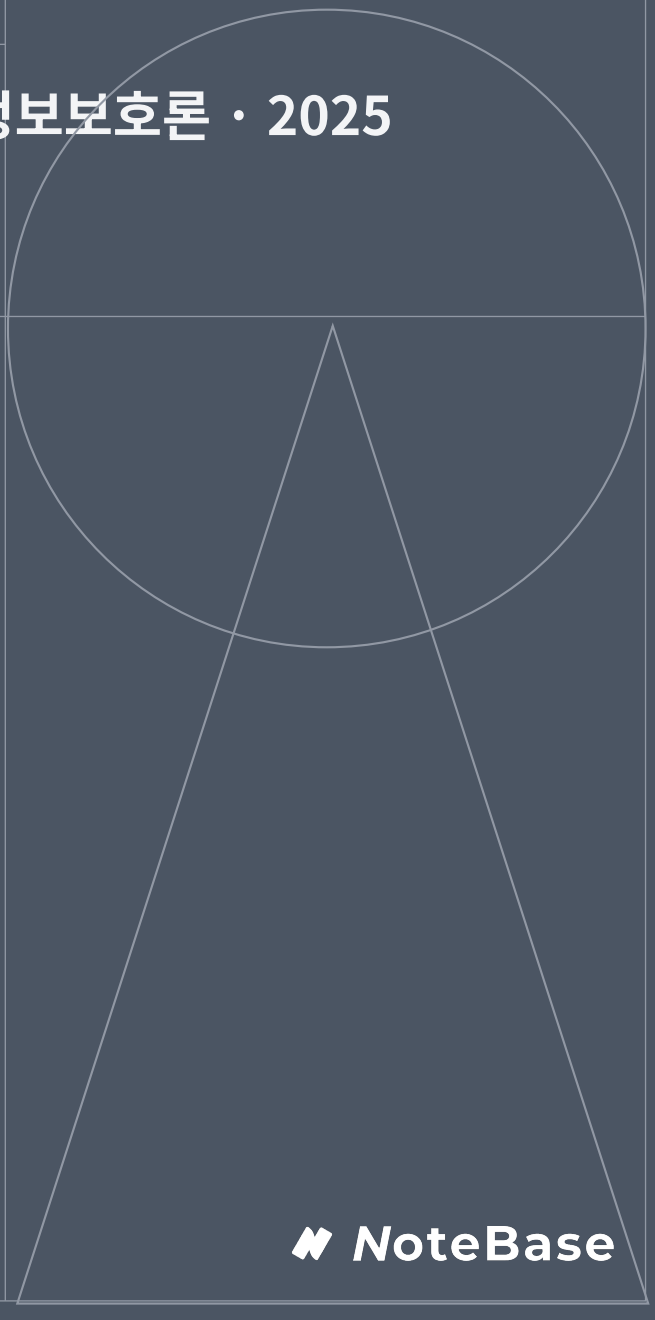
기출OX 해설집

공무원/경찰/공채(경위) · 정보보호론 · 2025



NoteBase

기출OX 해설집

공무원/경찰/공채(경위) · 정보보호론 · 2025

공무원/경찰/공채(경위) · 정보보호론 · 2025

문 1. 암호 알고리즘에 관한 설명으로 옳은 것만을 모두 고른 것으로 가장 적절한 것은?

가. 공개키 암호는 대칭키 암호보다 키 관리가 용이하다.
나. 대칭키 암호는 공개키 암호보다 암호화 속도가 빠르다.
다. AES는 암호화와 복호화를 위해 서로 다른 키를 사용한다.
라. 3DES는 128, 192, 256비트 길이를 갖는 3개의 키를 사용한다.

① 가, 나
② 다, 라
③ 가, 나, 다
④ 가, 나, 라

정답 1번

간단한 해설

공개키 암호는 **비밀키의 사전 분배 부담**을 줄이고, 대칭키 암호는 일반적으로 **대량 데이터 암호화가 빠르다**.
AES는 같은 비밀키로 암호화·복호화하며, 128·192·256비트는 3DES가 아니라 AES의 키 길이이다.

NoteBase

보기별 해설

가. O: 공개키 암호는 각 사용자가 공개키와 개인키의 쌍을 가지며, 공개키는 다른 사람에게 알려 줄 수 있다. 모든 사용자 쌍마다 비밀키를 안전하게 공유해야 하는 대칭키 방식과 비교하면 **비밀키의 사전 분배 부담이 작다**. 다만 공개키가 실제 상대방의 것인지 인증하는 절차는 필요하다.

나. O: 대칭키 암호는 일반적으로 공개키 암호보다 연산 부담이 작아 **대량 데이터의 암호화 속도가 빠르다**. 따라서 실제 통신에서는 공개키 방식으로 대칭키를 안전하게 설정하고, 본문 데이터는 대칭키 방식으로 암호화하는 구성을 많이 사용한다.

다. X: AES는 대칭키 블록 암호이므로 암호화와 복호화에 **같은 비밀키**를 사용한다. 공개키와 개인키처럼 서로 다른 키를 쓰는 비대칭키 암호와 구별된다.

라. X: 128·192·256비트는 **AES가 지원하는 키 길이**이다. 3DES는 DES 연산을 세 번 적용하며, 각 DES 키의 유효 길이는 56비트이다. 세 개의 서로 독립적인 DES 키를 쓰는 방식의 키 재료는 총 168비트이며, 이는 세 키가 각각 128·192·256비트라는 뜻이 아니다.

따라서 옳은 보기는 가, 나이며, 이에 해당하는 선택지는 ①이다.

NoteBase

문 2. 해시 함수(Hash Function)에 관한 설명으로 옳은 것만을 모두 고른 것으로 가장 적절한 것은?

가. 어느 메시지의 해시값이 주어졌을 때 그 해시값을 갖는 다른 메시지를 발견하는 것이 매우 곤란한 성질을 강한 충돌 내성이라고 한다.
나. 해시값으로부터 입력 메시지를 역으로 계산하는 것은 불가능해야 한다.
다. 입력 메시지가 다르면 생성되는 해시값도 달라야 하는 특성을 가져야 한다.

① 가, 나
② 가, 다
③ 나, 다
④ 가, 나, 다

정답 3번

간단한 해설

가의 설명은 **약한 충돌 내성**에 해당한다. 강한 충돌 내성은 특정 메시지를 미리 정하지 않은 상태에서 같은 해시값을 갖는 서로 다른 두 메시지를 찾기 어려운 성질이다. 다의 표현은 충돌 내성을 요구하는 취지이며, **충돌이 전혀 존재하지 않는다**는 뜻으로 이해해서는 안 된다.

보기별 해설

가. X: 특정 메시지와 같은 해시값을 갖는 다른 메시지를 찾기 어려운 성질은 **약한 충돌 내성**, 즉 제2역상 저항성이다. 강한 충돌 내성은 기준 메시지가 주어지지 않은 상태에서도 같은 해시값을 갖는 서로 다른 두 메시지를 찾기 어려운 성질이다. 주어진 메시지에 맞는 다른 메시지를 찾는지, 두 메시지를 모두 자유롭게 고르는지가 구별 기준이다.

나. O: 해시값이 주어져도 그 값을 만드는 입력 메시지를 찾는 것이 계산적으로 매우 어려워야 한다. 이를 **일방향성 또는 역상 저항성**이라고 한다. 여기서 '불가능'은 수학적으로 절대 불가능하다는 뜻이 아니라, 현실적인 시간과 자원으로 수행하기 어렵다는 의미이다.

다. O: 서로 다른 입력 메시지가 같은 해시값을 갖는 충돌을 쉽게 찾아낼 수 없어야 한다는 **충돌 내성의 요구**를 나타낸 설명으로 본다. 다만 '입력이 다르면 해시값도 달라야 한다'를 모든 입력에 대해 반드시 성립하는 보장으로 해석하면 부정확하다. 해시 함수는 다양한 길이의 메시지를 고정 길이의 값으로 압축하므로 충돌 자체는 존재하며, 보안상 요구되는 것은 **충돌을 찾기가 계산적으로 매우 어렵다**는 성질이다.

이와 같은 의미에서 옳은 보기는 나, 다이며, 이에 해당하는 조합은 ③이다.

NoteBase

문 3. AES에 대한 설명으로 옳은 것만을 모두 고른 것으로 가장 적절한 것은?

가. 라운드 키는 128비트를 사용한다.
나. 암호화 알고리즘과 복호화 알고리즘이 동일하지 않다.
다. 128비트 크기의 평문 블록을 사용하여 암호문을 생성한다.
라. 암호화에 사용되는 키 길이에 따라 라운드 수가 결정된다.

① 가, 나
② 가, 다, 라
③ 나, 다, 라
④ 가, 나, 다, 라

정답 4번

간단한 해설

AES의 블록과 각 라운드 키는 **128비트**이지만, 원래 비밀키는 128·192·256비트이고 그에 따라 10·12·14라운드를 수행한다. 복호화에서는 암호화 변환을 되돌리는 역변환을 사용한다.

보기별 해설

가. O: AES의 AddRoundKey에서는 128비트 상태와 같은 길이인 **128비트 라운드 키**를 XOR한다. 라운드 키는 원래 비밀키를 키 확장하여 얻으며, 원래 키가 192비트나 256비트여도 한 번의 AddRoundKey에 쓰는 키는 128비트이다.

나. O: AES 복호화는 암호화의 변환을 역으로 되돌리는 절차이다. SubBytes·ShiftRows·MixColumns에 대응하는 역변환을 사용하므로 **암호화 절차를 그대로 적용하는 것은 아니다**. AddRoundKey의 XOR는 자기 자신의 역연산이지만, 이것만으로 전체 암호화·복호화 알고리즘이 동일해지는 것은 아니다. 같은 비밀키를 사용하는 대칭키 방식이라는 사실과도 구별한다.

다. O: AES의 블록 크기는 키 길이에 관계없이 **128비트로 고정**된다. 128비트 평문 블록을 처리하여 같은 길이의 암호문 블록을 만든다. AES-192나 AES-256의 숫자는 블록 크기가 아니라 원래 비밀키의 길이이다.

라. O: 원래 비밀키 길이가 128비트이면 10라운드, 192비트이면 12라운드, 256비트이면 14라운드를 수행한다. 따라서 키 길이에 따라 라운드 수가 결정된다. 초기 AddRoundKey는 이 라운드 수와 별도로 있으며, 마지막 라운드에서는 MixColumns를 생략한다.

따라서 가, 나, 다, 라가 모두 옳으며, 해당 조합은 ④이다.

NoteBase

문 4. 블록 암호에 대한 설명으로 가장 적절한 것은?

① SEED는 SPN 구조로 이루어져 있다.

② ARIA는 256비트 크기의 블록을 사용한다.

③ CBC 모드는 오류 전파가 발생하지 않는다.

④ 암호 알고리즘에 따라 블록의 크기는 다를 수 있다.

정답 4번

간단한 해설

블록 암호가 한 번에 처리하는 **블록 크기는 알고리즘마다 다를 수 있다**. 블록 크기와 키 길이는 별개이며, ARIA의 256비트는 선택 가능한 키 길이이지 블록 크기가 아니다.

선지별 해설

블록 암호는 일정 길이의 평문 블록을 같은 길이의 암호문 블록으로 변환한다. 알고리즘 내부 구조, 처리 블록의 길이, 키 길이, 여러 블록을 연결하는 운영 모드는 서로 다른 개념이다.

① X: SEED는 SPN이 아니라 **16라운드 Feistel 구조**를 사용한다. 128비트 입력을 두 개의 64비트 부분으로 나누어 라운드 연산을 수행하며, SEED의 블록 크기와 키 길이는 각각 128비트이다.

② X: ARIA의 블록 크기는 **128비트**로 고정되어 있다. 128비트·192비트·256비트는 ARIA가 지원하는 키 길이이다. 256비트 키를 선택해도 한 번에 처리하는 블록이 256비트로 바뀌지 않는다.

③ X: CBC 모드에는 오류 전파가 있다. 복호화할 때 현재 암호문 블록을 복호한 값과 직전 암호문 블록을 XOR하기 때문이다. 전송 중 한 암호문 블록의 비트가 바뀌면 대응하는 평문 블록에 오류가 생기고, 다음 평문 블록의 같은 비트 위치에도 오류가 생긴다. 다른 오류나 블록 누락이 없다면 그 이후 블록까지 계속 전파되는 것은 아니다.

