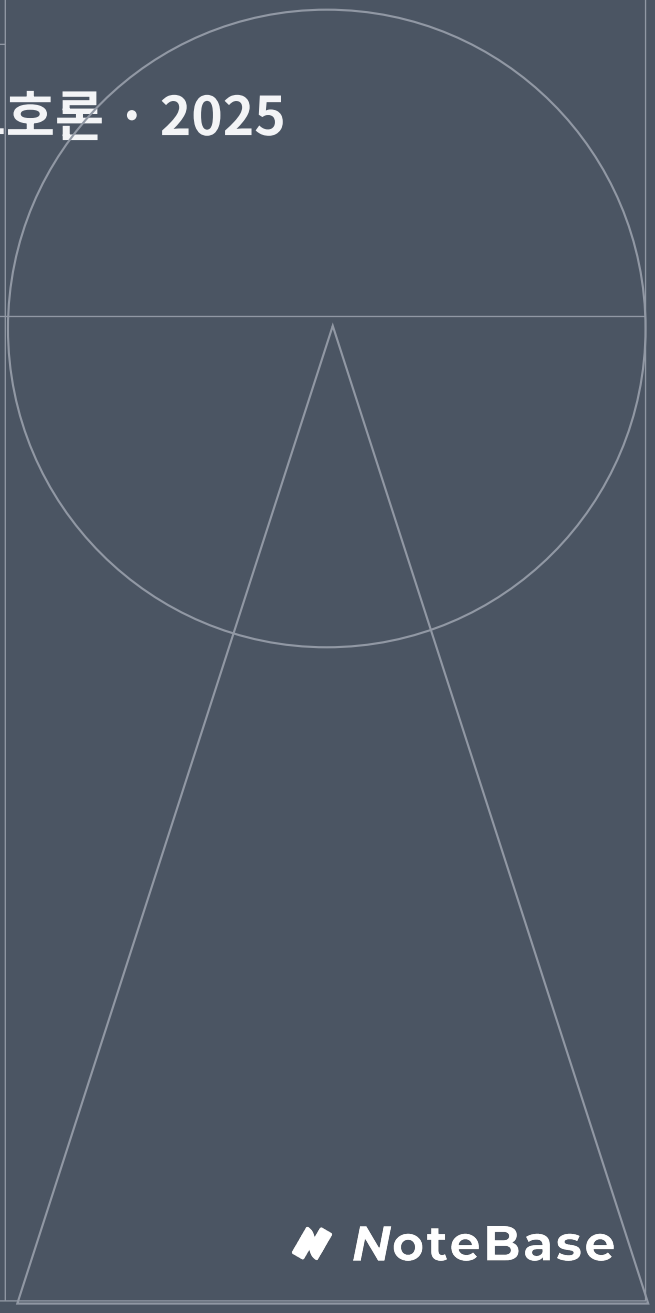
기출OX 해설집

공무원/군무원/9급 · 정보보호론 · 2025



NoteBase

기출OX 해설집

공무원/군무원/9급 · 정보보호론 · 2025

공무원/군무원/9급 · 정보보호론 · 2025

1. 2024년 7월 <가트너>는 AI하이프사이클 2024에서 소버린 AI를 2~5년 내 달성될 하이프 구역에 처음으로 배치하며 이 개념이 추상적인 것이 아니라 실제 비즈니스 측면에서 중요한 개념이라는 것을 확정했다. 다음 중 하이프사이클의 가로축(시간)에서 동원된 범주가 아닌 것은?
   ① 기대치 정점
   ② 환멸의 골짜기
   ③ 기술촉발 경사
   ④ 생산성의 고원

정답 3번

출제 포인트

가트너 하이프사이클을 구성하는 5단계의 명칭을 구별하는 문제이다.

핵심 개념

하이프사이클은 신기술에 대한 시장의 기대와 성숙 과정을 시간의 흐름에 따라 나타낸 모형이다. 단계는 혁신 촉발(Innovation Trigger) → 부풀려진 기대의 정점(Peak of Inflated Expectations) → 환멸의 골짜기(Trough of Disillusionment) → 계몽의 경사(Slope of Enlightenment) → 생산성의 고원(Plateau of Productivity) 순서로 진행된다.

NoteBase

선지별 해설

① O — 기대치 정점은 신기술에 대한 관심과 기대가 과도하게 높아지는 단계로, 하이프사이클의 범주에 해당한다. 보다 정확한 단계명은 '부풀려진 기대의 정점'이다.
② O — 환멸의 골짜기는 초기 기대에 미치지 못한 결과가 나타나 관심과 기대가 크게 낮아지는 단계로, 하이프사이클의 범주에 해당한다.
③ X — '기술촉발 경사'는 하이프사이클의 단계명이 아니다. 틀린 표현은 '기술촉발 경사'이며, 올바르게는 첫 단계인 '혁신 촉발'과 네 번째 단계인 '계몽의 경사'가 각각 별개의 범주이다.
④ O — 생산성의 고원은 기술의 실질적 효용이 인정되고 주류 채택이 확대되는 단계로, 하이프사이클의 범주에 해당한다.

오답 포인트

③은 실제 단계명에 쓰이는 '촉발'과 '경사'를 결합하여 그럴듯하게 만든 선택지이다. '촉발'은 첫 단계인 혁신 촉발에, '경사'는 네 번째 단계인 계몽의 경사에 속한다.

다시 나오면 이렇게 판단

하이프사이클 단계명을 묻는 경우 '촉발 → 정점 → 골짜기 → 경사 → 고원'의 흐름을 먼저 떠올리고, 서로 다른 단계의 단어를 섞은 명칭인지 확인한다.

암기 포인트

혁신 촉발 → 기대 정점 → 환멸 골짜기 → 계몽 경사 → 생산성 고원이다.

NoteBase

2. 해시값이 일치하는 다른 2개의 메시지를 찾기가 어렵다는 것을 의미하는 해시 함수의 특성으로 가장 적절한 것은?

① 역상 저항성 ② 비둘기집 원리

③ 약한 충돌 내성 ④ 강한 충돌 내성

정답 4번

출제 포인트

해시 함수의 역상 저항성, 약한 충돌 내성, 강한 충돌 내성을 공격자가 무엇을 미리 알고 있는지에 따라 구별하는 문제이다.

핵심 개념

역상 저항성: 주어진 해시값과 일치하는 입력 메시지를 찾기 어려운 성질이다.
약한 충돌 내성: 특정 메시지가 주어졌을 때 그 메시지와 해시값이 같은 다른 메시지를 찾기 어려운 성질이다.
강한 충돌 내성: 메시지가 미리 주어지지 않은 상태에서도 해시값이 같은 서로 다른 두 메시지를 찾기 어려운 성질이다.
핵심 대비는 '해시값이 주어짐 → 역상 저항성, 메시지 하나가 주어짐 → 약한 충돌 내성, 아무 메시지도 고정되지 않음 → 강한 충돌 내성'이다.

선지별 해설

① X — 역상 저항성은 주어진 해시값에 대응하는 입력 메시지 하나를 찾기 어렵다는 성질이다. '해시값이 일치하는 서로 다른 두 메시지를 찾기 어렵다'는 표현은 강한 충돌 내성으로 고쳐야 한다.
② X — 비둘기집 원리는 가능한 메시지 수가 해시값의 수보다 많으므로 충돌이 존재할 수밖에 없음을 설명하는 원리이지, 충돌 쌍을 찾기 어렵다는 보안 특성이 아니다. 해당 표현은 강한 충돌 내성으로 고쳐야 한다.
③ X — 약한 충돌 내성은 주어진 특정 메시지와 같은 해시값을 갖는 다른 메시지를 찾기 어렵다는 성질이다. 문제처럼 아무 메시지도 미리 고정하지 않고 해시값이 같은 두 메시지를 찾기 어렵다는 성질은 강한 충돌 내성이다.
④ O — 강한 충돌 내성은 해시값이 같은 서로 다른 두 메시지의 쌍을 찾는 것이 어렵다는 성질이므로 문제의 설명과 정확히 일치한다.

오답 포인트

③의 약한 충돌 내성과 ④의 강한 충돌 내성을 혼동하기 쉽다. 특정 메시지 하나가 먼저 주어지면 약한 충돌 내성이고, 특정 메시지의 지정 없이 충돌하는 임의의 두 메시지를 찾는 문제이면 강한 충돌 내성이다. 또한 비둘기집 원리는 충돌의 존재를 설명할 뿐, 충돌 탐색의 어려움을 뜻하지 않는다.

NoteBase

다시 나오면 이렇게 판단

공격자에게 주어진 대상을 먼저 확인한다. 해시값만 주어지면 역상 저항성, 메시지 하나가 주어지면 약한 충돌 내성, 아무 메시지도 고정하지 않고 같은 해시값의 두 메시지를 찾으면 강한 충돌 내성으로 판단한다.

암기 포인트

해시값에서 입력 찾기=역상, 주어진 메시지의 짝 찾기=약한 충돌, 임의의 충돌 쌍 찾기=강한 충돌이다.

NoteBase

3. 임의적 접근제어(DAC)에 대한 설명으로 가장 적절한 것은?
   ① 주체의 역할에 따라 다양한 접근 권한을 가질 수 있다.
   ② 객체 소유자가 해당 객체의 접근 통제 방법을 변경할 수 있다.
   ③ 주체와 객체 사이의 환경에 따라 동적 접근 권한 부여가 가능하다.
   ④ 중앙 집중적 접근제어 방식으로 모든 주체 및 객체에 대한 허용 등급을 설정해 주어야 한다.

정답 2번

출제 포인트

임의적 접근제어(DAC)에서 객체의 접근 권한을 결정·변경하는 주체가 누구인지, 다른 접근제어 방식과 구별할 수 있는지를 묻는 문제이다.

