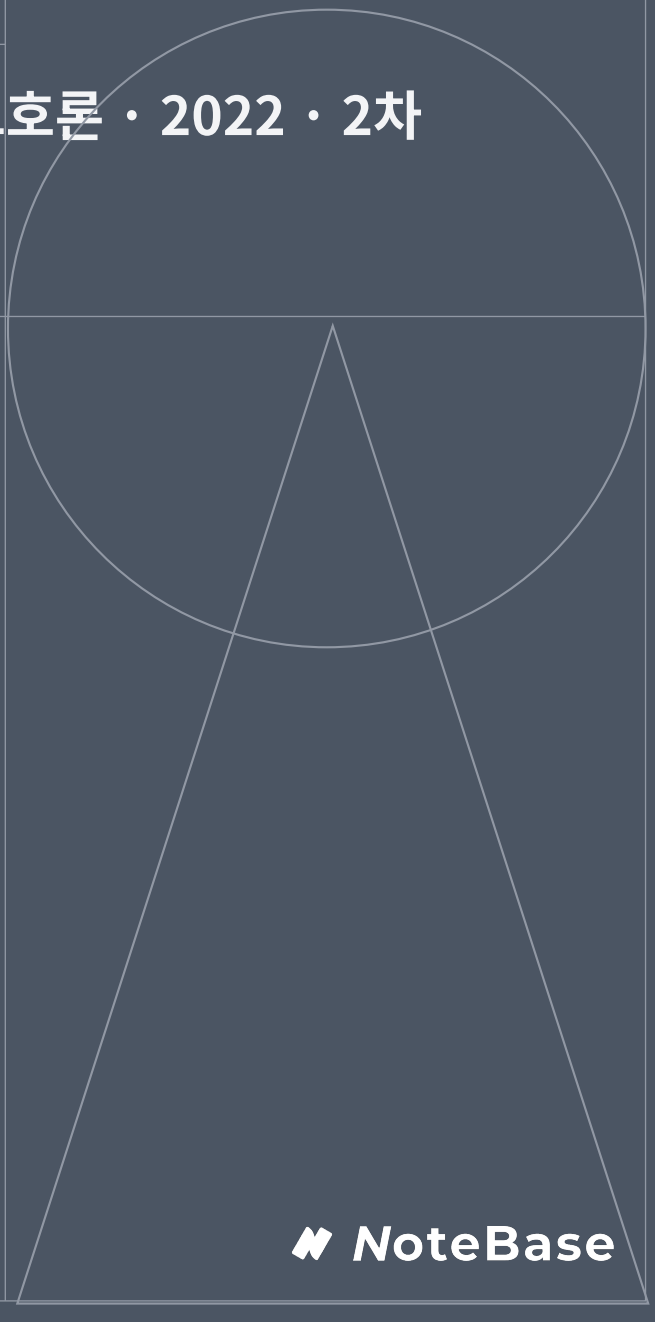
기출OX 해설집

공무원/국가직/7급 · 정보보호론 · 2022 · 2차



NoteBase

기출OX 해설집

공무원/국가직/7급 · 정보보호론 · 2022 · 2차

공무원/국가직/7급 · 정보보호론 · 2022 · 2차

문 1. 송신자가 수신자에게 전달하는 세션키를 공개키 암호 방식을 이용하여 암호화할 때 사용되는 키는?

① 송신자의 개인키

② 송신자의 공개키

③ 수신자의 개인키

④ 수신자의 공개키

정답 4번

출제 포인트

이 문제는 공개키 암호 방식에서 기밀성을 확보할 때 송신자가 누구의 공개키로 암호화하고 누구의 개인키로 복호화하는지를 묻는 문제이다.

핵심 개념

공개키 암호에서 기밀성 목적의 암호화는 수신자의 공개키로 수행하고, 복호화는 대응되는 수신자의 개인키로 수행한다. 송신자의 개인키는 보통 전자서명에 쓰이며 세션키 전달용 암호화 키가 아니다.

선지별 해설

1번: X. 송신자의 개인키는 본인만 사용할 수 있으므로 전자서명이나 송신자 인증에 대응되는 키이다. 틀린 표현은 "송신자의 개인키"이며, 올바르게는 "수신자의 공개키"이다.
2번: X. 송신자의 공개키로 암호화하면 대응되는 송신자의 개인키로만 복호화할 수 있으므로 수신자에게 세션키를 안전하게 전달하는 구조가 아니다. 틀린 표현은 "송신자의 공개키"이며, 올바르게는 "수신자의 공개키"이다.
3번: X. 수신자의 개인키는 수신자가 복호화할 때 사용하는 키이지 송신자가 암호화에 사용하는 키가 아니다. 틀린 표현은 "수신자의 개인키"이며, 올바르게는 "수신자의 공개키"이다.
4번: O. 송신자는 수신자만 복호화할 수 있도록 수신자의 공개키로 세션키를 암호화한다. 수신자는 자신의 개인키로 이를 복호화하므로 기밀성이 성립한다.

NoteBase

오답 포인트

공개키와 개인키의 짝은 기억하지만 암호화와 전자서명의 방향을 뒤섞으면 틀린다. 특히 "개인키로 암호화"를 세션키 전달과 연결하면 1번이나 3번으로 쉽게 흔들린다.

다시 나오면 이렇게 판단

문제가 세션키 전달이나 기밀성을 묻는다면 "암호화는 수신자의 공개키, 복호화는 수신자의 개인키" 순서로 판단한다. 반대로 송신자 인증이나 부인방지를 묻는다면 송신자의 개인키 사용 가능성을 본다.

암기 포인트

기밀성은 상대 공개키로 잠그고 상대 개인키로 연다. 서명은 내 개인키로 찍고 내 공개키로 확인한다.

NoteBase

문 2. 다음의 정보보호와 관련된 원칙을 제시한 사람은?

이 원칙은 공격자가 암호 알고리즘을 완전히 알고 있더라도 키가 없이는 복호화해 평문을 얻을 수 없어야 함을 의미하는 것으로, 암호 알고리즘의 안전성이 암호 알고리즘 설계 자체의 비밀성에 의존해서는 안 되고 키의 비밀성에 의존해야 함을 강조한다. 따라서 암호 알고리즘은 널리 공개해서 많은 암호학자의 검증을 거치는 과정을 통해 안전성을 인정받아야 한다.

① Rabin
② Hellman
③ Kerckhoffs
④ Koblitz

정답 3번

출제 포인트

암호 알고리즘의 안전성이 설계 비밀이 아니라 키의 비밀성에 의존해야 한다는 Kerckhoffs의 원칙을 묻는 문제이다.

핵심 정리

Rabin: Rabin 암호로 대표되며, 공개키 암호의 안전성을 소인수분해의 어려움과 연결하는 인물이다.
Hellman: Diffie-Hellman 키 교환과 time-memory tradeoff로 대표되며, 비밀키 공유와 공격 복잡도 절충으로 기억하는 인물이다.
Kerckhoffs: 공격자가 알고리즘을 모두 알아도 키 없이는 평문을 얻을 수 없어야 한다는 공개 설계 원칙을 제시한 인물이다.
Koblitz: 타원곡선 암호의 대표 인물로, ECC 적용과 연결되는 인물이다.

선지별 해설

① X: Rabin은 Rabin 암호와 소인수분해 기반 공개키 암호로 연결된다. 틀린 부분은 Rabin을 알고리즘 공개 전제의 보안 원칙과 연결한 점이다. 올바르게는 Rabin은 Rabin 암호 제안자로 본다.
② X: Hellman은 Diffie-Hellman 키 교환과 time-memory tradeoff로 연결된다. 틀린 부분은 Hellman을 Kerckhoffs의 원칙 제시자로 연결한 점이다. 올바르게는 Hellman은 공개 채널에서의 키 합의와 공격 복잡도 절충 개념으로 연결된다.
③ O: 지문은 공격자가 암호 알고리즘을 완전히 알아도 키 없이는 복호화할 수 없어야 하며, 보안은 설계 비밀이 아니라 키의 비밀성에 의존해야 한다고 설명한다. 이는 Kerckhoffs의 원칙이므로 Kerckhoffs가 맞다.
④ X: Koblitz는 타원곡선 암호와 연결되는 인물이다. 틀린 부분은 Koblitz를 알고리즘 공개와 키 비밀성의 원칙 제시자로 본 점이다. 올바르게는 Koblitz는 ECC의 대표 인물로 연결된다.

NoteBase

오답 포인트

Hellman도 매우 유명한 암호학자라서 헷갈리기 쉽지만, 지문의 핵심은 키 교환이 아니라 알고리즘 공개를 전제로 한 보안 설계 원칙이다. 인물의 유명세보다 대표 키워드가 지문과 정확히 맞는지를 봐야 한다.

다시 나오면 이렇게 판단

지문에 알고리즘 공개, 설계 비밀에 의존하지 않음, 키의 비밀성 같은 표현이 나오면 Kerckhoffs의 원칙으로 연결한다. 인물 매칭 문제는 이름보다 대표 문구를 먼저 대응시키면 판단이 빨라진다.

암기 포인트

Kerckhoffs는 알고리즘은 공개해도 되고 키만 비밀이면 된다는 원칙으로 기억한다.

NoteBase

문 3. (가), (나)에 들어갈 용어를 바르게 연결한 것은?

PGP 기법은 세션키로 메시지를 암호화하기 위해 (가) 알고리즘과 사용자 인증을 위한 전자서명에 이용하기 위해 (나) 알고리즘을 사용할 수 있다.

① (가): IDEA, (나): RSA
② (가): IDEA, (나): DES
③ (가): RSA, (나): IDEA
④ (가): RSA, (나): AES

정답 1번

출제 포인트

이 문제는 PGP에서 메시지 본문 암호화에 쓰는 대칭키 알고리즘과 전자서명에 쓰는 공개키 알고리즘을 구별할 수 있는지를 묻는다.

핵심 개념

IDEA는 PGP에서 메시지 내용을 빠르게 암호화하는 데 쓰는 대칭키 블록 암호이다.
RSA는 공개키와 개인키 쌍을 이용해 전자서명과 사용자 인증에 쓰는 공개키 알고리즘이다.
판단 축은 본문을 직접 암호화하는 대칭키 알고리즘인지, 서명과 인증에 쓰는 공개키 알고리즘인지이다.

선지별 해설

1번: O. IDEA는 PGP에서 세션키로 메시지 본문을 암호화할 때 사용하는 대표적인 대칭키 알고리즘이고, RSA는 전자서명과 사용자 인증에 사용할 수 있는 공개키 알고리즘이므로 연결이 맞다.
2번: X. 틀린 부분은 (나)의 "DES"이다. DES는 대칭키 알고리즘이므로 전자서명과 사용자 인증용 알고리즘으로 볼 수 없다. 올바르게는 (나)에 RSA가 들어간다.
3번: X. 틀린 부분은 (가)의 "RSA"와 (나)의 "IDEA"를 서로 바꿔 놓은 점이다. RSA는 본문을 세션키로 직접 암호화하는 알고리즘이 아니라 공개키 기반 서명과 키 관리에 가깝고, IDEA는 전자서명용이 아니라 대칭키 메시지 암호화용이다. 올바르게는 (가)는 IDEA, (나)는 RSA이다.
4번: X. 틀린 부분은 (가)의 "RSA"와 (나)의 "AES"이다. RSA는 세션키 알고리즘 자리에 맞지 않고, AES는 대칭키 알고리즘이어서 전자서명과 사용자 인증용 알고리즘이 아니다. 올바르게는 (가)는 IDEA, (나)는 RSA이다.

