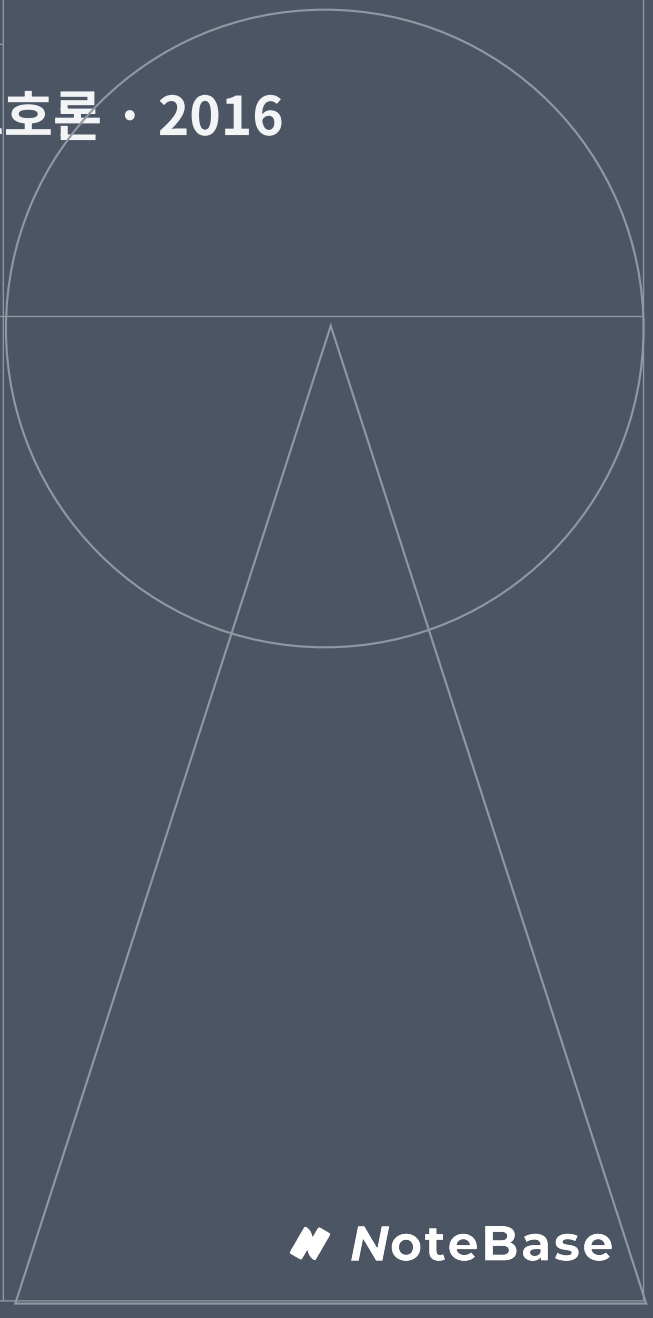
기출OX 해설집

공무원/지방직/9급 · 정보보호론 · 2016



NoteBase

기출OX 해설집

공무원/지방직/9급 · 정보보호론 · 2016

공무원/지방직/9급 · 정보보호론 · 2016

문 1. 보안 공격 유형 중 소극적 공격으로 옳은 것은?

① 트래픽 분석(traffic analysis)

② 재전송(replaying)

③ 변조(modification)

④ 신분 위장(masquerading)

정답 1번

간단한 해설

트래픽 분석은 통신 내용이나 흐름을 변경하지 않고 **통신량·발생 시각·빈도 등의 특성을 관찰**하여 정보를 추론하므로 소극적 공격에 해당한다.

공통 해설

소극적 공격은 통신을 엿듣거나 관찰하여 정보를 얻는 공격으로, **메시지를 삽입·변경하거나 통신 동작에 개입하지 않는다**. 공격의 피해가 작은지를 기준으로 구분하는 것이 아니라, 공격자가 정보를 관찰하는 데 그치는지가 기준이다.

트래픽 분석은 메시지의 길이, 통신량, 발생 시각과 빈도 등을 관찰하여 통신의 특성을 추론한다. 예를 들어 특정 시각에 통신량이 집중된다는 사실을 알아내는 것은 메시지를 변경하거나 새로 보내는 행위가 아니므로 소극적 공격이다.

재전송은 이전에 수집한 메시지를 다시 보내 통신에 개입하고, 변조는 메시지의 내용을 바꾸며, 신분 위장은 다른 사용자인 것처럼 행세하여 통신이나 시스템에 개입한다. 세 유형은 모두 적극적 공격이다. 특히 재전송은 **원래 메시지의 내용을 바꾸지 않더라도 다시 전송한다**는 점에서 단순 관찰과 구별된다.

NoteBase

문 2. 암호학적 해시 함수가 가져야 할 특성으로 옳지 않은 것은?

① 서로 다른 두 입력 메시지에 대해 같은 해시값이 나올 가능성은 있으나, 계산적으로 같은 해시값을 갖는 서로 다른 두 입력 메시지를 찾는 것은 불가능해야 한다.

② 해시값을 이용하여 원래의 입력 메시지를 찾는 것은 계산상으로 불가능해야 한다.

③ 입력 메시지의 길이에 따라 출력되는 해시값의 길이는 비례해야 한다.

④ 입력 메시지와 그 해시값이 주어졌을 때, 이와 동일한 해시값을 갖는 다른 메시지를 찾는 것은 계산상으로 불가능해야 한다.

정답 3번

간단한 해설

③의 '입력 메시지의 길이에 비례'한다는 설명이 잘못되었다. 암호학적 해시 함수는 입력 메시지의 길이가 달라도 **정해진 길이의 해시값**을 출력한다.

선지별 해설

① O: **충돌 저항성**에 관한 설명이다. 가능한 입력 메시지의 수가 해시값의 수보다 많으므로, 서로 다른 메시지에서 같은 해시값이 나오는 충돌은 존재한다. 다만 공격자가 그러한 두 메시지를 실제로 찾아내는 것은 계산적으로 어려워야 한다. 여기서 '불가능'은 수학적으로 존재하지 않는다는 뜻이 아니라 현실적인 시간과 자원으로 찾기 어렵다는 뜻이다.

② O: **역상 저항성**에 관한 설명이다. 해시값이 주어졌을 때 그 값을 출력하는 입력 메시지를 찾는 것이 계산적으로 어려워야 한다. 따라서 해시값에서 원래 메시지를 거꾸로 구하는 것도 어려워야 한다.