④ O: 블록 크기는 알고리즘의 설계에 따라 정해진다. 예를 들어 DES는 64비트 블록을 사용하지만 AES·SEED·ARIA는 128비트 블록을 사용한다. 따라서 블록 암호라는 공통 분류에 속해도 블록의 크기가 모두 같은 것은 아니다.

NoteBase

문 5. 다음 블록 암호 공격 기법에 관한 설명으로 가장 적절한 것은?

두 개의 평문 블록들의 비트 차이에 대하여 대응되는 암호문 블록들의 비트 차이를 이용하여 사용된 암호키를 찾아내는 방법이다.

① 통계적 분석(Statistical Analysis)
② 선형 해독법(Linear Cryptanalysis)
③ 전수 공격법(Exhaustive Key Search)
④ 차분 해독법(Differential Cryptanalysis)

정답 4번

간단한 해설

평문쌍의 차이가 암호문쌍의 차이에 어떻게 반영되는지를 분석하는 것은 차분 해독법이다. 차이의 확률적 편향을 이용하여 암호키의 후보를 좁힌다.

대응 관계 해설

제시문의 핵심은 **평문 두 개의 차이와 암호문 두 개의 차이 사이의 관계**를 이용한다는 점이다. 이는 차분 해독법에 해당한다. 비트열의 차이는 보통 두 값을 XOR한 결과로 정의하며, 단순히 서로 다른 비트의 개수만 세는 것과 구별된다.

차분 해독법은 일정한 입력 차이가 암호의 변환 과정을 거쳐 어떤 출력 차이를 만들 가능성이 큰지 분석한다. 많은 평문·암호문 쌍에서 관찰한 차이의 확률적 편향을 이용하여 키 후보를 좁히는 방식이다. **평문·암호문 한 쌍의 차이만 알면 언제나 키가 바로 나오는 것은 아니다**.

통계적 분석은 데이터의 분포나 편향을 이용하는 더 넓은 접근이다. 차분 해독도 통계적 성질을 활용하지만, 제시문처럼 입력·출력의 차이를 연결하는 구체적인 이름은 차분 해독법이다.

선형 해독법은 평문 비트·암호문 비트·키 비트 사이에 성립할 확률이 1/2과 다른 선형 근사관계를 이용한다.

전수 공격법은 가능한 키 후보를 차례로 시험한다. 따라서 두 평문과 두 암호문의 차이 전파를 분석한다는 단서와는 구별된다.

따라서 가장 적절한 것은 ④ 차분 해독법이다.

NoteBase

문 6. 전자서명에 대한 설명으로 옳은 것만을 모두 고른 것으로 가장 적절한 것은?

가. 개인키로 서명을 검증한다.
나. 키 배송 문제가 발생할 수 있다.
다. 부가형 전자서명은 원래의 메시지가 필요하다.
라. 메시지 복원형 전자서명은 RSA로 구현할 수 있다.

① 가, 나
② 나, 다
③ 가, 다, 라
④ 나, 다, 라

정답 4번

간단한 해설

전자서명은 **개인키로 생성하고 공개키로 검증**한다. 공개키가 진짜 서명자의 것인지 확인하는 문제는 남으며, 부가형은 원래 메시지를 함께 사용하고 복원형은 서명에서 메시지를 복원한다.

보기별 해설

가. X: 공개키 기반 전자서명은 서명자의 **개인키로 생성하고 대응하는 공개키로 검증**한다. 개인키는 서명자만 비밀리에 보관해야 하며, 검증자에게 전달하는 키가 아니다.

나. O: 검증자는 받은 공개키가 실제 서명자의 키인지 신뢰할 수 있어야 한다. 공개키가 전달되는 과정에서 공격자의 키로 바뀌면 잘못된 서명을 진짜 서명으로 오인할 수 있으므로, **공개키의 진위와 소유자 연결을 보장하는 배송·인증 문제**가 남는다. 이는 개인키를 검증자와 공유해야 한다는 뜻이 아니며, 인증서 등으로 대응한다.

다. O: 부가형 전자서명은 원래 메시지와 별도로 서명값을 붙이는 방식이다. 검증할 때 메시지와 서명값을 함께 입력받으므로, 서명값만으로는 부족하고 원래 메시지가 필요하다.

라. O: 메시지 복원형은 검증 과정에서 서명에 포함된 메시지를 복원할 수 있는 방식이다. RSA의 연산 구조를 이용하여 적절한 메시지 인코딩과 검증 절차를 갖춘 복원형 서명을 구성할 수 있다. RSA를 쓰는 모든 서명이 복원형인 것은 아니며, 메시지 해시에 서명하는 부가형 방식도 가능하다.

따라서 옳은 보기는 나, 다, 라이며, 이 조합은 ④와 일치한다.

NoteBase

문 7. PKI에 대한 설명으로 옳은 것만을 모두 고른 것으로 가장 적절한 것은?

가. 등록기관은 인증서 발급과 취소를 담당한다.
나. 인증기관, 등록기관, 저장소, 키배포 센터는 PKI의 구성요소에 해당한다.
다. 인증서와 사용자 관련 정보, 인증서 취소 목록 등을 저장 및 검색하는 장소를 저장소라고 한다.
라. 계층구조에서는 최상위 인증기관 간의 상호인증은 허용되지만 하위 인증기관 간의 상호인증은 허용되지 않는다.

① 가, 나
② 나, 다
③ 다, 라
④ 나, 다, 라

정답 3번

간단한 해설

인증서 발급·폐지는 **인증기관(CA)**의 역할이고, 키배포 센터는 대칭키 기반 분배체계의 구성요소이다. 저장소의 정보 제공 기능과 전형적인 계층형 신뢰모형의 연결 원칙은 이에 구별하여 이해해야 한다.

NoteBase

보기별 해설

PKI는 공개키와 그 소유자의 신원을 인증서로 연결하고, 인증서의 발급·등록·조회·폐지 정보를 관리하는 기반구조이다. 인증기관과 등록기관의 역할을 구분하고, 공개키 기반구조를 대칭키 분배체계와 혼동하지 않아야 한다.

가. X: 인증서를 발급하고 폐지하는 주체는 인증기관(CA)이다. 등록기관(RA)은 신청자의 신원을 확인하고 등록 요청을 심사하여 인증기관에 전달하는 역할을 맡는다. 등록기관이 폐지 요청의 접수나 확인을 지원할 수는 있지만, 그것을 인증서 발급·폐지의 책임 주체인 인증기관과 동일시해서는 안 된다.

나. X: 인증기관, 등록기관, 저장소는 PKI의 주요 구성요소이지만 **키배포 센터(KDC)는 대칭키 기반 키 분배체계**의 구성요소이다. KDC는 통신 당사자에게 공유 비밀키나 세션키를 제공하는 방식이며, 공개키 인증서를 발급·검증하는 PKI의 기본 구성요소로 분류하지 않는다.

다. O: 저장소는 인증서와 사용자 관련 정보, 인증서 폐지목록(CRL) 등을 보관하고 검색할 수 있게 하는 시스템이다. 이용자는 저장소에서 상대방의 인증서와 폐지 정보를 얻어 인증서 검증에 활용할 수 있다.

라. O: 이 문항이 전제하는 전형적인 계층형 신뢰모형은 최상위 인증기관에서 하위 인증기관으로 신뢰를 위임하는 구조이다. 서로 다른 계층형 영역을 연결할 때는 최상위 인증기관 사이에 상호인증을 두고, 하위 기관 사이의 임의적인 수평 상호인증은 허용하지 않는 방식으로 설명한다. 이는 계층구조의 운영 원칙이며, 모든 PKI 기술이나 인증서 형식에서 하위 기관의 교차인증이 원천적으로 불가능하다는 뜻은 아니다. 그런 연결을 허용하는 망형·혼합형 모형과 구별해야 한다.

따라서 옳은 보기는 다와 라이며, 이 조합은 ③에 해당한다.

NoteBase

문 8. 다음 RSA 암호화와 복호화 과정에 대한 설명으로 가장 적절하지 않은 것은?

◯ 암호문 = (평문)^E N
◯ 평문 = (암호문)^D N

① {D, N}을 개인키라고 한다.
② 암호문의 크기는 평문의 크기와 같다.
③ N이 소인수 분해되면 D를 찾을 수 있다.
④ N을 생성하기 위해 2개의 소수가 필요하다.

정답 2번

간단한 해설

RSA에서 평문과 암호문이 모두 N 미만의 정수로 표현된다고 해서 **두 값이나 원래 데이터 길이가 같은 것은 아니다**. 실제 패딩 방식에서는 원래 메시지보다 긴 고정 길이의 암호문이 만들어진다.

선지별 해설

① O: 제시된 복호화 식에서 D는 암호문을 평문으로 되돌리는 비밀 지수이다. 따라서 **D와 공통 모듈러스 N**이 개인키를 구성한다. 공개키는 E와 N이다. N 자체는 공개되어도 되지만 D는 비밀로 보호해야 한다.

② X: RSA의 모듈러 거듭제곱은 **평문과 암호문의 수치나 원래 데이터 길이가 같음을 보장하지 않는다**. 평문과 암호문을 모두 N 미만의 정수로 표현한다는 사실과 크기가 같다는 주장은 다르다. 실제 패딩을 적용하는 RSA 암호화에서는 원래 메시지보다 긴 고정 길이의 암호문을 출력한다. 다만 패딩 후의 입력 블록과 암호문을 같은 폭으로 표현할 수 있으므로, 모든 표현 방식에서 반드시 길이가 달라진다고 단정하는 것도 적절하지 않다.

③ O: N을 두 소수 p와 q로 소인수분해하면 $\varphi(N) = (p-1)(q-1)$을 계산할 수 있다. 공개 지수 E에 대해 ED≡1±od(N)을 만족하는 **모듈러 역원 D**를 구하면 복호화할 수 있다. 따라서 소인수분해의 어려움은 RSA 개인키 보호의 중요한 기반이다.

④ O: 이 문제의 기본적인 두 소수 RSA에서는 **서로 다른 두 소수 p와 q의 곱**으로 $N = pq$를 만든다. p와 q를 비밀로 유지하여 공개된 N에서 복호화에 필요한 정보를 쉽게 얻지 못하게 한다.

따라서 가장 적절하지 않은 설명은 ②이다.

NoteBase

문 9. 무결성을 위협하는 공격으로 옳은 것만을 모두 고른 것으로 가장 적절한 것은?

가. 부인(Repudiation)
나. 스누핑(Snooping)
다. 재전송(Replaying)
라. 트래픽분석(Traffic Analysis)

① 가, 다
② 가, 나, 라
③ 나, 다, 라
④ 가, 나, 다, 라

정답 1번

간단한 해설

부인은 거래 사실의 신뢰를, 재전송은 메시지의 정당한 처리와 신선성을 훼손하므로 **무결성 위협**으로 분류한다. 스누핑과 트래픽분석은 정보 노출에 관한 기밀성 위협이다.

NoteBase

보기별 해설

이 문항은 공격을 기밀성·무결성·가용성이라는 보안 목표에 따라 구분한다. 여기서 무결성 위협은 단순한 내용 변경뿐 아니라 메시지나 거래의 정당성과 신뢰성을 훼손하는 공격까지 포함한다.

가. O: 부인은 메시지를 보내거나 받았거나 거래에 참여한 사실을 나중에 부정하는 것이다. **행위·거래 사실에 대한 신뢰**를 훼손하므로 이 공격 분류에서는 무결성 위협에 포함한다. 보안 서비스를 세분할 때는 '부인방지'를 별도 서비스로 구분하기도 한다.

나. X: 스누핑은 권한 없이 데이터를 엿보거나 가로채어 내용을 알아내는 행위이다. 정보가 허가되지 않은 상대에게 노출되므로 주된 위협 대상은 **기밀성**이다. 무결성 위협을 고르는 항목에는 포함되지 않는다.

다. O: 재전송은 이전의 유효한 메시지를 확보한 뒤 다시 보내어 새로운 정상 요청처럼 처리되게 하는 공격이다. 예를 들어 과거 거래 요청이 중복 실행되면 거래의 정당성이 훼손된다. **원래 메시지의 비트를 바꾸지 않아도** 재사용 시점과 중복 처리 때문에 무결성을 위협할 수 있다.

라. X: 트래픽분석은 통신 내용 자체를 읽지 못하더라도 송수신 관계, 통신 시점·빈도·크기 등을 관찰하여 정보를 추론하는 행위이다. 통신 양상에 관한 정보의 노출이므로 주된 위협 대상은 기밀성이다.

