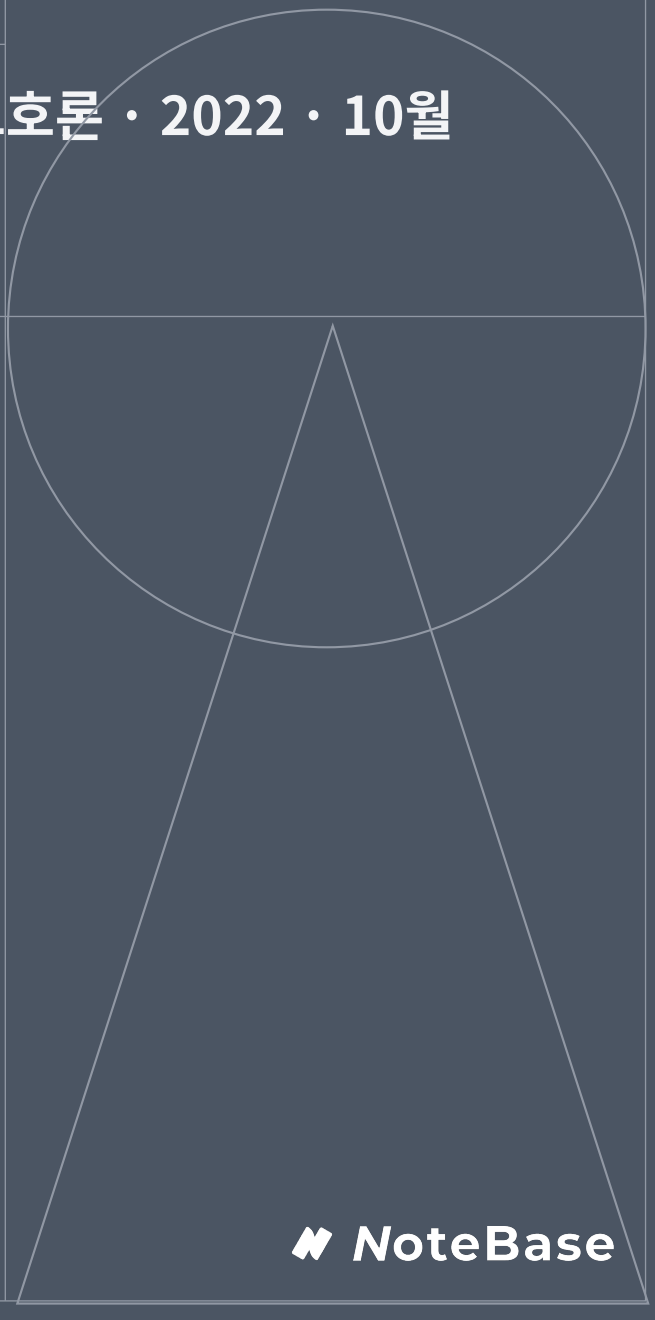
# 기출OX 해설집

공무원/서울시/7급 · 정보보호론 · 2022 · 10월



NoteBase

# 기출OX 해설집

## 공무원/서울시/7급 · 정보보호론 · 2022 · 10월

**공무원/서울시/7급 · 정보보호론 · 2022 · 10월**

**문 1. 블록암호 알고리즘 중 보안강도가 가장 높은 것은?**

① DES

② AES-192

③ 3TDEA

④ HIGHT

**정답 2번**

**출제 포인트**

이 문제는 블록암호의 보안강도를 키 길이와 실제 유효 보안수준으로 비교할 수 있는지를 묻는다.

**핵심 개념**

DES는 56비트 키를 사용하는 구형 블록암호이다.
AES-192는 192비트 키를 사용하는 AES 계열 블록암호이다.
3TDEA는 3중 DES로 명목 키 길이는 168비트이지만 일반적으로 유효 보안강도는 112비트 수준으로 본다.
HIGHT는 경량 블록암호로 128비트 키를 사용한다.
이 문항의 비교축은 블록암호 여부가 아니라 일반적인 키 탐색 기준의 보안강도 크기이다.

**선지별 해설**

1번 X: DES는 56비트 키를 사용하므로 제시된 보기 중 보안강도가 가장 높다고 볼 수 없다. 틀린 표현은 "가장 높은"이다. 올바르게는 "DES는 보기 중 보안강도가 가장 낮은 편이다"이다.
2번 O: AES-192는 192비트 키를 사용하므로 보기 중 가장 높은 보안강도를 가진다. 3TDEA의 실질 보안강도 112비트, HIGHT의 128비트 키보다 크다.
3번 X: 3TDEA는 3중 DES이므로 DES보다 강하지만 일반적으로 유효 보안강도는 112비트 수준으로 평가된다. 틀린 표현은 "가장 높은"이다. 올바르게는 "3TDEA는 DES보다 강하지만 AES-192보다는 낮다"이다.
4번 X: HIGHT는 128비트 키를 사용하는 경량 블록암호이므로 DES보다는 강하지만 AES-192보다 높지 않다. 틀린 표현은 "가장 높은"이다. 올바르게는 "HIGHT의 보안강도는 AES-192보다 낮다"이다.

NoteBase

### 오답 포인트

3TDEA의 명목 키 길이 168비트만 보고 AES-192와 비슷하거나 더 강하다고 오해하기 쉽다. 이 문제는 단순 명목 키 길이가 아니라 실제 유효 보안강도를 함께 보아야 맞힌다.

### 다시 나오면 이렇게 판단

블록암호 보안강도 비교 문제는 먼저 각 알고리즘의 키 길이를 확인하고, 그다음 다중암호처럼 유효 보안강도가 별도로 알려진 예외가 있는지를 본다. 보기 중 AES-192는 192비트, HIGHT는 128비트, 3TDEA는 유효 112비트, DES는 56비트로 정리된다.

### 암기 포인트

DES 56비트, 3TDEA 유효 112비트, HIGHT 128비트, AES-192 192비트이다.

NoteBase

**문 2. ISO/IEC 27001 통제 항목 및 통제 내용에 대한 설명으로 가장 옳지 않은 것은?**

① 운영관리 영역은 정보보호 정책, 정보보호 조직 구성 등을 통제한다.

② 인적자원 보호 영역은 내부 조직, 외부 기업, 고용 전, 고용 기간, 고용 변경 및 종료 등을 통제한다.

③ 접근통제 영역은 접근통제 요구사항, 사용자 접근관리, 사용자 책임, 네트워크 접근, 운영시스템 접근 등을 통제한다.

④ 통신 보안 영역은 네트워크 정보보호 관리, 매체 취급, 정보교환, 전자상거래서비스, 모니터링 등을 통제한다.

**정답 1번**

**출제 포인트**

이 문제는 ISO/IEC 27001의 통제 영역과 각 영역에 속하는 세부 통제 내용을 정확히 대응시키는지를 묻는 문제이다.

**핵심 개념**

정보보호 정책과 정보보호 조직은 운영관리 영역이 아니라 별도의 정책·조직 영역에 속한다.
인적자원 보호는 고용 전·중·변경·종료 과정에서 사람과 관련된 보안 책임을 다루는 영역이다.
접근통제는 접근 요구사항, 사용자 접근관리, 사용자 책임, 네트워크·운영체제 접근 통제를 다루는 영역이다.
통신 및 운영관리 계열은 네트워크 보안 관리, 매체 취급, 정보교환, 전자상거래서비스, 모니터링 같은 운영·통신 관련 통제를 다루는 영역이다.

NoteBase

**기출OX 해설집 · 공무원/서울시/7급 · 정보보호론 · 2022 · 10월**

**선지별 해설**

① X
틀린 부분은 "운영관리 영역은 정보보호 정책, 정보보호 조직 구성 등을 통제한다"는 표현이다.
정보보호 정책과 정보보호 조직은 운영관리 영역이 아니라 각각 정보보호 정책, 정보보호 조직 관련 영역에 해당한다.
올바르게는 운영관리 영역은 운영 절차, 악성코드 대응, 백업, 네트워크 보안 관리, 매체 취급, 정보교환, 모니터링 등 운영 과정의 보안을 통제한다고 이해해야 한다.

② O
인적자원 보호는 내부 인력과 외부 인력에 대해 고용 전, 고용 중, 고용 변경 및 종료 시점의 보안 책임과 통제를 다루므로 서술 취지가 맞다.
핵심 키워드는 사람과 고용 단계이다.

③ O
접근통제 영역은 접근통제 요구사항, 사용자 접근관리, 사용자 책임, 네트워크 접근, 운영시스템 접근 등을 포함하므로 맞는 설명이다.
누가 어떤 자원에 어떤 수준으로 접근할 수 있는지를 관리하는 영역이라는 점이 핵심이다.

④ O
네트워크 정보보호 관리, 매체 취급, 정보교환, 전자상거래서비스, 모니터링은 통신 및 운영관리 계열의 대표 통제 내용이므로 맞는 설명이다.
선지의 명칭 표현은 다소 축약되어 있어도 세부 통제 내용의 대응은 올바르다.

