特集 GDPR（EU一般データ保護規則）にどう取り組むか

GDPR対応の要諦と課題


小林慎太郎


名武大智


村瀬博俊

CONTENTS

要 約

1 EU（欧州連合）の新しい個人データ保護のルール「GDPR（EU一般データ保護規則）」が2018年５月25日に施行された。EEA（欧州経済領域）の住民の個人データを扱う場合に適用され、個人情報保護法よりも事業者に課される義務は格段に厳しく、違反時には高額の課徴金が科される。このため、EEAとかかわりのあるビジネスを展開している企業は対応が必要である。

2 GDPRが適用対象となる日本企業は、中小企業を含む全企業の１割弱と推計されるが、施行日を過ぎてもなお、多くの企業で対応が完了していない状況にある。そもそもGDPRへの認知や理解が低いこと、GDPRへの対応に時間がかかることが理由として考えられる。欧州の個人データ保護当局の執行体制がいまだ途上であるうちに、GDPRへなるべく迅速に対応していくことが重要である。

3 GDPRへ対応するための活動は、①欧州の個人データを取り扱う業務やデータベースの実態を把握して、講ずべきアクションを明確にする「計画フェーズ」、②越境移転規制への対応や規程類の整備など、基本的な体制を整備する「構築フェーズ」、③研修による現場への定着など、継続的にコンプライアンスを確保するための「運用フェーズ」、の３つのフェーズに区分される。各フェーズで押さえるべきポイントを紹介する。

4 GDPRには「忘れられる権利」をはじめ、個人が自身の情報をコントロールすることを認めるさまざまな権利が規定され、デジタルビジネスに取り組むすべての企業に対して、個人データの取り扱いに対する姿勢を、単なる事業者の義務から、より本質的な個人の権利保護へと改めることを迫っている。プライバシーバイデザイン／プライバシー影響評価の実践が求められている。

Ⅰ GDPRとは

GDPR（EU一般データ保護規則）は、2018年５月25日から施行された、EEA（欧州経済領域）というEU（欧州連合）を構成する28カ国にノルウェー、リヒテンシュタイン、アイスランドを含めた31カ国に共通して適用される個人データ保護の法律である。日本の個人情報保護法に相当するが、EUはプライバシーを重要な個人の権利としているため、保護対象とするデータの範囲は広く[注1]、事業者の義務も厳しい。何よりも課徴金が格段に高額で、違反すると最大で2000万ユーロか、世界年間総売上の４％のいずれか高い方を支払わなければならない。

これまでEUでは、1995年に発令された「EUデータ保護指令[注2]」（以下「指令」という）に基づき、各EU構成国が協調しつつ、個人情報保護に取り組んできた。しかし、インターネットが社会の隅々にまで行き渡って、ソーシャルメディアやスマートフォンなどが普及し、個人にまつわるデータが大規模に活用されるようになり、さらに近年では自動車の走行情報などのモノのデータまで分析されるなど、指令では想定していなかった形でのデータ活用がなされるようになった。

このため、一人一人が自分の情報を自分の意思でより確実にコントロールできるようにする必要が出てきた。また、EU単一市場政策を進めるにあたって、加盟国ごとに個人情報保護の法律が異なることの弊害も大きくなっていた（指令の施行にあたって、EU加盟国は個別に立法する必要があった）。

こうした状況から、GDPRは指令の基本理念を受け継ぎつつも、時代の変遷に合わせて個人の権利と事業者の義務を強化し、さらにそれをグローバルに通用するように刷新したのである。以下では主な規制について紹介する（表１）。

１　規則のEU域外への適用

物品やサービス提供などのためにEU住民の個人データを取り扱う場合は、EUにオフィスがあるかどうかは関係なく、企業はGDPRを遵守しなくてはならない。これは、プライバシーの権利はデータと一体不可分であり、EU域外で取り扱われる場合であっても域内と同じように保護されなければならないという思想による。

表1　GDPRの主な規制と違反時の課徴金

規則のEU域外への適用

EU域外へのデータ持ち出し制限
- EU住民の個人データは、特別な契約なしに日本へ持ち出せない

ビッグデータビジネスへの牽制
- 通知と同意の義務
- 忘れられる権利
- データポータビリティの権利
- プロファイリングを拒否する権利

台帳とリスクに応じた体制
- 個人データ台帳
- プライバシー影響評価（PIA）
- データ保護責任者（DPO）

漏洩時の通知
- 漏洩発覚後72時間以内に当局へ通知、本人にも速やかに通知

違反時の課徴金
最大で全世界における年間売上高の4%、または2,000万ユーロのいずれか高い方

2　EU域外へのデータ持ち出し制限

EUは、独自の基準に照らして個人データの保護が十分でないと判断される国へのデータの移転を規制（以下「越境移転規制」という）している。日本は、EUから個人データの保護が十分であると認められていないため、EU住民の個人データを日本へ持ち出すためには、EU当局の指定する特別な契約を締結しなければならない。

越境移転規制は、日本にとって、EUとの交易に直接的にかかわる長年の懸案事項であったが、個人情報保護委員会が規制解消に向けた交渉を続けており、2018年秋には実現する見込みである[注3]。

3　ビッグデータビジネスへの牽制

個人にまつわるデータを大量に収集して、さまざまな目的に利用するビッグデータビジネスからプライバシーを守るため、GDPRでは個人の権利が大幅に強化されている。グーグルやフェイスブックといった巨大IT企業を狙い撃ちしたとも揶揄されることがある。

個人データを取り扱う場合、本人から直接収集するケースと第三者から間接的に収集するケースの両方において、本人に通知しなくてはならない項目が厳格に規定されている。また同意の取得にあたっても、条件が細かく規定されており、適切に対応しないと無効と判断される恐れがある。

「忘れられる権利」は、本人が個人データの消去を要求できる権利である。斬新な発想と情緒的なネーミングで世の耳目を引いたが、個人データの消去の仕組みは実装することが難しく、多くの企業にとって課題となっている。

