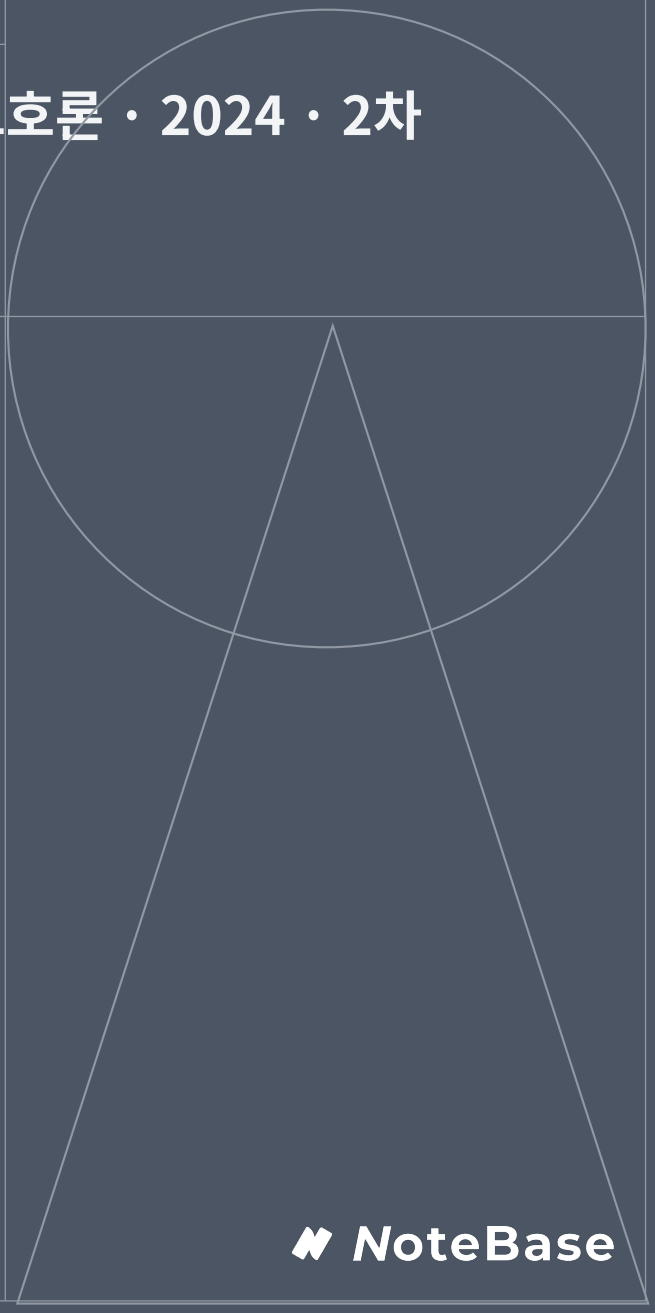
기출OX 해설집

공무원/국가직/7급 · 정보보호론 · 2024 · 2차



NoteBase

기출OX 해설집

공무원/국가직/7급 · 정보보호론 · 2024 · 2차

공무원/국가직/7급 · 정보보호론 · 2024 · 2차

문 1. 다음에서 설명하는 디지털 포렌식의 기본 원칙은?

증거는 절차를 통해 삭제 또는 손상된 파일이 복구되는 과정을 거칠 수 있다. 이 증거를 법정에 제출하려면 같은 환경에서 같은 결과가 나와야 한다.

① 재현의 원칙
② 신속성의 원칙
③ 무결성의 원칙
④ 연계 보관성의 원칙

정답 1번

출제 포인트

이 문제는 디지털 포렌식의 기본 원칙 중 재현의 원칙이 무엇인지 묻는 문제이다.

핵심 개념

재현의 원칙은 같은 데이터와 같은 절차를 적용하면 같은 결과가 나와야 한다는 원칙이다. 무결성의 원칙은 수집·분석 과정에서 증거가 변조되지 않아야 한다는 원칙이다. 연계 보관성의 원칙은 증거를 누가 언제 어떻게 취급했는지의 이력을 끊기지 않게 관리하는 원칙이다. 신속성의 원칙은 휘발성 높은 디지털 증거를 늦지 않게 확보하는 원칙이다.

NoteBase

선지별 해설

① O: 제시문은 삭제·손상된 파일을 일정한 절차로 복구하고, 같은 환경에서 같은 결과가 나와야 법정 증거로 활용될 수 있다고 설명한다. 이는 동일한 조건에서 동일한 결과가 반복되어야 한다는 재현의 원칙에 해당한다.
② X: 틀린 부분은 '신속성'이다. 신속성의 원칙은 시스템 종료 전 메모리나 로그처럼 사라지기 쉬운 증거를 빠르게 확보해야 한다는 뜻이며, 같은 환경에서 같은 결과가 나오는지와는 관련이 없다. 올바르게는 '같은 환경에서 같은 결과가 나와야 한다'는 설명은 재현의 원칙이다.
③ X: 틀린 부분은 '무결성'이다. 무결성의 원칙은 원본 증거가 수집·이동·분석 과정에서 변경되지 않았음을 보장하는 데 초점이 있다. 올바르게는 제시문의 핵심은 변조 방지 자체가 아니라 동일 절차에서 동일 결과가 재현되는지이므로 재현의 원칙이다.
④ X: 틀린 부분은 '연계 보관성'이다. 연계 보관성의 원칙은 증거의 소유·보관·이송·분석 이력을 문서화해 증거능력을 유지하는 것이다. 올바르게는 제시문은 증거 관리 이력보다 동일 실험 조건에서 동일 결과를 얻는 재현 가능성을 설명한다.

오답 포인트

무결성과 재현의 원칙을 섞어 헷갈리기 쉽다. '증거가 변하지 않아야 한다'는 표현이 나오면 무결성이고, '같은 조건에서 다시 해도 같은 결과가 나와야 한다'는 표현이 나오면 재현이다. 연계 보관성은 보관 이력, 신속성은 확보 시점의 문제이므로 질문의 초점이 다르다.

다시 나오면 이렇게 판단

디지털 포렌식 원칙 문제는 발문의 중심 동사를 먼저 본다. '보존한다, 변조되지 않는다'는 무결성이고, '같은 절차로 같은 결과가 나온다'는 재현이며, '누가 언제 보관했는지 남긴다'는 연계 보관성이고, '빨리 확보한다'는 신속성이다.

암기 포인트

재현은 같은 절차와 같은 결과, 무결성은 원본 보존, 연계 보관성은 보관 이력, 신속성은 휘발성 증거의 즉시 확보이다.

NoteBase

문 2. RSA 공개키 암호에서 공개키를 $(n = 11 \times 13,\ e = 7)$로 설정하였을 때, 공개키에 대응하는 개인키 d 값은?

① 41

② 87

③ 97

④ 103

정답 4번

출제 포인트

이 문제는 RSA에서 오일러 피 함수 $\varphi(n)$를 구한 뒤 공개지수 e의 모듈러 역원인 개인키 d를 찾을 수 있는지를 묻는다.

조건 정리

주어진 값은 $n = 11 \times 13 = 143, e = 7$이다.
구해야 할 값은 공개키 (n, e)에 대응하는 개인키 d이다.
RSA에서는 $\varphi(n) = (11 - 1)(13 - 1) = 10 \times 12 = 120$을 먼저 구해야 한다.

사용할 공식

개인키 d는 ed ≡ 1 ±od(n)를 만족하는 값이다.
이 공식을 쓰는 이유는 RSA 복호화 지수가 공개지수 e의 $\varphi(n)$에 대한 모듈러 역원이기 때문이다.

계산 과정

1. $n = 11 \times 13$이므로 $p = 11, q = 13$이다.
2. $\varphi(n) = (p - 1)(q - 1) = 10 \times 12 = 120$이다.
3. 7d ≡ 1 ±od120을 만족하는 d를 찾으면 된다.
4. 보기 ④를 대입하면 $7 \times 103 = 721$이고, $721 = 120 \times 6 + 1$이므로 721 ≡ 1 ±od120이다.
5. 따라서 $d = 103$이므로 정답은 4번이다.

NoteBase

선지 판단

1번: X. $7 \times 41 = 287$이고 $287 = 120 \times 2 + 47$이므로 $287 \equiv 47 \pm \mathrm{od} 120$이다. 개인키 d를 41로 본 것이 틀렸고, 올바른 값은 103이다.
2번: X. $7 \times 87 = 609$이고 $609 = 120 \times 5 + 9$이므로 $609 \equiv 9 \pm \mathrm{od} 120$이다. $ed \equiv 1$ 조건을 만족하지 못하므로 87은 개인키가 아니고, 올바른 값은 103이다.
3번: X. $7 \times 97 = 679$이고 $679 = 120 \times 5 + 79$이므로 $679 \equiv 79 \pm \mathrm{od} 120$이다. 97을 역원으로 판단한 것이 틀렸고, 올바른 값은 103이다.
4번: O. $7 \times 103 = 721$이며 $721 \equiv 1 \pm \mathrm{od} 120$이므로 공개지수 7의 모듈러 역원이다. 따라서 개인키 d 값은 103이 맞다.

오답 포인트

RSA 개인키 문제에서 가장 흔한 실수는 n 자체를 기준으로 계산하거나 $\varphi(n)$를 빼먹는 것이다. 이 문제도 143이 아니라 120을 법으로 두고 $ed \equiv 1$을 확인해야 한다는 점이 함정이다.

다시 나오면 이렇게 판단

RSA 수치 문제는 소인수분해로 p, q를 확인하고, $\varphi(n) = (p-1)(q-1)$를 구한 뒤, 마지막에 $\mathrm{ed} \equiv 1 \pm \mathrm{od}(\mathrm{n})$ 검산까지 마치면 안정적으로 판단할 수 있다.

암기 포인트

RSA 개인키 d는 공개지수 e의 $\varphi(n)$에 대한 모듈러 역원이다.

NoteBase

문 3. AES의 암호화 과정에서 마지막 라운드에 포함되지 않는 연산은?

① SubBytes

② ShiftRows

③ MixColumns

④ AddRoundKey

정답 3번

출제 포인트

이 문제는 AES 암호화 라운드에서 일반 라운드와 마지막 라운드의 구성 차이를 구별할 수 있는지를 묻는다.

핵심 개념

일반 라운드는 SubBytes, ShiftRows, MixColumns, AddRoundKey의 4단계로 구성된다.
마지막 라운드는 MixColumns를 제외하고 SubBytes, ShiftRows, AddRoundKey만 수행한다.
구별 기준은 열 단위 혼합 연산의 포함 여부이며, 키워드는 마지막 라운드에서는 확산 단계인 MixColumns가 빠진다는 점이다.

