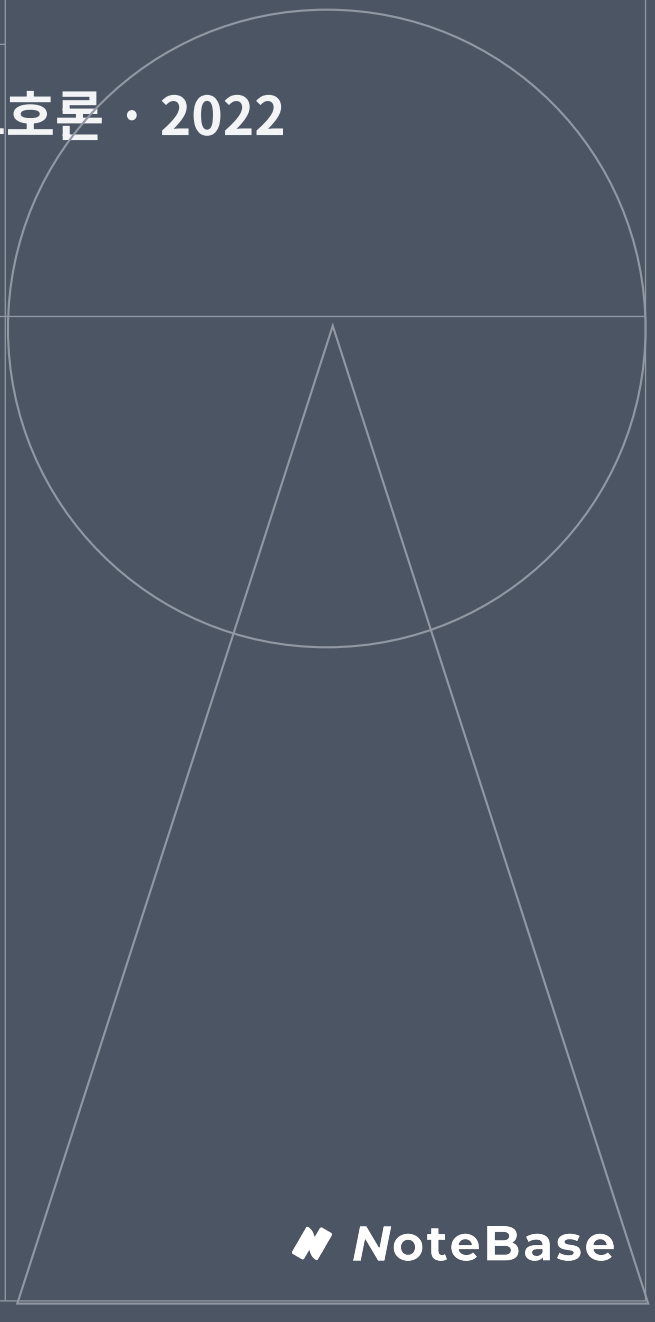
# 기출OX 해설집

공무원/군무원/9급 · 정보보호론 · 2022



NoteBase

# 기출OX 해설집

## 공무원/군무원/9급 · 정보보호론 · 2022

### 공무원/군무원/9급 · 정보보호론 · 2022

1. 다음 중 개인정보의 자기결정권에 대한 설명으로 가장 옳은 것은?
   ① 개인정보를 수집하는 경우에, 처리목적 달성에 필요한 최소한의 개인정보만을 수집해야 하는 책임
   ② 특정개인을 알아볼 수 있는 정보가 생성된 경우에는 즉시 처리중지, 회수·파기해야 하는 의무
   ③ 개인정보가 분실·도난·유출·위조·변조·훼손되지 않도록 안전성 확보를 해야 하는 책임
   ④ 자신에 관한 정보가 언제, 어떻게, 어느 범위까지 수집, 이용, 공개될 수 있는지를 정보주체가 스스로 통제, 결정할 수 있는 권리

**정답 4번**

**쟁점**

이 문제는 개인정보 자기결정권의 의미에 관한 문제이다. 핵심은 정보주체가 자신의 정보 처리 범위를 스스로 통제하는 권리와 개인정보처리자에게 부과되는 보호 책임을 구별하는 것이다.

**용어 풀이**

개인정보 자기결정권은 자신에 관한 정보가 언제, 누구에게, 어느 범위까지 알려지고 이용되도록 할 것인지를 정보주체가 스스로 결정할 수 있는 권리이다.

**핵심 구분**

개인정보 자기결정권의 주체는 정보주체이며, 핵심어는 자신의 정보에 대한 통제와 결정이다. 반면 최소 수집, 재식별 위험에 대한 조치, 분실·유출 방지를 위한 안전성 확보는 개인정보를 처리하는 자의 보호 원칙이나 책임에 해당한다.

NoteBase

**선지별 해설**

① X
처리 목적 달성에 필요한 최소한의 개인정보만 수집한다는 내용은 최소 수집 원칙에 따른 개인정보처리자의 책임이다. 정보주체가 자신의 정보 공개·이용 범위를 스스로 정하는 권리의 정의가 아니다.
틀린 표현: 개인정보 자기결정권을 최소한의 개인정보만 수집해야 하는 책임으로 설명한 부분
올바른 표현: 최소한의 개인정보만 수집해야 하는 것은 개인정보처리자의 최소 수집 책임이다.

② X
특정 개인을 알아볼 수 있는 정보가 생성된 때 처리중지·회수·파기 등의 조치를 한다는 내용은 재식별 위험에 대응하는 처리자의 조치에 관한 것이다. 정보주체의 자기 통제권을 설명하지 않는다.
틀린 표현: 개인정보 자기결정권을 재식별 정보 발생 시 처리자가 부담하는 조치 의무로 설명한 부분
올바른 표현: 개인정보 자기결정권은 정보주체가 자신의 정보가 알려지고 이용되는 시기·대상·범위를 스스로 결정하는 권리이다.

③ X
개인정보의 분실·도난·유출·위조·변조·훼손을 막기 위해 안전성을 확보한다는 내용은 개인정보처리자의 안전성 확보 책임이다. 개인정보 자기결정권의 정의가 아니다.
틀린 표현: 개인정보 자기결정권을 개인정보의 안전성 확보 책임으로 설명한 부분
올바른 표현: 분실·도난·유출 등을 방지하기 위한 안전성 확보는 개인정보처리자의 보호 책임이다.

④ O
자신에 관한 정보가 언제, 어떻게, 어느 범위까지 수집·이용·공개될 수 있는지를 정보주체가 스스로 통제하고 결정할 수 있는 권리라는 설명은 개인정보 자기결정권의 의미에 부합한다.

**오답 포인트**

①과 ③은 개인정보 보호에 필요한 올바른 책임을 말하므로 정답처럼 보이지만, 문제는 일반적인 개인정보 보호 원칙이 아니라 개인정보 자기결정권의 정의를 묻는다. 권리의 주체가 정보주체인지, 의무의 주체가 개인정보처리자인지를 구별해야 한다.

**다시 나오면 이렇게 판단**

선지에서 '정보주체가 스스로 결정·통제한다'는 구조가 나타나면 개인정보 자기결정권으로 판단한다.
'최소한으로 수집한다', '안전성을 확보한다', '회수·파기한다'처럼 처리자의 행위를 요구하면 처리자의 보호 책임이나 처리 원칙으로 구분한다.

**암기 포인트**

자기결정권은 '내 정보의 언제·누구에게·어느 범위를 내가 결정한다'이다.

NoteBase

2. 다음 중 접근제어 원칙으로 옳지 않은 것은?
① 통신규약
② 최소 권한
③ 알 필요성
④ 직무 분리

**정답 1번**

**출제 포인트**

접근제어의 기본 원칙과 통신을 위한 기술적 규칙을 구별하는 문제이다.

**핵심 개념**

접근제어는 사용자가 정보나 시스템 자원에 접근할 수 있는 범위와 권한을 제한하는 보안 통제이다.
최소 권한은 업무 수행에 필요한 최소한의 권한만 부여하는 원칙이고, 알 필요성은 업무상 알아야 할 정보에만 접근을 허용하는 원칙이며, 직무 분리는 중요한 업무의 권한과 단계를 여러 사람에게 나누는 원칙이다.
통신규약은 장치 간 데이터 통신의 형식과 절차를 정한 약속으로, 접근제어 원칙이 아니다.

**선지별 해설**

① X — 통신규약은 장치나 시스템이 데이터를 주고받기 위해 정한 형식·절차·규칙이다. 접근 권한을 제한하는 원칙이 아니므로 틀린 표현이며, 올바르게는 '통신규약은 데이터 통신을 위한 약속이다'라고 해야 한다.
② O — 최소 권한은 사용자에게 직무 수행에 꼭 필요한 최소 범위의 권한만 부여하여 권한 오용과 피해 범위를 줄이는 접근제어 원칙이다.
③ O — 알 필요성은 사용자의 직무상 필요한 정보에 대해서만 접근을 허용하는 접근제어 원칙이다.
④ O — 직무 분리는 한 사람이 중요한 업무의 모든 권한과 절차를 독점하지 못하도록 역할을 나누어 오류와 부정을 방지하는 접근제어 원칙이다.

**오답 포인트**

①의 '통신규약'도 정보보호 분야에서 자주 등장하는 용어이므로 접근제어 원칙으로 착각하기 쉽다. 그러나 통신규약은 통신 방법에 관한 약속이고, 나머지 세 용어는 권한과 정보 접근의 범위를 통제하는 원칙이다.

**다시 나오면 이렇게 판단**

용어가 '누가 어떤 정보와 권한에 접근할 수 있는가'를 제한하면 접근제어 원칙으로 판단한다. 데이터 전달의 형식이나 절차를 정하는 용어라면 통신 규칙에 해당한다.

**암기 포인트**

접근제어는 최소 권한·알 필요성·직무 분리이고, 통신규약은 데이터 통신의 약속이다.

NoteBase

3. 다음 중 대칭키와 비대칭키에 대한 설명으로 가장 옳은 것은?
① 대칭키: 빠른 처리 속도
비대칭키: 키 교환의 장점
② 대칭키: 암호화 및 복호화 키가 같음
비대칭키: 3개 이상의 키가 필요
③ 대칭키: 키 교환의 어려움
비대칭키: MD5(Message-Digest 5) 알고리즘
④ 대칭키: DES(Data Encryption Standard) 알고리즘
비대칭키: 개인키 및 공개키 모두 공개

**정답 1번**

**출제 포인트**

대칭키 암호와 비대칭키 암호의 키 구성, 처리 속도, 키 배포 방식 및 대표 알고리즘을 구별하는 문제이다.

