研究ノート

JIS　Q　15001

楊　　永城

（受付　2009 年 6 月 1 日）

目　　次

1. は　じ　め　に

1990年代に入って，情報処理技術の著しい発展は，パソコンによる大量，かつ，迅速的な情報処理を可能とし，個人のクレジットローンや消費者信用取引などにおいて，ニーズの多様化，個性化に対応した効率的な事業活動の発展を容易にしている。しかし，こうした情報化の急速な展開に伴って，さまざまな事業者が情報システムを利用し，個人情報を取扱うことが可能となった結果，個人情報が分散した形で保存・利用することが多くなり，情報の不適切な利用，改ざんなどが行われる恐れが高まってきている。このため，個人情報の適切な利用と保護が極めて重要となってきた。

前述の状況の下で，JIS　Q　15001：1999，個人情報保護法，個人情報保護ガイドライン，個人情報マネジメントシステムの重要性を明らかにすることに，学問的関心が移ってきた。そして個人情報保護法，個人情報保護ガイドライン，個人情報マネジメントシステムなどとの比較において，JIS　Q　15001：2006 を中心的課題として検討を行いたいと考えている。

本小論においては，まず，これまでの経緯を説明し（2）JIS　Q　15001 の概要を説明する（3），つぎに，この規格と個人情報保護法とを比較検討し（4），そして，この規格と個人情報保護ガイドライン（総務省の国民生活局ホームページ）とを比較検討する（5）。それらの検討を踏まえて，同規格と PMS（Protection Management Systems）との関係（6），同規

格とプライバシーマーク制度との関係を明らかにする（7）。

2. これまでの経緯

日本の政府においても，さらに国際的にも，個人情報セキュリティの強化に向けた取組が行われてきている。日本の政府は情報セキュリティに国民の関心を集めるために「国民のための情報セキュリティサイト」を運営している[1)]。国際的取組としては1970年代から，欧米諸国において，個人情報に関する法制の整備が進められ，1980年には，各国の規制の内容の調和を図る観点から，経済協力開発機構（OECD）[2)] 理事会勧告において，「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」が示された。その後1995年には EU 個人情報保護指令が出された。

このような状況を鑑みて，情報セキュリティに関する各種の「ガイドライン」が公表されてきた。例えば国土交通省ガイドライン，総務省ガイドライン，内閣官房情報セキュリティセンターガイドラインである。これらのガイドラインのほかに民間部門が取組んでいる自主規制として，日本工業規格（JIS）の「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年 3 月20日告示）とプライバシーマーク制度がある。

1989年，通商産業省が「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ついて」を公表し，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年にそのガイドラインを元に，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。2006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。

「JIS　Q　15001：1999」が「JIS　Q　15001：2006」に改定された理由は，大きく 2 つのポイントがある。一つは，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わかりづらかった，ということである。二つは，改定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[3)]。つまり，必要として最小限度の保護レベルを規定している個人情報保護法より高いレベルが要求されていることになる。

1）http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/

2）OECD：経済開発協力機構　1950年設立　本部パリ　現在参加国数は30カ国。
出所：http：//www.bvdp.de/index.htm?/files/politik-recht/

