個人情報保護マネジメントシステム

北　原　宗　律

（受付　2007 年 10 月 11 日）

要　　旨

1999年に，JIS 規格として，個人情報に関するコンプライアンス・プログラム要求事項が策定された。2006年に，それが改訂されて，個人情報保護マネジメントシステムとなった。その改訂の理由は，日本の個人情報保護法が制定・施行されたからである。個人情報保護に，マネジメントシステムを構築・運用する意義を検討する。

キーワード　個人情報，マネジメントシステム，個人情報保護法，JIS 規格，PDCA サイクル，リスク

1. は　じ　め　に

JIS 規格である「個人情報保護マネジメントシステム（JIS Q 15001:2006）」は，以前は，「個人情報に関するコンプライアンス・プログラムの要求事項（JIS Q 15001:1999）」と呼ばれていた。そして，2003年に個人情報保護法が制定され，2005年 4 月から全面的に施行された。JIS Q 15001:1999 が JIS Q 15001:2006 に改訂された理由はいくつかある[1)]。ひとつは，コンプライアンス・プログラムが策定されたのが同法制定以前であったため，法律によって新しく導入された概念に対応していないところがあり，法律への適合状況が分かりづらかった，ということである。したがって，同マネジメントシステムを導入・運用すれば，法律の遵守または法律違反がわかりやすくなるというのである。ひとつは，改訂された同マネジメントシステムの方が法律よりも高いレベルを求めている，ということである。そのため，同法では適法であっても，規格上では不適合となる場合が生まれるというのである。それで，法律を超えた高いレベルの個人情報保護水準を満たしているということを対外的にアピールできるということは，事業者にとって大きな利益になるというのである。

このことは，同マネジメントシステムの，法律が設定する基準の「上乗せ」あるいは「横出し」を意味する。筆者は，同マネジメントシステムの法律を超えた水準に大いなる関心を抱いた。環境分野の国の法律と自治体の条例との間で，この「上乗せ」「横出し」議論が起

1）JIPDEC・プライバシーマーク推進センター「JIS Q 15001:2006 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」（2006年）。

こったことがある。そういう議論と同じようなことが，個人情報保護についてもありうるのだろうか。法律の方については，すでにその検証を終えた[2)]。このたびは，個人情報保護マネジメントシステムについて検討してみようと思う。

2. 個人情報保護マネジメントシステムの概要

2.1 個人情報保護マネジメントシステム策定までの経緯

1980年10月，プライバシーの保護および個人データの越境流通に関する OECD 勧告が公表され，そこで個人情報保護に関する八原則が示された。この八原則は個人情報保護という場合に必ず引用されるもので，以後，世界の全ての個人情報保護に関する法令等はこれに準拠しているといっても過言ではない。当然，個人情報保護法も JIS Q 15001 もこれに準拠した内容になっている[3)]。

この OECD 八原則に対応するため，1989年，通商産業省（当時）が「民間部門における電子計算処理にかかわる個人情報の保護について（指針）」を公表した。その後，1995年10月，個人情報保護について大きな転換点となることが起きた。EU が，個人データ保護に関するガイドラインを採択し，加盟各国に，1998年10月24日までに国内法を整備するよう義務づけたことである。特に，個人データの保護水準が低い第三国への個人データの移動を禁止した点が，他地域・諸国に大きな影響を与えた。国際的なビジネスを展開している事業者にとって，これは死活問題である[4)]。

これに対応するため，通商産業省（当時）は上記指針を改定し，1997年，「民間部門における電子計算処理に係わる個人情報の保護に関するガイドライン」を策定した。さらに1999年，そのガイドラインを基に，個人情報保護に関するマネジメントシステム規格として，「個人情報保護に関するコンプライアンス・プログラムの要求事項　JIS Q 15001:1999」が策定された[5)]。

プライバシーマーク推進センターは，「個人情報保護を JIS のマネジメントシステム規格とした意義は，第三者認証制度の普及により，日本の個人データの保護水準を高めることが意図されたと言える」としている[6)]。すなわち，①民間部門の自主的取組の促進，②第三者認証の認証基準とすることにより取組へのインセンティブを確保，③認証基準の明確化により認証制度に対する社会的信頼性を確保，④ JIS 化することによる業種業態を超えた対応の

