Vol.2020-GN-111 No.3
Vol.2020-SPT37 No.3
2020/5/14

国内ウェブサイトを対象とした同意管理プラットフォームの実態調査

坂本 一仁[1,a)]　室園 拓也[1]　太田 祐一[1]

概要：同意管理プラットフォーム (CMP: Consent Management Platform) とは，個人データに対する個人の同意を管理するためのソフトウェアまたはサービスである．2018 年 5 月から EU 一般データ保護規則 (GDPR) が開始され，Cookie のようなオンライン識別子およびそれらに紐づくウェブ上の行動履歴も個人データとして扱われることになり，今日では多くのウェブサイトに CMP の導入が進んでいる．しかしながら，EU や米国における CMP 導入ウェブサイトの推移は明らかになってきている一方で，日本国内における状況は不透明である．また CMP のユーザーインターフェース (UI) に着目し，サイト利用者の認知に関するユーザスタディや，UI が GDPR に準拠しているかといった研究は行われているが，利用者の UI 操作が真に CMP の内部挙動に反映されているかといった詳細な調査は行われていない．そこで本稿では以降に示す 2 つの Research Questions (RQ) に対応する調査を実施した．**RQ1**: 日本向けウェブサイトにおいて，CMP 導入は増加しているか？ **RQ2**: CMP サービスの挙動は正確であるか？調査は日本向けウェブサイト約 18 万 URL に対して実施され，調査の結果，日本においても特定の CMP サービスが増加傾向にあること，詳細設定機能が確認された CMP のうち，約 65%は利用者の UI 操作が正確に内部挙動に反映されていないことが判明した．

キーワード：同意管理プラットフォーム，Cookie，GDPR，実態調査

An Investigation of Consent Management Platforms in Japan

Abstract:
Consent Management Platforms (CMPs) are softwares or services that manage an individual's consent to personal data. With the launch of the EU General Data Protection Regulation (GDPR) in May 2018, online identifiers such as cookies and the behavioral history on the web associated with them will also be treated as personal data, and many websites are nowadays implementing CMPs. The introduction of CMPs has been clarified by research reports and studies, but the situation in Japan is unclear. On the other hand, user studies have been conducted on the user interface (UI) of CMP, such as user perceptions of site users and whether the UI complies with the GDPR, but there are no detailed studies on whether users' UI operations are truly reflected in the internal behavior of CMPs. In this paper, we conducted a survey corresponding to the following two Research Questions (RQs). **RQ1**: are CMPs adoption increasing on Japanese websites? and **RQ2**: is the behavior of the major CMP services accurate? The survey was conducted on about 180,000 URLs of Japanese websites, and it was found that the number of specific CMP services is increasing in Japan, and that about 65% of the CMPs that were confirmed to have advanced cookie settings did not accurately reflect the user's UI operations in their internal behavior.

Keywords: Consent management platform, Cookie, GDPR, Investigation

1. はじめに

インターネットを利用したウェブサービスの増加に伴い，デジタルマーケティングは急速に発展し，ほとんどのウェブサイトにウェブ広告，アクセス解析ツール，効果測定ツール，ソーシャルプラグインなどが組み込まれている．すなわち，ウェブサイトは多くの外部サービスと連動してサイト利用者へ情報を配信し，利用者のウェブ上の行

[1] 株式会社 DataSign (DataSign Inc.)
[a)] sakamoto@datasign.jp

動や広告クリックといった情報は，巨大テックベンチャーをはじめとした数多くの事業者が常用的に収集・利用をしている．一方，サイト利用者は自身のデータに関する十分な情報開示を受けることや，利用者主体での積極的な関与が難しく，昨今においても利用者にとって自身のデータの使われ方が不透明な状況が続いている．このような状況を鑑み，2018 年 5 月に施行された EU 一般データ保護規則（GDPR）[10] は，ウェブ上の行動追跡に利用可能なオンライン識別子（代表的なものとしては Cookie）も個人データとして扱い，個人データの利用に対して自由に与えられた明確な同意を必要とすること，利用者のデータを透明かつ公平な方法で合法的に扱うことなどを事業者へ求めた．GDPR は EU 域内の市民が対象ではあるが，ウェブサービスにおいては利用者の地域を限定することが困難なことも多く，EU 域外の事業者であっても GDPR への対応を基準として，利用者のデータを透明かつ公平な方法で取り扱う方針をとるウェブサービス事業者も少なくない．このような背景から世界的に導入が進んでいるものが，同意管理プラットフォーム (CMP: Consent Management Platform) である．

CMP は，ウェブサイト利用者へ主にオンライン識別子である Cookie に関して，どのような目的で Cookie を利用するのかを明示し，利用者が選択した許諾を同意状態として管理するためのソフトウェアまたはサービスである（図 1）．Ad Tech Insights の CMP 導入サイト数の調査 [2] では，英国と米国のトップ 1 万サイトを対象に調査が実施され，2018 年から 2020 年にかけて CMP 導入サイトは増加しており，2020 年第 1 四半期には英国で 20.8%，米国で 19.8%のサイトに CMP が導入されていたことを報告している．さらに IAB Europe の Transparency and Consent Framework (TCF) [14] では 75 の CMP サービスが公式に登録されており，IAPP の 2019 Privacy Tech Report[16] では，CMP サービスを含む 250 以上の Privacy Tech ベンダーが存在することを報告している．このような調査から EU や米国では年々 CMP の導入サイトは増加し，CMP サービス事業者も増えていることが伺えるが，日本向けのウェブサイトにおいて CMP の導入がどのように推移しているのかといった調査は実施されていない．

