# 1주차

## 1

## 보안

자산의 본래가치가 손상되지 않도록 내, 외부의 위협으로부터 보호하는 것

## 정보보호

변조, 파괴, 서비스 등의 불법적 노출로부터 정보를 보호하는 것

## 정보보호 3대요소

1. 기밀성

인가된 사용자만 정보자산에 대한 접근을 허용

Ex) 도청, 도난

1. 무결성

데이터가 악의적으로 변경되지 않는 것

인가된 사용자가 인가된 방법으로 변경가능한 것

Ex)누군가 내 SNS의 대화명을 바꿨을 경우

1. 가용성

인가된 당사자가 원하는 시간에 데이터에 접근 가능한 것

Ex) 해커가 내가 접근이 불가능하게 계좌를 막았을 경우

디도스, 화재, 정전 등에 의해 깨질 수 있다.

## 정보보안을 위한 추가요소

1. 책임의 추적성

모든 행동에 대한 **기록**과 주체에 대한 추적을 **제공**하는 것

1. 인증

데이터, 서비스 이용을 위해 **신분을 식별하는 행위**

1. 접근제어(접근권한)

데이터나 서비스 이용에 대한 **허가 또는 거부**하는 기능

</br>

</br>

## 2

## 보안 위협

자산에 손상을 발생시킬 수 있는 **잠재적 가능성**이 있는 것

ex)

화산, 지진, 홍수 등의 자연재해

사전지식 없는 사용자에 의한 사고

테러리스트, 산업스파이 등등

## 보안 취약점

위협에 사용될 수 있는 **자산 내 약점**으로, 안전장치의 **부재 또는 미비**를 의미

ex)

자물쇠가 고장난 문

최신 엔진으로 업데이트 되지 않은 백신

## 정보통신 과정에서의 보안 위협

1. 가로막기

출발지로부터의 정보가 **분실**되거나 목적지에 **도착을 못하는** 경우

1. 가로채기

특수 장비 등을 이용해 제 3자가 **중간에 정보를 가로채** 기밀성을 침해하는 경우

1. 정보수정

제 3자가 송신된 정보를 변조 후 전송함으로 **정보의 일관성을 침해**하는 위험

1. 정보위조

허가 받지 않은 사용자가 **올바르지 못한 정보를 전송**하거나 시스템에 위조된 정보를 보내는 경우

## 최신 보안 위협 동향

1. 분산화

여러개의 PC를 활용하여 공격하는 방식

1. 소셜 공학

사람의 심리, 감정 등의 인간의 취약점을 이용한 공격의 증가

1. 스마트폰

악성 앱의 급증

</br>

</br>

## 3

## 보안의 분야

1. 시스템 보안

컴퓨터 **시스템의** **취약성을 이용한 공격**으로부터 자산 보호

계정관리, 세션관리, 권한관리 등의 일을 한다

1. 네트워크 보안

네트워크 **프로토콜의** **취약성을 이용한 공격**으로 부터 보호

분산공격, 세션 하이재킹, 디도스 공격, 스푸핑 공격 등이 있다

1. 물리적 보안

컴퓨터 및 정보 시스템을 화재, 파괴, 지진 등 **물리적 위험**으로부터 보호

시설관리, 보안교육, CCTV 침입탐지 등을 시행

1. 모바일 보안

모바일 운영체제의 불안정성, 이동성으로 인한 문제점으로부터 개인정보보호

버퍼 오버 플로우, 악성 앱 탐지 등이 행해진다

## 보안에 실패하는 이유

1. 복잡성

보안의 가장 큰 위험 요소

시스템에 내제된 **버그와 오류**가 취약점으로 연결

복잡도 증가시 증가된 보안 버그 내제도 증가

1. 공격자

다양한 목적의 공격자가 존재

장난, 절도, 사기, 감시, 테러 등

1. 인적 요인

많은 보안 문제가 **사람의 책임**에 의해 발생

엉성한 절차, 보안성 체크 무시 등

1. 투자

보안에 대한 투자 우선순위가 상대적으로 낮음