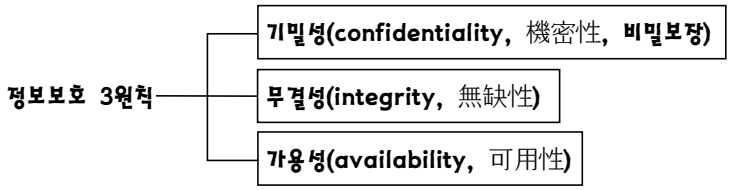
3. 정보보호 주요 3원칙

정보보호의 핵심 3원칙은 **"기밀성, 무결성, 가용성"**으로 분류한다.



◈ 기본 개념

가용성	• 정보시스템은 정당한 사용자에게 적절한 방법으로 **정보 서비스를 제공**해야 한다. • 인가된 사용자는 적절한 시간에 정보 접근 및 사용이 가능해야 한다. • 이용 불가능한 정보는 전혀 의미가 없다. • 예 : 고객이 자신 계좌에서 돈을 인출할 수 없으면, 은행은 어떻게 될 것인가?
무결성	• 허가 되지 않은 사용자 또는 객체가 **정보를 임의로 변조할 수 없도록** 한다. • 무결성 자체만으로는 메시지가 변조되지 않도록 하는 것은 아니다. • 따라서, 정보보호에서 변조를 발견할 수만 있으면 무결성이 제공된다고 한다. **//예 : 은행에서 고객이 입출금하면 계좌의 잔액은 변경되어야 한다.** • 정보가 변경되었다고 무조건 무결성 훼손은 아니다. • 정보는 정당하게 영속적으로 변경되어야 한다. • 즉, 인가된 사람에 의해 인가된 방법으로만 정보를 변경할 수 있도록 한다.
기밀성	• 허가 되지 않은 사용자 또는 객체는 **정보의 내용을 알 수 없도록** 한다. • 해킹(도청) 되어도 제3자는 정보의 내용을 알아 볼 수 없도록 하는 것이다. • 허가된(인증된) 집단만 데이터를 알아 볼 수 있도록 한다. • 기밀성은 개인정보보호(Privacy)와 밀접한 관계가 있다. • 기밀성은 원치 않는 정보 공개를 차단하기 위한 것이다. • 예 : 은행의 고객 계좌는 비밀이 유지되어야 한다.

◈ 위협 요소

가용성	• **가용성 위협 요소** : 서비스 거부 공격(DoS 공격), 웜(worm), 방해(가로막기) 등 • 가용성은 데이터 백업, 중복 저장 등으로 위협 요소로부터 보호할 수 있다.
무결성	• **무결성 위협 요소** : 변조, 위조, 유지보수, 부인, 재전송(replaying, 재연) 등 • 무결성의 환경적인 위협 요소 : 먼지, 열, 정전기, 서지(surge) 전류 등 • 서지(surge) 전류는 낙뢰 등에 의한 이상 전류를 의미한다. • 무결성은 접근통제, 엄격한 인증 절차 등으로 구현할 수 있다.
기밀성	• **기밀성 위협 요소** : 트래픽 분석, 도난, 도청, ***사회공학(social engineering)*** 등 • 기밀성은 암호화, 접근통제 등을 이용하여 구현할 수 있다. • 기밀성은 정보 보관 및 정보 전송에도 적용되어야 한다.

보안에서 사회공학(social engineering, 社會工學)

- 컴퓨터 보안학적 관점에서 사회공학은 기술적인 방법이 아닌 사람들 관계의 깊은 신뢰를 바탕으로 사람을 속여 비밀 정보를 획득하는 기법을 말한다.**(신뢰 기반의 해킹)**
- 사회공학적 해킹은 사람의 취약점을 공략하여 비밀정보를 획득하는 공격 기법이다.

