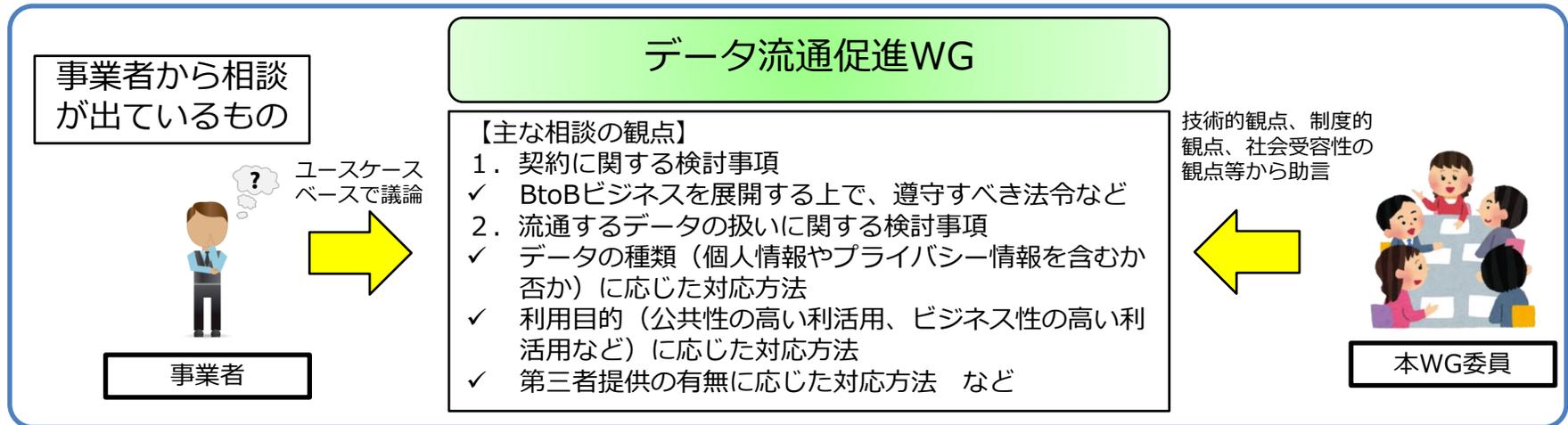


**「新たなデータ流通取引に関する  
検討事例集」  
第1分冊改訂版概要**

2022年3月  
総務省・経済産業省

# 「データ流通促進ワーキンググループ」について

- IoT推進コンソーシアム、総務省及び経済産業省では、分野・産業の壁を超えてデータに関する取引を活性化させることを目的として「データ流通促進ワーキンググループ」を2016年1月に設置し、事業者間でのデータ取引契約の際に課題となる事象についてユースケースに基づき議論（2022年3月までに、36件のユースケースについて審議）。



区分	氏名（順不同、敬称略）	所属	
座長	森川 博之	東京大学 工学系研究科	
	板倉 陽一郎	ひかり総合法律事務所	
	上田 淳	JEITA/株式会社日立製作所	
	菊池 浩明	明治大学 総合数理学部	
	クロサカ タツヤ	株式会社企	
	崎村 夏彦	OpenID Foundation	
	委員	高橋 克己	日本電信電話株式会社NTT社会情報研究所
		寺田 眞治	一般社団法人融合研究所
		林 いづみ	桜坂法律事務所
		平岩 久人	PwCあらた有限責任監査法人
古谷 由紀子		公益社団法人日本消費生活アドバイザー・コンサル タント・相談員協会 サステナビリティ消費者会議	



※2017年12月7日に公開形式で実施した様子

## ➤ 経緯

- 「データ流通促進ワーキンググループ」では、データ流通を伴うBtoBビジネスを検討している事業者から寄せられた相談事項に対して、本WG委員より、技術的観点・制度的観点・社会受容性の観点等から、その解決に向けた助言等を行うことで、事業化を後押し。
- 相談があった当該事業者のみならず他の事業者も後押しするために、本WGで助言があった内容等を整理し、2017年3月「新たなデータ流通取引に関する検討事例集ver1.0」を公開。2018年8月、2017年度の実施事例5件を加え「新たなデータ流通取引に関する検討事例集ver2.0」を公開。
- 2018年度以降は、2020年5月までに実施した事例についてまとめた事例集を第1分冊として公開。
- 2021年3月に2020年度分の事例を、第一分冊に追加し、第1分冊改訂版として公開。
- 2022年3月に2021年度分の事例を、第1分冊改訂版に追加。
- データ流通を伴うBtoBビジネスを検討している事業者が、本事例集を参照することで、検討すべき事項や解決の参考に資するものとなることを期待。

## ➤ 主な構成

### (1) 個別事例の検討結果

本WGで扱った個別事例について、概要とWG委員からの助言内容等を記載。なお、各社の事業に係るものなので、事業が特定されうる内容（社名、サービス名、サービス内容の詳細等）は特定できないように整理。（本WGは原則非公開）

### (2) 取引事例に関する共通意見の整理

(1)で取り扱ったBtoB（BtoBtoC含む）取引に関する事例のうち、特にデータ取得・加工・提供者が取引事例に共通して参照可能な項目について記載。具体的には、「データの利用目的」、「データの種類」、「データの利用範囲」等の観点から、データの流通サイクル（取得時、加工・蓄積時、提供・二次利用時）に沿って意見を整理。

# 個別事例の検討結果（1）

本WGで取り扱った個別事例について、概要と相談内容そしてWG委員からの助言内容等を記載。

No	ユースケース	扱うデータ	相談内容（一部）	実施年度
2-1-1	データ分析プラットフォームによるデータ活用	<ul style="list-style-type: none"> <li>観光客のデータ（国籍、趣味嗜好、訪れた観光地、購買データなど）</li> <li>上記を匿名加工したデータ</li> </ul>	<ul style="list-style-type: none"> <li>匿名加工情報の作成と利用を同一法人で実施する際の法的観点からの制約 他</li> </ul>	2018年度
2-1-2	修学データの流通	<ul style="list-style-type: none"> <li>修学データ</li> <li>上記を匿名加工したデータ</li> </ul>	<ul style="list-style-type: none"> <li>匿名加工情報の作成方法</li> <li>提供先の信頼性確保の方法 他</li> </ul>	2018年度
2-1-3	タッチポイント技術を活用したマーケティングサービス	<ul style="list-style-type: none"> <li>来店客のデータ（端末ID、アクセス日時、タッチポイントID（≒行動履歴）など）</li> </ul>	<ul style="list-style-type: none"> <li>扱うデータの個人情報の該当性</li> <li>プライバシー等の観点からの配慮事項</li> <li>データ提供に関する同意取得方法 他</li> </ul>	2018年度
2-1-4	健康診断データの活用	<ul style="list-style-type: none"> <li>受診者の基本情報（氏名、性別など）</li> <li>健診データ（保険者番号、検査記録など）</li> <li>受診者の生活に関するデータ（睡眠時間、歩数の推移など）</li> </ul>	<ul style="list-style-type: none"> <li>健診機関から健診データを取得するにあたっての留意事項（開示請求に関する制度上の制限、健診機関との契約形態など） 他</li> </ul>	2018年度
2-2-1	カメラ画像のマルチユース活用事例	<ul style="list-style-type: none"> <li>カメラ画像（各カメラ設置エリア通過時に撮影される人物画像）</li> <li>カメラ画像から自動計測した人流データ（歩行者数、性別、年齢）</li> </ul>	<ul style="list-style-type: none"> <li>複数事業者による異なる目的でのカメラ画像活用のための通知・公表の方法と制約について 他</li> </ul>	2019年度
2-2-2	カメラ画像を用いた顔認証によるポイント付与とサービスの提供	<ul style="list-style-type: none"> <li>カメラ画像（店舗内に設置されたカメラで撮影される人物画像）。</li> <li>カメラ画像から抽出した顔画像の特徴量データ</li> <li>特徴量データから推定した属性情報に仮IDを付し、個人を識別できない形で分析・活用したデータ</li> </ul>	<ul style="list-style-type: none"> <li>来店者に対する事前告知・通知と情報発信の方法について 他</li> </ul>	2019年度
2-3-1	ドライブレコーダー映像の利用流通	<ul style="list-style-type: none"> <li>ドライブレコーダー映像</li> </ul>	<ul style="list-style-type: none"> <li>ドライブレコーダーで撮影した映像の個人情報・個人データ該当性</li> <li>データの取得主体の義務</li> <li>撮影の際に必要な通知及び公表内容とその方法</li> </ul>	2020年度
2-3-2	個人の動体に特化したAIモデルの開発と利用流通	<ul style="list-style-type: none"> <li>ウェアラブルデバイスで収集した活動データ</li> <li>活動データを用いて作成したAI学習済みモデル</li> </ul>	<ul style="list-style-type: none"> <li>個人の動体に特化したAI学習済みモデルの個人情報該当性</li> <li>顧客企業と共同開発したAIデータの権利関係</li> <li>顧客企業の従業員から個人データ利用の同意を取得する方法と配慮すべき従業員のリスクについて</li> </ul>	2020年度

