

モダンブラウザにおける supercookie の調査:2017 年版

小芝 力太† 高橋 和司‡ 安田 昂樹‡ 田邊 一寿‡ 種岡 優幸‡ 細谷 竜平‡
 齋藤 祐太† 野田 隆文† 齋藤 孝道†
 †明治大学 ‡明治大学大学院

1 はじめに

Web 広告事業者は、Web の利用者を HTTP cookie を利用し Web 上での追跡（以降、追跡と呼ぶ）をしているとされている。利用者は HTTP cookie の削除で追跡を回避できる。しかし、supercookie というブラウザ記憶機構を利用した技術が考案され、HTTP cookie の削除だけでは追跡を回避できないことが明らかになった。supercookie は Web Storage API や IndexedDB などの要素で構成され、主にブラウザの履歴として管理される。

supercookie の有効性については先行研究 [1][2] で論じられてきたが、本論文では 2017 年現在のモダンブラウザにおける supercookie の有効性についてプライベートブラウジングは利用せずに、2つの調査をした。1つ目に被験者がブラウザの履歴を削除した時、複数ある supercookie の要素の中から消えずに残る要素を調査した（以降、調査 1 と呼ぶ）。2つ目にクラウドソーシングを利用し、被験者がブラウザの履歴を削除する際に選択する削除項目を調査した（以降、調査 2 と呼ぶ）。そして、その割合から履歴の削除後でも追跡される被験者の割合を算出した。その結果、一部の OS とブラウザにおいて履歴の削除だけでは追跡を回避できない被験者が存在することがわかった。追跡を回避するためには削除項目の選択時に選択項目を増やす必要がある。

2 関連知識

2.1 supercookie

利用者が追跡を回避するために HTTP cookie を削除した場合でも、継続して追跡する目的で supercookie が登場した。ブラウザ記憶機構である Local Shared Object や IndexedDB, Web Storage API, HTTP Etag などを複合的に利用した技術である。複数の要素を使用しているので、HTTP cookie と比較して削除しにくく、利用者を強力に追跡できることが知られている。HTTP cookie のみの削除で追跡を回避できると考えている利用者は、

supercookie の存在を知らず追跡される可能性がある。

2.2 ブラウザの履歴データの削除

各モダンブラウザには、HTTP cookie をはじめとするブラウザ記憶機構があり、様々な情報が保存される。利用者は、ブラウザの履歴削除機能を使用して、ブラウザの履歴などの保存情報を削除できる。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。本論文では、各ブラウザの削除項目の選択によって supercookie の要素が残るかを調査した。

3 調査手法

3.1 supercookie 調査サイト

本論文では Samy Kamkar 氏のサイト [3] を元に supercookie 調査サイト（以降、調査サイトと呼ぶ）を構築した。初回アクセス時、調査サイトは 14 個の supercookie の要素に対して、識別子として生成した乱数（以降、UID と呼ぶ）を保存する。二度目以降のアクセスでは supercookie の各要素を読み出し、初回アクセスで保存された UID が残るか確認する。なお、調査サイトは今回の調査の趣旨に同意した被験者のみ協力できるようにになっている。

3.2 調査 1 のサンプルと調査手順

調査 1 では、被験者がブラウザの履歴を削除した時に 14 個ある supercookie の中から消えずに残る要素を調査した。調査手順は、はじめに被験者が調査サイトにアクセスすることで、supercookie の各要素に UID が保存される。次に、被験者は履歴削除機能を用いてブラウザの履歴を削除する。この時の履歴の削除項目は被験者が選択可能であり、デフォルト設定とデフォルト設定から項目を変更した場合で分類した。その後ブラウザを閉じ、再度調査サイトにアクセスした時に、supercookie の要素に残っている UID を調査した。

3.3 調査 2 のサンプルと調査手順

調査 2 では、被験者がブラウザの履歴削除時の削除項目の選択方法に傾向があるのかクラウドソーシング

Research on supercookie in Modern Browser:2017

†Rikita KOSHIBA ‡Kazushi TAKAHASHI ‡Koki YASUDA

‡Kazuhisa TANABE ‡Masayuki TANEOKA ‡Ryohei HOSOYA

†Yuta SAITO †Takafumi NODA †Takamichi SAITO

†Meiji University

‡Graduate School of Meiji University

を利用して調査した。依頼では、被験者はブラウザの履歴削除画面を開き、現状の削除項目の選択状況について回答する。調査1により、削除項目の選択状況から supercookie の要素が残る状態がわかったので、この結果から supercookie の要素が一つでも残る場合を追跡可能とした。調査期間は2017年11月19日から2017年12月16日であり、計851件のデータを採取した。

