



サイバーセキュリティ

# 診断チェック表



## 第3回：ISMS などのフレームワークの種類と活用法の紹介

- check 01  自社に適したセキュリティフレームワークを選定している
- check 02  ISMS の要求事項に基づき情報資産を特定している
- check 03  ISMS 運用責任者を明確にしている
- check 04  ISMS の PDCA サイクルを定期的に回している
- check 05  NIST CSF の 6 機能を参考にしている
- check 06  CPSF を参照し、物理・制御系の対策を考慮している
- check 07  経営ガイドラインを基に経営層の役割を整理している
- check 08  フレームワークごとの目的と適用範囲を把握している
- check 09  複数フレームワークを組み合わせて自社基準を整備している
- check 10  情報セキュリティポリシーをフレームワークに沿って見直している
- check 11  リスクマネジメント方針を策定し、承認を得ている
- check 12  リスク特定・分析・評価の手順を文書化している
- check 13  リスク対応策を実施し、残留リスクを評価している
- check 14  リスク対応計画の進捗を定期的に点検している
- check 15  フレームワーク適合の教育に関係者に実施している
- check 16  外部監査または自己点検で ISMS の有効性を確認している
- check 17  法令や基準改定時にフレームワーク対応を更新している
- check 18  管理策の適用状況を評価し、改善を進めている
- check 19  リスクアセスメント結果を経営層に報告している
- check 20  ISO27005 に基づくリスク管理プロセスを運用している

令和7年度

中小企業サイバーセキュリティ支援事業 実践力強化プログラム

※当事業は東京都より委託を受け、株式会社 NTT ExC パートナー（エヌ・ティ・ティ エクシーパートナー）が運営しています。

事業の公式サイトはこちら

<https://zissenkyouka.metro.tokyo.lg.jp/>

