# 中国における個人情報保護法の制定に向けて

――諸外国の立法経験と運用に基づく提言――

周　小稚

## はじめに

個人情報保護の歴史を見ると、新たな課題ではないが、現在、個人情報保護に関する議論はさらに大きくなっている。その原因は情報技術が目覚ましく発展するにつれて、個人情報自体の価値とそれによって創造される新たな付加価値とがますます重視されているからである。

すなわち、公的機関にとっては、合理的な政策決定や地域の雇用機会の確保や自然災害への対応を行うために、個人情報を利・活用する必要がある。他方、民間事業者にとっては、消費者個人を把握し、消費ニーズにマッチした営業戦略の決定や経営判断などのためにしばしば個人情報を利・活用する必要がある。

しかし、個人の立場は公的機関や民間事業者とは異なる。個人は、高度な情報化社会の中で、特定の個人が識別されることが容易になっていく点に注目する。そして、生活する中で個人情報の漏洩や濫用や不正な利用などによって詐欺、誹謗中傷、風説の流布などが頻繁に起こるため、個人は自己の情報が安全に取り扱われているかどうかを危惧する。しかも、個人情報には商業的価値がある。そのため、個人は、自己の利益を保護するため、自分の個人情報をコントロールすることができるよう求める。

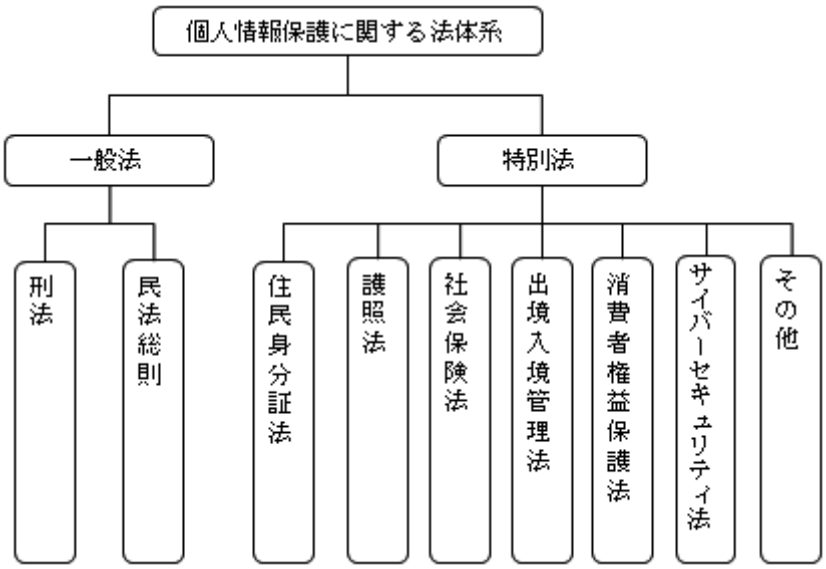
公的機関と民間事業者は情報の利・活用を求めるが、個人は情報の保護を求める。そのため、個人情報において利用と保護との衝突が常に起こる。世界的に見ると、個人情報保護法はよく利用と保護との衝突を調整させる工具とみなされる。

すなわち、国際組織のガイドラインは構成国が個人の尊厳と公共性を協調させることを要求している。たとえば、EU データ保護指令（1995 年）[1]を例としてみると、この指令の目的は自然人の個人情報の権利を保護すると同時に、構成国間の個人情報の自由な流通を制限し、または禁止してはならない（指令 1 条）とあり、各構成国がこの指令に従って国内規定を採択することを求めている（指令 4 条 1 項)。つまり、各構成国の国内法は個人情報を保護しながら、情報の流通を保護することを規定しなければならないのである。

また、諸外国の現行法の内容からみると、個人情報保護法は個人の尊厳と公共性との協調を目的としている。たとえば、日本は明文で「個人情報の適正かつ効果的な活用が新たな産業の創出並びに活力ある経済社会及び豊かな国民生活の実現に資するものであること、その他の個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とする」と規定している（個人情報保護法 2 条)。

2017 年までに個人情報保護法を制定した国は、90 か国になっている[2]。現在、中国には一元的な個人情報保護法はなく、関連の規定は他の法律の中に散在している(図 1 を参照)。

図 1　中国の個人情報保護に関する法体系イメージ




注：その他は中華人民共和国統計法、中華人民共和国教育法、中華人民共和国反恐怖主義法（テロリズム防止法）、中華人民共和国反間諜法（スパイ防止法）など本論文が紹介しない個人情報に関する法律である。
出典：筆者作成

図 1 のように、刑法、民法総則、住民身分証法、護照（パスポート）法、社会保険法、出入境（出入国）管理法、消費者権益保護法、サイバーセキュリティ法には個人情報に関する条文が設けられている。しかし、これらの規定には以下の 2 つの不備があることに注意する必要がある。

1 つは、個人情報の保護範囲に制限があることである。たとえば、住民身分証法は住民身分証の中の情報だけを保護の対象としており、護照法はパスポートの情報だけを保護の対象としている。すなわち、現行法はその法の領域だけの個人情報を規定している。

2 つは、諸法律の個人情報保護に関する規定は、個人情報を取り扱う過程の一部だけであることである。たとえば、住民身分証法、出入境（出入国）管理法、社会保険法、護照法などは主に守秘義務と職員の責任のみを規定しており、他のことは規定していない。

2019 年 3 月に開催された「中華人民共和国第十三回人民代表大会第二次会議」では、個人情報保護法の制定が 2020 年の立法計画に組み入れられた[3]。しかし、諸外国における個人情報保護法の発展の歴史からみると、当該法律の制定は非常に遅いと言わざるを得ない。たとえば、スウェーデンが初めて個人情報保護法を制定したのは 1973 年であり、アメリカは 1974 年であり[4]、日本は 1988 年である。したがって、スウェーデンやアメリカ、日本などの国における立法経験やその運用は中国の個人情報保護法づくりに一定の示唆を与え得ると考えられる。

他方、グローバル化の影響で、一国の立法は国内の状況のみを考えるだけでなく、国際

状況にも配慮しなければならなくなっている。EU データ保護指令（1995 年）も一般データ保護規則（2016 年）も EU 加盟国だけではなく、EU 加盟国以外の第三国の個人情報保護施策にも大きな影響を与えている。

