中国個人情報保護法の構想

汪　　淑　芳

（受付　2014 年 5 月 28 日）

1. は　じ　め　に

「人民網日本語版」（2012年 3 月16日）は，「中国初の『個人情報保護』基準が制定」という見出しで，「中国工業情報化省情報セキュリティ調整局の欧陽武副局長は15 日の『2012年度中国個人情報保護総会』で，中国初の『個人情報保護』国家基準である『情報セキュリティ技術：公共および商用サービス情報システムにおける個人情報保護指針』をすでに制定し，上級機関に提出したことを明らかにした。」という中国新聞社の記事を掲載した。さらに，「欧氏によると，指針は個人情報保護に関する概念を定義し，個人情報の収集，加工，移転，削除の各段階における情報主体，管理者，独立評価機関の役割と責任を明確にし，業界の個人情報保護の取り組みに準則を示している。」と報じている。

中国は，「電信及びインターネット利用者個人情報保護規定」を，2013年 9 月に施行した。同規定は，中国国内で電信サービス及びインターネット情報サービスを提供する際のインターネット利用者の個人情報の収集と使用について規定したものである。さらに，中国は，「消費者権益保護法」を大幅改正し，2014年 3 月15日より施行した。その新法は，経営者に対して，消費者個人情報の管理体制構築，安全確保，漏洩防止等を求めている。これらの規定の個人情報に関係する部分は，横断的な「個人情報保護法」に入れられるべき条項である。

これらに先だって，2013年 2 月 1 日から，いわゆる「個人情報保護基準」が実施されている。中国の標題は「信息安全技術公共及商用服務信息系統個人信息保護指南」（日本漢字使用）である。一定業種の国家機関等への適用は除外されている。なお，同基準の日本語訳全文を【参考】として添付した。

中国においては，2006年に，「中国個人情報保護法」が起草されたことがある。これは法律専門家による「法律提案」というもので，2014年 5 月現在いまだ立法化されていない。中国においても，個人情報をめぐる諸々の問題・課題の出現を背景に，いわゆる「個人情報保護法」制定の要望は小さくはない。

そこで，本小論では，中国個人情報保護法のあるべき法律構成について検討したい。その際，その種の法律の性格上，グローバル・国際的視点から考察するとともに，中国固有の政治的・経済的・文化的要素をも盛り込んだものとなろう。しかし，この検討の前に，「中国個人

情報保護基準」について追究する。同保護基準は，日本の「個人情報保護ガイドライン」に類似するものと考えている。

2.　個人情報保護基準

2.1　個人情報保護基準の概要

これまで，２本の基準が出されている。2012年12月28日の「全国人民会議常務委員会決定」(「2012年決定」という）と2011年12月の「産業情報技術省（MIIT）規則（2012年４月15日施行)」(「2011年規則」という）である。これらの基準の方が2013年基準よりも重要性が高い。しかしながら，2013年基準は，より広範囲の企業活動に適用され，そして，「データ海外移転」，「内密データ」，「データ主体のアクセス」，「修正権」というような重要項目にも及び，規定も詳細化している。これらのことは以前の基準には見られなかった。このような点は，個人データをめぐる「標準」であり，他の法律にも影響を与えることになろう[1]。

2.2　民間部門の範囲

個人情報保護基準は，「技術指針書」の体裁をなしており，「情報処理システムによる個人情報処理のすべてのまたは一部のステップを規律する」(A1)。「情報システム」は，「コンピュータ情報システム」として定義されるものの，「移動通信端末」や「ネットワーク」もこれに含まれる(A3.1)。コンピュータ情報システムは，必ずしも，インターネットに接続されていなくてもよい。

技術指針書は，「政府機関及び公的管理責任を行使するその他の機関を除くすべての組織と団体」に適用される(A1)。つまり，個人情報保護基準は，民間部門に広く適用されることになり，インターネット情報サービス事業者（IISP)，2011年規則と2012年決定の主体に限定されたものではない[2]。

「個人情報」とは，「情報システムで処理されるコンピュータデータのことで，ある自然人に関わるものであり，その自然人を識別するために，当該データのみがまたはその他の情報と組み合わせることによって利用される。」(3.2）このような定義は，最も多くの国々で使用される。個人情報は，「一般的個人情報」（中国語では，「個人一般信息」）と「内密的個人情報」（中国語では，「個人敏感信息」）に分けている(A3.8)。