**오답 포인트**

정책·조직에 관한 통제와 운영 과정에 관한 통제를 섞으면 틀리기 쉽다. ①은 "정보보호 정책, 정보보호 조직 구성"이라는 키워드를 운영관리 영역에 붙여 놓은 것이 함정이다.

**다시 나오면 이렇게 판단**

선지에서 제시한 세부 키워드를 먼저 본다. 정책·조직이면 정책 또는 조직 영역, 고용 전·중·종료면 인적자원 보호, 접근 요구사항·사용자 책임이면 접근통제, 네트워크 관리·매체 취급·정보교환·모니터링이면 통신 및 운영관리 계열로 연결하면 된다.

**암기 포인트**

정책·조직은 운영관리가 아니고, 운영관리는 네트워크·매체·정보교환·모니터링이다.

NoteBase

**문 3. XSS(Cross-Site Scripting) 공격에 대한 설명으로 가장 옳지 않은 것은?**

① XSS 공격은 쿠키에 저장된 DBMS의 SQL 구문의 취약점을 공격하는 기법이다.

② Stored XSS는 게시판 또는 자료실과 같이 사용자가 글을 저장하는 부분에 정상적인 평문이 아닌 스크립트 코드를 입력하는 기법이다.

③ Reflected XSS는 웹 애플리케이션에 스크립트를 저장하는 것이 아니라 URL의 변수 부분처럼 스크립트 코드를 입력하는 동시에 결과가 바로 전해지는 공격 기법이다.

④ CSRF 공격은 피해자가 인지하지 못하는 상태에서 피해자의 브라우저가 특정 사이트에 강제적으로 리퀘스트를 보내도록 하는 기법이다.

**정답 1번**

**출제 포인트**

이 문제는 XSS의 실행 위치와 유형(Stored XSS, Reflected XSS), 그리고 SQL Injection 및 CSRF와의 구별을 묻는 문제이다.

**핵심 개념**

XSS는 웹 페이지에 삽입된 악성 스크립트가 피해자의 브라우저에서 실행되도록 만드는 공격이다.
Stored XSS는 악성 스크립트가 게시글, 댓글, 자료실 글처럼 서버에 저장되었다가 이후 열람자에게 전달되는 유형이다.
Reflected XSS는 URL 변수나 요청 파라미터에 포함된 스크립트가 서버 응답에 즉시 반사되어 실행되는 유형이다.
SQL Injection은 서버 측 SQL 질의를 조작하는 공격이고, CSRF는 인증된 사용자의 브라우저로 원치 않는 요청을 보내게 하는 공격이다.

NoteBase

**선지별 해설**

① X
XSS는 SQL 구문의 취약점을 공격하는 기법이 아니라 웹 페이지에 스크립트를 삽입해 브라우저에서 실행되게 하는 기법이다.
틀린 부분은 "쿠키에 저장된 DBMS의 SQL 구문"이다.
올바르게는 "입력창, 게시글, URL 파라미터 등에 삽입된 스크립트가 사용자 브라우저에서 실행되도록 유도하는 공격"이다.

② O
Stored XSS는 게시판이나 자료실처럼 서버에 내용이 저장되는 위치에 악성 스크립트를 삽입해 두었다가 이후 사용자에게 전달하는 공격이므로 설명이 맞다.

③ O
Reflected XSS는 스크립트를 서버에 저장하지 않고 URL 변수, 검색어, 요청 파라미터 등에 포함시킨 뒤 그 값이 응답에 바로 반사되게 하므로 설명이 맞다.

④ O
이 선지는 XSS가 아니라 CSRF를 설명하고 있지만 진술 내용 자체는 맞다. CSRF는 로그인된 사용자의 브라우저가 본인 의사와 무관하게 특정 요청을 보내도록 만드는 공격이다.

**오답 포인트**

①은 XSS를 SQL Injection처럼 바꾸어 놓은 선지이고, ④는 XSS가 아닌 CSRF 설명을 섞어 공격 종류를 혼동하게 만든 선지이다. 브라우저에서 스크립트가 실행되는지, 서버의 SQL 질의가 변조되는지, 인증된 요청이 위조되는지로 구분하면 흔들리지 않는다.

**다시 나오면 이렇게 판단**

웹 공격 문제는 먼저 무엇이 실행되는지와 어디서 악용되는지를 본다. 브라우저에서 악성 스크립트가 실행되면 XSS, 서버의 SQL 질의문이 조작되면 SQL Injection, 로그인 사용자의 요청이 위조되면 CSRF로 판단한다.

**암기 포인트**

XSS는 스크립트 실행, SQL Injection은 질의문 조작, CSRF는 요청 위조가 핵심이다.

NoteBase

**문 4. 다양한 NAC(Network Access Control) 구현 방식에 대한 설명으로 가장 옳지 않은 것은?**

① 802.1x 방식은 802.1x 프로토콜과 RADIUS 서버를 이용하는 것으로, 실질적인 접근 허용이나 차단은 스위치에서 수행하고 신규 클라이언트에 대한 인증 요청은 실제로 인증을 수행하는 RADIUS 서버로 전달한다.

② VLAN 방식은 인가받지 않은 사용자라면 VLAN으로 미리 분리된 망 중에서 통신이 되지 않는 VLAN 망에 신규 클라이언트를 할당한다.

③ ARP 방식은 신규 클라이언트가 적법한 사용자라면 NAC가 게이트웨이의 정상적인 MAC 주소를 알려주고, 그렇지 않은 사용자라면 비정상적인 MAC 주소를 전송하여 네트워크에 대한 접근을 막는다.

④ 소프트웨어 에이전트 설치 방식은 네트워크에 접속하려는 모든 클라이언트에 에이전트를 설치하는 동시에 해당 클라이언트에서 차단 정책을 설정한다.

**정답 4번**

**출제 포인트**

이 문제는 NAC 구현 방식별 제어 지점과 접근 차단 원리를 구별할 수 있는지를 묻는다.

**핵심 개념**

802.1x 방식은 스위치나 AP 같은 인증자가 RADIUS 서버와 연동하여 포트 단위 접근을 통제하는 방식이다.
VLAN 방식은 비인가 단말을 격리 VLAN에 배치하여 정상 업무망과 분리하는 방식이다.
ARP 방식은 게이트웨이의 MAC 주소 정보를 제어하여 비인가 단말의 통신을 막는 방식이다.
소프트웨어 에이전트 설치 방식은 단말에 에이전트를 설치해 보안 상태를 점검하고, 서버 정책에 따라 에이전트를 통해 차단이나 격리를 수행하는 방식이다.

**선지별 해설**

① O: 802.1x NAC는 스위치가 인증자 역할을 하여 실제 포트 접근을 허용하거나 차단하고, 인증 자체는 RADIUS 서버가 수행한다. 선지의 설명은 제어 지점과 인증 주체를 올바르게 구분한다.
② O: VLAN 방식은 비인가 단말을 정상 업무망과 분리된 격리 VLAN이나 제한 VLAN으로 보내 통신 범위를 제한한다. 따라서 인가받지 않은 사용자를 통신이 제한된 VLAN에 할당한다는 설명은 맞다.
③ O: ARP 방식은 단말이 게이트웨이를 잘못 인식하도록 만들어 비인가 단말의 통신을 막는 방식이다. 적법한 사용자에게는 정상 게이트웨이 MAC 주소를 알려 주고, 비인가 사용자에게는 비정상적인 MAC 정보를 주어 접근을 차단한다는 설명이 맞다.
④ X: 틀린 부분은 '해당 클라이언트에서 차단 정책을 설정한다'는 표현이다. 소프트웨어 에이전트 설치 방식은 클라이언트에 에이전트를 설치하는 것은 맞지만, 차단 정책은 서버에서 설정하고 설치된 에이전트를 통해 해당 단말의 접근을 차단하거나 격리한다.

NoteBase

**오답 포인트**

에이전트가 단말에 설치된다는 이유만으로 정책까지 단말에서 설정한다고 보면 틀린다. 이 문항의 함정은 정책 설정 주체인 서버와 정책 집행 수단인 에이전트를 뒤바꿔 놓은 데 있다.

**다시 나오면 이렇게 판단**

NAC 방식은 먼저 어디가 제어 지점인지 보면 된다. 802.1x는 스위치와 RADIUS, VLAN은 격리 VLAN 할당, ARP는 게이트웨이 MAC 제어, 에이전트 방식은 서버 정책과 단말 에이전트의 조합으로 판단하면 된다.

**암기 포인트**

802.1x는 포트 인증, VLAN은 망 분리, ARP는 게이트웨이 MAC 제어, 에이전트 방식은 서버 정책과 단말 에이전트이다.

NoteBase

**문 5. 버퍼 오버플로우 공격을 고려할 때 가장 안전한 C언어 함수는?**

① snprintf( )

② strcpy( )

③ strcat( )

④ gets( )

**정답 1번**

**출제 포인트**

이 문제는 C 문자열 처리 함수들 중 버퍼 길이 검사를 수행하는 함수와 수행하지 않는 함수를 구별하는 문제이다.

