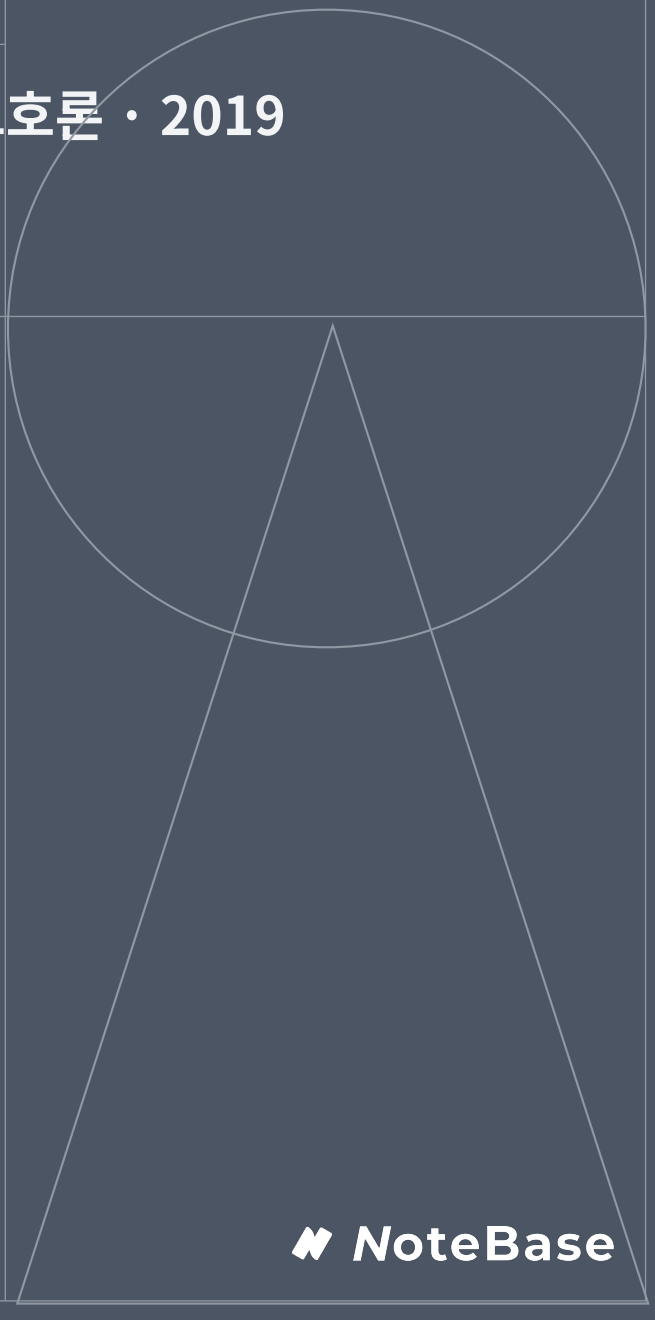
기출OX 해설집

공무원/국가직/7급 · 정보보호론 · 2019



NoteBase

기출OX 해설집

공무원/국가직/7급 · 정보보호론 · 2019

공무원/국가직/7급 · 정보보호론 · 2019

문 1. Biba 보안 모델에 대한 설명으로 옳은 것은?

① 이해가 상충되는 회사들 간의 정보 흐름이 일어나지 않도록 고안되었다.

② 자신의 보안 수준보다 낮거나 같은 수준의 객체만 읽을 수 있다.

③ 자신의 보안 수준보다 높거나 같은 수준의 객체에만 쓸 수 있다.

④ 자신의 무결성 수준보다 높거나 같은 수준의 객체만 읽을 수 있다.

정답 4번

출제 포인트

이 문제는 Biba 모델이 보호하는 대상이 기밀성이 아니라 무결성이며, 그에 따라 읽기·쓰기 방향이 어떻게 제한되는지를 묻는 문제이다.

핵심 개념

Biba 모델은 낮은 무결성 정보가 높은 무결성 주체를 오염시키지 못하게 하는 무결성 모델이다.
Bell-LaPadula 모델은 높은 기밀성 정보가 낮은 등급으로 새지 못하게 하는 기밀성 모델이다.
Chinese Wall 모델은 이해 상충 관계에 있는 기업 사이의 정보 흐름을 막는 이해상충 방지 모델이다.
Biba의 핵심 키워드는 무결성, no read down, no write up이다.

NoteBase

선지별 해설

① X: 이해가 상충되는 회사 간 정보 흐름 차단은 Chinese Wall 모델의 설명이다. 틀린 표현은 "Biba 보안 모델"이다. 올바르게는 "Chinese Wall 모델은 이해 상충 기업 간 정보 흐름을 제한한다"이다.
② X: 자신의 보안 수준보다 낮거나 같은 수준의 객체만 읽는다는 것은 Bell-LaPadula의 no read up에 해당한다. 틀린 표현은 "낮거나 같은 수준의 객체만 읽을 수 있다"이다. Biba에서는 낮은 무결성 객체를 읽지 못하므로 올바르게는 "자신의 무결성 수준보다 높거나 같은 수준의 객체만 읽을 수 있다"이다.
③ X: 자신의 보안 수준보다 높거나 같은 수준의 객체에만 쓸 수 있다는 것은 Bell-LaPadula의 no write down에 해당한다. 틀린 표현은 "높거나 같은 수준의 객체에만 쓸 수 있다"이다. Biba에서는 높은 무결성 객체를 오염시키지 않기 위해 올바르게는 "자신의 무결성 수준보다 낮거나 같은 수준의 객체에만 쓸 수 있다"이다.
④ O: Biba 모델의 단순 무결성 속성은 no read down이므로, 주체는 자신의 무결성 수준보다 높거나 같은 수준의 객체만 읽을 수 있다. 낮은 무결성 데이터를 읽으면 높은 무결성 주체가 오염될 수 있으므로 이 선지가 맞다.

오답 포인트

Biba와 Bell-LaPadula의 읽기·쓰기 방향을 서로 뒤집어 외우면 ②와 ③에 쉽게 걸린다. 또한 ①처럼 이해상충 방지 모델인 Chinese Wall을 무결성 모델과 섞어 내는 것도 대표적인 함정이다.

다시 나오면 이렇게 판단

선지에 무결성이라는 말이 나오면 먼저 Biba인지 확인하고, 낮은 무결성 정보가 높은 쪽을 오염시키지 못하게 한다는 방향으로 판단하면 된다. 따라서 읽기는 위로만 가능하고, 쓰기는 아래로만 가능하다고 정리할 수 있다.

암기 포인트

Biba는 무결성 보호이므로 no read down, no write up이고, Bell-LaPadula는 기밀성 보호이므로 no read up, no write down이다.

NoteBase

문 2. IT 재해복구체계 수립 시, 업무영향분석(BIA: Business Impact Analysis) 과정에서 고려하는 항목이 아닌 것은?

① MTD(Maximum Tolerable Downtime)

② MTU(Maximum Transfer Unit)

③ RTO(Recovery Time Objective)

④ RPO(Recovery Point Objective)

정답 2번

출제 포인트

이 문제는 업무영향분석(BIA)에서 사용하는 복구 목표 개념과 전혀 다른 네트워크 용어를 구별하는지를 묻는 문제이다.

핵심 개념

MTD는 업무가 중단되어도 견딜 수 있는 최대 허용 중단시간이다.
RTO는 재해 이후 서비스를 언제까지 복구해야 하는지를 정한 목표시간이다.
RPO는 어느 시점까지 데이터를 복구해야 하는지를 정한 목표복구시점이다.
MTU는 네트워크에서 한 번에 전송할 수 있는 최대 패킷 크기를 뜻하는 Maximum Transfer Unit으로, BIA의 복구 목표 항목이 아니다.

NoteBase

선지별 해설

① O
MTD는 Maximum Tolerable Downtime으로, 해당 업무가 중단되어도 조직이 감내할 수 있는 최대 중단시간을 뜻한다. BIA에서 핵심적으로 산정하는 값이다.

② X
틀린 부분은 "MTU(Maximum Transfer Unit)"를 BIA 고려 항목처럼 제시한 점이다.
실제로는 MTU는 네트워크 패킷의 최대 전송 단위를 뜻하는 통신 용어이다. BIA에서 고려하는 복구 목표 항목으로는 MTD, RTO, RPO 등이 사용된다.

③ O
RTO는 Recovery Time Objective로, 장애나 재해 발생 후 서비스를 목표 시간 내에 복구해야 한다는 기준이다. BIA 결과를 바탕으로 정해지는 대표 지표이다.

④ O
RPO는 Recovery Point Objective로, 데이터 손실을 어디까지 허용할 것인지를 시간 기준으로 정한 복구 시점 목표이다. 백업 주기와 데이터 복구 전략을 정할 때 함께 고려된다.

오답 포인트

약어가 모두 세 글자라서 MTD, RTO, RPO와 MTU를 같은 범주의 복구 용어로 착각하기 쉽다. 특히 ②는 약어 형식은 비슷하지만 재해복구가 아니라 네트워크 전송 단위라는 점이 함정이다.

다시 나오면 이렇게 판단

재해복구 문제에서 약어가 나오면 먼저 시간 목표인지, 데이터 복구 시점인지, 허용 중단시간인지를 확인한다. 복구 목표가 아니라 네트워크 전송, 패킷 크기 같은 통신 자체 용어이면 BIA 항목이 아니라고 판단할 수 있다.

