「個人情報保護法」マネジメントシステム構築の試み

北　原　宗　律

（受付　2010 年 11 月 1 日）

要　　旨

個人情報処理システムを設置している組織にとって，個人情報処理をめぐる規制が多様化・複雑化している。その負担を軽減し，個人情報保護規制のコンプライアンス文化を浸透させるため，同規制の標準化として，「個人情報保護法」マネジメントシステムの構築を試みる。本小論の目的は，その構築の可能性を展望するために，現行の個人情報保護マネジメントシステムの箇条と個人情報保護法の条項との対応関係を分析することにある。

キーワード　JISQ15001:2006，個人情報保護法，マネジメントシステム，個人情報保護方針，PDCA サイクル，データ監査，ポリシーライフサイクル，リスクマネジメントシステム，個人情報保護ガイドライン，クラウドコンピューティング，プライバシー，個人情報データ監査

1. は　じ　め　に

日本工業規格の「JIS Q 15001:2006」は，「個人情報保護マネジメントシステム」である。個人情報を「取り扱う」あらゆる規模の，あらゆる業種の事業者に適用される個人情報の管理手法のひとつといわれる。民間の事業者が自主的にこの個人情報保護マネジメントシステムを構築・運用することで，組織内での個人情報保護措置の改善を目指すものである。しかし，この種のマネジメントシステムはあくまでも内部統制の一手段にすぎない。民間事業者，とりわけ，個人情報取扱事業者と位置づけられるものには，さらに，個人情報保護法によって，個人情報の取扱に関する義務が課せられる。ならびに，同法の全般にわたるコンプライアンスが要請されるのは当然のことである。

それならば，個人情報保護法のコンプライアンスを前提にしたマネジメントシステムを構築・運用する方が，事業者にとって簡略・明瞭ではないかと思われる。本小論の目的はそこにあり，かかる意図の下に検討されたのが，「『個人情報保護法』マネジメントシステム」である。

2006年 8 月に，日本情報処理開発協会プライバシーマーク推進センターが「JISQ15001：2006をベースにした個人情報保護マネジメントシステム実施のためのガイドライン（第 1 版）」を公表した。同ガイドラインの第二部「JISQ15001:2006 各要求事項についてのポイント」

の説明において，各箇条に対応する個人情報保護法の条項が提示されている。この対応を参考にして，個人情報保護法マネジメントシステムの構築を試みることにした。

したがって，マネジメントシステムの構成は，JIS 規格を踏襲している。JIS 規格の箇条に対応する個人情報保護法の条項を当てている。JIS に説明のないところは，筆者が作成して追加した。JIS 規格（PMS）の箇条において，個人情報保護法と対応する条項が存在しないところでは，「(対応条項なし)」としてある。この部分は，マネジメントシステムの計画，点検および見直し・改善に関係するところであるので，法律の方に対応条項が存在しないのは当然のことである。本マネジメントシステムの構成においては，「実施・運用」のステップを抜き出して後半部に置かれている。その他のステップは PMS の箇条の並びに従っている。

2. クラウドコンピューティングとセキュリティ・プライバシー

クラウドコンピューティングの導入には数々の利点があるが，そこには大きな障壁も存在する。最大の障壁となるのがセキュリティとプライバシーであると指摘される（Mather［2009］, 30ff.)。すなわち，クラウドコンピューティングは新しいコンピューティングモデルであるため，ネットワーク，ホスト，アプリケーション，データなどすべてのレベルにおいてセキュリティがどのように実現されているか不透明なところがある。また，クラウドのプライバシー問題についても，「組織は，個人情報のプライバシー保護のために数々の複雑な要求事項に直面しており，このクラウドコンピューティングモデルが個人情報のような情報を適切に保護できるかどうか，あるいはこのような新しいモデルのために組織が今後規則違反を犯すかどうか不透明である」（Mather［2009］, ibid.)。

クラウドコンピューティング社会においては，情報収集，情報創造，情報利活用の一層の拡大を目指していることから，センサ情報，地理空間情報，個人の行動履歴情報・生活情報，企業の情報システムや企業間の情報流などがクラウドに移行することになる[1)]。個人情報の収集については，個人情報保護法第16条による「目的拘束性」と「事前同意原則」があり，第三者提供については，同法23条による「事前同意原則」がある。しかし，「個人情報の保管場所に関する制約はなく，委託先の監督など『個人情報保護法』で規定される事項を遵守する限りにおいて，国外も含め第三者の提供するサーバ上に個人情報を保管することは可能である」とする[2)]。

1） 経済産業省『「クラウドコンピューティングと日本の競争力に関する研究会」報告書』2010年 8 月，18ff.
2） 同上，p. 29。

3. 個人情報保護の意義と方法

あらゆる場面で個人情報の重要性が増大しているといいながらも，「個人情報保護」という用語の意味については，かえって，拡散しているような気がしてならない。その理由のひとつは，「個人情報はプライバシーである」，あるいは，「個人情報＝（イコール）プライバシー」という考え方が，むしろ，社会において一般的になっていることである。高裁の裁判官でさえ，そういってはばからないのである[3)]。個人情報は個人に関する「事実」であり，プライバシーは個人が置かれている「状態」を表現しているのである。一方は，Personal data であり，他方は，To be let alone である。

個人情報保護の議論は，あらゆる組織が個人情報処理を実施したことが契機となって起こってきたものである。つまり，個人情報処理がブラックボックス化して，組織に提供した個人情報がどのように処理されているか皆目見当がつかない，個人情報がどこに提供されているかわからない，個人情報が適切に消去されたのかわからない，というような人々が抱く不安が個人情報保護法制定へのアクセルになったのである。その端緒から「プライバシー」ということばは登場してこない。もちろん，個人情報保護法がプライバシーを保護するということを言ったことはない。

個人情報保護は，組織の個人情報処理，それも，電子的自動情報処理（いわゆる「コンピュータ処理」）に限定すべきである。そして，個人情報保護法は，原則的には，ある監督官庁（例えば，新設の「個人情報保護庁」や現在の「消費者庁」）に登録された「個人情報処理システム」にのみ適用されるという方法をとるしかないように思われる。もちろん，未登録の個人情報処理は違法となるのである。登録制度を導入することによって，個人情報処理が透明化し，組織の個人情報の保護意識が高まることになる。登録の条件に組織の個人情報処理に関する保護保全措置が含まれるからである。ここで検討中の「個人情報保護法」マネジメントシステムの構築・運用を登録の条件に加えることもひとつの方法である。

元々組織に提供される個人情報は，ある契約に基づいて，あるいは，ある法律に基づいて，当該組織に移転されるのである。そうすると個人情報の移転後が問題となる。前述の不安から，個人情報処理が「ホワイトボックス化」すれば，それらの不安の大半は解消されることになる。逆説的な表現になるが，個人情報処理に関する徹底した「情報公開」によって「個人情報保護」が実現することになる。いわば，個人情報処理に関する情報を非公開にしていたので，人々の不安が増大したのである。そこで，自己の個人情報もしくは個人情報処理を