2） 北原宗律「日本の『個人情報保護法』の問題点」修道法学第29巻第２号（2007年），23頁以下。
3） http://privacymark.jp/pdf/guideline_V1.0_060905.pdf
4） 同上。
5） 同上。
6） 同上。

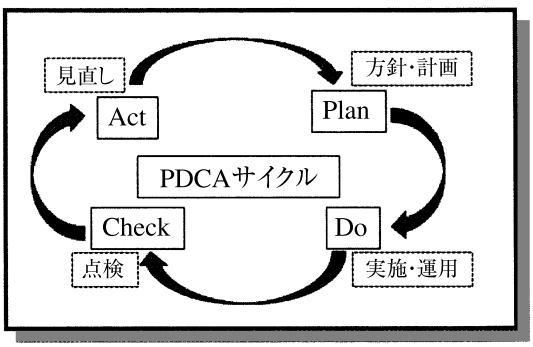
確保，という 4 点のメリットをあげている。

第三者認証制度である「プライバシーマーク制度」は1998年に創設され，その当時は1997年に公表された通商産業省（当時）の上記ガイドラインを認証基準としていたが，その JIS 規格化に伴い，認証基準を JIS Q 15001に変更し現在に至っている。

JIS Q 15001:1999 は，平成17（2005）年 4 月 1 日の個人情報保護法の全面施行を受けて平成18年 5 月に改訂され JIS Q 15001:2006 として公表された。それに伴い，プライバシーマークの認証基準も JIS Q 15001:2006 に移行した。

2.2　個人情報保護マネジメントシステム

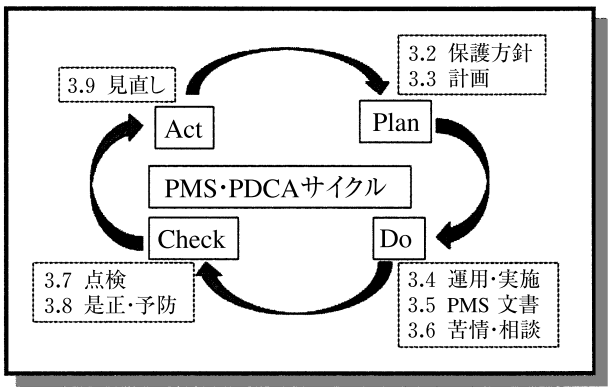
「マネジメントシステム」は，組織の目標や方針を実現し維持する管理手法のひとつである。マネジメントシステム原則は，方針を作成し，それに基づいて計画を作成し（Plan），それを実施し（Do），その実施内容が計画と整合しているかを点検し（Check），点検結果および環境変化等を踏まえて見直しを行う（Act）という一連の活動サイクル，つまり，それぞれの頭文字をとって，「PDCA サイクル」を継続的に繰り返すことにより，事業者の管理能力を高めていくことにある。このようなマネジメントシステムの管理手法を個人情報保護に適用したのが「個人情報保護マネジメントシステム」である。



当 JIS 規格は，その（2.7）において，「個人情報保護マネジメントシステム」を定義づけている。すなわち，それは，「事業者が，自らの事業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」であると。このような管理手法は，品質マネジメントシステム，環境マネジメントシステム，リスクマネジメントシステムなどのマネジメントシステムと共通している。

2.3 個人情報保護 PDCA サイクル

JIS Q 15001:2006 における PDCA サイクルの概要はその要求事項（Requirements）として描かれている。P（Plan：計画）には，3.2（個人情報保護方針），3.3（計画）の各条項が含まれる。D（Do：実施）には，3.4（実施及び運用），3.5（個人情報マネジメントシステム文書）および 3.6（苦情及び相談への対応）の各条項が含まれる。C（Check：点検）には，3.7（点検）および　3.8（是正処置及び予防処置）の各条項が含まれる。A（Act：見直し）には，3.9（事業者の代表による見直し）の条項が含まれる。



3. 個人情報保護マネジメントシステムの実施

3.1 実施ステップ

個人情報保護マネジメントシステムは，英語では “Personal Information Protection Management Systems” と表現されているので，“PMS” と略称することにする。

