5Z-8

Webサイトが採取するブラウザの特徴点の採取状況を検知する手法の提案と実装

山田　智隆[†]　磯　侑斗[‡]　桐生　直輝[‡]　齋藤　孝道[†]
明治大学[†]　明治大学大学院[‡]

1. はじめに

利用者の Web 上での行動を追跡し，利用者の趣味嗜好に合わせた情報を提示する行動ターゲティング型広告などを実現する仕組みがある．現在 Web 上で利用者を追跡する手法として，HTTP クッキーを用いる手法が一般的である．

しかし，その種の行動追跡（以降，Web トラッキングという）により趣味嗜好を分析されることを好ましく思わない利用者も少なからずおり，社会的にも Web トラッキング行為についてプライバシーに関する議論も多い[1].

利用者は，ブラウザの HTTP クッキーを削除，または拒否することで標準的な Web トラッキングを回避することが可能であるが，現在の Web の利用状況から，HTTP クッキーの利用は不可避であると言える．

他方，HTTP クッキーを用いることなく，利用者のブラウザから採取できる情報の特徴や HTTP 通信時のヘッダなどの特徴を用いて，利用者を識別する手法が発案[2]された．いわゆる，Web Browser Fingerprinting である．Web Browser Fingerprinting への対策としては，JavaScript を無効化することや，FireGloves[3]などの拡張機能を利用することで，一定の防御をすることが可能であると言える．しかし，JavaScript の無効化や FireGloves は全ての Web サイトに対して適用されてしまうので，Web Browser Fingerprinting を実装していない Web サイトの表示に悪影響を及ぼす可能性がある．

そこで本論文では，Web サイトが「JavaScript と Flash を用いてブラウザの特徴点を採取する行為」を検知する拡張機能を提案し，その実装を示す．

2. Web トラッキング

2.1 概要

Web Browser Fingerprinting に用いられる二つのクライアントの識別方法とそれによる Web トラッキングについて説明する．ここで，本論文では，ブラウザから採取することが可能で，かつそのブラウザが稼働する端末の識別に繋がるような情報を特徴点と呼ぶ.

2.2 HTTP クッキーによる Web トラッキング

閲覧者がアクセスした Web サイトのページ内に広告サーバが提供するバナー広告が含まれていた場合，広告サーバから HTTP クッキーが発行され，閲覧者のブラウザに保存される．二回目以降のアクセスの際，同じバナー広告を含む Web サイトにアクセスすると，ブラウザは自動的に保存している HTTP クッキーを広告サーバに送信する．広告サーバは HTTP クッキーと閲覧者がアクセスした Web サイトの URL を紐付けることによって，閲覧者の Web 上での行動追跡をすることができる．いわゆるサードパーティークッキーを用いた Web トラッキングである．

閲覧者はブラウザに保存されている HTTP クッキーを削除，または拒否することで追跡を回避することができる．

2.3 ブラウザの特徴点による Web トラッキング

ブラウザのプラグイン，フォント，（HTTP リクエストヘッダに含まれる）UserAgent や Accept-Language などの情報は，閲覧者を識別するための特徴点として利用することができる[2]．特徴点は組み合わせることで閲覧者を高い精度で一意に識別できる情報になり，アクセスした Web サイトの URL と紐付けることで Web トラッキングが可能になる．

M.Rausch[4]は特徴点による Web トラッキングを行っている Web サイトが存在すると述べている．

3. ブラウザの特徴点による Web トラッキングの対策

Web Browser Fingerprinting 対策を説明する．

3.1 スクリプトの停止

単純な対策として，ブラウザ上で稼働する JavaScript などの無効化がある．

NoScript[5]は，Firefox の拡張機能で，Web ページ読み込み時，JavaScript，Flash や，XSS などのコードの実行を，別途 Web 閲覧者が与えるホワイトリストの判定に応じて行う．

3.2 FireGloves

FireGloves とは，Firefox の拡張機能である．閲覧者は FireGloves を使用することで，自身が利用するブラウザの UserAgent や画面解像度などの特