**핵심 개념**

대칭키 암호는 암호화와 복호화에 같은 비밀키를 사용하는 방식이다. 처리 속도가 빠르지만, 통신 상대에게 비밀키를 안전하게 전달하고 관리해야 하는 문제가 있다.
비대칭키 암호는 서로 대응하는 공개키와 개인키의 한 쌍을 사용하는 방식이다. 공개키는 공개할 수 있고 개인키는 소유자만 비밀로 보관하므로 키 배포에 유리하지만, 일반적으로 대칭키 방식보다 처리 속도가 느리다.

**선지별 해설**

① O — 대칭키 암호는 연산이 비교적 단순하여 처리 속도가 빠르다. 비대칭키 암호는 공개키를 공개하고 개인키만 비밀로 유지하므로 사전에 동일한 비밀키를 안전하게 공유해야 하는 부담을 줄여 키 교환·배포에 유리하다.
② X — '대칭키는 암호화 및 복호화 키가 같음'은 맞지만, '비대칭키는 3개 이상의 키가 필요'가 틀렸다. 올바르게는 비대칭키 암호에는 서로 대응하는 공개키와 개인키의 두 키가 필요하다.
③ X — '대칭키는 키 교환이 어려움'은 맞지만, '비대칭키는 MD5 알고리즘'이 틀렸다. 올바르게는 MD5는 비대칭키 암호 알고리즘이 아니라 입력값을 고정 길이 해시값으로 바꾸는 해시 함수이다. 비대칭키 암호의 대표 예로 RSA가 있다.
④ X — '대칭키는 DES 알고리즘'은 맞지만, '비대칭키는 개인키 및 공개키 모두 공개'가 틀렸다. 올바르게는 공개키만 공개하고 개인키는 소유자가 비밀로 보관한다.

**오답 포인트**

②~④는 앞부분의 대칭키 설명은 맞게 제시하고 뒷부분의 비대칭키 설명만 틀리게 만든 선지이다. 특히 MD5를 암호 알고리즘으로 오인하거나, '공개키'라는 명칭 때문에 개인키까지 공개한다고 판단하기 쉽다.

NoteBase

**다시 나오면 이렇게 판단**

먼저 키의 수와 공개 범위를 확인한다. 같은 비밀키 하나를 공유하면 대칭키, 공개키와 비밀로 보관하는 개인키의 한 쌍을 사용하면 비대칭키이다. 이어서 대칭키는 빠른 처리, 비대칭키는 키 배포에 유리하다는 차이를 적용한다. 알고리즘은 DES는 대칭키, RSA는 비대칭키, MD5는 해시 함수로 구분한다.

**암기 포인트**

대칭키는 같은 키·빠른 속도·키 전달 부담, 비대칭키는 공개키와 개인키·키 배포 용이, MD5는 암호가 아니라 해시이다.

NoteBase

4. 다음 중 랜섬웨어에 대한 설명으로 가장 옳지 않은 것은?
① 인질의 몸값을 나타내는 'ransom'과 'software'의 합성어
② 파일 암호화로 피해자는 파일의 읽기 및 실행 불가
③ 백업과 같은 사전대비가 중요
④ 24시간 후 복호화는 가능하나 많은 양의 정보 손실 발생

**정답 4번**

**출제 포인트**

랜섬웨어의 어원, 피해 방식, 예방책과 복구 가능성에 관한 설명을 구별하는 문제이다.

**핵심 개념**

랜섬웨어는 파일이나 시스템의 사용을 막은 뒤 이를 풀어 주는 대가로 금전을 요구하는 악성 소프트웨어이다. 파일 암호화형 랜섬웨어는 파일을 읽거나 실행하기 어렵게 만들며, 복호화 가능 여부와 시점은 복호화 키의 확보나 백업 상태 등에 따라 달라진다.

**선지별 해설**

① O
'ransom'은 몸값을, 'software'는 소프트웨어를 뜻하므로 두 단어가 결합한 명칭이라는 설명은 옳다.

② O
파일 암호화형 랜섬웨어는 피해자의 파일을 암호화하여 정상적으로 읽거나 실행하지 못하게 한다.

③ O
중요 파일을 공격 대상과 분리된 저장 매체나 안전한 저장소에 백업해 두면 감염 뒤 데이터를 복구하는 데 도움이 되므로 사전 대비가 중요하다.

④ X
틀린 표현은 '24시간 후 복호화는 가능'이다. 랜섬웨어는 24시간이 지나면 자동으로 복호화된다는 일반적인 원리가 없으며, 복호화 키나 정상 백업을 확보하지 못하면 복구가 불가능할 수도 있다. 올바르게는 '복호화 가능 여부와 시점은 복호화 키의 확보와 백업 상태 등에 따라 달라지며, 감염 직후부터 정보 손실과 업무 중단이 발생할 수 있다'이다.

NoteBase

### 오답 포인트

④는 랜섬웨어가 일정 시간이 지나면 복호화된다는 존재하지 않는 공통 규칙을 제시한다. 공격자가 제한 시간을 표시하는 경우와 24시간 뒤 실제로 복호화되는 것은 전혀 다른 내용이다.

### 다시 나오면 이렇게 판단

랜섬웨어 선지에서는 '반드시 복구된다', '일정 시간이 지나면 복호화된다'처럼 복구를 보장하는 표현을 먼저 확인한다. 복구는 키와 백업의 확보 여부에 달려 있으므로 이러한 단정은 일반적으로 틀린 설명이다.

### 암기 포인트

랜섬웨어는 몸값을 요구하는 악성 소프트웨어이며, 핵심 대비책은 분리 백업이고 복호화는 보장되지 않는다.

NoteBase

5. 다음 중 정보보호 서비스 개념으로만 묶인 것으로 가장 옳은 것은?
① 은닉성, 보안성, 다형성
② 가용성, 기밀성, 부인방지
③ 무결성, 효율성, 인증
④ 대응성, 보호성, 소유성

**정답 2번**

**출제 포인트**

정보보호 서비스에 해당하는 핵심 개념인 가용성, 기밀성, 무결성, 인증, 부인방지를 다른 일반 용어나 악성코드 관련 용어와 구별하는 문제이다.

**핵심 개념**

기밀성은 허가된 대상만 정보에 접근하게 하는 성질이다. 무결성은 정보가 권한 없이 변경되거나 훼손되지 않도록 정확성과 완전성을 보장하는 성질이다. 가용성은 허가된 사용자가 필요할 때 정보와 시스템을 이용할 수 있게 하는 성질이다. 인증은 통신 주체나 데이터 출처가 주장한 대상이 맞는지 확인하는 서비스이다. 부인방지는 송신이나 수신 등의 행위를 나중에 부인하지 못하도록 증거를 제공하는 서비스이다.

NoteBase

**선지별 해설**

① X
은닉성·보안성·다형성은 정보보호 서비스의 핵심 개념만으로 묶인 표현이 아니다. 특히 다형성은 주로 악성코드가 형태를 바꾸어 탐지를 피하는 특성을 가리키며, 보안성은 포괄적인 일반 표현이다. 올바르게는 기밀성·무결성·인증처럼 정보보호 서비스의 정식 개념으로 묶어야 한다.

② O
가용성은 필요할 때 이용할 수 있게 하고, 기밀성은 비인가 접근을 막으며, 부인방지는 통신 행위를 사후에 부인하지 못하게 한다. 세 용어가 모두 정보보호 서비스 개념에 해당한다.

③ X
무결성과 인증은 정보보호 서비스 개념이지만 효율성은 처리 자원이나 성능에 관한 일반적 평가 기준으로, 정보보호 서비스의 핵심 개념이 아니다. 올바르게는 효율성을 기밀성·가용성·부인방지 중 하나로 고쳐야 한다.

④ X
대응성·보호성·소유성은 이 문항에서 묻는 정보보호 서비스의 표준적인 핵심 명칭으로만 이루어진 묶음이 아니다. 올바르게는 가용성·기밀성·부인방지 또는 기밀성·무결성·인증처럼 핵심 서비스 개념으로 표현해야 한다.

**오답 포인트**

①의 보안성과 ④의 보호성은 정보보호와 관련 있어 보이지만 지나치게 포괄적인 일반 표현이다. ③은 무결성과 인증이라는 두 개의 맞는 용어 사이에 효율성을 끼워 넣었다. 각 묶음에서 익숙한 단어의 개수가 아니라 모든 용어가 핵심 서비스 개념인지 확인해야 한다.

**다시 나오면 이렇게 판단**

각 용어를 기밀성·무결성·가용성·인증·부인방지의 핵심 범주에 하나씩 대응시킨다. 이 범주에 대응하지 않는 성능 용어, 포괄적 일반 용어, 악성코드 특성 용어가 하나라도 섞이면 '정보보호 서비스 개념으로만 묶인 것'이 아니다.

**암기 포인트**

기밀성·무결성·가용성에 인증·부인방지를 더해 기억한다.

NoteBase

6. 다음 중 문서의 무결성 비교를 위하여 사용되는 해시 값(함수)의 성질에 대한 설명으로 가장 옳지 않은 것은?
   ① 입력되는 가변의 데이터에 대해서 고정 길이의 해시 값이 발생한다.
   ② 입력되는 데이터가 다르면 해시 값도 다르다.
   ③ 해시 값 복호화를 위해서는 대칭키 알고리즘만 가능하다.
   ④ 해시 값으로부터 원래의 데이터 복구가 불가능하다.

**정답 3번**

**출제 포인트**

해시 함수의 고정 길이 출력, 입력 변화에 대한 민감성, 일방향성, 무결성 검증 방식의 차이를 묻는 문제이다.

**핵심 개념**

해시 함수는 임의 길이의 입력을 일정한 길이의 해시 값으로 변환하는 일방향 함수이다. 입력이 조금만 달라져도 출력이 크게 달라지는 특성이 있으며, 원래 입력을 해시 값에서 역산하기는 계산상 매우 어렵다.
무결성 검증은 원본의 해시 값과 수신한 데이터의 해시 값을 비교하여 변경 여부를 확인하는 방식이다. 이때 기준 해시 값을 안전하게 보호해야 하며, 대칭키 기반의 MAC·HMAC이나 비대칭키 기반의 전자서명도 사용할 수 있다.

NoteBase

**선지별 해설**

① O
해시 함수는 입력 데이터의 길이와 관계없이 해당 알고리즘이 정한 고정 길이의 해시 값을 출력한다.

② O
이 문항에서는 서로 다른 입력이나 작은 입력 변화가 일반적으로 서로 다른 해시 값을 만든다는 입력 민감성을 설명한 선지로 보아 옳게 취급한다. 다만 해시 값의 길이는 유한하므로, 서로 다른 입력이 언제나 서로 다른 해시 값을 갖는다는 절대적 의미는 아니며 충돌 가능성은 존재한다.