**핵심 개념**

snprintf는 출력 버퍼의 최대 길이를 인자로 받아 기록량을 제한하는 포맷 함수이다. 키워드는 길이 인자이다.
strcpy와 strcat는 복사·이어붙이기 과정에서 목적지 버퍼의 남은 크기를 스스로 검사하지 않는 함수이다.
키워드는 경계 검사 부재이다.
gets는 입력 길이 제한을 받지 않고 한 줄을 읽어 버퍼 오버플로우를 쉽게 일으키는 함수이다. 키워드는 사용 금지 수준의 위험성이다.

NoteBase

**선지별 해설**

① O
- snprintf()는 버퍼 크기를 인자로 받아 최대 기록 길이를 제한하므로, 제시된 선택지 중 버퍼 오버플로우 방어 측면에서 가장 안전하다.

② X
- 틀린 부분은 strcpy()를 가장 안전한 함수로 보는 판단이다.
- strcpy()는 원본 문자열 길이를 검사하지 않고 널 문자까지 복사한다.
- 올바르게는 길이 제한이 있는 snprintf()가 더 안전하다.

③ X
- 틀린 부분은 strcat()를 가장 안전한 함수로 보는 판단이다.
- strcat()는 기존 문자열 뒤에 계속 붙이면서도 목적지 버퍼의 남은 공간을 확인하지 않는다.
- 올바르게는 이어붙이기 전에도 길이 한계를 통제할 수 있는 함수가 안전하며, 이 문항에서는 snprintf()가 정답이다.

④ X
- 틀린 부분은 gets()를 안전한 함수로 보는 판단이다.
- gets()는 입력 길이 제한이 전혀 없어 대표적인 버퍼 오버플로우 원인 함수이며, C11에서 제거되었다.
- 올바르게는 문자열 입력은 길이를 제한할 수 있는 fgets() 계열을 사용하고, 제시된 보기 중에서는 snprintf()가 가장 안전하다.

**오답 포인트**

문자열을 다루는 함수라는 공통점만 보고 strcpy, strcat, gets를 같은 수준으로 판단하면 오답이 된다. 이 문제의 함정은 기능 이름이 아니라 길이 인자를 받는지 여부에 있다.

**다시 나오면 이렇게 판단**

버퍼 오버플로우 관련 함수 문제는 먼저 목적지 버퍼 크기를 인자로 명시하는지 확인한다. 길이 인자가 있으면 상대적으로 안전하고, 길이 검사가 없으면 오버플로우 위험 함수로 판단한다.

**암기 포인트**

길이 인자 있으면 안전성 상승, gets·strcpy·strcat는 경계 검사 부재로 위험하다.

NoteBase

**문 6. 생체기반 인증에 대한 설명으로 가장 옳지 않은 것은?**

① FRR은 오거부율을 말하며 시스템에 등록된 사용자 본인의 생체정보를 본인이 아닌 것으로 잘못 판단하여 인증을 거부하는 오류율이다.

② EER은 오인식률과 오거부율이 같아지는 비율을 말하며, EER이 높을수록 인증의 정확도가 높아진다.

③ 생체인식을 위해 이용되는 생체정보를 선택함에 있어서 고려해야 하는 요소인 보편성은 시스템을 이용하는 모든 사람들이 인증하는 데 사용되는 생체정보를 지니고 있어야 함을 의미한다.

④ FAR은 오인식률을 말하며, 시스템이 본인의 것이 아닌 다른 사람의 생체인식 정보를 본인의 것으로 잘못 판단하여 인증을 수락하는 오류율이다.

**정답 2번**

**출제 포인트**

이 문제는 생체인증의 정확도 지표인 FAR, FRR, EER와 생체정보 선택 기준인 보편성의 의미를 정확히 구별하는지를 묻는 문제이다.

**핵심 개념**

FAR는 타인의 생체정보를 본인으로 잘못 받아들이는 비율이고, FRR은 본인의 생체정보를 타인으로 잘못 거부하는 비율이다.
EER은 FAR와 FRR이 같아지는 지점의 오류율이며 값이 낮을수록 성능이 좋다.
보편성은 인증 대상이 되는 거의 모든 사용자가 그 생체특성을 공통적으로 가지고 있어야 한다는 성질이다.

**선지별 해설**

1번 O: FRR은 오거부율이다. 등록된 사용자의 정상적인 생체정보를 시스템이 본인이 아닌 것으로 판단하여 인증을 거부하는 경우이므로 설명이 맞다.
2번 X: EER이란 오인식률과 오거부율이 같아지는 지점의 오류율이라는 앞부분은 맞다. 틀린 부분은 "EER이 높을수록 인증의 정확도가 높아진다"는 표현이다. 실제로는 EER이 낮을수록 두 오류가 모두 작다는 뜻이므로 인증 정확도가 높다.
3번 O: 보편성은 시스템 이용자 대부분이 해당 생체특성을 가지고 있어야 한다는 뜻이다. 모두가 사용할 수 있는 생체정보인가를 보는 기준이므로 설명이 맞다.
4번 O: FAR는 타인의 생체정보를 본인의 것으로 잘못 받아들여 인증을 수락하는 비율이다. 즉 잘못된 수락의 오류율을 말하므로 설명이 맞다.

**오답 포인트**

EER의 정의와 성능 해석을 뒤집으면 틀린다. 수험생은 "같아지는 비율"이라는 정의만 기억하고 값의 방향성을 놓치기 쉬운데, EER은 낮을수록 우수하다는 점까지 함께 기억해야 한다.

NoteBase

**다시 나오면 이렇게 판단**

생체인증 지표 문제는 먼저 FAR가 잘못된 수락인지, FRR이 잘못된 거부인지 구분한 뒤, EER은 두 오류가 만나는 지점이며 값이 낮을수록 성능이 좋다는 순서로 판단하면 된다.

**암기 포인트**

FAR는 남을 받아들인 오류, FRR은 본인을 거부한 오류, EER은 낮을수록 우수한 지표이다.

NoteBase

**문 7. 접근통제 모델에 대한 설명으로 가장 옳은 것은?**

① Bell-LaPadula 모델에서 낮은 보안 수준의 권한을 가진 사람이 자신의 권한보다 높은 보안 수준을 가진 문서에 대해 쓰기가 불가능하다.

② Bell-LaPadula 모델은 보다 신뢰할 수 있는 정보, 즉 정보의 무결성을 높이는 데 목적이 있는 경우 사용된다.

③ Biba 모델에서는 낮은 무결성 수준의 권한을 가진 사람이 자신의 권한보다 높은 무결성 수준의 문서에 대해 읽기가 불가능하다.

④ Biba 모델에서는 높은 무결성 수준의 권한을 가진 사람이 자신의 권한보다 낮은 무결성 수준의 문서에 대해 쓰기가 가능하다.

**정답 4번**

**출제 포인트**

이 문제는 Bell-LaPadula 모델의 기밀성 규칙과 Biba 모델의 무결성 규칙을 서로 구분하는 문제이다.

**핵심 개념**

Bell-LaPadula는 기밀성 보호 모델로서 높은 등급 정보를 낮은 등급으로 새어 나가지 않게 하는 데 초점이 있다. 핵심 키워드는 no read up, no write down이다.
Biba는 무결성 보호 모델로서 낮은 신뢰 정보가 높은 신뢰 정보를 오염시키지 못하게 하는 데 초점이 있다. 핵심 키워드는 no read down, no write up이다.

**선지별 해설**

① X: Bell-LaPadula에서 틀린 부분은 "자신의 권한보다 높은 보안 수준을 가진 문서에 대해 쓰기가 불가능하다"는 표현이다. Bell-LaPadula의 쓰기 규칙은 no write down이므로 낮은 보안 수준 주체가 더 높은 보안 수준 객체에 쓰는 것은 가능하고, 더 낮은 보안 수준 객체에 쓰는 것이 금지된다.
② X: Bell-LaPadula에서 틀린 부분은 "정보의 무결성을 높이는 데 목적이 있는 경우 사용된다"는 표현이다. Bell-LaPadula는 기밀성 보호 모델이고, 무결성 보호가 목적일 때 사용하는 대표 모델은 Biba이다.
③ X: Biba에서 틀린 부분은 "자신의 권한보다 높은 무결성 수준의 문서에 대해 읽기가 불가능하다"는 표현이다. Biba의 읽기 규칙은 no read down이므로 높은 무결성 주체가 낮은 무결성 객체를 읽지 못하게 하는 것이 핵심이며, 낮은 무결성 주체가 더 높은 무결성 객체를 읽는 것을 막는 규칙은 아니다.
④ O: Biba의 쓰기 규칙은 no write up이므로 높은 무결성 수준의 권한을 가진 주체가 자신보다 낮은 무결성 수준의 문서에 쓰는 것은 가능하다. 높은 무결성 정보를 더 높은 쪽으로 올려 쓰는 것이 아니라 낮은 쪽으로 내려 쓰는 상황이므로 규칙에 어긋나지 않는다.

