JIS Q 15001の取得で 個人情報保護法の遵守をアピール

JIS Q 15001はISO Guide 72:2001*1に従って作成されたJIS規格で、事業者が業務上取り扱う個人情報を安全で適切に管理することを目的としています。2005年4月に施行された個人情報の保護に関する法律（個人情報保護法）によって、5,000件を超える個人情報をデータベース等で所持し事業に用いている事業者は、個人情報の収集にあたって利用目的を特定することや、目的外の個人情報の収集・取り扱いの禁止、収集手段および目的の公表、不正な手段による個人情報取得の禁止などが義務付けられていますが、JIS Q 15001を取得することで、対外的に個人情報保護法を遵守する組織としてアピールすることができます。

ISO 27001との組合せにより 個人情報の有効活用を実現

JIS Q 15001と同様に情報セキュリティの向上を目的とした規格としてISO 27001があります。ISO 27001は情報の機密性・可用性・完全性をバランスよくマネジメントし、情報資産の有効活用を可能にする仕組みの構築が求められているのに対し、JIS Q 15001は情報の機密性に重点を置いた規格となっています。そのため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することができ、サプライチェーンからの信頼を獲得することができます。

審査の効率化と最小限のコスト

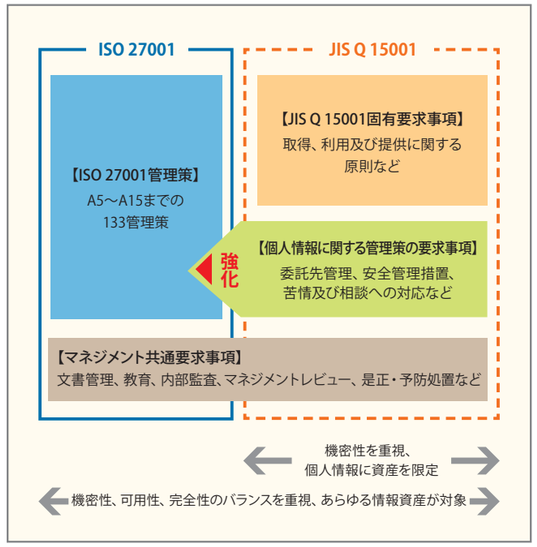
JIS Q 15001とISO 27001の要求事項にはマネジメントの要素など共通する部分（表1）が多くあります。既にISO 27001を取得されている組織の方は既存のマネジメントシステムにJIS Q 15001固有の要求事項を追加することでシステムを強化でき、組合せ審査によって受審準備、審査工数や費用なども必要最小限に抑えられます。また、適用範囲を限定して取得することもできます。個人情報を多く扱う部署や事業部に限定して取得することや自社の資源や進捗状況に応じた段階的な取得が可能です。

JIS Q 15001の固有の要求事項として「3.4.2 取得、利用及び提供に関する資料」「3.4.4 個人情報に関する本人の権利」があります。前者は個人情報を適法かつ公正な手段で取得する、利用にあたっては予め利用目的を設定することや利用目的等を公表あるいは本人に通知することが要求されています。さらに、書面（オンライン上の入力も含む）により直接取得する場合は、本人の同意を得ることを求めています。後者は個人情報を提供した本人から開示等の求め（利用目的の通知、開示、内容の訂正、追加または削除、利用の停止、消去および第三者への提供の停止）に対し、遅滞なく応じることを要求しています。

JQAの審査体制

JQAの審査は文書や記録の確認が中心ではなく、実際の現場の活動に重点を置いた審査を行っていますので、現状を十分認識したうえで問題や課題に対する改善の気づきをご提供することができます。また、830（国内登録件数：3776*2）を超えるISO 27001の認証実績と豊富な経験をもとに、JIS Q 15001組合せ審査についても充実した審査体制でサービスをご提供していきます。

図1: 組み合わせ審査サービスイメージ



*1 ISO Guide72:2001：マネジメントシステム規格の正当性及び作成に関する指針
*2 一般財団法人日本情報経済社会推進協会（JIPDEC）2011.3データより

■ 本件に関するお問合せ先
マネジメントシステム部門　企画・推進センター 事業推進部
TEL: 03-6212-9555

JQA Business Frontline

個人情報保護マネジメントシステム（JIS Q 15001）組合せ審査サービスを開始します

JQAは2011年7月から情報セキュリティマネジメントシステム規格のISO/IEC 27001と個人情報保護マネジメントシステム規格のJIS Q 15001を組み合わせた審査サービスを開始します。組み合わせ審査によって、組織の方々は受審準備、審査工数や費用などを必要最小限に抑えながら個人情報の管理をより一層強化することが可能になり、組織の個人情報保護の取り組みを対外的にアピールできます。

表1: ISO 27001とJIS Q 15001の要求事項の比較

ISO 27001	JIS Q 15001	
4.1　一般要求事項	3.1　一般要求事項	マネジメント共通要求事項
4.2　ISMS の確立及び運営管理	3.3.1　個人情報の特定	
	3.3.3　リスクなどの認識・分析	
	3.4.1　運用手順	
4.3　(1) 文書化に関する要求事項ー一般	3.5.1　文書の範囲	
	3.5.5　内部規程	
(2) 文書管理	3.5.2　文書管理	
(3) 記録の管理	3.5.3　記録の管理	
5.1　経営陣のコミットメント	3.3.4　資源、役割、責任及び権限	
5.2.1　経営資源の提供		
5.2.2　教育・訓練、認識及び力量	3.4.5　教育	
	3.3.6　計画書	
6.　内部監査	3.7.2　内部監査	
	3.3.6　計画書	
7.1　マネジメントレビューー一般	3.9　事業者の代表者による見直し	
7.2　マネジメントレビューへのインプット		
7.3　マネジメントレビューからの アウトプット	（該当なし）	
8.1　継続的改善	（該当なし）	
8.2　是正処置	3.8　是正処置及び予防処置	
8.3　予防処置		

ISO 27001		JIS Q 15001	
附属書「詳細管理策」	A.5.1　情報セキュリティ 基本方針文書	3.2　個人情報保護方針	個人情報に関する管理策強化・固有要求事項
	A.6.1　内部組織	3.7.1　運用の確認	
	A.6.2　外部組織	3.4.3.4　委託先の監督	
	A.7.1　資産に対する責任	3.3.1　個人情報の特定	
	A.7.2　情報の分類	（該当なし）	
	A.8.1　雇用前	3.4.3.3　従業員の監督 3.4.3.1　正確性の確保 3.4.3.2　安全管理措置 3.4.3.4　委託先の監督 (ISO 27001 の A 10.2 に対応)	
	A.8.2　雇用期間中		
	A.8.3　雇用終了・変更		
	A.9.　物理的・環境的セキュリティ		
	A.10.　通信・運用管理		
	A.11.　アクセス制御		
	A.12.　開発・保守		
	A.13.　インシデント管理	3.3.7　緊急事態への準備	
	A.14.　事業継続管理	3.6　苦情及び相談への対応	
	A.15.　適合性	3.3.2　法令、国が定める指針及びその他の規範	
（該当なし）		3.4.2　取得、利用及び提供に関する資料 3.4.4　個人情報に関する本人の権利	