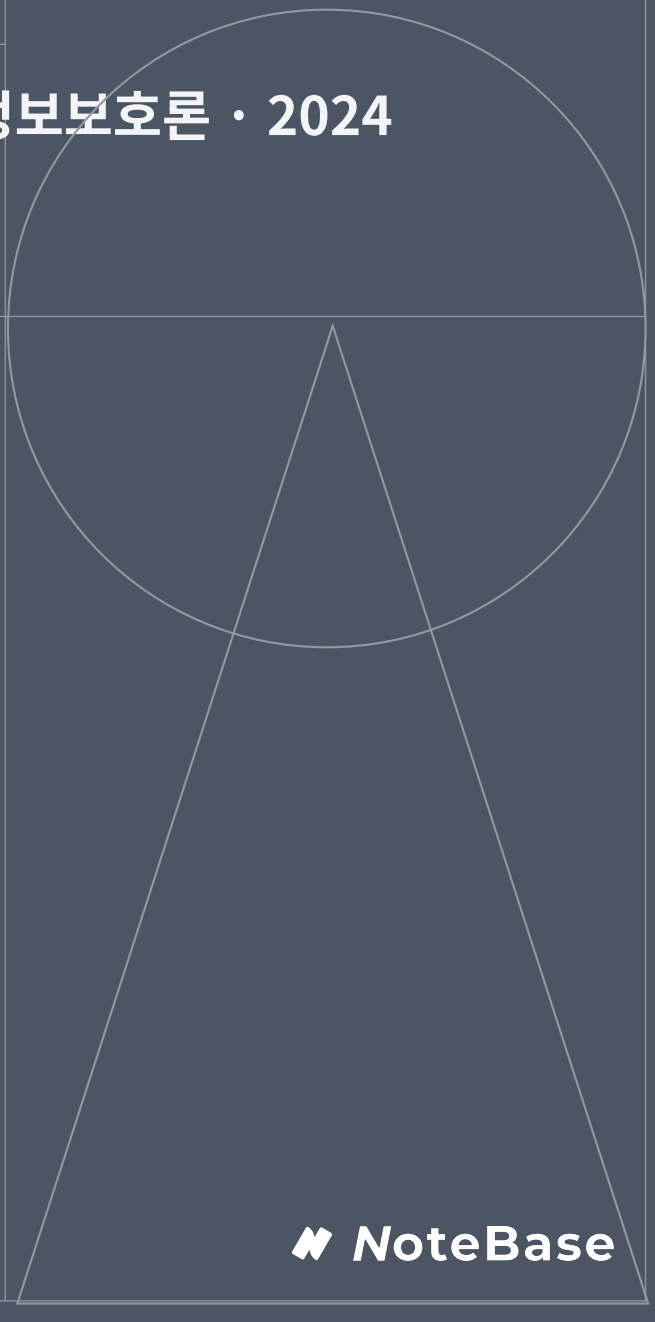
기출OX 해설집

공무원/경찰/공채(경위) · 정보보호론 · 2024



NoteBase

기출OX 해설집

공무원/경찰/공채(경위) · 정보보호론 · 2024

공무원/경찰/공채(경위) · 정보보호론 · 2024

문 1. 정보보안 용어에 대한 설명으로 가장 적절한 것은?

① 위협은 자산에 대한 위협원의 공격 행동이다.

② 취약점은 위협이 약점을 이용하여 해를 끼치는 순간이나 시점이다.

③ 위험은 자산이 가지고 있는 속성이거나 보안 대책의 미비점이다.

④ 노출은 자산에 악영향을 미치는 결과를 가져올 가능성이다.

정답 1번

간단한 해설

정답은 ①이다. 위협원의 공격 행동은 자산을 해칠 수 있는 위협의 한 형태이다. **취약점은 약점, 위험은 손실 가능성과 영향, 노출은 위협·위험의 영향을 받을 수 있는 상태**로 구별한다.

선지별 해설

① (O) 제시된 선지 중 가장 적절하다. 위협원은 피해를 일으킬 수 있는 원천이고, 그 원천의 공격 행동은 자산을 해칠 수 있는 **위협의 한 형태**이다. 다만 위협을 이미 실행된 공격 행동으로만 한정하면 좁은 설명이 된다. 일반적으로 위협은 자산에 악영향을 줄 수 있는 잠재적 사건·상황을 포함하며, 고의적 공격뿐 아니라 실수나 자연재해에서도 발생할 수 있다.

② (X) **취약점은 위협원이 악용하거나 촉발할 수 있는 약점**이다. 소프트웨어 결함, 부적절한 권한 설정, 보안 절차의 미비 등이 이에 해당한다. 약점이 실제로 이용되어 피해가 발생하는 순간이나 시점 자체를 취약점이라고 하지는 않는다.

③ (X) 자산이나 보안 대책에 존재하는 약점·미비점은 위험이 아니라 **취약점**에 해당한다. 위험은 위협이 취약점과 결합하여 손실을 초래할 가능성과 그 영향의 크기를 고려하는 개념이다. 예를 들어 취약한 접근통제가 약점이라면, 그 약점이 악용되어 정보가 유출될 가능성과 피해 정도가 위험 평가의 대상이다.

④ (X) 자산에 악영향을 미칠 결과가 발생할 가능성이라는 설명은 이 문항에서 **위험**에 대응한다. 노출은 자산이 위협이나 위험의 영향을 받을 수 있는 상태 또는 그 정도를 뜻한다. 즉 '피해를 입을 수 있는 상황에 놓여 있음'과 '손실 발생 가능성·영향을 평가함'을 구별해야 한다.

NoteBase

문 2. 보안 위협과 보안 위협이 영향을 주는 보안 목표와의 연결 관계로 가장 적절한 것은?

① 가로채기 - 가용성

② 가로막음 - 무결성

③ 변조 - 기밀성

④ 위조 - 인증

정답 4번

간단한 해설

위조는 가짜 메시지나 데이터를 정당한 주체가 만든 것처럼 받아들이게 하므로 **인증**을 위협한다. 메시지의 출처가 진짜인지 확인하는 목표와 연결된다.

선지별 해설

① X: 가로채기(interception)는 허가받지 않은 자가 정보를 엿보거나 복사하여 얻는 위협이다. 정보가 정당한 수신자에게 도착하더라도 제3자에게 노출될 수 있으므로 대표적으로 **기밀성**을 침해한다. 가용성은 정당한 사용자가 필요할 때 자원과 서비스를 사용할 수 있어야 한다는 목표이다.

② X: 가로막음(interruption)은 통신이나 서비스 이용을 중단시키거나 자원을 사용할 수 없게 만드는 위협이다. 따라서 대표적으로 **가용성**에 영향을 준다. 데이터가 무단으로 변경되지 않아야 한다는 무결성과는 구별된다.

③ X: 변조(modification)는 저장되거나 전송되는 데이터의 내용을 허가 없이 바꾸는 위협이다. 핵심 문제는 비밀을 읽는 것이 아니라 내용의 정확성과 완전성을 훼손하는 것이므로 **무결성**을 침해한다.

④ O: 위조(fabrication)는 실제로 생성되지 않은 메시지나 데이터를 만들어 정당한 주체가 보낸 것처럼 받아들이게 하는 위협이다. 따라서 주체나 메시지 출처가 진짜인지 확인하는 **인증** 목표와 직접 연결된다. 실제 공격은 여러 보안 목표를 함께 침해할 수 있지만, 제시된 대표 대응 중에서는 ④가 적절하다.

NoteBase

문 3. RSA에서 두 소수 p, q를 사용하여 $n = p * q$를 구성하고, 암호화키가 e일 때 복호화키 d는 법(modulus) $\varphi(n)$에서 e의 승산 역원이다. $p = 5, q = 11$이고 $e = 7$일 때 d의 값으로 가장 적절한 것은?

① 7

② 13

③ 23

④ 33

정답 3번

간단한 해설

$\varphi(55) = (5-1)(11-1) = 40$이므로 d는 **7d를 40으로 나눈 나머지가 1**이 되게 하는 수이다. $7 \times 23 = 161 = 4 \times 40 + 1$이므로 d = 23이다.

계산 과정

먼저 서로 다른 두 소수 p, q에 대해 오일러 피 함수는 $\varphi(n) = (p-1)(q-1)$이다. 따라서 $n = 5 \times 11 = 55$이고, $\varphi(55) = 4 \times 10 = 40$이다. **역원을 구하는 법은 n이 아니라 ϕ(n)**이라는 점에 주의한다.

복호화키 d는 ed≡1±od(n)을 만족해야 하므로 7d≡1±od40을 푼다. 7과 40의 최대공약수가 1이므로 승산 역원이 존재한다.

유클리드 호제법으로 $40 = 5 \times 7 + 5$, $7 = 1 \times 5 + 2$, $5 = 2 \times 2 + 1$을 얻는다. 이를 거꾸로 대입하면 $1 = 3 \times 40 - 17 \times 7$이다. 따라서 7의 역원은 법 40에서 −17과 같고, 양의 대표값은 −17 + 40 = 23이다.

검산하면 $7 \times 23 = 161 = 4 \times 40 + 1$로, 40으로 나눈 나머지가 1이다. 따라서 d = 23이며 ③에 해당한다.

NoteBase

문 4. Diffie-Hellman 키 분배 알고리즘에서 원시원소 $g = 2$이고 $p = 13$이며 $x = 125$일 때 가입자 A가 가입자 B에게 전송하는 메시지는 2^125 13이다. 이 값으로 가장 적절한 것은?

① 2

② 3

③ 6

④ 8

정답 3번

간단한 해설

13으로 나눈 나머지를 구할 때 2^12≡1±od13이므로 지수 125를 12로 나눈 나머지인 5로 줄일 수 있다. 따라서 $2^5 = 32$를 13으로 나눈 **나머지 6**이 전송하는 값이다.

계산 과정

Diffie-Hellman에서 A가 전송하는 값은 g^x p이다. 여기서 g는 거듭제곱의 밑인 원시원소, p는 나머지 연산의 기준인 소수, x는 A의 비밀 지수이다. 주어진 값은 g = 2, p = 13, x = 125이므로 2^{125}를 13으로 나눈 나머지를 구한다.

13은 소수이고 2는 13의 배수가 아니므로 페르마의 소정리에 따라 2^12≡1±od13이다. 이는 2^{12}를 13으로 나눈 나머지가 1이라는 뜻이다. 따라서 거듭제곱의 지수에서 **12의 배수 부분을 줄여도 나머지는 같다**.

$125 = 12 \times 10 + 5$이므로 $2^{125} = (2^{12})^{10} \cdot 2^5$로 나눌 수 있다. 앞의 인수 $(2^{12})^{10}$을 13으로 나눈 나머지는 1이므로, 구하려는 나머지는 2^5를 13으로 나눈 나머지와 같다.

$2^5 = 32$이고 $32 = 13 \times 2 + 6$이므로 나머지는 6이다. 따라서 A가 B에게 전송하는 값은 6으로, ③의 값과 일치한다.

NoteBase

문 5. 암호화 모드에 대한 설명으로 가장 적절한 것은?

① ECB 모드는 동일한 키에 의한 동일한 평문 블록은 항상 동일한 암호문이 출력된다.

② CBC 모드의 암호문 블록은 이전 암호문 블록과 독립적이다.

③ OFB 모드는 암호화할 때 피드백이 없다.

④ CTR 모드는 출력 암호문이 다음 평문 블록에 영향을 미친다.

정답 1번

간단한 해설

정답은 ①이다. ECB에서는 **같은 키로 같은 평문 블록을 암호화하면 같은 암호문**이 나온다. CBC는 이전 암호문을 연결하고, OFB는 암호 연산의 출력을 피드백하며, CTR은 카운터를 이용한다.

선지별 해설

① (O) ECB는 각 평문 블록을 같은 키로 독립적으로 암호화하므로 $C_i = E_K(P_i)$이다. 같은 키에서 평문 블록이 같으면 암호문 블록도 같다. 따라서 반복되는 평문 패턴이 암호문에 드러날 수 있다는 약점이 있다.

