

付属書 SL Appendix 3 と ISO/IEC 27001:2013 の比較 【規格の全体像】

付属書 SL Appendix 3	ISO/IEC 27001:2013	備考
序文	序文	序文、適用範囲、引用規格の項については同一の上位構造(条項)を採用。但し、内容は ISMS 特有の記述。
1. 適用範囲	1 適用範囲	
2. 引用規格	2 引用規格	
3. 用語及び定義	3 用語及び定義	同一の上位構造(条項)。ISO/IEC 27000 を引用
4. 組織の状況	4 組織の状況	同一の上位構造(条項)。要求事項を構成。
4.1 組織及びその状況の理解	4.1 組織及びその状況の理解	<p>4章が求めていること 組織は、何のために ISMS を導入するかを自らに問い、その目的のために適当な ISMS を構築する</p>
4.2 利害関係者のニーズ及び期待の理解	4.2 利害関係者のニーズ及び期待の理解	
4.3 XXX マネジメントシステムの適用範囲の決定	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 XXX マネジメントシステム	4.4 情報セキュリティマネジメントシステム	
5. リーダシップ	5 リーダシップ	<p>5章が求めていること 経営者の積極的な関与は、最重要</p>
5.1 リーダシップ及びコミットメント	5.1 リーダシップ及びコミットメント	
5.2 方針	5.2 方針	
5.3 組織の役割、責任及び権限	5.3 組織の役割、責任及び権限	<p>6章が求めていること 4章で明らかになった目的の達成と課題解決のために情報セキュリティリスクをどのように扱うかを計画 PDCA</p>
6. 計画	6 計画	
6.1 リスク及び機会に対処する活動	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 XXX 目的及びそれを達成するための計画策定	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	<p>7章が求めていること マネジメントシステムを支援する基本要素。業務遂行上、当たり前のこと。ISMS に特化したものではない。</p> <p>支援</p>
7. 支援	7 支援	
7.1 資源	7.1 資源	
7.2 力量	7.2 力量	
7.3 認識	7.3 認識	
7.4 コミュニケーション	7.4 コミュニケーション	
7.5 文書化した情報	7.5 文書化した情報	
7.5.1 一般	7.5.1 一般	
7.5.2 作成及び更新	7.5.2 作成及び更新	
7.5.3 文書化した情報の管理	7.5.3 文書化した情報の管理	
8. 運用	8 運用	
8.1 運用の計画及び管理	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	
9. パフォーマンス評価	9 パフォーマンス評価	<p>8章が求めていること 6章の計画を実践。リスクを特定し、対応策(管理策)を実施。PDCA</p>
9.1 監視、測定、分析及び評価	9.1 監視、測定、分析及び評価	<p>9章が求めていること 成果を確認。PDCA サイクルの基本。ISMS に特化したものではない。PDCA</p>
9.2 内部監査	9.2 内部監査	
9.3 マネジメントレビュー	9.3 マネジメントレビュー	
10. 改善	10 改善	<p>10章が求めていること 上手く行かない所を正す。PDCA サイクルの基本。ISMS に特化したものではない。PDCA</p>
10.1 不適合及び是正措置	10.1 不適合及び是正処置	
10.2 継続的改善	10.2 継続的改善	