

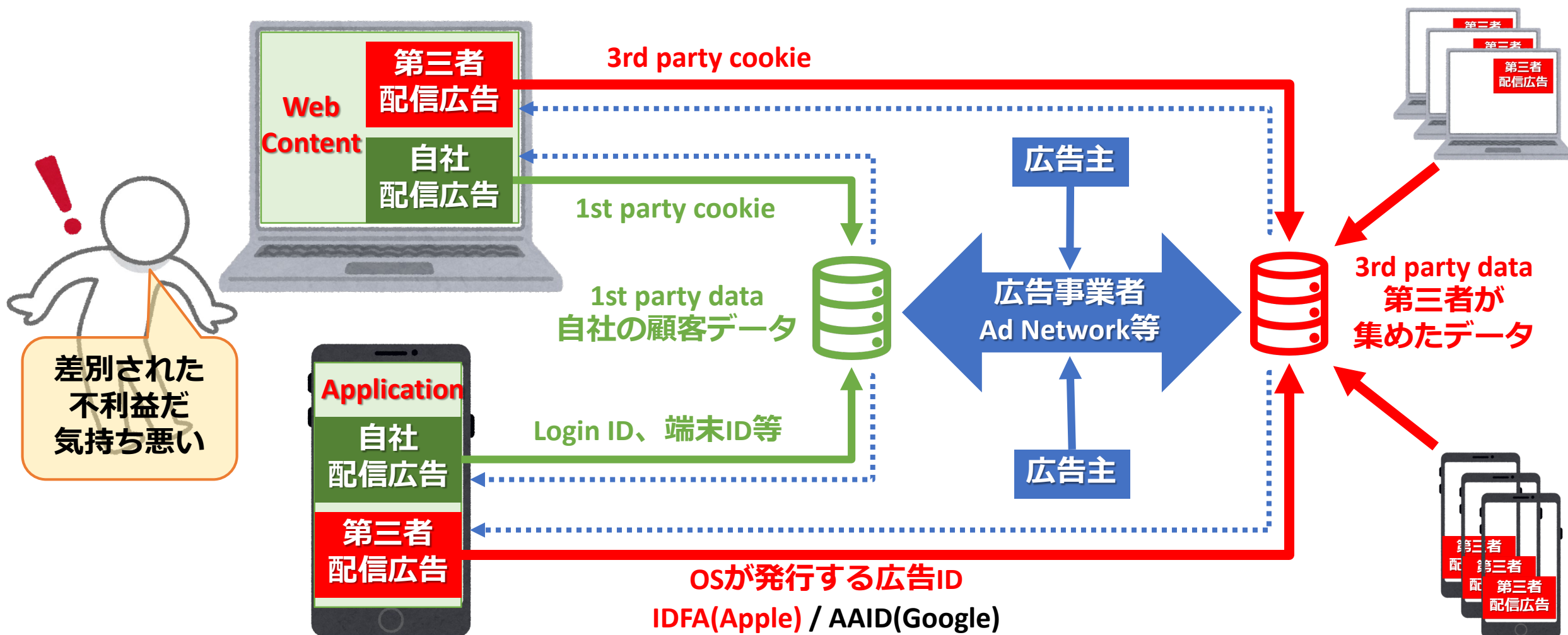
オンライン広告における 利用者情報取扱いの動向

一般財団法人 日本情報経済社会推進協会
主席研究員 寺田眞治

2021,4.22

本題に入る前に。。。。

問題意識の根幹は、Personal Dataをコンテンツやアプリ提供者以外が
ユーザーを特定もしくは識別し、サイトや事業者を越えて利用すること





cookieが使えなくなる
(cookieレス)