따라서 무결성을 위협하는 공격은 가와 다이며, 해당 조합은 ①이다.

NoteBase

문 10. 메시지 인증 코드(MAC)로 해결할 수 있는 것으로 옳은 것만을 모두 고른 것으로 가장 적절한 것은?

가. 인증
나. 기밀성
다. 무결성 검증
라. 제3자에 대한 증명

① 가, 다
② 가, 나, 라
③ 나, 다, 라
④ 가, 나, 다, 라

정답 1번

간단한 해설

MAC은 공유 비밀키를 이용하여 **메시지 출처 인증과 무결성 검증**을 제공한다. 내용을 암호화하지 않으며, 수신자도 같은 MAC을 만들 수 있어 제3자에게 송신 사실을 증명하는 용도로는 충분하지 않다.

NoteBase

보기별 해설

MAC은 메시지와 **송수신자가 공유하는 비밀키**를 입력으로 인증 태그를 생성하는 방식이다. 수신자는 같은 키로 태그를 검증하여 메시지의 출처와 변조 여부를 확인한다.

가. O: 적절한 MAC과 안전한 키 관리를 전제로, 유효한 태그는 공유키를 아는 주체가 생성한 메시지임을 확인하는 데 사용된다. 따라서 메시지 출처 인증을 제공한다. 다만 이것이 공개적으로 특정 개인의 신원을 증명한다는 뜻은 아니다.

나. X: MAC은 메시지의 인증 태그를 만들 뿐, **메시지 내용 자체를 숨기지 않는다**. 기밀성을 제공하려면 암호화를 별도로 적용하거나 인증 암호화 방식을 사용해야 한다.

다. O: 안전한 MAC과 적절한 태그 길이·키 관리를 전제로, 비밀키를 모르는 공격자가 변경한 메시지가 기존 태그로 검증을 통과할 가능성은 충분히 작다. 비밀키를 모르는 공격자가 변경된 메시지에 맞는 태그를 위조하기 어렵기 때문에 수신자는 MAC 검증을 통해 **무결성 위반을 탐지**할 수 있다. 메시지의 변경을 물리적으로 막는 것과는 구별된다.

라. X: 수신자도 송신자와 같은 비밀키를 갖고 있어 유효한 MAC을 직접 생성할 수 있다. 따라서 제3자는 MAC만 보고 송신자가 만들었는지 수신자가 만들었는지 판별할 수 없으므로, **송신 사실의 제3자 증명이나 부인 방지**를 제공하지 못한다. 공개 검증이 가능한 전자서명과 구별되는 지점이다.

해결할 수 있는 것은 가의 인증과 다의 무결성 검증이므로 ①과 일치한다.

NoteBase

문 11. 다음은 암호에 대한 설명이다. 빈칸 가, 나에 해당하는 것으로 가장 적절한 것은?

(가)는 하나의 문자를 다른 문자로 변경할 수 있으나 문자의 순서는 변하지 않는다. (나)는 평문 내의 문자들이 다른 위치로 변경될 수 있으나 문자 자체는 변하지 않는다.

① 가: 전치 암호, 나: 치환 암호

② 가: 치환 암호, 나: 전치 암호

③ 가: 치환 암호, 나: 공개키 암호

④ 가: 공개키 암호, 나: 치환 암호

정답 2번

간단한 해설

문자의 자리를 유지하면서 **문자 자체를 바꾸면 치환 암호**이고, 문자를 유지하면서 **위치만 바꾸면 전치 암호**이다.

빈칸별 해설

고전 암호의 기본 변환에서는 문자의 값 자체를 바꾸는지, 문자들이 놓인 위치를 바꾸는지를 구별한다. 이는 암호화·복호화에 사용하는 키의 관계에 따른 대칭키·공개키 분류와는 다른 기준이다.

가: 치환 암호이다. 평문 문자를 정해진 규칙에 따라 다른 문자로 바꾸되 문자들의 자리 순서는 유지한다. 예를 들어 각 문자를 알파벳에서 한 칸 뒤의 문자로 바꾸면 ABC는 BCD가 된다. 바뀌는 대상은 문자의 위치가 아니라 문자 자체이다.

나: 전치 암호이다. 평문에 사용된 문자 자체는 그대로 두고, 정해진 규칙에 따라 문자들의 위치를 재배열한다. 예를 들어 ABC를 CAB로 바꾸면 문자 A·B·C는 모두 유지되고 배열 순서만 달라진다. 따라서 문자별 출현 횟수도 보존된다.

따라서 가는 치환 암호, 나는 전치 암호이며, 이 대응은 ②와 일치한다.

NoteBase

문 12. 스트림 암호에 대한 설명으로 옳은 것만을 모두 고른 것으로 가장 적절한 것은?

가. RC4는 동기식 스트림 암호이다.
나. AES를 CFB 모드로 운용하면 스트림 암호로 사용할 수 있다.
다. 동기식 스트림 암호에서는 암호문에 비트 오류가 발생할 경우 오류 전이가 발생한다.
라. 동기식 스트림 암호에서는 키스트림 수열이 평문과 관계없이 생성되어 동기식으로 사용한다.

① 가, 다
② 가, 나, 라
③ 나, 다, 라
④ 가, 나, 다, 라

정답 2번

간단한 해설

동기식 스트림 암호는 평문과 독립적으로 키스트림을 생성하므로 암호문 한 비트의 값이 바뀌어도 **그 위치의 평문 비트에만 영향**을 준다. RC4는 동기식이며, AES를 CFB 모드로 운용하면 자기동기식 스트림 암호 방식으로 사용할 수 있다.

보기별 해설

가. O: RC4는 비밀키로 초기화한 내부 상태를 갱신하여 키스트림을 만들고 평문과 XOR하는 동기식 스트림 암호이다. **키스트림 생성이 평문이나 암호문에 의존하지 않으므로** 송신자와 수신자는 같은 상태와 같은 위치의 키스트림을 사용해야 한다.

나. O: CFB 모드는 이전 암호문을 블록 암호의 입력으로 피드백하고 그 암호화 출력의 일부 또는 전부를 평문과 XOR한다. 따라서 AES 자체는 블록 암호이지만 CFB 모드로 운용하면 **자기동기식 스트림 암호 방식**으로 사용할 수 있다.

다. X: 동기식 스트림 암호에서 암호문 한 비트가 다른 값으로 바뀌어도 키스트림의 생성 상태는 변하지 않는다. XOR 복호화에서는 **대응하는 평문 비트만 바뀌고 후속 비트로 오류가 전파되지 않는다**. 이는 비트의 삽입·삭제로 키스트림 위치가 어긋나는 동기 상실과 구별된다.

라. O: 동기식 스트림 암호의 키스트림은 비밀키와 초기 상태에 따라 생성되며 평문 내용과 독립적이다. 송수신자가 **동일한 키스트림의 동일한 위치**를 사용해야 암호화 때의 XOR을 복호화 때 되돌릴 수 있다.

따라서 옳은 보기는 가, 나, 라이며, 이에 해당하는 선택지는 ②이다.

NoteBase

문 13. 해시 함수(Hash Function)의 강한 충돌 내성을 위협하는 공격 방법으로 가장 적절한 것은?

① 중간자(Man In The Middle) 공격

② 무차별(Brute Force) 공격

③ 생일(Birthday) 공격

④ 사전(Dictionary) 공격

정답 3번

간단한 해설

강한 충돌 내성은 **같은 해시값을 만드는 임의의 두 메시지**를 찾기 어렵다는 성질이다. 생일 공격은 여러 해시값 사이에서 일치하는 쌍을 찾아 이 성질을 공격한다.

핵심 풀이

강한 충돌 내성은 공격자가 두 메시지를 모두 자유롭게 고르더라도 서로 다른 x와 y에 대해 $H(x) = H(y)$인 쌍을 찾기 어려워야 한다는 성질이다. 특정 메시지나 해시값 하나가 미리 고정된 경우와 달리, **어느 두 입력 사이에서든 같은 출력이 발견되면** 공격 목표가 달성된다.

생일 공격은 많은 메시지의 해시값을 모아 그중 같은 값이 나오는 쌍을 찾는다. 출력이 균등하게 분포하는 이상적인 n비트 해시에서 일반적인 충돌 탐색의 작업량은 대략 $2^{n/2}$ 규모이다. 예를 들어 128비트 출력이면 약 2^{64} 규모의 시도로 충돌을 찾는 생일 효과가 나타나므로, 출력 비트 수 전체만큼의 충돌 보안 강도를 기대할 수 없다.

무차별 공격은 가능한 후보를 반복 시험하는 넓은 범주의 표현이며, 생일 공격도 일반적인 충돌 탐색 기법이라는 점에서 여기에 포함될 수 있다. 다만 강한 충돌 내성과 직접 연결되는 구체적인 원리는 생일 역설이므로 생일 공격이 가장 적절하다. 중간자 공격은 통신 중개·변조, 사전 공격은 자주 쓰는 비밀번호 등 가능성 높은 후보의 시험에 초점을 둔다.

따라서 강한 충돌 내성을 위협하는 대표적인 공격은 생일(Birthday) 공격이며, ③과 일치한다.

NoteBase

문 14. 대칭키 암호의 키 배송 문제를 해결하기 위한 방법으로 옳은 것만을 모두 고른 것으로 가장 적절한 것은?

가. 키 사전 공유
나. RSA 암호 이용
다. 전자서명 이용

① 가, 나
② 가, 다
③ 나, 다
④ 가, 나, 다

정답 1번

간단한 해설

대칭키는 양쪽에 미리 안전하게 공유하거나 RSA 공개키 암호로 암호화하여 전달할 수 있다. **전자서명은 인증·무결성을 제공할 뿐 키를 비밀로 감추지 못하므로** 옳은 보기는 가, 나이다.

보기별 해설

가. (O) **키 사전 공유**는 통신 전에 안전한 경로로 같은 비밀키를 양쪽에 배포해 두는 방법이다. 통신을 시작할 때 공개된 통신망으로 비밀키를 새로 전달할 필요가 없어진다. 다만 최초 배포 경로의 안전성과 키 관리가 전제된다.

나. (O) **RSA 암호를 이용한 키 운송**에서는 송신자가 대칭키를 수신자의 공개키로 암호화하여 보내고, 수신자가 자신의 개인키로 복호화한다. 실제로는 공개키의 진위 확인과 안전한 암호화 방식이 필요하며, 메시지 본문은 전달된 대칭키로 암호화할 수 있다.

다. (X) **전자서명만으로는 키의 기밀성이 보장되지 않는다.** 전자서명은 서명자의 확인과 데이터 무결성·부인 방지에 이용되지만, 공개된 키 값을 비밀로 숨기는 기능은 아니다. 키 교환 과정의 인증에 활용할 수는 있어도 비밀키를 안전하게 배송하는 암호화 수단 자체를 대신하지는 못한다.

따라서 옳은 보기는 가, 나이며, 정답은 ①이다.

NoteBase

문 15. 클라우드 보안 서비스(SECaaS : Security as a Service)에 대한 설명으로 가장 적절하지 않은 것은?

① 보안 솔루션 도입 비용 절감과 유연성을 확보할 수 있다.

② 주요 기능으로 네트워크 보안, 웹 보안, 취약점 스캐닝 등의 서비스를 제공한다.

③ 보안 위협에 대응하기 위해서는 사용 기관에서 보안 업데이트를 직접 수행해야 한다.

④ 클라우드 환경과 솔루션을 투자하기 어려운 환경에서 서비스 형태로 이용할 수 있다.

정답 3번

간단한 해설

SECaaS에서는 서비스 제공자가 보안 기능을 운영하고 **서비스 측 업데이트와 유지보수를 관리**한다. 사용 기관이 모든 보안 업데이트를 직접 해야 한다는 설명은 서비스형 제공 방식과 맞지 않는다.

선지별 해설

① O: SECaaS는 보안 기능을 서비스 형태로 이용하므로 자체 장비·소프트웨어를 모두 구축할 때 필요한 초기 투자와 운영 부담을 줄일 수 있다. 필요에 따라 사용 규모나 기능을 조정하는 **확장성과 유연성**도 얻을 수 있다. 실제 총비용은 요금체계와 사용량 등에 따라 달라지므로 언제나 더 싸다는 의미는 아니다.

② O: SECaaS에는 네트워크 보안, 웹 보안, 취약점 점검 등 다양한 보안 기능이 포함될 수 있다. 필요한 기능을 서비스로 선택해 이용한다는 뜻이며, 모든 공급자의 단일 상품이 이러한 기능 전부를 제공한다는 뜻은 아니다.