③ X
틀린 표현은 '대칭키 알고리즘만 가능하다'이다. 해시를 이용한 무결성 확인은 단순 해시 비교, 대칭키 기반 MAC·HMAC, 비대칭키 기반 전자서명 등으로 구현할 수 있다. 올바르게는 '해시 값 보호와 무결성 검증에는 대칭키 방식뿐 아니라 비대칭키 방식 등도 사용할 수 있다'이다.

④ O
암호학적 해시 함수는 일방향성을 가지므로 해시 값만으로 원래 데이터를 복구하는 것은 계산상 불가능하도록 설계된다.

**오답 포인트**

③은 해시 함수 자체의 성질과 해시 값을 보호·인증하는 방법을 혼동하게 만든다. 무결성 검증 수단을 대칭키 방식 하나로 제한한 '만'이 결정적인 오류이다. 또한 ②를 충돌이 절대로 없다는 의미로 확대해서는 안 된다.

**다시 나오면 이렇게 판단**

해시 함수 문제에서는 먼저 '고정 길이 출력, 입력 변화에 민감, 일방향성'을 확인한다. 이어 '오직, 반드시, ~만'처럼 구현 방법을 하나로 제한하는 표현은 다른 방식이 가능한지 점검한다.

**암기 포인트**

해시는 고정 길이·민감한 변화·일방향성이고, 무결성 구현은 대칭키 방식만으로 제한되지 않는다.

NoteBase

7. 다음 중 개인정보의 가명처리에 대한 설명으로 가장 옳은 것은?
   ① 개인정보의 정당한 사용을 위하여 개인정보 소유자에게 권한을 위임받아 안전성 확보를 위한 행위를 처리하는 것
   ② 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것
   ③ 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 것
   ④ 개인정보의 수집 및 이용 목적의 범위를 넘어 정보를 제공받는 자의 이익을 위하여 위해 업무를 처리하는 것

**정답 2번**

**쟁점**

이 문제는 「개인정보 보호법」상 가명처리의 정의에 관한 문제이다. 핵심은 추가 정보 없이는 특정 개인을 알아볼 수 없게 만드는 처리와 개인정보처리자·처리·목적 외 이용 등의 개념을 구별하는 것이다.

**용어 풀이**

가명처리 = 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하여, 별도의 추가 정보 없이는 특정 개인을 알아볼 수 없도록 만드는 처리이다. 가명정보는 추가 정보를 사용·결합하면 원래 상태로 복원될 가능성이 있으므로 익명정보와 다르다.

**핵심 구분**

2022년 당시와 현행 「개인정보 보호법」 제2조 제1호의2는 가명처리를 '개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것'으로 규정한다. 판단 요소는 '일부 삭제 또는 대체'라는 방법과 '추가 정보 없이는 특정 개인을 식별할 수 없음'이라는 결과이다.

NoteBase

**선지별 해설**

① X
개인정보 소유자에게 권한을 위임받아 안전성 확보 행위를 하는 것은 법정 가명처리의 정의가 아니다. 법은 '개인정보 소유자'가 아니라 '정보주체'라는 용어를 사용하며, 권한 위임 여부도 가명처리의 정의 요소가 아니다.
틀린 표현: '개인정보 소유자에게 권한을 위임받아 안전성 확보를 위한 행위를 처리하는 것'
올바른 표현: '개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것'이다.

② O
개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하고, 추가 정보 없이는 특정 개인을 알아볼 수 없게 한다는 두 요소를 모두 담고 있으므로 법률상 가명처리의 정의와 일치한다.

③ X
이 문장은 가명처리의 방법이나 식별 불가능성에 관한 설명이 아니라 개인정보처리자의 정의 일부에 가깝다. 개인정보처리자는 업무 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통해 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 뜻한다.
틀린 표현: '업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 것'
올바른 표현: 위 요건을 갖추어 개인정보를 처리하는 '공공기관, 법인, 단체 및 개인 등'을 개인정보처리자라고 한다. 가명처리는 개인정보를 일부 삭제·대체하여 추가 정보 없이는 특정 개인을 알아볼 수 없도록 처리하는 것이다.

④ X
수집·이용 목적의 범위를 넘는 처리나 정보를 제공받는 자의 이익은 가명처리의 법정 정의 요소가 아니다. 가명처리 여부는 처리 목적이나 수익자가 아니라 삭제·대체 방법과 추가 정보 없이는 식별할 수 없는 상태인지로 판단한다.
틀린 표현: '수집 및 이용 목적의 범위를 넘어 정보를 제공받는 자의 이익을 위하여 위해 업무를 처리하는 것'
올바른 표현: '개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것'이다.

**오답 포인트**

③은 실제 법률상 개인정보처리자의 정의와 매우 비슷하여 가명처리의 정의로 착각하기 쉽다. 이 문제에서는 '누가 업무 목적으로 처리하는가'가 아니라 '어떤 방법으로 식별 가능성을 낮추는가'를 묻는다는 점이 함정이다.

NoteBase

### 다시 나오면 이렇게 판단

가명처리의 정의를 묻는 문제에서는 먼저 '일부 삭제 또는 일부·전부 대체'가 있는지 확인하고, 이어 '추가 정보 없이는 특정 개인을 알아볼 수 없음'이 명시되었는지 확인한다. 두 요소가 모두 있는 선지를 선택한다.

### 암기 포인트

가명처리는 '삭제·대체 + 추가 정보 없이는 식별 불가'이다.

NoteBase

8. 다음 중 리눅스에서 제공하는 방화벽 메커니즘과 호스트기반 접근 제어 시스템의 조합으로 옳은 것은?
① IPLogger, Wireshark
② IPtables, TCP Wrapper
③ Scanner, Sniffer
④ Portmap, Snort

**정답 2번**

**출제 포인트**

리눅스 보안 도구의 기능을 구분하여 방화벽 메커니즘과 호스트기반 접근 제어 시스템을 올바르게 연결하는 문제이다.

**핵심 개념**

IPtables: 리눅스 커널의 Netfilter 기능을 이용해 패킷을 허용·차단하는 방화벽 관리 도구이다.
TCP Wrapper: 네트워크 서비스에 접속하는 호스트를 기준으로 접근을 허용하거나 거부하는 호스트기반 접근 제어 방식이다.
따라서 방화벽 메커니즘은 IPtables, 호스트기반 접근 제어 시스템은 TCP Wrapper에 해당한다.

NoteBase

**선지별 해설**

① X
IPLogger는 IP 관련 접속 정보를 기록하는 로깅 도구이고 Wireshark는 패킷을 수집·분석하는 도구이므로, 방화벽 메커니즘과 호스트기반 접근 제어 시스템의 조합이 아니다. 틀린 조합 'IPLogger, Wireshark'는 'IPtables, TCP Wrapper'로 고쳐야 한다.

② O
IPtables는 패킷 필터링 규칙을 설정하는 리눅스 방화벽 도구이고 TCP Wrapper는 접속 호스트를 기준으로 서비스 접근을 통제하므로 두 기능의 조합이 정확하다.

③ X
Scanner는 시스템이나 네트워크의 포트·취약점 등을 탐색하는 도구이고 Sniffer는 네트워크 패킷을 포착·분석하는 도구이므로 요구된 두 기능에 해당하지 않는다. 틀린 조합 'Scanner, Sniffer'는 'IPtables, TCP Wrapper'로 고쳐야 한다.

④ X
Portmap은 RPC 프로그램 번호를 포트 번호에 대응시키는 서비스이고 Snort는 네트워크 트래픽을 분석해 침입을 탐지·방지하는 도구이므로 요구된 조합이 아니다. 틀린 조합 'Portmap, Snort'는 'IPtables, TCP Wrapper'로 고쳐야 한다.

**오답 포인트**

Wireshark·Sniffer·Snort처럼 네트워크 트래픽을 다루는 도구를 모두 방화벽으로 묶는 것이 함정이다. 패킷을 관찰·분석하거나 침입을 탐지하는 기능과, 규칙에 따라 패킷을 허용·차단하는 방화벽 기능을 구분해야 한다.

**다시 나오면 이렇게 판단**

'패킷 필터링 규칙으로 허용·차단'은 IPtables, '접속을 시도한 호스트를 기준으로 서비스 접근 통제'는 TCP Wrapper로 판단한다. 분석·탐지·탐색·포트 매핑 도구는 이 조합에서 제외한다.

**암기 포인트**

IPtables는 패킷 방화벽, TCP Wrapper는 호스트별 서비스 접근 통제이다.

NoteBase

9. 다음 중 인증시스템의 주요 기능인 인증을 제공하는 인증 수단과 예제로 가장 옳지 않은 것은?
① 알고 있는 것: 패스워드
② 자신의 신체: 홍채
③ 문제 및 계산: 인공 지능
④ 가지고 있는 것: 공인(공동) 인증서

**정답 3번**

**출제 포인트**

인증 수단을 사용자가 알고 있는 것, 신체적 특징, 수행하는 응답, 가지고 있는 것으로 구분하고 각 예가 올바르게 연결되었는지를 묻는 문제이다.

**핵심 개념**

알고 있는 것은 패스워드나 PIN처럼 사용자의 기억에 근거한 지식 요소이다. 자신의 신체는 홍채나 지문처럼 개인의 고유한 생체 특징을 이용하는 요소이다. 문제 및 계산은 제시된 문제에 사용자가 올바른 답이나 반응을 내놓는지를 확인하는 방식이다. 가지고 있는 것은 인증서, 보안 토큰처럼 사용자가 소지하거나 통제하는 매체·자격 증명을 이용하는 요소이다.

**선지별 해설**

① O — 패스워드는 사용자가 기억하여 입력하는 비밀정보이므로 '알고 있는 것'에 해당한다.
② O — 홍채는 개인마다 고유한 신체적 특징을 이용하므로 생체 인증의 예에 해당한다.
③ X — 틀린 표현은 '문제 및 계산: 인공 지능'이다. 인공 지능은 사용자의 신원을 증명하는 인증 요소가 아니라 문제를 처리하는 기술이다. 올바르게는 '문제 및 계산: 사용자가 제시된 문제에 대해 수행한 계산이나 응답'처럼 연결해야 한다.
④ O — 공인인증서 또는 공동인증서는 사용자가 파일이나 저장매체 등에 보유하고 통제하는 전자적 자격 증명으로 분류되므로 '가지고 있는 것'의 예에 해당한다.

**오답 포인트**

③의 '인공 지능'은 문제와 계산을 수행할 수 있다는 연상 때문에 그럴듯하지만, 인증의 대상인 사용자가 제시하는 증거가 아니다. 인증 기술과 사용자의 인증 요소를 혼동한 것이 함정이다.