「内密的個人情報」は，開示または修正された場合には情報主体に不利益をもたらすような情報である。諸分野に関わる内密的個人情報の内容は，情報主体の受けるべきサービスとサービス提供分野によって確定されるはずである。たとえば，内密的個人情報には，身分証明書番号，携帯電話番号，人種，政治的意見，宗教，生体的情報，指紋等が含まれる[3]。

2.3 当事者と責任：データ管理者，データ処理者等

「個人情報管理者」とは，「組織及び機関を意味し，個人情報処理の目的と方法の決定し，個人情報を実際に統制し，個人情報を処理するために情報ステムを利用する者。」(A3.4) 3条件すべてが満たされなければならない。そのため，データ処理者だけが「管理者」とはならない。管理者の責任は詳細に決められている(A4.1.3)。多くの計画と監視が個人情報に関して求められる。例えば，データ主体の利益を侵害するようなことがその個人情報に発生すれば，そのことをデータ主体に告知し，「重大事故」として関係部局へ連絡する，「個人情報の保護状況の評価のために第三者検証・評価者と協働する」。

「個人情報の『管理者』」と「個人情報の『個人的受理者』」とを区別する。情報システムから個人情報を取得し，個人情報の主体の意思に従って取得した個人情報を処理する。「受理者」が「データ処理者」として記述されているということは，保護基準中の受理者の役割の説明から明らかである。つまり，「個人情報の取得が他の当事者によって実施された情報処理目的に合致している場合には，個人情報受理者は，技術指針書及び実施契約に従って，個人情報を処理し，処理業務の完了後速やかに個人情報を削除しなければならない」(A4.1.4)。これがより明確になるのは，保護基準(3.5) が「個人情報主体の意思」よりもむしろ「個人情報管理者の指示」に言及している場合である。しかし，それにもかかわらず，重要なことは，その受領者または処理者はデータ主体が同意した目的に反して個人情報を処理してはならないということである[4]。

「検証・評価第三者機関」は，「専門的評価機関」として定義され，「個人情報管理者から独立しており」(A3.6)，「情報システムに関する検証と評価を実施する責務を負う」(A4.1.5)。それは，「個人情報の保護を評価，監督，指導するための個人的情報管理者に証明と基礎を提供する」。

2.4 八基礎原則

個人情報保護基準には「八基本原則」が置かれている。「個人情報管理者」は，この八原則に従わなければならない(A4.2)。

a) 明瞭目的原則－「確固した明瞭で合理的な目的の下で個人情報を取り扱うこと。利用範囲の拡張を禁止し，個人情報主体の同意なく個人情報の処理目的を変更することを禁止する。」

b) 必要最小限原則－情報処理の目的に必要な最小限の個人情報のみを取り扱うこと。処理目的が達成された時には，個人情報は最短期間で消去／廃棄されなければならない。

c) 公表原則－明瞭で，容易に理解可能で，適切な方法で，個人情報主体に対し，個人情報処理の目的，個人情報の収集・利用の範囲，個人情報保護措置およびその他の情報

を告知しなければならない。

d）本人同意原則－「個人情報処理について，情報主体から事前の同意を得なければならない。」（明示か黙示かは問わない）

e）情報質原則－「個人情報の秘密性，完全性及び可用性は最新のものでなければならない。」

f）安全性保証原則－安全保護措置は損害の可能性及び重大性と均衡をとらなければならない。」

g）誠実実行原則－法律の要求事項ならびにその他の要求事項を遵守するとともに，基準a）およびb）を実行すること。

h）責任明確原則－適切な措置の履行，遡及的調査のための処理の記録によって責任を明確にすること。

閲覧権や修正権に関する説明は存在しないが，このように，基本的なデータ保護原則を規定している。しかしながら，注目すべきことは，これらの原則がこの基準に現れるすべての義務を含んでいるわけではない。例えば，明瞭な同意が必要な場合，内密情報の特別な保護措置，海外移転に関する追加制限，侵害事案の報告義務，及びデータ主体の権利については説明がない[5]。

2.5　情報処理手順に関する手続

これらの基本原則とならんで，保護基準は，個人情報のいわば「一生涯」である四ステップ，すなわち，収集・処理・移転・消去で従うべき詳細な手続規定を置いている（A5）。これらの手続は，異なる当事者の責任（A4.1）にも八「基本原則」（A4.2）にも反映されていない。しかし，いくつかの点で進歩しており，旧基準にはなかったものが追加されている。

