「EU 一般データ保護規則（GDPR）」
に関わる実務ハンドブック
（第 29 条作業部会ガイドライン編）

・データポータビリティの権利

2018 年 2 月
日本貿易振興機構（ジェトロ）
ブリュッセル事務所
海外調査部　欧州ロシア CIS 課

2018年5月25日から適用が開始されるEUの「一般データ保護規則（General Data Protection Regulation：GDPR）」は、欧州経済領域（European Economic Area：EEA、EU加盟国28カ国、ノルウェー、アイスランド、リヒテンシュタイン）と個人データをやり取りする日本のほとんどの企業や機関・団体が適用対象となり（外交・防衛・警察などについて例外あり）、同規則への違反行為には高額の制裁金が科されるリスクもある。

ジェトロは2016年11月に、同規則の基本的な構造と基礎的な社内外の対応について概説した「実務ハンドブック（入門編）」[1]を、2017年8月に標準契約条項（Standard Contractual Clauses：SCC）と拘束的企業準則（Binding Corporate Rules：BCR）を中心とする企業のコンプライアンス対応を概説した「実務ハンドブック（実践編）」[2]を公表した。

GDPRに関するガイドラインを解説した本レポートは、同規則に詳しいギブソン・ダン・クラッチャー法律事務所ブリュッセルオフィスの杉本武重弁護士と川島章裕弁護士に委託し作成した。本レポートでは、「データポータビリティの権利」に関するガイドラインを2017年12月31日現在の情報を基に解説した。

【免責条項】
本レポートで提供している情報は、ご利用される方のご判断・責任においてご使用ください。
ジェトロでは、できるだけ正確な情報の提供を心掛けておりますが、本レポートで提供した内容に関連して、ご利用される方が不利益等を被る事態が生じたとしても、ジェトロおよび執筆者は一切の責任を負いかねますので、ご了承ください。　禁無断転載

[1] https://www.jetro.go.jp/world/reports/2016/01/dcfcebc8265a8943.html
[2] https://www.jetro.go.jp/world/reports/2017/01/76b450c94650862a.html

Copyright (C) 2018 JETRO. All rights reserved.

目　次

Copyright (C) 2018 JETRO. All rights reserved.

はじめに

本稿は、第 29 条作業部会[3]が公表している「一般データ保護規則（GDPR）」に関するガイドラインのうち、「データポータビリティの権利に関するガイドライン（WP242）」（2016 年 12 月 13 日付採択、2017 年 4 月 5 日改訂）[4]の内容を解説することを目的として作成したものである。

第 29 条作業部会が公表するガイドラインは制度の概要について知識を有していない読み手には必ずしも理解しやすい構成になっていないため、各章では、まずガイドラインの構成を示し、その後ガイドラインで説明されている事項のうち重要なものを必要に応じて再構成し、簡潔に概要を記載した。さらに、公表されているガイドラインの内容を概ね記載した上で実務上の論点を含む事項については、「コメント」という形で留意点を追加している。特に、DPO の選任義務は、データ保護に関わるビジネスの観点から、日本本社と欧州拠点の間における意思決定プロセスや組織関係に重要な影響を及ぼす可能性がある問題であるため、コメントとして比較的多くの記述を割くよう心掛けた。ガイドラインの内容を概ね記載することとしたのは、公表されているガイドラインは細部にわたって重要な事項を含む記述が多いことから、内容を省略せずに情報提供する方が読者の GDPR に対するより正確な理解に資すると考えたためである。もっとも、本稿もガイドラインの内容を完全に翻訳した内容ではないため、あくまで GDPR に関するガイドラインを理解するための出発点として活用頂ければ幸いである。

本稿執筆時点（2017 年 12 月 31 日）における第 29 条作業部会による GDPR に関するガイドラインの公表状況については、「データ保護責任者に関するガイドライン」の解説レポートにて紹介している。

なお、本稿において「EU」は特に言及がない限り、EEA（欧州経済領域、EU 加盟 28 カ国とノルウェー、アイスランド、およびリヒテンシュタイン）を意味するものとする。欧州委員会は EEA 内の EFTA 加盟国であるノルウェー、アイスランド、およびリヒテンシュタインとの間で GDPR を EEA 協定書に統合する作業を速やかに行う予定であり、当該作業完了後にこれら 3 ヵ国においても GDPR が適用されることとなる。

[3] Article 29 Working Party、EU 加盟各国の監督当局の代表、欧州委員会司法総局データ保護課の代表、欧州データ保護監察機関（EDPS）の代表によって構成される。特定の問題に関して共通の解釈と分析を提供することにより、EU 加盟国のデータ保護法の解釈にある程度の調和をもたらす。

4http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233

Copyright (C) 2018 JETRO. All rights reserved.

I. データポータビリティの権利に関するガイドラインの構成

データポータビリティの権利に関するガイドラインは、以下の項目によって構成される。

1. はじめに
2. データポータビリティの権利の要素は何か
3. どのような場合にデータポータビリティが適用されるか
4. データ主体の権利行使に関する一般的ルールはデータポータビリティにどのように適用されるか
5. ポータブルデータはどのように提供されるべきか

II. データポータビリティの制度の概要

1. データポータビリティの権利の概要

データポータビリティの権利とは、データ主体がデータ管理者に提供してきた個人データを、構造化され、一般的に利用され、機械可読な形式で受け取る権利、および、当該データを、管理者からの妨害を受けることなく、他の管理者に転送する権利によって構成される。データポータビリティの権利は、GDPR において、新しく認められたデータ主体の権利である。現行（2017 年 12 月現在）の「データ保護指令」（95/46/EC）では、データ主体が自己の個人データを管理者から取得するためには、アクセス権の行使によって管理者から管理者により選択される形式によって提供を受けることしかできなかったが、GDPR においては、相互運用可能な形式で提供を受けられるため、個人データを特定の IT 環境から他の IT 環境に移動させることが容易となる。このようなデータポータビリティの権利がデータ主体に認められる趣旨は、個人データに対する個人のコントロールを向上させ、データエコシステムの中で個人が積極的な役割を果たせるようにすることにある。

2. データポータビリティの権利の要素

データポータビリティの権利の要素は、（1）**個人データを受け取る権利**、および、（2）**あるデータ管理者から別のデータ管理者へ個人データを転送する権利**、に分類される。**個人データを受け取る権利**とは、データ管理者によって自己に関して処理が行われた個人データの部分的集合を受け取るデータ主体の権利であり、当該個人データを個人的な使用のために保管する権利である。他方で、**個人データを転送する権利**とは、あるデータ管理者から別のデータ管理者へ「妨害なしに」個人データを転送する権利である。後者の個人データを転送する権利は、個人データの転送が技術的に実現可能な場合に認められる権利であり、常に権利行使が可能なわけではない。

管理者の立場からは、データポータビリティの権利行使に対してどのように対応すべきかが重要となる。基本的な観点としては、管理者は、あくまでデータ主体のために行動することが求められるものであり、データを受信する他の企業などに対して義務を負うものではない。管理者の義務内容の詳細は後述するが、管理者がデータポータビリティの権利行使に対応する負担を軽減する観点からは、データポータビリティの権利を発生させないことがポイントとなる。そのためには、個人データを取得する際にはデータポータビリティの権利が発生しない法的根拠に基づくようにすること（下記「3　データポータビリティの権利の対象となる個人データ」参照）、削

Copyright (C) 2018 JETRO. All rights reserved.

除した個人データはデータポータビリティの権利の対象とならないことから、取得した個人データは必要以上に長期に保管せずに削除することといった対策が必要となる。

3. データポータビリティの権利の対象となる個人データ

データポータビリティの権利の対象となるのは、データ主体自身に関するデータであり、かつデータ主体がデータ管理者に対して提供したデータであり（GDPR 第 20 条第 1 項）、これには 3 つの要件が存在する。

第一に、データポータビリティの権利対象は、個人データに限られるため、匿名化されたデータは対象とならない。

第二に、データポータビリティの権利対象は、データ主体によって「提供された」データである。提供されたデータには、（1）データ主体により能動的かつ意識的に提供されたデータ、および、（2）サービスまたは装置の利用に関連してデータ主体の活動の観察・監視の結果としてもたらされるデータ（例えば、取引履歴、アクセス記録など）である。他方で、データ主体によって提供されたデータに基づいて管理者が生成した推測データ（Inferred data）または派生データ（Derived data）は、データポータビリティの権利の対象とはならない。

第三に、データポータビリティの権利は、他者の権利または自由に不利な影響を及ぼしてはならない。そのため、データポータビリティの権利行使の対象となるデータに第三者の個人データが含まれている場合、当該処理に関する法的根拠が必要となる。

4. データポータビリティの権利行使に関して管理者が取るべき対応

(1) データ主体に対する情報通知

GDPR において、管理者は、データ処理を行う場合、処理に関する公正性および透明性を確保するため、管理者の概要、処理の内容、当該処理に関してデータ主体が有する権利の内容などについてデータ主体に対して情報提供（情報通知）を行う義務を負う（第 12 条から第 14 条）。そして、データ処理に関してデータ主体にデータポータビリティの権利が発生する場合には、情報通知を行う際に、データ主体がデータポータビリティの権利を有する旨も明確に記載しておく必要がある（第 13 条第 2 項(b)号、第 14 条第 2 項(c)号）。

(2) データポータビリティの権利行使を行うデータ主体の認証方法

データ主体がデータポータビリティの権利を行使した場合、管理者がこれに応じなければ管理者は GDPR に違反することになるが、他方で、管理者としては当該権利行使に応じて個人データを外部に提供する前に当該人物が真にデータ主体であるかを確認したいところである。これについて、GDPR は、管理者がデータ主体の識別を必要としない目的で個人データを処理しており、そのデータ主体を識別できないことを立証できる場合を除いて、データ主体の権利行使（データポータビリティの権利を含む）に関して、データ管理者は当該主体の要求に基づく措置を拒絶してはならないと定める（第 12 条第 2 項）。また、データ主体の身元に関する合理的疑義を持つ場合、データ管理者は、データ主体の身元を確認するのに必要な追加情報の提供を要求することができる（第 12 条第 6 項）。データ主体が当該主体の識別を可能とする追加情報を提供した場合、データ管理者は要求に対する措置を拒絶できない（第 11 条第 2 項）。

Copyright (C) 2018 JETRO. All rights reserved.

