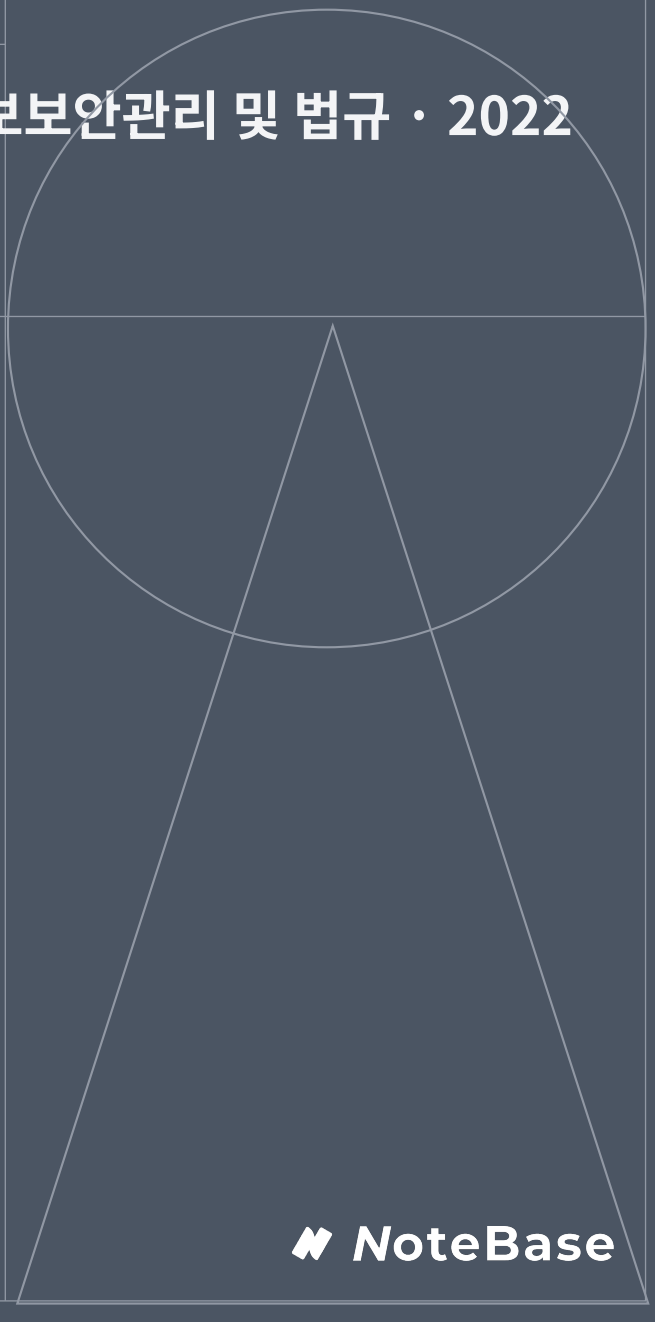
기출OX 해설집

공무원/경찰/경력채용 · 정보보안관리 및 법규 · 2022



NoteBase

기출OX 해설집

공무원/경찰/경력채용 · 정보보안관리 및 법규 · 2022

공무원/경찰/경력채용 · 정보보안관리 및 법규 · 2022

문 1. 다음 설명에 관한 위험 처리 전략으로 가장 적절한 것은?

고객 서비스 홈페이지 유지보수 협력업체, 개인정보 처리 수탁자 중 당사에서 직접 관리·감독할 수 없는 결제대행사, 본인확인기관 등과 같은 대형 수탁자에 대하여는 해당 수탁자가 법령에 의한 정부감독을 받거나 정부로부터 보안인증을 획득한 경우에는 개인정보 보호법에 따른 문서체결 이외의 별도 관리·감독은 생략할 수 있도록 한다.

① 위험 감소

② 위험 회피

③ 위험 전가

④ 위험 수용

정답 4번

간단한 해설

정부 감독·보안인증을 고려하여 추가 관리·감독을 하지 않고 **남아 있는 위험을 받아들이는** 결정이므로 위험 수용에 해당한다.

NoteBase

핵심 풀이

사례는 직접 감독하기 어려운 대형 수탁자가 정부 감독을 받거나 보안인증을 갖춘 경우, 문서 체결은 유지하되 별도의 관리·감독을 추가하지 않기로 한 결정이다. 핵심은 위탁 자체가 아니라 **기존 보호 수준을 고려하여 남은 위험을 감수**하는 데 있다. 정부 감독이나 보안인증이 있다는 사실이 위험이 전혀 없다는 뜻은 아니다.

① 위험 감소: 보호대책을 도입하거나 강화하여 **위험의 발생 가능성 또는 피해 규모를 낮추는** 전략이다. 사례의 결정은 추가 점검이나 통제를 강화하는 것이 아니라 별도 관리·감독을 생략하는 것이므로, 그 결정의 성격을 위험 감소로 보기는 어렵다.

② 위험 회피: 위험을 발생시키는 **활동을 중단하거나 위험을 피하도록 변경**하는 전략이다. 사례에서는 위탁이나 고객 서비스를 중단하지 않고 계속하므로 위험 회피에 해당하지 않는다.

③ 위험 전가: 보험이나 계약 등을 통해 **위험에 따른 손실 부담을 다른 주체로 이전**하는 전략이다. 수탁자가 등장한다는 이유만으로 전가라고 판단할 수는 없다. 제시된 결정에는 손실 부담을 새로 이전하는 조치가 없고, 별도 감독을 생략한다는 내용이 중심이다.

④ 위험 수용: 평가한 위험을 감내할 수 있는 수준으로 받아들이고 추가적인 위험 감소 조치 없이 유지하는 전략이다. 사례처럼 기존 정부 감독·보안인증을 고려하여 별도 감독을 생략하고 **남아 있는 위험을 받아들이는** 결정이므로 ④에 해당한다. 이는 위험 처리 전략을 분류한 것이며, 이 분류만으로 법령상 의무의 면제 여부까지 판단하는 것은 아니다.

NoteBase

문 2. 벨 라파듈라(Bell-La Padula) 보안 모델에서 무결성(integrity)을 침해하는 규칙으로 가장 적절한 것은?

① WD(Write Down) - 사용자의 보안 등급보다 낮은 보안 등급의 데이터에 쓰기
② WU(Write Up) - 사용자의 보안 등급보다 높은 보안 등급의 데이터에 쓰기
③ RD(Read Down) - 사용자의 보안 등급보다 낮은 보안 등급의 데이터를 읽기
④ RU(Read Up) - 사용자의 보안 등급보다 높은 보안 등급의 데이터를 읽기

정답 2번

간단한 해설

벨 라파듈라는 기밀성을 보호하므로 **상향 쓰기(WU)**를 허용할 수 있다. 이때 낮은 등급의 주체가 높은 등급의 데이터를 잘못 기록하거나 덮어쓸 수 있어, 기밀성 규칙만으로는 **무결성을 보장하지 못한다**.

개념 구분

벨 라파듈라 모델은 정보가 높은 보안등급에서 낮은 보안등급으로 유출되는 것을 막는 기밀성 모델이다. 기본 규칙은 상위 등급 읽기 금지(No Read Up)와 하위 등급 쓰기 금지(No Write Down)이다. 이 규칙만으로 데이터의 부당한 변경까지 방지되는 것은 아니다.

WD(Write Down): 높은 등급의 주체가 낮은 등급의 객체에 정보를 쓰면 기밀정보가 아래로 유출될 수 있다. 따라서 기본 기밀성 규칙에서 금지되는 동작이다.

WU(Write Up): 낮은 등급의 주체가 높은 등급의 객체에 쓰는 동작이다. 기밀정보가 아래로 유출되지는 않으므로 기본 기밀성 규칙상 허용될 수 있지만, **상위 등급 데이터에 잘못된 내용을 기록하거나 덮어쓰는 위험**이 남는다. 이것이 이 문항에서 묻는 무결성 보호의 한계이다.

RD(Read Down): 높은 등급의 주체가 낮은 등급의 데이터를 읽는 동작으로, 기본 기밀성 규칙상 허용될 수 있다. 읽기 자체는 상위 등급 객체의 내용을 직접 변경하는 동작이 아니므로, 문항이 지적하는 상향 쓰기의 문제와 다르다.

RU(Read Up): 낮은 등급의 주체가 높은 등급의 데이터를 읽으면 알 권한이 없는 기밀정보를 얻을 수 있다. 따라서 기본 기밀성 규칙에서 금지되는 동작이다.

따라서 벨 라파듈라 모델에서 허용될 수 있으면서 상위 등급 데이터의 무결성을 해칠 위험이 있는 동작은 ② WU이다.

NoteBase

문 3. 다음 권한 정보들을 통해 접근 제어를 수행하는 기법으로 가장 적절한 것은?

