ファーストパーティ，サードパーティを考慮した自己情報制御の提案

坂本 一仁† 松永 昌浩†

†セコム株式会社 IS 研究所
181-8528 東京都三鷹市下連雀 8-10-16 セコム SC センター
takah-sakamoto@secom.co.jp，m-matsunaga@secom.co.jp

あらまし Web サイトには，ファーストパーティのコンテンツと，サードパーティの広告や SNS 連動機能等が混在している．ユーザは，画面上に表示された Web サイトの内容や自身が入力した内容等，可視な情報を基にして，Web サイトの利用や自身の情報提供に関する判断を行っている．しかし，ユーザに不可視な状態で，多くのブラウザ情報と端末情報が送信されているため，ユーザは実質的な情報の利用，共有の範囲を認識することが難しい．本稿では，Web サイトを利用するユーザが，自身の提供している情報と，情報が共有される範囲を容易に理解でき，自身が管理する ID で，情報提供に対する選択と流通範囲の制御が可能な仕組みを提案する．

A Mechanism for Individual Control of First-Party and Third-party Accessibility to User Information

Takahito Sakamoto†and Masahiro Matsunaga†

†Intelligent Systems Laboratory, SECOM Co., Ltd.
SECOM SC Center, 8-10-16 Shimorenjaku, Mitaka, Tokyo 181-8528, JAPAN
takah-sakamoto@secom.co.jp，m-matsunaga@secom.co.jp

Abstract A website includes its own contents and third-party contents such as advertisements and SNS widgets. A user decides to use a website and to send his or her own data on the basis of visible information, which is displayed by the contents on the website and entered data by the user. However, a lot of browser data and device information is hidden from the user. Therefore, it is hard for users to determine how their information is actually used by third-parties, and to what extent that information is shared. This paper proposes a novel mechanism. A user manages his or her own ID by controlling what information is obtained and to what extent is shared to third-parties. By using this mechanism, the user has a clearer understanding of the accessibility of his or her own information.

1 はじめに

近年では，1 つのファーストパーティの Web サイトに，数多くのサードパーティの機能が埋め込まれるようになった．その理由は，広告表示機能，SNS 連動機能，アクセス解析機能など，自身の Web サイトに他のサイトが発行するスクリプトを手軽に導入できるようになったためである．その結果，Web サイトは，自身のサービスやコンテンツへの集客を増やして収益増加につなげることができ，ユーザは，便利に様々なサービスを利用できるようになったが，一方で問題となる点もある．

現状，ユーザは検索エンジンの結果などからファーストパーティにアクセスしていると認識していても，実際には認識できていない数多くのサードパーティへ同時にアクセスしていることとなる[1]．数多くのサードパーティは，ユーザのアクセスと同時に，ユーザのブラウザや端末情報を，ユーザに不可視な状態で取得し，個々のユーザを追跡，分析し，分析結果を共有している．しかし，ユーザは，自身の情報を共有している全ての事業者を把握できるわけではない．ユーザが自身の情報を管理するためには，ユーザが自身の情報の提供と流通範囲を負担なく認識でき，ユーザ主導で状況や目的に沿った選択ができ，継続的に制御できる必要がある．

本稿は，サードパーティとして行動ターゲティング広告を行う事業者に焦点を当て，ファーストパーティとサードパーティで，ユーザが認識できない部分を明確にする．そして，ユーザが利用するファーストパーティとサードパーティにおいて，ユーザが自身の提供している情報と，情報が共有される範囲を容易に理解でき，情報提供に対する選択と流通範囲の制御が可能な仕組みを提案する．具体的には，ブラウザ拡張機能において，ユーザ自身が生成する ID を導入し，ファーストパーティ，サードパーティとの情報流通の制御を実現することで，ユーザ主導で情報の流通範囲を制御するツールを提案する．

2 節では，ユーザの認識および選択と制御の現状について議論する．3 節では，現状の課題と研究の目標について述べる．4 節では，本稿で提案する仕組みを説明する．5 節では提案した仕組みがユーザだけでなく，ファーストパーティ，サードパーティにどのように貢献するかを考察する．6 節では，関連研究について述べる．7 節では，本稿のまとめと今後の課題を述べる．

