海外プライバシー規制の動向

寺田 眞治 ●一般財団法人日本情報経済社会推進協会 主席研究員
柊 紫央璃 ●一般財団法人日本情報経済社会推進協会 客員研究員

中国でついに個人情報保護法が施行。越境移転に関する規定は日本企業への影響が大きい。プライバシー保護の環境と制度が世界的に整う中、日本発のデータ流通はDFFTで攻勢に転じるか。

2021年も各国でプライバシー保護法の制定、あるいは制定に向けた動きが相次いだ。先進国や経済規模の大きい大国での法整備はほぼ一段落し、これからは中進国や発展途上国へと広がっていくことになる。世界の法制度のベースとなっているのはOECDの8原則とEUのGDPR（General Data Protection Regulation、一般データ保護規則）であるが、これをベースに各国の事情に合わせて内容を変えたり独自のものを追加したりしているのが一般的だ。

本稿では、2021年に最も話題となり、日本への影響が大きな中国の個人情報保護法について概説し、EU・米国・アジアの動向、世界の中での日本の立ち位置をお伝えする。

■中国の個人情報保護法

2021年11月1日、中華人民共和国個人情報保護法（以下、中国個人情報保護法）が施行された[1]。これにより、中国における個人情報保護の基本的な体系がほぼ完成し、実務面での行政法規やガイドラインの整備が急速に進められている段階である。

体系化の動きは、まず2017年10月に施行された中国民法総則に表れる。第111条において「自然人の個人情報は、法律による保護を受ける。他者の個人情報を取得する必要がある組織および個人は、法令に従って個人情報を取得し、個人情報の安全を確保しなければならず、他人の個人情報を違法に収集、利用、処理、または譲渡することは禁止する」と規定された。さらに上位となる中国民法典には、2021年1月施行においてプライバシーおよび個人情報保護に関する章（第4編第6章）が新たに設けられ、プライバシー権の定義が初めて規定された。

今回施行された中国個人情報保護法は中国民法典における個人情報保護の考えを受け継いで、個人情報処理規則、個人情報越境移転、個人の権利および個人情報処理者の義務などに対し、具体的に整理・規定したものとなっている。さらに、草案第2稿からの変更点として、第1条に「憲法に基づき、本法を制定する」との記述が追加されており、中国における個人情報保護制度の体系化を一通り整えたものとした。

適用対象は、中国国内において自然人の個人情報を取り扱う活動、中国国外において中国国内の自然人の個人情報を取り扱う活動が、以下のいずれかに該当する場合となっている。

①国内の自然人に向けて商品またはサービスを提供することを目的としている
②国内の自然人の行為を分析し、評価する
③法律または行政法規が規定するその他の状況

●個人情報の定義と取り扱いの原則・ルール

個人情報の定義は「電子的またはその他の方法で記録された、既に識別されまたは識別可能な自然人に関する各種情報をいうが、匿名化処理後の情報を含まない」となっている。「特定の個人」としていないことから、日本法とは異なりGDPRに近いものとなっている。

個人情報の取り扱いに関しては、中国個人情報保護法の第5条から第10条にかけて、以下の基本原則が定められている。

第5条：合法性、正当性、必要性および信義誠実
第6条第1項：明確かつ合理的な目的および目的との直接関連
第6条第2項：本人の権利利益への影響が最小となる方法・範囲の収集
第7条：公開および透明性の原則
第8条：個人情報の質と正確性の保証
第9条：セキュリティの保障
第10条：法令順守・国家安全・公共利益保護

具体的なルールとして、下記の7つの正当化事由のいずれかに該当しない限り個人情報の取り扱いはできないとしている。

①本人の同意を取得している場合
②本人が当事者の一方となる契約の締結もしくは履行に必要な場合、または適法に制定された労働規章制度および適法に締結された集団的契約に基づく人事管理を実施する上で必要な場合
③法定の職責または法定の義務の履行に必要な場合
④突発的な公衆衛生上の事案に対応し、または緊急状況下において自然人の生命、健康および財産の安全の保護のために必要な場合
⑤公共の利益のためにメディア報道や世論監督などの行為を実施し、合理的な範囲で個人情報を取り扱う場合
⑥本法の規定に基づき合理的な範囲で本人が自ら公開し、またはその他の適法に既に公開されている個人情報を取り扱う場合
⑦法律・行政法規が規定するその他の状況