암기 포인트

BIA는 MTD·RTO·RPO, MTU는 네트워크 전송 단위이다.

NoteBase

문 3. 다음에서 설명하는 위험 분석 접근 방법은?

◯ 정형화되고 구조화된 프로세스를 사용하는 대신, 분석가 개인의 지식 및 경험을 활용한다.
◯ 비교적 비용대비 효과가 우수하며 중 · 소규모 조직에 적합하다.
◯ 개인적인 경험에 의존하므로 정당성이나 일관성이 부족할 수 있다.

① 기준선 접근(Baseline Approach)
② 상세 위험 분석(Detailed Risk Analysis)
③ 비형식적 접근(Informal Approach)
④ 복합 접근(Combined Approach)

정답 3번

출제 포인트

이 문제는 위험 분석 접근 방법 중 비형식적 접근의 특징과 다른 접근 방법의 차이를 구별할 수 있는지를 묻는다.

핵심 개념

비형식적 접근은 정형화된 절차보다 분석가의 지식과 경험에 의존하는 방식이며 비용이 적게 들지만 일관성이 떨어질 수 있다.
기준선 접근은 최소한의 보안 기준을 정해 조직 전반에 공통 적용하는 방식이다.
상세 위험 분석은 자산, 위협, 취약성을 체계적으로 분석하는 정형적 방법이다.
복합 접근은 전체에는 기준선을 적용하고 중요한 부분만 상세 분석하는 혼합 방식이다.

선지별 해설

1번 X: 기준선 접근은 공통 최소 보안대책을 기준으로 일괄 적용하는 방식이다. 문제의 설명처럼 분석가 개인의 경험에 주로 의존하는 방식이 아니다. 틀린 표현은 위험 분석 접근 방법을 기준선 접근으로 본 부분이며, 올바르게는 기준선 접근은 표준화된 최소 통제를 적용하는 방법이다.
2번 X: 상세 위험 분석은 정형화되고 구조화된 절차로 자산 가치, 위협, 취약성을 세밀하게 평가하는 방법이다. 문제의 설명처럼 비정형적이고 경험 의존적인 방식이 아니다. 올바르게는 상세 위험 분석은 비용과 시간이 더 들지만 분석의 체계성과 타당성이 높다.
3번 O: 비형식적 접근은 분석가의 지식과 경험을 활용하고, 비교적 적은 비용으로 수행할 수 있어 중소규모 조직에 적합하다. 대신 개인 판단 의존도가 높아 정당성이나 일관성이 부족할 수 있으므로 제시문과 정확히 일치한다.
4번 X: 복합 접근은 기준선 접근과 상세 위험 분석을 함께 사용하는 방식이다. 문제의 설명처럼 전적으로 개인 경험에 의존하는 단일 접근이 아니다. 올바르게는 복합 접근은 일반 영역에는 기준선을 적용하고 중요 자산이나 핵심 시스템에는 상세 분석을 추가하는 방법이다.

NoteBase

오답 포인트

비형식적 접근과 기준선 접근은 모두 비교적 간편하게 보일 수 있어 혼동하기 쉽다. 그러나 비형식적 접근의 핵심은 분석가 개인 경험 의존이고, 기준선 접근의 핵심은 표준화된 최소 통제의 일괄 적용이라는 점에서 구별된다.

다시 나오면 이렇게 판단

선지나 제시문에 개인의 경험, 직관, 비정형, 낮은 비용, 일관성 부족이 함께 나오면 비형식적 접근을 먼저 떠올린다. 반대로 최소 기준의 공통 적용이면 기준선 접근, 체계적 세부 분석이면 상세 위험 분석, 둘을 섞으면 복합 접근으로 판단한다.

암기 포인트

비형식적 접근은 경험 중심, 기준선 접근은 최소기준 중심, 상세 위험 분석은 정밀분석 중심, 복합 접근은 혼합 중심이다.

NoteBase

문 4. 다음 수식에 의해 산출되는 것은?

$H[(K^+ \oplus opad) \| H[(K^+ \oplus ipad) \| M]]$
H: 해시 함수 K^+: 비밀키 K에 0을 덧붙인 것
M: 메시지 ipad, opad: 특정 상수
⊕: XOR ‖: 연결(concatenation)

① GMAC

② HMAC

③ CMAC

④ 전자 서명

정답 2번

출제 포인트

해시 기반 메시지 인증 코드인 HMAC의 수식 구조를 식별할 수 있는지를 묻는 문제이다.

조건 정리

주어진 식은 $H[(K^+ \oplus opad) \| H[(K^+ \oplus ipad) \| M]]$ 이다.
여기서 H는 해시 함수, M은 메시지, K^+는 블록 길이에 맞게 0을 덧붙인 키, $ipad$와 $opad$는 HMAC에서 쓰는 고정 패딩 상수이다.
구해야 할 값은 이 구조가 어떤 인증 방식인지이다.

사용할 공식

HMAC의 정의식은 $H[(K^+ \oplus opad) \| H[(K^+ \oplus ipad) \| M]]$ 이다.
이 공식을 쓰는 이유는 문제에 제시된 식이 내부 해시와 외부 해시의 이중 구조를 가지며, $ipad$와 $opad$를 함께 사용하는 전형적인 HMAC 형태이기 때문이다.

계산 과정

1. 식에 $ipad$, $opad$, K^+가 있는지 확인한다.
2. 메시지 M에 대해 먼저 내부 해시 $H[(K^+ \oplus ipad) \| M]$를 계산하는 구조인지 확인한다.
3. 그 결과에 다시 $K^+ \oplus opad$를 붙여 외부 해시를 하는 이중 해시 구조이므로 HMAC으로 판단한다.

NoteBase

선지별 해설

① X: GMAC은 GCM에서 파생된 블록 암호 기반 인증 코드이며 해시 함수의 *ipad*, *opad*를 사용하지 않는다. 틀린 표현은 "GMAC"이고, 올바르게는 "이 식은 HMAC 구조이다."이다.
② O: HMAC은 비밀키를 블록 길이에 맞춘 K^+에 *ipad*, *opad*를 XOR하여 내부 해시와 외부 해시를 수행하는 해시 기반 MAC이다. 제시된 식과 정확히 일치한다.
③ X: CMAC은 AES 같은 블록 암호와 서브키를 이용하는 CBC-MAC 계열 방식이며 *ipad*, *opad* 또는 이중 해시식을 사용하지 않는다. 틀린 표현은 "CMAC"이고, 올바르게는 "이 식은 HMAC이다."이다.
④ X: 전자 서명은 개인키와 공개키를 사용하는 비대칭 구조로 부인방지를 제공하며, 공유 비밀키와 해시 패딩 상수로 만드는 MAC 식과 다르다. 틀린 표현은 "전자 서명"이고, 올바르게는 "이 식은 메시지 인증 코드인 HMAC이다."이다.

오답 포인트

MAC라는 공통 기능만 보고 GMAC, CMAC, HMAC을 묶어 외우면 혼동하기 쉽다. 이 문제의 함정은 인증 기능의 이름이 아니라 구현 단서를 읽는 데 있으며, *ipad*와 *opad*가 보이면 HMAC으로 바로 연결되어야 한다.

다시 나오면 이렇게 판단

식에 해시 함수 H, 패딩된 키 K^+, 그리고 *ipad*, *opad*가 함께 나오면 HMAC 구조로 판단한다. 블록 암호 기반인지, 해시 기반인지부터 먼저 구분하면 GMAC과 CMAC을 빠르게 배제할 수 있다.

암기 포인트

HMAC은 *ipad*로 안쪽 해시를 하고 *opad*로 바깥 해시를 하는 이중 해시 MAC이다.

NoteBase

문 5. 「정보보호 및 개인정보보호 관리체계(ISMS-P)의 인증 등에 관한 고시」 상의 인증심사 기준 중, '개인정보 처리 단계별 요구사항'에 포함되지 않는 것은?

① 사용자 계정 관리

② 이용자 단말기 접근 보호

③ 영상정보처리기기 설치 · 운영

④ 개인정보처리방침 공개

정답 1번

쟁점

이 문제는 ISMS-P 인증심사 기준에서 개인정보 처리 단계별 요구사항에 속하는 항목과 정보보호 대책 요구사항에 속하는 항목을 구별하는 문제이다.

용어 풀이

개인정보 처리 단계별 요구사항은 개인정보의 수집, 보유·이용, 제공, 파기, 정보주체 권리보호 등 처리 흐름 단계마다 적용되는 보호조치이다.

핵심 구분

개인정보 처리 단계별 요구사항은 3.1 수집 시 보호조치, 3.2 보유 및 이용 시 보호조치, 3.3 제공 시 보호조치, 3.4 파기 시 보호조치, 3.5 정보주체 권리보호로 구성된다. 반면 사용자 계정 관리는 2.5 인증 및 권한관리 영역의 정보보호 대책 요구사항이므로 개인정보 처리 단계별 요구사항에 속하지 않는다.