2 現状

本節では，ユーザが利用するファーストパーティ，およびファーストパーティと連動しているサードパーティ（行動ターゲティング広告事業者）に対する現状のユーザの認識を明確にし，ユーザが現状利用できる自身の情報流通に関する選択と制御について議論する．

2.1 ユーザの認識の現状

ユーザが，サービスの内容や自身の取得されている情報の内容を認識できるかどうか，本稿では次のような尺度で議論する．

- ユーザが認識可能
  サービス内容や取得されている情報がブラウザの画面上で可視，または他の手段によりユーザが容易に把握できる状態である．
- ユーザが認識不可能
  サービス内容や取得されている情報がブラウザの画面上で不可視，かつユーザが容易に把握できる手段がない状態である．

2.1.1 行動ターゲティング広告

本稿では，サードパーティのサービスの代表として行動ターゲティング広告を取り上げる．現在の行動ターゲティング広告の主流は，HTTP Cookie を利用してユーザのブラウザを識別し，ユーザがメディアを訪問した際に，リアルタイムに広告料をオークション形式で入札し，広告を表示する方式である．事業者は大きく分類すると SSP（Supply Side Platform），DSP（Demand Side Platform），DMP（Data Management Platform）に分かれている．SSP は世の中に存在する広告表示在庫を測定し，DSP は広告主の入札を管理し，DMP は SSP，DSP やファーストパーティの CRM（Customer Relationship Management）と連携して，ユーザ情報の流通を促進させる．例えば，SSP は，あるファーストパーティにアクセスしてきたユーザを，SSP の Cookie に紐付いたユーザ情報から 30 代男性であると推定し，そのユーザに対する広告の入札リクエストを各 DSP に送信する．そして，それぞれの DSP はそのユーザに広告を表示するために広告料を提示し，最も高値を付けた DSP

[1] ファーストパーティとは，ユーザがアクセスした URL のドメインの事業者であり，サードパーティはユーザがアクセスした URL 以外のドメインの事業者である．

（広告主）が広告を表示できる仕組みである．この方式はRTB（Real Time Bidding）と呼ばれている．

また，RTBの一連の処理中に，各事業者は，Cookieによる IDの付与とCookie値のリダイレクト，専用Web APIを利用したパラメータ送信によって，アクセスしてきたユーザとユーザ情報を常に識別，参照できる状態を保っている．この処理はCookie Syncと呼ばれている．

実際，行動ターゲティング広告では，個々のユーザ情報のIPアドレス，閲覧履歴，閲覧時間帯等から個々のユーザをセグメント（30代，男性，独身，高級車など）に分類している．そして，そのセグメントをもとにそのユーザに効果があると推定される広告を表示している．

2.1.2　ユーザの認識

図1では，ファーストパーティおよび行動ターゲティング広告事業者（サードパーティ）において，ユーザが認識可能，不可能な部分を示す．

ファーストパーティの場合，ユーザはファーストパーティのWebサイトを利用する目的でアクセスし，Webサイトのコンテンツが画面上に表示される．そのため，サービスの内容は可視であるといえる．また，ユーザはファーストパーティのWebサイト上でページ遷移を行い，場合によっては自身の情報を登録する．そのため，自身の行動と提供情報をある程度把握できるといえる．実際にファーストパーティがユーザに不可視な状態でCookieや閲覧履歴を取得し，追跡していたとしても，ユーザは自身の行動から，ファーストパーティの追跡を把握できる．

一方で，ファーストパーティと連動している行動ターゲティング広告事業者の場合は，ユーザがアクセスしたファーストパーティのWebサイト上で，広告内容（広告主の宣伝情報）が表示される．しかし，実際にはユーザに不可視な状態で取得されたブラウザや端末情報等のユーザ情報が，広告主の広告を表示するまでに，20から30以上の数多くのサードパーティとファーストパーティで共有され，ユーザの属性を推定している[2]．この取得，共有されたユーザ情報と，