	데이터1	데이터2	데이터3
그룹1	읽기, 쓰기	-	읽기
그룹2	-	읽기	읽기, 쓰기
···	···	···	···

사용자	그룹(group)
사용자1	그룹1
사용자2	그룹2
사용자3	그룹2

① MAC(Mandatory Access Control)

② AAC(Arbitrary Access Control)

③ RBAC(Role Based Access Control)

④ DAC(Discretionary Access Control)

정답 4번

간단한 해설

이 문항의 정답은 ④ **DAC**이다. 사용자·소속 그룹과 데이터별 읽기·쓰기 권한을 연결한 표를 전형적인 재량적 접근 제어의 예로 해석한다. 그룹1의 권한은 사용자1에게, 그룹2의 권한은 사용자2·3에게 적용된다.

NoteBase

도식 해설

첫 번째 표는 그룹을 행, 데이터를 열로 두고 각 교차 칸에 허용된 연산을 적은 **접근 권한 행렬**이다. 읽기와 쓰기는 서로 구별되는 권한이며, “-”는 제시된 표에서 해당 권한이 부여되어 있지 않다는 뜻이다. 마지막의 말줄임표는 다른 항목이 생략되었음을 나타내므로 그 권한을 임의로 추정하지 않는다.

그룹1에는 **데이터1 읽기·쓰기**와 **데이터3 읽기**가 허용되고, 데이터2 권한은 없다. 두 번째 표에서 사용자1은 그룹1에 속하므로, 제시된 권한에 따르면 사용자1은 데이터1을 읽고 쓸 수 있으며 데이터3은 읽기만 할 수 있다. 데이터2에는 접근 권한이 없다.

그룹2에는 **데이터2 읽기**와 **데이터3 읽기·쓰기**가 허용되고, 데이터1 권한은 없다. 사용자2와 사용자3이 모두 그룹2에 속하므로 두 사용자는 같은 권한을 적용받는다. 각각 데이터2는 읽기만 가능하고 데이터3은 읽고 쓸 수 있으며, 데이터1에는 접근 권한이 없다.

이 문항은 사용자·그룹의 신원을 기준으로 객체별 권한을 지정하는 전형적인 재량적 접근 제어의 예로 해석하므로, 제공된 정답은 ④ **DAC(Discretionary Access Control)**이다. DAC에서는 객체의 소유자 또는 권한 설정을 위임받은 주체가 허용 범위 안에서 접근 권한을 정할 수 있다. 다만 두 표에 그 권한을 실제로 누가 부여했는지까지 표시되어 있는 것은 아니다.

RBAC는 역할에 권한을 연결하고 사용자에게 역할을 부여하는 방식이며, 그룹과 권한표를 이용해 구현할 수도 있다. 따라서 **그룹이 보인다는 이유만으로 DAC라고 단정할 수는 없다**. MAC의 보안 등급·강제 정책도 이 표에는 나타나지 않는다. 문항의 전형적인 DAC 해석과 별개로, 표만으로 모든 권한 부여 정책이나 구현 방식을 유일하게 확정할 수는 없다는 점을 구별해야 한다.

NoteBase

문 4. 다음 데이터 백업(data backup)에 관한 설명으로 ㉠~㉢에 해당하는 가장 적절한 것은?

(㉠) 백업 수행 후 아카이브 비트(archive bit)를 해제하지 않으므로, 마지막 전체 백업 시점 이후 변경된 파일 모두를 다음 (㉡) 백업 시점까지 계속 백업하는 방식을 (㉢) 백업이라 한다.

① ㉠: 차등, ㉡: 전체, ㉢: 차등

② ㉠: 차등, ㉡: 차등, ㉢: 전체

③ ㉠: 증분, ㉡: 전체, ㉢: 증분

④ ㉠: 증분, ㉡: 증분, ㉢: 전체

정답 1번

간단한 해설

차등 백업은 아카이브 비트를 해제하지 않아 마지막 전체 백업 이후의 변경 파일을 누적해서 백업한다. 다음 전체 백업이 이루어지면 누적의 기준점이 바뀐다.

빈칸별 해설

아카이브 비트는 파일이 생성·변경되어 백업 대상임을 표시하는 속성이다. 제시문은 이 비트를 사용하는 전체·차등 백업 주기를 설명한다.

㉠ 차등: 차등 백업은 대상 파일을 복사한 뒤에도 **아카이브 비트를 해제하지 않는다**. 따라서 한 번 백업한 파일도 다음 차등 백업에 다시 포함될 수 있다. 반면 증분 백업은 백업 후 비트를 해제하여 이후 새로 변경된 파일을 구분한다.

㉡ 전체: 이 주기에서는 다음 전체 백업이 전체 대상 파일을 복사하고 비트를 해제하여 **변경 여부를 판단할 기준점을 새로 설정**한다. 그때까지 차등 백업은 직전 차등 백업 이후가 아니라 마지막 전체 백업 이후의 변경 파일을 계속 포함한다.

㉢ 차등: 마지막 전체 백업 이후 변경된 파일을 **누적하여 백업**하는 방식이 차등 백업이다. 예를 들어 전체 백업 뒤 파일 A가 바뀌고, 다음 차등 백업 뒤 파일 B만 추가로 바뀌어도 그다음 차등 백업에는 A와 B가 모두 포함된다.

따라서 ㉠ 차등, ㉡ 전체, ㉢ 차등에 해당하는 ①이 정답이다.

NoteBase

문 5. 다음 CERT(Computer Emergency Response Team)에 관한 설명으로 옳은 것을 모두 고른 것은?

㉠ 보안 침해사고 대응을 수행하는 조직이다.
㉡ 사고 발생 시, 긴급히 조직되어 운영된다.
㉢ 카네기멜론 대학이 상표권을 등록하였다.
㉣ CSIRT, CIRT도 동일한 임무를 수행한다.
㉤ 정보보호 및 보안 전문가들로만 구성된다.

① ㉠㉡㉢
② ㉠㉡㉤
③ ㉠㉢㉣
④ ㉢㉣㉤

정답 3번

간단한 해설

CERT는 **사전에 대응체계를 갖추는 침해사고 대응 조직**이며, 필요에 따라 기술 분야 외의 인력도 참여·협력한다. CERT의 등록상표 보유자는 **카네기멜론 대학**이고, CSIRT·CIRT 역시 사고 대응 임무를 수행한다.

NoteBase

보기별 해설

㉠ O: CERT는 보안 침해사고에 대응하여 사고를 분석하고 피해를 줄이며 복구를 지원하는 조직이다. 사고 대응의 조정과 재발 방지를 위한 활동도 수행한다.

㉡ X: 사고가 난 뒤에야 급히 만드는 임시조직으로 한정할 수 없다. 효과적으로 대응하려면 **사전에 조직·역할·연락체계·대응 절차를 마련**하고 인력을 훈련해야 한다. 전담팀이나 기존 인력의 겸임 등 운영 형태는 달라질 수 있다.

㉢ O: **CERT는 카네기멜론 대학의 등록상표**이다. 따라서 사고 대응 조직 일반을 가리키는 용어인 CSIRT와 상표로서의 CERT를 구별할 필요가 있다.

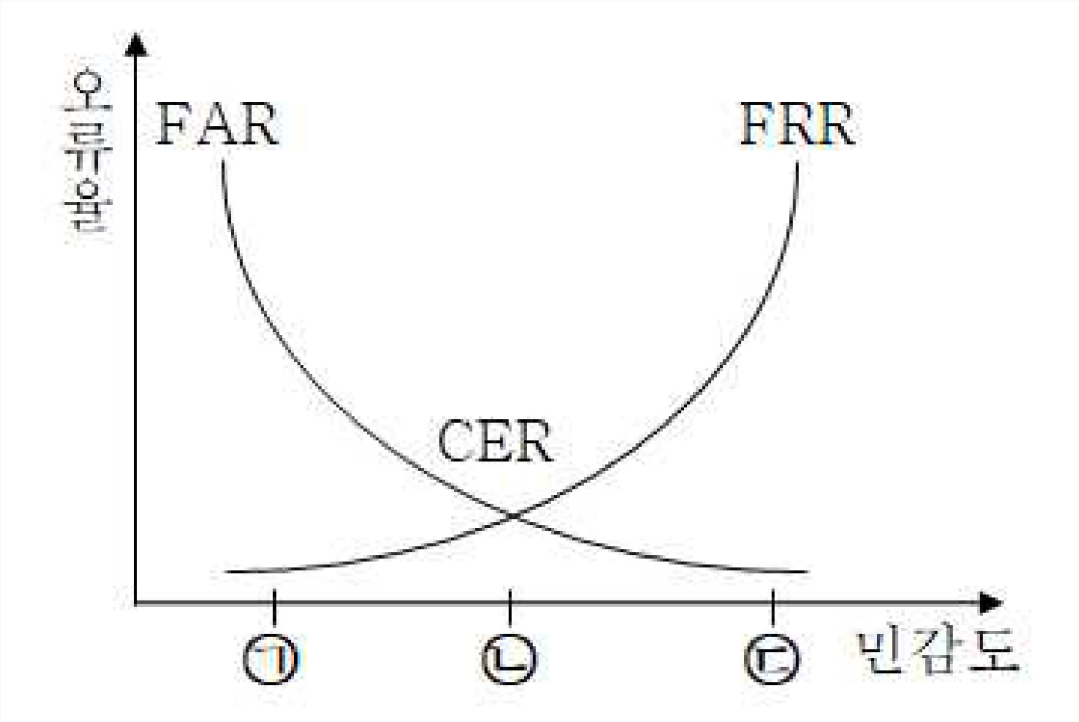
㉣ O: CSIRT는 Computer Security Incident Response Team, CIRT는 Computer Incident Response Team이다. 이들도 컴퓨터 보안사고에 대응·지원하는 임무를 수행한다. 같은 핵심 임무를 가리킨다는 뜻이며, 각 기관의 세부 서비스나 권한까지 모두 같다는 뜻은 아니다.

