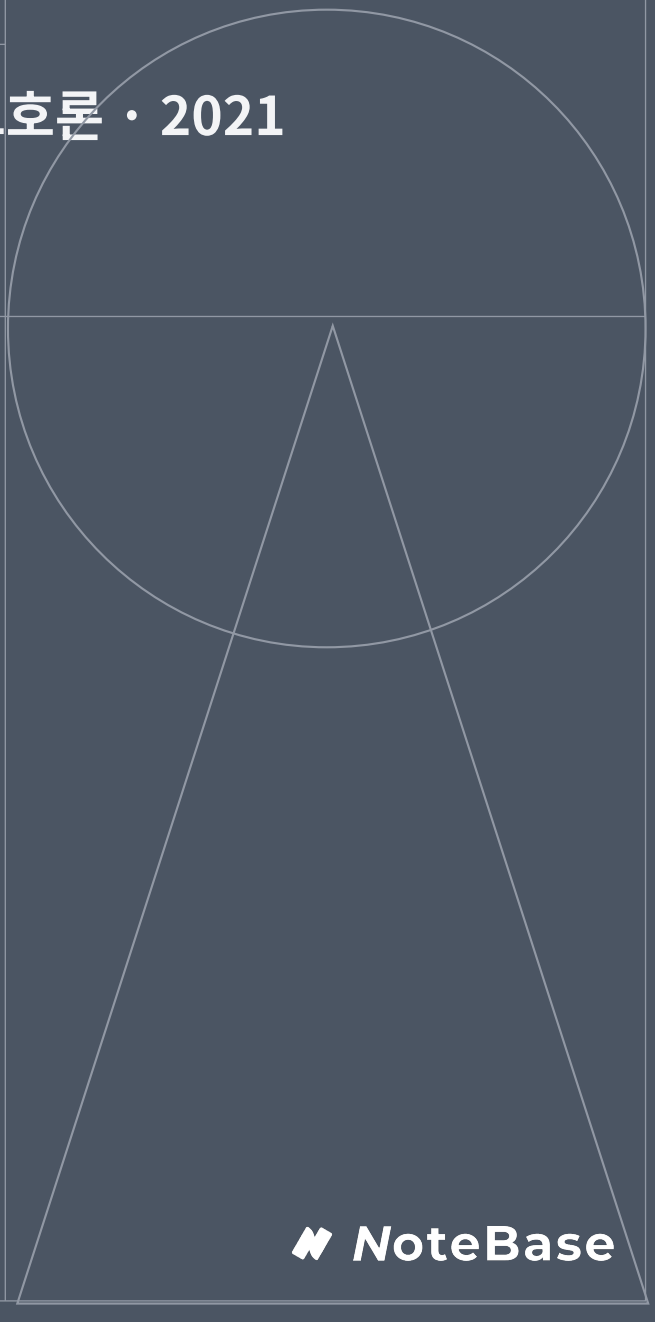
기출OX 해설집

공무원/군무원/9급 · 정보보호론 · 2021



NoteBase

기출OX 해설집

공무원/군무원/9급 · 정보보호론 · 2021

공무원/군무원/9급 · 정보보호론 · 2021

1. 응용 수준 취약점에 대한 설명으로 옳지 않은 것은?
   ① 버퍼오버플로우는 메모리나 버퍼의 블록 크기보다 더 많은 데이터를 넣음으로써 결함을 발생시키는 취약점이다.
   ② 크로스 사이트 스크립팅은 웹사이트 관리자가 아닌 이가 웹 페이지에 악성 스크립트를 삽입할 수 있는 취약점이다. 주로 전자 게시판에 악성 스크립트가 담긴 글을 올리는 형태로 이루어진다.
   ③ SSI인젝션은 조작된 XPath(XML Path) 쿼리를 보냄으로써 비정상적인 데이터를 쿼리해 올 수 있는 취약점이다.
   ④ SQL인젝션은 SQL문으로 해석될 수 있는 입력을 시도하여 데이터베이스에 접근할 수 있는 취약점이다.

정답 3번

출제 포인트

응용 프로그램 취약점의 공격 대상과 입력 형태를 구분하는 문제이다. 특히 SSI 인젝션과 XPath 인젝션을 혼동하지 않아야 한다.

핵심 개념

버퍼 오버플로우는 정해진 메모리 버퍼의 용량을 넘는 데이터를 입력하여 인접 메모리를 덮어쓰는 취약점이다.
크로스 사이트 스크립팅(XSS)은 공격자가 웹 페이지에 악성 스크립트를 삽입하여 다른 이용자의 브라우저에서 실행되게 하는 취약점이다.
SSI 인젝션은 웹 서버가 해석하는 SSI 지시문을 입력값에 삽입하여 서버 측에서 의도하지 않은 명령 실행이나 파일 접근 등을 일으키는 취약점이다.
XPath 인젝션은 조작된 XPath 쿼리를 주입하여 XML 데이터에 비정상적으로 접근하는 취약점이고, SQL 인젝션은 SQL로 해석될 입력을 주입하여 데이터베이스에 비정상적으로 접근하는 취약점이다.

NoteBase

선지별 해설

① O — 버퍼 크기보다 많은 데이터를 입력하면 버퍼 경계를 넘어 인접 메모리를 덮어써 오류나 비정상 동작을 일으킬 수 있으므로 옳다.
② O — 웹 페이지에 악성 스크립트를 삽입해 다른 이용자의 브라우저에서 실행되게 하는 취약점은 크로스 사이트 스크립팅이다. 전자 게시판에 악성 스크립트가 포함된 글을 저장하는 방식은 저장형 XSS의 대표적인 형태이므로 옳다.
③ X — 틀린 표현은 'SSI인젝션'이다. 조작된 XPath 쿼리를 보내 XML 데이터를 비정상적으로 조회하는 취약점은 SSI 인젝션이 아니라 XPath 인젝션이다. 올바르게는 'XPath 인젝션은 조작된 XPath 쿼리를 주입하여 XML 데이터에 비정상적으로 접근할 수 있는 취약점이다'이다.
④ O — 입력값이 SQL문의 일부로 해석되도록 조작하여 데이터베이스의 조회·변경 등 비정상적인 접근을 시도하는 취약점은 SQL 인젝션이므로 옳다.

오답 포인트

③에는 XPath라는 결정적 단서가 있는데 취약점 이름만 SSI 인젝션으로 바꾸어 놓았다. '인젝션'이라는 공통 표현만 보고 판단하면 SSI, XPath, SQL 인젝션을 혼동하기 쉽다.

다시 나오면 이렇게 판단

공격에 사용되는 언어와 해석 주체를 먼저 대응시킨다. XPath 쿼리와 XML 데이터는 XPath 인젝션, SQL문과 데이터베이스는 SQL 인젝션, 웹 서버가 해석하는 SSI 지시문은 SSI 인젝션으로 판단한다.

암기 포인트

XPath→XML, SQL→DB, SSI→서버 측 지시문으로 연결한다.

NoteBase

2. 전자서명법에 대한 설명으로 옳지 않은 것은?
① “전자문서”란 정보처리시스템에 의하여 전자적 형태로 작성되어 송신 또는 수신되거나 저장된 정보를 말한다.
② 당사자 간의 약정에 따라 행해진 서명, 서명날인 또는 기명날인 방식의 전자서명은 제3의 신뢰기관이 개입하지 않았으므로 전자서명법 상 효력을 가지지 않는다.
③ “인증서”란 전자서명생성정보가 가입자에게 유일하게 속한다는 사실 등을 확인하고 이를 증명하는 전자적 정보를 말한다.
④ “전자서명생성정보”란 전자서명을 생성하기 위하여 이용하는 전자적 정보를 말한다.

정답 2번

쟁점

이 문제는 전자서명법상 전자문서·전자서명인증·전자서명생성정보의 정의와 전자서명의 효력에 관한 문제이다. 핵심은 전자서명의 법적 효력이 제3의 신뢰기관 개입 여부만으로 결정되는 것은 아니라는 점이다.

용어 풀이

전자서명인증은 전자서명생성정보가 가입자에게 유일하게 속한다는 사실을 확인하고 증명하는 행위이다. 전자서명생성정보는 전자서명을 만들 때 이용하는 전자적 정보이다.

핵심 구분

전자서명법 제3조에 따르면 전자서명은 전자적 형태라는 이유만으로 서명·서명날인·기명날인으로서의 효력이 부인되지 않는다. 법령이나 당사자 간 약정에 따라 서명 등의 방식으로 전자서명을 선택한 경우에는 그에 따른 효력이 있다. 따라서 인증기관 등 제3자의 개입 여부와 전자서명의 효력 유무를 곧바로 동일시하면 안 된다.

NoteBase

선지별 해설

① O
전자문서는 정보처리시스템에 의하여 전자적 형태로 작성되어 송신 또는 수신되거나 저장된 정보를 말하므로 법률상 정의에 맞는다.

② X
제3의 신뢰기관이 개입하지 않았다는 사실만으로 전자서명법상 효력이 부정되는 것은 아니다. 전자서명은 전자적 형태라는 이유만으로 서명 등의 효력이 부인되지 않으며, 법령이나 당사자 간 약정에 따라 전자서명을 선택한 경우에는 그에 따른 효력이 있다.
틀린 표현: '제3의 신뢰기관이 개입하지 않았으므로 전자서명법상 효력을 가지지 않는다.'
올바른 표현: '제3의 신뢰기관이 개입하지 않았다는 이유만으로 전자서명의 효력이 부정되지는 않는다.'

③ O
전자서명인증은 전자서명생성정보가 가입자에게 유일하게 속한다는 사실 등을 확인하고 이를 증명하는 행위를 말하므로 옳다.

④ O
전자서명생성정보는 전자서명을 생성하기 위하여 이용하는 전자적 정보를 말하므로 옳다.

오답 포인트

②의 '제3의 신뢰기관이 개입하지 않았으므로 효력이 없다'는 표현이 함정이다. 인증 여부와 전자서명의 법적 효력은 같은 개념이 아니며, 제3자 개입은 모든 전자서명의 효력에 필요한 일률적 요건이 아니다.

다시 나오면 이렇게 판단

정의 선지는 법 조문의 핵심 동사와 대상을 대응시킨다. 효력 선지는 '전자적 형태라는 이유만으로 효력이 부인되는가'와 '제3자 인증이 반드시 필요한가'를 나누어 판단한다.

암기 포인트

전자문서=전자적 작성·송수신·저장, 전자서명인증=유일 귀속의 확인·증명, 전자서명생성정보=서명 생성에 쓰는 정보, 제3자 미개입≠당연 무효이다.

NoteBase

3. RSA 암호알고리즘을 위해 두 개의 소수가 p=3, q=11일 경우, 공개키(n)과 암호화 공개키(e=7)에 대응되는 복호용 개인키(d)로 적절한 것은?

① n=33, d=3 ② n=21, d=5

③ n=21, d=3 ④ n=33, d=5

정답 1번

출제 포인트

RSA에서 두 소수로 공개키의 모듈러스 n을 구하고, 공개 지수 e의 모듈러 역원인 복호용 개인키 d를 구하는 문제이다.

