ISO27001 要求事項と管理策対応表

要求事項	内容	-	管理策	内容
4.1	組織及びその状況の理解	⇒	ー	ー
		⇒	5.7	脅威インテリジェンス
4.2	利害関係者のニーズ及び期待の理解	⇒	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
5.1	リーダーシップ＆コミットメント	⇒	-	-
5.2	方針	⇒	-	-
5.3	責任及び権限	⇒	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
		⇒	5.15	アクセス管理
		⇒	5.16	識別情報の管理
		⇒	5.17	認証情報
		⇒	5.18	アクセス権
		⇒	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
6.1	計画策定	⇒	-	-
6.1.2	リスクアセスメント	⇒	-	-

7.1	資源	⇒	5.9	情報及びその他の関連資産の目録
		⇒	5.11	資産の返却
		⇒	5.14	情報の転送
		⇒	6.1	選考
		⇒	6.2	雇用条件
		⇒	6.4	懲戒手続
		⇒	6.5	雇用の終了又は変更後の責任
		⇒	6.7	リモートワーク
		⇒	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
		⇒	8.6	容量・能力の管理
		⇒	8.7	マルウェアに対する保護
		⇒	8.8	技術的脆弱性の管理
		⇒	8.9	構成管理
7.2	力量	⇒	6.3	情報セキュリティの意識向上、教育及び訓練
7.3	認識	⇒	6.6	秘密保持契約又は守秘義務契約
7.4	コミュニケーション	⇒	-	-
7.5	文書化した情報	⇒	5.10	情報及びその他の関連資産の許容される利用
		⇒	5.12	情報の分類
		⇒	5.13	情報のラベル付け
		⇒	5.37	操作手順書

8.1	運用の計画策定及び管理	⇒	8.10	情報の削除
		⇒	8.11	データマスキング
		⇒	8.12	データ漏洩防止
		⇒	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
8.3	情報セキュリティリスク対応	⇒	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
		⇒	6.8	情報セキュリティ事象の報告
		⇒	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

9.1	監視、測定、分析及び評価	⇒	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
		⇒	5.31	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、規則及び標準の遵守
		⇒	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ィテスト
		⇒	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
9.2	内部監査	⇒	-	-
9.3	マネジメントレビュー	⇒	-	-
10.1	不適合、是正処置	⇒	-	-
10.2	継続的改善	⇒	-	-