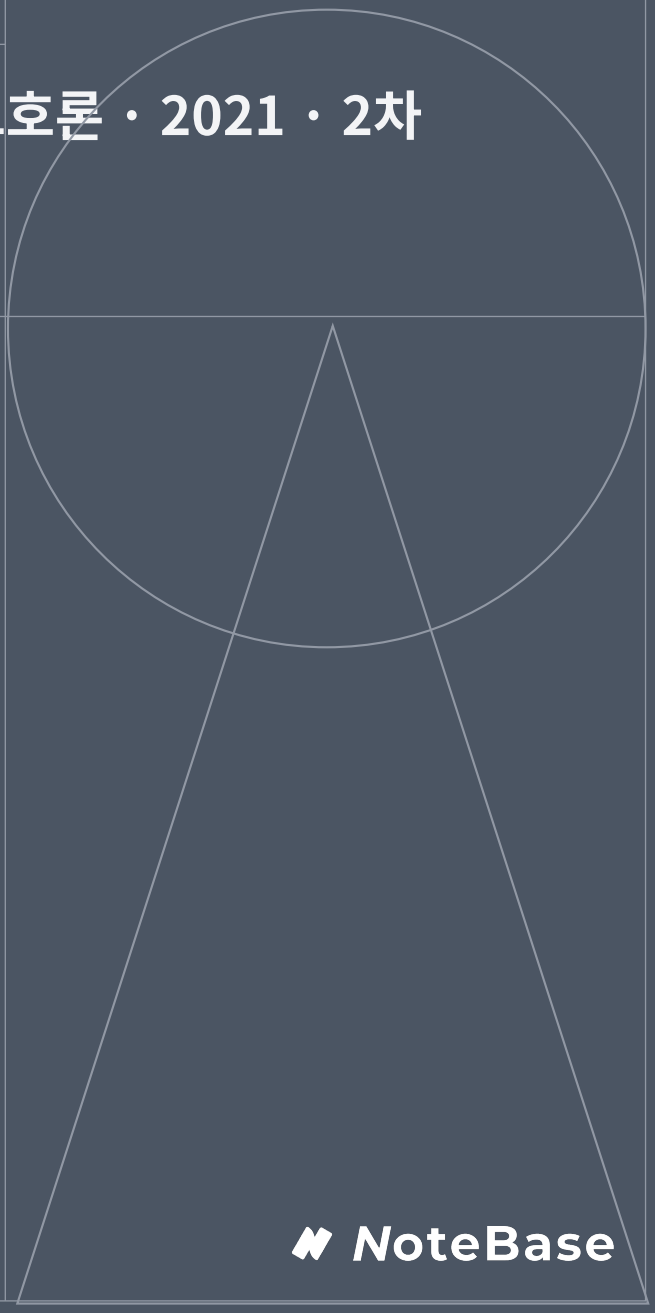
# 기출OX 해설집

공무원/국가직/7급 · 정보보호론 · 2021 · 2차



NoteBase

# 기출OX 해설집

## 공무원/국가직/7급 · 정보보호론 · 2021 · 2차

**공무원/국가직/7급 · 정보보호론 · 2021 · 2차**

**문 1. 사용자 인증에 사용되는 기술로 옳지 않은 것은?**

① Smart Card

② Single Sign On

③ One Time Password

④ Supervisory Control And Data Acquisition

**정답 4번**

**출제 포인트**

제시된 보기 중 사용자 인증(authentication)과 관련된 기술이 아닌 것을 골라내는 문제이다. Smart Card, Single Sign On, One Time Password는 모두 사용자의 신원을 확인하거나 인증 절차를 지원하는 정보보호 기술이고, Supervisory Control And Data Acquisition(SCADA)은 인증과 무관한 산업제어시스템이다.

**핵심 개념**

Smart Card는 내장된 칩에 인증서·비밀키 등을 저장해 소지 기반(what you have) 인증을 수행하는 매체이다. Single Sign On(SSO)은 사용자가 한 번의 로그인으로 여러 시스템·서비스에 접근할 수 있게 해 주는 통합 인증 체계이다. One Time Password(OTP)는 매번 새로운 값을 생성해 재사용을 막는 일회용 비밀번호 방식의 인증 기술이다. SCADA는 발전소·수처리시설·공장설비 등 산업 현장의 원격 감시와 제어를 담당하는 시스템으로, 사용자 인증이 아니라 산업제어 및 데이터 수집을 목적으로 한다.

**선지별 해설**

① Smart Card: O. 카드 내 저장된 인증 정보로 사용자를 식별·인증하는 대표적인 소지 기반 인증 기술이다.
② Single Sign On: O. 여러 시스템에 대해 한 번의 인증으로 접근을 허용하는 통합 인증 기술이다.
③ One Time Password: O. 매 인증 시도마다 다른 값을 사용하는 일회성 인증 기술이다.
④ Supervisory Control And Data Acquisition: X. SCADA는 산업제어시스템으로, 설비의 원격 감시·제어·데이터 수집을 위한 것이며 사용자 인증 기술이 아니다 → 인증 기술이 아니므로 이 문제의 정답.

NoteBase

### 오답 포인트

①②③은 모두 '사용자를 인증하는 방법'이라는 공통점이 있는데, ④ SCADA는 인증이 아니라 산업 설비를 감시·제어하는 시스템이라는 점에서 성격 자체가 다르다. 영문 약어의 겉모습만 보고 보안 관련 용어라서 인증 기술로 착각하지 않도록 주의한다.

### 다시 나오면 이렇게 판단

보기에 인증 방식(소지·지식·생체 기반 기술이나 SSO, OTP 등)과 전혀 다른 범주의 시스템(산업제어, 침입탐지, 방화벽 등)이 섞여 나오면, 그 항목이 '인증' 자체를 목적으로 하는지부터 확인한다. 목적이 다르면 바로 정답 후보로 본다.

### 암기 포인트

SCADA = 산업제어시스템(감시·제어·데이터 수집), 인증 기술 아님. Smart Card·SSO·OTP = 사용자 인증과 직결된 대표 기술로 묶어 기억해 둔다.

NoteBase

**문 2. 제로 데이 공격에 대한 설명으로 옳은 것은?**

① 서버의 성능을 크게 떨어뜨리거나 서버를 정지시키는 방법으로 서버의 정상적인 작동을 방해하는 공격 방법이다.

② 패스워드 사전 파일을 이용해 미리 지정한 아이디에 대입하여 접속계정을 알아내는 공격 방법이다.

③ 패치가 나오지 않은 시점에 이루어지는 공격 방법이다.

④ 버퍼에 일정 크기 이상의 데이터를 입력하여 프로그램을 공격하는 방법이다.

**정답 3번**

**출제 포인트**

제로 데이 공격(Zero-day Attack)의 정의를 다른 공격 기법(DoS, 사전 대입 공격, 버퍼 오버플로우)과 구분할 수 있는지를 묻는 문제이다. 제로 데이 공격은 공격 방식 자체의 기술적 특징이 아니라 '공격이 이루어지는 시점'을 기준으로 정의되는 개념이라는 점이 핵심이다.

**핵심 개념**

제로 데이 공격은 소프트웨어나 하드웨어의 취약점이 발견된 후 이를 제거할 패치나 보안 업데이트가 아직 배포되지 않은 상태에서 그 취약점을 이용해 이루어지는 공격이다. 취약점 공개(또는 발견)와 패치 배포 사이의 시간 간격, 즉 방어 수단이 존재하지 않는 '0일'의 시점을 노린다는 의미에서 이름이 붙었다. 반면 서비스 거부 공격은 서버 자원을 고갈시켜 정상 서비스를 방해하는 공격이고, 사전 대입 공격은 미리 준비한 단어 목록으로 비밀번호를 추측하는 공격이며, 버퍼 오버플로우 공격은 버퍼 크기를 초과하는 데이터를 입력해 메모리 영역을 침범하는 공격으로, 이들은 모두 공격 '방식'을 기준으로 정의된 별개의 개념이다.

**선지별 해설**

① X: 서버 성능 저하나 정지를 유발해 정상적인 서비스를 방해하는 방법은 서비스 거부 공격(DoS/DDoS)에 대한 설명이며, 제로 데이 공격의 정의가 아니다.
② X: 패스워드 사전 파일을 이용해 특정 아이디에 후보 비밀번호를 대입하는 방법은 사전 대입 공격(dictionary attack)에 대한 설명이며, 제로 데이 공격의 정의가 아니다.
③ O: 취약점이 발견되었으나 이를 해결할 패치가 아직 나오지 않은 시점, 즉 방어책이 마련되기 전의 공백 기간에 이루어지는 공격이 제로 데이 공격이다. 이는 공격 시점을 기준으로 한 정의로서 제로 데이 공격의 본질적 특징에 해당한다.
④ X: 버퍼에 정해진 크기 이상의 데이터를 입력해 프로그램의 실행 흐름이나 메모리를 조작하는 방법은 버퍼 오버플로우 공격에 대한 설명이며, 제로 데이 공격의 정의가 아니다.

NoteBase

**오답 포인트**

이 문제에서 틀리기 쉬운 이유는 ①·②·④가 모두 실제로 존재하는 유명한 공격 기법이어서 그럴듯하게 느껴지기 때문이다. 그러나 제로 데이 공격은 특정 침입 기술을 지칭하는 것이 아니라 '패치가 없는 시점을 노린다'는 시간적 조건으로 정의되는 개념이므로, 선지에 등장하는 공격 방식의 이름과 제로 데이 공격의 정의를 혼동하지 않도록 주의한다.

**다시 나오면 이렇게 판단**

선지에서 구체적인 공격 기법(성능 저하, 사전 대입, 버퍼 초과 입력 등)이 나열되면 우선 그 공격의 실제 명칭을 떠올려 제로 데이 공격과 다른 개념임을 확인한다. 그중 '패치·보안 업데이트가 아직 없는 시점'이라는 시간적 조건을 언급하는 선지가 있으면 그것이 제로 데이 공격에 해당한다고 판단한다.

**암기 포인트**

제로 데이 공격 = 취약점은 발견되었지만 패치가 나오지 않은 시점(방어 수단 부재 구간)에 이루어지는 공격. 서비스 거부 공격(자원 고갈로 서비스 방해), 사전 대입 공격(사전 파일로 비밀번호 추측), 버퍼 오버플로우 공격(버퍼 초과 입력으로 메모리 침범)과 구분해 암기한다.

NoteBase

**문 3. IPSec 프로토콜의 기능이 아닌 것은?**

① Pretty Good Privacy

② Authentication Header

③ Internet Key Exchange

④ Encapsulating Security Payload

**정답 1번**

**출제 포인트**

IPSec을 구성하는 프로토콜(AH, ESP, IKE)과 IPSec과는 별개인 이메일 암호화 표준(PGP)을 구분할 수 있는지를 묻는다. IPSec은 네트워크 계층(IP 계층)에서 동작하는 보안 프레임워크로, 그 하위에 인증·암호화·키 교환을 담당하는 세부 프로토콜들을 둔다.

**핵심 개념**

IPSec(IP Security)=IP 계층에서 데이터의 기밀성·무결성·인증을 제공하는 보안 프로토콜 집합이며, 대표 구성요소는 AH·ESP·IKE 세 가지이다. AH(Authentication Header)=출발지 인증과 무결성 검증을 제공하되 데이터 암호화는 제공하지 않는다. ESP(Encapsulating Security Payload)=데이터의 암호화(기밀성)와 함께 인증·무결성도 제공한다. IKE(Internet Key Exchange)=AH·ESP가 사용할 암호키를 안전하게 교환하고 보안연결(SA)을 협상하는 프로토콜이다. PGP(Pretty Good Privacy)=전자우편(이메일) 메시지를 암호화하고 전자서명하기 위한 응용 계층 프로그램으로, IP 계층에서 동작하는 IPSec과는 계층과 목적이 다른 별개의 기술이다.

**선지별 해설**

① Pretty Good Privacy: X → PGP는 이메일 암호화를 위한 응용 계층 도구이며 IPSec의 구성 프로토콜이 아니다. IPSec 기능이 아닌 것을 고르는 문제이므로 이 선지가 정답이다.
② Authentication Header: O → AH는 IPSec의 구성 프로토콜로 발신자 인증과 데이터 무결성 검증 기능을 제공한다.
③ Internet Key Exchange: O → IKE는 IPSec의 구성 프로토콜로 AH·ESP에 필요한 암호키 교환과 보안연결(SA) 설정을 담당한다.
④ Encapsulating Security Payload: O → ESP는 IPSec의 구성 프로토콜로 데이터의 암호화(기밀성)와 인증·무결성 기능을 함께 제공한다.

NoteBase

**오답 포인트**

PGP도 암호화라는 단어 때문에 IPSec의 하위 기능으로 착각하기 쉬우나, PGP는 이메일 보안을 위한 별도의 응용 계층 표준이고 IPSec은 IP 계층 보안 표준이라는 점에서 계층과 적용 범위가 전혀 다르다. AH·ESP·IKE는 세 가지 모두 IPSec의 핵심 구성요소라는 점을 함께 묶어 기억해 둔다.

**다시 나오면 이렇게 판단**

선지에 낯익은 보안 용어가 섞여 나오면 먼저 그 프로토콜이 동작하는 계층(응용 계층인지 IP 계층인지)을 확인한다. IPSec 관련 문제에서는 AH·ESP·IKE 세 가지가 나오면 모두 IPSec 구성요소이고, 그 외의 이메일·웹 보안 프로토콜(PGP, S/MIME, SSL/TLS 등)이 섞여 있으면 그것이 정답(구성요소가 아닌 것)일 가능성이 높다.

**암기 포인트**

IPSec 3요소는 AH(인증·무결성만), ESP(암호화+인증), IKE(키 교환)이다. PGP는 이메일용, IPSec은 IP 계층용으로 서로 다른 기술이라는 점을 짝지어 외워 둔다.

