欧州個人データ保護機関による法制度運用の実際


奥見紗和子


南島安平

CONTENTS

要 約

1 EU（欧州連合）における「GDPR（EU一般データ保護規則）」の施行に伴い、加盟各国に所在する監督機関は、監督機関同士または29条作業部会が改組した欧州データ保護会議との間で相互に連携を取りながら法執行活動を担うことになる。特に複数の加盟国にまたがる個人データの取り扱いにあたっては、主管監督機関を定め、法執行活動にかかわる窓口が統一される。

2 高額な課徴金ばかりに耳目が集まりがちなGDPRではあるが、監督機関が課徴金の納付命令を下すまでには、法執行活動に関するいくつかのプロセスを経ることが通例である。GDPRの適用後も法執行活動の運用の実態が大きく変わることはないと考えられ、監督機関との対話がないままに、ある日突然、課徴金の納付命令だけが下ることはないと想定される。

3 GDPRに基づく法執行活動について、事業者の理解を促す活動の一環としてGDPRに関するガイドラインが作成・公表されている。本稿ではガイドラインの全体像と、主要トピックである「データポータビリティ」「プロファイリング」「同意」に関するガイドラインのポイントを紹介する。

4 GDPRへの対応方法は、今後公表予定のガイドラインや監督機関の法執行活動の積み重ねを受け、徐々に明確になっていくものと考えられる。欧州の個人データを取り扱う企業は制度施行後も継続的に監督機関の動向を注視するとともに、取り扱いの見直し、拡充に努めることが重要である。

Ⅰ GDPRの制度運用を担う各組織とその関係性

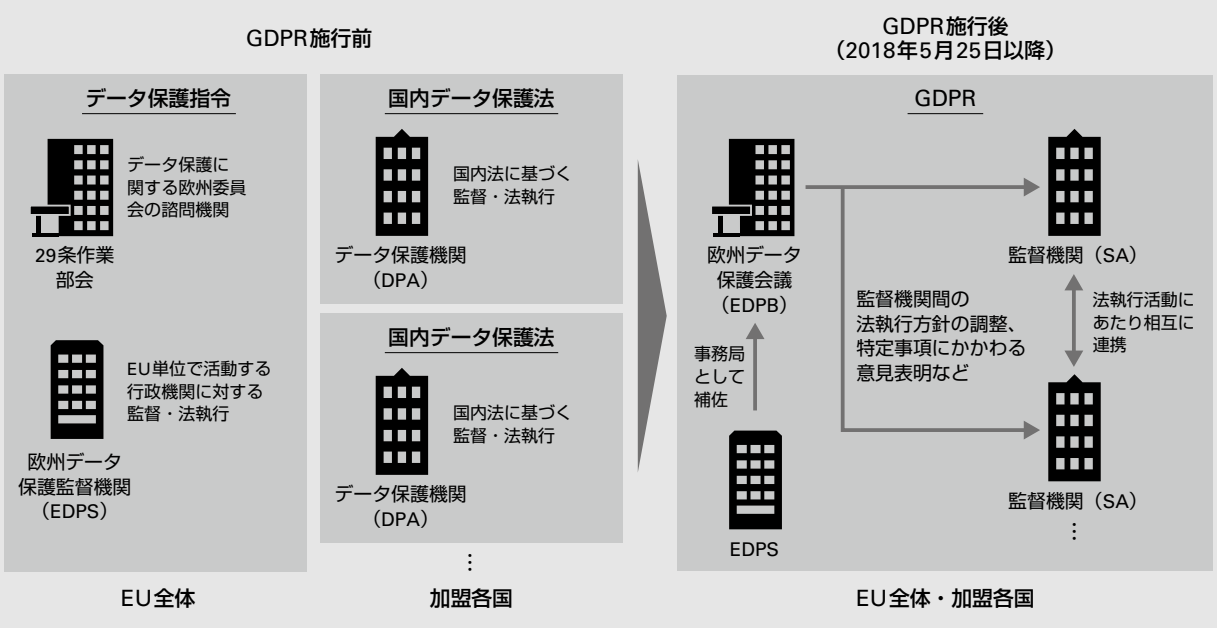
1 法執行体制の変化

EU（欧州連合）において「GDPR（EU一般データ保護規則）」が施行される前は、「データ保護指令[注1]」に基づき、EU加盟各国が独自にデータ保護法を立法し、国内法に基づく法執行活動が行われてきた。法執行活動の担い手は各国のデータ保護機関（DPA：Data Protection Authority）と呼ばれる組織である。データ保護機関は専任の職員を擁し、ほかの行政機関から独立した組織であるが、法執行活動に関するその職務権限は各国によって異なっていた[注2]。

