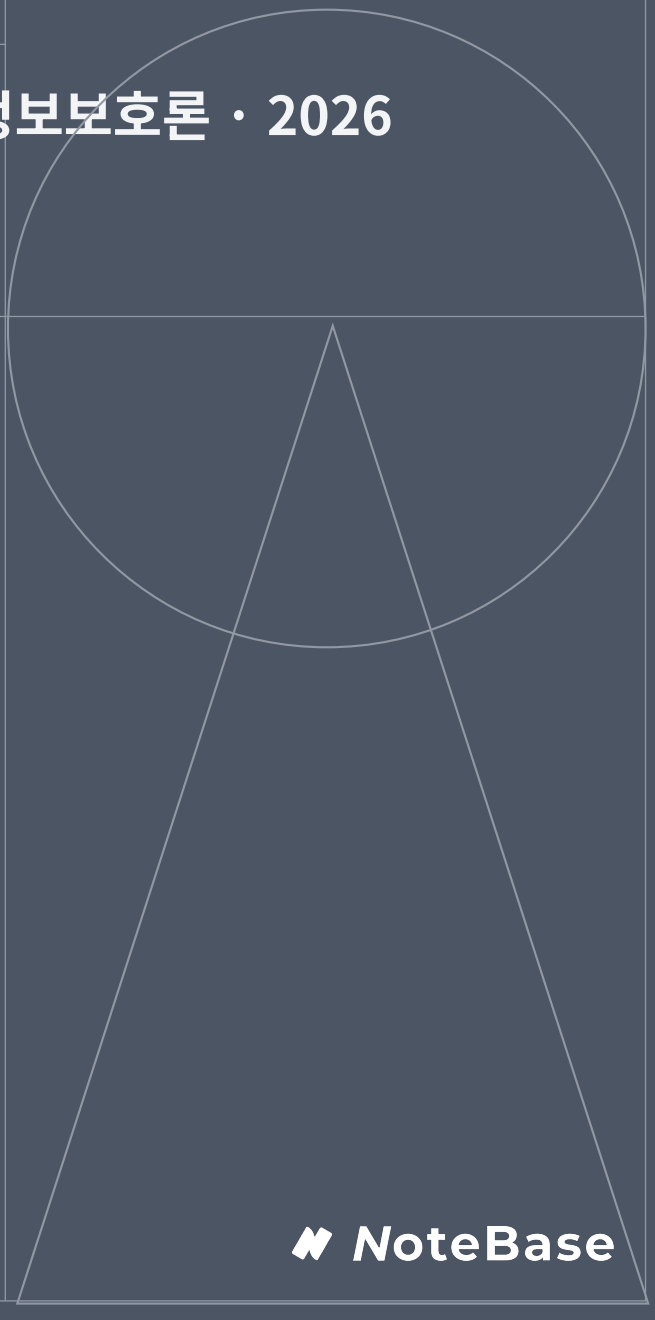
기출OX 해설집

공무원/경찰/공채(경위) · 정보보호론 · 2026



NoteBase

기출OX 해설집

공무원/경찰/공채(경위) · 정보보호론 · 2026

공무원/경찰/공채(경위) · 정보보호론 · 2026

문 1. 보안 공격에 대한 설명으로 가장 적절하지 않은 것은?

① 보안 공격은 수동적 공격과 능동적 공격으로 구분된다.

② 수동적 공격의 종류는 스니핑, 트래픽 분석, 가로채기 등이 있다.

③ 능동적 공격의 종류는 재사용 공격, 서비스 거부 공격 등이 있다.

④ 수동적 공격은 시스템 자원을 변경하거나 시스템 작동에 영향을 끼치는 공격이다.

정답 4번

간단한 해설

수동적 공격은 통신 내용이나 흐름을 **변경하지 않고 관찰·수집**하는 공격이다. 시스템 자원을 바꾸거나 정상 동작에 영향을 주는 것은 능동적 공격에 해당한다.

선지별 해설

① O: 보안 공격은 대상을 관찰하여 정보를 얻는 수동적 공격과, 데이터나 시스템의 상태·동작에 개입하는 능동적 공격으로 구분할 수 있다. 구분 기준은 공격자가 **정보와 동작을 변경하거나 방해하는지**이다.

② O: 스니핑은 통신 데이터를 엿보는 행위이며, 트래픽 분석은 통신량·시점·통신 상대 등의 패턴에서 정보를 추론하는 행위이다. 여기서 가로채기는 전송 정보를 몰래 포착하여 읽는 의미이므로 수동적 공격에 해당한다. 내용을 읽기만 하는 것과 내용을 변경·주입하는 것은 구별한다.

③ O: 재사용 공격은 이전에 수집한 유효한 메시지 등을 다시 전송하여 상대 시스템이 이를 받아들이도록 시도하는 공격이다. 정보를 수집한 뒤 **다시 주입하여 시스템 동작에 개입**하므로 능동적 공격이다. 서비스 거부 공격도 정상적인 서비스 이용을 방해하므로 능동적 공격에 해당한다.

④ X: 시스템 자원을 변경하거나 시스템 작동에 영향을 끼치는 공격은 **능동적 공격**이다. 수동적 공격은 데이터나 정상 동작을 직접 바꾸지 않고 정보를 획득하는 데 초점을 둔다. 따라서 두 공격 유형의 정의를 바꾸어 설명했다.

NoteBase

문 2. 다음은 보안 요소에 대한 설명이다. 빈칸 ㉠, ㉡, ㉢에 해당하는 것으로 가장 적절한 것은?

(㉠) 은 정보시스템의 알려진 손실이나 손상의 원인이 되는 환경을 이용해 원하지 않는 사건이 발생하여 손실 또는 부정적인 영향을 미칠 가능성이다.
(㉡) 은 정보시스템의 약점 또는 보호대책의 결핍 등 잠재적인 속성으로 공격에 이용 대상이 되는 것이다.
(㉢) 은 정보시스템의 손실이나 손상을 초래할 수 있는 원하지 않는 사고의 잠재적인 원인이다.

① ㉠: 위협, ㉡: 취약점, ㉢: 위험
② ㉠: 취약점, ㉡: 위험, ㉢: 위협
③ ㉠: 위험, ㉡: 취약점, ㉢: 위협
④ ㉠: 위협, ㉡: 위험, ㉢: 취약점

정답 3번

간단한 해설

피해를 일으킬 수 있는 잠재적 원인은 **위협**, 그 원인에 이용될 수 있는 약점은 **취약점**이다. 이로 인해 손실이나 부정적 영향이 생길 가능성은 위험이므로, 세 설명의 초점을 구별해야 한다.

빈칸별 해설

세 개념은 피해를 일으킬 수 있는 원인, 그 원인에 이용될 수 있는 약점, 그리고 실제 손실로 이어질 가능성을 구분하면 된다.

㉠ 위험: 사건이 발생하여 **손실이나 부정적 영향이 생길 가능성**에 초점을 둔다. 정보보호 위험을 평가할 때는 일반적으로 사건의 발생 가능성과 발생했을 때의 영향을 함께 고려한다. 원인이 존재한다는 사실 자체보다는 그것이 조직에 어떤 손실로 이어질 수 있는지가 핵심이다.

㉡ 취약점: 시스템의 약점이나 보호대책의 결핍처럼 **위협에 이용될 수 있는 약점**을 말한다. 예를 들어 보안 패치가 적용되지 않은 결함이나 부실한 접근통제가 이에 해당한다. 약점은 공격자가 활용하는 대상이지, 손실 가능성 그 자체를 뜻하지 않는다.

㉢ 위협: 정보시스템에 손실이나 손상을 가져올 수 있는 **원하지 않는 사고의 잠재적인 원인**이다. 악의적인 공격뿐 아니라 화재나 사용자 실수 등도 위협이 될 수 있으므로 고의적인 공격에만 한정하지 않는다.

따라서 ㉠ 위험, ㉡ 취약점, ㉢ 위협의 조합이며, 선택지 ③과 일치한다.

NoteBase

문 3. 통합 보안 관리 시스템(ESM)에 대한 설명 중 옳은 것의 개수로 가장 적절한 것은?

가. ESM은 firewall, IDS, VPN 등 다양한 보안 솔루션을 활용한다.
나. 관리콘솔, 매니저, 에이전트 등으로 구성된다.
다. 에이전트는 관리콘솔에서 설정한 정책을 적용하고 데이터 취합, 저장, 분석을 담당한다.
라. 여러 시스템의 보안 로그를 기반으로 상호 연관분석을 통해 분석적 침해 사고 대응이 가능하다.

① 1개
② 2개
③ 3개
④ 4개

정답 3번

간단한 해설

여러 보안 장비의 데이터를 중앙에서 **취합·저장·분석하는 역할은 매니저**에 해당한다. 에이전트는 주로 각 장비의 이벤트를 수집·전달하므로, 두 구성요소의 역할을 바꾼 다가 틀리다.

NoteBase

보기별 해설

ESM은 여러 보안 장비의 정보를 한곳에서 관리하고 연관성을 분석하는 통합 보안 관리 체계이다. 이 문제에서는 각 구성요소의 역할과 로그 분석 기능을 구별한다.

가. O: 방화벽은 통신 통제, IDS는 침입 탐지, VPN은 안전한 원격 연결 등의 기능을 제공한다. ESM은 이런 **서로 다른 보안 솔루션의 정보와 이벤트를 통합**하여 전체 보안 상태를 관리한다.

나. O: 대표적인 구성은 관리콘솔, 매니저, 에이전트이다. 관리콘솔은 관리자의 정책 설정과 결과 조회를 위한 인터페이스이고, 매니저는 중앙 관리·분석을 담당하며, 에이전트는 각 보안 시스템과 연계하여 이벤트를 수집·전달한다.

다. X: 여러 에이전트가 보낸 데이터를 중앙에서 **취합·저장·분석하는 주체는 매니저**이다. 에이전트의 주된 역할은 담당 장비의 로그·이벤트 수집과 전달이며, 구성에 따라 정책이나 명령을 해당 장비에 적용하는 역할도 한다. 선지는 중앙 관리 기능을 에이전트의 기능으로 설명했다.

라. O: 개별 로그만 보면 드러나지 않는 공격도 여러 장비의 이벤트를 시간·주소·행위 등의 기준으로 연결하면 파악할 수 있다. 이러한 **상호 연관분석**은 침해 징후를 식별하고 사고 대응의 근거를 마련하는 데 활용된다.

옳은 보기는 가, 나, 라의 3개이므로 ③에 해당한다.

NoteBase

문 4. 다음에서 설명하는 것으로 가장 적절한 것은?

◯ 공격 대상의 정보를 모으는 방법 중 하나이다.
◯ 비기술적인 방법을 통해 정보를 모으기도 한다.
◯ 기술적인 방법으로는 스캔, 운영체제 탐지, 방화벽 탐지 등의 방법이 있다.

① 허니팟
② 다중화
③ 풋프린팅
④ 스파이웨어

정답 3번

간단한 해설

풋프린팅은 공격을 준비하기 위해 대상의 정보를 수집하는 활동이다. 비기술적인 정보 수집뿐 아니라 스캔, 운영체제 탐지, 방화벽 탐지 같은 기술적 방법도 활용한다.

공통 해설

풋프린팅은 공격 대상의 조직·시스템·네트워크에 관한 정보를 모아 대상의 환경과 공격에 활용될 수 있는 단서를 파악하는 활동이다. 핵심은 특정 도구의 사용 여부가 아니라 **공격을 준비하기 위한 대상 정보 수집**이라는 목적에 있다.

정보를 얻는 방법은 기술적인 방법에 한정되지 않는다. 공개된 조직 자료를 살피거나 사람에게서 정보를 얻는 비기술적 방법도 활용한다. 기술적으로는 스캔으로 시스템과 서비스의 상태를 확인하고, 운영체제 탐지와 방화벽 탐지로 대상의 시스템 환경과 보안 구성을 파악한다. 따라서 제시된 세 설명은 모두 풋프린팅의 정보 수집 목적과 방법을 나타낸다.

NoteBase

문 5. 안드로이드 운영체제에 대한 설명으로 가장 적절하지 않은 것은?

① 개방형 운영체제로서 보안정책의 운영은 스마트폰 제조사에서 운영하도록 하고 있다.

② 안드로이드 앱의 권한 상승은 프로세스 간 통신 기법을 적용하면서 발생할 수 있다.

③ 루팅(rooting)은 운영체제 취약점을 해킹하여 스마트폰의 루트 권한을 얻는 방법이다.

④ 안드로이드는 앱 설치 시 사용할 퍼미션을 명시하고, 사용자가 이를 승인하도록 한다.

정답 1번

간단한 해설

개방형 운영체제라는 사실이 보안정책 운영을 스마트폰 제조사에 맡긴다는 뜻은 아니다. 안드로이드는 **플랫폼 차원의 공통 보안모델**을 제공하며, 제조사의 보안 구현·업데이트와 사용자의 앱 권한 통제가 함께 작동한다.