③ X: 해시값의 길이는 입력 메시지의 길이에 비례하지 않고 **사용하는 해시 함수에 따라 고정**된다. 예를 들어 SHA-256은 허용된 입력 길이 범위에서 짧은 메시지든 긴 메시지든 256비트 해시값을 출력한다. 입력이 길어지면 처리해야 할 데이터의 양은 늘어나지만 출력 해시값의 길이가 늘어나는 것은 아니다.

④ O: **제2역상 저항성**에 관한 설명이다. 특정 입력 메시지와 그 해시값이 주어진 상태에서, 같은 해시값을 만드는 다른 메시지를 찾는 것이 계산적으로 어려워야 한다. 충돌 저항성이 두 메시지를 모두 자유롭게 골라 같은 해시값을 찾는 공격을 막는 성질이라면, 제2역상 저항성은 이미 정해진 메시지와 충돌하는 다른 메시지를 찾는 공격을 막는 성질이다.

NoteBase

문 3. 다음 내용에 해당하는 공개키 기반 구조(PKI)의 구성요소로 옳은 것은?

◯ 사용자에 대한 공개키 인증서를 생성하고 이를 발급한다.
◯ 필요 시 사용자 인증서에 대한 갱신 및 폐기 기능을 수행한다.
◯ 인증서 폐기 목록(certificate revocation list)을 작성한다.

① 사용자
② 등록 기관
③ 인증 기관
④ 디렉토리

정답 3번

간단한 해설

인증 기관(CA)은 공개키 인증서를 생성·발급하고, 인증서의 갱신·폐기와 **인증서 폐기 목록(CRL) 작성**을 담당한다. 제시된 세 기능은 모두 인증 기관의 인증서 관리 역할에 해당한다.

공통 해설

인증 기관(CA)은 **사용자의 신원과 공개키의 연결을 보증하는 인증서**를 생성·발급하는 신뢰 주체이다. 인증서에 인증 기관의 전자서명을 붙이므로, 인증서를 이용하는 측은 그 서명을 검증하여 발급 주체와 인증서 내용의 위·변조 여부를 확인할 수 있다.

인증 기관은 발급 이후에도 필요에 따라 인증서를 갱신하거나 폐기한다. 예를 들어 사용자의 개인키가 유출되면 유효기간이 남아 있어도 해당 인증서를 폐기할 수 있다. 이처럼 **유효기간 만료 전에 폐기된 인증서**를 알리기 위해 작성하는 목록이 인증서 폐기 목록(CRL)이다. 따라서 제시된 생성·발급, 갱신·폐기, CRL 작성은 인증 기관의 역할이라는 하나의 기준으로 설명된다.

NoteBase

문 4. ㉠과 ㉡에 들어갈 용어로 옳은 것은?

(㉠) 은(는) 디지털 콘텐츠를 구매할 때 구매자의 정보를 삽입하여 불법 배포 발견 시 최초의 배포자를 추적할 수 있게 하는 기술이다.
(㉡) 은(는) 원본의 내용을 왜곡하지 않는 범위 내에서 사용자가 인식하지 못하도록 저작권 정보를 디지털 콘텐츠에 삽입하는 기술이다.

① ㉠: 크래커(Cracker), ㉡: 커버로스(Kerberos)
② ㉠: 크래커(Cracker), ㉡: 워터마킹(Watermarking)
③ ㉠: 핑거프린팅(Fingerprinting), ㉡: 커버로스(Kerberos)
④ ㉠: 핑거프린팅(Fingerprinting), ㉡: 워터마킹(Watermarking)

정답 4번

간단한 해설

핑거프린팅은 구매자별 정보를 삽입하여 불법 유출 경로를 추적하는 기술이고, **워터마킹**은 콘텐츠에 저작권 정보를 삽입하는 기술이다. 두 빈칸은 삽입하는 정보가 구매자 정보인지 저작권 정보인지로 구별한다.

빈칸별 해설

㉠ 핑거프린팅(Fingerprinting): 콘텐츠를 판매할 때 **구매자마다 구별되는 정보**를 삽입하여, 불법 배포된 사본이 누구에게 제공된 것인지 추적하는 기술이다. 예를 들어 같은 영상이라도 A와 B에게 서로 다른 식별 정보를 넣어 제공하면, 유출된 영상의 식별 정보를 확인하여 어느 구매자의 사본에서 유출되었는지 추적할 수 있다. 크래커는 시스템에 불법 침입하거나 피해를 주는 사람을 가리키므로 이 기술의 명칭이 아니다.

㉡ 워터마킹(Watermarking): 디지털 콘텐츠에 저작권자 등의 정보를 삽입하는 기술이다. 지문처럼 사용자가 알아차리지 못하도록 삽입하는 방식은 **콘텐츠의 이용을 방해하지 않으면서 저작권 정보를 담는** 비가시적 워터마킹에 해당한다. 커버로스는 티켓을 이용하는 네트워크 인증 방식이므로 콘텐츠에 저작권 정보를 삽입하는 기술과 구별된다.

㉠은 핑거프린팅, ㉡은 워터마킹이므로 두 용어의 조합은 ④와 일치한다.

NoteBase

문 5. 다음 내용에 해당하는 암호블록 운용 모드를 바르게 나열한 것은?

ㄱ. 코드북(codebook)이라 하며, 가장 간단하게 평문을 동일한 크기의 평문블록으로 나누고 키로 암호화하여 암호블록을 생성한다.
ㄴ. 현재의 평문블록과 바로 직전의 암호블록을 XOR한 후 그 결과를 키로 암호화하여 암호블록을 생성한다.
ㄷ. 각 평문블록별로 증가하는 서로 다른 카운터 값을 키로 암호화하고 평문블록과 XOR하여 암호블록을 생성한다.

① ㄱ: CBC, ㄴ: ECB, ㄷ: OFB
② ㄱ: CBC, ㄴ: ECB, ㄷ: CTR
③ ㄱ: ECB, ㄴ: CBC, ㄷ: OFB
④ ㄱ: ECB, ㄴ: CBC, ㄷ: CTR

정답 4번

간단한 해설

ㄴ처럼 **직전 암호블록을 현재 평문블록과 XOR한 뒤 암호화**하는 방식은 CBC이다. ㄷ처럼 **서로 다른 카운터 값을 암호화**한 결과를 평문블록과 XOR하는 방식은 CTR이며, 이전 암호화 출력을 다시 입력하는 OFB와 구별된다.

