

# JIS Q 27001 (ISO/IEC 27001)

## 情報セキュリティマネジメントシステム

### 情報セキュリティマネジメントシステムの必要性

インターネットの急速な拡大や高速化が進んでいます。また、情報機器は飛躍的な性能向上や大容量化が進み、情報システムは高度化・複雑化しています。このようなIT環境の変化は、企業経営に影響を及ぼすばかりではなく、電子政府や住基ネットの実現など行政面を始め社会的な変化をもたらしています。

一方、IT環境の進化とともに新たな脅威(リスク)も増大しています。不正アクセスやコンピュータウイルスなどによる情報の漏洩、改ざん、破壊といったインシデント(事件・事故)や、高度化されたシステムの故障、誤動作は事業活動の停止といった事態を引き起こします。

こうしたさまざまな脅威から重要な「情報資産」を守るため、機密性(Confidentiality)・完全性(Integrity)・可用性(Availability)をバランス良く保った「情報セキュリティ」を確保することが要求されています。

情報セキュリティマネジメントシステム(ISMS-Information Security Management System)は情報資産に対するリスクを低減するために必要な対策を実施するとともに、構築したシステムをPDCAサイクルによって継続的に改善していく仕組みです。

### 期待される効果

- 情報セキュリティに関するリスク低減
- 従業員の情報セキュリティ意識向上
- 継続的な情報セキュリティ維持
- 遵法性確保
- 安全な情報の取扱いに対する顧客からの信頼の確保
- 競合他社との差別化
- 情報セキュリティ要求への対応(取引・入札条件)
- 情報セキュリティ面からの事業継続の確保