決済サービス例：

Paypal

Amazon Pay

merpay

PAYGENT

Netcerera

Alipay

CAFIS

フィッシング等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）の可能性

# アンサー

---

◆ Q1. RESIPホストは悪性サイトと通信している？

➤ 5%前後の割合で通信している

◆ Q2. 広告不正をしている？

➤ 可能性あり

◆ Q3. マネタイズに使われている？

➤ 可能性あり

# RESIPホストに関する実験

---

- ◆ 実験 1 : RESIP 検出プログラムの開発と評価 (4.3.1)
  - RESIPホストの通信の調査、RESIP検出プログラムの作成
- ◆ 実験 2 : RESIPホスト比較実験 (4.3.2)
  - Q1、Q2の回答
- ◆ 実験 3 : RESIPホスト24時間観測 (4.3.3)
  - Q3の回答

# 実験 1 : RESIP検出

---

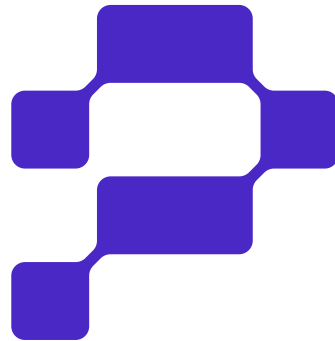
- 先行研究(Tosunらの手法)[6]
  - 3つのアルゴリズムから構成
    - 転送されるパケットの流れ
    - 転送されるパケットのサイズ
    - ホストで行われるDNSルックアップ
- 提案手法
  - 主要RESIPアプリの通信を観測
  - 観測結果をもとにしたブラックリストを作成
  - Pythonとpysharkライブラリを用いたRESIP検出プログラム

# 通信を観測したRESIPアプリ

	Hola VPN	ProxyRackアプリ	Honeygain
サービス開始年	2007	2014	2019
RESIPプロバイダ	Bright Data	ProxyRack	Oxylabs



<https://hola.org>



<https://www.proxyrack.com>



<https://www.honeygain.com>



# 観測回数上位10アドレス

数字は100回の観測で何回観測されたか

日時	2022/11/23-28
場所	自宅(東京都江東区)
ホスト	Windows 10

通常時		Hola VPN		Proxyrack		Honeygain	
204.79.x.x	27	162.125.x.x	99	38.84.x.x	98	34.237.x.x	89
20.198.x.x	21	3.94.x.x	55	209.205.x.x	68	20.198.x.x	82
117.18.x.x	17	3.228.x.x	52	23.227.x.x	60	104.26.x.x	75
13.107.x.x	16	3.228.x.x	47	192.30.x.x	58	104.26.x.x	75
20.43.x.x	16	3.94.x.x	44	192.34.x.x	56	104.16.x.x	56
204.79.x.x	9	206.189.x.x	34	23.227.x.x	55	20.198.x.x	55
20.212.x.x	4	40.70.x.x	28	44.233.x.x	55	20.198.x.x	53
117.18.x.x	3	20.198.x.x	26	104.21.x.x	40	104.16.x.x	47
40.90.x.x	3	192.81.x.x	24	199.7.x.x	38	104.16.x.x	41
104.78.x.x	2	159.223.x.x	21	213.248.x.x	32	23.60.x.x	41

# 作成したブラックリスト

---

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.

# 検知精度の比較

- 従来手法と比較して真陽性率(TP)は微減
- 真陰性率(TN)は増加

	Hola VPN	ProxyRackアプリ	Honeygain
Tosunら[6]の手法 TP	100	99	100
Tosunら[6]の手法 TN	88	88	88
提案手法 TP	99	98	100
提案手法 TN	<b>100</b>	<b>100</b>	<b>100</b>

# 結論

---

- ◆ RESIPサービスに関する不正行為の可能性を示した
- ◆ RESIPの検知は可能
- ◆ 今後の課題
  - ◆ 不正行為の詳細を明らかにすること
  - ◆ RESIPホストの通信観測を長期間行える環境をつくること