中国における個人情報保護に関する立法の動向（二・完）

葛　　虹

はじめに
1　中国における個人情報保護に関する現状
2　比較法的にみた個人情報保護の典型的法構造
3　中国研究者が起草した個人情報保護法案の全体構造
4　中国研究者が起草した個人情報保護法案の主な内容
（1）主管部門の地位、権限
（2）個人情報の取扱義務
（3）情報主体の権利（以上前号）
（4）個人情報の越境移動に関する制限
（5）法的責任
（6）センシティヴ情報
（7）自主規制
（8）適用除外規定
おわりに

4　中国研究者が起草した個人情報保護法案の主な内容

(4)　個人情報の越境移動に関する制限

Ⅰ　日本の場合

日本の「個人情報保護に関する法律」などには、個人情報の越境移動に関する規制は存在しない。

同様、「APEC プライバシー・フレームワーク」にもこの種の規制がない。その第 30 条は、次のように、情報の自由流通を阻害する結果をもたらすおそれがある措置について、特に慎重的な態度を示している。「プライバシー

保護措置の樹立又は再検討の一内容として、APEC プライバシー・フレームワーク及び現存の国内のプライバシー保護措置と調和するように、メンバー経済体は、情報流通に対する不要な障害を確認し、排除し、且つかかる障害の創設を回避するために、すべての合理的かつ適切な手段をとるものとする。（Consequently, as part of establishing or reviewing their privacy protections, Member Economie, consistent with the APEC Privacy Framework and any existing domestic privacy protections, should take all reasonable and appropriate steps to identify and remove unnecessary barriers to information flows and avoid the creation of any such barriers.）」

Ⅱ　中国研究者の提案の場合

「提案」の第 48 条によれば、主管部門は、一定の場合において、その他個人情報処理者による個人情報の中国国外への移動を制限することができる。

ここでいう「一定の場合」とは、次のものを指している。（ⅰ）国家の安全その他重大な国家利益に関わる場合；（ⅱ）中国政府の国際法上の義務の履行において特に必要とされる場合；（ⅲ）移動先の国家若しくは地域は、個人情報に対する充分な保護を行わない場合；（ⅳ）法律が規定するその他の場合。そして、主管部門は、（ⅲ）に該当する国家若しくは地域の認定作業を担当し、その認定に関わる具体的な基準、方法及び手続を定める権限がある。

「提案」の第 48 条は、「EU 個人データ保護指令」の第 25 条第 1 項の規定を手本に作られたものであると考えられる。前号 2（1）で説明したように、EU 諸国は「EU 個人データ保護指令」に従って、国内法において充分なレベルの保護措置を講じていない国への個人データの移転を禁止している。

具体的に言えば、カナダ、アルゼンチン、スイス、ニュージーランド、中

国香港など少数の国及び地域を、充分なレベルの保護措置を講じている国又は地域として、これらの国又は地域への個人データの移転を認めるが、中国本土を含む多くの国又は地域を、充分なレベルの保護措置を講じていない国又は地域として、これらの国又は地域への個人データの移転を禁止する。なお、アメリカとの関係においては、EU は、この問題での貿易摩擦の発生が EU 経済への悪影響を及ぼすことを回避するため、アメリカと「セーフ・ハーバー協定」を締結し、一定の条件の下で、EU からアメリカへの個人データの移転を容認する。

「EU 個人データ保護指令」の第 25 条第 1 項の規定に関して、以下のように評価は二つに割れている。一つは、この規定のおかげて EU の個人情報保護制度は、良い手本として、EU 諸国にとどまらず世界まで拡散し、日本を含む多くの国における個人情報保護法の整備を促した、との高い評価である。もう一つは、EU 諸国がこの規定を利用して、EU 以外の国の実情に合わない個人情報保護制度を他国に押し付け、対外貿易交渉上の有利な立場を図るためのカードに過ぎない、との低い評価である。

