제 1 장
정 보 보 호

박 종 혁 교수

Tel: 970-6702

Email: jhpark1@seoultech.ac.kr

정보보호 / 암호 개념

[시청]

- 해킹과 보안기술의 발전, 우리의 정보는 과연 안전한가**?** - 애쓰디애쓴 지식영상
- 스마트 시대의 사이버 보안 : 인공지능과 보안이 만나면 **?** – **KIRD**

Thinking

- Cryptography ?

vs

- Information Security?

정보보안의 세부 연구 분야

- 암호학/분석
- 대칭키/공개키연구
- 시스템
- 네트워크 / 인터넷(웹)
- 임베디드 / 하드웨어
- 멀티미디어
- 개인정보보호(프라이버시)
- 정보보호 법률/정책
- 보안프로토콜
- 디지털 포렌식
- 블록체인
- 인공지능보안
- 첨단 보안기술 분야
  - IoT보안, 클라우드 보안, 자동차 보안, 양자암호 등

1절 네트워크 사회와 정보보호

2절 정보보호란?

3절 정보의 특성

4절 정보보호의 인적 요소

1.1 업무 패턴의 변화

- 네트워크를 통한 업무 처리
  - 이메일
  - 오디오 컨퍼런싱
  - 비디오 컨퍼런싱
  - 인스턴트 메시지
  - 소셜 미디어
  - 텍스트 메시징

1.2 인터넷 환경

- 한 국가의 경제개발과 복지 수준에 ICT 활용 정도를 나타내는 지표
  - E-readiness
    - 연결성과 기술적 인프라
    - 비즈니스 환경
    - 사회 문화적 환경
    - 법률적 환경
    - 정부 정책과 비전
    - 소비자와 비즈니스 분야 적용도

1.3 스마트워크

- 시간과 공간 제약 탈피

- 스마트워크센터 URL LINK : Smartworkcenter
  - 생산성 향상
  - 일자리 창출
  - 교통량 감소
  - 고령화, 저출산 문제 해결

- 자료전송의 빈번화
  - 정보보호문제 대두

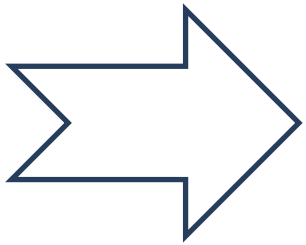
1.4 무슨 일이 벌어지는가?

- 네트워크를 통한 업무
  - 인터넷 쇼핑
  - 인터넷 뱅킹
  - 이메일 사용
  - 개인정보 제공
  - 생물학적 정보 제공
  - 유틸리티 활용
  - 프로그램 설치
  - 첨부된 파일 실행

- 위험하지 않을까?

1.5 무엇이 두려운가?

- 정보노출
- 정보변경
- 위장
- 정보전달의 지체
- 송신/수신 부정
- DoS 공격
- 신원 정보
- 신용카드 사용
- 온라인 송금
- 전자 상거래
- 이동전화 통신



정보보호

제2절 정보보호란?

2.1 정보보호란?

2.2 정보보호의 역사

2.3 보안과 보호

2.1 정보보호란?

- 정보의 수집, 가공, 저장, 검색, 송신, 수신 중에 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적, 기술적, 정책적 수단, 또는 그러한 수단으로 이루어지는 행위