「データポータビリティの権利」は、自身の個人データを持ち運びできるように、機械判読可能な形式で提供してもらうことを企業に要求できる権利である。巨大IT企業による個人データの寡占的な集積を解消し、個人の選択の自由の確保と市場活性化が権利創設の背景にある。

「プロファイリングを拒否する権利」は、機械処理のみによるプロファイリングを拒否することができるというもの。検索履歴や購買履歴などを解析して個人の趣味嗜好に合わせたサービスを提供する場合、背後で何らかのプロファイリングをしているため、同権利への対応が必要になる。

4　台帳とリスクに応じた体制

企業は、個人データの取り扱いを記した台帳を整備しなくてはならない。また、企業がプライバシーリスクの高い個人データの取り扱いをする場合、事前にその影響を評価して、適切な対策を講じる「プライバシー影響評価（PIA：Privacy Impact Assessment）[注4]」を実施しなくてはならず、独立的な立場で企業内の個人データの取り扱いを管理する担当者「データ保護責任者（DPO）」を任命しなければならない。

5　漏洩時の通知

個人データの漏洩に気づいた場合、企業は72時間以内に当局に通知しなければならない。あわせて、本人にも速やかに通知しなければならない。

Ⅱ　日本企業の対応状況

既にGDPRは施行されているが、実際に日

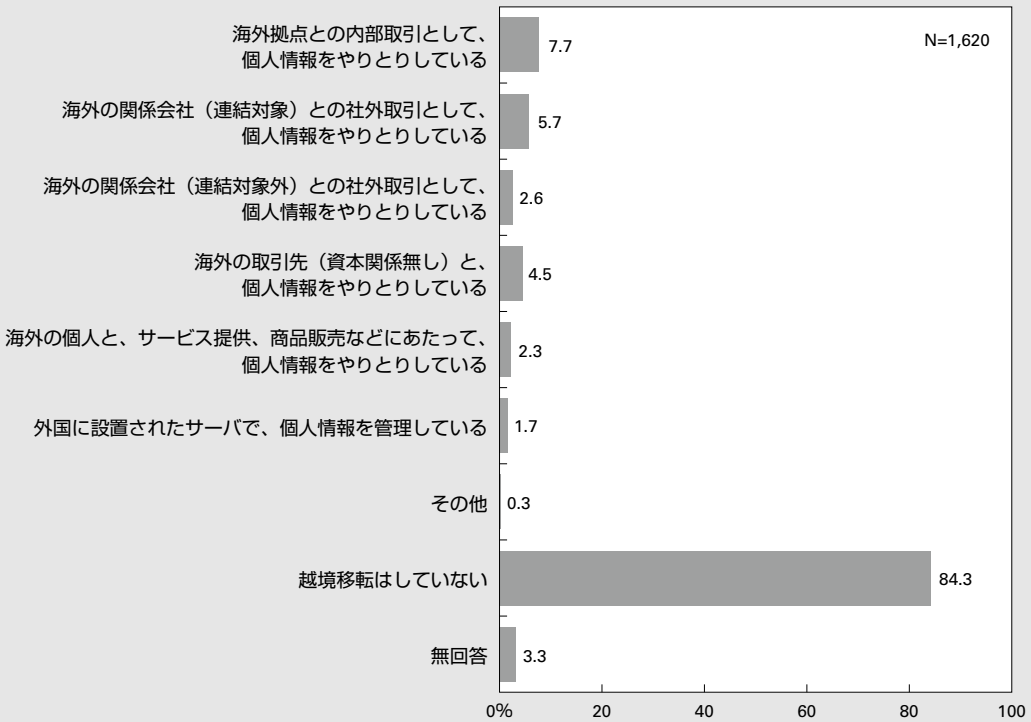
本企業はどこまで対応できているのであろうか。まず、どれだけの日本企業がGDPRの規制対象となるのか考える。

個人情報保護委員会の委託を受けて野村総合研究所（NRI）が実施した国内1620社を対象とする「個人情報の保護に関する事業者の取組実態調査」[注5]によると、全体の84.3％が、外国から日本への個人情報の「越境移転はしていない」と回答していることから、残りの約16％、およそ６社に１社が海外の個人情報を日本に越境移転しているものと推計される（図１）。さらに同調査によると、越境移転元となる外国の50.0％はEUなどの地域であることから、GDPRの適用対象となり得る日本企業は約８％、およそ12社に１社と推計される。すなわち、１割弱の日本企業がGDPRの規制を受ける可能性があると考えられる。

では、日本企業におけるGDPRへの対応はどのような状況なのか。日本経済新聞がGDPR施行直前（2018年５月23日）に、国内主要100社に対して実施したアンケートによると、GDPRへ「必要な対策はすべて終えた」と回答した企業は21％にとどまり、全体の８割の企業が対応を完了していない状況となっている[注6]。

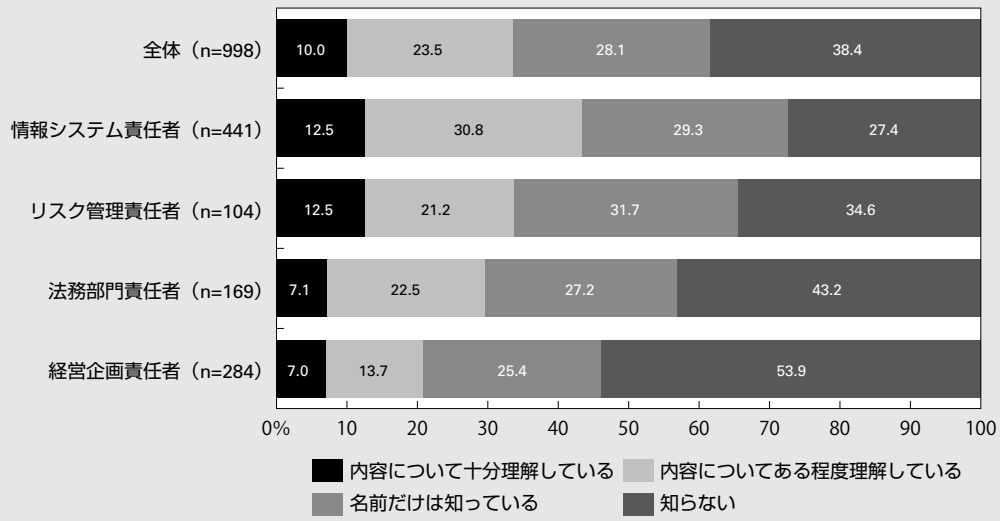
対応が遅れる背景としては大きく２点が考えられる。一つ目はGDPRに関する認知・理解不足である。トレンドマイクロが18年４月に国内事業者に対して実施した、GDPRに関する認知度・理解度の調査[注7]の結果では、「内容について十分理解している」と回答したのは全体のわずか10.0％にとどまった（図２）。このアンケートの対象者は、情報システム責任者、リスク管理責任者、法務部門責任者といった、GDPR対応において主導的な役割が期待される部門の責任者であることから、