そこで、本稿では、中国において間もなく行われる個人情報保護法の立法作業に向けて、参考となる示唆を探る目的で、諸外国の立法経験とその運用（現行法における法体系、メカニズム、個人情報の範囲、匿名化加工情報、個人情報の分類など）を紹介し、考察することにする。

## １　個人情報保護の法体系

現在、諸外国の個人情報保護法体系は大別して 3 種類に分けられる。まず、1 つは法律が公的部門と民間部門の双方を対象とするもので「オムニバス方式」と呼ばれるものである。2 つは、両者を別々の規範で規律するもので「セグメント方式」で、3 つ目は、これら 2 つの方式の折衷である[5]。この「折衷方式」は基本法的部分に関してはオムニバス方式で、一般法的部分に関してはセグメント方式を採るものである[6]。以下にこの 3 種類を説明する。

### ⑴　オムニバス方式

これを代表するのはドイツである。ドイツの連邦データ保護法（2009 年改正）は公的部門と民間部門を包括的に規律している。その第 1 章は総則であり、第 2 章は公的機関の個人情報保護であり、第 3 章は民間部門の個人情報保護である[7]。

### ⑵　セグメント方式

セグメント方式の代表はアメリカである。アメリカには個人情報保護の法律が多い。例えば、消費者の信用報告を保護対象とする公正信用報告法（1970 年）、公的部門の保有する個人情報を保護対象とするプライバシー法（1974 年）、医療の領域での個人情報を保護対象とする医療保険の携行と責任に関する法律（1996 年）、子どもの個人情報を保護対象とする子供オンライン・プライバシー保護法（1998 年）、金融分野での個人情報を保護対象とする金融サービス近代化法（1999 年）、消費者の個人情報を保護対象とする連邦取引委員会法（2005 年）などである[8]。

### ⑶　折衷方式

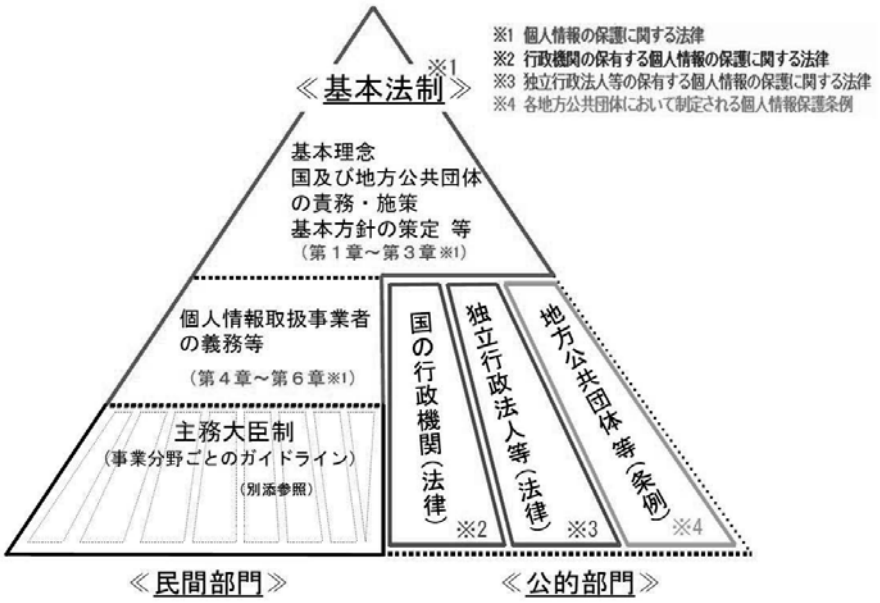
日本は折衷方式にあたる。日本の個人情報保護に関する法体系は国レベルでは個人情報保護法、行政機関個人情報保護法、独立行政法人等個人情報保護法で、地方公共団体ごとに制定した条例、各事業分野におけるガイドラインから構成されている。

このうち、個人情報保護法は、基本法にあたる部分（1 章～3 章）と民間部門の個人情報保護の一般法にあたる部分（4 章～7 章）の性格を併有しており、基本法と一般法の 2 層構造である[9]。すなわち、「個人情報保護法」の第 1 章から第 3 章までの基本理念や国及び地方

公共団体の責務・施策、基本方針の策定などは基本法制として個人情報のすべての領域に適用されているが、第 4 章以下は主として民間部門の保有する個人情報の領域に適用される。

一方、行政機関個人情報保護法と独立行政法人等個人情報保護法が適用される領域は、主として国の行政機関の保有する個人情報と独立行政法人等の保有する個人情報である。この 2 つの法律は国が関係する領域を含み、保護のシステムを構築している。また、個人情報保護条例は地方公共団体が保有する個人情報に適用される（図 2 参照)。

図 2　個人情報保護に関する法体系イメージ




注：このイメージ図は 2015 年の改正以前のものである。
2015 年 9 月に成立した改正個人情報保護法では、主務大臣制は新設の個人情報保護委員会に代わっている。この個人情報保護委員会は監督権限が一元化されている。
出典：内閣府「個人情報保護に関する法体系イメージ」（取得年月日：2018 年 8 月 15 日)。

冒頭に述べたように、中国にはまだ一元的な個人情報保護法はない（2020 年 1 月現在)。個人情報保護条項は諸々の個別法に散在しているだけである。このような現状に鑑み、できるだけ早く法整備を行う必要がある。しかし、世界の現行の 3 つの法体系に対して、中国がどれを選択して採用するかはなかなか難しい問題であろう。中国の現状を踏まえる必要がある。

## 2　個人情報保護のメカニズム

現在の世界には、個人情報保護のメカニズムは主に 2 つある。すなわち、欧州を代表とする個人情報保護に関する法制とアメリカを代表とする業界の自主規制である。以下ではこの 2 つのメカニズムとその効果を見てみる。

