Webトラッキング技術に関する対策技術の検証及び考察

小芝 力太[1]　田邉 一寿[1]　細谷 竜平[1]　野田 隆文[1]　齋藤 孝道[2]

概要：現在，スーパークッキーやブラウザフィンガープリンティングなどの Web トラッキング技術が発展し続けている．Web トラッキング対策としてはクッキーの削除やプライベートブラウジングの利用だけでは効果が低い可能性がある．考えられる Web トラッキング対策として，通常ブラウザの履歴の削除，ブラウザ拡張機能の利用，プライベートブラウジングの利用，Tor ブラウザの利用が挙げられるが，実際の効果については調査が必要であると考える．本論文では，上記 4 つの対策が，Web トラッキング技術に対してどの程度の効果があるかの調査を行った．その結果，対策技術によって有効性に差異が存在することが明らかになった．

キーワード：スーパークッキー，ブラウザフィンガープリンティング，トラッキング対策技術，Web 技術

On Study of Anti Web Tracking Technologies

Rikita Koshiba[1]　Kazuhisa Tanabe[1]　Ryohei Hosoya[1]　Takafumi Noda[1]　Takamichi Saito[2]

Abstract: Currently, Web tracking technologies such as supercookie and Browser Fingerprinting continue to be evolved. It might be not enough that deletion of HTTP cookie or use of private browsing as counter against the Web tracking technologies. For Anti Web tracking, there are 4 methods such as, deletion of history of browser, use of browser extension, use of private browsing, and use of Tor Browser, but the actual effect has not been unveiled. In this paper, we investigated the effect of the four methods as anti Web tracking technology. As a result, it concluded that there are differences in effectiveness depending on countermeasure method.

Keywords: Supercookie，Browser Fingerprinting，Anti Web Tracking Technology，Web Technology

1. はじめに

2012 年に行われた調査 [13] によると，Alexa ランキングトップ 500 のサイトの内，79%のサイトにおいて，DMP（Data Management Platform）事業者によるトラッキングが確認されたとのことである．その一方で，2017 年実施の調査 [5] によると，クッキーの 64%がブロックまたは削除されていたことがわかった．特に，モバイルでの拒否率は 75%であるとのことである．

しかし，スーパークッキーと呼ばれるブラウザ記憶機構を複数利用した技術や，ブラウザフィンガープリンティングと呼ばれる Web サイトにアクセスしてきた端末のブラウザを識別する技術が考案され，クッキーの削除だけではトラッキングを回避できない可能性がある．

本論文では，スーパークッキー及びブラウザフィンガープリンティングへの対策技術について調査及び実験を行い，2018 年現在における実情を調べた．具体的には，スーパークッキー及びブラウザフィンガープリンティングの対策として考えられる 4 つの対策として，通常ブラウザの履歴の削除，ブラウザ拡張機能の利用，プライベートブラウジングの利用，Tor ブラウザの利用を挙げ，それぞれを調査した．その結果，各対策技術におけるトラッキング対策としての有効性に差異が存在することが明らかになった．

[1] 明治大学大学院
Graduate School of Meiji University
[2] 明治大学
Meiji University

2. 背景知識

2.1 スーパークッキー

スーパークッキーとは，クッキーとは異なるブラウザの保存領域にデータを保存及び読み出しを行う仕組みである．クッキーとは異なる保存領域にデータが格納されるので，ブラウザが提供する履歴の削除機能を用いただけではデータが削除されない場合があり，クッキー削除後も引き続きトラッキングされる可能性がある．

スーパークッキーにはいくつか種類があるが，本論文ではクッキー削除後にブラウザを閉じた後もブラウザにデータとして残留することがわかった 7 個についてのみ扱う．

各スーパークッキーの仕組みを説明する．なお本論文では，各スーパークッキーを括弧内で記述されている略記で以降取り扱う．

HTML5 Local Storage (Local) Web Storage の 1 つ．機能はクッキーと類似しているが保存容量が大きく半永久的にデータを保存できる．localStorage プロパティ [2] の setItem メソッドでブラウザに保存を行い，getItem メソッドで読み込む．

RGB values in PNG images (PNG) HTML5 の Canvas ピクセルに関する情報．PNG 画像が所有している RGB の値を指す．

HTTP ETag (ETag) HTTP におけるキャッシュの有効性を確認するための手段の 1 つ．URL から得られるリソースに対する明確ではない識別子でサーバがレスポンスを送信するときに HTTP ヘッダの ETag フィールドにセットされる．キャッシュの効率化や回線帯域の節約に繋がる機能を備える．

