プライバシー情報マネジメントシステム ISO/IEC 27701の審査サービス をスタートしました

JQAは2021年4月、プライバシー情報マネジメントシステムISO/IEC 27701の審査サービスを開始した。実際の審査に携わる審査事業センター 情報審査部 部長の宮下卓士に、ISO/IEC 27701の概要や認証取得のメリットなどについて聞いた。

審査事業センター
情報審査部 部長
宮下 卓士

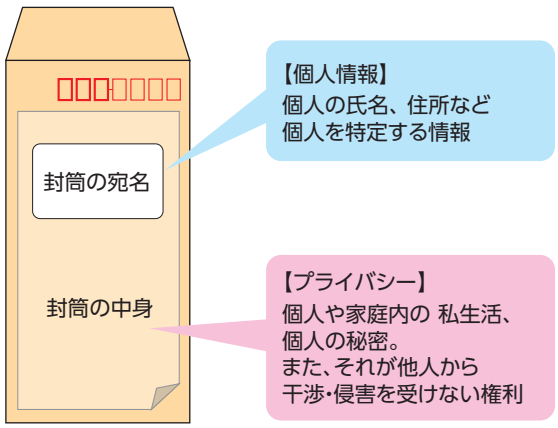
Q 2019年にプライバシー保護の国際規格であるISO/IEC 27701が発行されました。この規格が開発された背景について教えてください。

A インターネットが世界中に普及し、取り扱われるデータの質や量、生活に及ぼす影響が昔とは比べものにならないほど大きくなり、世界各国でプライバシー保護に関する法整備が進められてきました。また、法制に包括的に対応できるISOマネジメントシステム規格が求められるようになったため、2011年から国際規格化に向けた検討が進められ、2019年にISO/IEC 27001（情報セキュリティマネジメントシステム）およびISO/IEC 27002（情報セキュリティ管理策の実践のための規範）への拡張という形でISO/IEC 27701が発行されました。

Q ISO/IEC 27701が保護の対象とするプライバシーについて教えてください。

A プライバシーは、「個人や家庭内の私生活、個人の秘密。また、それらが他人から干渉・侵害を受けない権利」と定義されます。
日本では、個人情報とプライバシーという言葉を区別せずに使用するケースがありますが、JQAのISOセミナーでは、封筒を例にあげて、「封筒の宛名=個人情報」「封筒の中身=プライバシー」という説明をしています。

■ 図　個人情報とプライバシーの関係性



Q 国内では、個人情報保護法に対応した日本産業規格の JIS Q 15001がありますが、ISO/IEC 27701との違いについて教えてください。

A 保護対象が「個人情報」か「プライバシー」かという点と、順守する法令が日本の個人情報関連法令に限定されるか否かという点です。
まず保護対象が異なる点については、先ほどの封筒の例でいえば、JIS Q 15001は、宛名や住所などが示された「封筒=個人情報」自体の取り扱いを適正に行い保護することによって、結果的に「中身=プライバシー」も保護されるという考え方をしています。
一方、国際規格であるISO/IEC 27701は、規格が定義するPII（ピー・アイ・アイ／個人識別情報:

Personally Identifiable Information)の取り扱いによって、侵害される恐れのあるプライバシーを保護するという考え方です。このPIIには、氏名や生年月日、住所といった個人情報に加えて、Cookieなど、個人と直接的にはひもづけられない情報が相当するとされています。例えば「50代女性」という条件の場合では個人の特定は困難ですが、「JQAの審査事業センターの50代女性」のように、いくつかの関連ある情報を集めると個人が特定できるような情報はPIIに相当します。
次に順守法令が異なる点ですが、JIS Q 15001は日本の個人情報保護法に対応した規格であり、順守法令は個人情報保護法と関連法令に限定されますが、ISO/IEC 27701は取り扱うPII によって順守する法令が変わってきます。

Q 実際にISO/IEC 27701に基づいて構築するマネジメントシステムとJIS Q 15001に基づいて構築するマネジメントシステムに違いはあるのでしょうか。

A 両規格ともに、個人に関係する情報の適切な取り扱いを求めていることは同じであり、実際に構築すべきマネジメントシステムに大きな違いはありません。敢えて違いを述べるならば、処理記録の精度や一時ファイルの取り扱いなど、ISO/IEC 27701で詳細に要求している部分への対応を確実に実施することで、JIS Q 15001よりも厳しい保護策を取ることが可能になります。

Q JIS Q 15001のほかに、個人情報について適切な保護措置を講ずる体制を整備している事業者等を評価するプライバシーマーク(Pマーク)制度が国内には存在します。この制度に基づくプライバシーマークとISO/IEC 27701との違いについても教えてください。

A プライバシーマーク制度は、一般財団法人日本情報経済社会推進協会(JIPDEC)が創設した制度であり、JIS Q 15001に適合している事業者を評価した証として、プライバシーマークを付与します。ISO/IEC 27701との違いは、JIS Q 15001と同様、保護対象と順守法令が挙げられます。また、そのほかの違いとして、プライバシーマークは、「法人単位」での取得が必須であるのに対し、ISO/IEC 27701は、マネジメントシステムの認証範囲を、プライバシー保護に関与する「企業・組織(以下、企業)の一部」に限定して認証を取得することが可能であることが挙げられます。