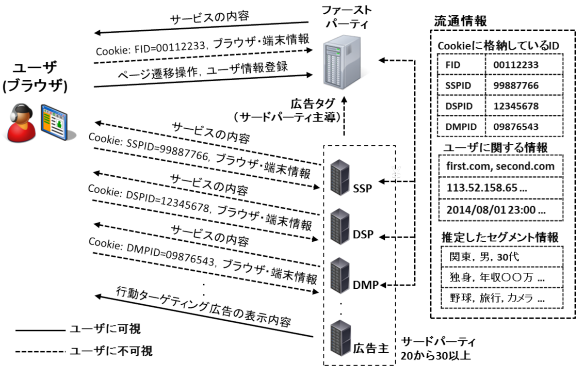

図 1: ユーザに可視，不可視の部分

推定されたユーザの属性（セグメント情報）は，ユーザに不可視であるといえる．また，広告を表示するための広告タグは，サードパーティ主導で生成されるため，サードパーティがユーザ情報の取得と共有範囲を決定しており，ユーザはその内容の把握が困難な状況となっている．

2.2　ユーザの選択と制御の現状

行動ターゲティング広告を行っているサードパーティの業界団体は，ユーザへの配慮として，自主規制ガイドライン [13, 1] を策定し，参加事業者に実施を促している．そして，参加事業者は，ユーザへ行動ターゲティング広告に対する選択と制御の機能を提供するため，行動ターゲティング広告に利用されているCookieのオプトアウト機能を提供している．オプトアウト機能は各事業者が個別に用意しているが，オプトアウトポータルサイト [3, 4, 11] も存在する．

2.2.1　オプトアウト

行動ターゲティング広告事業者が実施しているオプトアウト機能は，ユーザのブラウザに保存されているCookieによって実現されている．そのため，行動ターゲティング広告のオプトアウトを維持するには，下記の条件をすべて満たす必要がある．

[2]我々の調査では，大手ニュースサイト等への1回のアクセスで，20から30以上のサードパーティのドメインとCookie及びユーザ情報の共有が行われていることを確認している．

1. 広告事業者（サーバ）がオプトアウトする Cookie を持っており，オプトアウトが設定されている
2. ユーザ(ブラウザ)がオプトアウトする Cookie を持っている
3. ユーザ(ブラウザ)がオプトアウトする Cookie を送信する

例えば，ユーザが広告事業者に対してオプトアウト要求を行うと，事業者は保持しているユーザの Cookie にオプトアウトを設定する．以降，ユーザはオプトアウト設定されている Cookie と共にアクセスすれば，広告事業者はユーザに対して行動ターゲティングを行わない．

また，Cookie のオプトアウト以外の方式では，Federal Trade Commission（FTC）がプライバシーフレームワークとして進めている Do Not Track（DNT）[6] がある．さらに，サードパーティの Cookie による追跡を遮断する方法としては，ブラウザでサードパーティ Cookie を禁止する設定ができる．また，広告を完全に非表示にする方法として，広告をブロックするブラウザ拡張機能（広告ブロッキングツール）も存在する．

2.2.2 ユーザの選択と制御

現状においても，ユーザが利用できる行動ターゲティング広告に対するオプトアウト機能は提供されているが，Cookie のオプトアウトでは，ユーザがオプトアウトを継続できない場合がある．図 2 は，ユーザがオプトアウトを設定したが，再度行動ターゲティングが開始される例である．まず，ユーザ情報は Cookie Sync でサードパーティ全体に共有され，広告事業者 A に対してオプトアウトを設定している状態とする．ここで，ユーザ（ブラウザ）が保持している A の Cookie が削除または有効期限切れになるとする．そして，あるファーストパーティの Web サイトで A へのアクセスが発生すると，ユーザから A へ Cookie が送信されないため，A はユーザを新しいユーザだと認識する．その際に，A と広告事業者 B が Cookie Sync を実施すると，

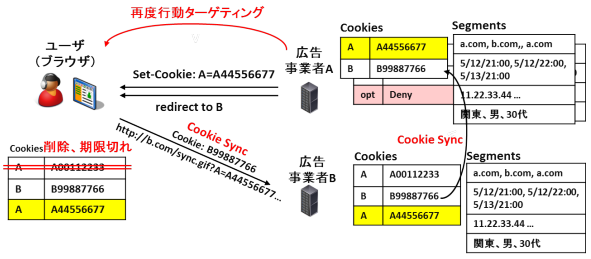

図 2: 再度行動ターゲティングが開始される例

B では以前のユーザだと認識され，B が保持しているユーザ情報が A と共有される．

このように，ユーザは A に対してオプトアウトを選択し，制御していても，再度 A によってオプトアウト以前と同じような行動ターゲティングが開始される可能性がある．