### ⑴ 欧州での立法の効果

欧州連合が制定したEUデータ保護指令（1995年）と一般データ保護規則（2016年）は全面的な個人情報保護基準を確立したものとして、世界中から注目を集めている。

EUデータ保護指令を見てみると、管理者（公的機関や民間部門を含む）と、情報主体の個人情報に関する権力あるいは権利と義務について詳しく規定している。たとえば、この指令は管理者の側に対して、個人情報を取り扱う時に遵守すべき原則（6条）、個人情報へのアクセス権（12条）、取り扱いの機密性と安全性の保障（16条、17条）、国民あるいは監督機関への通知の義務（10条、11条、18条、19条）、事前の調査の義務（20条）、作業の公開の義務（21条）、第三国への情報の移転の原則（25条）など権利（権力）と義務を規定している。同時に、情報主体に対する情報の取り扱いの同意（8条）、自己情報へのアクセス権（10条）、誤った情報の修正権（10条）、知る・同意（「認識・同意」）権（10条）、異議申立て権（14条）なども規定している。そして、EUの構成国は、この指令に従って国内法を制定しなければならないとなっている（4条）。

これは各構成国が全面的で一元的な個人情報保護法を制定する際の基本となっている。しかし、各構成国がこれを立法化するには時間を要する。その上、各構成国は文化や国情が異なるため、制定された各構成国の国内法が統一されるわけではない。

また、欧州連合は公的機関に監督を委託しすぎている。EUデータ保護指令によれば、監督機関は1つまたはそれ以上の公的機関で構成され（28条1項）、管理者[10]の名簿や取扱作業の記録を保管しなければならない（21条2項）。同時に指令はすべての構成国で管理者が個人情報の取り扱いを監督機関に通知しなければならないと定めている（18条）。この規定は、管理者の取り扱いの透明性には益するが、一方で、このように全部または一部の個人情報を取り扱う作業を政府機関に通知することは、時として政府を煩わす行為と思われる[11]。

また、業界による自主規制がない場合、法律や政府の指導は効果的に進まない。欧州連合の各構成国内の措置の統一的な適用に資するため、個人情報の取り扱いに係る個人の保護に関する作業部会（以下、作業部会）が設置される（30条）。この作業部会は各構成国が指名した代表者で構成され（29条）、職務は主として共同体域内及び第三国における保護のレベルに関する意見や共同体レベルで策定された行動規準に関して意見を提出することである。

しかし、実践してみると、法律や政策の指導だけでは個人情報の安全確保が不十分であることが証明された。そのため、作業部会は業界ルールを作ることを提案している。

### ⑵ アメリカにおける業界の自主規制の効果

アメリカでは、個人の尊厳と公共性との協調は公的部門と民間部門の2つの領域に分けて実施されている。公的部門の領域における個人の尊厳と公共性との協調は、個人情報保護に関する法律（プライバシー法）で行う。一方、民間部門における協調は主として自主規制に頼っている。

民間部門の自主規制はアメリカでは「業界の自主規制」と呼ばれ、すでに個人情報保護法制の重要な特徴になっている。いわゆる業界の自主規制は各部門が特定の産業や事案に応じて自主的に当該部門内に適用する規則を設け、事業者に行為規範を提供している。これは主に業界指導とオンラインプライバシープログラムで行う。具体的には、以下のようになっている。

**①業界指導**

この指導は組織内で制定され、組織のメンバーが遵守しなければならないもので、業界内に課す行為原則であり、アドバイスと同じものである[12]。アメリカにおける業界指導の組織は、古いものでは、1947 年に設立されたアメリカ計算機学会[13]、1951 年に設立されたデータ処理管理学会[14]があり、新しいものでは 1998 年に設定されたオンラインプライバシーアライアンス[15]などがある。

**②オンラインプライバシープログラム**

オンラインプライバシープログラムはプライバシー認証付与機関が個人情報保護の基準を満たす個人情報の利用者や事業者にプライバシーマークを付与することである[16]。例えば、TRUSTe というプライバシー認証付与機関がある。この組織には認証プログラムが 2 種類あり、それらは一般的なオンラインプライバシープログラムと特別な認証プログラムである。

一般的なオンラインプライバシープログラムの認証の内容はメンバーの個人情報の利用と保護の声明があるかどうか、消費者の情報のコントロールを保障できるかどうか、情報の安全のための措置があるかどうか、紛争解決の措置があるかどうかなどである[17]。特別な認証プログラムは主に児童のプライバシー認証プログラムとセーフ・ハーバー認証プログラムとメール認証プログラムである[18]。

理論的には、この自主規制の方式は市場の自動調整作用や私的自治や自助により、問題をタイミングよく解決できる。しかし、アメリカの実践からみると、自主規制は業界指導でもオンラインプライバシープログラムでも、個人の尊厳と公共性との協調において有効には作用していない。その理由を探ってみよう。

まず、業界指導組織についてである。業界指導は強制的ではない。たとえば、1998 年に設定されたオンラインプライバシーアライアンスという業界指導組織がある。この組織は詳細なオンラインプライバシーガイドラインと子供のプライバシーの保護の原則を規定した[19]。このガイドラインと原則に対して、オンラインプライバシーアライアンスはメンバーに個人情報を取り扱う時に遵守しなければならないことを要求している。しかし、この組織はガイドラインと原則の遂行状況を監督せず、その指導に違反した行為に対しても制裁を加えていない。また、メンバー数に変動がある。オンラインプライバシーアライアンスのメンバーは最大で 80 以上に達したが、2015 年には 30 くらいにまで減少し[20]、2019 年には 24 になっている[21]。

次に、オンラインプライバシープログラムにも欠陥がある。TRUSTe を例とすると、ア

メリカで 450 の会社がそのプライバシー認証マークを取得した。しかし、この数はアメリカのウエブサイト運営者の数に比べると少ない[22]。また、プライバシー認証マークを取得したとしても、それが会社の情報の取り扱いが合法であることを示すわけではない。例えば、GeoGties という会社は TRUSTe のプライバシー認証マークを取得したが、情報販売で連邦取引委員会に起訴されたことがある[23]。そして、TRUSTe のスポンサーの 50%は、オンラインプライバシープログラムやプライバシー認証マークの取得を望んでいないということである[24]。

このような結果に直面して、アメリカのフォーダム大学ロースクールの教授 Joel R. Reidenberg は、アメリカでは自主規制の発展自体が自助調整の構造的欠陥を証明しており[25]、政府による規制が行われる必要があるとして、「欧州とアメリカにおける個人情報保護法制の経験からみると、現在のビッグデータ時代にその中の学説の 1 つだけに頼るのは好ましい効果を得にくい」[26]と述べている。

