1.概要

ISO27001:2013 はマネジメントシステム規格の構成について ISO 指令（Annex SL）に準じ、新たに以下の章立てとなっています。

第 4 章：組織の状況
第 5 章：リーダーシップ
第 6 章：計画
第 7 章：支援
第 8 章：運用
第 9 章：パフォーマンス評価
第 10 章：改善

管理策の数は減り（2005 年の 133 項目から 2013 年では 114 項目へ）、管理群は増えました（2005 年の 11 項目から 2013 年では 14 項目へ）。

改訂版では、組織のプロセスの中に情報セキュリティを統合することを強調しています。また、組織がその外部状況及び内部状況、ならびに利害関係者のニーズ及び期待を決定しなければならないという要求事項もあります。これは本書に含まれていますが、これらの状況、利害関係者のニーズと期待の決定と適用は、当規格を通して繰返し言及されるテーマとなっています。

一方で文書化された手順に対しての要求は緩和されています。改訂版では、Annex SL から“文書化した情報”というコンセプトが導入されています。

リスクアセスメントの方法に対しても要求が緩和されています。2005 年版では資産に対するリスクアセスメントであったのに対し、改訂版では情報およびプロセスに対するリスクアセスメントとなっています。当規格でのリスクマネジメントの方法は ISO31000（リスクマネジメント - 原則と指針）に則しており、組織は様々な分野（例えば、情報セキュリティ、健康と安全、企業のリスクマネジメント）に渡ってリスクマネジメントを整合化することができるようになりました。

2.マネジメントシステムの章

【4. 組織の状況】

4.1 組織及びその状況の理解

組織の目的に関連し、かつ、その ISMS の意図した成果を達成する組織の能力に影響を与える、外部及び内部の課題を決定することを求めています。

ISO27001:2013 の他の多くの要求事項が、組織による外部及び内部の課題と利害関係者のニーズと期待をどう決定するかに左右されるということに注意してください。

外部状況の例:

- 政策
- 法律
- 規制
- 財政
- 技術
- 経済
- 自然環境
- 競合環境
- 地理／領土的範囲　- 国際的、国内、地域
- 外部ステークホルダーとの関係と認識
- 社会、文化　等

内部状況の例:

- 政策、目的、戦略
- ガバナンス、組織構成、役割、アカウンタビリティ
- 内部ステークホルダーとの関係、認識／価値
- 組織の文化
- 情報システム、情報の流れ、意思決定プロセス
- 組織が採用する規格、指針、モデル
- 契約関係
- 能力、資源（資本、時間、人、プロセス、システム、テクノロジー）、知識　等

4.2 利害関係者のニーズ及び期待の理解

利害関係者の要求事項には、法的及び規制の要求事項並びに契約上の義務を含めることが出来るので、内部及び外部の状況と矛盾がないことを確認すべきです。

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

適用範囲を定めるためには、外部及び内部の課題（4.1）とともに、利害関係者のニーズと期待（4.2）を検討しなければなりません。ここでも 4.1 および 4.2 が関わってきます。