(3) データポータビリティの権利行使に対応するための期限

管理者は、権利行使に関して管理者が行った対応に関する情報を不当に遅滞することなく、いかなる場合でもその要求を受け取ってから 1 カ月以内に、データ主体に提供しなければならない（GDPR 第 12 条第 3 項）。権利行使に関する要求が複雑な場合は、当該期間は 3 カ月まで延長することができるが（つまり、最初の 1 カ月間からさらに 2 カ月間の延長が可能である）、その場合、管理者は、要求を受け取ってから 1 カ月以内に、遅滞の理由をデータ主体に通知しなければならない。

5. ポータブルデータの提供

(1) ポータブルデータの提供方法

データポータビリティの権利行使がなされる場合、管理者の立場からは競合他社に自社が管理するデータが提供されることにつながるため、権利行使を妨害するインセンティブが潜在的に存在する。そのため、GDPRは、データ主体は、個人データを提供した管理者からの妨害受けることなく、データを他の管理者に移転する権利を有するものと規定している（第 20 条第 1 項）。「妨害」とは、データ主体または別の管理者によるアクセス、転送または再利用を抑制、または遅らせるために、管理者によってもたらされる法的、技術的または経済的な障害を意味する。また、データ主体は、技術的に実現可能な場合には、ポータブルデータをその他のデータ管理者に直接転送することができる権利を有する（第 20 条第 2 項）。データ管理者間の転送の技術的な実現可能性は、ケースバイケースで判断されるが、2 つのシステム間で安全な方法でコミュニケーションを図ることが可能であり、かつ受信側のシステムが入ってくるデータを技術的に受信できる状況があることが必要である。また、データを受信する側の管理者は、特定の技術に適合する処理システムを採用または維持する義務は負わないとされている（前文第 68 項）。

(2) 提供されるデータの形式

データポータビリティの権利は、個人データを取得または転送した後に再利用することを想定した権利であるため、ポータブルデータが利用しやすい形式で提供されることが重要である。これについて、GDPRは、個人データは、構造化され、一般的に利用され、機械可読な形式で提供されなければならないと規定している（第 20 条第 1 項）。もっとも、特定の形式を使用することが義務付けられているわけではないため、相互運用性および共通の形式をどのような内容にするかは産業団体などによる自主的な取り組みが期待されている。

(3) 大量または複雑な個人データにどのように対処すべきか

GDPRは、大量または複雑な個人データに関する対応方法について特段の規定を設けていないが、データポータビリティの権利に関するガイドラインは、個人データの提供を受けた個人が、個人データの定義、概要、構造について完全に理解できる状況が確保される必要があると述べている。具体例として、特定の個人データを容易に特定、認識、処理できるようなソフトウェア・アプリケーションの使用を示唆している。

(4) ポータブルデータをどのように保護し得るか

Copyright (C) 2018 JETRO. All rights reserved.

管理者がデータポータビリティの権利行使に対応する際には、①どのように個人データを正しい相手に安全に届けるか、②どのようにユーザーが自己のシステムに個人データを安全に保管することを支援するかというセキュリティの問題にも対処する必要がある。

上記①に関して、データ管理者としては、次の対応を含む適切なリスク軽減策を実施すべきである。

- データ主体の認証が既に必要な場合、「共有された秘密」などの追加の認証情報、またはワンタイムパスワードなどのその他の認証要素の使用
- アカウントが侵害されているとの疑義がある場合、送信の保留または凍結
- データ管理者から別のデータ管理者に直接転送される場合、トークンによる認証など委任による認証

上記②に関して、データ主体は自己のシステムにおける個人データを保護することについて責任を負うが、データ管理者側がデータ主体に安全に個人データを保管できるように適切なツールを推奨することがリーディング・プラクティスとして挙げられている。

Copyright (C) 2018 JETRO. All rights reserved.

Ⅲ.　データポータビリティの権利に関するガイドライン

1. はじめに

既述の通り、GDPR 第 20 条は、新たなデータポータビリティの権利を導入している。当該権利は、データ主体が、当該データ主体がデータ管理者に提供してきた個人データを、構造化され、一般的に利用され、機械可読な形式で受け取ること、そして当該データを、妨害なしに、他の管理者に転送することを認めている。当該権利は、特定の条件の下で、ユーザーの選択やユーザーの管理、そしてユーザーの権限を支えるものである。

データ保護指令に基づくアクセス権を利用する個人は、要求した情報の提供を受ける際にデータ管理者により選択された形式によって制約されていた。今回の新しいデータポータビリティの権利は、個人データをある IT 環境から別の IT 環境（自己の所有するシステム、信頼される第三者のシステム、または新しいデータ管理者のシステムであるかを問わない）へ移動、コピー、または転送する可能性を拡大し、データ主体に、自身の個人データに関する権限を与えることを目指すものである。

また、当該権利は、個々の人間の人格権や個人データに対する支配権を確約することにより、データ主体とデータ管理者の関係のバランスを取り戻す機会を提供する[5]。

個人データのポータビリティの権利は、サービス間の競争を（サービスの切り替えを促進することにより）促進する可能性もあるが、GDPR は個人データに関する規律であり、競争に関するものではない。特に、第 20 条は、ポータブルデータをサービスの切り替えのために必要または有益なものに限定していない[6]。

データポータビリティは新しい権利であるが、他の種類のポータビリティは既に存在しており、また、他の立法領域でも現在討議が行われている（例：契約終了、通信サービスのローミング、サービスへの越境アクセスなど）[7]。そうした異なるポータビリティは、組み合わされた形で提供された場合、個人に対する相乗効果あるいは恩恵がもたらされる可能性がある。ただし類似性については注意して処理する必要がある。

本ガイドラインは、データ管理者がそのプラクティス、過程、方針を更新し、データ主体が効率的にその新しい権利を使うことができるようデータポータビリティの意味を明確化するための指針を提供する。

2. データポータビリティの主な要素とは何か

GDPR はデータポータビリティの権利について第 20 条第 1 項で次の通りに規定している。

データ主体は、当該データ主体が管理者に提供した当該データ主体に関する個人データを、構造化され、一般的に利用され、機械可読な形式で受け取る権利を有し、当該データを、個人データの提供を受けた管理者の妨害なしに、他の管理者に転送する権利を有する。

(1)　<u>個人データを受け取る権利</u>

---

[5] （原文脚注 1）データポータビリティの主要な目的は、個人データに対する個人の支配権を改善し、データエコシステムの中で個人が積極的な役割を果たせるようにすることにある。

[6] （原文脚注 2）当該権利は、エネルギー供給サービスの一環として当初収集された個人データを利用して、ユーザーのコントロールに基づいて、銀行が追加的なサービスを提供することを可能とする可能性がある。

[7] （原文脚注 3）欧州委員会のデジタル単一市場に関するアジェンダ（https://ec.europa.eu/digital-agenda/en/digitalsingle-market）、特に、政策の第一の柱「デジタル製品およびサービスへのオンライン上でのアクセスの改善」参照。

Copyright (C) 2018 JETRO. All rights reserved.

