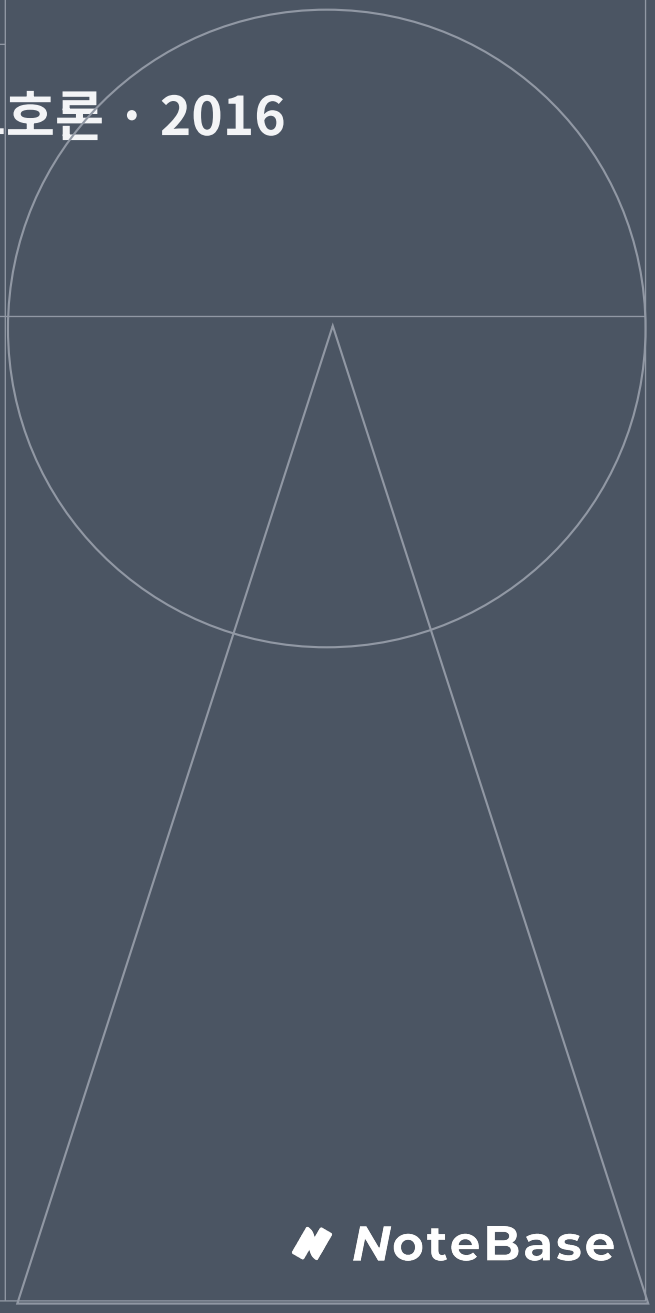
# 기출OX 해설집

공무원/국가직/7급 · 정보보호론 · 2016



NoteBase

# 기출OX 해설집

## 공무원/국가직/7급 · 정보보호론 · 2016

**공무원/국가직/7급 · 정보보호론 · 2016**

**문 1. 「개인정보 보호법」에서 규정하고 있는 개인정보 중 민감정보에 해당하지 않는 것은?**

① 주민등록번호

② 노동조합 · 정당의 가입 · 탈퇴에 관한 정보

③ 건강에 관한 정보

④ 사상 · 신념에 관한 정보

**정답 1번**

**쟁점**

이 문제는 개인정보 보호법상 민감정보와 고유식별정보의 구별에 관한 문제이다.
핵심은 주민등록번호가 민감정보가 아니라 고유식별정보라는 점을 구별하는 것이다.

**용어 풀이**

민감정보는 사상·신념, 노동조합·정당의 가입·탈퇴, 건강처럼 사생활 침해 우려가 큰 개인정보이다.
고유식별정보는 개인을 고유하게 식별하기 위하여 부여된 정보로서 주민등록번호 등이 여기에 해당한다.

**핵심 구분**

민감정보는 정보 내용 자체가 사생활 비밀을 깊게 드러내는 정보이고, 고유식별정보는 개인을 유일하게 특정하는 번호 정보이다.
주민등록번호는 민감정보가 아니라 고유식별정보이다.
반면 노동조합·정당의 가입·탈퇴 정보, 건강 정보, 사상·신념 정보는 민감정보에 해당한다.

NoteBase

### 선지별 해설

① O
- 주민등록번호는 개인정보 보호법상 민감정보가 아니라 고유식별정보에 해당하므로 '민감정보에 해당하지 않는 것'으로 맞다.

② X
- 노동조합·정당의 가입·탈퇴에 관한 정보는 정치적 견해와 결사의 자유 영역을 드러내므로 민감정보에 해당한다.
- 틀린 표현: 민감정보에 해당하지 않는다는 취지
- 올바른 표현: 노동조합·정당의 가입·탈퇴에 관한 정보는 민감정보에 해당한다.

③ X
- 건강에 관한 정보는 개인의 신체·질병 상태를 드러내는 대표적 민감정보이므로 오답 선택지이다.
- 틀린 표현: 민감정보에 해당하지 않는다는 취지
- 올바른 표현: 건강에 관한 정보는 민감정보에 해당한다.

④ X
- 사상·신념에 관한 정보는 내면적 가치관과 양심 영역을 드러내므로 민감정보에 해당한다.
- 틀린 표현: 민감정보에 해당하지 않는다는 취지
- 올바른 표현: 사상·신념에 관한 정보는 민감정보에 해당한다.

### 오답 포인트

이 문제를 틀렸다면 민감정보와 고유식별정보를 같은 범주로 묶어 기억했을 가능성이 높다. 둘 다 보호 강도가 높은 개인정보이지만, 주민등록번호는 민감정보가 아니라 고유식별정보라는 점이 함정이다.

### 다시 나오면 이렇게 판단

발문이 '해당하지 않는 것'인지 먼저 확인한 다음, 선지를 '사생활 내용형 정보'와 '식별번호형 정보'로 나누어 판단하면 된다. 사상·신념, 건강, 정당·노동조합 가입 여부처럼 내용 자체가 민감하면 민감정보이고, 주민등록번호처럼 개인을 특정하는 번호는 고유식별정보이다.

### 암기 포인트

주민등록번호는 고유식별정보, 사상·신념·건강·정당·노동조합 가입 여부는 민감정보이다.

NoteBase

**문 2. 메시지의 무결성 보장과 송신자에 대한 인증을 목적으로 공유 비밀키와 메시지로부터 만들어지는 것은?**

① 의사 난수

② 메시지 인증 코드

③ 해시

④ 인증서

**정답 2번**

### 출제 포인트

이 문제는 공유 비밀키를 함께 써서 메시지 무결성과 송신자 인증을 제공하는 MAC와, 단순 해시나 인증서의 역할을 구별하는 문제이다.

### 핵심 개념

메시지 인증 코드(MAC)는 공유 비밀키와 메시지를 함께 입력으로 하여 만든 값으로, 메시지가 바뀌지 않았는지와 같은 비밀키를 아는 송신자가 보냈는지를 확인하는 데 사용된다.
해시는 보통 메시지만으로 계산하는 고정 길이 요약값으로, 비밀키가 없으면 송신자 인증 기능은 없다.
인증서는 공개키와 신원을 연결하는 전자문서이며, 인증기관의 서명으로 신뢰를 부여한다.
의사 난수는 시드나 내부 상태에서 생성되는 난수열로, 특정 메시지의 무결성 검증값 자체를 뜻하지는 않는다.

### 선지별 해설

① X: 의사 난수는 난수열 생성이 목적이며 메시지와 공유 비밀키를 결합해 무결성과 송신자 인증을 확인하는 값이 아니다. 틀린 표현은 "공유 비밀키와 메시지로부터 만들어지는 것"에 의사 난수를 대응시킨 부분이다. 올바르게는 공유 비밀키와 메시지로부터 만들어져 무결성과 인증에 쓰이는 것은 MAC이다.
② O: 메시지 인증 코드(MAC)는 공유 비밀키와 메시지로부터 생성되며, 수신자가 같은 비밀키로 다시 계산해 비교함으로써 메시지 무결성과 송신자 인증을 확인할 수 있다.
③ X: 해시는 메시지 내용의 요약값이지만 일반적인 해시 함수는 공유 비밀키를 사용하지 않는다. 틀린 표현은 해시를 "송신자 인증" 목적의 공유 비밀키 기반 값으로 본 부분이다. 올바르게는 해시는 메시지 자체로 계산하는 요약값이고, 공유 비밀키를 이용한 인증값은 MAC이다.
④ X: 인증서는 공개키와 사용자 신원을 연결해 주는 증명서이며 인증기관의 서명이 핵심이다. 틀린 표현은 인증서를 "공유 비밀키와 메시지로부터 만들어지는 값"으로 본 부분이다. 올바르게는 인증서는 공개키 기반 인증 구조의 문서이고, 이 문제의 설명에 맞는 것은 MAC이다.

### 오답 포인트

③ 해시와 ② MAC를 같은 것으로 착각하기 쉽다. 둘 다 메시지에서 어떤 값을 만든다는 점은 비슷하지만, 공유 비밀키가 들어가면 MAC이고 비밀키 없이 메시지만 요약하면 해시이다.

NoteBase

**다시 나오면 이렇게 판단**

문제에 "공유 비밀키", "무결성", "송신자 인증"이 함께 나오면 먼저 MAC를 떠올리면 된다. 반대로 비밀키 없이 메시지 요약만 강조하면 해시, 공개키와 신원 연결을 묻으면 인증서로 판단한다.