③ X: 서비스로 제공되는 보안 기능의 운영·유지보수와 서비스 측 보안 업데이트는 일반적으로 **서비스 제공자가 관리**한다. 따라서 사용 기관이 해당 업데이트를 반드시 직접 수행해야 한다는 설명은 부적절하다. 다만 사용 기관의 단말 패치, 계정·접근권한 설정, 서비스 연동 등 고객 측 책임까지 모두 사라지는 것은 아니며 구체적인 역할은 계약과 서비스 구조에 따른다.

④ O: 자체 보안 인프라와 솔루션에 큰 투자를 하기 어려운 기관도 외부에서 제공하는 보안 기능을 서비스로 이용할 수 있다. 클라우드 자원을 보호하는 경우뿐 아니라 **자체 운영 환경을 클라우드 기반 보안 서비스로 보호**하는 방식도 가능하다.

NoteBase

문 16. 인증 수단의 사례로 가장 적절하지 않은 것은?

① 자신의 모습(Something you are) : 신분증

② 알고 있는 것(Something you know) : ID/PW

③ 위치하는 곳(Somewhere you are) : 사용자 IP

④ 가지고 있는 것(Something you have) : 스마트키

정답 1번

간단한 해설

신분증은 몸 자체의 특성이 아니라 **가지고 있는 물건**에 해당한다. 자신의 신체적 특성을 이용하는 인증의 예는 지문·홍채·얼굴 등이며, 신분증의 소지와 생체특성의 확인은 구별해야 한다.

선지별 해설

인증수단은 비밀정보를 아는지, 물건을 소지하는지, 고유한 생체특성을 제시하는지에 따라 구별할 수 있다. 접속 위치처럼 환경 정보를 이용하는 분류도 있으나, 이런 정보만으로 신원이나 실제 위치가 확실히 증명되는 것은 아니다.

① X: Something you are는 지문·홍채·얼굴 같은 생체특성을 이용하는 범주이다. 신분증이라는 문서는 **Something you have**, 즉 소지물에 해당한다. 신분증에 사진이 있어도 문서 자체가 생체특성은 아니며, 실제 얼굴과 사진을 대조하는 절차는 문서의 소지와 별도로 구분해야 한다.

② O: ID와 비밀번호를 입력하는 로그인은 통상 지식 기반 인증의 사례로 분류한다. 다만 ID는 대개 계정을 식별하는 이름이고, 본인만 알아야 하는 비밀번호가 인증의 비밀정보이다. ID 자체까지 비밀이거나 ID와 비밀번호가 서로 독립된 두 인증요소라는 의미는 아니다.

③ O: 사용자 IP 주소는 접속한 네트워크 위치를 판단하는 단서로 사용할 수 있어 위치 기반 분류의 사례가 된다. 다만 IP 주소는 네트워크상의 주소이며, 공유 주소나 프록시·VPN 등을 사용할 수 있으므로 사용자의 실제 물리적 위치나 신원을 정확히 보장하는 값은 아니다.

④ O: 스마트키는 사용자가 소지한 장치로 인증하는 사례이다. 장치에 저장된 키나 장치가 생성하는 응답 등을 확인하여 소유 여부를 검증하므로 소지 기반 인증으로 분류한다.

NoteBase

문 17. 퍼블릭 클라우드의 특징에 대한 설명으로 가장 적절하지 않은 것은?

① 사용자는 필요한 서비스를 언제나 이용할 수 있다.

② 대표적인 사례로 AWS, MS Azure 등의 서비스가 있다.

③ 클라우드 제공자가 하드웨어와 소프트웨어 및 기타 IT 자원을 소유한 형태이다.

④ 공공기관이 자체 데이터 센터 내에서 클라우드 환경을 구축하는 방식이다.

정답 4번

간단한 해설

퍼블릭 클라우드는 외부 제공자의 자원을 여러 고객이 이용하는 방식이다. 기관이 자체 데이터 센터에 자기 기관용 환경을 구축하는 방식은 **프라이빗 클라우드**이며, '퍼블릭'이 공공기관의 자체 구축을 뜻하지는 않는다.

선지별 해설

① O: 퍼블릭 클라우드는 네트워크를 통해 필요한 컴퓨팅 자원을 **요청에 따라 이용**할 수 있게 제공한다. 여기서 '언제나'는 사용자가 필요할 때 서비스를 요청해 이용하는 온디맨드 특성을 뜻하며, 모든 장애 상황에서도 서비스가 절대로 중단되지 않는다는 보장은 아니다.

② O: AWS와 MS Azure는 외부 고객에게 서버·저장 공간·데이터베이스 등의 자원을 제공하는 **대표적인 퍼블릭 클라우드 서비스**이다. 이용자는 필요한 자원을 선택하여 사용하고, 서비스 제공자가 운영하는 기반 시설을 활용한다.

③ O: 일반적인 퍼블릭 클라우드에서는 제공자가 하드웨어와 클라우드 서비스 운영에 필요한 소프트웨어 등 **기반 IT 자원을 소유·관리**하고 여러 고객에게 제공한다. 이는 이용자가 자신의 데이터나 직접 설치한 모든 응용 소프트웨어의 소유권까지 제공자에게 넘긴다는 의미는 아니다.

④ X: 공공기관이 자기 기관의 사용을 위해 자체 데이터 센터에 구축하는 방식은 **프라이빗 클라우드**에 해당한다. 퍼블릭의 '공개'는 공공기관이 직접 구축한다는 뜻이 아니라 여러 외부 고객이 이용할 수 있게 서비스를 제공한다는 뜻이다. 공공기관도 퍼블릭 클라우드를 이용할 수 있으므로 이용 기관의 공공성만으로 배포 유형을 구분하지 않는다.

따라서 가장 적절하지 않은 설명은 ④이다.

NoteBase

문 18. 다음에서 설명하는 내용으로 가장 적절한 것은?

가. 시스템을 사용할 수 없을 경우를 대비한 계획이다.
나. 사이버 테러 등의 피해가 발생되어 기관의 활동이 중지될 가능성에 대비한다.
다. 지진이나 화재 등의 재해로 인해 시스템을 사용할 수 없을 때를 대비하여 가용성을 확보하기 위한 방안이다.

① 데이터 품질 관리
② 업무 연속성 계획
③ 소프트웨어 결함 분석
④ 취약점 분석 계획 수립

정답 2번

간단한 해설

장애·사이버공격·재해로 시스템을 쓰지 못하더라도 **핵심 업무를 유지하고 재개**할 수 있도록 준비하는 것은 업무 연속성 계획이다. 공격이나 재해의 예방뿐 아니라 중단 이후의 대체 운영과 복구도 고려한다.

NoteBase

대응 관계 해설

세 설명은 **업무 연속성 계획(BCP)**에 대응한다. BCP는 장애·공격·재해로 정상 운영이 어려워져도 핵심 업무를 유지하거나 정해진 목표 안에서 재개할 수 있도록 인력, 절차, 시설, 정보시스템 등의 대응을 준비하는 계획이다.

가의 시스템을 사용할 수 없는 상황은 핵심 업무를 지원하는 자원이 중단된 경우이다. 대체 시스템이나 대체 업무 절차 등으로 **중단 중에도 필요한 업무를 이어 갈 방법**을 준비한다는 점이 BCP와 연결된다.

나의 사이버 테러 피해는 업무 중단을 일으킬 수 있는 원인 중 하나이다. BCP는 공격 예방만을 다루는 것이 아니라 실제 피해로 기관 활동이 멈출 때의 대응 체계와 재개 방안을 마련한다.

다의 지진·화재는 시스템과 업무 환경을 동시에 사용할 수 없게 할 수 있다. 대체 장소·자원과 복구 절차 등을 준비해 가용성과 업무 지속성을 확보한다. IT 시스템과 데이터의 복구에 중점을 둔 재해복구계획은 BCP와 연계되지만, **BCP는 조직의 업무 지속을 더 넓게 다룬다**.

데이터 품질 관리는 데이터의 정확성·완전성·일관성 등을 관리하는 활동이다.

소프트웨어 결함 분석은 프로그램의 결함과 원인을 분석하는 활동이며,

취약점 분석 계획은 보안 약점을 찾고 평가할 범위·방법 등을 정하는 것이다.

이들만으로 재해와 공격에 따른 기관 전체의 업무 중단에 대비하는 계획을 설명할 수는 없다.

따라서 가장 적절한 것은 ② 업무 연속성 계획이다.

NoteBase

문 19. 보안 솔루션의 특징에 대한 설명으로 가장 적절하지 않은 것은?

① 백신은 PC 또는 서버에 설치되어 시스템의 바이러스를 탐지한다.

② DRM(Digital Right Management)은 문서의 열람, 편집, 인쇄에 접근 권한을 설정하여 통제한다.

③ DLP(Data Loss Prevention)는 인터넷 회선을 임대 회선처럼 사용할 수 있도록 해주는 솔루션이다.

④ NAC(Network Access Control)는 MAC(Media Access Control) 주소를 기반으로 접근제어 및 인증을 수행하여 임의의 사용자가 접속할 수 없도록 한다.

정답 3번

간단한 해설

DLP는 **중요 정보의 외부 유출을 방지**하는 솔루션이다. 공용 인터넷에서 사설망과 같은 연결을 제공하는 것은 VPN이므로, 두 솔루션의 목적을 바꾸어 설명했다.

선지별 해설

① O: 백신은 PC나 서버 등 호스트에서 파일·메모리·실행 행위를 검사하여 바이러스와 여러 악성코드를 탐지한다. 제품과 설정에 따라 격리·삭제·실행 차단 등의 대응도 수행한다.

② O: 문서 보안에 사용하는 DRM은 암호화와 사용 권한 정책 등을 통해 누가 문서를 열람·편집·인쇄할 수 있는지 통제한다. 단순히 파일이 저장된 위치의 접근만 제한하는 것이 아니라, 보호된 문서의 이용 행위를 관리한다.

③ X: DLP는 **중요 정보가 외부로 유출되는 것을 탐지·차단**하는 솔루션이다. 이메일 전송, 파일 반출, 이동식 매체 저장 등에서 정책 위반을 검사할 수 있다. 인터넷 같은 공용망을 이용하여 전용 사설망처럼 안전한 연결을 제공하는 설명은 VPN에 해당한다. VPN이 실제 전용 회선의 대역폭까지 자동으로 보장하는 것은 아니다.

④ O: NAC는 접속하는 사용자·단말을 식별하고 정책에 따라 네트워크 접근을 허용·차단한다. MAC 주소를 등록된 단말 정보와 비교하는 방식도 사용할 수 있다. 다만 **MAC 주소만을 유일한 인증 수단으로 삼는 것은 아니며**, 사용자 인증·단말 보안 상태 검사 등을 함께 적용할 수 있다. MAC 주소는 위조될 수 있으므로 그 확인만으로 모든 무단 접속을 완벽히 방지하는 것은 아니다.

NoteBase

문 20. ISMS-P(정보보호 및 개인정보보호 관리체계)에 대한 설명으로 가장 적절하지 않은 것은?

① ISMS-P 제도에는 갱신 심사를 운영하지 않는다.

② 심사기관은 심사팀장과 심사원을 구성해 인증을 수행하는 기관이다.

③ ISMS의 인증범위는 정보 시스템의 운영 및 보호에 필요한 조직, 물리적 위치, 정보 자산을 포함한다.

④ 사후 심사는 인증을 취득한 이후 정보보호 관리체계가 지속적으로 유지되고 있는지 확인하는 것으로 인증 유효기간 중 매년 1회 이상 시행하는 심사이다.

정답 1번

①

ISMS-P는 **인증 유효기간을 연장하기 위한 갱신심사**를 운영한다. 인증을 취득한 자는 유효기간 만료 3개월 전에 갱신심사를 신청하여야 한다.

정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시 제28조(인증의 갱신)
① 인증을 취득한 자는 인증서 유효기간 만료 3개월 전에 갱신심사를 신청하여야 한다.

②

심사기관은 심사팀장과 심사원으로 **인증심사팀을 구성하여 관리체계가 인증기준에 적합한지 심사**하는 업무를 수행한다.

정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시 제2조(정의) 이 고시에서 사용하는 용어의 뜻은 다음 각 호와 같다.
4. "심사기관"이란 인증심사 업무를 수행할 수 있도록 정보통신망법 제47조제7항, 「개인정보 보호법 시행령」 제34조의6제1항제2호 및 제2항에 따라 과학기술정보통신부장관과 보호위원회가 지정하는 기관을 말한다.

