2. 인증(authentication)

• 먼저, 보안 관련 교재에서 가장 많이 나오는 단어가 뭘까? 바로 "**인증**"이다.
• 통신에서 "인증"은 매우 중요하다. 송수신자가 **비대면**으로 통신하기 때문이다.

◉ **개체 인증 / 메시지 인증**
개체 인증과 메시지 인증의 차이점을 구체적으로 살펴본다. - Forouzan 참조

인증	설 명
개체 인증	• 개체 인증은 **실시간으로 진행**된다. • 예를 들면, 개체 인증은 **자동현금지급기**에서 현금을 인출할 때 필요한 인증 절차이다. • 개체 인증은 주장자가 검증자에게 자신의 **신원**을 확인시켜야 한다.(정당성) **// 흥부가 놀부에게 개체 인증을 요구할 때** • 흥부가 놀부에 의해 개체 인증이 되기 전에는 실질적인 통신은 없다. • 흥부가 통신을 접속한 상태에서 놀부에 의해 인증이 통과되어야 한다. • 인증이 통과된 뒤에는 놀부와 흥부는 메시지를 주고받을 수 있다.
	• 개체 인증은 주장자에 대한 인증이 통과되면 그 **세션동안 유효**하다. • 즉, 한번의 인증이 통과되면 그 세션동안은 개체 인증이 유효하다.
메시지 인증	• 메시지 인증은 "**데이터 출처 인증**"이라고도 한다. • 메시지 인증은 **실시간으로 진행되지 않는다.** • 예를 들면, 메시지 인증은 **전자우편(이메일)**에 필요한 인증 절차이다. **// 놀부가 흥부에게 이메일을 보낸 경우** • 흥부가 이메일을 인증하는 시간에 놀부의 통신 상태 유지는 별개이다. • 즉, 놀부는 통신 상태일 수도 있고 아닐 수도 있다.
	• 메시지 인증은 **하나의 메시지에 대한 인증**이다. • 메시지 인증은 각 메시지마다 **별도의 인증이 필요**하다. • 즉, 모든 메시지에 대해 반복적인 인증 절차를 수행해야 한다.

◈ **전자서명이 제공하는 핵심 기능 – 3가지**
• 인증 : 서명은 신원이 올바른지 확인할 수 있다.
• 부인방지 : 서명의 고유성은 서명 소유자가 서명을 거부하지 못하도록 한다.
• 데이터 무결성 : 서명은 데이터 무결성을 확인할 수 있는 기능을 제공한다.

기출문제 분석

1. 사용자 신원을 검증하고 전송된 메시지 출처를 확인하는 정보보호 개념은? [2022년 국가 9급]

① 무결성 ② 기밀성 ③ 인증성 ④ 가용성

♤ **개체 인증 / 메시지 인증**

인증	설 명
개체 인증	• 개체 인증은 **실시간으로 진행**된다. • 예 : 개체 인증은 **자동현금지급기**에서 현금을 인출할 때 필요한 인증 절차이다. • 개체 인증은 주장자가 검증자에게 자신의 **신원**을 확인시켜야 한다.(정당성)
메시지 인증	• 메시지 인증은 "**데이터 출처 인증**"이라고도 한다. • 메시지 인증은 **실시간으로 진행되지 않는다.** • 예 : 메시지 인증은 **전자우편(이메일)**에 필요한 인증 절차이다. **// 놀부가 흥부에게 이메일을 보낸 경우** • 흥부가 이메일을 인증하는 시간에 놀부의 통신 상태 유지는 별개이다. • 즉, 놀부는 통신 상태일 수도 있고 아닐 수도 있다.

정답 : ③

2. 정보보호의 주요 목표 중 하나인 인증성(authenticity)을 보장하는 사례를 설명한 것으로 옳은 것은? [2014년 지방 9급]

① 대학에서 개별 학생들의 성적이나 주민등록번호 등 민감한 정보는 안전하게 보호되어야 한다. 따라서 이러한 정보는 인가된 사람에게만 공개되어야 한다.

② 병원에서 특정 환자의 질병 관련 기록을 해당 기록에 관한 접근권한이 있는 의사가 이용하고자 할 때 그 정보가 정확하며 오류 및 변조가 없었음이 보장되어야 한다.

③ 네트워크를 통해 데이터를 전송할 때는 데이터를 송신한 측이 정당한 송신자가 아닌 경우 수신자가 이 사실을 확인할 수 있어야 한다.

④ 회사의 웹 사이트는 그 회사에 대한 정보를 얻고자 하는 허가받은 고객들이 안정적으로 접근할 수 있어야 한다.

♤ **정보보호의 주요 목표**

① 기밀성(confidentiality) ② 무결성(integrity) ③ 인증성(authenticity) ④ 가용성(availability)

정답 : ③

3. 정보보호시스템이 제공하는 보안서비스 개념과 그에 대한 설명으로 옳은 것은? [2016년 국회 9급]

ㄱ. 기밀성(confidentiality) : 데이터가 위변조되지 않아야 함
ㄴ. 무결성(integrity) : 권한이 있는 자는 서비스를 사용하여야 함
ㄷ. 인증(authentication) : 정당한 자임을 상대방에게 입증하여야 함
ㄹ. 부인방지(non-repudiation) : 거래 사실을 부인할 수 없어야 함
ㅁ. 가용성(availability) : 비인가자에게는 메시지를 숨겨야 함

---

① ㄱ, ㄴ　② ㄱ, ㅁ　③ ㄴ, ㄷ
④ ㄷ, ㄹ　⑤ ㄹ, ㅁ

♤ **보안서비스**

ㄱ. 기밀성(confidentiality) : 데이터가 위•변조되지 않아야 함(×)
→ 기밀성은 허가되지 않은 사용자 또는 객체는 정보의 내용을 알 수 없도록 한다.
ㄴ. 무결성(integrity) : 권한이 있는 자는 서비스를 사용하여야 함(×)
→ 무결성은 허가되지 않은 사용자가 정보를 임의로 변조(수정)할 수 없도록 한다.
ㅁ. 가용성(availability) : 비인가자에게는 메시지를 숨겨야 함(×)
→ 가용성은 인가된 사용자는 적절한 시간에 정보 접근 및 사용이 가능해야 한다.

정답 : ④