他のオプトアウト方式として DNT があるが，DNT はユーザの意思を表明する仕組みであるため，事業者が実際にトラッキングをやめる仕組みを実装しなければ，オプトアウトは実施されない．

また，Cookie 以外のユーザを識別する技術として Fingerprinting[5, 10] があるが，広告事業者からオプトアウトの機能は提供されていない．

結局のところ，現状のサードパーティにより提供されているオプトアウトは，ユーザの状況や目的に合わせた選択と制御ができるものではなく，ユーザがオプトアウトを維持していくことは困難である．

3 課題と研究の目標

2 節の議論により，現状の課題として下記の 3 点があげられる．

1 つ目は，不可視なサードパーティが多過ぎる点である．ユーザがファーストパーティにアクセスすると同時に，数多くのサードパーティにユーザ情報が取得され，共有される．そのため，ユーザがサードパーティの保持している情報と共有範囲を認識する負担は大きく，認識できていないものに対して，個別に選択し，制御することはさらに負担が大きい．

2 つ目は，ファーストパーティとサードパーティ全体でユーザの情報が共有される点である．

サードパーティに取得されたユーザが認識していない情報も，ファーストパーティに結合されるため，ファーストパーティが保持しているユーザの情報をユーザが認識できない状態となる．また，全情報が結合されるため，ユーザは状況（仕事やプライベート等）や目的（旅行情報やスポーツ情報等）を反映した選択と制御ができず，現状では，広告を受け入れるか，広告を完全に遮断するか，どちらかの選択となる．

最後は，サードパーティ主導でユーザ情報を取得，共有しており，オプトアウトの実施権限は最終的にサードパーティにある点である．自主規制等を導入しているが，実際にはサードパーティの実装に依存しており，オプトアウトの継続性には課題がある．

上記の課題を解決するため，我々は次の 2 つの実現を目標とする．

1. ユーザが，自身の提供する情報と，流通範囲を負担なく認識できるようにする．
2. ユーザ主導で状況や目的に沿った選択ができ，継続的に制御できるようにする．

4 提案

我々は目標を実現するため，下記の内容をブラウザ拡張機能として実装する．

1. ユーザが，自身の状況や目的別に，自身で生成した ID（以降，ugID と呼ぶ）と属性情報をサードパーティに提供することで，サードパーティに対する自身の提供情報，共有範囲の認識を強化し，自ら選択できるようにする．
2. ユーザは，ファーストパーティ，サードパーティがユーザに不可視な状態で，ugID と属性情報を結合することができないように制御する．
3. ユーザは，ugID に対して行われるサードパーティの情報取得を観測し，ユーザが設定した属性情報と対比することにより，ユーザがサードパーティの振る舞いを推定，評価する．

4.1 モジュールと機能

提案するブラウザ拡張機能の主要モジュールと機能は下記の通りである．

(a) ugID，属性情報の生成・変更モジュール

ユーザ主導で状況や目的に沿った情報の提供と共有範囲の認識，および選択，制御を行うため，下記の機能を持つ．1）ugID の生成，および属性情報，状況・目的の設定機能，2）独自の HTTP Header パラメータを送信する機能．

(b) ユーザ情報制御モジュール

サードパーティ主導でユーザ情報の取得と共有を行うことを制御するため，下記の機能を持つ．1）サードパーティ Cookie の送信制御機能，2）サードパーティへのファーストパーティ Cookie の送信制御機能，3) ファーストパーティへの ugID の送信制御機能，4）Fingerprinting の抑制機能．

(c) サードパーティ計測，評価モジュール

サードパーティの振る舞いを計測し，自身の設定との対比をするため，下記の機能を持つ．1）アクセス先と送信情報の収集機能，2）セグメント情報の推定，評価機能．

4.2 情報共有の定義

我々はユーザ主導の仕組みを提案するが，提案した仕組みに対してもサードパーティ主導による ID の結合が行われる可能性がある．ID の結合が行われた場合，ユーザ主導で設定した状況や目的に応じた制御が困難になる．そのため，ID が結合される場合を定義し，提案するブラウザ拡張機能では，ID の結合を制御する．

