プライバシーポリシー・クッキーポリシーのつくり方

（連絡先）
TEL: 03-5288-1021（代表）
Email: m-watanabe@miyake.gr.jp
k-koshida@miyake.gr.jp
k-iwata@miyake.gr.jp
n-idenuma@miyake.gr.jp

弁護士法人 三宅法律事務所
弁護士　渡邉　雅之
同　越田　晃基
同　岩田　憲二郎
同　出沼　成真

1. プライバシーポリシーのつくり方

1．1　プライバシーポリシーとは？

- 我が国の個人情報保護法その他の法令・ガイドラインなどにおいて、プライバシーポリシーの明確な定義はなし。
- 企業は、「プライバシーポリシー」、「個人情報保護方針」、「個人情報保護宣言」などの名称のポリシーをウェブサイトなどに公表している例が多い。
- 個人情報保護法上は、「保有個人データに関する事項の公表等」（法32条）と安全管理措置（法23条）に関して、通則編ガイドラインが求める「基本方針」を併せたものを公表している例が多い。
- GDPRにおいては、「プライバシーノーティス」の作成が法令上求められている。

1．2　プライバシーポリシーの意義

- 対外的に顧客等の個人情報を適切に取り扱っていることを宣言し（透明性）、顧客等の信頼を得るため。
- 利用目的を通知・公表、明示することにより、個人情報（個人データ）の利活用を可能とするため。
- 個人データの第三者提供につき、プライバシーポリシーを通じて同意を取り、第三者提供を可能とするため。
- 保有個人データの開示、訂正等、利用停止等に応じる手続を示すため。
- 顧客等から苦情や質問がある場合に対応する窓口を示すため。

1．3　プライバシーポリシーの個情法上の根拠①

- 個人情報取扱事業者は、個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表しなければならない（法21条１項）。

- 個人情報取扱事象者は、書面・電磁的記録により、個人情報を取得する場合には、あらかじめ、本人に対して利用目的を明示しなければならない（法21条２項）。

- 個人情報取扱事業者は、個人データを第三者に提供する場合には、原則として、本人の同意を取得しなければならない（法27条１項）。

1．3　プライバシーポリシーの個情法上の根拠②

- 個人情報保護法32条の「保有個人データに関する事項の公表等」の公表等事項が根拠の一つとなる。もっとも、「本人の知り得る状態」に置くほか、「本人の求めに応じて遅滞なく回答をする場合」も認められているので、必ずしも全て公表をすることが求められているわけではない。

【公表等が求められている事項】
①当該個人情報取扱事業者の氏名・名称・住所（法人の場合は代表者の氏名）
②全ての保有個人データの利用目的
③開示、訂正等、利用停止等に応じる手続
④保有個人データの安全管理のために講じた措置（本人の知り得る状態に置くことにより当該保有個人データの安全管理に支障を及ぼすおそれがあるものを除く。）
⑤当該個人情報取扱事業者が行う保有個人データの取扱いに関する苦情の申出先
⑥当該個人情報取扱事業者が認定個人情報保護団体の対象事業者である場合には、当該認定個人情報保護団体の名称・苦情の解決の申出先

1．3　プライバシーポリシーの個情法上の根拠③

- 個人データの共同利用をする場合には以下の事項について、あらかじめ本人に通知または本人が容易に知り得る状態に置く必要がある（法27条5項3号）。

【公表等が求められている事項】
①特定の者との間で共同して利用される個人データが当該特定の者に提供される場合がある旨
②共同して利用される個人データの項目
③共同して利用する者の範囲
④利用する者の利用目的
⑤当該個人データの管理について責任を有する者の氏名・名称・住所（法人の場合は代表者の氏名）

1．3　プライバシーポリシーのガイドライン上の根拠①

- 安全管理措置（法23条）の一つとして、通則編ガイドラインにおいては、「基本方針の策定」（10－1）が求められる。

10－1　基本方針の策定

- 個人情報取扱事業者は、個人データの適正な取扱いの確保について組織として取り組むために、基本方針を策定することが重要である。
- 具体的に定める項目の例としては、例えば以下の事項が考えられる。

  ①事業者の名称
  ②関係法令・ガイドライン等の遵守
  ③安全管理措置に関する事項
  ④質問及び苦情処理の窓口

1．3　プライバシーポリシーのガイドライン上の根拠②

「金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針」では、基本方針に以下の事項を含め、公表することが求められている。

① 個人情報取扱事業者の名称
② 安全管理措置に関する質問及び苦情処理の窓口
③ 個人データの安全管理に関する宣言
④ 基本方針の継続的改善の宣言
⑤ 関係法令等遵守の宣言

1．3　プライバシーポリシーのガイドライン上の根拠③

「電気通信事業における個人情報等の保護に関するガイドライン」では、電気通信事業者は、プライバシーポリシー（当該電気通信事業者が個人データ等の適切な取扱いを確保する上での考え方や方針をいう。）を定め、公表することが適切であるとされ、以下の事項について定め、利用者に分かり易く示すことが求められる。

①電気通信事業者の氏名又は名称
②取得される情報の項目
③取得方法
④利用目的の特定・明示
⑤通知・公表又は同意取得の方法及び利用者関与の方法
⑥第三者提供の有無
⑦問合せ窓口・苦情の申出先
⑧プライバシーポリシーの変更を行う場合の手続
⑨利用者の選択の機会の内容、データポータビリティに係る事項
⑩委託に係る事項

1．3　プライバシーポリシーの法的根拠：特定電子メール法

- 「特定電子メール」とは、「営利を目的とする団体及び営業を営む場合における個人」である送信者が「自己又は他人の営業につき広告又は宣伝を行うための手段として送信する電子メール」である（同法2条2号）。
- 特定電子メールは、あらかじめ、送信をすることに同意する旨を送信者に対して通知しなければならない（同法3条1項1号）。
- 適正な「同意」が取得されていると言えるためには、通常の人間であれば広告・宣伝メールの送信が行われることが認識されるような形で説明等が行われていることが必要。
- 電子メールアドレスの登録時に、契約を申し込むサービスの約款や利用規約に同意の通知の相手方の名称及び特定電子メールを送信する旨の記載があっても、極めて小さい文字又は極めて目立たない色の文字で記載されている場合や、約款や利用規約が長くウェブサイトを膨大にスクロールして、注意しないと認識できないような場所に記載されている場合などのように、通常の受信者であればそれに気付くとは考えにくい場合などは、受信者が認識できるように表示されているとはいえない。
  （特定電子メールの送信等に関するガイドライン・総務省）
  ➡電子メールで送付するプライバシーポリシーについて同意を取得する場合にも上記に留意する必要がある。

1．3　プライバシーポリシーの法的根拠：特商法

- 特定商取引に関する法律（「特商法」）は、通信販売、連鎖販売取引、業務提供誘引販売取引に関して、承諾をしていない者に対して電子メール広告が原則禁止（特商法12条の3、36条の3、54条の3）。
- 消費者から承諾を受ける場合には、消費者が操作を行う際に認識できるように表示していないことにより、消費者の意に反する請求・承諾が容易に行われる状態に該当しないようにすることが求められる（特商法14条1項、同法施行規則42条2項1号）。
- 『電子メール広告をすることの承諾・請求の取得等に係る「容易に認識できるように表示していないこと」に係るガイドライン 』では、「容易に認識できるように表示していないこと」に該当するおそれがある場合として、「膨大な画面をスクロールしないと広告メールの送信についての承諾の表示にたどり着けず、かつ画面の途中に小さい文字で記述されているなど、消費者がよほどの注意を払わない限りは見落としやすく、広告メールの送信について承諾をしたこととなってしまう場合」が掲げられている。

  ➡通信販売において、電子メールにおいてプライバシーポリシーの承諾を得る場合には、上記に留意する必要がある。

1．3　プライバシーポリシーの法的根拠：GDPR①：域外適用

- EU一般データ保護規則は、以下の（a）または(b)に関連して、EU 域内に拠点のない管理者または処理者によるEU 在住のデータ主体の個人データの処理に適用される。（規則3条2項）
  （a） EU 在住のデータ主体に対する商品・サービスの提供に関する処理。
  ＊ウェブサイトにおいて、1つのEU加盟国で用いられる言語または通貨を利用して、商品・サービスの提供を行っている場合が該当する。（例：フランス語＋ユーロ）
  ＊単に管理者や処理者のウェブサイト、電子メールでアクセスできるだけでは該当しない。
  （b）EU 域内で行われるデータ主体の行動の監視に関する処理。
  ＊個人の嗜好、行動、態度を分析・予測してその人物に関する決定を下すために、個人がインターネット上で監視されているか否か。自然人のプロファイリングを構成する個人データ処理技術を利用する可能性も含まれる。
- たとえば、日本国内の旅館が、EU域内所在者向けにインターネット上で、EU言語（英語・フランス語など）で宿泊サービスというサービスを提供している場合で、インターネット経由で個人データ（住所・氏名・クレジットカード番号など）を登録してもらう場合には、GDPR上の管理者としての義務を負う。

1．3　プライバシーポリシーの法的根拠：Google Analyticsについて

Google Analytics（グーグルアナリティクス）は、Googleが無料で提供するWebページのアクセス解析サービス。

□ 使用目的

サイト訪問者の動向を把握することで、訪問者の欲求を知り、サイト内の人気ページや不人気ページ、問題のあるページを知り、サイトを改善することで訪問者の満足を高め、訪問者数を伸ばす。商用サイトであれば業務に寄与し、アフィリエイトサイトであれば収益を伸ばす。

□ アクセス情報

利用者と対象サイトを登録して対象サイト内にタグ埋め込むことで、基本的なアクセス情報として以下のものが入手できる。

- 訪問者数
- 閲覧ページ数
- 滞在時間・訪問回数・訪問頻度
- 訪問者のサイト内移動経路
- 訪問者の検索キーワード
- 訪問者の来訪前経由サイト
- 訪問者の最初に開いたページと最後に開いたページ
- 訪問者の使用PC等の画面解像度、ブラウザの種類、回線の種類、プロバイダ、アクセスしてきた国・地域
- 広告クリック数と収益

※Google Analyticsの利用規約において、同サービスについて利用者に情報提供することが求められているため、プライバシーポリシーに記載することが考えられる。

1．4　利用目的：個人情報保護法上の規律

（利用目的の特定）
第17条　個人情報取扱事業者は、個人情報を取り扱うに当たっては、その利用の目的（以下「利用目的」という。）をできる限り特定しなければならない。
２　個人情報取扱事業者は、利用目的を変更する場合には、変更前の利用目的と関連性を有すると合理的に認められる範囲を超えて行ってはならない。

（利用目的による制限）
第18条　個人情報取扱事業者は、あらかじめ本人の同意を得ないで、前条の規定により特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない。
２・３（略）

（適正な取得）
第20条　個人情報取扱事業者は、偽りその他不正の手段により個人情報を取得してはならない。
２　個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、要配慮個人情報を取得してはならない。
　一～六（略）

（取得に際しての利用目的の通知等）
第21条　個人情報取扱事業者は、個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表しなければならない。
２　個人情報取扱事業者は、前項の規定にかかわらず、本人との間で契約を締結することに伴って契約書その他の書面（電磁的記録を含む。以下この項において同じ。）に記載された当該本人の個人情報を取得する場合その他本人から直接書面に記載された当該本人の個人情報を取得する場合は、あらかじめ、本人に対し、その利用目的を明示しなければならない。ただし、人の生命、身体又は財産の保護のために緊急に必要がある場合は、この限りでない。
３　個人情報取扱事業者は、利用目的を変更した場合は、変更された利用目的について、本人に通知し、又は公表しなければならない。
４　前三項の規定は、次に掲げる場合については、適用しない。
　一～三（略）
　四　取得の状況からみて利用目的が明らかであると認められる場合

1．4　利用目的:個人情報保護委員会の指導･勧告①

令和元年 9 月 17 日

個人情報の保護に関する法律に基づく指導について

個人情報保護委員会は、令和元年9月 12 日付けで、JapanTaxi株式会社（以下「本件会社」という。）に対し、個人情報の保護に関する法律（平成15年法律第 57 号）第 41条の規定に基づき、次のとおり指導を行いましたので、お知らせします。

1．本件会社は、タクシー車内に設置したタブレット端末付属のカメラを用いてタクシー利用者の顔画像を撮影して広告配信に利用しているが、その旨をタクシー利用者に対して十分に告知していなかった。当委員会は、本件会社に対し、タクシー利用者に対する分かりやすい説 明の徹底等について、平成30年11月30日付けで指導を行ったが、今般、平成31年4月に至るまで改善策が実施されていなかったことが判明した。

2．当委員会は、タクシー利用者の権利利益に対する影響の程度や、事業者における顧客目線の重要性という観点に加え、当委員会の指導への対応に時間を要した組織体制上の問題点も考慮し、今回、再度の指導を実施することとした。

3．顔画像を撮影していることのタクシー利用者に対する説明については、本件会社において、平成31年4月以降、乗車時にタブレット端末の画面上で告知を表示する対応がなされているところ、その他の改善策についても方針に関する報告は受けており、引き続きフォローしてゆく。当委員会としては、事業者において適法性の検討が十分になされた上で、新たなデジタル技術を活用した事業やサービスが円滑に実現されるよう取り組んでまいります。

1．4　利用目的:個人情報保護委員会の指導・勧告②

〇個人情報の保護に関する法律に基づく行政上の対応について（令和2年7月29 日）

- 個人情報保護委員会は、本日、多数の破産者等の個人情報をウェブサイトに違法に掲載している2事業者に対し、個人情報の保護に関する法律（平成15 年法律第57 号）第42 条（※現148条）第2 項に基づき、当該ウェブサイトを直ちに停止等するよう命令を行いました。なお、当該2事業者の所在をいずれも知ることができなかったため、公示送達の手法により行いました。詳細は、別紙を参照願います。
- また、このようなウェブサイトの中には、マイニングツール等のプログラムが設置されており、パソコンの処理能力が意図せずに使用され、動作が遅くなるなどの事象が生じる可能性もございますので、いずれのサイトも閲覧されませんようお願いします。