3）北原宗律「個人情報マネジメントシステム」『経済科学研究』広島修道大学経済科学会，第 9 巻第 2 号2006年，199頁。

3.　JIS　Q　15001 の概要

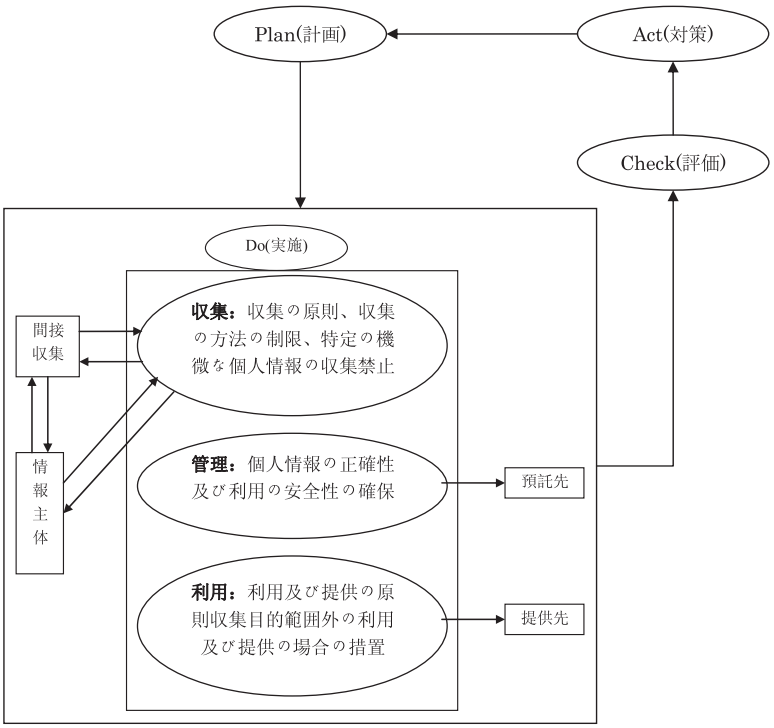
JIS　Q　15001 は，日本規格協会が発行した個人情報保護の基準を定めた JIS 規格の名称である。日本工業規格（Japanese Industrial Standards）の「鉱工業品」である「電子計算機」の「使用方法」に関する「管理システム」国家の統一的な工業標準をいう。Q は，「管理システム」を示す分類記号であり，15001は管理システム中の分類を示している（大分類 1，中分類 5，規格001）。原案は旧通産省のガイドラインを基に財団法人日本規格協会が作成し，日本工業標準調査会の審議を経て，通商産業大臣が「JIS　Q　15001」を策定した[4)]。

日本工業規格は工業標準化法第15条に基づき，5 年ごとに見直しを行うことになっている。1999年に作成された JIS　Q　15001 も2004年中に見直しを終える予定であった。しかし作業には着手していたものの，一時中断された。この間に個人情報保護法の成立・一部が実施された。「個人情報の保護に関する法律施行令」など政令が成立・施行し，「個人情報の保護に関する基本方針」の公表し，そして，「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」が公示されるなど，日本の個人情報保護法制が本格的に整備される時期であった[5)]。

JIS　Q　15001：1999 は，個人情報保護に対する事業者全体の取り組みを基準化しており，①個人情報方針の決定，②個人情報保護計画の策定（個人情報の特定・法令およびそのほかの規範・内部規程・計画書，③実施および運用（体制および責任，個人情報の収集に関する措置―収集の原則・収集方法の制限・特定の機微な個人情報の禁止・情報主体から直接収集する場合の措置・情報主体以外から間接的に収集する場合の措置，個人情報の利用および提供に関する措置―利用および提供の原則・収集目的の範囲外の利用および提供の場合の措置，個人情報の適正管理義務―正確性の確保・安全性の確保・委託処理に関する措置，情報主体の権利―個人情報に関する権利・利用または提供の拒否権，教育，苦情および相談，コンプライアンス・プログラム文書，文書管理），④審査・監査，⑤見直しという作業を行う。そして，この作業を繰り返すことにより，個人情報の管理システムを継続的に改善するという仕組みを取っている[6)]（図 1 ）。

2006年版は1999年版よりさらにマネジメントシステムのため規格として強調されている。①計画の面（Plan）でリスクなどの認識・分析及び対策，緊急事態への準備や点検などに強

4）北原宗律「個人情報マネジメントシステム」『経済科学研究』広島修道大学経済科学会，第 9 巻第 2 号2006年，19頁。
5）参照：鈴木正朝「JIS　Q　15001 個人情報保護マネジメントシステム入門」日本規格協会，2008年10頁。
6）岡村久道，新保史生「電子ネットワークと個人情報保護」経済産業調査会1998年，234頁。



出所：http://www.tokiorisk.co.jp/consulting/security/program.html

図 1　コンプライアンス・プログラムとは（一部を改変）

	目次の順番	JIS　Q　15001：2006（新追加）
1.	4.3.3	リスクなどの認識・分析及び対策
2.	4.3.7	緊急事態への準備
3.	4.4.1	運用手順
4.	4.4.2.1	利用目的の特定
5.	4.4.2.7	本人にアクセスする場合の措置
6.	4.4.3.3	従業者の監督
7.	4.4.4.2	開示などの求めに応じる手続き
8.	4.4.4.3	開示対象個人情報に関する周知など
9.	4.4.4.4	開示対象個人情報の利用目的の通知
10.	4.4.4.5	開示対象個人情報の開示
11.	4.4.4.6	開示対象個人情報の訂正，追加又は消除
12.	4.5.1	文書の範囲
13.	4.5.3	記録の管理
14.	4.7.1	運用の確認
15.	4.8	是正処置及び予防処置