㉤ X: 구성원을 **정보보호·보안 전문가로만 제한하지 않는다**. 기술 분석 인력 외에도 관리·조정 인력이 필요하며, 법무·인사·홍보 등 관련 담당자가 참여하거나 협력할 수 있다. 사고의 법적 처리, 직원 관련 조치, 대외 소통은 기술 대응만으로 해결되지 않는다.

옳은 보기는 ㉠·㉢·㉣이므로 이 조합을 제시한 ③에 해당한다.

NoteBase

문 6. 다음 생체 인증 장치의 인식율에 관한 설명으로 가장 적절하지 않은 것은?



① CER(Crossover Error Rate)은 EER(Equal Error Rate)과 동일한 값이다.

② FRR값이 높아지면 권한이 있는 사용자의 인증이 불가능한 경우가 증가한다.

③ 생체 인식 장치의 민감도가 ㉠보다 ㉢일 경우 보안적 측면에서 더 안전하다.

④ 생체 인식 장치의 민감도를 ㉡에서 ㉠으로 낮추는 것은 위험 감소 전략이다.

정답 4번

간단한 해설

민감도를 ㉡에서 ㉠으로 낮추면 **FAR이 증가**하여 비인가자를 잘못 인증할 위험이 커진다. FRR 감소로 정상 사용자의 편의는 높아질 수 있지만, 이를 비인가 접근 위험을 줄이는 전략이라고 볼 수 없다.

NoteBase

선지별 해설

그래프의 가로축은 민감도, 세로축은 오류율이다. 민감도가 ㉠에서 ㉢으로 높아질수록 비인가자를 잘못 받아들이는 FAR은 낮아지고, 정당한 사용자를 잘못 거부하는 FRR은 높아진다.

① O: CER은 FAR과 FRR이 같아지는 교차점의 오류율이다. EER도 두 오류율이 같을 때의 값을 뜻하므로 **CER과 EER은 같은 오류율**을 가리킨다. 그림에서는 ㉡에 해당하는 두 곡선의 교차점에서 그 값을 읽는다.

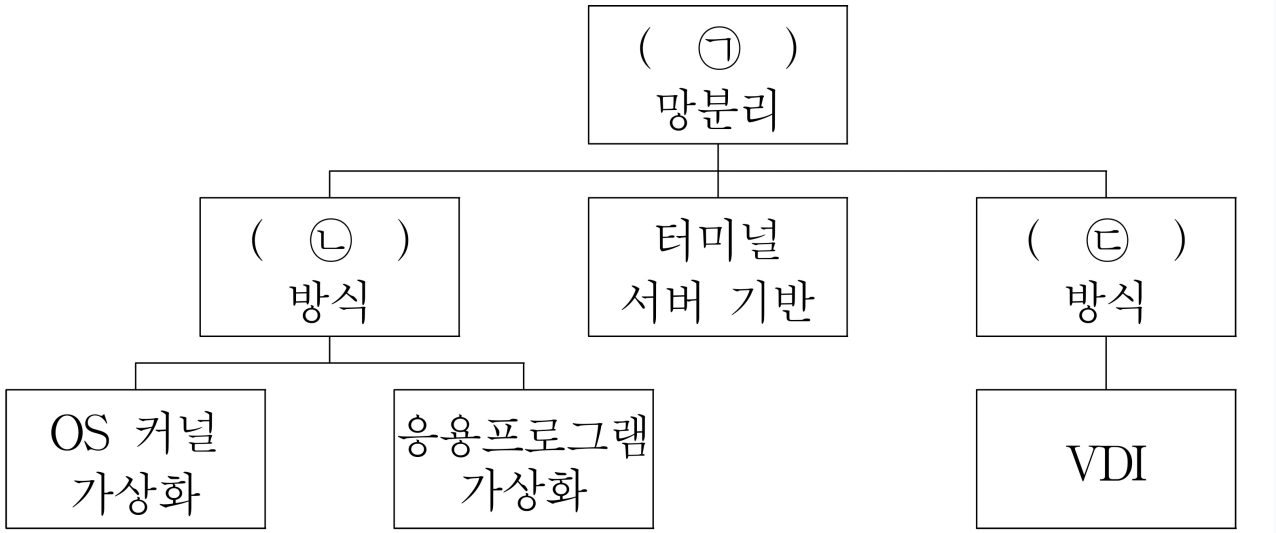
② O: FRR은 정당한 사용자의 인증 시도를 잘못 거부하는 비율이다. 이 값이 높아지면 **권한 있는 사용자의 오거부**가 많아져 정상 이용자가 인증을 통과하지 못하는 경우가 늘어난다.

③ O: ㉢에서는 ㉠보다 FAR 곡선이 낮으므로 **비인가자의 오인증 위험이 작다**. 이런 접근 차단의 보안 관점에서는 ㉢이 더 안전하다. 다만 FRR이 높아져 정당한 사용자의 이용 불편도 커지므로, 모든 이용 조건에서 무조건 유리하다는 뜻은 아니다.

④ X: 민감도를 ㉡에서 ㉠으로 낮추면 FRR은 감소하지만 **FAR은 증가**한다. 정상 사용자의 인증은 쉬워지는 대신 비인가자가 통과할 위험은 커지므로, 비인가 접근의 위험 감소 전략이라고 할 수 없다. 그 위험을 줄이려면 그래프에서 반대로 민감도를 높여 FAR을 낮추는 방향을 선택한다.

NoteBase

문 7. 다음 망분리 기술 분류와 관련하여 ㉠~㉢에 해당하는 가장 적절한 것은?



① ㉠: 논리적, ㉡: CBC, ㉢: SBC

② ㉠: 논리적, ㉡: SBC, ㉢: CBC

③ ㉠: 물리적, ㉡: CBC, ㉢: SBC

④ ㉠: 물리적, ㉡: SBC, ㉢: CBC

정답 1번

간단한 해설

OS 커널·응용프로그램을 사용자 컴퓨터에서 가상화하는 갈래는 **CBC**, VDI를 이용하는 서버 가상화 갈래는 **SBC**이다. 두 방식과 터미널 서버 기반 방식을 포괄하는 ㉠은 논리적 망분리이다.

NoteBase

도식 해설

㉠은 논리적 망분리이다. 도식의 세 가지 하위 갈래는 가상화나 원격 서버 접속을 이용하여 업무망과 인터넷망의 사용 환경을 나누는 방식이다. **가상 실행 환경을 이용해 분리**한다는 점에서, 별도의 장비·연결 경로 등으로 분리하는 물리적 망분리와 구별된다.

㉡은 CBC(Client Based Computing)이다. 왼쪽 갈래 아래의 OS 커널 가상화와 응용프로그램 가상화는 이 도식에서 **사용자 컴퓨터 안의 실행 영역을 분리**하는 구현 방법을 뜻한다. OS 수준의 가상 환경이나 특정 응용프로그램의 격리된 환경을 이용하므로 컴퓨터 기반 방식인 CBC에 대응한다.

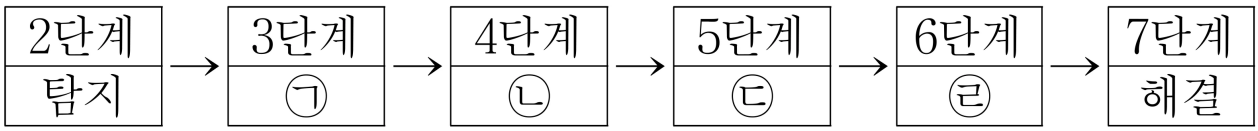
가운데의 터미널 서버 기반 방식은 컴퓨터에 설치된 접속 프로그램으로 원격 터미널 서버에 접속하여 작업하는 방식이다. **서버에서 작업을 실행**하고 단말은 화면 표시와 사용자 입력 등을 담당한다. 이 도식에서는 논리적 망분리의 한 갈래로 별도 표시되어 있다.

