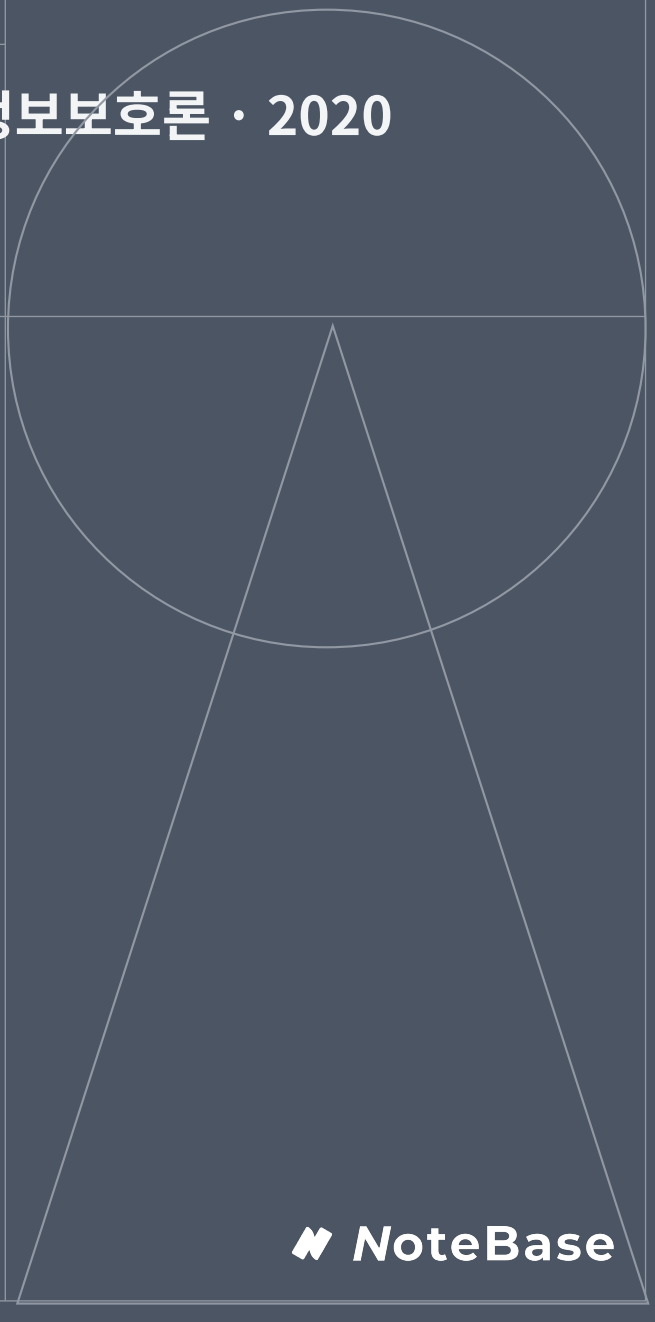
기출OX 해설집

공무원/경찰/공채(경위) · 정보보호론 · 2020



NoteBase

기출OX 해설집

공무원/경찰/공채(경위) · 정보보호론 · 2020

공무원/경찰/공채(경위) · 정보보호론 · 2020

문 1. 정보보호의 3대 목표 중 가용성(Availability)을 위협하는 행위로 옳은 것은 무엇인가?

① 데이터 변조(Modification)

② 서비스 거부(Denial of Service)

③ 신분 위장(Masquerading)

④ 트래픽 분석(Traffic Analysis)

정답 2번

간단한 해설

가용성은 정당한 사용자가 필요할 때 정보와 서비스를 이용할 수 있어야 한다는 성질이다. 서비스 거부 공격은 자원을 고갈시키거나 처리를 방해하여 **정상적인 서비스 이용을 불가능하게 하거나 지연**시킨다.

NoteBase

선지별 해설

정보보호의 3대 목표는 허가되지 않은 공개를 막는 기밀성, 부당한 변경을 막는 무결성, 필요할 때 정상적으로 이용할 수 있게 하는 가용성이다. 이 문제는 각 행위의 대표적이고 직접적인 침해 대상을 기준으로 판단한다.

① X: 데이터 변조는 허가 없이 데이터의 내용이나 값을 바꾸는 행위이다. 핵심 침해 대상은 **데이터의 정확성과 온전함인 무결성**이므로 가용성 침해의 대표적 행위로 고르는 것은 적절하지 않다.

② O: 서비스 거부는 과도한 요청으로 처리 능력이나 통신 자원을 소모시키는 등의 방법으로 정당한 사용자의 이용을 방해하는 행위이다. 정보가 유출되거나 내용이 바뀌지 않더라도 **필요한 서비스를 제때 이용할 수 없다**면 가용성이 침해된다.

③ X: 신분 위장은 다른 사용자나 시스템인 것처럼 가장하는 행위이다. 직접적인 문제는 **신원의 진정성과 인증의 훼손**이다. 이후 정보 열람이나 변경 등으로 이어질 수 있지만, 신분 위장 자체를 정상 서비스의 이용 가능성을 차단하는 행위로 분류하는 것은 적절하지 않다.

④ X: 트래픽 분석은 통신 내용뿐 아니라 송수신 관계, 통신량, 시각 등의 패턴을 살펴 정보를 추론하는 행위이다. 암호문을 해독하지 않고도 민감한 관계나 활동을 알아낼 수 있어 주로 **기밀성을 위협**하며, 서비스를 중단시키는 행위와 구별된다.

NoteBase

문 2. 다음 중 수동적 공격(Passive Attack)으로 가장 옳은 것은 무엇인가?

① 분산 서비스 거부(Distributed Denial of Service)

② 세션 하이재킹(Session Hijacking)

③ 스머프 공격(Smurf Attack)

④ 스니핑(Sniffing)

정답 4번

간단한 해설

수동적 공격은 데이터나 시스템을 변경하지 않고 정보를 관찰·수집하는 공격이다. 네트워크 통신을 엿듣는 스니핑 자체가 여기에 해당한다.

선지별 해설

수동적 공격은 통신을 관찰하거나 정보를 수집하되 **데이터나 시스템의 동작을 변경하지 않는** 공격이다. 각 선지가 이 기준에 해당하는지 판단한다.

① (X) 분산 서비스 거부 공격은 여러 공격 지점에서 요청이나 트래픽 등을 보내 자원을 소진시키고 정상 서비스를 방해한다. **가용성을 침해하는 능동적 공격**이므로 수동적 공격에 해당하지 않는다.

② (X) 세션 하이재킹은 성립된 통신 세션이나 인증된 사용자의 세션을 가로채 정상 사용자인 것처럼 활동하는 공격이다. 단순히 통신을 듣는 데 그치지 않고 **세션에 개입하여 권한을 악용**하므로 능동적 공격이다.

③ (X) 스머프 공격은 피해자의 주소로 위장한 ICMP 요청을 이용하여 많은 응답이 피해자에게 몰리게 하는 서비스 거부 공격이다. 패킷을 발생시켜 정상 통신을 방해하므로 능동적 공격으로 분류한다.

④ (O) 스니핑은 네트워크를 흐르는 패킷을 가로채 내용을 관찰·수집하는 도청 행위이다. **정보를 변경하지 않고 엿듣는** 스니핑 자체는 수동적 공격이다. 도청을 준비하기 위해 별도로 수행하는 ARP 스푸핑 같은 능동적 조작과는 구별한다.

따라서 수동적 공격에 가장 적합한 것은 스니핑인 ④이다.

NoteBase

문 3. 다음 설명 중 가장 옳은 것은 무엇인가?

① RC5 암호 알고리즘은 64비트의 고정된 키 길이를 사용한다.

② 3중 DES(Triple DES) 암호 알고리즘은 DES 암호 알고리즘을 개선한 것으로, DES에 비해 처리 속도가 3배 정도 빠르다.

③ IDEA 암호 알고리즘은 16라운드의 암호 방식을 적용하며, 암호화와 복호화에 사용되는 알고리즘이 달라 암호화 강도가 높다.

④ ARIA 암호 알고리즘에 사용되는 키와 블록의 길이는 AES와 동일하다.

정답 4번

간단한 해설

ARIA와 AES는 모두 **128비트 블록과 128·192·256비트 키**를 사용한다.

선지별 해설

① X. RC5는 키 길이가 고정되어 있지 않은 가변 매개변수형 블록 암호이다. 키 길이뿐 아니라 워드 크기와 라운드 수도 매개변수로 정한다. 따라서 64비트 고정 키를 사용하는 알고리즘이라는 설명은 틀리며, 블록 길이와 비밀키 길이도 구별해야 한다.

② X. Triple DES는 한 블록에 DES 연산을 세 번 적용하여 짧은 DES 키의 한계를 보완하려는 방식이다. 대표적으로 암호화·복호화·암호화의 세 단계를 거치므로 DES 한 번보다 연산량이 많아진다. 같은 처리 조건에서 3배 빠르다는 설명은 방향이 반대이며, 실제 속도 비율은 구현과 하드웨어에 따라 달라진다.

③ X. IDEA는 **8라운드와 마지막 출력 변환**으로 구성되며, 이를 흔히 8.5라운드라고 표현한다. 16라운드가 아니다. 복호화에는 순서와 값을 적절히 바꾼 서브키를 사용하여 같은 기본 처리 구조를 적용하므로, 서로 전혀 다른 암호화·복호화 알고리즘을 써서 강도가 높다는 설명도 적절하지 않다.

④ O. ARIA와 AES는 모두 **128비트 블록**을 처리하며, **128·192·256비트 키**를 지원한다. 따라서 지원하는 키 길이와 블록 길이가 같다는 설명은 맞다. 길이가 같다는 것은 두 알고리즘의 내부 연산이나 모든 구현 특성까지 동일하다는 뜻은 아니다.

따라서 ARIA와 AES의 키 길이 및 블록 길이를 올바르게 비교한 ④가 정답이다.

NoteBase

문 4. 다음 설명 중 가장 옳지 않은 것은 무엇인가?

① 5명이 서로 통신할 경우, 대칭키 암호 알고리즘과 공개키 암호 알고리즘에서 필요한 키의 개수가 다르다.

② 일반적으로 대칭키 암호 알고리즘이 공개키 암호 알고리즘보다 암호화 속도가 빠르다.

③ 공개키 암호 알고리즘의 종류로는 RSA, ECC, DSA 등이 있다.

④ 공개키 암호 알고리즘은 인증과 부인 방지를 제공한다.

정답 1번

간단한 해설

5명 사이의 쌍별 대칭키는 **10개**이고, 각자 공개키·개인키 한 쌍을 가지면 공개키 방식의 전체 키도 **10개**이다. 이 기본 모델에서는 개수가 같으므로 다르다고 한 ①이 옳지 않다.

선지별 해설

① X: 각 두 사람 사이에 서로 다른 대칭키를 하나씩 공유하는 기본 모델에서는 필요한 키가 $K_s = \frac{n(n-1)}{2}$개이다. 5명이면 $\frac{5 \times 4}{2} = 10$개이다. 공개키 방식은 한 사람당 공개키와 개인키 한 쌍을 사용하므로 전체 키 수는 $2 \times 5 = 10$개이다. 따라서 이 경우에는 **두 방식 모두 10개로 같다**. 공개키 방식의 '5쌍'을 '5개'와 혼동하거나 공개키만 세어 비교해서는 안 된다. 여기서는 공유키의 복사본 수가 아니라 서로 다른 키의 수를 센다.

② O: 대칭키 방식은 비교적 단순하고 반복적인 연산으로 많은 데이터를 처리할 수 있어, 일반적으로 공개키 방식보다 **대량 데이터 암호화가 빠르다**. 실제 통신에서 공개키 기술로 키를 안전하게 설정하고 본문은 대칭키로 암호화하는 혼합 방식이 널리 쓰이는 이유이다. 모든 구현과 연산의 속도가 예외 없이 같다는 뜻은 아니다.

③ O: 이 문항의 '공개키 암호 알고리즘'은 공개키 암호기술 전반을 가리키는 넓은 의미이다. RSA는 공개키 기반 암호화·서명에 사용되고, ECC는 타원곡선을 사용하는 공개키 암호기술 계열이며, DSA는 **공개키 기반 전자서명 알고리즘**이다. DSA가 데이터 암호화·복호화 알고리즘이라는 뜻은 아니다.

④ O: 공개키 기술을 **전자서명에 적절히 적용하면 서명자 인증과 부인 방지**를 지원한다. 개인키로 생성한 서명을 대응 공개키로 검증하여 서명자와 데이터의 관계를 확인한다. 이를 위해 공개키와 신원의 신뢰할 수 있는 연결, 개인키 보호 등도 필요하다. 단순히 수신자의 공개키로 암호화하는 것만으로 송신자 인증과 부인 방지가 자동으로 보장된다는 뜻은 아니다.

따라서 일반적인 쌍별 대칭키 모델과 사용자당 공개키·개인키 한 쌍을 비교하면, ①의 키 개수가 다르다는 설명이 틀리다.

NoteBase

문 5. SPN 구조와 Feistel 구조에 대한 설명 중 가장 옳은 것은 무엇인가?

① SPN 구조는 암호화와 복호화 과정이 동일하여 처리 속도가 빠르다.

② SPN 구조의 종류에는 AES, SEED, BLOWFISH 등이 있다.

③ Feistel 구조의 암호 강도를 결정짓는 요소는 평문 블록의 길이, 키의 길이, 라운드의 수이다.

④ Feistel 구조는 역변환 함수에 제약이 있으며, S-BOX와 P-BOX를 사용한다.

