参考資料9

第22回会合における構成員等からのご意見

２０２１年２月２５日

事　　務　　局

第22回会合における構成員からの主なご意見①

個人情報とプライバシー保護	■ 個人関連情報が個人情報になる前のウェブの閲覧履歴とその分析の情報等について、個人情報保護法、取引引透明化法、消費者優越、電気通信事業法等のうちどれでカバーするかという話について検討が必要。【森構成員】 ■ 個人情報になっていないものは個人情報保護法でというわけにはいかない。個人情報保護法は、令和２年改正で個人関連情報を導入しており行けるところまで行っており適切な改正がされている。取引透明化法は、取引透明化法の枠組みがあり、閲覧者の閲覧履歴を収集する、取得する場面において、消費者・閲覧者に対して一定の何か表示をしたり同意を取る等について義務づけられるような立てつけの法律ではない。消費者優越についてはまだなかなか具体的な法執行の段階に至っていないということもあり、やはりここをカバーできるのは電気通信事業法だけであると改めて認識する。ウェブサイト、ファーストパーティーのところでクッキーやフィンガープリントやそういったものについて情報を取得する行為、タグを設置して情報を取得する行為等については、それをカバーして規律するのは電気通信事業法であるのだと考えられる。【森構成員】
ウェブサイトにおけるCookie等の実情について	■ First Party CookieとThird Party Cookieがあり、Third Party Cookieには、SNS事業者、広告事業者、アクセス解析事業者、データ仲介事業者等に情報を送信するものが多く見られる。SNSのIDが付番されSNSアカウント情報と紐付けられ、取得されたデータは個人データになる可能性があるため、設置サイトの運営者が利用者に周知する必要があることが個人情報保護委員会から注意喚起されている。【DataSign太田氏】 ■ Third Partyによる情報取得の方法として、従来はイメージタグ（イメタグ：１ピクセルの見えない画像）をウェブサイトに貼ってCookie、IPアドレス、閲覧ページURL等を取得していたが、今はJavaScriptのタグ（JSタグ）が主流。イメタグより多くの情報取得（ページに表示される情報や入力される情報等も取得可能）やページ操作、他のJSタグの強制的読込み等も可能となっている。ウェブサイト運営者も知らないうちにJSタグがどんどん増えて制御困難な場合もあり、事業者間でID連係（Idsync）等がされる場合もある。【DataSign太田氏】

第22回会合における構成員からの主なご意見②

プラットフォーム事業者の最近の動きと対応	○ プラットフォーマーの提供するブラウザでThird Party Cookieによるトラッキングが制限され、2021年以降アプリにおけるIDFAの利用に同意が必要となり、Privacy Sandbox等の提案もある。一方、Canvas Finger Pringing等の別の手法や、同意を取得した上でメールアドレスに基づく情報やIDによるトラッキングを検討する動きもある。業界としてフィンガープリントやメールアドレスベースのトラッキングについてはオプトアウトの仕組みを準備することにより対応しようとしていると認識しているが、オプトアウトの信頼性の問題はある。【DataSign太田氏】 ○ Third Party Cookieはセキュリティやプライバシーを守るために使われる例もあるが、プライバシーを侵害する使い方が注目され全部やめるという風潮になっており、この辺りは結構慎重に扱うべきなのかと思う。Cookie等についてもプラットフォーム事業者が大きな力を持ってしまっており、競争法的な考え方というのも頭の片隅に入れておく必要がある。【崎村構成員】 ○ メールアドレスベースのIDについては、メールのリサイクル問題があり、間違ったプロファイリングがされてしまう可能性があることをちょっと危惧している。【崎村構成員】 ○ 固定的IDは問題という議論を経てリフレッシュできるIDFA等が導入された流れがある。一方、ブラウザーフィンガープリントやUnified ID2.0等がメールアドレスベースという時に簡単に変えられないと思うが、それは業界的に許容されるのか。そのようなIDを作ることをオプトインで同意する人が想定されるのか。色々なところで使っているものを一斉にオプトアウトすることは難しいのではないか。【森構成員】 ○ Unified ID2.0等についての一番根本的な違いは、最初に同意を取るか取らないかということ。本当にこれが業界でちゃんと話しをして、同意を取るというのを誰でも分かるような仕組みとか形にすれば、ある意味理想的な最初の入り口になると思う。オプトアウト系の問題は、データが流通していく中で、CMPといった仕組みで最後まで徹底的にトラッキングできるのどうかとのせめぎ合いが起きる。徹底的なトラッキングができれば、ちゃんと仕組みを作れば、オプトアウトとかも必要なところでできるということになるが、もう一方で、徹底的なトラッキングができてしまうことがいいのか・悪いのかという問題も起きているのは事実。業界だけではなく、消費者などの中でも、何が許され、どこまでは危ないか等の一種の線引きをしないと難しいと思う。【寺田構成員】

