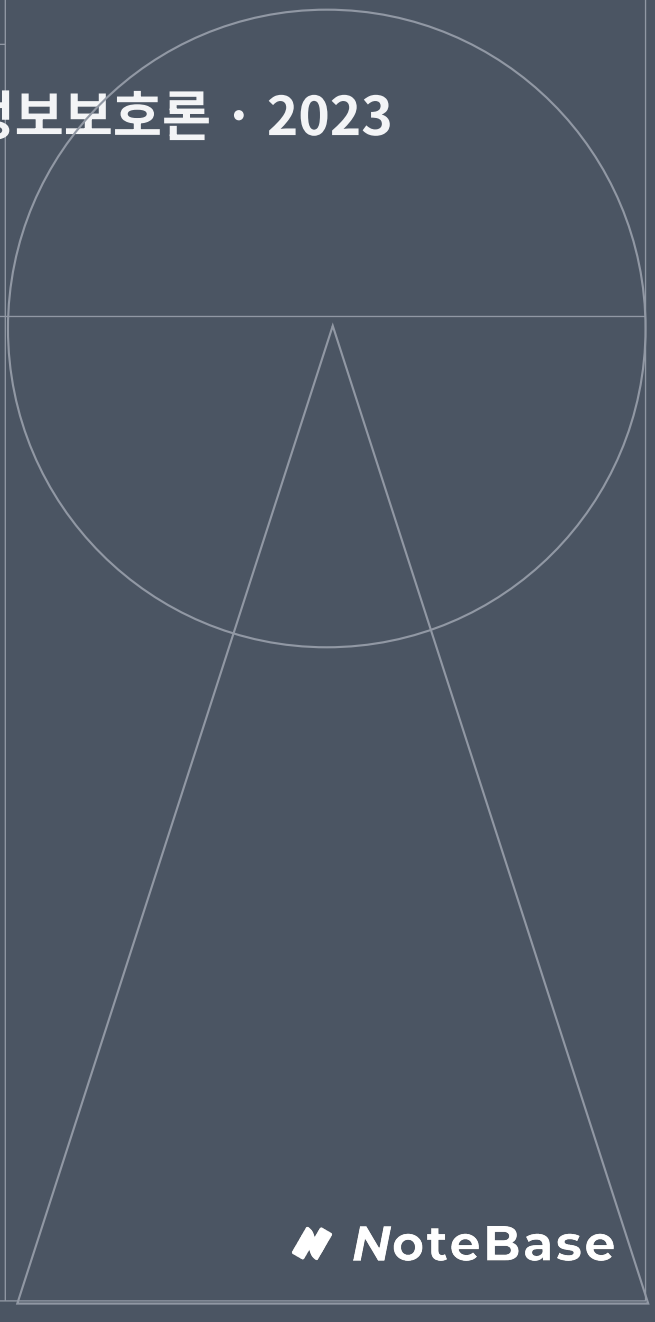
기출OX 해설집

공무원/경찰/공채(경위) · 정보보호론 · 2023



NoteBase

기출OX 해설집

공무원/경찰/공채(경위) · 정보보호론 · 2023

공무원/경찰/공채(경위) · 정보보호론 · 2023

문 1. 다음 보기에서 설명하고 있는 정보보호의 목표로 가장 적절한 것은?

가. 정보는 소유자의 인가를 받은 사람만 접근할 수 있다.
나. 인가되지 않은 정보는 절대로 공개되어서는 안된다.

① 기밀성(Confidentiality)
② 무결성(Integrity)
③ 가용성(Availability)
④ 인증성(Authentication)

정답 1번

간단한 해설

인가된 사람만 정보를 열람하게 하고 무단 공개를 막는 것은 **기밀성**을 보호하는 것이다. 두 보기 모두 정보가 허용되지 않은 대상에게 노출되는 것을 방지한다.

NoteBase

대응 관계 해설

기밀성은 인가되지 않은 주체에게 정보가 노출되거나 공개되지 않도록 보호하는 성질이다. 두 보기는 정보 접근과 공개의 허용 범위라는 서로 연결된 측면을 설명한다.

가: **기밀성의 접근 제한**에 해당한다. 정보에 접근할 수 있는 대상을 소유자의 인가를 받은 사람으로 한정하여 비인가자의 열람을 막는다. 여기서 핵심은 접근 허용 대상이며, 사용자가 주장하는 신원을 확인하는 인증 절차 자체를 설명한 것은 아니다.

나: **기밀성의 무단 공개 방지**에 해당한다. 문맥상 공개가 인가되지 않은 정보가 허가 없이 노출되어서는 안 된다는 뜻이다. 정보가 정확한지를 확인하거나 변경을 방지하는 내용과는 구별된다.

무결성은 정보의 무단 변경·훼손을 방지하는 성질이고, 가용성은 인가된 사용자가 필요할 때 정보와 서비스를 이용할 수 있는 성질이다. 인증은 사용자나 정보 출처가 주장하는 신원과 일치하는지 확인하는 것이다.

따라서 가와 나가 공통으로 설명하는 목표는 기밀성이며, ①과 일치한다.

NoteBase

문 2. 무결성을 위협하는 보안 공격으로 가장 적절하지 않은 것은?

① 스누핑(Snooping)

② 가장(Masquerading)

③ 재연(Replaying)

④ 부인(Repudiation)

정답 1번

간단한 해설

스누핑은 권한 없이 정보를 엿보거나 가로채는 행위로, 직접 위협하는 보안 목표는 **기밀성**이다. 정보의 정당한 생성·처리와 거래의 신뢰성을 해치는 무결성 위협과 구별된다.

선지별 해설

이 문항은 보안 공격을 기밀성·무결성·가용성의 관점에서 분류한다. 아래 O/X는 '무결성을 위협하는 공격에 해당하는가'를 나타낸다. 이 분류에서 무결성은 단순한 비트 변경뿐 아니라 정보의 진정성과 거래의 신뢰성까지 포함하는 넓은 의미로 사용된다.

① X: 스누핑은 허가받지 않은 사람이 통신이나 저장 정보를 엿보는 행위이다. 정보를 바꾸지 않고 내용을 알아내는 것이 중심이므로 직접적인 위협 대상은 **기밀성**이다. 따라서 무결성 위협을 고르는 분류에는 가장 적절하지 않다.

② O: 가장은 공격자가 정당한 사용자나 통신 상대인 것처럼 신분을 속이는 행위이다. 다른 사람의 이름으로 허위 메시지나 요청을 받아들이게 하여 **정보 출처의 진정성**을 해칠 수 있으므로 이 문항에서는 무결성 위협으로 분류한다.

③ O: 재연은 과거에 유효했던 메시지를 다시 전송하여 현재의 정당한 요청인 것처럼 처리되게 하는 공격이다. 메시지 내용 자체를 바꾸지 않아도 이미 처리된 거래가 다시 수행되는 등 **처리 순서와 최신성**을 훼손할 수 있으므로 무결성을 위협한다.

④ O: 부인은 메시지를 보내거나 받았다는 사실, 또는 거래에 참여했다는 사실을 나중에 부정하는 행위이다. 거래 사실과 책임의 신뢰성을 훼손하므로 이 문항의 넓은 무결성 위협 분류에 포함된다. 이를 막는 보안 서비스는 부인방지이며, 세분화된 보안 목표에서는 인증이나 부인방지를 별도로 구분하기도 한다.

따라서 주로 기밀성을 위협하는 공격인 ①이 가장 적절하지 않다.

NoteBase

문 3. 다음 중 개인정보보호를 위한 비식별화 기술에 대한 설명으로 가장 적절한 것은?

① 가명처리(Pseudonymization)는 개인식별이 가능한 데이터에 대하여 직접적으로 식별할 수 없는 다른 값으로 대체하는 방법이다.

② 총계 처리(Aggregation)는 개인을 식별하는데 기여할 확률이 높은 주요 개인 식별자에 대해 전체 또는 부분적으로 '*' 등의 대체값으로 변환하는 방법이다.

③ 데이터 삭제(Data Reduction)는 개인정보에 대하여 통계값을 적용하여 특정 개인을 판단할 수 없도록 하는 방법이다.

④ 데이터 마스킹(Data Masking)은 단일 식별 정보를 해당 그룹의 대푯값으로 변환하거나 구간값으로 변환하여 고유정보 추적 및 식별을 방지하는 방법이다.

정답 1번

간단한 해설

가명처리는 개인을 직접 식별할 수 있는 값을 **다른 대체값으로 바꾸어 직접 식별을 어렵게**하는 방법이다. 추가 정보와 결합한 재식별 가능성까지 자동으로 제거하는 것은 아니다.

선지별 해설

① O: 가명처리는 개인을 직접 가리키는 값을 **직접 식별할 수 없는 다른 값으로 대체**하는 방식이다. 예를 들어 분석용 자료의 이름을 임의의 식별 코드로 바꿀 수 있다. 다만 대응표나 다른 정보와 결합하면 다시 식별될 수 있으므로, 가명처리만으로 익명성이 언제나 보장되는 것은 아니다.

② X: 식별 정보의 전부 또는 일부를 별표나 공백 같은 대체값으로 가리는 것은 **데이터 마스킹**이다. 총계처리는 여러 관측값에 합계·평균 등의 통계값을 적용하여 개별 값이 직접 드러나지 않게 하는 방식이다. 단순히 문자를 가리는 처리와 통계값으로 묶는 처리는 구별된다.

③ X: 개인정보에 통계값을 적용한다는 설명은 **총계처리**에 해당한다. 데이터 삭제는 개인 식별에 기여하는 항목이나 값의 전부 또는 일부를 제거하는 방식이다. 예를 들어 분석에 필요 없는 상세 주소 항목을 자료에서 제거하는 경우가 해당한다.

④ X: 세부 정보를 해당 집단의 대표 범주나 구간으로 바꾸는 것은 **데이터 범주화**이다. 예를 들어 나이 27세를 '20대'로 바꾸면 정확한 수치 대신 넓은 범주만 남는다. 데이터 마스킹은 별표·공백 등으로 값을 가리는 방식이므로, 구간이나 범주로 일반화하는 설명과 다르다.

NoteBase

문 4. 다음 보기에서 설명하고 있는 패스워드 크랙 공격으로 가장 적절한 것은?

해시알고리즘별 패스워드 해시값을 저장시켜 놓은 데이터베이스를 가지고 있다. 크랙하고자 하는 패스워드의 해시값을 알고 있을 때, 기존 해시 데이터베이스와 비교하여 동일한 해시값이 매핑되면, 역으로 그 해시의 원래 평문값인 비밀번호를 추출할 수 있다.

① 무작위 대입 공격

② 레인보우테이블 이용 공격

③ 사전 공격

④ 차분 공격

정답 2번

간단한 해설

핵심은 **미리 계산한 해시 관련 자료를 조회하여 비밀번호 후보를 찾는 것**이다. 보기의 사전계산 방식은 레인보우테이블 이용 공격에 해당하며, 해시를 복호화하는 연산과는 다르다.

대응 관계 해설

보기의 '해시값을 저장시켜 놓은 데이터베이스'는 공격할 때마다 처음부터 모든 후보를 계산하는 대신 **미리 계산한 자료를 재사용**한다는 단서이다. 대상 해시와 맞는 자료를 찾아 대응하는 비밀번호 후보를 확인하는 사전계산 방식에 해당한다.

레인보우테이블은 이러한 사전계산을 이용하는 **시간·메모리 절충 기법**이다. 단순히 모든 비밀번호와 해시의 쌍을 빠짐없이 저장한 표와 완전히 같은 구조는 아니며, 저장량과 탐색 계산량을 절충한다. 보기의 '역으로 추출'은 해시함수에 복호화 연산을 적용한다는 뜻이 아니라, 사전에 계산한 관계를 이용하여 해시가 일치하는 후보를 찾는다는 뜻이다.

경쟁 개념과 구별하면, 무작위 대입 공격은 가능한 비밀번호 조합을 폭넓게 시도하고 사전 공격은 흔한 단어나 비밀번호 목록을 후보로 삼는다. 차분 공격은 입력 차이에 따른 출력 차이의 통계적 특성을 분석하는 암호분석 기법이다. 보기는 후보 선택 목록이나 차분 분석보다 **미리 구축한 해시 관련 자료와의 대조**를 강조한다.

