特 集

個人情報保護の最新動向 ～GDPRを中心に～

数藤 雅彦（64期）
●Masahiko Sudo
当会会員
情報公開･個人情報保護委員会 副委員長

〈略歴〉
2012年　弁護士登録（当会）
2013年　情報公開･個人情報保護委員会委員
2016年　同 副委員長

川野 智弘（65期）
●Tomohiro Kawano
当会会員
情報公開･個人情報保護委員会 委員

〈略歴〉
2012年　弁護士登録（当会）
2014年　情報公開･個人情報保護委員会委員

1 はじめに

近時、個人情報の保護をめぐる法整備が、国内外で大きく動いている。日本では改正個人情報保護法が2017年5月に施行され、EUではGDPR（General Data Protection Regulation：一般データ保護規則）が2018年5月に施行された。また、Facebookのケンブリッジ・アナリティカ事件や、国内大手通信教育事業者における大規模個人情報漏えい事件の第一審判決、さらに情報銀行をめぐる事業者の関心の高まりなど、個人情報に関する話題は後を絶たない。本稿では、GDPRの解説と、GDPRが国内の事業者に与える影響を中心に、個人情報をめぐる最新の動向を広く概説したい。

なお本稿の記載内容は、2018年9月時点のものであり、GDPR関連の訳語は、個人情報保護委員会により公表されている日本語仮訳*1を参照した。

2 GDPRの意義と制定経緯 数藤

GDPRは、EU域内*2の個人データ保護について定めた規則である。

もとよりEUにおいては、個人データの保護が、EU基本権憲章において明文で保障されており（EU基本権憲章8条1項）、基本権の人権問題として位置づけられていた。GDPR制定以前のEUでは、1995年制定の「EUデータ保護指令（Data Protection Directive 95）」に基づき、各国で国内法化がなされていた。

しかし、EUにおける「指令（Directive）」は、達成すべき結果については加盟国を拘束するものの、そのための形式及び手段の選択は加盟国に委ねている。その結果として、各加盟国で、適用される法制度に差異が生じていた。

＊1　前文仮訳（https://www.ppc.go.jp/files/pdf/gdpr-preface-ja.pdf）、本文仮訳（https://www.ppc.go.jp/files/pdf/gdpr-provisions-ja.pdf）
なお本稿記載のURLの最終確認日は2018年9月30日である。
＊2　正確には、GDPRの対象はEEA（欧州経済領域。EU加盟国に加え、欧州自由貿易連合のノルウェー、アイスランド、リヒテンシュタインを含めた共同市場）であるが、本稿ではこれを「EU域内」の語で表記する。

これに対して、「規則（Regulation）」は、国内立法がなくとも加盟国に対して直接適用される。そこで、個人データの保護に関する規則を「指令」から「規則」に引き上げることにより、EU域内でのより統一的な規制の枠組みを定め、自由なデータ流通を促進することが目指された。

また、近時のグローバル化により、国境を越えたデータのやり取りが日常的になり、かつアメリカを中心とする大手ITサービス事業者によるEU域内の個人データの収集が進んだことから、EU域内の個人データ保護の強化が求められていた。

更に、EUの重点政策であるデジタル単一市場（Digital Single Market）の構築に向けて、域内における競争の平等を保障し、事業者の法的安定性を改善することも必要と考えられていた。

これらの背景を踏まえて、欧州委員会が2012年にGDPR案を公表。議論を経て2016年4月にGDPRが制定され、2018年5月に施行された。GDPRの概要は、次章のとおりである。

3 GDPRの概要 川野

1 構成等

GDPRは、173項目からなる前文と、第1章から第11章までの全99条からなる条文とで構成されており、これに加えて、2018年9月時点までに、EUデータ保護指令の第29条作業部会（Article 29 Data Protection Working Party）、又は欧州データ保護会議（European Data Protection Board）において、**図表1**のとおり、11のガイドラインが策定・公表されている*3。また、欧州データ保護会議においては、今後も必要に応じてガイドラインが新たに策定・公表されることがあり、2018年9月には、日本においても影響の大きい、地理的範囲に関するガイドライン（Guidelines on territorial scope）の案が採択され、今後、意見公募に付される旨が発表されている。

なお、個人情報保護委員会は、GDPRの前文及び条文のほか、**図表1**のとおり、10のガイドラインに関しても日本語仮訳を公表しており、更に欧州委員会のウェブサイトにて掲載されている資料の一部に関しても、日本語仮

図表1 公表されているGDPR関連のガイドライン

ガイドライン名	個人情報保護委員会による仮訳名
Guidelines on the right to data portability	データポータビリティの権利に関するガイドライン
Guidelines on Data Protection Officers（'DPOs'）	データ保護オフィサー（DPO）に関するガイドライン
Guidelines for identifying a controller or processor's lead supervisory authority	管理者又は処理者の主監督機関を特定するためのガイドライン
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	データ保護影響評価（DPIA）及び取扱いが2016/679規則の適用上、「高いリスクをもたらすことが予想される」か否かの判断に関するガイドライン
Guidelines on the application and setting of administrative fines for the purpose of the Regulation 2016/679	規則における制裁金の適用及び設定に関するガイドライン
Guidelines on Personal data breach notification under Regulation 2016/679	規則に基づく個人データ侵害通知に関するガイドライン
Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679	自動化された個人に対する意思決定とプロファイリングに関するガイドライン
Guidelines on consent under Regulation 2016/679	同意に関するガイドライン
Guidelines on transparency under Regulation 2016/679	透明性に関するガイドライン
Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679	規則第49条の例外に関するガイドライン
Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679*4	本稿執筆時点では仮訳は公表されていない。