（別紙）

1 命令の原因となる事実

当該2事業者は、破産手続開始決定の公告として官報に掲載された破産者等の個人情報を取得するにあたり、利用目的の通知・公表を行わず（同法第18 条（※現21条））、当該個人情報をデータベース化した上、第三者に提供することの同意を得ないまま、これをウェブサイトに掲載していたものである（同法第23 条（※現27条）第1項）。

2 命令事項等

当委員会は、当該2事業者に対し、ウェブサイトを直ちに停止した上、前記利用目的の通知・公表を行うとともに、その個人データを第三者に提供することの同意を得るまでは、同ウェブサイトを再開してはならない旨の勧告を行ったが、対応期限の日までに措置が講じられなかったため、その勧告に係る措置をとるべきことを命令した。

本命令の対応期限（本年8月27 日）までに具体的な対応がなされない場合は、同法第84条（※現178条）の罰則適用を求めて刑事告発することを予定している。

1．4　利用目的：個人情報保護委員会の指導・勧告③

〇個人情報の保護に関する法律に基づく行政上の対応について（令和元年12月４ 日）
１ リクルート社及びリクルートキャリア社に対する勧告
⑴ 勧告の原因となる事実
③「リクナビ2020」プレサイト開設時（2018年６月）に、本サービスの利用目的が同サイト内に記載されたことをもって、サービス利用企業から提供を受けた氏名で突合し内定辞退率を、算出していた。しかしながら、プレサイト開設時のプライバシーポリシーには第三者提供の同意を求める記載はなく、2019年３月のプライバシーポリシー改定までの間、本人の同意を得ないまま内定辞退率をサービス利用企業に提供していた。

⑵ 主な勧告事項
個人データを取り扱う際に、適正に個人の権利利益を保護するよう、組織体制を見直し、経営陣をはじめとして全社的に意識改革を行い、以下の事項を含め、必要な措置をとること
〇（略）
〇 個人情報を取得する際は、商品等の内容をできる限り特定し、当該利用目的の通知又は公表を適切に行うこと
〇（略）
２ 本サービスを利用していた企業に対する指導
本サービス利用企業に対する調査の結果、本サービスに関する利用目的の通知又は公表等が不適切であったことや個人データを外部に提供する際の法的検討ないし当該法的整理に従った対応等が不適切であった。
このため別紙に掲載する企業に対し、以下の事項について適切に対応するよう指導を行った。
⑴ 利用目的の通知、公表等を適切に行うこと
⑵⑶（略）

1．4　利用目的：利用目的の特定①

〇通則編ガイドライン3-1-1（利用目的の特定（法第17条第 1 項関係））

個人情報取扱事業者は、個人情報を取り扱うに当たっては、利用目的をできる限り具体的 に特定しなければならないが、利用目的の特定に当たっては、利用目的を単に抽象的、一般 的に特定するのではなく、個人情報が個人情報取扱事業者において、最終的にどのような事 業の用に供され、どのような目的で個人情報を利用されるのかが、本人にとって一般的かつ 合理的に想定できる程度に具体的に特定することが望ましい（※）。なお、あらかじめ、個人情報を第三者に提供することを想定している場合には、利用目的 の特定に当たっては、その旨が明確に分かるよう特定しなければならない（3-4-1（第三者 提供の制限の原則）参照）。

【具体的に利用目的を特定している事例】

事例）事業者が商品の販売に伴い、個人から氏名・住所・メールアドレス等を取得するに当たり、「〇〇事業における商品の発送、関連するアフターサービス、新商品・サ ービスに関する情報のお知らせのために利用いたします。」等の利用目的を明示して いる場合

【具体的に利用目的を特定していない事例】

事例 1)「事業活動に用いるため」

事例 2)「マーケティング活動に用いるため」

1．4　利用目的：利用目的の特定②

○通則編ガイドライン3-1-1（利用目的の特定（法第17条第1項関係））（※1）

「利用目的の特定」の趣旨は、個人情報を取り扱う者が、個人情報がどのような事業の用に供され、どのような目的で利用されるかについて明確な認識を持ち、できるだけ具体的に明確にすることにより、個人情報が取り扱われる範囲を確定するとともに、本人の予測を可能とすることである。

本人が、自らの個人情報がどのように取り扱われることとなるか、利用目的から合理的に予測・想定できないような場合は、この趣旨に沿ってできる限り利用目的を特定したことにはならない。

例えば、本人から得た情報から、本人に関する行動・関心等の情報を分析する場合、個人情報取扱事業者は、どのような取扱いが行われているかを本人が予測・想定できる程度に利用目的を特定しなければならない。

【本人から得た情報から、行動・関心等の情報を分析する場合に具体的に利用目的を特定している事例】

事例1）「取得した閲覧履歴や購買履歴等の情報を分析して、趣味・嗜好に応じた新商品・サービスに関する広告のために利用いたします。」

事例2）「取得した行動履歴等の情報を分析し、信用スコアを算出した上で、当該スコアを第三者へ提供いたします。」

1．4　利用目的：利用目的の明示

〇通則編ガイドライン3-2-4
直接書面等による取得（法第21条第 2 項関係）
【利用目的の明示に該当する事例】
事例 1）利用目的を明記した契約書その他の書面を相手方である本人に手渡し、又は送付 する場合 なお、契約約款又は利用条件等の書面（電磁的記録を含む。）中に利用目的条項を 記載する場合は、例えば、裏面約款に利用目的が記載されていることを伝える、又は 裏面約款等に記載されている利用目的条項を表面にも記載し、かつ、社会通念上、本 人が認識できる場所及び文字の大きさで記載する等、本人が実際に利用目的を確認 できるよう留意することが望ましい。
事例 2）ネットワーク上において、利用目的を、本人がアクセスした自社のホームページ上に明示し、又は本人の端末装置上に表示する場合 なお、ネットワーク上において個人情報を取得する場合は、本人が送信ボタン等を クリックする前等にその利用目的（利用目的の内容が示された画面に 1 回程度の操 作でページ遷移するよう設定したリンクやボタンを含む。）が本人の目に留まるよう その配置に留意することが望ましい。
（※）「本人に対し、その利用目的を明示」とは、本人に対し、その利用目的を明確に 示すことをいい、事業の性質及び個人情報の取扱状況に応じ、内容が本人に認識 される合理的かつ適切な方法による必要がある。

➡プライバシーポリシーのウェブリンクを付けるだけでも個人情報保護法上は許される（リクナビ問題）

1．4　利用目的:カメラ画像利活用ガイドライン

事前告知には、例えば以下の内容を記載する。

- カメラ画像の内容及び利用目的
- 運用実施主体の名称及び一元的な連絡先
- カメラ画像の利活用によって生活者に生じるメリット
- カメラの設置位置及び撮影範囲
- カメラ画像から生成又は抽出等するデータの概要
- 生成又は抽出等したデータからの個人特定の可否
- 生成又は抽出等したデータを第三者への提供の有無、及び提供する場合、その提供先
- カメラ画像やカメラ画像から生成又は抽出等するデータの安全管理のために講じる措置
- データ利活用の開始時期

1．5　本人の同意が必要な場合

〇個人情報保護法上、本人の（事前の）同意が必要な場合

- **個人情報取扱事業者が特定された利用目的の達成に必要な範囲を超えて個人情報を取り扱う場合（同法18条1項）**
  ※同法18条3項各号の例外あり。
- **個人情報取扱事業者が要配慮個人情報を取得する場合（同法20条2項）**
  ※同法17条2項各号の例外あり。
- **個人情報取扱事業者が、個人データを第三者に提供する場合（同法27条1項）**
  ※同法27条1項各号の例外、2項のオプトアウト、5項各号の第三者に該当しない場合の例外あり。
- **個人情報取扱事業者が、個人データを第三者に提供する場合は「外国にある第三者への提供を認める旨の本人の同意」が必要（同法28条）**
  ※同法27条1項各号の例外等あり。

※JISQ15001 :2023（プライバシーマークの規格）において同意が追加的に必要な場合

本人から書面に記載された個人情報を直接取得する場合は、以下の事項を、**あらかじめ、書面によって本人に明示し、書面により同意を取得する必要がある。**

a) 組織の名称又は氏名
b) 個人情報保護管理者（若しくはその代理人）の氏名又は職名，所属及び連絡先
c) 利用目的
d) 個人情報を第三者に提供することが予定される場合の事項
－ 第三者に提供する目的
－ 提供する個人情報の項目
－ 提供の手段又は方法
－ 当該情報の提供を受ける者又は提供を受ける者の組織の種類，及び属性
－ 個人情報の取扱いに関する契約がある場合はその旨

1．5　ガイドラインが求める「本人の同意」

通則編ガイドライン2-12 「本人の同意」

- 「本人の同意」とは、本人の個人情報が、個人情報取扱事業者によって示された取扱方法で取り扱われることを承諾する旨の当該本人の意思表示をいう（当該本人であることを確認できていることが前提となる。）。
- また、「本人の同意を得（る）」とは、本人の承諾する旨の意思表示を当該個人情報取扱事業者が認識することをいい、事業の性質及び個人情報の取扱状況に応じ、本人が同意に係る判断を行うために必要と考えられる合理的かつ適切な方法によらなければならない。
- なお、個人情報の取扱いに関して同意したことによって生ずる結果について、未成年者、成年被後見人、被保佐人及び被補助人が判断できる能力を有していないなどの場合は、親権者や法定代理人等から同意を得る必要がある。

【本人の同意を得ている事例】

事例 1）本人からの同意する旨の口頭による意思表示
事例 2）本人からの同意する旨の書面（電磁的記録を含む。）の受領
事例 3）本人からの同意する旨のメールの受信
事例 4）本人による同意する旨の確認欄へのチェック
事例 5）本人による同意する旨のホームページ上のボタンのクリック
事例 6）本人による同意する旨の音声入力、タッチパネルへのタッチ、ボタンやスイッチ等による入力

１．５ 「本人の同意」に関するQ&A

１．オプトアウト的な「同意」はダメ

- 本人が同意に係る判断を行うために必要と考えられる合理的かつ適切な方法によらなければなりません。したがって、一定期間回答がなかったことのみをもって、一律に本人の同意を得たものとすることはできません。（QA１－56 ）

２．黙示の同意

- 同意は、本人による承諾の意思表示をいいますので、「明示の同意」以外に「黙示の同意」が認められるか否かについては、個別の事案ごとに、具体的に判断することとなります。（QA１－57）

３．子供の同意に関する法定代理人の同意

- 法定代理人等から同意を得る必要がある子どもの具体的な年齢は、対象となる個人情報の項目や事業の性質等によって、個別具体的に判断されるべきですが、一般的には 12 歳から 15 歳までの年齢以下の子どもについて、法定代理人等から同意を得る必要があると考えられます。（QA１－58）

４．包括的同意

- 必ずしも第三者提供のたびに同意を得なければならないわけではありません。例えば、個人情報の取得時に、その時点で予測される個人データの第三者提供について、包括的に同意を得ておくことも可能です。

1．5　GDPRの同意との比較①

	個人情報保護法	GDPR
同意取得が必要な場合	➢ 利用目的の達成の範囲を超えて個人情報を取扱う場合 ➢ 要配慮個人情報を取得する場合 ➢ 個人データを第三者提供する場合	処理（processing）一般 ※個人データの取得、利用、第三者提供を含む。
同意取得の例外	同意取得の例外として以下の場合（同法18条3項各号、27条1項各号） ① 法令に基づく場合 ② 人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。 ③ 公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき ④ 国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。 ※個人データの取扱いの委託は、法23条5項1号で、「第三者」と見られないため本人の同意不要。	適法な処理の根拠として「同意」のほか以下が認められる。（6条1項） ① 契約の履行のため必要な場合 ② 法的義務を遵守のため必要な場合 ③ データ主体等の重大な利益を保護する場合 ④ 公共の利益のため取扱いが必要な場合 ⑤ 管理者の「正当な利益のため」取扱いが必要な場合 例）ダイレクトメールの送付

1．5　GDPRの同意との比較②

	個人情報保護法	GDPR
同意の要件	本人の個人情報が、個人情報取扱事業者によって示された取扱方法で取り扱われることを承諾する旨の当該本人の意思表示 ➢ 個別的な同意取得のほか、包括的な同意取得も認められている。 ➢ 明示的な同意取得のほか黙示的な同意取得も認められる場合あり。 ➢ インフォームドコンセント（あらかじめ本人に情報提供）は求められていない。 ➢ オプトアウト的な同意取得は認められない。	**① 自由に与えられていること** ➢ 力の不均衡がないこと前提 ➢ 同意が契約履行に必要のない条件でないかどうか考慮 ➢ 同意事項の細分化必要 ➢ 同意撤回に不利益がなし **② 特定されていること** ➢ 同意取得の細分性必要 ➢ 同意を取得する情報を他の情報と明確に分離必要 **③ あらかじめ情報提供を受けていること（インフォームドコンセント）** **④ 明確な意思表示であること** ➢ 書面やチェックボックスなどの明確な積極的な行為
未成年者等の制限行為能力者の個人情報	未成年者、成年被後見人、被保佐人及び被補助人が判断できる能力を有していないなどの場合は、親権者や法定代理人等から同意を得る必要。 （12～15歳以下の子供からは親権者からの同意が一般的に必要）	➢ 子どもが16歳以下の場合は親権者の同意が必要 ➢ ターゲットに未成年者が含まれる場合は未成年者にも理解できる情報提供が必要
同意の撤回	権利として認められていない。	権利として認められている。