第一に、データポータビリティとは、データ管理者によって処理が行われた自己に関する個人データの部分的集合を受け取るデータ主体の権利であり、当該個人データを個人的な使用のために保管する権利である。当該保管は、必ずしもデータを別のデータ管理者に引き渡すだけではなく、個人のデバイスまたは個人のクラウド上でも行われ得る。

この点において、データポータビリティは、アクセス権を補完するものである。データポータビリティの１つの特異性は、データ主体に自分自身の個人データを管理して再使用するための簡単な方法を提供することである。こうしたデータは「構造化され、一般的に利用され、機械可読な形式」でなければならない。

例えば、データ主体は、どの曲を何回聞いたか調べるため、または別のプラットフォームでどの音楽を購入したい、もしくは聴きたいか検討するために、音楽ストリーミング・サービス上で自分のプレイリスト（または視聴した曲目の履歴）を検索することに関心を持つ可能性がある。あるいは、ウェブメール・アプリケーションから連絡先リストを検索して結婚式の招待リストを作成したり、異なる会員カードを使って購入した情報を取得したりすることなどを希望する可能性がある。

(2) あるデータ管理者から別のデータ管理者へ個人データを転送する権利

第二に、第 20 条第 1 項は、データ主体に、あるデータ管理者から別のデータ管理者へ「妨害なしに」個人データを転送する権利を与えている。データは、技術的に実現可能な場合には、データ主体の要請に基づいて、あるデータ管理者から別のデータ管理者に直接移転することも可能である（第 20 条第 2 項）。これに関して、前文第 68 項は、データ管理者がデータポータビリティを可能とする相互運用可能な形式を開発することを推奨するが[8]、管理者に対して技術的に適合する処理システムを採用または維持することを義務づけるものではない。もっとも、GDPR は、管理者がデータの転送に障壁を設けることを禁止している。

本質的に、データポータビリティの当該要素は、過去に提供した個人データを取得して再利用するだけでなく、別のサービスプロバイダーに転送する可能性をデータ主体に提供するものである[9]。「囲い込み」の防止による消費者の権限拡大に加え、データポータビリティの権利は、革新と、データ主体の管理の下においてデータ管理者間で安全かつ安心な方法で個人データを共有する機会を醸成するものと期待されている。データポータビリティは、組織間で、個人データのユーザーによる管理かつ限定された共有を推進し、サービスや顧客体験を豊かにし得る[10]。データポータビリティは、ユーザーが関心を持つ様々なサービス間で、ユーザーの個人データの転送や再利用を促し得る。

コメント１：個人データを転送する権利の要件

[8] （原文脚注 5）セクション「5［ポータブルデータはどのように提供されるべきか］」を参照。
[9] （原文脚注 7）英国の MiData（http://www.pcamidata.co.uk/）やフランスの新世代インターネット財団（FING）による MesInfos/SelfData（http://mesinfos.fing.org/）などの欧州におけるいくつかの実験的な応用事例を参照。

[10] （原文脚注 8）いわゆる自己定量化（自分の経験や行動などをあらゆるデバイスで測定、記録しておくこと）および IoT 産業は、フィットネスや活動、カロリー摂取などの個人の生活の様々な要素を結び付け、単一のファイルに個人の生活のより完全な全体像をまとめることのメリット(およびリスク)を示している。

Copyright (C) 2018 JETRO. All rights reserved.

個人データを転送する権利は、データポータビリティの権利の発生要件に加えて、個人データの転送が技術的に実現可能な場合にデータ主体に認められる権利である。データポータビリティの権利の中でも個人データを受領する権利と転送する権利とで要件が異なる点に留意する必要がある。

(3) 管理者であることについて

データポータビリティは、データ主体が希望に従って、個人データを受領し、処理する権利を保証する[11]。

GDPR 第 20 条の要件の下で、データポータビリティの要求に応じるデータ管理者は、データ主体、または個人データを受け取る別の企業によって扱われるデータ処理に対して責任を負わない。データ管理者は、個人データが別のデータ管理者に直接移転される場合を含めて、データ主体のために行動する。この点について、データ受信者を選択するのは送信側のデータ管理者ではないことに鑑みて、データ管理者は、受信側のデータ管理者によるデータ保護法の遵守について責任を負わない。同時に、管理者は、管理者が純粋にデータ主体のために行動することを確実にするための保護措置を講じる必要がある。例えば、送信される個人データの種類が、実際にデータ主体が送信を希望するものであることを確実にするための手続きを確立することが考えられる。当該手続きは、送信が行われる前、またはより早期の段階の、ある処理のための当初の同意が得られた時点もしくは契約が締結された時点において、データ主体から確認を得ることによって実現可能と考えられる。

データポータビリティの要請に対応するデータ管理者は、データの送信前に、データの質を確認および証明する明確な義務を負わない。当然のことながら、当該データは、GDPR 第 5 条第 1 項に定める原則に従って、既に正確で、最新のものである必要がある。さらに、データポータビリティは、個人データを必要以上に長い期間または指定された保管期間を越えて保管することをデータ管理者に義務付けていない[12]。特筆すべきは、単に将来の潜在的なデータポータビリティ要求に対応するために、当該データの保管をデータ管理者に別途適用される保存期間を超えて義務付けるような追加要件はない、という点である。

コメント２：保有する必要のない個人データを削除することによるデータポータビリティの権利行使の回避

削除された個人データについては、データ主体はデータポータビリティの権利を行使することはできない。従って、管理者としては、個人データの保持期間を適切に定め、不要な個人データを必要以上に長く保管しないようにすることが、データポータビリティの権利行使の場合の負担を減らす観点から有益である。

要請される個人データがデータ処理者によって処理される場合、GDPR 第 28 条に従って締結される［管理者と処理者の］契約は、「管理者が適切な技術的かつ組織的な対策によってデータ主体の権利の行使に対して対応すること」を支援する義務を規定しなければならない。データ管

[11] （原文脚注 9）データポータビリティの権利は、データ管理者の競合者が提供する類似のサービスにとって有益かつ関連した個人データに限定されない。

[12] （原文脚注 10）前述の例の場合、データ管理者がユーザーが再生した曲の記録を保管しなかった場合、この個人データはデータポータビリティの要求対象のデータには含まれない。

Copyright (C) 2018 JETRO. All rights reserved.

理者は、データポータビリティの要請に対応するためにデータ処理者と協力するための具体的な手続きを実行すべきである。共同管理者がいる場合[13]、契約はデータポータビリティの要請に対する処理に関して、各データ管理者間の責任分担を明確にすべきである。

コメント３：データポータビリティの権利行使の対応に関する処理者との協力 例えば、クラウド事業者が処理者として個人データの処理を支援している場合、個人データの提供のための形式やその他の個人データ提供に関する対策に関して効果的に対応するためには、クラウド事業者の支援を受けることが重要となる。

受信側のデータ管理者[14]は、提供されたポータブルデータが、新たなデータ処理と関連性があり、過度なものではないことを保証する責任がある。言い換えると、受信し、保管されるデータは、受信側のデータ管理者が提供するサービスに必要かつ関連するものに限定されるべきである。例えば、ウェブメール・サービスに対するデータポータビリティの要求において、電子メールを取得し、かつデータ主体が電子メールを安全な保管プラットフォームに送信するために当該要求が行われた場合、新しいデータ管理者はデータ主体の通信相手の連絡先詳細を処理する必要はない。当該情報が新たな処理の目的とは無関係である場合、保管または処理されるべきではない。いかなる場合も、受信側の管理者は、データポータビリティの要求がなされた後、送信された個人データを受信し、かつ処理する義務を負わない。同様に、データ主体が自分の口座取引の詳細を家計管理サービスへ転送することを要求した場合、受信側のデータ管理者は、新しいサービスのためにデータの分類が完了すれば、全てのデータを受領したり、全ての口座取引の詳細を保管したりする必要はない。

「受信側」の組織は、当該個人データの新しいデータ管理者となり、従って、GDPR 第 5 条に記述された基本原則を遵守しなければならない。従って、「新しい」受信側のデータ管理者は第 14 条に規定される透明性の要件に従って、ポータブルデータの転送要求を行う前に、要求内容に関わらず、新しい処理の目的を明確かつ直接的に明言しなければならない[15]。データ管理者の責任に基づいて実行されるその他のデータ処理に関して、データ管理者は、適法性、公正性および透明性、目的の限定、データの最小化、正確性、完全性および機密性、保存の制限、ならびに説明責任などの第 5 条に定められる原則を適用する必要がある[16]。

個人データを保有するデータ管理者は、データ主体のデータポータビリティの権利を支援する体制を整えておくべきである。データ管理者は、データ主体からのデータを受信することを選択することも可能であるが、義務ではない。

コメント４：データポータビリティの権利行使の結果としてポータブルデータを受信する管理者の対応

[13] EU に拠点を有する 2 つ以上の管理者が処理の目的および手段を共同で判断する場合。

[14] （原文脚注 11）データ主体がデータポータビリティ要求によって別のデータ管理者へ送るように指示した個人データを受け取る管理者。

[15] （原文脚注 12）さらに、新しいデータ管理者は、関連性のない個人データを処理すべきではなく、また、たとえ個人データがポータビリティ処理によって送信される、より包括的なデータセットの一部であったとしても、処理は新しい目的のために必要なものに限定されねばならない。新しい処理の目的を達成する上で必要ない個人データは、できるだけ早急に消去すべき。

[16] （原文脚注 13）データ管理者によって一度受信されると、データポータビリティの権利の一環として送信された個人データは、データ主体によって「提供された」ものと見なされ、データポータビリティの権利に関するその他の条件（すなわち、処理のための法的根拠）が充足される限りにおいて、データポータビリティの権利に従って再度転送することが可能である。

Copyright (C) 2018 JETRO. All rights reserved.