他方，GDPR 施行のタイミングから，CMP に対する調査研究も盛んに行われている．Kulyk ら [17] は，初期の CMP に対する利用者の反応をユーザスタディにより明らかにしており，大半のユーザは CMP を無視し，邪魔と感じるなどネガティブな印象を与えることが多いことを示している．Sanchez-Rola ら [23] は，CMP の UI 操作と Cookie の増減を調査し，ほとんどの CMP で拒否を選択しても Cookie が減少しないことを報告している．近年では Nouwens ら [21] が，CMP のユーザーインターフェース (UI) に着目し，GDPR の同意原則に準拠しているかを調査

図 1　CMP の表示例

しており，ほとんどの CMP は GDPR に準拠していないとしている．GDPR 準拠の同意は，GDPR 前文 (32)[10], [29] に記載されているように，利用者であるデータ主体に対して自由に与えられ，肯定的な行為で与えられなければならないものである．そのため，事前にチェックされた状態や，ウェブサイト利用の継続で同意とすることは，同意には当たらないことが，GDPR 前文 [10], [29] や GDPR の同意ガイドライン [11]，Information Commissioner's Office (ICO) のガイドライン [15] 等で明記されている．このように既存の調査では，CMP の UI に注目し，利用者の認知や GDPR への適法性を議論したもの，CMP の UI 操作と Cookie 数を比較したものが多い．しかしながら，CMP の内部的な挙動を詳細に分析し，その挙動が真に UI 操作と一致しているのか，利用者の UI 操作としては同意していない，または同意を撤回しているにもかかわらず，Cookie を利用したデータ取得が行われていないかを詳細に調査した研究は実施されていない．

世界的には CMP 導入サイトは増加傾向にあり，GDPR を基準とした利用者データの透明かつ公平な取り扱いを進める環境が普及し始めているが，日本においての状況が明らかでないこと，および UI や適法性の問題点は研究されているが，CMP の挙動の正確性が十分に調査されていないことに対応し，本稿では 2 つの Research Questions を解明することを目的とした．

RQ1: 日本向けウェブサイトにおいて，CMP 導入は増加しているか？

RQ2: CMP サービスの挙動は正確であるか？

本稿では日本の企業や組織が利用する IP アドレスによってホストされているウェブサイト約 18 万件を 2019 年 2 月から 2020 年 2 月の間の 12 ヶ月を対象に月次調査を実施し，CMP 導入サイトの推移を観測した．そして，代表的な CMP サービスが導入されているサイトを調査し，CMP の挙動が正確かどうかを手作業で分析した．本稿の調査によって得られた結果は，日本における CMP の現状を網羅的に把握し，問題点を明らかにすることで信頼される CMP の普及に寄与し，ウェブサイト利用者のプライバシーをより一層尊重していく活動に貢献することを期待する．

本稿で得られた主要な発見は以下の通りである．

1) 約 18 万件の日本向けウェブサイトを調査した結果，2020 年 2 月時点では 283 のウェブサイトに CMP が導入されていた．
2) 本調査で観測した CMP サービス全体では増加傾向にあ

るが，個別の CMP サービスで見ると，特定の CMP サービスが大幅に増加傾向にあり，他は増加していない．

3) CMP サービスの UI において設定機能が確認された 82 サイトのうち，約 65%は正確に動作していない CMP であった．

4) 日本向けサイトでは必ずしも GDPR 準拠である必要はないが，GDPR 準拠とみなされる可能性が高い UI を搭載し，内部挙動も正確に動作しいるサイトはわずか 12 サイトであった．

本稿の構成は以下のとおりである．2 章では RQ1 に対応した日本向けウェブサイトの CMP 導入に関する調査について報告する．3 章では RQ2 に対応した CMP の挙動調査の研究について報告する．4 章では国内 CMP の現状に関する議論を展開し，5 章では関連研究をまとめる，6 章にて本稿のまとめを行う．

2. RQ1: 国内の CMP 導入推移

本節では RQ1 に対応した調査として，日本の企業や組織が利用する IP アドレスによってホストされているウェブサイト約 18 万件を調査し，CMP 導入の推移結果を示す．

2.1 調査方法

国内 CMP 導入サイトの調査は，DataSign 社が提供する調査システム [4] を利用して実施した．この調査システムはウェブサイトが利用しているアクセス解析やソーシャルプラグインといった外部サービスを検出し，検出結果をデータベースに蓄積することができる．調査の流れを図 2 に示す．

(1) 調査者は対象の国内ウェブサイト URL リストを調査システムの処理サーバへ登録する．

(2) 処理サーバは複数存在するクロールサーバへ非同期に URL クローリングのタスクを割り振り，対象のウェブサイトをクロールする．この時，1 つのウェブサイトでは最大 10 リングまでクローリングし，ウェブサイトが利用している外部サービスを検出する．