정답 3번

간단한 해설

Feistel 암호의 안전성에는 **블록 길이, 키 길이, 라운드 수**가 영향을 준다. 블록과 키의 크기는 가능한 값의 범위를, 충분한 라운드 반복은 혼돈과 확산 및 분석 공격에 대한 저항성을 좌우한다.

선지별 해설

SPN은 치환과 순열·확산 변환을 반복하여 블록을 암호화하는 구조이다. Feistel은 블록을 두 부분으로 나누고 한쪽에 라운드 함수를 적용한 결과를 다른 쪽과 XOR한 뒤 역할을 바꾸는 구조로, 복호화에 필요한 역연산의 성질이 서로 다르다.

① X: 일반적인 SPN의 복호화는 암호화의 각 변환에 대응하는 **역변환을 역순으로 적용**하므로 암호화와 복호화 과정이 동일하다고 할 수 없다. 라운드 키를 역순으로 사용하여 같은 기본 구조로 복호화할 수 있는 것이 Feistel의 특징이다. 처리 속도는 구체적인 알고리즘과 구현에 따라 달라지므로 제시된 이유만으로 빠르다고 단정할 수도 없다.

② X: AES는 SPN 계열이지만 **SEED와 BLOWFISH는 Feistel 구조**를 사용한다. 따라서 세 알고리즘을 모두 SPN으로 묶은 분류가 잘못이다.

③ O: 블록 길이는 처리하는 데이터 블록과 가능한 블록 값의 범위를, 키 길이는 전수조사해야 할 키 공간의 크기를 결정한다. 라운드 수는 변환의 반복을 통해 혼돈과 확산을 충분히 형성하는 데 영향을 주므로 세 요소 모두 암호 강도를 좌우하는 주요 설계 요소이다. 다만 안전성이 이 세 수치만으로 보장되는 것은 아니며, 라운드 함수와 키 스케줄의 설계도 중요하다.

④ X: Feistel 구조는 **라운드 함수 자체가 가역적일 필요가 없다**. 복호화 때 이미 주어진 한쪽 블록으로 같은 함수값을 구하고 XOR를 다시 적용하면 다른 쪽의 이전 값을 복원할 수 있기 때문이다. DES처럼 S-BOX와 P-BOX를 사용하는 Feistel 암호도 있지만, 그것이 라운드 함수의 역변환을 요구한다는 뜻은 아니다. 각 변환의 가역성을 확보해야 하는 일반적인 SPN과 구별해야 한다.

NoteBase

문 6. 블록 암호 운영모드 중 OFB(Output FeedBack) 모드에 대한 설명으로 가장 옳지 않은 것은 무엇인가?

① 암호기의 출력과 평문 블록을 XOR 연산하여 암호문 블록을 생성한다.

② 암호문 블록 전송 도중 오류가 발생하더라도 다음 블록의 비트에 영향을 미치지 않는다.

③ CBC(Cipher Block Chaining) 모드나 CFB(Cipher FeedBack) 모드와 마찬가지로 초기화 벡터(IV)를 사용한다.

④ 암호화와 복호화의 구조가 다르고, 병렬 처리가 가능하다.

정답 4번

간단한 해설

OFB는 암호화와 복호화에서 같은 키스트림을 만들고 XOR하는 구조를 사용한다. 다음 키스트림을 만들 때 직전 출력이 필요하므로 생성 과정은 순차적이다.

선지별 해설

OFB는 블록 암호의 출력으로 키스트림을 만들고 이를 데이터와 XOR한다. 평문을 P_i, 암호문을 C_i, 키스트림 블록을 O_i, 키 K의 암호 함수를 E_K라 하면, $O_0 = IV$, $O_i = E_K(O_{i-1})$이다.

① (O) 생성한 키스트림과 평문을 XOR하여 $C_i = P_i \oplus O_i$를 얻는다. 다음 암호 함수의 입력으로 되돌리는 것은 **암호문이 아니라 암호 함수의 출력**이다.

② (O) 암호문을 피드백하지 않으므로, 전송 중 암호문 한 비트가 반전되어도 복호문에서 대응하는 비트만 달라지고 **다음 블록으로 오류가 전파되지 않는다**. 이는 비트 반전 오류에 관한 성질이며, 비트 삽입·삭제로 동기가 어긋나는 상황과는 구별한다.

③ (O) OFB는 첫 키스트림 블록을 생성하기 위한 **초기화 벡터(IV)**를 사용한다. CBC·CFB도 IV를 사용한다는 점은 같지만, OFB에서는 같은 키로 서로 다른 메시지를 처리할 때 IV를 재사용하지 않아야 한다.

④ (X) 암호화와 복호화는 **같은 암호 함수와 XOR 구조**를 사용한다. 복호화도 $P_i = C_i \oplus O_i$이며 블록 암호의 역함수를 쓰지 않는다. 또한 각 출력은 직전 출력에 의존하므로 **키스트림 생성은 순차적**이다. 키스트림을 미리 계산할 수는 있지만, 그 생성 연산 자체를 독립적인 블록들처럼 병렬 수행할 수 있다는 뜻은 아니다.

따라서 암·복호화 구조와 병렬 처리 가능성을 모두 잘못 설명한 ④가 옳지 않다.

NoteBase

문 7. 해시함수에 대한 설명 중 가장 옳지 않은 것은 무엇인가?

① 일방향 해시함수의 경우 입력되는 메시지의 길이가 다르더라도 출력되는 해시 값의 길이는 같다.

② 해시함수의 보안 요구사항 중 강한 충돌 내성은 같은 해시 값을 갖는 두 개의 다른 입력 값을 발견하는 것이 계산상 불가능해야 하는 것을 의미한다.

③ SHA-256의 블록 길이와 출력되는 해시 값의 길이는 256비트로 동일하다.

④ 해시함수에 대한 공격 중 하나인 생일 공격(Birthday Attack)은 일방향 해시함수의 강한 충돌 내성을 깨고자 하는 공격이다.

정답 3번

간단한 해설

SHA-256은 입력 메시지를 **512비트 블록** 단위로 처리하고 최종적으로 **256비트 해시 값**을 출력한다. 처리 블록의 길이와 출력 길이를 같다고 한 설명이 틀렸다.

선지별 해설

① O: 일반적인 고정 출력 길이의 암호학적 해시함수는 허용 범위 안에서 길이가 다른 메시지를 입력받아도 정해진 길이의 해시 값을 출력한다. 예를 들어 SHA-256의 출력은 입력 메시지 길이와 관계없이 256비트이다. 출력 길이가 같다는 것이 출력 값 자체가 같다는 뜻은 아니다.

② O: 강한 충돌 내성은 해시 값이 같은 **서로 다른 두 입력을 찾기가 계산상 어려워야 한다**는 성질이다. 두 입력 중 하나가 미리 주어질 필요는 없다. '계산상 불가능'은 현실적인 자원으로 찾기 어렵다는 뜻이며, 충돌이 수학적으로 존재하지 않는다는 뜻은 아니다.

③ X: SHA-256은 패딩된 입력을 **512비트 블록**으로 나누어 처리하며, 최종 출력인 메시지 다이제스트의 길이는 **256비트**이다. '256'이라는 이름은 출력 길이를 나타내므로 블록 길이를 뜻하는 것으로 혼동해서는 안 된다.

④ O: 생일 공격은 여러 입력의 해시 값을 구하여 그중 같은 값을 갖는 서로 다른 입력 쌍을 찾는 공격이다. 특정 입력 하나의 해시 값에 맞추는 것이 아니라 임의의 충돌 쌍을 찾으므로 강한 충돌 내성을 공격한다. 출력이 균등하게 분포하는 이상적인 n비트 해시라면 충돌을 찾는 데 필요한 시도 수의 규모는 대략 $2^{n/2}$이다.

NoteBase

문 8. 다음은 A와 B가 디피-헬만(Diffie-Hellman) 키 교환 알고리즘을 이용하여 서로 공유할 키를 생성하는 절차에 대한 설명이다. ㉠~㉢에 들어갈 내용으로 올바른 것은?

(1) A는 소수 p와 p의 원시근 g를 선택하여 사전에 B와 공유한다.
(2) A는 p보다 작은 양수 a를 선택하여 K_A =(㉠)를 계산한다.
(3) B도 p보다 작은 양수 b를 선택하여 K_B =(㉡)를 계산한다.
(4) A와 B가 서로 K_A와 K_B를 공유한다.
(5) A가 K_B^a p, B가 K_A^b p를 계산하여 서로 (㉢)라는 공통의 키를 공유하게 된다.

① ㉠: g^a p ㉡: g^b p ㉢: p^ab g
② ㉠: g^a p ㉡: g^b p ㉢: g^ab p
③ ㉠: p^a g ㉡: p^b g ㉢: p^ab g
④ ㉠: p^a g ㉡: p^b g ㉢: g^ab p

정답 2번

간단한 해설

상대의 공개값을 자기 비밀 지수로 거듭제곱하면 양쪽 모두 g^ab p를 얻는다. 이때 **밑은 g, 나머지를 구하는 법은 p**로 유지해야 한다.

빈칸별 해설

공개된 p는 나머지를 구할 때의 법이고, g는 거듭제곱의 밑으로 사용하는 원시근이다. A와 B는 각각 비밀값 a와 b를 공개하지 않고, g를 자기 비밀값만큼 거듭제곱한 나머지인 공개값을 교환한다.

㉠: g^a p. A는 비밀값 a로 K_A=g^a p를 계산한다. (4)에서 B에게 전달하는 것은 a 자체가 아니라 이 공개값이다.

㉡: g^b p. B도 같은 밑 g와 같은 법 p를 사용하여 K_B=g^b p를 계산한다. A와 B가 공통 매개변수를 사용하므로 이후 계산 결과를 일치시킬 수 있다.

㉢: g^ab p. A는 B의 공개값에 자신의 비밀 지수 a를 적용하므로 K_B^a p=g^ba p를 얻는다. B는 A의 공개값에 자신의 비밀 지수 b를 적용하므로 K_A^b p=g^ab p를 얻는다. **지수의 곱이 같으므로** 두 결과가 일치하며, 이것이 문제에서 말하는 공통의 키이다.

따라서 ㉠은 g^a p, ㉡은 g^b p, ㉢은 g^ab p인 ②가 정답이다. p와 g를 바꾼 식은 문제에서 정한 밑과 법의 역할에 맞지 않는다.

NoteBase

문 9. 전자 서명의 특성에 대한 설명 중 가장 옳지 않은 것은 무엇인가?

① 위조 불가(Unforgeable) : 합법적인 서명자 이외의 다른 사람이 전자 문서에 대한 전자 서명을 생성할 수 없어야 한다.

② 변경 불가(Unalterable) : 서명한 문서의 내용을 변경할 수 없어야 한다.

③ 재사용 불가(Not Reusable) : 전자 문서의 서명은 다른 전자 문서의 서명으로 사용할 수 없어야 한다.

④ 부인 방지(Non-Repudiation) : 누구든지 전자 서명의 서명자를 검증할 수 있어야 한다.

정답 4번

간단한 해설

누구든지 서명자를 검증할 수 있다는 설명은 **서명자 인증·검증 가능성**이다. 부인 방지는 서명자가 자신의 서명 사실을 나중에 부정하지 못하도록 하는 성질이므로, 두 개념을 혼동한 **④가 틀리다**.

선지별 해설

① O: '위조 불가'는 서명자의 개인키를 갖지 못한 제3자가 **그 서명자의 유효한 서명을 만들어 내기 어려워야 한다**는 성질이다. 공개된 검증키를 알고 있더라도 서명 생성 능력을 얻는 것은 아니다. 안전한 알고리즘과 키 보호를 전제로 하는 계산적 안전성의 의미이다.

② O: '변경 불가'는 서명 후 문서가 바뀌면 **기존 서명으로 정상 검증되지 않아야 한다**는 뜻이다. 전자서명은 문서의 내용과 연결되므로 내용을 변조하면 무결성 검증이 실패한다. 파일의 비트를 물리적으로 바꾸는 행위 자체를 불가능하게 만드는 쓰기 방지 기능이라는 뜻은 아니다.

③ O: '재사용 불가'는 어떤 문서에 대한 서명을 **내용이 다른 문서의 유효한 서명으로 전용할 수 없어야 한다**는 성질이다. 서명은 해당 문서 또는 그 해시값에 결부된다. 같은 문서와 서명을 복사할 수 없다는 뜻이나 통신에서의 재전송 공격을 전자서명만으로 모두 막는다는 뜻은 아니다.

④ X: 누구든지 적절한 공개 검증정보로 서명자를 확인할 수 있어야 한다는 설명은 **'서명자 인증' 또는 '검증 가능성'**에 해당한다. '부인 방지'는 서명자가 나중에 자신의 서명 사실을 부당하게 부정하지 못하도록 증거를 제공하는 성질이다. 공개키와 신원의 신뢰할 수 있는 연결 및 개인키 보호 등이 이를 뒷받침해야 한다.

따라서 특성 이름과 설명이 맞지 않는 것은 ④이다.

NoteBase

문 10. 다음 공개키 기반 구조(Public Key Infrastructure)에 대한 설명 중 가장 옳은 것은 무엇인가?

① 공개키 기반 구조는 대칭키 암호시스템에 기초하여 디지털 인증서를 생성하고 관리하는데 필요한 정책 및 절차이다.

② 정책 인증 기관(Policy Certification Authority)은 공개키 기반 구조 전반에 사용되는 정책과 절차를 수립하는 기관이다.

③ 등록 기관(Registration Authority)은 공개키 기반 구조의 필수 구성요소로서, 사용자의 신분과 소속을 확인하고 사용자에게 공개키 인증서를 발행하는 기능을 수행한다.

