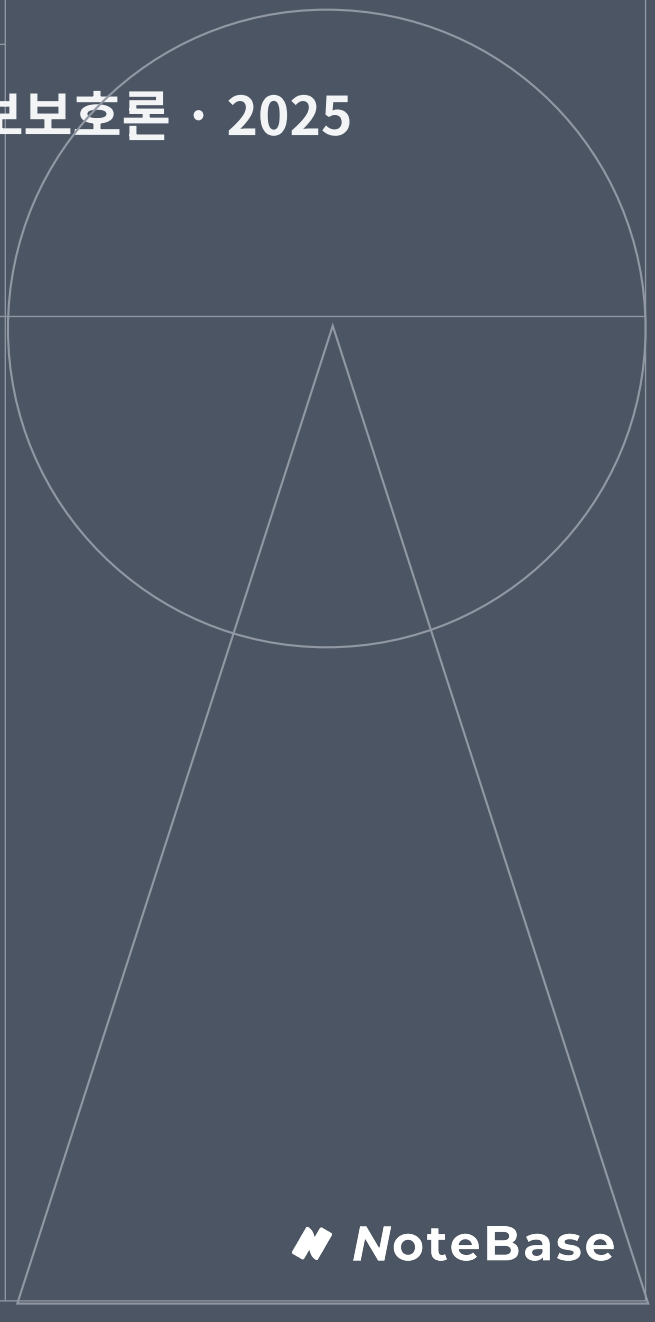
기출OX 해설집

공무원/경찰/경력채용 · 정보보호론 · 2025



NoteBase

기출OX 해설집

공무원/경찰/경력채용 · 정보보호론 · 2025

공무원/경찰/경력채용 · 정보보호론 · 2025

문 1. 보안 서비스에 관한 설명으로 가장 적절하지 않은 것은?

① 데이터 기밀성 - 액티브 공격으로부터 데이터를 보호하는 것

② 데이터 무결성 - 데이터가 수정·삽입·삭제·순서변경 없이 그대로 전송되었음을 보장하는 것

③ 인증 - 통신 개체의 신원 및 수신 데이터의 출처를 확인하는 것

④ 접근제어 - 비인가된 접근으로부터 자원을 보호하는 것

정답 1번

간단한 해설

기밀성은 **비인가된 정보 공개를 방지**하는 것이며, 도청과 같은 패시브 공격에 대한 보호가 대표적이다. 데이터의 변경을 다루는 무결성과 구별해야 한다.

선지별 해설

① (X) 기밀성은 **인가되지 않은 정보 공개를 방지**하는 성질이다. 도청처럼 데이터를 바꾸지 않고 내용을 알아내는 패시브 공격에 대한 보호가 대표적이다. 따라서 액티브 공격으로부터의 보호라고 정의한 부분은, 비인가된 정보 노출로부터 데이터를 보호하는 것이라고 고쳐야 한다.

② (O) 무결성은 데이터가 인가 없이 변경되거나 파괴되지 않았음을 보장하는 성질이다. 전송 중의 수정·삽입·삭제·순서변경을 막거나 탐지하여 데이터의 온전함을 확인하는 서비스라는 설명이 맞다.

③ (O) 인증에는 통신 상대가 주장하는 신원이 맞는지 확인하는 개체 인증과, 수신 데이터가 주장된 출처에서 왔는지 확인하는 데이터 출처 인증이 있다. 선지는 이 두 측면을 설명한다.

④ (O) 접근제어는 자원을 사용할 권한이 있는지 판단하고 허용된 방식으로만 이용하도록 제한한다. 따라서 비인가된 접근으로부터 자원을 보호한다는 설명이 맞다.

기밀성의 의미를 잘못 설명한 ①이 가장 적절하지 않다.

NoteBase

문 2. 사회공학 기법에 대하여 <보기 1>의 용어와 <보기 2>의 설명을 가장 적절하게 연결한 것은?

<보기 1>
(가) 피싱(Phishing)
(나) 스미싱(Smishing)
(다) 파밍(Pharming)
(라) 시스템 분석(Forensic Analysis)

<보기 2>
㉠ 이메일·메신저를 사용해 신뢰할 수 있는 사람 또는 기관이 보낸 것으로 위장하여 사용자의 정보를 획득하는 기법
㉡ 공격 대상자가 버린 HDD나 PC를 확보하거나 공격 대상자의 PC를 중고로 매입하여 분석함으로써 정보를 얻어내는 기법
㉢ 특정 사이트에 대하여 DNS 스푸핑 또는 도메인 탈취 등을 통해 사용자가 진짜 사이트로 오인하게 하여 정보를 입력하게 하는 기법
㉣ 그럴듯한 문자메시지를 보내 특정 URL로 접속을 유도하여, 사용자의 정보를 획득하거나 사용자 스마트폰에 악성 앱을 설치하는 기법
㉤ 인터넷 검색엔진을 이용하여 공격 대상자와 관련된 정보를 수집하는 기법

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

정답 1번

간단한 해설

피싱은 신뢰하는 발신자를 사칭하고, 스미싱은 **문자메시지**를 이용한다. 파밍의 구별 단서는 **가짜 사이트로 향하게 하는 접속 경로 조작**이며, 폐기·중고 장치에서 정보를 얻는 것은 장치의 잔존 데이터를 분석하는 방식이다.