いいえ。使えなくなるのは、Web browserの**3rd party cookie**です。
1st party cookieは基本的に従来通り。

Appleでアプリの広告ID
(IDFA) が使えなくなる

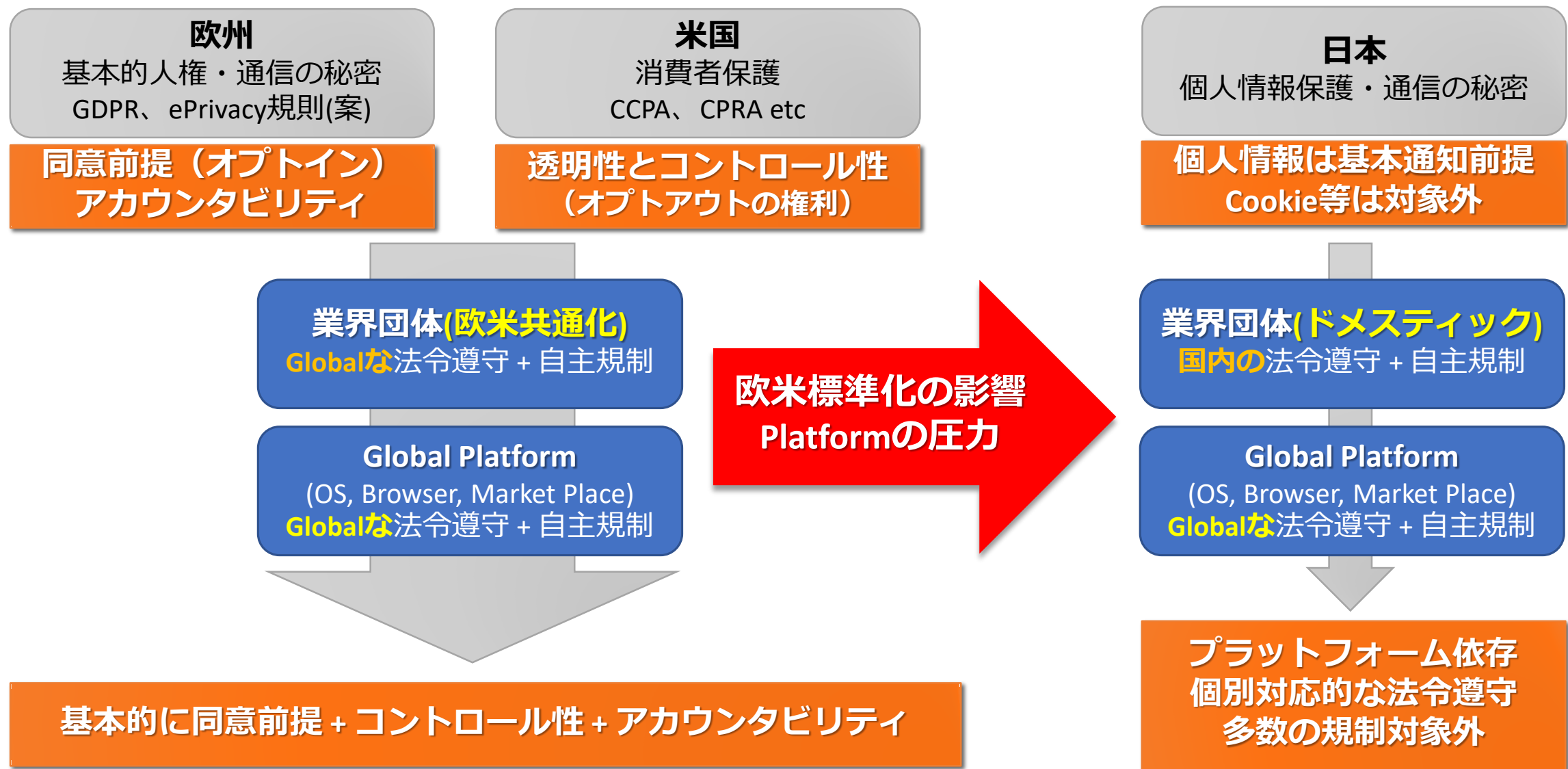
いいえ。広告IDを利用する場合に**同意が必須になることです**。
同意があれば、これまで通り流通・突合等が可能。

Googleでターゲティング
ができなくなる

いいえ。PCのWeb browserの3rd party cookieが**使えなくなるだけ**
で代替として**個人を特定しない集団としての識別子を準備中**。
1st party cookieも従来通り。

※GDPR、ePrivacy規則案では、Personal Dataとなる識別子（1st、3rdに関わりなく）は基本的に同意が必要。
CCPA、CPRAでは、透明性（説明）、コントロール性（開示等、オプトアウト等）の確保が必要

