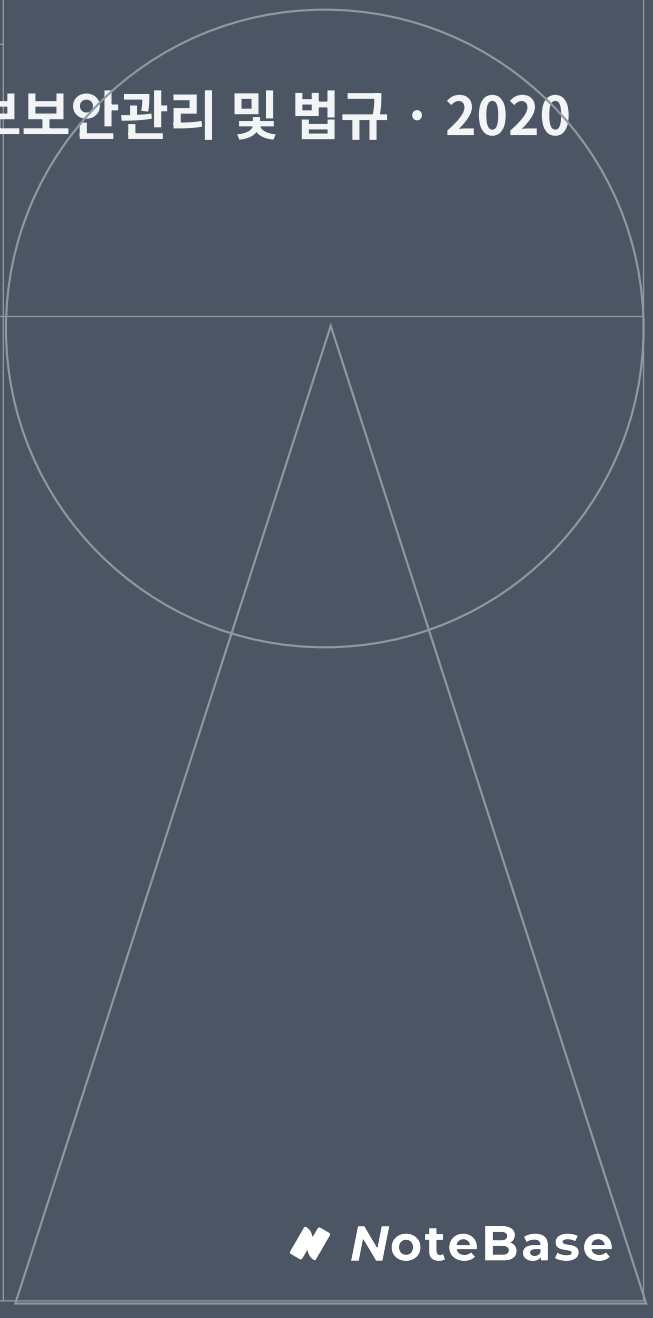
기출OX 해설집

공무원/경찰/경력채용 · 정보보안관리 및 법규 · 2020



NoteBase

기출OX 해설집

공무원/경찰/경력채용 · 정보보안관리 및 법규 · 2020

공무원/경찰/경력채용 · 정보보안관리 및 법규 · 2020

문 1. 물리적 보안에 해당하는 내용으로 가장 적절하지 않은 것은?

① 운영 서버 시스템의 도난 방지 또는 파괴 방지

② 정보시스템과 네트워크장비들의 위치 공간 분리

③ 조직 구성원의 보안구역 출입 통제

④ 조직 내 정보보안의 정책과 절차 수립

정답 4번

간단한 해설

장비와 공간을 직접 보호하는 조치는 물리적 보안에 해당한다. 조직의 보안 정책과 절차를 수립하는 ④는 **관리적 보안**이다.

선지별 해설

① O: 서버의 도난이나 파괴를 막는 것은 **장비 자체를 보호**하는 물리적 보안이다. 잠금장치, 보호용 함체, 감시·경비 등을 통해 장비의 무단 반출이나 훼손 위험을 줄일 수 있다.

② O: 정보시스템과 네트워크장비의 설치 위치를 나누는 것은 **물리적 공간을 분리**하는 조치이다. 구역별로 접근을 제한하고 한 구역의 사고가 다른 장비에 미치는 영향을 줄이는 데 활용할 수 있다. 논리적 주소나 통신 규칙만으로 나누는 네트워크 분리와 구별한다.

③ O: 보안구역 출입 통제는 허가된 사람만 해당 장소에 들어오게 하는 **물리적 접근 통제**이다. 조직 구성원이라도 업무상 출입 권한이 없는 구역에는 들어가지 못하게 할 수 있으며, 출입카드·문 잠금장치·경비 인력 등이 쓰인다.

④ X: 조직의 보안 정책과 절차를 수립하는 것은 책임, 기준, 수행 방법을 정하는 **관리적 보안**에 해당한다. 물리적 보안 조치를 운영하는 정책도 필요하지만, 정책을 수립하는 행위 자체와 출입 통제·장비 보호 같은 물리적 조치의 시행은 구별한다.

NoteBase

문 2. 정보보호 대책 수립을 위한 대응 전략으로 가장 적절하지 않은 것은?

① 위험전가는 위험이 발생하는 원인을 제3자를 통해 제거한다.

② 위험감소는 위험을 줄일 수 있는 대책을 채택하여 구현한다.

③ 위험회피는 위험이 존재하는 프로세스나 사업을 수행하지 않는다.

④ 위험수용은 식별된 위험을 받아들이고 비용을 감수한다.

정답 1번

간단한 해설

위험전가는 위험의 원인을 없애는 것이 아니라 **손실 부담이나 책임을 다른 주체에게 이전**하는 전략이다. 보험에 가입해도 사고 가능성이 사라지지는 않는다.

선지별 해설

① X: 위험전가는 보험이나 계약 등을 통해 **손실 부담이나 책임을 제3자에게 이전**하는 전략이다. 위험의 발생 원인 자체를 제거하는 것은 아니다. 예를 들어 보험에 가입해도 사고 가능성은 남지만 약정된 손실을 보험자가 부담한다.

② O: 위험감소는 보호대책을 실제로 적용하여 **발생 가능성이나 피해 규모를 낮추는** 전략이다. 접근통제 강화나 취약점 보완 등이 이에 해당한다.

③ O: 위험회피는 위험을 일으키는 활동을 시작하지 않거나 중단하여 그 위험에 노출되지 않도록 하는 전략이다. 위험이 있는 사업을 수행하지 않는 것은 회피의 예이다.

