資料２

プラットフォームサービスに係る利用者情報の取扱いに関するワーキンググループ

利用者情報の取扱いに関する諸外国の法令・自主規制・事例

株式会社野村総合研究所
コンサルティング事業本部

2022年3月16日

Share the Next Values!

目次

ePrivacy指令

ePrivacy指令ではCookieの利用について、説明と同意取得を求めている。ただし、厳密に必須なCookieについては規制が及ばない。

ePrivacy指令におけるCookieに関する規定（5条3項）

：加盟国は、情報を蓄積するための電子コミュニケーションネットワークの利用又はサブスクライバー又は**ユーザの端末機器に保存された情報へのアクセスは、**関係するサブスクライバー又はユーザがDirective 95/46/ECに従い、**明確かつ包括的な説明を受け**（とりわけデータ処理の目的について）た上で、**同意をした場合にのみ許される。**このことは、通信の伝達を促進するためのみに行われる電子コミュニケーションネットワークに対する技術上の保存やアクセス又はサブスクライバー又はユーザから明確に要求されている情報社会サービスを提供するために**厳格に必要な技術上の保存やアクセスを妨げるものではない**

ICOガイドライン（英）※1、CNILガイドライン（仏）※2 に示される厳密に必須なCookieへの該当有無

Cookieの利用目的	該当有無	
	ICO	CNIL
入力内容の保持（User input）	○	○
認証（Authentication）	○	○
セキュリティ対策（Security）	○	○
コンテンツの提供（Streaming content）	○	ー
ネットワーク管理（Network management）	○	○
ユーザーの嗜好の保存（User preference）	○	○

Cookieの利用目的	該当有無	
	ICO	CNIL
ソーシャルプラグイン（Social media plugins）	×	ー
ソーシャルメディアトラッキング（Social media tracking）	×	ー
オンライン広告（Online advertising）	×	×
クロスデバイストラッキング（Cross-device tracking）	×	ー
アクセス解析（Analytics）	×	○※3

凡例：○ 該当　× 非該当　ー 記載なし

※3 クロスサイト測定、統計化しないデータの利用、第三者へのデータ提供は不可

参考資料：「欧米におけるCookie規制の最新動向と今後の展望」（NBL1168号（2020.4.15）31頁）森・濱田松本法律事務所　岡田淳弁護士ほか著
情報提供：森・濱田松本法律事務所　田中浩之弁護士
※1　Guidance on the use of cookies and similar technologies（https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/）（2022年3月8日アクセス）
※2　Cookies et autres traceurs : la CNIL publie des lignes directrices modificatives et sa recommandation（https://www.cnil.fr/fr/cookies-et-autres-traceurs-la-cnil-publie-des-lignes-directrices-modificatives-et-sa-recommandation）（2020年10月1日）
Questions-réponses sur les lignes directrices modificatives et la recommandation « cookies et autres traceurs » de la CNIL（https://www.cnil.fr/fr/questions-reponses-lignes-directrices-modificatives-et-recommandation-cookies-traceurs）（2021年3月18日）

ICOガイドラインにおいて示される厳密必須Cookieへの該当の考え方（1/2）

Cookieの利用目的	該当有無	考え方
入力内容の保持（User input）	○	• 買い物かごやフォームへの入力内容を保持するためのCookieの利用は厳密に必須なものと認められる。ただし、永続的な利用は認められない。
認証（Authentication）	○	• ユーザーの認証を行うための1st PartyのセッションCookieの利用は厳密に必須なものと認められる。ただし、永続的な利用は認められない。 • また、認証のために利用するCookieをユーザーの行動やモニタリングにも利用する場合は同意取得が求められる。
セキュリティ対策（Security）	○	• 不正検知を含むセキュリティ目的で利用される1st Party Cookieの利用は厳密に必須なものと認められる。セッションCookieよりも長い期間の保持が認められる。 例：ログイン試行時の失敗数を検出するためのCookie • ただし、自サービス以外のオンライン・サービスのセキュリティに関連するCookieの利用や二次的な目的のために情報が処理される場合は同意が求められる。
コンテンツの提供（Streaming content）	○	• オンライン・コンテンツ・プロバイダーがビデオまたはオーディオコンテンツを提供するために利用するCookieは厳密に必要なものと認められる。 • ただし、コンテンツのパーソナライズや視聴状況のモニタリングに利用する場合は同意取得が求められる。 • また、オンラインサービスが、第三者のオンライン・コンテンツ・プロバイダーによって提供されるコンテンツを単に埋め込む場合（例：ウェブサイトがYoutubeのビデオを埋め込む場合）、適用免除が認められない場合があり、慎重に判断する必要がある。
ネットワーク管理（Network management）	○	• ロードバランシング（負荷分散）を目的としたCookieの利用は厳密に必須なものと認められる。
ユーザーの嗜好の保存（User preference）	○	• ユーザーの嗜好を保存するためのCookieの利用は厳密に必須なものと認められる。ただし、永続的な利用は認められない。 • 例えば、一定期間（例えば90日間）にわたってユーザーのCookie設定を記憶する、Cookie同意メカニズムの一部として使用されるCookieは、免除される可能性がある。 • オンラインサービスがレスポンシブデザインを使用し、デバイスの種類に応じてサイトを変更する際に利用するCookieも厳密に必須なものと認められうる。

（出所）https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/how-do-we-comply-with-the-cookie-rules/#comply16（2022年3月14日アクセス）

ICOガイドラインにおいて示される厳密必須Cookieへの該当の考え方（2/2）

Cookieの利用目的	該当有無	考え方
ソーシャルプラグイン（Social media plugins）	×（要同意取得）	• オンラインサービスがソーシャルメディアプラットフォームが提供するプラグイン等のツールを利用している場合（例：ウェブサイトにおける「いいね！」ボタンの設置）、プラグイン等が設定する全てのCookieの利用に関して同意取得が求められる。 • これは同サービスをソーシャルメディアのプラットフォームにログインしていないユーザー（ログアウトしたユーザー、またはそのネットワークの会員でないユーザー）も利用することが想定されるためである。
ソーシャルメディアトラッキング（Social media tracking）	×（要同意取得）	• ソーシャルメディアプラットフォームや第三者がオンライン広告・モニタリング・分析・マーケティング等の目的で会員・非会員のユーザーを追跡する場合、Cookieの利用に関して同意取得が求められる。
オンライン広告（Online advertising）	×（要同意取得）	• オンライン広告の目的でCookieを利用する場合、同意取得が求められる。 • これには、頻度制限、広告提携（アフィリエイト）、クリック詐欺の検出、市場調査、製品改善、デバッグ、その他の目的など、オンライン広告で使用されるすべての3rd Party Cookieが含まれる。
クロスデバイストラッキング（Cross-device tracking）	×（要同意取得）	• ユーザーのアカウントを特定のデバイスと結びつけるために、Cookieを利用する場合（例：アカウントプロファイルの一部として、第2の認証要素を提供するため、または広告を含むあらゆる目的のために複数のデバイスにわたってユーザーを追跡するため）、同意取得が求められる。
アクセス解析（Analytics）	×（要同意取得）	• ユーザーが求めるサービスを提供するために、分析目的のCookieの利用は厳密には必須なものではないため、同意取得が求められる。

（出所）https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/how-do-we-comply-with-the-cookie-rules/#comply16（2022年3月14日アクセス）

ePrivacy指令

Cookieの利用に関する同意取得にあたっては、GDPRの求める厳格な基準を満たす必要がある。

GDPRにおける同意の定義（4条11項）

：データ主体の「同意」とは、**自由に与えられ、特定され、事前に説明を受けた上での、不明瞭ではない、**データ主体の意思の表示を意味し、それによって、データ主体が、その陳述又は明確な積極的行為により、自身に関連する個人データの取扱いの同意を表明するものを意味する

ICOガイドライン（英）※1、、CNILガイドライン（仏）※2 、DSKガイダンス（独）※3に示される同意取得方法の有効性

同意の取得方法	同意の有効性		
	ICO	CNIL	DSK
ユーザーが同意取得用のチェックボックス等を操作することなく、ウェブサイトやアプリの閲覧、スクロール、別ページに遷移等をもって同意取得とすること	×	×	×
ブラウザやOSの設定のみに依拠して、同意取得していると判断すること	×（将来的な可能性は認める）	×（将来的な可能性は認める）	×
利用規約（terms and conditions ）に含める形など、個別的でない形で同意取得すること	×	×	×
Cookie取得の同意をウェブサイトへのアクセス条件とすること（いわゆるCookie Wall）	△※4	△※5	×
同意する方が拒否するよりも容易な/選択肢が目立つユーザーインターフェイスで同意取得すること	×	×	×
CMPによる同意管理	―	―	△※6

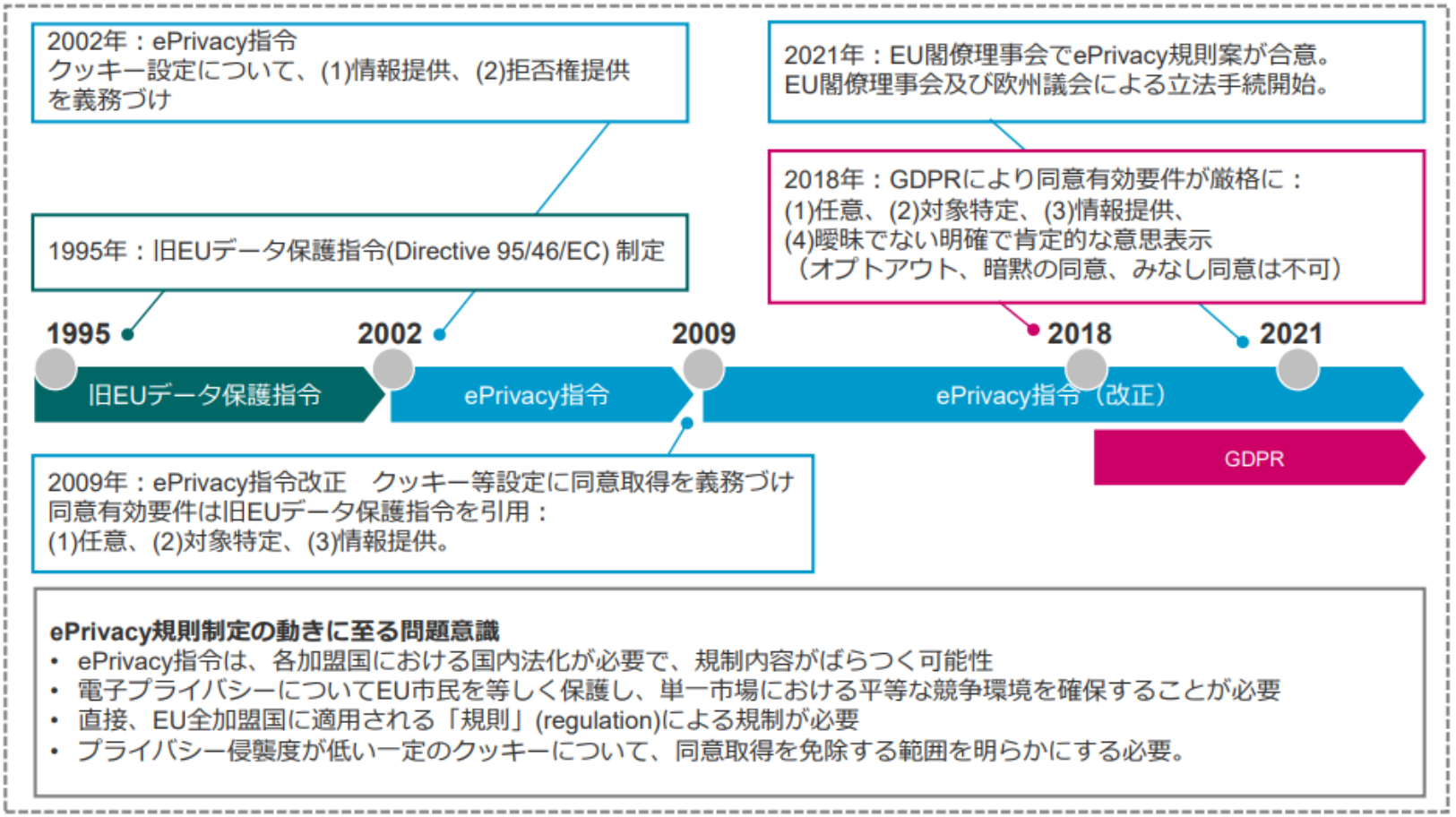
※4 正当な目的（アクセス解析や広告は含まれない）に基づき、一定のCookie利用につき同意しない場合に一定のコンテンツへのアクセスを制限することは許容
※5 ケースバイケースで判断。同意の自由を侵害する可能性がある
※6 CMPの使用方法等に依存。同意の有効性に関する責任はテレメディアサービス提供者が負う

参考資料：「欧米におけるCookie規制の最新動向と今後の展望」（NBL1168号（2020.4.15）31頁）森・濱田松本法律事務所　岡田淳弁護士ほか著
情報提供：森・濱田松本法律事務所　田中浩之弁護士
※1 ※2 P3と同様
※3　Germany: DSK publishes guidance on TTDSG（https://www.dataguidance.com/news/germany-dsk-publishes-guidance-ttdsg）（2021年12月21日）

ePrivacy指令

ePrivacy指令に基づく規制の経緯及び概要

EUでは、オンラインサービス利用者の端末装置でのデータ読み書きを対象に、目的等の情報提供及び事前同意取得を原則とする「クッキー規制」が行われている。クッキー規制をEU域内で統一するために、ePrivacy規則案の立法作業が2017年以来続いている。



（出所）総務省 プラットフォームサービスに係る利用者情報の取扱いに関するワーキンググループ第２回資料２
（ https://www.soumu.go.jp/main_content/000744406.pdf ）（2022年3月1日アクセス）

ePrivacy指令

規制対象：電子通信サービス (ECS) の定義（新定義）

- **欧州電子通信コード(EECC)（2020/12/21～）**

  - 通常は対価を伴い、電子通信網上で提供されるサービスで、以下を包摂(encompass)：
    a. インターネット接続サービス
    b. 個人間通信サービス（番号サービス、非番号サービス）
    c. 主として信号伝送を提供するサービス（例：M2M向け、放送向け）
  - 除外：伝送されるコンテンツを提供・編集するサービス

- **旧・枠組指令との違いを整理すると…**
  - 主として信号伝送を提供するサービス：共通
  - 番号サービス（電話、SMSなど）＋インターネット接続サービス：共通
  - 信号伝送しないコンテンツ提供事業の除外：共通　（例：情報を掲載するウェブサイト）

- **つまり、EECCでECS定義に追加されたのは、**
  信号伝送を主たる機能とせず、インターネットなどの通信網上で提供される個人間通信サービス。例えば、Webメール、メッセンジャーサービスなど

- 「対価を伴い」には、個人データ提供を対価とする運営、広告収入による運営も含まれる（EECC前文16項）

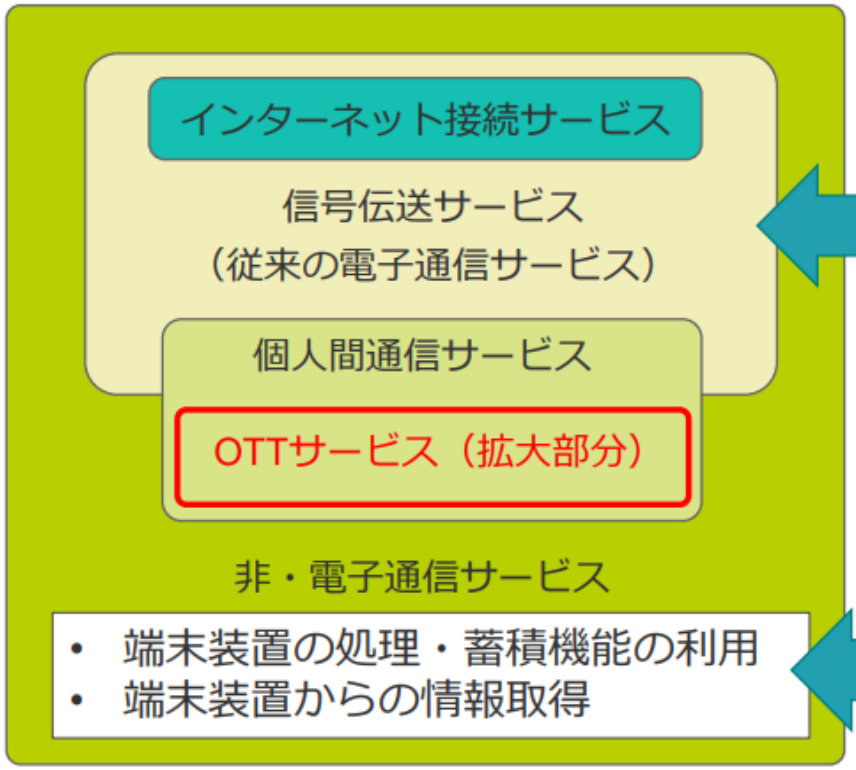
- 個人間通信サービスには、サービスに付随する補助的なもの（ゲームにおけるチャット）、機械間の情報交換は含まれない（EECC2(5), 前文17項）

EECC: European Electronic Communications Code (Directive 2018/1972)

（出所）総務省 プラットフォームサービスに係る利用者情報の取扱いに関するワーキンググループ第２回資料２
（ https://www.soumu.go.jp/main_content/000744406.pdf ）（2022年3月1日アクセス）

ePrivacy指令

適用対象を整理すると…



電子通信サービスに対する規制

- 通信の秘密
- 電子通信データの処理規制
- 電子通信コンテンツの処理規制
- 電子通信メタデータの処理規制

非・電子通信サービスにも及ぶ規制

- いわゆる**「クッキー等規制」**
  - 原則禁止
  - 同意など一定の場合禁止解除

- **OTTサービス** (Over-The-Top Service):
  インターネット上で提供される個人間通信サービス（Webメール、メッセンジャー）

（出所）総務省 プラットフォームサービスに係る利用者情報の取扱いに関するワーキンググループ第２回資料２
（ https://www.soumu.go.jp/main_content/000744406.pdf ）（2022年3月1日アクセス）

ePrivacy指令関連の執行事例

時期	国	対象企業	制裁金	概要
2019/10	ドイツ	Planet 49 GmbH	-	• あらかじめチェックされたチェックボックスを使用してCookieに関する同意を取得することは、有効な同意とはいえないという判決を欧州連合司法裁判所が下した。 • これを踏まえて、ドイツ連邦司法裁判所は、ePrivacy指令第5条3項がドイツの国内法に正しく移行されていないと判断し、当該条項を反映した「電気通信およびテレメディアにおけるデータ保護およびプライバシーの規制に関する連邦法（TTDSG）」が2021年12月1日に施行された。
2019/10	スペイン	Vueling（航空会社）	3万ユーロ	• Cookieを拒否するための同意管理プラットフォーム、またはCookie設定ツールへのアクセスをユーザーに提供しておらず、有効な同意を収集することができないとして、ePrivacy指令に基づくスペイン国内法であるLSSI法第 22 条 2 項に違反したと判断された。
2019/11	スペイン	Ikea Ibérica	1 万ユーロ	• 適切な通知や有効な同意取得がない状態で、ユーザーのパソコンやスマートフォンにCookieを設置しており、LSSI法第 22 条 2 項に違反したと判断された。
2020/7	スペイン	Just Landed, SL	3,000ユーロ	• スペイン領に拠点を置いているにもかかわらず、Cookieポリシーが存在せず、Cookieのインストールを許可、拒否、管理できるリンクや仕組みもなく、何もしなくてもCookieが読み込まれた状態であったため、eプライバシー指令第38条4項(g)に基づく「軽微な」違反とされた。
2020/12	フランス	Google、Amazon	6,000万ユーロ（Google LLC） 4,000万ユーロ（Google Ireland Limited） 3,500万ユーロ（Amazon Europe Core）	• ユーザーが容易にオプトアウトできないことに加え、Cookieによる追跡に関してユーザーに十分な透明性を提供していなかったことから、Cookieの配置に対する同意に係るePrivacyの規定に違反したと判断された。
2021/3	スペイン	Furnishyourspace SL	3,000ユーロ	• Cookieバナーに、Cookieを拒否する選択肢がなく、バナーやプライバシーポリシーを通じて提供される情報が不明確であったことから、LSSI法第 22 条 2 項の侵害があったと判断された。
2021/3	スペイン	Abanca Corporación Bancaria	5,000ユーロ （3,000ユーロに減額）	• ユーザーの同意を得る前に、ウェブサイト上で不要なCookieを使用したとして、LSSI法第 22 条 2 項に違反と判断された。
2022/1	フランス	Google、Meta	9,000万ユーロ（Google LLC） 6,000万ユーロ（Google Ireland Limited） 6,000万ユーロ（Meta Ireland）	• フランスのユーザーが、Cookieによる追跡を容易に拒否できないことにより、GoogleおよびMetaが執行された。

（出所）・CNILプレスリリース（https://www.cnil.fr/en/actualite）（2022年2月7日アクセス）
・OneTrust DataGuidance（https://www.dataguidance.com/opinion/germany-new-federal-act-regulation-data-protection）（2022年2月7日アクセス）
・AEPD公式HP（https://www.aepd.es/es）（2022年2月7日アクセス）

ePrivacy規則案

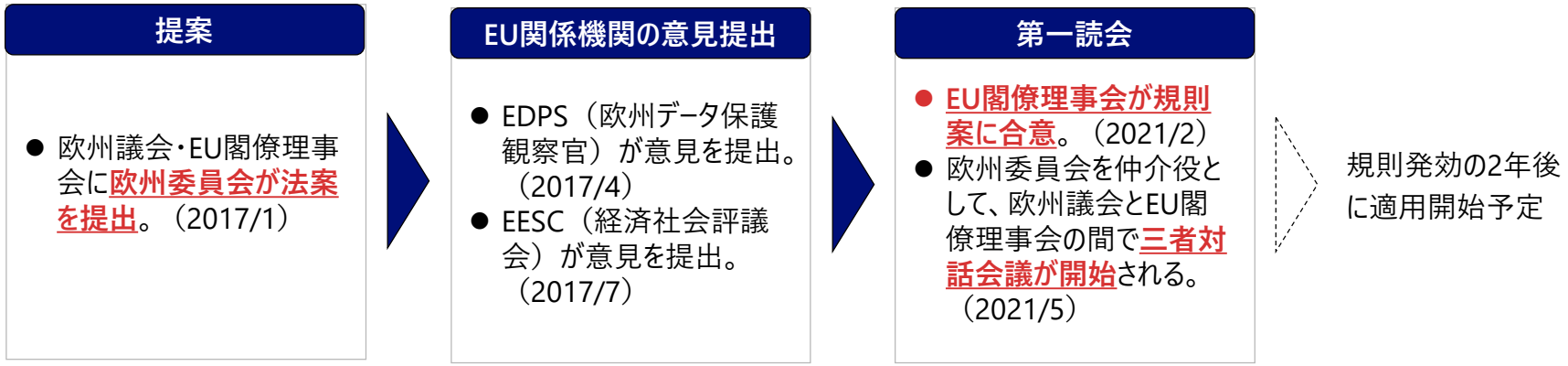
ePrivacy規則案

- ePrivacy規則案は、GDPR（General Data Protection Regulation：一般データ保護規則）の特別法に相当し、電子通信サービスにおけるプライバシー保護を目的としている。
- 電子通信サービスにおけるプライバシー保護について、これまでは2002年に制定されたePrivacy指令に基づき、各EU加盟国が国内法を定めていた。しかし、下記の問題意識もあり、GDPRと平仄を合わせる形で新しいルール策定が進められた。
  - ePrivacy指令は、EU全体に直接適用されず、各加盟国の国内法において規制内容がばらつく可能性がある。
  - ePrivacy指令は、従来の通信事業者のみを規制対象としており、メッセンジャーサービス等を含む電子通信分野の新しいプロバイダーには適用されない。（ただし、欧州電子通信コード（EECC：European Electronic Communication Code）指令により改正され、現在ではメッセンジャーサービス等を含むOTTサービスも対象となっている。）
- 2017年に欧州委員会が公表した規則案に対して、2021年2月、EU閣僚理事会が修正案（合意済み）を公表し、欧州議会を加えた三者対話会議（トリローグ）が進められている。
- 規則案（EU閣僚理事会案）に対しては、EDPB（European Data Protection Board：欧州データ保護委員会）や広告事業者の業界団体であるIAB EUROPEが意見を表明している。

ePrivacy規則案の立法プロセス

- ePrivacy規則案は、通常立法手続に基づき審議されており、欧州委員会からの提案に基づき、欧州議会とEU閣僚理事会が共同で規則を採択する。
- 通常立法手続は、1回または2回の読会と、そこで成立しなかった場合の調停手続き、および第三読会で構成される。
- 現在、ePrivacy規則案は第一読会のステータスにあり、欧州議会とEU閣僚理事会による交渉が行われている。

ePrivacy規則案の立法プロセス



（出所）
・EU官報（https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX:52017PC0010）（2022年1月13日アクセス）
・LEGISLATIVE TRAIN SCHEDULE（https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-jd-e-privacy-reform）（2022年1月13日アクセス）
・EU閣僚理事会プレスリリース（https://www.consilium.europa.eu/en/press/press-releases/2021/02/10/confidentiality-of-electronic-communications-council-agrees-its-position-on-eprivacy-rules/）（2022年1月13日アクセス）

ePrivacy規則案に係る議論の経緯（1/2）

時期	法案等の状況	EU関係機関の動向	業界団体の動向
2016/5	• GDPRの採択		
2017/1	• 欧州委員会がePrivacy規則案を発表		
2017/4		• 第29条作業部会が意見を発表 • EDPS（欧州データ保護観察官）が意見を提出	
2017/7		• EESC（経済社会評議会）が意見を提出	• IAB EuropeがePrivacy規則に対するポジションペーパーを公表
2017/9			• ICDPが、欧州議会の議員に向けた、ePrivacy規則が業界に与える影響について説明した書簡に署名
2017/10	• 欧州議会LIBE（市民的自由・司法・内務委員会）で修正採択	• EDPSが再度意見を提出	
2017/11			• ICDPが、欧州議会LIBEに対し、ePrivacy規則案に関する書簡を提出
2017/12	• EU閣僚理事会が修正版ePrivacy規則案を発表		
2018/3	• EU閣僚理事会が新たな規則案を発表		• EDiMAが、2017年10月のePrivacy規則案１～5条に関し意見を表明
2018/5		• EDPBが第1回総会にてePrivacy規則案に関する声明を採択	• 57者のステークホルダーが、TTE Councilに対してePrivacy規則案を慎重に検討するよう要請する書簡に共同署名
2018/7	• EU閣僚理事会が新たな規則案を発表		
2018/9	• EU閣僚理事会が新たな規則案を発表		
2018/10	• EU閣僚理事会が新たな規則案を発表		