선지별 해설

① X: 안드로이드가 개방형 운영체제라는 부분은 맞지만, 보안정책 운영을 스마트폰 제조사에 맡기는 구조라는 설명은 부적절하다. 안드로이드 플랫폼은 앱을 서로 격리하는 샌드박스, 권한 검사, 앱 서명 등의 **공통 보안모델**을 제공한다. 제조사는 기기에 이를 구현하고 보안 업데이트를 제공하며, 사용자는 앱의 권한 허용 여부를 통제한다. 제조사가 보안에 관여하는 것과 보안정책 운영을 제조사에 맡긴다는 것은 구별해야 한다.

② O: 프로세스 간 통신(IPC)은 서로 다른 앱이나 프로세스가 요청과 데이터를 주고받는 수단이다. 권한이 있는 앱이 외부 요청자의 권한을 제대로 확인하지 않고 민감한 기능을 대신 실행하면, 요청자는 **자신에게 없는 권한의 효과**를 얻을 수 있다. 예를 들어 연락처 접근 권한이 없는 앱이 IPC로 다른 앱을 악용하여 연락처를 전달받는 경우이다. IPC 자체가 항상 권한 상승을 일으키는 것은 아니며, 통신 인터페이스의 접근통제가 부실할 때 문제가 된다.

③ O: 루팅은 일반 사용자나 앱에 제한된 **루트 권한을 확보**하는 것이다. 운영체제나 커널의 취약점을 악용하여 권한을 상승시키는 방법으로 루팅할 수 있으며, 이를 통해 일반 앱에는 허용되지 않는 시스템 영역의 접근·변경이 가능해질 수 있다. 다만 루팅의 본질은 루트 권한의 획득이며, 부트로더를 해제하고 수정된 운영체제를 설치하는 방식도 있어 모든 루팅이 반드시 취약점 악용으로 이루어지는 것은 아니다.

④ O: 앱은 필요한 권한을 AndroidManifest.xml에 선언하고, 사용자 승인이 필요한 권한은 승인을 받아 사용한다. 선지의 '설치 시 승인'은 **구형 설치 시 권한 승인 모델**에 해당한다. Android 5.1 이하에서는 위험 권한을 설치·업데이트 시 승인했지만, Android 6.0 이상에서 런타임 권한 모델을 적용하는 앱은 위험 권한을 실행 중에 요청한다. 일반 권한은 설치 시 자동 부여되므로, 모든 버전과 모든 권한에 설치 시 사용자 승인이 필요하다는 뜻으로 확대하면 안 된다.

NoteBase

문 6. 디지털 포렌식에 대한 설명 중 옳은 것의 개수로 가장 적절한 것은?

가. 시스템 포렌식은 운영체제를 분석하여 증거를 확보한다.
나. 클라우드 환경에서는 디지털 포렌식을 통한 증거수집이 불가능하다.
다. 무결성의 원칙에 따라 컴퓨터 내부의 정보 획득은 신속하게 이루어져야 한다.
라. 디지털 데이터는 복사가 가능하므로 디지털 증거 능력 요건을 갖출 수 없다.

① 1개
② 2개
③ 3개
④ 4개

정답 1번

가

시스템 포렌식은 **운영체제의 로그·레지스트리·사용 기록 등을 분석**하여 증거를 확보한다.

나

클라우드에서도 **로그·저장 데이터·가상머신 등을 수집·분석하여 증거를 확보**할 수 있다. 데이터의 분산과 접근 권한 때문에 수집이 어려울 수 있으나 불가능한 것은 아니다.

다

정보가 사라지기 전에 신속히 확보해야 한다는 것은 **신속성의 원칙**이다. **무결성의 원칙은 수집·분석·보관 과정에서 증거가 훼손되거나 변경되지 않도록 유지**하는 것이다.

NoteBase

라

복사할 수 있다는 이유만으로 증거능력이 배제되지는 않는다. **원본과 복제본의 동일성·무결성이 입증되고 적법한 수집 등 증거능력 요건을 갖추면** 디지털 증거를 사용할 수 있다.

(2) 기록에 의하여 살펴보면, 국가정보원에서 피고인들 혹은 가족, 직원이 입회한 상태에서 원심 판시 각 디지털 저장매체를 압수한 다음 입회자의 서명을 받아 봉인하였고, 국가정보원에서 각 디지털 저장매체에 저장된 자료를 조사할 때 피고인들 입회하에 피고인들의 서명무인을 받아 봉인 상태 확인, 봉인 해제, 재봉인하였으며, 이러한 전 과정을 모두 녹화한 사실, 각 디지털 저장매체가 봉인된 상태에서 서울중앙지방검찰청에 송치된 후 피고인들이 입회한 상태에서 봉인을 풀고 세계적으로 인정받는 프로그램을 이용하여 이미징 작업을 하였는데, 디지털 저장매체 원본의 해쉬(Hash) 값과 이미징 작업을 통해 생성된 파일의 해쉬 값이 동일한 사실, 제1심법원은 피고인들 및 검사, 변호인이 모두 참여한 가운데 검증을 실시하여 이미징 작업을 통해 생성된 파일의 내용과 출력된 문건에 기재된 내용이 동일함을 확인한 사실을 알 수 있는바, 그렇다면 출력된 문건은 압수된 디지털 저장매체 원본에 저장되었던 내용과 동일한 것으로 인정할 수 있어 증거로 사용할 수 있고, 같은 취지의 원심의 판단은 정당하다. (대법원 2007. 12. 13. 선고 2007도7257 판결)

NoteBase

문 7. IPSec 동작에 대한 설명으로 가장 적절하지 않은 것은?

① IPSec은 개방형 IP(Internet Protocol)에 보안 기능을 추가한 것이다.

② IPSec은 사용 중인 응용 프로그램과는 무관하게 동작이 가능하다.

③ IPSec은 인증, 비밀성, 키 관리의 3가지 기능 영역을 포함한다.

④ ESP(Encapsulating Security Payload)의 authentication data를 통해서 재전송 공격(replay attack)을 방지할 수 있다.

정답 4번

간단한 해설

ESP에서 재전송 패킷을 구별하는 직접적인 기준은 **순서번호와 수신 윈도**이다. Authentication Data는 무결성과 인증을 위한 값이며, 그 값이 유효하다는 사실만으로 이미 수신한 패킷인지 판단할 수는 없다.

선지별 해설

① O: IPSec은 IP 계층에서 패킷의 인증·무결성·기밀성 등 보안 서비스를 제공하는 프로토콜 체계이다. 따라서 기본 IP 통신에 **네트워크 계층의 보안 기능**을 추가한 것으로 볼 수 있다.

② O: IPSec은 응용 계층보다 아래인 IP 계층에서 처리되므로 응용 프로그램별로 보안 기능을 새로 구현하지 않아도 동작할 수 있다. 호스트나 보안 게이트웨이에서 적용하여 **응용 프로그램과 독립적으로** IP 트래픽을 보호한다.

③ O: IPSec은 데이터의 출처와 무결성을 확인하는 인증 영역, 내용을 숨기는 비밀성 영역, 필요한 키와 보안 설정을 관리하는 영역을 포함한다. 키 관리에서는 IKE 등을 통해 **보안 연관(SA)과 키를 설정**한다.

④ X: 재전송 공격은 공격자가 유효한 과거 패킷을 그대로 다시 보내는 것이므로 Authentication Data가 맞는지만 확인해서는 막을 수 없다. 수신자는 **순서번호와 재전송 방지 윈도**를 이용해 중복되거나 오래된 패킷을 걸러 낸다. 무결성 검증은 순서번호의 위조를 막는 데 필요하지만, 재전송 여부를 판별하는 순서번호 검사 자체를 대신하지는 않는다.

NoteBase

문 8. 디지털 콘텐츠 보호 기법에 대한 설명으로 가장 적절한 것은?

① 스테가노그래피는 디지털 콘텐츠 생성과 이용까지 유통 전 과정에 걸쳐 안전하게 관리 및 보호하는 기술이다.

② 크립토그래피는 데이터 은폐 기술 중 하나로 데이터를 다른 데이터에 삽입하는 기술이다.

③ 워터마킹은 메시지의 내용을 읽지 못하게 하는 기술이다.

④ 핑거프린팅은 디지털 콘텐츠 구매 시 구매자의 정보를 삽입하여 불법 배포 발견 시 최초의 배포자를 추적할 수 있게 하는 기술이다.

정답 4번

간단한 해설

핑거프린팅은 콘텐츠마다 **구매자를 구별할 수 있는 정보**를 넣어 불법 유통된 복제본의 출처를 추적한다. 따라서 정답은 ④이다.

선지별 해설

① (X) 콘텐츠의 생성부터 이용까지 유통 전 과정에서 권한을 관리하고 보호하는 기술은 **디지털 저작권 관리(DRM)**이다. 스테가노그래피는 다른 데이터에 정보를 숨겨 정보나 통신의 존재 자체를 알아차리기 어렵게 하는 기술이다.

② (X) 데이터를 다른 데이터에 삽입하여 숨긴다는 설명은 **스테가노그래피**에 해당한다. 크립토그래피의 암호화는 평문을 암호문으로 바꾸어 권한 없는 사람이 내용을 이해하지 못하도록 하는 것으로, 정보가 존재한다는 사실까지 숨기는 것은 아니다.

③ (X) 메시지의 내용을 읽지 못하게 하는 것은 **암호화**의 기능이다. 워터마킹은 콘텐츠에 저작권자 등의 식별 정보를 삽입하여 소유권을 확인하거나 저작권을 보호하는 기술이므로, 콘텐츠 자체를 읽을 수 없게 만드는 기술과 구별된다.

④ (O) 핑거프린팅은 콘텐츠의 복제본마다 **구매자별 식별 정보**를 삽입하는 기술이다. 불법 유통된 복제본에서 이 정보를 검출하면 어느 구매자에게 제공한 콘텐츠가 유출되었는지 추적할 수 있다.

NoteBase

문 9. 디지털 서명이 제공하는 기능으로 가장 적절하지 않은 것은?

① 인증

② 무결성

③ 가용성

④ 부인방지

정답 3번

간단한 해설

디지털 서명은 서명자의 인증, 메시지 무결성, 부인방지를 지원하지만 **서비스의 지속적인 이용을 보장하는 가용성**을 직접 제공하지는 않는다.

선지별 해설

디지털 서명은 서명자가 개인키로 생성하고 검증자가 대응하는 공개키로 확인한다. 서명 대상 데이터와 서명자를 연결하는 기술이며, 신뢰할 수 있는 공개키와 안전한 개인키 관리가 전제된다.

① O: 검증자는 서명이 특정 공개키에 대응하는 개인키로 생성되었는지 확인한다. 그 공개키가 누구의 것인지 신뢰할 수 있게 확인되어 있다면 **서명자의 신원 또는 데이터 출처를 인증**하는 근거가 된다.

② O: 서명 후 메시지가 바뀌면 원래 서명과 변경된 데이터의 대응이 깨져 검증에 실패한다. 이처럼 **서명된 데이터의 변경을 탐지**하는 기능이 무결성이다. 서명이 데이터 수정을 물리적으로 막는다는 의미는 아니다.

③ X: 가용성은 권한 있는 사용자가 필요할 때 정보와 서비스를 정상적으로 이용할 수 있는 성질이다. 디지털 서명만으로 서버 장애나 서비스 거부 공격을 막거나 서비스 중단을 복구할 수는 없다. 가용성은 이중화, 장애 복구, 용량 확보 등의 별도 대책으로 높인다.

④ O: 검증 가능한 서명은 서명자가 나중에 **서명 행위를 부인하기 어렵게 하는 증거**로 사용된다. 이를 부인방지라고 한다. 실제 증거력은 개인키가 안전하게 관리되었는지, 공개키가 서명자와 신뢰성 있게 연결되는지 등의 조건에 의존한다.

NoteBase

문 10. 대칭키 알고리즘에 대한 설명으로 옳은 것만을 모두 고른 것으로 가장 적절한 것은?

가. Skipjack는 음성을 암호화하는데 주로 사용되며, 80비트 키와 32라운드를 갖는다.
나. RC5는 256비트 키를 사용하며, 입출력과 라운드 수가 가변이다.
다. IDEA는 128비트 키를 사용해서 64비트의 평문을 8라운드에 거쳐 64비트 암호문으로 만든다.
라. A5/1은 각 길이가 20, 20, 24인 LFSR을 사용하고, 키 생성기는 4비트 키 스트림을 생성한다.

① 가, 나
② 가, 다
③ 가, 다, 라
④ 나, 다, 라

정답 2번

간단한 해설

RC5는 블록 크기와 라운드 수뿐 아니라 **키 길이까지 가변**이다. A5/1의 세 LFSR 길이는 **19·22·23비트**이며, 출력 단계에서 키 스트림을 1비트씩 생성한다.

