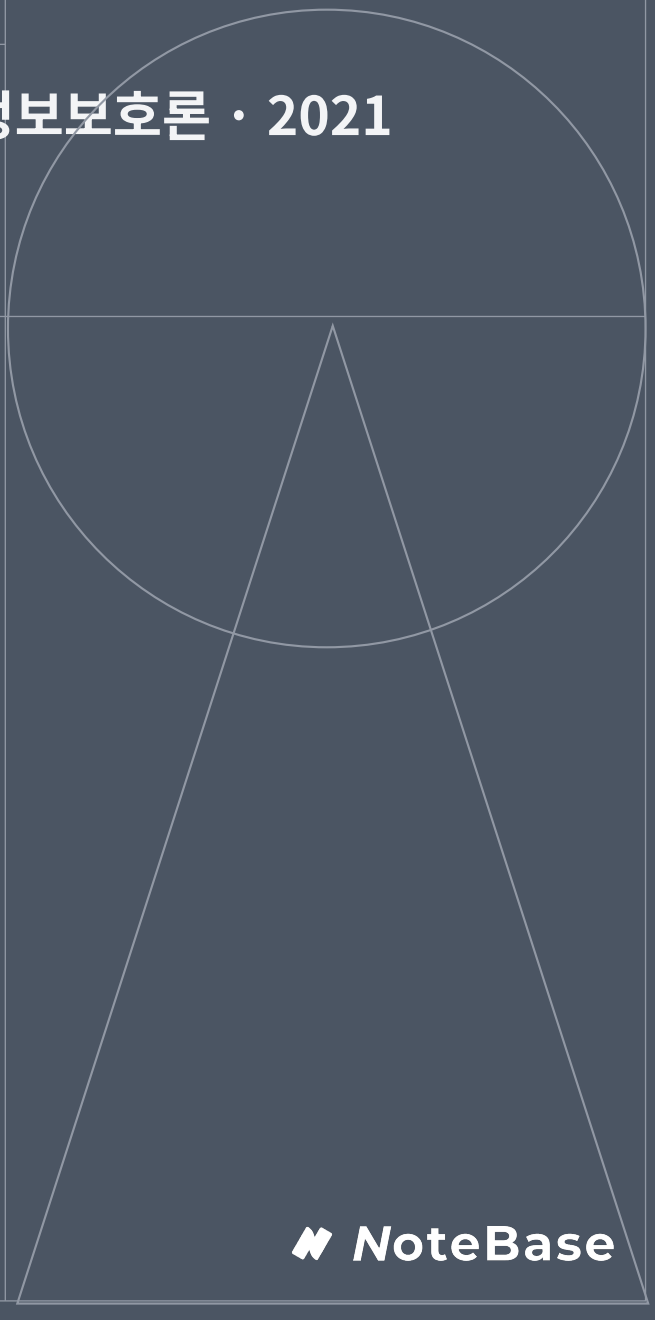
기출OX 해설집

공무원/경찰/공채(경위) · 정보보호론 · 2021



NoteBase

기출OX 해설집

공무원/경찰/공채(경위) · 정보보호론 · 2021

공무원/경찰/공채(경위) · 정보보호론 · 2021

문 1. 다음 중 정보보호의 목표에 대한 설명으로 가장 옳은 것은?

① 가용성(Availability)은 정보에 접근할 수 있는 객체의 자격이나 내용을 검증하는 데 사용되는 성질이다.

② 기밀성(Confidentiality)은 정당한 사용자가 정보 시스템의 데이터 또는 자원을 필요로 할 때 지체 없이 접근하여 사용할 수 있게 하는 성질이다.

③ 무결성(Integrity)은 정보의 내용이 불법적으로 생성, 변경 또는 삭제되지 않도록 하는 성질이다.

④ 인증성(Authentication)은 행위나 사건이 발생하였을 때 그것을 증명하여 나중에 그런 행위나 사건을 부인할 수 없도록 하는 성질이다.

정답 3번

간단한 해설

무결성은 정보가 권한 없이 생성·변경·삭제되어 내용이 훼손되지 않도록 보호하는 성질이다. 이용 가능 여부인 가용성이나 신원·진위 확인인 인증과 구별된다.

NoteBase

선지별 해설

① X: 접근 주체의 신원이나 자격, 정보의 진위를 검증한다는 설명은 **인증**과 관련된다. **가용성**은 정당한 사용자가 필요한 시점에 정보나 서비스를 이용할 수 있는 성질이다. 시스템 장애나 서비스 거부 공격으로 정상적인 이용이 막히면 가용성이 침해된다.

② X: 정당한 사용자가 필요할 때 데이터나 자원에 접근하여 사용할 수 있다는 설명은 **가용성**에 해당한다. **기밀성**은 허가되지 않은 사람에게 정보가 공개되거나 노출되지 않도록 하는 성질이다. 따라서 이용 가능성과 비밀 유지의 의미를 바꾸어 설명했다.

③ O: **무결성**은 정보의 정확성과 온전함을 보호하여 허가되지 않은 생성·변경·삭제를 방지하는 성질이다. 예를 들어 전송 중 내용이 몰래 바뀌거나 저장된 기록이 무단 삭제되는 것은 무결성 침해이다. 정당한 권한과 절차에 따른 수정까지 금지한다는 뜻은 아니다.

④ X: 행위나 사건이 실제로 있었음을 증명하여 당사자가 나중에 이를 부인하지 못하게 하는 것은 **부인방지**이다. **인증**은 사용자나 정보가 주장하는 신원·출처와 일치하는지 확인하는 것이다. 단순한 신원 확인과 사후 부인을 막을 수 있는 증거 확보는 구별해야 한다.

NoteBase

문 2. 다음 지문은 OECD의 개인정보보호 8원칙 중 무엇에 관한 설명인가?

◯ 정보주체의 개인정보 열람·정정·삭제 청구권 보장
◯ 정보주체가 합리적 시간과 방법에 의해 개인정보에 접근할 수 있도록 보장

① 수집 제한의 원칙(Collection Limitation Principle)
② 공개의 원칙(Openness Principle)
③ 안전성 확보의 원칙(Security Safeguard Principle)
④ 개인 참가의 원칙(Individual Participation Principle)

정답 4번

간단한 해설

정보주체가 자신의 개인정보에 접근하고 정정·삭제를 청구할 수 있도록 보장하는 것은 **개인 참가의 원칙**이다. 개인정보 처리에 정보주체가 직접 관여할 권리를 보장한다는 점이 핵심이다.

공통 해설

개인 참가의 원칙은 정보주체가 자신의 개인정보 보유 여부를 확인하고, 그 내용을 열람하며, 정보에 이의를 제기할 권리를 보장하는 원칙이다. 개인정보에 대한 접근은 **합리적인 시간과 방법**으로 이루어져야 한다. 정보에 대한 이의가 받아들여지면 해당 정보의 삭제·정정·보완 등이 이루어지도록 한다.

지문의 '열람·정정·삭제 청구권'과 '합리적 시간과 방법에 의한 접근'은 모두 **정보주체가 자신의 정보에 관해 권리를 행사**하도록 하는 내용이므로 개인 참가의 원칙에 해당한다. 단순히 개인정보 처리 방침 등을 알리는 공개와 구별하여, 본인이 실제로 정보에 접근하고 그 내용에 이의를 제기할 수 있다는 점에 주목한다.

NoteBase

문 3. 다음 지문에 주어진 암호문을 Caesar Cipher를 사용하여 복호화할 때 결과는?

다음은 SHIFT +3을 적용한 암호문이다.
SROLFHORYH

① VULNERABLE
② VUROIKRUBK
③ POLICEBEST
④ POLICELOVE

정답 4번

간단한 해설

암호화에서 각 문자를 +3칸 이동했으므로 복호화할 때에는 **각 문자를 3칸 앞쪽으로 되돌린다**. SROLFHORYH에 이를 적용하면 POLICELOVE가 된다.

계산 과정

Caesar Cipher는 알파벳을 일정한 칸 수만큼 이동시키는 치환 암호이다. **암호화가 SHIFT +3이면 복호화는 반대 방향으로 3칸 이동**해야 한다. A부터 Z까지를 0부터 25로 놓으면 암호화는 C=(P+3) 26, 복호화는 P=(C-3) 26이다. P는 평문 문자의 번호, C는 암호문 문자의 번호이며, mod 26은 알파벳 범위를 벗어나면 순환한다는 뜻이다.

암호문 SROLFHORYH의 각 문자를 3칸씩 되돌리면 다음과 같다.
S → P, R → O, O → L, L → I, F → C, H → E, O → L, R → O, Y → V, H → E

복호화한 문자를 원래 순서대로 연결하면 **POLICELOVE**가 된다. 이는 ④와 일치한다.

NoteBase

문 4. 다음 지문에서 대칭키 방식의 암호화 알고리즘은 모두 몇 개인가?

가. ARIA 나. DES 다. DSA 라. ElGamal
마. ECC 바. RSA 사. SEED

① 2개
② 3개
③ 4개
④ 5개

정답 2번

간단한 해설

ARIA·DES·SEED는 공유 비밀키를 사용하는 대칭키 블록암호이다. DSA는 공개키 기반 전자서명 알고리즘이고, ElGamal·ECC·RSA도 공개키 방식에 속한다.

NoteBase

보기별 해설

대칭키 암호는 송신자와 수신자가 공유하는 비밀키를 이용해 데이터를 암호화·복호화한다. 공개키 방식은 공개키와 개인키의 역할을 구분하며, 전자서명 알고리즘은 그 목적도 기밀성 제공을 위한 암호화와 다르다.

가. ARIA: **대칭키 블록암호**이다. 공유 비밀키를 사용하여 일정한 크기의 데이터 블록을 암호화·복호화하므로 대칭키 암호화 알고리즘에 포함된다.

나. DES: **대칭키 블록암호**이다. 암호화와 복호화가 공유 비밀키를 기반으로 이루어지므로 포함된다. 암호 내부에서 라운드별 키를 만들어 사용한다는 사실이 공개키 방식이라는 뜻은 아니다.

다. DSA: **공개키 기반 전자서명 알고리즘**이다. 개인키로 서명을 생성하고 공개키로 검증한다. 메시지의 기밀성을 위한 대칭키 암호화 알고리즘이 아니므로 제외한다.

라. ElGamal: **공개키 암호 방식**이다. 수신자의 공개키로 암호화하고 대응하는 개인키로 복호화하므로 대칭키 방식에서 제외한다.

마. ECC: **타원곡선에 기반한 공개키 암호기술 계열**이다. 타원곡선 위 연산을 활용하여 키 합의나 전자서명 등을 구성하며, 공유 비밀키로 데이터를 처리하는 대칭키 블록암호가 아니므로 제외한다.

바. RSA: **공개키와 개인키를 구분**하는 비대칭키 방식이다. 대칭키 암호화 알고리즘이 아니므로 제외한다.

사. SEED: **대칭키 블록암호**이다. 송수신자가 공유하는 비밀키를 기반으로 데이터 블록을 암호화·복호화하므로 포함된다.

대칭키 암호화 알고리즘은 가·나·사인 ARIA, DES, SEED의 3개이므로 ②에 해당한다.

NoteBase

문 5. 송신자 A와 수신자 B가 Diffie-Hellman 키 분배 알고리즘을 이용하여 동일한 비밀키를 분배받고자 한다. 다음과 같은 조건이 주어졌을 때 분배받은 비밀키 값으로 옳은 것은?

g^x p (p, g는 값은 공개되어 있고, x는 개인키)
송신자 A: $p = 7, g = 3, x = 3$
수신자 B: $p = 7, g = 3, x = 2$

① 1
② 3
③ 5
④ 7

정답 1번

간단한 해설

A와 B의 공개값은 각각 6과 2이다. **상대의 공개값에 자신의 개인키를 지수로 적용**하면 A는 2^3 7=1, B는 6^2 7=1을 얻으므로 공유 비밀키는 1이다.

계산 과정

조건과 계산 원리: p = 7과 g = 3은 두 사람이 함께 사용하는 공개값이다. A의 개인키를 $x_A = 3$, B의 개인키를 $x_B = 2$로 구분한다. 각자 y=g^x p를 계산해 교환하고, **상대방에게 받은 공개값을 자신의 개인키만큼 거듭제곱**한 뒤 p로 나눈 나머지를 공유 비밀키로 사용한다.

공개값 교환: A가 B에게 보내는 값은 y_A=3^3 7=27 7=6이다. B가 A에게 보내는 값은 y_B=3^2 7=9 7=2이다. 이때 6과 2는 **교환하는 공개값이며 최종 비밀키가 아니다**.