**암기 포인트**

MAC는 비밀키+메시지, 해시는 메시지만, 인증서는 신원+공개키이다.

NoteBase

**문 3. 사용자 인증을 위한 접근방법으로 사용자가 알고 있는 것, 사용자가 가지고 있는 것, 사용자 자신의 특성을 이용하는 것 등이 있다. 최근 사용이 증가하고 있는 OTP(One Time Password)에 대한 설명으로 옳은 것은?**

① 어떤 패스워드가 일정유형으로 반복해서 생성된다.

② 사용자가 알고 있는 정보에 의한 인증 기법이다.

③ 일반적으로 사용자 자신의 특성을 이용하는 기법들에 비하여 식별 오류 발생 가능성이 높다.

④ 생성 방식에 따라 사용자나 인증 서버의 관리 부담이 발생할 수 있다.

**정답 4번**

**출제 포인트**

이 문제는 OTP의 본질이 일회용 비밀번호라는 점과 인증 요소상 무엇을 소지한 인증에 가깝다는 점을 구별하는 문제이다.

**핵심 개념**

OTP는 로그인할 때마다 새롭게 생성되어 한 번만 사용하는 비밀번호이다.
정적 비밀번호는 같은 비밀번호를 반복 사용하지만, OTP는 시간 동기, 이벤트 동기, 챌린지-응답 방식 등으로 매번 다른 값이 생성된다.
인증 요소로는 사용자가 소지한 토큰, 카드, 휴대기기 등을 이용해 값을 만들어 내므로 일반적으로 무엇을 가지고 있는가에 해당한다.

**선지별 해설**

① X: 틀린 부분은 "일정유형으로 반복해서 생성된다"이다. OTP는 반복 사용하는 비밀번호가 아니라 인증 시마다 새로 생성되는 일회용 비밀번호이다.
② X: 틀린 부분은 "사용자가 알고 있는 정보에 의한 인증"이다. OTP는 암기한 고정 비밀번호 자체가 아니라 사용자가 소지한 토큰이나 기기로 생성한 값을 이용하므로 일반적으로 소지 기반 인증으로 본다.
③ X: 틀린 부분은 "사용자 자신의 특성을 이용하는 기법들에 비하여 식별 오류 발생 가능성이 높다"이다. 생체인증은 오인식과 오거부 같은 매칭 오류가 본질적으로 발생할 수 있지만, OTP는 그런 생체 특징 매칭 방식이 아니므로 이 진술은 적절하지 않다.
④ O: OTP는 생성 방식에 따라 시간 동기화 관리, 토큰 배포 및 분실 관리, 인증 서버의 동기화 유지 같은 운영 부담이 생길 수 있으므로 옳다.

NoteBase

**오답 포인트**

수험생은 비밀번호라는 단어만 보고 곧바로 "사용자가 아는 것"으로 분류하기 쉽다. 이 문항은 비밀번호의 형태보다 어떻게 생성되고 무엇으로 생성되는지를 묻는다. 또한 OTP를 생체인증과 비교해 오류율을 논하는 ③처럼 전혀 다른 인증 요소를 섞어 놓은 선지도 자주 함정으로 나온다.

**다시 나오면 이렇게 판단**

인증 문제는 먼저 세 요소인 지식, 소지, 생체로 나눈다. 그다음 해당 수단이 암기 정보인지, 별도 매체나 기기를 들고 있어야 하는지, 신체 특성을 읽는지로 판단하면 된다. OTP가 나오면 "일회용"과 "토큰·기기 기반"을 먼저 떠올리면 된다.

**암기 포인트**

OTP는 반복 암호가 아니라 일회용 암호이고, 분류는 지식보다 소지 인증에 가깝다.

NoteBase

**문 4. 위험 분석 방법 중 델파이법에 대한 설명으로 옳은 것은?**

① 위험 발생 빈도를 추정하는 계산식을 통해 위험을 계량하여 분석한다.

② 미지의 사건을 추정하는 데 사용되는 방법으로 확률적 편차를 이용해 최저, 보통, 최고의 위험도를 분석한다.

③ 전문가 집단으로 구성된 위험 분석팀의 위험 분석 및 평가를 통해 여러 가능성을 전제로 위험과 취약성에 대한 의견수렴을 통한 분석 방법이다.

④ 어떤 사건이 예상대로 발생하지 않는다는 사실에 근거하여 주어진 조건하에 발생 가능한 위험에 따른 결과를 예측하는 방법이다.

**정답 3번**

**출제 포인트**

이 문제는 델파이법과 정량적 위험분석, 확률적 추정 기법, What-if식 시나리오 분석을 구별하는 문제이다.

**핵심 개념**

델파이법은 전문가 집단의 의견을 반복적으로 수집하고 조정하여 합의된 판단을 도출하는 정성적 위험분석 방법이다. 결정 차이축은 계산식이나 확률모형을 쓰는지가 아니라 전문가 의견 수렴으로 판단하는지이다.
정량적 위험분석은 발생 가능성과 피해 규모를 수치화하여 위험도를 계산하는 방법이다.
확률적 추정 기법은 불확실한 값을 확률분포나 최저·보통·최고 추정치로 두고 결과 범위를 분석하는 방법이다.
What-if 분석은 어떤 사건이 예상과 다르게 일어날 때 가능한 결과를 시나리오로 예측하는 방법이다.

NoteBase

### 선지별 해설

① X
틀린 부분은 "계산식을 통해 위험을 계량화"이다. 이는 수치 계산을 사용하는 정량적 위험분석의 설명에 가깝다. 델파이법은 계산식보다 전문가 판단과 의견 수렴으로 위험을 분석한다.

② X
틀린 부분은 "확률적 편차를 이용해 최저, 보통, 최고의 위험도"이다. 이는 확률적 추정이나 시뮬레이션 계열 설명에 가깝다. 델파이법은 미지의 사건 예측에 활용될 수는 있지만, 핵심은 확률 편차 계산이 아니라 전문가 집단의 반복적 의견 수렴이다.

③ O
전문가 집단을 대상으로 위험과 취약성에 관한 의견을 모으고, 그 의견을 정리·수렴하여 판단하는 방식이라는 점이 델파이법의 핵심과 일치한다. 델파이법은 여러 가능성을 전제로 전문가 합의를 도출하는 정성적 분석 방법이다.

④ X
틀린 부분은 "어떤 사건이 예상대로 발생하지 않는다는 사실에 근거하여 ... 결과를 예측"이다. 이는 What-if처럼 가정된 조건 변화에 따른 결과를 따지는 시나리오 분석의 설명이다. 델파이법은 사건 가정의 결과 예측보다 전문가 의견 수렴 자체가 중심이다.

### 오답 포인트

델파이법도 미래 위험을 예측하는 데 쓰일 수 있으므로 ②와 혼동하기 쉽다. 그러나 선지에 계산식, 확률편차, 최저·보통·최고, 가정된 사건의 결과 예측 같은 표현이 나오면 델파이법이 아니라 다른 분석 기법일 가능성이 크다.

### 다시 나오면 이렇게 판단

선지에 전문가 집단, 반복 질의, 의견 수렴, 합의 형성이라는 말이 보이면 델파이법으로 판단한다. 반대로 계량화·계산식이면 정량적 분석, 최저·보통·최고나 확률분포이면 확률적 추정 기법, "만약 이런 일이 생기면" 식 결과 예측이면 What-if 분석으로 구분한다.

### 암기 포인트

델파이법은 계산이 아니라 전문가 반복 합의이고, What-if는 가정 결과 예측이며, 정량분석은 수치 계산이다.

NoteBase

**문 5. ARP(Address Resolution Protocol) 스푸핑(spoofing) 기법을 이용한 스니핑(sniffing) 공격의 대응책으로 적절하지 않은 것은?**

① 데이터를 암호화하여 전송한다.

② 라우터에 패킷 필터를 설정하여 서로 다른 LAN 간에 전송되는 패킷들을 검열하고 차단한다.

③ ARP 테이블 내의 MAC 주소 값을 정적(static)으로 설정한다.

④ 주기적으로 프러미스큐어스(promiscuous) 모드에서 동작하는 기기들이 존재하는지 검사함으로써 스니핑 중인 공격자를 탐지한다.

**정답 2번**

**출제 포인트**

이 문제는 ARP 스푸핑 기반 스니핑이 같은 LAN 내부의 ARP 캐시 위조로 성립한다는 점과, 이에 맞는 대응책을 구별할 수 있는지를 묻는다.

**핵심 개념**

ARP 스푸핑은 공격자가 거짓 IP-MAC 매핑을 주입해 같은 브로드캐스트 도메인 안의 트래픽을 자신에게 우회시키는 공격이다. 따라서 대응은 LAN 내부의 매핑 위조를 막거나, 가로채더라도 내용 유출을 줄이거나, 스니핑 장비를 탐지하는 방향이어야 한다.