오답 포인트

세션키 암호화와 전자서명을 모두 "암호화"라는 말로만 묶어 보면 RSA와 IDEA, DES, AES의 역할을 뒤섞기 쉽다. 이 문항의 함정은 알고리즘 이름을 묻는 것이 아니라 대칭키용인지 공개키용인지 역할을 묻는 데 있다.

NoteBase

다시 나오면 이렇게 판단

문장에서 "세션키로 메시지를 암호화"라고 하면 대칭키 알고리즘을 먼저 찾고, "전자서명"이나 "사용자 인증"이라고 하면 공개키 알고리즘을 찾으면 된다. 본문 암호화와 서명 기능을 분리해서 보면 정답을 고를 수 있다.

암기 포인트

PGP는 본문 암호화는 대칭키 IDEA, 서명과 인증은 공개키 RSA로 정리된다.

NoteBase

문 4. 쓰레기 처리장 또는 휴지통을 뒤져서 정보를 얻어내는 사회공학적 공격 기법은?

① Eavesdropping
② Shoulder Surfing
③ Dumpster Diving
④ Forensic Analysis

정답 3번

출제 포인트

이 문제는 정보 수집형 사회공학 기법의 정의를 구별하는 문제이다.

핵심 개념

Eavesdropping은 통신 내용이나 대화를 몰래 엿듣는 도청형 정보수집이다.
Shoulder Surfing은 사람의 어깨너머로 화면, 문서, 키 입력을 훔쳐보는 기법이다.
Dumpster Diving은 버려진 문서, 메모, 저장매체, 출력물을 뒤져 민감 정보를 수집하는 기법이다.
Forensic Analysis는 공격 기법이 아니라 사고 후 디지털 증거를 보존·분석하는 조사 절차이다.

선지별 해설

① X: Eavesdropping은 통신이나 대화를 몰래 듣는 행위이므로 휴지통이나 폐기물을 뒤지는 상황과 다르다. 틀린 표현은 "쓰레기 처리장 또는 휴지통을 뒤져서"에 대응시키는 부분이다. 올바르게는 "통신 내용이나 대화를 도청하여 정보를 얻는 기법"이다.
② X: Shoulder Surfing은 피해자의 화면, 서류, 비밀번호 입력을 옆이나 뒤에서 훔쳐보는 기법이다. 틀린 표현은 "휴지통을 뒤져서"에 대응시키는 부분이다. 올바르게는 "어깨너머 관찰로 정보를 얻는 기법"이다.
③ O: Dumpster Diving은 폐기된 문서나 저장매체를 뒤져 유용한 정보를 수집하는 사회공학 기법이므로 문제의 설명과 정확히 일치한다.
④ X: Forensic Analysis는 침해사고 이후 증거를 수집하고 원인을 분석하는 포렌식 절차이다. 틀린 표현은 이를 "사회공학적 공격 기법"으로 보는 부분이다. 올바르게는 "사후 조사 및 증거 분석 활동"이다.

오답 포인트

사회공학 문제에서는 "정보를 얻는 방식"을 기준으로 용어를 구별해야 한다. ①은 듣기, ②는 보기, ③은 버려진 자료 수집, ④는 사후 분석인데, 모두 정보와 관련된 단어라서 공격 단계와 수집 방식을 섞으면 헷갈리기 쉽다.

다시 나오면 이렇게 판단

발문에 나온 행동을 동사로 바꾸어 대응하면 빠르게 풀린다. 듣는 것은 Eavesdropping, 훔쳐보는 것은 Shoulder Surfing, 버린 것을 뒤지는 것은 Dumpster Diving, 사고 후 분석은 Forensic Analysis로 판단된다.

NoteBase

암기 포인트

Dumpster Diving은 버린 자료를 뒤지는 기법이고, Forensic Analysis는 공격이 아니라 분석 절차이다.

NoteBase

문 5. 접근제어(Access Control)에 대한 설명으로 옳지 않은 것은?

① 임의적 접근제어(Discretionary Access Control)는 정보 소유자가 정보의 보안 수준을 결정하고 그에 대한 접근제어까지 설정한다.

② BLP(Bell-LaPadula) 모델과 Biba 모델은 강제적 접근제어(Mandatory Access Control) 모델에 해당한다.

③ 역할 기반 접근제어(Role-Based Access Control)는 사람이 아닌 역할 또는 직책에 권한을 부여한다.

④ BLP 모델에서는 낮은 수준의 보안 권한을 가진 사람이 자신의 권한보다 높은 보안 수준의 문서에 쓸 수 없다.

정답 4번

출제 포인트

이 문제는 DAC, MAC, RBAC와 BLP·Biba 모델의 차이, 특히 BLP의 읽기·쓰기 방향을 구별할 수 있는지를 묻는다.

핵심 개념

DAC는 정보 소유자가 접근 권한을 정하는 모델이다.
MAC는 중앙 정책과 보안 등급에 따라 접근을 강제하는 모델이다.
RBAC는 개인이 아니라 역할이나 직무에 권한을 묶어 부여하는 모델이다.
BLP는 기밀성 보호 모델로 no read up, no write down이 핵심이고, Biba는 무결성 보호 모델로 no read down, no write up이 핵심이다.

선지별 해설

1번: O. DAC는 객체 소유자나 정보 소유자가 다른 주체의 접근 권한을 재량으로 설정하는 방식이다. 선지의 '정보 소유자가 ... 접근제어까지 설정한다'는 설명이 DAC의 특징에 맞다.
2번: O. BLP와 Biba는 모두 주체와 객체에 보안 등급을 두고 규칙에 따라 접근을 강제하는 대표적 MAC 모델이다.
3번: O. RBAC는 사용자 개인마다 권한을 직접 붙이는 대신 역할, 직책, 직무에 권한을 부여하고 사용자는 그 역할을 통해 권한을 얻는다.
4번: X. 틀린 표현은 '자신의 권한보다 높은 보안 수준의 문서에 쓸 수 없다'이다. BLP는 기밀성 모델이므로 낮은 등급의 주체는 높은 등급의 문서를 읽을 수 없고(no read up), 자신의 정보가 낮은 등급으로 내려가는 쓰기를 할 수 없다(no write down). 따라서 낮은 등급 주체가 더 높은 등급 문서에 쓰는 것은 금지 대상이 아니다.
올바르게는 '낮은 수준의 보안 권한을 가진 사람은 자신의 권한보다 높은 보안 수준의 문서를 읽을 수 없다' 또는 '자신의 권한보다 낮은 보안 수준의 문서에 쓸 수 없다'이다.

NoteBase

오답 포인트

BLP와 Biba의 쓰기 금지 방향을 서로 바꾸면 틀리기 쉽다. 4번은 BLP의 규칙을 Biba의 no write up처럼 뒤집어 놓은 선지이다.

다시 나오면 이렇게 판단

접근제어 문제는 먼저 누가 권한을 정하는지로 DAC, 역할에 권한을 묶는지로 RBAC, 등급 정책을 강제하는지로 MAC를 구분한다. 그다음 BLP는 기밀성이라 '위는 읽지 못하고 아래에는 쓰지 못한다', Biba는 무결성이라 '아래는 읽지 못하고 위에는 쓰지 못한다'로 판단한다.

암기 포인트

BLP는 기밀성 보호로 no read up, no write down이고, Biba는 무결성 보호로 no read down, no write up이다.

NoteBase

문 6. 윈도우 운영체제에서 컴퓨터의 MAC 주소를 출력하는 명령어는?

① ping
② ipconfig/all
③ ifconfig
④ nslookup

정답 2번

출제 포인트

이 문제는 윈도우 네트워크 명령어의 용도를 구분하여 MAC 주소를 확인하는 명령을 묻는 문제이다.

핵심 개념

MAC 주소는 네트워크 인터페이스에 부여된 물리적 주소이다.
`ping`은 통신 가능 여부를 확인하는 명령이고, `ipconfig /all`은 윈도우에서 IP 설정과 물리적 주소를 포함한 어댑터 상세 정보를 출력하는 명령이다.
`ifconfig`는 전통적으로 유닉스·리눅스 계열의 인터페이스 정보 확인 명령이고, `nslookup`은 DNS 질의 명령이다.

NoteBase

선지별 해설

① X
`ping`은 대상 호스트와의 도달 가능성 및 응답 시간을 확인하는 명령이다. MAC 주소 자체를 출력하지 않는다.
틀린 표현은 `MAC 주소를 출력`하는 용도라는 점이다. 올바르게는 네트워크 연결 상태를 점검하는 명령이다.

② O
윈도우에서 MAC 주소는 `ipconfig /all` 실행 결과의 물리적 주소(Physical Address) 항목에서 확인할 수 있다. 선지의 `ipconfig/all`는 공백이 생략된 표기이지만, 의도한 명령은 `ipconfig /all`이다.

③ X
`ifconfig`는 네트워크 인터페이스 정보를 확인하는 명령이지만, 일반적으로 윈도우 기본 명령이 아니라 유닉스·리눅스 계열에서 사용한다.
틀린 표현은 윈도우 운영체제에서 MAC 주소를 출력하는 대표 명령처럼 제시된 점이다. 올바르게는 유닉스·리눅스 계열 인터페이스 정보 확인 명령이다.

④ X
`nslookup`은 도메인 이름과 IP 주소를 조회하는 DNS 질의 명령이다. MAC 주소를 출력하는 기능이 아니다.
틀린 표현은 `MAC 주소를 출력`하는 용도라는 점이다. 올바르게는 DNS 서버를 통해 이름 해석 결과를 조회하는 명령이다.

오답 포인트

로컬 네트워크 인터페이스 정보 확인 명령과 네트워크 진단 명령을 섞어 놓은 점이 함정이다. 특히 `ifconfig`가 MAC 주소를 보여 줄 수 있다는 사실만 기억하면 운영체제 조건을 놓치기 쉽다.

다시 나오면 이렇게 판단

발문에서 운영체제를 먼저 확인한 뒤, 묻는 정보가 로컬 어댑터 상세 정보인지, 연결 상태인지, DNS 조회인지를 구분하면 된다. 윈도우에서 MAC 주소를 묻는다면 어댑터 상세 정보를 출력하는 `ipconfig /all`을 고르면 된다.

암기 포인트

윈도우 MAC 주소는 `ipconfig /all`, 연결 확인은 `ping`, DNS 조회는 `nslookup`이다.

