ISO/IEC 27701 FAQ (よくある質問と回答)

＜Pマークと関連性のある質問＞

Q: PマークとISO/IEC 27701の違いを教えてください。
A: Pマークは、JISQ 15001が規格要求事項（基準）であり、ISO/IEC 27701はISO/IEC 27001とISO/IEC 27701が規格要求事項（基準）となります。
参考：JISQ 15001は日本の個人情報保護法に関連性を持たせ作成されています。ISO/IEC 27701はプライバシー保護を組織の仕組みに組み込むという違いはあります。

Q: PマークとISO/IEC 27701の包含関係はなく、独立しているものと考えてよいですか？（PマークとISO/IEC 27701との関係について教えてください。）
A: ISO/IEC 27701は国際規格として策定されており、JISQ 15001は日本のみの規格として策定されています。そのためそれぞれの規格は独立していますが、対象としているのはどちらも個人情報になります。JISQ 15001は個人情報保護法に合わせて策定されているのに対して、ISO/IEC 27701はISOとなるためある地域の法律に準拠という観点はないということも特徴です。

Q: Pマークが日本においては一般的ですが、特にISO/IEC 27701の要求事項及び管理策とGAPが大きい点・懸念点があれば、可能な範囲でご教授いただけないでしょうか。
A: 弊社ISO/IEC 27701の有料セミナーをご受講して頂けるとより詳しく解説させて頂きます。ISO/IEC 27701とJISQ 15001は全く別物です。扱っているのはどちらも個人情報ですが、国内規格と国際規格も違いベースがISO/IEC 27701はISO/IEC 27001になっているためセキュリティ保護も含まれています。

Q:Pマークの要求事項との差分は多いですか？
A: 差分については、要求事項自体が違うため、多いか少ないかは組織によってその実行管理策の違いにより変わると考えます。

＜規格の解釈に関係する質問＞

Q: ISO/IEC 27701において、日本の個人情報保護法における要配慮個人情報のような、レベルの異なる個人情報（PII）の管理策を意識した部分はありますか？
A: 規格としては、レベルの違う管理などはリスクアセスメントなどで管理策の実装を検討するため、要配慮個人情報と言うものは明確にはありませんが、対応として管理策で該当するものが出てくる可能性はあります。

Q: ISO/IEC 27701運用にあたり、ISO/IEC 27001のなかにおいて、A18以外で特に留意すべき管理策があれば教えてください。
A: ISO/IEC 27001は資産のセキュリティ保護になりますが、ISO/IEC 27701は個人情報のプライバシー保護になります。ISO/IEC 27001のA18は個人情報のセキュリティ保護であり、ISO/IEC 27701はセキュリティ保護ではなく、プライバシー保護に焦点を当てております。（プライバシー保護をするにあたりまもるセキュリティがA18と考えるといいかと思います。）ですので、その観点であればISO/IEC 27701の箇条6に記載の通り各種ISO/IEC 27001の付属書の管理策もプライバシー保護の観点では考慮すべきと考えます。

ISO/IEC 27701 FAQ (よくある質問と回答) Page.2

Q:当社はISMS認証取得済みであるためISO/IEC 27001が適用されております。一方でISO/IEC 27701規格では、6以降はISO/IEC 27002を適用すると記載されている箇所があります。（例）”ISO/IEC 27002:2013 、XXXに規定する管理策、実施の手引き及び関連情報を適用する” この場合ISO/IEC 27001の管理策に加えて、ISO/IEC 27002の管理策も適用が必要でしょうか。もしくは、ISMS取得済み（ISO/IEC 27001適用済み）であればそれで問題ないでしょうか。
A: 箇条６， ７， ８はガイドであり、要求事項ではありません。ただしISO/IEC 27001のAはセキュリティ要素が記載されており、箇条６についてはセキュリティ管理策に対してプライバシー保護要素を考慮することとして考えてください。

Q:PIIと「プライバシー」を分けているように見えますが、この差異はどのように区別すればよいのでしょうか？
A: PIIは個人情報であり、プライバシーではありません。ですので分けているわけではなく、そもそも定義が違うものになります。

＜規格の位置付けに関する質問＞

Q: ISO/IEC 27701:2019のJIS化時期はいつになりますでしょうか。
A: 現在JIS化の予定はございません。

Q: 現在ISO/IEC 27018の取得を検討中ですが、ISO/IEC 27018とISO/IEC 27701の関係性・違いなど教えていただけますでしょうか。
A: ISO/IEC 27018については、規格の名前の通りパブリッククラウドサービス且つPIIプロセッサーのみしか取得できない規格であるのに対してISO/IEC 27701は特にクラウドなど関係なく、PIIコントローラ及びPIIプロセッサーのどちらでも取得できます。