（出所）
・EU官報（https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX:52017PC0010）（2021年12月14日アクセス）
・EDPB公式HP（https://edpb.europa.eu/our-work-tools/our-documents/publication-type/statements_en）（2021年12月14日アクセス）
・IAB europe 公式HP（https://iabeurope.eu/proposed-eprivacy-regulation/）（2021年12月14日アクセス）
・総務省プラットフォームサービスに関する研究会第3回資料2（https://www.soumu.go.jp/main_content/000592527.pdf）（2021年12月14日アクセス）

ePrivacy規則案に係る議論の経緯（2/2）

時期	法案等の状況	EU関係機関の動向	業界団体の動向
2018/11			• IAB EuropeがePrirvacy規則案に対するポジションペーパーを再度公表66者のステークホルダーが、TTE Councilに対してePrivacy規則案を慎重に検討するよう要請する書簡に共同署名
2019/2	• EU閣僚理事会が新たな規則案を発表		
2019/3	• EU閣僚理事会が新たな規則案を発表	• EDPBがePrivacy規則に関する声明を採択	
2019/7	• EU閣僚理事会が新たな規則案を発表		
2019/10	• EU閣僚理事会が新たな規則案を発表		
2019/11	• EU閣僚理事会が新たな規則案を発表		
2020/2	• EU閣僚理事会が新たな規則案を発表		
2020/3	• EU閣僚理事会が新たな規則案を発表		
2020/11	• EU閣僚理事会が新たな規則案を発表	• EDPBがePrivacy規則に関する声明を採択	
2021/2	**• EU閣僚理事会が規則案に合意**		
2021/3		**• EDPBがePrivacy規則に関する声明を採択**	
2021/4			**• IAB EuropeがePrirvacy規則案に対するポジションペーパーを再度公表**

（出所）
・EU官報（https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX:52017PC0010）（2021年12月14日アクセス）
・EDPB公式HP（https://edpb.europa.eu/our-work-tools/our-documents/publication-type/statements_en）（2021年12月14日アクセス）
・IAB europe 公式HP（https://iabeurope.eu/proposed-eprivacy-regulation/）（2021年12月14日アクセス）
・総務省プラットフォームサービスに関する研究会第3回資料2（https://www.soumu.go.jp/main_content/000592527.pdf）（2021年12月14日アクセス）

ePrivacy規則 EU閣僚理事会案の目次

※取り消し線は2017年1月に欧州委員会が発表した規則案から削除されたもの

（出所）ePrivacy規則EU閣僚理事会案（https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf）（2021年12月14日アクセス）

ePrivacy規則 EU閣僚理事会案の内容（1/2）

「クッキー等規制」（8条）

■ 端末装置の処理・蓄積機能の利用、端末装置からの情報の取得は、一般的に禁止され、以下の場合に限って許される。（次ページに参照条文）

列記された条件	想定される適用例
もっぱら電子通信サービス提供のために必要な場合	メッセージサービスのHTTPセッション維持
利用者の**同意**がある場合	ターゲティング広告、コンテンツのパーソナライズ
利用者が個別に求める**サービスの提供に必須**な場合	ユーザ入力、ログイン認証状態、表示言語の記憶
サービス提供者がもっぱら**オーディエンス測定**のために必要とする場合。GDPRに規定する処理者を利用する場合、GDPR第28条に従って処理者を管理監督すること	ウェブアクセス解析サービスを利用し、閲覧者がウェブサイトのどのページにどれくらいの時間滞在したかなどを分析する。
オンラインサービス又は端末装置の**セキュリティ維持・復旧、不正利用防止、障害検知・防止**のために必要な場合	ある利用者が通常利用しているブラウザとは別のブラウザからのログイン試行を検知し、警告する。
ソフトウェア・アップデートに必要な場合。ただし： • セキュリティ上の必要によるものであり、端末のプライバシー設定を変更しないこと • 個別アップデートごとに事前情報提供すること • 利用者が自動アップデートを延期又は中止できること	ブラウザが最新のセキュリティアップデートをインストールしているかどうかを確認する。ブラウザ設定ですべてのクッキーを拒否している場合、これを上書きしない。ブラウザ設定でこのようなアップデートの可否を設定できる。
緊急通報(例：112)において端末装置の位置を特定するために必要な場合	同左
同意又は一定の公益保護を目的とする法令上の根拠がある場合、及び二次利用の目的が当初の処理目的と相容れる(compatible)場合は、二次利用が可能。（GDPP6(4)と同様の規定）	不正ログイン検知情報を捜査協力目的で捜査機関に提供する。

（出所）総務省 プラットフォームサービスに係る利用者情報の取扱いに関するワーキンググループ第２回資料２
（ https://www.soumu.go.jp/main_content/000744406.pdf ）（2022年2月2日アクセス）

ePrivacy規則 EU閣僚理事会案の内容（2/2）

ePrivacy規則案による新「クッキー等規制」の意義

- **ターゲティング広告等**
  従来どおり、ターゲティング広告、コンテンツのパーソナライズなどを目的とするクッキーの設定については利用者の同意取得が必要
- **ウェブアクセス解析**
  - 同意不要：自社利用のための純粋なオーディエンス測定
  - 同意必要：アクセス解析以外の目的でも取得したデータを利用する場合（例：広告連動）
- **クッキー類似技術への規制適用**
  - 従来どおり、デバイス・フィンガープリンティングなど、類似技術にも規制適用（前文20項）

> Recital (20)
> Information related to the end-user's device may also be collected remotely for the purpose of identification and tracking, using techniques such as the so-called 'device fingerprinting',
> （仮訳）利用者の装置に関する情報は、「デバイス・フィンガープリンティング」等の技術の利用により、識別及び追跡の目的のために遠隔取得することもできる。

- **端末装置の処理機能の利用が新たな規制対象**
  - 規制対象の変化
    - 現ePrivacy指令：　端末装置における情報の蓄積又は蓄積された情報へのアクセス
    - 新ePrivacy規則案：　端末装置の**処理**・蓄積**機能の利用**及び端末装置からの情報の取得
  - 想定される影響
    - Google Privacy Sandboxは、ブラウザ内部処理で閲覧行動を分析し、利用者を属性グループに分類、このような属性情報を、広告コンテンツをリクエストする際に送信して実質的に広告ターゲティングを実現。このような処理は「端末装置の処理機能の利用」とされる可能性
    - 端末装置での蓄積を伴わないリアルタイム処理が規制対象となる可能性
      例えば、コネクテッド車両、IoT機器を対象とする遠隔リアルタイム処理

（出所）総務省 プラットフォームサービスに係る利用者情報の取扱いに関するワーキンググループ第２回資料２
（ https://www.soumu.go.jp/main_content/000744406.pdf ）（2022年2月2日アクセス）

ePrivacy規則案

EDPBは、ePrivacy規則案に対して、現行のePrivacy指令の保護レベルを低下させてはならず、GDPRの規定内容と整合する必要があるとの声明を発表している。

EDPBのePrivacy規則に関する声明の要点

Article	声明の要点
4a	• 公平な競争条件とするため、ユーザーフレンドリーな方法で、管理者が**同意**を得ることができる**メカニズム**を導入することを、**ブラウザとOSに義務付けるべき**である。
6.1(d), 7.4	• **法執行または国家安全保障の目的であっても、無差別にトラフィックや位置情報を保管する行為は欧州連合基本権憲章第7条、第8条等に反するため、そのような立法措置は認められないと解釈すべき**である。
6, 6a, 6b, 6c	• 電気通信データの処理に係る例外規定が幅広く設けられているため、**例外規定の対象となる目的を絞ったうえで明確化**すべきである。
6c, 8.1(g)	• データを収集した目的と異なる目的でのデータ処理について、禁止を前提としたうえで、例外は限定し、**同意取得を基本としている点は、ePrivacy規則案を支持**する。
8	• **GDPRが定める同意要件**を、ePrivacy規則の文脈で**Cookie等にも適用**し、いわゆる「Cookieウォール」のような不公正な慣行を禁止すべきである。
18, 19, 20	• EU全体で、調和のとれた解釈と施行を確保するため、GDPRの施行を担当する国家機関が、ePrivacy規則のパーソナルデータの処理に関わる条項を監視すべきである。加えて、GDPR第7章で規定される「協力と一貫性（Cooperation and consistency）」メカニズムは、ePrivacy規則の枠組みにおいても必要である。

（出所）EDPB「ePrivacy規則案に関する声明」（https://edpb.europa.eu/system/files/2021-03/edpb_statement_032021_eprivacy_regulation_en_0.pdf）（2021年12月21日アクセス）

ePrivacy規則案

広告事業者の業界団体であるIAB Europeは、オンラインサービス・コンテンツが引き続き広告収入をもとに運営可能となるように、ePrivacy規則案に対する意見を表明している。

IAB EuropeのePrivacy規則に関するポジションペーパーの要点

Article	ポジションペーパーの要点
前文20(aaaa)、前文21(aa)	• **マネタイズモデルに必要な広告目的のデータ処理**に対して、十分な説明を受けたうえでユーザーが同意することを、**オンラインサービスへのアクセス条件とすることを明確に許可すべき**である。 • 前文20(aaaa)、前文21(aa)において、「ジャーナリズム目的を含む表現と情報の自由に従って提供されるサービス」には、ユーザー端末情報の収集が必要な場合があることを明示的に認めた点は評価できる。
4a※1、前文20a	• **技術レベルで処理をブロックすることを、ブラウザやOSに要求しない中立な法律と**することで、競争の促進と技術革新を可能に**すべき**である。プライバシー設定によるブラウザのゲートキーパー化を求める第10条の規定は、競争上の問題等、複数の懸念から削除されたが、第4a条および前文20aにおいて事実上復活している。
8.1	• パーソナルデータの処理に係る**合法的根拠について、ePrivacy規則案第8条1項とGDPR第6条（取扱いの適法性）の整合性をとるべき**である。例えば、GDPR第6条において取扱いの根拠として認められる「正当な利益の目的」は、ePrivacy規則案第8条1項においては記載がない。これは、広告目的のデータ処理に対するユーザーの同意を、オンラインサービスへのアクセス条件とすることができるか不明確であることと相まって、データ処置の柔軟性と多様性を企業から奪っている。
8	• 測定、セキュリティ、不正防止等を目的として、Cookieなどの広告関連データを処理することは、広告収入に基づくビジネスに必要不可欠である。特に、広告パフォーマンスの効果的な測定のために、サードパーティのサービスプロバイダと連携することは、自社サイトのデータだけでは十分な情報が確保できない中小企業にとって重要であるため、そのような中小企業も考慮して第8条の規定を修正すべきである。

※1：「IAB Europe ポジションペーパー」にはArticle 4.2と記載があるものの、誤記と思われる。

（出所）IAB Europe ポジションペーパー（https://iabeurope.eu/wp-content/uploads/2021/05/20210412_IAB_Europe_ePR_position.pdf）（2021年12月21日アクセス）

ePrivacy規則案

同意取得に関連する第4a条および第8条について、EDPBおよびIAB Europeから、方向性の異なる意見が寄せられている。

ePrivacy規則案に関し、政府機関と業界団体とで意見の異なる箇所

意見の異なる箇所	主な意見	
	EDPB	IAB Europe
①ソフトウェアのプライバシー設定（第4a条）	• 公平な競争条件とするため、ユーザーフレンドリーな方法で管理者が**同意**を得ることができる**メカニズム**を導入することを、**ブラウザとOSに義務付けるべき**である。	• **技術レベルで処理をブロックすることを、ブラウザやOSに要求しない中立な法律と**することで、競争の促進と技術革新を可能に**すべき**である。 • プライバシー設定によるブラウザのゲートキーパー化を求める第10条の規定は、競争上の問題等、複数の懸念から削除されたが、第4a条および前文20aにおいて事実上復活している。
②ユーザー端末に保存された情報の保護（第8条）	• **GDPRが定める同意要件**を、ePrivacy規則の文脈で**Cookie等にも適用**し、いわゆる「Cookieウォール」のような不公正な慣行を禁止すべきである。	• 測定、セキュリティ、不正防止などの広告関連データの処理目的は、広告収入に基づくビジネスに必要不可欠である。 • 特に、広告パフォーマンスの測定のために、サードパーティのサービスプロバイダと連携することは、自社サイトのデータだけでは十分な情報が確保できない中小企業にとって重要であるため、第8条の規定を修正すべきである。
③ユーザー端末に保存された情報の収集が認められる場合（第8条1項）	• データを収集した目的と異なる目的でのデータ処理について、禁止を前提としたうえで、例外は限定し、同意取得を基本としている点は、ePrivacy規則案を支持する。	• パーソナルデータの処理に係る**合法的根拠について、ePrivacy規則案第8条1項とGDPR第6条（取扱いの適法性）の整合性をとるべき**である。GDPR第6条（取扱いの適法性）において取扱いの根拠として認められる「正当な利益の目的」が、ePrivacy規則案の例外条件に含まれないことは、広告目的のデータ処理に対するユーザーの同意を、オンラインサービスへのアクセス条件とすることができるか不明確であることと相まって、データ処置の柔軟性と多様性を企業から奪っている。

（出所）EDPB「ePrivacy規則案に関する声明」（https://edpb.europa.eu/system/files/2021-03/edpb_statement_032021_eprivacy_regulation_en_0.pdf）（2021年12月21日アクセス）
IAB Europe ポジションペーパー（https://iabeurope.eu/wp-content/uploads/2021/05/20210412_IAB_Europe_ePR_position.pdf）（2021年12月21日アクセス）

ePrivacy規則案

意見の異なる箇所①：ソフトウェアのプライバシー設定（第4a条）

■ 第4a条では、ブラウザおよびアプリにおける「Cookie設定等への同意」を有効な同意と認めている。

- EDPB：ユーザーの同意疲れを回避し、関係者の競争条件を公平にするために、**ブラウザとOSを明示的に規制対象として、ユーザーフレンドリーな方法で同意を表明・撤回できるメカニズムを導入することを義務付けるべき**
- IAB Europe：技術レベルで処理をブロックすることを**ブラウザやOSに要求しない中立な法律とする**ことで、競争の促進と技術革新を可能にすべき

ePrivacy規則案 第4a条（下線太字はNRI）

第4a条 同意

1. 規則2016/679/EUに基づき規定される同意に関する規定は、自然人及び法人に準用されるものとする。
1a. 第1項は、第三者との取引又は法的手続において法人を代理する権限を有する者の決定に関する国内法令を害するものではない。
2. 第1項を害することなく、技術的に可能かつ実行可能な場合には、第8条1項(b)の目的のために、インターネット上の情報の検索及び提示を含む電子通信を許可する市場に置かれたインターネットへのアクセスを可能にする**ソフトウェアアプリケーションの適切な技術設定を使用することによって、同意を表明することができます。**
2aa. 第2項に従ってエンドユーザーが直接表明した同意は、ソフトウェアの設定に優先するものとします。エンドユーザーがサービスに対して要求し、与えた同意は、情報の保存またはエンドユーザーの端末機器に既に保存されている情報へのアクセスが許可されている場合を含め、エンドユーザーの端末のアプリケーションによって、さらなる遅延なく、直接実施されるものとします。
2a. 提供者が情報主体を特定できない限り、第8条1項(b)によるエンドユーザーの同意を示すには、端末機器から同意がなされたことを示す技術的プロトコルで十分であるものとする。
3. この規則に従って電子通信データの処理に同意したエンドユーザーは、エンドユーザーがそのようなリマインダーを受け取らないよう要求しない限り、処理が継続する限り、［12ヶ月以内］の定期的な間隔で、同意を撤回する可能性について注意を促されるものとします。

（出所）ePrivacy規則EU閣僚理事会案（https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf）（2021年12月14日アクセス）

（参考）プライバシー設定によるブラウザのゲートキーパー化（第10条）

- 2017年1月に欧州委員会が公表した規則案では、第10条において、ユーザー端末情報の第三者による処理を拒否する機能を、ブラウザ等のソフトウェアに付けることが義務付けられていた。
- また、2017年10月に欧州議会LIBEが修正採択した際には、ソフトウェアは、ユーザー端末情報の取得を禁止することをデフォルトで設定することが追記された。
- しかし、各国政府との議論において、競争上の問題等が指摘され、2018年7月以降の閣僚理事会案では第10条全体が削除されている。

（参考）ePrivacy規則案第10条　欧州委員会案条文（下線太字はNRI ）

第10条 プライバシー設定のために提供される情報と選択肢

1. インターネット上の情報の検索及び提示を含む電子通信を許可する市場に出された**ソフトウェアは、第三者がエンドユーザーの端末機器に情報を保存すること又は当該機器に既に保存されている情報を処理することを防止するためのオプションを提供しなければならない**。
2. ソフトウェアは、インストール時に、エンドユーザーにプライバシー設定オプションについて通知し、インストールを続行するには、エンドユーザーが設定に同意することを要求するものとする。
3. 2018年5月25日に既にインストールされているソフトウェアの場合、第1項及び第2項の要件は、当該ソフトウェアの最初の更新時に、2018年8月25日までに遵守されるものとします。

（出所）
・ePrivacy規則欧州委員会案（https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0010&from=EN）（2022年1月13日アクセス）
・ePrivacy規則欧州議会LIBE修正案（https://www.europarl.europa.eu/doceo/document/A-8-2017-0324_EN.html?redirect）（2022年1月13日アクセス）

ePrivacy規則案

意見の異なる箇所②：ユーザー端末に保存された情報の保護（第8条）

■ 第8条では、ユーザー端末に保存された情報の収集を原則禁止したうえで、例外として認められる収集を行う場合は、GDPRに準じた、明確かつ分かりやすい通知を提供することを求めている。

- EDPB：GDPRが定める同意要件は、業界や資金調達モデルに関わらず、 ePrivacy規則の文脈で**すべてのサービス・プロバイダーに等しく適用されるべき**であるとしている。（前文21(aa)において、主に広告収入に基づくジャーナリズムを目的とするサービスは、ユーザー端末情報の収集が必要な場合があるとされたことを受けている。）

- IAB Europe：**測定、セキュリティ、不正防止等を目的として、Cookieなどの広告関連データを処理することは、**広告収入に基づくビジネスに**必要不可欠**であると主張している。特に、広告パフォーマンスの効果的な測定のために、サードパーティのサービス・プロバイダと連携することは、自社サイトのデータだけでは十分な情報が確保できない中小企業にとって重要であるため、そのような中小企業も考慮して第8条の規定を修正すべきであると述べている。

ePrivacy規則案第8条2a-4項条文

2a. 第2項(b)(c)の目的のために、少なくとも、収集の様式、その目的、責任者及び個人情報が収集される規則2016/679/EUの第13条に基づき要求されるその他の情報、並びに端末機器のエンドユーザーが収集を停止又は最小限に抑えるために取ることのできる手段を通知する明確かつ目立つ通知を掲示するものとします。
2b. 第2項(b)©の目的のために、当該情報の収集は、規則2016/679/EUの第32条に定めるリスクに見合ったセキュリティレベルを確保するための適切な技術的及び組織的措置が適用されていることを条件とします。
3. 第2a項に従って提供される情報は、容易に視認でき、分かりやすく、かつ明確に判読できる方法で、コレクションの有意義な概観を与えるために、標準化されたアイコンと組み合わせて提供することができる。
4. 欧州委員会は、第25条に基づき、標準化されたアイコンで表示すべき情報及び標準化されたアイコンを提供するための手続を決定する委任行為を採択する権限を有するものとする。

（出所）ePrivacy規則EU閣僚理事会案（https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf）（2021年12月14日アクセス）

意見の異なる箇所③：ユーザー端末に保存された情報の収集が認められる場合（第8条1項）

■ 第8条1項では、ユーザー端末に保存された情報の収集を原則禁止とし、例外となる場合を列挙している。

- **EDPB**：データを収集した目的と異なる目的でのデータ処理について、禁止を前提としたうえで、例外は限定し、同意取得を基本としている点は、ePrivacy規則案を支持している。
- **IAB Europe**：GDPR第6条（取扱いの適法性）において、取扱いの根拠として認められる「正当な利益の目的」が、ePrivacy規則案の例外条件に含まれないことは、広告目的のデータ処理に対するユーザーの同意を、オンラインサービスへのアクセス条件とすることができるか不明確であることと相まって、データ処置の柔軟性と多様性を企業から奪っているという意見を述べている。

（出所）ePrivacy規則EU閣僚理事会案（https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf）（2021年12月14日アクセス）

（参考）ePrivacy規則案第8条1項条文

第8条1項　端末機器の処理能力及び記憶能力の使用並びにエンドユーザーの端末機器からの情報（そのソフトウェア及びハードウェアに関するものを含む）の当該エンドユーザー以外による収集は、次の理由を除き、禁止されるものとする。
(a) 電子通信サービスを提供するためにのみ必要である場合。
(b) エンドユーザーの同意がある場合。
(c) エンドユーザーから特別に要求されたサービスを提供するために厳密に必要である場合。
(d) 視聴者測定のみを目的として必要な場合。ただし、当該測定は、該当する場合、規則（EU）2016/679の第26条または第28条に定める条件を満たすことを条件として、エンドユーザが要求したサービスの提供者、第三者、または第三者が要求したサービスの提供者に代わって、もしくは第三者と共同して実施される場合。
(da)情報社会サービスまたはエンドユーザーの端末機器のセキュリティの維持または修復、不正行為の防止、技術的障害の防止または検出のために、その目的のために必要な期間、必要である場合。
(e) ソフトウェアのアップデートのために必要である場合。
　(i) 当該アップデートはセキュリティ上の理由から必要であり、エンドユーザが選択したプライバシー設定を変更するものではないこと。
　(ii) アップデートがインストールされるたびに、エンドユーザーに事前に通知されること。
　(iii) エンドユーザーに、これらのアップデートの自動インストールを延期または停止する可能性が与えられていること。
(f) 第 13 条(3)に従い、エンドユーザーが欧州単一緊急番号「112」または国家緊急番号のいずれかに緊急通信を行う際に、端末機器の位置を特定する必要がある場合。
(g) 本項に基づき情報が収集された目的以外の目的のための処理が、エンドユーザーの同意又は第11条にいう目的を保護するために民主主義社会において必要かつ相当な措置を構成する連合法若しくは加盟国の法律に基づかない場合、処理及び保存能力を使用する者又はエンドユーザーの端末機器により処理され若しくは発せられ若しくは保存された情報を収集する者は、他の目的のための処理が電子通信データを当初収集した目的に適合するかどうかを確かめるため、特に以下の点を考慮するものとする。
　(i) 処理及び保存能力が使用された目的又は情報が収集された目的と意図された更なる処理の目的との間のあらゆる関連性。
　(ii) 処理及び保存能力が使用され、又は情報が収集された状況、特に関係するエンドユーザーとプロバイダーとの関係。
　(iii)規則(EU)2016/679の第9条または第10条に基づき、意図された更なる処理がデータのカテゴリーを明らかにし得る場合は特に、処理および保存機能または情報の収集の性質、ならびに意図された更なる処理の様式。
　(iv) エンドユーザーに対する意図された追加処理の起こりうる結果。
　(v) 暗号化や仮名化などの適切なセーフガードの存在。
(h) 第1項(g)に従った追加処理は、以下のように見なされます。適合する場合、以下の条件でのみ実施することができる。
　(i) 目的の達成に必要でなくなった時点で、情報を消去し、または匿名化する。
　(ii) 処理が仮名化された情報に限定されていること。
　(iii) 情報が、エンドユーザーの性質もしくは特徴を決定するため、またはエンドユーザーのプロファイルを構築するために使用されないこと。
　(i) 第1項 (g) 及び (h) の目的では、規則 (EU) 2016/697 の第28条に定める条件を満たすか、データが匿名化されない限り、データを第三者と共有してはならないものとします。

（出所）ePrivacy規則EU閣僚理事会案（https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf）（2021年12月14日アクセス）

（参考）法執行、国家安全保障目的の処理・保存（第6条1項(d)、第7条4項）

■ 第6条1項(d)、第7条4項では、法執行、国家安全保障の目的で電子通信データを処理・保存することを認めている。

- 現行のePrivacy指令第15条においても同様の規定が設けられているが、無差別にトラフィックや位置情報を保管することを電子通信サービス提供者に求める国内法（ドイツのデータ保持法等）は、EU法に抵触するとの見解を欧州司法裁判所が示している。
- EDPBは、法執行または国家安全保障の目的であっても、無差別にトラフィックや位置情報を保管することを規定する立法措置は認められないと解釈すべきであると主張している。

