最初の90日の実行地図

「何から手を付けるか」を、根拠つきで決める地図。最初の90日で着手し、1年で定着させる20タスク。

※ 20タスクは約12ヶ月の工程です。最初の90日＝フェーズ1の完遂と、全体の段取りづくり。

着手から定着まで（約12ヶ月）	追加費用0円で着手	投資判断が要る
20タスク	16タスク	4タスク

※ 金額例は従業員50〜200名規模を想定した目安です（関連資料『IT統制整備 標準ロードマップ』と同じ想定）。

関連資料：『【モデルプラン】IT統制整備 標準ロードマップ』——12ヶ月の全体像を示したモデルプランです。本書は最初の90日に焦点を絞っています。

見本・v0.9　2026/09/08　合同会社SecuROI　※本書は見本です。実際の優先順位は診断結果により異なります。

90日地図（タスク × 公的基準）

20タスクを着手順に。「追加費用0円」は既存の契約・設定の範囲で対応できる場合を指します。

※ 20タスクは約12ヶ月の工程です。最初の90日＝フェーズ1の完遂と、全体の段取りづくり。

見本・v0.9　2026/09/08

#	タスク	担い手	フェーズ	J-SOX の見方	ISO 27001 附属書 A	Pマーク	手段と費用
#1	**情報システム運用管理規程の制定・承認**	情シス→経営承認	フェーズ1	IT方針・規程体系の明文化	A.5.1 / A.5.37	組織的	0円
#2	**アカウント管理責任者・各システム管理者の選任**	管理部門＋情シス	フェーズ1	役割・責任の明確化	A.5.2	組織的	0円
#3	**SaaS・アカウント台帳の整備（全サービス棚卸）**	情シス	フェーズ1	統制対象範囲の特定	A.5.9	組織的	SaaS管理（例：ジョーシス等）・帯50〜150万円/年
#4	**退職・異動時のアカウント即時停止の運用**	情シス＋人事	フェーズ1	退職者権限の残存防止	A.5.18 / A.6.5	人的・技術的	0円（#3の台帳で運用）
#5	**エンドポイント保護の全端末適用**	情シス	フェーズ1	不正プログラム対策	A.8.7	技術的	0円（既存契約内）
#6	**端末管理（MDM）への全端末登録**	情シス	フェーズ2	構成管理・許可端末の特定	A.8.1 / A.8.9	技術的	0円（例：Intune等・既存契約内）
#7	**管理者権限への多要素認証の必須化**	情シス	フェーズ2	特権アクセスの保護	A.8.2 / A.8.5	技術的	0円（ID基盤の既存機能）
#8	**パスワード管理の全社標準化（使い回し排除）**	情シス	フェーズ2	認証情報の管理	A.5.17	技術的	パスワード管理（例：1Password等）・帯100〜300万円/年
#9	**監査ログの保存期間設定・改ざん防止**	情シス	フェーズ2	証跡の保全・改変防止	A.8.15	技術的	帯100〜300万円/年（既存プラン上位版で可の場合あり）
#10	**セキュリティ委員会（経営関与）の設置・定例化**	経営＋情シス	フェーズ2	経営者のIT関与・モニタリング	A.5.1 / A.5.35	組織的	0円
#11	**端末のディスク暗号化の全台適用**	情シス	フェーズ3	紛失・盗難時の情報保護	A.8.24	技術的	0円（既存契約内）
#12	**外部送信の検知（DLP）の導入**	情シス	フェーズ3	漏えいの防止・検知	A.8.12	技術的	外部送信検知ツール（DLP）（例：HENNGE等）・帯50〜150万円/年
#13	**クラウドの外部共有の原則禁止設定**	情シス	フェーズ3	正規操作による持ち出し防止	A.8.3 / A.5.14	技術的	0円（既存設定）
#14	**アクセス権限の定期棚卸（半期）**	情シス＋各部門	フェーズ3	不要権限ゼロの証明	A.5.18	組織的・技術的	0円
#15	**管理者操作ログの定期レビュー（月次）**	情シス	フェーズ3	特権行動のモニタリング	A.8.15 / A.8.16	組織的	0円
#16	**プログラム変更の承認制（記録の残る承認フロー）**	開発	フェーズ4	変更の承認・記録	A.8.32	組織的	0円（開発基盤の既存機能）
#17	**開発・テスト・本番環境の分離と職務分離**	開発	フェーズ4	職務分離・環境区分	A.8.31 / A.5.3	組織的・技術的	0円（同上）

#	タスク	担い手	フェーズ	J-SOX の見方	ISO 27001 附属書 A	Pマーク	手段と費用
#18	**リリース前テストの記録・承認**	開発	フェーズ4	移行手続の統制	A.8.29 / A.8.32	組織的	0円（同上）
#19	**インシデント対応手順の制定と年1回の訓練**	情シス全社	フェーズ4	IT問題の報告・対応体制	A.5.24–26	組織的・人的	0円
#20	**重要委託先の選定基準と定期評価（SOC報告書等の入手）**	情シス＋管理部門	フェーズ4	委託先管理	A.5.19–22	組織的	0円

※ 追加費用0円 16件／投資判断が要る 4件（合計 20件）。0円は既存契約の範囲で対応できる場合で、契約内容・構成により異なります。
※ 金額例は従業員50〜200名規模を想定した目安です（関連資料『IT統制整備 標準ロードマップ』と同じ想定）。
※ 本書は見本です。数字は貴社の入力から決定論で算出します——生成AIは判定に使いません。
※ 診断結果はセキュリティ準備度の目安であり、外部審査の合否を保証するものではありません。