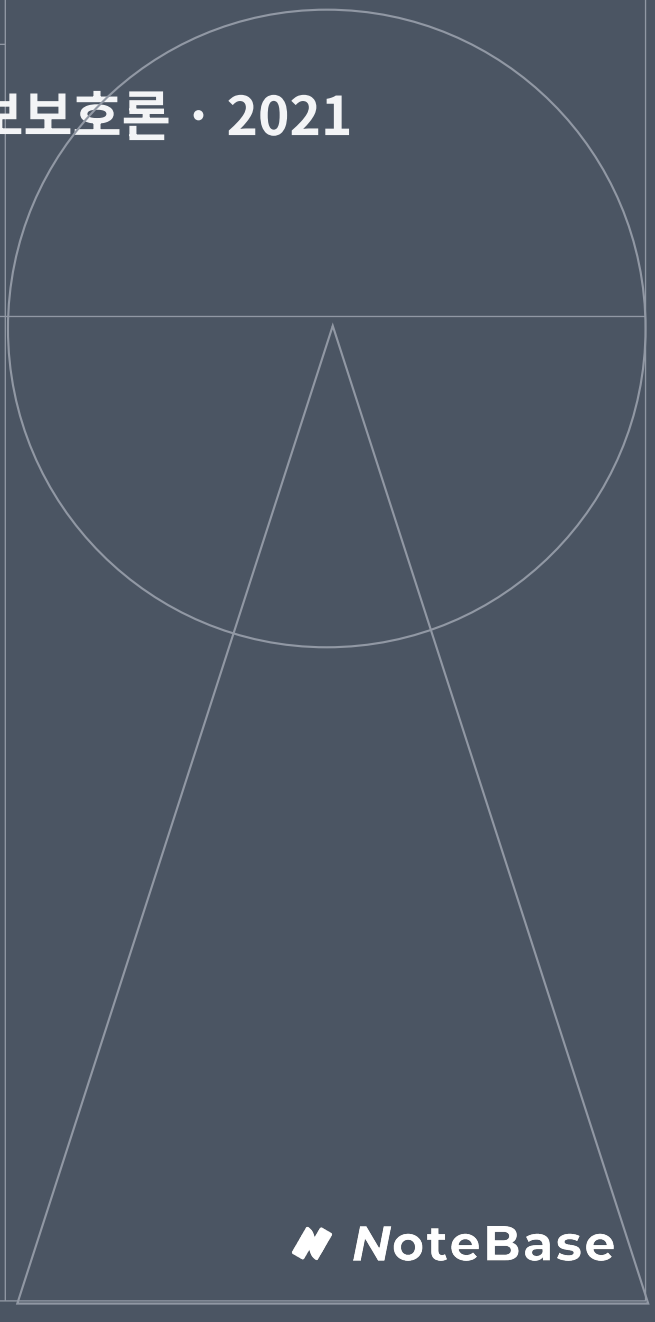
기출OX 해설집

공무원/경찰/경력채용 · 정보보호론 · 2021



NoteBase

기출OX 해설집

공무원/경찰/경력채용 · 정보보호론 · 2021

공무원/경찰/경력채용 · 정보보호론 · 2021

문 1. 정보보호의 속성에 대하여 <보기 1>의 설명과 <보기 2>의 용어를 가장 적절하게 연결한 것은?

<보기 1>
(가) 허락되지 않은 사용자 또는 객체가 정보를 함부로 수정할 수 없도록 하는 것이다.
(나) 허락된 사용자 또는 객체가 정보에 접근하고자 할 때 방해받지 않도록 하는 것이다.
(다) 허락되지 않은 사용자 또는 객체가 정보의 내용을 알 수 없도록 하는 것이다.
(라) 어떤 주체나 객체가 틀림없음을 보장하는 것이다.
<보기 2>
㉠ 무결성(Integrity)
㉡ 가용성(Availability)
㉢ 기밀성(Confidentiality)
㉣ 인증성(Authentication)

① (가): ㉣, (나): ㉡, (다): ㉢, (라): ㉠
② (가): ㉡, (나): ㉠, (다): ㉣, (라): ㉢
③ (가): ㉠, (나): ㉡, (다): ㉢, (라): ㉣
④ (가): ㉢, (나): ㉣, (다): ㉠, (라): ㉡

정답 3번

간단한 해설

무단 수정 방지는 무결성, 정당한 접근의 보장은 가용성, 내용의 비공개는 기밀성, 대상의 진위 확인은 인증성에 해당한다. 각 설명이 보호하려는 대상과 행위를 구별하면 연결할 수 있다.

NoteBase

대응 관계 해설

(가) → ㉠ 무결성: 허락되지 않은 사용자나 객체가 정보를 수정하지 못하게 하는 것은 **정보의 무단 변경을 방지**하는 무결성이다. 정보가 원래의 정확한 상태로 유지되는지가 기준이며, 내용을 읽지 못하게 하는 기밀성과 구별된다.

(나) → ㉡ 가용성: 허락된 사용자나 객체가 필요할 때 방해받지 않고 정보에 접근하는 것은 **정당한 이용자가 필요한 때 사용할 수 있음**을 뜻한다. 서비스 중단이나 접근 방해로 이용할 수 없게 되면 가용성이 침해된다.

(다) → ㉢ 기밀성: 허락되지 않은 사용자나 객체가 정보의 내용을 알 수 없도록 하는 것은 **인가되지 않은 열람과 공개를 막는** 기밀성이다. 내용을 몰래 읽는 행위는 정보를 수정하지 않더라도 기밀성을 침해할 수 있다.

(라) → ㉣ 인증성: 주체나 객체가 주장하는 대상과 실제로 일치하는지 확인하는 것은 **신원이나 출처의 진위를 확인**하는 인증에 해당한다. 다른 대상을 사칭한 것이 아님을 확인한다는 점이 앞의 세 속성과 구별된다.

따라서 (가) ㉠, (나) ㉡, (다) ㉢, (라) ㉣으로 연결되므로 정답은 ③이다.

NoteBase

문 2. 보안 공격(Security Attack)에 대한 설명으로 가장 적절하지 않은 것은?

① 적극적 공격(Active Attack)은 무결성과 가용성을 위협하며 변경, 재전송, 서비스 거부 공격 등이 있다.

② 대부분의 적극적 공격은 상당 기간 동안의 수동적 공격 수행을 통해 수집된 정보를 바탕으로 수행된다.

③ 소극적 공격(Passive Attack)은 기밀성을 위협하며 스누핑(Snooping), 트래픽 분석 공격 등이 있다.

④ 소극적 공격은 시스템 작동에 치명적인 피해를 입히며 예방보다는 탐지가 중요하다.

정답 4번

간단한 해설

소극적 공격은 시스템 동작을 바꾸지 않고 정보를 수집하여 기밀성을 위협한다. 탐지하기 어려우므로 **예방에 중점**을 두며, 시스템 동작에 직접 피해를 주고 탐지가 더 중요하다는 설명은 맞지 않는다.