NoteBase

**오답 포인트**

Bell-LaPadula와 Biba는 읽기와 쓰기 금지 방향이 서로 반대로 뒤집혀 있어 단어만 바꿔 넣은 선지에 흔들리기 쉽다. 특히 ①의 "높은 보안 수준에 쓰기 불가"와 ③의 "높은 무결성 수준 읽기 불가"는 금지 방향을 반대로 말한 함정이다.

**다시 나오면 이렇게 판단**

먼저 보호 대상이 기밀성인지 무결성인지 구분한다. 기밀성이면 Bell-LaPadula로 연결해 no read up, no write down을 적용하고, 무결성이면 Biba로 연결해 no read down, no write up을 적용하면 된다.

**암기 포인트**

Bell-LaPadula는 기밀성이라 위는 못 읽고 아래는 못 쓴다. Biba는 무결성이라 아래는 못 읽고 위는 못 쓴다.

NoteBase

**문 8. MAC(Message Authentication Code)에 대한 설명으로 가장 옳지 않은 것은?**

① 전송할 데이터가 변조되었는지 검증할 수 있도록 덧붙이는 코드이다.

② MAC을 통해 데이터의 기밀성을 보장할 수 있다.

③ 해시함수를 이용해 MAC을 구성하는 것이 HMAC(Hashed MAC)이다.

④ MAC이 사용되는 사례로는 IPSec, SSL/TLS 등이 있다.

**정답 2번**

**출제 포인트**

이 문제는 MAC의 핵심 기능이 무결성·메시지 인증인지, 아니면 기밀성까지 포함하는지를 구분하는 문제이다.

**핵심 개념**

MAC: 송신자와 수신자가 공유한 비밀키로 메시지에 붙이는 인증값으로, 메시지 변조 여부와 정당한 생성 여부를 확인하는 수단이다. 결정 차이축은 무결성·인증이다. 키워드는 변조 검출, 인증값이다.
암호화: 평문을 읽을 수 없게 바꾸어 내용을 숨기는 수단으로, 보호 대상의 핵심은 기밀성이다. 결정 차이축은 내용 은닉이다. 키워드는 기밀성, 복호화이다.
HMAC: 해시함수와 비밀키를 이용해 만드는 MAC 방식이다. 키워드는 keyed hash, 해시 기반 MAC이다.

**선지별 해설**

① O
전송 데이터에 MAC 값을 덧붙여 보내고, 수신 측이 같은 방식으로 다시 계산해 비교하면 데이터가 중간에 변조되었는지 확인할 수 있다. MAC의 대표 기능인 무결성 검증을 설명한 선지이므로 옳다.

② X
틀린 부분은 "데이터의 기밀성을 보장"한다는 표현이다. MAC은 메시지가 바뀌지 않았는지와 올바른 송신자가 만든 값인지를 확인할 수 있지만, 내용을 숨기지는 못한다. 올바르게는 "MAC을 통해 데이터의 무결성과 인증을 보장할 수 있다"이다.

③ O
HMAC은 해시함수와 비밀키를 이용해 MAC을 구성하는 방식이다. 해시 기반 MAC이라는 정의와 정확히 일치하므로 옳다.

④ O
MAC은 실제 통신 프로토콜에서 무결성 검증 용도로 널리 사용된다. IPsec과 SSL/TLS에서는 해시 기반 MAC이나 이에 준하는 메시지 인증 방식으로 데이터 변조 여부를 점검하므로 옳다.

NoteBase

**오답 포인트**

MAC에 비밀키가 들어간다는 이유만으로 암호화와 같은 기능이라고 오해하기 쉽다. 이 문항의 함정은 "기밀성"이라는 단어 하나이며, MAC은 내용을 숨기는 기술이 아니라 변조를 검출하는 기술이라는 점을 놓치면 ②를 맞는 선지로 착각하게 된다.

**다시 나오면 이렇게 판단**

보안 기술 문제에서는 먼저 보호 목표를 구분한다. 내용 숨김이면 기밀성이므로 암호화이고, 변조 검출과 송신자 확인이면 무결성·인증이므로 MAC이다. 선지에 기밀성이라는 말이 나오면 암호화 기능인지부터 분리해 판단한다.

**암기 포인트**

MAC은 변조 검출, 암호화는 내용 은닉, HMAC은 해시 기반 MAC이다.

NoteBase

**문 9. 리눅스 및 유닉스 계열의 운영체제에서 디렉터리 탐색 공격을 위해 사용되는 etc 디렉터리에 있는 passwd 파일을 다운로드하는 경로명으로 가장 옳은 것은?**

① ../root/bin/passwd

② ../etc/passwd

③ ../etc/sbin/passwd

④ /home/passwd

**정답 2번**

**출제 포인트**

이 문제는 디렉터리 탐색 경로와 리눅스·유닉스 계열의 계정 정보 파일 위치를 함께 묻는 문제이다.

**사례 정리**

대상 운영체제는 리눅스 및 유닉스 계열이다.
목표 파일은 etc 디렉터리에 있는 passwd 파일이다.
판단의 핵심은 passwd 파일의 실제 위치가 /etc/passwd인지와 제시된 경로가 그 위치를 올바르게 가리키는지이다.

**핵심 개념**

디렉터리 탐색은 ../ 로 상위 디렉터리로 이동한 뒤 목표 파일의 실제 경로를 이어 붙여 접근하는 방식이다.
리눅스 및 유닉스 계열에서 passwd 파일의 기본 위치는 /etc/passwd이며, 사용자 암호 해시 자체는 보통 /etc/shadow에 분리된다.

**적용 기준**

이 문항에서는 파일명이 passwd라는 점보다 그 파일이 들어 있는 디렉터리가 etc라는 점이 더 중요하다.
따라서 보기 중 /etc/passwd를 정확히 가리키는 경로를 찾으면 된다.

**선지별 해설**

① X: ../root/bin/passwd는 root/bin 아래의 passwd를 뜻하므로 계정 정보 파일 위치가 아니다. 틀린 표현은 root/bin이며, 올바르게는 ../etc/passwd이다.
② O: ../etc/passwd는 상위 디렉터리로 한 단계 이동한 뒤 etc 디렉터리의 passwd 파일을 가리키므로 옳다.
③ X: ../etc/sbin/passwd는 etc 아래 sbin 하위 경로를 전제로 하지만 passwd 파일은 그 위치에 있지 않다. 틀린 표현은 etc/sbin이며, 올바르게는 ../etc/passwd이다.
④ X: /home/passwd는 home 디렉터리 아래의 passwd를 뜻하므로 시스템 계정 정보 파일 경로가 아니다. 틀린 표현은 /home이며, 올바르게는 /etc/passwd 또는 상대 경로로 ../etc/passwd이다.

NoteBase

**오답 포인트**

passwd라는 이름만 보고 실행 파일 경로나 임의의 홈 디렉터리 경로를 떠올리면 틀리기 쉽다. 이 문제의 함정은 파일명보다 시스템 계정 정보 파일의 표준 위치가 /etc 아래라는 점과, 보기에서 상대 경로 ../ 가 함께 쓰였다는 점이다.

**다시 나오면 이렇게 판단**

리눅스 경로 문제는 먼저 목표 파일의 표준 절대경로를 떠올린 뒤, 제시된 보기가 절대경로인지 상대경로인지 구분해 대입하면 된다. passwd 파일을 묻는다면 기준 경로는 /etc/passwd이다.

**암기 포인트**

계정 정보 파일은 /etc/passwd, 암호 해시는 /etc/shadow이다.

NoteBase

**문 10. 악성코드의 특징과 사례에 대한 설명으로 가장 옳지 않은 것은?**

① 좀비 악성코드에 감염되면 외부 명령에 의해 DDoS 공격에 사용되기도 한다.

② 다형성 바이러스는 응용 프로그램에 의해 해석되는 매크로나 스크립팅 코드를 사용하며 주로 문서에 포함된다.

③ 바이러스, 웜, 좀비 악성코드는 자가 복제를 하는 특징이 있다.

④ Drive-by-Download 악성코드는 사용자가 이것을 심어 놓은 웹사이트를 방문할 때 자신도 모르게 다운로드된다.

**정답 2번**

**출제 포인트**

이 문제는 좀비 악성코드, 다형성 바이러스, Drive-by-Download의 특징을 서로 혼동하지 않고 정확히 구별할 수 있는지를 묻는 문제이다.

**핵심 개념**

좀비 악성코드는 감염된 호스트가 외부의 명령제어에 따라 원격 조종되는 악성코드 또는 그 상태를 말하며 봇넷 공격에 동원된다.
다형성 바이러스는 복제될 때마다 자신의 코드 형태나 서명을 바꾸어 탐지를 회피하는 바이러스이다.
매크로 바이러스는 응용 프로그램이 해석하는 매크로나 스크립트 코드를 사용하며 주로 문서 파일에 포함된다.
Drive-by-Download는 사용자가 악성 웹페이지를 방문하는 것만으로도 자신도 모르게 악성코드가 내려받아지는 방식이다.

NoteBase

### 선지별 해설

① O
좀비 악성코드에 감염된 시스템은 공격자의 명령제어 서버 지시에 따라 봇넷의 일부로 동작할 수 있고, 그 대표적 활용 사례가 DDoS 공격이다.