「提案」の研究チームはこの問題について複雑な思いを持っているようで、EU の個人情報保護制度全体の優れる点を肯定しながらも、後者の評価の考え方に賛同している(1)。研究者の間には、EU への対抗措置として、中国の個人情報の国外への移転を規制する規定を「提案」のなかに盛り込む必要があるとの意見がある。

そもそも中国が EU と比べて個人情報保護の後進国であるため、EU のように「充分なレベルの保護措置が講じられていない国又は地域への個人データの移転を禁止する」との規定を入れるだけではあまり意味がない。そこで、上記の第 48 条の iii の規定のほか、ⅰ、ii、iv の規定も「提案」のなかに入った。結局は、「提案」第 48 条の適用範囲は、「EU 個人データ保護指令」の第 25 条第 1 項よりも広汎になった。この問題については、「APEC プライバシー・フレームワーク」第 30 条に照らして、「情報流通に対する不要な障害」

に該当する可能性があるかどうかを検討する必要がある。

(5) 法的責任

Ⅰ　日本の場合

日本の裁判所は、従来から個人情報（センシティヴ情報、氏名・住所などの非センシティヴ情報を含む）の漏洩などに関する損害賠償責任を認めている(2)。そのため、「行政機関の保有する個人情報の保護に関する法律」と「個人情報保護に関する法律」の立法過程においては、民事責任に関する議論が殆どみられなかった。

刑事責任に関しては、「個人情報保護に関する法律」の条文を見る限り、違法な個人情報取扱行為自体に対する刑罰は存在しないが、個人情報取扱者が主務大臣に対する報告を怠ったり、虚偽の報告を行ったり、主務大臣の命令にかかる措置を講じなかったりした場合は、罰則（6ヶ月以下の懲役又は30万以下の罰金）が科せられる（56条、58条）。いわば「間接罰」の仕組みを採用している。

この間接罰については、抑制力が不十分であるとの指摘がある。特に医療、金融・信用、情報通信等個人情報保護の重要性・必要性が一層求められる特定分野においては、個人情報の適正な取扱いの厳格な実施を確保するために、義務違反行為に対し、直接に罰則を科すこと（直罰制）が必要であるとの意見がある(3)。

これに対し、間接罰の採用によって、法律上、直接に罰則を科すこと（直罰制）が完全にできなくなるわけではないという意見もある。同意見によれば、不正アクセス禁止法、刑法の窃盗罪の規定などに基づいて、個人情報の不正アクセス、個人情報データの不正持ち出し行為などに対し、直接に刑事責任を追及することができる(4)。

Ⅱ　中国研究者の提案の場合

「提案」第 5 章は「法的責任」の題名とし、政府機関その他個人情報処理者の個人情報の違法取扱行為、及び主管部門所属の職員のとく職行為などに関する行政責任、民事責任、刑事責任をそれぞれ規定する。本文は、民事責任と刑事責任を中心に説明する。

①　民事責任の明記

民事責任に関して、「提案」第 64 条は、「政府機関その他個人情報処理者は、その個人情報取扱行為が本法の規定に反し、情報主体の合法的な権利利益に損害を与えた場合は、法により賠償責任を負わなければならない」と規定する。

現行中国の成文法を見る限り、個人情報の漏洩、無断開示などによって生じた損害に関する民事責任の規定はもちろん、プライバシー侵害に関する民事責任の規定も存在しない。それにもかかわらず、1990 年以降、中国においてプライバシー意識の台頭とともに、個人情報の無断開示に対する損害賠償請求の民事訴訟はしばしば下級人民法院で提起された。これらの案件を対処するために、最高人民法院は「本人の同意を得ずに本人のプライバシーに関する記録を公開し、又は書面あるいは口頭で人のプライバシーを暴露し、名誉毀損のような結果を生じたとき、名誉権侵害に照らして処理しなければならない。」（1993 年 6 月 15 日付の最高人民法院審判委員会の「名誉権案件の審理についての若干の問題に関する解答」の第 7 の 3）という司法解釈(5)を公布した。