㉢은 SBC(Server Based Computing)이다. 오른쪽 갈래 아래의 VDI(Virtual Desktop Infrastructure)는 **서버에서 제공하는 가상 데스크톱**에 사용자 단말이 접속하는 방식이다. 가상 환경의 실행 자원이 서버에 있으므로 서버 기반 방식인 SBC에 대응한다.

따라서 ㉠은 논리적, ㉡은 CBC, ㉢은 SBC이며, 이 대응을 모두 만족하는 선지는 ①이다.

NoteBase

문 8. 다음 침해사고 대응 7단계 중 사고 발생 이후 과정으로 ㉠~㉣에 해당하는 가장 적절한 것은?



① ㉠: 초기대응, ㉡: 대응전략 체계화, ㉢: 사고조사, ㉣: 보고서 작성

② ㉠: 초기대응, ㉡: 사고조사, ㉢: 보고서 작성, ㉣: 대응전략 체계화

③ ㉠: 사고조사, ㉡: 초기대응, ㉢: 대응전략 체계화, ㉣: 보고서 작성

④ ㉠: 사고조사, ㉡: 초기대응, ㉢: 보고서 작성, ㉣: 대응전략 체계화

정답 1번

간단한 해설

탐지 후 초기 조사 결과로 **대응전략을 정한 다음 사고를 본격적으로 조사**한다. 조사 결과를 보고서로 정리한 뒤 해결·재발 방지 조치로 이어진다.

NoteBase

올바른 순서

탐지 → 초기대응 → 대응전략 체계화 → 사고조사 → 보고서 작성 → 해결

2단계 탐지: 보안장비의 이상 징후나 관리자의 확인을 통해 침해사고를 식별한다. 사고를 인지해야 대응 인력을 소집하고 초기 조치를 시작할 수 있다.

3단계 ㉠ 초기대응: 초기 조사로 사고의 기본 정황을 기록하고 대응팀을 소집하며 관련 부서에 알린다. 이때 확보한 **초기 조사 결과**가 다음 대응전략의 판단 자료가 된다.

4단계 ㉡ 대응전략 체계화: 초기 조사 내용을 바탕으로 대응 방향을 정하고 관리자 승인을 받는다. 수사기관과의 공조 필요성 등을 검토하여 **후속 조사 방침**을 정한다.

5단계 ㉢ 사고조사: 정한 방침에 따라 데이터를 수집·분석하여 사고 발생 경위와 피해를 파악한다. 보고서에는 추측이 아니라 **조사로 확인한 사실**을 담아야 하므로 보고서 작성보다 앞선다.

6단계 ㉣ 보고서 작성: 조사 결과를 의사결정자가 이해할 수 있도록 정리한다. 사고 원인과 대응 내용을 전달하여 이후 개선 조치의 근거를 마련한다.

7단계 해결: 분석·보고 결과를 토대로 보안정책과 절차를 개선하고 기술적 보완 계획을 세운다. **유사 사고의 재발 방지**까지 이어지는 단계이다.

NoteBase

문 9. 다음 설명에 해당하는 국가정보원 국가사이버안보센터 사이버위기경보 단계로 가장 적절한 것은?

·다수기관의 정보통신망 및 정보시스템 장애 발생
·다수기관의 정보유출 등 침해사고 확산 가능성 증가
·국내외 정치·군사적 위기발생 등 사이버 안보위해 가능성 고조

① 관심
② 주의
③ 경계
④ 심각

정답 2번

간단한 해설

다수기관의 시스템 장애, 침해사고의 확산 가능성 증가, 사이버안보 위해 가능성 고조는 **'주의' 단계**의 단서이다. '다수기관'이라는 표현만 보고 대규모 피해와 공조 대응이 필요한 '경계' 단계로 판단하지 않는다.

핵심 풀이

관심: 악성코드나 해킹기법으로 인한 피해 가능성이 커지거나, 해외 공격의 국내 유입이 우려되는 등 위협 징후에 주목하는 단계이다.

주의: 제시된 **다수기관의 정보통신망·정보시스템 장애 발생**, 정보유출 등 침해사고의 확산 가능성 증가, 정치·군사적 위기로 인한 사이버안보 위해 가능성 고조가 이 단계의 판단 단서이다. 단순히 공격 가능성에 관심을 두는 수준을 넘어 장애와 확산 위험에 대응할 필요가 커진 상황이다.

경계: 복수의 인터넷서비스제공자(ISP) 망이나 기간망에 피해가 생기거나, 대규모 침해사고·광범위한 피해 확산으로 다수기관의 공조 대응이 필요한 수준이다. 이 문항의 '다수기관'이라는 말만으로 경계로 판단하지 않고, **대규모 피해와 공조 대응 필요성**까지 구별한다.

심각: 전국적으로 네트워크·정보시스템을 사용할 수 없거나 핵심기반시설 피해로 국민 혼란이 발생하는 등 국가적 평가와 조치가 필요한 수준이다. 지문에는 이러한 전국적·국가적 피해가 제시되지 않았다.

따라서 세 가지 설명에 해당하는 단계는 ② '주의'이다.

NoteBase

문 10. 다음 ISMS-P의 최고책임자 지정 항목의 법률적 근거로 가장 적절하지 않은 것은?

최고경영자는 정보보호 업무를 총괄하는 정보보호 최고책임자와 개인정보보호 업무를 총괄하는 개인정보보호 책임자를 예산·인력 등 자원을 할당할 수 있는 임원급으로 지정하여야 한다.

① 개인정보 보호법 제29조(안전조치의무)

② 개인정보 보호법 제31조(개인정보 보호책임자의 지정)

③ 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제47조(정보보호 관리체계의 인증)

④ 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제45조의3(정보보호 최고책임자의 지정 등)

정답 3번

③

정보보호 관리체계가 인증기준에 적합한지를 확인하는 **인증제도**의 근거이다. 지문의 **정보보호 최고책임자 지정 의무**를 직접 규정한 조항은 제45조의3이다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제47조(정보보호 관리체계의 인증)
① 과학기술정보통신부장관은 정보통신망의 안정성 · 신뢰성 확보를 위하여 관리적 · 기술적 · 물리적 보호조치를 포함한 종합적 관리체계(이하 "정보보호 관리체계"라 한다)를 수립 · 운영하고 있는 자에 대하여 제4항에 따른 기준에 적합한지에 관하여 인증을 할 수 있다. <개정 2012.2.17, 2013.3.23, 2015.12.1, 2017.7.26>

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제45조의3(정보보호 최고책임자의 지정 등)
① 정보통신서비스 제공자는 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 대통령령으로 정하는 기준에 해당하는 임원(「상법」 제401조의2제1항제3호에 따른 자와 같은 법 제408조의2에 따른 집행임원을 포함한다)을 정보보호 최고책임자로 지정하고 과학기술정보통신부장관에게 신고하여야 하되, 「중소기업기본법」 제2조제2항에 따른 중기업의 정보보호 최고책임자의 지정에 대해서는 대통령령으로 정한다. 다만, 자산총액, 매출액 등이 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우에는 정보보호 최고책임자를 신고하지 아니할 수 있다. <개정 2014.5.28, 2017.7.26, 2018.6.12, 2021.6.8, 2026.3.31>

NoteBase

④

정보통신서비스 제공자에게 **정보보호 최고책임자를 지정할 의무**를 부과하는 조항이므로, 지문의 정보보호 최고책임자 지정에 관한 법적 근거이다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제45조의3(정보보호 최고책임자의 지정 등)
① 정보통신서비스 제공자는 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 대통령령으로 정하는 기준에 해당하는 임원(「상법」 제401조의2제1항제3호에 따른 자와 같은 법 제408조의2에 따른 집행임원을 포함한다)을 정보보호 최고책임자로 지정하고 과학기술정보통신부장관에게 신고하여야 하되, 「중소기업기본법」 제2조제2항에 따른 중기업의 정보보호 최고책임자의 지정에 대해서는 대통령령으로 정한다. 다만, 자산총액, 매출액 등이 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우에는 정보보호 최고책임자를 신고하지 아니할 수 있다. <개정 2014.5.28, 2017.7.26, 2018.6.12, 2021.6.8, 2026.3.31>

NoteBase

문 11. 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제26조(이용자 보호 등을 위한 정보 공개)에 관한 설명으로 가장 적절하지 않은 것은?

① 이용자는 클라우드컴퓨팅서비스 제공자에게 이용자 정보가 저장되는 국가의 명칭을 알려 줄 것을 요구할 수 있다.

② 과학기술정보통신부장관은 이용자 또는 정보통신서비스 이용자의 보호를 위하여 필요하다고 인정하는 경우에는 클라우드컴퓨팅서비스 제공자 또는 정보통신서비스 제공자에게 정보를 공개하도록 권고할 수 있다.