本WGでは、事業者から相談があった時点で制定されている関連法制度（個人情報保護法など）や、その他の国内外動向等に基づいて本WG委員から助言を行っている。

## 個別事例の検討結果（2）

本WGで取り扱った個別事例について、概要と相談内容そしてWG委員からの助言内容等を記載。

No	ユースケース	扱うデータ	相談内容（一部）	実施年度
2-3-3	データ流通事業者が、データ流通プラットフォームを構築し、利用者のデータの第三者提供を多段階で行うモデル。	<ul style="list-style-type: none"> <li>・ 利用者の購買データ</li> <li>・ 利用者の購買加工データ</li> <li>・ 利用者のID</li> </ul>	<ul style="list-style-type: none"> <li>・ 利用者とデータ流通事業者A社間 （1）利用者に提供すべき情報 他</li> <li>・ データ流通事業者A社と第三者提供先間 （1）第三者提供先の義務 他</li> </ul>	2020年度
2-4-1	顔認証によって紐付けられたユーザーの行動履歴の二段階同意に基づく利活用モデル。	<ul style="list-style-type: none"> <li>・ 本プラットフォームサービスの利用登録にあたり取得したユーザーの個人情報（顔特徴量データ含む）およびユーザーが設定した第三者提供の是非とその対象・範囲</li> <li>・ 特定空間および準公共空間に設置したカメラで撮影した生活者の画像と画像の顔認証により生成される行動履歴</li> </ul>	<ul style="list-style-type: none"> <li>・ 二段階同意方式による同意取得の有用性</li> <li>・ ユーザーが提供した情報を削除した場合のポイントの扱い</li> <li>・ サービス未登録の生活者に対する対応</li> <li>・ 顔認証における海外ユーザーに対する配慮事項</li> <li>・ 社会受容性の観点での課題</li> </ul>	2021年度
2-4-2	音声データの匿名化によるデータ流通利活用モデル。	<ul style="list-style-type: none"> <li>・ 従業員が店舗内で接客をする際に取得された、来店者と従業員自身の音声データ。</li> <li>・ 音声データのテキスト化により生成される個人情報を含む可能性のあるデータ。</li> <li>・ 音声データの匿名加工データおよび統計データ。</li> </ul>	<ul style="list-style-type: none"> <li>・ 取得した音声データの個人情報該当性</li> <li>・ 音声データ取得に関する通知と同意取得における配慮事項</li> <li>・ プラットフォーム提供事業者としての責任</li> </ul>	2021年度

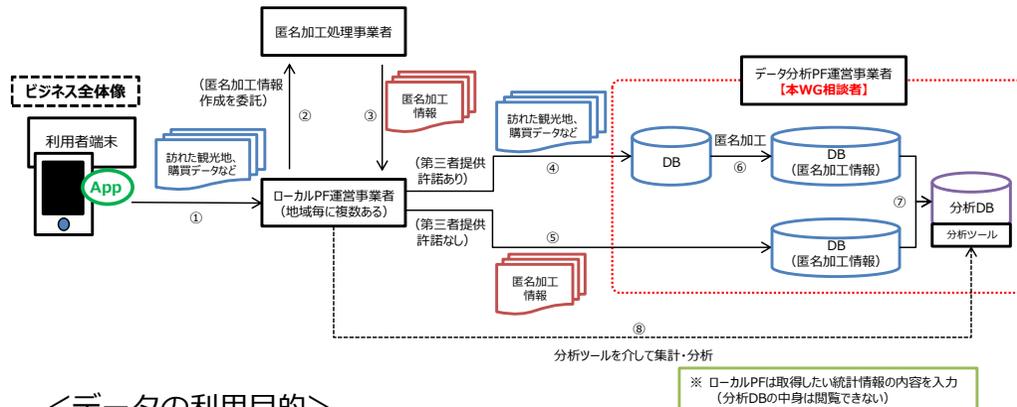
# 2018年度で追加された4件の詳細について①

## 2-1-1 <検討事例1>

### データ分析プラットフォームによるデータ活用

#### <概要>

各地域（ローカルPF）に集積された観光客を中心としたデータの提供を受け、PF横断したデータ分析等を行う基盤を提供するモデル。



#### <データの利用目的>

#### ローカルPF運営事業者

本WG相談者から提供を受けた分析ツールを介して得られた、観光客の属性や行動等に関する統計情報を基に、観光振興等の提案等を行う。

### 本WGでの審議

#### 1. 匿名加工情報の作成とデータ分析プラットフォームの運用の両方を同一法人が担う際に配慮すべき事項について

- 匿名加工処理事業者と匿名加工情報の利用者が同一事業者となるケースは、法律上禁止されておらず、同一事業者が担う場合に対する認定個人情報保護指針のような制度も見当たらない。監査制度を含む、適切なデータ活用に係るアカウントビリティの制度については、事業者の自主規制とすることがリーズナブルではあるが、実効性の有無をどのように判断するかが課題。

### 本WGでの審議

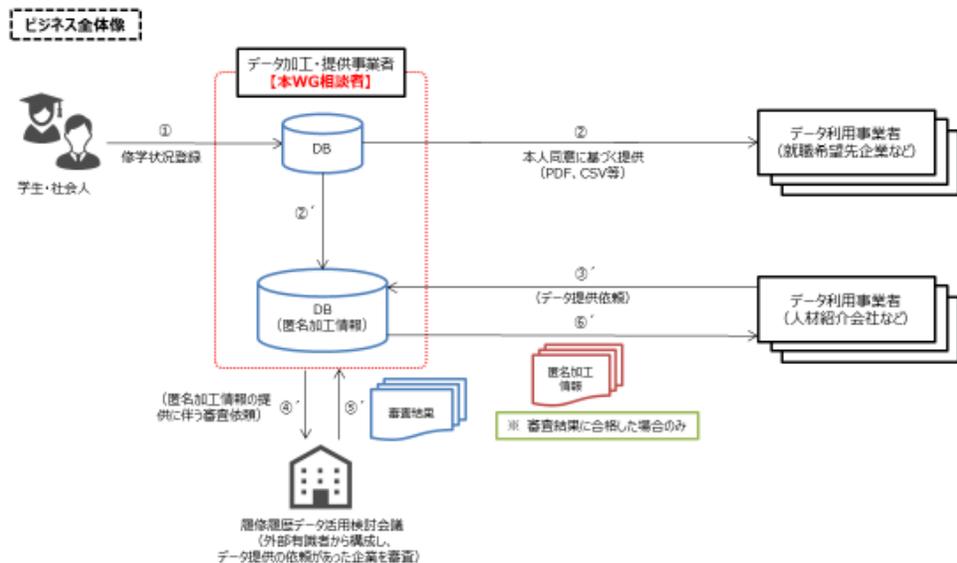
- 他方で、別法人であれば直ちに問題なしとするのでは不十分で、第三者の視点を入れる等、分離の実態を担保できる必要。匿名加工処理事業者と匿名加工情報の利用者は別事業者とし、さらに事業者間の関係に問題がないことを外部へ説明できることが求められる。