NoteBase

문 7. 다음 /etc/passwd 파일 내용의 일부에서 사용자의 그룹 ID는?

user05:x:1001:501:group05:/home/user05:/bin/bash

① x
② 1001
③ 501
④ group05

정답 3번

출제 포인트

이 문제는 /etc/passwd 항목의 필드 순서와 UID, GID의 의미를 구분하는 문제이다.

핵심 개념

/etc/passwd의 기본 형식은 사용자명:암호표시:UID:GID:설명필드:홈디렉터리:로그인셸이다.
UID는 사용자 ID이고 GID는 사용자의 기본 그룹 ID이다.
암호표시 필드의 x는 실제 암호 해시가 shadow 파일에 있음을 뜻하는 자리표시자이고, 다섯 번째 필드는 사용자 설명 정보(GECOS)이다.

선지별 해설

① X
x는 두 번째 필드로 암호 관련 자리표시자이다. 그룹 ID가 아니다.
틀린 표현은 x를 그룹 ID로 본 점이다. 올바르게는 x는 shadow 비밀번호 사용을 나타내는 값이다.

② X
1001은 세 번째 필드이므로 사용자 ID(UID)이다. 그룹 ID는 네 번째 필드이다.
틀린 표현은 1001을 그룹 ID로 본 점이다. 올바르게는 1001은 UID이다.

③ O
501은 네 번째 필드이므로 사용자의 기본 그룹 ID(GID)이다. /etc/passwd에서 그룹 ID는 숫자로 기록된다.

④ X
group05는 다섯 번째 필드에 있는 사용자 설명 정보로 볼 수 있으며 GID가 아니다. 그룹 ID는 이름이 아니라 숫자 필드로 저장된다.
틀린 표현은 group05를 그룹 ID로 본 점이다. 올바르게는 group05는 설명 필드 값이고 GID는 501이다.

NoteBase

오답 포인트

UID와 GID가 둘 다 숫자라서 세 번째와 네 번째 필드를 바꿔 읽기 쉽다. 또 group05라는 문자열 때문에 그룹 이름처럼 보이지만, /etc/passwd에서 묻는 그룹 ID는 네 번째 숫자 필드이다.

다시 나오면 이렇게 판단

/etc/passwd는 콜론 기준으로 끊어서 세 번째는 UID, 네 번째는 GID라고 바로 대입하면 된다. 문자열 필드보다 숫자 필드의 위치를 먼저 확인하면 오답을 피할 수 있다.

암기 포인트

/etc/passwd는 3번째 UID, 4번째 GID이다.

NoteBase

문 8. 다음은 블록 암호의 운영모드 중 하나를 표현하고 있다. 해당 운영모드에 대해 추론할 수 있는 설명으로 옳은 것은? (단, $i, j \geq 0, i \neq j$이다)

P_i: 평문 블록	$C_i = P_i \oplus O_i$
C_i: 암호문 블록	$P_i = C_i \oplus O_i$
E_k: 암호화 함수(키 k 이용)	$O_i = E_k(I_i)$
IV: 초기벡터(Initial Vector)	$I_i = O_{i-1}$(단, $I_0 = IV$)

① C_i에 비트 오류가 발생하더라도 복호화된 P_j에 영향을 미치지 않는다.

② P_i와 P_j가 동일할 경우 C_i와 C_j가 같아지는 문제점이 존재한다.

③ 고속의 암 · 복호화를 위해 별도의 전처리 없이 병렬처리가 가능하다.

④ 복호화에 사용되는 IV값은 암호화에 사용된 IV값과 다를 수 있다.

정답 1번

출제 포인트

이 문제는 도식의 수식 $C_i = P_i \oplus O_i$, $O_i = E_k(I_i)$, $I_i = O_{i-1}$를 보고 OFB 모드임을 식별한 뒤, OFB의 오류 전파 방식과 병렬 처리 가능 여부를 판단하는 문제이다.

핵심 개념

OFB는 블록 암호 출력 O_i를 키스트림처럼 만들어 평문과 XOR하는 스트림화 운용모드이다. 다음 입력이 이전 암호문이 아니라 이전 출력 O_{i-1}이므로, 암호문 비트 오류가 다음 평문 블록들로 전파되지 않는 특징이 있다.

NoteBase

선지별 해설

① O

$P_i = C_i \oplus O_i$이므로 암호문 C_i의 한 비트 오류는 같은 위치의 P_i 한 비트에만 영향을 준다. OFB는 다음 키스트림 생성에 C_i를 쓰지 않고 O_{i-1}를 쓰므로, C_i의 오류가 복호화된 다른 블록 P_j까지 번지지 않는다.

② X

OFB는 블록마다 서로 다른 키스트림 O_i와 XOR하므로, P_i와 P_j가 같아도 일반적으로 C_i와 C_j는 같아지지 않는다. 틀린 표현은 '같은 평문 블록이면 같은 암호문 블록이 된다'이고, 올바르게는 '같은 평문이라도 키스트림이 다르면 암호문도 달라진다'이다.

③ X

OFB는 O_i를 만들기 위해 바로 앞 출력 O_{i-1}가 필요하므로 키스트림 생성 과정이 순차적이다. 따라서 별도의 전처리 없이 각 블록을 즉시 병렬 생성할 수는 없다. 틀린 표현은 '별도의 전처리 없이 병렬처리가 가능하다'이고, 올바르게는 '키스트림을 미리 생성해 두면 XOR 단계는 병렬화할 수 있지만, 키스트림 생성 자체는 순차적이다'이다.

④ X

OFB는 복호화도 같은 키스트림을 XOR로 제거하는 방식이므로, 복호화에 쓰는 IV는 암호화 때의 IV와 같아야 한다. 틀린 표현은 '복호화에 사용되는 IV값은 암호화에 사용된 IV값과 다를 수 있다'이고, 올바르게는 '복호화에는 암호화와 동일한 IV를 사용해야 한다'이다.

오답 포인트

CBC와 OFB를 혼동하면 ①과 ③에서 틀리기 쉽다. CBC는 암호문 오류가 다음 블록 복호화에도 영향을 줄 수 있지만, OFB는 키스트림 기반이라 오류 전파가 거의 없다. 또한 OFB는 스트림처럼 보이더라도 키스트림 생성이 이전 출력에 연쇄되므로, CTR처럼 완전 병렬 모드로 보면 안 된다.

다시 나오면 이렇게 판단

도식에서 다음 입력이 이전 암호문 C_{i-1}인지, 이전 출력 O_{i-1}인지부터 확인한다. 이전 출력이 다시 암호화 함수 입력으로 들어가면 OFB로 판단하고, 이 경우 오류 전파는 작고 IV는 반드시 동일해야 하며 키스트림 생성은 순차적이라고 정리하면 된다.

암기 포인트

OFB는 출력 되먹임 방식이므로 '오류 전파는 적고, IV는 같아야 하며, 키스트림 생성은 순차적'인 모드이다.

NoteBase

문 9. 개인정보 보호법령상 민감정보와 고유식별정보를 바르게 연결한 것은?

① 유전자검사 등의 결과로 얻어진 유전정보 - 운전면허의 면허번호

② 정당의 가입정보 - 유전자검사 등의 결과로 얻어진 유전정보

③ 여권번호 - 외국인등록번호

④ 범죄경력자료 - 군번

정답 1번

쟁점

이 문제는 개인정보 보호법령상 민감정보와 고유식별정보의 범위를 구별하는 문제이다. 핵심은 유전정보·범죄경력자료·정당 가입정보는 민감정보에 해당하고, 고유식별정보는 법령이 열거한 번호 정보라는 점을 구별하는 것이다.

용어 풀이

민감정보 = 사생활 침해 우려가 커서 별도의 처리 제한이 문제되는 개인정보이다.
고유식별정보 = 법령에 따라 개인을 고유하게 구별하기 위하여 부여된 번호형 식별정보이다.

핵심 구분

민감정보에는 정당의 가입·탈퇴 정보, 유전자검사 등의 결과로 얻어진 유전정보, 범죄경력자료 등이 포함된다. 반면 고유식별정보는 주민등록번호, 여권번호, 운전면허의 면허번호, 외국인등록번호처럼 법령이 열거한 번호 정보로 한정된다. 여권번호와 외국인등록번호는 모두 고유식별정보이고, 군번은 여기에 포함되지 않는다.

NoteBase

선지별 해설

① O
- 유전자검사 등의 결과로 얻어진 유전정보는 민감정보이고, 운전면허의 면허번호는 고유식별정보이다. 두 정보를 바르게 연결하였다.

② X
- 정당의 가입정보는 민감정보에 해당한다. 유전자검사 등의 결과로 얻어진 유전정보도 고유식별정보가 아니라 민감정보이다.
- 틀린 표현: 유전자검사 등의 결과로 얻어진 유전정보를 고유식별정보로 본 부분이다.
- 올바른 표현: 정당의 가입정보와 유전정보는 모두 민감정보이다.

③ X
- 여권번호와 외국인등록번호는 모두 고유식별정보이다. 민감정보와 고유식별정보의 연결이 아니다.
- 틀린 표현: 여권번호를 민감정보 쪽 정보처럼 연결한 부분이다.
- 올바른 표현: 여권번호와 외국인등록번호는 모두 고유식별정보이다.

④ X
- 범죄경력자료는 민감정보이다. 그러나 군번은 개인정보일 수는 있어도 개인정보 보호법령상 고유식별정보로 열거된 정보는 아니다.
- 틀린 표현: 군번을 고유식별정보로 본 부분이다.
- 올바른 표현: 범죄경력자료는 민감정보이고, 고유식별정보는 주민등록번호·여권번호·운전면허의 면허번호·외국인등록번호이다.

오답 포인트

민감정보와 고유식별정보를 모두 '중요한 개인정보' 정도로 묶어 외우면 틀리기 쉽다. 민감정보는 사생활 내용 자체가 문제되는 정보이고, 고유식별정보는 법정 번호 정보라는 기준을 놓치면 ②처럼 유전정보를 번호 정보로 오인하거나 ③처럼 번호 정보끼리의 짝을 정답처럼 착각하게 된다.

다시 나오면 이렇게 판단

선지의 각 정보를 내용정보와 번호정보로 먼저 나눈다. 정당 가입정보·유전정보·범죄경력자료처럼 사생활 내용이면 민감정보로 보고, 주민등록번호·여권번호·운전면허번호·외국인등록번호처럼 법령이 열거한 번호이면 고유식별정보로 판단하면 된다.

암기 포인트

민감정보는 사생활 내용, 고유식별정보는 법정 4대 번호이다.

NoteBase

문 10. 개인정보보호위원회 고시에 따른 개인정보 영향평가 영역과 평가 분야를 짝 지은 것으로 옳지 않은 것은?

