

## II-2 中国個人情報保護法と最新の動向

一般財団法人日本情報経済社会推進協会 電子情報利活用研究部 客員研究員 柗 紫央璃  
主席研究員 寺田 眞治

2021年11月1日、中華人民共和国个人信息保护法（以下、「中国個人情報保護法」という。）が施行された。また、これを補完するネットワークセキュリティ管理条例（草案）、データ越境移転安全評価弁法（草案）が11月にパブリックコメントにかけている。現在の状況は、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。本稿では、中国個人情報保護法と補完する最新の行政法規等について概要を説明するとともに、日本企業が検討すべき事項について若干の示唆を加えている。

### 1. 制定の経緯

中国でプライバシー保護や個人情報保護が法制度として整備し始められたのは、比較的最近のことである。個人情報保護を明確に示したのは、2009年に可決された刑法改正案（七）にて「個人情報の販売・不正提供罪、個人情報の不正入手罪」を定めたのが端緒と考えられる。その後、2015年の刑法改正案（九）で改正案（七）の2つの罪を個人情報侵害罪として合併し、情報セキュリティ管理義務履行拒否罪を追加している。この頃からさまざまな国の行政機関や地方行政が独自に個人情報保護を目的とする規制を短期間に次々と制定するが、個人情報の定義も微妙に異なり、個別の問題への対処といった面が強いものであった。

体系化の動きは、まず2017年10月に施行された民法総則に表れる。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及び個人は、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ない。他人の個人情報を違法に収集、利用、処理、又は譲渡することは禁止される。」と規定された。さらに上位となる中華人民共和国民法典は、2021年1月施行においてプライバシー及び個人情報保護（第6章）という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る。

今回施行された個人情報保護法は、この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てさらに具体的に整理、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が一通り整ったと考えられる。

### 2. 概要

#### 2.1 適用対象

中国国内において自然人の個人情報を取り扱う活動に対し適用される。また、中国国外においても、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は適用される。

（一）国内の自然人に向けて商品又はサービスを提供することを目的としている。

（二）国内の自然人の行為を分析し、評価する。

（三）法律又は行政法規の規定するその他の状況。

ただし、自然人は個人または家庭の事務により個人情報を取り扱うことに関しては、本法を適用されない。

## 2.2 基本的定義

個人情報	電子的又はその他の方法で記録された、既に識別され又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。
センシティブ個人情報	一旦漏えいし又は不法に使用されると、容易に自然人の人格的尊厳が侵害され、又は人身、財産安全に危害を受けやすい個人情報を言い、生体識別、宗教信仰、特定身分、医療健康、金融口座、行方所在等の情報、及び14歳に満たない未成年の個人情報を含む。
個人情報の取扱い	個人情報の収集、保存、使用、加工、伝達、提供、公開、削除等を含む。
個人情報取扱者	個人情報の取扱活動において、自らが取扱目的、取扱方法を決定する組織、個人をいう。
匿名化	個人情報が処理を経て、特定の自然人を識別できず、かつ元に復元することをできないようにする過程をいう。

### 2.3 個人情報の取扱いにかかる原則とルール：

個人情報保護法の第5条から第10条にかけて、個人情報の取扱いに関する以下の基本原則が定められている：合法性、正当性、必要性及び信義誠実（第5条）、明確かつ合理的な目的及び目的との直接関連（第6条第1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6条第2項）、公

開及び透明性の原則（第7条）、個人情報の質と正確性の保証（第8条）、セキュリティの保障（第9条）、法令遵守・国家安全・公共利益保護（第10条）

具体的な取扱いルールとして、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扱いはできないとしている。

(一) 本人の同意を取得している場合	
(二) ~ (七) 本人の同意が不要な場合	本人が当事者の一方となる契約の締結若しくは履行に必要な場合、又は適法に制定された労働規章制度及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。
	法定の職責又は法定の義務の履行に必要な場合。
	突発的な公衆衛生上の事案に対応し、又は緊急状況下において自然人の生命、健康及び財産の安全の保護のために必要な場合。
	公共の利益のためメディア報道、世論監督等の行為を実施し、合理的範囲内で個人情報を取り扱う場合。
	本法の規定に基づき合理的な範囲で本人が自ら公開し又はその他適法に既に公開済みの個人情報を取り扱う場合。
	法律、行政法規の規定するその他の状況。