④ 인증서에는 버전, 일련번호, 유효기간 등의 정보가 담겨있다.

정답 4번

간단한 해설

공개키 인증서는 주체의 신원과 공개키를 연결하는 전자 문서로, **버전·일련번호·유효기간** 등을 담는다. 버전은 형식을, 일련번호는 발급된 인증서의 식별을, 유효기간은 사용 가능한 시간 범위를 나타낸다.

NoteBase

선지별 해설

공개키 기반 구조(PKI)는 공개키와 그 소유자의 신원을 신뢰할 수 있게 연결하고 인증서를 발급·배포·검증·폐지하기 위한 기술, 기관, 정책 및 절차의 체계이다. 정책을 정하는 역할, 신원을 확인하는 역할, 인증서를 발급하는 역할을 구별해야 한다.

① X: PKI의 기반은 대칭키 암호시스템이 아니라 **공개키 암호시스템**이다. 인증기관은 인증서에 전자서명하고, 이용자는 인증기관의 공개키로 서명을 검증하여 공개키와 주체의 연결이 인증기관에 의해 보증되었는지 확인한다.

② X: 전통적인 계층형 PKI의 역할 구분에서 **PKI 전반의 정책과 절차를 수립하는 기관은 정책승인기관(PAA)**이다. 정책인증기관(PCA)은 그 아래에서 자신의 도메인에 속한 인증기관과 사용자가 따라야 할 정책을 정하고 하위 인증기관을 인증하는 역할을 한다. PCA가 정책을 전혀 정하지 않는 것이 아니라, 선지의 '전반'이라는 범위가 잘못 연결되어 있다.

③ X: 등록기관(RA)은 신청자의 신분·소속 등을 확인하고 등록 절차를 수행하지만, **인증서를 발급하고 서명하는 주체는 인증기관(CA)**이다. 또한 RA는 별도 기관으로 반드시 두어야 하는 필수 구성요소가 아니며, 그 기능을 CA가 직접 수행할 수도 있다.

④ O: X.509 공개키 인증서에는 **버전, 일련번호, 유효기간**과 함께 발급자, 인증 대상 주체, 주체의 공개키 정보 등이 포함된다. 일련번호는 같은 발급기관이 발급한 인증서를 구분하고, 유효기간은 시작 시각과 종료 시각으로 표현된다. 공개키 인증서가 개인키를 공개하는 문서인 것은 아니다.

NoteBase

문 11. 다음 중 강제적 접근 제어(MAC : Mandatory Access Control)에 대한 설명으로 옳은 것은 모두 몇 개인가?

가. 유닉스(UNIX) 운영체제의 기본 접근제어 방식에 적용되었다.
나. 최초 객체에 설정된 강제적 접근 제어 관계는 복사된 객체에도 그대로 적용된다.
다. 부여된 역할에 기반하여 접근이 제어되므로 주로 군사용으로 사용된다.
라. 강제적 접근 제어의 대표적인 구현 형태는 ACL(Active Control List)이다.

① 0개
② 1개
③ 2개
④ 3개

정답 2번

간단한 해설

MAC는 **시스템이 정한 보안 정책**을 강제하므로, 정보를 복사했다고 사용자가 접근 제한을 임의로 풀 수 없다.
소유자가 권한을 정하는 DAC 및 역할별 권한을 배정하는 RBAC와 구별한다.

NoteBase

보기별 해설

강제적 접근 제어(MAC)는 사용자의 임의적인 권한 변경보다 시스템의 보안 정책을 우선하여 접근을 통제한다. 보안 등급을 사용하는 대표적인 MAC에서는 주체의 인가 수준과 객체의 보안 등급 등을 비교한다.

가. X: 전통적인 UNIX의 소유자·그룹·기타 사용자별 읽기·쓰기·실행 권한은 **임의적 접근 제어(DAC)**에 해당한다. 파일 소유자가 허용 권한을 정하는 방식이므로 MAC의 기본 적용 사례가 아니다. UNIX 계열에 MAC 기능을 추가할 수 있다는 사실과 기본 권한 방식은 구별한다.

나. O: MAC에서는 정보가 다른 객체로 복사되어도 **복사를 이유로 강제 보안 정책을 벗어날 수 없다**. 사용자가 복사본을 만들었다고 해서 원래 정보의 접근 제한을 임의로 해제하거나 권한 없는 주체에게 전달할 수 없도록 통제한다.

다. X: 사용자에게 부여한 **역할을 기준으로 권한을 배정하는 것은 RBAC**이다. 군사 보안에서 사용하는 대표적인 MAC은 비밀 등급과 취급 인가 수준 등을 바탕으로 정보를 보호한다. 역할에 따른 권한 배정 자체를 MAC의 정의로 삼을 수 없다.

라. X: 객체별로 접근 가능한 주체와 권한을 나열한 ACL은 **DAC의 대표적인 구현 수단**이다. MAC을 특징짓는 것은 사용자가 임의로 바꿀 수 없는 강제 보안 정책이다. 또한 ACL의 정확한 명칭은 'Access Control List'이며, 보기의 'Active Control List'는 잘못된 표현이다.

따라서 옳은 보기는 나 하나이므로 1개인 ②와 연결된다.

NoteBase

문 12. 다음 중 커버로스(Kerberos) 인증 프로토콜에 대한 설명으로 옳은 것은 모두 몇 개인가?

가. 커버로스는 개방형 분산 통신망에서 클라이언트와 서버 간의 상호 인증을 지원하는 인증 프로토콜이다.
나. 커버로스를 통해 데이터의 기밀성과 무결성을 보장할 수 있다.
다. 커버로스는 타임 스탬프(Time Stamp)를 이용하므로 다른 사람이 티켓을 복사하여 재사용하는 것을 방지할 수 있다.
라. 커버로스는 세사미(SESAME)의 기능을 확장하고 약점을 보완하기 위해 개발된 것이다.

① 1개
② 2개
③ 3개
④ 4개

정답 3번

간단한 해설

개발 관계가 반대로 제시되어 있다. **SESAME가 Kerberos를 확장·보완**하여 접근권한 관리와 공개키 활용 등의 기능을 추가한 체계이다.

보기별 해설

가. O: Kerberos는 신뢰할 수 있는 인증 서버와 티켓을 이용하여 분산 환경의 사용자·서비스 신원을 확인한다. 클라이언트의 신원뿐 아니라 서버의 신원도 확인하는 **상호 인증**을 지원한다.

나. O: 인증 과정에서 확보한 세션 키를 사용하여 응용 데이터의 기밀성과 무결성을 보호할 수 있다. Kerberos의 KRB_SAFE 메시지는 무결성 보호에, KRB_PRIV 메시지는 암호화된 데이터 전달에 이용된다. 다만 인증에 성공했다는 이유만으로 모든 응용 데이터가 자동으로 암호화되는 것은 아니며, 응용 프로그램이 해당 보호 기능을 사용해야 한다.

다. O: 티켓과 함께 제시하는 인증자의 타임스탬프로 요청의 최신성을 확인하여 재전송 공격을 방어한다. 실제로는 **허용 시각 차이 검사와 이미 사용한 인증자 기록** 등을 함께 적용한다. 정당한 사용자의 유효한 티켓 재사용 자체를 금지하는 것이 아니라, 다른 사람이 가로챈 인증 요청을 그대로 다시 사용하는 것을 막는 취지이다.

라. X: Kerberos가 SESAME를 확장한 것이 아니라, **SESAME가 Kerberos를 확장·보완**한 것이다. SESAME는 인증 외에 권한 정보에 기초한 접근 통제와 공개키 기술 활용 등을 보강한 분산 보안 체계이다.

옳은 보기는 가·나·다의 3개이므로 ③에 해당한다.

NoteBase

문 13. 일회용 패스워드(One Time Password)의 생성 및 인증 방식 중 시간 동기화 방식에 대한 설명으로 가장 옳지 않은 것은 무엇인가?

① OTP 생성 매체와 인증 서버의 시간 정보가 동기화되어 있어야 한다.

② 일정 시간 이상 인증을 받지 못하면 새로운 비밀번호 생성 시까지 기다려야 하는 문제점이 있다.

③ 질의응답 방식보다 사용은 간편하지만, 호환성이 낮다.

④ RSA사에서 만든 Secure ID가 대표적이다.

정답 3번

간단한 해설

시간 동기화 OTP는 별도의 질의값 입력 없이 표시된 코드를 제출해 기존 비밀번호 입력 절차와 연계하기 쉽다. 따라서 **사용은 간편하지만 호환성이 낮다고 한** ③이 가장 부적절하다. 다만 실제 상호 운용에는 알고리즘·비밀값·시간 기준의 일치가 필요하다.

선지별 해설

① O: 시간 동기화 방식은 생성기와 인증 서버가 공유 비밀값과 **서로 맞춰진 시간 기준**으로 같은 OTP를 계산하는 방식이다. 시간 구간의 길이 등 생성 조건도 일치해야 한다. 실제 시스템은 시계 오차와 전송 지연을 고려해 제한된 허용 구간을 둘 수 있으므로 두 시계가 오차 없이 완전히 같아야 한다는 뜻은 아니다.

② O: 시간 동기화 방식은 한 시간 구간 안에서 같은 코드가 유지되므로, **새로운 코드가 필요하면 다음 생성 시점까지 기다리는 불편**이 생길 수 있다. 지문은 정해진 시간 안에 인증을 마치지 못해 새 코드로 다시 시도해야 하는 시간 제약을 설명한다. 다만 모든 인증 실패 뒤에 반드시 한 주기 전체를 기다리는 것은 아니며, 이미 새 코드가 표시되었다면 그 유효한 코드로 바로 재시도할 수 있다. 재시도 허용 여부와 시간 오차 허용 범위는 서버 정책에 따른다.

③ X: 시간 동기화 방식은 서버의 질의값을 생성기에 옮겨 입력할 필요 없이 표시된 OTP를 제출하므로 사용이 간편하다. 또한 **별도의 질의·응답 입력 절차 없이 비밀번호 입력 방식에 연결하기 쉽다**는 점에서 호환성이 낮다고 설명하는 것은 부적절하다. 공통 알고리즘과 비밀값·시간 구간 등의 조건이 맞으면 상호 운용할 수 있다. 서로 다른 제품이나 서비스의 OTP를 아무 설정 없이 그대로 사용할 수 있다는 뜻은 아니다.

④ O: 지문의 'Secure ID'는 RSA의 **'SecurID'**를 가리킨다. 대표적인 시간 기반 토큰은 내장 시계와 등록된 비밀값을 이용하여 일정 주기마다 토큰 코드를 바꾸고 서버가 이를 검증한다. 대표적인 하드웨어 토큰의 주기는 60초이지만, 모든 시간 기반 OTP의 주기가 반드시 60초인 것은 아니다.

따라서 간편한 사용과 시스템 연계의 특성을 잘못 대비한 ③이 인정 정답에 해당한다.

NoteBase

문 14. 버퍼 오버플로우(Buffer Overflow) 공격에 대응하는 방법으로 가장 옳지 않은 것은 무엇인가?

① 버퍼 오버플로우 공격에 대응하기 위해 변수 타입과 그 타입에 허용되는 연산들에 대해 강력한 표기법을 제공하는 고급 수준의 프로그래밍 언어를 사용한다.

② gets(), scanf(), strcat() 함수 사용을 자제하고 fgets(), fscanf(), strcpy() 함수 사용을 권장한다.

③ 스택 배치를 랜덤하게 설정하고 프로그램 실행 시마다 다른 주소에 배치한다.

④ 스택상에 있는 공격자의 코드가 실행되지 못하도록 한다.

정답 2번

간단한 해설

fscanf()와 strcpy()는 **버퍼 크기를 자동으로 검사하는 안전한 대체 함수가 아니다**. 함수 이름만 바꾸는 것이 아니라 실제 저장 공간에 맞게 입력·복사 길이를 제한하고 문자열 종료 공간까지 확보해야 한다.

선지별 해설

버퍼 오버플로우는 할당된 버퍼의 경계를 넘어 데이터를 써서 인접 메모리를 손상시키는 문제이다. 경계를 넘는 쓰기를 예방하는 방법과, 취약점이 남아 있더라도 악용을 어렵게 하는 실행 환경의 방어 방법을 함께 구분한다.

① O: 타입과 허용 연산을 엄격히 검사하고 메모리 접근을 관리하는 고급 언어를 사용하면 잘못된 연산과 범위 밖 접근을 줄일 수 있다. 특히 **배열 경계 검사와 메모리 안전성을 제공하는 언어**는 임의 주소에 데이터를 쓰는 위험을 낮춘다. 단순히 타입 표기법이 엄격하다는 사실만으로 모든 메모리 오류가 사라지는 것은 아니다.

② X: gets()는 입력 길이를 제한할 수 없고, scanf() 계열의 문자열 입력과 strcat()도 적절한 길이 관리 없이 사용하면 넘침이 발생할 수 있다. 그러나 **fscanf()와 strcpy() 역시 자동으로 목적지 버퍼의 크기를 확인하지 않는다**. fscanf()의 문자열 입력에는 저장 공간을 고려한 폭 제한이 필요하고, strcpy()는 원본 문자열과 종료 문자가 모두 들어갈 공간이 있는지 별도로 확인해야 한다. fgets()도 실제 버퍼 용량에 맞는 크기 인수를 전달해야 하므로, 제시된 함수들로 일괄 교체하는 것만으로 안전해지지 않는다.