① 대상기관 개인정보보호 관리체계 - 개인정보 침해대응
② 대상시스템의 개인정보보호 관리체계 - 접근권한 관리
③ 개인정보처리 단계별 보호조치 - 이용 및 제공
④ 대상시스템의 기술적 보호조치 - 개인정보의 암호화

정답 2번

쟁점

이 문제는 개인정보보호위원회 고시의 개인정보 영향평가 별표에서 평가영역과 평가분야의 대응 관계를 구별하는 문제이다. 핵심은 대상기관 관리체계, 대상시스템 관리체계, 개인정보 처리 단계별 보호 조치, 대상시스템의 기술적 보호 조치에 속하는 평가분야를 정확히 짝짓는 것이다.

용어 풀이

평가영역은 큰 분류이고, 평가분야는 그 아래에 배치되는 세부 관리 주제이다.

핵심 구분

원칙적으로 대상기관 개인정보보호 관리체계에는 개인정보 보호 조직, 개인정보 보호 계획, 개인정보 침해대응, 정보주체 권리보장이 들어간다.
대상시스템의 개인정보보호 관리체계에는 개인정보취급자 관리, 개인정보파일 관리, 개인정보 처리방침, 공공시스템 내부관리계획이 들어간다.
개인정보 처리 단계별 보호 조치에는 수집, 보유, 이용·제공, 위탁, 파기가 들어간다.
대상시스템의 기술적 보호 조치에는 접근권한 관리, 접근통제, 개인정보의 암호화, 접속기록의 보관 및 점검, 악성프로그램 등 방지 등이 들어간다.

NoteBase

선지별 해설

① O
- 개인정보 침해대응은 고시 별표상 '대상기관 개인정보보호 관리체계'에 속하는 평가분야이다. 대상기관 차원의 침해사고 신고 안내와 유출사고 대응을 보는 항목이므로 짝이 맞다.

② X
- 접근권한 관리는 고시 별표상 '대상시스템의 기술적 보호 조치'에 속하는 평가분야이다. 계정 관리, 인증 관리, 권한 관리처럼 시스템 접근을 기술적으로 통제하는 내용이기 때문이다.
- 틀린 표현: 대상시스템의 개인정보보호 관리체계 - 접근권한 관리
- 올바른 표현: 대상시스템의 기술적 보호 조치 - 접근권한 관리

③ O
- 이용 및 제공은 고시 별표상 '개인정보 처리 단계별 보호 조치'에 속하는 평가분야이다. 개인정보 제공의 적합성, 목적 외 이용·제공 제한, 제공 시 안전성 확보 같은 내용이 여기에 포함되므로 짝이 맞다.

④ O
- 개인정보의 암호화는 고시 별표상 '대상시스템의 기술적 보호 조치'에 속하는 평가분야이다. 저장 시 암호화와 전송 시 암호화가 대표 세부 분야이므로 짝이 맞다.

오답 포인트

이 문제를 틀렸다면 '대상시스템의 개인정보보호 관리체계'와 '대상시스템의 기술적 보호 조치'를 혼동했을 가능성이 높다. 관리체계는 취급자 관리, 파일 관리, 처리방침처럼 운영체계 성격이 강하고, 접근권한 관리나 암호화는 기술적 보호조치라는 점이 함정이다.

다시 나오면 이렇게 판단

먼저 평가분야 이름이 조직·계획·침해대응 같은 운영체계인지, 수집·이용·제공 같은 처리단계인지, 접근권한·암호화 같은 시스템 보안기술인지 분류하면 된다. 기술통제 성격이 강하면 '대상시스템의 기술적 보호 조치'로 판단하는 방식이 가장 빠르다.

암기 포인트

접근권한과 암호화는 기술조치이고, 이용·제공은 처리단계이며, 침해대응은 대상기관 관리체계이다.

NoteBase

문 11. 사용자가 웹브라우저에서 정확한 웹페이지 주소를 입력하여도 가짜 웹페이지로 접속되는 피싱 공격은?

① 보이스 피싱(Voice Phishing)

② 메신저 피싱(Messenger Phishing)

③ 스미싱(Smishing)

④ 파밍(Pharming)

정답 4번

출제 포인트

이 문제는 보이스 피싱, 메신저 피싱, 스미싱, 파밍의 공격 매체와 유도 방식을 구별하는지를 묻는다.

핵심 개념

보이스 피싱: 전화를 이용해 개인정보나 금전을 편취하는 수법이다. 결정 차이축: 음성 통화 기반 / 키워드: 전화
메신저 피싱: 메신저 대화를 사칭해 송금이나 정보 제공을 유도하는 수법이다. 결정 차이축: 메신저 대화 기반 / 키워드: 메신저
스미싱: 문자메시지에 링크를 넣어 악성 앱 설치나 정보 입력을 유도하는 수법이다. 결정 차이축: SMS 링크 기반 / 키워드: 문자
파밍: 사용자가 정상 주소를 입력해도 DNS 변조 등으로 가짜 사이트에 접속하게 만드는 수법이다. 결정 차이축: 접속 경로 변조 / 키워드: 정상 URL 입력 후 가짜 사이트

NoteBase

선지별 해설

① X
보이스 피싱은 전화를 이용한 음성 기반 사기이므로, 웹브라우저에서 주소를 입력한 뒤 가짜 웹페이지로 연결되는 상황과 다르다.
틀린 표현은 "보이스 피싱"이다.
올바르게는 "전화를 통해 개인정보나 금전을 요구하는 피싱"이다.

② X
메신저 피싱은 카카오톡 등 메신저 계정을 사칭해 송금이나 정보 제공을 유도하는 수법이므로, 정상 URL 입력 후 위조 사이트로 연결되는 공격을 가리키지 않는다.
틀린 표현은 "메신저 피싱"이다.
올바르게는 "메신저 대화를 이용해 피해자를 속이는 피싱"이다.

③ X
스미싱은 문자메시지와 포함된 링크를 이용하는 공격이다. 이 문제의 핵심은 사용자가 정확한 주소를 직접 입력했는데도 가짜 사이트로 이동한다는 점이므로 스미싱과 구별된다.
틀린 표현은 "스미싱"이다.
올바르게는 "문자메시지의 링크를 통해 악성 행위로 유도하는 피싱"이다.

④ O
파밍은 DNS 변조나 호스트 파일 변조 등으로 정상 주소를 입력해도 공격자가 만든 가짜 웹페이지로 연결되게 하는 공격이므로 문제의 설명과 일치한다.

오답 포인트

가짜 웹페이지라는 표현만 보고 ③ 스미싱으로 오인하기 쉽다. 그러나 스미싱은 문자 링크가 출발점이고, 파밍은 사용자가 직접 정상 URL을 입력해도 접속 경로가 변조된다는 점이 결정적 차이이다.

다시 나오면 이렇게 판단

피싱 수법 문제는 먼저 공격 매체가 전화, 메신저, 문자, 접속 경로 변조 중 무엇인지 구분한다. 정상 URL을 직접 입력했는데도 위조 사이트로 연결되면 파밍으로 판단된다.

암기 포인트

보이스는 전화, 메신저는 대화창, 스미싱은 문자 링크, 파밍은 정상 주소 입력 후 가짜 사이트 연결이다.

NoteBase

문 12. DSS(Digital Signature Standard)에 대한 설명으로 옳지 않은 것은?

① 부인방지를 보장한다.

② 공개키 암호 방식을 사용한다.

③ 메시지의 길이에 비례하는 길이의 전자서명을 생성한다.

④ 사용되는 해시 함수는 일방향성과 충돌 저항성을 만족해야 한다.

정답 3번

출제 포인트

이 문제는 DSS가 해시 기반 전자서명으로 동작한다는 점과 전자서명의 길이를 결정하는 요소를 구별할 수 있는지를 묻는다.

핵심 개념

DSS는 공개키 방식의 전자서명 표준으로, 메시지 원문 전체가 아니라 해시값을 서명한다. 따라서 전자서명 길이는 메시지 길이에 비례하지 않고 사용 알고리즘과 키 파라미터에 의해 정해진다.

선지별 해설

1번 O: DSS는 서명자의 개인키로 서명하고 공개키로 검증하므로, 서명자가 나중에 자신이 서명한 사실을 부인하기 어렵게 하여 부인방지를 제공한다.
2번 O: DSS는 개인키와 공개키를 사용하는 비대칭키 기반 전자서명 방식이므로 공개키 암호 방식을 사용한다.
3번 X: 틀린 부분은 "메시지의 길이에 비례하는 길이의"이다. 실제로는 메시지를 해시한 고정 길이 요약값에 서명을 하므로 전자서명 길이는 메시지 길이에 비례하지 않는다. 올바르게는 "메시지의 길이와 무관한 전자서명을 생성한다"에 가깝다.
4번 O: DSS에서 사용하는 해시 함수는 원문 역산이 어려운 일방향성과 서로 다른 입력이 같은 해시값을 만들기 어려운 충돌 저항성을 만족해야 한다.

오답 포인트

전자서명이 메시지 전체에 그대로 붙는다고 생각하면 3번을 맞는 설명으로 오해하기 쉽다. DSS의 실제 서명 대상은 원문이 아니라 해시값이라는 점을 놓치면 틀린다.

다시 나오면 이렇게 판단

전자서명 문제는 먼저 공개키 방식인지 확인하고, 다음으로 원문 전체를 직접 처리하는지 해시값을 처리하는지를 본다. 해시 기반 서명이라면 서명 길이는 보통 메시지 길이와 직접 비례하지 않는다.

NoteBase

암기 포인트

DSS는 공개키 서명, 서명 대상은 원문이 아니라 해시값, 서명 길이는 메시지 길이와 무관하다는 흐름으로 정리된다.

NoteBase

문 13. KISA의 IoT 공통 보안 7대 원칙을 기반으로 IoT 보안을 수행할 때 옳지 않은 것은?

① 안전한 초기 보안 설정 방안을 제공하여 기본으로 설정된 파라미터 설정 후 재설정 금지

② 안전한 설치를 위한 보안 프로토콜 준수 및 안전한 파라미터 설정

③ IoT 제품과 서비스의 취약점 패치 및 업데이트 지속 이행

④ 안전한 운영 · 관리를 위한 정보보호 및 프라이버시 관리체계 마련

정답 1번

출제 포인트

이 문제는 KISA의 IoT 공통 보안 7대 원칙 중 '안전한 초기 보안 설정 방안 제공'과 '보안 프로토콜 준수 및 안전한 파라미터 설정'의 취지를 정확히 구분하는지를 묻는 문제이다.

핵심 개념

- 안전한 초기 보안 설정 방안 제공: 초기 상태에서 취약한 기본값을 두지 않고 안전한 기본 보안 설정을 제공하는 원칙이다.
- 보안 프로토콜 준수 및 안전한 파라미터 설정: 설치·재설치·구성 단계에서 검증된 보안 프로토콜을 사용하고 파라미터를 안전하게 설정하는 원칙이다.
- 취약점 보안패치 및 업데이트 지속 이행: 운영 단계에서 소프트웨어와 하드웨어의 취약점을 계속 점검하고 패치를 수행하는 원칙이다.
- 정보보호 및 프라이버시 관리체계 마련: 사용자 정보의 취득·사용·폐기 전주기를 보호하는 관리체계를 갖추는 원칙이다.