NoteBase

**문 4. 다음 설명에 해당하는 악성코드는?**

◯ 사용자 동의 없이 설치되어 컴퓨터의 정보를 수집하고 전송하는 악성소프트웨어
◯ 신용카드와 같은 금융정보 및 주민등록번호와 같은 신상정보, 암호를 비롯한 각종 정보를 수집

① ransomware
② spyware
③ backdoor
④ dropper

**정답 2번**

**출제 포인트**

제시된 두 특징(사용자 동의 없이 설치되어 정보를 수집·전송하는 점, 금융정보·주민등록번호·암호 같은 개인정보를 수집하는 점)을 보고 해당하는 악성코드 종류를 구분하는 문제이다. 악성코드는 감염 방식이나 목적에 따라 랜섬웨어, 스파이웨어, 백도어, 드로퍼 등으로 나뉘며 각각 핵심 동작이 다르다.

**핵심 개념**

스파이웨어(spyware)는 사용자 모르게 또는 동의 없이 시스템에 설치되어 사용자의 개인정보, 금융정보, 로그인 정보 등을 몰래 수집한 뒤 외부로 전송하는 악성소프트웨어이다. 랜섬웨어(ransomware)는 파일이나 시스템을 암호화하여 사용 불능 상태로 만들고 이를 풀어주는 대가로 금전을 요구하는 악성코드이다.
백도어(backdoor)는 정상적인 인증 절차를 우회해 시스템에 재침입할 수 있도록 만들어 둔 비밀 통로이다.
드로퍼(dropper)는 그 자체는 악성 행위를 하지 않고 다른 악성코드를 설치·실행시키는 역할을 하는 프로그램이다.

**선지별 해설**

① ransomware → X: 랜섬웨어는 파일을 암호화하고 금전을 요구하는 것이 핵심 동작이며, 정보를 몰래 수집·전송하는 것과는 목적이 다르다.
② spyware → O: 사용자 동의 없이 설치되어 정보를 수집·전송하고, 금융정보·주민등록번호·암호 같은 개인정보를 빼내는 것이 스파이웨어의 정의와 정확히 일치한다.
③ backdoor → X: 백도어는 인증을 우회해 시스템에 다시 접근할 수 있게 하는 통로를 만드는 것이 핵심이며, 정보 수집·전송 자체가 목적이 아니다.
④ dropper → X: 드로퍼는 다른 악성코드를 몰래 설치·전파하는 매개체 역할을 할 뿐, 정보를 직접 수집·전송하지 않는다.

NoteBase

### 오답 포인트

랜섬웨어·백도어·드로퍼는 모두 컴퓨터에 해를 끼치는 악성코드라는 공통점 때문에 헷갈릴 수 있지만, 지문의 핵심 단서는 '정보를 수집하고 전송'한다는 부분이다. 이 동작에 집중하면 정보 탈취가 목적인 스파이웨어로 바로 좁혀진다.

### 다시 나오면 이렇게 판단

지문에서 악성코드의 '목적'을 나타내는 동사에 주목한다. '정보를 수집·전송한다'는 스파이웨어, '암호화 후 금전을 요구한다'는 랜섬웨어, '재침입 통로를 만든다'는 백도어, '다른 악성코드를 설치한다'는 드로퍼로 매칭한다.

### 암기 포인트

spyware = 정보 훔쳐가는 도둑, ransomware = 인질극(암호화+금전 요구), backdoor = 뒷문(재침입 통로), dropper = 배달부(다른 악성코드 설치)로 이미지화해 기억해 둔다.

NoteBase

**문 5. 다음 설명에 해당하는 블루투스 공격을 옳게 짝지은 것은?**

(가) 공격이 가능한 블루투스 장치들을 검색하고 모델을 확인하는 공격
(나) 블루투스 장치 내 저장된 데이터에 대한 접근을 허용하는 공격
(다) 블루투스 지원 장치에 대한 접근권한을 획득하는 공격

① (가): bluesnarf, (나): bluebug, (다): blueprinting
② (가): bluesnarf, (나): blueprinting, (다): bluebug
③ (가): blueprinting, (나): bluebug, (다): bluesnarf
④ (가): blueprinting, (나): bluesnarf, (다): bluebug

**정답 4번**

**출제 포인트**

블루투스 공격 기법 3가지(블루프린팅, 블루스나프, 블루버그)를 공격 단계·행위 내용에 따라 구분할 수 있는지 묻는 문제이다. 세 공격은 순서상 정찰 단계(장치 탐색)부터 데이터 접근, 완전한 제어권 획득까지 위협 수준이 점점 커지는 구조로 이해하면 구분하기 쉽다.

**핵심 개념**

블루프린팅(blueprinting)은 공격 대상이 될 블루투스 장치를 검색하여 제조사·모델 등의 정보를 확인하는 사전 정찰 단계의 공격이다.
블루스나프(bluesnarf)는 블루투스 장치의 취약점을 이용해 장치 내에 저장된 연락처·문자·파일 등 데이터에 무단으로 접근하는 공격이다.
블루버그(bluebug)는 블루투스 장치에 대한 접근권한 자체를 탈취하여 통화, 문자 발송, 데이터 조작 등 장치를 원격으로 완전히 제어할 수 있게 되는 공격이다.

**선지별 해설**

① (가) bluesnarf / (나) bluebug / (다) blueprinting → X. (가)는 장치 검색·모델 확인이므로 blueprinting에 해당하고, (다)는 접근권한 획득이므로 bluebug에 해당하여 순서가 뒤바뀌었다.
② (가) bluesnarf / (나) blueprinting / (다) bluebug → X. (가)는 blueprinting, (나)는 저장 데이터 접근이므로 bluesnarf에 해당하여 순서가 뒤바뀌었다.
③ (가) blueprinting / (나) bluebug / (다) bluesnarf → X. (가)는 맞으나 (나) 저장 데이터 접근은 bluesnarf, (다) 접근권한 획득은 bluebug이므로 (나)와 (다)가 뒤바뀌었다.
④ (가) blueprinting / (나) bluesnarf / (다) bluebug → O. (가) 장치 검색·모델 확인=blueprinting, (나) 저장 데이터 접근 허용=bluesnarf, (다) 접근권한 획득=bluebug으로 모두 옳게 짝지어졌다.

NoteBase

**오답 포인트**

bluesnarf와 bluebug을 혼동하기 쉬운데, bluesnarf는 '저장된 데이터에 대한 접근'에 그치는 공격이고 bluebug은 그보다 강한 '장치 자체에 대한 접근권한 획득'까지 나아가는 공격이라는 점에서 구분한다. 또한 blueprinting은 공격이라기보다 공격 전 단계의 정찰(장치 검색·정보수집)에 해당한다는 점을 놓치지 않아야 한다.

**다시 나오면 이렇게 판단**

지문에 '검색', '모델 확인' 같은 표현이 나오면 blueprinting, '저장된 데이터 접근'이라는 표현이 나오면 bluesnarf, '접근권한 획득', '장치 제어'라는 표현이 나오면 bluebug으로 즉시 매칭한다. 세 용어를 공격의 진행 순서(정찰→데이터 열람→완전 제어)로 암기해두면 실수를 줄일 수 있다.

**암기 포인트**

blueprinting=장치 검색·정찰(Print=지도 그리듯 탐색), bluesnarf=데이터 훔쳐보기(snarf=낚아채다, 데이터 접근), bluebug=장치 자체를 조종(bug=도청·조종 장치 심기, 접근권한 획득).

NoteBase

**문 6. 암호화에 대한 설명으로 옳은 것은?**

① 대칭키 암호 방식은 암호화 키와 복호화 키가 다른 암호화 방법으로 암호화 키는 공개되고, 복호화 키는 공개되지 않는 구조로서 다수의 정보교환자 간의 통신에 적합하다.

② 공개키 암호에는 RSA, ElGamal 등이 있으며, 처리속도가 대칭키 알고리즘에 비해 매우 느린 단점이 있으나 키 전달이 편리하여 키교환 알고리즘으로 사용되며, 전자서명을 용이하게 구현할 수 있는 특징이 있다.

③ 블록 암호는 이진화된 평문과 키 이진수열을 배타적 논리합 이진 연산으로 결합하여 암호문을 생성하고, 블록 대칭 알고리즘에는 선형 쉬프트 레지스터 등이 있다.

④ 공개키 암호 방식은 암호화 키와 복호화 키가 동일한 암호화 방법으로 두 키가 동일하게 이용되며, 데이터를 변화하는 방법에 따라서 스트림암호와 블록암호로 나누어지고 기밀성용으로만 사용된다.

**정답 2번**

**출제 포인트**

대칭키 암호와 공개키(비대칭키) 암호의 키 구조·속도·용도 차이를 정확히 구분하는지, 그리고 블록 암호와 스트림 암호의 동작 방식을 구분하는지를 함께 묻는 문항이다.

**핵심 개념**

대칭키 암호는 암호화 키와 복호화 키가 동일하며 속도가 빨라 대량 데이터의 기밀성 보장에 주로 쓰이고, 스트림 암호와 블록 암호로 나뉜다. 스트림 암호는 평문 비트열과 키스트림을 배타적 논리합(XOR) 연산으로 결합해 암호문을 생성하며 선형 쉬프트 레지스터(LFSR) 등이 대표적으로 활용된다. 공개키(비대칭키) 암호는 암호화 키와 복호화 키가 서로 다르며, 공개키는 공개하고 개인키는 비밀로 유지하는 구조여서 다수의 정보교환자 간 통신에 적합하다. 대표 알고리즘으로 RSA, ElGamal 등이 있고 연산량이 많아 대칭키보다 처리 속도가 느리지만, 키 배송 문제를 해결할 수 있어 키교환 알고리즘으로 쓰이며 개인키로 서명하고 공개키로 검증하는 방식으로 전자서명 구현이 용이하다.

**선지별 해설**

① X - 암호화 키와 복호화 키가 다르고 암호화 키만 공개되는 구조는 대칭키 암호가 아니라 공개키(비대칭키) 암호에 대한 설명이다. 대칭키 암호는 두 키가 동일하다.
② O - 공개키 암호의 대표 알고리즘(RSA, ElGamal), 대칭키보다 느린 처리 속도, 키 전달의 편리함으로 인한 키교환 알고리즘 활용, 전자서명 구현의 용이성까지 모두 공개키 암호의 특징을 정확하게 설명하고 있다.
③ X - 평문과 키의 이진수열을 배타적 논리합으로 결합해 암호문을 만들고 선형 쉬프트 레지스터를 사용하는 방식은 블록 암호가 아니라 스트림 암호에 대한 설명이다.
④ X - 암호화 키와 복호화 키가 동일하여 스트림암호와 블록암호로 나뉘는 것은 공개키 암호가 아니라 대칭키 암호에 대한 설명이다. 또한 대칭키 암호는 기밀성뿐 아니라 메시지 인증 등 다른 용도로도 활용될 수 있어 기밀성용으로만 사용된다는 서술도 부정확하다.

NoteBase

**오답 포인트**

①과 ④는 대칭키와 공개키의 정의를 서로 뒤바꿔 제시한 함정이므로, '키가 같은가 다른가'와 '어느 키가 공개되는가'를 기준으로 먼저 구분해야 한다. ③은 블록 암호와 스트림 암호의 동작 원리를 뒤바꾼 함정으로, XOR 연산과 선형 쉬프트 레지스터는 스트림 암호의 특징임을 놓치기 쉽다.

**다시 나오면 이렇게 판단**

선지에서 '키가 같다/다르다', '어느 키가 공개된다'는 문구가 나오면 우선 대칭키인지 공개키인지부터 판별한다. 이어서 'XOR·키스트림·선형 쉬프트 레지스터'가 언급되면 스트림 암호, '블록 단위 치환·전치'가 언급되면 블록 암호로 구분한다.

**암기 포인트**

대칭키=키 동일·속도 빠름·기밀성 중심, 공개키=키 다름·속도 느림·키교환과 전자서명에 유리(RSA, ElGamal), 스트림 암호=XOR·LFSR·키스트림, 블록 암호=고정 길이 블록 단위 치환·전치 연산으로 정리해 둔다.

NoteBase

**문 7. 해시에 대한 설명으로 옳지 않은 것은?**

① 해시 알고리즘에는 MD5, SHA 등이 있다.

② 해시는 메시지의 무결성을 확인하기 위해서 사용한다.

③ 해시 알고리즘 SHA는 유럽 RIPE 프로젝트에 의해 개발된 해시함수이다.

④ 해시는 임의의 길이 메시지로부터 고정 길이의 해시값을 계산한다.

**정답 3번**

**출제 포인트**

해시(hash)의 기본 성질과 대표 해시 알고리즘의 개발 주체·표준화 배경을 정확히 알고 있는지를 묻는다. 특히 SHA 계열이 어디에서 만들어졌는지를 다른 유럽 표준 프로젝트와 혼동하지 않는지가 핵심이다.

**핵심 개념**

해시함수는 임의 길이의 입력 메시지를 고정 길이의 짧은 출력값(해시값, 다이제스트)으로 변환하는 함수이며, 입력이 조금만 달라져도 출력이 크게 달라지는 특성(눈사태 효과)과 동일 입력에 대해 항상 동일 출력을 내는 특성을 가진다. 이 성질 때문에 메시지가 전송 중 변조되었는지, 즉 무결성이 훼손되었는지를 확인하는 용도로 널리 쓰인다. 대표적인 해시 알고리즘으로 MD5와 SHA(SHA-1, SHA-2 등) 계열이 있다. MD5는 미국의 로널드 리베스트(Ronald Rivest)가 설계했고, SHA 계열은 미국 국가안보국(NSA)이 설계하여 미국 국립표준기술연구소(NIST)가 연방정보처리표준(FIPS)으로 제정한 해시함수이다. 반면 RIPEMD는 유럽의 RIPE(RACE Integrity Primitives Evaluation) 프로젝트에서 개발한 별도의 해시함수이며, SHA와는 개발 주체가 다르다.