（参考）ePrivacy規則案第6条1項(d)、第7条4項条文

第6条電子通信データの許可された処理
1. 電子通信ネットワーク及びサービスのプロバイダは、以下の場合に限り、電子通信データを処理することを許可されるものとする。
(a) 電子通信サービスを提供するために必要である場合。
(b) 電子通信ネットワークおよびサービスのセキュリティを維持もしくは回復するため、または電子通信ネットワークおよびサービスにおける技術的な欠陥、エラー、セキュリティリスクもしくは攻撃を検出するために必要であること。
(c) エンドユーザーの端末機器に対するセキュリティリスクまたは攻撃を検出または防止するために必要である場合。
(d) 組合法または加盟国法によって定められた、プロバイダが従うべき法的義務を遵守するために必要であり、基本的権利および自由の本質を尊重し、犯罪の防止、捜査、検出もしくは訴追または刑事罰の執行、および公共の安全に対する脅威の保護と防止を守るために民主主義社会において必要かつ適切な措置となる場合。

第7条 電子通信データの保存と消去
4. 連邦法又は加盟国法は、刑事犯罪の防止、捜査、探知若しくは訴追又は刑事罰の執行並びに公共の安全に対する脅威の保護及び防止を保護するために、基本的権利及び自由の本質を尊重し、民主社会における必要かつ相当な措置であるあらゆる保持措置の下で、電子通信メタデータを一定期間保持することを規定することができる。連合又は加盟国の公共の安全に対する脅威が継続する場合、保持の期間を延長することができる。

（出所）ePrivacy規則EU閣僚理事会案（https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf）（2021年12月14日アクセス）
欧州司法裁判所プレスリリース（https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-10/cp200123en.pdf）（2021年12月14日アクセス）

デジタルサービス規則案（DSA案）

デジタルサービス規則案（DSA案）

背景と議論状況

■ 2020年12月15日、欧州委員会は「デジタルサービス規則（DSA：Digital Services Act）案」および「デジタル市場規則（DMA：Digital Markets Act）案」を採択した。

■ これらは、「デジタルサービス法パッケージ」と呼ばれ、デジタル単一市場のゲートキーパーであるオンラインプラットフォーム及び、将来ゲートキーパーになり得るオンラインプラットフォームに様々な義務を課す内容となっている。

DSA、DMAの議論状況

時期	議論状況
2020/12	• 欧州委員会が両法案を採択。
2021/5	• EU閣僚理事会は、競争力諮問委員会（Competitiveness Council）にて、交渉継続指針に係る意見を交換。
2021/11	• EU閣僚理事会は、両法案に係る提案に関する見解（一般的アプローチ）に対し、賛成多数にて合意。
2021/12	• 欧州議会は、EU理事会による修正案に係る報告を承認。
2022/1	• 欧州議会がDSA案に係る見解を可決し、EU閣僚理事会、欧州委員会との三者対話の開始が可能な段階に移行。 • 欧州議会がDMA案に関して、EU閣僚理事会、欧州委員会との三者対話を開始。

（出所）
・EUR-Lex（https://eur-lex.europa.eu/legal-content/en/HIS/?uri=CELEX:52020PC0825）（2022年1月24日アクセス）
・EUR-Lex（https://eur-lex.europa.eu/legal-content/en/HIS/?uri=COM:2020:842:FIN）（2022年1月24日アクセス）
・欧州議会「EU Digital Markets Act and Digital Services Act explained」（https://www.europarl.europa.eu/news/en/headlines/society/20211209STO19124/eu-digital-markets-act-and-digital-services-act-explained）（2022年1月24日アクセス）

デジタルサービス規則案　概要

■目的：

- より安全なオンライン環境の構築
- マーケットプレイスやソーシャルメディアなどのプラットフォームに対する、明確な責任の定義
- 現状のデジタル上の課題への対処
  - 違法な商品、ヘイトスピーチ、偽情報
  - 透明性のあるデータ報告および監視

■特徴：

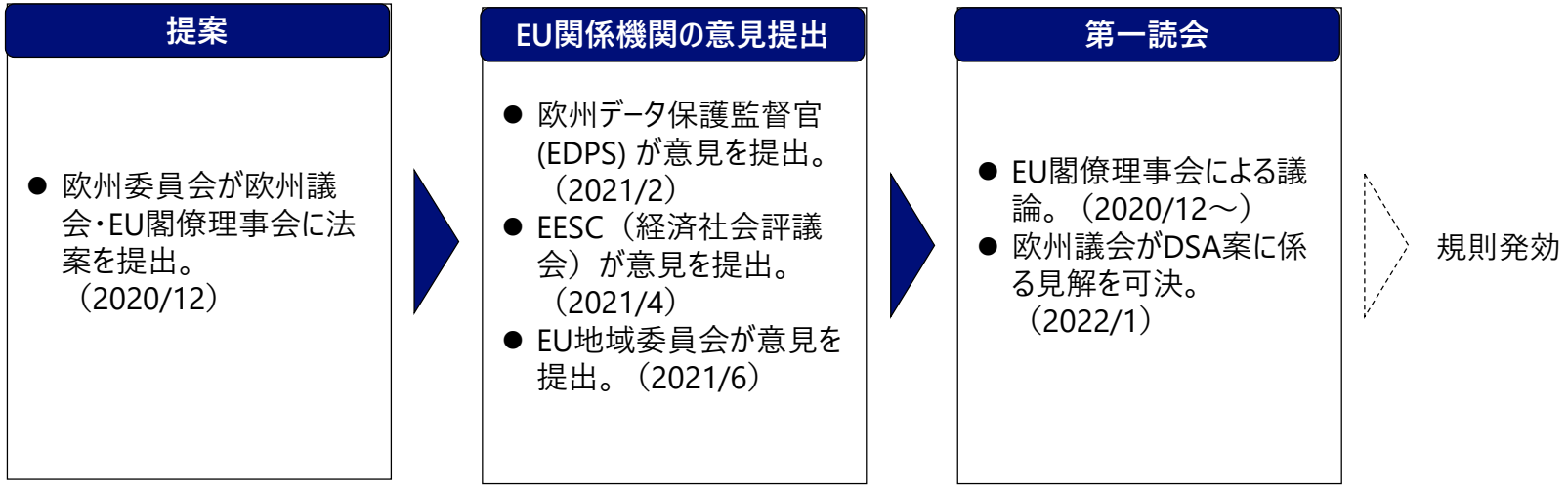
- 社会的影響が大きいとされる「オンライン仲介サービス」に対しては、より厳格な規則が適用されるように、規則が非対称に設計されている。
- デジタル時代に即したガバナンスの枠組みが提供されており、「オンライン仲介サービス」に対する明確なデューデリジェンス義務が規定されている。

（出所）
・欧州理事会「Infographic - Digital Services Act」（https://www.consilium.europa.eu/en/infographics/digital-services-act/）（2022年1月24日アクセス）
・欧州理事会「What is illegal offline should be illegal online: Council agrees position on the Digital Services Act」（https://www.consilium.europa.eu/en/press/press-releases/2021/11/25/what-is-illegal-offline-should-be-illegal-online-council-agrees-on-position-on-the-digital-services-act/）（2022年1月24日アクセス）

デジタルサービス法（DSA）案の立法プロセス

- DSA案は、通常立法手続に基づき審議されており、欧州委員会からの提案に基づき、欧州議会とEU閣僚理事会が共同で規則を採択する。
- 現在、DSA案は第一読会のステータスにあり、欧州議会、EU閣僚理事会、欧州委員会による三者対話の開始が可能な段階に移行している。

DSA案の立法プロセス



（出所）
・EUR-Lex（https://eur-lex.europa.eu/legal-content/en/HIS/?uri=CELEX:52020PC0825）（2022年2月14日アクセス）

デジタルサービス規則案（DSA案）

デジタルサービス法（DSA）案　構成

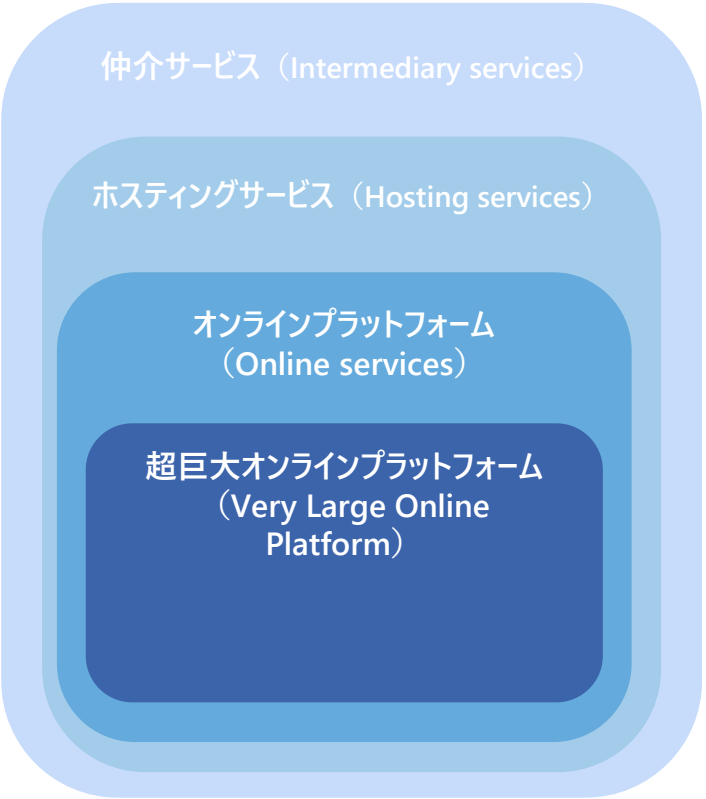
第Ⅰ章 総則	第1条～第2条	• 規則の主題と範囲、用語の定義
第Ⅱ章 仲介サービス提供者の責任	第3条～第9a条	• 違法コンテンツに対する措置命令への対応等
第Ⅲ章 透明で安全なオンライン環境のためのデューデリジェンス義務	第10条～第37条	• 第1節 すべての仲介サービス提供者に適用される規定 • 第2節 オンラインプラットフォームプロバイダを含むホスティングサービスプロバイダに適用される追加規定 • 第3節 オンラインプラットフォームプロバイダに適用される追加規定 • 第4節 システムリスクを管理するための超大規模オンラインプラットフォームの追加義務 • 第5節 デューデリジェンス義務に関するその他の規定
第Ⅳ章 実施、協力、制裁、執行	第38条～第70条	• 第1節 主務官庁及び各国デジタルサービス調整官 • 第2節 欧州デジタルサービス会議 • 第3節 超大規模オンライン・プラットフォームに関する監視、調査、遵守及びモニタリング • 第4節 遵守に関する共通規定 • 第5節 委任された行為
第Ⅴ章 最終条項	第71条～第74条	• eコマース指令の改正(第12条～第15条の削除：該当条項を本規則に取り込むため)、指令2020/XX/ECの改正、本規則の評価、発効と適用

（出所）総務省 プラットフォームサービスに関する研究会「インターネット上の違法・有害情報を巡るEUの動向 －Digital Services Act について－」（https://www.soumu.go.jp/main_content/000738571.pdf）（2022年1月24日アクセス）

デジタルサービス法（DSA）案の対象プロバイダ

■ DSA案は、対象プロバイダを役割、規模、影響力に応じて分類し、比例的に義務を規定している。

対象プロバイダ分類*



■ **仲介サービス**（Intermediary services）
- ネットワークインフラを提供する仲介サービス。単なる導管（mere conduit）、キャッシング（caching）、ホスティング（hosting）、オンライン検索エンジン（online search engine）の総称。

■ **ホスティングサービス***（Hosting services）
- クラウドやウェブホスティングなどのホスティングサービス。

■ **オンラインプラットフォーム**（Online services）
- オンラインマーケットプレイス、アプリストア、コラボレーションエコノミープラットフォーム、ソーシャルメディアプラットフォームなど、売り手と消費者を結びつけるオンラインプラットフォーム。

■ **超巨大オンラインプラットフォーム**（Very Large Online Platform）
- オンラインプラットフォームのうち、欧州での月間平均利用者が4,500万人を超えており、少なくとも4ヶ月以上サービスを提供している事業者。

*小規模オンラインプラットフォーム（micro or small enterprises）は規制対象除外

（出所）
・欧州委員会HP（https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en）（2022年1月24日アクセス）
・欧州議会修正案（https://www.europarl.europa.eu/doceo/document/TA-9-2022-0014_EN.pdf）（2022年1月24日アクセス）

デジタルサービス法（DSA）案における対象プロバイダごとの義務

	2022/1/20 欧州議会修正案における対応箇所	仲介サービス	ホスティングサービス	オンラインプラットフォーム	超巨大オンラインプラットフォーム
命令を受けた国家当局との協力とサービスの受け手の救済措置	第8条、第9条、第9a条	●	●	●	●
窓口および必要な場合は法定代理人	第10条、第10a条、第11条	●	●	●	●
基本的人権を考慮した利用規約の要求事項	第12条	●	●	●	●
透明性のある報告	第13条	●	●	●（第23条も追加）	●（第23条、第33条も追加）
オンライン・インターフェースの設計と構成	第13a条	●	●	●	●
ユーザーへの告知・対応と情報提供義務	第14条、第15条		●	●	●
犯罪行為の報告	第15a条		●	●	●
内部苦情処理システムと裁判外紛争解決	第17条、第18条			●	●
信頼できるフラガー（flaggers）	第19条			●	●
オンラインに関するアクセシビリティ要件	第19a条			●	●
不正使用に対する対策と保護	第20条			●	●
オンラインプラットフォームを利用する取引業者のトレーサビリティ	第22条			●	●
違法な製品・サービスに関する消費者・当局への情報提供	第22a条			●	●
オンライン広告のユーザー向け透明性	第24条			●	●
リコメンダーシステムの透明性	第24a条			●	●（第29条も追加）
ユーザーが作成したポルノコンテンツへの対策	第24b条			●	●
リスク管理義務とコンプライアンス・オフィサー	第26条、第27条、第32条				●
外部リスク監査と説明責任	第28条				●
オンライン広告の追加的な透明性	第30条				●
ディープフェイクの透明性	第30a条				●
当局や研究者とのデータ共有	第31条				●
行動規範	第35条、第36条				●
危機対応協力	第37条				●

出所）・欧州議会修正案（https://www.europarl.europa.eu/doceo/document/TA-9-2022-0014_EN.pdf）（2022年1月24日アクセス）
・張睿暎 EUにおけるプラットフォーム規制と「デジタルサービス法」規則案の意義獨協法学第115号（2021年8月）211-244頁

デジタルサービス規則案（DSA案）

オンライン広告の透明性を高めるため、リアルタイムで分かりやすい通知やリポジトリの公開がプラットフォーム事業者に求められる。（第24条、第30条）

オンラインプラットフォーム（第24条）	**【ユーザーへの通知】** • 個人に対して表示される広告ごとに、以下をユーザーが分かりやすい方法でリアルタイムに認識できるようにする。 (a) 表示された情報がオンライン広告であること（目立つ、整合のとれたマークによりその旨を示すことを含む。） (b)広告を代理で表示している自然人又は法人 (ba)広告に資金を提供する自然人又は法人（(b)で言及された自然人又は法人と異なる場合） (c) 広告が表示されるユーザーを特定するために使用されるパラメータに関する明確で、有意義かつ統一された情報、および該当する場合には、それらのパラメータを変更する方法に関する情報。
超巨大オンラインプラットフォーム（第30条）	**【リポジトリの公開】** • 広告がオンラインインタフェースに最後に表示されてから1年後まで、アプリケーションプログラミングインタフェースを介して、簡単にアクセスでき、効率的で信頼できるツールにより、以下を含むリポジトリを公開し、検索できるようにする。 (a) 広告の内容。商品名、サービス名 またはブランド、およびその対象広告。 (b)広告が表示されている自然人または法人。 (ba)広告に資金を提供する自然人又は法人（(b)で言及された自然人又は法人と異なる場合） (c)広告が表示されていた期間。 (d)広告がユーザーの一つ以上の特定のグループに特に表示されることを意図していたかどうか。該当する場合、特定のグループを除外するために使用されたパラメータを含む、その目的のために使用された主なパラメータ。 (da)開示されている場合、超巨大オンラインプラットフォームで公開された商業通信の内容のコピーで、超大型オンラインプラットフォームによって市販、販売または手配されておらず、適切な経路を通じて超巨大オンラインプラットフォームに対してそのように宣言されているもの。 (e)到達したユーザーの総数、および該当する場合、広告が特に対象とされたユーザーのグループ又は集団の総数。 (ea) 第14条に従って提出された通知又は第8条に従って出された命令に基づいて広告が削除された場合。 • 上記のリポジトリは、広告主ごとに、広告、広告のターゲット、広告主が到達したいユーザーに存在するすべてのデータポイントごとに多基準クエリを実行できることを保証する。また、広告が表示された、または表示され得たサービスの受信者の個人情報が含まれないことを保証し、情報が正確かつ完全であることを保証するために合理的な努力をする。

出所）・欧州議会修正案（https://www.europarl.europa.eu/doceo/document/TA-9-2022-0014_EN.pdf）（2022年1月24日アクセス）

デジタルサービス規則案（DSA案）

欧州委員会は、第24条・第30条の要件及び、より高いレベルのオンライン広告の透明性確保を目指し、自主的な規格・行動規範の作成を促進する。（第34条、第36条）

【第34条（標準規格）】　※オンライン広告に係る規定のみ抜粋

■ 欧州委員会は、第24条、第30条の要件について、関連する欧州および国際標準化団体が定めた自主的な規格の開発・実施を支援、促進する。

- 広告慣行（第24条）
- 広告仲介者間のデータ送信（第24条(b)(c)）
- リポジトリの公開を容易にするためのアプリケーションプログラミングインタフェースを含む特定のインタフェース（第30条）
- 広告リポジトリの相互運用性（第30条第2項）

【第36条（オンライン広告の行動規範）】

■ 欧州委員会は、第24条、第30条の要件より高い透明性確保を目指し、オンラインプラットフォームおよびその他の関連サービス提供者との間で、以下の項目に対応する連合レベルでの自主的な行動規範の作成を奨励、促進する。

- 第24条(b)(c)に定める要件に関して、オンライン広告の仲介を行うプロバイダーが保有する情報のユーザーへの伝達
- 第30条に基づき、オンライン広告配信事業者が保有する情報をリポジトリに送信すること
- 利用可能なデータの種類

■ 欧州委員会は、オンライン広告エコシステムのすべての関係者が、行動規範に記載されたコミットメントを支持し、遵守することを奨励する。

出所）欧州議会修正案（https://www.europarl.europa.eu/doceo/document/TA-9-2022-0014_EN.pdf）（2022年1月24日アクセス）

デジタルサービス規則案（DSA案）

欧州議会修正案では、ダークパターン規制が追加されている。（第13a条）

■ 第13a条（オンライン・インターフェースの設計と構成）は、以下の手法により、ユーザーが十分な情報を得たうえで意思決定を行う能力を歪めることを禁止している。

- いずれかの同意の選択肢をより視覚的に目立たせること。
- データ処理への同意が拒否された場合に、当該処理の範囲や目的にかかわらず、特にユーザー体験を阻害するポップアップを表示することにより、ユーザーに対してデータ処理への同意を繰り返し求めること。
- ユーザーが既に選択した後に、サービスの設定または構成を変更するよう促すこと。
- サービスの終了手続きを、サービスにサインアップするよりも著しく面倒にすること。
- GDPR第21条第5項に沿って、ユーザーが技術仕様を用いて、自動化された手段により異議を述べる権利を行使する場合に、同意を求めること。

■ 欧州委員会は、上記の禁止事項リストを更新するために、委任法を採択する権限を有する。

出所）欧州議会修正案（https://www.europarl.europa.eu/doceo/document/TA-9-2022-0014_EN.pdf）（2022年1月24日アクセス）

デジタルサービス規則案（DSA案）

仲介サービスの免責（第3条～第5条）

■仲介サービス事業者には、一定の免責条件が設けられている。

仲介サービス事業者の分類	免責条件
単なる導管 （サービス受信者によって提供される情報の通信ネットワークにおける伝送や、通信ネットワークへのアクセスを提供する）	サービスの受信者によって提供された情報の通信ネットワークにおける送信、または通信ネットワークへのアクセスの提供からなる情報社会サービスが提供される場合、サービス提供者は、以下を条件として、送信された情報に対して責任を負わない。 (a)送信を開始しない。 (b)送信の受信者を選択せず、かつ (c)伝送に含まれる情報を選択または変更しないこと。
キャッシング （サービス受信者によって提供される情報の通信ネットワークでの送信からなり、その情報の自動的、中間的、一時的な保存を含み、その情報の他の受信者の要求に応じて、その送信をより効率的にすることを唯一の目的として実行される）	サービスの受信者によって提供された情報の通信ネットワークにおける伝送からなる情報社会サービスが提供される場合、サービス提供者は、サービスの他の受信者の要求に応じて情報の送信をより効率的または安全にすることのみを目的として行われる、当該情報の自動的、中間および一時的保存について責任を負わないものとし、その条件は、以下のとおりである。 (a)情報を変更しないこと。 (b)情報へのアクセスに関する条件を遵守すること。 (c)業界で広く認識され使用されている方法で指定された、情報の更新に関する規則を遵守すること。 (d)情報の使用に関するデータを得るために、業界で広く認識され使用されている技術の合法的な使用を妨げないこと。 (e)最初の送信元における情報がネットワークから削除され、もしくはアクセスが不能になったこと、または裁判所もしくは行政当局が当該削除もしくは不能を命じたことを実際に知った場合には、保存している情報を削除し、またはアクセスを不能にするために迅速に行動すること。
ホスティング （サービスの受け手から提供された、または受け手の要求による情報の保存からなる）	1. サービスの受信者によって提供された情報の保存からなる情報社会サービスが提供される場合、サービスの提供者は、サービスの受信者の要求により保存された情報に対して、以下の条件で責任を負わない。 (a)違法行為または違法なコンテンツを実際に知らず、損害賠償請求に関しても、違法行為または違法なコンテンツが明白となる事実または状況を知らないこと。 (b)そのような知識または認識を得た後、違法なコンテンツを削除し、または違法なコンテンツへのアクセスを不能にするために迅速に行動した場合。 2. 第1項は、サービスの受領者が提供者の権限または管理の下で行動している場合には適用されない。 3. 第1項は、消費者が取引者と遠隔契約を締結することを可能にするオンラインプラットフォームの、消費者保護法に基づく責任に関して、当該オンラインプラットフォームが、情報の特定の項目、または取引の対象である製品もしくはサービスが、オンラインプラットフォーム自体またはその権限もしくは支配下で行動するサービスの受領者によって提供されると消費者が信じるような方法で、問題の特定の取引を提示するか、その他の方法で可能にする場合には適用しない。

出所）・欧州議会修正案（https://www.europarl.europa.eu/doceo/document/TA-9-2022-0014_EN.pdf）（2022年1月24日アクセス）

デジタルサービス規則案（DSA案）

仲介サービスの義務（第8条～第13a条）

条項	項目	内容
第8条	違法コンテンツに対する措置命令	• 仲介サービスのプロバイダは、適用されるEU法又は国内法に基づいて、関連する国の司法当局又は行政当局から受領し、発行された、一つ又は複数の特定の項目の違法コンテンツに対して行動する命令を、安全な通信チャネルを介して受信した場合、EU法に準拠し、命令を発行した当局に、不当に遅延することなく、実行した行動及び実行した時点を特定して、当該命令に与えられた効力を通知する。
第9条	情報提供の命令	• 仲介サービスのプロバイダは、1人以上の特定の個人のサービス受領者に関する特定の項目の情報を提供する命令を、安全な通信チャネルを介して受領した場合、関連する国の司法又は行政当局から、適用されるEU又は国の法律に基づいて、EU法に準拠して、不当に遅延なく、その命令の発行機関に、受領とその命令に与えられた効果を通知しなければならない。
第9a条	サービスの受け手に対する効果的な救済措置	• 第8条に従ってコンテンツが削除された、または第9条に従って情報が求められたサービスの受領者は、指令（EU）2016/680および規則（EU）2016/679に基づいて利用できる救済を害することなく、当該命令に対して、当該コンテンツが条件を遵守していたにもかかわらず、サービス提供者によって誤って違法とみなされた場合のコンテンツの復元を含め、場合によっては有効な救済を受ける権利を有する。
第10条	加盟国当局、欧州委員会、理事会の連絡先	• 仲介サービスのプロバイダーは、この規則の適用に関して、加盟国の当局、欧州委員会、および第47条に言及された委員会と電子的手段で直接連絡を取ることができる単一の窓口を指定するものとする。
第10a条	サービスの受け手に関する窓口	• 仲介サービスの提供者は、サービスの受領者が直接連絡を取ることができる単一の窓口を指定するものとする。
第11条	法定代理人	• 連合国内に施設を有しないが、連合国内で役務を提供する仲介役務の提供者は、書面により、提供者が役務を提供する加盟国のいずれかにおいて、法定代理人となる法人又は自然人を指名するものとする。
第12条	利用条件	• 仲介サービスの提供者は、公正で非差別的かつ透明性のある条件を用いるものとする。仲介サービスの提供者は、これらの条件を、明確、平易、ユーザーフレンドリーかつ曖昧でない言語で作成し、サービス提供先である加盟国の言語で、容易にアクセス可能かつ機械可読の形式で公に利用可能でなければならない。仲介サービスの提供者は、その条件において、憲章に謳われている表現の自由、メディアの自由と多元性、その他の基本的な権利と自由、および連合におけるメディアに適用される規則を尊重するものとする。
第13条	仲介サービスのプロバイダーに対する透明性報告義務	• 仲介サービスのプロバイダは、少なくとも年に一度、標準化された機械可読の形式かつ、容易にアクセスできる方法で、該当期間中に行った、すべてのコンテンツの修正に関する、明確かつ容易に理解できる詳細な報告書を公表しなければならない。
第13a条	オンライン・インターフェースの設計と構成	• 仲介サービスのプロバイダは、サービスの受領者が自由、自律的、かつ十分な情報を得た上で、意思決定または選択を行う能力を歪め、または損なうような、オンライン・インターフェースまたは、その一部の構造、機能または操作方法を用いてはならない。