#### 2. 観光客を対象としたデータの匿名加工において考慮すべき事項、特に位置情報（購買時、サービス利用時等）の扱いについて

- 移動情報の匿名加工において、移動情報と決済・購買情報やサービス利用情報を紐づけた状態で、特定の個人の識別リスクを排除することは難しいと思われるが、一般財団法人日本データ通信協会が公表した「位置情報の十分な匿名化に係るガイドライン」の『4.1.3.出口要件』において、再識別リスクが記載されており、順番に確認しておくことが有効。
  - 付帯情報として、移動履歴とその他の情報（決済情報等）との紐づけによる特定の個人の識別リスクを回避する必要がある。
  - 場所の特性として、自宅住所が判明するリスクの排除が必要。観光客であっても、3か月等、比較的長期にわたり滞在する場合は、配慮が必要。
  - 集団の規模として、匿名加工の対象とするデータベースの規模が小さい場合、特定の個人の識別リスクが高まることに注意が必要。
- データの組合せにより、特定の個人の識別リスクも変化する。データ利用者の能力、取得可能なデータを想像し、データ利用者において特定の個人の識別ができないような加工が求められる。
- モスクへの訪問等、位置情報の内容によっては、要配慮個人情報（信条の情報）にあたる可能性があることにも留意が必要である。
- 訪日観光客の移動履歴は、住所の識別につながらず、比較的扱いやすいデータかもしれない。
- 今回はGDPR対象国居住者のデータ取得を見送っているが、GDPRの思想に則り、目的の実現に必要な情報のみを提供し、それ以外の不要なデータを提供しないという対応を取ることで、GDPR対象国居住者のデータ取得も可能である。

## 2-1-2 <検討事例2> 修学データの流通

**<概要>**  
本人同意の下で修学状況に関する情報を取得・企業等へ提供するとともに、分析用として匿名加工し、信頼性が高いデータ利用事業者へ第三者提供するモデル。



### <データの利用目的>

#### データ利用事業者 (就職希望先企業など)

本WG相談者から提供を受けた修学状況データを用いて、就職採用時における判断材料等に用いる。

#### データ利用事業者 (人材紹介会社など)

・修学状況データを匿名加工したデータを分析し、企業ニーズと応募者ニーズに合致した就職/転職案内等を行う。

## 本WGでの審議

### 1. 匿名加工情報の作成に当たっての配慮事項について

- 提供項目の検討に当たっては、匿名加工情報に係るガイドラインを順に確認しながら特定の個人の識別リスクを検討することとなる。まず、大学名から都道府県単位で住所を推定できること、提供データの年度から年齢を推定できることには留意が必要。次に、講義名から特定の個人の識別を容易にする、講義の受講者データベースが流通していないことを確認しておくのがよい。最後に、個人情報の保護に関する法律施行規則第19条第4号、第5号に関連して、特に成績が優秀である等、特殊なケースを削除することが必要となる。
- 学科名の提供については、大学ごとに1つの学科に含まれる学生数は様々であり、特定の個人が識別されるリスクへの影響は異なる。大学の実態に通じているデータ利用事業者の観点から、特定の個人を識別されるリスクが低い提供データ項目を検討するのが適当である。

### 2. 匿名加工情報の提供先の信頼性確保の方法について

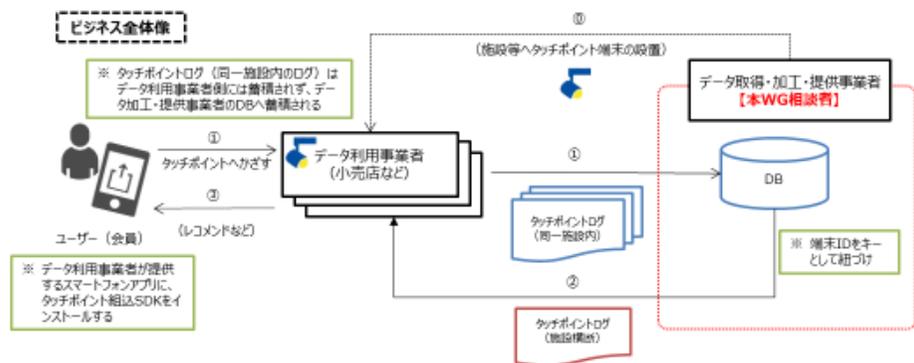
- データ提供先や利用目的を定めた上で、データ提供先との契約により他の情報との照合の禁止を定めるという対応で方向性に問題は無い。匿名加工に係る技術的な最大限の努力に加え、照合等による再識別のリスクへ契約等で備えるのが有効である。
- 技術的な対応を行い、提供するデータ項目から容易に特定の個人が識別されるリスクが低いことを確認する必要があるが、ガイドラインも100%特定が不可能であることまでは求めている。
- 情報信託機能の認定に係る指針ver1.0で示された、情報銀行と情報提供先との間のモデル約款の記載事項を参考に、利用目的の特定、再識別の禁止、セキュリティの確保、プライバシーマークの取得、漏えい等のインシデント時の報告等について契約の条項へ含めるのがよい。

### 3. その他

- 匿名加工情報を作成・提供する、匿名加工情報取扱事業者は、個人情報保護法に従い、作成・提供時に公表を行わなければならない。適切な匿名加工と契約に加え、個人情報の適切な取扱いを確保するためにどのような手段を採っているかを積極的に公開することがよいと考える。

## 2-1-3 <検討事例3> タッチポイント技術を活用したマーケティングサービス

**<概要>**  
施設（小売店等）に来場したお客様の店内の動き、及び施設横断（事業者横断）した動き等を一定期間において把握する仕組みを提供するモデル。



### <データの利用目的> データ利用事業者（小売店など）

・本WG相談者から提供を受けたタッチポイントログを用いて、ユーザーに（きめ細やかな）レコメンド情報の配信等を行う。

### 本WGでの審議

#### 1. 扱うデータの個人情報の該当性について

- ・タッチポイントログは移動履歴に近いものとなるため、理論上無限に取得する場合は、個人情報として扱うべきである。
- ・個人情報は全て厳格なルールの下で管理する企業も存在するが、個人情報であっても仮名化されている場合は扱いを緩和するなど、段階を付けて社内ルールを定めればよいのではないか。

### 本WGでの審議

#### 2. プライバシー等の観点からの配慮事項について

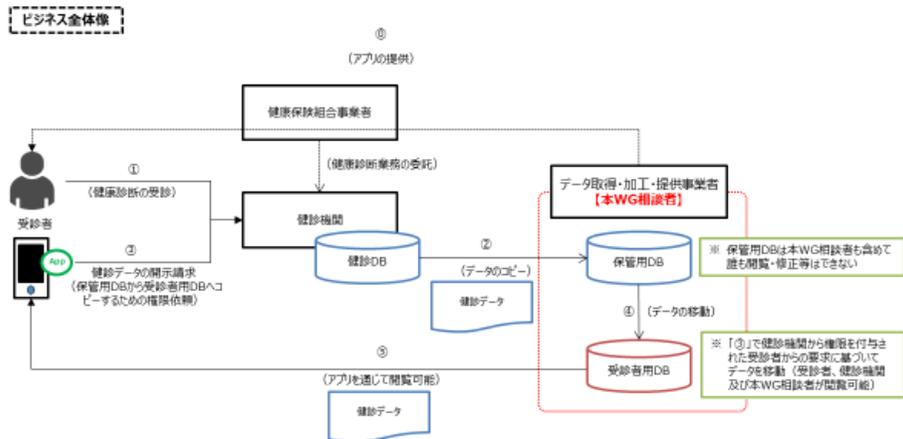
- ・データを紐づける期間について、広告事業者はロケーション履歴データを永続的に保有するのではなく、失効させる期間を議論しており、業界内の相場も定まりつつある。この相場を参考にするとよいのではないかと。
- ・オンラインでは提供範囲が必ずしも明確でないデータ利用も行われているが、リアルな空間ではデータがどこに提供され、どこからレコメンドが提供されるかを図示するなど、丁寧に説明することが好ましい。オンライン広告におけるDMP（Data Management Platform）の動向を参考にするとよいのではないかと。
- ・本WG相談事業者がデータを集中管理し、許容されるデータ利用方法及び許容されないデータ利用方法を取り決めることが現実的。タッチポイントサービスにより取得したデータを既存保有データと無制限に紐付けると転々流通リスクが発生するなど、想定されるプライバシーインパクトをデータ利用事業者へ説明し、必要に応じてデータの利用方法を契約で制限することが望ましい。また、データ利用事業者が既にDMPを保有していることも考えられ、タッチポイントサービスによる提供データが、どのようなデータと紐付けられるかを事前のプライバシー影響評価で考慮することが望ましい。