공유 비밀키 계산: A는 B에게 받은 2를 사용하므로 K_A=2^3 7=8 7=1이다. B는 A에게 받은 6을 사용하므로 K_B=6^2 7=36 7=1이다. 두 계산은 모두 g^x_Ax_B p를 구하는 것이므로 같은 결과가 나온다.

따라서 공유 비밀키 값은 1이며, 이에 해당하는 선택지는 ①이다.

NoteBase

문 6. 다음 중 암호학적 해시 함수(hash function)가 갖추어야 할 특성에 대한 설명으로 가장 옳지 않은 것은?

① 임의 길이의 메시지를 고정 길이의 해시값 출력으로 변환하여야 한다.

② 해시값 출력의 충돌을 방지하기 위해 입력 공간이 출력 공간보다 커야 한다.

③ 임의의 해시값 출력에 대한 입력 메시지를 구하는 것이 계산상 불가능해야 한다.

④ 같은 해시값 출력을 생성하는 임의의 2개의 입력값을 찾는 것이 계산상 불가능해야 한다.

정답 2번

간단한 해설

입력 공간이 출력 공간보다 크면 **비둘기집 원리에 의해 충돌이 반드시 존재**한다. 암호학적 해시 함수는 충돌이 전혀 없게 하는 것이 아니라, **충돌하는 입력 쌍을 찾기 어렵게** 해야 한다.

선지별 해설

① O: 통상적인 암호학적 해시 함수는 길이가 다양한 메시지를 받아 **고정 길이의 해시값**으로 변환한다. 같은 함수를 사용하면 짧은 입력과 긴 입력도 같은 길이의 결과를 내며, 동일한 입력에는 동일한 결과가 나온다. 메시지 전체를 일정한 길이의 값으로 요약하는 기능이다.

② X: 서로 다른 입력의 수가 가능한 출력의 수보다 많으면, 적어도 두 입력은 같은 출력에 대응해야 한다. 이것이 **비둘기집 원리**이다. 따라서 입력 공간이 출력 공간보다 큰 것은 충돌을 방지하는 조건이 아니라 충돌이 불가피한 이유이다. 요구되는 것은 충돌 자체의 부재가 아니라, 충돌하는 서로 다른 입력을 계산으로 찾아내기 어려운 성질이다.

③ O: 주어진 해시값에 대응하는 입력 메시지를 찾기 어려워야 한다는 것은 **역상 저항성**이다. 즉, 해시값 h가 주어졌을 때 $H(m) = h$를 만족하는 메시지 m을 찾는 일이 현실적인 계산 자원으로 매우 어려워야 한다. 원래 메시지와 똑같은 것을 찾는 것뿐 아니라 같은 해시값을 내는 어떤 입력을 찾는 것도 대상이다.

④ O: 공격자가 두 입력을 자유롭게 고르더라도 서로 다른 두 입력에 대해 $H(m_1) = H(m_2)$인 쌍을 찾기 어려워야 한다는 것은 **충돌 저항성**이다. 한 메시지가 미리 주어지고 그와 같은 해시값을 내는 다른 메시지를 찾기 어려워야 한다는 제2역상 저항성과는 문제의 조건이 다르다.

NoteBase

문 7. 다음 중 국산 해시 암호 알고리즘으로 올바르게 묶인 것은?

① SEED, HIGHT

② HAS-160, LSH

③ SHA-1, HAS-160

④ LSH, LEA

정답 2번

간단한 해설

HAS-160과 LSH는 모두 **국내에서 개발된 해시 함수**이므로 국산이라는 조건과 해시 알고리즘이라는 조건을 함께 충족한다.

개념 구분

이 문항에서는 **국내에서 개발되었는지**와 **해시 함수인지**를 함께 구분해야 한다. 해시 함수는 입력 메시지를 정해진 길이의 요약값으로 변환하며, 키로 평문을 암호화하고 복호화하는 블록암호와 역할이 다르다.

HAS-160과 LSH는 모두 **국산 해시 함수**이다. HAS-160은 160비트 해시값을 생성하며 국내 전자서명 알고리즘 KCDSA에 사용되는 해시 함수로 개발되었다. LSH도 국내에서 개발된 해시 함수로서 메시지 인증·전자서명 등의 암호 응용에 활용된다.

SEED·HIGHT·LEA는 국내에서 개발되었지만 **해시 함수가 아니라 블록암호**이다. 따라서 SEED와 HIGHT를 묶은 경우나 LSH에 LEA를 함께 넣은 경우에는 해시 함수라는 조건을 충족하지 못한다.

SHA-1은 해시 함수이지만 **미국에서 개발된 알고리즘**이다. HAS-160과 함께 묶어도 둘 다 국산이라는 조건은 성립하지 않는다.

두 조건을 모두 충족하는 쌍은 HAS-160과 LSH이므로 ②에 해당한다.

NoteBase

문 8. 다음 중 전자 서명에 대한 설명으로 가장 옳지 않은 것은?

① 은닉 서명은 문서의 내용을 공개하지 않고, 문서에 대한 서명을 받는다.

② 부가형 서명은 서명 검증 과정에서 메시지를 추출할 수 없다.

③ 부인 방지 서명은 대칭키 암호 알고리즘을 이용하여 구현된다.

④ 다중 서명 방식은 하나의 문서에 여러 명이 서명할 수 있다.

정답 3번

간단한 해설

부인 방지 서명은 **공개키·개인키를 사용하는 전자서명 방식**이며, 대칭키 암호만으로 구현하는 방식이 아니다. 검증자가 공유 비밀키로 인증값을 직접 만들 수 있는 대칭키 인증과 서명자의 고유한 서명 권한은 구별된다.

선지별 해설

전자서명의 변형은 서명자에게 원문을 공개하는지, 검증 때 원문이 별도로 필요한지, 검증에 서명자의 참여가 필요한지, 몇 명이 서명하는지 등에 따라 구별한다.

① O: 은닉 서명은 요청자가 문서를 알아볼 수 없게 변환한 뒤 서명자에게 서명을 받는 방식이다. 요청자는 결과에서 은닉 처리를 제거하여 원래 문서에 대한 유효한 서명을 얻는다. 핵심은 **서명자에게 문서 내용을 드러내지 않는 것**이며, 문서가 누구에게도 영원히 공개되지 않는다는 뜻은 아니다.

② O: 부가형 서명은 메시지와 별도로 생성한 서명값을 붙여 전달하는 방식이다. 검증에는 **메시지 자체가 별도로 필요**하며, 서명값을 검증하는 것만으로 원래 메시지가 복원되지는 않는다. 메시지를 서명에서 복원할 수 있는 복원형 서명과 구별된다.

③ X: 부인 방지 서명은 **공개키 기반 서명 방식**이다. 대표적인 형태에서는 서명의 유효성 확인에 서명자가 참여하며, 유효한 서명임을 확인하는 절차와 유효하지 않은 서명임을 증명하는 절차를 둔다. 단순한 대칭키 메시지 인증은 송신자와 수신자가 같은 비밀키를 공유하여 양쪽 모두 인증값을 만들 수 있으므로, 그것만으로 제3자에게 특정 서명자의 생성 사실을 입증하기 어렵다.

④ O: 다중 서명은 **동일한 문서에 여러 서명자가 참여**하도록 하는 방식이다. 공동 승인 등이 필요한 문서에서 각 참여자의 서명을 확인하거나 이들을 결합한 서명으로 여러 사람의 참여를 검증할 수 있다.

NoteBase

문 9. 정부가 추진하는 '5G+전략' 10대 핵심 산업과 가장 관련성이 없는 것은?

① 지능형 CCTV

② 미래형 드론

③ 정보보안

④ 나노 복제

정답 4번

간단한 해설

'5G+ 전략'의 선정 목록을 기준으로 비교하면 **나노 복제는 10대 핵심산업에 포함되지 않는다**. 기술의 첨단성 자체가 정책상 핵심산업의 선정 여부를 뜻하지는 않는다.

선지별 해설

2019년 발표된 '5G+ 전략'의 10대 핵심산업은 네트워크 장비, 차세대 스마트폰, VR·AR 디바이스, 웨어러블 디바이스, 지능형 CCTV, 미래형 드론, 커넥티드 로봇, 5G V2X, 정보보안, 엣지컴퓨팅이다. 이 문항의 비교 기준은 첨단기술 일반의 중요성이 아니라 이 전략에서 선정한 핵심산업인지 여부이다.

① 지능형 CCTV: 10대 핵심산업의 **스마트 디바이스** 분야에 포함된다. 영상정보를 활용하여 도시의 위험 상황을 실시간으로 감지하고 대응하는 장치로, 5G의 대용량·실시간 통신 활용과 연결된다.

② 미래형 드론: 10대 핵심산업의 **무인이동체** 분야에 포함된다. 5G를 통한 원격조종, 자율비행 지원, 고화질 영상의 실시간 전송 등을 바탕으로 시설물 관리나 원격 관측 등의 활용을 넓히는 분야이다.

③ 정보보안: 10대 핵심산업의 **보안·컴퓨팅** 분야에 포함된다. 센서·기기·서비스가 대규모로 연결되는 환경에서 5G 네트워크와 사물인터넷의 안전한 이용을 뒷받침한다.

④ 나노 복제: 해당 전략에서 정한 **10대 핵심산업에 포함되지 않는다**. 다른 첨단기술과의 잠재적 융합 가능성까지 부정하는 것이 아니라, 제시된 정책의 선정 목록에 속하지 않는다는 점에서 다른 세 산업과 구별된다.

따라서 '5G+ 전략'의 10대 핵심산업과 가장 관련성이 없는 항목은 ④이다.

NoteBase

문 10. 다음 지문에서 설명하고 있는 보안 통제 기법은?

임의의 객체에 포함되어 있는 정보가 명시적으로 혹은 암시적으로 보다 보호수준이 낮은 객체로 이동하는 것을 검사하여 부당한 데이터 전달을 제어하는 기술

① 접근 제어
② 흐름 제어
③ 추론 제어
④ 사후 추적

정답 2번

간단한 해설

보호수준이 높은 객체에서 낮은 객체로 정보가 부당하게 전달되는 것을 통제하는 것은 흐름 제어이다. 직접 복사하는 명시적 흐름뿐 아니라 처리 결과에 정보가 드러나는 암시적 흐름도 대상으로 한다.

구성 요소별 해설

통제 대상과 방향: 지문은 특정 사용자의 열람 자격보다 **객체 사이에서 정보가 어느 방향으로 전달되는지**에 주목한다. 높은 보호수준의 정보가 낮은 보호수준의 객체로 전달되면 권한이 낮은 사용자에게 노출될 수 있으므로, 보안 정책에 어긋나는 전달을 막는 '흐름 제어'에 해당한다.

명시적·암시적 이동: 정보를 직접 복사하거나 값을 대입해 전달하는 것은 명시적 흐름이다. 비밀정보에 따라 분기한 결과가 공개값에 드러나는 것처럼, 직접 복사하지 않아도 정보가 전달되는 것은 암시적 흐름이다. 따라서 지문의 '명시적으로 혹은 암시적으로'는 **직접적인 데이터 복사만 통제하는 것이 아님**을 나타낸다.

다른 통제 기법과의 구분: '접근 제어'는 어떤 주체가 객체에 읽기·쓰기 등의 연산을 할 수 있는지 제한한다. '추론 제어'는 허용된 자료나 통계 결과를 결합하여 비공개 정보를 알아내는 것을 제한한다. '사후 추적'은 기록을 통해 수행한 행위와 책임 소재를 확인하는 데 초점이 있다. 지문처럼 보호수준에 따른 객체 간 정보 전달 자체를 규제하는 설명과 구별된다.

따라서 지문의 조건에 대응하는 보안 통제 기법은 흐름 제어이며, 선택지는 ②이다.

NoteBase

문 11. 다음 지문에서 설명하고 있는 접근통제 모델은?

이 모델은 데이터의 기밀성을 희생하더라도 무결성을 보호하는 것에 초점을 둔 최초의 수학적 모델이며, 무결성 레벨을 계층적으로 정의한다. 이 레벨은 조직에 따라, 다루는 업무에 따라 달라질 수 있다. 이 모델에서 주체는 자신보다 낮은 무결성 수준의 데이터를 읽을 수 없다(단순 무결성 원칙). 주체는 자신보다 높은 무결성 수준에 있는 객체를 수정할 수 없다(스타 무결성 원칙).

① 벨 라파듈라 모델 (Bell Lapadula Model)

② 비바 모델 (Biba Model)

③ 래티스 모델 (Lattice Model)

④ 클라크 윌슨 모델 (Clark-Wilson Model)

정답 2번

간단한 해설

낮은 무결성 수준 읽기 금지와 **높은 무결성 수준 쓰기 금지**는 신뢰도가 낮은 정보의 영향을 차단하는 비바 모델의 규칙이다.

