【講演レポート】ISO/IEC 27001移行セミナー

ISO/IEC 27001：2022移行に係わる審査のポイント

日本マネジメントシステム認証機関協議会（JACB）
普及担当幹事　鈴木　浩二
森竹　由美子
情報技術委員会　委員長　中村　良和

日本マネジメントシステム認証機関協議会（JACB）とは、国際認定機関フォーラム（IAF）に加盟する認定機関によって認定され日本国内で事業活動を行うマネジメントシステム認証機関が集まった協議会です。今回のISO/IEC 27001：2022移行について、JACBとして認証組織の皆様が円滑に移行できるようサポートしていきたいと考えています。ここでは、審査側（認証機関）の観点をご紹介し、管理策の解釈に関しては各認証機関（審査機関）や研修機関等で今後セミナー等を実施する予定ですので、そちらをご活用ください。

ISO/IEC27001：2022改正のポイント

今回の改正ポイントは、大きく分けて以下の2点となります。

① ISO/IEC 27002：2022が先に改訂されており、それに伴い、管理策には新たな技術を取り込んでいく必要があるため、附属書Aが変更された。

② 規格固有の内容以外の部分については、ISOとして「調和させる構造（Harmonized Structure）」形式に合わせることが求められたため、当初は本文変更の必要はないと判断された本文にも変更が加わり、章立て等が変わった。

規格本文の改正概要～Harmonized Structureへの対応～

本文に関しては、大きな内容変更はなく、規格改正に伴う参照先文書名や文言変更、範囲の明確化等が行われています。

また、移行審査に大きく関わる点として、6.3に新規要求事項（組織がISMSの変更の必要性を決定したとき、その変更は、計画的な方法で行われなければならない）が追加されました。今回は規格が変更されているため、ここは審査で必ず確認される部分となります。

情報セキュリティ管理策の改正概要～ISO/IEC 27002:2022との整合～

改正のポイントは以下のとおりです。

① 管理策のカテゴリ見直し

A.5～A.18　→　5～8のように、附属書Aの管理策項番に「A.」をつけない表現となっています。

② 管理策の数が114→93に。ただし、削除された管理策はなく統廃合されており、新しい管理策も11追加されています。

情報セキュリティ管理策の新旧対応

情報セキュリティ管理策の新旧対応に関しては、ISO/IEC 27002:2022附属書Bに参考情報がありますが、それぞれの対応度合いに違いがある（ほぼ同じ内容であるもの、ほぼ同じ内容だが注意が必要なもの、単純対応ではないものに分かれる）ため、留意が必要です。

統廃合に関しては、ライフサイクルに合わせたり、特定の事象だけに限定せず管理策を一般化することによって統廃合されたりしたものがあります。また、一見、ほぼ同じ内容に見えても、細かな表現の変化により、対象範囲や想定リスクが変化している等、注意が必要なものが散見されるので、新旧の違いをしっかりと確認することが必要です。

審査にあたっては、ギャップ変化を遠隔で確認できるのであれば遠隔審査は可能ですが、その判断は認証機関が行うことになります。今回の2022年版では、物理的管理策の追加変更もあるため、それらが遠隔審査で確認できない場合には、現地で確認する必要があります。また、これまではコロナ禍での特別措置がありましたが、国際ルールとしてサーベイランス審査、再認証審査において100%のリモート審査は不可となっています。

細かいものも含めるとかなり変更点があるので、すべてが審査対象になるということではなく、それぞれの認証機関によっても、確認ポイント、審査工数が異なってくる点をご理解ください。

改正規格への移行の進め方

認証の移行

2022年度版への移行は2025年10月31日までとなっていますが、その段階で認証機関が証書を発行し終わっていることが条件となります。この条件を満たすためには、その1か月前までに審査が終了している必要があります。「JISが発行されてから」と審査を後ろ倒しにした場合、認証機関の審査キャパシティの問題で希望の時期に審査を受審できない可能性もあるので、できるだけ早めに審査を受けていただくようお願いします。

一方、2022年版発行月の最終日から18カ月（2024年4月30日）を超える初回認証及び再認証審査は2022年版によるもののみとなるので、旧版で審査を受ける場合は2024年4月30日までに審査が開始していることが必須となります。こちらも同様に、2024年4月30日直近に審査のお申し出をいただいても、4月中に審査を開始できるとは限らないので、定期審査を待たず早め早めに対応していただくことをお勧めします。

移行のための審査

移行のための審査は、定期審査（サーベイランス審査、再認証審査）と併せて実施することも、単独で実施することも可能なので、必ずしも定期審査を待たずに余裕をもって単独審査を受ける、または早めのサーベイランス審査を受けることもご検討ください。

移行審査のための追加工数は、IAFで最小工数のみが定められています。再認証審査と同時実施の場合は+0.5人日、サーベイランス審査と同時または単独審査の場合は+1.0人日が最低工数となっています

。どの認証機関もこれ以下にはならず、追加工数は審査を受ける組織の管理策の適用範囲や変化の度合い等によって変わってきます。

移行の進め方

実際に移行を進めていく上では、以下を行うことが必要になります。

① ギャップ分析と対応方針の決定

本文の違いを認識し、追加された管理策や要求事項を把握してギャップを分析し、管理策の変更点に対応する。審査では実行されているところまでを確認するので、「●●までに実施」といった計画だけでは審査を受けることはできません。

② 管理策の変更対応

管理策の変更をきちんと行っていただくことが一番大きな対応になると思います。文書の変化で済むものもあると思いますが、実行されていること、その実行面をきちんと監視（内部監査）することが重要になります。まずは、ギャップ分析を行った上で、新しい管理策をどのように実装していくかを検討してください。

③ ISMS関連文書の見直し

その後、マニュアル等関連文書の見直しを行います。特に、改正された規格の附属書Aに従って適用宣言書を見直すことが重要になります。

④ 変更されたISMSの運用及び評価

最後に、変更されたISMSに従って運用を開始し、PDCAを回すことになります。移行タイミングによっては臨時の内部監査やマネジメントレビューの実施が必要となりますが、今回のポイントは規格の移行なので、その視点から、どこ/誰に対して内部監査を行えばよいかを考え実行することになります。実行後は、結果をマネジメントレビューにインプットして、経営陣によるレビューを受けてください。

移行審査では、認証機関はこうした変更点を確認するということをご理解いただいた上で、移行準備を進めてください。

本内容は、2023年7月に開催された「ISO/IEC 27001:2022への移行に関するセミナー」での説明内容を取りまとめたものです。