

ISO26000と情報倫理

ISO26000 and Information ethics

井 上 尚 之

キーワード：ISO26000、JISQ15001、ISO27001、個人情報保護法、情報倫理

要 約

2011年11月1日に発行されたISO26000は、企業の消費に対する課題として情報に対する課題を含有しているが、本論文ではこの内容を闡明する。そしてISO26000を情報倫理教育に应用できることを主張する。

1. はじめに

社会的責任（Social Responsibility）に関する規格であるISO26000が、ISOにおける規格開発作業の開始から6年を経て2010年11月1日に発行された。ISO26000は、認証目的で用いられない。あくまでもガイダンス（手引き）である。

その内容は社会的責任を果たすための7つの原則、7つの中核主題、36の課題よりなる。その中から、各組織が必要なものを自らが判断選択して取り組んでいくことになる。

本論文は36の課題の1つである「項番6. 7. 7消費者課題5：消費者データ及びプライバシー」を中心に、ISO26000が求める情報倫理について考察する。このISO26000は組織が有する責任であり、個人に対しては適用されない。従ってここでの情報倫理は企業倫理ということになる。

2. 「消費者データ及びプライバシー」とは何か

規格では、「消費者データ及びプライバシー」について次のように説明している。

『消費者データ及び保護プライバシーは、収集される情報の種類、並びに情報の取得、使用及び保護の方法を限定することによって、消費者のプライバシー権を保護することを目的としている。大容量データベースの充実、並びに（金融取引を含む）電子通信及び遺伝子検査の利用増加に伴い、特に個人を特定できる情報に関し、どのように消費者のプライバシーを保護できるのかという問題生じている。

組織は、消費者データの取得、使用及び保護のための厳格なシステムの使用を通じて、自ら

の信頼性及び消費者の信用の維持に寄与することができる。』

さらに関連する行動及び期待として次のような内容を挙げている。

『個人データの収集および処理によってプライバシーが侵害されないよう、組織は次の事項を実施すべきである。』

- (1) 収集する個人データを、製品及びサービスの提供に不可欠な情報、又は消費者が情報を与えられ、自発的に同意した上で提供された情報に限定する。
- (2) サービス利用、又は特別価格の条件として、データの望ましくない利用への同意をマーケティング目的で消費者に求めることは控える。
- (3) 合法的かつ公正な手段だけを用いてデータを入手する。
- (4) 個人データの収集前又は収集時にデータの収集目的を定める。
- (5) 消費者が情報を与えられ、自発的に同意した場合、又は法によって義務付けられている場合を除き、個人データを開示、公開、又はマーケティングを含めた所定の目的以外で使用しない。
- (6) 法の定めに従い、その組織が自分に関するデータを保有しているか否かを検証する権利、及び係るデータに異議申し立てる権利を消費者に与える。異議申し立てが認められた場合には、係るデータは、適宜、消去したり、修正したり、完結したり、又は変更すべきである。
- (7) 十分な安全保護によって個人データを保護する。
- (8) 個人データに関する開発、慣行及び方針を明示して、個人データの存在、性質及び主な用途を速やかに開示する方法を設ける。
- (9) 組織内でデータ保護責任者（データ管理者という場合がある。）の氏名及び通常の勤務場所を開示し、上記の措置及び関連法を順守する責任をこの者に負わせる。

3. 個人情報保護法とISO26000の規格6.7.7との関係

ここでは、日本で2005年4月1日より施行された「個人情報保護法」とISO26000の規格6.7.7との関係を闡明する。

前項の(1)については、個人情報保護法（以下、保護法と略記）の第16条に該当する。

第16条 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。

前項の(2)、(3)については、保護法の第17条に該当する。

第17条 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。

ただし、(2)が不正手段かどうかは決められない面がある。この(2)については、後述の「JISQ 15001の規格3.4.2.2 適正な取得：事業者は、適法、かつ、公正な手段によって個人情報

報を取得しなければならない。」の内容に近い。

前項の(4)については、保護法の第15条に該当する。

第15条 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。

前項の(5)については、保護法の第15条2、第44条に該当する。

第15条2 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44条 認定個人情報保護団体は、認定業務の実施に際して知り得た情報を認定業務の用に供する目的以外に利用してはならない。