3） 参照，東京高裁平成14年１月16日判（『判例個人情報保護法』ぎょうせい166）。

「監視」または「監査」できる権利を個人情報保護法に盛り込むようになったのである。自己に関する個人情報処理を監査して，収集目的に適合した個人情報処理が実施されていることを確認できるわけである。これが，まさに，「個人情報保護」である。筆者は，この監査する権利を「個人情報保護の権利」と呼ぶことにしている。したがって，個人情報保護法の第一義的目的は，個人情報保護の権利を保障することである。同法には，そのほか，この権利の実現に向けて，個人情報管理責任者の義務および個人情報保護監査人の権限と任務についての規律が含まれる。

つぎに，個人情報を「物理的」に保護する規定が盛り込まれなければならない。個人情報の保全措置に関する規定である。個人情報の保全措置の実施は個人情報管理責任者の義務である。同責任者の最大の任務は「データ監査」である（北原［2008］）。すなわち，保有するすべての個人情報のライフサイクルの記録を残す作業である。どの組織おいても，データ量は膨大になるが，個人情報保護方針に則って，詳細かつ慎重に実施しなければならない。しかも，「データ監査報告書」として文書化し，情報主体の閲覧に供するとともに，監督官庁に提出しなければならない。

4. 個人情報保護方針

4.1 ポリシーの意味

個人情報保護方針は，組織の個人情報保護インフラストラクチュアの基礎である。これがなければ，組織は訴訟，金銭的損害や社会的評判から自らを擁護することは不可能である。個人情報保護方針は，組織が実施する個人情報の保護管理を高いレベルから記述する文書の集合である。方針（ポリシー）は，組織の個人情報保護規程を従業者に伝達するための手段であり，ポリシーを正式に明文化しないままでは裁判では何の効果もない。また，組織に対して次のような効果をもたらす（Andreas［2005］, 37）。

・組織の従業者や第三者に対する法的責任を軽減または免責をする。
・組織の個人情報を盗聴，悪用，不正な暴露および改竄から護る。
・組織の個人情報処理能力の浪費を防止する。

4.2 ポリシーのライフサイクル

ポリシーライフサイクルは，ポリシーを正しく策定し，実施し，監視するためのプロセスである（Andreas［2005］, 39–52）。

4.2.1 ポリシーの策定

ポリシーの策定はポリシーライフサイクルの最初のフェーズで行われる。リスク分析結果

によって明確になった組織のリスクを除去，軽減，あるいは転嫁するための個人情報保護対策を実施するために必要なポリシーを策定する。

組織の個人情報資産を脅かす最も大きいリスクは内部要員によるものである。組織にとって本当の脅威は内部の人間によるものである。したがって，個人情報保護ポリシーには組織内に向けた明確な方針を明記することが重要である。組織のネットワークに対する意図的な攻撃や不正アクセスは高度な技術によるものではなく，ポリシーや手順に内在する脆弱性を利用したものが一般的である。したがって，組織は，明確に，かつ従業者に負担とならないポリシーを作成する必要がある。このバランスを確立することが個人情報保護監査人の課題である（Andreas［2005］, 38）。

ポリシーは，文書にして組織の従業者に伝達されない限り効果がない。曖昧に記述したポリシーはインシデントを招く。サイトに最先端技術を用いた信頼性対策を実施していても，ポリシーが良くなければ，簡単に攻撃されて効果が発揮されない。ポリシー策定に失敗する最大の理由は，ポリシー策定にエンドユーザを関与させなかったことである。組織にとって最も効果的なポリシーを策定するためには，関係者全員をポリシー策定の初期から参加させることである（Andreas［2005］, ibid.）。

4.2.2　ポリシー実施

ポリシーライフサイクルの実施フェーズとは，ポリシーを組織内で確実に実施する期間である。ポリシーを遵守しないときにはその違反に見合う処罰を与えなければならない。また，すべてのポリシー違反に対して罰則を確実に執行する。罰則が確実に執行されていない場合，従業者の解雇のようなポリシー解釈は裁判で認められない可能性がある（Andreas［2005］, 40）。

4.2.3　ポリシー監視

監視フェーズが最後のフェーズになる。ポリシーライフサイクルでは常に実施されなければならない。このフェーズでは，ポリシーを定期的にレビューし，組織への妥当性および適切性を検証することになる（Andreas［2005］, 40）。

5.　個人情報保護法マネジメントシステムの構築

5.1　マネジメントシステムの適用範囲・用語・定義

1.　適用範囲

本マネジメントシステムは，特定の生存する個人を識別することができる個人に関する情報，すなわち，「個人情報」（第 2 条第 1 項），ならびに，個人情報データベース等を構成する「個人データ」および「保有個人データ」に適用される（第 2 条第 2 項）。また，本マネ

ジメントシステムは，「個人情報取扱事業者」に適用される（第２条３項）。

「個人情報データベース等」とは，「これに含まれる個人情報を一定の規則に従って整理することにより特定の個人情報を容易に検索することができるように体系的に構成した情報の集合物であって，目次，索引その他検索を容易にするためのものを有するものをいう」（個人情報の保護に関する法律施行令第２条）

これは個人情報保護「法」マネジメントシステムであるので，本マネジメントシステムの適用範囲は個人情報保護法の名宛人と同一の適用範囲となる。

個人情報保護の基本理念および個人情報保護の基本方針等を除いた部分は，やはり，特定の事業者のみに適用されるようにすべきである。特定の事業者とは，個人情報処理システム設置の届出を完了した事業者である。ただし，日本の個人情報保護法にはシステムの設置手続に関する規定は置かれていない。

2. 用語及び定義

個人情報は，「個人に関する情報であって，当該情報に含まれる氏名，生年月日その他の記述などによって特定の個人を識別できるもの」である。

個人情報保護管理者は，「代表者によって事業者の内部者から指名された者であって，個人情報マネジメントシステムの実施及び運用に関する責任及び権限をもつ者」である。

個人情報保護監査責任者は，「代表者によって事業者の内部者から指名された者であって，公平，かつ，客観的な立場にあり，監査の実施及び報告を行う責任及び権限をもつ者」である。

個人情報保護マネジメントシステムは，「事業者が，自ら事業の用に供する個人情報について，その有用性に配慮しつつ，個人の権利利益を保護するための方針，体制，計画，実施，点検及び見直しを含むマネジメントシステム」である。

「個人情報保護法」マネジメントシステムは，「事業者が，個人情報処理において，個人情報保護の権利の実現に向けて，個人情報保護方針の策定，実施および監視を含むことによって，個人情報保護法コンプライアンスを目指すマネジメントシステム」である。

