정보보호론 0313

★ NIST CIA 3대 요소

* 기밀성 : 허가 받은 사람만 공개
* 무결성 : 허가 받은 사람만 수정
* 가용성 : 필요한 시점 접근 가능

윤리 의식(조심)

정보보호 대상 : 다양한 분야

대상 선택 -> 취약점 및 위협 분석 -> 솔루션 탐색(기술, 정책)

넓은 범위를 많이 알아야 한다.(정보보호 전문가 하려면)

다양한 분야 지식을 알아야 한다.

암호학(Cryptography)

Kryptos : 비밀, grapho : 쓰다

메시지의 기밀성을 제공(전쟁에서 파생)

Crypto 암호의 넓은 범위, encryption : 메시지 암호화

암호기술(방법, 방어) : 알고리즘 설계(기밀성)

암호해독(분석, 공격), 암호시스템(시스템), 암호프로토콜(규칙)