

講義内容	1 時間 50 分
講義 1：改訂概要・組織的管理策 5.1～5.7	16 分
講義 2：組織的管理策 5.8～5.22	16 分
講義 3：組織的管理策 5.23～5.37	15 分
講義 4：人的管理策 6.1～6.8・物理的管理策 7.1～7.5	11 分
講義 5：物理的管理策 7.6～7.14	10 分
講義 6：技術的管理策 8.1～8.11	14 分
講義 7：技術的管理策 8.12～8.25	15 分
講義 8：技術的管理策 8.26～8.34・まとめ	13 分

講義 1：改訂概要・組織的管理策 5.1～5.7

16 分

頁 NO.

ISO/IEC27001 の改訂概要	1
管理策の改訂概要	6
新規管理策	7
管理策の監査の視点	8
5 組織的管理策	9
5.1 情報セキュリティのための方針群	9
5.2 情報セキュリティの役割及び責任	10
5.3 職務の分離	11
5.4 経営層の責任	12
5.5 関係当局との連絡	13
5.6 専門組織との連絡	14
5.7 脅威インテリジェンス (New)	15

講義 2：組織的管理策 5.8～5.22

16 分

頁 NO.

5 組織的管理策	
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	1
5.9 情報及びその他の関連資産の目録	2
5.10 情報及びその他の関連資産の許容される利用	3
5.11 資産の返却	4

5.12 情報の分類	5
5.13 情報のラベル付け	6
5.14 情報の転送	7
5.15 アクセス制御	8
5.16 識別管理	9
5.17 認証情報	10
5.18 アクセス権	11
5.19 供給者関係における情報セキュリティ	12
5.20 提供者との合意における情報セキュリティへの取扱い	13
5.21 情報セキュリティ技術(ICT)サプライチェーンにおける情報セキュリティの管理	14
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	15

講義 3：組織的管理策 5.23～5.37

15分

頁 NO.

5 組織的管理策	
5.23 クラウドサービス利用における情報セキュリティ (New)	1
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	2
5.25 情報セキュリティ事象の評価及び決定	3
5.26 情報セキュリティインシデントへの対応	4
5.27 情報セキュリティインシデントからの学習	5
5.28 証拠の収集	6
5.29 事業の中断・障害時の情報セキュリティ	7
5.30 事業継続のための ICT の備え (New)	8
5.31 法的、規制、及び契約上の要求事項	9
5.32 知的財産権	10
5.33 記録の保護	11
5.34 プライバシー及び個人識別可能情報(PII)の保護	12
5.35 情報セキュリティの独立したレビュー	13
5.36 情報セキュリティのための方針軍、規則及び基準への順守	14
5.37 操作手順書	15

講義 4：人的管理策 6.1～6.8・物理的管理策 7.1～7.5

11分

頁 NO.

6 人的管理策	
6.1 選考	1
6.2 雇用条件	2
6.3 情報セキュリティの意識向上、及び訓練	3
6.4 懲戒手続	4
6.5 雇用の終了又は変更後の責任	5
6.6 秘密保持契約又は守秘義務契約	6
6.7 リモートワーク	7
6.8 情報セキュリティ事象の報告	8
7 物理的管理策	
7.1 物理的セキュリティ境界	9
7.2 物理的入退	10
7.3 オフィス、部屋、及び施設のセキュリティ	11
7.4 物理的セキュリティに監視 (New)	12
7.5 物理的及び環境的脅威からの保護	13

講義 5：物理的管理策 7.6～7.14

10分

頁 NO.

7 物理的管理策	
7.6 セキュリティを保つべき領域での作業	1
7.7 クリアデスク・クリアスクリーン	2
7.8 装置の配置及び保護	3
7.9 構外にある資産のセキュリティ	4
7.10 記憶媒体	5
7.11 サポートユーティリティ	6
7.12 ケーブル配線のセキュリティ	7
7.13 装置の保守	8
7.14 装置のセキュリティを保った処分又は再利用	9

講義 6 : 技術的管理策 8.1～8.11

14分

頁 NO.

8 技術的管理策	
8.1 利用者エンドポイント機器	1
8.2 特権的アクセス権	2
8.3 情報へのアクセス制限	3
8.4 ソースコードへのアクセス	4
8.5 セキュリティを保った認証	5
8.6 容量・能力の管理	6
8.7 マルウェアに対する保護	7
8.8 技術的ぜい弱性の管理	8
8.9 構成管理 (New)	9
8.10 情報の削除 (New)	10
8.11 データマスキング (New)	11

講義 7 : 技術的管理策 8.12～8.25

15分

頁 NO.

8 技術的管理策	
8.12 データ漏えい防止 (New)	1
8.13 情報のバックアップ	2
8.14 情報処理施設・設備の冗長性	3
8.15 ログ取得	4
8.16 監視活動 (New)	5
8.17 クロックの同期	6
8.18 特権的なユーティリティプログラムの使用	7
8.19 運用システムへのソフトウェアの導入	8
8.20 ネットワークセキュリティ	9
8.21 ネットワークサービスのセキュリティ	10
8.22 ネットワークの分離	11
8.23 ウェブフィルタリング (New)	12
8.24 暗号の利用	13
8.25 セキュリティに配慮した開発のライフサイクル	14

ISO/IEC27001:2022 の改訂概要と管理策の内部監査の視点

～旧版との差分研修～

講座の概要（目次）

講義 8：技術的管理策 8.26～8.34・まとめ

13分

頁 NO.

	頁 NO.
8 技術的管理策	
8.26 アプリケーションのセキュリティの要求事項	1
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	2
8.28 セキュリティに配慮したコーディング (New)	3
8.29 開発及び受入れにおけるセキュリティテスト	4
8.30 外部委託による開発	5
8.31 開発環境、テスト環境、及び本番環境の分離	6
8.32 変更管理	7
8.33 テスト用情報	8
8.34 監査におけるテスト中の情報システムの保護	9
まとめ	10