② X
틀린 부분은 '다형성 바이러스는 응용 프로그램에 의해 해석되는 매크로나 스크립팅 코드를 사용하며 주로 문서에 포함된다'는 설명이다. 이는 다형성 바이러스가 아니라 매크로 바이러스의 특징이다. 올바르게는 '다형성 바이러스는 복제 과정에서 코드 형태를 계속 바꾸어 시그니처 기반 탐지를 어렵게 한다'이다.

③ O
바이러스와 웜은 대표적인 자가 복제형 악성코드이고, 좀비 악성코드도 감염 호스트를 늘려 봇넷을 구성하는 확산형 악성코드 문맥에서 자가 복제·전파 특성을 가진 유형으로 다룬다.

④ O
Drive-by-Download는 사용자가 악성 스크립트나 익스플로잇이 심어진 웹사이트를 방문하는 과정에서 별도 인지 없이 악성코드가 다운로드되는 공격 방식이므로 설명이 맞다.

### 오답 포인트

다형성 바이러스와 매크로 바이러스는 모두 탐지 회피나 문서 감염 문제와 연결되어 자주 혼동된다. 이 문항은 ②에서 '매크로나 스크립팅 코드', '주로 문서에 포함'이라는 매크로 바이러스의 키워드를 다형성 바이러스에 바꿔 붙인 점이 함정이다.

### 다시 나오면 이렇게 판단

문서 내부의 매크로·스크립트가 보이면 매크로 바이러스를 먼저 떠올리고, 복제할 때마다 코드 모양이 바뀌어 탐지를 피하면 다형성 바이러스로 판단한다. 외부 명령으로 원격 조종되면 좀비, 웹사이트 방문만으로 내려받아지면 Drive-by-Download로 구분된다.

### 암기 포인트

문서에 숨어 있으면 매크로, 모습이 바뀌면 다형성, 원격 조종되면 좀비, 방문만 해도 내려오면 Drive-by-Download이다.

NoteBase

**문 11. 공개키 암호 알고리즘인 RSA에 대한 설명으로 가장 옳지 않은 것은? (단, N은 서로 다른 두 개의 소수를 곱한 값이다.)**

① 공개키 암호 알고리즘은 암호화 키와 복호화 키를 사용하며, RSA는 디지털 서명에 사용할 수 있다.

② RSA의 암호문은 평문을 E제곱해서 mod N을 취하여 만들 수 있으며 여기서 E와 N으로 이뤄진 쌍이 공개키다.

③ RSA의 평문은 암호문을 D제곱해서 mod N을 취하여 만들 수 있으며 여기서 D와 N으로 이뤄진 쌍이 개인키다.

④ 큰 수의 소인수 분해를 고속으로 할 수 있는 방법이 발견되면 RSA를 해독할 수 있으며, 중간자 공격을 사용해도 RSA를 해독할 수 있다.

**정답 4번**

**출제 포인트**

이 문제는 RSA의 공개키·개인키 구성과 암복호화 원리, 그리고 RSA 자체의 취약점과 인증 부재 공격을 구분하는지를 묻는 문제이다.

**핵심 개념**

RSA는 서로 다른 두 소수의 곱 $N = pq$를 바탕으로 하는 공개키 암호이다. 공개키는 $(E, N)$, 개인키는 $(D, N)$이며 암호화는 C=M^E N, 복호화는 M=C^D N의 형태로 이해한다. 소인수분해가 빨라지면 RSA의 비밀키 유도가 쉬워질 수 있지만, 중간자 공격은 RSA 수학 자체를 깨는 공격이 아니라 인증이 없는 통신 상대를 속이는 공격이다.

NoteBase

### 선지별 해설

① O
공개키 암호는 암호화와 복호화에 서로 다른 키를 사용한다. RSA는 공개키 암호 방식이며 디지털 서명에도 사용할 수 있으므로 옳다.

② O
RSA 암호화는 평문 $M$에 대해 C=M^E N로 표현할 수 있다. 이때 $E$와 $N$의 쌍을 공개키로 사용하므로 옳다.

③ O
RSA 복호화는 암호문 $C$에 대해 M=C^D N로 표현할 수 있다. 이때 $D$와 $N$의 쌍이 개인키이므로 옳다.

④ X
앞부분인 '큰 수의 소인수 분해를 고속으로 할 수 있는 방법이 발견되면 RSA를 해독할 수 있다'는 RSA의 안전성이 큰 수의 소인수분해 난이도에 의존한다는 점에서 맞는 설명이다. 틀린 표현은 '중간자 공격을 사용해도 RSA를 해독할 수 있다'이다. 실제로는 중간자 공격은 인증되지 않은 공개키를 가로채 통신 상대를 속이는 공격이며, RSA 알고리즘 자체를 수학적으로 해독하는 공격은 아니다.

### 오답 포인트

④는 'RSA의 수학적 안전성'과 '통신 과정의 인증 문제'를 한 선지에 섞어 놓은 함정이다. 소인수분해 성공은 RSA 자체의 붕괴와 연결되지만, 중간자 공격은 공개키 진위 확인이 없을 때 발생하는 별개의 공격이라는 점을 구분해야 한다.

### 다시 나오면 이렇게 판단

RSA 문제는 먼저 공개키 $(E, N)$, 개인키 $(D, N)$, 암호화식 $M^E$, 복호화식 $C^D$를 확인한다. 그다음 공격 기법이 RSA의 수학적 기반을 깨는지, 아니면 인증 절차를 속이는 통신 공격인지를 분리해서 판단한다.

### 암기 포인트

RSA는 공개키 $(E, N)$, 개인키 $(D, N)$이고 소인수분해에는 약하지만 중간자 공격은 인증 문제이다.

NoteBase

**문 12. 무선 랜 프로토콜에 대한 설명으로 가장 옳지 않은 것은?**

① 802.11b는 와이파이라고 하며 WEP 방식의 보안 기능을 사용한다.

② 802.11 g는 802.11b에 802.11a의 속도 성능을 추가한 프로토콜이다.

③ 802.11n은 여러 안테나를 사용하는 다중 입력/다중 출력(MIMO) 기술로, 대역폭 손실을 최소화하며 최대 속도는 400Mbps이다.

④ 802.11ad는 60GHz 대역을 사용해 데이터를 전송하는 방식으로 대용량의 데이터 등 높은 비트레이트 동영상 스트리밍에 적합하다.

**정답 3번**

**출제 포인트**

이 문제는 802.11b, 802.11 g, 802.11n, 802.11ad의 대역, 전송속도, 핵심 기술을 구별할 수 있는지를 묻는다.

**핵심 개념**

802.11b는 2.4GHz 대역에서 동작한 초기 무선랜 표준으로 초창기 Wi-Fi와 WEP 보안이 함께 언급된다. 802.11 g는 2.4GHz를 유지하면서 802.11a급 속도 성능을 제공하는 표준이다. 802.11n은 MIMO를 도입해 처리량을 높인 표준이다. 802.11ad는 60GHz 대역에서 매우 높은 속도로 근거리 전송을 수행하는 표준이다.

**선지별 해설**

1번 O: 802.11b는 초창기 Wi-Fi로 널리 불린 무선랜 표준이며, 당시 보안 방식으로 WEP가 사용되었다. 표현이 다소 포괄적이지만 시험 문맥에서는 맞는 설명으로 본다.
2번 O: 802.11 g는 802.11b와 같은 2.4GHz 대역을 사용하면서 802.11a와 같은 54Mbps급 속도 성능을 제공한 표준이다. 802.11b와의 하위 호환성을 유지한다는 점도 핵심이다.
3번 X: 틀린 부분은 "최대 속도는 400Mbps이다"라는 표현이다. 802.11n은 MIMO 기술을 사용하며 표준상 최대 속도는 일반적으로 600Mbps로 본다. 올바르게는 "802.11n은 MIMO 기술을 사용하며 최대 속도는 600Mbps이다"이다.
4번 O: 802.11ad는 60GHz 대역을 이용하는 무선랜 표준으로, 매우 높은 전송률을 제공해 대용량 데이터 전송이나 높은 비트레이트의 동영상 스트리밍에 적합하다. 다만 도달거리는 짧은 편이다.

**오답 포인트**

802.11n에서 기억해야 할 핵심은 MIMO와 최대 속도이다. MIMO만 기억하고 최대 속도를 400Mbps로 잘못 줄여 외우면 3번 같은 선지에 걸린다.

NoteBase

**다시 나오면 이렇게 판단**

무선랜 표준 문제는 대역, 핵심 기술, 최대 속도를 한 묶음으로 확인하면 빠르게 풀린다. 특히 802.11 g는 2.4GHz에서 54Mbps, 802.11n은 MIMO와 최대 600Mbps, 802.11ad는 60GHz 초고속 근거리 전송으로 구별된다.

**암기 포인트**

b는 2.4GHz·WEP, g는 2.4GHz·54Mbps, n은 MIMO·600Mbps, ad는 60GHz·초고속이다.

