サイバーセキュリティ

診断チェック表

第５回：ISMS の構築と対策基準の策定と実施手順

check 01	☐	脅威や被害事例を収集し、経営層に共有している
check 02	☐	ランサムウェア被害について社内で注意喚起している
check 03	☐	取引先・委託先のセキュリティ状況を確認している
check 04	☐	テレワークやクラウド利用に対応した規程を整備している
check 05	☐	IoT 機器の利用状況とリスクを把握している
check 06	☐	個人情報保護法や GDPR への対応責任者を定めている
check 07	☐	法令遵守や漏洩リスクの教育を社員に実施している
check 08	☐	事故発生時の初動対応手順を文書化している
check 09	☐	インシデント時の社内外報告体制を整備している
check 10	☐	社員向けセキュリティ教育を定期実施している
check 11	☐	フィッシング対策やパスワード管理教育を行っている
check 12	☐	経営層がセキュリティ施策に主体的に関与している
check 13	☐	セキュリティ投資を事業継続の基盤として予算化している
check 14	☐	リスク評価を実施し、経営層が確認している
check 15	☐	対策の実施状況を点検し、改善している
check 16	☐	重大インシデントの対応計画を策定している
check 17	☐	重要データをバックアップし、復旧可能性を確認している
check 18	☐	セキュリティ方針や取組を社内で定期的に議論している
check 19	☐	最新の攻撃事例や法改正を継続的に収集している
check 20	☐	クラウドやゼロトラストの導入検討を開始している

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/