선지별 해설

① O: 적극적 공격은 데이터를 바꾸거나 시스템의 정상 동작에 영향을 주는 공격이다. 메시지 변경과 재전송은 무결성·인증을 위협하고, 서비스 거부는 정상적인 자원 이용을 방해하여 가용성을 위협한다.

② O: 이 선지는 수동적인 정보 수집을 후속 공격에 활용하는 준비 과정을 설명한다. 도청이나 트래픽 관찰로 얻은 통신 정보 등을 재전송·위장과 같은 적극적 공격에 이용할 수 있다. 다만 모든 적극적 공격에 장기간의 수동적 공격이 필수인 것은 아니며, '대부분'과 '상당 기간'은 공격의 정의나 고정된 수행 조건이 아니다.

③ O: 소극적 공격은 데이터나 시스템 동작을 바꾸지 않고 정보를 알아내려는 공격이다. 스누핑은 통신 내용 등을 엿보고, 트래픽 분석은 통신의 상대·시점·빈도 같은 특성에서 정보를 추론하므로 기밀성을 위협한다.

④ X: 소극적 공격은 시스템 동작을 직접 훼손하는 공격이 아니라 정보를 관찰·수집하는 공격이다. 흔적이 잘 드러나지 않아 탐지가 어려우므로 **탐지보다 예방**에 중점을 둔다. 암호화로 내용 노출을 줄이고, 필요하면 트래픽 패딩 등으로 통신 패턴의 노출도 줄인다. 시스템 동작 방해는 적극적 공격의 특성이다.

NoteBase

문 3. 스테가노그래피(Steganography)에 대한 설명으로 가장 적절하지 않은 것은?

① 비밀정보를 매체에 은닉하여 그 정보의 존재 자체를 숨기는 보안 기술이다.

② 메시지 정보를 은닉하며 트래킹이 불가능하다.

③ 비밀키를 이용하여 제3자가 메시지 내용을 알 수 없도록 변경하는 기술이다.

④ 정보가 제3자로부터 불법적으로 사용 및 변조되는 것을 방어하는 기술이다.

정답 3번

간단한 해설

스테가노그래피는 **정보의 존재를 숨기고**, 암호화는 내용을 알아볼 수 없는 형태로 바꾼다. 비밀키를 이용한 내용 변경은 암호화의 설명이다.

선지별 해설

① O — 스테가노그래피는 이미지·음성 등의 매체 안에 비밀정보를 넣어 **정보의 존재 자체**를 숨기는 기술이다. 제3자가 비밀 메시지가 있다는 사실을 알아차리기 어렵게 하는 데 목적이 있다.

② X — 메시지를 은닉한다는 부분은 맞지만, **트래킹이 불가능하다**고 단정한 부분은 부정확하다. 은닉 흔적이나 관련 처리·통신 행위를 분석하여 탐지할 수 있으므로, 탐지와 추적을 어렵게 하는 기술이라고 이해해야 한다.

③ X — 비밀키로 메시지 내용을 알아볼 수 없게 바꾸는 것은 **암호화**의 설명이다. 스테가노그래피의 본질은 내용을 암호문으로 바꾸는 것이 아니라 메시지의 존재를 숨기는 것이다. 암호화한 메시지를 다시 매체에 숨겨 두 기술을 함께 사용할 수는 있다.

④ O(보호 취지에 한정) — 정보를 숨겨 노출을 줄이면 제3자의 불법적인 사용·변조를 어렵게 하는 데 기여할 수 있다. 다만 **은닉 자체가 사용 통제나 무결성을 보장하지는 않는다**. 접근 제한이나 변조 검증이 필요하면 별도의 보안 수단을 함께 사용해야 하므로, 선지를 독립적인 변조 방지 보장으로 이해하면 부정확하다.

이 문항에서 스테가노그래피를 다른 기술인 암호화의 정의와 직접 혼동한 선지는 ③이다. ②의 절대적 표현과 ④의 보호 범위에도 위와 같은 한계가 있다.

NoteBase

문 4. 종단 간 암호화(End-to-End Encryption)에 대한 설명으로 가장 적절하지 않은 것은?

① 헤더를 포함한 모든 데이터를 암호화한다.

② 알고리즘에 대한 통제는 사용자가 한다.

③ 사용자 인증 등 보안 서비스 제공이 가능하다.

④ 중간 노드에서도 데이터가 암호문으로 존재한다.

정답 1번

간단한 해설

종단 간 암호화에서도 **전달 경로 결정에 필요한 헤더 정보**는 중간 장비가 읽을 수 있어야 한다. 헤더를 포함한 모든 데이터를 암호화한다고 한 ①이 적절하지 않다.

선지별 해설

① X: 종단 간 암호화는 통신 내용을 보호하지만, 중간 장비가 전달 경로를 결정할 수 있도록 **라우팅에 필요한 헤더 정보는 볼 수 있어야** 한다. 따라서 헤더를 포함한 모든 정보를 암호화한다는 설명은 성립하지 않는다. 일부 상위 계층 헤더가 암호화될 수 있다는 점과 모든 헤더가 감춰진다는 주장은 구별한다.

② O: 암호화와 복호화의 통제는 중간 전달망보다 **통신 양 끝의 사용자 측**에 있다. 송수신 종단의 시스템이 사용할 암호 방식과 키를 관리하여 중간 노드의 보호 기능에 의존하지 않고 내용을 보호한다. 사용자가 암호 알고리즘을 직접 구현해야 한다는 뜻은 아니다.

③ O: 종단 간 보안 통신에 상대의 신원을 확인하는 인증 절차나 전자서명 등을 함께 적용하면 **사용자 인증 등의 보안 서비스**도 제공할 수 있다. 다만 암호화만 했다는 사실이 상대의 신원을 자동으로 보증하는 것은 아니므로 인증 절차와 구별한다.

④ O: 송신 종단에서 암호화한 내용은 전달 중간의 노드에서 복호화하지 않고 **수신 종단에 도달할 때까지 암호문**으로 유지한다. 중간 라우터가 전달 정보를 읽는 것과 보호된 통신 내용의 평문을 읽는 것은 다르다.

따라서 가장 적절하지 않은 설명은 ①이다.

NoteBase

문 5. 보안모델에 대한 설명으로 가장 적절하지 않은 것은?

① 만리장성(Chinese Wall) 모델은 주체와 객체 사이에서 이해충돌을 야기하는 방식으로 정보가 전달되지 않도록 한다.

② 벨-라파듈라(Bell-LaPadula) 모델은 보안단계가 높은 정보가 보안단계가 낮은 사용자에게 전달되는 것을 방지하는 기밀성 유지의 특성을 가진다.

③ 비바(Biba) 모델은 벨-라파듈라 모델의 단점을 보완한 모델로 무결성을 보장할 수 있다.

④ 클락-윌슨(Clark-Wilson) 모델은 무결성 보장을 못하지만 모든 보안모델에 기본적으로 사용된다.

