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

総合数理学部 先端メディアサイエンス学科

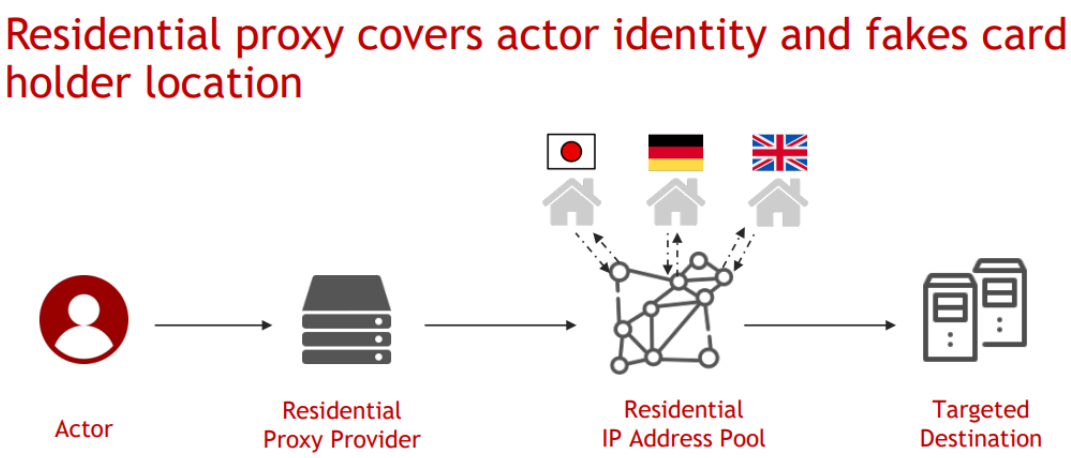
菊池研究室 4年

守屋 龍一

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

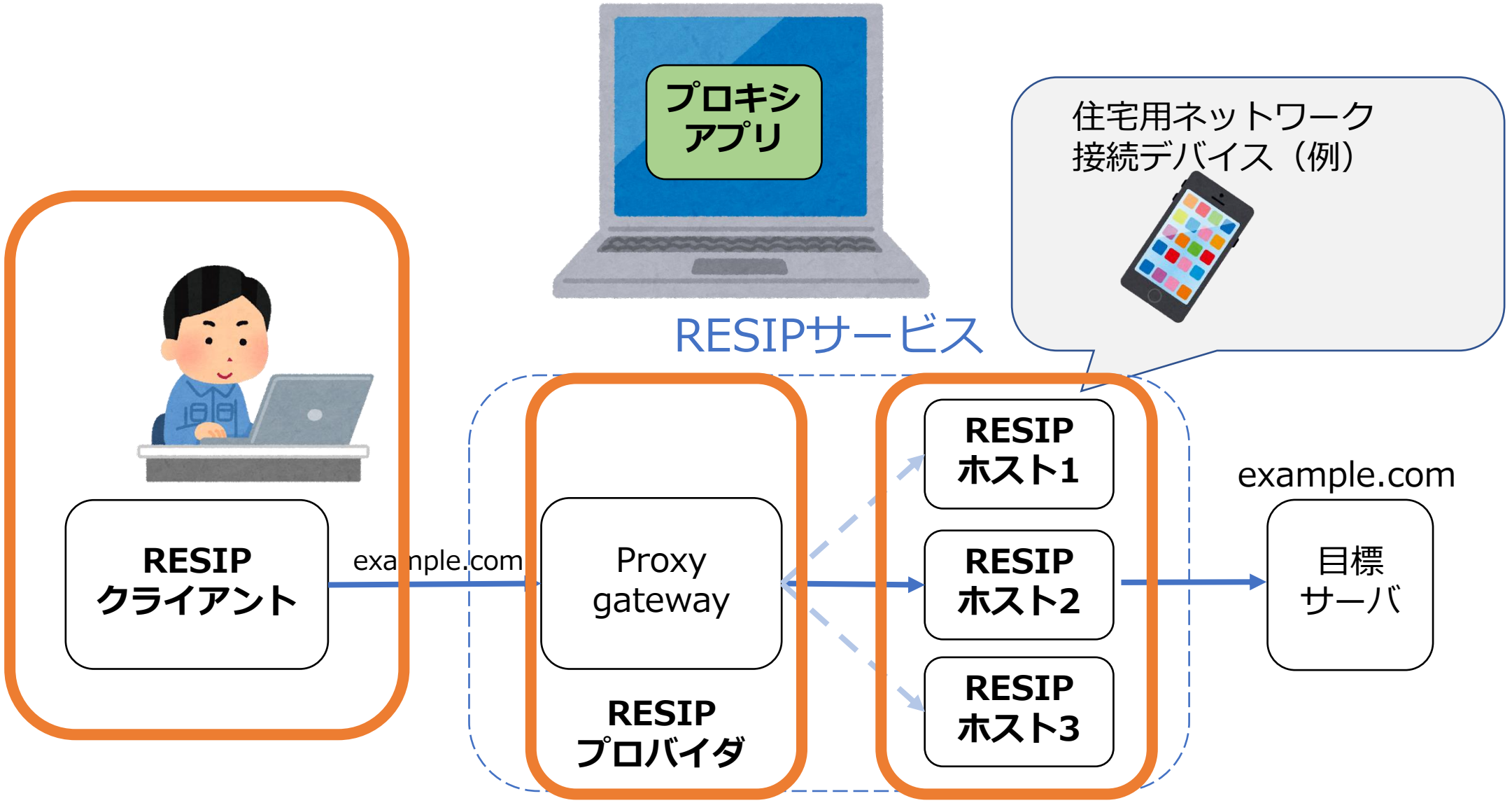


Major residential proxy used by fraudsters:
911 (China), oxylabs (Lithuania), BrightData (Israel)

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

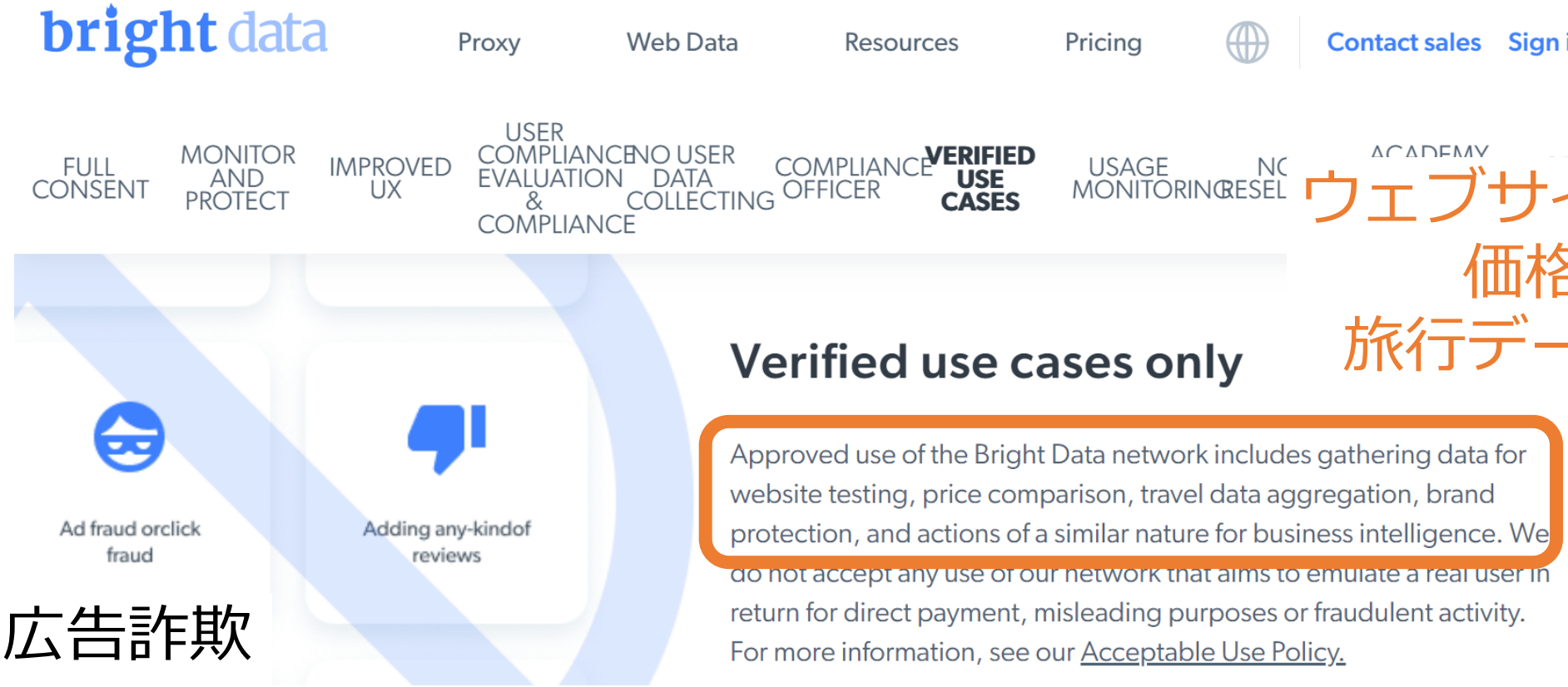
CODE BLUE 2022, Strawberry Donut, Understanding the Chinese underground card shop ecosystem and becoming a phishing master