1．6　いわゆる3年ごと見直し：「不適正な利用の禁止」「適正な取得」の規律の明確化

改正の方向性：本人の自律的な意思の選択が可能でない場合の不適正取得・不適正利用の規律の適用（実現可能性：60%）

- 「個情委の考え方」においては、「本人の自律的な意思の選択が可能でない場合」についての不適正取得（法20条）、不適正利用（法19条）の規律の適用が検討されている。
- 「本人の自律的な意思の選択が可能でない場合」とは、「本人との関係に照らして当然認められるべき利用目的以外の利用目的で個人情報を取得・利用すること」や、「当然認められるべき利用目的の達成に真に必要な範囲を越えて個人情報を取得・利用すること」などである。
- 具体的には、①個人情報取扱事業者が本人との関係で利用目的達成に必要な利用目的を超えた個人情報の利用目的の通知・公表（法21条1項）の明示（法21条2項）や、②本人との関係で必要のない利用目的の範囲外の目的外利用する場合の本人からの同意の取得（法18条1項）、本人との関係で個人データの提供の必要がない第三者への提供を認める包括的な第三者提供の本人からの同意の取得（法27条1項）などが想定される。
- 後者（②）については、代替困難なサービスの取引条件として個人情報の取扱いに関する同意が求められるなど、事実上、本人が自らの個人情報の提供等につき自ら判断・選択できないようなケースも問題視されている。
- これは、「本人の同意の任意性」の問題でもあると考えられるが、個人情報保護法では、本人からの同意の取得について「任意性」が必要であることは定められていない。
- GDPR（EU一般データ保護規則）においては、データ主体からの同意取得には任意性が必要とされており（GDPR第4条11号）、例えば、同意することがサービス提供等の条件とされている場合等については同意が自由に与えられていないとして任意性が否定されると考えられている。
- 改正の方向性としては、「本人の同意」の要件として、新たに「任意性」を追加するのではなく、「本人の同意の任意性が認められない場合」を含む「本人の自律的な意思の選択が可能でない場合」について、不適正取得（法20条）、不適正利用（法19条）の規律を適用することが検討されている。
- これは、我が国の個人情報保護法においては「本人の同意」が重視されており、GDPRのように、「契約の履行」や「正当な利益」などの他の「取扱い（処理）」の適法性の根拠が認められておらず、現行実務に混乱を来たす可能性もあることから、同意の効力を緩める「同意の任意性」を認めるのは困難との判断に基づくものであると考えられる 。
- もっとも、どのような場合が「本人の自律的な意思が選択できない場合」に該当するのかは判断が難しいものであり、事業者の萎縮的効果をもたらすものとして改正の可能性が必ずしも高いとは言えないかもしれない。

1．6　いわゆる3年ごと見直し：こどもの個人情報等に関する規律の在り方

個情委の考え方

- こどもの個人情報の取扱いに係る規律については、こどもの脆弱性・敏感性及びこれらに基づく要保護性を考慮するとともに、学校等における生徒の教育・学習に関するデータの有用性も考慮する必要がある。これを踏まえ、主要各国においてこどもの個人情報等に係る規律が設けられており、執行事例も多数見られることも踏まえ、こどもの権利利益の保護という観点から、規律の在り方の検討を深める必要がある。
- 他方で、第三者が公開したこどもの個人情報を取得する場合などにおいては、取得した情報にこどもの個人情報とこども以外の者の個人情報が含まれている場合や、こどもの個人情報が含まれているかが明らかでない場合があり得ることから、こうした場合における事業者の負担を考慮する必要がある。

法定代理人の関与	● 現行法上、原則として本人同意の取得が必要とされている場面において、こどもを本人とする個人情報について、法定代理人の同意を取得すべきことを法令の規定上明確化することを検討する必要がある。 ※目的外利用（法第18条第2項）、要配慮個人情報の取得（法第20条第2項）、個人データの第三者提供（法第27条第1項、第28条1項）、個人関連情報の第三者提供（法第31条第1項）など ● 本人に対する通知等が必要となる場面においても、こどもを本人とする個人情報について、法定代理人に対して情報提供すべきことを法令の規定上明文化することを検討する必要がある。 ※利用目的の通知（法第21条第1項）、本人から直接書面に記載された個人情報を取得する場合における利用目的の明示（同条第2項）、漏えい等に関する本人への通知（法第26条第2項）など
利用停止等請求権の拡張	● 現行法上、利用停止等請求権を行使できる場面は、保有個人データについて違法行為があった場合等限定的であるが、こどもの要保護性を踏まえると、こどもを本人とする保有個人データについては、他の保有個人データ以上に柔軟に事後的な利用停止を認めることについて検討する必要がある。ただし、取得について法定代理人の同意を得ている場合等、一定の場合においてはその例外とすることも考えられる。
安全管理措置義務の強化	● 重大なこどもの個人情報の漏えい事件が国内で発生しており、委員会においても前述の大手学習塾に対する指導に際して「こどもの個人データについては、こどもの「安全」を守る等の観点から、特に取扱いに注意が必要であり、組織的、人的、物理的及び技術的という多角的な観点からリスクを検討し、必要かつ適切な安全管理措置を講ずる必要がある」旨述べているところである。そこで、こどもの個人データについて安全管理措置義務を強化することがあり得る。
責務規定	● 各事業者の自主的な取組の促進という観点からは、こどもの個人情報等の取扱いについては、こどもの最善の利益を優先し特別な配慮を行うべき等、事業者等が留意すべき責務を定める規定を設けることも検討する必要がある。
年齢基準	● こどもの個人情報等の取扱いに係る年齢基準の考え方については、国内外の法制度において様々な年齢基準が設けられていることや、対象年齢によっては事業者等の負担が大きくなることも考慮する必要があるが、対象とするこどもの年齢についてはQ&Aの記載やGDPRの規定の例などを踏まえ、16歳未満とすることについて検討を行う。

1．6　要保護性の高い個人情報の取扱いについて（生体データ）

個情委の考え方

■ 生体データは、長期にわたり特定の個人を追跡することに利用できる等の特徴を持ち得るものであり、特に、特定の個人を識別することができる水準が確保されている場合において、通常の個人情報と比較して個人の権利利益に与える影響が大きく、保護の必要性が高いと考えられる。他方、生体データは本人認証に広く利用されているほか、犯罪予防や安全確保等のために利用することも想定されるものである。これを踏まえ、生体データの取扱いについて、諸外国における法制度なども参考にしつつ、特に要保護性が高いと考えられる生体データについて、実効性ある規律を設けることを検討する必要がある。この点について、関係団体からは、事業者の自主的な取組を促進すべきとの声もあるが、本人関与や安全管理措置等を通じた個人の権利利益の保護とのバランスを踏まえ検討を進める必要がある。

- まず、現行法上、個人情報の利用目的については、「できる限り特定」しなければならないとされているが（法第17条第１項）、生体データの要保護性を踏まえると、生体データを取り扱う場合においては、例えば、どのようなサービスやプロジェクトに利用するかを含めた形で利用目的を特定することを求めることが考えられる。
- また、個人の権利利益の保護という観点からは、生体データの利用について、本人がより直接的に関与できる必要がある。そのため、生体データの取扱いに関する一定の事項を本人に対し通知又は十分に周知することを前提に、本人による事後的な利用停止を他の保有個人データ以上に柔軟に可能とすることが考えられる。
- このほか、必要となる規律の在り方について、事業者における利活用の実態やニーズ、運用の負担、利用目的の違いによる影響なども考慮して検討する必要がある。

1．6 いわゆる3年ごと見直し：違法な第三者提供

個情委の考え方

■ 現行法においては、事業者が個人データを違法に第三者に提供した場合について、報告義務及び本人通知義務は存在しないが、個人データが漏えい等した場合については事業者にこれらの義務が課されることとの均衡から、漏えい等との違いの有無も踏まえ、その必要性や報告等の対象となる範囲を検討する必要がある。

改正の方向性：違法な第三者提供の報告等（実現可能性：80%）

■ 我が国における現在の実務上、「漏えい」と「提供」とは両立し得ない概念であり、両社の分水嶺は事業者の「意図」にあるとされる。その「意図」は、①第三者に提供する意図があるか（提供自体）、②意図した提供先に提供されているか（提供先）、③意図した個人データが提供されているか（個人データの対象・範囲）を踏まえて判断される 。

■ もっとも、このような「意図」は、本人の権利利益侵害のおそれとはさほど関係がないように思われ、違法な第三者提供であれば本人通知等のプロセスを経る必要がないとする現行法の規定にはややアンバランスな印象も拭いきれない。すなわち、過失によるうっかりの漏えいの場合は漏えい等報告が必要であるのに対して、故意による漏えいについては法27条の第三者提供制限の違反とはなるものの漏えい等報告は必要はないというのは不均衡であると考えられる。

■ 海外に目を向けると、GDPRは、漏えいと違法な個人情報の取扱いとを区別せず、「データ侵害」との概念を用いている。このようなGDPRにおける取扱いは、本項目に関する今後の改正内容を占うにあたっても参考になろう。

■ 違法な第三者提供については、現状、個人情報保護委員会への報告・本人への通知の義務がない状況であることに鑑みると、事業者が本来同意を取得しなければならないケースについては、法改正で義務化されるまでに違反行為を是正しておくことが望まれる。

1．6　本人同意を要しないデータ利活用等の在り方

個情委の考え方

■ 昨今のデジタル化の急速な進展・高度化に伴い、生成AI等の新たな技術の普及等により、大量の個人情報を取り扱うビジネス・サービス等が生まれている。また、健康・医療等の公益性の高い分野を中心に、機微性の高い情報を含む個人情報等の利活用に係るニーズが高まっている。このほか、契約の履行に伴う個人情報等の提供や、不正防止目的などでの利活用についてもニーズが寄せられている。

■ こうした状況を踏まえ、法で本人同意が求められる規定の在り方について、個人の権利利益の保護とデータ利活用とのバランスを考慮し、その整備を検討する必要がある。この場合においては、単に利活用の促進の観点から例外事由を認めるのは適当ではなく、本人の権利利益が適切に保護されることを担保することが必要である。

- 生成AIなどの、社会の基盤となり得る技術やサービスのように、社会にとって有益であり、公益性が高いと考えられる技術やサービスについて、既存の例外規定では対応が困難と考えられるものがある。これらの技術やサービスについては、社会的なニーズの高まりや、公益性の程度を踏まえて、例外規定を設けるための検討が必要である。この際、「いかなる技術・サービスに高い公益性が認められるか」について、極めて多様な価値判断を踏まえた上で高度な意思決定が必要になる。個人の権利利益の保護とデータ利活用の双方の観点から多様な価値判断が想定されるものであり、関係府省庁も含めた検討や意思決定が必要と考えられる。
- 医療機関等における研究活動等に係る利活用のニーズについても、公益性の程度や本人の権利利益保護とのバランスを踏まえて、例外規定に係る規律の在り方について検討する必要がある。例えば、医療や研究開発の現場における公衆衛生例外規定の適用のように、例外規定はあるものの、適用の有無に関する判断にちゅうちょする例があるとの指摘がある。こうした点等については、事業者の実情等も踏まえつつ、関係府省庁の関与を得ながら、ガイドラインの記載等についてステークホルダーと透明性のある形で議論する場の設定に向けて検討する必要がある。

1．６ いわゆる3年ごと見直し：本人同意を要しないデータ利活用等の在り方

改正の方向性：「契約の履行」や「正当な利益」などの例外規定について（実現可能性：20%）

- 業界団体からは、目的外利用（法18条１項）や第三者提供（法27条１項）の同意に関する例外規定として、GDPRにおける「契約の履行」や「正当な利益」のように、一定の条件下で個人情報を本人同意なく取り扱うことができる場合について検討をすることが要望されている（新経済連盟など）。
- しかしながら、「個情委の考え方」においてはこれらの例外規定については明示的に検討対象となっていない。
- 我が国の個人情報保護法が「本人の同意」を重視する制度であり、本人の同意がない場合には原則として特定された利用目的の範囲でしか個人情報を利用できず、限られた公益的理由がなければ取扱いが認められない制度であることに鑑みると、柔軟性の高い「契約の履行」や「正当な利益」のような取扱いは困難と個人情報保護委員会が考えているのではないかと思われる。
- 中間整理の第１回検討会では、構成員から新経済連盟に対して、『「正当な利益」によるデータ利活用への言及もある。私は「正当な利益」もあり得ると思うが、GDPRにおいては、「正当な利益」に基づく利用に対する異議申立てについても定めている。新経連としては、こうした異議申し立てもセットで考えているという趣旨か。』との質問がなされた。

1．7　GDPR①：域外適用（EUに拠点がない日本企業に適用される場合）

- EU一般データ保護規則は、以下の（a）または(b)に関連して、EU 域内に拠点のない管理者または処理者によるEU 在住のデータ主体の個人データの処理に適用される。（規則3条2項）
  （a） EU 在住のデータ主体に対する商品・サービスの提供に関する処理。
  ＊ウェブサイトにおいて、1つのEU加盟国で用いられる言語または通貨を利用して、商品・サービスの提供を行っている場合が該当する。（例：フランス語＋ユーロ）
  ＊単に管理者や処理者のウェブサイト、電子メールでアクセスできるだけでは該当しない。
  (b) EU 域内で行われるデータ主体の行動の監視に関する処理。
  ＊個人の嗜好、行動、態度を分析・予測してその人物に関する決定を下すために、個人がインターネット上で監視されているか否か。自然人のプロファイリングを構成する個人データ処理技術を利用する可能性も含まれる。
- たとえば、日本国内の旅館が、EU域内所在者向けにインターネット上で、EU言語（英語・フランス語など）で宿泊サービスというサービスを提供している場合で、インターネット経由で個人データ（住所・氏名・クレジットカード番号など）を登録してもらう場合には、GDPR上の管理者としての義務を負う。

1．7　GDPR①：域外適用される上での判断基準（地理的適用範囲のガイドライン）

- EUまたは少なくとも1つの加盟国が、提供された商品またはサービスに関して、明示されていること。
- データ管理者または処理者が、EU域内の消費者によるサイトへのアクセスを容易にするために、インターネット参照サービスの検索エンジン事業者に支払いを行っていること。または管理者または処理者が、EU加盟国の顧客に向けられたマーケティングおよび広告キャンペーンを開始すること。
- 特定の観光活動など、活動自体の国際的な性質。
- EU加盟国所在の顧客のための専用の住所やEU加盟国から掛けられる電話番号が記載されていること。
- 管理者または処理者が設立されている第三国以外のトップレベルのドメイン名（例：".de"）、または ".eu"などの中立トップレベルドメイン名を使用していること。
- 1つ以上の他のEU加盟国からサービスが提供される場所への旅行指示の説明があること。
- 様々なEU加盟国に所在する顧客からなる国際的な顧客、特に当該顧客によって書かれた口座の提示により言及していること。
- 商人の所在国で一般的に使用されている以外の言語または通貨、特に1つ以上のEU加盟国の言語または通貨を使用していること。
- データ管理者が、EU加盟国における商品の納品を提供すること。