Web cache (Cache) ブラウザが表示した Web ページや画像などのデータをブラウザに一時的に保存する仕組み．同一 Web サイトに再びアクセスする時，キャッシュを読み込むことでページの表示時間を短縮できる．

Database Storage via SQLite (DB) window オブジェクトの openDatabase メソッド [3] を用いてローカルデータベースに接続し，SQL 文によりデータベースを操作するための仕組み．Chrome や Safari など一部のブラウザでサポートされている．

IndexedDB (IDB) ファイルなどの構造化された多くの情報を保存するクライアントサイドの API．JavaScript ベースのオブジェクト指向データベースでデータの検索にインデックスを使用する．

HSTS スーパークッキー (HSTS) HSTS(Hypertext Strict Transport Security) の仕組みを使いブラウザの記憶領域に情報を記憶させる手法の 1 つ．HSTS とは，ブラウザからのリクエストに対するレスポンスに HSTS ヘッダを Web サーバが付加することで，次回以降ブラウザがそのドメインに HTTP でアクセスしたとき，内部で HTTPS にリダイレクトするように強制させる仕組みである．HSTS ヘッダはドメイン単位，もしくはサブドメイン単位で設定することができる．初回アクセス時には，複数用意したサブドメインに対して HSTS ヘッダの設定の有無を調節してリクエストを作成する．これによりブラウザは HSTS ヘッダが付加されたサブドメインをブラウザ上に記憶する．次回以降，ブラウザは初回のアクセス時に HSTS ヘッダが付加されていたサブドメインに対してのみ HTTPS でアクセスすることになる．このアクセスを観察することで，サーバはブラウザからビット列の情報を取得できるようになる．

2.2 ブラウザフィンガープリンティング

特徴点の組み合わせによって端末内のブラウザを識別する手法をブラウザフィンガープリンティング（以降，フィンガープリンティングと呼ぶ）という．最も初期のフィンガープリンティングの研究は Eckersley [7] であり，それ以降も多くの関連研究が行われている．

フィンガープリンティングに使用する特徴点の値[*1]の組み合わせをブラウザフィンガープリント（以降，フィンガープリントと呼ぶ）という．これには，IP アドレスや HTTP リクエストヘッダから採取可能な UserAgent 文字列と，JavaScript の実行によって得られる画面解像度（window.screen）などがある．

3. フィンガープリンティング対策技術に関する研究

FireGloves [1] は，Boda らによって開発された，利用者のフィンガープリントを，Web サイトにアクセスするたびに本来とは異なる値に変更する Firefox 用拡張機能である．アクセスごとにフィンガープリントを変更することで，識別される可能性が低くなる．

PriVaricator [12] は，Nikiforakis らによって提案された，フィンガープリントをランダム化する対策技術である．この対策技術は Chromium ブラウザを用いて実装されている．ランダム化の方針として，2 つの性質を満たしていることが示されている．1 つは結びつけることが困難なフィンガープリントを生成すること，もう 1 つは既存の Web サイトの表示を崩さないことである．しかし，ランダム化を行う特徴点はプラグインとフォントのみであり，他の特徴点のランダム化はできていない．また，フォントに関しては CSS による採取のみを対策しているので，Flash や Canvas を用いた手法の対策ができていない．

Blink [11] は，Laperdrix らによって提案された，仮想化

[*1] 特徴点：IP アドレス，フィンガープリント：192.168.1.1 など

技術を用いたフィンガープリンティング対策技術である．利用者がWebサイトへアクセスするときに，Blinkによって構築された複数の仮想環境を使い分けることでフィンガープリントをランダム化できる．この対策技術の強みは，フィンガープリントを加工すること無く，本来のプラットフォームからフィンガープリントを採取しているので，対策技術を取り入れていることを検知されにくい点である．しかし，Blinkは数百ものプラットフォームを一度に利用しリソースを逼迫するので，スペックの低いマシンでの利用は見込めない．