◈ **사회공학적 해킹 사례**

---

① 통신망에 접근권한이 있는 담당자와 신뢰를 쌓은 후에 비밀정보를 획득한다.
→ 상대방의 권한이나 자만심 등을 이용한다.
② 정보의 가치를 몰라서 보안을 소홀히 하는 조직의 무능을 이용한다.
③ 주요 고객, 기술 지원, 상급기관 직원 등으로 가장하여 경계심을 없앤 후 정보 획득
④ **피싱, 파밍, 인터넷 메신져, 연말연시에 이메일 및 SNS**를 이용한 악성코드 유포 등
⑤ 웨일링(whaling) 공격
- 웨일링은 유명 인사를 대상으로 공격하는 해킹을 말한다.(인터넷 개인정보 수집 이용)

◈ **소셜 네트워킹 서비스(Social Networking Service, SNS) - 사회관계망서비스**

- SNS는 사용자들 사이의 자유로운 의사소통, 정보공유, 인맥 확대 등을 통해 사회적 관계를 생성하고 강화해주는 온라인 플랫폼을 의미한다.
- SNS는 대부분이 웹 기반 서비스이다. 웹 이외에도 전자우편이나 메신저를 이용할 수 있다.
- 현재, SNS 시장을 주도하고 있는 것은 **페이스북(facebook)과 트위터(twitter)**이다.
- SNS 환경에서 사회공학적 해킹은 무엇보다 강력한 보안의 위협이다.
→ 물리적인 네트워크 및 시스템 보안이 중요한 만큼, 사람의 보안도 매우 중요하다.
- 최근 페이스북에 올라온 단축 URL 및 사진을 이용하여 랜섬웨어를 유포하는 사례가 있다.

◈ **문자메시지(SMS, Short Message Service) - 단문 문자메시지 서비스**

- 휴대전화 부가서비스 중 하나이다.
- 휴대전화에서 짧은 문장(80자 이내)을 상대방에게 보낼 수 있는 기능이다.

정보보호서비스 사례

◉ **가용성**
- 남한이 중국과 무역하는 것을 북한이 집요하게 방해하지만, 한중 무역은 활성화 중이다.
- 어떤 회사의 웹 사이트는 그 회사에 대한 정보를 얻고자 하는 허가받은 고객들이 안정적으로 사용할 수 있어야 한다.

◉ **무결성**
- 컴퓨터를 구입한 고객이 지불한 수표가 가짜라는 것을 상점 주인이 눈치 채다.
- 병원에서 특정 환자의 질병 관련 기록을 해당 기록에 관한 접근권한이 있는 의사가 이용하고자 할 때, 그 정보는 오류 및 변조가 없는 정확성이 보장되어야 한다.

◉ **기밀성**
- 조폐공사는 수표에 특별한 잉크를 사용한다.
- 대학에서 각 학생들의 주민등록번호, 성적, 전화번호, 건강상태, 신체적 특징 등 개인정보는 안전하게 보호되어야 하며, 이러한 정보는 인가된 사람에게만 공개되어야 한다.

◉ **인증성**
- 은행은 고객이 로그인할 때, 고객의 신원과 비밀번호를 요구한다.
- 교수는 수강생이 신원증명을 제공하지 않으면, 학생에게 성적을 메일로 보내지 않는다.
- 인터넷을 통해 데이터를 주고받을 때, 수신자는 "데이터를 전송한 송신자가 정당한지? 아닌지?"를 확인할 수 있어야 한다.

◉ **접근제어(access control)**
- 정보나 자원을 사용하려고 할 때 허가되지 않은 경우는 접근을 못하게 한다.
- 학생이 다음날 보는 시험지를 확보하기 위해 야간에 교수 사무실 침입을 시도 했지만 불발로 끝났다.

◉ **부인방지(부인봉쇄)**
- 인터넷에서 데이터를 송수신한 사람이 자신의 행위를 부인하지 못하도록 한다.
- 생쥐가 치즈를 먹지 않았다고 주장했지만, 고양이는 생쥐가 치즈를 먹은 것을 증명했다.

☞ **"부인방지"의 뜻**
- "서명자가 해당 거래내역을 부인하지 못한다"는 것이다. 검증이 가능하므로
- 해당 거래에 대하여 "자신이 서명자가 아니라는 주장을 못한다"는 것은 아니다.