そして、下級人民法院は、上記の司法解釈を根拠に名誉権規定の準用によって、私生活に係わる事実が公表されない利益に法的保護を与えるべきであるという旨の判決をいくつか下した(6)。しかし、全体としては、中国の人民法院は、プライバシーに対する解釈が非常に厳格で、私生活に係わるセンシ

ティヴ情報（例えば、性的関係、エイズ感染情報など）が無断開示された場合は、プライバシー侵害として損害賠償請求を認めるが、その以外の殆どの場合は、法的根拠を欠けるという理由で損害賠償請求を認めない。

「提案」第64条は、まさに研究チームはこの問題を意識して、私生活に係わるセンシティヴ情報に限らず、それ以外の個人情報の不正取扱によって生じた損害に対する賠償請求も可能にするために設けたものである。

② 刑事責任に関する直罰制の採用

主管部門は、個人情報の違法取扱について、行政処分を行う権限があるが、刑事責任を追究する権限を持たない。その違法行為が犯罪構成要件に該当すると思料するときは、刑事捜査部門に通報することになる。

刑事責任に関しては、「提案」は主管部門の職員（65条）、政府機関の責任者及びその職員（67条、69条1項）、その他個人情報処理者及びその職員（68条、69条2項）に関する刑事責任について、いずれも「犯罪構成要件に該当するときは、法により刑事責任が追及される」と規定している。中国法においては、刑法典以外の法律法令で個別の罪名及びその具体的な刑罰内容を定めることができないとされているため、通常個別法で刑事責任を言及する際に必ず上記の文言のような規定（「刑法とのつなぎ規定」と呼ばれる）を入れる。具体的な罪名及び刑罰の適用については、「刑法」の規定を根拠とする。

従来の中国刑法には、個人情報保護に関する特別の規定がなかった。2009年2月28日の中国刑法の改正で、以下のとおり「刑法」第253の1条が設けられた。

「国家機関又は金融、電信、交通、教育、医療などの団体の職員は、国家の規定に反し、職場における職責履行又はサービス提供の過程において獲得した公民の個人情報を第三者へ売り出し、違法に提供し、情状が深刻である場合は、三年以下の有期懲役又は拘役(7)に処し、罰金を併科し、又は単科する。

窃取その他の方法で前項の情報を違法に獲得し、情状が深刻である場合は、前項の規定によって処罰される。

組織が前二項の犯罪構成要件に該当する場合は、組織を罰金に処する。その直接責任を負う担当者その他の直接責任者は、各該当する項の規定によって処罰される。」

「刑法」第 253 の 1 条は、現在多発している個人情報漏洩、個人名簿売買などの問題を対処するため、個人情報保護法案を先行して制定されたものである。これに対し、研究者は、次のような問題を指摘している。①国家機関又は金融、電信、交通、教育、医療以外の分野における個人情報漏洩、不正取引について、本条を適用できないので、その適用範囲が狭すぎること、②第三者への違法提供についての要件が明確ではないこと、③刑罰手段だけで個人情報保護の問題の根本的な解決にはならないこと、である。

いずれにしても、「刑法」第 253 の 1 条は、中国の個人情報保護の推進者に朗報で、今後の適用が注目される。

(6) センシティヴ情報

Ⅰ　日本の場合

センシティヴ情報に関しては、「EU 個人データ保護指令」8 条 1 項は次のように規定する。「加盟国は、人種上のまたは民族的な出自、政治的信条、宗教又は哲学上の信仰、組合の所属に関する情報、及び健康上の又は性生活に関する情報の処理を禁止する。(Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.)」

これと対照的に、「APEC プライバシー・フレームワーク」は、センシティヴ情報について特に規定していない。

日本の「個人情報保護に関する法律」「行政機関の保有する個人情報保護に関する法律」にも、センシティヴ情報を対象とする特別な規定が存在しない。立法過程においては、「EU 個人データ保護指令」８条１項のようにセンシティヴ情報に関する特別規定を盛り込むべきかどうかをめぐり、議論が行われていたが、最後になってそれをあきらめた。その理由は、センシティヴ情報を類型的に定義するのが困難であること、センシティヴ情報であっても取扱う必要がある場合があり、その取得を一律に禁止することが困難であることなどが挙げられた(8)。