図1　日本企業による外国から日本への個人情報の越境移転の状況



出所）野村総合研究所「個人情報の保護に関する事業者の取組実態調査（平成29年度）報告書」（2018年3月）

図2　GDPRに関する認知度・理解度



出所）トレンドマイクロ「EU一般データ保護規則（GDPR）対応に関する実態調査」2018年5月17日

GDPR対応に向けた認知や理解が十分には進んでいないことがうかがえる。

対応が遅れるもう一つの理由は、そもそもGDPR対応には時間がかかることである。GDPR対応を進めるためには、まず社内の全部署に対して、GDPRの適用対象となる個人データの取り扱いを棚卸しして実態を把握する「データマッピング」と呼ばれるタスクの実行が必要である。このデータマッピングの作業には、一般に数カ月を要するといわれ、責任者がGDPRについて十分に認知・理解できていなかったり、海外の窓口担当者との意思疎通に問題があったりすると、さらに時間を要することになる。

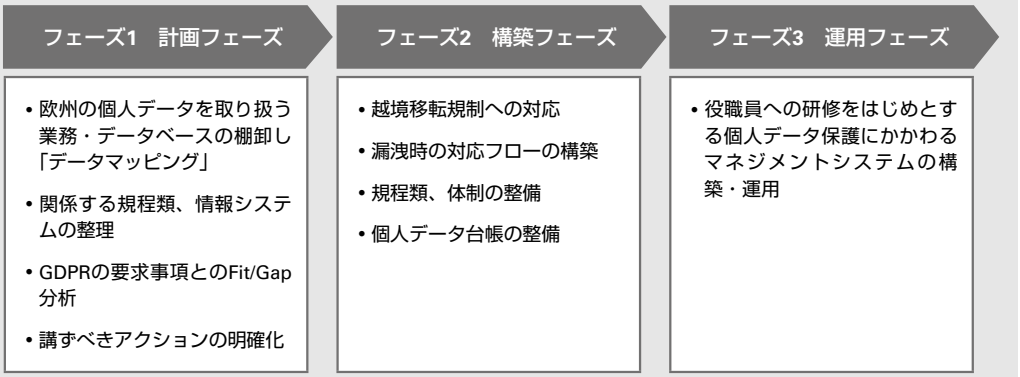
また、情報システムで個人データを管理している場合、サーバがどこの国に所在しているのか、クラウドを利用している場合、その事業者はGDPRに準拠しているのかなど、GDPRならではの確認項目も多い。こうしてデータマッピングに想定以上に時間がかかってしまい、その後のGDPR要求事項への具体的なアクションに遅れが生じてしまうことも多いと思われる。

一方、GDPRを所管する欧州の個人データ保護当局も、いまだGDPRを運用するための体制が十分に整っている状況とはいえない。ロイターの調査[注8]によれば、回答のあった24カ国の個人データ保護当局のうち17カ国で、十分な資金や体制が整わず、GDPRを運用するための準備を完了できていないという。予断を許さない状況にあるが、当局側の準備がいまだ途上であるうちに、GDPRへなるべく迅速に対応していくことが重要である。

Ⅲ GDPRへの対応の要諦

GDPRへ対応するための活動は、①欧州の個人データを取り扱う業務やデータベースの実態を把握して、講ずべきアクションを明確にする「計画フェーズ」、②越境移転規制へ

表2　GDPR対応の3つのフェーズ



の対応や規程類の整備など、基本的な体制を整備する「構築フェーズ」、③研修による現場への定着など、継続的にコンプライアンスを確保するための「運用フェーズ」、の3つのフェーズに区分される（表2）。以下では、各フェーズを進めるにあたって押さえるべきポイントについて述べる。

1　計画フェーズ

個人情報保護法へ対応するための活動と同じように、GDPRへの対応活動はここまでやればよいという一律の基準があるわけではない。各企業が、個人データの取り扱い実態を踏まえてプライバシー侵害のリスクを受容できる水準を考え、そのための管理の仕組みを自ら模索して構築しなければならない。

このため、GDPRへの対応は、欧州の個人データを取り扱う業務やデータベースを棚卸しして、取り扱いの実態を把握する「データマッピング」から始まる。個人データの取り扱い実態を明らかにし、GDPR要求事項との適合性の評価（Fit/Gap分析）を行って、講ずべきアクションを明確化する。

データマッピングでは、GDPRの要求事項について、アンケートやヒアリングなどの方法で、現場の個人データ管理を行っている担当者へ照会する。この際、個人情報保護法との違いとして、（1）個人データの対象、（2）個人データを取り扱う根拠、（3）データ管理者とデータ処理者の関係、の3点に注意する必要がある。

（1）個人データの対象

GDPRにおける個人データの定義[注9]は、個人を識別する可能性のある情報を幅広く包含するように記載されており、実際に日本の個人情報保護法では非個人情報とされるものも含まれるため、データマッピングの対象から漏れてしまわないように注意が必要である。

具体的には、欧州委員会のWebサイトで掲げられている例にある通り、IPアドレス、クッキーID、携帯電話の広告ID、さらには携帯電話の位置データまでが含まれている（表3）。こうしたデータは、過去の個人情報保護法の改正作業の中で個人情報に含めるべきか検討されたが、産業界から強い反対があって見送られた経緯がある。