**선지별 해설**

1번 O: 데이터를 암호화해 전송하면 공격자가 패킷을 가로채더라도 내용을 바로 해독하기 어렵다. 스니핑 자체를 없애지는 못해도 정보 유출 피해를 줄이는 적절한 대응이다.
2번 X: 틀린 부분은 "서로 다른 LAN 간에 전송되는 패킷들을 검열하고 차단한다"는 점이다. ARP 스푸핑은 같은 LAN 내부의 ARP 캐시를 속여 트래픽을 가로채는 공격이므로, 라우터의 LAN 간 패킷 필터만으로는 동일 세그먼트 내부 공격을 직접 막기 어렵다. 올바르게는 정적 ARP 설정, 동적 ARP 검사, 스위치 보안 기능, 암호화처럼 같은 LAN 내부의 위조 ARP와 도청을 줄이는 대책이 적절하다.
3번 O: ARP 테이블의 MAC 주소 값을 정적으로 고정하면 공격자가 가짜 ARP 응답으로 매핑을 바꾸기 어려워진다. 관리 부담은 있지만 대표적인 예방 대책이다.
4번 O: 프로미스큐어스 모드로 동작하는 장비를 주기적으로 점검하면 정상 호스트와 다른 수신 행태를 보이는 스니핑 장비를 탐지하는 데 도움이 된다. 예방보다는 탐지 성격이 강하지만 대응책으로는 적절하다.

**오답 포인트**

ARP 스푸핑을 단순한 패킷 필터링 문제로 보면 2번에 속기 쉽다. 이 공격의 핵심은 라우터를 지나는 다른 LAN 간 통신이 아니라, 같은 LAN 내부에서 IP-MAC 대응 관계를 속여 프레임 흐름을 바꾸는 데 있다.

NoteBase

### 다시 나오면 이렇게 판단

ARP, MAC, 스니핑이 함께 나오면 먼저 공격 범위가 같은 브로드캐스트 도메인 내부인지 확인한다. 대응책이 ARP 매핑 위조를 막거나 도청 피해를 줄이면 적절하고, 다른 네트워크 경계만 통제하면 부적절하다고 판단한다.

### 암기 포인트

ARP 스푸핑은 같은 LAN의 IP-MAC 속임수이고, 대응은 정적 ARP·ARP 검사·암호화·스니퍼 탐지이며 라우터의 LAN 간 필터는 핵심 대책이 아니다.

NoteBase

**문 6. 커버로스(Kerberos) 버전 4에 대한 설명으로 옳지 않은 것은?**

① 커버로스는 클라이언트와 응용서버 간의 상호 인증을 중재하는 제3자 인증 서비스를 제공한다.

② 커버로스 서버는 AS(Authentication Server)와 TGS(Ticket Granting Server)로 구성된다.

③ TGS가 발급하는 티켓은 응용서버의 공개키로 암호화된다.

④ 한번 인증을 받은 클라이언트는 TGS에 여러 차례 접속할 수 있고 여러 응용서버에 접속할 때 사용할 티켓들을 획득할 수 있다.

**정답 3번**

**출제 포인트**

이 문제는 Kerberos 버전 4의 기본 구조와 티켓 암호화 방식이 대칭키 기반이라는 점을 정확히 구별하는지를 묻는 문제이다.

**핵심 개념**

Kerberos는 신뢰된 제3자가 클라이언트와 서버의 인증을 중개하는 대칭키 기반 인증 시스템이다.
AS는 처음 로그인한 사용자를 인증하고 TGS를 이용할 수 있는 티켓을 준다.
TGS는 각 응용서버에 접근할 서비스 티켓을 발급하며, 이 티켓은 해당 응용서버만 해독할 수 있도록 그 서버의 비밀키로 암호화된다.

**선지별 해설**

① O: Kerberos는 클라이언트와 응용서버가 직접 비밀번호를 주고받지 않고, 신뢰된 제3자 인증 서버를 통해 상호 인증을 수행하게 하는 구조이므로 옳다.
② O: Kerberos의 핵심 구성은 사용자를 처음 인증하는 AS와 서비스 티켓을 발급하는 TGS이므로 옳다.
③ X: 틀린 부분은 '응용서버의 공개키'이다. Kerberos 버전 4는 공개키 기반 체계가 아니라 대칭키 기반 체계이므로, TGS가 발급하는 서비스 티켓은 응용서버의 공개키가 아니라 응용서버의 비밀키로 암호화된다.
④ O: 클라이언트는 한 번 AS에서 인증을 받고 TGT를 얻은 뒤, TGS에 여러 번 요청하여 여러 응용서버용 티켓을 받을 수 있으므로 옳다.

**오답 포인트**

③은 '티켓'이라는 말 때문에 공개키 인증서와 혼동하면 틀리기 쉽다. Kerberos 버전 4의 본질은 공개키가 아니라 비밀키를 공유한 대칭키 인증이라는 점이 함정이다.

**다시 나오면 이렇게 판단**

Kerberos 관련 선지를 보면 먼저 AS와 TGS의 역할을 나누고, 티켓 암호화가 공개키 방식인지 대칭키 방식인지를 확인하면 정답을 빠르게 가를 수 있다. '공개키'가 보이면 우선 의심할 수 있다.

NoteBase

**암기 포인트**

Kerberos V4는 AS로 처음 인증하고, TGS로 서비스 티켓을 받으며, 티켓 암호화는 공개키가 아니라 비밀키 기반이다.

NoteBase

**문 7. IPSec 프로토콜과 이를 이용한 두 가지 운용 모드에 대한 설명으로 옳지 않은 것은?**

① AH(Authentication Header) 프로토콜은 발신지 호스트를 인증하고 IP 패킷의 페이로드의 무결성을 제공한다.

② 전송 모드에서 IPSec은 본래의 IPv4 패킷 헤더를 암호화하지 않는다.

③ ESP(Encapsulating Security Payload) 프로토콜은 발신지 인증과 페이로드의 무결성 및 기밀성을 제공한다.

④ 터널 모드는 송신자와 수신자가 모두 호스트인 경우에 사용되어 네트워크 전 구간에서 전체 IP 패킷을 암호화한다.

**정답 4번**

**출제 포인트**

이 문제는 IPSec의 AH와 ESP의 기능, 그리고 전송 모드와 터널 모드의 적용 대상을 구별하는지를 묻는 문제이다.

**핵심 개념**

AH는 인증 헤더로서 데이터 원본 인증과 무결성을 제공하고 기밀성은 제공하지 않는다.
ESP는 캡슐화 보안 페이로드로서 기밀성을 중심으로 하며, 설정에 따라 데이터 원본 인증과 무결성도 제공할 수 있다.
전송 모드는 원래 IP 헤더를 유지한 채 payload를 보호하고, 터널 모드는 원래 IP 패킷 전체를 새 IP 헤더로 감싸 전달한다.

**선지별 해설**

① O: AH는 송신지 인증과 무결성을 제공하는 프로토콜이다. 기밀성은 제공하지 않지만 IP 패킷의 payload 무결성을 보장한다는 취지는 맞으므로 옳다.
② O: 전송 모드에서는 원래 IPv4 헤더를 그대로 두고 상위 계층 payload만 보호한다. 따라서 본래의 IP 헤더 자체는 암호화하지 않으므로 옳다.
③ O: ESP는 payload의 기밀성을 제공하는 것이 핵심이며, 필요하면 데이터 원본 인증과 무결성도 함께 제공할 수 있다. 선지는 ESP의 대표 기능을 올바르게 설명하므로 옳다.
④ X: 틀린 부분은 '송신자와 수신자가 모두 호스트인 경우에 사용되어'이다. 송신자와 수신자가 모두 종단 호스트인 경우에는 전송 모드를 사용하는 것이 일반적이다. 터널 모드는 보안 게이트웨이 간 또는 호스트와 게이트웨이 간 통신에서 원래 IP 패킷 전체를 새 IP 헤더로 캡슐화하여 전달하는 방식이다.

NoteBase

### 오답 포인트

전송 모드와 터널 모드는 둘 다 IPSec이라는 이유로 쉽게 섞인다. 특히 '전체 IP 패킷 보호'라는 표현만 보고 ④를 맞는 설명으로 오인하기 쉽지만, 출제자는 여기에 '양 끝이 모두 호스트'라는 조건을 붙여 전송 모드와 터널 모드를 뒤바꾸었다.

### 다시 나오면 이렇게 판단

먼저 AH와 ESP를 기능으로 나눈다. AH는 인증·무결성, ESP는 암호화 중심으로 본다. 다음으로 원래 IP 헤더가 그대로 보이면 전송 모드, 원래 IP 패킷 전체가 새 IP 헤더 안으로 들어가면 터널 모드로 판단한다.

### 암기 포인트

AH는 인증·무결성, ESP는 암호화 중심, 전송 모드는 헤더 유지, 터널 모드는 패킷 전체 캡슐화이다.

NoteBase

**문 8. ElGamal 공개키 암호 방식의 기본 원리인 이산 대수(discrete logarithm) 문제를 바르게 설명한 것은? (단, $p$, $q$는 소수, $a$는 $p$의 원시원소이고, $\phi()$는 Euler's totient 함수이다)**

① $a$, $p$, $y$가 주어졌을 때, y = a^x p를 만족하는 $x$를 구하는 문제

② $a$, $p$, $x$, $Y$가 주어졌을 때, Y = a^y p를 만족하는 a^xy p를 구하는 문제

③ $n$이 주어졌을 때, $n = pq$를 만족하는 $\phi(n)$을 구하는 문제

④ $n$과 $\phi(n)$과 서로소인 $e$가 주어졌을 때, $n = pq$이면서 ed ϕ(n) = 1을 만족하는 $d$를 구하는 문제

**정답 1번**

**출제 포인트**

이 문제는 이산대수 문제와 Diffie-Hellman 계열 계산 문제, $\phi(n)$ 계산, RSA 개인키 계산을 구별하는 문제이다.