(3) ウェブサイト毎に検出された外部サービスがクロール結果として保存される．

(4) クロール結果から CMP サービスが導入されているウェブサイトを抽出する．

国内ウェブサイトの URL リストはどこどこ JP の国内企業の 18 万件以上におよぶ URL リストを利用した．どこどこ JP のデータは，IP アドレスと地域や組織といった情報を紐付けた Geolocation Technology 株式会社が開発するデータベースである SURFPOINT^{TM} に基づいて構成されている [13]．本調査では，そのうちの IP アドレスと企業を紐づけたデータベースである SURFPOINT^{TM} BtoB に含まれるウェブサイト URL のデータを利用した．このデータは日本の企業や組織が利用する固定 IP アドレスを逆引きし，得られたホスト名を手がかりにウェブサイトにアクセスして確認されたものであり，日本向けのウェブサイトとして，調査対象とした．

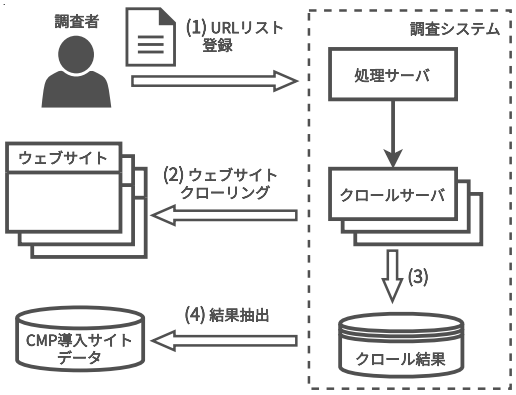

図 2 調査方法と結果の格納

また，本調査では対象とする CMP サービスは，本調査で利用した調査システムによって検出可能な下記に示す CMP とした．

- Cookiebot [3]
- CookiePro [22]
- Ensighten [8]
- Site Notice [12]
- TrustArc [26]

調査システムは，上記 CMP サービスが利用するドメインやパスに関する情報を保持しており，ウェブサイトのクローリングにおいてドメインやパスの出現からどの CMP サービスが利用されているかを判定している．

実際には，どこどこ JP の月毎の最新 URL データを利用して調査されており，月毎の外部サービス導入数などの調査結果は DataSign 社によって公開されている [5]．本調査では，2019 年 2 月から 2020 年 2 月まで 12 ヶ月（2019 年 10 月はデータ欠損）の調査結果から，上記 CMP サービスに該当する結果を抽出し，CMP サービスに関する月毎の導入サイト数を集計した．

2.2 調査結果

2019 年 2 月から 2020 年 2 月までの月毎の CMP 導入サイト数を，CMP サービス毎に図 3 に示す．CMP サービス全体としては増加傾向であるといえるが，各 CMP サービス個別に表示すると，OneTrust 社が提供する CookiePro が大きく増加している．Cookiebot に関しては少しの増加傾向が見られ，他の CMP サービスにおいては増加が確認できない．英国と米国の CMP 導入数を調査している adzerk の調査 [2] においても類似した結果が報告されている．このことから日本も含めた世界的に OneTrust 社の CMP サービスが多くのサイトへ導入が進んでいることが伺える．