*3 第29条作業部会において公表されている9つのガイドライン（http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360）、欧州データ保護会議において公表されている2つのガイドライン（https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en）

*4 個人データの域外移転の方法の1つである、データ保護措置の第三者機関による「認証」とその基準の決定に関するガイドラインである。

訳を公表している*5。

以下では、GDPRの前文及び条文のうち主要な項目について解説する。

2 適用対象

(1) 個人データ（personal data）

GDPRの保護対象となる「個人データ（personal data）」には、識別された自然人又は識別可能な自然人（データ主体（data subject））に関するあらゆる情報が含まれる（GDPR4条(1)）。識別可能な自然人とは、氏名や識別番号、位置データ、オンライン識別子（これにはIPアドレスやクッキー（cookie）*6、RFIDタグなどが含まれる）のような識別子により、又は、当該自然人固有の要素（身体的、生理的、遺伝的、精神的、経済的、文化的、社会的な同一性を示す要素等）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。日本の個人情報保護法*7（以下、「日本法」という。）と異なり、オンライン識別子が明確に含まれている点には留意が必要である*8。

なお、死亡した者の個人データは適用外である点（前文（27））は日本法と同様である。

また、日本法における匿名加工情報と類似の概念として、匿名化された個人データ（personal data rendered anonymous）と、個人データの仮名化（pseudonymisation）の2つがあり、このうち前者（匿名化）は不可逆的な識別防止処理がなされたものを意味し*9、GDPRは適用されない（前文(26)）。他方、後者（仮名化）については、追加的情報を分離保管し、かつ、技術上及び組織上の措置を講じて、当該追加的情報の利用なしにはデータ主体を特定できないようにする態様で行われる個人データの取扱いを意味するものとされるが（GDPR4条(5)）、追加的情報を用いれば自然人を識別可能であるため、個人データに含まれ、GDPRの適用対象となる。

その他、日本法における要配慮個人情報と類似の概念として、特別な種類の個人データ（同9条）と、有罪判決及び犯罪行為又は保護措置と関連する個人データ（同10条）の2つがあり、それぞれ通常の個人データとは異なる規律が課せられている。なお、特別な種類の個人データとは、人種的・民族的な出自、政治的な意見、宗教上・思想上の信条、労働組合への加入に関する個人データ、遺伝子データ、自然人を一意に識別することを目的とする生体データ、健康に関するデータ、性生活・性的指向に関するデータと定義されており、特に労働組合への加入に関するデータ、性生活・性的指向に関するデータなどの点で、日本法における要配慮個人情報との間に差異があるように思われる。

(2) 適用主体

GDPRの適用主体は、個人データの処理の目的及び手段を決定する「管理者（controller）」、あるいは管理者の代わりに個人データを取扱う「処理者（processor）」であり、法人格や営利性の有無は問われない（同4条(7)及び(8)）。

なお、行政機関については別の規則が適用され、宗教団体等についても別の規則が適用されうることとされ、更に一定の適用除外（自然人によって純粋に私的な行為又は家庭内の行為の過程において行われる場合など）（同2条2項）も設けられている。

(3) 適用対象行為

GDPRでは、規制の対象となる行為類型について、個人データの「取扱い（processing）」のみを挙げ、「自動的な手段によるか否かを問わず、収集、記録、編集、構成、記録保存、修正若しくは変更、検索、参照、使用、送信による開示、配布、又は、それら以外に利用可能なものとすること、整列若しくは結合、制限、消去若しくは破壊のような、個人データ若しくは一群の個人データに実施される業

＊5　https://www.ppc.go.jp/enforcement/cooperation/cooperation/GDPR/
＊6　ウェブサイトへのログイン状態やユーザー設定等を記録するためのファイルであり、ウェブサイト側にユーザーの個人設定を記憶させたり、ウェブサイトにアクセスする際のサインインを省略させたり、ユーザーが何回当該ウェブサイトにアクセスしたかを示すことなどが可能となる。
＊7　個人情報の保護に関する法律
＊8　そのため、EU域内を中心とする海外ウェブサイトでは、アクセスの際、はじめにクッキー等の取扱いについて同意を求められることが一般的である。
＊9　日本法の匿名加工情報の場合にも、非復元性の要件が存在するものの、これは全ての可能性を排除することまでを求めるものではなく、その意味で不可逆的な処理は不要とされ、事業者側に照合禁止義務が課せられることを背景として「個人情報」から除外されるものと解釈されているに過ぎない。そのため、日本法における匿名加工情報に該当しうる処理を施したとしても、なおGDPRの適用を受ける可能性がある点に注意が必要である。

務遂行又は一群の業務遂行を意味する。」と定義する（同4条(2)）。個人データに関連する行為はおよそ全て含まれると考えられる。

ただし、「移転（transfer）」については「取扱い」から除外され、別の行為と解されており、「取扱い」と「移転」ではそれぞれ別の規制が設けられている。なお、「移転」についてGDPRの規定上では明確な定義は設けられていないが、EUデータ保護指令下では、個人データの物理的・電磁的な送付だけでなく、外部からEU域内のサーバ上にアクセスして個人データを閲覧する行為等も含まれるものと解されており、同解釈はGDPR制定後も変わらないものと考えられる。