GDPRの施行後は、その統一的な適用を保障するため、加盟各国の監督機関（SA：Su-Supervisory Authority）と呼ばれる組織が法執行活動を担う。監督機関はデータ保護機関が移行する形で組織されたが、その職務権限やメンバーの任命要件などはGDPRにおいて一律に規定されている[注3]。監督機関は1つの加盟国内で複数設置することも認められているが、その場合は当該国の代表機関を設定するとともにそのほかの監督機関を含め、当該国内における統一的な法執行活動を担保する仕組みが求められる。

各監督機関の統一的な法執行活動に寄与するため、新たに「欧州データ保護会議（EDPB: European Data Protection Board）」が組織された。EDPBは各加盟国の監督機関および欧州データ保護監督機関（EDPS：European Data Protection Supervisor）[注4]の長（または代理人）によって構成される。EDPBの業務には、GDPRのガイドラインや個人データ保護に関するベストプラクティスなどの策定・公表に加えて、監督機関間で法執行にかかわる方針が異なる場合の調整や、各監督機関が行動規範や認証機関の認定基準など特定の事項を採択する際の意見表明などがあり、GDPRに基づく統一的な法執行活動における司令塔としての役割が期待されている。な

図1 GDPRの施行に伴う法執行体制の変化



お、EDPBはデータ保護指令に基づき設置されていた29条作業部会に代わる組織として認識されている（図１）。

２　個人データを取り扱う拠点の所在に応じた主管監督機関の設置

仮に、ある事業者がドイツとフランスで個人データを収集し、利用していた場合、データ保護指令の下では、ドイツ・フランスそれぞれのDPAが国内法に基づいて当該事業者を監督していた。今後、GDPRの下では、こうしたデータ管理者または処理者によって行われる国境を越えた取り扱い（以下「越境処理」）については、事業者の監督を主管する監督機関（以下「主管監督機関」）を定めることになる。主管監督機関は関係するEU加盟国の監督機関と協力して、越境処理に関する法執行活動を遂行することが求められる。

越境処理に該当する個人データの処理には２種類ある。１つは複数のEU加盟国の拠点における活動に関連して行われる個人データの処理である。たとえば、ある事業者がフランスとルーマニアに拠点を持ち、フランス住民の個人データを両国において処理するケースが該当する。もう１つは単一の加盟国の拠点で行われるデータ処理ではあるが、複数のEU加盟国の住民に影響を及ぼす、または実質的な影響を及ぼし得るような活動に関連して行われる個人データの処理である。これはたとえば、データ処理自体はフランスの拠点で行われるが、その結果はフランスとルーマニアの住民に影響を及ぼすケースが該当する。

主管監督機関は、原則として越境処理を行う事業者の統括部門が所在するEU加盟国の監督機関が務める。ただし、これは事業者の統括部門が越境処理の目的および手法の決定を行っているという想定に基づくものであり、ほかのEU加盟国に所在する別の拠点がこれを担う場合は柔軟に変更され得る。また、主管監督機関は個人データの取り扱いごとに設定される。これはたとえば、ある金融グループにおいて、銀行業務に関する個人データの処理はドイツの統括部門で意思決定を行っており、保険業務に関する処理のみオーストリアの拠点で意思決定を行っている場合、銀行業務の処理に関する法執行活動はドイツの監督機関が主管監督機関を務め、保険業務に関する処理はオーストリアの監督機関が務めることを意味する。

主管監督機関の設置は、事業者にとって越境処理に関する当局の窓口を集約することができる点でメリットがある。また、データ処理に関する意思決定を行う拠点は、一義的には事業者によって特定することができる[注5]ため、どの加盟国の監督機関を主管監督機関とするかという戦略的な判断の余地は事業者にあると考えられる。

なお、日本企業によってはEU加盟国内の拠点で個人データの取り扱いに関する意思決定を行っていない場合も想定される。この場合は従前の通り、当該取り扱いに関係するデータ主体が居住する加盟国の監督機関が個別に法執行活動を担うことになる[注6]。