欧州とアメリカの実践から言えることは、国の立法だけに頼るのも業界の自主規制のみに頼るのも欠陥があるということである。したがって、個人情報を有効的に保護するため、中国は国の立法と業界の自主規制とを同時に構築する必要がある。そして、これらが衝突せず、相互に協働することが構築の鍵である。これは、国の立法も業界の自主規制も経験に乏しい中国にとって、大きな挑戦であることは間違いない。

### 3　個人情報の範囲

諸外国の実定法から見ると、個人情報の範囲を判断する根拠には主に 3 つの捉え方が存在している。それは関連型、プライバシー型、識別型である。以下、詳細に見てみよう。

#### ⑴　関連型

関連型は、人に係わるすべての情報を個人情報と見るもので、その範囲は極めて広い。つまり、関連型の個人情報は、「人に関連している事実、判断や評価などの情報のすべてを指す。個人情報には、個人の私生活や名誉に係わる情報だけではなく、個人の社会文化活動や団体組織のメンバー活動などに係わるものも含まれている」[27]。関連型の代表国はカナダである。

#### ⑵　プライバシー型

プライバシー型においては、個人情報の概念は狭い意味と広い意味に分けられている。狭い意味の個人情報は、自己に関する事実を完全に私的な物として維持し、誰に、いつ・いかなる条件でそれを他人に知らせるべきかを自ら遠慮なく決定できることが個人にとって必要であるというものである[28]。

一方、広い意味の個人情報は、大きく 4 つに分けることができる。第 1 は、個人が 1 人でいることに対して干渉されないこと、第 2 は、人に知られたくない私的な事実を公開さ

れないこと、第 3 は、公衆に対して個人に対する誤った印象を与えないこと、第 4 は個人の名前や肖像が商業利用などをされないことである[29]。

しかし、判例の積み重ねから見ると、広い意味の個人情報は狭い意味の個人情報（私生活への侵入や私生活の公開などは、私生活からの情報収集であることに注目し、これを「狭い意味の個人情報」という）と「人格的自律権」（避妊の権利などは、私生活領域における「自己決定」であることから、これを人格的自律権という）を包括している。プライバシー型の代表国はアメリカと欧州諸国である。

### ⑶ 識別型

識別型情報は特定の個人を識別することができるものである。識別できる情報とするのは社会通念上である。例えば、特定の個人の身体の一部の特徴を電子計算機の用に供すために変換した文字、番号、記号、その他の符号であり、特定の個人を識別することができるものとして、顔認識データや指紋認識データが個人情報になっている[30]。また、対象者ごとに異なるものとなるように役務の利用、商品の購入または書類に付される符号として、運転免許証番号、旅券番号、基礎年金番号等も個人情報である[31]。これ以外に他の情報との照合により特定の個人を識別することができる情報も個人情報である。つまり、識別という個人情報はその情報と特定の個人との密接関連性、一意性（同一性）、不変性、共用性を強調している[32]。識別型の代表国は日本、スウェーデンである。

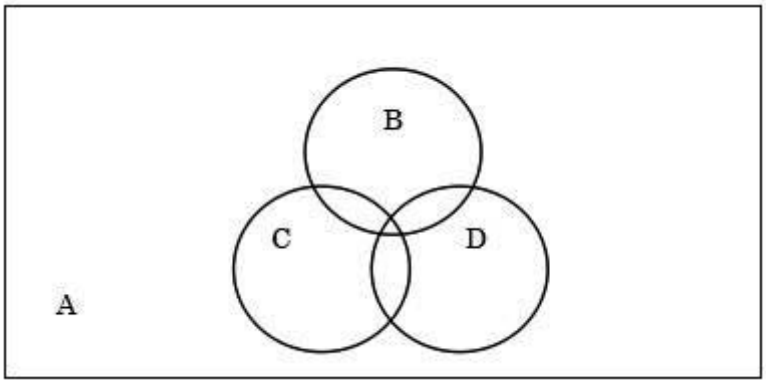
中国の現行法から見ると、「サイバーセキュリティ法」（2016 年）は中国の現行法の中で、唯一個人情報を定義づけた法律である。この法律の中で、個人情報とは何かが附則で規定されている。そこでは「個人情報とは、電子データ、その他の方式により記録され、単独又はその他の情報と組み合わせて自然人の個人の身分を識別することができる各種の情報をいう。これには、自然人の氏名、生年月日、身分証番号、個人の生物識別情報、住所、電話番号などを含むが、これらに限らない。」となっている。

この法条文によると、中国は個人情報の定義として識別型を採用している。しかし、ビッグデータ時代において、識別型の個人情報には以下の 2 つの問題が存在する。

まず、個人情報の範囲が広すぎることである。前述したように、識別型の個人情報は主として 2 つに分けられる。1 つは、単独で特定の個人を識別できる情報である。もう 1 つは、単独では識別できないが、他の情報と組み合わせて特定の個人を識別できる情報である。

単独で識別できる個人情報は、たとえば、個人番号や身分証番号や遺伝子情報や学生証番号などのような情報である。しかし、他の情報と組み合わせて特定の個人を識別できる情報の範囲は広すぎる。

図 3　特定の個人を識別するイメージ




出典：筆者作成

たとえば、上の図 3 に示したように、A を全体の人数、B を身長、C を体重、D を靴のサイズとする。かりに、A が 10 人以内のグループならば、B と C の情報を組み合わせると特定の個人が容易に識別できる。すなわち、特定の個人にとって、B、C の情報は個人に関する情報ではあるが、特別意味がある情報ではない。しかし、それらは特定の個人を識別できる可能性があるため、識別型の定義に基づく個人情報の範疇に属する。

これは、A が 50 人以内のグループでなければ、B、C だけでは特定の個人を識別できない。しかし、D の情報を追加すれば、特定の個人を容易に識別できる。このように A が何人いても、組み合わせる情報が十分あれば、特定の個人を識別することができることになってしまう。この点でいかなる情報も個人情報になる可能性がある。

次は、法律は個人情報を明確に定義することが困難であるということである。個人情報の内容は不変ではなく、技術の発展によって変わる。例えば、最初期には迷惑メールや迷惑メッセージや迷惑電話などは個人情報を侵害する行為ではないと認定された。しかし、その後、ドイツの判例は迷惑メッセージが個人情報を侵害する行為であると認定した[33]。そして、1991 年にアメリカの「電話消費者保護法」も迷惑メッセージを送る行為が個人情報を侵害する行為であると規定した[34]。