④ O: 위험수용은 식별된 위험과 그 영향을 이해한 뒤 조직이 이를 감당하기로 결정하는 전략이다. 사고가 발생하면 그에 따른 손실이나 비용을 부담하므로, 위험을 모르고 방치하는 것과는 다르다.

따라서 위험전가를 원인 제거로 설명한 ①이 가장 적절하지 않다.

NoteBase

문 3. ISO 27001에서 제시한 정보보안관리 PDCA 모델의 단계별 이행내용으로 가장 적절하지 않은 것은?

① Plan 단계에서 보안 정책, 목적, 프로세스 및 절차를 수립한다.

② Do 단계에서 정책, 통제, 위험처리 프로세스를 구현하고 수행한다.

③ Check 단계에서 프로세스 수행을 모니터링하고 점검한다.

④ Approve 단계에서 프로세스 진행에 대한 최고경영진의 승인을 획득한다.

정답 4번

간단한 해설

PDCA는 Plan, Do, Check, **Act**의 순환이다. A는 승인 획득을 뜻하는 Approve가 아니라, 점검 결과를 반영하여 관리체계를 **시정·개선하는 단계**를 뜻한다.

선지별 해설

① O: **Plan은 계획 수립 단계**이다. 정보보안 목표를 달성할 수 있도록 보안 정책과 목적을 정하고, 이를 실행할 프로세스와 절차를 수립한다. 무엇을 어떤 방법으로 수행할지 정하는 내용이므로 적절하다.

② O: **Do는 구현·운영 단계**이다. 계획한 정책과 통제를 실제로 적용하고 위험처리 프로세스를 수행하여 정보보안관리체계를 운영한다. 수립한 계획을 실행한다는 점이 핵심이다.

③ O: **Check는 점검·평가 단계**이다. 프로세스의 수행 상태와 결과를 모니터링하고, 정책과 목표에 맞게 운영되는지 확인한다. 점검 결과는 이후 개선 조치의 근거가 된다.

④ X: PDCA의 A는 **Act**이며 Approve가 아니다. Act는 점검 결과에 따라 필요한 시정 조치와 개선을 실행하여 관리체계를 지속적으로 보완하는 단계이다. 최고경영진의 승인이 필요할 수 있다는 사실과 별개로, 승인 획득을 독립된 PDCA의 네 번째 단계로 제시한 설명은 틀리다.

NoteBase

문 4. 정보보호 위험관리를 위한 요소와 설명으로 가장 적절하게 짝지어진 것은?

<요소>
(가) 자산 (Asset)
(나) 위험 (Risk)
(다) 위협 (Threat)
(라) 취약점 (Vulnerability)

<설명>
㉠ 보호 대상에 손실 및 피해를 유발할 가능성
㉡ 악의적인 공격이 발생하기 위한 조건 및 상황
㉢ 조직에서 보호해야 할 가치가 있는 자원
㉣ 보호 대상에 악영향을 미칠 수 있는 사건·행위

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

정답 3번

간단한 해설

자산은 보호할 자원, 위협은 해를 줄 수 있는 사건·행위, 취약점은 악용될 수 있는 약점이다. 위험은 **피해의 발생 가능성과 영향**을 함께 판단하는 개념으로 구별한다.

NoteBase

대응 관계 해설

(가) 자산 → ㉢: 자산은 조직이 **보호할 가치가 있는 자원**이다. 정보, 서버, 소프트웨어, 인력 등 업무 수행에 중요한 대상을 포함하며, 위험관리에서는 무엇을 보호할지 정하는 출발점이 된다.

(나) 위험 → ㉠: 위험은 보호 대상에 **손실·피해가 생길 가능성과 그 영향**을 함께 고려하는 개념이다. ㉠은 이 가운데 피해가 발생할 가능성을 중심으로 표현한 설명이다. 단순히 위협이 존재하는지와 달리 실제 피해의 발생 가능성과 크기를 평가한다.

(다) 위협 → ㉣: 위협은 자산에 악영향을 줄 수 있는 **사건이나 행위**이다. 침입·악성코드 공격 같은 의도적 행위뿐 아니라 화재나 장비 사고 등도 위협이 될 수 있다. 보호 대상 자체인 자산이나 대상에 내재한 약점과 구별한다.

(라) 취약점 → ㉡: 취약점은 위협에 의해 악용되거나 촉발될 수 있는 **시스템·절차·통제의 약점**이다. 원문의 공격이 발생하기 위한 조건·상황은 여기서 공격을 가능하게 하는 보안상 약점을 뜻한다. 예를 들어 보안 패치 누락나 허술한 출입 통제가 취약점이며, 취약점이 있다는 사실만으로 사고가 이미 발생한 것은 아니다.

따라서 (가)－㉢, (나)－㉠, (다)－㉣, (라)－㉡으로 연결되는 ③이 정답이다.

NoteBase

문 5. BCP(Business Continuity Planning) 5단계 접근방법론을 통한 복구 프로세스 개발 절차이다. ㉠~㉢에 들어갈 단계들이 가장 적절한 순서로 배열된 것은?

BCP 정책 및 계획수립 → ㉠ → ㉡ → ㉢ → 수행테스트 및 유지보수

① ㉠: 사업영향평가, ㉡: 복구전략개발, ㉢: 복구계획수립

② ㉠: 복구전략개발, ㉡: 사업영향평가, ㉢: 복구계획수립

③ ㉠: 사업영향평가, ㉡: 복구계획수립, ㉢: 복구전략개발

④ ㉠: 복구전략개발, ㉡: 복구계획수립, ㉢: 사업영향평가

정답 1번

간단한 해설

먼저 업무 중단의 영향을 분석해 복구 요구를 파악해야 한다. 그 요구에 맞는 **복구 방법을 선택한 뒤 실행 절차를 문서화**하므로, 복구전략개발은 사업영향평가 이후이자 복구계획수립 이전에 놓인다.

올바른 순서

BCP 정책 및 계획수립 → 사업영향평가 → 복구전략개발 → 복구계획수립 → 수행테스트 및 유지보수

BCP 정책 및 계획수립: 업무연속성 확보의 목적과 적용 범위, 추진 조직과 책임, 일정 등을 정한다. 이후 분석과 복구 방안을 마련할 **공통 기준과 추진 체계**를 갖추는 단계이다.

㉠ 사업영향평가: 업무 중단이 조직에 미치는 손실과 파급효과, 핵심 업무와 의존 자원을 분석한다. 이를 통해 **복구 우선순위와 허용 가능한 중단시간**을 파악해야 어떤 수준의 복구가 필요한지 판단할 수 있다.