따라서 보기의 설명에 가장 적절한 명칭은 ② **레인보우테이블 이용 공격**이다.

NoteBase

문 5. 최근의 정보보호시스템들은 기계학습·인공지능 기술을 적용하여 보안제품을 개발하고 있다. 기계학습은 학습유형에 따라 지도학습, 비지도학습 및 강화학습으로 구분될 수 있다. 다음 중 비지도학습 모델에 해당하는 것으로 가장 적절한 것은?

① Logistic Regression

② k-Means

③ Random Forest

④ Deep Q learning Network

정답 2번

간단한 해설

k-Means는 각 자료의 정답표지를 제공받지 않고, 데이터와 군집 중심 사이의 거리를 이용해 비슷한 자료를 묶는다. 이러한 **정답표지 없는 군집화**는 비지도학습에 해당한다.

선지별 해설

여기서 O/X는 각 모델이 비지도학습에 해당하는지를 표시한다. 지도학습은 입력과 정답표지의 관계를 배우고, 비지도학습은 정답표지 없이 데이터의 구조를 찾으며, 강화학습은 행동의 결과로 얻는 보상을 이용한다.

① X: 로지스틱 회귀는 **정답표지를 이용하는 분류 모델**이다. 입력 특징과 클래스 표지가 주어진 자료로 특정 클래스에 속할 확률을 학습하므로 지도학습에 속한다. 이름에 '회귀'가 들어가더라도 이 문맥에서는 연속값 예측이나 군집화가 아니라 분류에 사용된다.

② O: k-Means는 **정답표지 없이 유사한 데이터를 묶는 군집화** 방법이다. 정해 둔 k개의 중심에 각 자료를 배정하고, 각 군집의 평균으로 중심을 갱신하는 과정을 반복하여 군집 내부의 거리 제곱합을 줄인다. 군집 수 k를 지정하더라도 각 자료의 정답 클래스를 제공하는 것은 아니므로 비지도학습이다.

③ X: 랜덤 포리스트는 여러 의사결정나무의 예측을 결합하는 앙상블 모델로, 표준적인 **분류·회귀 지도학습**에 사용된다. 클래스 표지나 수치 목표값을 가진 학습자료로 나무를 만들고 그 예측을 결합하므로, 정답표지 없이 군집을 만드는 k-Means와 다르다.

④ X: DQN은 신경망으로 상태와 행동의 가치를 추정하는 **강화학습** 방법이다. 환경에서 행동한 뒤 얻는 보상과 다음 상태를 이용해, 장기적인 누적 보상이 큰 행동을 선택하도록 학습한다. 미리 정해진 정답 클래스가 없다는 사실만으로 비지도학습으로 분류하지 않는다.

따라서 비지도학습 모델에 해당하는 것은 ②이다.

NoteBase

문 6. 무결성(Integrity), 인증(Authentication)과 부인(Repudiation) 방지를 모두 제공하는 온라인 기술로 가장 적절한 것은?

① HMAC

② 일방향 해시

③ 접근제어

④ 디지털 서명

정답 4번

간단한 해설

디지털 서명은 개인키로 생성한 서명을 공개키로 검증하여 메시지의 변경 여부와 서명자를 확인한다. 공유키 방식과 달리 **제3자에게도 검증 가능한 서명 증거**를 제공하므로 부인 방지에 사용된다.

NoteBase

핵심 풀이

디지털 서명은 서명자의 개인키로 생성하고, 대응하는 공개키로 검증하는 암호기술이다. 안전한 알고리즘을 올바르게 사용하고 개인키를 보호하며 공개키와 서명자의 연결을 신뢰할 수 있다는 전제에서 세 가지 요구를 함께 충족한다.

무결성: 서명한 메시지가 바뀌면 서명 검증이 성립하지 않도록 설계되어 있으므로 **서명 후의 무단 변경**을 탐지할 수 있다.

인증: 신뢰할 수 있는 서명자의 공개키로 검증함으로써 해당 개인키를 가진 주체가 메시지에 서명했음을 확인한다. 따라서 데이터의 출처를 인증할 수 있다.

부인 방지: 검증자는 개인키 없이 공개키로 서명을 확인할 수 있다. 개인키가 서명자에게만 통제되는 등 필요한 조건이 충족되면 **제3자에게도 확인 가능한 서명 증거**가 되어 서명 사실의 부인을 방지하는 데 사용된다.

① HMAC은 송수신자가 같은 비밀키를 공유하므로 무결성과 메시지 인증에 사용되지만, 수신자도 같은 인증값을 만들 수 있다. 따라서 누가 만들었는지를 제3자에게 입증하는 부인 방지에는 적합하지 않다.

② 일방향 해시는 메시지의 요약값을 계산한다. 공격자가 메시지와 해시값을 함께 바꿀 수 있으므로 해시만으로 작성자 인증이나 부인 방지가 성립하지 않는다. 무결성을 검사하려면 비교할 해시값의 신뢰성도 확보해야 한다.

③ 접근제어는 주체가 자원에 수행할 수 있는 읽기·쓰기 등의 권한을 제한한다. 특정 메시지에 누가 서명했는지를 증명하는 기술과는 다르다.

따라서 무결성·인증·부인 방지를 함께 제공하는 기술은 ④ 디지털 서명이다.

NoteBase

문 7. 메시지 인증 코드(Message Authentication Code) 기술이 제공하는 기능으로 가장 적절한 것은?

① 접근제어와 부인방지

② 무결성 보장과 접근제어

③ 무결성 보장과 인증

④ 인증과 부인방지

정답 3번

간단한 해설

MAC은 공유 비밀키로 만든 인증값을 검증하여 **메시지의 무결성과 출처 인증**을 제공한다. 송신자와 수신자가 같은 키를 알기 때문에 부인방지 기능은 제공하지 않는다.

핵심 풀이

메시지 인증 코드(MAC)는 메시지와 비밀키를 입력하여 계산한 인증값이다. 송신자가 메시지와 MAC을 보내면 수신자는 공유한 비밀키로 검증하여 메시지가 올바른 키를 가진 주체가 만든 것인지 확인한다.

무결성: 메시지가 전송 중 변조되면 올바른 MAC 검증을 통과하기 어렵다. 안전한 MAC 알고리즘을 사용하고 키가 비밀로 유지된다는 전제에서 **허가받지 않은 내용 변경을 탐지**한다.

인증: 외부 공격자는 비밀키를 모르므로 유효한 MAC을 임의로 만들기 어렵다. 따라서 해당 키를 가진 통신 상대가 만든 메시지라는 **데이터 출처 인증**을 제공한다. 이는 키와 실제 사용자의 연결이 신뢰된다는 전제에 의존하며, 사람의 신원을 모든 상황에서 자동 증명하는 것은 아니다.

경쟁 기능의 구별: 접근제어는 어떤 주체가 어떤 자원을 이용할 수 있는지 결정·집행하는 기능으로 MAC 자체의 기능이 아니다. 부인방지는 송신자가 나중에 전송 사실을 부정하지 못하게 하는 기능인데, MAC의 수신자도 같은 키로 인증값을 만들 수 있으므로 제3자에게 송신자만 생성했다고 증명할 수 없다. 또한 MAC은 메시지 내용을 암호화하지 않으므로 기밀성도 별도로 확보해야 한다.

따라서 MAC이 직접 제공하는 기능의 조합은 ③ 무결성 보장과 인증이다.

NoteBase

문 8. 인터넷에는 악성코드를 배포하는 네트워크가 존재한다. 인터넷 서핑 중 웹 공격에 의해 악성코드가 감염되는 Drive-by Download가 발생하는데, 그 공격 절차로 가장 적절한 것은?

가. 익스플로잇 킷(exploit kit)에 의한 공격 수행
나. 경유지를 통해 이동(redirect)
다. 악성코드 설치 및 실행
라. 악성코드 링크를 통해 악성코드 다운로드
마. 공격자가 웹사이트를 변조하여 악성 링크를 심어 넣음

① 마→가→나→라→다
② 가→마→나→라→다
③ 가→마→라→나→다
④ 마→나→가→라→다

정답 4번

간단한 해설

경유지 이동으로 **공격 페이지에 도달한 뒤 취약점 악용**이 이루어지고, 그 결과 후속 악성코드가 유입될 수 있다. 내려받는 단계와 설치·실행 단계도 구별된다.

NoteBase

올바른 순서

마 → 나 → 가 → 라 → 다

마. 웹사이트 변조와 악성 링크 삽입: 공격자가 방문자가 유입될 웹사이트에 악성 연결 요소를 넣는다. 뒤의 이동과 감염이 시작될 경로를 준비하는 단계이다.

나. 경유지를 통한 이동: 사용자가 변조된 사이트를 방문하면 브라우저가 다른 주소를 거쳐 공격 페이지로 연결된다. **공격 페이지에 도달해야 그곳의 취약점 공격이 이어질 수 있다**는 점에서 익스플로잇 킷의 공격보다 앞선다.

가. 익스플로잇 킷에 의한 공격: 공격 페이지에서 브라우저나 관련 프로그램의 취약점을 악용하려는 시도가 이루어진다. 제시된 절차는 이 공격이 성공하여 후속 악성코드 유입이 가능해지는 경우를 다룬다. 단순한 주소 이동과 취약점 악용은 서로 다른 단계이다.

라. 악성코드 다운로드: 취약점 악용 이후 악성코드가 있는 주소에서 파일이 내려받아진다. **후속 악성코드를 받는 단계**이며, 아직 그 파일의 설치·실행과는 구분된다.

다. 악성코드 설치 및 실행: 내려받은 악성코드가 피해 시스템에서 설치·실행되어 감염으로 이어진다. 해당 파일을 확보하는 다운로드가 이 단계의 전제가 된다.

NoteBase

문 9. 블록암호화 모드의 복호화 수식으로 가장 적절하지 않은 것은? (단, C_i: i번째 암호문, P_i: i번째 평문, $E_K(P_i)$: Key를 이용한 P_i의 암호화, $D_K(C_i)$: Key를 이용한 C_i의 복호화)

① ECB: $P_i = D_K(C_i)$

② CBC: $P_i = D_K(C_i) \oplus C_{i-1}$

③ CFB: $P_i = D_K(C_{i-1}) \oplus C_i$

④ CTR: $P_i = E_K(Counter) \oplus C_i$

정답 3번

간단한 해설

CFB는 복호화할 때도 **이전 암호문에 암호화 함수**를 적용해 키스트림을 만든 뒤 현재 암호문과 XOR한다. 따라서 해당 식의 D_K를 E_K로 고쳐야 한다.

선지별 해설

① (O) ECB는 **각 암호문 블록을 독립적으로 복호화**한다. 암호화식이 $C_i = E_K(P_i)$이므로 역연산을 적용하면 $P_i = D_K(C_i)$가 된다. 이전 암호문이나 초기화벡터를 결합할 필요가 없다.

② (O) CBC 암호화는 현재 평문과 이전 암호문을 XOR한 뒤 암호화하므로 $C_i = E_K(P_i \oplus C_{i-1})$이다. 이를 되돌릴 때는 **현재 암호문을 복호화한 뒤 이전 암호문과 XOR**하여 $P_i = D_K(C_i) \oplus C_{i-1}$를 얻는다. 첫 블록에서는 C_0 대신 초기화벡터 IV를 사용한다.

③ (X) CFB는 복호화 과정에서도 **블록암호의 암호화 함수**를 사용한다. 한 블록 전체를 피드백하는 경우, 이전 암호문을 암호화하여 만든 값과 현재 암호문을 XOR하므로 올바른 식은 $P_i = E_K(C_{i-1}) \oplus C_i$이다. 같은 값을 두 번 XOR하면 원래 값이 복원되기 때문에 D_K가 필요하지 않다. 첫 블록의 입력은 이전 암호문 대신 IV이다.