この法律において「個人情報」とは，生存する個人に関する情報であって，当該情報に含まれる氏名，生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ，それにより特定の個人を識別することができることとなるものを含む。）をいう（第２条第１項）。

この法律において「個人情報データベース等」とは，個人情報を含む情報の集合物であって，次に掲げるものをいう（第２条第２項）。

一　特定の個人情報を電子計算機を用いて検索することができるように体系的に構成したもの

二　前号に掲げるもののほか，特定の個人情報を容易に検索することができるように体系的に構成したものとして政令で定めるもの

この法律において「個人情報取扱事業者」とは，個人情報データベース等を事業の用に供している者をいう。ただし，次に掲げる者を除く（第２条第３項）。

一　国の機関

二　地方公共団体

三　独立行政法人等（独立行政法人等の保有する個人情報の保護に関する法律（平成十五年法律第五十九号）第二条第一項に規定する独立行政法人等をいう。以下同じ。）

四　地方独立行政法人（地方独立行政法人法（平成十五年法律第百十八号）第二条第一項に規定する地方独立行政法人をいう。以下同じ。）

五　その取り扱う個人情報の量及び利用方法からみて個人の権利利益を害するおそれが少ないものとして政令で定める者

この法律において「個人データ」とは，個人情報データベース等を構成する個人情報をいう（第２条第４項）。

この法律において「保有個人データ」とは，個人情報取扱事業者が，開示，内容の訂正，追加又は削除，利用の停止，消去及び第三者への提供の停止を行うことのできる権限を有する個人データであって，その存否が明らかになることにより公益その他の利益が害されるものとして政令で定めるもの又は一年以内の政令で定める期間以内に消去することとなるもの以外のものをいう（第２条第５項）。

（保有個人データから除外されるもの）（政令）

第三条　法第二条第五項の政令で定めるものは，次に掲げるものとする。

一　当該個人データの存否が明らかになることにより，本人又は第三者の生命，身体又は財産に危害が及ぶおそれがあるもの

二　当該個人データの存否が明らかになることにより，違法又は不当な行為を助長し，又は誘発するおそれがあるもの

三　当該個人データの存否が明らかになることにより，国の安全が害されるおそれ，他国若しくは国際機関との信頼関係が損なわれるおそれ又は他国若しくは国際機関との交渉上不利益を被るおそれがあるもの

四　当該個人データの存否が明らかになることにより，犯罪の予防，鎮圧又は捜査その他の公共の安全と秩序の維持に支障が及ぶおそれがあるもの

（保有個人データから除外されるものの消去までの期間）（政令）

第四条　法第二条第五項の政令で定める期間は，六月とする。

この法律において個人情報について「本人」とは，個人情報によって識別される特定の個

人をいう（第 2 条第 6 項）。

「個人情報データベース等」（法律施行令第 1 条）

「個人情報取扱事業者から除外される者」（法律施行令第 2 条）

ただし，法律施行令第 2 条は本規格では適用しないとする。

（個人情報取扱事業者から除外される者）

第二条　法第二条第三項第五号の政令で定める者は，その事業の用に供する個人情報データベース等を構成する個人情報によって識別される特定の個人の数（当該個人情報データベース等の全部又は一部が他人の作成に係る個人情報データベース等であって，次の各号のいずれかに該当するものを編集し，又は加工することなくその事業の用に供するときは，当該個人情報データベース等の全部又は一部を構成する個人情報によって識別される特定の個人の数を除く。）の合計が過去六月以内のいずれの日においても五千を超えないものとする。

一　個人情報として次に掲げるもののみが含まれるもの

イ　氏名

ロ　住所又は居所（地図上又は電子計算機の映像面上において住所又は居所の所在の場所を示す表示を含む。）

ハ　電話番号

二　不特定かつ多数の者に販売することを目的として発行され，かつ，不特定かつ多数の者により随時に購入することができるもの又はできたもの

個人情報保護法は，「個人情報取扱事業者」のみを規定している。個人情報処理の管理責任者及び個人情報保護監査人というように，少なくとも，PMS でも定義されているような人的設備が必要である。個人情報の保護を含む情報セキュリティの問題においては，最終的には人的設備の問題に帰着する。つまり，組織の代表者，情報処理管理責任者および個人情報保護監査人の権限・責任・義務等を明確にしておかなければならないからである。

5.2　マネジメントシステムの計画

3.　要求事項

3.1　一般要求事項

事業者は，「個人情報保護法」マネジメントシステムを確立し，実施し，維持し，かつ，改善しなければならない。その要求事項は，箇条 3 で規定する。

3.2　個人情報保護方針

個人情報保護の理念を明確にした上で，個人情報保護方針を定め，これを実行し，かつ，維持しなければならない。同保護方針には，「適切な個人情報の取得・利用・提供，および目的外利用に関すること」を盛り込むこと。さらに，「法令・指針・その他の規範の遵守」，

「個人情報の漏えい，滅失・棄損の防止・是正に関すること」，「苦情・相談への対応に関すること」，「個人情報保護マネジメントシステムの継続的改善に関すること」，「代表者氏名」を盛り込まなければならない。

また，この方針を文書化し，従業者に周知し，一般人が入手可能な措置を講じること。個人情報保護法における「基本理念」も個人情報保護方針に含まれる。同法では以下のように規定されている。

個人情報は，個人の人格尊重の理念の下に慎重に取り扱われるべきものであることにかんがみ，その適正な取扱いが図られなければならない（第３条）。

PMS においては，個人情報保護法との対応として以下の部分が示されている。

「個人情報保護に関する基本方針」（平成16年４月２日閣議決定）

6　個人情報取扱事業者等が講ずべき個人情報の保護のための措置に関する基本的な事項

⑴　個人情報取扱事業者に関する事項 個人情報取扱事業者は，法の規定に従うほか，２の⑶の①の各省庁のガイドライン等に則し，個人情報の保護について主体的に取り組むことが期待されているところであり，事業者は，引き続き体制の整備等に積極的に取り組んでいくことが求められている。各省庁等におけるガイドライン等の検討及び各事業者の取組に当たっては，特に以下の点が重要であると考えられる。

①　事業者が行う措置の対外的明確化　事業者が個人情報保護を推進する上での考え方や方針（いわゆる，プライバシーポリシー，プライバシーステートメント等）を策定・公表することにより，個人情報を目的外に利用しないことや苦情処理に適切に取り組むこと等を宣言するとともに，事業者が関係法令等を遵守し，利用目的の通知・公表，開示等の個人情報の取扱いに関する諸手続について，あらかじめ，対外的に分かりやすく説明することが，事業活動に対する社会の信頼を確保するために重要である。