全体概要



欧米のオンライン広告に関する法制度の概要

背景

透明性とコントロール性に欠ける利用者情報の取扱いに対する不信と不安の増大。
特に技術革新によるオンライン広告の精度が高まることにより、企業に追いかけていることを消費者が認識できるようになったことから、プライバシー侵害への危機感が増大。

法制度



業界
団体

Global
Platform

広告主
事業者

欧州：Personal Dataの定義が広く、cookieをはじめ**端末内の情報の大半の取得には基本的に同意が必要対象として行動の監視**（行動履歴や購買履歴等）が含まれる（GDPR、ePrivacy規則案）



- ・同意取得に際しては具体的な利用方法等の説明が必要（透明性）
- ・説明内容について証明し責任を負わなければならない（アカウントビリティ）

※その他にプロファイリングを含む自動的処理のみに依拠した決定に服しない権利がある
また、DSAではプラットフォーム事業者に対して広告の透明性を求めている

米国：消費者保護の観点から、**個人情報を取り扱うにもかかわらずプライバシーポリシーを公表しないこと、あるいはプライバシーポリシーに反する行為を行うことは「欺瞞的行為」**（FTC法第5条）
不動産、雇用等では機会の平等、差別・不利益の排除の元にターゲティングが規制されている
（プライバシー保護の連邦法がないため、包括的な州法やセクター法による様々な規制が乱立）



- ・CCPA：通知の義務（透明性）
開示請求権、削除権、販売に対する停止権（コントロール権、オプトアウト権）
- ・CPRA：共有の停止権（コントロール権、オプトアウト権）

欧米の最も厳しい法制度（GDPR、CCPA等）に対応するため
自主規制の規格策定とこれを実現するためのツールの技術仕様を開発

法制度



業界
団体

Global
Platform

広告主
事業者

Transparency & Consent Framework v2.0 (TCFv2.0)

欧州インタラクティブ広告協議会（IAB Europe）とIABテックラボ（IAB Tech Lab）は、主にパブリッシャーとアドテクベンダーを対象として、**GDPRに準拠しながら従来からのプログラマティック広告** **を利用し続けられるようにするための業界標準規格**を2016年に策定、2019年v2.0に改訂。