NoteBase

선지별 해설

① X
안전한 초기 보안 설정 방안 제공은 취약한 기본 설정을 방치하지 말고 안전한 기본값을 제공하라는 뜻이다.
틀린 부분은 '파라미터 설정 후 재설정 금지'이다.
실제로는 재설정을 금지하는 원칙이 아니라 안전한 기본 보안 설정을 제공하는 원칙이며, 파라미터의 안전한 설정은 별도의 원칙으로 다루어진다.

② O
KISA 원칙 4는 보안 프로토콜 준수 및 안전한 파라미터 설정이다.
설치·재설치·구성 단계에서 검증된 보안 프로토콜과 안전한 파라미터 설정을 요구하므로 선지의 취지가 맞다.

③ O
KISA 원칙 5는 IoT 제품·서비스의 취약점 보안패치 및 업데이트 지속 이행이다.
운영 단계에서 취약점을 모니터링하고 패치를 계속 수행해야 하므로 선지의 내용이 맞다.

④ O
KISA 원칙 6은 안전한 운영·관리를 위한 정보보호 및 프라이버시 관리체계 마련이다.
사용자 정보의 전주기 보호와 프라이버시 관리체계를 갖추는 내용이므로 선지의 진술이 맞다.

오답 포인트

1번은 '안전한 초기 보안 설정'을 '한 번 설정하면 다시 못 바꾸게 하는 것'으로 바꿔 놓은 것이 함정이다. 이 원칙의 핵심은 재설정 금지가 아니라 취약한 기본값을 두지 않는 Secure by Default의 취지이다.

다시 나오면 이렇게 판단

IoT 공통 보안 원칙 문제에서는 각 원칙의 단계와 핵심 키워드를 먼저 대응시키면 된다. 초기 설정은 안전한 기본값 제공, 설치 단계는 보안 프로토콜과 파라미터 설정, 운영 단계는 패치와 관리체계로 구분하면 선지 판단이 쉬워진다.

암기 포인트

초기 설정은 안전한 기본값, 설치 단계는 프로토콜·파라미터, 운영 단계는 패치·관리체계이다.

NoteBase

문 14. 다음에서 설명하는 시스템 공격 기법은?

◯ 두 개 이상의 프로세스가 동시에 한정된 CPU 자원을 활용할 경우 서로 경쟁하는 상황이 발생
◯ 두 개의 프로세스는 일반 프로그램과 공격 프로그램에 의해 생성되며, 일반 프로그램은 파일 소유자가 root이며 임시파일을 생성하는 SetUID가 설정된 프로그램
◯ 공격자는 SetUID가 설정된 일반 프로그램이 생성하는 임시파일에 심볼릭 링크를 연결하여 일반 프로그램이 생성하는 임시파일을 공격 프로그램이 원하는 목표파일로 연결하는 공격

① Race Condition Attack
② Reverse Engineering Attack
③ Format String Attack
④ Heap Buffer Overflow Attack

정답 1번

출제 포인트

이 문제는 SetUID 프로그램의 임시파일 생성 과정에서 심볼릭 링크와 실행 시점 경쟁을 악용하는 공격을 보고 해당 공격 기법을 식별할 수 있는지를 묻는 문제이다.

사례 정리

핵심 사실 1: 두 개의 프로세스가 한정된 CPU 자원을 두고 경쟁하는 상황이 전제되어 있다.
핵심 사실 2: root 소유의 SetUID 프로그램이 임시파일을 생성한다.
핵심 사실 3: 공격자가 그 임시파일 경로에 심볼릭 링크를 걸어 원하는 목표파일로 연결한다.
판단에 중요한 조건: 공격의 핵심은 메모리 손상이나 코드 분석이 아니라 파일 생성 시점의 경쟁 상태를 노리는 점이다.

핵심 개념

Race Condition Attack은 둘 이상의 실행 흐름이 같은 자원이나 상태를 두고 경쟁할 때 그 짧은 시간차를 악용해 비정상 결과를 만드는 공격이다.
이 문항에서는 특히 SetUID 프로그램의 임시파일 생성 타이밍을 노려 심볼릭 링크로 권한 있는 쓰기 대상을 바꾸는 TOCTOU 성격의 경쟁 상태 공격이 문제된다.

적용 기준

이 사례에서는 공격자가 프로그램을 분석하거나 버퍼를 넘치게 하는 것이 아니라, 권한 있는 프로그램이 파일을 만들거나 여는 순간을 가로채 다른 파일에 쓰게 만드는지를 본다. 임시파일, SetUID, 심볼릭 링크, 경쟁 상황이 함께 나오면 Race Condition Attack을 우선 떠올리게 된다.

NoteBase

선지별 해설

① O: 제시문은 여러 프로세스의 경쟁 상태와 SetUID 프로그램의 임시파일 생성 시점을 악용해 심볼릭 링크로 목표파일을 바꾸는 공격을 설명한다. 이는 대표적인 Race Condition Attack이다.
② X: Reverse Engineering Attack은 실행 파일이나 시스템을 분석해 내부 로직, 알고리즘, 구조를 역추적하는 공격이다. 틀린 표현은 공격의 초점을 코드 분석으로 보는 점이며, 올바르게는 이 사례는 실행 타이밍과 파일 링크 조작을 악용하는 경쟁 상태 공격이다.
③ X: Format String Attack은 `printf(user_input)`처럼 포맷 문자열을 검증 없이 사용해 메모리 내용을 읽거나 쓰게 만드는 공격이다. 틀린 표현은 임시파일 심볼릭 링크 문제를 포맷 문자열 취약점으로 보는 점이며, 올바르게는 포맷 지정자 `%x`, `%n` 등의 오용이 있어야 Format String Attack이 성립한다.
④ X: Heap Buffer Overflow Attack은 힙 영역 버퍼의 경계를 넘겨 인접 메모리나 제어 데이터를 덮어쓰는 공격이다. 틀린 표현은 파일 생성 시점의 경쟁 문제를 버퍼 경계 초과로 보는 점이며, 올바르게는 힙 오버플로는 메모리 쓰기 범위 초과가 핵심이고 이 사례는 파일 경로 연결과 시점 경쟁이 핵심이다.

오답 포인트

SetUID와 root라는 단어 때문에 막연히 권한상승이나 메모리 취약점으로만 연결하면 ③이나 ④로 흔들리기 쉽다. 그러나 이 문제의 결정 단서는 임시파일과 심볼릭 링크, 그리고 프로세스 간 경쟁 상황이다. 공격 대상이 메모리가 아니라 파일 처리 시점이라는 점을 잡아야 한다.

다시 나오면 이렇게 판단

사례형 공격 문제는 먼저 공격 수단이 코드 분석인지, 메모리 손상인지, 입력 해석 오류인지, 자원 경쟁인지로 분류한다. 임시파일 생성, 링크 바꿔치기, SetUID, 시간차 악용이 보이면 Race Condition Attack으로 판단할 수 있다.

암기 포인트

임시파일 + SetUID + 심볼릭 링크 + 시간차 악용 = Race Condition Attack이다.

NoteBase

문 15. 무선랜 보안 기술에 대한 설명으로 옳지 않은 것은?

① TKIP는 WPA의 취약점을 해결하기 위해 도입되었다.

② CCMP는 CBC-MAC와 CTR 모드를 이용한다.

③ IEEE 802.11i는 TKIP와 CCMP 방식을 지원한다.

④ WPA2는 AES 암호 알고리즘을 이용한다.

정답 1번

출제 포인트

이 문제는 WEP, WPA, WPA2와 이에 대응하는 TKIP, CCMP, AES의 관계를 정확히 구분하는지를 묻는 문제이다.

핵심 개념

WEP는 초기 무선랜 보안 방식으로 구조적 취약점이 많다.
TKIP는 WEP 장비를 최대한 활용하면서 WEP의 취약점을 완화하려고 WPA에서 도입한 과도기적 보안 방식이다.
CCMP는 AES 기반의 강한 보안 방식으로 CBC-MAC과 CTR 모드를 결합하여 무결성과 기밀성을 함께 제공한다.
WPA2는 IEEE 802.11i를 바탕으로 CCMP(AES)를 본격 적용한 보안 체계이다.

NoteBase

선지별 해설

① X
틀린 부분은 "WPA의 취약점"이다.
TKIP는 WPA 자체의 취약점을 해결하려고 나온 것이 아니라, WEP의 취약점을 보완하기 위해 WPA에서 채택된 방식이다. 올바르게는 "TKIP는 WEP의 취약점을 보완하기 위해 WPA에서 도입되었다"이다.

② O
CCMP는 Counter Mode with CBC-MAC의 약자로, CBC-MAC으로 무결성을 확인하고 CTR 모드로 데이터를 암호화한다.

③ O
IEEE 802.11i는 강한 보안 방식으로 CCMP를 포함하고, 기존 장비 호환을 위해 TKIP도 함께 다룬다. 따라서 TKIP와 CCMP 방식을 지원한다는 설명은 맞다.

④ O
WPA2는 AES를 기반으로 하는 CCMP를 사용한다. 따라서 WPA2가 AES 암호 알고리즘을 이용한다는 설명은 맞다.

오답 포인트

TKIP와 WPA를 한 덩어리로 외우면 ①처럼 "WPA의 취약점 보완 기술"로 잘못 연결하기 쉽다. 실제 출제 포인트는 TKIP가 무엇을 고치기 위해 등장했는지, 즉 대상이 WEP인지 WPA인지의 구분이다.

다시 나오면 이렇게 판단

무선랜 보안 선지는 먼저 세대를 나누어 판단한다. WEP의 약점을 임시 보완한 것은 WPA의 TKIP이고, WPA2의 본격 보안 방식은 AES 기반 CCMP라는 축으로 정리하면 빠르게 판별된다.

암기 포인트

TKIP는 WEP 보완, WPA2는 AES-CCMP이다.

NoteBase

문 16. 스택 버퍼 오버플로우 공격에 대한 방어 기법으로 옳지 않은 것은?

① Stack Guard

② ASLR(Address Space Layout Randomization)

③ Stack Shield

④ Stack Frame

정답 4번

출제 포인트

스택 버퍼 오버플로우 방어 기법과 단순한 스택 구조 개념을 구별하는 문제이다.

핵심 개념

Stack Guard는 버퍼와 복귀 주소 사이에 카나리를 두어 덮어쓰기를 탐지하는 방어 기법이다.
ASLR은 스택, 힙, 라이브러리 등의 주소 배치를 무작위화하여 공격자가 정확한 위치를 예측하기 어렵게 하는 방어 기법이다.
Stack Shield는 복귀 주소 변조를 막거나 탐지하도록 설계된 스택 보호 기법이다.
Stack Frame은 함수 호출마다 생성되는 스택의 실행 단위 구조로서 지역 변수, 매개변수, 복귀 주소 등을 담는 개념이다.