2020 年 2 月では全体として 283 の国内ウェブサイトに CMP サービスが導入されていることを確認できた．2019

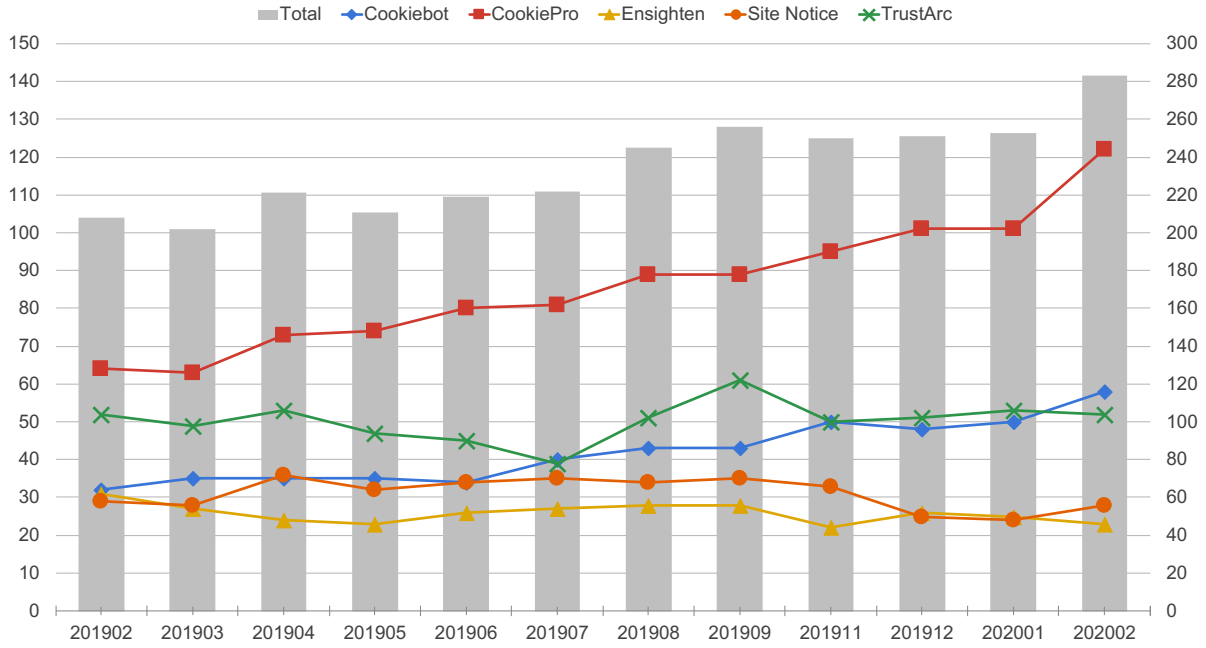

図 3 2019 年 2 月から 2020 年 2 月の間の国内ウェブサイト CMP 導入数の推移．
左軸は個別の CMP 導入数の目盛，右軸は Total な CMP 導入数の目盛．

年 2 月と比較すると，1 年で 75 サイトの増加である．日本における個人情報保護法においては，現時点で Cookie のようなオンライン識別子および，その識別子に紐付く行動履歴は個人情報として扱われていないが，海外からの流入が多いグローバル企業のウェブサイトを中心に，国内においても CMP の導入が増加していることが伺える．

3. RQ2: CMP の挙動調査

本節では RQ2 に対応した調査として，CMP の UI と内部挙動に着目し，UI の操作と Cookie が実際に利用されているかといった内部挙動の正確性について調査した結果を示す．

3.1 CMP の挙動

既存の CMP はオンライン識別子である Cookie 単位で Cookie の利用目的や利用ベンダーに対して同意を取得するものが大半である．これは GDPR が Cookie を個人データとし，自由に与えられた明確な同意のもとで Cookie に紐付くデータを処理することに対応している．

図 4 に既存の CMP サービスがどのように Cookie を管理し，UI 操作を反映させて Cookie の利用を制御しているかを示す．

(1) 管理者は CMP サービスを利用し，対象ウェブサイト（一般的に CMP を導入予定の管理者が所有するウェブサイト）で利用される Cookie を包括的に検出する．
(2) CMP サービスにおいて検出された Cookie を自動または手動で利用目的毎にグループ化された各グループへ分類する[*1]．
(3) 管理者はグループ化された Cookie の「Cookie グループ定義オブジェクト」と共に，CMP を対象サイトへ導入する．

この時点で CMP は対象ウェブサイト上で利用できるようになるが，CMP によって Cookie 利用を制御するためには，CMP が生成・編集する同意状態オブジェクト[*2]に格納されている同意状態[*3]を対象ウェブサイトに導入されているタグマネジメントサービスに連動させる必要がある．

(4) 管理者は対象ウェブサイトのアクセス解析タグや広告タグを管理しているタグマネジメントサービスにおいて，同意状態オブジェクトに格納されている Cookie グループの同意状態をタグ発火のトリガーとして設定し，該当するグループの Cookie を生成しているタグ発火を制御できるように連携する．
(5) CMP と連携したタグマネジメントサービスを対象ウェブサイトへ反映する．

以上のように管理者は CMP サービスによって検出された Cookie を正確にグループ化し，Cookie がどのタグから生成されているかを理解し，CMP サービスとタグマネジメントサービスを連動させることで，対象ウェブサイトで使

[*1] Cookie のグループ化を手動で行う場合，管理者は検出された Cookie の Name=Value から Cookie の利用目的を判断し，グループに割り当てる必要がある．
[*2] 同意状態オブジェクトは一般的に JavaScript のグローバルオブジェクトとして生成され，Cookie や localStorage に保存される．
[*3] 同意状態オブジェクトの同意状態は Cookie グループの ID が存在するか，同意状態のフラグが True か False かといった値によって判定される．

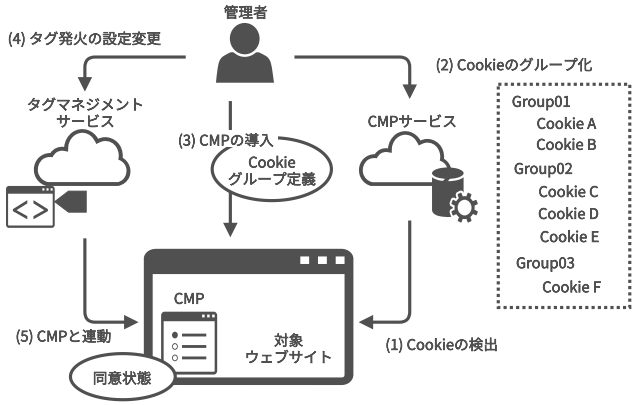

図 4 CMP の挙動（タグマネ連携型 CMP）

用されている Cookie を，サイト利用者の CMP に対する UI 操作によって正確に管理できるようになる．このような CMP を「タグマネ連動型 CMP」と呼ぶ．他方，CMP サービスとタグマネジメントサービスが一体となり，CMP 自体に広告タグなどを登録して制御するものも存在する．このような CMP を「タグマネ一体型 CMP」と呼ぶことにするが，本稿では調査の対象としない．

3.2 調査方法

前節で説明したような，現在多くのサイトに導入されている「タグマネ連動型 CMP」に関して，利用者の UI 操作によって正確に Cookie の挙動が制御されているかという観点から調査を実施した．