선지별 해설

1번 O: SubBytes는 바이트 단위 치환 연산으로 AES의 마지막 라운드에도 포함된다.
2번 O: ShiftRows는 행 단위 순환 이동 연산으로 마지막 라운드에서도 그대로 수행된다.
3번 X: 틀린 부분은 MixColumns가 마지막 라운드에 포함된다고 보는 점이다. 실제로는 MixColumns는 일반 라운드에만 들어가고 마지막 라운드에서는 제외된다.
4번 O: AddRoundKey는 라운드 키를 상태 행렬에 XOR하는 단계로 마지막 라운드에도 포함된다.

오답 포인트

일반 라운드의 4단계를 한 묶음으로 외우면 마지막 라운드도 동일하다고 착각하기 쉽다. 3번은 그 착각을 노린 선지이며, 마지막 라운드만 MixColumns가 빠진다는 예외를 놓치면 오답이 된다.

다시 나오면 이렇게 판단

AES 라운드 구성을 묻는 문제에서는 먼저 마지막 라운드인지 일반 라운드인지 구분한다. 마지막 라운드라면 MixColumns만 제외하고 나머지 세 연산은 유지된다고 판단하면 된다.

암기 포인트

AES 마지막 라운드 = SubBytes, ShiftRows, AddRoundKey이며 MixColumns는 없다.

NoteBase

문 4. 다음 설명에 해당하는 공격 기법은?

브라우저로 전달되는 데이터에 악성 스크립트가 포함되어 사용자의 브라우저에서 실행되면서 해킹이 수행된다. 일반적인 공격 목적은 웹 사용자의 정보를 추출하는 것이다.

① XSS(Cross Site Scripting)
② 리버스 텔넷(Reverse Telnet)
③ 디렉터리 리스팅(Directory Listing)
④ SQL(Structured Query Language) Injection

정답 1번

출제 포인트

이 문제는 웹 공격 기법 중 XSS의 정의와, 원격 접속·서버 노출·DB 질의 조작 공격과의 차이를 구분하는 문제이다.

핵심 개념

XSS는 웹 페이지에 악성 스크립트를 삽입해 사용자의 브라우저에서 실행되게 만드는 공격이다. 결정 차이축은 실행 위치가 브라우저인지, 공격 대상이 웹 사용자 정보인지이다. 키워드는 악성 스크립트, 브라우저 실행, 쿠키·세션 탈취이다.
리버스 텔넷은 대상 시스템이 공격자에게 역방향으로 접속하게 만들어 원격 셸 통로를 여는 방식이다. 키워드는 역접속, 원격 제어이다.
디렉터리 리스팅은 서버 설정 미흡으로 디렉터리 목록과 파일 구조가 노출되는 현상이다. 키워드는 목록 노출, 설정 오류이다.
SQL 인젝션은 입력값에 SQL 구문을 주입해 데이터베이스 질의를 조작하는 공격이다. 키워드는 질의 조작, 데이터베이스 접근이다.

NoteBase

선지별 해설

① O
브라우저로 전달된 데이터에 악성 스크립트가 포함되고, 그 스크립트가 사용자의 브라우저에서 실행되어 정보 탈취가 일어난다는 설명은 XSS의 전형적인 정의와 일치한다.

② X
틀린 부분은 리버스 텔넷으로 본 점이다.
리버스 텔넷은 피해 시스템이 공격자 쪽으로 접속을 열어 원격 제어 통로를 만드는 방식이지, 웹 페이지의 스크립트가 브라우저에서 실행되는 공격이 아니다. 올바르게는 리버스 텔넷은 역방향 원격 접속 공격이다.

③ X
틀린 부분은 디렉터리 리스팅으로 본 점이다.
디렉터리 리스팅은 서버의 폴더·파일 목록이 노출되는 문제이지, 사용자 브라우저에서 악성 스크립트가 실행되는 공격이 아니다. 올바르게는 디렉터리 리스팅은 서버 디렉터리 정보 노출이다.

④ X
틀린 부분은 SQL 인젝션으로 본 점이다.
SQL 인젝션은 입력값을 통해 SQL 문장을 조작하여 데이터베이스를 조회·변조하는 공격이지, 브라우저에서 스크립트를 실행하는 공격이 아니다. 올바르게는 SQL 인젝션은 데이터베이스 질의 조작 공격이다.

오답 포인트

공격 이름에만 반응하면 웹 관련 공격을 모두 비슷하게 보게 된다. 이 문항의 함정은 실행 위치와 직접 대상의 차이를 흐리는 데 있다. 브라우저에서 스크립트가 실행되면 XSS이고, DB 질의가 변형되면 SQL 인젝션이며, 서버 목록이 보이면 디렉터리 리스팅이다.

다시 나오면 이렇게 판단

먼저 악성 코드가 어디에서 실행되는지 본다. 사용자의 브라우저에서 스크립트가 실행되면 XSS로 판단한다. 데이터베이스 명령이 바뀌면 SQL 인젝션, 서버 파일 목록이 드러나면 디렉터리 리스팅, 역방향 접속 통로가 열리면 리버스 텔넷으로 판단한다.

암기 포인트

XSS는 브라우저 스크립트, SQL 인젝션은 DB 질의, 디렉터리 리스팅은 서버 목록 노출, 리버스 텔넷은 역접속 원격 제어이다.

NoteBase

문 5. 리눅스 시스템 명령어와 기능의 설명 중 옳지 않은 것은?

① mv - 파일의 이름 변경과 이동

② chmod - 파일의 사용 권한 변경

③ rm - 파일 및 디렉터리 목록 보기

④ umask - 생성하는 디렉터리의 기본 권한 설정

정답 3번

출제 포인트

이 문제는 리눅스 기본 명령어의 기능을 정확히 대응시키는지 묻는 문제이다.

핵심 개념

mv는 파일이나 디렉터리의 이름을 바꾸거나 위치를 옮기는 명령어이다.
chmod는 파일이나 디렉터리의 접근 권한을 변경하는 명령어이다.
rm은 파일이나 디렉터리를 삭제하는 명령어이다.
umask는 새로 만드는 파일·디렉터리에 적용될 기본 권한 마스크를 정하는 명령어이다.

선지별 해설

① O: mv는 move의 약자로 파일이나 디렉터리의 이름 변경과 이동에 사용된다.
② O: chmod는 읽기·쓰기·실행 권한을 변경하는 명령어이므로 파일의 사용 권한 변경이라는 설명이 맞다.
③ X: 틀린 부분은 "파일 및 디렉터리 목록 보기"이다. rm은 remove의 약자로 파일이나 디렉터리를 삭제하는 명령어이며, 목록을 보는 명령어는 ls이다.
④ O: umask는 새로 생성되는 디렉터리의 기본 권한에 영향을 주는 권한 마스크를 설정한다. 엄밀히는 파일과 디렉터리 모두의 기본 권한 마스크를 정한다.

오답 포인트

rm과 ls를 헷갈리면 ③을 맞는 설명처럼 보기 쉽다. 명령어 철자보다 기능 동사를 먼저 연결하면 혼동이 줄어든다.

다시 나오면 이렇게 판단

리눅스 명령어 문제는 명령어 이름보다 핵심 기능을 먼저 대응시켜 판단한다. mv는 이동·이름 변경, chmod는 권한 변경, rm은 삭제, ls는 목록 확인으로 구분하면 된다.

암기 포인트

mv는 이동, chmod는 권한, rm은 삭제, ls는 목록이다.

NoteBase

문 6. 윈도 명령 프롬프트 창에서 명령어 (가)를 실행한 화면의 일부이다. 이에 대한 설명으로 옳지 않은 것은? (단, 게이트웨이의 IP 주소는 172.21.70.1이고, 공격자의 IP 주소는 172.21.70.227이다)

C:\Users\windows> (가)

Interface: 172.21.70.180 --- 0xb
Internet Address Physical Address Type
172.21.70.1 18-67-e0-4d-40-5c dynamic
172.21.70.2 00-0c-db-58-27-2d dynamic
172.21.70.227 18-67-e0-4d-40-5c dynamic
172.21.70.253 00-0e-5e-fc-16-c4 dynamic

① 명령어 (가)는 arp -a이다.
② 게이트웨이의 ARP 테이블을 보여주는 화면이다.
③ 공격 대상의 IP 주소는 172.21.70.180임을 나타낸다.
④ 게이트웨이의 MAC 주소와 공격자의 MAC 주소가 같은 상태이다.

정답 2번

출제 포인트

이 문제는 윈도우 `arp -a` 출력 화면에서 로컬 호스트의 ARP 캐시가 무엇을 보여 주는지와 동일 MAC 매핑이 의미하는 바를 해석할 수 있는지를 묻는 문제이다.

선지별 해설

1번 O: 화면은 `Internet Address`, `Physical Address`, `Type` 형식으로 IP와 MAC 매핑을 보여 주는 윈도우 ARP 캐시 출력이므로 명령어 (가)는 `arp -a`로 보는 것이 타당하다.
2번 X: 이 화면은 게이트웨이 장비의 ARP 테이블이 아니라 `Interface: 172.21.70.180`로 표시된 로컬 호스트의 ARP 캐시이다. 틀린 표현은 `게이트웨이의 ARP 테이블`이고, 올바르게는 `공격 대상 호스트 172.21.70.180의 ARP 테이블`이다.
3번 O: `Interface: 172.21.70.180 --- 0xb`는 이 ARP 캐시를 보유한 인터페이스가 172.21.70.180임을 뜻하므로 공격 대상의 IP 주소가 172.21.70.180이라는 해석이 맞다.
4번 O: 화면상으로는 172.21.70.1과 172.21.70.227이 모두 `18-67-e0-4d-40-5c`로 매핑되어 있다. 따라서 현재 피해 호스트의 ARP 캐시 기준으로 게이트웨이 IP와 공격자 IP가 같은 MAC 주소로 보이는 상태이며, ARP 스푸핑 정황으로 해석할 수 있다.

NoteBase

오답 포인트

`Interface` 줄을 장비 소유자 식별 정보로 읽지 못하고 단순 접속 대상 정보로 오해하면 2번과 3번 판단이 뒤집힌다. 또 ARP 테이블은 명령을 실행한 호스트의 캐시라는 점을 놓치면 화면의 주체를 게이트웨이로 잘못 잡게 된다.

다시 나오면 이렇게 판단

ARP 출력 문제는 먼저 `명령을 누가 실행했는가`를 `Interface` 줄로 확인하고, 그다음 각 IP가 어떤 MAC으로 매핑되는지 비교한다. 특정 IP 둘이 동일 MAC으로 잡히면 해당 호스트의 ARP 캐시에서 스푸핑 또는 비정상 매핑이 발생한 것으로 판단할 수 있다.

암기 포인트

`arp -a`는 내 호스트의 ARP 캐시를 보여 주며, 게이트웨이 IP와 공격자 IP가 같은 MAC으로 보이면 ARP 스푸핑을 의심할 수 있다.

NoteBase

문 7. 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」에서 규정하고 있는 인증에 대한 설명으로 옳지 않은 것은?

① 인증심사의 종류는 예비심사, 최초심사, 사후심사, 갱신심사가 있다.