③ 정보통신서비스를 이용하는 자는 정보통신서비스 제공자에게 클라우드컴퓨팅서비스 이용 여부와 자신의 정보가 저장되는 국가의 명칭을 알려 줄 것을 요구할 수 있다.

④ 과학기술정보통신부장관이 정보를 공개하도록 권고하려는 경우에는 미리 개인정보보호위원회의 의견을 들어야 한다.

정답 4번

①

이용자는 클라우드컴퓨팅서비스 제공자에게 **이용자 정보가 저장되는 국가의 명칭**을 알려 달라고 요구할 수 있다.

클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제26조(이용자 보호 등을 위한 정보 공개)
① 이용자는 클라우드컴퓨팅서비스 제공자에게 이용자 정보가 저장되는 국가의 명칭을 알려 줄 것을 요구할 수 있다.

②

과학기술정보통신부장관은 이용자 보호에 필요하다고 인정하면 클라우드컴퓨팅서비스 제공자 또는 정보통신서비스 제공자에게 **클라우드컴퓨팅서비스 이용 여부와 정보 저장 국가에 관한 정보 공개를 권고할 수 있다**.

클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제26조(이용자 보호 등을 위한 정보 공개)
③ 과학기술정보통신부장관은 이용자 또는 정보통신서비스 이용자의 보호를 위하여 필요하다고 인정하는 경우에는 클라우드컴퓨팅서비스 제공자 또는 정보통신서비스 제공자에게 제1항 및 제2항에 따른 정보를 공개하도록 권고할 수 있다. <개정 2017.7.26>

NoteBase

③

정보통신서비스 이용자는 서비스 제공자에게 **클라우드컴퓨팅서비스 이용 여부와 자신의 정보가 저장되는 국가의 명칭**을 알려 달라고 요구할 수 있다.

클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제26조(이용자 보호 등을 위한 정보 공개)
② 정보통신서비스(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제2호에 따른 정보통신서비스를 말한다. 이하 제3항에서 같다)를 이용하는 자는 정보통신서비스 제공자(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제3호에 따른 정보통신서비스 제공자를 말한다. 이하 제3항에서 같다)에게 클라우드컴퓨팅서비스 이용 여부와 자신의 정보가 저장되는 국가의 명칭을 알려 줄 것을 요구할 수 있다.

④

과학기술정보통신부장관은 정보 공개를 권고하기 전에 **방송미디어통신위원회의 의견을 들어야 한다**.

클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제26조(이용자 보호 등을 위한 정보 공개)
④ 과학기술정보통신부장관이 제3항에 따라 정보를 공개하도록 권고하려는 경우에는 미리 방송미디어통신위원회의 의견을 들어야 한다. <개정 2017.7.26, 2025.10.1>

NoteBase

문 12. 「전자정부법」에서 정의한 용어에 관한 설명으로 가장 적절하지 않은 것은?

① “전자정부”란 정보기술을 활용하여 행정기관과 공공기관의 업무를 전자화하여 행정기관등의 상호 간의 행정업무 및 국민에 대한 행정업무를 효율적으로 수행하는 정부를 말한다.

② “행정기관”이란 국회·법원·헌법재판소·중앙선거관리위원회의 행정사무를 처리하는 기관, 중앙행정기관 및 그 소속 기관, 지방자치단체를 말한다.

③ “전자정부서비스”란 행정기관등이 전자정부를 통하여 다른 행정기관등 및 국민, 기업 등에 제공하는 행정서비스를 말한다.

④ “전자문서”란 종이문서와 그 밖에 전자적 형태로 작성되지 아니한 문서를 정보시스템이 처리할 수 있는 형태로 변환한 문서를 말한다.

정답 4번

①

전자정부는 **정보기술로 행정기관과 공공기관의 업무를 전자화**하여 기관 상호 간의 행정업무와 국민에 대한 행정업무를 효율적으로 수행하는 정부이다.

전자정부법 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다. <개정 2013.3.23, 2014.1.28, 2014.11.19, 2017.7.26, 2025.1.7>
1. "전자정부"란 정보기술을 활용하여 행정기관 및 공공기관(이하 "행정기관등"이라 한다)의 업무를 전자화하여 행정기관등의 상호 간의 행정업무 및 국민에 대한 행정업무를 효율적으로 수행하는 정부를 말한다.

②

행정기관에는 **국회·법원·헌법재판소·중앙선거관리위원회의 행정사무를 처리하는 기관, 중앙행정기관과 그 소속 기관, 지방자치단체**가 포함된다. 중앙행정기관에는 대통령 소속 기관과 국무총리 소속 기관도 포함된다.

전자정부법 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다. <개정 2013.3.23, 2014.1.28, 2014.11.19, 2017.7.26, 2025.1.7>
2. "행정기관"이란 국회 · 법원 · 헌법재판소 · 중앙선거관리위원회의 행정사무를 처리하는 기관, 중앙행정기관(대통령 소속 기관과 국무총리 소속 기관을 포함한다. 이하 같다) 및 그 소속 기관, 지방자치단체를 말한다.

NoteBase

③

전자정부서비스는 **행정기관등이 전자정부를 통하여 다른 행정기관등과 국민·기업 등에 제공하는 행정서비스**이다.

전자정부법 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다. <개정 2013.3.23, 2014.1.28, 2014.11.19, 2017.7.26, 2025.1.7>
5. "전자정부서비스"란 행정기관등이 전자정부를 통하여 다른 행정기관등 및 국민, 기업 등에 제공하는 행정서비스를 말한다.

④

종이문서 등 비전자문서를 정보시스템이 처리할 수 있는 형태로 변환한 문서는 **전자화문서**이다. 전자문서는 **정보처리능력을 지닌 장치로 전자적 형태로 작성되어 송수신되거나 저장되는 표준화된 정보**이다.

전자정부법 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다. <개정 2013.3.23, 2014.1.28, 2014.11.19, 2017.7.26, 2025.1.7>
7. "전자문서"란 컴퓨터 등 정보처리능력을 지닌 장치에 의하여 전자적인 형태로 작성되어 송수신되거나 저장되는 표준화된 정보를 말한다.
8. "전자화문서"란 종이문서와 그 밖에 전자적 형태로 작성되지 아니한 문서를 정보시스템이 처리할 수 있는 형태로 변환한 문서를 말한다.

NoteBase

문 13. 「개인정보 보호법」 제7조의2(보호위원회의 구성 등)에 따라 구성되는 개인정보보호위원회에서 위원 후보로 가장 적절한 자는?

① 개인정보 보호 업무를 담당하는 3급 이상 공무원(고위공무원단에 속하는 공무원을 포함한다)의 직에 있거나 있었던 사람

② 판사·검사·변호사의 직에 3년 이상 있거나 있었던 사람

③ 공공기관 또는 단체(개인정보처리자로 구성된 단체를 포함한다)에 2년 이상 임원으로 재직하였거나 이들 기관 또는 단체로부터 추천받은 사람으로서 개인정보 보호 업무를 2년 이상 담당하였던 사람

④ 개인정보 관련 분야에 전문지식이 있고 「고등교육법」 제2조 제1항에 따른 학교에서 조교수 이상으로 5년 이상 재직하고 있거나 재직하였던 사람

정답 1번

①

개인정보 보호 업무를 담당하는 **3급 이상 공무원(고위공무원단 소속 공무원 포함)**으로 재직 중이거나 재직한 사람은 위원 후보 자격에 해당한다.

개인정보 보호법 제7조의2(보호위원회의 구성 등)
② 보호위원회의 위원은 개인정보 보호에 관한 경력과 전문지식이 풍부한 다음 각 호의 사람 중에서 위원장과 부위원장은 국무총리의 제청으로, 그 외 위원 중 2명은 위원장의 제청으로, 2명은 대통령이 소속되거나 소속되었던 정당의 교섭단체 추천으로, 3명은 그 외의 교섭단체 추천으로 대통령이 임명 또는 위촉한다.
1. 개인정보 보호 업무를 담당하는 3급 이상 공무원(고위공무원단에 속하는 공무원을 포함한다)의 직에 있거나 있었던 사람

②

판사·검사·변호사의 직에 **10년 이상** 있거나 있었던 사람이어야 한다. 3년 이상이라는 경력 요건만으로는 부족하다.

개인정보 보호법 제7조의2(보호위원회의 구성 등)
② 보호위원회의 위원은 개인정보 보호에 관한 경력과 전문지식이 풍부한 다음 각 호의 사람 중에서 위원장과 부위원장은 국무총리의 제청으로, 그 외 위원 중 2명은 위원장의 제청으로, 2명은 대통령이 소속되거나 소속되었던 정당의 교섭단체 추천으로, 3명은 그 외의 교섭단체 추천으로 대통령이 임명 또는 위촉한다.
2. 판사 · 검사 · 변호사의 직에 10년 이상 있거나 있었던 사람

NoteBase

③

공공기관 또는 단체에서 **3년 이상 임원으로 재직하였거나 그 기관·단체로부터 추천받은 사람**으로서 **개인정보 보호 업무를 3년 이상** 담당한 사람이어야 한다. 선지는 두 경력 기간을 모두 2년으로 낮추었다.

