

明治大学総合数理学部

2022 年度

卒 業 研 究

ブロックチェーン **Ethereum** とマーケットプレイス **Magic Eden** での **NFT**  
取引の整合性の調査

学位請求者 先端メディアサイエンス学科

遠藤 冴花

# 目次

第 1 章	はじめに	2
第 2 章	Etherscan と Magic Eden	3
2.1	システム構成	3
2.2	Etherscan	4
2.3	Magic Eden	4
第 3 章	実験	5
3.1	目的	5
3.2	不整合の定義	5
3.3	使用プログラムと実験の流れ	6
3.4	実験結果	7
3.5	考察	7
第 4 章	おわりに	8
	参考文献	9
付録 A	ブラウザトラッキングにおける違法なサードパーティー cookie の調査	10
A.1	はじめに	10
A.2	準備	11
A.3	実験	13
A.4	おわりに	17
	参考文献	18

# 第1章

## はじめに

近年、暗号化した取引履歴を鎖のように繋いでいく技術であるブロックチェーン技術を利用した仮想通貨が注目を集めている。2008年に登場したビットコインをはじめとした様々な仮想通貨が用いられている中で2017年頃から特に注目されているものにNFTがある。NFT(Non-Fungible Token [非代替性トークン])は、デジタルアートをはじめとしたデジタル商品の唯一性とその所有者を保証することができるようになり、新しいマーケットプレイスとして浸透している。

NFTは公用分散型台帳ブロックチェーン技術を使用して取引の記録を確認することができる一方、その真正性は事業者にゆだねられている。そのため、取引を個人間で行うことから詐欺事件も発生している。2022年2月に最大手のNFTマーケットプレイスOpenSeaはユーザを狙ったフィッシング詐欺で300万ドルに相当するNFTの不正流出[1]があったことを公表している。

そこで、本研究では、NFT取引で主に使用されている通貨ETHの取引をブロックチェーンのエクスプローラとマーケットプレイスの2つのデータソースから観測し、取引が整合しているか調査を行い、NFT取引の信頼性を確認することを目的とする。

## 第 2 章

# Etherscan と Magic Eden

### 2.1 システム構成

本研究ではブロックチェーンエクスプローラーと NFT マーケットプレイスでの取引履歴をユーザごとに確認し、取引上の整合性を確認することを目的とする。システム構成図を図 2.1 に示す。

本研究ではブロックチェーンエクスプローラー Etherscan, NFT マーケットプレイス Magic Eden を調査する。

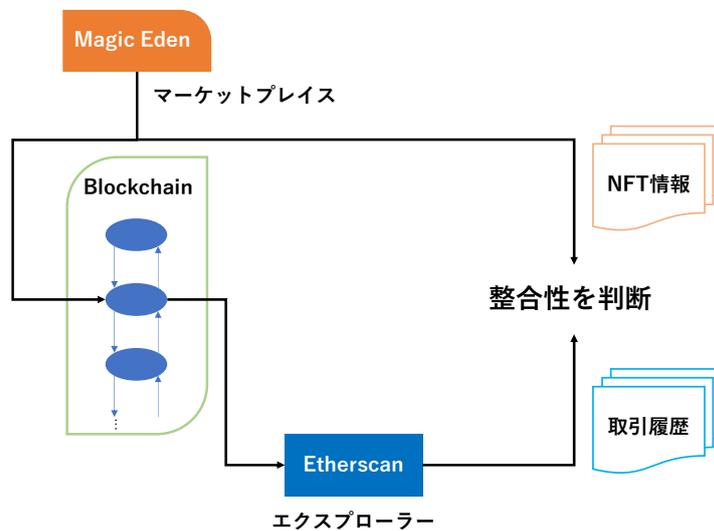


図 2.1 システム構成図

## 2.2 Etherscan

Etherscan はブロックチェーン Ethereum 上の NFT 取引で主に用いられている通貨である ETH でのやりとりの履歴を閲覧するサービスプラットフォームである。

NFT 取引で扱われている暗号資産は ETH が主流である。

## 2.3 Magic Eden

Magic Eden は多くある NFT マーケットプレイスの中の 1 つである。NFT の売買をするために利用するサービスのひとつで、Magic Eden は特にアートに分類される NFT の取引が活発である。