② 정보보호 관리체계 인증은 인증 신청인의 정보보호 관련 일련의 조치와 활동이 인증기준에 적합함을 한국인터넷진흥원 또는 인증기관이 증명하는 것이다.

③ 정보보호 및 개인정보보호 관리체계 인증기준은 관리체계 수립 및 운영, 보호대책 요구사항, 개인정보 처리 단계별 요구사항의 세 부분으로 구성되어 있다.

④ 최초심사를 통해 인증을 취득하면 3년의 유효기간이 부여되며, 유효기간 중 매년 1회 이상 사후심사를 신청하여야 한다.

정답 1번

쟁점

이 문제는 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」상 인증심사의 종류와 정보보호 및 개인정보보호 관리체계 인증기준의 구성을 구별하는 문제이다.

용어 풀이

최초심사는 처음 인증을 신청하거나 인증범위에 중요한 변경이 있어 다시 인증을 신청할 때 실시하는 인증심사이다.
사후심사는 인증 취득 후 유효기간 중 매년 실시하는 사후관리 심사이다.
갱신심사는 유효기간 만료 전에 인증을 갱신하기 위한 심사이다.
예비인증은 가상자산사업자에 대해 본인증 전에 부여되는 조건부 인증이지 일반적인 인증심사의 종류가 아니다.

핵심 구분

인증심사의 종류는 최초심사, 사후심사, 갱신심사이다. 반면 예비인증은 가상자산사업자에 대한 별도 인증유형이므로 심사종류에 포함되지 않는다.
정보보호 및 개인정보보호 관리체계 인증의 인증기준은 관리체계 수립 및 운영, 보호대책 요구사항, 개인정보 처리 단계별 요구사항의 세 부분으로 구성된다.

NoteBase

선지별 해설

① X
- 고시의 정의조항은 인증심사를 최초심사, 사후심사, 갱신심사로만 구분한다.
- 가상자산사업자에 대한 예비인증은 존재하지만 예비심사라는 일반 심사종류는 두지 않는다.
- 틀린 표현: '예비심사, 최초심사, 사후심사, 갱신심사가 있다.'
- 올바른 표현: '인증심사의 종류는 최초심사, 사후심사, 갱신심사가 있다.' 또는 '예비인증은 별도의 조건부 인증이지 인증심사의 종류가 아니다.'

② O
- 정보보호 관리체계 인증은 인증 신청인의 정보보호 관련 일련의 조치와 활동이 인증기준에 적합함을 인터넷진흥원 또는 인증기관이 증명하는 제도라는 정의와 일치한다.

③ O
- 정보보호 및 개인정보보호 관리체계 인증에는 별표 7 가목부터 다목이 적용되므로 인증기준은 관리체계 수립 및 운영, 보호대책 요구사항, 개인정보 처리 단계별 요구사항의 세 부분으로 구성된다.

④ O
- 인증서의 유효기간은 3년이며, 인증을 취득한 자는 그 유효기간 중 연 1회 이상 사후심사를 신청하여야 한다.
- 따라서 최초심사를 통해 인증을 취득한 뒤 3년의 유효기간이 부여되고 그 기간 동안 매년 사후심사를 받아야 한다는 설명은 맞다.

오답 포인트

이 문제를 틀렸다면 '예비심사'와 '예비인증'을 혼동했을 가능성이 높다. 출제자는 '예비'라는 비슷한 표현을 넣어 인증유형과 심사유형을 뒤섞는 함정을 만들었다.

다시 나오면 이렇게 판단

고시형 문항은 먼저 정의조항에서 종류, 주체, 유효기간을 확인하면 판단이 빨라진다. '예비'처럼 비슷한 용어가 보이면 인증유형인지 심사유형인지부터 구분하고, 인증기준은 조문이 가목부터 다목까지 무엇을 포함하는지로 대조하면 된다.

암기 포인트

심사 3종은 최초·사후·갱신이고, 예비는 심사가 아니라 가상자산사업자의 예비인증이다.

NoteBase

문 8. 블록암호 운영 모드 중 암호화 과정에서 초기벡터(IV)를 사용하지 않는 것은?

① CFB(Cipher Feedback)

② OFB(Output Feedback)

③ ECB(Electronic Codebook)

④ CBC(Cipher Block Chaining)

정답 3번

출제 포인트

이 문제는 블록암호 운영 모드별 초기벡터 사용 여부를 구별할 수 있는지를 묻는다.

핵심 개념

CFB는 이전 암호문 블록을 되먹임해 스트림처럼 동작시키는 모드이므로 시작점인 IV가 필요하다.
OFB는 출력 블록을 되먹임해 키스트림을 만드는 모드이므로 첫 출력 생성을 위한 IV가 필요하다.
CBC는 이전 암호문 블록과 평문 블록을 XOR한 뒤 암호화하므로 첫 블록 처리를 위해 IV가 필요하다.
ECB는 각 평문 블록을 서로 독립적으로 같은 키로 바로 암호화하므로 IV를 사용하지 않는다.

선지별 해설

1번 O/X: X이다. CFB는 첫 단계에서 되먹임할 이전 암호문이 없으므로 IV로 시작한다. 틀린 표현은 'IV를 사용하지 않는다'이고, 올바르게는 'CFB는 IV를 사용한다'이다.
2번 O/X: X이다. OFB는 암호화 함수의 출력을 계속 되먹임해 키스트림을 만들기 때문에 시작 상태를 정하는 IV가 필요하다. 틀린 표현은 'IV를 사용하지 않는다'이고, 올바르게는 'OFB는 IV를 사용한다'이다.
3번 O/X: O이다. ECB는 블록마다 독립적으로 암호화하므로 이전 블록과 연결되는 초기 상태가 없어서 IV를 사용하지 않는다.
4번 O/X: X이다. CBC는 첫 평문 블록을 IV와 XOR한 뒤 암호화하므로 IV가 반드시 필요하다. 틀린 표현은 'IV를 사용하지 않는다'이고, 올바르게는 'CBC는 IV를 사용한다'이다.

오답 포인트

CFB, OFB, CBC는 모두 블록 간 연쇄나 되먹임이 있어 시작값이 필요하다는 점을 놓치면 헷갈린다. 이름이 익숙하다는 이유로 CFB와 OFB만 IV를 쓴다고 좁게 외우면 CBC까지 같이 틀리게 된다.

다시 나오면 이렇게 판단

운영 모드를 보면 먼저 각 블록이 이전 결과와 연결되는지 확인한다. 이전 암호문, 출력 블록, 혹은 첫 블록 XOR가 필요하면 IV를 사용하고, 블록이 완전히 독립이면 ECB처럼 IV를 사용하지 않는다.

NoteBase

암기 포인트

ECB는 독립 블록이라 IV가 없고, CBC·CFB·OFB는 연결 구조라 IV가 있다.

NoteBase

문 9. TLS(Transport Layer Security) 1.3 프로토콜에 대한 설명으로 옳은 것만을 모두 고르면? (단, 세션 재개(resumption)와 PSK(Pre-Shared Key) 방식은 고려하지 않는다)

ㄱ. Handshake 프로토콜 이전에 클라이언트와 서버가 사용할 암호 알고리즘을 결정한다.
ㄴ. Handshake 프로토콜에서 서버를 인증하려면 클라이언트는 서버의 인증서를 이용한다.
ㄷ. Record 프로토콜에서 사용할 대칭키는 Handshake 프로토콜의 키교환으로부터 생성된다.
ㄹ. Record 프로토콜에서 메시지 단편화, 암호화, 메시지인증 코드 추가 등이 수행된다.

① ㄱ, ㄹ
② ㄴ, ㄷ
③ ㄱ, ㄴ, ㄹ
④ ㄴ, ㄷ, ㄹ

정답 4번

출제 포인트

이 문제는 TLS 1.3에서 Handshake 프로토콜과 Record 프로토콜의 역할, 그리고 암호군 협상·서버 인증·세션 키 생성 시점을 구별할 수 있는지를 묻는다.

핵심 개념

Handshake 프로토콜은 ClientHello와 ServerHello 등을 통해 사용할 암호군을 협상하고, 서버 인증서 검증과 키 교환을 수행하는 단계이다.
Record 프로토콜은 상위 메시지를 전송 단위로 단편화하고, 합의된 키로 암호화와 무결성 보호를 적용해 전달하는 계층이다.

NoteBase

선지별 해설

1번 X: ㄱ은 틀리고 ㄹ만 옳다. ㄱ의 틀린 표현은 'Handshake 프로토콜 이전에'이다. 사용할 암호군은 Handshake 안의 ClientHello와 ServerHello 교환에서 협상되므로, 올바르게는 'Handshake 프로토콜 과정에서 클라이언트와 서버가 사용할 암호 알고리즘을 결정한다'이다. ㄹ은 Record 계층이 단편화와 보호 처리를 담당하므로 옳다.
2번 X: ㄴ과 ㄷ은 옳지만 ㄹ도 옳으므로 옳은 것만 모두 고른 조합이 아니다. 올바른 조합은 'ㄴ, ㄷ, ㄹ'이다.
3번 X: ㄱ이 포함되어 있어서 틀리다. ㄱ의 틀린 표현은 역시 'Handshake 프로토콜 이전에'이며, 협상은 Handshake 이전이 아니라 Handshake 과정에서 이루어진다. 올바른 조합은 'ㄴ, ㄷ, ㄹ'이다.
4번 O: ㄴ은 클라이언트가 Handshake에서 서버가 보낸 인증서를 검증해 서버를 인증한다는 뜻이므로 옳다. ㄷ은 문항의 단서대로 세션 재개와 PSK를 제외하면 Record 계층에서 쓸 대칭키가 Handshake의 키 교환과 키 스케줄로부터 파생되므로 옳다. ㄹ은 Record 계층이 메시지를 단편화하고 암호화하며 무결성 보호값을 붙여 전송한다는 뜻이므로 옳다. TLS 1.3에서는 별도 MAC 대신 AEAD 인증 태그로 무결성을 보호하지만, 취지는 Record 계층의 인증 기능을 가리키므로 맞는 설명이다.

오답 포인트

ㄱ의 '이전' 한 단어와 ㄹ의 '메시지인증 코드' 표현이 함정이다. 암호군 협상은 Handshake 전에 끝나는 절차가 아니고 Handshake 자체의 내용이며, TLS 1.3의 Record 계층은 별도 MAC이라는 형식보다 넓게 보면 무결성 보호를 담당한다.

다시 나오면 이렇게 판단

TLS 문제는 먼저 각 기능을 협상·인증·키생성 단계와 전송·보호 단계로 나눈다. 그다음 각 진술을 개별적으로 O/X 판정한 뒤, 마지막에 조합 선택지에 빠진 참이나 포함된 거짓이 없는지 확인하면 된다.

암기 포인트

Handshake는 협상·인증·키생성, Record는 단편화·암호화·무결성보호이다.