핵심 개념

임의적 접근제어(DAC)는 객체의 소유자가 자신의 재량으로 다른 주체의 접근 권한을 부여하거나 변경하는 방식이다.
역할 기반 접근제어(RBAC)는 사용자의 역할에 권한을 연결하고, 상황·속성 기반 접근제어는 주체·객체·환경의 속성이나 조건을 이용하며, 강제적 접근제어(MAC)는 중앙 정책과 보안등급에 따라 접근을 통제한다.

선지별 해설

① X — 틀린 표현은 '주체의 역할에 따라'이다. 이는 역할에 권한을 할당하는 RBAC의 특징이며, DAC는 객체 소유자의 재량에 따라 접근 권한을 정한다.
② O — DAC에서는 객체 소유자가 해당 객체에 대한 접근 권한을 부여하거나 회수하는 등 접근 통제 방법을 변경할 수 있다.
③ X — 틀린 표현은 '주체와 객체 사이의 환경에 따라 동적 접근 권한 부여'이다. 이는 환경 조건이나 속성을 평가하는 상황·속성 기반 접근제어의 설명이며, DAC는 객체 소유자의 재량을 기준으로 권한을 부여한다.
④ X — 틀린 표현은 '중앙 집중적' 및 '모든 주체 및 객체에 대한 허용 등급을 설정'이다. 이는 중앙 정책과 보안등급에 따르는 MAC의 특징이며, DAC는 객체 소유자가 자신의 객체에 대한 접근 권한을 정하는 분산적 방식이다.

NoteBase

오답 포인트

①의 '역할', ③의 '환경에 따라 동적', ④의 '중앙 집중적·허용 등급'은 각각 다른 접근제어 모델을 가리키는 핵심 단서이다. DAC의 '임의적'은 통제가 무작위라는 뜻이 아니라 객체 소유자의 재량에 맡긴다는 뜻이다.

다시 나오면 이렇게 판단

권한 결정 기준을 확인한다. 객체 소유자의 재량이면 DAC, 역할이면 RBAC, 환경·속성이면 상황·속성 기반 접근제어, 중앙 정책과 보안등급이면 MAC으로 판단한다.

암기 포인트

DAC는 소유자 재량, RBAC는 역할, MAC은 등급과 중앙 정책이다.

NoteBase

4. 온디바이스 AI 기술의 장점으로 가장 적절하지 않은 것은?
① 로컬 데이터 처리
② 개인정보 보호 및 보안
③ 속도와 반응성
④ 인터넷 의존성 심화

정답 4번

출제 포인트

온디바이스 AI가 데이터를 기기 내부에서 직접 처리할 때 나타나는 장점과 그 반대 특성을 구별하는 문제이다.

핵심 개념

온디바이스 AI는 데이터를 외부 서버로 보내지 않고 스마트폰·가전·차량 등 사용자 기기 자체에서 AI 연산을 수행하는 방식이다. 핵심 키워드는 로컬 처리, 개인정보 외부 전송 감소, 짧은 응답 시간, 오프라인 활용이며, 클라우드 중심 AI와 달리 인터넷 의존성을 낮출 수 있다.

선지별 해설

① O — 로컬 데이터 처리는 온디바이스 AI의 기본 특성이자 장점이다. 데이터와 연산을 기기 내부에서 처리하여 외부 서버로의 전송을 줄인다.
② O — 개인정보가 기기 밖으로 전송되는 범위를 줄일 수 있으므로 개인정보 보호와 보안 측면에서 유리하다. 다만 기기 자체의 보안 대책도 함께 필요하다.
③ O — 네트워크 왕복과 서버 응답을 기다리는 시간을 줄여 빠른 처리와 높은 반응성을 확보할 수 있다.
④ X — 틀린 표현은 '인터넷 의존성 심화'이다. 실제로는 기기 안에서 직접 추론할 수 있어 인터넷 연결 의존성이 완화되고, 지원되는 기능은 오프라인에서도 사용할 수 있다.

오답 포인트

AI는 모두 서버나 인터넷 연결이 필요하다고 생각하면 ④를 장점으로 오인하기 쉽다. 온디바이스 AI는 클라우드 AI와 달리 연산의 중심이 사용자 기기에 있으므로 인터넷 의존성을 높이는 것이 아니라 낮춘다.

다시 나오면 이렇게 판단

연산 위치가 '기기 내부'라는 점에서 출발한다. 외부 전송 감소는 개인정보 보호로, 네트워크 왕복 감소는 속도·반응성 향상으로, 기기 자체 처리는 인터넷 의존성 완화로 연결된다.

NoteBase

암기 포인트

온디바이스 AI는 로컬 처리·보호 강화·빠른 반응·인터넷 의존성 완화이다.

NoteBase

5. 사회구조변동과 메타버스의 영향에 대한 설명으로 가장 적절하지 않은 것은?
① NFT(Non Fungible Token) 혁신
② 정체성 혁신
③ 커뮤니케이션 혁신
④ 사회경제적 혁신

정답 1번

출제 포인트

메타버스가 사회의 정체성·소통 방식·경제활동을 변화시키는 영향과, 이를 구현하는 개별 기술을 구별하는 문제이다. '적절하지 않은 것'을 고르는 부정형 문항이다.

핵심 개념

정체성 혁신은 아바타와 디지털 자아를 통해 자신을 표현하고 관계를 형성하는 방식의 변화이다.
커뮤니케이션 혁신은 가상공간에서 실시간·몰입형으로 상호작용하고 협업하는 방식의 변화이다.
사회경제적 혁신은 가상 재화의 생산·거래, 새로운 직업과 시장의 형성처럼 경제활동 구조가 확장되는 변화이다.
NFT는 대체 불가능 토큰으로, 디지털 자산의 고유성과 소유 관계를 표시하는 기술·자산 수단이다. 따라서 NFT 자체를 정체성·커뮤니케이션·사회경제와 나란한 사회구조 변화의 범주로 보는 것은 적절하지 않다.

선지별 해설

① X — 'NFT 혁신'은 메타버스의 사회구조 변화 범주라기보다 디지털 자산의 고유성과 소유 관계를 구현하는 개별 기술·수단이다. 틀린 표현은 'NFT 혁신'이며, 올바르게는 'NFT는 메타버스의 디지털 자산 거래 등을 지원하는 기술적 수단'이다.
② O — 이용자는 아바타와 디지털 자아를 만들고 표현하면서 현실과 다른 방식으로 정체성을 구성할 수 있으므로 정체성 혁신에 해당한다.
③ O — 메타버스는 공간의 제약을 줄이고 아바타를 통한 실시간 상호작용·협업을 가능하게 하므로 커뮤니케이션 혁신에 해당한다.
④ O — 가상 재화와 서비스의 생산·소비·거래, 새로운 시장과 직업의 형성은 사회경제적 활동 구조를 변화시키므로 사회경제적 혁신에 해당한다.

오답 포인트

NFT가 메타버스에서 자주 활용된다는 이유만으로 이를 곧바로 사회구조 변화의 한 범주로 보기 쉽다. 그러나 ②~④는 사회의 정체성·소통·경제활동이 어떻게 달라지는지를 나타내고, ①은 그 변화에 활용될 수 있는 특정 기술을 가리킨다는 점이 다르다.

NoteBase

다시 나오면 이렇게 판단

선지가 사람의 정체성, 상호작용 방식, 경제활동 구조의 변화를 설명하는지 먼저 확인한다. 특정 플랫폼이나 토큰 기술 자체를 제시한 선지는 사회구조적 영향의 범주가 아니라 구현 수단인지 구별한다.

암기 포인트

메타버스의 사회구조 변화는 정체성·소통·사회경제의 변화이고, NFT는 이를 지원할 수 있는 개별 기술·자산 수단이다.

NoteBase

6. SHA-1 알고리즘의 처리되는 블록의 크기, 해시값의 크기를 순서대로 나열한 것은?
① 512 비트 - 160 비트
② 512 비트 - 256 비트
③ 1024 비트 - 256 비트
④ 1024 비트 - 512 비트

정답 1번

출제 포인트

SHA-1이 입력 메시지를 처리하는 블록의 크기와 최종 출력하는 해시값의 크기를 구분하는 문제이다.

핵심 개념

SHA-1은 입력 메시지를 패딩한 뒤 512비트 단위의 블록으로 처리하여 최종적으로 160비트 길이의 해시값을 출력하는 암호학적 해시 함수이다. 따라서 처리 블록 크기는 512비트이고 해시값 크기는 160비트이다.

선지별 해설

① O: 처리 블록 크기 512비트와 해시값 크기 160비트를 올바르게 나열하였다.
② X: '해시값 256비트'가 틀렸다. 올바르게는 처리 블록 크기 512비트, 해시값 크기 160비트이다.
③ X: '처리 블록 1024비트'와 '해시값 256비트'가 모두 틀렸다. 올바르게는 처리 블록 크기 512비트, 해시값 크기 160비트이다.
④ X: '처리 블록 1024비트'와 '해시값 512비트'가 모두 틀렸다. 올바르게는 처리 블록 크기 512비트, 해시값 크기 160비트이다.

오답 포인트

256비트 해시값을 출력하는 SHA-256이나 1024비트 블록을 사용하는 다른 SHA 계열 규격의 수치를 SHA-1과 혼동하기 쉽다. 이 문항에서는 알고리즘 이름이 SHA-1인지 먼저 확인해야 한다.

다시 나오면 이렇게 판단

암호학적 해시 함수의 규격을 묻는 문항에서는 '입력을 몇 비트씩 처리하는가'와 '최종 결과가 몇 비트인가'를 별개의 값으로 확인한다. SHA-1이면 블록 512비트, 출력 해시 160비트로 판단한다.

암기 포인트

SHA-1은 512비트씩 처리하고 160비트를 출력한다.

NoteBase

7. 무결성 확인 및 메시지 인증을 하는 기술로 고정 비트 길이의 출력을 위해 송신자와 수신자가 공유하는 키를 사용하는 것으로 가장 적절한 것은?

① MAC ② Hash

③ Digest ④ Cookie

정답 1번

출제 포인트

이 문제는 고정 길이 출력이라는 공통점만 보지 않고, 송신자와 수신자가 공유하는 비밀키를 사용하여 메시지의 무결성과 인증을 함께 제공하는 기술을 구별하는 문제이다.