## 第 3 章

# 実験

### 3.1 目的

本実験は Etherscan と Magic Eden のユーザごとの取引データを集めて比較し、同じ取引が両方のデータに存在しているかを判別し、不整合が発生していないかを明らかにする。調査対象の Ethereum アドレスを表 3.1 に示す。

すべての取引データは公開されているので、マーケットプレイスの NFT データを照合することで、NFT の所有権を判断することができる。

### 3.2 不整合の定義

Magic Eden の取引履歴にあるが、Etherscan で確認できない取引と、その逆、すなわち、Ethereum のみにある取引を不整合と定める。不整合の割合を調査する。不整合率を Magic Eden での取引数の内、Magic Eden で確認されて Etherscan で確認できなかつた取引数の割合とする。式を図 3.1 に示す。

表 3.1 Ethereum アドレス一覧

	Ethereum アドレス
1	300d65b82c39ca315cbd8c26c9e20d2267f8edee
2	7dff47820fa7ef1c2eae54803b9c06a6fca40d
3	4749e63a25c34501bc579edcdaa364d3b2206073
4	1f8b5b6220eee763c60ac064da06fcd63533fd00
5	f81e01761184dcbf5e7475ea51e1dc497fdbc6ac
6	879f941bac811c379b2a0212f158d8ecbd741c91
7	40661c8a3c48f7f8ecac1f962a6ce8a1b7dc614c
8	d2c0c0cfbeb4a72042c53a31b863a29f9d7cdcd0
9	28f8969540165a0a0978d0ec62ae8c9dde843232
10	4c6686ed75d0c6685cc26fdab818cb975b5256e3

$$\text{不整合率} = \frac{\text{Etherscan} \times, \text{Magic Eden} \circ \text{の取引数}}{\text{Magic Edenでの取引数}}$$

図 3.1 不整合率の定義

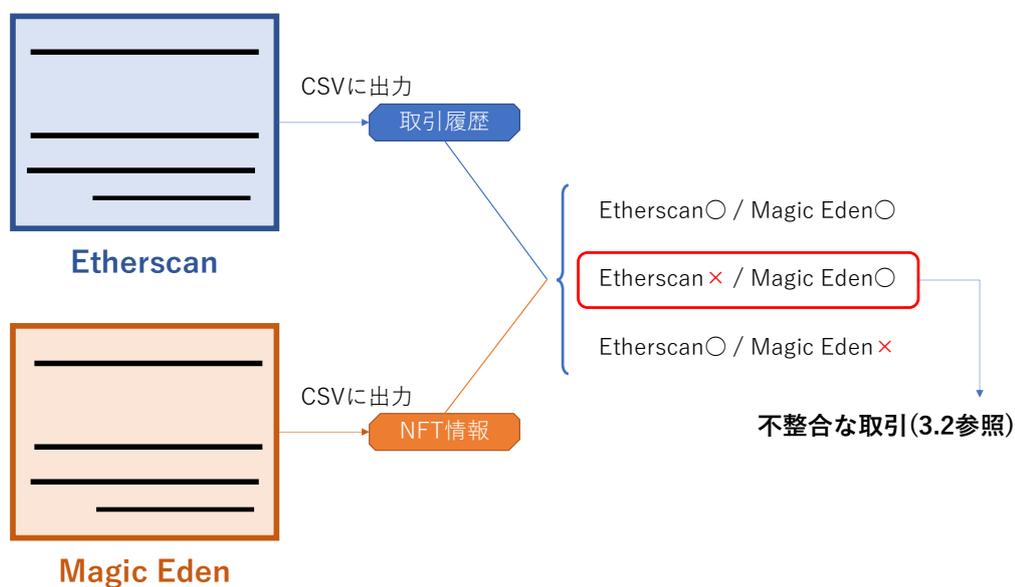


図 3.2 実験の流れ

### 3.3 使用プログラムと実験の流れ

本研究では、同様の実験を Opensea で行っている Yang Liyi のプログラム [2] を使用し行う。このプログラムは Magic Eden の NFT 取引情報を収集するために selenium webdriver を使用して、NFT 取引に使用されている Ethereum スマートコントラクトと Etherscan で確認できる NFTID の取得を行う。プログラムから得られたデータを csv に出力し、それらを比較し 3.2 で述べた不整合にあたる取引数を調査する。実験の流れを図 3.2 に示す。