出所：JISC　日本工業標準調査会
http://www.meti.go.jp/policy/it_policy/privacy/jis_shian.pdf

図 2　JIS　Q　15001 の新追加の項目

化し，具体的になった。②実施及び運用の面（Do）で利用目的の特定，本人にアクセスする場合の措置，従業者の監督を加えた。また，開示になどの求めに応じる手続，開示対象個人情報に関する周知など，開示対象個人情報の利用目的の通知，開示対象個人情報の開示，開示対象個人情報の訂正・追加又は消除について取り上げ，事業者に義務を規定された。さらに文書の範囲を説明し，記録の管理も強調され，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証するために必要な記録を作成し，維持しなければならない。③点検の面（Check）では運用の確認を追加し，事業者は，個人情報保護マネジメントシステムが適切に運用されていることを事業者の各部門及び階層において定期的に確認しなければならない。さらに，是正処置及び予防処置には5つの手順があって，確立・実施・維持しなければならない。④見直し（Act）6つの観点から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ればならない（図2）。

4.　JIS　Q　15001と個人情報保護法

1970年代に入り，欧米諸国では，個人情報保護やプライバシー保護を目的とする法律が制定され始めた。1980年に，OECD（経済協力開発機構）においては，個人データの自由な流通とプライバシー，個人の自由の保護との調和を図ることを目的として，1980年9月に，「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に関する理事会勧告」が制定された。また，CE（欧州評議会）においても，「個人データの自動処理に係る個人の保護に関する条約」が採択されている。

日本においては，ICT化の進展と前述のOECD勧告を踏まえて，行政機関向けの個人情報保護法（正式には，行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律）が1988年に制定された[7)]。この法律は，行政機関の保有する電子計算機処理に係わる個人情報の取り扱いに関する基本的事項を定めることにより，個人の権利利益を保護することを目的としている。

2004年にJIS　Q　15001は一時中断され，この期間は日本の法律の1つで，個人情報保護法（正式名称は「個人情報の保護に関する法律」）が2005年4月1日より全面施行され，個人情報に関して本人の権利や利益を保護するため，個人情報を取扱う事業者などに一定の義務を課す法律である[8)]。

7）この法律の概要及び問題点については，参照，北原宗律「わが国の『個人情報保護法』の問題点――その基本的構成をめぐって――」『法とコンピューター』　No. 8　1990年，65－83頁。

8）この法律の概要及び問題点については，参照，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，201－224頁。

一方，JIS　Q　15001：1999 が2006年 5 月に改訂され「JIS　Q　15001：2006」として公表された。「マネジメントシステムを構築・維持するための項目」と「個人情報の取扱に関する項目」では，大別することができる。JIS　Q　15001：2006 における要求事項は個人情報を適切に保護し，管理するために必要な PDCA を規定したものであり，その内容も個人情報保護法それ自体が規定するところに比べ法律より詳細である。

JIS　Q　15001：2006 とは，個人情報保護を進めるために必要とされる要求事項を定めたものであり，業種・規模を問わずすべての事業者に対して適用可能なものである。

個人情報を特定個人の識別情報として定義する点で基本的に異なるところはない。しかし，個人情報保護法は，「生存者」，「個人に関する」，「特定の個人を識別する」情報に限定している。JIS　Q　15001：2006 は，生存者に限定せず，個人情報保護法よりも範囲が広くなっている。さらに JIS　Q　15001：2006 は，「特定の機微な個人情報」[9] という概念を採用しており，個人情報を機微かどうかという観点から区分し，特定の機微な個人情報に該当するものにいついては，特に厳格な取扱いを求めている（図 3 ）。