そのほか、センシティブな個人情報を取り扱う場合や個人情報が越境移転される場合などにおいては、本人に個別的同意または書面による同意を得なければならないと法律または行政法規が規定していれば、当該規定に従わなければならない。

さらに、同意の必要の有無にかかわらず告知の義務が課せられている。具体的には「目立つ方式で、明確かつ理解しやすい表現を用いて、本人に対し、真実を、正確かつ完全に」告知しなければならない。同意および告知の要件にはいずれも「法律・行政法規の規定するその他の状況」のようなバスケット条項が設けられているため、今後法律などによって追加されるかを注視しておく必要がある。

日本の要配慮個人情報に相当するものとしてセンシティブな個人情報が定義されているが、その取り扱いの要件には「特定の目的と十分な必要性」および「厳格な保護措置」が定められており、同意および告知に関しても通常の事項に加えて特則がある。特に注意したいのは、14歳未満の情報がセンシティブな個人情報に含まれるようになり、その場合は、さらに親またはその他の監護者の同意を取得し、かつ専門的な個人情報取り扱いルールを設けなければならないという点である。

●自動的決定

GDPR第22条第1項の「自動化された意思決定およびプロファイリングの規制」に類似した、自動的決定規制がある。自動的決定とは、コンピュータープログラムを通じて自動的に本人の行為習慣、興味、嗜好または経済、健康、信用状況などを分析・評価し、決定を行う活動をいう。個人情報取扱者が個人情報を利用して自動的決定を行う場合には、「決定の透明度および結果の公平性・公正性を保障しなければならない。本人に対し、取引価格などの取引条件において不合理な差別的待遇を実施してはならない」との原則を据えた上で、「自動的決定の方法によって本人に対し、情報配信、商業的マーケティング活動を実施する場合には、同時に当該本人の特徴に基づかない選択項目を提供し、または本人に対し簡便な拒絶方法を提供しなければならない」としている。

●データポータビリティ

中国個人情報保護法第45条第3項は、データポータビリティに関して規定している。本人が指定する個人情報取扱者に当該本人の個人情報を移転するように請求した場合、それが国家インターネット情報部門の定める条件に合致していれば、個人情報取扱者は移転方法を提供しなければならないとしている。

●越境移転

日本企業が最も注意しなければならないのが、越境移転に関する規定であろう。すべての個人情報取扱者を対象とした一般的な移転のルールとしては、必要事項の告知と個別の同意の取得に加え、以下の条件のいずれかを満たさなければならないとされている。

①国家インターネット情報部門による安全評価に合格した場合
②国家インターネット情報部門の規定に基づく専門機構による個人情報保護の認証を得ている場合
③国家インターネット情報部門が制定する標準的契約を域外の移転先と締結し、双方の権利および義務を約定する場合
④法律、行政法規または国家インターネット情報部門の規定するその他の条件

さらに、重要情報インフラ運営者および取り扱う個人情報が国家インターネット情報部門の規定する数量に達した個人情報取扱者に対し、中国域内で収集し、または発生した個人情報を国内で保存しなければならず、確かに域外に提供する必要がある場合には原則的に国家インターネット情報部門による安全評価に合格しなければならないとしている。

重要情報インフラ運営者は、中国個人情報保護法では定義されていないが、2017年6月施行のサイバーセキュリティ法によると「公共通信・情報サービス、エネルギー、交通、水利、金融、公共サービス、電子政府などの重要な産業および分野、並びにひとたび機能の破壊、喪失またはデータの漏えいに遭遇した場合、国の安全、国民経済と民生、公共の利益に重大な危害を与え得るその他の重要情報インフラの運営者」とされている。

規定する数量については、データ越境移転安全評価弁法（草案）を見ると「取り扱った個人情報が100万人に達した個人情報取扱者が越境移転する場合」「累計で10万人以上の個人情報または1万人以上のセンシティブな個人情報を越境移転した個人情報取扱者」とあり、これが目安となると考えられる。ネットワークデータセキュリティ管理条例（草案）では、データ越境移転安全評価に合格しなければならない対象者を「越境データに重要データが含まれている場合、重要情報インフ

ラ事業者、および100万人以上の個人情報を取り扱うデータ取扱事業者」としている。さらに、中国個人情報保護法にはデータ越境移転セキュリティ管理の章（第5章）が設けられており、「個人情報の越境移転に際しては、国外のデータ受領者の関連情報などを本人に通知するだけでなく、個別の同意を得なければならない」としている。同管理条例（草案）ではデータ越境移転する場合のデータ取扱者の義務が明確に規定されており、国によって「データ越境移転セキュリティゲートウエイ」を設置するコンセプトが打ち立てられていることにも注目したい。