선지별 해설

1번 O: 사용자 계정 관리는 2.5.1 항목으로, 사용자 등록·해지와 접근권한 부여·변경·말소를 통제하는 정보보호 대책 요구사항이다. 따라서 개인정보 처리 단계별 요구사항에는 포함되지 않는다.
2번 X: 이용자 단말기 접근 보호는 3.2.4 항목으로, 개인정보 보유 및 이용 시 보호조치에 포함된다. 틀린 판단은 이 항목이 개인정보 처리 단계별 요구사항에 포함되지 않는다고 보는 점이다. 올바르게는 이용자 단말기 정보나 기능에 접근할 때 알림과 동의를 요구하는 단계별 항목이다.
3번 X: 영상정보처리기기 설치·운영은 3.1.6 항목으로, 개인정보 수집 시 보호조치에 포함된다. 틀린 판단은 이 항목이 개인정보 처리 단계별 요구사항 바깥에 있다고 보는 점이다. 올바르게는 공개된 장소에 영상정보처리기기를 설치·운영할 때 법적 요구사항과 보호대책을 준수하는 수집 단계 항목이다.
4번 X: 개인정보처리방침 공개는 3.5.1 항목으로, 정보주체 권리보호에 포함된다. 틀린 판단은 이 항목이 개인정보 처리 단계별 요구사항에 포함되지 않는다고 보는 점이다. 올바르게는 정보주체가 언제든지 쉽게 확인할 수 있도록 공개하고 현행화하여야 하는 권리보호 단계 항목이다.

NoteBase

오답 포인트

사용자 계정 관리처럼 보안 통제 성격이 강한 항목과 개인정보 처리 단계별 항목을 한 묶음으로 외우면 틀리기 쉽다. 숫자 체계를 함께 보면 2번대는 정보보호 대책 요구사항, 3번대는 개인정보 처리 단계별 요구사항이라는 구분이 분명해진다.

다시 나오면 이렇게 판단

ISMS-P에서 특정 항목의 소속을 묻는 문제는 먼저 대분류 번호를 확인한다. 3.1부터 3.5까지는 개인정보의 수집부터 권리보호까지의 처리 단계이고, 계정·권한관리처럼 공통 보안통제는 2번대 정보보호 대책 요구사항으로 판단한다.

암기 포인트

개인정보 처리 단계별 요구사항은 3번대이고, 사용자 계정 관리는 2.5.1 권한관리 항목이다.

NoteBase

문 6. 다음 리눅스 /etc/shadow 파일 항목에 대한 설명으로 옳지 않은 것은?

abcd:1qPZPGTVz$RDqazm48WaMXw3Mvy4OQb1:17562:0:99999:7:3::

① 계정명은 abcd이다.
② 계정 패스워드의 해시값 계산에 사용된 해시 함수는 MD-5이다.
③ 솔트(salt)값은 qPZPGTVz이다.
④ 계정 패스워드의 유효기간은 7일이다.

정답 4번

출제 포인트

이 문제는 /etc/shadow 한 줄을 계정명, 암호 해시 형식, 패스워드 정책 필드 순서로 정확히 해석할 수 있는지를 묻는다.

자료 읽는 순서

1. 콜론(:) 기준으로 필드를 나눈다.
2. 두 번째 필드에서 `$id$salt$hash` 형식을 읽어 해시 방식과 salt를 확인한다.
3. 뒤의 숫자 필드를 `마지막 변경일:최소 사용일수:최대 사용일수:만료 경고일수:만료 후 비활성 일수` 순서로 대응한다.

핵심 근거

`17562:0:99999:7:3::`는 각각 마지막 변경일, 최소 사용일수 0일, 최대 사용일수 99999일, 만료 경고 7일, 만료 후 비활성 3일을 뜻한다.

선지별 해설

1번 O: 첫 번째 필드 `abcd`는 로그인 계정명이다.
2번 O: 두 번째 필드의 `$1$`은 MD5 해시 방식을 뜻한다.
3번 O: 암호 필드는 `$id$salt$hash` 형식이므로 salt는 `qPZPGTVz`이다.
4번 X: `7`은 패스워드 유효기간이 아니라 만료 전 경고 일수이다. 유효기간에 해당하는 최대 사용 일수는 `99999`이다. 틀린 표현은 `유효기간은 7일`이고, 올바르게는 `만료 경고 기간은 7일이고 최대 사용 기간은 99999일이다.`

오답 포인트

shadow 파일의 숫자 필드를 순서 없이 읽으면 `99999`와 `7`의 의미를 바꿔 해석하기 쉽다. 이 문항은 경고 기간을 유효기간으로 착각하는지를 노린 문제이다.

NoteBase

다시 나오면 이렇게 판단

/etc/shadow는 `계정명:암호:마지막변경:최소:최대:경고:비활성:만료:예약` 순서로 읽는다. 숫자 값이 여러 개 나오면 필드명을 먼저 고정한 뒤 값을 대입하면 된다.

암기 포인트

`$1$`은 MD5, `99999`는 최대 사용 기간, `7`은 만료 경고 기간이다.

문 7. 「개인정보 보호법」상 개인정보처리자가 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있는 경우에 해당하지 않는 것은?

① 정보주체로부터 별도의 동의를 받은 경우

② 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우

③ 범죄의 예방을 위하여 필요한 경우

④ 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우

정답 3번

쟁점

이 문제는 2019년 시험 당시 개인정보 보호법상 개인정보의 목적 외 이용 또는 제3자 제공이 허용되는 예외 사유를 구별하는 문제이다. 핵심은 별도 동의, 비식별 형태의 통계·학술연구 제공, 급박한 생명·신체·재산 보호는 예외이지만, '범죄의 예방'은 이 조문의 예외 문언이 아니라는 점이다.

용어 풀이

목적 외 이용·제공은 원래 수집한 목적 범위를 넘어 개인정보를 이용하거나 제3자에게 제공하는 것을 말한다.

핵심 구분

원칙적으로 개인정보는 목적 외로 이용하거나 제3자에게 제공할 수 없다. 다만 2019년 당시 개인정보 보호법 제18조 제2항은 별도 동의, 통계작성 및 학술연구 등의 목적을 위한 비식별 제공, 급박한 생명·신체·재산 보호 등은 예외로 두었다. 반면 수사 관련 예외 문언은 '범죄의 수사와 공소의 제기 및 유지'이므로, '범죄의 예방'과는 구별된다.

NoteBase

선지별 해설

① O
- 정보주체로부터 별도의 동의를 받으면 목적 외 이용이나 제3자 제공이 가능하다. 별도 동의는 제18조 제2항의 대표적인 예외 사유이다.

② O
- 2019년 당시에는 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우가 예외 사유에 포함되었다. 비식별 형태로 제공된다는 점이 판단 기준이다.

③ X
- 이 조문의 예외는 '범죄의 수사와 공소의 제기 및 유지'이지 '범죄의 예방'이 아니다. 범죄 예방은 다른 조문 문언과 혼동하기 쉬우나, 제18조 제2항의 예외 사유로 그대로 적시되어 있지 않다.
- 틀린 표현: '범죄의 예방을 위하여 필요한 경우'
- 올바른 표현: '범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우'

④ O
- 정보주체 또는 그 법정대리인이 의사표시를 할 수 없거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서, 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되면 예외적으로 허용된다. 긴급성과 동의 불가능성이 함께 요구되는 경우이다.

오답 포인트

③의 '범죄의 예방'은 공개장소 영상정보처리기기 설치 사유처럼 다른 조문에서 자주 보이는 표현이라서 쉽게 끌려간다. 그러나 목적 외 이용·제공 제한 조문은 문언이 더 좁아서 '수사와 공소의 제기 및 유지'로 기억해야 한다.

다시 나오면 이렇게 판단

개인정보 목적 외 이용·제공의 예외 문제는 먼저 조문 키워드를 동의, 비식별 연구, 급박한 생명·신체·재산, 수사·공소 유지처럼 묶어서 확인한다. 그다음 보기의 문구가 조문 문언과 한 글자라도 다르면 다른 제도의 문구가 섞인 것으로 보고 배제한다.

암기 포인트

제18조 예외는 예방보다 수사이고, 연구 제공은 비식별이어야 한다.

NoteBase

문 8. 「전자정부 SW 개발·운영자를 위한 소프트웨어 개발보안 가이드」상 분석·설계 단계 보안요구항목과 그에 대한 설명으로 옳지 않은 것은?

① 인증 수행 제한 - 인증 반복시도 제한 및 인증실패 등에 대한 인증제한 기능 설계

② 암호키 관리 - 암호키 생성, 분배, 접근, 파기 등 안전하게 암호키 생명주기를 관리할 수 있는 방법 설계

③ 예외 처리 - 보안기능 동작을 위해 사용되는 입력값과 함수의 외부입력값 및 수행결과에 대한 처리방법 설계

④ 시스템 자원 접근 및 명령어 수행 입력값 검증 - 시스템 자원접근 및 명령어 수행을 위해 사용되는 입력값에 대한 유효성 검증방법과 유효하지 않은 값에 대한 처리방법 설계

정답 3번

쟁점

이 문제는 「전자정부 SW 개발·운영자를 위한 소프트웨어 개발보안 가이드」의 분석·설계 단계 보안요구항목 명칭과 설명의 정확한 대응을 묻는 문제이다. 핵심은 예외 처리와 보안기능 동작에 사용되는 입력값 검증을 구별하는 것이다.

용어 풀이

예외 처리 = 오류 상황이나 예상 밖의 수행 결과가 발생했을 때 시스템이 안전하게 종료·복구·차단되도록 처리 흐름을 설계하는 것이다.
보안기능 동작에 사용되는 입력값 검증 = 인증·인가·권한부여 같은 보안기능에 들어가는 입력값, 함수의 외부입력값, 수행결과를 검증하고 그 처리방법을 설계하는 것이다.