NoteBase

문 10. 다음과 같은 특성을 갖추고 있는 보안 모델은?

◯ 최초의 수학적 모델이다.
◯ 강제적 접근 통제 방식으로 접근을 통제하며, 시스템 내부에 있는 정보의 기밀성을 보호한다.
◯ 주체는 주체보다 같거나 낮은 보안 수준의 객체만 읽을 수 있고, 주체보다 같거나 높은 보안 수준의 객체만 쓸 수 있다.

① 비바(Biba) 모델
② 만리장성(Chinese Wall) 모델
③ 클락-윌슨(Clark-Wilson) 모델
④ 벨-라파둘라(Bell-LaPadula) 모델

정답 4번

출제 포인트

이 문제는 보안 모델별 보호 목표와 접근 통제 규칙을 연결하는 문제이며, 기밀성을 위한 강제적 접근 통제와 no read up, no write down 규칙을 묻는다.

핵심 정리

비바(Biba) 모델: 무결성을 보호하는 모델이며 낮은 무결성 데이터가 높은 무결성 주체를 오염시키지 못하게 하는 데 초점이 있다.
만리장성(Chinese Wall) 모델: 이해상충을 방지하기 위해 같은 충돌 집합 내부의 경쟁 회사 정보 접근을 차단하는 모델이다.
클락-윌슨(Clark-Wilson) 모델: 잘 형성된 트랜잭션과 직무 분리를 통해 상업적 환경의 무결성을 보장하는 모델이다.
벨-라파둘라(Bell-LaPadula) 모델: 기밀성 보호를 위한 최초의 수학적 보안 모델이며 강제적 접근 통제를 바탕으로 no read up, no write down을 적용한다.

NoteBase

선지별 해설

① X: 비바 모델은 기밀성이 아니라 무결성을 보호하는 모델이다. 제시문처럼 강제적 접근 통제로 기밀성을 지키고 주체가 자신보다 낮거나 같은 등급만 읽고 높거나 같은 등급만 쓰는 설명은 비바가 아니라 벨-라파둘라 모델에 해당한다.
② X: 만리장성 모델은 이해상충 방지가 핵심이며, 이미 접근한 회사와 이해가 충돌하는 다른 회사 정보에 접근하지 못하게 하는 모델이다. 강제적 접근 통제로 기밀성을 보호하는 최초의 수학적 모델이라는 설명으로 고치면 벨-라파둘라 모델이 된다.
③ X: 클락-윌슨 모델은 무결성을 위한 상업용 보안 모델이며 잘 형성된 트랜잭션, 무결성 검증 절차, 직무 분리가 핵심이다. 제시문처럼 보안 등급 기반 읽기·쓰기 규칙을 적용하는 모델로 고치면 벨-라파둘라 모델이 된다.
④ O: 벨-라파둘라 모델은 기밀성을 보호하는 대표적인 다단계 보안 모델이다. 최초의 수학적 보안 모델로 알려져 있고 강제적 접근 통제를 사용하며, 주체는 자신보다 같거나 낮은 보안 수준의 객체만 읽고 자신보다 같거나 높은 보안 수준의 객체만 쓸 수 있다.

오답 포인트

비바와 벨-라파둘라는 읽기·쓰기 방향이 서로 반대처럼 출제되어 자주 혼동된다. 이 문항의 함정은 모델 이름보다 보호 목표를 먼저 보지 않으면 비바를 고르기 쉽다는 점이며, 제시문에 기밀성이라고 명시된 순간 벨-라파둘라로 좁혀진다.

다시 나오면 이렇게 판단

보안 모델 문제는 먼저 보호 목표가 기밀성인지 무결성인지부터 구분하면 된다. 그다음 기밀성이면서 강제적 접근 통제, 낮은 등급 읽기 가능, 높은 등급 쓰기 가능이 나오면 벨-라파둘라로 판단한다.

암기 포인트

벨-라파둘라 = 기밀성 = no read up, no write down이다.

NoteBase

문 11. FIPS 202에서 명시된 SHA-3 표준에 대한 설명으로 옳지 않은 것은?

① KECCAK을 기반으로 한 해시함수 표준이다.

② SHAKE128, SHAKE256은 가변길이의 해시값을 출력한다.

③ SHA3-512는 256비트의 프리이미지 저항성을 갖는다.

④ SHA-2와 다른 스펀지(sponge) 구조를 이용한다.

정답 3번

출제 포인트

SHA-3 계열의 구조, SHAKE의 출력 특성, SHA3-512의 보안강도를 구분하는 문제이다.

핵심 개념

SHA-3는 KECCAK 기반의 스펀지 구조 해시 표준이다. SHAKE128과 SHAKE256은 XOF로서 원하는 길이의 출력을 생성할 수 있다. SHA3-512는 512비트 출력 해시이므로 프리이미지 저항성은 512비트 수준이고 충돌 저항성은 256비트 수준이다.

선지별 해설

① O: SHA-3 표준은 KECCAK 알고리즘을 기반으로 제정된 해시함수 표준이므로 옳다.
② O: SHAKE128과 SHAKE256은 XOF이므로 출력 길이가 고정되지 않고 가변길이 해시값을 출력하므로 옳다.
③ X: 틀린 부분은 "256비트의 프리이미지 저항성"이다. SHA3-512는 512비트 출력 해시이므로 프리이미지 저항성은 512비트 수준이다. 올바르게는 "SHA3-512는 512비트의 프리이미지 저항성과 256비트의 충돌 저항성을 갖는다"이다.
④ O: SHA-3는 SHA-2와 달리 스펀지 구조를 사용하므로 옳다. SHA-2는 머클-댐가드 계열 압축함수 반복 구조에 가깝다.

오답 포인트

③은 프리이미지 저항성과 충돌 저항성의 비트를 뒤바꾸는 함정이다. 512비트 출력 해시에서 256비트는 충돌 저항성으로 연결되고, 프리이미지 저항성에 그대로 대응하지는 않는다.

다시 나오면 이렇게 판단

SHA-3 계열 문항은 먼저 KECCAK 기반 스펀지 구조인지, SHAKE처럼 가변길이 출력인지, 고정 출력 해시라면 출력 길이를 기준으로 프리이미지 저항성과 충돌 저항성을 구분해 판단한다.

NoteBase

암기 포인트

SHA-3는 KECCAK 기반 스펀지 구조이고, SHAKE는 가변길이 출력이며, SHA3-512는 프리이미지 512비트·충돌 256비트로 정리된다.

NoteBase

문 12. 해시함수에 대한 설명으로 옳지 않은 것은?

① 무결성을 보장하는 HMAC은 두 단계의 해시 과정으로 안전성을 높인다.

② SHA-256을 생일공격으로 분석하려면 최소 2^{256}개의 해시값을 계산해야 한다.

③ DSA의 서명알고리즘은 메시지를 해시한 후 그 해시값을 이용하여 서명값을 생성한다.

④ 해시함수가 충돌저항성을 만족하면 제2 프리이미지 저항성도 만족한다.

정답 2번

출제 포인트

이 문제는 해시함수의 보안 성질과 전자서명 관련 해시 활용 방식을 정확히 구분하는지를 묻는 문제이다.

핵심 개념

해시함수의 주요 성질은 역상 저항성, 제2 프리이미지 저항성, 충돌저항성으로 나뉜다.
생일공격은 충돌을 찾는 공격이므로 n비트 해시에 필요한 계산량은 보통 $2^{n/2}$ 수준이다.
HMAC은 비밀키와 함께 내부 해시와 외부 해시를 적용해 메시지 인증과 무결성 검증에 사용된다.
DSA는 메시지 원문이 아니라 메시지의 해시값을 바탕으로 서명값을 생성한다.

선지별 해설

① O
HMAC은 내부 해시와 외부 해시의 2단 구조를 사용해 단순 해시보다 안전한 메시지 인증을 제공한다. 무결성 검증에 사용된다는 설명도 맞다.

② X
틀린 부분은 "생일공격으로 분석하려면 최소 2^{256}개의 해시값을 계산해야 한다"는 표현이다. 생일공격은 충돌 탐색 공격이므로 SHA-256에서는 보통 2^{128} 수준의 계산량이 필요하다. 2^{256}은 전수 역상 탐색에 가까운 크기이다.

③ O
DSA는 메시지를 직접 서명하는 것이 아니라 먼저 해시한 뒤 그 해시값을 이용해 서명값을 계산한다. 해시를 사용하는 전자서명 방식이라는 점에서 맞는 설명이다.

④ O
충돌저항성은 서로 다른 두 입력이 같은 해시값을 갖는 쌍을 찾기 어려운 성질이다. 이 성질이 성립하면 특정 입력과 같은 해시값을 갖는 다른 입력을 찾는 제2 프리이미지 공격도 일반적으로 더 어렵기 때문에 제2 프리이미지 저항성도 만족하는 것으로 본다.

NoteBase

오답 포인트

②는 해시 길이 n과 생일공격 복잡도 $2^{n/2}$를 구분하지 못하면 바로 흔들리는 선지이다. 충돌 탐색과 역상 탐색을 같은 수준으로 착각하면 SHA-256에 대해 2^{256}을 답처럼 고르기 쉽다.

다시 나오면 이렇게 판단

해시 문제는 먼저 무엇을 찾는 공격인지 구분하면 된다. 충돌을 찾으면 생일공격이므로 $2^{n/2}$, 특정 해시의 원래 입력을 찾으면 역상 공격이므로 2^{n} 수준으로 판단한다. 전자서명 선지는 "메시지 원문"이 아니라 "메시지의 해시값"으로 서명한다는 점을 기준으로 본다.

암기 포인트

생일공격은 충돌 탐색이므로 $2^{n/2}$, 역상 탐색은 2^{n}이다.

NoteBase

문 13. 「개인정보 보호법」상 개인정보처리자가 준수해야 할 개인정보보호 원칙에 대한 설명으로 옳지 않은 것은?

① 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.

② 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 비공개하여야 하며, 열람청구권 등 정보주체의 권리는 보장하여야 한다.

③ 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.

④ 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.

정답 2번

쟁점

이 문제는 개인정보처리자가 준수해야 하는 개인정보 보호 원칙 중 공개 원칙과 다른 보호 원칙을 정확히 구별하는 문제이다.

용어 풀이

개인정보 처리방침은 개인정보를 어떤 기준과 절차로 처리하는지를 정보주체에게 공개하는 기준 문서이다.

핵심 구분

개인정보의 처리에 관한 사항은 원칙적으로 공개하여야 하고, 정보주체의 열람청구권 등 권리도 함께 보장하여야 한다. 반면 정확성·완전성·최신성 보장, 목적 외 이용 금지, 사생활 침해 최소화는 각각 별도의 원칙이다.