조건 정리

주어진 값: 두 소수는 $p = 3, q = 11$이고 암호화 공개 지수는 $e = 7$이다.
구해야 할 값: 공개키의 모듈러스 n과 복호용 개인 지수 d이다.
주의할 조건: d는 ed를 $\varphi(n)$으로 나눈 나머지가 1이 되게 하는 수이다.

사용할 공식

$n = pq$
$\varphi(n) = (p-1)(q-1)$
ed≡1±od(n)
RSA는 서로 다른 두 소수의 곱을 모듈러스 n으로 사용하고, 복호 지수 d를 공개 지수 e의 $\varphi(n)$에 대한 모듈러 역원으로 정하므로 이 공식을 사용한다.

계산 과정

1. 모듈러스를 계산하면 $n = pq = 3 \times 11 = 33$이다.
2. 오일러 피 함수의 값을 계산하면 $\varphi(n) = (3-1)(11-1) = 2 \times 10 = 20$이다.
3. 7d≡1±od20을 만족해야 한다. $d = 3$이면 $7 \times 3 = 21 = 20 + 1$이므로 조건을 만족한다.
따라서 $n = 33, d = 3$이다.

NoteBase

선지 판단

① O — $n = 3 \times 11 = 33$이고 7×3=21≡1±od20이므로 $d = 3$이다. 계산 결과와 모두 일치한다.
② X — $n = 21$이 틀렸고 $d = 5$도 틀렸다. 올바르게는 $n = 33$, $d = 3$이다. n은 $p + q$나 다른 조합이 아니라 pq로 계산하며, $7 \times 5 = 35$는 20으로 나눈 나머지가 15이므로 역원 조건을 만족하지 않는다.
③ X — $d = 3$은 맞지만 $n = 21$이 틀렸다. 올바르게는 $n = pq = 3 \times 11 = 33$이므로 $n = 33$, $d = 3$이다.
④ X — $n = 33$은 맞지만 $d = 5$가 틀렸다. 올바르게는 7d≡1±od20을 만족하는 $d = 3$이므로 $n = 33$, $d = 3$이다.

오답 포인트

핵심 함정은 n을 두 소수의 곱으로 계산하지 않거나, d를 임의로 고르는 것이다. 특히 선지 ③은 $d = 3$만 맞고 $n = 21$이 틀리며, 선지 ④는 $n = 33$만 맞고 $d = 5$가 틀린 부분 정답형 선지이다.

다시 나오면 이렇게 판단

RSA 키 계산 문제는 먼저 $n = pq$를 구하고, 다음으로 $\varphi(n) = (p - 1)(q - 1)$을 구한 뒤, 마지막으로 ed≡1±od(n)을 만족하는 d를 찾는 순서로 판단한다.

암기 포인트

RSA에서는 $n = pq$, $\varphi(n) = (p - 1)(q - 1)$, d=e^-1±od(n)이다.

NoteBase

4. Diffie-Hellman 키 공유 프로토콜에서, 공개정보인 소수 p=11, 원시원소 g=7 인 경우, 갑이 자신의 비밀키(x)를 5로, 을이 자신의 비밀키(y)를 3으로 선택했을 경우, 갑과 을이 공유하는 세션키로 옳은 것은?

① 10 ② 7
③ 8 ④ 5

정답 1번

출제 포인트

Diffie-Hellman 키 공유에서 상대방의 공개키를 자신의 비밀키만큼 거듭제곱한 뒤 소수 p로 나눈 나머지를 구하는 문제이다.

조건 정리

주어진 값: 소수 $p = 11$, 원시원소 $g = 7$, 갑의 비밀키 $x = 5$, 을의 비밀키 $y = 3$이다.
구해야 할 값: 갑과 을이 공유하는 세션키이다.
주의할 조건: 거듭제곱의 결과 자체가 아니라 이를 $p = 11$로 나눈 나머지를 사용한다.

사용할 공식

을의 공개키는 Y=g^y p이고, 갑이 구하는 공유 세션키는 K=Y^x p이다. 따라서 K=g^xy p가 된다.
이 공식을 쓰는 이유: Diffie-Hellman에서는 각자가 상대방의 공개키에 자신의 비밀키를 지수로 적용하므로 양쪽 모두 같은 값 g^xy p를 얻는다.

계산 과정

1. 을의 공개키를 계산하면 Y=7^3 11=343 11=2이다.
2. 갑은 을의 공개키에 자신의 비밀키 $x = 5$를 적용한다.
K=2^5 11=32 11=10
3. 따라서 공유 세션키는 10이다.

선지 판단

① O — 계산 결과 공유 세션키가 10이므로 옳다.
② X — 7은 공개된 원시원소 g일 뿐 공유 세션키가 아니다. 틀린 값 7은 10으로 고쳐야 한다.
③ X — g^xy p=7^15 11의 값은 8이 아니라 10이다. 틀린 값 8은 10으로 고쳐야 한다.
④ X — 5는 중간 계산인 7^2 11에서 나오는 값이며 최종 공유 세션키가 아니다. 틀린 값 5는 10으로 고쳐야 한다.
계산 결과가 10이므로 정답은 1번이다.

NoteBase

오답 포인트

공개된 원시원소 7을 세션키로 착각하거나, 거듭제곱 도중 나온 나머지 5를 최종값으로 선택하기 쉽다. 상대방의 공개키를 구한 뒤 자신의 비밀키만큼 다시 거듭제곱하고 마지막에 *p*로 나눈 나머지까지 계산해야 한다.

다시 나오면 이렇게 판단

먼저 상대방의 공개키 g^상대 비밀키 p를 구하고, 그 값에 자신의 비밀키를 지수로 적용한 뒤 다시 *p*로 나눈다. 또는 곧바로 g^xy p를 계산해도 같은 결과가 나온다.

암기 포인트

Diffie-Hellman 공유키는 K=g^xy p이며, 공개키 계산과 공유키 계산의 두 단계에서 모두 모듈러 연산을 적용한다.

NoteBase

5. 정보보호의 3대 요소로 옳지 않은 것은?
① 비인가자, 불법 침입자의 접근 제어를 통해 비밀 정보가 누출되지 않도록 보장하는 기밀성
② 메시지의 송수신이나 교환 후, 또는 통신이나 처리가 실행된 후에 그 사실을 증명함으로써 사실 부인을 방지하는 부인방지
③ 인가된 사용자가 적시, 적소에 필요 정보에 접근할 수 있고 사용 가능하도록 보장하는 가용성
④ 불법 사용자에 의해 정보 및 소프트웨어가 변경, 삭제, 생성되는 것으로부터 보호하여 원래 상태를 보존 유지하는 무결성

정답 2번

출제 포인트

정보보호의 3대 요소인 기밀성·무결성·가용성의 의미와 부인방지를 구별하는 문제이다.

핵심 개념

기밀성: 인가된 사용자만 정보에 접근할 수 있도록 하여 무단 노출을 막는 성질이다. 키워드는 접근 통제와 비밀 유지이다.
무결성: 정보가 권한 없이 변경·삭제·생성되지 않고 정확한 상태로 유지되는 성질이다. 키워드는 변조 방지와 정확성이다.
가용성: 인가된 사용자가 필요할 때 정보와 시스템을 정상적으로 이용할 수 있는 성질이다. 키워드는 적시 접근과 서비스 이용이다.
부인방지: 메시지의 송수신이나 행위가 이루어진 뒤 당사자가 그 사실을 부인하지 못하게 하는 성질이다.
정보보호의 3대 요소에는 포함되지 않는다.

선지별 해설

① O — 비인가자나 불법 침입자의 접근을 통제하여 비밀 정보의 누출을 막는 것은 기밀성이다.
② X — '송수신·교환 또는 처리 사실의 부인을 방지한다'는 설명은 부인방지에 해당하며, 정보보호의 3대 요소에 포함되지 않는다. 올바르게는 '부인방지는 행위 후 그 사실을 부인하지 못하도록 보장하는 보안 특성이다'라고 해야 한다.
③ O — 인가된 사용자가 필요할 때 정보에 접근하여 사용할 수 있도록 보장하는 것은 가용성이다.
④ O — 불법 사용자가 정보나 소프트웨어를 변경·삭제·생성하지 못하게 하여 원래의 정확한 상태를 유지하는 것은 무결성이다.

NoteBase

오답 포인트

②는 실제 보안 목표인 부인방지를 설명하므로 그 자체는 틀린 정의가 아니다. 그러나 문제는 정보보호의 '3대 요소'를 묻고 있으므로 CIA에 속하지 않는 부인방지가 정답이다.

다시 나오면 이렇게 판단

누출 방지는 기밀성, 무단 변경 방지는 무결성, 필요할 때 이용 가능은 가용성으로 판단한다. 행위 사실을 나중에 부인하지 못하게 한다는 표현은 부인방지로 분류한다.

암기 포인트

CIA는 기밀성(Confidentiality)·무결성(Integrity)·가용성(Availability)이고, 부인방지는 CIA 밖의 추가 보안 특성이다.

NoteBase

6. 우리나라가 개발해 국제표준화한 암호 알고리즘만으로 짝지은 것은?
   ① 블록 암호 알고리즘(SEED) - 서명 알고리즘(KCDSA)
   ② 블록 암호 알고리즘(AES) - 서명 알고리즘(RSA)
   ③ 블록 암호 알고리즘(triple DES) - 서명 알고리즘(DSA)
   ④ 블록 암호 알고리즘(ARIA) - 서명 알고리즘(ECDSA)

정답 1번

출제 포인트

우리나라가 개발하고 국제표준으로 채택된 블록 암호 알고리즘과 전자서명 알고리즘을 구별하는 문제이다.

핵심 개념

SEED: 우리나라에서 개발된 128비트 블록 암호 알고리즘으로 국제표준에 포함되었다.
KCDSA: 우리나라에서 개발된 전자서명 알고리즘으로 국제표준에 포함되었다.
ARIA: 우리나라에서 개발된 블록 암호 알고리즘으로 국제표준에 포함되었지만, ECDSA는 우리나라가 개발한 알고리즘이 아니다.
AES·RSA·triple DES·DSA·ECDSA는 국제적으로 널리 쓰이지만 우리나라가 개발한 알고리즘은 아니다.