4 調査結果

4.1 調査1の結果

調査1の結果を表1に示す。ブラウザの履歴の削除項目の設定がデフォルトの場合（以降、デフォルト設定と呼ぶ）とデフォルト設定から削除項目を追加、削除期間を変更した場合で分類し、調査した。表1でブラウザの上付き文字Dは前者、Mは後者を表す（Mが示す状態は脚注に記載）。表1に supercookie の要素が記載されている場合、ブラウザの履歴削除後もその要素が残ったことを表す。また“x”はブラウザの履歴削除後に supercookie が残らなかったことを表し、“-”はサポート外のOSなので調査対象外としたことを表す。

表1: OS とブラウザの supercookie 残留表

	Windows	macOS	Linux	iOS	Android
Chrome ^D	x	x	x	x	x
Chrome ^M	x	x	x	x	x
Firefox ^D	localStorage IndexedDB	localStorage IndexedDB	localStorage IndexedDB	x	IndexedDB
Firefox ^M	IndexedDB*	IndexedDB*	localStorage IndexedDB [†]	x	IndexedDB [‡]
IE ^D	x	-	-	-	-
IE ^M	x	-	-	-	-
Opera ^D	x	x	x	png etag cache cookie dbdata IndexedDB localStorage	x
Opera ^M	x	x	x	x	x
Safari ^D	-	x	-	x	-
Safari ^M	-	x	-	x	-
Edge ^D	x	-	-	-	-
Edge ^M	x	-	-	-	-

iOS の Opera は iOS 版の Opera Mini を使用した。調査1の結果、ブラウザの履歴を削除したにも関わらず一部の supercookie の要素が残ることがわかった。デフォルト設定のまま削除をしても追跡を回避できない場合があることがわかる。そのため利用者自身がブラウザの履歴の削除項目をデフォルト設定から増やす必要が

*削除項目はデフォルトのまま、削除期間を「1時間」から「全ての期間」に変更しても残る。削除項目を全て選択すると残らない。
[†]削除項目はデフォルトのまま、削除期間を「1時間」から「全ての期間」に変更すると localStorage が消え、IndexedDB が残る。削除項目を全て選択し、削除期間を全てにしても IndexedDB が残る。
[‡]削除項目を全て選択しても残る（期間の設定項目なし）。

ある。また、全ての削除項目を選択しても、Linux および Android の Firefox では追跡を回避できない。

4.2 調査2の結果

調査2の結果を表2に示す。また、履歴の削除項目がデフォルト設定の被験者数も記載。デフォルト設定数と追跡可能数の割合をデータ数から算出した。なお、Safari は履歴の削除項目がないので調査対象外とした。

表2: 各ブラウザのデフォルト設定数と追跡可能数

	データ数	デフォルト設定数	追跡可能数
Chrome	300	131 (43.7%)	107 (35.7%)
Firefox	192	65 (33.9%)	162 (84.4%)
IE	222	101 (45.5%)	42 (18.9%)
Opera	43	15 (34.9%)	6 (14.0%)
Edge	94	48 (51.1%)	12 (12.8%)

調査2の結果、Firefox で追跡を回避できない場合が最も多く84.4%となった。他のブラウザでは Chrome で35.7%、IE で18.9%、Opera で14.0%、Edge で12.8%となった。追跡可能数が最も高い Firefox は、デフォルト設定でも追跡できるので最も割合が高くなった。追跡可能であったデータの内訳として、HTTP cookie のみを選択している場合が多かった。しかし、削除項目がデフォルト設定や HTTP cookie のみである場合、実際には supercookie の要素が残ってしまうので追跡可能になってしまう。

5 まとめ

調査の結果、削除項目がデフォルト設定や HTTP cookie のみである場合、追跡を回避できないことがわかった。また、利用者は全ての削除項目を選択しても、Linux および Android の Firefox では IndexedDB が残ってしまい、追跡を回避できない。追跡を回避するためには利用者自身が対策手法を取り入れる必要がある。

参考文献

[1] Jonathan R. Mayer and John C. Mitchell. Third-Party Web Tracking: Policy and Technology. In *Proceedings of in IEEE Symposium on Security and Privacy, S&P'12*, 2012.
 [2] Mika D. Ayenson, Dietrich J. Wambach, Ashkan Soltani, Nathaniel Good, and Chris Jay Hoofnagle. Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning. Available at SSRN 1898390, 2011.
 [3] Samy Kamkar. evercookie, 2010. <https://samy.pl/evercookie/>.