（4）地理的適用範囲

GDPR適用の地理的範囲としては、個人データの取扱いがEU域内で行われるものであるか否かを問わず、管理者又は処理者（以下、「管理者等」という。）がEU域内に拠点を有する場合、当該拠点の活動の過程における個人データの取扱いに適用される（同3条1項）。

更に、管理者等がEU域内に拠点を有しない場合でも、①EU域内のデータ主体に対する物品又はサービスの提供に関連して個人データが取り扱われる場合や、②EU域内で行われるデータ主体の行動の監視に関連して個人データが取り扱われる場合には、その適用がある（同3条2項）。（詳細については4章の第2「EU域内に拠点を有しない事業者等の場合（域外適用の問題）」にて述べる。）

3 個人データの取扱いについて

（1）基本原則

GDPRでは、個人データの取扱いに関連する原則として、①適法性、公正性及び透明性の原則、②目的の制限の原則、③データの最小化の原則、④正確性の原則、⑤保存期間の制限の原則、⑥完全性及び機密性の原則が掲げられており（同5条1項）、管理者等はこれらの原則を遵守する義務を負い、かつ、その遵守を証明することができなければならない（同5条2項）。

（2）取扱いの適法性要件

個人データの取扱いは、データ主体が特定の目的のための取扱いに関し同意を与えた場合のほか、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必要となる場合や、管理者が服する法的義務を遵守するために必要となる場合（なお、ここでいう法的義務とは、EU法又はEU域内の国内法に依拠したものに限られる。）、生命に関する利益を保護するために必要となる場合、正当な利益の目的のために取扱いが必要となる場合など、一定の事由に該当する場合にのみ、許容される（同6条）。

なお、日本法の場合、同意に関する特段の要件は定められていないが、GDPRの場合、有効な同意とは、「自由に与えられ、特定され、事前に説明を受けた上での、不明瞭ではない、データ主体の意思の表示を意味し、それによって、データ主体が、その陳述又は明確な積極的行為により、自身に関連する個人データの取扱いの同意を表明するものを意味する。」と定義されており（同4条(11)）、同意取得の場面において、一定の要件を充足する必要がある。加えて、管理者等の側ではデータ主体による同意の撤回を認めなければならないなど、GDPRでは厳格なルールが設けられており、日本法における場合とは異なり、同意を得ることが万能な対応策とはならない面がある。

また、適法性要件の1つである、正当な利益の目的のために取扱いが必要となる場合に関しては、「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。」との但書きが明記されており、正当な利益目的があれば常に個人データの取扱いが適法となるわけではない。なお、GDPRにおいて「子ども」とは、原則として16歳未満とされているが、各加盟国において個別に13歳まで引き下げることも可能とされている（同8条1項）。

4 データ主体の権利

GDPRにおいては、日本法における開示請求権に相当する「アクセスの権利」（同15条）や、訂正請求権に相当する「訂正の権利」（同16条）、

消去請求権に相当する「消去の権利（忘れられる権利）」（同17条）、利用停止請求権に相当する「取扱いの制限を得る権利」（同18条）のほか*10、日本法では必ずしも認められていないものとして、「データポータビリティの権利」*11（同20条）や「異議を述べる権利」*12（同21条）、「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」（同22条）を有することが明示されている。

また、管理者は、データ主体に対し、簡潔で、透明性があり、理解しやすく、容易にアクセスできる方式により、明確かつ平易な文言を用いて、個人データの取扱いに関する各種の情報や、上記の各権利の行使の関係での連絡を提供するための適切な措置を講じなければならない、とされているため（同12条1項）、データ主体は各種の情報を入手することが可能となる。

なお、データ主体は、管理者等によるGDPR違反に対し、監督機関への異議申立て（同77条）をすることができるほか、監督機関の決定に不服があれば司法救済を得る権利を有しており（同78条）、また、管理者等に対し、管理者等が拠点をもつ加盟国の裁判所において司法救済を求めることもできる（同79条）。更に、損害を被った場合には、管理者等から賠償を受けることも可能、と明記されている（同82条）。

5 管理者の義務

管理者は、GDPR に従った個人データの取扱いが遂行されるように、各種の適切な技術上及び組織上の措置を実装することが義務付けられている（同24条、25条、32条）。

その他、管理者等がEU域内に拠点を有さない場合の、EU域内における代理人指定の義務（同27条）、個人データの取扱活動の記録保管義務（同30条）、監督機関への協力義務（同31条）、個人データ侵害時の監督機関への72時間以内の通知義務（同33条）、個人データ侵害時のデータ主体への連絡義務（同34条）、一定の場合におけるデータ保護影響評価及び事前協議実施の義務（同35条、36条）、一定の場合におけるデータ保護オフィサーの指名義務（同37条）などが規定されている。

なお、データ保護オフィサーとは、日本法にはない制度であるが、説明責任に基づく法令遵守というGDPRの法的枠組みにおける核心的な役割として位置付けられており、管理者等及びその従業員に対する助言やトレーニング、監視等を行うものとされ（同39条）、管理者等はデータ保護オフィサーに対し、独立性の確保など、一定の地位を与えなければならないものとされている（同38条）。

6 個人データの域外移転

個人データのEU域内から「第三国又は国際機関」（以下、「EU域外」という。）への移転、あるいは当該移転先であるEU域外から別のEU域外への転送については、一定の要件を充足する場合にのみ認められている（同44条）。