表3　個人データに該当する例、該当しない例

個人データに該当する例	個人データに該当しない例
• 氏名 • 自宅住所 • name.surname@company.comのような電子メールアドレス • 位置データ（例：携帯電話で用いられる位置データ） • IPアドレス • クッキー ID • 携帯電話の広告ID	• 法人登録番号 • info@company.comのような電子メールアドレス • 匿名化されたデータ

出所）欧州委員会Webサイト“What is personal data?” https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en（2018年6月確認）

（2） 個人データを取り扱う根拠

GDPRでは、個人データを取り扱う場合、その根拠を明確にすることが求められる。言い換えると、適切な根拠がない限り、個人データの取り扱いは認められない。個人情報保護法にはない概念であるが、EUでは個人データの取り扱いにあたって重要視されるため、データマッピングの際に意識して確認することが肝要である。

個人データを取り扱う根拠には6種類あり、このうちのいずれか、または複数に該当することを、個人データの取り扱いやデータベースごとに確認する（表4）。

表4　個人データを取り扱う根拠（GDPR第6条）

(a) 本人が、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り扱いに関し、同意を与えた場合。

(b) 本人が契約当事者となっている契約の履行のために取り扱いが必要となる場合、又は、契約締結の前に、本人の要求に際して手段を講ずるために取り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り扱いが必要となる場合。

(d) 本人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り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り扱いが必要となる場合。

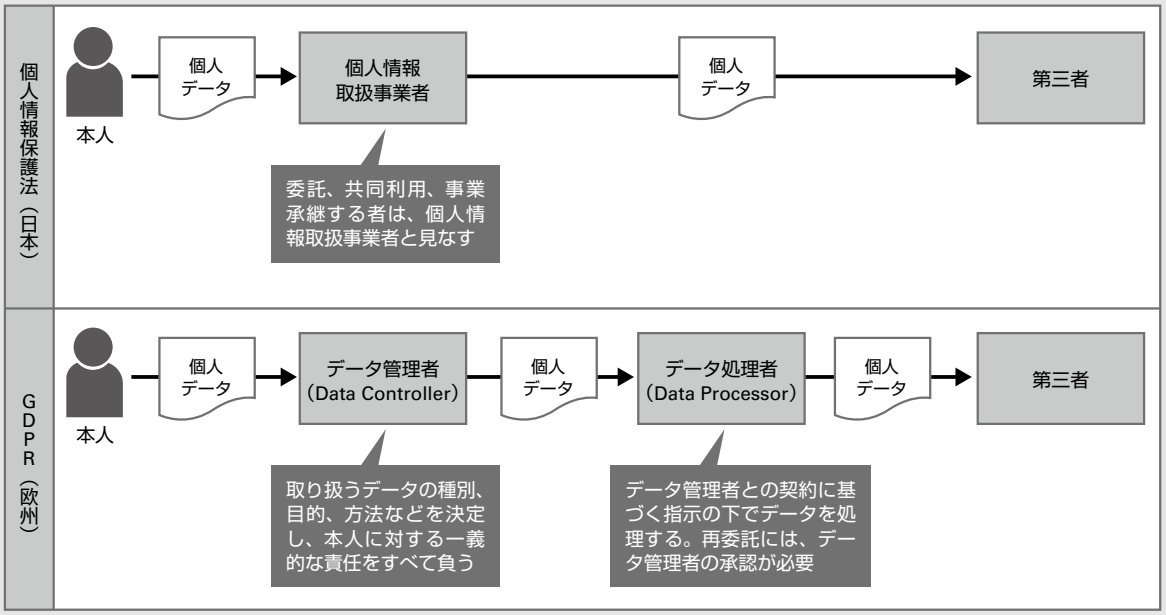
(f) 管理者によって、又は、第三者によって求められる正当な利益の目的のために取り扱いが必要となる場合。ただし、その利益よりも、個人データの保護を求める本人の利益並びに基本的な権利及び自由のほうが優先する場合、特に、その本人が子どもである場合を除く。

（3） データ管理者とデータ処理者の関係

GDPRでは、個人情報保護法では登場しない「データ処理者（Data Processor）」というアクターの位置づけと役割を理解する必要がある（図3）。日本の個人情報保護法では、登場する主体は大きく分けると、本人、個人情報取扱事業者、第三者という3者である。委託、共同利用、事業承継する相手の事業者は、個人情報取扱事業者と一体のものと見なすことに合理性があるとして、第三者には該当しないものとされている[注10]。

一方、GDPRでは、登場する主体は、本人、データ管理者（Data Controller）、データ処理者（Data Processor）、第三者の4者となっている。データ管理者の位置づけは日本の個人情報取扱事業者におよそ対応するが、データ処理者（Data Processor）については、役割としては委託先や下請け事業者に相当する場合があったとしても、そもそもの位置づけがない。この4者が登場するモデルは、国際標準規格「ISO/IEC29100：プライバシーフレームワーク」においても採用されてお

図3　日本とGDPRやISO/IEC29100規格のアクターの比較



り、EUに限らず諸外国で広く通用するものである[注11]。

データ処理者とは、GDPRによると、「データ管理者の代わりに個人データを取り扱う主体」として定義されているだけだが、英国の情報コミッショナーの解説[注12]によると、データ処理者には、マーケティング会社、決済事業者、ITベンダーやクラウド事業者のようなITサービス事業者、さらには弁護士・会計士といった専門家も該当する。一方、郵便・宅配事業者は、宛名を除き直接個人データを処理する主体ではないので、データ処理者に原則該当しないとされる。

2　構築フェーズ

本フェーズでは、GDPRの仕組みを計画フェーズで策定したアクションプランに基づいて構築する。以下では、優先的に対応が求められる活動の要諦について述べる。

（1） 越境移転規制への対応

前述の通り、EUは独自の基準に照らして、個人データの保護が十分でないと判断される国へのデータの移転を制限している。これまで日本は保護が十分であるとはEUから認められておらず、この結果、EUから個人データを日本に移転するためには、企業は特別の契約[注13]を、各EU加盟国当局の監督の下で交わさなければならない状況にあり、大きな負担となっていた。