대응 관계 해설

ㄱ. ECB: 전자 코드북(Electronic Codebook) 모드이다. 평문을 일정한 크기의 블록으로 나누고 **각 블록을 독립적으로 암호화**한다. 같은 키로 동일한 평문블록을 암호화하면 동일한 암호블록이 나오므로, 평문의 반복 무늬가 암호문에도 드러날 수 있다.

ㄴ. CBC: 암호블록 연쇄(Cipher Block Chaining) 모드이다. 현재 평문블록을 **직전 암호블록과 XOR한 후 암호화**하므로, 앞 블록의 암호화 결과가 다음 블록의 암호화에 연결된다. 첫 블록에는 직전 암호블록이 없으므로 초기화 벡터(IV)를 사용한다. 평문블록을 바로 암호화하는 ECB와 이 점에서 다르다.

ㄷ. CTR: 카운터(Counter) 모드이다. 블록마다 증가하는 서로 다른 카운터 값을 암호화하여 키스트림을 만들고, 이를 평문블록과 XOR하여 암호블록을 생성한다. **암호화 함수의 입력이 카운터 값**이라는 점이 핵심이다. OFB는 초기화 벡터에서 시작하여 이전 암호화 출력을 다시 암호화함으로써 키스트림을 생성하므로, ㄷ의 설명과 다르다.

ㄱ은 ECB, ㄴ은 CBC, ㄷ은 CTR로, ④의 대응과 일치한다.

NoteBase

문 6. 네트워크 공격에 대한 설명으로 옳지 않은 것은?

① Spoofing: 네트워크에서 송·수신되는 트래픽을 도청하는 공격이다.

② Session hijacking: 현재 연결 중인 세션을 가로채는 공격이다.

③ Teardrop: 네트워크 프로토콜 스택의 취약점을 이용한 공격 방법으로 시스템에서 패킷을 재조립할 때, 비정상 패킷이 정상 패킷의 재조립을 방해함으로써 네트워크를 마비시키는 공격이다.

④ Denial of Service: 시스템 및 네트워크의 취약점을 이용하여 사용 가능한 자원을 소비함으로써, 실제 해당 서비스를 사용하려고 요청하는 사용자들이 자원을 사용할 수 없도록 하는 공격이다.

정답 1번

간단한 해설

송·수신되는 트래픽을 도청하는 공격은 **스니핑(Sniffing)**이다. 스푸핑(Spoofing)은 주소나 신원 정보를 위조하여 **신뢰할 수 있는 대상으로 가장**하는 공격이다.

선지별 해설

① X: 트래픽을 가로채어 내용을 엿보는 것은 **스니핑(Sniffing)**이다. 스푸핑(Spoofing)은 주소나 신원 정보를 위조하여 다른 대상으로 가장하는 공격이다. 예를 들어 패킷의 출발지 IP 주소를 다른 호스트의 주소처럼 꾸미는 것은 IP 스푸핑이다.

② O: 세션 하이재킹(Session hijacking)은 **이미 연결된 정상 세션을 탈취**하여 통신 당사자처럼 행동하는 공격이다. 웹에서는 유효한 세션 식별자를 탈취하여 해당 사용자의 세션으로 서비스에 접근하는 방식이 이에 해당한다.

③ O: 티어드롭(Teardrop)은 **IP 단편의 재조립 처리 취약점**을 이용하는 서비스 거부 공격이다. 단편들의 데이터 영역이 겹치도록 비정상적인 단편 오프셋을 설정해 보내면, 이를 제대로 처리하지 못하는 시스템에서 재조립 오류나 시스템 중단이 발생할 수 있다. 핵심은 단순히 패킷을 많이 보내는 것이 아니라 비정상 단편을 처리하는 과정에 오류를 일으키는 데 있다.

④ O: 서비스 거부 공격(Denial of Service)은 정상 사용자가 시스템이나 네트워크 자원을 이용하지 못하게 하여 **가용성을 침해**한다. 대역폭·CPU·메모리 등의 자원을 소모시키거나 취약점을 악용해 서비스를 중단시키며, 선지는 이 중 자원 소모를 통한 방식을 설명한다.

NoteBase

문 7. 스택 버퍼 오버플로우 공격의 수행 절차를 순서대로 바르게 나열한 것은?

ㄱ. 특정 함수의 호출이 완료되면 조작된 반환 주소인 공격 쉘 코드의 주소가 반환된다.
ㄴ. 루트 권한으로 실행되는 프로그램 상에서 특정 함수의 스택 버퍼를 오버플로우시켜서 공격 쉘 코드가 저장되어 있는 버퍼의 주소로 반환 주소를 변경한다.
ㄷ. 공격 쉘 코드를 버퍼에 저장한다.
ㄹ. 공격 쉘 코드가 실행되어 루트 권한을 획득하게 된다.

① ㄱ → ㄴ → ㄷ → ㄹ
② ㄱ → ㄷ → ㄴ → ㄹ
③ ㄷ → ㄴ → ㄱ → ㄹ
④ ㄷ → ㄱ → ㄴ → ㄹ

정답 3번

간단한 해설

공격 쉘 코드를 버퍼에 저장한 뒤 **반환 주소를 그 코드의 주소로 변경**해야 한다. 함수가 종료되어 조작된 반환 주소로 실행 흐름이 이동하면, 쉘 코드가 루트 권한으로 실행된다.

올바른 순서

ㄷ → ㄴ → ㄱ → ㄹ

ㄷ. 공격 쉘 코드를 버퍼에 저장한다. 이후 실행 흐름을 이 코드로 돌릴 수 있도록 **실행할 코드를 먼저 준비**하는 단계이다.

ㄴ. 루트 권한으로 실행되는 프로그램의 스택 버퍼를 넘치게 하여 저장된 반환 주소를 덮어쓴다. 반환 주소는 함수가 끝난 뒤 실행을 재개할 위치이므로, 이를 **쉘 코드가 저장된 버퍼의 주소**로 바꾸어 둔다. 주소를 바꾸는 것만으로 쉘 코드가 즉시 실행되는 것은 아니다.