② (X) CBC는 현재 평문 블록과 이전 암호문 블록을 배타적 논리합(XOR)한 뒤 암호화한다. 즉 $C_i = E_K(P_i \oplus C_{i-1})$이고 첫 블록에서는 이전 암호문 대신 초기화 벡터(IV)를 사용한다. 따라서 현재 암호문 블록은 이전 암호문 블록과 독립적이지 않다.

③ (X) OFB는 블록 암호의 출력값을 다음 암호화 입력으로 되돌려 사용하므로 **출력 피드백이 존재한다.** 생성된 출력은 평문과 XOR하여 암호문을 만든다. 피드백되는 것은 최종 암호문이 아니라 키스트림을 생성하는 블록 암호의 출력이라는 점을 구별해야 한다.

④ (X) CTR은 블록마다 서로 다른 카운터 값을 암호화하여 키스트림을 만들고 평문과 XOR한다. 이전 암호문을 다음 블록 처리에 피드백하지 않으므로 출력 암호문이 다음 평문 블록의 암호화에 영향을 주지 않는다. 이 구조 덕분에 서로 다른 블록을 병렬로 처리할 수 있다.

NoteBase

문 6. 공개키 암호 방식을 이용하여 전자서명을 생성하고 검증할 때에는 공개키와 개인키가 사용된다. 송신자가 전자서명을 생성하고 수신자에게 전자서명을 전송하는 경우, 수신자가 전자서명을 검증할 때 사용하는 키로 가장 적절한 것은?

① 송신자의 개인키

② 송신자의 공개키

③ 수신자의 개인키

④ 수신자의 공개키

정답 2번

간단한 해설

서명은 송신자의 개인키로 생성하고, **송신자의 공개키**로 검증한다. 검증하는 사람이 수신자라고 해서 수신자의 키를 사용하는 것은 아니다.

핵심 풀이

전자서명에서는 서명자가 자신의 개인키로 서명을 생성하고, 검증자는 **그 개인키와 짝을 이루는 서명자의 공개키**로 서명을 검증한다. 이 문제의 서명자는 송신자이므로 키의 소유자를 송신자에 맞추어야 한다.

송신자의 개인키: 서명을 생성하는 데 사용하며 외부에 공개하지 않는다. 수신자가 검증을 위해 이 개인키를 전달받아야 하는 것은 아니다.

송신자의 공개키: 송신자의 개인키로 생성된 서명을 검증하는 키이다. 수신자는 메시지와 서명이 해당 공개키에 대해 유효한지 확인하며, 실제 사용에서는 그 공개키가 송신자에게 속한다는 점도 신뢰할 수 있게 확인해야 한다.

수신자의 키 쌍과의 구별: 수신자의 개인키·공개키는 수신자가 소유한 별개의 키 쌍이므로 송신자의 서명을 검증하는 키가 아니다. 기밀성 목적의 공개키 암호에서는 수신자의 공개키로 암호화하고 수신자의 개인키로 복호화한다는 관계와 혼동하지 않는다.

따라서 수신자가 송신자의 전자서명을 검증할 때 사용하는 키는 송신자의 공개키이며, ②에 해당한다.

NoteBase

문 7. SHA(Secure Hash Algorithm)에 대한 설명으로 가장 적절하지 않은 것은?

① SHA-1은 160비트의 해시값을 출력한다.

② SHA-224는 라운드 수가 80이다.

③ SHA-256의 블록 크기는 512비트이다.

④ SHA-384는 입력되는 데이터의 크기가 $2^{128} - 1$비트로 제한된다.

정답 2번

간단한 해설

SHA-224의 라운드 수는 **80이 아니라 64**이다. SHA-256과 같은 계열의 압축 구조를 사용하며, 최종 해시값의 길이는 224비트이다.

선지별 해설

① O: SHA-1의 메시지 다이제스트, 즉 최종 해시값은 **160비트**이다. 입력을 처리하는 블록 크기 512비트와 결과의 길이는 서로 다른 속성이므로 구별해야 한다.

② X: SHA-224는 SHA-256과 같은 계열의 압축 구조를 사용하며 한 블록을 처리할 때 **64라운드**를 수행한다. 초기값과 최종 출력 길이 등이 SHA-256과 다르며, 출력은 224비트이다. 80라운드는 SHA-1이나 SHA-384·SHA-512 계열에 해당하므로 ②가 가장 적절하지 않다.

③ O: SHA-256은 패딩을 마친 메시지를 **512비트 블록**으로 나누어 처리한다. 이름의 256은 블록 크기가 아니라 최종 해시값의 길이인 256비트를 뜻한다.

④ O: SHA-384의 원래 메시지 길이 L은 비트 단위로 0≤ L2^128이어야 한다. 따라서 정수 비트 길이의 최대값은 $2^{128} - 1$**비트**이다. 이는 입력 메시지 전체의 길이 제한이며, 처리 블록 크기 1,024비트나 출력 길이 384비트와 구별된다.

NoteBase

문 8. 다음 ElGamal 암호 방식에 대한 설명으로 옳은 것의 개수로 가장 적절한 것은?

가. ElGamal 기법은 공개키 암호 방식이다.
나. ElGamal 기법은 소인수 분해 어려움을 이용한다.
다. ElGamal 기법은 전자서명, 암호화, 키교환에 사용될 수 있다.
라. ElGamal 기법은 일반적으로 암호문의 길이가 평문의 길이보다 짧다.

① 1
② 2
③ 3
④ 4

정답 2번

간단한 해설

정답은 ②이다. 옳은 보기는 **가·다의 2개**이다. ElGamal은 이산로그 계열의 공개키 방식이며, 기본 암호문은 두 군 원소로 구성되어 평문보다 길어진다.

보기별 해설

가. (O) ElGamal은 **공개키와 개인키를 사용하는 비대칭 암호 방식**이다. 암호화에서는 수신자의 공개키로 암호문을 만들고 수신자가 자신의 개인키로 복호화한다. 송신자와 수신자가 같은 비밀키를 미리 공유하는 대칭키 암호와 구별된다.

나. (X) ElGamal은 소인수분해가 아니라 **이산로그 문제와 관련된 군 연산의 어려움**을 바탕으로 한다. 예를 들어 공개된 g와 g^x로부터 비밀 지수 x를 구하는 문제이다. 소인수분해 문제와 연결되는 대표적인 공개키 방식인 RSA와 혼동하면 안 된다.

다. (O) ElGamal 계열에는 **공개키 암호화 방식과 전자서명 방식**이 있다. 암호화를 이용하여 세션키를 안전하게 전달하는 등 키 분배에도 활용할 수 있으며, 암호화 구조는 Diffie–Hellman의 공유 비밀 생성 원리와 연결된다. 다만 암호화·서명·키교환이 완전히 동일한 알고리즘이라는 뜻은 아니다.

라. (X) 기본 ElGamal 암호는 평문 군 원소 하나를 **두 개의 군 원소로 된 암호문**으로 바꾼다. 공개키가 $y = g^x$일 때 임의의 지수 k를 사용하여 (g^k, my^k) 형태의 암호문을 생성한다. 따라서 일반적으로 평문보다 짧아지는 것이 아니라 길이가 증가한다.

옳은 보기는 가와 다의 **2개**이므로 ②를 고른다.

NoteBase

문 9. 타원 곡선 암호시스템(Elliptic Curve Cryptosystem)에 대한 설명으로 가장 적절한 것은?

① 타원 곡선 방정식은 $y^2 = x^3 + ax^2 + b$ 형태를 갖는다.

② 타원 곡선상의 두 점 P, Q의 덧셈은 P와 Q를 연결하는 직선과 교차하는 곡선상의 점이다.

③ 타원 곡선상의 모든 점은 덧셈 역원을 갖는다.

④ 타원 곡선상의 한 점 $P = (x_1, x_2)$에 상수 k를 곱한 $Q = kP$인 경우 Q의 점은 $Q = (kx_1, kx_2)$가 된다.

정답 3번

간단한 해설

타원곡선의 점들과 무한원점은 덧셈에 대해 군을 이루므로 **모든 점에 덧셈 역원이 존재**한다. 점의 덧셈과 상수배는 일반적인 좌표별 덧셈·곱셈이 아니라 곡선 위의 군 연산이다.

선지별 해설

타원곡선 암호는 유한체 위의 타원곡선 점에 정의된 군 연산을 사용한다. 항등원은 무한원점 O이며, 실수 곡선의 직선·접선 그림은 점 연산을 이해하기 위한 기하학적 설명이다.

① X: 특성이 2와 3이 아닌 체에서 흔히 쓰는 짧은 바이어슈트라스 표준형은 $y^2 = x^3 + ax + b$이며, 선지처럼 ax^2로 적은 식을 그 대표 표준형으로 설명하는 것은 적절하지 않다. 다만 더 일반적인 표현에는 제곱항이 들어갈 수 있으므로, 선지 모양의 식이 어떤 계수에서도 타원곡선이 될 수 없다는 뜻은 아니다. 유한체와 비특이성 조건도 필요하다.

② X: 서로 다른 두 점을 잇는 직선이 곡선과 만나는 세 번째 점을 R이라고 하면, 그 점 자체가 아니라 **R의 덧셈 역원**이 두 점의 합이다. 짧은 바이어슈트라스형의 실수 그림에서는 R을 x축에 대칭이동한 점이다. 두 점이 같을 때는 접선을 사용하며, 역원끼리 더하면 무한원점이 된다.

③ O: 곡선의 점들은 무한원점을 포함하여 덧셈에 대한 군을 이루므로 모든 점에 역원이 있다. 짧은 바이어슈트라스형에서 $P = (x, y)$의 역원은 $-P = (x, -y)$이고, $P + (-P) = O$이다. 유한체에서는 좌표의 음수도 그 체의 연산으로 해석하며, 무한원점은 자기 자신의 역원이다.

④ X: kP는 정수 k에 대한 **점 덧셈의 반복인 스칼라곱**이다. 양의 정수라면 P를 k번 더하는 군 연산이며, 일반적으로 각 좌표에 k를 곱한 점과 다르다. 0배는 무한원점이고 음의 정수배는 역원을 이용한다.

NoteBase

문 10. MDC(Modification Detection Code)와 MAC(Message Authentication Code) 기법에 대한 설명으로 가장 적절하지 않은 것은?

① MDC는 일반적으로 키와 메시지를 이어붙인 K|M에 해시함수를 적용하여 h(K|M)을 생성한다.

② 축소(nested) MAC 기법은 두 단계로 해싱이 이루어진다.

③ HMAC 기법은 일방향 해시 함수를 이용하여 메시지 인증 코드를 구성한다.

④ CMAC(Cipher-based MAC) 기법은 암호시스템의 CBC(Cipher Block Chaining) 모드와 유사한 방법이다.

정답 1번

간단한 해설

①이 가장 적절하지 않다. MDC는 일반적으로 **비밀키 없이 메시지의 해시값**을 생성한다. 비밀키를 사용하여 메시지의 무결성과 인증을 제공하는 MAC과 구별해야 한다.

선지별 해설

① (X) MDC는 비밀키를 사용하지 않는 해시값으로 메시지의 변경 여부를 확인하는 방식이다. 기본 형태는 $h(M)$이며, 키를 결합한 $h(K\|M)$을 일반적인 MDC의 생성 방식으로 설명한 것은 틀리다. 단순 해시만으로는 공격자가 메시지와 해시값을 함께 바꾸는 것을 막지 못하므로 인증을 위해서는 별도의 보호가 필요하다.

② (O) nested MAC은 안쪽 해시 처리 결과를 다시 바깥쪽 해시의 입력으로 사용하는 중첩 구조이다. 따라서 내부 해싱과 외부 해싱의 두 단계로 구성된다는 설명이 맞다. 두 단계라는 것은 해시 함수 내부의 압축 연산이 전체 메시지에서 정확히 두 번만 실행된다는 뜻은 아니다.