しかし、先の個人情報保護法の改正により、GDPRの保護水準に大きく近づいたことを踏まえ、個人情報保護法を所管する個人情報保護委員会がEU当局と対話を続け、EUから日本の個人情報保護制度の十分性が認定されて（以下「十分性認定」という）、越境移転規制が解除されることが確実な情勢となっている[注14]。

ただし、十分性認定は無条件ではない。

表5　個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン（EU域内から十分性認定により移転を受けた個人データの取扱い編）（案）」で示された義務

1. **要配慮個人情報の範囲**
   - 性生活、性的指向（LGBT）、労働組合を、要配慮個人情報として扱う
2. **保有個人データの範囲**
   - 6カ月以内に消去することとなる個人データについても保有個人データとして扱う
3. **利用目的の特定**
   - 第三者から提供を受けた個人情報について、利用目的を特定する
4. **日本から外国への個人データの再移転**
   - 本人の同意に基づき再移転する場合は、契約などで保護措置を確保する
5. **匿名加工情報**
   - EUから移転された個人データを匿名加工情報として扱う場合、加工方法に関する情報を削除する

EU当局からGDPRと比較して、個人情報保護法が不足すると判断された5項目について、制度的に担保することが求められたのである。このため、個人情報保護委員会は、新たにガイドライン（「個人情報の保護に関する法律についてのガイドライン（EU域内から十分性認定により移転を受けた個人データの取扱い編）（案）」）を策定し、EUから個人データを日本国内に移転する場合に、事業者が守るべき義務を上乗せすることにしたのである（表5）。

十分性認定が確定した後は、日本の事業者は、このガイドラインへ対応することでEUから個人データを移転することの適法性を確保することができ、越境移転規制への対応にかかわる負担は大幅に軽減されることになる。なお、EUから受け取った個人データを日本からさらに第三国へ移転したり、または第三国にあるサーバで個人データを管理したりする場合は、別途、越境移転規制対応が生じることがあるので留意が必要である。

（2） 漏洩時の対応フロー

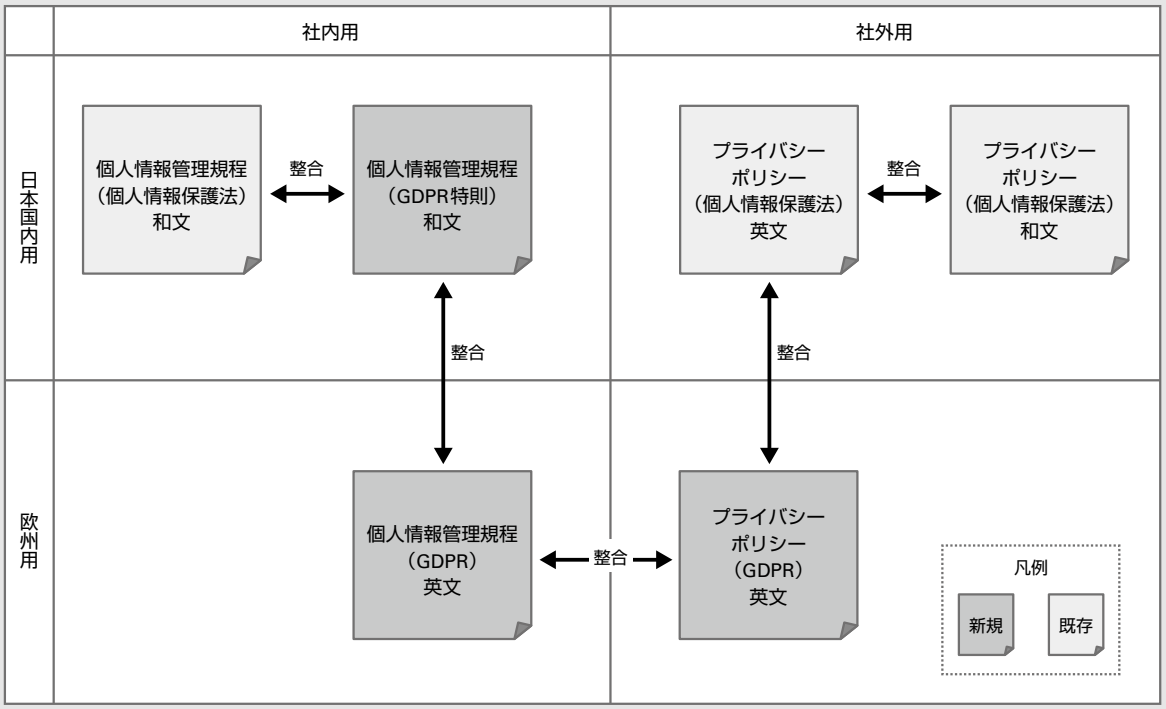
漏洩時の対応は、事故の事実を認知してから72時間以内に当局へ通知すること、本人にも速やかに通知すること、の2点がデータ管理者に義務づけられており、単に社内ルールを整備するだけではなく、実際に機能する仕組みを整えなければならない。このため社内のレポートラインを明確にした上で、複数の事故発生シナリオを想定して、連絡、意思決定ができるプロセス、体制を整備する。

GDPRは欧州の法律であり、その規制は日本にも適用されるとはいっても、常に欧州の規制当局が日本に来て企業の個人データの取り扱いを監督することはない。しかし、大規模に欧州人の個人データの漏洩事件が発生したとなると話は別で、重い課徴金が科される可能性がある。漏洩時の対応については、越境移転規制とともに、優先して対応すべき課題である。

（3） 規程類の整備

これまで、個人情報保護法を念頭に整備されてきたプライバシーポリシーや個人情報管理規程といった規程類を、GDPRに対応させようとする場合、①GDPRの内容を取り込んで規程類を再構築する、②GDPRに関する規