정답 4번

간단한 해설

Clark-Wilson은 **무결성 보장을 목적으로 하는 모델**이다. 잘 형성된 트랜잭션과 직무 분리로 부적절한 데이터 변경을 막으므로 무결성을 보장하지 못한다는 설명이 틀렸다.

선지별 해설

① O: Chinese Wall은 **이해충돌을 일으키는 정보 접근과 흐름**을 제한한다. 예를 들어 한 회사의 비공개 정보를 읽은 주체가 같은 이해충돌 집합에 속한 경쟁 회사의 비공개 정보에 접근하지 못하게 하며, 과거의 접근 이력에 따라 이후의 허용 범위가 달라진다.

② O: Bell-LaPadula는 높은 보안등급의 정보가 낮은 등급으로 유출되지 않도록 하는 **기밀성 중심** 모델이다. 기본 규칙인 상위 등급 읽기 금지(No Read Up)와 하위 등급 쓰기 금지(No Write Down)를 통해 정보의 하향 유출을 제한한다.

③ O: Biba는 데이터가 부적절하게 변경되지 않도록 **무결성 보호**를 다루는 모델이다. 선지의 '보완'은 기밀성을 주된 목적으로 하는 Bell-LaPadula만으로는 다루지 못하는 무결성 요구를 다룬다는 의미이다. Biba 자체가 기밀성과 무결성을 모두 자동으로 보장한다는 뜻은 아니다.

④ X: Clark-Wilson은 **잘 형성된 트랜잭션과 직무 분리**를 통해 무결성을 보호하는 모델이다. 데이터를 정해진 검증된 처리 절차로만 변경하게 하고 역할을 분리하여 부정행위와 오류를 줄인다. 따라서 '무결성 보장을 못한다'는 설명은 반대이며, 모든 보안모델에 기본적으로 쓰이는 공통 모델이라는 설명도 맞지 않는다.

무결성 모델인 Clark-Wilson의 특성을 부정한 ④가 가장 적절하지 않은 설명이다.

NoteBase

문 6. 다음에서 설명하는 대칭키 암호 알고리즘의 유형으로 가장 적절한 것은?

· 선정 기준은 안전성, 비용, 구현 효율성이며 Rijndael이 최종 선정되었다.
· 암호화 과정의 각 라운드는 [바이트치환(Substitute Bytes)] → [행이동(Shift Rows)] → [열혼합(Mix Columns)] → [라운드키더하기(Add Round Key)] 단계의 변환을 적용한다.
· 마지막 라운드는 [열혼합(Mix Columns)] 단계를 제외한 3개의 변환을 적용한다.

① AES(Advanced Encryption Standard)
② Blowfish
③ ARIA(Academy Research Institute Agency)
④ DES(Data Encryption Standard)

정답 1번

간단한 해설

Rijndael을 채택하고, 일반 라운드의 네 변환 중 **마지막 라운드에서 열혼합을 생략**하는 알고리즘은 AES이다.

핵심 풀이

선정 이력: AES는 안전성, 비용, 구현 특성 등을 평가한 공개 공모를 거쳐 Rijndael을 채택한 대칭키 블록 암호 표준이다. ‘Rijndael이 최종 선정되었다’는 단서만으로도 ① AES를 특정할 수 있다.

일반 라운드: 암호화 시작 시 초기 라운드키 더하기를 수행한 뒤, 마지막 라운드 전까지 바이트치환 → 행이동 → 열혼합 → 라운드키더하기를 적용한다. 바이트치환은 각 바이트를 S-Box로 치환하고, 행이동과 열혼합은 데이터의 위치와 값을 섞으며, 라운드키더하기는 현재 상태와 라운드키를 XOR한다.

마지막 라운드: 열혼합을 생략하고 **바이트치환 → 행이동 → 라운드키더하기**만 수행한다. 따라서 마지막에도 네 변환을 모두 수행하는 것이 아니며, 이 예외 규칙 역시 AES의 암호화 구조와 일치한다.

NoteBase

문 7. 블록 암호의 운영 모드인 CBC(Cipher Block Chaining)에 대한 설명으로 가장 적절한 것은?

① 각각의 평문 블록은 암호화되기 전에 이전 암호문 블록과 AND 연산한다.

② 전송 도중 암호문 블록 C_j에서 한 비트 오류가 발생하면 평문 블록 P_j에서 한 비트에서만 오류가 발생된다.

③ 초기벡터가 필요하며 암호화에서는 병렬처리를 할 수 없다.

④ 내부적으로 1씩 증가하는 카운터(Counter)가 필요하다.

정답 3번

간단한 해설

CBC는 첫 블록에 초기벡터를 사용하고, 이후에는 **이전 암호문 블록에 의존하여 순차적으로 암호화**한다. 따라서 초기벡터가 필요하며 암호화의 블록별 병렬 처리가 불가능하다는 설명이 부합한다.

선지별 해설

① X: 평문과 이전 암호문을 결합하는 연산은 AND가 아니라 **배타적 논리합(XOR)**이다. 키 K의 암호화 함수를 E_K, 평문과 암호문 블록을 각각 P_j, C_j라 하면 $C_j = E_K(P_j \oplus C_{j-1})$로 계산한다. 첫 블록에서는 이전 암호문 대신 초기벡터 $C_0 = IV$를 사용한다.

② X: CBC 복호화는 $P_j = D_K(C_j) \oplus C_{j-1}$이므로, C_j의 한 비트 오류가 복호화 함수 D_K의 입력을 바꾸어 **현재 평문 블록의 여러 비트에 오류**를 일으킬 수 있다. 다음 블록이 있으면 $P_{j+1} = D_K(C_{j+1}) \oplus C_j$에서 **같은 위치의 한 비트만 반전**된다. 따라서 현재 블록의 한 비트에만 오류가 생긴다는 설명은 잘못이다.

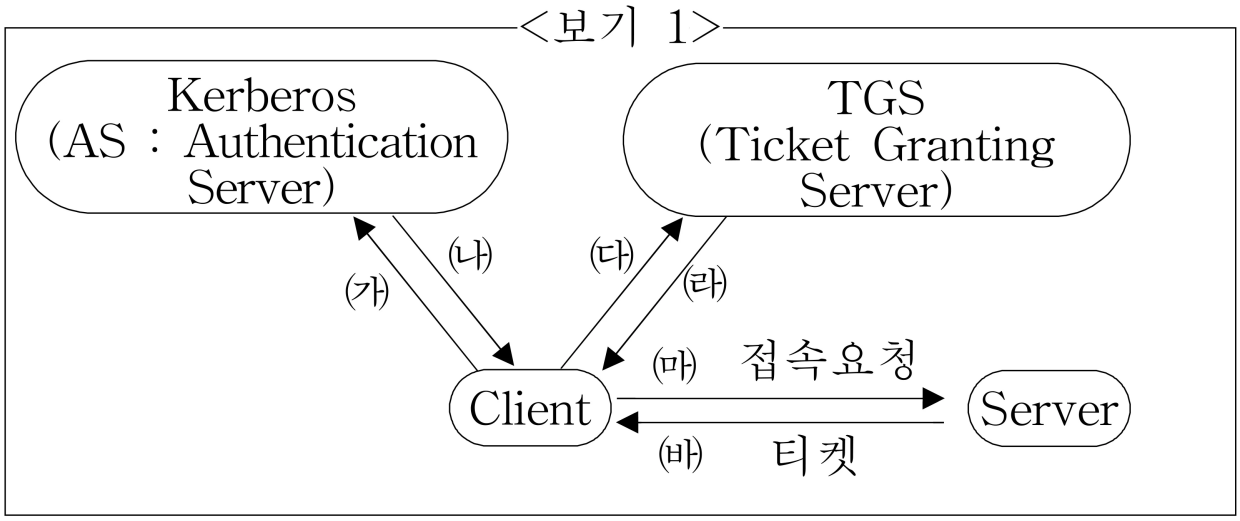
③ O: 첫 평문 블록과 결합할 초기벡터가 필요하다. 또한 하나의 CBC 연쇄에서 현재 암호문을 만들려면 **이전 블록의 암호화 결과를 먼저 알아야 하므로** 블록별 암호화를 병렬로 수행할 수 없다. 반면 복호화는 이미 받은 암호문 블록들을 입력으로 사용하므로 블록별 병렬 처리가 가능하다.