선지별 해설

① O — SEED는 우리나라가 개발한 블록 암호 알고리즘이고, KCDSA는 우리나라가 개발한 전자서명 알고리즘이다. 두 알고리즘 모두 국제표준에 포함되었으므로 옳은 짝이다.
② X — 틀린 표현은 'AES—RSA가 우리나라가 개발해 국제표준화한 알고리즘의 짝'이라는 부분이다. AES는 벨기에에서 개발된 Rijndael을 미국이 표준으로 선정한 블록 암호이고, RSA도 우리나라가 개발한 전자서명 알고리즘이 아니다. 올바르게는 AES와 RSA 모두 우리나라 개발 알고리즘이 아니다.
③ X — 틀린 표현은 'triple DES—DSA가 우리나라가 개발해 국제표준화한 알고리즘의 짝'이라는 부분이다. triple DES는 DES를 세 번 적용하도록 확장한 블록 암호이고, DSA는 미국의 전자서명 표준으로 제정된 알고리즘이다. 올바르게는 triple DES와 DSA 모두 우리나라 개발 알고리즘이 아니다.
④ X — ARIA는 우리나라가 개발하고 국제표준화한 블록 암호이지만, ECDSA는 타원곡선 암호를 이용하는 전자서명 알고리즘으로 우리나라가 개발한 알고리즘이 아니다. 틀린 부분은 ECDSA까지 우리나라 개발 알고리즘이라는 전제이며, ECDSA를 KCDSA로 고치면 우리나라가 개발해 국제표준화한 알고리즘끼리의 짝이 된다.

NoteBase

오답 포인트

④는 ARIA가 우리나라 개발 알고리즘이라는 점을 이용한 함정이다. 한쪽만 조건을 만족해서는 안 되며, 연결된 두 알고리즘이 모두 '우리나라 개발'과 '국제표준화' 조건을 충족해야 한다.

다시 나오면 이렇게 판단

먼저 블록 암호와 전자서명 알고리즘을 나눈 뒤 개발 주체를 확인한다. 우리나라 개발 블록 암호인 SEED·ARIA와 우리나라 개발 전자서명 알고리즘인 KCDSA를 기준으로 각 짝의 두 항목을 모두 검사한다.

암기 포인트

국산 블록 암호는 SEED·ARIA, 국산 전자서명은 KCDSA이다.

NoteBase

7. 일어날 수 있는 모든 가능한 경우에 대하여 조사하는 형태의 공격으로 적절한 것은?
① 전수조사 공격 ② 중간자 공격
③ 생일 공격 ④ 사전 공격

정답 1번

출제 포인트

이 문제는 공격자가 탐색하는 후보의 범위와 공격 방식에 따라 전수조사 공격, 중간자 공격, 생일 공격, 사전 공격을 구별할 수 있는지를 묻는다.

핵심 개념

전수조사 공격: 가능한 키나 비밀번호 후보를 빠짐없이 하나씩 대입하여 정답을 찾는 공격이다. 키워드는 '모든 가능한 경우'이다.
사전 공격: 사전에 수집한 단어와 자주 쓰는 비밀번호 후보만 우선 대입하는 공격이다. 키워드는 '선별된 단어 목록'이다.
중간자 공격: 통신하는 두 당사자 사이에 공격자가 끼어들어 정보를 가로채거나 변조하는 공격이다. 키워드는 '통신 사이 개입'이다.
생일 공격: 해시 함수에서 같은 해시값을 갖는 서로 다른 입력, 즉 충돌을 생일 문제의 확률적 성질을 이용해 찾는 공격이다. 키워드는 '해시 충돌'이다.

선지별 해설

① O — 전수조사 공격은 가능한 모든 후보를 차례로 검사하므로 문제의 설명과 정확히 일치한다.
② X — 틀린 표현은 '중간자 공격'이다. 올바르게는 통신 당사자 사이에 개입하여 정보를 가로채거나 변조하는 공격이며, 모든 후보를 조사하는 공격은 전수조사 공격이다.
③ X — 틀린 표현은 '생일 공격'이다. 올바르게는 해시값의 충돌을 확률적으로 찾는 공격이며, 모든 가능한 경우를 대입하는 공격은 전수조사 공격이다.
④ X — 틀린 표현은 '사전 공격'이다. 올바르게는 사전에 준비한 단어·비밀번호 목록의 후보를 우선 대입하는 공격이며, 모든 후보를 빠짐없이 조사하는 공격은 전수조사 공격이다.

오답 포인트

④ 사전 공격도 여러 후보를 대입한다는 점 때문에 ①과 혼동하기 쉽다. 그러나 사전 공격은 가능성이 높은 후보 목록만 사용하고, 전수조사 공격은 가능한 경우 전체를 탐색한다는 차이가 있다.

NoteBase

다시 나오면 이렇게 판단

‘모든 경우·가능한 조합 전체’가 보이면 전수조사 공격, ‘단어 목록’이면 사전 공격, ‘통신 사이 개입’이면 중간자 공격, ‘해시 충돌’이면 생일 공격으로 판단한다.

암기 포인트

전체 후보는 전수조사, 단어 목록은 사전, 통신 사이에는 중간자, 해시 충돌은 생일 공격이다.

NoteBase

8. 정보보호제품 평가인증제도에 대한 설명으로 옳지 않은 것은?

① 정보보호제품의 보증수준을 정하기 위한 공통평가기준에서 미리 정의된 보증등급으로, EAL1, EAL2, EAL3, EAL4, EAL5, EAL6의 6개의 보증 등급으로 구분된다. EAL1은 최고의 평가보증등급이고, EAL6은 최저의 평가보증등급이다.

② 정보보호시스템의 성능과 신뢰도에 관한 기준을 정하여 고시하고, 정보보호시스템을 제조하거나 수입하는 자에게 그 기준을 지킬 것을 권고할 수 있다.

③ 공통평가기준 1부는 정보보호시스템 보안성 평가의 원칙과 일반개념을 정의하고 평가의 일반적인 모델을 설명하는 소개부분으로, IT 보안목적을 표현하고 IT 보안요구사항을 선택·정의하며, 제품 및 시스템의 상위수준 명세를 작성하기 위한 구조를 소개한다.

④ "보호프로파일"이라 함은, 평가대상 범주를 위한 특정 소비자의 요구에 부합하는 구현에 독립적인 보안요구사항의 집합을 말하며, "보안목표명세서"라 함은 식별된 평가대상의 평가를 위한 근거로 사용되는 보안요구사항과 구현 명세의 집합을 말한다.

정답 1번

쟁점

정보보호제품 평가인증제도의 공통평가기준(CC), 평가보증등급(EAL), 보호프로파일(PP), 보안목표명세서(ST)의 의미를 구별하는 문제이다. 핵심은 EAL의 등급 수와 보증 수준의 방향을 정확히 아는 것이다.

NoteBase

용어 풀이

평가보증등급(EAL)은 정보기술 제품이나 시스템이 보안 요구사항을 충족한다는 확신의 정도를 평가 깊이와 엄격성에 따라 나타낸 등급이다.
보호프로파일(PP)은 일정한 제품·시스템 유형에 공통으로 적용할 수 있도록 특정 소비자 요구를 반영한 구현 독립적 보안요구사항의 집합이다.
보안목표명세서(ST)는 식별된 특정 평가대상(TOE)의 평가 근거가 되는 구현 의존적 보안요구사항과 구현 명세의 집합이다.

핵심 구분

EAL은 EAL1부터 EAL7까지 7개 등급이며, 숫자가 커질수록 평가의 깊이와 엄격성이 높아져 보증 수준도 높아진다. 따라서 EAL1이 최저 등급이고 EAL7이 최고 등급이다. PP는 제품군에 공통되는 구현 독립적 요구사항이고, ST는 특정 평가대상에 대한 구현 의존적 명세이다.

선지별 해설

① X — ‘EAL1부터 EAL6까지 6개 등급’, ‘EAL1은 최고’, ‘EAL6은 최저’라는 부분이 모두 틀렸다. 올바르게는 EAL1부터 EAL7까지 7개 등급으로 구분하며, EAL1이 최저이고 EAL7이 최고이다. 따라서 옳지 않은 설명이다.
② O — 정보보호시스템의 성능과 신뢰도에 관한 기준을 정하여 고시하고 제조자나 수입자에게 준수를 권고할 수 있다는 설명이다. 이는 현행 지능정보화 기본법의 정보보호시스템 기준 고시 규정과 부합한다.
③ O — 공통평가기준 제1부는 정보기술 보안성 평가의 원칙·일반 개념과 평가의 일반 모델을 설명하고, 보안목적·보안요구사항의 선택과 정의 및 PP·ST 같은 상위 수준 명세 작성을 위한 전체 구조를 제시하는 소개 부분이다.
④ O — PP는 제품군에 대한 특정 소비자 요구를 담은 구현 독립적 보안요구사항의 집합이고, ST는 식별된 특정 평가대상의 평가 근거가 되는 보안요구사항과 구현 명세의 집합이므로 설명이 옳다.

오답 포인트

①에서 등급의 개수를 6개로 줄이고 높고 낮음의 방향까지 뒤집은 것이 함정이다. EAL의 숫자는 단순한 식별 번호가 아니라 보증 수준의 상승 방향을 나타낸다. 또한 ④에서는 PP의 ‘구현 독립적·제품군’과 ST의 ‘구현 의존적·특정 평가대상’을 바꾸지 않도록 주의한다.

다시 나오면 이렇게 판단

EAL 선지는 먼저 ‘1~7의 7단계’와 ‘숫자가 클수록 높은 보증’인지 확인한다. PP와 ST 선지는 적용 대상과 구현 의존성을 기준으로 판단한다. 제품군·구현 독립이면 PP이고, 특정 평가대상·구현 의존이면 ST이다.

암기 포인트

EAL은 1이 최저, 7이 최고이다. PP는 제품군의 공통 요구, ST는 특정 제품의 평가 명세이다.

NoteBase

9. 정보 보안 시스템을 설계하거나 운영할 때 고려하는 요소 중 하나인 가용성을 보존하기 위해 행해지는 활동으로 옳지 않은 것은?
① 백업
② 네트워크 증설
③ 침입탐지시스템 운용
④ 전자서명

정답 4번

출제 포인트

정보 보안의 가용성을 보장하는 활동과 인증·무결성·부인방지를 위한 활동을 구분하는 문제이다.

핵심 개념

가용성은 인가된 사용자가 필요할 때 정보와 시스템을 정상적으로 이용할 수 있도록 보장하는 성질이다. 백업과 네트워크 이중화는 장애 발생 시 복구 또는 서비스 지속을 가능하게 하고, 침입탐지시스템은 서비스 중단을 일으킬 수 있는 공격을 탐지하여 가용성 유지에 기여한다. 반면 전자서명은 서명자의 인증, 전자문서의 무결성 확인, 부인방지를 주된 목적으로 한다.

선지별 해설

① O — 백업은 원본 데이터가 손상되거나 소실되었을 때 데이터를 복구하여 정보와 서비스를 다시 이용할 수 있게 하므로 가용성을 보장하는 활동이다.
② O — 네트워크 증설은 통신 용량이나 대체 경로를 확보하여 과부하와 장애로 인한 서비스 중단 가능성을 줄이므로 가용성 향상에 기여한다.
③ O — 침입탐지시스템 운영은 서비스 거부 공격 등 시스템의 정상 이용을 방해하는 침입 징후를 탐지하고 대응하게 하므로 가용성 유지에 기여한다.
④ X — 틀린 표현은 전자서명을 가용성 보장 활동으로 본 부분이다. 전자서명은 서명자 인증, 전자문서의 무결성 확인 및 부인방지를 위한 활동이며, 가용성 보장을 위해서는 백업·이중화·장애 복구 체계 등을 운용한다.