④ (O) CTR는 해당 블록의 카운터를 암호화하여 만든 키스트림과 암호문을 XOR한다. 따라서 $P_i = E_K(\text{Counter}_i) \oplus C_i$로 복호화하며, **카운터에 적용하는 함수는 암호화 함수**이다. 선지의 Counter는 현재 블록에 대응하는 카운터를 뜻한다. 안전한 운용을 위해 같은 키 아래에서는 카운터 입력이 재사용되지 않아야 한다.

NoteBase

문 10. 128비트 데이터 블록을 사용한 Rijndael알고리즘을 기반으로 하는 반복 암호로 가장 적절한 것은?

① DES

② Skipjack

③ AES

④ Blowfish

정답 3번

간단한 해설

AES는 **Rijndael 기반의 대칭키 블록 암호**로, 128비트 데이터 블록에 라운드 변환을 반복 적용한다. 블록 길이는 키 길이 128·192·256비트 중 어느 것을 쓰더라도 128비트이다.

핵심 풀이

Rijndael 기반의 암호: **AES**는 Rijndael을 바탕으로 표준화된 대칭키 블록 암호이다. 한 블록의 데이터에 라운드 변환을 여러 차례 적용하는 반복 암호이며, 발문의 알고리즘 이름이 AES를 식별하는 핵심 단서이다.

128비트 데이터 블록: AES는 **키 길이와 관계없이 128비트 블록**을 처리한다. 사용할 수 있는 키 길이는 128·192·256비트이므로, AES-256이라는 이름의 256은 블록 길이가 아니라 키 길이를 뜻한다.

다른 암호와의 구분: DES는 64비트 블록을 처리하며 실제 암호화에 쓰이는 유효 키는 56비트이다. Skipjack은 64비트 블록과 80비트 키를 사용하고, Blowfish도 64비트 블록을 사용하는 암호이다. 이들은 발문의 128비트 블록과 Rijndael 기반이라는 조건을 충족하지 않는다.

따라서 해당 암호는 ③ AES이다.

NoteBase

문 11. 블록 암호화 과정에서 마지막 평문 블록이 단위 블록 길이에 미치지 못할 경우에 적당한 길이의 비트열을 추가하여, 단위 블록의 길이에 맞도록 데이터를 채워 넣는 것으로 가장 적절한 것은?

① 패킷
② 패딩
③ 필드
④ 패치

정답 2번

간단한 해설

마지막 평문 블록의 부족한 부분에 데이터를 덧붙여 블록 길이를 맞추는 처리는 **패딩**이다. 추가한 데이터는 복호화 후 원문과 구별할 수 있도록 정해진 규칙에 따라 구성한다.

개념 구분

패딩(padding)은 데이터를 정해진 처리 단위의 길이에 맞추기 위해 규칙에 따라 추가 데이터를 붙이는 것이다. 완전한 블록 단위의 입력을 요구하는 암호 운용에서 마지막 평문 블록이 짧으면 **부족한 길이를 채워 블록 크기를 맞춘다**. 예를 들어 블록 크기가 16바이트이고 마지막 부분이 13바이트라면 3바이트를 추가해 16바이트로 만들 수 있다.

패딩 데이터는 복호화 후 원래 메시지와 구별하여 제거할 수 있도록 정해진 규칙을 따라야 한다. 단순히 임의의 0을 붙이는 것만으로 항상 원문 길이를 복원할 수 있는 것은 아니다. 패딩의 필요 여부와 구체적인 규칙은 암호 운용 방식에 따라 달라진다.

① 패킷은 네트워크에서 전송되는 데이터 단위이다. 보통 전달을 위한 제어정보와 실제 데이터를 포함하며, 블록 길이를 채우는 처리의 이름은 아니다.

③ 필드는 데이터 형식 안에서 특정 의미를 가진 항목이다. 예를 들어 메시지 형식의 길이 필드나 주소 필드처럼 구조의 일부를 가리킨다.

④ 패치는 프로그램의 오류나 취약점을 수정하기 위한 변경·수정 코드이다. 암호 입력의 길이를 맞추는 작업과 구별된다.

따라서 마지막 블록에 비트열을 추가하여 정해진 길이를 맞추는 것은 ② 패딩이다.

NoteBase

문 12. 하이브리드 암호 시스템으로 가장 적절하지 않은 것은?

① 대칭암호의 암호화에서 사용한 세션 키는 의사난수 생성기로 생성한다.

② 메시지는 대칭 암호로 암호화한다.

③ 대칭암호의 암호화에서 사용한 세션 키는 개인 키 암호로 암호화한다.

④ 공개 키 암호의 암호화에서 사용하는 키는 하이브리드 암호 시스템의 외부로부터 부여된다.

정답 3번

간단한 해설

하이브리드 암호에서는 메시지를 대칭키로 암호화하고, 그 세션 키를 **수신자의 공개키**로 암호화하여 전달한다. 수신자는 자신의 개인키로 세션 키를 복구하므로, 세션 키를 개인키 암호로 암호화한다는 설명은 적절하지 않다.

선지별 해설

하이브리드 암호는 대칭키 암호의 빠른 데이터 처리와 공개키 암호의 키 전달 기능을 결합한다. 이 문항은 대칭 세션 키를 공개키로 암호화하여 전달하는 기본 구조를 묻는다.

① O: 메시지 암호화에 사용할 세션 키는 **예측하기 어려운 난수**로 생성해야 한다. 이를 위해 충분한 엔트로피를 바탕으로 하는 암호학적으로 안전한 의사난수 생성기를 사용할 수 있다. 일반적인 시뮬레이션용 의사난수 생성기가 아무 조건 없이 적합하다는 뜻은 아니다.

② O: 실제 메시지는 생성된 세션 키를 이용해 **대칭키 암호로 암호화**한다. 메시지 전체를 공개키 암호로 처리하는 것보다 효율적이며, 공개키 연산은 주로 세션 키 보호에 이용한다.

③ X: 세션 키는 기본 구조에서 **수신자의 공개키로 암호화**하고, 그에 대응하는 수신자의 개인키로 복호화한다. 개인키로 암호화하여 전달한다는 설명은 공개키·개인키의 역할을 혼동한 것이다. 송신자의 개인키를 이용하는 전자서명은 송신자 인증을 위한 별도의 기능이며, 이 세션 키의 기밀 전달과 같지 않다.

④ O: 세션 키를 보호하는 데 쓰는 수신자의 공개키는 인증서, 공개키 저장소 또는 사전 공유 등 외부의 키 배포 경로를 통해 확보한다. 여기서 외부에서 부여된다는 것은 해당 메시지를 위한 세션 키와 달리 **이미 준비된 수신자 공개키를 입력받아 사용**한다는 뜻이다. 공격자의 키로 바꿔치기되지 않도록 공개키의 소유자와 진위를 확인해야 한다.

따라서 세션 키의 보호에 쓰는 키를 잘못 설명한 ③이 가장 적절하지 않다.

NoteBase

문 13. RSA 암호 알고리즘에서 두 소수 $p = 3$, $q = 11$과 키값 $e = 3$을 선택한 경우, 평문 $m = 8$에 대한 암호문 c로 가장 적절한 것은?

① 15

② 17

③ 19

④ 21

정답 2번

간단한 해설

RSA 암호화는 평문을 공개 지수만큼 거듭제곱한 뒤 두 소수의 곱으로 나눈 나머지를 구한다. $8^3 = 512$를 33으로 나누면 **나머지가 17**이다.

계산 과정

RSA의 기본 암호화 연산은 공개키의 법 n과 지수 e를 이용해 c=m^e n을 계산한다. 여기서 mod는 법으로 나눈 나머지를 뜻한다. 주어진 값은 p = 3, q = 11, e = 3, m = 8이며, 구할 값은 정수 암호문 c이다.

두 소수를 곱해 법을 구한다.
$n = pq = 3 \times 11 = 33$
평문 8은 0 이상 33 미만이므로 이 연산의 입력 범위에 들어간다. 나머지를 구할 때 쓰는 수는 **e가 아니라 n = 33**이다.

평문에 공개 지수 3을 적용한다.
$m^e = 8^3 = 512$
따라서 구할 암호문은 512를 33으로 나눈 나머지이다.

$512 = 33 \times 15 + 17$
그러므로 **나머지는 17**이며, 암호문 c = 17은 선택지 ②와 일치한다.

NoteBase

문 14. 일방향 해시 함수의 성질로 가장 적절하지 않은 것은?

① 정해진 길이 입력값을 받아 정해진 길이 결과값을 출력한다.

② 해시 알고리즘에는 MD5, SHA-2 등이 있다.

③ 해시는 메시지의 무결성을 확인하기 위해서 사용한다.

④ 결과값으로부터 입력값을 역산할 수 없다.

정답 1번

간단한 해설

해시 함수는 보통 **가변 길이 입력을 고정 길이 해시값으로 변환**한다. 출력 길이가 일정하다는 성질을 입력 길이까지 고정된다는 뜻으로 설명한 것이 잘못이다.

선지별 해설

① (X) 일반적인 고정 출력 길이 해시 함수는 **가변 길이의 입력을 고정 길이의 출력으로 변환**한다. 알고리즘이 허용하는 범위 안에서 메시지 길이는 달라질 수 있지만, 같은 알고리즘을 쓰면 해시값의 길이는 일정하다. 내부에서 일정 크기의 블록으로 나누어 처리하는 것과 전체 입력의 길이가 고정되어 있다는 주장은 다르다.

② (O) MD5와 SHA-2는 모두 **해시 알고리즘에 속한다**. MD5는 128비트 해시값을 만들고, SHA-2 계열에는 SHA-256·SHA-512 등이 있다. 다만 알고리즘의 분류와 보안성은 별개이다. MD5는 충돌 취약성이 알려져 있으므로, 충돌 저항성이 필요한 보안 용도에 안전한 알고리즘이라는 뜻은 아니다.

③ (O) 수신하거나 보관 중인 메시지의 해시값을 다시 계산하여 **신뢰할 수 있는 기준 해시값과 비교**하면 변경 여부를 확인하는 데 이용할 수 있다. 이 때문에 해시는 메시지 무결성 검증의 구성 요소로 쓰인다. 공격자가 메시지와 기준 해시값을 함께 바꿀 수 있다면 단순 비교만으로 악의적인 변조를 막을 수 없으므로, 기준값의 신뢰성을 확보해야 한다.

④ (O) 일방향성은 주어진 해시값에서 그에 대응하는 입력을 찾는 것이 **계산적으로 매우 어렵다**는 의미이다. 암호문을 키로 복호화하듯 원문을 되돌리는 역연산이 제공되는 것이 아니다. 다만 후보 입력이 매우 적거나 쉽게 추측되는 경우에는 후보의 해시를 계산해 대조할 수 있으므로, '역산할 수 없다'를 어떤 상황에서도 입력을 알아낼 수 없다는 절대적 의미로 해석하지 않는다.

NoteBase

문 15. 일방향 해시 함수 SHA-3에 대한 설명으로 가장 적절하지 않은 것은?

① 미국의 표준화 기구 NIST는 2012년 KECCAK이라는 알고리즘을 최종 표준으로 선정했다.

② SHA-1과 SHA-2와는 전혀 다른 스펀지구조로 흡수단계와 추출단계를 통해서 해시값을 출력한다.

③ SHA-2의 강한 충돌(Strong Collision) 내성이 깨졌다는 사실을 알고, NIST에서 공모하여 선정했다.

④ 선정조건 중 하나는 “구조를 명확히 하여 해석이 쉬울 것”이다.

정답 3번

간단한 해설

SHA-3는 **SHA-2의 충돌 내성이 깨졌기 때문에 선정된 것이 아니다**. 기존 해시함수에 대한 공격의 발전에 대비하여 SHA-2와 구조가 다른 대안을 확보하고 암호 설계의 다양성을 높이려는 목적이었다.

선지별 해설

SHA-3는 KECCAK을 바탕으로 한 해시함수 계열이다. 표준 알고리즘을 고른 시점, 실제 표준을 발행한 시점, 공모를 시작한 보안상의 배경을 구별한다.