**핵심 개념**

이산대수 문제는 $a$, $p$, $y$가 주어졌을 때 y ≡ a^x ±od p를 만족하는 지수 $x$를 역으로 찾는 문제이다.
Diffie-Hellman 계열 계산 문제는 보통 $a^x$와 $a^y$로부터 a^xy p를 구하는 문제이다.
RSA에서 ed ≡ 1 ±odϕ(n)를 만족하는 $d$를 구하는 것은 공개지수 $e$의 모듈러 역원을 구하는 문제이다.

NoteBase

### 선지별 해설

① O
이산대수 문제의 정의를 그대로 적은 선지이다. 밑 $a$, 법 $p$, 결과값 $y$가 주어졌을 때 지수 $x$를 찾는 역문제가 핵심이다.

② X
틀린 부분은 $a, p, x, Y$가 주어졌을 때 a^xy p를 구하는 문제라고 본 점이다. 이는 이산대수 문제의 설명이 아니고, 형태상으로는 Diffie-Hellman 공유값 계산에 가까우며 $x$가 주어지면 Y^x p로 계산할 수 있다. 올바르게는 이산대수 문제는 y = a^x p에서 미지수 $x$를 구하는 문제이다.

③ X
틀린 부분은 $n = pq$를 만족하는 $\phi(n)$을 구하는 문제라고 본 점이다. 이는 오일러 피 함수 계산 또는 소인수분해와 관련된 문제이지 이산대수 문제가 아니다. 올바르게는 $n = pq$이면 $\phi(n) = (p-1)(q-1)$이고, 이것은 지수 $x$를 역으로 찾는 문제와 다르다.

④ X
틀린 부분은 ed ≡ 1 ±odϕ(n)를 만족하는 $d$를 구하는 문제라고 본 점이다. 이는 RSA에서 개인키 지수 $d$를 구하는 모듈러 역원 계산이다. 올바르게는 이산대수 문제는 RSA 역원 계산이 아니라 y = a^x p에서 $x$를 찾는 문제이다.

### 오답 포인트

출제자는 이산대수의 핵심이 지수를 역으로 찾는 것이라는 점을 흐리고, ②처럼 $a^{xy}$ 계산을 제시해 Diffie-Hellman과 혼동하게 만든다. ③과 ④는 각각 소인수분해·오일러 피 함수 계산, RSA 역원 계산을 섞어 공개키 암호 전반을 한 덩어리로 외운 수험생을 노린 선지이다.

### 다시 나오면 이렇게 판단

결과값이 주어지고 숨은 지수 $x$를 찾으면 이산대수 문제이다. $a^{xy}$ 같은 공유값을 계산하면 Diffie-Hellman 계열 문제이고, $\phi(n)$이나 $d$를 구하면 RSA 또는 소인수분해 계열 문제로 구분하면 된다.

### 암기 포인트

이산대수는 값을 계산하는 문제가 아니라 지수를 역으로 찾는 문제이다.

NoteBase

**문 9. 「개인정보 보호법」상 개인정보처리자는 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호책임자를 지정하도록 명시하고 있다. 개인정보 보호책임자의 업무에 해당하지 않는 것은?**

① 개인정보 처리방침의 수립 및 공개

② 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선

③ 개인정보 유출 및 오용 · 남용 방지를 위한 내부통제시스템의 구축

④ 개인정보 보호 교육 계획의 수립 및 시행

**정답 1번**

### 쟁점

이 문제는 개인정보 보호책임자의 법정 업무를 정확히 구별하는 문제이다.
핵심은 개인정보 보호 계획과 개인정보 처리방침을 혼동하지 않는 것이다.

### 용어 풀이

개인정보 보호책임자 = 기관이나 사업자의 개인정보 처리 전반을 총괄해서 책임지는 사람이다.
개인정보 처리방침 = 개인정보처리자가 정보주체에게 공개하는 개인정보 처리 기준과 절차에 관한 문서이다.

### 핵심 구분

당시 법상 개인정보 보호책임자의 업무는 개인정보 보호 계획의 수립 및 시행, 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선, 불만 처리 및 피해 구제, 내부통제시스템 구축, 개인정보 보호 교육 계획의 수립 및 시행, 개인정보파일의 보호 및 관리·감독 등이다.
처리방침의 수립·공개와 보호책임자의 법정 업무 목록은 구별해야 한다. 보기 ①은 '보호 계획'을 '처리방침'으로 바꾸어 놓은 것이므로 틀리다.

NoteBase

**선지별 해설**

① X
- 개인정보 보호책임자의 법정 업무는 '개인정보 보호 계획의 수립 및 시행'이다. 보기처럼 '개인정보 처리방침의 수립 및 공개'라고 적으면 업무 명칭이 달라지므로 틀리다.
- 틀린 표현: 개인정보 처리방침의 수립 및 공개
- 올바른 표현: 개인정보 보호 계획의 수립 및 시행

② O
- 개인정보 처리 실태 및 관행을 정기적으로 조사하고 개선하는 것은 개인정보 보호책임자의 업무에 해당한다. 실제 운영 상태를 점검하고 미비점을 고치는 기능이다.

③ O
- 개인정보 유출과 오용·남용을 막기 위한 내부통제시스템의 구축은 개인정보 보호책임자의 핵심 업무에 해당한다. 기술적·관리적 통제체계를 갖추는 취지이다.

④ O
- 개인정보 보호 교육 계획의 수립 및 시행도 개인정보 보호책임자의 업무에 해당한다. 임직원 교육은 개인정보 침해 예방의 기본 수단이다.

**오답 포인트**

①의 '처리방침'이라는 표현이 익숙해서 쉽게 맞는 문장처럼 보인다는 점이 함정이다. 이 문제는 개인정보처리자의 일반 의무와 개인정보 보호책임자의 법정 업무를 섞어서 물었다.

**다시 나오면 이렇게 판단**

개인정보 보호책임자 문제는 업무 목록을 먼저 떠올린 뒤 보기의 핵심 명사를 대조하면 된다. '보호 계획'인지 '처리방침'인지처럼 한 단어만 바꿔 놓은 선지를 우선 의심하면 빠르게 정리된다.

**암기 포인트**

보호책임자 업무는 처리방침이 아니라 보호 계획에서 시작한다.

NoteBase

**문 10. 사전에 A와 B가 공유하는 비밀키가 존재하지 않을 때, A가 B에게 전달할 메시지 M의 기밀성을 제공할 목적으로 공개키와 대칭키 암호화 기법을 모두 활용하여 암호화한 전송 메시지를 아래의 표기 기호를 사용하여 바르게 표현한 것은?**

$PU_X$: X의 공개키
$PR_X$: X의 개인키
$K_{AB}$: A에 의해 임의 생성된 A와 B 간의 공유 비밀키
$E(k, m)$: 메시지 $m$을 암호키 $k$로 암호화하는 함수
||: 두 메시지의 연결

① $E(K_{AB}, M) \,||\, E(PU_A, K_{AB})$
② $E(PR_A, (E(K_{AB}, M)||K_{AB}))$
③ $E(K_{AB}, M) \,||\, E(PR_A, K_{AB})$
④ $E(K_{AB}, M) \,||\, E(PU_B, K_{AB})$

**정답 4번**

**출제 포인트**

이 문제는 공개키 암호와 대칭키 암호를 함께 쓰는 하이브리드 암호화에서 메시지와 세션키를 각각 어떤 키로 암호화해야 기밀성이 성립하는지를 묻는 문제이다.

**핵심 개념**

대칭키 암호는 송수신자가 같은 비밀키로 데이터를 빠르게 암호화하는 방식이다.
공개키 암호는 수신자의 공개키로 암호화하고 수신자의 개인키로 복호화하는 방식이므로, 세션키 전달에 적합하다.
이 문제의 핵심은 메시지 $M$은 임시 대칭키 $K_{AB}$로 암호화하고, 그 $K_{AB}$ 자체는 B만 풀 수 있도록 $PU_B$로 암호화해야 한다는 점이다.

NoteBase

### 선지별 해설

① X
- $E(K_{AB}, M)$까지는 맞지만, $E(PU_A, K_{AB})$가 틀렸다.
- $PU_A$로 암호화한 값은 A의 개인키 $PR_A$로 풀어야 하므로 B가 세션키를 복호화할 수 없다.
- 틀린 표현은 $E(PU_A, K_{AB})$이다. 올바르게는 $E(PU_B, K_{AB})$이어야 한다.

② X
- $PR_A$로 $(E(K_{AB}, M)||K_{AB})$를 암호화하는 것은 기밀성 제공 방식이 아니다.
- 개인키로 처리한 값은 대응 공개키 $PU_A$로 확인하거나 풀 수 있으므로, A의 공개키를 아는 누구나 $K_{AB}$를 얻을 수 있어 B에게만 비밀이 보장되지 않는다.
- 틀린 표현은 $E(PR_A, (E(K_{AB}, M)||K_{AB}))$이다. 올바르게는 메시지는 $E(K_{AB}, M)$, 세션키는 $E(PU_B, K_{AB})$처럼 분리해 암호화해야 한다.

③ X
- 메시지를 $K_{AB}$로 암호화한 부분은 맞지만, 세션키를 $PR_A$로 암호화한 부분이 틀렸다.
- $PR_A$로 암호화한 $K_{AB}$는 $PU_A$로 확인 가능하므로 세션키의 기밀성이 없다.
- 틀린 표현은 $E(PR_A, K_{AB})$이다. 올바르게는 $E(PU_B, K_{AB})$이다.

④ O
- 메시지 $M$을 대칭키 $K_{AB}$로 암호화한 $E(K_{AB}, M)$는 효율적이다.
- 세션키 $K_{AB}$를 B의 공개키 $PU_B$로 암호화한 $E(PU_B, K_{AB})$는 B의 개인키 $PR_B$로만 복호화할 수 있으므로 기밀성이 성립한다.
- 따라서 하이브리드 암호화의 올바른 표현이다.

