改正個人情報保護法のポイントと EU 一般データ保護規則の概要

企業を取り巻く個人情報保護に係る規制への対応

西出 三輝 Mitsuteru Nishide
リスクマネジメント事業本部
ERM 事業部
上席コンサルタント

はじめに

個人情報保護法の一部を改正する法案が 2015 年 9 月 3 日に成立し、2017 年 5 月 30 日から全面施行された。今回改正された個人情報保護法（以下「改正法」）では、これまで個人情報保護法第 4 章（個人情報取扱事業者の義務等）の対象外であった事業者が対象に含まれたり、個人情報の取扱いについて新たな義務が課される等、様々な点が変更となっている。また、改正法は、平時における個人情報の取組みだけでなく、個人情報漏えい等の事態が発生した際に適切な対応に努めることも事業者に求めている。

さらに、個人情報保護法に関連する大きな動きとして、2017 年 7 月 6 日に日本と欧州連合（以下「EU」）が経済連携協定（EPA）および戦略的パートナーシップ協定（SPA）について大枠合意した際に、「個人データの越境移転に関する政治宣言[1]」も外務省から発表された。この政治宣言で、日本の個人情報保護法と EU の一般データ保護規則[2]（以下「一般データ保護規則」）については、双方で十分なレベルの保護を見出すことによりデータの交換を促進するための新しい枠組みを 2018 年の早期に作ることを日本と EU で確認した。そのため、2018 年に新しい枠組みを作ることを目指して、改正法及び関連するガイドラインなどが今後改正されることも考えられる。

本稿では、改正法で定められた平時の個人情報の取組みと個人情報漏えい等が発生した際の対応について改めて確認するとともに、一般データ保護規則の概要について解説する。

1. 改正法の概要

1.1. 改正の経緯

個人情報保護法は 2003 年に制定され、2005 年から全面施行された。しかし、現在、施行から 10 年以上が

[1] 「個人データの越境移転に関する政治宣言」の詳細については、同宣言の仮訳（外務省 HP, http://www.mofa.go.jp/mofaj/files/000270697.pdf, （アクセス日：2017 年 8 月 4 日））を参照。
[2] EU の一般データ保護規則の概要については、本稿 8 頁「3.一般データ保護規則」を参照。

経過し、情報技術（以下「IT」）・ネットワークの飛躍的な発展やグローバル化の進行など、社会の状況は当時と比較して大きく変化している。

そのため、2005 年に施行された個人情報保護法（以下「旧法」）では想定されなかった、以下のような個人情報の利活用による問題点が発生していた（表 1）。

表 1　個人情報の利活用に係る問題点[3]

①個人情報に該当するかどうかの判断が困難な、いわゆる「グレーゾーン」となるデータの種類が拡大している。
②パーソナルデータ[4]を含むビッグデータの適正な利活用ができる環境が整備されていない。
③事業活動がグローバル化したにもかかわらず、国境を越えたパーソナルデータの流通に対する環境が整備されていない。

これらの問題点に対応し個人情報の保護を図るとともに、事業者によるパーソナルデータの円滑な利活用を促進させ新産業・新サービスを創出するための環境を整備することを目的に、今回、旧法が改正された。

1.2. 主な改正のポイント

改正法は、旧法と比較して主に以下の点が改正された（表 2）。

表 2　改正法の主なポイント[5]

①個人情報保護委員会の新設 ・個人情報保護に関する独立した機関の創設
②法令の規制対象の拡大 ・取扱う個人情報が 5,000 件以下である事業者を規制の対象外とする制度を廃止
③個人情報の定義の明確化 ・個人情報の定義に身体的特徴等が対象になることを明確化 ・要配慮個人情報を新たに定義
④個人情報の有用性の確保 ・匿名加工情報の利活用に係る規定を新設
⑤適正な個人情報の流通を確保 ・オプトアウトの手続きの厳格化 ・個人データの第三者提供に係る確認記録作成等を義務化 ・個人情報データベース等不正提供罪の新設
⑥個人情報の取扱いのグローバル化 ・外国にある第三者への個人データの提供制限、個人情報保護法の国外適用、個人情報保護委員会による外国執行当局への情報提供に係る規定を新設

