特集Ⅲ

個人情報保護マネジメントシステム JIS Q 15001:2017の発行

2017年12月20日、個人情報保護マネジメントシステムの要求事項JIS Q 15001:2017が発行されました。

ここではJQA審査事業センター 情報審査部 部長 秋山 宏幸と、JIS Q 15001審査員の中村 春雄が、JIS Q 15001の2006年版から2017年版への改正の経緯と新規格の特長、および組織がJIS Q 15001を活用するためのポイントを解説します。

審査事業センター
情報審査部 部長
秋山 宏幸

JIS Q 15001 審査員
中村 春雄

個人情報保護に対する社会的関心の高まりと法改正

JIS Q 15001は、個人情報保護を目的として、さまざまな組織が個人情報を適切に管理するためにマネジメントシステムを確立し、実施・維持し、継続的に改善するための要求事項を定めた日本工業規格です。2017年版のJIS Q 15001は、同年5月に改正施行された「個人情報の保護に関する法律（以下 改正個人情報保護法）」への整合を図るために2006年版のJIS Q 15001が改正されたもので、1999年の第1版から数えて第3版に相当します。

近年、個人情報保護の社会的関心が一段と高まっています。その背景にはインターネットをはじめとする情報通信技術の急速な発展と革新があります。スマートフォンやクラウドコンピューティングなどがめざましい勢いで普及し、IoT（モノのインターネット）(*1)やビッグデータ、AI（人工知能）の活用が急速に進んでおり、革新的な技術やサービスが続々と登場しています。また、ビジネスのグローバル化と相まって、個人情報も国境を越えてやり取りされるようになっています。

このような社会の変化に伴い、個人情報が漏洩し、悪用されるリスクも一段と高まっています。情報システムへのウイルス感染や不正アクセスによって、大量の個人情報が漏洩する事故も数多く発生しており、その結果、組織の信用の失墜や事業の停滞に加え、損害賠償や罰金などによる財務的損失などの不利益も増大しています。例えば欧州で1995年10月に採択された「EU個人情報保護指令」が、2018年5月に「EU一般データ保護規則（GDPR(*2)）」として改正施行されます。欧州に子会社などがある日本企業が同規則の個人情報保護義務に違反した場合、その企業は2千万ユーロ（1€≒130円として、約26億円）、あるいは全世界の年間総売上の4%のいずれか高い方という高額の制裁金が科せられることになりました。

一方、ビッグデータやAIの活用では、位置情報や購買履歴などの蓄積した大量のデータ分析により、マーケティングや個人へのサービスの向上に加えて、道路の渋滞緩和や移動時間の短縮、人々の健康・医療情報の活用により医療の発展や病気の予防に役立てるなど、新たな技術革新が期待されています。そのために、個人情報の利用は単に制限するだけでなく、適切なルールのもとで個人情報の有用性を確保する必要が高まっています。

このような個人情報を取り巻く環境変化を受けて、わが国では個人情報保護法が改正されました。同法の改正のポイントは、1.個人情報の定義の明確化、2.適切な規律のもとでの個人情報の有用性の確保、3.個人情報の流通過程の適正さ確保、4.権限が強化された個人情報委員会の新設、5.個人情報の取り扱いのグローバル化への対応、6.本人の開示、訂正、利用停止等の求めは、裁判でも行使できる請求権であることの明確化、の6点です。

2017年版JIS Q 15001のポイント

今回のJIS Q 15001改正の目的は、この規格のマネジメントシステムとしての位置づけを明確化するとともに、2017年5月に施行された改正個人情報保護法に対応する管理策を追加することです。JIS Q 15001:2017には、以下のようなポイントがあります。

（*1）Internet of things:
無線タグなどのセンサーやコンピューターが組み込まれたあらゆるモノがインターネットに接続されること。そこから得られるデジタルデータを利用して新たな価値やサービスを提供することができるため、例えば製造業ではハードウエアにとどまらず「モノ＋サービス」のビジネスへの新展開も期待されている。