**다시 나오면 이렇게 판단**

각 예가 사용자에게서 얻는 신원 증거인지 확인한다. 기억한 비밀이면 지식 요소, 신체 특징이면 생체 요소, 소지·통제하는 자격 증명이면 소유 요소, 제시된 과제에 대한 답이나 행동이면 수행 요소로 판단한다.

NoteBase

**암기 포인트**

패스워드는 기억, 홍채는 신체, 인증서는 소유, 문제의 답은 수행이다. 인공 지능 자체는 사용자 인증 요소가 아니다.

NoteBase

10. 다음 중 블록체인 네트워크의 합의 알고리즘에 대한 공격으로 가장 옳은 것은?
① 51% 공격
② 코인 Flooding 공격
③ 지갑 파밍 공격
④ 2:8 공격

**정답 1번**

**출제 포인트**

블록체인 합의 과정에서 공격자가 합의 결정력을 장악하는 대표적 공격을 구별하는 문제이다.

**핵심 개념**

51% 공격은 작업증명 방식 등에서 한 주체 또는 집단이 합의에 필요한 연산력과 같은 자원의 과반을 확보하여 정상 체인보다 우세한 체인을 만들 수 있게 되는 공격이다. 이 경우 최근 거래의 순서를 바꾸거나 자신의 거래를 되돌려 이중 지불을 시도할 수 있다. 핵심 구별 기준은 단순히 거래량이나 지갑 수를 늘리는 것이 아니라 합의 결정에 사용되는 자원의 과반을 장악하는지이다.

**선지별 해설**

① O — 51% 공격은 공격자가 합의 자원의 과반을 장악하여 블록 생성과 체인 선택에 영향력을 행사하는 대표적인 합의 알고리즘 공격이다.
② X — 틀린 표현은 '코인 Flooding 공격'이다. 다량의 거래나 데이터를 보내 네트워크 처리를 방해하는 플러딩은 통신·처리 자원을 소모시키는 가용성 공격에 가깝고, 합의 결정력의 과반을 장악하는 공격을 뜻하지 않는다. 올바르게는 합의 자원의 과반을 장악하는 '51% 공격'이다.
③ X — 틀린 표현은 '지갑 파밍 공격'이다. 다수의 지갑을 만들거나 보상 획득을 노리는 행위만으로는 블록체인의 합의 결정권을 장악하지 못하므로 대표적인 합의 알고리즘 공격이 아니다. 올바르게는 연산력 등 합의 자원을 과반 확보하는 '51% 공격'이다.
④ X — 틀린 표현은 '2:8 공격'이다. 2:8은 합의 자원의 지배 기준을 나타내는 표준적인 블록체인 공격 명칭이 아니다. 올바르게는 공격자가 과반의 합의 자원을 확보한다는 뜻의 '51% 공격'이다.

**오답 포인트**

②의 Flooding처럼 실제 보안 공격에 쓰이는 용어가 포함되어 있어도 곧바로 합의 알고리즘 공격이 되는 것은 아니다. 이 문항에서는 네트워크를 혼잡하게 하는 공격과 합의 결정력을 장악하는 공격을 구분해야 한다.

NoteBase

### 다시 나오면 이렇게 판단

공격 설명에서 해시 파워, 지분 등 합의 자원의 과반 장악과 체인 재구성 가능성이 핵심이면 51% 공격으로 판단한다. 트래픽 폭증, 다량 거래, 지갑 대량 생성만 언급되면 합의 장악 공격과 구별한다.

### 암기 포인트

합의 자원의 과반 장악은 51% 공격, 네트워크 혼잡은 플러딩 공격이다.

NoteBase

11. 다음 중 컴퓨터 바이러스에 대한 설명으로 가장 옳지 않은 것은?
① 원시형: 단순하게 자기복제 기능과 데이터 파괴 기능만을 가지고 있다.
② 은폐형: 바이러스 코드를 암호화하여 코드를 은닉한 바이러스이다.
③ 다형성: 프로그램이 실행될 때마다 바이러스 코드를 변경한다.
④ 매크로: 주로 오피스 프로그램의 매크로 기능을 통해 감염된다.

**정답 2번**

**출제 포인트**

컴퓨터 바이러스를 원시형·은폐형·다형성·매크로형으로 구분하고, 각 유형의 핵심 작동 방식이 올바르게 연결되었는지를 묻는 문제이다.

**핵심 개념**

원시형은 자기복제와 데이터 파괴 같은 기본 기능만 수행하는 단순한 바이러스이다.
은폐형은 감염 사실을 숨기기 위해 운영체제의 동작이나 정보 확인 과정에 개입하여 정상 상태처럼 보이게 하는 바이러스이다.
암호형은 바이러스 코드를 암호화하여 코드의 형태를 숨기는 바이러스이다.
다형성 바이러스는 실행이나 감염 때마다 코드 형태를 바꾸어 동일한 패턴으로 탐지하기 어렵게 한다.
매크로 바이러스는 문서 프로그램의 매크로 기능을 이용하여 문서 파일 등을 감염시킨다.

**선지별 해설**

① O — 원시형 바이러스는 구조가 단순하며 자기복제와 데이터 파괴 같은 기본적인 기능을 중심으로 동작한다.
② X — 틀린 표현은 '바이러스 코드를 암호화하여 코드를 은닉한 바이러스'이다. 이는 은폐형이 아니라 암호형 바이러스의 설명이다. 은폐형 바이러스는 감염으로 달라진 파일 크기나 시스템 정보 등을 정상인 것처럼 보이게 하여 감염 사실을 숨긴다.
③ O — 다형성 바이러스는 실행 또는 감염이 반복될 때마다 복호화 부분이나 코드 형태를 변화시켜 고정된 바이러스 패턴에 의한 탐지를 어렵게 한다.
④ O — 매크로 바이러스는 워드프로세서나 스프레드시트 같은 오피스 프로그램의 매크로 기능을 이용하여 문서에 감염되고 실행된다.

NoteBase

**오답 포인트**

②의 '은닉'이라는 말만 보고 은폐형으로 판단하기 쉽다. 그러나 분류 기준은 숨기는 대상과 방식이다. 바이러스 코드 자체를 암호화하는 것은 암호형이고, 감염으로 생긴 시스템의 변화를 정상처럼 보이게 하는 것은 은폐형이다.

**다시 나오면 이렇게 판단**

선지의 핵심 동사를 기준으로 구분한다. '기본 복제·파괴'는 원시형, '감염 흔적 숨김'은 은폐형, '코드 암호화'는 암호형, '실행·감염 때마다 형태 변경'은 다형성, '문서의 매크로 이용'은 매크로형에 연결한다.

**암기 포인트**

은폐형은 감염 흔적을 숨기고, 암호형은 코드를 암호화하며, 다형성은 코드 형태를 계속 바꾼다.

NoteBase

12. 다음 중 포렌식으로 증거를 획득할 때 지켜야 할 기본 원칙에 대한 설명으로 가장 옳지 않은 것은?
① 정당성의 원칙: 모든 증거는 적법한 절차를 거쳐서 얻은 것이어야 한다.
② 신속성의 원칙: 컴퓨터 내부의 정보는 휘발성을 가진 것이 많기 때문에 신속해야 한다.
③ 연계 보관성의 원칙: 증거를 획득한 뒤에는 이송, 분석, 보관, 법정제출이라는 일련의 과정이 명확해야 한다.
④ 무결성의 원칙: 수집된 증거는 경찰 및 검찰이 관여한 경우에만 변경 가능하다.

**정답 4번**

**출제 포인트**

포렌식 증거를 획득하고 다룰 때 지켜야 할 정당성, 신속성, 연계 보관성, 무결성의 의미를 구별하는 문제이다.

**핵심 개념**

정당성은 증거를 적법한 절차에 따라 획득해야 한다는 원칙이다.
신속성은 휘발성 정보가 사라지거나 바뀌기 전에 신속하게 확보해야 한다는 원칙이다.
연계 보관성은 증거의 이송·분석·보관·법정 제출 전 과정과 취급자를 기록하여 증거의 흐름을 명확히 해야 한다는 원칙이다.
무결성은 획득한 증거가 원래 상태에서 변경·훼손되지 않았음을 보장해야 한다는 원칙이다.

**선지별 해설**

① O — 정당성의 원칙은 증거를 적법한 절차에 따라 획득해야 한다는 뜻이므로 옳다.

② O — 컴퓨터의 메모리나 실행 상태처럼 휘발성이 큰 정보는 시간이 지나면 소실되거나 변할 수 있으므로 신속히 확보해야 한다.

③ O — 연계 보관성의 원칙은 증거 획득 이후 이송, 분석, 보관, 법정 제출에 이르는 과정과 취급 이력을 명확히 유지하는 것이므로 옳다.

④ X — 틀린 표현은 '경찰 및 검찰이 관여한 경우에만 변경 가능하다'이다. 무결성의 원칙상 수집된 증거는 수사기관의 관여 여부와 관계없이 원본 상태가 변경되지 않도록 보존해야 한다. 분석이 필요할 때에는 원본을 보존하고 검증된 복제본을 사용하며, 처리 과정도 기록해야 한다.

NoteBase

**오답 포인트**

④는 경찰이나 검찰이 관여하면 증거 변경이 허용되는 것처럼 예외를 만들었다. 무결성은 누가 관여했는지가 아니라 증거가 원래 상태 그대로 유지되고 변경 여부를 검증할 수 있는지를 따지는 원칙이다.

**다시 나오면 이렇게 판단**

적법한 획득은 정당성, 소실 전 확보는 신속성, 취급 과정의 기록은 연계 보관성, 원본의 비변경 보장은 무결성으로 대응시킨다. 무결성에 특정 기관의 관여를 이유로 증거 변경을 허용하는 표현이 나오면 틀린 설명으로 판단한다.

**암기 포인트**

정당성은 적법하게, 신속성은 사라지기 전에, 연계 보관성은 과정이 끊기지 않게, 무결성은 원본이 바뀌지 않게 한다.

NoteBase

13 RSA 공개키 암호에서 2개의 소수 p=3와 q=7가 주어지고 복호화 키(d) 5로 고정했을 때, 암호화 키(e)값과 메시지 2에 대한 암호문 값(C)은?

① e = 3 , C = 5
② e = 4 , C = 7
③ e = 5 , C = 11
④ e = 6 , C = 15

**정답 3번**

### 출제 포인트

RSA에서 두 소수로 오일러 피 함수 값을 구한 뒤, 복호화 키의 모듈러 역원인 암호화 키와 암호문을 계산하는 문제이다.