핵심 구분

예외 처리는 오류 상황 대응에 관한 항목이다. 반면 보안기능 동작에 사용되는 입력값 검증은 보안기능에 쓰이는 입력값과 결과값의 신뢰성 검증에 관한 항목이다. 따라서 3번의 설명 자체는 맞는 내용이지만, 그 설명이 가리키는 항목명은 예외 처리가 아니라 보안기능 동작에 사용되는 입력값 검증이다.

NoteBase

선지별 해설

① O
인증 수행 제한은 반복 인증 시도 제한, 인증 실패 횟수 통제, 잠금 처리 같은 인증 제한 기능 설계에 관한 항목이므로 설명과 항목명이 맞게 대응된다.

② O
암호키 관리는 암호키의 생성, 분배, 저장, 접근, 교체, 파기까지 포함한 생명주기 관리 설계 항목이므로 설명과 일치한다.

③ X
제시된 설명인 "보안기능 동작을 위해 사용되는 입력값과 함수의 외부입력값 및 수행결과에 대한 처리방법 설계"는 예외 처리의 설명이 아니다. 이 설명은 보안기능 동작에 사용되는 입력값 검증에 해당한다.
틀린 표현: 예외 처리
올바른 표현: 보안기능 동작에 사용되는 입력값 검증

④ O
시스템 자원 접근 및 명령어 수행 입력값 검증은 파일 경로, 운영체제 명령어 인자 등 시스템 자원 접근이나 명령 수행에 사용되는 입력값의 유효성을 검증하고, 유효하지 않은 값의 처리방법을 설계하는 항목이므로 설명과 맞다.

오답 포인트

3번은 설명 내용만 보면 보안 관련 입력값 검증 일반론처럼 보여 그럴듯하다. 그러나 문제는 설명의 타당성 자체가 아니라 항목명과 설명의 매칭을 묻는다. "보안기능 동작", "외부입력값", "수행결과"라는 표현이 나오면 예외 처리보다 보안기능 입력값 검증 항목을 먼저 떠올려야 한다.

다시 나오면 이렇게 판단

분석·설계 단계 보안요구항목 문제는 설명 속 핵심 명사를 기준으로 분류하면 된다. 인증 실패·반복 시도는 인증 수행 제한, 키 생성·분배·파기는 암호키 관리, 시스템 자원·명령어는 자원 접근 및 명령어 수행 입력값 검증, 보안기능 입력값·외부입력값·수행결과는 보안기능 동작에 사용되는 입력값 검증으로 연결하면 된다.

암기 포인트

예외 처리는 오류 대응이고, 보안기능 입력값 검증은 인증·인가 등에 쓰이는 입력값과 결과값 검증이다.

NoteBase

문 9. 두 소수, p = 13, q = 11을 사용하는 RSA 시스템에서 키값 (e, d)로 사용할 수 있는 쌍은?

① (7, 11)

② (7, 23)

③ (13, 37)

④ (13, 47)

정답 3번

출제 포인트

이 문제는 RSA에서 $n = pq$, $\phi(n) = (p-1)(q-1)$를 구한 뒤 키쌍 (e, d)가 ed ≡ 1 ±odϕ(n)을 만족하는지 판단하는 문제이다.

조건 정리

주어진 값: $p = 13$, $q = 11$
구해야 할 값: RSA 키쌍 (e, d)
주의할 조건: e는 $\phi(n)$와 서로소이고, d는 ed ≡ 1 ±odϕ(n)를 만족해야 한다.

사용할 공식

$n = pq$, $\phi(n) = (p-1)(q-1)$, ed ≡ 1 ±odϕ(n)
이 공식을 쓰는 이유: RSA에서는 먼저 두 소수로 n과 $\phi(n)$를 구하고, 그다음 e와 d가 서로 역원 관계인지 확인해야 올바른 키쌍이 된다.

계산 과정

1. $n = 13 \times 11 = 143$이다.
2. $\phi(n) = (13-1)(11-1) = 12 \times 10 = 120$이다.
3. 각 보기의 (e, d)에 대해 ed ≡ 1 ±od120인지 확인한다.
4. ①은 $7 \times 11 = 77$이므로 1이 아니다.
5. ②는 $7 \times 23 = 161$, $161 \equiv 41$ ±od120이므로 1이 아니다.
6. ③은 $13 \times 37 = 481$, $481 = 120 \times 4 + 1$이므로 $481 \equiv 1$ ±od120이다.
7. ④는 $13 \times 47 = 611$, $611 \equiv 11$ ±od120이므로 1이 아니다.

NoteBase

선지 판단

1번: X. (7, 11)은 $e = 7$ 자체는 가능하지만 $7 \times 11 = 77$이라서 ed ≡ 1 ±od120을 만족하지 못한다. 틀린 부분은 $d = 11$이고, 올바르게는 d가 7의 모듈러 역원이어야 한다.
2번: X. (7, 23)은 $7 \times 23 = 161$, 즉 161 ≡ 41 ±od120이므로 개인키 조건을 만족하지 못한다. 틀린 부분은 $d = 23$이고, 올바르게는 ed를 120으로 나눈 나머지가 1이 되는 값이어야 한다.
3번: O. (13, 37)은 $13 \times 37 = 481$, 즉 481 ≡ 1 ±od120이므로 올바른 키쌍이다. 또한 gcd(13, 120) = 1이어서 e 조건도 만족한다.
4번: X. (13, 47)은 $13 \times 47 = 611$, 즉 611 ≡ 11 ±od120이므로 역원 관계가 아니다. 틀린 부분은 $d = 47$이고, 올바르게는 $d = 37$처럼 13d ≡ 1 ±od120을 만족해야 한다.

오답 포인트

RSA 문제에서는 $n = pq$만 계산하고 끝내면 틀린다. 이 문항의 함정은 $\phi(n) = 120$을 구한 뒤 각 보기의 곱을 120으로 나눈 나머지를 확인해야 하는데, 단순히 소수 여부나 숫자 크기만 보고 고르기 쉽다는 점이다.

다시 나오면 이렇게 판단

RSA 키쌍 문제는 $\phi(n) = (p-1)(q-1)$를 먼저 구하고, 각 보기마다 $\gcd(e, \phi(n)) = 1$인지와 ed ≡ 1 ±odϕ(n)인지 순서대로 확인하면 된다.

암기 포인트

RSA 키쌍의 핵심은 $\phi(n)$에 대한 역원 관계이며, 정답 판별식은 ed ≡ 1 ±odϕ(n)이다.

NoteBase

문 10. 암호 화폐인 비트코인이 채택한 블록체인의 블록 헤더에 포함되는 구성 요소가 아닌 것은?

① 이전 블록의 헤더를 두 번 연속 해시한 값

② 해당 블록에 포함된 모든 트랜잭션의 해시로부터 추출된 merkle root 해시값

③ 작업증명(proof of work) 조건을 만족하는 nonce 값

④ 블록 생성자(miner)의 계정

정답 4번

출제 포인트

이 문제는 비트코인 블록 헤더에 실제로 들어가는 필드와 블록 본문이나 코인베이스 트랜잭션에 들어가는 정보를 구분하는 문제이다.

핵심 개념

블록 헤더는 블록 식별과 작업증명에 필요한 요약 정보만 담는 영역이다.
이전 블록 해시: 직전 블록을 연결하는 값으로, 비트코인에서는 이전 블록 헤더의 이중 SHA-256 해시값을 넣는다.
머클 루트: 블록 안의 모든 트랜잭션 해시를 머클 트리로 결합해 얻는 대표 해시값이다.
nonce: 작업증명 조건을 만족하는 해시가 나오도록 바꾸어 보는 32비트 값이다.
채굴자 계정: 보상 수령 주소나 식별 정보는 보통 코인베이스 트랜잭션 쪽에서 표현되며 블록 헤더 필드는 아니다.

NoteBase

선지별 해설

① O
이전 블록 해시값은 비트코인 블록 헤더의 핵심 필드이다. 선지의 표현은 이전 블록 헤더를 두 번 해시한 값을 가리키므로 헤더 구성요소 설명으로 볼 수 있다.

② O
머클 루트 해시값은 해당 블록의 모든 트랜잭션 해시를 결합해 만든 대표값으로 블록 헤더에 포함된다.

③ O
nonce 값은 채굴 과정에서 작업증명 조건을 만족시키기 위해 바꾸어 가며 찾는 값이므로 블록 헤더 구성요소가 맞다.

④ X
틀린 부분은 "블록 생성자(miner)의 계정"이다.
올바르게는 채굴자 계정이나 보상 수령 주소는 블록 헤더가 아니라 코인베이스 트랜잭션의 출력 등 블록 내용에 반영된다.

오답 포인트

블록과 블록 헤더를 같은 것으로 섞어 생각하면 ④에 흔들리기 쉽다. 채굴자가 블록을 만들었다는 사실과 채굴자 계정이 헤더에 저장된다는 것은 다른 말이다.

다시 나오면 이렇게 판단

블록 헤더 문제는 먼저 연결 정보, 무결성 요약값, 작업증명 관련 값만 들어간다고 본다. 사람이나 계정, 보상 주소처럼 거래 주체 정보가 나오면 헤더가 아니라 트랜잭션 영역일 가능성이 크다.