ㄱ. 해당 함수가 실행을 마치고 복귀할 때 조작된 반환 주소를 사용한다. 이에 따라 원래 호출 지점으로 돌아가는 대신 **공격 쉘 코드가 있는 위치로 실행 흐름이 이동**한다. 따라서 이 단계보다 반환 주소 변경이 먼저 이루어져야 한다.

ㄹ. 실행 흐름이 도달한 공격 쉘 코드가 실행되어 루트 권한을 획득한다. 문제에서는 대상 프로그램이 이미 루트 권한으로 실행되고 있으므로, 공격 코드는 **그 프로그램의 루트 권한**으로 동작하게 된다.

NoteBase

문 8. 접근통제(access control) 모델에 대한 설명으로 옳지 않은 것은?

① 임의적 접근통제는 정보 소유자가 정보의 보안 레벨을 결정하고 이에 대한 정보의 접근제어를 설정하는 모델이다.

② 강제적 접근통제는 중앙에서 정보를 수집하고 분류하여, 각각의 보안 레벨을 붙이고 이에 대해 정책적으로 접근제어를 설정하는 모델이다.

③ 역할 기반 접근통제는 사용자가 아닌 역할이나 임무에 권한을 부여하기 때문에 사용자가 자주 변경되는 환경에서 유용한 모델이다.

④ Bell-LaPadula 접근통제는 비밀노출 방지보다는 데이터의 무결성 유지에 중점을 두고 있는 모델이다.

정답 4번

간단한 해설

④는 Bell-LaPadula 모델의 보호 목표를 잘못 설명했다. 이 모델은 데이터의 무결성보다 **기밀성, 즉 허가받지 않은 정보 공개의 방지**에 중점을 둔다.

선지별 해설

① O: 임의적 접근통제(DAC)는 정보 소유자가 자신의 정보에 누가 어떤 방식으로 접근할 수 있는지를 정하는 모델이다. 소유자가 다른 사용자에게 읽기나 쓰기 권한을 부여하는 것처럼, 접근 허용 범위를 **소유자의 재량**으로 설정한다는 점이 핵심이다.

② O: 강제적 접근통제(MAC)는 중앙의 보안정책에 따라 정보에 보안등급을 부여하고, 사용자의 인가 수준과 정보의 보안등급 등을 기준으로 접근을 통제한다. 정보 소유자가 임의로 허용하더라도 **중앙의 보안정책을 위반하는 접근은 허용되지 않는다**.

③ O: 역할 기반 접근통제(RBAC)는 **역할에 권한을 부여하고 사용자에게 역할을 할당**한다. 예를 들어 회계 담당자 역할에 회계자료 조회 권한을 설정해 두면, 담당자가 바뀔 때 기존 사용자의 역할 할당을 해제하고 새 사용자에게 그 역할을 할당하면 된다. 따라서 사용자 변동이 잦은 환경에서도 권한을 일관되게 관리하기 쉽다.

④ X: Bell-LaPadula 모델은 **기밀성 보호**를 목적으로 정보가 허가되지 않은 사용자에게 노출되는 것을 막는 접근통제 모델이다. 선지의 '데이터의 무결성 유지에 중점'은 '비밀노출 방지에 중점'으로 고쳐야 한다. 무결성은 정보가 부적절하게 변경되거나 훼손되지 않도록 하는 성질이며, 이를 보호하는 대표적인 접근통제 모델은 Biba 모델이다.

NoteBase

문 9. 개인정보 보호법령상 개인정보 영향평가에 대한 설명으로 옳지 않은 것은?

① 공공기관의 장은 대통령령으로 정하는 기준에 해당하는 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 위험요인분석과 개선 사항 도출을 위한 평가를 하고, 그 결과를 행정자치부장관에게 제출하여야 한다.

② 개인정보 영향평가의 대상에 해당하는 개인정보파일은 공공기관이 구축·운용 또는 변경하려는 개인정보파일로서 50만명 이상의 정보주체에 관한 개인정보파일을 말한다.

③ 영향평가를 하는 경우에는 처리하는 개인정보의 수, 개인정보의 제3자 제공 여부, 정보주체의 권리를 해할 가능성 및 그 위험정도, 그 밖에 대통령령으로 정한 사항을 고려하여야 한다.

④ 행정자치부장관은 제출받은 영향평가 결과에 대하여 보호위원회의 심의·의결을 거쳐 의견을 제시할 수 있다.

정답 2번

간단한 해설

②의 '50만 명 이상'은 **다른 개인정보파일과 연계한 결과**에 적용되는 기준이다. 별도의 연계 조건 없이 구축·운용 또는 변경하려는 개인정보파일의 인원 기준은 **100만 명 이상**이다.

NoteBase

선지별 해설

문항에 제시된 행정자치부장관 명칭을 사용하던 당시 법령을 기준으로 판단한다.

① O: 당시 개인정보 보호법 제33조제1항은 공공기관의 장이 대통령령상 기준에 해당하는 개인정보파일의 운용으로 개인정보 침해가 우려되면 영향평가를 실시하도록 규정하였다. 영향평가는 **위험요인을 분석하고 개선사항을 도출**하는 평가이며, 그 결과는 행정자치부장관에게 제출하여야 했다.

② X: 개인정보 보호법 시행령 제35조제3호의 기준은 구축·운용 또는 변경하려는 개인정보파일로서 **100만 명 이상**의 정보주체에 관한 개인정보파일이다. 제2호의 '50만 명 이상'은 이미 구축·운용 중인 파일을 해당 공공기관 내부 또는 외부의 다른 개인정보파일과 연계하려는 경우, **연계 결과 포함되는 정보주체 수**에 관한 기준이다. 이 조의 대상은 개인정보를 전자적으로 처리할 수 있는 개인정보파일이므로, 단순히 50만 명 이상이라는 이유만으로 모두 영향평가 대상이 되는 것은 아니다.

③ O: 당시 개인정보 보호법 제33조제2항은 처리하는 개인정보의 수, 제3자 제공 여부, 정보주체의 권리를 해할 가능성과 그 위험 정도, 그 밖에 대통령령으로 정한 사항을 고려하도록 규정하였다. 따라서 **개인정보의 규모와 권리 침해 위험**을 함께 살펴야 하며, 인원수만으로 평가를 마치는 것은 아니다.

