資料２－１

個人情報保護を巡る国内外の動向
（GDPRの運用・対応状況）

令和元年９月12日

目次

※ 本資料は、株式会社野村総合研究所調査「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」（個人情報保護委員会委託調査）をもとに作成。

1．調査内容

- 2018年度、EUにおけるGDPRの運用及び実態について外部委託調査を実施。
- 具体的には、GDPRにおいて新たに導入された**プロファイリング**、**データポータビリティの権利**について、EUのデータ保護機関・企業の動向を調査。

（1）プロファイリングについて

- EUの各国企業で**どのように運用**されているか、及びデータ保護機関・企業における**課題意識**についてヒアリング。
  - ✓ **データの「取扱い」が許容される法的根拠**（GDPR第6条：取扱いの適法性）について、「同意」、「契約の履行又は締結」、「法的義務の遵守」、「生命に関する利益の保護」、「職務の遂行」、「正当な利益」のいずれに基づいているか。
  - ✓ **異議を述べる権利**（GDPR第21条）についての対応状況。
  - ✓ **プロファイリングを含むもっぱら自動化された取扱い**（GDPR第22条）の適用対象となるか。
  - ✓ その他関連する規制（GDPR第15条アクセスの権利、第16条訂正の権利、第17条忘れられる権利、第35条データ保護影響評価　等）への対応状況。

（2）データポータビリティの権利について（GDPR第20条）

- EUの各国企業で**どのように運用**されているか、及びデータ保護機関・企業における**課題意識**についてヒアリング。

【調査対象機関】

- 9か国のデータ保護機関、企業、法律事務所、業界団体、シンクタンク計40以上。
  - ※　英国、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
  - ※　うちデータ保護機関は6か国：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

2．プロファイリング

（1）GDPRにおけるプロファイリングの位置付け

- プロファイリングの概念（第４条に定義）は、個人を評価するために分析・予測する、あらゆる形式の自動的な取扱いと大変広いが、「データ処理の一つの方法であり、必ずしも追加的な保護措置が必要というわけではなく、第６条に定める取扱いの法的根拠を含め、企業がアカウンタビリティを果たすべきもの＜欧州データ保護機関＞」と理解されている。

- その上で、第22条において、「法的効果を発生させる」又は「重大な影響を及ぼす」プロファイリングを含むもっぱら自動化された取扱いに基づく決定の対象とならないことを権利として規定。

  ただし、その例外として次の根拠を認めている。
  - ✓ 契約の締結又はその履行のために必要となる場合。
  - ✓ EU法又は国内法によって認められる場合。
  - ✓ 明示的な同意に基づく場合。

2．プロファイリング

（2）EU企業が行っているプロファイリングの事例・対応及び課題認識

- 同じ個人データの取扱いの場合でも、企業やデータ保護機関が認識する法的根拠に違いがあるなど、**対応は様々であり、EU企業側も説明責任を果たすため試行錯誤**している様子がうかがえる。
- プロファイリングに関するデータ主体からの**苦情は相対的に多くない**。また、**異議を述べる権利**（GDPR第21条）**を行使した状況は本調査で確認されなかった**。

EUで多くみられるプロファイリングの事例

○ **与信目的**

正当な利益の目的又は法的義務を遵守することを根拠として行われており、外部から入手したデータを利用する例もある。現状では、人間の判断が皆無というケースはあまりなく、第22条の対象とはみなされていない。

○ **採用目的**

同意、正当な利益、あるいは契約の履行又は締結に必要な場合を根拠に行われているが、人間が関与することにより、第22条の対象ではないと解しているケースもある。

○ **マーケティング**

同意又は正当な利益を根拠に行われているが、「法的効果」を生じない範囲で行われていれば、第22条の対象とはならない。

2．プロファイリング

EU企業等の課題認識の例

① マーケティングを目的としたプロファイリングについて

- マーケティングを目的としたプロファイリングの法的根拠として、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。
- プロファイリングについて、データ保護方針等で説明を行うことにより、これまでのところ問題とはなっておらず、利用者とのコミュニケーションが重要との見方をする業者もある。

② 「もっぱら自動化された取扱い」について

- 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方が精度の高い意思決定がなされる可能性がある。

  ⇒ GDPRでは、データ主体の権利保護のための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いう指摘もある