#### 3. データ提供に関する同意取得方法について

- ・タッチポイント端末にスマホをかざすユーザーは、自身の情報が取得されること等を大まかに理解していると考えられる。加えてどの程度の情報がどこに提供されてレコメンドが表示されるのかをユーザーへ上手く示せば、本人同意の下でのデータ利用であるとみなすことができる。
- ・事業者横断して紐づけたデータをデータ利用事業者へ提供する場合、情報収集モジュール（タッチポイント組込SDK）の導入時に、個人顧客の同意を取得することに加え、オプトアウトの仕組みを持つことが必要。広告業界の取組等を参考にして、アプリケーションからのオプトアウト方法を設けるのに加え、情報収集モジュールに係る本WG 相談事業者のプライバシーポリシーを表示するWebページの中にもオプトアウトの仕組みを設けるべき。

## 2-1-4 <検討事例4> 健康診断データの活用

**<概要>**  
健康診断を受けた本人が健診機関から健診データを入手し、健診結果とその経年変化をいつでも確認できる仕組みを提供するモデル。



<データの利用目的>

### 健診機関

・受診者に対して定期的な案内(健診スケジュールなど)等を行う等で、生活習慣の見直しや受診率の向上等につなげる。

## 本WGでの審議

### 1. 受診者本人による健診機関への健診データの開示請求について

・健康診断データの保有者は、安全衛生面から健康診断(以下、健診)を指示する企業と、健診を実施する健診機関の両方である。個人が健診を行った病院で、改めて受診した場合、当該病院は健診結果を参照せずに新たなカルテを作成することは考えにくく、健診結果を利用するものと考えられる。このとき、本人からの開示請求への回答や、本人のPDSとなる本WG相談者へのデータ提供を行うことに問題は無い。

## 本WGでの審議

・健診機関から本WG相談者へのデータ提供が行えない状況は正しくない。まず、個人の権利と企業間の契約のどちらが優先するかという切り口が考えられる。ヨーロッパでは個人の権利が優先すると考えられるが、日本にはそのような制度が存在しない。次に健診データは、本人に利用許諾権が常に属するようなデータであると考えられるため、本人の利用許諾が無ければどの主体であっても健診データを利用できず、反対に本人の利用許諾があれば本WG相談者も健診データを利用できるのではないか。これらの権利や本人の利用許諾と比較すると、健康保険組合事業者による健診業務の業務委託に基づく主張は弱い。

### 2. 本WG相談者と健診機関との契約形態について

・本WG相談者と健診機関は再委託契約を締結すべきとの考えは、健保組合と健診機関の関係を重視し、受診者を軽視していないか。本WG相談者による健診データの利用は、健診により直接便益を受ける受診者の便益を高め、受診者と健診機関の関係を強化するものであることを強調するのがよい。

### 3. 取得した健診データの管理に関する留意事項について

・健診機関が保有する健診DBと本WG相談者が保有する保管用DBが分かれているのは妥当である。受診者の意向に関わらず、保管用サーバに健診データのコピーを作成し、セキュアにデータ活用が可能な状態しておく仕組みの意義を、十分に理解して運用することが重要である。  
・DBとしてパブリッククラウドを利用している場合は、3省3ガイドラインへの対応を検討するとよい。

### 4. その他について

・データポータビリティの制度設計に留意する必要がある。健診業務の業務委託契約を重視する法制度では、健診機関に対してデータポータビリティを行使できない可能性があることを、関係者は留意してほしい。  
・アメリカでは保険会社が医療費削減のためにPHR等の施策を進めている。日本の国民皆保険は良い制度だが、健保組合が医療費削減のインセンティブを持てるとより良い制度となるのではないか。

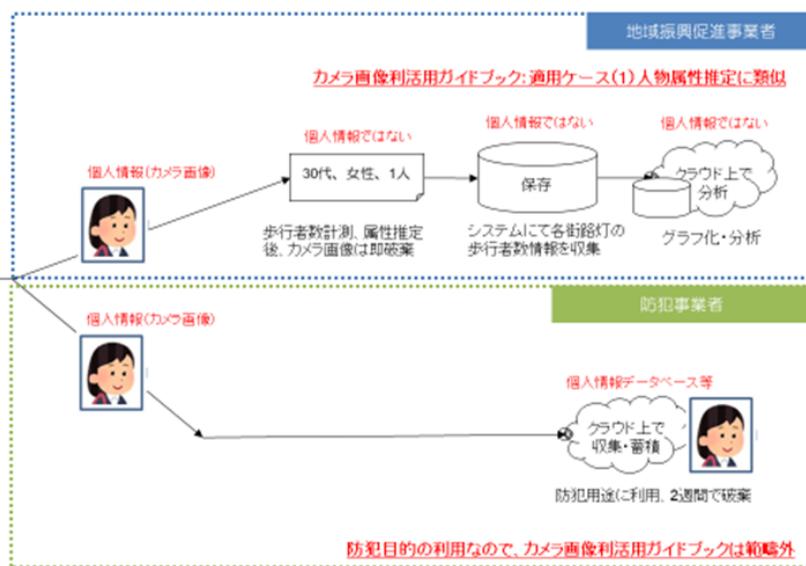
# 2019年度追加された2件の詳細について①

## 2-2-1 <検討事例5>

### カメラ画像のマルチユース活用事例

#### <概要>

公道に設置されたカメラで撮影した画像を、異なる事業者が地域振興および防犯のそれぞれの目的のために活用するモデル。



#### <データの利用目的>

##### 本WG相談者

・自ら管理するカメラで取得した画像から自動測定したデータをもとに、当該地域への来街者の属性や行動等に関する統計情報を作成し、地域振興のために活用する。

##### データ利用事業者

・地域振興促進事業者が管理するカメラが取得した人物画像を含むカメラ画像を管理し、防犯のために活用する。

#### 本WGでの審議

##### 1. 複数事業者によるカメラ画像マルチユースにおける事業者連携と配慮事項について

- ・各事業者が連絡先を掲示し、問い合わせに対応できる体制を構築する必要がある。
- ・自らの事業に関する問い合わせ窓口を設置することに加えて、双方が担当事業者の連絡先を伝える等、丁寧な対応が可能な体制の構築が求められる。
- ・防犯目的での利用について、警察の捜査目的での防犯カメラの情報提供が常に許される訳ではない。過去の最高裁判決で違憲という判例があるなど、デリケートな問題も出ている。警察に提出する情報は何なのか、どのような問合せにどう対応するのか、明確化する必要がある。

