EU における GDPR（一般データ保護規則）の運用及び対応に関する動向調査

調査報告書

株式会社野村総合研究所

2019 年 3 月 29 日

目次

第 1 章　調査の背景と目的、調査手法

第 1 節　本調査の背景と目的

EU において 2018 年 5 月 25 日から適用が開始された GDPR（一般データ保護規則:General Data Protection Regulation）については、EU 域内に拠点を有する事業者に加えて EU 域内に拠点を有していなくても EU 向けにサービス等を提供している事業者も影響があるところ、「個人情報の適正かつ効果的な活用が新たな産業の創出並びに活力ある経済社会及び豊かな国民生活の実現に資するものであることその他の個人情報の有用性に配慮しつつ、個人の権利利益を保護するため、個人情報の適正な取扱いの確保を図ること」という個人情報保護委員会の任務（個人情報保護法第 60 条）に照らして、当委員会においては、事業者に対して適切な情報提供を行う必要があることから、株式会社野村総合研究所は当委員会から委託を受け、EU における GDPR の運用及び対応の実態について調査した。

本調査では、EU における GDPR の運用及び対応の実態について調査を行うこととし、具体的には、プロファイリングに関する規制及びデータポータビリティの権利の欧州におけるデータ保護機関(Data Protection Authority: DPA)の運用及び EU の民間事業者の対応、並びに、その他 DPA 及び EU の民間事業者のそれぞれが抱えている GDPR に関する課題とそれに対する対応の状況を精査した。

第 2 節　調査手法

調査手法は、以上の背景と目的を踏まえ、特に現地でのヒアリング調査を中心に検討した。すなわち、GDPR 本体やガイドライン、各社のプライバシーポリシーや業界レベルでの取組といった文献調査を実施しつつ、それらが具体的にどのように作成され、解釈され、そして業務やシステムに適用されているのか、という点を現地調査で浮かび上がらせることを基本方針とした。

結果、2019 年 1 月から 2 月にかけて、現地調査では 6 か国（イタリア、スウェーデン、スペイン、ドイツ、オランダ、フランス）の DPA を含む、合計 9 か国（イギリス、イタリア、オランダ、スウェーデン、スペイン、ドイツ、フランス、ベルギー、ポルトガル）の 40 以上の DPA、企業、法律事務所、業界団体、シンクタンクといった組織に対してヒアリングを実施した。

なお、事業者数の限られるスペインとオランダについては、本件調査をより有益なものとすべく、弊社がポルトガル並びにベルギーを対象国としてそれぞれ付け加えた。

以下、本報告書では第 2 章でプロファイリング規制を、第 3 章でデータポータビリティについて扱う。それぞれ、出発点となる GDPR 等の法令、それを受けた現地企業の対応状況、企業並びに DPA の抱える課題を分析し、最後にまとめとしての日本企業への示唆をまとめている。

第２章　プロファイリング

GDPR では、プロファイリングを「自然人と関連する一定の個人的側面を評価するための、特に、当該自然人の業務遂行能力、経済状態、健康、個人的嗜好、興味関心、信頼性、行動、位置及び移動に関する側面を分析又は予測するための、個人データの利用によって構成される、あらゆる形式の、個人データの自動的な取扱い」（第 4 条第 4 項）と定義している。以降、特別な断りがない限り、本報告書においてプロファイリングとは、GDPR の定義に該当するデータの取扱いを意味する。

本章では、まず第 1 節において、GDPR のプロファイリングに関する規制（以下「プロファイリング規制」という。）に目を向け、企業がプロファイリングを行う際の法的義務について確認する。次に第 2 節において、EU 企業が取り組むプロファイリングについて、取扱いの詳細とその法的根拠を明らかにし、EU におけるプロファイリング規制の運用状況を確認し、第 3 節、第 4 節では、EU 企業・DPA がプロファイリング規制に対して抱いている課題意識を整理する。その上で、第 5 節において、運用状況・課題を踏まえ、日本企業がプロファイリングを行う際、参考となる考え方を整理する。

第１節　プロファイリングに関連する法的義務

プロファイリング規制について主に規定するのは、GDPR 第 21 条、第 22 条であるが、プロファイリング自体は個人データの取扱いの態様の 1 つに過ぎず、他の取扱いと同様に、基本原則を遵守しつつ、取扱いの適法性を確認し、データ主体の権利（情報提供を受ける権利、アクセスの権利、訂正・消去・取扱いの制限の権利等）に対応することが求められる。第 2 節において詳述するが、EU 企業・DPA もプロファイリングの実施自体をもって特別な取扱いとは捉えておらず、他の取扱いと同様に、取り扱う個人データの種類、量等に応じてリスク評価を行った上で、対応することを求めている。主なプロファイリング規制について、図表 1 のとおり整理した。

図表 1　主なプロファイリング規制

条項	規制の内容
第 5 条	個人データの取扱いと関連する基本原則
第 6 条	取扱いの適法性
第 9 条	特別な種類の個人データの取扱い
第 13 条	データ主体から個人データが取得される場合において提供される情報
第 14 条	個人データがデータ主体から取得されたものではない場合において提供される情報
第 15 条	データ主体によるアクセスの権利
第 16 条	訂正の権利
第 17 条	消去の権利（「忘れられる権利」）

条項	規制の内容
第 18 条	取扱いの制限の権利
第 21 条	異議を述べる権利
第 22 条	プロファイリングを含む個人に対する自動化された意思決定
第 35 条	データ保護影響評価
第 37 条	データ保護オフィサーの指名
第 38 条	データ保護オフィサーの地位
第 39 条	データ保護オフィサーの職務

プロファイリングを含むもっぱら自動化された意思決定は、データ主体に対して法的効果（又は同様の重大な影響）を及ぼす場合、GDPR 第 22 条において原則として禁止されているが、データ主体から明示的な同意を取得している、データ主体との契約の履行若しくは締結に必要である、又は所定の条件を満たす EU 法若しくは加盟国の国内法で認められる場合においては、許容される。こうした例外に基づき取扱いを行う場合、管理者（Controller）は適切な保護措置を講じることが求められる。具体的な保護措置の一環としてデータ保護影響評価（DPIA：Data Protection Impact Assessment）の実施義務を負う。そこで本調査では、GDPR 第 35 条、第 37～第 39 条についてもプロファイリング規制と見なして調査を行った。

各プロファイリング規制に対する具体的な調査の視点は次のとおりである。

図表 2　各プロファイリング規制に対する調査の視点

規制	調査の視点
第 5 条：基本原則 第 6 条： 取扱いの適法性 第 9 条： 特別な種類の個人データの取扱い	・ 同意、契約の履行若しくは締結[1]、法的義務の遵守、正当な利益又はその他のいずれの法的根拠に基づき、どのようなプロファイリングを行っているか。 ・ 特別な種類の個人データを用いたプロファイリングを行っているか。
第 13-14 条： 情報提供を受ける権利	・ プロファイリングについて、データ主体に対しどのような情報の提供を行っているか。
第 15 条：	・ プロファイル作成に用いたインプットデータ並びにプロファ

[1] 本書においては、取扱いの法的根拠と、プロファイリングを含むもっぱら自動化された意思決定が認められる例外事由の双方について「契約の履行若しくは締結」と表現するが、厳密には前者における「契約の締結」に必要な取扱いは、データ主体による要求に基づくものに限定される点に留意が必要である。

規制	調査の視点
アクセスの権利	イル及びデータ主体が位置づけられたセグメントに関する情報として、どのような情報にデータ主体がアクセスできるようにしているか。どのような形式で提供しているか。
第 16-18 条： 訂正・消去・取扱いの制限の権利	・ データ主体が権利を行使する上で、どのようなフロー（窓口・ユーザーインターフェイス、役割分担、対応にかかる期間等）を整備しているか。
第 21 条： 異議を述べる権利	・ （仮に正当な利益を法的根拠としてプロファイリングを行っている場合、）異議を述べる権利について、データ主体に対しどのような形で通知を行っているか。 ※ GDPR 第 21 条では、異議を述べる権利について、明示的にデータ主体の注意を引くようにされ、かつ、他の情報とは明確に分けて表示されなければならないと規定されている。 ・ データ主体が権利行使を行う上で、どのようなフロー（窓口・ユーザーインターフェイス、役割分担、対応にかかる期間等）を整備しているか。
第 22 条： プロファイリングを含む個人に対する自動化された意思決定	・ どのような取扱いが GDPR 第 22 条の適用対象として捉えられているか。 ・ データ主体が意思決定への自然人の介入を求めた場合や決定結果に異議を表明した場合、どのように対応しているか。
第 35 条： データ保護影響評価 第 37-39 条： データ保護オフィサー	・ DPIA をどのように実施しているか。 ・ プロファイリングの実施有無と DPIA の実施有無がどう関連しているか。 ・ データ保護オフィサー（DPO：Data Protection Officer）はどのように DPIA に関与しているか。

第 2 節　EU におけるプロファイリングの運用状況

（1）EU 企業の具体的なプロファイリングの状況

EU 企業が行っているプロファイリングは顧客を対象とするものと従業員を対象とするものとに 2 分される。それぞれの分類で把握されたプロファイリングの具体例及びこれに対応する法的根拠は図表 3、4 のとおりである。

本調査では、具体例ごとにその法的根拠を把握したが、調査対象国ごとに見解が異なる例も散見された。例えば、後述するとおり、英国の独立系 DPO によると、与信条件の設定を目的としたプロファイリングはデータ主体からの同意取得が難しいため、正当な利益を根拠としているが、現地 DPA によると、融資を行う前に顧客の信用確認を行うことは法的義