③ 自動化された意思決定の結果が与える影響等について

- どのようなデータに基づきそのような意思決定が下されたのかを問うことができるはずで、自動化された意思決定の内容を正したり、確認したりすることは必要な権利であると認識されているものの、第22条の問題点は、正当な利益による処理を禁止したこととの見方もあり、人的介入の必要性が小さくなるとともに、正当な利益を法的根拠にするプロファイリングへのニーズは高まっているとの意見がある。
- 第22条の例外規定は、AIや機械学習の競争に影響を及ぼしているのではないかとの見方もある。

2．プロファイリング

（3）データ保護機関にとっての課題認識

- 規制当局も、**執行のしづらさなどを含め、課題を認識し、試行錯誤している**様子がうかがえる。

① プロファイリングの全体的課題

- プロファイリングについて、顧客には目的や用途を明確に伝えなければならない。そのためには、データ収集を行う前に、安全管理措置を施さなければならない。プロファイリングは、EU各国においても新しい規定であるため、まさに今、手探りの中で対応している最中の事案である。

② 企業による透明性の確保

- データ保護機関は、企業に対し過大な負荷をかけることなく、どのように透明性の確保を図るよう企業に求めるかという点に苦慮している。

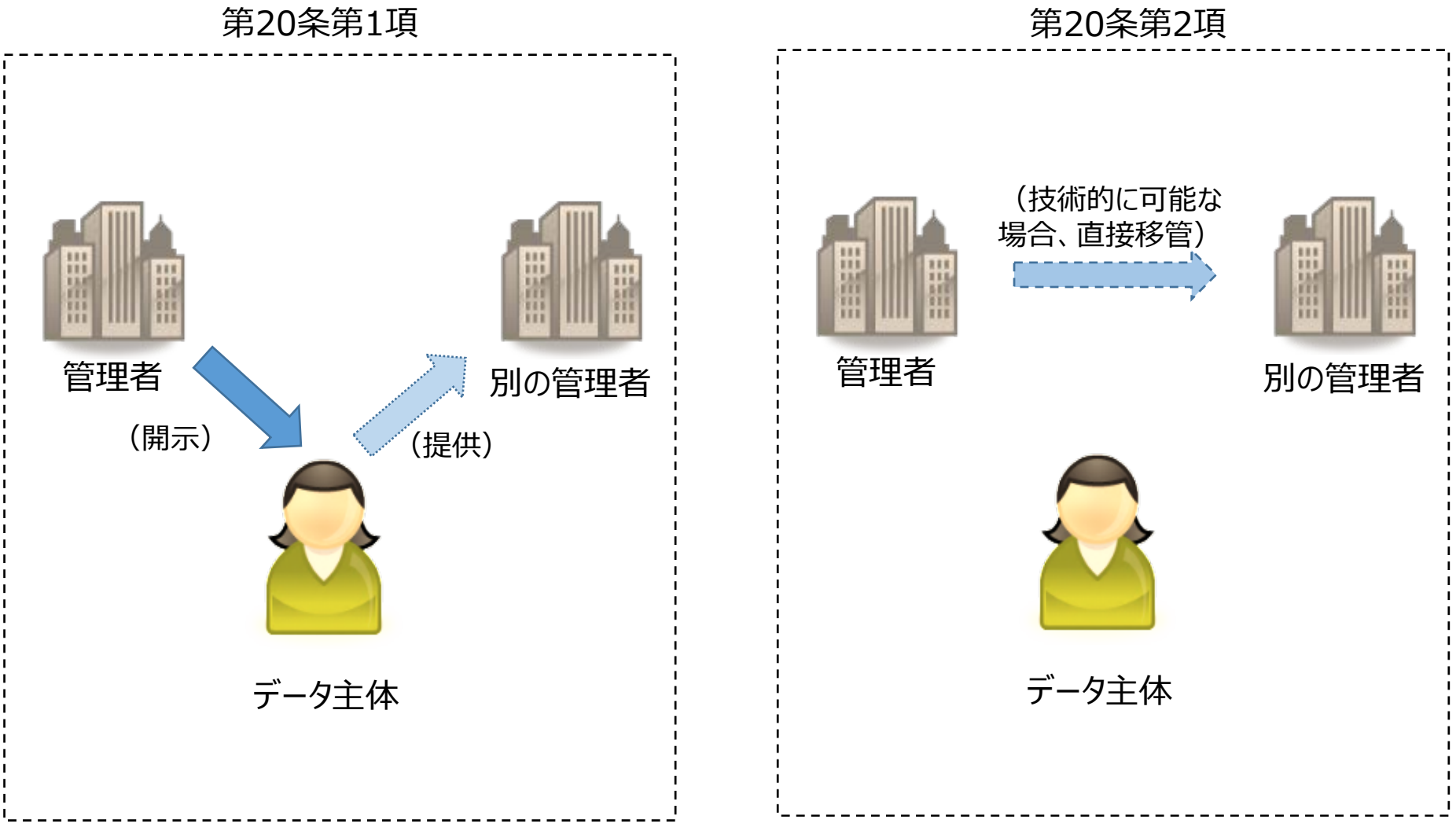
③ 法違反時の立証の難しさ

- 技術が高度化する中で、プロファイリングの実態把握の難しさを感じている。

3. データポータビリティの権利

（1）GDPRの制度概要（イメージ）

＜構造化され、一般的に利用され機械可読性のある形式で＞



3．データポータビリティの権利

（2）EU企業の対応・課題認識

- EU企業においては、**データポータビリティの権利の行使をほとんど受けていない**。
- データポータビリティの権利への対応には、未だ広く適用できる標準的手法が確立されておらず、**手探りの状態で履行**されているが、データポータビリティの権利のみならず、GDPR全体の義務履行等のため、データマッピング（データの所在を把握し管理等行う作業）を実施することにより、データポータビリティの権利への対応も行うなど、**試行錯誤しているEU企業もある**。

（背景と見られる事情）

① 企業はデータポータビリティの権利に対応するインセンティブを感じていない。