2.6　明示的・黙示的同意

このような「一生涯」基準は，「明示的同意」を求めることがしばしばある。それは，同意が個人情報主体によって明示的に行われ，その証拠が残されたということを意味する（A3.11）。しかしながら，「情報主体からの明示的な反対がない場合には，それは情報主体による同意したものと見なされるのである。」（つまり，「黙示の同意」である（A3.10））。しかし，これは，黙示の同意が含まれるという意味であると理解すべきではない。なぜなら，黙示的同意がすでになされたと思われないうちに，情報主体に「反対」の機会が与えられなければならないと考えるのが合理的であるからである。データ主体が反対しない限り，その同意が，もしくは，データ主体に明示的不同意への誘いが推測されるということをデータ主体に告知すべきであった（A4.2（d））。事実，それはオプアウト条項であるが，オプトアウトが

どんなものであるか詳細は知らされていない。

この区別は重要である。なぜなら，明示的同意は，内密的個人情報の収集（A5.2.3），未成年者からの情報の収集（A5.2.7），個人情報の開示（A5.3.4），データ移転（A5.4.5），及び内密的個人情報の保有（A5.2.2）との関係で求められるからである。

2.7　個人情報の収集

個人情報の収集前に，9項目がデータ主体に告知されなければならない（A5.2.2）。すなわち，a）収集の目的と内容，b）収集の方法手段，c）収集情報の利用範囲，d）個人情報の安全保護措置，e）情報管理者の氏名・住所，f）情報提供後の情報主体に関わる危険性，g）情報提供を拒否したときの情報主体の不利益，などの9つのメタデータである。データが「他の組織に移転した」場合の状況は明示的に告知されなければならない。目的，内容及び情報受領者の情報である。中国および海外では受領者間に区別はない。「別の組織」が社内の海外移転を含むかどうかは不明であるが，データ海外移転制限を受けることになる[6]。

他の収集基準（A5.2.）は，情報収集の不明瞭な，間接的な方法は禁止されると規定する。また，未成年者または障害者からの内密的個人情報の収集には，保護者の同意を必要とする。そして，同意があっても，最小限の収集に限定される。

2.8　情 報 処 理

処理基準（A5.3）は，再び，安全性及び明示的同意に関する要求事項，ならびに，可用性に関する諸義務を掲げている。最も重要なことは，処理基準が利用者の権利に言及していることである。

「2011年規制」及び「2012年決定」は，双方とも，個人情報の管理者の義務を規定している。しかし，双方とも，個人情報主体の権利については明確に規定していない。このたびの保護基準は，初めて，情報管理者に課せられた義務に中に閲覧権及び修正権が含まれるものと考えられる[7]。つまり，個人情報保護基準は，データ主体が「本人の個人情報の閲覧を申し出た時」（A5.3.7）の情報管理者の対応方法を規定しており，また，「個人情報主体が本人の情報に不備を発見し，その修正を申し出た時には，情報管理者は修正または補足に応じなければならないと規定する（A5.3.6）。おそらくこれらの権利はこのたびの保護基準に照らして，既存の法律の中にも準用されるものであろう[8]。

情報管理者に対する苦情や調査の申し出でというデータ主体の権利は，「個人情報主体」の責任という項目で繰り返されている（A4.1.2）。さらに，「個人情報保護の担当部局である管理部局への苦情申し出で」という選択肢も追加されている。

2.9　情報移転－開示厳格化とデータ移転制限

これまでの中国のデータ保護指令には個人データの海外移転に関する制限はなかった。しかし，保護基準（5.4.5）は明確に述べている。すなわち，「個人情報主体の明確な同意が存在しない場合，明文の法律的及び規則的許可が存在しない場合，監督官庁の同意が存在しない場合，個人情報の管理者は，当該個人情報を海外の個人情報受領者に移転してはならない。海外に居住する個人および海外に登録する組織及び機関に対しても同様である。」

これは極めて強い制限である。データ主体からの明確な同意がなければ，個人データを海外に移転することはできない。しかも，海外移転を許容する法律と監督官庁の同意が不可欠である。「一般的」個人情報（非－内密情報）に関して，通知と黙示の同意で十分であるが，これはデータの移転には妥当しない。明示的同意が必須である。会社内部での移転にも例外はない。拘束企業規則に関する条項もない。また，以前の収集データとの関係での「承継」もない。中国に住所を置く企業によるクラウドコンピューティングサービスの利用に関して興味深い問題も起こっている。クラウドサービス事業者のサーバは「海外」にあるといっていいだろう。しかし，海外の受領者への移転はあり得るのか[9]。

