TRC EYE Vol. 63

東京海上日動リスクコンサルティング（株）
所属　リスクコンサルティング室情報グループ
主任研究員　脇田　修二

個人情報保護法とプライバシーマークの相違

１．はじめに

2005 年 4 月 1 日の個人情報保護法（「個人情報の保護に関する法律」平成 15 年 5 月 30 日法律第 57 号）全面施行を境に、個人情報取扱事業者にとって個人情報保護は法律上の義務となった。各事業者は、監督官庁や業界団体からリリースされたガイドラインなどを参考に取り組みを進めているが、法適合の先を目指して「プライバシーマーク」や「ISMS」といった第三者認証を取得する動きも加速している。本稿では、個人情報保護に特化した認証制度として最も実績のある「プライバシーマーク制度」について、個人情報保護法の義務と比較しながら認証取得に必要な取り組みを考察する。

２．プライバシーマーク制度の概要

プライバシーマーク制度は、「JIS Q 15001:1999『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』」（以下、JISQ15001 という）に対する適合性の観点から、事業者における個人情報保護の取り組みを評価する制度である。評価は第三者機関により認証審査として客観的に行われ、適合していると認められた事業者には認定が付与される。認定を受けた事業者は、「プライバシーマーク」と呼ばれるロゴマークを、名刺、ホームページ、店頭、広告用資料等に利用することが許可される。プライバシーマーク取得の最大のメリットは、マークを通じて自らの個人情報の適切な取扱いを一般消費者や取引先などにアピールし、競争上の優位性を得ることであろう。しかし、結果としてのマーク取得ばかりでなく、取得に到る道のりや認証を維持する取り組みの側面から、組織にとって次のような副次的なメリットが存在することがわかる。

- 明確かつ社会的に認知されたゴールを置くことによる緊張感の維持やモチベーションの向上
- 認証審査や取得後の継続審査をトリガーとした形骸化の防止

何より、JISQ15001 で定義された仕組み（マネジメントシステム※1）の構築・運用は、個人情報保護の実効性を担保し形骸化を防ぐ上で極めて効果的なアプローチであることは間違いない。

したがって、認証取得には相応のコスト（ヒト・モノ・カネ）負担を強いられることを差し引いても、取得するあるいは取得をめざすことの意義は大きい。

３．個人情報保護法と JISQ15001 の相違

それではどのような取り組みを行えば、プライバシーマークを取得することができるのだろうか。個人情報を保護する上で満たすべき最低限の水準は、個人情報保護法への適合である。そこで本稿では、既に法適合を果たしている前提で必要となる追加の対応を検討する。これは、プライバシーマークの取得条件が JISQ15001 への適合であることから考えると、『個人情報保護法に定められた義務』と『JISQ15001 に定められた要件』の差に他ならない。すなわち、個人情報保護法では求められていないが JISQ15001 で求められている事項を満たすことが、プライバシーマーク取得への道筋となるのである。

（JISQ15001 の要件）－（個人情報保護法上の義務）⇒プライバシーマーク取得に必要な取り組み

個人情報保護法と JISQ15001 は、共に OECD8 原則※2 という同じルーツを持つため、個人情報の取得・利用の条件、安全管理、第三者提供の制限、個人情報保護に関する教育や苦情対応など、テーマや構成は似通っているものの、定められている内容には異なる部分も多い。両者の内容を比較した結果は次の 4 種類に分類することができる（図 1）。

① 個人情報保護法にのみ規定されている項目
② 両者に規定されており内容が同じ項目
③ 両者に規定されているが内容が異なる項目
④ JISQ15001 にのみ規定されている項目