㉡ 복구전략개발: 사업영향평가 결과를 바탕으로 백업, 대체 시설, 인력·자원 확보 등 가능한 복구 방안을 검토하고 선택한다. **필요한 복구 수준을 충족할 방법**을 결정하는 단계이므로 영향평가보다 앞설 수 없다.

㉢ 복구계획수립: 선택한 전략을 실제 실행할 수 있도록 복구 절차, 담당자, 연락 체계와 필요한 자원을 구체화하고 문서화한다. **결정된 전략을 실행 절차로 구체화**하는 것이므로 복구전략개발 다음에 놓인다.

수행테스트 및 유지보수: 수립한 계획대로 복구할 수 있는지 시험·훈련하여 누락이나 실행상의 문제를 확인한다. 발견한 문제와 업무·시스템의 변경사항을 반영해 계획을 수정함으로써 **실행 가능성을 검증하고 최신 상태를 유지**한다.

NoteBase

문 6. 재해복구 수준별 핵심 지표에 대한 설명으로 가장 적절한 것은?

① RTO는 복구 완료가 필요한 기능의 우선순위이다.

② RPO는 서비스 중단에 따른 데이터 보호 계획이다.

③ RP는 실제 업무 기능 복구까지 걸리는 시간이다.

④ MTD는 서비스를 중단할 수 있는 최소시간이다.

정답 3번

간단한 해설

정답은 ③이다. RP는 **실제 복구에 걸린 기간**을 의미한다. RTO는 복구 목표 시간, RPO는 복구 목표 시점, MTD는 최대 허용 중단 시간으로 구별한다.

선지별 해설

① X. RTO(Recovery Time Objective)는 **복구 목표 시간**이다. 재해 후 시스템이나 업무 기능을 언제까지 복구해야 하는지를 정한 시간 기준이므로, 복구할 기능들의 우선순위라는 설명은 틀리다. 우선순위는 업무의 중요도와 중단 영향을 분석하여 정하고, 각 기능에 필요한 RTO를 설정하는 데 활용한다.

② X. RPO(Recovery Point Objective)는 **복구 목표 시점**이다. 장애 발생 전 어느 시점의 데이터까지 되돌려 복구할 것인지를 정하며, 허용 가능한 데이터 손실 범위를 시간으로 나타내는 기준이다. 따라서 데이터 보호 계획 자체가 아니라, 그 계획에서 백업·복제 수준을 정할 때 고려하는 목표로 고쳐야 한다.

③ O. RP(Recovery Period)는 이 문항에서 **실제 업무 기능 복구까지 소요된 시간**을 뜻한다. 사전에 정한 목표인 RTO와 실제 복구에 걸린 기간을 구별하는 것이 핵심이다. 예를 들어 복구 목표가 4시간이고 실제 복구에 3시간이 걸렸다면, 목표 시간은 4시간이고 실제 복구 기간은 3시간이다. 따라서 가장 적절한 설명은 ③이다.

④ X. MTD(Maximum Tolerable Downtime)는 조직이 감당할 수 있는 **최대 허용 중단 시간**이다. 업무 중단이 허용 한계를 넘는 영향을 일으키기 전까지 버틸 수 있는 시간의 상한이므로, 최소시간이라는 표현을 최대시간으로 바로잡아야 한다.

NoteBase

문 7. TCSEC(Trusted Computer System Evaluation Criteria)에 제시된 보안 등급과 보호 수준에 대한 연결이 가장 적절한 것은?

① A 등급 - 통제된 보호(Controlled Protection)

② B 등급 - 검증된 보호(Verified Protection)

③ C 등급 - 임의적 보호(Discretionary Protection)

④ D 등급 - 최대 보호(Maximum Protection)

정답 3번

간단한 해설

TCSEC의 큰 등급은 A의 검증된 보호, B의 강제적 보호, **C의 임의적 보호**, D의 최소 보호로 구분된다. 특히 D의 Minimal을 Maximum으로, A의 Verified를 다른 등급의 명칭으로 바꾸지 않도록 구별해야 한다.

선지별 해설

① X: A 등급의 명칭은 **검증된 보호(Verified Protection)**이다. 선지의 통제된 보호는 A 등급의 이름이 아니며, C 등급의 하위 클래스 C2는 통제된 접근 보호(Controlled Access Protection)로 구분된다. 큰 등급인 A와 하위 클래스 C2의 명칭을 혼동하면 안 된다.

② X: B 등급은 **강제적 보호(Mandatory Protection)**이다. 보안 등급 표지와 강제적 접근통제 규칙을 통해 보호를 수행하는 수준으로, 선지에 제시된 검증된 보호는 A 등급의 명칭이다.

③ O: C 등급은 **임의적 보호(Discretionary Protection)**이다. 권한을 가진 사용자가 객체에 대한 접근·공유 권한을 정할 수 있는 임의적 접근통제를 중심으로 한다. C 등급은 C1과 C2로 세분되므로 등급과 보호 수준의 연결이 맞다.

④ X: D 등급은 **최소 보호(Minimal Protection)**이다. 평가를 받았지만 더 높은 평가 클래스의 요구사항을 충족하지 못하는 시스템이 여기에 해당한다. 따라서 최대 보호라는 연결은 반대이며, TCSEC의 큰 등급 중 최상위는 A이다.

NoteBase

문 8. ISMS-P 인증의 '관리체계 수립 및 운영' 분야와 항목에 대한 연결이 가장 적절하지 않은 것은?

① 관리체계 기반 마련 - 경영진 참여, 최고책임자 지정, 조직 구성, 정책 수립, 자원 할당

② 위협관리 - 정책의 유지관리, 조직의 유지관리, 외부자 보안 이행관리, 개인정보 수집제한

③ 관리체계 운영 - 보호대책 구현, 보호대책 공유, 운영현황 관리

④ 관리체계 점검 및 개선 - 법적 요구사항 준수 검토, 관리체계 점검, 관리체계 개선

정답 2번

간단한 해설

위험 관리 분야의 항목은 **정보자산 식별, 현황 및 흐름분석, 위험 평가, 보호대책 선정**이다. 정책·조직 유지관리, 외부자 보안 이행관리, 개인정보 수집제한은 각각 다른 보호 요구사항에 속한다.

선지별 해설

① O: 경영진 참여, 최고책임자 지정, 조직 구성, 정책 수립, 자원 할당은 모두 관리체계를 운영할 책임·조직·방침·자원을 갖추는 기반 마련 항목이다. 이 분야에는 선지에 제시된 다섯 항목 외에 **범위 설정**도 포함된다.