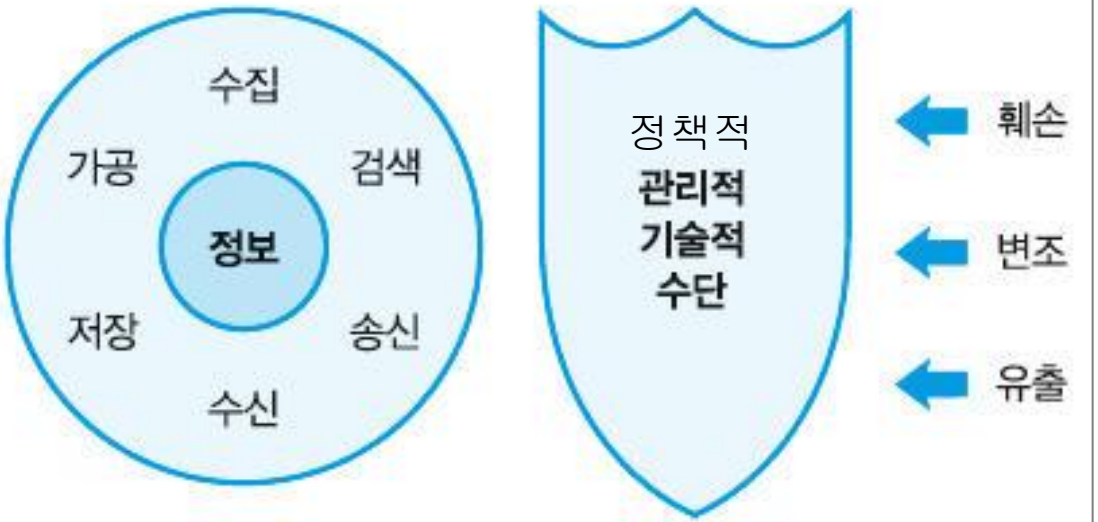


그림 1-2 • 정보보호

정보의 가용성과 안전성

- 정보의 활용과 정보의 통제 사이의 균형감각을 갖는 행위

그림 1-3 • 정보의 가용성과 안전성

2.2 정보보호의 역사

- 60년대 – 냉전 시대
- 70년대 – 네트워크 확산 시대
- 80년대 – PC와 네트워크
- 90년대 – WWW
- 2000년대 – 전자 상거래
- 현재 – 무선 네트워크와 이동성

60년대 – 냉전 시대

- 그물형 네트워크의 탄생
- ARPANET
- 정보보호 개념 부재
- Rand Report R-609
  - 보안 개념의 변화 계기
  - 보안 문제
    - 데이터 보안
    - 데이터 접근 제한
    - 인적 구성원에 대한 보안
- MULTICS(Multiplexed Information and computing Service) 개발 시작

70년대 - 네트워크 확산시대

- 4개의 노드로 시작
- 네트워크에 연결된 노드 수의 폭발적 증가
- ARPANET 의 보안문제 심각
  - 패스워드 구조와 형식의 취약성
  - 공중 전화망을 통한 접속의 안전성 결여
  - 사용자 시스템 접근 허락문제
- 암호를 이용한 전송
- 비대칭 암호의 발견

80년대 - PC와 네트워크

- PC 보급과 네트워크 연결
- TCP/IP 채택
- 인터넷 환경 구축
- 보안문제 급증
  - 네트워크를 통한 사기, 산업 스파이, 컴퓨터 해킹, 불법 접속
  - PC와 소규모 LAN을 대상으로 하는 공격

90년대 - WWW

- WWW 웹 브라우저 등장
- 인터넷 확산
- 정보보호의 산업화 표준 부족
- 물리적 보안이 주류

현재 - 무선 네트워크와 이동성

- 보안에 대한 개념 부족
- 유선보안에서 무선보안 문제로 진화
- 개인정보보호문제 심각
- 개인정보보호법 등 법적 제도 마련
- 정보보호는 한 컴퓨터의 안전만으로 해결되지 않는다.

- 해킹과 보안기술의 발전 (해커, 암호, 공개키, 랜섬웨어) (12m)

2.3 보안과 보호

국어사전 의미 차이

- **보안 (保安)**
  - 정의

    보안[1] 保安 ★

    1. 명사 안전을 유지함.
    2. 명사 사회의 안녕과 질서를 유지함.

  - 외부의 위협으로부터 중요한 정보를 보호하는 데 중점을 둠
  - 예시: 정보보안, 국가보안, 보안시설
- **보호 (保護)**
  - 정의

    보호[1] 保護 ★★

    1. 명사 위험이나 곤란 따위가 미치지 아니하도록 잘 보살펴 돌봄.
    2. 명사 잘 지켜 원래대로 보존되게 함.