その要件とは、欧州委員会から十分性認定*13を受けているEU域外への移転か否か（同45条）、十分性認定を受けていないとしても、管理者等が適切な保護措置（企業グループ間での拘束的企業準則（BCR）や、標準データ保護条項（SDPC）など、従前のEUデータ保護指令下にて活用されてきた方法のほか、第三者機関により認証を受けるというGDPRにおいて新設された方法なども含まれる。）を提供しており、かつ、データ主体の執行可能な権利及びデータ主体のための効果的な司法救済が利用可能であること（同46条）、あるいは、明示的な同意、データ主体と管理者との間の契約の履行のためなどの特定の状況下での例外に該当すること（同49条）である。

＊10　なお、日本法においては、6か月以内に消去することとされている個人データについては保有個人データに該当せず、開示や訂正等の対象から除外されるが、GDPRにおいてそのような区別は設けられておらず、個人データに該当するもの全てが各種権利の対象となる。
＊11　一定の場合に、「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」、及び「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」と定義されている。
＊12　個人データの取扱い一般に対するもののほか、ダイレクトマーケティングの目的のために個人データが取り扱われる場合に、当該取扱いに対して異議を述べる権利が認められている。
＊13　十分性認定とは、欧州委員会において、EU域外の国等におけるデータ取扱いの保護水準について、法制度や法令の遵守状況など様々な要素を踏まえて評価し、「十分なデータ保護の水準を確保している」と欧州委員会が決定することをいう。

7 監督機関による是正権限の行使

管理者等がGDPRに違反した場合、あるいは違反のおそれがある場合には、監督機関は、当該管理者等に対し、警告、懲戒、データ主体の要求に従う旨の命令、GDPR遵守を求める命令、個人データ侵害に関するデータ主体への連絡命令、個人データの取扱い禁止等の制限、個人データの訂正・削除・取扱い制限等の命令、認証の取消等、制裁金を科すこと、EU域外の取得者へのデータ流通の停止命令などの措置を講ずることができる（同58条2項）。

このうち、制裁金については、非常に高額となる仕組みが導入されており、違反の内容に応じて、①1,000万ユーロ以下、又は事業者である場合は前会計年度の全世界年間売上高の2%以下のいずれか高い方、あるいは②2,000万ユーロ以下、又は事業者である場合は前会計年度の全世界年間売上高の4%以下のいずれか高い方、との制裁金が科されうることとなる（同83条4項及び5項）。ただし、実際に監督機関が制裁金を科すか否か、またその額に関する判断は、違反行為の性質や重大性、持続期間、違反行為による被害範囲、損害の程度、故意過失の別、データ主体が被った損失に対する軽減措置、管理者等の責任の程度、過去の違反状況、監督機関との協力の程度、影響を受けた個人データの種類、管理者等自らによる監督機関への通知の有無等、などの様々な事項を適正に考慮に入れることとされており（同83条2項）、違反により直ちに高額の制裁金が科されるということではないと考えられる。

8 加盟国による国内法整備

EUデータ保護指令と異なり、GDPRはEU域内の加盟国に直接適用されるが、EU域内の個人データの取扱いに関してGDPRにより完結するわけではない。一定の範囲の事項（取扱いの適法性要件の一部（同6条）、子供の同意に係る年齢制限（同8条）、特別な種類の個人データの取扱い（同9条）、消去の権利（忘れられる権利）（同17条）など）について、各国の国内法によって、より詳細な、あるいはより厳格なルールを設定することが認められており、規制内容が変わりうる点には留意が必要である。

4 GDPRの日本への影響とその対応 川野

1 既にEU域内に拠点を有している事業者等の場合

前述のとおり、EU域内に拠点を有する管理者等については、GDPRの適用を受けることとなるが、これらの事業者等に関しては、既に進出先の国内データ保護法の適用下にあったのであり、一定の対応を行っていたものと考えられる。そのような事業者等の場合、むしろ、GDPRの施行により、各国の規制の差異が一定程度解消されることとなり、EU域内全体のルールが原則として統一されるため、EU域内における個人データの取扱いに関する個別対応への負担感が軽減することが見込まれる。

なお、後述のとおり、日本に対しても十分性認定がなされる見込みであるが、あくまでこれは個人データの域外移転に関する話であり、EU域内の事業所等における個人データの取扱いに関しては、十分性認定の有無にかかわらず、GDPRへの適切な対応が求められることとなる。

2 EU域内に拠点を有しない事業者等の場合（域外適用の問題）

前述のとおり、EU域内に拠点を有しない日本国内の事業者等であっても、GDPRの地理的適用範囲がEU域外に及ぶため、一定の場合にはGDPRがそのまま適用されることとなる。

（1）EU域内のデータ主体に対する物品又はサービスの提供

「EU域内のデータ主体」とは、EU域内に所在する自然人の全てを指すものと解されており、EU域内の国籍を有する居住者のほか、日本から出向している従業員等や、出張・旅行などの短期滞在中の者も含まれることとなる。