② X: 공식 분야명은 '위협관리'가 아니라 **위험 관리**이며, 해당 항목은 정보자산 식별, 현황 및 흐름분석, 위험 평가, 보호대책 선정이다. 선지의 정책·조직 유지관리는 '정책, 조직, 자산 관리', 외부자 보안 이행관리는 '외부자 보안'에 속하며, 이들은 보호대책 요구사항이다. 개인정보 수집제한은 개인정보 처리 단계별 요구사항 중 '개인정보 수집 시 보호조치'에 속한다.

③ O: 보호대책 구현, 보호대책 공유, 운영현황 관리는 관리체계 운영 항목이다. 선정한 대책을 실행하고 관련자가 알도록 하며 운영 활동과 수행 내역을 관리한다는 점에서 연결된다.

④ O: 법적 요구사항 준수 검토, 관리체계 점검, 관리체계 개선은 관리체계 점검 및 개선 항목이다. 요구사항과 운영 상태를 확인하고 발견된 문제를 시정하여 관리체계의 효과성을 높이는 활동이다.

따라서 서로 다른 요구사항의 항목을 잘못 묶은 ②가 가장 적절하지 않다.

NoteBase

문 9. 정보보호 정책 구현 요소와 관련된 ㉠~㉣ 설명의 연결이 가장 적절한 것은?

㉠ 정보보호에 대한 상위 수준의 목표 및 방향을 제시한다.
㉡ 선택적이거나, 권장 혹은 권고적인 내용으로 예측할 수 없는 상황에 유연성을 제공한다.
㉢ 정책을 만족하기 위해 수행되는 단계적인 작업으로 구체적이고 세부적인 방법을 기술한다.
㉣ 정책을 만족하기 위한 의무적 활동, 행위, 또는 규칙으로 요구사항에 관해 정의한다.

① 절차 — ㉠
② 비전 — ㉡
③ 지침 — ㉢
④ 표준 — ㉣

정답 4번

간단한 해설

표준은 정책을 충족하기 위해 따라야 하는 **의무적 요구사항**을 정하므로 ㉣과 연결된 ④가 정답이다.

선지별 해설

① X: 절차는 정책을 이행하기 위해 **어떤 작업을 어떤 순서로 수행하는지** 구체적으로 정한 것이므로 ㉢에 해당한다. ㉠의 상위 수준 목표·방향 제시는 세부 작업 순서를 기술하는 절차의 역할이 아니다.

② X: ㉠은 정보보호에 대한 상위 수준의 목표와 방향을 제시하는 정책에 해당한다. 표준·지침·절차는 이러한 정책을 구체적으로 구현하기 위한 요소이다. ㉡의 **선택적·권고적이며 유연한 적용**을 돕는 내용은 지침에 해당한다.

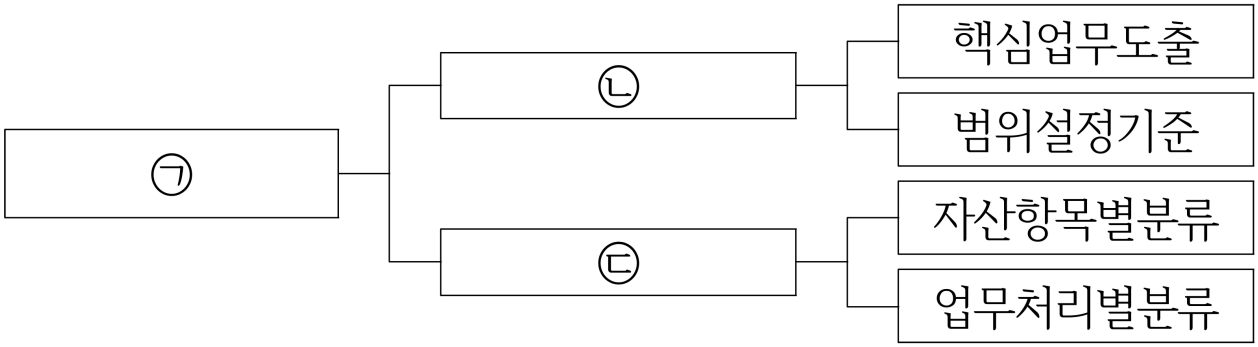
③ X: 지침은 정책을 구현할 때 참고할 권장 방법을 제시하므로 ㉡에 해당한다. ㉢처럼 **구체적인 단계별 실행 방법**을 정하는 것은 절차이다. 권고 중심의 안내와 정해진 작업 순서를 구별해야 한다.

④ O: 표준은 정책의 요구를 충족하도록 조직에서 공통적으로 따라야 할 활동·행위·규칙을 정한다. 따라서 ㉣의 **의무적 요구사항**과 연결된다. 지침의 권고적 성격과 달리 준수해야 할 기준을 제시한다.

제시된 연결 중 표준과 ㉣을 짝지은 ④가 정답이다.

NoteBase

문 10. 자산식별 과정의 일부 중 ㉠~㉢에 들어갈 내용으로 가장 적절한 것은?



① ㉠ 자산조사 ㉡ 자산목록 작성 ㉢ 자산범위 설정

② ㉠ 자산목록 작성 ㉡ 자산조사 ㉢ 자산범위 설정

③ ㉠ 자산조사 ㉡ 자산범위 설정 ㉢ 자산목록 작성

④ ㉠ 자산목록 작성 ㉡ 자산범위 설정 ㉢ 자산조사

정답 3번

간단한 해설

정답은 ③이다. 핵심업무도출·범위설정기준과 연결된 ㉡은 **자산범위 설정**, 두 분류 항목과 연결된 ㉢은 **자산목록 작성**이다. 이 둘을 포괄하는 ㉠은 자산조사이다.

도식 해설

도식은 왼쪽 ㉠을 상위 활동으로 두고, 오른쪽의 ㉡과 ㉢ 및 각각의 세부 항목으로 나누고 있다. 따라서 가로 배치를 단순한 시간 순서로 읽기보다 **상위 활동과 세부 활동의 관계**로 해석해야 한다.

㉡은 **자산범위 설정**이다. 연결된 핵심업무도출은 어떤 업무를 중심으로 보호 대상을 파악할지 정하는 것이고, 범위설정기준은 어떤 자산을 조사 대상에 포함할지 정하는 기준이다. 두 항목 모두 조사 대상의 경계를 정하는 활동에 해당한다.

㉢은 **자산목록 작성**이다. 연결된 자산항목별분류는 자산의 종류나 항목을 기준으로 정리하는 방식이고, 업무처리별분류는 자산이 지원하는 업무를 기준으로 정리하는 방식이다. 두 분류를 통해 식별한 자산을 체계적인 목록으로 정리한다.