보기별 해설

가. O: Skipjack은 음성 통신 보호용 장치 등에 사용되도록 개발된 대칭키 블록암호이다. **80비트 키와 32라운드**를 사용하며, 한 번에 처리하는 데이터 블록의 크기는 64비트이다. 키 길이와 데이터 블록 길이는 서로 다른 규격이다.

나. X: RC5는 블록 크기와 라운드 수뿐 아니라 **키 길이도 가변**인 알고리즘이다. 따라서 키를 256비트로 고정하여 설명하는 것은 부정확하다. 256비트 키를 선택할 수 있는지와 알고리즘의 키 길이가 256비트로 정해져 있다는 주장은 구별한다.

다. O: IDEA는 **128비트 키로 64비트 블록**을 암호화하여 64비트 암호문 블록을 만든다. 같은 구조의 8개 정규 라운드를 수행한 뒤 별도의 출력 변환을 거친다. 이 최종 변환을 반 라운드로 세어 전체를 8.5라운드라고도 표현하므로, 보기의 8라운드는 정규 라운드 수를 뜻한다.

라. X: A5/1은 길이가 **19비트·22비트·23비트**인 세 LFSR을 사용하는 스트림암호이다. 출력 단계에서는 세 레지스터의 출력 비트를 XOR하여 매 클록마다 키 스트림 1비트를 만든다. 따라서 레지스터 길이를 20·20·24로 쓴 부분과 한 번에 4비트를 생성한다는 부분이 모두 잘못이다.

따라서 옳은 보기는 가, 다이며, 이를 고른 ②와 일치한다.

NoteBase

문 11. DoS 공격에 대한 설명으로 옳은 것만을 모두 고른 것으로 가장 적절한 것은?

가. 티어드롭 공격은 패킷을 전송할 때 출발지 IP와 목적지 IP를 같은 값으로 설정하여 공격하는 방법이다.
나. 자원 고갈 공격에는 SYN 플러딩, HTTP CC, Ping of death 등이 있다.
다. HTTP GET 플러딩 공격은 웹 서버가 정상적으로 보이는 TCP 세션과 HTTP GET 요청을 받아 시스템에 부하가 걸리게 하는 공격이다.
라. 스머프 공격은 패킷의 시퀀스 넘버와 길이를 조작하여 패킷 간의 데이터 부분이 겹치거나 빠진 상태의 패킷으로 전송하는 공격이다.

① 가, 나
② 나, 다
③ 다, 라
④ 가, 라

정답 2번

간단한 해설

출발지와 목적지 IP가 같은 패킷을 이용하는 것은 **랜드 공격**이고, 비정상적인 단편의 재조립을 이용하는 것은 **티어드롭 공격**이다. 가와 라는 공격 명칭을 잘못 연결했다.

NoteBase

보기별 해설

DoS는 정상 사용자가 서비스를 이용하지 못하게 하는 공격이다. 공격 이름을 구별할 때는 주소 조작, 연결 자원 점유, 웹 요청 부하, 단편 재조립 오류 중 무엇을 이용하는지 확인한다.

가. X: 출발지 IP와 목적지 IP를 같게 설정하는 것은 **랜드(LAND) 공격**의 특징이다. 티어드롭은 IP 단편의 위치와 길이 정보를 비정상적으로 구성하여, 취약한 시스템이 단편을 재조립하는 과정에서 오류를 일으키는 공격이다.

나. O: SYN 플러딩은 연결 대기 자원을 점유하고, HTTP CC는 캐시의 응답 효과를 줄이는 요청으로 웹 서버의 처리 부담을 키운다. Ping of Death는 비정상적으로 큰 패킷의 재조립 과정에서 메모리 처리 오류 등을 유발하여 시스템을 마비시킨다. 자원 고갈형은 연결 자원이나 CPU·메모리 등의 가용 자원 또는 처리 한도를 소진시키는 방식이고, Ping of Death는 비정상 패킷 처리의 구현 취약점을 악용하는 방식이라는 차이가 있다. 이 문항은 공식 채점상 Ping of Death를 포함한 나를 옳은 보기로 인정하지만, 작동 원리를 엄밀히 나누면 두 유형은 구별된다. 특히 **Ping of Death는 단순한 대량 핑 전송과 구별**된다.

다. O: HTTP GET 플러딩은 정상 요청처럼 보이는 세션과 GET 요청을 대량으로 처리하게 하여 웹 서버의 CPU, 메모리, 연결 등의 자원을 소모시킨다. **요청 형식이 정상처럼 보여도** 과도한 처리량 때문에 정상 사용자의 서비스 이용이 방해될 수 있다.

라. X: 단편 데이터가 겹치도록 위치·길이 정보를 조작하여 재조립 오류를 일으키는 설명은 **티어드롭 공격**에 해당한다. 스머프는 피해자의 주소로 위장한 ICMP 요청에 대해 여러 호스트의 응답이 피해자에게 몰리게 하는 반사·증폭형 공격이다. IP 단편 재조립에서는 TCP 시퀀스 번호와 구별되는 단편 오프셋이 중요하다.

옳은 보기는 나, 다이므로 이 조합을 제시한 ②에 해당한다.

NoteBase

문 12. 다음에서 설명하는 암호 알고리즘으로 가장 적절한 것은?

이산 대수 문제의 어려움에 기반을 둔 암호 알고리즘으로서, 이 방식 암호화에서는 암호문 길이가 평문의 2배로 늘어나는 특징이 있다.

① ECC
② RSA
③ Rabin
④ ElGamal

정답 4번

간단한 해설

ElGamal은 이산 대수 문제에 기반을 두며, 평문 한 블록을 암호화할 때 **두 성분으로 이루어진 암호문**을 만든다. 평문과 각 성분을 같은 길이로 표현하는 기본 방식에서는 암호문 길이가 평문의 2배가 된다.

핵심 풀이

이산 대수 문제: 적절히 선택한 유한체에서 거듭제곱의 밑과 계산 결과를 알아도 그 지수를 구하기는 어렵다는 문제이다. ElGamal은 이 어려움을 이용하여 공개된 값에서 비밀 지수를 쉽게 알아낼 수 없도록 한다.

암호문 길이: ElGamal은 암호화할 때 새 난수를 선택하고, 그 난수에서 만든 값과 평문을 가린 값을 함께 보낸다. 첫 성분은 수신자가 자신의 개인키로 암호화에 쓰인 비밀값을 구하는 데 필요하고, 둘째 성분은 그 비밀값을 평문에 곱하여 만든 값이다. 따라서 **평문 한 블록에 암호문 두 성분**이 대응한다. 평문과 각 성분을 같은 비트 길이로 표현하는 기본 ElGamal 암호화에서는 암호문 길이가 평문의 2배가 된다.

다른 후보와의 구분: RSA와 Rabin은 큰 정수의 소인수분해 어려움과 관련된 방식이므로 이산 대수 문제라는 단서와 구별된다. ECC는 타원곡선 위의 이산 대수 문제를 이용하는 암호 체계이므로 첫 단서만으로는 배제할 수 없다. 그러나 **암호문 길이가 항상 평문의 2배라는 것은 ECC 전체의 공통 특성이 아니다**. 두 성분을 보내는 기본 암호화 구조까지 함께 지칭하는 명칭은 ElGamal이다.

NoteBase

문 13. S/MIME에 대한 설명으로 가장 적절하지 않은 것은?

① 전자서명을 위해 DSS를 사용한다.

② 해시 알고리즘은 SHA-1을 사용한다.

③ 세션 키 암호화에는 AES를 사용한다.

④ X.509로 정의되는 인증기관에 의해 서명된 공개 키 인증서를 사용한다.

정답 3번

간단한 해설

기존 S/MIME v3에서는 세션 키를 **RSA 등 공개키 방식**으로 보호하고 메시지 본문은 세션 키를 이용해 **3DES**로 암호화한다. 세션 키 자체를 보호하는 방식과 본문을 암호화하는 방식을 구분해야 한다.

출제 포인트

S/MIME의 전자서명, 해시, 세션 키 보호, 공개 키 인증서가 각각 어떤 역할을 하는지 구분하는 문제이다.

핵심 개념

S/MIME는 전자우편의 MIME 데이터에 전자서명과 암호화 기능을 더하는 표준이다. 전자서명은 발신자 인증과 메시지 무결성 확인에, 암호화는 내용의 기밀성 보호에 사용된다.
세션 키는 메시지 본문을 암호화하는 대칭키이다. 본문은 이 키로 암호화하고, 키를 수신자에게 전달할 때는 공개키 방식으로 보호한다. RSA 방식에서는 수신자의 공개키로 세션 키를 암호화하며, 수신자는 자신의 개인키로 이를 복호화한다.
기존 S/MIME v3(RFC 2633)의 대표적인 알고리즘 구분은 서명에 DSS의 DSA, 해시에 SHA-1, 본문 암호화에 3DES이다.

NoteBase

선지별 해설

① O
DSS는 전자서명 표준이며, 기존 S/MIME v3에서는 DSS에 정의된 DSA를 지원한다. 서명자는 자신의 개인키로 서명하고, 수신자는 서명자의 공개키로 검증한다.

② O
기존 S/MIME v3에서는 메시지의 해시값을 구하는 알고리즘으로 SHA-1을 지원한다. 해시값은 메시지의 변경 여부를 확인하는 전자서명 절차에 사용된다.

③ X
'세션 키 암호화에는 AES를 사용한다'는 표현이 틀렸다. 세션 키 자체의 암호화는 RSA와 같은 공개키 방식으로 설명하며, S/MIME v3의 키 관리에는 Diffie-Hellman 키 합의도 포함된다. 세션 키를 이용한 본문 암호화를 뜻하더라도 기존 v3의 필수 지원 알고리즘은 AES가 아니라 3DES이다. 따라서 세션 키 보호는 공개키 방식, 본문 암호화는 대칭키 방식으로 고쳐 구분한다.

④ O
S/MIME는 X.509 형식의 공개 키 인증서를 사용한다. 인증서는 인증기관의 전자서명으로 주체의 신원과 공개키의 연결을 확인할 수 있게 하므로, 서명 검증과 암호화에 사용할 공개키의 신뢰를 확인하는 데 필요하다.

오답 포인트

③의 '세션 키 암호화'와 '세션 키로 본문을 암호화'는 대상이 다르다. AES가 대칭키 알고리즘이라는 사실만 보고 세션 키 자체의 보호 수단으로 판단하면 두 역할을 혼동하게 된다.

다시 나오면 이렇게 판단

먼저 암호화 대상이 본문인지 세션 키인지 확인한다. 본문 암호화에는 대칭키 알고리즘을, 세션 키 전달에는 공개키를 이용한 암호화나 키 합의를 연결한다. 전자서명·해시·인증서는 각각 서명 생성과 검증, 해시값 계산, 공개키 신뢰 확인으로 구분한다.

암기 포인트

기존 S/MIME v3: 서명은 DSS, 해시는 SHA-1, 본문은 3DES, 키 보호는 RSA·DH, 인증서는 X.509이다.

NoteBase

문 14. 다음은 암호에 대한 설명이다. 빈칸 ㉠, ㉡에 해당하는 것으로 가장 적절한 것은?

(㉠)는 곱셈과 덧셈을 결합하여 암호화하는 방법으로서 ax+b(26)로 암호화한다. (㉡)는 트리테미우스 암호표를 사용하지만, 문자의 순서가 i번째이면 암호표에서 i번째를 적용하지 않고, 암호화 키에 따라 암호표를 적용하여 규칙성을 벗어난 암호화 방법이다.

① ㉠: 아핀 암호
㉡: 비게네르 암호

② ㉠: 아핀 암호
㉡: 시저 암호

③ ㉠: 시저 암호
㉡: 비게네르 암호

④ ㉠: 시저 암호
㉡: 아핀 암호

정답 1번

간단한 해설

곱셈과 덧셈을 결합한 변환식은 **아핀 암호**의 특징이다. 문자 위치가 아니라 키에 따라 암호표의 행을 선택하는 방식은 **비게네르 암호**이다.

빈칸별 해설

㉠ 아핀 암호: 알파벳을 0부터 25까지의 수로 대응시키고 E(x)=(ax+b) 26으로 변환한다. **곱셈에 의한 치환과 일정한 값의 덧셈**을 결합한 것이 핵심이다. 복호화가 가능하려면 a와 26이 서로소여야 한다. 시저 암호는 모든 문자에 같은 이동량을 더하는 방식으로, 이 식에서 a = 1인 특수한 경우이다.

㉡ 비게네르 암호: 암호화 키의 각 문자에 따라 서로 다른 이동량을 적용하는 다중 치환 암호이다. 문자 위치에 따라 암호표의 행을 순서대로 쓰는 것이 아니라 **키가 지정하는 행을 선택**한다. 따라서 같은 평문 문자도 대응하는 키 문자에 따라 다른 암호문 문자가 될 수 있다.