선지별 해설

① O: Stack Guard는 스택 카나리 값을 이용해 버퍼 오버플로우로 복귀 주소가 훼손되었는지 검사하므로 대표적인 방어 기법이다.
② O: ASLR은 메모리 배치를 무작위화하여 공격 코드가 복귀 주소나 셸코드 위치를 정확히 맞히기 어렵게 하므로 방어 기법에 해당한다.
③ O: Stack Shield는 스택의 복귀 주소 보호를 통해 버퍼 오버플로우 악용을 막는 기법이므로 방어 기법으로 보는 것이 맞다.
④ X: 틀린 부분은 "방어 기법"이다. Stack Frame은 방어 기법이 아니라 함수 호출 시 만들어지는 스택 구조 단위이다.

오답 포인트

보기 이름에 모두 Stack이 들어가므로 ④도 보호 기술처럼 보이기 쉽다. 그러나 Frame은 보호 기능이 아니라 스택 메모리의 구성 단위를 가리키는 일반 구조 용어이다.

NoteBase

다시 나오면 이렇게 판단

용어가 실제로 공격을 탐지하거나 주소 예측을 어렵게 만들어 악용을 막는 기능을 하면 방어 기법이고, 메모리의 구성이나 호출 구조 자체를 설명하면 방어 기법이 아니다.

암기 포인트

Guard, Shield, ASLR은 방어이고 Frame은 구조이다.

NoteBase

문 17. IDS(Intrusion Detection System)에 대한 설명으로 옳지 않은 것은?

① 비정상행위(Anomaly) 침입탐지는 오용(Misuse) 침입탐지 대비 낮은 오탐률을 보이지만 알려지지 않은 새로운 공격에 취약하다.

② 호스트 기반 IDS는 트로이목마, 백도어, 내부자에 의한 공격을 탐지할 수 있다.

③ '외부망 Ⓐ↔ 라우터 Ⓑ↔ 내부망'으로 구성된 네트워크에서 네트워크 기반 IDS를 Ⓐ 위치에 설치할 경우, Ⓑ 위치에 설치할 경우보다 이론적으로 더 많은 네트워크 공격을 탐지할 수 있지만 처리할 데이터가 더 많다는 단점이 있다.

④ IDS 설계 시 침입자의 행동을 엄격하게 정의할수록 공격탐지의 부정오류(False Negative)가 증가한다.

정답 1번

출제 포인트

이 문제는 IDS의 탐지 방식, 설치 위치, 탐지 기준 엄격도에 따른 특성을 구별할 수 있는지를 묻는다.

핵심 개념

오용 침입탐지는 알려진 공격 패턴과 일치하는지를 찾는 방식이므로 알려진 공격에는 정확도가 높지만 새로운 공격 탐지에는 약하다.
비정상행위 침입탐지는 정상 행위 기준에서 벗어나는지를 찾는 방식이므로 알려지지 않은 공격도 탐지할 수 있지만 오탐률이 높아지기 쉽다.
호스트 기반 IDS는 개별 시스템의 로그, 파일, 프로세스 변화를 보고 탐지하고, 네트워크 기반 IDS는 네트워크 구간을 지나는 트래픽을 보고 탐지한다.

선지별 해설

1번: X. 틀린 표현은 '낮은 오탐률'과 '알려지지 않은 새로운 공격에 취약하다'이다. 비정상행위 침입탐지는 정상 기준에서 벗어난 행위를 잡는 방식이어서 오용 침입탐지보다 오탐률이 높아지기 쉽고, 오히려 알려지지 않은 새로운 공격 탐지에 강점이 있다. 올바르게는 '비정상행위 침입탐지는 오용 침입탐지보다 오탐률이 높지만 알려지지 않은 새로운 공격 탐지에 유리하다'이다.
2번: O. 호스트 기반 IDS는 시스템 로그, 파일 무결성, 프로세스, 계정 사용 흔적을 직접 보므로 트로이목마, 백도어, 내부자에 의한 오남용 공격을 탐지할 수 있다.
3번: O. A 위치는 라우터 바깥쪽이므로 내부망으로 들어오기 전의 더 많은 트래픽을 본다. 따라서 B 위치보다 더 많은 네트워크 공격 시도를 이론적으로 포착할 수 있지만, 그만큼 처리해야 할 데이터와 불필요한 외부 트래픽도 많아진다.
4번: O. IDS의 침입 기준을 너무 엄격하게 잡으면 침입으로 인정되는 경우가 줄어들어 실제 공격을 놓치는 부정오류가 증가할 수 있다. 반대로 기준을 느슨하게 잡으면 정상 행위를 공격으로 보는 오탐이 늘기 쉽다.

NoteBase

오답 포인트

비정상행위 탐지와 오용 탐지의 장단점을 서로 뒤바꾸면 틀리기 쉽다. 특히 '새로운 공격 탐지'는 비정상행위 탐지의 장점이고, '오탐률이 낮다'는 오용 탐지 쪽 특징에 가깝다.

다시 나오면 이렇게 판단

먼저 탐지 방식이 패턴 일치형인지 정상 기준 이탈형인지 구분한다. 다음으로 센서가 호스트를 보는지 네트워크 구간을 보는지 확인한다. 마지막으로 기준이 엄격해질수록 놓침은 늘고, 기준이 느슨해질수록 오탐은 늘어난다는 상충관계를 적용하면 된다.

암기 포인트

오용 탐지는 알려진 패턴에 강하고, 비정상행위 탐지는 새로운 공격 탐지에 강하다. 기준이 엄격하면 부정오류가 늘고, 느슨하면 오탐이 늘어난다.

NoteBase

문 18. 리눅스 사용자 user02의 현재 패스워드 유효기간을 60일로 지정하는 명령어는?

① passwd -l 60 user02

② passwd -w 60 user02

③ chage -M 60 user02

④ chage -W 60 user02

정답 3번

출제 포인트

이 문제는 리눅스에서 passwd와 chage 명령의 옵션 중 비밀번호 최대 사용 기간을 설정하는 옵션을 구별하는지를 묻는다.

핵심 개념

passwd는 비밀번호 설정, 잠금, 경고일수 같은 계정 속성을 다루는 명령이고, chage는 비밀번호 만료 정책을 관리하는 명령이다.
`-M`은 최대 사용 일수, `-W`와 `-w`는 만료 전 경고 일수, `-l`은 잠금 기능이다.

선지별 해설

1번 X: `passwd -l`의 `-l`은 계정의 비밀번호를 잠그는 옵션이므로 유효기간 60일을 지정하는 기능이 아니다. 틀린 표현은 `-l 60`이다. 올바르게는 잠금은 `passwd -l user02`이고, 최대 사용 기간 60일 지정은 `chage -M 60 user02`이다.
2번 X: `passwd -w 60 user02`의 `-w`는 비밀번호 만료 전에 60일 동안 경고하도록 설정하는 옵션이다. 틀린 표현은 `현재 패스워드 유효기간`이다. 올바르게는 경고 일수 설정이며, 최대 사용 기간 설정은 `chage -M 60 user02`이다.
3번 O: `chage -M 60 user02`의 `-M`은 비밀번호의 최대 사용 일수를 뜻하므로 현재 비밀번호 유효기간을 60일로 지정하는 명령이 맞다.
4번 X: `chage -W 60 user02`의 `-W`도 만료 전 경고 일수를 뜻하므로 유효기간 60일 설정 명령이 아니다. 틀린 표현은 `-W 60`을 유효기간으로 본 부분이다. 올바르게는 만료 60일 전에 경고를 주는 설정이다.

오답 포인트

이 문항은 `M`과 `W/w`, `l`의 의미를 바꿔 기억하면 틀리도록 만든 문제이다. 특히 chage의 `-M`은 Max days이고, `-W`와 passwd의 `-w`는 Warning days라는 점이 핵심 함정이다.

NoteBase

다시 나오면 이렇게 판단

먼저 명령이 기간 정책 관리용인지 확인하고, 그다음 옵션 문자의 의미를 대응시키면 된다. 최대 사용 기간이면 `M`, 만료 전 경고면 `W` 또는 `w`, 잠금이면 `l`로 판단하면 된다.

암기 포인트

비밀번호 유효기간은 `chage -M`, 만료 경고는 `-W` 또는 `passwd -w`, 잠금은 `passwd -l`이다.

NoteBase

문 19. 데이터베이스 암호화 방식에 대한 설명으로 옳지 않은 것은?

① Plug-In 방식은 구축 시 일부 응용프로그램 수정이 필요할 수 있으며 DB 성능에 대한 검토가 필요하다.

② Hybrid 방식은 일반적으로 Plug-In 방식과 TDE(Transparent Data Encryption) 방식이 조합된 것이다.

③ API 방식은 응용프로그램 서버에 설치하는 방식으로써 응용프로그램의 수정이 필요하다.

④ TDE 방식은 DBMS 내부 또는 옵션으로 제공되는 암호화 기능을 이용한다.

정답 2번

출제 포인트

이 문제는 데이터베이스 암호화 방식인 API 방식, Plug-In 방식, TDE 방식, Hybrid 방식의 구현 위치와 특징을 구별하는 문제이다.

핵심 개념

API 방식은 응용프로그램에서 암·복호화 API를 호출하는 방식이므로 응용프로그램 수정이 필요하다.
Plug-In 방식은 DB 서버 쪽에 암호화 모듈을 붙이는 방식으로 구축 방식에 따라 일부 응용프로그램 수정과 성능 검토가 필요할 수 있다.
TDE 방식은 DBMS 내부 또는 옵션 기능을 이용해 데이터 파일 단위 암호화를 제공하는 방식이다.
Hybrid 방식은 일반적으로 API 방식과 Plug-In 방식의 장점을 조합하는 방식으로 설명된다.

선지별 해설

① O
Plug-In 방식은 DB 서버에 암호화 모듈을 설치해 처리하는 방식이다. 구축 환경에 따라 일부 응용프로그램 수정이 필요할 수 있고, DB 서버 부하와 성능 영향에 대한 검토가 필요하므로 옳은 설명이다.

② X
틀린 부분은 'Plug-In 방식과 TDE 방식이 조합'이다. Hybrid 방식은 일반적으로 API 방식과 Plug-In 방식을 조합한 형태로 설명된다. 따라서 Plug-In 방식과 TDE 방식의 조합이라고 한 이 선지가 옳지 않다.

③ O
API 방식은 응용프로그램 서버에서 암호화 API를 호출하도록 구현하는 방식이다. 따라서 응용프로그램 수정이 필요하다는 설명은 옳다.

④ O
TDE(Transparent Data Encryption) 방식은 DBMS 내부 기능이나 옵션으로 제공되는 암호화 기능을 이용하는 방식이다. 응용프로그램에는 비교적 투명하게 적용된다는 점이 특징이므로 옳은 설명이다.

NoteBase

오답 포인트

Hybrid라는 이름 때문에 아무 방식이나 섞은 것으로 생각하면 ②를 지나치기 쉽다. 이 문제에서는 Hybrid를 API 방식과 Plug-In 방식의 조합으로 잡아야 한다.