③ O: 주소 공간 배치 난수화(ASLR)는 스택 등 메모리 영역의 주소 배치를 실행마다 달라지게 하여 **공격에 필요한 주소의 예측을 어렵게**한다. 이는 버퍼 경계 검사 자체를 대신하는 것이 아니라 취약점의 악용 가능성을 낮추는 방어 기법이다.

④ O: 스택을 실행 불가 영역으로 설정하면 스택에 주입된 데이터를 명령어로 실행하지 못하게 할 수 있다. NX·DEP와 같은 실행 방지는 **스택에 주입한 코드의 실행을 차단**하는 데 유효하다. 다만 메모리 손상 자체나 기존 코드의 재사용까지 모두 막는 것은 아니므로 다른 방어와 함께 적용한다.

NoteBase

문 15. 유닉스(Unix) 운영체제에서 명령어 ‘chmod 752 test.c’를 실행한 파일의 접근 권한에 대한 설명으로 가장 옳은 것은 무엇인가?

① group 권한 : 읽기(X) 쓰기(O) 실행(X)

② user 권한 : 읽기(O) 쓰기(O) 실행(O)

③ group 권한 : 읽기(O) 쓰기(O) 실행(O)

④ user 권한 : 읽기(O) 쓰기(X) 실행(O)

정답 2번

간단한 해설

752의 맨 앞자리 7은 파일 소유자의 권한이며, 7 = 4 + 2 + 1이므로 **읽기·쓰기·실행이 모두 허용**된다. 세 자리를 소유자·그룹·기타 사용자의 순서로 구분하는 것이 핵심이다.

계산 과정

‘chmod 752 test.c’에서 세 자리 숫자는 왼쪽부터 파일 소유자(user), 소유 그룹(group), 그 밖의 사용자(others)의 권한을 나타낸다. 각 자리에서 읽기 r은 4, 쓰기 w는 2, 실행 x는 1로 표시하며, 허용할 권한의 값을 더한다.

소유자 권한 7: 7 = 4 + 2 + 1이므로 읽기·쓰기·실행 권한이 모두 있다. 기호로는 **rwx**이며, 읽기(O)·쓰기(O)·실행(O)에 해당한다.

그룹 권한 5: 5 = 4 + 1이므로 읽기와 실행 권한은 있지만 쓰기 권한은 없다. 기호로는 r-x이며, 읽기(O)·쓰기(X)·실행(O)에 해당한다.

기타 사용자 권한 2: 쓰기 권한만 있고 읽기와 실행 권한은 없다. 기호로는 -w-이다. 따라서 전체 권한 비트는 rwxr-x-w-이며, 끝자리 2를 그룹의 권한으로 읽어서는 안 된다.

따라서 소유자(user)에게 읽기·쓰기·실행이 모두 허용된다고 한 ②가 정답이다. 문제는 설정된 권한 비트를 묻는 것이므로, 파일 이름의 확장자가 .c라는 사실로 이 권한 계산을 바꾸지 않는다.

NoteBase

문 16. 다음에서 설명하는 윈도우 인증의 구성 요소로 가장 옳은 것은 무엇인가?

- 사용자의 계정과 패스워드가 일치하는 사용자에게 고유의 SID(Security Identifier)를 부여한다.
- SID에 기반을 두어 파일이나 디렉터리에 대한 접근의 허용 여부를 결정하고 이에 대한 감사 메시지를 생성한다.

① LSA(Local Security Authority)

② SRM(Security Reference Monitor)

③ SAM(Security Account Manager)

④ SSH(Secure Shell)

정답 2번

간단한 해설

파일·디렉터리에 대한 **접근 허용 여부를 검사하고 감사 메시지를 생성**하는 구성 요소는 SRM이다. 사용자 신원 확인보다 인증 후 자원 접근을 통제하는 기능이 결정적인 단서이다.

공통 해설

SRM(Security Reference Monitor)은 윈도우 커널에서 **접근 권한 검사와 보안 감사**를 수행하는 구성 요소이다. 접근 토큰에 담긴 사용자·그룹의 SID 등 보안 정보와 대상 파일·디렉터리의 접근 제어 정보를 대조하여 요청한 작업을 허용할지 판단한다. 또한 감사 정책과 대상의 감사 설정에 따라 관련 감사 메시지를 생성한다. 따라서 지문의 'SID에 기반을 둔 접근 허용 여부 결정과 감사 메시지 생성'은 SRM의 기능에 해당한다.

다만 '계정과 패스워드가 일치하는 사용자에게 고유의 SID를 부여한다'는 표현은 엄밀히 구분해야 한다. **계정 SID는 계정 생성 시 부여**되며, 로그인에 성공하면 기존 SID 등이 포함된 접근 토큰이 생성된다. SRM이 비밀번호를 확인하거나 로그인할 때마다 새로운 계정 SID를 발급하는 것은 아니다. LSA가 관여하는 사용자 인증과 SRM의 자원 접근 권한 검사를 구분하면, 이 문항에서 SRM을 가리키는 결정적인 기능을 파악할 수 있다.

NoteBase

문 17. 유닉스(Unix)와 관련된 설명 중 가장 옳지 않은 것은 무엇인가?

① /etc 디렉터리에는 시스템의 환경 설정 및 주요 설정 파일이 있다.

② pacct는 시스템에 로그인한 모든 사용자가 로그아웃할 때까지 수행한 프로그램 정보와 관련된 로그 파일이다.

③ 파일시스템의 i-Node는 파일의 유형, 파일 수정시각, 파일의 이름 등의 정보를 가지고 있다.

④ SetUID가 설정된 파일은 실행되는 동안 파일 소유자의 권한으로 실행된다.

정답 3번

간단한 해설

i-Node는 파일의 유형·권한·크기·시각 등의 메타데이터를 보관하지만 **파일 이름은 보관하지 않는다**. 파일 이름과 i-Node 번호의 연결은 디렉터리 엔트리에 저장된다.

선지별 해설

유닉스에서는 시스템 설정 파일, 프로세스 사용 기록, 파일 메타데이터, 실행 권한을 서로 다른 구조와 기능으로 관리한다. 특히 파일 이름을 관리하는 디렉터리와 파일의 속성을 관리하는 i-Node를 구분해야 한다.

① O: /etc 디렉터리는 시스템 전반의 환경과 서비스 동작을 정하는 **주요 설정 파일을 두는 위치**이다. 사용자별 개인 설정이나 일반 실행 프로그램을 모아 두는 디렉터리와 역할이 다르다.

② O: pacct는 프로세스 어카운팅이 활성화된 시스템에서 사용자가 실행한 프로그램과 자원 사용 등을 기록하는 로그 파일이다. 이를 통해 로그인 후 수행한 프로그램의 흔적을 확인할 수 있다. 보통 **프로세스가 종료될 때 기록**되며, 로그인·로그아웃 시각 자체만을 기록하는 파일과 구별된다. 선지의 표현은 사용자 활동의 범위를 설명한 것이지, 로그아웃 때에만 기록된다는 뜻은 아니다.

③ X: i-Node에는 파일 유형, 접근 권한, 소유자, 크기, 수정시각과 데이터 위치 등의 정보가 있으나 **파일 이름은 디렉터리 엔트리**에 저장된다. 디렉터리 엔트리는 이름을 i-Node 번호와 연결하므로 여러 이름이 같은 i-Node를 가리키는 하드 링크도 가능하다.

④ O: SetUID가 정상적으로 적용되는 실행 파일은 실행한 사용자가 아니라 **파일 소유자의 유효 사용자 ID**를 사용하여 동작한다. 따라서 소유자의 권한이 필요한 제한된 작업을 수행할 수 있다. 항상 관리자 권한을 얻는다는 뜻은 아니며, 파일 소유자가 누구인지에 따라 권한이 달라진다.

NoteBase

문 18. 방화벽(Firewall)에 대한 다음 설명 중 옳지 않은 것은 모두 몇 개인가?

가. 패킷 필터링(Packet Filtering) 방화벽은 패킷을 조사하여 허용 여부를 결정하면 되므로 동작 방식이 간단하여 구현하기 쉽다.
나. 스테이트풀 패킷 검사(Stateful Packet Inspection) 방화벽은 종단-대-종단 TCP 연결을 허용하지 않고, 두 개의 TCP 연결을 설정한다.
다. 회로 레벨 프록시(Circuit Level Proxy) 방화벽은 TCP 순서번호를 추적하므로 순서번호를 이용한 세션 하이재킹과 같은 공격을 막을 수 있다.
라. 애플리케이션 게이트웨이(Application Gateway) 방화벽은 프록시 서버를 통해 외부 네트워크와의 직접적인 연결을 피할 수 있다.

① 1개
② 2개
③ 3개
④ 4개

정답 2번

간단한 해설

옳지 않은 설명은 **나, 다의 2개이므로** ②이다. 두 TCP 연결을 만들어 중계하는 것은 회로 레벨 프록시이고, 연결 상태와 TCP 순서번호를 추적하여 비정상 패킷을 검사하는 것은 스테이트풀 패킷 검사에 해당한다.

NoteBase

보기별 해설

가. O. 패킷 필터링 방화벽은 출발지·목적지 IP 주소, 포트 번호, 프로토콜 등 헤더 정보를 규칙과 대조하여 통과 여부를 정한다. 연결 상태나 응용 데이터의 의미까지 분석하는 방식보다 구조가 단순하여 구현하기 쉽다.

나. X. 종단 간 연결을 끊고 내부 호스트와 프록시, 프록시와 외부 호스트 사이에 두 개의 TCP 연결을 설정하는 것은 **회로 레벨 프록시의 동작**이다. 스테이트풀 패킷 검사는 연결 상태표를 유지하면서 통과하는 패킷이 정상적인 연결 흐름에 속하는지를 확인하는 방식이다.

다. X. 이 문항의 방화벽 유형 구분에서 TCP 순서번호를 연결 상태와 함께 추적하여 비정상 패킷을 걸러 내는 기능은 **스테이트풀 패킷 검사**의 특징에 해당한다. 회로 레벨 프록시의 중심 기능은 연결을 두 구간으로 나누어 허용된 세션의 데이터를 중계하는 것이다. 순서번호 검사를 통한 방어는 유효 범위를 벗어난 패킷 주입 등을 차단한다는 뜻이며, 모든 세션 하이재킹을 막는다는 보장은 아니다.

라. O. 애플리케이션 게이트웨이는 응용 프로토콜을 이해하는 프록시가 통신을 대신 처리한다. 내부 사용자는 프록시에 연결하고 프록시가 외부 서버에 별도로 연결하므로, 내부와 외부 호스트가 직접 연결하지 않도록 할 수 있다.

옳지 않은 보기는 나와 다이므로 개수는 2개이며, 이에 대응하는 선택지는 ②이다.

NoteBase

문 19. 침입탐지시스템(IDS)에 대한 설명으로 가장 옳은 것은 무엇인가?

① 침입 경로를 찾을 수 있도록 탐지대상으로부터 생성되는 로그를 제공한다.

② Host-IDS는 운영체제에 독립적이다.

③ 오용 침입탐지 기법은 오탐률(False Positive)이 높다.

④ '침입분석 및 탐지 → 데이터수집 → 데이터 가공 및 축약 → 보고 및 대응'의 단계로 실행된다.

정답 1번

간단한 해설

IDS가 남기는 이벤트·탐지 로그는 시간과 접근 대상 등을 연결해 **침입 경로를 조사하는 근거**가 된다. 탐지 결과를 알리는 것뿐 아니라 사고 분석에 필요한 기록을 제공하는 기능에 주목해야 한다.

선지별 해설

① O. IDS는 호스트의 감사기록이나 네트워크에서 관찰한 이벤트 등을 수집·분석하고, 탐지 결과와 관련 정보를 로그로 남긴다. 시간, 주소, 계정, 접근 대상 등의 기록은 침입이 어떤 경로와 순서로 진행되었는지 조사하는 근거가 된다. 다만 로그가 있다는 사실만으로 모든 침입 경로나 공격자의 신원이 자동으로 확정되는 것은 아니다.

② X. Host-IDS는 개별 호스트의 시스템 호출, 감사 로그, 파일 변경 등 운영체제가 제공하는 정보를 바탕으로 동작한다. 설치할 에이전트와 수집 방식이 해당 운영체제의 구조·버전·기능에 맞아야 하므로 **운영체제에 종속적**이다. 여러 운영체제를 지원하는 제품이 있다는 것과 운영체제에 독립적이라는 것은 다르다.

③ X. 오용 침입탐지는 알려진 공격의 패턴이나 시그니처와 관찰된 활동을 비교하는 방식이다. 명확한 공격 패턴을 기준으로 하므로 일반적으로 이상 탐지보다 오탐을 줄이기 쉬우며, 대표적 한계는 알려지지 않은 공격이나 변형을 놓칠 수 있다는 점이다. 정상 활동을 공격이라고 판단하는 **오탐(False Positive)**이 많이 발생하기 쉽다는 특징은 정상 범위에서 벗어난 활동을 탐지하는 이상 탐지에서 주로 문제 된다. 실제 오탐률은 규칙과 환경에 따라 달라지므로 오용 탐지에서 오탐이 전혀 없다는 뜻은 아니다.

④ X. 기본 흐름은 **데이터 수집 → 데이터 가공 및 축약 → 침입분석 및 탐지 → 보고 및 대응**이다. 먼저 로그·패킷 등의 자료를 얻고 분석 가능한 형태로 정리한 뒤, 공격 징후를 판단하여 결과를 알리거나 대응한다. 분석할 자료를 수집하기 전에 침입분석을 먼저 수행한다고 제시한 순서가 잘못되었다.

따라서 로그를 통해 침입 경로의 조사를 지원한다는 ①이 정답이다.