암기 포인트

비트코인 블록 헤더는 이전 블록 해시, 머클 루트, 시간, 난이도, nonce 같은 요약값 중심이며 채굴자 계정은 헤더 밖 정보이다.

NoteBase

문 11. 다음에서 설명하는 해시 함수H의 특성은?

주어진 메시지 x에 대해, $H(y) = H(x)$를 만족하면서 $y \neq x$인 y를 찾는 것이 계산상 매우 어려워야 한다.

① 의사난수성(Pseudo-randomness)
② 역상 저항성(Pre-image Resistance)
③ 약한 충돌 저항성(Weak Collision Resistance)
④ 강한 충돌 저항성(Strong Collision Resistance)

정답 3번

출제 포인트

주어진 메시지 x가 있을 때 같은 해시값을 내는 다른 y를 찾기 어려운 성질이 무엇인지 구별하는 문제이다.

핵심 개념

역상 저항성은 해시값 $H(x)$만 주어졌을 때 그 입력을 찾기 어려운 성질이다. 키워드는 출력에서 입력으로의 역추적 곤란이다.
약한 충돌 저항성은 특정 입력 x가 주어졌을 때 $H(y) = H(x), y \neq x$인 다른 입력 y를 찾기 어려운 성질이다. 키워드는 고정된 x에 대한 제2역상 탐색 곤란이다.
강한 충돌 저항성은 어떤 두 입력이든 자유롭게 골라 같은 해시값을 갖는 충돌쌍을 찾기 어려운 성질이다. 키워드는 두 입력 모두 자유 선택이다.
의사난수성은 출력이 난수처럼 보여 예측이 어려운 성질을 뜻하며, 이 문제의 충돌·역상 구분 축과는 다르다.

선지별 해설

① X. 의사난수성은 해시 출력이 난수처럼 보이는 성질을 뜻한다. 문제는 특정 x가 주어진 상태에서 같은 해시값을 만드는 다른 y를 찾는 난이도를 묻는다. 틀린 표현은 "의사난수성"이다. 올바르게는 "약한 충돌 저항성"이다.
② X. 역상 저항성은 $H(x)$라는 해시값만 보고 원래 입력을 찾기 어려운 성질이다. 문제처럼 이미 x가 주어져 있고 $y \neq x$인 다른 입력을 찾는 것은 역상 탐색이 아니라 제2역상 탐색이다. 틀린 표현은 "역상 저항성"이다. 올바르게는 "주어진 x에 대한 약한 충돌 저항성"이다.
③ O. 특정 메시지 x가 주어진 상태에서 $H(y) = H(x), y \neq x$인 y를 찾기 어렵다는 정의와 정확히 일치한다. 이는 제2역상 저항성이라고도 하며, 이 문항에서는 약한 충돌 저항성으로 표현하였다.
④ X. 강한 충돌 저항성은 공격자가 x와 y를 모두 자유롭게 골라 $H(x) = H(y)$인 임의의 충돌쌍을 찾기 어려운 성질이다. 문제는 x가 이미 고정되어 있으므로 강한 충돌 저항성보다 범위가 좁다. 틀린 표현은 "강한"이다. 올바르게는 "약한 충돌 저항성"이다.

NoteBase

오답 포인트

역상 저항성과 약한 충돌 저항성은 모두 "찾기 어렵다"는 표현이 들어가서 혼동되지만, 해시값만 주어졌는지 아니면 입력 x가 미리 고정되었는지가 핵심 구분점이다. 또 약한 충돌 저항성과 강한 충돌 저항성은 충돌쌍의 한쪽을 문제에서 고정해 주는지 여부로 갈린다.

다시 나오면 이렇게 판단

먼저 문제에서 무엇이 주어졌는지 확인하면 된다. 해시값만 주어지면 역상 저항성, 특정 입력 x가 주어지면 약한 충돌 저항성, 두 입력을 모두 스스로 찾아야 하면 강한 충돌 저항성으로 판단한다.

암기 포인트

해시값만 주어지면 역상, x가 고정되면 약한 충돌, 둘 다 자유로우면 강한 충돌이다.

NoteBase

문 12. ㉠~㉢에 들어갈 윈도우 운영체제 보안 컴포넌트를 모두 바르게 제시한 것은?

(㉠)은 로컬 사용자에 관련된 보안 정보 및 계정 데이터를 저장하는 데이터베이스이다.
(㉡)은 커널 모드에서 수행되며, 사용자나 프로세스가 어떤 객체를 열려고 시도하면, 접근 권한을 확인한다.
(㉢)는 사용자 모드에서 수행되며, 로컬 보안 정책을 집행하는 책임이 있다.

① ㉠: SAM, ㉡: SRM, ㉢: LSA

② ㉠: SRM, ㉡: SAM, ㉢: LSA

③ ㉠: SAM, ㉡: SRM, ㉢: SID

④ ㉠: SRM, ㉡: SAM, ㉢: SID

정답 1번

출제 포인트

이 문제는 윈도우 운영체제 보안 컴포넌트의 역할과 실행 모드를 정확히 구분하는지를 묻는 문제이다.

핵심 개념

SAM은 로컬 사용자 계정과 관련된 보안 정보를 저장하는 계정 데이터베이스이다.
SRM은 커널 모드에서 동작하며 객체 접근 요청이 들어오면 접근 권한을 검사하는 보안 참조 모니터이다.
LSA는 사용자 모드에서 동작하며 로그온 검증, 감사, 로컬 보안 정책 적용을 담당하는 보안 서브시스템이다.
SID는 사용자나 그룹을 구별하는 보안 식별자이며, 보안 정책을 집행하는 실행 컴포넌트가 아니다.

NoteBase

선지별 해설

① O
(ㄱ)=SAM, (ㄴ)=SRM, (ㄷ)=LSA의 대응이 모두 맞다. SAM은 계정 데이터베이스이고, SRM은 커널 모드 접근 통제 모듈이며, LSA는 사용자 모드에서 보안 정책을 집행한다.

② X
틀린 부분은 (ㄱ)=SRM, (ㄴ)=SAM이라는 대응이다. SRM은 데이터베이스가 아니라 커널 모드 접근 통제 컴포넌트이고, SAM이 계정 정보를 저장하는 데이터베이스이다. (ㄷ)=LSA는 맞지만 앞의 두 대응이 틀려 오답이다.

③ X
틀린 부분은 (ㄷ)=SID라는 대응이다. SID는 사용자나 그룹에 부여되는 식별값일 뿐 로컬 보안 정책을 집행하는 사용자 모드 컴포넌트가 아니다. 올바르게는 (ㄷ)=LSA이다.

④ X
틀린 부분은 (ㄱ)=SRM, (ㄴ)=SAM, (ㄷ)=SID라는 대응 전부이다. (ㄱ)은 SAM이어야 하고, (ㄴ)은 SRM이어야 하며, (ㄷ)은 LSA이어야 한다.

오답 포인트

SAM, SRM, LSA, SID가 모두 약어라서 저장소, 참조 모니터, 보안 서브시스템, 식별자를 서로 바꿔 기억하기 쉽다. 특히 SID를 보안 기능을 수행하는 모듈로 착각하거나, SRM과 SAM의 역할을 뒤집으면 오답이 된다.

다시 나오면 이렇게 판단

저장하는가, 검사하는가, 정책을 집행하는가, 단순 식별자인가의 축으로 나누면 된다. 계정 정보를 저장하면 SAM, 커널에서 접근 권한을 검사하면 SRM, 사용자 모드에서 보안 정책과 로그온을 담당하면 LSA, 주체를 나타내는 식별값이면 SID이다.

암기 포인트

SAM은 저장소, SRM은 심사, LSA는 정책 집행, SID는 식별자이다.

NoteBase

문 13. 다음의 블록암호 운용모드 중, 암호 과정에서는 암호화 함수 E를, 복호 과정에서는 E와 다른 복호화 함수 D를 필요로 하는 것만을 모두 고르면?

ㄱ. ECB ㄴ. CBC ㄷ. CFB ㄹ. OFB

① ㄱ

② ㄱ, ㄴ

③ ㄷ, ㄹ

④ ㄱ, ㄴ, ㄹ

정답 2번

출제 포인트

이 문제는 블록암호 운용모드별로 복호 과정에서 암호화 함수 *E* 대신 별도의 복호화 함수 *D*가 필요한지 비교하는 문제이다.

핵심 개념

ECB는 각 평문 블록을 그대로 블록암호에 넣어 암호문을 만드는 모드이므로 복호 때는 해당 암호문 블록에 *D*를 적용한다.
CBC는 평문에 이전 암호문 블록을 XOR한 뒤 *E*를 적용하는 모드이므로 복호 때는 먼저 현재 암호문 블록에 *D*를 적용한 뒤 이전 암호문 블록과 XOR한다.
CFB는 블록암호의 출력으로 피드백 값을 만들어 평문 또는 암호문과 XOR하는 모드이므로 암복호 모두 *E*를 사용한다.
OFB는 블록암호 출력으로 키스트림을 계속 생성해 XOR하는 모드이므로 암복호 모두 *E*를 사용한다.
결정 차이축은 복호 시 암호문 블록 자체를 되돌리기 위해 *D*가 필요한지, 아니면 *E*로 생성한 출력과 XOR만 하면 되는지이다.