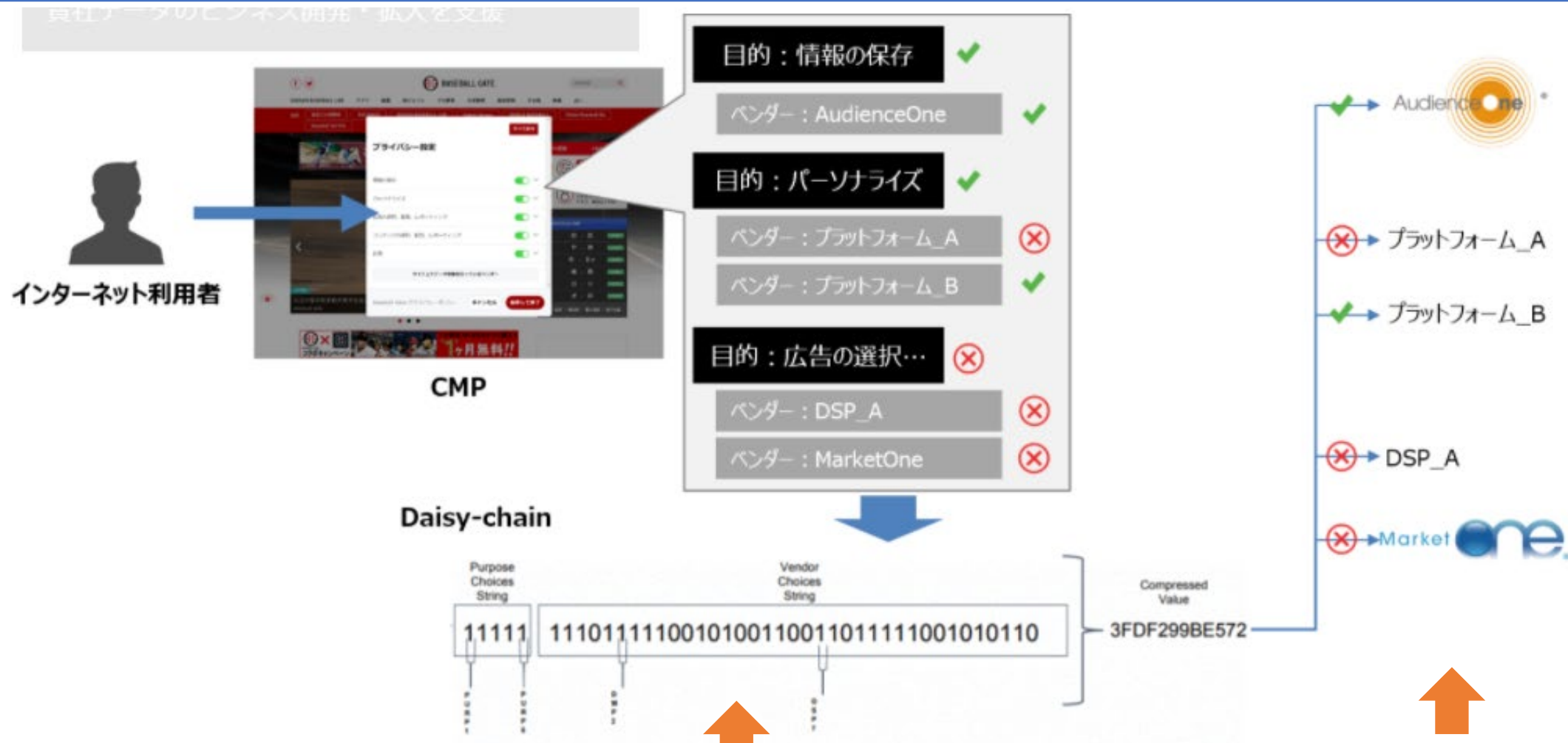
Consent Management Platform (CMP)

Webサイトやアプリ上で**ユーザーのデータ取得や利用に関する情報を提供し同意を得るためのツール**。**TCFに準拠した業界標準の技術仕様はIAB Tech Labが開発し、採用企業の登録等の運用**を行っている。自身のデータがどのような目的（広告の最適化、レポーティング、コンテンツ配信、計測など）で、どの3rdパーティベンダー（アクセス解析ツール、広告プラットフォーム、DMP、タグマネジメントツール等）に提供されているかが把握できる。自身のデータが使われて欲しくない場合は目的やベンダーごとにデータ提供を止めることができる。

※TCFに準拠していないものもCMPと称しているため、注意が必要

元々3rd party cookie利用の適正化が主眼であったが、現在は全てのPersonal Dataを対象とすることができる

(参考) IAB TechによるCMPの概要



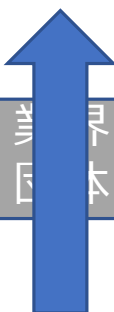
出典：DACの資料を基に筆者作成

何について同意または拒否したかが記録され、ベンダー間で流通する

データにアクセスできるベンダーは登録されており、同意取得のステータスに従って対応する

欧米の最も厳しい法制度（GDPR、CCPA等）に対応するため
自主規制とこれを実現するためのソリューションを開発

法制度



Global
Platform

広告主
事業者

Apple

iOS 14.5(Mobile) : プライバシー保護機能の強化（ATT : App Tracking Transparency）により、**広告ID（IDFA : Identifier For Advertising）を利用する場合にはユーザー同意が必須**となる

Safari(PC/Mobile) : ITP(Intelligent Tracking Prevention)により**3rd party cookieをはじめクロスサイトトラッキングをブロック**。1st party cookieについても制限有（有効期限等）

App Store(Mobile) : アプリケーションによって収集するデータの詳細な取得・用途の開示を義務付け

Google

Chrome : 3rd party cookieの段階的な廃止（2022年に完全廃止）し、自社の広告商品においては**ユーザーレベルIDを採用しない**

Google Play(Mobile) : 規約の改定により徐々に透明性と同意に関する規制が強化。広告・分析利用は広告ID以外では禁止、また個人を特定できるまたは永続的なIDとの関連付けには同意が必須

