

- ・ ウイルス攻撃
- ・ サービス不能（DoS：Denial of Service）攻撃
- ・ 情報漏えい 等

(b) 非意図的要因による IT 障害

- ・ システムの仕様やプログラム上の欠陥（バグ）
- ・ 操作ミス
- ・ 故障
- ・ 情報漏えい 等

(c) 災害による IT 障害

- ・ 地震、水害、落雷、火災等の災害による電力供給の途絶
- ・ 地震、水害、落雷、火災等の災害による通信の途絶
- ・ 地震、水害、落雷、火災等の災害によるコンピュータ施設の損壊等
- ・ 地震、水害、落雷、火災等の災害による重要インフラ事業者等における IT の機能不全

これらの脅威に対し、対策を行うことにより、発生可能性を低減し、リスクを實際上問題のないレベルにまで小さくすることが必要になる。

### C. 最低限のガイドライン

1. 情報システムで扱う情報をすべてリストアップしていること。
2. リストアップした情報を、安全管理上の重要度に応じて分類を行い、常に最新の状態を維持していること。
3. このリストは情報システムの安全管理者が必要に応じて速やかに確認できる状態で管理していること。
4. リストアップした情報に対してリスク分析を実施していること。
5. この分析の結果得られた脅威に対して、6.3～6.11 に示す対策を行っていること。

### D. 推奨されるガイドライン

1. 上記の結果を文書化して管理していること。