- ✓ 企業にデータポータビリティの権利に関する苦情や請求を受けた事例がほとんどない。
- ✓ データ主体にもデータポータビリティの権利についての知識、関心がほとんどない。

② 対応する方法がわからない、あるいは対応が困難。

- ✓ 対象となるデータについて明確に定義されておらず、多くの企業において検討中の状況。
  - ➢ なお、ガイドラインにおいて「提供されたデータ」、「観察データ」 は対象となるとされている一方、「推定データ」、「派生データ」は範囲に含まれないとされているところ、ユーザーの便宜のため自主的に対象を後者にまで広げている企業もある。
- ✓ 移行するデータの形式が統一化されていない。

- なお、金融・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。
  - ➢ 金融業界には、決済関係のデータ交換の規定が存在（「決済サービス指令」(Payment Service Directive 2)）
  - ➢ 通信業界には、通信会社の切替後に電話番号の変更なく継続できる枠組みが存在（「ナンバー・ポータビリティ制度」）。

3. データポータビリティの権利

（3）データ保護機関にとっての課題認識

- データ保護機関のデータポータビリティの権利への対応は、優先順位が高く位置づけられているわけではない状況。
- 規制当局においても、具体的な対応から権利の位置付けまで、当面の間、**取組みを模索する段階**にあると考えられる。

- 一部のデータ保護機関は、データポータビリティの権利に関する議論が途上である点を捉え、当面、データポータビリティの権利に関する事案については執行を控える姿勢を明らかにした。
- データポータビリティの権利の対象については、データ保護機関の間でも様々議論がなされていることがうかがえる。
  - ガイドラインにおいて「観察データ」（位置情報等）もデータポータビリティの権利の対象となるとされている一方、一部のデータ保護機関は、位置情報について、データ主体が提供したものではなく企業が獲得したデータであると指摘している。
  - 一部のデータ保護機関は、GDPR（前文68）では、データ保護機関から業界に対して働きかけるということが読み取れる表現になっているが、特定の業界に対して働きかけている事例は聞いたことがないと指摘している。