また、個人情報の取扱いに際し、センシティブ個人情報を取り扱う場合や個人情報の越境移転の場合など、本人の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する場合には、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。「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、真実で、正確でかつ完全に」以下の事項を告知しなければならない。

共通	個人情報取扱者の名称又は姓名及び連絡先
	個人情報の取扱目的、取扱方法、取り扱う個人情報の種類及び保存期限
	本人が本法の規定する権利を行使する方法及び手続
	法律及び行政法規が告知すべきと規定するその他の事項
個人情報取扱者の合併、分割、解散、破産宣告等によって個人情報の移転が発生する場合	移転先の名称又は姓名及び連絡先
他の個人情報取扱者に個人情報を提供する場合	受領者の名称又は姓名、連絡先、取扱目的、取扱方法及び個人情報の種類
センシティブ個人情報を取り扱う場合	センシティブ個人情報を取り扱う必要性及び本人の権利利益への影響
越境移転の場合	移転先の名称又は姓名、連絡先、取扱目的、取扱方法、個人情報の種類及び本人が域外移転先に対する権利を行使する方法及び手続等の事項

このように、同意、告知の要件として、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、今後法律等によって追加されるかをウォッチしておく必要がある。

たとえば、2021年11月にパブリックコメントが開始されたネットワークセキュリティ管理条例（草案）において、本人の同意に基づき個人情報を取り扱う場合の要件を以下のとおり具体的に提示している（第19条）。

- （一）取り扱う個人情報は、サービスの提供に必要であり、又は法律、行政法規で定める義務の履行のために必要である。
- （二）取扱いの目的を達成するための最短期間、最低頻度に限定し、個人の権利・利益への影響が最小となる方法を用いる。
- （三）サービスの提供に必要な個人情報以外の情報の提供を拒否したことを理由に、サービスの提供を拒否し、又は本人のサービスの正常な利用を妨げてはならない。

同意と告知についても、個人情報の第三者移転の場合は「個人情報を提供する目的、種類、方法、範囲、保管期間、保存場所を本人に告知し、かつ本人の同意を個別に取得する」としている。

## 2.4 センシティブ個人情報の取扱いに関する特則

センシティブ個人情報の取扱いの要件として、

「特定の目的及び十分な必要性」および「厳格な保護措置」が定められている。同意および告知に関しては2.3で整理したとおりに通常の事項に加えて特則がある。

特に注意したいのは、草案第2稿からの変更点として14歳未満の情報がセンシティブ個人情報に含まれるようになったことであり、その場合はさらに父母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扱ルールを設けなければならないという点である。

## 3. その他の主な特徴

### 3.1 域外適用

中国個人情報保護法は、中国国内の自然人に製品、サービスを提供し、または中国域内の自然人の行為を分析し評価する中国国外における個人情報の取扱いを適用範囲としている。これはGDPRの域外適用規定にきわめて近い考え方で、たとえば日本のゲーム会社がアプリストアを通じて中国国内の自然人にゲームを提供し、個人情報の取扱いを行う場合、直接適用されることになる。域外適用規定が置かれていることから、中国に関連会社がある企業に留まらず、自社またはグループ会社の非中国企業が適用を受けないかについて確認する必要が出てくる。

### 3.2 自動的決定の規制

自動的決定は、コンピュータ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、信用状況等を分析、評価し、決定を行う活動をいう。

これは、草案第2稿を審議した際に殊に条項の強化を指示された部分で、APIによる過剰な個人情報収集や、それに伴うビッグデータによる差別的な取引価格などの不合理な取引の実施が、近年中国で問題となっていることが背景にある。GDPR第22条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ている。

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、「決定の透明度及び結果の公平性・公正性を保障しなければならない。本人に対し、取引価格等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、又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（第24条）。

### 3.3 データポータビリティ権

第45条3項のデータポータビリティに関する規定も最終稿に新たに加えられた内容である。本人が指定する個人情報取扱者へ当該本人の個人情報を移転するよう請求した場合、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されている。しかし、対象となる個人情報の範囲や具体的な条件、実務面における移転方法の提供をどのように実現するかについては記載されていない。ただし、前述のネットワークセキュリティ管理条例（草案）において、以下のようにある程度の規定が提示されている（第24条）。

- (一) 移転請求がなされた個人情報が同意に基づく場合、又は契約の締結、履行のために収集が必要な個人情報である場合。
- (二) 移転請求がなされた個人情報が本人の情報又は請求者が合法的に入手した他人の情報であり、かつ他人の意思に反していない場合。