다시 나오면 이렇게 판단

DB 암호화 방식은 암호화 처리가 어디서 일어나는지로 구분한다. API는 응용프로그램, Plug-In은 DB 서버 모듈, TDE는 DBMS 내부 기능, Hybrid는 API와 Plug-In 조합으로 판단한다.

암기 포인트

DB 암호화 방식은 API-응용프로그램 수정, Plug-In-DB 서버 모듈, TDE-DBMS 내부 기능, Hybrid-API+Plug-In으로 정리한다.

NoteBase

문 20. 섹터의 크기가 512바이트이고, 4개의 섹터로 구성된 하나의 클러스터에 600바이트 크기의 데이터 파일이 저장되어 있을 때, RAM 슬랙의 크기[바이트]와 파일 슬랙의 크기[바이트]를 바르게 연결한 것은?

① RAM 슬랙의 크기: 424, 파일 슬랙의 크기: 1024

② RAM 슬랙의 크기: 424, 파일 슬랙의 크기: 1448

③ RAM 슬랙의 크기: 1024, 파일 슬랙의 크기: 424

④ RAM 슬랙의 크기: 1024, 파일 슬랙의 크기: 1448

정답 2번

출제 포인트

이 문제는 섹터 크기, 클러스터 크기, 파일 크기를 이용해 RAM 슬랙과 파일 슬랙을 구분하여 계산하는 문제이다.

조건 정리

- 섹터 크기: 512바이트
- 클러스터 크기: 4섹터 = 2048바이트
- 파일 크기: 600바이트
- RAM 슬랙: 파일이 끝난 마지막 사용 섹터의 남은 공간이다.
- 파일 슬랙: 할당된 클러스터에서 실제 파일 데이터를 제외하고 남은 전체 공간이다.

사용할 공식

RAM 슬랙은 마지막으로 사용한 섹터의 남은 바이트 수이므로 512 - 마지막 섹터에 기록된 데이터 크기로 구한다.
파일 슬랙은 할당된 클러스터의 전체 크기에서 실제 파일 크기를 뺀 값이므로 $2048 - 600$으로 구한다.
이 공식을 쓰는 이유는 600바이트 파일이 1개 클러스터를 할당받되, 두 번째 섹터 중 일부까지만 사용하고 끝나기 때문이다.

계산 과정

1. 600바이트 파일은 첫 번째 섹터 512바이트를 모두 쓰고, 두 번째 섹터에 88바이트를 더 쓴다.
2. RAM 슬랙은 두 번째 섹터의 남은 공간이므로 $512 - 88 = 424$바이트이다.
3. 클러스터 전체는 2048바이트이므로 파일 슬랙은 $2048 - 600 = 1448$바이트이다.
4. 이때 드라이브 슬랙은 남은 두 개 섹터이므로 $2 \times 512 = 1024$바이트이고, 파일 슬랙은 $424 + 1024 = 1448$바이트이다.

NoteBase

선지별 해설

① X: RAM 슬랙 424바이트는 맞지만, 파일 슬랙 1024바이트는 틀리다. 1024바이트는 남은 두 섹터의 드라이브 슬랙만 뜻한다. 파일 슬랙은 RAM 슬랙까지 포함하므로 올바르게는 1448바이트이다.
② O: RAM 슬랙 424바이트, 파일 슬랙 1448바이트로 둘 다 맞다. 따라서 정답에 해당한다.
③ X: 1024바이트는 RAM 슬랙이 아니라 드라이브 슬랙이다. RAM 슬랙은 마지막 사용 섹터의 남은 공간이므로 424바이트이다. 파일 슬랙도 424바이트가 아니라 클러스터 전체 남는 공간 1448바이트이다.
④ X: 파일 슬랙 1448바이트는 맞지만, RAM 슬랙 1024바이트는 틀리다. 1024바이트는 마지막 섹터의 남은 공간이 아니라 마지막 섹터 뒤에 통째로 비어 있는 두 섹터의 크기이다. 올바르게는 RAM 슬랙이 424바이트이다.

오답 포인트

RAM 슬랙과 파일 슬랙을 같은 개념으로 보면 1024바이트를 그대로 파일 슬랙으로 고르기 쉽다. 이 문항은 마지막 사용 섹터 내부의 남은 공간과, 그 뒤에 남은 클러스터 공간 전체를 구분하는지를 묻는다.

다시 나오면 이렇게 판단

슬랙 문제는 먼저 파일이 몇 번째 섹터에서 끝나는지를 계산한다. 그다음 RAM 슬랙은 마지막 사용 섹터의 남은 공간으로 구하고, 파일 슬랙은 할당된 클러스터 크기에서 실제 파일 크기를 뺀 값으로 판단한다.

암기 포인트

RAM 슬랙은 마지막 사용 섹터의 남은 공간이고, 파일 슬랙은 클러스터 전체에서 실제 파일을 제외한 남는 공간이다.

NoteBase

문 21. ISMS-P(정보보호 및 개인정보보호 관리체계 인증)의 보호대책 요구사항에 해당되지 않는 분야는?

① 정책, 조직, 자산 관리

② 외부자 보안

③ 개인정보 제공 시 보호 조치

④ 접근통제

정답 3번

출제 포인트

이 문제는 ISMS-P 인증기준에서 보호대책 요구사항에 속하는 분야와 개인정보 처리 단계별 요구사항에 속하는 분야를 구분할 수 있는지를 묻는다.

핵심 개념

보호대책 요구사항은 조직이 정보보호를 위해 갖추어야 할 통제 영역을 묶은 분류이다.
개인정보 처리 단계별 요구사항은 개인정보의 수집, 이용, 제공, 파기 등 처리 단계에서 지켜야 할 보호조치를 묶은 분류이다.
따라서 '정책, 조직, 자산 관리', '외부자 보안', '접근통제'는 보호대책 요구사항 쪽이고, '개인정보 제공 시 보호 조치'는 개인정보 처리 단계별 요구사항 쪽이다.

선지별 해설

1번: O. '정책, 조직, 자산 관리'는 보호대책 요구사항의 분야에 해당한다. 조직의 보안 정책 수립, 역할과 책임, 자산 식별과 관리 같은 기본 통제를 다루는 영역이므로 맞는 선지이다.
2번: O. '외부자 보안'은 보호대책 요구사항에 포함되는 분야이다. 외부 인력이나 외부자와 관련된 보안 통제를 다루므로 보호대책 요구사항으로 분류한다.
3번: X. 틀린 부분은 '보호대책 요구사항'이다. '개인정보 제공 시 보호 조치'는 보호대책 요구사항이 아니라 개인정보 처리 단계별 요구사항에 해당한다.
4번: O. '접근통제'는 보호대책 요구사항의 대표적인 분야이다. 사용자와 시스템의 접근 권한을 제한하고 통제하는 영역이므로 맞는 선지이다.

오답 포인트

ISMS-P는 큰 틀에서 '보호대책 요구사항'과 '개인정보 처리 단계별 요구사항'이 함께 나오므로, 개인정보라는 단어가 들어간 항목을 모두 보호대책으로 오인하기 쉽다. 3번은 '개인정보 제공'이라는 처리 단계 표현을 보호대책 분야처럼 섞어 놓은 점이 함정이다.

NoteBase

다시 나오면 이렇게 판단

선지에 정책, 자산, 접근권한, 외부자 관리처럼 보안 통제 영역명이 나오면 먼저 보호대책 요구사항을 떠올린다. 반대로 수집, 이용, 제공, 파기처럼 개인정보 처리 행위의 단계가 직접 나오면 개인정보 처리 단계별 요구사항으로 판단한다.

암기 포인트

보호대책은 통제 영역, 개인정보 수집·이용·제공·파기는 처리 단계라는 구분이 핵심이다.

NoteBase

문 22. 「개인정보 보호법」상 개인정보처리자가 개인정보의 수집 및 이용 동의를 받을 때 정보주체에게 알릴 의무가 있는 사항이 아닌 것은?

① 개인정보를 제공받는 자

② 동의 거부 시 불이익이 있을 경우 그 불이익 내용

③ 수집하려는 개인정보의 항목

④ 개인정보의 보유 및 이용 기간

정답 1번

쟁점

이 문제는 개인정보 수집·이용 동의 시 고지사항과 제3자 제공 동의 시 고지사항을 구별하는 문제이다. 핵심은 수집·이용 동의에서는 목적·항목·보유 및 이용 기간·거부권 및 불이익을 알리고, "개인정보를 제공받는 자"는 제3자 제공 동의에서 문제된다는 점이다.

용어 풀이

개인정보의 수집·이용 동의는 개인정보처리자가 자신의 업무 목적을 위해 개인정보를 모아 사용하는 데 대한 동의이다.
개인정보의 제공 동의는 수집한 개인정보를 제3자에게 넘기는 데 대한 별도의 동의이다.

핵심 구분

원칙적으로 개인정보의 수집·이용 동의를 받을 때에는 수집·이용 목적, 수집하려는 개인정보의 항목, 보유 및 이용 기간, 동의 거부권 및 불이익을 알린다. 반면 개인정보를 제공받는 자는 제3자 제공 동의를 받을 때 고지하는 사항이다. 수집·이용과 제공은 동의 구조 자체가 다르므로, 제공받는 자가 보이면 제3자 제공 동의 영역으로 구분된다.

NoteBase

선지별 해설

① X
- "개인정보를 제공받는 자"는 제3자 제공 동의에서 알릴 사항이지, 수집·이용 동의에서 알릴 사항이 아니다.
- 틀린 표현: 개인정보를 제공받는 자
- 올바른 표현: 수집·이용 동의에서는 개인정보의 수집·이용 목적, 수집 항목, 보유 및 이용 기간, 동의 거부권 및 불이익을 알린다.

② O
- 동의를 거부할 권리가 있다는 사실과, 거부에 따른 불이익이 있으면 그 불이익의 내용을 알려야 하므로 옳다.

③ O
- 수집하려는 개인정보의 항목은 수집·이용 동의의 기본 고지사항이므로 옳다.

④ O
- 개인정보의 보유 및 이용 기간은 수집·이용 동의 시 반드시 알려야 하는 사항이므로 옳다.

오답 포인트

이 문제를 틀렸다면 수집·이용 동의와 제3자 제공 동의를 한 묶음으로 외운 경우가 많다. 특히 "개인정보를 제공받는 자"는 익숙한 표현이라 수집 단계에도 들어간다고 착각하기 쉽지만, 이는 제공 단계의 고지사항이다.

다시 나오면 이렇게 판단

선지에 "제공받는 자", "제공하는 개인정보", "제공받는 자의 이용 목적" 같은 표현이 보이면 제3자 제공 동의인지부터 구분한다. 수집·이용 동의는 목적·항목·기간·거부권 구조로 판단하고, 제공 동의는 제공받는 자 관련 사항이 추가된 구조로 판단한다.

암기 포인트

수집·이용은 목적·항목·기간·거부권이고, 제공은 제공받는 자를 본다.

NoteBase

문 23. ISO 27001에 대한 설명으로 옳지 않은 것은?