図 3 は，我々が提案する仕組みの概要である．ファーストパーティがユーザを識別する ID は，従来通りの Cookie の仕組みを利用する．サードパーティに対しては従来の Cookie による識別を禁止し，ユーザが状況と目的に合わせて生成した ugID と属性情報（S：図 3 では $S_{third_i,k}$ のように表記）を利用する．ユーザからの任意のトランザクション T は Cookie や ugID，属性情報等のその他の情報を含む集合とする．ここで，あるファーストパーティへのトランザク

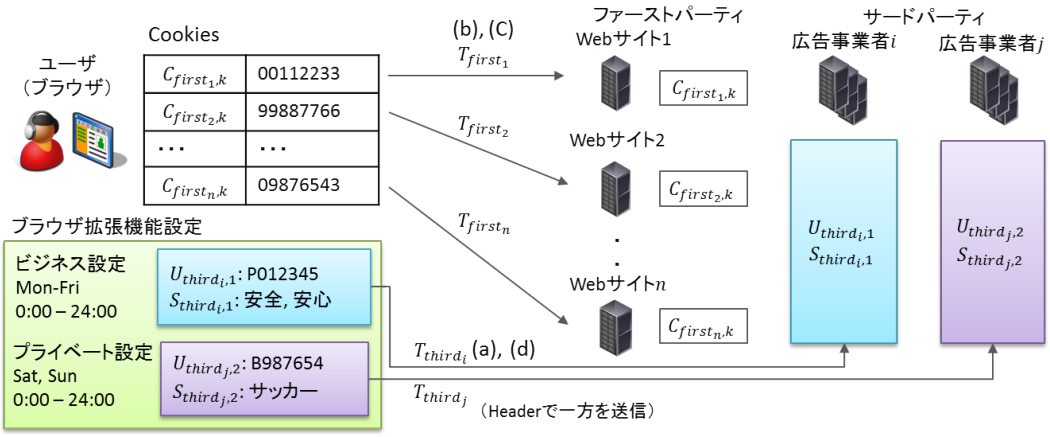

図 3: 提案するユーザ主導の仕組み

ションを T_{first_i} とし，あるサードパーティへのトランザクションを T_{third_i} とする．そして T_{first_i} 以外のあるファーストパーティへのトランザクションを $T_{first_j}(i \neq j)$ と表し，T_{third_i} 以外のあるサードパーティへのトランザクションを $T_{third_j}(i \neq j)$ と表す．あるファーストパーティが Cookie で持つ ID を $C_{first_i,k}$ とし，あるサードパーティが持つ ugID を $U_{third_i,k}$ とする．

ID の結合による情報共有は，ユーザからの 1 つのトランザクションで，各ドメインが持っている ID を同時に 2 つ以上送信し，既に各ドメインが持っている ID と送信された ID を結合することで実現される．下記の (a) から (d) は，情報共有が実現される場合である．提案する仕組みでは，下記の 4 つの場合を監視し，共有を制御する．

(a)　サードパーティへファーストパーティ Cookie が送信される場合

$\{C_{first_i,k}, U_{third_i,k}\} \subset T_{third_i}$ となる．例えば，$C_{first_i,k}$ を JavaScript で画像タグのパラメータに加えたり，iframe で呼び出し URI のパラメータに加えて，Cookie を送信する方法がある．

(b)　ファーストパーティへ ugID が送信される場合

$\{U_{third_i,k}, C_{first_i,k}\} \subset T_{first_i}$ となる．例えば，サードパーティが $U_{third_i,k}$ を Header で受け取り，JavaScript に埋め込んで，ユーザのブラウザで実行させて $C_{first_i,k}$ と共にファーストパーティに送信する方法がある．

(c)　ファーストパーティとして Cookie を設定したドメインがサードパーティとなってファーストパーティへ自身の Cookie を送信する場合

$\{C_{first_i,k}, C_{first_j,k}\} \subset T_{first_i}$ となる．

(d)　サードパーティへ他のサードパーティの ugID が送信される場合

$\{U_{third_i,k}, U_{third_j,k}\} \subset T_{third_i}$ となる．

5　考察

本節では提案した仕組みの効果と影響について考察する．また，情報共有の制御について考察する．

5.1　効果と影響

ユーザ，ファーストパーティ，サードパーティに対する，効果と影響を整理する．

(a)　ユーザへの効果と影響

ユーザへの効果として，3 節で示した目標の効果が得られる．また，ファーストパーティのページロードにおいてサードパーティ主導の Cookie Sync のトラフィック量の減少が期待できるため，ブラウジングが快適になると予想される．影響としては，ブラウザへの拡張機能のインストール，ugID の生成と属性情報の設定がある．しかし，現状の個別にサードパーティを認識し，選択するというユーザの負担を考慮すると，影響としては大きくないと考えられる．