前項の(6)については、保護法の第25条、第26条に該当する。

第25条 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。

第26条 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續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。

前項の(7)については、保護法第20条に該当する。

第20条 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。

前項の(8)については、保護法第43条などに該当する。

第43条 認定個人情報保護団体は、対象事業者の個人情報の適正な取扱いの確保のために、利用目的の特定、安全管理のための措置、本人の求めに応じる手續その他の事項に関し、この法律の規定の趣旨に沿った指針（以下「個人情報保護指針」という。）を作成し、公表するよう努めなければならない。

(9)については特に条項は見当たらないが、次章以下で述べるJISQ15001の次の規格が該当する。「規格3. 3. 4 資源、役割、責任及び権限：…事業者の代表は、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責任者を事業者の内部のものから指名し、個人情報保護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。」

次にISO26000規格における「組織は、消費者データの取得、使用及び保護のための厳格なシステム」にはどのようなシステムがあるのだろうか。

4. 情報管理システム プライバシーマーク制度

ここでは、個人情報保護に関する情報システムであるプライバシーマーク制度について概観する。

1980年9月、OECDにおいて「プライバシー保護と個人データの国際流通について」のガイドラインに関する理事会勧告が採択され、そこで個人情報保護に関する8つの原則が示された。世界各国の個人情報保護に関する法令はこれに準拠している。日本の個人情報保護法もこの8原則を基にしている。以下にこの8つの原則を示す。

(1) 収集制限の原則

個人情報の収集には限度があり、かつ収集は適法かつ公正な手段によらなければならない。場合によっては、本人の認識又は同意が必要である。(ISO26000の(3)の一部)

(2) データ内容の原則

個人情報は、利用目的の達成に必要な範囲内において、正確で完全で最新のものでなければならない。(ISO26000の(2)の一部)

(3) 目的明確化の原則

個人情報の収集目的は、遅くとも収集時には特定されていなければならない、その利用収集目的を達成する範囲内に限られる。(ISO26000の(4)の一部)

(4) 利用制限の原則

個人情報は、特定された収集目的を超えて開示、提供又は利用されてはならない。ただし本人の同意がある場合又は法令に基づく場合はこの限りではない。(ISO26000の(5)の一部)

(5) 安全保護の原則

個人情報の保護のために、紛失、無制限でのアクセス、破壊、利用、改ざん又は漏洩といったリスクに対して合理的な安全対策を講じなければならない。(ISO26000の(7)の一部)

(6) 公開の原則

個人情報の取扱いについては公開するという基本方針がなければならない。個人情報の存在や種類、その主要な利用目的、その管理者及び所在地を明確にする手段が容易に利用できなければならない。(ISO26000の(8)の一部)

(7) 個人参加の原則

本人は次の権利を有する。

- (a) 個人情報の管理者等から、当該本人に関する情報を有しているか否か確認を得る。
- (b) 当該本人に関する情報についての本人からの求めに回答を得る（個人情報の管理者は、合理的な期間内で、手数料を定めた場合は合理的な金額で、合理的な方法で、かつ当該本人に容易に理解できる形式で応じなければならない。）。
- (c) 本人の求めに応じない場合にその理由のその説明を求め異議を唱える。
- (d) 当該本人に関する情報の正当性について異議を唱え、もしその主張が正しければ、当該情報は消去又は訂正される。

(ISO26000の(6)の一部)

(8) 責任の原則

個人情報の管理者は、上記(1)～(7)の原則を定めたルールに準拠する責任を負う。(ISO26000の(9)の一部)

この OECD 8 原則に対応するため1989年、通産省は「民間部門における電子計算機処理に係る個人情報保護について（指針）」を公表した。1995年10月に EU で「個人情報保護指令」が採択された。EU 加盟各国は、1998年10月24日までに同指令に従う国内法の整備が義務付けられた。同指令には EU 域内から個人情報の保護水準が低い第3国への個人データの移転禁止が義務付けられていたので他地域諸国へも大きな影響を与えることになった。国際的なビジネスを展開している事業者にとっては大問題となった。