㉠은 범위를 정하고 목록을 만드는 두 활동을 포괄하는 **자산조사**이다. 따라서 ㉠ 자산조사, ㉡ 자산범위 설정, ㉢ 자산목록 작성에 해당하는 ③이 정답이다.

NoteBase

문 11. 다음의 위험분석 방법에 대한 설명으로 가장 적절한 것은?

전문가 지식과 경험을 활용하여 위험분석을 수행하므로 상대적으로 신속한 결과를 도출할 수 있는 장점이 있다. 하지만 전문가의 개인적 지식 및 주관적 판단에 지나치게 의존하기 때문에 분석 결과가 일관성이 부족하거나 왜곡될 가능성이 있다. 따라서 전문성이 높은 인력이 수행하지 않으면 위험분석 결과의 완전도가 낮을 수 있으며 심지어 실패할 위험이 존재한다.

① 기준선 접근법(Baseline Approach)

② 비정형화된 접근법(Informal Approach)

③ 상세 위험 분석 접근법(Detailed Risk Analysis Approach)

④ 복합 접근법(Combined Approach)

정답 2번

간단한 해설

비정형화된 접근법은 전문가의 지식과 경험을 중심으로 위험을 분석한다. 신속하게 수행할 수 있지만 개인적 판단에 의존하므로 분석의 일관성과 완전성이 부족할 수 있다.

핵심 풀이

비정형화된 접근법: 정해진 분석 모형과 절차를 엄격히 적용하기보다 **전문가의 지식과 경험**을 이용해 위험을 분석한다. 따라서 비교적 빠르게 결과를 얻을 수 있지만, 수행자의 주관과 전문성 차이로 결과가 달라지고 익숙하지 않은 위험을 놓칠 수 있다. 제시문의 신속성, 개인적 판단 의존, 일관성·완전성 부족 가능성이 이 방법의 특징이다.

기준선 접근법: 표준이나 권고사항에 따른 **기본 보호대책**을 기준으로 보안 수준을 점검한다. 이미 정해진 기준을 활용하므로 빠르게 적용할 수 있지만, 전문가 개인의 경험에 의존한다는 제시문의 핵심과는 다르다.

상세 위험 분석 접근법: **구조화된 절차**에 따라 자산·위협·취약성을 자세히 분석하여 위험과 필요한 대책을 평가한다. 분석에 많은 시간과 자원이 들 수 있으며, 개인의 비정형적 판단을 주된 근거로 하는 방법과 구별된다.

복합 접근법: 중요하거나 위험이 큰 영역에는 상세 위험 분석을 실시하고 다른 영역에는 기준선 접근법을 적용하는 등 **여러 접근법을 결합**한다. 제시문에는 이러한 구분 적용이나 결합이 나타나지 않는다.

따라서 제시문이 설명하는 것은 ② 비정형화된 접근법이다.

NoteBase

문 12. 「개인정보 보호법」상 개인정보처리자가 개인정보를 수집할 수 있는 경우로 가장 적절하지 않은 것은?

① 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우
② 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우
③ 개인정보처리자가 법에서 정한 방법을 통해 정보주체의 동의를 받는 경우
④ 법률에 특별한 규정이 없지만, 사회 통념상 관행을 준수하기 위한 경우

정답 4번

①

정보주체와의 계약 이행이나 **계약 체결 과정에서 정보주체가 요청한 조치의 이행에 필요한 경우**에는 개인정보를 수집할 수 있다.

개인정보 보호법 제15조(개인정보의 수집 · 이용)
① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다. <개정 2023.3.14>
4. 정보주체와 체결한 계약을 이행하거나 계약을 체결하는 과정에서 정보주체의 요청에 따른 조치를 이행하기 위하여 필요한 경우

②

공공기관은 **법령 등에서 정한 소관 업무를 수행하기 위하여 불가피한 경우** 정보주체의 동의 없이 개인정보를 수집할 수 있다.

개인정보 보호법 제15조(개인정보의 수집 · 이용)
① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다. <개정 2023.3.14>
3. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우

③

개인정보처리자가 **법정 절차에 따라 정보주체의 동의를 받으면** 개인정보를 수집하고 그 수집 목적의 범위에서 이용할 수 있다.

개인정보 보호법 제15조(개인정보의 수집 · 이용)
① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다. <개정 2023.3.14>
1. 정보주체의 동의를 받은 경우

NoteBase

④

법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우에는 개인정보를 수집할 수 있지만, **사회 통념상 관행 준수만으로는 수집할 수 없다**.

개인정보 보호법 제15조(개인정보의 수집 · 이용)
① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다. <개정 2023.3.14>
2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우

NoteBase

문 13. 「개인정보 보호법」상 개인정보 보호 원칙에 대한 설명으로 가장 적절하지 않은 것은?

① 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최대한의 개인정보를 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.

④ 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리하여야 한다.

정답 1번

①

개인정보처리자는 처리 목적을 명확히 하고, 그 목적에 필요한 **최소한의 개인정보만** 적법하고 정당하게 수집해야 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

개인정보는 **처리 목적에 필요한 범위에서 적합하게 처리**해야 하며, **목적 외 활용을 금지**하는 것이 개인정보 보호의 원칙이다.

개인정보 보호법 제3조(개인정보 보호 원칙)
② 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.

③

개인정보처리자는 처리 목적에 필요한 범위에서 개인정보의 **정확성·완전성·최신성**이 유지되도록 해야 한다.

개인정보 보호법 제3조(개인정보 보호 원칙)
③ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.

NoteBase

④

개인정보처리자는 처리 방법과 정보의 종류 등에 따른 **정보주체의 권리 침해 가능성과 위험 정도**를 고려하여 개인정보를 안전하게 관리해야 한다.

개인정보 보호법 제3조(개인정보 보호 원칙)
④ 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리하여야 한다.

NoteBase

문 14. 「개인정보 보호법」상 다음과 같은 경우로 법원이 배상액을 정할 때에 고려해야 하는 사항으로 가장 적절하지 않은 것은?

개인정보처리자의 고의 또는 중대한 과실로 인하여 개인정보가 분실·도난·유출·위조·변조 또는 훼손된 경우로서 정보주체에게 손해가 발생한 때에는 법원은 그 손해액의 3배를 넘지 아니하는 범위에서 손해배상액을 정할 수 있다. 다만, 개인정보처리자가 고의 또는 중대한 과실이 없음을 증명한 경우에는 그러하지 아니하다.