**선지별 해설**

① O — 해시 알고리즘의 대표적인 예로 MD5와 SHA를 드는 것은 옳은 설명이다.
② O — 해시값을 비교하면 메시지가 전송·저장 과정에서 변경되었는지 확인할 수 있으므로, 해시는 메시지 무결성 확인에 사용된다는 설명은 옳다.
③ X — 틀린 표현: "SHA는 유럽 RIPE 프로젝트에 의해 개발된 해시함수이다" → 올바른 표현: SHA는 미국 NSA가 설계하고 NIST가 표준으로 채택한 해시함수이며, 유럽 RIPE 프로젝트가 개발한 해시함수는 RIPEMD이다. 따라서 SHA를 RIPE 프로젝트의 산물로 설명한 것은 옳지 않다.
④ O — 해시함수는 입력 메시지의 길이와 무관하게 항상 고정된 길이의 해시값을 계산해 내는 것이 정의적 특성이므로 옳은 설명이다.

NoteBase

### 오답 포인트

①·②·④는 해시함수의 일반적 정의(고정 길이 출력)와 대표적 용도(무결성 확인), 대표 알고리즘 예시를 그대로 진술한 옳은 문장이라 오답 근거가 없다. 함정은 ③처럼 실제로 존재하는 고유명사(RIPE 프로젝트, RIPEMD)를 가져와 다른 알고리즘(SHA)의 개발 주체인 것처럼 뒤바꾸는 방식이다. SHA와 RIPEMD를 개발 기관 기준으로 구분하지 못하면 이런 선지에서 헷갈리기 쉽다.

### 다시 나오면 이렇게 판단

선지에 해시 알고리즘 이름과 개발 기관·프로젝트명이 같이 나오면, 그 알고리즘이 실제로 어느 기관에서 만들어졌는지를 짝지어 확인한다. SHA=미국 NSA/NIST, MD5=리베스트(미국), RIPEMD=유럽 RIPE 프로젝트로 구분해 두면 이런 형태의 함정 선지를 바로 걸러낼 수 있다.

### 암기 포인트

SHA는 미국(NSA 설계, NIST 표준화), RIPEMD는 유럽(RIPE 프로젝트)에서 나왔다는 개발 주체 구분을 기억해 둔다. 해시함수의 공통 성질은 '임의 길이 입력 → 고정 길이 출력'이며 무결성 검증에 쓰인다는 점도 함께 정리해 둔다.

NoteBase

**문 8. PPTP 프로토콜에 대한 설명으로 옳은 것은?**

① 3계층인 네트워크 계층에서 동작한다.

② 마이크로소프트가 제안한 VPN 프로토콜로 PPP를 기반으로 한다.

③ 데이터를 스니핑한 뒤 해당 데이터를 다시 보내는 replay attack을 막을 수 있다.

④ 데이터가 전송 도중에 변조되었는지를 확인할 수 있도록 데이터 무결성을 검사한다.

**정답 2번**

**출제 포인트**

PPTP(Point-to-Point Tunneling Protocol)가 어떤 계층에서 동작하는 어떤 성격의 VPN 프로토콜이며, 어떤 보안 한계를 가지는지를 정확히 아는지를 묻는다. 계층 위치, 개발 주체와 기반 프로토콜, 그리고 재전송 공격·무결성 검사 관련 취약점이 함께 출제된다.

**핵심 개념**

PPTP는 마이크로소프트가 주도적으로 제안한 VPN 터널링 프로토콜로, PPP(Point-to-Point Protocol) 프레임을 캡슐화하여 전송하는 방식으로 동작한다. OSI 3계층(네트워크 계층)이 아니라 2계층(데이터 링크 계층)에서 동작하는 프로토콜이다. PPTP는 구조가 단순하고 구현이 쉬워 널리 쓰였지만, 인증 방식(MS-CHAPv2 등)의 취약점과 암호화 방식(MPPE)의 한계로 인해 재전송 공격(replay attack) 방어와 데이터 무결성 검증 기능이 취약한 프로토콜로 알려져 있다.

**선지별 해설**

① X: PPTP는 3계층인 네트워크 계층이 아니라 2계층인 데이터 링크 계층에서 동작하는 터널링 프로토콜이다. → 틀린 표현 "3계층인 네트워크 계층에서 동작한다" → 올바른 표현 "2계층인 데이터 링크 계층에서 동작한다"
② O: PPTP는 마이크로소프트가 주도하여 제안한 VPN 프로토콜이며, PPP를 기반으로 PPP 프레임을 캡슐화하여 터널링한다. 계층·개발 주체·기반 프로토콜 설명이 모두 옳다.
③ X: PPTP는 자체적으로 강력한 재전송 방지 메커니즘을 갖추지 못해 스니핑한 데이터를 재전송하는 replay attack에 취약한 프로토콜로 지적된다. → 틀린 표현 "replay attack을 막을 수 있다" → 올바른 표현 "replay attack에 취약하여 막기 어렵다"
④ X: PPTP는 IPsec처럼 별도의 무결성 검증(인증) 필드를 두어 데이터 변조 여부를 확인하는 기능이 취약하다. 전송 중 변조 확인을 위한 무결성 검사가 충분히 보장되지 않는 것이 PPTP의 대표적인 한계로 지적된다. → 틀린 표현 "데이터 무결성을 검사한다" → 올바른 표현 "데이터 무결성 검사 기능이 취약하다"

NoteBase

### 오답 포인트

①은 계층을 헷갈리기 쉬운데, PPTP는 PPP 프레임을 GRE로 캡슐화하는 2계층(데이터 링크 계층) 프로토콜이다. ③, ④는 PPTP를 IPsec 같은 강력한 보안 프로토콜로 착각해 보안 기능이 뛰어나다고 서술한 오답으로, 실제로는 PPTP가 인증·암호화 방식의 구조적 약점 때문에 재전송 공격 방어와 무결성 검사 기능이 취약하다는 점이 반대로 출제된 것이다.

### 다시 나오면 이렇게 판단

'PPTP'가 나오면 우선 마이크로소프트가 만든 PPP 기반의 2계층 VPN 프로토콜이라는 정체성부터 떠올린다. 그 다음 선지에서 계층 번호(2계층 vs 3계층)가 맞는지, 그리고 보안 기능(무결성 검사·재전송 방지)을 '갖추고 있다'고 서술했는지를 확인한다 — PPTP는 구조가 단순한 만큼 이런 보안 기능이 취약한 프로토콜이라는 점이 핵심 함정이다.

### 암기 포인트

PPTP = 마이크로소프트 제안, PPP 기반, 2계층(데이터 링크 계층) VPN 프로토콜, 재전송 공격 방어·데이터 무결성 검사 기능은 취약함.

NoteBase

**문 9. 「개인정보 보호법」 제24조의2(주민등록번호 처리의 제한)에서 제24조제1항에도 불구하고 개인정보처리자가 주민등록번호를 처리할 수 있는 경우가 아닌 것은?**

① 수탁자가 위탁받은 해당 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공하는 경우

② 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우

③ 제24조의2제1항제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 개인정보 보호위원회가 고시로 정하는 경우

④ 법률 · 대통령령 · 국회규칙 · 대법원규칙 · 헌법재판소규칙 · 중앙선거관리위원회규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우

**정답 1번**

**쟁점**

「개인정보 보호법」 제24조의2제1항은 주민등록번호 처리를 원칙적으로 금지하면서, 그 예외로 처리가 허용되는 경우를 제한적으로 열거한다. 이 문항은 그 열거된 세 가지 예외 사유(제1호~제3호)에 해당하지 않는 선지를 골라내는 것이 핵심이다. 열거 사유를 그대로 외우고 있으면 바로 답이 보인다.

**용어 풀이**

주민등록번호 처리 제한 = 정보주체의 동의만으로는 주민등록번호를 처리할 수 없고, 법령에서 별도로 허용한 경우에만 처리할 수 있도록 한 원칙(제24조의2). 수탁자 = 개인정보 처리 업무를 위탁받아 처리하는 자로, 위탁 범위 내에서만 처리할 수 있는 자를 말한다.

**핵심 구분**

주민등록번호를 처리할 수 있는 경우(제24조의2제1항 열거) vs 그 밖의 위법한 처리를 구분하는 문제이다. 열거된 세 가지는 '① 법령상 근거(법률·대통령령·각종 규칙에서 구체적으로 요구·허용) / ② 급박한 생명·신체·재산 이익을 위해 명백히 필요 / ③ 제1호·제2호에 준하여 불가피한 경우로서 보호위원회가 고시로 정하는 경우'이다. 반면 '수탁자가 위탁 범위를 초과하여 이용·제공하는 경우'는 오히려 위탁에 관한 규정(제26조)에서 금지·제재하는 위법행위이지, 주민등록번호 처리를 허용하는 사유가 아니다.

NoteBase

### 선지별 해설

① X: '수탁자가 위탁받은 해당 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공하는 경우'는 제24조의2제1항의 허용 사유가 아니다. 이는 위탁 규정에서 금지되는 위법한 처리에 해당한다. 처리를 '허용하는 경우'가 아니라 오히려 처벌 대상이 되는 행위이므로, 처리할 수 있는 경우가 아닌 것으로 골라야 한다 → 정답.
② O: '정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우'는 제24조의2제1항제2호에 규정된 허용 사유이다.
③ O: '제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 개인정보 보호위원회가 고시로 정하는 경우'는 제24조의2제1항제3호에 규정된 허용 사유이다.
④ O: '법률·대통령령·국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우'는 제24조의2제1항제1호에 규정된 허용 사유이다.

### 오답 포인트

②③④는 모두 제24조의2제1항 각 호의 문구를 거의 그대로 옮긴 것이라 '틀린 부분 찾기'로 접근하면 함정에 빠진다. 발문이 '처리할 수 있는 경우가 아닌 것'을 묻고 있으므로, 조문에 없는 사유를 담은 ①을 골라야 한다. ①은 문장 자체가 위탁 범위 초과라는 위법행위를 서술하고 있어, 허용 사유가 될 수 없다는 점만 잡으면 된다.

### 다시 나오면 이렇게 판단

주민등록번호 처리 허용 사유는 '법령 근거(제1호)·급박한 생명신체재산 이익(제2호)·보호위원회 고시로 정하는 준하는 경우(제3호)' 세 가지뿐이라는 점을 축으로 삼는다. 선지에 '위탁 범위 초과', '동의를 받은 경우', '홍보·마케팅 목적' 같이 조문에 없는 사유가 섞여 있으면 그것이 정답(허용되지 않는 경우)이다.

### 암기 포인트

주민등록번호 처리 허용 3사유 = 법령 근거 / 급박한 생명·신체·재산 이익 / 보호위원회 고시(제1호·제2호에 준하여 불가피). 위탁 범위 초과 이용·제공은 허용 사유가 아니라 금지·처벌 대상임을 함께 기억한다.

NoteBase

**문 10. 블록체인의 비트코인 블록헤더 구조에 대한 설명으로 옳지 않은 것은?**

① Nonce는 4바이트로 구성된다.

② Timestamp는 블록을 생성한 시간이다.

③ Previous Block Hash는 32바이트로 구성된다.

④ Block Header는 5가지 필드로 구성하고 크기는 60바이트로 고정되어 있다.

**정답 4번**

**출제 포인트**

비트코인 블록헤더(Block Header)를 구성하는 6개 필드의 종류와 각 필드의 바이트 크기, 그리고 헤더 전체 크기(80바이트)를 정확히 알고 있는지를 묻는다.

**핵심 개념**

비트코인 블록헤더는 Version(4바이트), Previous Block Hash(32바이트), Merkle Root(32바이트), Timestamp(4바이트), Bits(난이도 목표값, 4바이트), Nonce(4바이트) 총 6개 필드로 구성되며, 이를 모두 더하면 크기는 80바이트로 고정된다. 필드 개수는 6개이지 5개가 아니며, 크기도 60바이트가 아니라 80바이트이다.

**선지별 해설**

① Nonce는 4바이트로 구성된다. → O. 채굴 시 해시값을 변화시키기 위해 반복적으로 바꾸는 값인 Nonce는 4바이트 필드이다.
② Timestamp는 블록을 생성한 시간이다. → O. Timestamp 필드는 블록이 생성된 시각을 유닉스 타임 형식으로 기록한 4바이트 값이다.
③ Previous Block Hash는 32바이트로 구성된다. → O. 직전 블록 헤더의 해시값을 저장하는 필드로 32바이트이며, 이를 통해 블록들이 사슬(chain) 형태로 연결된다.
④ Block Header는 5가지 필드로 구성하고 크기는 60바이트로 고정되어 있다. → X. 블록헤더는 Version, Previous Block Hash, Merkle Root, Timestamp, Bits, Nonce의 6가지 필드로 구성되며 전체 크기는 80바이트로 고정된다. 필드 개수(5→6)와 전체 크기(60바이트→80바이트) 모두 틀린 설명이다.

**오답 포인트**

블록헤더 구성 필드 중 Merkle Root(트랜잭션들의 머클트리 루트값, 32바이트)를 빠뜨리고 5개로 잘못 세는 경우가 많다. 각 필드 크기를 4+32+32+4+4+4로 직접 더해 80바이트임을 확인하는 습관이 필요하다.

NoteBase

### 다시 나오면 이렇게 판단

블록헤더 관련 문제는 필드 개수(6개)와 전체 크기(80바이트)를 먼저 떠올리고, 제시된 숫자가 이와 다르면 바로 오답으로 판단한다. 각 필드가 몇 바이트인지 개별적으로 대조하면 함정 선지를 쉽게 걸러낼 수 있다.