表 3.2 観測された取引数

	Etherscan	Magic Eden	Eth ○ ME ×	Eth × ME ○
1	186	173	17	21
2	147	140	21	15
3	119	132	8	11
4	158	151	12	0
5	171	156	38	7
6	17	72	0	6
7	166	179	3	2
8	31	22	0	0
9	13	15	2	0
10	20	10	1	0
total	<b>1028</b>	<b>1059</b>	<b>102</b>	<b>62</b>

表 3.3 不整合率

	不整合率	Eth 未確認	ME・OS 取得数
Magic Eden	5.85%	62	1059
Open Sea	4.42%	32	724

### 3.4 実験結果

実験結果を表 3.2 に、本研究で不整合と判断したものの割合 (不整合率) を表 3.3 に示す。アドレスごとにトラザクション数に偏りはある。Etherscan で確認できたトラザクション数は 1028、Magic Eden で確認できたトラザクション数は 1059 である。不整合と定義される Magic Eden で確認でき、Etherscan で確認できなかったトラザクション数の合計は 62 である。結果から求められる不整合率は 5.85% となり、Open Sea と Etherscan で調査した [2] 不整合率は 4.42% となった。

### 3.5 考察

このように NFT マーケットプレイスで行われた取引の履歴がブロックチェーンエクスプローラーのほうで確認されない不整合率は Magic Eden と Open Sea での結果に大きな差がみられなかったことからほかのマーケットプレイスで同じ手法で調査した場合も同じような結果になるのではないかと予想する。マーケットプレイスが Etherscan 側に取引情報を送信したときに何かしらの原因、例えばトラザクション情報の送信のラグ等が考えられる。

## 第 4 章

# おわりに

実験結果から Magic Eden で購入した NFT の取引が Etherscan で確認できないものは約 5.85% あることが分かった。Opensea での不整合率は約 4.42% となり、ほぼ同量である。実際に不整合があるものを観測し、原因を直接確認する等でより高い精度を目指すことを今後の課題とする。

## 参考文献

- [1] THE BLOCK - Supposed 17-year-old artist sells \$138,000 worth of fake NFTs and disappears (<https://www.theblock.co/post/119150/supposed-17-year-old-artist-sells-138000-worth-of-fake-nfts-and-disappears>)
- [2] Yang Liyi, “ブロックチェーン Ethereum とマーケットプレイス OpenSea における NFT 取引の整合性の調査”, 2022 年度明治大学卒業論文, 2022
- [3] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system” (<https://bitcoin.org/bitcoin.pdf>), 2008.
- [4] G. Wood, “Ethereum: A secure, decentralised generalised transaction ledger” (<https://gavwood.com/paper.pdf>)
- [5] X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen, “A survey on the security of blockchain systems” Future Gener. Comput. Syst. 2017. (<http://dx.doi.org/10.1016/j.future.2017.08.020>.)
- [6] R. Matzutt, M. Henze, J. H. Ziegeldorf, J. Hiller, F. K. Wehrle, “Thwarting Unwanted Blockchain Content Insertion”, 2018 IEEE International Conference on Cloud Engineering (IC2E), pp.364–370,2018.
- [7] T. Sato, M. Imamura, K. Omote, “Threat Analysis of Poisoning Attack against Ethereum Blockchain,” Proc. WISTP2019,pp.139–154,Dec.2019.
- [8] 陳 浩太, 江村 恵太, 面 和成 “入札額の上限漏洩を防止した 資金拘束型の封印入札オークション”, コンピュータセキュリティシンポジウム 2021 論文集, 1124-1131, 2021-10-19

## 付録 A

# ブラウザトラッキングにおける違法なサードパーティー cookie の調査

### A.1 はじめに

近年インターネット上における広告への関心が高まってきている。2019年にはインターネットの広告費がテレビによる広告費を上回り、その額は2兆円にもものぼる [1]。これはユーザの検索履歴や年齢・性別といった属性などに連動して表示される広告や、SNSに表示される広告などが伸び続けた結果である。その上げ幅は6年間つづけて百分率で2桁の伸びとなっている。しかし、この広告を表示するときにユーザの履歴を取得して追跡することがプライバシー上の問題につながる可能性がある。