これに対応するため通産省は、上記指針を改定し、1997年3月に「民間部門における電子計算機処理に係る個人情報の保護に関するガイドライン」を策定した。さらにそのガイドラインを基に「個人情報の保護に関するマネジメントシステム規格 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（JISQ15001：1999）」が制定された。

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3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のである。つまり以下に示す狙いがあった。

- ・ 民間部門の自主的取り組みの促進
- ・ 第3者認証の認証基準とすることにより取り組みへのインセンティブを確保。
- ・ 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
- ・ JIS 化することにより業務態を超えた対応の確保

第3者認証制度であるプライバシーマーク制度は1998年4月に創設され、その当時は1997年に公表された通商産業省の上記ガイドラインを認証基準としていたが、その JIS 化に伴い、認

証基準をJISQ15001に変更し、現在に至っている。

JISQ15001：1999は、2005年4月1日の個人情報保護法の全面施行を受けて2006年5月に改正されJISQ15001：2006として公表された。これに伴い、プライバシーマークの認証基準もJISQ15001：2006に移行した。このプライバシーマークを認証している機関は、JIPDEC（現在の一般財団法人日本情報経済社会推進協会）である。

日本がプライバシー制度を第3者認証制度に持ちこんだ背景には、品質マネジメントシステムISO9001と環境マネジメントシステムISO14001の第3者認証の成功がある。ISO本部が発表した（2007年）ISO9001認証組織数は73136であり、中国、イタリアに次ぎ世界3位である。ISO14001認証組織数は27955組織であり、中国に次いで2位である⁽¹⁾。

1993年に日本でISO9001の認証を審査する審査機関をする認定機関として日本適合性認定協会（JAB）が設立された。同年より日本の審査機関がISO9001の認証審査を始めた。1996からはISO14001が発行し、日本の審査機関がISO14001の認証審査を始めた。

しかし、「プライバシー保護」については、1999年時点ではISO化されていなかったもので、日本国内でのみ通用するJISQ15001：1999による第3者認証制度が1999年よりスタートするのである。

さらに環境分野では、環境省が簡易版ISO14001として日本でのみ通用する環境マネジメントシステム認証制度である「エコアクション21」を創設し、2004年10月からスタートさせている。

ここで、次項のISO/IEC 27001：2005と比較するために、JISQ15001の内容を挙げる。

- 1 適用範囲
- 2 用語及び定義
- 3 要求事項
 - 3.1 一般要求事項
 - 3.2 個人情報保護方針
 - 3.3 計画
 - 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 個人条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
 - 3.6 苦情及び相談への対応
 - 3.7 点検

- 3. 8 是正処置及び予防処置
- 3. 9 事業者の代表者による見直し

プライバシーマーク制度はこのJISQ15001を確実に順守しているかどうかを審査する制度である。

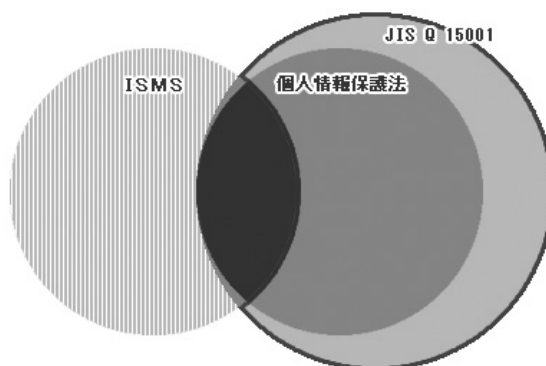
5. 情報管理システム ISO/IEC 27001 : 2005

ISO/IEC 27001 : 2005は2006年に JIS 化され、JISQ27001 : 2006となっている。プライバシーマーク制度と同様に第 3 者認証を行う。ISO/IEC 27001 : 2005の内容を次に示す。

- 1 適用範囲
- 2 引用規格
- 3 用語及び定義
- 4 情報セキュリティマネジメントシステム
 - 4. 1 一般要求事項
 - 4. 2 ISMS (Information Security Management System) の確立及び運営管理
 - 4. 2. 1 ISMS の確立
 - 4. 2. 2 ISMS の導入及び運用
 - 4. 2. 3 ISMS の監視及びレビュー
 - 4. 2. 4 ISMS の維持及び改善
 - 4. 3 文書に関する要求事項
- 5 経営者の責任
 - 5. 1 経営陣のコミットメント
 - 5. 2 経営資源の運用管理
- 6 ISMS の内部監査
- 7 ISMS のマネジメントレビュー
- 8 ISMS の改善
 - 8. 1 継続的改善
 - 8. 2 是正処置
 - 8. 3 予防処置