선지별 해설

1번 X: ㄱ만 고른 것이 틀렸다. ECB는 복호에 *D*가 필요하지만 CBC도 복호 과정에서 현재 암호문 블록에 *D*를 적용해야 하므로 빠지면 안 된다. 올바르게는 'ㄱ, ㄴ'이다.
2번 O: ㄱ ECB와 ㄴ CBC는 모두 복호 과정에서 *E*와 다른 복호화 함수 *D*가 필요하므로 맞다.
3번 X: ㄷ, ㄹ을 고른 것이 틀렸다. CFB와 OFB는 스트림처럼 동작하여 복호 때도 *E*의 출력과 XOR만 사용하므로 별도의 *D*가 필요하지 않다. 올바르게는 'CFB와 OFB는 제외한다'이다.
4번 X: 'ㄱ, ㄴ, ㄹ'에서 ㄹ이 틀렸다. OFB는 키스트림 생성에 *E*만 반복 사용하므로 ECB, CBC와 달리 복호 함수 *D*가 필요하지 않다. 올바르게는 'ㄱ, ㄴ'이다.

NoteBase

오답 포인트

CFB와 OFB도 이름에 '복호'가 들어가므로 당연히 D를 쓸 것처럼 착각하기 쉽다. 그러나 두 모드는 블록암호를 직접 복호하는 구조가 아니라 E로 만든 출력과 XOR하는 구조라는 점이 함정이다.

다시 나오면 이렇게 판단

운용모드를 보면 먼저 '복호 시 현재 암호문 블록을 원래 블록으로 되돌리는 단계가 있는가'를 본다. 그런 단계가 있으면 ECB, CBC처럼 D가 필요하고, 키스트림이나 피드백 출력을 XOR하는 구조이면 CFB, OFB처럼 암복호 모두 E를 사용한다.

암기 포인트

ECB·CBC는 블록을 되돌리므로 D가 필요하고, CFB·OFB는 스트림처럼 흘리므로 E만 쓴다.

NoteBase

문 14. 「개인정보 보호법」상 '정보주체의 권리 보장'에 대한 설명으로 옳지 않은 것은?

① 정보주체는 개인정보처리자가 처리하는 자신의 개인정보에 대한 열람을 해당 개인정보처리자에게 요구할 수 있다.

② 자신의 개인정보를 열람한 정보주체는 개인정보처리자에게 그 개인정보의 정정 또는 삭제를 요구할 수 있다. 다만, 다른 법령에서 그 개인정보가 수집 대상으로 명시되어 있는 경우에는 개인정보 보호위원회의 심의를 거쳐 요구할 수 있다.

③ 개인정보처리자는 정보주체가 열람등요구를 할 수 있는 구체적인 방법과 절차를 마련하고, 이를 정보주체가 알 수 있도록 공개하여야 한다.

④ 개인정보처리자는 정보주체가 열람등요구에 대한 거절 등 조치에 대하여 불복이 있는 경우 이의를 제기할 수 있도록 필요한 절차를 마련하고 안내하여야 한다.

정답 2번

쟁점

이 문제는 「개인정보 보호법」상 정보주체의 열람권, 정정·삭제권, 그리고 열람등요구 절차 보장 의무를 정확히 구별하는 문제이다.

용어 풀이

정보주체는 개인정보의 주체가 되는 사람이다.
열람등요구는 열람, 정정·삭제, 처리정지 등 자신의 개인정보와 관련한 권리행사를 말한다.

핵심 구분

열람은 자신의 개인정보를 확인하게 하는 권리이고, 정정·삭제는 열람 후 잘못된 개인정보를 바로잡거나 지우게 하는 권리이다.
원칙적으로 정보주체는 열람 후 정정 또는 삭제를 요구할 수 있다. 다만 다른 법령에서 그 개인정보를 수집 대상으로 명시한 경우에는 정정은 가능할 수 있어도 삭제는 요구할 수 없다.
또한 열람등요구 절차의 마련·공개와 불복 절차 안내는 개인정보처리자의 의무이다.

NoteBase

선지별 해설

1번 O: 정보주체는 개인정보처리자가 처리하는 자신의 개인정보에 대한 열람을 해당 개인정보처리자에게 요구할 수 있으므로 옳다. 열람권의 기본 내용 자체를 그대로 서술한 문장이다.
2번 X: '다른 법령에서 그 개인정보가 수집 대상으로 명시되어 있는 경우에는 개인정보 보호위원회의 심의를 거쳐 요구할 수 있다'는 부분이 틀렸다. 다른 법령에서 수집 대상으로 명시된 경우에는 삭제를 요구할 수 없는 것이 원칙이고, 보호위원회 심의를 거쳐 삭제를 요구하는 구조가 아니다. 올바르게는 '다른 법령에서 그 개인정보가 수집 대상으로 명시되어 있는 경우에는 그 삭제를 요구할 수 없다'이다.
3번 O: 개인정보처리자는 정보주체가 열람등요구를 할 수 있는 구체적인 방법과 절차를 마련하고 공개하여야 하므로 옳다. 정보주체가 실제로 권리를 행사할 수 있게 절차를 외부에 드러내는 의무를 말한다.
4번 O: 개인정보처리자는 열람등요구에 대한 거절 등 조치에 불복이 있는 경우 이의를 제기할 수 있도록 필요한 절차를 마련하고 안내하여야 하므로 옳다. 권리행사를 막는 것이 아니라 불복 절차까지 보장해야 한다는 취지이다.

오답 포인트

2번은 '다른 법령에서 수집 대상으로 명시된 경우'라는 예외 문구를 보여 준 뒤 '보호위원회 심의'라는 다른 조문 계열의 표현을 끼워 넣은 것이 함정이다. 삭제 제한 규정과 목적 외 이용·제공의 예외 심의 구조를 섞으면 틀리게 된다.

다시 나오면 이렇게 판단

정보주체 권리 문제는 먼저 열람, 정정·삭제, 처리정지 중 어떤 권리를 묻는지 나눈다. 그다음 예외 문구가 나오면 '삭제 자체가 금지되는 예외인지', '절차를 마련·공개해야 하는 개인정보처리자의 의무인지'를 구별하면 정답이 갈린다.

암기 포인트

열람은 요구할 수 있고, 열람 후 정정·삭제를 요구할 수 있으나 법령상 수집대상이면 삭제는 막힌다.

NoteBase

문 15. 패스워드를 이용해서 원격 사용자를 인증하는 경우, 호스트는 비표(nonce)라는 일회성 임의 숫자 r를 생성하고 이와 함께 두 함수 h()와 f()를 사용자에게 제시한다. 사용자는 이에 대한 응답으로 f(r', h(P'))를 반환한다. 호스트는 r' = r, h(P') = h(사용자 패스워드)의 여부를 판단하여 인증을 완료한다. 이때, r를 사용하는 것은 어떤 공격에 대비하기 위한 것인가?

① 전사 공격(Brute-Force Attack)

② 트래픽 스니핑 공격(Traffic Sniffing Attack)

③ 패스워드 사전 공격(Password Dictionary Attack)

④ 재전송 공격(Replay Attack)

정답 4번

출제 포인트

이 문제는 일회성 난수인 nonce의 역할과 각 공격 유형의 목적을 구별하는지를 묻는 문제이다.

핵심 개념

nonce는 매 인증 때마다 새로 생성하는 일회성 임의값으로, 이전에 만든 응답을 다시 보내도 통하지 않게 하는 신선성 확인 값이다.
재전송 공격은 과거의 정상 메시지나 인증 응답을 가로채 그대로 다시 보내 인증을 우회하려는 공격이다.
전사 공격은 가능한 값을 전부 대입하는 공격이고, 트래픽 스니핑은 네트워크를 엿들어 데이터를 수집하는 공격이며, 사전 공격은 자주 쓰는 비밀번호 후보를 중심으로 추측하는 공격이다.

NoteBase

선지별 해설

① X
전사 공격은 가능한 비밀번호를 무차별 대입하는 공격이다. nonce를 넣는다고 비밀번호 후보의 수가 줄어들거나 탐색 공간이 커지는 것은 아니므로 전사 공격 자체를 막기 위한 장치는 아니다.
틀린 표현은 "r를 사용하는 것은 전사 공격에 대비"라는 부분이다. 올바르게는 "r를 사용하는 것은 매 세션 응답의 재사용을 막기 위한 것"이다.

② X
트래픽 스니핑은 통신 내용을 도청하는 공격이다. nonce를 써도 공격자는 패킷 자체를 볼 수 있으므로 스니핑 자체가 막히는 것은 아니다. 이 값의 핵심 역할은 도청 방지보다 응답의 일회성 보장에 있다.
틀린 표현은 "r를 사용하는 것은 트래픽 스니핑 공격에 대비"라는 부분이다. 올바르게는 "r를 사용해 스니핑으로 획득한 과거 응답을 그대로 재사용하지 못하게 한다"이다.

③ X
사전 공격은 사전에 있는 비밀번호 후보를 대입해 맞추는 공격이다. nonce의 직접 목적은 비밀번호 추측을 어렵게 만드는 것이 아니라 이전 인증 응답을 재사용하지 못하게 하는 것이다.
틀린 표현은 "r를 사용하는 것은 패스워드 사전 공격에 대비"라는 부분이다. 올바르게는 "r를 사용하는 것은 인증 응답의 신선성을 확인해 재전송을 막기 위한 것"이다.