③ (O) HMAC은 암호학적 해시 함수와 공유 비밀키를 결합하여 메시지 인증 코드를 만든다. 내부·외부 패딩을 이용한 중첩 해싱으로 구성하며, 단순히 키와 메시지를 한 번 이어 붙여 해시하는 것과는 구조가 다르다.

④ (O) CMAC은 대칭키 블록 암호를 이용하는 MAC으로 CBC-MAC 계열의 연결 구조를 사용한다. 마지막 블록에는 메시지 길이와 패딩 여부에 따라 서브키를 적용하는 등의 처리가 추가된다. CBC와 유사한 구조라는 설명은 맞지만, CMAC의 목적은 메시지 인증이며 평문을 숨기는 암호화 모드 그 자체는 아니다.

NoteBase

문 11. X.509 인증서에 들어있는 필드에 대한 설명으로 가장 적절한 것은?

① 서명 알고리즘 ID 필드는 인증서를 서명한 알고리즘을 식별하기 위해 사용된다.

② 발행자(issuer) 이름 필드는 공개키의 소유자인 개체를 나타낸다.

③ 주체(subject) 개인키 필드는 발행자의 개인키를 나타낸다.

④ 서명(signature) 필드는 두 부분으로 이루어진다.

정답 1번

간단한 해설

서명 알고리즘 ID는 **인증서 서명에 사용한 알고리즘**을 식별한다. 발행자 정보와 공개키 소유자 정보, 서명값과 공개키 정보는 서로 다른 필드이다.

선지별 해설

① O: 서명 알고리즘 ID는 **인증서 발행자가 인증서에 서명할 때 사용한 알고리즘**을 나타낸다. 인증서를 확인하는 측은 이 정보를 이용해 어떤 알고리즘으로 서명을 검증해야 하는지 알 수 있다.

② X: 발행자(issuer) 이름은 인증서를 발급하고 서명한 인증기관 등 **발행 주체**를 나타낸다. 인증서에 담긴 공개키와 연결되는 개체는 주체(subject)로 구별한다.

③ X: X.509 인증서에는 주체의 개인키가 아니라 **주체의 공개키 정보**가 들어간다. 개인키는 소유자가 비밀로 관리해야 하며, 발행자의 개인키 역시 인증서에 넣어 배포하지 않는다. 발행자의 개인키는 인증서 서명을 생성하는 데 사용된다.

④ X: 실제 서명값 필드는 인증서의 서명 대상 내용을 대상으로 생성한 전자서명을 담는다. 이를 모든 인증서에서 두 부분으로 구성된다고 일반화할 수는 없다. 표준 구조에서 두 요소인 알고리즘 식별자와 공개키 비트열로 구성되는 것은 **주체 공개키 정보**이다. 인증서 전체는 서명 대상 내용, 서명 알고리즘, 서명값으로 구분되므로 서명값 자체와 혼동하지 않아야 한다.

NoteBase

문 13. 다음 설명에 해당하는 기술로 가장 적절한 것은?

암호문 상태에서도 연산이 가능한 차세대 암호기술이다. 데이터를 기존 암호알고리즘을 통해 비식별화하는 경우 클라우드에서 암호화된 데이터에 대한 연산이 불가능하지만, 이 암호기술을 활용하면 민감정보를 안전하게 보호하면서도 유용하게 데이터를 활용할 수 있다.

① 동형암호(Homomorphic Encryption)
② 양자내성암호(Post-Quantum Cryptography)
③ 배낭암호(Knapsack Cryptography)
④ TPM(Trusted Platform Module)

정답 1번

간단한 해설

정답은 ①이다. **동형암호는 복호화하지 않은 암호문에 연산**을 수행하고, 복호화했을 때 대응하는 평문 연산 결과를 얻을 수 있게 하는 기술이다.

대응 관계 해설

‘암호문 상태에서도 연산이 가능하다’는 단서는 **동형암호(Homomorphic Encryption)**에 대응한다. 암호문에 정해진 연산을 수행한 뒤 결과를 복호화하면, 원래 평문에 대응하는 연산을 수행한 결과를 얻을 수 있다.

‘클라우드에서 민감정보를 보호하면서 데이터를 활용한다’는 설명도 동형암호의 활용 목적에 맞는다. 연산을 수행하는 서버가 원문을 복호화하지 않고 계산할 수 있으므로, 데이터의 내용을 서버에 직접 공개하는 부담을 줄일 수 있다. 다만 모든 동형암호가 임의의 연산을 제한 없이 지원하는 것은 아니며, 지원 연산과 횟수는 방식에 따라 다르다.

② 양자내성암호는 **양자컴퓨터를 이용한 공격에도 견디도록 설계하는 암호**를 뜻한다. 핵심 분류 기준이 양자 공격에 대한 안전성이므로, 암호문 상태의 연산 기능을 설명한 지문에 대응하는 명칭은 아니다.

③ 배낭암호는 부분합·배낭 문제와 관련된 수학적 구조를 이용하는 암호 계열이다.

④ TPM은 키 보호, 암호 연산 및 시스템 무결성 측정 등을 지원하는 **신뢰 기반 보안 모듈**이다. 어느 쪽도 지문의 기능을 가리키는 일반적인 명칭은 아니다.

따라서 지문의 설명과 연결되는 기술은 ① **동형암호**이다.

NoteBase

문 14. 지적 재산권 보호에 사용되는 스테가노그래피(steganography), 워터마킹(watermarking), 핑거프린팅(fingerprinting)에 대한 설명으로 가장 적절한 것은?

① 스테가노그래피는 핑거프린팅보다 저작권 증명이 우수하다.

② 워터마크는 핑거프린팅보다 상대적으로 불법 예방 효과가 좋다.

③ 스테가노그래피의 은닉정보는 주로 판매자 정보이다.

④ 핑거프린팅의 특징에는 비가시성, 견고성, 복잡성 등이 있다.

정답 4번

간단한 해설

핑거프린팅은 배포본마다 수신자를 구별할 정보를 넣어 불법 유출 경로를 추적한다. 표식이 잘 드러나지 않는 **비가시성**, 변형에도 남는 견고성, 삽입·검출에 드는 계산복잡도 등이 주요 고려 특성이다.

선지별 해설

① X: 스테가노그래피는 메시지를 다른 매체 안에 숨겨 **통신이나 정보의 존재 자체를 드러내지 않는 것**에 주된 목적이 있다. 저작권자나 수신자를 식별하는 증거를 남기도록 설계되는 워터마킹·핑거프린팅보다 저작권 증명이 우수하다고 일반화할 수 없다. 여기서 핑거프린팅은 배포본마다 수신자 식별 표식을 삽입하는 기술을 뜻한다.

② X: 일반적인 저작권 워터마킹은 권리자 정보를 표시하여 소유권 확인에 활용하지만, 핑거프린팅은 **구매자·배포 대상마다 다른 식별정보**를 넣어 불법 복제물이 어느 배포본에서 나왔는지 추적할 수 있게 한다. 이러한 추적 가능성은 불법 재배포를 억제하는 수단이 되므로, 워터마킹의 불법 예방 효과가 상대적으로 더 좋다고 단정한 설명은 적절하지 않다.

③ X: 스테가노그래피에 숨기는 내용은 전달하려는 비밀 메시지 등으로, 판매자 정보로 한정되지 않는다. **저작권자나 판매자의 식별정보**를 콘텐츠에 넣는 것은 통상 저작권 보호용 워터마킹과 연결하고, 구매자별 식별정보는 핑거프린팅과 연결하여 구별한다.

④ O: 핑거프린팅에서는 표식 때문에 콘텐츠 품질이 눈에 띄게 나빠지지 않아야 한다는 **비가시성**, 압축·편집 등의 변형 뒤에도 표식을 식별할 수 있어야 한다는 견고성, 표식 삽입·검출·추적에 드는 계산량인 복잡성 등을 고려한다. 복잡성은 무조건 높아야 좋다는 뜻이 아니라, 실제 배포와 검출에서 감당할 수 있는 처리 비용이어야 한다는 성능 특성이다.

NoteBase

문 15. 접근제어(Access Control) 시스템의 일반적인 구분과 특성으로 가장 적절하지 않은 것은?

① 파일 리스트 접근제어(File List Access Control)-접근리스트 기반

② 임의적 접근제어(Discretionary Access Control)-신분 기반

③ 비임의적 접근제어(Non-Discretionary Access Control)-역할 기반

④ 강제적 접근제어(Mandatory Access Control)-규칙 기반

정답 1번

간단한 해설

접근제어 목록(ACL)은 객체에 대해 누가 어떤 권한을 갖는지 기록하는 **권한 표현·구현 방식**이다. 이를 파일 리스트 접근제어라는 독립적인 일반 정책 유형으로 분류한 것은 적절하지 않다.

선지별 해설

접근제어 정책은 접근을 허용하는 판단 기준과 권한을 결정하는 주체에 따라 구분한다. DAC·MAC·역할 기반 통제 같은 정책과, 권한을 목록으로 저장하는 구현 수단은 구별해야 한다.

① X: 파일 리스트 접근제어는 DAC·MAC 등과 나란히 놓는 일반적인 정책 분류가 아니다. **접근제어 목록(ACL)**은 파일 등의 객체별로 사용자나 그룹과 허용 권한을 기록하는 방식이며, 예를 들어 DAC를 구현하는 데 활용할 수 있다. 목록이 존재한다는 사실만으로 별도의 정책 유형이 정해지는 것은 아니다.

② O: 임의적 접근제어는 사용자나 그룹의 신분을 바탕으로 접근권한을 판단하며, 객체 소유자 등에게 권한 부여의 재량이 있다. 소유자가 다른 사용자에게 읽기·쓰기 권한을 부여하는 방식이 대표적이다.

③ O: 비임의적 접근제어는 개별 소유자의 재량이 아니라 조직 차원의 정책에 따라 권한을 정하는 접근이다. 역할 기반 접근제어는 직무·역할에 권한을 부여하고 사용자를 역할에 배정하는 대표적 형태이다. 비임의적 접근제어 전체가 역할 기반만을 뜻한다는 의미로 한정하지 않는다.

④ O: 강제적 접근제어는 시스템이 정한 보안 정책과 규칙을 강제하며, 개별 소유자가 임의로 바꾸지 못한다. 주체의 보안등급과 객체의 보안표지 등을 규칙에 따라 비교하는 방식이 대표적이다. 규칙을 사용한다는 이유만으로 모든 접근제어가 MAC이 되는 것은 아니다.

NoteBase

문 16. Bell-LaPadula 모델에 대한 설명으로 가장 적절한 것은?

① 높은 등급의 정보가 낮은 레벨로 유출되는 것을 통제하는 모델이다.

② 정보는 Top Secret, Secret, Unclassified로 분류하고 정보의 무결성 보장에 초점을 두고 있다.

③ No Write-Down 정책은 주체는 자신보다 낮은 등급의 객체에 정보를 쓸(write) 수 있다.

④ No Read-Up 정책은 주체는 자신보다 높은 등급의 객체를 읽고 쓸(read/write) 수 없다.

정답 1번

간단한 해설

정답은 ①이다. Bell-LaPadula는 높은 등급의 정보가 낮은 등급으로 흐르지 않도록 하여 **기밀성**을 보호한다. 기본 규칙은 '위로 읽기 금지'와 '아래로 쓰기 금지'이다.

선지별 해설

① (O) Bell-LaPadula 모델은 보안 등급에 따른 정보 흐름을 통제하여 높은 등급의 비밀이 낮은 등급으로 유출되는 것을 막는 데 초점을 둔다. 핵심 보호 목표는 **기밀성**이다.

② (X) 보안 등급을 구분하여 접근을 통제한다는 부분은 모델의 취지에 부합하지만, 초점은 무결성이 아니라 기밀성이다. 무결성 보호와 관련하여 대표적으로 구별하는 모델은 Biba 모델이다. 등급 명칭이나 개수 자체가 Bell-LaPadula의 본질은 아니다.