Q JQAがISO/IEC 27701の審査サービスを開始した経緯について教えてください。

A 以前よりJIS Q 15001の審査サービスを提供してきましたが、ISO/IEC 27701がISO/IEC 27018(PII処理者としてパブリッククラウド内のPIIを保護するための実践の規範)やISO/IEC 29151(個人を特定できる情報保護のための実施標準)、GDPR(ジー・ディー・ピー・アール/EU一般データ保護規則:General Data Protection Regulation)をカバーしており、海外取引のある企業のニーズに対応できることや、ISO/IEC 27001と統合したマネジメントシステムの構築が可能であるという規格の特性から社会的なニーズがあると判断し、ISO/IEC 27701の審査サービスを開始しました。

Q ISO/IEC 27701規格の構成について教えてください。

A この規格は、プライバシーマネジメントに関するISO/IEC 27001およびISO/IEC 27002への拡張という形で、PIMS(プライバシー情報マネジメントシステム)を確立、実施、維持、継続的に改善するための要求事項について規定し、手引きを提供する構成となっています。

Q ISO/IEC 27701の認証取得のメリットを教えてください。

A 次のようなメリットが考えられます。

●ISO/IEC 27701は、ISO/IEC 27001および

ISO/IEC 27002の拡張規格です。ISO/IEC 27001の認証とプライバシーマークの両方を取得しているが、マネジメントシステムを別々に構築しているという企業は、すでに運用している情報セキュリティマネジメントシステムと一体運用することが可能です。また、個人情報を取り扱う部署が一部に限定されている企業にとっては、認証範囲を限定することができます。

- ●PII管理者/PII処理者としての要求事項が整理されています。そのため、PII管理者においては企業の業務に応じて適切な要件の選択を行うこと、PII処理者に対して適切な委託契約を行うことが可能です。また、PII処理者においても、JIS Q 15001より明確にPII処理者としての要求事項が定義されていますので、業務に応じて適切な要件の選択を行うことができます。
- ●国内で事業を行う企業にとっては、個人情報保護法など、日本の個人情報関連法令への順守を示すことが可能です。
- ●国内外で事業を行う企業にとっては、プライバシーの保護において重要とされている「忘れられる権利」「プライバシー・バイ・デザイン(*1)」、プライバシー・バイ・デフォルト(*2)」等に配慮している企業であることをアピールできます。

(*1) プライバシー侵害のリスクを低減させるために、システムの開発においてあらかじめプライバシー対策を考慮し、企画から保守段階までシステムライフサイクルで一貫した取り組みを行うこと。
(*2) 初期状態で、プライバシーが保護された状態にすること。

Q ISO/IEC 27701の認証を取得するための条件を教えてください。

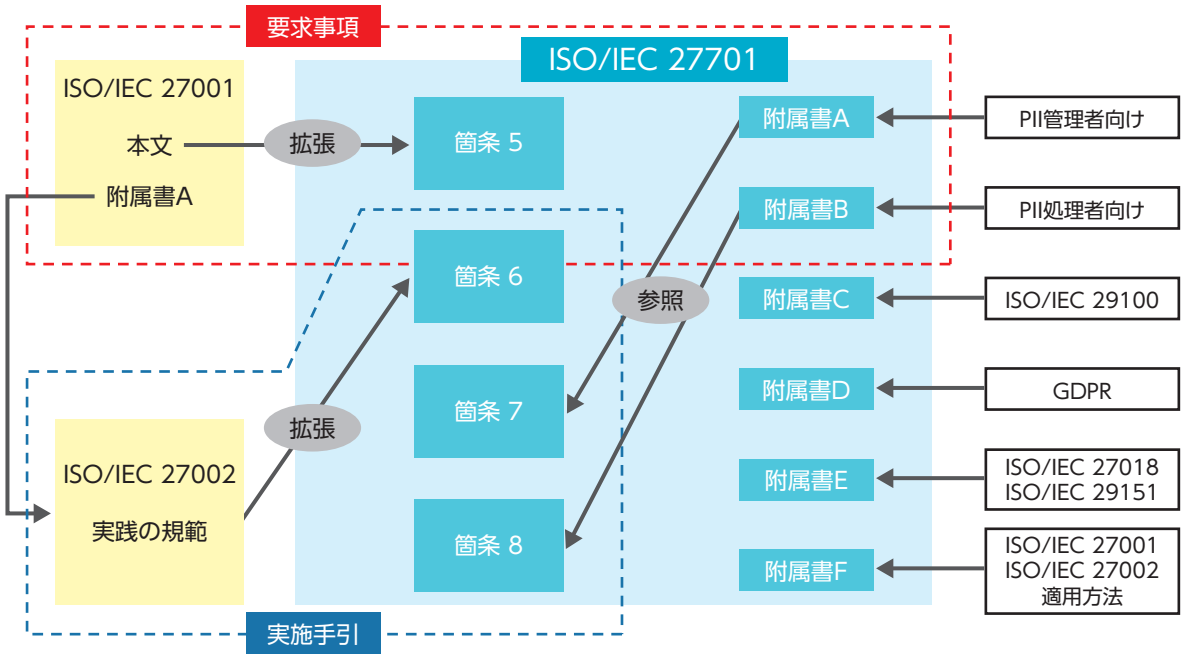
A このISO/IEC 27701は、ISO/IEC 27001の拡張規格の位置付けであるため、ISO/IEC 27001の認証取得が必須です(*3)。また、ISO/IEC 27701の認証範囲は、ISO/IEC 27001の認証範囲と同一か、ISO/IEC 27001の認証範囲に包含されていることが必要です。