기출문제 분석

1. 대표적인 공격 유형으로 방해(interrupt)와 가로채기(intercept), 위조(fabrication), 변조(modification) 공격이 있다. 이 중 가로채기 공격에서 송수신되는 데이터를 보호하기 위한 정보 보호 요소는? [2014년 국가 7급]

① 기밀성(confidentiality)
② 무결성(integrity)
③ 인증(authentication)
④ 부인방지(non-repudiation)

♤ **기밀성(confidentiality, 機密性, 비밀보장)**

- 허가 되지 않은 사용자 또는 객체는 정보의 내용을 알 수 없도록 한다.
  → 해킹(도청) 되어도 제3자는 정보의 내용을 알아 볼 수 없도록 하는 것이다.
  → 허가된(인증된) 집단만 데이터를 알아 볼 수 있도록 한다.
- 기밀성 위협 요소로 **도난, 도청(가로채기), 사회공학(**social engineering) 등이 있다.

정답 : ①

2. 다음에서 설명하는 공격방법은? [2015년 국가 9급]

정보보안에서 사람의 심리적인 취약점을 악용하여 비밀정보를 취득하거나 컴퓨터 접근권한 등을 얻으려고 하는 공격방법이다.

① 스푸핑 공격
② 사회공학적 공격
③ 세션 가로채기 공격
④ 사전 공격

♤ **사회공학적 공격**

- 컴퓨터 보안학적 관점에서 사회공학은 기술적인 방법이 아닌 사람들 관계의 깊은 신뢰를 바탕으로 사람을 속여 비밀 정보를 획득하는 기법을 말한다.(신뢰 기반의 해킹)
- 사회공학적 해킹은 사람의 취약점을 공략하여 비밀 정보를 획득하는 공격 기법이다.
- 사회공학적 해킹은 상대방의 권한이나 자만심 등을 이용한다.

정답 : ②

3. 정보보호 서비스에 대한 설명으로 옳지 않은 것은? [2019년 국가 9급]

① Authentication – 정보교환에 의해 실체의 식별을 확실하게 하거나 임의 정보에 접근할 수 있는 객체의 자격이나 객체의 내용을 검증하는 데 사용한다.
② Confidentiality – 온오프라인 환경에서 인가되지 않은 상대방에게 저장 및 전송되는 중요 정보의 노출을 방지한다.
③ Integrity – 네트워크를 통하여 송수신되는 정보의 내용이 불법적으로 생성 또는 변경되거나 삭제되지 않도록 보호한다.
④ Availability – 행위나 이벤트의 발생을 증명하여 나중에 행위나 이벤트를 부인할 수 없도록 한다.

♤ **정보보호 서비스**

- Availability – 행위나 이벤트의 발생을 증명하여 나중에 행위나 이벤트를 **부인**할 수 없도록 한다.**(×)**
  → 컴퓨터 시스템에서 Availability은 **가용성**, 이용률 등을 의미한다.

정답 : ④

4. 무결성을 위협하는 공격이 아닌 것은? [2019년 지방 9급]

① 스누핑 공격(snooping attack)
② 메시지 변조 공격(message modification attack)
③ 위장 공격(masquerading attack)
④ 재전송 공격(replay attack)

♤ **위협요소**

가용성	• 가용성 위협 요소 : 서비스 거부 공격(DoS 공격), 웜(worm), 방해(가로막기) 등 • 가용성은 데이터 백업, 중복 저장 등으로 위협 요소로부터 보호할 수 있다.
무결성	• 무결성 위협 요소 : 변조, 위조, 유지보수, 부인, 재전송(replaying, 재연) 등 • 무결성은 접근통제, 엄격한 인증 절차 등으로 구현할 수 있다.
기밀성	• 기밀성 위협 요소 : 트래픽 분석, 도난, **도청**, 사회공학(social engineering) 등 • 기밀성은 암호화, 접근통제 등을 이용하여 구현할 수 있다. • 기밀성은 정보 보관 및 정보 전송에도 적용되어야 한다.

- 스누핑 공격(snooping attack)은 **도청**이다. **기밀성** 위협요소이다.