とはいえ、センシティヴ情報に対する特別な配慮が見られる。例えば、日本の多くの地方公共団体が制定した個人情報保護条例にはセンシティブ情報の収集禁止等の規定がある。その代表例の一つとして、「神奈川県個人情報保護条例」(9)をあげることができる。同条例第６条はセンシティヴ情報の範囲について、思想、信条及び宗教に関する事項、人種、民族、犯罪歴その他の社会的差別の原因となる事項を列挙している。

また、「個人情報保護に関する法律」第８条に基づいて作られた主務大臣の指針、たとえば「電気通信事業における個人情報保護のガイドライン」、「金融分野における個人情報保護に関するガイドライン」にも、原則としてセンシティヴ情報の取得禁止などの規定がある。

そのほか、日本工業規格「JISQ15001 個人情報保護マネジメントシステム－要求事項(10)」にも、原則として明示的な本人の同意などがなければ、センシティヴ情報(11)の取得、利用などをしてはならないとの規定がある。

Ⅱ　中国研究者の提案の場合

「提案」には、センシティヴ情報に関する特別規定が存在しない。「研究報告」は、センシティヴ情報に関する定義及びその範囲の確定が困難であることを指摘するほか、以下の問題も提示している(12)。

一部の個人情報、例えば健康、性生活など個人のプライバシーに直接に関わる個人情報に対する保護の程度をその他の個人情報より高くする必要があることについては否定しない。しかし、「EU 個人データ保護指令」８条１項にいうセンシティヴ情報の範囲は、健康医療情報、性生活情報に止まらず、政治的権利、宗教信仰、結社の自由などに関わるものにも及ぶ。仮に中国の個人情報保護法において、政治的権利、宗教信仰、結社の自由に関する個人情報をセンシティヴ情報として扱うとすれば、現行憲法に抵触する可能性がある。なぜならば、中国憲法はその本文で政治的権利（34 条）、宗教信仰（36 条１項）、結社の自由（35 条）について規定する一方、他方でその序言で「中国共産党の指導の下でマルクス・レーニン主義、毛沢東思想、鄧小平理論および『三つの代表(13)』の重要思想に導かれ、人民民主専制を堅持し、社会主義の道を堅持し、改革開放を堅持する」と規定するからである。仮に政治的権利、宗教信仰、結社の自由に関するものをセンシティヴ情報から排除すれば、中国の人権保護が不十分であると国際社会から指摘される可能性がある。

結果としては、研究チームはセンシティヴ情報に敢えて言及しないほうが無難であると考え、それに関する規定を断念したのであろう。

（7）自主規制

Ⅰ　日本の場合

「個人情報保護に関する法律」は、第二節として「民間団体による個人情報の保護の推進」を規定し、認定個人情報保護団体の制度を設け、個人情報の保護の推進を図ろうとしている。

例えば、経済産業大臣および総務大臣により認定を受けた「日本情報処理開発協会」は、代表的な認定個人情報保護団体の一つである。その主な業務

は、①業務の対象となる事業者の個人情報の取扱に関する苦情の処理、②個人情報の適正な取扱の確保に寄与する事項についての対象事業者に対する情報の提供（個人情報保護指針の作成、公表、当該指針を遵守させるための指導など）、③プライバシーマーク制度(14)運用の担当などである。

Ⅱ　中国研究者の「提案」の場合

「提案」第３章には「業界の自主規制の仕組み」との一節があり、民間部門での業界自主規制の推進について、「国家は、その他個人情報処理者が自由意思による業界別の自主規制組織の創設を奨励し、政府の管理機能を次第に業界の自主規制組織に移転させるための条件を整備する」と書いてある（第 53 条）。