NoteBase

문 20. 가상사설망(VPN)에 대한 설명으로 가장 옳지 않은 것은 무엇인가?

① 공중 네트워크를 이용하여 사설 네트워크와 같은 효과를 제공한다.

② VPN에 사용되는 터널링(Tunneling)은 터미널이 형성되는 양 호스트 사이에 전송되는 패킷을 추가 헤더 값으로 인캡슐화하는 기술이다.

③ L2F(Layer2 Forwarding)는 PPTP(Point-to-Point Tunneling Protocol)와 L2TP(Layer2 Tunneling Protocol)를 결합한 방식이다.

④ VPN은 데이터 암호화, 접근제어 등의 보안 서비스를 제공한다.

정답 3번

간단한 해설

L2F와 PPTP의 개념과 기능을 통합하여 발전시킨 프로토콜은 **L2TP**이다. L2F가 PPTP와 L2TP를 결합한 방식이라는 설명은 관계가 뒤바뀌었다.

선지별 해설

① O: VPN은 인터넷 같은 공중망 위에 논리적인 전용 통신 경로를 구성하여 **사설망과 같은 연결 효과**를 제공한다. 별도 전용 회선을 모든 구간에 설치하지 않고도 지점 간 또는 원격 사용자와 내부망 사이를 연결할 수 있다.

② O: 터널링은 원래 전송할 패킷을 다른 프로토콜의 패킷 안에 넣고 **추가 헤더로 캡슐화**하여 터널의 양 끝점 사이로 전달하는 기술이다. 수신 측 끝점은 추가 헤더를 제거하여 원래 패킷을 얻는다. 선지의 '터미널이 형성되는'이라는 표현은 부정확하지만, 양 끝점 사이의 패킷 캡슐화라는 핵심 설명은 터널링에 해당한다.

③ X: L2F와 PPTP의 개념과 기능을 통합하여 발전시킨 것은 **L2TP**이다. L2F가 PPTP와 L2TP를 결합한 결과라는 설명은 발전 관계를 거꾸로 제시했다.

④ O: 보안 VPN은 암호화로 전송 내용의 기밀성을 보호하고, 인증과 접근제어로 허용된 사용자·통신만 연결되도록 한다. 다만 **터널링 자체가 암호화를 보장하는 것은 아니다**. 예를 들어 L2TP에 IPsec 같은 보안 수단을 결합하여 전송 데이터를 보호한다.

따라서 L2F·PPTP·L2TP의 관계를 뒤바꾼 ③이 가장 옳지 않다.

NoteBase

문 21. 다음에서 설명하는 시스템으로 가장 옳은 것은 무엇인가?

· 서로 다른 보안장비에서 발생한 로그를 하나의 화면에서 모니터링 할 수 있는 통합 관리 시스템
· 보안 정책 통합 관리와 적용을 통한 보안 운영 관리의 일관성 제공

① NAC (Network Access Control)
② PMS (Patch Management System)
③ BCM(Business Continuity Management)
④ ESM (Enterprise Security Management)

정답 4번

간단한 해설

서로 다른 보안장비의 로그와 보안 정책을 **통합 관리**하는 것이 ESM의 특징이다. 장비별 정보를 한 화면에서 확인하고 정책을 일관되게 적용한다는 두 설명이 이에 해당한다.

공통 해설

ESM(Enterprise Security Management, 통합보안관리)은 여러 종류의 보안장비를 연계하여 **보안 정보와 정책을 중앙에서 통합 관리**하는 시스템이다. 로그는 장비에서 발생한 사건이나 동작의 기록이다. 예를 들어 방화벽의 접속 차단 기록과 침입탐지시스템의 공격 탐지 기록을 모으면, 관리자는 각 장비의 화면을 따로 열지 않고 하나의 화면에서 보안 상황을 확인할 수 있다. 이는 지문의 첫 번째 특징인 서로 다른 보안장비의 로그 통합 모니터링에 해당한다.

보안 정책도 통합하여 관리하고 관련 장비에 적용하면, 장비마다 정책을 따로 설정하면서 생길 수 있는 불일치를 줄일 수 있다. 이는 두 번째 특징인 **보안 운영 관리의 일관성**을 제공한다는 뜻이다. 따라서 두 특징은 모두 여러 보안장비를 하나의 관리 체계로 묶는 ESM의 기능을 설명한다.

NoteBase

문 22. 다음에서 설명하는 블루투스(Bluetooth)의 보안 취약점으로 가장 적절하게 연결된 것은?

㉠ : 다른 데이터의 이동이나 변조를 가하는 것이 아니기에 사용자를 귀찮게 하는 문제 외에는 별다른 위험이 없다.
㉡ : 블루투스 장치끼리 인증 없이 정보를 간편하게 교환하기 위해 개발된 OPP(OBEX Push Profile) 기능을 사용하여 블루투스 장치로부터 주소록 등의 내용을 요청해 이를 열람하는 등의 공격 방법이다.
㉢ : 해커가 모바일 장치를 물리적으로 소유한 것처럼 다른 사람의 모바일 장치가 전화를 걸거나 다른 기능들을 수행하도록 할 수 있다.

① ㉠: 블루재킹(Bluejacking), ㉡: 블루스나핑(Bluesnarfing), ㉢: 블루버깅(Bluebugging)
② ㉠: 블루재킹(Bluejacking), ㉡: 블루버깅(Bluebugging), ㉢: 블루프린팅(Blueprinting)
③ ㉠: 블루재킹(Bluejacking), ㉡: 블루스나핑(Bluesnarfing), ㉢: 블루프린팅(Blueprinting)
④ ㉠: 블루버깅(Bluebugging), ㉡: 블루스나핑(Bluesnarfing), ㉢: 블루프린팅(Blueprinting)

정답 1번

간단한 해설

블루투스 공격은 **원치 않는 메시지 전송, 저장 정보 탈취, 기기 기능 제어**를 구분하면 대응시킬 수 있다. 각각 블루재킹, 블루스나핑, 블루버깅에 해당한다.

NoteBase

대응 관계 해설

세 설명은 블루투스를 이용해 상대방에게 무엇을 하는지를 기준으로 구분한다. 메시지를 보내 불편을 주는 것, 상대방의 데이터를 가져오는 것, 상대방 기기의 동작을 지시하는 것은 서로 다른 공격이다.

㉠: 블루재킹(Bluejacking)이다. 주변 기기에 사용자가 원하지 않는 메시지나 전자명함 등을 보내 귀찮게 하는 행위로, 그 자체가 **저장 데이터를 탈취하거나 기기를 장악하는 공격은 아니다**. 지문의 '별다른 위험이 없다'는 표현은 이 직접적인 작용을 구별한 것이며, 악성 메시지에 반응하도록 유도하는 사회공학적 위험까지 항상 없다는 뜻은 아니다.

㉡: 블루스나핑(Bluesnarfing)이다. 취약한 블루투스 장치의 정보 교환 기능을 악용하여 사용자 허락 없이 주소록 등 **저장된 정보를 열람하거나 가져오는 것**이 핵심이다. 지문에서 OPP 기능을 이용해 주소록 내용을 요청한다는 부분은 데이터 탈취라는 판단 근거이며, 모든 장치에서 정상적인 정보 교환이 곧 공격이라는 뜻은 아니다.

㉢: 블루버깅(Bluebugging)이다. 취약점을 이용해 장치의 명령이나 기능에 접근하여 **전화 걸기 등 기기 동작을 원격으로 제어**하는 공격이다. 주소록을 읽는 데 그치는 블루스나핑보다 기기의 기능을 조작한다는 단서가 중요하다.

블루프린팅(Blueprinting)은 블루투스 장치의 특징을 수집하여 기기 종류나 구현 특성을 식별하는 핑거프린팅이다. 이후 공격에 활용할 정보를 모으는 것이며, 지문의 전화 걸기와 같은 기능 제어 자체를 뜻하지 않는다.

따라서 ㉠은 블루재킹, ㉡은 블루스나핑, ㉢은 블루버깅으로 연결되며, 이 대응을 모두 충족하는 선택지는 ①이다.

NoteBase

문 23. 무선 랜 보안과 관련한 설명으로 옳지 않은 것은 모두 몇 개인가?

가. 무선 랜의 취약점을 보완하기 위해 IEEE 802.1x와 RADIUS(Remote Authentication Dial-In User Service) 서버를 이용해 무선 사용자를 인증한다.
나. WPA(Wifi Protected Access)는 WEP(Wired Equivalent Privacy) 암호의 약점을 보완한 CCMP(Counter mode with CBC-MAC Protocol) 암호화 방식을 사용한다.
다. WPA2는 보안 강화를 위해 RC4 대신 AES 알고리즘을 사용한다.
라. KRACK(Key Reinstallation Attacks)은 WPA2의 4-way 핸드셰이크(handshake) 과정에서 메시지를 조작하고 재전송하여 정보를 획득하는 공격이다.

① 0개
② 1개
③ 2개
④ 3개

정답 2번

간단한 해설

초기 WPA의 대표 보호 방식은 TKIP이고, **AES 기반 CCMP는 WPA2**의 대표 방식이다. 두 방식을 바꾸어 연결한 나가 틀렸으므로, 이 문항은 틀린 보기의 수를 세어야 한다.

NoteBase

보기별 해설

가. O. 기업용 무선 랜에서는 IEEE 802.1X의 포트 기반 접근제어와 인증 서버를 이용하여 접속 사용자를 인증한다. 무선 단말의 인증 메시지를 액세스 포인트가 중계하고, RADIUS 서버가 계정·인증정보 등을 확인하는 구성이 대표적이다. 이는 보안을 강화하는 인증 방식에 대한 설명이며, 사전 공유키를 사용하는 모든 개인용 무선 랜에 RADIUS 서버가 필수라는 뜻은 아니다.

나. X. WEP의 약점을 보완하기 위해 도입된 초기 WPA의 대표적인 데이터 보호 방식은 **TKIP**이다. TKIP는 RC4 기반 구조를 유지하면서 패킷별 키 처리와 무결성 검사를 보완했다. 보기에 제시한 **AES 기반 CCMP는 WPA2의 대표 방식**이므로 WPA와 WPA2의 기본 구분을 바꾸어 설명했다.

다. O. WPA2의 대표적인 보호 방식인 CCMP는 AES를 사용한다. WEP와 초기 WPA의 TKIP에서 사용하던 RC4 대신 AES 기반의 암호화와 무결성 보호를 적용하여 보안을 강화한다는 설명이다. 이 문항은 두 세대의 표준적인 보호 방식을 비교하므로 구형 장비와의 혼합 운용 설정과 구분해야 한다.

라. O. KRACK은 WPA2의 4-way 핸드셰이크에서 재전송되는 메시지의 처리를 악용하여 이미 사용 중인 키를 다시 설치하게 하는 공격이다. 이때 함께 초기화된 nonce나 재전송 방지 카운터가 재사용되어, 조건에 따라 통신 내용의 복호화나 재전송 공격 등이 가능해진다. AES 알고리즘 자체를 깨거나 무선 랜 비밀번호를 알아내는 공격이라는 뜻은 아니다.

따라서 옳지 않은 보기는 나 하나이므로 정답은 ②의 1개이다.

NoteBase

문 24. 네트워크 기반의 공격들과 이에 대한 보안 대책으로 가장 옳지 않은 것은 무엇인가?

① Land Attack - 패킷 필터링 도구를 이용하여 자신의 시스템 주소와 동일한 소스(Source) 주소를 가진 외부 패킷을 필터링 한다.

② ARP Spoofing - ARP 테이블을 ARP reply 메시지에 따라 동적(Dynamic)으로 관리하여 작성한다.

③ DNS Spoofing - 중요한 사이트에 대해서는 IP 주소를 확인해 hosts 파일에 등록해 둔다.

④ TCP Connection Hijacking - TCP 연결설정 과정에서 시작 순서번호(Initial Sequence Number)를 임의의 번호로 할당한다.

정답 2번

간단한 해설

ARP 응답을 검증하지 않고 테이블에 동적으로 반영하면 **위조된 IP·MAC 주소 대응으로 오염**될 수 있다. 정적 대응 정보를 사용하거나 ARP 응답의 유효성을 검사해야 한다.

선지별 해설

① O: Land 공격은 출발지와 목적지 IP 주소 및 포트를 피해 시스템 자신으로 위조한 패킷으로 비정상적인 처리를 유발한다. 따라서 외부에서 들어오면서 **출발지 주소가 내부의 자기 주소인 패킷**을 차단하면 이러한 위조 패킷을 걸러낼 수 있다.

② X: 검증되지 않은 ARP 응답에 따라 IP 주소와 MAC 주소의 대응을 동적으로 바꾸는 동작은 **ARP 캐시 오염의 원인**이 될 수 있다. 공격자가 거짓 응답으로 정상 호스트의 IP 주소에 자기 MAC 주소를 연결할 수 있기 때문이다. 중요한 대응 정보를 정적 ARP 항목으로 고정하거나, 스위치의 동적 ARP 검사(DAI)로 응답의 IP·MAC 연결을 검증하는 것이 대책이다.

③ O: 신뢰할 수 있는 방법으로 확인한 도메인과 IP 주소의 대응을 hosts 파일에 등록하면, **그 로컬 대응을 우선 사용하는 이름 해석**에서는 위조된 DNS 응답에 의존하지 않고 주소를 찾을 수 있다. 다만 파일의 무결성과 주소의 최신성을 유지해야 하며, hosts 파일을 사용하지 않는 이름 해석 방식까지 보호하는 것은 아니다.