しかも、現在認定されている個人情報は、個人を識別できる情報だけではない。アメリカの連邦取扱委員会法は、特定のパソコンと装置（device）をリンクできる可能性がある情報も個人情報と認定した[35]。

したがって、中国では、個人情報保護法を制定するにあたって、識別型の抱える上記の問題点を意識しながら、個人情報の定義やその範囲を明確に定める必要があろう。

### 4　匿名化加工

いわゆる匿名化加工とは個人情報が特定の人を識別できないように加工することであり、これによって得られる情報は匿名化加工情報と呼ばれている。個人情報と非個人情報とを

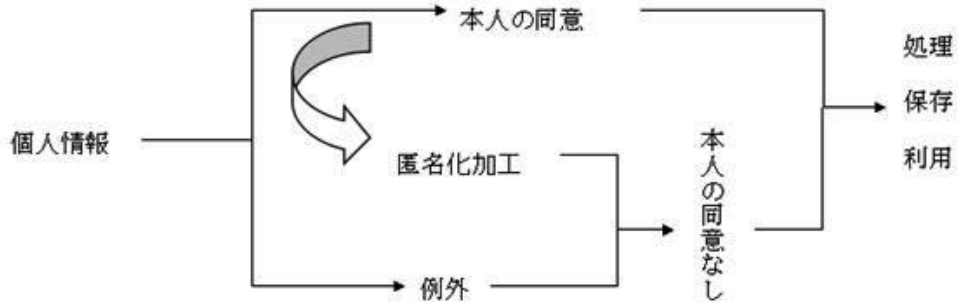
変換する手段である匿名化加工は、多くの外国ではすでに立法化されている。

スウェーデンを例とすると、スウェーデンの個人データ法（1998 年改正）は、復元できないように匿名化加工された情報は個人情報ではないと規定している[36]。この規定は匿名化加工された情報は個人データ法が適用されないとしている。簡単に言えば、匿名化加工された情報の取り扱いは個人データ法に従う必要はないのである。

日本にも 2015 年に初めて導入され、同年の日本の個人情報保護法改正の 1 つのハイライトと見なされた匿名化加工の規定がある。この法律において匿名化加工情報とは、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て得られる個人に関する情報であり、当該個人情報を復元することができないようにしたものをいう（2 条 9 項）。

匿名化加工は個人情報を非個人情報に転換する措置である。また、日本では匿名化加工の導入により「知る・同意」（「認識・同意」）という伝統的な枠を緩和しようとしている。個人情報保護法に基づいて、例外を除き、事業者は個人情報の処理・保存・利用・第三者への提供などの取り扱いを行う前に個人情報の本人の同意を得なければならない。しかし、当該個人情報が特定個人を識別できないように匿名化加工された場合、事業者は個人情報の本人の同意のあるなしにかかわらず、個人情報を処理・保存・利用・提供することができる。具体的には、図 4 のようになる。

図 4　日本における個人情報の利用と流通との転換イメージ




出典：日本の「個人情報保護法」により、筆者作成。

中国の現行法には匿名化加工に関する規定がない。しかし、学説や学者たちは外国の立法経験に基づく匿名化加工を中国に導入したがっている。たとえば、王利明によると、情報の保有者が個人情報を匿名化加工して得る情報は一般的な技術で特定の個人を識別することができない。これによって、ある程度情報と特定の個人との関連性が断ち切られよう[37]。中国人民大学教授の張新宝も匿名化加工情報は直接的に特定の個人を識別できないため、不正な取り扱いによる個人の損害リスクを下げることができると述べている[38]。

しかし、日常生活の中では、匿名化加工の役割は疑わしい。その理由は、特定の個人を識別できるかどうかは匿名化加工したかどうかでなく、情報保有者の側の保有する情報の内容次第だからである。

たとえば、1997 年、ハーバード大学と政府と技術の専門家の Latanya Sweeney は、アメリカのマサチューセッツ州のケンブリッジで選挙人名簿と 54,805 人の人口統計データを対照し、以下の結果を得ている[39]。

①個人の誕生日（年月日）だけを対照した場合、12%の選挙人を識別できる。

②個人の誕生日（年月日）と性別を対照した場合、29%の選挙人を識別できる。

③個人の誕生日（年月日）と 5 桁の郵便番号を対照した場合、69%の選挙人を識別できる。

④個人の誕生日（年月日）と 9 桁の郵便番号を対照した場合、97%の選挙人を識別できる。

これによると、匿名化された選挙人名簿でも、他の情報と組み合わせて特定の人物を再識別することができることが分かる。こうした状況では匿名化加工情報の意味はなくなる。

したがって、今後中国の法制定に際して、匿名化加工の規定を導入するだけでなく、その実効性の確保も考えなければならない。

### 5　個人情報の分類

諸外国の立法を見ると、個人情報を一般的な個人情報と機微性を持つ個人情報に分類し、利用と保護との協調を一つの重要な措置として立法化している事例も現われている。

たとえば、スウェーデンのデータ法（1998 年改正）においては、犯罪に関する事実、刑罰、強制処分、病気、健康状態、社会扶助の受給、個人の政治的または宗教的見解に関する情報を特別情報として蓄積することやファイルの設置が厳密に規定された。これらの情報を内容とする個人ファイルの設置及び保有に関しては、法令により権限が与えられている官庁以外の者に対しては、これを取り扱ってはならないとした（データ法 4 条）。

日本では、機微性を持つ個人情報は要配慮個人情報と呼ばれる。個人情報保護法の 2 条 3 項によれば、要配慮個人情報とは、本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実、その他本人に対する不当な差別、偏見、その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定めた記述等である（2 条 3 項に基づく）。これ以外の特定の個人を識別できる情報が一般的な個人情報である。一般的な個人情報よりも、個人情報保護法は要配慮個人情報をより慎重に取り扱うべきであると規定している。そのため、要配慮個人情報に対する取得は原則として禁止されている（2 条 2 項 3 号）。

アメリカは機微性を持つ個人情報を明文で規定してはいないが、医療分野、金融分野、教育分野における個人に関する情報と未成年者の個人情報は機微性を持つとしている[40]。そのため、これらの情報に対する規定は一層厳格である。一般的に、事業者は個人から個人情報を収集する時、収集の目的を個人に通知し、個人の同意を得れば、収集することができる。情報を収集した後、事業者は個人に自己情報へのアクセスや訂正、削除の権利を与えなければならない。しかし、子供オンライン・プライバシー保護法（1998 年）では、商