RESIPサービスについて



問題点

◆ RESIPプロバイダは適切に使用されていると主張



ウェブサイトのテスト、
価格比較、
旅行データの集計など

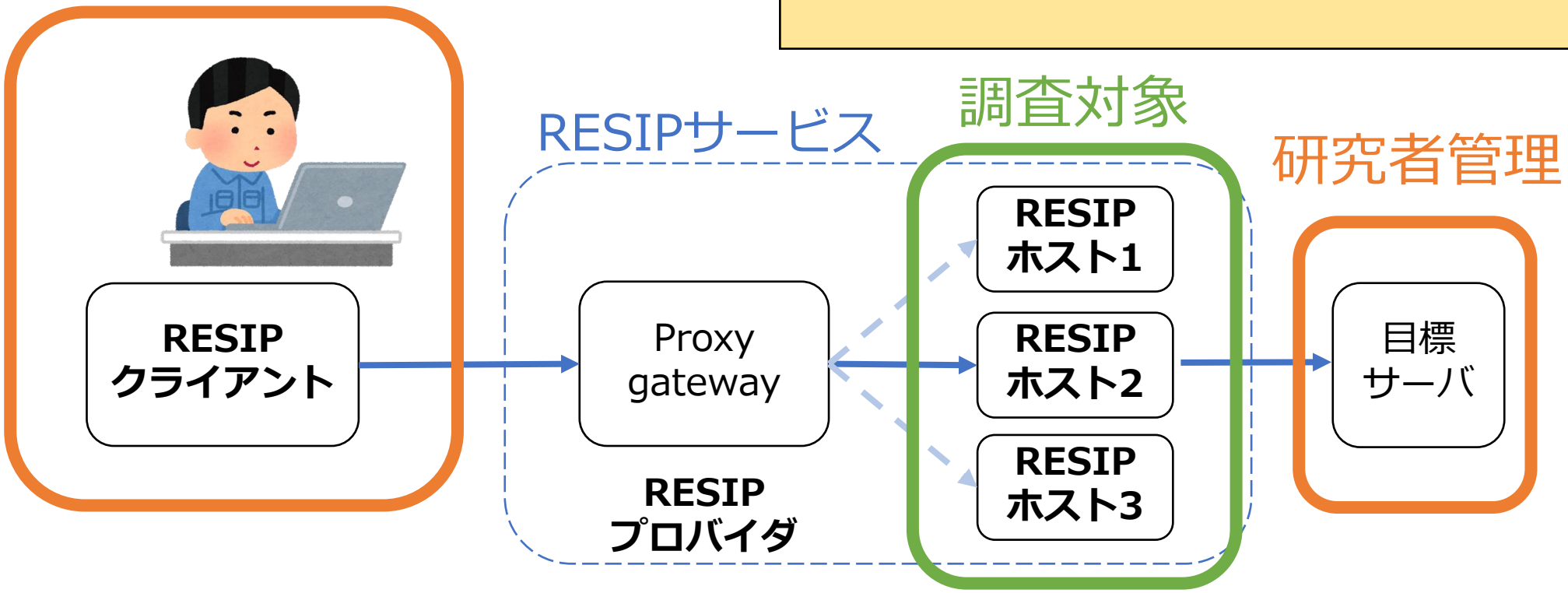
広告詐欺

https://brightdata.jp/ethical
（2023/1/17 閲覧）

問題点

◆ RESIPクライアントになった際の通信情報の調査[3][4] （半澤ら、住友ら）

一般のRESIPクライアントの行動が不明



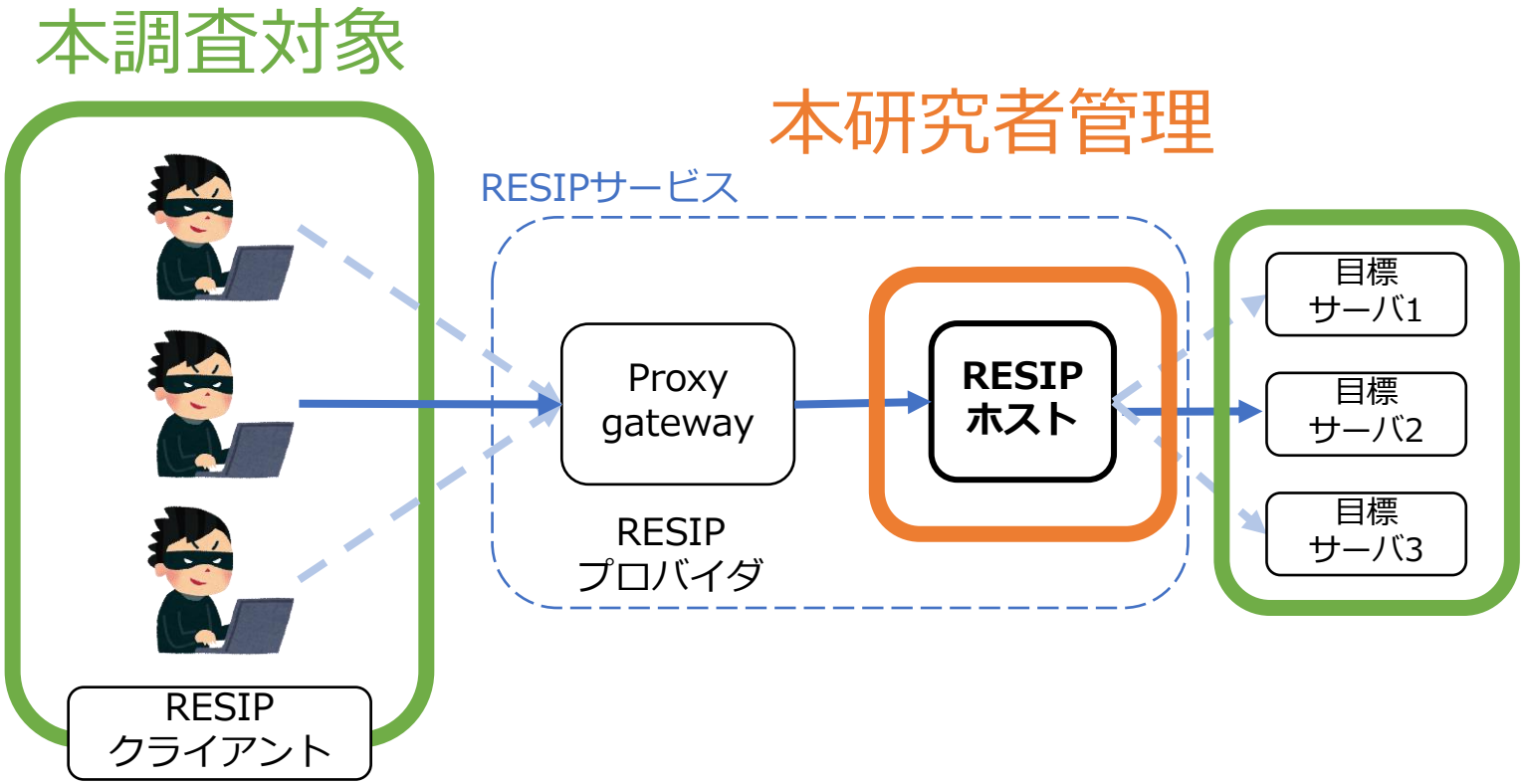
クエスチョン

- 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？

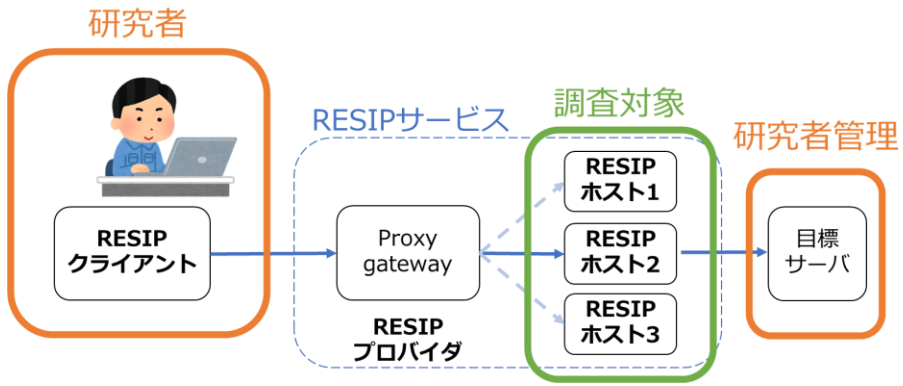
解決策

◆ 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



先行研究[3][4]



実験方法 (4.1 & 4.2 & 4.3)

◆ 実験１：RESIPホスト比較実験 (4.3.1)

- **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

◆ 実験２：RESIPホスト24時間観測 (4.3.2)

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

- ドメイン
- IPアドレス
- 通信時間分布 など

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 (4.4.1 & 4.5.1)

観測したIPアドレスとドメイン総数 (表 7, 表８)

	IPアドレス総数	ドメイン総数
Bright Data	645	430
Proxyrack	376	68
Oxylabs	95	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 (表 9)

	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 (表 11)

ドメインカテゴリ	Bright Data	Proxyrack	Oxylabs
Travel	5%	1%	2%
Shopping	13%	5%	4%
Advertisments	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 (4.5.2)

ドメインの悪性判定結果 (表 10)

	Bright Data	Proxyrack	Oxylabs	先行研究[2]
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

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**」

- 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

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 (4.5.3)

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アドレスを
変更可能（ボットの検出が困難）

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 ヵ月で中継可能な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**