「物品又はサービスの提供」の該当性判断の

ポイントとしては、EU域内のデータ主体に対して管理者等がサービスを提供しようとする意図が明白か否か、であるとされ、管理者等へのアクセスの可能性、使用言語、決済通貨、ウェブサイト等での記載内容などの要素により判断されうる（前文(23)）。英語表記のウェブサイトを用意しているなどの事情だけで、直ちにEU域内のデータ主体へのサービス提供の意図が明白であると評価されるおそれは低いと思われるものの、英語以外のEU域内の言語や通貨にも対応したウェブサイトにて商品等の販売を行っているような場合や、ウェブサイトにおいて、EU域内の特定の国に向けてサービス提供を行う旨の意図が明らかな記述を記載しているような場合には、EU域内のデータ主体への物品又はサービスの提供の意図が明白であると評価される可能性が高まるように思われる。なお、本稿執筆時点においては、ガイドライン等による具体的な解釈等については何ら示されていないが、欧州データ保護会議において地理的範囲に関するガイドラインの案が採択され、今後、意見公募に付される予定であり、その動向や内容を注視する必要がある。

（2）EU域内で行われるデータ主体の行動の監視

「データ主体の行動の監視」の該当性判断のポイントとしては、「自然人のプロファイリングを構成する個人データの取扱い技術が後に使用される可能性を含め、自然人がインターネット上で追跡されているかどうか、特に、データ主体に関連する判断をするため、又は、データ主体の個人的な嗜好、行動及び傾向を分析又は予測するために追跡されているか」である（前文(24)）。ここでも、「物品又はサービスの提供」と同様、ガイドライン等によるこれ以上の具体的な解釈等は示されておらず、現時点においてはその適用範囲は不明確であるが、クッキーやSNSなどを通じたあらゆる形態のインターネット上における追跡行為のほか、データ主体によるウェブサイト閲覧時の各種情報（IPアドレス、ブラウザの情報、OS、プラグインの有無や言語・タイムゾーンの設定など）と他の情報とを組み合わせることで閲覧者の「個人的な嗜好、行動及び傾向を分析又は予測する」ことが可能な場合には、「データ主体の行動の監視」に該当するものと解すべきであろう。

3 域外適用への対応策

（1）現状分析（データマッピング）

EU域内に事業所等を有していない事業者等は特に、これまで個人情報の取扱いに関しては国内法上の対応のみを実施してきたものと考えられる。上述のとおり、GDPRの域外適用の範囲はなお限定的なものであるため、国内向けにのみサービス提供を行っている場合など、およそGDPR適用の可能性のない事業者等については、対応策を検討する必要はない。

他方で、域外適用の可能性のある事業者等に関しては、まず、EU域内のデータ主体に関する個人データの取扱いの有無、部門ごとでの個人データの所在及び処理態様の特定、サービスの提供範囲、決済方法、ウェブサイトの内容、アクセス情報解析の内容など、現状の確認を網羅的に行い、GDPR適用の可能性の有無を検討する必要がある。

（2）対策の検討

GDPRが適用される可能性がある場合には、現状分析にて把握した個人データの取扱い状況を踏まえ、GDPRの具体的な規制内容との整合性の有無を個々に検討し、リスクの大きさを考慮した上で、社内規程等の整備、顧客等の外部向け対応の整備、他の事業者等との間の契約等における留意事項の確認などの措置を順次講じていくこととなる。

5 個人情報の保護をめぐる国内外の最新動向 数藤

1 総論

GDPR以外にも、近年では個人情報の保護をめぐって国内外で多くの動向が見られた。以下では、近年の主要な動向を、国内（第2「国内の動向～十分性認定を中心に」）と海外（第3「海外の主な動向」）に分けて概説する。

2 国内の動向～十分性認定を中心に

（1）個人情報保護法の平成27（2015）年改正

個人情報保護法は、2015年に改正され、2017年5月に全面施行された*14。主要な改正事項としては、個人情報保護委員会の新設、要配慮個人情報の創設、匿名加工情報の創設、外国にある第三者への個人データ提供に関する規制、第三者提供の際の確認・記録義務の新設、取扱い数5,000件以下の小規模取扱事業者への適用等が挙げられる。全面施行から1年余を経た現在、個人情報保護委員会により、事業者への指導・助言等が行われている*15。

個人情報保護法は、施行後3年ごとに「施行の状況について検討」が加えられることになっており（附則12条3項）、次は2020年に検討がなされる見込みである。

（2）十分性認定に関する国内動向

上記のとおり、個人情報保護法が改正されて個人情報の保護が強化されたものの、EUの法制度とはなお相違点が見られたことなどから、日本はEUからの十分性認定を得られていなかった。2018年5月のGDPR施行時においてもなお十分性認定はなされていなかったところ、近時の個人情報保護委員会と欧州委員会との対話を踏まえ、2018年中に、十分性認定がなされる見込みである。

すなわち個人情報保護委員会は、2018年7月に欧州委員会との間で、「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」に至った*16。両委員会は、2018年の秋までに当該個人データ移転の枠組みを運用可能とするため、双方において必要な国内手続を完了させる予定である*17。そして、EUでは同年9月、日本に対する十分性認定の手続を正式に開始することを閣議決定した*18。

一方日本では、個人情報保護委員会が同年8月に「個人情報の保護に関する法律に係る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に関する補完的ルール*19」（以下、「補完的ルール」という。）を公表した。補完的ルールにおいては、EU域内から十分性認定に基づいて移転した個人データについて**図表2**の各事項が規定されており、施行日は、十分性認定が日本で効力を生ずる日とされている*20。

なお個人情報保護委員会によると、補完的ルールは「法的拘束力を有する規律」であり、本ルールに基づく権利及び義務は「法の規定と同様に個人情報保護委員会の執行対象となる」、補完的ルールが定める権利及び義務に対する侵害があった場合には、「本人は裁判所からも救済を得ることができ」、個人情報取扱事業者が補完的ルールに定める義務を遵守しない場合には、「個人情報保護委員会は法第42条に基づく措置（筆者注：勧告、命令等の措置）を講ずる権限を有する」とされる*21。しか