この保護基準は明らかに自主的な指針であるけれども，中国からの個人データの海外への移転は，データ主体の明示的な同意がなければ，高いリスクを含んだ事業なると思われる。その上，移転に関する基準（A5.4）は，同意と安全性の要求事項を繰り返し，そして個人情報の移転前に，当該情報の受領者の責任を明確にしなければならないということを繰り返している。

2.10　削　　除

保護基準（A5.5）は，「正当な理由」による個人情報の適切な時期の削除の権利を，追加的利用者の権利としている。そして，収集目的が完了した場合の削除の義務，もしくは，継続的処理が必要な場合の識別不能化，破産や経営不能の場合の削除手順を定めている。

3.　将来の第三の方針

総じて，この保護基準は，最も包括的であり，2011年規則や2012年決定にくらべて良く組織化されている。

中国の軍事防衛の「第三方針」または「第三前線」と同様に，中国のデータ保護のこのような第三方針は幾分神秘的である。これは，一連の自主的基準として影の存在であり続けるのか。しかし，他の法律や標準，そしてそれらの適用に影響を与えることもあるのだろうか。あるいは，極めて熟慮された構造と考えられた詳細が与えられ，そして一端強行性が与えら

れたならば，それは中国の将来のデータ保護法のひとつのモデルになるのではないか。いずれにしても，中国は，大きくかけ離れた分野別のデータプライバシー法（幾分アメリカに似ているが）のパッチワーク的なものから，少なくとも民間部門全体に横断的に適用されるような同じ原理を持った一貫的構造へと向かっている。中国全土を覆うような法律が現れるにはまだ時間を要する。しかし，それが現実になるときは，この「第三の方針」の保護基準が大きな影響を与えることになることが理解できる。「重慶に学べ」というスローガンはもはや人々には覚えられてはいないが，この保護基準こそ影響を与え続ける「第三の方針」である［10］。

4. 中国個人情報保護法の構成

4.1 法律構成の概要

中国個人情報保護法は，法律の目的，適用範囲，定義，情報プライバシー保護原則，例外事項，法律違反と救済，個人情報保護監査人の創設，同監査人の任命・解任・権限などの項目から構成される［11］。

4.2 法律の構成

4.2.1 法律の目的

「この法律は，法律の名において，中国人民の情報プライバシーの保護を認めるものである」。

4.2.2 適用範囲

「1. 法律は明晰で一貫性がなければならない。
2. 立法者の目的は，中国における個人情報の保護である。
3. 法律は公的部門ならびに民間部門に適用される。両部門の間で法律適用の差別はなく，かつ中国全土で統一的に適用される。
4. 法律は記録された個人情報に適用されるものとする。
5. 法律は中国において特定のデータ，組織および部門に適用されるものとする。
6. 法律は，プライバシー法および個人情報保護法の国際的潮流と矛盾しないものとする。」

4.2.3 定義

「1. 法律は最初に「個人情報」を定義する。EU 指令（95/46/EC）（個人データ処理をめぐる個人の保護と個人データの自由な移転に関する）に含まれる定義を採用すべきと考える。
2. この法律において，事業は個人情報の処理であり，規律対象者は個人情報を処理する者である。法律は，「情報利用者」および「情報主体」を各々定義すべきである。

3. この法律において注意深く定義されるべき用語は「データ」である。法律は，記録された個人情報を適切に覆うことを保証すべきである。」

4.2.4　情報プライバシー保護原則

情報プライバシー保護原則は，個人情報の収集，取扱，利用および開示に関する基本的規則である。それゆえ，情報プライバシー保護原則は，中国において個人情報を保有し処理するすべての組織と個人に課せられる基準である。

「1. 情報プライバシー保護原則は，この法律の中核をなすものである。したがって，法律の実効性は，これらの原則の構成にかかっている。

2. 情報プライバシー保護原則は，長期的展望に基づいて提示されるべきである。

3. 情報プライバシー保護原則は，中国おける一般的適用のための最低限の基準となるべきである。

4. 特定の事例に関する例外は他のところで取り扱われるものとする。

5. 情報プライバシー保護原則の基準は，「プライバシー保護と個人データの国際流通に関する OECD 指針」および「個人データ処理をめぐる個人の保護と個人データの自由な移転に関する EU 指令（95/46/EC）」で要請された基準を満たすものとする。