第22回会合における構成員からの主なご意見③

プライバシーポリシーについて	■ ウェブサイト管理者が実情を把握しにくく、プライバシー・ポリシーをきちんと書けていないサイトが多い。例えばSNSのIDは個人データと紐付く場合も多いが、多くのサイトでcookieが個人情報と紐付くことはないと記載している。また多数の事業者にデータを送付しているがその旨の記載がない事例も多い。【DataSign太田氏】
海外におけるプライバシーポリシーや同意取得に係る工夫	■ GDPRの通知・同意取得に当たって推奨される方法や留意すべき事項は、透明性と同意のガイドラインにおいて解説されている。GDPR第12条「簡潔で、透明性があり、理解しやすく、容易にアクセスできる方式」の実現のためにガイドラインで示された推奨される通知方法・工夫の例として、階層的なプライバシーステートメント、丁寧な説明、公開討論・消費者テストの実施、トップページからのタップ数等がガイドラインで示されている。ICOにおいて推奨される通知・同意取得における工夫は、①階層的アプローチ、②ダッシュボード（この延長としてCMP等もある）、③ジャストインタイム、④アイコン、⑤モバイル及びスマートデバイスの機能性の５つの手法である。【NRI南島氏】 ■ 欧州においてGDPR及びePrivacy指令に基づきCookie取得に際して同意が求められている。ICOガイドラインにおいて、Cookie取得に同意しないとウェブ画面を閲覧できない同意画面（クッキーウォール)や黙示の同意、デフォルトオンは認められないとされている。CNILガイドラインにおいても、階層的な表示が有効とされ、同意取得に当たり個人を誘導することがない形が推奨されている。【NRI南島氏】 ■ CCPA規則においては個人情報の収集やオプトアウト権に関する消費者への通知はプライバシーポリシーとは別に消費者への通知が必要とされる。例えば、個人情報の収集に係る通知内容は、収集する個人情報の種類、利用目的、オプトアウトページのURL、プライバシーポリシーへのリンク等とされる。【NRI南島氏】 ■ NIST Privacy Frameworkに係るSP800-53文書において、同意や通知に関する具体的に推奨される手法として、Tailored Consent、ジャストインタイムの同意、同意の撤回などICOやCNILと同様の工夫が示されている。【NRI南島氏】 ■ CPRAにおいて「共有するな」ボタンの義務化があり、Do not tracking2.0という言われ方をしている。そういう仕組みの提案がある。【寺田構成員】

