JIS Q 27001:2014 FAQ

その１

注意事項：

① 本書に示した回答は、一般的な事例です。考え方の一つとして参考にする程度が望まれます。

② 各規格項番及び附属書 A. の各管理策は、それぞれが単独で存在するのではなく、全てがオーバーラップする構造になっています。したがって、同じ事例が本書での説明で使用する管理策と、他で発信される情報で使用される管理策と相違する場合があります。それは、中心をどこに置いて考えるかで変わってきます。そのような要素を持っていると認識することが重要です。

No.	項番	質問	回答
1	6.1.3 d)	Q1. 「適用宣言書」は改訂する必要がありますか？	A1.「適用宣言書」は附属書 A.に対して以下のことを示すものです。従って、移行審査を受けるにあたって 2014 年版に対応したものでなければなりません。 (1) 必要な管理策[6.1.3 の b 及び c 参照]及びそれらの管理策を含めた理由 (2) それらの管理策を実施しているか否か (3) 附属書 A に規定する管理策を除外した理由
2	7.2 a) 9.2 a)2)	Q2. 2014 年版に移行する際に行う内部監査員の力量はどこまで要求されますか？	A2. 2014 年版に適合していることを確認できる力量が必要です。
3	全般	Q3. 2006 年版に比べて抽象的な表現が多くなり分かりにくくなりました。何故ですか？	A3. (1)2006 年版の手段、基準及び技術的な要素は、適用組織自身が考えることとして排除されました。 (2)“Policy”を中核とした規格構造になっています（日本語では“方針”と訳していますが、正確な日本語訳がありません)。組織自身が Policy でフレームワークを明確にし、Policy に従った具体的手段を決定し、その妥当性を客観的に評価し、改善する仕組みを規格が規定しています。
4	6.1	Q4. ベースラインアプローチに終始しています。全面的にやり直しが必要ですか。	A4. 規格はリスクアセスメントの手順を要求するものではありませんが、6.1.1 項～6.1.2 項の要求事項は満たす必要があります。 全てをベースラインアプローチで行っていると、項目を満たさない可能性があります。

No.	項番	質問	回答
5	全般	Q5. 一部から移行を始めた場合の注意事項を教えてください。	A5. 根拠を持って移行する優先順位などを決めませんと、論理不整合が出る可能性があります。 また、一部を移行すると移行した箇所と、残された箇所間でも不整合を起こす可能性があります。
6		Q6. “予防処置”が無くなりました。不要と言うことでしょうか？当社では、現場からの仕組み改善提言を対象にしています。	A6. 予防処置はリスクマネジメントそのものであるため、6.1 の「望ましくない影響を防止する…」という文章にあらわれています。
7	附属書 A.8.1.1	Q7. 資産目録の内容が変わりましたが、どのように変わったのですか？	A7. 以前はすべての重要な資産の目録を作成し、維持しなければなりませんでしたが、情報及び情報処理施設に関連する資産の目録作成と維持に限定されました。
8	4.3	Q8. 適用範囲をどう決めればよいのか？	A8. (1)内部・外部の課題や利害関係者のニーズを考慮して決定する。 (2) 少なくても ISMS の構築・維持管理に必要な経営資源を用意することができる権限を持った人が、トップマネジメントに位置づけされること。適用範囲と適用範囲外の境界を管理できることが必要です。
9	5.1	Q9. リーダーシップは、現場の管理職まで要求されるのですか？	A9. 規格の 5.項は、すべてトップマネジメント（複数も可）に対する要求になっています。ただし、5.1 h)では、その他関連する管理層の責任の領域において、(それら管理層の)リーダーシップを実証するよう、それら管理層の役割を支援することがトップマネジメントに求められており、間接的には、管理層にもそれぞれの責任に応じたリーダーシップは求められていることになります。
10	5.3	Q10. 2006 年版の構築時にコンサルタントから 5.2.1 項は、ISMS 管理責任者を置くことを要求していると言われました。 2014 年版では、ISMS 管理責任者は置かなくても良いですか？	A10. 2006 年版でも ISMS 管理責任者の設定要求はありませんでした。 2014 年版でも変更はありません。 ISMS の効果的な管理の考え方で決定して下さい。

No.	項番	質問	回答
11	6.1	Q11. リスクアセスメントプロセスが大きく変わりました。2006年版で構築したリスクアセスメントマニュアルは無効と言うことでしょうか？	A11. 2006年版の中で、情報セキュリティリスクにさほど影響のない資産まで棚卸をすることがありました。 2014年版では、リスクアセスメントに当たって、まずその対象を絞り込んでから行うことを推奨しています。 情報のリスクアセスメント手順そのものは、2006年版と大きく変わるものでありません。
12	6.1	Q12. 新規格には、あらたな追加要求として、6.1リスク及び機会に対処する活動がありますが、この機会の定義は、どのように解釈したらよいか、 具体的にどんなものが想定されるのか、	A12. 用語「機会(opportunity)」に対してISOの中では定義がありません。意味は、例えば、マネジメントレビューの決定、監査や審査における改善指摘(C指摘)への対応など「継続的改善のための機会」と理解するとよいでしょう。しかし、これら機会に対して突き詰めて考えると、リスクへの対応に該当し、リスク及び機会の違いを厳密に区別することはできないかもしれません。 JIPDEC ISMS ユーザーズガイドでは、“この「機会」をどのように解釈するかということよりも、リスクマネジメントにおける事業リスクを理解することが重要です。（中略）「4.1 組織及びその状況の理解」との整合性を確保することが、リスクマネジメントの重要なポイントであると考えられます。”とあり、厳密な用語の違いに捕らわれるよりも、組織及びその状況に適したISMSを構築、維持し、継続的改善を進めることが重要であるとしています。
13	6.1.2	Q13. リスクアセスメントプロセスでは“脅威”、“脆弱性”の言葉が無くなりました。考慮は不要になったのでしょうか？	A13. JIPDECユーザーズガイドでは、“脅威”及び“脆弱性”は、リスクを生じさせる要素の典型例であるとの記載があり、また、脅威と脆弱性を用いたリスクアセスメントの例も紹介されています。“脅威”、“脆弱性”として個々に特定する要求はなくなりましたが、脅威、脆弱性に関する何らかの考慮は必要であり、まったく考慮が不要になった訳ではありません。

No.	項番	質問	回答
14	6.1.2	Q14. a) 2)“情報セキュリティリスクアセスメントを実施するための基準”とは、どのようなものを決めれば良いですか？	A14. リスクアセスメントの見直しを行う基準を求めています。要素として、次の 2 点があります。 (1)定期的に行う (2)臨時に行う
15	全般	Q15. 移行審査の対象となる期間の途中まで 2006 年版での活動になりますが、それでも大丈夫ですか？	A15. システム移行までは当然 2006 年版になりますので、問題はありません。 2014 年版での運用期間が関係する場合がありますので、詳細は認証サービス部　ISMS 担当にお問い合わせください。
16	全般	Q16. 移行審査を受審する期限が 2015 年 5 月で、再認証審査やサーベイランス審査のタイミングで行うことを進めていますが、当社の場合はチャンスが 1 回しかありません。	A16. 審査時期に関しては、再認証審査やサーベイランス審査のタイミングで行う以外に、臨時の変更審査を行うこともできます。担当営業にご相談ください。