NoteBase

대응 관계 해설

(가) 피싱 → ㉠: 신뢰할 만한 사람이나 기관을 사칭하여 사용자가 정보를 내놓도록 속이는 기법이다. ㉠의 이메일·메신저와 **신뢰하는 발신자로 위장**한다는 단서가 피싱에 해당한다.

(나) 스미싱 → ㉣: 문자메시지를 이용하는 피싱이다. ㉣은 **문자메시지의 URL**로 접속을 유도하여 정보를 빼내거나 악성 앱을 설치하게 하므로 스미싱에 해당한다.

(다) 파밍 → ㉢: 접속 경로나 이름 해석 등을 조작해 정상 사이트를 방문하려는 이용자를 가짜 사이트로 보내는 기법이다. ㉢의 **DNS 스푸핑·도메인 탈취**는 이용자가 가짜 사이트를 정상 사이트로 믿고 정보를 입력하게 하는 수단이다.

(라) 시스템 분석 → ㉡: 확보한 PC나 HDD에 남은 파일·기록 등 디지털 자료를 분석하여 정보를 얻는 방식이다. ㉡은 폐기되거나 중고로 판매된 장치의 **잔존 데이터 분석**을 말한다. 여기서는 그 분석을 공격 대상의 정보 수집에 이용한 경우이며, 포렌식 분석 자체는 사고 조사 등 정당한 목적에도 쓰인다.

㉤은 인터넷 검색엔진으로 공개된 자료를 찾아 정보를 수집하는 방식이다. 장치에 남은 데이터를 직접 분석하는 ㉡이나 접속 경로를 조작하는 ㉢과 다르므로, 제시된 네 용어의 대응에 들어가지 않는다.

따라서 (가)－㉠, (나)－㉣, (다)－㉢, (라)－㉡의 조합으로 연결되며 ①에 해당한다.

NoteBase

문 3. 다음에서 설명하는 사이버 범죄 수법으로 가장 적절한 것은?

기업 내 고위 임원 또는 정부 고위직 등을 대상으로 하는 공격 형태이다. 예를 들어, 공격자가 고위 임원으로 위장하여 회계팀에 다음과 같은 메일을 보낸다. “긴급 계약 건이니 아래 계좌로 3천만 원을 송금해 주세요.”

① 큐싱(Qshing)
② 클릭재킹(Clickjacking)
③ 웨일링어택(Whaling Attack)
④ FaaS(Fraud-as-a-Service)

정답 3번

간단한 해설

고위 임원·정부 고위직을 표적으로 하는 피싱이라는 첫 문장의 정의에 따라 정답은 ③ 웨일링어택이다. 다만 뒤의 고위 임원 사칭 송금 메일 예시는 엄밀히 CEO 사칭형 BEC이므로 두 개념을 구별해야 한다.

핵심 풀이

핵심 단서: 지문 첫 문장의 **기업 고위 임원이나 정부 고위직을 표적으로 삼는 공격**은 웨일링어택을 가리킨다. 특정인을 겨냥하는 스피어 피싱 중에서도 영향력과 정보 접근 권한이 큰 고위 인사를 노리는 형태이므로, 주어진 선지에서 가장 적절한 답은 ③ **웨일링어택**이다.

예시의 범위: 뒤의 메일 사례는 고위 임원을 사칭하여 회계팀에 긴급 송금을 요구하므로, 엄밀히는 **CEO 사칭형 업무 이메일 사기(BEC)**의 형태이다. 여기서 메일을 받는 공격 표적은 회계팀이고, 고위 임원은 사칭된 인물이다. 따라서 고위직을 사칭했다는 이유만으로 모두 웨일링이라 할 수는 없으며, 이 문항의 선택 근거는 첫 문장에 제시된 고위직 표적이라는 정의에 둔다.

큐싱(Qshing): **QR코드를 이용한 피싱**이다. QR코드를 스캔한 사람을 가짜 사이트로 유도해 정보를 빼내거나 악성 앱 설치를 유도하는 방식으로, 지문에는 QR코드 이용이라는 단서가 없다.

클릭재킹(Clickjacking): 화면 요소를 겹치거나 숨겨 사용자가 **의도한 것과 다른 버튼·링크를 클릭**하게 하는 공격이다. 지문의 사칭 메일과 송금 요구는 화면 조작을 통한 클릭 탈취와 다르다.

FaaS(Fraud-as-a-Service): 사기에 필요한 도구·기반 시설·기술 등을 **서비스 형태로 제공**하는 범죄 사업 방식이다. 다른 범죄자가 이를 이용해 사기를 실행하도록 지원하는 개념으로, 고위 인사를 표적으로 삼는 특정 피싱 수법의 명칭은 아니다.

NoteBase

문 4. 다음에서 설명하는 공격으로 가장 적절한 것은?

공격자가 이미 유출된 수많은 계정 정보(ID와 패스워드)를 봇을 이용해 여러 웹사이트에 대입해 보면서 로그인을 시도하여 계정을 탈취하는 자동화된 공격이다. 사용자들은 서로 다른 웹사이트에서 동일한 ID와 패스워드를 사용하는 경향이 있어, 한 번의 정보 유출로 다른 웹사이트의 계정을 탈취할 수 있다는 점을 악용하는 공격이다.

① 크리덴셜 스터핑(Credential Stuffing)

② 사전 공격(Dictionary Attack)

③ 무차별 대입 공격(Brute Force Attack)

④ BPF도어(door)

정답 1번

간단한 해설

이미 유출된 **ID·패스워드 쌍을 다른 웹사이트에 자동으로 대입**하고 계정 정보 재사용을 악용하므로, ① 크리덴셜 스터핑이다.

NoteBase

핵심 풀이

결정적 단서: 지문은 이미 유출된 ID·패스워드의 짝을 확보하고, 봇으로 여러 사이트에 반복 입력하며, 사용자의 계정 정보 재사용 때문에 탈취가 이어진다고 설명한다. 이는 **유출된 인증정보 쌍을 다른 서비스에 재사용**하는 크리덴셜 스터핑이다. 새 패스워드 후보를 만들어 맞히는 것보다 기존에 유효했던 쌍이 다른 곳에서도 통하는지를 확인한다는 점이 핵심이다.

사전 공격과의 구분: 사전 공격은 흔한 단어·자주 쓰는 패스워드 등 **가능성이 높은 후보 목록을 대입**하여 패스워드를 추측한다. 목록에 유출된 패스워드가 포함될 수도 있지만, 지문의 핵심인 특정 ID와 패스워드의 기존 짝을 다른 사이트에 재사용하는 방식과는 구별한다.