（1）個人情報保護委員会の新設

旧法では、事業分野ごとに主務大臣が事業者を監督していた。しかし、改正法では、監督権限は個人情報保護委員会に一元化された。

個人情報保護委員会は、個人情報の有用性に配慮しつつその適正な取扱いを確保するために設置された国

[3] 個人情報の利活用と保護に関するハンドブック,個人情報保護委員会,P1,https://www.ppc.go.jp/files/pdf/personal_280229sympo_pamph.pdf ,（アクセス日：2017 年 8 月 4 日）をもとに当社作成

[4] パーソナルデータとは、「個人情報」に限定されない、個人の行動・状態に関するデータを示す。

[5] 個人情報の利活用と保護に関するハンドブック,個人情報保護委員会,P2,https://www.ppc.go.jp/files/pdf/personal_280229sympo_pamph.pdf ,（アクセス日：2017 年 8 月 4 日）をもとに当社作成

の独立機関である。同委員会は、事業者の監督、個人データの円滑な国際的流通の確保、個人情報の保護と適正かつ効果的な活用について広報・啓発等の活動をしている。

（2）法令の規制対象の拡大

規制の対象となる事業者について、旧法第 4 章で、取扱う個人情報の数が 5,000 件以下である事業者を規制の対象外と規定していた。しかし、改正法では当該規定が廃止され、個人情報を取扱うほとんどの事業者[6]は改正法に準拠する必要がある。

営利目的の企業や団体だけでなく、NPO 法人、自治会・町内会及び同窓会のような非営利の活動をしている団体も、個人情報取扱事業者として規制を受ける可能性があるため、注意する必要がある。

（3）個人情報の定義の明確化

旧法第 2 条に明記されている個人情報の定義「生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日、その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができるものを含む。）をいう。」については、改正法でも第 2 条で定義されている。改正法では、さらに、「特定の個人を識別することができるもの」（個人識別符号）として、以下のような情報も個人情報として定義された（表 3）。

表 3　個人識別符号の定義と例[7]

定義 1：特定の個人の身体の一部の特徴を電子計算機のために変換した符号 例：指紋認証データ、顔認識データ等
定義 2：対象者ごとに異なり、役務の利用や書類において対象者ごとに割り振られる符号 例：旅券番号、免許証番号等

また、これら個人情報のうち、特に配慮が求められるものとして、「要配慮個人情報」が定義された。これにより、以下のような差別や偏見を生じさせる情報については取得する際に本人の同意が必要となり、オプトアウト（後述）による第三者提供ができない等、旧法にはなかった取扱い義務が発生している（表 4）。

表 4　要配慮個人情報に該当する具体的な事項[8]

①人種 ②信条 ③社会的身分 ④病歴 ⑤犯罪の経歴 ⑥犯罪により害を被った事実 ⑦身体障害、知的障害、精神障害（発達障害を含む。）その他の個人情報保護委員会規則で定める心身の機能の障害があること。 ⑧本人に対して医師その他医療に関連する職務に従事する者（「医師等」）により行われた疾病の予防及び早期発見のための健康診断その他の検査（「健康診断等」）の結果 ⑨健康診断等の結果に基づき、又は疾病、負傷その他の心身の変化を理由として、本人に対して医師等により心身の状態の改善のための指導又は診療若しくは調剤が行われたこと。 ⑩本人を被疑者又は被告人として、逮捕、捜索、差押え、勾留、公訴の提起その他の刑事事件に関する