2の⑶の①とは以下の部分である。

2　国が講ずべき個人情報の保護のための措置に関する事項

⑶　分野ごとの個人情報の保護の推進に関する方針

①　各省庁が所管する分野において講ずべき施策

個人情報の保護については，法の施行前も，事業者の取り扱う個人情報の性質や利用方法等の実態を踏まえつつ，事業等分野ごとのガイドライン等に基づく自主的な取組が進められてきたところである。

このような自主的な取組は，法の施行後においても，法の定めるルールの遵守と相まって，個人情報保護の実効を上げる上で，引き続き期待されるところであり，尊重され，また，促進される必要がある。このため，各省庁は，法の個人情報の取扱いに関するルールが各分野に共通する必要最小限のものであること等を踏まえ，それぞれの事業等の分野の実情に応じ

たガイドライン等の策定・見直しを検討するとともに，事業者団体等が主体的に行うガイドラインの策定等に対しても，情報の提供，助言等の支援を行うものとする。

また，悪質な事業者の監督のため，個人情報取扱事業者に対する報告の徴収等の主務大臣の権限等について，これを適切に行使するなど，法等の厳格な適用を図るものとする。

3.3 計画

3.3.1 個人情報の特定

事業者は，自らの事業の用に供するすべての個人情報を特定するための手順を確立し，かつ，維持しなければならない。

この法律において「個人情報取扱事業者」とは，個人情報データベース等を事業の用に供している者をいう（第２条第３項）[4)]。

組織内で取扱っている個人情報を特定することを意味する。つまり，このマネジメントシステムにおいて，保護保全の対象となるものを明確にすることである。特定に当たっては，当該個人情報の利用目的，入手経路，組織内での取扱経路（取扱部署），保管場所，保管形態，保管期間，廃棄方法等について台帳等にまとめる（PMS［2006］, 9）。

これは個人情報のライフサイクルを記録することであり，組織が保有するあらゆる個人情報について「データ監査」を実施することに他ならない（北原［2006］, 205）。

3.3.2 法令，指針，その他の規範

（対応条項なし）

個人情報の取扱いに関する法令，国の指針，その他の規範を特定し，参照できる手順を確立し，かつ，維持しなければならない。

個人情報保護法の他に，様々な法律に個人情報の保護に関する条項を含まれている（北原［2010］, 130ff.）。それらの条項と本法との関係，「横出し」，「上乗せ」というものがないか精査する必要がある。

3.3.3 リスクなどの認識，分析及び対策

（対応条項なし）

特定した個人情報について，目的外利用を行わないための対策を講じる手順を確立し，維持する。個人情報の取扱いにおけるリスクを認識し，分析し，対策を講じる手順を確立し，維持する。リスクの例として，個人情報の漏えい，滅失，棄損など，法令・指針・その他の規範に対する違反，経済的不利益・社会的信用の失墜，本人への影響など，が上げられる。

ここでは，「個人情報リスクマネジメントシステム」の構築を考えるべきである（北原［2008］, 21ff.）。

4）「個人情報の特定」の箇条に「個人情報取扱事業者」の定義が対応するとされる。参照，PMS［2006］，24頁。

3.3.4　資源，役割，責任及び権限

(対応条項なし)

事業者代表者は，個人情報保護マネジメントシステムを確立し，実施し，維持し，かつ，改善するために不可欠な資源を用意しなければならない。

代表者は，個人情報保護マネジメントシステムを効果的に実施するために役割，責任及び権限を定め，文書化し，かつ，従業者に周知しなければならない。

代表者は，この規格の内容を理解し実践する能力のある個人情報保護管理者を事業者の内部から指名し，個人情報保護マネジメントシステムの実施・運用に関する責任・権限を他の責任にかかわりなく与え，業務を行わせなければならない。

個人情報保護管理者は，個人情報保護マネジメントシステムの見直し・改善の基礎として，事業者の代表者に個人情報保護マネジメントシステムの運用状況を報告しなければならない。

3.3.5　内部規程

(対応条項なし)

事業者は，内部規程を文書化し，維持しなければならない。その内部規程に盛り込まれる項目は以下の通りである。

a)　個人情報の特定手順に関する規定。
b)　法令，指針，その他の規範の特定・参照・維持に関する規定。
c)　個人情報に関するリスクの認識・分析・対策の手順に関する規定。
d)　事業者の各部門・階層における個人情報保護のための権限・責任に関する規定。
e)　緊急事態（漏洩・滅失・棄損）への準備・対応に関する規定。
f)　個人情報の取得・利用・提供に関する規定。
g)　個人情報の適正管理に関する規定。
h)　本人からの開示等の求めへの対応に関する規定。
i)　教育に関する規定。
j)　個人情報保護マネジメントシステム文書の管理に関する規定。
k)　苦情・相談への対応に関する規定。
l)　点検に関する規定。
m)　是正処置・予防処置に関する規定。
n)　代表者による見直しに関する規定。
o)　内部規程の違反に関する罰則規定。

3.3.6　計画書

(対応条項なし)

「個人情報保護法」マネジメントシステムを確実に実施するために必要な教育，監査など

の計画を立案し，文書化し，維持しなければならない。

3.3.7　緊急事態への準備

(対応条項なし)

事業者は，緊急事態を特定するための手順，緊急事態への対応の手順を確立・実施・維持しなければならない。実際の対応としては，事態発生に関わる本人，関係者への通知，二次被害発生防止，類似事案発生回避，事実関係・発生原因・対応策の公表などである。そして，この事態に関わる一部始終を監督官庁に報告しなければならない。このような事態に関する手順は内部規程において，規定化されているはずである。

5.3　マネジメントシステムの実施及び運用

3.4　実施及び運用

3.4.1　運用手順

事業者は，個人情報保護マネジメントシステムを確実に実施するために，運用手順を明確にしなければならない。

3.4.5　教育

事業者は，従業者に，定期的に適切な教育を行わなければならない。事業者は，従業者に，関連する各部門及び階層における次の事項を理解させる手順を確立し，かつ，維持しなければならない。

a)　個人情報保護マネジメントシステムに適合することの重要性及び利点

b)　個人情報保護マネジメントシステムに適合するための役割及び責任

c)　個人情報保護マネジメントシステムに違反した際に予想される結果

事業者は，教育の計画及び実施，結果の報告及びそのレビュー，計画の見直し並びにこれらに伴う記録の保持に関する責任及び権限を定める手順を確立し，実施し，かつ，維持しなければならない。

3.5　個人情報保護マネジメントシステム文書

3.5.1　文書の範囲

(対応条項なし)

事業者は，次の個人情報保護マネジメントシステムの基本となる要素を書面で記述しなければならない。

a)　個人情報保護方針

b)　内部規程

c)　計画書

d)　この規格が要求する記録及び事業者が個人情報保護マネジメントシステムを実施する

上で必要と判断した記録

3.5.2　文書管理

(対応条項なし)