徴点になり得る情報を任意の偽の値に設定することができる．閲覧者から採取できる特徴点の値を毎回変化させることで，特徴点による閲覧者の識別を困難にさせる．

しかし，ブラウザの特徴点を偽の値に設定すると，その設定が全ての Web サイトに対して適用されるので，Web Browser Fingerprinting とは無関係の Web サイトの表示が，Web サイトの作成者の意図しない表示になる可能性がある．

4. 提案手法

4.1 概要

ブラウザの UserAgent や，フォントなどの特徴点は，JavaScript の特定のプロパティおよび Flash の関数を使用することで採取することができる．多くの Web Browser Fingerprinting で JavaScript が利用されている[1]．そこで，提案する方式では，特徴点を採取するためのプロパティや関数を上書きすることで，Web サイトが特徴点を採取した際にそれを拡張機能側で検知することができる．

本論文で実装したシステムが検知できる特徴点の数は，21 個である．すなわち，JavaScript の navigator オブジェクトから採取できる情報(userAgent，appVersion，appName，appCodeName，product，productSub，vendor，platform，language，cookieEnabled，mimeTypes，plugins，javaEnabled)，window オブジェクトから採取できる情報(screen.width，screen.height，screen.colorDepth，sessionStorage，localStorage)，Date オブジェクトから採取できる情報(getTimezoneOffset，getHours)，そして Flash から採取できる情報(Font)である．

4.2 動作

関数の書き換えはコンテントスクリプトに，独自に追記して行う．コンテントスクリプトとは拡張機能を構成するファイルの 1 つで，閲覧中の Web サイトに適用させる JavaScript が記述されている．

```
function add(){
    var script = document.createElement("script");
    script.appendChild(document.createTextNode(
                        (1)
    ));
    document.documentElement.appendChild(script);
```

図 1　Web ページに script タグを追加

コンテントスクリプトは描画する Web ページの JavaScript に対してアクセスするが，関数や変数を共有することができない．そこで，図 1 のように script タグとして Web ページに埋め込むことで，コンテントスクリプトは Web ページの JavaScript と関数や変数を共有することが可能になる．

```
"navigator._userAgent = navigator.userAgent;¥n "+
"navigator.__defineGetter__('userAgent',function(){
" +
"if(fp.ua == 0){ " +
"fp.ua = 1; " +
"fpcount++; " +
"fp.fpcount++; " +
"}¥n" +
"fpset(); " +
"return navigator._userAgent; " +
"});¥n" +
```

図 2　関数の上書き

図 2 は，特徴点となり得るプロパティを__defineGetter__を用いて上書きするコードであり，図 1 の(1)に入る．navigator.userAgent の本来の機能は損なわずに，navigator.userAgent が呼び出されたことを変数の変化によって示す機能を追加している．同様の処理を他のプロパティや関数にも行う．

Flash を用いてフォントの採取を試みることを検知するために，提案する拡張機能では Web サイトに適用される全ての Flash ファイルをデコンパイルし，ソースコードに変換する．フォントを採取する関数である enumerateFonts，あるいは getFontList がソースコードに含まれていた場合，Web サイトはフォントを採取しているとみなすことができる．

上記の処理を行うことで，Web サイトが特徴点の採取を試みる際に，本提案手法を用いて，拡張機能側で検知することが可能になる．

5. まとめ

本論文では，Web サイトが「JavaScript と Flash を用いてブラウザの特徴点を採取する行為」の検知を提案した．提案システムを用いて，Web Browser Fingerprinting に関連する Web サイトだけに対策をすることが可能である．

6. 参考文献

[1] 齋藤，磯，桐生，2014，Web Browser Fingerprinting に関する技術的観点での一考察，SCIS2014 予稿集

[2] Peter Eckersley, 2010, How Unique Is Your Web Browser? https://panopticlick.eff.org/browser-uniqueness.pdf

[3] Cross-browser fingerprinting test 2.0 http://fingerprint.pet-portal.eu/?menu=6

[4] Searching for Indicators of Device Fingerprinting in the JavaScript Code of Popular Websites http://www.truststc.org/education/reu/13/Papers/RauschM_Paper.pdf

[5]https://addons.mozilla.org/ja/firefox/addon/noscript/