④ O: 당시 개인정보 보호법 제33조제3항에 따라 행정자치부장관은 제출받은 영향평가 결과에 대하여 **보호위원회의 심의·의결을 거쳐** 의견을 제시할 수 있었다. 의견 제시는 의무가 아니라 가능한 조치였으며, 그 절차로 보호위원회의 심의·의결이 요구되었다.

NoteBase

문 10. 정보보호 시스템에서 사용된 보안 알고리즘 구현 과정에서 곱셈에 대한 역원이 사용된다. 잉여류 Z_{26}에서 법(modular) 26에 대한 7의 곱셈의 역원으로 옳은 것은?

① 11

② 13

③ 15

④ 17

정답 3번

간단한 해설

곱셈의 역원은 원래 수와 곱한 값을 26으로 나누었을 때 **나머지가 1**이 되는 수이다. 7 × 15 = 105 = 26 × 4 + 1이므로 7의 곱셈 역원은 15이다.

계산 과정

법 26에서 7의 곱셈 역원을 x라 하면 7x≡1±od26을 만족해야 한다. 즉, **7x와 1의 차이가 26의 배수**여야 한다. 7과 26은 서로소이므로 곱셈 역원이 존재한다.

유클리드 호제법으로 26 = 3 × 7 + 5, 7 = 1 × 5 + 2, 5 = 2 × 2 + 1을 얻는다. 마지막 식부터 거꾸로 대입하면 $1 = 3 \cdot 5 - 2 \cdot 7$이고, 여기에 $5 = 26 - 3 \cdot 7$을 대입하면 $1 = 3 \cdot 26 - 11 \cdot 7$이다. 따라서 $7 \cdot (-11) \equiv 1 \pm od26$이므로 −11이 7의 곱셈 역원이다.

법 26에서는 26의 배수만큼 차이 나는 수를 같은 잉여류로 본다. 따라서 −11에 26을 더한 **15도 같은 역원**을 나타낸다. 검산하면 7 × 15 = 105 = 26 × 4 + 1이므로 나머지가 1이다. 이는 ③의 15에 해당한다.

NoteBase

문 11. 응용 계층 프로토콜에서 동작하는 서비스에 대한 설명으로 옳지 않은 것은?

① FTP: 파일전송 서비스를 제공한다.

② DNS: 도메인 이름과 IP 주소 간 변환 서비스를 제공한다.

③ POP3: 메일 서버로 전송된 메일을 확인하는 서비스를 제공한다.

④ SNMP: 메일전송 서비스를 제공한다.

정답 4번

간단한 해설

SNMP는 메일 전송이 아니라 **네트워크 장비의 상태 감시와 관리**에 사용하는 프로토콜이다. 메일 전송에는 **SMTP**를 사용한다.

선지별 해설

① O: FTP는 클라이언트와 서버 사이에서 **파일을 업로드하거나 다운로드**하는 데 사용하는 응용 계층 프로토콜이다. 따라서 파일전송 서비스를 제공한다는 설명이 맞는다.

② O: DNS는 **도메인 이름에 대응하는 IP 주소를 조회**하는 서비스를 제공한다. 역방향 조회를 통해 IP 주소에 대응하는 도메인 이름도 확인할 수 있으므로, 이름과 주소 간 변환이라는 설명에 해당한다.

③ O: POP3는 **메일 서버에 도착한 메일을 가져오는** 프로토콜이다. 메일 프로그램이 서버의 우편함에 접근하여 메일을 내려받아 확인할 수 있게 한다.

④ X: SNMP는 라우터나 스위치 등 네트워크 장비의 상태와 관리 정보를 조회하고 설정을 관리하는 프로토콜이다. 따라서 메일전송 서비스라는 설명은 **네트워크 관리 서비스**로 고쳐야 한다. 메일을 보내거나 메일 서버 사이에서 전달하는 데 사용하는 프로토콜은 SMTP이다.

NoteBase

문 12. 「개인정보 보호법」상 용어 정의로 옳지 않은 것은?

① 개인정보: 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)

② 정보주체: 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인

③ 처리: 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기, 그 밖에 이와 유사한 행위

④ 개인정보파일: 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물

정답 2번

간단한 해설

②는 **개인정보처리자**의 정의를 정보주체의 정의로 제시했다. **정보주체**는 처리되는 정보로 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람이다.

선지별 해설

① O: 개인정보는 살아 있는 개인에 관한 정보로서 그 개인을 알아볼 수 있는 정보이다. 성명이나 영상 등으로 직접 알아볼 수 있는 경우뿐 아니라, **다른 정보와 쉽게 결합하여 알아볼 수 있는 경우**도 포함한다(개인정보 보호법 제2조제1호).

② X: 업무 목적으로 개인정보파일을 운용하기 위해 스스로 또는 다른 사람을 통해 개인정보를 처리하는 공공기관·법인·단체·개인 등은 **개인정보처리자**이다(제2조제5호). 정보주체는 처리되는 정보로 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람이다(제2조제3호). 예를 들어 회사가 고객명부를 업무용으로 관리하면 회사는 개인정보처리자이고, 명부에 기재된 정보로 식별되는 고객은 정보주체이다.

③ O: 처리는 개인정보를 수집하고 이용하는 행위에 한정되지 않는다.
생성·연계·연동·기록·저장·보유·가공·편집·검색·출력·정정·복구·제공·공개·파기 등 **개인정보를 다루는 다양한 행위**를 포괄한다. 따라서 정보를 보관하거나 삭제하는 것도 처리에 해당한다(제2조제2호).

④ O: 개인정보파일은 개인정보를 쉽게 검색할 수 있도록 **일정한 규칙에 따라 체계적으로 배열하거나 구성한 집합물**이다. 예를 들어 고객별 정보를 고객번호에 따라 정리하여 검색할 수 있게 구성한 고객명부가 이에 해당한다. 핵심은 단순히 개인정보가 모여 있다는 점이 아니라 검색할 수 있도록 체계적으로 구성되어 있다는 점이다(제2조제4호).

NoteBase

문 13. 다음 설명에 해당하는 OECD 개인정보보호 8원칙으로 옳은 것은?

개인정보는 이용 목적상 필요한 범위 내에서 개인정보의 정확성, 완전성, 최신성이 확보되어야 한다.