事業者は，個人情報保護マネジメントシステム及びこの規格の要求事項への適合を実施するために必要な記録を作成し，かつ，維持しなければならない。

事業者は，記録の管理についての手順を確立し，実施し，かつ，維持しなければならない。

3.6　苦情及び相談への対応

事業者は，個人情報の取扱い及び個人情報保護マネジメントシステムに関して，本人からの苦情及び相談を受けて，適切，かつ，迅速な対応を行う手順を確立し，かつ，維持しなければならない。

事業者は，上記の目的を達成するために必要な体制の整備を行わなければならない。

個人情報取扱事業者は，個人情報の取扱いに関する苦情の適切かつ迅速な処理に努めなければならない（第31条第１項)。

個人情報取扱事業者は，前項の目的を達成するために必要な体制の整備に努めなければならない（第31条第２項)。

(認定個人情報保護団体)

個人情報取扱事業者の個人情報の適正な取扱いの確保を目的として次に掲げる業務を行おうとする法人（法人でない団体で代表者又は管理人の定めのあるものを含む。次条第三号ロにおいて同じ。）は，主務大臣の認定を受けることができる（第37条第１項)。

一　業務の対象となる個人情報取扱事業者（以下「対象事業者」という。）の個人情報の取扱いに関する第四十二条の規定による苦情の処理

二　個人情報の適正な取扱い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

三　前二号に掲げるもののほか，対象事業者の個人情報の適正な取扱いの確保に関し必要な業務

前項の認定を受けようとする者は，政令で定めるところにより，主務大臣に申請しなければならない（第37条第２項)。

主務大臣は，第一項の認定をしたときは，その旨を公示しなければならない（第37条第３項)。

5.4 マネジメントシステムの点検

3.7 点検

3.7.1 運用の確認

(対応条項なし)

事業者は，個人情報保護マネジメントシステムのこの規格への適合状況及び個人情報保護マネジメントシステムの運用状況を定期的に監査しなければならない。

事業者の代表者は，公平，かつ，客観的な立場にある個人情報保護監査責任者を事業者の内部の者から指名し，監査の実施及び報告を行う責任及び権限を他の責任にかかわりなく与え，業務を行わせなければならない。

個人情報保護監査責任者は，監査を指揮し，監査報告書を作成し，事業者の代表者に報告しなければならない。監査員の選定及び監査の実施においては，監査の客観性及び公平性を確保しなければならない。

事業者は，監査の計画及び実施においては，結果の報告並びにこれに伴う記録の保持に関する責任及び権限を定める手順を確立し，実施し，かつ，維持しなければならない。

3.7.2 監査

(対応条項なし)

事業者は，個人情報保護マネジメントシステムのこの規格への適合状況及び個人情報保護マネジメントシステムの運用状況を定期的に監査しなければならない。

事業者の代表者は，公平，かつ，客観的な立場にある個人情報保護監査責任者を事業者の内部の者から指名し，監査の実施及び報告を行う責任及び権限を他の責任にかかわりなく与え，業務を行わせなければならない。

個人情報保護監査責任者は，監査を指揮し，監査報告書を作成し，事業者の代表者に報告しなければならない。監査員の選任及び監査の実施においては，監査の客観性及び公平性を確保しなければならない。

事業者は，監査の計画及び実施，結果の報告並びにこれに伴う記録の保持に関する責任及び権限を定める手順を確立し，実施し，かつ，維持しなければならない。

5.5 マネジメントシステムの改善・見直し

3.8 是正措置及び予防措置

(対応条項なし)

事業者は，不適合に対する是正措置及び予防措置を確実に実施するための責任及び権限を定める手順を確立し，実施し，かつ，維持しなければならない。その手順には，次の事項を含めなければならない。

a） 不適合の内容を確認する。

b） 不適合の原因を特定し，是正処置及び予防処置を立案する。

c） 期限を定め，立案された処置を実施する。

d） 実施された是正処置及び予防処置の結果を記録する。

e） 実施された是正処置及び予防処置の有効性をレビューする。

3.9 事業者の代表者による見直し

(対応条項なし)

事業者の代表者は，個人情報の適切な保護を維持するために，定期的に個人情報保護マネジメントシステムを見直さなければならない。

事業者の代表者による見直しにおいては，次の事項を考慮しなければならない。

a） 監査及び個人情報保護マネジメントシステムの運用状況に関する報告

b） 苦情を含む外部からの意見

c） 前回までの見直しの結果に対するフォローアップ

d） 個人情報の取扱いに関する法令，国の定める指針その他の規範の改正状況

e） 社会情勢の変化，国民の認識の変化，技術の進歩などの諸環境の変化

f） 事業者の事業領域の変化

g） 内外から寄せられた改善のための提案

3.4.2 取得・利用・提供に関する原則

3.4.2.1 利用目的の特定

個人情報取扱事業者は，個人情報を取り扱うに当たっては，その利用の目的をできる限り特定しなければならない（第15条第１項)。

個人情報取扱事業者は，利用目的を変更する場合には，変更前の利用目的と相当の関連性を有すると合理的に認められる範囲を超えて行ってはならない（第15条第２項)。

3.4.2.2 適正な取得

個人情報取扱事業者は，偽りその他不正の手段により個人情報を取得してはならない（第17条)。

3.4.2.3 特定の機微な個人情報の取得・利用・提供の制限

(対応条項なし)

個人情報保護法には「機微な個人情報」（subtle personal information）という概念は存在しない。「機微な個人情報」として，

a） 思想，信条又は宗教に関する事項

b） 人種，民族，門地，本籍地，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

c） 勤労者の団結権，団体交渉権その他の団体行動の行為に関する事項

d） 集団示威行為への参加，請願権の行使その他政治的権利の行使に関する事項

e） 保健医療又は性生活に関する事項

が挙げられている。

事業者は，これらの内容を含む個人情報の取得，利用又は提供は，行ってはならない。ただし，これらの取得，利用又は提供について，明示的な本人の同意がある場合及び法令に基づく場合等には，この限りでない。

個人情報処理には，「目的拘束性の原則」が適用される。すなわち，個人情報の収集から消去に至るまで，個人情報のライフサイクルにおいて，最初に設定された，つまり情報主体が同意した目的が最優先されるはずである。その目的に従った情報収集が行われるならば，いわゆる「機微個人情報」を必要とする事業者も，必要としない事業者も存在するであろう。したがって，あくまでも，「目的に従った」という基準で十分なように思われる。

個人情報処理システム登録制度の下では，収集する個人情報の種類が届出事項の一つになっているので，その手続の段階でチェックされる。また，「データ監査報告書」にも記録として残される。

3.4.2.4 本人からの直接書面によって取得する場合の措置

個人情報取扱事業者は，個人情報を取得した場合は，あらかじめその利用目的を公表している 場合を除き，速やかに，その利用目的を，本人に通知し，又は公表しなければならない（第18条第１項）。