핵심 개념

MAC(Message Authentication Code): 송신자와 수신자가 공유하는 비밀키와 메시지를 입력으로 하여 고정 길이의 인증값을 생성하는 기술이다. 수신자는 같은 키로 값을 확인하여 메시지의 변조 여부와 정당한 키 보유자가 생성했는지를 검증한다.
Hash: 메시지를 고정 길이의 해시값으로 변환하는 함수이다. 일반적인 해시 함수 자체는 공유 비밀키를 사용하지 않으므로 무결성 확인에는 활용되지만 송신자 인증까지 보장하지는 않는다.
Digest: 해시 함수를 적용하여 얻은 고정 길이의 결과값인 메시지 다이제스트를 뜻한다. 그 자체가 공유키 기반 인증 기술은 아니다.
Cookie: 웹 서버가 상태 관리 등을 위해 이용자의 브라우저에 저장하게 하는 데이터이다. 일반적인 쿠키는 메시지 인증 코드와 다른 개념이다.

선지별 해설

① O — MAC은 공유 비밀키와 메시지로 고정 길이의 인증값을 만들며, 이를 통해 메시지 무결성과 메시지 인증을 제공하므로 문제의 설명에 정확히 해당한다.
② X — 틀린 부분은 일반적인 Hash가 '송신자와 수신자가 공유하는 키를 사용하여 메시지를 인증한다'고 보는 것이다. 올바르게는 Hash는 보통 키 없이 고정 길이의 해시값을 생성하며, 공유키를 결합해 인증 기능을 제공하는 HMAC 등은 MAC의 한 방식이다.
③ X — 틀린 부분은 Digest를 '공유키를 사용하는 메시지 인증 기술'로 보는 것이다. 올바르게는 Digest는 해시 함수가 산출한 고정 길이의 결과값이며, 다이제스트만으로 송신자를 인증하지는 못한다.
④ X — 틀린 부분은 Cookie를 '무결성 확인과 메시지 인증을 위한 공유키 기반 기술'로 보는 것이다. 올바르게는 Cookie는 웹에서 상태 정보 등을 브라우저에 저장·전달하기 위한 데이터이고, 문제의 기술은 MAC이다.

NoteBase

오답 포인트

② Hash와 ③ Digest도 고정 길이 출력과 관련되므로 혼동하기 쉽다. 그러나 문제의 결정적 표현은 '송신자와 수신자가 공유하는 키'와 '메시지 인증'이다. 이 두 조건을 함께 만족하는 것은 MAC이다.

다시 나오면 이렇게 판단

고정 길이 출력만 제시되면 Hash를 검토하고, 공유 비밀키를 이용한 무결성 확인과 메시지 인증이 함께 제시되면 MAC으로 판단한다. 공개키 기반 전자서명과 달리 MAC은 송신자와 수신자가 같은 비밀키를 공유한다.

암기 포인트

Hash는 키 없이 해시값, Digest는 그 결과값, MAC은 공유키로 만드는 인증값이다.

NoteBase

8. 개인정보보호법에서 고정형 영상정보처리기기의 설치·운영 제한에 관한 설명으로 가장 적절하지 않은 것은?

① 누구든지 개인의 사생활을 현저히 침해할 우려가 있는 장소의 내부를 볼 수 있도록 고정형 영상정보처리기기를 설치·운영하여서는 아니 된다.

② 영상정보처리기기 운영자가 영상정보처리기기의 설치·운영에 관한 사무를 위탁하는 것은 불법으로 영상정보처리기기는 운영자가 직접 운영하여야 한다.

③ 영상정보처리기기를 설치·운영하는 자는 정보주체가 쉽게 인식할 수 있도록 설치 목적 및 장소, 촬영 범위 및 시간, 관리책임자의 연락처 등의 사항이 포함된 안내판을 설치하여야 한다.

④ 영상정보처리기기 운영자는 설치 목적과 다른 목적으로 영상정보처리기기를 임의로 조작하거나 다른 곳을 비춰서는 아니 되며, 녹음기능은 사용할 수 없다.

정답 2번

쟁점

이 문제는 개인정보 보호법상 고정형 영상정보처리기기의 설치·운영 제한에 관한 문제이다. 핵심은 사생활 침해 장소에서의 설치 금지, 안내판의 기재사항, 목적 외 조작·녹음 금지와 설치·운영 사무의 위탁 가능 여부를 구별하는 것이다.

용어 풀이

고정형 영상정보처리기기 = 일정한 공간에 설치되어 지속적 또는 주기적으로 사람이나 사물의 영상을 촬영하거나 이를 유·무선망으로 전송하는 장치이다. 대표적인 예가 CCTV이다.

NoteBase

핵심 구분

개인정보 보호법 제25조는 사생활을 현저히 침해할 우려가 있는 장소의 내부를 볼 수 있도록 고정형 영상정보처리기기를 설치·운영하는 것을 원칙적으로 금지한다. 설치·운영 시에는 안내판을 두어야 하고 목적 외 임의 조작·다른 곳 촬영 및 녹음기능 사용도 금지된다. 반면 설치·운영 사무의 위탁 자체는 금지되지 않으며, 운영자는 이를 위탁할 수 있다. 공공기관이 위탁하는 경우에는 대통령령이 정한 절차와 요건을 따라야 한다.

선지별 해설

① O
개인의 사생활을 현저히 침해할 우려가 있는 목욕실·화장실·발한실·탈의실 등의 내부를 볼 수 있도록 고정형 영상정보처리기기를 설치·운영하는 것은 원칙적으로 금지된다. 다만 법령에 근거하여 사람을 구금하거나 보호하는 교정시설 등 대통령령으로 정하는 시설에는 예외가 있다.

② X
개인정보 보호법 제25조 제8항은 고정형영상정보처리기기운영자가 설치·운영 사무를 위탁할 수 있다고 명시한다. 공공기관이 위탁할 때에는 대통령령상 절차와 요건을 지켜야 할 뿐, 위탁 자체가 불법인 것은 아니다.
틀린 표현: '사무를 위탁하는 것은 불법으로 운영자가 직접 운영하여야 한다.'
올바른 표현: '운영자는 설치·운영 사무를 위탁할 수 있으며, 공공기관이 위탁하는 경우에는 대통령령으로 정하는 절차 및 요건에 따라야 한다.'

③ O
안내판에는 설치 목적 및 장소, 촬영 범위 및 시간, 관리책임자의 연락처 등이 포함되어야 한다. 정보주체가 촬영 사실과 관리 주체를 쉽게 알 수 있게 하려는 규정이다.

④ O
운영자는 설치 목적과 다른 목적으로 기기를 임의로 조작하거나 다른 곳을 비춰서는 안 되며, 녹음기능도 사용할 수 없다. 이는 개인정보 보호법 제25조 제5항의 내용과 일치한다.

오답 포인트

'운영자에게 관리 책임이 있다'는 사실을 '반드시 직접 운영해야 한다'는 뜻으로 확대하면 ②를 놓치기 쉽다. 법은 위탁을 허용하되, 특히 공공기관의 위탁에는 별도의 절차와 요건을 부과한다.

다시 나오면 이렇게 판단

고정형 영상정보처리기기 문제에서는 장소, 안내, 기기 조작, 위탁을 나누어 판단한다. 사생활 침해 장소는 원칙적 설치 금지, 안내판은 목적·장소·범위·시간·연락처 표시, 목적 외 조작과 녹음은 금지, 설치·운영 사무의 위탁은 허용으로 정리한다.

NoteBase

암기 포인트

사생활 장소는 금지, 안내판은 필수, 목적 외 조작·녹음은 금지, 위탁은 가능이다.

NoteBase

9. 접촉하는 두 물체 사이에 반드시 흔적이 남는다는 교환법칙을 주장한 디지털 포렌식(Digital Forensic)의 이론적 기초를 제공한 학자는?

① Locard ② Whetstone
③ Scherbius ④ Worm

정답 1번

출제 포인트

접촉하는 두 물체 사이에는 반드시 물질이나 흔적의 교환이 일어난다는 원칙과 이를 제시한 인물을 연결하는 문제이다.

핵심 정리

Locard: 로카르의 교환법칙 — 모든 접촉은 흔적을 남긴다는 관점으로, 범죄 현장과 사람·물체 사이의 흔적을 수집하고 분석하는 포렌식의 이론적 토대가 된다.
Whetstone: 플레이페어 암호 — 두 글자씩 묶어 암호화하는 고전 암호 방식과 연결되는 인물이다.
Scherbius: 에니그마 — 회전자식 암호기인 에니그마를 개발한 인물이다.
Worm: 자기 복제 악성코드 — 사람이나 학자가 아니라 네트워크 등을 통해 스스로 복제·확산하는 악성코드 유형이다.

선지별 해설

① O — Locard는 접촉하는 두 대상 사이에 흔적이 상호 이전된다는 로카르의 교환법칙을 제시하였다. 디지털 포렌식에서도 행위와 접촉의 결과로 흔적이 남는다는 기본 관점으로 이어진다.
② X — Whetstone을 교환법칙의 제안자로 연결한 부분이 틀렸다. Whetstone은 플레이페어 암호와 연결되며, 교환법칙을 주장한 학자는 Locard이다.
③ X — Scherbius를 교환법칙의 제안자로 연결한 부분이 틀렸다. Scherbius는 에니그마 암호기를 개발한 인물이며, 교환법칙을 주장한 학자는 Locard이다.
④ X — Worm을 학자로 제시한 부분이 틀렸다. Worm은 자기 복제와 확산을 특징으로 하는 악성코드 유형이며, 교환법칙을 주장한 학자는 Locard이다.

출제자가 노린 함정

Whetstone과 Scherbius도 정보보호의 암호 분야에서 등장하는 이름이므로 혼동하기 쉽다. 그러나 '접촉', '교환', '흔적'이라는 표현은 암호가 아니라 로카르의 교환법칙을 가리킨다.