3.2.1 CMP の UI

2.2 節で示した CMP 導入サイトにアクセスし，代表的なタグマネ連動型 CMP の表示を手作業で確認する．そして，CMP の表示が確認されたウェブサイトにおいて，さらに下記にあげる既存研究で確認されているような 4 つ UI コンポーネントの内容について調査する．

- Cookie ウォールかどうか
- すべての Cookie を許可ボタンの有無
- すべての Cookie を拒否ボタンの有無
- Cookie の詳細設定ボタンの有無

Cookie ウォールとは CMP がモーダルポップアップとして表示され，CMP の操作をしない限りページの閲覧や操作ができないものをいう．GDPR においては同意は自由に与えられる必要がある [10], [29] とされているため，Cookie ウォールによる同意の強制は無効であるとされている．また，同意と同意の拒否または撤回は同じぐらい容易にできる必要があるとされており，すべての Cookie を許可ボタンと拒否ボタンは同じぐらいの操作粒度で存在する必要がある．さらに同意は利用目的毎に個別に与えられるものと解釈されているため，利用目的毎の詳細な内容が確認できる画面へ遷移するための詳細設定ボタンも重要である．本調査は，CMP の UI 操作と内部的な挙動を分析することが目的であるため，Cookie の詳細設定ボタンが確認された CMP について，次節の通り利用目的の初期設定を確認し，内部挙動を観測する．

3.2.2 CMP の初期設定と調査手順

Cookie の詳細設定が可能な CMP は利用目的毎にグループ化された Cookie を UI 操作により On/Off することで Cookie の利用に対して明確な同意，または同意の拒否・撤回を実施することができる．ここで CMP の初期設定の状態を 3 つに分類する．

- Optin
  - 必要な Cookie グループとして設定されているもの以外の Cookie グループが，すべて Off の状態である．
- Optout
  - Cookie グループが，すべて On の状態である．
- Hybrid
  - 必要な Cookie グループとして設定されているもの以外の Cookie グループに，On の状態のもの，Off の状態のものが混在している．

本調査では，具体的に CMP の挙動の正確性を以下の 2 つの観点で調査した．

(1) Optin や Hybrid などの初期状態が Off の Cookie グループの Cookie が，UI 操作で Cookie を許可する前に利用されていないか．

(2) Optout や Hybrid などの初期状態が On の Cookie グループの Cookie が，UI 操作で Cookie を拒否すると，正確に Cookie の利用が停止されるか．

(1) に関する調査は，いわゆるゼロクッキーロードの動きが実現されているかどうかである．GDPR 準拠の同意では，事前に On になっていない状態から，利用者の積極的な行動によって On にすることで同意が成立するとしている．しかしながら，CMP の UI としては事前に Off の状態で Cookie の利用が行われていない表示であっても，3.1 節で示したようにタグマネジメントサービスとの連携がうまくいっていないなど，ゼロクッキーロードが実現されていない可能性がある．

(2) に関する調査は，同意の拒否や撤回が真に実施されるかという調査である．GDPR 準拠の同意では，不利益を受けずに同意を拒否または撤回できなければならないとされているが，(1) で示したように，UI 操作によって同意の撤回が完了している表示であっても，内部の Cookie 利用が正確に制御されていない可能性がある．

本調査は，既存研究 [23], [25] で実施されているような，単純に Cookie 数をカウントするのみの調査ではなく，図 4 で説明したような，Cookie と利用目的の分類が定義されている「Cookie グループ定義オブジェクト」の内容，CMP が生成・編集して同意状態を格納する「同意状態オブジェクト」の内容と UI 操作に連動した挙動，さらに通信内容を詳細に分析する．例えば，ファーストパーティ Cookie

表 1　CMP の UI に関する調査結果

項目	ウェブサイト数	割合 (%)
CMP の UI 確認	97	-
Cookie ウォール	6	6.19
すべて許可ボタン	83	85.57
すべて拒否ボタン	3	3.09
詳細設定ボタン	82	84.54

表 2　詳細設定における初期状態と正確性の結果 ($N = 82$)

初期状態	#正確 (%)	#不正確 (%)	#合計 (%)
Optin (すべて Off)	12 (14.63)	12 (14.63)	24 (29.27)
Optout (すべて On)	12 (14.63)	35 (42.68)	47 (57.32)
Hybrid (混在)	5 (6.10)	6 (7.32)	11 (13.41)
#合計 (%)	29 (35.37)	53 (64.63)	82 (100.00)

として保存されているアクセス解析用 Cookie の Cookie グループを，CMP の UI を利用してオプトアウトした場合であっても，そのアクセス解析用 Cookie はファーストパーティ Cookie として存在し続けるが，サードパーティのアクセス解析用サーバへ Cookie の内容が送信されていないのであれば，正確に挙動していると言える[*4]．