出所）・欧州議会修正案（https://www.europarl.europa.eu/doceo/document/TA-9-2022-0014_EN.pdf）（2022年1月24日アクセス）

デジタルサービス規則案（DSA案）

ホスティングサービスの義務（第14条～第15a条）

条項	項目	内容
第14条	通知と措置のメカニズム	• ホスティングサービスの提供者は、個人または団体が違法コンテンツとみなす特定の情報項目が、そのサービス上に存在することを通知できる仕組みを導入するものとする。これらのメカニズムは、アクセスが容易でユーザーフレンドリーであり、電子的手段のみによる通知の提出が可能なものとする。
第15条	理由説明書	• ホスティングサービスの提供者が、サービスの受領者によって提供された特定の情報項目に関して、その情報の検出、特定、アクセスの削除または無効化に使用される手段およびその決定の理由にかかわらず、削除、アクセス無効化、降格、その他の措置を課すことを決定した場合、遅くとも削除またはアクセス無効化の時点で、受領者にその決定を通知し、その決定の理由を明確かつ具体的に説明しなければならない。この義務は、コンテンツが欺瞞的な大量の商業コンテンツである場合、または司法当局もしくは法執行当局から、犯罪捜査が進行中のため、犯罪捜査が終了するまで受領者に通知しないよう要請された場合には適用されない。
第15a条	刑事犯罪の疑いの届出	• ホスティングサービスのプロバイダは、人の生命または安全に対する差し迫った脅威を伴う重大な犯罪が行われた、行われている、または行われる予定であると疑いうる情報を知った場合、その疑いを加盟国または関係加盟国の法執行機関または司法機関に速やかに知らせ、その要請に応じて、利用できるすべての関連情報を提供しなければならない。

出所）・欧州議会修正案（https://www.europarl.europa.eu/doceo/document/TA-9-2022-0014_EN.pdf）（2022年1月24日アクセス）

デジタルサービス規則案（DSA案）

オンラインプラットフォームの義務（第17条～第24b条）（1/3）

条項	項目	内容
第17条	内部苦情処理システム	• オンラインプラットフォームは、本項で言及された決定から少なくとも6ヶ月の期間、サービスの受領者に対し、受領者が提供した情報が、違法コンテンツまたはその条件に適合しないという理由で、オンラインプラットフォームが行った以下の決定に対して、電子的かつ無料で苦情を申し立てることができる有効な内部苦情処理システムへアクセスできるようにするものとする。 (a) 情報の削除、降格、アクセス不能、または可視性、利用可能性またはアクセス性を制限するその他の措置を課す決定。 (b)受領者に対するサービスの全部または一部の提供を停止、終了、または制限する決定。 (c)受領者のアカウントを停止または終了させる決定。 (c)受領者が提供するコンテンツのマネタイズ能力を制限する決定。
第18条	裁判外紛争解決	• オンラインプラットフォームが、受領者が提供する情報が違法コンテンツである、またはその条件に適合しないことを理由に行った、第17条第1項の決定に対応するサービスの受領者は、同条の内部苦情処理システムによって解決できなかった苦情を含め、これらの決定に関する紛争を解決するために、第2項に従って認定された法廷外紛争解決機関を選択する権利があるものとする。
第19条	信頼できるフラガー（flaggers）	• オンラインプラットフォームは、第14条に言及されたメカニズムを通じて、その指定された専門領域内で行動する、信頼できるフラグ作成者によって提出された通知が、適正手続を考慮し、優先的かつ迅速に処理および決定されることを保証するために必要な、技術的および組織的な措置を講じるものとする。
第19a条	オンラインに関するアクセシビリティ要件	• 連合内でサービスを提供するオンラインプラットフォームのプロバイダーは、指令（EU）2019/882の附属書Iのセクション III、セクションIV、セクションVI及びセクションVIIIに定めるアクセシビリティ要件に従ってサービスを設計し、提供することを保証するものとする。
第20条	不正使用に対する対策と保護	• オンラインプラットフォームは、合理的な期間、事前警告を行った後、違法なコンテンツを頻繁に提供し、法的または事実的な調査を行うことなく違法性が立証され、または過去12ヶ月間に2回以上の違法コンテンツに関する措置命令を受けたサービスの受領者に対する、サービスの提供を停止する権利を有するものとする（これらの命令が後に覆された場合を除く）。
第22条	取引業者のトレーサビリティ	• 消費者が取引業者と遠隔契約を締結することを可能にするオンラインプラットフォームは、取引業者が、それらの目的のためにサービスを利用する前に、以下の情報を提供された場合にのみ、連合内に所在する消費者に対するメッセージの宣伝、または製品もしくはサービスの提供を行うためにサービスを利用できることを保証するものとする。

出所）・欧州議会修正案（https://www.europarl.europa.eu/doceo/document/TA-9-2022-0014_EN.pdf）（2022年1月24日アクセス）

デジタルサービス規則案（DSA案）

オンラインプラットフォームの義務（第17条～第24b条）（2/3）

条項	項目	内容
第22a条	違法な製品・サービスに関する消費者・当局への情報提供義務	• 消費者が販売者との遠隔契約を締結できるオンラインプラットフォームが、そのプラットフォームのインターフェース上で販売者が提供する製品またはサービスが、連合法または国内法の適用要件に照らして違法であることを認識した場合、使用する手段に関わらず、そのプラットフォームは以下のことを行わなければならない。 (a) インターフェースから違法な製品またはサービスを迅速に削除し、必要に応じて市場監視当局または税関当局などの関連当局に決定事項を通知する。 (b) オンラインプラットフォームがサービスの受領者の連絡先を知っている場合、当該製品またはサービスを取得したサービスの受領者に、違法性、取引者の身元、救済を求めるための選択肢を通知すること。 (c) 過去12ヶ月間にプラットフォームから削除された違法な製品及びサービスに関する情報を含むリポジトリを編集し、アプリケーションプログラミングインタフェースを通じて一般に利用可能にすること。
第23条	オンラインプラットフォームのプロバイダーに対する透明性報告義務	• オンライン・プラットフォームは、第13条の情報に加え、同条の報告書に以下の情報を記載するものとする。 (a)第18条に言及される、法廷外紛争解決機関に提出された紛争の数、紛争解決の結果、および紛争解決手続きの完了に要した平均時間。 (aa) 第17条の内部苦情処理システムを通じて受領した、苦情の件数、苦情の根拠、これらの苦情に関して行われた決定、これらの決定に要した平均時間及び中央値並びにこれらの決定が取り消された場合の件数。 (b)第20条に基づき課された停止措置の件数。違法コンテンツの提供、明白な根拠のない通知の提出、明白な根拠のない苦情の提出を理由に課された停止措置は区別される。 (c)正確な目的の特定、目的を達成するために自動化された手段の正確さの指標、および適用された保護を含む、コンテンツ調整の目的のために自動化された手段の使用。 (ca)オンラインプラットフォームによって削除、ラベル付け、または無効化された広告の数および、その決定の正当性
第24条	オンライン広告の透明性	• オンライン・インターフェースに広告を表示するオンライン・プラットフォームは、サービスの受領者が、個々の受領者に表示される特定の広告ごとに、明確、簡潔、かつ曖昧でない方法で、リアルタイムに識別できるようにするものとする。 (a) インターフェースに表示された情報又はその一部がオンライン広告であることを、目立つように調和された表示によって識別することを含む。 (b)広告が表示されている自然人又は法人。 (ba)広告に資金を提供する自然人又は法人（この者が(b)で言及された自然人又は法人と異なる場合）。 (c) 広告が表示される受領者を決定するために使用されるパラメータに関する、明確で、有意義かつ統一された情報、および該当する場合には、それらのパラメータを変更する方法に関する情報。

出所）・欧州議会修正案（https://www.europarl.europa.eu/doceo/document/TA-9-2022-0014_EN.pdf）（2022年1月24日アクセス）

デジタルサービス規則案（DSA案）

オンラインプラットフォームの義務（第17条～第24b条）（3/3）

条項	項目	内容
第24a条	リコメンダーシステムの透明性	• オンライン・プラットフォームは、その利用規約において、コンテンツが推奨される際に、オンライン・プラットフォームのオンライン・インターフェースから直接到達し、容易に発見可能な指定オンライン・リソースを通じて、そのリコメンダーシステムで使用される主要パラメータ、およびサービスの受領者が利用可能な主要パラメータを修正、または影響のあるオプションについて、明確でアクセス可能、かつ容易に理解できる方法で定めなければならない。
第24b条	主に、ユーザー作成ポルノコンテンツの普及に使用されるプラットフォームに対する追加義務	• オンラインプラットフォームが主に、ユーザーが作成したポルノコンテンツの普及のために使用される場合、プラットフォームは、確実にするために必要な技術的および組織的な措置を講じるものとする。 (a) コンテンツを発信するユーザーは、電子メールと携帯電話のダブルオプトイン登録によって本人確認を行っていること。 (b) 違法である可能性の高いコンテンツを含む、画像ベースの性的虐待を識別するために訓練された、専門的な人間のコンテンツモデレーション。 (c) 第14条に言及されたメカニズムに加えて、個人が、自分を描写した、または自分を描写していると称する画像素材が、本人の同意なしに流布されているという主張をプラットフォームに通知し、本人の物理的同一性の一応の証拠を提供できる形式での適格通知手続きの利用性；この手続きを通じて通知されたコンテンツは、不当に遅れることなく停止されなければならないこと。

出所）・欧州議会修正案（https://www.europarl.europa.eu/doceo/document/TA-9-2022-0014_EN.pdf）（2022年1月24日アクセス）

デジタルサービス規則案（DSA案）

超巨大オンラインプラットフォームの義務（第26条～第37条）（1/3）

条項	項目	内容
第26条	リスク評価	• 超巨大オンラインプラットフォームは、第25条第4項第2号で言及された適用日から、その後少なくとも年に1回、いかなる場合でも新しいサービスを開始する前に、そのサービスの設計、アルゴリズムシステム、固有の特性、機能および連合内での使用に起因する重大なシステミック・リスクの可能性と重大性を、効果的かつ熱心に特定、分析、評価するものとする。リスク評価は、サービスが提供される加盟国ごと、および連合全体、特に特定の言語または地域に対するリスクを考慮するものとする。このリスク評価は、技術設計、ビジネスモデルの選択など、そのサービスや活動に特有のものでなければならず、以下のシステミック・リスクを含むものでなければならない。 (a) 自己のサービスを通じて違法なコンテンツを流布すること、またはそのようなコンテンツがあること。 (b) 消費者保護、人間の尊厳の尊重、私生活と家族生活、個人情報の保護、表現と情報の自由、メディアの自由と多元性、差別の禁止、男女平等の権利、憲章の1条、7条、8条、11条、21条、23条、24条、38条にそれぞれ謳われている子どもの権利などの基本権の行使に対する、実際および予見可能な、あらゆる否定的影響。 (c) 不正使用や自動搾取によるものを含む、サービスの誤作動や意図的な操作、または違法コンテンツの増幅、利用規約に違反したコンテンツ、未成年者やサービスの受領者の、その他の弱者グループの保護、民主的価値、メディアの自由、表現の自由、市民的言説、選挙プロセスや公共の安全に関する実際または予見可能な影響など、サービスの意図した運用に内在するリスク。 (ca) 公衆衛生の保護、行動依存症、またはその人の身体的、精神的、社会的、経済的な幸福に対するその他の深刻な悪影響に対する実際および予測可能な悪影響。
第27条	リスクの軽減	• 超大型オンラインプラットフォームは、第26条により特定された、特定のシステミック・リスクに合わせた、合理的、透明、比例的かつ効果的な緩和策を導入するものとする。
第28条	独立監査人による監査	• 超巨大オンライン・プラットフォームは、自己の費用で、少なくとも年に一度、以下の遵守状況を評価するための独立した監査を受けるものとする。 (a)第III章に規定される義務 (b) 第35条および第36条で言及される行動規範、および第37条で言及される危機プロトコルに従って実施されるすべてのコミットメント。
第29条	リコメンダーシステム	• 第24a条に定める要件に加えて、リコメンダーシステムを使用する超大型オンラインプラットフォームは、規則（EU）2016/679の第4条（4）の意味において、プロファイリングに基づかない、少なくとも一つのリコメンダーシステムを提供するとともに、サービスの受領者が、自分に提示される情報の相対順序を決定するリコメンダーシステムのそれぞれについて、自分の好む選択肢をいつでも選択し修正できるよう、オンラインインタフェース上で容易にアクセスできる機能を提供するものとする。

出所）・欧州議会修正案（https://www.europarl.europa.eu/doceo/document/TA-9-2022-0014_EN.pdf）（2022年1月24日アクセス）

デジタルサービス規則案（DSA案）

超巨大オンラインプラットフォームの義務（第26条～第37条）（2/3）

条項	項目	内容
第30条	オンライン広告の追加的な透明性	• オンラインインタフェースに広告を表示する超巨大オンラインプラットフォームは、広告がそのオンラインインタフェースに最後に表示されてから1年後まで、アプリケーションプログラミングインタフェースを介して、簡単にアクセスでき、効率的で信頼できるツールを介して、公に検索できるように、第2項に記載の情報を含むリポジトリをコンパイルし、作成するものとする。彼らは、広告主ごとに、広告、広告のターゲット、広告主がターゲットとする観客に存在する、すべてのデータポイントごとに、多基準クエリを実行できることを保証しなければならない。リポジトリには、広告が表示された、または表示され得たサービスの受領者の個人データが含まれないことを保証し、情報が正確かつ完全であることを保証するために合理的な努力をしなければならない。
第30a条	ディープフェイク	• 超巨大オンラインプラットフォームは、あるコンテンツが、既存の人物、物、場所、その他の実体または出来事に著しく類似し、人に本物または真実であると偽って見える、生成または操作された画像、音声または動画コンテンツであることを認識した場合（ディープフェイク）、プロバイダは、そのコンテンツが本物ではないことを知らせ、サービスの受領者が明確に見える方法で、そのコンテンツを表示するものとする。
第31条	データアクセスおよび精査	• 超巨大オンラインプラットフォームは、設立のデジタル・サービス・コーディネーターまたは委員会に対し、その合理的な要求に基づき、指定された合理的な期間内に遅延なく、本規則の遵守を監視し評価するために必要なデータへのアクセスを提供するものとする。そのデジタル・サービス・コーディネーターと委員会は、それらの目的のためにのみ、そのデータを要求し、アクセスし、使用するものとする。
第32条	コンプライアンス・オフィサー	• 超巨大オンラインプラットフォームは、本規則の遵守を監視する責任者である、1人以上のコンプライアンスオフィサーを任命しなければならない。
第33条	超巨大オンライン・プラットフォームに対する透明性報告義務	• 超巨大オンラインプラットフォームは、第25条（4）で言及された申請日から6か月以内、その後6か月ごとに、標準化され、機械可読で容易にアクセスできるフォーマットで、第13条で言及された報告書を公表するものとする。
第35条	行動規範	• 第26条第1項の意味における重大なシステミック・リスクが、複数の超巨大オンラインプラットフォームに関連して発生した場合、欧州委員会は、当該超巨大オンラインプラットフォーム、その他の超大型オンラインプラットフォーム、その他のオンラインプラットフォームおよび仲介サービスのプロバイダー、ならびに適切な場合には、関係当局、市民社会団体およびその他の関係者に、特定のリスク軽減措置をとる約束、ならびにとられた措置およびその結果に関する定期報告の枠組みを設定することなど、行動規範の作成に参加するよう要請できる。

出所）・欧州議会修正案（https://www.europarl.europa.eu/doceo/document/TA-9-2022-0014_EN.pdf）（2022年1月24日アクセス）

デジタルサービス規則案（DSA案）

超巨大オンラインプラットフォームの義務（第26条～第37条）（3/3）

条項	項目	内容
第36条	オンライン広告の行動規範	• 欧州委員会は、オンライン広告のエコシステムにおける、すべての関係者の透明性の向上に寄与するため、第24条および第30条の要件を超えて、オンラインプラットフォームと、オンライン広告仲介サービスのプロバイダーやサービスの受け手を代表する組織、市民社会団体、関係当局などのその他の関連サービス提供者との間で、連合レベルでの自主的な行動規範の作成を奨励、促進するものとする。
第37条	危機管理プロトコル	• 委員会は、超巨大オンラインプラットフォーム、および適切な場合には、その他のオンラインプラットフォームが、委員会の関与のもと、以下の措置の一つ以上を含む危機対応手順の作成、試験、適用に参加することを奨励、促進しなければならない。 (a)加盟国当局またはEUレベルで提供される危機的状況についての情報を目立つように表示すること。 (b)第10条に言及された連絡先が、危機管理の責任を負うことを保証すること。 (c)該当する場合、第14条、17条、19条、20条及び27条に定める義務の遵守に充てる資源を、危機的状況の必要性に応じて適合させること。

出所）・欧州議会修正案（https://www.europarl.europa.eu/doceo/document/TA-9-2022-0014_EN.pdf）（2022年1月24日アクセス）

Transparency and Consent Framework（TCF）

Transparency and Consent Framework（TCF）

- Cookie、広告ID、端末識別子及び、その他のトラッキング技術の取扱いにあたり、GDPR及びeプライバシー指令を遵守するため、IAB Europeが提唱する行動規範。主にポリシーと技術仕様により構成される。
  - 技術仕様はIAB Tech Labが作成している。
  - ポリシー・技術仕様に加えて、TCFを遵守するベンダーリストとCMP事業者リストが存在する。
- Consent Management Platform（CMP）を導入することで、利用者情報の取扱いに関する同意状況を、利用者がベンダー（アドサーバ等の提供事業者）に送信する仕組みを規定している。
- 2018年4月28日にv1.1が発表され、その後パブリッシャーや業界団体からのフィードバックを受け、2019年8月21日にv2.0に改定された。

TCF2.0改定のポイント

ポイント	内容
選択（Choice）	• 利用者情報の処理の目的を、より細分化して定義している。
透明性（Transparency）	• 事業者の「正当な利益」に基づく利用者情報の処理について明確化するとともに、利用者がCMPを通じて「正当な利益」に基づく処理を撤回する方法を紹介している。
コントロール（Control）	• パブリッシャーによる、よりきめ細やかなベンダーコントロールを可能としている。
コンプライアンス（Compliance）	• TCFを利用するユーザーに対するサポートや投資を拡大する。

（出所）IAB Europe（https://iabeurope.eu/transparency-consent-framework/）（2021年11月30日アクセス）

参考：
IAB Europeについて

■ IABとは

- Interactive Advertising Bureauの略称
- 1996年に設立された非営利団体で、本部はニューヨークに設置。45の国際組織より構成されるグローバルのネットワークを持つ。
  - 加入企業の多くは米国と欧州に所在。
  - 加入企業の例：アドビ、コカコーラ、ディズニー、グーグル、インテル、トヨタ等
- オンライン広告における技術的標準規格の策定を始め、動向調査や自主規制の整備などを行っている。

■ IAB Europe

- IABにおける欧州の拠点団体
- メディア、テクノロジー、マーケティング企業、各国のIABを会員とし、政治的な表現をリードし、業界のコラボレーションを促進することで、欧州市場でのビジネスの成功を可能にするフレームワーク、標準、業界プログラムを提供することを使命としている。

※　TCF作成のワーキンググループ：

- TCFの管理組織IAB Europeは、TCFステアリンググループ（SG）を設立。
- SGは、10カ国のIABと、EUレベルの協会、出版社、メディアオーナー、技術プロバイダー、メディアエージェンシーを含む55以上の組織で構成されている。

TCFはGDPR・eプライバシー指令の遵守を目的に策定されたが、ベルギーのデータ保護当局よりGDPR違反の指摘を受けている。

■ 指摘の経緯：

- 2020年11月、ベルギーのデータ保護当局（APD）によるレビューで、TCFにおけるIAB Europeの役割に関し、懸念事項が指摘される。
- 2021年11月5日 裁定案の確定が近づいている旨、APDから連絡を受けたとIAB Europeが公表。
- 裁定案は、2021年11月中に欧州の他のデータ保護当局によりレビューされ、APDまたは欧州データ保護委員会（EDPB）により確定される見込み。

■ 争点：

- TCFでは、CMPを通じてベンダーに配信される利用者の同意取得状況等のデジタル信号を「TC Strings」と規定している。
- APDは「TC Strings」が個人データに該当し、デジタル広告のリアルタイム入札の中で、IAB Europeが「TC Strings」の共同管理者（joint controller）になりうると指摘している。

■ 今後の対応：

- 裁定確定後6か月以内の是正が求められており、IAB Europeの行動計画についてAPDが監督する。
- IAB Europeは本是正措置の結果、TCFがGDPRに完全に準拠した行動規範であることが公に認められるとして、裁定を歓迎する旨を表明している。

TC String Updates - String includes new signals

TCF version 2.0 Transparency and Consent String Contents:

- General Metadata
- User Consent
- Legitimate Interest
- Publisher Controls
  - purposes
  - legal basis*

CMP ID	Vendor Consent	Purpose Consent	Vendor LI	Purpose LI	Special Feature opt-in	Global consent	OOB Allowed?	Custom Stacks	Pub Controls
###	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	###

Blue: Present in v1.0
Green: New in v2.0

* only if the Vendor indicates flexibility

（出所）IAB Europeニュースリリース（https://iabeurope.eu/all-news/update-on-the-belgian-data-protection-authoritys-investigation-of-iab-europe/）（2021年11月30日アクセス）
IAB Europe「FULL OVERVIEW FOR CMPS & VENDORS」

Transparency and Consent Framework（TCF）

2022年2月2日、TCFに対するGDPR違反の決定※が下された。決定ではTCFの利用までを禁止してはいないが、IAB Europeに対して制裁金の過料と是正措置の立案を求めている。

■ 決定の内容：

- IAB EuropeはTC stringsを通じたユーザーからの同意取得に関してデータ管理者として行動していると認められるが、データ管理者に求められる義務を果たしていない。
- CMPのインターフェースを通じてユーザーに与えられる情報は広告ビジネスにおけるリアルタイム入札の仕組みなどに鑑みるとあまりに一般的的かつ曖昧で、ユーザー自身が自分の情報を管理し続けることを難しくさせている。
- IAB Europeに25万ユーロの制裁金を課すとともに、２か月以内のアクションプランの提出を求める。

■ 是正のポイント：

- 事業者の正当な権利を根拠とした処理の禁止
- TCF参加企業のGDPR遵守状況に対する厳格な審査、モニタリング

■ IAB Europeの反応：

- 業界団体の１つであるIAB Europeが広告業界全体のデータ処理活動に関して責任を負うことはありえないとして、2月11日、ベルギー市場裁判所（the Belgian Market Court）に控訴した。
- また、アクションプランの提出と是正措置期間（６か月）が認められているにも関わらず、複数のデータ保護当局がパブリッシャーに対しTCFの利用切り替えを助言していることに抗議している。

※ 本決定はGDPRにおける協調メカニズム（the one-stop-shop mechanism）の下くだされており、欧州域内の大部分のデータ保護当局による承認を得たうえで実施されている。

（出所）
the Belgian DPAのプレスリリース（https://www.dataprotectionauthority.be/citizen/iab-europe-held-responsible-for-a-mechanism-that-infringes-the-gdpr）（2022年2月17日アクセス）
IAB Europeのプレスリリース（https://iabeurope.eu/all-news/belgian-dpa-decision-of-2nd-february-are-other-dpas-right-to-warn-about-continued-use-of-the-tcf/）（2022年2月17日アクセス）
IAB Europeのプレスリリース（https://iabeurope.eu/all-news/iab-europe-to-appeal-belgian-data-protection-authority-ruling/）（2022年2月17日アクセス）

TCP2.0ポリシーでは、利用目的（Purpose）と処理（Feature）に応じて、CMPによる同意取得の要件を定めている。

TCF2.0ポリシーにおける同意取得要件

利用目的・機能	概要	該当例
同意機会**有**の利用目的 （Purpose）	• CMPにより利用者に通知し、同意の選択機会が与えられる目的 ※該当例1以外は、法的根拠として、同意以外に「正当な利益」も認められている	1. デバイスへの情報の保存やアクセス→**これは同意必須** 2. 基本的な広告の選択 3. パーソナライズド広告のプロファイル作成 4. パーソナライズド広告の選択 5. パーソナライズドコンテンツのプロファイルの作成 6. パーソナライズドコンテンツの選択 7. 広告効果の測定 8. コンテンツパフォーマンスの測定 9. オーディエンスの洞察のための市場調査 10. 製品の開発・改善
同意機会**無**の利用目的 （Special Purpose）	• CMPにより利用者に通知するが、同意の選択機会が与えられない目的	1. セキュリティの確保、不正の防止、デバッグ 2. 広告やコンテンツの技術的な配信
個別同意**不要**の処理 （Feature）	• 個別同意を必要としない処理	1. オフラインのデータソースとの照合・結合 2. 異なるデバイスのリンク 3. 自動送信されるデバイスの特性を使用した本人の識別
個別同意**要**の処理 （Special Feature）	• 個別同意を必要とする処理	1. 正確な位置情報の使用 2. 本人の識別を目的としたデバイス特性のアクティブスキャン