정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시 제24조(인증심사팀 구성)
① 심사수행기관은 인증심사 일정이 확정된 때에는 인터넷진흥원에 심사원 모집을 요청하여 인증심사팀을 구성하여야 한다.

NoteBase

③

ISMS의 인증범위에는 정보시스템의 운영과 보호에 필요한 **조직, 물리적 위치, 정보자산**이 포함된다.

정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시 제23조(인증심사 기준)
① 다음 각 호의 인증의 구분에 따라 별표 7의 인증기준을 적용한다.
2. 정보보호 관리체계 인증 : 별표 7 가목 및 나목

https://d2u7om5rih5x7z.cloudfront.net/ox-images/drive-repair/1IlBTIPt-QWfecenP8UF-PBtcWI7edD-2.webp

④

사후심사는 인증 후에도 **정보보호 관리체계가 지속적으로 유지되는지** 확인하며, 인증 유효기간 중 **매년 1회 이상** 실시한다.

정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시 제27조(사후관리)
① 인증을 취득한 자는 인증서 유효기간 중 연 1회 이상 심사수행기관에 사후심사를 신청하여야 한다.

NoteBase

문 21. 다음 블록체인 설명 중 옳은 것의 총 개수는?

가. 비트코인 블록체인은 트랜잭션들을 기록한 데이터베이스이다.
나. 블록체인 헤더에는 이전 블록 해시값이 포함되어 있다.
다. 반감기가 지날 때마다 비트코인 지급은 반으로 줄어들게 된다.
라. 난이도를 통해 비트코인 공급이 예측 가능하고 특정 일정을 따르도록 할 수 있다.

① 1개
② 2개
③ 3개
④ 4개

정답 4번

간단한 해설

비트코인은 거래를 기록한 블록을 이전 블록의 해시로 연결한다. **신규 발행 보조금의 반감**과 **평균 블록 간격을 조절하는 난이도**가 결합하여 신규 공급의 흐름을 예측할 수 있게 한다.

보기별 해설

가. O: 비트코인 블록체인은 검증된 트랜잭션들을 블록에 모아 순서대로 연결한 **분산 거래 원장**이다. 여러 노드가 이를 보관하고 합의 규칙에 따라 거래와 블록의 유효성을 확인하므로 거래 기록 데이터베이스라고 설명할 수 있다.

나. O: 비트코인의 블록 헤더에는 **이전 블록 헤더의 해시값**이 들어간다. 이 참조가 블록들을 연쇄적으로 연결하며, 이전 블록의 내용이 바뀌면 연결된 해시 관계를 통해 변경을 탐지할 수 있다. 최초 블록은 참조할 이전 블록이 없는 예외이다.

다. O: 반감기에는 채굴자가 새 블록을 만들 때 받을 수 있는 **신규 발행 보조금**이 절반으로 줄어든다. 비트코인은 210,000블록마다 이 규칙을 적용한다. 거래 수수료까지 포함한 채굴자의 총 수입이나 이미 보유한 비트코인 수량이 절반이 된다는 의미는 아니다.

라. O: 채굴 난이도는 계산 능력이 달라져도 **평균 블록 생성 간격이 약 10분**이 되도록 주기적으로 조정된다. 이 조정이 블록별 발행량·반감기 규칙과 함께 작동하여 시간에 따른 신규 공급을 예측하기 쉽게 한다. 개별 블록의 생성 시각이나 반감기의 정확한 날짜까지 고정하는 것은 아니다.

따라서 가, 나, 다, 라의 4개가 모두 옳으며, 선택지는 ④이다.

NoteBase

문 22. TLS(Transport Layer Security) 프로토콜에 대한 설명으로 가장 적절하지 않은 것은?

① TLS는 SSL(Secure Socket Layer)을 기반으로 구성한 프로토콜이다.

② Record 프로토콜은 프로토콜 개체의 가용성을 모니터링 할 때 사용하는 프로토콜이다.

③ TLS 1.2에는 안전하지 않은 프로토콜이 포함되어 있으므로 사용 시 주의할 필요가 있다.

④ Handshake 프로토콜을 사용하여 서버와 클라이언트가 서로 인증하고, TLS 레코드 안에 송신 데이터를 보호하는데 사용할 암호화키를 협상할 수 있다.

정답 2번

간단한 해설

Record는 가용성 감시가 아니라 전송 데이터의 기밀성과 무결성 보호를 담당한다. 이를 가용성 모니터링 프로토콜로 설명한 ②가 가장 적절하지 않다.

선지별 해설

① (O) TLS는 **SSL을 계승하여 표준화한 보안 프로토콜**이다. SSL의 구조를 발전시켜 통신 데이터의 기밀성과 무결성 등을 제공한다. 다만 TLS와 구형 SSL을 같은 버전이나 동일한 안전성의 프로토콜로 보아서는 안 된다.

② (X) Record 프로토콜의 역할은 **전송 데이터를 레코드로 나누어 보호하는 것**이다. 협상된 암호 방식에 따라 암호화와 무결성 검증을 수행한다. 프로토콜 개체의 생존 여부나 가용성을 감시하는 기능을 Record의 역할로 설명한 것은 잘못이다.

③ (O) TLS 1.2에서 선택 가능한 암호 방식에는 보안상 피해야 할 구형 암호군도 있으므로 **버전뿐 아니라 암호군과 설정도 점검**해야 한다. 안전한 암호군을 사용해야 한다는 취지이며, TLS 1.2를 사용한 모든 연결이 곧바로 안전하지 않다는 뜻은 아니다.

④ (O) Handshake는 **인증과 암호 방식 협상 및 공유 키 재료 설정**을 담당한다. 이를 통해 레코드 보호에 사용할 키를 도출한다. 서버·클라이언트 상호 인증을 지원하지만, 모든 TLS 연결에서 클라이언트 인증이 반드시 수행되는 것은 아니다.

NoteBase

문 23. SQL Injection 공격의 종류와 설명으로 가장 적절한 것은?

① Blind SQL Injection 공격은 오류 메시지가 아닌 쿼리 결과의 참과 거짓을 통해 의도하지 않은 SQL 문을 실행하여 DB를 비정상적으로 공격하는 방법이다.

② Form SQL Injection 공격은 DB 쿼리에 대한 에러값을 기반으로 한 단계씩 점진적으로 DB 정보를 획득하는 방법이다.

③ Union SQL Injection 공격은 게시판이나 자료실과 같은 사용자 글을 저장할 수 있는 부분에 정상적인 평문이 아닌 스크립트 코드를 입력하는 방법이다.

④ Error-based SQL Injection 공격은 피해자가 공격을 인지하지 못하는 상태에서 피해자의 브라우저가 특정 사이트에 강제적으로 request를 보내도록 하는 방법이다.

정답 1번

간단한 해설

Blind SQL Injection은 쿼리 결과나 상세 오류가 직접 보이지 않을 때도 **조건의 참·거짓에 따른 응답 차이** 등을 이용해 정보를 추론한다. 오류 메시지를 이용하는 방식, 저장형 XSS, CSRF와 구별해야 한다.

선지별 해설

SQL Injection은 외부 입력이 안전하게 처리되지 않아 데이터베이스 쿼리의 구조나 의미를 의도하지 않게 바꾸는 취약점을 이용한다. 입력이 들어오는 경로와 결과를 관찰하는 방식은 서로 다른 분류 기준이다.

① O: 선지는 불리언 기반 Blind SQL Injection을 설명한다. 데이터나 오류가 직접 출력되지 않아도 조건이 참일 때와 거짓일 때 나타나는 페이지 내용 등의 차이를 관찰하여 정보를 추론할 수 있다. Blind 방식에는 응답 시간의 차이를 이용하는 형태도 있으므로, 모든 Blind 공격이 화면의 참·거짓 차이만 이용한다는 뜻은 아니다.

② X: 데이터베이스의 오류 메시지에 드러나는 정보를 활용하는 것은 **Error-based SQL Injection**이다. Form이라는 표현은 보통 로그인 등 입력 폼을 통한 주입 경로를 가리키며, 오류를 관찰하는 기법과 동일한 분류가 아니다. 폼 입력을 통해서도 여러 종류의 SQL Injection이 발생할 수 있다.

③ X: 게시판 등에 공격용 스크립트를 저장하고 다른 사용자가 이를 열람할 때 브라우저에서 실행되게 하는 것은 **저장형 XSS**이다. Union 기반 SQL Injection은 SQL의 UNION 연산을 이용하여 다른 조회 결과를 기존 쿼리 결과에 결합하는 방식으로, 브라우저 스크립트의 저장·실행과 구별된다.

④ X: 피해자의 브라우저가 본인의 의사와 다른 요청을 보내도록 유도하고 사이트가 가진 인증 상태 등을 악용하는 것은 **CSRF**이다. Error-based SQL Injection은 데이터베이스 오류에 노출되는 정보를 활용하는 기법이므로, 요청 위조를 설명한 선지와 맞지 않는다.

NoteBase

문 24. 다음에서 설명하는 내용으로 가장 적절한 것은?

가. 구축 시 새로운 프로토콜이나 라이브러리를 도입할 필요는 없다.
나. 네트워크 상의 모든 호스트를 인터넷에 연결된 호스트처럼 취급한다.
다. 호스트가 어디에 있든 상관 없이 네트워크에 해커가 존재하며 언제든 공격할 준비가 되어 있다고 가정한다.
라. 네트워크 상의 설정을 담당하는 시스템을 컨트롤 플레인이라고 부르며, 컨트롤 플레인이 설정하고 관리하는 다른 모든 부분은 데이터 플레인이라고 한다.

① 아마존 웹 서비스(Amazon Web Service)
② 제로 트러스트 네트워크(Zero Trust Networks)
③ 구글 클라우드 플랫폼(Google Cloud Platform)
④ 서비스 수준 계약(Service Level Agreement)

정답 2번

간단한 해설

제로 트러스트는 **네트워크 내부라는 이유만으로 신뢰하지 않고** 사용자·단말과 접근 요청을 검증한다. 어디서든 침해가 가능하다고 가정한다는 단서가 이 보안 원칙을 가리킨다.

NoteBase

대응 관계 해설

가. 기존 기술을 이용한 구축: 제로 트러스트는 특정한 새 프로토콜이나 라이브러리의 이름이 아니라 보안 설계 원칙이다. 기존 인증·암호화·접근 통제 기술을 조합하여 구현할 수 있다는 의미이며, 실제 도입 과정에서 제품·설정·업무 절차의 변경이 전혀 필요 없다는 뜻은 아니다.

나. 위치에 따른 묵시적 신뢰 배제: 내부망의 호스트라도 인터넷상의 호스트처럼 신뢰 여부를 검증한다. **내부 네트워크에 있다는 이유만으로 접근을 허용하지 않고** 사용자·단말의 신원과 상태, 요청한 자원의 권한 등을 확인한다. 모든 호스트를 실제 인터넷에 공개하라는 뜻은 아니다.

다. 침해 가능성을 전제로 한 방어: 공격자가 내부에도 존재할 수 있다고 가정하여, 한 번 로그인하거나 내부에 들어왔다는 이유로 이후 접근을 무조건 신뢰하지 않는다. 최소 권한과 지속적인 상태 확인을 통해 공격자의 이동과 피해 확산을 제한한다.

라. 제어 영역과 데이터 영역의 분리: 컨트롤 플레인은 접근 정책의 판단과 연결 설정·관리를 담당하고, 데이터 플레인은 그 정책에 따라 실제 통신과 자원 접근이 이루어지는 영역이다. 이는 정책을 결정·관리하는 기능과 실제 데이터 전달 기능을 구분한 설명이다.

대안과의 구별: 아마존 웹 서비스와 구글 클라우드 플랫폼은 클라우드 서비스 플랫폼이며, 서비스 수준 계약은 제공할 서비스의 품질·가용성 등을 정하는 계약이다. 클라우드에서도 제로 트러스트를 적용할 수 있지만, 내부 위치를 신뢰 근거로 삼지 않는다는 제시문의 보안 원칙 자체를 뜻하는 것은 아니다.

따라서 제시된 특징은 제로 트러스트 네트워크에 대응하며, ②와 일치한다.

NoteBase

문 25. WAF(Web Application Firewall)에 대한 설명으로 가장 적절하지 않은 것은?

① 웹 애플리케이션을 겨냥한 전형적인 공격으로부터 시스템을 보호한다.