個人情報取扱事業者は，前項の規定にかかわらず，本人との間で契約を締結することに伴って契約書その他の書面（電子的方式，磁気的方式その他人の知覚によっては認識することができない方式で作られる記録を含む。以下この項において同じ。）に記載された当該本人の個人情報を取得する場合その他本人から直接書面に記載された当該本人の個人情報を取得する場合は，あらかじめ，本人に対し，その利用目的を明示しなければならない。ただし，人の生命，身体又は財産の保護のために緊急に必要がある場合は，この限りでない（第18条第２項）。

個人情報取扱事業者は，利用目的を変更した場合は，変更された利用目的について，本人に通知し，又は公表しなければならない（第18条第３項）。

前三項の規定は，次に掲げる場合については，適用しない（第18条第４項）。

一 利用目的を本人に通知し，又は公表することにより本人又は第三者の生命，身体，財産その他の権利利益を害するおそれがある場合

二 利用目的を本人に通知し，又は公表することにより当該個人情報取扱事業者の権利又は正当な利益を害するおそれがある場合

三　国の機関又は地方公共団体が法令の定める事務を遂行することに対して協力する必要がある場合であって，利用目的を本人に通知し，又は公表することにより当該事務の遂行に支障を及ぼすおそれがあるとき。

四　取得の状況からみて利用目的が明らかであると認められる場合

3.4.2.5　個人情報を（3.4.2.4）以外の方法によって取得した場合の措置

基本法は，取得に際しての利用目的の通知又は公表（第18条第１項）および利用目的の通知又は公表の例外（第18条第４項）の規定を適用する。

3.4.2.6　利用に関する措置

個人情報取扱事業者は，あらかじめ本人の同意を得ないで，前条の規定により特定された利用目的の達成に必要な範囲を超えて，個人情報を取り扱ってはならない（第16条第１項）。

個人情報取扱事業者は，合併その他の事由により他の個人情報取扱事業者から事業を承継することに伴って個人情報を取得した場合は，あらかじめ本人の同意を得ないで，承継前における当該個人情報の利用目的の達成に必要な範囲を超えて，当該個人情報を取り扱ってはならない（第16条第２項）。

前二項の規定は，次に掲げる場合については，適用しない（第16条第３項）。

一　法令に基づく場合

二　人の生命，身体又は財産の保護のために必要がある場合であって，本人の同意を得ることが困難であるとき。

三　公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって，本人の同意を得ることが困難であるとき。

四　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって，本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

3.4.2.7　本人にアクセスする場合の措置

個人情報保護法には，本箇条に直接該当する条項は見あたらない（対応条項なし）。

3.4.2.8　提供に関する措置

個人情報取扱事業者は，次に掲げる場合を除くほか，あらかじめ本人の同意を得ないで，個人データを第三者に提供してはならない（第23条第１項）。

一　法令に基づく場合

二　人の生命，身体又は財産の保護のために必要がある場合であって，本人の同意を得ることが困難であるとき。

三　公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって，本人の同意を得ることが困難であるとき。

四　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって，本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

個人情報取扱事業者は，第三者に提供される個人データについて，本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止することとしている場合であって，次に掲げる事項について，あらかじめ，本人に通知し，又は本人が容易に知り得る状態に置いているときは，前項の規定にかかわらず，当該個人データを第三者に提供することができる（第23条第２項）。

一　第三者への提供を利用目的とすること。

二　第三者に提供される個人データの項目

三　第三者への提供の手段又は方法

四　本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止すること。

個人情報取扱事業者は，前項第二号又は第三号に掲げる事項を変更する場合は，変更する内容について，あらかじめ，本人に通知し，又は本人が容易に知り得る状態に置かなければならない（第23条第３項）。

次に掲げる場合において，当該個人データの提供を受ける者は，前三項の規定の適用については，第三者に該当しないものとする（第23条第４項）。

一　個人情報取扱事業者が利用目的の達成に必要な範囲内において個人データの取扱いの全部又は一部を委託する場合

二　合併その他の事由による事業の承継に伴って個人データが提供される場合

三　個人データを特定の者との間で共同して利用する場合であって，その旨並びに共同して利用される個人データの項目，共同して利用する者の範囲，利用する者の利用目的及び当該個人データの管理について責任を有する者の氏名又は名称について，あらかじめ，本人に通知し，又は本人が容易に知り得る状態に置いているとき。

個人情報取扱事業者は，前項第三号に規定する利用する者の利用目的又は個人データの管理について責任を有する者の氏名若しくは名称を変更する場合は，変更する内容について，あらかじめ，本人に通知し，又は本人が容易に知り得る状態に置かなければならない（第23条第５項）。

さらに，個人情報保護法第16条第３項（目的外利用で同意が不要の場合）が適用される。

OECD 八原則は，第三者提供において，その個人情報が収集された組織と同レベル以上の個人情報保護措置を実施していない国へのデータの転送を禁止している。この原則は国内のデータ処理事業者間にも妥当する。

3.4.3　適正管理

3.4.3.1　正確性の確保

個人情報取扱事業者は，利用目的の達成に必要な範囲内において，個人データを正確かつ最新の内容に保つよう努めなければならない（第19条）。

3.4.3.2　安全管理措置

個人情報取扱事業者は，その取り扱う個人データの漏えい，滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない（第20条）。

個人データの安全管理のため，組織的，人的，物理的及び技術的という 4 種類の安全管理措置を講じなければならないとする（ガイドライン［2009］, 25）。

3.4.3.3　従業者の監督

個人情報取扱事業者は，その従業者に個人データを取り扱わせるに当たっては，当該個人データの安全管理が図られるよう，当該従業者に対する必要かつ適切な監督を行わなければならない（第21条）。

3.4.3.4　委託先の監督

個人情報取扱事業者は，個人データの取扱いの全部又は一部を委託する場合は，その取扱いを委託された個人データの安全管理が図られるよう，委託を受けた者に対する必要かつ適切な監督を行わなければならない（第22条）。

3.4.4　個人情報に関する本人の権利

3.4.4.1　個人情報に対する権利

個人情報保護法には，情報主体の権利に関する条項は存在しない。PMS 実施のためのガイドラインは，個人情報保護法第 2 条第 5 項，同法施行令第 3 条および第 4 条が対応するとしている。ただし，施行令第 4 条は本規格では適用しないとする。

この法律において「保有個人データ」とは，個人情報取扱事業者が，開示，内容の訂正，追加又は削除，利用の停止，消去及び第三者への提供の停止を行うことのできる権限を有する個人データであって，その存否が明らかになることにより公益その他の利益が害されるものとして政令で定めるもの又は一年以内の政令で定める期間以内に消去することとなるもの以外のものをいう（第 2 条第 5 項）。