業目的のウェブサイトやオンライン・サービスの管理者は 13 歳未満の子供からインターネットを通じて個人情報を収集する場合、一段と厳しい規定を設けている。具体的には、以下のようになっている[41]。

①オンライン・プライバシーの告知は本人が容易に知り得る状態でなければならない。

②個人情報を収集・使用・公開する前に、親に直接通知しなければならない。

③個人情報を収集・使用・公開する前に、親の同意を得なければならない。

④親に対して児童の個人情報へのアクセス、訂正、削除の方法を提供しなければならない。

⑤子供がオンライン活動に参加するための条件として、必要以外の個人情報の提供を求めてはならない。

⑥児童の個人情報の機密性、安全性を完全に保護するため、必要な手段を講じなければならない。

以上のように、諸外国では個人情報を一般的な個人情報と機微性を持つ個人情報に区別することが多い。そして、一般的な個人情報か機微性を持つ個人情報かによって、異なる取扱いの基準を適用しており、子どもの個人情報は機微性を持つ情報と見なされることが多い。このように、一般の個人情報よりも機微性を持つ個人情報に適用する基準は一段と厳しい。

匿名化加工と同様、個人情報の分類に関する規定も中国の現行法の中にはない。この事実を受けて、多くの提案がなされている。例えば、個人情報が機微性を持つか否かによって、個人情報を一般的な個人情報と機微性を持つ個人情報とに区別することや一般的な個人情報に対しては情報の利用を可とするが、機微性を持つ個人情報に対しては保護することなどである。

このような措置は個人情報に対して絶対的に保護するか、利用するかに画一的に対処することを避けているのである。しかし、匿名化加工と同様、ビッグデータ時代にこの措置が機能を果たすかどうかは疑わしい。それは、ICT（Information and Communicaion Technology）の急速な進展につれて、一般的な個人情報から機微性を持つ個人情報を容易に推測することができる可能性があるからである。

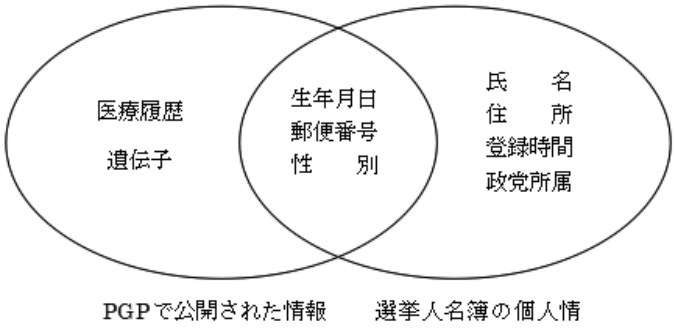
たとえば、電子商取引の運営者は消費者の購入履歴を分析することを通し、消費者の思想や興味といった人間の内面を知ることができる[42]。例えば、ある消費者が宗教に関するものをよく買うとすると、どんな宗教を信仰しているかが分かる。

また、一般的な個人情報と匿名化された機微性を持つ情報を照合すれば、特定の個人が識別される可能性がある。たとえば、2013 年に Latanya Sweeney ほかが「Identifying Participants in the Personal Genome Project by Name」について、次のような実験をしたことを発表した[43]。

Sweeney らは the Personal Genome Project（PGP）が公開した個人情報と選挙人名簿の中の個人情報を組み合わせた。PGP が公開した個人情報は 100,000 人のボランティアの

匿名化された生年月日、性別、郵便番号、医療履歴、遺伝子などである。選挙人名簿の個人情報は選挙人の基本的な情報である。結果は 84%～87%の高い確率で個人を特定することができた（図 5 を参照のこと）。

図 5　The Personal Genome Project が公開した個人情報と選挙人名簿の組み合わせ




出典：「Identifying Participants in the Personal Genome Project by Name」により、筆者作成。

以上のように、一般の個人情報から、機微性を持つ個人を容易に推測できる可能性がある。そのため、機微性を持つ個人情報をどのようにして保護するかは、中国も含めて世界共通の難題であろう。

**まとめと若干の提言**

現在、諸外国では個人情報保護法体系は大別してオムニバス方式、セグメント方式、折衷方式の 3 種類に分けられている。更に、個人情報保護のメカニズムは国の立法と業界の自主規制の 2 種類がある。しかし、国の立法だけに頼るのも業界の自主規制のみに頼るのも欠陥がある。したがって、個人情報の利用と保護を有効的に協調するため、国の立法と業界の自主規制とを同時に構築する必要があると思われる。

また、情報技術が急速に進展した現在、ビッグデータと人口知能の利用は政府・民間事業者・個人の情報分析力を増大させた。政府・民間事業者・個人は個人情報をビッグデータと人口知能によって特定の個人を識別できるようになった。また、匿名情報に対する復元が容易になっている。機微性を持つ個人情報も、何種類かの情報を組み合わせればできる。つまり、現在は、①いかなる情報も個人情報になる可能性がある。②匿名化加工した情報も特定の個人を識別できる。③機微性を持つ個人情報が侵害されることが容易になっている。したがって、諸外国の現行法の中で、規定された個人情報の範囲や匿名化加工情報や個人情報の分類などの措置を如何にするかはビッグデータ時代の今日、世界共通の課題である。

以上の諸外国の立法経験とその運用を参考にしつつ、今後中国における個人情報保護法の制定に向けて、いくつかの提言を述べておく。

### ⑴ 折衷方式の法体系

目下の中国では、オムニバス方式、セグメント方式、折衷方式のいずれをとるべきかについては、オムニバス方式が強く主張されている。例えば、北京師範大学教授の劉徳良はオムニバス方式で統一的な個人情報保護法を制定することを提言している[44]。また、中国社会科学院教授の周漢華は自説の中でどちらを選択するかを明言していないものの、2006 年に発表した個人情報保護大綱では、ドイツの連邦データ保護法のように公的部門と民間部門を包括的に規定するとしている。これにより、周漢華もオムニバス方式を主張していることが分かる。