項　　目	個人情報保護法と異なる点
同意取得の原則	本人から直接書面にて個人情報を取得する場合は，必要事項を通知し，同意を得なければならない。この内容は個人情報保護法にはない。
機微な情報の取扱の制限	特定の機微な個人情報の取得，利用又は提供は，行ってはならない。取得，利用又は提供を行う場合は，明示的な本人の同意を得なければならない。この内容は個人情報法にはない。
個人情報に関する本人の権利	①対象個人情報の範囲 本人からの開示等の求めに応じなければならない個人情報を「開示対象個人情報」と定めている。これは法律の「保有個人データ」とほぼ同義である。しかし，法律では政令によって，6 ヶ月以内に消去するものは対象外なのに対し，JIS　Q　15001 では，そのような期間に関する定義はない。 ②利用停止等の求めについて 法律では，法令に違反した場合に，事業者は本人からの個人情報の利用停止などの求めに応じなければならない。一方，JIS　Q　15001 では本人からの求めに対して原則すべて応じなければならない。

出所：下島和彦，清水口咲子「個人情報保護マネジメントシステムの構築実例集」日科技連 6 頁

図 3　JIS　Q　1500：2006 と個人情報保護法の異なる点

9）特定の機微な個人情報とは，本人の思想，信条に関する事項や人種，勤務先，地位，学歴，本籍地，身体・精神障害に関する事項，犯罪歴，保健医療に関する事項など，「センシティブ情報（Sensitive Information）」と呼ばれる。

5. JIS Q 15001と個人情報保護ガイドライン

2005年4月1日より，個人情報保護法が全面施行され，事業者は個人情報の適正な取扱が求められることとなった。経済産業省においては，個人情報保護法で規定された事業者の義務規定をより具体化・詳細化し，経済産業分野の事業者及び業界団体等における個人情報保護の取組みを促すために，ガイドラインを策定・見直し，個人情報保護法及びガイドラインの普及啓発に努めている[10)]。

国の行政機関や地方公共団体などの公的部門の個人情報の制度化が立法によって進められてきた一方，民間部門の個人情報保護は，立法には消極的で自主規制に任せられてきた。最初に作成された民間部門のガイドラインは，1987年の財団法人金融情報システムセンター（FISC）の「金融機関などにおける個人データ保護のための取扱指針」である。翌年，財団法人日本情報処理開発協会（JIPDEC）が「民間部門における個人情報保護のためのガイドライン」を策定した。また，旧行政機関個人情報保護法の立法過程で，衆参両院で「民間部門にも必要な共通課題となっている現状にかんがみ，政府は早急に検討を進めること」との附帯決議がなされたため，政府においては，主に旧通産省（現在，経済産業省）を中心として民間部門における個人情報の保護の検討が進められた。ここでは，個人情報保護に関する作業部会を新たに設置し，指針・ガイドラインを策定するという形式が取られた。そして，関係事業者団体に対しては，このような指針やガイドラインは，情報化の進展や個人情報漏洩問題に伴い改訂され，関係事業者団体に示され，普及啓発活動が行われてきた。

政府の主なガイドラインとしては，旧通産省の「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」や旧郵政省（現在，郵政事業庁）の「電気通信事業における個人情報保護に関するガイドライン」，「放送における視聴者の加入個人情報の保護

個人情報の保護に関するガイドラインについて 平成20年4月1日現在 総務省の国民生活局	
1. 民間事業者	事業等を所管する各省庁において，審議会の議論等を経て，24分野について37のガイドラインを策定。
2. 行政機関	総務省において，各行政機関及び独立行政法人等の安全確保措置についてのガイドラインを策定。2分野：行政機関と独立行政法人2ガイドライン

出所：http://www5.cao.go.jp/seikatsu/kojin/gaidorainkentou.html

図4 内閣府国民生活局個人情報保護の個人情報保護に関するガイドラインについて

10）http://www.meti.go.jp/policy/it_policy/privacy/

に関するガイドライン」及び「発信者情報通知サービスの利用における発信者個人情報の保護に関するガイドライン」などがある。これらのガイドラインは，OECD 8 原則や EU 指令を参考にしている。関係事業者団体の個別ガイドラインはこれら省庁のガイドラインに拠りながら作成されるため，勢い同原則・指令に類似する内容となっている[11)]（図 4 ）。

6. JIS Q 15001 と個人情報保護マネジメントシステム

個人情報保護マネジメントシステム規格である JIS Q 15001：2006 は，マネジメントシステムを作成する場合の国際規約である ISO Guide 72（「マネジメントシステム規格の