선지별 해설

1번: O. 개인정보는 처리 목적에 필요한 범위에서 정확성, 완전성 및 최신성이 보장되도록 해야 한다는 원칙에 맞는 설명이다.
2번: X. 틀린 표현은 '비공개하여야 하며'이다. 개인정보 처리방침 등 개인정보의 처리에 관한 사항은 공개하여야 하며, 열람청구권 등 정보주체의 권리도 보장하여야 한다.
3번: O. 개인정보는 처리 목적에 필요한 범위에서 적합하게 처리해야 하고, 그 목적 외의 용도로 활용해서는 안 된다는 원칙에 맞는 설명이다.
4번: O. 개인정보는 정보주체의 사생활 침해를 최소화하는 방법으로 처리해야 한다는 원칙에 맞는 설명이다.

오답 포인트

2번은 뒤의 '열람청구권 등 정보주체의 권리 보장'이라는 맞는 문장을 붙여 앞의 '비공개'를 놓치게 만든다. 공개의무와 비밀보호를 같은 방향으로 오해하면 틀리기 쉽다.

NoteBase

다시 나오면 이렇게 판단

개인정보 보호 원칙 문제는 선지의 핵심 동사를 먼저 확인하는 방식으로 판단한다. '공개하여야 한다', '목적 외 활용하여서는 아니 된다', '최소화하여 처리한다'처럼 조문 원칙을 그대로 담은 표현은 옳고, 이를 반대로 뒤집은 표현은 오답이다.

암기 포인트

개인정보 보호 원칙은 목적 내 처리, 정확성 보장, 처리사항 공개, 사생활 침해 최소화의 흐름으로 정리된다.

NoteBase

문 14. 양자 컴퓨팅과 그에 대응하는 암호기법에 대한 설명으로 옳지 않은 것은?

① 양자 컴퓨팅은 양자 중첩과 양자 얽힘 등의 양자역학 특성을 이용한다.

② AES-256은 이상적인 양자 컴퓨팅하에서 256비트 안전성을 보장한다.

③ 이상적인 양자 컴퓨팅하에서 RSA 및 타원곡선암호(ECC)는 더 이상 안전하지 않다.

④ 미국 NIST는 양자 컴퓨팅에 대응하기 위해 양자내성암호(PQC, Post-Quantum Cryptography) 표준을 발표하였다.

정답 2번

출제 포인트

이 문제는 양자 컴퓨팅이 대칭키 암호와 공개키 암호에 미치는 영향, 그리고 이에 대응하는 양자내성암호의 개념을 구분하는지 묻는 문제이다.

핵심 개념

양자 컴퓨팅은 양자 중첩과 양자 얽힘을 이용해 특정 계산을 고전 컴퓨터보다 훨씬 빠르게 수행할 수 있다.
대칭키 암호는 양자 환경에서도 바로 붕괴하지는 않지만 그로버 알고리즘 때문에 체감 보안 강도가 대체로 절반 수준으로 감소한다.
공개키 암호인 RSA와 ECC는 쇼어 알고리즘에 의해 정수분해와 이산로그 문제가 빠르게 풀릴 수 있어 이상적인 양자 컴퓨터 앞에서는 안전하지 않다.
양자내성암호는 이런 공개키 계열 취약점을 대체하기 위해 설계된 암호 표준이다.

선지별 해설

① O: 양자 컴퓨팅은 양자 중첩과 양자 얽힘 같은 양자역학적 성질을 계산에 활용한다. 이 진술은 양자 컴퓨팅의 핵심 원리를 정확히 설명한다.
② X: 틀린 부분은 "256비트 안전성을 보장한다"는 표현이다. 대칭키 암호인 AES는 양자 컴퓨터에서도 즉시 깨지는 구조는 아니지만, 그로버 알고리즘의 영향으로 AES-256의 보안 강도는 대략 128비트 수준으로 본다. 올바르게는 "AES-256은 이상적인 양자 컴퓨팅하에서도 약 128비트 수준의 보안 강도를 기대할 수 있다"이다.
③ O: RSA와 ECC는 각각 정수분해와 이산로그 문제의 어려움에 의존하는데, 이상적인 양자 컴퓨터에서는 쇼어 알고리즘으로 이 문제가 효율적으로 풀릴 수 있다. 따라서 더 이상 안전하지 않다는 설명이 맞다.
④ O: NIST는 양자 컴퓨팅 위협에 대비하기 위해 PQC 표준화를 진행했고, 실제로 양자내성암호 표준을 발표하였다. 이 진술은 PQC 도입 방향을 올바르게 설명한다.

NoteBase

오답 포인트

②처럼 AES를 "256비트 키 길이 = 256비트 양자 안전성"으로 그대로 연결하면 틀리기 쉽다. 양자 환경에서는 대칭키와 공개키의 영향 방식이 다르며, 대칭키는 강도가 줄어들고 공개키는 구조적으로 붕괴할 수 있다는 차이를 구분해야 한다.

다시 나오면 이렇게 판단

양자 컴퓨팅 관련 선지는 먼저 대칭키와 공개키를 나누어 본다. 대칭키는 그로버 알고리즘으로 보안 강도가 대체로 절반 수준으로 감소하고, 공개키의 RSA·ECC는 쇼어 알고리즘 때문에 안전하지 않으며, 대응책은 PQC라는 흐름으로 판단하면 된다.

암기 포인트

양자 시대에는 AES는 반감, RSA·ECC는 붕괴, 대응책은 PQC이다.

NoteBase

문 15. A가 전자서명 및 공개키 암호기법을 이용하여, 메시지(M)를 안전하게 B에게 전송하는 과정이다. 동작 순서를 바르게 나열한 것은? (단, A는 B의 공개키를 알고 있다)

(가) A의 서명키로 해시값을 전자서명한다.
(나) A의 서명검증키와 암호문을 B에게 전송한다.
(다) 메시지(M)의 해시값을 구한다.
(라) B의 공개키를 이용한 하이브리드 방식으로 메시지(M)와 전자서명값을 암호화한다.

① (가) → (다) → (나) → (라)
② (가) → (라) → (다) → (나)
③ (다) → (가) → (라) → (나)
④ (다) → (라) → (나) → (가)

정답 3번

출제 포인트

이 문제는 전자서명과 공개키 기반 기밀성 확보 절차에서 해시 계산, 서명 생성, 암호화, 전송의 선후관계를 묻는다.

올바른 순서

1. (다) 메시지(M)의 해시값을 구한다.
2. (가) 구한 해시값을 A의 서명키로 전자서명한다.
3. (라) 메시지(M)와 전자서명값을 B의 공개키를 이용한 하이브리드 방식으로 암호화한다.
4. (나) A의 서명검증키와 암호문을 B에게 전송한다.

왜 이 순서: 전자서명은 먼저 해시값이 있어야 만들 수 있고, 암호화는 서명값이 만들어진 뒤에야 메시지와 함께 보호할 수 있으므로 (다) → (가) → (라) → (나) 순서가 된다.

선지별 해설

① X: (가)가 (다)보다 앞에 와서 전자서명값을 만들 입력인 해시값이 아직 없다. 틀린 표현은 '(가) → (다)'이다. 올바르게는 '(다) → (가)'이다.
② X: (가) 다음에 바로 (라)가 오면 해시 계산이 뒤로 밀려 서명 생성의 전제가 무너진다. 틀린 표현은 '(가) → (라) → (다)'의 배치이다. 올바르게는 '(다) → (가) → (라)'이다.
③ O: 해시 계산 후 서명을 만들고, 그 결과를 메시지와 함께 암호화한 뒤 전송하므로 전자서명과 기밀성 확보 절차가 맞는다.
④ X: (다) 다음에 (라)를 먼저 두면 아직 생성되지 않은 전자서명값을 메시지와 함께 암호화할 수 없다. 틀린 표현은 '(다) → (라) → (나) → (가)'이다. 올바르게는 '(다) → (가) → (라) → (나)'이다.

NoteBase

오답 포인트

전자서명과 암호화를 서로 독립 단계로 보고 순서를 바꾸기 쉽다. 이 문항의 함정은 서명은 해시값이 선행되어야 하고, 최종 암호화는 메시지와 전자서명값이 모두 준비된 뒤에야 가능하다는 의존관계를 놓치게 만드는 데 있다.

다시 나오면 이렇게 판단

보안 절차 순서 문제는 생성물의 입력 관계로 판단한다. 해시값이 있어야 서명할 수 있고, 서명값이 있어야 메시지와 함께 암호화할 수 있으며, 전송은 모든 산출물이 준비된 뒤 마지막에 온다.

암기 포인트

해시 계산 → 서명 생성 → 암호화 → 전송 순으로 보면 된다.

NoteBase

문 16. 정보보호시스템 공동평가기준(Common Criteria)의 등급별 EAL(Evaluation Assurance Level)의 목적에 대한 설명으로 옳지 않은 것은? (단, TOE(Target of Evaluation)는 평가대상이다)

① EAL1: 보안 행동을 이해하기 위해 기능 및 인터페이스 명세, 설명서를 이용하여 제한적인 보안목표명세서에 포함된 보안기능요구사항을 분석함으로써 기초적인 수준의 보증을 제공한다.

② EAL2: 보안 행동을 이해하기 위해 기능 및 인터페이스 명세, 설명서, TOE 구조의 기본적 설명을 이용하여 완전한 보안목표명세서에 포함된 보안기능요구사항을 분석함으로써 보증을 제공한다.

③ EAL3: 보안 행동을 이해하기 위해 기능 및 인터페이스 명세, 설명서, TOE 설계의 아키텍처 설명을 이용하여 완전한 보안목표명세서에 포함된 보안기능요구사항을 분석함으로써 보증을 제공한다.

④ EAL4: 보안 행동을 이해하기 위해 기능 및 완전한 인터페이스 명세, 설명서, TOE에 대한 설계 서술, 구현을 이용하여 완전한 보안목표명세서에 포함된 보안기능요구사항을 분석함으로써 보증을 제공한다.

정답 4번

출제 포인트

이 문제는 EAL1부터 EAL4까지에서 보안기능요구사항을 분석할 때 요구되는 명세와 설계 자료의 범위가 어떻게 단계적으로 커지는지를 구별하는 문제이다.

핵심 개념

EAL1은 제한적 보안목표명세서와 기능·인터페이스 명세, 설명서를 바탕으로 기초적 수준의 보증을 제공하는 단계이다.
EAL2는 완전한 보안목표명세서와 TOE의 기본 구조 설명까지 포함하여 보증 수준을 높인 단계이다.
EAL3은 TOE 설계의 아키텍처 설명까지 요구하여 설계 단계 점검을 강화한 단계이다.
EAL4는 기능 및 완전한 인터페이스 명세, 설명서, TOE의 기본적인 모듈 설계 설명, 구현의 일부를 사용하여 보안 동작을 이해하는 단계이다.