### 암기 포인트

비트코인 블록헤더 6대 필드(4+32+32+4+4+4=80바이트): Version(4)-Previous Block Hash(32)-Merkle Root(32)-Timestamp(4)-Bits(4)-Nonce(4).

NoteBase

**문 11. OSI 7계층 중 각 층에 해당하는 프로토콜을 모두 옳게 짝지은 것은?**

① Network - IP, NetBIOS, SMTP

② Transport - ICMP, SSL, FTP

③ Presentation - ASCII, JPEG, MPEG

④ Application - HTTP, PPP, IGMP

**정답 3번**

**출제 포인트**

OSI 7계층 모델에서 각 계층이 담당하는 기능과 그 계층에서 동작하는 대표 프로토콜을 정확히 짝지을 수 있는지를 묻는다. 계층 자체의 정의뿐 아니라 각 프로토콜이 실제로 어느 계층에서 동작하는지를 개별적으로 알아야 선지를 가려낼 수 있다.

**핵심 개념**

물리 계층은 전기적 신호와 케이블 규격을 다루고, 데이터링크 계층은 MAC 주소 기반 프레임 전송(예: PPP, HDLC)을 담당한다. 네트워크 계층은 IP, ICMP, IGMP 등 논리 주소 지정과 라우팅을 담당한다. 전송 계층은 TCP, UDP처럼 종단간 신뢰성 있는 데이터 전달을 담당하며, SSL/TLS는 전송 계층 위에서 동작하는 보안 계층으로 흔히 세션·표현 계층과 함께 다뤄진다. 세션 계층은 통신 세션의 수립·유지·종료를 담당한다. 표현 계층은 데이터의 형식 변환, 인코딩, 압축, 암호화를 담당하며 ASCII 같은 문자 코드 체계, JPEG·MPEG 같은 압축 표준이 대표적이다. 응용 계층은 HTTP, FTP, SMTP, NetBIOS처럼 사용자와 직접 상호작용하는 서비스 프로토콜을 담당한다.

**선지별 해설**

① Network - IP, NetBIOS, SMTP → 틀린 표현: IP는 네트워크 계층이 맞지만 NetBIOS와 SMTP는 응용 계층 프로토콜이다 → 올바른 표현: Network 계층에는 IP, ICMP, IGMP 등이 해당한다.
② Transport - ICMP, SSL, FTP → 틀린 표현: ICMP는 네트워크 계층, FTP는 응용 계층 프로토콜이다. SSL은 전송 계층 위에서 동작하는 보안 프로토콜로 통상 전송 계층 고유 프로토콜로 분류하지 않는다 → 올바른 표현: Transport 계층에는 TCP, UDP 등이 해당한다.
③ Presentation - ASCII, JPEG, MPEG → 옳은 표현: ASCII는 문자 인코딩 방식, JPEG와 MPEG는 각각 정지영상과 동영상의 압축 표준으로 모두 데이터의 표현 형식(인코딩·압축·변환)을 다루는 표현 계층의 대표 예시에 해당한다.
④ Application - HTTP, PPP, IGMP → 틀린 표현: HTTP는 응용 계층이 맞지만 PPP는 데이터링크 계층, IGMP는 네트워크 계층 프로토콜이다 → 올바른 표현: Application 계층에는 HTTP, FTP, SMTP, NetBIOS 등이 해당한다.

NoteBase

### 오답 포인트

이 문제의 오답 선지들은 모두 계층 이름은 맞게 제시하면서 그 안에 다른 계층의 프로토콜을 하나씩 섞어 넣는 방식으로 구성되어 있다. 예를 들어 ①에서는 IP만 맞고 나머지 둘이 응용 계층 프로토콜이며, ②에서는 ICMP(네트워크)와 FTP(응용)가 섞여 있고, ④에서는 PPP(데이터링크)와 IGMP(네트워크)가 섞여 있다. 프로토콜 이름을 계층과 통째로 암기하기보다 각 프로토콜을 개별적으로 어느 계층 소속인지 정확히 구분해야 이런 혼합형 오답을 걸러낼 수 있다.

### 다시 나오면 이렇게 판단

선지에 여러 프로토콜이 나열되어 있으면 한꺼번에 판단하지 말고 프로토콜 하나하나를 따로 떼어 어느 계층 소속인지 확인한다. 하나라도 계층이 어긋나면 그 선지 전체가 오답이 된다. 표현 계층 관련 문제에서는 ASCII, JPEG, MPEG, GIF, MIME처럼 데이터 형식·압축·인코딩과 관련된 이름들을 표현 계층으로 묶어 기억해 둔다.

### 암기 포인트

물리: 케이블·전기신호. 데이터링크: MAC, PPP, HDLC. 네트워크: IP, ICMP, IGMP, 라우팅. 전송: TCP, UDP. 세션: 세션 수립·유지. 표현: ASCII, JPEG, MPEG 등 인코딩·압축·변환. 응용: HTTP, FTP, SMTP, NetBIOS 등 사용자 서비스.

NoteBase

**문 12. VPN에 대한 설명으로 옳은 것은?**

① TCP, FTP는 VPN에서 사용하는 터널링 프로토콜이다.

② 공용 회선을 대신하여 저렴한 사설 임대 회선을 이용하는 공중 암호화망이다.

③ 사설 임대 회선에 터널을 형성하고 패킷을 캡슐화하지 않고 전달하는 방법을 사용한다.

④ 인터넷과 같은 공중 네트워크를 이용하여 사설망과 같은 전용선처럼 사용할 수 있는 보안 솔루션이다.

**정답 4번**

**출제 포인트**

VPN(가상사설망, Virtual Private Network)의 정의와 동작 원리를 정확히 이해하고 있는지를 묻는다. VPN은 인터넷과 같은 공중(공용) 네트워크 위에 암호화된 터널을 만들어, 마치 전용 사설 회선을 쓰는 것처럼 안전하게 통신할 수 있게 해 주는 보안 솔루션이다. 핵심은 '공중망을 이용하되 사설망처럼 사용'한다는 방향성이며, 이를 반대로 진술하거나 터널링·캡슐화 개념을 잘못 서술한 선지를 가려낼 수 있어야 한다.

**핵심 개념**

터널링(tunneling)은 원본 패킷을 다른 패킷(헤더) 안에 캡슐화하여 공중망 구간을 통과시키는 기술이며, VPN에서는 여기에 암호화를 더해 기밀성과 무결성을 보장한다. 대표적인 터널링 프로토콜은 PPTP, L2TP, IPSec, SSL/TLS 기반 VPN 등이며, TCP나 FTP는 터널링 프로토콜이 아니라 각각 전송 계층 프로토콜과 응용 계층 파일 전송 프로토콜이다. 또한 VPN의 경제적 이점은 비싼 사설 임대 회선을 새로 구축하는 대신 이미 존재하는 저렴한 공중 네트워크(인터넷)를 활용한다는 데 있으며, 이는 선지 ②가 뒤바꿔 서술한 부분이다.

**선지별 해설**

① X — TCP는 전송 계층 프로토콜, FTP는 파일 전송을 위한 응용 계층 프로토콜로, 둘 다 VPN에서 사용하는 터널링 프로토콜이 아니다. → VPN 터널링 프로토콜에는 PPTP, L2TP, IPSec, SSL/TLS 등이 있다.
② X — '공용 회선을 대신하여 저렴한 사설 임대 회선을 이용'한다는 서술은 방향이 반대이다. VPN은 오히려 비용이 큰 사설 임대 회선을 대신하여 저렴한 공중(인터넷) 회선을 이용하면서, 암호화 터널로 사설망 수준의 보안을 확보하는 기술이다. → '사설 임대 회선을 대신하여 저렴한 공중 회선을 이용하는 사설 암호화망'이 되어야 한다.
③ X — VPN은 공중(또는 사설) 회선에 터널을 형성한 뒤 원본 패킷을 캡슐화하여 전달하는 방법을 사용한다. '캡슐화하지 않고 전달한다'는 서술은 터널링의 핵심 동작을 반대로 설명한 것이다. → '패킷을 캡슐화하여 전달하는 방법을 사용한다'가 되어야 한다.
④ O — VPN은 인터넷과 같은 공중 네트워크를 이용하면서도 암호화된 터널을 통해 사설망 전용선처럼 안전하게 사용할 수 있게 해 주는 보안 솔루션이라는 정의와 정확히 일치한다.

NoteBase

### 오답 포인트

①은 TCP·FTP를 터널링 프로토콜과 혼동한 함정이다. TCP는 전송 계층, FTP는 응용 계층 프로토콜로 애초에 계층과 역할이 다르다. ②와 ③은 공통적으로 VPN의 핵심 동작 방향을 뒤바꿔 놓은 함정으로, '공중 vs 사설'의 위치와 '캡슐화 함 vs 하지 않음'을 서로 반대로 진술해 얼핏 보면 그럴듯하게 읽힌다. 문장을 읽을 때 어느 쪽이 원본이고 어느 쪽이 대체 수단인지, 캡슐화를 하는지 안 하는지를 끝까지 뒤집어 확인해야 한다.

### 다시 나오면 이렇게 판단

'VPN'이 나오면 먼저 '공중망(인터넷)을 이용해 사설망처럼 쓰는 보안 솔루션'이라는 정의를 떠올리고, 선지에서 공중/사설의 위치가 뒤바뀌어 있지 않은지, 캡슐화 여부가 반대로 서술되어 있지 않은지, 터널링 프로토콜 자리에 TCP·FTP처럼 계층이 다른 프로토콜이 끼워져 있지 않은지 세 가지를 순서대로 점검한다.

### 암기 포인트

VPN = 공중망(인터넷) 이용 + 암호화 터널 + 캡슐화 → 사설망(전용선)처럼 사용. 터널링 프로토콜 예시: PPTP·L2TP·IPSec·SSL/TLS(TCP·FTP 아님).

NoteBase

**문 13. 정보보호 및 개인정보보호 관리체계 인증 기준에서 정하고 있는 보호대책 요구사항은?**

① 인증 및 권한관리

② 관리체계 기반 마련

③ 정보주체 권리보호

④ 관리체계 점검 및 개선

**정답 1번**

### 쟁점

정보보호 및 개인정보보호 관리체계(ISMS-P) 인증 기준은 크게 세 영역으로 구성된다. 이 문항은 각 선지가 세 영역 중 어디에 속하는지를 구분해, '보호대책 요구사항' 영역에 해당하는 항목을 골라내는 문제이다.

### 용어 풀이

ISMS-P 인증 기준의 세 영역: 1. 관리체계 수립 및 운영 / 2. 보호대책 요구사항 / 3. 개인정보 처리 단계별 요구사항. 이 중 '2. 보호대책 요구사항'은 조직이 실제로 적용해야 하는 기술적·물리적·관리적 통제 항목을 모아 놓은 영역이다.

### 핵심 구분

관리체계 수립 및 운영 = 관리체계 기반 마련·위험 관리·운영·점검 및 개선(정책과 운영 절차의 큰 틀). 보호대책 요구사항 = 정책·조직·자산 관리, 인적 보안, 외부자 보안, 물리 보안, 인증 및 권한관리, 접근통제, 암호화 적용, 정보시스템 도입 및 개발 보안, 시스템 및 서비스 운영·보안관리, 사고 예방 및 대응, 재해복구(실제 적용하는 통제 항목). 개인정보 처리 단계별 요구사항 = 수집·이용·제공·파기 등 처리 단계별 조치와 정보주체 권리보호.

### 선지별 해설

① 인증 및 권한관리: O. 보호대책 요구사항 영역의 세부 분야(사용자 계정 관리, 인증 수단, 접근 권한 부여·회수 등)에 해당한다. 정답이다.
② 관리체계 기반 마련: X. 이는 '관리체계 수립 및 운영' 영역의 첫 번째 분야로, 정책 수립·조직 구성·자원 배분 등 관리체계의 토대를 다루는 항목이다. → 보호대책 요구사항이 아니라 관리체계 수립 및 운영에 속한다.
③ 정보주체 권리보호: X. 이는 '개인정보 처리 단계별 요구사항' 영역에 속하는 항목으로, 동의 철회·열람·정정·삭제 등 정보주체의 권리를 보장하는 조치이다. → 보호대책 요구사항이 아니라 개인정보 처리 단계별 요구사항에 속한다.
④ 관리체계 점검 및 개선: X. 이는 '관리체계 수립 및 운영' 영역의 마지막 분야로, 법적 요구사항 준수 검토·관리체계 점검·개선을 다루는 항목이다. → 보호대책 요구사항이 아니라 관리체계 수립 및 운영에 속한다.

NoteBase

### 오답 포인트

②·④는 이름에 '관리체계'가 들어가 있어 관리체계 수립 및 운영 영역임을 비교적 알아채기 쉽지만, ③ 정보주체 권리보호를 개인정보 관련 통제라는 이유로 보호대책 요구사항으로 착각하기 쉽다. 정보주체 권리보호는 개인정보 처리 단계별 요구사항 영역이라는 점을 분명히 구분한다. 보호대책 요구사항은 조직 전반에 걸친 기술적·물리적·관리적 통제라는 성격으로 기억하면 인증 및 권한관리가 여기에 들어가는 것이 자연스럽다.

### 다시 나오면 이렇게 판단

ISMS-P 세 영역의 대표 키워드를 먼저 떠올린다. '기반 마련·위험 관리·운영·점검 및 개선'이 보이면 관리체계 수립 및 운영, '수집·이용·제공·파기·정보주체 권리'가 보이면 개인정보 처리 단계별 요구사항, 그 밖의 접근통제·인증·암호화·물리 보안·사고 대응 등 실제 통제 항목이면 보호대책 요구사항으로 배정한다. 선지 중 통제 항목 성격을 가진 것이 정답이다.