④ O: 시작 순서번호를 예측하기 어렵게 정하면 공격자가 유효한 TCP 순서번호를 추측하여 데이터를 끼워 넣거나 연결을 가로채기 어려워진다. 이는 특히 **통신 내용을 보지 못하는 공격자의 순서번호 추측**을 어렵게 하는 대책이다. 이미 패킷을 관찰하는 공격까지 모두 막는 완전한 보호 수단은 아니다.

따라서 검증 없는 동적 ARP 갱신을 방어 대책으로 제시한 ②가 가장 옳지 않다.

NoteBase

문 25. 네트워크 스캐닝(Scanning)과 관련한 설명으로 가장 옳지 않은 것은 무엇인가?

① 대표적인 스캔 도구로 NMAP(Network Mapper)이 있다.

② 스텔스(Stealth) 스캔의 종류로 플래그(Flag) 값을 모두 설정하여 전송하는 Xmas 스캔과 플래그(Flag) 값을 모두 설정하지 않고 전송하는 NULL 스캔 등이 있다.

③ 스캔하고자 하는 포트를 대상으로 UDP 연결을 시도할 때, 아무런 응답이 없다면 해당 포트의 비활성화를 의미한다.

④ TCP Full Open 스캔은 신뢰성은 높지만, 속도가 느리고 로그가 남는다.

정답 3번

간단한 해설

UDP 스캔에서 **무응답만으로 포트가 닫혀 있다고 판단할 수 없다**. 열린 서비스가 탐색 패킷에 응답하지 않거나 방화벽이 패킷을 버린 경우에도 응답이 없을 수 있다.

선지별 해설

① O: Nmap은 대상 호스트의 포트와 서비스 상태를 조사하는 대표적인 네트워크 스캐닝 도구이다. TCP·UDP 등 여러 방식의 스캔을 지원한다.

② O: Xmas 스캔과 NULL 스캔은 정상적인 TCP 연결을 완성하지 않고 비정상적인 플래그 조합에 대한 반응을 살피는 스텔스 스캔에 속한다. '모두 설정'은 전체 플래그를 켠 크리스마스트리 패킷을 가리키는 용례이다. 다만 **Nmap의 Xmas 스캔은 FIN·PSH·URG만 설정**하므로 모든 구현에서 모든 TCP 플래그를 켠다는 뜻으로 일반화해서는 안 된다. NULL 스캔은 플래그를 모두 0으로 둔다. 스텔스라는 명칭이 탐지 장비에 전혀 기록되지 않는다는 뜻은 아니다.

③ X: UDP는 연결을 설정하지 않는 프로토콜이며, UDP 스캔은 탐색 데이터그램과 그 응답으로 포트 상태를 추정한다. 무응답은 열린 서비스가 불필요한 요청을 무시했거나 필터링 장비가 패킷을 버린 결과일 수 있으므로 **열림과 필터링을 구분할 수 없는 상태**이다. 일반적으로 닫힌 UDP 포트는 ICMP 'Port Unreachable' 응답을 보내므로, 무응답을 곧바로 포트 비활성화로 해석한 부분이 잘못되었다.

④ O: TCP Full Open 스캔은 3방향 핸드셰이크를 완료해 실제 연결 수립 여부를 확인하므로 연결 가능성 판단의 신뢰성이 높다. 연결을 완성하지 않는 방식보다 패킷 교환과 처리가 많아 상대적으로 느리고, **서비스에 연결 기록을 남기기 쉽다**.

NoteBase

문 26. 인터넷 프로토콜(IP)에 대한 설명으로 가장 옳지 않은 것은 무엇인가?

① 클래스 기반 주소 지정에서 처음 세 비트의 값이 '110'으로 시작하는 주소를 클래스 C주소라고 한다.

② IPv4의 데이터그램(Datagram)에서 첫 번째 필드는 선택사항(Option)을 포함한 헤더(header)의 길이 값이다.

③ IPv6에서는 헤더(header)가 40바이트로 고정되어 있어 헤더의 길이 필드가 불필요하다.

④ IPv6에서는 IPv4에서 사용하던 체크섬(Checksum) 필드가 삭제되었다.

정답 2번

간단한 해설

IPv4 데이터그램의 첫 번째 필드는 **버전(Version)**이고, 헤더 길이 IHL은 두 번째 필드이다. 따라서 첫 필드를 헤더 길이라고 한 **②가 옳지 않다**.

선지별 해설

① O. 클래스 기반 IPv4 주소 체계에서 클래스 C는 첫 세 비트가 110이다. 따라서 첫 번째 옥텟은 이진수 11000000부터 11011111까지, 즉 십진수 192~223의 범위에 해당한다.

② X. IPv4 헤더의 첫 번째 필드는 **4비트 버전(Version)**이며 값은 4이다. 선택사항을 포함한 헤더 길이를 나타내는 IHL(Internet Header Length)은 그 다음 4비트 필드이다. IHL은 32비트, 즉 4바이트 단위이므로 옵션이 없는 기본 헤더의 IHL 값 5는 20바이트를 뜻한다.

③ O. IPv6의 **기본 헤더는 40바이트로 고정**되어 있으므로 IPv4의 IHL과 같은 기본 헤더 길이 필드가 필요 없다. 필요한 부가 정보는 확장 헤더로 표현할 수 있으며, 확장 헤더까지 포함한 전체 길이가 항상 40바이트라는 뜻은 아니다.

④ O. IPv6 기본 헤더에는 IPv4의 헤더 체크섬 필드가 없다. 따라서 라우터가 홉 제한 값을 바꿀 때 IPv4처럼 IP 헤더 체크섬을 다시 계산하지 않는다. 이는 상위 계층에서 사용하는 TCP·UDP 등의 오류 검출 기능까지 없앴다는 뜻은 아니다.

첫 필드와 두 번째 필드를 혼동한 ②가 정답이다.

NoteBase

문 27. FTP(File Transfer Protocol)의 보안 대책에 대한 설명으로 옳은 것을 모두 고른 것은?

가. Bounce Attack을 예방하기 위해 20번 포트를 통한 명령은 제한한다.
나. TFTP가 필요한 경우, Secret Mode로 운영한다.
다. /etc/passwd 파일에서 Anonymous FTP에 불필요한 항목을 제거한다.
라. /etc/ftpusers에 등록된 사용자만이 FTP에 접근할 수 있으므로, root와 같은 중요 계정은 등록하지 않는다.

① 가, 다
② 나, 라
③ 나, 다
④ 다, 라

정답 1번

간단한 해설

ftpusers는 허용 목록이 아니라 **FTP 로그인을 금지할 계정 목록**이므로 root 같은 중요 계정을 등록해 차단한다. TFTP를 필요한 범위에서 제한적으로 운영하는 설정도 'Secret Mode'가 아니라 **Secure Mode**이다.

NoteBase

보기별 해설

FTP 보안에서는 데이터 연결을 다른 서비스 공격에 악용하지 못하게 하고, 익명 사용자에게 노출되는 정보와 접근 가능한 계정을 최소화한다. TFTP는 별도의 간단한 파일 전송 프로토콜이므로 그 운영 방식도 구분한다.

가. O: Bounce Attack은 FTP 서버의 데이터 연결을 중계 수단으로 악용하여 다른 호스트나 서비스에 데이터를 보내게 하는 공격이다. 선지의 '20번 포트를 통한 명령'은 **능동 FTP의 데이터 연결을 이용한 명령 데이터의 중계**를 제한한다는 취지이다. 서버가 임의의 제3자나 부적절한 목적지 포트로 데이터 연결을 만들지 못하게 제한하는 것이 방어의 핵심이다. 일반 FTP 제어 명령을 받는 포트는 21번이며, 20번을 제어 포트라고 이해해서는 안 된다.

나. X: TFTP가 꼭 필요한 경우에는 **Secure Mode** 등으로 접근 가능한 디렉터리와 파일을 제한하여 운영한다. 'Secret Mode'라는 명칭이 잘못이다. 이러한 제한은 파일 접근 범위를 줄이는 것으로, TFTP 자체에 사용자 인증이나 전송 암호화가 자동으로 추가된다는 뜻은 아니다.

다. O: 익명 FTP 이용자에게 불필요한 계정 정보가 드러나면 시스템 계정 등을 파악하는 데 악용될 수 있다. 따라서 **익명 FTP 환경에서 필요한 계정 정보만 남기고 불필요한 항목은 제거**한다. 특히 익명 FTP의 격리된 환경에 passwd 파일을 두는 구성에서는 시스템 전체 계정 정보를 그대로 노출하지 않도록 최소화한다. 운영체제의 필수 계정을 무조건 삭제하라는 의미는 아니다.

라. X: /etc/ftpusers는 일반적으로 **FTP 접속을 거부할 사용자 목록**이다. 따라서 root 같은 중요 계정은 이 파일에 등록하여 FTP 로그인을 제한해야 한다. 등록된 사용자만 허용한다는 설명과 중요 계정을 등록하지 않는다는 조치가 모두 반대이다.

옳은 보기는 가와 다이므로, 이를 묶은 선택지 ①과 일치한다.

NoteBase

문 28. 전자우편 보안에 사용되는 기술들에 대한 설명으로 가장 옳지 않은 것은 무엇인가?

① PGP(Pretty Good Privacy)는 전자우편 메시지의 인증과 기밀성 제공을 위해 개발된 전자우편 보안의 표준안이다.

② S/MIME이 제공하는 보안 서비스에는 기밀성, 무결성, 송신 사실 부인방지, 사용자 인증 등이 있다.

③ S/MIME은 X.509 버전3 규정을 준수하여 공개키 인증서를 사용한다.

④ PEM(Privacy Enhanced Mail)은 분산화된 키 인증 방식을 통해 관리가 용이하여 대중적으로 사용되고 있다.

정답 4번

간단한 해설

PEM은 인증기관을 연결한 **계층적 인증서 관리**를 사용한다. 사용자 간 공개키 인증을 바탕으로 한 분산적 신뢰망은 전통적인 PGP의 특징이다.

선지별 해설

① O: PGP는 전자우편과 파일을 보호하기 위해 **암호화와 전자서명**을 결합한 기술이다. 암호화로 기밀성을, 전자서명으로 발신자 인증과 무결성을 제공한다. PGP 계열의 메시지 형식은 OpenPGP로 표준화되어 사용된다.

② O: S/MIME은 MIME 전자우편에 보안 기능을 추가한다. **암호화는 기밀성**을 제공하고, **전자서명은 인증·무결성·송신 부인방지**를 지원한다. 서명 검증은 해당 개인키로 메시지가 서명되었다는 근거를 제공하므로, 인증서 검증과 개인키 보호도 중요하다.

③ O: S/MIME은 공개키를 신원과 연결하는 **X.509 v3 공개키 인증서**를 사용한다. 수신자는 인증서의 신뢰 경로와 유효성 등을 검증하여 서명 검증이나 암호화에 사용할 공개키를 신뢰할 수 있는지 판단한다.

④ X: PEM은 인증기관을 계층적으로 연결하는 **계층적 인증서 관리 구조**를 전제로 한다. 최상위 정책등록기관 아래에 정책인증기관과 인증기관을 두는 방식으로, 인증 기반을 구축·운영해야 한다. 사용자들이 서로의 공개키를 인증하는 분산적 신뢰 방식은 전통적인 PGP의 '신뢰망'과 관련된다. 이를 PEM의 간편한 관리와 대중적 사용의 근거로 설명한 연결은 잘못되었다.

따라서 PEM을 분산형 키 인증 방식으로 설명한 ④가 가장 옳지 않다.

NoteBase

문 29. 데이터베이스 보안 통제에 대한 설명 중 가장 옳지 않은 것은 무엇인가?

① 흐름통제 : 접근 가능한 객체 간의 정보 흐름을 통제하는 것으로, 낮은 보안 등급에서 높은 보안 등급으로 정보 흐름 발생 시 기밀성이 위반되지 않도록 통제하는 것이다.

② 추론통제 : 간접적인 데이터 노출로부터 데이터를 보호하는 것으로, 비밀 정보의 은폐, 데이터 위장 등의 방법으로 통제할 수 있다.

③ 접근통제 : 인증된 사용자에게 허가된 범위 내에서만 접근을 허용하여 내부의 정보에 대한 접근을 통제하는 것이다.

④ 뷰(View) : 기본 테이블로부터 유도되어 만들어지는 가상 테이블로, 데이터의 논리적 독립성을 제공한다.

정답 1번

간단한 해설

기밀성을 지키기 위한 흐름통제는 **높은 보안 등급의 정보가 낮은 등급으로 새어 나가는 것**을 막는 데 초점이 있다. 낮은 등급에서 높은 등급으로의 흐름을 기밀성 침해 방향으로 설명한 부분이 잘못되었다.

NoteBase

선지별 해설

① X. 흐름통제는 서로 다른 보안 등급의 주체·객체 사이에서 정보가 이동하는 방향을 통제한다. **기밀성**을 보호할 때 막아야 할 핵심 흐름은 **높은 보안 등급의 정보가 낮은 보안 등급으로 유출되는 것**이다. 낮은 등급에서 높은 등급으로 정보가 올라가는 것 자체를 기밀성 침해의 방향으로 설명한 부분이 반대이다. 높은 신뢰 수준의 자료가 낮은 신뢰 수준의 자료에 의해 훼손되는 문제는 무결성과 관련된 별도의 관점이다.

② O. 추론통제는 직접 공개하지 않은 비밀을 공개된 자료나 여러 질의 결과의 조합으로 알아내는 간접 노출을 막는 것이다. 민감한 값을 감추거나 일부 결과의 공개를 제한하는 은폐 방식, 값에 변화를 주어 원자료를 정확히 추정하기 어렵게 하는 위장 방식 등을 사용할 수 있다. 단순히 원자료에 대한 직접 읽기 권한을 차단하는 것만으로는 이런 추론을 충분히 막지 못할 수 있다.