오답 포인트

전자서명도 정보 보안 기술이라는 이유만으로 가용성 통제로 판단하기 쉽다. 그러나 이 문항에서는 보안 기술인지가 아니라 시스템을 필요할 때 계속 이용하게 하는 기능인지가 판단 기준이다.

다시 나오면 이렇게 판단

장애·공격 이후에도 서비스의 지속이나 복구를 가능하게 하면 가용성 통제로 판단한다. 데이터가 변조되지 않았음을 확인하거나 행위자의 신원을 증명하고 부인을 막는 기능이면 무결성·인증·부인방지 통제로 구분한다.

NoteBase

암기 포인트

가용성은 백업·이중화·복구, 전자서명은 인증·무결성·부인방지이다.

10. 디지털 포렌식 원칙에 해당하지 않는 것은?
① 정당성의 원칙
② 재현의 원칙
③ 연계보관성의 원칙
④ 무죄 추정의 원칙

정답 4번

출제 포인트

디지털 증거의 수집·분석·보관 과정에서 지켜야 할 디지털 포렌식 원칙과 형사절차의 일반 원칙을 구별하는 문제이다.

핵심 개념

디지털 포렌식 원칙은 디지털 증거가 법적 증거로 신뢰받도록 수집·분석·보관 전 과정의 적법성, 반복 검증 가능성, 이력 관리, 무결성 등을 확보하는 기준이다.
정당성은 적법한 권한과 절차에 따라 증거를 취득해야 한다는 뜻이고, 재현성은 같은 조건과 방법으로 분석했을 때 같은 결과가 나와야 한다는 뜻이다. 연계보관성은 증거의 수집부터 법정 제출까지 취급자와 이동·보관 이력을 끊김 없이 기록해야 한다는 뜻이다.

선지별 해설

① O — 정당성의 원칙은 디지털 증거를 적법한 권한과 절차에 따라 수집·분석해야 한다는 원칙이므로 디지털 포렌식 원칙에 해당한다.
② O — 재현의 원칙은 동일한 조건과 분석 방법을 적용했을 때 동일한 결과가 나와야 한다는 원칙이므로 디지털 포렌식 원칙에 해당한다.
③ O — 연계보관성의 원칙은 증거의 수집·이송·보관·분석·제출 과정과 취급자를 기록하여 증거 관리의 연속성을 입증하는 원칙이므로 디지털 포렌식 원칙에 해당한다.
④ X — '무죄 추정의 원칙'은 유죄 판결이 확정되기 전까지 피고인을 무죄로 추정하는 형사절차의 원칙으로, 디지털 증거의 수집·분석·보관 방법을 규율하는 디지털 포렌식 원칙이 아니다. 틀린 표현인 '무죄 추정의 원칙'은 디지털 포렌식 원칙인 '무결성의 원칙' 등으로 고쳐야 한다.

오답 포인트

④의 '무죄 추정'도 형사사법과 관련된 중요한 원칙이어서 디지털 포렌식 원칙처럼 보일 수 있다. 그러나 무죄 추정은 피고인의 법적 지위에 관한 원칙이고, 정당성·재현성·연계보관성은 디지털 증거의 신뢰성과 증거능력을 뒷받침하는 처리 원칙이다.

NoteBase

다시 나오면 이렇게 판단

선지가 증거의 적법한 취득, 동일 결과의 반복 검증, 취급 이력의 연속성, 원본 훼손 방지와 관련되면 디지털 포렌식 원칙으로 판단한다. 피고인의 권리나 재판상 지위를 규정하는 원칙이면 형사절차의 일반 원칙으로 구별한다.

암기 포인트

포렌식은 증거 처리의 정당성·재현성·연계보관성·무결성, 무죄 추정은 피고인의 법적 지위에 관한 원칙이다.

NoteBase

11. 개인정보보호법 제3조(개인정보보호원칙)에 명시된 내용으로 옳지 않은 것은?

① 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.

② 개인정보처리자는 정보주체의 동의를 받은 경우 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다.

③ 개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리를 보장하여야 한다.

④ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.

정답 2번

쟁점

이 문제는 개인정보 보호법 제3조의 개인정보 보호 원칙에 관한 문제이다. 핵심은 개인정보 처리의 기본 원칙과 개인정보를 수집·이용할 수 있는 법적 근거를 구별하는 것이다.

용어 풀이

개인정보 보호 원칙은 개인정보처리자가 개인정보의 수집부터 이용·관리까지 전 과정에서 지켜야 하는 기본 기준이다.

핵심 구분

개인정보 보호법 제3조는 목적 명확화와 최소 수집, 목적 범위 내 적합한 처리와 목적 외 이용 금지, 정확성·완전성·최신성 보장, 처리 사항 공개와 정보주체의 권리 보장 등을 규정한다. 반면 정보주체의 동의를 받은 경우 개인정보를 수집하고 수집 목적의 범위에서 이용할 수 있다는 내용은 제15조 제1항의 수집·이용 근거이다. 따라서 법률상 옳은 내용이라도 제3조에 명시된 원칙이 아니면 이 문항에서는 정답이 된다.

NoteBase

선지별 해설

① O
개인정보처리자는 처리 목적에 필요한 범위에서 개인정보를 적합하게 처리하여야 하고, 그 목적 외의 용도로 활용해서는 안 된다. 개인정보 보호법 제3조 제2항의 내용이다.

② X
정보주체의 동의를 받은 경우 개인정보를 수집하고 수집 목적의 범위에서 이용할 수 있다는 내용은 개인정보 보호법 제15조 제1항의 수집·이용 근거이지, 제3조에 명시된 개인정보 보호 원칙이 아니다.
틀린 표현: 정보주체의 동의를 받은 경우 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다.
올바른 표현: 개인정보처리자는 처리 목적을 명확하게 하고, 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다. 또한 처리 목적에 필요한 범위에서 적합하게 처리하고 목적 외 용도로 활용해서는 안 된다.

③ O
개인정보처리자는 개인정보 처리방침 등 처리에 관한 사항을 공개하고, 열람청구권 등 정보주체의 권리를 보장하여야 한다. 개인정보 보호법 제3조 제5항의 내용이다.

④ O
개인정보처리자는 처리 목적에 필요한 범위에서 개인정보의 정확성·완전성·최신성이 보장되도록 하여야 한다. 개인정보 보호법 제3조 제3항의 내용이다.

오답 포인트

②는 개인정보 보호법에 실제로 존재하는 내용이어서 옳은 선지처럼 보이지만, 제3조가 아니라 제15조의 내용이다. 이 문제는 문장 자체의 적법성보다 해당 내용이 제3조에 명시되어 있는지를 묻는다.

다시 나오면 이렇게 판단

특정 조문의 내용을 묻는 문제에서는 법률 전체에서 맞는 문장인지와 해당 조문에 들어 있는 문장인지를 나누어 판단한다. 제3조는 최소 수집·목적 제한·정보 품질·안전 관리·투명성·권리 보장 등의 원칙이고, 동의를 비롯한 구체적인 수집·이용 근거는 제15조이다.

암기 포인트

제3조는 보호 원칙, 제15조는 수집·이용 근거이다. '동의를 받은 경우 수집·이용 가능'은 제15조이다.

NoteBase

12. 공개키 기반구조에 대한 설명으로 옳지 않은 것은?

① X.509 국제표준에 기반하며, 정보의 기밀성, 무결성, 인증, 부인방지 등 신뢰 서비스를 제공하는데 이용된다.

② 공개키 인증서를 발행하는 인증기관, 실체의 신원을 확인하는 등록기관, 인증서 폐지 목록을 관리하는 보관소, 최종 실체 등으로 구성된다.

③ 기업 및 기관 단위에서 사용자들에게 특정 시스템 및 애플리케이션에 접근할 수 있는 권한을 차등 부여해주는 관리 체계이다.

④ 공개키 인증서를 생성, 관리, 배포, 이용, 저장 및 폐지하기 위해 필요한 기능, 정책, 하드웨어, 소프트웨어 및 절차의 집합이다.

정답 3번

출제 포인트

이 문제는 공개키 기반구조(PKI)의 목적·구성요소·기능과 접근통제 체계의 역할을 구별하는 문제이다.

핵심 개념

공개키 기반구조(PKI): 신뢰할 수 있는 기관이 사용자의 신원과 공개키를 인증서로 결합하고, 인증서의 발급부터 폐지까지 전 생명주기를 관리하는 체계이다. / 키워드: 공개키 인증서, 인증기관, 등록기관, 저장소, 인증서 폐지 목록

접근통제·권한관리 체계: 인증된 사용자에게 시스템이나 애플리케이션 자원에 대한 접근 권한을 차등 부여하고 통제하는 체계이다. / 키워드: 권한 부여, 자원 접근 통제

PKI는 공개키와 신원의 신뢰성을 보장하는 기반이고, 접근통제는 누가 어떤 자원에 접근할 수 있는지를 결정한다.

NoteBase

선지별 해설

① O — PKI는 X.509 형식의 공개키 인증서를 기반으로 공개키의 소유자를 확인한다. 이를 바탕으로 암호화와 전자서명을 활용하여 기밀성, 무결성, 인증, 부인방지 등의 보안 서비스를 지원한다.
② O — 인증기관(CA)은 인증서를 발행하고, 등록기관(RA)은 신청자의 신원을 확인하며, 저장소는 인증서와 인증서 폐지 목록(CRL)을 게시·관리한다. 최종 사용자나 시스템인 종단 실체도 PKI의 구성요소이다.
③ X — 틀린 표현은 '사용자들에게 특정 시스템 및 애플리케이션에 접근할 수 있는 권한을 차등 부여해주는 관리 체계'이다. 이는 접근통제 또는 권한관리 체계의 설명이다. 올바르게는 'PKI는 신원과 공개키를 인증서로 결합하고 공개키 인증서의 발급·관리·배포·이용·저장·폐지를 지원하는 신뢰 체계'라고 해야 한다.
④ O — 인증서의 생성, 관리, 배포, 이용, 저장 및 폐지에 필요한 기능과 정책뿐 아니라 이를 구현하는 하드웨어, 소프트웨어 및 절차를 모두 포함한다는 설명은 PKI의 범위에 부합한다.

오답 포인트

③은 '인증된 사용자에게 권한을 부여한다'는 접근통제 기능을 '사용자와 공개키의 관계를 인증한다'는 PKI 기능처럼 바꾸어 놓은 선지이다. 인증과 권한 부여는 연결되지만 서로 다른 기능이다.