Web Browserのすべてで3rd party cookieは利用できなくなる
Mobile Applicationでは、Platformが用意する識別子以外は禁止

既存の広告ビジネスへの批判への対応
一方で独自のルールメイキングによるビジネスの独占との懸念

法制度

Apple

ATT(Mobile Apps) : App Tracking Transparency Frameworkによる同意に基づくIDFAの利用
SKAdNetwork(Mobile) : 広告を掲載する媒体やアドネットワークがAppleの連携パートナーになることによって、アプリのインストールが発生した際に通知を受け取ることが可能になる（アプリ内のみ、一定時間内、誰がではなくどの媒体かがわかるだけ等制限が多い）

業界
団体

Google (Privacy Sandbox Project)

FLoC(Browser) : Federated Learning of CohortsはローカルのChrome Browserの中で行動履歴をAIによって分析し、同種の興味関心を持つ人を数千人のグループ（コホート）としてターゲティング広告の対象とする。
FLEDGE(Browser) : First Locally-Executed Decision over Groups Experimentは広告のオークションを「（第三者の）信頼できるサーバ」にて行うというもの。

Global
Platform

広告主
事業者

Appleの仕様は従来のモデルについて「同意取得」を強制するもの
Googleは個人レベルのTrackingを排除しようとするもの

アドテク企業、パブリッシャーによるGlobal Platformへの対抗動向

上に政策あり、下に対策あり
Platformによる支配への抵抗

法制度

代替ID

Unified ID 2.0 : Trade Desk社が策定した**暗号化したメールアドレスをIDとするもの**で、利用方法自体は3rd party cookieとほぼ同じ。（取得と利用に関しては同意の取得を前提としている）

Device Fingerprint : **端末内の様々な情報を取得してIDとするもの**。端末搭載の機能、ソフトウェア、設定等が異なることを利用して同一端末であることを確認しようとするもの。

業界
団体

1st party cookieの活用

これまで3rd party cookieに頼っていたパブリッシャーが、1st party cookieによるターゲティングを重視すると同時に1st party dataを連携したDMP（Data Management Platform）によるメディア横断を模索。

Global
Platform



広告主
事業者

Contextual Targeting

ユーザーが閲覧しているWebページをAIで分析し、コンテキストに合致する広告を掲出。

事業者は法制度対応より、Global Platformによる規制への対策に重点が移っている
法規制はあいまいな部分が多く事前調査等もあるが、Platformによる規制は施行と同時に影響を受けるため

対策に対する対策 一方で、アーキテクチャの再構築を図る動きも

法制度

代替IDに対するGlobal Platformの対策

- Apple : Device Fingerprintは規約にて禁止（技術的な対応も随時）
Google : User Level Trackingに反対（自社商品では採用しないが、それ以外については不明）

業界
団体

Architectureの再構築

Project Rearc : IAB Techが中心になってオンライン広告におけるプライバシー保護と広告ビジネスの共存を図るArchitectureの再構築をめざしたプロジェクト（3月意見募集草案発表）

※Global Privacy Platform(GPP) : TCFv2.0をベースに各国の規制に対応する規格

Accountability Platform : 同意や設定を広告サプライチェーン全域で監査可能にする仕様(PRAMと共同策定)

PRAM : Partnership for Responsible Addressable Mediaは、Unified ID 2.0を主導するアドテク企業と全米広告業協会（4A's）、全米広告主協会（ANA）、インタラクティブ広告協議会（IAB）等により、代替IDの基準等を策定中。