Q: ISO/IEC 29100（JIS X 9250）でISO認証を取得している組織がありますが、下記についてご教示ください。
①ISO/IEC 29100とISO/IEC 27701の内容、認証の違い
②ISO/IEC 29100認証とISO/IEC 27701認証の効果の違いEUが承認したGDPR認証手段としてISO/IEC 27701を開発する計画はありますか？
A: ISO/IEC 29100(JIS X 9250)は、「情報技術―セキュリティ技術―プライバシーフレームワーク（プライバシー保護の枠組み及び原則）」であり、ISO/IEC 27701の参照規格となります。

ISO/IEC 27701 FAQ (よくある質問と回答) Page.3

＜GDPRに関連する質問＞

Q: GDPRや日本の個人情報保護法に対しての適応性について教えてください。
A: ある国の法規制に準拠するという認証ではないため参考とはなりますが、GDPRや個人情報保護法に準拠という証明ではございません。

Q: GDPRを意識している企業であれば、ISO/IEC 27701の導入はこれからは必須だと言えるのか？
A: ISOの認証はある特定地域の法規制の認証にはなりえません。そのためGDPRがあるから認証が必須というものではありません。ただし、各国の法規制への準拠フレームとしては有用と考えます。

Q: GDPRコンプライアンスのためにクライアントを支援するという観点から、ISO/IEC 27701認証の価値提案は何ですか？
A: ISO/IEC 27701には、標準の関連セクションをGDPRにマッピングする付属書があるため、GDPR要件への準拠をサポートするマネジメントシステムを支援およびサポートします。マネジメントシステムの基本的な考え方は、要件を満たすためのガバナンスフレームワークを提供することです。

＜審査に関係する質問＞

Q: 審査に向けた準備が十分に出来ていませんが、審査受審は可能でしょうか？
また、審査から認証取得まではどのくらいの期間がかかるのでしょうか？
A: 認証取得に必要な準備ができていないと、審査を受けても重大な不適合がでる可能性があるので、受審はできないと考えます。 審査から認証取得までの期間はISO/IEC 27701のフレームが出来てから、そのPDCAが一通り回る期間として約3ヵ月ほどの期間がかかるとお考え頂けたらと思います。
詳しい審査受審時期などについては、別途営業にご相談ください。

Q:ISO/IEC 27701 はリモート審査が可能なのでしょうか？可能であればどのような手順を踏むことになるのでしょうか？
A: 状況が整えば可能です。ご希望の場合には弊社営業にご相談ください。

ISO/IEC 27701 FAQ (よくある質問と回答) Page.4

Q:審査費用はどの位かかるのでしょうか？また、ISMS単独の審査と比べて、ISMS＋PIMSセットの審査の場合、審査時間はどれぐらい増加しますか？
A: 事業者様がPIIコントローラーなのか、それともPIIプロセッサーなのか、また、組織様の規模によっても審査工数/費用は異なります。概算費用の御案内も可能ですので、是非、営業部宛にお問合せください。

Q:毎年のサーベランスでも、ISO/IEC 27701も考慮したものになるのでしょうか？
A: ISO/IEC 27701はISO/IEC 27001のアドオン認証となるためISO/IEC 27001と一緒に審査を行います。

＜研修に関係する質問＞

Q: BSIでISO/IEC 27701の審査員研修はありますでしょうか？当方、ISMS ISO/IEC 27017 クラウド審査員です。
A: BSIを含めISO/IEC 27701の審査員研修を提供している教育機関はありません。(2021年3月2日時点)

Q: ISO/IEC 27701の研修は他社と比較した際、どのような違いがありますか？また、BSIのISO/IEC 27701 研修を受講するメリットなどがあれば教えてください。
A: 他社は、ISO/IEC 27701に関連する研修を提供しておりません。(2021年3月2日時点)

BSIではISO/IEC 27701:2019 要求事項解説研修(JRCA登録CPDコースISMS)を開催しております。
BSIの当コースを受講するメリットとしましては下記があげられます。

1) （他社が実施していないことを前提条件として）国内で唯一、ISO/IEC 27701を学べる研修の機会です。

2) JRCA登録CPDコース（ISMS）なので、5時間のCPDを獲得できます。

3) 『ISO/IEC 27701』『ISO/IEC 27001』『ISO/IEC 27002』の規格書（BSI翻訳抜粋版）が無料で入手できます。

4) その他、メリットとしては、

- ●個人識別可能情報 (PII)を保護するための仕組みを理解できます。
- ●プライバシー情報マネジメントシステム (PIMS)の構築に必要な知識を身につけることができます。

詳しい内容のご確認、研修のお申し込みは下記よりお願いいたします。
https://www.bsigroup.com/ja-JP/iso-27701-privacy-information-management/iso-27701-training-courses/