Ⅱ　法執行活動のプロセス

高額な課徴金ばかりに耳目が集まりがちなGDPRではあるが、監督機関が課徴金の納付命令を下すまでには、法執行活動に関するいくつかのプロセスを経ることが通例である。

野村総合研究所（NRI）が過去に実施した、DPAによる法執行活動の実態についてのヒアリングを含む調査によれば、各機関ともおおむね共通したプロセスを経ることが判明した（図2）。また、GDPRの適用後も実態が大きく変わることはない模様である。

以下、法執行活動に関する各プロセスを詳述する。

1　苦情受付

監督機関が個人データの取り扱いにかかる苦情（complaints）を受け付けることは、その職務として規定（第57条第1項f号）されているが、GDPRでは受付の方法として電子メールやWebサイト上の問い合わせフォームのような電子的に完了することができる手段を用意することが併せて規定（第57条第2項）されている。

苦情を受け付けた監督機関は法令違反にあたるか判断し、疑いがある場合は必要に応じて調査を行う。なお、調査の進捗状況・結果については合理的な期間内に苦情を申し立てた者に通知する旨が規定されているが、相当数の苦情が未処理のまま翌年度に持ち越されているとのことである[注7]。

2　調査

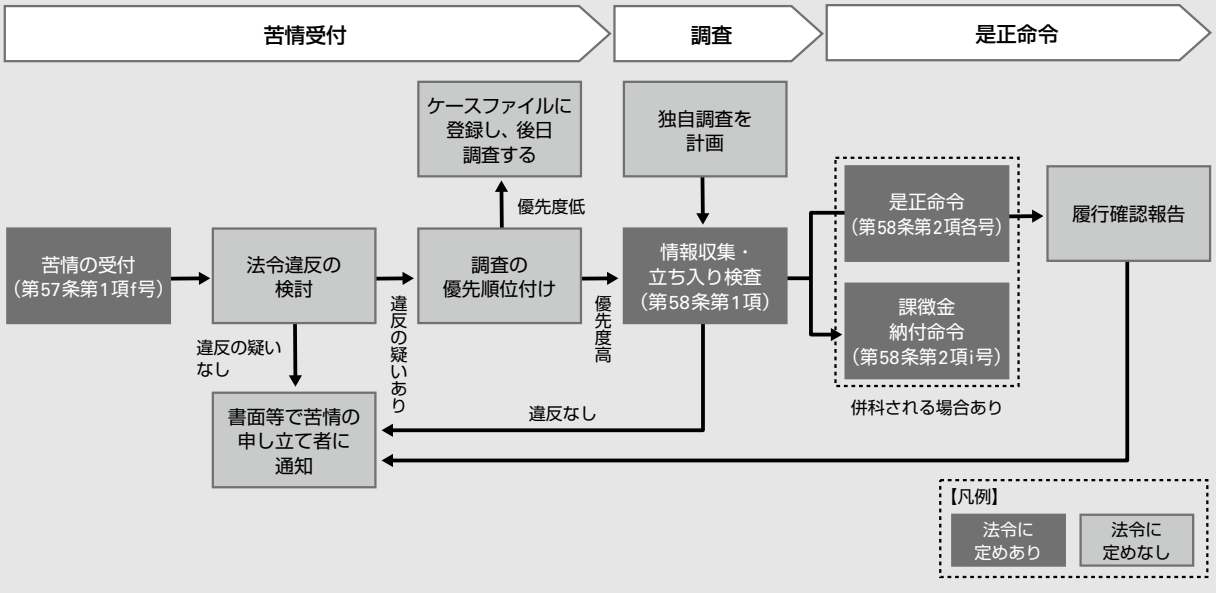
監督機関が行う調査には苦情に基づくものと自主的な調査計画に基づくものとがある。後者は金融や電気通信など大量の個人データの取り扱いが行われていると想定される業界・事業者を特定して行われることが多い。

調査の手法は各監督機関によって異なるが、まず書面による照会をし、回答が不十分と判断される場合は追加の照会や事業所などへの立入検査を行う。

3　是正命令

調査の結果、法令違反の恐れがあると判断される場合は、監督機関は当該管理者または処理者に対して警告を発する（第58条第2項a号）。法令違反と判断される場合は、取り扱いの是正・停止命令を下す。事案内容に応じて課徴金の納付命令が、是正命令に追加ま