（出所）IAB Europe「TFC2.0 Policy」Appendix A　よりNRI作成

利用目的・処理の通知にあたっては、ユーザーフレンドリーな表現についても言及している。

TCF2.0ポリシーにおいて示される利用者理解を促す通知例

利用目的		該当例	通知例（User-friendly text）※
同意機会**有**	同意必須	1．デバイスへの情報の保存やアクセス	• Cookie、デバイス識別子、またはその他の情報は、お客様に提示された目的のために、お客様のデバイスに保存、またはアクセスすることができます。
		2．基本的な広告の選択	• 広告は、お客様がご覧になっているコンテンツ、使用しているアプリ、お客様のおおよその場所、またはお客様のデバイスの種類に基づいて表示されます。
		3．パーソナライズド広告のプロファイル作成	• お客様とお客様の関心事についてのプロファイルを作成し、お客様に関連するパーソナライズされた広告を表示することができます。
		4．パーソナライズド広告の選択	• お客様に関するプロフィールに基づいて、パーソナライズされた広告を表示することができます。
		5．パーソナライズドコンテンツのプロファイルの作成	• お客様とお客様の関心事についてのプロファイルを作成し、お客様に関連するパーソナライズされたコンテンツを表示することができます。
		6．パーソナライズドコンテンツの選択	• お客様に関するプロフィールに基づいて、パーソナライズされたコンテンツを表示することができます。
		7．広告効果の測定	• お客様がご覧になった、または操作した広告のパフォーマンスや効果を測定することができます。
		8．コンテンツパフォーマンスの測定	• お客様がご覧になった、または操作したコンテンツのパフォーマンスや効果を測定することができます。
		9．オーディエンスの洞察のための市場調査	• 市場調査は、サイト/アプリを訪れ、広告を閲覧するオーディエンスの詳細を知るために利用できます
		10．製品の開発・改善	• お客様のデータは、既存のシステムやソフトウェアの改良、新製品の開発に利用されます。
同意機会**無**		1．セキュリティの確保、不正の防止、デバッグ	• お客様のデータは、不正行為を監視・防止し、システムやプロセスが適切かつ安全に機能するようにするために使用されることがあります。
		2．広告やコンテンツの技術的な配信	• お客様のデバイスは、お客様が広告やコンテンツを見たり、利用したりするための情報を受信および送信することができます。

※　原則として法的通知の記載は必須であり、加えて利用者理解のために必要であれば、ユーザーフレンドリーなテキストの利用も認められている

（出所）IAB Europe「TFC2.0 Policy」Appendix A　よりNRI作成

参考：利用目的ごとの通知・ベンダー向けガイダンスの例

Number	1
Name	Store and/or access information on a device
Legal text	Vendors can: • Store and access information on the device such as cookies and device identifiers for the purposes presented to a user.
User-friendly text	Cookies, device identifiers, or other information can be stored or accessed on your device for the purposes presented to you.
Vendor guidance	• Allowable Lawful Basis: Consent. • Purpose 1 is meant to signal whether the condition for lawful storing and/or accessing information on a user's device is met where this is required. It is not a purpose for personal data processing in itself, unlike all other Purposes the Framework covers. Purpose 1 corresponds to the obligation of Article 5(3) of the ePrivacy Directive. While Purpose 1 is not a data processing purpose, is technically treated the same way for signalling purposes. • Purpose 1 does not apply to processing identifiers or client information, etc. that is not accessed on a user device. For example, reading a device's IDFA falls within Purpose 1, however processing an IDFA outside of reading it from a device, e.g. when receiving it as part of information sent through an ad request is not covered by Purpose 1. • If information stored or accessed falls within the information covered by Special Feature 2 or Feature 3, Vendors must make sure to adhere to the opt in requirement of Special Feature 2 and the disclosure requirement of Feature 3 respectively in addition to the consent requirement of Purpose 1. • Controllers may register for Purpose 1 only in conjunction with another Purpose, Feature, Special Purpose, and/or Special Feature. Any personal data stored and/or accessed via Purpose 1 still requires another Purpose to actually be processed. For example, reading a user identifier from a stored cookie cannot be used to create a personalised ads profile without having obtained consent or met requirements for processing under a legitimate interest for the Purpose 3. Personal data stored and/or accessed via Purpose 1 may not require another Purpose to be processed where a Vendor is acting as a data processor for purposes for which the data controller responsible for the processing has established a legal basis. In such cases, processors of Vendors on the GVL or publishers using the Publisher TC String should only process data in accordance with the Signals of their controller.

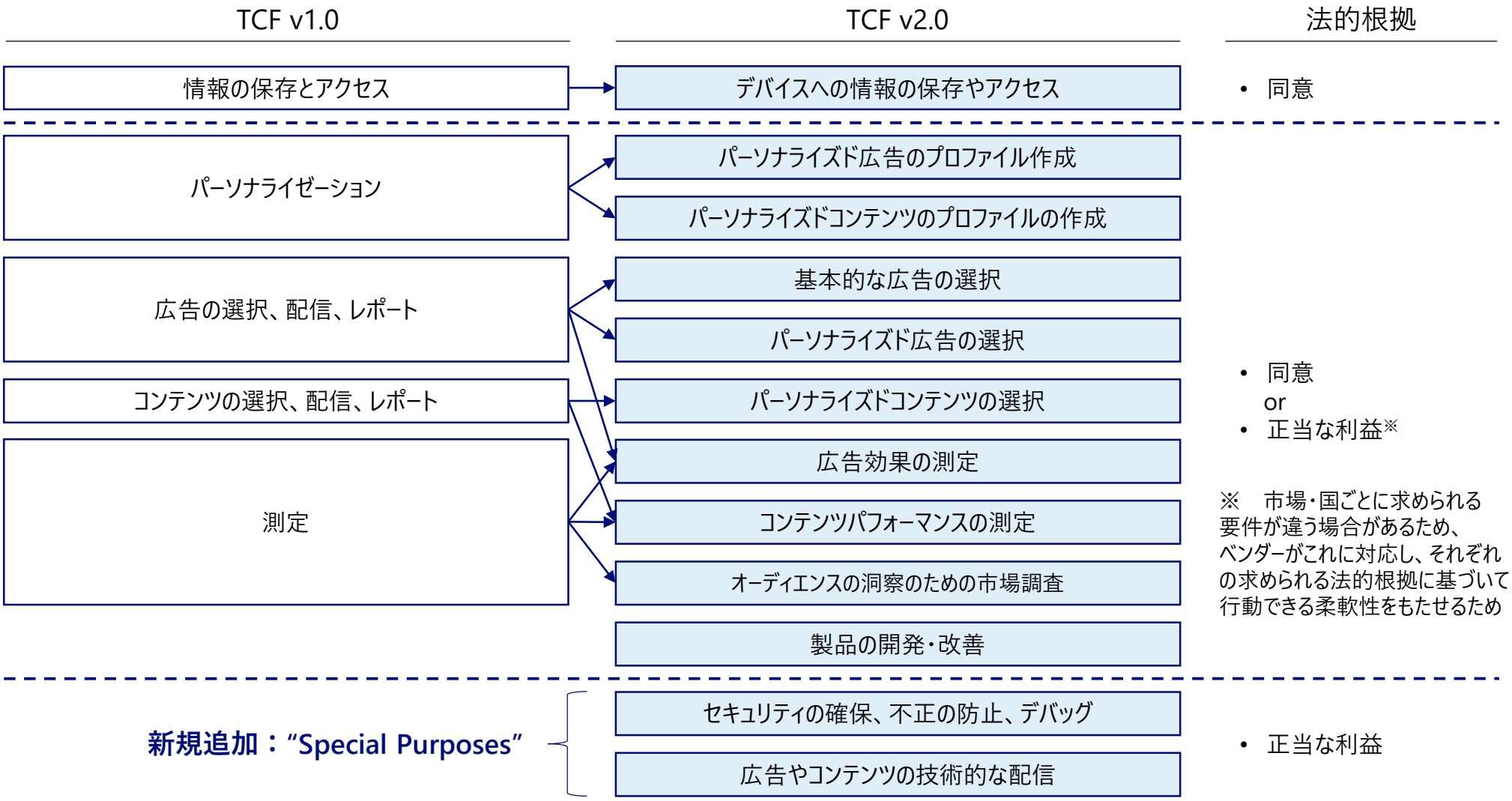
法的な通知内容
ステークホルダーが実施可能な
作業等について記載

法的な通知内容とは別に、
ユーザーフレンドリーな通知内容が
紹介されている

ベンダー向けには、詳細な説明が
記載されている

（出所）IAB Europe「TFC2.0 Policy」Appendix A　よりNRI作成

参考：v2.0へのアップデートにあたり、Purposeの構成が詳細化・一部新規追加



出所）IAB Europe公式Youtube「IAB Europe webinar for CMPs & Vendors - TCF v2 0 Release for Public Comment」（https://www.youtube.com/watch?v=iCHgaF_ZkLk）（2021年11月30日アクセス）内容よりNRI作成

TCF2.0では、利用目的（Purpose）や処理（Feature）を組み合わせグループ化した「Stacks」を設定し、事業者によるポリシーの解釈・利用を補助している。

■ Stacksとは：個人データを処理する目的・処理を組み合わせたもの。
- 2つ以上の「目的」および／または「特別な処理」に関する、初期階層での説明を置き換え/補足するために使用できる

TCF2.0ポリシーにおいて示されているStacksの例

Stacks 3 ：パーソナライズド広告

説明文：「プロフィールに基づいて広告をパーソナライズできます。さらにデータを追加することで、広告をよりパーソナライズすることができます。」

Purpose 2：基本的な広告の選択 ＋ Purpose 3：パーソナライズド広告のプロファイル作成 ＋ Purpose 4：パーソナライズド広告の選択 → Stack3：パーソナライズド広告

Stacks20：広告やコンテンツの測定、オーディエンスインサイト、製品開発

説明文：「広告やコンテンツのパフォーマンスを測定できます。広告やコンテンツを見たオーディエンスに関するインサイトを得ることができます。ユーザーエクスペリエンス、システム、ソフトウェアの構築や改善にデータを利用できます。」

Purpose 7：広告効果の測定 ＋ Purpose 8：コンテンツパフォーマンスの測定 ＋ Purpose 9：オーディエンスの洞察のための市場調査 ＋ Purpose 10：製品の開発・改善 → Stacks20：広告やコンテンツの測定、オーディエンスインサイト、製品開発

TCF2.0ポリシーでは、ユーザーインタフェース（UI）についての要件を整理している。具体的なUI要件の前に、まず前提となる情報やルールについて言及している。

		内容
スコープ	対象者	• フレームワークに関連したユーザーインターフェース（UI）を提供するパブリッシャー・CMP事業者 （例）プライベートCMPを運営するパブリッシャー/商業CMPのサービスに依存するパブリッシャーなど、利用者接点のある事業者
	UIの前提	• フレームワークポリシーおよび仕様書では、フレームワークに関連するUIの言語、デザイン、およびその他の要素に関する最低要件を定めている • TCFはEUのプライバシー法、およびデータ保護法の要件に沿うことが目的であり、EU法との間に矛盾がある場合は、EU法が優先される • 別段の記載がない限り、最低要件を超えるUIの作成も制限されていない
要件	一般ルール	• 「階層的アプローチ」※1と呼ばれる手法を用いることができる • グローバルベンダーリストで命名・定義された「目的」「処理」、もしくはポリシーや仕様書に準拠したStacksの利用にのみ基づく ✓ 「目的」「処理」については、標準的な法的文書が利用可能でなければならないが、それが利用可能かつ決定的であることが説明されている場合は、ユーザーフレンドリーな文章で代用や補足をしてもよい • 英語以外の言語を使う場合、グローバルベンダーリストに掲載されている「目的」「処理」の名称と定義は公式の翻訳にのみ基づく • ベンダーの透明性については、グローバルベンダーリストで公表されているように、ベンダーにより提供された情報とベンダーの宣言にのみ基づく • フレームワークによってカバーされていない目的及び／またはベンダーにもUIを使用できるが、それらがフレームワークの一部だと誤解を与えないように、登録ベンダー・定義された目的と、それ以外が区別できるようにする • UI では下記を利用者に通知する ①「ベンダーの選択は同意機会**有**の「目的」、個別同意**要**の「処理」に限定されること」 ②「開示されたベンダーが同意機会**無**の「目的」のために個人データを処理することに、異議を唱えられないこと」 ③「利用者の選択にかかわらず、個別同意**要**の「処理」が「同意機会**無**の利用目的１：セキュリティの確保、不正の防止、及びデバッグ」のために使用される可能性があること」
	UIの具体要件	• 「利用者の同意」を求める場合 • 「legitimate interests（正当な利益）」※2に基づく場合

→次頁以降に記載

※1「階層的アプローチ」：重要な情報は、すぐに見られる初期階層に記載し、興味のある利用者には、より詳細な情報を追加の階層で提供する手法
※2「legitimate interests」：GDPR第6条(f)号でも記載されている合意以外の法的根拠で、「データ処理を行う適切な業務上の理由」のこと

TCF2.0ポリシーでは、CMPにおいて同意取得する際のユーザーインタフェース（UI）要件のうち、特に階層的アプローチを使用する際の記載内容について細かく説明している。

利用者の同意	階層的アプローチ	初期階層	Must	① 情報が利用者のデバイスに保存／利用者のデバイスからアクセスされている事実（例：Cookieやデバイス識別子、その他デバイスデータの使用など）に関する情報 ② 個人データが処理されていることと、**処理された個人データの性質**（例：固有の識別子、閲覧データなど）に関する情報 ③ 第三者のベンダーが利用者情報を保存・アクセスし、個人データの処理を行うことと、**名前付きの第三者のリストへのリンク** ④ ベンダーがデータを処理している**明確かつ個別の「目的」**のリスト（※ポリシーで定義した「目的」か「Stacks」名称を利用） ⑤ データ処理時にベンダーが用いる**「個別同意が必要な処理」に関する情報** ⑥ 同意の**選択範囲**に関する情報（サービス固有orグループ固有など）。グループ固有の場合は、グループの情報を含むリンク ⑦ 利用者が、**いつでも同意撤回可能であること**、また**同意撤回のためにUIを再表示する方法**についての情報 ⑧ 利用者が同意を表明するための行動喚起※1（「Accept」「Okay」「Approve」など） ⑨ 利用者が選択肢をカスタマイズするための行動喚起（「詳細設定」や「選択肢のカスタマイズ」など）
			Should	① 同意あり／なし（撤回含む）それぞれ実施したの場合の結果についての情報（もしあれば） ② 同意を求めず、正当な利益に基づいて利用者のデータを処理しているベンダーがあること、**利用者が、それに異議を唱える権利があること**、及び正当な利益に基づく処理について、より多くの情報が得られる関連リンクの情報
	その他			
正当な利益	階層的アプローチ	二次階層		① 指定ベンダーのリスト、**ベンダーの「目的」と「処理」**、関連する法的根拠、**各ベンダーのプライバシーポリシーへのリンク**を確認できること ② AppendixAの「目的」「処理」リストを確認し、**ベンダーが、どの目的に同意を求めているか確認できる**方法があること ③ パブリッシャーが各ベンダーや、ベンダーに代わって同意を得ることになった目的に関して、**詳細かつ具体的な同意の選択を行える**こと ④ パブリッシャーがベンダーに代わってオプトインを取得する「個別同意要の処理」に関して、**詳細かつ具体的なオプトインの選択を行える**こと ⑤ ベンダーのデバイスの**最大保管期間と、その更新有無**、仕様書に従い、ベンダーが提供する追加の目的別保管先とアクセス情報の見直し ⑥ 例）デバイスの保管期間に関する記載例：「継続期間は、お客様が最後に本物件と接触した日から[n] で終了する可能性があります」 → [n]は、パブリッシャーが利用者の同意を有効とみなす最大期間を表しているとみなす ⑦ （第1階層で表示しない場合）一部ベンダーが同意を求めず、正当な利益に基づいて利用者のデータを処理している場合、その事実や利用者がそれに異議を唱える権利があること、及び正当な利益に基づく処理について、より多くの情報が得られる関連リンクの情報 ⑧ （第1階層で表示しない場合）同意あり／なし（撤回含む）それぞれ実施した場合の結果についての情報
	その他			

※1 行動喚起（コールトゥアクション）：サイト上で訪問者を具体的な行動に誘導すること。多くの場合ボタンやリンクで表示される

（出所）IAB Europe「TFC2.0 Policy」Appendix B　よりNRI作成

TCF2.0ポリシーでは、CMPにおいて同意取得する際のユーザーインタフェース（UI）要件として、記載位置やデザイン、デフォルトの選択肢等についても言及している。

利用者の同意

階層的アプローチ

その他

UI全体に係るルール

① 同意のUIは、サイトまたはアプリの**コンテンツすべて、または実質全てをカバーするモーダル※1またはバナー**で、一般条件やプライバシーポリシー等の**他の情報とは別に、目立つように**表示しなければならない

② 階層的アプローチでの個別同意・オプトインの要件に基づいて、各目的について個別同意するためのレイヤーにアクセスする場合や、「同意が必要な処理」のオプトインの選択を行う場合、**デフォルトでは「同意なし」「オプトインなし」または「オフ」**でなければならない

③ フレームワーク参加が IAB Europe に登録されていないベンダーを UI で表示する場合は、利用者が**フレームワークに登録されたベンダーと登録されていないベンダーとを区別できる**ようにしなければならない（登録していないベンダーがフレームワークに参加していると誤解されないようにしなければならない）

④ パブリッシャーのウェブサイトやアプリケーションに掲載されているプライバシーポリシーなど、**容易にアクセスできるリンクから、本フレームワークのUIを再表示できなければならない**。その際は、利用者が同意を撤回するための行動喚起※2（例：“Withdraw consent”）を含めることで、**同意を与えたときと同様、簡単に同意を撤回することができる**ようにする

⑤ UIの行動喚起は見えなかったり、判読できなかったり、無効に見えたりしてはいけない。また、行動喚起の内容は同一でなくてよいが、**テキスト処理（フォントやフォントサイズ、フォントのスタイル）は統一し、それぞれのテキストは、コントラスト比を5：1以上**にする必要がある

正当な利益

階層的アプローチ

その他

例外条件

- ポリシーC(c)(iii)(iv)、C(d)の例外として、パブリッシャーが、**利用者が他に個別同意なしでコンテンツにアクセスできる方法（例：同意のいらない有料アクセスの提供など）を実装している場合**、利用者による具体的な個別の同意やオプトインの選択は必要ない

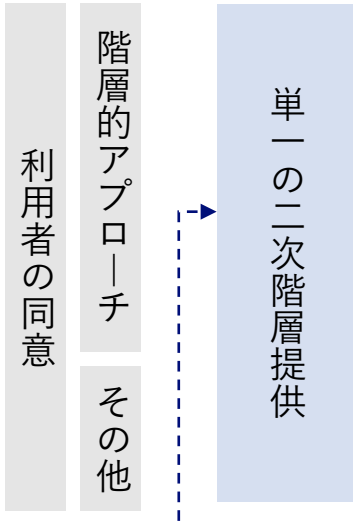
※ポリシーC：同意取得のためのUI要件

- ✓ ポリシーC (c)：階層的アプローチのうち、利用者に詳細を伝える2階層目以降で記載すべき内容
  - ✓ (iii)：ベンダーごと・目的ごとに個別同意の選択ができること
  - ✓ (iv)：パブリッシャーがベンダーに代わってオプトインを取得する「同意が必要な処理」について、詳細かつ具体的なオプトインの選択ができること
- ✓ ポリシーC (d)：ポリシーC(c)(iii)に基づいて、各目的について個別同意するためのレイヤーにアクセスする場合や、ポリシーC(c)(iv)に基づいて「同意が必要な処理」のオプトインの選択を行う場合、デフォルトでは「同意なし」「オプトインなし」または「オフ」でなければならない

※1 モーダル：モーダルウィンドウ。元のウィンドウの上に別枠で表示され、指定の操作を行うまで表示され続け、その間、他のウィンドウに移ることができない
※2 行動喚起（コールトゥアクション）：サイト上で訪問者を具体的な行動に誘導すること。多くの場合ボタンやリンクで表示される

（出所）IAB Europe「TFC2.0 Policy」Appendix B　よりNRI作成

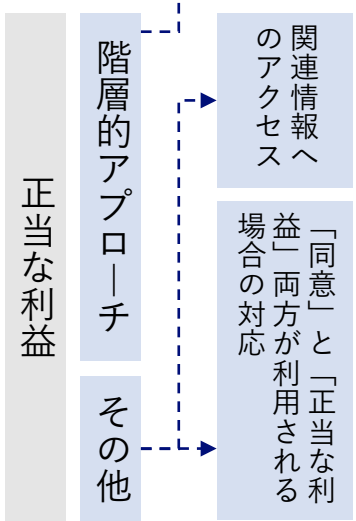
また、TCF2.0ポリシーでは、「正当な利益」として利用者の情報を利用する際に必要なUIの要件についても言及している。



単一の二次階層提供

※利用者に対して下記を可能にするために、単一の二次階層ページを提供することが求められる

① 個人データが処理されていることと、処理された個人データの性質に関する情報の表示
② **「正当な利益」によるデータ処理の範囲、および当該処理に対する異議申し立ての範囲**に関する情報（＝サービス固有orグループ固有など）の確認。グループ固有の場合は、グループの情報を含むリンクも必要
③ UI内でのアクセス制御、**「正当な利益」に基づく個人データの処理に対する異議申し立て**
④ Appendix A に定義された、標準的な名称及び標準的で完全な説明を含む「目的」（同意の要不要問わず）のリストを確認し、**どのベンダーが「正当な利益」に基づき、それぞれの「目的」のためにデータを処理しているか確認する方法**
⑤ 各ベンダーの「正当な利益」に基づく処理、およびベンダーの透明性確立を支援するために、パブリッシャーが選択した各目的に関して、**利用者が異議を唱える権利の行使**
⑥ ベンダーのリスト、その「目的」「処理」、および法的根拠の確認と、各ベンダーのプライバシーポリシーへのリンクの見直し



関連情報へのアクセス

- 目的、処理、およびベンダーに関する透明性を、「正当な利益」に関連して提供する場合は、**「正当な利益」に基づく処理について記載された、UI上の関連ページに容易にアクセスできるリンク**を提供しなければならない

「同意」と「正当な利益」両方が利用される場合の対応

- 「目的」「処理」、およびベンダーに関する透明性を提供するために、利用者の同意と正当な利益の両方が用いられる場合、同意の要件（ポリシーC(a)）と正当な利益の要件（ポリシーD(a)）を共に満たす必要がある
  ↓
- 同意に関する通知を「サイトまたはアプリのコンテンツの実質全てをカバーするモーダルまたはバナーで、他の情報とは別に目立つように表示」する際に、**初期階層に、「正当な利益」に基づく処理についての記載ページにアクセスできるリンクを含まなければ**ならない

（出所）IAB Europe「TFC2.0 Policy」Appendix B　よりNRI作成

CCPA/CPRA

CCPA：California Consumer Privacy Acts of 2018
CPRA：California Privacy Rights Act of 2020

2020年のCCPA施行・CPRA成立以降、州単位で包括的なプライバシー保護法を制定する動きがある。直近では連邦法制定に向けた議論も進められている。

CCPA施行以降のプライバシー保護法制定の動き

カリフォルニア州	バージニア州	コロラド州
2020年1月1日 CCPA施行		
2020年7月1日 CCPA執行開始		
2020年8月14日 CCPA規則成立・執行開始		
2020年11月3日 CPRA成立		
	2021年3月2日 VCDPA成立	
		2021年7月7日 CPA成立
2022年7月1日 CPRA規則成立期限		
2023年1月1日 CPRA施行	2023年1月1日 VCDPA施行	
2023年7月1日 CPRA執行開始		2023年7月1日 CPA施行

この他にニューヨーク州、ワシントン州において法案提出がされている。

CCPA：California Consumer Privacy Acts of 2018
CPRA：California Privacy Rights Act of 2020
VCDPA：the Virginia Consumer Data Protection Act
CPA：the Colorado Privacy Act

2021年７月、カリフォルニア州の司法長官がCCPAの執行事例を公表した。

- 2020年7月1日のCCPA執行開始から1年を経て、Rob Bonta司法長官はCCPA執行活動の報告を行った。
- 司法長官室が公表する27件の執行事例のうち、執行理由としては「プライバシーポリシーがCCPAに準拠していない」が14件で最多となっている。