### 암기 포인트

ISMS-P 3영역: 관리체계 수립 및 운영(기반 마련→위험 관리→운영→점검 및 개선), 보호대책 요구사항(정책·조직·자산, 인적·외부자·물리 보안, 인증 및 권한관리, 접근통제, 암호화, 개발 보안, 운영·보안관리, 사고 대응, 재해복구), 개인정보 처리 단계별 요구사항(처리 단계별 조치+정보주체 권리보호). '인증 및 권한관리 = 보호대책'으로 묶어 외워 둔다.

NoteBase

**문 14. 「개인정보 보호법」 제4조(정보주체의 권리)에서 정보주체가 자신의 개인정보 처리와 관련해서 가지는 권리로 옳지 않은 것은?**

① 개인정보의 처리 정지, 정정·삭제 및 파기를 요구할 권리

② 개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리

③ 개인정보의 목적 외 수집, 오용·남용 및 무분별한 감시·추적 등에 따른 폐해를 방지하여 인간의 존엄과 개인의 사생활 보호를 도모하기 위한 시책을 강구할 권리

④ 개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리

**정답 3번**

### 쟁점

「개인정보 보호법」 제4조가 규정한 '정보주체의 권리'와, 제5조가 규정한 '국가와 지방자치단체의 책무'를 구별하는 문제이다. 선지 ③은 정보주체의 권리처럼 보이지만 실제로는 국가와 지방자치단체가 이행해야 할 시책(책무)의 내용이므로, 정보주체가 가지는 권리로는 옳지 않다.

### 용어 풀이

정보주체: 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.
처리: 개인정보의 수집, 생성, 기록, 저장, 보유, 이용, 제공, 공개, 파기 등 개인정보를 대상으로 하는 모든 행위를 말한다.
시책: 어떤 목적을 이루기 위한 정책상의 조치로, 그 이행 주체는 국가와 지방자치단체이다.

### 핵심 구분

정보주체의 권리(제4조)=정보주체 개인이 '가지는' 권리(정보 제공받을 권리, 동의 여부·범위를 선택·결정할 권리, 열람·전송 요구권, 처리정지·정정·삭제·파기 요구권, 피해 구제받을 권리).
국가 등의 책무(제5조)=국가와 지방자치단체가 '이행하는' 시책·의무(목적 외 수집·오용·남용·무분별한 감시·추적 등 폐해 방지 시책 강구 등).
주어가 '정보주체'가 아니라 '국가·지방자치단체'로 바뀌면 권리가 아니라 책무이다.

NoteBase

### 선지별 해설

① O: 개인정보의 처리 정지, 정정·삭제 및 파기를 요구할 권리는 제4조가 정한 정보주체의 권리에 해당한다.
② O: 개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리는 제4조가 정한 정보주체의 권리에 해당한다.
③ X: 목적 외 수집·오용·남용·무분별한 감시·추적 등에 따른 폐해를 방지하여 인간의 존엄과 사생활 보호를 도모하기 위한 시책을 강구하는 것은 제5조가 정한 국가와 지방자치단체의 책무이지 정보주체가 가지는 권리가 아니다. '정보주체가 시책을 강구할 권리' → '국가·지방자치단체가 시책을 강구할 책무'로 바로잡아야 한다.
④ O: 개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리는 제4조가 정한 정보주체의 권리에 해당한다.

### 오답 포인트

선지 ③의 문장 자체는 법에 실제로 존재하는 표현이라 익숙하게 느껴져 옳은 것으로 넘기기 쉽다. 그러나 그 조문은 제4조가 아니라 제5조(국가 등의 책무)이며, 행위 주체가 정보주체가 아니라 국가·지방자치단체이다. '시책을 강구'라는 표현이 나오면 개인의 권리가 아니라 공적 주체의 의무 신호로 읽어야 한다.

### 다시 나오면 이렇게 판단

정보주체의 권리를 묻는 문제에서는 각 선지의 주어와 서술어가 '정보주체가 ~을 요구·선택·결정·제공받는다'인지 먼저 확인한다. '방지하여', '도모하기 위한 시책을 강구' 같은 정책적·공적 서술이 나오면 국가·지방자치단체의 책무(제5조)를 옮겨 놓은 함정 선지로 본다.

### 암기 포인트

제4조 정보주체의 권리 다섯 축=①정보 제공받을 권리 ②동의 여부·범위 선택·결정 권리 ③열람(사본 발급 포함)·전송 요구 권리 ④처리정지·정정·삭제·파기 요구 권리 ⑤피해 구제받을 권리. '목적 외 수집·오용·남용·감시·추적 폐해 방지 시책 강구'는 제5조 국가 등의 책무로 따로 외워 둔다.

NoteBase

**문 15. 웹 해킹 공격에 대한 설명으로 옳지 않은 것은?**

① Reverse Telnet은 특정 사용자를 대상으로 하지 않고 불특정 다수를 대상으로 로그인된 사용자가 자신의 의지와 무관하게 공격자가 의도한 행위를 하도록 한다.

② Cross Site Scripting은 악성스크립트를 게시판에 등록하는 글에 포함시켜, 이에 접근한 사용자 컴퓨터에서 실행하도록 한다.

③ File Upload는 첨부파일 업로드 기능을 이용해 해킹 프로그램을 업로드한 후, 웹서버의 권한 획득을 가능하도록 한다.

④ Directory Listing은 취약한 서버 설정으로 브라우징되는 디렉토리의 모든 파일이 인터넷 사용자에게 노출되어 파일의 열람을 가능하도록 한다.

**정답 1번**

**출제 포인트**

웹 해킹 공격 기법 각각의 정의와 동작 방식을 정확히 구분할 수 있는지를 묻는다. 특히 공격 대상이 서버인지 다른 사용자(클라이언트)인지, 공격자가 직접 조작하는 방식인지 피해자가 무심코 행위를 실행하게 만드는 방식인지를 구분하는 것이 핵심이다.

**핵심 개념**

Reverse Telnet=방화벽이나 NAT 등으로 외부에서 내부로 직접 접속이 막힌 상황에서, 공격자가 이미 장악한 서버(웹셸 등)로 하여금 공격자의 시스템으로 역방향 접속을 걸게 하여 원격 셸(명령행 제어권)을 획득하는 기법이다. 즉 공격자가 이미 침투한 서버의 제어권을 안정적으로 유지·확장하기 위한 후속 기법이며, 로그인된 일반 사용자를 속여 의도치 않은 행위를 하게 만드는 기법이 아니다. Cross Site Request Forgery(CSRF)=공격자가 조작한 요청을 로그인된 사용자가 자신도 모르게 실행하게 만들어 사용자의 권한으로 원치 않는 행위(비밀번호 변경, 송금 등)를 수행시키는 공격이다. Cross Site Scripting(XSS)=게시판 등에 악성 스크립트를 삽입해 이를 열람하는 다른 사용자의 브라우저에서 스크립트가 실행되도록 하는 공격이다. File Upload 공격=첨부파일 업로드 기능의 검증 미비를 악용해 웹셸 등 해킹 프로그램을 서버에 올린 뒤 이를 실행시켜 서버의 제어권(권한)을 획득하는 공격이다. Directory Listing=웹서버 설정 취약점으로 디렉토리 내 파일 목록이 그대로 노출되어 인터넷 사용자가 파일을 열람할 수 있게 되는 취약점이다.

NoteBase

### 선지별 해설

① X — 지문의 설명(특정 사용자를 대상으로 하지 않고 불특정 다수의 로그인된 사용자가 자신의 의지와 무관하게 공격자가 의도한 행위를 하도록 함)은 Cross Site Request Forgery(CSRF)의 정의이다. Reverse Telnet은 공격자가 이미 확보한 서버 접근 권한을 이용해 외부로 역접속을 걸어 원격 명령 셸을 얻는 기법으로, 일반 사용자를 속이는 것과는 무관하다. 틀린 표현 → 올바른 표현: "Reverse Telnet은 …" → "Cross Site Request Forgery(CSRF)는 …"이어야 한다.
② O — Cross Site Scripting은 악성 스크립트를 게시글 등에 삽입해 이를 열람하는 사용자의 컴퓨터(브라우저)에서 실행되도록 하는 공격이 맞다.
③ O — File Upload 공격은 첨부파일 업로드 기능을 악용해 해킹 프로그램(웹셸 등)을 서버에 올린 후 웹서버의 권한을 획득하도록 하는 공격이 맞다.
④ O — Directory Listing은 취약한 서버 설정으로 디렉토리 내 모든 파일이 노출되어 인터넷 사용자가 파일을 열람할 수 있게 되는 취약점 설명이 맞다.

### 오답 포인트

Reverse Telnet과 CSRF를 혼동하기 쉬운데, 두 개념을 구분하는 기준은 '누가 누구를 속이는가'이다. CSRF는 서버가 아니라 로그인된 사용자(피해자)의 브라우저가 공격자 의도대로 요청을 보내게 만드는 공격이고, Reverse Telnet은 이미 장악한 서버가 공격자에게 역접속하여 셸 권한을 넘겨주는 기법으로 사용자를 속이는 절차가 없다. 이 차이를 놓치면 ①을 옳은 설명으로 착각하기 쉽다.

### 다시 나오면 이렇게 판단

선지에서 공격 기법 이름과 설명이 짝지어 나오면, 먼저 '공격 대상이 서버인지 사용자(브라우저)인지'와 '피해자의 개입(클릭·로그인 상태 이용)이 있는지'를 따진다. 로그인된 사용자가 자신의 의지와 무관하게 행위를 하게 된다는 서술이 나오면 CSRF를 의심하고, 서버 권한 획득이나 원격 접속·제어를 위한 후속 기법 서술이 나오면 Reverse Telnet, 웹셸 업로드, 백도어 등을 의심한다.

### 암기 포인트

Reverse Telnet=서버 장악 후 외부로 역접속해 원격 셸 획득(서버측 후속 기법). CSRF=로그인된 사용자가 모르게 원치 않는 요청을 대신 실행. XSS=악성 스크립트가 다른 사용자 브라우저에서 실행. File Upload 공격=업로드 취약점으로 웹셸 실행 후 서버 권한 획득. Directory Listing=디렉토리 목록·파일 노출 취약점.

NoteBase

**문 16. NAC에 대한 설명으로 옳지 않은 것은?**

① 사용자 식별과 인증을 수행한다.

② 단말 무결성 검증을 제공한다.

③ 해커를 유인해서 정보를 얻거나 잡으려고 설치한다.

④ 802.1x 방식, VLAN 방식 등으로 구현된다.

**정답 3번**

**출제 포인트**

NAC(Network Access Control, 네트워크 접근제어)가 실제로 수행하는 기능과, NAC과 혼동되기 쉬운 다른 보안 솔루션(허니팟 등)의 기능을 구분할 수 있는지를 묻는 문항이다. NAC은 내부 네트워크에 접속하려는 단말과 사용자를 통제하는 솔루션이고, 공격자를 유인해 정보를 수집하는 것은 허니팟(decoy system)의 역할이므로 이 둘을 섞으면 안 된다.

**핵심 개념**

NAC은 사내 네트워크에 접속하는 모든 단말을 사전에 통제하기 위한 솔루션으로, 크게 세 가지 기능을 수행한다. 첫째, 접속하려는 사용자의 신원을 확인하는 식별·인증 기능이다. 둘째, 접속하려는 단말이 백신 설치 여부, 보안 패치 적용 여부 등 정책에 부합하는 상태인지 검사하는 무결성(상태) 검증 기능이다. 셋째, 인증·검증을 통과하지 못한 단말을 격리하거나 접근을 차단하는 통제 기능으로, 이는 실무에서 802.1x(포트 기반 접근제어) 방식이나 VLAN 분리 방식 등으로 구현된다. 반면 허니팟은 정상 시스템처럼 위장해 공격자를 유인하고 공격 행위·정보를 수집·분석하기 위한 별도의 유인 시스템으로, NAC의 기능 범주에 속하지 않는다.

**선지별 해설**

① 사용자 식별과 인증을 수행한다. → O. NAC의 기본 기능으로, 네트워크에 접속하려는 사용자·단말의 신원을 확인하고 인증하는 절차를 거친다.
② 단말 무결성 검증을 제공한다. → O. 접속 단말의 보안 상태(백신, 패치, 정책 준수 여부 등)를 점검하는 것은 NAC의 핵심 기능이다.
③ 해커를 유인해서 정보를 얻거나 잡으려고 설치한다. → X. 이는 NAC이 아니라 허니팟에 대한 설명이다. NAC은 접근 통제 솔루션이지 공격자를 유인해 정보를 수집하는 목적의 시스템이 아니므로 옳지 않은 설명이다.
④ 802.1x 방식, VLAN 방식 등으로 구현된다. → O. NAC의 접근 통제 기능은 실제로 802.1x 인증 방식이나 VLAN을 이용한 네트워크 분리 방식 등으로 구현된다.

NoteBase

### 오답 포인트

NAC과 허니팟을 혼동하면 안 된다. NAC은 '누가, 어떤 상태의 단말로 접속하는가'를 통제하는 사전 예방적 접근제어 솔루션이고, 허니팟은 공격자를 의도적으로 유인해 공격 정보를 수집하는 기만·탐지용 시스템이다. 목적과 동작 방식이 근본적으로 다르므로 NAC의 설명으로 허니팟의 기능이 제시되면 옳지 않은 선지가 된다.

### 다시 나오면 이렇게 판단

선지에 '유인', '기만', '가짜 시스템으로 잡는다' 같은 표현이 나오면 NAC이 아니라 허니팟이나 디코이 시스템의 특징임을 바로 떠올린다. NAC 관련 문항은 식별·인증, 무결성(상태) 검증, 접근 통제(802.1x·VLAN)라는 세 축으로 선지를 분류해 판단한다.