務の遵守であるとのことであった。このように同様の目的での取扱いをしていても、異なる法的根拠を聴取した場合は、それぞれに印を記載している。単一のデータの取扱いに対して複数の法的根拠を見出しうるというのは一般に生じる現象であり、これ自体が問題となるわけではないが、以降に示すプロファイリングの具体例及びこれに対応する法的根拠は、いずれも現地でのヒアリング調査に基づく事例であり、調査対象国における当該取扱いの総体や DPA による公式な判断を示すものではない点に留意が必要である。

図表 3　EU 企業が行っているプロファイリングの具体例と取扱いの法的根拠（顧客を対象としたプロファイリング 1/2）

対象	分野	プロファイリングを含む意思決定の内容	取扱いの法的根拠			
			同意	契約の履行＊	法的義務の遵守	正当な利益
顧客	金融	✓ 申込み情報と信用調査機関からの情報に基づく、クレジットカードの発行可否の判定	－	○	○	－
		✓ 申込み情報と信用調査機関からの情報に基づく、与信条件の設定	－	○	○	○
		✓ 借入額、返済状況等に基づく、リスク評価（貸し倒れ額の算定等）	－	－	○	－※
		✓ 送金内容等に基づく、不正送金（マネーロンダリングを含む）・詐欺の検知	－	－	○	－※
		✓ 申込情報と口座利用情報に基づく、顧客動向を分析した上での、マーケティング活用	○	－	－	－
		✓ 取引履歴、世帯構成等に基づく、提案する金融商品の決定	○	○	－	－
	信用調査	✓ 信用情報に基づく、信用スコアの算出	－	－	－	○

黄色の網掛け：当該プロファイリングを行うEU企業において、GDPR第22条の適用対象と認識されている事例を含む。

＊　厳密には「データ主体が契約当事者となっている契約の履行のために取扱いが必要となる場合、又は、契約締結の前に、データ主体の要求に際して手段を講ずるために取扱いが必要となる場合」であり、契約締結の前段階における取扱いを含むことは前述のとおりである。「契約の履行若しくは締結」と記載すべきところ、スペースの関係から「契約の履行」とのみ記載している。

※　リスク評価や不正送金・詐欺の検知を目的としたプロファイリングはGDPR第22条の適用対象と認識されているが、他方で、同取扱いの法的根拠として正当な利益を挙げるEU企業もあった。この理由としては、同取扱いに関するプロファイリングが複数あり、GDPR第22条の適用対象となるもの、ならないものがあるという状況が考えられる。

図表 4　EU 企業が行っているプロファイリングの具体例と取扱いの法的根拠（顧客を対象としたプロファイリング 2/2）

対象	分野	プロファイリングを含む意思決定の内容	取扱いの法的根拠			
			同意	契約の履行＊	法的義務の遵守	正当な利益
顧客	通信	✓ 申込み情報と信用調査機関からの情報に基づく、契約可否の判定	－	○	－	○
		✓ 契約内容、利用状況等に基づく、解約率の予測	○	－	－	－
		✓ 通信状況に基づく、回線設備の保守整備の優先度を判定	－	－	－	○
	その他	✓ 閲覧、購入履歴に基づく、利用者の Web 上のマイページの表示内容の切り替えや電子メールの配信	○	－	－	○
		✓ 運転状況等に基づく、製品開発の参考材料生成	－	－	－	○
		✓ 実店舗における消費者の購買行動の分析に基づく、マーケティング活用	○	－	－	○

黄色の網掛け：当該プロファイリングを行う EU 企業において、GDPR 第 22 条の適用対象と認識されている事例を含む。
＊　厳密には「データ主体が契約当事者となっている契約の履行のために取扱いが必要となる場合、又は、契約締結の前に、データ主体の要求に際して手段を講ずるために取扱いが必要となる場合」であり、契約締結の前段階における取扱いを含むことは前述のとおりである。「契約の履行若しくは締結」と記載すべきところ、スペースの関係から「契約の履行」とのみ記載している。

図表 5　EU 企業が行っているプロファイリングの具体例と取扱いの法的根拠（従業員を対象としたプロファイリング）

対象	分野	プロファイリングを含む意思決定の内容	取扱いの法的根拠			
			同意	契約の履行＊	法的義務の遵守	正当な利益
従業員	採用	✓ 求職者が回答した性格判断の質問結果に基づく、職業適性の判定	○	－	－	○
		✓ 履歴書の内容に基づく、採用選考時のスクリーニング	－	○	－	－
	人事評価	✓ 従業員の性格的な特徴と給料等に基づき、マネージャーが人事評価を行う際の参考材料生成	－	○	－	－
	事故予防	✓ 事務作業のミス検知	－	－	－	○
	業務管理	✓ 従業員の業務状況の把握	－	－	－	○

黄色の網掛け：当該プロファイリングを行う EU 企業において、GDPR 第 22 条の適用対象と認識されている事例を含む。
＊　厳密には「データ主体が契約当事者となっている契約の履行のために取扱いが必要となる場合、又は、契約締結の前に、データ主体の要求に際して手段を講ずるために取扱いが必要となる場合」であり、契約締結の前段階における取扱いを含むことは前述のとおりである。「契約の履行若しくは締結」と記載すべきところ、スペースの関係から「契約の履行」とのみ記載している。

（2）プロファイリングの具体例（顧客に対するプロファイリング）

顧客に対するプロファイリングを含む意思決定は分野によってその内容が異なっている。特にプロファイリングの利用が進んでいる分野として、金融、信用調査、通信が挙げられる。他方で、マーケティングを目的としたプロファイリングは業種や分野に限らず、広く利用されていることが確認された。本節では、図表 3、4 において整理した、各分野におけるプロファイリングを含む意思決定の個別の運用状況について記載する。

① 金融

ヒアリングによって把握された、金融業界におけるプロファイリング及びこれを用いた意思決定について、個人データの取扱いの詳細とその法的根拠を整理する。

①－1：申込み情報と信用調査機関からの情報に基づくクレジットカードの発行可否の判定

【運用状況】

消費者がクレジットカードを申し込む際、消費者の申込情報や、信用調査機関から信用スコア等の情報を基にプロファイリングを行い、クレジットカードの発行可否を判断する、という用途であり、スウェーデンや英国にて運用が確認された。ヒアリング先によれば、この運用は、法的効果、又は同様の重大な影響を及ぼすプロファイリングではあるものの、少なくとも現時点ではもっぱら自動化された意思決定を伴っていないため、GDPR 第 22 条の適用は受けないという認識であるとのことである。

【法的根拠】

スウェーデンにおいては、銀行は返済能力がある顧客にしかクレジットカードを発行してはいけないという業法があり、これにのっとって金融機関は顧客の自己資本が十分であるか検査する必要があり、法的義務の遵守が法的根拠となっている。

他方、英国においては、クレジットカードの発行におけるプロファイリングの利用は、契約上必要な行為として認識されている。

①－2：申込み情報と信用調査機関からの情報に基づく、与信条件の設定

【運用状況】

①－1 と類似する運用だが、クレジットカードの発行可否ではなく与信の条件を設定するというもので、より多くのヒアリング先（オランダ、スウェーデン、英国）にて運用が確認された。英国によると判定に利用する個人データは、企業が自社で取得したものと、データブローカーから購入したものの両方を用いている。

【法的根拠】

英国の独立系 DPO によると、与信目的のプロファイリングはデータ主体からの同意取得が難しいため、正当な利益を根拠に実施しているというコメントがある一方、同国の法律事務所によると、ローンを組む際のプロファイリングは契約上必要な行為として認識

されており、同じ国でも法的根拠についての認識が異なっている。

また、現地の DPA によると、融資を行う前に顧客の信用確認を行うことは法的義務があるとされている。

①－3：借入額、返済状況等に基づく、リスク評価（貸し倒れ額の算定等）

【運用状況】

金融機関の顧客の口座情報などに基づいて、融資に対するリスク評価、又は適性検査（Suitability assessment）を実施する。スウェーデンの金融機関によると、適性検査では、顧客の口座情報以外に、年齢などの情報も参考にしている。

他方、イタリアの金融機関によると、生命保険事業者が、年齢などの個人データに基づいてリスク評価を実施している。この運用は、法的効果、又は同様の重大な影響を及ぼすプロファイリングであり、もっぱら自動化された意思決定を含む場合があるため、第 22 条の適用を受けるものもあると認識されている。

【法的根拠】

イタリアの例にあった生命保険事業者のリスク評価は、GDPR 第 22 条の適用範囲と想定されるため、法的義務の遵守が法的根拠となっている。

他方、スウェーデンの金融機関から指摘があった融資におけるリスク評価・適性検査については、銀行の信用力を保つために必要な運用として認識されており、金融機関の正当な利益が法的根拠となる。

①－4：送金内容等に基づく、不正送金（マネーロンダリングを含む）・詐欺の検知

【運用状況】

いわゆる不正検知に関する運用であり、スウェーデン、イタリア、ベルギー、ドイツ、スペイン、英国など、金融機関へのヒアリングにおいて最も多くの事例が確認された。

内容もマネーロンダリングの防止や E コマースにおける不正検知、テロリストによる口座開設を阻止するなど多岐にわたる。例えば、スペインの法律事務所によると、顧客の全ての情報を 1 つのシステムに統合して管理しており、テロリストによる口座開設を阻止することなどに使われているとのことである。

この運用は、法的効果、又は同様の重大な影響を及ぼすプロファイリングであり、もっぱら自動化された意思決定を含む場合があるため、GDPR 第 22 条の適用を受けるものもあると認識されている。

【法的根拠】

多くの国で、金融機関における不正防止の法令遵守が法的根拠となると認識されている。例えば、イタリアや英国、スペインなどではマネーロンダリングを防止する国内法が定められている。

