


# 정보보호개론

성균관대학교  
민무홍



# 제1절 정보보호와 관리



# 정보보호 개요 - 정보보호 개념

- 정보보호는 정보 자산을 공개·노출·변조·파괴·지체 등의 위협으로부터 보호하여 정보의 기밀성, 무결성, 가용성을 확보하는 것



# 정보보호 개요 - 정보보호 목표

- 기밀성
- 무결성
- 가용성



# 정보보호 관리 - 정보보호 정책

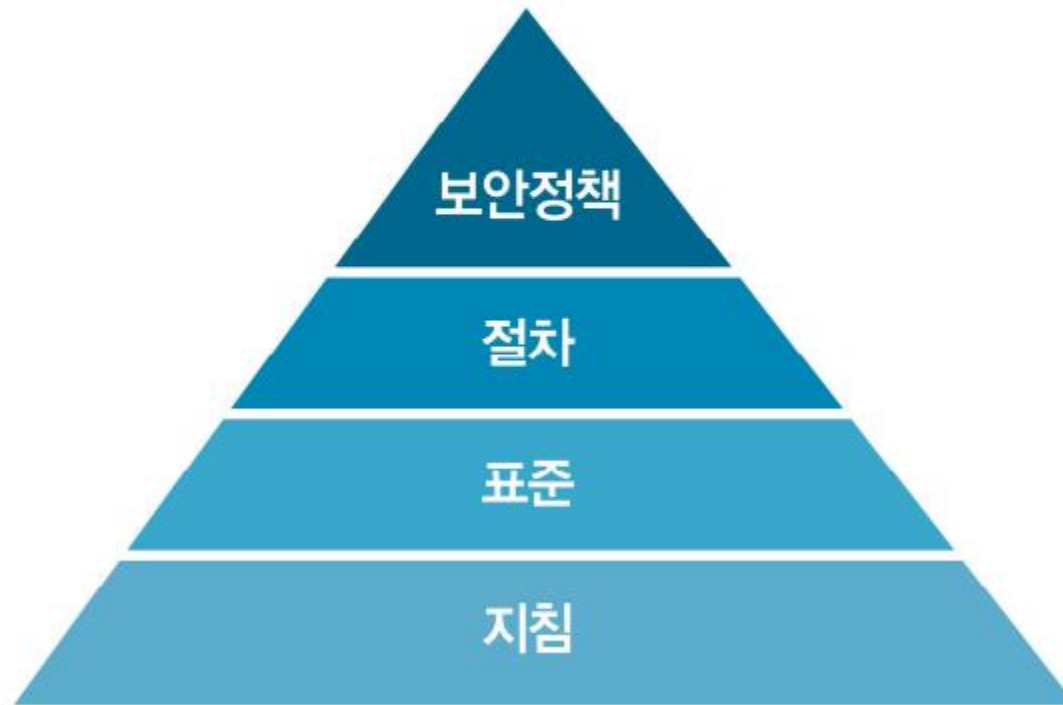
## ▮ 정보보호 정책, 표준, 지침, 절차 ▮

구분	정의 및 특성
정책 (Policy)	<ul style="list-style-type: none"><li>• 정보보호에 대한 상위 수준의 목표 및 방향을 제시</li><li>• 조직의 경영목표를 반영하고 정보보호 관련 상위 정책과 일관성을 유지</li><li>• 정보보호를 위해 관련된 모든 사람이 반드시 지켜야 할 요구사항을 전반적이며 개략적으로 규정</li></ul>
표준 (Standard)	<ul style="list-style-type: none"><li>• 정보보호 정책과 마찬가지로 반드시 지켜야 하는 요구사항에 대한 규정이지만, 정책의 만족을 위해 반드시 준수해야 할 구체적인 사항이나 양식을 규정</li><li>• 조직의 환경 또는 요구사항에 따라 관련된 모든 사용자들이 준수하도록 요구되어지는 규정</li></ul>
지침 (Guidelines)	<ul style="list-style-type: none"><li>• 반드시 지켜야 하는 것이 아니라 선택 가능하거나 권고적인 내용이며 융통성 있게 적용할 수 있는 사항을 설명</li><li>• 정보보호 정책에 따라 특정 시스템 또는 특정 분야별로 정보보호 활동에 필요하거나 도움이 되는 세부 정보를 설명</li></ul>
절차 (Procedure)	<ul style="list-style-type: none"><li>• 정책을 만족하기 위하여 수행하여야 하는 사항을 순서에 따라 단계적으로 설명</li><li>• 정보보호 활동의 구체적 적용을 위해 필요한 적용 절차 등의 구체적이고 세부적인 방법을 기술</li></ul>