### 암기 포인트

NAC = 식별·인증 + 단말 무결성 검증 + 802.1x·VLAN 기반 접근 통제. 유인·기만은 허니팟의 몫이라는 것을 세트로 암기해 둔다.

NoteBase

**문 17. WTLS 레코드 프로토콜의 하위 프로토콜에 해당하는 것은?**

① Handshake Protocol

② Change CipherSpec Protocol

③ Alert Protocol

④ Wireless Datagram Protocol

**정답 4번**

**출제 포인트**

WAP(무선 응용 프로토콜) 스택에서 WTLS(Wireless Transport Layer Security)가 차지하는 위치와, WTLS 내부 구조를 구분하는 문제이다. WTLS 자체를 구성하는 상위 프로토콜들과, WTLS보다 아래 계층에 위치하는 프로토콜을 구별해야 한다.

**핵심 개념**

WAP 프로토콜 스택은 위에서부터 응용 계층(WAE), 세션 계층(WSP), 트랜잭션 계층(WTP), 보안 계층(WTLS), 전송 계층(WDP) 순으로 쌓인다. WTLS는 TLS/SSL과 유사한 구조를 가지며, 그 안에 레코드 프로토콜(Record Protocol)과 이를 이용하는 상위의 세 프로토콜, 즉 Handshake Protocol, Change CipherSpec Protocol, Alert Protocol이 존재한다. 이 세 프로토콜은 레코드 프로토콜이 제공하는 전송 서비스를 이용하여 동작하므로 레코드 프로토콜의 상위 프로토콜에 해당한다. 반면 WDP(Wireless Datagram Protocol)는 WTLS 계층 자체보다 아래에 위치한 전송 계층 프로토콜로서, WTLS 레코드 프로토콜이 실제 데이터를 주고받을 때 딛고 서는 하위 계층 프로토콜이다.

**선지별 해설**

① Handshake Protocol → X: 레코드 프로토콜 위에서 세션 키 협상 등을 수행하는 프로토콜로, 레코드 프로토콜의 상위 프로토콜이다.
② Change CipherSpec Protocol → X: 새로 협상된 암호 규격 적용을 알리는 프로토콜로, 역시 레코드 프로토콜 위에서 동작하는 상위 프로토콜이다.
③ Alert Protocol → X: 오류나 세션 종료 등을 통지하는 프로토콜로, 레코드 프로토콜 위에서 동작하는 상위 프로토콜이다.
④ Wireless Datagram Protocol → O: WAP 스택에서 WTLS보다 아래 계층에 위치한 전송 프로토콜로, WTLS 레코드 프로토콜이 데이터를 전달할 때 이용하는 하위 프로토콜에 해당한다.

NoteBase

### 오답 포인트

Handshake, Change CipherSpec, Alert 세 프로토콜은 레코드 프로토콜의 서비스를 '이용하는' 쪽이므로 상위 프로토콜로 분류되는데, 이름만 보고 레코드 프로토콜과 나란히 있는 하위 구성요소로 착각하기 쉽다. '레코드 프로토콜의 하위'라는 표현이 WTLS 내부 구조가 아니라 WAP 스택 상의 계층 관계(레코드 프로토콜보다 아래 계층)를 묻고 있다는 점에 주의한다.

### 다시 나오면 이렇게 판단

TLS/SSL 계열 프로토콜 문제에서는 먼저 레코드 프로토콜을 기준으로 '레코드 프로토콜 위에서 동작하는 프로토콜'(Handshake, ChangeCipherSpec, Alert 등)과 '레코드 프로토콜보다 아래 계층에 있는 프로토콜'(전송 계층 프로토콜)을 나누어 정리한다. 문제에서 상위/하위 방향을 명확히 확인한 뒤 해당 방향에 맞는 프로토콜을 고른다.

### 암기 포인트

WAP 스택 순서: WAE(응용) - WSP(세션) - WTP(트랜잭션) - WTLS(보안) - WDP(전송). WTLS 내부: Handshake/ChangeCipherSpec/Alert Protocol은 레코드 프로토콜의 상위, WDP는 WTLS 자체의 하위 계층 프로토콜로 정리해 둔다.

NoteBase

**문 18. 보안 솔루션에 대한 설명으로 옳지 않은 것은?**

① IPS는 유해 트래픽이나 다양한 유형의 공격을 사전에 탐지하고 자동화된 알고리즘에 의해 탐지된 공격을 차단하는 능동형 보안 기능을 제공한다.

② IDS는 전통적인 방화벽이 탐지할 수 없는 악의적인 네트워크 트래픽이나 컴퓨터 사용을 탐지하고 이를 알려주는 역할만 한다는 점에서 공격 자체를 차단하는 방화벽과 차이가 있다.

③ DLP는 이미지 및 오디오 파일과 같은 다양한 디지털 매체를 통해 메시지를 숨겨 전송한다.

④ Firewall은 외부 네트워크에서 내부 네트워크로 유입되는 침입을 막는 역할을 한다.

**정답 3번**

**출제 포인트**

IPS·IDS·DLP·Firewall 등 대표적인 보안 솔루션 각각이 실제로 수행하는 기능을 정확히 구분할 수 있는지를 묻는다. 이름은 비슷해 보여도 탐지·차단·유출방지라는 역할이 서로 다르므로, 각 솔루션의 정의를 다른 솔루션의 정의와 뒤바꿔 놓았는지 확인하는 것이 핵심이다.

**핵심 개념**

IPS(Intrusion Prevention System)는 유해 트래픽이나 공격을 탐지함과 동시에 자동으로 차단까지 수행하는 능동형(예방적) 보안 솔루션이다. IDS(Intrusion Detection System)는 악의적인 트래픽이나 사용을 탐지하고 관리자에게 알리는 역할만 하며, 차단 기능은 없다는 점에서 방화벽이나 IPS와 구분된다. Firewall은 사전에 정의된 규칙에 따라 외부 네트워크에서 내부 네트워크로 들어오는 침입을 차단하는 경계 보안 솔루션이다. DLP(Data Loss Prevention, 데이터 유출 방지)는 조직 내부의 중요 정보(개인정보·기밀문서 등)가 외부로 유출되는 것을 탐지·차단하는 솔루션으로, 이미지·오디오 파일 등 디지털 매체 속에 메시지를 은닉해 전송하는 것은 스테가노그래피(steganography)의 정의이지 DLP의 기능이 아니다.

**선지별 해설**

① IPS에 대한 설명으로 옳다. IPS는 탐지된 공격을 자동화된 알고리즘으로 즉시 차단하는 능동형 보안 기능을 제공한다.
② IDS에 대한 설명으로 옳다. IDS는 탐지 및 알림 기능만 수행하고 직접 차단하지 않는다는 점에서 방화벽과 차이가 있다.
③ DLP에 대한 설명으로 옳지 않다. → 틀린 표현: DLP가 이미지·오디오 파일 등 디지털 매체를 통해 메시지를 숨겨 전송한다. → 올바른 표현: 이는 스테가노그래피에 대한 설명이며, DLP는 내부의 중요 데이터가 외부로 유출되는 것을 탐지하고 차단하는 솔루션이다.
④ Firewall에 대한 설명으로 옳다. Firewall은 외부에서 내부로 유입되는 침입을 차단하는 역할을 한다.

NoteBase

**오답 포인트**

DLP라는 명칭만 보고 '매체를 통해 정보를 숨긴다'는 문장을 그럴듯하게 받아들이기 쉬운데, 이는 정보를 은닉하는 기술인 스테가노그래피의 정의를 DLP에 뒤바꿔 놓은 함정이다. DLP는 '숨겨서 전송하는' 주체가 아니라 '유출을 막는' 주체라는 점을 혼동하지 않아야 한다.

**다시 나오면 이렇게 판단**

보안 솔루션 명칭이 나오면 먼저 그 솔루션의 목적(예방/탐지/차단/유출방지)이 무엇인지부터 떠올린 뒤 선지 내용과 대조한다. IPS=탐지+차단, IDS=탐지+알림만, Firewall=경계에서 침입 차단, DLP=내부 데이터 유출 방지라는 네 가지 역할을 서로 헷갈리지 않도록 짝지어 기억해 둔다.

**암기 포인트**

IPS는 막는다(Prevention), IDS는 알린다(Detection, 차단 없음), Firewall은 경계를 지킨다, DLP는 내부 정보의 유출을 막는다(Loss Prevention)로 각각의 핵심 동사를 짝지어 외워 둔다.

NoteBase

**문 19. CERT에 대한 설명으로 옳은 것은?**

① 컴퓨터 긴급 관리팀으로 불리며, 영국의 옥스포드대학에서 만들었다.

② 웜 사고에 대응하기 위해 만들어졌지만, 현재는 웜뿐만 아니라 해커의 침입에 대한 대응과 추적에 대한 업무까지 맡고 있다.

③ 정부에서만 CERT를 운영하고 있다.

④ CERT팀은 법률 대리인, 대외 언론 및 외부 기관 대응 전문가로만 구성된다.

**정답 2번**

**출제 포인트**

CERT(Computer Emergency Response Team, 컴퓨터 비상 대응팀)의 유래와 현재의 역할 범위를 정확히 아는지를 묻는다. 최초 설립 배경(웜 사고)과 운영 주체의 다양성, 팀 구성원의 범위가 핵심 판단 지점이다.

**핵심 개념**

CERT는 1988년 모리스 웜(Morris Worm) 사고를 계기로 미국 카네기멜론대학교(CMU) 산하에 최초로 설립된 침해사고 대응 조직이다. 이후 각국 정부기관·대학·기업·민간 보안업체 등 다양한 주체가 자체 CERT 또는 CERT/CC(Coordination Center) 형태의 조직을 운영하며, 대응 범위도 웜·바이러스뿐 아니라 해킹, 침입 탐지 및 추적, 취약점 분석, 사고 통계 관리 등으로 확대되었다. CERT팀 구성은 기술적 분석·대응을 담당하는 보안 전문가가 핵심이며, 필요에 따라 법률 자문·홍보(대외 언론) 담당자가 보조적으로 포함되는 것이지, 팀 전체가 법률·홍보·외부 기관 대응 인력만으로 구성되는 것은 아니다.

**선지별 해설**

① X: CERT는 '컴퓨터 긴급 대응팀'으로 불리며, 최초로 만든 곳은 영국 옥스포드대학이 아니라 미국 카네기멜론대학교(CMU)이다. 설립 국가와 기관명이 모두 틀린 표현이다.
② O: CERT는 1988년 모리스 웜 사고를 계기로 웜에 대응하기 위해 만들어졌으나, 현재는 웜 대응에 그치지 않고 해커의 침입에 대한 대응과 추적 등 침해사고 전반의 업무를 수행하고 있다. 설립 배경과 현재 역할 확장을 모두 정확히 서술한 옳은 설명이다.
③ X: CERT는 정부에서만 운영하는 조직이 아니다. 정부기관형 CERT 외에도 대학, 민간 기업, 학술·연구 네트워크 등 다양한 주체가 자체적으로 CERT를 구성해 운영하고 있다. '정부에서만'이라는 한정이 틀린 표현이다.
④ X: CERT팀은 법률 대리인, 대외 언론 담당자, 외부 기관 대응 전문가만으로 구성되지 않는다. 팀의 중심은 침해사고를 실제로 분석·대응·추적하는 기술 보안 전문가이며, 법률·홍보 인력은 필요 시 보조적으로 참여하는 구성원일 뿐이다. '~로만 구성된다'는 한정이 틀린 표현 → 기술 대응 전문가를 중심으로 구성되고 법률·홍보 인력이 보조적으로 포함된다.

NoteBase

### 오답 포인트

①은 설립 기관과 국가를 뒤바꿔 혼동을 유발하는 선지로, CMU라는 고유명사를 정확히 기억하지 못하면 옥스포드대학 같은 그럴듯한 오답에 흔들리기 쉽다. ③, ④는 '~만', '~로만'처럼 범위를 과도하게 한정하는 단정적 표현이 오답의 신호라는 점을 놓치면 틀리기 쉽다.

### 다시 나오면 이렇게 판단

CERT 관련 문항은 먼저 '~만', '~뿐' 같은 배타적 한정 표현이 있는 선지부터 의심한다. 실제 CERT는 운영 주체(정부·대학·민간)와 구성원(기술 전문가 중심+법률·홍보 보조), 대응 범위(웜에서 해킹 전반으로 확대)가 모두 다양화·확장된 조직이므로, 한정적으로 서술한 선지는 오답일 가능성이 높다.

### 암기 포인트

CERT 최초 설립: 1988년 모리스 웜 사고 계기, 미국 카네기멜론대학교(CMU). 현재 대응 범위: 웜뿐 아니라 해킹·침입 대응·추적까지 확대. 운영 주체: 정부뿐 아니라 대학·민간도 운영. 팀 구성: 기술 보안 전문가 중심 + 법률·홍보 인력은 보조.

NoteBase

**문 20. 정보 보안 거버넌스의 구현 요건에 대한 설명으로 옳지 않은 것은?**

① 전략적 연계: 정보 보안 사고의 잠재적 위험을 줄이려면 조직에 적합한 위험 관리 체계를 수립하고 지속적으로 관리해야 한다.

② 가치 전달: 정보 보안 투자의 효과를 높이기 위해서는 구성원들에게 정보 보안의 중요성과 가치를 교육하고 국제 표준을 기준으로 정보 보안 관리 체계를 갖추어 운영해야 한다.

③ 자원 관리: 정보 보안 지식과 자원을 효율적으로 관리하기 위해 중요한 정보 자산과 인프라를 포함하는 전사적 정보 보안 아키텍처를 확보해야 한다.