6. 中国における情報プライバシー保護原則は，つぎの事項を含むものとする。

（a）個人情報収集について，その方法と目的

（b）データの質

（c）個人情報を含むデータの安全性

（d）個人情報を含むデータの貯蔵

（e）個人情報を含むデータの公開性

（f）個人情報を含むデータの閲覧

（g）個人情報を含むデータの修正

（h）個人情報の正確性監査事項

（i）個人情報を含むデータの利用と処分（廃棄）」

4.2.5　例外事項

EU 指令（95/46/EC）に基づいて，法律は，情報プライバシー保護原則草案の要求事項から除外された一定の情報処理例外事項を認めるものとする。

「1. 想定される例外事項は最低限にするべきである。プライバシー保護が可能な限り広範囲に適用されることを保証することが重要であると考えるからである。

2. 想定される例外は，法律の一つの部所にまとめられるべきである。それは，例外条項の閲覧をより容易にするという配慮からである。

3. 想定される例外規定は過度に複雑であってはならない。」

4.2.6　法律違反と救済

立法は，情報利用者が保有する個人情報の主体に対して，情報の不正確および無権限アクセスによって損害を被った場合に，その損害の賠償を当該情報利用者に請求する権利を認めるべきである。

4.2.7　個人情報保護監査人の創設

法律は，個人情報保護監査人を創設すべきである。

4.2.8　個人情報保護監査人の任命と解任

監査人は中国政府によって任命されるが，解任は NPC の承諾のみに基づいて行われる。

4.2.9　監査人の職務と権限

「1. 監査人の職務は以下の通りである。

（a）情報プライバシー保護原則の推進と実施。

（b）研究と調査（中国において悪影響を最小化するために，法律の実施状況，情報処理およびコンピュータ技術の発展を研究・調査する。）

（c）個人情報を取り扱う機関のプライバシー保護原則の遵守を監視する。

（d）すべての合理的領域における中国情報プライバシー立法政策とプライバシーと他の競合する利益との間での消極的対立の縮小化の保証。

（e）プライバシーに関する中国の国際的義務と関連する国際的指針の検討。

（f）中国 NPC，中国政府に対する助言。

2. 監査人の権限は以下の通りである。

（a）法律の執行を監視する権限。全体的監視権限は，技術的発展と教育への助言，調査，監督に関わる。

（b）法律が遵守されるているかどうかを監視する権限およびプライバシー問題を調査する権限のような法律遵守の監視および推進の権限。

（c）監査人は，また，苦情処理の権限。苦情の調査権限，苦情申立人に救済を与えるかどうかを決定する権限。

（d）公式見解を提示する権限。

（e）全国人民会議への特別報告の権限。

（f）決定事項の実施とレビューの権限。

4.2.10　専門家支援条項

専門家から支援を受けられるようにする権限を，情報プライバシー保護委員会に附与する条項を法律の中に規定するものである。その支援は，あくまでも，個人情報の保護を目的とするものである。ここでいう「専門家」とは，情報処理技術，インターネットならびにシステム等に関する専門的知識及び専門的技術を修得した者を意味する。

4.2.11　職員

1. 情報プライバシー保護局の職員は，個人情報の保護の実現に熱意と専門知識有する者がなる。

2. 職員は，中国情報プライバシー保護局によって採用され，同局の管理と命令の下で職務を遂行するものとする。

5. おわりに

個人情報保護は，先進的情報技術によってもたらされた，「古くて新しい」人間個人に関わる問題である。技術の導入は国を選ぶことはない。しかし，その技術導入によってもたらされた問題の解決には，それに相当の文化的・政治的・社会的体制が必要であると考える。個人情報保護法，データ保護法，あるいはプライバシー法を持つ諸国においても，その立法化までには約10年間から30年間の年月を要した。この問題は普遍的でありながら，その解決にはそれぞれの国のさまざまな条件を考慮しなければならない。

「中国個人情報保護基準」の観点から「中国個人情報保護法構成」を評価すべきであったが，両者の時間的乖離が大きいこともあり，それは，今後の研究課題としたい。

引用・参照文献

［1］ G. Greenleaf/G.Y. Tian, China expands data protection through 2013 Guidelines: A ‘third line’ for Personal Information Protection, with a translation of the Guidelines, *Privacy Law & Business International Report*, Issue 122, 1, 4–6, April 2013, p. 2.
［2］ Ibid.
［3］ Ibid., p. 3.
［4］ Ibid.
［5］ Ibid., p. 4.
［6］ Ibid., p. 5.
［7］ Ibid.
［8］ Ibid.
［9］ Ibid.
［10］ Ibid., p. 6.
［11］ Hao Wang, Protecting Privacy in China: A Research on China's Privacy Standards and the Possibility of Establishing the Right to Privacy and the Information Privacy Protection Legislation in Modern China, Springer 2011, pp. 165ff.