実は、中国の業界団体は、個人情報保護法案の成立に先行して、日本の認定個人情報保護団体制度を学び、業界の自主規制による個人情報保護の試行を既に展開している。例えば、日本企業を相手とするアウトソーシング・サービス企業が集中する大連には、業界自律組織――大連ソフト業界協会（大連軟件行業協会）がある。当該協会は、OECD 理事会のガイドラインと「日本工業規格 JISQ15001 個人情報保護マネジメントシステム要求事項」を参考にして、「大連ソフトウェア及び情報サービス業個人情報保護規範」（以下「規範」という）を策定し、2006 年に公表した。この「規範」に基づいて、大連ソフト業界協会は、日本の「プライバシーマーク制度」を手本とする PIPA（Personal information protection assessment の略称）マーク制度を創設した。PIPA マーク制度は、大連にある事業者を対象として「規範」に従い個人情報を適切に取り扱う者に PIPA マークを付与する個人情報保護評価制度である。大連ソフト業界協会所属の PIPA 事務室は PIPA マーク制度の具体的な運営を担当する。2008 年６月末まで認証した企業の数が 19 社に達している。さらに、2008 年６月 19 日に、日本情報処理開発協会と大連ソフト業界協会

は「プライバシーマーク制度と PIPA マーク制度の相互承認に関する協定書」に調印し、相互承認プログラムを開始した。これによって、プライバシーマークの認定を受けた日本事業者が申請により大連の PIPA 制度を利用し、日本企業を相手とするアウトソーシング・サービス企業で PIPA 認証された大連の事業者が申請により日本のプライバシーマーク制度を利用することができる。相互承認を受けた事業者は、両者のマークをあわせて作成された相互承認マークを付与される。

上記の「規範」、PIPA マーク制度及び日本との相互承認制度は、日本企業を相手とする大連のアウトソーシング・サービス企業の個人情報保護レベルを確保するための有効手段として機能している。

(8) 適用除外に関する規定

Ⅰ　日本の場合

「個人情報保護に関する法律」の立法過程において、個人情報の保護と憲法上の基本的人権としての表現の自由、学問の自由、信教の自由、政治活動の自由などとの衝突調整の問題が注目されていた。個人情報保護の名目で、民間部門の個人情報取扱の義務を厳しく設定することは、不当なマスメディア規制に連なるおそれがあるのではないかと指摘された。

この問題を解決するために、「個人情報の保護に関する法律」第 50 条は設けられた。つまり、マスメディアによる報道目的の個人情報取扱、著述業者による著述目的の個人情報取扱、大学などの研究機関による研究目的の個人情報取扱、宗教団体による宗教活動のための個人情報取扱及び政治団体による政治活動のための個人情報取扱については、個人情報取扱事業者の義務を規定する「個人情報の保護に関する法律」第 4 章を適用しないことになる。

学説上、憲法上保障された基本的人権が、第 50 条に列挙されたものに限

られず、その他の基本的人権（例えば、出版の自由など）も当然のことながら、適用除外の対象となりうるという意見もある(15)。

Ⅱ　中国研究者の提案の場合

「提案」には、日本の「個人情報の保護に関する法律」第50条のような規定が存在しない。研究チームは「提案」の作成過程で、この種の規定を入れるかどうか検討したようである。しかし、最終的には、以下の理由で、それを盛り込まないことにした。

（ア）中国国内には個人情報保護に関する経験が殆どない。しかも、中国ではマスメディアの報道の自由、宗教の自由に関して、外国と異なる特殊性をもち、そのままに模倣することができない(16)。

（イ）法律上明確な適用除外の規定又は適用制限の規定がない以上、その個人情報保護法の規定はすべて平等に適用されることになる。そうしないと、法適用を回避する脱法的行為が大量に発生しかねない。