FPGuard [8] は，FaizKhademiらによって提案されたフィンガープリンティング対策技術である．この対策技術は，Chromiumブラウザと Chrome拡張機能の組み合わせにより実現され，フィンガープリンティングの検知と対策の両方を行う．FPGuardはハードコードされたヒューリスティックによりフィンガープリンティングを検知し，複数回アクセス時のフィンガープリントのランダム化を行う．しかし，ランダム化には利用者の承認を求める仕組みとなっており，信頼できるWebサイトであるかどうかの判断ができない利用者が誤って，偽装されていないフィンガープリントを送信してしまう可能性がある．また，Flashによるフィンガープリンティングの対策として，Flashの機能を止めることが提案されているが，これによってFlashを利用しているWebサイトのデザインが崩れてしまう．

FP-Block [14] は，Torresらによって提案されたフィンガープリンティング対策技術である．この技術は異なるドメイン間でのトラッキングを対策し，同一ドメインでのトラッキングを許可することを目的として提案された．FP-BlockはFirefoxのプラグインとして実装されており，Webサイトアクセス時にフィンガープリントを送信するHTTPリクエストなどの通信をインターセプトし，ドメインごとに異なるフィンガープリントを送信する仕組みとなっている．しかし，FP-Blockは，特徴点の偽装をWebサイトに検知されてしまう可能性がある．

Disguised Chromium Browser（以降，DCBと呼ぶ）[6] は，Baumanらによって提案されたフィンガープリンティング対策技術である．この対策技術は，Chromiumベースのブラウザとして実装されており，検知されにくく，ユーザビリティを損なわない対策手法を提案している．DCBの戦略として，‘1:N’と‘N:1’という2つの手法が紹介されている．‘1:N’は，1つのブラウザが，複数（N個）の種類のフィンガープリントを提供することである．これにより，Webサイト側は1つのブラウザによる複数回アクセス時にそのブラウザをトラッキングすることが困難となる．‘N:1’は，複数 (N個) のブラウザが，1種類のみのフィンガープリントを提供することである．これにより，Webサイトは複数のブラウザを識別することが困難となる．また，DCBには端末から採取したフィンガープリントがデータベースに蓄積されており，Webサイトにアクセスするときは，そのデータベースに格納されているフィンガープリントを利用することで，利用者が対策手法を導入していることを検知されないようにしている．

FPRandom [10] は，Laperdrixらによって提案されたフィンガープリンティング対策技術である．この対策技術では，ユーザビリティを維持しつつ，特にCanvasフィンガープリントやAudio Contextフィンガープリントをランダム化する手法を提案している．Canvasフィンガープリンティングに関しては，Canvasの描画時にRGBの値を均等に増加及び減少をさせることで，ランダム化を行っている．Audio Contextフィンガープリンティングに関しては，AudioContext APIによって出力される音量を僅かに下げることで，ランダム化を行っている．

4. 既存の対策技術

4.1 ブラウザの履歴データの削除

ブラウザには，保存しているクッキーやキャッシュ，フォームへの入力履歴を削除するための機能（以降，ブラウザの履歴削除機能という）が搭載されている．ブラウザの履歴削除機能では，複数ある削除項目を選択することでその項目に対応する保存情報を削除できる．

4.2 トラッキング対策のブラウザ拡張機能

ブラウザには，ブラウザの基本機能を拡張するための仕組みとして，拡張機能がある．プライバシー対策を行う拡張機能として，サードパーティによるトラッキング防止機能，広告やスクリプトをブロックしWebの動作を向上させるもの，Do Not Trackを送信するもの，フィンガープリントを偽造する機能などが挙げられる．

4.3 プライベートブラウジング

プライベートブラウジングは，複数の利用者が同一の端末を利用する場合に，利用後当該ブラウザウィンドウを閉じることで利用者の情報が削除される機能である．ブラウザによって機能の差異はあるが，主に以下の2つの機能を有する．

(1) Webページの閲覧履歴，フォームへの入力情報をブラウザに保存しない
(2) クッキーやWebサイトのデータをブラウザ使用中にのみ保存し，ブラウザが閉じられたときに削除する

4.4 Torブラウザ

Torブラウザとは，TCP/IPにおける通信経路の匿名化を行うTorネットワークを使用するように設計されたFirefoxベースのブラウザである．

Torブラウザでは IPアドレスを匿名化するだけでなく，フォントリストや UserAgent 文字列，Canvas フィンガー

プリントを固定化することで対策する．

5. 調査実験

5.1 調査したシステム環境

実験を行うにあたり，StatCounter[4] が公表しているブラウザ及び OS のシェアを参照し，実験に使用するシステム環境を選定した．表 1，表 2 は 2018 年 7 月現在の日本，世界の全プラットフォームにおける主要なブラウザ及び OS のシェアである．表の-はそのシェアが極めて低い理由から StatCounter が公表していないものを示す．