他方、スウェーデンの金融機関によると、不正防止のためのプロファイリングは金融機

関における正当な利益に基づくものであり、支払いの実行のため、不可避な対応と考えられている。

①－5：申込情報と口座利用情報に基づく、顧客動向を分析した上でのマーケティング活用

【運用状況】

英国の金融機関によると、オンラインショッピングの動向、口座開設理由、居住地域、社会背景、学歴などアンケートを通じて把握・分析し、マーケティングに活用している。

また、ポルトガルの金融機関によると、顧客属性に応じてダイレクトマーケティングを実施するケースがある。（例：ゴルフを好きな顧客がいた場合、ゴルフのイベントに声をかける等）

【法的根拠】

この運用の場合、法的根拠はデータ主体からの同意となっている。特にポルトガルにおけるダイレクトマーケティング事例の場合、オプトインを前提としており、プロファイリングのデータの活用方法は法務部と相談をしながら進めるなど丁寧なプロセスが確認された。

①－6：取引履歴、世帯構成等に基づく、提案する金融商品の決定

【運用状況】

①－5 と殆ど同じプロセスだが、マーケティング対象が保険など金融商品に限定されている。イタリアやスペインで、保険商品の説明や推奨に当たって、家族構成など様々な情報をマーケティング目的で取得したり、顧客との面談を通じて得た資産情報を始めとする個人情報を基にプロファイリングが行われ、銀行の商品を勧める際に使ったりといった事例が確認された。

【法的根拠】

イタリアのケースでは、顧客から同意を取得した上でプロファイリングを実施していたが、スペインのケースでは顧客との契約を履行する上で必要なものとして整理されていた。

②信用調査機関による信用スコアの算出

【運用状況】

Trans Union、Experian、Equifax といった信用調査機関はクレジットスコアの作成、マーケティング活動といった領域でプロファイリングを実施している。金融機関、エネルギー事業者、携帯端末事業者などに信用スコアを提供している。

例えば、英国においては携帯端末事業者が、信用スコアに基づいて、ハイエンド端末（iPhone 等）の支払いが可能かどうか判断している。また、スペインでは、Experian、Equifax などが信用情報報告システムを運用し、データ主体の滞納履歴の有無を元にブラ

ックリストを作成し、コモディティの契約、例えば金融サービス（融資、クレジットカードの発行)、通信サービスや CATV、電力・ガスの契約審査に活用されている。

スコアリングは法的効果、又は同様の重大な影響を及ぼすプロファイリングであり、自動化された個人データの取扱いとなっており、多くの調査対象国において、GDPR 第 22 条の適用範囲と認識されているが、ヒアリング先の 1 つである DPA によると、スコアリングの基準自体は人間が作り、それを機械が採点しているだけであり、自動化された意思決定とは認められないという意見も確認された。

【法的根拠】

信用調査機関による信用スコアの算出は、正当な利益を法的根拠として行われている。

③通信

通信会社も契約可否の判定や解約率の予測といった用途でプロファイリングを活用している。ヒアリングで確認されたプロファイリングを用いた意思決定の種別ごとに、個人データの取扱いの詳細とその法的根拠を整理する。

③－1：申込み情報と信用調査機関からの情報に基づく、契約可否の判定

【運用状況】

通信会社は顧客からの契約の申込みがあった際、その申込情報や信用調査機関からの情報にもとづいて契約可否を判定している。本調査ではスウェーデンやドイツにて運用が確認された。スウェーデンの通信会社によると信用情報のチェックはもっぱら自動化された意思決定プロセスとなる場合があり、GDPR 第 22 条の適用範囲と認識されている。

【法的根拠】

スウェーデンの通信会社によると、信用情報を活用したプロファイリングは契約の履行を法的根拠としている。

また、DPA によると、消費者が債務過多に陥るリスクを回避する正当な利益として認められており、もっぱら自動化された意思決定プロセスを含まない運用の場合、正当な利益が法的根拠となりうる状況が確認された。

③－2：契約内容、利用状況等に基づく、解約率の予測

【運用状況】

スウェーデンやスペインの通信会社によると、解約予測（Churn Prediction）にプロファイリングが活用されており、データ分析の結果に応じて職員が顧客に直接連絡することもある。

【法的根拠】

上記のようなプロファイリングは顧客の同意を法的根拠に実施されている。

③－3：通信状況に基づく、回線設備の保守整備の優先度を判定

【運用状況】

DPA やスウェーデンの通信会社によると、通信会社が接続環境改善のための設備投資を目的としたプロファイリングを実施している。

【法的根拠】

上記のようなプロファイリングは通信会社における正当な利益を法的根拠に実施されている。

④その他

一般的なマーケティングを目的としたプロファイリングは業種や分野に限らず、広く利用されていることが確認された。プロファイリング及びこれを用いた意思決定の種別ごとに、個人データの取扱いの詳細とその法的根拠を整理する。

④－1：閲覧、購入履歴に基づく、利用者の Web 上のマイページの表示内容の切り替えや電子メールの配信

【運用状況】

ドイツやイタリア、スペイン、スウェーデンで確認された用途で、以下のような具体例が確認された。

① 個人の住所、年齢等に応じてプロモーションする商品を変更するケース（スウェーデン）
② Web サイトの訪問状況や、商品の購入状況から提示する広告を変えるケース（イタリア）
③ 電子メールをデータベースに登録し、広告メール送付後のクリック数や Cookie 等の情報を取得するケース（ドイツ）
④ 過去に商品を購入した顧客を登録し、その商品の新しいモデルを紹介するケース（スペイン）

【法的根拠】

法的根拠はデータ主体からの同意取得、又は事業者の正当な理由という 2 種類が確認される。スウェーデンやイタリア、ドイツでのヒアリング結果によると、マーケティング利用のプロファイリングは同意を取る運用が一般的である。ただしスペインの法律事務所によると、自分の既存の顧客を対象にマーケティングを実施する場合（例：既存の顧客に、購入した商品の新しいモデルを紹介する）、正当な利益が法的根拠として認められる。

④－2：運転状況等に基づく、製品開発の参考材料生成

【運用状況】

スウェーデンの自動車メーカーによると、R&D 部門にて自社製品の利用状況を取得しプロファイリングすることで製品開発の参考材料としているケースが確認された。

【法的根拠】

上記運用の法的根拠は事業者の正当な利益が適用されると認識されている。

④－3：実店舗における消費者の購買行動の分析に基づく、マーケティング活用

【運用状況】

英国の法律事務所によると、ショッピングセンターでは駐車場所の情報と消費者の購買行動に関する情報を取得・分析しマーケティングに活用している。また、同様の取組は、SNS やホテル、銀行等、大企業では一般的に行われているとのことであった。

【法的根拠】

上記目的における法的根拠について明確なコメントは得られなかったが、④－１と同様にデータ主体からの同意取得、又は事業者の正当な理由という 2 種類となると想定される。

（3）プロファイリングの具体例（従業員に対するプロファイリング）

従業員に対するプロファイリングは採用時、人事評価時、業務状況の把握といった領域で運用されている。ここではヒアリングによって把握された個別の運用状況について記載する。なお、留意点については（2）と同様である。

①：求職者が回答した性格判断の質問結果に基づく、職業適性の判定

【運用状況】

ドイツの法律事務所によると、採用時に求職者が質問に答えると回答結果に基づくプロファイリングと職業適性が自動で判定されるようなサービスが存在する。

【法的根拠】

このような運用はデータ主体の同意を根拠に実施している。また、既存従業員に対し、同様の取扱いを行う際は、ドイツの場合、プロファイリングがデータ主体にネガティブな影響を与えない、という条件のもと国内の雇用法（Employment law）にもとづき運用が可能となっている。

②：履歴書の内容に基づく、採用選考時のスクリーニング

【運用状況】

ポータルサイトを通じた応募者の情報をスクリーニングすることで業務効率化が図られるケースなどが該当する。

ドイツの法律事務所によると、履歴書を活用したスクリーニングは GDPR 第 22 条の適用対象となる重要な意思決定を含むため、個人データの取扱いに当たっては、採用担当

の部署と IT セキュリティ担当の部署が取扱いの責任分担について議論を行っている。

【法的根拠】

企業が採用で個人データを集める目標は、煎じ詰めれば従業員との雇用契約を結ぶことなので、契約の履行を法的根拠としている。もっとも、この行為は厳密には契約締結の前段階であるが、契約の履行は GDPR 第 6 条において、「契約締結の前に、データ主体の要求に際して手段を講ずるために取扱いが必要となる場合（in order to take steps at the request of the data subject prior to entering into a contract）」を含んでいるため、これに含まれるとの解釈が一般的である。

このようなプロファイリングはもっぱら自動化された意思決定を含んでおり、GDPR 第 22 条の適用を受けると考えられ、例えば、ヒアリング先の DPA によると、第 22 条の適用範囲となるため、企業の契約履行を法的根拠とすべき、とのことである。

③：従業員の性格的な特徴と給料等に基づき、マネージャーが人事評価を行う際の参考材料生成

【運用状況】

勤務時間、有給取得状況、既往歴といったデータからプロファイリングを行い、評価に活用するケース、従業員の特徴と給料等をプロファイリングし、各マネージャーに共有するケースなどが確認された。

【法的根拠】

従業員の評価にプロファイリングが使われる場合、従業員との雇用契約が法的根拠になると想定される。オランダのヒアリングでは、この運用は従業員との契約において必要なプロセスであるとのコメントを得た。

④：事務作業のミス検知

【運用状況】

ベルギーの金融機関へのヒアリングで、ミスを犯した従業員の情報からプロファイリングを行い、今後のミスの防止に活用する運用事例が確認された。なお、当該プロファイリングの実施時には、匿名化したデータが用いられている[2]。