図2　法執行活動に関するプロセス



たは代わって行われる。

2018年６月20日、フランスの監督機関であるCNILはWebサイト上の顧客情報を十分に保護していない[注8]として、同国のアイウエア企業Optical Center社に25万ユーロの課徴金納付命令を下した。命令を下した理由としてCNILは、顧客情報にアクセスする前に顧客を確認する機能は今日必須のものであること、および同社が05年にWebセキュリティの欠陥に基づき、５万ユーロの課徴金納付を既に一度命じられていることを挙げている。このように事案内容に加え、過去の違反状況に応じて課徴金額は上昇すると考えられる。

なお、是正命令を受けたデータ管理者または処理者は監督機関に異議を申し立て、司法救済を得る権利を有する（第77条、第78条）。

Ⅲ GDPRガイドラインのポイント

GDPRに基づく法執行活動について、データ管理者および処理者の理解を促す活動の一環として、2016年12月頃より29条作業部会がGDPRに関するガイドラインを作成・公表している。本章ではガイドラインの全体像と、主要トピックのポイントを紹介する。

1 GDPRガイドラインとは

GDPRに関するガイドラインとは、データ管理者および処理者がGDPRを遵守する上でより詳細な説明を必要とする規定について、当該規定に関する補足情報（定義、具体例、解釈方法など）を提示するために、29条作業部会が作成・公表した文書である。2018年７月初めの時点で、11のガイドラインが公表されている（うち、２つが未確定）[注9]。

なお、29条作業部会が18年４月に開催した全体会議（Plenary Meeting）では、11のガイドラインに加えて認証（Certification、第42条関連）、GDPRの適用範囲（The territorial scope of the GDPR、第３条関連）、行動規範（Codes of conduct、第40条、第41条関連）に関するガイドラインの公表準備を継続する旨、合意されている[注10]。今後も必要に応じて追加されていくものと推測される（表１）。

ガイドラインは、テーマにより分量や具体性に差はあるものの、非常に分かりやすく書かれている。すべてのテーマについて紹介したいところであるが、紙面の都合上、本章においては、日本の個人情報保護法では明確に規定されていないGDPRならではのテーマといえる３つ（データポータビリティ、プロファイリング、同意）について概要を紹介したい。

2 データポータビリティ

GDPRの第20条では、個人は以下の２つの「データポータビリティ」に関する権利を有すると規定している。

①データ管理者から自らのデータを扱いやすい電子的な形式で受け取る権利

②あるデータ管理者から別のデータ管理者にデータを移転する権利

①に関してたとえば、音楽のストリーミングサービスを利用する消費者が、特定の曲の視聴回数を知るために、当該ストリーミングサービスから自分のプレイリストや視聴履歴をダウンロードすることが挙げられる。また、②のデータ管理者間の個人データの直接移転に関して、ガイドラインではデータ管理者が相互移転可能なデータフォーマットを開

発することを推奨している[注11]。

こうしたデータポータビリティの権利に関して、権利行使にあたっての原則的な考え方や事業者のデータポータビリティ実現要件についてガイドラインの説明を紹介したい。

あるデータについて次に挙げる3つの基準すべてに該当する場合、当該データはデータポータビリティの権利行使の対象となる[注12]。1つ目は、「個人に関するデータであること」である。つまり匿名データは対象とはならないが、個人と容易に照合可能な場合はデータポータビリティの対象となる。

2つ目は「個人から提供されたデータであること」である。この基準には個人が能動的かつ意図的に提供したデータ（住所、氏名、年齢など）に加えて、サービスまたはデバイスの使用に基づくデータ（検索履歴、位置情報履歴、ウエアラブル端末によって測定される心拍数などのローデータなど）であることも含まれる。ただし、個人から提供されたデータを分析することで、データ管理者によって推定・作成された派生的なデータ（利用者の健康状態の判定結果やクレジットカードの信用スコアリングなど）は権利行使の対象とはならない。

3つ目は、「データポータビリティの権利行使が第三者の権利・自由を侵害しないこと」である。たとえば、通話履歴のようなデータは権利行使を行う本人に加えて、通話先の第三者の個人データを含んでいるが、本人の個人的な利用においてのみ、データポータビリティの権利行使が認められる。