しかし、3 種類（オムニバス方式、セグメント方式、折衷方式）の法体系の中で折衷方式が中国に適していると思われる。その理由は 2 つある。

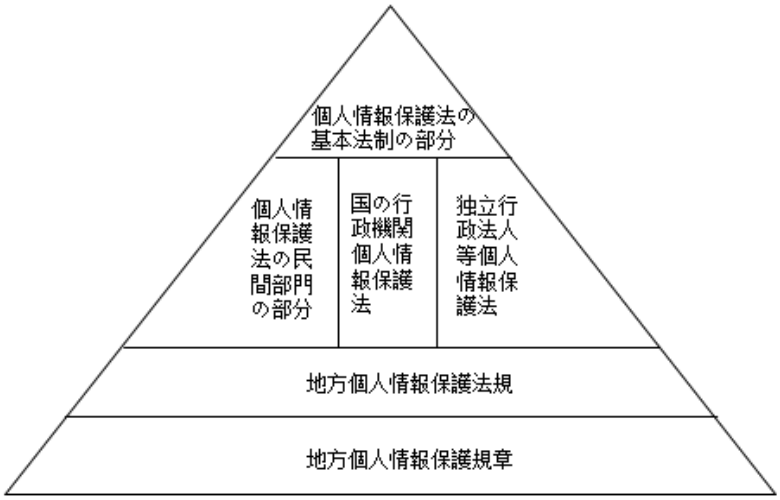
1 つは、公的部門と民間部門における個人情報保護の法律関係が異なっていることである。公的部門における個人情報保護は行政法律関係に属するが、民間部門は民事法律関係に属する。国民の公的部門と民間部門に対する要求は異なるため、オムニバス方式は中国にはふさわしくない。

2 つ目の理由は、中国には現在、個人情報保護に関する規定は各種の法律に散在している。この方式はセグメント方式に似ているが、その現状をみると、このような方式では、個人情報は十分に保護されておらず、個人情報の漏洩事件が頻発している。

そこで、中国は日本の個人情報保護法体系を参照し、中国の現状を鑑み、折衷方式の法体系を構築する必要がある。具体的には、中国の個人情報保護法体系は個人情報保護法、国の行政機関個人情報保護法、独立行政法人等個人情報保護法、地方個人情報保護法規、地方個人情報保護規章から構成する。

この内、「個人情報保護法」は 2 つの部門に分け、すなわち、基本法制と民間部門の個人情報保護規定である。基本法制は基本的な原則として、すべて個人情報保護領域に適用する。国の行政機関個人情報保護法、独立行政法人等個人情報保護法も国の行政機関の保有する個人情報と独立行政法人等の保有する個人情報領域に適用する。地方個人情報保護法規は個人情報保護法と国の行政機関個人情報保護法と独立行政法人等個人情報保護法に基づき、地方人民代表大会及び地方人民代表大会常務委員会が制定し、地方に適用する。地方個人情報保護規章は個人情報保護法、国の行政機関個人情報保護法、独立行政法人等個人情報保護法、地方個人情報保護法規の 4 法に基づき、地方政府が制定し、地方に適用する規定とする。これらの法段階は、以下の図 6 のようになる。

図 6　中国の個人情報保護法体系の法段階イメージ




出典：本文より筆者作成

### ⑵　立法と業界の自主規制の両立

国の立法と業界の自主規制とを同時に構築する鍵は、両者が衝突しないように相互に協働することである。中国は国の立法と業界の自主規制との両立のメカニズムを構築する時に、以下の 2 点に注意すべきであろう。

1 つは、国の立法である。国家ができるだけ早く一元的な個人情報保護法を構築しなければならない。そして、この法律には個人情報の取り扱いに関する規定だけでなく、業界に対して自主的に個人情報の管理の権限を与える。つまり、個人情報保護法に従って、業界は個人情報保護に対して具体的なルールを規定する権限があり、各組織はそのルールを遵守しなければならない。こうすれば、業界の自主規制には法的な根拠があることになり、それにより規定したルールには強制力がある。

2 つは、業界の自主規制である。これは組織が個人情報を取り扱うに際して、情報の保護のために設立する自粛システムである。このシステムは技術規制と制度規制の 2 つの規範を含む。具体的には、以下のようにする。

まず、技術規制は、組織の内部が制定し、保有した個人情報の漏洩を防止するため、採用すべき技術を求める規制である。これには必ずアンチウイルスやファイアウォールやウイルスの隔離、情報のスクランブラーなどの技術が規定されなければならない。

次の制度規制は主に職員の行為を規範化するために規定するもので、それは少なくとも以下の点を含むべきである。

①個人情報へのアクセスに関する職員の要件。

②職員の個人情報の処理の権限。

③個人情報の処理の記録。

④個人情報保護の責任。

### ⑶ 個人情報の範囲に関する「文脈的」規定

諸外国の現行法から見ると、多くの国は個人情報を識別型と定義づけている。例えば、日本、欧州諸国などである。中国のサイバーセキュリティ法も個人情報を識別型としている。それに鑑み、中国における個人情報の範囲を諸外国と一致させるため、中国の一元的な個人情報保護法は識別型の個人情報を維持するべきである。すなわち、個人情報とは単独であるいは他の情報と組み合わせて、特定の個人を識別できる情報とする。

しかし、この定義は現在、上手く適用できていない。情報技術の発展によって、昔は情報でなかったものも現在は、特定の個人を識別できる重要な情報となっている。そのため、文脈的完全性理論を参照し、個人情報の範囲の判断に適用する。

文脈的完全性理論によると、いかなる情報や事物の領域も情報の流れの影響を受けるようになっている[45]。たとえば、私たちが実行したことや発生した事件や実施した取引などは、その時点と場所だけでなく、政治、慣習、文化などの背景と関係がある。したがって、ある特定の行為が個人情報を侵害するかどうかは、多変数関数であると見なされる[46]。その変数は状況、背景、文脈、文脈における情報の性質、情報を受け取ったエージェントの役割、エージェントと情報主体との関係、情報をシェアする条件、情報を転換する条件などを含む。

同様に個人情報の判断もその背景、文脈、文脈における情報の性質などの変数を考える必要がある。変数に対して分析を通じ、情報やものが個人情報であるかどうかをはっきりさせる。こうした方法は、情報技術の進展による個人情報の範囲の変化に適用できる。