① 영국의 BSI(British Standards Institute)에서 제정한 BS 7799를 기반으로 구성되어 있는 보안 프레임워크이다.

② ISO 27001:2013은 7개의 관리과정으로 구성되어 있으며, 정보보호 통제 요구사항은 10개 영역, 114개 통제 항목으로 구성되어 있다.

③ ISO 27001:2013의 관리과정을 PDCA 모델에 적용할 때, 조치(Act)에 해당하는 항목은 개선(Improvement)이다.

④ ISO 27001에서 제시한 프레임워크에 따라 조직의 위험을 관리하고 이를 개선해나가는 체계를 갖추더라도 보안 침해는 발생할 수 있다.

정답 2번

출제 포인트

이 문항은 ISO 27001:2013의 관리체계 본문 구조와 Annex A 통제영역 수를 정확히 구별하는지를 묻는 문제이다.

핵심 개념

ISO 27001은 정보보호관리체계(ISMS) 요구사항 표준이다. 2013판의 본문 요구사항은 4장부터 10장까지의 7개 관리 조항으로 운영되며, Annex A의 정보보호 통제는 14개 영역 114개 통제로 정리된다. PDCA로 보면 Act는 개선에 해당하고, ISMS는 위험을 줄이는 체계이지 사고를 0으로 보장하는 체계는 아니다.

NoteBase

선지별 해설

① O
BS 7799 계열 표준이 ISO/IEC 27001의 출발점이 되었으므로 맞는 설명이다. 영국 BSI가 만든 BS 7799를 바탕으로 정보보호관리체계 표준이 국제표준으로 발전하였다.

② X
틀린 부분은 "10개 영역"이다. ISO 27001:2013의 Annex A 통제는 10개 영역이 아니라 14개 영역, 114개 통제로 구성된다. 본문 요구사항을 7개 관리 조항으로 보는 설명은 가능하지만, 통제영역 수를 10개로 적은 부분이 오답이다.

③ O
ISO 27001:2013을 PDCA에 대응시키면 Act는 개선에 해당한다. 개선은 시정조치와 지속적 개선을 포함하는 단계이므로 조치(Act)에 해당한다.

④ O
ISO 27001은 조직이 위험을 식별, 평가, 처리하고 지속적으로 개선하도록 요구하지만, 보안 침해 자체를 완전히 없애는 표준은 아니다. 잔여위험이 남을 수 있으므로 체계를 갖추고도 사고는 발생할 수 있다.

오답 포인트

수험생이 가장 많이 헷갈리는 지점은 관리 조항 수와 Annex A 통제영역 수를 뒤섞는 것이다. 특히 ②처럼 "7개 관리 조항"이라는 맞는 정보 옆에 "10개 영역"이라는 틀린 숫자를 붙여 놓으면 전체를 맞는 설명으로 오인하기 쉽다.

다시 나오면 이렇게 판단

ISO 27001 문제는 먼저 본문 요구사항과 Annex A 통제를 분리해서 본다. 숫자가 나오면 본문은 7개 관리 조항, Annex A는 14개 영역 114개 통제라는 축으로 대조하면 빠르게 판단할 수 있다. 또 ISMS는 위험 감소 체계이지 무사고 보장 체계가 아니라는 점을 함께 확인하면 ④ 같은 선지도 흔들리지 않는다.

암기 포인트

2013판은 본문 7개 관리 조항, Annex A 14개 영역 114개 통제, Act는 Improvement이다.

NoteBase

문 24. CC(Common Criteria)에서 사용하는 EAL(Evaluation Assurance Level)과 설계, 시험 및 검토 수준을 짝 지은 것으로 옳은 것은?

① EAL 1 - 구조적 시험 (structurally tested)

② EAL 3 - 방법론적 설계, 시험과 검토 (methodically designed, tested, and reviewed)

③ EAL 5 - 준정형적 설계와 시험 (semiformally designed and tested)

④ EAL 6 - 정형적으로 검증된 설계와 시험 (formally verified design and tested)

정답 3번

출제 포인트

이 문제는 CC의 EAL 단계별 공식 명칭을 정확히 대응시키는지를 묻는 문제이다.

핵심 개념

EAL은 보증 수준이 올라갈수록 functionally tested → structurally tested → methodically tested and checked → methodically designed, tested, and reviewed → semi-formally designed and tested → semi-formally verified design and tested → formally verified design and tested 순으로 엄격해진다. EAL1은 기능적 시험, EAL2는 구조적 시험, EAL3은 방법론적 시험과 점검, EAL4는 방법론적 설계·시험·검토, EAL5는 준정형적 설계와 시험, EAL6는 준정형적으로 검증된 설계와 시험, EAL7은 정형적으로 검증된 설계와 시험이다.

선지별 해설

① X: 틀린 부분은 "EAL 1 - 구조적 시험"이다. EAL1은 structurally tested가 아니라 functionally tested이므로 올바르게는 "EAL 1 - 기능적 시험"이다.
② X: 틀린 부분은 "방법론적 설계, 시험과 검토"이다. 이는 EAL4의 명칭에 해당한다. EAL3은 methodically designed, tested, and reviewed가 아니라 methodically tested and checked이므로 올바르게는 "EAL 3 - 방법론적 시험과 점검"이다.
③ O: EAL5는 semi-formally designed and tested로, 준정형적 설계와 시험에 해당한다. EAL4보다 높은 수준이지만 EAL6처럼 검증된 설계 단계까지 포함하는 수준은 아니다.
④ X: 틀린 부분은 "정형적으로 검증된 설계와 시험"이다. EAL6는 formally verified가 아니라 semi-formally verified design and tested이므로 올바르게는 "EAL 6 - 준정형적으로 검증된 설계와 시험"이다. "정형적으로 검증된 설계와 시험"은 EAL7에 해당한다.

NoteBase

오답 포인트

EAL3과 EAL4는 tested and checked와 designed, tested, and reviewed를 서로 바꾸어 내기 쉽고, EAL5와 EAL6은 designed와 verified를 바꾸어 내기 쉽다. 특히 ④처럼 "정형적"과 "준정형적"을 한 단계씩 밀어 놓으면 암기만 한 경우 쉽게 흔들린다.

다시 나오면 이렇게 판단

EAL 번호를 보면 먼저 핵심 동사를 대응시켜 판단한다. 1은 functionally, 2는 structurally, 3은 tested and checked, 4는 designed/tested/reviewed, 5는 semi-formally designed, 6는 semi-formally verified, 7은 formally verified로 끊어 보면 선지의 오답 표현이 바로 드러난다.

암기 포인트

EAL 1 기능, 2 구조, 3 점검, 4 설계·검토, 5 준정형 설계, 6 준정형 검증, 7 정형 검증이다.

NoteBase

문 25. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상 정보통신서비스 제공자는 서비스 제공을 위해 이용자의 이동통신단말장치 내에 저장되어 있는 정보 및 이동통신단말장치에 설치된 기능에 대하여 접근할 수 있는 권한이 필요한 경우 이용자의 동의를 받도록 하고 있다. 이에 대한 사항으로 옳은 것은?

① 해당 서비스를 제공하기 위하여 반드시 필요한 접근권한인 경우, 접근권한 허용에 대하여 동의하지 아니할 수 있다는 사실을 알리고 동의를 받아야 한다.

② 접근권한이 필요한 정보는 알리고 동의를 받아야 하지만 접근권한이 필요한 이유는 알릴 필요가 없다.

③ 접근권한의 범위 및 동의의 방법은 대통령령으로 정한다.

④ 이용자 정보 보호를 위하여 필요한 조치 및 그 밖에 필요한 사항은 과학기술정보통신부령으로 정한다.

정답 3번

쟁점

이 문제는 이동통신단말장치 접근권한에 관한 동의사항과 세부사항의 위임 형식을 구별하는 문제이다.
핵심은 반드시 필요한 접근권한과 반드시 필요하지 않은 접근권한의 고지사항 차이, 그리고 세부사항이 대통령령 사항인지 부령 사항인지 구별하는 데 있다.

용어 풀이

접근권한 = 정보통신서비스 제공자가 이용자의 이동통신단말장치에 저장된 정보나 설치된 기능에 접근할 수 있는 권한이다.

핵심 구분

원칙적으로 접근권한이 필요하면 이용자에게 필요한 정보 및 기능의 항목과 그 이유를 알리고 동의를 받아야 한다. 다만 접근권한 허용에 동의하지 아니할 수 있다는 사실은 반드시 필요한 접근권한이 아닌 경우에만 추가로 고지한다.
또한 접근권한의 범위, 동의의 방법, 이용자 정보 보호를 위한 필요한 조치 등 세부사항은 대통령령으로 정한다.

NoteBase

선지별 해설

① X
- "동의하지 아니할 수 있다는 사실"은 반드시 필요한 접근권한이 아닌 경우에 고지하는 사항이다. 반드시 필요한 접근권한에 대해서까지 그 사실을 알리도록 한 것은 틀리다.
- 틀린 표현: "반드시 필요한 접근권한인 경우 … 동의하지 아니할 수 있다는 사실을 알리고"
- 올바른 표현: 반드시 필요한 접근권한인 경우에는 필요한 정보 및 기능의 항목과 그 이유를 알리고 동의를 받는다.

② X
- 법은 접근권한이 필요한 정보 및 기능의 항목뿐 아니라 접근권한이 필요한 이유도 함께 알리도록 한다. 이유는 알릴 필요가 없다는 부분이 틀리다.
- 틀린 표현: "접근권한이 필요한 이유는 알릴 필요가 없다"
- 올바른 표현: 접근권한이 필요한 정보 및 기능의 항목과 접근권한이 필요한 이유를 모두 알려야 한다.

③ O
- 법은 접근권한의 범위 및 동의의 방법을 대통령령으로 정한다고 둔다. 선지는 위임 형식을 정확하게 적었다.

④ X
- 이용자 정보 보호를 위하여 필요한 조치 및 그 밖에 필요한 사항도 대통령령으로 정한다.
과학기술정보통신부령으로 정한다는 부분이 틀리다.
- 틀린 표현: "과학기술정보통신부령으로 정한다"
- 올바른 표현: 대통령령으로 정한다.

오답 포인트

이 문제를 틀렸다면 ①의 "반드시 필요한 접근권한"과 "반드시 필요하지 않은 접근권한"의 고지사항을 뒤섞었거나, ④의 대통령령과 부령을 혼동했을 가능성이 높다. 특히 "동의하지 아니할 수 있다는 사실"은 임의적 접근권한에만 붙는 문구라는 점이 함정이다.

다시 나오면 이렇게 판단

접근권한 문제는 먼저 반드시 필요한 권한인지 아닌지부터 나눈다. 그다음 고지사항에 "항목", "이유", "동의 거부 가능 사실"이 각각 어디까지 붙는지 확인하고, 마지막으로 세부 위임 형식이 대통령령인지 부령인지 판별하면 된다.

암기 포인트

접근권한은 항목·이유 고지, 거부 가능 사실은 선택권한, 세부 위임은 대통령령이다.

NoteBase