④ X: 카운터 값을 변화시키며 블록 암호에 입력하는 방식은 **CTR 모드**의 특징이다. CBC는 카운터가 아니라 초기벡터와 이전 암호문 블록을 연결에 사용한다. CTR에서는 같은 키 아래 카운터 블록이 중복되지 않게 관리하며, 값을 1씩 증가시키는 방식이 대표적인 구성 방법이다.

NoteBase

문 8. 다음은 커버로스(Kerberos)에 대한 인증 절차를 나타낸 것이다. <보기 1>의 (가)~(라)와 <보기 2>의 용어를 가장 적절하게 연결한 것은?

<보기 1>



<보기 2>

㉠ 패스워드

㉡ 인증값

㉢ 티켓

① (가): ㉠, (나): ㉡, (다): ㉡, (라): ㉢

② (가): ㉡, (나): ㉠, (다): ㉢, (라): ㉡

③ (가): ㉠, (나): ㉢, (다): ㉢, (라): ㉡

④ (가): ㉡, (나): ㉠, (다): ㉠, (라): ㉢

정답 1번

간단한 해설

커버로스에서는 **패스워드 기반 초기 인증**을 거친 뒤 그 인증 결과로 TGS에 서비스 티켓을 요청한다. 도식의 용어 대응과 실제 메시지 구성은 구분해야 하며, **패스워드 자체는 네트워크로 전송하지 않는다**.

NoteBase

도식 해설

커버로스는 인증 서버(AS)에서 초기 인증을 거친 뒤 티켓 발급 서버(TGS)를 통해 서비스 이용에 필요한 티켓을 얻는다. 이 도식의 용어는 각 단계의 역할을 간략히 표현한 것이므로 **실제 전송 메시지의 구성과 구분**해야 한다.

(가) Client → AS: 문항에서는 초기 인증의 기반을 ㉠ **패스워드**로 연결한다. 다만 패스워드 기반 방식에서도 패스워드는 클라이언트 내부에서 키를 도출하는 데 쓰이며, **패스워드 자체를 AS로 전송하지 않는다**. 이 화살표는 패스워드 자체의 전송을 의미하지 않는다.

(나) AS → Client: 문항의 ㉡ **인증값**에 해당하는 초기 인증 결과이다. 실제 AS 응답에는 TGS에 제시할 티켓인 TGT와, 클라이언트가 사용할 세션 키 등을 담은 암호화 자료가 포함된다. 따라서 '인증값'은 이 응답 전체를 엄밀하게 명명한 프로토콜 용어가 아니라 도식의 간략한 표현이다.

(다) Client → TGS: 앞 단계의 인증 결과를 바탕으로 서비스 티켓을 요청하므로 문항에서는 ㉡ **인증값**으로 연결한다. 실제 요청에는 **TGT와 인증자(authenticator)**가 들어간다. 인증자는 클라이언트의 신원·시각 등의 정보를 세션 키로 보호한 것으로, TGT와 함께 정당한 요청임을 확인하는 데 쓰인다. 패스워드를 다시 보내는 단계가 아니다.

(라) TGS → Client: 요청한 서버를 이용할 수 있도록 ㉢ **티켓**을 발급하는 단계이다. 실제 TGS 응답에는 해당 서버에 제시할 서비스 티켓과 클라이언트가 사용할 세션 키 등의 암호화 자료가 포함된다.

(마)에서는 클라이언트가 서비스 티켓과 인증자를 서버에 제시하여 접속을 요청한다.

(바)의 원본 '티켓' 표기는 실제 절차와 차이가 있다. 상호 인증을 하는 경우 서버의 응답은 **AP-REP**이며, 서버가 클라이언트에게 새 서비스 티켓을 발급하는 과정이 아니다.

따라서 문항의 간략한 역할 대응은 (가) ㉠, (나) ㉡, (다) ㉡, (라) ㉢으로, ①에 해당한다.

NoteBase

문 9. 인증기관(Certification Authority)에 대한 설명으로 가장 적절하지 않은 것은?

① 공개키 인증서를 발행하고 필요에 따라 취소한다.

② 사용자의 개인키를 포함한 인증정보를 인증기관의 개인키로 서명한다.

③ 인증서 위조를 방지하기 위해서 인증기관의 공개키는 반드시 신뢰할 수 있어야 한다.

④ 인증서 폐지목록(Certificate Revocation List) 등을 관리한다.

정답 2번

간단한 해설

인증기관이 서명하는 인증정보에는 **사용자의 공개키**가 들어간다. 인증기관의 개인키는 서명 생성에 사용하지만, 사용자의 개인키를 인증서에 담는 것은 아니다.

선지별 해설

① O — 인증기관은 사용자의 신원과 공개키를 연결하는 **공개키 인증서를 발행**한다. 개인키 유출 등으로 인증서를 더 이상 신뢰할 수 없으면 유효기간이 남아 있어도 폐지할 수 있다.

② X — 인증서에 포함하는 것은 **사용자의 공개키**이며, 개인키가 아니다. 인증기관은 사용자의 공개키와 신원 등 인증서 내용에 **인증기관의 개인키**로 서명한다. 사용자의 개인키는 비밀로 보호해야 하므로 공개적으로 배포되는 인증서에 넣지 않는다.

③ O — 인증서의 서명은 **신뢰할 수 있는 인증기관의 공개키**로 검증해야 한다. 이 공개키가 공격자의 키로 바뀌면 공격자가 만든 서명을 정상으로 받아들일 수 있다. 따라서 신뢰하는 루트 인증기관과 인증 경로 등을 통해 검증키의 신뢰성을 확보해야 한다.