事業者は情報の収集のためにサードパーティー cookie を用いている。これに対し、Apple 社の標準ブラウザである safari は 2020 年にサードパーティー cookie をユーザの同意を取ることを義務づけている。Google 社は Chrome のサードパーティー cookie を 2023 年までに段階的に規制していくと公表している [3]。

そこで、本研究ではサードパーティー cookie の利用実態を調査し、違法性が認められるものの割合を明らかにすることを目的とする。しかし、その為には多様な cookie を取得する必要がある、人手で大規模なサイトを調べるのは困難である。そこで、本研究は OpenWPM に注目する。本ツールを用いて、自動でブラウザ上の cookie 収集を可能とする。500 サイト分のデータを自動で取得する。違法性は明確な指標はないため本研究では独自の定義で調査し、その精度を報告する。

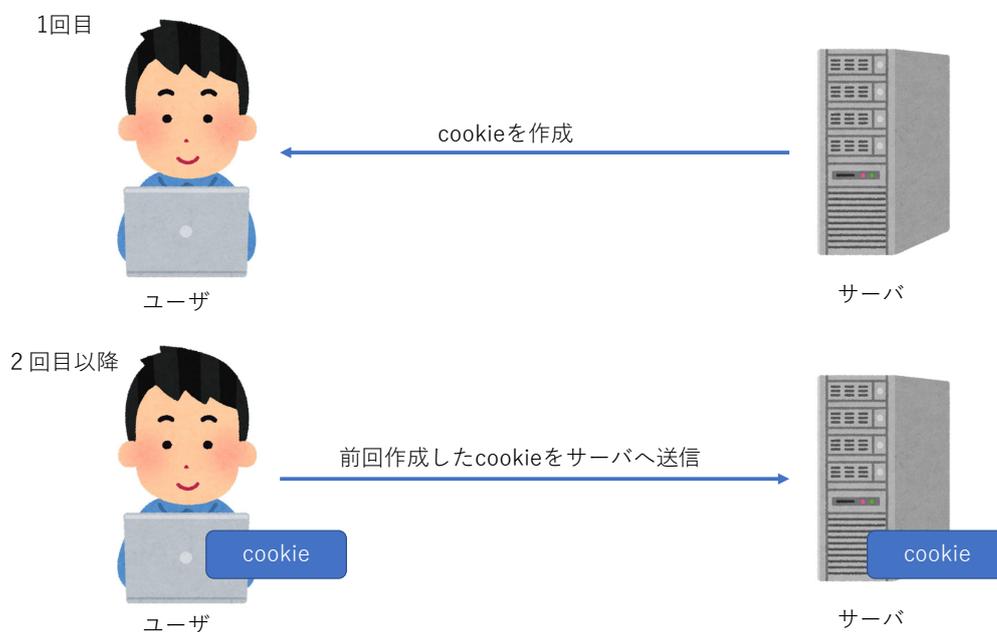


図 A.1 cookie の概要図

## A.2 準備

### A.2.1 サードパーティー cookie

本研究で調査するサードパーティー cookie の概要を図 A.1 に示す [2]. cookie はブラウザ上に保存されるユーザの情報のことで、特定のウェブサーバにアクセスしたときに cookie 内にある情報をそのサーバに送る。これによって一度アクセスしたことのあるサイトに再度アクセスし、ログイン等をしようとするとき自動的に情報を補完してくれる。主にユーザ情報やショッピングサイトにおけるカート内の商品情報などを格納している。cookie は、ファーストパーティー cookie とサードパーティー cookie の 2 つ種類がある。この 2 つの違いを図 A.2 に示す。ファーストパーティー cookie はサーバにアクセスしている時しか読み出せず、サードパーティーのサーバからはアクセスできない。そこで、iframe や画像などを用いてサードパーティーのコンテンツを埋め込み、ユーザのサイトをまたいだ行動を追跡し、ユーザの情報、検索履歴などを得ている。これがプライバシー保護の観点から問題視されている。