（*2）GDPR:
26ページのコラム参照。

1. ISOマネジメントシステム規格の共通要素に基づいた規格構成の採用

2017年版のJIS Q 15001では、マネジメントシステムに関する要求事項を記載した本文と、管理目的及び管理策を記載した附属書Aに分離されました。さらに、附属書Aの管理策に関する補足を記載した附属書Bと、安全管理措置に関する管理目的及び管理策を記載した附属書C、新旧規格の箇条の対応を目次ベースで示した附属書Dからなっています。

このうち規格の本文は、ISOマネジメントシステム規格の共通要素（ISOマネジメントシステム規格を開発または改定する際に用いる規格構造、共通テキスト（要求事項）、共通用語・定義）が採用され、規格の基本構造が他のISOマネジメントシステム規格と共通になりました。さらに、個人情報保護と情報セキュリティとは安全管理措置の点で共通する事項が多いことから、情報セキュリティマネジメントシステムの要求事項ISO/IEC 27001:2013をほぼそのまま引用しています。基本的には、ISO/IEC 27001の「情報セキュリティ」という言葉をJIS Q 15001では「個人情報保護」に置き換えたと考えてよいと思います。

2. 2006年版の要求事項を踏襲し移行に配慮

2017年版のJIS Q 15001では、2006年版の要求事項を附属書A「管理項目及び管理策」に、箇条を含めてほぼそのまま引用したうえで、新たに改正個人情報保護法への対応を追加しています。2006年版の考え方を踏襲することで、2006年版に基づいて構築された個人情報保護マネジメントシステムからの移行も容易になるよう配慮されています。

また、管理策に関する補足を記載した附属書Bは、2006年版のJIS Q 15001の要求事項解説をほぼそのまま引用しています。附属書Bは、箇条が附属書Aと完全に対応しており、附属書Aの各管理策に対応していることが明確になっています。

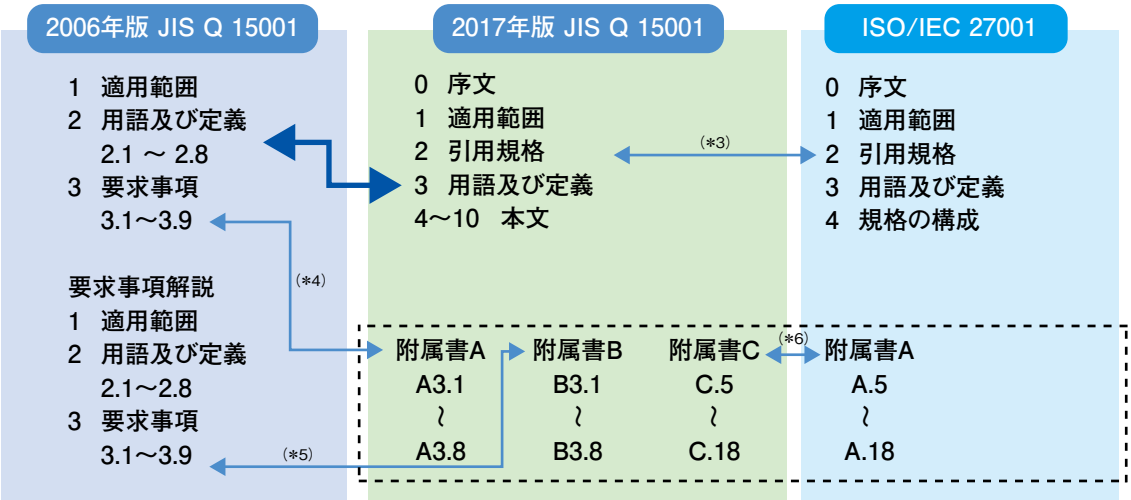
3. 改正個人情報保護法に対応した要求事項を追加

附属書Aでは、個人情報保護法の改正に対応して、以下の項目が変更または追加されています。

a) “特定の機微な個人情報”を、“要配慮個人情報”に変更
b) “個人情報”としていた要求事項の一部を、個人情報保護法の規定に合わせて“個人データ”に変更
c) “開示対象個人情報”を“保有個人データ”に変更
d) 外国にある第三者への提供の制限を追加
e) 第三者提供に係わる記録の作成などを追加
f) 第三者提供を受ける際の確認などを追加
g) 匿名加工情報を追加

a)～c)は、改正個人情報保護法の用語に合わせて変更されました。また、d)は、グローバル対応のため追加された項目。e)～f)は、個人情報が不正に名簿業者に提供された事件を受けて追加された項目です。g)の「匿名加工情報」というのは、特定の個人を識別することができないように個人情報を加工したものを指し、その加工方法を定めるとともに、事業者による公表などその取り扱いについての規律を設けたものです。ビッグデータの活用によ