表 1 日本，世界の全プラットフォームにおけるブラウザのシェア

	Chrome	Safari	IE	Firefox	Edge	UC Browser	Opera
日本	41.96%	31.83%	11.50%	6.63%	4.29%	-	-
世界	58.94%	13.70%	3.12%	5.17%	-	7.46%	3.50%

表 2 日本，世界の全プラットフォームにおける OS のシェア

	Windows	iOS	macOS	Android	Linux
日本	41.74%	27.43%	15.30%	11.76%	0.40%
世界	35.93%	12.82%	5.39%	42.26%	0.77%

表 1 から，UC Browser を除く 6 つのブラウザと Tor ブラウザを選定した．UC Browser がデフォルトで備えるブロック機能によりスーパークッキー採取サイトにアクセスできないので対象から外した．また，表 2 から，シェアの高い上位 4 つの OS を選定した．以上により選定したブラウザと OS のバージョンを表 3 に示す．

各 OS の端末情報は以下の通りである．

- Windows:Windows 8.1 64-bit，Windows 10　64-bit（Edge 使用時に利用）
- macOS:Mac OS X 10.13.6 64-bit
- iOS:iPhone8，11.4（15F79）
- Android:Android（Android8.0.0;SH-01K Build/S6151）

なお，表 3 の iOS 版 Opera は Operamini を，iOS 版の Tor は Onion Browser を，Android 版の Tor は Orfox をそれぞれ使用した．

5.2 スーパークッキーに関する実験

5.2.1 スーパークッキー採取サイト

本論文では Samy Kamkar 氏の Web サイト [9] を参考にスーパークッキーを採取する Web サイト（以降，スーパークッキー採取サイトと呼ぶ）を構築し実験をした．

利用者がスーパークッキー採取サイトに初めてアクセスしたとき，スーパークッキー採取サイトは各スーパークッキーに対して，識別子として生成した乱数（以降，UID と呼ぶ）を保存する．2 回目以降のアクセスでは各スーパークッキーを読み出し，初回アクセス時に保存された UID が残留するか確認する．

5.2.2 各 OS とブラウザのスーパークッキー対応状況

表 4 に 2.1 節で列挙したスーパークッキーの対応状況を OS とブラウザごとに示す．なお，その性質上，1 つでもスーパークッキーが対応する場合をトラッキング可能とする．また，表記の都合上 Windows を W，macOS を M，iOS を I，Android を A としている．表の○はスーパークッキーを対応していることを，-は対応していないことを，△は括弧内に記載された OS が対応していることを示している．また表 4 の HSTS では初回アクセス時と 2 回目のアクセス時に異なる UID が確認できたものを対応するとした．

表 4 から同一ブラウザでも，OS によって対応するスーパークッキーに違いがあることがわかった．また，ブラウザによって対応するスーパークッキーにも違いがある．

5.3 フィンガープリントに関する実験

5.3.1 フィンガープリント採取サイト

フィンガープリントを採取する Web サイト（以降，フィンガープリント採取サイトと呼ぶ）を用意し，アクセスした端末のフィンガープリントを採取した．採取したフィンガープリントは，それと紐付けて生成したクッキー（以降，UID と呼ぶ）と併せて，フィンガープリント採取サイトのデータベースに保存され，同一端末のブラウザからのアクセスであることを判定する．

実験では，対策技術を使用した場合と使用していない場合におけるフィンガープリントを比較し，フィンガープリントが変化した場合，トラッキング対策の観点における有効性があると判断する．

5.3.2 フィンガープリントに用いる特徴点の選定

我々の先行研究 [15] 結果より，識別の精度が最も高くなる特徴点の組み合わせの 18 個を選定した．

5.3.3 拡張機能の選定

拡張機能の選定にあたり，フィンガープリンティング対策を陽に示すものがなかったので，プライバシー対策を行うブラウザ拡張機能から選んだ．

本節の実験では，利用者が主に拡張機能を使用するとされている 3 つのブラウザ（Chrome，Firefox，Safari）で実験をした．Safari での実験を行うために OS は macOS とした．