# 정보보호 관리 - 정보보호 정책

▮ 정보보호 정책, 표준, 지침, 절차 ▮ \* 보안정책 --> 보호정책





# 정보보호 관리 - 정보보호 관련 위협과 취약성

- 위협(Threat)은 정보시스템에 손상을 입히거나 정보의 기밀성, 무결성, 가용성에 피해를 줄 수 있는 모든 사건
- 위협은 일반적으로 자산이 지니고 있는 취약성(Vulnerability)을 이용하여 자산에 손상을 입히게 됨



# 정보보호 관리 - 정보보호 관련 위협과 취약성

- 위협의 종류
  - 환경(자연)에 의한 위협
  - 인간과 관련된 위협





# 정보보호 관리 - 정보보호 관련 위협과 취약성

- 취약성(Vulnerability)은 위협에 의해 이용될 수 있는 자산의 약점으로 자산이 잠재적으로 갖고 있는 약점
- 취약성의 종류
  - 물리적 취약성
  - 자연적 취약성
  - 환경적 취약성
  - 하드웨어 취약성
  - 소프트웨어 취약성
  - 매체 취약성
  - 전자파 취약성
  - 통신 취약성
  - 인적 취약성



# 정보보호 관리 - 정보보호 대책

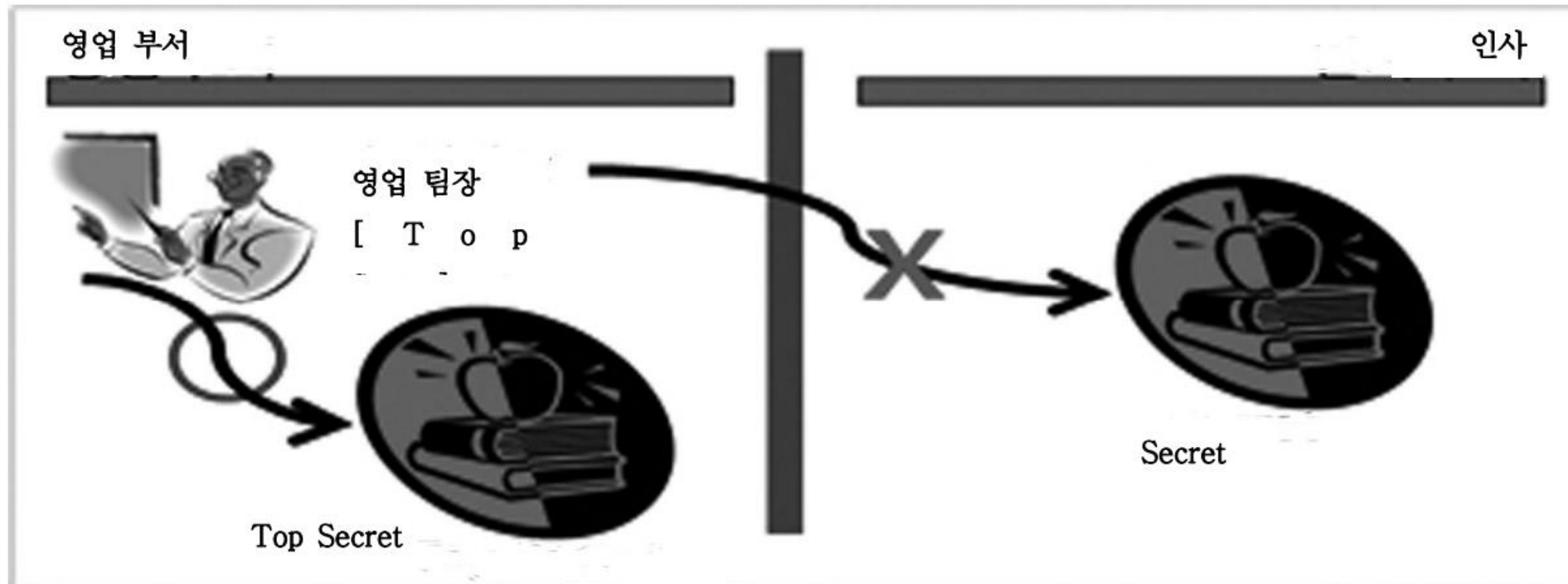
- 예방통제(Preventive Controls)
- 탐지통제(Detective Controls)
- 교정통제(Corrective Controls)



