Part 7. 정보보호 관리

Section 40. 정보보호 정책 및 조직

Section 41. 위험관리

Section 42. BCP/DRP

BCP

- 사업영향분석(BIA, Business Impact Analysis)
- 복구 전략
  - 미러 사이트(Mirror Site) : 재해 발생시 복구 소요 시간(RTO)=0 (이론적)
  - 핫 사이트(Hot Site) : 동일 수준의 시스템을 재해복구센터에 대기상태(stand by)로 둠
  - 웜 사이트(Warm Site) : 핫 사이트와 유사하나, 중요성이 높은 정보기술자원만 부분 보유
  - 콜드 사이트(Cold Site) : 일 단위 or 주 단위로 원격지에 백업. 구축 및 유지비용이 가장 저렴하지만 복구 소유시간이 매우 길고 신뢰성이 낮다.

Section 43. 침해사고 대응

Section 44. 국제/국가 표준 및 인증체계

[1] 보안 제품 평가방법 및 기준

[TCSEC, Trusted Computer System Evaluation Criteria]

- 1985년 미국 최초, 오렌지 북이라고도 함
- 보안등급(A1, B3, B2, B1, C2, C1)
- <기밀성, 무결성, 가용성> 중에서 기밀성을 중요시함

[ITSEC]

- 1991년 TCSEC을 참조해 만든 유럽 공통 평가기준
- <기밀성, 무결성, 가용성> 모두 평가기준 수용
- E0(부적합), E6~E1(6등급)

[CC, Common Criteria]

- 현재 3.1버전까지 공개
- 1999년 6월 8일 ISO 15408 표준으로 채택된 정보 보호 평가 기준
- 보안등급 EAL0 부적합 EAL1~EAL7(7등급)

[2] 정보보호관리체계 인증

[BS7799(ISO/IEC 17799)]

[KISA-ISMS]

[3] 개인정보 보호 관리체계 인증(PIMS)

- PIMS(Personal Information Management System)