##### 2. 複数事業者によるカメラ画像のマルチユースにおける事前告知・通知と配慮事項について

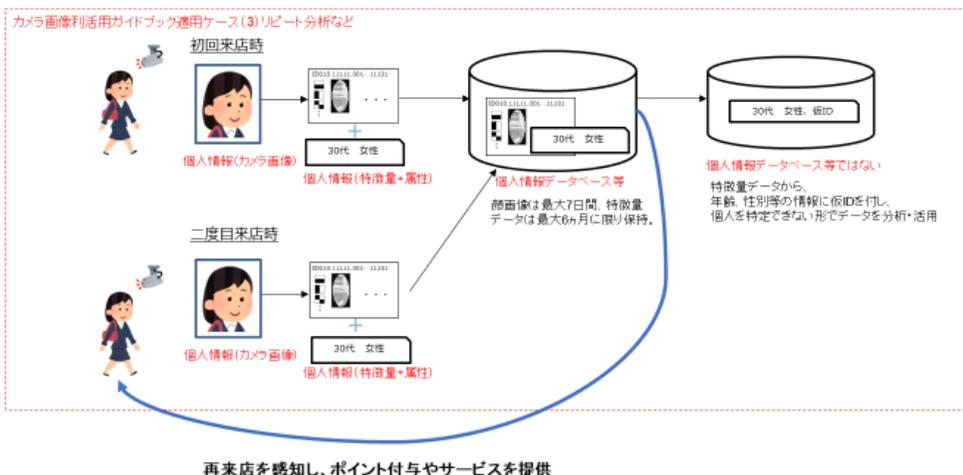
- ・防犯と人流測定の両方を一つのカメラで行うことの妥当性がある。どの地域でも起きうる話であり、その上で二つを分けて来街者へ事前告知・通知することは良いことだと考える。
- ・事前告知・通知は、通行する人が見やすい位置に設置する必要がある。その場で知るべき最低限の情報を分かりやすく記載し、QRコード等を添付して詳しく知りたい人がアクセスできるようにすることは有効。
- ・来街者の多い地域の場合、通知の際の紙サイズや分かりやすさの重要性以上に、ステークホルダーへ通知する姿勢が重要。
- ・プライバシーインパクトを重んじると、識別性が高い状態であれば個人データに近いという考え方があり。撮影される側からすると、たとえ識別の粒度が粗くても、複数台のカメラが連続で機能することで、追跡・追尾可能であるということに不安を感じる人もいますので、その点も配慮すべき。
- ・どこの自治体・地域であっても本モデルのようなケースが起こり得る。特に、このような営みは商店街等の地域振興推進事業の運営上必要なこととして、その必要性を主張すべき。

## 2-2-2 <検討事例6>

### カメラ画像を用いた顔認証によるポイント付与とサービスの提供

#### <概要>

店舗に設置されたカメラで撮影した画像から個人の特徴量を抽出し、顔認証を行うことによりポイントの付与とサービスの提供をするモデル。



#### <データの利用目的>

#### 本WG相談者

- ・店舗に設置されたカメラで取得した画像から、特徴量データを取得、最大で6か月間保持し、再来店時にカメラから取得された画像を照合し、個人を識別することで、ポイントの付与やサービスの提供を実施する。
- ・特徴量データから属性推定、動線情報、リポート分析を実施し、店舗のサービスの向上に用いる。

### 本WGでの審議

#### 1. 来店者に対する通知と配慮事項について

- ・ Webページや通知のツールのひな型を顧客企業となる店舗にAIベンダーが提供している。
  - 来店者の視点に立つと、店舗が取得主体であることを想定していなかった、という感覚になる可能性がある。AIベンダーが、技術提供をしている立場ということをわかりやすく表示できるとよい。
  - 通知のツールについては顧客企業である店舗に貼るように求めることになるので、詳細を記載しようとする顧客企業側の手間を掛けさせることになり対応してもらえない場合もある。
- ・ 現状の対応としては、AIベンダーが、きちんとした通知のツールを用意し、問い合わせ先を引き受けている。
- ・ 事前告知や通知のツールを作成して顧客に配布する、という取組のように、顧客企業が取るべき取組の認識改善に努めることは、今後もAIベンダーの役割として期待したい。
- ・ 店舗側に来店状況を把握されることを気持ち悪く感じる可能性もある。サービスの展開の仕方にもよるが、炎上しかねないため配慮が必要な場合もありうる。
- ・ 再来店時サービス提供など、特定の個人を識別して個人向けに何らかの具体的なサービスを返すことを目的とする場合には、最新のプライバシーの流れや社会受容性を注視し、サービス内容によってはオプトイン型も含めて検討することも必要となり得る。来店者が享受するメリットについて、踏み込んだ事前告知や通知を行えば、来店客との認識の齟齬が生じにくくなるのではないかと。

#### 2. 特徴量データの保存期間について

- ・ 特徴量データと紐づけたIDを6ヵ月を超えて保有し続けるのであれば、個人データを6ヵ月を超えて保有することとなるため、保有個人データとして対応が必要。

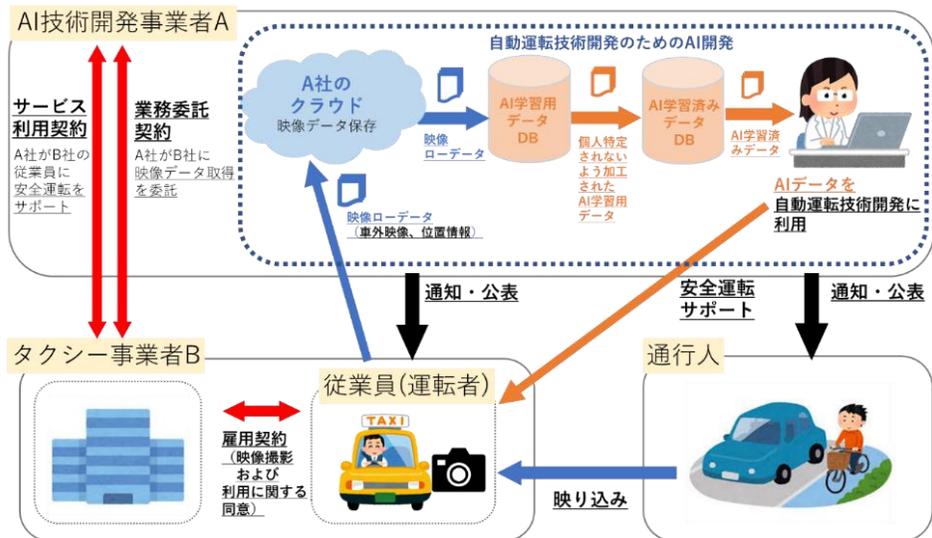
# 2020年度で追加された3件の詳細について①

## 2-3-1 <検討事例7>

### ドライブレコーダー映像の利用流通

#### <概要>

AI技術開発事業者が、「自動運転における物体の認識」と「運転者の安全運転」を目的として営業車両保有事業者にドライブレコーダーの映像データ取得を委託する。取得した映像データをAIの学習用データとして利用するモデル。



#### <データの利用目的>

##### AI技術開発事業者A

- 映像に映り込んだ通行人個人を特定せず、人は人、道路は道路と認識する「自動運転における物体の認識等」を可能にするAI技術開発を行う。
- 従業員（運転者）の安全運転をサポートする。

#### 本WGでの審議

##### 1. ドライブレコーダーで撮影した映像が、個人情報・個人データ該当性

- ドライブレコーダーのカメラの解像度が高いので、個人が特定される。
- 撮影画像の法的性質については意見が分かれたが、個人データおよび個人情報どちらであっても、事業者がすべきことは変わらないと意見が一致した。

#### 本WGでの審議

##### 2. データの取得主体の義務について

- 「いつ」「誰が」「どこにいた」という情報はプライバシーインパクトが大きい可能性もある。データの利用目的上、位置があまり関係ないなら、位置情報がわからないように加工して保管・処理するというのはデータミニマイゼーションという観点からは大事。
- 事業者A から事業者Bにデータの取得を委託している場合、事業者Aが通行人から同意をとらないといけないわけではないが、A社がB社に委託して、映像を取得するという業務委託形式の場合には、防犯カメラのような目的の告知・公表は、難しい。
- 重要なのは、取得の目的と使い方を丁寧に説明して理解してもらうことである。車体を見た一瞬の「誰に」「映像が撮られている」ことがわかるという点は重要ではない。