① O: NIST는 **2012년에 KECCAK을 SHA-3 공모의 최종 승자**로 선정했다. 선지의 '최종 표준으로 선정'은 새 표준의 기반 알고리즘을 선택했다는 의미이다. SHA-3를 규정한 FIPS 202가 최종 발행된 해는 2015년으로, 선정 연도와 표준 발행 연도는 다르다.

② O: SHA-3는 SHA-1·SHA-2의 반복 압축함수 기반 구성과 다른 **스펀지 구조**를 사용한다. 흡수 단계에서는 패딩한 메시지 블록을 내부 상태에 반영하면서 순열을 적용하고, 추출 단계에서는 그 상태에서 필요한 출력 비트를 얻는다. 출력이 더 필요하면 순열을 다시 적용하여 추출을 이어 간다.

③ X: NIST는 해시함수 분석기법의 발전과 기존 방식의 잠재적 취약성에 대비하여 새로운 설계를 공모했다. 그러나 KECCAK 선정 당시에도 **SHA-2는 안전한 일반 용도 해시함수로 평가**되었으며, SHA-2의 충돌 내성이 이미 깨졌다는 사실이 공모의 전제였던 것은 아니다. 구조가 다른 SHA-3는 SHA-2를 보완하는 대안으로 마련되었다.

④ O: 구조와 설계 근거가 명확하면 공개된 알고리즘을 분석하고 보안성을 검토하기 쉽다. NIST도 KECCAK의 명료한 구조와 분석 용이성을 장점으로 평가했다. 여기서 '해석이 쉽다'는 것은 원래 메시지를 쉽게 복원하거나 충돌을 쉽게 찾을 수 있다는 뜻이 아니라, **알고리즘의 작동과 안전성을 검토하기 쉽다**는 의미이다.

NoteBase

문 16. 주어진 메시지 x에 대해, $H(y) = H(x)$를 만족하면서 $y \neq x$인 y를 찾는 것이 계산적으로는 불가능해야 하는 해시 함수의 특성으로 가장 적절한 것은?

① 의사난수성(Pseudo-randomness)

② 일방향성(Onewayness)

③ 약한 충돌 저항성(Weak Collision Resistance)

④ 강한 충돌 저항성(Strong Collision Resistance)

정답 3번

간단한 해설

메시지 x가 먼저 고정되어 있고 그와 같은 해시값을 갖는 다른 메시지를 찾기 어렵다는 조건은 약한 충돌 저항성, 즉 제2원상 저항성이다. 두 메시지를 모두 자유롭게 골라 충돌을 찾는 경우와 구분된다.

개념 구분

약한 충돌 저항성: 발문에서는 **메시지 x가 먼저 주어져 고정**되어 있다. 이 x와는 다르면서 같은 해시값을 갖는 y, 즉 y는 x와 다르고 $H(y) = H(x)$인 y를 찾기 어려워야 한다는 성질이다. 이를 '제2원상 저항성'이라고도 한다. 이미 정해진 문서를 같은 해시값의 다른 문서로 바꾸는 공격을 어렵게 하는 성질에 해당한다.

일방향성과의 구분: 일방향성, 즉 원상 저항성은 **해시값 h만 주어진 상태**에서 $H(x) = h$를 만족하는 입력 x를 찾기 어려워야 한다는 뜻이다. 발문처럼 원래 메시지 x를 알고 다른 입력 y를 찾는 조건과 출발점이 다르다.

강한 충돌 저항성과의 구분: 강한 충돌 저항성은 어느 한 메시지가 미리 고정되지 않은 상태에서, **같은 해시값을 갖는 서로 다른 두 입력을 함께 찾기** 어려워야 한다는 성질이다. 반면 발문의 약한 충돌 저항성에서는 주어진 x를 마음대로 바꿀 수 없다.

의사난수성과의 구분: 의사난수성은 출력이 난수와 유사한 특성을 보이는지에 관한 개념이며, 주어진 입력에 대한 다른 충돌 입력을 찾기 어렵다는 조건의 명칭은 아니다. 또한 해시 함수의 '계산적 불가능'은 충돌이 전혀 존재하지 않는다는 뜻이 아니라, 현실적인 계산 자원으로 해당 입력을 찾아내기 어렵다는 뜻이다.

따라서 발문에 해당하는 특성은 ③ 약한 충돌 저항성이다.

NoteBase

문 17. PKI(Public Key Infrastructure)에 대한 설명으로 가장 적절하지 않은 것은?

① PKI의 3가지 구성요소는 사용자, 인증기관, 저장소이다.

② X.509 인증서는 개인키를 포함한다.

③ PKI 환경에서 공개키 암호를 이용할 경우 CA(Certification Authority)는 인증서를 발급한다.

④ 공개키 인증서를 발행하여 무결성, 인증과 부인(Repudiation) 방지를 보장한다.

정답 2번

간단한 해설

X.509 인증서는 소유자 정보와 **공개키를 연결**하는 자료이다. 대응하는 **개인키는 인증서에 넣어 공개하지 않고** 별도로 비밀 관리한다.

선지별 해설

① O: PKI를 기본 기능으로 묶으면 인증서를 사용하는 사용자, 인증서를 발급하는 인증기관, 인증서·폐지정보 등을 보관·배포하는 저장소로 설명할 수 있다. 등록기관(RA)처럼 신원 확인을 맡는 역할을 별도로 두는 구성도 있으므로, 이 세 구분은 **기본 기능 중심의 요약**으로 이해한다.

② X: X.509 공개키 인증서에는 소유자를 나타내는 정보와 그에 연결된 **공개키**, 발급자·유효기간·서명 등의 정보가 담긴다. 대응하는 **개인키는 인증서에 포함해 공개하지 않고 비밀로 보호**한다. 개인키가 인증서와 함께 노출되면 다른 사람이 소유자를 가장해 서명할 수 있기 때문이다.

③ O: CA는 인증 정책에 따른 확인을 거쳐 주체 정보와 공개키를 연결한 인증서를 발급한다. CA가 인증서에 서명하면 이용자는 신뢰하는 발급 경로를 통해 **해당 공개키의 소유자 연결을 검증**할 수 있다. 등록기관이 신원 확인을 대행하더라도 인증서 발급·서명의 주체와 역할은 구별된다.

④ O: PKI는 인증된 공개키를 이용하는 전자서명 검증을 통해 데이터의 변경 여부와 서명자를 확인하고, 서명 행위를 부인하지 못하게 하는 근거를 제공한다. 이 의미에서 **무결성·인증·부인방지 서비스를 뒷받침**한다. 인증서 발급만으로 모든 통신에 자동 적용되는 것은 아니며, 개인키 보호와 인증서 유효성 확인 및 적절한 서명 절차가 전제된다.

NoteBase

문 18. 난수와 PKI에 대한 설명으로 가장 적절하지 않은 것은?

① 난수의 성질에는 무작위성, 예측 불가능성, 재현 불가능성이 있다.

② PKI 환경에서 등록기관은 공개키 인증서를 발급하고, 또 필요에 따라 취소한다.

③ ANSI X9.17에는 의사난수 생성기의 보다 구체적인 구성 방법이 기술되어 있다.

④ 저장소는 인증서와 사용자 관련 정보, 상호 인증서 쌍 및 인증서 취소목록 등을 저장 및 검색하는 장소를 말한다.

정답 2번

간단한 해설

공개키 인증서를 서명해 발급하는 기관은 **인증기관 CA**이다. 등록기관 RA는 신청자의 신원 확인과 등록 심사 등을 담당하므로, RA를 인증서 발급 주체로 설명한 것이 잘못이다.

선지별 해설

① (O) 무작위성·예측 불가능성·재현 불가능성은 **난수의 특성을 구분하는 기준**이다. 무작위성은 통계적으로 편향이나 규칙성이 드러나지 않는 성질, 예측 불가능성은 관측한 값으로 다음 값을 알아내기 어려운 성질, 재현 불가능성은 같은 수열을 의도적으로 다시 만들어 내기 어려운 성질을 말한다. 다만 의사난수 생성기는 동일한 시드와 입력 상태를 주면 같은 결과를 재현하므로, 모든 난수 생성기가 세 성질을 무조건 갖는다는 뜻은 아니다.

② (X) 공개키 인증서를 서명하여 발급하는 주체는 **인증기관 CA**이다. 등록기관 RA는 신청자의 신원 확인, 신청 접수·심사 등 CA가 위임한 등록 업무를 수행한다. RA가 취소 요청의 접수나 검증 등에 관여할 수는 있지만, RA의 역할을 인증서 발급기관으로 설명한 것은 잘못이다. 선지의 발급·취소 관리 주체는 기본적으로 CA로 구별해야 한다.

③ (O) ANSI X9.17에는 **의사난수 생성기의 구체적인 구성 방법**이 제시되어 있다. 금융기관의 키 관리에 관한 이 표준의 부록에는 의사난수 키와 초기화벡터의 생성 절차가 포함되어 있다. 이는 해당 표준의 내용에 관한 설명이며, 그 역사적 알고리즘을 지금도 모든 용도에 권장한다는 의미는 아니다.

④ (O) 저장소는 **인증서와 관련 정보를 보관하고 조회하게 하는 구성 요소**이다. 사용자 인증서와 관련 정보, 인증기관 사이의 신뢰관계에 쓰이는 상호 인증서, 효력 취소 상태를 알리는 인증서 취소목록 CRL 등을 저장·배포하여 인증서 검증을 지원한다. 정보를 저장·검색하는 기능과 인증서를 발급·서명하는 CA의 기능은 구별된다.

NoteBase

문 19. Biba 보안모델에 대한 설명으로 가장 적절한 것은?

① 시스템 내부 정보의 무결성 유지보다 기밀성을 보장하는 것이 목표이다.

② 정보 주체는 응용 프로그램을 통해서만 정보 객체에 대한 접근이 가능하다.

③ 임의적 접근제어 방식으로 직무 분리를 통해 무결성 침해를 방지한다.

④ 보안등급이 낮은 주체는 보안등급이 높은 객체에 쓰기가 금지된다.

정답 4번

간단한 해설

Biba 모델은 신뢰도가 낮은 정보가 높은 등급의 정보를 오염시키지 못하도록 무결성을 보호한다. 이에 따라 **낮은 무결성 등급의 주체가 높은 등급의 객체에 쓰는 것**을 금지한다.

선지별 해설

Biba의 엄격한 무결성 정책은 주체와 객체의 무결성 등급을 비교하여 정보 흐름을 통제한다. 핵심은 낮은 신뢰수준의 정보가 높은 신뢰수준의 데이터나 처리에 영향을 주지 못하게 하는 것이다. 이 문항의 보안등급은 무결성 등급으로 이해한다.

① X: Biba의 주된 목표는 **무결성 보호**이다. 신뢰도가 낮은 주체의 변경이나 낮은 등급 정보의 유입으로 중요한 정보가 오염되는 것을 막는다. 기밀성 보호를 중심으로 하는 대표적인 등급 기반 모델은 Bell-LaPadula이다.

② X: 인가된 프로그램의 정형화된 처리 절차를 통해 무결성 보호 대상 데이터를 다루도록 하는 것은 **Clark-Wilson 모델**의 특징이다. 단순히 아무 응용 프로그램이나 거치면 된다는 의미는 아니며, 인증된 변환 절차와 허가된 사용자·데이터의 관계가 중요하다. Biba는 이런 프로그램 경유 여부보다 무결성 등급에 따른 읽기·쓰기 규칙으로 접근을 제한한다.

③ X: Biba는 객체 소유자가 임의로 권한을 나누어 주는 임의적 접근제어를 핵심으로 삼지 않는다. **무결성 등급에 따른 강제적 정보 흐름 통제**가 중심이다. 직무 분리와 정형화된 트랜잭션으로 상업적 데이터의 무결성을 확보하는 설명은 Clark-Wilson 모델과 관련된다.

④ O: 낮은 무결성 등급의 주체가 높은 등급의 객체를 수정하면 신뢰도가 낮은 내용이 중요한 데이터에 들어갈 수 있다. 이를 막는 규칙이 **상위 등급 쓰기 금지(No Write Up)**이다. 엄격한 Biba 정책은 높은 등급의 주체가 낮은 등급 정보를 읽어 오염되는 것도 막기 위해 하위 등급 읽기 금지(No Read Down)를 함께 적용한다.