④ 성과 관리: 정보 보안 거버넌스의 효과적인 운영을 위한 척도로 모니터링이나 보고 및 성과 평가 체계를 운영해야 한다.

**정답 1번**

**출제 포인트**

정보 보안 거버넌스(information security governance)를 실현하는 데 필요한 여러 활동 영역(요건)이 각각 무엇을 의미하는지 정확히 구분하는 문제이다. 정보 보안 거버넌스는 이사회·경영진이 조직의 정보 보안 활동을 지휘·통제하기 위한 체계로, 전략적 연계·위험 관리·가치 전달·자원 관리·성과 관리·보증(감사) 활동 등 서로 다른 성격의 요건들로 구성된다. 이 문제는 각 요건에 붙은 이름표와 그 설명 내용이 서로 짝이 맞는지를 확인하도록 요구한다.

**핵심 개념**

전략적 연계=정보 보안 전략을 조직의 사업 전략 및 목표와 일치시키는 활동이다. 가치 전달=정보 보안에 대한 투자가 조직에 실질적인 가치(효율성·신뢰성 향상 등)로 이어지도록 표준화된 관리 체계를 갖추고 그 중요성을 구성원에게 전달·교육하는 활동이다. 위험 관리=정보 보안 사고로 인한 잠재적 위험을 조직 수준에 맞게 식별·평가하고 이를 지속적으로 관리하는 체계를 수립하는 활동이다. 자원 관리=보안 지식과 인력·예산·인프라 등 자원을 효율적으로 배분하고, 중요 자산을 포함하는 전사적 보안 아키텍처를 갖추는 활동이다. 성과 관리=거버넌스 활동이 제대로 작동하는지 모니터링·보고·평가하는 척도를 운영하는 활동이다.

NoteBase

### 선지별 해설

① X: '전략적 연계'라는 이름표를 달고 있지만 설명 내용은 '정보 보안 사고의 잠재적 위험을 줄이기 위해 위험 관리 체계를 수립하고 지속적으로 관리한다'는 것으로, 이는 전략적 연계가 아니라 위험 관리에 해당하는 설명이다. 전략적 연계는 보안 전략과 사업 전략·목표를 일치시키는 것을 의미하므로 이름표와 설명이 어긋난다. 틀린 표현 → 올바른 표현: '전략적 연계' → '위험 관리'로 바꾸어야 설명과 일치한다.
② O: '가치 전달'은 보안 투자의 효과를 높이기 위해 구성원 교육과 국제 표준 기반의 관리 체계 운영을 요구하는 내용으로, 투자를 실질적 가치로 연결한다는 가치 전달의 취지와 부합한다.
③ O: '자원 관리'는 보안 지식과 자원을 효율적으로 관리하기 위해 중요 정보 자산과 인프라를 포함하는 전사적 보안 아키텍처를 확보한다는 내용으로, 자원의 효율적 관리라는 취지와 부합한다.
④ O: '성과 관리'는 거버넌스의 효과적 운영을 위한 척도로 모니터링·보고·성과 평가 체계를 운영한다는 내용으로, 성과를 측정·관리한다는 취지와 정확히 부합한다.

### 오답 포인트

이 문제의 함정은 선지마다 붙은 이름표(전략적 연계, 가치 전달, 자원 관리, 성과 관리)를 그대로 믿고 넘어가는 것이다. 각 요건의 이름과 그 아래 설명 내용이 실제로 같은 개념을 가리키는지 대조해야 한다. ①은 이름은 전략적 연계이지만 내용은 위험 관리의 정의이므로, 이름과 내용의 불일치를 찾아내는 것이 핵심이다.

### 다시 나오면 이렇게 판단

정보 보안 거버넌스 요건이 제시되면 각 항목을 이름표만으로 판단하지 말고, 설명 문장이 실제로 어떤 개념(전략 연계/위험 관리/가치 전달/자원 관리/성과 관리/보증)을 서술하는지 먼저 파악한 뒤 이름표와 대조한다. 설명 속 핵심 동사(줄이다·관리하다=위험 관리, 교육하다·표준 갖추다=가치 전달, 효율적으로 배분·아키텍처 확보=자원 관리, 모니터링·보고·평가=성과 관리, 전략·목표와 일치=전략적 연계)를 단서로 삼는다.

### 암기 포인트

정보 보안 거버넌스 요건 다섯 가지를 키워드로 구분해 둔다. 전략적 연계=사업 전략과 일치, 위험 관리=위험을 줄이기 위한 체계 수립·관리, 가치 전달=투자 효과·교육·표준화, 자원 관리=지식·자원의 효율적 배분과 전사적 아키텍처, 성과 관리=모니터링·보고·평가 척도 운영.

NoteBase

**문 21. 「정보통신기반 보호법」 제8조제1항에서 규정하고 있는 주요정보통신기반시설 지정 기준에 해당하지 않는 것은?**

① 해당 정보통신기반시설을 관리하는 기관이 수행하는 업무의 국가 사회적 중요성

② 정보통신산업의 기반을 조성하기 위하여 산업입지의 조성 및 정보통신산업 기반시설의 지원

③ 다른 정보통신기반시설과의 상호연계성

④ 침해사고가 발생할 경우 국가안전 보장과 경제사회에 미치는 피해 규모 및 범위

**정답 2번**

**쟁점**

「정보통신기반 보호법」 제8조제1항은 중앙행정기관의 장이 소관 분야의 정보통신기반시설 중 전자적 침해행위로부터 보호가 필요한 시설을 '주요정보통신기반시설'로 지정할 때 고려하는 기준(각 호)을 열거한다. 이 문제는 그 법정 고려 기준에 '해당하지 않는' 선지를 고르는 부정형 문항이므로, 각 선지가 제8조제1항 각 호의 내용과 일치하는지를 대조하는 것이 핵심이다.

**용어 풀이**

주요정보통신기반시설: 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등 업무와 관련된 전자적 제어·관리 시스템 및 정보통신망 중, 전자적 침해행위로부터 보호가 필요하다고 인정되어 법에 따라 지정된 시설을 말한다.
전자적 침해행위: 정보통신기반시설을 대상으로 해킹·컴퓨터바이러스·논리폭탄·메일폭탄·서비스거부(DoS)·고출력 전자기파 등으로 침해하는 행위를 말한다.

**핵심 구분**

제8조제1항의 지정 고려 기준(각 호)은 '그 시설이 얼마나 중요하고, 침해될 경우 얼마나 위험한가'라는 보호 필요성 판단 요소들로 구성된다. 구체적으로 관리기관 업무의 국가사회적 중요성, 그 업무의 정보통신기반시설 의존도, 다른 정보통신기반시설과의 상호연계성, 침해사고 발생 시 국가안전보장·경제사회에 미치는 피해 규모 및 범위, 침해사고의 발생 가능성 또는 복구의 용이성이 기준이다. 반면 '정보통신산업 육성·산업입지 조성·산업기반시설 지원'은 산업 진흥 정책 목적의 사항으로, 보호 대상 지정 기준과 성격이 전혀 다르다.

NoteBase

### 선지별 해설

① O: 관리기관이 수행하는 업무의 국가 사회적 중요성은 제8조제1항 각 호에 명시된 지정 고려 기준이다.
② X: 정보통신산업의 기반 조성을 위한 산업입지 조성 및 정보통신산업 기반시설 지원은 산업 진흥 성격의 내용으로 제8조제1항의 지정 기준에 없다 → 지정 기준은 시설의 중요성·의존도·상호연계성·피해 규모·침해 가능성 및 복구 용이성이다. 이 선지가 정답이다.
③ O: 다른 정보통신기반시설과의 상호연계성은 제8조제1항 각 호에 명시된 지정 고려 기준이다.
④ O: 침해사고 발생 시 국가안전보장과 경제사회에 미치는 피해 규모 및 범위는 제8조제1항 각 호에 명시된 지정 고려 기준이다.

### 오답 포인트

②의 '정보통신산업', '산업입지 조성', '기반시설 지원' 같은 표현은 산업 육성·진흥 정책의 언어로, 침해로부터 시설을 보호하기 위한 '지정 기준'과는 목적 자체가 다르다. 나머지 세 선지는 모두 '중요성·연계성·피해'처럼 보호 필요성을 재는 요소여서 결이 같은데, ②만 홀로 산업 진흥 쪽으로 튀는 점을 포착하면 부정형 문항에서 빠르게 걸러낼 수 있다.

### 다시 나오면 이렇게 판단

제8조제1항 지정 기준을 묻는 변형이 나오면, 선지가 '이 시설이 얼마나 중요하고 침해되면 얼마나 위험한가'를 재는 보호 필요성 요소인지부터 확인한다. 산업 육성·지원·조성처럼 진흥 정책 냄새가 나는 선지는 지정 기준이 아니다. 실제 각 호에 포함되는 요소는 국가사회적 중요성, 정보통신기반시설 의존도, 상호연계성, 피해 규모 및 범위, 침해사고 발생 가능성 또는 복구 용이성 다섯 가지다.

### 암기 포인트

제8조제1항 지정 기준 5요소: 중요성(국가사회적 중요성), 의존도(업무의 시설 의존도), 연계성(다른 시설과 상호연계성), 피해규모(침해 시 국가안전·경제사회 피해 규모·범위), 발생·복구(침해 발생 가능성 또는 복구 용이성). '산업 진흥·산업입지·기반시설 지원'은 지정 기준이 아니라는 점을 함정 선지로 외워 둔다.

NoteBase

**문 22. TCSEC의 등급에 대한 설명으로 옳은 것은?**

① C2 등급에서는 레이블된 정보보호(labeled security)를 평가한다.

② D 등급에서는 검증된 정보보호(verified design)를 평가한다.

③ A1 등급에서는 최소한의 보호(minimal protection)만 가능하다.

④ A1, B1, B2, B3, C1, C2, D 등급으로 구분된다.

**정답 4번**

**출제 포인트**

TCSEC(Trusted Computer System Evaluation Criteria, 미 국방부 오렌지북)의 보안등급 체계와 각 등급이 요구하는 평가 항목을 정확히 짝지을 수 있는지를 묻는다. 등급의 개수·명칭과 각 등급의 핵심 특징이 서로 뒤바뀌어 제시되는 것이 이 유형의 전형적인 오답 함정이다.

**핵심 개념**

TCSEC은 신뢰도가 낮은 것부터 높은 것 순으로 D, C1, C2, B1, B2, B3, A1의 7개 등급으로 구분된다. D=최소한의 보호(Minimal Protection), C1=임의적 접근통제(Discretionary Security Protection), C2=통제된 접근보호(Controlled Access Protection), B1=레이블된 보안보호(Labeled Security Protection), B2=구조화된 보호(Structured Protection), B3=보안영역(Security Domain), A1=검증된 설계(Verified Protection/Verified Design)이다. 즉 '레이블(labeled)'은 B1의 특징이고, '검증된 설계(verified design)'는 A1의 특징이며, '최소한의 보호(minimal protection)'는 D의 특징이다.

**선지별 해설**

① X: '레이블된 정보보호(labeled security)'는 C2가 아니라 B1 등급의 평가 항목이다. C2는 통제된 접근보호(Controlled Access Protection)를 평가하는 등급이다.
② X: '검증된 정보보호(verified design)'는 D가 아니라 A1 등급의 특징이다. D 등급은 최소한의 보호만 제공하는 가장 낮은 등급이다.
③ X: '최소한의 보호(minimal protection)'는 A1이 아니라 D 등급의 특징이다. A1은 TCSEC 중 가장 신뢰도가 높은 최상위 등급으로 형식적 방법을 통한 검증된 설계를 요구한다.
④ O: TCSEC은 낮은 등급부터 D, C1, C2, B1, B2, B3, A1의 총 7개 등급으로 구분되며, 이는 A1·B1·B2·B3·C1·C2·D를 모아 놓은 것과 같은 집합이므로 옳은 설명이다.

**오답 포인트**

①②③은 모두 실제로 존재하는 TCSEC의 특징 문구(레이블된 보안, 검증된 설계, 최소한의 보호)를 가져오되 그 특징이 속한 등급을 서로 바꿔치기한 함정이다. 등급명과 특징 문구를 짝지어 외우지 않으면 그럴듯하게 보여 틀리기 쉽다.

NoteBase

**다시 나오면 이렇게 판단**

선지에 특정 등급명(D, C1, C2, B1, B2, B3, A1)과 영문 특징 문구(labeled security, verified design, minimal protection 등)가 짝지어 제시되면, 먼저 신뢰도 순서(D<C1<C2<B1<B2<B3<A1)를 떠올리고 각 등급의 대표 특징을 순서대로 대응시켜 맞는 조합인지 확인한다. 등급의 총 개수나 명칭 나열 자체를 묻는 선지는 7개 등급명이 모두 맞게 나열되어 있는지만 확인하면 된다.

**암기 포인트**

D(최소보호) - C1(임의적 접근통제) - C2(통제된 접근보호) - B1(레이블된 보안보호) - B2(구조화된 보호) - B3(보안영역) - A1(검증된 설계) 순으로 신뢰도가 높아진다. 'D는 바닥, A1은 정상(검증된 설계)'으로 양끝만 확실히 기억해도 함정 선지(②③)를 걸러낼 수 있다.

NoteBase

**문 23. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제23조의3에 따라 본인확인기관 지정을 위한 심사 사항으로 옳지 않은 것은?**

① 본인확인업무의 안전성 확보를 위한 물리적 · 기술적 · 관리적 조치계획

② 이동통신사업자의 본인확인업무 수행과 관련하여 이용자의 주민등록번호를 수집 · 이용하기 위한 계획

③ 본인확인업무 관련 설비규모의 적정성

④ 본인확인업무의 수행을 위한 기술적 · 재정적 능력

**정답 2번**

### 쟁점

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제23조의3(본인확인기관의 지정 등)은 방송통신위원회가 본인확인업무를 안전하고 신뢰성 있게 수행할 수 있는 자를 본인확인기관으로 지정할 때 심사해야 하는 사항을 정한다. 이 조항이 열거한 세 가지 심사 사항이 무엇인지, 그리고 그에 해당하지 않는 항목을 골라내는 것이 쟁점이다.