따라서 ㉠은 아핀 암호, ㉡은 비게네르 암호이며, 이 조합은 ①과 일치한다.

NoteBase

문 15. 무선랜 보안에 대한 설명으로 가장 적절하지 않은 것은?

① WEP(Wired Equivalent Privacy)는 TKIP(Temporal Key Integrity Protocol)를 사용한다.

② WPA(Wi-Fi Protected Access)는 WPA-개인과 WPA-엔터프라이즈가 있다.

③ WPA-엔터프라이즈는 RADIUS 인증 서버를 사용하는 경우를 의미한다.

④ WPA-2에서 사용하는 CCMP(CCM mode Protocol)는 AES 블록 암호 방식을 사용한다.

정답 1번

간단한 해설

TKIP는 WEP가 아니라 WPA에서 도입한 방식이다. WEP는 RC4를 사용하지만, WPA의 TKIP가 추가한 패킷별 키 혼합과 무결성 강화 기능을 갖춘 것은 아니다.

선지별 해설

① X: WEP는 RC4 스트림 암호를 이용하는 초기 무선랜 보안 방식이다. TKIP는 WEP의 취약점을 보완하기 위해 **WPA에서 도입**되었으며 패킷별 키 혼합과 무결성 검사 등을 강화했다. 두 방식이 RC4를 이용한다는 공통점 때문에 WEP 자체가 TKIP를 사용한다고 보아서는 안 된다.

② O: WPA에는 **개인용과 엔터프라이즈용 인증 방식**이 있다. 개인용은 사전 공유 키를 사용하는 방식이며, 엔터프라이즈용은 사용자별 인증을 수행하는 802.1X/EAP 기반 방식이다.

③ O: WPA-엔터프라이즈는 일반적으로 **RADIUS 인증 서버를 연계**하여 사용자 인증을 중앙에서 처리한다. 무선 단말의 인증 정보를 액세스 포인트를 통해 인증 서버와 교환하므로, 공통 사전 공유 키에 의존하는 WPA-개인과 구별된다.

④ O: WPA2의 CCMP는 **AES 블록 암호**를 기반으로 데이터의 기밀성과 무결성을 제공한다. 암호화에는 카운터 모드, 인증에는 CBC-MAC을 결합하는 CCM 방식을 사용하며, RC4 기반 TKIP와 구별된다.

NoteBase

문 16. AWS 서비스에 대한 설명으로 가장 적절한 것은?

계정 관리 전반 및 프로비저닝 기능을 포함한 포괄적인 의미의 계정 관리 솔루션으로 고객의 요구를 반영한 기능 조합 및 확장이 가능하다. 업무 효율성, 생산성, 보안성의 극대화가 가능한 비즈니스 도구이다.

① SSO(Single Sign-On)
② IAM(Identity and Access Management)
③ EAM(Extranet Access Management)
④ KMS(Key Management Service)

정답 2번

간단한 해설

IAM은 사용자 계정과 접근 권한을 포괄적으로 관리하는 체계이다. 지문의 '계정 관리 전반 및 프로비저닝'은 로그인뿐 아니라 **계정 생성과 권한 부여까지 관리**한다는 뜻이다.

공통 해설

IAM(Identity and Access Management)은 사용자의 신원 정보와 자원에 대한 접근 권한을 함께 관리하는 체계이다. 사용자가 누구인지 확인하는 인증, 어떤 자원을 사용할 수 있는지 정하는 권한 부여뿐 아니라 **계정의 생성·변경·폐기에 이르는 생애주기**를 관리한다.

지문의 '프로비저닝'은 사용자가 업무에 필요한 시스템을 이용할 수 있도록 계정을 만들고 적절한 권한을 설정하는 작업이다. 예를 들어 신규 직원에게 계정을 발급하고 담당 업무에 필요한 권한을 부여하는 것이 이에 해당한다. IAM은 이후의 직무 변경이나 퇴사에 따른 권한 변경·회수도 관리한다.

따라서 지문의 판단 기준은 특정 로그인 기능이나 암호키 관리가 아니라 **계정과 접근 권한을 포괄적으로 관리하는가**이다. 이 정의에 해당하는 명칭은 IAM이며, AWS IAM도 사용자·역할과 정책을 통해 AWS 자원에 대한 접근 권한을 관리한다.

NoteBase

문 17. Hyperledger Fabric에 대한 설명으로 가장 적절하지 않은 것은?

① PBFT 알고리즘을 사용하기 때문에 블록체인의 분기가 발생할 수 있다.

② 사용되는 체인코드는 Init, Invoke, Query의 3가지 처리를 구현한다.

③ 리눅스 기반의 Hyperledger Project는 분산 원장 기술의 정립을 목표로 한다.

④ 합의 알고리즘의 특성상 여러 컴퓨터가 있는 상태에서 일부 컴퓨터가 고장나거나 네트워크에 장애가 발생하더라도 정상적으로 작동하도록 설계되어 있다.

정답 1번

간단한 해설

PBFT는 허용 장애 범위 안에서 노드들이 같은 결과를 확정하도록 하여 **원장의 분기를 방지**하는 합의 방식이다. 이를 분기 발생의 원인으로 설명한 ①이 부적절하다.

선지별 해설

① (X) PBFT는 참여 노드들이 거래 순서와 처리 결과에 합의하여 **확정된 원장의 일관성**을 유지하도록 하는 합의 방식이다. 허용 장애 범위 등 합의의 전제가 충족되면 서로 충돌하는 블록을 각각 확정하지 않는다. 따라서 PBFT를 사용하기 때문에 작업증명 방식과 같은 일시적 분기가 발생한다는 설명은 부적절하다.

② (O) 초기 Fabric의 체인코드 인터페이스에서는 **Init·Invoke·Query**의 세 처리를 구분한다. Init는 초기 상태를 설정하고, Invoke는 거래 로직을 실행하여 상태를 변경할 수 있으며, Query는 상태를 바꾸지 않고 정보를 조회한다. 이 구형 인터페이스의 구분을 모든 후속 버전에 그대로 적용하는 것은 아니다.

③ (O) Hyperledger는 **리눅스 재단이 주도한 오픈소스 협력 프로젝트**로, 산업 분야에서 활용할 분산 원장 기술과 공통 기반을 발전시키는 것을 목표로 한다. Fabric은 그에 속한 허가형 블록체인 프레임워크이며, 단순히 가상화폐 하나를 개발하는 프로젝트와 구별된다.

④ (O) 여러 노드에 원장을 복제하고 합의를 수행함으로써 **일정 범위의 노드 고장과 통신 장애**를 견디도록 설계되어 있다. 다만 합의에 필요한 노드 수와 통신 조건이 유지되어야 거래 처리가 계속될 수 있다. 모든 노드가 고장 나거나 필요한 정족수가 통신할 수 없는 상황에서도 무조건 작동한다는 뜻은 아니다.

NoteBase

문 18. 재해복구 시스템에 대한 설명 중 옳은 것의 개수로 가장 적절한 것은?

가. 미러 사이트는 주센터와 재해복구센터 모두 액티브 상태로 실시간 동시 서비스하는 방식이다.
나. 핫 사이트는 주센터에 장애 발생 시 재해복구센터의 정보시스템을 액티브로 전환하여 서비스하는 방식이다.
다. 웜 사이트는 중요도가 높은 정보기술 자원만을 부분적으로 재해복구센터에 저장하는 방식이다.
라. RTO(Recovery Time Objective)는 재해 발생으로 서비스가 중단되었을 때, 서비스를 복구할 때까지 걸리는 최소 허용 시간이다.

① 1개
② 2개
③ 3개
④ 4개

정답 3번

간단한 해설

RTO는 서비스 중단 후 복구가 완료되어야 하는 **최대 허용 시간**을 정한 목표이다. 복구에 필요한 최소 시간을 뜻하지 않는다.

보기별 해설

가. O: 미러 사이트는 주센터와 재해복구센터를 **모두 액티브 상태로 운영**하여 실시간으로 서비스를 제공하는 방식이다. 한쪽에서 장애가 발생해도 다른 쪽이 서비스를 이어 갈 수 있도록 동일 수준의 운영 환경을 갖춘다.

나. O: 핫 사이트는 주센터와 유사한 운영 환경을 재해복구센터에 준비해 두되 평상시에는 대기시키는 방식이다. 주센터에 장애가 발생하면 **대기 센터를 액티브로 전환**하여 서비스를 제공한다. 양쪽이 동시에 서비스하는 미러 사이트와 구별된다.

다. O: 웜 사이트는 주센터의 모든 정보기술 자원을 동일하게 갖추기보다 **중요한 자원을 우선하여 부분적으로 확보**하는 방식이다. 재해 시 추가 자원 확보와 구성 작업이 필요할 수 있어 완전한 핫 사이트보다 복구에 시간이 더 걸릴 수 있다.

라. X: RTO는 재해로 서비스가 중단된 뒤 복구가 이루어져야 하는 목표시간으로, **허용 가능한 최대 복구시간**을 뜻한다. '최소 허용 시간'이 아니며, 정해진 RTO 이내에 서비스를 복구하도록 계획한다.

옳은 보기는 가·나·다의 3개이므로 ③과 일치한다.

NoteBase

문 19. SET(Secure Electronic Transaction)에 대한 설명으로 가장 적절하지 않은 것은?

① SET는 전자봉투와 이중서명(dual signature) 방식을 사용한다.

② 상점이 신용카드 사용자의 계좌번호와 같은 지불정보를 볼 수 없도록 암호화하였다.

③ SET의 구성은 신용카드 사용자, 상점, 지불게이트웨이, 신용카드 회사, 은행, 인증기관으로 구성된다.

④ 은행은 신용카드 사용자가 구매한 물건을 확인할 수 있으며 상점이 요구한 결제 대금이 정확한지 확인할 수 있다.

정답 4번

간단한 해설

SET는 **주문정보와 지불정보를 분리**하여 상점에는 카드 정보를, 은행에는 구체적인 구매 내역을 숨긴다. 은행이 결제를 검증할 수 있다는 사실이 구매한 물건까지 볼 수 있다는 뜻은 아니다.

선지별 해설

SET는 신용카드 기반 전자상거래의 인증과 정보 보호를 위한 프로토콜이다. 거래 당사자가 자신의 업무에 필요한 정보만 보면서 주문과 결제가 같은 거래에 속하는지 확인하도록 설계되었다.

① O: 전자봉투는 데이터를 대칭키로 암호화하고 그 키를 수신자의 공개키로 보호하는 방식이다. 이중서명은 주문정보와 지불정보의 해시를 결합하여 서명함으로써, **두 정보의 내용을 모두 공개하지 않고도 연결 관계를 검증**하게 한다.

② O: 카드번호 등 민감한 지불정보는 지불게이트웨이 측에서 처리할 수 있도록 암호화된다. 상점은 주문을 처리하고 암호화된 지불정보를 전달할 수 있지만, **그 지불정보의 평문을 읽지는 못하도록** 한다.

③ O: 카드 사용자는 구매와 지불을 요청하고 상점은 주문을 처리한다. 지불게이트웨이는 상점과 금융 결제망을 연결하며, 카드회사와 은행은 발급·승인·매입 등 결제 업무를 수행한다. 인증기관은 공개키 인증서를 발급하여 참여자 인증을 뒷받침한다.

④ X: 은행·지불게이트웨이에는 결제에 필요한 지불정보가 제공되지만, **구체적으로 어떤 물건을 샀는지는 공개되지 않는다**. 필요한 해시와 이중서명 등을 이용해 주문과 지불의 연결 및 결제금액의 일치 여부를 검증하는 것과 주문 상세를 직접 열람하는 것은 다르다.

NoteBase

문 20. 클라우드 서비스에 대한 설명 중 옳은 것의 개수로 가장 적절한 것은?

가. 기업이 직접 구축하고 운영하는 클라우드 환경을 온프레미스 환경이라고 한다.
나. IaaS 서비스는 제공되는 클라우드의 미들웨어를 이용해 소프트웨어 개발환경을 구성할 수 있다.
다. 여러 사용자가 자원을 공유하기 위해 가상영역으로 분리해주는 가상화 기술은 클라우드의 핵심기술이다.
라. 하이퍼바이저는 하나의 물리 서버에 여러 개의 가상 서버를 구동하는 가상화 엔진으로 리눅스의 하이퍼-V가 있다.

① 1개
② 2개
③ 3개
④ 4개

정답 2번

간단한 해설

미들웨어와 개발 도구까지 제공하는 서비스는 **PaaS**이며, IaaS는 서버·저장장치·네트워크 같은 기반 자원을 제공한다. 또한 Hyper-V는 리눅스의 기술이 아니라 **마이크로소프트의 가상화 기술**이다.