④ O — 인증기관은 인증서의 폐지 상태를 알리기 위해 **인증서 폐지목록(CRL)** 등을 관리한다. CRL에는 폐지된 인증서의 일련번호와 폐지 시각 등의 정보가 들어가며, 이용자는 이를 확인하여 유효기간 내에 폐지된 인증서를 걸러낸다.

NoteBase

문 10. 메시지 인증코드(Message Authentication Code)에 대한 설명으로 가장 적절하지 않은 것은?

① 메시지 인증 방식에는 메시지 암호화 방식, 해시함수를 이용하는 방식 등이 있다.

② 임의 길이의 메시지와 송·수신자가 공유하는 비밀키를 입력하여 가변비트 길이의 출력을 계산하는 함수이다.

③ IPSec과 SSL/TLS는 통신 내용의 인증과 무결성을 확인하기 위해 메시지 인증코드로 사용한다.

④ 송·수신자가 같은 키를 갖고 있으므로 제3자에 대한 증명을 할 수 없으며 부인방지(non-repudiation)를 할 수 없다.

정답 2번

간단한 해설

MAC은 메시지와 공유 비밀키를 입력받아 **정해진 길이의 인증값**을 만든다. 입력 메시지의 길이가 달라져도 같은 알고리즘과 출력 길이 설정에서는 인증값의 길이가 일정하다.

선지별 해설

① O: 메시지 인증에는 암호 알고리즘이나 해시함수를 이용하는 방식이 있다. MAC의 예로는 블록 암호 기반 CMAC과 해시함수에 비밀키를 결합한 HMAC이 있다. 다만 비밀키 없는 해시값을 메시지와 함께 보내는 것만으로는 공격자가 둘 다 바꿀 수 있어 송신자 인증을 보장하지 못한다.

② X: MAC은 메시지와 공유 비밀키로 **정해진 길이의 인증값**을 계산한다. 메시지 길이가 달라져도 같은 알고리즘과 출력 길이 설정을 사용하면 인증값의 길이는 일정하다. 따라서 '가변비트 길이의 출력'은 '고정된 비트 길이의 출력'으로 고쳐야 한다.

③ O: IPSec과 SSL/TLS에는 MAC을 이용하여 통신 데이터의 출처와 무결성을 확인하는 방식이 있다. 예를 들어 HMAC은 비밀키를 가진 상대가 생성한 인증값인지 검증한다. 실제 적용 방식은 프로토콜 버전과 선택한 암호 방식에 따라 달라진다.

④ O: 공유 비밀키를 가진 송신자와 수신자 모두 같은 메시지의 MAC을 생성할 수 있다. 따라서 MAC만으로는 제3자에게 어느 쪽이 생성했는지 입증할 수 없으므로 부인방지를 제공하지 않는다.

NoteBase

문 11. 임의적 접근제어(Discretionary Access Control)에 대한 설명으로 가장 적절하지 않은 것은?

① 중앙 집중화된 환경에서 제어되는 것이 아니며 강제적 접근제어(Mandatory Access Control)의 정적인 역할에 비해 사용자에게 동적으로 정보에 접근할 수 있도록 해준다.

② 접근 권한 관리가 매우 편리하여 DBMS 및 운영체제의 파일 시스템 등에 널리 사용된다.

③ 접근 권한 부여를 오직 식별자에게만 의존하므로 데이터의 의미(Semantics)에 대해 아무런 지식도 갖고 있지 않아 데이터에 의한 통제를 할 수 있는 방법이 전혀 없다.

④ 모든 접근 데이터에 대해 보안 레이블을 정의하고 보안정책을 확인해야 하므로 성능이 좋지 않고 개발 및 구현이 쉽지 않다.

정답 4번

간단한 해설

DAC의 핵심은 **객체 소유자의 재량에 따른 권한 부여**이다. 모든 데이터의 보안 레이블과 중앙의 강제 정책을 기준으로 통제하는 설명은 MAC에 가깝다.

NoteBase

선지별 해설

① O: DAC에서는 **객체 소유자가 접근권한을 부여·변경할 재량**을 가진다. 중앙의 강제 정책을 소유자가 임의로 바꾸지 못하는 MAC과 비교하면 정보 공유를 유연하게 조정할 수 있다는 뜻이다. 여기서 중앙 집중화 여부는 권한 결정의 주체에 관한 설명이지, DAC를 중앙 서버에서 구현할 수 없다는 뜻은 아니다.

② O: 파일 소유자가 다른 사용자에게 읽기·쓰기 권한을 주거나 데이터베이스 객체 소유자가 권한을 부여하는 식으로 **객체별 공유 권한을 직접 관리**할 수 있다. 이런 유연성 때문에 파일 시스템과 DBMS에서 널리 사용된다. 다만 사용자와 객체가 많아지면 개별 권한 관리가 복잡해질 수 있어, 모든 규모에서 관리가 쉽다는 뜻으로 일반화하지는 않는다.

③ O: 전통적인 식별자 기반 DAC는 사용자·그룹의 식별정보와 객체에 설정된 권한으로 접근을 판단하며, **데이터 내용의 의미를 자체적으로 해석하지 않는다**. 따라서 기본 DAC만으로 내용의 민감성이나 접근 후 정보 흐름을 자동 통제하기 어렵다는 한계를 설명한 것이다. 선지의 '전혀 없다'를 별도의 내용 기반 정책을 추가한 시스템까지 불가능하다는 뜻으로 확대해서는 안 된다.

④ X: **보안 레이블과 중앙의 강제 정책**을 기준으로 접근을 판단하는 것은 DAC보다 MAC의 특징에 해당한다. DAC의 핵심은 소유자의 재량에 따른 권한 부여이므로 모든 데이터에 보안등급 레이블을 붙이는 것을 필수로 하지 않는다. 레이블·정책 관리에는 추가 부담이 생길 수 있지만, 성능과 구현 난이도는 실제 설계에 따라 달라진다.

따라서 MAC의 레이블 기반 통제 특징을 DAC의 특성으로 제시한 ④가 가장 적절하지 않다.

NoteBase

문 12. 다음에서 설명하는 내용으로 가장 적절한 것은?

· 암호 알고리즘은 모든 내용이 공개되어도 키가 노출되지 않으면 안전해야 한다.
· 암호시스템의 안전성은 암호 알고리즘의 비밀을 지키는데 의존되어서는 안되며 키의 비밀을 지키는데 기반을 두어야 한다.

① 비둘기집(Pigeon Hole)의 원리
② 오일러(Euler)의 정리
③ 페르마(Fermat)의 정리
④ 케르히호프(Kerckhoff)의 원리

정답 4번

간단한 해설

암호 알고리즘이 공개되어도 키가 비밀이면 안전하도록 설계해야 한다는 것은 **케르히호프의 원리**이다. 안전성의 기반을 알고리즘의 비공개가 아니라 키의 비밀 유지에 둔다는 점이 결정적인 단서이다.