① 이용 제한의 원칙(Use Limitation Principle)
② 정보 정확성의 원칙(Data Quality Principle)
③ 안전성 확보의 원칙(Security Safeguards Principle)
④ 목적 명시의 원칙(Purpose Specification Principle)

정답 2번

간단한 해설

개인정보의 **정확성·완전성·최신성**을 이용 목적에 필요한 범위에서 확보하도록 하는 것은 '정보 정확성의 원칙'이다. 이용할 정보의 품질을 유지하라는 의미이다.

공통 해설

정보 정확성의 원칙(Data Quality Principle)은 개인정보가 이용 목적에 적합해야 하며, 그 목적에 필요한 범위에서 **정확하고 완전하며 최신의 상태**로 유지되어야 한다는 원칙이다. 정확성은 정보가 사실과 맞아야 한다는 뜻이고, 완전성은 목적 달성에 필요한 내용이 빠지지 않아야 한다는 뜻이며, 최신성은 변경된 사실이 반영되어야 한다는 뜻이다.

지문은 개인정보를 이용할 때 확보해야 할 세 가지 품질을 함께 제시하므로 정보 정확성의 원칙에 해당한다.
여기서 '이용 목적상 필요한 범위'는 품질 확보의 기준을 한정한다. 완전성을 이유로 목적과 무관한 개인정보까지 모두 갖추어야 한다는 뜻은 아니다.

NoteBase

문 14. 현행 우리나라의 정보보호관리체계(ISMS) 인증에 대한 설명으로 옳지 않은 것은?

① 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 근거를 두고 있다.

② 인증심사의 종류에는 최초심사, 사후심사, 갱신심사가 있다.

③ 인증에 유효기간은 정해져 있지 않다.

④ 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계를 수립·운영하고 있는 자에 대하여 인증 기준에 적합한지에 관하여 인증을 부여하는 제도이다.

정답 3번

간단한 해설

ISMS 인증의 유효기간은 **3년**으로 정해져 있다. 유효기간 중에는 사후심사로 관리체계의 유지 여부를 확인하고, 기간을 연장하려면 갱신심사를 받아야 한다.

선지별 해설

① O: ISMS 인증은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 **제47조**에 근거한 제도이다. 같은 조 제1항은 정보보호 관리체계를 수립·운영하는 자에 대하여 인증기준에 적합한지를 확인하여 인증할 수 있도록 규정한다.

② O: 인증심사는 **최초심사·사후심사·갱신심사**로 구분한다. 최초심사는 인증을 처음 취득하거나 인증범위의 중요한 변경으로 다시 신청할 때 실시한다. 사후심사는 인증 취득 후 관리체계가 지속적으로 유지되는지 확인하기 위해 유효기간 중 매년 1회 이상 실시하고, 갱신심사는 유효기간 만료 시 인증기간을 연장하기 위해 실시한다.

③ X: '유효기간은 정해져 있지 않다'는 설명을 **'유효기간은 3년이다'**로 고쳐야 한다. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조 제5항은 ISMS 인증의 유효기간을 3년으로 정한다. 따라서 한 번 인증을 취득했다고 무기한 유지되는 것은 아니며, 계속 인증을 유지하려면 만료 시 갱신심사를 받아야 한다.

④ O: ISMS는 정보통신망의 안정성과 신뢰성을 확보하기 위해 **관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계**의 적합성을 인증하는 제도이다. 같은 법 제47조 제1항의 내용에 해당하며, 특정 보안장비의 성능만이 아니라 조직이 수립·운영하는 정보보호 관리체계를 심사한다.

NoteBase

문 15. 보안 서비스에 대한 설명을 바르게 나열한 것은?

ㄱ. 메시지가 중간에서 복제·추가·수정되거나 순서가 바뀌거나 재전송됨이 없이 그대로 전송되는 것을 보장한다.
ㄴ. 비인가된 접근으로부터 데이터를 보호하고 인가된 해당 개체에 적합한 접근 권한을 부여한다.
ㄷ. 송·수신자 간에 전송된 메시지에 대해서, 송신자는 메시지 송신 사실을, 수신자는 메시지 수신 사실을 부인하지 못하도록 한다.

① ㄱ: 데이터 무결성, ㄴ: 부인봉쇄, ㄷ: 인증
② ㄱ: 데이터 가용성, ㄴ: 접근통제, ㄷ: 인증
③ ㄱ: 데이터 기밀성, ㄴ: 인증, ㄷ: 부인봉쇄
④ ㄱ: 데이터 무결성, ㄴ: 접근통제, ㄷ: 부인봉쇄

정답 4번

간단한 해설

ㄴ은 신원을 확인하는 인증이 아니라 **접근 권한을 정하는 접근통제**이다. ㄷ은 송·수신자가 전송 사실을 나중에 부인하지 못하게 하는 **부인봉쇄**이다.

대응 관계 해설

ㄱ. 데이터 무결성: 메시지의 내용과 순서가 훼손되지 않고 전달되도록 하는 서비스이다. 제시된 복제·추가·수정·순서 변경·재전송은 **원래 메시지나 메시지 흐름을 변형**한다는 공통점이 있다. 데이터 기밀성은 비인가자에게 내용이 노출되지 않도록 하는 것이고, 데이터 가용성은 인가된 사용자가 필요할 때 데이터를 이용할 수 있도록 하는 것이므로 ㄱ과 구별된다.

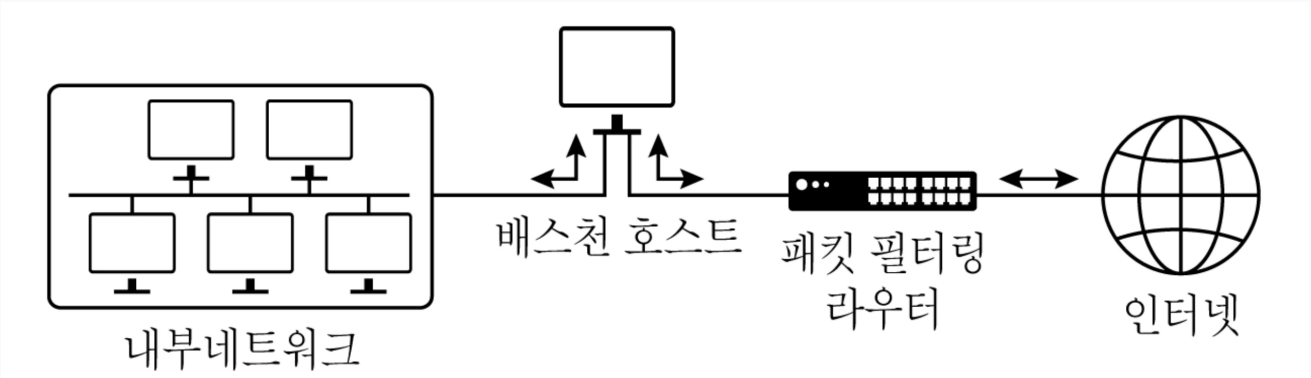
ㄴ. 접근통제: 비인가된 접근을 막고, 인가된 개체가 허용된 범위에서만 데이터에 접근하도록 권한을 부여·제한하는 서비스이다. 예를 들어 같은 파일에 대해 어떤 사용자에게는 읽기만, 다른 사용자에게는 수정까지 허용하는 것이다. 인증이 '누구인지'를 확인한다면, 접근통제는 **'무엇을 할 수 있는지'**를 정한다.