  - 어떤 대상이 위험이나 손상으로부터 안전하게 지켜지도록 도와주는 것
  - 예시: 환경 보호, 인권 보호, 아동 보호

2.3 보안과 보호

정보통신망법 의미 차이

- **정보보안**
  - 정보 시스템과 네트워크를 안전하게 보호하기 위한 기술적, 물리적 방법
  - 해킹, 바이러스, 악성 코드와 같은 사이버 위협으로부터 시스템과 정보를 보호하는 것에 집중

- **정보보호**
  - 정보의 기밀성, 무결성, 가용성을 유지하고 보호하기 위한 전반적인 노력과 시스템
  - 사용자 개인정보와 중요한 데이터를 외부 위협으로부터 보호하고, 불법 유출 및 손실을 방지하는 활동에 집중

- **정보보안과 정보보호는 여러 분야에서 혼용 되어 사용**
  - 목적에 따라 다르게 사용될 필요

2.3 보안과 보호

- **정보보안**
  - 가치 있는 유형과 무형 자산을 도난, 소실, 유출로부터 보호하는 것
  - 네트워크 보안 및 시스템 보안에 대한 구체적인 기술적 대응이 강조
  - 기술적 / 실무적 성격 강조 / 필드에서 주로 사용

- **정보보호**
  - 정보를 저장하거나 유통하는 전반적인 시스템의 안정
  - 보안 사고를 예방하기 위한 법적 규제와 관리 절차를 포함
  - 관리적, 정책적 / 포괄적 / 학문적 성격 강조 / 학계에서 주로 사용

다중보안시스템

- 물리적 보안(Physical Security)
- 인적 보안(Personal Security)
- 운용 보안(Operation Security)
- 통신 보안(Communication Security)
- 네트워크 보안(Network Security)
- 정보보호(Information Security)

정보보호시스템

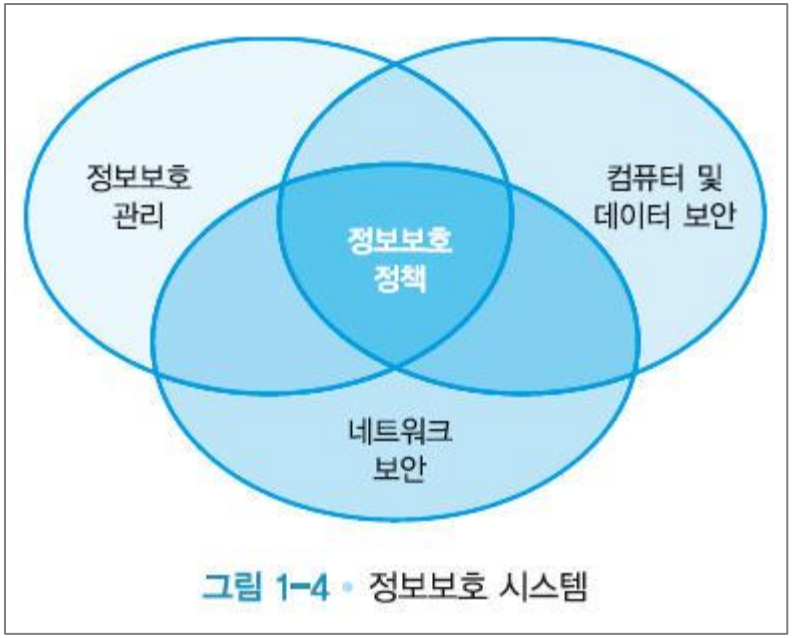


그림 1-4 • 정보보호 시스템

CIA Triad

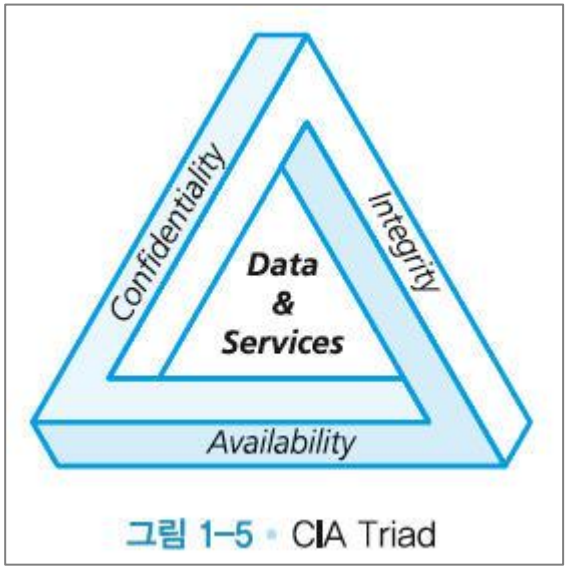


그림 1-5 • CIA Triad

- 기밀성(Confidentiality)
- 무결성(Integrity)
- 가용성(Availability)