### 오답 포인트

공개키 암호에서 누구의 공개키를 써야 하는지와 개인키 암호화의 의미를 혼동하면 틀리기 쉽다. ①은 공개키를 쓰기는 했지만 수신자인 B가 아니라 송신자인 A의 공개키를 썼고, ②와 ③은 개인키를 기밀성 수단처럼 써서 전자서명과 비슷한 방향으로 뒤집힌 선택지이다.

### 다시 나오면 이렇게 판단

기밀성만 묻는 하이브리드 암호화 문제이면 먼저 본문은 대칭키로 암호화한다고 본다. 그다음 그 대칭키를 누가 반드시 풀어야 하는지를 보고, 그 사람의 공개키로 세션키를 암호화했는지 확인하면 된다.

### 암기 포인트

본문은 세션키로, 세션키는 수신자 공개키로 보낸다.

NoteBase

**문 11. 인가된 사용자가 조직의 정보자산에 적시에 접근하여 업무를 수행할 수 있도록 유지하는 것을 목표로 하는 정보 보호 요소는?**

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

**정답 3번**

### 출제 포인트

이 문제는 정보보호의 기본 요소인 기밀성, 무결성, 가용성, 인증성의 의미를 구별하는 문제이다.

### 핵심 개념

기밀성은 비인가자에게 정보가 노출되지 않도록 보호하는 성질이다.
무결성은 정보가 인가되지 않은 변경 없이 정확하고 완전하게 유지되는 성질이다.
가용성은 인가된 사용자가 필요할 때 정보자산과 서비스에 지체 없이 접근해 사용할 수 있는 성질이다.
인증성은 접근 주체의 신원을 확인하는 기능으로, 가용성처럼 접근 가능 상태를 유지하는 개념은 아니다.

### 선지별 해설

① X: 기밀성은 정보의 비밀 유지가 핵심이므로 비인가자의 열람이나 유출을 막는 개념이다. 틀린 표현은 '즉시에 접근하여 업무를 수행'이다. 올바르게는 '비인가자가 정보에 접근하지 못하도록 보호하는 것'이다.
② X: 무결성은 정보가 임의로 변조·훼손되지 않고 정확성과 완전성을 유지하는 개념이다. 틀린 표현은 '인가된 사용자가 즉시에 접근'이다. 올바르게는 '정보가 정확하고 완전한 상태로 유지되는 것'이다.
③ O: 가용성은 인가된 사용자가 필요 시 정보자산에 즉시 접근하여 업무를 계속 수행할 수 있도록 보장하는 개념이므로 발문과 정확히 일치한다.
④ X: 인증성은 사용자가 주장하는 신원이 맞는지 확인하는 기능이다. 틀린 표현은 '즉시에 접근하여 업무를 수행할 수 있도록 유지'이다. 올바르게는 '접근 주체의 신원을 확인하는 것'이다.

### 오답 포인트

발문에 '인가된 사용자'가 들어 있어 인증성을 먼저 떠올리기 쉽지만, 핵심은 신원 확인이 아니라 업무를 계속할 수 있도록 자산에 접근 가능한 상태를 유지하는 데 있다. '누가 맞는 사람인가'를 묻으면 인증성이고, '필요할 때 바로 쓸 수 있는가'를 묻으면 가용성이다.

NoteBase

### 다시 나오면 이렇게 판단

발문의 중심 동사를 먼저 본다. 비밀 유지이면 기밀성, 변조 방지이면 무결성, 필요 시 접근과 사용 보장이면 가용성, 사용자 확인이면 인증성으로 판단된다.

### 암기 포인트

기밀성은 숨김, 무결성은 그대로, 가용성은 바로 사용, 인증성은 신원 확인이다.

NoteBase

**문 12. 발신지 IP 주소가 공격대상의 IP 주소로 위조된 ICMP 패킷을 특정 브로드캐스트 주소로 보내어 공격대상이 다량의 ICMP reply 패킷을 받도록 하는 공격기법은?**

① SYN flooding

② Smurf attack

③ Land attack

④ Teardrop

**정답 2번**

**출제 포인트**

이 문제는 ICMP 기반 반사형 서비스 거부 공격인 Smurf attack과 다른 고전적 네트워크 공격 기법을 구별하는 문제이다.

**핵심 개념**

Smurf attack: 출발지 IP를 피해자 IP로 위조한 ICMP Echo Request를 브로드캐스트 주소로 보내, 다수 호스트의 Echo Reply가 피해자에게 몰리게 하는 반사형 DoS 공격이다.
SYN flooding: TCP 3-way handshake의 반개방 연결을 대량으로 만들어 서버의 연결 대기 큐를 고갈시키는 공격이다.
Land attack: 출발지와 목적지의 IP 주소와 포트 번호를 동일하게 조작한 비정상 패킷으로 시스템 혼란을 유발하는 공격이다.
Teardrop: 겹치거나 비정상적인 단편화 오프셋을 가진 IP 조각을 보내 재조립 과정의 오류를 유발하는 공격이다.

**선지별 해설**

① X: SYN flooding은 TCP SYN을 대량 전송해 반개방 연결을 쌓는 공격이다. 틀린 표현은 이를 브로드캐스트 ICMP 반사 공격으로 보는 점이다. 올바르게는 서버의 연결 대기 큐를 고갈시키는 TCP 기반 DoS이다.
② O: Smurf attack은 발신지 IP를 피해자 IP로 위조한 ICMP Echo Request를 브로드캐스트 주소로 보내 다수 호스트의 Echo Reply를 피해자에게 집중시키는 공격이다. 문제의 설명과 정확히 일치한다.
③ X: Land attack은 출발지와 목적지 IP 주소를 동일하게 만든 비정상 패킷을 대상에게 보내는 공격이다. 틀린 표현은 브로드캐스트를 이용해 다수의 ICMP Reply를 유발한다는 점이다. 올바르게는 자기 자신에게서 온 것처럼 보이는 패킷으로 시스템 오류를 노리는 공격이다.
④ X: Teardrop은 조작된 IP 단편 조각을 보내 재조립 오류를 일으키는 공격이다. 틀린 표현은 이를 ICMP Echo Reply 증폭 공격으로 보는 점이다. 올바르게는 IP fragmentation 취약점을 노리는 공격이다.

NoteBase

### 오답 포인트

발신지 IP 위조라는 말만 보고 Land attack으로 오인하기 쉽지만, 결정적 단서는 브로드캐스트 주소와 다량의 ICMP Reply이다. 이 두 표현이 함께 나오면 반사형 ICMP 증폭 공격을 먼저 떠올리게 된다.

### 다시 나오면 이렇게 판단

피해자 IP로 위조한 뒤 브로드캐스트에 뿌려 여러 호스트의 응답을 피해자에게 몰아주면 Smurf attack이다. TCP SYN으로 연결 대기 큐를 고갈시키면 SYN flooding이고, 출발지와 목적지가 같으면 Land attack이며, 단편 조작으로 재조립 오류를 노리면 Teardrop이다.

### 암기 포인트

Smurf는 브로드캐스트 ICMP에 여러 호스트가 한꺼번에 응답해 피해자에게 몰리는 반사형 DoS 공격으로 기억해 둔다.

NoteBase

**문 13. 중간자(man-in-the-middle) 공격에 대한 설명으로 옳은 것은?**

① Diffie-Hellman 키 교환 프로토콜은 중간자 공격에 대비하도록 설계된 것이다.

② 공격대상이 신뢰하고 있는 시스템을 불능상태로 만들고 공격자가 신뢰시스템인 것처럼 동작한다.

③ 공격자가 송 · 수신자 사이에 개입하여 송신자가 보낸 정보를 가로채고, 조작된 정보를 정상적인 송신자가 보낸 것처럼 수신자에게 전달한다.

④ 여러 시스템으로부터 한 시스템에 집중적으로 많은 접속 요청이 발생하여, 해당 시스템이 정상적인 동작을 못하게 된다.

**정답 3번**

**출제 포인트**

이 문제는 중간자 공격의 정의와 이를 다른 공격 유형과 구별하는 핵심 특징을 묻는 문제이다.

**핵심 개념**

중간자 공격은 공격자가 송신자와 수신자 사이에 끼어들어 통신 내용을 가로채고, 양쪽에는 정상 통신처럼 보이게 하면서 내용을 중계하거나 변조하는 공격이다.
Diffie-Hellman 키 교환은 인증 절차가 없으면 중간자 공격에 취약하다.
서비스 거부 공격은 대량 요청으로 시스템을 마비시키는 공격이고, 스푸핑이나 가장은 신뢰된 상대인 것처럼 속여 접근하는 공격이다.

NoteBase

### 선지별 해설

① X
Diffie-Hellman 키 교환 자체는 상대방 인증 기능이 없어서 중간자 공격을 막도록 설계된 것이 아니다.
틀린 표현은 "중간자 공격에 대비하도록 설계된 것"이다. 올바르게는 "인증이 없는 Diffie-Hellman은 중간자 공격에 취약하므로 전자서명이나 인증서 같은 인증 수단이 함께 필요하다"이다.