1．7　GDPR②：データ主体への通知（12条）

①簡潔かつ透明で、分かりやすく、容易にアクセス可能でなければならない（第12条1項）。

「簡潔かつ透明」

情報は、契約条項や一般的な利用規約など、他の非プライバシー関連情報とは明確に区別する必要。オンラインでは階層化されたプライバシー・ステートメント/ノーティスを使用すること。

「分かり易いこと」

意図された視聴者の平均的なメンバーによって理解されるべき。理解度は、明確で平易な言葉を使用するという要件に密接に関連。

「容易にアクセス可能であること」

オンラインで階層化されたプライバシー・ステートメント/ノーティス、FAQ、データ件名がオンライン形式で記入されたときに稼働するコンテクスト・ポップアップ、またはチャットボット・インターフェースを介した双方向的なデジタルコンテクスト

②明瞭かつ平易な文言を使用しなければならない（第12条1項）。

- 複雑な文章や言語の構造を避けて、できるだけシンプルに情報を提供すること。
- 情報は具体的かつ決定的であること。抽象的または相反する用語で表現されるべきではなく、異なる解釈のための余地を残すべきはない。
- 個人データの処理の目的と法的根拠は明確でなければならない。
- 「may」（かもしれない）、「might」（だろう）、「some」（いくつかの）、「often」（しばしば）および「possible」（可能性がある）などの言語修飾子も避ける。
- 文章は受動的な文章ではなく主体的な文章にする必要があり、余分な名詞は避けるべき。データ主体に提供される情報は、過度の法律、技術または専門用語または用語を含むべきではない。
- すべての翻訳が正確であること、および翻訳された文章を解読し、再解釈する必要がないように、言い回しおよび構文が第2言語で意味をなすことを確保する必要。

③明瞭かつ平易な文言の要件は、子供に情報を提供する場合に重要である（第12条1項）。

④書面で、または適切な場合は電子的手段その他の手段によって行われなければならない（12条1項）。

- 管理者がウェブサイトを有する場合、ウェブサイトの訪問者が特定のプライバシー・ステートメント/プライバシー・ノーティスのうち、彼らが最も関心のあるものに案内することが可能である階層的なプライバシー・ステートメント/ノーティスを用いることが推奨される。
- 個人情報を取り込むデバイスに、そのデバイスにアクセスするための画面（IoTデバイスやスマートデバイスなど）がない場合は、ハードコピーの処理説明書にプライバシー・ステートメント/ノーティスを提示するか、オンラインのプライバシー・ステートメント/ノーティスを行うことができるURLウェブサイトアドレス（すなわち、ウェブサイト上の特定のページ）を提示するなど、ハードコピーの指示書またはパッケージに記載。

⑤データ主体が要求する場合、口頭で提供することができる（第12条1項）。

⑥一般的に無償で提供されなければならない（第12条5項）

1．7　GDPR②：明瞭かつ平易な文言

〇不十分な実践例

以下の表現は、処理の目的に関しては十分に明確ではない。

- 「個人情報を使用して新しいサービスを開発することができます」（「サービス」とは何か、またはデータがサービスを開発する上でどのように役立つかは不明）。
- 「私たちは研究目的であなたの個人データを使用することができます（これがどのような「調査」の種類であるかは不明）。
- 「個人向けのサービスを提供するためにお客様の個人データを使用することがあります」（「個人向けの」が何を意味するのかは不明）。

〇優れた実践例

- 「あなたのショッピング履歴を保持し、以前に購入した製品の詳細を使用して、他の製品についてもあなたが興味を持っていると思われるものを提案する」（どのような種類のデータが処理されるのか、データサブジェクトは製品のターゲット広告の対象となり、そのデータはこれを可能にするために使用される。）
- 「当社は、あなたの最近のウェブサイトへの訪問に関する情報およびあなたが当社のウェブサイトのさまざまなセクションをどのように移動するかに関する情報を、人々がどのように当社のウェブサイトを利用しているかについて理解し、それがより分かりやすくするという分析目的のために保有し評価いたします。」（どの種類のデータが処理されるのか、管理者が実行する分析の種類が明確）。
- 「当社はあなたがクリックしたウェブサイト上の記事を記録し、その情報を、あなたが読まれた記事に基づいて特定したあなたの興味に関連するウェブサイト広告をお送りするために利用します。」（パーソナライゼーション（特定の個人に向けたものにしていること）が何を伴うのか、データ主体が有する興味がどのように識別されたのかが明確）

1．7　GDPR③：プライバシーノーティス

必要となる情報の種類	関連条文（個人データが直接データ主体から取得される場合	関連条文（個人データがデータ主体から取得されない場合）
管理者（および代理人）の本人特定事項および連絡先	13条1(a)項	14条1項(a)
データ保護オフィサーの連絡情報（該当する場合）	13条1項(b)	14条1項(b)
処理の目的および法的根拠	13条1項(c)	14条1項(c)
正当な利益が処理の法的根拠である場合、管理者または第三者が追求した正当な利益	13条1項(d)	14条1項(d)
関連する個人データの種類	非該当	14条1項(d)
個人データの受領者（または受領者の種類）	13条1項(e)	14条1項(e)
第三国への移転の詳細、その事実、関連する保護措置の詳細（欧州委員会の十分性認定の有無を含む）、およびそれらのコピーを入手する手段または入手可能となった場所	13条1項(f)	14条1項(f)
保管期間（または可能でない場合は、その期間の決定に使用される基準）	13条2項(a)	14条2項(a)
データ主体の権利： ・開示 ・訂正 ・消去 ・処理の制限 ・処理に対する異議 ・ポータビリティ	13条2項(b)	14条2項(c)
処理が同意（または明示的同意）に基づいている場合、いつでも同意を取り消す権利	13条2項(c)	14条2項(d)
監督機関に苦情を申し立てる権利	13条2項(d)	14条2項(d)
情報を提供するための法的または契約上の要件、または契約を締結する必要があるかどうか、または情報を提供する義務があるかどうか、また失敗の可能性があるかどうか。	13条2項(e)	非該当
個人データの発信元、および該当する場合は、公開されている情報源からのものかどうか	非該当	14条2項(f)
プロファイリング、適用可能であれば、使用されているロジックに関する意義ある情報、データ主体に対するそのような処理の意義と想定される結果を含む自動化された意思決定の存在	13条2項(f)	14条2項(g)

2. クッキーポリシーのつくり方

2．1　Cookie（クッキー）

1　Cookieとは

- Cookie（クッキー）は、ウェブサイトがブラウザにコンピュータまたはモバイルデバイスに保存するように要求する小さなデータ。Cookieを使用すると、ウェブサイトは個人の行動や嗜好を時間の経過とともに「記憶」することができる。ほとんどのブラウザはCookieをサポートしているが、ユーザーはブラウザにおいてCookieを使用しないように設定できる。

2　ウェブサイトにおけるCookieの用途

- ウェブサイトは主にCookieを、①ユーザーの識別、②ユーザーのカスタム設定の記憶、③ユーザーのサイトを閲覧するときにサイトに入らずにタスクを完了できるようにすること、に使用できる。Cookieは、オンラインの行動ターゲット広告に使用して、過去にユーザーが検索したものに関連する広告を表示することもできる。
- ウェブページを提供するウェブサーバは、ユーザーのコンピュータまたはモバイルデバイス上にクッキーを格納することができる。ファイルをホストする外部Webサーバは、Cookieを格納するためにも使用できる。これらのCookieはすべて、http header Cookieと呼ばれる。Cookieを保存する別の方法は、そのページに含まれているJavaScriptコードを使用する方法。
- ユーザーが新しいページを要求するたびに、WebサーバはCookieのセットの値を受け取ることができる。同様に、JavaScriptコードは、そのドメインに属するCookieを読み取り、それに応じてアクションを実行することができる。

3　Cookieの種類

（1）存続期間による分類

①**セッションCookie**：ユーザーがブラウザを閉じたときに消去されるCookie
②**永続Cookie**：事前定義された期間、ユーザーのコンピュータ/デバイスに残るCookie

（2）帰属による分類

①**ファーストタイプCookie**: Webサーバによって設定され、同じドメインを共有するCookie
②**サードパーティCookie**:訪問したページのドメインとは別のドメインによって保存されたCookie
このCookieは、Webページがそのドメイン外にあるJavaScriptなどのファイルを参照しているときに発生。

2．1　Cookieは個人情報に該当するか？

〇個人情報保護法2条1項
「個人情報」とは、生存する個人に関する情報であって、次の各号のいずれかに該当するものをいう。
① １号個人情報
- **当該情報に含まれる氏名、生年月日その他の記述等（文書、図画若しくは電磁的記録（電磁的方式（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式をいう。）で作られる記録をいう。）に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項（個人識別符号を除く。）をいう。）により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）**

②　２号個人情報
- **個人識別符号が含まれるもの**

➡Cookieは、それ自体では特定の個人を識別することができず、（１号）個人情報には該当しない。ただし、他の情報と容易に照合することができ、それにより特定の個人を識別することができる場合には、個人情報に該当する。

２．２　リクルートキャリアに対する勧告

- 令和元年（2019年）12月14日に、個人情報保護委員会は、就職情報サイト「リクナビ」を運営する株式会社リクルートキャリア（「リクルートキャリア社」）及びその親会社である株式会社リクルート（「リクルート社」）に対して、いわゆる内定辞退率を提供するサービスに関して、個人情報の保護に関する法律（以下「個人情報保護法」という。）に基づく勧告を行った。また、同サービスの利用企業に対し、同法に基づく指導を行った。（「12月14日勧告等」）

- リクルートキャリア社に対しては、8 月 26 日付で勧告等を行っていた が、当該勧告等の原因となった事項以外にも個人情報保護法に抵触する事実が確認されたため、改めて勧告を行ったもの。

2．2　勧告①（アンケートスキーム（2019年2月以前の仕組み））

【勧告①】
2018年度卒業生向けの「リクナビ2019」におけるサービスでは、個人情報である氏名の代わりにCookieで突合し、特定の個人を識別しないとする方式で内定辞退率を算出し、第三者提供に係る同意を得ずにこれを利用企業に提供していた。リクルートキャリア社は、内定辞退率の提供を受けた企業側において特定の個人を識別できることを知りながら、提供する側では特定の個人を識別できないとして、個人データの第三者提供の同意取得を回避しており、法の趣旨を潜脱した極めて不適切なサービスを行っていた。

〇アンケートスキーム

- リクルートキャリアが契約企業から学生の姓名・メールアドレス等の個人情報の提供を受けるのではなく、契約企業が学生向けに実施したウェブアンケートを通じて、リクルートキャリアの委託先である株式会社リクルートコミュニケーションズ（「リクルートコミュニケーションズ」）が①契約企業固有の応募者管理 ID（契約企業が付与していた応募者の管理 ID）、②Cookie 情報、③選考プロセスにおける辞退・承諾情報を直接取得。
- リクルートコミュニケーションズは、『リクナビ』のウェブサイトを通じて「Cookie情報」およびリクナビサイト上での「業界ごとの閲覧履歴」を直接取得。
- リクルートコミュニケーションズは「契約企業固有の応募者管理ID」とリクナビサイト上での「業界ごとの閲覧履歴」をウェブアンケートとリクナビサイトの「Cookie情報」によって紐づけ、スコアを算出 。リクルートコミュニケーションズでは、これらの情報だけでは特定の個人を識別することは不可。
- 契約企業においては、「応募者管理ID」は特定の個人の姓名と紐づけられているので、個人を特定してスコアを活用してフォローに利用することが可能。

管理ID	スコア	内定辞退可能性
C333	0.40	★★
C444	0.53	★★★
C555	0.61	★★★

令和2年の個人関連情報に関する改正の契機となった勧告

2．2　勧告②（アンケートスキーム下のイレギュラーケース）

【勧告②】
本サービスにおける突合率を向上させるため、ハッシュ化すれば個人情報に該当しないとの誤った認識の下、サービス利用企業から提供を受けた氏名で突合し内定辞退率を算出していた。ハッシュ化されていても、リクルートキャリア社において特定の個人を識別することができ、本人の同意を得ずに内定辞退率を利用企業に提供していた。

〇アンケートスキーム下におけるイレギュラーケース

- 2019年2月以前に実施していたアンケートスキームにおいて、一部の契約企業との間で、対象学生のCookie情報を利用した特定（突合）率を向上させる目的で、アンケートスキームとは異なるスキームでスコア算出を実施するケースがあった。このイレギュラーケースにおいては、当該一部の契約企業から氏名等の個人情報の提供を受けていた。
- リクルートコミュニケーションズにおいて取扱うデータがハッシュ化されたものであれば、契約企業に提供する際も非個人情報として取扱えるという誤った認識のもと、契約企業から預かった学生の情報とリクナビ会員の情報がハッシュ化された状態で紐づけられており、これを通じて算出したスコアは、学生本人の同意なく当該契約企業に対して第三者提供されていた。