NoteBase

문 20. 다음 보기에서 강제적 접근제어(MAC, Mandatory Access Control)에 해당하는 것을 모두 고른 것으로 가장 적절한 것은?

가. 비밀성을 갖는 객체에 대하여 주체가 갖는 권한에 근거하여 객체에 대한 접근을 제어하는 방법이다.
나. 주체와 객체의 수에 관계 없이 접근 규칙의 수가 정해지며 개별 주체와 개별 객체 단위의 접근 제한 설정은 불가능하다.
다. 신분 기반의 접근제어 방식으로 접근 권한 관리가 간단하며 보안 관리자의 개입 없이 다른 사용자에게 접근 권한 부여가 가능하다.
라. 사용자는 보호 대상 정보나 자원에 대한 접근 권한을 얻기 위해서는 해당 접근 권한이 배정된 역할의 구성원이 되어야 한다.
마. 접근 권한 주체와 접근 권한 대상이 어떠한 환경에 처해 있는가를 동적으로 분석하여 접근 권한을 부여하는 방법이다.

① 가, 나
② 나, 다
③ 나, 라
④ 다, 마

정답 1번

간단한 해설

강제적 접근제어는 객체의 보안등급과 주체의 인가를 **중앙의 공통 보안정책**에 따라 대조한다. 전형적인 등급 기반 모형에서는 소유자가 개별 사용자에게 정책과 별개의 권한을 임의로 부여하지 못한다.

NoteBase

보기별 해설

가. 강제적 접근제어(MAC): 객체가 가진 정보의 민감도를 보안등급으로 표시하고, 주체에게 부여된 인가등급과 대조하여 접근을 결정한다. 여기서 주체의 '권한'은 소유자가 자유롭게 나누어 주는 허가가 아니라 **중앙 보안정책에 따른 인가**라는 의미이다.

나. 강제적 접근제어(MAC): 전형적인 등급 기반 MAC에서는 **정해진 등급 체계의 공통 규칙**을 적용한다. 따라서 사용자나 파일이 늘어날 때마다 각 주체·객체 쌍의 재량적 허가 규칙을 새로 만드는 방식과 다르다. '개별 단위의 설정이 불가능하다'는 표현은 이 비교 문맥에서 소유자가 공통 정책과 별개로 개별 사용자에게 임의의 접근 권한을 부여할 수 없다는 취지이다. 중앙 관리자가 개별 대상의 라벨을 지정하거나 정당한 절차로 보안정책을 조정하는 것까지 불가능하다는 뜻은 아니다.

다. 임의적 접근제어(DAC): 사용자의 신원을 바탕으로 객체의 소유자 등 권한 있는 사용자가 접근 허가를 정하고 다른 사용자에게 권한을 부여할 수 있다. **소유자 등의 재량에 따른 권한 부여**가 핵심이므로 MAC과 구분된다. 개별 허가를 설정하기는 쉽지만, 사용자와 객체가 많아지면 권한 관리 전체가 항상 간단한 것은 아니다.

라. 역할 기반 접근제어(RBAC): 접근 권한을 역할에 배정하고 사용자를 그 역할에 소속시켜 권한을 행사하게 한다. **사용자와 권한을 역할이 연결**하므로, 정보의 보안등급과 인가등급을 기준으로 하는 MAC의 설명과 다르다.

마. 상황을 고려한 접근제어: 현재 시간·접속 위치 등 요청 당시의 환경을 평가하여 접근을 결정하는 방식이다. 이러한 동적 환경 조건은 속성 기반 접근제어(ABAC)에서도 주체·객체의 속성과 함께 평가한다. 이 보기의 핵심은 **요청 당시의 환경 조건**이므로 전형적인 등급 기반 MAC을 설명한 가·나와 구분된다.

따라서 강제적 접근제어에 해당하는 보기는 가, 나이며 ①이다.

NoteBase

문 21. 다음 중 커버로스 프로토콜(Kerberos Protocol)에 대한 설명으로 가장 적절한 것은?

① 인증 서버가 다운되어도 새로운 사용자의 로그인이 가능하다.

② 요청을 주고받는 호스트들 간에 시간 동기화 없이 인증이 가능하다.

③ 커버로스는 세사미(SESAME)의 약점을 보완하기 위해 개발되었다.

④ 대칭키 기반으로 동작하는 컴퓨터 네트워크 인증 프로토콜이다.

정답 4번

간단한 해설

커버로스는 **대칭키와 신뢰하는 키 분배 센터가 발급한 티켓**을 이용하여 네트워크상의 주체를 인증한다. 최초 인증에는 이용 가능한 인증 서버가 필요하고, 재전송 공격을 막기 위해 시각 정보도 검사한다.

선지별 해설

커버로스는 신뢰하는 키 분배 센터(KDC)가 발급하는 티켓과 세션 키를 이용해 클라이언트와 서비스의 신원을 확인하는 인증 방식이다.

① X: 새로운 사용자가 최초 인증을 받으려면 인증 서버(AS)에 요청하여 티켓 발급 티켓(TGT) 등을 받아야 한다. **이용 가능한 인증 서버가 없으면 새로운 최초 인증을 진행할 수 없다**. 이미 발급받은 유효한 서비스 티켓을 사용하는 경우나 복제된 다른 인증 서버를 이용하는 경우는 구별해야 한다.

② X: 인증자에 포함된 시각과 티켓의 유효기간을 검사하므로 호스트 간 시계는 **허용 오차 안에서 동기화**되어야 한다. 시각 차이가 허용 범위를 벗어나면 정상 요청도 거절될 수 있다. 완전히 같은 시각일 필요는 없지만 시간 동기화가 불필요한 것은 아니다.

③ X: 개발 관계가 반대이다. 커버로스가 먼저 개발되었고, **세사미는 커버로스 기술을 바탕으로 공개키 인증과 권한 관리 등을 확장**한 보안 체계이다. 커버로스가 세사미의 약점을 보완하기 위해 만들어진 것은 아니다.

④ O: 기본 커버로스는 **대칭키 암호를 기반으로 한 네트워크 인증 프로토콜**이다. KDC와 각 주체 사이의 비밀키 및 발급된 세션 키를 이용하여 티켓과 인증자를 보호한다. 공개키를 이용한 초기 인증 확장이 존재하더라도 기본 구조가 대칭키 기반이라는 설명과 모순되지 않는다.

NoteBase

문 22. DB 암호화 방법 중 API 방식에 대한 설명으로 가장 적절한 것은?

① 암복호화 모듈을 애플리케이션 서버 내 설치하여 운영한다.

② 블록 암호화에 적합한 방식으로 고속으로 동작한다.

③ 애플리케이션의 수정이 필요 없어 편리하다.

④ 암복호화할 때 DB 서버의 사용으로 부하가 발생한다.

정답 1번

간단한 해설

API 방식은 **애플리케이션 서버에서 암복호화 모듈을 호출**하여 DB에 저장할 데이터와 조회한 데이터를 처리한다. 암복호화 기능을 응용 프로그램에 연동한다는 점이 핵심이다.

선지별 해설

① O: API 방식은 **애플리케이션 서버에 암복호화 모듈을 설치**하고, 응용 프로그램이 제공된 함수를 호출해 데이터를 처리한다. 저장할 데이터는 애플리케이션에서 암호화한 뒤 DB에 보내고, 조회한 암호문은 애플리케이션에서 복호화한다. 설치 위치와 호출 주체를 정확하게 설명한 진술이다.

② X: API 방식의 구별 기준은 **애플리케이션에서 암복호화 함수를 호출한다는 점**이다. DB의 저장 블록을 일괄적으로 암호화하는 방식은 테이블스페이스 단위의 TDE 등과 구별하며, API 방식 자체가 특정 처리 속도를 보장하지도 않는다. API에서 AES 같은 블록 암호 알고리즘을 사용할 수 있다는 사실과 DB 암호화의 적용 단위·구현 방식을 혼동해서는 안 된다.

③ X: 기존 프로그램에 API 방식을 적용하려면 암호화할 데이터를 저장하거나 읽는 부분에 **암복호화 함수 호출을 반영하는 수정**이 필요하다. DBMS 내부에서 투명하게 암복호화를 처리하는 방식의 장점을 API 방식의 일반적인 특징으로 옮긴 설명이다.

④ X: API 방식의 암복호화 연산은 **애플리케이션 서버에서 수행**하므로 그 연산 부하도 주로 해당 서버가 부담한다. DB 서버에서 암복호화 모듈을 실행하는 플러그인 방식과 구별된다. DB의 저장·조회 부하까지 없어지는 것은 아니지만, 암복호화 연산 자체를 DB 서버가 맡는다는 설명은 적절하지 않다.

NoteBase

문 23. 취약점 데이터베이스로 가장 적절하지 않은 것은?

① Exploit-db

② CVE

③ NIST NVD

④ Shodan

정답 4번

간단한 해설

Shodan은 **인터넷에 연결된 장치와 서비스 정보를 검색하는 엔진**이다. 취약점 자체의 식별정보·설명·분석자료를 중심으로 정리하는 취약점 데이터베이스와 주된 목적이 다르다.

선지별 해설

이 문항은 취약점 정보의 목록·분석·관련 자료를 축적하는 서비스와, 인터넷에 노출된 개별 장치의 정보를 찾아주는 서비스를 구별한다. O/X는 취약점 데이터베이스 또는 관련 정보 저장소에 해당하는지를 뜻한다.

① O: Exploit-db는 공개된 **취약점 악용 사례와 개념증명 자료**, 관련 취약 소프트웨어 정보를 모아 제공하는 데이터베이스이다. 일반적인 보안 권고문 목록보다는 취약점의 재현·연구에 쓰이는 자료를 중심으로 한다.

② O: CVE는 공개된 보안 취약점을 공통 식별자로 구별하고 기록하는 체계이자 목록이다. 서로 다른 보안 도구와 기관이 같은 취약점을 지칭할 수 있게 하는 **공통 식별정보**를 제공한다. 상세 분석이나 위험평가 전체를 대신하는 것은 아니지만, 취약점 정보의 기본 목록에 해당한다.

③ O: NIST의 NVD는 취약점 관리 데이터를 제공하는 데이터베이스이다. CVE로 식별된 취약점에 영향받는 제품, 취약점 유형, 심각도 등의 분석정보를 연결하여 취약점 평가와 관리에 활용하도록 한다.

④ X: Shodan의 주된 대상은 **인터넷에 연결되어 응답하는 장치와 서비스**이다. 서비스 배너, 소프트웨어 버전 등 노출 정보를 수집·검색하는 데 사용된다. 취약점 관련 정보를 연계하여 보안 점검을 도울 수는 있지만, 그 기능 때문에 서비스의 기본 성격이 취약점 목록 데이터베이스가 되는 것은 아니다.

NoteBase

문 24. ISO 27001의 정보보호 통제 영역으로 가장 적절하지 않은 것은?

① 자산 관리

② 업무 연속성 관리

③ 컴플라이언스

④ 품질보증 관리

정답 4번

간단한 해설

문항이 사용하는 구판의 정보보호 통제영역에는 자산 관리, 업무 연속성 관련 관리, 컴플라이언스가 포함된다. **품질보증 관리는 해당 통제영역의 명칭이 아니다**.

선지별 해설

① (O) 자산 관리는 **보호할 정보자산과 관리 책임을 식별**하고, 자산의 중요성에 맞게 분류·취급하는 영역이다. 이 문항에 사용된 구판의 통제영역 분류에 포함되며, 정보·장비·매체 등에 적절한 보호조치를 적용하기 위한 기반이 된다.

② (O) 업무 연속성 관리는 **장애나 재난 상황에서도 필요한 업무와 정보보호를 유지**하기 위한 영역이다. 중단에 대비한 계획과 복구 절차, 필요한 자원의 확보 등을 다룬다. 구판의 업무 연속성 관리 영역은 2013판에서 업무 연속성 관리의 정보보호 측면을 다루는 영역으로 이어진다.