[6] 個人情報保護法第 76 条に示されている適用除外に該当する場合はその限りではない。

[7] 個人情報の保護に関する法律についてのガイドライン（通則編），個人情報保護委員会，平成 28 年 11 月（平成 29 年 3 月一部改正），P6-11，https://www.ppc.go.jp/files/pdf/guidelines01.pdf，（アクセス日：2017 年 8 月 4 日）をもとに当社作成

[8] 個人情報の保護に関する法律についてのガイドライン（通則編），個人情報保護委員会，平成 28 年 11 月（平成 29 年 3 月一部改正），P12-16，https://www.ppc.go.jp/files/pdf/guidelines01.pdf，（アクセス日：2017 年 8 月 4 日）をもとに当社作成

手続が行われたこと。
⑪本人を少年法に規定する少年又はその疑いのある者として、調査、観護の措置、審判、保護処分その他の少年の保護事件に関する手続が行われたこと。

（4）個人情報の有用性の確保

改正法では、膨大なパーソナルデータを収集・分析し新たなビジネスを生み出す、いわゆるビッグデータの利活用に合わせ、個人情報とは別に「匿名加工情報」が新たに定義された。

「匿名加工情報」とは、特定の個人を識別することができないように個人情報を加工し、当該個人情報を復元できないようにした情報である。匿名加工情報は、本人からあらかじめ同意を得ずに第三者提供できるなど個人情報の取扱いよりも緩和された規律にすることで、有用性に配慮された情報と言える。

しかし、「匿名加工情報」を作成する際は、個人情報保護委員会が定める方法で個人情報を加工する必要がある。具体的には、経済産業省から発行されている「事業者が匿名加工情報の具体的な作成方法を検討するにあたっての参考資料（匿名加工情報作成マニュアル）」[9]に基づいて加工しなければ、「匿名加工情報」と認められない可能性がある。認められない場合、個人情報の取扱いよりも緩和された規律は適用されない。

（5）適正な個人情報の流通を確保

個人データの第三者提供については、頻発する情報漏えいや、いわゆる名簿屋対策を目的として、旧法より取扱いが厳格になり、以下のような義務が新たに課されている（表 5）。

なお、個人データの第三者提供は、委託、事業継承、共同利用など第三者提供の例外となる事項も多いため、自組織の業務を精査し、実際に個人データの第三者提供にあたる事例があるか、調査することをお勧めしたい。

表 5　旧法より厳格になった個人情報の第三者提供に係る義務[10]

①オプトアウト手続による第三者提供
②第三者提供時の提供者及び受領者の記録作成

・オプトアウト手続による第三者提供

個人データを第三者へ提供する前に本人からの同意を得ることが原則である。しかし、事業上あらかじめ本人の同意を得ることが困難な場合、本人の求めに応じて提供行為を停止する等の義務が課されることを条件に、本人同意を得ずに第三者提供できる。これをオプトアウトと言う。

旧法でも本規定はあった。しかし、改正法ではより厳格に本規定を運用するため、オプトアウトを希望する事業者は、オプトアウトで課された義務に対応できる体制を整えたうえで個人情報保護委員会に届出をする必要がある。

また、届出内容が認められた場合、個人情報保護委員会の HP に事業者名が公表されることになっている。

・第三者提供時の提供者及び受領者の記録作成

第三者提供の方法を問わず、個人データを第三者提供する事業者及び当該個人データを受領する事

[9] 経済産業省 HP, http://www.meti.go.jp/policy/it_policy/privacy/downloadfiles/tokumeikakou.pdf, （アクセス日：2017 年 8 月 4 日）
[10] 個人情報の保護に関する法律についてのガイドライン（通則編）, 個人情報保護委員会, 平成 28 年 11 月（平成 29 年 3 月一部改正）, P46　P56-58, https://www.ppc.go.jp/files/pdf/guidelines01.pdf, （アクセス日：2017 年 8 月 4 日）をもとに当社作成