「提供元基準」では個人情報（個人データ）の第三者提供に該当する場合（法27条違反）

2．2　勧告③（プライバシーポリシースキーム（2019年３月以降））

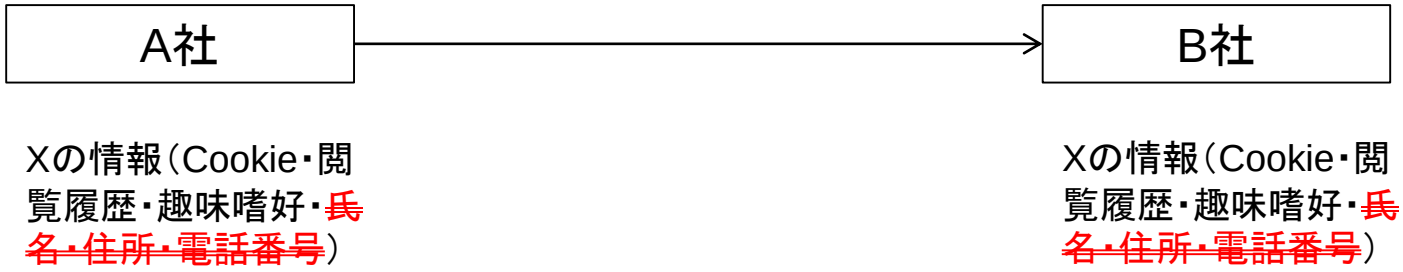
【勧告③】
「リクナビ2020」プレサイト開設時（2018年６月）に、本サービスの利用目的が同サイト内に記載されたことをもって、サービス利用企業から提供を受けた氏名で突合し内定辞退率を、算出していた。しかしながら、プレサイト開設時のプライバシーポリシーには第三者提供の同意を求める記載はなく、2019年３月のプライバシーポリシー改定までの間、本人の同意を得ないまま内定辞退率をサービス利用企業に提供していた。

〇プライバシーポリシースキーム（2019年３月以降）

- 『リクナビ2020』では、2019年3月に、プライバシーポリシーを『リクナビDMPフォロー』の提供にあたって、学生が使用する複数の画面においてプライバシーポリシーに同意をしてもらうサイト構成に変更された。この中には、契約企業への第三者提供の同意も含まれていた。
- リクルートキャリアは、契約企業の委託先企業として、契約企業より、委託業務に必要な限度で氏名などの個人情報の提供を受ける。その後、当社委託先であるリクルートコミュニケーションズにおいて、提供された個人情報とリクナビに登録された個人情報を紐づけた上で、当該学生のリクナビサイト上での「業界ごとの閲覧履歴」などからスコアを算出していた。
- 契約企業からは、学生に関する①応募者管理ID（契約企業が付与していた応募者の管理ID）、②姓名、メールアドレス、③大学、学部、学科、④選考プロセスにおける辞退・承諾情報の提供を受けていた。
- また、契約企業によって異なる「企業独自管理情報」の提供を受けていた場合もある。一例としては、①契約企業の説明会予約有無、②エントリーシートの記述内容、③契約企業が利用していた適正検査の項目の値、④応募職種が挙げられる。

本人の同意がない第三者提供（法27条違反）

2．2　提供元基準



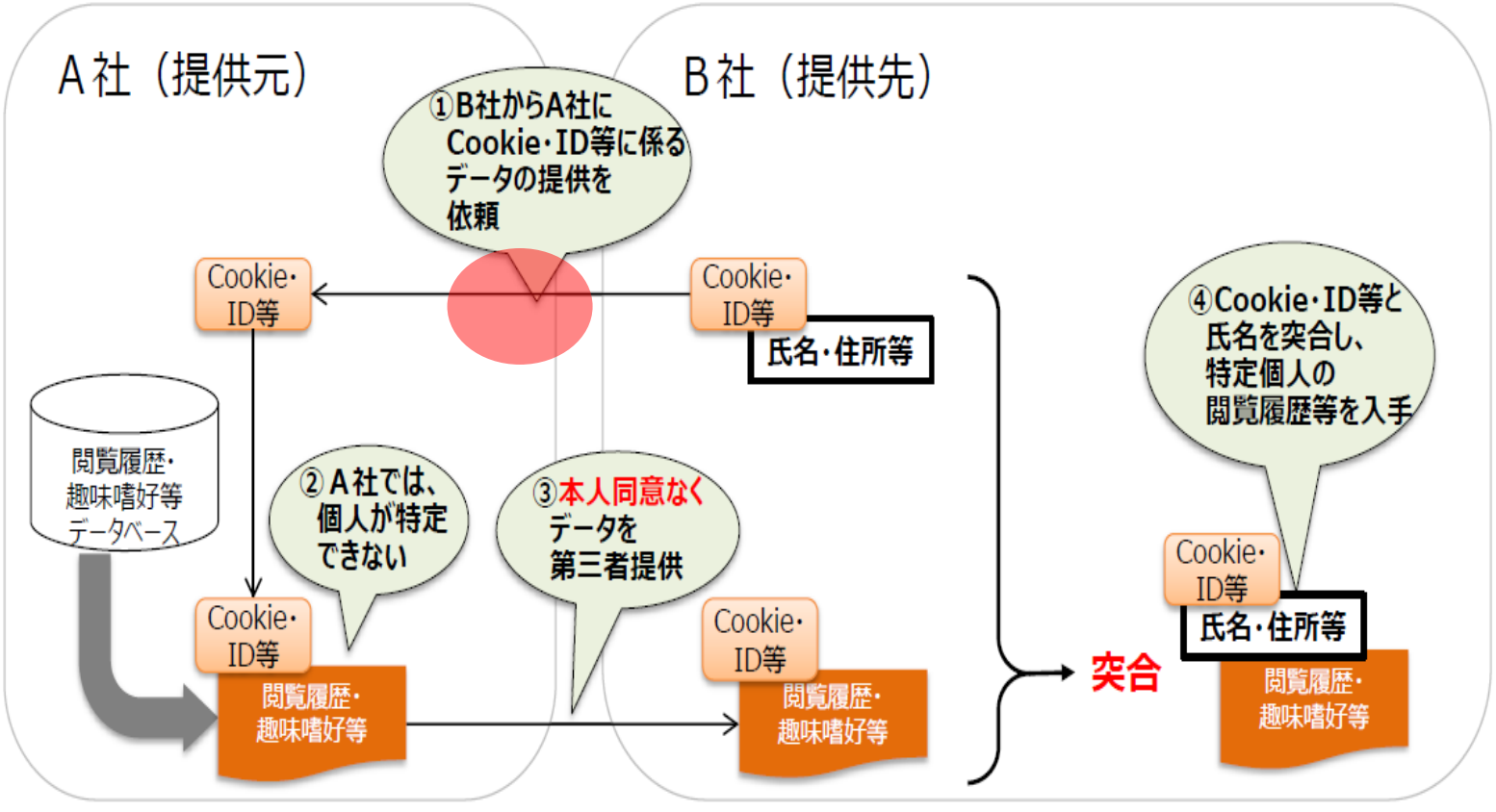
（提供元基準）：個人情報保護委員会の見解
「他の情報と容易に照合でき、それにより特定の個人を識別できる」か否かは提供元で判断する。A社（提供元）において容易に照合できる限りは、A社による情報提供は、「個人データ（個人情報）」の提供には該当し、X（本人）の事前の同意の取得が原則必要。

（提供先基準）：従前有力だった見解
「他の情報と容易に照合でき、それにより特定の個人を識別できる」か否かは提供先で判断する。B社（提供先）において容易に照合できない限りは、A社による情報提供は、「個人データ（個人情報）」の提供には該当せず、X（本人）の事前の同意の取得は不要。

2．2　本人の同意なきデータの第三者提供

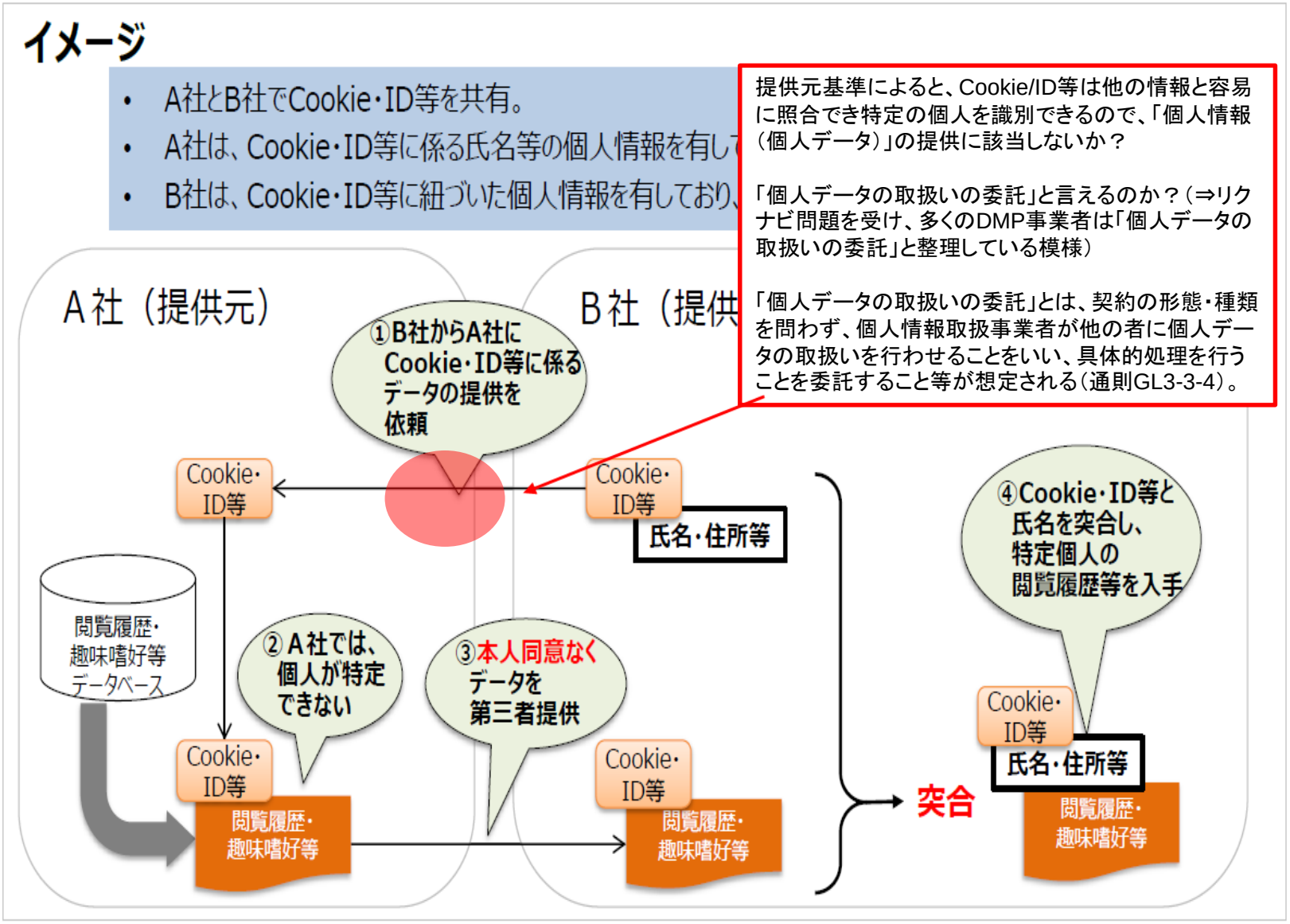
イメージ

- A社とB社でCookie・ID等を共有。
- A社は、Cookie・ID等に係る氏名等の個人情報を有していない。
- B社は、Cookie・ID等に紐づいた個人情報を有しており、A社はその事実を知っている。



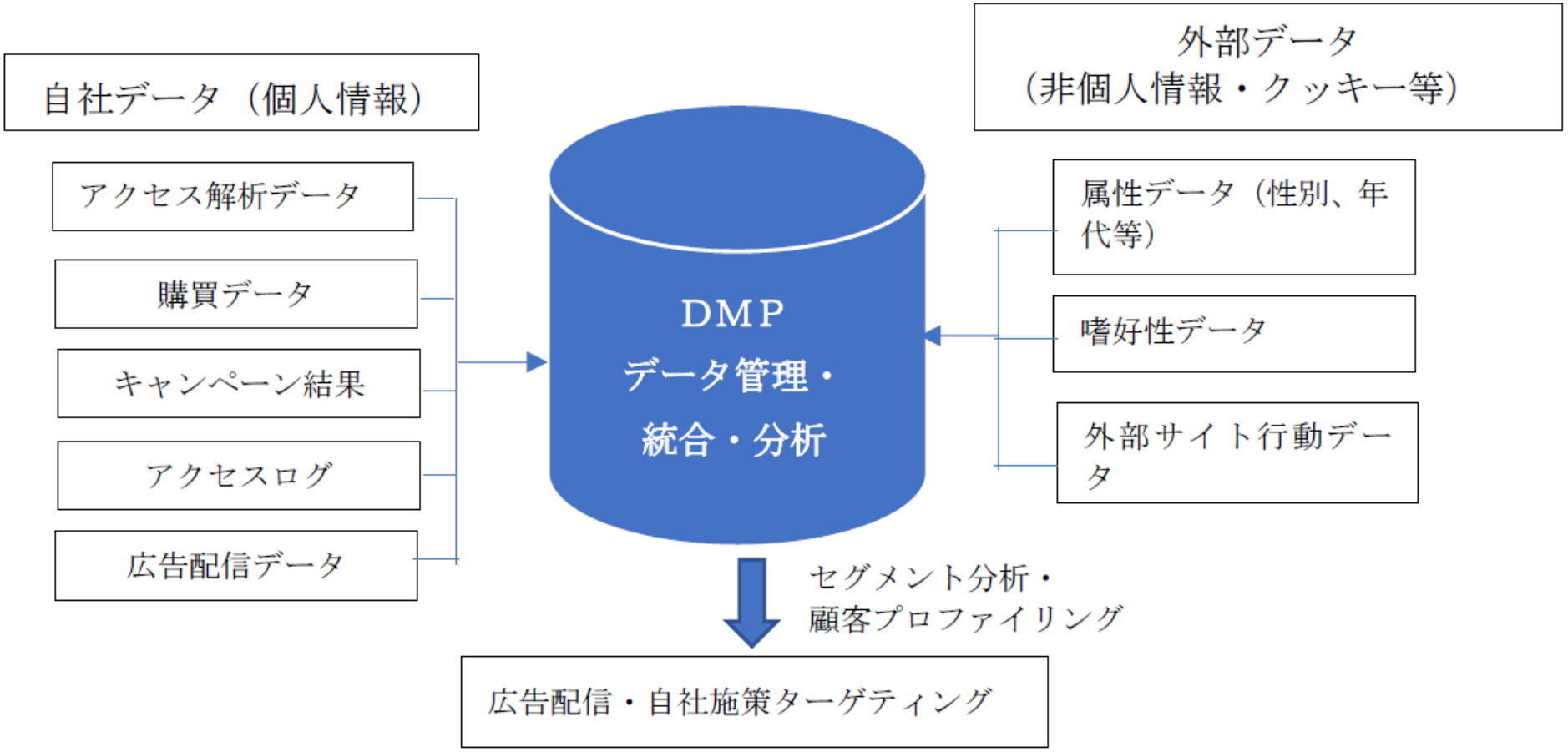
出所：個人情報保護委員会資料を修正

2．2　本人の同意なきデータの第三者提供



出所：個人情報保護委員会資料を修正

2．2　DMPについて


自社データ（個人情報）
アクセス解析データ
購買データ
キャンペーン結果
アクセスログ
広告配信データ
外部データ
（非個人情報・クッキー等）
属性データ（性別、年代等）
嗜好性データ
外部サイト行動データ
DMP
データ管理・
統合・分析
セグメント分析・
顧客プロファイリング
広告配信・自社施策ターゲティング