図4　個人情報保護規程とプライバシーポリシーの構成例



程を別途とりまとめ、欧州の個人データを取り扱う場合にのみ適用する、という大きく分けて2つの選択肢が考えられる。EU向けに事業を大規模に展開する事業者は前者を選択することがあるが、そのほかの多くの事業者は後者を選択するのが一般的であるため、ここでは後者の方式について述べる。

一般に、個人情報の取り扱いを定める規程類は、社内用に用いるものと社外用に用いるものとを分けて整備・運用されている。ここでは社内用を「個人情報管理規程」、社外用を「プライバシーポリシー」と便宜的に呼ぶことにすると、新規に整備が必要なのは、GDPRに対応した個人情報管理規程とプライバシーポリシーである。欧州用には英文（または現地語）での整備が必要となるため、規程間の整合性を確保しながら作成することが重要である（図4）。

3　運用フェーズ

GDPRへ対応するための仕組みを一通り整えた後は、それを実際に日々の業務の中で運用して定着を図っていく必要がある。前フェーズまでのような期限付きの取り組みとは異なり、定常業務として行うことになる。本フェーズでポイントとなる役職員への研修、情報セキュリティ部門との連携、定期的なモニタリングについて述べる。

（1）役職員への研修

個人情報保護法と同じく、GDPRへのコンプライアンスを確保するためには、組織の上層部から末端まで研修を行うことが必要である。一方で、すべての役職員に対して同じ水

準の理解を求めることは現実的には難しい。このため、個人データの保護責任者向けと、一般の役職員向けとの二つに研修プログラムを分けて実施することが効率的である。具体的には、個人データの保護責任者向けには集合研修やワークショップなどによって、GDPRの趣旨から具体的なプラクティスまでを身につけてもらい、一般の役職員に対しては、eラーニングなどでGDPRを認知・理解してもらうことが有効である。

(2) 情報セキュリティ部門との連携

個人データの保護部門と情報セキュリティ部門とは業務で重なる部分があり、別々に運用すると現場にとって負担感が大きくなる。このため、両部門が連携して、効率的に役割分担をしていくことが重要である。たとえば、情報セキュリティ部門が作成する研修プログラムにGDPRを含む個人データ保護の内容を一体化させたり、個人データの漏洩の業務を、情報セキュリティ部門が主管する機密情報のインシデント報告ルートと一体的に運用したりすることが考えられる。

(3) 定期的なモニタリング

ビジネスを取り巻く環境は日々変化しており、それに合わせて個人データの保護のあり方も見直しが必要である。特にGDPRは施行されたばかりであり、今後、新たにガイドラインが出されたり、執行事例が出て、判断基準が示されたりすることが想定される。定期的に規程類の見直しを行ったり、モニタリング調査を行って、現場の個人データの取り扱い状況を確認したりするなど、不断の努力が肝要である。

Ⅳ デジタルビジネスにおける課題——プライバシーバイデザインをいかに実践するか

GDPRには「忘れられる権利」「プロファイリングを拒否する権利」「データポータビリティの権利」など個人の権利が規定され、個人データに対する本人のコントロールの権限を大幅に強化している。2012年1月にGDPRの草案が公表された時、これらの権利は、グーグルやフェイスブックなどの米国のビッグデータビジネスを狙い撃ちしている、と多くのメディアが報じた。しかし、これらの権利は、ビッグデータビジネスに限らず、ITを活用して収益を生み出そうとするデジタルビジネスに取り組むすべての企業に対して、個人データの取り扱いに対する姿勢を、単なる事業者の義務から、より本質的な個人の権利保護へと改めることを迫っている。

「忘れられる権利」を例にとって考えてみる。多くの企業において、これまで個人データを管理する場合、保管期限を定めて、期限が来たら消去するような運用はきちんと行われてこなかった。先般の個人情報保護法の改正によって、新たに消去の規定が入ったものの、努力義務の範囲にとどまっており、いまだ企業に普及しているとはいえない状況にある。大量の個人データが、無期限に保存されているのが多くの企業の実態であろう。

しかし、個人データを無為に保有し続けると、データの漏洩リスクが高まったり、古くて誤った情報に基づいて処理したりするリスクが高まる恐れがある。そこへ本人からの消去リクエストにも応えなければならなくなると、不要になったデータはなるべく迅速に消

去することが企業にとって合理的な選択となろう。このようにGDPRは企業に対して、発想の転換を促しているのである。

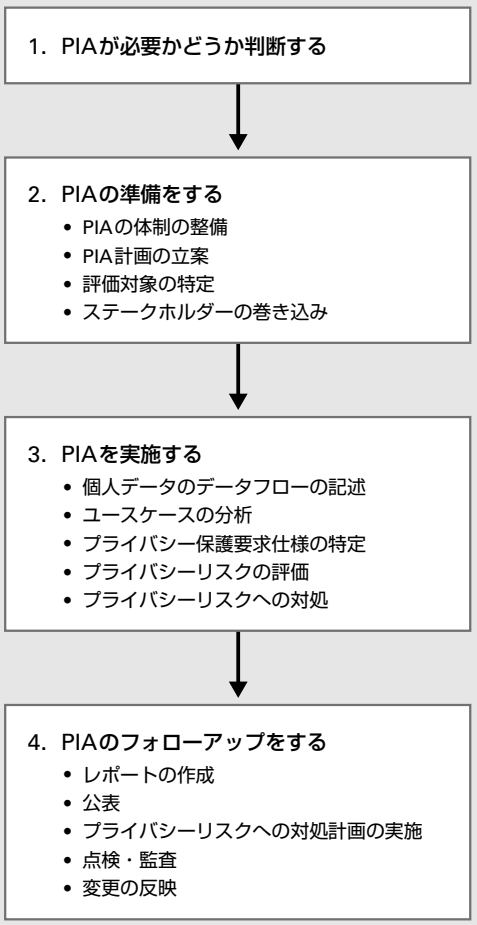
個人データを高度に取り扱うデジタルビジネスにおいて、忘れられる権利をはじめとする個人の権利へ対応するためには、業務や情報システムの設計段階から取り組む必要がある。これは文字通り、GDPRで新たに導入された概念である「プライバシーバイデザイン[注15]」であり、その具現化手法である「プライバシー影響評価（PIA：Privacy Impact Assessment）」の実践が求められている。