データ主体がデータポータビリティの権利を行使した結果、ポータブルデータを受信することになった管理者は、当該個人データを受信後は管理者として第5条に規定される基本原則に従って処理を行う義務を負う。業務上、ポータブルデータを受信する可能性のある事業者は、ポータブルデータを受信した際の対応方法について予め個人データの管理規程などにおいて定めておくことが望ましい。

(4) データポータビリティとデータ主体の他の権利

一個人がそのデータポータビリティの権利を行使する場合、他の権利（GDPRにおいて他の権利が関わる場合）に影響を与えることなく行わねばならない。データポータビリティの実行後であっても、データ主体は引き続きデータ管理者のサービスを利用し、恩恵を受けることができる。データポータビリティは、データ管理者のシステムからのデータ消去を自動的に誘発するものではなく、転送されたデータに適用される当初の保管期間に影響を及ぼさない。データ主体は、データ管理者がまだデータ処理を行っている限りは、自己の権利を行使できる[17]。

コメント５：削除された個人データとデータポータビリティの権利
個人データが削除されている場合には、データ主体は当該個人データに関してデータポータビリティの権利を行使することはできない。

同様に、データ主体が削除権（第 17 条に基づく「忘れられる権利」）を行使したい場合、データ管理者は、削除を遅らせる、または拒否する手段としてデータポータビリティを使用することはできない。

別の分野における特定の EU 法または加盟国法が、関係するデータについて何らかの形式によるデータポータビリティを規定する場合、これらの特定の法令において定められる条件も、GDPRに基づいて要求されるデータポータビリティに対応する際に考慮されなければならない。また、データ主体の意思が GDPR に基づく権利を行使することではなく、むしろ特定の制度に基づく権利のみを行使することであることが、データ主体による要求から明らかである場合、GDPR のデータポータボリティの規定は当該要求に適用されない。

他方で、当該要求が GDPR に基づくポータボリティを目的とするものである場合は、当該特定の制度の存在することをもって、GDPRで定められるデータ管理者に対するデータポータビリティの原則の一般的な適用に優先するものではない[18]。もっとも、仮に当該特定の制度があったとしても、当該制度がデータポータビリティの権利に対してどの程度影響を及ぼす可能性があるかについては、事案毎に判断しなければならない。

3. どのような場合にデータポータビリティが適用されるか

(1) どの処理行為がデータポータビリティの権利の対象となるか

GDPRにおいてデータ処理を適法に行うためには、データ管理者は個人データの処理のために明確な法的根拠に基づいて処理を行う必要がある（第 6 条第 1 項）。

GDPR 第 20 条第 1 項(a)号に基づき、次の法的根拠に基づく処理行為がデータポータビリティの権利の対象となる。

[17] （原文脚注 14）GDPR 第 17 条の規定の通りである。
[18] （原文脚注 15）例えば、データ主体の要求が、「支払いサービス指令 2（PSD2）」で定められる目的のために、自己の銀行口座履歴へのアクセスを口座情報サービスプロバイダーに提供することを明確に求めている場合、当該アクセスは当該指令の規定に従って与えられるべきである。

Copyright (C) 2018 JETRO. All rights reserved.

- データ主体の同意（第 6 条第 1 項(a)号、または特別カテゴリーの個人データに入る場合は第 9 条第 2 項(a)号による）
- 第 6 条第 1 項(b)号に基づくデータ主体が当事者である契約（例えば、個人がオンライン書店から購入した本のタイトルや、音楽ストリーミング・サービスを通じて聴いた音楽は、データ主体が当事者である契約の実行に基づいて処理されるデータであるため、一般的にデータポータビリティの範囲内に入る）。

GDPRにおいて、個人データの処理が同意または契約に基づいていない場合は、データポータビリティの一般的権利は成立しない。例えば、金融機関は、マネーロンダリングおよびその他の経済犯罪を防止し、探知する義務の一環として処理する個人データに関するデータポータビリティの要求に回答する義務を負わない。同様に、データ主体の同意、またはデータ主体が当事者となる契約に基づかずに処理が行われる場合は、企業間の関係において処理された業務上の連絡先の詳細はデータポータボリティの対象とならない。

コメント６：個人データ処理の法的根拠の選択とデータ主体のデータポータビリティの権利および削除権

GDPR において、個人データを適法に処理するためには、次のいずれかに該当する必要がある（第 6 条第 1 項）。（1）データ主体の同意がある場合、（2）データ主体が当事者となっている契約の履行のために処理が必要である場合、もしくは契約締結前のデータ主体の要請に応じる手続きを行うために処理が必要である場合、（3）管理者が従うべき法的義務を遵守するために処理が必要である場合、（4）データ主体もしくは他の自然人の重大な利益を保護するために処理が必要である場合、（5）公共の利益もしくは管理者に与えられた公的権限の行使のために行われる業務の遂行において処理が必要な場合、（6）管理者または第三者によって追求される正当な利益のために処理が必要な場合（ただし、データ主体（特に子供がデータ主体である場合）の個人データの保護に関する基本的権利および自由が当該利益に優先する場合を除く）

データポータビリティの権利は、上記の 6 つの法的根拠のうち、（1）データ主体の同意、または、（2）契約の履行のために必要な処理に関する法的根拠に基づいて処理が行われる場合に発生する。従って、管理者側は、組織としてデータ主体の同意や契約の履行を法的根拠とせずに個人データの処理を行うことで、データポータビリティの権利を発生させないようにし、当該権利の行使に応じる負担を回避することが可能となる。

なお、データ主体の他の権利との比較における観点からは、例えば、削除権（第 17 条）は、データポータビリティの権利とは異なる要件[19]に基づいて発生するため、個人データ処理の法的根拠の選択によって必ずしも削除権の発生を回避することはできない。

[19] 削除権は、（1）個人データが収集された目的に関して不要となった場合、（2）同意に基づき取得された個人データについてデータ主体が同意を撤回した場合、（3）データ主体が異議権（第 21 条）を行使し、処理に関して優先するその他の法的根拠がない場合、（4）個人データが違法に処理された場合、（5）個人データが、管理者が従うべき EU 法または加盟国法における法的義務の遵守のために削除されなければならない場合、（6）個人データが情報社会サービス（第 8 条第 1 項）の提供に関して提供された場合、にデータ主体に生じる。

Copyright (C) 2018 JETRO. All rights reserved.

従業員のデータについて、データポータボリティの権利は、通常、データ主体が当事者である契約に基づいて処理が行われる場合にのみ適用される。多くの場合は、雇用者と従業員の間には力の不均衡があることから、この状況において、同意が自由になされたとは解されないであろう[20]。もっとも、人事における一定の処理は、正当な利益という法的根拠に基づくか、または雇用の分野における特定の法的義務を遵守するために必要なものである。実務上は、人事に関連するデータポータボリティの権利は間違いなく一定の処理業務に関係するものと考えられるが（支払、補償サービス、内部求人）、その他の多くの場合には、データポータビリティの権利に適用される全ての条件が充足されているかを判断するためにケースバイケースのアプローチが必要となるであろう。

コメント７：従業員の個人データの処理の法的根拠

雇用者が従業員の個人データを処理する場合、雇用者と従業員の力関係から従業員の自由な同意が期待できず、従業員の同意の有効性に疑義が生じやすいため、従業員の同意に基づく処理を行うことは極力回避すべきである。また、管理者がデータポータビリティの権利の発生を回避したい場合、従業員の同意または雇用契約のために必要な処理に依拠せずに個人データを処理する必要がある。

雇用者の正当な利益（legitimate interest）は時々に法的根拠として利用可能であるが、当該雇用者による従業員の個人データの処理が当該正当な利益にとって厳密に必要であって、かつ当該処理が比例性および従属性の原則を遵守する場合のみ利用可能となる[21]。

データポータビリティの権利は、データ処理が「自動的手段によって行われている」場合にのみ適用され、ほとんどの紙のファイルは対象外である。

(2) どのような個人データを含めるべきか

GDPR 第 20 条第 1 項により、次の個人データが、データポータビリティの権利の対象となる。

- データ主体自身に関する個人データ
- データ主体がデータ管理者に対して提供したもの

第 20 条第 4 項は、当該権利が他者の権利および自由に不利な影響を与えてはならないと規定している。

第一要件：データ主体に関する個人データ

データポータビリティの要求の対象範囲は、個人データに限られる。従って、匿名データ[22]またはデータ主体に関しないデータは、一切その範囲に入らない。しかし、明らかにデータ主体に結びつく仮名化データ（例：第 11 条第 2 項により、データ主体が識別を可能とする事実を提供する場合）は対象範囲内となる。

---

[20] （原文脚注 17）第 29 条作業部会が、意見書 8/2001（2001 年 9 月 13 日付）（WP48）においてその旨概説している。［http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf］

[21] 第 29 条作業部会「職場でのデータ処理に関する意見書 2/2017」（2017 年 6 月 8 日付採択）23 ページ参照。http://ec.europa.eu/newsroom/document.cfm?doc_id=45631

[22] （原文脚注 18）http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

Copyright (C) 2018 JETRO. All rights reserved.