NoteBase

**문 13. <보기>의 설명에 가장 적합한 용어는?**

<보기>
• DDoS와 같은 서비스 거부 공격의 대응 방법으로 사용된다.
• 특정 IP 주소로부터의 패킷들을 드롭시키는 방법을 적용한다.

① IP spoofing
② Security patches
③ Port scanning
④ Blackholing

**정답 4번**

**출제 포인트**

DDoS 대응 기법인 블랙홀링의 개념과 유사 보안 용어를 구별하는 문제이다.

**핵심 개념**

Blackholing은 공격 트래픽을 특정 경로로 보내 버리도록 만들어 서비스 거부 공격의 영향을 줄이는 대응 기법이다.
IP spoofing은 출발지 IP 주소를 위조하는 공격 기법이다.
Security patches는 소프트웨어 취약점을 수정하는 보안 업데이트이다.
Port scanning은 열려 있는 포트와 서비스를 탐색하는 정찰 기법이다.

**선지별 해설**

① X: IP spoofing은 패킷의 출발지 주소를 속이는 공격 기법이므로 DDoS 대응 방법이 아니다. 틀린 표현은 '대응 방법'이다. 올바르게는 출발지 IP를 위조하는 공격 기법이다.
② X: Security patches는 취약점을 제거하거나 완화하는 업데이트이지 특정 IP의 패킷을 드롭하는 기법이 아니다. 틀린 표현은 '패킷들을 드롭시키는 방법'이다. 올바르게는 시스템 취약점을 수정하는 보안 업데이트이다.
③ X: Port scanning은 대상 시스템의 포트 상태를 조사하는 정찰 행위이므로 공격 트래픽을 차단하는 대응 기법이 아니다. 틀린 표현은 'DDoS 대응 방법'이다. 올바르게는 열려 있는 포트와 서비스를 탐지하는 스캐닝 기법이다.
④ O: Blackholing은 특정 목적지나 출발지와 관련된 트래픽을 블랙홀 경로로 보내 폐기하는 방식이므로 DDoS 대응에 사용된다. 보기의 '특정 IP 주소로부터의 패킷들을 드롭'한다는 설명과 가장 잘 맞는다.

NoteBase

### 오답 포인트

보기의 핵심은 '공격을 막기 위해 패킷을 드롭한다'는 점이다. 스푸핑과 포트 스캐닝은 공격 또는 정찰 기법이고, 패치는 사전 보완 조치이므로 실시간 트래픽 폐기와는 결이 다르다.

### 다시 나오면 이렇게 판단

선지에 특정 IP나 특정 목적지의 트래픽을 버려 공격 영향을 줄인다는 설명이 나오면 블랙홀링 계열 대응으로 판단한다. 주소를 속이면 spoofing, 포트를 훑으면 scanning, 취약점을 고치면 patching으로 구별한다.

### 암기 포인트

블랙홀링은 공격 트래픽을 버리는 대응이고, 스푸핑은 주소를 속이는 공격이다.

NoteBase

**문 14. IKE(Internet Key Exchange) 프로토콜에 대한 설명으로 가장 옳지 않은 것은?**

① IPSec의 구성 요소 중 하나로 SA(Security Association)를 성립하는 데 필요한 데이터들을 안전하게 전달하기 위해 사용된다.

② ISAKMP를 토대로 만들어진 IPSec 전용의 키 교환 프로토콜이다.

③ IKEv2와 IKEv1은 서로 호환된다.

④ Diffie-Hellman 키 교환 프로토콜이 IKE에서 사용된다.

**정답 3번**

**출제 포인트**

이 문제는 IKE의 역할과 구성 요소, 그리고 IKEv1과 IKEv2의 호환성 여부를 구별하는 문제이다.

**핵심 개념**

IKE는 IPsec에서 SA를 협상하고 키 교환에 필요한 정보를 안전하게 교환하는 프로토콜이다.
SA는 IPsec 통신에서 사용할 알고리즘, 키, 모드 같은 보안 매개변수의 약속이다.
IKEv1과 IKEv2는 목적은 같지만 메시지 형식과 절차가 달라 서로 직접 호환되지 않는다.

**선지별 해설**

① O
IKE는 IPsec의 SA를 설정하는 데 필요한 인증, 키 교환, 보안 매개변수 협상 정보를 안전하게 주고받는 데 사용된다. 선지의 설명은 IKE의 역할에 부합한다.

② O
IKE는 ISAKMP 프레임워크를 바탕으로 IPsec에서 키 관리와 SA 협상을 수행하도록 설계된 프로토콜이다. 시험 수준에서는 맞는 설명으로 본다.

③ X
틀린 부분은 "IKEv2와 IKEv1은 서로 호환된다"는 표현이다.
실제로는 IKEv2와 IKEv1은 패킷 구조와 교환 절차가 달라 상호 운용되지 않는다. 올바르게는 "IKEv2와 IKEv1은 같은 목적의 후속 버전이지만 서로 직접 호환되지는 않는다"이다.

④ O
IKE는 안전한 공유 비밀을 만들기 위해 Diffie-Hellman 키 교환 방식을 사용한다. 따라서 이 설명은 옳다.

NoteBase

**오답 포인트**

③은 "상위 버전이므로 하위 버전과 자동으로 호환될 것"이라는 직관을 노린 선지이다. 프로토콜은 이름이 비슷해도 메시지 형식과 절차가 바뀌면 상호 호환되지 않을 수 있다는 점이 함정이다.

**다시 나오면 이렇게 판단**

IKE 문제에서는 먼저 "SA 협상과 키 교환을 담당하는가"를 보고, 다음으로 "버전이 달라도 직접 통신 가능한가"를 따져 본다. 기능 설명은 대체로 맞고, 버전 호환성처럼 단정적으로 쓰인 표현이 오답 포인트가 된다.

**암기 포인트**

IKE는 SA 협상과 DH 키 교환, IKEv1과 IKEv2는 비호환이다.

NoteBase

**문 15. 개인정보 보호법령상 개인정보의 안전성 확보 조치를 위한 개인정보처리자의 업무로 가장 옳지 않은 것은?**

① 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치

② 개인정보 유출 및 오용 · 남용 방지를 위한 내부통제 시스템의 구축

③ 개인정보를 안전하게 저장 · 전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치

④ 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조 · 변조 방지를 위한 조치

**정답 2번**

### 쟁점

이 문제는 개인정보 보호법령상 안전성 확보 조치의 법정 항목을 정확한 명칭으로 구별하는 문제이다.
핵심은 내부 관리계획, 접근 권한 제한, 접근 통제, 암호화, 접속기록 보관이 각각 독립된 조치라는 점을 구별하는 것이다.

### 용어 풀이

안전성 확보 조치 = 개인정보의 유출, 훼손, 오남용을 막기 위해 개인정보처리자가 해야 하는 기술적·관리적·물리적 보호조치이다.
내부 관리계획 = 개인정보 보호 조직, 교육, 접근권한 관리 등 안전조치 이행 사항을 담아 수립·시행·점검하는 내부 기준이다.

### 핵심 구분

개인정보 보호법 시행령 제30조는 안전성 확보 조치로 내부 관리계획의 수립·시행 및 점검, 접근 권한 제한, 접근 통제, 암호화, 접속기록의 보관 및 위조·변조 방지 등을 둔다.
따라서 법령상 명칭은 '내부 관리계획'이지 선지 ②의 '내부통제 시스템의 구축'이 아니다. ②는 법정 용어를 바꾸고 여러 조치를 섞어 쓴 표현이므로 틀리다.

NoteBase

**선지별 해설**

① O
개인정보에 대한 접근 통제와 접근 권한 제한은 시행령상 안전성 확보 조치에 해당한다.
접근 권한의 부여·변경·말소 기준 수립과 인증수단 운영 등이 이에 포함된다.

② X
시행령은 '개인정보 유출 및 오용·남용 방지를 위한 내부통제 시스템의 구축'을 독립된 법정 항목으로 두지 않는다.
틀린 표현: '내부통제 시스템의 구축'
올바른 표현: '개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행 및 점검'이다.
또는 접근 통제, 암호화, 접속기록 보관 등 개별 안전조치를 각각 구분하여 표현해야 한다.

③ O
개인정보를 안전하게 저장·전송하기 위한 암호화 기술의 적용 또는 이에 상응하는 조치는 시행령상 안전성 확보 조치에 해당한다.
비밀번호의 암호화 저장, 개인정보 송수신 시 암호화 등이 대표적이다.

④ O
개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관과 위조·변조 방지 조치는 시행령상 명시된 항목이다.
접속일시, 처리내역 등의 접속기록을 저장·점검하고 안전하게 보관하는 내용이 여기에 포함된다.

**오답 포인트**

이 문제를 틀렸다면 법령의 정확한 항목명과 취지를 혼동했을 가능성이 높다. 특히 '내부 관리계획'을 막연한 '내부통제 시스템'으로 바꿔 쓰면 그럴듯해 보여도 법령상 표현과 맞지 않아 오답이 된다.

