CQI 及び IRCA メンバーの ISO/IEC 27001:2022 への移行に関する推奨事項

ISO/IEC 27001:2022 - 情報セキュリティ、サイバーセキュリティ及びプライバシー保護 - 情報セキュリティマネジメントシステム - 要求事項

本書は、ISO/IEC 27001 の改定に伴い、ISO/IEC 27001:2022 が発行されたことに伴う CQI の立場を説明するために作成されたものです。IRCA 登録 ISMS 審査員の移行研修の要求事項を記載しています。

移行に関する詳細な情報は、IRCA 登録 ISMS 審査員に直接通知されます。

はじめに

ISO/IEC 27001:2022 - 情報セキュリティ、サイバーセキュリティ及びプライバシー保護 - 情報セキュリティマネジメントシステム - 要求事項は、組織の文脈の中で、情報セキュリティマネジメントシステムを確立、実施、維持及び継続的に改善するための要求事項を規定しています。また、組織のニーズに合わせた情報セキュリティリスクの評価と対応に関する要求事項も規定しています。

この規格は、組織の情報資産を保護することを意図して作成されています。情報資産とは、組織にとって「価値がある」と認識されている、あらゆる方法で保存されている定義可能な情報と考えることができます。情報資産の例には以下が含まれます。

- 戦略、計画、到達点 (goals)、目的 (objectives)
- 特許権、著作権、商標権
- プロジェクトの記録
- マーケティングメディア
- 運用及び財務データ
- 法務及びコンプライアンス情報
- 研究開発の記録

ISO/IEC 27001:2022 は、一連の管理策と組み合わせたマネジメントシステムの適用により、このような情報の機密性、完全性、可用性を維持することを目指しています。これらの管理は、ISO/IEC 27001 だけでなく、ISO/IEC 27002 にも記載されています。

ISO/IEC 27001:2022 の変更点概要

第 0 条から第 10 条までの実質的な本文は、2 つの版においてほとんど変更されていませんが、構造、用語、語順などには、気を付けるべき修正が加えられています。

しかし、最も大きな影響は、この文書の附属書 A (規定) の再編成から生じます。この附属書に記載されている管理策は、2022 年 3 月に発行された ISO/IEC 27002 - Information Security, Cybersecurity and Privacy Protection - Information Security Controls (情報セキュリティ、サイバーセキュリティ及びプライバシー保護 – 情報セキュリティ管理策) から直接引用されています。これらの管理策には、大幅な改訂が行われました。管理策のカテゴリーが変更され (14 から 4 つの「テーマ」に減少)、管理目的が附属書に表示されなくなり、2013 年版の個々の管理策は更新、統合、番号変更、場合によっては削除されました。さらに、11 個の新しい管理策が追加されました。

また、新しい ISO/IEC 27002:2022 に基づく管理策の分類と順序についても、学習者に伝える必要がある変更があります。

IRCA 登録 ISMS 審査員の移行要求事項

グレードに関係なく、すべての IRCA 認定 ISMS 審査員は、2025 年 10 月の 3 年間の移行期間終了までに、ISO/IEC 27001:2022 に関する知識、スキル、経験を最新ものにしておくことが求められています。

そのためには、CQI 及び IRCA 認定の適切な ISO/IEC 27001:2022 審査員トレーニングコースを修了することが推奨されます。あるいは、審査員は、適切な CPD を通じて、知識、スキル、経験の習得を証明する必要があります。適切な CPD には、トレーニングコース、コンファレンス、セミナーへの参加、オンライン学習またはウェビナーコースへの参加、個人学習及び読書が含まれますが、これらに限定されるものではありません。

また、情報セキュリティマネジメントシステムに責任を持つ CQI メンバーは、適切な CPD を通じて必要な知識、スキル、理解を習得することが強く奨励されます。

附属書 - ISO/IEC 27002 附属書 A の変更点

附属書 A は附属書 (規定) のままですが、2022 年版では「管理目的及び管理策」から「情報セキュリティ管理策」に名称が変更されます。

管理目的は 2022 年版の管理策のリストからは削除されます。

ISO/IEC 27002:2022 で行われた大幅な変更に呼応して、この附属書の内容も大幅に変更されました。

これまでの 14 種類の管理策（情報セキュリティのための方針群、情報セキュリティのための組織、人的資源のセキュリティ、資産の管理、アクセス制御、暗号、物理的及び環境的セキュリティ、運用のセキュリティ、通信のセキュリティ、システムの取得、開発及び保守、供給者関係、情報セキュリティインシデント管理、事業継続マネジメントにおける情報セキュリティの側面、順守）は、新たな 4 つの「テーマ」、組織の管理策 (Organizational Controls)、人々の管理策 (People Controls)、物理的管理策 (Physical Controls)、及び技術的管理策 (Technological Controls) に置き換わりました。

2013 年版の 14 のカテゴリーに関連する管理目的は、すべて削除されました。

ISO/IEC 27002 の第 3 版はまた

- 管理策を「是正型 corrective」「予防型 preventive」「検出型 detective」に分類し、その管理策が「機密性」、「完全性」、「可用性」のいずれかを、またこれらの組合せをサポートしようとしているのかを特定し、
- その管理策が「識別 identify」、「保護 protect」、「検出 detect」、「対応 respond」または「回復 recover」のためのものなのかどうかを特定し、
- それらの管理策が、ガバナンス、資産の管理、情報の保護、人的資源のセキュリティ、物理的セキュリティ、システム及びネットワークのセキュリティ、アプリケーションのセキュリティ、セキュアな構成、アイデンティティ及びアクセスの管理、脅威及び脆弱性の管理、継続性、サプライヤー関係のセキュリティ、法務及びコンプライアンス、情報セキュリティイベント管理、情報セキュリティの保証に関連するものかどうかを特定し、
- その管理策が、ガバナンスとエコシステム (Governance and Ecosystem)、保護 (Protection)、防衛 (Defence)、レジリエンス (Resilience) に関連するものかどうかを特定しています。

管理策の総数は 114 から 93 に削減されました。2013 年版の管理策は、一部が統合され、一部が削除され、一部は「そのまま」引き継がれました。これら変更されたものは、2022 年版の 93 の管理策のうち 82 を占めます。これに加え、11 個の新しい管理策が追加されました。

- Threat Intelligence (脅威インテリジェンス)
- Information security for use of cloud services (クラウドサービス利用時の情報セキュリティ)
- ICT readiness for business continuity (事業継続のための ICT 準備度)
- Physical security monitoring (物理的なセキュリティ監視)
- Configuration management (構成管理)
- Information deletion (情報の削除)
- Data masking (データマスキング)
- Data leakage prevention (データ漏えい防止)
- Monitoring activities (監視活動)
- Web filtering (Web フィルタリング)
- Secure coding (セキュアコーディング)

ISO/IEC 27002:2022 の附属書 B には、2022 年版の管理策を 2013 年版の管理策に、またその逆にマッピングする 2 つの便利な対応表が 含まれています。

このブリーフィングノートの内容に関して、さらに説明が必要な場合は、policy@quality.org までご連絡ください。