NoteBase

구성 요소별 해설

보호 목표와 등급: **비바 모델**은 기밀성보다 데이터의 무결성 보호에 초점을 둔 대표적인 형식적 접근통제 모델이다. 주체와 객체에 무결성 수준을 부여하고, 신뢰성이 낮은 정보가 높은 수준의 정보나 처리에 영향을 미치지 못하도록 통제한다. 수준의 구체적 의미는 조직과 업무에 맞게 정해진다.

단순 무결성 원칙: 주체는 자신보다 낮은 무결성 수준의 객체를 읽지 못한다. 이를 **No Read Down**이라고 한다. 낮은 신뢰도의 데이터를 읽어 높은 신뢰도가 요구되는 판단이나 처리에 사용하는 것을 막는 규칙이다.

스타 무결성 원칙: 주체는 자신보다 높은 무결성 수준의 객체에 쓰거나 수정하지 못한다. 이를 **No Write Up**이라고 한다. 낮은 무결성 수준의 주체가 더 신뢰할 수 있어야 하는 데이터를 오염시키지 못하도록 한다.

벨 라파듈라 모델은 기밀성을 보호하기 위해 상위 보안등급 읽기와 하위 보안등급 쓰기를 제한하는 모델이다. 지문의 **무결성 보호와 읽기·쓰기 제한 방향**은 이 모델과 다르다.

래티스 모델은 보안등급 사이의 지배 관계를 격자 구조로 표현하는 일반적인 틀이다. 등급을 계층화한다는 단서만으로는 부족하며, 지문처럼 하향 읽기와 상향 쓰기를 금지하는 무결성 규칙이 구체적인 모델을 가르는 단서이다.

클라크 윌슨 모델도 무결성을 중시하지만, 허용된 변환 절차를 통한 데이터 변경과 직무분리 등을 강조한다. 지문의 등급별 읽기·쓰기 금지 규칙과는 접근 방식이 다르다.

따라서 무결성 수준, 하향 읽기 금지, 상향 쓰기 금지라는 구성 요소를 함께 만족하는 것은 ② **비바 모델**이다.

NoteBase

문 12. 다음 지문은 사회공학을 기반으로 한 공격 중 무엇에 관한 설명인가?

사람들은 바빠서 사무실에 들어갈 때 누가 바짝 따라와 같이 들어가더라도 그 사실을 인지하지 못한다.
핸드폰으로 통화시늉을 하고, 미소를 지으며 문을 잡아 준다. 사무실에 들어가 빈자리를 찾아 AP를 연결하고 외부에 있는 (차량에 탄) 동료의 무선네트워크가 연결되면, 이를 통해 내부네트워크를 해킹할 수 있다.

① Phishing
② Pretexting
③ Tailgating
④ Vishing

정답 3번

간단한 해설

핵심은 **출입 권한이 있는 사람을 바짝 따라 사무실에 들어가는 행동**이다. 사람의 주의 부족이나 호의를 이용해 물리적 출입통제를 우회하는 Tailgating에 해당한다.

NoteBase

구성 요소별 해설

지문의 공격은 사람의 주의 부족과 자연스러운 대인 행동을 이용해 물리적 출입통제를 우회한 뒤, 내부 접근을 정보시스템 침해로 연결하는 구조이다. 공격의 이름을 가르는 핵심은 최초의 출입 방식이다.

동반 진입: 누군가 사무실에 들어갈 때 다른 사람이 바짝 따라 들어오는 부분이 핵심이다. **출입 권한이 있는 사람을 뒤따라 제한구역에 무단으로 들어가는 행위**를 Tailgating이라고 한다. 출입자의 주의 부족이나 문을 열어 주는 관행을 이용한다.

자연스러운 행동을 통한 위장: 통화하는 시늉과 미소는 출입하는 사람이 자신을 수상하게 여기지 않도록 하는 요소이다. 실제 전화 상대를 속여 정보를 얻는 장면은 아니므로, **휴대전화가 등장한다는 이유만으로 Vishing은 아니다**. Vishing은 음성통화를 이용해 정보를 빼내거나 특정 행동을 유도하는 피싱이다.

내부 접근 이후의 침해: 지문의 AP는 무선 접속 지점을 뜻하며, 사무실 안에 들어간 뒤 외부에서 내부망에 접근할 수 있게 하는 데 악용된다. 이는 **물리적 보안 침해가 네트워크 침해로 이어지는 결과**를 보여 준다. AP 연결 자체가 Tailgating의 정의는 아니다.

다른 선택지와의 구별: Phishing은 신뢰할 만한 주체인 것처럼 속이는 메시지나 가짜 사이트 등으로 정보 제공·행동을 유도하는 방식이다. Pretexting은 거짓 신분이나 상황을 꾸며 신뢰를 얻는 방식으로, Tailgating을 돕는 수단으로 결합될 수 있다. 다만 이 지문에서 가장 구체적인 식별 단서는 거짓 사연 자체가 아니라 다른 사람을 따라 출입통제를 통과하는 행동이다.

따라서 지문의 중심 공격은 Tailgating이며, ③에 해당한다.

NoteBase

문 13. 다음 중 리눅스에서 루트(root)가 자신이 소유한 /etc/inetd.conf 파일의 권한을 설정할 때 가장 옳은 것은?

① #chmod 400 /etc/inetd.conf

② #chmod 555 /etc/inetd.conf

③ #chmod 600 /etc/inetd.conf

④ #chmod 777 /etc/inetd.conf

정답 3번

간단한 해설

600은 파일 소유자인 root에게 **읽기·쓰기 권한만 부여**하고 그룹과 기타 사용자에게는 권한을 주지 않으므로, 관리자용 설정 파일의 관리와 보호에 적합하다.

핵심 풀이

/etc/inetd.conf는 inetd가 제공할 네트워크 서비스와 실행할 서버 프로그램 등을 지정하는 설정 파일이다. 관리자에게 필요한 읽기·쓰기 권한을 주되 **그룹과 다른 사용자에게 불필요한 접근 권한을 주지 않는 것**이 핵심이다. 설정 내용을 읽어 사용하는 파일이므로 파일 자체의 실행 권한은 필요하지 않다.

세 자리 숫자 권한은 왼쪽부터 소유자·그룹·기타 사용자를 나타낸다. 각 자리에서 읽기는 4, 쓰기는 2, 실행은 1이며 허용할 권한의 값을 더한다. 따라서 600은 **소유자에게 읽기·쓰기, 그룹과 기타 사용자에게는 권한 없음**을 뜻하며 기호로는 rw-------이다.

400은 소유자의 읽기 비트만 켠 설정이다. 외부 접근을 제한하지만 소유자의 쓰기 비트까지 제거하므로, 관리에 필요한 읽기·쓰기를 함께 명시하는 600과 구별된다. 다만 root의 특권에 따른 접근은 일반 권한 검사와 구별되므로, 400으로 설정하면 root도 절대로 수정할 수 없다고 해석해서는 안 된다.

555는 모든 사용자에게 읽기와 실행을 허용하고 쓰기 비트는 두지 않는다. 설정 파일에 불필요한 실행 권한을 주고 일반 사용자에게 내용도 공개한다. 777은 여기에 **모든 사용자의 쓰기 권한까지 허용**하여 서비스 설정이 임의로 변경될 위험이 있다.

따라서 제시된 명령 중 관리자용 설정 파일을 읽고 수정하면서 다른 사용자의 접근을 제한하는 것은 ③의 chmod 600 /etc/inetd.conf이다.

NoteBase

문 14. 다음은 /etc/shadow 파일의 일부이다. 설명한 내용 중 가장 옳지 않은 것은?

```
pol_admin:!:15964:0:99999:7:0:11323:
police:$5$C7n1nPnI$a6nCwOTqrNR2oDulKirRZ:14684:0:99999:7:::
```

① pol_admin 계정은 패스워드 미설정 상태이다.

② police 계정은 SHA-256 해시 암호 알고리즘을 사용하였다.

③ police 계정은 salt와 패스워드로 암호화된 필드가 있다.

④ /etc/shadow 파일에 사용자 패스워드 최소 길이 필드가 있다.

정답 4번

간단한 해설

/etc/shadow의 최소 사용기간 필드는 비밀번호를 다시 바꿀 수 있을 때까지의 **일수**를 나타낸다. 비밀번호의 **최소 문자 수를 저장하는 필드는 없다**.

NoteBase

선지별 해설

/etc/shadow의 한 행은 콜론으로 구분한 9개 필드로 구성된다. 순서대로 사용자명, 비밀번호 정보, 마지막 변경일, 최소 사용기간, 최대 사용기간, 만료 전 경고기간, 만료 후 비활성기간, 계정 만료일, 예약 필드이다.

① O: 그림에서 pol_admin의 비밀번호 필드는 '!' 하나이며, 사용 가능한 비밀번호 해시가 들어 있지 않다. 따라서 이 보기의 '미설정'은 **인증에 사용할 해시가 없는 상태**라는 의미로 이해한다. 정확히는 '!'가 비밀번호 인증을 잠그므로, 비밀번호 필드가 비어 있는 상태나 비밀번호 없이 로그인할 수 있는 상태와 같지 않다. 이 표시만으로 과거에 비밀번호를 설정한 적이 전혀 없었다고까지 단정하지는 않는다.

② O: police의 비밀번호 필드 앞부분에 있는 **'5'는 SHA-256 기반 crypt 방식**을 지정하는 식별자이다. 단순히 SHA-256을 한 번 적용했다는 뜻은 아니며, salt와 반복 처리를 이용하는 비밀번호 해싱 방식이다. 다만 그림에 적힌 해시 결과 부분은 표준 SHA-256 crypt의 43자보다 짧으므로, 이 예시 문자열 전체가 실제로 유효한 인증용 해시라는 뜻으로 해석해서는 안 된다. 여기서 식별하는 것은 표시된 알고리즘이다.

③ O: police의 두 번째 콜론 구분 필드는 알고리즘 식별자, salt, 비밀번호에서 계산한 해시 결과를 담는 형식이다. salt는 같은 비밀번호라도 서로 다른 결과가 나오도록 해싱에 함께 사용하는 값이다. 보기의 '암호화된 필드'는 이 비밀번호 해시 저장 부분을 가리킨다. **평문 비밀번호를 저장하거나 복호화하여 원문을 되찾는 방식은 아니다**.

④ X: /etc/shadow에는 비밀번호의 최소 문자 수를 정하는 필드가 없다. 그림의 마지막 변경일 다음에 나오는 '0'은 비밀번호를 바꾼 뒤 다시 변경할 때까지 기다려야 하는 **최소 사용기간**을 나타내며 단위는 일이다. 0은 이 대기기간의 제한이 없음을 뜻한다. 최소 길이와 복잡도는 PAM 등 별도의 비밀번호 정책에서 관리한다.

따라서 최소 사용기간을 최소 길이 필드로 잘못 설명한 ④가 가장 옳지 않다.

NoteBase

문 15. 다음 지문에서 설명하고 있는 메모리 보호 기법은?

함수 진입 시 스택에 리턴 주소와 프레임포인터 정보를 저장할 때 정보를 보호하기 위해 특정한 값(Canary)을 기록한다.

① ASLR (Address Space Layout Randomization)
② NX (No-eXecute)
③ SSP (Stack Smashing Protector)
④ Format String

정답 3번

간단한 해설

스택에 Canary를 기록하고 함수 반환 전에 변조 여부를 검사하는 것은 SSP이다. 검사값의 변화를 통해 리턴 주소 등으로 이어지는 스택 손상을 탐지한다.

구성 요소별 해설

보호 대상: 함수 호출 때 스택에 저장되는 리턴 주소는 함수가 끝난 뒤 실행을 이어 갈 위치를 나타내고, 저장된 프레임포인터는 호출한 함수의 스택 프레임 복원에 쓰인다. 스택 버퍼를 넘친 데이터가 이 영역을 덮으면 제어 흐름이 손상될 수 있다.

Canary의 역할: 'SSP'는 보호 대상 함수의 스택에 **Canary라는 검사값을 두고 반환 전에 변조 여부를 확인**한다. 검사값이 바뀌어 있으면 스택 손상을 탐지하여 정상 반환을 중단하고 프로그램을 종료하는 등의 대응을 한다. 리턴 주소를 그대로 신뢰하기 전에 이상을 찾아내는 방식이며, 모든 메모리 오류를 사전에 차단한다는 뜻은 아니다.