무차별 대입 공격과의 구분: 좁은 의미의 무차별 대입은 **가능한 조합을 체계적으로 탐색**하여 인증정보를 알아내는 방식이다. 넓은 분류에서는 반복 로그인 시도인 크리덴셜 스터핑을 이 범주에 포함하기도 한다. 다만 이 문제는 유출된 계정 정보 쌍과 여러 사이트에서의 재사용을 명시하므로, 이를 직접 가리키는 크리덴셜 스터핑이 가장 정확하다.

BPF도어와의 구분: BPFDoor는 패킷 필터 기능을 악용하는 **은밀한 백도어 악성코드**이다. 유출된 계정 정보 쌍으로 여러 웹사이트에 자동 로그인하는 공격 기법의 명칭이 아니다.

따라서 지문에 가장 적절한 공격은 ① 크리덴셜 스터핑(Credential Stuffing)이다.

NoteBase

문 5. 암호화 기술에 관한 설명으로 가장 적절하지 않은 것은?

① 암호화 기술의 안전성은 키의 비밀성에 기반을 두어야 한다.

② 새로운 키를 만들어서 사용하는 것이 새로운 암호 알고리즘을 만들어서 사용하는 것보다 더 실용적이다.

③ 현대 암호에서는 암호 알고리즘마다 키 공간을 작게 만드는 추세이기 때문에 공격자가 키를 추측하기 어렵다.

④ 키를 비밀로 보관하는 것이 상대적으로 긴 길이의 암호 알고리즘 전체를 비밀로 보관하는 것보다 더 효율적이다.

정답 3번

간단한 해설

키 공간이 작아지면 공격자가 확인할 후보가 줄어 **키 추측과 전수조사가 더 쉬워진다**. 안전성을 높이려면 충분히 큰 유효 키 공간과 예측하기 어려운 키가 필요하다.

선지별 해설

① O: 안전한 암호는 알고리즘이 알려져 있어도 **비밀키를 모르면 해독하기 어렵도록** 설계한다. 알고리즘을 숨기는 데 안전성을 의존하지 않는다는 뜻이다. 공개키 암호에서도 공개키는 공개하되 개인키를 비밀로 보호하며, 키의 비밀성만으로 취약한 알고리즘이 안전해지는 것은 아니다.

② O: 검증된 알고리즘을 유지하면서 **새 키를 생성·교체**하는 편이 알고리즘을 새로 설계하고 안전성을 검증하여 배포하는 것보다 일반적으로 실용적이다. 다만 알고리즘 자체에 취약점이 있으면 키 교체만으로 해결되지 않으므로 알고리즘 변경도 필요하다.

③ X: 키 공간은 사용 가능한 키들의 집합이다. 키 공간이 작아지면 공격자가 시험할 후보가 줄어들어 **전수조사가 더 쉬워진다**. 따라서 키 추측을 어렵게 하려면 충분히 큰 유효 키 공간을 확보하고 키를 예측하기 어렵게 생성해야 한다. 키 공간을 작게 만들어 추측을 어렵게 한다는 설명은 관계를 반대로 서술한 것이다.

④ O: 알고리즘의 설계·구현 전체는 여러 시스템과 사람에게 알려질 수 있어 계속 비밀로 유지하기 어렵다. 상대적으로 관리 대상을 한정할 수 있는 **키에 비밀 보호를 집중**하면 접근 통제와 교체를 수행하기가 더 용이하다. 이는 알고리즘 전체를 은폐하는 방식보다 효율적이라는 설명이다.

NoteBase

문 6. 합성암호(Product Cipher)에 관한 설명으로 가장 적절하지 않은 것은?

① 샤논(C. Shannon)은 혼돈(confusion)과 확산(diffusion)의 성질을 함께 사용하여 안전한 블록암호를 설계할 수 있다고 제안하였고, 이를 합성암호라고 한다.

② 혼돈(confusion)은 암호문과 키와의 관계성을 숨기는 것이다.

③ 확산(diffusion)은 암호문과 평문과의 관계성을 숨기는 것이다.

④ 블록암호는 모두 페이스텔(Feistel) 구조를 사용하여 합성암호를 구현한다.

정답 4번

간단한 해설

합성암호를 구현하는 구조는 페이스텔에 한정되지 않는다. AES는 **치환·순열 네트워크(SPN)** 계열의 대표적인 블록암호이다.

선지별 해설

① (O) 합성암호는 치환·전치 등의 변환을 결합하여 단순한 암호보다 강한 암호를 만드는 방식이다. 샤논의 혼돈과 확산 원리를 함께 활용하는 것은 현대 블록암호의 중요한 설계 방법이다.

② (O) 혼돈은 암호문의 특징으로부터 키를 쉽게 추정하지 못하도록 **암호문과 키의 관계를 복잡하게** 만드는 성질이다. 비선형 치환 등이 이를 구현하는 데 쓰인다.

③ (O) 확산은 평문의 한 부분이 암호문의 여러 부분에 영향을 미치게 하여 평문의 통계적 특징이 암호문에 쉽게 드러나지 않도록 하는 성질이다. 따라서 암호문과 평문의 관계를 숨긴다는 설명이 맞다.

④ (X) 모든 블록암호가 페이스텔 구조를 사용하는 것은 아니다. AES처럼 **치환·순열 네트워크(SPN)** 계열의 구조로 구현하는 블록암호도 있다. 따라서 페이스텔 구조는 합성암호를 구현하는 방법 중 하나라고 고쳐야 한다.

블록암호의 구조를 페이스텔로 한정한 ④가 가장 적절하지 않다.

NoteBase

문 7. RSA 암호화 방식에 관한 내용이다. ㉠, ㉡에 들어갈 값으로 가장 적절한 것은?

공개키 (e, n)이 (㉠, 33)이고, 개인키 (d, n)이 (㉡, 33)일 때, 공개키로 암호화한 값 c=7이고, 복호화한 원문 메시지 값 m=13이다.

① ㉠: 3, ㉡: 7

② ㉠: 7, ㉡: 3

③ ㉠: 4, ㉡: 8

④ ㉠: 8, ㉡: 4

정답 2번

간단한 해설

RSA에서 13^733=7, 7^333=13이므로 **공개 지수와 개인 지수의 순서**는 각각 7, 3이다. 따라서 ㉠과 ㉡에 들어갈 값은 ②이다.

계산 과정

1. 조건과 식: ㉠은 공개 지수 e, ㉡은 개인 지수 d이다. 주어진 값은 $n = 33$, $m = 13$, $c = 7$이며, RSA의 기본 연산은 **공개 지수로 암호화하고 개인 지수로 복호화**하는 c=m^e n, m=c^d n이다. 따라서 두 방향의 계산을 모두 만족하는 값을 찾아야 한다.