3.3　調査結果

2 章の調査から発見した代表的なタグマネ連動型 CMP に関して，CMP の挙動の正確性を手動調査した結果を示す．本調査では国内ウェブサイトにおいて代表的な CMP サービスが発見できた 97 サイトの CMP を調査対象とした．まず表 1 に UI コンポーネントに関する結果を示す．ほとんどのウェブサイトの CMP が「すべて許可ボタン」を搭載している（85.57%）．また，Cookie に関する「詳細設定ボタン」もほとんどのサイトで確認ができた（84.54%）．一方で，「Cookie ウォール」の形態を取っているサイトは少なく（6.19%），「すべて拒否ボタン」が搭載された CMP も少ない（3.09%）という結果であった．Degeling らの調査 [6] では，「すべて許可」と「すべて拒否」が同じぐらい容易な UI（横並びで存在する UI）は 12.6%と報告されており，国内ウェブサイトではそれよりも低い水準の可能性がある．

次に「詳細設定ボタン」が存在する CMP に対して，初期状態と内部挙動の調査結果をクロス集計したものを表 2 に示す．結果として，CMP の UI 操作と連動して，正確にタグの発火条件が管理され，Cookie の利用が制限されているサイトは 35.37%であったが，CMP の UI 操作が正確に内部動作に反映されていないサイトは 64.63%と，不正確な挙動を示すサイトの方が多く存在した．また，初期状態で Cookie の利用がすべて On になっている Optout 式の CMP が大半を占めていた（57.32%）．本調査の対象は国内ウェブサイトであり，必ずしも GDPR 準拠が必要ではないが，GDPR 準拠の同意と考えられる Optin 式であり，かつ内部挙動も正確に動作しているサイトはわずか 12 サイトであった．

[*4] この場合は Cookie 数が変化することはなく，単純に Cookie 数の増減を観測するのみでは，正確にオプトアウトが実施されているかどうかを判断できない．

4.　議論

4.1　なぜ正確な動作が難しいのか？

既存の CMP 導入サイト数の調査や本調査からタグマネ連動型の CMP が多くのサイトに導入されていることが確認される．図 4 で示したように，このタイプの CMP を正確に動作させるためには，下記の困難な点が存在すると考えられる．

(1) 対象ウェブサイトにおける Cookie の正確な分類
(2) Cookie とタグの関係性の理解

CMP では，多くのサイトで利用されているアクセス解析などの特徴的な Cookie は，既知の Cookie としてデータベースに保持しているが，未知の Cookie はウェブサービス開発過程や，マイナーな第三者サービスを呼び出すタグの追加などで簡単に増加し，未知の Cookie が対象ウェブサイトに出現する可能性は高い．また，未知の Cookie の利用目的を正確に定義し，正確に Cookie グループに分類するためには，Cookie やウェブサービスに対する高い専門性が必要となる．このように Cookie の定義が困難なことから，CMP で管理されていない Cookie やその Cookie を生成する HTML/スクリプトタグが存在してしまっていると考えられる．

さらに，タグマネ連動型 CMP では Cookie グループに対する同意状態でタグの発火を管理する必要がある．しかし，該当する Cookie グループに属する Cookie が，どのタグから生成されているものかを理解していないと，同意状態によるタグ発火の制御が困難となる．また，1 つのタグから複数の第三者サービスを呼び出し，様々なドメインの Cookie が数多く設定される場合もあり，Cookie グループに対する同意状態を正確にタグの発火制御に反映することが困難と考えられる．

我々の調査から，大半の CMP が正確に動作していないことが判明したが，CMP の文言等に「同意ボタンを押したことで Cookie の使用を承諾」と記載しているにもかかわらず，内部的に不正確な Cookie の利用であると，同意の有効性が疑問視されることとなる．タグマネ連動型の CMP を導入する際は上記で示したような困難な点に注意し，基本的に必要最小限のタグと Cookie の利用を前提として，正確に Cookie グループに対する同意を内部挙動に反映させることが望まれる．

4.2　各法規制と CMP の実装

CMP は世界的に数多くのウェブサイトへ導入が進んでいる．本稿では GDPR 遵守の同意に対する CMP を基本として議論を展開してきたが，各国の法規制や業界団体ガ

イドラインによって，CMP の形態は様々である．EU においては GDPR 以外に，2009 年の ePrivacy 指令の改定から [9]，Cookie の利用をわかりやすく通知することが求められるようになり，以前から Cookie 通知としてウェブサイトに導入されてきた．GDPR 施行後は，同意状態の管理という目的も追加され，現状の CMP の形態になっていると考えられる．また GDPR へ準拠した運用型広告配信の実現に向けて，IAB Europe は同意状態を広告ネットワークに流通させるプロトコルとして TCP[14] を提唱しており，TCF v2.0 対応の CMP も増加している．

米国では，以前から広告業界団体の自主規制ガイドライン [1] により，行動ターゲティング広告に対するオプトアウトが実施されているが，2020 年にカリフォルニアにおいて，California Consumer Privacy Act (CCPA) [24] が施行され，Cookie に対する規制がはじめて州法となった．しかしながら，GDPR とは異なり Cookie 利用についてはオプトアウトが求められる水準に留められており，CMP は同意取得のツールではなく，オプトアウト情報を通知するツールとして普及してきている．

日本においては，個人情報保護法の改正が予定されているが，Cookie の利用について現行法でも改正案でも規制対象とはなっていない．しかしながら，改正案では Cookie 情報を第三者に提供する際に，提供先において個人情報となる場合については，提供先による同意が必要となり，その同意取得ツールとして CMP が注目されてきている．ただし，CMP によって対応できる範囲が狭いため法規制への対応ではなく，ウェブサイト利用者のプライバシーへの配慮として Cookie 利用をわかりやすく通知し，オプトアウトできるツールを導入することによるブランドイメージ向上の施策として期待されている．