ASLR과 NX: 'ASLR'은 스택·힙·라이브러리 등의 배치 주소를 무작위화하여 공격자가 목표 주소를 예측하기 어렵게 한다. 'NX'는 데이터용 메모리 영역에서 명령 실행을 금지하는 방식이다. 각각 **주소 예측 방해와 실행 권한 제한**이 핵심이며, Canary를 기록하고 검사하는 기법과 구별된다.

Format String: 포맷 문자열은 출력 함수 등이 데이터의 해석·출력 형식을 지정하는 문자열이다. 신뢰할 수 없는 입력이 포맷 문자열로 처리되면 정보 노출이나 메모리 변조 취약점이 생길 수 있다. 이 선택지는 Canary 기반 메모리 보호 기법의 이름이 아니다.

따라서 지문에 대응하는 것은 SSP(Stack Smashing Protector)이며, 선택지는 ③이다.

NoteBase

문 16. 다음 지문에서 설명하고 있는 보안 공격 기법은?

알고리즘의 약점을 찾기보다 연산시간 분석, 소비전력, 방출 전자기파, 소리 등을 통해 정보를 추출하는 공격이다.

① 부 채널 공격 (Side Channel Attack)

② 스펙터 (Spectre)

③ 멜트다운 (Meltdown)

④ 고스트다운 (Ghostdown)

정답 1번

간단한 해설

연산시간·전력·전자기파·소리처럼 **장치 동작에 수반되어 새어 나오는 정보**를 분석하는 것이 부 채널 공격이다. 알고리즘 자체의 수학적 약점보다 구현 과정의 정보 누출을 이용한다.

NoteBase

구성 요소별 해설

공격의 공통 원리: **부 채널 공격**은 알고리즘의 수학적 구조 자체를 해독하는 대신, 실제 장치가 연산하면서 외부로 드러내는 부수 정보를 이용해 비밀 정보를 추론한다. 안전한 알고리즘을 사용하더라도 구현 방식에서 정보가 새면 공격이 가능하다.

연산시간: 입력값이나 내부 처리에 따라 걸리는 시간이 달라질 수 있다. 공격자는 이러한 **시간 차이**와 처리 내용의 관계를 분석하여 비밀 정보의 단서를 얻는다.

소비전력: 장치가 수행하는 연산이나 처리하는 데이터에 따라 전력 소비 양상이 달라질 수 있다. 이 차이를 관찰하는 전력 분석도 부 채널 공격에 포함된다.

방출 전자기파: 전자회로의 동작에 따라 외부로 나오는 전자기 신호에 연산 관련 정보가 반영될 수 있다. 그 신호를 분석하여 내부 처리 정보를 추정하는 경우이다.

소리: 장치나 부품이 동작할 때 발생하는 음향 신호에도 처리 상태의 차이가 나타날 수 있다. 이처럼 시간·전력·전자기파·음향은 모두 정상적인 출력값과 별개로 새어 나오는 정보의 통로이다.

스펙터와 멜트다운은 CPU의 실행 방식과 메모리 보호의 허점을 이용하는 구체적인 공격이며, 정보를 알아내는 과정에서 부 채널을 활용한다. 따라서 이들을 부 채널 공격과 완전히 무관한 것으로 보면 안 된다. 다만 지문은 특정 CPU 공격을 한정하지 않고 여러 부수 정보의 이용을 포괄하므로, 설명하는 일반적 범주는 ① **부 채널 공격**이다.

NoteBase

문 17. 다음 중 클라우드에서 제공하는 정보보호 서비스인 SecaaS(Security as a Service)에 대한 설명으로 가장 옳지 않은 것은?

① 보안의 책임을 기업으로부터 보안 서비스 제공자로 이관하게 된다.

② 보안 서비스를 사용한 만큼 비용을 지불하는 방식이다.

③ 클라우드 컴퓨팅의 서비스 모델 중에서 IaaS에 해당된다.

④ 접근 관리, 웹보안, 이메일 보안 등의 서비스를 제공한다.

정답 3번

간단한 해설

SecaaS는 보안 기능을 클라우드 서비스로 제공하는 방식으로, 통상 **SaaS 형태의 보안 서비스**로 이해한다. 서버·저장장치·네트워크 같은 기반 자원을 제공하는 IaaS와는 제공 대상이 다르다.

선지별 해설

SecaaS는 기업이 보안 시스템을 모두 직접 구축·운영하는 대신, 외부 제공자가 운영하는 보안 기능을 서비스로 이용하는 방식이다. 보안 서비스를 소비하는 관점과 그 서비스를 뒷받침하는 인프라는 구별해야 한다.

① O: 위탁한 보안 기능의 구축·운영·관리 책임을 서비스 제공자가 맡는다는 취지이다. 기업의 자체 운영 부담을 줄일 수 있다. 다만 **위탁 범위의 운영 책임을 넘기는 것**이지, 기업의 계정·권한 설정이나 데이터 관리, 서비스 감독 등 모든 보안 책임이 사라지는 것은 아니다.

② O: 보안 장비와 소프트웨어를 직접 구입하는 방식에 비해, **서비스 이용 규모에 따라 비용을 부담**하는 형태로 제공될 수 있다. 처리량·사용자 수·이용 기간 등을 기준으로 한 종량제나 구독형 요금이 대표적이며, 구체적인 과금 기준은 계약에 따라 달라진다.

③ X: IaaS는 가상 서버, 저장공간, 네트워크 등 컴퓨팅 기반 자원을 제공하는 모델이다. SecaaS는 접근관리·악성코드 차단 같은 **보안 기능 자체를 서비스로 제공**하며, 일반적으로 SaaS 형태로 설명된다. 보안 서비스가 내부적으로 IaaS를 이용해 운영될 수 있다는 사실과 이용자에게 IaaS를 제공한다는 것은 다르다.

④ O: 접근관리는 사용자 인증과 권한을 관리하고, 웹보안은 악성 웹 접근이나 웹 기반 위협을 통제하며, 이메일 보안은 스팸·피싱·악성 첨부파일 등을 차단한다. 이들은 모두 **클라우드에서 제공할 수 있는 보안 기능**이다.

NoteBase

문 18. 비트코인과 이더리움 등 가상화폐의 시세가 급등할수록 보안 위협은 증가한다. 이때 해킹으로 블록체인 플랫폼에 커다란 손상이 발생하거나 소프트웨어에 심각한 결함이 발견된다. 이에 신규 기능이 추가된 최신 블록체인 노드를 이전 버전의 블록체인과 호환되지 않도록 업데이트시키는 기술은?

① Hard Fork

② Secure Fork

③ Smart Fork

④ Soft Fork

정답 1번

간단한 해설

기존 합의 규칙과 호환되지 않는 변경은 하드 포크이다. 새 규칙을 따르려는 노드의 업데이트가 필요하며, 구버전에서도 새 블록을 유효하게 받아들일 수 있는 소프트 포크와 구별된다.

개념 구분

결정적 단서: '이전 버전의 블록체인과 호환되지 않도록' 합의 규칙을 바꾸는 업데이트는 **하드 포크(Hard Fork)**이다. 새 규칙에서 유효한 블록이 기존 규칙에서는 무효가 될 수 있어, 구버전 노드는 그대로는 새 규칙의 체인을 받아들일 수 없다. 새 규칙을 따르려는 노드는 업데이트해야 한다.

소프트 포크와의 차이: '소프트 포크(Soft Fork)'는 기존에 허용하던 블록이나 거래의 범위를 더 좁히는 방식의 규칙 변경이다. 새 규칙을 만족하는 블록을 구버전 노드도 기존 기준에서 유효하다고 받아들일 수 있다는 **하위 호환성**이 핵심이다. 다만 구버전 노드가 새 제한 조건까지 직접 검증한다는 뜻은 아니다.

업데이트 목적과 명칭의 구분: 보안 결함 대응과 기능 추가는 업데이트의 목적이며, 하드 포크를 판별하는 기준 자체는 기존 규칙과의 호환 여부이다. 모든 하드 포크가 해킹 뒤에만 발생하거나 반드시 별개의 두 체인을 지속시키는 것은 아니다. Secure Fork와 Smart Fork는 이 문항에서 설명한 비호환적 합의 규칙 변경을 지칭하는 표준 분류명이 아니다.

따라서 지문의 비호환 업데이트에 해당하는 선택지는 ① Hard Fork이다.

NoteBase

문 19. 다음 중 TCP와 UDP에 대한 설명으로 가장 옳지 않은 것은?

① TCP와 UDP는 전송 계층(Transport layer)에 해당하는 프로토콜이다.

② TCP는 가상 회선 방식이며, UDP는 데이터그램 방식으로 동작한다.

③ TCP는 전송 순서를 보장하며, UDP에 비해 높은 신뢰성을 갖고 있다.

④ TCP는 연결 지향적이며, UDP에 비해 상대적으로 전송 속도가 빠르다.

정답 4번

간단한 해설

TCP는 신뢰성 있는 전달을 위해 연결 설정·확인응답·재전송 등의 처리를 수행한다. 따라서 **연결 지향적이므로 UDP보다 빠르다는 설명**은 타당하지 않으며, 일반적인 처리 부담은 UDP가 더 작다.

선지별 해설

① O: TCP와 UDP는 모두 **전송 계층** 프로토콜로, 포트 번호를 이용하여 종단 호스트의 응용프로그램 사이에 데이터를 전달한다. IP가 호스트 사이의 패킷 전달을 담당하는 것과 구분된다.

② O: TCP는 양쪽 종단이 연결 상태를 유지하며 데이터를 교환하는 **논리적인 가상 회선** 서비스를 제공한다. 여기서 가상 회선은 고정된 물리 경로나 대역폭을 미리 예약한다는 뜻이 아니다. UDP는 연결 설정 절차 없이 개별 메시지를 데이터그램 단위로 보내는 비연결형 방식이다.

③ O: TCP는 순서 번호로 데이터를 재정렬하고, 확인응답과 필요한 재전송을 통해 손실·중복 등에 대응하여 응용프로그램에 **순서 있는 바이트 스트림**을 제공한다. UDP 자체는 도착 순서나 전달 성공을 보장하지 않으므로, 전송 계층이 제공하는 신뢰성은 TCP가 더 높다. UDP 위의 응용프로그램이 별도로 신뢰성 기능을 구현할 수 있다는 점은 이 구분과 별개이다.

④ X: TCP가 연결 지향적이라는 부분은 옳지만, 그 때문에 UDP보다 상대적으로 빠르다고 한 부분이 잘못되었다. TCP에는 연결 설정, 확인응답, 재전송, 흐름·혼잡 제어 등의 부가처리가 있으므로, 이러한 기능이 없는 UDP가 일반적으로 **프로토콜 처리 부담이 작고 지연을 줄이기 쉽다**. 다만 실제 전송률과 소요시간은 망 상태·손실·응용프로그램 구현 등에 따라 달라지므로 UDP가 언제나 더 빠르다는 절대 법칙으로 바꾸어 이해해서도 안 된다.

따라서 연결 지향성과 전송 속도의 관계를 잘못 설명한 ④가 가장 옳지 않다.

NoteBase

문 20. 다음 중 OSI 7계층에 대한 설명으로 가장 옳지 않은 것은?

① 물리 계층은 장치들 간의 물리적인 접속과 비트 정보를 다른 시스템에 전송하는 데 필요한 규칙을 정의하며, 이 계층에서 다루는 데이터를 비트스트림(Bit Stream)이라고 한다.

② 데이터 링크 계층은 통신 경로상의 지점간(link-to-link) 회선 제어, 흐름 제어, 오류 제어를 담당하며, 이 계층에서 다루는 데이터를 프레임(Frame)라고 한다.

③ 네트워크 계층은 두 사용자 사이의 신뢰성 있는 데이터 전송을 위한 종단간(end-to-end) 제어를 담당하며, 이 계층에서 다루는 데이터를 세그먼트(Segment)라고 한다.

④ 세션 계층은 두 응용프로그램 간의 연결설정, 이용 및 연결 해제 등 대화를 유지하기 위한 구조를 제공하며, 이 계층에서 다루는 데이터를 메시지(Message)라고 한다.

정답 3번

간단한 해설

신뢰성 있는 **종단간 제어와 세그먼트는 전송 계층**에 해당한다. 네트워크 계층은 논리 주소에 따른 경로 선택과 패킷 전달을 담당하므로 두 계층을 구별해야 한다.

선지별 해설

① O: 물리 계층은 전압·신호·전송 매체와 접속 규격 등 비트 전송에 필요한 물리적 조건을 정의한다. 이 계층은 상위 계층 데이터의 의미를 해석하기보다 **연속된 비트를 신호로 전달**하므로, 다루는 데이터를 비트 또는 비트스트림으로 표현한다.

