【講演レポート】ISO/IEC 27001移行セミナー

# ISMS適合性評価制度におけるISO/IEC 27001：2022への対応について

一般社団法人情報マネジメントシステム認定センター（ISMS-AC）
理事　星　昌宏
事務局次長　保木野　昌稔

## ISMS適合性評価制度

ISMS適合性評価制度は、国際規格に基づき認定/認証を行うことで、世界的に同等レベルの情報セキュリティマネジメントシステムの品質を維持する制度です。ISMS認証を受ける組織は、認証機関に申請しISO/IEC 27001に基づいた審査を受けます。私たちISMS-ACのような認定機関は、認証機関が適切に、同レベルで認証審査を行っているかどうかをISO/IEC 17021-1、ISO/IEC 27006に基づき審査し認定しています。

さらに認定機関に関しては、国際認定フォーラムの下、ISO/IEC 17011に基づいた審査を経てISMSの国際相互承認協定（MLA）に署名した認定機関は、他のMLA署名認定機関と同等の認定の有効性が国際的に認められています。現在、ISMSで同等だと認められている認定機関は、世界全体で45機関あり、私たちISMS-ACもMLAに署名しているため、ISMS-ACが認定した認証機関で企業が認証を受けた場合、その認証は国際的にも同等レベルであるということが言えます。

2000年より以前には「情報処理サービス業情報システム安全対策実施事業所認定制度」（安対制度）がありましたが、これは情報処理サービス業が運用するシステムの物理的な安全性を認定する制度でした。時代の流れの中で様々な組織においてIT活用が進み、マネジメントシステム全体を見ることが必要となってきたため、2000年度に見直しが行われ、制度廃止の受け皿としてJIPDECでISMS適合性評価制度が生れました。当時は国際規格もなかったため、英国規格協会の情報セキュリティBS-7799-2をもとに策定された日本独自のISMS認証基準をもとに世界に先駆けて運用を開始し、その後2005年に国際規格が発行され世界的に統一された基準で運用されています。ISMS、ISMS適合性評価制度という言葉は、適正に利用していただくため、JIPDECが商標登録して管理しています。

ISMS認証取得組織は右肩上がりに推移しており、2023年6月末現在、日本国内では7,413組織が認証を取得しています。また、ISMS-ACが認定している認証機関は、現在26機関になります。

デジタル社会のニーズを踏まえ、ISMSのセクター認証として2016年にISMSクラウドセキュリティ認証、2020年にISMS-PIMS認証を開始しています。これらは、従来のISMSに上乗せする形で審査/認証するもので、ISMSクラウドセキュリティ認証は現時点で438組織、PIMS認証は47組織が認証を受けています。

## ISO/IEC 27001：2022への移行について

認証の移行期間は3年間（2025年10月31日まで）となっていますが、JIS Q 27001：2014での初回認証及び再認証（更新）を希望する場合は、2024年4月30日までに審査を開始している必要があります。

現在、ISMS-ACでは認定機関として認証機関の審査認定を進めており、今年10月までにはどの認証組織でも新しい規格での認証審査が可能となる予定です。

移行にあたっては、ISO/IEC 27001:2022のJISが発行されるまでは、日本規格協会から発行された対訳版ISO/IEC 27001:2022を参考として使用してください。この場合、認証文書への規格表示は「ISO/IEC 27001:2022」となります。

## よくある質問

Q:JIS版の発行時期は？

A:セミナー配布資料（非公開）では「「2023年度中には日本規格協会より発行公示される予定」とご説明しましたが、現在、対応するJISQ 27001の改正作業が最終段階に入っており、順調に進めば9月頃に発行予定です。質疑応答レポートも併せてご確認ください。

Q:移行審査はどのように実施されるか

A:移行審査は、サーベイランス審査、再認証審査と同時に受けることも、個別に審査を受けることも可能です。移行審査では、新しい規格のもとで新たなマネジメントシステムが構築されPDCAが動かされていることを確認する必要があるので、そこが審査ポイントになります。認証機関が目的を達成できると判断した場合には遠隔審査も可能です。

Q:追加の審査工数は？

A:移行の確認審査を再認証審査と同時に実施する場合は、少なくとも0.5人日が審査工数として追加されます。また、サーベイランス審査と同時実施、または単独審査として実施する場合は、少なくとも1日人の審査工数追加が必要となります。

これは、全ての組織に共通な事項を確認するための最小審査工数のため、実際にかかる工数は、認証機関にご確認ください。

Q:移行審査後、認証の有効期限は変更になりますか？

A:移行審査による認証サイクルの変更はありません。ただし、2025年10月31日を以てその認証は無効となります。

Q:移行審査の前にすべきことは

A: 移行審査では、組織の構築したISMSがISO/IEC 27001:2022に基づいて適切に運用管理されていることを確認するため、移行審査前にISMSの変更の必要性*を決定し、適用宣言書やリスク対応計画の更新、管理策の実施およびその有効性の評価（内部監査、マネジメントレビュー等）を行っておく必要があります。なお、今回はISO/IEC 27001:2022に変更があるため、ISMSの変更が行われることになります。

*ISMSの変更の必要があると決定されたときは、変更の計画策定（ISO/IEC 27002:2022の6.3）をします。

Q:適用宣言書の作り方

A:既存の認証を取得している場合は、新旧規格のギャップ分析を行い、その結果をもとに管理策の対応を確認、新規管理策についてはリスク分析を行い実施の可否を検討します。これらの結果を新たな適用宣言書に反映してください。

Q:ISMSクラウドセキュリティ認証も移行が必要か？

A: ISMSクラウドセキュリティ認証は、認証基準であるJIP-ISMS517-1.0の要求事項に変更はない(注)ので、移行はありません。ただし、その基となるISMS認証がISO/IEC 27001:2022へと変更になるため、それに合わせた対応は必要です。対応状況はISMS認証の移行審査の中で確認されます。

注）JIP-ISMS517-1.0内のJIS Q 27001:2014(ISO/IEC 27001:2013)はISO/IEC 27001:2022に読み替えるものとします。

- ISO/IEC 27001:2022の発行に伴うISMSクラウドセキュリティ認証及びISMS-PIMS認証の対応について（ISMS-AC）

講師所属組織

一般社団法人情報マネジメントシステム認定センター（ISMS-AC）

【センター概要】

ISMS適合性評価制度において、組織の審査・認証を行う認証機関の能力を審査し認定する、認定機関。

※ 2018年4月に、認定機関としての独立性をより明確にし、引き続き客観性及び公平性のある認定活動を推進していくために、JIPDEC（一般財団法人日本情報経済社会推進協会）から独立し、認定業務を行う「一般社団法人情報マネジメントシステム認定センター（略称：ISMS-AC）」として法人化した。

https://isms.jp/

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。