最後に CMP の UI 実装では，ダークパターンとの関係が注目されている．ダークパターンとは，利用者の意図せず，選択を強制させる UI のことをいう [20]．既存の研究では，CMP のダークパターンに着目し，その影響をユーザスタディによって明らかにしている [19], [21], [27]．本調査において，ほとんどの CMP の UI は，「Cookie をすべて許可」ボタンのみが目立つようにハイライトされていた．ダークパターンによる選択の誘導が，GDPR が提唱している自由に与えられた同意にどのように影響するかは議論の最中であるが，利用者が正しく理解した上で，公平に選択できる CMP の普及が望まれる．

4.3 制限事項と研究倫理

本稿の調査は，どこどこ JP の国内企業 URL データを利用し，国内ウェブサイトを対象に調査を実施した．CMP の挙動調査に関してもサンプルは国内ウェブサイトのため，グローバルな調査は今後の取り組みとする．また，CMP サービスの検出は DataSign 社が定義している CMP サービスのドメインやパスに依存しており，定義されていないドメインやパスが存在する場合は，検出数が増加する可能性がある．

本稿の調査は，情報処理学会倫理綱領 [30] やサイバーセキュリティ研究における倫理的配慮のためのチェックリスト [28] を参考に，特定のウェブサイトまたは CMP サービスへのネガティブな影響を最小化するために，CMP の挙動調査における具体的なウェブサイト名および CMP サービス名は非公表としている．また，ウェブサイトのクローリング調査では 1 つのウェブサイトへの過度なアクセス負荷を避けるため，連続アクセスを抑制して，調査を行っている．

5. 関連研究

Cookie のようなオンライン識別子によるトラッキングの大規模調査はいくつか実施されている．Englehardt ら [7] は，100 万サイトをクローリングし，数多くのサイトでオンライントラッキングが常用的に行われていることを示した．Libert ら [18] は，GDPR 施行の前後で Cookie を使ったトラッキングに違いはあるかを調査し，彼らの報告では，調査した EU7 カ国の平均で，GDPR 施行後に 1 ページあたり 22%のサードパーティ Cookie の減少が見られたとしている．

CMP と Cookie に関する調査として，Trevisan ら [25] は，EU25 カ国における 25 カテゴリのウェブサイトを対象に，プロファイリング系の Cookie がサイト訪問時に利用されるかを調査している．彼らの報告としては，平均して 49%が事前同意なしの Cookie 利用であったことを示している．Sanchez-Rola らの 2,000 ウェブサイトに対する拡張機能を利用した手動調査 [23] では，92%のウェブサイトで Cookie によるトラッキング行われていること，CMP が存在するウェブサイトにおいて Cookie を拒否した場合，一部の Cookie が消去されるのはわずか 2.5%としている．

CMP の UI に対する初期の調査として，Kulyk らは CMP の記述文言について分類し調査を行った [17]．彼らの報告では，Cookie 利用に対する詳細な文言が，利用者のウェブサイト利用に影響を与えることを示唆している．Degeling らの CMP に対する調査 [6] では，EU28 カ国の CMP 導入率を調査しており，GDPR 施行後は 16 ポイントの増加が合ったとしている．また，CMP の製品やライブラリの機能，UI について詳細な分類を行っている．

CMP のダークパターンやナッジの影響を調査した報告が近年多く出てきている．Utz ら [27] は，クローリングで集めた 5,087 の同意通知から 1,000 をサンプリングして手動で UI を分類し，UI の影響についてユーザスタディを実施した．彼らの報告では，ボタン強調や事前チェックといったナッジは利用者の選択に影響があるとしている．Nouwens ら [21] は 680 の CMP 導入サイトを調査し，

GDPR 準拠の基準を設定して CMP が GDPR 準拠の同意を実施しているかを調査した．彼らの報告では，12.6%のサイトがすべて許可とすべて拒否が同じぐらい簡単であり，11.8%のサイトが GDPR 基準であったと結論付けている．また，8 種類の CMP デザインを利用したダークパターンの影響実験では，「すべて拒否」のボタンを設置しない方が「すべて許可」を選択する傾向が 22%増加するとしている．Machuletz ら [19] は，CMP のダークパターンに焦点を当て，4 つの仮説を検証している．結果として，「すべて許可」ボタンをハイライトしたものは，ハイライトなしと比べて 4 倍の影響があるが，必ずしも利用者が納得した上で選択しているものではないことを示唆している．

6. まとめ

本稿では，世界的にウェブサイトへの導入が進んでいる CMP に対して，「日本向けウェブサイトにおいて，CMP 導入は増加しているか？」「CMP サービスの挙動は正確であるか？」の 2 つの解明に取り組んだ．日本向けウェブサイト約 18 万件を 1 年以上調査した結果，日本おいても CMP 導入は増加傾向にあり，英国や米国の既存調査同様，特定の CMP サービスのみが増加してることが確認された．CMP の UI 操作と内部挙動を詳細に分析した結果からは，大半の CMP が正確に動作していないことが明らかとなった．さらに CMP を正確に動作させるための問題点について議論を展開した．CMP は利用者のプライバシーに配慮した重要な取り組みであるが，CMP の UI 上の文言や操作結果と，内部での Cookie を利用したデータ取得に齟齬が生じる場合，CMP の同意状態が疑問視され，サイト利用者からの信頼にも影響が出る可能性がある．本稿の結果が，利用者に自由に与えられた同意を提供し，正確に動作する信頼性の高い CMP の普及に貢献することを期待する．