(*3) ISO/IEC 27001の認証とISO/IEC 27701の認証を同時に取得することは可能です。

Q ISO/IEC 27701の認証を取得する企業として、想定される主な企業を教えてください。

A 業種・業態を問わず、あらゆる企業が利用し、認証を取得することができますが、特に次のような企業による認証の取得が想定されます。

■ 図　ISO/IEC 27701規格の構成



●GDPRの影響を受ける企業。EUに子会社・支店・営業所・駐在員事務所を有している企業、日本からEUに商品やサービスを提供している企業、EUから個人データの処理の委託を受けているデータセンター・クラウドサービスベンダー。
●B to Cの企業。オンライン販売やオンラインゲームを提供している企業。
●B to B to Cの企業。PII処理者としてPII管理者にサービスを提供する企業、ダイレクトメールの印刷・送付事業者、通販業者、コールセンター事業者、クラウド事業者、データセンター事業者。

Q ISO/IEC 27701の認証を取得する想定企業のひとつに、「GDPRの影響を受ける企業」を挙げられましたが、ISO/IEC 27701に取り組むことはGDPRへの対応に有効と考えますか。

A プライバシー情報に特化したISO/IEC 27701には、GDPRとの対応を示した附属書Dがあり、GDPR第5条～第49条（欧州委員会など監督機関特有のごく一部の条項を除く）の指標との対応が示されています。そのため、ISO/IEC 27701の取り組みをGDPRへの対応の根拠とすることは、有効であると考えます。

Q JQAでは、2021年4月にISO/IEC 27701の審査サービスを開始しましたが、お客さまより認証取得のお申し込みはありますか。

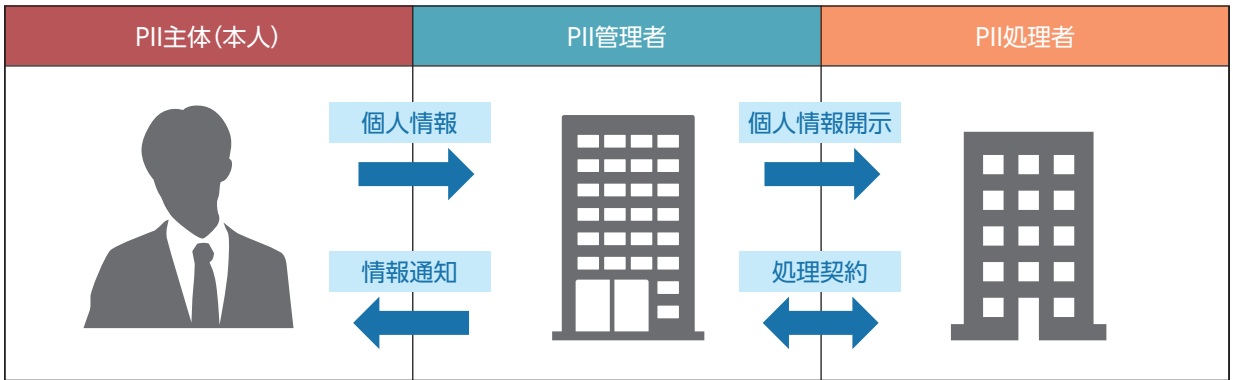
A すでにISO/IEC 27001を取得している企業からお申し込みを受け、JQAとして初のISO/IEC 27701認証を付与いたしました。ISO/IEC 27701の認証取得をご検討中のお客さまは、ぜひJQAにご相談いただければと思います。

Q ISO/IEC 27701の要求事項は、どちらで入手できるのでしょうか。

A 一般財団法人日本規格協会のWebサイトより購入可能です。なお、2021年5月時点で、JIS版は発行されておらず、現時点でのJIS化は未定です。

■

■ 図　PII管理者とPII処理者



PII主体（本人）	PII管理者	PII処理者
PIIに関連する個人	私的な目的でデータを使う個人を除く、PIIを処理するための目的及び手段を決定するプライバシー利害関係者	PII管理者に代わり、かつ、その指示に従ってPIIを処理する利害関係者
例）アンケートに答える個人勤務時間等の情報をわたす社員	例）市場調査のためアンケートを実施して個人情報を収集する事業者	例）委託元からの指示に従い、給与計算サービスを提供する電算センター