2．3　個人関連情報に関する定義規定

「個人関連情報」
生存する個人に関する情報であって、個人情報、仮名加工情報及び匿名加工情報のいずれにも該当しないものをいう。
⇒郵便番号、メールアドレス、性別、職業、趣味、顧客番号、Cookie情報、IPアドレス、契約者・端末固有IDなどの識別子情報および位置情報、閲覧履歴、購買履歴と言ったインターネットの利用にかかるログ情報などの個人に関する情報で特定の個人が識別できないものが該当すると考えられる。

「個人関連情報データベース等」
「個人関連情報」を含む情報の集合物であって、特定の個人関連情報を電子計算機を用いて検索することができるように体系的に構成したものその他特定の「個人関連情報」を容易に検索することができるように体系的に構成したものとして政令で定めるものをいう。
⇒具体的には、CookieやIPアドレス等の識別子情報（個人関連情報）に紐づけられた閲覧履歴や趣味嗜好のデータベースが該当すると考えられる。

「個人関連情報取扱事業者」
「個人関連情報データベース等」を事業の用に供している者で、国、地方公共団体、独立行政法人等、地方独立行政法人を除いたものをいう。
⇒具体的には、CookieやIPアドレス等の識別子情報（個人関連情報）に紐づけられた閲覧履歴や趣味嗜好のデータベース（個人関連情報データベース等）から、特定のCookieやID等の識別子に紐付けられた閲覧履歴や趣味嗜好の情報を利用企業（第三者）に提供するDMP事業者が「個人関連情報取扱事業者」に該当するものと考えられる。

2．3　個人関連情報に関する規律（第三者の責務）

①同意取得義務（法31条1項1号）

- 「**個人関連情報取扱事業者**」から「**個人関連情報**」の提供を受ける「**第三者**」は、「**個人関連情報**」（「**個人関連情報データベース等**」を構成するものに限る。）を**個人データとして取得することが想定されるとき**は、法23条1項各号に該当する場合を除いて、「**個人関連情報取扱事業者**」から「**個人関連情報**」の提供を受けて本人が識別される**個人データとして取得することを認める本人の同意を取得**する必要がある（法26条の2第1項1号）。

②確認にあたっての偽りの禁止（法31条3項の準用する法30条2項）

- 上記①の「**第三者**」は、「**個人関連情報取扱事業者**」が本人の同意を取得したことの確認を行う場合、当該「**個人関連情報取扱事業者**」に対して、当該**確認に係る事項**を**偽ってはならない。**

2．3　個人関連情報に関する規律（第三者の責務）

①同意取得義務（法31条1項1号）

- 「**個人関連情報取扱事業者**」から「**個人関連情報**」の提供を受ける「**第三者**」は、「**個人関連情報**」（「**個人関連情報データベース等**」を構成するものに限る。）を個人データとして取得することが想定されるときは、法23条1項各号に該当する場合を除いて、「**個人関連情報取扱事業者**」から「**個人関連情報**」の提供を受けて本人が識別される個人データとして取得することを認める本人の同意を取得する必要がある（法26条の2第1項1号）。

②確認にあたっての偽りの禁止（法31条3項の準用する法30条2項）

- 上記①の「**第三者**」は、「**個人関連情報取扱事業者**」が本人の同意を取得したことの確認を行う場合、当該「**個人関連情報取扱事業者**」に対して、当該**確認に係る事項**を**偽ってはならない。**

2．3　個人関連情報取扱事業者の義務

①確認義務（法31条１項１号）

- **「個人関連情報取扱事業者」**は、**「第三者」**が**「個人関連情報」（「個人関連情報データベース等」を構成するものに限る。）を個人データとして取得することが想定されるとき**は、法27条１項各号に該当する場合を除いて、当該**「第三者」**が**「個人関連情報取扱事業者」から「個人関連情報」の提供を受けて本人が識別される個人データとして取得することを認める本人の同意**を得ていることを**確認**する必要がある。

②記録の作成・保存義務（法31条３項、法30条３項・４項）

- **「個人関連情報取扱事業者」**は、上記①の確認を行ったときは、個人情報保護委員会規則で定めるところにより、当該個人関連情報を提供した年月日、当該確認に係る事項その他の個人情報保護委員会規則で定める事項に関する**記録を作成**しなければならない（法31条３項、法30条３項）。
- また、**「個人関連情報取扱事業者」**は、当該記録を、当該記録を作成した日から**個人情報保護委員会規則で定める期間保存**しなければならない（法31条４項、法30条４項）。

2．3　本人の同意の取得方法（通則編ガイドライン）

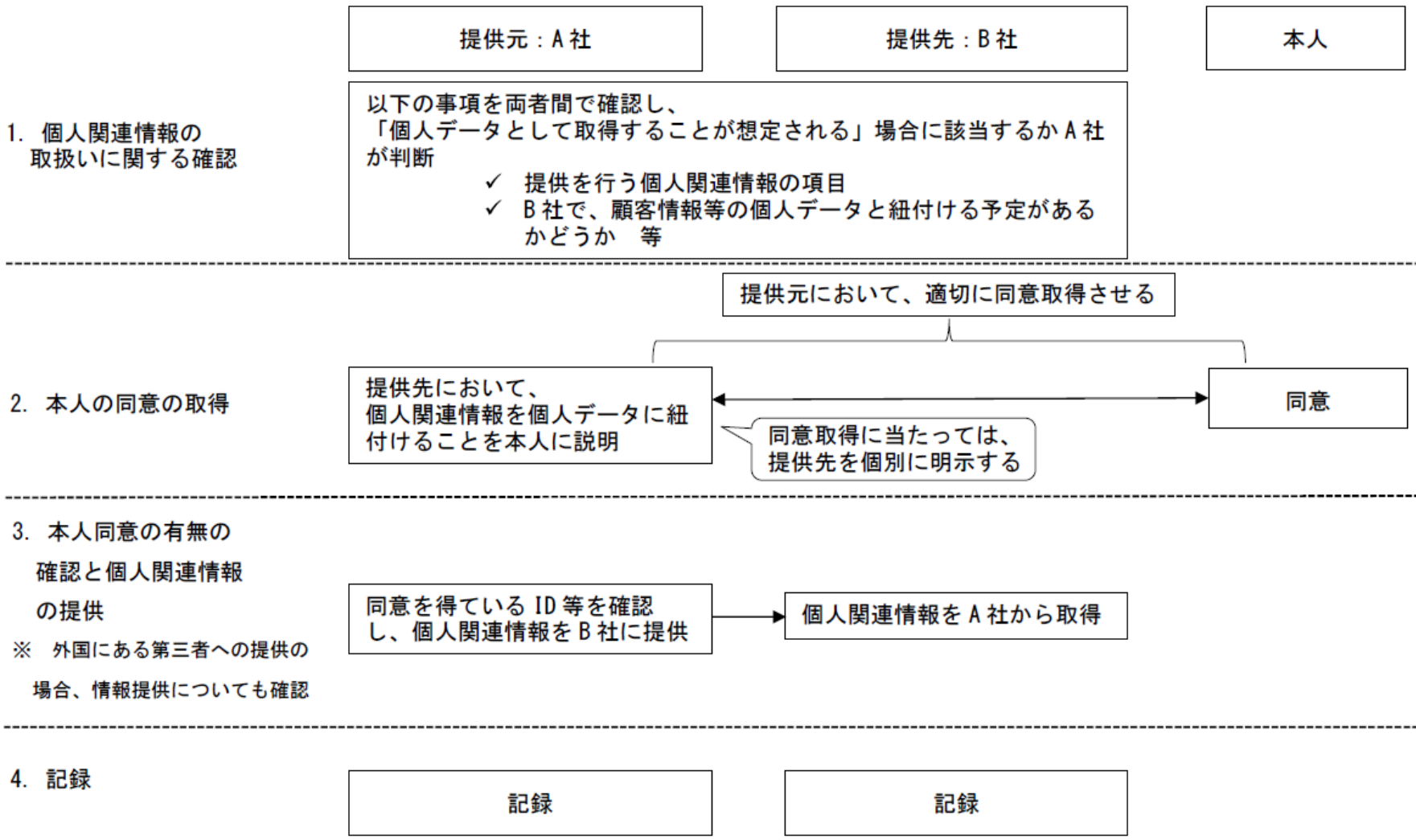
1．同意を取得する主体

- 法31条1項第1号の「本人の同意」を取得する主体は、本人と接点を持ち、情報を利用する主体となる提供先の第三者であるが、同等の本人の権利利益の保護が図られることを前提に、同意取得を提供元の個人関連情報取扱事業者が代行することも認められる。

2．同意取得の方法

- 同意取得の方法としては、様々な方法があるが、例えば、本人から同意する旨を示した書面や電子メールを受領する方法、確認欄へのチェックを求める方法がある。ウェブサイト上で同意を取得する場合は、単にウェブサイト上に本人に示すべき事項を記載するのみでは足りず、それらの事項を示した上でウェブサイト上のボタンのクリックを求める方法等によらなければならない。
- 同意取得に際しては、本人に必要な情報を分かりやすく示すことが重要であり、例えば、図を用いるなどして工夫することが考えられる。

2．3　個人関連情報の第三者提供につき、提供元で同意取得を代行する場合の一般的なフロー



出所：通則編ガイドライン

2．3　他社のタグの設置

（法第 31 条の適用の有無について）
Q8－10 A 社が自社のウェブサイトに B 社のタグを設置し、B 社が当該タグを通じて A社ウェブサイトを閲覧したユーザーの閲覧履歴を取得している場合、A 社は B 社にユーザーの閲覧履歴を提供したことになりますか。

A8－10 個別の事案ごとに判断することとなりますが、A 社が B 社のタグにより収集される閲覧履歴を取り扱っていないのであれば、A 社が B 社に閲覧履歴を「提供」したことにはならず、B 社が直接にユーザーから閲覧履歴を取得したこととなると考えられます。このため、B 社がそのタグを通じて閲覧履歴を取得することについて、法第 31 条第１項は適用されないと考えられます。なお、個人情報取扱事業者である B 社は、閲覧履歴を個人情報として取得する場合には、偽りその他不正の手段によりこれを取得してはならず（法第 20 条第１項）、また、個人情報の利用目的を通知又は公表する必要があります（法第 21 条第１項）。

2．4　外部送信規律の適用

●電気通信事業者・第三号事業者（内容、利用者の範囲及び利用状況を勘案して利用者の利益に及ぼす影響が少なくないものとして総務省令で定める電気通信役務を提供する者に限る。）に外部送信規律が適用される。

- 電気通信事業者の場合は、登録・届出が前提となる（電気通信事業法2条4項）ため、迷うことは少ない（既に登録・届出しているから）。

●第三号事業（電気通信事業法164条1項3号）とは？

- 電気通信設備を用いて他人の通信を媒介する電気通信役務以外の電気通信役務（一定の役務を除く）を電気通信回線設備を設置することなく提供する電気通信事業をいう。

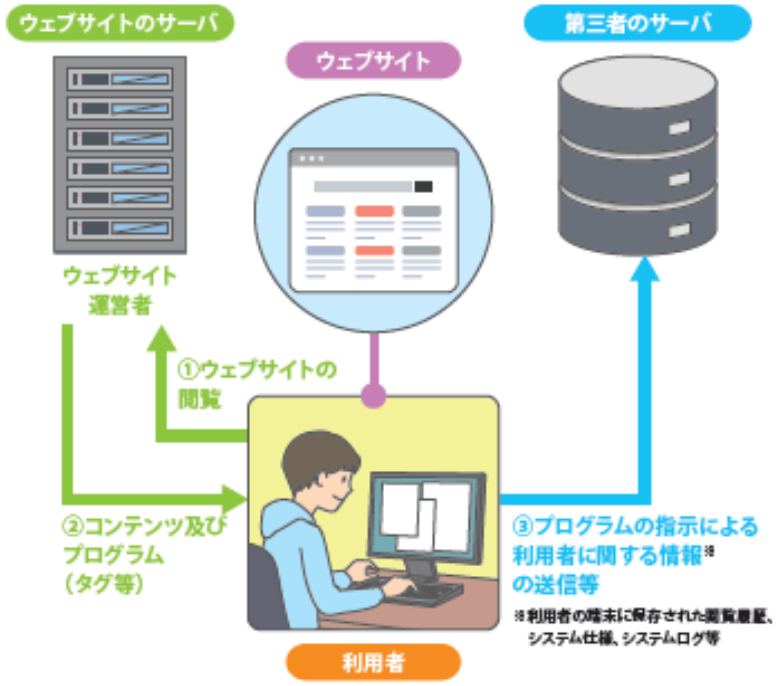
⇒通信媒介すら行わないものを含むため、インターネットを経由する事業はだいたいこれに含まれるように思われる。