제3절 정보의 특성

3.1 정보보호 서비스의 종류

3.2 정보보호의 대상

3.3 컴퓨터의 양면성

3.4 가용성과 보안성

3.1 정보보호 서비스의 종류

- 가용성(availability)
- 기밀성(confidentiality)
- 무결성(integrity)
- 인증(authentication)
- 부인방지(nonrepudiation)
- 소유권(possession)
- 정확성(accuracy)
- 활용성(utility)

정보보호 서비스의 종류

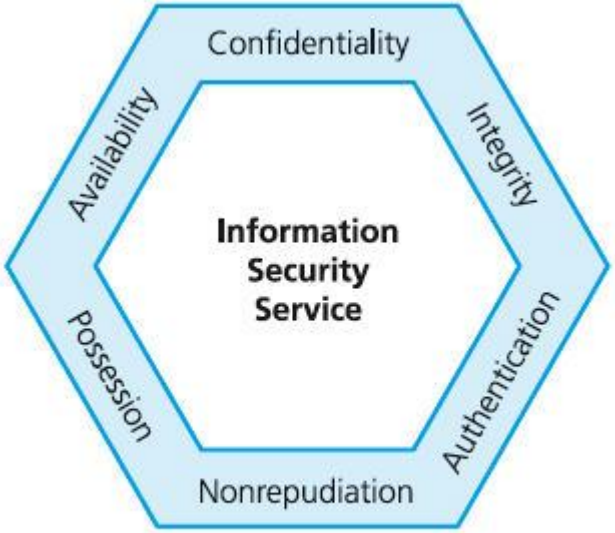


그림 1-6 • 정보보호 서비스의 종류

3.2 정보보호의 대상

- 소프트웨어(software)
- 하드웨어(hardware)
- 데이터(data)
- 인적 요소(personnel)
- 절차(procedure)
- 네트워크(network)

3.3 컴퓨터의 양면성

- 보안공격의 주체
- 공격의 대상
- 직접공격
- 간접공격

3.4 가용성과 보안성

- 정보보호는 보안과 가용성의 균형감을 유지하는 것
- 사용자의 요구와 보안관리자의 전문성 사이에서 균형점인 타협점 찾기

사람이 바로 조직의 정보보호 프로그램의 링크 중에서 가장 취약한 링크

4.1 정보보호의 인적요소

- 사회공학적 공격(social engineering attack)
- 사람의 심리적인 취약점을 활용하여 정보를 취득하거나 컴퓨터 접근권한을 얻거나 정보제공을 재정적 이득과 연결하여 시스템을 공격하는 방법