【法的根拠】

この運用は事業者の正当な利益が法的根拠となっている。

⑤：従業員の業務状況の把握

【運用状況】

スペインの法律事務所によると、PC の操作履歴の取得や、GPS 等による従業員の現在位置の監視なども行われている。

[2] これは、ベルギーにおいて、従業員のモニタリングが厳格に規制されていることによる。

【法的根拠】

ヒアリングでは法的根拠について明確なコメントを得られなかったが、従業員に対しては、一般に、雇用者との立場の違いゆえに自由な意思に基づくものであることが必要な同意を取得することが困難であるため、④と同様に事業者の正当な利益が法的根拠となっていると想定される。

（4）今後想定されるプロファイリング

本調査のヒアリングでは、今は顕在化していないが、今後想定されうるプロファイリングの具体例が指摘された。例えば、英国の法律事務所によると、医療分野等では、人的なバイアスを低減することができるという意味で、機械による自動化された意思決定が今後診断で活用される可能性がある、というコメントを得た。

また、同じく英国の法律事務所より、特定消費者に対して web コンテンツのアクセス制限を設け、例えば子供が有害な web サイトへアクセスすることを未然に防いだり、ギャンブルに強い関心を持つ人が不用意にギャンブル関連の web サイトへアクセスしないよう保護したりする、といった用途へのプロファイリング活用の可能性を指摘された。

（5）データ主体からの苦情の状況

上述のとおり、EU 企業においてプロファイリングは広く利用されているが、調査対象国の DPA によれば、プロファイリングに関するデータ主体からの苦情は、アクセスの権利や保存期間に関するものと比べ、相対的にそれほど多く寄せられていない。

データ主体からの苦情が少ない背景について、DPA はプロファイリングの実施をデータ主体がよく分かっていないことが原因にあると考えている。データ主体は、自らの行動が期待どおりに実を結ばなかった又は不利益な取扱いを受けたと感じたタイミングで DPA に苦情を寄せるが、その後の DPA の調査によって初めて企業によるプロファイリングの実施が判明することが多いという。このように、プロファイリング行為は、外形的に認知しづらいという性質があり、透明性の確保や同意取得の実施が十分でないことが苦情の原因となっていると DPA は考えている。

（6）DPIA の実施状況

調査の結果、プロファイリングの実施有無に関らず[3]多くの EU 企業において、個人データの取扱いに当たり、DPIA を実施していることが判明した[4]。ヒアリング先の通信会社によれば、新規プロジェクトの開始前に DPIA の対象となるか否かを判断しており、この際、

[3] ただし、ヒアリングを行った法律事務所の多くは、プロファイリングを実施する場合は、データ主体への侵害性が高まるため、DPIA の実施を助言しているとのことである。

[4] ヒアリング先企業、業界団体及び弁護士等の専門家からの聴取結果に基づく記述であり、企業規模、分野により実施状況の濃淡があるものと考えられる。

機微情報である通話情報を取り扱う場合はすべてDPIAの対象としているとのことである。このように自社の基準を設けて実施の判断を行っている企業も見られた。

DPIAの実施に当たっては、法務・ITの部署の担当者がチームを組み、DPOがチームに助言する形で実施している。

第3節　プロファイリングのEU企業にとっての課題認識

本節では主として現地調査を通じて判明したプロファイリングに関するEU企業の課題認識を紹介する。紹介する課題認識は本調査のヒアリング先企業、業界団体及び弁護士等の専門家によるもので、調査対象国のEU企業の総体が同様の認識にあるか検証が済んでいるものではない点に留意する必要がある。

プロファイリングに関するEU企業の課題認識として次の3点が挙げられる。

①　管理者の正当な利益を法的根拠とするマーケティング目的での
**　　プロファイリングの実施可否**
②　GDPR第22条の適用を受けるプロファイリングを含む取扱いの適切な運用の仕方
③　今後、人工知能の発展が見込まれる中での自然人の介在の仕方

①について、マーケティング（特にオンラインでのダイレクトマーケティング）を目的としたプロファイリングはEU企業において広く利用されている。取扱いの法的根拠として、データ主体から同意を取得する企業と正当な利益を根拠とする企業があり、対応は個社によって異なる。GDPR前文47には、「ダイレクトマーケティングのための個人データの取扱いは、正当な利益のために行われるものとみなされうる。[5]」という記述があるが、他方で、マーケティングを目的としたプロファイリングの実施に当たり、データ主体からの同意取得が全く必要ないか、という点については専門家でも意見が分かれており、企業は判断に苦慮している。

この点に関して調査対象国において、各国で企業の対応が異なる点も見られる。例えば、イタリアではGDPR施行以前は個人データの統計処理に関する行動規範（Code of Conduct）において、プロファイリングに当たり同意取得が求められていた[6]。そのため、イタリア企業はマーケティング目的の場合においても例外なく同意取得を行っており、その慣習がGDPR施行後も依然として残っているとのことである。

また、スペインの企業によれば、スペインでは、正当な利益に基づくマーケティングが認められる場合として、マーケティングを自分の既存の顧客を対象に実施する場合があると考えられている。このような場合であれば、企業は既に顧客から個人データの取得と一

[5] 原文では「The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.」と表現されている。
[6] 文書自体は、現在は参照不可。イタリアのDPA、現地法律事務所及び企業の複数ヒアリング先からの聴取内容に基づき記載。

定の利用目的に関する同意を取っているため、侵害性が小さいためである。例えば、既存の顧客に、購入した商品の新しいモデルを紹介する場合等が、正当な利益が認められる典型例である。

GDPR の施行後、日が浅いこともあり、実務における考え方の統一が図られていない点が伺える。

②について、GDPR 第 22 条の適用対象となるプロファイリングを含む取扱いは同意、契約の履行若しくは締結への必要又は所定の条件を満たす EU 法若しくは加盟国の国内法で認められていることのいずれかの場合にのみ認められており、正当な利益を法的根拠とするのみの取扱いは許容されない。また、データ主体から同意を取得するに当たっても、「明示的な同意を取得すること」（GDPR 第 22 条）と GDPR 第 6 条における同意と区別した形での同意取得が求められており、明示的な同意取得の実務的な対応方法が浸透していない状況において、実質的に GDPR 第 22 条の適用対象となるプロファイリングを含む取扱いは、契約の履行若しくは締結への必要が認められるか、又は所定の条件を満たす EU 法若しくは加盟国の国内法で認められている場合でしか実施することができず、厳しい制限がかかっている状況に EU 企業は不満に感じている。

③について、近年、人工知能の発展により特定の取扱いにおいては、意思決定のプロセスを完全に自動化しても、自然人が関与しても、結果は変わらない、又は機械に判断を委ねたほうが精度の高い意思決定ができうる状況を踏まえ、GDPR では実効性のある形での自然人の介在の仕方が規定されていないとして、課題に感じている状況が確認された。

第 4 節　プロファイリングの DPA にとっての課題認識

調査対象国の DPA がプロファイリングについて抱いている課題認識として次の 3 点が挙げられる。

① 業界ごとのガイダンスの必要性
② 企業による透明性の確保
③ 違反時の立証の難しさ

①について、第 2 節のとおり、プロファイリングは対象とするデータ主体や利用される分野によって、様々な取扱いがされている。こうした状況は DPA も把握するところであり、現地 DPA によれば、法執行に当たっては業界等の特性を加味した運用方針を検討する必要を感じている。

②は企業に対し過大な負荷をかけることなく、どうやって透明性の確保を図るよう求めるかという点である。この点に関して、多角的な取組として、イギリスの DPA では人工

知能を用いたアプリケーションを監査するフレームワークの起草を行っている。フレームワークは人工知能を用いたアプリケーションが透明で公正であることを確認するための確立された方法論を考案することを目的としている[7]。

③は②に関連する課題であるが、ある企業において、消費者が企業の web サイトにアクセスする際用いているスマートフォン端末の機種に基づき、その消費者の富裕度を判定して[8]提示商品の価格を変更していたと仮定する。そうした取扱いの違法性を証明するに当たっては、類似する属性の消費者がスマートフォンの機種を除く同一の条件のもと商品の価格を確認するといった綿密な調査を要することになる。このように技術が高度化する中での違法なプロファイリングの検知に難しさを感じている。

なお、調査の結果、人種、政治的意見・信条、生体データ等の特別な種類の個人データをインプットとするプロファイリングや、同データを推知する目的で行うプロファイリングについて DPA が喫緊、認識している課題は確認されなかった。

第 5 節　日本企業への示唆

プロファイリングの運用状況及び企業・DPA の課題認識を踏まえ、日本企業がプロファイリングを行う際、参考となる考え方を整理した。整理に当たっては、第 1 節で確認した各プロファイリング規制に対応する形でとりまとめを行っている（図表 6）。

実務的な示唆としては、プロファイリングに関してデータ主体から DPA に寄せられている苦情は相対的には多くなく、EU ではプロファイリングも個人データの取扱いの 1 つであると企業及び DPA に捉えられている、という考え方から検討を始めることが有益であろう。したがって、取扱いの一類型であるプロファイリングを実施する場合、先ずは、どのような種類の個人データをどの程度用い、どのような利用目的で取り扱うか明らかにしなければならない。また、同時にここでは GDPR 第 6 条における取扱いの法的根拠を明確にしておく必要がある。複数種類の取扱いの法的根拠が考えられるのは既に述べたとおりである。

また、取扱いに当たってはデータ主体の権利に適切に対応することが求められる。主には、データ主体に対し取扱いについて情報提供を行い、データ主体からの請求（個人データへのアクセス、個人データの訂正・消去・取扱いの制限及び取扱いに対する異議）に対応することが想定される。