NoteBase

선지별 해설

1번 O: EAL1은 제한적 보안목표명세서에 포함된 보안기능요구사항을 기능·인터페이스 명세와 설명서로 분석하여 기초적 수준의 보증을 제공하므로 옳다.
2번 O: EAL2는 완전한 보안목표명세서를 전제로 하고, 기능·인터페이스 명세, 설명서, TOE의 기본 구조 설명을 이용하므로 옳다.
3번 O: EAL3은 완전한 보안목표명세서를 바탕으로 기능·인터페이스 명세, 설명서, TOE 설계의 아키텍처 설명을 사용하므로 옳다.
4번 X: 틀린 표현은 "TOE에 대한 설계 서술, 구현"이다. EAL4는 설계 전반이나 구현 전체를 쓰는 단계가 아니라, TOE의 기본적인 모듈 설계 설명과 구현의 일부를 이용하는 단계이다. 올바르게는 "기능 및 완전한 인터페이스 명세, 설명서, TOE의 기본적인 모듈 설계 설명, 구현의 일부를 이용하여 완전한 보안목표명세서의 보안기능요구사항을 분석한다"이다.

오답 포인트

EAL3과 EAL4는 둘 다 완전한 보안목표명세서를 전제로 하므로 구분점이 흐려지기 쉽다. 4번은 EAL4의 "완전한 인터페이스 명세"라는 표현은 맞게 가져왔지만, "기본적인 모듈 설계"를 빼고 구현 범위를 전체처럼 넓혀 상위 단계 설명으로 바꾼 점이 함정이다.

다시 나오면 이렇게 판단

EAL 문항은 보안목표명세서가 제한적인지 완전한지, 설계 설명이 기본 구조인지 아키텍처인지 모듈 설계인지, 구현 자료가 없는지 일부인지 전체인지 순서대로 확인하면 판단할 수 있다. 제한적 ST면 EAL1, 기본 구조 설명이면 EAL2, 아키텍처 설명이면 EAL3, 완전한 인터페이스 명세와 구현의 일부가 나오면 EAL4이다.

암기 포인트

EAL1은 제한적 ST, EAL2는 기본 구조, EAL3은 아키텍처 설계, EAL4는 완전한 인터페이스와 구현의 일부이다.

NoteBase

문 17. 「개인정보 보호법 시행령」상 개인정보처리자가 정보주체의 동의 없이 개인정보를 이용 또는 제공하려는 경우 고려하여야 할 사항이 아닌 것은?

① 당초 수집 목적과 관련성이 있는지 여부

② 정보주체의 이익을 부당하게 침해하는지 여부

③ 개인정보 수집기관의 영업이익이 지속적으로 발생하는지 여부

④ 가명처리 또는 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부

정답 3번

쟁점

이 문제는 개인정보처리자가 정보주체의 동의 없이 개인정보를 추가적으로 이용하거나 제공하려는 경우 시행령상 고려사항을 구별하는 문제이다.
핵심은 법정 고려요소와 무관한 영업이익 요소를 구별하는 것이다.

용어 풀이

개인정보의 추가적인 이용 또는 제공은 당초 수집 목적과 합리적으로 관련된 범위에서 정보주체의 별도 동의 없이 개인정보를 다시 이용하거나 제공하는 것을 말한다.

핵심 구분

개인정보 보호법 시행령 제14조의2는 추가적 이용 또는 제공 시 ① 당초 수집 목적과의 관련성, ② 수집 정황 또는 처리 관행에 비추어 본 예측 가능성, ③ 정보주체 이익의 부당한 침해 여부, ④ 가명처리·암호화 등 안전성 확보 조치 여부를 고려하도록 한다.
개인정보처리자나 수집기관의 영업이익 지속 여부는 고려요소에 포함되지 않는다.

NoteBase

선지별 해설

① O
- 당초 수집 목적과 관련성이 있는지 여부는 시행령이 명시한 고려사항이다.

② O
- 정보주체의 이익을 부당하게 침해하는지 여부도 시행령이 명시한 고려사항이다.
- 추가적 이용 또는 제공이 가능하더라도 정보주체에게 과도한 불이익을 주면 허용될 수 없다는 취지이다.

③ X
- 개인정보 수집기관의 영업이익이 지속적으로 발생하는지 여부는 시행령상 고려사항이 아니다.
- 틀린 표현: "개인정보 수집기관의 영업이익이 지속적으로 발생하는지 여부"
- 올바른 표현: "개인정보를 수집한 정황 또는 처리 관행에 비추어 볼 때 개인정보의 추가적인 이용 또는 제공에 대한 예측 가능성이 있는지 여부"

④ O
- 가명처리 또는 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부는 시행령이 명시한 고려사항이다.
- 추가적 이용 또는 제공의 허용 여부를 판단할 때 보호조치의 존재를 함께 본다.

오답 포인트

③은 법정 고려사항 자리에 사업자 관점의 영업이익 요소를 끼워 넣은 선지이다. 시행령은 목적 관련성, 예측 가능성, 정보주체 이익 보호, 안전성 확보 조치를 보지 영업상 수익성을 보지 않는다.

다시 나오면 이렇게 판단

개인정보의 추가적 이용·제공 문제는 먼저 정보주체 보호 관점의 4요소인지 확인하면 된다. 목적 관련성, 예측 가능성, 정보주체 불이익, 안전조치에 해당하지 않는 사업편의·수익성 문구가 나오면 오답으로 판단된다.

암기 포인트

추가 이용·제공 4요소는 목적, 예측, 침해, 안전이다.

NoteBase

문 18. 다음의 사이버 공격 유형 (가) ~ (다)와 이에 대한 설명 A ~ C를 바르게 연결한 것은?

(가) 스미싱(smishing)
(나) 백도어(backdoor)
(다) 키로깅(keylogging)
A. 사용자가 키보드로 입력하는 정보를 몰래 가로채는 방법으로 트로이 목마 같은 악성코드와 결합하여 동작한다.
B. 정상적인 사용자 인증 절차를 거치지 않고 응용 프로그램이나 시스템에 접근할 수 있는 보안 허점을 이용한다.
C. 신뢰할 수 있는 사람이 보낸 문자메시지처럼 가장하여 링크 접속을 유도한 뒤 개인정보를 빼내는 수법이다.

① (가): A, (나): B, (다): C
② (가): B, (나): C, (다): A
③ (가): C, (나): A, (다): B
④ (가): C, (나): B, (다): A

정답 4번

출제 포인트

이 문제는 스미싱, 백도어, 키로깅의 정의를 구분하여 설명문과 정확히 연결할 수 있는지를 묻는다.

핵심 개념

스미싱: 문자메시지(SMS)를 이용해 링크 접속이나 정보 입력을 유도하는 피싱 공격이다. 결정 차이축은 공격 매체와 유인 방식이며, 키워드는 문자메시지, 링크 유도, 개인정보 탈취이다.
백도어: 정상 인증 절차를 우회하여 시스템에 접근할 수 있게 만든 은닉된 접근 경로나 보안 허점이다. 결정 차이축은 접근 방식과 인증 우회 여부이며, 키워드는 우회 접근, 인증 생략, 숨겨진 통로이다.
키로깅: 사용자의 키보드 입력 내용을 몰래 기록하거나 가로채는 공격이다. 결정 차이축은 탈취 대상 정보이며, 키워드는 키 입력, 기록, 가로채기이다.

NoteBase

선지별 해설

1번: X. 틀린 부분은 (가)에 A를, (다)에 C를 연결한 점이다. A는 키보드 입력을 몰래 가로채는 설명이므로 키로깅에 해당하고, C는 문자메시지로 링크 접속을 유도하는 설명이므로 스미싱에 해당한다. 올바르게는 (가)=C, (나)=B, (다)=A이다.
2번: X. 틀린 부분은 (가)에 B를, (나)에 C를 연결한 점이다. B는 정상 인증 절차를 거치지 않고 접근하는 백도어 설명이고, C는 스미싱 설명이다. 올바르게는 (가)=C, (나)=B, (다)=A이다.
3번: X. 틀린 부분은 (나)에 A를, (다)에 B를 연결한 점이다. A는 키로깅 설명이고 B는 백도어 설명이므로 두 항목이 서로 뒤바뀌었다. 올바르게는 (가)=C, (나)=B, (다)=A이다.
4번: O. C는 신뢰할 수 있는 사람이 보낸 문자처럼 가장해 링크 접속을 유도하는 스미싱 설명이고, B는 인증 절차를 우회하는 백도어 설명이며, A는 키 입력을 가로채는 키로깅 설명이므로 연결이 모두 정확하다.

오답 포인트

스미싱과 백도어를 모두 악성코드 공격으로만 뭉뚱그리면 연결이 흔들린다. 이 문항의 함정은 공격 수단이 문자메시지인지, 인증 우회 통로인지, 키 입력 탈취인지의 차이를 놓치게 만드는 데 있다.

다시 나오면 이렇게 판단

먼저 설명문에서 무엇을 탈취하거나 우회하는지 핵심 행위를 잡으면 된다. 문자메시지와 링크 유도는 스미싱, 인증 절차 우회와 은닉 통로는 백도어, 키보드 입력 기록은 키로깅으로 대응시키면 된다.

암기 포인트

스미싱은 문자 피싱, 백도어는 숨은 출입문, 키로깅은 키 입력 기록이다.

NoteBase

문 19. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상 전자적 전송매체를 이용하여 영리목적의 광고성 정보를 전송하는 자에 대한 금지행위가 아닌 것은?

① 광고성 정보 수신자의 수신거부 또는 수신동의의 철회를 회피·방해하는 행위

② 영리목적의 광고성 정보를 전송할 목적으로 전화번호 또는 전자우편주소를 자동으로 등록하는 행위

③ 광고성 정보 전송자의 신원이나 광고 전송 출처를 감추기 위한 각종 행위

④ 수신자가 수신거부나 수신동의의 철회를 할 때 발생하는 전화요금 등의 금전적 비용을 수신자가 부담하지 않도록 하는 행위

정답 4번

쟁점

이 문제는 정보통신망법상 영리목적의 광고성 정보 전송에서 금지행위와 수신거부 비용부담 방지의무를 구별하는 문제이다.

용어 풀이

수신거부 또는 수신동의 철회는 수신자가 광고를 더 받지 않겠다는 의사를 표시하는 것이다.
금지행위는 법이 해서는 안 된다고 막는 행위이고, 비용부담 방지의무는 법이 하여야 한다고 요구하는 조치이다.

핵심 구분

정보통신망법 제50조 제5항은 광고성 정보 전송자가 해서는 안 되는 금지행위를 열거하고, 제50조 제6항은 수신거부나 수신동의 철회 시 전화요금 등의 비용을 수신자에게 부담시키지 않도록 필요한 조치를 하여야 한다고 정한다.
즉 1번부터 3번까지는 금지행위이고, 4번은 금지행위가 아니라 수신자 보호를 위한 의무이다.