정보보호의 인적요소

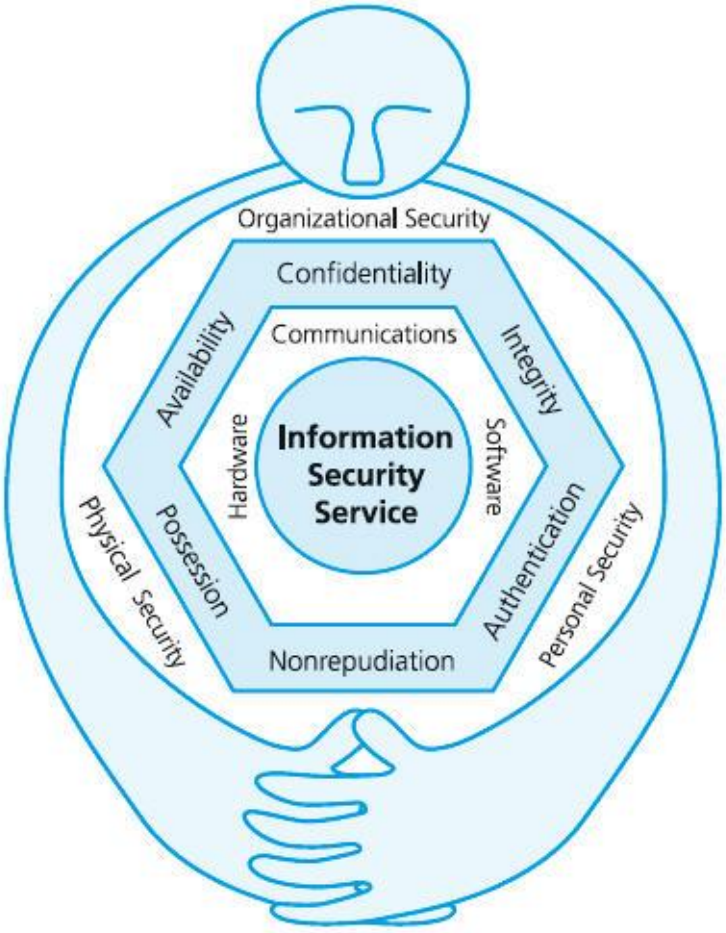


그림 1-7 • 정보보호의 인적 요소

정보보호 기초개념

정보보호 ?

- 정보보호(Information Security)의 법률적 의미

“정보보호’란 정보의 수집, 가공, 저장, 검색, 송신, 수신 중 발생할 수 있는 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적·기술적 수단을 마련하는 것”[1)]

- 정보보호의 사전적 의미

“정보의 수집, 가공, 저장, 검색, 송신, 수신 중에 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적·기술적 수단 또는 그러한 수단으로 이루어지는 행위”[2)]

일반적으로 정보는 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)을 유지해야 함

---

1) 「국가정보화 기본법」 제3조제6항

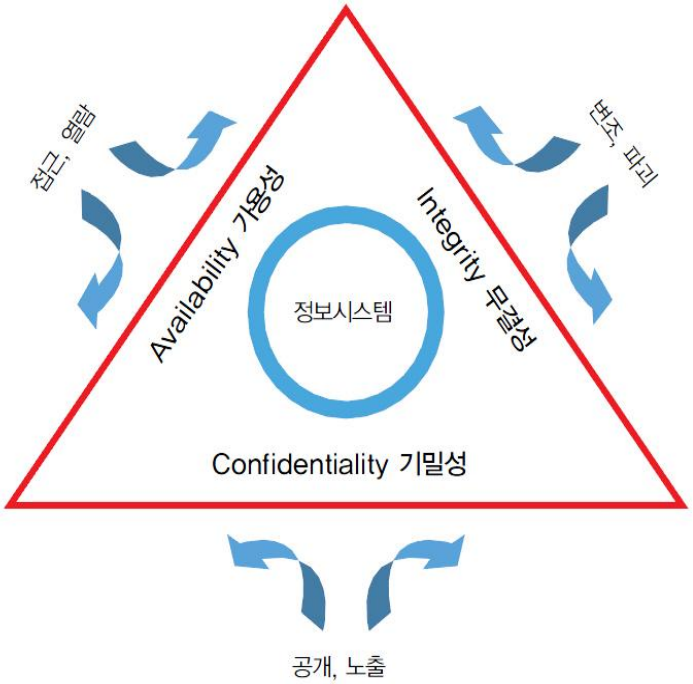
2) 한국정보통신기술협회의(TTA, Telecommunications Technology Association) 용어의 정의

정보보호의 기본 목표(3대 목표: CIA)

- 기밀성(Confidentiality)
  - 허락되지 않은 사용자 또는 객체가 정보의 내용을 알 수 없도록 하는 것
- 무결성(Integrity)
  - 허락되지 않은 사용자 또는 객체가 정보를 함부로 수정할 수 없도록 하는 것
- 가용성(Availability)
  - 허락된 사용자 또는 객체가 정보에 접근하고자 할 때 방해 받지 않도록 하는 것

6대 목표: 아래 3항목 추가

- 책임추적성(Accountability)
- 인증성(Authentication)
- 신뢰성(Reliability)



정보보호의 3요소

- 책임추적성(Accountability)
  - 각 객체의 행위를 유일하게 추적할 수 있음을 보장

- 인증성(Authentication)
  - 어떤 주체나 객체가 틀림없음을 보장
  - 정보시스템 상에서 이루어지는어떤 활동이 정상적이고 합법적으로 이루어진 것을 보장