③ (X) No Write-Down은 주체가 자신보다 낮은 보안 등급의 객체에 정보를 쓰지 못하도록 하는 규칙이다. 높은 등급의 정보를 읽을 수 있는 주체가 낮은 등급의 객체에 그 내용을 기록하면 비밀이 유출될 수 있기 때문이다. 선지는 '쓸 수 있다'고 하여 규칙을 반대로 설명하였다.

④ (X) No Read-Up은 주체가 자신보다 높은 보안 등급의 객체를 **읽지 못한다**는 규칙이다. 높은 등급의 객체에 쓰는 행위까지 이 규칙이 금지하는 것은 아니다. 기본 Bell-LaPadula 정보 흐름 규칙에서는 위로 쓰기가 금지 대상이 아니며, 실제 쓰기 허용 여부는 다른 접근 권한도 함께 충족해야 한다.

NoteBase

문 17. 스트림 암호 방식과 블록 암호 방식에 대한 설명으로 가장 적절한 것은?

① 스트림 암호는 실시간 처리에 부적합하다.

② RC4는 바이트 단위 스트림 암호이다.

③ ARIA는 키 크기와 라운드 수가 AES와 동일한 규격이다.

④ 블록 암호 방식에는 RC5, 3DES, AES, SEED, HIGHT, LSH 등이 있다.

정답 2번

간단한 해설

정답은 ②이다. **RC4는 바이트 단위 스트림 암호**이다. ARIA와 AES는 키 크기는 같지만 라운드 수가 다르고, LSH는 블록 암호가 아니라 해시 함수이다.

선지별 해설

① (X) 스트림 암호는 비트 또는 바이트 등 작은 단위의 데이터를 키스트림과 결합하여 순차적으로 처리하므로 **실시간 처리에 활용하기 적합**하다. 큰 블록이 모두 채워질 때까지 기다려야만 암호화를 시작하는 방식으로 이해하면 안 된다.

② (O) RC4는 **바이트 단위 키스트림을 생성하는 스트림 암호**이다. 생성한 키스트림 바이트와 평문 바이트를 XOR하여 암호문을 만들고, 같은 키스트림으로 다시 XOR하여 복호화한다. 이 설명은 알고리즘의 분류와 동작 원리를 나타낸다.

③ (X) ARIA와 AES는 모두 128비트 블록 및 128·192·256비트 키를 사용하지만 **라운드 수는 다르다.** 키 길이 128·192·256비트에 대하여 ARIA는 각각 12·14·16라운드이고, AES는 각각 10·12·14라운드이다. 키 크기가 같다는 사실을 라운드 수까지 같다는 뜻으로 확대하면 안 된다.

④ (X) RC5, 3DES, AES, SEED, HIGHT는 블록 암호에 해당하지만 **LSH는 암호학적 해시 함수**이다. 해시 함수는 메시지로부터 요약값을 계산하는 기능이며, 비밀키로 평문을 암호화하고 복호화하는 블록 암호와 역할이 다르다.

NoteBase

문 18. 다음 지문에 대한 설명으로 가장 적절한 것은?

JavaScript와 HTML5의 Blob, download, anchor, click 등의 특성을 이용하여 인터넷 사용자가 특정 HTML 페이지 방문 시 자동으로 파일을 다운받도록 하는 기법이다.

① HTML Smuggling
② HTML Injection
③ Dangling Markup Injection
④ JavaScript Injection

정답 1번

간단한 해설

Blob과 HTML5 다운로드 기능을 결합하여 **사용자 브라우저에서 파일을 구성하고 내려받게 하는 것**이 HTML Smuggling의 특징이다. 단순히 페이지에 HTML이나 스크립트를 삽입하는 기법과 구별된다.

대응 관계 해설

지문과 명칭의 대응: JavaScript와 HTML5 기능을 이용하여 브라우저 안에서 파일 데이터를 구성하고 내려받도록 하는 특징은 **HTML Smuggling**에 해당한다. 완성된 파일을 그대로 전송하는 방식과 달리, HTML에 담긴 데이터가 사용자 측에서 파일로 만들어질 수 있다는 점이 핵심이다.

단서의 역할: Blob은 브라우저에서 파일 데이터처럼 취급할 수 있는 데이터 객체이다. anchor는 링크 요소이고 download는 다운로드를 지시하는 속성이며, click은 링크 동작을 유발하는 기능이다. 지문은 이 기능들의 결합을 통해 **브라우저 측 파일 생성·다운로드**가 이루어지는 모습을 설명한다. 다운로드되었다는 사실과 파일이 실행되었다는 사실은 구별해야 한다.

다른 명칭과의 구별: HTML Injection은 의도하지 않은 HTML을 삽입해 페이지 내용이나 구조에 영향을 주는 것이고, JavaScript Injection은 스크립트가 삽입·실행되게 하는 것이다. Dangling Markup Injection은 완결되지 않은 마크업이 뒤따르는 페이지 내용을 끌어들이도록 하는 주입 방식이다. 지문의 결정적 단서는 단순한 코드 삽입이 아니라 HTML·JavaScript 기능을 이용한 파일 전달 방식이다.

따라서 지문에 대응하는 명칭은 HTML Smuggling이며 ①에 해당한다.

NoteBase

문 19. 스마트폰에 메시지가 뜨면, 근처의 다른 블루투스를 인식한 스마트폰에 같은 메시지를 퍼트릴 수 있는 보안 위협으로 가장 적절한 것은?

① 블루프린팅(Blueprinting)
② 블루재킹(Blue-jacking)
③ 블루스나프(BlueSnarf)
④ 블루버그버그(Blue-bugbug)

정답 2번

간단한 해설

근처의 블루투스 기기에 원치 않는 메시지를 보내는 것은 **블루재킹**이다. 메시지 전달이 핵심이며, 그 자체를 악성코드의 자동 자기복제로 보는 것은 아니다.

개념 구분

블루투스 보안 위협은 메시지를 보내는지, 정보를 훔치는지, 기기를 제어하는지 구분하면 된다. 이 사례의 결정적 단서는 근처의 블루투스 기기에 같은 메시지를 전달한다는 점이다.

블루프린팅(Blueprinting)은 블루투스 주소와 서비스 정보 등 기기가 드러내는 특징을 조합하여 제조사·모델 등을 식별하는 기법이다. 주변 기기의 정보를 알아내는 것으로, 메시지 전송을 뜻하지 않는다.

블루재킹(Blue-jacking)은 블루투스를 이용하여 상대가 요청하지 않은 메시지나 연락처 정보를 보내는 행위이다. 사례의 메시지 전달과 연결된다. 다만 메시지가 표시되었다는 사실만으로 기기가 감염되어 자동으로 다른 기기에 복제된다고 단정할 수는 없다.

블루스나프(BlueSnarf)는 취약한 블루투스 연결을 악용하여 연락처·일정 등 기기 내부 정보를 무단으로 가져오는 공격을 가리킨다. 메시지를 보내는 것과 정보 유출은 구별해야 한다.

④의 '블루버그버그(Blue-bugbug)'는 원문 표기이다. 통상 알려진 블루버깅(Bluebugging)은 취약한 기기의 기능을 무단으로 제어하는 공격으로, 단순히 원치 않는 메시지를 전달하는 블루재킹과 다르다.

따라서 메시지 전송이라는 사례의 핵심에 해당하는 선택지는 ② 블루재킹이다.

NoteBase

문 20. 웹셸(Web shell) 공격의 설명으로 가장 적절하지 않은 것은?

① 예방책으로 시큐어 코딩과 취약점 패치, 키워드와 명령어 필터링이 있다.

② 웹셸공격은 서버로부터 명령을 클라이언트에서 실행시켜주는 프로그램을 말한다.

③ 웹셸공격은 제어권 탈취, 정보탈취, 변조의 악성행위를 한다.

④ 웹셸공격 프로그램은 ASP, PHP, JSP 언어를 사용한다.

정답 2번

간단한 해설

②가 가장 적절하지 않다. 웹셸은 클라이언트가 아니라 **침해된 웹 서버에서 실행**되며 외부 요청에 따라 서버 측 명령이나 기능을 수행하게 한다. 실행 위치와 명령 전달 방향을 구별해야 한다.

선지별 해설

① (O) 안전한 코딩과 취약점 패치는 웹셸이 업로드되거나 실행될 수 있는 취약점을 줄이는 예방책이다. 입력값과 위험 명령에 대한 검증도 보조적으로 활용할 수 있다. 다만 특정 키워드를 차단하는 것만으로 충분하지 않으므로 업로드 파일의 검증, 실행 권한 제한, 최소 권한 설정 등을 함께 적용해야 한다.

② (X) 웹셸은 일반적으로 침해된 **웹 서버에서 실행**되면서 외부의 요청을 받아 서버 측 기능이나 명령을 수행하게 하는 프로그램이다. 공격자가 클라이언트에서 요청하고 그 실행 결과를 받는 것이므로, 서버의 명령을 클라이언트에서 실행한다는 설명은 방향과 실행 위치를 반대로 서술한 것이다.

③ (O) 웹셸이 가진 권한과 서버의 상태에 따라 서버 제어, 파일·정보의 열람과 유출, 파일 변조 등의 악성행위에 이용될 수 있다. 웹셸이 있다는 사실만으로 언제나 관리자 최고 권한까지 자동으로 얻는 것은 아니지만, 서버 보안에 중대한 위협이 된다.

④ (O) ASP·PHP·JSP 등 서버 측에서 처리되는 기술로 웹셸을 만들 수 있다. 파일이 서버에서 실행될 수 있는 환경이어야 그 기능이 작동하므로 단순히 특정 확장자의 파일이 있다는 것만으로 웹셸 여부가 결정되는 것은 아니다. 제시된 언어·기술이 웹셸 구현에 사용될 수 있다는 설명은 맞다.

NoteBase

문 21. 웹 방화벽(Web firewall) 설명으로 가장 적절하지 않은 것은?

① Cross-site scripting, SQL injection 공격을 탐지하고, 차단한다.

② 웹 서버를 통과하는 PPTP 메시지는 공개키로 복호화한다.

③ 애플리케이션 계층의 분석과 정규화 기술을 사용한다.

④ URL에 따른 접근제어 기능과 SSL 트래픽을 복호화하여 검사한다.

정답 2번

간단한 해설

웹 방화벽은 HTTP·HTTPS 요청을 검사하는 보안 장비이다. **PPTP 메시지를 공개키로 복호화한다**는 것은 검사 대상과 암호화 처리 방식을 모두 잘못 연결한 설명이다.

선지별 해설

① O: 웹 방화벽은 HTTP 요청의 경로·헤더·매개변수·본문 등을 분석하여 **XSS와 SQL 삽입 같은 웹 애플리케이션 공격**을 탐지하고 설정된 정책에 따라 차단한다. 다만 모든 공격을 완벽하게 막는다는 뜻은 아니며 탐지 규칙과 운영 설정에 따라 효과가 달라진다.

② X: 웹 방화벽의 주된 검사 대상은 HTTP·HTTPS 웹 트래픽이며, PPTP는 VPN 터널링에 사용하는 별개의 프로토콜이다. 또한 PPTP에서 사용하는 MPPE의 데이터 암호화는 대칭키 방식이므로 **공개키로 PPTP 메시지를 복호화한다**는 설명은 맞지 않는다. HTTPS 본문 역시 공개키만으로 해독하는 것이 아니라 적절히 설정된 TLS 종단에서 세션키를 이용해 처리한다.

③ O: 웹 방화벽은 네트워크 주소와 포트만 검사하는 데 그치지 않고 **애플리케이션 계층의 요청 내용**을 해석한다. URL 인코딩 등 여러 표현을 정규화한 뒤 규칙과 비교하면 같은 공격 내용이 다른 표현으로 전달되는 경우도 일관된 기준으로 분석하는 데 도움이 된다.