■ JIS Q 15001とISO/IEC 27001の関係図



(*3)2017年版 JIS Q 15001はISO/IEC 27001をほぼそのまま引用
(*4)附属書Aは2006年版JIS Q 15001を箇条も含めてほぼそのまま引用
(*5)附属書Bは2006年版JIS Q 15001要求事項解説をほぼそのまま引用
(*6)附属書CはISO/IEC 27001附属書Aをほぼそのまま引用

る革新的なビジネスやサービスの向上のための追加項目です。

4. 情報の安全管理措置については、ISO/IEC 27001を引用

附属書Cでは、ISO/IEC 27001の附属書Aをほぼそのまま引用しています。2006年版は、安全管理措置について、経済産業省のガイドラインをはじめとした各省庁から出ているガイドラインを参考にしていましたが、2017年版では、リスクアセスメントの結果、必要であれば実施する管理策としてISO/IEC 27001の管理策が規定され、JIS Q 15001とISO/IEC 27001の関係が明確化されました。

2017年版JIS Q 15001のメリット

2017年版のJIS Q 15001には、上記のようなポイントがあることから、今後組織が個人情報保護に取り組むうえで、さまざまなメリットが期待できます。

1. 個人情報の管理体制を確立、顧客からの信頼向上

組織として活動するうえで、ほとんど全ての組織が内外のさまざまな個人情報を取り扱います。また、国際ビジネスにおいても個人情報保護の重要性が一段と高まり、適切な管理を行わないことによる不利益が増大しつつあります。このため、JIS Q 15001は、今後業種や組織の規模を問わず個人情報保護を扱うあらゆる組織が取り組み、有効に活用できるマネジメントシステムです。

組織がJIS Q 15001に取り組むことで、以下のような効果が期待できます。

- 個人情報保護におけるリスクの低減
- 個人情報を適切に管理・利用する組織体制の確立
- 個人情報に関連する内外の法改正や変化への対応・維持
- 認証取得による取引先からの信頼向上
- 第三者監査を受けることによる自社とは違った視点での改善点の発見

2. 他のマネジメントシステムとの一体運用がしやすい

2017年版のJIS Q 15001では、規格の構成にISOマネジメントシステム規格の共通要素が採用されたことにより、ISO/IEC 27001やISO 9001など他のマネジメントシステムを運用する組織が、JIS Q 15001をそれらと一体的に運用することが一段と容易になりました。

ISO/IEC 27001が、機密性、完全性、可用性をバランスよく維持することを目的とするマネジメントシステムであるのに対して、JIS Q 15001は機密性、完全性、可用性の維持に加えて、本人からの同意を得た利用目的以外の利用をしないなど個人情報保護法への対応を含めたマネジメントシステムです。したがって、ISO/IEC 27001を運用してきた組織は、組織の個人情報管理の追加部分に取り組むことで、個人情報を含めた情報管理が可能になります。