개념 구분

케르히호프의 원리: 공격자가 암호 알고리즘과 동작 방식을 알고 있더라도, 비밀키를 모르면 암호시스템의 안전성이 유지되도록 설계해야 한다는 원리이다. 지문의 두 설명은 모두 **알고리즘의 은폐가 아니라 키의 비밀에 안전성의 기반을 둔다**는 같은 뜻이다. 단순히 키만 숨기면 어떤 부실한 알고리즘도 안전해진다는 뜻은 아니다.

비둘기집의 원리: $n + 1$개 이상의 대상을 n개의 상자에 넣으면 **적어도 한 상자에는 두 개 이상**이 들어간다는 원리이다. 가능한 결과의 수보다 입력의 수가 많을 때 중복이 생김을 설명하는 데 쓰이며, 알고리즘 공개 여부에 관한 설계 원리와는 다르다.

오일러의 정리: 정수 a와 $n > 1$이 서로소이면 a^(n)≡1±od n이 성립한다. 여기서 $\varphi(n)$은 1부터 n까지의 정수 중 n과 서로소인 수의 개수이다. **서로소 조건에서의 거듭제곱 합동식**을 설명하는 정리이다.

페르마의 정리: 이 암호학 문맥에서는 페르마의 소정리를 뜻한다. p가 소수이고 a가 p의 배수가 아니면 a^p-1≡1±od p가 성립한다. **소수를 법으로 하는 거듭제곱의 성질**이며 키의 비밀 유지에 관한 원리와 구별된다.

따라서 지문의 설명에 해당하는 것은 ④ 케르히호프의 원리이다.

NoteBase

문 13. IPSec Protocol에 대한 설명으로 가장 적절하지 않은 것은?

① ESP(Encapsulating Security Payload)는 IP 데이터그램에서 제공하는 선택적 인증과 무결성, 기밀성, 재전송 공격 방지 기능이 있다.

② AH(Authentication Header)는 인증서비스, 재전송 공격 방지 서비스를 제공하며 기밀성을 보장한다.

③ Tunnel Mode는 IP 헤더를 포함한 전체에 대해서 보호 서비스를 제공하며 여러 호스트에 대해서 같은 터널을 사용할 수 있다.

④ Transport Mode는 종단 간 서비스를 제공하며 트래픽 분석에 취약할 수 있다.

정답 2번

간단한 해설

AH는 무결성과 출처 인증, 재전송 공격 방지 기능을 제공하지만 **암호화에 의한 기밀성은 제공하지 않는다**. 기밀성을 얻으려면 암호화를 사용하는 ESP가 필요하다.

선지별 해설

① O: ESP는 **암호화에 의한 기밀성**과 무결성·데이터 출처 인증을 제공할 수 있고, 순서번호를 검사하여 재전송 공격도 방지할 수 있다. 실제 적용되는 서비스 조합은 보안 연관(SA)의 설정에 따라 정해지므로, 모든 ESP 패킷이 언제나 모든 기능을 동시에 사용한다는 뜻은 아니다.

② X: AH는 무결성과 데이터 출처 인증을 제공하며, 순서번호와 재전송 방지 창을 이용해 중복 패킷을 탐지할 수 있다. 그러나 **내용을 암호화하지 않으므로 기밀성을 제공하지 않는다**. 기밀성이 필요하면 암호화를 사용하는 ESP를 적용해야 한다.

③ O: 터널 모드는 **원래 IP 헤더를 포함한 패킷 전체를 캡슐화**한 뒤 새 외부 IP 헤더를 붙인다. 보호 대상에는 내부 IP 헤더와 데이터가 포함되며, 보안 게이트웨이 사이의 터널로 여러 내부 호스트의 트래픽을 함께 운반할 수 있다. 암호화를 사용하는 ESP 터널에서는 내부 패킷이 암호화되지만 전달에 필요한 외부 IP 헤더는 남는다.

④ O: 전송 모드는 주로 두 종단 호스트 사이에서 원래 IP 헤더 뒤의 상위 계층 데이터를 보호한다. 특히 ESP 전송 모드에서도 **원래 송·수신 IP 주소가 외부에 드러나므로** 통신 상대나 전송 빈도 등을 이용한 트래픽 분석이 가능하다. 데이터를 암호화하는 것만으로 통신의 모든 특징이 숨겨지는 것은 아니다.

따라서 AH가 기밀성을 보장한다고 한 ②가 가장 적절하지 않다.

NoteBase

문 14. 사이버 공격 유형에 대한 <보기 1>의 설명과 <보기 2>의 용어를 가장 적절하게 연결한 것은?

<보기 1>
(가) 사용자에게 실제 사이트와 동일한 경험을 제공하면서 ID나 비밀번호 등 중요 정보를 중간에 탈취하는 공격
(나) 특정인(조직)을 표적으로 신뢰할만한 발신인이 보낸 것처럼 위장한 메일을 이용하여 악성 웹 사이트 유도, 악성 첨부파일로 악성코드를 감염시키는 방식
(다) 해당 사이트가 공식적으로 운영하고 있는 도메인 자체를 탈취하는 공격
(라) 스마트폰에 첨부된 URL을 실행하면 악성 앱이 설치되어 개인정보나 금융정보를 탈취하는 방식

<보기 2>
㉠ 액티브 피싱(Active Phishing) ㉡ 파밍(Pharming)
㉢ 스피어 피싱(Spear Phishing) ㉣ 스미싱(Smishing)

① (가): ㉠, (나): ㉢, (다): ㉡, (라): ㉣
② (가): ㉣, (나): ㉠, (다): ㉢, (라): ㉡
③ (가): ㉢, (나): ㉡, (다): ㉠, (라): ㉣
④ (가): ㉠, (나): ㉢, (다): ㉣, (라): ㉡

정답 1번

간단한 해설

중간 탈취·특정 표적·도메인 접속 조작·스마트폰 악성 URL을 각각 구별한다. 액티브 피싱은 실제 사이트와의 통신 중간에서 정보를 가로채고, 스피어 피싱은 공격 대상을 특정한다는 점이 핵심이다.

NoteBase

대응 관계 해설

(가) → ㉠ **액티브 피싱**: 사용자와 실제 사이트 사이에 공격자가 개입하여 정상 사이트를 사용하는 것처럼 보이게 하면서 로그인 정보를 가로챈다. 실제 사이트와의 상호작용을 유지한 채 정보를 중간에서 탈취한다는 점이 단서이다.

(나) → ㉢ **스피어 피싱**: 특정 개인이나 조직을 표적으로 삼는 피싱이다. 믿을 만한 발신인을 사칭한 맞춤형 메일로 악성 링크나 첨부파일을 실행하도록 유도한다.

(다) → ㉡ **파밍**: 정상 도메인으로 접속하려는 사용자를 가짜 사이트로 연결시키는 공격이다. 도메인의 연결 정보를 탈취·조작하거나 DNS·호스트 설정을 변조하는 방식 등이 해당한다. 핵심은 정상 주소로 향하는 접속을 가짜 사이트로 돌리는 데 있다.

(라) → ㉣ **스미싱**: 스마트폰 문자메시지 등의 악성 URL로 접속을 유도해 악성 앱을 설치시키거나 정보를 탈취하는 방식이다. 이 설명에서는 스마트폰의 URL 실행과 악성 앱 설치가 식별 단서이다.