拡張機能選定の基準は以下の通りである．

(1) Firefox，Chrome:キーワード検索で「Fingerprint」，「Tracking」に該当し，トラッキング防止の有効性があると判断でき，評価が 4.0 以上かつ利用者数が上位 5 位以内のものを各キーワードで 5 個ずつ選定した．
(2) Safari:キーワード検索で「Fingerprint」に該当するものはなかった．よって，「Tracking」で該当した 18 個のうち，トラッキング防止の有効性があると判断でき

表 3　調査実験に用いたブラウザと OS のバージョン

	Chrome	Safari	IE	Firefox	Opera	Edge	Tor
Windows	65.03325.181	-	11.112.17134.0	61.01	54.0.2952.60	42.17134.1.0	7.5.6
macOS	67.0.3396.99	11.1.2(13605.3.8)	-	61.01	54.0.2952.60	-	7.5.6
iOS	67.0.3396.87	604.1	-	12.1(10941)	16.0.11	42.3.4	2.1.0
Android	67.03396.87	-	-	61.0	46.3.2246.127744	42.0.0.2059	7.5.1

表 4　各 OS とブラウザのスーパークッキー対応状況

	Chrome	Safari	IE	Firefox	Opera	Edge	Tor
対応 OS	W, M, I, A	M, I	W	W, M, I, A	W, M, I, A	W, I, A	W, M, I
Local	○	○	○	○	○	○	○
PNG	○	○	○	△ (I)	○	○	△ (I)
ETag	○	○	-	○	○	○	○
Cache	○	○	○	△ (I)	○	○	-
DB	○	○	-	△ (I)	○	△ (I, A)	△ (I)
IDB	○	○	○	○	○	○	△ (I)
HSTS	△ (W, M, A)	-	-	△ (M)	△ (W, M, A)	△ (A)	-

た 10 個（利用者数，評価の記述なし）を選定した．

6. 実験結果及びその考察

6.1 ブラウザの履歴削除後に残留するスーパークッキー

ブラウザの履歴削除機能を用いて利用者がブラウザの履歴を削除するときの操作として想定される 3 つのケースについて考える．

(1) クッキーのみを削除したケース
(2) ブラウザのデフォルトの設定で削除したケース
(3) 全ての設定項目を削除したケース

実験の結果を付録の表 A·1 に示す．

表 A·1 において，ブラウザの履歴削除後にスーパークッキーが残留した場合はそのスーパークッキーの名前，残留しなかった場合は x，OS がブラウザをサポートしていない場合は-を記載した．

（1）のケースでは，削除されずに残留してしまうスーパークッキーが多く存在する．ブラウザと OS の組み合わせによって異なるが，具体的には，PNG，ETag，Cache. Local，IDB，DB，HSTS が残留することが実験により確認された．特に，Safari 以外のブラウザでは対応している多くの OS においてスーパークッキーが残留する．そのため，クッキーのみの削除ではトラッキング対策として不十分であり，多くのブラウザにおいてスーパークッキーが残留するのでトラッキングを回避できない．

（2）のケースでは，Firefox において Local，IDB，HSTS が残留し，Opera では HSTS が残留する．そのため，Firefox と Opera ではデフォルトの設定でブラウザの履歴削除機能を利用した場合でも，スーパークッキーによるトラッキングを回避できず，さらに削除項目を増やす必要がある．一方で，Chrome，IE，Edge ではスーパークッキーが残留しない．したがって Chrome，IE，Edge ではデフォルトの設定でブラウザの履歴削除機能を用いることでトラッキングを回避できる．

（3）のケースでは，全ての削除項目を選択したにも関わらず，Android の Firefox では Local が，Opera では HSTS が残留する．そのため，ブラウザの履歴削除機能のみではトラッキング対策として不十分な場合があり，他の対策技術を講じて削除する必要がある．

6.2 プライベートブラウジングによるスーパークッキー対策

プライベートブラウジングを使用した場合のスーパークッキー残留状況について実験した．

調査実験の結果を表 5 に示す．なお，残留するスーパークッキーが存在しない場合は x，OS がブラウザをサポートしていない場合は-とした．

表 5　プライベートブラウジング使用時のスーパークッキー

	Windows	macOS	iOS	Android
Chrome	x	x	x	x
Safari	-	x	x	-
IE	x	-	-	-
Firefox	x	x	x	x
Opera	x	x	x	x
Edge	x	-	x	x

ブラウザを閉じ，プライベートブラウジングを終了することで，OS やブラウザに関わらずスーパークッキーが残留しないことが確認できた．すなわち，プライベートブラウジング使用時には，ブラウザを閉じることでスーパークッキーによるトラッキングを回避できる．

