1W-08

Browser Fingerprinting 対策ツールの評価

柳沢 進也† 高橋 和司‡ 安田 昂樹‡ 田邉 一寿‡ 種岡 優幸‡ 細谷 竜平‡
小芝 力太† 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 サーバが Web ブラウザから，アクセスしてきた端末の特定に繋がる IP アドレス等の情報（以降，特徴点という）を採取する Browser Fingerprinting（以降，Fingerprinting という）という手法がある．Fingerprinting は採取した情報から利用者の嗜好の判断や，ターゲティング広告等の効果的な広告を実現するために用いられる．また，端末の特定に繋がる具体的な値を Browser Fingerprint（以降，Fingerprint という）という．Fingerprinting は利用者の許可を得ずに行えるので，対策ツールを用いて Fingerprint の偽装を行う利用者もいる．しかし，多くの対策ツールの有効性は示されていない．そこで本論文では，Fingerprint の偽装を行う Firefox のアドオンや Chrome の拡張機能（以降，対策ツールという）が特徴点をどの程度偽装できるのかについて調査した．その結果，特徴点の一部のみしか偽装できない対策ツールと，全く偽装ができない対策ツールが存在することが明らかになった．これにより，追跡を逃れる目的で対策ツールを使用している利用者は，これらの対策ツールを使用した場合でも Fingerinting により追跡される可能性があることがわかった．

2 調査内容

2.1 Fingerprint 採取サイト

本研究グループ [1] では Fingerprint を採取するための Web サイト（以降，Fingerprint 採取サイトという）を運営している．Fingerprint 採取サイトは，Fingerprint の採取が終了した後に採取した特徴点の値を一覧で表示する．調査では，各種対策ツールを有効にした場合と無効にした場合で採取後に出力される特徴点の値を比較し，変化した場合は特徴点が偽装されていると判定した．なお，Fingerprint 採取サイトでは本論文の趣旨に同意した被験者のみが調査に協力している．

2.2 調査環境

調査では，OS は Windows10（64bit），ブラウザは Firefox57.0（64bit），Chrome61.0.3163.100（64bit）を使用した．

2.3 対策ツールの選定基準

調査対象とする対策ツールを選定するにあたり，次の 3 つの基準を設けた．(1) 特徴点の偽装が可能である旨が説明されている対策ツール (2) Firefox に関しては，プライバシー/セキュリティのカテゴリーに属する利用者数 1 万人以上の対策ツール (3) Chrome に関しては利用者補助機能のカテゴリーに属する評価が 4.0 以上かつ利用者数 1 万人以上の対策ツール

この選定基準により，Firefox では 15 個，Chrome では 10 個の対策ツールが調査対象に該当した．

3 調査結果

3.1 対策ツールにより偽装された特徴点

調査対象の対策ツールを有効にした状態で Fingerprinting を行ったところ, 一部の対策ツールで特定の特徴点が偽装されたことを確認した．偽装が確認できた各特徴点が何件の対策ツールで偽装されていたかを表 2 に示す．本研究の調査により，User-Agent 文字列（以降，UA 文字列という），IP アドレス（表中では IP と記載する），OS Fingerprinting [2]，及び，Canvas Fingerprinting [3]（表中では Canvas と記載する）の 4 つの特徴点において，特徴点の偽装が確認できた．調査結果の詳細を表 3 に示す（表中の FP 採取可否は Fingerprint 採取サイトで特徴点が採取できたかを表す.）．

3.2 特徴点を偽装する効果がある対策ツール

Fingerprinting に対して，特徴点を偽装する効果がある対策ツールを表 1 に集計した．調査の結果，一部の対策ツールを有効にした際に Fingerprint の採取が終了しない場合があった．原因として，Fingerprinting を実行するスクリプトを対策ツールが止めていると推察される．この現象は Firefox の 6 個の対策ツールと Chrome の 1 個の対策ツールで発生した．

Evaluation of countermeasure tools against Browser Fingerprinting
†Shinya YANAGISAWA ‡Kazushi TAKAHASHI ‡Koki YASUDA ‡Kazuhisa TANABE ‡Masayuki TANEOKA ‡Ryohei HOSOYA †Rikita KOSHIBA †Yuta SAITO †Takafumi NODA †Takamichi SAITO
†Meiji University
‡Graduate School of Meiji University

表 1: 効果がある対策ツールの件数

ブラウザ	総数	効果あり	効果なし	不明
Firefox	15	7	2	6
Chrome	10	9	0	1

表 2: 偽装されていた特徴点と件数

	件数	
特徴点	Firefox	Chrome
IP	6	4
UA 文字列	1	3
OS Fingerprint	7	4
Canvas	1	2

4 まとめ

今回の調査で，対策ツールによる偽装を確認した特徴点は UA 文字列，IP アドレス，OS Fingerprinting，Canvas Fingerprinting の 4 点だった．しかしながら，これは Fingerprinting で採取する特徴点の一部であり，これらの特徴点を部分的に偽装した場合では追跡される可能性が依然として残る．これにより，追跡を逃れる目的で本論文の調査対象である対策ツールを使用したとしても，利用者は Fingerprinting により追跡されうることを明らかにした．

参考文献

[1] 磯侑斗, 桐生直輝, 塚本耕司, 高須航, 山田智隆, 武居直樹, 齋藤孝道. Web browser fingerprint を採取する web サイトの構築と採取データの分析. コンピュータセキュリティシンポジウム 2014, 2014.

[2] p0f v3. `http://lcamtuf.coredump.cx/p0f3/`.

[3] K Mowery and H Shacham. Pixel Perfect: Fingerprinting Canvas in HTML5. In *Proceedings of Web 2.0 Security and Privacy*, W2SP, 2012.

表 3: 調査結果の詳細

ブラウザ名	対策ツール	主な機能	FP 採取可否	偽装された特徴点
Firefox	Privacy Badger	トラッキング防止	○	
	friGate	プロキシ拡張	x	
	Adguard Adbrocker	広告ブロック	x	
	anonymoX	IP 偽装	○	IP,OS Fingerprint
	IPFlood	IP 偽装	○	
	Random Agent Spoofer	UA 文字列偽装	x	
	Proxy Tool	プロキシ拡張	x	
	Modify Headers	HTTP ヘッダ変更	x	
	Disconnect	トラッキング防止	○	IP,OS Fingerprint
	User-Agent Swicher	UA 文字列偽装	○	UA 文字列,OS Fingerprint
	Browsec VPN	VPN	○	IP,OS Fingerprint
	Windscribe	VPN, 広告ブロック	x	
	Stealthy	IP 偽装	○	IP,OS Fingerprint
	CanvasBlocker	Canvas 防止	○	IP,OS Fingerprint,Canvas
	Best Proxy Swicher	プロキシ拡張	○	IP,OS Fingerprint
Chrome	ZenMate VPN	VPN	○	IP,OS Fingerprint
	Hotspot Shield	VPN	○	IP,OS Fingerprint
	TouchVPN	VPN	○	IP,OS Fingerprint
	MobileLayouter	UA 文字列偽装	○	UA 文字列
	User-Agent Swicher	UA 文字列偽装	○	UA 文字列
	CanvasFingerprintBlock	Canvas 防止	○	Canvas
	Canvas Defender	Canvas 防止	○	Canvas
	Script Safe	秘匿性向上	x	
	Random User-Agent	UA 文字列偽装	○	UA 文字列
	Hide My IP	IP 偽装,VPN	○	IP,OS Fingerprint