第二要件：データ主体により提供されたデータ

第二要件は、データ主体によって「提供された」という範囲にデータの条件を絞っている。オンラインフォームを通じて提供されたアカウント情報（郵送先住所、ユーザー名、年齢）など、データ主体から認識的かつ能動的に「提供された」個人データの例は数多く存在する。

データ主体によって「提供された」データは、データ主体の活動の監視からもたらされることもある。従って、第 29 条作業部会は、データポータビリティの権利を完全に有効なものとするために、「提供された」との文言は、スマートメーターやその他の種類の接続された機器によって処理された生データ（raw data）、または、活動記録、ウェブサイトの使用履歴、検索履歴のような、ユーザーの活動を観察して得られた個人データも含めるべきだと考えている[23]。

この後者のカテゴリーの［データ主体により提供された］データには、例えばスマートメーターから収集された生データの分析によって作成されたユーザープロファイルといったような、データ管理者によって（観察またはインプットとして直接提供データの活用から）生成されたデータは含まれない。

データポータビリティの権利の対象となるかどうか判断するために、データの出所によってデータを異なるカテゴリーに区分することができる。次のカテゴリーは、「データ主体によって提供された」と見なされる。

- データ主体により能動的かつ認識的に提供されたデータ（例：郵送先住所、ユーザー名、年齢など）。
- サービスまたは装置の利用によって、データ主体により提供された観察データ。例えば、個人の検索履歴、トラフィック・データ、位置データなどが含まれる。また、ウェアラブル・デバイスによって記録した心拍数のような生データもこのカテゴリーに含めることができる。

対照的に、推測データや派生データは、「データ主体により提供された」データを基にデータ管理者によって生成される。例えば、リスク管理および金融規制（例えば、与信評価の実施またはマネーロンダリング対策規制の遵守）に関連して作成される、ユーザーの健康またはプロファイルに関する評価結果などは、データ主体「により提供された」ものとは見なされない。そうしたデータは、データ管理者が保管する個人のプロファイルの一部かもしれず、データ主体によって（例えば、当人の活動を通じて）提供されたデータの解析から推測もしくは派生したものだとしても、通常そのようなデータは「データ主体により提供された」データとは見なされず、この新しい権利の対象範囲には入らない[24]。

一般的に、データポータビリティの権利の政策目標に鑑み、「データ主体により提供された」という言葉は広義に解釈されねばならず、かつサービスプロバイダーによって生成された個人デ

[23] （原文脚注 19）データ主体は、データ主体の活動の観察から得られたデータを回収することが可能となるため、観察対象となるデータの範囲に関してデータ管理者が選択した実施内容についてより優れた視点を持つことも可能となり、類似のサービスを利用するために提供を望むデータをより選択しやすい状況に身を置き、どの程度データ主体のプライバシーが尊重されているかを認識するようになる。

[24] （原文脚注 20）しかしながら、データ主体は、GDPR 第 15 条(アクセス権に関する条項)により「管理者から当該データ主体に関する個人データを処理しているか否かを確認し、処理している場合、個人データにアクセスする権利」、ならびに「プロファイリングを含め、第 22 条第 1 項および第 4 項で定める自動化された意思決定の存在、少なくともそのような状況において、関連するロジックに関する有意な情報、データ主体に関する当該処理の意義および予測される結果」に関する情報にアクセスする権利を行使することができる。

Copyright (C) 2018 JETRO. All rights reserved.

ータ（例えば、アルゴリズムによる結果）を含む「推測データ」および「派生データ」を除外すべきである。データ管理者は、これらのデータを除外できるが、管理者によって提供された技術的手段を通じてデータ主体によって提供された他の全ての個人データを含むべきである[25]。

従って、「提供された」という言葉には、データ主体の活動または個人の行動の観察結果に関連する個人データが含まれるが、行動に関する分析は含まれない。一方、例えばパーソナライゼーションまたはレコメンデーション処理[26]など、ユーザーのカテゴリー抽出[27]やプロファイリングなどによるデータ処理の一部としてデータ管理者により生成された個人データは、データ主体によって提供された個人データから派生または推測されたデータであり、従ってデータポータビリティの権利の対象とはならない。

コメント８：データポータビリティの権利の対象となるデータ主体によって提供されたといえる個人データ

第二要件との関係で、データポータビリティの権利の対象であるか（データ主体によって提供された個人データといえるか）について、個人データの類型に応じて次のように整理することができる。

データ主体によって提供された個人データといえるか	個人データの類型	具体例
データ主体によって提供された個人データである	データ主体により**能動的かつ認識的に提供された個人データ**	オンラインフォームを通じてデータ主体によって提供された郵送先住所、ユーザー名、年齢など
	サービスまたは装置を利用したことに起因してデータ主体により提供された**観察データ**	個人の検索履歴、トラフィック・データ、位置データ ウェアラブル・デバイスによって記録した心拍数のような生データ
データ主体によって提供された個人データではない	個人の行動の分析の結果として得られる**推測データ（Inferred data）**および**派生データ（Derived data）**	健康または与信評価に関連するユーザーの分類やプロファイリングなどのデータ処理の一部としてデータ管理者により生成された個人データ

[25]（原文脚注 21）これには、取引履歴やアクセス記録などの、データ収集を目的とする活動中に、データ主体に関して観察された全てのデータが含まれる。データ主体の追跡や記録を通じて収集されたデータ（心拍数を記録するアプリや情報閲覧に関する行動を追跡するために使われる技術）は、データ主体によって能動的もしくは意識的に送信されたデータではないにしても、データ主体により「提供された」ものと見なされるべきである。

[26] ユーザーの購買履歴や属性情報などに基づいて、個々の消費者に対して適切な商品やサービスを推奨すること

[27] 第 29 条作業部会は、検索エンジンによる広告の個人化手法の 1 つと位置づけている。

Copyright (C) 2018 JETRO. All rights reserved.

第三要件：データポータビリティの権利は、他者の権利や自由に不利な影響を及ぼしてはならない

他のデータ主体に関する個人データについて：

第三要件は、他のデータ主体の権利および自由に不利な影響を与えるように処理される可能性が高い場合における、他の（同意していない）データ主体の個人データを含むデータの回収や新しいデータ管理者への転送を避けることを意図している（GDPR 第 20 条第 4 項）[28]。

このような不利な影響は、例えば、あるデータ管理者から別のデータ管理者へのデータの転送が、GDPR の下で第三者がデータ主体としてその権利（アクセス権など）を行使することを妨げる場合に発生し得る。

データ主体が自分のデータを別のデータ管理者へ転送することは、その新しいデータ管理者に当該データの処理を認めること、またはその新しいデータ管理者と契約を交わすことを意味する。第三者の個人データがデータセットに含まれている場合、処理の別の法的根拠を特定しなければならない。例えば、データ管理者は、GDPR 第 6 条第 1 項(f)号に基づく正当な利益を追求することができる。特に、データ管理者がデータ主体に対し、当該データ主体が純粋に個人または世帯の活動のために個人データを処理できるようにするサービスを提供することを目的とする場合がそれに当てはまる。個人的な活動の文脈でデータ主体が着手した処理作業で、第三者に関係し、潜在的に影響を及ぼすものについては、当該処理がいかなる意味においてもデータ管理者によって決定されていない限り、データ主体の責任の下で行われる。

例えば、ウェブメール・サービスによって、データ主体の連絡先、知人、親戚、家族、およびより広範な環境などのディレクトリの作成が可能になる場合がある。そうしたデータは、データポータビリティの権利の行使を欲する識別可能な個人に関連しており、また、そうした個人によって作成されるものであるため、データ管理者は送受信電子メールのディレクトリ全体を、当該データ主体へ送信すべきである。

同様に、データ主体の銀行預金口座は、口座保有者のみならずその他の個人の取引に関する個人データを含む可能性がある（例えば、第三者が口座保有者に振込を行った場合）。第三者の権利および自由は、ポータビリティの要求が行われて預金口座の情報が口座保有者に送信されることによって不利な影響を受ける可能性は低い―ただし、いずれの例においても、このようなデータが同じ目的のために使われる場合に限る（すなわちデータ主体によってのみ使われる連絡先住所、またはデータ主体の預金口座の履歴として使われる場合）。

逆に、新しいデータ管理者がその他の目的のために個人データを使用した場合、第三者の権利と自由は尊重されていない（例えば、受信側のデータ管理者がデータ主体の連絡先名簿のその他の個人の個人データをマーケティング目的のために使用した場合）。

従って、関連する第三者への不利な影響を防ぐために、別の管理者によるこのような個人データの処理は、ユーザーの単独管理の下で保管され、かつ純粋に個人的または世帯でのニーズのためのみに管理されている範囲内でのみ認められる。

[28] （原文脚注 22）前文第 68 項は「複数のデータ主体が関連する、一部の個人データのセットに関しては、個人データを受け取る権利は、本規則による他のデータ主体の権利および自由を害してはならない」と規定している。

Copyright (C) 2018 JETRO. All rights reserved.

受信側の「新しい」データ管理者（ユーザーの要求でデータが送信される相手）は、送信された第三者のデータを、製品やサービスの別のデータ主体へのマーケティング提案など、管理者自身の目的のために使ってはならない。

例えば、この情報を、第三者であるデータ主体の認識および同意なく、当該データ主体のプロファイルを改良し、当該データ主体の社会的環境を再現するために使用してはならない[29]。個人データが既にデータ管理者によって保有されているとしても、当該第三者に関する情報を回収し、固有のプロファイルを作成するために使用することもできない。さもなければ、このような処理は、特に関連する第三者がデータ主体としての権利を知らされておらず、データ主体としての権利を行使できない場合には、違法かつ不公平なものとなる可能性が高い。

全てのデータ管理者（送信側と受信側の両方）が、データ主体が回収し転送することを希望する関連データを選択し、他のデータ主体のデータを（関連する場合には）除外できるようなツールの導入は、リーディング・プラクティスとなる。これは、個人データが送信される可能性のある第三者にとってのリスク軽減をさらに促進するものとなる。

さらに、データ管理者は、関連する他のデータ主体のための同意メカニズムを導入し、他のデータ主体が積極的に同意する意思を有する場合（例えば、他のデータ主体も自己のデータを別のデータ管理者へ送信することを希望する場合）、データ送信を容易にすべきである。例えば、そうした状況はソーシャルネットワークで発生する可能性があるが、こうしたリーディング・プラクティスに従うとの判断を行うか否かはデータ管理者次第である。

