

4 情報セキュリティマネジメントシステム

4.1 一般要求事項

本文では、プロセスアプローチを採用することを推奨しており、PDCA の各ステップを以下のように規定しています。

■ Plan - 計画 (ISMSの確立)

組織の全般的な基本方針及び目標に沿った結果を出すための、リスクマネジメント及び情報セキュリティの改善に関連する情報セキュリティ基本方針、目的、対象、プロセス及び手順を確立する。

■ Do - 実施 (ISMSの導入及び運用)

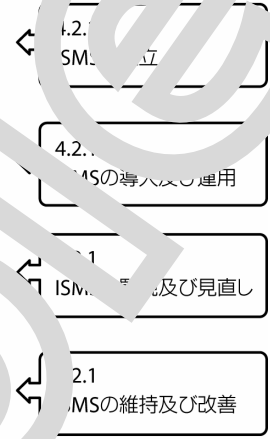
その情報セキュリティ基本方針、管理策、プロセス及び手順を実施し運用する。

■ Check - 点検 (ISMSの監視及び見直し)

情報セキュリティ基本方針、目標及び経験に照らしてプロセスの実行状況を評価し、可能な場合これを測定し、その結果を見直しのために経営陣に報告する。

■ Act - 処置 (ISMSの維持及び改善)

ISMSの継続的な改善を達成するために、マネジメントレビューの結果に基づいて是正処置及び予防処置を講ずる。



4.2 ISMS の確立及び運営管理

4.2.1 ISMS の確立

4.2.1 ISMS の確立では、確立の手順を以下のステップで規定しています。