# 정보보호 관리 - 접근통제

- ① 강제적 접근통제(Mandatory Access Control, MAC)

## MAC의 예





# 정보보호 관리 - 접근통제

- ② 임의적 접근통제(Discretionary Access Control, DAC)

## ■ DAC의 예 ■

5월 실적 보고서 -> (Object)	
(Subject) — [	John R, W
	David R
	Miki W, X
= (Authorization) —	



# 정보보호 관리 - 접근통제

- ③ 비임의적 접근통제(Non-Discretionary Access Control, Non-DAC)

## 최소 권한 정책과 직무분리의 원칙 원칙

- 최소 권한 정책(Least Privilege Policy) :  
최소 권한 정책은 Need To Know 원칙으로 사용자들은 자신의 업무를 수행하기 위해 꼭 필요한 권한만을 갖도록 접근 권한을 부여하는 것이다. 즉, 사용자에게 최소의 권한만을 허용하여 권한의 남용을 방지하고 해킹 등으로부터 시스템을 보호할 수 있다.
- 직무분리의 원칙(Separation of Duty) :  
직무분리의 원칙은 업무의 발생에서부터 배포에 이르기까지 모든 업무의 프로세스가 한 사람에 의해 처리될 수 없도록 하는 강제적 보안정책이다. 즉, 시스템 상에서 오용을 일으킬 정도의 충분한 특권을 가진 사용자를 없게 하는 것이다.

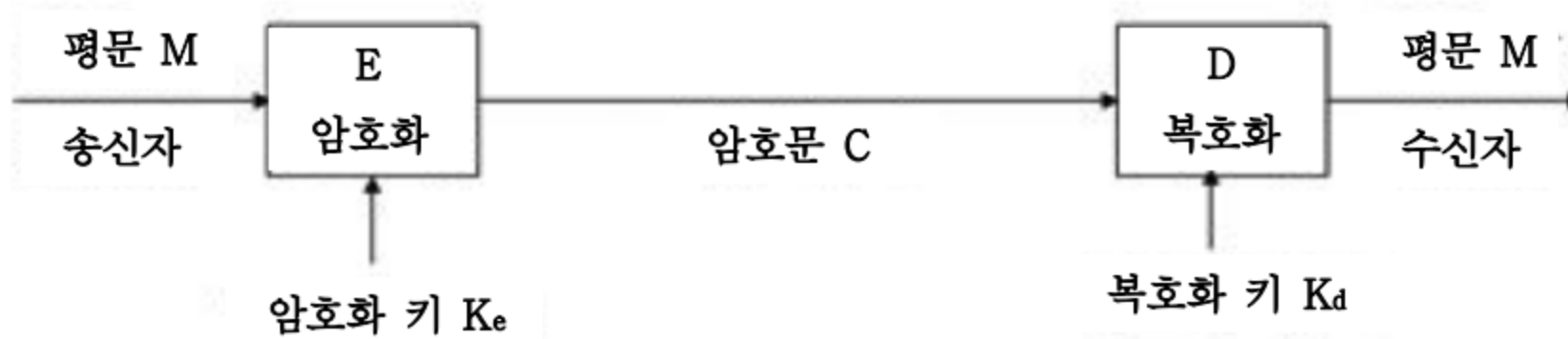


## 제2절 암호학



# 암호의 이해

## ■ 암호 방식 ■





# 암호 알고리즘 - 암호 알고리즘의 분류

- ① 대칭키 암호 방식
- ② 공개키 암호 방식

## ┃ 공개키 암호 방식 ┃







# 암호 알고리즘 - 대칭키 암호 알고리즘

- 대칭키 암호 방식 알고리즘으로는 DES(Data Encryption Standard), AES(Advanced Encryption Standard), SEED, ARIA, SKIPJACK, IDEA(International Data Encryption Algorithm), RC5(Ron's Code 5) 등이 있다.