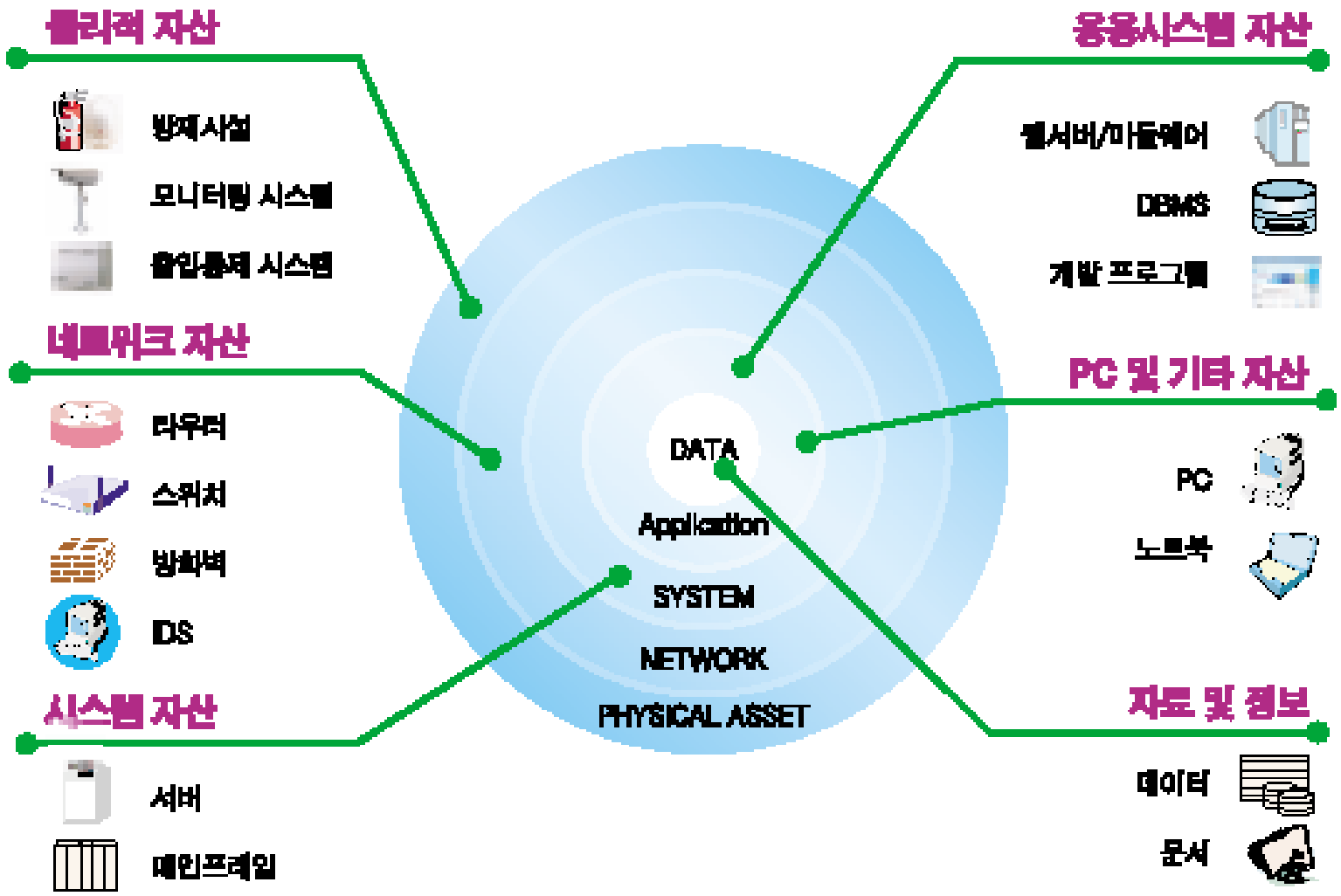
- 신뢰성(Reliability)
  - 의도된 행위에 대한 결과의 일관성을 유지
  - 정보나 정보시스템을 사용함에 있어서 일관되게 오류의 발생 없이
    계획된 활동을 수행하여 결과를 얻을 수 있도록 하는 환경을 유지