④ O
재전송 공격은 예전에 캡처한 정상 응답을 다시 보내 인증을 통과하려는 공격이다. 호스트가 매번 새로운 nonce r를 보내면 사용자의 응답은 그 r에 종속되므로, 과거 응답을 다시 보내도 현재의 r와 맞지 않아 인증에 실패한다.

오답 포인트

challenge-response에서 해시 함수와 비밀번호만 보이면 사전 공격이나 도청 방지를 먼저 떠올리기 쉽다. 그러나 이 문항은 "왜 nonce를 따로 넣는가"를 묻기 때문에, 핵심은 비밀번호 은닉이 아니라 응답의 재사용 차단이다.

다시 나오면 이렇게 판단

프로토콜에 nonce, timestamp, sequence number처럼 매번 바뀌는 신선성 값이 들어가면 먼저 재전송 공격 방어 장치인지 본다. 과거 메시지를 그대로 다시 써도 통하지 않게 만드는 요소이면 replay 대응으로 판단한다.

암기 포인트

nonce는 일회성 값, 핵심 기능은 신선성 확인, 대표 방어 대상은 재전송 공격이다.

NoteBase

문 16. HTTP 버전 1.1에 대한 설명으로 옳지 않은 것은?

① TCP를 전송 프로토콜로 사용한다.

② 요청 메시지의 첫 줄인 요청 라인에는 메소드, URL, HTTP 버전 필드가 포함된다.

③ 요청과 그에 대한 응답이 같은 연결로 보내지는 지속 연결(persistent connection)을 기본으로 하며, 분리된 별도의 연결을 이용하는 비지속 연결(non-persistent connection)도 지원한다.

④ HTTP 서버가 클라이언트에 대한 정보를 유지하는 상태(stateful) 프로토콜이다.

정답 4번

출제 포인트

이 문제는 HTTP 1.1의 전송 계층 사용 방식, 요청 라인 구성, 지속 연결, 무상태성의 차이를 정확히 구분하는지를 묻는다.

핵심 개념

HTTP는 웹에서 요청과 응답 형식을 정한 응용 계층 프로토콜이며 일반적으로 TCP 위에서 동작한다.
HTTP 1.1의 요청 라인은 메서드, 요청 대상 URL 또는 URI, HTTP 버전으로 구성된다.
지속 연결은 한 TCP 연결을 여러 요청과 응답에 재사용하는 방식이고, 무상태성은 서버가 기본적으로 클라이언트의 이전 상태를 저장하지 않는 성질이다.

선지별 해설

1번 O: HTTP 1.1은 일반적으로 TCP를 전송 계층 프로토콜로 사용한다. 신뢰성 있는 연결 지향 전송 위에서 요청과 응답을 주고받는다는 설명이므로 옳다.
2번 O: HTTP 요청 메시지의 첫 줄인 요청 라인은 메서드, 요청 대상, HTTP 버전으로 이루어진다. 선지의 URL은 요청 대상을 가리키는 표현으로 이해할 수 있으므로 옳다.
3번 O: HTTP 1.1은 지속 연결을 기본으로 하여 같은 연결에서 여러 요청과 응답을 처리할 수 있다. 필요하면 별도 연결을 매 요청마다 쓰는 비지속 연결 방식도 사용할 수 있다는 취지이므로 옳다.
4번 X: 틀린 표현은 "상태(stateful) 프로토콜"이다. HTTP 자체는 서버가 클라이언트 상태를 기본적으로 유지하지 않는 무상태(stateless) 프로토콜이다. 상태 유지가 필요하면 쿠키, 세션 같은 별도 메커니즘을 추가로 사용한다.

오답 포인트

지속 연결과 상태 유지를 같은 개념으로 섞으면 4번에 속기 쉽다. 연결을 오래 유지하는 것은 TCP 연결 재사용에 관한 성질이고, 상태성은 서버가 이전 요청의 문맥을 기억하는지에 관한 성질이므로 서로 다른 축의 개념이다.

NoteBase

다시 나오면 이렇게 판단

HTTP 문제에서는 먼저 계층과 기본 성질을 분리해 본다. TCP 사용 여부는 전송 방식, persistent connection은 연결 재사용, stateless는 서버의 상태 기억 여부로 나누어 판단하면 선지가 빠르게 정리된다.

암기 포인트

HTTP 1.1은 기본 지속 연결이고, HTTP 자체는 무상태이다.

NoteBase

문 17. 서버가 응용 메시지를 여러 개의 TCP 세그먼트로 나누어 클라이언트에게 전송하는 경우, TCP의 동작에 대한 설명으로 옳은 것은?

① 클라이언트와 서버 간의 TCP 연결 설정 후, 첫 번째 세그먼트의 순서 번호는 일반적으로 0부터 시작한다.

② 두 번째 세그먼트의 순서 번호는 첫 번째 세그먼트가 운반에 성공한 데이터의 바이트 수를 첫 번째 세그먼트의 순서 번호에 더한 것이다.

③ 일정량의 데이터를 포함한 세그먼트를 정상적으로 수신한 클라이언트는 수신한 세그먼트의 순서 번호에 1을 더한 값을 확인응답 번호로 하여 응답하고 다음 세그먼트를 기다린다.

④ 클라이언트가 FIN 세그먼트를 보내고 서버가 이에 대한 ACK 세그먼트를 보냄으로써 서버의 데이터 전송을 위한 연결이 완전히 종료된다.

정답 2번

출제 포인트

이 문제는 TCP가 바이트 단위 순서 번호와 확인응답 번호를 어떻게 계산하는지, 그리고 FIN이 연결의 어느 방향만 종료시키는지를 묻는 문제이다.

핵심 개념

TCP는 세그먼트 개수 기준이 아니라 바이트 기준으로 순서 번호와 확인응답 번호를 관리한다.
순서 번호는 해당 세그먼트 데이터의 첫 바이트 번호이며, 다음 세그먼트의 순서 번호는 이전 세그먼트의 순서 번호에 전송한 데이터 바이트 수를 더해 정해진다.
확인응답 번호는 방금 받은 세그먼트 번호가 아니라 다음에 받기를 기대하는 바이트 번호이다.
FIN은 연결 전체를 즉시 끊는 신호가 아니라 한 방향의 데이터 전송 종료를 알리는 제어 비트이다.

NoteBase

선지별 해설

① X: TCP의 초기 순서 번호는 일반적으로 0으로 고정되지 않는다. 연결마다 초기 순서 번호가 정해지며 첫 데이터 세그먼트는 그 값부터 시작한다. 틀린 표현은 "일반적으로 0부터 시작한다"이다. 올바르게는 "첫 번째 세그먼트의 순서 번호는 연결 시 정해진 초기 순서 번호부터 시작한다"이다.
② O: TCP는 바이트 스트림 프로토콜이므로 두 번째 세그먼트의 순서 번호는 첫 번째 세그먼트의 순서 번호에 첫 번째 세그먼트가 실은 데이터 바이트 수를 더한 값이 된다. 세그먼트 개수가 아니라 누적 바이트 수로 다음 순서 번호가 정해진다.
③ X: 확인응답 번호는 수신한 세그먼트의 순서 번호에 1을 더한 값이 아니라 다음에 기대하는 바이트 번호이다. 따라서 데이터가 여러 바이트이면 ACK는 그 데이터 길이만큼 증가한다. 틀린 표현은 "순서 번호에 1을 더한 값"이다. 올바르게는 "수신한 데이터 바이트 수만큼 더한 다음 기대 바이트 번호를 확인응답 번호로 보낸다"이다.
④ X: 클라이언트가 FIN을 보내고 서버가 ACK를 보내면 클라이언트에서 서버로 가는 방향만 닫힌다. 서버는 아직 남은 데이터를 보낼 수 있으며, 연결이 완전히 종료되려면 서버도 FIN을 보내고 클라이언트가 이에 ACK해야 한다. 틀린 표현은 "연결이 완전히 종료된다"이다. 올바르게는 "그 단계에서는 한쪽 방향의 종료만 확인되며 전체 종료에는 서버의 FIN과 이에 대한 ACK가 추가로 필요하다"이다.

오답 포인트

세그먼트마다 번호가 하나씩 올라간다고 생각하면 ③처럼 ACK를 1씩 증가시키는 것으로 오해하기 쉽다. 그러나 TCP는 패킷 번호가 아니라 바이트 번호를 관리한다. 또한 ④처럼 FIN과 ACK 한 번이면 연결 전체가 끝난다고 착각하기 쉬우나, TCP 종료는 양방향을 따로 닫는 절차이다.

다시 나오면 이렇게 판단

TCP 관련 선지는 먼저 바이트 기준인지 세그먼트 기준인지부터 구분하면 된다. 순서 번호와 ACK 번호가 나오면 다음 바이트 번호를 묻는지 확인하면 된다. FIN이 나오면 그 순간 닫히는 것이 한 방향인지 전체 연결인지 구분하면 된다.

암기 포인트

TCP는 세그먼트가 아니라 바이트를 센다. ACK는 다음에 받을 바이트 번호이고, FIN 하나로는 연결 전체가 끝나지 않는다.

NoteBase

문 18. 다음에서 설명하는 네트워크 기반 공격 방법은?

◯ TCP 헤더 정보를 보고 패킷을 걸러내는 방화벽을 우회하기 위한 공격 방법이다.
◯ IP 단편 옵션을 이용하여 매우 작게 패킷을 나누어서 TCP 헤더 자체가 분리되도록 만든다.
◯ 일부 패킷 필터는 첫 번째 단편만 검사하고, 나머지 단편은 모두 통과시키기 때문에 이러한 공격 방법이 유효할 수 있다.