カリフォルニア州司法長官室が公表したCCPAの執行事例（一部抜粋）

業種	執行理由	内容
オンライン衣料品販売業者	プライバシーポリシーがCCPAに準拠していない	• CCPAが定める消費者の権利や、知る権利および消去の権利を行使する方法を通知しなかった。また、過去12か月間のパーソナルデータの販売、提供の有無についても明確に知らせていなかった。違反通知後に、プライバシーポリシーを更新して対応した。
データブローカー	オプトアウト方法がCCPAに準拠していない	• データ収集をオプトアウトするWebフォームにおいて、パーソナルデータの販売もオプトアウト可能か明らかにしていなかった。違反通知後に、オプトアウトページを更新して、Webフォームを、より目立つように表示し、当該Webフォームによって、パーソナルデータの販売も含めて、オプトアウト権を行使できることを明確にした。
ソーシャルメディアネットワーク	他社との契約がCCPAに準拠していない	• サービスプロバイダーに対し、契約で指定されたサービスを実行する以外の目的で、パーソナルデータを保持、利用、開示することを契約上禁止していなかった。違反通知後に、サービスプロバイダーとの契約内容を変更した。
ソーシャルメディア	CCPA要求にタイムリーに対応していない	• ユーザーから受けたCCPA要求に対して、タイムリーに応答しなかった。違反通知後に、適切な応答に向けて、CCPA要求への対応システムをアップデートした。

（出所）https://oag.ca.gov/privacy/ccpa/enforcement（2022年1月25日アクセス）

CCPAの執行事例は幅広い業界・執行理由を含んでいるものの、いずれも民事制裁金の賦課には至っておらず、直接の執行よりも消費者保護を強化する側面に寄与している。

執行事例における対象および執行理由

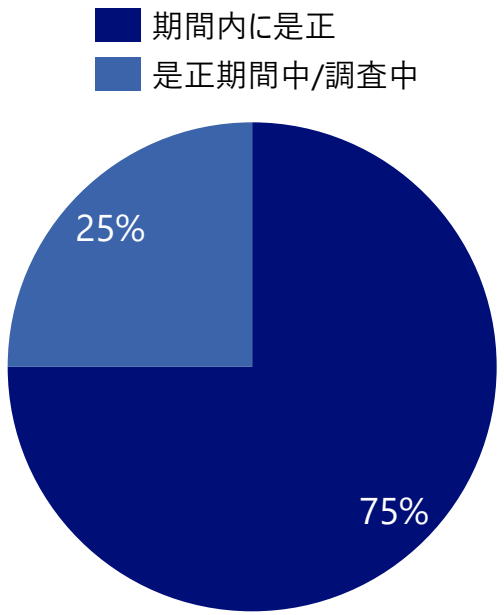
- CCPAの27件の執行事例は、オンラインゲーム、自動車、ペット産業等の幅広い業界を対象として、16の執行理由を含んでおり、CCPAの中核的な規定や特定業界に限定して執行が行われるわけではないことを示す狙いがあったと思われる。
- ただし、今回の公表は執行対象に関する詳細や、調査が実際に完了したかどうかを明らかにしていないため、不完全な内容となっている。

執行理由（一部抜粋）	件数
プライバシーポリシーのコンプライアンス違反	14
請求方法なし	6
消費者への通知	5
「Do Not Sell My Personal Information」のリンクなし	4
個人情報の売却	4
オプトアウトプロセスのコンプライアンス違反	3
認定代理人	2
サービス提供者契約のコンプライアンス違反	2
CCPA上の消費者請求に対する対応の遅れ	1
CCPA上の消費者請求に料金徴収	1
金銭的インセンティブの未通知	1
着信課金用電話番号なし	1

（出所）https://oag.ca.gov/privacy/ccpa/enforcement（2022年1月25日アクセス）

是正期間（Cure period）内の対応状況

- CCPA違反の疑いの通知を受け取った企業のうち、75％は30日内に違反を是正した。
- 27の執行事例は、いずれも民事制裁金の賦課には至っていないことから、企業に是正期間を認めることにより、民事制裁金の賦課に至る前に消費者保護が強化される結果となっている。



2023年1月1日からはCPRAが発効される見込みである。

CPRAによる主な修正・拡張事項

1．定期監査とリスク評価の実施義務

- 消費者のプライバシーまたはセキュリティーに重大なリスクを生じさせる処理を行う事業者に対して、以下の義務が規定される。
  - **1年ごとのサイバーセキュリティ監査**
  - **定期的なリスク評価のプライバシー保護局への提出**

2．自動意思決定(プロファイリングを含む)

- 自動意思決定技術の使用について、消費者が開示請求権とオプトアウト権を有する旨のほか、当該開示請求権への対応として、事業者に以下の情報の開示を義務付ける。
  - 自動意思決定プロセスに使用されている、ロジックに関する意味のある情報
  - 自動意思決定プロセスにより、消費者に起こる可能性の高い結果

3．カリフォルニア州プライバシー保護局の創設

- 新たに創設されるプライバシー保護局は、CPRAの執行権、規則の制定権、対象事業者の調査権および監査権等を有する。

4．訂正する権利

- 消費者の権利として、新たに訂正請求権が追加される。

5．「共有」という概念の新設

- CCPAにおける「売却」とは異なる概念として「共有」の定義が新設される。
- 消費者がオプトアウト権を有するなど、多くの場面で「売却」と同様の規制が課せられる。

6．センシティブ情報

- 「センシティブ情報」というカテゴリが新設され、当該情報の利用を、一定の場面に制限することを求める権利が消費者に認められる。
- 消費者が上記の権利を行使するため、**事業者はホームページ上に「Limit the Use of My Sensitive Personal Information」という明確かつ目立つリンクを提供することが義務付け**られる。

7．開示請求

- 2022年1月1日以降に収集されたパーソナルデータに関して、事業者が不可能または不均衡な努力を要することを証明しない限り、過去12ヶ月より前のパーソナルデータも開示対象となる。

（出所） https://cppa.ca.gov/regulations/pdf/invitation_for_comments.pdf （2022年1月25日アクセス）

CPRA施行規則の制定にあたり、2021年11月8日を期限にパブリックコメントが募集されていた。

■ コメントの対象項目は限定されていないが、同庁はCPRAで新設または拡張された項目に関するコメントに、特に関心を寄せている。

CPRA規則に対するパブリックコメントの主なトピック

No.	トピック
1	消費者のプライバシーまたはセキュリティーに重大なリスクを生じさせる処理：企業が実施するサイバーセキュリティ監査とリスク評価
2	自動意思決定(プロファイリングを含む)
3	カリフォルニア州プライバシー保護庁が実施する監査
4	削除する権利、訂正する権利、知る権利
5	第三者の販売および共有をオプトアウトする権利、センシティブ情報の使用と開示を制限する権利
6	センシティブ情報の使用と開示を制限する権利
7	消費者の開示請求に応じて提供する情報
8	定義とカテゴリー
9	その他

（出所） https://cppa.ca.gov/regulations/pdf/invitation_for_comments.pdf （2022年1月25日アクセス）

CCPA/CPRA

パブリックコメントには計70件以上の意見が寄せられた。GoogleはGDPRやVCDPA等の他法令との整合性をとることを主張している。

Googleがパブリックコメントに寄せた意見（抜粋）

No.	カリフォルニア州プライバシー保護庁が特にコメントを募集していたトピック	Googleの意見
1	消費者のプライバシーまたはセキュリティーに重大なリスクを生じさせる処理：企業が実施するサイバーセキュリティ監査とリスク評価	• 「消費者のプライバシーまたはセキュリティに重大なリスクを生じさせる処理」に該当する処理は、特定の処理における被害のリスクを扱うプライバシー法およびデータセキュリティ法（カリフォルニア州データ侵害通知法等）を参照しつつ、それらと整合するように定めるべきである。 • サイバーセキュリティ監査とリスク評価の提出において、無許可の第三者への開示や利用が機密保持条項によって禁止されていることを確認するよう求める。 • CPRAの下で課される監査および評価義務は、プライバシーおよびセキュリティに関する、**他の法的制度や業界基準等の下で実施されたレビューを使用または再利用することを可能にすべき**である。
2	自動意思決定(プロファイリングを含む)	• **自動意思決定の定義を既存の法律と整合させるべき**である。 • 他の国内外の規制基準と一致させるため、自動意思決定に関する規則を、クレジット、雇用、保険、賃貸住宅、免許、その他の政府給付に対する消費者の資格など、法的効果または同様の重要性を持つ効果を生み出す、完全自動意思決定に焦点を当てることを求める。例えば、GDPR の第15 条と第 22 条は、自動意思決定が、法的または類似の重大な影響をもたらす範囲でのみデータ主体の透明性の権利を提供している。同様に、コロラド州とバージニア州の新しいプライバシー法は、「消費者に関する法的または類似の重大な影響をもたらす意思決定の促進」の範囲内でのみ「プロファイリング」を規制している。
9	その他	• 事業者が2023年までにCPRAの基本要件に準拠できるように、十分な時間を与えることを強く求める。**法律が施行される直前に、追加の義務を導入すべきではない**。 • 他の法律の下で課されるプライバシー要件との整合性を図るべきである。 • 形式よりも実質を優先した方法で消費者の要求に応えられるよう、事業者に柔軟性を与えるべきである。（詳細を次ページに記載）

出所）カリフォルニア州プライバシー保護庁HP（https://cppa.ca.gov/regulations/pdf/preliminary_rulemaking_comments_1.pdf）（2021年12月28日アクセス）

CCPA/CPRA

Googleは、消費者による権利行使やオプトアウト方法に関して、事業者に柔軟な対応を認めるべきと主張している。

■ Googleは、以下の点について、形式的な規定を設けるのではなく、事業者に柔軟な対応を認めるべきとしている。

論点	CPRA規則に求める対応
簡単にアクセスできるセルフサービスツールを通じて行われる消費者の権利行使	• 統一された文言や手順を企業に強制するのではなく、多くの企業が、**すでに導入しているセルフサービスツールを認めるべき**である。
プラットフォームまたは他の技術によって送信されるオプトアウト信号	• 事業者が、どのような信号を探し、どのように当該信号に対応すべきか、明確にすべきである。例えば、新しいオプトアウトツールを明確な基準に照らして評価する承認プロセスを採用することが考えられる。最低でも、信号が、有効なオプトアウト信号とみなされるために必要な基準を明確にすべきである。 • 同様に、オプトアウト信号を受信したが、その信号と矛盾する可能性のある消費者との既存の関係や、消費者からの同意がある場合、事業者に対する期待を明確にすべきである。 • 機密情報の特定の使用との関連で、自動化された信号が、どのように使用されるべきか、事業者が、そのような信号に対応することを意図しているか、および、そのような信号は、パーソナルデータの販売および共有をオプトアウトするために使用されるものと区別することができるかを明確にするべきである。

出所）カリフォルニア州プライバシー保護庁HP（https://cppa.ca.gov/regulations/pdf/preliminary_rulemaking_comments_1.pdf）（2021年12月28日アクセス）

米国その他州法の状況

米国その他州法の状況

CPRA、VCDPA、CPAの比較

CPRA：カリフォルニアプライバシー権利法
VCDPA：バージニア消費者データ保護法
CPA：コロラドプライバシー法

1．通知

- CPRA、VCDPA、CPAの通知項目は概ね同じだが、CPRAでは新たに保存期間を通知することが求められる。
- CPRA、VCDPA、CPAに共通して、分かりやすい通知の提供が規定されている。

2．同意

- CPRA、CPAでは、同意に該当しないケースとしてダークパターンが挙げられている。
- 各州法において、パーソナルデータの販売のオプトアウト権が認められているが、「販売」の定義は微妙に異なる。
  - CPRA、CPA：パーソナルデータを金銭的またはその他の価値ある対価と交換すること
  - VCDPA：パーソナルデータを金銭的対価と交換すること

※ネバダ州 " Nevada Revised Statutes CHAPTER 603A SECURITY AND PRIVACY OF PERSONAL INFORMATION"は、「販売」を「管理者またはデータブローカーが、対象情報を第三者にライセンス供与または販売するために、金銭的対価と交換すること」と定義している。

3．センシティブ情報

- センシティブ情報の処理に係る要件
  - CPRA：センシティブ情報の処理を制限する権利が、消費者に認められている
  - VCDPA、CPA：センシティブ情報の処理には、消費者の同意取得が必要とされる
- センシティブ情報の対象はCPRAにおいて最も広く、クレジットカード情報や電子メールの内容等を含む。

4．子どものデータ

- CPRAでは、子どものデータの販売または共有に関して、事前の同意取得が求められる。
- VCDPA、CPAでは、Children's Online Privacy Protection Act（COPPA）の対象データは、COPPAに沿った対応が求められている。

出所）杉本 武重「GDPR・CCPA・CPRAの主要論点比較」
（https://www.jetro.go.jp/ext_images/biz/seminar/2021/2e7c9eec1a269310/3.pdf） （2021年11月30日）

通知項目

ISO/IEC 29184（16項目）	カリフォルニアプライバシー権利法（CPRA）		バージニア消費者データ保護法（VCDPA）	コロラドプライバシー法（CPA）
	ノーティス	ポリシー		
1. サービスの概要				
2. 利用目的	○	○	○	○
3. 利用目的の詳細説明				
4. 取扱いの主体				
5. 取得されるデータ項目	○	○	○	○
6. 取得方法		○		
7. データ取得のタイミングと場所				
8. 利用方法				
9. 保管場所				
10. 第三者提供	○	○	○	○
11. 保存期間	○			
12. 本人による関与	○	○	○	○
13. 問い合わせ先		○		○
14. 同意設定の確認				
15. データ処理の根拠				
16. リスク				

出所）杉本 武重「GDPR・CCPA・CPRAの主要論点比較」
（https://www.jetro.go.jp/ext_images/biz/seminar/2021/2e7c9eec1a269310/3.pdf）（2021年11月30日）

CPRAでは新たに、保存期間に関する通知が義務付けられる。

	カリフォルニアプライバシー権利法（CPRA）	バージニア消費者データ保護法（VCDPA）	コロラドプライバシー法（CPA）
利用目的	• パーソナルデータの利用目的 • センシティブ情報の利用目的	• パーソナルデータの利用目的	• パーソナルデータの利用目的
取得されるデータ項目	• パーソナルデータの種類 • センシティブ情報の種類	• 管理者が処理するパーソナルデータの種類	• 管理者または処理者が収集、または処理するパーソナルデータの種類
第三者提供	• パーソナルデータが販売または共有されるかどうか • センシティブ情報が販売または共有されるかどうか	• 管理者が第三者に対して共有するパーソナルデータの種類 • 管理者がパーソナルデータを共有する第三者の種類	• 管理者が第三者に対して共有するパーソナルデータの種類 • 管理者がパーソナルデータを共有する第三者の種類
保存期間	• **事業者がセンシティブ情報を含むパーソナルデータの各種類の保持を意図する期間、または、それが可能でない場合、当該期間を定めるために利用される基準**	–	–
本人による関与	• 消費者による権利行使方法 • 「Do Not Sell or Share My Personal Information」というタイトルのリンク • 「Limit the Use of My Sensitive Personal Information」というタイトルのリンク	• 消費者による権利行使方法（不服申立を行う手続を含む） • 管理者がパーソナルデータを第三者に対して販売している場合、又はターゲティング広告目的で処理している場合には、当該処理及び消費者によるオプトアウト権の行使方法	• 消費者による権利行使方法（管理者の問い合わせ先を含む） • 管理者がパーソナルデータを第三者に対して販売している場合、又はターゲティング広告目的で処理している場合には、当該処理及び消費者によるオプトアウト権の行使方法
その他	• プライバシーポリシーへのリンク	–	–

出所）杉本 武重「GDPR・CCPA・CPRAの主要論点比較」（https://www.jetro.go.jp/ext_images/biz/seminar/2021/2e7c9eec1a269310/3.pdf）（2021年11月30日）

通知方法

■ 各州法により、分かりやすくアクセスしやすい通知方法が求められる。

カリフォルニアプライバシー権利法（CPRA）	バージニア消費者データ保護法（VCDPA）	コロラドプライバシー法（CPA）
消費者にとって読みやすく、理解できる態様にて作成されるとともに、消費者に提供されなければならず、かつ、次の内容を遵守する。 • 平易で、直截な表現を用い、技術的または法的な専門用語を避ける • 通知に対して消費者の注意を惹き、（もし利用する場合は小さな画面上でも）通知を読みやすくするフォーマットを用いる • 通常の業務の過程において、契約条件、免責事項、販売告知その他の、カリフォルニア州の消費者に対する情報を提供する際に用いている言語で利用可能とする • 障害のある消費者にとって、合理的にアクセス可能とする	• 合理的にアクセス可能で、明確かつ意味のあるプライバシーノーティスを提供する • 「オプトアウト権の行使方法」について、明確かつ目立つ形で公開する	• 合理的にアクセス可能で、明確かつ意味のあるプライバシーノーティスを提供する • 「オプトアウト権の行使方法」について、明確かつ目立つ形で公開する

出所）杉本 武重「GDPR・CCPA・CPRAの主要論点比較」
（https://www.jetro.go.jp/ext_images/biz/seminar/2021/2e7c9eec1a269310/3.pdf）（2021年11月30日）

参考）CPRAにおけるプライバシーポリシーの記載事項・開示方法

	カリフォルニアプライバシー権利法（CPRA）　※赤字はCPRAによる修正・拡張箇所
記載事項	• 過去12か月間に収集したパーソナルデータの種類 • パーソナルデータの収集源の種類 • パーソナルデータの収集、販売または共有の事業上または商業目的 • パーソナルデータを開示する第三者の種類（販売、共有または事業目的で開示したパーソナルデータの種類ごとに記載） • 過去12か月間に第三者に販売または共有したパーソナルデータの種類（販売または共有していない場合にはその旨） • 過去12か月間に第三者に事業目的で開示したパーソナルデータの種類（事業目的で開示していない場合にはその旨） • 事業者が16歳未満の消費者のパーソナルデータを販売または共有しているとの現実の認識を有しているか否か • 事業者が16歳未満の消費者のパーソナルデータを販売または共有しているとの現実の認識を有している場合には、オプトイン権を行使するプロセスの説明 • 消費者に、知る権利、削除請求権、訂正請求権、オプトアウト権、センシティブ情報の利用・開示の制限権および差別を受けない権利がある旨 • 検証可能な消費者の知る請求、削除請求または訂正請求の提出方法の指示、（もしあれば）オンライン上の請求フォームまたは請求のためのポータルへのリンク • オプトアウト権の通知の内容、またはオプトアウトのページのリンク • センシティブ情報の利用・開示の制限権の通知の内容、またはセンシティブ情報の利用・開示の制限のページ • 消費者請求を確認するために用いる手続（消費者が提供しなければならない情報を含む）の一般的な説明 • 権利行使のための代理人を指定する方法の指示 • 最終更新日 • 連絡先 • 受領した知る請求、削除請求、訂正請求、オプトアウト請求、制限請求の件数および、それらの請求に対する対応または拒絶の状況、ならびに、それらの請求に対して、実質的に対応するまでに要する日数の中央値をまとめたマトリックス（年間1,000万件以上のパーソナルデータを購入し、商業目的で受領し、販売し、または商業目的で共有している場合に限る）
開示方法	• 事業者のウェブサイトまたはアプリのダウンロード、もしくはランディングページ上の「privacy」という単語を用いた明確なリンクを通じて、オンラインで掲出する（ウェブサイトを運営していない事業者は、オンラインで掲示する必要はないが、消費者が明確に利用できるようにする） • 少なくとも12か月に1回はアップデートする

※CCPA規則、CPRA条文に基づく整理であるため、CPRA規則によって内容が異なる可能性がある。

出所）杉本 武重「GDPR・CCPA・CPRAの主要論点比較」
（https://www.jetro.go.jp/ext_images/biz/seminar/2021/2e7c9eec1a269310/3.pdf）（2021年11月30日）

CPRA・CPAでは、同意に該当しないケースとして、ダークパターンが挙げられている。

	カリフォルニアプライバシー権利法（CPRA）	バージニア消費者データ保護法（VCDPA）	コロラドプライバシー法（CPA）
「同意」の定義	消費者が自由に与えた、具体的な情報に基づく明確な意思表示であり、消費者もしくはその法定後見人、代理権を持つ者、または消費者の後見人として行動する者が、声明または明確な肯定的行動によって、狭く定義された特定の目的のために、自分に関連するパーソナルデータを処理することに合意すること	消費者の自由意思に基づく、具体的かつ十分に情報が与えられたうえでの、不明瞭でない合意を示す明確かつ肯定的な行為のこと	消費者の自由意思に基づく、具体的かつ十分に情報が与えられたうえでの、不明瞭でない合意を示す明確かつ肯定的な行為のこと
「同意」に該当しないケース	• パーソナルデータの処理に関する記述を含む、一般的または広範な利用規約またはそれに類する文書を、他の無関係な情報と一緒に受諾する。 • コンテンツの上にカーソルを置いたり、ミュートしたり、一時停止したり、閉じたりする。 • ダークパターンを通じて同意を得る。	–	• パーソナルデータの処理に関する記述を含む、一般的または広範な利用規約またはそれに類する文書を、他の無関係な情報と一緒に受諾する。 • コンテンツの上にカーソルを置いたり、ミュートしたり、一時停止したり、閉じたりする。 • ダークパターンを通じて同意を得る。

出所）杉本 武重「GDPR・CCPA・CPRAの主要論点比較」（https://www.jetro.go.jp/ext_images/biz/seminar/2021/2e7c9eec1a269310/3.pdf）（2021年11月30日）

オプトアウト権の対象

■ 各州法のオプトアウトの対象は、下表の通りである。

■ CPRAでは、新たに「共有」という概念が規定され、オプトアウト権の対象となった。「共有」は、クロスコンテキスト行動ターゲティング広告のために、第三者がパーソナルデータを利用できるようにすることを意味しており、ターゲティング広告規制が導入されたことになる。

		カリフォルニアプライバシー権利法（CPRA）	バージニア消費者データ保護法（VCDPA）	コロラドプライバシー法（CPA）
オプトアウト権の対象	販売	○	○	○
	ターゲティング広告	○	○	○
	プロファイリング	○	○	○
（参考）「販売」の定義		パーソナルデータを**金銭的またはその他の価値ある対価**と交換すること	パーソナルデータを**金銭的対価**と交換すること	パーソナルデータを**金銭的またはその他の価値ある対価**と交換すること

※ネバダ州 " Nevada Revised Statutes CHAPTER 603A SECURITY AND PRIVACY OF PERSONAL INFORMATION"は、「販売」を「管理者またはデータブローカーが対象情報を第三者にライセンス供与または販売するために、金銭的対価と交換すること」と定義している。

出所）杉本 武重「GDPR・CCPA・CPRAの主要論点比較」
（https://www.jetro.go.jp/ext_images/biz/seminar/2021/2e7c9eec1a269310/3.pdf）（2021年11月30日）

センシティブ情報の処理に係る要件

カリフォルニアプライバシー権利法（CPRA）	バージニア消費者データ保護法（VCDPA）	コロラドプライバシー法（CPA）
• 消費者は、事業者に対して、いつでもセンシティブ情報の利用を以下の範囲に制限するよう指示する権利を有する。 1. サービスまたは商品を求める平均的な消費者によって、合理的に求められる当該サービスまたは商品を提供するため 2. 以下のサービスを実施するために必要な範囲 ➢ 消費者のパーソナルデータの利用が、その目的に対して合理的に必要であり、かつ比例的に行われる範囲で、セキュリティと完全性の確保を支援するため。 ➢ 消費者と事業者の進行中のやりとりの一部として示される、個別化されていない広告を含むが、これに限定されない短期の一時的な利用のため。（ただし、消費者のパーソナルデータが第三者に開示されず、かつ、消費者についてのプロファイル作成または、その時のやりとり以外における消費者の体験の改変に利用されない場合に限る。） ➢ 事業者の代わりのサービスの実施のため。（事業者のためのアカウントの維持もしくは提供、カスタマーサービスの提供、注文および取引の処理もしくは履行、顧客情報の検証、支払いの処理、解析サービスの提供、保管、または類似サービスの提供を含む。） ➢ 事業者により所有、製造、管理される、もしくは事業者のために製造されるサービス・デバイスの品質・安全性を検証・維持し、改善、アップグレードするための活動を行うこと。 3. CPRA規則によって認められる範囲	• センシティブ情報の処理には、消費者の同意が必要となる。 • 消費者が子ども(13才未満)である場合には、連邦法であるChildren's Online Privacy Protection Actに従った処理を行う。	• センシティブ情報の処理には、消費者の同意が必要となる。 • 消費者が子ども(13才未満)である場合には、その親の事前の同意を得る。

※連邦法案では、民主党案（COPRA）・共和党案（SDA）ともに、センシティブ情報の処理にあたり、消費者の同意取得を義務付けている。

出所）杉本 武重「GDPR・CCPA・CPRAの主要論点比較」（https://www.jetro.go.jp/ext_images/biz/seminar/2021/2e7c9eec1a269310/3.pdf）（2021年11月30日）

センシティブ情報に該当する項目

	カリフォルニアプライバシー権利法（CPRA）	バージニア消費者データ保護法（VCDPA）	コロラドプライバシー法（CPA）
子どものデータ	–	○	○
市民権・移民的状態を明らかにする個人データ	–	○	○
正確な地理的位置情報	○	○	–
健康情報	○	○	○
性的指向	○	○	○
人種的・民族的起源	○	○	○
宗教または哲学上の信念	○	○	○
遺伝的データ・バイオメトリックデータ	○	○	○
その他	• ソーシャルセキュリティ番号、運転免許証番号、州IDカード番号、パスポート番号 • アカウントへのアクセスを可能とするセキュリティ・コードもしくはアクセス・コード、パスワード、又は認証情報と組み合わせられた、アカウント・ログイン情報、金融機関口座情報、デビットカード情報、クレジットカード情報 • 労働組合への加入状況 • 郵便・電子メール・テキストメッセージの内容（事業者が、これらの通信の受信者として意図されている場合を除く）	–	–