③ O. 접근통제는 확인된 사용자에게 허용된 자원과 연산의 범위 안에서만 접근하도록 하는 것이다. 예를 들어 같은 테이블이라도 어떤 사용자는 조회만, 다른 사용자는 수정까지 허용할 수 있다. 사용자가 누구인지 확인하는 인증과 그 사용자에게 무엇을 허용할지 정하는 권한 통제를 구별하되 함께 적용한다.

④ O. 뷰는 기본 테이블에 대한 질의로 정의되는 가상 테이블이다. 사용자에게 필요한 열이나 행을 중심으로 논리적 표현을 제공하며, 기본 테이블의 구조가 바뀌어도 뷰의 인터페이스를 유지하도록 설계하면 응용프로그램에 미치는 영향을 줄일 수 있어 논리적 데이터 독립성에 도움이 된다. 또한 뷰와 권한 설정을 함께 사용하면 사용자가 볼 수 있는 데이터 범위를 제한할 수 있다.

따라서 기밀성 보호에서 제한해야 할 정보 흐름의 방향을 뒤집어 설명한 ①이 정답이다.

NoteBase

문 30. 다음 웹 서비스 공격 기법에 대한 설명으로 바르게 짝지어진 것은?

(가) 공격자가 게시판에 악성 스크립트를 저장하여 피해자가 해당 글을 읽을 경우 악성 스크립트가 실행되도록 하는 공격 기법
(나) 공격자가 입력 폼 및 URL 입력란에 SQL 문을 삽입하여 정보를 열람하거나 조작하는 공격 기법
(다) 공격자가 의도한 웹사이트 사용행위를 사용자 자신의 의도와는 무관하게 특정 웹사이트에 요청하게 만드는 공격 기법

① (가): XSS, (나): SQL Injection, (다): XXE
② (가): XSS, (나): SQL Injection, (다): CSRF
③ (가): XXE, (나): SQL Injection, (다): CSRF
④ (가): XXE, (나): CSRF, (다): XSS

정답 2번

간단한 해설

(가)는 저장한 악성 스크립트를 피해자 브라우저에서 실행하는 **XSS**, (나)는 질의를 변조하는 **SQL Injection**, (다)는 사용자 의사와 무관한 요청을 보내게 하는 **CSRF**이다. 이 대응이 일치하는 것은 ②이다.

NoteBase

대응 관계 해설

(가) XSS. 게시판에 저장된 악성 스크립트가 글을 열람한 피해자의 브라우저에서 실행되는 것은 **저장형 XSS**이다. 신뢰하는 웹페이지에 공격자의 스크립트가 섞여 실행된다는 점이 핵심이다. 악성 코드가 서버에 저장되어도 이 설명에서의 실행 위치는 피해자의 브라우저이다.

(나) SQL Injection. 입력값을 안전하게 처리하지 않아 공격자의 SQL 구문이 데이터베이스 질의의 일부로 해석되는 공격이다. 그 결과 원래 의도한 질의를 변형하여 정보를 조회하거나 데이터를 조작할 수 있다. 단순히 입력란에 SQL처럼 생긴 글자를 쓰는 것만으로 성립하는 것이 아니라, 그 입력이 질의의 구조나 의미에 영향을 주어야 한다.

(다) CSRF. 사용자의 의사와 무관하게 공격자가 원하는 요청을 대상 웹사이트로 보내게 만드는 **사이트 간 요청 위조**이다. 통상 로그인된 사용자의 브라우저가 세션 쿠키 등을 자동으로 첨부하는 성질을 악용하여, 서버가 요청을 사용자의 정상 행위로 받아들이게 한다. 핵심은 스크립트 자체의 실행이 아니라 사용자 권한을 이용한 원치 않는 요청이다.

XXE는 XML 파서의 외부 엔터티 처리 기능을 악용하는 공격으로, 게시판 스크립트 저장이나 사용자 의사와 무관한 요청을 설명한 (가)·(다)의 명칭이 아니다.

따라서 (가) XSS, (나) SQL Injection, (다) CSRF이며, 이 조합은 ②와 일치한다.

NoteBase

문 31. 블록체인(Block Chain)에 대한 설명으로 옳은 것은 모두 몇 개인가?

가. 비트코인에서 최초로 구현되었다.
나. 블록체인의 한 블록에는 앞의 블록에 대한 정보가 포함되어 있다.
다. 블록체인 기술에서는 작업 증명이나 지분 증명 등과 같은 합의 알고리즘을 사용한다.
라. 제네시스 블록(Genesis block)은 블록체인의 가장 첫 번째 블록을 말한다.

① 1개
② 2개
③ 3개
④ 4개

정답 4번

간단한 해설

블록체인은 **이전 블록의 해시를 통한 연결**과 참여자 간 합의로 기록을 유지한다. 첫 블록인 제네시스 블록에는 이전 블록이 없으며, 현대적 블록체인의 실용화는 비트코인에서 출발했다.

보기별 해설

가. O: 비트코인은 해시로 연결된 블록과 분산 합의를 결합한 **현대적 블록체인의 최초 실용 사례**이다. 2008년 설계가 공개되고 2009년 네트워크가 가동되었다. 다만 해시 연결과 전자문서 타임스탬프의 선행 연구까지 비트코인에서 처음 시작되었다는 뜻은 아니다.

나. O: 일반적인 후속 블록은 **이전 블록의 해시값**을 포함하여 앞 블록과 연결된다. 앞 블록의 내용이 바뀌면 그 해시와 이후 연결 관계가 달라지므로 변경을 탐지할 수 있다. 이전 블록이 없는 첫 제네시스 블록은 예외이다.

다. O: 분산된 참여자들이 원장의 상태와 추가할 블록에 동의하도록 **합의 알고리즘**을 사용한다. 작업 증명(PoW)은 계산 작업을, 지분 증명(PoS)은 참여자의 지분을 주요 기반으로 삼는다. 블록체인마다 선택하는 방식이 다르며 두 방식을 모두 사용해야 하는 것은 아니다.

라. O: 제네시스 블록은 **블록체인의 첫 블록**으로, 이후 블록들이 연결되는 출발점이다. 그 앞에는 연결할 블록이 없다.

따라서 가·나·다·라가 모두 해당하므로 옳은 설명은 4개이며 ④와 연결된다.

NoteBase

문 32. 디지털 포렌식의 기본 원칙 중 '무결성의 원칙'에 대한 설명으로 옳은 것은 무엇인가?

① 증거자료는 같은 환경에서 같은 결과가 나오도록 재현이 가능해야 한다.

② 컴퓨터 내부의 정보 획득은 신속하게 이루어져야 한다.

③ 증거가 획득되고 이송, 보관, 분석, 법정 제출 등의 과정이 명확해야 한다.

④ 획득된 정보는 위·변조되지 않았음을 입증할 수 있어야 한다.

정답 4번

간단한 해설

무결성의 원칙은 디지털 증거가 수집·보관·분석 과정에서 **위조되거나 변조되지 않았음을 입증**할 수 있어야 한다는 것이다. 같은 결과를 다시 얻는 재현성이나 취급 이력을 추적하는 연계보관성과 구별된다.

개념 구분

디지털 포렌식의 기본 원칙들은 증거를 믿을 수 있게 하는 서로 다른 조건이다. 이 문제의 구별 기준은 결과를 반복할 수 있는지, 정보가 사라지기 전에 확보했는지, 누가 어떻게 관리했는지, 내용이 변경되지 않았는지이다.

재현성: 같은 환경과 절차에서 같은 결과를 다시 얻을 수 있어야 한다는 원칙이다. 도구와 분석 절차를 기록하여 다른 분석자가 과정을 반복하고 결과를 확인할 수 있도록 하는 것으로, ①의 설명에 해당한다.

신속성: 시간이 지나거나 시스템 상태가 바뀌면서 정보가 소실·변경될 수 있으므로 필요한 정보를 적시에 확보해야 한다는 원칙이다. 특히 휘발성 정보의 보존과 관련되며, ②의 설명에 해당한다. 신속하다는 이유로 적법한 절차나 무결성 보존을 생략할 수 있다는 뜻은 아니다.

연계보관성: 증거의 획득부터 이송·보관·분석·제출까지 **취급자, 시각, 인계 관계와 수행 행위가 추적**되어야 한다는 원칙이다. ③은 증거 관리의 연속적인 이력을 명확히 하는 이 원칙을 설명한다.

무결성: 획득한 정보가 **위·변조되지 않고 보존되었음을 확인**할 수 있어야 한다는 원칙이다. 원본의 변경을 방지하고, 복제본으로 분석하며, 수집·복제 전후의 해시값과 처리 기록 등을 대조하는 방식으로 뒷받침한다. 해시값 비교는 데이터 변경 여부를 확인하는 수단이고, 증거를 누가 취급했는지는 별도의 관리 기록으로 남긴다.

따라서 '획득된 정보는 위·변조되지 않았음을 입증할 수 있어야 한다'는 ④가 무결성의 원칙에 해당한다.

NoteBase

문 33. 다음 중 ISO 27001:2013의 통제 항목에 해당하지 않는 것은 무엇인가?

① 정보보호 조직(Organization of information security)

② 운영 보안(Operations security)

③ 공급자 관계(Supplier relationship)

④ 모니터링과 검토(Monitoring and review)

정답 4번

간단한 해설

이 문제는 ISO 27001:2013 부속서 A의 **통제 영역 명칭**을 구별한다. 모니터링과 검토는 필요한 보안 관리 활동이지만, 그 자체가 독립된 통제 영역의 이름은 아니다.

선지별 해설

① O — 정보보호 조직은 부속서 A.6의 통제 영역이다. 조직 내부의 정보보호 역할과 책임을 정하고, 모바일 기기와 원격근무에서의 보안 등을 다룬다.

② O — 운영 보안은 부속서 A.12의 통제 영역이다. 운영 절차, 악성코드 방지, 백업, 로그 기록과 모니터링 등 정보처리 환경을 안전하게 운영하기 위한 내용을 포함한다.

③ O — 공급자 관계는 부속서 A.15의 통제 영역이다. 외부 공급자와의 관계에서 정보보호 요구사항을 정하고, 공급자가 제공하는 서비스를 관리하는 내용이다.

④ X — '모니터링과 검토'는 앞의 세 항목과 같은 수준의 독립된 통제 영역 명칭이 아니다. 다만 모니터링·검토 활동 자체가 표준에 없다는 뜻은 아니다. 예를 들어 공급자 관계 영역에는 '공급자 서비스의 모니터링과 검토'라는 하위 통제가 있다. 이 문제는 부속서 A의 영역 명칭을 구별하는 것이므로, 해당하지 않는 것은 ④이다.

NoteBase

문 34. 위험이 존재하는 프로세스나 사업을 수행하지 않고 포기하는 정보보호의 위험처리 전략으로 가장 옳은 것은 무엇인가?

① 위험 회피
② 위험 감소
③ 위험 전가
④ 위험 수용

정답 1번

간단한 해설

위험이 생기는 활동을 아예 수행하지 않거나 포기하는 것은 **위험 회피**이다. 따라서 정답은 ①이다.

개념 구분

위험 회피는 **위험을 발생시키는 활동 자체를 시작하지 않거나 중단하는 전략**이다. 문제의 '프로세스나 사업을 수행하지 않고 포기'한다는 단서는 위험 원인이 되는 활동에서 벗어나겠다는 뜻이다.

위험 감소는 사업을 계속하면서 보안 통제를 적용하여 사고의 발생 가능성이나 피해 규모를 낮추는 것이다. 접근 통제 강화나 취약점 보완처럼 활동을 유지한 채 위험을 줄이는 경우가 해당한다.

위험 전가는 보험이나 계약 등을 통해 위험에 따른 손실 부담의 일부를 다른 주체에게 이전하는 것이다. 위험이 발생할 가능성이나 조직의 모든 책임이 저절로 사라지는 것은 아니다.

위험 수용은 위험을 인식하고 평가한 뒤 그 수준을 감수하기로 결정하는 것이다. 아무 검토 없이 위험을 방치한다는 뜻이 아니라, 허용 가능한 범위에서 잔여 위험을 받아들이는 선택이다.

이 문제는 통제 강화, 부담 이전, 잔여 위험 감수가 아니라 활동 자체의 포기를 제시하므로 ① 위험 회피에 해당한다.

NoteBase

문 35. 다음에서 설명하는 사이버 위기 경보의 단계로 가장 옳은 것은 무엇인가?

- 침해 사고가 다수 기관에서 발생했거나 대규모 피해로 발전될 가능성 증가
- 복수 정보통신서비스제공자(ISP)망/기간망의 장애 또는 마비

① 관심
② 주의
③ 경계
④ 심각

정답 3번

간단한 해설

침해사고가 다수 기관에서 발생하거나 대규모 피해로 발전할 가능성이 커지고, 복수 ISP망이나 기간망에 장애·마비가 발생하는 상황은 **경계 단계**의 기준에 해당한다. 핵심은 단순한 위협 징후를 넘어 **피해가 여러 기관과 주요 통신망으로 확산되는 수준**이라는 점이다.

공통 해설

사이버 위기 경보는 침해사고의 발생·확산 가능성과 피해 범위에 따라 위협 수준을 구분한다. '경계'는 **다수 기관의 침해사고 또는 대규모 피해로의 발전 가능성 증가**, 복수 ISP망이나 기간망의 장애·마비 등으로 다수 기관의 공조 대응이 필요한 수준이다. ISP는 인터넷 접속 서비스를 제공하는 사업자이며, 기간망은 통신망의 중심을 이루는 망이다. 제시된 두 단서는 모두 이러한 경계 단계의 피해 범위와 확산 수준을 나타낸다.