6.3 Tor ブラウザによるスーパークッキー対策

Tor ブラウザを使用した場合のスーパークッキーの残留状況について実験した．

調査実験の結果を表 6 に示す．なお，残留するスーパークッキーが存在しない場合は x，OS が当該ブラウザをサポートしてない場合は-とした．

表 6　Tor ブラウザ使用時のスーパークッキー実験

	Windows	macOS	iOS	Android
ブラウザを閉じた場合	x	x	x	-

ブラウザを閉じ，Tor ブラウザを終了することで 3 つの

OS においてスーパークッキーが残留しないことを確認できた．Android の Orfox では JavaScript の動作を止めてしまいスーパークッキーを採取できなかった．

すなわち，Tor ブラウザを閉じれば，スーパークッキーによるトラッキングを回避できる．

6.4 拡張機能利用によるフィンガープリンティング対策

5.3.3 項で選定した拡張機能がフィンガープリンティング対策として有効かどうか実験した．

調査実験の結果を付録の表 A·2 に示す．

フィンガープリントの採取ができる拡張機能と採取ができない拡張機能が存在することを確認できた．採取ができない理由として，その拡張機能が JavaScript の動作を止めてしまうことが考えられる．この場合，フィンガープリントの採取はできず，UI/UX は悪くなるがトラッキング対策として有効性は高い．ただし，JavaScript を停止しても，JavaScript を使わないパッシブフィンガープリント対策にはならないことに注意されたい．

フィンガープリントを変化させる拡張機能には，選定の際に検索ワード「Fingerprint」に該当するものが多く，「Tracking」に該当するものでは，フィンガープリントの変化はほとんど見られなかった（計 20 個のうち 1 個）．つまり，トラッキング対策が目的の対策技術はフィンガープリンティング対策としての有効性は低く，アドブロックやその他トラッキング防止機能を備えていても，フィンガープリントが採取された場合，フィンガープリントによりトラッキングされてしまう可能性がある．

一方で，検索ワード「Fingerpirnt」に該当するものは，その拡張機能が訴える偽造機能を備えたものが多く見られた．つまり，検索ワード「Fingerpirnt」に該当するものはフィンガープリンティング対策として有効であり，有効性をさらに高めるためにはそれらを組み合わせればよいと言える．

6.5 プライベートブラウジングによるフィンガープリンティング対策

プライベートブラウジングの使用の有無によって採取できるフィンガープリントに違いが生じるのかを実験した．

実験環境統一の観点から使用した OS とブラウザは 6.4 節のそれと同様にした．なお，プライベートブラウジングのデフォルト設定で Do Not Track が有効になる場合が多い．

プライベートブラウジングの使用の有無によるフィンガープリントを比較し，違いが生じた特徴点を表 7 に示す．フィンガープリントに違いが見られなかった場合は x とした．

プライベートブラウジング利用時に変化するフィンガープリントは Safari，Firefox の Do Not Track のみで，他の特徴点では変化がなかった．なお，Chrome では特徴点に変化がなかった．

表 7 プライベートブラウジング時にフィンガープリントが変化した特徴点

	Fingerprint が変化した特徴点
Chrome	x
Safari	Do Not Track
Firefox	Do Not Track

すなわち，プライベートブラウジング時においてもフィンガープリントの採取が通常ブラウジングとほとんど変わらずにできてしまい，トラッキングにおける有効性は極めて低いと言える．

6.6 Tor ブラウザによるフィンガープリンティング対策

Tor ブラウザ利用時のフィンガープリントを Firefox 利用時のものと比較し違いが生じるのかを実験した．

6.5 節と同様，実験環境統一の観点から macOS を対象 OS とした．双方ブラウザのフィンガープリントを比較し，違いが生じた特徴点を以下の表 8 に示す．

表 8 Tor ブラウザ利用時にフィンガープリントが変化した特徴点

Fingerprint が変化した特徴点
UserAgent 文字列，画面解像度，GPU，Web Worker，Canvas，WebGL Render，ssdeep，フォントリスト，Google Geolocation API

Tor ブラウザを使用した場合，多くのフィンガープリントが変化した．変化した特徴点の中には，Google Geolocation API による位置情報や UserAgent 文字列，画面解像度などが挙げられる．すなわち，Tor ブラウザ利用時には多くのフィンガープリントが変化するので，トラッキングにおける有効性は高いと言える．一方で，多くのフィンガープリントが変化してしまうので，UI/UX における懸念もある．