### 용어 풀이

본인확인기관: 주민등록번호를 대체하는 본인확인 수단(예: 아이핀, 휴대전화 본인확인 등)의 개발·제공·관리 업무, 즉 본인확인업무를 안전하게 수행할 수 있다고 인정되어 방송통신위원회로부터 지정받은 기관이다.
본인확인업무: 정보통신서비스 이용 시 주민등록번호를 대신하여 이용자 본인 여부를 확인해 주는 업무이다.

### 핵심 구분

제23조의3제1항이 정한 심사 사항은 세 가지로 한정된다. 첫째 본인확인업무의 안전성 확보를 위한 물리적·기술적·관리적 조치계획, 둘째 본인확인업무의 수행을 위한 기술적·재정적 능력, 셋째 본인확인업무 관련 설비규모의 적정성이다. 곧 안전성 조치계획·수행 능력·설비 적정성 세 축이 심사 대상이다. 반면 주민등록번호를 수집·이용하기 위한 계획은 심사 사항이 아니며, 오히려 본인확인 제도는 주민등록번호를 사용하지 않고 본인을 확인하는 대체수단을 전제로 하므로 방향 자체가 반대이다.

NoteBase

### 선지별 해설

① O: 본인확인업무의 안전성 확보를 위한 물리적·기술적·관리적 조치계획은 제23조의3제1항의 심사 사항에 해당한다.
② X: 이동통신사업자가 본인확인업무 수행과 관련하여 이용자의 주민등록번호를 수집·이용하기 위한 계획은 심사 사항에 포함되지 않는다. 본인확인기관 제도는 주민등록번호를 대체하는 수단의 안전한 운영을 목적으로 하므로, 주민등록번호 수집·이용 계획은 심사 항목이 될 수 없다(틀린 표현 '주민등록번호를 수집·이용하기 위한 계획' → 올바른 표현 '본인확인업무의 안전성·수행 능력·설비규모에 관한 사항').
③ O: 본인확인업무 관련 설비규모의 적정성은 제23조의3제1항의 심사 사항에 해당한다.
④ O: 본인확인업무의 수행을 위한 기술적·재정적 능력은 제23조의3제1항의 심사 사항에 해당한다.

### 오답 포인트

②의 문장이 '이동통신사업자', '본인확인업무 수행'처럼 관련 용어를 그럴듯하게 섞어 놓아 심사 사항처럼 보이지만, 핵심은 '주민등록번호를 수집·이용하기 위한 계획'이라는 부분이다. 본인확인 제도의 취지가 주민등록번호를 쓰지 않는 대체수단 제공이라는 점을 놓치면 ②를 옳은 선지로 오인하기 쉽다. 나머지 ①·③·④가 모두 실제 심사 사항이라는 점을 확인하면 소거법으로도 ②가 답임이 분명해진다.

### 다시 나오면 이렇게 판단

본인확인기관 지정 심사 사항을 묻는 문항은 '안전성 조치계획 / 수행을 위한 기술적·재정적 능력 / 설비규모의 적정성'이라는 세 가지 축을 기억하면 된다. 이 세 축에 들어가지 않거나, 특히 '주민등록번호 수집·이용'처럼 제도 취지에 정면으로 어긋나는 표현이 있는 선지가 있으면 그것이 옳지 않은 것이다.

### 암기 포인트

본인확인기관 지정 심사 3요소는 '안전성 조치계획 · 기술적·재정적 능력 · 설비규모 적정성'으로 외워 둔다. 본인확인 제도의 목적 자체가 주민등록번호를 대체하는 것이므로 '주민등록번호 수집·이용'이 들어간 선지는 심사 사항이 아니라는 점을 함께 기억한다.

NoteBase

**문 24. RADIUS에 대한 설명으로 옳은 것은?**

① 주로 서버/클라이언트 방식으로 동작한다.

② 분산형 접근 제어방식으로 인터넷을 이용하여 직접적으로 사용자를 인증하는 프로토콜이다.

③ 등록되지 않은 사용자를 인증한다.

④ 보안 강화를 위하여 TCP를 사용한다.

**정답 1번**

**출제 포인트**

RADIUS(Remote Authentication Dial-In User Service)의 동작 구조와 통신 방식에 대한 기본 이해를 묻는 문제이다. RADIUS는 원격 접속 사용자에 대한 인증·인가·계정관리(AAA)를 중앙집중식으로 처리하기 위한 프로토콜로, NAS(Network Access Server)와 RADIUS 서버 사이의 관계, 사용 프로토콜, 인증 대상의 범위를 정확히 구분해야 한다.

**핵심 개념**

RADIUS는 사용자가 원격 접속을 시도하면 NAS(클라이언트 역할)가 사용자의 인증 정보를 RADIUS 서버로 전달하고, 서버가 이를 검증하여 인증·인가 결과를 회신하는 서버/클라이언트 구조로 동작한다. 인증 정보는 중앙의 RADIUS 서버 하나에 등록된 사용자 데이터베이스를 기준으로 검증되므로 분산형 접근 제어가 아니라 중앙집중형 접근 제어에 해당한다. 또한 RADIUS는 전송 계층에서 UDP를 사용하며(포트 1812/1813 등), 신뢰성 있는 연결형 전송이 필요한 TCP를 사용하지 않는다.

**선지별 해설**

① RADIUS는 NAS가 클라이언트, RADIUS 서버가 서버 역할을 수행하며 사용자 인증 요청과 응답을 주고받는 서버/클라이언트 방식으로 동작한다 → 옳은 설명이다.
② RADIUS는 분산형이 아니라 중앙집중형 접근 제어 방식이며, 사용자가 인터넷을 통해 RADIUS 서버를 직접 인증하는 것이 아니라 NAS를 경유하여 인증이 이루어진다 → 틀린 표현 → 올바른 표현: 중앙집중형 접근 제어방식으로 NAS를 통해 간접적으로 사용자를 인증하는 프로토콜이다.
③ RADIUS는 사전에 등록된 사용자 정보를 기준으로 인증을 수행하므로 등록되지 않은 사용자는 인증에 실패한다 → 틀린 표현 → 올바른 표현: 등록된 사용자를 인증한다.
④ RADIUS는 전송 프로토콜로 TCP가 아닌 UDP를 사용한다 → 틀린 표현 → 올바른 표현: 보안 강화가 아닌 전송 효율을 위하여 UDP를 사용한다.

NoteBase

**오답 포인트**

②는 '분산형'이라는 표현과 '직접적으로 인증'이라는 표현 두 곳에서 함정을 만든다. RADIUS는 여러 NAS가 하나의 중앙 RADIUS 서버를 공유하는 중앙집중형 구조이고, 사용자는 NAS를 거쳐 간접적으로 인증받는다. ③은 인증 대상 범위를 반대로 뒤집은 오답이며, ④는 RADIUS가 UDP 기반이라는 사실과 반대로 서술한 오답이다.

**다시 나오면 이렇게 판단**

RADIUS 관련 문제는 (1) 서버/클라이언트 구조인지, (2) 중앙집중형인지 분산형인지, (3) 등록된 사용자만 인증하는지, (4) UDP를 쓰는지 TCP를 쓰는지 네 가지 축으로 선지를 점검하면 빠르게 정답을 가려낼 수 있다.

**암기 포인트**

RADIUS = 서버/클라이언트 구조 + 중앙집중형 접근 제어 + 등록된 사용자만 인증 + UDP 사용으로 정리해 둔다.

NoteBase

**문 25. 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」에서 규정하고 있는 인증 기준에 대한 설명으로 옳지 않은 것은?**

① 정보자산 식별: 조직의 업무 특성에 따라 정보자산 분류기준을 수립하여 관리체계 범위 내 모든 정보자산을 식별 · 분류하고 중요도를 산정한 후 그 목록을 최신으로 관리하여야 한다.

② 사용자 인증: 정보시스템과 개인정보 및 중요정보에 대한 사용자의 접근은 안전한 인증절차와 필요에 따라 강화된 인증방식을 적용하여야 한다. 또한 로그인 횟수 제한, 불법 로그인 시도 경고 등 비인가자 접근 통제방안을 수립 · 이행하여야 한다.

③ 원격접근 통제: 보호구역 이외 장소에서의 정보시스템 관리 및 개인정보 처리는 원칙으로 금지하고 재택근무 · 장애대응 · 원격협업 등 불가피한 사유로 원격접근을 허용하는 경우 책임자 승인, 접근 단말 지정, 접근 허용범위 및 기간 설정, 강화된 인증, 구간 암호화, 접속 단말 보안(백신, 패치 등) 등 보호대책을 수립 · 이행하여야 한다.

④ 사용자 계정 관리: 개인정보 및 주요정보 보호를 위하여 법적 요구사항을 반영한 암호화 대상, 암호 강도, 암호 사용 정책을 수립하고 개인정보 및 주요정보의 저장 · 전송 · 전달 시 암호화를 적용하여야 한다.

**정답 4번**

**쟁점**

「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」의 인증기준(ISMS-P 상세 통제항목) 각 항목의 이름과 그 항목이 요구하는 내용이 서로 맞게 짝지어졌는지를 묻는 문항이다. 각 선지는 실제 인증기준 항목의 요구사항 문구를 거의 그대로 옮긴 것이라, 항목명과 본문 내용의 대응이 어긋난 선지 하나를 찾는 것이 핵심이다.

**용어 풀이**

인증기준: ISMS-P(정보보호 및 개인정보보호 관리체계) 인증에서 조직이 충족해야 할 통제항목으로, 크게 관리체계 수립·운영 영역과 보호대책 요구사항 영역으로 나뉜다. 보호대책 요구사항에는 정보자산 관리, 사용자 계정 관리, 사용자 인증, 원격접근 통제, 암호정책 적용 등이 각각 별개 항목으로 규정되어 있다.

**핵심 구분**

사용자 계정 관리 = 계정과 접근권한의 생성·등록·변경 절차 수립과 최소권한 부여를 요구하는 항목이다. 반면 암호화 대상·암호 강도·암호 사용 정책 수립과 저장·전송·전달 시 암호화 적용은 별개 항목인 암호정책 적용의 요구사항이다. 두 항목의 이름과 내용을 서로 바꾸어 놓은 것이 이 문항의 함정이다.

NoteBase

### 선지별 해설

① O: 정보자산 관리 항목의 내용과 일치한다. 업무 특성에 따른 분류기준 수립, 범위 내 모든 정보자산의 식별·분류, 중요도 산정, 목록의 최신 유지는 정보자산 관리에서 요구하는 사항이다.
② O: 사용자 인증 항목의 내용과 일치한다. 안전한 인증절차와 필요 시 강화된 인증방식 적용, 로그인 횟수 제한과 불법 로그인 시도 경고 등 비인가자 접근 통제방안 수립·이행을 요구한다.
③ O: 원격접근 통제 항목의 내용과 일치한다. 보호구역 이외 장소에서의 관리·처리는 원칙적으로 금지하되, 불가피한 사유로 허용 시 책임자 승인·접근 단말 지정·허용범위 및 기간 설정·강화된 인증·구간 암호화·접속 단말 보안 등 보호대책 수립·이행을 요구한다.
④ X: 항목명은 '사용자 계정 관리'라고 되어 있으나 본문 내용은 암호화 대상·암호 강도·암호 사용 정책 수립과 저장·전송·전달 시 암호화 적용으로, 이는 '암호정책 적용' 항목의 요구사항이다. 사용자 계정 관리는 계정 및 접근권한의 생성·등록·변경 절차 수립과 최소권한 부여를 요구하는 항목이므로, 항목명과 내용의 대응이 어긋난다. '사용자 계정 관리: 암호화 대상·암호 강도·암호 사용 정책 수립…' → '암호정책 적용: 암호화 대상·암호 강도·암호 사용 정책 수립…'으로 짝지어야 옳다.

### 오답 포인트

④의 본문 자체는 실제 인증기준(암호정책 적용)에 그대로 나오는 정상적인 문구여서, 내용만 읽으면 맞는 설명처럼 보인다. 함정은 앞에 붙은 항목명이 바뀐 데 있다. 인증기준 문제는 '설명 내용의 진위'가 아니라 '항목명과 내용의 대응'으로 정답이 갈릴 수 있으므로, 각 선지의 콜론 앞 항목명과 콜론 뒤 요구사항을 분리해서 맞춰 보아야 한다.

### 다시 나오면 이렇게 판단

각 선지가 'A항목: (내용)' 형식으로 제시되면, 내용의 옳고 그름보다 먼저 그 내용이 원래 어느 인증기준 항목의 것인지를 떠올린다. 암호화 대상·강도·정책과 저장·전송 시 암호화 = 암호정책 적용, 계정·권한 생성/변경 절차와 최소권한 = 사용자 계정 관리, 인증절차·로그인 제한 = 사용자 인증으로 고정해 두면 이름 바꿔치기 선지를 바로 걸러낼 수 있다.

### 암기 포인트

ISMS-P 보호대책 항목 대응: 사용자 계정 관리=계정·권한 생성·변경·최소권한, 사용자 인증=인증절차·강화 인증·로그인 제한, 원격접근 통제=원칙 금지+예외 시 승인·단말 지정·구간 암호화, 암호정책 적용=암호화 대상·암호 강도·암호 정책 및 저장·전송·전달 시 암호화. 계정 관리와 암호정책을 헷갈리지 않도록 '계정=권한, 암호정책=암호화'로 묶어 외워 둔다.

NoteBase