(b)　ファーストパーティへの効果と影響

ファーストパーティへの効果として，ファーストパーティが把握できないサードパーティによる情報取得が軽減でき，より詳細な規約やポリシーの下，信頼されるサービスを提供できるようになると考えられる．影響としては，サードパーティのユーザ情報を容易に取り入れることが難しくなる．しかし，提案する仕組みで，ユーザの許諾により，情報共有を許可する機能を追加することも考えられる．

(c)　サードパーティへの効果と影響

サードパーティへの効果としては，ugID と属性情報を利用することにより，即座にユーザに適した広告を表示することができる点がある．また，現状ではサードパーティ Cookie をオフにされると，ランダム広告を出力するしかなく，また，広告ブロッキングツールが導入されると，広告を表示できなかったが，提案した仕組みでは，ユーザが望む広告を出すことが可能となる．影響としては，サードパーティ主導のユーザ識別，情報取得が難しくなる．しかし，ユーザ主導で生成された ugID を利用して，ユーザを解析することは可能であり，ユーザから提供される属性情報を参考に，広告を選択することができる．たとえ，ユーザが設定した属性情報が，本当のユーザの性質に沿わないものとなっている場合であっても，ユーザがその属性情報に関連するものに興味があると考えれば，広告を出稿する価値はあると考えられる．

5.2　情報共有の制御について

4.2 節では，情報共有の定義を 4 つの場合に分けて行った．情報共有はトランザクション T に 2 つ以上の ID が含まれる時に成立する．提案する仕組みでは，4 つの場合それぞれを監視し，情報共有を制御する．しかし，4.2(a)，(b) の場合に関しては，単純な Cookie 値や ugID 値による制御では限界があると考察される．

例えば，4.2(a) の場合では，JavaScript 等で $C_{first_i,k}$ に紐づく仮 ID（$C_{first_i,k}{}'$）をクライアントサイドで生成し，ファーストパーティとサードパーティに $C_{first_i,k}{}'$ を送信し，ファーストパーティとサードパーティ間で $C_{first_i,k}{}'$ で問い合わせを行うような方法が考えられる．

また，4.2(b) の場合では，$U_{third_i,k}$ を Header で受け取り，$U_{third_i,k}$ に紐づく仮 ID（$U_{third_i,k}{}'$）をサーバサイドで生成し，JavaScript に埋め込んで，ファーストパーティで実行させて $U_{third_i,k}{}'$ をファーストパーティに送信し，ファーストパーティとサードパーティ間で $U_{third_i,k}{}'$ で問い合わせを行うような方法が考えられる．

このようにブラウザで観測できない ID を任意に生成されると，拡張機能において Cookie 値や ugID 値により制御することが難しくなる．そのため，パラメータ名などを推測する機能や振る舞いを推測する機能等，さらに高度な機能が必要になると考えられる．しかし，5.1 節で考察した通り，提案した仕組みでサードパーティに十分な利点を提供できれば，サードパーティが ID を紐づける動機がそもそもなくなると考えられる．

なお，4.2(c) の場合は，サードパーティ Cookie を禁止するため，情報共有を実現することはできないと考えられる．また，4.2(d) の場合は，ugID を同時刻に 1 つしか送信しない設計とするため，T_{third_i} に ugID が含まれるならば，それは必ず 1 つだけになり，情報共有は実現しないと考えられる．

6　関連研究

本稿で提案するような，行動ターゲティング広告の選択や制御を促進する先行研究を示す．

Privad[8] では，ユーザ（ブラウザ）と広告事業者の間にディーラーと呼ばれるプロキシ事業者を導入することを提案している．プロキシがユーザのアクセスに対し，匿名の ID を生成することで，広告事業者に対し，ユーザの匿名性を保っている．

