情報セキュリティ　ー 2017/09/28

# 1 情報セキュリティの考え方

## 1.1 情報セキュリティの 6 要素

機密性（Confidentiality）　-　許可されたものだけがアクセスできる
完全性（Integrity）　-　情報・処理の方法が正確かつ完全
可用性（Availavility）　-　許可されたものが必要な時に情報にアクセス可

↓

情報セキュリティの CIA

＋

責任追跡性（Accountability）
真正性（Authenticity）
信頼性（Reliability）

確認）それぞれの用語・考え方を確認してみましょう！

## 1.2 時系列（時間の経過）で検討

事前対策
発生時の対応
発生後の対応
＋
日常の運用

↓

継続的な改善活動が必要！

PDCA サイクルで考える ISMS（情報セキュリティマネージメントシステム）

ポイント）

IT 技術は変化し、そのままにしておくと時代遅れになりうる

IT システムを安全にし、壊されにくくする
＋
セキュリティを破られたときにどうするか？を考える
＝被害を最小にとどめるには？
＝絶対安全というものは現状では存在しない

## 1.3 管理方法(対策の内容)で検討

技術面　　-　　IT, ICT 技術的な対策
運用面　　-　　物理的な対策
セキュリティポリシー面　　-　　人的な対策
　　+
外部委託による対策

ポイント)
　原因のほとんどは人的な問題である
　　= 技術的な対策には限界あり
　コンピュータは誰でも使用する(仕事上必要)　だが、セキュリティ知識はバラツキあり

## 1.4 リスクで検討

リスクコントロール
　抑止
　予防
　検知
　回復

リスク管理
　許容
　低減
　移転
　回避

　ポイント)
　　リスクの可能性と損害の大きさによってどれを選ぶのかが異なる

　検討) 保険に加入することはリスク管理上のどれに該当しますか？

リスクと損失
　リスクの要因
　実際の損失
　リスクの大きさ

　ポイント)
　　リスクの大きさを見積もることは、情報資産の価値を考えることでもある
　　優先順位付けや投資枠なども明確になる

## 1.5 情報資産

紙文書 - 有形のもの ← 複製に手間
電子データ - 無形のもの ← 複製が簡単
パソコン・システム -

↓

IT, ICT への依存と利便性向上

↓

使えなくなると業務が停止する場合あり

= 業務上必要な資産(守るべきもの) = 情報資産

ポイント)

資産の価値はそれぞれ異なる
情報の「形」によって、セキュリティ対策は異なる
情報がどこにどんな形で存在するか考える
情報資産の重要性を意識すること

**検討）みなさんの周囲にはどんなコンピュータがありますか？**

**検討）みなさんにとっての情報資産とは？どんな対策を考えていますか？**

**検討）紙情報と電子情報の扱いの違いは？**