② 통신 식별 방식으로 블랙리스트 방식과 화이트리스트 방식 모두 사용한다.

③ 발견된 공격 패턴을 WAF에 등록하고 등록된 패턴과 매치되면 부정 접속으로 간주한다.

④ SQL 인젝션 공격, XSS 공격을 방어하기 어렵다.

정답 4번

간단한 해설

SQL 인젝션과 XSS는 **WAF의 대표적인 탐지·차단 대상**이다. WAF는 웹 트래픽에 보안 규칙을 적용해 방어하지만, 애플리케이션 취약점 수정까지 대신하거나 모든 공격을 완벽하게 막는 것은 아니다.

선지별 해설

① O: WAF는 웹 애플리케이션과 주고받는 HTTP 트래픽을 애플리케이션 계층에서 분석한다. 요청의 경로·매개변수·헤더·본문 등에 규칙을 적용하여 **웹 애플리케이션을 겨냥한 공격**을 탐지하고 정책에 따라 차단한다.

② O: 블랙리스트 방식은 알려진 공격 특성이나 금지한 패턴을 탐지하여 차단하는 방식이다. 화이트리스트 방식은 허용된 요청 형태·값·경로 등을 정의하고 그 범위를 벗어난 접근을 제한한다. WAF는 이 두 접근을 활용하거나 조합할 수 있으며, 구체적인 지원 기능과 운영 방식은 제품·설정에 따라 달라진다.

③ O: 알려진 공격 패턴을 규칙으로 등록하고 요청이 그 패턴과 일치하는지 검사하는 것은 **시그니처 기반 탐지**의 설명이다. 규칙에 일치하면 공격성 요청으로 분류하여 차단 등의 조치를 할 수 있다. 다만 패턴 일치가 실제 공격을 항상 증명하는 것은 아니므로 정상 요청을 오탐하지 않도록 조정해야 한다.

④ X: SQL 인젝션과 XSS는 WAF가 탐지·차단하도록 설계된 **대표적인 웹 공격 유형**이다. 따라서 이 공격들을 방어하기 어렵다는 것을 WAF의 일반적 특성으로 설명하는 것은 부적절하다. 다만 우회나 미탐이 가능하고 애플리케이션 내부의 모든 문맥을 완전히 알 수 없으므로, WAF만으로 모든 공격을 막거나 취약점 자체를 없앨 수 있다는 뜻도 아니다. 안전한 쿼리 처리와 출력 인코딩 등 애플리케이션 보완이 함께 필요하다.

NoteBase

문 26. CVSS(Common Vulnerability Scoring System)에 대한 설명으로 가장 적절하지 않은 것은?

① 기업이나 담당자의 경험에 의존한다.

② 정량적으로 취약점의 심각도를 비교할 수 있다.

③ 취약점에 대한 개방적이고 범용적인 평가 방법으로 국제적으로 사용되고 있다.

④ 취약점에 대해 동일한 기준으로 비교할 수 있기 때문에 우선적으로 대응해야 할 내용을 판단할 수 있다.

정답 1번

간단한 해설

CVSS는 담당자의 경험에만 의존하지 않고 **표준화된 지표와 산정 규칙**으로 취약점의 심각도를 점수화한다. 공통 기준으로 비교할 수 있어 대응 우선순위 판단에 활용된다.

선지별 해설

① X: CVSS는 기업이나 담당자의 개인적인 경험만으로 취약점을 평가하는 방식이 아니라 **공통 평가 지표와 정해진 산정 규칙**을 사용하는 체계이다. 지표를 판단할 때 전문 지식은 필요하지만, 경험에만 의존하는 주관적 평가와는 구별된다.

② O: 공격에 필요한 조건과 보안상 영향 등의 지표를 점수로 나타내므로 취약점의 **기술적 심각도를 정량적으로 비교**할 수 있다. 다만 같은 버전과 평가 조건을 확인해야 비교의 의미를 정확히 이해할 수 있다.

③ O: CVSS는 평가 방법이 공개된 **개방적이고 범용적인 공통 체계**이다. 여러 조직과 제품의 취약점 정보를 공통된 표현으로 전달할 수 있어 국제적으로 활용된다.

④ O: 공통 기준의 점수는 취약점 사이의 심각도를 비교하여 **대응 우선순위를 정하는 근거**로 활용할 수 있다. 다만 기본 점수만으로 조직의 실제 위험이나 최종 조치 순서를 모두 결정하는 것은 아니며, 실제 악용 여부와 자산의 중요도·노출 환경 등을 함께 고려해야 한다.

따라서 가장 적절하지 않은 설명은 ①이다.

NoteBase

문 27. 다음의 동작 과정에 해당하는 공격으로 가장 적절한 것은?

가. 웹 브라우저에서 실행 가능한 웹 프로그램을 파일 업로드를 통해 웹 서버에 업로드하여 공격자가 명령을 입력할 수 있는 명령 창을 획득한다.
나. 서버 게시판의 파일 업로드 기능을 이용하여 공격에 활용할 도구를 업로드한다.
다. 서버의 공격용 도구를 활용하여 공격자에게 신호를 보내면 공격자는 이를 통해 명령을 입력할 수 있도록 한다.

① 포트 스캔
② 리버스 텔넷
③ 중간자 공격
④ 세션 하이재킹

정답 2번

간단한 해설

침해된 서버가 **공격자 쪽으로 연결을 시작**하고 그 연결로 명령을 받는 점이 리버스 텔넷의 핵심이다. 웹셸과 도구 업로드는 이러한 역방향 명령 통로를 마련하는 과정이다.

NoteBase

구성 요소별 해설

핵심은 공격자가 서버에 직접 접속을 시작하는 것이 아니라, 침해된 서버가 공격자 쪽으로 연결을 시작하여 명령 통로를 제공한다는 점이다. 제시된 가·나·다는 이 통로를 마련하는 준비 요소와 연결 요소를 설명한다.

가: 업로드된 웹 프로그램을 통해 서버에서 명령을 실행할 수 있는 웹셸 형태의 통로를 확보하는 단계이다. 브라우저는 이 프로그램에 접근하는 수단이고, 서버 명령은 서버 측에서 실행된다. 단순히 파일이 저장되었다는 것만으로 명령 실행이 가능한 것은 아니며, 제시문은 업로드한 프로그램이 서버에서 실행되는 취약한 상태를 전제한다.

나: 파일 업로드 기능을 이용해 이후의 원격 연결에 필요한 도구를 서버에 두는 과정이다. 이는 명령 통로를 확장하기 위한 준비에 해당하며, 이 단계만으로 공격 종류가 결정되지는 않는다.

다: 서버의 도구가 공격자에게 연결을 시작하고, 그 연결을 통해 공격자가 서버에 명령을 전달할 수 있게 하는 부분이다. **서버에서 공격자 방향으로 시작되는 역방향 연결**이 결정적인 특징이다. 이를 리버스 텔넷 또는 역방향 셸 연결의 맥락에서 설명한다.

포트 스캔은 열린 포트나 서비스의 탐색, 중간자 공격은 통신 당사자 사이에 개입하는 행위, 세션 하이재킹은 이미 성립한 세션을 탈취하는 행위이다. 제시된 과정은 서버가 공격자 쪽으로 명령 연결을 만드는 것이므로 ② 리버스 텔넷에 해당한다.

NoteBase

문 28. 개인정보보호법 제4조(정보주체의 권리)는 정보주체의 개인정보 처리와 관련된 권리를 규정하고 있다. 이 조항과 관련된 정보주체의 권리로 가장 적절하지 않은 것은?

① 개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리
② 개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리
③ 완전히 자동화된 개인정보 처리에 따른 결정을 거부하거나 그에 대한 설명 등을 요구할 권리
④ 개인정보의 처리에 관한 실태조사 및 개인정보 보호 수준을 평가할 권리

정답 4번

①

정보주체에게는 개인정보 처리로 입은 피해를 **신속하고 공정한 절차로 구제받을 권리**가 보장된다.

개인정보 보호법 제4조(정보주체의 권리) 정보주체는 자신의 개인정보 처리와 관련하여 다음 각 호의 권리를 가진다. <개정 2023.3.14>
5. 개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리

②

정보주체는 자신의 개인정보 처리에 관하여 **동의 여부와 동의 범위 등을 스스로 선택하고 결정할 권리**를 가진다.

개인정보 보호법 제4조(정보주체의 권리) 정보주체는 자신의 개인정보 처리와 관련하여 다음 각 호의 권리를 가진다. <개정 2023.3.14>
2. 개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리

③

정보주체의 권리에는 **완전히 자동화된 개인정보 처리에 따른 결정의 거부와 설명 등의 요구**가 포함된다.

개인정보 보호법 제4조(정보주체의 권리) 정보주체는 자신의 개인정보 처리와 관련하여 다음 각 호의 권리를 가진다. <개정 2023.3.14>
6. 완전히 자동화된 개인정보 처리에 따른 결정을 거부하거나 그에 대한 설명 등을 요구할 권리

NoteBase

④

개인정보 처리 실태를 조사하고 보호수준을 평가하는 것은 **개인정보보호위원회의 권한·업무**이다. 정보주체에게 보장된 개인정보 처리 관련 권리에 해당하지 않는다.

개인정보 보호법 제11조(자료제출 요구 등)
② 보호위원회는 개인정보 보호 정책 추진, 성과평가 등을 위하여 필요한 경우 개인정보처리자, 관계 중앙행정기관의 장, 지방자치단체의 장 및 관계 기관 · 단체 등을 대상으로 개인정보관리 수준 및 실태파악 등을 위한 조사를 실시할 수 있다. <신설 2015.7.24, 2017.7.26, 2020.2.4>

개인정보 보호법 제11조의2(개인정보 보호수준 평가)
① 보호위원회는 공공기관 중 중앙행정기관 및 그 소속기관, 지방자치단체, 그 밖에 대통령령으로 정하는 기관을 대상으로 매년 개인정보 보호 정책 · 업무의 수행 및 이 법에 따른 의무의 준수 여부 등을 평가(이하 "개인정보 보호수준 평가"라 한다)하여야 한다.

NoteBase

문 29. 개인정보보호위원회에 대한 설명으로 옳은 것만을 모두 고른 것으로 가장 적절한 것은?

가. 개인정보 보호에 관한 사무를 독립적으로 수행하기 위하여 국무총리 소속으로 둔다.
나. 위원회는 상임위원 2명을 포함한 11명의 위원으로 구성한다.
다. 위원장과 부위원장은 정무직 공무원으로 임명한다.

① 가, 나
② 가, 다
③ 나, 다
④ 가, 나, 다

정답 2번

가

개인정보 보호에 관한 사무를 **독립적으로 수행**하기 위하여 개인정보 보호위원회를 **국무총리 소속**으로 둔다.

개인정보 보호법 제7조(개인정보 보호위원회)
① 개인정보 보호에 관한 사무를 독립적으로 수행하기 위하여 국무총리 소속으로 개인정보 보호위원회(이하 "보호위원회"라 한다)를 둔다. <개정 2020.2.4>

나

보호위원회는 **상임위원 2명(위원장 1명, 부위원장 1명)을 포함한 총 9명**으로 구성한다.

개인정보 보호법 제7조의2(보호위원회의 구성 등)
① 보호위원회는 상임위원 2명(위원장 1명, 부위원장 1명)을 포함한 9명의 위원으로 구성한다.

다

위원장과 부위원장은 **정무직 공무원**으로 임명한다.

개인정보 보호법 제7조의2(보호위원회의 구성 등)
③ 위원장과 부위원장은 정무직 공무원으로 임명한다.

NoteBase

문 30. 개인정보보호법 제17조(개인정보의 제공)에서 개인정보 처리자는 정보의 주체의 동의를 받고 정보주체의 개인정보를 제3자에게 제공할 수 있다. 이 경우에 제3자에게 개인정보를 제공하는 개인정보처리자가 정보주체에게 알려할 항목에 해당하지 않은 것은?

① 개인정보를 제공받는 자

② 개인정보의 수집 출처

③ 개인정보를 제공받는 자의 개인정보 이용 목적

④ 개인정보를 제공받는 자의 개인정보 보유 및 이용기간

정답 2번

①

제3자 제공 동의를 받을 때에는 **개인정보를 제공받는 자**를 정보주체에게 알려야 한다.