PMS の実施にあたって，実施ステップを踏まなければならない。実施ステップは13段階から構成されているが，それは，さらに，準備段階，構築段階，および運用段階の 3 つに区分することができる。

①準備段階

S1：PMS 策定のための組織を立ち上げる。

S2：個人情報保護方針を定め，その方針を文書化する。

S3：PMS 策定の作業計画を立てる。

S4：個人情報保護方針を組織内に周知する。

②構築段階

S5：個人情報を特定する。

S6：法令，国の指針（ガイドライン）その他の規範を特定する。

S7：個人情報のリスクを認識し，リスク分析とリスク対策を検討する。

S8：必要な資源を確保する。

S9：PMS の内部規定を策定する。

③運用段階

S10：PMS を周知するための教育を実施する。

S11：PMS の運用を開始する。

S12：PMS の運用状況を点検し改善する。

S13：PMS の見直しを行う。

3.2 PMS の構成

この PMS も一つのマネジメントシステムであることは前述の通りであるが，その要求事項のほとんどが，PDCA に該当する。そのことを明らかにするために，当該 PMS の各条項を PDCA サイクルに分類する。

PLAN（P：計画）

3.3 計画

3.3.1 個人情報の特定

3.3.2 法令，国が定める指針その他の規範

3.3.3 リスクなどの認識，分析及び対策

3.3.4 資源，役割，責任及び権限

3.3.5 内部規定

3.3.6 計画書

3.3.7 緊急事態への準備

DO（D：実施）

3.4 実施及び運用

3.4.1 運用手順

3.4.2 取得，利用及び提供に関する原則

3.4.3 適正管理

3.4.4 個人情報に関する本人の権利

3.4.5 教育

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

3.5.2 文書管理

3.5.3 記録の管理

3.6 苦情及び相談への対応

CHECK（C：点検）

3.7 点検

3.7.1 運用の確認

3.7.2 監査

3.8 是正処置及び予防措置

ACT（A：見直し）

3.9 事業者の代表者による見直し

4. PMS 実施ガイドライン

4.1 個人情報保護方針

PMS（3.2）は，「個人情報保護方針」を規定している。すなわち，「事業者の代表者は，『個人情報保護の理念』を明確にした上で，次の事項を含む個人情報保護方針を定めるとともに，これを実行し，かつ，維持しなければならない（『 』は筆者が挿入）」。そして，「次の事項」に含まれる項目は，a）適切な個人情報の取得，利用及び提供に関すること（「目的外利用」の禁止を含む。），b）個人情報の取り扱いに関する法令，指針等の遵守，c）個人情報の安全対策措置，d）苦情・相談への対応，e）PMS の継続的改善，f）代表者氏名，である。さらに，「事業者の代表者は，この方針を文書化し，従業者に周知させるとともに，一般の人が入手可能な措置を講じなければならない」と規定されている。

「個人情報保護の理念」の明確化・文書化，これが，最大の難関であろう。これが，そのほかの条項に反映するのであるから，PMS 策定組織のなかで，真摯に議論をしなければならない。「理念」は当該事業者が個人情報保護に取り組む姿勢や基本的な考え方を事業の内容と関係づけて記述されるものである。「方針」では，この「理念」と経営責任等を明確にしなければならない。したがって，「方針」「理念」ともに，組織の最高責任機関の決議等が必要である。

「国の指針」とは，各所管庁が作成したガイドライン・指針などである。当該組織の事業内容によって，複数のガイドラインの遵守が必要になることも考えておかなければならない。「その他の規範」には，関係諸外国の「個人データ保護法」や国際団体の条約，ガイドライン等が含まれる。

「方針」の公開方法としては，一般的にはウェブサイトに載せる方法がある。その他，組織のパンフレットやハンドブックに掲載する方法がある。送付の依頼があれば，それにも応えなければならないだろう。

4.2 個人情報の特定

PMS（3.3.1）は，「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」と規定する。もちろん，この規定は，「特定のための手順書」の作成のみを義務づけているわけではない。それどころか，個人情報の特定作業を遂行しなければならない。個人情報を特定するということは，組織が利用する個人情報の範囲を定め，保護管理の対象を明確にするということである。もっといえば，組織が保有するすべての個人情報の「一生」，すなわち，個人情報の「収集」または「誕生」か