第22回会合における構成員からの主なご意見④

同意の位置付け（続き）	■ スマートフォンが使われ始めた頃に総務省の会議でどれだけ情報取得がされているかという発表を聞き大変驚いたが、その実態がほぼ変わっていない状況で、利用者にとって何となく情報が取得されているのかなと思いつつそうしないと使えないというはかりにかけたようなバランスで使っている。同意画面については、とにかく分かりにくい。消費者としては使いたいほうが先で、細かくて分からないだろうしと思い、そのまま同意してしまうというのが正直な気持ちである。Consent Reciptのように、自分が何に同意しているか分かることは大変大切だと思う。【木村構成員】 ■ プラットフォーム研で通知と同意の検討をすることは非常に重要であり、世界的にもそういう認識があるから色々なところで同意に関するガイドラインが出てきて同意の有効性が厳しく検討されている。しかし、事柄が複雑になればなるほど、同意の果たす役割は少なくならざるをえず、ユーザーが同意したからよいではなく、そもそもの仕組みから話しをする必要がある。例えば、本日のJavaScriptの話も、同意は２段階目の話で、まず１段階目としてどういう情報取得・情報提供が発生するウェブサイトにするのかファーストパーティーがまず検討しなければならないのはないか。【森構成員】 ■ 同意をどのように取得するのかという手続、同意の取得の対象範囲、個別同意か包括同意か等は、様々な場面で検討されている。クッキー取得時の同意やユーザーインターフェース等も精緻な検討が進められている。一方、同意の効力については、法律行為か事実行為かも意見がある。今後同意取得が更に重要になる中で、同意のそもそもの効力、本人の同意による責任や事業者側への法的効力等もなども少し整理する場があってもよいのではないか。【新保座長代理】 ■ 同意についてどんどん細かくなり手続関係の話になるが、そもそもの同意の目的が忘れられ形骸的なものになってきつつあると感じる。同意を取るのに必要などんなデータ（位置情報等）か、利用目的か、第三者に提供・加工する等かなにが重要なのか考えている。本当に重要なのはその結果利用者に与える影響、アウトカムではないか。手続論・ルールベースの話になってしまうが、アウトカムベースでもう一度見直してどう整理するか考える必要がある。グローバルの流れも、リスクマネジメントの考え方で（SP800-53等も）少しづつアウトカムベースに変わりつつあり、そのような視点を持つ必要がある【寺田構成員】

第22回会合における構成員からの主なご意見⑤

同意の位置付け	■ 寺田構成員の意見に大賛成。アウトカムをしっかりと一度整理していく必要があると強く感じる。それと併せて、今までやってきている内容・手続論とどうやってそれらが結びつくかという点を最後はゴールとして考えて整理していくというのを一度やるべきかなと思っている。【手塚構成員】 ■ アウトカムベースに賛成。手段を規制するのは限界があり、いたちごっこになるので、どういうアウトカムになってはいけないのかというアウトカムベースでやるように規制対象を変えていかないといけない。【崎村構成員】 ■ ISOの通知・同意取得に関する標準規格において、レイヤードアプローチやジャストインタイムの通知とともに、有効な同意を高める手法として同意の証跡（Consent Receipt）がある。【NRI南島氏】 ■ ウェブサイト上における利用者の同意管理ツール（CMP）において、同意前から情報取得、取得拒否しても取得が継続されるなど、正しく動作していない場合も多みられる。提供先は包括同意を取られると実効性はほぼないと思われる。提供元（ウェブサイト・アプリ側）で、どういう事業者がどういう情報を取得しているか公表を明確化しちゃんと拒否できるとよいのではないか。【DataSign太田氏】 ■ アドブロッカーについては物にもよるが、ほとんどのサイトにおいては非常に有効なものだと思う。一方、広告がブロックされてしまうと、メディアとして収益をどう確保するかという問題がある。ドラスティックに広告のエコシステムが変わることがないので、広告を表示して収益を発生させることと、個人が広告をブロックできることをどう両立するかは非常に難しい問題かなと思う。【DataSign太田氏】
スマートフォンプライバシーイニシアティブ、スマートフォン・プライバシー・アウトルック	■ スマートフォンのアプリについては、広告ID（iOS：IDFA,アンドロイド：AAID)があるが、アプリを起動するとニュース等を閲覧するだけでも広告やトラッキング系の情報提供が数多く行われていた。調査した結果、位置情報を取得するアプリのうち半数はプライバシー・ポリシーにその旨記載がなかった。【DataSign太田氏】 ■ 太田氏の説明を伺い、やはりこれは木村構成員からもお話があったがスマートフォン　プライバシー　イニシアティブの話だと改めて思う。スマートフォン　プライバシー　イニシアティブは、ユーザーに対する情報提供にフォーカスしているが、状況は変わらず、深刻な問題状況にある。アプリのプライバシー・ポリシーの掲載率は上がったが、書かれたとおりになっていなかったり、IDが固定的なものとなったり、事態がよくなったとはいえない。やはりもう一段階踏み込んだことをしないといけない状態であることがはっきりしたのではないか。【森構成員】

第22回会合における構成員からの主なご意見⑥

利用者情報を取り扱う事業者の取組	■ NIST Privacy FrameworkのCoreにおいて、８つ定められており、1-5がPrivacy Framework独自で通知・同意取得に当たりプロセスをきちんと確立し社内で浸透させまようという形の規定がされている。6-8はCybersecurity Frameworkと重複。【NRI南島氏】