PIAの具体的な方法について“ISO/IEC 29134–Guidelines for privacy impact assessment”（以下「ISOガイドライン」）の考え方に基づいて紹介する。ISOガイドラインは、GDPRの施行に先立つ2017年に発行されている。ISOガイドラインの作成には、EUの個人データ保護当局の担当者が起草段階から参加しており、PIAの有効な手法として公式に承認されているものである[注16]。

ISOガイドラインでは、PIAの実施プロセスを４つのステップに分けている（図５）。

以下では、各ステップを順に見ていくことにする。

図5　PIAの実施手順*



*）ISO/IEC 29134–Guidelines for privacy impact assessmentによる

1　PIAが必要かどうか判断する

PIAを実施する必要があるのか、実施する場合はどの程度の規模で実施すればよいのかを最初の段階でふるい分けを行う。個人データを取り扱う事案は多く、すべてを対象に厳格なPIAを実施することは現実的ではなく、非効率でもあるからである。この手順は、「予備評価」「しきい値判断[注17]」などと呼ばれる。GDPRによる法定のPIA実施義務のある個人データの取り扱いについては、次の３つの類型が示されている。

①プロファイリングを含む自動処理に基づく判断によって、本人に重大な影響を及ぼすリスクがある場合（例：人事評価、信用力の評価）

②要配慮個人情報と関連する個人データを大規模に取り扱う場合

③公衆がアクセス可能な場所の、システムによる監視が大規模に行われる場合（例：監視カメラ）

さらなる詳細は、EU当局のガイドラインを参照されたい[注18]。ISOガイドラインのガイダンスでは、次のような場合に、PIAを実施することとしている。

- 新たな技術やサービス、取り組みにおいて個人データを取り扱う場合
- 機微な個人データを取り扱う場合
- 関連する法制度、社内の規程や標準、情報システムの運用、データ処理の目的や手段、データフローに変更があった場合
- 事業を拡大したり、吸収合併したりする場合

2 PIAの準備をする

PIAの実施が決まったら、PIAに必要な体制を整備し、計画を立て、評価対象を特定し、ステークホルダーの巻き込みを行う。ISOガイドラインでは、ステークホルダーの巻き込みについてさらに、ステークホルダーの識別、協議にかかわる計画立案、協議の実施、の3つのプロセスに分解して実施することを推奨している。

ステークホルダーには、個人データの本人、従業員や消費者の代表、委託先事業者、ビジネスパートナー、アプリやデータベースの管理者、ネットワーク管理者など、さまざまな主体が想定される。

PIAは、対象とする個人データの取り扱いに応じて、リスクの影響度も発生可能性も異なることから、リスクの評価基準を事案ごとに選定する必要がある。このため、透明性を確保しつつ、データ活用の便益とプライバシー保護とのバランスを追求するためには、ステークホルダーとの協議が重要で、PIAの準備段階でしっかり計画を立てておく必要がある。

3 PIAを実施する

PIAの実施は、データフローを記述し、ユースケースの分析を行い、プライバシー保護要求仕様を特定し、プライバシーリスクの評価、そしてリスクへの対処を行う。

データフローでは、誰が、誰から、何の個人データをどのように取得し、利用し、誰と共有し、誰へ提供するのかといった基本的なデータの流れを整理し、データの流れを可視化する。データの取得から廃棄までの一連の流れを記述し、データのライフサイクル全般での保護を検討するための基礎資料となり、ステークホルダーとの対話においても、全体感を共有するためのコミュニケーションツールとなる。

データフローが整理できたら、それを基にプライバシー関連リスクを抽出し、その影響を評価する。ここでは、データのライフサイクルごとに主なプライバシーリスクを例示する。なお、本稿はプライバシー保護が主眼のため、セキュリティに関するリスクの例示は最小限にとどめている。

①データの取得

- 利用目的が特定されていない、または制限されていない
- 提示した利用目的を超えてデータが取得される
- オプトアウトができない、または分かりづらい
- 初期設定において、本人が想定している以上にデータの共有・提供範囲が広い

②データの管理

- 本人が自己のデータへアクセスすることができない
- 本人がデータの利用停止（プロファイリング行為を含む）、消去、ダウンロードをすることができない
- 取得された情報が不必要に保存・管理されているため、重複レコードが生成され、データの正確性が損なわれる
- セキュリティ対策が十分に取られていない

③データの利用・提供

- 情報が利用・提供されるコンテキストが、時間を経るうちに変わってしまい、本人が認知しないまま違う目的で利用される。本人が同意した時のコンテキストから想定できないデータの利用がなされる
- 非個人データとして取り扱っていたデータが、ほかの情報との組み合わせによって、実質的に個人を識別してプライバシーを侵害するような利用がなされる
- データの共有・統合が、本人が想像するよりも幅広い範囲で行われる
- ほかのデータとの照合によって、プライバシーを侵害するような利用がなされる

④データの廃棄

- 廃棄のポリシーや仕組みが未整備で、データの不正利用や漏洩するリスクが高まる
- 廃棄行為としてデータの匿名化処理をする場合、匿名化レベルが不十分で、特定の個人が識別されるリスクがある

PIA実施の最後のステップは、評価結果を確実に反映させることである。プライバシーバイデザインの思想に基づくPIAでは、事前にリスクへ対処することが目的であるため、サービスや情報システムの設計にPIAの結果を取り込めるタイミングである、概念設計が終了するまでの間に反映する。

4 PIAのフォローアップをする

このプロセスでは、PIAの実施結果として、個人データの取り扱い、プライバシーリスク、及びリスクへの対処方策についてレポートに取りまとめ、ステークホルダーによる承認を得る。また、PIAは定期・不定期に見直しを行って、適宜個人データの取り扱いに反映させる。