したがって、法律の中で、個人情報とは具体的な文脈により特定の個人を識別できる情報であり、あるいは文脈により差別、偏見などの不利益を生じさせる情報であることを規定すべきであろう。

### ⑷ 個人情報の利用に対する厳密な規定

冒頭で述べたように、現在、匿名化加工された情報も特定の個人を識別できる。いくつかの一般的な個人情報を組み合わせると、機微性を持つ個人情報も容易に得られる。そのため、匿名化加工情報や情報の分類により異なる基準を適用（一般的な個人情報よりも、機微性を持つ情報に対しては厳格に基準を適用する）することを強調してもは意味はない。

したがって、法律は個人情報の利用に対して厳格に規定すべきであり、個人情報の利用によって個人の利益を侵害してはならない。そのため、法律は個人情報の利用目的をはっきり規定するべきである。事業者はいくつかの一般的な個人情報を組み合わせ、機微性を持つ個人情報を得てはならない。また、匿名化加工した情報を復元してはならない。そして、刑法はそれに対応する刑罰を設けなければならない。

本稿では、諸外国の現行法における法体系、メカニズム、個人情報の範囲、匿名化加工情報、個人情報の分類などに考察を加えることにより、中国における個人情報保護法の制

定に向けていくつかの提言をまとめた。人々の意識や技術は急速に進展しているため、個人情報の保護は大変困難の問題である。今後中国の個人情報保護法整備の動向に注意しながらさらに掘り下げたいと思う。

［注］

1 EU データ保護指令（1995 年）の翻訳は堀部政男研究室仮訳を参照。

2 「全球 90 個国家和地区制定個人情報保護法律」、souhu 新聞、https://www.sohu.com/a/163633504_157267、取得年月日 2018 年 12 月 11 日。

3 https://baijiahao.baidu.com/s?id=1642453496709596738&wfr=spider&for=pc、取得年月日 2020 年 1 月 7 日。

4 塩入みほも「個人情報保護法制の体系と地方公共団体における個人情報保護の現状」、『駒澤大學法學部研究紀要』(76)、2018 年、pp.1-55。

5 宇賀克也『個人情報保護法の逐条解説（第 5 版)』、有斐閣、2016 年、p.27。

6 前掲注 5、p.64。

7 劉金瑞『個人信息与権利配置——個人信息自決権的反思和出路』、法律出版社、2017 年、pp.286-342。

8 Monika Kuschewsky, Data Protection& Privacy, Thomson Reuters, 2016, pp.1093-1117.

9 前掲注 5、p.27。

10 管理者とは、単独で又は他と共同して、個人情報の取り扱いの目的及び手段を決定する自然人、法人、公的機関、民間機関又はその他の団体をいう（2 条、堀部政男研究室訳文を参照）。

11 Joel R. Reidenberg, Restoring Americans' Privacy in Electronic Commerce, Berkeley Technology Law Journal, 1999, p.784.

12 斉愛民『拯救信息社会中的人格』、中国・北京大学出版会、2009 年、p.188。

13 https://www.acm.org/about－acm、取得年月日 2019 年 5 月 30 日。

14 https://dpmapc.com/about－us/、取得年月日 2019 年 5 月 30 日。

15 https://dpmapc.com/about－us/、取得年月日 2019 年 5 月 30 日。

16 蒋坡『国際信息政策法律比較』、法律出版社、2001 年、pp.449-450。

17 李媛『大数拠時代個人信息保護研究』、華中科技大学出版社、2019 年、p.50。

18 前掲注 17、p.50。。

19 Online Privacy Alliance Will Serve As Vanguard Of Industry Efforts To Protect Privacy In Cyberspace、http://www.privacyalliance.org/news/06221998/、取得年月日 2019 年 6 月 1 日。

20 前掲注 17、p.50。

21 http://www.privacyalliance.org/members/、取得年月日 2019 年 6 月 1 日。

22 Joel R. Reidenberg, Restoring Americans' Privacy in Electronic Commerce, Berkeley Technology Law Journal, 1999, p.777.

23 前掲注 22。

24 前掲注 22。

25 前掲注 22。

26 前掲注 22、p.781。

27 范姜真薇「政府公开与个人隐私之保护」、『法令月刊』(5)、2001 年、p.21。

28 長谷部恭男『人権の射程』、法律文化社、2010 年、p.139 を参照。

29 平松毅『個人情報保護——理論と運用』、有信堂、2009 年。

[30] 宇賀克也ほか「鼎談」、『行政法研究』、2016 年、pp.5-6。

[31] 前掲注 30、p.5。

[32] 前掲注 30、p.5。

[33] 王利明「隠私権的新発展」、『人大法律評論』(01)、2009 年、pp.18‐19。

[34] 劉徳良「譲網絡信息保護更具可操作性」、『中国紀検監察報』、2013 年 1 月 14 日第 004 版。

[35] Monika Kuschewsky, Data Protection & Privacy, Thomson Reuters, 2016, p.1094.

[36] 前掲注 35、p.959。

[37] 王利明「数据共享与個人信息保護」、『現代法学』(41)、2019 年、pp.56。

[38] 張新宝「従隠私到個人情報：利益再衡量的理論与制度安排」、『中国法学』(3)、2015 年、p.57。

[39] Latanya Sweeney, Weaving Technology and Policy Together to Maintain Confidentiality, Law, Medicine&Ethics, 1997, p.100.

[40] Monika Kuschewsky, Data Protection& Privacy, Thomson Reuters, 2016, p.1106.

[41] 前掲注 40、p.1102.

[42] 立山紘毅「個人情報保護法とネットワーク・学術研究：利用と保護のはざまで」、『個人情報保護法と人権：プライバシーと表現の自由をどう守るか』、明石書店、2002 年、p.39。

[43] Latanya Sweeney, Akua Abu, Julia Winn, Identifying Participants in the Personal Genome Project by Name. https://privacytools.seas.harvard.edu/files/privacytools/files/1021‐1.pdf、取得年月日 2019 年 6 月 1 日。

[44] 劉徳良「互連網対隠私保護制度的影響与対策」、『中国信息安全』、2011 年、p.38。

[45] Helen Nissenbaum, Privacy as Contextual Integrity, Washington Law Review, 2014, p.119.

[46] 前掲注 45、pp.137-138。

所属：山口大学大学院東アジア研究科
E-mail アドレス：shushochi@yahoo.co.jp