

講義内容	2 時間 36 分
講義 1 : 規格要求事項の基本となる表現 / ISMS 規格の構成 / 箇条 4 組織の状況	17 分
講義 2 : 箇条 5 リーダーシップ	14 分
講義 3 : 箇条 6 計画策定①	21 分
講義 4 : 箇条 6 計画策定②	17 分
講義 5 : 箇条 7 支援	18 分
講義 6 : 箇条 8 運用	10 分
講義 7 : 箇条 9 パフォーマンス評価 / 箇条 10 改善	27 分
講義 8 : 附属書 A 情報セキュリティ管理策① 5 組織的管理策	16 分
講義 9 : 附属書 A 情報セキュリティ管理策② 6 人的管理策 ~ 8 技術的管理策	16 分

講義 1~5 は ISO/IEC27001:2022 要求事項テキストを、

講義 8~9 は ISO/IEC27001:2022 附属書 A — 情報セキュリティ管理策をご活用ください。

講義 1 : 規格要求事項の基本となる表現 / ISMS 規格の構成 / 17 分
 箇条 4 組織の状況

規格要求事項の基本となる表現
ISMS 規格の構成
4. 組織の情報 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
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

講義 2 : 箇条 5 リーダーシップ 14 分

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

講義 3 : 箇条 6 計画策定①

21 分

- | | |
|--------------------|-------------------------|
| 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 |

講義 4 : 箇条 6 計画策定②

17 分

- | | |
|--------------------------------|---------------------|
| 6.1 リスク及び機会に対処する活動 | 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 | |

講義 5 : 箇条 7 支援

18 分

- | | |
|---------------|------------------|
| 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 |

講義 6 : 箇条 8 運用

10 分

- | | |
|-----------------------|--|
| 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 | |

講義 7 : 箇条 9 パフォーマンス評価 / 箇条 10 改善

27 分

- | | |
|-------------|-------------------------|
| 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 |

講義 8 : 附属書 A 情報セキュリティ管理策① 5 組織的管理策

16 分

附属書 A の管理策群	～旧版との比較～
附属書 A に新しく追加された管理策	
附属書 A の管理策	～5 組織的管理策～
附属書 A の管理策	～6 人的管理策/ 7 物理的管理策～
附属書 A の管理策	～8 技術的管理策～
5 組織的管理策	5.1 情報セキュリティのための方針群～5.5 関係当局との連絡
	5.6 専門組織との連絡～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～5.16 識別情報の管理
	5.17 認証情報～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～5.28 証拠の収集
	5.29 事業の中断・阻害時の情報セキュリティ～
	5.34 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～5.37 操作手順書

講義 9 : 附属書 A 情報セキュリティ管理策② 6 人的管理策 ～ 8 技術的管理策 16 分

6 人的管理策	6.1 選考～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～7.7 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～7.14 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～8.7 マルウェアに対する保護
	8.8 技術的ぜい弱性の管理～8.14 情報処理施設・設備の冗長性
	8.15 ログ取得～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～
	8.26 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～
	8.32 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