② X
이 선지는 공격대상이 신뢰하는 시스템을 쓰지 못하게 만들고 공격자가 그 시스템인 것처럼 가장하는 상황을 설명한다. 핵심은 송신자와 수신자 사이에서 통신을 중계하는 것이 아니라 신뢰 주체를 사칭하는 데 있다.
틀린 표현은 "공격자가 신뢰시스템인 것처럼 동작한다"를 중간자 공격 설명으로 본 점이다. 올바르게는 "이는 스푸핑, 가장, 또는 신뢰 관계 악용 공격에 가까운 설명이다"이다.

③ O
공격자가 송신자와 수신자 사이에 개입하여 정보를 가로채고, 조작한 뒤에도 정상 송신자가 보낸 것처럼 수신자에게 전달하는 것이 중간자 공격의 전형적인 형태이다. 중간 개입, 가로채기, 위장 전달이 모두 들어 있어 정확하다.

④ X
여러 시스템이 한 시스템에 과도한 요청을 보내 정상 동작을 못 하게 만드는 것은 분산 서비스 거부 공격의 설명이다.
틀린 표현은 "한 시스템에 집중적으로 많은 접속 요청이 발생하여"를 중간자 공격 설명으로 본 점이다.
올바르게는 "이는 DDoS 공격 설명이며, 중간자 공격은 통신 경로에 끼어들어 내용을 중계하거나 변조하는 공격이다"이다.

### 오답 포인트

중간자 공격은 '사이에 끼어든다'는 위치 개념이 핵심인데, ②처럼 신뢰 대상을 사칭하는 공격이나 ④처럼 시스템을 마비시키는 공격과 섞어서 보면 오답이 된다. ①도 암호 프로토콜 이름이 나오면 안전하다고 오해하기 쉬우나, 인증 없는 키 교환은 중간자 공격을 막지 못한다.

### 다시 나오면 이렇게 판단

선지를 볼 때 먼저 공격자가 통신 당사자 둘 사이에 들어가 내용을 가로채고 다시 전달하는지 확인하면 된다. 사이 개입과 중계·변조가 보이면 중간자 공격이고, 사칭만 하면 스푸핑 계열이며, 대량 요청으로 마비시키면 서비스 거부 공격이다.

NoteBase

**암기 포인트**

중간자 공격은 사이 개입·가로채기·재전달이고, DDoS는 대량 요청 마비이며, 인증 없는 Diffie-Hellman은 중간자 공격에 취약하다.

NoteBase

**문 14. 다중수준 보안(multi-level security) 시스템을 대상으로 다음 사항을 준수하는 보안 모델은?**

◯ 주체는 자신과 같거나 자신보다 낮은 보안 수준의 객체만 읽을 수 있음(no read up)
◯ 주체는 자신과 같거나 자신보다 높은 보안 수준의 객체에만 쓸 수 있음(no write down)

① 벨라파둘라(Bell-Lapadula)
② 비바(Biba)
③ 클락윌슨(Clark-Wilson)
④ 중국인벽(Chinese wall)

**정답 1번**

**출제 포인트**

이 문제는 다중수준 보안 시스템에서 기밀성을 보장하는 Bell-LaPadula 모델과 무결성을 보장하는 다른 모델들의 차이를 묻는 문제이다.

**핵심 개념**

Bell-LaPadula는 기밀성 중심 모델로서 상위 등급 정보를 하위 등급으로 새게 하지 않도록 no read up, no write down 규칙을 둔다.
Biba는 무결성 중심 모델로서 낮은 무결성 정보가 높은 무결성 주체를 오염시키지 않도록 no read down, no write up 규칙을 둔다.
Clark-Wilson은 상업 환경의 무결성 모델로서 잘 형성된 트랜잭션과 직무 분리를 통해 데이터의 일관성을 보호한다.
Chinese Wall은 이해상충 방지 모델로서 같은 충돌 집합 내 다른 회사 정보에 대한 접근을 제한한다.

NoteBase

**선지별 해설**

① O
Bell-LaPadula 모델은 다중수준 보안에서 기밀성을 보호하는 대표 모델이다. 제시문처럼 주체는 자신과 같거나 더 낮은 보안 수준의 객체만 읽을 수 있고(no read up), 자신과 같거나 더 높은 보안 수준의 객체에만 쓸 수 있다(no write down).

② X
틀린 부분은 비바를 정답 모델로 보는 판단이다. Biba는 기밀성이 아니라 무결성을 보호하는 모델이다. 올바르게는 제시된 no read up, no write down 규칙을 만족하는 모델은 Bell-LaPadula이다.

③ X
틀린 부분은 클락윌슨을 다중수준 기밀성 모델로 보는 판단이다. Clark-Wilson은 무결성 보장을 위해 인증 절차, 잘 형성된 트랜잭션, 직무 분리를 강조하는 모델이다. 올바르게는 다중수준 기밀성 규칙을 직접 설명하는 모델은 Bell-LaPadula이다.

④ X
틀린 부분은 중국인벽을 다중수준 기밀성 모델로 보는 판단이다. Chinese Wall은 이해상충 방지를 위한 접근통제 모델로서 동일 충돌 집합 내 다른 기업 정보 접근을 막는다. 올바르게는 no read up, no write down 규칙을 갖는 모델은 Bell-LaPadula이다.

**오답 포인트**

Bell-LaPadula와 Biba는 규칙 문구가 서로 반대로 출제되어 자주 혼동된다. 이 문항은 제시문에 no read up, no write down이 직접 주어졌는데도 Biba를 떠올리면 기밀성과 무결성의 방향을 뒤집어 오답이 된다.

**다시 나오면 이렇게 판단**

문장에 no read up, no write down이 보이면 기밀성 중심의 Bell-LaPadula로 판단한다. 반대로 no read down, no write up이 보이면 무결성 중심의 Biba로 판단한다. Clark-Wilson은 트랜잭션과 직무 분리, Chinese Wall은 이해상충 방지라는 키워드로 구분된다.

**암기 포인트**

Bell-LaPadula는 기밀성, Biba는 무결성, Clark-Wilson은 상업적 무결성, Chinese Wall은 이해상충 방지이다.

NoteBase

**문 15. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 근거하여 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계를 수립·운영하고 있는 자에 대하여 일정 기준에 적합한지에 관하여 인증하는 것은?**

① CC 인증

② ITSEC 인증

③ PIMS 인증

④ ISMS 인증

**정답 4번**

**쟁점**

이 문제는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상 정보보호 관리체계 인증이 무엇인지를 묻는 문제이다.
핵심은 조직의 종합적 정보보호 관리체계를 인증하는 제도와 정보보호제품 또는 개인정보보호 중심 제도를 구별하는 데 있다.

**용어 풀이**

정보보호 관리체계(ISMS)는 정보통신망의 안정성과 신뢰성 확보를 위해 조직이 수립·운영하는 종합적 정보보호 관리체계이다.
개인정보보호 관리체계(PIMS)는 개인정보의 수집·이용·보관·파기 등 개인정보보호 활동이 적정한지를 보는 관리체계이다.

**핵심 구분**

원칙적으로 ISMS는 조직 차원의 정보보호 관리체계 인증이다. 반면 PIMS는 개인정보보호 관리체계 인증이다.
또한 CC와 ITSEC은 정보보호제품 또는 IT 보안성 평가 기준에 관한 범주이므로, 법문에 나온 종합적 관리체계 인증과는 성격이 다르다.

NoteBase

### 선지별 해설

① X
CC 인증은 공통평가기준에 따른 정보보호제품의 보안기능 적합성 평가에 관한 인증이다. 조직이 수립·운영하는 종합적 관리체계 인증이 아니다.
틀린 표현: CC 인증을 법문상의 종합적 관리체계 인증으로 본 부분이다.
올바른 표현: CC 인증은 정보보호제품의 보안기능을 평가하는 인증이다.

② X
ITSEC은 IT 보안 평가 기준 또는 그에 따른 평가 체계에 관한 개념이다. 정보통신망법상 정보보호 관리체계 인증과는 대상이 다르다.
틀린 표현: ITSEC 인증을 조직의 정보보호 관리체계 인증으로 본 부분이다.
올바른 표현: ITSEC은 관리체계 인증이 아니라 IT 보안성 평가 기준의 범주이다.

③ X
PIMS 인증은 개인정보보호 관리체계 인증이므로 개인정보 처리 전 과정의 보호체계 적정성을 본다. 발문처럼 정보통신망의 안정성·신뢰성 확보를 위한 정보보호 관리체계 인증 자체를 가리키는 말은 아니다.
틀린 표현: PIMS 인증을 정보보호 관리체계 인증과 동일하게 본 부분이다.
올바른 표현: PIMS는 개인정보보호 관리체계 인증이다.

④ O
ISMS 인증은 정보통신망의 안정성·신뢰성 확보를 위해 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계를 수립·운영하는 자가 기준에 적합한지를 인증하는 제도이므로 발문과 정확히 일치한다.

### 오답 포인트

이 문제를 틀렸다면 관리체계 인증과 제품 평가 인증을 섞었을 가능성이 높다. 특히 PIMS와 ISMS는 둘 다 관리체계라는 말이 들어가지만, PIMS는 개인정보보호 중심이고 ISMS는 정보통신망의 정보보호 관리체계라는 점이 구별점이다.

### 다시 나오면 이렇게 판단

발문에 정보통신망의 안정성·신뢰성, 관리적·기술적·물리적 보호조치, 종합적 관리체계라는 문구가 나오면 먼저 조직 차원의 정보보호 관리체계 인증인지 본다. 개인정보 처리 단계가 중심이면 PIMS 계열이고, 제품의 보안기능 평가가 중심이면 CC 계열로 판단한다.

### 암기 포인트

ISMS는 조직의 정보보호 관리체계, PIMS는 개인정보보호 관리체계, CC·ITSEC은 제품·시스템 보안성 평가 범주이다.