図表2 EU域内から十分性認定に基づいて移転した個人データに適用される「補完的ルール」の概要

①性生活、性的指向又は労働組合に関する情報についても要配慮個人情報と同様に取り扱うこと
②6か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取り扱うこと
③個人データの提供を受けた第三者においても、提供元によって特定された利用目的の範囲内で利用目的を特定し、その範囲内で当該個人データを利用すること
④個人データを外国にある第三者に提供するにあたっては、一定の場合を除き、本人が同意に係る判断を行うために必要な移転先の状況についての情報を提供した上で、あらかじめ本人の同意を得ること
⑤匿名加工情報として取り扱う場合には、加工の方法に関する情報等を削除し、何人による再識別も不可能とすること

*14 なお、国の行政機関については「行政機関の保有する個人情報の保護に関する法律」が、独立行政法人については「独立行政法人等の保有する個人情報の保護に関する法律」がそれぞれ適用されるところ、いずれも個人情報保護法の改正を踏まえて2016年に改正され、2017年5月に施行された。改正の概要としては、いわゆる非識別加工情報制度を導入し、民間事業者が一定の条件の下で行政機関や独立行政法人等の有する非識別加工情報を利用できるようになった点などが挙げられる。
*15 平成29年度個人情報保護委員会年次報告35頁（https://www.ppc.go.jp/files/pdf/300612_annual_report_h29.pdf）によると、2017年5月30日から2018年3月31日までの期間における指導・助言は270件であり、勧告・命令については記載がないため0件と思われる。
*16 https://www.ppc.go.jp/news/press/2018/20180717/
*17 https://www.ppc.go.jp/files/pdf/300717_houdou.pdf
*18 https://www.ppc.go.jp/files/pdf/300906_houdou.pdf
*19 https://www.ppc.go.jp/files/pdf/Supplementary_Rules.pdf
*20 https://www.ppc.go.jp/personal/legal/
*21 補完的ルール1頁

し、補完的ルールにより執行が可能かという点については、法律の留保原則の観点からなお議論の余地もある。

(3) 個人情報の利活用に関する動向

個人情報保護法の平成27年改正においては、「個人情報の適正かつ効果的な活用」が目的の1つとされていた（同法1条参照）。個人情報の利活用をめぐる近時の注目すべき動向としては、以下で述べる医療分野の研究開発、カメラ画像の利用、情報銀行等が挙げられる。

ア　医療分野の研究開発

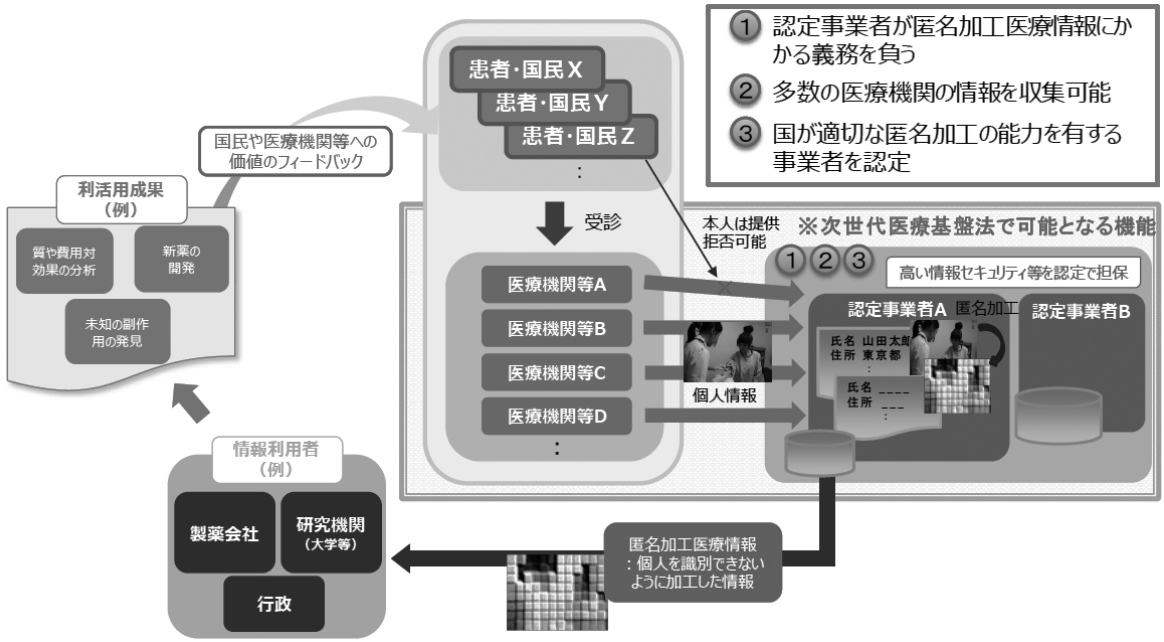
個人情報保護法では、病歴等の要配慮個人情報についてはオプトアウトによる第三者提供が認められていないものの（同法23条2項）、要配慮個人情報を加工して匿名加工情報を作成した場合には、本人の同意なく第三者への提供が可能となる。そして、医療分野においては、健康・医療に関する先端的研究開発等のために、匿名加工された医療情報を安心して円滑に利活用するための仕組みが求められていた。そのような背景を踏まえ、次世代医療基盤法*22が2017年に成立し、2018年5月に施行された（同法の全体像につき 図表3 参照）。