業者は、追認性（トレーサビリティ）を確保するため、記録を作成する必要がある。

また、記録する事項についても決められているため、改正法に基づいて記録を作成し、定められた期間、保管する義務が課されている。

事業者や個人がこれらの義務に違反して個人データを提供した場合、新設された罰則「個人情報データベース等不正提供罪」が適用される恐れがある。

この罰則では、不正な利益を図る目的で個人情報データベース等を提供・盗用した場合、1 年以下の懲役又は 50 万円以下の罰金に科されることがある。

（6）個人情報の取扱いのグローバル化

個人情報の取扱いは日本国内の事業者だけにとどまらない。グローバル化の進行に伴い、国外の事業者に業務を委託するなど、個人情報の取扱いは、世界中に広がっている。そのため、改正法では個人情報の取扱いのグローバル化に合わせて様々な義務が事業者に課されている。特に「外国の第三者への個人データの提供制限」については、事業者は注意する必要がある。

まず、改正法で示されている「外国の第三者」とは、個人データを提供する個人情報取扱事業者とは別組織であり、かつ日本国外に事務所を設置している組織を指す。

そのため、グループ企業において国内にある個人情報取扱事業者の親会社が国外にある場合、その親会社は「外国の第三者」に該当する。

次に「提供」とは、「1.2.」の（5）で示した国内における個人データの第三者提供とは異なり、委託、事業継承、共同利用についても例外事項には該当せず、「提供」として扱われる。

個人情報取扱事業者には、再委託先についても同様の義務が課される。したがって、自組織で国内の事業者に委託し当該委託先が外国の事業者に再委託した場合には、その再委託先に対しては外国の第三者への個人データの提供とみなされるため、事業者は必要な措置を講じなければならない。

このことから、自組織の委託先に外国の事業者が含まれていないとしても、再委託先に当該事業者が存在する可能性があるため、委託先に確認することをお勧めしたい。

なお、改正法では、原則として本人の同意を得なければ外国にある第三者に個人データを提供できない（委託、事業継承、共同利用を含む）。しかし、以下に該当する場合には、例外として本人の同意を得ずに当該第三者への提供が可能とされている（表 6）。

表 6　外国への第三者提供の例外事項[11]

①外国の第三者が日本の個人情報保護制度と同等の水準であると認められる国にある場合 ②外国の第三者が個人情報保護法に相当する措置を継続的に行うために必要な体制を整備している場合

上記①に該当する国については現在指定されていないが、今後、新たに公表される可能性がある。②の具体的な取組みとしては、個人情報保護法に定められた義務に基づく当該事業者との契約や覚書の締結、グループ企業間であればグループ共通の規程などの整備が挙げられる。委託先や再委託先が外国にある場合は、当該組織の体制や締結している契約内容について確認することをお勧めしたい。

[11] 個人情報の保護に関する法律についてのガイドライン（通則編），個人情報保護委員会，平成 28 年 11 月（平成 29 年 3 月一部改正），P55，https://www.ppc.go.jp/files/pdf/guidelines01.pdf，（アクセス日：2017 年 8 月 4 日）をもとに当社作成

2. 緊急時対応

2.1. 緊急時対応の必要性

個人情報漏えい等[12]の対応については、個人情報保護委員会への速やかな報告が努力義務として、二次被害の防止など漏えい等の事故対応は望ましい対応として、それぞれ改正法に示されている。しかし、個人情報に対する昨今の傾向として、漏えい等に適切に対応しなかった場合、事業者には社会から厳しい説明責任が求められる。

そのため、事業者にとって、漏えい等による被害者保護のみならず、風評被害を含めた事業継続の観点からも、有事においても適切に対応できる体制をあらかじめ整備することが重要となる。

個人情報保護委員会が発行した『個人データの漏えい等の事案が発生した場合等の対応について』(以下「緊急時対応ガイドライン」) では、事業者が個人情報の漏えい等の際にすることが望ましい措置として以下の事項が示されている（表 7)。

表 7　漏えい等事案が発覚した場合に講ずべき措置[13]