NoteBase

**문 16. 버퍼 오버플로우 공격의 대응수단으로 적절하지 않은 것은?**

① 스택상에 있는 공격자의 코드가 실행되지 못하도록 한다.

② 프로세스 주소 공간에 있는 중요 데이터 구조의 위치가 변경되지 않도록 적재 주소를 고정시킨다.

③ 함수의 진입(entry)과 종료(exit) 코드를 조사하고 함수의 스택 프레임에 대해 손상이 있는지를 검사한다.

④ 변수 타입과 그 타입에 허용되는 연산들에 대해 강력한 표기법을 제공하는 고급수준의 프로그래밍 언어를 사용한다.

**정답 2번**

**출제 포인트**

이 문제는 버퍼 오버플로우 대응기법의 핵심 원리와 각 기법이 실제로 무엇을 막는지를 구분하는 문제이다.

**핵심 개념**

실행 방지 기법은 스택이나 힙 같은 데이터 영역을 실행 불가로 두어 주입된 코드가 실행되지 못하게 하는 방법이다.
주소 공간 배치 난수화(ASLR)는 코드, 스택, 힙, 라이브러리의 적재 주소를 매 실행 시 달라지게 하여 공격자가 주소를 예측하지 못하게 하는 방법이다.
스택 보호 기법은 함수 진입 시 보호값을 두고 함수 종료 시 이를 검사하여 반환 주소나 스택 프레임 훼손을 탐지하는 방법이다.
메모리 안전성이 높은 언어는 타입과 경계 검사를 강하게 적용하여 버퍼 경계 초과 쓰기 위험을 줄이는 방법이다.

NoteBase

### 선지별 해설

① O
스택에 주입된 공격자 코드가 실행되지 못하게 하는 것은 NX, DEP 같은 실행 방지 기법의 핵심이다. 버퍼 오버플로우가 발생하더라도 데이터 영역을 실행 불가로 두면 코드 실행 단계가 차단된다.

② X
틀린 부분은 "적재 주소를 고정시킨다"이다.
버퍼 오버플로우 대응에서는 주소를 고정하는 것이 아니라 무작위화한다. 실제로는 ASLR을 적용하여 중요 데이터 구조와 코드의 위치가 실행 때마다 달라지게 만들어 공격자가 정확한 점프 주소를 예측하지 못하게 한다.

③ O
함수의 진입과 종료 부분에 보호 코드를 넣고 스택 프레임 손상 여부를 검사하는 것은 StackGuard, 스택 카나리 같은 보호 기법의 설명에 해당한다. 반환 주소가 덮어써졌는지 탐지하는 대표적 대응수단이다.

④ O
강한 타입 체계와 안전한 연산 모델을 제공하는 고급 언어를 사용하면 버퍼 경계 초과 쓰기 자체를 줄일 수 있다. 이는 버퍼 오버플로우 취약점을 예방하는 방향의 적절한 대응수단이다.

### 오답 포인트

②는 "위치가 변경되지 않도록"이라는 표현으로 안정성을 높이는 것처럼 보이게 만들지만, 실제 보안 효과는 반대이다. 버퍼 오버플로우 완화에서는 주소를 예측하기 어렵게 해야 하므로 고정 주소는 방어가 아니라 공격자 편의에 가깝다.

### 다시 나오면 이렇게 판단

버퍼 오버플로우 대응 선지는 무엇을 막는지로 나누면 빠르게 판단된다. 코드 실행을 막으면 실행 방지, 주소 예측을 어렵게 하면 ASLR, 반환 주소 훼손을 잡으면 스택 보호, 취약한 메모리 조작 자체를 줄이면 안전한 언어 사용이다. 반대로 주소를 고정한다는 표현이 나오면 ASLR의 반대이므로 오답으로 본다.

### 암기 포인트

DEP는 실행을 막고, ASLR은 주소를 섞고, 카나리는 훼손을 잡고, 안전 언어는 초과 쓰기를 줄인다.

NoteBase

**문 17. 네트워크상에서 교환되는 인증 정보에 대한 재전송 공격(replay attack)을 막기 위한 방법으로 적절하지 않은 것은?**

① 시도-응답(challenge-response) 인증 방식을 사용한다.

② 메시지에 사전에 동기화된 현재 시각에 해당하는 타임스탬프(timestamp)를 포함하여 전송한다.

③ 메시지에 송신자의 개인키로 서명한 전자서명(digital signature)을 포함하여 전송한다.

④ 메시지에 수신자로부터 받은 일회용 랜덤 값에 해당하는 nonce를 포함하여 전송한다.

**정답 3번**

**출제 포인트**

이 문제는 전자서명이 보장하는 무결성·송신자 인증과, 재전송 공격 방지에 필요한 신선성 보장의 차이를 묻는 문제이다.

**핵심 개념**

재전송 공격 방지: 과거에 가로챈 인증 메시지를 다시 보내도 유효하지 않게 만드는 것이다. 결정 차이축은 메시지의 진위가 아니라 신선성 여부이다. 키워드는 timestamp, nonce, challenge-response이다.
전자서명: 송신자의 개인키로 서명하여 무결성, 송신자 인증, 부인방지를 제공하는 것이다. 키워드는 변조 검출과 서명 검증이다.
challenge-response: 수신자가 그때그때 내는 임의값에 맞춰 응답하게 하여 이전 메시지의 재사용을 막는 방식이다. 키워드는 일회성 도전값이다.

NoteBase

### 선지별 해설

① O
시도-응답 인증은 수신자가 새로운 challenge를 보내고 송신자가 그 값에 맞는 응답을 돌려주므로, 과거 응답을 그대로 재전송해도 현재 challenge와 맞지 않아 거부된다.

② O
사전에 동기화된 시각을 바탕으로 timestamp를 포함하면 허용 시간 창을 벗어난 오래된 메시지를 걸러낼 수 있으므로 재전송 공격 방지에 적절하다.

③ X
틀린 부분은 전자서명만 포함하면 재전송 공격을 막을 수 있다는 취지이다.
전자서명은 메시지가 송신자에게서 왔고 중간에 변조되지 않았음을 보여 주지만, 예전에 정상적으로 서명된 메시지를 다시 보내는 것까지 막지는 못한다.
올바르게는 전자서명에 nonce, timestamp, sequence number 같은 신선성 정보를 함께 넣어야 재전송 공격 방지 수단이 된다.

④ O
수신자로부터 받은 일회용 랜덤 값인 nonce를 메시지에 포함하면 이번 세션에만 유효한 값이 되므로, 이전에 캡처한 메시지를 다시 보내도 nonce가 맞지 않아 거부된다.

### 오답 포인트

③은 전자서명의 기능을 재전송 방지까지 확대해서 착각하게 만드는 선지이다. 전자서명은 진위와 무결성을 보장하지만, 예전의 정상 메시지를 다시 보내는 공격은 별도의 신선성 정보가 없으면 그대로 통과할 수 있다.

### 다시 나오면 이렇게 판단

재전송 공격 문제는 먼저 그 기법이 과거 메시지의 재사용을 구별할 장치를 갖는지 본다. timestamp, nonce, challenge-response처럼 매번 달라지는 값이 있으면 방지 수단이고, 전자서명처럼 진위만 확인하고 신선성 정보가 없으면 단독으로는 부족하다.

### 암기 포인트

전자서명은 진위, nonce·timestamp는 신선성이다.

NoteBase

**문 18. AES(Advanced Encryption Standard) 알고리즘을 구성하는 변환 과정 중, 상태 배열의 열 단위의 행렬 곱셈과 같은 형태로 표현되는 것은?**

① 바이트 치환(substitute bytes)

② 행 이동(shift row)

③ 열 혼합(mix columns)

④ 라운드 키 더하기(add round key)

**정답 3번**

**출제 포인트**

이 문제는 AES의 네 가지 기본 변환 중 어떤 단계가 상태 배열의 각 열을 대상으로 GF(2^8)에서 고정 행렬과 곱하는 방식으로 동작하는지를 묻는 문제이다.

**핵심 개념**

SubBytes는 각 바이트를 S-Box로 독립적으로 치환하는 단계이다.
ShiftRows는 상태 배열의 각 행을 서로 다른 칸 수만큼 순환 이동시키는 단계이다.
MixColumns는 각 열을 하나의 벡터처럼 보고 고정 행렬과 곱해 열 내부 바이트들을 혼합하는 단계이다.
AddRoundKey는 상태 배열과 라운드 키를 바이트 단위 XOR로 결합하는 단계이다.

**선지별 해설**

① X: 바이트 치환은 각 바이트를 S-Box 값으로 바꾸는 비선형 치환 단계일 뿐, 열 단위 행렬 곱셈 형태가 아니다. 틀린 표현은 "열 단위의 행렬 곱셈"에 대응시킨 점이다. 올바르게는 "바이트별 S-Box 치환"이다.
② X: 행 이동은 각 행을 왼쪽으로 순환 시프트하는 단계이다. 행의 위치를 바꾸어 열 조합을 돕지만 행렬 곱셈은 수행하지 않는다. 올바르게는 "행 단위 순환 이동"이다.
③ O: 열 혼합은 상태 배열의 각 열을 입력 벡터로 두고 고정 계수 행렬을 곱해 새 열을 만든다. 문제의 "상태 배열의 열 단위의 행렬 곱셈과 같은 형태"에 정확히 해당한다.
④ X: 라운드 키 더하기는 상태 배열과 라운드 키를 XOR하는 단계이다. 키를 더한다는 이름이 붙지만 실제 연산은 행렬 곱셈이 아니라 비트 단위 배타적 논리합이다. 올바르게는 "상태와 라운드 키의 XOR 결합"이다.