さらに、取扱いがプロファイリングを含むもっぱら自動化された意思決定であり、かつ

---

[7] イギリスの DPA におけるフレームワークの検討に関して、次の記事が参考になる。
https://ai-auditingframework.blogspot.com/2019/03/simon-mcdougall-director-for-technology.html

[8] 例えば、最新の高額機種を用いてアクセスしている場合は、富裕度合いが高いと判定される。

取扱いの結果がデータ主体に対して法的効果又は同様の重大な影響を及ぼすと思われる場合、GDPR 第 22 条の適用対象となるか考慮が必要となる。仮に適用対象になると認識される場合、取扱いの法的根拠によっては追加的な要件を充足する必要が生じる点に留意する必要がある。

なお、プロファイリングの実施有無に限らず、EU 企業において DPIA は広く実施されており、プロファイリングの実施に当たっての検討プロセスについても、DPO からの助言を得つつ、DPIA 等を通じて継続的に検討されるものである。

図表 6　日本企業がプロファイリングを行う際、参考となる考え方

規制	運用状況・課題意識に基づく考え方
第 5 条：基本原則 第 6 条： 取扱いの適法性 第 9 条： 特別な種類の個人データの取扱い	・ 第 2 節において整理したプロファイリングを各法的根拠に基づき EU 企業は実施している。 ・ プロファイリングに関してデータ主体から DPA に寄せられている苦情は相対的には多くなく、EU 企業・DPA においてプロファイリングも個人データの取扱いの 1 つであると認識されている。 ・ マーケティングを目的としたプロファイリングの実施に当たっては、同意を要するか、正当な利益のみを法的根拠としてよいかについて、専門家の間でも意見が分かれている。さらに、各国の解釈も微妙に異なっており、例えばスペインでは、DPA を含め、既存の顧客については正当な利益を根拠としてこれに基づいてマーケティングを実施している。他方、イタリアでは DPA により、事実上同意を必須とする運用が行われている。 ・ 本調査のヒアリング先にメディア・医療関係企業を含んでいない点は留意が必要だが、調査の結果、人種、政治的意見・信条、生体データ等の特別種類の個人データをインプットとするプロファイリングや、同データを推知する目的で行うプロファイリングは確認されなかった。プロファイリングに関する DPA の課題認識として、そのような取扱いについて言及がされなかった状況に鑑みると、企業による実施の有無は別として、EU において現状、重大な問題として俎上に挙げられている状況にはないことが伺われる。
第 13-14 条： 情報提供を受ける権利	・ 調査対象国の DPA によれば、プロファイリングは個人データの取扱いの態様の 1 つに過ぎず、プロファイリングについて、特出した形での通知を行う指導は行っていない。なお、GDPR 第 21 条への対応の仕方は後述する。
第 15 条： アクセスの権利	・ 調査の結果、プロファイリングに関してデータ主体がアクセスの権利（いわゆる開示請求権）を行使することは、生じていないことが判明した。他方で、プロファイリングに特化しない形の開示請求全般は多く寄せられており、企業としては他の個人データと併せて対応を図っている。

規制	運用状況・課題意識に基づく考え方
第 16-18 条： 訂正・消去・取扱いの制限の権利	・ 開示請求と同様にプロファイリングに特化した消去請求はデータ主体から寄せられていないが、他の個人データを含めた消去請求は発生しており、企業として対応が求められている。
第 21 条： 異議を述べる権利	・ 仮に正当な利益を法的根拠としてプロファイリングを行っている場合、GDPR 第 21 条では、異議を述べる権利について、明示的にデータ主体の注意を引くようにされ、かつ、他の情報とは明確に分けて表示されなければならないと規定されている。異議を述べる権利についてデータ主体への通知に当たっては、EDPB が示している透明性のガイドライン[9]が参考になる。方法は複数あるが、例えば、異議を申し立てる権利について明確に示すとは、階層を分けることが該当する。DPA によれば、文章のパラグラフを分けることもこれに対応していると考えられる。実際にこの対応を図っていると考えられる EU 企業のプライバシーポリシーを図表 7 において例示する。 ・ なお、実際に GDPR 第 21 条に基づき異議を述べる権利を行使した状況は本調査において確認されなかった。
第 22 条： プロファイリングを含む個人に対する自動化された意思決定	・ 調査対象国において、GDPR 第 22 条の適用対象として認識されている主な取扱いは第 2 節における整理のとおりである。 ・ 一般的なプロファイリングが個人データの取扱いの態様の 1 つとして特別視されていないのに対し、GDPR 第 22 条の適用については EU 企業においても意識されている。ベルギーの金融機関によれば、GDPR 第 22 条に該当しうる取扱いはなるべく避けようとしているとのことである。これは、GDPR 第 22 条の適用対象となるプロファイリングを含む取扱いが、現状は非常に限定された場合でのみ運用されている状況を裏付けるものといえる。 ・ GDPR 第 22 条の適用について、①取扱いがプロファイリングを含むもっぱら自動化された意思決定に該当する、②取扱いの結果がデータ主体に対して法的効果（又は同様の重大な影響）を及ぼす、の両方を満たすこ

[9] Guidelines on Transparency under Regulation 2016/679 (wp260rev.01)　同ガイドラインは第 29 条作業部会により採択されたものを 2018 年 5 月 25 日 EDPB においても追認されている。

規制	運用状況・課題意識に基づく考え方
	とが条件となるが、採用時にプロファイリングを行う企業においては、採否の判断は人事担当者が行っているため①に該当せず、結果として適用対象とはならないと認識しており、他方で、ダイレクトマーケティングを行う企業においてはマーケティングの結果が②に該当しないため、適用対象とはならないと認識している。このようにいずれかの条件に該当しないため、GDPR 第 22 条の適用対象とならないと整理している企業も多い。 ・ GDPR 第 22 条の適用可能性について、DPA によれば、適用対象となるか否かは自然人の関与が意味あるものかどうかによって判断される。データの取扱いのプロセスの中において、意味ある決定の前にプロファイリングが位置しているならば問題ないが、プロファイリングの後にそうしたプロセスがないならば、取扱いの見直しを行わねばならないとのことである。DPA によっては、基準を人間が作成していれば、それを当てはめて判断する作業そのものは完全に機械化されていても第 22 条の対象とはならないとの解釈を取っているところもある。 ・ また、イギリスの DPA では「GDPR 第 22 条の適用対象となる場合にすべきこと」という名目で Web サイト上にガイダンス[10]を公表しており、企業の判断、理解を支援している。
第 35 条： データ保護影響評価 第 37-39 条： データ保護オフィサー	・ GDPR で求められる水準どおりとまではいかないが、多くの企業において DPIA が実施されている。これはプロファイリングの実施有無によらず個人データの取扱いにおける通常の保護措置として受け止められている。 ・ DPO は DPIA に当たり、評価者、アドバイザなどの第三者的立場で関与を行っている。

[10] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-else-do-we-need-to-consider-if-article-22-applies/

図表 7　EU 企業のプライバシーポリシーにおける通知内容（例）

事業者名	Klarna（スウェーデン）
事業者の概要	・ 2005 年にスウェーデンのストックホルムにおいて設立。 ・ オンラインショッピング時の後払い決済サービスを提供。 ・ 2019 年時点で 14 カ国（独、英、オランダ等）において操業。加盟店数 10 万、ユーザ数 6,000 万人。 ・ 2017 年の売上高は約 26.5 億米ドル。
プロファイリング内容	・ ユーザが入力した個人情報（メールアドレス、氏名、住所等）から取得した信用情報及び過去の購買履歴を分析し、ユーザの購入決定時点での商品の発送（後払いでの決済が可能）を行っている。
プライバシーポリシーにおける説明内容	・ プライバシーポリシー[11]において、プロファイリングに関して、以下の説明を実施 **Profiling and automated decision making.** “Profiling” means automated processing of personal data to evaluate certain personal aspects relating to you to for example analyse or predict aspects of your economic situation or your preferences. We profile the data we have on you to decide what marketing content that would be interesting to you (and you can of course always object to such marketing). To effectively and responsibly handle credit applications, we also profile your data if you apply for a credit. “Automated decision making” means that we offer certain services such as granting you credit solely based on automatic means, without any interaction from any of our employees. By making this automated we increase objectivity and transparency when offering those services. These decisions are based on your purchase history and earlier payments to us, together with information about you received from credit reference. You always have the right to challenge an automated decision and get a Klarna employee to look at your case.