### 조건 정리

주어진 값: $p = 3$, $q = 7$, 복호화 키 $d = 5$, 메시지 $m = 2$이다.
구해야 할 값: 암호화 키 $e$와 암호문 $C$이다.
주의할 조건: $n = pq$이고, $e$와 $d$는 $\varphi(n)$을 법으로 서로 모듈러 역원이어야 한다.

### 사용할 공식

$n = pq, \qquad \varphi(n) = (p-1)(q-1)$
ed≡1±od(n)
C≡ m^e±od n
두 소수로 만든 RSA 모듈러스이므로 $\varphi(n)$을 계산하고, 공개 지수와 개인 지수의 역원 관계로 $e$를 정한 다음 메시지를 공개 지수만큼 거듭제곱하여 암호문을 구한다.

### 계산 과정

1. $n = 3 \times 7 = 21$이고, $\varphi(n) = (3-1)(7-1) = 12$이다.
2. 5e≡1±od12를 만족해야 한다. 5×5=25≡1±od12이므로 $e = 5$이다.
3. C≡2^5±od21=32±od21=11이다. 따라서 $e = 5$, $C = 11$이다.

NoteBase

**선지 판단**

① X — $e = 3$이면 5e=15≡3±od12이므로 역원 조건을 만족하지 않는다. 또한 2^321=8이므로 $C = 5$도 아니다. 올바르게는 $e = 5$, $C = 11$이다.
② X — $e = 4$이면 5e=20≡8±od12이므로 역원 조건을 만족하지 않는다. 또한 2^421=16이므로 $C = 7$도 아니다. 올바르게는 $e = 5$, $C = 11$이다.
③ O — 5×5≡1±od12이고, 2^521=11이므로 두 값이 모두 맞는다.
④ X — $e = 6$이면 5e=30≡6±od12이므로 역원 조건을 만족하지 않는다. 또한 2^621=1이므로 $C = 15$도 아니다. 올바르게는 $e = 5$, $C = 11$이다.

**오답 포인트**

ed≡1±od n으로 잘못 계산하는 것이 핵심 함정이다. 역원 관계의 법은 $n = 21$이 아니라 $\varphi(n) = 12$이며, 암호문 계산에서만 $n = 21$을 법으로 사용한다.

**다시 나오면 이렇게 판단**

RSA 키 계산은 $n$과 $\varphi(n)$ 계산 → ed≡1±od(n)로 $e$ 결정 → C≡ m^e±od n 계산 순서로 판단한다.

**암기 포인트**

키의 역원은 $\varphi(n)$을 법으로, 암호화 거듭제곱은 $n$을 법으로 계산한다.

NoteBase

14. 미국 NIST가 표준으로 제정한 AES(Advanced Encryption Standard) 암호의 특징으로 가장 옳지 않은 것은?
① 평문과 암호문의 크기가 128비트인 블록 암호이다.
② 키는 128비트, 192비트, 256비트 중 선택하여 사용한다.
③ Substitution-and-Permutation Network 형태의 암호 체계이다.
④ Weak Key가 존재한다.

**정답 4번**

**출제 포인트**

AES의 블록 크기, 키 길이, 암호 구조, 약한 키(Weak Key) 존재 여부를 구분하는 문제이다.

**핵심 개념**

AES는 128비트 크기의 데이터 블록을 암호화하는 대칭키 블록 암호이다. 키 길이는 128비트, 192비트, 256비트 중 하나이며, 대치(substitution)와 순열(permutation)을 반복하는 SPN(Substitution-and-Permutation Network) 구조를 사용한다. AES에는 DES에서 문제 되는 것과 같은 알려진 Weak Key가 없다.

**선지별 해설**

① O - AES는 평문 128비트 블록을 암호문 128비트 블록으로 변환하므로 평문 블록과 암호문 블록의 크기는 모두 128비트이다.
② O - AES가 지원하는 키 길이는 128비트, 192비트, 256비트이다. 키 길이에 따라 라운드 수는 각각 10회, 12회, 14회가 된다.
③ O - AES는 대치와 순열을 여러 라운드에 걸쳐 반복하는 SPN 형태의 암호 체계이다.
④ X - 틀린 표현은 ‘Weak Key가 존재한다’이다. 올바르게는 AES에는 DES처럼 알려진 Weak Key가 존재하지 않는다고 해야 한다.

**오답 포인트**

‘블록 크기’와 ‘키 길이’를 혼동하기 쉽다. AES의 블록 크기는 항상 128비트이지만 키 길이는 128비트, 192비트, 256비트 중에서 선택한다. 또한 Weak Key는 DES의 대표적 취약점이므로 이를 AES의 특징으로 옮겨 붙이면 안 된다.

NoteBase

**다시 나오면 이렇게 판단**

AES의 특징은 '블록 128비트, 키 128·192·256비트, SPN 구조, 알려진 Weak Key 없음'의 네 기준으로 판단한다. 블록 크기와 키 길이를 먼저 분리한 뒤 각 선지를 대조하면 된다.

**암기 포인트**

AES는 블록 128, 키 128·192·256, SPN, Weak Key 없음이다.

NoteBase

15. 다음 중 내부자 공격 등을 방지하는 영지식 증명 기법의 조건에 가장 해당하지 않는 성질은?
① 완전성(completeness)
② 정당성(soundness)
③ 유일성(uniqueness)
④ 영지식성(zero knowledge)

**정답 3번**

**출제 포인트**

영지식 증명이 갖추어야 할 표준 성질인 완전성, 정당성, 영지식성을 구별하는 문제이다.

**핵심 개념**

완전성(completeness): 명제가 참이고 증명자와 검증자가 절차를 정직하게 따르면 검증자가 증명을 받아들이는 성질이다.
정당성(soundness): 명제가 거짓이면 부정한 증명자가 검증자를 속여 증명을 받아들이게 하기 어려운 성질이다.
영지식성(zero knowledge): 검증자가 명제가 참이라는 사실 외에는 비밀에 관한 추가 정보를 얻지 못하는 성질이다.
영지식 증명의 표준 세 성질은 완전성·정당성·영지식성이며, 유일성은 이에 포함되지 않는다.

**선지별 해설**

① O — 완전성은 참인 명제에 대해 정직한 증명자가 정직한 검증자를 설득할 수 있게 하는 영지식 증명의 표준 성질이다.
② O — 정당성은 거짓인 명제를 참인 것처럼 주장하는 부정한 증명자가 검증자를 속이지 못하게 하는 표준 성질이다.
③ X — 유일성은 영지식 증명의 표준 조건이 아니다. 틀린 표현은 '유일성'이며, 올바르게는 영지식 증명의 조건을 '완전성·정당성·영지식성'으로 정리한다.
④ O — 영지식성은 검증 과정에서 명제의 참·거짓 판단에 필요한 사실 외의 비밀 정보가 드러나지 않게 하는 표준 성질이다.

**오답 포인트**

'유일성'이 보안에 필요한 일반적 성질처럼 보이는 점이 함정이다. 영지식 증명에서는 증명이나 해답이 하나뿐일 필요가 없으며, 핵심은 참이면 통과하고, 거짓이면 속이기 어렵고, 비밀은 새지 않는다는 세 조건이다.

NoteBase

**다시 나오면 이렇게 판단**

영지식 증명의 조건을 묻는 경우 ‘참인 명제의 수락=완전성’, ‘거짓 명제의 기만 방지=정당성’, ‘추가 정보의 비공개=영지식성’으로 대응시킨다. 이 세 범주에 들지 않는 유일성은 표준 조건에서 제외한다.

**암기 포인트**

참이면 통과(완전성), 거짓이면 기만 차단(정당성), 비밀은 비공개(영지식성)이다.

NoteBase

16. 다음 중 개인정보 보호법에 위배되지 않는 것은?
① 지인으로부터 수신한 제3자의 개인정보를 이용하여 주식 투자에 사용하였다.
② 돌아가신 아버님이 생전에 좋아하시던 곳이나 취미를 알기 위하여 관련 정보를 수집하였다.
③ 상사의 책상 위에 기록되어있는 상사의 ID와 패스워드를 이용하여 상사가 사용하는 컴퓨터를 접근하였다.
④ 인터넷상에 유통되는 개인정보를 활용하여 본인의 대리 인증 목적으로 활용하였다

**정답 2번**

### 쟁점

이 문제는 개인정보 보호법상 개인정보의 범위와 부정한 개인정보 이용의 금지를 묻는 문제이다. 핵심은 개인정보가 원칙적으로 살아 있는 개인에 관한 정보라는 점과 타인의 개인정보를 권한 없이 이용해서는 안 된다는 점을 구별하는 것이다.

### 용어 풀이

개인정보 = 살아 있는 개인에 관한 정보로서 그 개인을 알아볼 수 있거나 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보 등을 말한다.
개인정보 처리 = 개인정보를 수집·이용하거나 그 밖에 이와 유사한 행위를 하는 것을 말한다.

### 핵심 구분

현행 개인정보 보호법 제2조는 개인정보를 살아 있는 개인에 관한 정보로 정의한다. 따라서 사망한 사람만을 알아보기 위한 정보는 원칙적으로 이 법이 보호하는 개인정보에 해당하지 않는다. 다만 그 정보가 유족 등 살아 있는 사람을 식별하는 정보이기도 하다면 그 부분은 개인정보가 될 수 있다. 한편 같은 법 제59조는 부정한 수단으로 개인정보를 취득하는 행위와 정당한 권한 없이 다른 사람의 개인정보를 이용하는 행위를 금지한다.

NoteBase

**선지별 해설**

① X
지인에게서 받은 제3자의 개인정보를 그 제3자의 동의나 적법한 근거 없이 주식 투자에 이용하는 것은 타인의 개인정보를 정당한 권한 없이 이용하는 행위에 해당한다.
틀린 표현: 제3자의 개인정보를 이용하여 주식 투자에 사용하였다.
올바른 표현: 제3자의 동의나 법률상 근거 등 정당한 권한이 있는 범위에서만 그 개인정보를 이용하여야 한다.

② O
아버지가 이미 사망하였으므로 아버지가 생전에 좋아한 꽃이나 취미에 관한 정보는 원칙적으로 '살아 있는 개인에 관한 정보'가 아니다. 제시된 목적과 내용만으로는 개인정보 보호법 위반에 해당하지 않는다.

③ X
상사의 ID와 패스워드를 허락 없이 이용하여 상사의 컴퓨터에 접근하는 것은 타인의 식별·인증 정보를 부정하게 취득·이용하는 행위이다.
틀린 표현: 상사의 ID와 패스워드를 이용하여 상사가 사용하는 컴퓨터에 접근하였다.
올바른 표현: 상사의 명시적인 허락이나 업무상 권한 없이 상사의 ID와 패스워드를 이용하여 컴퓨터에 접근해서는 안 된다.