3. データポータビリティの権利

（4）民間における自主的な取組み

- 我が国の情報銀行と同様に、本人の関与によりデータの移転を円滑にする仕組みが運用されている事例がある。

事例

- 12年前に始まったサービスでは、データの取得等、全て同意に基づき、個人がwebダッシュボード上でデータを管理して、利用者は自らの情報を何らかの価値（金銭、情報から得られる経験やコミュニケーション等）に交換することができる。データは匿名化（anonymization）した形で取り扱われ、利用者がアカウントを削除すれば、クラウド上のデータも消去される。

- 個人向けのパーソナルデータストア（PDS）に近いもので、個人はデータを移転したり取り戻したりすることのできる、GDPRの権利に則ったモジュールサービス。また、アクセス権や消去する権利・ポータビリティ権を容易に行使することができる。複数企業にばらばらに分散している個人のデータを、まとめて的確に管理することも可能にしている。

4. GDPR関連条文：第4、6条　（個人情報保護委員会日本語仮訳）

第4条 定義

(4) 「プロファイリング」とは、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を意味する。

第6条 取扱いの適法性

1. 取扱いは、以下の少なくとも一つが適用される場合においてのみ、その範囲内で、適法である：
   (a) データ主体が、一つ又は複数の特定の目的のための自己の個人データの取扱いに関し、同意を与えた場合。
   (b) 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。
   (c) 管理者が服する法的義務を遵守するために取扱いが必要となる場合。
   (d) データ主体又は他の自然人の生命に関する利益を保護するために取扱いが必要となる場合。
   (e) 公共の利益において、又は、管理者に与えられた公的な権限の行使において行われる職務の遂行のために取扱いが必要となる場合。
   (f) 管理者によって、又は、第三者によって求められる正当な利益の目的のために取扱いが必要となる場合。ただし、その利益よりも、個人データの保護を求めるデータ主体の利益並びに基本的な権利及び自由のほうが優先する場合、特に、そのデータ主体が子どもである場合を除く。

第1項(f)は、公的機関によってその職務の遂行のために行われる取扱いには適用されない。

2. 加盟国は、第1項(c)及び(e)を遵守する取扱いに関し、第9章に定めるその他の特別の取扱いの状況に関する場合を含め、適法かつ公正な取扱いを確保するため、取扱いのためのより詳細で細目的な要件及びその他の措置を定めることによって、本規則の規定の適用を調整するためのより細目的な条項を維持し、又は、これを導入できる。

3. 第1項(c)及び(e)に定める取扱いのための根拠は、以下によって定められる：
   (a) EU法。又は、
   (b) 管理者が服する加盟国の国内法。

取扱いの目的は、その法的根拠に従って決定され、又は、第1項(e)に定める取扱いに関しては、公共の利益において、若しくは、管理者に与えられた公的な権限の行使において行われる職務の遂行のために必要なものとする。その法的根拠は、本規則の規定の適用を調整するための特別の条項を含みうる。特に、管理者による取扱いの適法性を規律する一般的な条件、取扱いの対象となるデータの種類、関係するデータ主体、個人データが開示されうる組織及びその目的、目的の限定、記録保存期間、並びに、第9章中に定めるその他の特別の取扱いの状況のための措置のような適法かつ公正な取扱いを確保するための措置を含めた取扱業務及び取扱手続を含めることができる。EU法又は加盟国の国内法は、公共の利益の目的に適合するものであり、かつ、その求める正当な目的と比例的なものとする。

4. GDPR関連条文：第6、20条　（個人情報保護委員会日本語仮訳）

第6条 取扱いの適法性（続き）

4. 個人データが収集された目的以外の目的のための取扱いが、データ主体の同意に基づくものではなく、又は、第23条第1項に定める対象を保護するために民主主義の社会において必要かつ比例的な手段を構成するEU法若しくは加盟国の国内法に基づくものではない場合、管理者は、別の目的のための取扱いが、その個人データが当初に収集された目的と適合するか否かを確認するため、特に、以下を考慮に入れる。

(a) 個人データが収集された目的と予定されている追加的取扱いの目的との間の関連性。

(b) 特にデータ主体と管理者との間の関係と関連して、その個人データが収集された経緯。

(c) 個人データの性質、特に、第9条により、特別な種類の個人データが取扱われるのか否か、又は、第10条により、有罪判決又は犯罪行為と関係する個人データが取扱われるのか否か。