11 http://cdn.klarna.com/1.0/shared/content/legal/terms/Klarna/en_gb/privacy （2019 年 3 月 20 日アクセス）

第 3 章　データポータビリティ

第 1 節　データポータビリティに関連する法的義務

GDPR 第 20 条によれば、データ主体は、管理者に対し、同意又は契約に基づくものであり、自動化された手段によって行われる取扱いに対して、自己が管理者に対して提供した自己と関係する個人データを移転する権利を有する（いわゆるデータポータビリティ権）。

この権利の趣旨について、EU データ保護指令[12]において規定され、また GDPR にも引き継がれているアクセスの権利においては、データの形式が管理者の指定するそれに制約されていたところ、データポータビリティ権のように IT システムで容易に利用可能な形式と指定することで、データ主体がより自らのデータに対する権利行使を拡大させることが可能になる点が、ガイドラインにおいて指摘されている[13]。

ここで、同条によれば、データポータビリティ権とは 2 つの種類の権利である。第一は、同条第 1 項にあるとおり管理者から、構造化され一般的に利用され機械可読性のある形式で受け取り、それを妨害されることなく他の管理者に移行する権利であり、第二は第一の権利の加重型であり、同条第 2 項にある「技術的に可能な場合、（データ主体を介さず）直接に管理者間での移転させる権利」である。本書では第一の場合を「①間接移転型」、後者の場合を「②直接移転型」と呼ぶこととする。

ガイドラインでは、間接型の例として、例えば音楽ソフトのプレイリストや電子メールサービスの連絡先（アドレス帳）をユーザーが機械判読可能な形で受け取り、自ら利用するといった事例が挙げられている。

また、前文 68 によれば、「管理者は、データポータビリティを可能とする相互運用可能なフォーマットの開発を奨励されなければならない」とされ、管理者の自主的な取組が奨励されると共に、奨励されなければならない（should be encouraged to）との文言から、DPA 等においてもフォーマットの策定を管理者に対して積極的に働きかけていく必要性が認められる可能性もある。実際、EU の一部の DPA ではそのような解釈を取っているところもある。

以上のように、データポータビリティ権に関しては、GDPR 第 20 条と前文 68 がその中核をなすが、他方、GDPR の他の関連規定を参照して、体系的・一体的に理解する必要がある。

まず、データポータビリティ権に対応するデータの保管期限の問題がある。この点、ガイドラインは、データポータビリティ権に対応するために、GDPR 上一般に、すなわち同第 5

---

12 「個人データ取扱いに係る個人の保護及び当該データの自由な移動に関する 1995 年 10 月 24 日の欧州議会及び理事会の 95/46/EC 指令（Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data）」

13 「データポータビリティの権利に関するガイドライン」（個人情報保護委員会仮訳）、5 頁

条で必要とされる以上に保管期限を延長する必要はない点を指摘している[14]。

また、同様に削除権に基づく削除請求がなされた場合にも、データポータビリティ権の行使を理由にそれを妨げてはならない。

次に、データポータビリティ権を実現するに当たって、特にデータの取扱いを委託している場合には委託先の協力が必要となることもある。GDPR 上、データの取扱いに際して、管理者と処理者は GDPR 第 28 条に規定される一定の義務を含めたデータ処理契約（Data Processing Agreement）を締結する必要があり、ここでは管理者がデータ主体の権利を実現するに当たって処理者が必要な技術的及び組織的措置に基づく協力を行う義務が定められている。

また、直接移転型において、データ主体の移転要求に基づいて新たに個人データを取得した事業者もまた、管理者となる。そのため、第 5 条における義務を遵守すると共に、第 14 条に基づいて通知を行う義務が課される。

以上を念頭に、より実務的に重要な留意点について述べたい。事業者にとって重要な点として、データポータビリティ権は、法文から明らかなとおり、特定の法的根拠に基づく、特定のデータに対してのみ行使できるという点である。

第一に、法令上、対象となるデータの取扱いは、同意又は契約に基づくものに限られる。例えば、金融機関がマネーロンダリングの防止に関して個人データを取り扱った場合には、（この場合の取扱いの法的根拠は金融関連法令に基づく義務の遵守又は正当な利益であるから）データポータビリティ権の対象とはならない。同様に、従業員データの取扱いについても、例えば法令上の義務に基づく場合には適用されない。

第二に、対象となるデータは「データ主体が管理者に提供した」「自己と関係する」個人データである。匿名化されている場合には、「自己と関係する」個人データとはいいがたいため、対象とならない。他方、発着信記録などは第三者の情報も含まれていても本人に関連するデータといえる。

次に、データ主体が管理者に提供した、という点が問題になる。ガイドラインによれば、これは単にユーザーが自発的に提供したデータのみならず、ユーザーの行動を管理者が観察した結果として生じたデータ、例えば検索履歴、位置情報等をも含むものとされている。これは、このようにデータの範囲を拡大しなければ、データ主体の十全な権利行使が確保できないためである。

ただし、管理者がユーザーからの提供データを元に加工、分析等を加えたデータについては、データポータビリティ権の対象とならない。これらはユーザーが「提供した」とはいいがたいためである。このようなデータの例として、心拍数や歩行数などを元に管理者が分析

[14] データポータビリティの権利に関するガイドライン」（個人情報保護委員会仮訳）、10-11 頁

した健康状態の評価や、同じく資産などから管理者が分析した信用リスクの評価等が該当する。

以上をまとめると、データポータビリティ権の対象となるデータは、図表8のとおりとなる。

図表 8　データポータビリティの対象となるデータ

区分	概要	データ例	ポータビリティ権の対象
①提供データ	データ主体が主体的かつ認識して提供したデータ	氏名、住所、メールアドレス	○
②観察データ	サービス又は機器を利用する事でデータ主体が提供したデータ	検索履歴、交通データ	○
③推定・派生データ	①、②を元にデータ管理者が作成したデータ	健康状態の評価、信用評価	×

以上のほか、データが営業秘密や知的財産権の保護に該当する場合には、当該データを除くデータについて、データ主体に対してデータポータビリティ権を実現させる必要がある点にも留意する必要がある[15]。

第 2 節　EU 企業のデータポータビリティ権の対応状況

次に、第 1 節で述べた法的義務を元にした、EU 企業におけるデータポータビリティ権への対応状況について概観したい。ただし、弊社が 2019 年 1 月～2 月に実施した EU 諸国での現地調査によれば、EU 企業においては、データポータビリティ権の請求がほとんどないという点に留意する必要がある。これは、そもそもデータポータビリティ権が GDPR で初めて導入された権利であり、データ主体の同権の認知が十分行き渡っていないこと、アクセスの権利に比べて権利の範囲が限定されていること、データを機械判読可能な形で入手したとしてもユーザーがそれを活用する用途が限られていること、といった理由が挙げられよう。

このように限定された請求数に対応すれば十分であるため、データポータビリティ権の実務については、現地でも洗練されたものがあるとはいえず、たぶんに手探りの状態で履行されているというのが現状である。以下の記載はこの現状を念頭に置いて理解する必要がある点に留意していただきたい。

15 「データポータビリティの権利に関するガイドライン」（個人情報保護委員会仮訳）、25 頁

データポータビリティ権の行使に対応するには、まず適切にデータの所在を把握していくことから始まる。これが欠けては、請求を受けるたびにデータの所在を全社で確認して対応することが必要になり、非常に手間がかかるためである。多くの場合、EU 企業では、データマッピングを実施することから始めている。これはデータポータビリティ権の行使に対応するために実施するものではなく、GDPR の他の義務の履行、例えば第 30 条で要求される台帳の整備や DPIA を実施する過程で結果的に実施されるものである。加えていえば、データマッピングは、データポータビリティ権よりも対象とする個人データの範囲の広いアクセスの権利への対応のために、そもそも必要なものである。

したがって多くの EU 企業の場合、データマッピングは実施済みという段階からデータポータビリティ権への対応が開始される。なお、データマッピングの方法については、EU と日本とで変わるところがない。すなわち、もし任命されていれば DPO の助言のもと、法務又は IT の担当部門が質問票の作成・配布などを通じて各部署のデータの処理、保管状況や第三者移転の状態などを把握し、それを集約するという流れが一般的である。

（1）間接移転型

間接移転型については、通常のアクセスの権利に基づく請求と異なるところが少なく、実質的にはデータを機械判読可能な形で提供するなど、GDPR 第 20 条に規定された一定の要件を満たす形でユーザーに開示（送付）すれば足りる。したがって、業務フローも基本的にはアクセスの権利に基づく請求と同一であり、対応窓口を設置し、当該窓口が社内の関連データを収集して、ユーザーに対し送付を行う形となる場合が一般的である。

まず対応窓口であるが、DPO やそのサポートスタッフが担う場合、法務部門が担う場合等があり、会社の状態によって異なっている。このような対応窓口がユーザーとのやり取りを実施することとなるが、既にデータマッピングが実施されているため、ある程度手間をかけずに社内のどこにユーザーに関連するデータが存在しているかが判明している状態となっている。そこで、窓口役の部署がユーザーデータを取りまとめて返送することとなる。

ここでは本人確認を実施することとなるが、ID の発行等を通じて既にユーザーの本人確認を実施している場合は不要であり、他方、新規に本人確認を実施する場合には一定の公的証明書（国民 ID カード、パスポートなど）を要求する場合が多い。

また、個人データ全てだと対象がかなり広範になる場合もあり、その場合、開示対象となるデータについて、ユーザーに対して特定を求める場合もある。例えば、標準的な開示項目をあらかじめユーザーに提示し、それに足りないものを追加でユーザーに特定してもらうことで業務負荷を削減している場合等がそれに当たる。

こうして開示先のデータ主体を確認し、必要なデータを特定すると、次はデータの送付に移ることとなる。データの形式は通例、元となったデータベースの形式をそのまま送付することが多く、例えば csv 形式や Excel 形式、最近では json 形式などが採用されている。

送付形態としては電子メールでの送付が多いが、個人データを送付することとなるため、暗号化などの安全管理措置を施しておくことが一般的である。

また、特にセキュリティ意識の高い企業においては、請求件数が少ないこともあり、暗号化したUSBメモリに格納し、配達記録が可能な郵送で実施する、としているところもあるが、その場合は対応に係る人件費も含め、一回の請求で数万円程度の経費がかかっている。これが今後件数の増加がなされた場合にも対応できるかは不明である。