③ (O) 컴플라이언스는 **법규·계약 및 정보보호 요구사항의 준수**를 다루는 영역이다. 조직에 적용되는 요구사항을 식별하고, 정보의 처리와 보안 운영이 이에 맞게 이루어지는지 확인한다. 따라서 이 문항의 통제영역에 해당한다.

④ (X) 품질보증 관리는 제품이나 서비스가 정해진 품질 요구사항을 충족하도록 하는 품질경영의 개념으로, **문항에 제시된 정보보호 통제영역의 명칭에는 포함되지 않는다**. 품질경영시스템의 대표 표준인 ISO 9001과 정보보호경영시스템의 ISO/IEC 27001을 구별해야 한다. 다만 표준의 판에 따라 통제 분류는 달라지며, 2022판은 조직적·인적·물리적·기술적 통제의 네 주제로 재구성되었으므로 구판의 영역명을 현행 최상위 분류와 동일시하지 않는다.

NoteBase

문 25. 위험분석 방법 중 정성적 위험분석 유형으로 가장 적절하지 않은 것은?

① 델파이법

② 시나리오법

③ 순위결정법

④ 확률분포법

정답 4번

간단한 해설

확률분포법은 발생 가능성과 손실규모를 확률분포로 나타내 수치적으로 평가하는 **정량적 위험분석** 방법이다. 위험의 성격이나 상대적 우선순위를 중심으로 판단하는 정성적 분석과 구분된다.

선지별 해설

정성적 위험분석은 전문가의 판단, 위험의 높고 낮음이나 상대적 우선순위 등을 이용하여 위험을 평가한다. 정량적 위험분석은 발생확률·빈도·손실규모 등을 수치 모형으로 다룬다. 여기서 O/X는 각 기법이 문항의 정성적 분석 유형에 해당하는지를 뜻한다.

① O: 델파이법은 **전문가의 의견을 반복적으로 수렴**하여 위험을 판단하는 방법이다. 전문가들이 익명으로 응답하고, 종합된 의견을 돌려받아 판단을 수정하는 과정을 거쳐 합의에 접근한다. 이 문항에서는 이러한 경험·판단 중심의 평가를 정성적 방법으로 분류한다.

② O: 시나리오법은 **발생 가능한 사고의 전개 상황**을 구성하여 위험을 분석한다. 어떤 위협이 어떤 취약점을 통해 피해로 이어질 수 있는지 검토하고 그 영향과 대응을 판단하므로 정성적 분석 방법으로 분류된다. 시나리오에 확률이나 손실액을 부여하는 정량적 분석을 추가로 결합할 수도 있다.

③ O: 순위결정법은 위험요소들을 비교하여 **상대적 중요도와 처리 우선순위**를 정하는 방법이다. 어느 위험이 다른 위험보다 더 중요한지를 판단하는 것이 중심이며, 순서를 1위·2위처럼 숫자로 표시하더라도 위험의 절대 크기나 발생확률을 측정한 것은 아니다.

④ X: 확률분포법은 사건의 발생이나 손실규모를 **확률분포로 표현하여 수치적으로 분석**하므로 정량적 위험분석에 해당한다. 예를 들어 여러 손실규모와 각각의 발생확률을 이용해 기대손실이나 손실이 특정 수준을 넘을 가능성을 계산할 수 있다. 전문가가 확률 추정에 참여하더라도 확률분포를 이용한 분석 자체는 정량적이다.

따라서 정성적 위험분석 유형으로 적절하지 않은 것은 ④이다.

NoteBase

문 26. 정보보호 위험관리에 대한 설명으로 가장 적절하지 않은 것은?

① 위험분석의 목적은 자산을 식별하고 그 자산의 위험 수준을 측정하여, 그 위험이 허용 가능한 수준인지 아닌지 판단할 수 있는 근거를 마련하는 것이다.

② 자산은 조직이 보호해야 할 대상으로 정보, 하드웨어, 소프트웨어, 시설, 인력, 데이터베이스 등 유형 및 무형자산을 포함한다.

③ 위험분석에서 사용하는 연간예상손실액(ALE)은 단일손실예상액(SLE)과 연간발생빈도(ARO)의 곱으로 계산한다.

④ 정보보안 위험처리 방식 중 위험회피는 위험에 대한 책임을 회피하기 위해 제3자와 공유하는 것으로, 잠재적 손실을 보험 등을 통해 제3자에게 할당하는 것이다.

정답 4번

간단한 해설

보험 등을 이용해 손실 부담을 제3자에게 넘기는 것은 **위험전가 또는 위험공유**이다. 위험회피는 위험을 유발하는 활동을 중단하거나 시작하지 않는 방식이다.

선지별 해설

① O: 위험분석은 보호할 자산과 그 자산에 영향을 주는 위협·취약점을 파악하고, 위험의 발생 가능성과 영향을 분석하는 과정이다. 이를 통해 위험 수준을 조직의 허용 기준과 비교할 수 있으므로 **위험 수용 여부와 대응 우선순위의 판단 근거**를 마련한다.

② O: 정보보호에서 자산은 조직이 가치를 부여하여 보호할 필요가 있는 대상이다. 서버·시설 같은 유형 자산뿐 아니라 정보·소프트웨어·데이터베이스와 인력 및 그 전문성 등도 포함한다. 따라서 자산을 장비나 금전적 재산으로만 한정하지 않는다.

③ O: 단일손실예상액(SLE)은 사고가 한 번 발생할 때의 예상 손실액이고, 연간발생빈도(ARO)는 1년 동안 예상되는 사고 발생 횟수이다. 두 값을 곱하면 1년의 예상 손실액이 된다. 관계는 $ALE = SLE \times ARO$이며, ARO는 1보다 작은 값도 가능하다. 이는 **기대 손실액**이므로 매년 반드시 그 금액의 손실이 발생한다는 뜻은 아니다.

④ X: 보험이나 계약을 통해 손실 부담의 일부를 제3자에게 넘기거나 나누는 것은 **위험전가 또는 위험공유**이다. 위험회피는 위험을 유발하는 활동이나 서비스를 중단하거나 시작하지 않아 그 위험에 노출되지 않는 방식이다. 보험 가입으로 손실 부담을 이전하더라도 사고 발생 가능성이나 조직의 모든 책임이 사라지는 것은 아니다.

NoteBase

문 27. 보안 관제 조직 중 컴퓨터 침해 대응팀(CERT: Computer Emergency Response Team)의 역할로 가장 적절하지 않은 것은?

① 침해 사고 대응 기술 연구

② 이상 트래픽 분석을 통한 침해 여부 판단

③ 침해 사고 시스템의 사용자에 대한 조사

④ 취약점 진단과 침해 사고 예방 활동

정답 3번

간단한 해설

③의 '사용자에 대한 조사'를 **범죄 혐의를 밝히는 수사**로 보면 수사기관의 역할에 해당한다. CERT는 기술적 침해 분석과 대응을 담당하며, 이 과정에서 사용자에게 사고 경위를 확인하는 면담은 할 수 있다.

선지별 해설

① O: 침해 사고 대응 기술 연구는 공격 기법과 악성코드의 동작을 분석하고, 탐지·차단·복구 방법을 개선하는 활동이다. 사고 발생 시 **신속하고 효과적으로 대응할 기술을 확보**하는 것이므로 CERT의 역할에 해당한다.

② O: 비정상적인 통신량이나 접속 패턴을 분석하면 공격 또는 침해의 징후를 확인할 수 있다. CERT는 이러한 트래픽과 관련 로그를 분석하여 **실제 침해인지 정상 활동에 따른 이상 징후인지**를 판단한다. 트래픽이 비정상적이라는 이유만으로 침해를 확정하는 것은 아니다.

③ X: '사용자에 대한 조사'를 **사용자 개인의 범죄 혐의를 밝히는 수사**로 해석하면, 이는 수사기관의 역할에 해당한다. CERT의 중심 역할은 시스템·네트워크의 침해 원인과 피해 범위를 분석하고 대응·복구하는 것이다. 다만 사고 경위를 파악하기 위한 사용자 면담이나 행위 분석은 수행할 수 있으므로, 사용자와 관련된 조사 자체가 모두 CERT의 역할 밖이라는 뜻은 아니다.

④ O: 취약점 진단은 공격에 악용될 수 있는 시스템·네트워크의 약점을 찾아 보완하기 위한 활동이다. CERT는 취약점 정보 제공과 보완 조치 안내 등을 통해 **침해 사고의 사전 예방과 재발 방지**에도 기여한다.

NoteBase

문 28. 다음은 국제공통평가기준(CC)의 구성 요소에 대한 내용이다. 빈칸 ㉠, ㉡에 해당하는 가장 적절한 것은?

가. 같은 부류에 속하는 정보시스템은 (㉠)을(를) 새로 작성할 필요 없이 기존에 작성된 (㉠)을(를) 활용할 수 있음
나. 작성자는 정보시스템의 기술적인 구현 가능성을 고려하여 (㉡)을(를) 작성하고, 같은 부류의 제품이라도 개별적으로 정의함

① ㉠ 보호프로파일(PP) ㉡ 보안목표명세서(ST)
② ㉠ 보안목표명세서(ST) ㉡ 보호프로파일(PP)
③ ㉠ 평가보증등급(EAL) ㉡ 평가대상(TOE)
④ ㉠ 평가대상(TOE) ㉡ 평가보증등급(EAL)

정답 1번

간단한 해설

같은 부류의 제품에 공통으로 적용하는 보안 요구사항은 **보호프로파일(PP)**에, 실제 평가대상 제품의 구체적인 보안 요구사항은 **보안목표명세서(ST)**에 담는다.

빈칸별 해설

㉠ 보호프로파일(PP): PP는 특정 제품의 구현 방식에 의존하지 않고 **같은 부류의 제품에 공통으로 요구되는 보안 요구사항**을 정리한 문서이다. 따라서 적용 대상과 보안 요구가 맞는 기존 PP가 있으면 같은 부류의 정보시스템이 이를 활용할 수 있다. 개별 제품마다 전혀 새로운 PP를 작성해야 하는 것은 아니다.

㉡ 보안목표명세서(ST): ST는 **구체적인 평가대상 제품의 보안 요구사항과 구현 내용**을 기술하는 문서이다. 제품이 어떤 보안 문제를 다루고 어떤 보안 기능으로 요구사항을 충족하는지 명세하므로 실제 구현 가능성을 고려한다. 같은 부류에 속하더라도 개별 제품의 기능과 구현이 다르면 각 평가대상에 맞는 ST를 작성한다.

평가보증등급(EAL)은 평가에 적용할 보증 요구사항을 단계별로 묶은 것이며, 평가대상(TOE)은 평가받는 소프트웨어·펌웨어·하드웨어와 관련 문서 등이다. 둘은 각각 같은 부류의 보안 요구사항 문서와 개별 제품의 보안목표 문서를 뜻하는 PP·ST를 대신할 수 없다.

따라서 ㉠은 PP, ㉡은 ST이며, 이 대응에 맞는 선택지는 ①이다. ②는 두 문서의 적용 범위를 뒤바꾸었고, ③과 ④는 문서의 역할에 맞지 않는 EAL·TOE를 넣었다.

NoteBase

문 29. TCSEC 보안등급에 대한 설명으로 가장 적절하지 않은 것은?

① A1등급은 가장 높은 보안등급으로 엄격한 인증, 제한 및 감사를 요구한다.

② B1등급은 레이블된 보안 보호, 보안정책을 적용할 수 있다.

③ C1등급은 통제적 접근 보호, 각 계정별 로그인이 가능하고, 그룹 ID로 통제 가능하다.

④ D등급은 가장 낮은 등급으로 최소한의 보호만을 요구한다.

정답 3번

간단한 해설

C1은 **임의적 보안 보호**이고, '통제적 접근 보호'는 C2의 명칭이다. C1도 식별·인증과 개인·그룹별 접근 통제를 제공하며, C2에서 감사 등을 통한 개인별 책임추적성이 강화된다.

선지별 해설

TCSEC은 보안 기능과 그 기능이 신뢰할 수 있게 구현되었음을 보이는 보증 수준을 평가한다. 정규 등급은 낮은 순서로 D, C1, C2, B1, B2, B3, A1이다.