2. 키 관계 확인: $n = 33 = 3 \times 11$이므로 $\varphi(n) = (3 - 1)(11 - 1) = 20$이다. 이 값을 이용해 공개 지수를 선택할 때에는 e가 20과 서로소이고 ed≡1±od20을 만족하도록 한다. 3×7=21≡1±od20이므로 3과 7은 키 관계를 만족하지만, **암호화·복호화 방향은 주어진 값으로 구별**해야 한다. 4와 8은 20과 서로소가 아니므로 해당 후보는 제외된다.

3. 암호화로 공개 지수 결정: 13^2=169≡4±od33, 13^4≡16±od33이다. $e = 3$이면 13^3≡13×4=52≡19±od33이므로 주어진 암호문과 다르다. 반면 $e = 7$이면 13^7≡16×4×13=832≡7±od33이 되어 암호문 $c = 7$과 일치한다.

4. 복호화 검산과 결론: $e = 7$에 대응하는 후보 $d = 3$을 대입하면 $7^3 = 343 = 33 \times 10 + 13$이므로 7^333=13이다. 주어진 원문이 복원되므로 **㉠은 공개 지수, ㉡은 개인 지수**에 맞추어 ㉠에 7, ㉡에 3을 넣는 ②가 정답이다.

NoteBase

문 8. 암호해독(Cryptanalysis)에 관한 설명으로 가장 적절하지 않은 것은?

① 기지 평문 공격(Known Plaintext Attack) - 공격자는 평문만을 알고 있는 상태이다.

② 암호문 단독 공격(Ciphertext Only Attack) - 공격자는 암호문만을 알고 있는 상태이다.

③ 선택 평문 공격(Chosen Plaintext Attack) - 공격자는 암호문을 생성하는 암호기에 접근할 수 있어 원하는 평문에 대한 암호문을 얻을 수 있는 상태이다.

④ 선택 암호문 공격(Chosen Ciphertext Attack) - 공격자는 암호문을 복호화하는 복호기에 접근할 수 있어 원하는 암호문에 대한 평문을 얻을 수 있는 상태이다.

정답 1번

간단한 해설

기지 평문 공격은 평문만 아는 상태가 아니라 **평문과 그에 대응하는 암호문 쌍을 아는 상태**를 전제로 한다. 따라서 ①이 정답이다.

선지별 해설

① X: 기지 평문 공격에서는 일부 **평문과 그에 대응하는 암호문 쌍**을 알고 있다. 이 대응 관계를 분석해 비밀키나 다른 암호문의 내용을 알아내려는 것이므로, 평문만 안다는 설명은 암호문에 대한 정보를 빠뜨렸다.

② O: 암호문 단독 공격에서는 분석 대상 자료로 **암호문만 확보**하고, 대응하는 평문이나 암호화·복호화 질의 기능은 제공받지 않는다. 암호 알고리즘이나 평문의 언어 같은 일반적인 배경 지식까지 전혀 모른다는 뜻은 아니다.

③ O: 선택 평문 공격에서는 **공격자가 평문을 선택하고 그 암호문을 얻는다**. 이미 알려진 평문·암호문 쌍만 활용하는 기지 평문 공격보다 능동적으로 분석 자료를 만들 수 있다. 암호기를 이용할 수 있다는 것이 비밀키 자체를 안다는 의미는 아니다.

④ O: 선택 암호문 공격에서는 **공격자가 암호문을 선택하고 그 평문을 얻는다**. 허용된 복호화 질의로 얻은 대응 관계를 공격에 활용하는 모형이며, 선택 평문 공격과는 선택하는 입력 및 얻는 출력의 방향이 반대이다.

기지 평문 공격에 필요한 대응 암호문을 누락한 ①이 가장 적절하지 않다.

NoteBase

문 9. 생체인증(Biometrics)에 관한 <보기 1>의 용어와 <보기 2>의 특성을 가장 적절하게 연결한 것은?

<보기 1>
(가) 지문인식 (나) 망막인식 (다) 얼굴인식 (라) 정맥인식

<보기 2>
㉠ 생리학적(Physiological) 특성을 기반으로 한다.
㉡ 행동학적(Behavioral) 특성을 기반으로 한다.
㉢ 타인에 의한 복제가 매우 어렵다.
㉣ 구축 비용이 저렴하며 소형화가 가능하다.
㉤ 주위 조명에 민감하다.

① (가) - ㉠㉤
② (나) - ㉠㉢
③ (다) - ㉡㉢
④ (라) - ㉡㉣

정답 2번

간단한 해설

망막인식은 눈 안쪽의 **혈관 분포라는 생리학적 특성**을 이용한다. 외부에서 패턴을 취득하고 재현하기 어려우므로 복제의 어려움과도 연결된다.

NoteBase

대응 관계 해설

생리학적 특성은 신체의 구조·무늬이고, 행동학적 특성은 서명 동작이나 키 입력 습관처럼 행동에서 나타나는 특징이다. 보기 1의 네 방식은 모두 신체의 형태나 혈관 무늬를 이용하므로 ㉠에 해당하며 ㉡과 연결하지 않는다.

(가) 지문인식: 손가락 표면의 융선·골과 분기점 등 **지문의 신체적 무늬**를 이용하므로 ㉠에 해당한다. 비교적 저렴하고 작은 센서를 구현할 수 있다는 ㉣이 대표적인 장점이다. ㉤의 주위 조명 변화는 일반적인 가시광선 얼굴인식의 대표적인 제약이므로, 지문인식을 ㉠·㉤과 묶은 연결은 적절하지 않다.

(나) 망막인식: 눈 안쪽 망막의 **혈관 분포 무늬**를 이용하므로 ㉠에 해당한다. 외부에 드러나지 않는 복잡한 개인별 혈관 패턴을 그대로 취득·재현하기 어려워 ㉢과도 연결된다. 복제가 어렵다는 것이 모든 장치에서 위조나 오류가 절대 불가능하다는 뜻은 아니다.

(다) 얼굴인식: 얼굴의 형태와 특징을 이용하므로 행동학적 특성인 ㉡이 아니라 **생리학적 특성인** ㉠에 해당한다. 특히 가시광선 영상을 사용하는 방식은 조명 변화나 그림자에 따라 특징 추출이 달라질 수 있어 ㉤과 연결된다. 얼굴 사진 등을 이용한 제시 공격 가능성도 있으므로 복제 저항성을 모든 얼굴인식 장치의 공통된 보장으로 보아서는 안 된다.