同法では、主務大臣が、申請に基づき、医療情報の管理や利活用のための匿名化を適正かつ確実に行う法人（認定匿名加工医療情報作成事業者。以下「認定事業者」という。）を認定することができる（同法8条1項）。そして、医療機関等があらかじめ本人に通知し、本人が提供を拒否しない場合には、認定事業者に対して医療情報を提供することができる（同法30条1項参照。本人への通知を前提にした、言わば丁寧なオプトアウト手続）。本稿執筆時点では、未だ認定事業者の申請はなされていないものの、同法により、大量の実診療データの研究を通じた最適医療の提供や、異なる医療機関・医療領域の情報を統合した治療成績の評価等が可能と考えられていることから、今後の動向が注目されている。

イ　カメラ画像の利用

近年における撮影機器や顔認証技術の発達に伴い、カメラの撮影を通じて様々なデータを取得することが可能となった。中でも、街中や店舗等に設置されたカメラ画像に関しては、人流情報や棚割り情報の分析につながることから利活用のニーズが高い反面、被撮影

図表3　次世代医療基盤法のイメージ＊23



＊22　医療分野の研究開発に資するための匿名加工医療情報に関する法律
＊23　内閣官房健康・医療戦略室内閣府日本医療研究開発機構・医療情報基盤担当室「医療分野の研究開発に資するための匿名加工医療情報に関する法律について」3頁より
https://www.kantei.go.jp/jp/singi/kenkouiryou/jisedai_kiban/pdf/sanko.pdf

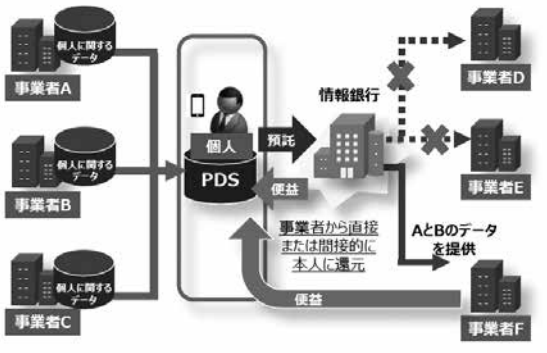
者の不安を払拭する必要もある*24。そこで、2018年3月に、IoT推進コンソーシアム、総務省及び経済産業省が、個人を特定する以外の目的（例えば、来店客の属性の推定、行動履歴の生成、リピート分析等の目的）でカメラ画像を利活用する事業者を対象に、「カメラ画像利活用ガイドブックver2.0」*25を公表した。同ガイドブックでは、事業者がカメラ画像の撮影及び利活用を行う際の、事前告知時、取得時、取扱い時、管理時の配慮事項や具体的なユースケース等が解説されており、実務上の参考になる*26。

ウ　情報銀行

個人情報を含むパーソナルデータを安全に流通、利活用できる環境整備に向けて、内閣では、かねてからPDS（Personal Data Store）や、情報銀行、データ取引市場の仕組みが検討されてきた*27。

このうち、情報銀行が近時注目を集めている。情報銀行は、行動履歴や購買履歴等のパーソナルデータを、本人が指定した条件の下で管理し、企業等の第三者に提供する仕組みを指す（**図表4** 参照）。2018年6月には、総務省と経済産業省が、情報銀行の認定基準やモデル約款の記載事項等を定めた「情報信託機能の認定に係る指針ver1.0」を公表した*28。同年8月以降においては、大手銀行、広告代理店、電機メーカー、保険会社等が情報銀行事業への参入を表明しているほか、IT事業者の業界団体が情報銀行の妥当性を判断するための認定事業を開始するなど、事業者の関心が高まっている。情報銀行の仕組みに関しては、パーソナルデータの利活用による本人への便益の還元が期待される反面、事業者による透明性の確保や、本人による情報のコントローラビリティの確保といった点に注意が必要である。

図表4　情報銀行のイメージ*29



※本人には便益が還元されず、社会全体にのみ便益が還元される場合もある。

（4）個人情報漏えいに関する近時の裁判例

2014年に、国内の大手通信教育事業者から約4,900万人分の個人情報が漏えいし、大きな社会問題となった。多数の顧客が、同通信教育事業者（以下、「被告通信教育事業者」という。）とシステム開発・運用の委託先事業者（以下、「被告委託先事業者」という。）に対して慰謝料等の支払いを求める訴えを提起していたところ、地裁判決（東京地判平成30年6月20日）は、次の注目すべき判断を行った。

1点目は、委託先の監督義務に関する判断である。判決は、被告通信教育事業者が被告委託先事業者の「セキュリティソフトウェアの変更について適切に監督をすべき注意義務」があったにもかかわらず、「業務用パソコンのセキュリティソフトウェアの変更をすべき旨を指摘することなく放置していた（更新すらされていなかった）結果、本件漏えいを回避できなかった」ことから、委託先の監督にかかる注意義務違反を認めた。しかしながら、委託先企業のセキュリティソフトウェアの変更まで確認している事業者は必ずしも多くないと思われるため、実務に影響しうる判示と言える。

2点目は、損害についての判断である。判決は、氏名や住所などの情報が、「思想信条や性的指向等の情報に比べ、一般的に『自己が欲しない他者にはみだりに開示されたくない』私的