Adnostic[12] では，広告事業者がブラウザに対し 10 から 20 の広告候補を提供し，ブラウザ拡張機能がユーザの興味に沿った広告を算出して表示する仕組みを提案している．

Repriv[7] では，ブラウザ拡張機能内で，サードパーティがセキュアにマイニングツールを開

発できる仕組みを提案する．ユーザがポリシーを設定し，セキュアな API を通じてブラウザ内のユーザ情報にアクセスする機構を有する．

CoP[2] では，JavaScript で行動ターゲティングのキーワードを演算し，Cookie に格納する機能を提案している．

AdReveal[9] では，ブラウザ拡張機能でユーザのブラウジングログを解析し，行動ターゲティング広告のトラッキングスコアを算出している．トラッキングスコアに基づきカテゴリ別に制御しやすい環境をユーザに提供する．

前述の [8, 12, 7, 2] に関しては，既存の広告配信システムを大きく変更しなければならず，普及が難しいと考えられる．AdReveal[9] は，ブラウザ拡張機能のインストールのみで，ユーザにフレンドリーなシステムを目指しているが，ユーザ主導で広告を選択する仕組みではない．

本稿で提案する仕組みは，意図的に行動ターゲティング広告の機能を抑制するが，ユーザ主導で ugID と属性情報を提供することで，既存の広告配信システムを変更せずに，行動ターゲティング広告を許可する．そして，その中で行われるサードパーティ主導の行動ターゲティングをユーザが常に監視し，評価することを可能とする．

7　おわりに

本稿では，ユーザが自身の情報の利用と共有の範囲を容易に認識でき，ユーザ自身で ID を管理することにより，ユーザが提供する情報の選択と流通範囲の制御が可能な仕組みを提案した．

本稿で提案した仕組みは，ユーザだけでなく，ファーストパーティやサードパーティおよび，行動ターゲティング広告配信システム全体に有益であると考察した．

今後は，提案した仕組みの実装，並びに有用性の評価を行う．

参考文献

[1] AAAA, ANA, BBB, DMA and IAB. Self-Regulatory Principles for Online Behavioral Advertising, Jul 2009.

[2] Mikhail Bilenko, Matthew Richardson, and Janice Y Tsai. Targeted, not tracked: Client-side solutions for privacy-friendly behavioral advertising. In *The 11th Privacy Enhancing Technologies Symposium (PETS 2011)*. Citeseer, 2011.

[3] Data Driven Advertising Initiative (DDAI). オプトアウト（オプトイン）. `http://www.ddai.info/optout`. (accessed 2014.08.25).

[4] Digital Advertising Alliance (DAA). Opt Out From Online Behavioral Advertising. `http://www.aboutads.info/choices/`. (accessed 2014.08.25).

[5] Peter Eckersley. How unique is your web browser? In *Privacy Enhancing Technologies*, pp. 1–18. Springer, 2010.

[6] Federal Trade Commission (FTC). FTC Issues Final Commission Report on Protecting Consumer Privacy, 2012.

[7] Matthew Fredrikson and Benjamin Livshits. Repriv: Re-imagining content personalization and in-browser privacy. In *Security and Privacy (SP), 2011 IEEE Symposium on*, pp. 131–146. IEEE, 2011.

[8] Saikat Guha, Bin Cheng, and Paul Francis. Privad: Practical privacy in online advertising. In *NSDI*, 2011.

[9] Bin Liu, Anmol Sheth, Udi Weinsberg, Jaideep Chandrashekar, and Ramesh Govindan. Adreveal: improving transparency into online targeted advertising. In *Proceedings of the Twelfth ACM Workshop on Hot Topics in Networks*, p. 12. ACM, 2013.

[10] Keaton Mowery and Hovav Shacham. Pixel perfect: Fingerprinting canvas in html5. *Proceedings of W2SP*, 2012.

[11] Network Advertising Initiative (NAI). CONSUMER OPT-OUT. `http://www.networkadvertising.org/choices/`. (accessed 2014.08.25).

[12] Vincent Toubiana, Arvind Narayanan, Dan Boneh, Helen Nissenbaum, and Solon Barocas. Adnostic: Privacy preserving targeted advertising. In *NDSS*, 2010.

[13] インターネット広告推進協議会（JIAA）. 行動ターゲティング広告ガイドライン, 2014. (改定).