共通分野	要　素
1. 方　針	1.1 方針及び原則
2. 計画策定	2.1 ニーズと要求事項の特定及び重要な問題の分析
	2.2 対応すべき重点項目の選択
	2.3 目的及び目標の策定
	2.4 資源の特定
	2.5 組織体制，役割，責務，権限の明確化
	2.6 運営プロセスの計画
	2.7 予見可能な事柄に関する不測の事態への準備及び対応
3. 実施及び運営	3.1 運営管理
	3.2 人的資源のマネジメント
	3.3 その他の資源運用管理
	3.4 文書化及びその管理
	3.5 コミュニケーション
	3.6 供給者及び請負契約者
4. パフォーマンスの評価	4.1 監視及び測定
	4.2 不適合の分析及び取扱
	4.3 マネジメントシステムの監査
5. 改　善	5.1 是正処置
	5.2 予防処置
6. マネジメントレビュー	6.1 継続的改善
	6.2 マネジメントレビュー

出所：五井　孝，稲垣隆一「プライバシーマークのための JIS Q 15001 の読み方」日科技連 9 頁

図 5　ISO Guide 72 に示されるマネジメントシステムの共通要素

11）参照：総務省国民生活局「個人情報保護に関するガイドラインについて（平成20年 4 月 1 日）」

正当性及び作成に関する指針（2001）」）に従って作成されている。例えば品質マネジメントシステム・環境マネジメントシステムやリスクマネジメントシステムなどがある。これらのマネジメントシステムに共通のマネジメントシステム原則を採用している（図5）。

JIS　Q　15001：2006にはマネジメントシステムの考えが取入れられている。その趣旨は，方針を作成し，「必要な最小限を守る義務」に基づいて，組織が方針および目標を定め，計画を作成し（Plan），実施し，（DO），点検し（Check），見直し（Act）を行うという，いわゆるPDCAサイクルをスパイラル的に継続することにより，事業者の管理能力を高めていくことにある。この仕組みを採用することで，事業者は個人情報の保護レベルを上げていく，目標を達成することが期待される。

個人情報は，組織における重要な情報資産のひとつである。情報資産を保護し，適切に関するためのプレームワークとして，情報セキュリティマネジメントシステム（ISMS：Information Security Management System）がある。情報セキュリティマネジメントシステムの国際認証規格である。「ISO/IEC27001：2005情報技術―セキュリティ技術―情報セキュリティマネジメントシステム―要求事項」の「A.15　順守」の中に「A.15.1.4　個人データ及び個人情報の保護」として「個人データ及び個人情報の保護は，関連する法令，規制，及び適用がある場合には，契約条項の中の要求に従って確実にしなければならない。」と規定されている。

JIS　Q　15001とISO　27001を比較すると，その共通点はどちらもマネジメントシステムを構築するということである（図6）。

	JIS　Q　15001	ISO　27001
対　　象	個人情報	資　　産 1.　情報資産（個人情報含む） 2.　ハードウェア 3.　ソフトウェアなど
内　　容	個人情報のライフサイクル（取得，利用，保管，提供，委託，廃棄など）全般にわたる個人情報の取扱にかかわるマネジメントシステム	情報システムを中心とした情報セキュリティにかかわるマネジメントシステム

出所：五井　孝，稲垣隆一「プライバシーマークのためのJIS　Q　15001の読み方」日科技連11頁

図6　JIS　Q　15001とISO　27001の比較

7.　JIS　Q　15001とプライバシーマーク制度

1980年のOECDガイドライン8原則（収集制限，データの正確性，目的明確化，利用制限，安全保護，公開，個人参加，責任）を踏まえ，1989年の通商産業省（現在経済産業省）

の「民間部門における個人情報保護のためのガイドライン」に準拠し，個人情報の取扱を適切に行っている民間事業者に「プライバシーマーク」の使用を認める制度である。1998年4月1日より運用を開始した。その後，2006年5月よりプライバシーマークの認定基準であるJIS　Q　15001：1999が7年ぶりに改正され，2006年JIS　Q　15001：2006（マネジメントシステム―要求事項）になり，個人情報保護を進める上で事業者に対し一つの指針を示すものである。旧版である1999年版から今回の改正までの間に，個人情報に関わる大きな動きがあったのは，2005年全面実施された「個人情報の保護に関する法律」（以下，個人情報保護法という）。いわゆる「個人情報保護法」の成立，施行である。この法律によって，個人情報を取扱っている企業などの事業者は，個人情報を適切に管理し，保護することを義務付けられることとなった。