NoteBase

보기별 해설

가. O: 온프레미스는 기업이 **자체 시설에 IT 시스템을 구축하여 운영하는 방식**이다. 보기의 직접 구축·운영은 외부 클라우드 사업자의 기반 시설을 빌리는 방식과 대비되는 자체 구축 환경을 가리킨다. 다만 프라이빗 클라우드는 한 조직만 사용하는 배치 형태이므로, 외부 시설에서 운영될 수도 있어 온프레미스와 언제나 같은 뜻은 아니다.

나. X: 공급자가 미들웨어와 개발·실행 환경을 제공하고 이용자가 이를 바탕으로 응용프로그램을 개발하는 것은 **PaaS**의 특징이다. IaaS는 가상 서버·저장장치·네트워크 등의 기반 자원을 제공하고, 운영체제와 미들웨어의 설치·관리는 기본적으로 이용자가 담당한다. IaaS에서 개발 자체가 불가능한 것이 아니라 제공·관리되는 서비스 계층이 다르다.

다. O: 가상화는 물리적인 컴퓨팅 자원을 **서로 분리된 논리적 환경으로 나누어 공유**할 수 있게 한다. 하나의 물리 서버에 여러 가상 머신을 두고 자원을 배분하는 방식으로 자원 활용률과 유연성을 높이므로, 클라우드의 자원 풀링과 탄력적 제공을 뒷받침하는 핵심 기술이다.

라. X: 하이퍼바이저가 한 물리 서버에서 여러 가상 서버를 구동하게 하는 가상화 엔진이라는 설명은 맞다. 그러나 Hyper-V는 **마이크로소프트가 제공하는 Windows 계열의 가상화 기술**이다. Hyper-V의 가상 머신에서 리눅스를 실행할 수 있다는 사실과 Hyper-V 자체가 리눅스의 기술이라는 주장은 다르다.

따라서 옳은 보기는 가, 다의 2개이며, ②와 일치한다.

NoteBase

문 21. 유닉스에 대한 설명으로 가장 적절하지 않은 것은?

① 셸(shell)은 명령어를 해석하고 실행하는 도구이다.

② 슈퍼유저로 권한을 변경하기 위해서 su 명령어를 사용한다.

③ 응용 프로그램은 커널의 장치 드라이버를 사용하여 하드웨어를 직접적으로 제어한다.

④ 커널은 운영체제의 핵심으로 컴퓨터 자원을 효율적으로 관리하기 위한 방식을 지원한다.

정답 3번

간단한 해설

일반 응용 프로그램은 하드웨어를 직접 제어하는 것이 아니라 **시스템 호출로 커널에 처리를 요청**한다. 커널과 장치 드라이버가 필요한 장치 동작을 수행하므로 응용 프로그램의 하드웨어 접근은 간접적이다.

선지별 해설

① O: 셸은 사용자가 입력한 **명령어를 해석하는 인터페이스**이다. 내장 명령을 수행하거나 외부 프로그램을 실행하고, 입출력 방향 변경과 파이프 연결 같은 명령 실행 환경을 구성한다.

② O: su는 다른 사용자의 신원으로 셸을 실행하는 명령이다. 일반적으로 대상 사용자를 생략하면 root를 대상으로 하므로 **인증과 권한 조건을 충족하여 슈퍼유저로 전환**할 때 사용할 수 있다. 사용자 이름을 지정하면 root 이외의 계정으로도 전환할 수 있다.

③ X: 응용 프로그램이 커널의 장치 드라이버를 이용한다는 것은 하드웨어를 직접 제어한다는 뜻이 아니다. 일반 응용 프로그램은 **시스템 호출을 통해 커널에 입출력을 요청**하고, 실제 장치 제어는 커널과 장치 드라이버가 담당한다.

④ O: 커널은 운영체제의 핵심으로 프로세스 실행과 CPU 배분, 메모리, 파일, 입출력 장치 등의 자원을 관리한다. 여러 프로그램이 자원을 안전하고 효율적으로 이용하도록 **자원 배분과 보호를 수행**한다.

NoteBase

문 22. 접근 통제 단계에 대한 설명으로 가장 적절한 것은?

① 식별은 주체의 신원을 검증하기 위한 사용 증명 활동이다.

② 인증은 주체가 자신의 행동에 권한이 있다는 것을 보증하는 것이다.

③ 책임 추적성은 본인이 누구라는 것을 시스템에 밝히는 것이다.

④ 인가는 인증된 주체에게 접근을 허용하고 특정 업무를 수행할 권리를 부여하는 것이다.

정답 4번

간단한 해설

인증이 주장한 신원을 확인하는 절차라면, **인가는 확인된 주체가 무엇을 할 수 있는지 정하는 절차**이다. 접근 허용과 특정 업무 수행 권리의 부여는 인가에 해당한다.

선지별 해설

접근 통제에서는 식별, 인증, 인가를 구별하며, 수행된 행위를 특정 주체에게 연결할 수 있어야 책임 추적성도 확보할 수 있다. 신원 주장, 신원 검증, 권한 결정, 행위 추적은 서로 다른 기능이다.

① X: 신원을 검증하기 위해 증명 수단을 확인하는 활동은 **인증**이다. 식별은 사용자 ID 등을 제시하여 자신이 누구라고 주장하는 단계이며, 그 주장 자체가 참인지를 입증하지는 않는다.

② X: 주체의 행동에 필요한 권한이 있는지 판단하는 것은 **인가**에 해당한다. 인증은 비밀번호, 인증서 등의 증명 수단을 통해 주장된 신원을 확인하는 것이므로, 인증에 성공했다고 모든 작업이 허용되는 것은 아니다.

③ X: 본인이 누구라고 시스템에 밝히는 것은 **식별**이다. 책임 추적성은 누가 어떤 행위를 했는지 고유하게 연결하여 추적할 수 있는 성질이며, 고유 계정과 신뢰할 수 있는 감사 로그 등이 이를 뒷받침한다.

④ O: 인가는 인증된 주체에게 보안정책에 따른 접근 권한을 부여하고 해당 요청의 허용 여부를 결정하는 과정이다. 같은 시스템에 로그인한 사용자라도 역할에 따라 파일 읽기는 허용되고 수정은 금지될 수 있다.

NoteBase

문 23. 다음에서 설명하는 보안 모델로 가장 적절한 것은?

◯ 충돌을 야기하는 어떠한 정보의 흐름도 차단해야 한다는 모델로 이익 충돌 회피를 위한 모델이다.
◯ 직무 분리를 접근 통제에 반영한 개념이 적용되며 자유재량과 강제적 접근 제어 개념을 모두 이용한다.

① 벨-라파듈라 모델
② 비바 모델
③ 클락-윌슨 모델
④ 만리장성 모델

정답 4번

간단한 해설

만리장성 모델은 **경쟁 관계에서 생기는 이익 충돌**을 막기 위해 정보 접근을 제한한다. 한 회사의 비밀정보에 접근한 사용자가 경쟁 회사의 비밀정보에도 접근하지 못하도록 통제한다.

공통 해설

만리장성 모델은 경쟁 관계에 있는 조직 사이에서 비밀정보가 흘러 이익 충돌이 생기는 것을 막는 접근 통제 모델이다. 접근 가능 여부는 **사용자가 이전에 어느 조직의 정보에 접근했는지**에 따라 달라진다.

예를 들어 경쟁사 A와 B가 같은 이익 충돌 집합에 속한다면, A의 비밀정보를 열람한 담당자는 B의 비밀정보에 접근할 수 없다. 서로 충돌하는 고객의 정보를 한 사람이 함께 취급하지 못하게 하는 것으로, 지문의 직무 분리는 이러한 업무와 정보 접근의 분리를 뜻한다.

처음에는 충돌 회피 조건 안에서 접근할 대상을 선택할 재량이 있지만, 선택 이후에는 경쟁 대상의 정보 접근을 정책으로 강제 차단한다. 이처럼 **재량적 선택과 강제적 제한을 결합**한다는 설명도 만리장성 모델에 부합한다.

NoteBase

문 24. 국제 표준 및 인증체계에 대한 설명으로 가장 적절한 것은?

① ITSEC는 시스템의 안전성을 향상시키기 위하여 취할 수 있는 사항을 등급으로 구분하고 단일 기준으로 정보보호 제품을 평가하는 표준안이다.

② TCSEC의 B1 레벨은 모듈별 분석과 테스트를 할 수 있는 단계로 운영체제 내부 보안에 불필요한 부분이 모두 제거되어야 한다.

③ TCSEC의 C2 레벨은 통제된 접근 보호로 각 사용자의 작업 내용을 기록하고 감사할 수 있는 기능을 제공하는 UNIX, VMS, AOS, NOS 시스템 등이 있다.

④ ITSEC의 E1 레벨은 시스템에 정형화된 보안 정책이 존재하며 E2 등급의 기능을 모두 포함한 소스코드를 제공해야 한다.

정답 3번

간단한 해설

TCSEC의 C2는 사용자별 접근을 통제하고 **보안 관련 행위의 기록·감사로 개인별 책임을 확인**하는 수준이다. 따라서 ③이 적절하다.

선지별 해설

① (X) ITSEC는 **보안 기능과 보증 수준을 분리**하여 평가한다. 어떤 보안 기능을 제공하는지와 그 기능이 올바르고 효과적으로 구현되었음을 얼마나 신뢰할 수 있는지를 구별한다. 보안 기능과 보증 요건을 하나의 등급 체계에 결합한 TCSEC의 평가 방식과 혼동한 설명이다.

② (X) 보안 정책 집행에 불필요한 코드를 신뢰컴퓨팅기반(TCB)에서 제외하고, 분석·시험이 가능하도록 복잡성을 줄이는 것은 **B3의 보안 영역** 수준에 해당한다. B1은 C2의 요건에 보안 레이블과 강제적 접근통제 등을 추가한 '레이블된 보안 보호' 수준이다.

③ (O) C2는 **통제된 접근 보호** 수준으로, 사용자별 식별·인증과 세분화된 임의적 접근통제, 보안 관련 행위의 감사 기록 등을 요구한다. 누가 어떤 보안 관련 작업을 했는지 추적하여 개인별 책임을 확인할 수 있어야 한다. 제시된 운영체제 이름은 이러한 기능을 갖춘 구현의 예로 이해하며, 모든 버전과 구성이 자동으로 C2 인증을 받는다는 뜻은 아니다.

④ (X) E1에서는 보안목표, 비정형적인 구조 설계 설명과 기능시험 등이 요구된다. **E2의 요건에 소스코드 등의 평가를 추가하는 수준은 E3**이며, 정형적 보안정책 모델은 E4에서 추가로 요구된다. 낮은 E1이 E2의 요건을 모두 포함하고 소스코드를 요구한다는 설명은 등급의 관계를 잘못 설명한 것이다.

NoteBase

문 25. 국제 공통평가(Common Criteria) 기준에 대한 설명으로 가장 적절한 것은?

① Part 2는 TOE를 위한 보증 요구사항을 표현하는 표준화된 방법으로 보증컴포넌트 세트를 포함하고 있다.

② 구성요소 중 패키지는 정보제품이 갖춰야 할 공통적인 보안 요구사항들을 모아 놓은 것으로 EAL과 기능 및 보증 요구 컴포넌트 등의 집합으로 구성된다.

③ 정보보호 제품의 평가 기준을 규정한 국제표준으로 국제사회 내에 널리 사용되는 IT 보안의 평가 기준이다.

④ 보안 등급과 보안 기능에 대한 등급을 가지고 있어 국제표준 ISO 27001로 지정된 최초의 정보기술 보안에 관한 것이다.

정답 3번

간단한 해설

국제 공통평가기준(CC)은 **IT 제품과 시스템의 보안성을 평가하는 공통 기준**이며 ISO/IEC 15408 계열과 연결된다. 보안 기능에 대한 요구사항과 그 기능을 신뢰할 근거인 보증 요구사항을 구분한다.

선지별 해설

CC는 평가대상인 TOE가 어떤 보안 기능을 제공해야 하며, 그 기능이 적절히 구현되었다고 어느 정도 신뢰할 수 있는지를 평가하는 체계이다. 기능 요구사항과 보증 요구사항은 목적이 다르다.

① X: **Part 2는 보안 기능 요구사항**을 표현하기 위한 기능 컴포넌트를 다룬다. TOE에 대한 보증 요구사항과 보증 컴포넌트는 Part 3의 내용이다. 선지는 기능 요구사항과 보증 요구사항의 위치를 바꾸었다.

② X: 패키지는 함께 사용하기에 적합한 보안 컴포넌트 또는 요구사항에 이름을 붙인 재사용 가능한 묶음이다. **기능 패키지와 보증 패키지를 구별**하며, 한 패키지에 기능·보증 요구사항을 섞어 정의하지 않는다. EAL은 패키지에 별도 요소로 덧붙이는 대상이 아니라, 미리 정의된 보증 패키지의 한 종류이다.