(d) 予定されている追加的取扱いの結果としてデータ主体に発生する可能性のある事態。

(e) 適切な保護措置の存在。これには、暗号化又は仮名化を含むことができる。

第20条　データポータビリティの権利

1. データ主体は、以下の場合においては、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、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る権利をもち、また、その個人データの提供を受けた管理者から妨げられることなく、別の管理者に対し、それらの個人データを移行する権利を有する。

(a) その取扱いが第6条第1項(a)若しくは第9条第2項(a)による同意、又は、第6条第1項(b)による契約に基づくものであり。かつ、

(b) その取扱いが自動化された手段によって行われる場合。

2. データ主体は、第1 項により自己のデータポータビリティの権利を行使する際、技術的に実行可能な場合、ある管理者から別の管理者へと直接に個人データを移行させる権利を有する。

3. 本条の第1項に規定する権利の行使は、第17条を妨げない。この権利は、公共の利益において、又は、管理者に与えられた公的な権限の行使において行われる職務の遂行のために必要となる取扱いには適用されない。

4. 第1項に規定する権利は、他の者の権利及び自由に不利な影響を及ぼしてはならない。

4. GDPR関連条文：第21、22条　（個人情報保護委員会日本語仮訳）

第21条　異議を述べる権利

1. データ主体は、自己の特別な状況と関連する根拠に基づき、第6 条第1 項(e)又は(f)に基づいて行われる自己と関係する個人データの取扱いに対し、それらの条項に基づくプロファイリングの場合を含め、いつでも、異議を述べる権利を有する。管理者は、データ主体の利益、権利及び自由よりも優先する取扱いについて、又は、訴えの提起及び攻撃防御について、やむをえない正当な根拠があることをその管理者が証明しない限り、以後、その個人データの取扱いをしない。

2. 個人データがダイレクトマーケティングの目的のために取扱われる場合、データ主体は、いつでも、そのようなマーケティングのための自己に関係する個人データの取扱いに対して、異議を述べる権利を有する。その取扱いは、そのようなダイレクトマーケティングと関係する範囲内で、プロファイリングを含む。

3. データ主体がダイレクトマーケティングの目的のための取扱いに対して異議を述べる場合、その個人データは、そのような目的のために取扱われてはならない。

4. 遅くともデータ主体への最初の連絡の時点で、第1 項及び第2 項に規定する権利は、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。

5. 情報社会サービスの利用の過程において、かつ、指令2002/58/EC にかかわらず、データ主体は、技術的な仕様を用いる自動化された仕組みによって異議を述べる自己の権利を行使できる。

6. 第89 条第1 項により科学的研究若しくは歴史的研究の目的又は統計の目的で個人データが取扱われる場合、データ主体は、公共の利益のための理由によって行われる職務の遂行のためにその取扱いが必要となる場合を除き、自己の特別な状況と関連する根拠に基づき、自己と関係する個人データの取扱いに対して、異議を述べる権利を有する。

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

1. データ主体は、当該データ主体に関する法的効果を発生させる、又は、当該データ主体に対して同様の重大な影響を及ぼすプロファイリングを含むもっぱら自動化された取扱いに基づいた決定の対象とされない権利を有する。

2. 第1項は、以下のいずれかの決定には、適用されない。

(a) データ主体とデータの管理者の間の契約の締結又はその履行のために必要となる場合。

(b) 管理者がそれに服し、かつ、データ主体の権利及び自由並びに正当な利益の安全性を確保するための適切な措置も定めるEU法又は加盟国の国内法によって認められる場合。又は、

(c) データ主体の明示的な同意に基づく場合。

3. 第2項(a)及び(c)に規定する場合においては、そのデータの管理者は、データ主体の権利及び自由並びに正当な利益、少なくとも、管理者の側での人間の関与を得る権利、データ主体の見解を表明する権利及びその決定を争う権利の保護を確保するための適切な措置を実装するものとする。

4. 第9条第2項(a)又は(g)が適用され、かつ、データ主体の権利及び自由並びに正当な利益の保護を確保するための適切な措置が設けられている場合を除き、第2項に規定する決定は、第9条第1項に規定する特別な種類の個人データを基礎としてはならない。