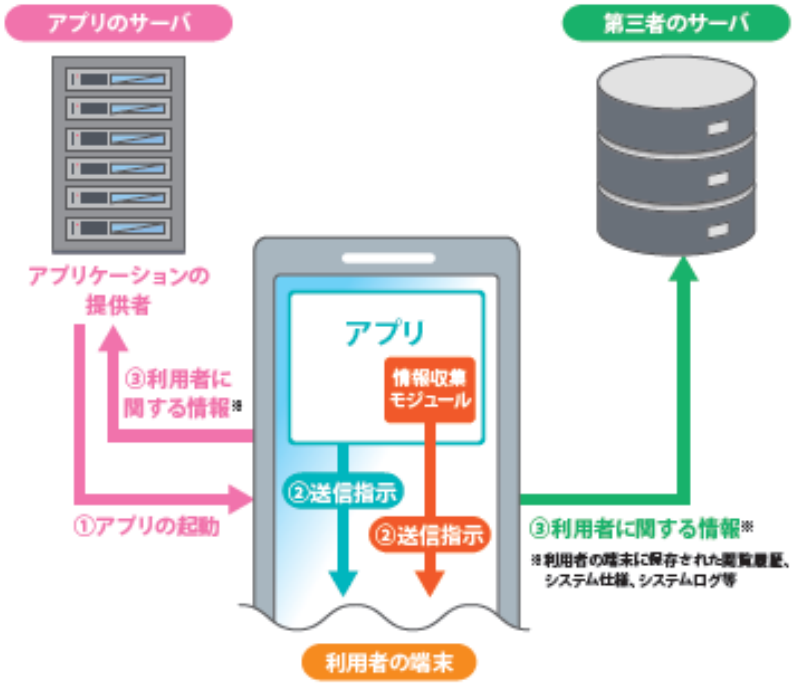
2．4　外部送信規律の概要

- 利用者のパソコンやスマートフォン等の端末で起動されるブラウザやアプリケーションを通じて電気通信役務を提供する事業者が、利用者の端末に対して、当該端末に記録された利用者に関する情報を外部に送信するよう指令するプログラム等を送信するがある。
- 外部送信規律は、このような場合において、電気通信役務を提供する事業者（電気通信事業者・第三号事業者）に対し、当該プログラム等により送信されることとなる利用者に関する情報の内容や送信先について、当該利用者に確認の機会を付与する義務を課すもの。
- 確認の機会の付与の方法としては、①通知、②利用者が容易に知り得る状態に置く（いわゆる公表）、③同意取得又は④オプトアウト措置の提供のいずれかを行う必要がある。
- ただし、利用者の端末に適正な画面表示をするためなど、当該電気通信役務の利用のために送信することが必要な情報や、当該電気通信役務を提供する事業者が利用者を識別するために自身に送信させる識別符号（いわゆる1st Party Cookieに保存されたID）の外部送信については、確認の機会の付与は不要。

2．4　外部送信規律のイメージ

電気通信事業を営む者（ウェブサイト運営者、アプリケーション提供者等）は、利用者の端末に外部送信を指示するプログラムを送る際は、あらかじめ、送信される利用者に関する情報の内容等を、通知・公表（利用者が容易に知り得る状態に置く）等しなければなりません。





出所：「外部送信規律について」（総務省総合通信基盤局）

２．４　外部送信規律の導入の背景

- Webサイトや、スマートフォン等のアプリ等を閲覧・利用する際に、Webサイトに埋め込まれたタグや、アプリに組み込まれている情報収集モジュールといったプログラムが利用者の端末に送信され、その結果、利用者が認識しないまま、当該端末に記録された利用者に関する情報が、当該利用者以外の者に送信される状況が生じている。
- 送信される利用者に関する情報は、Cookieや広告ID等の識別子、閲覧履歴・行動履歴など幅広く、様々な用途に用いられる可能性がある。
- 利用者が認識しないままにこのような情報の外部送信が行われていると、利用者が安心して電気通信サービスを利用することができず、ひいては、電気通信サービスの信頼性が損なわれ、電気通信サービスの健全な発達に支障を及ぼすおそれがある。
- このようなことを踏まえ、電気通信事業法を改正し、利用者が安心して電気通信サービスを利用することができるように、このような情報の外部送信について、利用者に確認の機会を付与することを義務付けたもの。（2023年６月16日施行）

2．4　外部送信規律の適用対象事業者

●電気通信事業者又は第三号事業を営む者（いずれも電気通信事業を営む者）で、「利用者の利益に及ぼす影響が少なくない電気通信役務」を提供している電気通信事業者。

●「利用者の利益に及ぼす影響が少なくない電気通信役務」（法27条の12柱書）とは、以下のいずれかの電子通信役務のうち、ブラウザやアプリを通じて提供されているもの（規則22条の２の27）

①利用者間のメッセージ媒介等（同条１号）

②SNS、電子掲示版、動画共有サービス、オンラインショッピングモール等（同条２号）

③オンライン検索サービス（同条３号）

④ニュース配信、気象情報配信、動画配信、地図等の各種情報のオンライン提供（同条４号）

●「電気通信事業（法２条４号）」を営んでいない場合は、法の適用を受けないので、仮に情報の外部送信が行われていたとしても、外部送信規律の対象にはならない。

2．4　利用者の利益に及ぼす影響が少なくない電気通信役務（規則22条の2の27）

1. 他人の通信を媒介する電気通信役務
2. その記録媒体に情報を記録し、又はその送信装置に情報を入力する電気通信を利用者から受信し、これにより当該記録媒体に記録され、又は当該送信装置に入力された情報を不特定の利用者の求めに応じて送信する機能を有する電気通信設備を他人の通信の用に供する電気通信役務

例）SNS、電子掲示版、動画共有サービス、オンラインショッピングモール等

3. 入力された検索情報（検索により求める情報をいう。…）に対応して、当該検索情報が記録された全てのウェブページ（通常の方法により閲覧ができるものに限る。…）のドメイン名その他の所在に関する情報を出力する機能を有する電気通信設備を他人の通信の用に供する電気通信役務

例）オンライン検索サービス

4. 前号に掲げるもののほか、不特定の利用者の求めに応じて情報を送信する機能を有する電気通信設備を他人の通信の用に供する電気通信役務であつて、不特定の利用者による情報の閲覧に供することを目的とするもの

例）ニュース配信、気象情報配信、動画配信、地図等の各種情報のオンライン提供

➢一応例示はあるものの、極めて広汎にわたり得る定義であるために、その外縁は不明確であるといわざるを得ない。

外縁につきどのような議論がされているか？

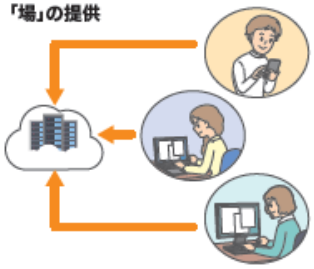
2．4　外部送信規律の適用対象事業者

1.メッセージ媒介サービス

メッセージングアプリなど、特定の利用者間のメッセージ交換をテキスト、音声、画像、動画によって媒介するもの。

ビジネスマッチングサイトやオンラインゲームなど、サービスの一部として特定の利用者間でのダイレクトメッセージ機能を提供している場合も含む。

2.SNS



不特定多数の利用者間での、テキスト、音声、画像、動画の投稿・閲覧機能により発信者と閲覧者がやりとりを行う「場」を提供するもの。

3.検索サービス

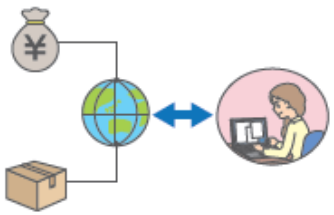
広範なWebサイトのデータベースを構築し、検索語を含むWebサイトのURL等を、利用者に提供するもの。

4.ホームページの運営
［ニュースサイト、まとめサイト等各種情報のオンライン提供］

インターネット経由で天気予報やニュース、映像などの情報を利用者へ提供するもの。

ただし、以下の場合は、電気通信事業に該当しないため、
対象にはなりません

4.ホームページの運営
［自社商品等のオンライン販売］



小売業者の提供するオンラインショッピングや、銀行・証券会社が提供するネットバンキング（ネット専業を含む。）など、インターネット経由で顧客からの要求・注文に対応するもの。

4.ホームページの運営
［企業等のホームページ運営・個人ブログ］

企業・個人等が自己の情報発信のため（自己の需要のため）に運営しているもの。

出所：「外部送信規律について」（総務省総合通信基盤局）

2．4　外部送信規律フローチャート

このフローチャートは、事業者が「各種情報のオンライン提供サービス等」を提供している場合に、そのサービスが外部送信規律の適用対象役務となるかを表しています。「各種情報のオンライン提供サービス等」以外にも、P7～P8の1.2.3をはじめとして、外部送信規律の適用対象役務となる場合がありますが、そのような場合については、このフローチャートは対象にしていません。

1 ブラウザやアプリケーションを通じて、各種情報のオンライン提供サービス等（以下「当該サービス」という。）を行っているか

［例］ニュースや気象情報等の配信を行うウェブサイトやアプリケーション、動画配信サービス、オンライン地図サービス等の場合は、YESです。

NO

YES（外部送信規律の適用対象役務に該当する可能性あり）

2 当該サービスを、自己（サービス提供者自身）の情報発信のために提供しているか

［例］企業・個人・自治会等のホームページについて、自己の情報発信のために運営している場合は、YESです。

YES
（自己の需要のために提供するものであるため、電気通信事業法の適用対象外）

NO（自己の需要のために提供するものではない）

3 当該サービスを、電気通信役務を前提としない、別の自らの本来業務の遂行手段として活用しているか

［例］金融事業者による証券・金融商品等についてのオンライン販売、小売事業者によるモノ・商品についてのオンライン販売、メーカーによる製造した商品についてのオンライン販売など、別の自らの本来業務（電気通信役務を前提としないもの）の遂行手段としてオンラインを活用している場合は、YESです。ただし、別の自らの本来業務（電気通信役務を前提としないもの）と関連していたとしても、当該本来業務とは独立して当該サービスを行っている場合はNOの場合があります。

YES
（自己の需要のために提供するものであるため、電気通信事業法の適用対象外）

NO（自己の需要のために提供するものではない）

4 当該サービスを行うことで、利益を得ようとしているか（実際に利益が出ていない場合も含む。）

［例］個人事業主として利益を上げる目的で、広告やアフィリエイトプログラムなどを利用した各種情報提供サイト等を運営している場合は、YESです。

NO
（電気通信事業を「営む」に該当しないため、電気通信事業法の適用対象外）

YES（電気通信事業を「営む」に該当）

外部送信規律の対象

外部送信規律の対象外

出所：「外部送信規律について」（総務省総合通信基盤局）

2．4　クッキーポリシー作成

●クッキーポリシーの法的記載事項
- ➢送信されることとなる利用者に関する情報の内容
- ➢当該情報を取り扱うこととなる者の氏名又は名称
- ➢当該情報の電気通信事業者における利用目的
- ➢当該情報の送信先における利用目的

●クッキーポリシーの任意的記載事項（ガイドライン解説）
- ➢ オプトアウト措置の有無
- ➢ 送信される情報の送信先における保存期間
- ➢ 電気通信事業者における問合せ先
- ➢ どの国・地域に送信されることになるか　等

2．4　通知・容易に知り得る状態の留意点

●**通知・容易に知り得る状態に置く場合の共通事項**

① **日本語**を用い、**専門用語を避け**、及び**平易な表現**を用いること。

② 操作を行うことなく**文字が適切な大きさ**で利用者の電気通信設備の映像面に表示されるようにすること。（**画面の拡大・縮小等の追加的な操作を行うことなく文字が適切な大きさで表示**）

③ ①・②のほか、利用者が通知等すべき事項について容易に確認できるようにすること。（**視認性の高い文字色・量が多い場合はウェブページの階層化**）

● **通知の場合**

① 通知等すべき事項又は当該事項を掲載した画面の所在に関する情報を当該利用者の電気通信設備の映像面に即時に表示すること（当該事項の一部のみを表示する場合には、利用者がその残部を掲載した画面に容易に到達できるようにすること。）（**ウェブサイトやアプリケーションの画面上で、ポップアップ形式によって即時通知を行うこと**等）

② ①と同等以上に利用者が容易に認識できること。

●**容易に知り得る状態に置く場合（ウェブサイト・アプリ）**

① **情報送信指令通信を行うウェブページ**又は**当該ウェブページから容易に到達できるウェブページ**において、通知等すべき事項を表示すること（**ウェブサイトの場合：1回程度の操作で到達できる遷移先のウェブページ**）

② 情報送信指令通信を行うソフトウェアを利用する際に、利用者の電気通信設備の映像面に**最初に表示される画面**又は**当該画面から容易に到達できる画面**において、通知等すべき事項を表示すること（**アプリを利用する場合**）

③ ①・②と同等以上に利用者が容易に到達できること

2．５　SNSの「ボタン」等の設置に係る留意事項（個人情報保護委員会）

https://www.ppc.go.jp/news/careful_information/sns_button/
一部のソーシャルネットワーキングサービス（SNS）は、ログインした状態で、当該SNSの「ボタン」等が設置されたウェブサイトを閲覧した場合、当該「ボタン」等を押さなくとも、当該ウェブサイトからSNSに対し、ユーザーID・アクセスしているサイト等の情報（※）が自動で送信されていることがあります。
SNSがユーザーID等を他の情報と紐づけて個人情報として管理している場合、当該ユーザーIDは個人情報となります。

このため、サイト運営者においては、SNSの「ボタン」等の設置を検討する際には、各SNSのプライバシーポリシー等を十分確認し、実態を正確に把握したうえで判断する必要があります。
また、サイト運営者は、SNSに情報送信されるような「ボタン」等をウェブサイトに設置する場合には、ボタン等を押さなくとも閲覧しただけで当該SNSに情報が送信されることがあることを一般の利用者が十分に認識するよう、当該SNSに情報が送信されていること及び送信されている情報の範囲等をプライバシーポリシー等においてわかりやすく明示する等、丁寧にご対応ください。

