情報セキュリティとは（1章）

- セキュリティ上の危険や脅威から情報資産を保護し、情報システムの信頼性を高める→利用者の安全・安心
- 3つの観点：
  - 機密性(confidentiality)：許可された者だけがアクセス可能
  - 完全性(integrity)：情報が正確で過不足がない
  - 可用性(availability)：正当な利用者が必要時に確実にアクセス可能
- 「正当な利用者」を正しく認証できることも重要

情報セキュリティの対策方法

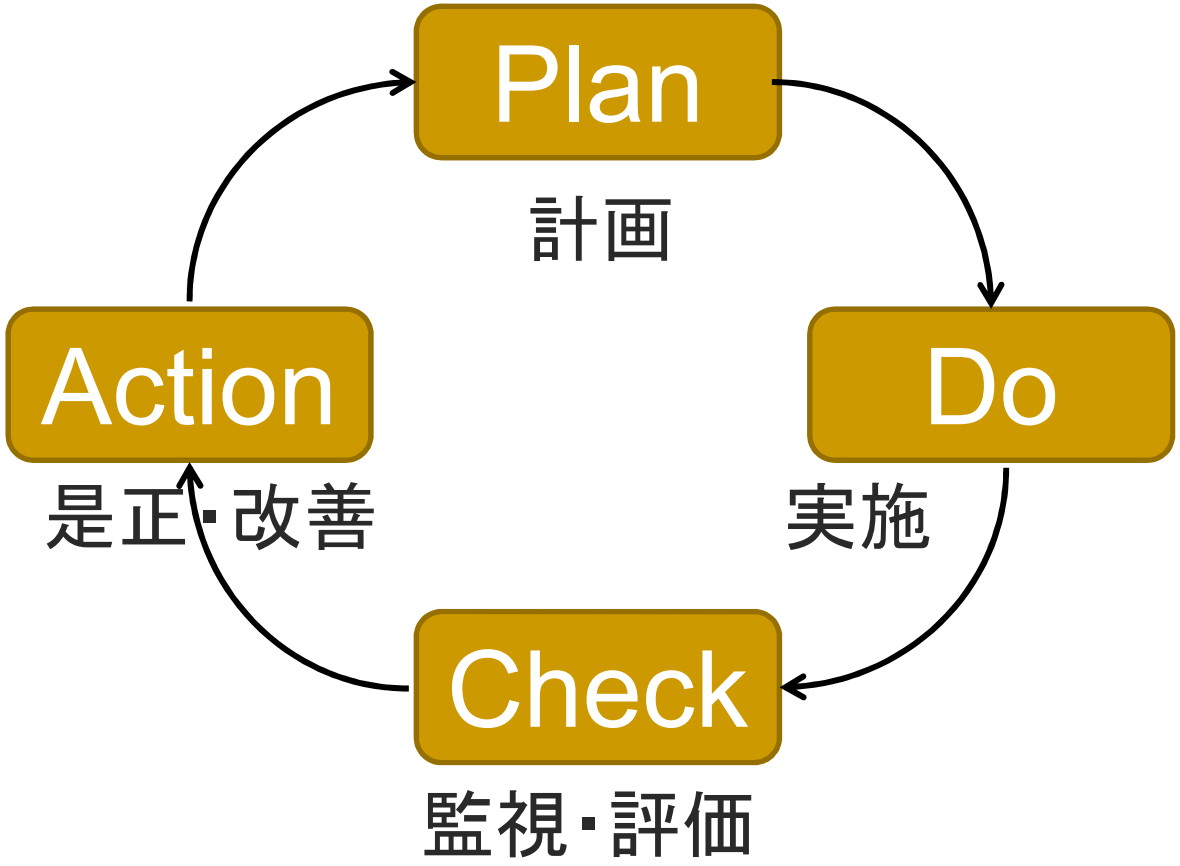
- 技術
  - 暗号・認証技術、ファイアウォール、電子透かし、バイオメトリクス等
  - 技術だけではだめ（悪用されることもある）
- 管理・運営（11章、12章）
  - セキュリティポリシー
  - ISO15408（技術面）、ISO27001（組織面）
- 法制度（15章）
  - 個人情報保護法、著作権法、電子署名法、不正アクセス禁止法等
- 倫理・教育

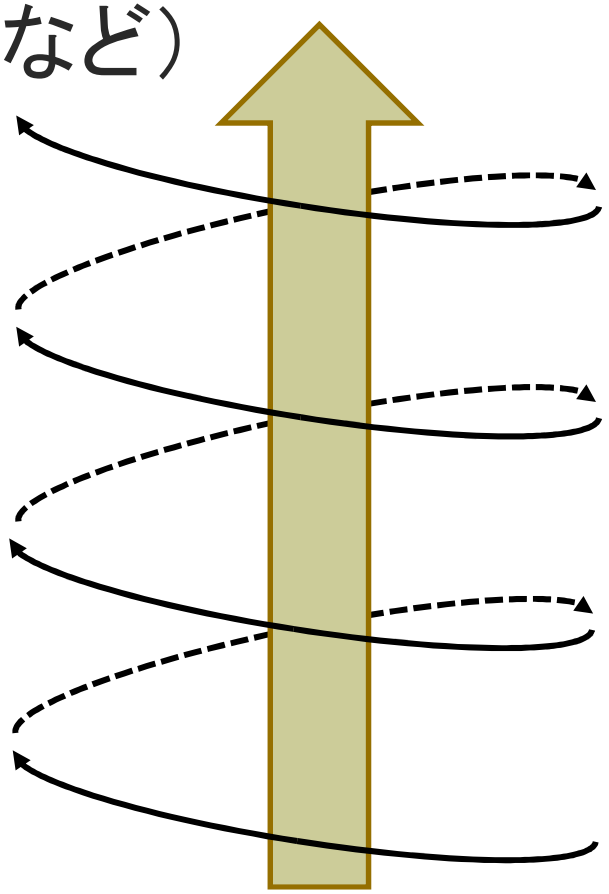
情報セキュリティの脅威に対処する段階

- 抑止
  不正者の意欲をそぐ
  （法律、セキュリティ対策（組織、技術））
- 防止
  被害が発生しないように対策する
  （ファイアウォール、ウイルス対策、教育）
- 検出
  被害が発生してもすぐに検出できる
  （侵入検知システム、改ざん検知ツール、運用組織）
- 回復
  被害が発生した後すぐに正常に戻せる
  （バックアップツール、BCP(事業継続計画)の策定）

組織における情報セキュリティ対策

- PDCAモデル（ISO27001など）





ディジタルフォレンジック（１４章）

- 情報システムに対する不正侵入や不正操作、改ざん等に対する証拠保全、その調査手法（ディジタル鑑識学）
- 「証拠」が残りやすいようなシステム作り
- 目的：
  - 法執行機関（警察など）による調査
  - 企業における内部統制、訴訟対策