다시 나오면 이렇게 판단

선지의 중심 대상이 공개키 인증서의 발급·검증·저장·폐지이면 PKI로 판단한다. 반면 사용자별로 시스템 자원에 대한 접근 권한을 정하거나 차등 부여하는 내용이면 접근통제·권한관리 체계로 판단한다.

암기 포인트

PKI는 '신원과 공개키를 인증서로 연결', 접근통제는 '사용자와 자원 권한을 연결'이다.

NoteBase

13. 완성된 바이너리 형태의 소프트웨어를 역으로 분석하여 원래 소스 코드의 구조를 파악하는 리버스 엔지니어링의 목적으로 옳지 않은 것은?
① 취약점 분석
② 악성코드 분석
③ 디지털 포렌식
④ 컴파일 및 링킹

정답 4번

출제 포인트

완성된 바이너리에서 프로그램의 구조와 동작을 거꾸로 분석하는 리버스 엔지니어링의 활용 목적을 묻는 문제이다.

핵심 개념

리버스 엔지니어링은 실행 파일이나 바이너리 같은 결과물을 분석하여 원래 프로그램의 구조, 동작 방식, 취약점 등을 파악하는 작업이다. 반면 컴파일 및 링킹은 소스 코드를 목적 코드와 실행 파일로 만드는 정방향 빌드 과정이다.

선지별 해설

① O — 취약점 분석은 바이너리의 제어 흐름, 메모리 사용, 입력 처리 등을 조사하여 보안 결함을 찾는 것이므로 리버스 엔지니어링의 목적에 해당한다.
② O — 악성코드 분석은 실행 파일을 분해하고 동작을 추적하여 감염 방식, 명령 수행, 통신 행위 등을 파악하므로 대표적인 리버스 엔지니어링 활용 분야이다.
③ O — 디지털 포렌식에서는 바이너리와 실행 흔적을 분석하여 프로그램의 기능이나 사건 관련 행위를 규명할 수 있으므로 리버스 엔지니어링이 활용된다.
④ X — 틀린 표현은 '컴파일 및 링킹'이다. 컴파일 및 링킹은 원래 소스 코드에서 실행 가능한 바이너리를 생성하는 정방향 빌드 과정이며, 완성된 바이너리로부터 원래 구조를 파악하는 리버스 엔지니어링의 목적이 아니다. 올바르게는 '바이너리의 구조와 동작 분석' 등이 리버스 엔지니어링의 목적이다.

오답 포인트

④도 바이너리와 관련된 용어이므로 혼동하기 쉽다. 그러나 취약점 분석, 악성코드 분석, 디지털 포렌식은 이미 만들어진 결과물을 조사하는 활용 목적이고, 컴파일 및 링킹은 소스 코드로 결과물을 만드는 생성 과정이다.

NoteBase

다시 나오면 이렇게 판단

‘결과물에서 원래 구조와 동작을 추적하는가’이면 리버스 엔지니어링이고, ‘소스 코드에서 실행 파일을 만드는가’이면 컴파일·링킹 과정으로 판단한다.

암기 포인트

컴파일·링킹은 소스에서 바이너리로, 리버스 엔지니어링은 바이너리에서 구조와 동작으로 향한다.

NoteBase

14. 정보통신기반 보호에 대한 설명으로 옳지 않은 것은?

① 중앙행정기관의 장은 소관분야의 정보통신기반시설 중 업무의 국가사회적 중요성, 업무의 정보통신기반시설에 대한 의존도, 국가안전보장과 경제사회에 미치는 피해규모 및 범위 등을 고려하여 정보통신기반시설을 주요정보통신기반시설로 지정할 수 있다.

② 주요정보통신기반시설 보호계획에는 주요정보통신기반시설의 취약점 분석·평가, 침해사고에 대한 예방·백업·복구대책, 보호에 관하여 필요한 사항을 포함해야 한다.

③ 정보통신기반보호위원회는 주요정보통신기반시설에 대하여 보호지침을 제정하고 해당 분야 관리기관의 장에게 이를 지키도록 권고할 수 있다.

④ "정보통신기반시설"이라 함은 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 및 정보통신망을 말한다.

정답 3번

쟁점

이 문제는 「정보통신기반 보호법」상 주요정보통신기반시설의 지정 기준, 보호계획의 내용, 보호지침의 제정 주체 및 정보통신기반시설의 정의를 구별하는 문제이다. 핵심은 정보통신기반보호위원회와 관계중앙행정기관의 장의 권한을 구분하는 것이다.

용어 풀이

주요정보통신기반시설은 국가안전과 국민생활에 중요한 정보통신기반시설 가운데 전자적 침해행위로부터 특별히 보호할 필요가 있어 지정된 시설이다.
관계중앙행정기관은 주요정보통신기반시설을 관할하는 중앙행정기관을 말한다.

핵심 구분

정보통신기반보호위원회는 주요정보통신기반시설의 보호정책과 보호계획의 종합·조정 등 주요 사항을 심의한다. 반면 관계중앙행정기관의 장은 소관 분야의 보호지침을 제정하고 관리기관의 장에게 이를 지키도록 명령할 수 있다. 이는 현행 「정보통신기반 보호법」 제3조·제4조와 제10조의 역할 구분이다.

NoteBase

선지별 해설

① O
중앙행정기관의 장은 업무의 국가사회적 중요성, 정보통신기반시설에 대한 의존도, 다른 기반시설과의 상호연계성, 침해사고 발생 시 피해규모·범위, 침해사고 발생 가능성 또는 복구의 용이성 등을 고려하여 소관 시설을 주요정보통신기반시설로 지정할 수 있다. 법 제8조의 지정 기준과 일치한다.

② O
주요정보통신기반시설보호계획에는 취약점 분석·평가, 주요정보통신기반시설 및 관리 정보의 침해사고에 대한 예방·백업·복구대책, 그 밖에 보호에 필요한 사항이 포함되어야 한다. 법 제6조 제3항의 내용과 일치한다.

③ X
보호지침을 제정하는 주체는 정보통신기반보호위원회가 아니라 관계중앙행정기관의 장이다. 위원회는 주요 보호정책 등을 심의하는 기관이다.
틀린 표현: 정보통신기반보호위원회는 보호지침을 제정하고 해당 분야 관리기관의 장에게 이를 지키도록 권고할 수 있다.
올바른 표현: 관계중앙행정기관의 장은 소관 분야의 주요정보통신기반시설에 대한 보호지침을 제정하고 해당 분야 관리기관의 장에게 이를 지키도록 명령할 수 있다.

④ O
정보통신기반시설은 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 및 정보통신망을 말한다. 법 제2조 제1호의 정의와 일치한다.

오답 포인트

③은 위원회가 보호정책을 심의한다는 사실을 보호지침 제정 권한과 섞은 선지이다. 또한 현행법의 표현은 관리기관의 장에게 준수를 ‘권고’하는 것이 아니라 ‘명령할 수 있다’는 것이다.

다시 나오면 이렇게 판단

기관별 동사를 구분한다. 위원회는 보호정책과 보호계획 등을 ‘심의’하고, 관계중앙행정기관의 장은 소관 시설을 ‘지정’하며 보호지침을 ‘제정’하고 그 준수를 ‘명령’할 수 있다.

암기 포인트

위원회는 심의, 중앙행정기관의 장은 지정·지침 제정·준수 명령이다.

NoteBase

15. 암호화에 대한 설명으로 옳지 않은 것은?

① 순서보존 암호화(Order-preserving encryption)는 원본정보의 순서와 암호값의 순서가 동일하게 유지되는 암호화 방식이다.

② 형태보존 암호화(Format-preserving encryption)는 원본 정보의 형태와 암호값의 형태가 동일하게 유지되는 암호화 방식이다.

③ 동형 암호화(Homomorphic encryption)는 암호화된 상태에서의 연산이 가능한 암호화 방식이다.

④ 일방향 암호화는 원문에 대한 암호화만 가능하며 추가정보가 있으면 암호문에 대한 복호화가 가능하다.

정답 4번

출제 포인트

순서보존 암호화, 형태보존 암호화, 동형 암호화, 일방향 암호화의 핵심 성질을 구별하는 문제이다.

핵심 개념

순서보존 암호화: 평문의 대소·순서 관계가 암호문에서도 유지되는 방식이다.
형태보존 암호화: 평문과 암호문의 길이, 문자 집합 등 형식이 같게 유지되는 방식이다.
동형 암호화: 암호문 상태에서 연산한 결과를 복호화하면 평문에 대응 연산을 한 결과를 얻을 수 있는 방식이다.
일방향 암호화: 원문을 변환할 수는 있지만 그 결과로부터 원문을 복원하는 역연산은 현실적으로 불가능하도록 하는 방식이다. 추가 정보인 트랩도어가 있을 때 역연산이 가능해지는 성질은 트랩도어 일방향 함수와 구별한다.

선지별 해설

① O — 순서보존 암호화는 평문 값의 순서 관계가 암호문 값에서도 동일하게 유지되므로 옳다.
② O — 형태보존 암호화는 원문의 길이·문자 집합과 같은 형식을 암호문에서도 유지하므로 옳다.
③ O — 동형 암호화는 데이터를 복호화하지 않고 암호문 상태에서 연산할 수 있으므로 옳다.
④ X — 틀린 표현은 '추가정보가 있으면 암호문에 대한 복호화가 가능하다'이다. 일방향 암호화는 원문 복원을 위한 복호화를 전제로 하지 않으며, 추가 정보인 트랩도어로 역연산할 수 있는 것은 트랩도어 일방향 함수의 성질이다. 올바르게는 '일방향 암호화는 원문을 일방향으로 변환하며 그 결과로부터 원문을 현실적으로 복원할 수 없다'이다.

NoteBase

오답 포인트

④의 '추가정보'라는 말 때문에 비밀키나 개인키를 떠올리기 쉽다. 그러나 일반적인 일방향 암호화는 복호화 가능성을 전제하지 않으며, 특정 비밀정보로 역연산이 가능하다는 설명은 트랩도어 일방향 함수에 해당한다.

다시 나오면 이렇게 판단

각 암호화의 이름이 무엇을 보존하거나 허용하는지 확인한다. 순서보존은 값의 순서, 형태보존은 데이터 형식, 동형 암호화는 암호문 연산을 뜻한다. 일방향이라는 표현이 나오면 원문 복원이 가능한지부터 판단하고, 트랩도어가 제시되면 별개의 개념으로 구분한다.

암기 포인트

순서보존은 순서, 형태보존은 형식, 동형은 암호문 연산, 일방향은 복원 불가이다.

NoteBase

16. 온라인상 본인확인서비스에 대한 설명 중 옳지 않은 것은?

① “연계정보”라 함은 정보통신서비스 제공자의 온·오프라인 서비스 연계를 위해 본인확인기관이 이용자의 주민등록번호와 본인확인기관 간 공유 비밀정보를 이용하여 생성한 정보를 말한다.