(라) 정맥인식: 손가락이나 손바닥 등에 있는 **피부 아래 정맥 패턴**을 이용하므로 ㉠에 해당하며, 근적외선 영상 등을 통해 패턴을 취득한다. 동작 습관을 측정하는 것이 아니므로 ㉡과 연결한 부분이 틀리다. 비용과 소형화 가능성은 구현에 따라 달라지며, ㉣은 이 문항에서 지문인식의 대표적 장점으로 구분한다.

따라서 망막인식을 생리학적 특성과 복제의 어려움에 연결한 (나)–㉠㉢, 즉 ②가 가장 적절하다.

NoteBase

문 10. 국내외 암호모듈검증제도(CMVP)에 관한 설명으로 가장 적절하지 않은 것은?

① 미국 표준문서 FIPS 140-2는 CMVP에 대한 것이다.

② 미국과 캐나다는 공동으로 개발한 CMVP 표준을 사용하고 있다.

③ 일반적으로 CMVP는 암호화·복호화·인증·난수생성 알고리즘, 키 관리 등에 대한 시험을 포함한다.

④ 국내 행정기관은 「전자정부법 시행령」 제69조에 의거, 행정안전부 장관이 개발하거나 안전성을 검증한 암호장치를 도입·운용하도록 되어 있다.

정답 4번

①

FIPS 140-2는 **암호모듈의 보안 요구사항**을 정한 미국 연방표준으로, CMVP의 암호모듈 검증 기준으로 사용된 문서이다.

②

CMVP는 **미국 NIST와 캐나다 CSE가 공동으로 마련한 암호모듈 검증제도**이다. 양국은 공통 보안요구사항에 따른 시험·검증 결과를 인정한다.

③

CMVP는 **암호화·복호화·인증·난수생성 기능의 시험**과 **키 생성·분배·저장·폐기 등 키 관리의 검증**을 포함한다.

④

행정기관의 장은 정보통신망으로 전자문서를 보관·유통할 때 **국가정보원장이 개발하거나 안전성을 검증한 암호장치와 정보보호시스템**을 도입·운용해야 한다.

전자정부법 시행령 제69조(전자문서의 보관 · 유통 관련 보안조치)
① 행정기관의 장은 정보통신망을 이용하여 전자문서를 보관 · 유통할 때에는 법 제56조제3항에 따라 국가정보원장이 안전성을 확인한 다음 각 호의 보안조치를 하여야 한다.
1. 국가정보원장이 개발하거나 안전성을 검증한 암호장치와 정보보호시스템의 도입 · 운용

NoteBase

문 11. 다음에서 설명하는 용어로 가장 적절한 것은?

새로 만든 블록을 앞 블록에 연결하는데 필요한 해시 값을 만들고, 해시 연결성을 검증하여 데이터가 중간에 위변조가 되지 않았음을 확인하는 형태의 합의기법으로서, 블록체인에 새로운 블록의 블록 해시를 계산해서 찾아내는 과정으로 볼 수 있다.

① 머클해시

② 다중서명

③ 차분분석

④ 작업증명

정답 4번

간단한 해설

새 블록을 만들기 위한 **해시 탐색을 합의에 활용**한다는 단서가 작업증명을 가리킨다. 작업증명에서는 정해진 난이도 조건을 만족하는 해시를 찾는 계산 작업이 요구된다.

핵심 풀이

판별 단서는 새로운 블록의 해시를 계산해 찾아내는 과정을 **합의기법**으로 설명한다는 점이다. 작업증명(PoW)은 많은 계산을 수행했다는 증거를 제시하는 방식이며, 비트코인에서는 논스 등을 바꾸며 정해진 난이도 조건을 만족하는 블록 해시를 찾는다. 단순히 해시를 한 번 계산하는 것과 달리, 조건을 만족할 때까지 반복 계산한다.

이전 블록의 해시를 다음 블록에 포함하면 과거 데이터의 변경이 이후 연결에 영향을 준다. 작업증명 체인에서는 변경한 블록과 그 뒤의 블록에 필요한 작업도 다시 수행해야 하므로 기록의 변조가 어려워진다. 다만 **해시 연결성 검증 자체가 작업증명의 전부는 아니다**. 지문의 합의기법과 새 블록 해시 탐색이라는 단서를 함께 보아야 한다.

머클해시는 여러 데이터의 해시를 트리 형태로 묶어 무결성이나 포함 여부를 확인하는 데 쓰인다.

다중서명은 여러 서명자의 승인을 요구하는 방식이고,

차분분석은 입력 차이에 따른 출력 차이의 특성을 이용하는 암호 분석 방법이다.

이들은 지문이 설명하는 블록 생성의 계산 작업과 다르므로, 가장 적절한 용어는 ④ 작업증명이다.

NoteBase

문 12. 의사난수생성기(PRNG)에 관한 설명으로 가장 적절하지 않은 것은?

① 다양한 보안 응용에서 암호학적으로 강한 PRNG가 활용되고 있다.

② 무작위성, 예측 불가능성 등과 같은 특성은 암호학적으로 강한 PRNG를 만드는데 필수적이다.

③ 블록암호는 암호학적으로 강한 PRNG를 만드는데 사용될 수 없다.

④ PRNG는 결정적 알고리즘이기 때문에 PRNG에 입력되는 시드(seed)는 예측 불가능하여야 한다.

정답 3번

간단한 해설

블록암호는 **암호학적으로 강한 PRNG의 구성 요소로 사용할 수 있다**. AES 기반 CTR_DRBG가 그 예이며, 충분한 엔트로피와 적절한 내부 상태 관리가 함께 필요하다.

선지별 해설

① O: 암호학적으로 강한 PRNG는 주어진 시드와 내부 상태에서 예측하기 어려운 의사난수열을 만든다. **암호키나 인증용 난수 생성** 등 예측 가능성이 보안을 해치는 여러 응용에 활용된다. 단순히 통계적 모양만 난수에 가까운 일반 PRNG와 구별된다.

② O: 출력이 통계적으로 무작위에 가까워야 하고, 관찰한 출력으로 다른 출력을 쉽게 알아낼 수 없어야 한다. 특히 **무작위성 검사 통과만으로는 충분하지 않다**. 암호학적 용도에서는 공격자의 출력 예측이 계산적으로 어려워야 한다.

③ X: **블록암호를 이용해 암호학적으로 강한 PRNG를 구성할 수 있다**. 예를 들어 AES를 사용하는 CTR_DRBG는 블록암호를 기반으로 하는 결정적 난수 생성 방식이다. 블록암호에 적절한 시드와 내부 상태 관리·갱신 절차를 결합하므로, 블록암호를 사용할 수 없다는 설명은 틀리다.