개인정보 보호법 제7조의2(보호위원회의 구성 등)
② 보호위원회의 위원은 개인정보 보호에 관한 경력과 전문지식이 풍부한 다음 각 호의 사람 중에서 위원장과 부위원장은 국무총리의 제청으로, 그 외 위원 중 2명은 위원장의 제청으로, 2명은 대통령이 소속되거나 소속되었던 정당의 교섭단체 추천으로, 3명은 그 외의 교섭단체 추천으로 대통령이 임명 또는 위촉한다.
3. 공공기관 또는 단체(개인정보처리자로 구성된 단체를 포함한다)에 3년 이상 임원으로 재직하였거나 이들 기관 또는 단체로부터 추천받은 사람으로서 개인정보 보호 업무를 3년 이상 담당하였던 사람

④

교원 경력 요건은 **부교수 이상으로 5년 이상 재직 중이거나 재직한 것**이다. 조교수 이상이라는 요건만으로는 부족하다.

개인정보 보호법 제7조의2(보호위원회의 구성 등)
② 보호위원회의 위원은 개인정보 보호에 관한 경력과 전문지식이 풍부한 다음 각 호의 사람 중에서 위원장과 부위원장은 국무총리의 제청으로, 그 외 위원 중 2명은 위원장의 제청으로, 2명은 대통령이 소속되거나 소속되었던 정당의 교섭단체 추천으로, 3명은 그 외의 교섭단체 추천으로 대통령이 임명 또는 위촉한다.
4. 개인정보 관련 분야에 전문지식이 있고 「고등교육법」 제2조제1호에 따른 학교에서 부교수 이상으로 5년 이상 재직하고 있거나 재직하였던 사람

NoteBase

문 14. 「정보통신기반 보호법」상 주요정보통신기반시설보호계획의 수립에 관한 설명으로 가장 적절하지 않은 것은?

① 관계중앙행정기관의 장은 전년도 주요정보통신기반시설보호계획의 추진실적과 다음 연도의 주요정보통신기반시설보호계획을 위원회에 제출하여 그 심의를 받아야 한다. 다만, 위원회의 위원장이 보안이 요구된다고 인정하는 사항에 대하여는 그러하지 아니하다.

② 과학기술정보통신부장관과 방송통신위원장은 협의하여 주요정보통신기반시설보호대책 및 주요정보통신기반시설보호계획의 수립지침을 정하여 이를 관계중앙행정기관의 장에게 통보할 수 있다.

③ 주요정보통신기반시설보호계획에는 주요정보통신기반시설의 취약점 분석·평가에 관한 사항이 포함되어야 한다.

④ 관계중앙행정기관의 장은 소관분야의 주요정보통신기반시설의 보호에 관한 업무를 총괄하는 자를 지정하여야 한다.

정답 2번

①

관계중앙행정기관의 장은 **전년도 추진실적과 다음 연도 보호계획을 위원회에 제출하여 심의**를 받아야 한다. 다만, **위원장이 보안이 요구된다고 인정하는 사항은 예외**이다.

정보통신기반 보호법 제6조(주요정보통신기반시설보호계획의 수립 등)
②관계중앙행정기관의 장은 전년도 주요정보통신기반시설보호계획의 추진실적과 다음 연도의 주요정보통신기반시설보호계획을 위원회에 제출하여 그 심의를 받아야 한다. 다만, 위원회의 위원장이 보안이 요구된다고 인정하는 사항에 대하여는 그러하지 아니하다.

②

보호대책과 보호계획의 수립지침을 협의하여 정하는 주체는 **과학기술정보통신부장관과 국가정보원장**이다. 선지는 국가정보원장을 방송통신위원장으로 잘못 제시하였다.

정보통신기반 보호법 제6조(주요정보통신기반시설보호계획의 수립 등)
④과학기술정보통신부장관과 국가정보원장은 협의하여 주요정보통신기반시설보호대책 및 주요정보통신기반시설보호계획의 수립지침을 정하여 이를 관계중앙행정기관의 장에게 통보할 수 있다. <개정 2007.12.21, 2008.2.29, 2013.3.23, 2017.7.26>

NoteBase

③

주요정보통신기반시설보호계획에는 **주요정보통신기반시설의 취약점 분석·평가에 관한 사항을 반드시 포함**하여야 한다.

정보통신기반 보호법 제6조(주요정보통신기반시설보호계획의 수립 등)
③주요정보통신기반시설보호계획에는 다음 각호의 사항이 포함되어야 한다. <개정 2015.1.20>
1. 주요정보통신기반시설의 취약점 분석 · 평가에 관한 사항

④

관계중앙행정기관의 장은 소관분야의 주요정보통신기반시설 **보호업무를 총괄하는 정보보호책임관을 지정**하여야 한다.

정보통신기반 보호법 제6조(주요정보통신기반시설보호계획의 수립 등)
⑤관계중앙행정기관의 장은 소관분야의 주요정보통신기반시설의 보호에 관한 업무를 총괄하는 자(이하 "정보보호책임관"이라 한다)를 지정하여야 한다.

NoteBase

문 15. 다음 「전자금융거래법」 위반 행위를 한 자 중 법정형이 나머지와 다른 하나는?

① 위조되거나 변조된 접근매체를 판매알선·판매·수출 또는 수입하거나 사용한 자

② 전자금융기반시설에 접근하거나 저장된 데이터를 조작·파괴·은닉 또는 유출한 자

③ 분실되거나 도난된 접근매체를 판매알선·판매·수출 또는 수입하거나 사용한 자

④ 강제로 빼앗거나, 횡령하거나, 사람을 속이거나 공갈하여 획득한 접근매체를 판매알선·판매·수출 또는 수입하거나 사용한 자

정답 2번

공통 해설

②의 전자금융기반시설 침해행위는 **10년 이하의 징역 또는 1억원 이하의 벌금**에 처한다. ①·③·④의 접근매체 관련 위반행위는 모두 **7년 이하의 징역 또는 5천만원 이하의 벌금**에 처하므로 법정형이 다르다.

전자금융거래법 제49조(벌칙)
① 다음 각 호의 어느 하나에 해당하는 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처한다. <신설 2014.10.15, 2025.12.16>
1. 제21조의4제1호를 위반하여 전자금융기반시설에 접근하거나 저장된 데이터를 조작 · 파괴 · 은닉 또는 유출한 자
②다음 각 호의 어느 하나에 해당하는 자는 7년 이하의 징역 또는 5천만원 이하의 벌금에 처한다. <개정 2013.5.22, 2014.10.15>
2. 위조되거나 변조된 접근매체를 판매알선 · 판매 · 수출 또는 수입하거나 사용한 자
3. 분실되거나 도난된 접근매체를 판매알선 · 판매 · 수출 또는 수입하거나 사용한 자
5. 강제로 빼앗거나, 횡령하거나, 사람을 속이거나 공갈하여 획득한 접근매체를 판매알선 · 판매 · 수출 또는 수입하거나 사용한 자

NoteBase

문 16. 다음 「전자금융거래법」 제22조(전자금융거래기록의 생성·보존 및 파기)의 일부분으로 ㉠, ㉡에 해당하는 가장 적절한 것은?

· 금융회사등은 전자금융거래의 내용을 추적·검색하거나 그 내용에 오류가 발생할 경우에 이를 확인하거나 정정할 수 있는 기록을 생성하여 (㉠)의 범위 안에서 대통령령이 정하는 기간동안 보존하여야 한다.
· 금융회사등은 제1항에 따라 보존하여야 하는 기간이 경과하고 금융거래 등 상거래관계가 종료된 경우에는 (㉡) 이내에 전자금융거래기록을 파기하여야 한다.

① ㉠: 3년, ㉡: 5년
② ㉠: 5년, ㉡: 3년
③ ㉠: 5년, ㉡: 5년
④ ㉠: 3년, ㉡: 3년

정답 3번

㉠

금융회사등은 거래내용의 추적·검색 및 오류 확인·정정을 위한 기록을 생성하여 **5년의 범위 안에서 대통령령이 정하는 기간** 동안 보존하여야 한다.

전자금융거래법 제22조(전자금융거래기록의 생성 · 보존 및 파기)
①금융회사등은 전자금융거래의 내용을 추적 · 검색하거나 그 내용에 오류가 발생할 경우에 이를 확인하거나 정정할 수 있는 기록(이하 이 조에서 "전자금융거래기록"이라 한다)을 생성하여 5년의 범위 안에서 대통령령이 정하는 기간동안 보존하여야 한다. <개정 2013.5.22, 2014.10.15>

㉡

금융회사등은 **법정 보존기간이 경과하고 상거래관계가 종료되면 5년 이내**에 전자금융거래기록을 파기하여야 한다. 신용정보는 이 파기 대상에서 제외되며, 다른 법률상 의무 이행에 불가피하거나 금융위원회가 정한 보관 필요 사유가 있으면 파기 의무의 예외가 된다.