② “중복가입확인정보”라 함은 웹사이트에 가입하고자 하는 이용자의 중복가입 여부를 확인하는 데 사용되는 정보로서 본인확인기관이 이용자의 주민등록번호, 웹사이트 식별번호 및 본인확인기관 간 공유비밀정보를 이용하여 생성한 정보를 말한다.

③ “공유비밀정보”라 함은 본인확인기관이 특정 이용자에 대해 동일한 중복가입확인정보와 연계정보를 생성하기 위해 공유하는 정보를 말한다.

④ 전자서명법에 따른 “전자서명인증사업자”는 “정보통신망 이용촉진 및 정보보호 등에 관한 법률”에 근거해 지정되는 본인확인기관으로 간주된다.

정답 4번

쟁점

이 문제는 온라인상 본인확인서비스에서 사용하는 연계정보·중복가입확인정보·공유비밀정보의 뜻과 본인확인기관의 지정 요건을 구별하는 문제이다.

용어 풀이

본인확인기관은 주민등록번호를 직접 쓰지 않는 본인확인 대체수단을 제공하며, 정보통신망법에 따라 지정받은 자이다.

연계정보는 서로 다른 온·오프라인 서비스에서 같은 이용자를 연계하기 위한 정보이고, 중복가입확인정보는 특정 웹사이트에서 동일 이용자의 중복 가입 여부를 확인하기 위한 정보이다.

NoteBase

핵심 구분

현행 「본인확인기관 지정 등에 관한 기준」 제2조는 연계정보, 중복가입확인정보, 공유비밀정보를 각각 정의한다. 한편 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제23조의3은 본인확인업무를 안전하고 신뢰성 있게 수행할 능력이 있다고 인정되는 자를 심사하여 본인확인기관으로 지정할 수 있도록 한다.
전자서명인증사업자라는 지위와 본인확인기관 지정은 서로 같지 않다.

선지별 해설

① O — 연계정보는 정보통신서비스 제공자의 온·오프라인 서비스 연계를 위하여 본인확인기관이 이용자의 주민등록번호와 본인확인기관 간 공유비밀정보를 이용해 생성한 정보이다.

② O — 중복가입확인정보는 웹사이트 가입자의 중복가입 여부를 확인하기 위하여 주민등록번호, 웹사이트 식별번호 및 본인확인기관 간 공유비밀정보를 이용해 생성한 정보이다.

③ O — 공유비밀정보는 본인확인기관들이 특정 이용자에 대하여 동일한 중복가입확인정보와 연계정보를 생성하기 위해 공유하는 정보이다.

④ X — 전자서명인증사업자가 모두 본인확인기관으로 자동 간주되는 것은 아니다. 전자서명법 시행령도 전자서명인증사업자가 본인확인기관인 경우와 아닌 경우를 구분한다.
틀린 표현: 전자서명인증사업자는 본인확인기관으로 간주된다.
올바른 표현: 전자서명인증사업자도 정보통신망법상 요건에 따라 본인확인기관으로 지정받은 경우에만 본인확인기관에 해당한다.

오답 포인트

④의 ‘전자서명인증사업자’와 ‘본인확인기관’을 모두 전자적 신원확인을 수행하는 기관이라는 이유만으로 같은 법적 지위라고 생각하기 쉽다. 그러나 전자서명인증업무를 한다는 사실만으로 본인확인기관 지정이 자동으로 이루어지지는 않는다.

다시 나오면 이렇게 판단

정보의 정의는 생성 목적과 구성 요소를 함께 본다. 서비스 연계가 목적이면 연계정보, 웹사이트 내 중복가입 확인이 목적이면 중복가입확인정보, 두 정보를 기관 간 동일하게 생성하기 위해 공유하면 공유비밀정보이다.
기관의 법적 지위는 업무 명칭이 아니라 별도의 지정 요건과 지정 여부로 판단한다.

암기 포인트

연계정보는 서비스 간 연결, 중복가입확인정보는 사이트 내 중복 확인, 공유비밀정보는 기관 간 동일값 생성이다.
전자서명인증사업자와 본인확인기관은 자동으로 동일하지 않다.

NoteBase

17. 인터넷과 같은 공중망에 터널을 형성하고 이를 통해 패킷을 캡슐화해서 전달함으로써 사설망과 같은 전용 회선처럼 사용할 수 있게 하는 기술로 적절한 것은?

① 가상 사설망 ② 접근 제어
③ 회선 관리 ④ 세션 관리

정답 1번

출제 포인트

공중망에서 터널을 만들고 패킷을 캡슐화하여 사설망처럼 이용하게 하는 가상 사설망(VPN)의 핵심 원리를 묻는 문제이다.

핵심 개념

가상 사설망(VPN)은 인터넷과 같은 공중망에 논리적인 전용 통로인 터널을 구성하고, 원래 패킷을 다른 패킷 안에 캡슐화하여 사설망처럼 통신하게 하는 기술이다. 핵심 키워드는 공중망, 터널링, 캡슐화이다.

선지별 해설

① O — 가상 사설망은 공중망 위에 터널을 만들고 패킷을 캡슐화하여 전용 회선과 유사한 사설 통신 환경을 제공하므로 제시된 설명과 일치한다.
② X — 접근 제어는 사용자나 시스템이 자원에 접근할 수 있는지를 인증 정보와 권한에 따라 허용하거나 차단하는 기능이다. 틀린 부분은 '터널을 형성하고 패킷을 캡슐화하는 기술'을 접근 제어로 본 점이며, 올바르게는 가상 사설망이다.
③ X — 회선 관리는 통신 회선의 상태, 장애, 성능 등을 관리하는 기능이지 공중망에 터널을 구성하는 기술이 아니다. 틀린 부분은 '공중망을 전용 회선처럼 사용하게 하는 기술'을 회선 관리로 본 점이며, 올바르게는 가상 사설망이다.
④ X — 세션 관리는 통신 당사자 사이의 연결을 설정·유지·종료하는 기능이다. 틀린 부분은 '패킷 캡슐화와 터널링'을 세션 관리로 본 점이며, 올바르게는 가상 사설망이다.

오답 포인트

문제에 '전용 회선'이라는 표현이 있어 ③ 회선 관리를 고르기 쉽지만, 결정적 단서는 '공중망에 터널 형성'과 '패킷 캡슐화'이다. 이는 물리적 회선 관리가 아니라 VPN의 터널링 원리이다.

다시 나오면 이렇게 판단

공중망을 이용하면서 터널링과 캡슐화로 사설망 또는 전용망과 같은 통신 환경을 만든다는 설명이 나오면 가상 사설망(VPN)으로 판단한다.

NoteBase

암기 포인트

공중망 + 터널링 + 캡슐화 = 가상 사설망(VPN)이다.

18. ARP Spoofing 공격에 대한 설명으로 옳지 않은 것은?
① ARP(Address Resolution Protocol)이 인증을 하지 않기 때문에 발생한다.
② 근거리 네트워크 환경에서 발생한다.
③ ARP 테이블 변경을 동적으로 관리함으로 예방할 수 있다.
④ 중간자 공격 기법을 통해 이루어진다.

정답 3번

출제 포인트

ARP Spoofing의 발생 원인, 공격 범위, 대응 방법, 공격 형태를 구분하는 문제이다.

핵심 개념

ARP Spoofing은 위조된 ARP 응답을 보내 피해자의 ARP 캐시에 공격자의 MAC 주소를 정상 장비의 주소처럼 등록시키는 공격이다. ARP는 응답의 진위를 인증하지 않으며, 동적으로 학습한 ARP 정보는 위조 응답으로 변경될 수 있다. 따라서 일반적인 ARP 동적 갱신 자체는 예방법이 아니며, 중요 장비의 ARP 정보를 정적으로 고정하거나 동적 ARP 검사(DAI) 등으로 검증해야 한다.

선지별 해설

① O — ARP에는 응답 송신자를 인증하는 기능이 없으므로 공격자가 위조된 IP 주소와 MAC 주소의 대응 관계를 주입할 수 있다.
② O — ARP는 같은 로컬 네트워크의 IP 주소를 MAC 주소로 변환할 때 사용하는 프로토콜이므로, ARP Spoofing은 일반적으로 동일한 근거리 네트워크 또는 브로드캐스트 도메인 안에서 발생한다.
③ X — 틀린 표현은 ‘ARP 테이블 변경을 동적으로 관리함으로’이다. 동적 ARP 항목은 수신한 위조 ARP 응답에 의해 갱신될 수 있으므로 그 자체로는 공격을 예방하지 못한다. 올바르게는 중요 ARP 항목을 정적으로 설정하거나 동적 ARP 검사(DAI) 같은 검증 기능을 사용하면 예방할 수 있다고 표현해야 한다.
④ O — 공격자가 피해자와 게이트웨이 사이의 ARP 정보를 각각 위조하면 양쪽 트래픽이 공격자를 거치게 되어 중간자 공격이 가능하다.

오답 포인트

③의 ‘동적으로 관리’가 자동 방어처럼 보이는 것이 함정이다. ARP 캐시의 동적 갱신은 신뢰성 검증 기능이 아니라 위조 정보가 캐시에 반영되는 통로가 될 수 있다.

NoteBase

다시 나오면 이렇게 판단

ARP Spoofing 선지는 ‘인증 부재’, ‘동일 브로드캐스트 도메인’, ‘ARP 캐시 변조’, ‘중간자 공격’을 핵심 특징으로 판단한다. 대응책은 단순한 동적 갱신이 아니라 정적 ARP 설정이나 ARP 정보 검증 기능인지 확인한다.

암기 포인트

ARP는 인증하지 않고, 동적 캐시는 속을 수 있다. 방어의 핵심은 정적 고정 또는 검증이다.

NoteBase

19. 공개된 네트워크 환경에서 통신하는 두 당사자가 공유키를 만드는 데 사용되는 Diffie-Hellman 알고리즘에 대한 설명으로 옳지 않은 것은?
① 비밀키 알고리즘의 일종이다.
② 안전을 위해 일반적으로 1024비트 이상의 큰 소수를 사용해야 한다.
③ 상대방에 대한 인증을 제공하지 않기 때문에 중간자 공격이 가능하다.
④ 안전을 위해 충분히 안전한 난수 생성 알고리즘을 사용해야 한다.

정답 1번

출제 포인트

Diffie-Hellman의 알고리즘 분류와 안전한 키 교환을 위한 조건, 인증 부재에 따른 취약점을 구별하는 문제이다.

핵심 개념

Diffie-Hellman은 공개된 통신로에서 두 당사자가 공통의 비밀값을 합의하는 공개키 기반의 키 교환 방식이다. 통신 당사자는 큰 소수와 생성자 등의 공개 매개변수를 사용하고, 각자 안전하게 생성한 비밀 난수로 공개값과 공유 비밀을 계산한다. 다만 상대방의 신원을 인증하는 기능은 자체적으로 제공하지 않으므로 인증 절차 없이 사용하면 중간자 공격에 취약하다.