# 암호 알고리즘 - 공개키 암호 알고리즘

■ 안전한 암호 알고리즘(예시)(2016년9월 기준) ■

구분	공공기관	민간부문(법인·단체·개인)
대칭키 암호 알고리즘	SEED, LEA, <b>HIGHT</b> , ARIA-128/192/256	SEED ARIA-128/192/256 AE-128/192-256 Blowfish Camela-128/192/256 MISTY1 KASUMI 등
공개키 암호 알고리즘 (메시지 암호·복호화)	RSAES-OAEP	RSA RSAES-OAEP RSAES-PKCS1 등
일방향 암호 알고리즘	SHA-224/226/384/512	RHA-224/245/384/512 whirlpool 등



# 암호화 구현 및 키 관리 - 전송 시 암호화

■ 웹서버와 웹브라우저 간 전송시 암호화 방식 비교 ■

방식	데이터 부분암호화	개발비용
SSL 방식	지원하지 않음	낮음
응용프로그램 방식	지원함	높음

개인정보처리시스템 간 암호화

방식	VPN 서버부하	NAT 통과
IPSec VPN	낮음	어려움
SSL VPN	다소 높음	쉬움
SSH VPN	다소 높음	쉬움



# 암호화 구현 및 키 관리 - 전송 시 암호화

개인정보 취급자 간 암호화

방식		공인인증서 필요 여부	표준형식
이메일 암호화	PGP	필요하지 않음	PGP 자체정의
	S/MIME	필요함	X509, PKCS#7
이메일 첨부문서 암호화		필요하지 않음	없음



# 암호화 구현 및 키 관리 - 저장 시 암호화

■ 모듈·위치별 암호화 방식 ■

## • ① 개인정보처리시스템 암호화 방식

암호화 방식	암·복호화 모듈 위치	암·복호화 요청 위치	설 명
응용프로그램 자체 암호화	어플리케이션 서버	응용프로그램	<ul style="list-style-type: none"> <li>- 암·복호화 모듈이 API 라이브러리 형태로 어플리케이션 서버에 설치되고, <b>응용프로그램에서</b> 해당 암·복호화 모듈을 호출하는 방식</li> <li>- DB 서버에 영향을 주지 않아 DB 서버의 성능 저하가 적은 편이지만 <b>구축 시</b> 응용프로그램 전체 또는 일부 수정 필요</li> <li>- 기존 API 방식과 유사</li> </ul>
DB서버 암호화	DB서버	응용프로그램	<ul style="list-style-type: none"> <li>- 암·복호화 모듈이 <b>DB서버에</b> 설치되고 <b>DB서버에서</b> 암·복호화 모듈을 호출하는 방식</li> <li>- 구축 시 응용프로그램의 수정을 최소화할 수 있으나, <b>DB서버에</b> 부하가 발생하며 <b>DB스키마의</b> 추가 필요</li> <li>- 기존 Plug-In 방식과 유사</li> </ul>
DBMS 자체 암호화	DB서버	DB서버	<ul style="list-style-type: none"> <li>- <b>DB서버의</b> DBMS 커널이 자체적으로 암·복호화 기능을 수행하는 방식</li> <li>- 구축 시에 응용프로그램 수정이 거의 없으나, DBMS에서 <b>DB스키마의</b> 지정 필요</li> <li>- 기존 커널 방식(TDE)과 유사</li> </ul>
DBMS 암호화 기능 호출	DB서버	응용프로그램	<ul style="list-style-type: none"> <li>- 응용프로그램에서 <b>DB서버의</b> DBMS 커널이 제공하는 암·복호화 API를 호출하는 방식</li> <li>- 구축 시에 암·복호화 API를 사용하는 응용프로그램의 수정이 필요</li> <li>- 기존 커널 방식(DBMS 함수 호출)과 유사</li> </ul>
운영체제 암호화	파일 서버	운영체제 (OS)	<ul style="list-style-type: none"> <li>- OS에서 발생하는 물리적인 입출력(I/O)을 이용한 암·복호화 방식으로 DBMS의 데이터파일 암호화</li> <li>- <b>DB서버의</b> 성능 저하가 상대적으로 적으나 OS, DBMS, 저장장치와의 호환성 검토 필요</li> <li>- 기존 DB 파일암호화 방식과 유사</li> </ul>



# 암호화 구현 및 키 관리 - 저장 시 암호화

- ① 개인정보처리시스템 암호화 방식

분류	고려사항
일반적 고려사항	구현 용이성, 구축 비용, 기술지원 및 유지보수 여부
	암호화 성능 및 안정성
	공공기관의 경우, 국가정보원 인증 또는 검증 여부
기술적 고려사항	암·복호화 위치(어플리케이션 서버, DB서버, 파일서버 등)
	색인검색 가능 유무, 매치처리 가능 여부