ら「消滅」または「廃棄」に至るまでの全過程を漏れなく把握していなければならない。そして，その記録を作成しておかなければならない。

「個人情報の特定」の方法は，個人情報のデータ監査の中でとられる手法または手順とまったく同じものでよい。というのは，データ監査は，個人データ処理の実態を把握するために実施されるものであるからである[7)]。まず，個人情報を含むすべてのデータ・ファイルが特定される。つぎに，「それらの個人情報はどこから来たのか」，「個人情報はどのように収集されたのか」，「個人情報はどのように処理されたのか」，「個人情報はどのように修正されたのか」，「個人情報はどのように開示されたのか」，「個人情報はどこに提供されたのか」，「個人情報はどのくらいの期間保存されているのか」，「個人情報は，いつ，そして，どのような方法で最終的に消去されたのか」，というようなことが明らかにされなければならない。

このようなデータ監査の結果は，個人情報保護方針や個人情報保護の理念に，ある修正をもたらすことになるかも知れれない。そういう意味では，個人情報の特定が何の問題もなく実施できれば，そのことだけで，個人情報保護に関するコンプライアンスを維持しているといえるのである。

4.3　個人情報のリスク認識・リスク分析・リスク対策

PMS（3.3.3）は，「事業者は，3.3.1によって特定した個人情報について，『目的外利用』を行わないため，必要な対策を講じる手順を確立し，かつ，維持しなければならない」と規定する。さらに，「事業者は，3.3.1によって特定した個人情報について，その取り扱いの各局面におけるリスク（個人情報の漏えい，滅失又はき損，関連する法令，国が定める指針その他の規範に対する違反，想定される経済的な不利益及び社会的な信用の失墜，本人への影響などのおそれ）を認識し，分析し，必要な対策を講じる手順を確立し，かつ，維持しなければならない」とする。

PMS は，「目的外利用」「漏えい」「滅失」「き損」「法令・指針等の違反」「経済的不利益」「社会的信用の失墜」および「本人への影響」を「個人情報のリスク」であるとしている。これが「個人情報のリスク認識」である。つまり，個人情報をめぐってこういう種類の問題が発生する危険性があるということである。まず，組織が保有する個人情報のリスク認識からはじめなければならない。

特定した個人情報の収集・取得・入力，編集・接続・照合・修正，移送・送信，利用・加工，保管・蓄積・貯蔵・複製，消去・廃棄・封鎖に至る個人情報処理の連続した流れの各ステップにおいて，適正な安全保護措置を講じない場合に想定されるリスクを洗い出さなけれ

7）北原宗律「個人データ処理と人的設備――データ管理者・データ監査人・データ保護監査人――」広島修道大学経済科学研究第11巻第1号（2007年），88頁。

ばならない。

つぎに，洗い出したリスクを評価する。これが「リスク分析」である。この段階では，そのまま「リスク評価」と呼んでもよい。洗い出したリスクに対して，その評価に相応した合理的な対策を講じなければならない。個人情報の場合，その目的外利用もリスクの一つと考えられる。そいうことが公なれば，個人情報を収集することが難しくなり，個人情報の利用がビジネスの根底にあるならば，それ以上のビジネスの展開に支障を来すことになる。個人情報処理において，前述のリスクが公になった段階で，その組織の社会的信頼は崩れてしまう。そのことは，法律違反においても同様の事態を招くことになる。

そのつぎは，「リスク対策」である。個人情報をめぐるリスクが存在することが認識され，リスクの評価として，損害の程度・範囲・頻度等が明確化されたので，そのリスクに対する安全保護措置の検討に入らなければならない。つまり，事業者は，事業の内容や規模に応じ，経済的に実行可能な，すなわち，合理的な対策を講ずることで十分なのである。

結局のところ，ここでは，「個人情報リスクマネジメントシステム」を構築した方がよい。「マネジメントシステム」が入れ子構造になっているが，同じように，PDCA サイクルを回すのである。（続）