出所）杉本 武重「GDPR・CCPA・CPRAの主要論点比較」（https://www.jetro.go.jp/ext_images/biz/seminar/2021/2e7c9eec1a269310/3.pdf）（2021年11月30日）

未成年者の保護者によるオプトイン手続き

	カリフォルニアプライバシー権利法（CPRA）	バージニア消費者データ保護法（VCDPA）	コロラドプライバシー法（CPA）
基準となる年齢	16歳未満	13歳未満	13歳未満
センシティブ情報への該当性	×	○	○
オプトイン手続きに係る規定	• 子どもと分かっている者から収集したパーソナルデータについて、**消費者が13歳以上16歳未満の場合には当該消費者自身**が、または**消費者が13歳未満の場合にはその親または保護者**が、積極的に同意しない限り、**販売または共有してはならない**。 • 消費者の年齢を意図的に無視する事業者は、その消費者の年齢について認識していたとみなされる。 • 子どものパーソナルデータの販売または共有に関して同意されない場合、当該パーソナルデータの販売または共有をしてはならず、再び同意を求めるためには、12か月以上、または消費者が16歳に達するまで待たなければならない。	• 連邦法である**Children's Online Privacy Protection Act（COPPA）に従った処理をしなければならない**。 • 子どもの親または法的保護者は、その子どもと分かっている者のパーソナルデータの処理に関して、子どもに代わって消費者の権利を行使することができる。	• 管理者は、最初に子どもの親または法的保護者から同意を得ない限り、子どもと分かっている者のパーソナルデータを**処理してはならない**。※**COPPAの対象となるデータは適用対象外**

出所）杉本 武重「GDPR・CCPA・CPRAの主要論点比較」
（https://www.jetro.go.jp/ext_images/biz/seminar/2021/2e7c9eec1a269310/3.pdf）（2021年11月30日）

連邦法制定に向けた議論状況

連邦法制定に向けた議論状況

連邦データプライバシー法の制定を求めて、議員と民間団体による働きかけが行われている。

■ 2021年7月に、共和党のRoger Wicker上院議員等が、包括的なデータプライバシー法の制定を優先的に進めることを求める書簡をバイデン大統領に送付した。新型コロナウイルスの影響で、オンラインでの活動機会が増加したことにより、パーソナルデータの盗難は、過去1年間で3,000%増加したというFTCのデータもあることから、統一的なデータ保護基準を確立して、連邦全土の消費者のパーソナルデータ保護を推進する狙いがある。※1

■ 2021年11月に、民主党のAnna G. Eshoo議員およびZoe Lofgren議員が、2019年に同議員等が提起したオンラインプライバシー法案を再提案した。当該オンラインプライバシー法案は、電子プライバシー情報センター（EPIC）、アメリカ消費者団体連盟（CFA）などのプライバシー擁護団体や消費者団体に支持されている。※2

■ 2022年1月13日に、米商工会議所を含む20団体が、プライバシーに係る連邦法の成立を求める書簡を提出した。書簡では、バージニア州、コロラド州等、州ごとのプライバシー法は企業のコンプライアンスを困難にしており、連邦取引委員会のプライバシーに関する取組みも問題を複雑化させていると指摘されている。※3

※1：米国上院通商科学運輸委員会 プレスリリース(https://www.commerce.senate.gov/2021/7/committee-leaders-urge-president-to-prioritize-data-privacy-legislation）（2021年11月30日アクセス）
※2： Anna G. Eshoo 議員公式HP(https://eshoo.house.gov/media/press-releases/eshoo-and-lofgren-reintroduce-sweeping-privacy-legislation）（2021年11月30日アクセス）
※3：米商工会議所（https://www.uschamber.com/technology/data-privacy/coalition-letter-on-national-privacy-legislation）（2022年1月21日アクセス）

連邦データプライバシー法案として、COPRAおよびSDAが有力視されている。

■ 連邦データプライバシー法案では、現政権の民主党案であるCOPRAが最有力と見られており、次いで共和党案であるSDAも注目されている。

	COPRA※1 （Consumer Online Privacy Rights Act）	SDA※2 （SAFE DATA Act）
通知内容	• プライバシーポリシーにおいて、以下の記載が必要とされる。 a. 事業者名と問い合わせ先 b. 収集するデータ項目 c. データの転送先のカテゴリと名称、転送の目的 d. 保存期間 e. 消費者の権利の行使方法 f. データセキュリティポリシー g. プライバシーポリシーの発効日	• プライバシーポリシーにおいて、以下の記載が必要とされる。 a. 事業者名と問い合わせ先 b. 収集するデータ項目 c. 収集するデータのカテゴリごとの利用目的 d. データの転送の有無、転送先のカテゴリ、転送の目的 e. 保存期間と保存目的 f. 消費者の権利行使方法 g. データセキュリティプラクティスに関する説明 h. プライバシーポリシーの発効日
オプトアウト	• データの転送に対するオプトアウト権が認められている。 • オプトアウト方法に関しては、消費者の手続きを最小限に抑えるため、できる限り一元化すること、明確で目立つオプトアウト通知と、消費者に優しいメカニズムを提供することが求められる。	• データの収集、処理、転送を行う前に、消費者にそれらをオプトアウトする機能を提供することが求められる。 • 消費者の不作為やサービスの継続的な使用から、消費者が明示的同意を提供したことを推論することは認められない。 • 同意を撤回するための明確で目立つ手段を消費者に提供することが義務付けられる。
センシティブデータ	• 処理にあたって、消費者の同意が必要となる。	• 処理にあたって、消費者の同意が必要となる。
州法との関係	• COPRA と州法が直接的に対立する場合において、COPRA は州法に優先する。 • 一方で、COPRA よりも高いレベルの保護を州法の規定が提供する場合、直接的な対立とは見なされない。	• 州政府が、データプライバシーまたはデータセキュリティおよび関連活動に関する法律や規則等を採択・維持することは認められない。

※1： COPRA法案 (https://www.cantwell.senate.gov/imo/media/doc/COPRA%20Bill%20Text.pdf) （2021年11月30日アクセス）
※2： SDA法案 (https://www.commerce.senate.gov/services/files/BD4D6CB6-AE64-4453-8299-BAC4328BDC56) （2021年11月30日アクセス）

Banning Surveillance AdvertisingAct（監視広告禁止法）

「Banning Surveillance AdvertisingAct（監視広告禁止法）」

■ 時期：2022年1月18日、米連邦議会に提出された法案

- 提出者：Anna Esho下院議員（カリフォルニア州）、Jan Schakowsky下院議員（イリノイ州）、Cory Booker上院議員（ニュージャージー州）

■ 概要

〈Sec2〉ターゲット広告の禁止

a. **広告の作成者（Facebook、Google DoubleClick、データブローカーなど）への禁止・規定事項：**
- 広告の配信をターゲットにすることを禁止し、また故意に第三者に広告の配信を許可することを禁止する。
- 故意に第三者に広告のターゲティングをさせることを禁止する。
- 以下のことを明確にしている。
  - コンテクスト広告が禁止されていないこと
  - 広告配信に関連して収集された情報がさらなるターゲティングに使用されないこと
  - 広告主から提供されたターゲットとなる個人のリストには、
    ①広告主がターゲットとしていることを証明する書面
    ②広告主が(b)項の禁止事項に違反していないこと、を示す書面による証明を添付しなければならないこと

b. **広告主への禁止事項：**
- 第三者から取得した（例えば、データブローカーから購入した）**個人情報**、または保護されたクラスのステータスやその代理人に関連する個人情報に基づいて、広告の配信ターゲットにすること、または広告ファシリテーターや第三者にターゲットにさせること（カスタムオーディエンスなどの個人のリストを提供することを含む）

c. **'recognized place.'へのターゲティングは免除**
※"recognized place"：州、インディアンの土地、市町村、国勢調査で指定された場所、ニールセンTVの市場、または議会地区

個人または接続機器にリンクしている、または合理的にリンク可能なデータであり、推論および派生データ、通信内容、インターネット閲覧履歴、広告の識別子を含む。

〈Sec3〉施行

違反行為は、連邦取引委員会、各州の検事総長、または民間の訴訟によって取り締まることができる

a. FTCに、本法の違反行為を取り締まる権限（コモンキャリアおよび営利目的で組織されていない組織に対するものを含む）、および本法を管理するために行政手続法に基づいて規制を公布する権限を与える
b. 州の検事総長に本法の違反を取り締まる権限を与え、FTCがそのような訴訟に介入することを可能にする。
c. 過失による違反に対しては100～1,000ドル、無謀、故意、意図的な違反に対しては500～5,000ドル、さらに弁護士費用や裁判所が適切と判断したその他の救済措置を講じる私人訴訟権を規定。本法の違反に関連する強制仲裁条項を無効とする。

出所）Eshoo, Schakowsky, Booker Introduce Bill to Ban Surveillance Advertising（アンナ・エシュー下院議員サイト）（ https://eshoo.house.gov/media/press-releases/eshoo-schakowsky-booker-introduce-bill-ban-surveillance-advertising ）（2022年1月24日アクセス）

FTCの執行状況

プライバシー・セキュリティに関連するFTCの執行事例（2021年以降）

時期	対象企業	執行理由	概要
2021/4	Vivint Smart Home, Inc.	情報の不正利用	• スマートホーム製品を提供する同社が顧客の信用情報を不正使用した • FTCは同社に対して、2,000万ドルの制裁金の支払いを命じた
2021/5	Support King, LLC (SpyFone.com)	通知内容と利用実態との乖離	• ストーカーウェア（サイバー上の監視ツール）を提供する同社はユーザーとの規約に反し、密かにデータを取得・開示していた。 • FTCは同社および同社のCEOを監視ビジネスから追放するよう命じた。
2021/5	Everalbum, Inc.	顔認識技術の不正利用、オプトアウトの未対応	• 同社が提供する写真アプリにおいて、顔認識機能が自動的に機能し、オフにすることができなかった。また、アカウントを解除したユーザーの写真やビデオを削除する規約をまもっていなかった。 • FTCは同社に対し、明示的な同意取得を行うよう命じるとともに、アカウント解除ユーザーのデータを使って開発したモデル・アルゴリズムを削除するよう命じた。
2021/6	Flo Health, Inc.	通知内容と利用実態との乖離	• 同社はユーザにデータは非開示のものであると通知していたが、実際は不妊治療アプリを通じて取得していた機密性の高い健康データをFacebookやGoogleなどのマーケティング会社や分析会社と共有していた。 • FTCは通知内容の改定と共有済みのデータの廃棄を命じた。
2021/7	Kuuhuub Inc、Kuu Hubb Oy、Recolor Oy	子供の個人データの収集に関する同意未取得	• 3社は保護者の同意なしに塗り絵アプリを利用する13歳未満の子供から個人情報を収集していた。 • FTCは同意取得と未成年者への返金を命じた。
2021/12	OpenX Technologies, Inc.	子供の個人データの収集に関する同意未取得、オプトアウトの未対応	• 広告プラットフォーム「OpenX」は保護者の同意なしに13歳未満の子供から個人情報を収集していた。また、オプトアウトを申し出たユーザーから引き続き位置情報を収集していた。 • FTCは同社に対して、200万ドルの制裁金の支払いを命じた。
2021/12	Ascension Data & Analytics, LLC	安全管理措置の未実施	• Ascension社は住宅ローン書類のスキャン業務を第三者に委託していた。委託先では氏名、生年月日、社会保障番号などの個人情報を含む書類の内容を、不正アクセスを阻止するための保護を一切せずに、平文でクラウド上のサーバーに保存しており、その結果、数十回不正アクセスされる事態が発生した。 • FTCは同社に対して、委託先の監督を強化するよう命じた。

（出所）・CNILプレスリリース（https://www.cnil.fr/en/actualite）（2022年2月7日アクセス）
・OneTrust DataGuidance（https://www.dataguidance.com/opinion/germany-new-federal-act-regulation-data-protection）（2022年2月7日アクセス）
・AEPD公式HP（https://www.aepd.es/es）（2022年2月7日アクセス）

FTCの執行状況

苦情件数の増加を受けて、FTCはダークパターンに対する執行を強化している。

■ 2021年10月に、連邦取引委員会（FTC）は、ダークパターンによって、消費者をサブスクリプション契約に留めさせる企業に対して警告を行うためのポリシーステートメントを発行した。

■ 当該ポリシーステートメントは、以下の3つの対応を行っていない場合に、法的措置を実行することを企業に通知している。

① 登録プロセスにおける明確な事前の情報提供
最初のオファーの段階で事前に情報提供し、当該情報提供は、オファーそのものと同じくらい目立つようにする。

② 消費者のインフォームドコンセントの取得
製品またはサービスの料金請求前に、明示的なインフォームドコンセントを取得する。これには、消費者がネガティブオプション機能を受け入れるようにすることが含まれる。

③ 容易なキャンセル手段の提供
消費者が、最初に製品やサービスを購入するために使用した方法と同じくらい、容易なキャンセルメカニズムを提供する。

■ FTCは、不正な請求やキャンセル不可能な継続的請求等に関する苦情の増加に伴い、ダークパターンに対する執行を強化しており、これまでに、以下のような慣行への執行事例がある。

- 料金請求に関する事実を、目立たない場所やオファーページ以外のページに隠していること
- キャンセルを希望する消費者に対して、保留にしたり、長い広告を聞かせること
- 無料トライアルが終了する前に、無料トライアルを有料サブスクリプションに切り替えること
- 広く宣伝されているサブスクリプションの、重要なメリットが利用できなくなったことを開示しなかったこと

出所） FTCプレスリリース （https://www.ftc.gov/news-events/press-releases/2021/10/ftc-ramp-enforcement-against-illegal-dark-patterns-trick-or-trap）（2021年11月30日アクセス）

FTCの執行状況

2021年10月FTCはインターネットサービスプロバイダ事業者による利用者情報の取得・利用状況について、調査内容をまとめたスタッフレポートを公表した。

■ レポートの名称：
A Look At What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers

■ 調査対象（６社で米国のモバイルインターネット市場の98%を占める）

- AT&T Mobility
- Cellco Partnership (Verizon Wireless)
- Charter Communications Operating
- Comcast Cable Communications (Xfinity)
- T-Mobile US
- Google Fiber

各社の広告系子会社
- AT&T：Appnexus（現Xandr）
- Verizon：Verizon Online
- Oath Americas（現Verizon Media）

■ レポート内容：

- 調査対象事業者が**利用者情報をどのように取得・利用しているか**、また、**どのようなプライバシー保護措置を講じているか**、提出資料やミーティングを通じて収集した情報をまとめるとともに、調査結果に対するFTCの見解を示している。

（出所）https://www.ftc.gov/news-events/blogs/business-blog/2021/10/look-what-isps-know-about-you-must-read-report-ftc （2022年3月3日アクセス）

FTCスタッフレポート「A Look At What ISPs Know About You」：調査対象事業者による利用者情報の取得・利用実態

■ 調査対象事業者の多くが、4つの主要な目的で利用者情報を取得・利用している。

1. コアとなる通信サービスの提供（インターネット、音声、ビデオ）
2. その他のサービスの提供（例：IoT、ビデオやウェブサイトのコンテンツ）
3. 広告
4. 企業向けのその他のサービスの提供

■ 事業者によっては以下の態様がみられる。

ISP：インターネットサービスプロバイダ事業者

事業者	利用者情報の取得・利用の態様
Some ISPs（3社）	• コアサービスを含む**複数のサービスから取得したデータを結合**している。 サービスの例：TVやビデオストリーミングサービス、ホームオートメーションやセキュリティ製品、接続型ウェアラブルなど
Some ISPs	• 広告宣伝力を上げるため、**通信サービスの提供に必要としないデータ**（アプリの利用履歴など）を**取得**している。
A Few ISPs（2社）	• 行動ターゲティング**広告の配信を目的として閲覧データを利用**（利用する権利を有している）している。
Many ISPs	• 広告主からの依頼を受けて、行動ターゲティング広告を配信している。その際、利用者の**センシティブな情報**を明らかにし、広告主が人種、民族、性的指向、経済状況、政治的所属、宗教的信条**によって広告主が利用者をターゲットできる**ようにしている。
Some ISPs（3社）	• 広告目的で利用者のパーソナルデータ、アプリの利用データ、Webの閲覧データを結合している。
A Significant Number of ISPs	• **リアルタイムの位置情報を第三者に提供**（Share）している。

（出所）https://www.ftc.gov/news-events/blogs/business-blog/2021/10/look-what-isps-know-about-you-must-read-report-ftc （2022年3月3日アクセス）

FTCスタッフレポート「A Look At What ISPs Know About You」：調査対象事業者によるプライバシー保護措置

■ 調査対象事業者は通知・公表、同意・選択、開示、修正、削除の各業務において講じているプライバシー保護措置に関して報告した。

■ FTCは以下の懸念を示している。

FTCの懸念点	懸念を生じさせている事業者の態様
不透明性	• いくつかの事業者は、利用者に**データを売却しないと通知しているが、売却以外にデータを利用、移転、収益化する方法が無数にあること**を利用者に対して**明らかにしておらず**、多くの場合、そうした開示はプライバシーポリシーの細部に埋もれてしまっている。 • また、調査対象事業者のうち3社は、利用者のパーソナルデータを親会社や関連会社と共有する権利を留保しており、データを販売しないという約束に反しているように思われる。
幻想的な選択	• データの使用に関して利用者に**選択肢を提供していると事業者は説明しているが、インターフェースに問題があり**、結果利用者の混乱や潜在的なオプトアウト率の低下につながっている可能性がある。
意味のある開示の欠如	• 多くの事業者が利用者自身によるデータへのアクセス（開示）機会を提供していると説明しているが、そうしたデータは文脈を無視して判読できないか、無意味なことが多く、開示請求が少ないことにつながっている可能性がある。
データの保持と削除	• 調査対象事業者の中には、**データの保持期限**を定めているところもあるが、多くは、ビジネス上必要とされる限り情報を保持していると主張している。しかし、何をもってビジネス上必要とされるかを定義する権利は事業者に与えられており、**事実上自由裁量権を与えている。**

（出所）https://www.ftc.gov/news-events/blogs/business-blog/2021/10/look-what-isps-know-about-you-must-read-report-ftc （2022年3月3日アクセス）

FTCスタッフレポート「A Look At What ISPs Know About You」：調査結果に対するFTCの見解

- 調査対象としたISP事業者は機密性の高い利用者情報を大量に蓄積している。ホームセキュリティ、ビデオストリーミング、広告、電子メール、検索、ウェアラブル、コネクテッドカーなどの他のサービスと垂直統合されたデータは大量であるだけでなく、個々の利用者に関する非常に細かな情報を含んでいる。
- また、ISP業界では、利用者情報を第三者であるデータブローカーから提供を受けたデータと組み合わせる傾向があり、その結果、利用者本人だけでなく、その家族や世帯についても極めて詳細な洞察や推論が得られるようになっている。
- **利用者は**ISP事業者が通信サービスを提供する一環として、訪問先ウェブサイトに関する**情報を取得すること自体は認識しているが、**利用者が必要とした**サービスとは無関係の目的で取得・結合されるデータの範囲に驚くと思われる。**
- 多くのISP事業者が**利用者に選択の機会を提供していると説明しているが、**それらの機会の中には明確に**提供されているとは言えない**ものもあり、実際に、利用者をより多くのデータ共有へと誘導している。
- 調査対象とした**ISP事業者は大規模な広告プラットフォーム（Google、Facebook、Amazon）と同様にプライバシーを侵害する可能性がある。**
  4つの理由があげられる。
  1. 多くのISP事業者が利用者の暗号化されていないインターネット・トラフィックにアクセスできる
  2. 多くのISP事業者が利用者の身元を確認できる
  3. いくつかのISP事業者がウェブサイトや地理的位置に関して消費者を追跡できる
  4. 相当数のISP事業者が利用者の閲覧・視聴履歴を、彼らが提供する付加的な製品・サービスから得られる他の大量の情報と結合することができる。

（出所）https://www.ftc.gov/news-events/blogs/business-blog/2021/10/look-what-isps-know-about-you-must-read-report-ftc （2022年3月3日アクセス）

事例：通知・同意取得における工夫

事例：通知・同意取得における工夫）

GDPRを踏まえ、より効果的に通知・同意取得を行うことができる工夫として、ICO※では以下を挙げている。

ICOにおいて推奨される通知・同意取得における工夫

1. **階層的アプローチ（ A layered approach ）**
   重要な通知内容を含む短い通知文に、より詳細な情報を追加する層を設ける。

2. **ダッシュボード（ Dashboards ）**
   管理ツールで、データの使用方法を通知し、データの使用状況を管理できるようにする。

3. **ジャストインタイム通知（ Just-in-time notices ）**
   個々の情報を収集するとき等に、情報をどのように利用するか簡単な表示を行う。

4. **アイコン（ Icons ）**
   特定の種類のデータ処理の存在を示す、意味のある小さなシンボル。

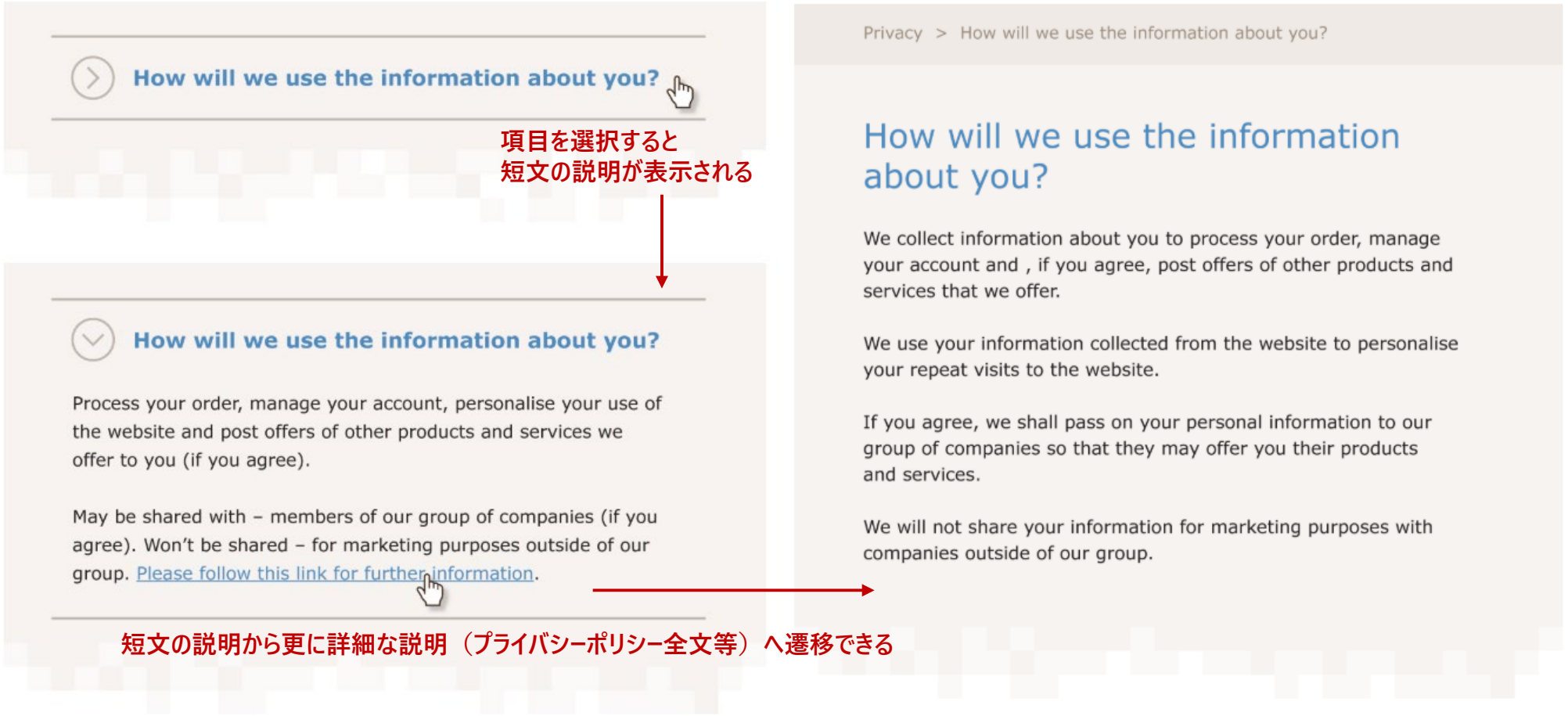
5. **モバイルおよびスマートデバイスの機能性（ Mobile and smart device functionalities ）**
   ポップアップ、音声アラート、モバイルデバイスのジェスチャーなど。

※　ICO（The Information Commissioner's Office）：イギリスのデータ保護機関

事例：通知・同意取得における工夫

階層的アプローチ（ A layered approach ）

- 重要な通知内容を含む短い通知文に、より詳細な情報を追加する層を設ける。
- プライバシー情報の取扱い以外に通知すべき情報があるとき（金融業界における不正利用禁止など）に役立つ。