【参　　考】

「中国個人情報保護基準」（同保護基準は，G. Greenleaf らによる英語の the Guidelines を日本語訳したものである。）

情報セキュリティ技術――公的・商用業務情報システムにおける個人情報保護基準――

情報技術の広範な利用とインターネットの普及にともなって，個人情報が社会経済活動において顕著な役割を演じている。同時に，個人情報の濫用事案も現れ，社会秩序および個人の利益を侵害する事態になっている。

かかる状況を顧みて，本技術指針書は個人情報の適切な利用を推進するために作成されたものである。個人情報を処理するための情報システム利用の指針・指導に資することになれば幸いである。

1　保護基準の範囲

本技術指針書は，情報システムによる個人情報の処理プロセスのすべてまたは一部を規律する。本指針書は，情報システムにおける個人情報処理の各ステージにおける個人情報保護に関する指針を規定する。

本技術指針書は，情報システムにおける個人情報の保護において任務を遂行するために，電気通信，金融，医療等の分野における公益施設のように，政府機関及び公的管理責任を行使するその他の機関を除くすべての組織と団体に適用される。

2　規範的根拠

以下の文書は本書技術指針書の適用に不可欠のものである。改訂版については，最新版が本書に適用される。未改訂版については，最終版（全ての改訂を含む）が本書に適用される。

GB/T 20269-2006 Information Security technology Information system security management requirements

GB/Z 20986-2007 Information Security technology Guideline on classification nd grading of information security incident

3　用語と定義

本指針書における用語と定義は「GB/T 20269-2006」及び「GB/Z 20986-2007」の中で定義され，以下の定義は本書技術指針書に適用される。

3.1　情報システム

コンピュータ情報システムとは，コンピュータ（携帯型通信端末を含む）及び外部補助装置と設備（ネットワークを含む）から構成され，情報の収集・処理・貯蔵・移動・検索を実行することができ，一定の処理目的を達成するものである。

3.2　個人情報

「個人情報」とは，情報システムで処理されるコンピュータデータのことで，ある自然人に

関わるものであり，その自然人を識別するために，当該データのみがまたはその他の情報と組み合わせることによって利用される。個人情報は，「内密的個人情報」（中国語では，「個人敏感信息」）と「一般的個人情報」（中国語では，「個人一般信息」）とに分けられる。

3.3　個人情報の主体

「個人情報の主体」とは，個人情報によって指し示される自然人をいう。

3.4　個人情報の管理者

「個人情報管理者」とは，個人情報処理の目的と方法の決定し，個人情報を実際に統制し，個人情報を処理するために情報ステムを利用する組織及び機関を意味する。

3.5　個人情報の受理者

「個人情報の受理者」とは，情報システムから個人情報を受理し，個人情報主体の要求や意思に従って受理した個人情報を取り扱いまたは処理する個人，組織及び機関を意味する。

3.6　第三者的検証及び評価機関

「第三者的検証・評価機関」とは，個人情報管理者から独立した専門的評価機関を意味する。

3.7　内密的個人情報

「内密的個人情報」とは，開示または修正された場合には情報主体に不利益をもたらすような情報である。諸分野に関わる内密的個人情報の内容は，情報主体の受けるべきサービスとサービス提供分野によって確定されるはずである。たとえば，内密的個人情報には，身分証明書番号，携帯電話番号，人種，政治的意見，宗教，生体的情報，指紋等が含まれる。

3.8　一般的個人情報

「一般的個人情報」とは，内密的個人情報以外のすべての個人情報を意味する。

3.9　個人情報の処理

「個人情報処理」とは，収集，処理，移転及び消去を含む個人情報を取り扱う行為を意味する。

3.10　黙示の同意

情報主体から明示的な反対の意思表示がなければ，情報主体による同意があったものと見做す。

3.11　明示的同意

「明示的同意」とは，情報主体によって明示的に示された同意で，その証拠が残されていなければならない。

4　個人情報保護の概要

4.1　役割と責任

4.1.1　概要

個人情報処理システムにおける個人情報保護の役割は，個人情報の主体，個人情報の管理，個人情報の受理者，及び独立の評価機関を含む。その責任については，以下の［4.1.2］から［4.1.5］を参照せよ。

4.1.2　個人情報主体

個人情報の提供前に，次のことが情報主体に告知されなければならない；個人情報管理者の当該個人情報の収集と利用の目的，情報主体の要求に従った個人情報の提供であること；個人情報の暴露，消失，改変が明らかになった場合に個人情報管理者に対して苦情の申立ができること。さもなければ，個人情報保護担当の行政部局に苦情申立ができる。