정답 : ①

5. 정보 보안 시스템을 설계하거나 운영할 때의 목표로 옳지 않은 것은? [2017년 국회 9급]

① 기밀성 보장 ② 무결성 보장
③ 가용성 보장 ④ 책임회피성 보장 ⑤ 사용자 인증

♤ **정보 보안 시스템**

- 정보보호의 3원칙은 "가용성, 무결성, 기밀성"으로 분류하고
- 그 외에 인증성, 접근제어, 부인방지 등으로 분류한다.
- 책임회피성은 부인과 같은 개념으로 정보보호가 될 수 없다.

정답 : ④

6. 사회공학적 공격 방법에 해당하지 않는 것은? [2018년 서울 9급]

① 피싱 ② 파밍
③ 스미싱 ④ 생일 공격

♤ **사회공학적 공격 방법**

- 생일 공격(×)
  → 생일 공격(birthday attack)은 암호학적 해시함수의 충돌을 찾아내는 암호해독 공격이다.
  → 생일 공격은 사람의 취약점을 공략하여 비밀정보를 획득하는 공격 기법이 아니다.
- 사회공학적 해킹은 사람의 취약점을 공략하여 비밀정보를 획득하는 공격 기법이다.

정답 : ④

7. 보안의 3대 요소 중 적절한 권한을 가진 사용자가 인가한 방법으로만 정보를 변경할 수 있도록 하는 것은? [2021년 지방 9급]

① 무결성(integrity) ② 기밀성(confidentiality)
③ 가용성(availability) ④ 접근성(accessability)

♤ **정보보호 주요 3원칙**

- 적절한 **권한**을 가진 사용자가 인가한 방법으로만 정보를 **변경**할 수 있도록 하는 것 → **무결성**
- 정보보호의 핵심 3원칙은 **"기밀성, 무결성, 가용성"**으로 분류한다.

정답 : ①

8. 다음 중 정보보호서비스 개념으로만 묶인 것으로 가장 옳은 것은? [2022년 군무원 9급]

① 은닉성, 보안성, 다형성
② 가용성, 기밀성, 부인방지
③ 무결성, 효율성, 인증
④ 대응성, 보호성, 소유성

♤ **정보보호서비스**

◉ **가용성**
- 남한이 중국과 무역하는 것을 북한이 집요하게 방해하지만, 한중 무역은 활성화 중이다.
- 어떤 회사의 웹 사이트는 그 회사에 대한 정보를 얻고자 하는 허가받은 고객들이 안정적으로 사용할 수 있어야 한다.

◉ **무결성**
- 컴퓨터를 구입한 고객이 지불한 수표가 가짜라는 것을 상점 주인이 눈치 채다.
- 병원에서 특정 환자의 질병 관련 기록을 해당 기록에 관한 접근권한이 있는 의사가 이용하고자 할 때, 그 정보는 오류 및 변조가 없는 정확성이 보장되어야 한다.

◉ **기밀성**
- 조폐공사는 수표에 특별한 잉크를 사용한다.
- 대학에서 각 학생들의 주민등록번호, 성적, 전화번호, 건강상태, 신체적 특징 등 개인정보는 안전하게 보호되어야 하며, 이러한 정보는 인가된 사람에게만 공개되어야 한다.

◉ **인증성**
- 은행은 고객이 로그인할 때, 고객의 신원과 비밀번호를 요구한다.
- 교수는 수강생이 신원증명을 제공하지 않으면, 학생에게 성적을 메일로 보내지 않는다.
- 인터넷을 통해 데이터를 주고받을 때, 수신자는 "데이터를 전송한 송신자가 정당한지? 아닌지?"를 확인할 수 있어야 한다.

◉ **접근제어(access control)**
- 정보나 자원을 사용하려고 할 때 허가되지 않은 경우는 접근을 못하게 한다.
- 학생이 다음날 보는 시험지를 확보하기 위해 야간에 교수 사무실 침입을 시도 했지만 불발로 끝났다.

◉ **부인방지(부인봉쇄)**
- 인터넷에서 데이터를 송수신한 사람이 자신의 행위를 부인하지 못하도록 한다.
- 생쥐가 치즈를 먹지 않았다고 주장했지만, 고양이는 생쥐가 치즈를 먹은 것을 증명했다.

정답 : ②