① 개인정보처리자의 재산상태
② 개인정보주체가 취득한 경제적 이익
③ 고의 또는 손해 발생의 우려를 인식한 정도
④ 개인정보처리자가 정보주체의 피해구제를 위하여 노력한 정도

정답 2번

①

법원은 가중 손해배상액을 정할 때 **개인정보처리자의 재산상태**를 고려하여야 한다.

개인정보 보호법 제39조(손해배상책임)
④ 법원은 제3항의 배상액을 정할 때에는 다음 각 호의 사항을 고려하여야 한다. <신설 2015.7.24>
6. 개인정보처리자의 재산상태

②

고려대상은 정보주체가 얻은 이익이 아니라 **위법행위로 개인정보처리자가 취득한 경제적 이익**이다.

개인정보 보호법 제39조(손해배상책임)
④ 법원은 제3항의 배상액을 정할 때에는 다음 각 호의 사항을 고려하여야 한다. <신설 2015.7.24>
3. 위법행위로 인하여 개인정보처리자가 취득한 경제적 이익

③

법원은 가중 손해배상액을 정할 때 **고의 또는 손해 발생의 우려를 인식한 정도**를 고려하여야 한다.

개인정보 보호법 제39조(손해배상책임)
④ 법원은 제3항의 배상액을 정할 때에는 다음 각 호의 사항을 고려하여야 한다. <신설 2015.7.24>
1. 고의 또는 손해 발생의 우려를 인식한 정도

NoteBase

④

법원은 가중 손해배상액을 정할 때 **개인정보처리자가 정보주체의 피해구제를 위하여 노력한 정도**를 고려하여야 한다.

개인정보 보호법 제39조(손해배상책임)
④ 법원은 제3항의 배상액을 정할 때에는 다음 각 호의 사항을 고려하여야 한다. <신설 2015.7.24>
8. 개인정보처리자가 정보주체의 피해구제를 위하여 노력한 정도

NoteBase

문 16. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상 정보통신서비스 제공자가 해당 서비스를 제공하기 위하여 이용자의 이동통신단말장치 내에 저장되어 있는 정보 및 이동통신단말장치에 설치된 기능에 대하여 접근권한이 필요한 경우를 두 가지로 설명하고 있다. 이 두가지 경우에서 이용자의 동의를 받기 위해 이용자가 명확하게 인지할 수 있도록 알려야 하는 것 중 공통사항으로만 가장 적절하게 짝지어진 것은?

㉠ 접근권한이 필요한 이유
㉡ 접근권한이 필요한 정보 및 기능의 항목
㉢ 접근권한이 필요한 서비스의 과금 정보
㉣ 접근권한 허용에 대하여 동의하지 아니할 수 있다는 사실

① ㉠㉡
② ㉠㉢
③ ㉠㉡㉢
④ ㉠㉡㉢㉣

정답 1번

㉠

필수 접근권한과 선택적 접근권한 모두 **접근권한이 필요한 이유**를 이용자가 명확히 인지하도록 알리고 동의를 받아야 한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제22조의2(접근권한에 대한 동의)
① 정보통신서비스 제공자는 해당 서비스를 제공하기 위하여 이용자의 이동통신단말장치 내에 저장되어 있는 정보 및 이동통신단말장치에 설치된 기능에 대하여 접근할 수 있는 권한(이하 "접근권한"이라 한다)이 필요한 경우 다음 각 호의 사항을 이용자가 명확하게 인지할 수 있도록 알리고 이용자의 동의를 받아야 한다.
1. 해당 서비스를 제공하기 위하여 반드시 필요한 접근권한인 경우
나. 접근권한이 필요한 이유
2. 해당 서비스를 제공하기 위하여 반드시 필요한 접근권한이 아닌 경우
나. 접근권한이 필요한 이유

NoteBase

㉡

필수 접근권한과 선택적 접근권한 모두 **접근하려는 정보 및 기능의 항목**을 이용자가 명확히 인지하도록 알리고 동의를 받아야 한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제22조의2(접근권한에 대한 동의)
① 정보통신서비스 제공자는 해당 서비스를 제공하기 위하여 이용자의 이동통신단말장치 내에 저장되어 있는 정보 및 이동통신단말장치에 설치된 기능에 대하여 접근할 수 있는 권한(이하 "접근권한"이라 한다)이 필요한 경우 다음 각 호의 사항을 이용자가 명확하게 인지할 수 있도록 알리고 이용자의 동의를 받아야 한다.
1. 해당 서비스를 제공하기 위하여 반드시 필요한 접근권한인 경우
가. 접근권한이 필요한 정보 및 기능의 항목
2. 해당 서비스를 제공하기 위하여 반드시 필요한 접근권한이 아닌 경우
가. 접근권한이 필요한 정보 및 기능의 항목

㉢

두 경우의 공통 고지사항은 **접근 대상 정보·기능의 항목과 접근권한이 필요한 이유**이다. 서비스의 과금 정보는 접근권한 동의를 위한 법정 고지사항에 포함되지 않는다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제22조의2(접근권한에 대한 동의)
① 정보통신서비스 제공자는 해당 서비스를 제공하기 위하여 이용자의 이동통신단말장치 내에 저장되어 있는 정보 및 이동통신단말장치에 설치된 기능에 대하여 접근할 수 있는 권한(이하 "접근권한"이라 한다)이 필요한 경우 다음 각 호의 사항을 이용자가 명확하게 인지할 수 있도록 알리고 이용자의 동의를 받아야 한다.
1. 해당 서비스를 제공하기 위하여 반드시 필요한 접근권한인 경우
가. 접근권한이 필요한 정보 및 기능의 항목
나. 접근권한이 필요한 이유
2. 해당 서비스를 제공하기 위하여 반드시 필요한 접근권한이 아닌 경우
가. 접근권한이 필요한 정보 및 기능의 항목
나. 접근권한이 필요한 이유
다. 접근권한 허용에 대하여 동의하지 아니할 수 있다는 사실

NoteBase

㉡

동의하지 않을 수 있다는 사실은 **서비스 제공에 반드시 필요하지 않은 선택적 접근권한**의 고지사항이다. 필수 접근권한에는 이 고지사항이 없어 두 경우의 공통사항이 아니다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제22조의2(접근권한에 대한 동의)
① 정보통신서비스 제공자는 해당 서비스를 제공하기 위하여 이용자의 이동통신단말장치 내에 저장되어 있는 정보 및 이동통신단말장치에 설치된 기능에 대하여 접근할 수 있는 권한(이하 "접근권한"이라 한다)이 필요한 경우 다음 각 호의 사항을 이용자가 명확하게 인지할 수 있도록 알리고 이용자의 동의를 받아야 한다.
1. 해당 서비스를 제공하기 위하여 반드시 필요한 접근권한인 경우
가. 접근권한이 필요한 정보 및 기능의 항목
나. 접근권한이 필요한 이유
2. 해당 서비스를 제공하기 위하여 반드시 필요한 접근권한이 아닌 경우
다. 접근권한 허용에 대하여 동의하지 아니할 수 있다는 사실

NoteBase

문 17. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상 통신과금서비스제공자가 재화 등의 판매·제공의 대가가 발생한 때 및 대가를 청구할 때 통신과금서비스이용자에게 고지하여야 하는 사항으로 가장 적절하지 않은 것은?