この規格では個人情報保護というような言葉は全く出てこない。

JISQ15001 (プライバシーマーク制度) と ISO27001 (I S M S) の相違を図示すると次のようになろう。



つまり、JISQ15001は個人情報保護法順守の為の規格であり、ISMS は組織における組織の機密にすべき多様な情報、たとえば会社情報、従業員個人情報、顧客情報、アンケート情報などの機密を保護するためのマネジメントシステムである。これは、「4. 2 ISMS (Information Security Management System) の確立及び運営管理」の部分に該当している。

以上より、個人情報保護法の順守を目指すならば、当然のことながらJISQ15001を選択する。つまり認証取得するならばプライバシーマークということになる。しかしISO27001における組織は、消費者データの取得、使用及び保護のための厳格なシステムの使用を通じて、自らの信頼性及び消費者の信用の維持に寄与することができる。

6. ISO26000とISO27001とJISQ15001の関係

ISO26000における「項番6. 7. 7 消費者問題5：消費者データ及びプライバシー」に近い規格はJISQ15001である。ISO26000における「規格6. 7. 7 消費者問題5：消費者データ及びプライバシー」は、日本の個人情報保護法を超えた内容も含むが、個人情報保護法を順守するために造られたJISQ15001は個人情報保護法を包含すると同時にISO26000における規格6. 7. 7により近い内容になっているといえる。

ISO26000における「項番6. 7. 7(2)サービス利用、又は特別価格の条件として、データの望ましくない利用への同意をマーケティング目的で消費者に求めることは控える。」についてであるが、ISO27001ならば、「4. 2 ISMS (Information Security Management System) の確立及び運営管理」でその部分を文書に明記すればよい。JISQ15001ならば、「3. 4. 5 教育」の教育の部分で教えればよい。

以上より、ISO26000の項番6. 7. 7にある「組織は、消費者データの取得、使用及び保護のための厳格なシステムの使用を通じて、自らの信頼性及び消費者の信用の維持に寄与することができる。」のくだりのシステムはつづまるところ、ISO27001とJISQ15001のどちらでも可能ということになる。

7. 情報倫理教育

ISO27001では、4. 2. 2のe)に「教育・訓練及び意識向上のためのプログラムを実施する」とあり、5. 2. 2は、「教育・訓練、意識向上及び力量」の項目が挙げられている。また、JISQ15001には「3. 4. 5 教育」の項目がある。

これらの教育の内容に、ISO26000の「項番6. 7. 7 消費者課題5：消費者データ及びプライバシー」を取り上げるべきであることを、筆者は提案したい。

さらに、情報倫理教育として、企業は消費者に対する情報発信についても教育すべきと筆者は考える。消費者に対する情報発信については、ISO26000では次の項番がある。

「6. 7. 3 消費者課題1：公正なマーケティング、事実に即した偏りのない情報、及び公正な契約履行」

この項番の説明は要約すると次のようになる。

- ・公正なマーケティング、事実に即した偏りのない情報、及び公正な契約履行を通じて、消費者が理解できる製品及びサービスに関する情報が提供される。
- ・消費者は、この正しい情報を得た上で消費及び購買に関する決定を下したり、異なる製品及びサービスの特徴を比較することができる。
- ・責任あるマーケティングを行うためには、ライフサイクル及びバリューチェーン全体における社会的、経済的及び環境的影響に関する情報の提供が必要となる。
- ・供給業者によって提供される製品及びサービスの詳細情報は、消費者が入手できる唯一のデータであるため、この情報は購買の意思決定において重要な役割を果たす。
- ・不公正、不完全、誤解を招く又は虚偽的なマーケティング及び情報は、消費者のニーズを満たしていない製品及びサービスの購入という結果をもたらし、資金、資源及び時間の浪費につながるばかりでなく、消費者又は環境を害する。さらに消費者が誰に又は何を信頼してよいのか分からなくなるため、消費意欲の低下につながる。これはより持続可能な製品及びサービスに向けた市場の成長に悪い影響を及ぼす可能性がある。