③ O: CC는 IT 제품과 시스템의 보안 요구사항을 일관되게 명시하고 평가할 수 있도록 마련된 국제적인 공통 기준이다. 서로 다른 제품의 보안 기능과 보증에 대해 공통된 평가 틀을 제공하므로 국제적으로 활용된다.

④ X: CC에 대응하는 국제표준은 **ISO/IEC 15408**이다. ISO/IEC 27001은 조직의 정보보호 관리체계인 ISMS의 요구사항을 규정한 표준으로, IT 제품의 보안 기능을 평가하는 CC와 평가 대상과 목적이 다르다.

NoteBase

문 26. 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 중 제14조의 설명으로 가장 적절하지 않은 것은?

① 과학기술정보통신부장관은 클라우드컴퓨팅에 관한 전문인력을 양성하기 위하여 필요한 정책을 수립하고 추진할 수 있다.

② 클라우드컴퓨팅 관련 교육훈련 지정기관이 정당한 사유없이 지정일로부터 1년 이상 교육실적이 없는 경우 그 지정을 2년 이내 취소할 수 있다.

③ 클라우드컴퓨팅 전문인력 양성을 위해 필요한 정책의 수립이나 교육기관의 지정요건 및 지정취소 절차와 지원 내용 등 필요한 사항은 대통령령으로 정한다.

④ 클라우드컴퓨팅 관련 교육훈련을 실시하는 교육기관 중 지정요건을 갖춘 기관에 필요한 경비의 전부를 지원할 수 있다.

정답 2번

①

과학기술정보통신부장관은 클라우드컴퓨팅 전문인력 양성에 필요한 **정책을 수립하고 추진할 수 있다**.

클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제14조(전문인력의 양성)
① 과학기술정보통신부장관은 클라우드컴퓨팅에 관한 전문인력을 양성하기 위하여 필요한 정책을 수립하고 추진할 수 있다. <개정 2017.7.26>

②

과학기술정보통신부장관은 **정당한 사유 없이 지정일부터 1년 이상 교육 실적이 없는 기관의 지정을 취소할 수 있다**. 취소 시기를 '2년 이내'로 제한하는 규정은 없다.

클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제14조(전문인력의 양성)
③ 과학기술정보통신부장관은 제2항에 따라 지정한 교육기관이 다음 각 호의 어느 하나에 해당하는 경우 그 지정을 취소할 수 있다. 다만 제1호에 해당하는 경우에는 그 지정을 취소하여야 한다. <개정 2017.7.26, 2025.1.31>
3. 정당한 사유 없이 교육기관 지정일부터 1년 이상 교육 실적이 없는 경우

NoteBase

③

전문인력 양성 정책의 수립, 교육기관의 지정 요건과 지정·지정취소 절차, 지원 내용 등에 필요한 사항은 **대통령령으로 정한다**.

클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제14조(전문인력의 양성)
④ 제1항부터 제3항까지에 따른 정책의 수립, 교육기관의 지정 요건, 지정 및 지정 취소 절차와 지원 내용 등에 필요한 사항은 대통령령으로 정한다.

④

과학기술정보통신부장관은 요건을 갖춘 교육기관을 지정하여 **필요한 경비의 전부 또는 일부를 지원할 수 있다**. 전액 지원도 허용된다.

클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제14조(전문인력의 양성)
② 과학기술정보통신부장관은 클라우드컴퓨팅 관련 교육훈련을 실시하는 교육기관 중 대통령령으로 정하는 요건을 갖춘 기관을 지정하여 필요한 경비의 전부 또는 일부를 지원할 수 있다. <개정 2017.7.26>

NoteBase

문 27. KECCAK에 대한 설명으로 옳은 것만을 모두 고른 것으로 가장 적절한 것은?

가. SHA-3으로 선정된 일방향 해시 함수 알고리즘이다.
나. 입력되는 데이터의 크기는 $2^{64} - 1$로 제한된다.
다. 흡수 단계와 추출 단계라는 두 개의 상태를 갖는 스펀지 구조가 사용된다.

① 가, 나
② 가, 다
③ 나, 다
④ 가, 나, 다

정답 2번

간단한 해설

KECCAK은 SHA-3의 기반으로 선정된 스펀지 방식 해시 알고리즘이며 **흡수와 추출 단계**를 사용한다. 입력은 임의 길이로 정의되므로 특정 64비트 길이 상한을 그대로 적용하지 않는다.

보기별 해설

가. O: KECCAK은 NIST의 SHA-3 공모에서 선정된 해시 알고리즘이며 SHA-3 표준의 기반이 되었다. 해시값으로부터 입력을 구하기 어렵도록 하는 **일방향 해시 함수**를 구성한다.

나. X: KECCAK과 SHA-3는 **임의 길이의 입력 메시지**를 처리하도록 정의된다. 입력 길이를 $2^{64} - 1$로 제한한다는 설명은 맞지 않는다. 실제 프로그램의 메모리나 인터페이스 한계와 알고리즘이 정한 메시지 길이 범위는 구별한다.

다. O: 스펀지 구조는 입력 블록을 내부 상태에 결합하는 **흡수 단계**와, 그 상태에서 필요한 출력 비트를 얻는 **추출 단계**로 이루어진다. 각 단계에서 내부 순열을 반복 적용하여 입력을 처리하고 출력을 생성한다.

따라서 옳은 보기는 가·다이며, 이 조합은 ②와 일치한다.

NoteBase

문 28. PBE(Password Based Encryption)에 대한 설명으로 가장 적절하지 않은 것은?

① PBE는 암호화와 복호화에서 같은 패스워드를 사용한다.

② 사용자가 입력한 패스워드를 이중 암호화하여 KEK를 생성한다.

③ 의사난수 발생기를 사용해서 세션 키를 생성하고, KEK로 세션 키를 암호화한다.

④ PBE의 복호화는 KEK 복원, 세션 키 복호화, 메시지 복호화로 이루어진다.

정답 2번

간단한 해설

KEK는 패스워드를 두 번 암호화해서 만드는 키가 아니라, 패스워드와 솔트 등에 **키 유도 함수**를 적용해 만드는 키이다. KEK는 메시지 자체보다 **메시지 암호화용 세션 키를 보호**하는 데 사용된다.

선지별 해설

① O: PBE는 패스워드를 바탕으로 암호키를 유도하는 방식이다. 복호화할 때도 **암호화 때와 같은 패스워드**를 사용하고, 동일한 솔트와 키 유도 조건을 적용해야 같은 키를 재생성할 수 있다. 패스워드를 그대로 암호 알고리즘의 키로 사용하는 것과는 구별된다.

② X: KEK는 '키 암호화 키'로, 다른 암호키를 암호화하여 보호하는 키이다. 패스워드에 솔트와 반복 횟수 등을 결합하여 **키 유도 함수로 KEK를 생성**한다. 예를 들어 PBKDF2는 의사난수 함수를 반복 적용한다. 이는 패스워드를 이중 암호화한다는 설명과 다르므로, 가장 적절하지 않은 진술은 ②이다.

③ O: 이 문항의 키 분리 구조에서는 암호학적으로 안전한 의사난수 발생기로 메시지 암호화에 쓸 세션 키를 생성한다. **세션 키는 메시지를 암호화하고, KEK는 세션 키를 암호화**한다. 이렇게 데이터 암호화용 키와 그 키를 보호하는 키의 역할을 분리한다.

④ O: 먼저 같은 패스워드와 저장된 솔트·키 유도 조건으로 KEK를 다시 만든다. 그 KEK로 암호화된 세션 키를 복호화한 다음, 복원한 세션 키로 메시지를 복호화한다. **KEK 재생성 → 세션 키 복호화 → 메시지 복호화**의 의존 관계이며, 여기서 KEK 복원은 패스워드를 역으로 알아내는 과정이 아니다.

NoteBase

문 29. 위험분석(Risk Analysis)에 대한 설명으로 가장 적절한 것은?

① 베이스라인 접근법은 모든 시스템에 대해 표준화된 정보보호 대책 세트를 제공하기 때문에 분석 비용과 시간이 절약된다.

② 상세분석 접근법은 전문가의 지식과 경험을 사용해 위험분석을 수행하는 방법으로 소규모 조직에 적합하다.

③ 비정형 접근법은 자산의 가치, 위협, 취약점을 구체적으로 분석하는 방법으로 분석 비용과 시간이 많이 소요된다.

④ 복합 접근법은 베이스라인 접근법과 상세분석 접근법을 조합해 분석하는 방법으로 고위험 영역의 경우 베이스라인 접근법을 수행하고, 그 외의 다른 영역은 상세분석 접근법을 사용한다.

정답 1번

간단한 해설

베이스라인 접근법은 표준화된 기본 보호대책을 활용하여 **위험분석에 드는 시간과 비용을 절약**한다. 따라서 ①이 적절하다.

선지별 해설

① (O) 베이스라인 접근법은 표준이나 지침에 제시된 **공통의 기본 보호대책**을 적용하는 방법이다. 시스템마다 자산·위협·취약점을 처음부터 상세히 분석하지 않아도 되므로 시간과 비용을 줄일 수 있다. 다만 개별 시스템의 특수한 위험까지 충분히 반영하지 못할 수 있다.

② (X) 전문가의 지식과 경험을 활용하여 비교적 간편하게 위험을 판단하는 것은 **비정형 접근법**이다. 자원이 적은 소규모 조직에서 활용하기 쉽지만, 분석자의 역량과 주관에 결과가 좌우될 수 있다. 상세분석 접근법은 자산·위협·취약점을 체계적으로 조사하는 방법이다.

③ (X) 자산의 가치와 위협·취약점을 구체적으로 분석하여 많은 시간과 비용이 필요한 것은 **상세분석 접근법**이다. 조직과 시스템의 특성에 맞는 보호대책을 도출할 수 있다는 장점이 있다. 비정형 접근법은 이와 달리 전문가의 경험과 판단에 크게 의존한다.

④ (X) 복합 접근법은 분석 자원을 집중할 영역을 먼저 가려낸 뒤 **고위험·핵심 영역에는 상세분석**을 적용하고, 그 밖의 영역에는 베이스라인 접근법을 적용한다. 선지는 두 방법의 적용 대상을 반대로 설명했다. 모든 영역에 같은 수준의 상세분석을 수행하지 않아 비용과 필요한 보호 수준의 균형을 맞출 수 있다.

NoteBase

문 30. 다음에서 설명하는 의사난수 생성 방법으로 가장 적절한 것은?

◯ 현재 의사난수의 값을 A배하고 C를 더한 다음, M으로 나눈 나머지를 다음 의사난수로 하는 방법이다.
◯ 최초 의사난수 R_0=(A× 종자+C)modM
◯ R_1=(A× R_0+C)modM
◯ R_n+1=(A× R_n+C)modM

① 선형 합동법
② 무작위 방법
③ 암호를 사용하는 방법
④ ANSI X9.17

정답 1번

간단한 해설

현재 값에 일정한 수를 곱하고 상수를 더한 뒤, 일정한 수로 나눈 **나머지를 다음 값으로 삼는** 점화식은 **선형 합동법**의 특징이다.

공통 해설

선형 합동법은 R_n+1=(A· R_n+C) M의 규칙으로 의사난수를 생성한다. A는 곱하는 상수, C는 더하는 상수, M은 나머지를 구할 때의 나누는 수이다. 현재 값에 대한 곱셈과 덧셈이 '선형'에, **M으로 나눈 나머지를 취하는 연산**이 '합동'에 해당한다. 지문에 제시된 점화식이 바로 이 생성 규칙이다.

지문에서는 시작값인 종자에 같은 연산을 적용하여 최초 값 R_0을 구하고, 이를 다시 입력하여 R_1을 구한다. 이후에도 직전 값을 입력으로 사용한다. **상수와 종자가 같으면 같은 수열이 생성**되므로, 매번 독립적으로 값을 뽑는 것이 아니라 정해진 규칙으로 난수처럼 보이는 수열을 만드는 방법이다.

NoteBase

문 31. 다음에서 설명하는 블록 암호 모드로 가장 적절한 것은?

◯ 평문 블록을 암호화한 것이 그대로 암호문 블록이 되며, 마지막 평문 블록이 블록 길이에 미치지 못하면 패딩(padding)을 추가하여 블록 길이를 맞춘다.
◯ 이 모드에서는 초기화 벡터가 필요하지 않으며, 재전송 공격이 가능하다.

① CBC(Cipher Block Chaining)
② CFB(Cipher FeedBack)
③ ECB(Electric CodeBook)
④ OFB(Output FeedBack)

정답 3번

간단한 해설

ECB는 각 평문 블록을 **독립적으로 암호화**하여 그 결과를 그대로 암호문 블록으로 사용한다. 이전 블록의 처리 결과를 연결하지 않으므로 **초기화 벡터가 필요하지 않다**.