こうした中で，既に5,932社の事業者がプライバシーマークの認定を受けている[12)]。主体的にプライバシーマークを取得して，個人情報の管理強化を図るとともに，企業価値を高めようとしている事業者が増え続けている。

プライバシーマークを取得する上ではJIS　Q　15001に準拠しなければならない。逆に，JIS　Q　15001の要求事項を満たしていれば，個人情報保護法で規定されている本人の保護に直接関わる事項は満たされる。

プライバシーマーク制度とは，JIS　Q　15001に適合したコンプライアンス・プログラムを整備し，個人情報の取り扱いを適切に行っている事業者に対し，第三者機関である財団法人日本情報処理開発協会（JIPDEC）およびその指定機関が評価・認定し，その証としてプライバシーマークというロゴの使用を許諾する制度である。

「個人情報」の英訳「Personal Information」の頭文字「P」「I」を組み合わせて擬人化し，これを楕円で囲むことにより，「個人の情報が保護されている」というイメージを表現した。次に，「P」は「Privacy」「Protect」（守る，保護する）の頭文字でもあるので，特に象徴的に用いて，目立つようにしている（図7）。

プライバシーマーク制度の目的は，①民間事業者が個人情報保護に関する信頼確保へのインセンティブを提供し，個人情報保護システムの確立を促進（JIS　Q　15001の普及）することと，②一般消費者が事業者の個人情報の取り扱いの適切性を容易に判断できる材料（マーク）を提供し，もって個人情報を自分で守る意識の向上を図ることである。

具体的な運用は，JIPDEC（日本情報処理開発協会）が制度全体の運営管理を行い，業界団体ごとにプライバシーマーク付与認定指定機関を指定する。2002年4月現在で，指定機関として指定されているのは，情報サービス産業協会，日本マーケティングリサーチ協会，全

12）財団法人情報処理開発協会　プライバシーマーク推進センター「プライバシーマーク付与認定事業者数が8,000を超える」平成21年3月19日

出所：http://www.privacymark.jp/privacy_mark

図 7　プライバシーマークのデザインと各部分の説明

国が学習塾協会の 3 機関である。これらの指定機関が事業者からのマーク取得申請を受理し，JIS　Q　15001 に基づいた個人情報保護を行っているか否かを審査（書類審査と現地審査）し，マーク使用許諾を認定する（図 8 ）。

農　　業	2社	運輸・通信業	406社
林　　業	0社	卸売・小売業，飲食店	730社
漁　　業	0社	金融・保険業	205社
鉱　　業	0社	不動産業	144社
建 設 業	91社	サービス業	7,395社
製 造 業	1,253社	公　　務	0社
電気・ガス・熱供給・水道業	10社	分類不能の産業	0社

出所：http://www.privacymark.jp/certification_info/list/clist.htm

図 8　平成21年 4 月までのプライバシーマーク使用許諾事業者業種に分け

マーク付与の認定を受けた事業者は，マーク使用料を支払い，マークの使用を行うことができる。2 年ごとに更新が可能である。認定後には指定機関または JIPDEC が，消費者からのクレームなどを受け，報告書の提出を求め調査を行ったうえ，改善の必要性のある場合には改善の勧告や要請を行う。事業者がこれに従わない場合には，マークの使用許諾の認定が取り消される。

なお，現在ではアメリカの BBBOnline（Better Business Bureaus OnLine）[13] との相互マークの申請により，事業者が英語版のインターネット・ホームページにおいて相互マークを使用し，国外の消費者に対しても個人情報の保護の適切性を示すことができるようになっている。プライバシーマークに類似の制度としては，財団法人日本データ通信協会の個人情報保護マーク制度がある。これは，電気通信事業者及び発信者情報通知サービス（ナンバーディスプレイ）の事業を行っている事業者を対象に，旧郵政省の「電気通信事業における個人情報保護に関するガイドライン」に準拠した社内制度をとっていることの認定を受けるものである[14]。