① O: A1은 정규 등급 중 가장 높은 '검증된 설계' 등급이다. 강한 접근 통제·인증·감사 요구를 포함하며, B3의 기능적 요구에 더해 **형식적 명세와 검증** 등으로 보안 설계의 타당성을 엄격하게 입증한다. 인증이나 감사만 있다는 이유로 A1이 되는 것은 아니다.

② O: B1은 **'레이블된 보안 보호'** 등급이다. 주체와 객체의 보안 등급을 나타내는 민감도 레이블을 이용하여 강제적 접근 통제 정책을 적용하고, 기존 임의적 접근 통제도 유지한다.

③ X: **'통제적 접근 보호'는 C2**의 명칭이며, C1은 '임의적 보안 보호'이다. C1도 사용자 식별·인증과 개인 또는 그룹에 따른 자원 공유 통제를 제공하므로 로그인과 그룹 통제가 전혀 없다는 뜻은 아니다. C2는 더 세밀한 접근 통제와 감사, 자원 격리 등을 통해 개인별 행위의 책임추적성을 강화한다.

④ O: D는 **'최소 보호'**로 분류되는 가장 낮은 등급이다. 정확히는 평가를 받았지만 상위 등급의 요구를 충족하지 못한 시스템을 포함한다. 이 명칭이 일정한 보안 기능이나 충분한 보호 수준을 보증한다는 뜻은 아니다.

NoteBase

문 30. 디지털 증거의 특성으로 가장 적절하지 않은 것은?

① 복제 용이성

② 비가독성

③ 대량성

④ 변조 난해성

정답 4번

간단한 해설

디지털 자료는 내용이나 메타데이터가 비교적 쉽게 변경·삭제될 수 있어 **무결성 보존과 확인**이 중요하다. 따라서 '변조 난해성'은 디지털 증거의 일반적인 특성으로 적절하지 않다.

선지별 해설

여기서 O/X는 디지털 증거의 일반적인 특성에 해당하는지를 나타낸다.

① O: 디지털 자료는 비트열을 복사하여 **내용이 동일한 복제본**을 만들 수 있다. 적절한 이미징 절차로 확보한 복제본을 분석하면 원래 저장매체를 반복해서 다루면서 변경시킬 위험을 줄일 수 있다. 다만 복제본을 만들었다는 사실만으로 정확한 복사가 보장되는 것은 아니므로 동일성과 무결성을 확인해야 한다.

② O: 저장매체에 기록된 비트열은 사람이 그 상태 그대로 내용을 읽기 어려우며, **장치와 프로그램을 통한 해석·출력**이 필요하다. 이를 비가독성이라고 한다. 화면에 표시된 문자를 읽을 수 없다는 뜻이나 모든 디지털 증거가 암호화되어 있다는 뜻은 아니다.

③ O: 디지털 저장장치에는 문서·사진·전자우편·로그 등 많은 자료가 저장되고, 시스템 사용 중에도 데이터가 지속적으로 생성될 수 있다. 따라서 **방대한 자료 속에서 관련 정보를 선별**해야 하는 대량성이 문제된다. 개별 파일 하나가 반드시 대용량이라는 의미는 아니다.

④ X: 디지털 자료의 일반적인 특성은 '변조 난해성'보다 **변경·삭제되기 쉬운 취약성**이다. 의도적 수정뿐 아니라 프로그램 실행이나 부주의한 취급으로도 내용·메타데이터가 달라질 수 있다. 이 때문에 쓰기 방지, 해시 비교, 취급 과정 기록 등을 통해 무결성을 보존하고 확인한다. 이러한 보호조치가 필요한 것과 디지털 자료 자체가 본래 변조되기 어렵다는 것은 다르다.

따라서 디지털 증거의 특성으로 적절하지 않은 것은 ④이다.

NoteBase

문 31. 다음 보기에서 설명하는 「형사소송법」 조항과 가장 관련성이 깊은 디지털포렌식의 원칙은?

제308조의2(위법수집증거의 배제) 적법한 절차에 따르지 아니하고 수집한 증거는 증거로 할 수 없다.

① 정당성의 원칙
② 무결성의 원칙
③ 재현성의 원칙
④ 신속성의 원칙

정답 1번

공통 해설

정당성의 원칙은 **디지털 증거를 적법한 절차와 방법으로 수집해야 한다**는 원칙이다. 위법수집증거의 배제는 이러한 절차적 적법성을 확보하기 위한 규정이다.

형사소송법 제308조의2(위법수집증거의 배제) 적법한 절차에 따르지 아니하고 수집한 증거는 증거로 할 수 없다.

NoteBase

문 32. 다음은 「형사소송법」 제106조(압수)에 대한 내용이다. 빈칸 ㉠, ㉡에 해당하는 가장 적절한 것은?

③ 법원은 압수의 목적물이 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체인 경우에는 기억된 정보의 범위를 정하여 출력하거나 복제하여 제출받아야 한다. 다만, 범위를 정하여 출력 또는 복제하는 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란하다고 인정되는 때에는 정보저장매체등을 압수할 수 있다.
④ 법원은 제3항에 따라 정보를 제공받는 경우 (㉠) 제2조 제3호에 따른 (㉡)에게 해당 사실을 지체 없이 알려야 한다.

① ㉠ 개인정보보호법 ㉡ 정보주체
② ㉠ 경찰관의 정보수집 및 처리등에 관한 규정 ㉡ 보관자
③ ㉠ 개인정보보호법 ㉡ 보관자
④ ㉠ 경찰관의 정보수집 및 처리등에 관한 규정 ㉡ 정보주체

정답 1번

공통 해설

법원이 정보저장매체에 저장된 정보를 제공받으면 **정보주체에게 해당 사실을 지체 없이 알려야 한다**.

형사소송법 제106조(압수)
④ 법원은 제3항에 따라 정보를 제공받은 경우 「개인정보 보호법」 제2조제3호에 따른 정보주체에게 해당 사실을 지체 없이 알려야 한다. <신설 2011.7.18>

NoteBase

문 33. OECD의 개인정보보호 원칙에 대한 설명으로 가장 적절하지 않은 것은?

① 개인 참가의 원칙: 정보주체가 제공한 개인정보에 대해 열람, 정정, 삭제를 요구할 수 있는 절차를 마련해야 한다.

② 안전성 보호의 원칙: 개인정보의 분실, 불법적인 접근, 훼손, 사용, 변조, 공개 등의 위험에 대비하여 합리적인 보호조치를 마련해야 한다.

③ 목적 명확성의 원칙: 개인정보는 그 이용목적에 부합되는 것이어야 하며 이용목적에 필요한 범위 내에서 정확하고 완전하며 최신의 상태를 유지해야 한다.

④ 공개의 원칙: 개인정보 관리자의 주소 등을 비롯하여 개인정보의 이용목적, 관련된 정책 등에 대한 내용이 포함된 공개방침이 있어야 한다.

정답 3번

간단한 해설

이용목적에 맞는 정보를 정확하고 완전하며 최신 상태로 유지하는 것은 **정보의 질 원칙**이다. 목적 명확성의 원칙은 늦어도 개인정보 수집 시점까지 수집 목적을 특정하도록 한다.

선지별 해설

① O: 개인 참가의 원칙은 정보주체가 **자신에 관한 정보의 처리에 관여할 권리**를 보장한다. 자신에 관한 정보의 보유 여부를 확인하고 내용을 열람하며, 부정확한 정보 등에 이의를 제기하여 정정·보완·삭제를 요구할 수 있어야 한다. 요구가 거절되면 그 이유를 알고 다툴 수 있어야 하며, 요청만 하면 모든 정보를 무조건 삭제해야 한다는 뜻은 아니다.

② O: 안전성 보호의 원칙은 분실, 권한 없는 접근·이용·공개, 훼손·변조 등의 위험에 대비하여 **합리적인 보안 보호조치**를 갖추라는 원칙이다. 접근 권한 통제 등 위험에 맞는 보호조치를 통해 개인정보를 안전하게 관리하도록 한다.

③ X: 이용목적과의 관련성 및 정확성·완전성·최신성 유지는 **정보의 질, 즉 데이터 품질의 원칙**이다. 목적 명확성의 원칙은 개인정보를 왜 수집하는지 늦어도 수집 시점까지 특정하고, 이후 이용을 그 목적이나 이에 양립할 수 있으며 변경 시 특정된 목적에 맞추도록 하는 원칙이다.

④ O: 공개의 원칙은 개인정보 처리에 관한 정책과 관행을 투명하게 알리는 원칙이다. 개인정보의 존재·성격, 주요 이용목적, 관리자의 신원과 소재지 등을 쉽게 확인할 수 있어야 한다. 여기서 공개하는 것은 **처리 방침과 관리에 관한 정보**이며, 개인의 정보를 누구나 볼 수 있게 공개하라는 뜻은 아니다.

NoteBase

문 34. 「개인정보보호법」상 개인정보 보호책임자의 업무로 가장 적절하지 않은 것은?

① 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
② 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
③ 개인정보의 처리와 관련한 고충처리·권리구제 및 개인정보에 관한 분쟁의 조정
④ 개인정보 보호 교육 계획의 수립 및 시행

정답 3번

①
개인정보 보호책임자는 **개인정보 처리 및 보호의 실태와 관행을 정기적으로 조사하고 개선**하는 업무를 수행한다.

개인정보 보호법 제31조(개인정보 보호책임자의 지정 등)
④ 개인정보 보호책임자는 다음 각 호의 업무를 수행한다. <개정 2023.3.14, 2026.3.10>
4. 개인정보 처리 및 보호의 실태와 관행에 대한 정기적인 조사 및 개선

②
개인정보 보호책임자는 **개인정보 유출 및 오용·남용을 방지하기 위한 내부통제시스템을 구축**한다.

개인정보 보호법 제31조(개인정보 보호책임자의 지정 등)
④ 개인정보 보호책임자는 다음 각 호의 업무를 수행한다. <개정 2023.3.14, 2026.3.10>
6. 개인정보 유출 및 오용 · 남용 방지를 위한 내부통제시스템의 구축

③
고충처리·권리구제 및 개인정보에 관한 분쟁의 조정은 **개인정보 보호위원회의 소관 사무**이다. 개인정보 보호책임자는 **개인정보 처리와 관련한 불만의 처리 및 피해 구제**를 담당한다.

개인정보 보호법 제7조의8(보호위원회의 소관 사무) 보호위원회는 다음 각 호의 소관 사무를 수행한다. <개정 2023.3.14>
4. 개인정보의 처리와 관련한 고충처리 · 권리구제 및 개인정보에 관한 분쟁의 조정

개인정보 보호법 제31조(개인정보 보호책임자의 지정 등)
④ 개인정보 보호책임자는 다음 각 호의 업무를 수행한다. <개정 2023.3.14, 2026.3.10>
5. 개인정보 처리와 관련한 불만의 처리 및 피해 구제

NoteBase

④

개인정보 보호책임자는 **개인정보 보호 교육 계획을 수립하고 시행**한다.

개인정보 보호법 제31조(개인정보 보호책임자의 지정 등)
④ 개인정보 보호책임자는 다음 각 호의 업무를 수행한다. <개정 2023.3.14, 2026.3.10>
7. 개인정보 보호 교육 계획의 수립 및 시행

NoteBase

문 35. 「개인정보보호법」 제23조(민감정보의 처리 제한)과 그 시행령 제18조(민감정보의 범위)에서 규정하는 민감정보로 가장 적절하지 않은 것은?

① 사상·신념에 관한 정보
② 교육 이력에 관한 정보
③ 정치적 견해에 관한 정보
④ 건강·성생활에 관한 정보

정답 2번

①

법률은 **사상·신념에 관한 정보를 민감정보로 명시**한다.

개인정보 보호법 제23조(민감정보의 처리 제한)
①개인정보처리자는 사상 · 신념, 노동조합 · 정당의 가입 · 탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보(이하 "민감정보"라 한다)를 처리하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다. <개정 2016.3.29>
1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우
2. 법령에서 민감정보의 처리를 요구하거나 허용하는 경우

NoteBase

②

교육 이력에 관한 정보는 **법률과 시행령이 정한 민감정보 항목에 포함되지 않는다**.