4.1.3　個人情報管理者

個人情報管理者は，国の法律，規則及び本技術指針書に従って情報システムにおける個人情報処理プロセスを計画・設計・確立しなければならない。さらに，個人情報管理システム／ルールを開発し，個人情報管理に関わる責任を遂行すること；当該組織内での個人情報保護担当部局／担当者を任命し，情報主体からの苦情・要求を受理すること；個人情報保護に関する教育・訓練の計画／プログラムを開発し実施案を作成すること；個人情報保護のための内部統制機構を確立し，当該情報システムの個人情報安全性レベルに関する評価を実施し，当該情報システム，当該保護システムおよび実施状況の個人情報の安全性レベルの評価を自己検証するか独立の評価機関に委託評価させること。

情報システムによる個人情報処理プロセスにおける危険性を掌握し管理すること，および，露見／暴露，喪失，損傷，改変，濫用等の個人情報処理上の想定される事故対応計画を作成すること。個人情報の漏えい，喪失，損傷，改変および濫用が発見された場合には，当該事案の拡大を防ぐために適切な措置を講ずるとともに，個人情報主体に速やかに通知しなければならない。重大な事案が発生した場合には，個人情報保護担当部局に通報しなければならない。

個人情報管理部局による個人情報保護措置に関する査察，監督および指導を受け入れること。

情報システムの個人情報保護措置の評価のために，第三者的検証評価機関と積極的に協力しなければならない。

4.1.4　個人情報受理者

個人情報の取得が第三者による情報処理目的のためである場合には，個人情報受理者は技術指針書ならびに契約条項に従って，個人情報を処理し，処理業務終了後には直ちに削除さ

れなければならない。

4.2　基本原則

個人情報管理者は，個人情報処理のために情報システムを利用する際には以下の基本原則に従わなければならない。

a）明瞭目的原則――確固した明瞭で合理的な目的の下で個人情報を取り扱うこと。利用範囲の拡張を禁止し，個人情報主体の同意なく個人情報の処理目的を変更することを禁止する。

b）必要最小限原則――情報処理の目的に必要な最小限の個人情報のみを取り扱うこと。処理目的が達成された時には，個人情報は最短期間で消去／廃棄されなければならない。

c）公表原則――明瞭で，容易に理解可能で，適切な方法で，個人情報主体に対し，個人情報処理の目的，個人情報の収集・利用の範囲，個人情報保護措置およびその他の情報を告知しなければならない。

d）本人同意原則――個人情報処理について，情報主体から事前の同意を得なければならない。

e）情報質原則――個人情報の秘密性，完全性及び可用性は最新のものでなければならない。

f）安全性保証原則――安全保護措置は損害の可能性及び重大性と均衡をとらなければならない。

g）誠実実行原則――法律の要求事項ならびにその他の要求事項を遵守するとともに，基準 a）および b）を実行すること。

h）責任明確原則――適切な措置の履行，遡及的調査のための処理の記録によって責任を明確にすること。

5　個人情報保護

5.1　概要

情報システムにおける個人情報処理のプロセスは，収集，処理，移転及び削という 4 つの主要なステップに分かれる。個人情報保護はその 4 つのステップを通して考慮されなければならない。

a）収集とは，個人情報を受理し記録することである。

b）処理とは，（データ）の入力，貯蔵，修正，参照，検索，保護に関する操作である。

c）移転とは，公的な開示，特定組織への開示，業務委託のための外部情報システムへの個人情報の複製のように，個人情報の受理者へ個人情報を提供する行為を意味する。

d） 削除／消去とは，当該個人情報が情報システムで利用できない状態をいう。

5.2 個人情報の収集

5.2.1 目的の特定性・明瞭性・合法性

個人情報収集の目的は特定され，明瞭でかつ合法的でなければならない。

5.2.2 個人情報収集の前に，情報種主体に対し容易に認識できる方法で，以下の事項について告知されなければならない；

a） 個人情報の処理目的；

b） 個人情報収集の方法と手段，収集さるべき特定内容，および，保存の時期と期間；

c） 収集個人情報の利用範囲，ならびに，他の組織と機関に開示または提供される個人情報の範囲；

d） 個人情報の安全保護措置；

e） 個人情報管理者の氏名・住所，連絡先情報等；

f） 情報提供後の情報主体に関わる危険性；

g） 情報提供を拒否したときの情報主体の不利益；

h） 情報主体が苦情を申し出る方法；

i） 個人情報が別の組織に移転または委託される場合には，情報主体には，以下の事項が知らされなければならない：移転または委託の目的；移転または委託される個人情報の特定の内容と利用の範囲；委託個人情報の受理者の氏名，住所および連絡方法。