선지별 해설

① X — 틀린 표현은 '비밀키 알고리즘의 일종'이다. Diffie-Hellman은 사전에 공유한 비밀키로 암호화하는 비밀키 알고리즘이 아니라, 공개값을 교환하여 공통 비밀을 만드는 공개키 기반의 키 교환 알고리즘이다.
② O — 이산대수 문제의 계산을 어렵게 만들기 위해 일반적으로 1024비트 이상의 큰 소수를 사용한다는 설명이다.
③ O — 기본 Diffie-Hellman은 상대방의 신원을 인증하지 않는다. 공격자가 양쪽 사이에서 각각 별도의 키를 합의할 수 있으므로 중간자 공격이 가능하다.
④ O — 각 당사자의 비밀 지수는 예측하기 어려워야 한다. 충분히 안전한 난수 생성 알고리즘으로 이를 생성해야 공유 비밀의 추측이나 비밀값 노출 위험을 줄일 수 있다.

오답 포인트

공유 결과가 비밀키라는 점 때문에 Diffie-Hellman 자체를 비밀키 알고리즘으로 오인하기 쉽다. 그러나 분류 기준은 만들어진 값의 용도가 아니라 공개값을 이용해 키를 합의하는 방식이다. 또한 키 합의 기능과 상대방 인증 기능은 서로 다르므로, 키를 합의할 수 있다는 사실만으로 중간자 공격이 방지되지는 않는다.

NoteBase

다시 나오면 이렇게 판단

Diffie-Hellman 선지는 '공개값으로 공유 비밀을 합의한다', '큰 소수와 안전한 비밀 난수가 필요하다', '자체 인증이 없어 중간자 공격에 취약하다'의 세 기준으로 판단한다. 이를 비밀키 암호 알고리즘 자체라고 분류한 표현은 틀린다.

암기 포인트

Diffie-Hellman은 공개키 기반 키 합의이며, 인증이 없으면 중간자 공격에 취약하다.

NoteBase

20. 미국 국방부에 의해 개발된 컴퓨터 보안 평가 방법론인 TCSEC에 대한 설명으로 옳지 않은 것은?
① 가장 낮은 평가 수준은 D이고 가장 높은 수준은 A이다.
② 운영체제에 중점을 두어 평가하기 때문에 방화벽 등에 적용하기 어렵다.
③ 기밀성, 무결성, 가용성에 대한 요구 사항을 균형적으로 다루고 있다.
④ 평가 수준별로 기능 요구 사항과 보증 요구 사항을 포함한다.

정답 3번

출제 포인트

TCSEC의 평가 등급 체계와 주된 보호 목표, 평가 요구사항의 특징을 구별하는 문제이다.

핵심 개념

TCSEC는 미국 국방부가 신뢰할 수 있는 컴퓨터 시스템의 보안성을 평가하기 위해 마련한 기준이다. 등급은 낮은 수준에서 높은 수준으로 D, C, B, A 계열로 구분되며, 주로 기밀성 보호를 위한 접근통제와 신뢰성을 평가한다. 각 등급에는 보안 기능에 관한 요구와 그 기능이 제대로 설계·구현되었음을 확인하는 보증 요구가 함께 제시된다.

선지별 해설

① O — TCSEC의 가장 낮은 평가 수준은 D이고 가장 높은 수준은 A 계열이다. 세부 등급까지 보면 A1이 최상위 등급이다.

② O — TCSEC는 독립된 컴퓨터 시스템, 특히 운영체제와 신뢰 컴퓨팅 기반의 평가에 초점을 둔 기준이다. 따라서 네트워크 경계에서 동작하는 방화벽과 같은 제품에 그대로 적용하기에는 한계가 있다.

③ X — 틀린 표현은 '기밀성, 무결성, 가용성에 대한 요구 사항을 균형적으로 다룬다'이다. 올바르게는 TCSEC는 세 요소를 균형 있게 평가하는 기준이라기보다 기밀성 보호를 중심으로 접근통제와 보증을 다루며, 무결성과 가용성을 동등한 비중으로 포괄하지 않는다.

④ O — TCSEC는 평가 등급별로 보안 정책·책임추적성 등 보안 기능에 관한 요구와 운영·개발 과정의 보증 요구 및 문서화 요구를 제시한다.

NoteBase

오답 포인트

현대 정보보호의 기본 목표인 기밀성·무결성·가용성을 TCSEC도 균형 있게 다룬다고 생각하기 쉽다. 그러나 ③의 '균형적으로'가 함정이며, TCSEC의 중심은 기밀성이다.

다시 나오면 이렇게 판단

TCSEC 관련 선지는 먼저 'D에서 A로 갈수록 높은 등급', '운영체제 중심', '기밀성 중심', '기능 요구와 보증 요구'라는 네 기준에 대조하여 판단한다.

암기 포인트

TCSEC는 D→C→B→A, 운영체제·기밀성 중심, 기능+보증 요구이다.

NoteBase

21. 개인정보 가명처리에 대한 설명으로 옳지 않은 것은?

① 가명정보는 개인정보를 가명처리함으로써 원래의 상태로 복원하기 위한 추가정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보이다.

② 가명정보는 처리(제공) 환경에 따라 가명정보처리자 내부에서 활용(자체활용 또는 내부 제공·결합)하는 경우와 제3자에게 제공하는 경우로 구분할 수 있다.

③ 가명정보처리자는 가명정보 또는 추가정보의 안전한 관리를 위하여 기술적 안전조치와 관리적 안전조치를 취해야 하며, 물리적 안전조치를 취하지 않아도 무방하다.

④ 가명정보는 개인정보처리자의 정당한 처리 범위 내에서 통계작성, 과학적 연구, 공익적 기록보존 등의 목적으로 정보주체의 동의 없이 처리할 수 있다.

정답 3번

쟁점

이 문제는 가명정보의 정의, 처리 환경, 안전조치 의무 및 동의 없는 처리 요건에 관한 문제이다. 핵심은 가명정보도 보호 대상이므로 기술적·관리적 조치뿐 아니라 물리적 조치까지 모두 필요하다는 점이다.

용어 풀이

가명정보는 개인정보를 가명처리하여, 원래 상태로 복원하기 위한 추가정보를 사용하거나 결합하지 않고서는 특정 개인을 알아볼 수 없게 한 정보이다. 추가정보는 가명정보를 원래 개인정보와 연결하거나 복원하는 데 사용될 수 있는 정보이다.

핵심 구분

「개인정보 보호법」 제2조 제1호 다목은 가명정보를 추가정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보로 정의한다. 같은 법 제28조의2 제1항은 통계작성, 과학적 연구, 공익적 기록보존 등을 위해 정보주체의 동의 없이 가명정보를 처리할 수 있도록 한다. 그러나 제28조의4 제1항은 가명정보 처리 시 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 모두 하도록 규정한다.

NoteBase

선지별 해설

① O
가명정보는 추가정보를 사용하거나 결합하지 않고서는 특정 개인을 알아볼 수 없도록 가명처리한 정보이므로 법률상 정의에 부합한다.

② O
가명정보의 처리 환경은 처리자 내부에서 자체 활용하거나 내부 제공·결합하는 경우와 외부의 제3자에게 제공하는 경우로 나누어 볼 수 있다. 제3자 제공은 처리 환경에 대한 통제 가능성이 내부 활용과 달라 별도로 구분된다.

③ X
가명정보처리자는 가명정보와 추가정보의 안전성 확보를 위하여 기술적·관리적 조치뿐 아니라 물리적 조치도 하여야 한다. 물리적 조치를 면제하는 규정은 없다.
틀린 표현: '물리적 안전조치를 취하지 않아도 무방하다'
올바른 표현: '기술적·관리적 및 물리적 안전조치를 모두 취하여야 한다'

④ O
개인정보처리자는 정당한 처리 범위에서 통계작성, 과학적 연구, 공익적 기록보존 등을 위해 정보주체의 동의 없이 가명정보를 처리할 수 있다. 이는 「개인정보 보호법」 제28조의2 제1항의 내용이다.

오답 포인트

③의 '물리적 안전조치를 취하지 않아도 무방하다'라는 문구가 함정이다. 가명처리로 식별 위험이 낮아졌더라도 가명정보는 여전히 개인정보에 해당하므로 안전조치 의무가 사라지지 않는다. 특히 법문은 기술적·관리적 '및' 물리적 조치를 모두 요구한다.

다시 나오면 이렇게 판단

가명정보 문항에서는 정의, 활용 목적, 제3자 제공, 안전조치를 순서대로 구분한다. 안전조치 선지에 '물리적 조치는 불필요하다'거나 일부 조치만 하면 된다는 표현이 있으면 법문의 '기술적·관리적 및 물리적 조치'와 대조하여 판단한다.

암기 포인트

가명정보는 동의 없이 활용할 수 있는 경우가 있어도 보호 의무가 없는 정보는 아니다. 안전조치는 기술·관리·물리의 세 가지를 모두 갖춘다.

NoteBase

22. 접근 권한이 시스템 전체적으로 보안 정책 및 관련 규칙에 따라 결정되기 보다는 자원의 소유자에 의해 결정되는 접근 제어 모델에 해당하는 것으로 옳은 것은?
① 강제적 접근 제어
② 임의적 접근 제어
③ 역할 기반 접근 제어
④ 규칙 기반 접근 제어

정답 2번

출제 포인트

접근 권한의 결정 주체와 기준을 바탕으로 강제적·임의적·역할 기반·규칙 기반 접근 제어를 구별하는 문제이다.

핵심 개념

임의적 접근 제어(DAC)는 자원의 소유자가 자신의 판단에 따라 접근 권한을 부여하거나 회수하는 방식이다.
강제적 접근 제어(MAC)는 시스템 전체의 보안 정책과 보안 등급에 따라 접근을 통제한다.
역할 기반 접근 제어(RBAC)는 사용자의 직무나 역할에 권한을 연결한다.
규칙 기반 접근 제어는 미리 정한 시스템 규칙이나 조건에 따라 접근 허용 여부를 결정한다.

선지별 해설

① X — 강제적 접근 제어는 자원 소유자가 아니라 시스템 전체의 보안 정책과 보안 등급에 따라 권한을 결정한다. 틀린 표현인 '강제적 접근 제어'는 '임의적 접근 제어'로 고쳐야 한다.
② O — 임의적 접근 제어는 자원의 소유자가 접근 권한을 부여·변경·회수할 수 있으므로 제시된 설명에 해당한다.
③ X — 역할 기반 접근 제어는 자원 소유자가 아니라 사용자가 맡은 직무나 역할을 기준으로 권한을 결정한다. 틀린 표현인 '역할 기반 접근 제어'는 '임의적 접근 제어'로 고쳐야 한다.
④ X — 규칙 기반 접근 제어는 자원 소유자의 재량이 아니라 미리 정한 시스템 규칙이나 조건에 따라 접근을 통제한다. 틀린 표현인 '규칙 기반 접근 제어'는 '임의적 접근 제어'로 고쳐야 한다.