**오답 포인트**

AES의 네 단계 이름은 모두 짧아서 기능이 섞여 보이기 쉽다. 특히 ② ShiftRows와 ③ MixColumns는 둘 다 "배열을 섞는 단계"처럼 보이므로, 이동인지 곱셈인지 연산 단위를 구분하지 않으면 혼동하기 쉽다.

NoteBase

### 다시 나오면 이렇게 판단

AES 단계 문제는 먼저 연산 단위를 본다. 바이트 하나를 바꾸면 SubBytes, 행을 밀면 ShiftRows, 열 전체를 고정 계수로 섞으면 MixColumns, 키와 XOR하면 AddRoundKey로 판단된다.

### 암기 포인트

AES는 바이트 치환, 행 이동, 열 혼합, 키 XOR의 순서로 구분되며, 행렬 곱셈 형태는 MixColumns이다.

NoteBase

**문 19. 「정보통신기반 보호법」상 정보통신기반시설과 관련된 사항으로 옳지 않은 것은?**

① 미래창조과학부장관과 국가정보원장등은 특정한 정보통신기반시설을 주요정보통신기반시설로 지정할 필요가 있다고 판단되는 경우에는 중앙행정기관의 장에게 해당 정보통신기반시설을 주요정보통신기반시설로 지정하도록 권고할 수 있다.

② 누구든지 주요정보통신기반시설의 운영을 방해할 목적으로 일시에 대량의 신호를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보처리에 오류를 발생하게 하는 행위를 하여서는 아니된다.

③ 관리기관의 장은 침해사고가 발생하여 소관 주요정보통신기반시설의 교란·마비 또는 파괴된 사실을 인지한 때에는 관계행정기관이나 수사기관에 그 사실을 통지할 수 있다.

④ 정부는 정보통신기반시설의 보호에 필요한 기술개발을 효율적으로 추진하기 위하여 필요한 때에는 정보보호 기술개발과 관련된 연구기관 및 민간단체로 하여금 이를 대행하게 할 수 있다.

**정답 3번**

### 쟁점

이 문제는 「정보통신기반 보호법」상 주요정보통신기반시설의 지정 권고, 운영방해 금지, 침해사고 통지, 기술개발 대행 규정을 구별하는 문제이다.
핵심은 임의규정인 "할 수 있다"와 의무규정인 "하여야 한다"를 정확히 나누는 데 있다.

### 용어 풀이

주요정보통신기반시설은 국가안전보장, 행정 기능, 국민생활에 중대한 영향을 줄 수 있어 법에 따라 지정된 정보통신기반시설이다.
침해사고의 통지는 이런 시설이 교란·마비·파괴된 사실을 인지했을 때 관계 기관에 알려 후속 대응이 이루어지게 하는 의무이다.

### 핵심 구분

지정 권고는 권한 규정이므로 "권고할 수 있다"로 표현된다. 반면 침해사고 통지는 대응을 위한 법정 의무이므로 "통지하여야 한다"로 표현된다.
즉 권고는 재량, 통지는 의무라는 점이 정답을 가른다.

NoteBase

### 선지별 해설

① O
미래창조과학부장관과 국가정보원장등은 특정한 정보통신기반시설을 주요정보통신기반시설로 지정할 필요가 있다고 판단하면 중앙행정기관의 장에게 지정하도록 권고할 수 있다. 지정 권고의 주체와 상대방을 묻는 전형적인 조문 확인 선지이다.

② O
누구든지 주요정보통신기반시설의 운영을 방해할 목적으로 대량의 신호를 보내거나 부정한 명령을 처리하게 하여 정보처리에 오류를 발생하게 하는 행위를 하여서는 아니 된다. 운영방해 목적의 전자적 침해행위를 금지한 규정에 부합한다.

③ X
침해사고가 발생하여 소관 주요정보통신기반시설의 교란·마비 또는 파괴 사실을 인지한 때의 통지는 재량이 아니라 의무이다. 따라서 "통지할 수 있다"가 틀린 표현이다.
틀린 표현: "그 사실을 통지할 수 있다"
올바른 표현: "그 사실을 법이 정한 관계 기관에 통지하여야 한다"

④ O
정부는 정보통신기반시설 보호에 필요한 기술개발을 효율적으로 추진하기 위하여 필요하면 정보보호 기술개발과 관련된 연구기관 및 민간단체로 하여금 이를 대행하게 할 수 있다. 기술개발을 외부 전문기관에 맡길 수 있다는 취지이므로 옳다.

### 오답 포인트

③은 문장 전체가 자연스러워 보여서 수험생이 그냥 넘어가기 쉽지만, 법령 문제에서는 "할 수 있다"와 "하여야 한다"가 가장 자주 출제되는 함정이다. 이 문항은 침해사고 통지를 임의행위처럼 바꿔 놓은 점이 핵심 함정이다.

### 다시 나오면 이렇게 판단

법령 선지에서는 먼저 주체, 그다음 행위의 성격이 권한인지 의무인지 확인한다. 특히 보고·통지·제출·조치처럼 사후 대응과 연결되는 규정은 의무규정으로 출제되는 경우가 많으므로 조동사를 먼저 본다.

### 암기 포인트

지정은 권고할 수 있고, 침해사고는 통지하여야 한다.

NoteBase

**문 20. 무선 LAN 보안에 관한 설명 중 ㉠ ~ ㉣에 들어갈 용어를 바르게 나열한 것은?**

강도 높은 프라이버시 및 인증 기능을 포함하는 무선 LAN 보안 표준인 IEEE (㉠)가 진화하는 과정에서 Wi-Fi 연합이 WPA/WPA2를 공표하였다. WPA는 WEP 암호의 약점을 보완한 (㉡)를 사용한다. 위 표준과 유사한 WPA2는 (㉢)를 채택하여 보다 강력한 보안을 제공한다. (㉣)는 엄격한 보안이 요구되는 네트워크에서 확장된 인증 과정을 수행하는 인증 프로토콜이다.

① ㉠: 802.11i, ㉡: TKIP, ㉢: AES, ㉣: EAP

② ㉠: 802.11i, ㉡: DES, ㉢: TKIP, ㉣: RADIUS

③ ㉠: 802.1x, ㉡: DES, ㉢: TKIP, ㉣: EAP

④ ㉠: 802.1x, ㉡: TKIP, ㉢: AES, ㉣: RADIUS

**정답 1번**

**출제 포인트**

이 문제는 무선 LAN 보안에서 802.11i와 802.1X의 역할, WPA와 WPA2의 암호화 방식, EAP와 RADIUS의 차이를 정확히 구분하는지를 묻는 문제이다.

**핵심 개념**

802.11i는 강한 인증과 암호화를 포함하는 무선 LAN 보안 표준이다. 802.1X는 네트워크 접근 제어를 위한 포트 기반 인증 프레임워크이다.
TKIP는 WPA가 WEP의 약점을 보완하려고 사용한 방식이고, AES는 WPA2가 채택한 더 강한 암호화 방식이다. EAP는 확장 인증 절차를 수행하는 인증 프로토콜이고, RADIUS는 인증 정보를 전달하고 AAA 기능을 수행하는 서버 측 프로토콜이다.

**선지별 해설**

① O: ㉠은 802.11i, ㉡은 TKIP, ㉢은 AES, ㉣은 EAP로 모두 맞다. 802.11i는 무선 LAN 보안 표준이고, WPA는 TKIP를 사용하며, WPA2는 AES를 채택하고, 확장 인증 절차는 EAP가 담당한다.
② X: 틀린 부분은 ㉡의 DES, ㉢의 TKIP, ㉣의 RADIUS이다. 실제로는 WPA가 사용하는 것은 TKIP이고, WPA2가 사용하는 것은 AES이며, 확장 인증 프로토콜은 RADIUS가 아니라 EAP이다.
③ X: 틀린 부분은 ㉠의 802.1x, ㉡의 DES, ㉢의 TKIP이다. 실제로 무선 LAN 보안 표준은 802.11i이고, WPA는 TKIP를 사용하며, WPA2는 AES를 사용한다. ㉣의 EAP만 맞는 표현이다.
④ X: 틀린 부분은 ㉠의 802.1x와 ㉣의 RADIUS이다. 실제로 ㉠은 802.11i가 맞고, 확장 인증 과정을 수행하는 것은 RADIUS가 아니라 EAP이다. ㉡의 TKIP와 ㉢의 AES는 맞는 대응이다.

NoteBase

### 오답 포인트

802.11i와 802.1X를 모두 인증 관련 용어로만 보고 섞으면 오답이 된다. 또한 EAP와 RADIUS도 함께 쓰이는 경우가 많아 같은 역할로 착각하기 쉽지만, EAP는 인증 절차 자체이고 RADIUS는 이를 운반하고 관리하는 AAA 프로토콜이라는 점이 다르다.

### 다시 나오면 이렇게 판단

보기의 용어를 표준, 암호화 방식, 인증 프로토콜로 역할별로 끊어 맞추면 된다. 무선 LAN 보안 표준은 802.11i, WPA는 TKIP, WPA2는 AES, 확장 인증은 EAP로 대응시키면 정답이 정리된다.

### 암기 포인트

802.11i는 무선 LAN 보안 표준, WPA는 TKIP, WPA2는 AES, 인증 절차는 EAP, AAA 서버 연동은 RADIUS이다.

NoteBase