같은 피해 범위 기준으로 보면, '관심'은 피해 발생 가능성이나 해외 공격의 국내 유입 우려에 초점을 두고, '주의'는 일부 기관·네트워크의 피해와 다수 기관으로의 확산 가능성을 다룬다. 반면 '심각'은 전국적인 침해사고나 국가적 차원의 네트워크·정보시스템 사용 불가능 등으로 국가적 공동 대처가 필요한 수준이다. 따라서 제시문의 복수 통신망 장애·마비를 곧바로 심각 단계로 판단하지 않고, **다수 기관·복수 통신망 수준과 전국적·국가적 수준**을 구별해야 한다.

NoteBase

문 36. 「개인정보보호법」에서 사용하는 용어의 뜻으로 가장 옳지 않은 것은 무엇인가?

① 개인정보 - 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.

② 정보주체 - 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.

③ 개인정보파일 - 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물을 말한다.

④ 개인정보처리자 - 개인정보취급자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 임직원, 파견근로자, 시간제근로자 등을 말한다.

정답 4번

①

개인정보에는 **살아 있는 개인을 직접 알아볼 수 있는 정보와 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보**가 포함된다. 결합의 용이성은 다른 정보의 입수 가능성과 식별에 드는 시간·비용·기술 등을 합리적으로 고려하여 판단한다.

개인정보 보호법 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다. <개정 2014.3.24, 2020.2.4, 2023.3.14>
1. "개인정보"란 살아 있는 개인에 관한 정보로서 다음 각 목의 어느 하나에 해당하는 정보를 말한다.
가. 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보
나. 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보. 이 경우 쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려하여야 한다.

②

정보주체는 **처리되는 정보로 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람**이다.

개인정보 보호법 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다. <개정 2014.3.24, 2020.2.4, 2023.3.14>
3. "정보주체"란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.

NoteBase

③

개인정보파일은 **쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물**이다.

개인정보 보호법 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다. <개정 2014.3.24, 2020.2.4, 2023.3.14>
4. "개인정보파일"이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.

④

개인정보처리자는 **업무를 목적으로 개인정보파일을 운용하기 위해 스스로 또는 다른 사람을 통해 개인정보를 처리하는 공공기관·법인·단체·개인 등**이다. 그 지휘·감독을 받아 개인정보를 처리하는 임직원·파견근로자·시간제근로자 등은 **개인정보취급자**이다. 선지는 두 용어와 지휘·감독 관계를 뒤바꾸었다.

개인정보 보호법 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다. <개정 2014.3.24, 2020.2.4, 2023.3.14>
5. "개인정보처리자"란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.

개인정보 보호법 제28조(개인정보취급자에 대한 감독)
① 개인정보처리자는 개인정보를 처리함에 있어서 개인정보가 안전하게 관리될 수 있도록 임직원, 파견근로자, 시간제근로자 등 개인정보처리자의 지휘 · 감독을 받아 개인정보를 처리하는 자(이하 "개인정보취급자"라 한다)의 범위를 최소한으로 제한하고, 개인정보취급자에 대하여 적절한 관리 · 감독을 하여야 한다. <개정 2023.3.14>

NoteBase

문 37. 「개인정보보호법」 제25조 제1항 '누구든지 다음 각 호의 경우를 제외하고는 공개된 장소에 영상정보처리기기를 설치·운영하여서는 아니 된다.'의 각 호에 해당하지 않는 것은 모두 몇 개인가?

가. 법령에서 구체적으로 허용하고 있는 경우
나. 범죄의 예방 및 수사를 위하여 필요한 경우
다. 시설안전 및 화재 예방을 위하여 필요한 경우
라. 교통단속을 위하여 필요한 경우
마. 교통정보의 수집·분석 및 제공을 위하여 필요한 경우

① 0개
② 1개
③ 2개
④ 3개

정답 1번

가

법령에서 구체적으로 허용하는 경우에는 공개된 장소에 고정형 영상정보처리기기를 설치·운영할 수 있다.

개인정보 보호법 제25조(고정형 영상정보처리기기의 설치 · 운영 제한)
① 누구든지 다음 각 호의 경우를 제외하고는 공개된 장소에 고정형 영상정보처리기기를 설치 · 운영하여서는 아니 된다. <개정 2023.3.14>
1. 법령에서 구체적으로 허용하고 있는 경우

나

범죄의 예방 및 수사를 위하여 필요한 경우는 공개된 장소에서 고정형 영상정보처리기기의 설치·운영이 허용되는 사유이다.

개인정보 보호법 제25조(고정형 영상정보처리기기의 설치 · 운영 제한)
① 누구든지 다음 각 호의 경우를 제외하고는 공개된 장소에 고정형 영상정보처리기기를 설치 · 운영하여서는 아니 된다. <개정 2023.3.14>
2. 범죄의 예방 및 수사를 위하여 필요한 경우

NoteBase

다

시설안전 및 화재 예방은 공개된 장소의 고정형 영상정보처리기기 설치·운영이 허용되는 목적에 포함된다. 해당 목적의 설치·운영은 **정당한 권한을 가진 자**가 해야 한다.

개인정보 보호법 제25조(고정형 영상정보처리기기의 설치 · 운영 제한)
① 누구든지 다음 각 호의 경우를 제외하고는 공개된 장소에 고정형 영상정보처리기기를 설치 · 운영하여서는 아니 된다. <개정 2023.3.14>
3. 시설의 안전 및 관리, 화재 예방을 위하여 정당한 권한을 가진 자가 설치 · 운영하는 경우

라

교통단속은 공개된 장소의 고정형 영상정보처리기기 설치·운영이 허용되는 목적에 포함된다. 해당 목적의 설치·운영은 **정당한 권한을 가진 자**가 해야 한다.

개인정보 보호법 제25조(고정형 영상정보처리기기의 설치 · 운영 제한)
① 누구든지 다음 각 호의 경우를 제외하고는 공개된 장소에 고정형 영상정보처리기기를 설치 · 운영하여서는 아니 된다. <개정 2023.3.14>
4. 교통단속을 위하여 정당한 권한을 가진 자가 설치 · 운영하는 경우

마

교통정보의 수집·분석 및 제공은 공개된 장소의 고정형 영상정보처리기기 설치·운영이 허용되는 목적에 포함된다. 해당 목적의 설치·운영은 **정당한 권한을 가진 자**가 해야 한다.

개인정보 보호법 제25조(고정형 영상정보처리기기의 설치 · 운영 제한)
① 누구든지 다음 각 호의 경우를 제외하고는 공개된 장소에 고정형 영상정보처리기기를 설치 · 운영하여서는 아니 된다. <개정 2023.3.14>
5. 교통정보의 수집 · 분석 및 제공을 위하여 정당한 권한을 가진 자가 설치 · 운영하는 경우

NoteBase

문 38. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 의한 형사 처벌 대상이 아닌 것은 무엇인가?

① 이용자의 동의를 받지 아니하고 개인정보를 수집하는 프로그램을 이용자의 컴퓨터나 그 밖에 대통령령으로 정하는 정보처리장치에 설치한 정보통신서비스 제공자

② 정보통신망에 의하여 처리·보관 또는 전송되는 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설한 자

③ 법정대리인의 동의를 받지 아니하거나 법정대리인이 동의하였는지를 확인하지 아니하고 만 14세 미만인 아동의 개인정보를 수집한 정보통신서비스 제공자

④ 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망에 침입한 자

정답 1, 3번

①

이용자의 동의 없이 개인정보 수집 프로그램을 설치한 행위는 **3천만원 이하의 과태료** 대상이다. 과태료는 형벌이 아니므로 이 설치행위 자체는 형사처벌 대상에 해당하지 않는다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제50조의5(영리목적의 광고성 프로그램 등의 설치)
정보통신서비스 제공자는 영리목적의 광고성 정보가 보이도록 하거나 개인정보를 수집하는 프로그램을 이용자의 컴퓨터나 그 밖에 대통령령으로 정하는 정보처리장치에 설치하려면 이용자의 동의를 받아야 한다. 이 경우 해당 프로그램의 용도와 삭제방법을 고지하여야 한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제76조(과태료)
② 다음 각 호의 어느 하나에 해당하는 자와 제7호부터 제11호까지의 경우에 해당하는 행위를 하도록 한 자에게는 3천만원 이하의 과태료를 부과한다. <개정 2011.3.29, 2012.2.17, 2013.3.23, 2014.5.28, 2015.6.22, 2015.12.1, 2016.3.22, 2017.7.26, 2018.9.18, 2020.2.4, 2021.6.8, 2023.1.3, 2024.1.23, 2024.2.13, 2025.10.1, 2026.3.31>
10. 제50조의5를 위반하여 이용자의 동의를 받지 아니하고 프로그램을 설치한 자

NoteBase

②

정보통신망으로 처리·보관·전송되는 타인의 정보를 훼손하거나 비밀을 침해·도용·누설하면 **5년 이하의 징역 또는 5천만원 이하의 벌금**에 처한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제49조(비밀 등의 보호) 누구든지 정보통신망에 의하여 처리 · 보관 또는 전송되는 타인의 정보를 훼손하거나 타인의 비밀을 침해 · 도용 또는 누설하여서는 아니 된다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제71조(벌칙)
①다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다. <개정 2016.3.22, 2018.12.24, 2024.1.23, 2026.3.31>
14. 제49조를 위반하여 타인의 정보를 훼손하거나 타인의 비밀을 침해 · 도용 또는 누설한 자

③

아동의 개인정보 보호는 개인정보 보호법이 규율한다. 동의가 필요한 개인정보 처리에서 **법정대리인의 동의를 받지 않은 경우**는 5년 이하의 징역 또는 5천만원 이하의 벌금 대상이지만, **동의 여부의 확인만 누락한 경우까지 형사처벌하는 것은 아니다**.

개인정보 보호법 제22조의2(아동의 개인정보 보호)
① 개인정보처리자는 만 14세 미만 아동의 개인정보를 처리하기 위하여 이 법에 따른 동의를 받아야 할 때에는 그 법정대리인의 동의를 받아야 하며, 법정대리인이 동의하였는지를 확인하여야 한다.

개인정보 보호법 제71조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다. <개정 2016.3.29, 2020.2.4, 2023.3.14>
3. 제22조의2제1항(제26조제8항에 따라 준용되는 경우를 포함한다)을 위반하여 법정대리인의 동의를 받지 아니하고 만 14세 미만인 아동의 개인정보를 처리한 자

NoteBase

④

접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망에 침입하면 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제48조(정보통신망 침해행위 등의 금지)
① 누구든지 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망에 침입하여서는 아니 된다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제71조(벌칙)
①다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다. <개정 2016.3.22, 2018.12.24, 2024.1.23, 2026.3.31>
11. 제48조제1항을 위반하여 정보통신망에 침입한 자

NoteBase

문 40. 「정보통신기반 보호법」에 관한 설명으로 가장 옳지 않은 것은 무엇인가?

① 전자적 침해행위라 함은 정보통신기반시설을 대상으로 해킹, 컴퓨터바이러스, 논리·메일폭탄, 서비스거부 또는 고출력 전자기파 등에 의하여 정보통신기반시설을 공격하는 행위를 말한다.

② 정보통신기반보호위원회의 위원은 위원장 1인을 포함한 25인 이내의 위원으로 구성한다.

③ 정보통신기반보호위원회는 주요정보통신기반시설 보호와 관련된 제도의 개선에 관한 사항 등을 심의한다.

④ 관리기관의 장은 대통령령이 정하는 바에 따라 정기적으로 소관 주요정보통신기반시설의 취약점을 분석·평가할 수 있다.

정답 4번

①

해킹, 컴퓨터바이러스, 논리·메일폭탄, 서비스거부 또는 고출력 전자기파 등으로 **정보통신기반시설을 공격하는 행위**는 전자적 침해행위에 해당한다.

정보통신기반 보호법 제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다. <개정 2007.12.21, 2020.6.9>
2. "전자적 침해행위"란 다음 각 목의 방법으로 정보통신기반시설을 공격하는 행위를 말한다.
가. 해킹, 컴퓨터바이러스, 논리 · 메일폭탄, 서비스거부 또는 고출력 전자기파 등의 방법

②

정보통신기반보호위원회는 **위원장 1인을 포함하여 25인 이내**의 위원으로 구성한다.

정보통신기반 보호법 제3조(정보통신기반보호위원회)
②위원회의 위원은 위원장 1인을 포함한 25인 이내의 위원으로 구성한다.

③

정보통신기반보호위원회의 심의 사항에는 **주요정보통신기반시설 보호와 관련된 제도의 개선**이 포함된다.

정보통신기반 보호법 제4조(위원회의 기능) 위원회는 다음 각호의 사항을 심의한다. <개정 2007.12.21, 2018.2.21, 2020.6.9>
4. 주요정보통신기반시설 보호와 관련된 제도의 개선에 관한 사항

NoteBase

④

관리기관의 장은 소관 주요정보통신기반시설의 취약점을 **정기적으로 분석·평가하여야 한다**. 선지는 법적 의무를 임의사항으로 표현하였다.

정보통신기반 보호법 제9조(취약점의 분석 · 평가)
①관리기관의 장은 대통령령으로 정하는 바에 따라 정기적으로 소관 주요정보통신기반시설의 취약점을 분석 · 평가하여야 한다. <개정 2020.6.9>

NoteBase