広告主
事業者

Global Platform対アドテク企業といういたちごっこ
業界全体として調和を図ろうとする動きが同時並行

ターゲティングにおける争点のポイント

ターゲティングの何が問題なのか
個人の特定/識別、クロスサイト、同意の質。。。

ユーザーレベルID：特定もしくは識別された個人を対象とすることの是非

各国の法規制においても、**有効な同意**があれば規制されるものではないというのが原則。

AppleはIDFAについては法規制の原則に準じる方向性だが、**IDFA以外のユーザーレベルIDは禁止する方向**。

Googleは**ユーザーレベルID自体を禁止**する方向（少なくともMobileを除く自社商品内においては）

クロスサイト・トラッキング：ドメインを越えて情報を共有することの是非

法規制の原則では**有効な同意**があれば規制されるものではない。

Appleは法規制の原則（**同意前提**）に準ずる。（ただし利用できるのはIDFAのみ）

Googleは**ユーザーレベルIDでなければ規制していない**（Chromeにおける他社商品利用については不明）

有効な同意：定義、有効性の持続期間と流通範囲、「処理/加工＝突合/融合/拡張」の同意可否

- ・ 1st partyにおいて同意取得されたデータについて、一定程度具体的な広告利用が同意されたとしても、どのように処理/加工され、どこまで流通してさらにどのような処理/加工されるかが不明でよいのか？
- ・ Web Browser内であってもPersonal Dataを利用して個人を識別しない集団識別IDを生成する場合は利用について同意が必要か、集団識別IDはPersonal Dataかが不明（自動処理に服しない権利との関係も不明）