오답 포인트

'시스템 전체의 정책 및 규칙에 따르지 않는다'는 앞부분만 보고 강제적 또는 규칙 기반 접근 제어를 고르면 틀린다. 결정적인 표현은 '자원의 소유자에 의해 결정된다'이며, 이는 임의적 접근 제어의 핵심 특징이다.

다시 나오면 이렇게 판단

권한의 결정 기준을 먼저 찾는다. 소유자이면 임의적 접근 제어, 보안 정책·등급이면 강제적 접근 제어, 직무·역할이면 역할 기반 접근 제어, 사전 정의된 조건·규칙이면 규칙 기반 접근 제어이다.

NoteBase

암기 포인트

소유자 재량은 DAC, 정책·등급은 MAC, 직무·역할은 RBAC, 사전 규칙은 규칙 기반 접근 제어이다.

NoteBase

23. 윈도우를 비롯한 시스템에서 하드웨어 레벨에서 보안을 향상시키는 방안으로 TPM(Trusted Platform Module)이 있다. TPM에 대한 설명으로 옳지 않은 것은?
① 암·복호화 및 전자서명 기능 제공
② 부팅 과정에서 인증을 통해 신뢰성 제공
③ 디바이스 및 플랫폼 인증
④ 운영체제에 의존하여 명령어가 동작함

정답 4번

출제 포인트

TPM이 제공하는 하드웨어 기반 보안 기능과 운영체제로부터의 독립성을 구별하는 문제이다.

핵심 개념

TPM은 암호 키의 생성·보관과 암호 연산, 플랫폼 무결성 측정 및 인증 등을 안전하게 수행하는 하드웨어 보안 모듈이다. 일반 소프트웨어보다 격리된 하드웨어에 신뢰의 근원을 두므로 운영체제가 변조되더라도 핵심 비밀과 측정값을 보호할 수 있다.

선지별 해설

① O — TPM은 암호 키를 안전하게 생성·보관하고 암호화·복호화 및 전자서명에 필요한 암호 연산을 지원한다.
② O — TPM은 부팅 구성요소의 측정값을 기록·검증하는 신뢰 부팅 및 측정 부팅에 활용되어 부팅 과정의 신뢰성을 높인다.
③ O — TPM에 안전하게 저장된 키와 증명 기능을 이용하면 특정 장치와 그 플랫폼의 상태 또는 신원을 인증할 수 있다.
④ X — 틀린 표현은 '운영체제에 의존하여 명령어가 동작함'이다. TPM은 운영체제에 보안의 근거를 두는 소프트웨어 모듈이 아니라 별도의 하드웨어 보안 모듈이며, 올바르게는 운영체제로부터 독립된 하드웨어 기반으로 보안 기능을 수행한다고 표현해야 한다.

오답 포인트

TPM을 운영체제가 호출할 수 있다는 사실과 TPM의 보안 기능이 운영체제에 의존한다는 주장을 혼동하기 쉽다. 운영체제나 응용 프로그램이 TPM 명령을 요청하더라도 키 보호와 암호 연산의 신뢰 기반은 TPM 하드웨어에 있다.

NoteBase

다시 나오면 이렇게 판단

TPM 관련 선지는 ‘하드웨어 기반 신뢰의 근원’, ‘안전한 키 보관과 암호 연산’, ‘부팅 무결성 측정’, ‘플랫폼 인증’에 해당하면 옳다고 판단한다. 운영체제에 보안 기능이 종속된다고 하면 TPM의 핵심 성격과 반대이므로 틀린 선지로 판단한다.

암기 포인트

TPM은 키·측정·인증을 담당하는 하드웨어 신뢰의 근원이며, 운영체제 의존형 보안 모듈이 아니다.

NoteBase

24. 블록체인 합의 알고리즘에 대한 설명으로 옳지 않은 것은?

① 분산 시스템에서 합의란 네트워크에 존재하는 독립적인 참여자들이 동일한 블록체인 원장을 유지할 수 있도록 원장에 포함할 블록을 결정하는 방식이다.

② 분산원장 시스템에서는 다양한 합의 알고리즘들이 사용될 수 있으며, 예로는 작업증명(PoW: Proof of Work), 지분증명(PoS: Proof of Stake), 위임지분증명(DPoS: Delegated Proof of Stake) 등이 존재한다.

③ 지분 증명은 블록을 생성하는 노드가 작업(예: 특정 조건을 충족해야하는 해시 연산 등 높은 비용/자원이 필요한 작업)을 통해 스스로의 신뢰성을 증명하는 합의 방식이다.

④ 분산원장 시스템 내의 모든 노드가 일관성 있는 분산원장을 보유할 수 있도록 통신을 통해 새로운 기록의 공유, 검증 및 추가에 대한 전체의 동의를 이끌어 내는 알고리즘이다.

정답 3번

출제 포인트

블록체인 합의 알고리즘의 역할과 작업증명(PoW)·지분증명(PoS)의 검증 기준을 구별하는 문제이다.

핵심 개념

합의 알고리즘: 중앙 관리자 없이 분산된 참여자들이 유효한 거래와 원장의 상태에 합의하도록 하는 절차이다.
작업증명(PoW): 노드가 많은 계산 자원을 투입해 해시 문제를 해결한 작업 결과로 블록 생성 자격을 증명한다. / 키워드: 연산 작업
지분증명(PoS): 노드가 보유하거나 예치한 지분을 바탕으로 검증자와 블록 생성 참여자를 정한다. / 키워드: 지분
위임지분증명(DPoS): 지분 보유자들이 대표 검증자를 선출해 합의에 참여하게 한다. / 키워드: 대표자 위임

NoteBase

선지별 해설

① O — 합의 알고리즘은 독립적인 참여자들이 동일한 원장 상태를 유지할 수 있도록 원장에 반영할 블록을 결정하는 방식이다.
② O — 분산원장에는 PoW, PoS, DPoS 등 여러 합의 알고리즘이 사용될 수 있다.
③ X — 틀린 표현은 '지분 증명'과 '높은 비용·자원이 필요한 해시 연산 작업'의 연결이다. 해시 연산 작업으로 블록 생성 자격을 증명하는 방식은 작업증명(PoW)이다. 지분증명(PoS)은 보유하거나 예치한 지분을 기준으로 검증자와 블록 생성 참여자를 정하는 방식으로 고쳐야 한다.
④ O — 합의 알고리즘은 참여 노드들이 새 기록의 유효성과 원장 상태에 합의하게 하여 일관된 분산원장을 유지하고, 검증된 기록을 공유·추가할 수 있게 한다.

오답 포인트

③은 '증명'이라는 공통 명칭 때문에 PoW와 PoS의 기준을 바꾸어 놓았다. 해시 연산과 계산 자원은 PoW의 특징이고, 지분의 보유·예치는 PoS의 특징이다.

다시 나오면 이렇게 판단

선지에서 합의 방식의 자격 기준을 확인한다. 해시 계산·연산 경쟁이면 PoW, 보유·예치 지분이면 PoS, 지분 보유자가 선출한 대표 검증자이면 DPoS로 판단한다.

암기 포인트

PoW는 작업, PoS는 지분, DPoS는 지분으로 뽑은 대표이다.

NoteBase

25. 유닉스나 리눅스 파일 설정 권한 중에서 일반 사용자가 실행 시 일시적으로 관리자(root)의 권한으로 실행되도록 함으로써 시스템의 보안에 허점을 초래할 수 있는 것으로 옳은 것은?

① SetGID ② SetUID
③ Sticky Bit ④ touch

정답 2번

출제 포인트

유닉스·리눅스의 특수 권한인 SetUID, SetGID, Sticky Bit의 실행 효과를 구별하고, 일반 사용자의 프로세스가 파일 소유자의 권한으로 실행되는 기능을 찾는 문제이다.

핵심 개념

SetUID: 실행 파일에 설정하면 그 파일을 실행한 프로세스가 실행자의 권한이 아니라 파일 소유자의 유효 사용자 ID 권한으로 동작한다. 따라서 root 소유 실행 파일에 SetUID가 설정되면 일반 사용자도 실행 중 일시적으로 root 권한을 사용할 수 있다.
SetGID: 실행 파일에 설정하면 프로세스가 파일 소유 그룹의 유효 그룹 ID 권한으로 동작한다.
Sticky Bit: 주로 공유 디렉터리에서 파일 삭제·이름 변경을 파일 소유자, 디렉터리 소유자 또는 root로 제한한다.
touch: 파일을 만들거나 파일의 접근·수정 시각을 갱신하는 명령이다.

선지별 해설

① X — SetGID는 프로세스를 파일 소유 그룹의 권한으로 실행하게 하는 특수 권한이다. 틀린 표현은 '관리자(root)의 권한으로 실행'이라는 취지이며, 올바르게는 '파일 소유 그룹의 유효 그룹 ID 권한으로 실행'이다.
② O — SetUID가 설정된 실행 파일은 실행 중 파일 소유자의 유효 사용자 ID 권한으로 동작한다. 파일 소유자가 root라면 일반 사용자가 실행해도 일시적으로 root 권한이 부여되므로, 잘못 설정하면 권한 상승 취약점이 생길 수 있다.
③ X — Sticky Bit는 일반 사용자의 프로세스를 root 권한으로 실행시키는 기능이 아니다. 틀린 표현은 '관리자 권한으로 실행'이라는 취지이며, 올바르게는 '공유 디렉터리에서 다른 사용자가 소유한 파일을 함부로 삭제하거나 이름을 바꾸지 못하게 제한'하는 기능이다.
④ X — touch는 특수 실행 권한이 아니라 파일 생성 또는 접근·수정 시각 갱신에 사용하는 명령이다. 틀린 표현은 '실행 시 관리자 권한을 부여하는 권한'이라는 취지이며, 올바르게는 '파일을 생성하거나 타임스탬프를 변경하는 명령'이다.

NoteBase

오답 포인트

SetUID와 SetGID는 모두 실행 시 신원을 바꾸지만 기준이 다르다. SetUID의 U는 사용자 ID, SetGID의 G는 그룹 ID를 뜻한다. 문제의 핵심 표현인 ‘root의 권한’은 root가 파일 소유자인 경우의 SetUID와 연결된다.

다시 나오면 이렇게 판단

실행 파일 소유자의 사용자 권한으로 동작하면 SetUID, 파일 소유 그룹의 권한으로 동작하면 SetGID, 공유 디렉터리의 삭제를 제한하면 Sticky Bit로 판단한다. root 소유 실행 파일과 일시적 root 권한이 함께 제시되면 SetUID를 선택한다.

암기 포인트

SetUID는 소유자(User) 권한, SetGID는 소유 그룹(Group) 권한, Sticky Bit는 공유 디렉터리의 삭제 제한이다.

NoteBase