전자금융거래법 제22조(전자금융거래기록의 생성 · 보존 및 파기)
② 금융회사등은 제1항에 따라 보존하여야 하는 기간이 경과하고 금융거래 등 상거래관계가 종료된 경우에는 5년 이내에 전자금융거래기록(「신용정보의 이용 및 보호에 관한 법률」에 따른 신용정보는 제외한다. 이하 이 항에서 같다)을 파기하여야 한다. 다만, 다음 각 호의 경우에는 그러하지 아니하다. <신설 2014.10.15>
1. 다른 법률에 따른 의무를 이행하기 위하여 불가피한 경우
2. 그 밖에 전자금융거래기록을 보관할 필요성이 있는 경우로서 금융위원회가 정하는 경우

NoteBase

문 17. 「전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법」 제4조(지급정지)에 따라 금융회사는 거래내역 등의 확인을 통하여 전기통신금융사기(속칭 보이스피싱)에 이용된 계좌로 의심할 만한 사정이 있다고 인정되면 계좌 지급정지 조치를 하여야 하는바, 이에 해당하는 경우로 가장 적절하지 않은 것은?

① 피해자의 피해구제 신청이 있는 경우

② 수사기관 또는 금융감독원 등으로부터 사기이용계좌로 의심된다는 정보제공이 있는 경우

③ 피해의심거래계좌에 대한 본인확인조치 결과 명의도용 계좌로 추정되는 경우

④ 금융기관의 지급정지 요청이 있는 경우

정답 3번

①

피해자의 피해구제 신청이 있고 거래내역 확인 결과 사기이용계좌등으로 의심할 만한 사정이 인정되면, 금융회사등은 즉시 해당 계좌등 전부를 지급정지해야 한다.

전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법 제4조(지급정지)
① 금융회사등은 다음 각 호의 어느 하나에 해당하는 경우 거래내역 등의 확인을 통하여 전기통신금융사기의 사기이용계좌등으로 의심할 만한 사정이 있다고 인정되면 즉시 해당 사기이용계좌등의 전부에 대하여 지급정지 조치를 하여야 한다. <개정 2014.1.28, 2023.5.16, 2024.2.27, 2026.3.31>
1. 제3조제1항에 따른 피해구제 신청이나 같은 조 제2항 또는 제4항에 따른 지급정지 요청이 있는 경우

②

수사기관이나 금융감독원 등의 사기이용계좌 의심 정보 제공은 지급정지 사유이다. 금융회사등은 거래내역 확인 결과 의심할 만한 사정이 인정되면 즉시 해당 계좌등 전부를 지급정지해야 한다.

전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법 제4조(지급정지)
① 금융회사등은 다음 각 호의 어느 하나에 해당하는 경우 거래내역 등의 확인을 통하여 전기통신금융사기의 사기이용계좌등으로 의심할 만한 사정이 있다고 인정되면 즉시 해당 사기이용계좌등의 전부에 대하여 지급정지 조치를 하여야 한다. <개정 2014.1.28, 2023.5.16, 2024.2.27, 2026.3.31>
2. 수사기관 또는 「금융위원회의 설치 등에 관한 법률」에 따라 설립된 금융감독원(이하 "금융감독원"이라 한다) 등으로부터 사기이용계좌등으로 의심된다는 정보제공이 있는 경우

NoteBase

③

본인확인조치 결과 **사기이용계좌등으로 추정되는 경우**가 지급정지 사유이다. 단순히 명의도용 계좌로 추정되는 경우를 규정한 것이 아니다.

전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법 제4조(지급정지)
① 금융회사등은 다음 각 호의 어느 하나에 해당하는 경우 거래내역 등의 확인을 통하여 전기통신금융사기의 사기이용계좌등으로 의심할 만한 사정이 있다고 인정되면 즉시 해당 사기이용계좌등의 전부에 대하여 지급정지 조치를 하여야 한다. <개정 2014.1.28, 2023.5.16, 2024.2.27, 2026.3.31>
3. 제2조의5제2항에 따른 피해의심거래계좌등에 대한 본인확인조치 결과 사기이용계좌등으로 추정되는 경우

④

피해구제 신청 등을 받은 금융회사등은 피해자산이 다른 금융회사등의 사기이용계좌등으로 송금·이체·이전되면 해당 금융회사등에 지급정지를 요청해야 한다. **이러한 금융회사등의 지급정지 요청**도 법정 지급정지 사유이다.

전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법 제3조(피해구제의 신청 등)
④ 제1항에 따른 피해구제의 신청 및 제2항에 따른 지급정지의 요청을 받은 금융회사등은 다른 금융회사등의 사기이용계좌등으로 피해자산이 송금 · 이체 또는 이전된 경우 해당 금융회사등에 대하여 필요한 정보를 제공하고 지급정지를 요청하여야 한다. <개정 2023.5.16, 2026.3.31>

전기통신금융사기 피해 방지 및 피해자산 환급에 관한 특별법 제4조(지급정지)
① 금융회사등은 다음 각 호의 어느 하나에 해당하는 경우 거래내역 등의 확인을 통하여 전기통신금융사기의 사기이용계좌등으로 의심할 만한 사정이 있다고 인정되면 즉시 해당 사기이용계좌등의 전부에 대하여 지급정지 조치를 하여야 한다. <개정 2014.1.28, 2023.5.16, 2024.2.27, 2026.3.31>
1. 제3조제1항에 따른 피해구제 신청이나 같은 조 제2항 또는 제4항에 따른 지급정지 요청이 있는 경우

NoteBase

문 18. 다음은 「위치정보의 보호 및 이용 등에 관한 법률」 제29조 제2항의 내용이다. 밑줄 친 부분에 해당하지 않는 것은?

「국가경찰과 자치경찰의 조직 및 운영에 관한 법률」에 따른 경찰청·시·도경찰청·경찰서(이하 “경찰관서”라 한다)는 위치정보사업자에게 다음 각 호의 어느 하나에 해당하는 개인위치정보의 제공을 요청할 수 있다.

① 생명·신체를 위협하는 급박한 위험으로부터 자신 또는 다른 사람 등 구조가 필요한 사람을 보호하기 위하여 구조를 요청한 경우 구조를 요청한 자의 개인위치정보

② 구조받을 사람이 다른 사람에게 구조를 요청한 경우 구조받을 사람의 개인위치정보

③ 실종아동등의 생명·신체를 보호하기 위하여 보호자가 실종아동등에 대한 긴급구조를 요청한 경우 실종아동등의 개인위치정보

④ 실종아동등이 구조된 후 2촌 이내의 친족과의 연락이 필요한 경우 2촌 이내 친족의 개인위치정보

정답 4번

①

급박한 생명·신체의 위험에서 자신이나 다른 사람을 보호하려고 구조를 요청한 경우에는 **구조를 요청한 사람의 개인위치정보**를 요청할 수 있다. 다만, 다른 사람을 위해 구조를 요청한 **목격자의 위치정보를 제공받으려면 그 목격자의 동의**가 필요하다.

위치정보의 보호 및 이용 등에 관한 법률 제29조(긴급구조를 위한 개인위치정보의 이용)
② 「국가경찰과 자치경찰의 조직 및 운영에 관한 법률」에 따른 경찰청 · 시 · 도경찰청 · 경찰서(이하 "경찰관서"라 한다)는 위치정보사업자에게 다음 각 호의 어느 하나에 해당하는 개인위치정보의 제공을 요청할 수 있다. 다만, 제1호에 따라 경찰관서가 다른 사람의 생명 · 신체를 보호하기 위하여 구조를 요청한 자(이하 "목격자"라 한다)의 개인위치정보를 제공받으려면 목격자의 동의를 받아야 한다. <개정 2020.12.22>
1. 생명 · 신체를 위협하는 급박한 위험으로부터 자신 또는 다른 사람 등 구조가 필요한 사람(이하 "구조받을 사람"이라 한다)을 보호하기 위하여 구조를 요청한 경우 구조를 요청한 자의 개인위치정보
2. 구조받을 사람이 다른 사람에게 구조를 요청한 경우 구조받을 사람의 개인위치정보
3. 「실종아동등의 보호 및 지원에 관한 법률」 제2조제2호에 따른 실종아동등(이하 "실종아동등"이라 한다)의 생명 · 신체를 보호하기 위하여 같은 법 제2조제3호에 따른 보호자(이하 "보호자"라 한다)가 실종아동등에 대한 긴급구조를 요청한 경우 실종아동등의 개인위치정보

NoteBase

②

구조받을 사람이 다른 사람에게 구조를 요청한 경우에는 **구조받을 사람의 개인위치정보**가 제공 요청의 대상이다. 다른 사람이 경찰관서에 구조를 요청하면 경찰관서는 **구조받을 사람의 의사**를 확인하여야 한다.