##### 3. 撮影の際に必要な通知および公表内容とその方法

- 事業者Aから通行人への通知および公表内容とその方法
  - カメラ画像活用ガイドブックに準拠し、車上にデータ取得と利用目的を記載し、写り込む者と運転者に対して表示することに加えて、データ取得主体がwebサイトで公表する必要がある。公表内容については、通行人のプライバシーリスクに応じた対応が求められる。
  - 通行人のプライバシーリスクが高い場合、将来AI技術に使われる可能性があるとなると、同意が得られない可能性があるため、利用目的は明確にした方が良い。「ドライブレコーダーが何を」「どこに情報が行くか」というのが、その都度、明確に理解できるような状況を作る必要がある。「データをどう使うか、どこまで使うか」ということが明確に通知されることが必要。
  - 通行人のプライバシーリスクが低い場合、通行人が、その瞬間には撮影されている旨や取組を理解しなかったとしても、撮影されていたことを知った後に、対応が可能。例えば、本事例における取組がニュースで流れたときに、ウェブサイトを確認可能な状態にすることでフォローするというやり方等。
- 事業者Aから事業者Bの従業員への通知および公表内容とその方法
  - 運転中の従業員が映像に映り込む可能性もあるため、配慮が必要。
  - A社がデータ取得主体なので、本来はA社と従業員（運転者）との契約があるべき。B社と従業員（運転者）の雇用関係で曖昧にするべきではなく、A社がどこまで責任をもつかを明確にしたほうが良い。



# 2020年度で追加された3件の詳細について③

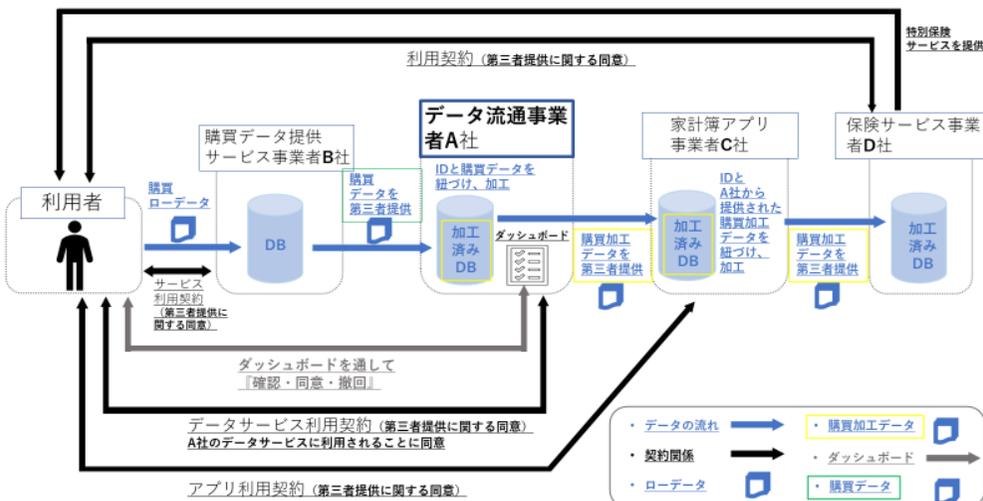
## 2-3-3 <検討事例9>

### 多段階で行うデータの第三者提供に関するご相談

#### <概要>

データ流通事業者が、データ流通プラットフォームを構築し、利用者のデータの第三者提供を多段階で行うモデル。

※サービス全体ではなく、論点に関わる部分のみを図示しています。



#### <データの利用目的>

#### 本WG相談者

- ・統計データとして販売：生活者から収集した購買データを統計化してデータ及びレポートとして提供する。
- ・購買加工データの第三者提供：他のアプリとID連携して購買加工データを第三者提供する。

#### 本WGでの審議

#### 1. 利用者とデータ流通事業者A社間

##### (1) 利用者に提供すべき情報

- ・「説明事項」「データ提供の停止方法」「説明の頻度・タイミング」などの、プライバシーステートメントに書くべき事項は、2020年6月に出たISO29184の規格が参考になる。

#### 本WGでの審議

##### (2) データ流通事業者A社のサービスに備えるべき機能

- ・現在ISO29184のフォローアップとして、ISO27556において、コンセントレシートについての議論をしている。データを受け取り、利用者から同意を取得すると、その結果を利用者の指定したところへ送るといったもの。利用者は、データの行き先がわかり、事業者がどのようなプライバシーポリシーで権利を持っているのかも分かる。
- ・家計簿アプリ事業者C社から保険サービス事業者D社へのデータ連携が止まると、不利益が生じる可能性がある。これを、アラートなどの方法で利用者に知らせなければならない。現状は、停止フラグのようなものを家計簿アプリ事業者C社に投げるように連携する方法のみだが、家計簿アプリ事業者C社側が対応できるのか、という問題がある。また、関連する金融商品に繋がる場合、個人の財産が減少する、さらに生命、身体へ影響があるかもしれない。そのため、手続きを2段階3段階にする必要がある。
- ・保険サービス事業者D社と利用者の契約は、eKYCを行うべき。この時に、利用者の元にデータが来なくなると不利益になる可能性がある。そのため、保険などの金融商品に関するデータを用いる場合は、ワンタッチで終わらないように再度eKYCを行うことが必要である。

##### (3) データの利用停止や削除を求められた場合の義務

- ・利用者は、購買データ提供サービス事業者B社からデータ流通事業者A社へのデータ提供を中止したつもりが、思いがけず家計簿アプリ事業者C社から保険サービス事業者D社へのデータ提供も停止してしまう場合がある。これは、透明性の問題でもある。公正取引委員会のデジタル市場における競争政策に関する研究会の検討を参考にすべき。
- ・データ流通事業者A社が、エコシステム全体において顧客接点、すなわち利用者（データエンティティ）と対峙する最大の事業者となるのであれば、データ流通事業者A社が停止や消去に関する影響の説明を、データが行き渡る全ての利用者と事業者の双方にすべき。

##### (4) 利用者のIDの取扱い

- ・サービス利用時のログインIDについて、メールアドレスをログインIDとして利用する、または、パスワードとして利用することは避けるべき。メールアドレスや携帯電話番号は識別子として再利用可能なため、そこで溜まったデータが他人に開示されてしまう可能性がある。同意の取り方、また、パスワードを預けることで生じるリスクの大きさなどは再検討すべきである。

# 2020年度で追加された3件の詳細について④

## 2-3-3 <検討事例9>

### 多段階で行うデータの第三者提供に関するご相談

#### 本WGでの審議

#### 2. データ流通事業者A社と第三者提供先間

##### (1) 第三者提供先の義務

- データ流通を行う事業者間において、事業者間で共通した（または少なくとも法解釈や取扱いが一貫した）ガバナンスと技術的手段に基づき運用されるCMP（コンセンスマネジメントプラットフォーム）の導入などが考えられる。エンドユーザーから見て、どこを切ってもデータエコシステムは同じエコシステムの中にいるということが理解できる状況が望ましい。この観点や先行しているアプローチを参照することから、データ流通事業者A社が第三者提供先に要求することが分かっていくだろう。

##### (2) データ流通事業者A社の義務

- 情報銀行の認定指針やガイドブックなどのモデル約款や契約が参考になる。認定指針は、JISX9250を参照しており、それが元になっているISO29100もある。その中の11の原則を見るべき。
- 情報銀行の認定スキームでは、認定を受けるために監査が義務化されることから、顧客である第三者提供先に対して監査を受けてもらいやすいという利点がある。このメリットがない中で、データ流通事業者A社はどのように対応すべきか検討する必要がある。

##### (3) データ流通事業者A社と第三者提供先の責任範囲

- 責任範囲が曖昧になる境界がどこなのか、責任分界点を設定する場合は、プライバシー影響が十分に低下している状態を維持する仕組みを、（利用者から見た一次的なデータコントローラーである）データ流通事業者A社と取引先が相互に確認し、適宜モニタリングを実施して、状態把握に努めることが望ましい。