NoteBase

선지별 해설

1번: X
광고성 정보 수신자의 수신거부 또는 수신동의 철회를 회피·방해하는 행위는 정보통신망법 제50조 제5항 제1호의 금지행위이다. 따라서 '금지행위가 아닌 것'이라는 발문에는 맞지 않는다.
틀린 표현: 금지행위가 아닌 것
올바르게는: 금지행위에 해당하는 것이다.
2번: X
영리목적의 광고성 정보를 전송할 목적으로 전화번호 또는 전자우편주소를 자동으로 등록하는 행위는 같은 조 제5항 제3호의 금지행위이다. 자동 생성과 자동 등록은 구별되지만, 이 선지는 자동 등록을 묻고 있으므로 역시 금지행위에 해당한다.
틀린 표현: 금지행위가 아닌 것
올바르게는: 금지행위에 해당하는 것이다.
3번: X
광고성 정보 전송자의 신원이나 광고 전송 출처를 감추기 위한 각종 행위는 같은 조 제5항 제4호의 금지행위이다. 발신자나 출처를 숨기는 행위는 수신자 보호와 추적 가능성을 해치므로 허용되지 않는다.
틀린 표현: 금지행위가 아닌 것
올바르게는: 금지행위에 해당하는 것이다.
4번: O
수신자가 수신거부나 수신동의 철회를 할 때 발생하는 전화요금 등의 금전적 비용을 수신자가 부담하지 않도록 하는 것은 정보통신망법 제50조 제6항이 요구하는 의무이다. 따라서 금지행위가 아니라 사업자가 준수하여야 하는 보호조치이므로 정답이다.

오답 포인트

이 문제는 '금지행위'와 '준수의무'를 섞어 놓은 함정이다. 제50조 제5항의 각 호만 금지행위로 보고, 제6항처럼 수신자 보호를 위해 하여야 하는 조치는 금지행위가 아니라는 점을 구별하지 못하면 4번을 틀리기 쉽다.

다시 나오면 이렇게 판단

먼저 발문이 '금지행위가 아닌 것'인지 확인한 다음, 각 선지가 법문에서 '하여서는 아니 된다'에 해당하는지, 아니면 '하여야 한다'에 해당하는지를 구분하면 된다. 금지목록인지 의무조항인지를 먼저 가르면 정답을 빠르게 고를 수 있다.

암기 포인트

정보통신망법 제50조 제5항은 하지 말아야 할 금지행위이고, 제6항은 수신자에게 비용을 떠넘기지 않도록 하여야 하는 의무이다.

NoteBase

문 20. 국가사이버안보센터가 24시간 365일 국내 사이버 위협 수준을 평가하고 발령하는 사이버 위기 경보단계에 대한 설명으로 옳지 않은 것은?

① 정상: 웜 · 바이러스, 해킹기법 등에 의한 피해발생 가능성이 증가

② 심각: 국가적 차원의 평가와 조치가 필요하다고 판단되는 사고가 발생

③ 주의: 다수기관의 정보통신망 및 정보시스템에 장애가 발생

④ 경계: 복수분야에서 광범위한 피해가 발생하는 등 대규모 피해로 확대될 가능성이 높아 다수기관의 공조대응이 필요

정답 1번

출제 포인트

이 문제는 국가사이버안보센터의 사이버 위기 경보단계에서 각 단계의 핵심 징후를 정확히 대응시키는지를 묻는 문제이다.

핵심 개념

정상은 인터넷 소통과 사용에 큰 지장이 없는 평시 상태이다.
관심은 웜·바이러스, 취약점, 해킹기법 출현 등으로 피해 발생 가능성이 증가한 단계이다.
주의는 다수기관의 정보통신망 및 정보시스템 장애가 발생하거나 정보유출 피해의 확산 가능성이 커진 단계이다.
경계는 복수 분야에서 광범위한 피해가 나타나 대규모 피해로 확대될 가능성이 높고 다수기관의 공조대응이 필요한 단계이다.
심각은 국가적 차원의 평가와 조치가 필요하다고 판단되는 사고가 발생한 단계이다.

NoteBase

선지별 해설

① X
정상 단계에 해당하지 않는다. "웜·바이러스, 해킹기법 등에 의한 피해발생 가능성이 증가"는 정상이 아니라 관심 단계의 설명이다.
틀린 표현은 "정상"이다. 올바르게는 "관심: 웜·바이러스, 해킹기법 등에 의한 피해발생 가능성이 증가"이다.

② O
심각 단계는 국가적 차원의 평가와 조치가 필요하다고 판단되는 사고가 발생한 상태를 말한다. 보기의 설명은 심각 단계의 핵심 징후와 맞는다.

③ O
주의 단계는 다수기관의 정보통신망 및 정보시스템 장애가 발생하고 정보유출 등 피해가 확산될 가능성이 커진 상태를 가리킨다. 보기의 서술은 주의 단계의 상황과 부합한다.

④ O
경계 단계는 복수 분야에서 광범위한 피해가 발생하여 대규모 피해로 확대될 가능성이 높고, 다수기관의 공조대응이 필요한 상태이다. 보기의 설명은 경계 단계의 특징을 정확히 짚고 있다.

오답 포인트

출제자가 노린 함정은 정상과 관심을 바꿔 놓은 점이다. "피해발생 가능성 증가"라는 표현은 평시인 정상이 아니라 위험 징후가 구체화된 관심 단계의 키워드이다. 또 주의와 경계는 모두 피해 확산을 다루므로, "다수기관 장애"는 주의, "광범위한 피해와 공조대응"은 경계로 구분해야 한다.

다시 나오면 이렇게 판단

경보단계 문제는 단계명보다 핵심 키워드를 먼저 대응시키면 된다. 피해발생 가능성 증가는 관심, 다수기관의 정보통신망 및 정보시스템 장애는 주의, 복수분야의 광범위한 피해와 공조대응은 경계, 국가 차원의 평가·조치는 심각으로 판단한다.

암기 포인트

정상은 평시, 관심은 피해 가능성 증가, 주의는 다수기관 장애, 경계는 광범위 피해와 공조대응, 심각은 국가 차원 조치이다.

NoteBase

문 21. 리눅스 시스템의 로그 파일에 대한 설명으로 옳지 않은 것은?

① history: 텔넷이나 FTP, 원격 접속 등 인증과정을 거치는 로그를 저장한다.

② wtmp: 사용자의 로그인과 로그아웃한 정보 등을 저장한다.

③ lastlog: 사용자 이름, 포트, 마지막 로그인 시간 등을 저장한다.

④ utmp: 현재 로그인한 사용자 이름, 로그인한 디바이스 등을 저장한다.

정답 1번

출제 포인트

이 문제는 history, wtmp, lastlog, utmp가 각각 어떤 종류의 기록을 남기는지 구분하는 문제이다.

핵심 개념

history는 셸에서 실행한 명령 이력을 저장하는 기록이다.
wtmp는 로그인과 로그아웃 같은 사용자 세션 이력을 누적하는 파일이다.
lastlog는 사용자별 마지막 로그인 시각과 접속 터미널 또는 원격지 정보를 확인하는 기록이다.
utmp는 현재 로그인 중인 사용자 상태를 보여 주는 기록이다.

선지별 해설

1번: X. history는 텔넷이나 FTP의 인증 로그를 저장하는 파일이 아니라 셸에서 실행한 명령 이력을 저장하는 기록이다. 틀린 표현은 "인증과정을 거치는 로그"이다. 올바르게는 "사용자가 실행한 명령 이력을 저장한다"이다.
2번: O. wtmp는 사용자의 로그인과 로그아웃 기록을 누적해서 남기는 세션 이력 파일이므로 설명이 맞다.
3번: O. lastlog는 사용자별 마지막 로그인 기록을 보여 주며 마지막 로그인 시간과 접속 포트 또는 터미널 정보를 확인할 수 있으므로 설명 취지가 맞다.
4번: O. utmp는 현재 로그인한 사용자와 로그인한 터미널 또는 디바이스 상태를 담아 who, w 같은 명령이 참고하는 정보이므로 설명이 맞다.

오답 포인트

wtmp, utmp, lastlog는 모두 로그인 관련 기록이라 이름이 비슷해 보여 혼동하기 쉽다. 하지만 현재 접속 상태인지, 누적 세션 이력인지, 마지막 로그인 기록인지를 구분하면 정리된다. 여기에 셸 명령 이력인 history를 같은 부류로 묶으면 틀리기 쉽다.

다시 나오면 이렇게 판단

로그 파일 문제는 먼저 명령 이력인지, 현재 접속 상태인지, 로그인·로그아웃 누적 이력인지, 마지막 1회 로그인 기록인지를 구분하면 빠르게 판단할 수 있다.

NoteBase

암기 포인트

history는 명령 이력, utmp는 현재 접속, wtmp는 로그인·로그아웃 누적, lastlog는 마지막 로그인 기록이다.

NoteBase

문 22. 침입탐지시스템(IDS)에 대한 설명으로 옳지 않은 것은?

① 시그니처 기반(Signature-based) 침입탐지시스템은 신종 공격이나 변형된 공격을 능동적으로 탐지할 확률이 높은 장점이 있다.

② 비정상 기반(Anomaly-based) 침입탐지시스템은 정상적인 행위에 대한 모델을 만들어 놓고 그 모델에서 벗어나면 비정상으로 판단한다.

③ 호스트 기반(Host-based) 침입탐지시스템은 호스트에서 실행 중인 시스템 및 응용 프로그램의 로그를 이용하여 호스트 시스템에 가해지는 공격을 탐지한다.

④ 네트워크 기반(Network-based) 침입탐지시스템은 네트워크에서 전송되는 트래픽을 수집하고 정제한 후 분석하여 공격을 탐지한다.

정답 1번

출제 포인트

이 문제는 시그니처 기반 IDS와 비정상 기반 IDS의 탐지 원리, 그리고 호스트 기반 IDS와 네트워크 기반 IDS의 관찰 위치를 구분하는지를 묻는다.

핵심 개념

시그니처 기반 IDS는 이미 알려진 공격 패턴이나 규칙과 일치하는지를 보는 방식이다. 비정상 기반 IDS는 정상 행위의 기준선을 만든 뒤 그 범위를 벗어나는 행위를 이상으로 판단한다. 호스트 기반 IDS는 개별 호스트 내부의 로그와 행위를 보고, 네트워크 기반 IDS는 네트워크 구간의 트래픽을 본다.

선지별 해설

① X. 틀린 부분은 '신종 공격이나 변형된 공격을 능동적으로 탐지할 확률이 높은'이다. 시그니처 기반 IDS는 알려진 공격의 시그니처가 있을 때 탐지에 유리하지만, 신종 공격이나 시그니처를 바꾼 변형 공격에는 약하다. 올바르게는 '이미 알려진 공격 패턴을 빠르게 탐지하는 데 유리하다'이다.
② O. 비정상 기반 IDS는 정상 행위 모델을 먼저 만들고, 그 모델에서 벗어나는 행위를 비정상으로 판단한다.
③ O. 호스트 기반 IDS는 호스트 내부의 시스템 로그, 응용 프로그램 로그, 파일 변경, 프로세스 행위 등을 이용해 해당 호스트에 대한 공격을 탐지한다.
④ O. 네트워크 기반 IDS는 네트워크에서 전송되는 패킷과 트래픽을 수집해 분석함으로써 공격 징후를 탐지한다.