また、ガイドラインでは、データポータビリティに関する一般原則として、以下の4点

表1　2018年7月初めまでに公表されたGDPRに関するガイドライン一覧

No.	対象テーマ	ガイドライン名称	主な関連条項	公表年月日
1	DPIA	Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01)	第35条	2017/10/13
2	データポータビリティ	Guidelines on the right to "data portability" (wp242rev.01)	第20条	2017/10/27
3	DPO	Guidelines on Data Protection Officers ('DPOs') (wp243rev.01)	第37～第39条	2017/10/30
4	主管監督機関	Guidelines on the Lead Supervisory Authority (wp244rev.01)	第60～第62条	2017/10/31
5	課徴金	Guidelines on the application and setting of administrative fines (wp253)	第83条	2018/2/13
6	データ侵害時の対応	Guidelines on Personal data breach notification under Regulation 2016/679 (wp250rev.01)	第33条、第34条	2018/2/13
7	プロファイリング	Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01)	第22条	2018/2/13
8	透明性	Guidelines on Transparency under Regulation 2016/679 (wp260rev.01)	第12～第14条	2018/4/13
9	同意	Guidelines on Consent under Regulation 2016/679 (wp259rev.01)	第4条11項、第6条1項a号、第7条	2018/7/6
10	特定の状況における例外	Guidelines on Article 49 of Regulation 2016/679	第49条	※2018年7月初め時点で未確定
11	認証機関の適合性評価	Guidelines on the accreditation of certification bodies	第43条	※2018年7月初め時点で未確定

を提示している。

①データ管理者はあらかじめ、データポータビリティの権利が存在することを本人に通知する

②個人の識別を行えないことを証明できる場合を除き、データ管理者は本人からのデータ移転要求を断るべきではない

③データ管理者は、遅滞なく、データの移転要求の受領から遅くとも1カ月以内に、本人に求められるデータを提供する[注13]

④データ管理者は、データの移転要求が明らかに不当で過大なもの（特に反復的なもの）と証明できない限り、対応にあたり手数料の請求を行ってはならない

最後に、データポータビリティを実現させるための要件について紹介したい。まず、GDPRでは移転するデータのフォーマットに関して特段の推奨は行っていない。業界ごとに最適なフォーマットの利用が想定されている。共通的なフォーマットがない業界の場合は、一般的に使用されているオープンフォーマット（XML、JSON、CSVなど）を使用して個人データを提供し、可能な限り細かいレベルで有用なデータを提供する必要がある。また、ガイドラインでは、データ量が膨大である場合にも、本人が移転したいデータに容易にアクセスできるように、ダッシュボードを用いるなどの工夫をするよう提案している。

さらにガイドラインでは、データ管理者は個人データを安全に本人に送信する方法（セキュリティ質問などの追加の認証情報やワンタイムパスワードなどの別の認証要素の駆使など）を用いることや、本人が自身の端末で受け取ったデータを安全に保管できるように補助することを推奨している。

以上の通り、GDPRのガイドラインでは、データポータビリティに関する概念や具体例の説明は行っているものの、その実現方法について技術的な制約や義務を課してはいない。この点は、業界標準やベストプラクティスを作り上げていくことで、データポータビリティの実現性がさらに高められていくよう、事業者・業界団体などに期待しているものと推察される。

3　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人格的側面を評価することを目的として、とりわけ当該自然人の業務遂行能力、経済状況、健康、個人的嗜好、興味関心、信頼性、行動、位置および移動に関する分析または予測をするために、個人データの利用によって構成されるすべての形態の個人データの自動的な取り扱いを意味する」と定義している（第4条第4項）。当該定義に基づき、プロファイリングは以下の3要素により構成されると解される。

①処理が自動化されている

②個人データを取り扱う

③自然人の個人的な側面の評価を目的とする

ガイドラインでは上記の3要素のうち、特に「①処理が自動化されている」について詳述している。ガイドラインによれば、自動化された意思決定とは、「自然人による関与を含まない手法」によるものを指す。これはたとえば、自動化処理により生成された信用スコアリングを参考にしつつ、銀行員が住宅ロ

ーンの貸し出し判定を行うことは、自動化された意思決定に該当しないということを意味する。一方で、たとえばカメラ判定に基づき、自動的にスピード違反を検知し摘発することは、自動化された意思決定に該当する。

なお、ガイドラインでは、子どもに対するプロファイリングについて特別に配慮するよう言及している[注14]。たとえばWebの閲覧履歴をプロファイリングしターゲッティング広告を配信する活動について、子どもを対象とする場合は影響が大きいとしてプロファイリングを控えるよう求めている。