따라서 (가)–㉠, (나)–㉢, (다)–㉡, (라)–㉣으로 연결한 ①이다.

NoteBase

문 15. 영지식 인증(Zero Knowledge Authentication)에 대한 설명으로 가장 적절하지 않은 것은?

① 증명하려는 자는 자신의 비밀정보를 노출하지 않으면서 자신이 비밀정보를 알고 있음을 증명할 수 있다.

② Fiat-Shamir 프로토콜, Feige-Fiat-Shamir 프로토콜 등이 있다.

③ 정당성(Soundness), 완전성(Completeness), 영지식성(Zero Knowledgeness)을 만족해야 한다.

④ 모든 프로토콜에 대해 반복 수행 없이 정당성을 높일 수 있다.

정답 4번

간단한 해설

영지식 인증에서는 **검증의 반복**으로 부정한 증명자의 성공 확률을 낮추는 방식이 사용된다. 모든 프로토콜에서 반복 없이 정당성을 높일 수 있다는 설명은 지나친 일반화이다.

선지별 해설

① O: 영지식 인증은 비밀정보 자체를 전달하지 않고도 증명자가 그 정보를 알고 있음을 검증자가 확인하게 한다. 검증자는 주장에 대한 확인 외에 비밀정보를 알아내는 데 도움이 되는 추가 지식을 얻지 않아야 한다.

② O: Fiat-Shamir와 Feige-Fiat-Shamir는 비밀을 직접 공개하지 않는 인증을 위한 대표적인 프로토콜이다. 검증자의 도전에 대해 비밀을 아는 증명자가 적절히 응답하는 과정을 이용한다.

③ O: 완전성은 정당한 비밀정보를 가진 증명자가 절차를 따를 때 검증에 성공하는 성질이다. 정당성은 비밀을 모르는 부정한 증명자가 검증자를 속여 통과하기 어렵다는 성질이며, 영지식성은 검증 과정에서 비밀에 관한 추가 정보가 드러나지 않는 성질이다.

④ X: 한 차례의 검증에서 부정한 증명자가 우연히 통과할 가능성이 남는 프로토콜은 **독립적인 검증을 반복**하여기만 성공 확률을 낮출 수 있다. 따라서 모든 프로토콜에서 반복 없이 정당성을 높일 수 있다는 단정은 옳지 않다. 정당성을 강화하는 방법은 해당 프로토콜의 구조와 매개변수에 따라 달라진다.

문 16. SSL(Secure Socket Layer)에 대한 설명으로 가장 적절하지 않은 것은?

① SSL 보안 서비스는 클라이언트와 서버 상호 인증, 메시지 무결성 등이 있다.

② Handshake 프로토콜은 [보안설정] → [클라이언트 인증과 키교환] → [서버 인증과 키교환] → [종료] 단계로 진행된다.

③ Alert 프로토콜은 통신 과정에서 발생하는 오류를 통보하기 위해 사용한다.

④ Record 프로토콜은 단편/결합, 암호화/복호화, 압축/압축풀기 등의 기능을 제공한다.

정답 2번

간단한 해설

SSL의 전체 핸드셰이크에서는 보안 설정 후 **서버 인증과 키 교환**을 먼저 수행하고, 이어서 클라이언트 인증과 키 교환을 진행한다. 선지는 이 두 단계의 순서를 바꾸었다.

선지별 해설

① O: SSL은 상대방 인증, 기밀성, 메시지 무결성을 제공하는 보안 프로토콜이다. 서버 인증뿐 아니라 클라이언트 인증도 지원하므로 **상호 인증이 가능**하다. 다만 클라이언트 인증은 선택적이어서 모든 연결에서 반드시 상호 인증을 수행하는 것은 아니다.

② X: **서버 인증과 키 교환이 먼저**이고, 클라이언트 인증과 키 교환이 그 뒤에 온다. 전체 핸드셰이크의 기본 흐름은 보안 설정 → 서버 인증과 키 교환 → 클라이언트 인증과 키 교환 → 종료이다. Hello 메시지로 보안 조건을 협상한 뒤 서버가 인증서와 필요한 키 교환 정보를 제공해야 클라이언트가 이를 확인하고 후속 키 교환을 진행할 수 있다. 여기서 종료는 통신 연결을 끊는 것이 아니라 Finished 메시지로 핸드셰이크 완료를 확인하는 단계이다.

③ O: Alert 프로토콜은 **오류의 내용과 심각도**를 상대방에게 알린다. 인증서 오류나 무결성 검사 실패 등을 통보하며, 치명적 오류이면 연결을 종료한다. 정상적인 연결 종료를 알리는 close_notify도 Alert 메시지에 해당한다.

④ O: Record 프로토콜은 상위 계층 데이터를 전송 가능한 레코드로 나누고 보호한다. 송신 측은 단편화, 합의된 압축 처리, **MAC을 이용한 무결성 보호와 암호화**를 수행하고, 수신 측은 복호화·무결성 확인·압축 해제 후 데이터를 상위 계층에 전달한다. 여러 상위 메시지를 한 레코드로 묶을 수도 있으며, 압축하지 않는 방식도 선택할 수 있다.

NoteBase

문 18. 블록체인(Block Chain)에 대한 설명으로 가장 적절하지 않은 것은?

① 앞 블록의 내용을 변경하면 뒤에 이어지는 블록은 변경할 필요가 없다.

② 키를 분실할 경우 자산 이전이 불가능해질 수 있으며 공격자가 키를 획득하여 악용한 경우에도 확인이 불가능하다.

③ 퍼블릭 블록체인은 모든 참여자가 권한을 보유하지만 프라이빗 블록체인은 구성원에 따라 사용 가능한 권한 지정이 가능하다.

④ 특정기관이나 제3자의 거래를 보증하지 않고 거래 당사자끼리 가치를 교환할 수 있다.

정답 1번

간단한 해설

블록체인은 **이전 블록의 해시값으로 연결**된다. 앞 블록을 바꾸면 후속 블록의 연결도 불일치하므로, 뒤 블록을 변경할 필요가 없다는 ①이 가장 적절하지 않다.

선지별 해설

① X: 각 블록은 이전 블록의 해시값을 포함하므로 앞 블록의 내용이 바뀌면 그 해시값도 달라져 뒤 블록에 저장된 참조와 불일치한다. 변경된 내용에 맞는 체인을 만들려면 **후속 블록의 해시 연결도 다시 계산**해야 하며, 네트워크의 합의 조건까지 충족해야 한다. 따라서 뒤 블록을 변경할 필요가 없다는 설명은 잘못이다.

② O: 개인키를 잃고 복구할 수 없으면 자산 이전에 필요한 서명을 만들지 못할 수 있다. 공격자가 그 키를 얻으면 유효한 서명을 만들 수 있으므로 **서명 검증만으로 실제 소유자와 공격자를 구별할 수 없다**. 선지의 “확인이 불가능하다”는 이 한계를 뜻하는 것으로 이해해야 하며, 거래 기록 조회나 추가 조사까지 불가능하다는 의미는 아니다.