오답 포인트

시그니처 기반과 비정상 기반의 장단점을 서로 뒤집어 놓으면 틀리기 쉽다. '신종·변형 공격 탐지'는 비정상 기반의 강점으로 자주 연결되고, 시그니처 기반의 핵심은 '이미 알려진 패턴과의 일치 여부'이다.

NoteBase

다시 나오면 이렇게 판단

IDS 문제가 나오면 먼저 탐지 기준이 알려진 패턴 일치인지, 정상 모델 이탈인지부터 구분한다. 그다음 관찰 위치가 호스트 내부인지 네트워크 구간인지 확인하면 선지의 O/X를 빠르게 정리할 수 있다.

암기 포인트

시그니처 기반은 알려진 패턴 탐지, 비정상 기반은 정상 기준선 이탈 탐지, HIDS는 호스트 내부 관찰, NIDS는 네트워크 트래픽 관찰이다.

NoteBase

문 23. 랜섬웨어(ransomware)에 대한 설명으로 옳지 않은 것은?

① 공격자는 사용자의 컴퓨터를 장악하거나 데이터를 암호화한 후 정상적인 작동을 조건으로 대가를 요구한다.
② 암호화된 파일을 풀어 주는 대가로 비트코인(Bitcoin) 등 가상자산을 요구하는 공격으로 진화하고 있다.
③ 랜섬웨어 중 하나인 워너크라이(WannaCry)는 리눅스의 원격 접속 프로토콜의 취약점을 활용하였다.
④ 랜섬웨어를 제작하여 공급·판매하는 방식인 RaaS(Ransomware as a Service)가 등장하였다.

정답 3번

출제 포인트

이 문제는 랜섬웨어의 일반적 특징과 대표 사례인 워너크라이의 감염 경로를 정확히 구별할 수 있는지를 묻는다.

핵심 개념

랜섬웨어는 시스템이나 데이터를 사용할 수 없게 만든 뒤 금전을 요구하는 악성코드이다.
워너크라이는 2017년에 대규모로 확산된 랜섬웨어로, 리눅스 원격 접속 프로토콜이 아니라 윈도우의 SMB 취약점을 악용한 사례이다.
RaaS는 랜섬웨어를 서비스처럼 제작·배포·판매하여 공격자가 쉽게 이용하게 한 범죄 비즈니스 모델이다.

선지별 해설

1번: O. 랜섬웨어는 시스템을 잠그거나 데이터를 암호화하여 정상 사용을 방해한 뒤, 이를 복구해 주는 조건으로 대가를 요구하는 방식이 핵심이다.
2번: O. 최근 랜섬웨어는 파일 복호화 대가로 비트코인 등 추적이 상대적으로 어려운 가상자산을 요구하는 형태로 널리 사용된다.
3번: X. 틀린 표현은 "리눅스의 원격 접속 프로토콜"이다. 워너크라이는 리눅스 원격 접속 취약점을 이용한 것이 아니라 윈도우의 SMB 파일 공유 프로토콜 취약점(EternalBlue 계열)을 악용하여 확산되었다.
4번: O. RaaS는 랜섬웨어를 직접 개발하지 않아도 임대·구매하여 공격에 활용할 수 있게 한 서비스형 범죄 모델로, 실제로 랜섬웨어 생태계 확산에 큰 역할을 하였다.

오답 포인트

워너크라이를 단순히 "원격 접속 취약점 악용" 정도로만 기억하면 운영체제와 프로토콜을 혼동하기 쉽다. 이 문항은 3번에서 리눅스와 원격 접속 프로토콜이라는 말을 끼워 넣어 SMB 기반 확산 사실을 흐리게 만든 점이 함정이다.

다시 나오면 이렇게 판단

랜섬웨어 문항은 먼저 일반 특징인지 대표 사례의 세부 감염 경로인지 구분한 뒤 판단한다. 사례형 선지에서는 운영체제, 악용 프로토콜, 공격 방식 같은 고유 사실이 바뀌었는지를 확인하면 정오를 빠르게 가를 수 있다.

NoteBase

암기 포인트

랜섬웨어는 암호화·금전요구, 워너크라이는 윈도우 SMB 취약점, RaaS는 서비스형 랜섬웨어이다.

문 24. IPSec 터널모드에 대한 설명으로 옳지 않은 것은?

① 양측 호스트가 속한 라우터 또는 게이트웨이 간에 IPSec 터널링을 설정한다.

② 호스트가 생성한 전송계층의 세그먼트를 페이로드(payload)로 취급하고 IP 헤더를 추가한다.

③ ESP와 결합하면, 터널링 구간에서 양측 호스트의 IP 주소는 외부 공격자에게 숨겨진다.

④ SA(Security Association) 생성, 키교환 및 상호인증을 위해 IKE 프로토콜을 사용한다.

정답 2번

출제 포인트

이 문제는 IPSec 터널 모드가 무엇을 캡슐화하는지와 ESP, IKE의 역할을 구별할 수 있는지를 묻는다.

핵심 개념

터널 모드는 원래의 IP 패킷 전체를 새로운 IP 패킷의 페이로드로 감싸는 방식이다. 전송 모드는 원래 IP 헤더는 유지하고 전송계층 payload만 보호하는 방식이다. ESP는 기밀성과 무결성 보호를 담당하고, IKE는 SA 생성, 키교환, 상호인증을 담당한다.

선지별 해설

1번 O: 터널 모드는 보통 양 끝단의 보안 게이트웨이 또는 라우터 사이에 설정되어 사이트 간 통신을 보호한다. 양측 호스트가 속한 네트워크 경계 장비 사이에 터널을 만든다는 설명이므로 옳다.
2번 X: 틀린 부분은 "전송계층의 세그먼트를 페이로드로 취급"한다는 표현이다. 터널 모드는 세그먼트가 아니라 기존 IP 헤더를 포함한 원래 IP 패킷 전체를 payload로 캡슐화하고 그 앞에 새로운 IP 헤더를 추가한다.
3번 O: 터널 모드에서 ESP를 사용하면 원래 IP 패킷 전체가 암호화되어 내부 호스트의 IP 주소가 외부에 직접 드러나지 않는다. 외부에서는 새로 붙은 바깥쪽 IP 헤더의 주소만 보이므로 옳다.
4번 O: IPSec에서 SA 협상, 키교환, 상호인증은 IKE가 담당한다. 따라서 IKE 프로토콜을 사용한다는 설명은 옳다.

오답 포인트

터널 모드와 전송 모드를 모두 "IP 헤더를 붙인다"는 수준으로만 외우면 2번에 속기 쉽다. 이 문항의 함정은 무엇을 payload로 보느냐에 있으며, 터널 모드는 기존 IP 패킷 전체, 전송 모드는 상위계층 payload라는 차이를 묻는다.

다시 나오면 이렇게 판단

문장에서 캡슐화 대상이 세그먼트인지 기존 IP 패킷 전체인지부터 확인하면 된다. 기존 IP 헤더를 숨기고 새 IP 헤더를 붙이면 터널 모드이고, 기존 IP 헤더를 유지한 채 상위계층 데이터만 보호하면 전송 모드이다.

NoteBase

암기 포인트

터널 모드는 패킷 전체를 한 번 더 감싸고, 전송 모드는 원래 IP 헤더를 둔 채 payload만 보호한다.

NoteBase

문 25. 「개인정보 보호법 시행령」상 개인정보보호위원회가 개인정보처리자에게 자료의 제출을 요구할 수 있는 사항에 해당하지 않는 것은?

① 개인정보처리자가 처리하는 이동형 영상정보처리기기의 설치·운영에 관한 사항

② 개인정보 보호책임자에게 부과된 과태료에 관한 사항

③ 개인정보의 안전성 확보를 위한 기술적·관리적·물리적 조치에 관한 사항

④ 정보주체의 열람, 개인정보의 정정·삭제·처리정지의 요구 및 조치 현황에 관한 사항

정답 2번

쟁점

이 문제는 「개인정보 보호법 시행령」상 개인정보보호위원회가 개인정보처리자에게 자료 제출을 요구할 수 있는 범위에 관한 문제이다.
핵심은 자료제출 요구 대상에 포함된 사항과 포함되지 않은 사항을 구별하는 것이다.

용어 풀이

개인정보 보호책임자란 법 제31조에 따라 개인정보 처리에 관한 업무를 총괄해서 책임지는 자이다.

핵심 구분

시행령 제13조 제1항은 자료제출 요구 범위를 열거하고 있다.
여기에는 이동형 영상정보처리기기의 설치·운영, 안전성 확보 조치, 정보주체의 열람·정정·삭제·처리정지 요구 및 조치 현황이 포함된다.
반면 개인정보 보호책임자와 관련해서는 지정 여부만 포함될 뿐, 과태료 부과 사항은 포함되지 않는다.

NoteBase

선지별 해설

1번 O
- 자료제출 요구 범위에는 개인정보파일의 관리와 고정형 또는 이동형 영상정보처리기기의 설치·운영에 관한 사항이 포함된다.
- 따라서 이동형 영상정보처리기기의 설치·운영에 관한 사항은 요구할 수 있는 사항이다.

2번 X
- 시행령이 열거한 것은 개인정보 보호책임자의 지정 여부에 관한 사항이지, 개인정보 보호책임자에게 부과된 과태료에 관한 사항이 아니다.
- 틀린 표현: "개인정보 보호책임자에게 부과된 과태료에 관한 사항"
- 올바른 표현: "법 제31조에 따른 개인정보 보호책임자의 지정 여부에 관한 사항"

3번 O
- 자료제출 요구 범위에는 개인정보의 안전성 확보를 위한 기술적·관리적·물리적 조치에 관한 사항이 포함된다.
- 따라서 3번은 시행령의 열거 내용과 일치한다.

4번 O
- 자료제출 요구 범위에는 정보주체의 열람, 개인정보의 정정·삭제·처리정지 요구 및 조치 현황에 관한 사항이 포함된다.
- 따라서 4번도 요구할 수 있는 사항에 해당한다.

오답 포인트

개인정보 보호책임자와 관련된 내용이면 모두 자료제출 요구 대상이라고 넓게 잡으면 틀린다. 이 조문은 포괄적으로 묻지 않고 지정 여부처럼 열거된 사항만 인정한다는 점이 함정이다.

다시 나오면 이렇게 판단

열거형 법령 문제는 먼저 조문이 무엇을 항목별로 포함하는지 본다. 그다음 선지의 표현이 조문 문구와 정확히 일치하는지, 아니면 비슷한 주제를 다른 표현으로 바꿔 넣은 것인지를 구별하면 된다.

암기 포인트

자료제출 요구 범위는 장비 운영, 안전조치, 정보주체 권리 조치 현황, 보호책임자 지정 여부까지이고, 과태료는 아니다.

NoteBase