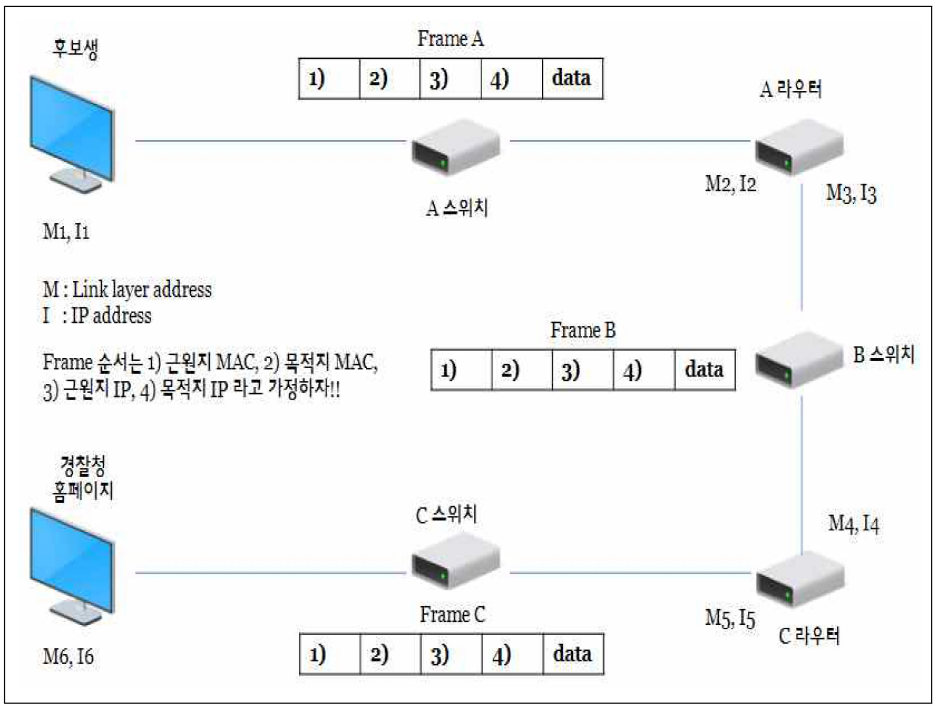
② O: 데이터 링크 계층은 하나의 링크로 연결된 인접 지점 사이에서 데이터를 프레임 단위로 주고받도록 한다. 프레임의 경계와 전송 절차를 정하고 링크 수준의 흐름 제어·오류 제어 등을 제공한다. 제어 범위가 **인접 지점 사이의 링크**라는 점에서 전송 계층의 종단간 제어와 구별된다.

③ X: 신뢰성 있는 전송을 위한 종단간 제어와 세그먼트는 **전송 계층**의 설명이다. 예를 들어 TCP는 종단 사이에서 순서·재전송·흐름 제어를 수행하고 세그먼트를 사용한다. 네트워크 계층은 논리 주소와 경로 선택을 바탕으로 서로 다른 네트워크 사이에 데이터를 전달하며, 그 데이터 단위는 일반적으로 **패킷**이라고 한다.

④ O: 세션 계층은 응용프로그램 사이의 대화를 설정·유지·종료하고, 대화 진행과 동기화 등을 관리할 수 있는 구조를 제공한다. 핵심은 **응용프로그램 간 대화의 관리**이다. 이 문항의 일반적인 계층별 데이터 단위 구분에서는 세션 계층을 포함한 상위 계층의 데이터를 메시지로 표현한다.

NoteBase

문 21. 간부후보생이 경찰청 홈페이지에 접속하여 정보를 검색할 때, 후보생의 요청정보가 홈페이지 서버에 전달된다. 이때 각 스위치 구간(A, B, C 스위치)에서 해커가 볼 수 있는 프레임의 네트워크 정보를 맞게 설명한 것은? (단, 후보생이 경찰청 홈페이지로 요청하는 정보만을 가정한다.)



① A스위치: M1,M2,I1,I6 B스위치: M3,M4,I1,I6 C스위치:M5,M6,I1,I6

② A스위치: M1,M2,I1,I2 B스위치: M3,M4,I3,I4 C스위치:M5,M6,I5,I6

③ A스위치: M1,M3,I1,I6 B스위치: M3,M5,I1,I6 C스위치:M5,M6,I1,I6

④ A스위치: M1,M3,I1,I2 B스위치: M3,M5,I3,I4 C스위치:M5,M6,I5,I6

정답 1번

간단한 해설

라우터를 지날 때 **MAC 주소는 다음 링크에 맞게 바뀌고**, 요청 패킷의 **출발지·목적지 IP는 I1·I6으로 유지**된다. 따라서 각 구간은 M1·M2, M3·M4, M5·M6의 MAC 주소 쌍을 사용한다.

NoteBase

도식 해설

그림에서 M은 링크 계층 주소인 MAC 주소이고 I는 IP 주소이다. 문항이 정한 순서에 따라 각 프레임을 **출발지 MAC, 목적지 MAC, 출발지 IP, 목적지 IP**로 읽는다. 요청은 후보생에서 홈페이지 서버로 가므로 최종 출발지와 목적지는 각각 I1과 I6이다.

주소가 바뀌는 기준: 라우터는 들어온 링크 계층 프레임을 벗기고, 다음 구간에 맞는 새 프레임에 IP 패킷을 담아 전달한다. 따라서 **MAC 주소는 구간마다 바뀌지만, 출발지·목적지 IP 주소는 I1·I6으로 유지**된다. 이는 그림에 제시된 일반적인 라우팅 경로를 기준으로 하며 별도의 주소 변환은 가정하지 않는다. IP 주소가 유지된다는 것이 TTL 등 IP 헤더의 모든 값까지 그대로라는 뜻은 아니다.

A 스위치 구간: 후보생의 MAC 주소는 M1이고, 같은 링크에서 다음으로 받을 A 라우터의 인터페이스 주소는 M2이다. 따라서 프레임 A의 네 주소는 **M1, M2, I1, I6**이다.

B 스위치 구간: A 라우터의 출력 인터페이스는 M3이고, 다음 라우터의 입력 인터페이스는 M4이다. 따라서 프레임 B의 네 주소는 **M3, M4, I1, I6**이다. I3·I4는 중간 라우터 인터페이스의 주소이지 이 요청 패킷의 양 끝 IP 주소가 아니다.

C 스위치 구간: 마지막 라우터의 출력 인터페이스는 M5이고, 최종 홈페이지 서버의 MAC 주소는 M6이다. 따라서 프레임 C의 네 주소는 **M5, M6, I1, I6**이다.

세 구간의 MAC 주소는 각각 M1·M2, M3·M4, M5·M6이고 IP 주소는 모두 I1·I6이므로 ①과 일치한다. 라우터를 넘어 다음 구간까지 최초 출발지 MAC 주소를 유지하거나, 목적지 IP를 매번 다음 라우터의 주소로 바꾸는 해석은 잘못이다.

NoteBase

문 22. 다음 중 인터넷 프로토콜과 그 용도가 올바르게 짝지어진 것은?

① CIDR : 혼잡 제어를 통해 신뢰성 있는 순차적 메시지 전송에 사용

② FTP : IP 주소를 물리적 네트워크 주소로 대응시키는 데 사용

③ ICMP : 호스트와 인접 라우터가 멀티캐스트 멤버십을 구성하는 데 사용

④ SNMP : IP 네트워크 상의 장치 정보를 수집하고 관리하는 데 사용

정답 4번

간단한 해설

SNMP는 관리 대상 장비의 상태와 성능 같은 정보를 수집하고 관리하는 프로토콜이다. 따라서 **SNMP와 장치 정보 수집·관리**를 연결한 ④가 옳다.

선지별 해설

① X: 'CIDR'는 주소를 고정된 클래스 경계로 나누지 않고 접두부 길이에 따라 할당·집계하는 **클래스 없는 주소 및 라우팅 방식**이다. 혼잡 제어와 신뢰성 있는 순서 보장 전송은 TCP의 기능에 해당한다. 엄밀히 말해 TCP는 메시지 경계를 보존하는 방식이 아니라 바이트 스트림을 전달한다.

② X: 'FTP'는 클라이언트와 서버 사이의 **파일 전송**에 사용한다. 로컬 네트워크에서 IPv4 주소에 대응하는 MAC 주소 등의 링크 계층 주소를 알아내는 프로토콜은 ARP이다. 따라서 제시한 용도와 FTP의 연결이 잘못되었다.

③ X: IPv4에서 호스트의 멀티캐스트 그룹 가입 상태를 인접 라우터에 알리고 관리하는 프로토콜은 **IGMP**이다. 'ICMP'는 목적지 도달 불가·시간 초과 같은 오류 정보를 전달하거나 Echo 메시지로 통신 상태를 진단하는 데 쓰인다. IPv6의 멀티캐스트 수신자 관리는 ICMPv6 기반 MLD를 사용하지만, 이는 이 선지의 일반적인 IPv4 ICMP 설명과 구별된다.

④ O: 'SNMP'는 네트워크 장비의 관리 정보를 조회하고 필요한 설정을 제어하는 네트워크 관리 프로토콜이다. 관리자는 장비의 에이전트가 제공하는 정보를 이용해 상태·성능·장애 등을 파악하므로, **장치 정보의 수집과 관리**라는 용도에 부합한다.

NoteBase

문 23. 다음 중 ARP 스푸핑(Spoofing)을 이용한 스니핑(sniffing) 공격에 대한 대응책으로 가장 옳지 않은 것은?

① 공격자가 내용을 알 수 없도록 데이터를 암호화하여 전송한다.

② ARP테이블을 동적으로 설정하여 융통성 있게 관리한다.

③ 주기적으로 무차별(promiscuous) 모드로 동작하는 기기가 있는지 검사한다.

④ 스위치 각 포트에 대해 접근 제한(Port Security)을 설정한다.

정답 2번

간단한 해설

ARP 스푸핑은 거짓 ARP 정보로 **IP 주소와 MAC 주소의 대응 관계를 오염**시킨다. ARP 테이블을 동적으로 갱신하게 두는 것만으로는 이를 막을 수 없으며, 중요한 대응 관계의 정적 등록이나 ARP 정보 검증이 필요하다.

선지별 해설

ARP 스푸핑을 이용한 스니핑은 단말이 잘못된 MAC 주소로 통신하도록 유도하여 공격자가 트래픽을 엿보는 공격이다. 대응은 주소 대응 관계의 보호, 비인가 기기 제한, 이상 징후 탐지, 유출 내용의 보호를 함께 고려한다.

① O: 적절한 통신 암호화는 공격자가 패킷을 수집하더라도 **통신 내용을 해독하기 어렵게** 만든다. 상대 인증이 결합된 안전한 암호화 통신을 사용해야 한다. 이는 도청 피해를 줄이는 방법이며, ARP 테이블의 오염 자체를 직접 차단하는 것과는 다르다.

② X: 동적 ARP 테이블은 수신한 ARP 정보에 따라 대응 관계를 자동 갱신한다. 이를 단순히 동적으로 설정하는 것은 거짓 정보를 구별하는 대책이 아니다. 중요한 IP·MAC 대응 관계를 **정적으로 등록**하거나, 스위치에서 신뢰할 수 있는 바인딩 정보와 ARP 패킷을 대조하는 검증 기능을 활용해야 한다.

③ O: 무차별 모드는 일반적인 목적지 MAC 주소 필터링을 완화하여 네트워크 인터페이스가 받은 여러 프레임을 처리하도록 한다. 이를 비정상적으로 사용하는 기기를 점검하면 **스니핑 의심 징후를 탐지**하는 데 도움이 된다. 다만 정상적인 분석 도구도 이 모드를 사용할 수 있고, ARP 스푸핑으로 자신에게 전달되도록 만든 프레임은 무차별 모드 없이도 수신할 수 있으므로 이 검사만으로 공격을 모두 찾을 수는 없다.

④ O: Port Security는 포트에서 허용하는 MAC 주소나 그 개수를 제한하여 **비인가 기기의 네트워크 연결**을 줄이는 데 도움이 된다. 다만 허용된 MAC 주소를 사용하는 기기의 거짓 ARP 정보까지 모두 검증하는 기능은 아니므로, ARP 패킷 검증 등과 함께 사용해야 한다.

NoteBase

문 24. 다음 중 세션 하이재킹(Session Hijacking) 공격을 방어하는 수단으로 가장 옳지 않은 것은?

① 동기화 상태 탐지

② ACK Storm 탐지

③ 데이터 암호화

④ MAC 주소 고정

정답 1번

간단한 해설

전통적인 TCP 세션 하이재킹의 탐지에서는 정상 동기화가 아니라 순서 번호와 확인응답 관계가 어긋나는 **비동기화 상태**가 중요한 단서이다. ACK Storm은 이러한 비동기화에 수반될 수 있는 이상 징후이다.