# 암호화 구현 및 키 관리 - 저장 시 암호화

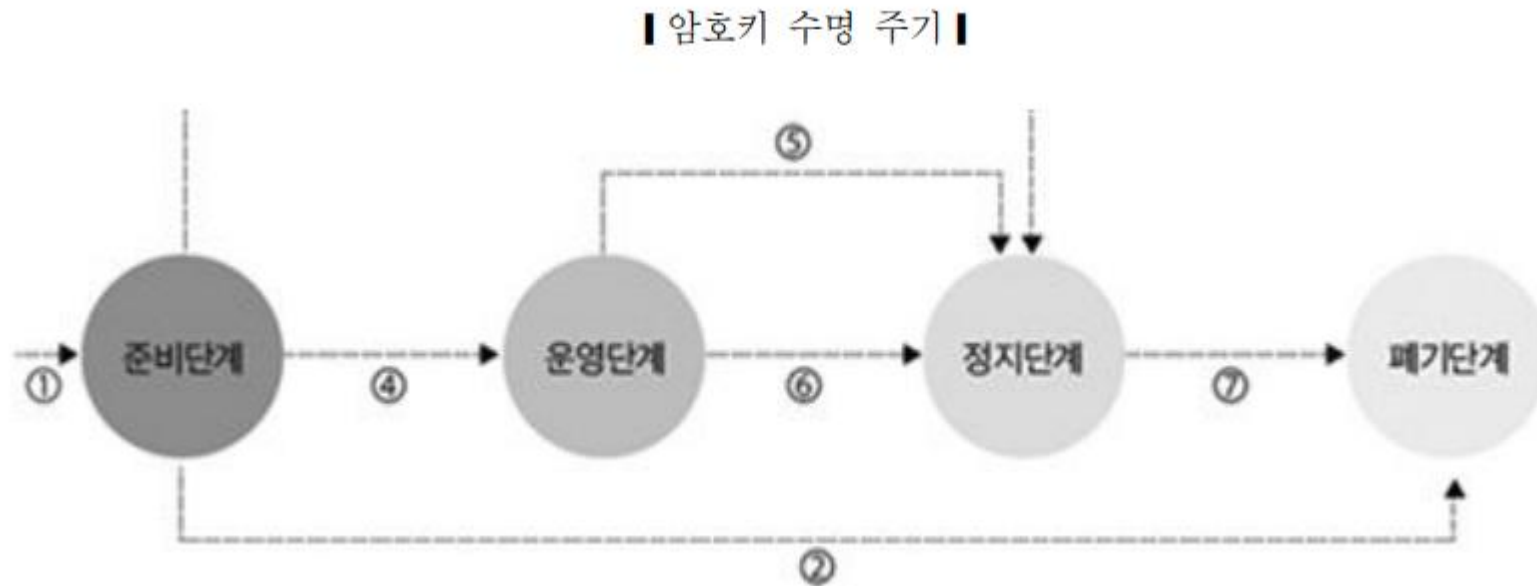
## • ② 업무용 컴퓨터 및 보조저장매체 암호화 방식

분류	특성
문서도구 자체 암호화	- 업무용 컴퓨터에서 사용하는 문서도구의 자체 암호화 기능을 통하여 개인정보 파일 암호화
암호 유틸리티를 이용한 암호화	- 업무용 컴퓨터의 OS에서 제공하는 파일 암호 유틸리티 또는 파일 암호 전용 유틸리티를 이용한 개인정보 파일, 디렉토리의 암호화
DRM (Digital Right Management)	- DRM을 이용하여 다양한 종류의 파일 및 개인정보 파일의 암호화 - 암호화 파일의 안전한 외부 전송이 가능
디스크 암호화	- 디스크에 데이터를 기록할 때 자동으로 암호화하고, 읽을 때 자동으로 복호화하는 기능을 제공 - 디스크 전체 또는 일부 디렉터리를 인가되지 않은 사용자에게 보이지 않게 설정하여 암호화 여부와 관계없이 특정 디렉터리 보호 가능



# 암호화 구현 및 키 관리 - 암호키 관리

- ① 암호키 수명주기







# 암호의 응용

---

- (1) 전자 서명
- (2) 해쉬 함수



**감사합니다**