ただし、「研究報告」は、将来の中国において、一定の個人情報保護の経験を積んだ後、特殊分野の個人情報保護に関する立法の可能性を以下のように示唆している。（ⅰ）「国務院情報資源主管部門が行政規則を作成し、一部の特殊分野に対する個人情報保護法の適用を除外し又は制限することができる」。（ⅱ）「別個独立の立法によって個人情報保護法より厳しい規制を含む別段の規定が可能であれば、その特別法が優先的に適用される」。

研究チームは、当面いかに迅速に個人情報保護の大枠を樹立させ、中国社会に定着させるかを重視しているようである。この目標を達成するために、立法技術を駆使し、現在の政治体制に抵触するおそれのある問題又は論争を呼びやすく短期間に解決不可能な問題をできる限り回避している。

筆者はこのような立法戦略の妥当性を疑問視している。そもそも、情報主体の権利利益の保護と、対立する権利利益との衝突は、避けられない問題で

ある。これらの問題をうまく解決しなければ、対立するその他の権利利益が犠牲となる。ついては、個人情報保護法の存在意義も低下することになろう。

おわりに

「提案」が作成された後の 2006 年 6 月に、中国社会科学院法学研究所が「個人情報保護及びその立法」と題する研究討論会を主催した。参加者のなかには中国、EU、アメリカ及びオーストラリアの個人情報保護法の専門家、中国の全国人民代表大会、国務院（最高行政機関）、人民銀行（中央銀行）などの関係者のほか、マイクロソフト、VISA、インテルなどの国際有力企業の関係者も含まれていた。参加者が各国の個人情報保護の経験を紹介すると同時に、中国における個人情報保護法案の制定作業自体について好意的な意見が多く寄せられた。しかし、企業の関係者たちは、将来法律が成立する場合、個人情報の取扱に対する過剰な規制によって、企業の健全な経営に支障が生じるかもしれないという懸念を表明した。

いずれにしても、この「提案」は、中国における個人情報保護立法の出発点である。今後は、この「提案」に基づいて新たな法案が作成されると考えられる。中国における個人情報保護に関する立法の動きについては、引き続き注目しなければならない。

（1）　「個人情報保護法（専門家提案）及び立法研究報告」の第 87 頁。

（2）　例えば、宇治市住民情報データ流出事件（1998 年）があげられる。宇治市役所から市乳幼児健診システムの開発の委託を受けた IT 会社の従業員が、市役所内で住民基本台帳データ（氏名、住所、性別、生年月日が記載された）約 21 万人分を MO（光磁気ディスク）に複写して持ち出し、名簿業者に販売した。名簿業者はこれらの個人情報をインターネットで売り出していた。そして、市議会議員と市民は、市に対し精神的苦痛を理由に損害賠償請求の民事訴訟を起こした。京都地裁は「開発会社の社員を指揮・監督して、データ管理に万全を尽くすことが要請されていた」と宇治市の使用

者責任（民法 715 条）を認め、一人あたり 1 万円の慰謝料の支払いを命じた（京都地判平成 13 年 2 月 23 日）。二審の大阪高裁（大阪高判平成 13 年 12 月 25 日）、上告審の最高裁（最判平成 14 年 7 月 11 日）もその判断を支持した（http:// www.law.co.jp / cases / uji2.htm）。

（3） 平野征人「『個人信用情報』にかかわる個別法の必要性」ジュリスト 1253 号 64 頁（2003 年）。

（4） 宇賀克也・藤原静雄・藤井昭夫「（鼎談）個人情報保護法の立法過程を振り返って」ジュリスト 1253 号 19 頁（2003 年）。

（5） 「司法解釈」とは、最高人民法院が、裁判における法令の具体的適用について、規範的な解釈を示すものを指す。中国における法の有権解釈の一種で、中国独自の制度である。中国では、判例の先例拘束力が認められないので、それに代わる（あるいはそれ以上の）役割を果たすのは、「司法解釈」である。