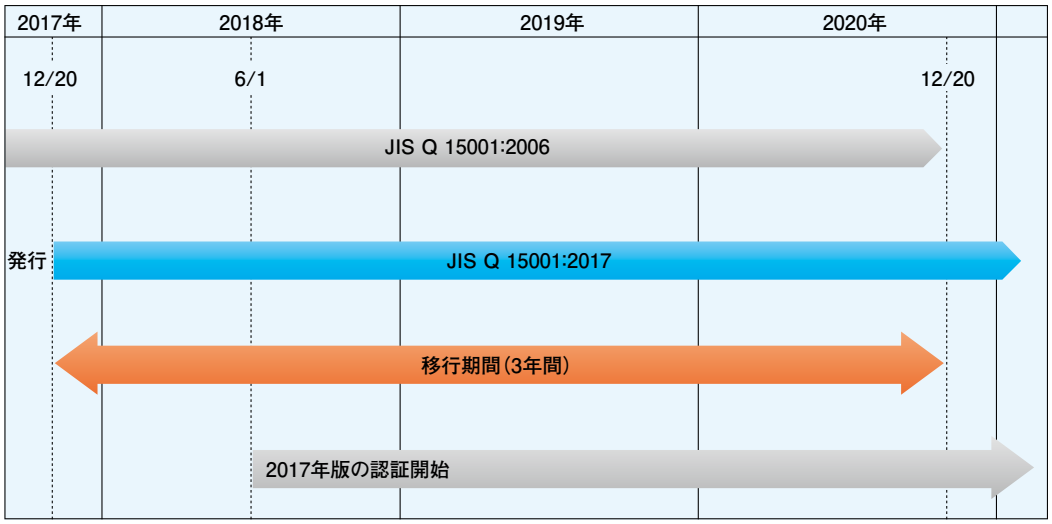
JQAでは、JIS Q 15001単独での審査に加え、ISO/IEC 27001との組合せ審査サービスも提供しています。JIS Q 15001とISO/IEC 27001の両者を組み合わせることで、個人情報の管理をより一層強化し、効率的で効果的な情報資産の保護と活用を実現することができます。

3. 情報セキュリティマネジメントシステムのエントリーモデルとしても活用が可能

ISO/IEC 27001は組織が持つ情報全般を対象としていますが、JIS Q 15001は個人情報のみを対象とします。

「情報セキュリティについて管理体制を確立する必要があるが、情報全体に取り組むことは負担が大きい」と考

■ 2017年版JIS Q 15001の認証および移行スケジュール



■ JIS Q 15001:2017の構成

えている組織は、JIS Q 15001は範囲が個人情報に限定されているので情報セキュリティマネジメントシステムのエントリーモデルとして、まずJIS Q 15001に取り組み、社内および委託先や顧客の個人情報を適切に管理し、段階的に技術情報や財務情報を含めた情報セキュリティマネジメントシステムに体制を拡大するという進め方も現実的な方法です。

4. 2006年版からの移行も容易

2017年版のJIS Q 15001は2006年版の要求事項をほぼ踏襲していることから、2006年版で認証を取得している組織は、変更された要素と新たに加わった要素に取り組むだけで容易に移行できます。

また、先述しているとおり、2017年版では2006年版と違い、ISOマネジメントシステムの共通要素を採用していることから、規格の基本構造と用語、共通テキストが他のISOマネジメントシステム規格と共通になりました。この点、JQAでは従来からJIS Q 15001をISO規格同様にマネジメントシステムとして審査、認証を行ってきましたので、JQAで認証を取得されているお客さまは、2017年版に違和感なく取り組めると考えられます。

2017年版での審査および移行審査のスケジュール

JQAでは、2017年版のJIS Q 15001の認証を2018年6月1日から開始します。また、2006年版から2017年版への移行期間は、規格発行から3年間です。したがって移行期限は2020年12月20日です。

■

欧州連合で2018年5月に施行 個人データ保護を強化する規則(GDPR)

一般データ保護規則(GDPR: General Data Protection Regulation)は、欧州経済領域(EU加盟28ヵ国、ノルウェー、アイスランド、リヒテンシュタイン)と個人データをやり取りするほとんどの企業や機関・団体が適用対象となり、同規則への違反行為には高額の制裁金が科されるリスクがある。日本貿易振興機構(JETRO)では、2017年8月に「EU一般データ保護規則(GDPR)」に関わる実務ハンドブック(実践編)の公開を通じて、EUの個人情報保護対応は、日本企業の欧州向けビジネスに大きな影響を与える経営事項であり、高い優先順位をつけて対応を行う必要があると警告している。

また、2018年2月には、日本経済新聞社がGDPRに対する日本企業と経済産業省、総務省の対応と個人情報保護規制の整備と運用強化に関する記事を掲載している。

JETRO Webサイト

この記事は、2018年2月末現在の情報に基づいています。