中国個人情報保護法は、外形的にはGDPRに類似していることから、一見すると既にGDPR対応をしている企業にとっては比較的整合性を取りやすいように思われる。だが、実態としては排他的傾向が強いものとなっている。それは、同法のバスケット条項に基づき別途策定される法律や行政法規に表れており、いわゆるデータローカライゼーションといわれるデータの国内保存義務や越境移転について、厳しい規定が多く見られることからも明らかである。

■EUの動向

GDPRが2018年に施行されてから3年が過ぎ、違反に対する執行の事例が増えるのと同時にEU域内での定着も進んでいる。域外事業者に対する執行も、その制裁金の大きさで目立つことから、EUを対象とする海外事業者へのインパクトが大きく、GDPR対応は一種のトレンドになっている。さらに、各国でGDPRに類似する制度の制定が進んでいることから、デファクトスタンダードとしての位置付けにもなりつつあると言えるだろう。

一方で、拡大するオンラインビジネスに対応する電子通信を対象とし、GDPRを補完するePrivacy規則の制定は大きく遅れている[2]。2021年2月にEU閣僚会議において同意がなされ立法手続きに入ったものの、その後の進展は聞こえてこない。新型コロナウイルス感染症（COVID-19）パンデミックによるPublic Health Emergency（公衆衛生の緊急事態）への対応も影響していると考えられるが、最終草案に対しても各ステークホルダーの不協和音は解消されていないことから、まだ先行きに不透明感が残っている。規制程度の強弱については多少の変化はあるかもしれないが、いわゆるCookie規制と呼ばれる端末内のあらゆる情報の取得と第三者提供については同意を原則とする厳しいものになることは間違いないだろう。

ePrivacy規則の成立を待つまでもなく、ターゲティング広告やプロファイリングについてはGDPRの範ちゅうとして訴訟が提起されるなど、実質的に規制は有効化されていると見なせる状況にある。それは、米グーグル、米フェイスブック（現・メタ）、米アップルなど、デジタルプラットフォームであるビッグテックが着々と対応を進めていることからもうかがい知ることができる。

一方で、この規制はデジタルプラットフォームによる独自のルール策定の根拠ともなっており、いっそう支配力を高める原因ともなっていることで、プライバシー保護から市場競争や公正取引へと規制の視点が移行している。これについては「3-1 法律と政策：デジタルプラットフォーム規制の動向」にて詳説しているので参照されたい。

■米国の動向

米国では2020年1月にCCPA（California Consumer Privacy Act、カリフォルニア州消費者プライバシー法）が施行され[3]、2023年1月にはCPRA（California Privacy Rights Act、カリフォルニア州プライバシー権利法）が施行される予

定となっている。いずれも州法ではあるが、カリフォルニア州は米国において最大の人口とネット関連企業を擁することからその影響は極めて大きく、実質、米国のプライバシー保護についての規制をけん引し実体化していると見てもいいだろう。両法を手本としたような州法が続々と現れていることからも、それは確認できる。

一方で、米国全体を対象とする連邦法の制定は進んでいない。超党派による提案もなされており議論も行われてはいるが、成立のめどは立っていないのが実態のようだ。

対して、執行機関であるFTC（Federal Trade Commission、連邦取引委員会）の動きが活発になっている。2021年に相次いで、規制派と目されるリナ・カーン氏の委員長指名とアルバロ・ベドヤ氏の委員指名があり、FTCの権限および規模の拡大、規制法の制定が予想されている。それは、確定した予算によっても裏付けられている。

プライバシー保護についての技術的なアプローチも着々と進展している。NIST（National Institute of Standards and Technology、国立標準技術研究所）は、Privacy Flamework、既にデファクトスタンダードと見なせるCyber Security Flamework、これらの管理策となるSP 800-53 Rev. 5を発行しており、これらを機械可読化するOSCAL（Open Security Controls Assessment Language）の開発も進んでいる。さらに、国際標準としての地位獲得を目指すISO（International Organization for Standardization、国際標準化機構）への提案活動も活発である。