①事業者内部における報告及び被害の拡大防止
②事実関係の調査及び原因の究明
③影響範囲の特定
④再発防止策の検討及び実施
⑤影響を受ける可能性のある本人への連絡等
⑥事実関係及び再発防止策等の公表

2.2. 緊急時対応の具体的な取組み

(1) 事業者内部における報告及び被害の拡大防止

緊急時対応ガイドラインでは、「責任ある立場の者に直ちに報告するとともに、漏えい等事案による被害が発覚時よりも拡大しないよう必要な措置を講ずる。」とある。実際に本活動をするために、事業者は、次の事項をあらかじめ定めておく必要がある。

・役割責任

事故発生時の対応責任者や実務担当などを決定しておく必要がある。特に責任者については、組織全体の状況を把握し、その後の事故対応に向けた指揮命令をすることを考慮して役職者を選定することが必要である。

・事故の定義と報告基準

現場の従業員が事故の状況を理解していなければ事故の報告がされない恐れがある。そのため、事故を明確に定義することが望ましい。

また、事故は、実際に事故が発生したか否か不明確な状況（事故の予兆）から始まるケースも多い。そのため、顧客からの苦情や情報システムの異常など、普段と異なる兆候が見られた場合には、従業

[12] 「漏えい等」とは、個人情報の漏えい、目的外利用など改正法に違反する活動を指す。
[13] 個人データの漏えい等の事案が発生した場合等の対応について,個人情報保護委員会,P2,
https://www.ppc.go.jp/files/pdf/iinkaikokuzi01.pdf, (アクセス日：2017 年 8 月 4 日）をもとに当社作成

員がすぐに担当部門等へ相談・報告をしやすい基準を設けておくことも重要である。

・被害の拡大防止策

被害拡大防止に向けて応急処置をすることは重要である。しかし、従業員が事故の状況に合わせた応急処置の方法をあらかじめ理解していなければ、有事の際に適切な応急処置ができない恐れがある。

そのため、応急処置の方法を普段から従業員に周知する等、平時から適切に情報提供することが重要である。

(2) 事実関係の調査及び原因の究明

発生した漏えい等の内容により調査手法は異なると考えられる。例えば、サイバー攻撃など技術的な問題による漏えい事故では、被害の範囲や侵入経路などを容易に把握できない場合もあり、事業者は、専門調査会社などに調査を依頼する必要がある。

また、調査にあたっては、被害を受けた情報システムを停止させることも想定されることから、事業上重要なシステムが停止することによる事業への影響をあらかじめ分析しておくことが望ましい。

(3) 影響範囲の特定

漏えい事故については、調査により、漏えいした件数、要配慮個人情報など機密性の高い情報の有無、自社の事業停止の可能性等、被害者本人への影響や事業への影響の範囲を特定することができる。

調査結果によって、今後取るべき対応方針は大きく変わることもあるため、正確な情報に基づいて影響範囲を特定することが事業者には求められる。

(4) 再発防止策の検討及び実施

判明した原因に基づいて、二度と同様の事故を発生させないための対策を検討・実施することが事業者には求められている。しかし、再発防止策の検討・実施に時間がかかるようであれば、被害者保護の観点からも、優先的に漏えい等の事実の通知・公表や苦情相談の受付などをすることが望まれる。

(5) 影響を受ける可能性のある被害者本人への連絡等

事業者が漏えい等の事実をその影響を受ける可能性のある被害者本人に連絡する手段として、各被害者へ個別に連絡する方法と HP 等で公表する方法の 2 通りが考えられる。

被害者をすべて特定できており速やかに連絡することができるような人数の場合には、個別に連絡する方法で対応可能である。しかし、漏えい等の範囲を限定できない、被害者の人数が膨大である、被害者の連絡先を把握できていないといった場合には、HP 等で公表する方法を採用することが考えられる。