（6） 例えば「性転換手術の報道事件」があげられる。性同一性障害に悩んでいたＸは、性転換手術を受けたため、会社に解雇された。その後、彼が地元を離れ、ほかの町で仕事を見つけ新生活を始めた。ところが、新聞記者Ｙは彼に取材し、写真付きの実名記事を書いて発表した。結局、Ｘは再び社会的な偏見を受け、職を失い、その町を離れざるをえないことになった。そして、Ｘは、Ｙ及び新聞社を相手に、侵害停止、謝罪および慰謝料の支払いを求める訴えを提起した。蘭州市中級人民法院は、Ｘが性転換に関する事項の発表行為が、極めて不適当なもので、Ｘの静穏な生活を送る利益を侵害したと判断し、名誉権侵害としてＸの請求を認めた。最高人民法院中国応用法学研究所編『人民法院案例選（第 31 巻）』（人民法院出版社 2000 年）166 頁。

（7） 拘役は、中国の刑法に定められた犯罪者の人身の自由を短期間はく奪するという刑罰である。拘役の期間は 15 日以上 6 ヶ月以下とされる。その特徴は懲役より軽く、期間も短く、犯人を監獄の代わりに警察署の留置所に拘置することにある。

（8） 岡村久道『個人情報保護法』（商事法務、2004 年 11 月）55 頁。

（9） 「神奈川県個人情報保護条例」第 6 条は、「実施機関は次に掲げる事項に関する個人情報を取り扱ってはならない。ただし、法令若しくは条例（以下「法令等」という。）の規定に基づいて取り扱うとき、又はあらかじめ神奈川県個人情報保護審議会（以下「審議会」という。）の意見を聴いた上で正当な事務若しくは事業の実施のために必要があると認めて取り扱うときは、この限りでない。ｉ思想、信条及び宗教； ii 人種及び民族；iii犯罪歴； iv 社会的差別の原因となる社会的身分。」と規定する。

（10） 民間事業者が業務上取り扱う個人情報を安全で適切に管理するための標準として、1999 年に策定された日本工業規格の一つである。

（11） そのセンシティヴ情報の範囲には、ｉ思想、信条又は宗教に関する事項； ii 人種、民族、門地、本籍地（所在都道府県に関する情報を除く。）、身体・精神障害、犯罪歴

その他社会的差別の原因となる事項；iii勤労者の団結権、団体交渉その他団体行動の行為に関する事項； iv 集団示威行為への参加、請願権の行使その他の政治的権利の行使に関する事項、 v 保健医療又は性生活に関する事項が含まれる。

(12)　「個人情報保護法（専門家提案）及び立法研究報告」の第 79 頁。

(13)　「『三つの代表』の重要思想」とは、2000 年に当時の党の総書記だった江沢民が、市場経済化の一層の促進に対応するための党体制を確立するために提示したものである。共産党は、①中国の先進的社会生産力の発展の要求、②中国の先進的文化の前進の方向、③中国の最も広範な人民の根本的利益、の忠実な代表でなければならないというものである。これを受け、2002 年に、中国共産党の全国代表大会は、資本家、企業主の入党も可能にするように、党規約の入党に関する規定を改正した。

(14)　プライバシーマーク付与の対象者は、日本国内に活動拠点を持ち、JIS Q 15001 の要求を満たし、個人情報保護に関して適切な処置を行っていると判断される民間事業者である。一回の認定によるプライバシーマーク付与の有効期間は、2 年間となっている。更新の手続きによってさらに 2 年間の延長が可能である。2008 年 6 月までプライバシーマークの認定事業者数は 9547 社である。プライバシーマーク制度の目的は、①消費者の目に見えるプライバシーマークを示すことによって、個人情報の保護に関する消費者の意識の向上を図ること；②適切な個人情報の取扱いを推進することによって、消費者の個人情報の保護意識の高まりにこたえ、社会的な信用を得るためのインセンティブを事業者に与えること、である。

(15)　岡村久道『個人情報保護法』（商事法務、2004 年 11 月）238 頁。

(16)　「個人情報保護法（専門家提案）及び立法研究報告」の第 76 頁。