④ O: URL 경로 등의 조건에 따라 요청을 허용하거나 차단할 수 있다. 또한 TLS 종료 등 적절한 구성에서는 암호화된 웹 트래픽을 복호화한 뒤 내용을 검사하고 필요하면 다시 암호화해 서버로 전달한다. 이는 **암호화 트래픽을 검사할 수 있도록 구성한 경우**의 기능이며, 아무 키나 종단 설정 없이 모든 SSL/TLS 내용을 읽는다는 뜻은 아니다.

NoteBase

문 22. 블록체인(Block Chain) 거래의 설명 중 가장 적절한 것은?

① 이중지불(Double spending)은 사용자가 자산에 대한 거래를 확정 후에 거래를 취소하거나 자산을 재사용하는 것이다.

② 합의 가로채기(Consensus hijacking)는 사용자 자산의 거래 대금 중, 합의된 수수료를 가로채는 것을 말한다.

③ Dapp(Decentralized application)은 블록체인의 중앙시스템에서 실행되므로, Dapp이 처리하는 정보의 공유를 쉽게 하여 거래를 활성화한다.

④ 거래 수수료(Transaction fee)는 거래를 블록에 추가하는 작업에 대한 수수료를 의미한다.

정답 4번

간단한 해설

정답은 ④이다. **거래 수수료는 거래 처리와 블록 포함에 대한 대가**이다. 이중지불은 동일 자산의 중복 지출, 합의 가로채기는 합의 과정에 대한 지배·조작으로 구별한다.

선지별 해설

① (X) 이중지불의 핵심은 **동일한 디지털 자산을 둘 이상의 거래에서 중복하여 지출하거나 지출하려는 것**이다. 거래가 먼저 확정되어야만 발생하는 것은 아니며, 단순히 거래를 취소하는 행위 자체를 모두 이중지불이라고 할 수도 없다. 다만 체인 재구성 등으로 기존 지급을 되돌리고 같은 자산을 다시 쓰는 공격은 이중지불의 한 형태가 될 수 있다. 따라서 선지처럼 '확정 후 취소 또는 재사용'으로 정의하는 것은 정확하지 않다.

② (X) 합의 가로채기는 **블록체인의 합의 과정에 대한 지배력을 확보하여 거래 승인이나 기록을 조작하는 공격**을 가리킨다. 예를 들어 작업증명 체계에서 과도한 연산력을 확보한 공격자는 거래 배제나 체인 재구성을 시도할 수 있다. 합의된 수수료를 단순히 가로채는 행위를 뜻하지 않는다.

③ (X) Dapp은 **분산형 애플리케이션**이다. 블록체인 기반 Dapp의 핵심 로직은 분산 네트워크의 스마트 계약 등을 통해 실행되며, 블록체인의 중앙시스템에서 실행된다는 설명은 적절하지 않다. 다만 사용자 화면이나 일부 부가 서비스까지 모두 완전히 분산되어야 한다는 뜻은 아니다.

④ (O) 거래 수수료는 일반적으로 **거래를 처리하고 블록에 포함시키는 데 드는 대가**이다. 블록을 생성·검증하는 참여자에게 보상을 제공하고 한정된 블록 공간의 사용을 조절하는 역할을 한다. 구체적인 수수료 배분이나 소각 방식은 블록체인 설계에 따라 달라질 수 있다.

NoteBase

문 23. 블록체인(Block Chain) 기술 설명 중 가장 적절하지 않은 것은?

① 앵커링(Anchoring)은 합의된 거래 및 블록의 무결성 보장을 강화하기 위한 타 블록체인을 활용하는 기술이다.

② 작업 증명(Proof of work)은 블록을 생성하는 경량 노드(Light node)가 거래량과 권한을 부여하는 작업 증명 방식이다.

③ 비잔틴 장애 허용(Byzantine Fault Tolerance)은 일부 노드가 결함이 있어도, 이를 허용할 수 있는 합의 방식이다.

④ 메인 체인(Main chain)은 합의 알고리즘에 따라 선정된 블록체인으로 가장 긴 블록체인을 말한다.

정답 2번

간단한 해설

작업 증명은 **난이도 조건을 만족하는 계산 작업의 수행**을 입증하는 방식이다. 경량 노드가 거래량이나 권한을 부여한다는 설명과는 다르다.

선지별 해설

① O: 앵커링은 한 블록체인의 거래나 블록을 대표하는 해시 등 검증 정보를 **다른 블록체인에 기록**하여 외부의 검증 기준점으로 삼는 기술이다. 나중에 원래 기록이 바뀌었는지 비교할 수 있어 무결성 검증을 강화한다. 원래 거래 내용의 진실성까지 자동으로 보장하는 것은 아니다.

② X: 작업 증명은 채굴 노드가 정해진 난이도 조건을 만족하는 해시를 찾는 등 **계산 작업을 수행했음을 증명**하는 방식이다. 다른 노드는 그 증명과 블록의 유효성을 확인한다. 경량 노드가 거래량이나 권한을 부여하는 방식이 아니며, 경량 노드는 일반적으로 전체 블록 데이터를 직접 검증하는 부담을 줄인 참여 방식이다.

③ O: 비잔틴 장애는 노드가 고장 나거나 서로 모순된 정보를 보내는 등 임의로 잘못 행동하는 상황을 포함한다. 비잔틴 장애 허용 합의는 정해진 장애 허용 한도와 통신 조건 안에서 **일부 노드가 잘못 행동해도 정상 노드들이 합의**할 수 있게 한다. 모든 노드의 오류를 무제한 허용한다는 뜻은 아니다.

④ O: 메인 체인은 분기된 후보들 가운데 합의 규칙에 따라 정식 기록으로 선택된 체인이다. 작업 증명 체인의 전통적인 설명에서는 이를 '가장 긴 체인'이라고 부른다. 다만 비트코인의 정확한 기준은 **유효한 체인 중 누적 작업량이 가장 큰 체인**이므로, 블록 개수만 많으면 언제나 선택된다는 뜻은 아니다. 다른 합의 방식에도 단순 길이 기준을 그대로 적용하지 않는다.

NoteBase

문 24. 전자지불시스템의 정보보호 요구사항으로 가장 적절하지 않은 것은?

① 거래하는 전자화폐는 위조불가능(unforgeability) 해야 한다.

② 송신자와 수신자가 전자지불시스템의 합법적인 사용자임이 인증되어야 한다.

③ 개인들의 신상관련 정보들이 통신망 상에서는 익명성(anonymity)으로 보호되어야 한다.

④ 암호화폐와 가상화폐는 개인별로 법정통화와 교환이 보장되어야 한다.

정답 4번

간단한 해설

④가 가장 적절하지 않다. 법정통화와의 교환 보장은 모든 전자지불시스템에 공통으로 요구되는 정보보호 조건이 아니다. **위조 방지·사용자 인증·개인정보 보호**가 보안 요구사항에 해당한다.

선지별 해설

① (O) 전자화폐를 권한 없는 자가 임의로 만들어 내거나 유효한 지급 수단인 것처럼 위조할 수 없어야 한다. 위조불가능성은 거래 가치와 지급 수단의 신뢰성을 지키기 위한 기본적인 보안 요구사항이다. 유효한 전자화폐를 반복 사용하는 이중 지불의 방지와도 구별하여 관리해야 한다.

② (O) 지급을 요청하거나 수령하는 주체가 시스템을 이용할 정당한 권한을 가진 사용자임을 확인해야 한다. 인증이 부실하면 다른 사용자를 사칭한 지급 요청이나 계정의 부정 사용이 가능해지므로 사용자 인증은 중요한 보안 요구사항이다.

③ (O) 전자지불 과정에서 개인의 신상정보가 통신망에 불필요하게 드러나지 않도록 개인정보와 거래 프라이버시를 보호해야 한다. 문항은 이를 익명성 요구로 표현하고 있다. 사용 자격을 확인하는 인증과 통신 과정에서 실명을 불필요하게 노출하지 않는 보호는 함께 설계할 수 있으며, 인증 절차 자체를 없앤다는 뜻은 아니다.

④ (X) 암호화폐나 가상화폐를 개인별로 법정통화와 교환할 수 있도록 보장하는 것은 **모든 전자지불시스템에 공통되는 정보보호 요구사항이 아니다.** 교환 가능성이나 상환 보장은 해당 지급 수단의 제도·계약·운영 방식에 관한 조건이다. 사용자 인증, 위조 방지, 개인정보 보호와 같은 보안 요구와 구별해야 한다.

NoteBase

문 25. 버퍼 오버플로우(buffer overflow) 공격의 대응책으로 가장 적절하지 않은 것은?

① 스택에서 실행(execute) 권한을 제거하여, 프로그램을 실행할 수 없도록 한다.

② 컴파일러가 프로그램 함수 호출 시 RET 앞에 Canary 값을 주입하고, 종료 시, Canary 값이 변조되었는지 확인한다.

③ 함수 호출 시 RET를 Global RET 스택에 저장하고, 종료 시 RET 값이 변조되었는지 확인한다.

④ 스택과 라이브러리의 데이터 영역 주소를 암호화하고, strcat() 함수 사용 시 복호화하여 변조되었는지 확인한다.

정답 4번

간단한 해설

ASLR은 스택과 라이브러리 등의 **배치 주소를 무작위화**하는 방어이다. 주소를 암호화한 뒤 strcat()에서 복호화해 변조를 검사한다는 설명은 해당 원리와 다르다.

선지별 해설

① O: 스택을 데이터 저장 영역으로 두고 실행 권한을 제거하면, 버퍼 오버플로우로 스택에 주입된 코드를 실행하려는 시도를 막을 수 있다. 이는 DEP 또는 실행 불가 메모리 보호의 원리이다. 여기서 실행할 수 없게 하는 대상은 **스택에 놓인 코드**이며, 정상적인 코드 영역에서 프로그램이 실행되는 것까지 금지한다는 뜻은 아니다.

② O: 컴파일러는 함수의 스택 프레임에 카나리라는 감시값을 두고 함수가 반환되기 전에 그 값이 보존되었는지 검사하는 코드를 삽입할 수 있다. 전형적으로 버퍼에서 **저장된 반환주소 쪽으로 덮어쓰기가 진행**되면 카나리도 변하므로 이를 탐지하고 비정상 종료 등으로 대응한다. 선지의 RET는 이러한 반환주소를 가리키는 맥락이다.

③ O: 반환주소를 일반 스택과 별도의 보호된 저장 영역에 복사해 두면 함수 반환 시 원래 값과 비교하여 변조를 탐지하거나 안전한 복사본으로 복원할 수 있다. **반환주소의 별도 보관과 검증**을 이용하는 Stack Shield·섀도 스택 계열 방어의 원리이며, 카나리처럼 인접 감시값만 확인하는 방식과 구별된다.

④ X: 스택이나 라이브러리의 배치 주소를 예측하기 어렵게 만드는 대표 방어는 **주소 공간 배치 난수화(ASLR)**이다. 주소를 암호화했다가 strcat()을 호출할 때 복호화하여 변조를 확인하는 방식이 아니다. strcat()은 목적지 버퍼의 남은 용량을 자동으로 검사하지 않으므로, 문자열 길이와 버퍼 크기를 확인하거나 적절한 길이 제한 수단을 사용하는 등 별도의 경계 검사가 필요하다.

NoteBase

문 26. OWASP TOP 10 LIST, 2021의 A01, A02, A03 내용으로 가장 적절하지 않은 것은?

① Security Misconfiguration

② Injection

③ Cryptographic Failures

④ Broken Access Control

정답 1번

간단한 해설

정답은 ①이다. 2021년 기준 A01은 Broken Access Control, A02는 Cryptographic Failures, A03은 Injection이다. **Security Misconfiguration은 A05**이므로 지정 범위에 해당하지 않는다.