NoteBase

선지별 해설

세션 하이재킹은 이미 성립한 통신을 가로채 상대방을 사칭하거나 데이터를 끼워 넣는 공격이다. 이 문항의 동기화 상태와 ACK Storm은 전통적인 TCP 세션 하이재킹에서 관찰하는 징후를 가리킨다.

① X: TCP 통신이 정상적으로 동기화되어 있다는 사실 자체는 공격 징후가 아니다. 이 공격의 탐지에서 주목하는 것은 양쪽 종단이 관리하는 순서 번호와 확인응답 번호가 어긋나는 **비동기화 상태**이다. 따라서 방어수단으로 제시해야 할 표현은 '동기화 상태 탐지'가 아니라 '비동기화 등 비정상 상태 탐지'이다.

② O: 비동기화된 양쪽 종단이 상대의 패킷을 정상적인 순서로 받아들이지 못하고 확인응답을 반복하면 ACK 패킷이 급증하는 **ACK Storm**이 나타날 수 있다. 이러한 비정상 트래픽을 감시하면 공격 의심 세션을 찾아 대응할 수 있다. 다만 모든 세션 하이재킹에서 반드시 발생하는 현상은 아니므로, 탐지만으로 모든 공격을 차단한다고 볼 수는 없다.

③ O: TLS나 SSH처럼 통신 내용을 암호화하고 상대 인증과 무결성 검증을 제공하는 방식을 사용하면, 공격자가 내용을 읽거나 유효한 데이터를 위조하여 세션에 끼워 넣기 어려워진다. 이때 중요한 것은 **암호화와 함께 인증·무결성을 보장하는 것**이다. 암호화만으로 단말 감염이나 이미 유출된 세션 식별자의 모든 악용까지 해결되는 것은 아니다.

④ O: 같은 LAN에서 정당한 상대의 IP 주소와 MAC 주소 대응을 정적 ARP 항목 등으로 고정하면, 거짓 ARP 응답으로 트래픽을 공격자 쪽으로 유도하는 행위를 줄일 수 있다. 이는 **ARP 스푸핑을 이용한 가로채기 경로**를 막는 보조 수단이다. 단순히 자기 장치의 MAC 주소를 바꾸지 않는다는 뜻은 아니며, 모든 경로의 세션 탈취를 막는 일반적인 인증 수단도 아니다.

따라서 탐지해야 할 비정상 상태를 '동기화 상태'로 잘못 제시한 ①이 가장 옳지 않다.

NoteBase

문 25. 다음 중 취약점 분석을 위해 사용하는 nmap의 사용법과 그에 대한 설명으로 가장 옳지 않은 것은?

① nmap -sU -p 53 192.168.xxx.xxx : 192.168.xxx.xxx의 53번 포트에 대한 UDP 스캔을 수행한다.

② nmap -sP 192.168.xxx.xxx : 192.168.xxx.xxx의 활성화 여부를 ping을 통해 검사한다.

③ nmap -sR -p 1-4000 192.168.xxx.xxx : 192.168.xxx.xxx의 1번 포트부터 4000번 포트까지 RPC 포트를 검색하여 보여준다.

④ nmap -sT -p 4000- 192.168.xxx.xxx : 192.168.xxx.xxx의 4000번 이하의 포트들에 대해 TCP Connect 스캔을 수행한다.

정답 4번

간단한 해설

-p 4000-은 끝 포트 번호가 생략된 범위로, **4000번부터 65535번까지**를 뜻한다. 따라서 4000번 이하를 검사한다는 설명은 범위의 방향을 반대로 해석한 것이다.

선지별 해설

① O: -sU는 **UDP 스캔**을, -p 53은 검사할 포트를 53번으로 지정한다. 따라서 해당 주소의 UDP 53번 포트 상태를 조사하는 명령이다. 포트 번호가 같더라도 TCP와 UDP의 포트는 구분된다.

② O: -sP는 호스트가 응답하는지 확인하는 **호스트 탐색, 즉 ping 스캔**의 예전 옵션 이름이다. 현재의 -sn에 해당하며 일반적인 포트 스캔은 수행하지 않는다. 여기서 ping은 호스트 탐색을 넓게 부르는 말로, 환경에 따라 ICMP뿐 아니라 TCP 탐색 패킷이나 ARP 등을 사용할 수 있다.

③ O: -p 1-4000은 검사 범위를 1번부터 4000번까지로 한정한다. -sR은 원래 **RPC 서비스 탐지**를 지정하던 옵션으로, 응답을 통해 RPC 프로그램과 버전 등을 식별한다. 이후 -sV의 별칭으로 통합되어 일반 서비스·버전 탐지에 RPC 탐지가 포함되므로, RPC 포트를 찾아 보여준다는 설명은 성립한다.

④ X: -sT가 TCP Connect 스캔을 뜻한다는 부분은 맞지만, -p 4000-의 범위를 반대로 설명하였다. 하이픈 뒤의 끝값을 생략하면 최대 포트 번호까지를 뜻하므로 실제 범위는 **4000번부터 65535번까지**이다. 1번부터 4000번까지 지정하려면 -p 1-4000 또는 -p -4000으로 표현한다.

NoteBase

문 26. 다음 중 IPSec에 대한 설명으로 가장 옳지 않은 것은?

① IPSec 운영 모드 중 터널 모드는 종단 노드(end point) 구간에서 사용되며 전체 IP패킷을 보호하지 않는다.

② AH(Authentication Header) 프로토콜은 발신지 호스트를 인증하고 IP패킷으로 전달되는 페이로드의 무결성을 보장하기 위해 설계되었다.

③ ESP(Encapsulating Security Payload)는 발신지 인증, 무결성, 프라이버시를 제공하는 프로토콜이다.

④ IPSec은 IP 계층의 보안을 위해 IETF에 의해 제안되었으며, VPN 구현에 사용되고 있다.

정답 1번

간단한 해설

터널 모드는 **원래 IP 헤더와 페이로드 전체를 내부 패킷으로 보호**하고 새 외부 IP 헤더를 붙인다. 따라서 전체 IP 패킷을 보호하지 않는다는 ①의 설명이 틀리다.

선지별 해설

① X: **터널 모드는 원래 IP 헤더를 포함한 전체 IP 패킷을 내부 패킷으로 캡슐화하여 보호**하고, 전송을 위한 새 외부 IP 헤더를 붙인다. 종단 호스트 사이에서 원래 IP 헤더를 유지하고 주로 상위 계층 데이터를 보호하는 설명은 전송 모드에 가깝다. 터널 모드는 보안 게이트웨이 간 또는 호스트와 게이트웨이 간 VPN에서 흔히 쓰이지만 호스트 간에도 사용할 수 있으므로, 종단 노드라는 표현만으로 불가능하다고 판단하지 않는다. 명백한 오류는 터널 모드가 전체 원래 IP 패킷을 보호하지 않는다는 부분이다.

② O: 'AH'는 전달 데이터의 **무결성과 데이터 발신지 인증**을 제공한다. IP 페이로드뿐 아니라 전송 중 변하지 않거나 수신 시 값을 예측할 수 있는 IP 헤더 부분도 인증 범위에 포함한다. TTL처럼 경로에서 바뀌는 필드를 그대로 인증하는 것은 아니며, AH 자체는 암호화에 의한 기밀성을 제공하지 않는다.

③ O: 'ESP'는 암호화를 통한 기밀성과 데이터 발신지 인증·무결성 서비스를 제공할 수 있다. 선지의 프라이버시는 여기서 내용이 노출되지 않도록 하는 기밀성을 뜻한다. 실제로 적용되는 서비스는 보안 연관 설정과 선택한 알고리즘에 따르므로, ESP를 쓰면 언제나 모든 서비스가 자동으로 활성화된다는 뜻은 아니다.

④ O: 'IPSec'은 IETF가 표준화한 **IP 계층 보안 프로토콜 체계**이다. AH·ESP 등을 이용해 IP 통신을 보호하며, 공용망 위에서 사설망 간 또는 원격 사용자와 사설망 간 통신을 보호하는 VPN 구현에 사용된다.

NoteBase

문 27. 다음 중 PGP(Pretty Good Privacy) 프로토콜에 대한 설명으로 가장 옳지 않은 것은?

① 안전한 전자 우편 송수신을 위해 Phil Zimmermann에 의해 제안되었다.

② 제3자의 개입 없이 수신자에 대한 인증과 부인방지 기능을 제공한다.

③ 하나의 파일을 여러 개의 파일로 분할하는 기능을 제공한다.

④ 별도의 인증기관은 필요 없으며, 키 링(Key ring)을 이용하여 공개키를 인증한다.

정답 2번

간단한 해설

PGP의 전자서명은 **송신자의 개인키로 생성**하고 송신자의 공개키로 검증하므로, 인증과 송신 부인방지의 대상은 송신자이다. 이를 **수신자에 대한 기능이라고 한 부분**이 잘못이다.

선지별 해설

① O: **PGP**는 Phil Zimmermann이 개발한 전자우편·파일 보안 방식이다. 공개키 암호, 대칭키 암호, 해시와 전자서명 등을 결합하여 기밀성, 메시지 인증과 무결성 등의 보안 기능을 제공한다.

② X: PGP에서 송신자는 자신의 개인키로 메시지에 전자서명을 하고, 수신자는 송신자의 공개키로 이를 검증한다. 따라서 전자서명이 제공하는 것은 **송신자 인증과 송신 부인방지**이지 수신자의 수신 사실에 대한 부인방지가 아니다. 부인방지는 서명키의 정당한 소유 관계와 안전한 개인키 관리 등을 전제로 한다. 수신자의 공개키로 세션키를 암호화하는 기능은 수신자만 내용을 복호화하도록 하는 기밀성 기능이므로 전자서명의 인증 대상과 구별해야 한다.

③ O: 전통적인 PGP는 전송 환경의 메시지 크기 제한 등을 고려하여 큰 메시지나 파일의 전송 표현을 **여러 부분으로 분할하고 다시 결합**할 수 있도록 한다. 이 분할 기능은 암호 알고리즘이 메시지를 내부 블록으로 나누는 것과 구별되는 전송상의 기능이다.

④ O: PGP는 중앙의 인증기관을 반드시 두는 방식이 아니라 사용자가 키를 보관·관리하고 신뢰 관계를 판단하는 **신뢰망** 방식을 사용할 수 있다. 키 링에는 공개키와 관련 인증 서명 등의 정보가 저장되며, 직접 확인한 키나 신뢰하는 사람의 서명을 바탕으로 공개키와 소유자의 연결을 확인한다. 단순히 키 링에 저장했다는 사실만으로 그 키가 자동 인증되는 것은 아니다.

NoteBase

문 28. 다음 중 HTTP 프로토콜에서 요청 메시지에 적합한 인증 부족(Unauthorized)이라는 클라이언트 오류를 의미하는 상태 코드는?

① 200

② 301

③ 401

④ 503

정답 3번

간단한 해설

'Unauthorized'의 핵심은 요청한 자원에 필요한 **유효한 인증정보가 없다는 것**이다. 성공·리다이렉션·서버 장애가 아니라 클라이언트 인증과 관련된 4xx 응답으로 구분한다.

개념 구분

HTTP 상태 코드는 첫 자리로 응답의 종류를 구분한다. 2xx는 성공, 3xx는 리다이렉션, 4xx는 클라이언트 오류, 5xx는 서버 오류이다. 이 문제는 4xx 중에서도 유효한 인증정보가 부족한 경우를 찾는다.

200 OK: 요청이 성공적으로 처리되었음을 나타낸다. **성공 응답**이므로 인증 부족 오류와 구별된다.

301 Moved Permanently: 요청한 자원이 새로운 위치로 영구 이동했음을 나타낸다. **영구 리다이렉션** 응답이며, 보통 Location 헤더로 새 위치를 안내한다.

401 Unauthorized: 요청한 자원에 접근하는 데 필요한 **유효한 인증정보가 없는 경우**이다. 서버는 WWW-Authenticate 헤더로 인증에 필요한 요구사항을 제시한다. 단순히 요청 수행을 거부하는 403 Forbidden과 구별하며, 코드의 영문 명칭만 보고 일반적인 권한 부족으로만 해석하지 않는다.

503 Service Unavailable: 서버가 일시적인 과부하나 유지보수 등으로 요청을 처리할 수 없는 경우이다. **서버 측의 일시적인 서비스 불가**를 나타내므로 클라이언트 인증 부족과 다르다.

따라서 인증정보 부족을 뜻하는 상태 코드는 401이며, ③에 해당한다.

NoteBase

문 29. 다음 중 SSL/TLS 설명으로 가장 옳지 않은 것은?