③ O: 퍼블릭 블록체인은 일반적으로 누구나 거래 제출이나 검증 등에 참여할 수 있는 개방형 구조이고, 프라이빗 블록체인은 허가된 구성원에게 읽기·쓰기·검증 등의 권한을 다르게 부여할 수 있다. 여기서 “모든 참여자가 권한을 보유”한다는 표현은 **참여의 개방성**에 관한 것으로, 타인의 자산을 임의로 처분할 권한을 뜻하지 않는다.

④ O: “제3자의 거래를 보증하지 않고”라는 표현은 다소 부정확하지만, 중앙기관이나 중개자의 보증에 의존하지 않고 당사자끼리 거래할 수 있다는 취지이다. 거래의 유효성은 **전자서명 검증과 네트워크 합의**로 확인하므로 별도의 중앙 보증 주체가 반드시 필요한 것은 아니다.

따라서 가장 적절하지 않은 것은 ①이다.

NoteBase

문 19. OTP(One Time Password)에 대한 설명으로 가장 적절하지 않은 것은?

① 시간 동기화(Time-Synchronous) 방식은 해시 체인에 기반하고 있으며 해시함수의 일방향성(one-way)을 이용한다.

② 시도-응답(Challenge-Response) 방식은 서버에서 난수 발생 등을 통해 임의의 수를 생성하여 클라이언트에 보낸다.

③ 시간-이벤트 동기화(Time-Event Synchronous) 방식은 OTP 생성 입력값으로 시간값과 카운트값을 모두 사용한다.

④ 이벤트 동기화(Event-Synchronous) 방식은 서버와 클라이언트가 카운트(Count) 값을 동일하게 증가시켜 OTP를 생성한다.

정답 1번

간단한 해설

시간 동기화 OTP의 기준은 **시간값**이다. 일방향 해시를 반복 적용하는 해시 체인 방식의 특징을 시간 동기화 방식으로 설명한 ①이 가장 적절하지 않다.

선지별 해설

① (X) 시간 동기화 방식은 서버와 클라이언트가 공유한 비밀키와 **시간값**을 이용해 OTP를 생성한다. 대표적인 TOTP는 일정 시간 간격으로 계산한 시간 카운터를 사용한다. 해시를 반복 적용한 값을 역순으로 사용하는 해시 체인 방식과는 구별되므로, 이를 시간 동기화 방식의 특징으로 설명한 ①이 가장 적절하지 않다. TOTP도 해시 기반 연산을 이용하지만, 해시를 사용한다는 사실과 해시 체인에 기반한다는 것은 다르다.

② (O) 시도-응답 방식에서는 서버가 난수 등으로 만든 시도값을 클라이언트에 전달한다. 클라이언트는 이 값과 비밀정보를 이용해 응답값을 계산하고, 서버는 응답이 올바른지 검증한다. 따라서 서버가 임의의 수를 생성하여 보내는 과정은 시도-응답 방식에 해당한다.

③ (O) 시간-이벤트 동기화 방식은 **시간값과 카운트값**을 함께 OTP 생성 입력으로 사용한다. 시간에 따른 변화와 OTP 생성 등의 이벤트에 따른 변화를 모두 반영하는 방식이므로, 두 값을 모두 사용한다는 설명이 옳다.

④ (O) 이벤트 동기화 방식은 서버와 클라이언트가 공유하는 증가형 카운터를 기준으로 OTP를 생성·검증한다. 여기서 카운트값을 동일하게 증가시킨다는 것은 양쪽의 카운터 상태를 맞추어 사용한다는 뜻이다. 대표적인 HOTP에서는 토큰이 새 OTP를 생성할 때, 서버는 인증에 성공할 때 카운터를 증가시키므로 실제 증가 시점은 다를 수 있으며, 값이 어긋나면 재동기화가 필요하다.

NoteBase

문 20. 「개인정보 보호법」상 개인정보가 유출되었음을 알게 되었을 때에 개인정보처리자가 해당 정보주체에게 알려야 하는 사항으로 가장 적절하지 않은 것은?

① 유출된 개인정보의 항목 및 유출된 시점과 그 경위

② 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법

③ 개인정보처리자가 운영하는 시스템 정보

④ 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

정답 3번

①

개인정보가 유출되었음을 알게 되면 **유출된 개인정보의 항목**과 **유출 시점 및 경위**를 해당 정보주체에게 알려야 한다.

개인정보 보호법 제34조(개인정보 유출등의 통지 · 신고)
① 개인정보처리자는 개인정보가 유출등이 되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 다음 각 호의 사항을 알려야 한다. 다만, 정보주체의 연락처를 알 수 없는 경우 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다. <개정 2023.3.14, 2026.3.10>
1. 유출등이 된 개인정보의 항목
2. 유출등이 된 시점과 그 경위

②

유출 피해를 최소화하기 위해 **정보주체가 할 수 있는 방법에 관한 구체적인 정보**를 알려야 한다.

개인정보 보호법 제34조(개인정보 유출등의 통지 · 신고)
① 개인정보처리자는 개인정보가 유출등이 되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 다음 각 호의 사항을 알려야 한다. 다만, 정보주체의 연락처를 알 수 없는 경우 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다. <개정 2023.3.14, 2026.3.10>
3. 유출등으로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 구체적인 정보

NoteBase

③

개인정보처리자가 운영하는 **시스템 정보는 법정 유출 통지사항에 포함되지 않는다**. 통지사항에는 개인정보처리자의 대응조치 및 피해 구제절차 등이 포함된다.

개인정보 보호법 제34조(개인정보 유출등의 통지 · 신고)
① 개인정보처리자는 개인정보가 유출등이 되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 다음 각 호의 사항을 알려야 한다. 다만, 정보주체의 연락처를 알 수 없는 경우 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다. <개정 2023.3.14, 2026.3.10>
1. 유출등이 된 개인정보의 항목
2. 유출등이 된 시점과 그 경위
3. 유출등으로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 구체적인 정보
4. 개인정보처리자의 대응조치 및 피해 구제절차
5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처
6. 개인정보 유출등으로 인한 제39조에 따른 손해배상과 제39조의2에 따른 법정손해배상의 청구 및 제43조에 따른 분쟁조정 등 피해를 입은 정보주체의 법적 권리와 그 행사 방법 등에 관한 정보
7. 그 밖에 개인정보가 유출등이 된 정보주체의 보호를 위하여 대통령령으로 정하는 사항

④

피해를 입은 정보주체가 신고 등을 할 수 있도록 **신고 접수 담당부서와 연락처**를 알려야 한다.

개인정보 보호법 제34조(개인정보 유출등의 통지 · 신고)
① 개인정보처리자는 개인정보가 유출등이 되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 다음 각 호의 사항을 알려야 한다. 다만, 정보주체의 연락처를 알 수 없는 경우 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다. <개정 2023.3.14, 2026.3.10>
5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

NoteBase