ただし、サイバー攻撃等による漏えいの場合は、公表することによってかえって被害の拡大につながる恐れがあると考えられる。そのため、公的機関等に相談し、適切な対応を検討することが求められる。

また、事故の事実を通知・公表した場合、被害者だけでなく様々なステークホルダーから連絡が入ることが考えられる。そのため、通知・公表は以下の事項を検討したうえで、することをお勧めしたい（表 8)。

表 8　通知・公表前に検討すべき事項の例[14]

①警察への連絡

サイバー攻撃をはじめ悪意による事故発生の場合に被害届を実施するなどの対応を検討する。

②弁護士との連係

謝罪文書など外部へ公開する文書のチェックや賠償等を求められた場合の相談先として検討する。

③コールセンターの利用

被害者数が大規模で社内で電話を受けきれない恐れがある場合、外部への委託を検討する。

④個人情報保護委員会への連絡

原則、監督機関である個人情報保護委員会等へ事故報告する。ただし、改正法第 47 条第 1 項に規定する認定個人情報保護団体の対象事業者である個人情報取扱事業者は、当該認定個人情報保護団体に報告する。

上記にかかわらず、改正法第 40 条第 1 項に規定する個人情報保護委員会の権限（報告徴収及び立入検査）が事業所管大臣に委任されている分野における個人情報取扱事業者については別に定める一覧表[15]に基づき報告する。

⑤従業員への連絡

事前に従業員へ事故の事実や対応方針などを示し、被害者からの連絡や相談が入った場合の対応等について周知する。

⑥その他関係機関への連絡

重要な取引先、グループ企業等、組織の状況に応じて通知・公表前に報告する必要がある関係先を検討する。

（6）事実関係及び再発防止策等の公表

通知・公表する内容に事実関係や再発防止策も含めて被害者本人に連絡することは、漏えい事故により失墜する信頼を回復するためにも、事業者にとって重要である。

また、再発防止策等については、個人情報保護委員会等へも報告する必要があるため、被害者本人だけでなく、必要に応じてその他関係機関へも連絡することが望ましい。

3. 一般データ保護規則

3.1. 一般データ保護規則の全体像

2018 年 5 月 25 日に EU で施行が予定されている一般データ保護規則は、全 11 章 99 カ条で構成されており（表 9）、個人データの取扱いに係る本人の保護に関する規定及び個人データの自由な流通を目的としている。

一般データ保護規則は、EU 域内の事業者だけでなく、EU 域外の事業者についても適用されることがある。また、EU 在住の個人に対して商品・サービスを提供している場合、EU 域内での個人の行動を監視している場合にも適用される。

[14] 当社作成

[15] 改正個人情報保護法に基づく権限の委任を行う業種等及び府省庁並びに当該業種等における漏えい等事案発生時の報告先, 個人情報保護委員会, https://www.ppc.go.jp/files/pdf/170530_kengeninin_list_detail.pdf, （アクセス日：2017 年 8 月 4 日）

表 9　一般データ保護規則の全体構成[16]

第 1 章 総則：1 条～4 条
第 2 章 諸原則 5 条～11 条
第 3 章 データ主体の権利：12 条～23 条
第 1 節 透明性及び手続 12 条，第 2 節 情報及び個人データへのアクセス 13 条～15 条，第 3 節 訂正及び消去 16 条～20 条，第 4 節 異議を唱える権利及び個人に対する自動化された意思決定 21 条～22 条，第 5 節 制限 23 条
第 4 章 管理者及び取扱者：24 条～43 条
第 1 節 一般的義務 24 条～31 条，第 2 節 個人データの保護 32 条～34 条，第 3 節 データ保護影響評価及び事前協議 35 条～36 条，第 4 節 データ保護オフィサー37 条～39 条，第 5 節 行動規範及び認証 40～43 条
第 5 章 第三国又は国際機関への個人データ移転：44 条～51 条
第 6 章 独立監督機関：51 条～59 条
第 1 節 独立的地位 51 条～54 条，第 2 節 管轄、業務及び権限 55 条～59 条
第 7 章 協力及び一貫性：60 条～76 条
第 1 節 協力 60 条～62 条，第 2 節 一貫性 63 条～67 条，第 3 節 欧州データ保護会議 68 条～76 条
第 8 章 救済、法的責任及び制裁：77 条～84 条
第 9 章 特別な取扱い状況に関する条項：85 条～91 条
第 10 章 委任行為及び実施行為：92 条～93 条
第 11 章 最終条項：94 条～99 条