- (三) 請求者の合法的な身分を検証できるデータ取扱者は、個人情報を受領する他のデータ取扱者が個人情報を不正に取り扱うリスクを発見した場合は、個人情報の移転請求に対して合理的なリスク提示を行わなければならない。

### 3.4 域外移転のルールとデータ国内保存義務

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、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。

- (一) 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。
- (二) 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。
- (三) 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、双方の権利及び義務を約定する場合。
- (四) 法律、行政法規又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。

(一)の安全評価に関しては、さっそくデータ越境移転安全評価弁法（草案）がパブリックコメントに出され、11月28日まで意見募集が行われた。(二)の個人情報保護の認証はまだ詳細が明かされていない。(三)の「標準契約」もまだ策定中のようだが、GDPRのSCCとの類似点についても注目したい。

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を対象に、第40条では中華人民共和国域内で収集し、または発生した個人情報を国内で保存しなければならないと、たし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。重要情報インフラについて個人情報保護法では定義の扱いがないが、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、電子政府等の重要な産業及び分野、並びにひとたび機能の破壊、喪失又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（第31条）。また、規定する数量は、前述のデータ越境移転安全評価弁法を見ると「取り扱った個人情報100万人に達した個人情報取扱者が越境移転する場合」（第4条第3号）、「累計で10万人以上の個人情報又は1万人以上の機微な個人情報を越境移転した個人情報取扱者」（第4条第4号）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）でも、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（第37条第1号）、重要情報インフラ事業者、及び100万人以上の個人情報を取り扱うデータ取扱事業者（第37条第2号）としている。

さらに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、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。また、同管理条例の草案では、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（第39条、40条）、国によって「データ越境移転セキュリティゲートウェイ」を設置する（第41条）コンセプトが打ち立てられていることにも注目したい。

#### 4. 今後の動向と日本企業の対応

中国個人情報保護法は基本的な方向性と原則を定めたものであり、外形的にはEUのGDPRに類似している。すでに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一見思われるが、実態としては排他的傾向が強いものとなっている。それは本法律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言われるデータの国内保存義務や越境移転について、厳しい規定が多くみられることから明らかだ。ただし、これらは必ずしも国外の事業者の締出しを図るためのものではなく、国内の事業者による

無秩序なデータの流出を阻止する意味合いの方が大きいと考えられている。特に最近締付けを厳しくしている中国国内のプラットフォーム事業者や新興の大企業をターゲットにしていると思われる。したがって、ただちに日本企業に対して取締まりが行われるかと言えば、その可能性は現時点ではさほど大きくはないと見られている。しかし、法律制定時の見せしめ的な一斉取締まり、対外環境の悪化などさまざまな不確実性を勘案すると、あまり良い言い方ではないが「不運な」状況に陥る企業が出てくるのも避けられないだろう。

法律の遵守は当然のことなので、本来「不運」とは言えないが、この法律だけで具体的で明確な対応を行うことは現実的には困難である。今後策定される補完的な、あるいは領域別、場合によっては地域別の法律、行政法規、さらにはガイドラインが出てくるまでは想定されるリスク範囲を大きく設定して対応するしかないのが実態である。過去に制定されたさまざまな規定も参考にはなるが、本法律に合わせて改定されたり無効にされたりするものもあると思われるので、実効性を十分に見極める必要がある。

また、現地の政策動向や国際環境変化などの外部の情報に注意を払うことは当然のことではあるが、現地従業員に対する教育や個人情報を扱う委託事業者の管理など、ガバナンスの強化も必須である。中国サイバーセキュリティ法が2017年6月に施行されて以降、個人情報を含むデータセキュリティに関する規定やガイドラインが大量に策定されている。同様に今回の個人情報保護法に合わせて、本稿でも触れているように個人情報の安全管理措置に該当するセキュリティに関連する規定の策定が相次いで予定されている。企業は取扱いのルールを策定するだけでなく、これを遵守できる体制の確立が喫緊の課題となるであろう。

中国のプライバシー保護、個人情報保護に関する基本的な法体系の確立が、今回の個人情報保護法の施行で一応の完成に達したと考えられる。今後は、この法体系の下にあらゆる領域において実効的な整備が急速に進められることが想定される。中国の法制度の普及や執行のスピードはきわめて速いことから、各企業もこれを見越した対応が必要であり、リスクマネジメントの最大のポイントになるであろう。