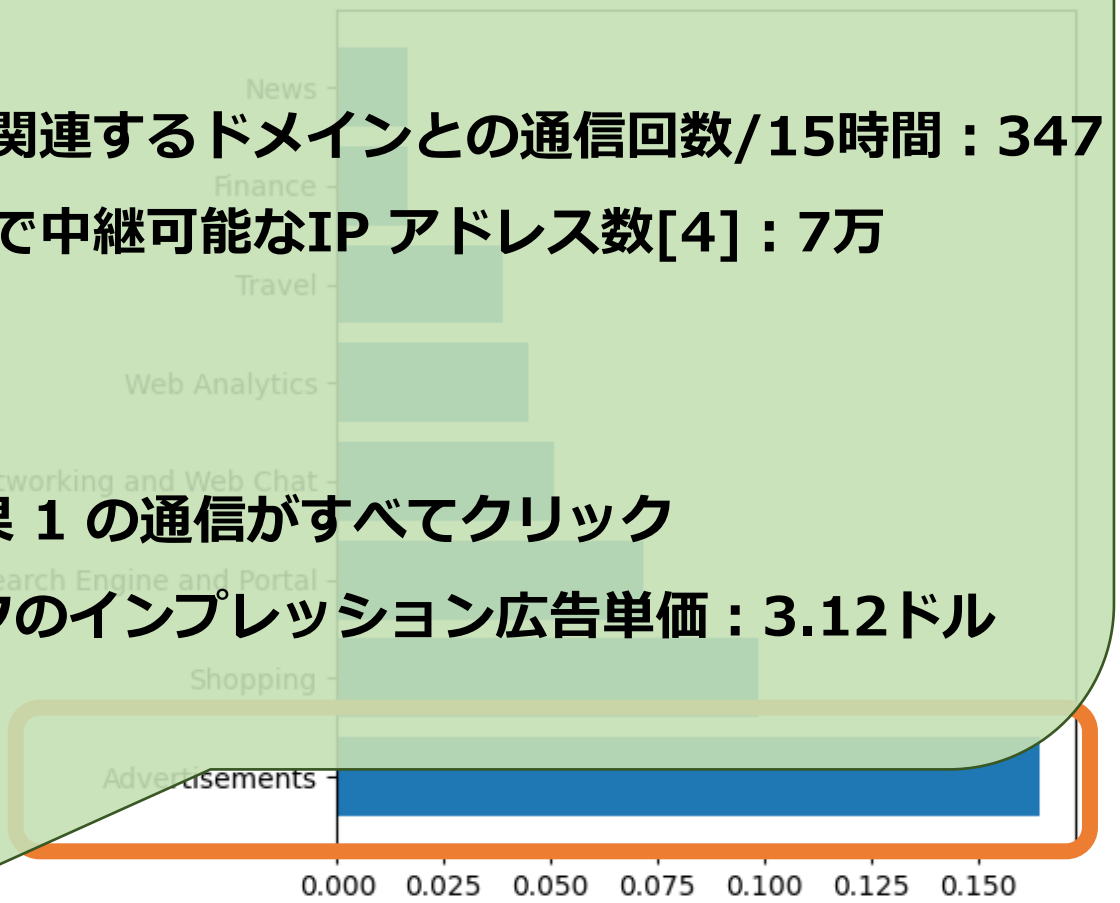


図 3 全通信のドメインカテゴリ割合

◆ **広告クリック詐欺の可能性**

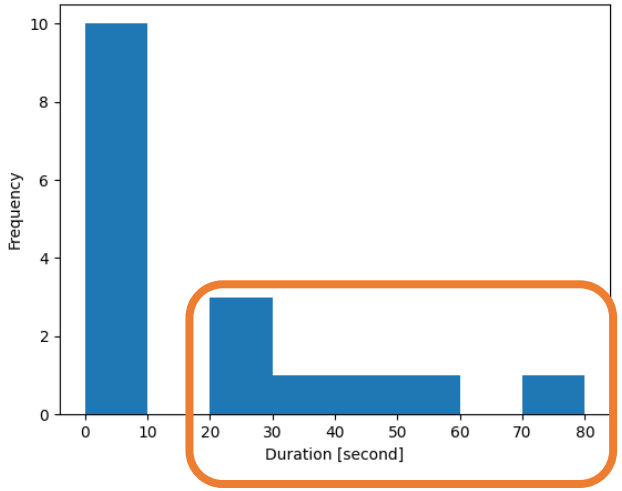
◆ **RESIP サービス全体での被害額**
3,637,670 ドルが見積もられる（1か月間）

マネタイズ (4.5.4)

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（図５）

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

結論

◆ 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