ISO/IEC 27001:2022（JIS Q 27001:2023）要求事項体系図

ISO/IEC専門業務用指針第1部　統合版ISO補足指針
附属書SL Appendix 2
MSSのための調和させる構造
（共通の箇条番号，箇条タイトル，テキスト並びに共通用語及び中核となる定義）

- 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 XXX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
- 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 XXX方針
  - 5.3 役割，責任及び権限
- 6 計画策定
  - 6.1 リスク及び機会への取組
  - 6.2 XXX目的及びそれを達成するための計画策定
  - 6.3 変更の計画策定
- 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
    - 7.5.1 一般
    - 7.5.2 文書化した情報の作成及び更新
    - 7.5.3 文書化した情報の管理
- 8 運用
  - 8.1 運用の計画策定及び管理
- 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
    - 9.2.1 一般
    - 9.2.2 内部監査プログラム
  - 9.3 マネジメントレビュー
    - 9.3.1 一般
    - 9.3.2 マネジメントレビューへのインプット
    - 9.3.3 マネジメントレビューの結果
- 10 改善
  - 10.1 継続的改善
  - 10.2 不適合及び是正処置

※組織が自律的に実施し，維持し，継続的に改善できるシステムの確立

PLAN

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

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

DO

※優先順位付けをし，戦略的なレベルでの取り組み

PLAN

6 計画策定
- 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
- 6.3 変更の計画策定

比較検証

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
  - 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

DO

8 運用

※現場レベルでの実施プロセス

PLAN
- 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

DO
- 8.3 情報セキュリティリスク対応

CHECK

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
  - 9.2.1 一般
  - 9.2.2 内部監査プログラム
- 9.3 マネジメントレビュー
  - 9.3.1 一般
  - 9.3.2 マネジメントレビューへのインプット
  - 9.3.3 マネジメントレビューの結果

ACT

10 改善
- 10.1 継続的改善
- 10.2 不適合及び是正処置

附属書A

5 組織的管理策
- 5.1 情報セキュリティのための方針群
- 5.2 情報セキュリティの役割及び責任
- 5.3 職務の分離
- 5.4 管理層の責任
- 5.5 関係当局との連絡
- 5.6 専門組織との連絡
- 5.7 脅威インテリジェンス
- 5.8 プロジェクトマネジメントにおける情報セキュリティ
- 5.9 情報及びその他の関連資産の目録
- 5.10 情報及びその他の関連資産の許容される利用
- 5.11 資産の返却
- 5.12 情報の分類
- 5.13 情報のラベル付け
- 5.14 情報の転送
- 5.15 アクセス制御
- 5.16 識別情報の管理
- 5.17 認証情報
- 5.18 アクセス権
- 5.19 供給者関係における情報セキュリティ
- 5.20 供給者との合意における情報セキュリティの取扱い
- 5.21 情報通信技術(ICT)サプライチェーンにおける情報セキュリティの管理
- 5.22 供給者のサービス提供の監視，レビュー及び変更管理
- 5.23 クラウドサービスの利用における情報セキュリティ
- 5.24 情報セキュリティインシデント管理の計画策定及び準備
- 5.25 情報セキュリティ事象の評価及び決定
- 5.26 情報セキュリティインシデントへの対応
- 5.27 情報セキュリティインシデントからの学習
- 5.28 証拠の収集
- 5.29 事業の中断・阻害時の情報セキュリティ
- 5.30 事業継続のためのICTの備え
- 5.31 法令，規制及び契約上の要求事項
- 5.32 知的財産権
- 5.33 記録の保護
- 5.34 プライバシー及び個人識別可能情報(PII) の保護
- 5.35 情報セキュリティの独立したレビュー
- 5.36 情報セキュリティのための方針群，規則及び標準の順守
- 5.37 操作手順書

6 人的管理策
- 6.1 選考
- 6.2 雇用条件
- 6.3 情報セキュリティの意識向上，教育及び訓練
- 6.4 懲戒手続
- 6.5 雇用の終了又は変更後の責任
- 6.6 秘密保持契約又は守秘義務契約
- 6.7 リモートワーク
- 6.8 情報セキュリティ事象の報告

7 物理的管理策
- 7.1 物理的セキュリティ境界
- 7.2 物理的入退
- 7.3 オフィス，部屋及び施設のセキュリティ
- 7.4 物理的セキュリティの監視
- 7.5 物理的及び環境的脅威からの保護
- 7.6 セキュリティを保つべき領域での作業
- 7.7 クリアデスク・クリアスクリーン
- 7.8 装置の設置及び保護
- 7.9 構外にある資産のセキュリティ
- 7.10 記憶媒体
- 7.11 サポートユーティリティ
- 7.12 ケーブル配線のセキュリティ
- 7.13 装置の保守
- 7.14 装置のセキュリティを保った処分又は再利用

8 技術的管理策
- 8.1 利用者エンドポイント機器
- 8.2 特権的アクセス権
- 8.3 情報へのアクセス制限
- 8.4 ソースコードへのアクセス
- 8.5 セキュリティを保った認証
- 8.6 容量・能力の管理
- 8.7 マルウェアに対する保護
- 8.8 技術的ぜい弱性の管理
- 8.9 構成管理
- 8.10 情報の削除
- 8.11 データマスキング
- 8.12 データ漏えい防止
- 8.13 情報のバックアップ
- 8.14 情報処理施設・設備の冗長性
- 8.15 ログ取得
- 8.16 監視活動
- 8.17 クロックの同期
- 8.18 特権的なユーティリティプログラムの使用
- 8.19 運用システムへのソフトウェアの導入
- 8.20 ネットワークセキュリティ
- 8.21 ネットワークサービスのセキュリティ
- 8.22 ネットワークの分離
- 8.23 ウェブフィルタリング
- 8.24 暗号の利用
- 8.25 セキュリティに配慮した開発のライフサイクル
- 8.26 アプリケーションセキュリティの要求事項
- 8.27 セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則
- 8.28 セキュリティに配慮したコーディング
- 8.29 開発及び受入れにおけるセキュリテイテスト
- 8.30 外部委託による開発
- 8.31 開発環境，テスト環境及び本番環境の分離
- 8.32 変更管理
- 8.33 テスト用情報
- 8.34 監査におけるテスト中の情報システムの保護

2024.04.16