4 同意

GDPRによれば、同意とは「自由に与えられ、特定され、事前に説明を受けた上での、その言辞または明確に肯定的な行動により、彼もしくは彼女に関連する個人データの取り扱いの同意を表明するもの」と定義される（第4条第11項）。この定義に基づき、ガイドラインは、下記の同意を4つの要素に分け、説明している。

①（同意が）自由に与えられていること
②（同意が）特定されていること
③（同意が）事前に説明を受けて与えられていること
④（同意が）不明瞭ではない、本人の意思の表示を意味していること

同意に関するガイドラインは、この4つの要素についてかなり詳細に説明や具体例を紹介している。たとえば①については、同意を拒否することで不利益を被る場合や、同意すべき内容の粒度が荒く同意したくない内容も含めて一括同意を求めている場合などは「同意が自由に与えられている」とはいえないと指摘している。また、②に関しては、いわゆるファンクション・クリープ[注15]の事例を取り上げ、同意の目的を明確に、かつ細かく説明するよう要請している。

さらに、④に関しては技術的な側面にまで踏み込んで解説をしている。たとえば、事前にチェックされたオプトインボックスやオプトアウトの設計は、本人の同意プロセスを妨げることから、GDPRでは認められていないと説明している。また、電子的方法により同意を取得する場合には、「クリック疲れ」[注16]による同意メカニズムの持つワーニング機能の低下を念頭に置かなくてはならないと、ガイドラインは指摘している。

最後に、ガイドラインでは適法な同意を取得するための追加条件をいくつか提示している。紙面の都合上、すべては紹介できないが、ここでは「同意の立証」と「子どもへの配慮」について紹介したい。

ガイドラインでは、データ管理者が本人から適切に同意を取得したことを立証できるようにしておくことを要求している。立証の仕方として、たとえば、病院がある科学研究プログラムを立ち上げ、無作為に患者のリストからサンプルデータを抽出し、個人データの取り扱いに関する同意を得る場合に、依頼と同意を得る電話での会話を記録すれば、本人から明確な同意を取得したことを立証できると説明している。

また、ガイドラインでは、GDPR第8条に規定されている「子ども」に関する定義[注17]を基に、子どもから同意を得たことを立証できるように、どのような同意取得ステップを踏むのが適切かについて具体例を示し説明して

表2　子どもから同意を取得する適法なステップ例

ステップ	実施内容
1	利用者に、16歳未満かどうかを確認する
2	16歳未満と答えた利用者に対して、親権者の同意が必要である旨を通知し、親権者のメールアドレスを登録するよう求める
3	事業者は電子メールを通じて親権者に子どもの個人データの取り扱いに関する同意を求めるとともに、当該電子メールの宛先の人物が親権を本当に有しているか確認する
4	苦情があった場合には、管理者は利用者の年齢を確認する追加的なステップを踏む

出所）同意に関するガイドライン“Guidelines on Consent under Regulation 2016/679（wp259rev.01）”より作成

いる。たとえば、オンラインゲームを提供する事業者が子どもの利用者に対して、表2のステップで同意を取得している場合には、GDPR上は適法であると説明している。

確認のステップに関して、ガイドラインでは技術的な要請は控えられているが、「データ管理者は定期的に適切な技術とプロセスを見直し続ける必要がある」と付記されている。

Ⅳ 制度運用の今後の展望

第Ⅲ章では欧州の当局者が考えるGDPRの制度運用について、ガイドラインで示された考え方や具体例を一部紹介した。それでは実際にGDPRはガイドラインがイメージする通りに運用されていくのだろうか。筆者は制度運用の今後の展望を左右する要素は2つあると考えている。

1つ目は業界標準の進捗である。GDPRガイドラインでは具体例を提示しながら細かなサービス設計を要求している箇所もあれば、技術的な進歩やベストプラクティスが将来的に蓄積されることを期待しつつ、現時点では詳細な説明を控えている箇所もある。筆者が欧州の弁護士事務所などを訪問した際にも、多くの事業者がデータポータビリティや忘れられる権利（個人データの消去）への対応方法などについて、試行錯誤していると聞いた。GDPRにどこまで対応すればよいのか・するべきかについては、監督機関の法執行状況を見つつ、各事業者が継続的に試行錯誤しながら具体化していくものと考える。