# 2021年度で追加された2件の詳細について①

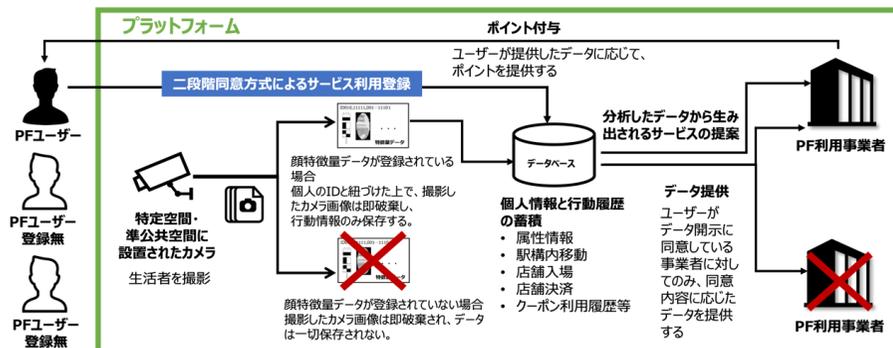
## 2-4-1 <検討事例10>

### 情報提供者に配慮した情報の第三者提供同意スキームの構築

#### <概要>

プラットフォーム提供事業者が、特定空間（店舗内等、事業者が管理権限を持つ空間で、準公共空間以外の空間）および準公共空間（駅や空港等、事業者が管理権限を持つが、不特定多数の生活者が自由にアクセスでき、通ることができる空間）に設置したカメラで撮影した画像を用いて、顔認証を実施しユーザーの行動履歴を取得する。プラットフォーム提供事業者は、ユーザーの行動履歴を分析し、ユーザーの同意に基づき、ユーザーの行動履歴をプラットフォーム利用事業者に提供するとともに、行動分析をした結果得られたサービスアイデアを提案する。ユーザーは、プラットフォーム利用事業者から、データの提供に対する報酬としてポイントを付与される。

データの提供については、情報提供者であるユーザーのプライバシーへ配慮した第三者への情報提供の仕組みとして二段階同意方式を採用する。顔認証によって紐付けられたユーザーの行動履歴の二段階同意に基づく利活用モデル。



#### 二段階同意方式

##### STEP1. サービスの利用同意 (スマホ登録)

- ✓ 認証のための顔画像を保存する
- ✓ 情報開示設定の範囲で第三者に提供する

同意する

情報開示についてデフォルトは**非開示**  
サービス利用に個人情報の第三者提供が**必須ではない**

##### STEP2. 情報提供先の設定

開示先事業者を選択すると、情報提供先事業者毎の**個別の利用規約**に飛び、利用用途やどのように扱われるか？を確認、**納得**した上で情報提供するか否かを決められる

<企業リスト>

提供先一覧  
〇〇株式会社  
XX株式会社  
△△鉄道  
...

各事業者の利用規約  
\*\*\*\*\*  
\*\*\*\*\*  
 同意する

改札入退ログ  
構内移動経路  
店舗内動線  
店舗内決済  
クーポン利用履歴  
...

情報開示先の設定、情報提供のon/offは**自分自身**でいつでも**変更可能**

#### <データの利用目的>

#### 本WG相談者

- ・ 特定空間および準公共空間に設置されたカメラで撮影した画像からユーザーの行動履歴を取得することで、行動特性を分析する。
- ・ 顔認証に基づく個人の行動特性を分析できるプラットフォームの提供および行動履歴を分析した結果得られたサービスアイデアを提案する。

#### ユーザーの行動履歴の提供を受けるプラットフォームサービスの利用事業者

- ・ 取得したデータを分析・活用し、自らのサービス・商品の開発や改善のために用いる。
- ・ 提供されたデータに応じたポイントをユーザーに付与する。

#### 本WGでの審議

#### 1. 二段階同意方式による同意取得の有用性

- ・ 二段階同意方式における通知と同意について
  - 通常のサービスは、サービスの利用規約と個人情報の提供が一括同意になっていることが多いため、二段階同意方式において、サービス利用開始時に個人情報の提供が必須でないことは、重要で望ましいと考えられる。
  - サービス利用とデータの第三者提供について、二段階で同意を取得することは、ユーザーの納得感も高くなり、丁寧で良いと思われる。
  - 同意取得の際に、「同意する」ボタンしかない、同意を強制しているように見える。「同意しない」ボタンを設置して、本人が選択できる仕組みにした方が良いのではないかと。
  - 第三者提供に関する二段階目の同意において、提供先の利用規約確認後に、「同意しない」ことを選択できるようにした方が良いと思われる。
  - 個人情報の提供先について、いつでも変更可能であることが予め提示されることで、ユーザーは安心してサービスの利用登録ができるのではないかと。
  - 通知と同意については、ISO/IEC29184情報技術－オンラインにおけるプライバシーに関する通知及び同意のJIS化も進めているので参照すると良い。

# 2021年度で追加された2件の詳細について②

## 2-4-1 <検討事例10>

### 情報提供者に配慮した情報の第三者提供同意スキームの構築

#### 本WGでの審議

- プラットフォーム提供事業者に求められるユーザーへの対応
  - データ主体であるユーザーから見ると、プラットフォーム提供事業者が提供するプラットフォームが、データの第三者提供先も含めたワンストップのプラットフォームとなることから、一般的なサービスプロバイダーがデータを取得する時よりも、プラットフォーム提供事業者の責任は重くなるのではないかと。
  - プラットフォーム提供事業者は、プラットフォーム利用事業者とユーザーの結節点を握ることとなるため、二段階同意方式に加えて、わかりやすく詳細な通知をすることが求められるだろう。例えば、サービスについて図やイラストを用いて説明する、ユーザーエクスペリエンスのジャーニーを示すなどといったことが、今日的には求められていくのではないかと。
  - 取得データの機微性とセンシティブリティが高いことから、二段階同意方式にとどまらず、より高い次元でのわかりやすさやコントロールのしやすさを目指すことが求められるため、予め、プラットフォーム提供事業者に求められる水準が高いと認識することが重要と考える。
  - プラットフォーム提供事業者に求められる第三者提供先への対応
  - 二段階同意において、第三者提供先の個別の利用規約を確認する際に、利用目的・用途が単に「マーケティング用途」という記載である場合、利用用途が不明瞭のまま、ユーザーに同意を迫ることになり、既存の一段階同意取得と変わらなくなる。
  - ユーザーが本サービスを利用する際には、プラットフォーム提供事業者のブランドへの信頼に基づき、データ提供に同意する人が多くなることが予想される。そのため、プラットフォーム提供事業者は、第三者提供先の利用規約の内容を精査し、データの利用目的・用途を明確に記述するよう依頼する等、プラットフォーム提供事業者として管理することが必要となると思われる。

#### 2. ユーザーが提供した情報を削除した場合のポイントの扱い

- ポイントの扱いについては、プラットフォーム提供事業者ではなく、ポイントを提供するプラットフォーム利用事業者が決めることになる。ただし、プラットフォーム提供事業者が一定の規律を作成することもありうることから、各事業者がきちんとルールを作って決めるべきである。

#### 本WGでの審議

- ユーザーの提供情報削除時のポイントの扱いについては、ポイント付与のタイミングで処理することがあり得る。一定期間、データを活用する期間があってから、ポイントが付与されるのであれば、サービスに登録してデータを提供し、ポイント取得後すぐにデータの削除依頼をすることで、不当にポイントが取得されることも避けられるのではないかと。プラットフォーム提供事業者に求められるユーザーへの対応

#### 3. サービス未登録の生活者に対する対応

- サービス登録者への説明だけではなく、このサービスの使用や撮影を避けたい人、知らずに写り込んでしまった人への説明についても、十分に検討する必要がある。
- サービス開始時は、一定程度、カメラのある場所が認知されている状態を作れると思うが、サービスが進展してデジタルサイネージなどの連携が進むと、一般の生活者には、どのカメラで情報が取得されているかわからなくなると考えられる。本サービスは監視カメラとは異なる目的で個人情報を取得することから、より丁寧な説明が必要である。

#### 4. 顔認証における海外ユーザーに対する配慮事項

- 海外在住者がユーザー登録をして、外国にいる段階でサービスを利用可能な状態とすると、外国でのユーザーの追跡に該当し、GDPR等の諸外国の法律が適用されると思われるため、国内だけでアプリを起動させるようにした方が良いのではないかと。外国でもデータを追跡するアプリを作成したい場合には、域外適用を前提としたものとすべきではないかと。

