

## 4 情報セキュリティポリシーと関連法規

### 4.1 情報セキュリティポリシー

ポリシー(policy)とは？

文書化されて管理

- ・ 「何を何からどのように守るか」の**基本的考え方**  
+
- ・ セキュリティを確保するための**体制と運用方針**



基本は3階層

1. **情報セキュリティ基本方針(基本ポリシー)**  
基本宣言, 基本的な考え方, 取り組み姿勢  
→ なぜ(why)必要なのか?
2. **情報セキュリティ対策基準(スタンダード)**  
基本ポリシーを実現するために何をすべきかを表現  
実際に守るべき具体的な規定  
適用範囲・対象者を明らかにする  
→ 何を(what)実施しなければならないか
3. **情報セキュリティ実施手順(プロシージャ)**  
スタンダードを実施するための詳細な手順, 具体的な内容  
マニュアル的な位置づけ  
→ どのように(how)実施するか

ポリシーのルール化の効果

- ユーザの意識をレベルを高める
  - 内部犯行の抑止
  - 情報漏えい危険性の抑止
- 取り組み姿勢の明確化(対外的なアピール)

実習) 外部接続に関するセキュリティポリシー の サンプル をみてみましょう

→ 教科書 and インターネット

## 4.2 情報セキュリティの国際標準と法規

**ISMS** : Information Security Management System

情報セキュリティマネジメントシステム

- 情報セキュリティを適切に管理するための枠組み
- 経営者を頂点とした組織的な取組み

組織内のセキュリティルールをしっかりと作る・運用する  
セキュリティと可用性のバランスをとる

ISMS 認証

- 国際・国内基準になっている
- JIS Q 27001 (ISO/IEC 27001)

ポイント

- セキュリティの3要素の維持
- リスクアセスメント(リスク評価)
- PDCAによる改善プロセス

個人情報保護法

- ・個人情報とは?  
個人が特定できる情報
- ・個人情報取扱事業者 (N > 5000人)
- ・ポイント
  - 1 安全管理措置の義務
  - 2 利用目的の通知
  - 3 個人情報を本人がコントロールできる権利

関連) プライバシーマーク制度

サイバー刑法

- ・サイバー犯罪への対応を目的に刑法を改正
  - 電磁的記録の保護
  - ウイルス作成・供用罪**
  - 財産・知的財産の保護
  - 通信の秘密の保護
  - 不正アクセス罪

不正アクセス禁止法

- ・不正アクセス(改ざん, 破壊など)の禁止
- ・他人のユーザアカウントの不正使用を禁止, 無断公開禁止
- ・セキュリティホールからの侵入禁止

その他関連

- ・ガイドライン
  - ＝あるものごとに関する**基準** (ルールや規範)
- ・標準化
  - ＝互換性、利便性を確保するために**規格**を定める
  - JIS, IEEE, ISO

- ・ 倫理

- ・ 情報倫理

- ネチケット

- ・ 企業倫理

- CSR (Corporate Social Responsibility)

- = 企業の社会的責任

- SRI = CSR を数値化した株式指数

- コンプライアンス (compliance)

- = 遵守する

- 企業として、法律、モラル、マナーを守る