コメント９：他者の権利および自由の対象となる個人データの特定

上記の通り、他者の権利および自由の対象となる個人データについては、データポータビリティの権利行使に制約がある。従って、管理者がデータポータビリティの権利行使に円滑に対応するためには、管理者は、個人データ処理に関する記録（第 30 条）において、保有する個人データが他者の権利および自由の対象となる可能性についてある程度事前に把握しておくことが望ましい。

知的財産や企業機密の対象となるデータについて：

他者の権利および自由は、第 20 条第 4 項で言及されている。ポータビリティに直接関連しないが、これは「企業機密または知的財産、および、特にソフトウェアを保護する著作権を含む他者の権利および自由」であると理解することができる。しかしながら、データポータビリティの要求に応じる前にそうした権利を考慮すべきであるとしても、「そうした考慮の結果は、全ての情報をデータ主体に提供することを拒否するものであるべきではない」。

さらに、データ管理者は、その他の契約上の権利の侵害を理由として、データポータビリティの要求を拒絶すべきではない（例えば、債務不履行またはデータ主体との取引に関する紛争）。

コメント 10：知的財産または企業機密の対象となるデータに関するデータポータビリティの権利行使への対応

管理者は、データポータビリティの権利行使があった場合、1 カ月以内に実施した措置に関する情報をデータ主体に提供する必要があり、要求が複雑な場合にはさらに最長で 2 カ月間の延長期間を得られる。データポータビリティの権利行使の対象である個人データが知的財産

[29] （原文脚注 23）ソーシャル・ネットワーキング・サービスは、透明性の原則を遵守し、かつ当該特定の処理に関する適切な法的根拠に確実に依拠することなく、データポータビリティの権利の一環としてデータ主体によって送信された個人データを利用して会員のプロファイルを改良してはならない。

Copyright (C) 2018 JETRO. All rights reserved.

または企業機密に関連する場合、管理者は、可能な限り1カ月以内に、データポータビリティの権利行使に応じることが可能な範囲と知的財産権などの関係で別途対応が必要な範囲を確定させ、必要に応じて期間の延長を求めることになると考えられる。また、一定の時間的制約の中でデータポータビリティの権利行使に応じる義務を履行するためには、データポータビリティの権利行使への対応策を整理したマニュアルを事前に作成し、必要なフローを記載しておくことが望ましい。

4. データ主体の権利行使に関する一般規則は、データポータビリティにどのように適用されるか

(1) どのような情報がデータ主体に対して予め提供されるべきか

データポータビリティという新たな権利に対応するために、第13条第2項(b)号および第14条第2項(c)号で義務付けられているように、データ管理者はデータ主体に、データポータビリティに関する新たな権利の存在を通知しなければならない。

「個人データがデータ主体から取得されていない場合」、第 14 条第 3 項は、データが取得された後、1 カ月を超えない合理的な期間、または、最初のコミュニケーションがデータ主体と行われている間、もしくは第三者に対して開示された時のいずれかに情報が提供されることを求めている[30]。

データ管理者は、データポータビリティの権利を他の権利と確実に区別しなければならない。従って、第 29 条作業部会は、特に、データ管理者が、データ主体がアクセス権またはポータビリティ権を通じて受け取ることができるデータの種類の違いについて、明確に説明することを推奨している。

コメント11：データ主体の他の権利行使との関係
本項目「4. 」における説明は、データポータビリティの権利以外のデータ主体の権利行使への対応においても参考となる。

さらに、第 29 条作業部会は、データ主体が保有するアカウントを閉鎖する前に、データ管理者が常にデータポータビリティの権利に関する情報提供を行うことを推奨している。これにより、契約終了前に、ユーザーは各自の個人データを調べ、データを自身のデバイスまたは別のプロバイダーへ容易に送信することができる。

最後に、「受け取る側の」データ管理者のリーディング・プラクティスとして、第 29 条作業部会は、データ管理者がデータ主体に対して、そのサービスの遂行に関連した個人データの性質について完全な情報を提供することを推奨している。公正な処理を行うことを強調することに加え、これにより、ユーザーは、第三者に対するリスクを限定し、また他のデータ主体が関わっていない場合でも個人データの不要な複製を制限することもできる。

(2) データ主体の要求に応じる前に、データ管理者はどのようにしてデータ主体を識別し得るか

データ主体を認証する方法について GDPR は規範的な要求は何も規定していない。ただし、GDPR 第 12 条第 2 項は、管理者がデータ主体の識別を必要としない目的で個人データを処理し

[30] （原文脚注 24）必要な情報を提供するにあたり、第 12 条は、「あらゆる通知を［...］簡潔で、透明性があり、理解しやすくかつ容易にアクセスし得る形態をもって、とりわけ子供のために特に記載される情報は明確かつ平易な言葉で」提供することをデータ管理者に義務付けている。

Copyright (C) 2018 JETRO. All rights reserved.

ており、そのデータ主体を識別できないことを立証できる場合を除いて、データ主体の権利（データポータビリティの権利を含む）行使に関して、データ管理者は当該主体の要求に対する措置を拒んではならないと規定している。しかし、第 11 条第 2 項は、このような状況において、データ主体は、当該データ主体の識別を可能とする追加的な情報を提供できると規定している。

さらに、第 12 条第 6 項は、データ主体の身元に関する合理的疑義を持つ場合、データ管理者は、データ主体の身元を確かめるのに必要な追加情報の提供を要求することができると規定している。データ主体が当該主体の識別を可能とする追加情報を提供した場合、データ管理者は要求に対する措置を拒んではならない。オンラインで収集した情報やデータが偽名もしくは独自の ID に結び付けられている場合も、データ管理者は、個人がデータポータビリティの要求を行い、当該個人に関するデータを受け取ることができるような適切な手続きをとることができる。いずれにせよ、データ管理者は、自分の個人データを要求したり、または、より一般的に GDPR で認められた権利を行使したりしようとするデータ主体の身元を明確に識別するための認証手続きを導入しなければならない。

これらの認証手続きはしばしば、既に存在している。データ主体はしばしば、契約を締結する前、または処理に対するデータ主体の同意を取得する前に既に認証されている。従って、処理に関係する個人を登録するために使用された個人データが、ポータビリティの目的のためにデータ主体を認証するための証拠として利用されることもあり得る[31]。

これらの事案において、データ主体の事前の本人確認のために、法的な本人性の証拠を要求することが必要となる可能性があるが、データと当該個人の間の関連性は公式または法的な本人性とは関係ないため、そのような本人確認はデータと当該個人の間の関連性を評価する上では意味をなさない可能性がある。本質的には、本人性の評価を行うために追加の情報を要求するデータ管理者の権利は、過剰な要求、および、個人と要求された個人データの間の関連性を確固たるものとする上で意味をなさない、または必要性のない個人データの収集の原因となってはならない。

多くの場合、このような認証手続きは既に設けられている。例えば、個人が自身の電子メールアカウント、ソーシャルネットワークアカウント、その他の様々なサービスに使われるアカウントにアクセスできるようにするために、通常ユーザー名やパスワードが使われており、場合によってはそのフルネームや識別情報を開示しないで使用することを個人が選択できるようになっている。

データ主体によって要求されたデータのサイズが、インターネット経由で送信する上で問題となる場合、要求に応じるために[32]延長された最長 3 カ月の期間を見越す代わりに、データ管理者はストリーミングの使用、CD や DVD その他の物理的媒体へのデータ保存、（技術的に可能である場合は GDPR 第 20 条第 2 項で規定されているように）別のデータ管理者へ個人データを直接送信するなどの別のデータ提供方法を検討する必要が生じる可能性がある。

コメント 12：データ主体の認証手続き

管理者は、データ主体の身元を確認するための認証手続きを設けておく必要がある。データ主体とオンライン上のアカウントなどでやり取りを行っている場合には、アカウントのログイン手続きによって本人であることの認証を行うことが可能である。そのような認証手続きを行うことができないケースについては、事前に認証手続きのフローを整理しておく必要がある。

31 （原文脚注 25）例えば、データ処理がユーザーのアカウントに関連する場合、関連するログインおよびパスワードを提供することはデータ主体を特定するのに十分であり得る。

32 （原文脚注 26）第 12 条第 3 項「管理者は、要求に応じて行われた措置を提供する」。

Copyright (C) 2018 JETRO. All rights reserved.