개인정보 보호법 제17조(개인정보의 제공)
② 개인정보처리자는 제1항제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.
1. 개인정보를 제공받는 자

②

제3자 제공 동의 시에는 제공받는 자, 이용 목적, 제공 항목, 보유·이용 기간, 동의 거부권과 거부에 따른 불이익이 있으면 그 내용을 알려야 하며, **개인정보의 수집 출처는 고지 사항에 포함되지 않는다**.

개인정보 보호법 제17조(개인정보의 제공)
② 개인정보처리자는 제1항제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.
1. 개인정보를 제공받는 자
2. 개인정보를 제공받는 자의 개인정보 이용 목적
3. 제공하는 개인정보의 항목
4. 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간
5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

NoteBase

③

제3자 제공 동의를 받을 때에는 **개인정보를 제공받는 자의 개인정보 이용 목적**을 정보주체에게 알려야 한다.

개인정보 보호법 제17조(개인정보의 제공)
② 개인정보처리자는 제1항제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.
2. 개인정보를 제공받는 자의 개인정보 이용 목적

④

제3자 제공 동의를 받을 때에는 **개인정보를 제공받는 자의 개인정보 보유 및 이용 기간**을 정보주체에게 알려야 한다.

개인정보 보호법 제17조(개인정보의 제공)
② 개인정보처리자는 제1항제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.
4. 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간

NoteBase

문 31. 개인정보보호법 시행령 제19조(고유식별정보의 범위)에서 정하는 고유식별정보로 가장 적절하지 않은 것은?

① 유전자검사 등의 결과로 얻어진 유전정보
② 주민등록번호
③ 운전면허의 면허번호
④ 외국인등록번호

정답 1번

①

유전자검사 등의 결과로 얻어진 유전정보는 **민감정보**에 해당하며, 고유식별정보로 열거된 정보에는 포함되지 않는다.

개인정보 보호법 시행령 제18조(민감정보의 범위) 법 제23조제1항 각 호 외의 부분 본문에서 "대통령령으로 정하는 정보"란 다음 각 호의 어느 하나에 해당하는 정보를 말한다. 다만, 공공기관이 법 제18조제2항제5호부터 제9호까지의 규정에 따라 다음 각 호의 어느 하나에 해당하는 정보를 처리하는 경우의 해당 정보는 제외한다. <개정 2016.9.29, 2020.8.4>
1. 유전자검사 등의 결과로 얻어진 유전정보

개인정보 보호법 시행령 제19조(고유식별정보의 범위) 법 제24조제1항 각 호 외의 부분에서 "대통령령으로 정하는 정보"란 다음 각 호의 어느 하나에 해당하는 정보를 말한다. 다만, 공공기관이 법 제18조제2항제5호부터 제9호까지의 규정에 따라 다음 각 호의 어느 하나에 해당하는 정보를 처리하는 경우의 해당 정보는 제외한다. <개정 2016.9.29, 2017.6.27, 2020.8.4>
1. 「주민등록법」 제7조의2제1항에 따른 주민등록번호
2. 「여권법」 제7조제1항제1호에 따른 여권번호
3. 「도로교통법」 제80조에 따른 운전면허의 면허번호
4. 「출입국관리법」 제31조제5항에 따른 외국인등록번호

NoteBase

②

주민등록번호는 법령에서 열거한 **고유식별정보**에 해당한다.

개인정보 보호법 시행령 제19조(고유식별정보의 범위) 법 제24조제1항 각 호 외의 부분에서 "대통령령으로 정하는 정보"란 다음 각 호의 어느 하나에 해당하는 정보를 말한다. 다만, 공공기관이 법 제18조제2항제5호부터 제9호까지의 규정에 따라 다음 각 호의 어느 하나에 해당하는 정보를 처리하는 경우의 해당 정보는 제외한다. <개정 2016.9.29, 2017.6.27, 2020.8.4>
1. 「주민등록법」 제7조의2제1항에 따른 주민등록번호

③

운전면허의 면허번호는 법령에서 열거한 **고유식별정보**에 해당한다.

개인정보 보호법 시행령 제19조(고유식별정보의 범위) 법 제24조제1항 각 호 외의 부분에서 "대통령령으로 정하는 정보"란 다음 각 호의 어느 하나에 해당하는 정보를 말한다. 다만, 공공기관이 법 제18조제2항제5호부터 제9호까지의 규정에 따라 다음 각 호의 어느 하나에 해당하는 정보를 처리하는 경우의 해당 정보는 제외한다. <개정 2016.9.29, 2017.6.27, 2020.8.4>
3. 「도로교통법」 제80조에 따른 운전면허의 면허번호

④

외국인등록번호는 법령에서 열거한 **고유식별정보**에 해당한다.

개인정보 보호법 시행령 제19조(고유식별정보의 범위) 법 제24조제1항 각 호 외의 부분에서 "대통령령으로 정하는 정보"란 다음 각 호의 어느 하나에 해당하는 정보를 말한다. 다만, 공공기관이 법 제18조제2항제5호부터 제9호까지의 규정에 따라 다음 각 호의 어느 하나에 해당하는 정보를 처리하는 경우의 해당 정보는 제외한다. <개정 2016.9.29, 2017.6.27, 2020.8.4>
4. 「출입국관리법」 제31조제5항에 따른 외국인등록번호

NoteBase

문 32. 정보통신기반 보호법 시행령 제20조(보호지침의 제정)에서 보호지침에 포함되어야 할 사항으로 가장 적절하지 않은 것은?

① 정보보호체계의 관리 및 운영

② 유사한 침해사고의 방지를 위한 예방대책

③ 취약점 분석·평가 및 침해사고 예방

④ 침해사고에 대한 대응 및 복구

정답 2번

①

보호지침에는 **정보보호체계의 관리 및 운영**에 관한 사항이 포함되어야 한다.

정보통신기반 보호법 시행령 제20조(보호지침의 제정)
①법 제10조의 규정에 의한 보호지침에는 주요정보통신기반시설 보호에 필요한 다음 각호에 관한 사항이 포함되어야 한다.
1. 정보보호체계의 관리 및 운영

②

유사한 침해사고의 방지를 위한 예방대책은 **반드시 대책본부회의를 거쳐야 하는 사항**이다. 보호지침의 필수 사항으로 열거된 항목은 아니다.

정보통신기반 보호법 시행령 제20조(보호지침의 제정)
①법 제10조의 규정에 의한 보호지침에는 주요정보통신기반시설 보호에 필요한 다음 각호에 관한 사항이 포함되어야 한다.
1. 정보보호체계의 관리 및 운영
2. 취약점 분석 · 평가 및 침해사고 예방
3. 침해사고에 대한 대응 및 복구

정보통신기반 보호법 시행령 제23조(대책본부의 운영)
②대책본부장은 침해사고 피해의 효율적인 수습을 위하여 필요하다고 인정할 때에는 제22조제1항의 규정에 의한 대책본부의 구성원이 참여하는 회의(이하 "대책본부회의"라 한다. 이하 이 조에서 같다)를 소집할 수 있다. 다만, 다음 각호의 사항에 관하여는 반드시 대책본부 회의를 거쳐야 한다.
4. 유사한 침해사고의 방지를 위한 예방대책

NoteBase

③

보호지침에는 **취약점 분석·평가 및 침해사고 예방**에 관한 사항이 포함되어야 한다.

정보통신기반 보호법 시행령 제20조(보호지침의 제정)
①법 제10조의 규정에 의한 보호지침에는 주요정보통신기반시설 보호에 필요한 다음 각호에 관한 사항이 포함되어야 한다.
2. 취약점 분석 · 평가 및 침해사고 예방

④

보호지침에는 **침해사고에 대한 대응 및 복구**에 관한 사항이 포함되어야 한다.

정보통신기반 보호법 시행령 제20조(보호지침의 제정)
①법 제10조의 규정에 의한 보호지침에는 주요정보통신기반시설 보호에 필요한 다음 각호에 관한 사항이 포함되어야 한다.
3. 침해사고에 대한 대응 및 복구

NoteBase

문 33. 다음은 개인정보보호법 및 동법 시행령에서 개인정보의 열람에 대한 내용과 개인정보 유출 등의 통지에 대한 내용이다. 빈 칸 ㉠, ㉡에 해당하는 것으로 가장 적절한 것은?

가. 정보주체가 개인정보처리자에게 자신의 개인정보에 대한 열람을 요청할 경우, 개인정보처리자는 (㉠) 이내에 정보주체가 해당 개인정보를 열람할 수 있도록 하여야 한다.
나. 개인정보처리자는 개인정보가 분실·도난·유출되었음을 알게 되었을 때에는 (㉡) 이내에 정보주체에게 알려야 한다.

① ㉠: 5일, ㉡: 24시간

② ㉠: 7일, ㉡: 24시간

③ ㉠: 10일, ㉡: 72시간

④ ㉠: 14일, ㉡: 72시간

정답 3번

가

개인정보처리자는 열람 요구를 받은 날부터 원칙적으로 **10일 이내에 해당 개인정보를 열람할 수 있도록** 해야 한다. 다만, 그 기간 내에 열람할 수 없는 정당한 사유가 있으면 정보주체에게 사유를 알리고 연기할 수 있으며, 사유가 소멸하면 지체 없이 열람하게 해야 한다.

개인정보 보호법 제35조(개인정보의 열람)
③ 개인정보처리자는 제1항 및 제2항에 따른 열람을 요구받았을 때에는 대통령령으로 정하는 기간 내에 정보주체가 해당 개인정보를 열람할 수 있도록 하여야 한다. 이 경우 해당 기간 내에 열람할 수 없는 정당한 사유가 있을 때에는 정보주체에게 그 사유를 알리고 열람을 연기할 수 있으며, 그 사유가 소멸하면 지체 없이 열람하게 하여야 한다.

개인정보 보호법 시행령 제41조(개인정보의 열람절차 등)
④ 법 제35조제3항 전단에서 "대통령령으로 정하는 기간"이란 10일을 말한다. <개정 2017.10.17>

NoteBase

나

개인정보처리자는 개인정보의 분실·도난·유출을 **알게 된 때부터 원칙적으로 72시간 이내**에 정보주체에게 알려야 한다. 추가 유출 방지 등의 긴급조치가 필요하거나 천재지변 등 부득이한 사유로 기한 내 통지가 곤란한 경우에는 해당 사유가 해소된 후 즉시 알릴 수 있다.

개인정보 보호법 시행령 제39조(개인정보 유출 등의 통지)
① 개인정보처리자는 개인정보가 유출등이 되었음을 알게 되었을 때에는 서면등의 방법으로 72시간 이내에 법 제34조제1항 각 호의 사항을 정보주체에게 알려야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 해당 사유가 해소된 후 즉시 정보주체에게 알릴 수 있다. <개정 2026.9.10>
1. 유출등이 된 개인정보의 확산 및 추가 유출등을 방지하기 위하여 접속경로의 차단, 취약점 점검 · 보완, 유출등이 된 개인정보의 회수 · 삭제 등 긴급한 조치가 필요한 경우
2. 천재지변이나 그 밖에 부득이한 사유로 인하여 72시간 이내에 통지하기 곤란한 경우

NoteBase

문 34. 약칭 정보통신망법 시행령 제55조의2(정보보호 관리등급 부여의 심사기준)에서 정보보호 관리등급 부여의 심사기준으로 가장 적절하지 않은 것은?

① 정보보호 관리체계의 구축 범위 및 운영기간

② 정보보호를 위한 전담조직 및 예산

③ 정보보호 관리체계를 수립·운영하는 방법과 절차

④ 정보보호 관리 활동 및 보호조치 수준

정답 3번

①

정보보호 관리체계의 구축 범위 및 운영기간은 정보보호 관리등급 부여의 심사기준이다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제55조의2(정보보호 관리등급 부여의 심사기준)
① 법 제47조의5제1항에 따른 정보보호 관리등급 부여의 심사기준은 다음 각 호와 같다.
1. 정보보호 관리체계의 구축 범위 및 운영기간

②

정보보호를 위한 전담조직 및 예산은 정보보호 관리등급 부여의 심사기준이다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제55조의2(정보보호 관리등급 부여의 심사기준)
① 법 제47조의5제1항에 따른 정보보호 관리등급 부여의 심사기준은 다음 각 호와 같다.
2. 정보보호를 위한 전담조직 및 예산

③

정보보호 관리등급의 심사기준은 **구축 범위 및 운영기간, 전담조직 및 예산, 관리 활동 및 보호조치 수준**이다.
관리체계를 수립·운영하는 방법과 절차는 이 심사기준에 포함되지 않는다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제55조의2(정보보호 관리등급 부여의 심사기준)
① 법 제47조의5제1항에 따른 정보보호 관리등급 부여의 심사기준은 다음 각 호와 같다.
1. 정보보호 관리체계의 구축 범위 및 운영기간
2. 정보보호를 위한 전담조직 및 예산
3. 정보보호 관리 활동 및 보호조치 수준

NoteBase

④

정보보호 관리 활동 및 보호조치 수준은 정보보호 관리등급 부여의 심사기준이다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제55조의2(정보보호 관리등급 부여의 심사기준)
① 법 제47조의5제1항에 따른 정보보호 관리등급 부여의 심사기준은 다음 각 호와 같다.
3. 정보보호 관리 활동 및 보호조치 수준

NoteBase

문 35. 위치정보의 보호 및 이용에 관한 법률 시행령 제20조 (위치정보의 관리적·기술적 보호조치)에서 관리적 보호조치에 해당하는 것으로 가장 적절한 것은?