공통 해설

ECB는 같은 키로 각 평문 블록을 독립적으로 암호화하는 모드이다. 각 블록의 암호화 결과가 그대로 해당 암호문 블록이 되며, 이전 블록의 암호문이나 별도의 초기값을 섞지 않는다. 따라서 **초기화 벡터 없이** 암호화할 수 있다. CBC·CFB·OFB는 모두 초기화 벡터를 사용하므로, 제시된 조건을 충족하는 모드는 ECB이다.

블록 암호는 정해진 길이의 블록을 입력받으므로, ECB에서 마지막 평문 블록의 길이가 부족하면 패딩을 덧붙여 완전한 블록으로 만든다. 패딩은 **부족한 블록 길이를 채우는 처리**이며, 암호화 시작에 사용하는 초기화 벡터와는 역할이 다르다.

같은 키를 사용하는 ECB에서는 동일한 평문 블록이 항상 동일한 암호문 블록으로 바뀌고, 동일한 암호문 블록도 항상 동일한 평문 블록으로 복호화된다. 따라서 공격자가 이전 암호문을 다시 보내도 ECB 자체는 그것이 과거에 사용된 암호문인지 구별하지 못한다. 수신 측에 **중복 수신이나 메시지의 최신성을 확인하는 별도 장치가 없으면** 재전송 공격이 가능하다. 다만 재전송 방지 기능이 없다는 사실만으로 ECB를 특정하는 것은 아니며, 이 문항에서는 블록별 독립 처리와 초기화 벡터 불필요라는 조건이 함께 ECB를 가리킨다.

NoteBase

문 32. 암호 기술에 대한 설명으로 옳은 것만을 모두 고른 것으로 가장 적절한 것은?

가. Diffie-Hellman 키 교환 방법은 중간자 공격에 취약하다.
나. 메시지 인증 코드는 메시지 무결성과 사용자 인증을 제공한다.
다. 일방향 해시 함수를 통해서 문서의 기밀성을 보장할 수 있다.

① 가, 나
② 가, 다
③ 나, 다
④ 가, 나, 다

정답 1번

간단한 해설

인증 없는 Diffie-Hellman은 상대방을 확인하지 못해 중간자 공격에 취약하고, MAC는 무결성과 송신 출처 인증을 제공한다. 반면 해시만으로는 기밀성을 보장하지 못하므로 **가·나를 고른** ①이 정답이다.

보기별 해설

가. O: 기본 Diffie-Hellman 키 교환에는 **상대방의 신원을 확인하는 인증 기능이 없다**. 공격자가 양쪽 사이에서 교환값을 바꿔 전달하면 각 당사자와 별도의 공유 키를 만들 수 있으므로 중간자 공격에 취약하다. 전자서명이나 인증서 등으로 키 교환의 상대방을 인증하면 이러한 공격에 대응할 수 있다.

나. O: 메시지 인증 코드(MAC)는 공유 비밀 키와 메시지로 계산한 인증값을 검증하여 **메시지 무결성과 송신 출처의 인증**을 제공한다. 여기서 사용자 인증은 해당 비밀 키를 아는 당사자가 메시지를 만들었다는 의미이다. 송신자와 수신자가 같은 키를 공유하므로 제3자에게 특정 송신자의 작성 사실을 증명하는 부인방지 기능과는 다르다.

다. X: 일방향 해시 함수는 문서로부터 해시값을 생성할 뿐, **문서 자체를 암호화하지 않는다**. 신뢰할 수 있는 원래 해시값과 비교하면 문서의 변경 여부를 확인하는 데 활용할 수 있지만, 해시 함수만으로 문서의 열람을 막아 기밀성을 보장할 수는 없다.

따라서 옳은 보기는 가와 나이며, 이를 묶은 선택지는 ①이다.

NoteBase

문 33. DES 구조인 페이스텔 네트워크의 1라운드 순서로 가장 적절한 것은?

가. 라운드의 입력을 L과 R로 나눈다.
나. 라운드 함수 F는 R과 서브키 K_1을 입력으로 사용하여 랜덤하게 보이는 비트열을 계산한다.
다. R을 그대로 R로 보낸다.
라. R을 라운드 함수 F로 보낸다.
마. 얻어진 비트열과 L을 XOR 한다. 그 결과를 다음 라운드의 L로 사용한다.

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

정답 3번

간단한 해설

R을 라운드 함수에 입력해 **F의 출력 비트열을 먼저 구한 뒤**, 그 결과를 L과 XOR해야 한다. R은 함수 계산에 사용되는 동시에 원래 값이 별도 경로로 전달된다.

NoteBase

올바른 순서

가 → 다 → 라 → 나 → 마

가. DES의 라운드 입력 64비트를 L과 R이라는 두 32비트 블록으로 나눈다. 이후 R은 라운드 함수의 입력으로 사용하고, L은 함수의 출력과 XOR하는 데 사용한다.

다. R의 원래 값을 함수 계산과 별도의 경로로 그대로 전달한다. 이는 R을 함수에 입력하는 동안에도 **원래 R을 보존**하는 경로이다. 이 전달과 라의 함수 입력은 같은 R에서 갈라지는 두 경로이므로, 둘 사이에 계산 결과를 기다려야 하는 의존 관계는 없다.

라. R을 라운드 함수 F의 입력으로 보낸다. 함수가 R과 서브키를 이용해 비트열을 계산하려면 **먼저 R이 입력**되어야 하므로 나보다 앞선다.

나. F가 R과 첫 라운드의 서브키 K_1을 이용해 32비트 출력 비트열을 계산한다. 여기서 랜덤하게 보인다는 것은 매번 임의의 값을 생성한다는 뜻이 아니라, **같은 R과 서브키에는 같은 출력**이 정해진다는 전제에서 출력이 복잡하게 섞여 보인다는 뜻이다. 이 출력이 있어야 마의 XOR을 수행할 수 있다.

마. F의 출력 비트열을 L과 비트별 XOR한다. XOR은 대응하는 두 비트가 다르면 1, 같으면 0을 만드는 연산이다. 다만 보기의 출력 반쪽 명칭은 표준 DES와 다르다. 표준 DES에서는 **그대로 전달한 R이 다음 라운드의 L**이 되고, **L과 F의 출력을 XOR한 결과가 다음 라운드의 R**이 된다. 보기의 다와 마에 적힌 출력 명칭을 표준 DES의 관계로 외우지 않도록 구별해야 한다.

NoteBase

문 34. 정보보안 위험관리(Risk Management)에 대한 설명으로 가장 적절하지 않은 것은?

① 자산에 대한 위협을 분석하고 해석하여 자산의 취약점을 식별하는 과정이다.

② 조직 내 주요한 자산의 가치 및 민감도를 측정하고 이에 대한 위협을 분석하는 것이다.

③ 위협과 취약성을 분석해 비용 대비 적절한 보호 대책을 마련함으로 위험을 감수할 수 있는 수준을 유지하는 과정이다.

④ 보호대상, 위협요소, 취약점 등의 위험관리를 위해 순위결정법, 시나리오 기법 등 정량적 분석 기법을 이용한다.

정답 4번

간단한 해설

순위결정법과 시나리오 기법은 위험의 상대적 크기나 예상 상황을 판단하는 **정성적 분석 기법**으로 분류한다. 손실액·발생 빈도 등을 수치화하여 위험을 계산하는 **정량적 분석**과 구별된다.

선지별 해설

① O: 위험관리에는 자산에 어떤 위협이 존재하고, 그 위협이 악용할 수 있는 취약점이 무엇인지 파악하는 과정이 포함된다. 위협은 손해를 일으킬 수 있는 원인이나 사건이고, **취약점은 위협에 이용될 수 있는 약점**이다. 두 요소의 관계를 분석해야 자산이 노출된 위험을 평가할 수 있다.

② O: 자산의 가치와 민감도를 평가하면 자산 훼손·유출·서비스 중단이 조직에 미칠 영향을 판단할 수 있다. 이를 바탕으로 해당 자산에 대한 위협을 분석하여 **보호 우선순위와 필요한 보호 수준**을 정한다. 자산평가와 위협분석은 위험관리의 기초가 되는 활동이다.

③ O: 위험관리는 위협·취약성과 예상 피해를 평가한 뒤 비용과 효과를 고려하여 적절한 보호 대책을 선택하고, 남은 위험을 조직이 수용할 수 있는 수준으로 관리하는 과정이다. 목표는 **모든 위험을 무조건 제거하는 것이 아니라 수용 가능한 수준으로 통제**하는 데 있으며, 대책 적용 후에도 잔여 위험을 점검한다.

④ X: 순위결정법은 상대적 중요도나 위험 수준에 따라 우선순위를 정하고, 시나리오 기법은 예상되는 위협 상황과 영향을 검토한다. 이 문항에서 두 기법은 **정성적 분석**에 해당하므로 '정량적'이라는 분류가 잘못이다. 정량적 분석은 손실액과 발생 확률·빈도 등 의미 있는 수치를 이용하여 예상 손실을 평가하는 방식이다.

NoteBase

문 36. 「지능정보화 기본법」 제2조의 '정의'에서 지능정보 기술에 대한 설명으로 가장 적절하지 않은 것은?

① 전자적 방법으로 학습·추론·판단 등을 구현하는 기술이다.
② 정보를 생산·유통·활용해 사회 각 분야를 활동할 수 있게 하거나 활동의 효율화를 이끌어 내는 것이다.
③ 문자, 음성 및 영상 데이터 등을 전자적 방법으로 수집·분석·가공 처리하는 기술이다.
④ 무선 또는 유·무선이 결합된 초연결지능정보통신 기반 기술이다.

정답 2번

①

전자적 방법으로 **학습·추론·판단 등을 구현하는 기술**은 지능정보기술에 해당한다.

지능정보화 기본법 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.
4. "지능정보기술" 이란 다음 각 목의 어느 하나에 해당하는 기술 또는 그 결합 및 활용 기술을 말한다.
가. 전자적 방법으로 학습 · 추론 · 판단 등을 구현하는 기술

②

정보를 생산·유통·활용하여 사회 각 분야의 활동을 가능하게 하거나 효율화하는 것은 **'정보화'의 정의**이며,
지능정보기술의 정의가 아니다.

지능정보화 기본법 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.
2. "정보화"란 정보를 생산 · 유통 또는 활용하여 사회 각 분야의 활동을 가능하게 하거나 그러한 활동의 효율화를 도모하는 것을 말한다.

③

문자·음성·영상 등의 데이터를 **전자적으로 수집·분석·가공하는 기술**은 지능정보기술에 포함된다.

지능정보화 기본법 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.
4. "지능정보기술" 이란 다음 각 목의 어느 하나에 해당하는 기술 또는 그 결합 및 활용 기술을 말한다.
나. 데이터(부호, 문자, 음성, 음향 및 영상 등으로 표현된 모든 종류의 자료 또는 지식을 말한다)를 전자적 방법으로 수집 · 분석 · 가공 등 처리하는 기술

NoteBase

④

지능정보기술에는 **무선 또는 유·무선이 결합된 초연결지능정보통신기반 기술**이 포함된다.

지능정보화 기본법 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.
4. "지능정보기술" 이란 다음 각 목의 어느 하나에 해당하는 기술 또는 그 결합 및 활용 기술을 말한다.
마. 무선 또는 유 · 무선이 결합된 초연결지능정보통신기반 기술

NoteBase

문 37. 「개인정보보호법」 제3조 '개인정보 보호 원칙'에 대한 설명으로 가장 적절하지 않은 것은?

① 개인정보처리자는 개인정보의 처리 목적을 달성하기 위해서 모든 개인정보를 익명처리하여 수집해야 한다.

② 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 최소한의 개인정보를 수집, 생성 및 신뢰성을 보장해야 한다.

③ 개인정보처리자는 제30조에 따른 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하고 정보주체의 권리를 보장해야 한다.

④ 개인정보처리자는 개인정보의 처리 목적을 명확하게 하고 개인정보 수집은 적법하고 정당하게 수집해야 한다.

정답 1번

①

익명 또는 가명으로도 수집목적을 달성할 수 있는 경우, **익명처리가 가능하면 익명으로, 익명처리로 목적을 달성할 수 없으면 가명으로** 처리해야 한다. 모든 개인정보를 반드시 익명처리하여 수집해야 하는 것은 아니다.

개인정보 보호법 제3조(개인정보 보호 원칙)
⑦ 개인정보처리자는 개인정보를 익명 또는 가명으로 처리하여도 개인정보 수집목적을 달성할 수 있는 경우 익명처리가 가능한 경우에는 익명에 의하여, 익명처리로 목적을 달성할 수 없는 경우에는 가명에 의하여 처리될 수 있도록 하여야 한다. <개정 2020.2.4>

②

개인정보의 수집·생성 등 처리는 **목적에 필요한 범위로 제한**해야 하며, 최소한의 개인정보를 수집해야 한다. 정보의 신뢰성을 확보하도록 **정확성·완전성·최신성**을 보장해야 한다.