(3) ポータビリティの要求に応じるための期限とは

第 12 条第 3 項では、データ管理者は、「行われた措置に関する情報」を「不当な遅滞なし」に、いかなる場合でもその要求を受け取ってから 1 カ月以内に、データ主体に提供しなければならないと定めている。この 1 カ月の期間は、要求が複雑な場合は最長 3 カ月まで延長することができるが、その場合、管理者は、要求を受け取ってから 1 カ月以内に、遅滞の理由をデータ主体に通知しなければならない。

コメント 13：データポータビリティの権利行使の対応フロー
データポータビリティの権利行使への回答には期限があるため、権利行使に関する連絡を受けた部署がどのようなフローで管理者としての対応を決定するか、組織内で事前に整理しておく必要がある。組織構造や個人データ処理の内容によっては、欧州統括拠点が行う場合や EU 域外の拠点が行う場合もあるため、そのような観点からもフローを検討しておく必要がある。

情報社会サービス[33]を運営するデータ管理者は、要求に対してごく短時間で応じることができるようにより良い設備が備わっている可能性が高い。ユーザーの期待に応えるために、データポータビリティの要求に標準的に応じることができる期限を決め、それをデータ主体に連絡することがグッド・プラクティスである。

データ管理者がポータビリティの要求に応じない場合、第 14 条に従って、データ管理者はデータ主体に対し「その拒否の理由、および監督当局に苦情を申し立て、法的救済を求めることができる旨」を、要求を受けてから 1 カ月以内に通知しなければならない。

データ管理者は、たとえそれが拒絶の内容であっても、与えられた期限内に応答する義務に従わねばならない。すなわち、データ管理者はデータポータビリティの要求に応じるよう求められた時に、ただ沈黙を守り続けることはできない。

コメント 14：データポータビリティの権利行使に回答する義務
データポータビリティの権利行使に応じない場合にも、管理者はその旨を回答する義務がある。

(4) どのような場合にデータポータビリティの要求を拒むまたは料金を課することができるか

第 12 条は、その要求が明らかに無根拠または過度であり「特に反復する性質による」場合であることを証明できる場合を除き、データ管理者が個人データの提供に課金することを禁じている。個人データの自動化された処理に特化した情報社会サービスにとって、アプリケーション・プログラミング・インターフェイス（API）[34]などの自動化されたシステムを実施することは、データ主体とのやり取りをより容易にし得るものであり、反復した要請から生じる潜在的な負担

[33] （指令 98/34/EC 第 1 条第２項、指令 98/48/EC）サービスの受け手となる個人の要請を受け、電子的手段によって遠隔的に、通常対価のために提供されるあらゆるサービスのこと。

[34] （原文脚注 27）API とは、データ管理者のシステムがその他のシステムまたはアプリケーションとリンクし、共に作動できるように、データ管理者が提供するアプリケーションまたはウェブサービスのインターフェースを意味する。

Copyright (C) 2018 JETRO. All rights reserved.

を軽減するものである。データ管理者が要求された情報提供を拒否することを正当化できるケースは、たとえ複数のデータポータビリティの要求があったとしても、極めて稀である。

さらに、データポータビリティの要求に応じるために作成された処理の全体的なコストは、要求が過度か否かを判断する上で考慮されるべきではない。実際に、GDPR 第 12 条は、データ管理者が複数のデータ主体から受け取る要求の件数ではなく、単一のデータ主体が要求する件数に重点を置いている。従って、全体的なシステム実装費用はデータ主体に課金されるべきではなく、また当該費用を根拠としてポータビリティの要求を拒むことはできない。

コメント 15：データ主体の無償の権利行使が可能であること

データ主体は、第 12 条第 5 項に基づき、無償でデータポータビリティの権利を含む権利行使を行うことができる。

5. ポータブルデータはどのように提供されるべきか

(1) データ管理者がデータの提供のために実施することが期待される方法とは

GDPR 第 20 条第 1 項は、データ主体が、個人データを提供した管理者からの妨害を受けることなく、データを他の管理者に移転する権利を有するものと規定している。

当該妨害は、データ主体または別のデータ管理者によるアクセス、送信または再利用を抑制し、または遅らせるために、管理者がもたらす法的または技術的、経済的な障害と特徴づけられる。例えば、当該妨害は、データの送信のために要求される手数料、データ形式・API・提供される形式の相互運用性またはアクセスの欠如、完全なデータセットの回収に関する過剰な遅延または複雑性、データセットの意図的な難読化、不当または過剰な特定のセクターに特化した標準化または認証要求、の形態をとり得る[35]。

第 20 条第 2 項は、「技術的に実現可能な場合」にポータブルデータをその他のデータ管理者に直接送信することをデータ管理者に対して義務付けている。

コメント 16：技術的に実現可能か否かの検討および文書化

技術的な実現可能性は解釈に幅が生じ得る概念であるが、管理者は個人データの転送の要請に応じない場合は、技術的に実現可能ではないことについて説明する責任を負う（第 12 条第 4 項）。従って、管理者は、技術的な実現可能性の有無の判断過程について説明できるように、文書化しておくことが望ましい。

データ主体のコントロール下での、データ管理者からデータ管理者への転送信の技術的な実現可能性は、ケースバイケースで評価すべきである。前文第 68 項は、「管理者が技術的に適合する処理システムを採用、または維持する義務を発生させるべきではない」と規定しており、何が「技術的に実現可能」であることの限度を一層明確にしている。

[35] （原文脚注 28）いくつかの正当な障害は、第 20 条第 4 項で言及される他者の権利および自由との関連において、また、管理者のシステムの安全性との関連において、発生する可能性がある。データ管理者は、当該障害が正当なものとなり得るものであり、第 20 条第 1 項の意味するところの妨害を構成するものではないことを正当化する責任を負う。

Copyright (C) 2018 JETRO. All rights reserved.

データ管理者は、相互運用可能な形式によって個人データの転送を行うことが期待されるが、このことは、その他のデータ管理者に対して当該形式を維持することを義務付けるものではない。ある管理者から別の管理者に対して直接の転送が行われる可能性があるのは、2 つのシステム間で安全な方法[36]でコミュニケーションを図ることが可能であり、かつ受信側のシステムが送信されたデータを技術的に受信できる状況にある場合である。

技術的な障害が直接的な送信を妨げている場合、データ主体の要求に対して措置を講じることを拒否したことと実質的に同様の決定を行ったことになることから（第 12 条第 4 項）、データ管理者はこれらの障害をデータ主体に説明することが規定されている。

技術的なレベルにおいて、データ管理者は、ポータブルデータをデータ主体またはその他のデータ管理者に利用可能とするために 2 つの異なる補足的な方法を検討、評価する必要がある。

- ポータブルデータのデータセット全体の直接的な送信（またはデータセット全体の複数の箇所の抜粋）
- 関連するデータの抜粋が可能となる自動化されたツール

この 2 番目の方法は、データ主体の要求に応じた、データ主体に関連するデータセットの一部の抜粋を可能とするものであり、リスクを最小化する上で有益であり、データの同期メカニズム[37]の利用を許容し得るものであるため、複雑かつ大規模なデータセットが関わる場合において、データ管理者が（例えば、データ管理者の間での定期的なコミュニケーションの文脈において）優先的に選択するものと考えられる。この方法は、「新しい」データ管理者のコンプライアンスを確実なものとする上でより良い方法となり得るものであり、最初のデータ管理者側における、プライバシーに関するリスクを軽減するためのグッド・プラクティスの構成要素となるであろう。

関連するポータブルデータを提供するための、これら 2 つの異なった、おそらく補足的な方法は、様々な手段を通じてデータを入手可能にすることによって実行し得る。こうした手段としては、例えば、セキュアなメッセージ、SFTP サーバー、セキュアな WebAPI または Web ポータルなどが挙げられる。個人データを保有かつ保存し、データ管理者に必要に応じて個人データにアクセスし、処理を行う許可を与えるため、データ主体が、個人データ・ストア、または個人情報管理システム[38]、その他の信頼できる第三者によるその他の種類のものを利用できるようにすべきである。

(2) 期待されるデータ形式とは

GDPR はデータ管理者に対し、個人から要求された個人データを再利用可能な形式で提供することを要求している。具体的には、GDPR 第 20 条第 1 項は、個人データは「構造化され、一般的に利用され機械可読な形式で」提供されなければならないと規定している。さらに、前文第 68 項は、この形式は、次の通り定義されている[39]相互運用性を有すべきだとしている。

---

[36] （原文脚注 29）必要な水準のデータ暗号化を伴う認証されたコミュニケーションを通じて行う。

[37] （原文脚注 30）同期メカニズムは「個人データは正確でなければならず、必要な場合には更新されるものとする」と規定する GDPR 第 5 条に基づく一般的な義務を果たす上で有益である。

[38] （原文脚注 31）個人情報管理システム（PIMS）については、例えば、EDPS 意見書 9/2016 参照。
https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-10-20_PIMS_opinion_EN.pdf

[39] （原文脚注 32）「欧州行政機関における相互運用性ソリューション（ISA）に関する 2009 年 9 月 16 日付欧州議会・理事会決定 922/2009/EC」第 2 条（2009 年 10 月 3 日付 EU 官報 L260、20 ページ）

Copyright (C) 2018 JETRO. All rights reserved.