① 통신과금서비스 이용일시

② 통신과금서비스를 통한 구매·이용 금액과 그 명세

③ 통신과금서비스제공자의 이용자 개인정보보호 대책

④ 이의신청 방법 및 연락처

정답 3번

①

통신과금서비스제공자는 재화 등의 대가가 발생한 때와 대가를 청구할 때 **통신과금서비스 이용일시**를 이용자에게 고지하여야 한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제58조(통신과금서비스이용자의 권리 등)
① 통신과금서비스제공자는 재화등의 판매 · 제공의 대가가 발생한 때 및 대가를 청구할 때에 통신과금서비스이용자에게 다음 각 호의 사항을 고지하여야 한다. <개정 2011.4.5, 2014.5.28>
1. 통신과금서비스 이용일시

②

통신과금서비스제공자는 재화 등의 대가가 발생한 때와 대가를 청구할 때 **통신과금서비스를 통한 구매·이용 금액과 그 명세**를 이용자에게 고지하여야 한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제58조(통신과금서비스이용자의 권리 등)
① 통신과금서비스제공자는 재화등의 판매 · 제공의 대가가 발생한 때 및 대가를 청구할 때에 통신과금서비스이용자에게 다음 각 호의 사항을 고지하여야 한다. <개정 2011.4.5, 2014.5.28>
3. 통신과금서비스를 통한 구매 · 이용 금액과 그 명세

NoteBase

③

대가 발생·청구 시 고지사항은 이용일시, 거래 상대방의 상호와 연락처, 구매·이용 금액과 명세, 이의신청 방법과 연락처이다. **이용자 개인정보보호 대책은 이 고지사항에 포함되지 않는다.**

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제58조(통신과금서비스이용자의 권리 등)
① 통신과금서비스제공자는 재화등의 판매 · 제공의 대가가 발생한 때 및 대가를 청구할 때에 통신과금서비스이용자에게 다음 각 호의 사항을 고지하여야 한다. <개정 2011.4.5, 2014.5.28>
1. 통신과금서비스 이용일시
2. 통신과금서비스를 통한 구매 · 이용의 거래 상대방(통신과금서비스를 이용하여 그 대가를 받고 재화 또는 용역을 판매 · 제공하는 자를 말한다. 이하 "거래 상대방"이라 한다)의 상호와 연락처
3. 통신과금서비스를 통한 구매 · 이용 금액과 그 명세
4. 이의신청 방법 및 연락처

④

통신과금서비스제공자는 재화 등의 대가가 발생한 때와 대가를 청구할 때 **이의신청 방법 및 연락처**를 이용자에게 고지하여야 한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제58조(통신과금서비스이용자의 권리 등)
① 통신과금서비스제공자는 재화등의 판매 · 제공의 대가가 발생한 때 및 대가를 청구할 때에 통신과금서비스이용자에게 다음 각 호의 사항을 고지하여야 한다. <개정 2011.4.5, 2014.5.28>
4. 이의신청 방법 및 연락처

NoteBase

문 18. 「위치정보의 보호 및 이용 등에 관한 법률」상 개인위치정보를 대상으로 하지 아니하는 위치정보사업만을 하려는 자가 대통령령으로 정하는 바에 따라 방송통신위원회에 신고해야 하는 사항으로 가장 적절하지 않은 것은?

① 위치정보서비스 이용자 수와 매출액

② 위치정보사업의 종류 및 내용

③ 주된 사무소의 소재지

④ 위치정보시스템을 포함한 사업용 주요 설비

정답 1번

①

신고사항은 상호, 주된 사무소의 소재지, 위치정보사업의 종류 및 내용, 위치정보시스템을 포함한 사업용 주요 설비이다. **이용자 수와 매출액은 법정 신고사항에 포함되지 않는다.**

위치정보의 보호 및 이용 등에 관한 법률 제5조의2(개인위치정보를 대상으로 하지 아니하는 위치정보사업의 신고)
① 개인위치정보를 대상으로 하지 아니하는 위치정보사업만을 하려는 자는 다음 각 호의 사항을 대통령령으로 정하는 바에 따라 방송미디어통신위원회에 신고하여야 한다. <개정 2025.10.1>
1. 상호
2. 주된 사무소의 소재지
3. 위치정보사업의 종류 및 내용
4. 위치정보시스템을 포함한 사업용 주요 설비

②

개인위치정보를 대상으로 하지 않는 위치정보사업을 하려는 자는 **위치정보사업의 종류 및 내용**을 신고해야 한다.

위치정보의 보호 및 이용 등에 관한 법률 제5조의2(개인위치정보를 대상으로 하지 아니하는 위치정보사업의 신고)
① 개인위치정보를 대상으로 하지 아니하는 위치정보사업만을 하려는 자는 다음 각 호의 사항을 대통령령으로 정하는 바에 따라 방송미디어통신위원회에 신고하여야 한다. <개정 2025.10.1>
3. 위치정보사업의 종류 및 내용

NoteBase

③

개인위치정보를 대상으로 하지 않는 위치정보사업을 하려는 자는 **주된 사무소의 소재지**를 신고해야 한다.

위치정보의 보호 및 이용 등에 관한 법률 제5조의2(개인위치정보를 대상으로 하지 아니하는 위치정보사업의 신고)
① 개인위치정보를 대상으로 하지 아니하는 위치정보사업만을 하려는 자는 다음 각 호의 사항을 대통령령으로 정하는 바에 따라 방송미디어통신위원회에 신고하여야 한다. <개정 2025.10.1>
2. 주된 사무소의 소재지

④

개인위치정보를 대상으로 하지 않는 위치정보사업을 하려는 자는 **위치정보시스템을 포함한 사업용 주요 설비**를 신고해야 한다.

