ISO27001：2013、JIS Q 27001：2014の概要（主旨）

**１．4章の主旨**

**組織をとりまく内外の状況や利害関係者のニーズ及び期待を理解、決定し、それら**

**を考慮に入れたうえでISMSの適用範囲を定めることが求められている。**

４ 組織の状況

4.1 組織及びその状況の理解

4.2 利害関係者のニーズ及び期待の理解

4.3 情報セキュリティマネジメントシステムの適用範囲の決定

4.4 情報セキュリティマネジメントシステム

**２．5章の主旨**

**ISMSを推進し、関係者の意識向上を図るためには、トップマネジメントの強力なリ**

**ーダーシップが不可欠である。ここでは、トップマネジメントの果たすべき役割につ**

**いて規定している。**

5 リーダーシップ

5.1 リーダーシップ及びコミットメント

5.2 方針

5.3 組織の役割、責任及び権限

**３．6章の主旨**

**ISMSにおけるリスク及び機会を決定し、情報セキュリティリスクアセスメント、情報セキュリティリスク対応のプロセスを定めて適用することが求められている。**

**「規定」である「附属書A管理目的及び管理策」は、6.1.3において、附属書Aの管理**

**策と組織が適用した管理策を比較し、除外した場合にはその理由を適用宣言書に**

**記載することが求められている。**

6 計画

6.1 リスク及び機会に対処する活動

　6.1.1 一般

**6.1.2 情報セキュリティリスクアセスメント**

**6.1.3 情報セキュリティリスク対応**

6.2 情報セキュリティ目的及びそれを達成するための計画策定

**４．7章の主旨**

**ＩＳＭＳの各箇条で要求される文書類を文書化し、管理し、維持しながら、要員の力量、並びに利害関係者との反復的かつ必要に応じたコミュニケーションを確立する**

**ことを通じた、ISMSの運用の支援について規定している。**

7 支援

7.1 資源

7.2 力量

7.3 認識

7.4 コミュニケーション

7.5 文書化した情報

**５．8章の主旨**

**情報セキュリティの要求事項を実現するために必要なプロセス群の、策定、導入・実施、及び管理について規定している。また、そのために不可欠な情報セキュリティリスクアセスメント、情報セキュリティリスク対応の実施についても規定している。**

8 運用

8.1 運用の計画及び管理

**8.2 情報セキュリティリスクアセスメント**

**8.3 情報セキュリティリスク対応**

**６．9章の主旨**

**情報セキュリティパフォーマンスの評価（監視、測定、分析及び評価）、内部監査及びマネジメントレビューについて規定している。**

9 パフォーマンス評価

9.1 監視、測定、分析及び評価

9.2 内部監査

9.3 マネジメントレビュー

７．10章の主旨

**不適合発生時の処置、及びとった処置の文書化と、ISMSの適切性、妥当性及び有**

**効性の継続的改善について規定している。**

10 改善

以上