선지별 해설

① (X) Security Misconfiguration은 보안 설정 오류로, 2021년 목록의 **A05**에 해당한다. 불필요한 기능 활성화, 부적절한 기본 설정, 과도한 오류정보 노출 등 설정 관리 문제를 다룬다. OWASP Top 10 항목이기는 하지만 문제에서 지정한 A01·A02·A03에는 포함되지 않는다.

② (O) Injection은 2021년 목록의 **A03**이다. 신뢰할 수 없는 입력이 명령어나 질의문의 일부로 해석되어 의도하지 않은 실행을 일으키는 문제를 다룬다. SQL 삽입 등이 대표적이며, 2021년 분류에서는 XSS도 이 범주에 포함되었다.

③ (O) Cryptographic Failures는 2021년 목록의 **A02**이다. 민감한 데이터를 보호하기 위한 암호화가 누락되거나 약한 암호·부적절한 키 관리 등으로 보호에 실패하는 문제를 다룬다.

④ (O) Broken Access Control은 2021년 목록의 **A01**이다. 사용자가 허용된 권한을 넘어 다른 사람의 데이터나 관리자 기능 등에 접근하는 문제를 다룬다. 따라서 문제의 세 항목 중 하나에 해당한다.

NoteBase

문 27. 실시간 위험탐지 및 대응을 위해 이벤트 로그(event log) 데이터를 실시간으로 수집하고 분석하는 기능을 가지고 있으며, 공격 로그의 포렌식(Forensic) 분석을 위한 데이터 검색 및 리포트 기능을 제공하는 것으로 가장 적절한 것은?

① SIEM(Security Information Event Management)

② PGP(Pretty Good Privacy)

③ PPTP(Point-to-Point Tunneling Protocol)

④ L2F(Layer 2 Forwarding)

정답 1번

간단한 해설

SIEM은 여러 시스템의 보안 로그를 통합하여 위협을 탐지하고, 저장된 로그의 검색·보고를 통해 사고 분석도 지원한다. 실시간 탐지와 사후 분석을 함께 제공한다는 점이 핵심이다.

핵심 풀이

SIEM은 여러 보안 장비·서버·응용프로그램의 로그와 이벤트를 모아 분석하는 보안 정보 및 이벤트 관리 체계이다. 단일 장비의 경보만 보는 것이 아니라 여러 출처의 사건을 연관 지어 위협을 찾아낸다.

SIEM의 수집·분석 기능은 문제의 실시간 이벤트 로그 수집과 위험 탐지에 대응한다. 축적된 로그를 검색하고 시간순 사건을 재구성하거나 보고서를 만드는 기능은 사고 이후 포렌식 분석을 지원한다. 따라서 실시간 탐지와 사후 분석을 함께 지원한다는 단서가 중요하다.

PGP는 공개키 방식과 대칭키 방식을 결합하여 전자우편·파일 등의 기밀성을 보호하고 전자서명으로 무결성 및 발신자 확인을 지원한다. 여러 장비의 이벤트 로그를 통합 분석하는 체계는 아니다.

PPTP는 PPP 트래픽을 IP 망에서 터널링하기 위한 프로토콜이고, L2F는 계층 2 프레임을 터널로 전달하는 기술이다. 두 기술의 중심은 원격 접속 트래픽 전달이며 보안 로그의 상관 분석·검색·보고가 아니다.

따라서 로그의 실시간 수집·분석과 사고 분석용 검색·보고를 함께 제공하는 것은 ① SIEM이다.

NoteBase

문 28. '소프트웨어 개발 보안'의 적용 사례로 가장 적절하지 않은 것은?

① CLASP(Comprehensive, Lightweight Application Security Process)

② CMVP(Cryptographic Module Validation Program)

③ Seven Touchpoints

④ MSDL(Microsoft Secure Development Lifecycle)

정답 2번

간단한 해설

정답은 ② **CMVP**이다. CMVP는 암호모듈 검증 프로그램이며, CLASP·Seven Touchpoints·Microsoft SDL처럼 **개발 생명주기에 보안 활동을 통합하는 프로세스**와는 성격이 다르다.

선지별 해설

① (O) CLASP는 기존 소프트웨어 개발 과정에 보안 활동을 통합하도록 제시한 프로세스이다. 역할별 보안 책임과 개발 단계별 활동을 정하여 요구사항·설계·구현 등에서 취약점을 예방하려는 소프트웨어 개발 보안의 사례이다.

② (X) CMVP는 **암호모듈의 보안 요구사항 충족 여부를 검증하는 프로그램**이다. 안전한 암호모듈을 선택하는 데 중요하지만, 소프트웨어 개발 생명주기 전반에 보안 활동을 통합하는 개발 방법론이나 프로세스 자체는 아니다. 나머지 세 항목과 목적 및 적용 범위가 다르다.

③ (O) Seven Touchpoints는 코드 검토, 아키텍처 위험 분석, 보안 요구사항과 보안 테스트 등 주요 보안 활동을 소프트웨어 개발 과정의 접점에 배치하는 접근이다. 완성 후 취약점을 찾는 데만 의존하지 않고 개발 전반에서 위험을 줄이려는 개발 보안의 사례이다.

④ (O) Microsoft의 SDL은 보안 요구사항, 위협 모델링, 안전한 구현과 검증 등의 활동을 개발 생명주기에 통합하는 보안 개발 프로세스이다. 따라서 문항에서 제시한 MSDL은 소프트웨어 개발 보안을 적용하는 사례에 해당한다.

NoteBase

문 29. GDPR(General Data Protection Regulation)에 대한 설명으로 가장 적절하지 않은 것은?

① EU 내 사업장을 운영하며 개인정보를 처리하는 기업에 적용

② EU 거주자의 행동을 모니터링하는 기업에 적용

③ 전자상거래를 통해 해외에서 EU 주민의 개인정보를 처리하는 기업에 적용

④ 최대 과징금은 중요한 위반사항인 경우, 전 세계 매출액의 5% 혹은 3천만 유로 중 높은 금액

정답 4번

①

EU 내 사업장의 활동과 관련하여 개인정보를 처리하는 기업에는 GDPR이 적용된다. 실제 개인정보 처리 장소가 EU 밖이어도 같다.

②

EU 밖의 기업도 **EU 내 정보주체의 EU 내 행동을 모니터링하는 것과 관련하여 개인정보를 처리**하면 GDPR의 적용을 받는다.

③

EU 밖의 기업도 **EU 내 정보주체에게 전자상거래로 상품·서비스를 제공하는 것과 관련하여 개인정보를 처리**하면 GDPR의 적용을 받는다.

④

중대한 위반에 대한 기업의 과징금 상한은 **직전 회계연도 전 세계 연간 매출액의 4%와 2천만 유로 중 큰 금액**이다.

NoteBase

문 30. ISMS-P(정보보호 및 개인정보보호 관리체계) 인증 기준에서 정하고 있는 관리체계 수립 및 운영 영역의 분야로 가장 적절하지 않은 것은?

① 관리체계 기반 마련

② 위험관리

③ 관리체계 점검 및 개선

④ 정책, 조직, 자산 관리

정답 4번

①

관리체계 기반 마련은 경영진 참여, 책임자 지정, 조직 구성 등을 통해 관리체계의 토대를 갖추는 분야로, **관리체계 수립 및 운영 영역**에 속한다.

https://d2u7om5rih5x7z.cloudfront.net/ox-images/drive-repair/1PJbaf-7cmgIB1pBR1ZfGCZ9tLSocNoa3.webp

②

위험 관리는 정보자산 식별, 현황 및 흐름분석, 위험 평가, 보호대책 선정을 다루는 분야로, **관리체계 수립 및 운영 영역**에 속한다.

https://d2u7om5rih5x7z.cloudfront.net/ox-images/drive-repair/1DK8crcnoacWPUU11hdOXxkcdwUYQzVPY.webp

③

관리체계 점검 및 개선은 법적 요구사항 준수 검토, 관리체계 점검과 개선을 다루는 분야로, **관리체계 수립 및 운영 영역**에 속한다.

https://d2u7om5rih5x7z.cloudfront.net/ox-images/drive-repair/1LvgFwhMiWzq-gfmkHyrXMomcTnqTwV98.webp

NoteBase

④

정책, 조직, 자산 관리는 **보호대책 요구사항 영역**에 속한다. 관리체계 수립 및 운영 영역의 분야는 관리체계 기반 마련, 위험 관리, 관리체계 운영, 관리체계 점검 및 개선이다.

https://d2u7om5rih5x7z.cloudfront.net/ox-images/drive-repair/1cBTIqKK7aB855bO2Qx_D8shTRKXRk7pK.webp

NoteBase

문 31. 'ISO 27001:2022 Annex A 정보보안 통제'에서 기술적 보안(Technological Controls) 항목으로 가장 적절하지 않은 것은?

① 시스템 네트워크 보안

② 애플리케이션 보안

③ 물리적 보안

④ 보안 구성

정답 3번

간단한 해설

정답은 ③이다. **물리적 보안은 물리적 통제라는 독립 범주**이며 기술적 통제에 속하지 않는다. 시스템·네트워크, 애플리케이션, 보안 구성 관리는 기술적 통제에 해당한다.

선지별 해설

① (O) 시스템과 네트워크를 보호하는 통제는 **기술적 통제**에 해당한다. 예를 들어 네트워크 보안, 네트워크 서비스의 보안, 네트워크 분리 등은 정보시스템의 통신과 접근을 기술적으로 보호하는 영역이다.

② (O) 애플리케이션 보안도 **기술적 통제**에 포함된다. 애플리케이션의 보안 요구사항을 정하고, 안전하게 개발·시험하여 소프트웨어의 취약점과 부적절한 동작을 줄이는 것이 그 예이다.

③ (X) **물리적 보안은 별도의 물리적 통제 범주**이다. ISO/IEC 27001:2022 부속서 A는 조직적 통제, 인적 통제, 물리적 통제, 기술적 통제의 네 범주로 구분된다. 건물 출입 통제나 장비의 물리적 보호처럼 장소·시설·장비를 보호하는 조치는 기술적 통제 범주와 구별한다.

④ (O) 보안 구성은 시스템·소프트웨어·네트워크의 설정을 안전하게 정하고 유지하는 **구성 관리**와 관련되며 기술적 통제에 해당한다. 물리적인 시설 보호와 달리 정보기술 환경의 설정 상태를 관리하는 내용이다.

NoteBase

문 32. 정보보호 시스템 공통평가 기준(Common Criteria)의 보증 요구사항으로 'Methodically Designed, Tested and Reviewed(방법론적 설계, 시험, 검토)'에 해당되는 평가보증등급(EAL)으로 가장 적절한 것은?

① EAL2

② EAL3

③ EAL4

④ EAL5

정답 3번

간단한 해설

공통평가기준에서 '방법론적 설계·시험·검토'는 **EAL4**의 명칭이다. 방법론적 시험·점검인 EAL3 및 준정형적 설계·시험인 EAL5와 구별한다.

개념 구분

EAL은 공통평가기준에서 평가 대상의 보안성을 어느 정도의 엄격함과 깊이로 확인하는지를 나타내는 보증 요구사항 묶음이다. 제품의 기능 수나 절대적인 안전성을 직접 나타내는 점수와는 구별한다.

EAL2는 구조적 시험(Structurally tested)에 해당한다.

EAL3는 방법론적 시험 및 점검(Methodically tested and checked)에 해당하므로, 제시된 '설계·시험·검토'와는 명칭이 다르다.

EAL4는 방법론적 설계·시험·검토(Methodically designed, tested and reviewed)이다. 문제에 제시된 영문 명칭의 designed와 reviewed까지 모두 일치하는 등급을 찾으면 된다.

EAL5는 준정형적 설계 및 시험(Semiformally designed and tested)이다. 방법론적이라는 표현과 준정형적이라는 표현을 구별해야 한다.

따라서 제시된 보증 요구사항의 명칭에 해당하는 것은 ③ EAL4이다.

NoteBase

문 33. 다음은 「개인정보보호법」 제2조(정의)에 대한 내용이다. 빈칸 ㉠, ㉡에 해당하는 가장 적절한 것은?