2．6　いわゆる3年ごと見直し：個人関連情報への不適正取得・不適正利用の規律の適用

改正の方向性：個人関連情報への不適正取得・不適正利用の規律の適用（実現可能性：80%）

- 「個情委の考え方」においては、「個人関連情報については、事業者が、電話番号、メールアドレス、Cookie IDなど、個人に対する連絡が可能な情報を有している場合には、個人関連情報の取扱いによりプライバシーなどの個人の権利利益が侵害される蓋然性が認められ、その侵害の程度・蓋然性は、事業者による利用の方法によっては、個人情報と同様に深刻なものになり得る」として、プライバシーなど個人の権利利益の侵害の蓋然性のある一定の個人関連情報について、不正取得・不適正利用等への規制を改正により追加することが検討されている。
- データの利活用の推進の観点から、広告配信業者などの一部の事業者の反対は予測できるが、プライバシー保護の観点から、個人関連情報のうち、「電話番号、メールアドレス、Cookie IDなど、個人に対する連絡可能な情報を有している場合」には、個人情報と同様に、不適正取得・不適正利用の規律が新たに設けられる可能性は大きいと思われる。

2．6　いわゆる3年ごと見直し:「個人関連情報」を「個人情報」として扱うこと

改正の方向性:「個人関連情報」を「個人情報」として扱うこと（30%）

- 中間整理の「個情委の考え方」には記載されていないものの、関係団体の意見が激しく対立しているのが、「個人関連情報」を「個人情報」として扱うことである。
- 全国消費者団体連絡会は、『「個人関連情報」である、電話番号、メールアドレス、Cookie ID などについて、それぞれが単体のレベルでも「個人情報」として扱うべき』としている。その理由は、『個人関連情報である、電話番号、メールアドレス、Cookie ID などの漏えいや意図的な抜き取りにより、電話やメールで悪質な勧誘が多様に行われている実態がある。悪質な勧誘が個人の権利利益の侵害につながる事案も多いことから、個人情報の概念を拡大して、取り扱い方を厳しくして、被害抑止につなげることが出来ると考える。』としている。
- 全国消費生活相談員協会も、『いわゆる個人関連情報は個人情報であると整理するべき。現状では、事業者が個人関連情報を取得し、それによって本人へのアクセスが可能になり、個人がさまざまな被害にあうケースが増加している。またスマートフォンのアプリ等を通じて、端末識別符号や利用状況などの情報を、本人が知らない内に密かに収集するなどの行為も見受けられる。個人関連情報を個人情報と整理することが不正行為の抑止にもっとも効果的であると思われまる。欧州等では電話番号、メールアドレス、cookie 等は単体で個人情報とされていますが、そのことによる問題は聞いていない。』と同様の見解を述べている。
- これに対して、日本IT団体連盟は、『連絡可能という理由で個人関連情報に対して個人情報と同様の規制をすることには強く反対』とする。
- 中間整理の「個情委の考え方」では、①「個人関連情報」にも「不適正利用」「不適正取得」の規律を適用するレベルで検討されており、消費者団体側の主張する消費者被害の問題にも一定の対応が可能であること、また、②「個人関連情報」を「個人情報」として取り扱う場合には重大な実務上の影響があり得ることに鑑みると、「個人関連情報」を「個人情報」として扱うという改正までは実現する可能性は低いものと考えられる。

2.7 EUによるCookie関連規制①

■ EUにおけるCookie関連規制としては、GDPR（EU一般データ保護規則）のほか、ePrivacy指令（Directive on privacy and electronic communications（通称、e-Privacy Directive））がある。

■ ePrivacy指令
- ✓ 契約者または利用者の端末装置に蓄積された情報を保管し、また、それらの情報にアクセスするためには、原則として、当該契約者または利用者が明確かつ包括的な情報を提供された上で、同意をした場合に限り、許容されると定められている（ ePrivacy指令５条３項）。
- ✓ ここでいう「同意」はGDPRにおける「同意」と同義とされている（ePrivacy指令２条（f）号）。
- ✓ 例えば、ウェブサイトの運営者がウェブサイトの訪問者のパソコンにターゲティング目的でCookieやその類似技術を設置する場合、原則として同意を得ることが求められる。

■ GDPR
- ✓ GDPRによる「個人データ」とは、識別された又は識別され得る個人（「データ主体」）に関するあらゆる情報を意味する。識別され得る個人は、特に、氏名、識別番号、位置データ、オンライン識別子のような識別子、又は当該個人に関する物理的、生理的、遺伝子的、精神的、経済的、文化的若しくは社会的アイデンティティに特有な一つ若しくは複数の要素を参照することによって、直接的に又は間接的に、識別され得るものをいう（GDPR４条１項）と定義されている。
- ✓ したがって、CookieやIPアドレスなどのオンライン識別子、位置データなども個人データに該当すると考えられている。
- ✓ 例えば、Cookieによって情報収集するウェブサイトの運営者は、そのCookie情報の処理の適法化根拠を確保しなければならないこと（GDPR6条1項）、データ主体に情報提供しなければならないこと（同13条）および国際移転ルールを遵守しなければいけないこと（同44～49条）等の義務を負うことになる。

2.7 EUによるCookie関連規制②

■ ePrivacy指令とGDPRの適用関係
- ✓ ePrivacyは、GDPRと同様の事項を対象にしているルールについては、GDPRに優先される（ ePrivacy指令1条2項及び前文10項、GDPR95条および前文173項）。
- ✓ ePrivacy指令がGDPRのルールについてより具体的な規定が定められている場合、その規定は特別法としてGDPRに優先する一方で、そのような規定が定められていない場合は、GDPRが優先される。
- ✓ 例えば、Cookieの端末への保存や保存されたアクセスに係る同意については、ePrivacy指令の規制が優先されるものの、取得後に行われる個人データの処理については、GDPRが適用される。

■ ePrivacy規則案（2017年1月10日に欧州委員会により公表。未だ施行されず）
- ✓ ePrivacy指令と異なり、GDPRと同様、EU各国で直接適用が予定されている。
- ✓ 同規則案の「電子通信データ」（4条3項（a））に含まれる「電子通信メタデータ」（4条3項(c)）に、Cookieが該当する。
- ✓ 「電子通信データ」を処理できる場合は限定されている（6条）。電子通信サービスのプロバイダは、通信の達成に必要な場合等を除き（6条1項、2項）、以下の場合に限り、電子通信コンテンツを処理することができる（6条3項(a)(b)）。
  - エンドユーザーに特定のサービスを提供することのみを目的とし、関係するエンドユーザーまたはエンドユーザーが自分の電子通信コンテンツの処理およびそのサービスの提供に同意した場合（そのようなコンテンツの処理なしには成し遂げられない場合に限る。）。
  - 関連する全てのエンドユーザーが、匿名化された情報を処理することによっては満たすことができない1以上の特定の目的のために電子通信コンテンツの処理に同意した場合。
- ✓ 第6条(1)(b)および第6条(3)(a)(b) の場合を除き、電子通信サービスの提供者は、電子通信コンテンツを消去するか、または意図された1人または複数の受信者による電子通信コンテンツの受信後にそのデータを匿名化しなければならない。（7条）

2.7 EUによるCookie関連規制③

■ ePrivacy指令における「同意」

- EUのePrivacy指令（Directive on privacy and electronic communications（通称、e-Privacy Directive））5条3項においては、ユーザーの端末装置に蓄積された情報を保管し、また、それらの情報にアクセスするためには、クッキーの利用目的を分かりやすく説明した上で同意を取得すること（インフォームド・コンセント）が必要。すなわち、ウェブサイトにおいて、ほとんど全てのCookieや類似の技術（例えば、Webビーコンや Flash Cookieなど）を使用する前にユーザーの同意を取得することが必要。
- 同意が有効であるためには、それは通知され、具体的で自由に与えられなければならず、個人の真の意思を反映するものでなければならない。（GDPRと同様）
- ただし、①コミュニケーションの伝達を行う唯一の目的のために使用され、通信の伝達を目的とする場合（通信の例外）、②ユーザーが明示的に必要とする情報社会サービスの提供者がそのサービスを提供するために絶対に必要な場合（絶対的な必要性の例外）には、Cookieについての同意が免除。

【同意が明確に免除されるCookie】（29条委員会）

- オンラインフォーム、ショッピングカートなどの記入時にユーザーの入力を追跡するファーストパーティのクッキーなどのユーザー入力クッキー（セッションID）、セッションの持続時間または場合によっては数時間に制限される永続Cookie
- ユーザーを識別する認証Cookie
- 認証濫用の検出に使用されるユーザー中心のセキュリティCookie
- セッション中のマルチメディアコンテンツプレーヤーのCookie
- セッションの間、Cookieのロードバランシング
- セッションの期間（またはわずかに長い）の間、言語や設定などのユーザーインターフェイスカスタマイズのCookie
- ソーシャルネットワークのログインしたメンバーのための第三者のソーシャルプラグインコンテンツ共有Cookie

2.7　ePrivacy指令に基づくCookieについての同意の具体例

Cookieについての同意に関しては、①インフォームド・コンセントを必要とするCookieを使用してウェブサイトの全てのページにCookieヘッダーバナーを掲載し、②Cookie通知のページへのウェブリンクにアクセスできるようにし、③Cookieを使用しているページについて、ユーザーが同意した場合のみコンテンツを表示できるようにすることが考えられる。

Cookies
This site uses cookies to offer you a better browsing experience. Find out more on how we use cookies and how you can change your settings.
I accept cookies
I refuse cookies

Cookie
このサイトでは、ブラウジングの経験を向上させるためにCookieを使用しています。Cookieの使用方法と設定の変更方法の詳細については、こちらをご覧ください。
私はCookieを受け取る
私はCookieを拒否する

2.8 CCPAによるCookie関連規制①

- アメリカ合衆国カリフォルニア州において、包括的なプライバシー法であるCCPA（California Consumer Privacy Act（カリフォルニア州プライバシー権法））が施行されている。
- Cookieやモバイル広告識別子等で収集されるデータは、CCPAにおける個人情報に該当する。

- CCPAに対応するためのポイント

1. Notice at Collectionの設置

✓ CCPA準拠の「Notice at Collection」をウェブサイト上に掲載する必要あり。

✓ 「Notice at Collection」への記載事項は、収集情報の種類、利用目的、個人情報保持期間、個人情報の第三者への「販売」または「共有」の有無、個人情報を第三者に「販売」（※1）または「共有」（※2）するか否か、オプトアウトページへのリンク（リンク名「Do Not Sell or Share My Personal Information」）、プライバシーポリシーへのリンク。

（※1）第三者に金銭又はその他の価値のある対価のために、事業者が他の事業者又は第三者に対して、消費者の個人情報を、販売し、賃貸し、公表し、開示し、広め、利用可能にさせ、移転し、又は、その他口頭で、書面で、電子的若しくはその他の方法により伝えること

（※2）金銭や「価値ある対価」と引き換えであるか否かに関わらず、サイトやアプリをまたいで収集された個人情報に基づく行動ターゲティング広告を行うために、第三者に個人情報の開示を行うこと

2. オプトアウト機会の提供

✓ クッキーバナーを利用してオプトアウト機会を提供する場合の留意すべき実装のポイント

i. プライバシーノーティスとして表示する第1層のクッキーバナーにおいて、「Do Not Sell or Share My Personal Information」というタイトルのリンクを設置する。

ii. 「Do Not Sell or Share My Personal Information」リンクがクリックされた場合には、第2層のクッキーバナーを表示し、消費者のオプトアウト権についての説明を記載すると共に、実際にオプトアウトの操作を可能とするインターフェースを用意する。

2.8 CCPAによるCookie関連規制②

i. ウェブサイトのホームページ（トップページ）のヘッダー、またはフッターにも、「Do Not Sell or Share My Personal Information」というタイトルのリンクを設置し、当該リンクから第2層バナーを呼びだして、いつでもオプトアウトを可能とする
ii. 消費者からのオプトアウト要求に対して、特定の利用目的についてのみ、オプトアウトする選択肢を提示することも可能。しかし、その場合は他の目的も含めたすべての目的について一括オプトアウトする機会も同時に提供することが条件となる。そのため、クッキーバナーにおいて、クッキーの利用目的ごとのオプトアウトボタン（トグルスイッチ）のみになっている場合は、一括オプトアウトボタンの設置を行う。

3. <u>Opt-Out Preference Signalsへの対応</u>

✓ 「 Opt-Out Preference Signals 」とは、ユーザーが事業者全般に対し、個人情報の「販売」や「共有」からオプトアウトを一括して選択できるように講じられたオンライン信号をいう。
✓ 「Opt-Out Preference Signals」をユーザーの有効なオプトアウトの要求として扱わなければならない
✓ 「Opt-Out Preference Signals」によるオプトアウト要求と「消費者と特定事業者間でのプライバシー設定」が矛盾する場合、当該Signalsを有効な要求として処理する必要がある
✓ 「Opt-Out Preference Signals」を受けた際、ユーザーがアカウントログインをしている等で事業者にとってユーザー本人が特定できている場合、要求を送信したブラウザから取得する個人情報だけではなく、そのユーザーアカウントに紐づく個人情報、例えばオフラインでの購買履歴等にもオプトアウトを適用しなければならない

4. <u>再同意を求めるまでの期間</u>

✓ 一度オプトアウトをしたユーザーに再度同意を求める場合、オプトアウトされた時点から最低12か月は待たなければならない

2.8 CCPAによるCookie関連規制③

5. ダークパターンの回避

✓ ダークパターンとは、特定の選択を促したり強制したりするような事業者の作為的な操作手順をいう。

✓ 例えば、

- ユーザーが「Do Not Sell or Share My Personal Information」のリンクを選択した際、すぐにオプトアウトの権利を行使できない場合（例えば、リンク先が複数ページにわたるプライバシーポリシーの冒頭であり、オプトアウトの権利行使をプライバシーポリシーの中に隠してあるような場合）
- ユーザーがクッキーバナーを利用してCookie制限をする場合、Cookieを「全て受け入れる」と「その他オプション」という選択肢のみにし、プライバシー保護度の低い選択肢と比較し、プライバシー保護度の高い選択肢の選択には複雑な操作が必要な場合
- ユーザーにわかりづらい選択トグルの表示がなされている場合

などが挙げられる。