7. 研究倫理

実験に使用した 2 つの採取サイトは，スーパークッキー並びにフィンガープリントを採取する旨を提示して採取を行なっている．また，採取データから，個人の特定をしていない．採取データは，セキュリティ対策を施した上で保管し，第三者への提供・販売をしない．

8. まとめ

本論文では Web トラッキング技術であるスーパークッキーとフィンガープリンティングの対策技術の有効性を検証するために実験をした．

ブラウザの履歴から単にクッキーのみを削除した場合，多くのブラウザでスーパークッキーが残留し，トラッキングに繋がる可能性がある．よって，ブラウザの履歴を削除するときは，利用者自身で削除項目の追加をした上で履

歴を削除する必要がある．また，プライベートブラウジングや Tor Browser の場合，ブラウザを閉じることで，スーパークッキーによるトラッキングの可能性が低くなる．

一方，フィンガープリンティングに対して，ブラウザの拡張機能を確かめたところ，フィンガープリンティング対策になるものとならないものが存在した．トラッキングを回避するためにはフィンガープリントを変化させる拡張機能を選定する必要があり，複数組み合わせることで有効性を高められると推察される．また，プライベートブラウジングでの変化は，Do Not Track 宣言のみであり，フィンガープリンティング対策としては効果がないと言える．Tor ブラウザのフィンガープリンティング対策は有効だが，UI/UX に懸念がある．

参考文献

[1] FireGloves, https://fingerprint.pet-portal.eu/?menu=6.

[2] LocalStorage, https://developer.mozilla.org/ja/docs/Web/API/Window/localStorage.

[3] openDatabase, https://developer.mozilla.org/en-US/docs/Mozilla/Thunderbird/Thunderbird_extensions/HowTos/Common_Thunderbird_Extension_Techniques/Use_SQLite.

[4] StatCounter https://gs.statcounter.com/.

[5] 64% Of Tracking Cookies Are Blocked, Deleted By Web Browsers, https://www.mediapost.com/publications/article/316757/64-of-tracking-cookies-are-blocked-deleted-by-we.html?edition=108287 (Mar 2018).

[6] Baumann, P., Katzenbeisser, S., Stopczynski, M. and Tews, E. Disguised Chromium Browser: Robust Browser, Flash and Canvas Fingerprinting Protection, Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society, WPES '16, New York, NY, USA (2016), ACM.

[7] Eckersley, P. How Unique Is Your Web Browser?, Proceedings of the 10th international conference on Privacy enhancing technologies, PETS'10 (2010).

[8] FaizKhademi, A., Zulkernine, M. and Weldemariam, K. FPGuard: Detection and Prevention of Browser Fingerprinting, Data and Applications Security and Privacy XXIX (ed.Samarati, P.), Cham (2015), Springer International Publishing.

[9] Kamkar, S. evercookie (2010), https://samy.pl/evercookie/.

[10] Laperdrix, P., Baudry, B. and Mishra, V. FPRandom: Randomizing core browser objects to break advanced device fingerprinting techniques, ESSoS 2017 - 9th International Symposium on Engineering Secure Software and Systems, Bonn, Germany (July 2017).

[11] Laperdrix, P., Rudametkin, W. and Baudry, B. Mitigating Browser Fingerprint Tracking: Multi-level Reconfiguration and Diversification, 2015 IEEE/ACM 10th International Symposium on Software Engineering for Adaptive and Self-Managing Systems (May 2015).

[12] Nikiforakis, N., Joosen, W. and Livshits, B. PriVaricator: Deceiving Fingerprinters with Little White Lies, Proceedings of the 24th International Conference on World Wide Web, WWW '15, Republic and Canton of Geneva, Switzerland (2015), International World Wide Web Conferences Steering Committee.

[13] Roesner, F., Kohno, T. and Wetherall, D. Detecting and Defending Against Third-Party Tracking on the Web, Presented as part of the 9th USENIX Symposium on Networked Systems Design and Implementation (NSDI 12), San Jose, CA (2012), USENIX.

[14] Torres, C. F., Jonker, H. and Mauw, S. FP-Block: Usable Web Privacy by Controlling Browser Fingerprinting, Computer Security – ESORICS 2015 (eds.Pernul, G., Y A Ryan, P. and Weippl, E.), Cham (2015), Springer International Publishing.