위치정보의 보호 및 이용 등에 관한 법률 제5조의2(개인위치정보를 대상으로 하지 아니하는 위치정보사업의 신고)
① 개인위치정보를 대상으로 하지 아니하는 위치정보사업만을 하려는 자는 다음 각 호의 사항을 대통령령으로 정하는 바에 따라 방송미디어통신위원회에 신고하여야 한다. <개정 2025.10.1>
4. 위치정보시스템을 포함한 사업용 주요 설비

NoteBase

문 19. 「개인정보 보호법」상 보호위원회에 대한 내용으로 가장 적절하지 않은 것은?

① 위원장은 보호위원회를 대표하고, 보호위원회의 회의를 주재하며, 소관 사무를 총괄한다.

② 위원장이 부득이한 사유로 직무를 수행할 수 없을 때에는 부위원장이 그 직무를 대행한다.

③ 보호위원회는 상임위원 2명(위원장과 부위원장)을 제외한 9명으로 구성한다.

④ 보호위원회의 위원장과 부위원장은 정무직 공무원으로 임명한다.

정답 3번

①

위원장은 보호위원회를 **대표하고, 회의를 주재하며, 소관 사무를 총괄**한다.

개인정보 보호법 제7조의3(위원장)
① 위원장은 보호위원회를 대표하고, 보호위원회의 회의를 주재하며, 소관 사무를 총괄한다.

②

위원장이 부득이한 사유로 직무를 수행할 수 없으면 **부위원장이 그 직무를 대행**한다. 위원장과 부위원장 모두 직무를 수행할 수 없으면 위원회가 미리 정한 위원이 대행한다.

개인정보 보호법 제7조의3(위원장)
② 위원장이 부득이한 사유로 직무를 수행할 수 없을 때에는 부위원장이 그 직무를 대행하고,
위원장 · 부위원장이 모두 부득이한 사유로 직무를 수행할 수 없을 때에는 위원회가 미리 정하는 위원이 위원장의 직무를 대행한다.

③

보호위원회는 위원장과 부위원장인 **상임위원 2명을 포함한 총 9명의 위원**으로 구성한다. 상임위원을 제외한 나머지 위원은 7명이다.

개인정보 보호법 제7조의2(보호위원회의 구성 등)
① 보호위원회는 상임위원 2명(위원장 1명, 부위원장 1명)을 포함한 9명의 위원으로 구성한다.

④

보호위원회의 위원장과 부위원장은 **정무직 공무원**으로 임명한다.

개인정보 보호법 제7조의2(보호위원회의 구성 등)
③ 위원장과 부위원장은 정무직 공무원으로 임명한다.

NoteBase

문 20. 「전자금융거래법」과 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상 다음에서 설명하는 업무를 수행 및 총괄하는 자로 가장 적절한 것은?

<전자금융거래법>
· 전자금융거래의 안정성 확보 및 이용자 보호를 위한 전략 및 계획의 수립
· 정보기술부문의 보호
· 정보기술부문의 보안에 필요한 인력관리 및 예산편성
· 전자금융거래의 사고 예방 및 조치

<정보통신망 이용촉진 및 정보보호 등에 관한 법률>
· 정보보호관리체계의 수립 및 관리·운영
· 정보보호 취약점 분석·평가 및 개선
· 침해사고의 예방 및 대응
· 사전 정보보호대책 마련 및 보안조치 설계 및 구현 등
· 중요 정보의 암호화 및 보안서버 적합성 검토

① 개인정보처리자
② 클라우드컴퓨팅서비스 제공자
③ 정보보호최고책임자
④ 개인위치정보사업자

정답 3번

NoteBase

①

제시된 전자금융 보안과 정보보호 총괄 업무를 맡는 법정 직위는 **개인정보처리자가 아니라 정보보호최고책임자**이다.

전자금융거래법 제21조의2(정보보호최고책임자 지정)
④ 제1항에 따른 정보보호최고책임자는 다음 각 호의 업무를 수행한다. <개정 2014.10.15>
1. 제21조제2항에 따른 전자금융거래의 안정성 확보 및 이용자 보호를 위한 전략 및 계획의 수립
2. 정보기술부문의 보호
3. 정보기술부문의 보안에 필요한 인력관리 및 예산편성
4. 전자금융거래의 사고 예방 및 조치
5. 그 밖에 전자금융거래의 안정성 확보를 위하여 대통령령으로 정하는 사항

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제45조의3(정보보호 최고책임자의 지정 등)
④ 정보보호 최고책임자의 업무는 다음 각 호와 같다. <개정 2021.6.8, 2026.3.10, 2026.3.31>
1. 정보보호 최고책임자는 다음 각 목의 업무를 총괄한다.
가. 정보보호 계획의 수립 · 시행 및 개선
나. 정보보호 실태와 관행의 정기적인 감사 및 개선
다. 정보보호 위험의 식별 평가 및 정보보호 대책 마련
라. 정보보호 교육과 모의 훈련 계획의 수립 및 시행
마. 정보보호에 필요한 인력 관리 및 예산 편성
바. 정보보호 현황 및 주요 사항의 이사회에 대한 보고
사. 그 밖에 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 대통령령으로 정하는 사항

NoteBase

③

정보보호최고책임자는 **전자금융거래의 안전성 확보·정보기술부문 보안·사고 예방 업무를 수행**하고, **정보보호 계획 수립과 위험 평가·보호대책 마련을 총괄**한다.

전자금융거래법 제21조의2(정보보호최고책임자 지정)
④ 제1항에 따른 정보보호최고책임자는 다음 각 호의 업무를 수행한다. <개정 2014.10.15>
1. 제21조제2항에 따른 전자금융거래의 안정성 확보 및 이용자 보호를 위한 전략 및 계획의 수립
2. 정보기술부문의 보호
3. 정보기술부문의 보안에 필요한 인력관리 및 예산편성
4. 전자금융거래의 사고 예방 및 조치
5. 그 밖에 전자금융거래의 안정성 확보를 위하여 대통령령으로 정하는 사항

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제45조의3(정보보호 최고책임자의 지정 등)
④ 정보보호 최고책임자의 업무는 다음 각 호와 같다. <개정 2021.6.8, 2026.3.10, 2026.3.31>
1. 정보보호 최고책임자는 다음 각 목의 업무를 총괄한다.
가. 정보보호 계획의 수립 · 시행 및 개선
나. 정보보호 실태와 관행의 정기적인 감사 및 개선
다. 정보보호 위험의 식별 평가 및 정보보호 대책 마련
라. 정보보호 교육과 모의 훈련 계획의 수립 및 시행
마. 정보보호에 필요한 인력 관리 및 예산 편성
바. 정보보호 현황 및 주요 사항의 이사회에 대한 보고
사. 그 밖에 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 대통령령으로 정하는 사항

NoteBase