2つ目は、各国の監督機関の協調である。GDPRはEU加盟国に直接適用されるが、これまで各国では、独自のデータ保護法に基づき法執行の方針やベストプラクティスが培われてきた。EU加盟国の中には、GDPRに抵触しない範囲で従前の制度を活かした追加規定を設けるところもある[注18]。また、罰則の上限はGDPRで大きく引き上げられたものの、実際の執行にあたっては、各国の監督機関が自国の刑法等の規定を踏まえつつ判断していくことになる。こうした状況を踏まえると、EU加盟国がGDPRを統一的に協調して運用していくためには、各国の監督機関同士が具体的な事例に基づく法執行の方針や判断の基準について、相当程度、議論の積み重ねを行っていく必要があると考える。

GDPRへの対応方法は、公表予定のガイドラインや監督機関の活動の積み重ねを受け、徐々に明確になっていくと考えられる。欧州の個人データを取り扱う企業は継続的に監督機関の動向を注視するとともに、取り扱いの見直し、拡充に努めることが重要である。

注

1　正式名称は「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」

2 DPAが担う法執行活動には苦情受付、調査、是正命令（課徴金の納付命令を含む）とあるが、ベルギー、オーストリア、ポーランドの3カ国のDPAは法令上直接に課徴金の納付を命令することはできず、裁判所の介在などが規定されていた

3 メンバーとは日本の個人情報保護委員会における「委員」に相当する者を指す。任命要件の一例として、4年以上の任期が挙げられる

4 欧州単位の行政機関における個人データの取り扱いに対して法執行活動を行う組織

5 主管監督機関の特定については取り扱いの実態を踏まえ、関係する監督機関が事業者の特定結果に異義を唱え、変更することができる

6 29条作業部会が2017年4月5日に採択した「Guidelines for identifying a controller or processor's lead supervisory authority」を参照のこと

7 アイルランドの監督機関（Data Protection Commission）は2018年5月25日のGDPRの施行から5月31日までの約1週間で1,300件を超える苦情が寄せられたと発表（https://iapp.org/news/a/gdpr-enforcement-is-it-really-about-the-fines/）しており、苦情の受付処理にこれまで以上に追われていることが想像される

8 Optical CenterのWebサイトURLを操作することで顧客の氏名、住所、健康データ、国民識別番号などにアクセスすることができた。違反時は334,000件以上のレコードが侵害された

9 ガイドラインは修正、採択を繰り返しながら、欧州委員会のWebサイトにて公表されている（http://ec.europa.eu/newsroom/article29/news.cfm?item_type＝1360）（2018年7月17日アクセス）

10 欧州委員会Webサイト（http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id＝624044）（2018年7月17日アクセス）

11 ただし、GDPRではデータ管理者に対してそうした直接移転を可能にする互換性のあるデータ処理システムの設置を義務付けてはいない（前文第68項）

12 データポータビリティの権利はデータ処理が自動化された手段によって実行される場合にのみ適用されるため、3つの基準すべてに該当したとしても紙媒体による取り扱いの場合には適用されない

13 複雑な事案の場合、最大3カ月まで延長することができるが、その場合は元の要求から1カ月以内に遅延理由を本人に通知しなければならない

14 一般的に認められることであっても、子どもを対象とする場合、より厳格な基準を課すGDPRの姿勢は、プロファイリングのみならず同意のガイドラインなどでも確認できる

15 設計されたときの本来の目的のための機能が、いつの間にかほかの目的にも拡大流用される現象をいう

16 利用者が、日々、画面をスワイプし、チェックボックスにクリックすることを要求するような同意の要請を、多くのサービス機能から受けていることにより、クリックすることに疲れ、内容を詳細に確認しなくなってしまうような状況に陥ることをいう

17 GDPRでは16歳未満を子どもと定義し、子どもの個人データを取り扱う際は、親権者の同意または承認が必要としている（第8条第1項）。なお、子どもと見なす年齢は、各EU加盟国の裁量により引き下げる（ただし、13歳を下回ってはならない〈第8条第1項〉）ことが認められている

18 たとえば、ラトビアでは既に存在するDPOのような役割を担う人材を国家試験で認定する制度をそのまま継続運用する方針である

著者

奥見紗和子（おくみさわこ）
金融コンサルティング部主任コンサルタント
専門は個人情報保護、クレジットカード事業戦略、CSV・ESG戦略など

南島安平（みなみしまやすへい）
アナリティクス事業部主任コンサルタント
専門は制度対応、事業戦略の立案支援