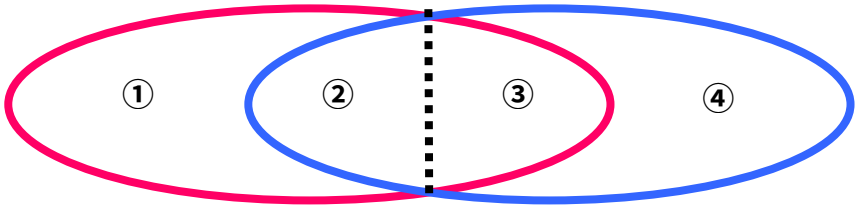

図 1　個人情報保護法と JISQ15001 の比較

本稿では、確実に満たしておかなければならない個人情報保護法に定められた義務（上記①、②）についての解説は割愛し、個人情報保護法と異なる要件、特に追加の対応が必要な部分（上記③および④）について考察する。尚、要点のみついて解説するため、詳細は個人情報保護法および JISQ15001 を直接参照頂きたい。

3．1　両者に規定されているが内容が異なる項目

両者には、趣旨は同じであるが定められた内容の異なる項目が存在する。個人情報保護法の義務が JISQ15001 の要件を包含する項目は特に問題とならないが、個人情報保護法を満たすだけでは JISQ15001 を充足できない項目については追加の対応を行う必要がある。後者について、下表に整理しそれぞれ内容を確認する。

項目	対応する個人情報保護法の条項	対応する JISQ15001 の項番
（Ⅰ）用語の定義	第 2 条　定義	3.　定義
（Ⅱ）取得・利用	第 15 条　利用目的の特定 第 18 条　取得に際しての利用目的の通知等	4.4.2.1　収集の原則 4.4.2.4　情報主体から直接収集する場合の措置 4.4.2.5　情報主体以外から間接的に収集する場合の措置
（Ⅲ）第三者提供	第 23 条　第三者提供の制限	4.4.3.1　利用および提供の原則 4.4.3.2　収集目的の範囲外の利用および提供の場合の措置
（Ⅳ）本人の権利（利用停止請求）	第 27 条　利用停止等	4.4.5.2　個人情報の利用又は提供の拒否権

表 1　両者に規定されているが内容が異なる項目

（Ⅰ）用語の定義

両者はそれぞれ異なる用語の定義を行っている。「取得（個人情報保護法）」と「収集（JISQ15001）」

など本質的な違いのない用語の差異は特に問題とはならないが、保護対象の範囲に関わる用語については確認しておく必要がある（表 2の網掛け部分）。これは、個人情報保護法では個人情報の取扱い形態によって適用される義務の範囲が異なるのに対し、JISQ15001 では原則としてあらゆる個人情報を保護の対象としているためである。

個人情報保護法 （第 2 条　定義）	JISQ15001 （3　定義）	考察
個人情報	個人情報	両者共に同じ用語が用いられており、個人に関する情報であって「特定の個人を識別できるもの（個人情報保護法）」、「当該個人を識別できるもの（JISQ15001）」と定義されている。ただし、個人情報保護法は「生存する個人に関する情報」と対象を限定しているのに対し、JISQ15001 は特に対象を限定していない。
本人	情報主体	「本人」は個人情報から識別される特定の個人と表現されているのに対し、「情報主体」はこれに加えて識別され得る個人も含む。しかし、実務上は問題にならない程度の差異である。
個人情報データベース等 個人データ 保有個人データ	（対応する定義なし）	個人情報保護法のみに採用されている考え方であり、同じ個人情報であっても取扱いの形態により個人情報保護法上の義務が異なる。一方、JISQ15001 の要件はすべての個人情報を対象としている。
個人情報取扱事業者	事業者	個人情報保護法と規格はそれぞれ適用対象としての性格が異なるため単純に比較することはできないが、いずれも法人、団体、個人、営利／非営利によらず個人情報を利用して事業を営むものを指している。