■アジアの動向

アジアで注目されるのは、インドのPDPB（Personal Data Protection Bill、個人情報保護法）である。執筆時点では国会での審議中であるが、年末もしくは年明けに成立する可能性が高い。ベースとなっているのはGDPRであるが、より厳しい規制が追加されている。特にデータの国内保存（データローカライゼーション）が規定されており対象から政府機関が除外されているため、政府による検閲などのガバメントアクセスをはじめ、海外事業者にとってはリスクマネジメントへの影響が大きいとみられている。

2021年12月に、韓国がGDPRの十分性認定を得たことも大きなトピックだ[4]。EUと同等の保護制度があると認定されたことにより、日本とも同等であると見なすことができる。今後は日本の越境移転先として、日本と同等の保護制度がある国に指定されるかが焦点になるだろう。

その他のアジアの国々も続々とプライバシー保護の制定を進めているが、そのほとんどはGDPRを手本としており、その意味では今後のデータ流通の拡大に寄与すると考えられる。しかし、一方でデータローカライゼーションやガバメントアクセスの導入も少なくなく、DFFT（Data Free Flow with Trust）の面からは問題が山積している状況である。

■世界と日本

日本においても2022年4月に、改正された個人情報保護法が施行される。新たに仮名加工情報や個人関連情報が定義されたことにより、一段とGDPRに近づくことになる。また、越境移転に際して移転先の保護制度やプライバシーに影響を与える制度については、情報を利用者に提供することが各国に対してDFFTをプロモーションしていく上での重要なアピールともなる。

総務省の電気通信事業法の改正に向けた動向にも注視する必要がある。当初は対象を設備からサービスへ、端末内の情報全般へと、ePrivacy規則案に近い改正が検討されていた。2022年の年明け時点では、事業者側の反発や政策的な駆け引

きの結果、かなり後退した内容となっている。しかし、消費者側の要求や欧米とのハーモナイゼーションに鑑みると、いずれ、より踏み込んだものへと向かうことは間違いないだろう。改正法案は2022年の通常国会への提出を目指しており、施行されれば、遅れているといわれていた日本のプライバシー保護制度も欧米並みに近づくことになる。

さらに、日本の事業者が各国・地域とのデータ流通をハーモナイズするためのツールとして、国際標準規格や多国間での認証制度などの普及も進められている。

国際標準規格としてはISO/IEC 27000シリーズが代表的であるが、この中でPII（Personally Identifiable Information、個人情報）を取り扱う場合に特化したISO/IEC 27701が日本でも認証可能になっている。個人情報保護委員会が推奨しているPIA（Privacy Impact Assessment、プライバシー影響評価）についても、ISO/IEC 29134がJIS X 9251として2021年2月にJIS化された。さらに2022年半ばには、通知と同意に関するISO/IEC 29184がJISとして発行される予定である。

多国間の認証システムとしては、APEC（Asia Pacific Economic Cooperation、アジア太平洋経済協力会議）のCBPR（Cross Border Privacy Rules、越境プライバシールール）がある。順調に参加国が増えており、日本でも大手IT企業が取得手続きに入っている[5]。

以上のように、日本のプライバシー保護制度も次第に欧米の内容に近づいており、併せて、世界に流通させるためのツールも利用できるようになってきている。出遅れ感のある世界でのデータ流通において、プライバシー保護については制度と環境が整いつつあると言える。政府のDFFT推進とともに攻勢に転ずることができるかが、2022年の見どころとなるだろう。

1. http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml
2. https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation
3. https://www.ppc.go.jp/enforcement/infoprovision/laws/CCPA/
4. https://ec.europa.eu/commission/presscorner/detail/en/statement_21_6915
5. https://www.jipdec.or.jp/protection_org/cbpr/

インターネット白書 ARCHIVES

1996,1997,1998,1999,2000....

［インターネット白書ARCHIVES］ご利用上の注意

このファイルは、株式会社インプレスR&Dおよび株式会社インプレスが1996年～2022年までに発行したインターネットの年鑑『インターネット白書』の誌面をPDF化し、「インターネット白書ARCHIVES」として以下のウェブサイトで公開しているものです。

https://IWParchives.jp/

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、データ、URL、名称など）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真・図の作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は掲載されていない場合があります。
- このファイルの内容を改変したり、商用目的として再利用したりすることはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用される際は、出典として媒体名および年号、該当ページ番号、発行元などの情報をご明記ください。
- オリジナルの発行時点では、株式会社インプレスR&Dおよび株式会社インプレスと著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

お問い合わせ先　インプレス・サステナブルラボ　✉ iwp-info@impress.co.jp