개인정보 보호법 제23조(민감정보의 처리 제한)
①개인정보처리자는 사상 · 신념, 노동조합 · 정당의 가입 · 탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보(이하 "민감정보"라 한다)를 처리하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다. <개정 2016.3.29>
1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우
2. 법령에서 민감정보의 처리를 요구하거나 허용하는 경우

개인정보 보호법 시행령 제18조(민감정보의 범위) 법 제23조제1항 각 호 외의 부분 본문에서 "대통령령으로 정하는 정보"란 다음 각 호의 어느 하나에 해당하는 정보를 말한다. 다만, 공공기관이 법 제18조제2항제5호부터 제9호까지의 규정에 따라 다음 각 호의 어느 하나에 해당하는 정보를 처리하는 경우의 해당 정보는 제외한다. <개정 2016.9.29, 2020.8.4>
1. 유전자검사 등의 결과로 얻어진 유전정보
2. 「형의 실효 등에 관한 법률」 제2조제5호에 따른 범죄경력자료에 해당하는 정보
3. 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 정보
4. 인종이나 민족에 관한 정보

③

법률은 **정치적 견해에 관한 정보를 민감정보로 명시**한다.

개인정보 보호법 제23조(민감정보의 처리 제한)
①개인정보처리자는 사상 · 신념, 노동조합 · 정당의 가입 · 탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보(이하 "민감정보"라 한다)를 처리하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다. <개정 2016.3.29>
1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우
2. 법령에서 민감정보의 처리를 요구하거나 허용하는 경우

NoteBase

④

법률은 **건강과 성생활에 관한 정보를 민감정보로 명시**한다.

개인정보 보호법 제23조(민감정보의 처리 제한)
①개인정보처리자는 사상 · 신념, 노동조합 · 정당의 가입 · 탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보(이하 "민감정보"라 한다)를 처리하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다. <개정 2016.3.29>
1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우
2. 법령에서 민감정보의 처리를 요구하거나 허용하는 경우

NoteBase

문 37. 「개인정보보호법」 제3절 가명정보의 처리에 관한 특례에 관한 설명으로 가장 적절하지 않은 것은?

① 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있다.

② 개인정보처리자는 가명정보를 처리하는 과정에서 특정 개인을 알아볼 수 있는 정보가 생성된 경우에는 즉시 해당 정보의 처리를 중지하고, 지체 없이 회수·파기하여야 한다.

③ 개인정보처리자는 가명정보를 제3자에게 제공하는 경우에는 특정 개인을 알아보기 위하여 사용될 수 있는 정보를 포함해서는 아니 된다.

④ 개인정보처리자는 가명 정보 결합을 수행한 기관 외부로 결합된 정보를 반출하려는 경우에는 소속기관의 장의 승인을 받아야 한다.

정답 4번

①

통계작성·과학적 연구·공익적 기록보존 등을 위한 가명정보 처리는 **정보주체의 동의 없이 가능**하다.

개인정보 보호법 제28조의2(가명정보의 처리 등)
① 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있다.

②

통계작성 등을 위한 가명정보 처리 과정에서 특정 개인을 알아볼 수 있는 정보가 생성되면 **즉시 해당 정보의 처리를 중지하고, 지체 없이 회수·파기**하여야 한다.

개인정보 보호법 제28조의5(가명정보 처리 시 금지의무 등)
② 개인정보처리자는 제28조의2 또는 제28조의3에 따라 가명정보를 처리하는 과정에서 특정 개인을 알아볼 수 있는 정보가 생성된 경우에는 즉시 해당 정보의 처리를 중지하고, 지체 없이 회수 · 파기하여야 한다. <개정 2023.3.14>

③

통계작성 등의 목적으로 가명정보를 제3자에게 제공할 때에는 **특정 개인을 알아보는 데 사용될 수 있는 정보를 포함해서는 안 된다**.

개인정보 보호법 제28조의2(가명정보의 처리 등)
② 개인정보처리자는 제1항에 따라 가명정보를 제3자에게 제공하는 경우에는 특정 개인을 알아보기 위하여 사용될 수 있는 정보를 포함해서는 아니 된다.

NoteBase

④

결합된 정보를 기관 외부로 반출할 때 승인권자는 **결합을 수행한 전문기관의 장**이다.

개인정보 보호법 제28조의3(가명정보의 결합 제한)
② 결합을 수행한 기관 외부로 결합된 정보를 반출하려는 개인정보처리자는 가명정보 또는 제58조의2에 해당하는 정보로 처리한 뒤 전문기관의 장의 승인을 받아야 한다.

NoteBase

문 39. 다음 보기에서 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조의 정보보호 관리체계 인증(ISMS) 의무 대상자를 모두 고른 것으로 가장 적절한 것은?

가. 집적정보통신시설 사업자
나. 전기통신사업법 제6조 1항에 따른 등록을 한 자로서 대통령령으로 정하는 바에 따라 정보통신망서비스를 제공하는 자
다. 연간 매출액 1000억 이상의 상급 종합병원
라. 정보통신서비스 부문 전년도(법인의 경우 전 사업연도를 말한다) 매출액이 50억원 이상인 자
마. 정보통신서비스 부문 3개월 간의 일일평균 이용자수가 100만명 이상인 자

① 가, 나
② 가, 마
③ 나, 다, 마
④ 나, 라, 마

정답 1번

가

집적정보통신시설 사업자는 정보보호 관리체계 인증을 받아야 하는 의무대상자로 명시되어 있다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제47조(정보보호 관리체계의 인증)
② 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자로서 다음 각 호의 어느 하나에 해당하는 자는 제1항에 따른 인증을 받아야 한다. <신설 2012.2.17, 2015.12.1, 2018.12.24, 2020.6.9, 2024.1.23, 2026.3.31>
2. 집적정보통신시설 사업자

NoteBase

나

등록을 하고 대통령령에서 정한 범위의 정보통신망서비스를 제공하는 자는 **주요정보통신서비스 제공자**에 해당하므로 정보보호 관리체계 인증을 받아야 한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제45조(정보통신망의 안정성 확보 등)
⑤ 「전기통신사업법」 제6조제1항에 따른 등록을 한 자로서 대통령령으로 정하는 바에 따라 정보통신망서비스를 제공하는 자(이하 "주요정보통신서비스 제공자"라 한다), 제46조제1항제1호에 따른 집적정보통신시설 사업자, 그 밖에 대통령령으로 정하는 정보통신서비스 제공자는 정보보호 분야 전문성을 갖춘 인력과 충분한 예산을 확보하도록 노력하여야 한다. <신설 2026.3.31>

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제47조(정보보호 관리체계의 인증)
② 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자로서 다음 각 호의 어느 하나에 해당하는 자는 제1항에 따른 인증을 받아야 한다. <신설 2012.2.17, 2015.12.1, 2018.12.24, 2020.6.9, 2024.1.23, 2026.3.31>
1. 주요정보통신서비스 제공자

다

상급종합병원의 의무인증 매출액·세입 기준은 **전년도 1,500억원 이상**이다. 1,000억원 이상이라는 기준은 법정 기준보다 낮다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제47조(정보보호 관리체계의 인증)
② 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자로서 다음 각 호의 어느 하나에 해당하는 자는 제1항에 따른 인증을 받아야 한다. <신설 2012.2.17, 2015.12.1, 2018.12.24, 2020.6.9, 2024.1.23, 2026.3.31>
3. 전년도 매출액 또는 세입 등이 1,500억원 이상이거나 정보통신서비스 부문 전년도 매출액이 100억원 이상 또는 전년도 일일평균 이용자수 100만명 이상으로서, 대통령령으로 정하는 기준에 해당하는 자

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제49조(정보보호 관리체계 인증 대상자의 범위)
② 법 제47조제2항제3호에서 "대통령령으로 정하는 기준에 해당하는 자"란 다음 각 호의 어느 하나에 해당하는 자를 말한다. <개정 2016.5.31, 2024.7.23>
1. 전년도 매출액 또는 세입이 1,500억원 이상인 자로서 다음 각 목의 어느 하나에 해당하는 자
가. 「의료법」 제3조의4에 따른 상급종합병원

NoteBase

라

정보통신서비스 부문의 매출액에 따른 의무인증 기준은 **전년도 매출액 100억원 이상**이다. 50억원 이상이라는 사실만으로는 이 기준을 충족하지 않는다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제47조(정보보호 관리체계의 인증)
② 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자로서 다음 각 호의 어느 하나에 해당하는 자는 제1항에 따른 인증을 받아야 한다. <신설 2012.2.17, 2015.12.1, 2018.12.24, 2020.6.9, 2024.1.23, 2026.3.31>
3. 전년도 매출액 또는 세입 등이 1,500억원 이상이거나 정보통신서비스 부문 전년도 매출액이 100억원 이상 또는 전년도 일일평균 이용자수 100만명 이상으로서, 대통령령으로 정하는 기준에 해당하는 자

마

이용자 수 기준은 3개월 평균이 아니라 **전년도 일일평균 이용자 수 100만 명 이상**이다. 다만, 전자금융거래법상 금융회사는 이 기준의 인증 의무 대상에서 제외된다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제47조(정보보호 관리체계의 인증)
② 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자로서 다음 각 호의 어느 하나에 해당하는 자는 제1항에 따른 인증을 받아야 한다. <신설 2012.2.17, 2015.12.1, 2018.12.24, 2020.6.9, 2024.1.23, 2026.3.31>
3. 전년도 매출액 또는 세입 등이 1,500억원 이상이거나 정보통신서비스 부문 전년도 매출액이 100억원 이상 또는 전년도 일일평균 이용자수 100만명 이상으로서, 대통령령으로 정하는 기준에 해당하는 자

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제49조(정보보호 관리체계 인증 대상자의 범위)
② 법 제47조제2항제3호에서 "대통령령으로 정하는 기준에 해당하는 자"란 다음 각 호의 어느 하나에 해당하는 자를 말한다. <개정 2016.5.31, 2024.7.23>
3. 전년도 일일평균 이용자 수가 100만명 이상인 자. 다만, 「전자금융거래법」 제2조제3호에 따른 금융회사는 제외한다.

NoteBase

문 40. 다음은 「정보통신기반보호법」 제3조 정보통신기반보호위원회에 대한 내용이다. 빈칸 ㉠, ㉡에 해당하는 가장 적절한 것은?

① 제8조에 따라 지정된 주요정보통신기반시설의 보호에 관한 사항을 심의하기 위하여 국무총리 소속하에 정보통신기반보호위원회(이하 '위원회'라 한다)를 둔다.
② 위원회의 위원은 위원장 1인을 포함한 (㉠)인 이내의 위원으로 구성한다.
③ 위원회의 위원장은 (㉡)이 되고, 위원회의 위원은 대통령령으로 정하는 중앙행정기관의 차관급 공무원과 위원장이 위촉하는 사람으로 한다.

① ㉠ 20 ㉡ 국무조정실장
② ㉠ 25 ㉡ 국무조정실장
③ ㉠ 20 ㉡ 과학기술정보통신부 장관
④ ㉠ 25 ㉡ 과학기술정보통신부 장관

정답 2번

㉠

정보통신기반보호위원회는 **위원장 1인을 포함하여 25인 이내**의 위원으로 구성한다.

정보통신기반 보호법 제3조(정보통신기반보호위원회)
②위원회의 위원은 위원장 1인을 포함한 25인 이내의 위원으로 구성한다.

㉡

위원장은 **국무조정실장**이며, 위원은 **대통령령으로 정하는 중앙행정기관의 차관급 공무원과 위원장이 위촉하는 사람**으로 한다.

정보통신기반 보호법 제3조(정보통신기반보호위원회)
③위원회의 위원장은 국무조정실장이 되고, 위원회의 위원은 대통령령으로 정하는 중앙행정기관의 차관급 공무원과 위원장이 위촉하는 사람으로 한다. <개정 2007.12.21, 2008.2.29, 2013.3.23, 2020.6.9>

NoteBase