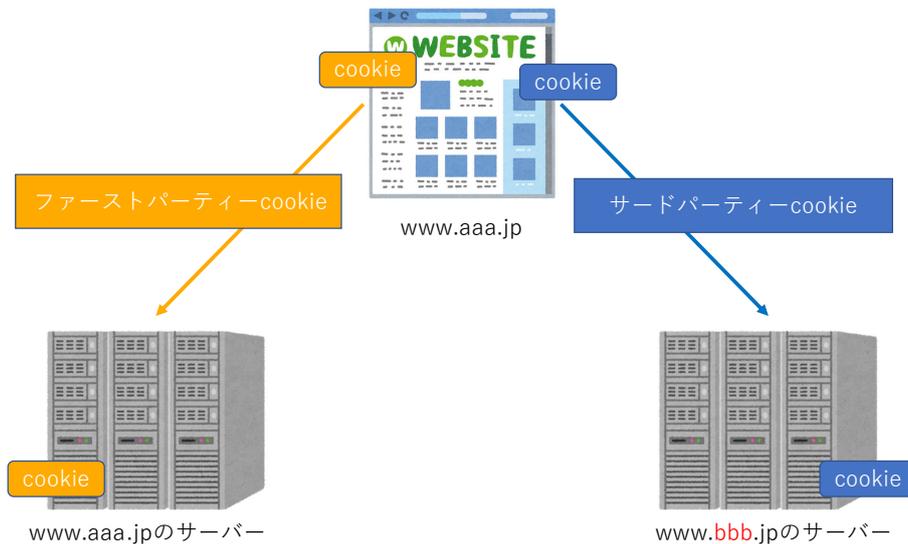


図 A.2 サードパーティー cookie とファーストパーティー cookie の違い

## A.2.2 自動クロールツール OpenWPM

cookie 情報を自動的に得るために OpenWPM を使用する。OpenWPM はプリンストン大学で行われた cookie 調査の先行研究の中で開発された自動的にクロールを行うツールである [6]。OpenWPM の機能概要図を図 A.3 に示す。OpenWPM はサイトのクロールを自動的に行い、取得した情報をデータベースで管理する。

OpenWPM で得られるデータ内容を表 A.1 に示す。本研究では cookie に関連する Javascript.cookie のテーブルのデータベースを集計する。本テーブルのスキーマを A.2 に示す。

## A.2.3 違法性の定義

javascript\_cookies のテーブル内の javascript\_cookies\_host 列(cookie を埋め込んだホスト)と site\_visit\_site\_url 列(ブラウザがアクセスしているサイト)に同じ文字列を含んでいるものを合法、それ以外を違法なサードパーティー cookie と定義する。判定の例を図 A.5 に示す。

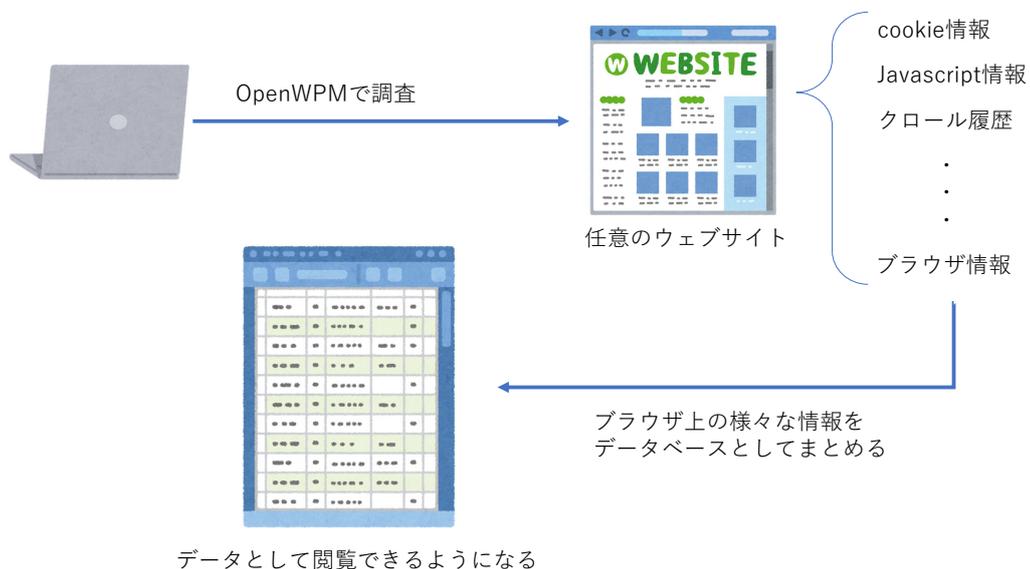


図 A.3 OpenWPM 概要図

## A.3 実験

### A.3.1 実験目的

主要なウェブサイト上の違法なサードパーティー cookie の割合を求め、インターネット上の cookie の安全性を調査することを目的とする。また、提案する違法なサードパーティー cookie を判別する手法の精度も明らかにする。