1. “개인정보”란 살아 있는 개인에 관한 정보로서 다음 각 목의 어느 하나에 해당하는 정보를 말한다.
가. (㉠), 주민등록번호 및 (㉡) 등을 통하여 개인을 알아볼 수 있는 정보
나. 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 (㉢)하여 알아볼 수 있는 정보

① ㉠ 성명 ㉡ 전화번호 ㉢ 연계
② ㉠ 성별 ㉡ 전화번호 ㉢ 연계
③ ㉠ 성명 ㉡ 영상 ㉢ 결합
④ ㉠ 성별 ㉡ 영상 ㉢ 연동

정답 3번

가

살아 있는 개인의 성명·주민등록번호·영상 등으로 **그 개인을 알아볼 수 있는 정보는 개인정보**이다.

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 정보만으로 식별되지 않아도 **다른 정보와 쉽게 결합하여 개인을 알아볼 수 있으면 개인정보**이다. 결합의 용이성은 **다른 정보의 입수 가능성과 식별에 드는 시간·비용·기술**을 합리적으로 고려한다.

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.
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.

NoteBase

문 34. 「개인정보 보호법 시행령」에서 명시하는 개인정보 영향평가의 대상에 대한 설명으로 가장 적절하지 않은 것은?

① 구축·운용 또는 변경하려는 개인정보파일로서 10만명 이상의 정보주체에 관한 민감정보 또는 고유식별정보의 처리가 수반되는 개인정보파일

② 구축·운용하고 있는 개인정보파일을 해당 공공기관 내부 또는 외부에서 구축·운용하고 있는 다른 개인정보파일과 연계하려는 경우로서 연계 결과 50만명 이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일

③ 구축·운용 또는 변경하려는 개인정보파일로서 100만명 이상의 정보주체에 관한 개인정보파일

④ 영향평가를 받은 후에 개인정보 검색체계 등 개인정보파일의 운용체계를 변경하려는 경우 그 개인정보파일. 이 경우 영향평가 대상은 변경된 부분으로 한정한다.

정답 1번

①

구축·운용 또는 변경하려는 전자적 개인정보파일이 민감정보 또는 고유식별정보의 처리를 수반하면, 영향평가 대상의 인원 기준은 **정보주체 5만명 이상**이다.

개인정보 보호법 시행령 제35조(개인정보 영향평가의 대상) 법 제33조제1항에서 "대통령령으로 정하는 기준에 해당하는 개인정보파일"이란 개인정보를 전자적으로 처리할 수 있는 개인정보파일로서 다음 각 호의 어느 하나에 해당하는 개인정보파일을 말한다. <개정 2016.9.29>
1. 구축 · 운용 또는 변경하려는 개인정보파일로서 5만명 이상의 정보주체에 관한 민감정보 또는 고유식별정보의 처리가 수반되는 개인정보파일

②

공공기관의 개인정보파일을 내부 또는 외부의 다른 개인정보파일과 연계하려는 경우, **연계 결과 50만명 이상의 정보주체에 관한 개인정보가 포함**되면 영향평가 대상이다.

개인정보 보호법 시행령 제35조(개인정보 영향평가의 대상) 법 제33조제1항에서 "대통령령으로 정하는 기준에 해당하는 개인정보파일"이란 개인정보를 전자적으로 처리할 수 있는 개인정보파일로서 다음 각 호의 어느 하나에 해당하는 개인정보파일을 말한다. <개정 2016.9.29>
2. 구축 · 운용하고 있는 개인정보파일을 해당 공공기관 내부 또는 외부에서 구축 · 운용하고 있는 다른 개인정보파일과 연계하려는 경우로서 연계 결과 50만명 이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일

NoteBase

③

구축·운용 또는 변경하려는 전자적 개인정보파일에 **100만명 이상의 정보주체에 관한 개인정보**가 포함되면 영향평가 대상이다.

개인정보 보호법 시행령 제35조(개인정보 영향평가의 대상) 법 제33조제1항에서 "대통령령으로 정하는 기준에 해당하는 개인정보파일"이란 개인정보를 전자적으로 처리할 수 있는 개인정보파일로서 다음 각 호의 어느 하나에 해당하는 개인정보파일을 말한다. <개정 2016.9.29>
3. 구축 · 운용 또는 변경하려는 개인정보파일로서 100만명 이상의 정보주체에 관한 개인정보파일

④

영향평가를 받은 뒤 개인정보 검색체계 등 파일의 운용체계를 변경하려는 경우에도 영향평가 대상이 되며, **평가범위는 변경된 부분으로 한정**한다.

개인정보 보호법 시행령 제35조(개인정보 영향평가의 대상) 법 제33조제1항에서 "대통령령으로 정하는 기준에 해당하는 개인정보파일"이란 개인정보를 전자적으로 처리할 수 있는 개인정보파일로서 다음 각 호의 어느 하나에 해당하는 개인정보파일을 말한다. <개정 2016.9.29>
4. 법 제33조제1항에 따른 개인정보 영향평가(이하 "영향평가"라 한다)를 받은 후에 개인정보 검색체계 등 개인정보파일의 운용체계를 변경하려는 경우 그 개인정보파일. 이 경우 영향평가 대상은 변경된 부분으로 한정한다.

NoteBase

문 35. 「개인정보보호법」에서 명시하는 영상정보처리기기의 설치·운영 제한과 관련하여 정보주체가 쉽게 인식하도록 설치하는 안내판의 기재 항목으로 가장 적절하지 않은 것은?

① 설치 목적

② 촬영 범위

③ 저장 방식

④ 관리책임자 연락처

정답 3번

①

고정형 영상정보처리기기의 안내판에는 **설치 목적 및 장소**를 기재해야 한다.

개인정보 보호법 제25조(고정형 영상정보처리기기의 설치 · 운영 제한)
④ 제1항 각 호에 따라 고정형 영상정보처리기기를 설치 · 운영하는 자(이하 "고정형영상정보처리기기운영자"라 한다)는 정보주체가 쉽게 인식할 수 있도록 다음 각 호의 사항이 포함된 안내판을 설치하는 등 필요한 조치를 하여야 한다. 다만, 「군사기지 및 군사시설 보호법」 제2조제2호에 따른 군사시설, 「통합방위법」 제2조제13호에 따른 국가중요시설, 그 밖에 대통령령으로 정하는 시설의 경우에는 그러하지 아니하다. <개정 2016.3.29, 2023.3.14>
1. 설치 목적 및 장소

②

고정형 영상정보처리기기의 안내판에는 **촬영 범위 및 시간**을 기재해야 한다.

개인정보 보호법 제25조(고정형 영상정보처리기기의 설치 · 운영 제한)
④ 제1항 각 호에 따라 고정형 영상정보처리기기를 설치 · 운영하는 자(이하 "고정형영상정보처리기기운영자"라 한다)는 정보주체가 쉽게 인식할 수 있도록 다음 각 호의 사항이 포함된 안내판을 설치하는 등 필요한 조치를 하여야 한다. 다만, 「군사기지 및 군사시설 보호법」 제2조제2호에 따른 군사시설, 「통합방위법」 제2조제13호에 따른 국가중요시설, 그 밖에 대통령령으로 정하는 시설의 경우에는 그러하지 아니하다. <개정 2016.3.29, 2023.3.14>
2. 촬영 범위 및 시간

NoteBase

③

안내판의 법정 기재사항은 설치 목적·장소, 촬영 범위·시간, 관리책임자의 연락처 등이며, **저장 방식은 법정 기재사항이 아니다**.

개인정보 보호법 제25조(고정형 영상정보처리기기의 설치 · 운영 제한)
④ 제1항 각 호에 따라 고정형 영상정보처리기기를 설치 · 운영하는 자(이하 "고정형영상정보처리기기운영자"라 한다)는 정보주체가 쉽게 인식할 수 있도록 다음 각 호의 사항이 포함된 안내판을 설치하는 등 필요한 조치를 하여야 한다. 다만, 「군사기지 및 군사시설 보호법」 제2조제2호에 따른 군사시설, 「통합방위법」 제2조제13호에 따른 국가중요시설, 그 밖에 대통령령으로 정하는 시설의 경우에는 그러하지 아니하다. <개정 2016.3.29, 2023.3.14>
1. 설치 목적 및 장소
2. 촬영 범위 및 시간
3. 관리책임자의 연락처
4. 그 밖에 대통령령으로 정하는 사항

④

고정형 영상정보처리기기의 안내판에는 **관리책임자의 연락처**를 기재해야 한다.

개인정보 보호법 제25조(고정형 영상정보처리기기의 설치 · 운영 제한)
④ 제1항 각 호에 따라 고정형 영상정보처리기기를 설치 · 운영하는 자(이하 "고정형영상정보처리기기운영자"라 한다)는 정보주체가 쉽게 인식할 수 있도록 다음 각 호의 사항이 포함된 안내판을 설치하는 등 필요한 조치를 하여야 한다. 다만, 「군사기지 및 군사시설 보호법」 제2조제2호에 따른 군사시설, 「통합방위법」 제2조제13호에 따른 국가중요시설, 그 밖에 대통령령으로 정하는 시설의 경우에는 그러하지 아니하다. <개정 2016.3.29, 2023.3.14>
3. 관리책임자의 연락처

NoteBase

문 36. 다음은 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제23조의2(클라우드컴퓨팅서비스의 보안인증)에 대한 내용이다. 빈칸 ㉠, ㉡에 해당하는 내용으로 가장 적절한 것은?

① (㉠)은 정보보호 수준의 향상 및 보장을 위하여 보안인증기준에 적합한 클라우드컴퓨팅서비스에 대하여 대통령령으로 정하는 바에 따라 인증(이하 "보안인증"이라 한다)을 할 수 있다.
② 보안인증의 유효기간은 인증 서비스 등을 고려하여 대통령령으로 정하는 (㉡) 내의 범위로 하고, 보안인증의 유효기간을 연장받으려는 자는 대통령령으로 정하는 바에 따라 유효기간의 갱신을 신청하여야 한다.

① ㉠ 한국인터넷진흥원장 ㉡ 3년
② ㉠ 한국인터넷진흥원장 ㉡ 5년
③ ㉠ 과학기술정보통신부장관 ㉡ 3년
④ ㉠ 과학기술정보통신부장관 ㉡ 5년

정답 4번

㉠

과학기술정보통신부장관은 정보보호 수준의 향상 및 보장을 위하여 보안인증기준에 적합한 클라우드컴퓨팅서비스에 보안인증을 할 수 있다.

클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제23조의2(클라우드컴퓨팅서비스의 보안인증)
① 과학기술정보통신부장관은 정보보호 수준의 향상 및 보장을 위하여 보안인증기준에 적합한 클라우드컴퓨팅서비스에 대하여 대통령령으로 정하는 바에 따라 인증(이하 "보안인증"이라 한다)을 할 수 있다.

㉡

보안인증의 유효기간은 인증 서비스 등을 고려하여 **5년 내의 범위에서 대통령령으로 정한다**. 유효기간을 연장받으려는 자는 **대통령령에 따라 유효기간의 갱신을 신청하여야 한다**.

클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제23조의2(클라우드컴퓨팅서비스의 보안인증)
② 보안인증의 유효기간은 인증 서비스 등을 고려하여 대통령령으로 정하는 5년 내의 범위로 하고, 보안인증의 유효기간을 연장받으려는 자는 대통령령으로 정하는 바에 따라 유효기간의 갱신을 신청하여야 한다.

NoteBase

문 37. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조(정보보호 관리체계의 인증)에 대한 내용이다. 가장 적절한 것은?

① 과학기술정보통신부는 정보통신망의 안정성·신뢰성 확보를 위하여 정보통신망 보호조치를 포함한 관리체계를 수립·운영하고 있는 자에 대하여 인증을 할 수 있다.