① Source Routing Attack
② Ping of Death
③ Trinoo
④ Tiny Fragment Attack

정답 4번

출제 포인트

이 문제는 IP 단편화를 이용해 TCP 헤더 검사 기반의 패킷 필터링 방화벽을 우회하는 Tiny Fragment Attack의 개념을 묻는 문제이다.

핵심 개념

Tiny Fragment Attack은 IP 단편화를 악용해 패킷을 매우 작은 조각으로 나누고 TCP 헤더 정보를 분리하여 필터가 첫 단편만 검사하는 허점을 노리는 공격이다.
Source Routing Attack은 송신자가 패킷의 경로를 지정하는 IP 옵션을 악용하는 공격이다.
Ping of Death는 재조립 결과가 비정상적으로 큰 ICMP 패킷이 되도록 만들어 시스템 오류를 유발하는 공격이다.
Trinoo는 다수의 좀비 호스트를 이용해 대량 트래픽을 보내는 DDoS 도구 계열이다.

NoteBase

선지별 해설

① X: Source Routing Attack은 IP 옵션으로 경로를 지정하거나 우회하는 공격이다. 제시문처럼 매우 작은 단편으로 TCP 헤더를 분리해 방화벽 검사를 피하는 방식이 아니다. 틀린 표현은 Source Routing Attack이다. 올바르게는 Tiny Fragment Attack이다.
② X: Ping of Death는 비정상적으로 큰 패킷을 재조립하게 만들어 오류를 일으키는 공격이다. 첫 번째 단편만 검사하는 패킷 필터의 허점을 노리는 방화벽 우회 공격이 아니다. 틀린 표현은 Ping of Death이다. 올바르게는 Tiny Fragment Attack이다.
③ X: Trinoo는 분산 서비스 거부 공격에 쓰이는 도구이다. 패킷을 잘게 쪼개 TCP 헤더를 숨기는 단편화 기반 공격과는 유형이 다르다. 틀린 표현은 Trinoo이다. 올바르게는 Tiny Fragment Attack이다.
④ O: Tiny Fragment Attack은 IP 단편화를 이용해 TCP 헤더가 한 번에 보이지 않게 만들고, 일부 필터가 첫 단편만 검사하는 점을 이용해 통과를 노리는 공격이다. 제시문의 설명과 정확히 일치한다.

오답 포인트

단편화라는 단어만 보고 ② Ping of Death와 혼동하기 쉽다. 그러나 이 문항의 핵심은 시스템 장애 유발이 아니라 TCP 헤더 검사 회피와 방화벽 우회이다. ①은 경로 지정, ③은 DDoS 도구라는 점에서 공격 목적과 수단이 전혀 다르다.

다시 나오면 이렇게 판단

문장에 IP 단편화, 매우 작은 조각, TCP 헤더 분리, 첫 단편만 검사, 패킷 필터 우회가 함께 나오면 Tiny Fragment Attack으로 판단한다. 반대로 비정상적으로 큰 패킷이면 Ping of Death, 경로 지정이면 Source Routing, 다수 에이전트 기반 대량 트래픽이면 Trinoo로 구분한다.

암기 포인트

Tiny Fragment Attack은 작은 단편으로 TCP 헤더를 쪼개 방화벽 검사를 비껴 가는 공격이다.

NoteBase

문 19. 다음은 「정보보호산업의 진흥에 관한 법률」상 정보보호산업의 활성화를 위한 구매수요정보의 제공에 관한 조항의 일부이다. ㉠, ㉡에 들어갈 용어를 바르게 연결한 것은?

「전자정부법」 제2조제2호에 따른 행정기관 또는 공공기관의 장은 소관 기관·시설의 정보보호 수준을 강화하기 위하여 (㉠) 정보보호기술등에 대한 구매수요 정보를 (㉡)에게 제출하여야 한다.

① ㉠: 매년, ㉡: 과학기술정보통신부장관

② ㉠: 매년, ㉡: 행정안전부장관

③ ㉠: 2년마다, ㉡: 과학기술정보통신부장관

④ ㉠: 2년마다, ㉡: 행정안전부장관

정답 1번

쟁점

이 문제는 정보보호기술등 구매수요정보의 제출 주기와 제출 상대 기관을 구별하는 문제이다.
핵심은 법 제6조의 제출의무 주체와 시행령 제4조의 제출시기를 함께 맞추는 데 있다.

용어 풀이

구매수요정보 = 행정기관 또는 공공기관이 정보보호기술등을 언제 어떤 규모로 도입하려는지에 관한 수요 정보이다.

핵심 구분

원칙적으로 행정기관 또는 공공기관의 장은 구매수요정보를 소관 부처가 아닌 과학기술정보통신부장관에게 제출한다.
제출 시기는 2년마다가 아니라 매년이며, 시행령상 해당 연도분과 다음 연도분을 각각 연중 정해진 기한까지 제출하는 구조이다.

NoteBase

선지별 해설

① O
매년 제출하고 제출 상대방도 과학기술정보통신부장관이므로 옳다. 법은 구매수요정보 제출의무를 두고, 시행령은 이를 매년 제출하도록 구체화한다.

② X
제출 주기인 '매년'은 맞지만 제출 상대방이 틀리다.
틀린 표현: 행정안전부장관
올바른 표현: 과학기술정보통신부장관

③ X
제출 상대방인 과학기술정보통신부장관은 맞지만 제출 주기가 틀리다.
틀린 표현: 2년마다
올바른 표현: 매년

④ X
제출 주기와 제출 상대방이 모두 틀리다.
틀린 표현: 2년마다, 행정안전부장관
올바른 표현: 매년, 과학기술정보통신부장관

오답 포인트

이 문제를 틀렸다면 정보보호 관련 총괄 부처를 행정안전부로 착각했거나, 정기 제출주기를 중장기 계획 주기처럼 2년 단위로 오인했을 가능성이 높다. 보기 조합형 문항에서는 한 요소만 맞아도 정답처럼 보이는 착시가 생긴다.

다시 나오면 이렇게 판단

법령형 조합 문항에서는 먼저 주체와 제출 상대방을 확인하고, 다음으로 기간이나 횟수 문구를 분리해서 본다. 한 보기 안에 두 요소가 섞여 있으면 둘 다 맞아야 정답이 된다.

암기 포인트

구매수요정보는 매년 제출하고, 제출처는 과기정통부장관이다.

NoteBase

문 20. IEEE 802.11i에서 정의한 무선 랜 데이터 보안 프로토콜로, 메시지 무결성 코드(MIC)와 RC4 암호 알고리즘을 이용하여 메시지 무결성과 데이터 기밀성을 제공하는 것은?

① EAP

② WEP

③ CCMP

④ TKIP

정답 4번

출제 포인트

IEEE 802.11i에서 EAP, WEP, CCMP, TKIP의 역할과 사용하는 암호 방식의 차이를 구별하는 문제이다.

핵심 개념

EAP는 무선 접속에서 사용자 인증을 위한 확장 인증 프레임워크이다.
WEP는 초기 무선랜 보안 방식으로 RC4와 ICV를 사용하지만 무결성 보호가 약하다.
CCMP는 AES 기반의 블록 암호 모드로 기밀성과 무결성을 제공한다.
TKIP는 WEP의 약점을 보완하기 위해 RC4에 키 혼합과 MIC를 추가한 과도기적 보안 프로토콜이다.

선지별 해설

1번 X: EAP는 인증 절차를 위한 프레임워크이지 데이터 암호화와 무결성 보호를 직접 담당하는 무선 랜 데이터 보안 프로토콜이 아니다. 틀린 표현은 "데이터 보안 프로토콜"이다. 올바르게는 인증 프레임워크이다.
2번 X: WEP는 RC4를 사용하므로 기밀성은 일부 제공하지만, 문제에서 말한 MIC를 사용하지 않는다. 틀린 표현은 "무결성 코드(MIC)와 RC4"이다. 올바르게는 RC4와 ICV를 사용하는 초기 보안 방식이다.
3번 X: CCMP는 기밀성과 무결성을 제공하는 것은 맞지만 RC4가 아니라 AES 기반으로 동작한다. 틀린 표현은 "RC4 암호 알고리즘"이다. 올바르게는 AES 기반의 CCMP이다.
4번 O: TKIP는 IEEE 802.11i에서 정의된 과도기적 무선 랜 보안 프로토콜로, MIC와 RC4를 함께 사용하여 메시지 무결성과 데이터 기밀성을 제공한다.

오답 포인트

WEP와 TKIP가 모두 RC4를 쓴다는 점 때문에 2번과 4번이 헷갈리기 쉽다. 이 문제의 결정 단서는 MIC 포함 여부이며, MIC를 추가한 것은 TKIP이다.

다시 나오면 이렇게 판단

먼저 인증 프로토콜인지 데이터 보호 프로토콜인지 구분한다. 그다음 RC4 기반인지 AES 기반인지 보고, RC4에 MIC까지 붙으면 TKIP, RC4만 떠오르면 WEP, AES 기반이면 CCMP로 판단한다.

NoteBase

암기 포인트

EAP는 인증, WEP는 RC4, TKIP는 RC4+MIC, CCMP는 AES이다.

NoteBase