ISMS認証基準（ISO/IEC 27001）の改訂

一般財団法人日本情報経済社会推進協会　セキュリティマネジメント推進室　室長　**成田 康正**

ISMS適合性評価制度における認証基準のISO/IEC 27001が2022年10月25日に改訂されました。

JIPDECは、経済産業省の協力を得ながら2002年度からISMS適合性評価制度を開始し、ISMS（情報セキュリティマネジメントシステム）の普及に取り組んできており、ISO/IEC JTC 1/SC 27における国際標準化活動に積極的に貢献してきました。現在、国内認証機関に対する認定業務は、関連法人である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）に移管しており、ISMS-AC認定下の被認証組織数は増加し続けています（2022年11月現在、約7,100件）。

ISO/IEC 27001は、企業などの組織がISMSを構築・運用するための際に適合すべき事項が定められています。今回の改訂では、ISO/IEC 27001の附属書Aにある情報セキュリティの対策集（情報セキュリティ管理策）を更新しました。附属書Aの管理策は情報セキュリティ対策実施のためのガイダンス規格であるISO/IEC 27002と整合がとられていますが、ISO/IEC 27002が2022年２月に改訂されたため、附属書Aが更新されました。管理策は、最新の動向を考慮して再構成され、追加・統合されて、15分類の構成から４分類（組織的、人的、物理的、技術的）に簡素化されました（管理策数は114から93になりました）。追加された管理策としては、たとえば、「データマスキング（匿名化／仮名化）」「監視活動」等、情報に着目した管理策や積極的な監視・情報収集のための管理策等があります。さらに、管理策の位置づけや効果を理解するための情報として、各管理策に「属性」（attribute）が設けられました。なお、ISO/IEC 27001:2022本文は最新のISOマネジメントシステム共通要素[1]を反映するために若干更新されましたが、大きな変更はなくISO/IEC 27001:2013から高い連続性を維持しています。

ISMS-ACでは、ISMS適合性評価制度の認定機関の立場として、ISMS認証機関が適切にISMSの認証審査を実施できる体制・能力をもっているかを審査し、認定しています。

認証登録証等で認証機関のマーク（図の左）と認定シンボル（図の右）とが２つ並んでいることは、その認証機関が国際規格に従った適切な審査を実施していることを、認定機関であるISMS-ACが保証していることを示します。

認証機関マーク（左）と認定シンボル（右）が並んだ表示例

なお、ISMS認証の移行計画はISMS-ACから発表されており、認証の移行期間として３年間が設定されています。JIPDECおよびISMS-ACでは、認証取得組織が適切にISO/IEC 27001:2022へ認証の移行ができるよう、さまざまな面で情報発信していく予定です。

https://isms.jp/topics/news/20221025.html

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）：https://isms.jp

1　ISO/IEC Directives, Part 1, Annex SL（normative）Harmonized approach for management system standards：マネジメントシステム規格（MSS）の共通要素（共通箇条、共通テキスト、用語等）を定めた附属書