3.2. 一般データ保護規則の特徴

一般データ保護規則における事業者の義務の中には、日本の改正法にはない様々な義務が明文化されている。一般データ保護規則の対象事業者は改正法の対応だけでなく、同規則で定められている義務についても遵守できる体制を整備することが必要である。

日本の改正法にはない一般データ保護規則の義務等は、以下の通りである。

（1）消去の権利（忘れられる権利）（第 17 条）

本人が自身に関する個人データについて、本規則に定める基準を満たせば、管理者に遅滞なく消去させる権利である。

なお、改正法では、利用停止等を求める権利（改正法第 30 条）が明記されており、改正法に定める基準に基づき事業者は当該情報の利用を停止しなければならない。しかし、本規定は必ずしも消去を義務づけたものではない。

（2）データポータビリティの権利（第 20 条）

本人が事業者に提供した本人に関する個人データの移動に係る権利について定められている。具体的には、当該個人データが構造化され、一般的に利用される、機械可読性（コンピューターでの文書の読み取りやす

[16] 個人データの取扱いに係る自然人の保護及び当該データの自由な移転に関する欧州議会及び欧州理事会規則（一般データ保護規則）（仮日本語訳），一般財団法人日本情報経済社会推進協会，2016 年 8 月,P2, https://www.jipdec.or.jp/archives/publications/J0005075,（アクセス日：2017 年 8 月 4 日）をもとに当社作成

さ）のある形式で受け取る権利や当該個人データが提供された管理者の妨害なしに他の管理者に移行する権利を定めている。

例えば、プロバイダ A 社で利用していたメールサービスにおいて、当該メールデータを A 社から標準フォーマットで受け取ることや、プロバイダ B 社に乗り換えるために直接データを B 社へ移動するように A 社へ依頼するといったことを示している。

（3）プロファイリングを含む自動化された個人意思決定（第 22 条）

データ主体となる個人は、本人に関する法的効果をもたらすか、または本人に同様の重大な影響をもたらすプロファイリングなどの自動化された取扱いのみに基づいた決定に服しない権利を持つと定めている。

IT やネットワークの発達により、インターネットの閲覧データから当該本人の趣味・嗜好を分析することや、GPS データから当該本人の行動パターンなどを分析するなどといった処理が自動でされるようになった。そのため、本人が知覚しないうちに様々なパーソナル情報が作り出されることもあるが、本規定では当該情報のみで様々な重要な決定がされることに服しない権利について定められている。

（4）第三国又は国際機関への個人データ移転（第 5 章：第 44 条～第 50 条）

EU 域内に所在する者の個人データを域外に移転することは原則禁止とすることが定められている。以下に示すような事項のいずれかを満たせば移転が可能となる（表 10）。

表 10　EU 域外へのデータ移転に係る例外事項の例[17]

①個人情報保護に関して十分なレベルを保証していると欧州委員会が決定した場合
②事業者が本規則に定める拘束的企業準則を定めて監督機関が承認している場合
③欧州委員会が認める標準データ保護約款に基づいている場合
④事業者が本規則に定める行動規範を定めて監督機関が承認している場合
⑤事業者が本規則に定める認証を取得している場合
⑥データ移転に係るリスクを示した後、本人から明示的な同意を得ている場合
⑦その他特例における例外事項