정보보호 용어

	용 어	의 미
Attacker	공격자	시스템을 공격하거나 위협하는 존재
Attack	공격	시스템의 보안 서비스를 회피하여 보안 정책을 위반하려는 의도된 시도
Countermeasure	대응/대책	위해를 최소화하거나 적절한 대응을 위해 탐지, 보고하여 위협, 노출, 공격을 제거하거나 방지하는 행위, 장비, 기법
Risk	위험	특정 위협이 가져올 확률적으로 표현되는 예상되는 손실
Security Policy	보안 정책	시스템이나 기관이 민감하고 중요한 시스템 자원들에 보안 서비스를 제공하기 위해 명시한 규정과 업무
Asset	시스템 자원 (자산)	정보 시스템내의 데이터, 시스템의 서비스, 처리 기능, 통신 대역폭, 시스템 장비(하드웨어, 펌웨어, 소프트웨어, 문서), 시스템 장치 설비
Threat	위협	보안을 침해하고 손해를 가져올 수 있는 상황, 행위, 이벤트가 존재할 때 잠재적 보안 위반
Vulnerability	취약성	시스템 보안 정책을 위반할 수 있는 시스템 설계, 구현, 혹은 운영, 관리상의 오류 혹은 약점

*** 참고문헌: RFC 2828, internet Security Glossary**

- 유형별 취약성 분석 대상


물리적 자산
방재시설
모니터링 시스템
출입통제 시스템
네트워크 자산
라우터
스위치
방화벽
IDS
시스템 자산
서버
메인프레임
응용시스템 자산
웹서버/미들웨어
DBMS
개발 프로그램
PC 및 기타 자산
PC
노트북
자료 및 정보
데이터
문서
DATA
Application
SYSTEM
NETWORK
PHYSICAL ASSET

- 보안 위협 분류

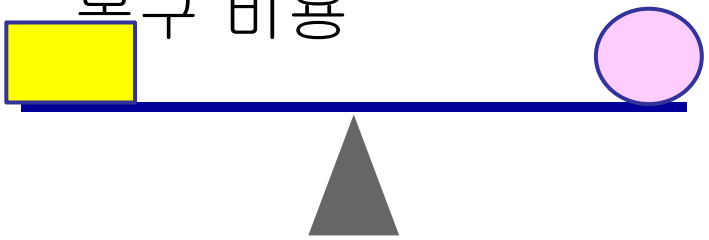
분 류		내용
자연에 의한 위협		• 화재, 홍수, 지진, 전력 차단 등 자연에 의한 대표적인 위협으로부터 발생하는 재난을 항상 예방 하기 어려움 • 화재경보기, 온도계, 무정전 시스템 등을 설치하여 피해를 최소화
인간에 의한 위협	비의도적 위협	• 정보시스템의 보안 사고를 일으키는 가장 큰 위협: **인간의 실수와 태만** – 패스워드의 공유, 데이터 백업의 부재 등 • 실제 정보보호 문제를 일으키는 가장 중요한 요인
	의도적 위협	• 컴퓨터 바이러스, 해커, 사이버 테러리스트 등으로부터 발생 – 도청, 신분 위장에 의한 불법 접근 – 정당한 정보에 대한 부인 – 악의적인 시스템 장애 유발

정보 정책

- 시스템이나 조직이 민감하고 치명적인 시스템 자원에 제공하는 보안 서비스 방법에 대한 일반적이고 형식적인 규칙

- 고려 사항
  - 보호하고자 하는 자산의 가치
  - 시스템 취약점
  - 잠재적인 위협과 공격 가능성

- 고려해야 할 절충 사항
  - 사용의 용이성 VS 보안성
  - 보안 비용 VS 오류 및 복구 비용



정보보호대책(Countermeasure)

- **정의**

  “위협에 대응하여 정보자산을 보호하기 위한 관리적, 물리적, 기술적 대책”

  – 방화벽, 침입탐지시스템 등의 정보보호시스템 뿐만 아니라
  – 정책, 지침, 절차 등의 모든 통제사항이 포함

- **보호대책 선택시 중요 고려사항**
  – 위험분석을 통해 조직의 환경과 문화에 맞는 것을 선택하는 것

- **비용 산정시 고려사항**
  – 구축비용뿐만 아니라 운영에 따른 관리비용을 반드시 고려해야 함

참고문헌

- 정보 보안 개론 (4판), 양대일, 한빛아카데미 (2021)
- 보호 / 보안, 네이버 국어사전, 2025
- Stallings, 컴퓨터보안 (Computer Security(GE), 복두출판사, 2016
- 장상수, 정보보호총론 , 생능출판사, 2015
- 김경신, 정보보안과 사이버해킹의 기초, 복두출판사, 2016
- 전정훈 외 2인, 정보보호개론, 사이텍미디어, 2009

Q & A

Thank You!