参考文献

[1] AAAA, ANA, BBB, DMA and iab: Self-regulatory principles for online behavioral advertising, http://www.iab.net/media/file/ven-principles-07-01-09.pdf (2009).
[2] adzerk: Ad Tech Insights - Q1 '20 Report, https://adzerk.com/assets/reports/AdTechInsights_Aug2019.pdf (2020).
[3] Cybot: Cookiebot, https://www.cookiebot.com/en/.
[4] DataSign Inc.: DataSign FE, https://fe.datasign.co/.
[5] DataSign Inc.: DataSign Report, https://datasign.jp/tags/?tag=datasign\%20report.
[6] Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F. and Holz, T.: We value your privacy... now take some cookies: Measuring the GDPR's impact on web privacy, Network and Distributed Systems Security (NDSS) Symposium 2019 (2019).
[7] Englehardt, S. and Narayanan, A.: Online Tracking: A 1-million-site Measurement and Analysis, *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, ACM, pp. 1388–1401 (2016).
[8] Ensighten: https://www.ensighten.com/.
[9] European Union: Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (ePrivacy Directive), https://eur-lex.europa.eu/eli/dir/2009/136/oj.
[10] European Union: General Data Protection Regulation (GDPR), https://eur-lex.europa.eu/eli/reg/2016/679/oj.
[11] European Union: Guidelines on Consent under Regulation 2016/679 (wp259rev.01), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.
[12] Evidon: Site Notice, https://www.evidon.com/solutions/site-notice/.
[13] Geolocation Technology: どこどこ JP データ (SURFPOINT^{TM}), https://www.surfpoint.jp/btob/index.html.
[14] IAB Europe: Transparency & Consent Framework, https://iabeurope.eu/transparency-consent-framework/.
[15] Information Commissioner's Office (ICO): Guide to the General Data Protection Regulation (GDPR), https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies.
[16] International Association of Privacy Professionals (IAPP): 2019 IAPP Privacy Tech Vendor Report, https://iapp.org/resources/article/2019-privacy-tech-vendor-report/.
[17] Kulyk, O., Hilt, A., Gerber, N. and Volkamer, M.: 'This website uses cookies': Users' perceptions and reactions to the cookie disclaimer, *European Workshop on Usable Security (EuroUSEC)* (2018).
[18] Libert, T., Graves, L. and Nielsen, R. K.: Changes in third-party content on European news websites after GDPR, https://reutersinstitute.politics.ox.ac.uk/our-research/changes-third-party-content-european-news-websites-after-gdpr (2018).
[19] Machuletz, D. and Böhme, R.: Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR, *Proceedings on Privacy Enhancing Technologies (PoPETs)* (2020).
[20] Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M. and Narayanan, A.: Dark patterns at scale: Findings from a crawl of 11K shopping websites, *Proceedings of the ACM on Human-Computer Interaction*, Vol. 3, No. CSCW, pp. 1–32 (2019).
[21] Nouwens, M., Liccardi, I., Veale, M., Karger, D. and Kagal, L.: Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence, *Proceedings of the ACM on Human-Computer Interaction* (2020).
[22] OneTrust: CookiePro, https://www.cookiepro.com/.
[23] Sanchez-Rola, I., MatteoDell' Amico, Kotzias, P., Balzarotti, D., Bilge, L., Vervier, P.-A., Santos, I. : Can I Opt Out Yet? GDPR and the Global Illusion of Cookie Control, *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*, Association for Computing Machinery, pp. 340–351 (2019).
[24] State of California Department of Justice: California Consumer Privacy Act (CCPA), https://oag.ca.gov/privacy/ccpa.
[25] Trevisan, M., Traverso, S., Bassi, E. and Mellia, M.: 4 years of EU cookie law: Results and lessons learned, *Proceedings on Privacy Enhancing Technologies*, Vol. 2019, No. 2, pp. 126–145 (2019).
[26] TrustArc Inc.: TrustArc, https://trustarc.com/cookie-consent-manager/.
[27] Utz, C., Degeling, M., Fahl, S., Schaub, F. and Holz, T.: (Un) informed Consent: Studying GDPR Consent Notices in the Field, *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pp. 973–990 (2019).
[28] コンピュータセキュリティシンポジウム (CSS)2019 研究倫理委員会：サイバーセキュリティ研究における倫理的配慮のためのチェックリスト，https://www.iwsec.org/css/2019/ethics_list.html (2019). (参照 2019-08-20).
[29] 個人情報保護委員会：GDPR 前文仮日本語訳，https://www.ppc.go.jp/files/pdf/gdpr-preface-ja.pdf.
[30] 情報処理学会：情報処理学会倫理綱領，https://www.ipsj.or.jp/ipsjcode.html.