NoteBase

다시 나오면 이렇게 판단

문장에 '모든 접촉은 흔적을 남긴다' 또는 '두 물체 사이의 흔적 교환'이 제시되면 Locard를 선택한다. 암호기나 암호 방식이 언급되면 Whetstone·Scherbius와 구분한다.

암기 포인트

Locard = 접촉 → 교환 → 흔적이다.

NoteBase

10. CTR 블록암호 운용 모드에 대한 설명으로 가장 적절하지 않은 것은?
① OFB 모드와 같은 스트림 암호의 일종이다.
② 암호화 및 복호화에 병렬 처리가 가능하다.
③ 암호화와 복호화가 완전히 같은 구조는 아니다.
④ 비트 단위의 에러가 있는 암호문을 복호화하면 평문의 대응하는 비트만 에러가 난다.

정답 3번

출제 포인트

이 문제는 CTR 모드가 카운터 값을 암호화해 만든 키스트림과 데이터를 XOR하는 방식이라는 점을 바탕으로 병렬 처리, 암·복호화 구조, 오류 전파 특성을 구별하는 문제이다.

핵심 개념

CTR 모드는 서로 다른 카운터 블록을 블록암호의 암호화 함수에 넣어 키스트림을 만들고, 이를 평문 또는 암호문과 XOR하는 블록암호 운용 모드이다. 각 블록의 카운터를 독립적으로 처리하므로 병렬 처리가 가능하고, 암호화와 복호화 모두 같은 암호화 함수와 XOR 연산을 사용한다. 또한 암호문의 한 비트 오류는 복호화된 평문의 대응 비트에만 영향을 준다.

선지별 해설

① O — CTR은 블록암호 운용 모드이지만, OFB와 마찬가지로 생성한 키스트림을 데이터와 XOR하므로 스트림 암호처럼 동작한다.

② O — 각 블록에 서로 다른 카운터 값을 사용해 키스트림을 독립적으로 만들 수 있으므로 암호화와 복호화 모두 병렬 처리가 가능하다.

③ X — 틀린 표현은 '암호화와 복호화가 완전히 같은 구조는 아니다'이다. 실제로는 암호화와 복호화가 모두 카운터를 블록암호의 암호화 함수에 입력해 키스트림을 만든 뒤 데이터와 XOR하므로 구조가 같다.

④ O — CTR에서는 암호문의 특정 비트가 바뀌면 XOR 특성상 복호화된 평문의 대응 비트만 바뀌고 다른 비트로 오류가 전파되지 않는다.

NoteBase

오답 포인트

③에서 복호화라는 말만 보고 블록암호의 복호화 함수를 사용한다고 생각하기 쉽다. CTR의 복호화도 암호화 함수로 동일한 키스트림을 만든 뒤 암호문과 XOR한다.

다시 나오면 이렇게 판단

CTR은 '카운터를 암호화해 키스트림 생성 → 데이터와 XOR'으로 판단한다. 이 구조에서 병렬 처리 가능, 암·복호화 구조 동일, 암호문 비트 오류의 제한적 전파라는 성질이 함께 도출된다.

암기 포인트

CTR은 카운터 암호화, 양방향 XOR, 병렬 가능, 오류는 대응 비트에만 발생한다.

NoteBase

11. 키 공간(Key Space)이 가장 큰 것은?
① DES ② DES-EDE2
③ AES ④ SHA-256

정답 3번

출제 포인트

대칭키 암호 알고리즘의 키 공간 크기를 비교하고, 해시 함수의 출력 길이를 키 길이와 혼동하지 않는지를 묻는 문제이다.

핵심 개념

키 공간은 알고리즘에서 사용할 수 있는 서로 다른 키의 전체 집합이며, 키 길이가 n비트이면 일반적으로 가능한 키의 수는 2^n개이다.
DES는 유효 키 길이가 56비트이고, DES-EDE2는 서로 독립인 DES 키 2개를 사용하므로 명목상 키 길이가 112비트이다. AES는 128비트, 192비트, 256비트 키를 지원하므로 최대 키 공간이 가장 크다. SHA-256의 256은 키 길이가 아니라 해시 출력 길이 256비트를 뜻한다.

선지별 해설

① X — DES의 유효 키 길이는 56비트이므로 키 공간은 2^{56}개이다. 틀린 판단은 DES의 키 공간이 가장 크다는 것이며, 올바르게는 네 선지의 대칭키 암호 가운데 키 공간이 가장 작다.
② X — DES-EDE2는 서로 독립인 DES 키 2개를 사용하여 명목상 112비트의 키 공간을 갖지만, AES가 지원하는 최대 256비트 키 공간보다 작다. 틀린 판단은 DES-EDE2가 가장 크다는 것이며, 올바르게는 AES의 최대 키 공간이 더 크다.
③ O — AES는 128비트, 192비트, 256비트 키를 지원하므로 최대 256비트의 키 공간을 가지며 선지 중 가장 크다.
④ X — SHA-256은 고정된 비밀키를 사용하는 대칭키 암호가 아니라 256비트 해시값을 출력하는 해시 함수이므로, 여기서 256을 암호키 길이나 키 공간으로 볼 수 없다. 틀린 표현은 'SHA-256의 256은 키 길이'라는 판단이며, 올바르게는 해시 출력 길이이다.

오답 포인트

④의 '256'을 보고 AES-256과 같은 256비트 키로 오인하기 쉽다. SHA-256의 숫자는 출력되는 해시값의 길이이고, AES의 128·192·256은 지원하는 키 길이이다.

NoteBase

다시 나오면 이렇게 판단

먼저 선지가 비밀키를 사용하는 암호 알고리즘인지 확인한 다음 유효 키 길이를 비교한다. DES는 56비트, DES-EDE2는 명목상 112비트, AES는 최대 256비트이며, SHA-256의 256비트는 키가 아니라 출력 길이로 판단한다.

암기 포인트

DES 56, EDE2 112, AES 최대 256, SHA-256의 256은 해시 출력 길이이다.

NoteBase

12. 다음 보안 공격과 이를 방어하기 위한 보안 기술의 순서로 가장 적절한 것은?

공격자가 자신을 밥(BoB)이라고 속여 엘리스(Alice)에게 이메일을 보낸다.

① Repudiation – Hash
② Replay – Access Control
③ Sniffing – Cryptography
④ Masquerade – Digital Signature

정답 4번

출제 포인트

공격자가 다른 사용자로 신분을 위장해 메시지를 보내는 가장 공격과, 송신자의 신원을 검증하는 디지털 서명의 대응 관계를 묻는 문제이다.

핵심 개념

Masquerade(가장 공격): 공격자가 정당한 사용자로 위장하여 시스템에 접근하거나 메시지를 보내는 공격이다. 키워드는 신분 위장이다.
Digital Signature(디지털 서명): 송신자의 개인키로 생성한 서명을 공개키로 검증하여 송신자 인증, 메시지 무결성, 부인방지를 제공하는 기술이다.
Replay(재전송 공격): 가로챈 정상 메시지를 나중에 다시 보내는 공격이며, 난수·타임스탬프·순서번호 등으로 막는다.
Sniffing(스니핑): 통신 내용을 몰래 엿듣는 공격이며, 통신 내용을 암호화하여 기밀성을 보호한다.
Repudiation(부인): 행위자가 자신이 한 송신이나 행위를 나중에 부인하는 것이며, 디지털 서명은 이에 대한 부인방지 수단이 된다.

NoteBase

선지별 해설

① X — Repudiation은 자신이 수행한 행위를 부인하는 것이지만, Hash만으로는 누가 해시값을 만들었는지 증명할 수 없어 부인방지를 제공하지 못한다. 틀린 표현은 ‘Hash’이며, 올바르게는 ‘Repudiation - Digital Signature’이다.
② X — Replay는 이미 전송된 정상 메시지를 가로채 다시 보내는 공격이다. Access Control은 자원에 대한 접근 권한을 제한하는 기술이므로 재전송 여부를 직접 판별하는 대응 기술이 아니다. 틀린 표현은 ‘Access Control’이며, 올바르게는 ‘Replay - 난수·타임스탬프·순서번호를 이용한 재전송 방지’이다.
③ X — Sniffing은 통신 내용을 엿듣는 공격이고 암호화는 그 내용을 알아보지 못하게 하는 적절한 일반적 방어이다. 그러나 제시된 상황은 통신 내용을 엿들은 것이 아니라 밥으로 신분을 위장해 메일을 보낸 것이므로 공격 유형이 Sniffing이 아니다. 틀린 표현은 이 사례에 대한 ‘Sniffing - Cryptography’이며, 사례에 맞게 고치면 ‘Masquerade - Digital Signature’이다.
④ O — 공격자가 자신을 밥이라고 속여 앨리스에게 이메일을 보냈으므로 Masquerade에 해당한다. 디지털 서명을 검증하면 메일이 밥의 개인키로 서명되었는지 확인할 수 있으므로 송신자 위장을 방어하는 데 적절하다.

오답 포인트

③의 Sniffing과 Cryptography는 일반적인 공격·방어 관계만 보면 자연스럽지만, 문제의 사례에는 도청이 없다. ‘밥이라고 속여’라는 행위가 가장 공격을 결정하는 핵심 단서이다. 또한 해시는 무결성 확인에는 쓰이지만 그 자체만으로 송신자 인증이나 부인방지를 보장하지 않는다.

다시 나오면 이렇게 판단

다른 사람인 척하면 Masquerade, 정상 메시지를 다시 보내면 Replay, 통신 내용을 엿보면 Sniffing, 자신의 행위를 부인하면 Repudiation으로 구분한다. 송신자 신원 검증이 핵심이면 Digital Signature를 대응시킨다.

암기 포인트

신분 위장 = Masquerade, 서명으로 신원 확인 = Digital Signature이다.

NoteBase

13. 제로 트러스트 아키텍처의 핵심 원칙에 대한 설명으로 가장 적절하지 않은 것은?

