

## 1. ISO/IEC27001:2022 移行についてのよくある質問r1

1	質問	すでに ISO 27001:2013 の認証を取得していますが、現時点で必要な手続きはありますか？
	回答	現在、有効な ISO 27001:2013 認証をお持ちの場合は、正式に ISO 27001:2022 が発行された時に移行が必要になります。2022 年 10 月 25 日に ISO 27001:2022 は発行されました。ISO/IEC は英語のため、日本語版は JIS Q 27001 の発行をお待ちいただくことになります。JIS については、現状発行予定は未定です。前回(2013 年時)の改訂では、年明け 3 月でしたので、2023 年 3 月までに発行される見込みです。
2	質問	ISO 27001:2022 はいつ発行されますか？
	回答	2022 年 10 月 25 日に正式に発行されました。 ガイドラインに該当する ISO 27002:2022 は先行して、2022 年 2 月 15 日に発行されました。
3	質問	現在有効な ISO 27001:2013 を 27001:2022 にいつ移行すればいいですか？ (現在の認証が廃止されるのはいつですか?)
	回答	組織は、2022 年版の発行月の最終日から 36 か月以内に、既存の ISO 27001:2013 から ISO 27001:2022 に移行する必要があります。2025 年 10 月末までに移行審査を完了する必要があります。それ以降は 2013 年版は無効となります。  注 1: 認証機関 (Certification Europe 等) は、ISO 27001:2022 の発行月の最終日から 12 か月以内に ISO 27001:2022 の審査と認証を開始しなければなりません。また、すべての被認証組織の移行が 36 か月以内に完了するよう IAF MD26:2022 に規定されています。
4	質問	ISO 27001:2022 移行審査はどのように実施されますか？
	回答	認証機関は、実施予定のサーベイランス審査もしくは再認証審査と併せて移行審査をするか、または (認証サイクル内の審査に加えて) 別途、移行審査のみ行うことができます。認証機関が認定機関の審査を受け、移行審査の許可を得てから、受審組織に移行審査を提供いたします。発行後 12 ヶ月以内に開始することが求められています。
	注 2:	一般的に、実施予定のサーベイランス審査と併せて移行審査を実施する場合は、移行審査のみ実施する場合よりも審査時間は短くなります。
	注 3:	移行審査は、特に条項 8 の技術的管理策の審査について、文書のレビューだけでなく、インタビューと観察も必要になります。注 2: 一般的に、実施予定のサーベイランス審査と併せて移行審査を実施する場合は、移行審査のみ実施する場合よりも審査時間は短くなります。
5	質問	移行審査にはどのくらいの追加時間が必要になる可能性がありますか？
	回答	移行審査はサーベイランス審査の一貫として行われるか、個別の審査として行われるかにかかわらず、ISMS の移行を確認するために少なくとも 0.5 工数を追加しなければなりません。
6	質問	移行審査はどのように発動され、計画されるのですか？
	回答	移行審査は認証機関の ISO27001 審査プログラムの一部として発動され、計画されなければなりません。これには認証機関が「移行審査申込書」(仮)に記入するために貴組織に連絡を取り、その後、合意された適切かつ十分な移行審査計画(質問 2～質問 5 の回答の要求事項)を作成するために協力しなければならないことが含まれています。
7	質問	認証機関の移行審査はどのように決定されますか？
	回答	認証機関は、移行審査の結果/所見に基づいて移行を判定し、受審組織の ISMS が ISO27001:2022 の要求事項を満たした場合、新しい登録証を発行します。(現在の認証サイクルは変更されません。)
8	質問	現在の ISO 27001:2013 はいつ失効しますか？
	回答	ISO 27001:2013 に基づくすべての登録証は、移行期間(36 か月)終了後に失効または取り消されます。
9	質問	ISO 27001:2013 の認証を取得していますが、今後どうすればいいですか？
	回答	2022 年版の発行月の最終日から 36 か月以内に移行することになります。2025 年 10 月末までの定期審査にて移行審査を同時に受審いただくか、それとは別に移行審査を単独で受審することで 2022 年版への移行を行うことができます。コンサルタントの指導を受けている組織は、コンサルタントと移行計画をご相談ください。コンサルタントの指導を受けていない場合、適切なコンサルをお探しであればご連絡願います。

10	質問	組織として、ISO 27001:2022 への適合を保証するために、どのように ISMS を移行すればよいのでしょうか？
	回答	<p>ここでは、2つの移行アプローチを例示します。</p> <p><b>1. すべてリプレイス(再配置)する場合:</b> この移行アプローチでは、ISMS のリスクアセスメントとリスク対応を ISO 27001:2022 に基づいて総点検します。そして、ISO27001:2013 附属書 A(適用宣言書)の管理策の参照をすべて解除し、ISO 27001:2022 附属書 A の順に設定し直し、参照する手順との整合を再度行います。“完全な置き換え”型移行アプローチを反映し、ISO 27001:2022 附属書 A の管理策を参照できるように全面的に再配置する必要があります。</p> <p><b>2. 2013 年版の附属書 A(管理策)を継続使用する場合:</b> この移行アプローチでは、ISO 27001:2013 附属書 A の管理策を継続して運用します。既存の ISO 27001:2013 附属書 A(適用宣言書)の管理策と新しい ISO 27001:2022 附属書 A の管理策を比較し、追加・統合された管理策について、もれなく適合しているという(文書化した)証拠が必要となります。照合表の作成や追加の管理策の統合、内部監査での附属書 A の審査方法等、上記 1 よりも知識が必要となると考えられます。</p> <p>どちらにつきましても ISO 27002:2022 と ISO 27002:2013 を比較した ISO 27001:2022 附属書 B の参照が推奨されます。さらに既存の適用宣言書から ISO 27001:2022 附属書 A の管理策を参照することを確実にするために、適用宣言書の技術的な更新/変更を行う必要があり、そのための知識の習得が必須となります。</p>