ターゲティングが失われることによる留意事項

効果の低下による広告枠単価の低廉化
同等の効果を得るためには広告量を増大



広告枠の増加

広告の収益低下によるコンテンツ有料化



情報格差、ネットリテラシー格差の拡大



実際に起こるのかは不明

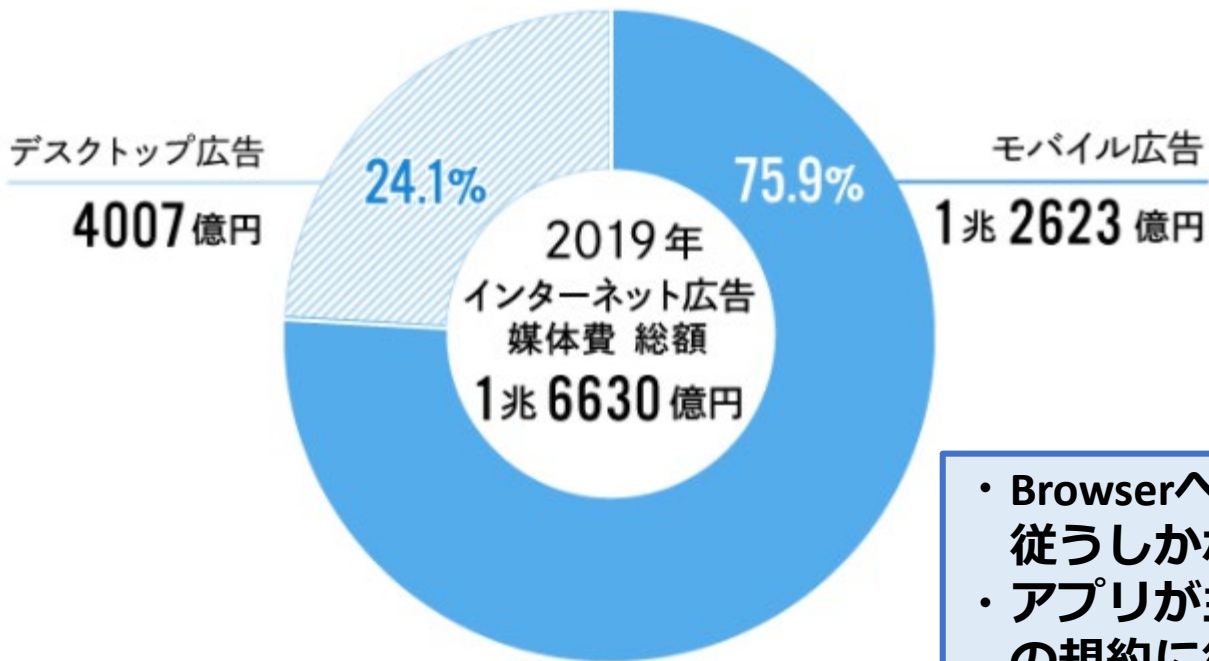
無差別化により、不快な広告の露出増加や青少年への有害広告の露出



**コンテキストベースでの対策は可能だが閲覧時の興味関心でしかないので
対象者属性をはじめ精度はかなり落ちる**

デスクトップとモバイルと新たな広告ビジネスの台頭

インターネット広告媒体費のデバイス別構成比（参考値）



<https://dentsu-ho.com/articles/7227>

デスクトップ

Browserによる3rd party cookie禁止で統一

モバイル

Apple : iOSは広告ID取得の同意必須

Safariは3rd party cookie禁止

Google : Android OSに特段の規制は無し

アプリによる情報取得はMarket Placeの審査に依存
→ 規制は強化されており、情報取得は同意前提、
透明性やコントロール性等も必須になる方向

- Browserへの広告配信が主流のデスクトップでは、Browserの制限に従うしかなく、3rd party cookieは事実上終焉を迎える
- アプリが主流のモバイルはAppleとGoogleの技術仕様とMarket placeの規約に従うしかなく、Platform規制の強化により規制はさらに進む
- **SNS、ECサイト、動画内の広告等は、Platform事業者による1st partyとしての膨大なデータ収集があるため、3rd party cookie禁止の影響は小さく、むしろ好機と考えて自社経済圏における広告事業を拡大中。ただしPlatform間の連携が困難であるため、これらの間を橋渡しする1st/2nd party dataによるアドテクの興隆が预言されている**

我が国における広告業界の対応

日本

1. 国内の法令、ガイドラインの遵守



個人情報の取得・利用は通知または公表

2. 個人情報以外のPersonal Dataは自主規制



cookieポリシーの公表、オプトアウトの推奨等
※UnifiedID2.0、Device Fingerprintは国内法では
個人情報に該当しないことを前提に個社判断

3. Global Platformへの明確な意見表明はない



海外の団体、プロジェクトには参加し情報収集

欧米

広告に関連するPersonal Dataのほぼすべてで

- ・取得/利用には同意が必要
- ・Personal Dataの透明性確保にcookieも包含
- ・利用者によるコントロール性確保にcookieも包含

Global Platformへの牽制、対抗は、規制当局だけでなく、国内外の広告関連団体、消費者団体、研究機関等、広範囲なステークホルダーが連携。

日本はプライバシー保護や消費者保護の概念よりも国内における**コンプライアンスを重視**
Global Platformに対して対等なポジションではなく、むしろ依存する傾向がみられる

広告配信先の爆発的増加、アドテクノロジーの急激な進化にともなう
広告配信経路の多様化、複雑化、リアルタイム化が管理不全を引き起こしている

ブランドセーフティ (Brand Safety)

インターネット広告の掲載先に紛れ込む違法・不当なサイト、ブランド価値を毀損する不適切なページやコンテンツに配信されるリスクから広告主のブランドを守り、安全性を確保する取り組み。

アドフラウド (Ad Fraud)

自動化プログラム (Bot) を利用したり、スパムコンテンツを大量に生成したりすることで、インプレッションやクリックを稼ぎ、不正に広告収入を得る悪質な手法。

ビューアビリティ (Viewability)

広告の視認可能性。

出典：日本インタラクティブ広告協会のインターネット広告基礎用語集2019年度版より

利用者情報取扱いの適正化によって解決されるのか？

不適切な露出のメカニズムに対して有効か？

Contextual Targetingが進展すれば、配信先コンテンツの内容を確認することになり、不適切なコンテンツへの配信は抑制される可能性がある。（ニュースサイトではなく政治家の「不適切な発言」にも対応できる）

欧米の業界団体による利用者情報の取扱いに関する取組（TCF、CMP、データ透明性ラベル※等）により、配信経路の各事業者の登録やプライバシー保護意識の向上が進むことで、健全化への取組みが期待される。

Platformへの規制に伴う広告ビジネスの透明化要求は、違法なビジネスの排除や適正な指標の確立への圧力となるとも考えられる。

その一方で、アドフラウドは意図的にシステムの脆弱性を狙ったり、悪用するなど技術的に巧妙化しており、異なるアプローチが必要。

不可視領域への
広告露出

※データ透明性ラベル（Data Transparency Label）：IABのテックラボ（Tech Lab）により、どのデータを誰から購入するかを決めるのに必要な情報を広告主が見つけやすくすることを目的に策定