ㄷ. 부인봉쇄: 메시지를 보냈다는 사실이나 받았다는 사실을 당사자가 나중에 부인하지 못하도록 증거를 제공하는 서비스이다. 송신 사실의 부인 방지와 수신 사실의 부인 방지를 모두 포함한다. 핵심은 **송·수신 사실에 대한 사후 부인 방지**이며, 단순히 상대방의 신원을 확인하는 인증과 구별된다.

ㄱ은 데이터 무결성, ㄴ은 접근통제, ㄷ은 부인봉쇄에 대응하므로 ④의 연결과 일치한다.

NoteBase

문 16. 다음에 해당하는 방화벽의 구축 형태로 옳은 것은?



◯ 인터넷에서 내부네트워크로 전송되는 패킷을 패킷 필터링 라우터에서 필터링함으로써 1차 방어를 수행한다.
◯ 배스천 호스트에서는 필터링 된 패킷을 프록시와 같은 서비스를 통해 2차 방어 후 내부네트워크로 전달한다.

① 응용 레벨 게이트웨이(Application-level gateway)
② 회로 레벨 게이트웨이(Circuit-level gateway)
③ 듀얼 홈드 게이트웨이(Dual-homed gateway)
④ 스크린 호스트 게이트웨이(Screened host gateway)

정답 4번

간단한 해설

패킷 필터링 라우터의 1차 방어와 배스천 호스트의 프록시를 통한 2차 방어를 결합한 구조는 **스크린 호스트 게이트웨이**이다. 프록시의 존재뿐 아니라 **라우터와 배스천 호스트의 결합**이 구축 형태를 판별하는 기준이다.

공통 해설

스크린 호스트 게이트웨이는 **패킷 필터링 라우터와 배스천 호스트를 결합**한 방화벽 구축 형태이다. 배스천 호스트는 외부 접근에 대응하도록 보안을 강화한 호스트로, 프록시 등의 서비스를 제공한다. 그림에서 인터넷 쪽에 있는 패킷 필터링 라우터가 패킷을 먼저 걸러 내고, 그 안쪽의 배스천 호스트가 허용된 통신을 프록시로 중계하며 추가로 통제한다. 지문의 1차 방어와 2차 방어는 이 두 구성 요소의 역할에 각각 대응한다.

이 문제는 개별 게이트웨이의 처리 방식보다 **장비를 어떻게 결합했는지**를 묻는다. 응용 레벨 게이트웨이와 회로 레벨 게이트웨이는 각각 응용 서비스와 연결 수준에서 통신을 중계·통제하는 방식을 가리키므로, 라우터와 배스천 호스트를 결합한 전체 구축 형태의 명칭과 구별한다. 듀얼 홈드 게이트웨이는 두 네트워크 인터페이스를 가진 호스트로 내·외부 네트워크를 분리하는 구성이며, 제시된 라우터와 배스천 호스트의 결합을 식별하는 명칭은 스크린 호스트 게이트웨이이다.

NoteBase

문 17. SSH(Secure SHell)를 구성하고 있는 프로토콜 스택으로 옳지 않은 것은?

① SSH User Authentication Protocol

② SSH Session Layer Protocol

③ SSH Connection Protocol

④ SSH Transport Layer Protocol

정답 2번

간단한 해설

SSH의 기본 프로토콜 구성에는 **SSH Session Layer Protocol이 포함되지 않는다**. 셸 세션 등에 쓰이는 논리 채널은 SSH Connection Protocol이 제공한다.

공통 해설

SSH의 기본 프로토콜 구성은 **Transport Layer Protocol, User Authentication Protocol, Connection Protocol의 세 가지**이다.

Transport Layer Protocol은 서버 인증과 통신의 기밀성·무결성을 제공한다.

User Authentication Protocol은 이 보호된 통신 위에서 서버에 접속하려는 사용자를 인증한다.

Connection Protocol은 하나의 암호화된 연결을 여러 논리 채널로 나누어 셸 세션 등의 통신을 지원한다.

따라서 User Authentication Protocol, Connection Protocol, Transport Layer Protocol은 모두 SSH의 구성 요소이다. 반면 **SSH Session Layer Protocol이라는 별도의 기본 구성 요소는 없다**. SSH가 셸 세션을 지원한다는 사실과 'Session Layer Protocol'이라는 프로토콜이 기본 구성에 포함된다는 주장은 구별해야 한다.

NoteBase

문 18. 위험분석 방법에 대한 설명을 바르게 나열한 것은?

ㄱ. 시스템에 관한 전문적인 지식을 가진 전문가 집단을 구성하고 토론을 통해 정보시스템이 직면한 다양한 위협과 취약성을 분석하는 방법이다.
ㄴ. 자산의 가치 분석, 위협 분석, 취약점 분석을 수행하여 위험을 분석하는 방법이다.
ㄷ. 표준화된 보호대책의 세트를 체크리스트 형태로 구현하여 이를 기반으로 보호대책을 식별하는 방법이다.

① ㄱ: 시나리오법 ㄴ: 기준선 접근법 ㄷ: 상세 위험 분석 접근법
② ㄱ: 시나리오법 ㄴ: 상세 위험 분석 접근법 ㄷ: 기준선 접근법
③ ㄱ: 델파이법 ㄴ: 기준선 접근법 ㄷ: 상세 위험 분석 접근법
④ ㄱ: 델파이법 ㄴ: 상세 위험 분석 접근법 ㄷ: 기준선 접근법

정답 4번

간단한 해설

자산의 가치·위협·취약점을 개별적으로 분석하는 것은 **상세 위험 분석 접근법**이고, 표준화된 보호대책을 체크리스트로 적용하는 것은 **기준선 접근법**이다. 두 방법은 해당 시스템의 위험을 직접 분석하는지, 미리 마련된 보호대책을 기준으로 점검하는지에서 구별된다.