**다시 나오면 이렇게 판단**

법령형 문제에서는 선지의 핵심 명칭이 조문에 그대로 있는지를 먼저 본다. 낯선 합성 표현으로 여러 조치를 한 문장에 뭉뚱그린 선지는 원문 용어와 대응시켜 보면 오답이 드러난다.

**암기 포인트**

안전성 확보 조치는 내부 관리계획, 권한 제한, 접근 통제, 암호화, 접속기록, 악성프로그램 방어, 물리적 보호로 묶여 기억된다.

NoteBase

**문 16. <보기>에서 설명하는 블록암호 운영 모드로 가장 옳은 것은?**

<보기>
CTR과 CBC-MAC을 통합한 블록암호 모드로 기밀성과 인증, 무결성을 제공한다. 핵심적인 알고리즘의 구성 요소는 AES 암호 알고리즘, CTR 모드, CBC-MAC이다. NIST에 의해 IEEE 802.11 WiFi 보안 요구사항을 지원하기 위해 표준화되었다.

① CCM
② GCM
③ CFB
④ OFB

**정답 1번**

**출제 포인트**

이 문제는 AEAD 블록암호 운용 모드인 CCM의 구성 요소와 GCM·CFB·OFB와의 차이를 묻는 문제이다.

**핵심 개념**

CCM은 Counter with CBC-MAC의 약자로, CTR 모드로 암호화를 수행하고 CBC-MAC으로 인증을 수행하여 기밀성과 무결성을 함께 제공하는 운용 모드이다.
GCM은 CTR 암호화에 GHASH 기반 인증을 결합한 운용 모드이다.
CFB와 OFB는 블록암호를 스트림처럼 사용하게 하는 운용 모드이지만, 자체적으로 인증용 MAC을 포함하지 않는다.

NoteBase

**선지별 해설**

① O
CCM은 CTR과 CBC-MAC을 결합한 모드이므로 보기의 설명과 정확히 일치한다. IEEE 802.11 무선 LAN 보안에서 사용하는 CCMP도 AES 기반 CCM을 사용한다.

② X
틀린 부분은 GCM을 CBC-MAC 기반 모드처럼 보는 점이다. GCM은 CTR 모드와 GHASH 기반 인증을 결합한 모드이다. 올바르게는 "GCM은 CTR과 GHASH를 결합해 기밀성과 무결성을 제공한다."이다.

③ X
틀린 부분은 CFB가 인증과 무결성까지 제공하는 모드라는 점이다. CFB는 암호문 피드백을 이용해 블록암호를 스트림처럼 사용하는 운용 모드일 뿐이다. 올바르게는 "CFB는 기밀성 중심의 운용 모드이고, 별도 MAC 없이는 인증·무결성을 보장하지 않는다."이다.

④ X
틀린 부분은 OFB가 CTR과 CBC-MAC을 통합한 AEAD 모드라는 점이다. OFB는 출력 피드백으로 키스트림을 만드는 운용 모드일 뿐이다. 올바르게는 "OFB도 기밀성 중심의 운용 모드이며, 인증·무결성 기능은 별도로 붙여야 한다."이다.

**오답 포인트**

CTR이라는 단어만 보고 GCM과 CCM을 함께 떠올리면 혼동하기 쉽다. 이 문제의 결정 단서는 인증 방식이 CBC-MAC인지 여부이다. CFB와 OFB는 이름은 익숙하지만 MAC이 없으므로 보기의 '인증, 무결성 제공'과 맞지 않는다.

**다시 나오면 이렇게 판단**

보기에서 "CTR + CBC-MAC", "기밀성 + 인증 + 무결성", "802.11 WiFi 보안"이 함께 나오면 CCM으로 판단한다. CTR과 GHASH가 나오면 GCM이고, CFB·OFB처럼 피드백 계열만 나오면 인증 기능이 없는 일반 운용 모드로 구분한다.

**암기 포인트**

CCM은 CTR + CBC-MAC, GCM은 CTR + GHASH이다.

NoteBase

**문 17. <보기>는 정보보호 및 개인정보보호 관리체계(ISMS-P)의 개인정보 수집 제한에 대한 인증 기준이다. 이 기준에 대한 주요 확인사항으로 가장 옳지 않은 것은?**

<보기>
개인정보는 서비스 제공을 위해 필요한 최소한의 정보를 적법하고 정당하게 수집하여야 하며, 필수정보 이외의 개인정보를 수집하는 경우에는 선택항목으로 구분하여 해당 정보를 제공하지 않는다는 이유로 서비스 제공을 거부하지 않아야 한다.

① 개인정보를 수집하는 경우 서비스 제공 또는 법령에 근거한 처리 등을 위해 필요한 범위 내에서 최소한의 정보만을 수집하고 있는가?

② 수집 목적에 필요한 최소한의 정보 외의 개인정보를 수집하는 경우 정보주체(이용자)가 해당 개인정보의 제공 여부를 선택할 수 있도록 하고 있는가?

③ 정보주체(이용자)가 수집 목적에 필요한 최소한의 정보 이외의 개인정보 수집에 동의하지 않는다는 이유로 서비스 또는 재화의 제공을 거부하지 않도록 하고 있는가?

④ 법적 근거에 따라 정보주체(이용자)의 주민등록번호 수집이 가능한 경우에도 아이핀, 휴대폰 인증 등 주민등록번호를 대체하는 수단을 제공하고 있는가?

**정답 4번**

**출제 포인트**

이 문제는 ISMS-P의 개인정보 수집 제한 기준에서 최소 수집, 선택항목 구분, 선택정보 미제공 시 서비스 거부 금지와 주민등록번호 대체수단 제공을 구별하는 문제이다.

**핵심 개념**

개인정보 수집 제한은 서비스 제공이나 법적 근거에 필요한 최소한의 개인정보만 수집하는 기준이다.
필수정보 외 정보는 선택항목으로 구분되어야 하며, 선택정보를 주지 않았다는 이유로 서비스 제공을 거부하면 안 된다.
주민등록번호를 대신하는 수단 제공은 주민등록번호 처리 최소화와 대체 인증수단 확보에 관한 통제이지, 일반적인 개인정보 수집 제한의 핵심 확인사항과는 결이 다르다.

NoteBase

### 선지별 해설

① O: 서비스 제공 또는 법적 근거에 따른 처리에 필요한 범위 안에서 최소한의 정보만 수집하는지는 개인정보 수집 제한의 핵심 확인사항이다. 보기의 '필요한 최소한의 정보'와 직접 대응한다.
② O: 수집 목적상 꼭 필요하지 않은 개인정보는 선택항목으로 분리하고, 정보주체가 제공 여부를 선택할 수 있어야 한다. 이는 필수정보와 선택정보를 구분하는 기준에 해당한다.
③ O: 정보주체가 최소 필요정보 외 개인정보 수집에 동의하지 않는다는 이유만으로 서비스나 재화 제공을 거부하지 않아야 한다. 보기의 마지막 문장을 그대로 점검하는 항목이다.
④ X: 주민등록번호 수집이 가능한 경우 대체수단을 제공하는지는 주민등록번호 처리 제한 또는 주민번호 대체수단 제공과 관련된 점검이다. 틀린 부분은 '개인정보 수집 제한의 주요 확인사항'이라는 연결이다. 올바르게는 주민등록번호와 같은 고유식별정보의 처리 최소화와 대체 인증수단 제공 여부를 점검하는 별도의 취지로 보는 것이 맞다.

### 오답 포인트

④는 '최소 수집'이라는 큰 틀과 비슷해 보여 쉽게 끌리지만, 실제 문항의 보기와 ①~③은 모두 필수정보 최소화, 선택항목 구분, 미동의 시 서비스 거부 금지라는 같은 축에 있다. 반면 ④는 주민등록번호라는 특정 고유식별정보의 대체수단 문제로 축이 다르다.

### 다시 나오면 이렇게 판단

보기나 기준문에 '최소한의 정보', '선택항목', '미제공을 이유로 거부 금지'가 나오면 일반 개인정보 수집 제한 기준으로 본다. 선지가 주민등록번호, 아이핀, 휴대폰 인증처럼 특정 식별수단의 대체 여부를 묻기 시작하면 일반 수집 제한이 아니라 주민등록번호 처리 제한 쪽으로 분리해서 판단한다.

### 암기 포인트

수집 제한은 최소 수집·선택 분리·미동의 거부 금지이고, 주민번호 대체수단은 별도 통제이다.

NoteBase

**문 18. 블록암호 알고리즘을 구성하는 데 사용되는 페이스텔(Feistel) 구조와 SPN 구조에 대한 설명으로 가장 옳은 것은?**

① 정상적으로 복호화 과정이 수행되기 위해서 페이스텔 구조의 라운드 함수는 가역적(invertible)이어야 한다.

② 페이스텔 구조를 사용하는 대표적인 블록암호 알고리즘으로 AES가 있다.

③ SPN 구조는 Shannon의 혼동(confusion)과 확산(diffusion)이론을 바탕으로 한 구조이다.

④ SPN 구조의 암호화 과정은 최소 2라운드 반복 수행해야 전체 평문이 암호화된다.