### A.3.2 OpenWPM を使用した cookie 調査

本実験では OpenWPM を使用し cookie を計測する。"TOP500"[5] に掲載されているサイトを調査対象とし、国内国外の有名サイト 450 サイトを選ぶ。消費者庁から公開されている悪質な海外ウェブサイト一覧 [4] から 50 サイトを加えて、計 500 サイトに対してクローリングを行う。500 サイトの例を表 A.3 に示す。

OpenWPM とともに配布されている demo.py を実行する。demo.py は指定したドメインへアクセスし、そこで得た情報を sqlite にまとめて出力する。これを利用し違法なサードパーティー cookie 数を調査する。実験概要図を図 A.4 に示す。

表 A.1 Open WPM のデータ

	テーブル名	説明
1	callstacks	不明
2	crawl	クローリングを始めたタイミングの記録
3	crawl_history	クローリングの履歴
4	dns_responses	DNS サーバーからの応答
5	http_redirects	HTTP リダイレクトで変更された URL
6	http_requests	クライアントが要求した HTTP
7	http_responses	サーバが返した HTTP
8	incomplete_visits	不明
9	javascript	Javascript の情報
10	javascript_cookies	cookie の情報
11	navigations	サイト上にあるナビゲーションの情報
12	site_visits	訪れたサイトの URL と ID の情報
13	sqlite_sequence	各テーブル最後の連番情報
14	task	不明

表 A.2 javascript\_cookies の列内容

	列名	説明	値の例
1	visit_id	ブラウザ毎に発行される id	33774826310247(youtube)
2	extension_session_uuid	一意な識別子	de86fc9c...6eef
3	expiry	cookie の有効期限	2021-11-06T12:01:47.000z
4	host	cookie の URL	.youtube.com
5	name	cookie の名前	GPS
6	value	cookie の値	true
7	time_stamp	データを取得した日時	2021-11-06T11:31:47.742Z

### A.3.3 cookie 数とサードパーティー cookie における誤差の評価

表 A.4 に 500 サイトに存在した cookie 数と違法なサードパーティー cookie の数とその割合を示す。500 サイトに存在した cookie の総数は 37051 でその中で違法なサードパーティー cookie と判定されたものは 19052 あり、割合としては約 52 %である。また 50 サイトの悪質なウェブサイトの cookie を調べてみると 106 とかなり少なく、その中身は約 25 %が違法なサードパーティー cookie と判定された。これは広告などを自サイトで行っているからだと考えられる。表 A.5 に提案した違法なサードパーティー cookie を見分ける手法の精度を示す。500 サイトからランダムにサンプリングした 5 サイトの精度を測定した。結果は 84.7 %の精度だった。誤差の原因はドメインが異なるが同一法人の下で取得されている cookie を違法と判定してしまうことと考えられる。例えば、この定義だと Youtube のサイトにアクセスしたときに存在する Google の cookie を違法と判定してしまうが、実際は違法ではない (Youtube は Google に買収されているため)。

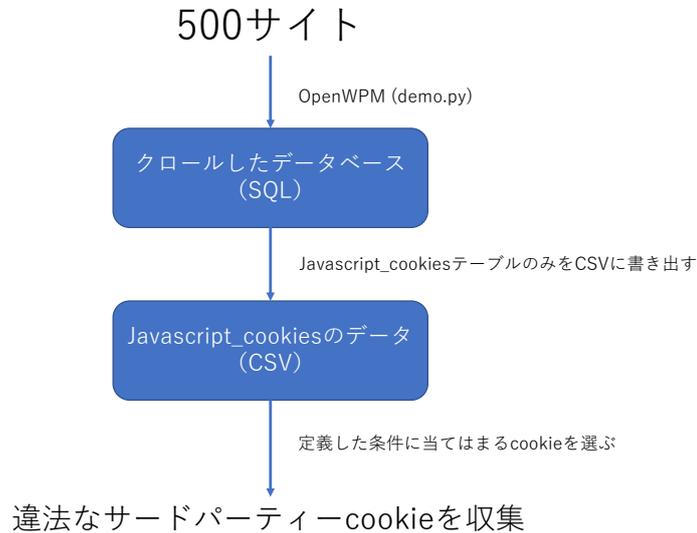


図 A.4 実験概要図

表 A.3 調査 500 サイトの一部

	ドメイン名
1	https://www.youtube.com/
2	https://www.google.com/
3	https://www.apple.com/
:	:
498	http://www.balenshop.jp/
499	http://www.gctokyo.com/
500	http://www.gucciclub.tokyo/

