

## 8. 情報セキュリティ監査

### 用語：

信頼性・正当性を

担保する = (根拠に基づいて) 保障する

遵守 = 順守

統制 = control (2.5 参照)

### 8.1 情報セキュリティについてのコンプライアンス

#### 情報セキュリティの目標：

OECD/SC21 (1992)

機密性, 完全性, 可用性 (CIA)

↓

+ OECD/SC27 (1998) によって追加

信頼性 (安定性 reliability)

真正性 (信憑<sup>びよう</sup>性 authenticity)

責任追跡性 (説明責任 accountability)

### 8.2 情報セキュリティ監査

#### 種類：

準拠性監査 …… 基準に達しているか (法令や社内規程に従っているか)

妥当性監査 …… 上記より厳しい (しかし主観が入る)

## 8.3 コンピュータ・フォレンジクス

### ログ取得の目的：

- (1) 民事訴訟に備える。
- (2) 刑事訴訟に備える。
- (3) 踏み台にされたとき、きちんと対応していたことを証明する。

### 用語と保存：

文書 (document) = 変更がありうるもの → バックアップ

記録 (record) = 変更がないもの → アーカイブ (古文書)

### 用字：

- **フォレンジクス** (forensics)
- **エコノミクス** (economics)
- **エレクトロニクス** (electronics)
- **グラフィクス** (graphics)
- **ジムナスティクス** (gymnastics)