【講演レポート】ISO/IEC 27001:2022移行に関するセミナー

当日頂いた主なご質問への回答

今回はISO/IEC 27001:2022移行のためのセミナーであり、一般的な移行の審査ポイント等をお伝えするものです。そのため、ISO/IEC 27002:2022の新管理策の解釈や、組織様個別のケースの解釈、及びISMSクラウドセキュリティ認証・ISMS-PIMS認証に関するご質問への回答は控えさせて頂いておりますので、何卒ご了承ください。

【ISO及びJIS関連】

Q: JIS Q 27001 及び JIS Q 27002 の発行日はいつ頃でしょうか？

A: 当該JISの原案作成団体である（一財）日本規格協会に確認したところ、現時点では、
ISO/IEC 27001:2022を対応国際規格としたJIS Q 27001は、2023年9月公示の見込み（東京で開催したセミナーにおける質疑応答においては、この点の説明が不十分でした）、ISO/IEC 27002:2022を対応国際規格としたJIS Q 27002は、2024年春頃公示の見込みとのことです。
なお、今後の状況に応じ、公示時期は変更となる可能性がありますのでご了承ください。

Q: 翻訳したISMSの規格ガイドラインを展開頂くことは可能でしょうか？また、審査の際に規格ガイドラインは備えておく必要はあるのでしょうか？

A: ISO/IEC 27001:2022対訳版は、（一財）日本規格協会様のWebサイトから購入可能です。
管理策のガイダンスであるISO/IEC 27002:2022があれば、より理解が深まりますが、必須ではありません。

【ISO/IEC 27002（JIS Q 27002）について】

Q: ISO/IEC 27001:2022対応のJIS発行後は、JIS Q 27001認証になる（認証登録証にはJIS Q 27001が明記される）とのことですが、JIS Q 27002改訂版が発行される前（ISO/IEC 27002は対訳版）でも同様の扱いとなりますか？

A: ISMS適合性評価制度の認証基準は ISO/IEC 27001（JIS Q 27001）のため、ガイドラインであるISO/IEC 27002（JIS Q 27002）改訂版発行の有無については、認証には影響しません。

Q: ISO/IEC 27001:2022 では、附属書 A の管理策に関する目的が記載されていないということは、ISO/IEC 27002:2022 も審査の規準文書となるという理解でよろしいでしょうか？

A: 認証基準はISO/IEC 27001:2022 であり、ガイドラインであるISO/IEC 27002には要求事項はないため、審査の基準にはなりません。ただし、組織内でISMSを運用するにあたっては、管理策のガイドラインとして ISO/IEC 27002:2022 を参考にしていただくことに問題はありません。

【移行期間・審査のタイミング】

Q: ISO/IEC 27001:2022に対応するJISの発行が遅れているので、ISO/IEC 27001:2022 への移行期間（2025/10/31）を延長される可能性はあるのでしょうか？

A: ISO/IEC 27001:2022への移行はIAF MD26で移行期間が決定されているためJISの発行は影響しないことから、延長されることはありません。

Q: 今後（来年初頭以降）初回審査を受審予定だが、当初からISO/IEC 27001:2022に合わせてやっていった方が良いでしょうか？
A: 組織のISMS運用の進捗や準備状況に合わせてご判断いただくことになります。JIS Q 27001:2014 (ISO/IEC 27001:2013)に基づいた運用を開始しているのであれば、JIS Q 27001:2014 (ISO/IEC 27001:2013) で初回審査を受け、その後の定期審査のタイミングで移行を行うという選択肢もありえます。ただし、JIS Q 27001:2014 (ISO/IEC 27001:2013)を認証基準とした初回審査の期限（2024年4月30日までに開始）と、ISO/IEC 27001:2022への移行期限（2025年10月31日）についてはご注意ください。

Q: 2013年度版 (ISO/IEC 27001:2013) で審査を受ける方法はありますか？
A: 新規取得及び再認証審査の場合は2024年4月30日までに審査を開始しているように受審ください。サーベイランス審査の場合は2025年10月31日までに2022年版での証書が発行されるスケジュールで受審ください。

【審査全般】
Q: ISO/IEC 27001:2022対訳版を元に検討を開始して問題ないでしょうか？
A: （一財）日本規格協会が発行する対訳版に基づいて開始されても、問題ありません。ただし、JIS Q 27001:2023発行後には、JISをもとに確認してください。

Q: サーベイランス審査と同時に移行審査を受審する場合、現行規格文書と改訂規格文書を二重管理する必要があるのでしょうか？
A: サーベイランス審査等の審査種別に関わらず、旧版としての管理は必要となると考えます。活動実績を見る際にはその時点での適切な版を基準とするためです。

Q: 移行審査と再認証審査を一緒に実施する場合、再認証審査の工数に、移行審査の工数がプラスされる認識で良いでしょうか？
A：サーベイランス審査及び再認証審査と同時に行われる場合は、通常の定期審査工数に追加で移行審査の工数が必要となります。

Q:移行審査の際にギャップ分析を行ったというエビデンスの提示も求められるのでしょうか？
A:移行審査では、ギャップ分析の結果を確認することになります。そのため、ISO/IEC 27001:2022への移行対応として、何を実施したのかについて確認できる証跡をご用意いただく、と想定ください。

Q: ISO/IEC 27001:2022 への移行審査を受ける上で、適用宣言書に2013年版 (ISO/IEC 27001:2013) とのギャップ分析の結果を文書化する必要はありますか？
A: 適用宣言書にギャップ分析の結果を記載することは要求事項ではありません。ただし、移行審査にお

いては、ギャップ分析の結果は必ず確認する必要があります。その確認を審査機関が行う上での証跡は必要となります。

Q: 組織内部で作成したISMSマニュアル、適用宣言書、各種規定等について、JIS Q 27001:2014対応版とISO/IEC 27001:2022対応版の新旧対応表は移行審査時に必須でしょうか？
A: 新旧対応表の文書化は要求事項ではないため、必須ではありません。ただし、移行審査ではISO/IEC 27001:2022対応として各種文書の改訂状況を確認することになるため、新旧対応表あるいはそれに準ずるような作業記録は、審査対応としては有用であると考えます。

【リスクアセスメント】

Q: 規格移行の審査を受ける際に、情報セキュリティリスクアセスメントの実施は必要ですか？
A: IAF MD26の要求事項の通り実施する必要があります。

Q: ISO/IEC 27001:2022 では附属書Aの管理策のいくつかが変更となったが、それに伴うリスクアセスメントは、移行審査を受審する前に、必ず実施する必要があるのでしょうか？
A: 附属書Aの変更という理由だけでなく、IAF MD26での要求の通りリスクアセスメントの実施はする必要があります。

【管理策全般】

Q: 「2022年版 (ISO/IEC 27001:2022) の初回審査」と「2013年版 (ISO/IEC 27001:2013) から2022年版への移行審査」で、管理策に関する審査の観点に違いはありますでしょうか？
A: 認証基準として2022年版 (ISO/IEC 27001:2022) を使うため観点の違いはありません。

Q: 新規に増えた管理策の中で、適用除外が考えられる管理策はありますか？
A: 附属書Aに示されている管理策の採用・除外は、それぞれの組織が実施する事業や状況により異なります。特定の管理策の採用・除外については、従来どおり組織の置かれている状況により判断されることに変わりはありませんので、組織のリスクアセスメントの結果に基づいて必要な対策を検討することで判断ください。

本内容は、2023年7月3、7、18日にハイブリッド（会場及びZoom）で開催された「ISO/IEC 27001:2022移行に関するセミナー」における質疑応答の内容を取りまとめたものです。