**정답 3번**

**출제 포인트**

이 문제는 페이스텔 구조와 SPN 구조의 성질, 특히 라운드 함수의 가역성 요구 여부와 대표 알고리즘 및 혼동·확산 개념을 구별하는 문제이다.

**핵심 개념**

페이스텔 구조는 블록을 좌우로 나누어 한쪽에 라운드 함수를 적용한 뒤 다른 쪽과 결합하는 구조이므로, 복호화 시 라운드 함수를 역함수로 만들 필요가 없다.
SPN 구조는 치환과 순열을 여러 라운드 반복하여 Shannon의 혼동과 확산을 구현하는 구조이다.
페이스텔은 대표적으로 DES 계열, SPN은 대표적으로 AES가 해당한다.

NoteBase

### 선지별 해설

① X
틀린 부분은 "라운드 함수는 가역적(invertible)이어야 한다"는 표현이다.
페이스텔 구조는 XOR와 좌우 교환 구조 덕분에 복호화가 가능하므로 라운드 함수 자체는 가역적일 필요가 없다.

② X
틀린 부분은 "페이스텔 구조를 사용하는 대표적인 블록암호 알고리즘으로 AES가 있다"는 표현이다.
AES는 페이스텔 구조가 아니라 SPN 구조의 대표적인 블록암호이다. 페이스텔 구조의 대표 예시는 DES이다.

③ O
SPN 구조는 치환으로 혼동을, 순열과 반복 라운드로 확산을 높이는 방식이므로 Shannon의 혼동과 확산 이론을 바탕으로 한다.

④ X
틀린 부분은 "최소 2라운드 반복 수행해야 전체 평문이 암호화된다"는 표현이다.
SPN은 여러 라운드를 반복해 안전성을 높이는 구조이지만, 최소 2라운드가 구조적으로 반드시 필요하다고 단정할 수는 없다. 올바르게는 여러 라운드를 통해 혼동과 확산을 충분히 확보하도록 설계된다고 보는 것이 맞다.

### 오답 포인트

①은 "복호화"라는 말 때문에 역함수가 꼭 필요하다고 오해하기 쉽다. 그러나 페이스텔의 핵심은 전체 구조가 역연산 가능하다는 점이지 라운드 함수 자체의 가역성이 아니다. ②는 AES와 DES의 구조를 뒤바꾸는 대표 함정이고, ④는 "반복 라운드"라는 사실을 "최소 2라운드 필수"로 과장한 선지이다.

### 다시 나오면 이렇게 판단

블록암호 구조 문제가 나오면 먼저 대표 알고리즘을 구조와 연결한다. DES는 페이스텔, AES는 SPN으로 본다. 그다음 페이스텔은 라운드 함수 비가역 가능, SPN은 혼동과 확산 구현이라는 두 축으로 선지를 판별하면 된다.

### 암기 포인트

페이스텔은 함수 비가역 가능, SPN은 혼동·확산, AES는 SPN, DES는 페이스텔이다.

NoteBase

**문 19. 타원 곡선 암호(ECC: Elliptic Curve Cryptography)에 대한 설명으로 가장 옳은 것은?**

① 사용되는 키의 길이가 RSA보다 짧다.

② 타원 곡선 위의 실숫값을 이용하여 계산하는 기술이다.

③ 데이터 암호화와 복호화에 사용되며, 디지털 서명에는 사용이 불가능하다.

④ 타원 곡선상의 점 G와 정수 x에 대하여, xG를 계산하는 데 시간이 오래 걸린다는 성질을 이용한다.

**정답 1번**

**출제 포인트**

이 문제는 ECC의 핵심 원리와 RSA 대비 특징을 구별할 수 있는지를 묻는 문제이다.

**핵심 개념**

ECC는 타원 곡선 위 점들의 연산을 이용하는 공개키 암호 방식이며, 같은 보안 수준에서 RSA보다 짧은 키 길이로 구현할 수 있다.
ECC의 연산은 실수체가 아니라 소수체나 이진체 같은 유한체 위에서 수행된다.
ECC의 안전성은 점 $G$와 정수 $x$에 대해 $xG$는 계산할 수 있지만, $G$와 $xG$만으로 $x$를 구하기 어려운 타원곡선 이산로그 문제에 있다.

NoteBase

**기출OX 해설집 · 공무원/서울시/7급 · 정보보호론 · 2022 · 10월**

### 선지별 해설

① O
ECC는 같은 수준의 안전성을 확보할 때 RSA보다 훨씬 짧은 키 길이를 사용할 수 있다. 따라서 ①은 옳다.

② X
틀린 부분은 "실수값"이다.
실제로는 타원 곡선 위의 점 연산을 유한체에서 수행한다. ECC를 실수값으로 계산하는 기술이라고 보는 것은 잘못이다.

③ X
틀린 부분은 "디지털 서명에는 사용이 불가능하다"이다.
실제로는 ECC는 ECDSA와 같이 디지털 서명에 널리 사용된다. 데이터 암호화·복호화에도 응용될 수 있으므로 서명에 사용 불가라고 단정할 수 없다.

④ X
틀린 부분은 "$xG$를 계산하는 데 시간이 오래 걸린다"이다.
실제로는 $xG$ 계산 자체가 핵심 난제가 아니다. ECC는 $G$와 $xG$가 주어졌을 때 $x$를 역으로 구하기 어려운 성질을 이용한다.

### 오답 포인트

④처럼 "계산이 어렵다"는 표현이 나오면 정방향 계산과 역문제를 구분해야 한다. ECC에서 어려운 것은 $xG$ 계산이 아니라 $G$와 $xG$로부터 $x$를 찾는 것이다. ②의 "실수값"도 자주 섞어 넣는 함정이다.

### 다시 나오면 이렇게 판단

ECC 선지는 먼저 "짧은 키", "유한체", "디지털 서명 가능", "어려운 것은 역산" 네 가지 기준으로 본다. 이 네 기준과 어긋나는 표현이 들어가면 오답일 가능성이 크다.

### 암기 포인트

ECC는 짧은 키를 쓰고, 유한체에서 연산하며, ECDSA 서명이 가능하고, 어려운 것은 $G$, $xG \rightarrow x$ 역산이다.

NoteBase

**문 20. RAID level과 그 특성을 옳게 짝지은 것은?**

① RAID 0: striping, RAID 1: mirroring, RAID 5: distributed parity

② RAID 0: mirroring, RAID 1: striping, RAID 5: parity

③ RAID 0: parity, RAID 1: mirroring, RAID 5: multiple storage

④ RAID 0: mirroring, RAID 1: striping, RAID 5: fast mirroring

**정답 1번**

**출제 포인트**

이 문제는 RAID 0, RAID 1, RAID 5의 대표 저장 방식과 핵심 키워드를 정확히 구별하는지를 묻는다.

**핵심 개념**

RAID 0은 데이터를 여러 디스크에 나누어 기록해 성능을 높이는 스트라이핑 방식이다.
RAID 1은 동일한 데이터를 복제해 저장하는 미러링 방식이다.
RAID 5는 블록 단위 스트라이핑과 분산 패리티를 함께 사용해 성능과 장애 허용성을 같이 확보하는 방식이다.

**선지별 해설**

1번: O. RAID 0은 striping, RAID 1은 mirroring, RAID 5는 distributed parity가 맞다. 각 RAID 레벨의 대표 특징을 정확히 연결한 선택지이다.
2번: X. 틀린 부분은 RAID 0을 mirroring, RAID 1을 striping으로 바꿔 적은 표현이다. RAID 0은 미러링이 아니라 striping이고, RAID 1은 스트라이핑이 아니라 mirroring이다. RAID 5의 parity 자체는 맞지만 앞의 대응이 틀려서 오답이다.
3번: X. 틀린 부분은 RAID 0을 parity로, RAID 5를 multiple storage로 적은 표현이다. RAID 0의 핵심은 parity가 아니라 striping이다. RAID 5의 핵심 표현도 단순한 multiple storage가 아니라 distributed parity이다.
4번: X. 틀린 부분은 RAID 0을 mirroring, RAID 1을 striping, RAID 5를 fast mirroring으로 적은 표현이다. 올바르게는 RAID 0은 striping, RAID 1은 mirroring, RAID 5는 distributed parity이다. RAID 5를 미러링 계열로 보는 것 자체가 잘못이다.

**오답 포인트**

출제자는 striping, mirroring, parity처럼 자주 함께 외우는 키워드의 위치를 서로 바꿔 놓아 혼동을 유도한다. 특히 RAID 0과 RAID 1의 대응을 뒤집거나, RAID 5를 막연히 고급 미러링처럼 착각하면 틀리기 쉽다.

NoteBase

**다시 나오면 이렇게 판단**

먼저 RAID 0은 성능 중심의 striping, RAID 1은 복제 중심의 mirroring, RAID 5는 distributed parity라는 세 축을 확정한 뒤 선택지의 대응이 한 칸씩 바뀌지 않았는지만 확인하면 된다.

**암기 포인트**

RAID 0은 분산 기록, RAID 1은 동일 복제, RAID 5는 분산 패리티이다.

NoteBase