#### A.3.4 450 サイトと 50 サイトのサードパーティー cookie 数に関する考察

調査結果から悪質なサイトである 50 サイトに存在していたサードパーティー cookie の数は他 450 サイトの割合と比較しかなり低かったことが分かった。これは当初の仮定とは反対の結果になった。理由として考えられるのはサードパーティー cookie の目的であるユーザーの情報の取得・広告の最適化を行う必要が無いからだと考えられる。悪質なサイトの広告枠は全体的にファーストパーティ cookie、つまり自サイトで完結して



図 A.5 判定方法

表 A.4 cookie の調査結果

	総 cookie 数	平均	違法 cookie 数	割合 [%]
一般サイト 450	36945	82.1	19475	52.7
違法性のあるサイト 50	106	6.8	27	25.5
全サイト	37051	74.1	19502	52.6

いるものが多かった。

表 A.5 精度の検証結果

ドメイン名	OpenWPM を用いた場合（本実験での手法）	手動で調査した場合（真値）	OpenWPM による違法 cookie の精度 [%]	相対誤差
https://www.mozilla.org/ja/	0	0	100	-
https://www.linkedin.com/	20	17	85	0.15
https://www.adobe.com/	37	31	83	0.19
https://www.cloudflare.com/hp/	5	0	0	-
https://www.microsoft.com/ja-jp/	69	63	91	0.10
	131	111	84	0.18

## A.4 おわりに

本実験では 500 サイトを対象に cookie の調査を行った。調査した cookie の約 52 %が違法の可能性があること。

今後は OpenWPM の機能をよく理解し、javascript.cookies の情報以外を用いることを今後課題とする。

## 参考文献

- [1] 電通, ”2020 年 日本の広告費” (<https://www.dentsu.co.jp/news/release/pdf-cms/2021012-0225.pdf>), 閲覧日時 2021.12.12
- [2] 総務省, ”Cookie の仕組み” ([https://www.soumu.go.jp/main\\_sosiki/joho\\_tsusin/security\\_previous/kiso/k01\\_cookie.htm](https://www.soumu.go.jp/main_sosiki/joho_tsusin/security_previous/kiso/k01_cookie.htm)), 閲覧日時 2021.12.12
- [3] 西正広, ”サードパーティ cookie とは? Apple ・ Google の規制による影響を解説”, 閲覧日時 2021.12.12 (<https://moltsinc.co.jp/data-strategy/9987/>)
- [4] 消費者庁, ”悪質な海外ウェブサイト一覧” ([https://www.caa.go.jp/policies/policy/consumer\\_policy/international\\_affairs/assets/consumer\\_policy\\_cms105\\_210701\\_01.pdf](https://www.caa.go.jp/policies/policy/consumer_policy/international_affairs/assets/consumer_policy_cms105_210701_01.pdf)), 閲覧日時 2021.8.20
- [5] TOP500site, TOP500 The List. (<https://www.top500.org/>), 閲覧日時 2021.8.20
- [6] Steven Englehardt and Arvind Narayanan, ”Online Tracking : A 1-million-site Measurement and Analysis”, ACM CCS 2016, pp.1388-1401, 2016
- [7] Adam Lerner, Anna Kornfeld Simpson, Tadayoshi Kohno, and Franziska Roesner, University of Washington Internet Jones and the Raiders of the Lost Trackers: An Archaeological Study of Web Tracking from 1996 to 2016,25th USENIX Security Symposium August 10–12, 2016 Austin,TX
- [8] 西林孝, 株式会社 VOYAGE GROUP, アドネットワークにおける広告配信計画の最適化, 人工知能,2017 年 32 巻 4 号 p487-493