表 2　用語の定義の差異

（Ⅱ）　取得・利用

個人情報の取得（収集）・利用については両者間に大きな差異があり、JISQ15001 では個人情報保護法よりも高いハードルが設けられている。

まず、本人（情報主体）から個人情報を取得する際に通知すべき事項が、個人情報保護法と JISQ15001 で異なる（表 3）。個人情報保護法では取得の際に利用目的のみを伝えればよいとされているが、JISQ15001 は利用目的（収集目的）の他に、組織の個人情報管理者の名前、外部委託する旨（外部委託を行う場合）、個人情報の開示等本人の権利や権利行使の方法などについても伝えなければならないと定めている。

個人情報保護法	JISQ15001
①利用目的 ②共同利用に関する事項（共同利用を行う場合） ③第三者提供に関する事項（第三者提供を行う場合）	①収集目的 ②個人情報に関する管理者の氏名 ③第三者提供の有無、提供先の組織の種類など（第三者提供を行う場合） ④預託の有無（外部委託を行う場合） ⑤個人情報を提供することの任意性と提供しない場合のデメリット ⑥本人の権利および権利行使の方法

表 3　個人情報取得（収集）時に通知すべき事項

また、個人情報保護法では個人情報の取得・利用に際し必ずしも本人の同意を必要としていないが（目的外の利用などの場合を除く）、JISQ15001 は**原則として本人の同意の無い個人情報の収集・利用を認めていない（オプトイン原則※3）**。これは、第三者を介して間接的に個人情報を収集するケースにも適用されるため、同意を得ない限り電話帳や公開された名簿を利用してダイレクトメールを送付したり、テレマーケティングを行うことができない。したがって、このような個人情報の利用を行っている事業者は業務に大きな制約が課せられることになる。

（Ⅲ）第三者提供

個人情報保護法では、取得した個人情報を第三者に提供する場合に「（不特定多数への）第三者提供」と「（限られた範囲での）共同利用」の考え方のいずれか該当する方を適用し、第三者提供を適用する場合には本人の同意、共同利用を適用する場合には必要事項の通知がそれぞれ必要となる。一方、JISQ15001 は共同利用の考え方を認めていないため、提供の範囲が特定／不特定に関わらずすべて本人の同意を得なければならないとしている。また、個人情報保護法で認められている第三者提供のオプトアウト※2 は、JISQ15001 では認められていないため本人の同意が必要となる。したがって、電話帳や名簿の販売などを業として行っている事業者にとっては、本要件がプライバシーマーク取得の高いハードルとなる可能性がある。

（Ⅳ）本人の権利（利用停止請求）

個人情報保護法は、本人から利用停止または第三者提供停止の請求を受けた場合であっても、個人情報保護法に抵触する取扱いを行っていない限り必ずしも請求に応える義務はないとしている。これに対し、JISQ15001 では特に例外を設けることなく、本人から受けた利用停止、第三者提供停止の請求に対して無条件に応えることが求められている。しかし、現実には本人から利用停止などの請求を受けた場合、法的な義務が無くとも顧客満足の観点からはこれに応える努力が求められるため、対応にあたっては大きな違いは無いと言えよう。

３．２　JISQ15001 にのみ規定されている項目

JISQ15001 にのみ規定されている要件は、プライバシーマークを取得するために新たに対応しなければならない。これに該当する項目は大きく「（Ⅰ）マネジメントシステムに関わる要件」と「（Ⅱ）マネジメントシステム以外の要件」の２つのグループに分けることができる。

（Ⅰ）マネジメントシステムに関わる要件

JISQ15001 は、個人情報保護の実効性を担保するためマネジメントシステムとしてのコンプライアンス・プログラムの採用を必須としており、継続的な改善による取り組みの形骸化防止を求めている。このような個人情報保護を実現する仕組みは、個人情報保護法の義務には定めがない（※経済産業省のガイドラインなど各省庁のガイドラインにおいては、同等の仕組みを求めているものもある）。しかし、前述の通り個人情報保護におけるマネジメントシステムが有用なツールであることは間違いなく、その導入は極めて効果が高い。