#### 5. 社会受容性の観点での課題

- データ管理者としてのプラットフォーム提供事業者とプラットフォーム利用事業者との責任分界点、役割やコントロールの分担を明確化する必要があると思われる。
  - 例えば、情報漏えいなどのインシデント発生時のエスカレーションルールや体制、情報共有、データ主体への通知に関するオペレーションなどについて、サービス構想・設計時から検討した方が良い。
- ユーザーとのコミュニケーションについて、規約などをわかりやすく説明したとしても、不安な点やお困りの点が発生するため、あらかじめ問合せ窓口を公表しておくなど、サービスとしてのUI/UXの観点からも整備をしておくこと、ユーザーにとっても安心感が出てくると考えられる。

# 2021年度で追加された2件の詳細について③

## 2-4-2 <検討事例11>

### 店舗における従業員および顧客の音声データの利活用事例

#### <概要>

プラットフォーム提供事業者は、データ取得事業者との間で業務委託契約を締結し、当該データ取得事業者から提供された音声データの管理・分析をする（異なったデータ取得事業者の音声データを含めた分析は行わない）ためのプラットフォームサービスを提供する。データ取得事業者は、自らが運営する店舗において、来店者の同意を取得した上で、従業員が接客中の会話を録音し、プラットフォームに音声データを保存する。プラットフォーム提供事業者は、保存された音声データをテキスト化および匿名加工処理を施した上で、データを統計化する。データ取得事業者は、プラットフォーム上で統計化されたデータを閲覧し、従業員の接客の改善や顧客の購買欲求情報（インサイト）の分析を行うことが可能となる。音声データの匿名化によるデータ流通利活用モデル。

#### PF提供事業者

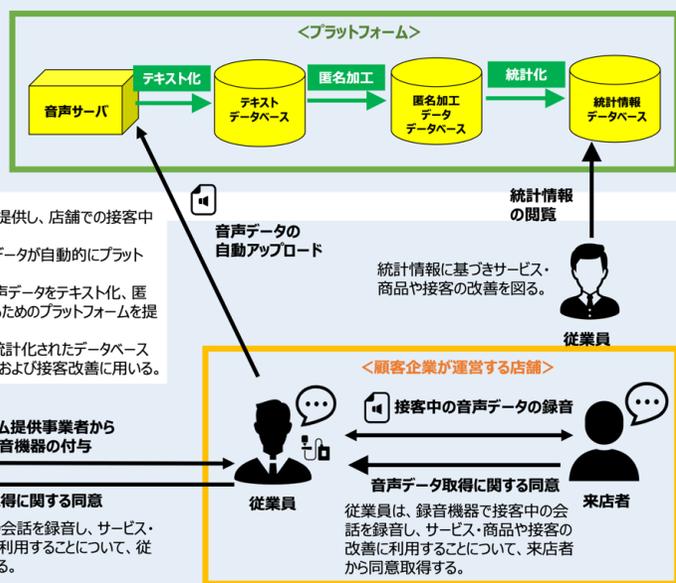


#### 業務委託契約

- 顧客企業は従業員に録音機器を提供し、店舗での接客中の音声データを取得する。
- 従業員が接客中に録音した音声データが自動的にプラットフォームにアップロードされる。
- プラットフォーム提供事業者は、音声データをテキスト化、匿名加工し、データを統計処理するためのプラットフォームを提供する。
- 顧客企業は、プラットフォーム上で統計化されたデータベースにアクセスし、自社のサービス・商品および接客改善に用いる。



#### 顧客企業



#### <データの利用目的>

#### 本WG相談者

- 接客中の会話からしか得られない、来店者のリアルな意見や要求を知るために音声データを取得し分析することで、データ取得事業者のサービスや商品の品質改善等に用いる。
- 接客中の音声データの分析により優秀な従業員の接客態様を可視化し、他の従業員の接客サービスの改善に用いる。

#### 本WGでの審議

#### 1. 取得した音声データの個人情報該当性

- 取得した音声データの会話内容が特定の個人を識別できるものの場合
  - 録音された会話が、氏名等により、特定の個人を識別できるようなものは、個人情報に該当すると思われる。
  - 個人情報に該当する音声データをデータベース化すれば、個人データに該当するのではないか。
  - 録音された音声データの個人情報該当性は、テキスト化前後で変わるものではなく、取得の際には、会話が特定の個人を識別できるものである可能性も考慮し、個人情報の取得を前提とした対応が必要となるのではないか。
- 個人識別符号としての声紋取得の可能性
  - 録音した音声から特徴量を抽出し、本人を認証可能なデータに変換した場合、当該データは個人識別符号に該当すると思われる。しかし、本ケースは、このような個人識別符号の取得には当たらないと思われる。

#### 2. 音声データ取得に関する通知と同意取得における配慮事項

- 音声データ取得目的の限定
  - コールセンターなどの苦情対応や、商談の契約段階において具体的な説明が必要となる場面などの音声データ取得は、利用目的が明確で生活者に納得してもらいやすいと思われる。ただし、それ以外のシーンでは、カメラ画像よりも音声データの方が生活者にとっては抵抗が強くなる可能性があるのではないか。
  - 特に、会話が取得されることは、自分の考えや行動そのものが取得されることになるため、より抵抗感が強くなり得ると思われる。そのため、カメラ画像よりも、利用目的を限定的なものとして、生活者が納得する形での同意を取得する必要があるのではないか。

# 2021年度で追加された2件の詳細について④

## 2-4-2 <検討事例11>

### 店舗における従業員および顧客の音声データの利活用事例

#### 本WGでの審議

##### ・ 音声データ取得の事前告知と通知

- 音声データ取得に同意している来店者ばかりではなく、音声データを取得される店舗には行きたくないとする生活者や、音声データ取得に同意していない来店者の音声を意図せずに拾ってしまう可能性もあることから、それらの人にも配慮した対応が望ましい。
- 音声データ取得の事前告知や通知は、カメラ画像の場合と同様では足りないと思われる。カメラ画像の場合には、カメラ設置場所周辺で事前告知をすれば良いが、音声データの場合には、ピンマイクを付けていても通常はその用途はわからないため、録音機器を装着している人の周りの音声データが取得されることが、来店者がすぐに判別できるような状態とすることが望ましい。
- 音声データの取得の際には、誰が録音しているか、いつ録音を開始し、いつ終了するのかがわかるように説明をし、同意を得た上で録音を行うことが望ましい。

##### 3. プラットフォーム提供事業者の責任

##### ・ データ取得事業者に対する対応

- 業務委託契約であるならば、責任は委託元企業側にあるため、委託の条件や契約をきちんと定め、責任分界を明確にする必要があると考えられる。
- 業務委託先であるプラットフォーム提供事業者が、Application Service Providerとしてツールを提供する場合には、通知または公表は委託元となるデータ取得事業者がすべきことであると考えられる。ただし、一般的に委託元企業にはそれらに関する知見が乏しい場合もあるため、来店者や従業員への対応について、データ取得事業者に情報を提供し、教育をすることは、プラットフォーム提供事業者の責任となると思われる。

##### ・ データ取得事業者と従業員への対応

- データ取得事業者の従業員にとっては、ピンマイクの装着や自らの接客中の音声データの収集を、企業側の優越的地位の濫用により行わされている可能性があり得る。

#### 本WGでの審議

- 従業員に対しては、一定程度の音声データの取得は、雇用契約の範囲で可能な場合もあるが、音声データ取得に同意しないことで不利益を被ることがないようにし、事前の意思確認を行い、自由意志のもとで同意書にサインを求める等の対応が必要であると考えられる。新たな用途で音声データを取得する場合には、その都度、同意書を取得することが望ましい。
- 大規模に導入する場合には、事前に労働組合と話をすることなどの対応を行うことが望ましい。
- 委託元企業が、従業員が同意せざるを得ない状況で対象者全員から同意書を取得する可能性もあり得るため、委託先であるプラットフォーム提供事業者が、委託元企業による優越的地位の濫用が生じないようにサポートをする必要があると考えられる。