＊24　2014年には、JR大阪駅の駅ビル内に多数のカメラを設置し、通行人の顔を撮影して人流を調べる実証実験が予定されていたところ、市民団体の反対等を受け一時延期された。詳しくは、映像センサー使用大規模実証実験検討委員会「調査報告書」（http://www.nict.go.jp/nrh/iinkai/report.pdf）参照。
＊25　http://www.meti.go.jp/press/2017/03/20180330005/20180330005-1.pdf
＊26　なお関連して、ドローンによる撮影映像と個人情報の関係については、個人情報保護法の平成27年改正施行前の資料ではあるが、総務省「「ドローン」による撮影映像等のインターネット上での取扱いに係るガイドライン」（平成27年9月）を参照
http://www.soumu.go.jp/main_content/000376723.pdf
＊27　内閣官房IT総合戦略本部データ流通環境整備検討会「AI、IoT時代におけるデータ活用ワーキンググループ　中間とりまとめ」（平成29年3月）
https://www.kantei.go.jp/jp/singi/it2/senmon_bunka/data_ryutsuseibi/dai2/siryou2.pdf
＊28　http://www.meti.go.jp/press/2018/06/20180626002/20180626002-2.pdf
＊29　内閣官房IT総合戦略室「AI、IoT時代におけるデータ活用ワーキンググループ　中間とりまとめの概要」（平成29年3月）7頁より
https://www.kantei.go.jp/jp/singi/it2/senmon_bunka/data_ryutsuseibi/dai2/siryou2.pdf

領域の情報という性格は低い情報」であり、また漏えいにより「ダイレクトメール等が増えたような気がするという程度を超えて、原告らに何らかの実害が生じたことはうかがわれない」などと判断した上で、被告通信教育事業者の持株会社が顧客に対しお詫びの文書を送付するとともに、顧客の選択に応じて500円相当の金券を配布したこと等も考慮し、「少なくとも現時点においては、最も多くの種類の個人情報（氏名、性別、生年月日、郵便番号、住所、電話番号、メールアドレス及び出産予定日）が漏えいした原告らであっても、民法上、慰謝料が発生する程の精神的苦痛があると認めることはできない」として、原告らの損害発生を否定した。本件は控訴中であるため、控訴審以降の動向にも注意が必要である。

3 海外の主な動向

海外においても、GDPR制定後に様々な動向が見られた（簡易な整理として**図表5**参照）。特に欧米との関係では、次の2点が注目される。

1点目は、EUがいわゆる「eプライバシー規則案*30」を公表したことである。これは、EUで2002年に制定された「eプライバシー指令」を、加盟国に直接適用される規則に引き上げ、EU域内における統一的規制を図るものである。GDPRに続き、eプライバシー規則案においても日本の事業者に対する域外適用が考えられることから、今後の動向に注意が必要である。

2点目は、米国におけるプライバシー法制定に向けての動きである。2018年に発覚したFacebookのケンブリッジ・アナリティカ事件等を機に、諸外国ではプライバシーの保護強化に関する議論が活発化していたところ、その一端として、同年6月には米国カリフォルニア州でいわゆる消費者プライバシー法*31が成立した。更に同年9月には、米議会の議員がAmazon社、Apple社、Google社、Twitter社の関係者らを招いて連邦プライバシー法のあり方に関する公聴会を開催するなど、連邦法制定に向けての議論が活発化している。これらの法規制も、日本の事業者に対する影響が考えられることから、今後の動向に注意が必要である。

6 終わりに

以上で見てきたように、GDPRをはじめ、個人情報をめぐる近時の国内外の動向には目まぐるしいものがある。本稿も、執筆時である2018年9月時点の動向を概説したものにすぎず、公刊時点では更に各種の動向が進展している可能性もある。弁護士として個人情報関連の業務を扱う際には、法令や裁判例の動向だけにとどまらず、法制度外の動向も含め、常に最新の動向をチェックする必要があることに留意されたい。

図表5 海外での個人情報をめぐる主要な動向

時期	表題	概要
2017年1月	EUがeプライバシー規則案を公表	電子通信データの処理に関する規制、クッキー（cookie）等の端末装置保存情報等に関する規制、ダイレクトマーケティングに関する規制等を整備。規則案の成立時期は未定。
2017年6月	中国でサイバーセキュリティ法（网络安全法）が施行	個人情報の国外移転に関するセキュリティアセスメント等の規制を整備。
2018年3月	Facebook&ケンブリッジ・アナリティカ事件発生	イギリスのデータ分析会社ケンブリッジ・アナリティカが、ケンブリッジ大学の研究者が収集したFacebookユーザー最大8,700万人分の情報を不正に入手し、2016年のアメリカ大統領選挙でドナルド・トランプ氏の陣営の選挙工作に利用。
2018年6月	カリフォルニア州で消費者プライバシー法が成立	ケンブリッジ・アナリティカ事件などを背景に、カリフォルニア州で消費者からの個人情報の開示請求権等を定めた法律が成立。2020年1月に施行予定だが、同法の成立を機に、連邦プライバシー法制定の議論も活発化。
2018年9月	Facebookで大規模な個人情報漏えいが発覚	Facebookが、最大5,000万人分のアクセストークン（ユーザーログイン時にパスワード入力を不要とするデジタルキーの機能を有するもの）が流出した可能性があると発表。

＊30　Regulation on Privacy and Electronic Communications
＊31　The California Consumer Privacy Act of 2018