④ X
인터넷에 유통되는 개인정보라고 하여 누구나 자유롭게 이용할 수 있는 것은 아니다. 이를 본인인 것처럼 대리 인증에 사용하면 정당한 권한 없이 타인의 개인정보를 이용하는 행위가 된다.
틀린 표현: 인터넷상에 유통되는 개인정보를 본인의 대리 인증 목적으로 활용하였다.
올바른 표현: 인터넷에 공개·유통된 개인정보도 정당한 권한 없이 본인 사칭이나 대리 인증에 활용해서는 안 된다.

**오답 포인트**

'정보를 수집했다'는 행위만 보고 ②를 위반으로 판단하기 쉽다. 그러나 먼저 그 정보가 살아 있는 개인에 관한 개인정보인지 확인해야 한다. 반대로 ①과 ④처럼 타인의 정보가 이미 전달되거나 인터넷에 유통되고 있다는 사정만으로 이용 권한이 생기는 것은 아니다.

**다시 나오면 이렇게 판단**

먼저 정보의 대상이 살아 있는 개인인지 확인하고, 개인정보라면 수집·이용에 정보주체의 동의나 법률상 근거 등 정당한 권한이 있는지를 차례로 판단한다. 사망자 정보는 원칙적으로 제외되지만, 살아 있는 유족을 식별하는 정보가 함께 포함되는지는 별도로 확인한다.

NoteBase

**암기 포인트**

개인정보는 ‘살아 있는 개인’의 정보이고, 공개·전달된 정보도 이용 권한까지 공개된 것은 아니다.

NoteBase

17. 공격자가 존재하는 공개된 채널을 통해 보안 통신을 원하는 갑과 을에만 비밀정보를 생성하는 Diffie Hellman 키 공유 방식에서 공개변수로 소수 p=11, 생성원 g=3이 주어졌다. 갑과 을의 개인키가 각각 2와 3일 때 공유하는 비밀 값은?

① 4
② 6
③ 8
④ 10

**정답 1, 2, 3, 4번**

**출제 포인트**

Diffie-Hellman 키 공유에서 상대방의 공개키에 자신의 개인키를 거듭제곱한 뒤 공개 소수로 나눈 나머지를 구하는 문제이다. 계산상 비밀 값은 3이지만 이 값이 보기에 없으므로, 제시된 답안표에서는 네 선지가 모두 정답으로 인정된다.

**조건 정리**

공개 소수: $p = 11$
생성원: $g = 3$
갑의 개인키: $a = 2$
을의 개인키: $b = 3$
구해야 할 값: 갑과 을이 공유하는 비밀 값 $K$

**사용할 공식**

갑의 공개키는 A=g^a p, 을의 공개키는 B=g^b p이다. 공유 비밀 값은 다음과 같다.
K=B^a p=A^b p=g^ab p
양쪽이 상대방의 공개키에 자신의 개인키를 적용하면 모두 $g^{ab}$가 되므로 같은 값을 얻는다.

**계산 과정**

1. 갑의 공개키는 A=3^2 11=9이다.
2. 을의 공개키는 B=3^3 11=27 11=5이다.
3. 갑이 구한 공유 비밀 값은 K=B^a 11=5^2 11=25 11=3이다.
4. 을이 구해도 K=A^b 11=9^3 11=729 11=3으로 일치한다.

NoteBase

**선지 판단**

① X — 4는 계산 결과 3과 다르다. 올바르게는 '공유하는 비밀 값은 3이다'이다. 다만 보기에 3이 없으므로 제시된 답안표에서는 ①도 정답으로 인정된다.
② X — 6은 3^2×3 11=3과 다르다. 올바르게는 6이 아니라 3이다. 다만 보기에 3이 없으므로 제시된 답안표에서는 ②도 정답으로 인정된다.
③ X — 8은 갑이 계산한 5^2 11=3과 다르다. 올바르게는 8이 아니라 3이다. 다만 보기에 3이 없으므로 제시된 답안표에서는 ③도 정답으로 인정된다.
④ X — 10은 을이 계산한 9^3 11=3과 다르다. 올바르게는 10이 아니라 3이다. 다만 보기에 3이 없으므로 제시된 답안표에서는 ④도 정답으로 인정된다.
따라서 수학적 계산값은 3이고, 제시된 답안표상 정답은 1번, 2번, 3번, 4번이다.

**오답 포인트**

생성원 3과 개인키를 단순히 곱하거나 더하는 것이 아니라 모듈러 거듭제곱을 해야 한다. 또한 $3^{2\times3} = 729$를 그대로 답으로 삼지 않고 반드시 11로 나눈 나머지 3을 구해야 한다. 이 문항은 계산값 3이 보기에 없다는 점이 핵심적인 보기 구성 오류이다.

**다시 나오면 이렇게 판단**

먼저 각자의 공개키 g^a p, g^b p를 구한 뒤, 상대 공개키에 자신의 개인키를 거듭제곱하여 다시 *p*로 나눈다. 마지막에는 양쪽 계산이 같은지와 계산값이 실제 보기에 존재하는지를 함께 확인한다.

**암기 포인트**

Diffie-Hellman의 공유 비밀은 K=g^ab p이다. 이 문항에서는 3^6 11=3이다.

NoteBase

18. 다음 중 부채널 공격에 해당하지 않는 것은?
① 공격 대상 장비에서 암호 연산에 소요되는 시간이나 전력 소모 정보를 관찰하여 비밀 정보를 유추한다.
② 공격 대상 장비에서 방사되는 전자파 정보 등과 같은 무선 신호를 수집하여 비밀정보를 유추한다.
③ 비밀 정보가 가질 수 있는 모든 가용 공간에서 가능한 값을 모두 대입하여 탐색해 비밀 정보를 유추한다.
④ 정상적인 동작을 하고 있는 공격 대상 장비에 인위적으로 오동작을 발생하도록 하여 비밀 정보를 추출한다.

**정답 3번**

**출제 포인트**

부채널 공격과 전수조사 공격을 정보 획득 방식에 따라 구별하는 문제이다.

**핵심 개념**

부채널 공격: 암호 알고리즘의 수학적 구조를 직접 깨는 대신, 장비가 암호 연산을 수행할 때 드러나는 시간·전력·전자파·오류 결과 등의 부가 정보를 분석하여 비밀 정보를 알아내는 공격이다.
전수조사 공격: 가능한 키나 비밀값 후보를 차례로 모두 대입하여 정답을 찾는 공격이다. 물리적 누출 정보를 이용하지 않는다는 점에서 부채널 공격과 구별된다.

NoteBase

**선지별 해설**

① O
암호 연산 시간이나 전력 소모의 차이를 관찰하여 비밀 정보를 유추하므로 각각 타이밍 공격과 전력 분석 공격에 해당한다.

② O
장비가 동작할 때 방사되는 전자파 신호를 수집·분석하여 비밀 정보를 알아내므로 전자파 분석을 이용한 부채널 공격에 해당한다.

③ X
틀린 표현은 '모든 가용 공간에서 가능한 값을 모두 대입하여 탐색'하는 방식을 부채널 공격으로 본 부분이다. 이는 장비에서 새는 부가 정보를 분석하는 것이 아니라 후보값을 모두 시도하는 전수조사 공격이다. 올바르게는 '가능한 키나 비밀값 후보를 모두 대입하여 탐색하는 전수조사 공격이다'라고 해야 한다.

④ O
정상 동작 중인 장비에 의도적으로 오류를 일으키고 그 오류 결과를 분석하여 비밀 정보를 추출하는 오류 주입·오류 분석 공격에 해당한다. 장비의 물리적 동작에서 얻은 부가 정보를 이용하므로 이 문항에서 말하는 부채널 공격에 포함된다.

**오답 포인트**

③도 결국 비밀 정보를 찾는 공격이므로 부채널 공격처럼 보이지만, 판단 기준은 '무엇을 이용해 찾는가'이다. 시간·전력·전자파·오류 결과처럼 구현 과정에서 생기는 정보를 이용하면 부채널 공격이고, 가능한 값을 모두 대입하면 전수조사 공격이다.

**다시 나오면 이렇게 판단**

선지에서 관찰하거나 분석하는 대상부터 확인한다. 장비의 시간·전력·전자파·오류 결과를 이용하면 부채널 공격으로 판단하고, 후보값을 하나씩 모두 대입하면 전수조사 공격으로 판단한다.

**암기 포인트**

부채널은 장비가 흘린 흔적을 분석하고, 전수조사는 후보를 끝까지 대입한다.

NoteBase

19. 분산 반사 서비스 거부 공격(DRDoS, Distributed Reflection Denial of Service)의 설명으로 가장 옳지 않은 것은?
① 서비스의 응답 특성을 이용한 새로운 형태의 서비스 거부 공격이다.
② 공격을 시도하는 IP 근원지를 추적하기가 용이하다.
③ 별도의 에이전트 설치 없이 프로토콜 상의 취약점을 이용하여 정상적인 서비스를 운영하는 시스템을 공격 에이전트로 활용한다.
④ UDP 프로토콜을 사용하는 DNS, NTP, SNMP 등의 서비스는 반사와 증폭 공격 형태를 나타낸다.

**정답 2번**

**출제 포인트**

이 문제는 DRDoS의 반사·증폭 원리와 공격 근원지 추적의 난점을 묻는 문제이다.

**핵심 개념**

DRDoS는 공격자가 피해자의 IP 주소로 출발지 주소를 위조한 요청을 여러 정상 서버에 보내고, 그 서버들의 응답이 피해자에게 집중되도록 하는 분산 반사 서비스 거부 공격이다. 요청보다 큰 응답을 돌려주는 서비스를 이용하면 트래픽이 증폭되며, 공격자는 반사 서버 뒤에 숨어 실제 근원지 추적을 어렵게 한다.

**선지별 해설**

① O — DRDoS는 정상 서비스가 요청에 응답하는 특성을 역이용하여 응답 트래픽을 피해자에게 반사시키는 서비스 거부 공격이다.
② X — 틀린 표현은 'IP 근원지를 추적하기가 용이하다'이다. 실제로는 출발지 IP가 피해자의 주소로 위조되고 다수의 반사 서버를 거치므로 실제 공격 근원지 추적이 어렵다.
③ O — 공격 대상이나 반사 서버에 별도의 공격 에이전트를 설치하지 않고, 정상 운영 중인 서버의 프로토콜 특성이나 취약한 설정을 이용해 그 서버를 반사 서버로 활용할 수 있다.
④ O — DNS, NTP, SNMP처럼 UDP를 사용하는 서비스는 출발지 주소 위조가 쉽고 요청보다 큰 응답을 만들 수 있어 반사·증폭 공격에 악용될 수 있다.