① 사용자, 장치를 기본적으로 신뢰하지 않으며 접속 요청 시마다 엄격한 검증을 수행한다.

② 사용자는 반드시 필요한 자원에 대해서만 최소한의 권한으로 접근할 수 있도록 정책이 설정된다.

③ 조직의 내부 네트워크를 신뢰 구역, 외부를 비신뢰 구역으로 나누고 외부 침입에 대한 강력한 인증을 수행한다.

④ 인증 후에도 세션 동안 사용자 행동, 장비 상태, 네트워크 위치 등을 지속적으로 감시하여 이상 징후를 탐지한다.

정답 3번

출제 포인트

제로 트러스트 아키텍처의 핵심인 명시적 검증, 최소 권한, 위치와 무관한 불신, 지속적 감시를 구별하는 문제이다.

핵심 개념

제로 트러스트는 사용자·장치·네트워크 위치를 기본적으로 신뢰하지 않고, 자원 접근마다 신원과 상태 등을 검증하여 필요한 범위에서만 권한을 부여하는 보안 모델이다.
핵심은 '내부이므로 신뢰'가 아니라 '항상 검증'이며, 인증 이후에도 세션과 행위를 계속 관찰한다. 네트워크 분리는 내부 전체를 신뢰 구역으로 만드는 것이 아니라 침해 확산 범위를 줄이는 세분화 방식으로 활용된다.

NoteBase

선지별 해설

① O — 사용자와 장치를 기본적으로 신뢰하지 않고 각 접근 요청의 신원, 장치 상태, 맥락 등을 엄격히 확인하는 것은 명시적 검증 원칙에 부합한다.

② O — 필요한 자원에 필요한 수준으로만 접근을 허용하는 최소 권한 원칙에 부합한다. 권한의 범위와 지속 시간을 제한하면 계정이나 장치가 침해되었을 때 피해 범위를 줄일 수 있다.

③ X — 틀린 표현은 '조직의 내부 네트워크를 신뢰 구역'으로 정하는 부분이다. 제로 트러스트는 내부와 외부라는 네트워크 위치만으로 신뢰를 부여하지 않는다. 올바르게는 내부·외부를 불문하고 모든 접근 주체와 요청을 검증하며, 네트워크 세분화로 침해의 확산을 제한한다고 해야 한다.

④ O — 최초 인증만으로 세션 전체를 신뢰하지 않고 사용자 행동, 장비 상태, 네트워크 위치 등의 변화를 지속적으로 감시하는 것은 지속적 검증과 이상 징후 탐지 원칙에 부합한다.

오답 포인트

③은 '외부 침입에 대한 강력한 인증'이라는 맞는 표현에 '내부는 신뢰한다'는 전통적 경계 보안 관점을 섞었다. 제로 트러스트에서는 내부에 있다는 사실 자체가 신뢰의 근거가 되지 않는다.

다시 나오면 이렇게 판단

선지에 내부망·인증 완료·기존 접속자라는 이유만으로 지속적인 신뢰를 부여하는 내용이 있으면 제로 트러스트 원칙에 어긋나는 것으로 판단한다. 접근 때마다 검증, 최소 권한, 위치와 무관한 통제, 지속적 감시는 제로 트러스트의 핵심 기준이다.

암기 포인트

제로 트러스트는 '내부도 예외 없이 검증, 권한은 최소로, 인증 후에도 계속 감시'이다.

NoteBase

14. Oracle DBMS 설치 시 자동 생성되며, 시스템 데이터 사전의 모든 객체를 소유하는 기본 관리자 계정으로 가장 적절한 것은?

① DBA ② SYS

③ SYSMAN ④ SYSTEM

정답 2번

출제 포인트

Oracle의 기본 관리자 계정 가운데 시스템 데이터 사전 객체의 소유자가 누구인지 묻는 문제이다.

핵심 개념

SYS는 Oracle 설치 시 생성되는 핵심 관리자 계정이며 데이터 사전의 기본 테이블과 뷰 등 주요 시스템 객체를 소유한다. SYSTEM도 기본 관리 계정이지만 일반적인 데이터베이스 관리 작업을 담당하며 데이터 사전의 소유자는 아니다. DBA는 계정명이 아니라 여러 관리 권한을 묶은 사전 정의 역할이고, SYSMAN은 Oracle Enterprise Manager 관리에 사용되는 계정이다.

선지별 해설

① X — DBA는 시스템 데이터 사전 객체를 소유하는 계정이 아니라 데이터베이스 관리 권한을 묶어 둔 역할이다. 틀린 표현은 '기본 관리자 계정'이며, 올바르게는 '사전 정의된 관리자 역할'이다.
② O — SYS는 Oracle 설치 시 자동 생성되는 핵심 관리자 계정으로, 시스템 데이터 사전의 주요 객체를 소유한다.
③ X — SYSMAN은 Oracle Enterprise Manager의 관리 기능을 위한 계정이지 시스템 데이터 사전의 소유자가 아니다. 틀린 표현은 '데이터 사전의 모든 객체를 소유하는 기본 관리자 계정'이며, 올바르게는 'Enterprise Manager 관리용 계정'이다.
④ X — SYSTEM은 Oracle 설치 시 생성되는 기본 관리자 계정이지만 데이터 사전 객체의 소유자는 SYS이다. 틀린 표현은 '시스템 데이터 사전의 모든 객체를 소유한다'이며, 올바르게는 '일반적인 데이터베이스 관리 작업에 사용하는 관리자 계정'이다.

오답 포인트

SYS와 SYSTEM이 모두 기본 관리자 계정이라는 점 때문에 ④를 고르기 쉽다. 그러나 선지의 결정적 표현은 '시스템 데이터 사전의 객체를 소유'이며, 이 소유자는 SYS이다. 또한 DBA는 이름이 관리자처럼 보이지만 사용자 계정이 아니라 역할이다.

NoteBase

다시 나오면 이렇게 판단

‘데이터 사전 소유자’를 물으면 SYS, ‘일반 관리 작업용 기본 계정’을 물으면 SYSTEM, ‘관리 권한의 묶음’을 물으면 DBA 역할로 구분한다.

암기 포인트

데이터 사전의 주인은 SYS, 일반 관리 계정은 SYSTEM, 권한 묶음은 DBA이다.

NoteBase

15. ios 모바일 환경에서 클라이언트 측 인젝션으로부터 애플리케이션을 보호하기 위한 대응 방안으로 가장 적절하지 않은 것은?
① 자바스크립트와 플러그인 지원이 Web Views를 사용하지 않는지 확인한다.
② SQLite 인젝션에서 쿼리를 설계할 때 사용자가 입력한 값이 매개변수화된 쿼리에 전달되도록 해야 한다.
③ NSFileManager 콜에 대해 입력값 유효성 검증을 수행한다.
④ XML 인젝션에서 NSXMLParser 대신 LibXML2를 사용한다.

정답 1번

출제 포인트

이 문제는 iOS 애플리케이션에서 입력값이 해석기나 파일·데이터 처리 API로 전달될 때 적용하는 클라이언트 측 인젝션 방어 방법을 구분하는 문제이다.

핵심 개념

클라이언트 측 인젝션은 신뢰할 수 없는 입력이 SQL, JavaScript, 파일 경로, XML 등의 명령이나 구조로 해석되어 의도하지 않은 동작을 일으키는 취약점이다. 핵심 방어는 외부 입력을 실행 구문과 분리하고, 사용 지점에 맞게 검증·정제하며, 더 안전한 API와 파서를 선택하는 것이다.

NoteBase

선지별 해설

① X
틀린 표현은 '자바스크립트와 플러그인 지원이 Web Views를 사용하지 않는지 확인한다'이다. 이는 iOS의 Web View 기반 JavaScript 인젝션을 막는 직접적인 입력 통제가 아니다. 올바르게는 Web View에 신뢰할 수 없는 내용을 표시하기 전에 입력값을 검증·정제하고, 허용할 문자·URL·콘텐츠만 통과시키며, 불필요한 스크립트 실행 기능은 제한해야 한다. 따라서 가장 적절하지 않은 대응이다.

② O
사용자 입력을 SQL 문자열에 직접 이어 붙이지 않고 매개변수화된 쿼리의 값으로 전달하면 입력값이 SQL 명령 구조로 해석되는 것을 막을 수 있다. 즉 쿼리문과 데이터를 분리하는 올바른 SQLite 인젝션 대응이다.

③ O
NSFileManager 호출에 사용되는 파일명이나 경로를 검증하면 경로 조작을 통한 비인가 파일 접근과 로컬 파일 포함 위험을 줄일 수 있다. 허용된 디렉터리와 파일 형식의 범위 안에 있는 값인지 확인하는 것이 올바른 대응이다.

④ O
문항에서 제시한 iOS XML 인젝션 대응 기준에서는 NSXMLParser 대신 libxml2를 사용하는 것이 더 안전한 파서 선택에 해당한다. 다만 파서 교체만으로 끝나는 것은 아니며, 신뢰할 수 없는 XML 입력의 메타문자를 검증·이스케이프하고 외부 엔터티 처리도 제한해야 방어가 완성된다.

오답 포인트

①은 Web View와 JavaScript라는 보안 관련 용어가 들어 있어 그럴듯하지만, 선지의 확인 대상이 입력값 검증이나 스크립트 실행 제한으로 연결되지 않는다. 반면 ②는 SQL 구문과 값의 분리, ③은 파일 경로 입력 검증, ④는 XML 파서 선택이라는 구체적인 공격 지점별 대응이다.

다시 나오면 이렇게 판단

인젝션 대응 선지는 '외부 입력이 어느 해석기로 들어가는가'를 먼저 찾는다. SQL은 매개변수화, Web View는 렌더링 전 입력 검증·정제와 실행 기능 제한, 파일 API는 경로 검증, XML은 안전한 파서 설정과 메타문자·외부 엔터티 통제로 연결하면 된다.

암기 포인트

SQL은 값 분리, Web View는 렌더링 전 검증, 파일은 경로 검증, XML은 안전한 파서와 입력 통제이다.