下表に、JISQ15001 が求めるコンプライアンス・プログラム（マネジメントシステム）の要件を PDCA サイクルのプロセスに沿って整理しておく。

PDCA サイクル	コンプライアンス・プログラムの要件（括弧内は JISQ15001 の項番）
Plan Do	**●個人情報保護方針の策定（4.2）** 個人情報保護に対する事業者の取り組みの方針を定め文書化する。 **●体制と責任の明確化（4.4）** 個人情報保護を実現するために必要な体制を整備する。 ・ 事業者の代表者によるコンプライアンス・プログラムの実質的な管理者の任命 ・ コンプライアンス・プログラムの実施に関する役割、責任、権限の明確化、文書化および周知　など

	●個人情報の特定（4.3.1） 保護の対象とすべき個人情報の特定（棚卸）を行い、台帳などによる管理を行う。また、それぞれの個人情報に関わるリスク（従業員による持ち出し、配送時の紛失など）を評価した上で、合理的な水準の対策を講じる。 **●内部規定の策定と維持（4.3.3）** 個人情報保護方針を具現化して個人情報保護を実現するために、個人情報保護に関する教育や監査などの内部規程（基準、ルール、手順など）を定める。また、事業環境の変化などを勘案した上で、定めた規程の妥当性を維持する。 **●計画の立案と文書化（4.3.4）** 内部規定を運用するための計画を作成して文書化する。 **●文書管理（4.4.8、4.4.9）** 個人情報保護方針や主要な内部規定など、コンプライアンス・プログラムの基本的な要素を文書化し、常に最新の状態で維持する。
Check	**●監査（4.5）** 適切なコンプライアンス・プログラムが確立・運用されていることを、下記の観点から定期的にチェックする。 ・ 定めたコンプライアンス・プログラムが JISQ15001 に適合していること ・ 定めたコンプライアンス・プログラムに従って実際に運用されていること ※ 実際の監査は、内部監査のほか第三者による外部監査などが行われる
Act	**●見直し（4.6）** 監査の結果や事業環境の変化などを考慮し、定期的にコンプライアンス・プログラムを見直し、個人情報保護の取り組みに反映させる。

表 4 コンプライアンス・プログラムの PDCA サイクル

（Ⅱ）マネジメントシステム以外の要件

JISQ15001 には、マネジメントシステムに関わる項目以外にも個人情報保護法には定めのない要件が存在する（表 5）。しかしながら、これらの要件はより適切な個人情報保護を実現するためのオプションであり、かつ個人情報保護を進める上で事業者に特段の負担を強いるものではないため、プライバシーマーク取得を考えていない事業者であっても採用を検討しておきたい。

JISQ15001 の要件（括弧内は JISQ15001 の項番）
法令およびその他の規範（4.3.2） 個人情報保護に関わる法令およびその他の規範を特定して一覧を作成、維持することが求められている。個人情報保護法をはじめ監督官庁のガイドライン、各都道府県の条例、業界の自主ルールなども遵守すべき対象リストアップしておく必要がある。
特定の機微な個人情報の収集の禁止（4.4.2.3） 健康医療、本籍地など機微な情報の取得を、原則禁止している（本人の同意を得た場合には例外的に利用可能）。個人情報保護法には同様の規定はないが、省庁のガイドラインには同等の規制を設けているものもある。

表 5 マネジメントシステム以外の要件

4．まとめ

個人情報保護法の義務を超える JISQ15001 の要件の中には、直接・間接収集におけるオプトイン原則や、共同利用の適用不可など事業者の業態によっては過大な負担を強いるものも含まれるが、多くの要件がより高いレベルで本人の権利を尊重し、またより効果的な個人情報保護を実現するために不可欠な内容であると言える。個人情報保護法は、広くあまねく事業者を対象とする法律であるため最低限守