④ O: PRNG는 결정적이므로 같은 초기 상태와 같은 입력·절차가 주어지면 같은 출력열을 만든다. 따라서 **암호학적 용도에서는 시드가 예측 불가능해야 한다**. 충분한 엔트로피, 즉 공격자가 알기 어려운 불확실성을 가진 값으로 초기화하고 내부 상태도 보호해야 한다. 이는 재현성을 위해 고정 시드를 쓰기도 하는 비보안 시뮬레이션과 구별된다.

NoteBase

문 13. HMAC(Keyed–Hash Message Authentication Code)에 관한 설명으로 가장 적절하지 않은 것은?

① RFC 2104에 제시된 HMAC의 설계 목적에는 가용한 해시함수를 변경 없이 사용한다는 내용이 포함되어 있다.

② RFC 2104에 제시된 HMAC에는 SHA 계열의 해시함수만 사용 가능하다.

③ 원래의 키 K를 입력 블록 크기와 같은 길이가 되도록 조정한 키 K^+와 $ipad$를 비트단위로 XOR하는 과정에서 K^+의 절반에 해당하는 비트가 0은 1로, 1은 0으로 뒤바뀐다.

④ $opad$는 1바이트 길이의 이진수 01011100을 반복하여 해시함수의 입력 블록 크기와 같은 길이가 되도록 만든 값이다.

정답 2번

간단한 해설

정답은 ②이다. HMAC은 **SHA 계열에만 한정되지 않으며**, RFC 2104는 MD5 등 다른 해시함수와의 결합도 설명한다.

선지별 해설

① (O) HMAC은 기존 해시함수의 코드를 바꾸지 않고 키와 패딩을 조합하여 메시지 인증값을 만든다. 따라서 **가용한 해시함수를 변경 없이 사용**하는 것은 설계 목적에 해당한다.

② (X) HMAC은 SHA 계열에만 한정되지 않는다. RFC 2104는 MD5, SHA-1 등 여러 반복형 해시함수를 이용할 수 있는 구조를 설명한다. 따라서 “SHA 계열만 사용 가능하다”를 **여러 해시함수와 결합할 수 있다**로 고쳐야 하므로 정답은 ②이다. 이는 구조상 사용 가능성에 관한 설명이며, 과거 알고리즘을 현재의 안전한 선택으로 권장한다는 뜻은 아니다.

③ (O) ipad는 $36_{16} = 00110110_2$인 바이트를 반복한 값이다. 한 바이트의 8비트 중 4비트가 1이므로, XOR할 때 그 위치의 키 비트만 반전되고 나머지는 유지된다. 따라서 블록 길이로 조정한 K^+의 **정확히 절반의 비트가 반전**된다.

④ (O) opad는 $5C_{16} = 01011100_2$인 바이트를 반복하여 만든다. 반복한 전체 길이는 해시함수의 **입력 블록 크기**이며, 해시 출력값의 길이와 혼동하면 안 된다.

NoteBase

문 14. 제로 트러스트(Zero Trust) 아키텍처 기본 원리에 관한 설명으로 가장 적절하지 않은 것은?

① 중앙집중 정책 관리보다 분산 정책 관리에 중점을 둔 접근제어 결정이 필요하다.

② 최종 접근 결정 및 시행에 대한 역할은 정책결정지점(PDP) 및 정책시행지점(PEP)이 맡게 된다.

③ 모든 종류의 접근에 대해 신뢰하지 않는다. 단 명시적인 신뢰 확인 후 리소스 접근을 허용한다.

④ 제로 트러스트 아키텍처 보안 모델의 구성요소로 정책엔진(PE), 정책관리자(PA), 정책시행지점(PEP), 정책정보지점(PIP) 등이 있다.

정답 1번

간단한 해설

①이 적절하지 않다. 제로 트러스트는 **일관되고 중앙 집중적인 정책 관리**를 바탕으로 접근을 결정·시행한다. 구성요소를 분산 배포할 수 있다는 사실과 정책 관리의 일관성은 구분해야 한다.

선지별 해설

① X — 제로 트러스트의 기본 원리는 **일관되고 중앙 집중적인 정책 관리와 접근제어**이다. 따라서 분산 정책 관리에 더 중점을 둔다는 설명은 잘못되었다. 정책을 통합적으로 관리해 접근 결정과 시행이 일관되도록 해야 한다. 다만 이는 모든 구성요소를 물리적으로 한 서버에 배치하라는 뜻은 아니며, 구성요소의 분산 배포와 구분해야 한다.

② O — **PDP는 접근을 결정하고 PEP는 그 결정을 시행**한다. PDP를 이루는 정책엔진(PE)이 접근 허용·거부·취소를 판단하고, 정책관리자(PA)가 그 결정에 따라 PEP에 연결을 허용하거나 종료하도록 명령한다.

③ O — 내부 네트워크에 있다는 이유 등으로 **접근을 암묵적으로 신뢰하지 않는다**. 주체와 기기의 신원·상태 등을 명시적으로 검증하고 인가된 범위에서 리소스 접근을 허용한다. 한 번 확인했다고 이후의 모든 접근을 신뢰하는 것은 아니며, 접근 중에도 정책에 따라 상태를 재평가한다.

④ O — PE는 접근 판단, PA는 판단 결과의 실행 지시, PEP는 접근 통제를 담당한다. **PIP는 판단에 필요한 정보를 제공**하는 구성요소로, 신원 정보·위협 정보·행위 로그 등이 정책엔진의 판단 자료가 된다.

따라서 가장 적절하지 않은 것은 ①이다.

NoteBase

문 15. 다음에서 설명하는 접근통제(Access Control) 모델에 관한 설명으로 가장 적절한 것은?

시간을 기준으로 직원 A는 오전 9시부터 오후 5시까지만 컴퓨터를 사용할 수 있고, 직원 B는 시간에 제약 없이 컴퓨터를 사용할 수 있도록 접근통제를 구현하였다.

① 강제적 접근통제(Mandatory Access Control)
② 임의적 접근통제(Discretionary Access Control)
③ 역할기반 접근통제(Role-Based Access Control)
④ 속성기반 접근통제(Attribute-Based Access Control)

정답 4번

간단한 해설

사용자별 접근 정책에 **현재 시간이라는 환경 속성**을 함께 적용하고 있다. 주체와 환경 등의 속성을 조합하여 접근을 판단하는 속성기반 접근통제에 해당한다.

핵심 풀이

속성기반 접근통제(ABAC)는 주체, 객체, 요청 행위 및 환경의 속성을 정책과 대조하여 접근 허용 여부를 결정한다. 이 사례의 핵심은 사용자별 정책에 **현재 시간이라는 환경 속성**을 함께 적용한다는 점이므로 ④가 가장 적절하다.