（個人情報の保護に関する法律施行令）（政令）

第三条　法第二条第五項の政令で定めるものは，次に掲げるものとする。

一　当該個人データの存否が明らかになることにより，本人又は第三者の生命，身体又は財産に危害が及ぶおそれがあるもの

二　当該個人データの存否が明らかになることにより，違法又は不当な行為を助長し，又は誘発するおそれがあるもの

三　当該個人データの存否が明らかになることにより，国の安全が害されるおそれ，他国若しくは国際機関との信頼関係が損なわれるおそれ又は他国若しくは国際機関との交渉上不利益を被るおそれがあるもの

四　当該個人データの存否が明らかになることにより，犯罪の予防，鎮圧又は捜査その他の公共の安全と秩序の維持に支障が及ぶおそれがあるもの

（保有個人データから除外されるものの消去までの期間）

第四条　法第二条第五項の政令で定める期間は，六月とする。

自己の個人情報の開示「請求権」をめぐる問題である。ある裁判においても，個人情報の開示の「求め」では，裁判手続で開示請求できないと判示されている[5)]。個人情報保護法が情報主体による苦情を当事者間の自主的解決にゆだねる趣旨で制定されたものであるから，直接裁判上の開示請求がされることになると，紛争解決手段に関する法の規定が空文化してしまうというのが判示理由である。この裁判所の論理を貫くと，これ以下の訂正，追加，削除，提供中止，利用停止等の「求め」も「請求権」ではなくなってしまうのである[6)]。

3.4.4.2　開示等の求めに応じる手続

個人情報取扱事業者は，第二十四条第二項，第二十五条第一項，第二十六条第一項又は第二十七条第一項若しくは第二項の規定による求め（以下この条において「開示等の求め」という。）に関し，政令で定めるところにより，その求めを受け付ける方法を定めることができる。この場合において，本人は，当該方法に従って，開示等の求めを行わなければならない（第29条第１項）。

個人情報取扱事業者は，本人に対し，開示等の求めに関し，その対象となる保有個人データを特定するに足りる事項の提示を求めることができる。この場合において，個人情報取扱事業者は，本人が容易かつ的確に開示等の求めをすることができるよう，当該保有個人データの特定に資する情報の提供その他本人の利便を考慮した適切な措置をとらなければならない（第29条第２項）。

開示等の求めは，政令で定めるところにより，代理人によってすることができる（第29条第３項）。

個人情報取扱事業者は，前三項の規定に基づき開示等の求めに応じる手続を定めるに当たっては，本人に過重な負担を課するものとならないよう配慮しなければならない（第29条第４項）。

5）参照，東京地裁平成19年６月27日判（『判例個人情報保護法』ぎょうせい302）。

6）参照，藤原静雄『逐条個人情報保護法』弘文堂2003年，p. 98。「本条１項に反して開示が行われなかったら，本人は個人情報取扱事業者による開示義務の履行を求めて，裁判上の訴えができる。したがって，これを請求権と呼ぶことは不自然ではないと思われる」。

（個人情報の保護に関する法律施行令）（政令）

第七条　法第二十九条第一項の規定により個人情報取扱事業者が開示等の求めを受け付ける方法として定めることができる事項は，次に掲げるとおりとする。

一　開示等の求めの申出先

二　開示等の求めに際して提出すべき書面（電子的方式，磁気的方式その他人の知覚によっては認識することができない方式で作られる記録を含む。）の様式その他の開示等の求めの方式

三　開示等の求めをする者が本人又は次条に規定する代理人であることの確認の方法

四　法第三十条第一項の手数料の徴収方法

（開示等の求めをすることができる代理人）

第八条　法第二十九条第三項の規定により開示等の求めをすることができる代理人は，次に掲げる代理人とする。

一　未成年者又は成年被後見人の法定代理人

二　開示等の求めをすることにつき本人が委任した代理人

3.4.4.3　開示対象個人情報に関する事項の周知など

個人情報取扱事業者は，保有個人データに関し，次に掲げる事項について，本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）に置かなければならない（第24条第１項）。

一　当該個人情報取扱事業者の氏名又は名称

二　すべての保有個人データの利用目的（第十八条第四項第一号から第三号までに該当する場合を除く。）

三　次項，次条第一項，第二十六条第一項又は第二十七条第一項若しくは第二項の規定による求めに応じる手続（第三十条第二項の規定により手数料の額を定めたときは，その手数料の額を含む。）

四　前三号に掲げるもののほか，保有個人データの適正な取扱いの確保に関し必要な事項として政令で定めるもの

個人情報取扱事業者の個人情報の適正な取扱いの確保を目的として次に掲げる業務を行おうとする法人（法人でない団体で代表者又は管理人の定めのあるものを含む。次条第三号ロにおいて同じ。）は，主務大臣の認定を受けることができる（第37条第１項）。

一　業務の対象となる個人情報取扱事業者（以下「対象事業者」という。）の個人情報の取扱いに関する第四十二条の規定による苦情の処理

二　個人情報の適正な取扱い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

三　前二号に掲げるもののほか，対象事業者の個人情報の適正な取扱いの確保に関し必要な業務

前項の認定を受けようとする者は，政令で定めるところにより，主務大臣に申請しなければならない（第37条第２項）。

主務大臣は，第一項の認定をしたときは，その旨を公示しなければならない（第37条第３項）。

3.4.4.4　開示対象個人情報の利用目的の通知

個人情報取扱事業者は，本人から，当該本人が識別される保有個人データの利用目的の通知を求められたときは，本人に対し，遅滞なく，これを通知しなければならない。ただし，次の各号のいずれかに該当する場合は，この限りでない（第24条第２項）。

一　前項の規定により当該本人が識別される保有個人データの利用目的が明らかな場合

二　第十八条第四項第一号から第三号までに該当する場合

個人情報取扱事業者は，前項の規定に基づき求められた保有個人データの利用目的を通知しない旨の決定をしたときは，本人に対し，遅滞なく，その旨を通知しなければならない（第24条第３項）。

個人情報取扱事業者は，第二十四条第三項，第二十五条第二項，第二十六条第二項又は前条第三項の規定により，本人から求められた措置の全部又は一部について，その措置をとらない旨を通知する場合又はその措置と異なる措置をとる旨を通知する場合は，本人に対し，その理由を説明するよう努めなければならない（第28条）。

3.4.4.5　開示対象個人情報の開示

個人情報取扱事業者は，本人から，当該本人が識別される保有個人データの開示（当該本人が識別される保有個人データが存在しないときにその旨を知らせることを含む。以下同じ。）を求められたときは，本人に対し，政令で定める方法により，遅滞なく，当該保有個人データを開示しなければならない。ただし，開示することにより次の各号のいずれかに該当する場合は，その全部又は一部を開示しないことができる（第25条第１項）。