るべきラインを定めた緩やかな規制となっていることは否めず、お客様などの個人情報を高度に活用して業務を行う事業者であれば、顧客満足の観点からも JISQ15001 の要件を満たして然るべきであろう。特にマネジメントシステムの仕組みを用いた個人情報保護の実現は、個人情報保護法でこそ規定されてはいないが、多くの関連ガイドラインで推奨されていることからも、あらゆる事業者にとって必須の取り組みと言える。

一般消費者や取引先に対してより高いレベルの安心を提供し顧客満足を高めるためには、プライバシーマークの取得を目指す、目指さないに関わらず、個人情報保護法よりも一段高いレベルの対応が求められていることは間違いない。

（注）

※1　マネジメントシステム

JISQ15001 に定義された「コンプライアンス・プログラム」は、個人情報を保護するための体系的かつ経営活動に統合されたマネジメントシステムである。具体的には、ISO9001 の品質マネジメントシステムや ISO14001 の環境マネジメントシステムと共通の考え方が採用され、いわゆる PDCA サイクル（Plan-Do-Check-Act：図 2）により取り組みの形骸化を防止して継続的改善を進める仕組みになっている。

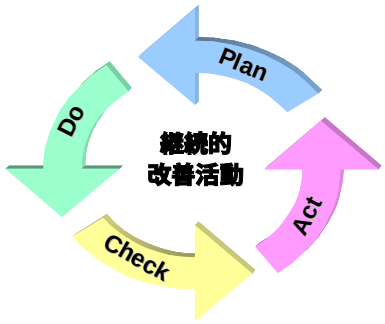

図 2　PDCA サイクルによる継続的改善

※2　OECD８原則

欧・米・日などが加盟する OECD（経済協力開発機構）は、多国間で個人情報をやり取りするうえで満たすべき個人情報保護のレベルを一定程度に保つため、１９８０年に「プライバシー保護と個人データの国際流通についてのガイドライン」を策定し、加盟国はガイドラインに従って自国の法制度を整備することに合意した。このガイドラインに含まれる基本原則がいわゆる「OECD８原則」と呼ばれるものであり、各国ではこれに従って個人情報保護に関する個人情報保護法が制定されている。日本の個人情報保護法もこの「OECD８原則」に従って定められている。8 つの原則は次のとおり。「１.収集制限の原則 （Collection Limitation Principle）」、「２.データ内容の原則（Data Quality Principle）」、「３.目的明確化の原則 （Purpose Specification Principle）」、「４.利用制限の原則（Use Limitation Principle）」、「５.安全保護の原則 （Security Safeguards Principle）」、「６.公開の原則 （Openness Principle）」、「７.個人参加の原則 （Individual Participation Principle）」、「８.責任の原則（Accountability Principle）」。

※3　オプトインとオプトアウト

オプトイン（opt-in）は、「選択」を表す英単語であり（動詞は opt で、「選択する」を意味する自動詞）、本人が選択したサービスのみを提供する場合などに用いられる。例えば、事前に本人が受け取りを許可したダイレクトメールを「オプトインメール（opt-in mail）」と呼ぶ。JISQ15001 における個人情報の収集・利用にはオプトイン原則が採用されており、本人が「同意（選択）」した場合に限り収集・利用が認められている。尚、個人情報保護法における取得・利用は利用目的の通知・公表を義務としているが本人の同意までは求めていない。

これに対し、本人が事前に承諾していないサービスを提供し、本人の拒否によりサービスを停止することをオプトアウト（opt-out）という。例えば、事前承諾を得ずに送付されるダイレクトメールなどで、末尾に「今後このようなご案内が不要の方は、下記連絡先までお申し出下さい」などと記載されている場合がこれにあたり、このような広告を「オプトアウトメール（opt-out mail）」と呼ぶ。個人情報保護法では、個人情報の第三者提供においてオプトアウトが認められており、本人から否定の意思表示を受けた場合に提供を中止する条件を満たせば「同意（選択）」がなくとも、個人情報を第三者に提供してもよいとされている。