[15] 田邉一寿, 細谷竜平, 高橋和司, 安田昂樹, 種岡優幸, 小芝力太, 齋藤祐太, 齋藤孝道 Browser Fingerprinting における特徴の組み合わせに関する考察, コンピュータセキュリティシンポジウム 2017(CSS2017) (2017).

付　　録

A.1 付録

実験 6.1 の結果を A·1 に，実験 6.4 の結果を A·2 に示す．

表 A·1　各ブラウザの履歴を削除した場合のスーパークッキー残留状況

	Windows	macOS	iOS	Android
Chrome（1）	PNG，ETag，Cache	PNG，ETag，Cache，HSTS	x	PNG，ETag，Cache，HSTS
Chrome（2）	x	x	x	x
Chrome（3）	x	x	x	x
Safari（1）	-	x	x	-
Safari（2）	-	x	x	-
Safari（3）	-	x	x	-
IE（1）	PNG，Cache	-	-	-
IE（2）	x	-	-	-
IE（3）	x	-	-	-
Firefox（1）	Local，IDB，ETag	Local，IDB，ETag，HSTS	PNG，ETag，Cache	Local，IDB，ETag
Firefox（2）	Local，IDB	Local，IDB，HSTS	x	Local
Firefox（3）	x	x	x	Local
Opera（1）	PNG，ETag，Cache，HSTS	PNG，ETag，Cache，HSTS	x	HSTS
Opera（2）	x	x	x	HSTS
Opera（3）	x	x	x	HSTS
Edge（1）	x	-	PNG，ETag，Cache，Local，IDB，DB	Png，ETag，Cache，HSTS
Edge（2）	x	-	x	x
Edge（3）	x	-	x	x

表 A·2　拡張機能利用時のフィンガープリント変化状況

ブラウザ名	検索ワード	対策ツール	主な機能	FP 採取可否	Fingerprint が偽装された特徴点	バージョン
Firefox	Fingerprint	Canvas Blocker	Canvas のブロック	○	Canvas	0.5.0.1b
		Temporary Containers	プライバシーが強化されたタブを開く	○	変化なし	0.90
		ScriptSafe	ブラウザのセキュリティ向上	x	-	1.0.9.8
		Blend In	UserAgent 文字列を Windows7 にする	○	UserAgent 文字列，ssdeep	61.0t52
		WebAPI Manager	WebAPI の管理	○	変化なし	0.9.27
	Tracking	uBlock Origin	悪質なサイト・アドブロック	○	変化なし	1.16.14
		Ghostery	アドブロック	○	変化なし	8.2.1
		DuckDuckGo Privacy Essentials	トラッキングのブロック	○	変化なし	2018.6.28
		Privacy Badger	Do Not Track の送信	○	Do Not Track	2018.7.18.1
		AdBlocker Ultimate	全広告のブロック	○	変化なし	2.31
Chrome	Fingerprint	Privacy Badger	Do Not Track の送信	○	Do Not Track	2018.5.10
		ScriptSafe	ブラウザのセキュリテイ向上	x	-	1.0.9.3
		JustBlock Security	マルウェア・アドブロック	○	変化なし	2.0.36
		Random User-Agent	UserAgent 文字列の変更	○	UserAgent 文字列，ssdeep	2.2.5
		Canvas Defender	Canvas の秘匿化	○	Canvas，WebGL Render	1.1.0
	Tracking	uBlock Origin	アドブロック	x	-	1.16.12
		AdBlock	アドブロック	○	変化なし	3.31.2
		Adguard AdBlocker	アドブロック	○	変化なし	2.9.2
		Fair AdBlocker	アドブロック	○	変化なし	1.404
		AdBlocker Ultimate	アドブロック	○	変化なし	2.26
Safari	Tracking	Adamant	アドブロック	○	変化なし	1.3
		JS Blocker 5	トラッキング防止，プライバシー保護	○	変化なし	5.2.2
		UntrackMe	トラッキングに関連する URL のブロック	x	-	1.2.1=2
		Better	トラッキング防止	○	変化なし	1.0
		Sanitize	アドブロック	○	変化なし	1.4
		Just Content	アドブロック	○	変化なし	1.0.1
		Ka-Block!	アドブロック	○	変化なし	3.1
		Ad-Blocker	アドブロック	x	-	1.0
		Findx Privacy Control	トラッキング防止	○	変化なし	1.16.0
		280blocker	モバイルサイトに特化したアドブロッカー	○	変化なし	2.1.1