本稿の「はじめに」で示した「個人データの越境移転に関する政治宣言」の通り、表 10 の①で、日本が個人情報保護に関して十分なレベルを保証していると欧州委員会が決定し、日本へのデータ移転が認められれば、事業者は、②以降の事業者個別の承認等を取得することなく、データを移転することが可能となる。

もし、このデータ移転が認められない場合、各事業者において欧州の監督機関等から個別に承認されなければデータを移転することはできないため、承認までに多くの時間が費やされることが考えられる。

（5）救済、法的責任及び制裁（第 8 章：第 77 条～第 84 条）

例外措置に該当しない方法でデータの移転や漏えい事故を知覚してから 72 時間以内に監督機関に事実報告しなかった場合等、一般データ保護規則に違反した際は、厳しい制裁措置が用意されている。

制裁措置は、同規則の義務違反となる類型によって異なる。EU から当該事業者へ最大 2000 万ユーロ、または前会計年度の全世界年間売上高の 4%までのどちらか高い方を制裁金として科される恐れがある。

[17] 個人データの取扱いに係る自然人の保護及び当該データの自由な移転に関する欧州議会及び欧州理事会規則（一般データ保護規則）（仮日本語訳），一般財団法人日本情報経済社会推進協会，2016 年 8 月,P61-P70, https://www.jipdec.or.jp/archives/publications/J0005075,（アクセス日：2017 年 8 月 4 日）をもとに当社作成

おわりに

改正法への対応は、個人情報取扱事業者にとって必須である。その際は、規定された義務のみをリスクの対象とせず、事業内容・規模・特性から、リスクに応じて創意工夫のある対策を実現することが事業者には求められる。

昨今のサイバー攻撃による事件等において、行政への事故報告や事実の公表など法令で求める対策を表面的に講じたとしても、その他の対応手法や企業姿勢に問題があると社会から厳しい批判を浴びせられ、事業活動に影響を与える事例等も発生している。

また、グローバル化した社会においては、前述した一般データ保護規則をはじめ日本国外の法令が自社の事業に与える影響についても考慮する必要がある。

個人情報保護については、IT やネットワークの急速な発展やグローバル化など社会状況によってリスクが変化することを認識し、自社の業務においてどこまで対策をするべきか、改めて検討することが重要である。

参考文献

第 24 回日 EU 定期首脳協議, 個人データの越境移転に関する政治宣言（仮訳）, 外務省 HP
個人情報の保護に関する法律についてのガイドライン（通則編）, 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（外国にある第三者提供編）, 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（確認記録義務編）, 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（匿名加工情報編）, 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」及び「個人データの漏えい等の事案が発生した場合等の対応について」に関するＱ＆Ａ, 個人情報保護委員会
個人データの漏えい等の事案が発生した場合等の対応について, 個人情報保護委員会
個人データの取扱いに係る自然人の保護及び当該データの自由な移転に関する欧州議会及び欧州理事会規則（一般データ保護規則）（仮日本語訳）, 一般財団法人日本情報経済社会推進協会

執筆者紹介

西出 三輝　Mitsuteru Nishide

リスクマネジメント事業本部 ERM 事業部
上席コンサルタント
専門は情報セキュリティ

ＳＯＭＰＯリスケアマネジメントについて

ＳＯＭＰＯリスケアマネジメント株式会社は、ＳＯＭＰＯホールディングスグループのグループ会社です。
「リスクマネジメント事業」「健康指導・相談事業」「メンタルヘルスケア事業」を展開し、全社的リスクマネジメント（ERM）、事業継続（BCM・BCP）、健康経営推進支援、特定保健指導・健康相談、メンタルヘルス対策などのソリューション・サービスを提供しています。

本レポートに関するお問い合わせ先

ＳＯＭＰＯリスケアマネジメント株式会社
経営企画部　広報担当
〒160-0023 東京都新宿区西新宿 1-24-1 エステック情報ビル
TEL：03-3349-5468（直通）