NoteBase

**오답 포인트**

반사에 사용된 서버의 IP가 드러난다는 사실을 실제 공격자의 IP도 쉽게 확인된다는 뜻으로 오해하기 쉽다. 확인되는 것은 주로 응답을 보낸 반사 서버이며, 피해자 주소로 위조된 요청을 보낸 실제 공격자는 그 뒤에 숨는다.

**다시 나오면 이렇게 판단**

‘출발지 IP 위조 → 정상 서버가 피해자에게 응답 → 다수 서버의 응답 집중’ 구조를 먼저 확인한다. 이 구조이면 반사 서버 식별과 실제 공격자 추적을 구분하고, 요청보다 응답이 큰지는 증폭 여부로 판단한다.

**암기 포인트**

DRDoS는 피해자 IP로 위조하고, 정상 서버에 반사시키며, 큰 응답으로 증폭한다. 실제 공격자 추적은 어렵다.

NoteBase

20. Log4j 악성 코드에 대한 설명 및 대책 중 가장 옳지 않은 것은?

① 최초 제로데이 취약점(CVE-2021-44228)이 발견된 이후에도 다수의 추가 취약점이 발견되었다.

② 다양한 제품에 패키지 형태로 내장된 프로그램이라 발견하기가 대단히 어렵다.

③ 제품 패치 이후에도 내부 중요 시스템에 전반적인 비정상 프로세스 여부 등 다양한 관점에서 점검이 필요하다.

④ 사용자가 많은 공개 소프트웨어는 검증된 것으로 인식하고 자유롭게 사용한다.

**정답 4번**

### 출제 포인트

Log4j 취약점의 특성과 오픈 소스 구성요소를 안전하게 관리하는 방법을 묻는 문제이다.

### 핵심 개념

Log4j 취약점은 제품 내부에 포함된 Java 로깅 라이브러리에서 발생한 보안 취약점이다. 외부 패키지나 하위 의존성으로 제품에 내장될 수 있으므로, 사용 여부와 버전을 파악하고 패치한 뒤에도 침해 흔적과 비정상 동작을 계속 점검해야 한다. 공개 소프트웨어의 사용자 수가 많다는 사실은 해당 소프트웨어가 보안상 검증되었다는 뜻이 아니다.

NoteBase

**선지별 해설**

① O — 최초로 크게 알려진 CVE-2021-44228 이후에도 Log4j와 관련된 추가 취약점이 발견되었다. 따라서 최초 취약점 하나만 조치했다고 대응이 끝나는 것은 아니다.

② O — Log4j는 여러 제품에 직접 또는 다른 패키지의 하위 의존성으로 포함될 수 있다. 제품 표면에서 드러나지 않는 내장 구성요소까지 확인해야 하므로 발견과 영향 범위 파악이 어렵다.

③ O — 패치는 취약한 코드의 악용 가능성을 줄이는 조치일 뿐, 패치 전에 이미 발생한 침해나 잔존 악성 프로세스까지 자동으로 제거하지는 않는다. 패치 후에도 중요 시스템의 비정상 프로세스, 로그, 네트워크 통신 등 침해 징후를 점검해야 한다.

④ X — 틀린 표현은 '사용자가 많은 공개 소프트웨어는 검증된 것으로 인식하고 자유롭게 사용한다'이다. 올바르게는 사용자 수나 공개 여부만으로 안전성을 단정하지 않고, 알려진 취약점, 유지관리 상태, 사용 버전과 의존 관계를 확인한 뒤 사용해야 한다.

**오답 포인트**

④는 '사용자가 많다'와 '보안 검증이 끝났다'를 같은 의미로 바꾼 것이 함정이다. 널리 쓰이는 공개 소프트웨어도 취약점이 있을 수 있고 여러 제품에 광범위하게 내장되어 피해 범위가 커질 수 있다.

**다시 나오면 이렇게 판단**

오픈 소스 보안 선지는 인기나 공개 여부가 아니라 구성요소 식별, 취약 버전 확인, 신속한 패치, 패치 전 침해 여부 점검의 흐름으로 판단한다. '사용자가 많으므로 검증되었다'처럼 인기도를 안전성의 근거로 삼는 표현은 틀린 설명이다.

**암기 포인트**

많이 사용됨은 안전성 검증과 같지 않다. Log4j 대응은 '찾기-버전 확인-패치-침해 점검'이다.

NoteBase

21. 인터넷에 연결 시 노드가 사용하는 IP 주소를 자동으로 할당해 주는 프로토콜로 옳은 것은?
① DHCP(Dynamic Host Configuration Protocol)
② ICMP(Internet Control Message Protocol)
③ IGMP(Internet Group Management Protocol)
④ ARP(Address Resolution Protocol)

**정답 1번**

**출제 포인트**

인터넷에 연결되는 노드에 IP 주소와 네트워크 설정을 자동으로 할당하는 프로토콜을 구별하는 문제이다.

**핵심 개념**

DHCP: 호스트에 IP 주소, 서브넷 마스크, 기본 게이트웨이, DNS 서버 등의 네트워크 설정을 자동으로 제공하는 프로토콜이다. 키워드는 'IP 주소 자동 할당'이다.
ICMP: IP 통신 과정의 오류 보고와 상태 진단에 사용하는 제어 메시지 프로토콜이다.
IGMP: IPv4 네트워크에서 호스트의 멀티캐스트 그룹 가입·탈퇴를 관리하는 프로토콜이다.
ARP: 같은 로컬 네트워크에서 알고 있는 IPv4 주소에 대응하는 MAC 주소를 알아내는 프로토콜이다.

**선지별 해설**

① O — DHCP는 노드가 네트워크에 접속할 때 사용할 IP 주소와 관련 설정을 자동으로 할당하므로 문제의 설명에 해당한다.
② X — 틀린 부분은 ICMP를 IP 주소 자동 할당 프로토콜로 본 점이다. 올바르게는 ICMP는 IP 패킷 전달 중 발생한 오류를 알리거나 통신 상태를 진단하는 데 사용한다.
③ X — 틀린 부분은 IGMP를 IP 주소 자동 할당 프로토콜로 본 점이다. 올바르게는 IGMP는 호스트와 인접 라우터 사이에서 멀티캐스트 그룹의 가입과 탈퇴를 관리한다.
④ X — 틀린 부분은 ARP를 IP 주소 자동 할당 프로토콜로 본 점이다. 올바르게는 ARP는 로컬 네트워크에서 IPv4 주소에 대응하는 MAC 주소를 확인한다.

**오답 포인트**

②~④도 네트워크 계층 주변에서 자주 접하는 프로토콜이지만 역할이 다르다. '주소'라는 말만 보고 ④ ARP를 고르면 안 된다. ARP는 이미 알고 있는 IP 주소를 MAC 주소로 대응시키며, IP 주소 자체를 자동으로 배정하는 것은 DHCP이다.

NoteBase

**다시 나오면 이렇게 판단**

문장에서 동작 키워드를 찾는다. ‘IP 설정 자동 할당’이면 DHCP, ‘오류 보고·진단’이면 ICMP, ‘멀티캐스트 그룹 관리’이면 IGMP, ‘IP 주소에 대응하는 MAC 주소 확인’이면 ARP로 판단한다.

**암기 포인트**

DHCP는 동적 주소 할당, ICMP는 오류·진단, IGMP는 멀티캐스트 그룹, ARP는 IP-to-MAC 대응이다.

NoteBase

22. 유닉스 시스템에서 사용자의 계정 정보 등의 기본 정보가 평문 형태로 저장되어 있는 파일로 옳은 것은?
① /etc/passwd
② /etc/shadow
③ /etc/group
④ /etc/services

**정답 1번**

**출제 포인트**

유닉스 시스템의 주요 /etc 파일이 저장하는 정보의 종류를 구별하는 문제이다.

**핵심 개념**

/etc/passwd는 사용자 이름, 사용자 ID(UID), 기본 그룹 ID(GID), 홈 디렉터리, 로그인 셸 등 계정의 기본 정보를 읽을 수 있는 텍스트 형식으로 저장한다. 실제 비밀번호 해시 등 보호가 필요한 인증 정보는 일반적으로 /etc/shadow에 분리해 저장한다. /etc/group은 그룹 정보를, /etc/services는 네트워크 서비스 이름과 포트 번호의 대응 정보를 저장한다.

**선지별 해설**

① O — /etc/passwd는 사용자 계정의 기본 정보를 텍스트 형식으로 저장하는 파일이므로 옳다. 다만 현재 일반적인 시스템에서는 비밀번호 자체가 아니라 비밀번호 필드의 대체 표시가 들어가고, 실제 비밀번호 해시는 /etc/shadow에 저장된다.
② X — 틀린 부분은 계정의 기본 정보 파일을 /etc/shadow로 본 것이다. /etc/shadow는 비밀번호 해시와 비밀번호 변경·만료 정보 등 보호가 필요한 인증 정보를 저장하며, 계정의 기본 정보 파일은 /etc/passwd이다.
③ X — 틀린 부분은 계정의 기본 정보 파일을 /etc/group으로 본 것이다. /etc/group은 그룹 이름, 그룹 ID(GID), 그룹 구성원 등 그룹 정보를 저장하며, 사용자 계정의 기본 정보는 /etc/passwd에 저장된다.
④ X — 틀린 부분은 계정의 기본 정보 파일을 /etc/services로 본 것이다. /etc/services는 네트워크 서비스 이름과 포트 번호 및 프로토콜의 대응 정보를 저장하며, 사용자 계정의 기본 정보는 /etc/passwd에 저장된다.

**오답 포인트**

‘평문 형태’라는 표현을 ‘비밀번호가 평문으로 저장된다’는 뜻으로 오해하기 쉽다. 이 문항에서 평문은 /etc/passwd가 사람이 읽을 수 있는 텍스트 파일이라는 의미이며, 실제 비밀번호 해시는 /etc/shadow에 분리되어 있다.

NoteBase

**다시 나오면 이렇게 판단**

파일명과 정보 종류를 연결한다. 사용자 기본 정보는 passwd, 비밀번호 해시·만료 정보는 shadow, 그룹 정보는 group, 서비스명·포트 대응은 services이다.

**암기 포인트**

passwd는 사용자 기본 정보, shadow는 비밀번호 보호 정보, group은 그룹, services는 서비스와 포트이다.

23. 다음 중 국가에서 중소기업에 제공하는 '정보보안 지원 서비스'에 대한 설명으로 가장 옳지 않은 것은?