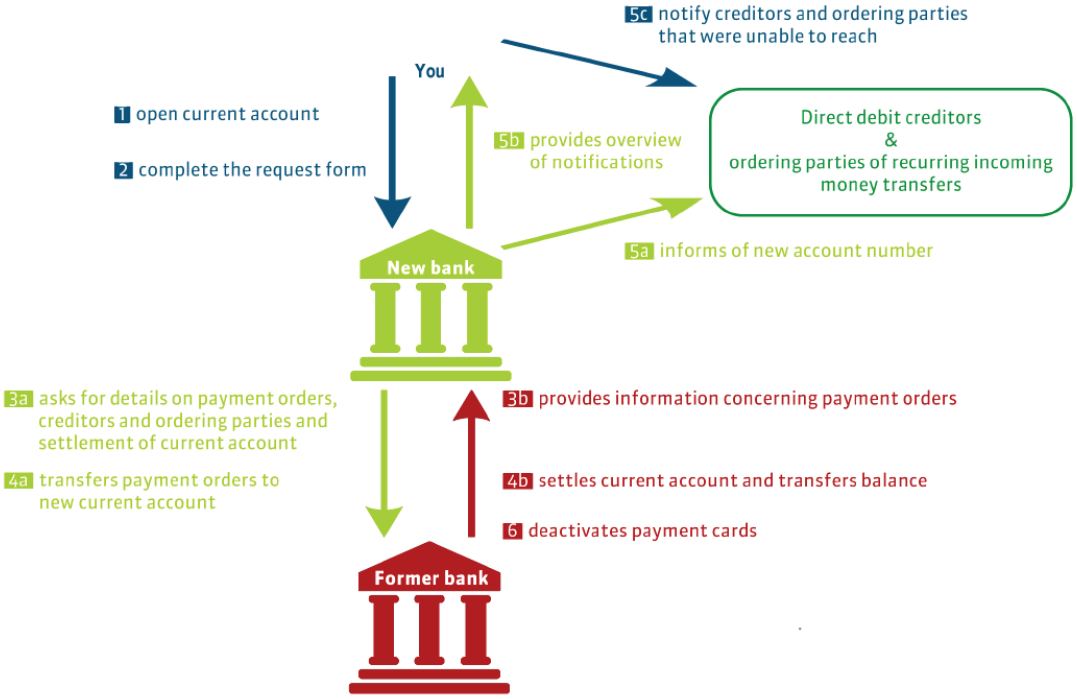
以上、EU企業の対応状況について概略を取りまとめた。現在のEU企業の業務体制は、大企業であっても、1企業当たり数件～十数件程度の対応が出来る業務フローであるため、これが件数の増加を経た場合にどの程度機能するかは未知数である点には留意する必要がある。

（2）直接移転型

直接移転型は、金融や通信等、あらかじめデータフォーマットが統一されている限定された業種間においてのみ、萌芽的な事例が見られる。

GDPRが施行されるよりも前から、国内でのユーザーの利便性の拡大といった、他の政策目的実現のために導入された事例がある。例えばベルギーでは銀行口座間の乗り換えが、携帯電話の番号同様にスムーズに実施できる、"Bank Switch"と呼ばれるサービスが国内法レベルで導入されており、これが頻繁に利用されているとのことである。具体的なサービスの流れは図表9を参照いただきたい。

図表 9　ベルギーの口座の銀行間移転サービス Bank Switch の流れ[16]



また、個別企業によるポータビリティ実現の取組も生じつつある。例えば Google や Facebook、Twitter などの米系 IT 企業が 2017 年より取り組んでいる"Data Transfer Project"や[17]、スペイン Telefonica がドイツテレコム等と、通信会社がデータ移転のハブになるための協業を発表した事例がある[18]。

また、フランス等においてはパーソナルデータストア（PDS）を目指して、個人データ流通のハブを目指そうとする事業者も出てきている。ヒアリングによれば、同社が他のサービス提供者から顧客データを移転する際には、自社にデータを蓄えることのメリットを説明し、顧客にデータポータビリティ権の行使をしてもらうことでパーソナルデータを集約しているとのことであった。このように、PDS への集約を容易にしてデータ流通を促進するという役割がデータポータビリティ権にあることは事実であり、将来的にはこのような動きが広がる可能性がある点には留意する必要があろう。

第 3 節　データポータビリティ権の EU 企業にとっての課題認識

調査の結果、多くの EU 企業においてデータポータビリティ権への対応は十分洗練されたものとはなっていないことが判明した。その背景及び EU 企業の課題認識として、下記の 2 点が指摘できる。

---

16 https://www.ing.be/assets/nuid/documents/Bankswitching-EN-2018-as_a_private_customer.pdf
17 https://datatransferproject.dev/
18 https://www.gsma.com/gsmaeurope/resources/secured_data_hub/

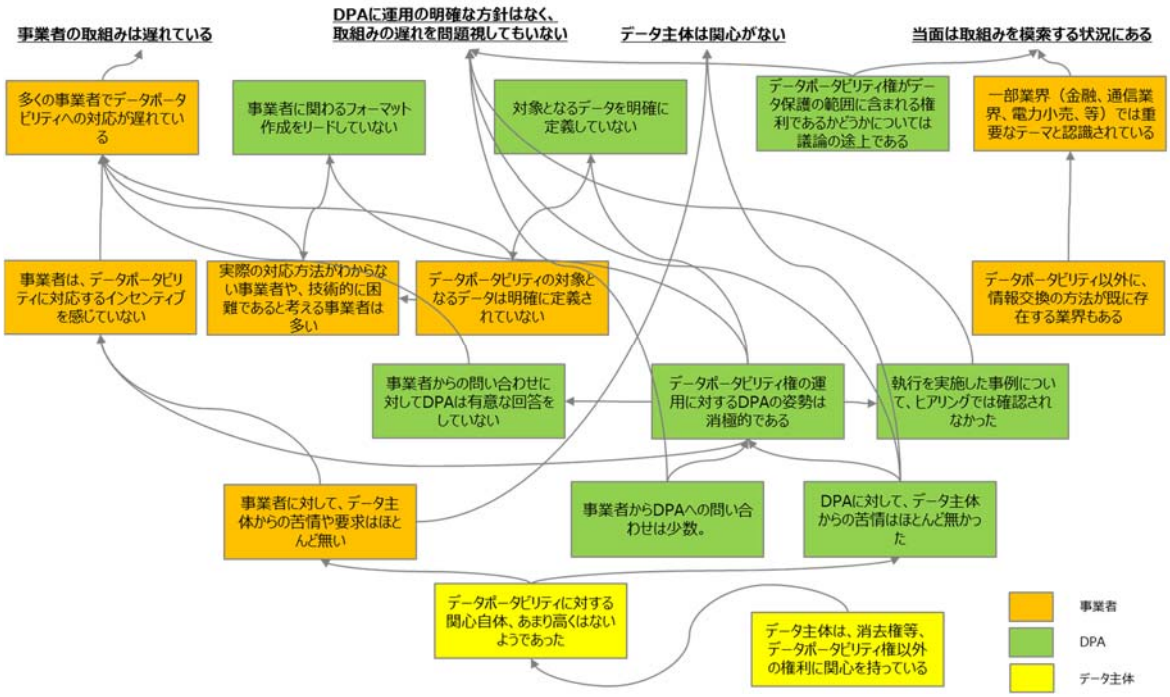
① データポータビリティ権に対応するインセンティブを感じていない

② 実際の対応方法がわからないあるいは対応が困難である

①データポータビリティ権に対応するインセンティブを感じていない理由として、前述のとおり、EU 企業がデータ主体からデータポータビリティ権に関する苦情や請求を受ける事例はほとんど無かった。既に豊富な件数のあるアクセスの権利の行使に比べると、非常に数が限られるというのが実態である。これは、データ主体自身も、データポータビリティ権に関する知識や関心がほとんど無いという状況であることが一因として考えられる。さらに、EU の DPA も、苦情が寄せられる件数の少なさなどから、データポータビリティ権の義務違反に対して、それを積極的に取り締まろうという姿勢は見られない。企業、データ主体、DPA がそれぞれに関心を寄せない結果、現時点では、EU においてデータポータビリティ権はまだほとんど問題になっていないといえよう。

以上を整理すると次の図表のようになり、出発点としてデータ主体のデータポータビリティ権に対する関心が高くないことが、現在の状況を生み出していることが明らかになる。

図表 10　データポータビリティが問題となっていない状況の構図



②実際の対応方法がわからない、あるいは対応が困難である理由として、EU において（業界単位であっても）データポータビリティ権の対象となるデータは、まだ明確に定義されていないことがわかった。どのようなデータを対象とし、データ主体に提供するべきなのかは、多くの企業及び法律事務所において検討中の事項であった。また、調査を行った DPA においても、対象となるデータを明確に定義していなかった。

なお、前述のとおり、GDPR のガイドラインにおいては、データ主体により提供されたデータ（provided data）と、観察データ（observed data）をデータポータビリティ権の対象となる個人データとしている。対照的に、推定データ（inferred data）や派生データ（derived data）はデータポータビリティ権の範囲には含まれないとしている。しかし、EU 企業の中には、データポータビリティ権の対象を推定データや派生データまで広げている企業もあった。もっとも、これはユーザーの便宜のため自主的に対応しているものである。

また、特に直接移転型のデータポータビリティ権の実現に当たっては、データを移動させる際の統一されたフォーマットの作成が進んでいないことも、対応が困難である理由の一つであった。例えば、データ主体へデータを提供する際、どのようなデータフォーマットで用意すればよいかわからない企業がほとんどということであった。他の企業へ移す際にも企業間でフォーマットが異なるため、統合が難しいという企業もいた。また、データが体系化されていないため、必要なデータを探し出すことが容易ではないという企業もいた。なお、こうした状況に対して、GDPR の前文 68 で示されているように、DPA が企業に関わるフォーマット作成を奨励するような状況は見られなかった。

ただし、金融、通信、SNS、電力小売等、一部の業界においては重要なテーマと認識されていた。これらの業界では、GDPR 施行以前からデータを交換する方法が存在している場合が多い。金融業界では PSD2（決済サービス指令：Payment Service Directive 2）が標準的なデータ交換方法として確立されている。また、通信業界では、通信会社の切り替え後も、同じ電話番号を引き続き使用できるよう、ナンバーポータビリティ（Number Portability）という制度が既に存在している。既にデータの交換が行われているこれらの業界では、データポータビリティ権の検討が先行しやすいようであった。逆にいえば、データポータビリティ権の導入によってデータの移行が進んだ、という事例はきわめて限られている。