② 연간 매출액 또는 세입 등이 1,000억원 이상이거나 정보통신서비스 부문 전년도 매출액이 100억원 이상 또는 3개월간의 일일평균 이용자수 100만명 이상으로서, 대통령령으로 정하는 기준에 해당하는 자는 인증을 받아야 한다.

③ 한국인터넷진흥원, 정보보호 관리체계 인증기관 및 정보보호 관리체계 심사기관은 정보보호 관리체계의 실효성 제고를 위하여 연 1회 이상 사후관리를 실시한다.

④ 정보보호 관리체계 인증의 유효기간은 2년으로 한다.

정답 3번

①

정보보호 관리체계의 인증 권한을 가진 주체는 **과학기술정보통신부장관**이다. 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계가 인증기준에 적합한지를 심사하여 인증할 수 있다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제47조(정보보호 관리체계의 인증)
① 과학기술정보통신부장관은 정보통신망의 안정성 · 신뢰성 확보를 위하여 관리적 · 기술적 · 물리적 보호조치를 포함한 종합적 관리체계(이하 "정보보호 관리체계"라 한다)를 수립 · 운영하고 있는 자에 대하여 제4항에 따른 기준에 적합한지에 관하여 인증을 할 수 있다. <개정 2012.2.17, 2013.3.23, 2015.12.1, 2017.7.26>

②

매출액·세입 기준은 **전년도 1,500억원 이상**이고, 이용자 수 기준은 **전년도 일일평균 100만명 이상**이다. 정보통신서비스 부문 전년도 매출액 100억원 이상이라는 기준은 맞지만, 선지의 1,000억원과 3개월간이라는 기준은 다르다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제47조(정보보호 관리체계의 인증)
② 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자로서 다음 각 호의 어느 하나에 해당하는 자는 제1항에 따른 인증을 받아야 한다. <신설 2012.2.17, 2015.12.1, 2018.12.24, 2020.6.9, 2024.1.23, 2026.3.31>
3. 전년도 매출액 또는 세입 등이 1,500억원 이상이거나 정보통신서비스 부문 전년도 매출액이 100억원 이상 또는 전년도 일일평균 이용자수 100만명 이상으로서, 대통령령으로 정하는 기준에 해당하는 자

NoteBase

③

한국인터넷진흥원, 정보보호 관리체계 인증기관 및 심사기관은 **연 1회 이상 사후관리를 실시**하고 그 결과를 과학기술정보통신부장관에게 통보하여야 한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제47조(정보보호 관리체계의 인증)
⑧ 한국인터넷진흥원, 정보보호 관리체계 인증기관 및 정보보호 관리체계 심사기관은 정보보호 관리체계의 실효성 제고를 위하여 연 1회 이상 사후관리를 실시하고 그 결과를 과학기술정보통신부장관에게 통보하여야 한다. 이 경우 사후관리는 현장심사와 서면심사의 방법을 병행하여 실시한다. <신설 2012.2.17, 2013.3.23, 2015.12.1, 2017.7.26, 2026.3.31>

④

정보보호 관리체계 인증의 유효기간은 **3년**이다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제47조(정보보호 관리체계의 인증)
⑤ 제1항에 따른 정보보호 관리체계 인증의 유효기간은 3년으로 한다. 다만, 제47조의5제1항에 따라 정보보호 관리등급을 받은 경우 그 유효기간 동안 제1항의 인증을 받은 것으로 본다. <신설 2012.2.17, 2015.12.1>

NoteBase

문 38. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」에서 명시하는 집적정보통신시설 사업자등의 서비스 중단 보고 방법에 대한 설명으로 가장 적절하지 않은 것은?

① 연속해서 30분 이상 서비스 중단 시 보고한다.

② 24시간 이내에 2회 이상 중단된 경우에는 그 중단된 기간의 합이 45분 이상 시 보고한다.

③ 보고 시 발생한 일시 및 장소, 발생 원인 및 피해내용, 응급조치 사항, 대응 및 복구대책, 향후 조치계획 등을 포함해야 한다.

④ 집적정보통신시설 사업자등은 정보통신서비스 제공의 중단이 발생하였을 때에는 과학기술정보통신부장관에게 즉시 유선으로 보고해야 한다.

정답 4번

①

정보통신서비스 제공이 **연속해서 30분 이상 중단**되면 보고 대상이다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제40조(집적정보통신시설 사업자등의 서비스 중단 보고 방법)
① 법 제46조제6항에서 "대통령령으로 정하는 기간"이란 다음 각 호의 어느 하나에 해당하는 기간을 말한다.
1. 연속해서 30분 이상

②

24시간 이내에 2회 이상 중단되고 중단 기간의 합이 45분 이상이면 보고 대상이다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제40조(집적정보통신시설 사업자등의 서비스 중단 보고 방법)
① 법 제46조제6항에서 "대통령령으로 정하는 기간"이란 다음 각 호의 어느 하나에 해당하는 기간을 말한다.
2. 24시간 이내에 2회 이상 중단된 경우에는 그 중단된 기간의 합이 45분 이상

NoteBase

③

보고에는 **중단 발생 일시·장소, 원인·피해내용, 응급조치 사항, 대응·복구대책, 향후 조치계획**과 그 밖에 대응·복구에 필요한 사항을 포함해야 한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제40조(집적정보통신시설 사업자등의 서비스 중단 보고 방법)
② 법 제46조제6항에 따른 보고에는 다음 각 호의 사항이 포함되어야 한다.
1. 정보통신서비스 제공의 중단이 발생한 일시 및 장소
2. 정보통신서비스 제공의 중단이 발생한 원인 및 피해내용
3. 응급조치 사항
4. 대응 및 복구대책
5. 향후 조치계획
6. 그 밖에 정보통신서비스 제공의 중단에 대한 대응 및 복구에 필요한 사항

④

집적정보통신시설 사업자등은 서비스 중단을 과학기술정보통신부장관에게 **문서로 보고**해야 하므로, 유선 보고를 요구한다는 부분이 틀리다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제40조(집적정보통신시설 사업자등의 서비스 중단 보고 방법)
③ 집적정보통신시설 사업자등은 법 제46조제6항에 따라 정보통신서비스 제공의 중단이 발생하였을 때에는 과학기술정보통신부장관에게 문서로 보고해야 한다.

NoteBase

문 39. 「정보통신기반 보호법」에서 지정한 주요정보통신기반시설로 가장 적절하지 않은 것은?

① 도로, 철도, 지하철, 공항, 항만 등 주요 교통시설

② 전력, 가스, 석유 등 에너지·수자원 시설

③ 인터넷 포털, 전자상거래의 정보통신시설

④ 원자력, 국방과학, 첨단방위산업관련 정부출연연구기관의 연구시설

정답 3번

①

도로·철도·지하철·공항·항만 등 주요 교통시설은 **국가안전보장에 중대한 영향을 미치는 주요정보통신기반시설**로 열거되어 있다.

정보통신기반 보호법 제7조(주요정보통신기반시설의 보호지원)
②국가안전보장에 중대한 영향을 미치는 다음 각 호의 주요정보통신기반시설에 대한 관리기관의 장이 제1항에 따라 기술적 지원을 요청하는 경우 국가정보원장에게 우선적으로 그 지원을 요청하여야 한다. 다만, 국가안전보장에 현저하고 급박한 위험이 있고, 관리기관의 장이 요청할 때까지 기다릴 경우 그 피해를 회복할 수 없을 때에는 국가정보원장은 관계중앙행정기관의 장과 협의하여 그 지원을 할 수 있다. <개정 2007.12.21>
1. 도로 · 철도 · 지하철 · 공항 · 항만 등 주요 교통시설

②

전력·가스·석유 등 에너지·수자원 시설은 **국가안전보장에 중대한 영향을 미치는 주요정보통신기반시설**로 열거되어 있다.

정보통신기반 보호법 제7조(주요정보통신기반시설의 보호지원)
②국가안전보장에 중대한 영향을 미치는 다음 각 호의 주요정보통신기반시설에 대한 관리기관의 장이 제1항에 따라 기술적 지원을 요청하는 경우 국가정보원장에게 우선적으로 그 지원을 요청하여야 한다. 다만, 국가안전보장에 현저하고 급박한 위험이 있고, 관리기관의 장이 요청할 때까지 기다릴 경우 그 피해를 회복할 수 없을 때에는 국가정보원장은 관계중앙행정기관의 장과 협의하여 그 지원을 할 수 있다. <개정 2007.12.21>
2. 전력, 가스, 석유 등 에너지 · 수자원 시설

NoteBase

③

국가안전보장에 중대한 영향을 미치는 시설로 열거된 통신시설은 **방송중계·국가지도통신망 시설**이다. 인터넷 포털·전자상거래 시설은 이 열거에 포함되지 않는다.

정보통신기반 보호법 제7조(주요정보통신기반시설의 보호지원)
②국가안전보장에 중대한 영향을 미치는 다음 각 호의 주요정보통신기반시설에 대한 관리기관의 장이 제1항에 따라 기술적 지원을 요청하는 경우 국가정보원장에게 우선적으로 그 지원을 요청하여야 한다. 다만,
국가안전보장에 현저하고 급박한 위험이 있고, 관리기관의 장이 요청할 때까지 기다릴 경우 그 피해를 회복할 수 없을 때에는 국가정보원장은 관계중앙행정기관의 장과 협의하여 그 지원을 할 수 있다. <개정 2007.12.21>
1. 도로 · 철도 · 지하철 · 공항 · 항만 등 주요 교통시설
2. 전력, 가스, 석유 등 에너지 · 수자원 시설
3. 방송중계 · 국가지도통신망 시설
4. 원자력 · 국방과학 · 첨단방위산업관련 정부출연연구기관의 연구시설

④

원자력·국방과학·첨단방위산업 관련 정부출연연구기관의 연구시설은 **국가안전보장에 중대한 영향을 미치는 주요정보통신기반시설**로 열거되어 있다.

정보통신기반 보호법 제7조(주요정보통신기반시설의 보호지원)
②국가안전보장에 중대한 영향을 미치는 다음 각 호의 주요정보통신기반시설에 대한 관리기관의 장이 제1항에 따라 기술적 지원을 요청하는 경우 국가정보원장에게 우선적으로 그 지원을 요청하여야 한다. 다만,
국가안전보장에 현저하고 급박한 위험이 있고, 관리기관의 장이 요청할 때까지 기다릴 경우 그 피해를 회복할 수 없을 때에는 국가정보원장은 관계중앙행정기관의 장과 협의하여 그 지원을 할 수 있다. <개정 2007.12.21>
4. 원자력 · 국방과학 · 첨단방위산업관련 정부출연연구기관의 연구시설

NoteBase

문 40. 다음은 「정보통신기반 보호법 시행령」에 대한 내용이다. 빈칸 ㉠, ㉡에 해당하는 내용으로 가장 적절한 것은?

제8조(주요정보통신기반시설보호대책의 수립)에서는 주요정보통신기반시설보호대책을 수립하여 매년 (㉠)까지 (㉡)의 장에게 제출하여야 한다.

① ㉠ 5월 31일 ㉡ 관계중앙행정기관

② ㉠ 8월 31일 ㉡ 관계중앙행정기관

③ ㉠ 5월 31일 ㉡ 위원회

④ ㉠ 8월 31일 ㉡ 위원회

정답 2번

공통 해설

관리기관의 장 및 지방자치단체의 장은 다음 연도의 주요정보통신기반시설보호대책을 수립하여 **매년 8월 31일까지 관계중앙행정기관의 장에게 제출**해야 한다.

정보통신기반 보호법 시행령 제8조(주요정보통신기반시설보호대책의 수립) 법 제5조제2항 또는 제3항에 따라 관리기관의 장 및 지방자치단체의 장은 다음 연도의 법 제5조제1항에 따른 주요정보통신기반시설보호대책(이하 "주요정보통신기반시설보호대책"이라 한다)을 수립하여 매년 8월 31일까지 관계중앙행정기관의 장에게 제출하여야 한다.

NoteBase