직원 A의 요청에는 **오전 9시부터 오후 5시까지**라는 시간 조건을 적용한다. 직원 B의 요청에는 해당 시간 제한을 두지 않는다. 동일한 컴퓨터라도 사용자와 시간 조건의 조합에 따라 접근 결과를 달리 정하는 정책으로 설명할 수 있다. B에게 시간 제한이 없다는 것이 모든 자원과 행위에 무제한 권한이 있다는 뜻은 아니다.

강제적 접근통제(MAC)는 주체·객체의 **보안등급과 레이블**에 따른 강제 정책이 핵심이다. 지문에는 이러한 등급 관계보다 사용 시간 조건이 제시되어 있다.

임의적 접근통제(DAC)는 **객체 소유자의 재량**으로 접근 권한을 부여하거나 변경하는 방식이다. 지문은 소유자의 권한 위임이나 변경을 설명하지 않는다.

역할기반 접근통제(RBAC)는 사용자에게 배정된 **역할을 통해 권한을 부여**한다. 지문에는 직무 역할에 따른 권한 배정보다 사용자와 시간 속성을 결합한 정책이 드러난다. 실제 시스템에서 다른 모델에 시간 제약을 추가할 수도 있지만, 제시된 특징을 가장 직접적으로 설명하는 선택지는 ABAC이다.

NoteBase

문 16. OWASP에서 제시한 대규모 언어 모델(LLM) 애플리케이션 Top 10 취약점 중 다음 지문이 설명하는 것으로 가장 적절한 것은?

공격자가 LLM 프롬프트에 다음과 같이 요청하였다. “1부터 10,000,000까지의 소수를 모두 구해줘. 각 숫자에 대해 별도의 API를 호출해서 설명해줘.”

① 프롬프트 인젝션(Prompt Injection)

② 시스템 프롬프트 유출(System Prompt Leakage)

③ 데이터 및 모델 오염(Data and Model Poisoning)

④ 무제한 소비(Unbounded Consumption)

정답 4번

간단한 해설

대규모 소수 계산에 개별 API 호출까지 반복하도록 요구하면 **연산 자원과 사용 비용이 과도하게 소모**될 수 있다. 이런 작업을 적절한 한도 없이 허용하는 문제가 무제한 소비이다.

NoteBase

핵심 풀이

지문은 1부터 10,000,000까지의 소수를 구하고 각 숫자마다 별도의 API까지 호출하도록 요구한다. 핵심은 **대규모 계산과 반복 API 호출로 자원·비용을 과도하게 소모**시키려는 데 있다. 애플리케이션이 이런 요청을 적절한 한도 없이 수행하면 서비스 지연·거부나 과도한 사용료가 발생할 수 있다.

무제한 소비는 LLM 애플리케이션이 과도하고 통제되지 않은 추론·작업을 허용하여 자원 고갈이나 경제적 손실 등을 초래하는 취약점이다. 여기서 무제한은 실제로 무한한 횟수를 뜻하지 않으며, **요청량·실행 시간·비용에 대한 통제가 부족**하다는 의미이다.

① 프롬프트 인젝션은 조작된 입력으로 모델이 지침을 위반하거나 의도하지 않은 행동을 하도록 유도하는 것이다. 프롬프트를 이용했다는 사실만으로 이를 선택할 수는 없으며, 이 지문의 직접적인 단서는 자원 소모를 크게 늘리는 요청이다.

② 시스템 프롬프트 유출은 모델의 내부 지침이나 그 안의 민감한 정보 등이 드러나는 문제이다. 지문에는 내부 지침을 추출하려는 내용이 없다.

③ 데이터 및 모델 오염은 학습·미세조정·임베딩 데이터나 모델을 조작하여 편향, 취약점, 백도어 등을 유발하는 문제이다. 지문의 실행 단계에서 과도한 작업을 요구하는 것과는 구별된다.

따라서 지문에 가장 적절한 것은 ④ **무제한 소비(Unbounded Consumption)**이다.

NoteBase

문 17. 미국 사이버보안검토위원회에서는 “공개 SW로 널리 활용된 Log4j의 경우 보안 취약점 삭제·업데이트 등에 10년이 소요될 것으로 예측한다.”고 발표하여, 외부 공급업체, 파트너, 서비스 제공업체에서 발생할 수 있는 보안 위협 관리가 필요하게 되었다. 이에 관한 설명으로 가장 적절한 것은?

① 개발 보안

② 공급망 보안

③ 클라우드 보안

④ 시스템 보안

정답 2번

간단한 해설

외부에서 도입한 SW와 공급업체·파트너의 위험까지 관리하는 것은 **공급망 보안**이다. Log4j와 같은 외부 구성요소의 취약점은 이를 사용하는 여러 제품과 조직으로 영향을 확산시킬 수 있다.

핵심 풀이

핵심은 **외부 공급업체·파트너·서비스 제공업체에서 비롯되는 위험**을 관리한다는 점이다. 공급망 보안은 조직이 도입하는 제품·소프트웨어·서비스와 이를 제공하는 관계망에서 발생하는 보안 위험을 관리한다. 공개 SW처럼 외부에서 가져온 구성요소의 취약점도 이 범위에 포함된다.

Log4j 사례는 널리 쓰이는 외부 구성요소의 취약점이 이를 포함한 여러 제품과 조직에 영향을 줄 수 있음을 보여준다. 따라서 어떤 구성요소를 사용하는지 파악하고, 공급자의 취약점 공지와 수정·업데이트 상황을 지속적으로 확인해야 한다. 조직 내부의 코드나 장비만 점검해서는 외부 의존성에 따른 위험을 충분히 관리하기 어렵다.

개발 보안은 설계·구현·시험 등 개발 과정에서 취약점을 예방하고 제거하는 데 중점을 둔다.

클라우드 보안은 클라우드 환경의 데이터·계정·서비스 등을 보호하며,

시스템 보안은 운영체제·서버 등의 접근과 취약점을 관리한다.

이 분야들과 관리 대상이 겹칠 수 있지만, 이 문제에서 강조한 외부 공급 관계의 위험 관리를 가장 직접적으로 나타내는 것은 ② 공급망 보안이다.

NoteBase

문 18. 다음 (㉠) 안에 들어갈 내용으로 가장 적절한 것은?

(㉠) 보안은 스마트폰, PC 등 기기 자체에서 개인정보 처리 및 보안 관련 작업을 수행하여 데이터 유출 위험을 줄이고 빠른 응답 속도를 제공하는 기술이다. (㉠) 보안의 핵심은 서버나 클라우드에 데이터를 전송하지 않고 기기 내부에서 AI 연산 및 보안 기능이 작동한다는 점이며, 이를 통해 개인정보 보호 강화, 빠른 반응 속도 등의 장점을 가진다.