一　本人又は第三者の生命，身体，財産その他の権利利益を害するおそれがある場合

二　当該個人情報取扱事業者の業務の適正な実施に著しい支障を及ぼすおそれがある場合

三　他の法令に違反することとなる場合

個人情報取扱事業者は，前項の規定に基づき求められた保有個人データの全部又は一部について開示しない旨の決定をしたときは，本人に対し，遅滞なく，その旨を通知しなければならない（第25条第２項）。

他の法令の規定により，本人に対し第一項本文に規定する方法に相当する方法により当該本人が識別される保有個人データの全部又は一部を開示することとされている場合には，当

該全部又は一部の保有個人データについては，同項の規定は，適用しない（第25条第３項）。

個人情報取扱事業者は，第二十四条第三項，第二十五条第二項，第二十六条第二項又は前条第三項の規定により，本人から求められた措置の全部又は一部について，その措置をとらない旨を通知する場合又はその措置と異なる措置をとる旨を通知する場合は，本人に対し，その理由を説明するよう努めなければならない（第28条）

（個人情報の保護に関する法律施行令）（政令）

（個人情報取扱事業者が保有個人データを開示する方法）

第六条　法第二十五条第一項の政令で定める方法は，書面の交付による方法（開示の求めを行った者が同意した方法があるときは，当該方法）とする。

3.4.4.6　開示対象個人情報の訂正，追加又は削除

個人情報取扱事業者は，本人から，当該本人が識別される保有個人データの内容が事実でないという理由によって当該保有個人データの内容の訂正，追加又は削除（以下この条において「訂正等」という。）を求められた場合には，その内容の訂正等に関して他の法令の規定により特別の手続が定められている場合を除き，利用目的の達成に必要な範囲内において，遅滞なく必要な調査を行い，その結果に基づき，当該保有個人データの内容の訂正等を行わなければならない（第26条第１項）。

個人情報取扱事業者は，前項の規定に基づき求められた保有個人データの内容の全部若しくは一部について訂正等を行ったとき，又は訂正等を行わない旨の決定をしたときは，本人に対し，遅滞なく，その旨（訂正等を行ったときは，その内容を含む。）を通知しなければならない（第26条第２項）。

3.4.4.7　開示対象個人情報の利用又は提供の拒否権

（利用停止等）

個人情報取扱事業者は，本人から，当該本人が識別される保有個人データが第十六条の規定に違反して取り扱われているという理由又は第十七条の規定に違反して取得されたものであるという理由によって，当該保有個人データの利用の停止又は消去（以下この条において「利用停止等」という。）を求められた場合であって，その求めに理由があることが判明したときは，違反を是正するために必要な限度で，遅滞なく，当該保有個人データの利用停止等を行わなければならない。ただし，当該保有個人データの利用停止等に多額の費用を要する場合その他の利用停止等を行うことが困難な場合であって，本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは，この限りでない（第27条第１項）。

個人情報取扱事業者は，本人から，当該本人が識別される保有個人データが第二十三条第一項の規定に違反して第三者に提供されているという理由によって，当該保有個人データの第三者への提供の停止を求められた場合であって，その求めに理由があることが判明したと

きは，遅滞なく，当該保有個人データの第三者への提供を停止しなければならない。ただし，当該保有個人データの第三者への提供の停止に多額の費用を要する場合その他の第三者への提供を停止することが困難な場合であって，本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは，この限りでない（第27条第２項）。

個人情報取扱事業者は，第一項の規定に基づき求められた保有個人データの全部若しくは一部について利用停止等を行ったとき若しくは利用停止等を行わない旨の決定をしたとき，又は前項の規定に基づき求められた保有個人データの全部若しくは一部について第三者への提供を停止したとき若しくは第三者への提供を停止しない旨の決定をしたときは，本人に対し，遅滞なく，その旨を通知しなければならない（第27条第３項）。

（理由の説明）

個人情報取扱事業者は，第二十四条第三項，第二十五条第二項，第二十六条第二項又は前条第三項の規定により，本人から求められた措置の全部又は一部について，その措置をとらない旨を通知する場合又はその措置と異なる措置をとる旨を通知する場合は，本人に対し，その理由を説明するよう努めなければならない（第28条）。

6. お わ り に

個人情報処理システムを設置する組織にとって，個人情報処理をめぐる規制が数種類存在し，かつ煩雑化している。その負担を軽減し，さらに，個人情報保護規範のコンプライアンス文化を浸透させるために，「個人情報保護法」をマネジメントシステムに載せることを思いついた次第である。同法がマネジメントシステム向きに策定されていなかったことは当然であり，PMS と同法の間の乖離は，ところどころで大きいものがあった。しかしながら，両者の目的は，ただひとつ「個人情報保護」ということであるので，今後の検討次第では，理想的なマネジメントシステムになることを信じている。現 PMS の構築手法に示唆を仰ぎながら，個人情報保護法の条項を中心としたマネジメントシステム構築の展望が開かれているように思われる。かかる意味では，この研究自体が，まさに，マネジメントシステム的手法を以て改善されることであろう。まだまだ「β（ベータ）版」である。

参 考 文 献

［1］ Morgan［2004］, R. Morgan/R. Boardman, *Data Protection Strategy*, THOMSON 2004.
［2］ 島田［2004］，島田祐次『個人情報保護法への企業の実務対応――モデル規程によるマネジメントシステムの構築と運用のポイント』日科技連2004年。
［3］ Andreas［2005］，Amanda Andreas 著戸田巌監訳『実践情報セキュリティ人・運用・技術』オーム社2005年。

［4］ 北原［2006］，北原宗律「イギリス・データ保護法におけるデータ監査とコンプライアンス」経済科学研究第9巻第2号199–223。
［5］ PMS［2006］，『JISQ15001:2006 をベースにした個人情報保護マネジメントシステム実施のためのガイドライン第1版』（財）日本情報処理開発協会プライバシーマーク推進センター2006年。
［6］ 下島［2006］，下島和彦／清水口咲子『プライバシーマーク対応個人情報保護マネジメントシステムの構築実例集――実例でわかる JISQ15001 の導入・運用実務』日科技連2006年。
［7］ 北原［2008］，北原宗律「個人情報保護マネジメントシステム」経済科学研究第11巻第2号15–22。
［8］ Whitman［2008］, M. E. Whitman/H .J. Mattord, *Management of Information Security*, THOMSON 2008.
［9］ ガイドライン［2009］，経済産業省「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」（平成21年10月9日厚生労働省・経済産業省告示第2号）平成21（2009）年。
［10］ Mather［2009］, Tim Mather/Subra Kumaraswamy/Shahed Latif, *Cloud Security and Privacy*, O'REILY 2009.
［11］ 北原［2009］，北原宗律『法情報論』ふくろう出版2009年。
［12］ 下道［2010］，下道高志監訳『クラウド　セキュリティ＆プライバシー：リスクとコンプライアンスに対する企業の視点』オライリー・ジャパン2010年。
［13］ 北原［2010］，北原宗律『情報社会法』ふくろう出版2010年。