① SSL은 TLS 이전 버전이며, 현재 릴리즈 버전은 TLS 1.4이다.

② HTTPS, SMTPS, FTPS는 TLS를 지원한다.

③ TLS 통신은 대칭키와 비대칭키 암호를 사용한다.

④ 브라우저 벤더들의 경우, 2020년까지 TLS 1.0/1.1 지원을 중단할 예정이다.

정답 1번

간단한 해설

출제 당시 최신 TLS 표준은 **TLS 1.4가 아니라 TLS 1.3**이었다. SSL이 TLS의 전신이라는 부분은 맞지만, 버전 번호를 잘못 제시한 ①이 옳지 않다.

선지별 해설

① X: SSL은 TLS의 전신이며, TLS는 SSL을 계승해 표준화한 보안 프로토콜이다. 이 문항의 출제 당시 최신 표준 버전은 **TLS 1.3**으로, 2018년에 표준화되었다. 따라서 'TLS 1.4'라는 버전 설명이 틀리다. 선지의 '현재'는 당시 기준으로 이해한다.

② O: HTTPS는 HTTP 통신을 TLS로 보호한다. SMTPS와 FTPS 역시 각각 메일 전송과 파일 전송에 SSL/TLS 보안 계층을 적용하는 방식이므로 TLS를 지원한다. FTPS는 SSH 기반 파일 전송 방식인 SFTP와는 다른 개념이다.

③ O: 인증서 기반의 일반적인 TLS 통신은 **비대칭키 기법으로 인증·키 합의를 수행하고, 대칭키로 실제 데이터를 보호**하는 혼합 구조를 사용한다. 공개키 연산은 안전한 통신 관계를 설정하는 데 쓰이고, 효율적인 대칭키 암호는 본문 데이터 처리에 쓰인다. 다만 사전 공유키 방식도 있으므로 모든 TLS 연결이 반드시 인증서나 비대칭키 연산을 사용한다는 절대적 의미는 아니다.

④ O: 이 선지는 당시 브라우저 업체들이 발표한 **2020년경 TLS 1.0·1.1 지원 중단 계획**을 설명한다. 주요 업체들은 2018년에 이 계획을 공표하여 TLS 1.2 이상으로의 전환을 유도했다. 원문의 '예정'은 발표된 계획에 관한 표현이며, 모든 제품에서 동일한 날짜에 실제 지원 제거가 완료되었다는 진술이나 지금도 미래의 일정이라는 뜻으로 읽지 않는다.

NoteBase

문 30. 소프트웨어 보안 취약점 유형 중, 입력값 검증 누락, 잘못된 검증으로 인해 발생할 수 있는 취약점으로 가장 옳지 않은 것은?

① 레이스 컨디션(Race Condition)

② 크로스 사이트 스크립팅(Cross Site Scripting)

③ SQL 삽입(SQL Injection)

④ 크로스 사이트 요청 위조(Cross Site Request Forgery)

정답 1번

간단한 해설

레이스 컨디션은 입력 문자의 형식보다 공유자원에 접근하는 **시점·순서·동기화**가 핵심인 취약점이다. 검사와 사용 사이에 상태가 바뀌는 문제 등을 다루므로 '시간 및 상태' 범주로 분류한다.

NoteBase

선지별 해설

이 문항은 소프트웨어 보안약점의 '입력데이터 검증 및 표현' 범주에 해당하는지를 묻는다. 이 범주는 외부 데이터의 내용·형식뿐 아니라 출력 시 해석 방식과 요청의 정당성 검증도 함께 다룬다.

① X: 레이스 컨디션은 여러 실행 흐름이 공유자원에 접근할 때 **실행 순서와 동기화를 적절히 제어하지 못해** 결과가 달라지는 문제이다. 예를 들어 파일을 검사한 뒤 실제 사용하기 전 다른 실행 흐름이 그 파일의 상태를 바꾸면, 검사 당시의 안전성이 사용 시점에는 유지되지 않을 수 있다. 이는 대표적으로 '시간 및 상태' 범주에 해당한다. 입력값을 한 번 검사하는 것만으로 해결되지 않으며, 잠금이나 원자적 처리 등으로 검사·사용 사이의 상태를 보호해야 한다.

② O: 크로스 사이트 스크립팅(XSS)은 신뢰할 수 없는 데이터가 웹 문서에 안전하지 않게 포함되어 **피해자의 브라우저에서 코드로 실행**되는 문제이다. 입력을 적절히 검증하지 않거나 출력 위치에 맞게 인코딩하지 않으면 발생할 수 있으므로 입력데이터 검증 및 표현 범주에 해당한다. 단순한 금지 문자열 검사만으로 충분하지 않으며, HTML·속성·스크립트 등 출력 문맥에 맞는 안전한 처리가 중요하다.

③ O: SQL 삽입은 외부 입력을 SQL 문장에 직접 결합하여 **데이터가 SQL 명령의 일부로 해석**되면서 발생한다. 공격자가 조회 조건이나 실행할 명령의 의미를 바꿀 수 있으므로 입력데이터 검증 및 표현 범주에 해당한다. 매개변수화된 질의로 SQL 구조와 입력 데이터를 분리하고, 입력값의 허용 범위도 검증해야 한다.

④ O: 크로스 사이트 요청 위조(CSRF)는 사용자의 브라우저가 기존 인증정보를 포함해 보낸 요청을 서버가 사용자의 정당한 의사에 따른 요청인지 확인하지 못하여, 원하지 않는 동작을 수행하는 문제이다. 이 분류에서는 **요청의 정당성 검증 누락**과 관련된 입력데이터 검증 및 표현 약점으로 다룬다. CSRF 토큰이나 요청 출처 등을 서버에서 검증해야 하며, 입력 문자의 형태만 검사하거나 로그인이 되어 있는지만 확인하는 것으로는 충분하지 않다.

따라서 주된 원인이 시간·상태·동기화 관리에 있는 ① 레이스 컨디션이 질문의 범주에 가장 적합하지 않다.

NoteBase

문 31. 다음 중 전자 상거래를 위한 SET(Secure Electronic Transaction)에 대한 설명으로 가장 옳지 않은 것은?

① SET은 전자 지갑이라는 개념없이 간편한 전자 상거래를 지원한다.

② 인증기관(CA)은 참여자들의 신원을 확인하고 인증서를 발급한다.

③ SET은 이중 서명(dual signature) 방식으로 은닉 서명을 지원한다.

④ SET은 대칭키 및 공개키 방식의 암호화 알고리즘을 모두 사용한다.

정답 1번

간단한 해설

SET은 **전자 지갑 소프트웨어를 이용해** 구매자의 카드 결제를 처리한다. 따라서 '전자 지갑이라는 개념없이' 전자 상거래를 지원한다는 설명은 SET의 구성과 맞지 않는다.

선지별 해설

① X: SET에서 구매자는 **전자 지갑 소프트웨어**를 사용한다. 이 소프트웨어는 결제에 필요한 정보를 관리하고, 전자서명과 암호화 등으로 SET 결제 메시지를 생성한다. 따라서 '전자 지갑이라는 개념없이'라는 부분은 '전자 지갑 소프트웨어를 이용하여'로 고쳐야 한다.

② O: 인증기관(CA)은 인증서 발급에 앞서 참여자의 신원을 확인하고, 그 참여자와 공개키의 관계를 증명하는 인증서를 발급한다. 거래 상대방은 신뢰하는 CA의 서명을 검증하여 **공개키가 누구의 것인지** 확인할 수 있다.

③ O: 여기서 '은닉'은 **수신자별로 불필요한 거래정보를 숨긴다**는 의미로 이해한다. SET은 주문정보와 지불정보 각각의 해시값을 결합한 뒤 다시 해시하여 구매자의 개인키로 서명하는 이중 서명을 사용한다. 암호화와 이중 서명을 결합하여 판매자는 지불정보의 내용을, 지급결제기관은 주문정보의 내용을 알지 못하면서도 두 정보의 연결 관계를 검증할 수 있게 한다. 다만 이는 서명자에게 메시지 내용을 숨긴 채 서명을 받는 은닉서명(Blind Signature)과는 구별해야 한다.

④ O: SET은 **대칭키 암호와 공개키 암호를 함께** 사용한다. 지불정보는 대칭키로 암호화하고, 그 대칭키는 지급결제기관의 공개키로 암호화하여 전달한다. 지급결제기관은 자신의 개인키로 대칭키를 복구한 다음 지불정보를 복호화한다.

NoteBase

문 32. 다음 지문에서 설명하고 있는 전자 입찰 시스템의 요구사항은?

각 입찰 참여자 간의 공모를 방지하여야 하며, 입찰 공고자와 서버의 독단이 발생하지 않도록 한다.

① 비밀성
② 무결성
③ 공평성
④ 안전성

정답 4번

간단한 해설

입찰 참여자의 **공모를 방지**하고 입찰 공고자·서버의 **독단을 막는** 것은 전자 입찰의 안전성에 해당한다. 관계자의 부정한 개입으로 입찰 과정과 결과가 좌우되지 않도록 하는 요구이다.

공통 해설

전자 입찰의 안전성은 참여자들이 서로 짜거나 입찰 공고자·서버가 권한을 남용하여 입찰을 부당하게 조작하지 못하도록 하는 요구사항이다. 공모는 여러 관계자가 사전에 뜻을 맞추어 부당한 이익을 얻으려는 행위이고, 독단은 입찰 공고자나 서버가 정해진 절차를 벗어나 일방적으로 입찰 처리를 좌우하는 것을 뜻한다.

지문은 참여자 간의 공모뿐 아니라 입찰을 공고하고 처리하는 주체의 독단까지 방지하도록 요구한다. 이처럼 **공모와 독단에 의한 부정한 개입을 막는** 요구사항을 안전성이라고 한다.

NoteBase

문 33. 저장매체의 물리적인 공간과 실제 사용되는 논리적 공간의 차이로 발생하는 낭비 공간을 의미한다. 디지털포렌식 관점에서는 공격자가 의도적으로 이 공간에 정보를 은닉할 수 있어 검사가 필요하다. 이 공간을 무엇이라고 하는가?

① 히든 공간 (Hidden Space)

② 슬랙공간 (Slack Space)

③ 짓 공간 (Git Space)

④ 그레이 공간 (Gray Space)

정답 2번

간단한 해설

파일에 **할당된 공간과 실제 데이터 크기의 차이**로 남는 부분이 슬랙공간이다. 파일의 논리적 끝 뒤에 데이터가 남거나 숨겨질 수 있어 포렌식에서 확인할 필요가 있다.

개념 구분

슬랙공간은 할당된 저장 공간 중 실제 데이터가 사용하지 않는 남는 부분을 말한다. 대표적인 파일 슬랙은 파일의 논리적인 끝에서 그 파일에 마지막으로 할당된 클러스터의 끝까지의 공간이다. 파일 시스템이 바이트 단위가 아니라 클러스터 같은 할당 단위로 공간을 배정하기 때문에 생긴다.

예를 들어 클러스터 크기가 4 KiB이고 파일 내용이 6 KiB이면 2개 클러스터, 즉 8 KiB가 할당된다. 실제 내용은 6 KiB이므로 마지막 클러스터의 남은 2 KiB가 파일 슬랙이다. 이는 설명을 위한 예시이며 지문이 특정 크기를 제시한 것은 아니다.

포렌식에서 중요한 이유는 **파일의 논리적 내용 밖에 잔존 데이터나 은닉 정보가 남을 수 있기 때문**이다. 일반적인 파일 읽기로 보이는 내용만 확인하면 이 부분을 놓칠 수 있다. 다만 슬랙공간이 존재한다는 사실만으로 악의적인 은닉이 있었다고 단정할 수는 없다.

파일에 할당된 단위 내부의 남는 공간과, 어떤 파일에도 할당되지 않은 비할당 공간은 구별한다. 지문은 물리적 할당량과 실제 사용량의 차이로 생기는 공간을 말하므로 ② **슬랙공간**에 해당한다.

NoteBase

문 34. 다음 지문에서 설명하고 있는 디지털포렌식의 원칙은?

디지털포렌식 과정을 통해 수집된 증거는 획득되고 난 뒤, 이송, 분석, 보관, 법정제출이라는 일련의 과정이 명확해야 한다. 그리고 증거를 전달하고 전달받은 담당자 및 책임자에 대한 추적성이 명확하여 증거물의 진정성을 유지해야 한다.

① 전문배제성

② 독수독과성

③ 연계보관성

④ 수집신속성

정답 3번

간단한 해설

증거를 획득한 뒤 법정에 제출할 때까지 **인계 과정과 담당자를 추적할 수 있게 하는 것**이 연계보관성이다. 증거의 관리 이력을 이어서 확인함으로써 증거물의 진정성을 뒷받침한다.