相互運用性：各々の ICT システム間でのデータ交換による、それぞれがサポートする業務プロセスを通じた組織間での情報や知識の共有を含む、異なる様々な組織同士が、相互利益および合意した共通の目的に向けて相互に作用する能力。

「構造化され」、「一般的に利用され」、「機械可読な形式」という文言は、データ管理者により提供されるデータ形式の相互運用性を促す最低限の要件のセットである。このように、相互運用性が望ましい結果であるのに対して、「構造化され、一般的に利用され、機械可読な」は、その手段の仕様である。

「公的セクター情報の再利用に関する指令 2003/98/EC を修正する指令 2013/37/EU17」の前文第 21 項は、「機械可読性」を以下のように定義している[40]。

機械可読性：個別の事実の記載を含む特定のデータを、ソフトウェア・アプリケーションが容易に特定、認識、抽出できるよう構造化されたファイル形式、およびその内部構造。機械可読な形式で構造化されたファイル内にエンコードされたデータは、機械可読なデータである。機械可読な形式は、オープン形式もしくは独自形式のいずれでもよく、正式な標準であってもなくてもよい。データが抽出できない、または、容易に抽出できないために、自動処理が限られたファイル形式でエンコードされた文書は、機械可読な形式とは見なされない。加盟国は、適切である場合、オープンで機械可読な形式を推奨すべきである。

データ管理者が処理する可能性があるデータの種類の多様性に鑑み、GDPR は、提供される個人データの形式に関する具体的な推奨を行っていない。最適な形式はセクターによって異なり、また適切な形式が既に存在し得るが、解釈可能で、データ主体に幅広いデータポータビリティを可能にするという目的を達成できる形式を選択すべきである。高額な費用を伴うライセンスの制約を受ける形式は、適切なアプローチとは見なされない。

GDPR 前文第 68 項は「データ主体が自身に関する個人データを転送もしくは受け取る権利は、技術的に互換性のある処理システムを採用もしくは維持することを管理者に義務付けるものではない」と明確に述べている。従って、ポータビリティは相互運用性のあるシステムの作成を目指すものであり、互換性のあるシステムを目指すものではない[41]。

個人データは、内部的な、または独自形式から高いレベルで抽象化された形式で提供されることが期待されている。従って、データポータビリティは、プラットフォームからデータを抽出し、かつポータビリティの範囲外の個人データ（推測データやはシステムのセキュリティに関するデータ）を除去するための、データ管理者による追加的なデータ処理の段階が伴うことになる。このように、データ管理者は、自己のシステム上でポータビリティの対象範囲内にあるデータを事前に特定しておくことが推奨される。しかし、このような追加のデータ処理は、データ管理者によって定義された新しい目的を達成するために実行されるものではないので、単に主たるデータ処理に付帯するものと見なされる。

---

[40] （原文脚注 34）EU 用語集（http://eur-lex.europa.eu/eli-register/glossary.html）は、機械可読性、相互運用可能性、オープンフォーマット、標準、メタデータなど、このガイドラインで使用される概念に関して期待される内容についてさらに明確に規定している。

[41] （原文脚注 35）ISO/IEC2382-01 は、相互運用性を次の通り定義している。「各種の機能単位の間で、利用者がそれらの機能単位に固有の特性をほとんどあるいは全く知ることなく、通信したり、プログラムを実行したり、データを送信したりできる能力」。

Copyright (C) 2018 JETRO. All rights reserved.

特定の産業または状況において一般的に使用されている形式が存在しない場合、データ管理者は、高度の抽象性を維持しながら、**可能な限り最高の粒度レベルの有益なメタデータと共に、一般に使用されるオープン形式（例えば、XML、JSON、CSV など）を用いて個人データを提供すべきである。**交換される情報の意味を正確に記載するために、適切なメタデータが使用されるべきである。このメタデータは、企業機密を明らかにすることなく、データの機能と、再利用を可能にするために十分な内容である必要がある。例えば、個人に対して電子メール受信箱を PDF 版で提供することは、受信箱のデータを容易に再利用することを可能とするために十分に構造化され、記述的な内容であるとは言えない。電子メールデータは、データを効果的に再利用できるよう、全てのメタデータを保持した形式で提供されなければならない。従って、個人データを提供するために使われるデータ形式を選択する場合、データ管理者はその形式が、データを再利用する個人の権利にどのように影響を与えるか、もしくはどのように妨げるかを考慮しなければならない。データ管理者がデータ主体に対して、希望する個人データの形式の選択を可能にできる場合、データ管理者はデータ形式の選択による影響について、データ主体に対して明確な説明をすべきである。しかし、データポータビリティの要求に応じる上で必要または要望があるかもしれない、という意図のみで追加のメタデータを処理することは、このような処理のための正当な理由とはならない。

第 29 条作業部会は、産業界の利害関係者や産業団体が協力し、データポータビリティの権利の要件を提示するために、相互運用性基準と形式の共通セットを作成することを強く推奨する。この課題については、欧州相互運用性フレームワーク（European Interoperability Framework：EIF）による取り組みも進んでいる。EIFは、共同で公共サービスを提供することを希望する団体のための、合意に基づく相互運用性のアプローチを策定した。その適用範囲内において、EIF は、用語、概念、原則、方針、ガイドライン、推奨事項、標準、仕様、プラクティスなどの共通要素の一式を明示している[42]。

(3) 大量または複雑な個人データにどのように対処すべきか

GDPRは、データ管理者またはデータ主体に困難をもたらし得る大量のデータの集合や、複雑なデータ構造、その他の技術的問題が発生した場合、そうした課題にどのように対応すべきか特に述べていない。

しかし、こうした場合も、データ管理者によって提供される可能性のある個人データの定義と概要、構造を、個人が完全に理解できる立場に置かれていることが極めて重要である。例えば、データ主体が個人データの全体ではなく一部を移動できるような「ダッシュボード」[43]機能を使用し、まずは要約形式のデータを提供することもあり得る。データ管理者は、データ主体が特定の目的に関連して、どのデータをダウンロードし、他のデータ管理者に転送できるかついて明確な情報を常に得られるように、「明瞭かつ平易な言葉で、簡潔で、透明性があり、理解しやすくかつ容易にアクセスし得る形態」（GDPR 第 12 条第 1 項を参照）で概要を提供すべきである。

例えば、データ主体は、ソフトウェア・アプリケーションを使って、特定のデータを容易に特定、認識、処理できる立場に置かれるべきである。

上述の通り、データ管理者がデータポータビリティの要求に応じることができる実務的な方法として、セキュアで適切に記述された API を提供するという方法が考えられる。これにより、GDPR 第 20 条第 2 項に指定されているように、個人は自身の個人データを自分のソフトウェアもしくは第三者のソフトウェアを使ってデータ管理者に要求することや、または（別のデータ管

42 （原文脚注 36）出所：http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf
43 複数の情報源からデータを集め、概要をまとめて一覧表示する機能や画面、ソフトウェアのこと。

Copyright (C) 2018 JETRO. All rights reserved.

理人などの）自分の代理人に許可を与えて要求させることができる。外部からアクセス可能なAPIを通じてデータへのアクセスを許可することで、データ管理者に負担をかけずに、完全なダウンロード、もしくは前回のダウンロードからの変更のみを含む差分機能として個人がデータを後から要求できるような、より洗練されたアクセスシステムを提供することも可能となり得る。

(4) ポータブルデータをどのように保護できるか

一般に、GDPR第5条第1項(f)号に従い、データ管理者は「適切な技術的または組織的対策を用いて、無権限または違法な処理に対する保護、および偶発的な滅失または破壊、または毀損に対する保護を含む、個人データの適切なセキュリティ」を保証しなければならない。

しかし、個人データをデータ主体へ送信することにより、次に述べるようなセキュリティの課題が生じる可能性がある。

データ管理者はどのように個人データを正しい相手に安全に届けるか

データポータビリティは、データ管理者の情報システムから個人データを取得することを目的としているため、データ送信は、そうしたデータに関する（特に送信中のデータ侵害に関する）リスク要因となる可能性がある。データ管理者は、正しい対象者へ（例：堅固な認証方法を使用）個人データを安全に送信すること（例：エンド・トゥ・エンド[44]またはデータ暗号化の使用）のみならず、システム内に留まる個人データを継続的に保護すると共に、データ漏洩が発生した場合の透明性のある対応手続きを確実に行うために、必要な全てのセキュリティ措置を講じる責任がある[45]。従って、データ管理者は、データポータビリティに関連する特定のリスクを評価し、適切なリスク軽減対策を行うべきである。

当該リスク軽減対策として考えられる、次のようなものなどを使用すべきである。

- データ主体の認証が既に必要な場合、「共有された秘密」などの追加の認証情報、またはワンタイムパスワードなどのその他の認証要素の使用
- アカウントが侵害されているとの疑義がある場合、送信の保留または凍結
- データ管理者から別のデータ管理者に直接送信される場合、トークンによる認証などの委任による認証

このような保護措置には、妨害的な特性があってはならず、ユーザーがその権利を行使するのを妨げるもの（例：追加コストの負担）であってはならない。

どのようにユーザーが自分自身のシステムに個人データを安全に保管することを支援するか

オンラインサービスから個人データを回収することにより、ユーザーがサービス会社によって提供されていた保管システムよりも安全性が劣るシステムにデータを保管するというリスクがある。データを要求するデータ主体は、自己のシステムにおける個人データを保護するために、正しい手段を特定する責任を負う。ただし、データ主体が自分が受け取った情報を守る処置をとるためには、この潜在的なリスクを認識する必要がある。リーディング・プラクティスの例として、データ管理者は、データ主体が安全な保管という目標を達成できるよう、適切な形式や暗号化ツール、その他の安全対策などをデータ主体に推奨し得る。

---

[44] 通信プロトコルの操作は可能な限り通信システムの終端で行い、また制御対象のリソースになるべく近いところで行うべきであるという原理。

[45] （原文脚注37）保護措置は「EUにおけるネットワークおよび情報システムのセキュリティの高度な共通水準のための対策に関する指令(EU)2016/1148」との適合性が必要。

Copyright (C) 2018 JETRO. All rights reserved.

レポートをご覧いただいた後、アンケート（所要時間：約１分）にご協力ください。
https://www.jetro.go.jp/form5/pub/ora2/20170096

「EU 一般データ保護規則(GDPR)」

（第 29 条作業部会ガイドライン編）

データポータビリティの権利

作成者　日本貿易振興機構（ジェトロ）海外調査部 欧州ロシア CIS 課

〒107-6006　東京都港区赤坂 1- 12-32

Tel.03-3582-5569

2018.2
Copyright (C) 2018 JETRO. All rights reserved.