NoteBase

16. 개인정보보호법 제4조에 명시된 정보주체자의 권리로 가장 적절하지 않은 것은?
① 개인정보의 처리에 관한 정보를 제공받을 권리
② 개인정보의 자동 수집 기능을 무조건 거부할 권리
③ 개인정보의 처리 여부를 확인하고 개인정보에 대하여 열람을 요구할 권리
④ 개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리

정답 2번

쟁점

이 문제는 개인정보 보호법 제4조가 열거한 정보주체의 권리에 관한 문제이다. 핵심은 법이 보장하는 선택·결정권과 법에 없는 무조건적 거부권을 구별하는 것이다.

용어 풀이

정보주체는 처리되는 개인정보로 알아볼 수 있는 사람으로서 그 정보의 주인이 되는 사람이다.

핵심 구분

개인정보 보호법 제4조는 처리 정보의 제공을 받을 권리, 동의 여부와 동의 범위 등을 선택·결정할 권리, 처리 여부 확인 및 열람·전송 요구권, 처리 정지·정정·삭제·파기 요구권, 피해구제권, 완전히 자동화된 개인정보 처리에 따른 결정의 거부·설명 요구권을 규정한다. 동의 여부를 선택할 권리는 개인정보의 자동 수집 기능을 어떠한 경우에도 무조건 거부할 권리와 같지 않다.

선지별 해설

① O — 개인정보의 처리에 관한 정보를 제공받을 권리는 개인정보 보호법 제4조에 명시되어 있다.
② X — 제4조는 개인정보의 자동 수집 기능을 무조건 거부할 권리를 규정하지 않는다.
틀린 표현: '개인정보의 자동 수집 기능을 무조건 거부할 권리'
올바른 표현: '개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리'이다.
③ O — 정보주체는 개인정보의 처리 여부를 확인하고 자신의 개인정보에 대한 열람을 요구할 권리가 있다.
④ O — 정보주체는 개인정보 처리에 관한 동의 여부와 동의 범위 등을 선택하고 결정할 권리가 있다.

오답 포인트

②의 '무조건'이 함정이다. 법은 동의 여부와 범위를 선택·결정할 권리를 보장하지만, 이를 모든 자동 수집 기능에 대한 예외 없는 거부권으로 규정하지 않는다.

NoteBase

다시 나오면 이렇게 판단

정보주체의 권리를 묻는 문제에서는 제공받기, 동의 선택·결정, 확인·열람·전송, 정지·정정·삭제·파기, 피해구제, 자동화된 결정의 거부·설명 요구라는 제4조의 권리 묶음과 선지의 표현을 대조한다. '무조건', '모든 경우'처럼 범위를 과도하게 넓힌 표현은 조문에 실제로 있는지 확인한다.

암기 포인트

정보주체의 권리는 '정보 제공 — 동의 선택 — 확인·열람·전송 — 정지·정정·삭제·파기 — 피해구제 — 자동화 결정 거부·설명'으로 정리한다.

NoteBase

17. 보안 솔루션에 대한 설명으로 가장 적절한 것은?
① DRM: 모든 패킷에 대한 패턴을 분석하고 정상 패킷이 아닌 트래픽을 차단한다.
② VPN: 문서의 열람, 편집 등의 세부 접근 권한을 설정하여 통제할 수 있다.
③ IPS: 인터넷 회선을 전용선과 같은 용도로 사용할 수 있게 한다.
④ SIEM: 다양한 IT시스템 및 보안 시스템의 로그 분석을 통해 이상 징후를 파악하고 보고할 수 있다.

정답 4번

출제 포인트

DRM, VPN, IPS, SIEM이 각각 무엇을 보호하고 어떤 방식으로 작동하는지를 구별하는 문제이다.

핵심 개념

DRM: 디지털 콘텐츠의 이용 권한과 복제·열람·편집 등을 통제하는 기술이다. 키워드는 콘텐츠 권한 관리이다.
VPN: 공용 인터넷에 암호화된 가상 통신 경로를 만들어 사설망처럼 안전하게 연결하는 기술이다. 키워드는 암호화 터널이다.
IPS: 네트워크 트래픽을 감시하여 침입이나 악성 행위를 탐지하고 차단하는 시스템이다. 키워드는 침입 탐지·차단이다.
SIEM: 여러 IT·보안 시스템의 로그와 이벤트를 통합 수집·분석하여 이상 징후를 탐지하고 보고하는 체계이다. 키워드는 로그 통합 분석이다.

NoteBase

선지별 해설

① X
‘모든 패킷에 대한 패턴을 분석하고 정상 패킷이 아닌 트래픽을 차단한다’는 설명은 DRM의 기능이 아니다. DRM은 디지털 콘텐츠의 열람·편집·복제·배포 등 이용 권한을 관리한다. 패킷을 분석하여 공격성 트래픽을 탐지·차단하는 기능은 IPS에 해당한다.

② X
‘문서의 열람, 편집 등의 세부 접근 권한을 설정하여 통제한다’는 설명은 VPN의 기능이 아니다. 이는 콘텐츠 이용 권한을 관리하는 DRM에 해당한다. VPN은 공용 인터넷상에 암호화 터널을 구성하여 안전한 사설망 연결을 제공한다.

③ X
‘인터넷 회선을 전용선과 같은 용도로 사용할 수 있게 한다’는 설명은 IPS의 기능이 아니다. 이는 공용 인터넷을 사설망처럼 이용하게 하는 VPN에 해당한다. IPS는 네트워크 침입을 실시간으로 탐지하고 악성 트래픽을 차단한다.

④ O
SIEM은 다양한 IT 시스템과 보안 장비의 로그 및 이벤트를 통합 분석하여 이상 징후를 파악하고 경보·보고할 수 있으므로 적절한 설명이다.

오답 포인트

각 선지는 보안 솔루션의 이름과 기능을 서로 바꾸어 놓았다. 특히 ①의 패킷 분석·차단은 IPS, ②의 문서 이용 권한 통제는 DRM, ③의 인터넷 기반 사설망 연결은 VPN의 기능이다. ④만 SIEM의 핵심인 여러 시스템의 로그 통합 분석을 정확히 설명한다.

다시 나오면 이렇게 판단

보호 대상과 동작을 함께 확인한다. 콘텐츠 권한은 DRM, 암호화된 가상 사설망은 VPN, 침입 트래픽의 탐지·차단은 IPS, 여러 시스템의 로그 통합 분석은 SIEM으로 판단한다.

암기 포인트

DRM은 권한, VPN은 터널, IPS는 침입 차단, SIEM은 로그 통합이다.

NoteBase

18. 블록체인을 구성하는 주요 기술로 가장 적절하지 않은 것은?
① 비대칭 암호화
② 하이퍼 프록시(Hyper Proxy)
③ P2P 커뮤니케이션 프로토콜
④ 작업증명(PoW)

정답 2번

출제 포인트

블록체인을 구성하는 핵심 기술인 암호 기술, P2P 네트워크, 합의 알고리즘을 서로 구별하는 문제이다.

핵심 개념

블록체인은 여러 참여자가 P2P 네트워크에서 원장을 공유하고, 암호 기술로 거래의 진위와 무결성을 확인하며, 합의 알고리즘으로 기록할 블록을 결정하는 분산원장 기술이다. 비대칭키 기반 전자서명은 거래 주체와 서명의 진위를 검증하고, P2P 프로토콜은 중앙 서버 없이 데이터와 블록을 전파하며, 작업증명은 참여 노드들이 유효한 블록에 합의하도록 하는 대표적 합의 방식이다.

선지별 해설

① O — 비대칭 암호 기술은 공개키와 개인키를 이용한 전자서명과 검증에 활용되므로 블록체인의 주요 기반 기술에 해당한다.

② X — '하이퍼 프록시(Hyper Proxy)'는 블록체인을 구성하는 일반적인 핵심 기술이 아니다. 틀린 표현인 '하이퍼 프록시'는 '해시 함수와 같은 암호 기술'로 고치면 적절하다. 해시 함수는 블록과 거래 데이터의 변경 여부를 확인하고 블록들을 연결하는 데 이용된다.

③ O — P2P 커뮤니케이션 프로토콜은 중앙 서버 없이 노드들이 거래와 블록 정보를 직접 주고받게 하므로 블록체인의 분산 네트워크를 구성하는 주요 기술이다.

④ O — 작업증명(PoW)은 계산 작업을 먼저 완료한 참여자가 블록을 제안하고 다른 노드가 이를 검증하게 하는 대표적인 합의 알고리즘이므로 주요 기술에 해당한다. 다만 모든 블록체인이 작업증명을 사용하는 것은 아니다.

오답 포인트

②의 '하이퍼'라는 표현을 블록체인 플랫폼인 하이퍼레저(Hyperledger)와 혼동하기 쉽다. 하이퍼 프록시는 비대칭키, P2P, 합의 알고리즘처럼 블록체인의 보편적인 구성 원리를 나타내는 용어가 아니다.

NoteBase

다시 나오면 이렇게 판단

선지가 거래의 인증·무결성을 위한 암호 기술, 노드 간 직접 통신을 위한 P2P, 원장 상태를 일치시키는 합의 알고리즘 가운데 하나에 해당하는지 판단한다. 이 세 기능과 직접 관련되지 않은 프록시 용어는 핵심 구성 기술에서 제외한다.

암기 포인트

블록체인의 세 축은 암호, P2P, 합의이다. 프록시는 핵심 축이 아니다.

NoteBase

19. 능동적 공격으로 가장 적절하지 않은 것은?
① 사회공학
② DoS/DDoS
③ 세션 하이재킹(Session Hijacking)
④ 스니핑(Sniffing)

정답 4번

출제 포인트

능동적 공격과 수동적 공격을 공격자의 개입 방식에 따라 구분하는 문제이다.