대응 관계 해설

ㄱ. 델파이법: **전문가 집단의 지식과 판단을 종합**하여 위험을 분석하는 방법이다. 제시문은 시스템을 잘 아는 전문가들이 위협과 취약성을 분석한다는 점에 초점이 있다. 반면 시나리오법은 특정 조건에서 위협이 현실화될 때 발생할 수 있는 상황과 결과를 구성하여 추정하는 방법이다.

ㄴ. 상세 위험 분석 접근법: **자산 가치·위협·취약점을 각각 분석**하고 이를 종합하여 위험을 평가한다. 자산 가치 분석은 보호할 대상의 중요성을, 위협 분석은 자산에 피해를 줄 수 있는 원인을, 취약점 분석은 그 위협에 이용될 수 있는 약점을 파악하는 것이다. 따라서 제시된 세 가지 분석을 수행한다는 설명이 이 접근법에 해당한다.

ㄷ. 기준선 접근법: 표준화된 보호대책을 체크리스트로 마련하고, 이를 기준으로 필요한 대책과 이행 여부를 점검한다. 시스템마다 위험요소를 처음부터 상세히 분석하기보다 **미리 정한 기본 보호수준**을 확보하는 데 초점이 있다. 제시문의 '표준화된 보호대책의 세트'와 '체크리스트'가 이 방법을 가리킨다.

ㄱ은 델파이법, ㄴ은 상세 위험 분석 접근법, ㄷ은 기준선 접근법으로 대응하므로 ④의 조합과 일치한다.

NoteBase

문 19. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상 개인정보 취급방침에 포함되어야 할 사항이 아닌 것은?

① 이용자 및 법정대리인의 권리와 그 행사 방법

② 개인정보에 대한 내부 관리 계획

③ 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항

④ 개인정보의 수집·이용 목적, 수집하는 개인정보의 항목 및 수집 방법

정답 2번

간단한 해설

②의 내부 관리 계획은 개인정보를 안전하게 취급하기 위해 **사업자 내부에서 수립·시행하는 보호조치**이다. 구 정보통신망법상 개인정보 취급방침에 반드시 포함하여 공개할 사항과는 구별된다.

선지별 해설

① O: 구 정보통신망법 제27조의2제2항제5호는 **이용자 및 법정대리인의 권리와 그 행사방법**을 개인정보 취급방침에 포함하도록 규정하였다. 이용자가 자신의 개인정보에 관한 권리와 이를 행사하는 절차를 알 수 있도록 공개하는 사항이다.

② X: 개인정보에 대한 내부 관리 계획은 구 정보통신망법 제27조의2제2항에 열거된 필수 공개사항에 포함되지 않는다. 이는 같은 법 제28조제1항제1호에 따라 개인정보를 안전하게 취급하기 위해 **수립·시행해야 하는 내부관리계획**으로, 기술적·관리적 보호조치에 해당한다. 계획을 수립할 의무와 그 계획을 취급방침에 반드시 포함하여 공개할 의무는 구별해야 한다.

③ O: 구 정보통신망법 제27조의2제2항제6호는 개인정보 자동 수집 장치의 **설치·운영 및 그 거부에 관한 사항**을 포함하도록 규정하였다. 인터넷 접속정보파일 등으로 개인정보가 자동 수집되는 방식과 이를 거부하는 데 필요한 사항을 이용자에게 알리기 위한 것이다.

④ O: 구 정보통신망법 제27조의2제2항제1호는 개인정보의 **수집·이용 목적, 수집 항목 및 수집방법**을 포함하도록 규정하였다. 이용자가 어떤 개인정보를 어떤 방법으로 수집하며 무엇에 사용하는지 확인할 수 있게 하는 사항이다.

NoteBase

문 20. 전자서명 방식에 대한 설명으로 옳지 않은 것은?

① 은닉 서명(blind signature)은 서명자가 특정 검증자를 지정하여 서명하고, 이 검증자만이 서명을 확인할 수 있는 방식이다.

② 부인방지 서명(undeniable signature)은 서명을 검증할 때 반드시 서명자의 도움이 있어야 검증이 가능한 방식이다.

③ 위임 서명(proxy signature)은 위임 서명자로 하여금 서명자를 대신해서 대리로 서명할 수 있도록 한 방식이다.

④ 다중 서명(multisignature)은 동일한 전자문서에 여러 사람이 서명하는 방식이다.

정답 1번

간단한 해설

①의 '특정 검증자만 서명을 확인'한다는 설명은 은닉 서명의 특징이 아니다. 은닉 서명은 **서명자가 메시지 내용을 알 수 없도록** 가린 상태에서 서명을 받는 방식이다.

선지별 해설

① X: 은닉 서명은 **서명할 메시지의 내용을 서명자에게 숨기는** 방식이다. 요청자가 메시지를 은닉하여 보내면 서명자는 그 내용을 모르는 상태에서 서명하고, 요청자는 은닉을 해제하여 원래 메시지에 대한 유효한 서명을 얻는다. 핵심은 서명자가 메시지 내용을 알 수 없다는 것이며, 특정 검증자만 확인할 수 있도록 검증 권한을 제한하는 것이 아니다.

② O: 부인방지 서명(undeniable signature)은 서명의 유효성을 확인할 때 **서명자의 협력이 필요한** 방식이다. 검증자가 공개키만으로 독립적으로 확인하는 일반적인 전자서명과 달리, 서명자가 검증 프로토콜에 참여해야 한다.

③ O: 위임 서명은 원래 서명자가 자신의 **서명 권한을 다른 사람에게 위임**하여, 위임받은 사람이 원래 서명자를 대신해 서명하도록 하는 방식이다. 대리 서명을 하는 주체가 위임 서명자이다.

④ O: 다중 서명은 **동일한 전자문서에 여러 서명자가 참여**하여 공동으로 서명하는 방식이다. 여러 사람의 서명이 필요한 문서에서 이들의 공동 서명 사실을 확인할 수 있도록 한다.

NoteBase