① 위치정보 제공사실 등을 기록한 취급대장의 운영·관리

② 위치정보 및 위치정보시스템의 접근권한을 확인할 수 있는 식별 및 인증 실시

③ 위치정보시스템에 대한 접근사실의 전자적 자동 기록·보존 장치의 운영

④ 위치정보시스템의 침해사고 방지를 위한 보안프로그램 설치 및 운영

정답 1번

①

위치정보 제공사실 등을 기록한 취급대장을 운영·관리하는 것은 **관리적 보호조치**에 해당한다.

위치정보의 보호 및 이용 등에 관한 법률 시행령 제20조(위치정보의 관리적 · 기술적 보호조치)
① 법 제16조제1항에 따른 관리적 조치에는 다음 각 호의 내용이 포함되어야 한다. <개정 2018.10.16>
4. 위치정보 제공사실 등을 기록한 취급대장의 운영 · 관리

②

위치정보 및 위치정보시스템의 접근권한을 확인하기 위한 식별·인증은 관리적 조치가 아니라 **기술적 보호조치**이다.

위치정보의 보호 및 이용 등에 관한 법률 시행령 제20조(위치정보의 관리적 · 기술적 보호조치)
② 법 제16조제1항에 따른 기술적 조치에는 다음 각 호의 내용이 포함되어야 한다. <개정 2022.4.19, 2025.10.1>
1. 위치정보 및 위치정보시스템의 접근권한을 확인할 수 있는 식별 및 인증 실시

③

위치정보시스템에 대한 접근사실을 전자적으로 자동 기록·보존하는 장치의 운영은 **기술적 보호조치**이다.
취급대장 운영·관리와 구별한다.

위치정보의 보호 및 이용 등에 관한 법률 시행령 제20조(위치정보의 관리적 · 기술적 보호조치)
② 법 제16조제1항에 따른 기술적 조치에는 다음 각 호의 내용이 포함되어야 한다. <개정 2022.4.19, 2025.10.1>
3. 위치정보시스템에 대한 접근사실의 전자적 자동 기록 · 보존장치의 운영

NoteBase

④

위치정보시스템의 침해사고를 방지하기 위한 보안프로그램 설치·운영은 관리적 조치가 아니라 **기술적 보호조치**이다.

위치정보의 보호 및 이용 등에 관한 법률 시행령 제20조(위치정보의 관리적 · 기술적 보호조치)
② 법 제16조제1항에 따른 기술적 조치에는 다음 각 호의 내용이 포함되어야 한다. <개정 2022.4.19, 2025.10.1>
4. 위치정보시스템의 침해사고 방지를 위한 보안프로그램 설치 및 운영

NoteBase

문 36. ISMS-P(정보보호 및 개인정보보호 관리체계) 보호대책 요구사항 영역에 있는 인증 및 권한관리 분야의 항목으로 가장 적절하지 않은 것은?

① 사용자 계정 관리
② 사용자 식별
③ 비밀번호 관리
④ 직무 분리

정답 4번

①

사용자 계정 관리는 **인증 및 권한관리 분야**에 속한다. 사용자 등록·해지와 접근권한 부여·변경·말소 절차를 수립하여 비인가 접근을 통제하고 업무상 필요한 최소한의 권한을 부여한다.

https://d2u7om5rih5x7z.cloudfront.net/ox-images/drive-repair/1-yy5NsU8J_sp3myOPLiLKB_WeSshopEJ.webp

②

사용자 식별은 **인증 및 권한관리 분야**에 속한다. 사용자별로 구분할 수 있는 고유한 식별자를 부여하고, 식별자를 공유할 때에는 책임자 승인과 책임추적성 확보 등의 보완대책을 마련한다.

https://d2u7om5rih5x7z.cloudfront.net/ox-images/drive-repair/1mKNWliqb2cYJtis-nXFQlFfHmV9l5UEu.webp

③

비밀번호 관리는 **인증 및 권한관리 분야**에 속한다. 법적 요구사항과 외부 위협요인을 고려하여 정보시스템 사용자와 이용자의 비밀번호 관리절차를 수립·이행한다.

https://d2u7om5rih5x7z.cloudfront.net/ox-images/drive-repair/1Vzy3zw_YeUd6toRKO3kXIpajUadENWX0.webp

④

직무 분리는 인증 및 권한관리 분야가 아니라 **인적 보안 분야**의 항목이다.

https://d2u7om5rih5x7z.cloudfront.net/ox-images/drive-repair/11gVOl0u9yCaEiuQMjnIE-myB_vCWQ-Ai.webp

NoteBase

문 37. CC(공통 평가 기준)의 보안 기능 요구사항으로 가장 적절하지 않은 것은?

① 취약성 평가

② 식별 및 인증

③ 암호 지원

④ 보안 감사

정답 1번

간단한 해설

취약성 평가(AVA)는 보안 기능이 아니라 보안 보증 요구사항이다. 식별 및 인증, 암호 지원, 보안 감사는 보안 기능 요구사항이므로 정답은 ①이다.

선지별 해설

① (X) 취약성 평가(AVA)는 **보안 보증 요구사항**에 속한다. 평가대상에 악용 가능한 취약점이 있는지를 분석·시험하여 보안성에 대한 신뢰를 확보하는 평가 활동이지, 제품이 제공할 보안 기능의 분류가 아니다.

② (O) 식별 및 인증(FIA)은 **보안 기능 요구사항**이다. 사용자가 누구인지를 식별하고, 제시한 신원의 진위를 확인하는 기능 등을 다룬다.

③ (O) 암호 지원(FCS)은 **보안 기능 요구사항**이다. 암호키 관리와 암호 연산 등 평가대상의 암호 기능에 관한 요구사항을 규정한다.

④ (O) 보안 감사(FAU)는 **보안 기능 요구사항**이다. 보안 관련 사건의 기록 생성·보호·검토 등 감사에 필요한 기능을 다룬다. 여기서 감사는 외부 평가자가 수행하는 보증 평가 자체가 아니라 제품이 제공하는 감사 기능을 뜻한다.

NoteBase

문 38. 동일한 데이터가 2개 이상의 디스크에 동시에 저장되는 RAID 유형으로 가장 적절한 것은?

① RAID 0

② RAID 1

③ RAID 2

④ RAID 5

정답 2번

간단한 해설

RAID 1은 **미러링**으로 동일한 데이터를 여러 디스크에 복제하여 저장한다. 데이터를 나누어 저장하는 스트라이핑이나 패리티를 통한 복구와 구별된다.

핵심 풀이

동일한 데이터를 두 개 이상의 디스크에 복제하여 기록하는 방식은 **미러링**이며, RAID 1이 이에 해당한다. 한 디스크에 장애가 생겨도 정상적인 복제본이 남아 있으면 데이터를 이용할 수 있다. 같은 용량의 디스크 두 개를 미러링하면 사용 가능한 용량은 디스크 한 개분이다.

RAID 0은 데이터를 여러 디스크에 **나누어 기록하는 스트라이핑** 방식이며, 동일한 데이터의 복제본을 저장하지 않는다. 중복 정보가 없으므로 디스크 장애에 대한 복구 기능도 제공하지 않는다.

RAID 2는 데이터를 비트 단위로 나누고 해밍 코드와 같은 오류정정 정보를 별도의 디스크에 저장하는 방식이다. 각 디스크에 동일한 데이터 전체를 복제하는 미러링과 다르다.

RAID 5는 블록 단위로 데이터를 분산하고 **패리티도 여러 디스크에 분산**하여 저장한다. 데이터 전체의 동일한 복제본 대신 데이터와 패리티의 관계를 이용하여 디스크 한 개의 장애에 대응한다.

따라서 주어진 특징에 해당하는 것은 RAID 1이며, 선택지는 ②이다.

NoteBase

문 39. 다음 보기에서 설명하는 재해복구시스템의 복구 수준별 유형으로 가장 적절한 것은?

가. 주 센터와 재해복구센터 모두 액티브 상태이며 실시간으로 동시 서비스하는 방식이다.
나. 재해 발생 시 복구까지의 소요시간은 이론적으로 0이다.

① hot site
② warm site
③ mirror site
④ cold site

정답 3번

간단한 해설

미러 사이트는 **두 센터가 모두 활성 상태로 동시에 서비스**하므로, 한쪽이 중단되어도 다른 쪽이 서비스를 이어 갈 수 있다. 이 때문에 이론적인 복구 소요시간을 0으로 설명한다.

대응 관계 해설

가. 두 센터의 동시 서비스 → 미러 사이트: 주 센터와 재해복구센터가 모두 활성 상태로 운영되며 데이터를 동기화하고 동시에 서비스를 제공하는 방식이다. **대기 중인 센터를 새로 가동하는 것이 아니라 이미 서비스 중인 센터가 계속 처리**한다는 점이 핵심이다.

나. 이론적 복구시간 0 → 미러 사이트: 한 센터가 중단되더라도 다른 센터가 서비스를 계속할 수 있도록 구성하므로, 이론적으로 복구시간목표(RTO)를 0에 가깝게 설정한다. 실제로는 장애 감지·경로 전환 등에 지연이 있을 수 있으므로 현실의 모든 장애에서 중단 시간이 정확히 0임을 보장한다는 뜻은 아니다.

다른 유형과의 구별: 핫 사이트는 신속히 전환할 수 있도록 시스템과 데이터를 준비하지만, 이 문항의 분류에서는 두 센터가 평상시 동시에 서비스하는 미러 사이트와 구별된다. 웜 사이트는 일부 설비를 준비해 두고 재해 후 데이터 복원과 추가 구성을 수행한다. 콜드 사이트는 주로 공간·전력·통신 같은 기반 시설만 준비하므로 장비 설치와 복구에 더 많은 시간이 필요하다.

따라서 두 설명에 대응하는 복구 유형은 mirror site이며, ③과 일치한다.

NoteBase

문 40. 소프트웨어 개발 보안 가이드에서 설계단계 보안항목으로 가장 적절하지 않은 것은?

① DBMS 조회 및 결과 검증

② 허용된 범위내 메모리 접근

③ 암호키 관리

④ 종료되지 않은 반복문 재귀함수

정답 4번

간단한 해설

종료되지 않는 반복문이나 재귀함수는 **구현 단계의 '시간 및 상태' 보안약점**으로 분류된다. 설계 보안항목의 명칭과 코드 구현에서 제거할 보안약점을 구별해야 한다.

선지별 해설

① O: 'DBMS 조회 및 결과 검증'은 설계 단계의 입력데이터 검증 및 표현 항목이다. SQL 질의에 쓰이는 입력값과 조회 결과의 유효성을 어떻게 확인하고, 부적합한 값을 어떻게 처리할지 정한다.

② O: '허용된 범위내 메모리 접근'도 설계 단계의 입력데이터 검증 및 표현 항목이다. 메모리의 읽기·쓰기가 **허용된 버퍼 경계를 넘지 않도록** 검사하고, 범위를 벗어난 접근을 처리하는 방법을 설계한다.

③ O: '암호키 관리'는 설계 단계의 보안기능 항목이다. 키의 생성·분배·접근·파기 등 **생명주기 전반의 보호 방법**을 정한다.

④ X: '종료되지 않은 반복문 재귀함수'는 설계 보안항목의 명칭이 아니라, **구현 단계의 '시간 및 상태'**에 속하는 보안약점이다. 종료 조건이 없거나 제대로 작동하지 않아 반복·재귀가 계속되는 문제를 뜻하며, 종료 조건과 실행 한도를 적절히 구현해야 한다. 이 분류는 해당 위험을 설계 단계에서 미리 고려하면 안 된다는 뜻은 아니다.

NoteBase