現在、情報倫理を扱う教科書は多く販売されている。これらの教科書は、企業のみならず、大学でも使用されている。その内容は、ITを利用するときの行動規範が主である。法律では、「個人情報保護法」「著作権法」を主として扱っている。

しかしながら多くの情報倫理を扱った教科書には正しい情報を消費者に与えることが重要であるという視点が欠落している。「公正なマーケティング、事実に即した偏りのない情報」を供給者が行うことがいかに重要であるかを知ることが、企業と消費者の両者の利益になり、最終的にはマーケットの拡大につながることを理解させることが重要である。これは、情報倫理を包含する職業倫理に近いものであるといってもよいかもしれない。

企業では、ISO26000の「項番6. 7. 7 消費者課題5：消費者データ及びプライバシー」

および「6. 7. 3 消費者課題1：公正なマーケティング、事実に即した偏りのない情報、及び公正な契約履行」は情報倫理教育に是非とも取り入れたい内容である。さらに現在就職難に悩む大学生に対しても職業倫理を含む情報倫理教育として取り入れていきたい内容である。

8. 結論

いままで議論してきたことを箇条書きにしてまとめ結論としたい。

- (1) ISO26000において情報セキュリティを扱っている部分は、「項番6. 7. 7 消費者課題5：消費者データ及びプライバシー」である。
- (2) 「項番6. 7. 7 消費者課題5：消費者データ及びプライバシー」は、個人情報保護法と概ね重なるが、一部その範囲を超えている。しかし、個人情報保護法の第3者認証を目指した規格であるJISQ15001は個人情報保護法よりもよりISO26000の項番6. 6. 7に近い。
- (3) ISO27001は組織における組織の機密にすべき多様な情報、たとえば会社情報、従業員個人情報、顧客情報、アンケート情報などの機密を保護するための第3者認証を伴うマネジメントシステムである。
- (4) ISO26000の項番6. 7. 7にある「組織は、消費者データの取得、使用及び保護のための厳格なシステムの使用を通じて、自らの信頼性及び消費者の信用の維持に寄与することができる。」のくだりのシステムはつづまるところ、ISO27001とJISQ15001のどちらでも可能。
- (5) 企業の従業員に対する情報倫理教育においては、消費者保護という視点が欠落している。「公正なマーケティング、事実に即した偏りのない情報」を供給者が行うことがいかに重要であるかを知ることが、企業と消費者の両者の利益になり、最終的にはマーケットの拡大につながることを理解させることが重要である。
- (6) ISO26000の「項番6. 7. 7 消費者課題5：消費者データ及びプライバシー」及び「項番6. 7. 3 消費者課題1：公正なマーケティング、事実に即した偏りのない情報、及び公正な契約履行」の部分は企業の情報倫理教育のみならず大学の情報倫理教育に使用すれば有用であろう。

註

- (1) 「The ISO Survey-2007」『ISO ホームページ』<http://www.iso.org/survey2007.pdf>

(引用文献)

- ・日本規格協会編『ISO26000：2010社会的責任に関する手引き』（2011、日本規格協会）
- ・財団法人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編『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2版）』（2010、日本規格協会）
- ・平野芳行・吉田建一郎『ISO/IEC 27001：2005（JISQ27001：2006）詳解情報セキュリティマネジメントシステム—要求事項』（2011、日本規格協会）

(参考文献)

- ・小暮仁『教科書情報倫理』(2008、日科技連)
- ・佐々木良一、会田和弘『情報セキュリティ入門—情報倫理を学ぶ人のために』(2010、共立出版)
- ・情報教育学研究会・情報倫理教育研究グループ『インターネット社会を生きるための情報倫理 2011 インターネット』(2011、実教出版株式会社)
- ・静谷啓樹『情報倫理ケーススタディ』(2008、サイエンス社)
- ・村田潔編『情報倫理—インターネット時代の人と組織』(2004、有斐閣選書)
- ・ISO/IEC 編著、JIPDEC 監訳『わかりやすい情報セキュリティマネジメントシステム ISO/IEC 27001実践ガイド』(2011、日本規格協会)