内部監査の基礎

株式会社Purpom Media Lab

ISMS教育教材（内部監査員向け）

doc_id: EDU-MAT-005 ／ version: 1.0

制定日: 2024年4月1日

1. 内部監査とは

内部監査とは、ISMSが規格要求事項および組織の方針・手順に適合しているかを確認するための、組織内部による独立した評価活動です（JIS Q 27001 箇条9.2）。

> **内部監査の目的**
>
> - ISMSが効果的に機能しているかを確認する
> - 不適合・改善点を早期に発見する
> - 外部審査前の事前チェック
> - 継続的改善のインプットを提供する

2. 内部監査員の要件

- 監査対象部門・業務を担当していない者が実施する（独立性の確保）
- JIS Q 27001の要求事項を理解している

- 客観的かつ公平に評価できる

当社では **杉浦悠太** が内部監査員を担当しています。

3. 内部監査のプロセス

ステップ	内容
①計画	監査計画書の作成（対象・日程・目的・基準・監査員）
②準備	チェックリスト作成・関連文書の事前確認
③実施	インタビュー・記録確認・観察
④報告	監査報告書の作成・不適合事項の記録
⑤フォローアップ	是正処置の確認・有効性の評価

4. 監査の判定区分

区分	定義	対応
不適合	要求事項を満たしていない	是正処置が必須
観察事項	現時点では問題ないが将来リスクあり	改善を推奨
良好事例	要求事項を超えた優れた取り組み	他部門への展開を検討

5. 監査チェックリストの例

情報セキュリティ方針（箇条5.2）

- □ 情報セキュリティ方針が文書化されているか
- □ 方針が全員に周知されているか
- □ 方針の定期的なレビューが実施されているか

リスクアセスメント（箇条6.1.2）

- □ リスクアセスメントの手順が定義されているか
- □ 定期的にリスクアセスメントが実施されているか
- □ リスク対応計画が策定されているか

監視測定（箇条9.1）

- □ 監視測定の対象・頻度が定義されているか
- □ 記録が適切に保持されているか
- □ 目標に対する達成状況が評価されているか

6. 監査報告書の構成

- 監査日時・場所・監査員・被監査部門
- 監査の目的・範囲・基準
- 監査結果（適合・不適合・観察事項）
- 不適合事項の詳細（該当箇条・事実・根拠）
- 是正処置の要求事項と期限
- 結論

> **受講確認**
> 本教材の内容を理解し、内部監査員として客観的・公正な監査を実施できることを確認しました。