第 4 節　データポータビリティ権の DPA にとっての課題認識

端的にいえば、DPA はポータビリティ権に対する関心は低く、それを問題視することもない、というのが実態である。

EU の DPA において、データポータビリティ権への対応は優先順位が高く位置づけられているわけではない。これは主にデータ主体からの苦情が多くない点に起因していると思われる。結果、一部の DPA においては対象となるデータの範囲について内部で議論しているものの、企業間でデータポータビリティを進める統一フォーマットの作成をリードするに至る DPA は存在しない、といった状況であった。

一方で、調査を行った DPA において、データポータビリティ権への検討が遅れていることを問題視する様子は見られなかった。また、データポータビリティ権に関して DPA が執行を実施した事例について、本調査では確認されなかった。さらに、このように EU 全体としてデータポータビリティ権に関する議論が発展途上である点を捉え、一部 DPA では当面の間データポータビリティ権に関する事案については執行を控える姿勢を明らかにするところもあった。

また、データポータビリティ権自体、データ保護に係る権利としてのみ捉えてよいかどうか、議論の余地があることがわかった。本調査では、データポータビリティ権により、サービスプロバイダを変えられるようになることで、企業間の競争が促進されることや、消費者のより自由なサービスプロバイダの選択が可能になるといったことがいくつかの DPA において指摘された。仮にデータポータビリティ権が企業間の競争の促進や消費者の保護に繋がるのであれば、そうした点は DPA のみが考慮すべきものではなく、例えば消費者保護や競争といった他の関連当局との連携にもつながっていく可能性がある。データポータビリティ権は、具体的な対応からその権利の位置付けまで当面の間、取組を模索する段階にあると考えられる。

本調査を行った DPA のうち、一部の現地 DPA においては、データポータビリティ権の対象となるデータについて、より深い議論が行われていた。

第 3 節でも述べたように、GDPR のガイドラインにおいては、データ主体により提供さ

れたデータ及び観察されたデータがデータポータビリティ権の対象となると述べられている。しかし、同 DPA は観察されたデータを、データポータビリティ権の対象に含めるかどうかについて慎重な態度をとっていた。同 DPA によれば、位置情報等、予備的に多くのデータをデータポータビリティ権の対象とすることで、データ主体のプライバシーに係るデータが企業に蓄積され、かえってデータ主体を危険にさらす可能性があるということであり、この点はガイドラインの見解と異なる。同 DPA は、観察データを一様のものとみなすのではなく、レベルを分けて更に詳細な議論を行っていく必要があると指摘していた。

なお、今回調査を行った各国においては、これまでに述べてきたとおり、いずれもデータポータビリティ権の行使が少ない結果、検討も十分進んでいるとはいいがたい状況であるが、一部の国においては、当該権利と経済成長の関係についてのレポートが公表されたり、一部の事業者が自主的に取り組んでいたりするといった状況が観察された。

第 5 節　日本企業への示唆

以上を踏まえ、日本企業への示唆を取りまとめたい。まず指摘すべきは、第 3 節、第 4 節で指摘したとおり、データポータビリティ権については EU 企業や DPA でも運用上、十分にルールが確立されていない。日本企業にとっては、まず EU の状況を把握することが重要であり、具体的な対策は EU において実務が固まってから施しても遅くはないと推察される。以下は、日本企業が具体的な対策を進める上での現時点での実務に基づく示唆である点に留意いただきたい。

第 2 節で述べたとおり、日本企業は EU 企業に比べ、DPIA や台帳（第 2 節で解説した GDPR 第 30 条を参照）の整備が十分ではなく、スタートラインとしてのデータマッピングの実施状況が大きく異なっている点である。したがって、日本企業はまず、データマッピングを適切に実施する必要がある。

（1）データマッピングとシステム的な対応の可能性検討

データマッピングの手法自体は既に公開されているものも多く、一般的には、第 2 節で解説したとおり、主管部やチームが自社に応じた各部署宛の調査票を作成し、データの種類や取扱いの法的根拠といったものを中心に、どのデータベースにおいて、どの程度の情報が保管され、それを誰が管理しているか把握していくこととなる。

この過程では、主幹部やチーム（通例はコンプライアンスを担う法務部やシステムの現状に詳しい IT システムの担当部署からなる混成チーム）を定め、DPO 等の助言を得つつ進めていくこととなる。ただし、一度の回答で全容が把握できるわけではなく、多くの場合、個別部署へのヒアリングも必要となってくる。なお、このようなデータマッピングについて EU 企業では数ヶ月程度で実施できることが一般的であるとの見解が聞かれた。また、DPIA を実施する場合にも同様の手順が必要となるため、DPIA とあわせて実施する

ことも有効である。

次に、上記のプロセスをシステム的に落とし込むことも考慮に値する。例えば、このような過程を元に、EU 企業においては連携システムを介す等して自社のデータベースを一元的に管理できるようなシステムを構築しているところもあった。日本企業においても検討に値する手法であろう。このようなシステム的な一元化を実現することは、単にデータポータビリティ権への対応を進めるだけでなく、自社のデータをより統合的に活用できることにつながり、ビジネスを成長させる投資としても一考に値するように思われる（実際、EU 企業もこのような攻めの考え方を元にデータベースを統合している企業もある）。

（2）業務フローの設計

データマッピング実施後に、業務フローの設計を行う。ここでは、データ主体からの問い合わせを受ける担当部署を決定するが、第 2 節で述べたとおりデータポータビリティ権はアクセスの権利に類似する対応が求められるため、通例はアクセスの権利に基づく請求（開示請求）への対応の担当がそのままデータポータビリティ権への対応を担うことが効率的であると思われる。両者の違いはデータ主体に対して開示するデータの範囲と送付形式であって、これらを自社内で取り決めておく必要がある。

データの範囲については、第 2 節、第 3 節で述べたとおり、どの範囲までを対象とするかの判断が、ガイドラインや DPA においても一致しているわけではない。氏名やメールアドレス等のデータ主体が意図的かつ明示的に提供したデータが対象となることは間違いないが、どこまでが観察データで、どこまでが推定・派生データであるか、といった区分は曖昧なまま残されているため、当座、ガイドラインに沿ってデータ区分に関する検討を実施しておくことが安全であると思われる。

この点、データポータビリティ権では、データ主体の権利行使と事業者の経済的な負担や、持っているノウハウ等の無形財産の保護との間で、適切なバランスを考慮する必要がある。ここでは、自社にとって対応のコスト、さらされるビジネスリスク（営業秘密や知的財産等が含まれるか等）を勘案しつつ、ユーザーが納得する対応をすることが重要である。他方、第 1 節で引用した GDPR ガイドラインにおいて、本権利への十全な対応には、ある程度、「提供した」という文言の範囲を広く捉える傾向が記載されている点に留意しつつ対応を進めていく必要があるだろう。

また、データポータビリティ権の行使対象は、取扱いの法的根拠が「契約」と「同意」に限られている点にも留意すべきであり、たとえば「正当な利益」などに基づく場合には対応は不要である。

さらに、データポータビリティ権に対応するために保存期間などを変更する必要が無い点も、ガイドライン指摘のとおりである。

（3）業務のモニタリング

現在 EU においてもこの段階にある企業はほとんどなく、未知数であるが、企業側としては将来の件数増加に備えて、受付件数や標準的な処理期間など、適切な運営がなされているか、また、継続的な改善を促すためのモニタリングの仕組みを備えておく必要が、一般的には指摘できよう。

おわりに

日本と EU との間における個人情報の移転を相互に促進する枠組み（いわゆる「十分性認定」の枠組み。）が、2019 年 1 月 23 日に運用を開始し、我が国の個人情報保護制度は名実ともに、グローバルにおいて高い水準にあることが国内外に示された。その発足以来、EU と粘り強く交渉を重ねてきた個人情報保護委員会及び関係機関の努力が実を結んだといえよう。

十分性認定によって、EU と同等の保護水準にあると認められた我が国の個人情報保護制度ではあるが、個別の規定レベルでは、当然のことながら、文化・社会・歴史といった背景を異にする EU の法である GDPR との間には多くの差異がある。本調査では、それら差異のうち、特に我が国において言及されることの多い、プロファイリング規制とデータポータビリティ権の二つを取り上げ、基礎となる法制度を整理するとともに、DPA や法律事務所による解釈、EU 企業の具体的なプラクティスを調べ、日本企業への示唆として取りまとめた。

GDPR は既に施行済みではあるものの、両テーマについては、いずれも DPA において、現在進行形で適切な取扱いについて検討が続けられており、技術の進展や社会の変容に応じて対応方針は変わってくるものと想定される。事実、調査を通じて、DPA をはじめ、主体ごとに規定に対する解釈や対応の仕方に大きな幅があり、それぞれ試行錯誤しながらも、創意工夫して対応している実態が明らかとなった。このため、本報告書の内容は、あくまでも現時点における整理として参照いただきたい。

日系企業のプラクティスへの示唆という意味では、弊社の方で最大公約数的に整理を行いつつ、弊社が過去に実施した日本企業の GDPR 対応支援の知見を交えて、日本企業の抱える課題解決に資するようにとりまとめを実施した。詳細な現地調査で収集したファクトからは、欧州における GDPR 対応の現状を感じ取っていただける内容となっているのではないかと考えている。

末尾となったが、ヒアリングに応じて本報告書のために貴重な時間を割いていただき、多くの有益なご知見を提供くださった全ての皆様に感謝し、そのご協力に敬意を表したい。本報告書が日本企業の GDPR 対応、ひいては我が国の個人情報保護制度の充実の一助となれば幸いである。