위치정보의 보호 및 이용 등에 관한 법률 제29조(긴급구조를 위한 개인위치정보의 이용)
② 「국가경찰과 자치경찰의 조직 및 운영에 관한 법률」에 따른 경찰청 · 시 · 도경찰청 · 경찰서(이하 "경찰관서"라 한다)는 위치정보사업자에게 다음 각 호의 어느 하나에 해당하는 개인위치정보의 제공을 요청할 수 있다. 다만, 제1호에 따라 경찰관서가 다른 사람의 생명 · 신체를 보호하기 위하여 구조를 요청한 자(이하 "목격자"라 한다)의 개인위치정보를 제공받으려면 목격자의 동의를 받아야 한다. <개정 2020.12.22>
2. 구조받을 사람이 다른 사람에게 구조를 요청한 경우 구조받을 사람의 개인위치정보
③ 제2항제2호에 따라 다른 사람이 경찰관서에 구조를 요청한 경우 경찰관서는 구조받을 사람의 의사를 확인하여야 한다.

③

보호자가 실종아동등의 생명·신체를 보호하기 위해 긴급구조를 요청한 경우에는 **실종아동등 본인의 개인위치정보**를 요청할 수 있다.

위치정보의 보호 및 이용 등에 관한 법률 제29조(긴급구조를 위한 개인위치정보의 이용)
② 「국가경찰과 자치경찰의 조직 및 운영에 관한 법률」에 따른 경찰청 · 시 · 도경찰청 · 경찰서(이하 "경찰관서"라 한다)는 위치정보사업자에게 다음 각 호의 어느 하나에 해당하는 개인위치정보의 제공을 요청할 수 있다. 다만, 제1호에 따라 경찰관서가 다른 사람의 생명 · 신체를 보호하기 위하여 구조를 요청한 자(이하 "목격자"라 한다)의 개인위치정보를 제공받으려면 목격자의 동의를 받아야 한다. <개정 2020.12.22>
3. 「실종아동등의 보호 및 지원에 관한 법률」 제2조제2호에 따른 실종아동등(이하 "실종아동등"이라 한다)의 생명 · 신체를 보호하기 위하여 같은 법 제2조제3호에 따른 보호자(이하 "보호자"라 한다)가 실종아동등에 대한 긴급구조를 요청한 경우 실종아동등의 개인위치정보

NoteBase

④

실종아동등의 긴급구조를 위해 요청할 수 있는 정보는 **실종아동등 본인의 개인위치정보**이다. **구조 후 친족과 연락하기 위한 그 친족의 개인위치정보**는 이 요청 대상에 포함되지 않는다.

위치정보의 보호 및 이용 등에 관한 법률 제29조(긴급구조를 위한 개인위치정보의 이용)
② 「국가경찰과 자치경찰의 조직 및 운영에 관한 법률」에 따른 경찰청 · 시 · 도경찰청 · 경찰서(이하 "경찰관서"라 한다)는 위치정보사업자에게 다음 각 호의 어느 하나에 해당하는 개인위치정보의 제공을 요청할 수 있다. 다만, 제1호에 따라 경찰관서가 다른 사람의 생명 · 신체를 보호하기 위하여 구조를 요청한 자(이하 "목격자"라 한다)의 개인위치정보를 제공받으려면 목격자의 동의를 받아야 한다. <개정 2020.12.22>
1. 생명 · 신체를 위협하는 급박한 위험으로부터 자신 또는 다른 사람 등 구조가 필요한 사람(이하 "구조받을 사람"이라 한다)을 보호하기 위하여 구조를 요청한 경우 구조를 요청한 자의 개인위치정보
2. 구조받을 사람이 다른 사람에게 구조를 요청한 경우 구조받을 사람의 개인위치정보
3. 「실종아동등의 보호 및 지원에 관한 법률」 제2조제2호에 따른 실종아동등(이하 "실종아동등"이라 한다)의 생명 · 신체를 보호하기 위하여 같은 법 제2조제3호에 따른 보호자(이하 "보호자"라 한다)가 실종아동등에 대한 긴급구조를 요청한 경우 실종아동등의 개인위치정보

NoteBase

문 19. 다음 「개인정보 보호법」 제2조에서 정의하는 용어에 관해 ㉠, ㉡에 해당하는 가장 적절한 것은?

1. ‘개인정보’란 (㉠) 개인에 관한 정보로서 다음 각 목의 어느 하나에 해당하는 정보를 말한다.
가. 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보
나. 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보. 이 경우 쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려하여야 한다.
다. 가목 또는 나목을 제1호의2에 따라 (㉡)함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보
1의2. (㉡)란 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것을 말한다.

① 보호할 가명처리
② 살아 있는 개인정보처리
③ 살아 있는 가명처리
④ 보호할 개인정보처리

정답 3번

㉠
개인정보는 **살아 있는 개인**에 관한 정보로서, **그 자체로 개인을 알아볼 수 있는 정보, 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보, 가명정보**를 포함한다. 쉽게 결합할 수 있는지는 다른 정보의 입수 가능성과 개인을 알아보는 데 드는 시간·비용·기술 등을 합리적으로 고려하여 판단한다.

개인정보 보호법 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다. <개정 2014.3.24, 2020.2.4, 2023.3.14>
1. "개인정보"란 살아 있는 개인에 관한 정보로서 다음 각 목의 어느 하나에 해당하는 정보를 말한다.
가. 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보
나. 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보. 이 경우 쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려하여야 한다.
다. 가목 또는 나목을 제1호의2에 따라 가명처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용 · 결합 없이는 특정 개인을 알아볼 수 없는 정보(이하 "가명정보"라 한다)

NoteBase

ㄴ

가명처리는 개인정보의 **일부를 삭제하거나 일부 또는 전부를 대체**하는 등의 방법으로 **추가 정보 없이는 특정 개인을 알아볼 수 없도록 처리**하는 것이다.

개인정보 보호법 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다. <개정 2014.3.24, 2020.2.4, 2023.3.14>
1의2. "가명처리"란 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것을 말한다.

NoteBase

문 20. 「정보통신기반 보호법」 제8조(주요정보통신기반시설의 지정 등)에 따라 중앙행정기관의 장은 소관 분야의 정보통신기반시설 중 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정할 수 있다. 이때 고려해야 할 사항으로 가장 적절하지 않은 것은?

① 정보통신기반시설을 관리하는 기관이 수행하는 업무의 국가 사회적 중요성

② 정보통신기반시설을 관리하는 기관이 수행하는 업무의 정보통신기반시설에 대한 의존도

③ 다른 정보통신기반시설과의 분리 독립성

④ 침해사고가 발생할 경우 국가안전보장과 경제사회에 미치는 피해규모 및 범위

정답 3번

①

주요정보통신기반시설 지정 시 관리기관이 수행하는 업무의 **국가사회적 중요성**을 고려한다.

정보통신기반 보호법 제8조(주요정보통신기반시설의 지정 등)
①중앙행정기관의 장은 소관분야의 정보통신기반시설중 다음 각호의 사항을 고려하여 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정할 수 있다. <개정 2019.12.10, 2020.6.9>
1. 해당 정보통신기반시설을 관리하는 기관이 수행하는 업무의 국가사회적 중요성

②

주요정보통신기반시설 지정 시 관리기관이 수행하는 업무의 **정보통신기반시설에 대한 의존도**를 고려한다.

정보통신기반 보호법 제8조(주요정보통신기반시설의 지정 등)
①중앙행정기관의 장은 소관분야의 정보통신기반시설중 다음 각호의 사항을 고려하여 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정할 수 있다. <개정 2019.12.10, 2020.6.9>
2. 제1호에 따른 기관이 수행하는 업무의 정보통신기반시설에 대한 의존도

NoteBase

③

주요정보통신기반시설 지정 시 고려하는 것은 다른 정보통신기반시설과의 분리·독립성이 아니라 **상호연계성**이다.

정보통신기반 보호법 제8조(주요정보통신기반시설의 지정 등)
①중앙행정기관의 장은 소관분야의 정보통신기반시설중 다음 각호의 사항을 고려하여 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정할 수 있다. <개정 2019.12.10, 2020.6.9>
3. 다른 정보통신기반시설과의 상호연계성

④

주요정보통신기반시설 지정 시 침해사고가 발생할 경우 **국가안전보장과 경제사회에 미치는 피해규모 및 범위**를 고려한다.

정보통신기반 보호법 제8조(주요정보통신기반시설의 지정 등)
①중앙행정기관의 장은 소관분야의 정보통신기반시설중 다음 각호의 사항을 고려하여 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정할 수 있다. <개정 2019.12.10, 2020.6.9>
4. 침해사고가 발생할 경우 국가안전보장과 경제사회에 미치는 피해규모 및 범위

NoteBase