5.2.3 個人情報の処理に先立って，個人情報主体から，黙示または明示の同意を得なければならない。「一般的」個人情報収集の場合には黙示の同意でもよいものとする。個人情報主体が明示的に拒否した場合には，その収集が中止されるかまたは個人情報は削除または消去されなければならない；「内密的」個人情報が収集される場合には，個人情報主体は明確にその同意を与えなければならない。

5.2.4 告知された目的を達成するのに十分な最小限の情報のみを収集しなければならない。

5.2.5 個人情報主体から個人情報を収集する場合には，告知または公知された直接的に収集する手段と方法を採用しなければならない。個人情報を収集する場合には，不明瞭な方法でまたは間接的な方法で収集してはならない。

5.2.6 個人情報を継続的に収集する場合にはその理由を明示しなければならない。また，個人情報収集の目的の変更等を情報主体に説明しなければならない。

5.2.7 16歳以下の未成年者および限定的民事責任者から直接的に内密的個人情報を収集してはならない。その必要性がある場合には，法的補佐人の明示的同意を得なければならない。

5.3　処理段階

5.3.1　収集段階における個人情報の利用についての公知または知らされた目的を侵害してはならないし，個人情報の公知または告知された範囲を超えてはならない。

5.3.2　公知または告知された方法と手段を採用すること。

5.3.3　個人情報の処理においては，個人情報の処理とは無関係の個人，組織，および機によって個人情報が収集されることはない。

5.3.4　処理された個人情報は個人情報主体の明示的な同意なくしていかなる個人，組織および機関にも提供してはならない。

5.3.5　個人情報の処理において，個人情報が完璧で，利用可能で，かつ最新の状態に維持できるように，情報システムは継続的にかつ安定的に運営されていることを保証しなければならない。

5.3.6　個人情報主体が本人の情報に不備を発見し，その修正を申し出た時には，個人情報管理者は個人情報主体の要求に応じて検査・検証し，個人情報の修正または補足に応じなければならない。

5.3.7　個人情報の状態に関する詳細な記録を保持しなければならない。個人情報主体が本人の個人情報の検証を要求した場合には，個人情報管理者はそれが本人の個人情報であるかどうか，個人情報処理の状態およびその他の事項を誠実にかつ無料で知らせなければならない。ただし，その費用または要求の頻度が合理的範囲を超えていればその限りではない。

5.4　移転段階

5.4.1　個人情報の移転は，収集段階での告知された移転目的に違反してはならないし，公知のまたは告知の移転範囲を超えてはならない。

5.4.2　個人情報の他の組織または機関への移転に先立って，当該組織または機関が本技術指針書の要求事項を満たしているかどうかを評価し，個人情報保護における当該組織または機関の責任を明確にしなければならない。

5.4.3　移転プロセスにおいて個人情報が個人情報受理者以外のいかなる個人，組織，機関にも提供されないことを保証しなければならない。

5.4.4　移転の前後を通して，個人情報の完全性，可用性および最新性が保証されなければならない。

5.4.5　個人情報主体の明確な同意が存在しない場合，明文の法律的及び規則的許可が存在しない場合，監督官庁の同意が存在しない場合，個人情報管理者は，当該個人情報を海外の個人情報受理者に移転してはならない。海外に居住する個人および海外に登録する組織

及び機関に対しても同様である。

5.5　削除／消去段階

5.5.1　個人情報主体が正当な理由により個人情報の削除または消去を求めた場合には，当該個人情報は速やかに削除または消去されなければならない。

5.5.2　収集段階で告知された個人情報の利用目的が達成された場合には，当該個人情報は削除または消去されなければならない；継続的処理が必要な場合には，当該個人情報の個人を識別できる内容を削除しなければならない；内密的個人情報の継続的処理が必要な場合には，当該個人情報主体の明示的な同意を得なければならない。

5.5.3　収集段階で告知された個人情報の保有期間が経過したならば，当該個人情報は速やかに削除されなければならない；保有期間が明確に定められていた場合には，その条件が実行されなければならない。

5.5.4　個人情報管理者が倒産または破産した場合で，個人情報の処理目的の遂行が困難な場合には個人情報を削除しなければならない。当該個人情報の削除または消去が法律執行機関による調査および証拠収集に影響を及ぼす場合には，当該個人情報に適切な保存・保全措置を施さなければならない。