8. JIS　Q　15001：2006 の問題点

これまでの研究おいて，以下のような問題点が明らかになった。したがって，これらの問題点を今後の研究課題としたい。

1.「個人情報保護法」実施などに伴う改定ということで，センシティブ情報の原則取得禁止は従前の JIS と同じで，法律にはない原則である。

2. JIS　Q　15001 が「個人情報保護法」に上乗せ・横出しになり，今後「個人情報保護法」を強化し，適切な見直しが必要となる。

3. 従業者教育：JIS　Q　15001：2006 の4.4.5（教育）において，従業者に個人情報保護マネジメントシステム（PMS）の運用を確実に実施できる力を備えさせるための教育について規定されている。教育を効果的に実施することは難しいが，アンケートや小テストの実施などにより，従業者の理解度を把握し，教育の内容及び実施方法などについて，定期的に評価を行い，直しを行うことが重要だと思う。また，教育を受けたことを自覚させる仕組みを取り入れることも重視すべきである。

4. 一方，JIS　Q　15001：2006 の4.4.3.3（従業者の監督）において，安全管理措置の遵守について，従業者に対し必要かつ適切な監督を行うことを規定している。従業者との雇用契約時または委託契約時に，個人情報の非開示契約の締結や PMS に違反した場合の措置の実施などが，内部犯罪・内部不正行為の抑止にも繋がることを認識し，従業員の監督を行うことも重要である。

13）BBBOnLine：（Better Busness Bureaus OnLine）とは，米国でプライバシーマーク（シール）を認定，発行している機関のことである。米 Council of Better Business Bureaus（CBBB ＝商事改善協会）は，従来のビジネスモデルで「品質保証」制度を実施してきた実績を持っており，インターネットビジネスに対して信頼性を保証する子会社として BBBOnLine 社を設立した。
http://www.secomtrust.net/secword/bbbonline.html

14）三宅　弘，小町谷育子「個人情報保護法―逐条分析と展望」青林書院2003年 9 月77頁。

5. 外部委託先などの管理：JIS　Q　15001：2006 の4.4.3.4（委託先の監督）について，特に委託先との契約内容が適切に遂行されていることを確認することが規定されていることから，委託先において事項が発生した場合，基本的に委託元が全責任を負うことを認識することが重要である。

6. 事故が発生した場合の経済的の損失より，本人に及ぼす影響や社会的信用などの重要性を認識し，管理のポイントでもある。

7. 監査の重要性：個人情報の取扱における事故などの発生は，PMS の内容や，運用に問題があることが原因の一つと考えられ，PMS の点検（運用の確認，監査）機能が重要である。

8. 監査においては，JIS 規格（JIS　Q　15001）への適合状況および，運用状況の監査がポイントとなる。

9. 監査以外でも，日常業務において，PMS が適切に運用されているかを確認し，その結果を踏まえた注意を強化し，改善に結びつけることが重要である[15)]。

9. お　わ　り　に

本稿は JIS　Q　15001（JIS　Q　15001：2006）について，研究したものである。情報社会の発展に伴う，情報通信技術および情報サービスの発展は，経済・社会・生活・文化などの様々な社会活動の発展の原動力となっているだけでなく，企業活動，個人の生活，社会活動，価値そのもののあり方に大きな変革をもたらしている。

さらに，ネットワーク化の進展は，オープン技術であるインターネットが中心であり，外部からの不正侵入，サービス妨害やホームページの改ざんなどのコンピューター犯罪やネットワーク犯罪が生まれ，大きな社会問題となっている。特に，個人情報が悪用されて様々なトラブルを起こりつつある。個人情報漏洩によって，個人，企業，社会に大きな問題を与えている。

こうした高度情報化社会，ICT 社会が進展するに従い，1999年に「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」が策定された。その規格は，2006年 5 月に改訂され，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「JIS　Q　15001：2006」が公表された。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。こうして，個人情報保護の重要性を認識し，前述の新規格に先立って，2003年 5 月，「個人情報保護法」が成立し，全面施行され，事業者は個人情報の適正な取扱が求められることとなった。さらに個人情報ガイドラインを策定・見直し，個人情報

15）参照：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（平成18年度）「個人情報の地理扱いにおける事故報告にみる傾向と注意点」平成19年 6 月11日

法及びガイドラインの普及啓発に努めている。2006年版は1999年版よりさらにマネジメントシステムのため規格として強調されている。リスクなどの認識，分析及び対策などを取り上げ，今後事業者は，顧客又は消費者等に対して，個人情報の取扱について一定の義務を負うことになる。さらに，問題点を把握し，今後の改善を図るために，事業者・企業等が個人情報の保護に向けた取組みの方向性を模索するに当たって，一助となることを期待している。