① 휘슬(웹셸 탐지도구): 홈페이지 게시판 등을 통해 공격자가 업로드 한 웹셸(해킹 도구)을 탐지하는 전용 도구로 웹셸 뿐만 아니라 악성코드 은닉 사이트 탐지 기능도 가지고 있다.

② 캐슬(웹 방화벽): 웹 취약점을 악용한 공격을 사전 차단할 수 있는 웹 방화벽 프로그램으로, 주요 웹 취약점을 이용한 웹 해킹 공격을 차단한다.

③ 디도스 사이버대피소: 피해 웹사이트로 향하는 DDoS 트래픽을 대피소로 우회하여 분석, 차단함으로써 정상적으로 운영될 수 있도록 한다.

④ 정보보호 관리체계: SQL 인젝션, XSS 등의 웹 취약점을 원격으로 점검해 주는 서비스로 발견된 취약점을 보완하여 웹사이트의 보안을 강화할 수 있다.

**정답 4번**

### 출제 포인트

중소기업 대상 정보보안 지원 서비스의 명칭과 기능이 올바르게 연결되었는지 묻는 문제이다.

### 핵심 개념

휘슬은 웹셸 등 홈페이지의 악성 파일을 탐지하는 도구이고, 캐슬은 웹 취약점 공격을 차단하는 웹 방화벽이다. 디도스 사이버대피소는 공격 트래픽을 대피소로 우회하여 분석·차단하고, 웹 취약점 점검은 SQL 인젝션·XSS 등의 취약점을 찾아 보완하도록 지원한다. 정보보호 관리체계는 이러한 원격 취약점 점검 서비스의 명칭이 아니라 조직이 정보보호를 체계적으로 관리하는 절차와 기준을 뜻한다.

NoteBase

### 선지별 해설

① O — 휘슬은 홈페이지 게시판 등에 숨어 있는 웹셸과 악성코드를 탐지하는 전용 도구라는 설명이 맞다.

② O — 캐슬은 웹 취약점을 이용한 해킹 공격을 사전에 탐지·차단하는 웹 방화벽 프로그램이라는 설명이 맞다.

③ O — 디도스 사이버대피소는 피해 웹사이트로 향하는 DDoS 트래픽을 대피소로 우회시킨 뒤 분석·차단하여 정상 서비스가 운영되도록 지원한다.

④ X — 틀린 표현은 '정보보호 관리체계'가 SQL 인젝션·XSS 등을 원격 점검해 주는 서비스라는 부분이다. 올바르게는 이러한 기능은 '웹 취약점 점검'에 해당하며, 정보보호 관리체계는 조직의 정보보호 활동을 체계적으로 수립·운영·관리하는 기준과 절차이다.

### 오답 포인트

④는 '웹사이트의 보안을 강화한다'는 넓은 목적만 보면 그럴듯하지만, 원격으로 SQL 인젝션·XSS를 검사하는 구체적 기능은 정보보호 관리체계가 아니라 웹 취약점 점검에 해당한다. 서비스의 목적보다 작동 방식과 명칭의 대응을 확인해야 한다.

### 다시 나오면 이렇게 판단

탐지·차단·우회의 작동 방식으로 구분한다. 웹셸 탐지는 휘슬, 웹 공격 차단은 캐슬, DDoS 트래픽 우회·차단은 사이버대피소, SQL 인젝션·XSS 원격 진단은 웹 취약점 점검으로 연결한다. 관리체계라는 말이 나오면 개별 보안 도구가 아니라 조직 차원의 관리 절차와 기준인지 판단한다.

### 암기 포인트

휘슬은 웹셸 탐지, 캐슬은 웹 공격 차단, 사이버대피소는 DDoS 우회, 웹 취약점 점검은 SQL 인젝션·XSS 진단, 정보보호 관리체계는 조직 차원의 관리 기준이다.

NoteBase

24. 개인정보보호위원회에 관한 법률 조항 중 각 괄호에 해당하는 것은?

> (1) 개인 정보 보호에 관한 사무를 독립적으로 수행하기 위하여 ( ㄱ ) 소속으로 개인정보 보호위원회를 둔다.
> (2) 개인정보보호위원회는 상임위원 2명(위원장 1명, 부위원장 1명)을 포함한 ( ㄴ ) 명의 위원으로 구성한다.

| | (ㄱ) | (ㄴ) |
|---|---|---|
| ① | 대통령 | 6 |
| ② | 국무총리 | 6 |
| ③ | 대통령 | 9 |
| ④ | 국무총리 | 9 |

**정답 4번**

### 쟁점

이 문제는 개인정보보호위원회의 소속과 위원 정수에 관한 문제이다. 핵심은 위원회가 국무총리 소속인지 대통령 소속인지, 그리고 상임위원 2명을 포함하여 총 몇 명으로 구성되는지를 구별하는 것이다.

### 용어 풀이

상임위원은 위원회 업무를 상시 수행하는 위원이다. 개인정보보호위원회의 상임위원 2명은 위원장 1명과 부위원장 1명이다.

### 핵심 구분

2022년 당시 「개인정보 보호법」 제7조 제1항에 따르면, 개인정보 보호에 관한 사무를 독립적으로 수행하기 위하여 국무총리 소속으로 개인정보보호위원회를 둔다. 같은 법 제7조의2 제1항에 따르면, 위원회는 상임위원 2명인 위원장 1명과 부위원장 1명을 포함한 9명의 위원으로 구성한다. 따라서 (ㄱ)은 국무총리, (ㄴ)은 9이다. 현행법에서도 이 두 내용은 동일하다.

NoteBase

### 선지별 해설

① X
- 위원회의 소속과 위원 정수를 모두 잘못 연결하였다.
- 틀린 표현: 대통령, 6명
- 올바른 표현: 국무총리, 9명

② X
- 국무총리 소속이라는 부분은 맞지만, 상임위원 2명을 포함한 전체 위원은 6명이 아니라 9명이다.
- 틀린 표현: 6명
- 올바른 표현: 9명

③ X
- 9명이라는 위원 정수는 맞지만, 위원회는 대통령 소속이 아니라 국무총리 소속이다.
- 틀린 표현: 대통령 소속
- 올바른 표현: 국무총리 소속

④ O
- 개인정보보호위원회는 국무총리 소속이며, 상임위원 2명을 포함한 9명의 위원으로 구성되므로 두 빈칸을 모두 옳게 채웠다.

### 오답 포인트

위원의 임명권자와 위원회의 소속을 혼동하기 쉽다. 위원은 대통령이 임명 또는 위촉하지만, 위원회 자체의 소속은 국무총리이다. 또한 상임위원 2명은 전체 정원이 아니라 9명 중 일부이다.

### 다시 나오면 이렇게 판단

위원회 문제에서는 소속 기관, 위원 임명권자, 상임위원 수, 전체 위원 수를 각각 분리하여 판단한다.
개인정보보호위원회는 '국무총리 소속－상임 2명－전체 9명'의 조합으로 판단한다.

### 암기 포인트

개인정보보호위원회는 국무총리 소속, 상임 2명, 전체 9명이다.

NoteBase

25. 다음 중 역할 기반 접근 제어(Role-Based Access Control)에 대한 설명으로 옳은 것은 몇 개인가?

ㄱ. 다중 사용자 및 프로그래밍 환경에서의 접근 제어를 위하여 사용자의 역할에 기반을 두고 통제하는 방식으로 강제적 및 임의적 접근 제어를 보완한 방식이다.
ㄴ. 접근대상 정보를 보안등급을 지정하여 분류한다.
ㄷ. 접근 제어 목록을 이용하여 각 객체에 대한 권한을 명시한다.
ㄹ. 사용자의 역할이 변경되면 이에 따른 접근 제어 권한을 변경한다.

① 0개
② 1개
③ 2개
④ 3개

**정답 3번**

**출제 포인트**

역할 기반 접근 제어(RBAC)의 기준이 사용자의 신원이나 객체별 목록이 아니라 역할이라는 점을 알고, 이를 강제적 접근 제어(MAC) 및 임의적 접근 제어(DAC)와 구별하는 문제이다.

**핵심 개념**

RBAC: 권한을 역할에 부여하고 사용자를 역할에 배정하여 접근을 통제하는 방식이다. 사용자의 담당 역할이 바뀌면 역할 배정을 조정하여 유효 권한을 함께 바꿀 수 있다.
MAC: 정보와 사용자에게 부여된 보안등급을 기준으로 접근을 통제한다.
DAC: 객체의 소유자 등이 재량으로 권한을 부여하며, 객체별 접근 제어 목록(ACL)으로 주체별 권한을 명시할 수 있다.

NoteBase

**제시문 판단**

ㄱ O: RBAC는 다중 사용자 환경에서 사용자의 역할을 기준으로 권한을 묶어 관리하며, 전통적인 강제적·임의적 접근 제어를 보완할 수 있다.
ㄴ X: 틀린 부분은 '접근대상 정보를 보안등급으로 지정하여 분류한다'이다. 이는 보안등급을 기준으로 통제하는 MAC의 특징이며, RBAC는 역할을 기준으로 권한을 부여한다.
ㄷ X: 틀린 부분은 '접근 제어 목록을 이용하여 각 객체에 대한 권한을 명시한다'이다. 이는 객체별 ACL을 사용하는 DAC의 전형적인 설명이며, RBAC는 역할별 권한을 정의하고 사용자에게 역할을 배정한다.
ㄹ O: 사용자의 담당 역할이 변경되면 역할 배정을 변경함으로써 그 사용자에게 적용되는 접근 권한도 변경된다.
따라서 옳은 것은 ㄱ과 ㄹ의 2개이다.

**선지별 해설**

① X: 옳은 설명이 0개라는 부분이 틀렸다. 올바르게는 ㄱ과 ㄹ의 2개이다.
② X: 옳은 설명이 1개라는 부분이 틀렸다. 올바르게는 ㄱ과 ㄹ의 2개이다.
③ O: ㄱ과 ㄹ이 옳고 ㄴ과 ㄷ이 틀리므로 옳은 설명은 2개이다.
④ X: 옳은 설명이 3개라는 부분이 틀렸다. 올바르게는 ㄱ과 ㄹ의 2개이다.

**오답 포인트**

ㄴ의 '보안등급'과 ㄷ의 '객체별 ACL'을 RBAC의 특징으로 오인하기 쉽다. 보안등급은 MAC, 객체별 ACL은 DAC, 역할별 권한 묶음은 RBAC를 가리킨다.

**다시 나오면 이렇게 판단**

접근 통제의 기준어를 찾는다. '역할·직무'이면 RBAC, '보안등급·허가등급'이면 MAC, '소유자 재량·객체별 ACL'이면 DAC로 판단한다.

**암기 포인트**

RBAC는 역할, MAC은 등급, DAC는 소유자와 ACL이다.

NoteBase