개인정보 보호법 제3조(개인정보 보호 원칙)
① 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.
② 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.
③ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.

NoteBase

③

개인정보처리자는 **개인정보 처리방침 등 처리에 관한 사항을 공개**하고, **열람청구권 등 정보주체의 권리를 보장**해야 한다.

개인정보 보호법 제3조(개인정보 보호 원칙)
⑤ 개인정보처리자는 제30조에 따른 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리를 보장하여야 한다. <개정 2023.3.14>

④

개인정보처리자는 **처리 목적을 명확히** 하고, 그 목적에 필요한 **최소한의 개인정보만 적법하고 정당하게 수집**해야 한다.

개인정보 보호법 제3조(개인정보 보호 원칙)
① 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.

NoteBase

문 38. 「개인정보보호법 시행령」의 정보주체로부터 동의를 받아 수집된 개인정보를 정보주체의 별도 동의 없이 추가적으로 이용·제공할 수 있는 경우에 대한 설명으로 가장 적절하지 않은 것은?

① 수집된 개인정보 이용 시 정보주체의 이익이 부당하게 침해되지 않을 때는 개인정보의 안전성을 확보한 상태에서 추가로 이용될 수 있다.

② 개인정보 수집 시 가명처리나 암호화 등 안전성이 확보된 개인정보는 개인정보 처리방침에 따라 기간 내 제공이 될 수 있다.

③ 수집된 개인정보가 당초 수집 목적과 합리적으로 관련된 범위에서는 개인정보 처리방침에 따라 추가로 이용할 수 있다.

④ 개인정보를 수집한 정황 또는 처리 관행에 비추어볼 때 개인정보의 추가적인 이용 또는 제공에 대한 예측이 가능했다면 별도 조치없이 제3자에게 정보를 제공할 수 있다.

정답 4번

①

별도 동의 없는 추가 이용은 당초 수집 목적과 합리적으로 관련된 범위에서 허용된다. 이때 **정보주체의 이익 침해 여부와 가명처리·암호화 등 안전조치 여부**를 고려하므로, 부당한 침해 없이 안전성을 확보하여 이용할 수 있다.

개인정보 보호법 제15조(개인정보의 수집 · 이용)
③ 개인정보처리자는 당초 수집 목적과 합리적으로 관련된 범위에서 정보주체에게 불이익이 발생하는지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 대통령령으로 정하는 바에 따라 정보주체의 동의 없이 개인정보를 이용할 수 있다. <신설 2020.2.4>

개인정보 보호법 시행령 제14조의2(개인정보의 추가적인 이용 · 제공의 기준 등)
① 개인정보처리자는 법 제15조제3항 또는 제17조제4항에 따라 정보주체의 동의 없이 개인정보를 이용 또는 제공(이하 "개인정보의 추가적인 이용 또는 제공"이라 한다)하려는 경우에는 다음 각 호의 사항을 고려해야 한다.
3. 정보주체의 이익을 부당하게 침해하는지 여부
4. 가명처리 또는 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부

NoteBase

②

추가 제공 여부를 판단할 때는 **가명처리·암호화 등 안전성 확보조치**를 고려한다. 수집 목적과 합리적으로 관련된 범위에서 제공할 수 있으며, 지속적으로 제공하면 **판단기준을 처리방침에 공개하고 그 준수 여부를 점검**해야 한다. 보유기간 경과 등으로 불필요해진 정보는 법령상 보존 사유가 없으면 지체 없이 파기한다.

개인정보 보호법 제17조(개인정보의 제공)
④ 개인정보처리자는 당초 수집 목적과 합리적으로 관련된 범위에서 정보주체에게 불이익이 발생하는지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 대통령령으로 정하는 바에 따라 정보주체의 동의 없이 개인정보를 제공할 수 있다. <신설 2020.2.4>

개인정보 보호법 제21조(개인정보의 파기)
① 개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성, 가명정보의 처리 기간 경과 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다. <개정 2023.3.14>

개인정보 보호법 시행령 제14조의2(개인정보의 추가적인 이용 · 제공의 기준 등)
① 개인정보처리자는 법 제15조제3항 또는 제17조제4항에 따라 정보주체의 동의 없이 개인정보를 이용 또는 제공(이하 "개인정보의 추가적인 이용 또는 제공"이라 한다)하려는 경우에는 다음 각 호의 사항을 고려해야 한다.
4. 가명처리 또는 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부
② 개인정보처리자는 개인정보의 추가적인 이용 또는 제공이 지속적으로 발생하는 경우에는 제1항 각 호의 고려사항에 대한 판단 기준을 법 제30조제1항에 따른 개인정보 처리방침에 공개하고, 법 제31조제1항에 따른 개인정보 보호책임자가 해당 기준에 따라 개인정보의 추가적인 이용 또는 제공을 하고 있는지 여부를 점검해야 한다. <개정 2023.9.12>

NoteBase

③

추가 이용은 **당초 수집 목적과 합리적으로 관련된 범위**에서 정보주체의 불이익과 안전조치 등을 고려하여 허용된다. 지속적으로 추가 이용하는 경우에는 그 판단기준을 **개인정보 처리방침에 공개**하고 보호책임자가 준수 여부를 점검해야 한다.

개인정보 보호법 제15조(개인정보의 수집 · 이용)
③ 개인정보처리자는 당초 수집 목적과 합리적으로 관련된 범위에서 정보주체에게 불이익이 발생하는지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 대통령령으로 정하는 바에 따라 정보주체의 동의 없이 개인정보를 이용할 수 있다. <신설 2020.2.4>

개인정보 보호법 시행령 제14조의2(개인정보의 추가적인 이용 · 제공의 기준 등)
① 개인정보처리자는 법 제15조제3항 또는 제17조제4항에 따라 정보주체의 동의 없이 개인정보를 이용 또는 제공(이하 "개인정보의 추가적인 이용 또는 제공"이라 한다)하려는 경우에는 다음 각 호의 사항을 고려해야 한다.
1. 당초 수집 목적과 관련성이 있는지 여부
② 개인정보처리자는 개인정보의 추가적인 이용 또는 제공이 지속적으로 발생하는 경우에는 제1항 각 호의 고려사항에 대한 판단 기준을 법 제30조제1항에 따른 개인정보 처리방침에 공개하고, 법 제31조제1항에 따른 개인정보 보호책임자가 해당 기준에 따라 개인정보의 추가적인 이용 또는 제공을 하고 있는지 여부를 점검해야 한다. <개정 2023.9.12>

④

추가 제공의 예측 가능성은 고려사항 중 하나이다. **예측 가능하다는 이유만으로 필요한 안전성 확보조치가 면제되지는 않으므로**, 가명처리·암호화 등 안전조치 여부도 함께 고려해야 한다.

개인정보 보호법 시행령 제14조의2(개인정보의 추가적인 이용 · 제공의 기준 등)
① 개인정보처리자는 법 제15조제3항 또는 제17조제4항에 따라 정보주체의 동의 없이 개인정보를 이용 또는 제공(이하 "개인정보의 추가적인 이용 또는 제공"이라 한다)하려는 경우에는 다음 각 호의 사항을 고려해야 한다.
2. 개인정보를 수집한 정황 또는 처리 관행에 비추어 볼 때 개인정보의 추가적인 이용 또는 제공에 대한 예측 가능성이 있는지 여부
4. 가명처리 또는 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부

NoteBase

문 39. 「개인정보보호법」 중 제28조의8 '개인정보의 국외 이전'에 대한 설명으로 가장 적절한 것은?

① 개인정보처리자는 정보 수집단계에서 향후 사업확장을 고려해 정보주체로부터 국외 이전에 관한 별도의 동의를 받고 정보를 수집하던 중 사업확장이 결정되었다면 개인정보를 별도 조치 없이 국외로 제공·처리위탁 및 보관할 수 있다.

② 개인정보처리자는 정보주체와의 계약 체결 및 이행을 위해 개인정보의 처리위탁·보관이 필요한 경우에는 별도의 동의 없이도 개인정보를 국외로 제공·처리위탁 및 보관할 수 있다.

③ 개인정보처리자는 법률이나 대한민국을 당사자로 하는 조약 내용에 개인정보의 국외 이전에 관한 규정이 있는 경우에는 개인정보를 국외로 제공·처리위탁 및 보관할 수 있다.

④ 개인정보처리자는 정보 수집단계에서 정보주체로부터 국외 이전에 대한 별도 동의를 받고 주민번호와 전화번호 등 개인정보를 회사 내 서버에 수집하던 중 회사가 국외로 이전하게 되면 서버를 이전하여 보관할 수 있다.

정답 3번

①

국외 이전 동의는 이전 국가·시기·방법·이전받는 자 등 **법정 고지사항을 미리 알리고** 받아야 하며, 그 사항이 변경되면 **다시 알리고 동의**를 받아야 한다. 별도 동의를 받았더라도 **국외 이전에 필요한 보호조치**는 이행해야 하므로, 사업확장 결정만으로 별도 조치 없이 이전할 수는 없다.

개인정보 보호법 제28조의8(개인정보의 국외 이전)
② 개인정보처리자는 제1항제1호에 따른 동의를 받을 때에는 미리 다음 각 호의 사항을 정보주체에게 알려야 한다.
1. 이전되는 개인정보 항목
2. 개인정보가 이전되는 국가, 시기 및 방법
3. 개인정보를 이전받는 자의 성명(법인인 경우에는 그 명칭과 연락처를 말한다)
4. 개인정보를 이전받는 자의 개인정보 이용목적 및 보유 · 이용 기간
5. 개인정보의 이전을 거부하는 방법, 절차 및 거부의 효과
③ 개인정보처리자는 제2항 각 호의 어느 하나에 해당하는 사항을 변경하는 경우에는 정보주체에게 알리고 동의를 받아야 한다.
④ 개인정보처리자는 제1항 각 호 외의 부분 단서에 따라 개인정보를 국외로 이전하는 경우 국외 이전과 관련한 이 법의 다른 규정, 제17조부터 제19조까지의 규정 및 제5장의 규정을 준수하여야 하고, 대통령령으로 정하는 보호조치를 하여야 한다.

NoteBase

②

계약 체결·이행에 필요한 경우의 동의 예외는 **처리위탁·보관에 한정되며 제3자 제공까지 포함하지 않는다**.
처리위탁·보관도 **국외 이전의 법정 고지사항을 개인정보 처리방침에 공개하거나 정보주체에게 알린 경우**에만 이 근거로 동의 없이 할 수 있다.

개인정보 보호법 제28조의8(개인정보의 국외 이전)
① 개인정보처리자는 개인정보를 국외로 제공(조회되는 경우를 포함한다) · 처리위탁 · 보관(이하 이 절에서 "이전"이라 한다)하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 국외로 이전할 수 있다.
3. 정보주체와의 계약의 체결 및 이행을 위하여 개인정보의 처리위탁 · 보관이 필요한 경우로서 다음 각 목의 어느 하나에 해당하는 경우
가. 제2항 각 호의 사항을 제30조에 따른 개인정보 처리방침에 공개한 경우
나. 전자우편 등 대통령령으로 정하는 방법에 따라 제2항 각 호의 사항을 정보주체에게 알린 경우

③

법률이나 대한민국을 당사자로 하는 조약 등에 **개인정보의 국외 이전에 관한 특별한 규정**이 있으면, 그 규정에 따라 개인정보를 국외로 제공·처리위탁·보관할 수 있다.

개인정보 보호법 제28조의8(개인정보의 국외 이전)
① 개인정보처리자는 개인정보를 국외로 제공(조회되는 경우를 포함한다) · 처리위탁 · 보관(이하 이 절에서 "이전"이라 한다)하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 국외로 이전할 수 있다.
2. 법률, 대한민국을 당사자로 하는 조약 또는 그 밖의 국제협정에 개인정보의 국외 이전에 관한 특별한 규정이 있는 경우

NoteBase

④

주민등록번호는 **정보주체의 동의만으로 수집·보관할 수 없으며**, 법령상 구체적 근거나 급박한 생명·신체·재산의 이익 등 법정 예외가 필요하다. 따라서 국외 이전 동의를 받았다는 사정만으로 주민등록번호가 든 서버를 해외로 옮겨 보관할 수는 없다.

개인정보 보호법 제24조의2(주민등록번호 처리의 제한)
① 제24조제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다. <개정 2014.11.19, 2016.3.29, 2017.7.26, 2020.2.4>
1. 법률 · 대통령령 · 국회규칙 · 대법원규칙 · 헌법재판소규칙 · 중앙선거관리위원회규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우
2. 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우
3. 제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 보호위원회가 고시로 정하는 경우

NoteBase