

2013/04/05

カイゼン総合支援研究所

三角 忠茂

## ISO27001、27002次期改定について

はじめに

本年3月末に本年9月末 IS 発行予定の DIS (Draft International Standard) が発行され、改定作業はいよいよ佳境を迎えつつある。これに先立ち2012年2月に今後発行される国際規格の構成 ; Annex SL (旧 Guide 83) も改定され、以後発行予定の MSS はマネジメントシステム共通構造 (HLS ; High level structure) の採否を決定し、発行されることになり ISO27001 はこれを採用し改定されている。

### 1. 国際規格改定作業6ステージ

Step1 ; **NP** (New Work Item Proposal)

Step2 ; **WD** (Working Draft)

Step3 ; **CD** (Committee Draft)

Step4 ; **DIS** (Draft International Standard) 2013/3

Step5 ; **FDIS** (Final Draft International Standard)

Step6 ; **IS** (International Standard)

2013年9月末 IS 発行、2014年3月末 JIS 版発行予定

### 2. 改定の目的、目標

27001 ;

- ・通常の3年の見直しとして作業着手
- ・必要最小限度の変更、用語の両立性及び明確化
- ・ISO マネジメントシステム共通構造 HLS の採用

27002 ; 附属書 A

- ・通常の3年の見直しとして作業着手
- ・最新の開発管理策 (IT 技術) への更新及び27001との重複排除
- ・逸脱や遅延の極小化
- ・管理目的との整合

### 3.2005年版と2013年版の章立

2005	2013
序文	序文
1. 適用範囲	1. 適用範囲
2. 引用規格	2. 引用規格
3. 用語及定義	3. 用語及定義
4. ISMS要求事項	4. 組織の状況
4.1 一般要求事項	4.1 組織及びその状況の理解
4.2.1 ISMSの確立	4.2 利害関係者のニーズ及び期待の理解
4.2.2 ISMSの導入及び運用	4.3 ISMSの範囲の決定
4.2.3 ISMSの監視及び見直し	4.4 ISMS
4.2.4 ISMSの維持及び改善	5. リーダーシップ
4.3.1 一般	5.1 一般
4.3.2 文書管理	5.2 リーダーシップ及びコミットメント
4.3.3 記録の管理	5.3 方針
5.1 経営陣のコミットメント	5.4 組織の役割、責任及び権限
5.2.1 経営資源の提供	6. 計画
5.2.2 教育・訓練、認識及び力量	6.1 リスク及び機会への取り組み
6. 内部監査	6.2 目的及びその達成のための計画策定
7. マネジメントレビュー	7. サポート
8. ISMSの改善	7.1 資源
8.1 継続的改善	7.2 力量
8.2 是正処置	7.3 認識(自覚)
	7.4 コミュニケーション
	7.5 文書化した情報
	7.5.1 一般
	7.5.2 作成及び更新
	7.5.3 文書化した情報の管理
	8. 運用
	8.1 運用の計画及び管理
	8.2 アセスメント
	8.3 リスク対応
	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
	10. 改善
	10.1 不適合及び是正処置
	10.2 継続的改善

おわりに

今回お伝えした情報は、今後の改定ステージの進捗状況に応じて変更されるであろうが、改定は着実に進捗している。改定後もこの MSS を活用しようと計画されている組織は、以下のことに考慮・留意する必要があるかもしれない。

- 1.現在の MS は真に規格の意図を漏れなく反映しかつ導入の目的を満たし、狙ったパフォーマンスが上がっているか
- 2.追加要求事項又は見直すべきシステムについての理解、システム化準備の設計開発をどのように進めていくのか