핵심 개념

능동적 공격: 공격자가 시스템이나 통신 과정에 적극적으로 개입하여 데이터를 변조하거나 세션을 탈취하고 서비스 운영을 방해하는 공격이다. 키워드는 개입·변조·탈취·방해이다.
수동적 공격: 시스템이나 통신 내용을 몰래 관찰·수집하지만 데이터나 시스템 상태를 직접 변경하지 않는 공격이다. 키워드는 도청·감청·관찰이다.
능동적 공격은 대상에 변화를 일으키는 공격이고, 수동적 공격은 들키지 않게 정보를 엿보는 공격이다.

선지별 해설

① O — 사회공학은 공격자가 사람에게 직접 접근하여 속이거나 심리를 조종해 정보 제공 또는 특정 행동을 유도하므로 능동적 공격에 해당한다.
② O — DoS/DDoS는 대량의 요청이나 트래픽으로 시스템 자원을 고갈시켜 정상적인 서비스 제공을 방해하므로 대표적인 능동적 공격이다.
③ O — 세션 하이재킹은 정상 사용자의 세션 식별 정보나 연결을 탈취하여 해당 세션에 개입하는 공격이므로 능동적 공격이다.
④ X — 스니핑은 네트워크를 흐르는 패킷을 몰래 가로채 내용을 관찰·수집하는 방식으로, 통신 내용을 직접 변조하거나 서비스를 방해하지 않는 수동적 공격이다. 틀린 표현은 스니핑을 능동적 공격의 예로 본 부분이며, 올바르게는 '스니핑은 수동적 공격에 해당한다'이다.

오답 포인트

스니핑도 불법적으로 정보를 얻는 공격이므로 '능동적'이라고 생각하기 쉽다. 그러나 능동·수동의 구분 기준은 공격의 위험성이나 불법성 여부가 아니라 대상 시스템이나 통신 상태에 직접 개입하여 변화를 일으키는지 여부이다.

NoteBase

다시 나오면 이렇게 판단

변조·세션 탈취·서비스 방해처럼 대상에 직접 개입하면 능동적 공격으로, 패킷 감청처럼 내용을 관찰·수집하는 데 그치면 수동적 공격으로 판단한다.

암기 포인트

능동은 바꾸고 방해하며, 수동은 몰래 엿본다. 스니핑은 수동적 공격이다.

NoteBase

20. ISMS-P의 보호대책 요구사항 인증영역으로 가장 적절하지 않은 것은?
① 암호화 적용
② 외부자 보안
③ 정보주체 권리보호
④ 시스템 및 서비스

정답 3번

출제 포인트

ISMS-P 인증기준 중 '보호대책 요구사항'에 속하는 분야와 '개인정보 처리단계별 요구사항'에 속하는 분야를 구별하는 문제이다.

핵심 개념

ISMS-P 인증기준은 관리체계 수립 및 운영, 보호대책 요구사항, 개인정보 처리단계별 요구사항으로 구분된다. 보호대책 요구사항은 조직이 정보자산과 시스템을 보호하기 위해 적용하는 관리적·물리적·기술적 통제를 다루며, 외부자 보안·암호화 적용·시스템 및 서비스 운영관리·시스템 및 서비스 보안관리 등이 포함된다. 정보주체 권리보호는 개인정보 열람·정정·삭제·처리정지 등 정보주체의 권리 보장과 관련된 분야이므로 개인정보 처리단계별 요구사항에 속한다.

선지별 해설

① O — 암호화 적용은 보호대책 요구사항의 2.7 분야로, 중요정보의 저장·전송 시 기밀성과 안전성을 확보하는 통제이다.
② O — 외부자 보안은 보호대책 요구사항의 2.3 분야로, 외부 인력이나 외부 서비스 이용에 따른 보안 위험을 관리한다.
③ X — 정보주체 권리보호는 보호대책 요구사항이 아니다. 틀린 표현은 '보호대책 요구사항 인증영역'이라는 분류이며, 올바르게는 '개인정보 처리단계별 요구사항의 3.5 분야'이다. 따라서 가장 적절하지 않은 선지이다.
④ O — 시스템 및 서비스 관련 통제는 보호대책 요구사항의 2.9 시스템 및 서비스 운영관리와 2.10 시스템 및 서비스 보안관리에 포함된다.

오답 포인트

③의 '정보주체 권리보호'도 넓은 의미에서는 보호 활동처럼 보이지만, ISMS-P의 공식 분류에서는 일반 보안 통제가 아니라 개인정보 처리단계별 요구사항에 배치된다. 일상적 의미가 아니라 인증기준의 대분류와 세부 분야 번호로 판단해야 한다.

NoteBase

다시 나오면 이렇게 판단

암호화·접근통제·외부자·물리 보안·시스템 운영처럼 정보자산과 시스템을 지키는 통제는 보호대책 요구사항으로 판단한다. 개인정보의 수집·이용·제공·파기 또는 정보주체의 권리에 관한 항목은 개인정보 처리단계별 요구사항으로 판단한다.

암기 포인트

보호대책은 시스템과 정보자산의 보안 통제, 정보주체 권리보호는 개인정보 처리단계의 권리 보장이다.

NoteBase

21. 검색엔진의 검색을 피하기 위해 특정 파일에 들어가는 필드에 대한 설명 중 가장 적절하지 않은 것은?
① User-agent: googlebot(구글 검색엔진이 검색하는 것을 막기 위해 사용)
② Disallow: dbconn.ini(dbconn.ini를 검색하지 못하게 하기 위해 robots.ini 파일에 입력함)
③ User-agent: *(모든 검색로봇의 검색을 막기 위해 입력하는 것)
④ Disallow: /admin/(admin 디렉터리에 접근하지 못하게 입력하는 것)

정답 2번

출제 포인트

검색로봇의 크롤링 범위를 정하는 robots.txt 파일에서 User-agent와 Disallow의 역할 및 올바른 경로 표기를 구별하는 문제이다.

핵심 개념

robots.txt는 검색로봇에게 어떤 URL을 크롤링해도 되는지 알리는 규칙 파일이다.
User-agent는 규칙을 적용할 검색로봇을 지정하며, googlebot은 Google 검색로봇을, *는 모든 검색로봇을 뜻한다.
Disallow는 해당 검색로봇이 크롤링하지 않도록 요청할 URL 경로를 지정한다. 경로는 /로 시작하며, 설정 파일의 이름은 robots.ini가 아니라 robots.txt이다.

선지별 해설

① O — User-agent: googlebot은 뒤에 이어지는 Disallow 규칙을 Googlebot에 적용하겠다는 뜻이다. 이 지시어로 Google 검색로봇을 지정한 뒤 차단할 경로를 설정할 수 있다.
② X — 틀린 표현은 Disallow: dbconn.ini와 robots.ini이다. 올바르게는 robots.txt 파일에 Disallow: /dbconn.ini와 같이 /로 시작하는 URL 경로를 적어야 한다.
③ O — User-agent: *는 뒤에 이어지는 규칙을 모든 검색로봇에 적용하겠다는 뜻이다. 따라서 모든 검색로봇의 크롤링 범위를 제한할 때 사용하는 지정 방식이다.
④ O — Disallow: /admin/은 현재 User-agent로 지정된 검색로봇에게 /admin/ 아래의 URL을 크롤링하지 않도록 요청하는 올바른 경로 표기이다. 다만 이는 서버의 실제 접근 권한을 차단하는 보안 설정은 아니다.

NoteBase

오답 포인트

②는 확장자 ini가 반복되어 그럴듯해 보이지만, 검색로봇 규칙 파일의 정확한 이름은 robots.txt이다. 또한 Disallow에는 단순 파일명이 아니라 /로 시작하는 URL 경로를 적는다는 점이 함정이다.

다시 나오면 이렇게 판단

User-agent에서는 적용 대상을 확인하고, Disallow에서는 /로 시작하는 제한 경로인지 확인한다. 마지막으로 규칙이 들어가는 파일명이 robots.txt인지 확인하면 된다.

암기 포인트

User-agent는 로봇 지정, Disallow는 /경로 제한, 파일명은 robots.txt이다.

NoteBase

22. 디지털 포렌식에 의해 확보된 자료가 법정에서 증거로 효력을 가지기 위한 원칙 중 가장 적절하지 않은 것은?
① 정당성(Legitimacy)의 원칙
② 무결성(Integrity)의 원칙
③ 재현(Reproducibility)의 원칙
④ 지속성(Continuity)의 원칙

정답 4번

출제 포인트

디지털 포렌식으로 확보한 자료가 법정에서 증거능력과 신뢰성을 인정받기 위해 지켜야 할 기본 원칙을 구별하는 문제이다.

핵심 개념

정당성(Legitimacy): 적법한 권한과 절차에 따라 증거를 수집·분석해야 한다는 원칙이다.
무결성(Integrity): 증거가 수집된 뒤 보관·분석·제출되는 전 과정에서 변경되거나 훼손되지 않았음을 보장하는 원칙이다. 해시값 비교 등이 이를 확인하는 대표적 방법이다.
재현성(Reproducibility): 같은 자료에 같은 분석 절차와 조건을 적용하면 동일한 결과를 다시 얻을 수 있어야 한다는 원칙이다.
연계보관성(Chain of Custody): 증거를 누가 언제 어디서 인수·보관·이송·분석했는지 전 과정을 기록하여 증거의 동일성과 관리 연속성을 입증하는 원칙이다.

선지별 해설

① O — 정당성의 원칙은 적법한 권한과 절차에 따른 증거 수집을 요구하므로 법정에서 증거로 쓰이기 위한 원칙에 해당한다.
② O — 무결성의 원칙은 원본 증거가 수집 이후 변조·훼손되지 않았음을 보장하므로 증거의 신뢰성을 뒷받침한다.
③ O — 재현성의 원칙은 동일한 조건과 절차에서 같은 분석 결과가 나와야 함을 뜻하므로 분석 결과의 객관적 검증에 필요하다.
④ X — '지속성(Continuity)'은 디지털 증거의 법적 효력을 위한 일반적인 기본 원칙의 명칭으로 보기 어렵다. 틀린 표현은 '지속성의 원칙'이며, 올바르게는 증거의 취급 이력을 끊김 없이 기록하는 '연계보관성(Chain of Custody)의 원칙'이라고 해야 한다.