공통 해설

연계보관성(Chain of Custody)은 증거를 획득한 때부터 이송·분석·보관·법정 제출에 이르기까지 **취급·인계 이력을 끊김 없이 기록하고 관리**하는 원칙이다. 누가 언제 증거를 보관하거나 전달했고 누가 이를 전달받았는지 확인할 수 있어야 한다. 이러한 기록은 법정에 제출된 증거가 처음 획득한 증거에서 이어진 것임을 설명하고, 그 과정에서 부당한 접근이나 변경이 있었는지 확인하는 근거가 된다.

지문은 획득 이후의 모든 과정을 명확히 하고, 증거를 주고받은 담당자와 책임자를 추적하여 진정성을 유지하도록 요구한다. 이처럼 **증거의 관리 이력과 책임의 연결**을 강조하므로 연계보관성에 해당한다. 증거를 얼마나 신속하게 수집했는지가 판단 기준은 아니다.

NoteBase

문 35. 다음 중 정보보호 시스템 평가기준인 국제공통평가기준(Common Criteria)에 대한 설명으로 가장 옳지 않은 것은?

① EAL1에서 EAL7까지 7단계로 구성되어 있다.

② 우리나라는 CCP(Certificate Consuming Participants)로 분류된다.

③ 정보보호 측면에서 정보보호 기능이 있는 IT 제품의 안전성을 보증·평가한다.

④ 보안기능 요구사항과 보증 요구사항으로 구성된다.

정답 2번

간단한 해설

우리나라는 CCRA에서 **인증서 수용국인 CCP가 아니라 인증서 발행국인 CAP**이다. 2006년 인증서 발행국 지위로 가입했으므로 ②가 옳지 않다.

선지별 해설

① O: CC의 평가보증등급은 **EAL1부터 EAL7까지 7단계**이다. 등급이 높아질수록 일반적으로 요구되는 평가의 깊이와 엄밀성, 증거의 범위가 커진다. 이는 보증 수준의 구분이지 보안기능의 개수나 절대적인 공격 불가능성을 나타내는 순위는 아니다.

② X: 우리나라는 2006년 5월 국제상호인정협정(CCRA)에 **인증서 발행국인 CAP**의 지위로 가입했다. CAP는 Certificate Authorizing Participants, CCP는 Certificate Consuming Participants를 뜻한다. CCP는 다른 발행국의 인증서를 수용하는 지위이므로, 우리나라를 CCP로 분류한 설명이 잘못되었다.

③ O: CC는 정보보호 기능을 가진 IT 제품 등의 보안 요구사항과 구현을 공통 기준에 따라 평가하여, 정해진 보안기능이 의도대로 작동한다는 신뢰를 제공한다. 다만 **평가 대상·구성·운용환경과 요구사항의 범위 안에서 보증**하는 것이며, 모든 환경에서 모든 취약점이 없음을 무조건 보장하지는 않는다.

④ O: CC는 '보안기능 요구사항'과 '보증 요구사항'을 구분한다. 전자는 식별·인증, 접근통제 등 제품이 어떤 보안기능을 제공해야 하는지를 규정하고, 후자는 설계·개발 증거, 시험, 취약성 분석 등을 통해 그 기능을 얼마나 신뢰할 수 있는지 평가하는 기준을 규정한다.

NoteBase

문 37. 다음 중 「개인정보 보호법 시행령」으로 규정되어 있는 사항이 아닌 것은?

① 개인정보 침해요인 평가의 절차와 방법에 관하여 필요한 사항
② 개인정보의 파기방법 및 절차 등에 필요한 사항
③ 개인정보 보호책임자의 지정요건, 업무, 자격요건, 그 밖에 필요한 사항
④ 개인정보처리자의 자율적 개인정보 보호활동을 지원하기 위하여 필요한 사항

정답 4번

①

개인정보 침해요인 평가의 절차와 방법에 필요한 사항은 **대통령령으로 정하도록 위임**되어 있다.

개인정보 보호법 제8조의2(개인정보 침해요인 평가)
③ 제1항에 따른 개인정보 침해요인 평가의 절차와 방법에 관하여 필요한 사항은 대통령령으로 정한다.

②

개인정보의 파기방법과 절차 등에 필요한 사항은 **대통령령으로 정하도록 위임**되어 있다.

개인정보 보호법 제21조(개인정보의 파기)
④ 개인정보의 파기방법 및 절차 등에 필요한 사항은 대통령령으로 정한다.

NoteBase

③

개인정보 보호책임자의 자격요건과 업무 등에 필요한 사항은 **대통령령으로 정하며**, 시행령에서 공공기관과 그 밖의 개인정보처리자를 구분하여 **지정할 수 있는 사람의 기준**도 정한다.

개인정보 보호법 제31조(개인정보 보호책임자의 지정 등)
⑩ 제1항에 따른 개인정보 보호책임자의 자격요건, 제3항제2호에 따른 신고의 방법 및 절차, 제4항에 따른 업무 및 제7항에 따른 독립성 보장 등에 필요한 사항은 매출액, 개인정보의 보유 규모 등을 고려하여 대통령령으로 정한다. <개정 2023.3.14, 2026.3.10>

개인정보 보호법 시행령 제32조(개인정보 보호책임자의 지정 등)
② 개인정보처리자는 법 제31조제1항에 따라 개인정보 보호책임자를 지정하려는 경우에는 다음 각 호의 구분에 따라 지정해야 한다. 이 경우 제3항에 따른 개인정보처리자는 다음 각 호의 구분에 따른 사람 중 별표 1에 따른 개인정보 보호책임자의 자격을 갖춘 사람을 개인정보 보호책임자로 지정해야 한다. <개정 2016.7.22, 2024.3.12, 2026.9.10>
1. 공공기관: 다음 각 목의 구분에 따른 기준에 해당하는 공무원 등
가. 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관 및 중앙행정기관: 고위공무원단에 속하는 공무원(이하 "고위공무원"이라 한다) 또는 그에 상당하는 공무원
나. 가목 외에 정무직공무원을 장(長)으로 하는 국가기관: 3급 이상 공무원(고위공무원을 포함한다) 또는 그에 상당하는 공무원
다. 가목 및 나목 외에 고위공무원, 3급 공무원 또는 그에 상당하는 공무원 이상의 공무원을 장으로 하는 국가기관: 4급 이상 공무원 또는 그에 상당하는 공무원
라. 가목부터 다목까지의 규정에 따른 국가기관 외의 국가기관(소속 기관을 포함한다): 해당 기관의 개인정보 처리 관련 업무를 담당하는 부서의 장
마. 시 · 도 및 시 · 도 교육청: 3급 이상 공무원 또는 그에 상당하는 공무원
바. 시 · 군 및 자치구: 4급 이상 공무원 또는 그에 상당하는 공무원
사. 제2조제5호에 따른 각급 학교: 해당 학교의 행정사무를 총괄하는 사람. 다만, 제3항제2호에 해당하는 경우에는 교직원을 말한다.
아. 가목부터 사목까지의 규정에 따른 기관 외의 공공기관: 개인정보 처리 관련 업무를 담당하는 부서의 장. 다만, 개인정보 처리 관련 업무를 담당하는 부서의 장이 2명 이상인 경우에는 해당 공공기관의 장이 지명하는 부서의 장이 된다.
2. 공공기관 외의 개인정보처리자: 다음 각 목의 어느 하나에 해당하는 사람
가. 사업주 또는 대표자
나. 임원(「상법」 제401조의2제1항제3호에 따라 회사의 업무를 집행한 자와 같은 법 제408조의2제1항에 따른 집행임원을 포함하며, 임원이 없는 경우에는 개인정보 처리 관련 업무를 담당하는 부서의 장을 말한다)

NoteBase

④

자율적 개인정보 보호활동을 지원하기 위하여 필요한 사항은 **보호위원회가 마련해야 할 시책으로 법률에 직접 규정**되어 있다.

개인정보 보호법 제13조(자율규제의 촉진 및 지원) 보호위원회는 개인정보처리자의 자율적인 개인정보 보호활동을 촉진하고 지원하기 위하여 다음 각 호의 필요한 시책을 마련하여야 한다. <개정 2013.3.23, 2014.11.19, 2017.7.26, 2020.2.4>
5. 그 밖에 개인정보처리자의 자율적 개인정보 보호활동을 지원하기 위하여 필요한 사항

NoteBase

문 38. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(제44조의8 대화형정보통신서비스에서의 아동 보호)에 관한 사항 중 괄호 안에 들어갈 내용은?

정보통신서비스 제공자는 ( )의 아동에게 문자·음성을 이용하여 사람과 대화하는 방식으로 정보를 처리하는 시스템을 기반으로 하는 정보통신서비스를 제공하는 경우에는 그 아동에게 부적절한 내용의 정보가 제공되지 아니하도록 노력하여야 한다.

① 만 12세 미만
② 만 13세 미만
③ 만 14세 미만
④ 만 15세 미만

정답 3번

공통 해설

정보통신서비스 제공자는 **만 14세 미만의 아동**에게 문자·음성 기반의 대화형정보통신서비스를 제공할 때, **부적절한 내용의 정보가 제공되지 않도록 노력할 의무**를 부담한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제44조의8(대화형정보통신서비스에서의 아동 보호)
정보통신서비스 제공자는 만 14세 미만의 아동에게 문자 · 음성을 이용하여 사람과 대화하는 방식으로 정보를 처리하는 시스템을 기반으로 하는 정보통신서비스를 제공하는 경우에는 그 아동에게 부적절한 내용의 정보가 제공되지 아니하도록 노력하여야 한다.

NoteBase

문 39. 다음 중 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 명시된 정보보호 최고책임자의 업무에 해당하지 않는 것은?

① 사전 정보보호대책 마련 및 보안조치 설계·구현

② 정보보호 인증·평가 등의 실시 및 지원

③ 정보보호관리체계의 수립 및 관리·운영

④ 중요 정보의 암호화 및 보안서버 적합성 검토

정답 2번

①

정보보호 최고책임자는 **정보보호 계획의 수립·시행과 위험에 대한 보호대책 마련**을 총괄한다. 사전 정보보호대책 마련과 보안조치의 설계·구현은 이 업무에 포함된다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제45조의3(정보보호 최고책임자의 지정 등)
④ 정보보호 최고책임자의 업무는 다음 각 호와 같다. <개정 2021.6.8, 2026.3.10, 2026.3.31>
1. 정보보호 최고책임자는 다음 각 목의 업무를 총괄한다.
가. 정보보호 계획의 수립 · 시행 및 개선
다. 정보보호 위험의 식별 평가 및 정보보호 대책 마련

②

정보보호 인증·평가 등의 실시 및 지원은 **한국인터넷진흥원의 사업**이다. 기업 내부의 정보보호 업무를 총괄하는 정보보호 최고책임자의 업무와 구별한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제52조(한국인터넷진흥원)
③ 인터넷진흥원은 다음 각 호의 사업을 한다. <개정 2009.4.22, 2012.2.17, 2013.3.23, 2014.11.19, 2015.6.22, 2017.7.26, 2020.2.4, 2020.6.9, 2021.6.8, 2022.6.10, 2024.1.23, 2025.10.1>
7. 정보보호 관리체계의 인증, 정보보호시스템 평가 · 인증, 정보통신망연결기기등의 정보보호인증, 소프트웨어 개발보안 진단 등 정보보호 인증 · 평가 등의 실시 및 지원

NoteBase

③

정보보호 최고책임자는 **관리적·기술적·물리적 보호조치를 포함한 정보보호 계획의 수립·시행 및 개선**을 총괄한다. 정보보호관리체계의 수립과 관리·운영은 이 업무에 포함된다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제45조의3(정보보호 최고책임자의 지정 등)
④ 정보보호 최고책임자의 업무는 다음 각 호와 같다. <개정 2021.6.8, 2026.3.10, 2026.3.31>
1. 정보보호 최고책임자는 다음 각 목의 업무를 총괄한다.
가. 정보보호 계획의 수립 · 시행 및 개선

④

중요 정보의 암호화와 보안서버 적합성 검토는 정보의 유출 위험을 줄이기 위한 보호조치이다. 이를 포함한 **정보보호 위험의 식별·평가 및 보호대책 마련**을 정보보호 최고책임자가 총괄한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제45조의3(정보보호 최고책임자의 지정 등)
④ 정보보호 최고책임자의 업무는 다음 각 호와 같다. <개정 2021.6.8, 2026.3.10, 2026.3.31>
1. 정보보호 최고책임자는 다음 각 목의 업무를 총괄한다.
다. 정보보호 위험의 식별 평가 및 정보보호 대책 마련

NoteBase