先進諸外国の事例を見ると、公的機関の場合、PIAのレポートやレポートの概要を公開することが一般に行われている。一方、民間事業者では営業秘密やセキュリティを理由に、自発的にPIAレポートが公開されることはあまりない。ただし、個人データの利活用にあたって、プライバシー保護の説明責任（アカウンタビリティ）を高めるため、PIAレポートを作成し、個人データ保護当局から照会があった際には、迅速に開示できるようにしておくことが有効である。

多くの日本企業にとって、GDPRは厳しすぎると感じられるかもしれない。しかし、グローバルの視点で見ると、個人データ保護のルール形成に対するEUの影響力は大きく、南米やオセアニア、近年ではアジアに至るまで、諸外国の個人情報保護法制度が、GDPRを基準に見直されるようになってきている。すなわち、GDPRに対応することは、グロー

バルで個人データを保護する仕組み作りであり、それはデジタル時代に求められる基盤といえよう。

実際に、グーグルやフェイスブックなどの米国のビッグデータビジネスIT企業は、GDPRの厳しい基準をクリアするため、プライバシー保護担当者を多数採用して取り組んでいる。日本においても楽天のように、GDPRを基準にプライバシーポリシーを構成してグループ全体に展開している企業もある。

そう考えれば、GDPR対応は一過性のものではなく、長期的に腰を落ち着けて取り組むべき活動であることが理解できよう。そしてその活動は、顧客や従業員からの「信頼」という最も重要な資産となって、各企業の繁栄につながっていくものと思われる。

注

1 日本では、特定の個人を識別することのできる情報が「個人情報」として法制度の対象となるが、EUでは、個人の特定までには至らなくても個人を識別し得るデータは原則、法制度の対象となるとしている。たとえば、Web閲覧時に取得されるクッキーに関する情報は、日本では一般に非個人情報と解されているが、EUでは保護の対象として、データの収集・利用にあたっては、明示的に本人の同意を取得することを求めている

2 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

3 EUから日本への個人データの越境移転規制を大幅に緩和することについて日EU間で最終合意された（個人情報保護委員会「日EU間の相互の円滑な個人データ移転を図る枠組み構築に係る最終合意」2018年７月17日）

4 GDPRでは、Data Protection Impact Assessment（DPIA）と呼称されるが、国際規格をはじめ、世界的にプライバシー影響評価（PIA: Privacy Impact Assessment）と呼ばれることが多いため、本稿では、後者で統一して用いる

5 野村総合研究所「個人情報の保護に関する事業者の取組実態調査（平成29年度）報告書」（2018年３月）https://www.ppc.go.jp/files/pdf/personal_report_3003_jigyosya.pdf

6 日本経済新聞「EUデータ新規制GDPR、主要企業８割が対応未了」https://www.nikkei.com/article/DGXMZO30864980T20C18A5MM8000/

7 トレンドマイクロ「EU一般データ保護規則（GDPR）対応に関する実態調査」2018年５月17日 https://www.trendmicro.com/ja_jp/about/press-release/2018/pr-20180517-01.html

8 “European regulators:We’re not ready for new privacy law”2018年５月８日 https://www.reuters.com/article/us-europe-privacy-analysis/european-regulators-were-not-ready-for-new-privacy-law-idUSKBN1I915X

9 「個人データ」とは、識別された自然人又は識別可能な自然人（「データ主体」）に関する情報を意味する。識別可能な自然人とは、特に、氏名、識別番号、位置データ、オンライン識別子のような識別子を参照することによって、又は、当該自然人の身体的、生理的、遺伝的、精神的、経済的、文化的又は社会的な同一性を示す一つ又は複数の要素を参照することによって、直接的又は間接的に、識別されうる者をいう（GDPR第４条第１号）

10 経済産業分野ガイドライン第23条第４項関連の解説に基づく

11 ISO/IEC29100では、データ管理者を「個人識別情報（PII）管理者」、データ処理者を「個人識別情報（PII）処理者」として呼称する

12 情報コミッショナー局（ICO：Information Commissioner’s Office）“Data controllers and data processors: what the difference is and what the governance implications are”（2014年５月６日）

13 契約方法としては「標準契約条項（SCC：Stan-

dard Contractual Clauses)」または「拘束的企業準則（BCR: Binding Corporate Rules)」のいずれかを選択することができる

14 本稿執筆時点（2018年７月）では、いまだ十分性認定は確定していない

15 GDPRでは、データ保護バイデザイン“Data Protection by Design”と呼称されるが、国際規格をはじめ、世界的にプライバシーバイデザインと呼称されることが多いため、本稿では後者で統一して用いる。なおプライバシーバイデザインは、アン・カブキアン博士が提唱したもので、７つの原則（事前・予防的、初期状態で保護、設計への組み込み、すべてを機能させる、ライフサイクル全体を通じて保護、可視化・透明性、利用者を尊重）を適用する

16 筆者も、同規格の策定にISO/IEC JTC1/SC27日本代表団の一員として参加した

17 マイナンバー制度の特定個人情報保護評価における呼称

18 Guidelines on Data Protection Impact Assessment（DPIA）and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679（2017年10月４日採択）

著者

小林慎太郎（こばやししんたろう）
ICTメディア・サービス産業コンサルティング部
パブリックポリシーグループマネージャー／上級コンサルタント
専門はICT公共政策･経営。著書に『パーソナルデータの教科書――「個人情報保護」から「プライバシー保護」へとルールが変わる』（日経BP社、2014年）など

名武大智（なたけたいち）
ICTメディア・サービス産業コンサルティング部
副主任コンサルタント
専門は情報通信・精密機械・環境分野における市場環境分析、事業戦略および国内外の政策動向調査。個人情報に関しては、GDPR施行に伴う欧州各国の執行体制調査や、民間企業のGDPR対応支援を実施

村瀬博俊（むらせひろとし）
ICTメディア・サービス産業コンサルティング部コンサルタント
専門は情報通信・運輸物流・消費財分野における市場環境分析、事業戦略策定、業務改革および国内外の政策動向調査。個人情報に関しては、GDPR施行に伴う民間企業のGDPR対応支援を実施