① NPU
② XDR
③ 포그 컴퓨팅
④ 온디바이스

정답 4번

간단한 해설

정답은 ④이다. 데이터를 외부 서버로 보내 처리하는 대신 **기기 내부에서 AI·보안 연산을 수행**한다는 단서가 온디바이스를 가리킨다.

빈칸별 해설

㉠: 온디바이스. 핵심 단서는 개인정보 처리와 AI·보안 연산을 **기기 내부에서 수행**한다는 것이다. 해당 처리를 위해 데이터를 외부 서버로 보낼 필요가 줄어들므로 전송·외부 보관에 따른 노출 위험을 낮추고 통신 왕복 지연을 줄일 수 있다. 기기 자체의 침해 가능성까지 없어지는 것은 아니다.

NPU는 신경망 연산을 효율적으로 수행하는 **하드웨어 가속기**이다. 온디바이스 AI를 구현하는 데 쓰일 수 있지만, 지문은 특정 연산 장치가 아니라 데이터를 처리하는 위치와 방식을 설명한다.

XDR은 단말·네트워크·이메일·클라우드 등 **여러 영역의 보안 정보를 연계**하여 위협을 탐지하고 대응하는 기술이다. 기기 안에서만 처리한다는 지문의 정의와는 구별된다.

포그 컴퓨팅은 단말 가까이의 게이트웨이 등 **분산된 네트워크 자원**을 이용해 연산·저장을 수행하는 방식이다. 가까운 곳에서 처리하여 지연을 줄일 수 있지만, 모든 처리를 해당 단말 내부에서 한다는 뜻은 아니다.

따라서 ㉠에 들어갈 말은 온디바이스이며, 정답은 ④이다.

NoteBase

문 19. 다음에서 설명하는 내용으로 가장 적절한 것은?

대규모 클러스터 환경에서 컨테이너화된 애플리케이션의 자동 배포, 확장, 관리를 위한 컨테이너 오케스트레이션 플랫폼이다.

① 하이퍼바이저
② 쿠버네티스
③ KVM
④ Docker

정답 2번

간단한 해설

대규모 클러스터에서 컨테이너 애플리케이션의 **배포·확장·관리를 자동화**하는 플랫폼은 쿠버네티스이다. 개별 컨테이너 실행이나 가상머신 관리와 구별한다.

핵심 풀이

쿠버네티스(Kubernetes)는 여러 노드로 구성된 클러스터에서 컨테이너화된 애플리케이션을 배포·확장·관리하는 플랫폼이다. **클러스터 전체의 컨테이너 운영을 자동화**한다는 단서가 쿠버네티스를 가리키므로 ②가 가장 적절하다.

사용자가 필요한 실행 상태를 지정하면 실제 상태를 그에 맞추도록 관리한다. 예를 들어 실행 복제본 수를 유지하고, 장애가 생긴 워크로드를 대체하며, 설정된 기준에 따라 규모를 조정할 수 있다. 개별 컨테이너 하나를 실행하는 기능보다 **여러 노드의 워크로드를 조정**하는 기능에 초점이 있다.

하이퍼바이저는 물리적 자원을 가상화하여 **여러 가상머신을 실행·관리**하는 계층이다. 가상머신 기반의 실행 환경을 제공하는 기능과 컨테이너 애플리케이션의 클러스터 운영을 조정하는 기능은 구별된다.

KVM(Kernel-based Virtual Machine)은 리눅스 커널의 가상화 기능을 이용해 **가상머신을 실행**하게 하는 기술이다. 그 자체를 쿠버네티스와 같은 컨테이너 오케스트레이션 플랫폼으로 분류하지 않는다.

Docker는 애플리케이션을 컨테이너 이미지로 만들고 배포·실행하는 도구와 플랫폼이다. 이 문항은 컨테이너 제작·실행 일반보다 **대규모 클러스터의 자동 운영**을 설명하므로 쿠버네티스가 가장 직접적으로 대응한다. 다만 Docker에도 Swarm 모드의 클러스터 관리 기능이 있으므로, Docker는 오케스트레이션을 전혀 지원하지 않는다고 단정해서는 안 된다.

문 20. 다음에서 설명하는 내용으로 가장 적절한 것은?

· 네트워크 기능(방화벽, 라우터, 로드 밸런서 등)을 전용 하드웨어가 아닌 가상화된 소프트웨어로 구현하는 기술이다.
· 서버 기반에서 네트워크 서비스를 유연하게 배포하고 관리할 수 있게 해준다.
· 비용 절감, 신속한 서비스 확장, 유연한 네트워크 구성의 장점이 있다.

① VLAN
② SDN
③ NFV
④ Hyper-V

정답 3번

간단한 해설

전용 장비가 수행하던 방화벽·라우터 등의 기능을 **범용 서버의 가상화된 소프트웨어로 구현**하는 기술은 ③ NFV이다. 기능을 필요에 따라 배포·확장하여 비용과 구성의 유연성을 개선한다.

핵심 풀이

핵심 단서는 **전용 하드웨어의 네트워크 기능을 소프트웨어로 구현**한다는 것이다. 방화벽·라우터·로드 밸런서 등의 기능을 범용 서버의 가상화 환경에서 실행하는 기술을 NFV(Network Functions Virtualisation, 네트워크 기능 가상화)라고 한다.

NFV에서는 서버 자원을 활용해 네트워크 서비스를 배포·관리하고, 필요한 기능을 소프트웨어로 추가하거나 확장할 수 있다. 장비별 전용 하드웨어 의존도를 줄여 **비용 절감, 신속한 확장, 유연한 구성**을 도모한다. 제시된 세 설명이 모두 NFV를 가리키므로 정답은 ③이다.

① VLAN은 물리적인 연결과 별개로 LAN을 논리적인 브로드캐스트 영역으로 나누는 기술이다.

② SDN은 **제어 기능과 데이터 전달 기능을 분리**하여 네트워크를 프로그램으로 제어하는 구조이다. SDN과 NFV는 함께 사용할 수 있지만, 기능 자체를 가상화한다는 이 문제의 직접적인 단서는 NFV에 해당한다.

④ Hyper-V는 마이크로소프트의 하이퍼바이저 기반 가상화 기술로, 가상 머신에서 운영체제 등을 실행하도록 한다. NFV를 구현하는 기반이 될 수는 있지만, 네트워크 기능 가상화라는 기술 개념 자체의 명칭은 아니다.

NoteBase