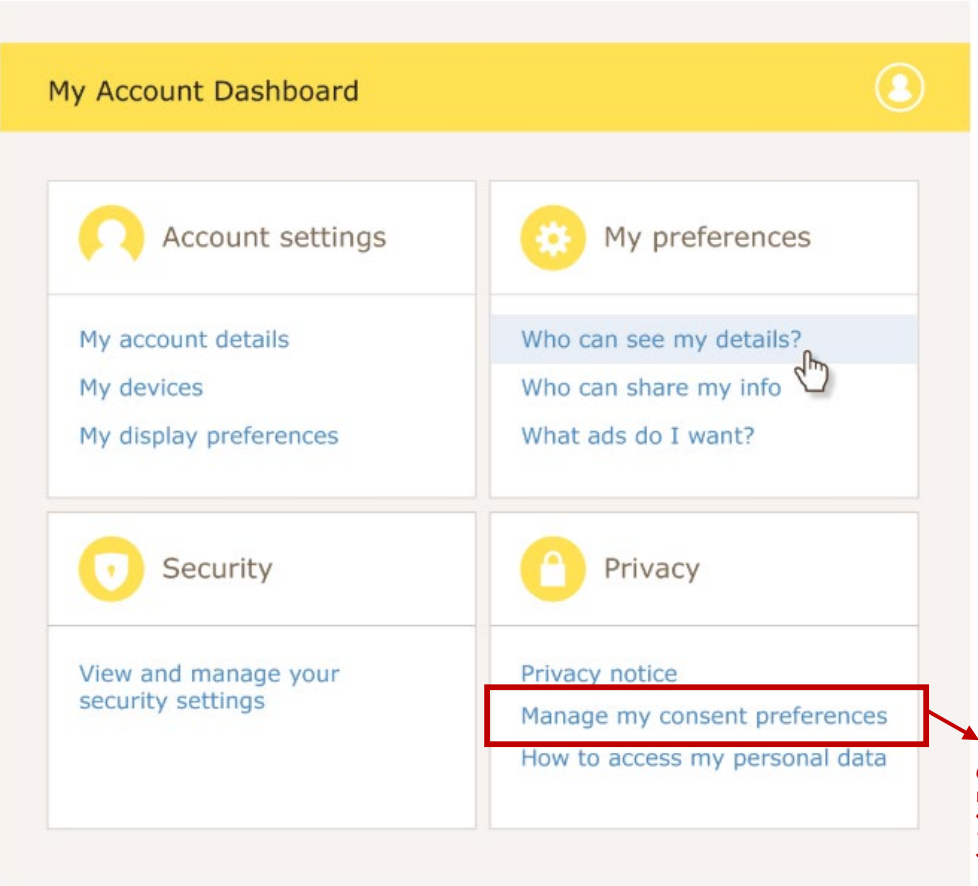


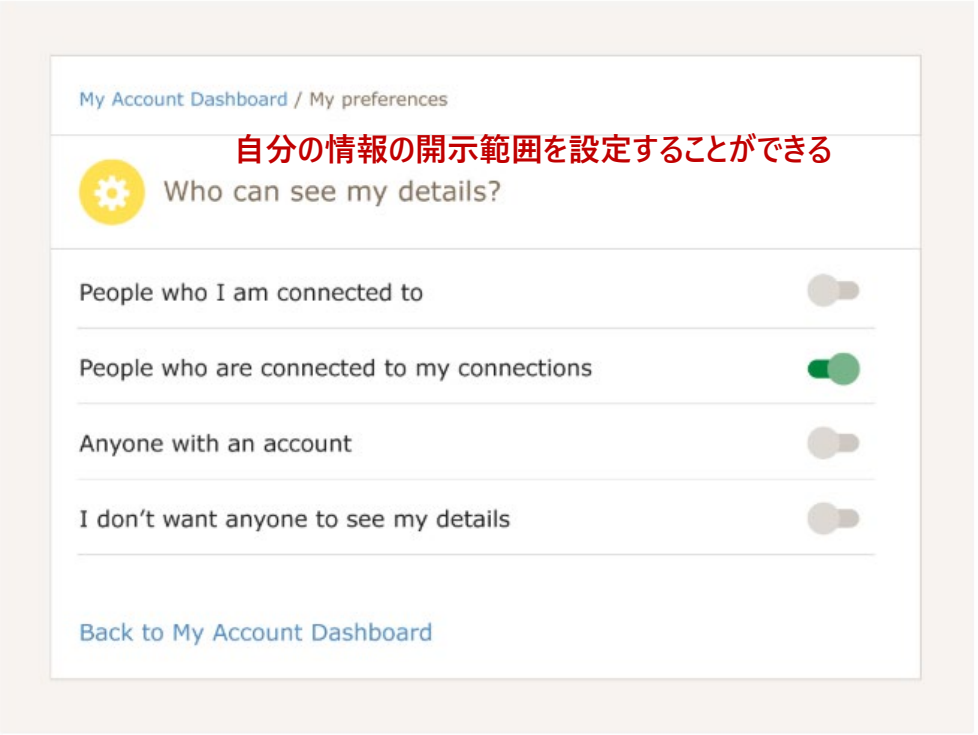
（出所）ICO ウェブサイト： 2020年11月25日アクセスhttps://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/what-methods-can-we-use-to-provide-privacy-information/

事例：通知・同意取得における工夫

ダッシュボード（ Dashboards ）

- 管理ツールで、データの使用方法を通知し、データの使用状況を管理できるようにする。
- 同意と同程度容易に同意の撤回ができなければならないというGDPRの要件を満たすことに役立つ。





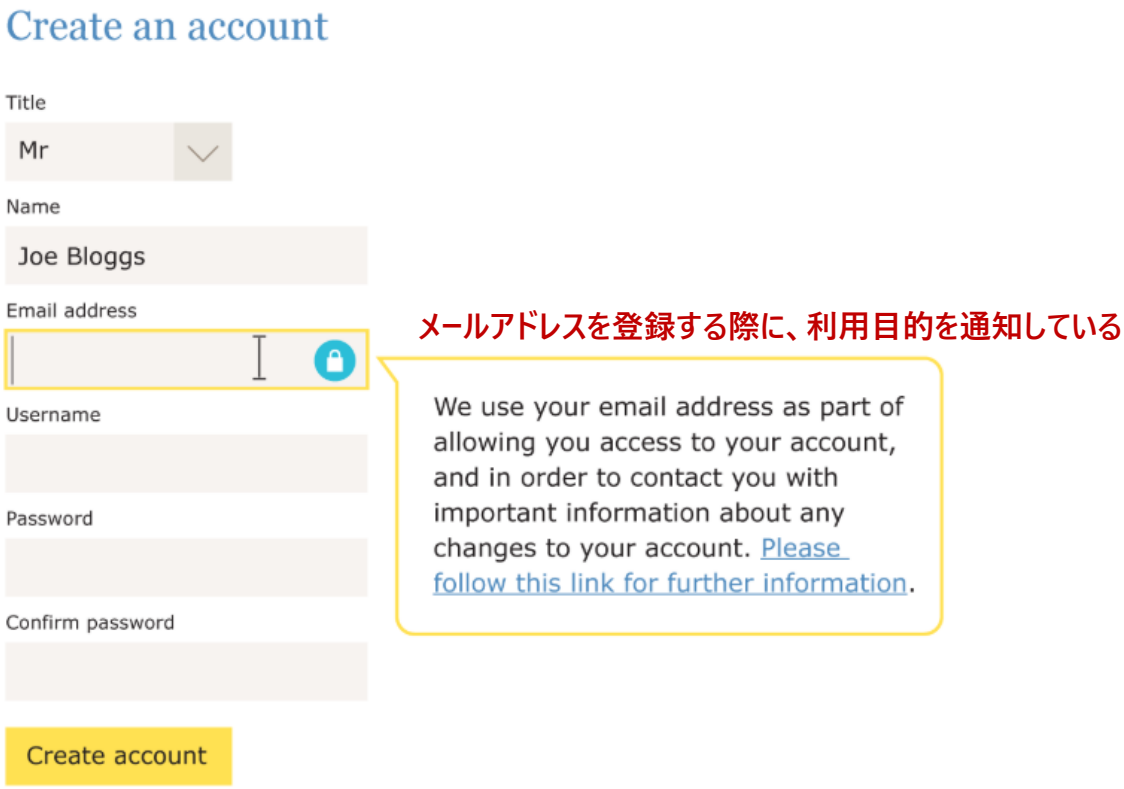
この仕組みを応用する形で、利用目的の種類や第三者提供先について、個別に同意・管理することができるコンセント・マネジメント・プラットフォームサービスが提供され始めている。

（出所）ICO ウェブサイト： 2020年11月25日アクセスhttps://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/what-methods-can-we-use-to-provide-privacy-information/

事例：通知・同意取得における工夫

ジャストインタイム通知（ Just-in-time notices ）

- 個々の情報を収集するとき等に、情報をどのように利用するか簡単な表示を行う。
- 収集時に限らず、購入時等異なるタイミングで通知を行うことで、あらためて個人が、情報を提供していることを認識するのに役立つ。



（出所）ICO ウェブサイト： 2020年11月25日アクセスhttps://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/what-methods-can-we-use-to-provide-privacy-information/

事例：通知・同意取得における工夫

アイコン（ Icons ）

- 特定の種類のデータ処理の存在を示す、意味のある小さなシンボル。
- アイコンを用いることで、データの処理が行われていることを個人にリマインドするのに役立つ。

アイコンの利用方法①

- 個人がオンラインフォームにメールアドレスを入力すると、情報がマーケティングに使用されることを示すアイコンを表示する。アイコンの上にカーソルを置くと、「マーケティング」という言葉が表示され、それをクリックすると、メールアドレスを使って何が行われるかについての、より詳細な説明が表示される。

アイコンの利用方法②

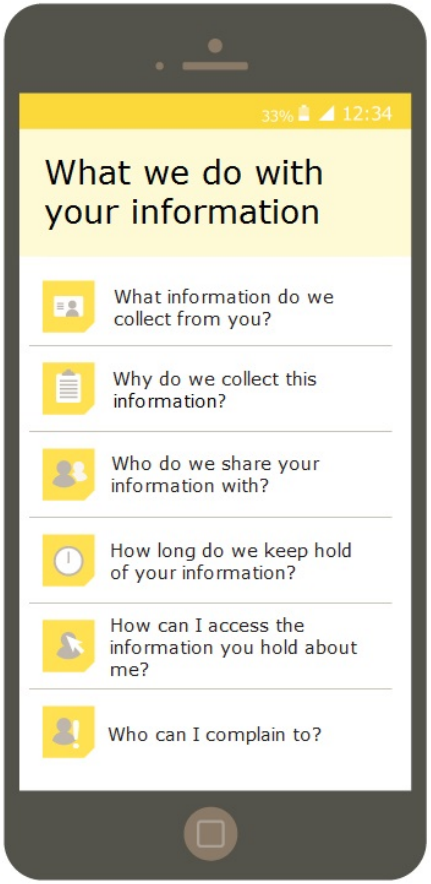
- データ処理が断続的に行われている場合、データ処理が行われていることを示す便利なリマインダーとしてアイコンを使用する。
- このアプローチは特定のアプリが位置情報を処理しているかどうかを示すために、ステータスバーに認識可能なアイコンを配置することで、スマートフォンでよく使用されている。

（出所）ICO ウェブサイト： 2020年11月25日アクセスhttps://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/what-methods-can-we-use-to-provide-privacy-information/

事例：通知・同意取得における工夫

モバイルおよびスマートデバイスの機能性（ Mobile and smart device functionalities ）

■ スマートフォンやタブレットなどのモバイル端末は画面の大きさに制約がある反面、ポップアップ、音声アラート、ジェスチャーなどの独自の機能を利用することができる。



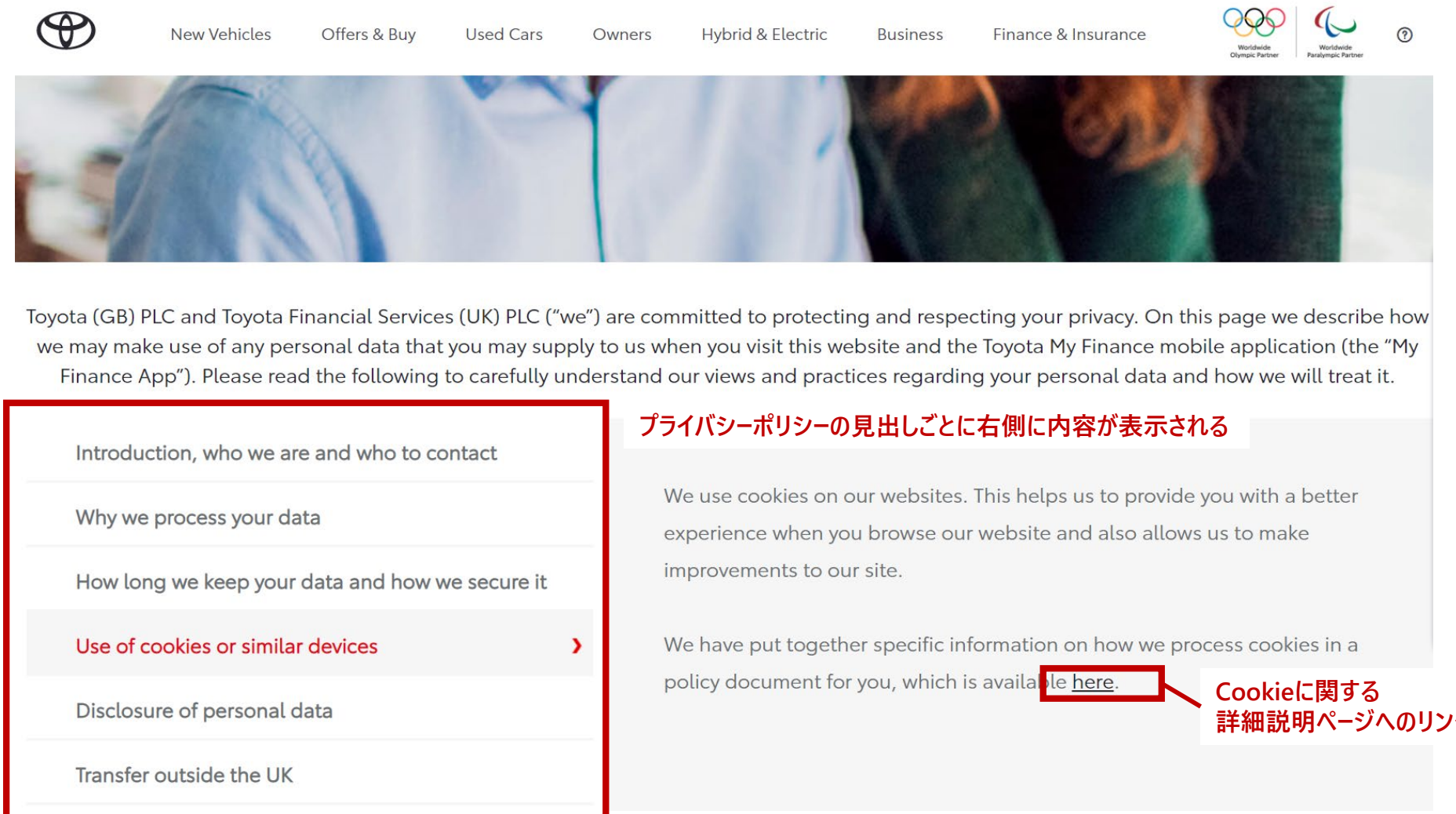
【モバイル端末独自の機能を利用した通知・同意取得の例】

- ジャストインタイムの通知を配信するためのポップアップ。
- 音声、音、振動（または触覚フィードバック）による特定のデータ使用を示すアラート（例：wifiや位置情報の追跡）。
- 圧力感知ディスプレイを使用して、個人がそのページを離れることなく、プライバシー情報の追加レイヤーにアクセスできるようにする。
- より詳細な情報を表示したり、データの異なる使用方法を制御したりするために、スワイプ等モバイルデバイスの一般的なジェスチャーを使用する。

（出所）ICO ウェブサイト： 2020年11月25日アクセスhttps://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/what-methods-can-we-use-to-provide-privacy-information/

事例：通知・同意取得における工夫

階層的アプローチを用いた「通知」の例
Toyota (GB) PLC and Toyota Financial Services (UK) PLC



（出所）https://www.toyota.co.uk/footer/privacy-policy（2022年3月8日アクセス）

事例：通知・同意取得における工夫

CCPAに準拠した「個人情報の収集に伴う通知」の例

Los Angeles Times

Los Angeles Timesのウェブサイトトップページ

Copyright © 2020, Los Angeles Times | Terms of Service | Privacy Policy | CA Notice of Collection | Do Not Sell My Info

ホームページ最下部に利用規約、プライバシーポリシー、CCPA通知、オプトアウトのリンクを分けて記載している

Los Angeles Times

PRIVACY POLICY

16.2

California Notice of Collection

プライバシーポリシーのCCPAに関するセクションに遷移する

Do Not Sell My Info

California residents may opt out of the "sale" of their personal information. We sell certain of your information to third parties to provide you with offers and promotions and opportunities that may be of interest to you.

Under the CCPA, sale is defined such that it may include allowing third parties to receive certain information, such as cookies, IP address, and/or browsing behavior, to deliver targeted advertising on the Services or other services. Advertising, including targeted advertising, enables us to provide you certain content for free and allows us to provide you offers relevant to you.

Depending on what Services you use, we may provide the following categories of personal information to third parties for these purposes:

- For online targeted advertising purposes: demographic and statistical information, user-generated content, device information and identifiers, browser and usage data, geolocation, and social media information.
- For sharing with third parties to send you relevant offers, products, promotions and opportunities: contact and registration information, demographic and statistical information, employment and education data, user-generated content, device information and identifiers, and geolocation.

オプトアウト権とメールでオプトアウト要求をする方法について記載している

If you would like to opt out of our use of your information for such purposes that are considered a "sale" under California law, you may do so as outlined on the following page: Do Not Sell My Info. You can also submit a sale opt-out request by emailing us at privacy@latimes.com. Please note that we do not knowingly sell the personal information of minors under 16 years of age without legally-required affirmative authorization.

Los Angeles Times

Notice of Right to Opt-Out

Opting out of Personalized Advertising

Opt-Out Tools

Opt-Out Tools

To unsubscribe from Los Angeles Times marketing messages, you can adjust your settings here: https://membership.latimes.com/settings.

If you are a California resident, to opt out of the sale of your personal information (and as a result, opt out of personalized advertising), **you must utilize the following toggle (and all 3 tools below)**.

Do Not Sell My Info

ワンクリックでオプトアウトができるようになっている

Save

2020年7月30日アクセス　https://www.latimes.com/

事例：通知・同意取得における工夫

CCPAに準拠した「個人情報の収集に伴う通知」の例
Miller Toyota of Anaheim（カリフォルニア州で営業するトヨタ自動車のディーラー）

Miller Toyota of Anaheim – Notice at Collection of Private Information

Miller Toyota of Anaheim ("Dealership," "we," "us" or "our") respects the privacy of the information our customers entrust to us. This Notice at Collection applies to both the online and offline collection of information. We share personal information unless you instruct us not to do so by submitting a request a (click here) or by calling 833-220-8200. For more information regarding our privacy practices and consumer rights under the California Consumer Privacy Act, view our Privacy Policy also a (click here).

オプトアウトのリンク

プライバシーポリシーへのリンク

Categories of personal information we collect from you	The business or commercial purpose(s) for which it will be used:
Identifiers, such as: Name, postal address, email address, IP address, identification numbers (e.g., social security number, driver's license number, state identification number, military identification number or passport number)	To respond to your requests and inquiries; communicate with you regarding our products or services; enter into transactions with you; process your transactions; send you marketing communications; complete government forms; confirm your identity and that you are at least 18 years old; and/or confirm you are licensed to drive our vehicles or take delivery of a vehicle you have purchased or leased from us
Other personal information described in Civil Code Section 1798.80(e), such as: Phone number; insurance information; bank account number, credit card number, debit card number, or other financial information; and/or your signature	To respond to your requests and inquiries; communicate with you regarding our products or services; enter into transactions with you; process your transactions; send you marketing communications; confirm your insurance coverage; confirm your identity; obtain authorization to collect payment from you; collect payment from you; confirm acknowledgement of receipt of docu ms
Physical de ifications under Calif A photo eveals personal information. For example: • Driver's license/state identification card - includes your image, date of birth, physical description and gender • Permanent resident card - includes your image, date and place of birth; • Social security card - includes your social security number • Passport - includes your image, date and place of birth and your nationality • Military ID - includes your image and rank Completion of a Translated Contract Acknowledgement or signing of translated documents reveals your primary language	To confirm s or take de rm eligibili ss apply such rebate; determine coverage under the Military Lending Act; provide you with copies of certain documents written in the language in which your transaction was primarily negotiated, as required by law; and/or to complete government forms
Commercial information from selling/providing products or services to you, such as: Information, including vehicle information and ownership information, regarding a transaction in which we sell or lease a	To process your transactions; appraise your current vehicle; send you informational and marketing communications; retain records of transactions as required by law; fulfill the terms of a written warranty or product recall; to process warranty, insurance or service contract claims;

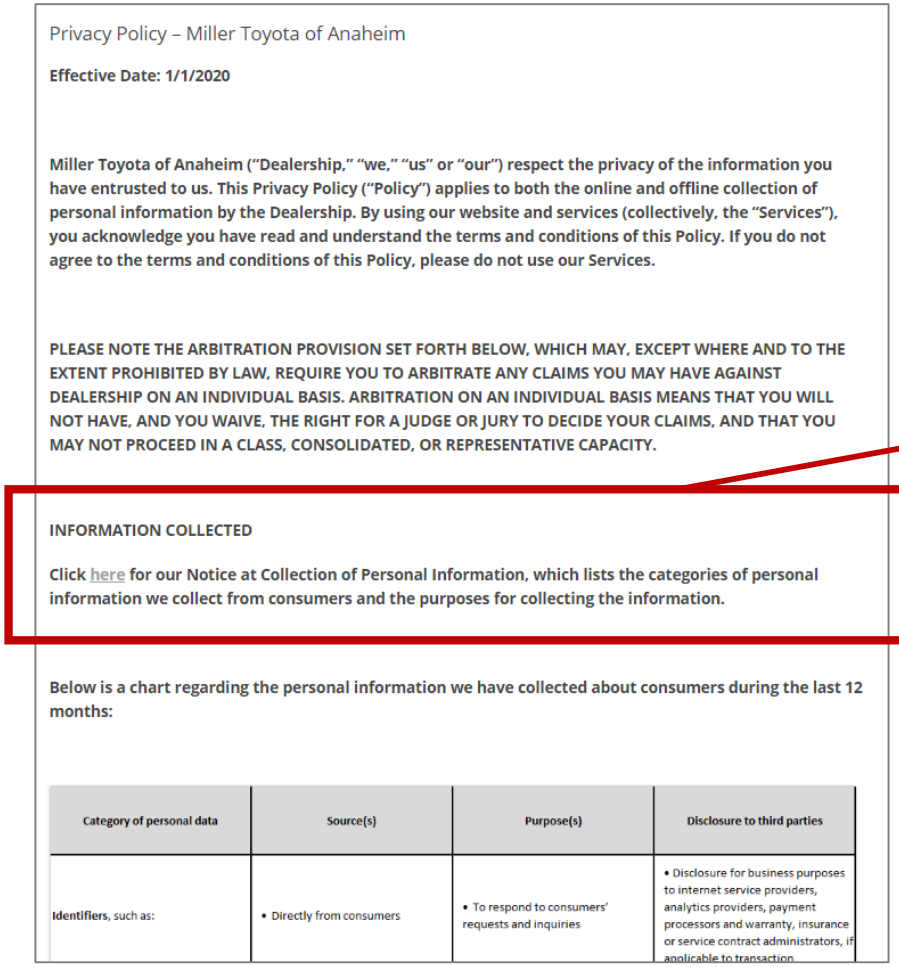
収集する個人情報の種類（カテゴリ）の一覧

個人情報の種類ごとの、事業上または商業上の利用目的

2020年7月30日アクセス https://gpipp.com/MTA/

事例：通知・同意取得における工夫

CCPAに準拠した「プライバシーポリシー」の例
Miller Toyota of Anaheim（カリフォルニア州で営業するトヨタ自動車のディーラー）



Privacy Policy – Miller Toyota of Anaheim

Effective Date: 1/1/2020

Miller Toyota of Anaheim ("Dealership," "we," "us" or "our") respect the privacy of the information you have entrusted to us. This Privacy Policy ("Policy") applies to both the online and offline collection of personal information by the Dealership. By using our website and services (collectively, the "Services"), you acknowledge you have read and understand the terms and conditions of this Policy. If you do not agree to the terms and conditions of this Policy, please do not use our Services.

PLEASE NOTE THE ARBITRATION PROVISION SET FORTH BELOW, WHICH MAY, EXCEPT WHERE AND TO THE EXTENT PROHIBITED BY LAW, REQUIRE YOU TO ARBITRATE ANY CLAIMS YOU MAY HAVE AGAINST DEALERSHIP ON AN INDIVIDUAL BASIS. ARBITRATION ON AN INDIVIDUAL BASIS MEANS THAT YOU WILL NOT HAVE, AND YOU WAIVE, THE RIGHT FOR A JUDGE OR JURY TO DECIDE YOUR CLAIMS, AND THAT YOU MAY NOT PROCEED IN A CLASS, CONSOLIDATED, OR REPRESENTATIVE CAPACITY.

INFORMATION COLLECTED

Click here for our Notice at Collection of Personal Information, which lists the categories of personal information we collect from consumers and the purposes for collecting the information.

Below is a chart regarding the personal information we have collected about consumers during the last 12 months:

Category of personal data	Source(s)	Purpose(s)	Disclosure to third parties
Identifiers, such as:	• Directly from consumers	• To respond to consumers' requests and inquiries	• Disclosure for business purposes to internet service providers, analytics providers, payment processors and warranty, insurance or service contract administrators, if applicable to transaction

個人情報の収集に伴う通知のリンク

2020年7月30日アクセス https://gpipp.com/MTAPP/


Share the Next Values!