NoteBase

오답 포인트

④의 Continuity를 증거 관리가 계속 이어진다는 일상적 의미로 받아들이면 정식 원칙처럼 보일 수 있다. 그러나 핵심은 단순한 '지속'이 아니라 증거의 수집부터 법정 제출까지 취급자·시간·장소·절차를 기록하는 연계보관성이다.

다시 나오면 이렇게 판단

선지의 용어를 증거 효력의 구체적 요구와 연결한다. 적법한 수집은 정당성, 변조 방지는 무결성, 동일 결과의 반복 검증은 재현성, 취급 이력의 기록은 연계보관성으로 판단한다. 구체적 요구와 연결되지 않는 임의의 명칭은 부적절한 선지로 본다.

암기 포인트

적법하게 수집하고(정당성), 바뀌지 않게 지키며(무결성), 다시 해도 같아야 하고(재현성), 누가 다뤘는지 이어서 기록한다(연계보관성).

NoteBase

23. 생성형 AI에 대한 설명으로 가장 적절하지 않은 것은?

① 환각 성향은 검증되지 않은 데이터 사용, 생성된 답변의 타당도를 포함함으로써 적절히 제어될 것이다.

② AI가 초래할 수 있는 최악의 위험을 완화하기 위한 규제와 도구가 생겨날 것이다.

③ AI는 카메라나 마이크와 같은 기기로부터 직접 학습해 인간이 만든 콘텐츠에 대한 의존도를 점차 낮출 것이다.

④ AI는 사용 중에도 끊임없이 학습할 수 있을 것이다.

정답 1번

출제 포인트

생성형 AI의 환각, 위험 완화, 멀티모달 학습, 지속 학습에 관한 설명을 구분하고 환각을 줄이는 방법을 판단하는 문제이다.

핵심 개념

환각은 생성형 AI가 사실과 다르거나 근거가 부족한 내용을 그럴듯하게 만들어 내는 현상이다. 검증되지 않은 데이터와 답변의 그럴듯함은 환각을 억제하는 장치가 아니라 오히려 오류를 사실처럼 보이게 할 수 있는 요인이다. 환각을 줄이려면 검증된 데이터, 신뢰할 수 있는 근거와의 연결, 사실 확인, 인간의 검토 등이 필요하다.

NoteBase

선지별 해설

① X — 검증되지 않은 데이터를 사용하는 것을 환각 통제 방법으로 제시한 부분이 틀리다. 검증되지 않은 데이터는 잘못된 정보를 학습하거나 생성하게 할 수 있으므로 환각 위험을 높인다. 생성된 답변의 타당도와 사실성을 확인하는 절차 자체는 환각 완화에 도움이 될 수 있으며, 검증된 데이터와 신뢰할 수 있는 근거를 사용하고 사실 확인과 인간의 검토를 거쳐야 한다.
② O — AI가 초래할 수 있는 중대한 위험을 줄이기 위해 안전 기준과 규제, 위험 평가, 필터링·모니터링 같은 기술적 도구가 마련될 수 있다는 설명은 적절하다.
③ O — 카메라나 마이크에서 얻은 시각·음성 정보를 직접 처리하고 학습하는 멀티모달 AI가 발전하면, 사람이 미리 작성한 텍스트 콘텐츠에만 의존하는 정도가 낮아질 수 있다는 설명은 적절하다.
④ O — 사용 과정에서 새 데이터와 피드백을 반영하는 지속 학습·적응형 학습이 발전하면 AI가 운용 중에도 성능을 갱신할 수 있다는 설명은 적절하다.

오답 포인트

①은 '타당도'라는 긍정적으로 들리는 표현으로 함정을 만든다. 그러나 답변의 개연성이나 그럴듯함은 사실의 정확성과 다르며, 검증되지 않은 데이터까지 사용하면 환각 통제에 역행한다.

다시 나오면 이렇게 판단

환각 대책을 묻는 선지에서는 데이터와 근거가 검증되었는지, 생성 결과를 사실 확인하는 절차가 있는지를 먼저 본다. '그럴듯한 답변'이나 '검증되지 않은 데이터'를 통제 방법으로 제시하면 부적절한 설명으로 판단한다.

암기 포인트

환각은 그럴듯함이 아니라 사실성의 문제이다. 검증된 근거와 사실 확인이 핵심이다.

NoteBase

24. 스탠퍼드 대학과 구글 연구팀은 3단계를 통해 인간과 유사한 AI 에이전트를 구현하고자 했다. 3단계로 가장 적절하지 않은 것은?
① 기억(Memory)과 검색(Retrieval)
② 반영(Reflection)
③ 사고의 연결고리(Chain-of-Thought)
④ 계획(Planning)

정답 3번

출제 포인트

인간과 유사한 AI 에이전트를 구현하기 위해 제시된 세 단계와, 일반적인 추론 기법을 구별하는 문제이다.

핵심 개념

기억과 검색은 경험을 저장하고 현재 상황에 필요한 기억을 불러오는 단계이다. 반영은 축적된 기억을 종합하여 더 높은 수준의 통찰이나 결론을 만드는 단계이다. 계획은 기억과 반영 결과를 바탕으로 앞으로의 행동을 구성하는 단계이다. 따라서 세 단계는 기억·검색, 반영, 계획으로 정리된다.

선지별 해설

① O — 기억(Memory)과 검색(Retrieval)은 에이전트가 경험을 저장하고 현재 판단에 관련된 기억을 찾아 활용하게 하므로 세 단계에 포함된다.
② O — 반영(Reflection)은 여러 기억을 종합해 일반화된 통찰을 형성하게 하므로 세 단계에 포함된다.
③ X — 사고의 연결고리(Chain-of-Thought)는 중간 추론 과정을 이어 가는 일반적인 추론 기법을 뜻하며, 이 연구가 제시한 세 단계 중 하나가 아니다. 틀린 표현은 '사고의 연결고리'이며, 올바르게는 세 단계를 '기억·검색, 반영, 계획'으로 정리한다.
④ O — 계획(Planning)은 기억과 반영 결과를 토대로 미래 행동의 순서와 방향을 세우는 단계이므로 세 단계에 포함된다.

오답 포인트

③의 사고의 연결고리는 AI의 인간 유사 추론과 관련된 익숙한 용어이므로 연구의 구성 단계처럼 보이기 쉽다. 그러나 이 문항은 AI 기법 전반이 아니라 해당 연구가 제시한 세 단계만을 묻는다.

다시 나오면 이렇게 판단

연구 모형의 구성 요소를 묻는 문항에서는 일반적으로 관련 있어 보이는 AI 용어를 고르지 않고, 제시된 모형의 고유한 구성인 기억·검색, 반영, 계획에 해당하는지를 확인한다.

NoteBase

암기 포인트

기억을 꺼내고, 반영해 통찰을 만들고, 계획해 행동한다.

NoteBase

25. 시스템 해킹에 사용되는 취약점으로 가장 적절하지 않은 것은?
① 패스워드 터미널
② 버퍼 오버플로
③ 동적 포맷 스트링
④ 레이스 컨디션

정답 1번

출제 포인트

시스템 해킹에 이용되는 대표적인 소프트웨어 취약점과 취약점이 아닌 용어를 구별하는 문제이다.

핵심 개념

시스템 취약점은 메모리 경계 검사, 입력 형식 처리, 동시 실행 순서와 같은 구현상의 결함으로 인해 공격자가 비정상 동작이나 권한 상승을 유발할 수 있는 약점이다. 버퍼 오버플로는 버퍼 경계를 넘는 쓰기, 포맷 스트링은 외부 입력의 서식 문자열 사용, 레이스 컨디션은 실행 시점과 순서에 따른 상태 불일치가 핵심이다.

선지별 해설

① X — '패스워드 터미널'은 버퍼 오버플로와 같은 표준적인 시스템 취약점 명칭이 아니다. 패스워드 관련 취약점을 뜻하려면 '약한 패스워드' 또는 '기본 패스워드 방치'처럼 공격 가능한 결함 상태로 표현해야 한다. 따라서 가장 적절하지 않은 선지이다.
② O — 버퍼 오버플로는 정해진 버퍼 크기를 넘어서 데이터를 기록하여 인접 메모리나 제어 흐름을 훼손하는 취약점이다. 공격자는 이를 악용해 비정상 종료, 임의 코드 실행, 권한 상승 등을 시도할 수 있다.
③ O — 포맷 스트링 취약점은 사용자 입력을 검증하지 않고 출력 함수의 서식 문자열로 사용할 때 발생한다. 공격자가 서식 지정자를 조작하면 메모리 내용을 읽거나 특정 위치에 값을 기록할 수 있다.
④ O — 레이스 컨디션은 둘 이상의 작업 결과가 실행 시점이나 순서에 따라 달라지는 동시성 취약점이다. 검사 시점과 사용 시점 사이의 상태 변화를 악용하면 권한 검사를 우회하거나 보호된 자원에 접근할 수 있다.

오답 포인트

문제가 '취약점'과 '공격에 관련된 듯한 용어'를 섞고, 부정형으로 가장 적절하지 않은 것을 묻는다는 점이 함정이다. ②~④는 각각 메모리 경계, 입력 형식, 실행 순서의 결함을 가리키지만 ①은 취약점의 명칭이나 결함 상태를 나타내지 않는다.

NoteBase

다시 나오면 이렇게 판단

각 용어가 공격 가능한 구체적 결함을 나타내는지 확인한다. 메모리 경계 위반은 버퍼 오버플로, 서식 문자열 오용은 포맷 스트링, 동시 실행 순서의 문제는 레이스 컨디션으로 연결하고, 단순 장치명이나 불명확한 표현은 취약점과 구별한다.

암기 포인트

경계 초과는 버퍼 오버플로, 서식 오용은 포맷 스트링, 순서 경쟁은 레이스 컨디션이다.

NoteBase