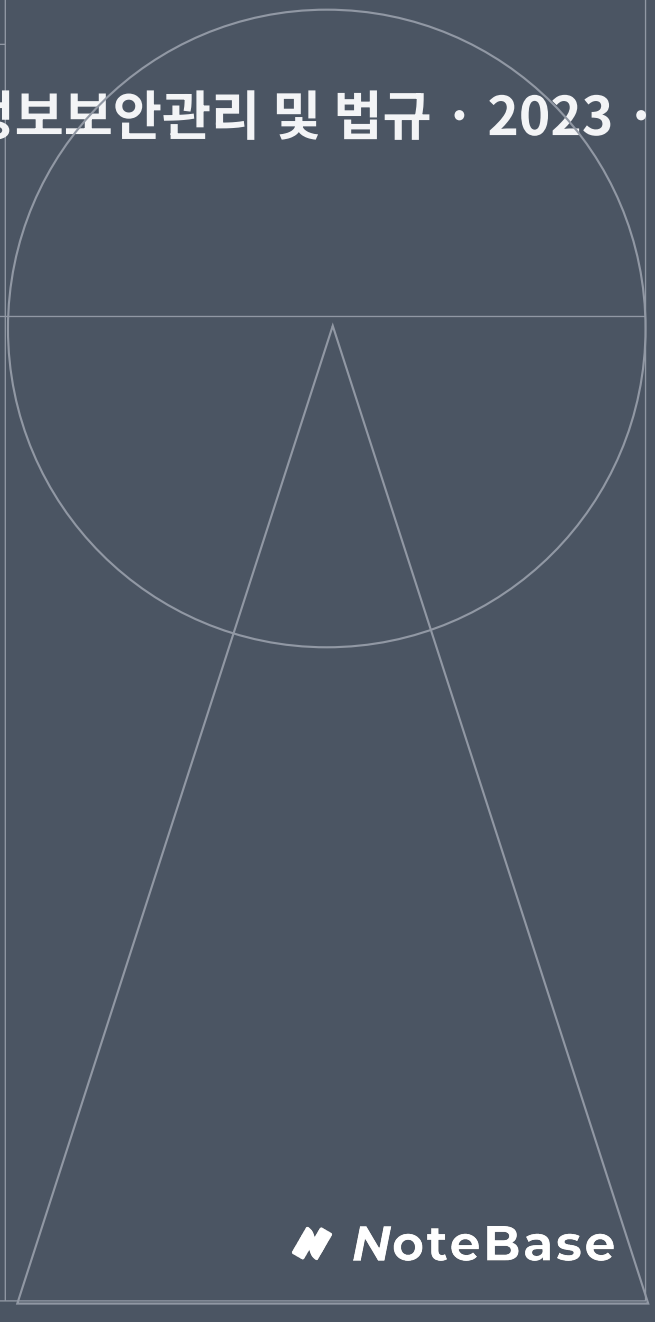
기출OX 해설집

공무원/경찰/공채(순경) · 정보보안관리 및 법규 · 2023 · 1차



NoteBase

기출OX 해설집

공무원/경찰/공채(순경) · 정보보안관리 및 법규 · 2023 · 1차

공무원/경찰/공채(순경) · 정보보안관리 및 법규 · 2023 · 1차

문 1. 시스템에 접근한 주체가 시스템에 어떤 행위를 하고 있는지를 기록함으로써 문제 발생 시 원인 및 책임 소재를 파악하기 위한 것으로 가장 적절한 것은?

① 책임추적성

② 식별

③ 인증

④ 인가

정답 1번

출제 포인트

시스템 이용자의 행위를 기록하여 사후에 행위 주체와 책임 소재를 확인하는 보안 속성이 책임추적성임을 묻는 문제이다.

핵심 개념

책임추적성은 각 주체의 행위를 로그 등으로 기록하고 특정 주체와 연결하여 사후에 책임 소재를 확인할 수 있게 하는 성질이다.
식별은 사용자가 자신이 누구인지를 시스템에 제시하는 과정이고, 인증은 그 신원이 진짜인지 확인하는 과정이며, 인가는 인증된 주체에게 허용할 자원과 행위의 범위를 정하는 과정이다.

선지별 해설

① O — 책임추적성은 시스템에서 누가 언제 어떤 행위를 했는지를 기록하여 사고 발생 시 원인과 책임 주체를 추적할 수 있게 한다. 지문의 '행위를 기록'하고 '책임 소재를 파악'한다는 표현에 정확히 대응한다.
② X — '식별'은 사용자가 아이디 등을 통해 자신의 신원을 시스템에 제시하는 과정이므로, 행위를 기록하여 책임 소재를 파악하는 개념이 아니다. 틀린 표현 '식별'은 '책임추적성'으로 고쳐야 한다.
③ X — '인증'은 비밀번호, 인증서, 생체정보 등으로 제시된 신원이 실제로 맞는지를 검증하는 과정이므로, 사후 행위 추적을 뜻하지 않는다. 틀린 표현 '인증'은 '책임추적성'으로 고쳐야 한다.
④ X — '인가'는 인증된 주체가 어떤 자원에 어떤 방식으로 접근할 수 있는지 권한을 부여하거나 확인하는 과정이므로, 행위 기록을 통한 책임 확인과 다르다. 틀린 표현 '인가'는 '책임추적성'으로 고쳐야 한다.

NoteBase

오답 포인트

식별·인증·인가는 접근 전에 신원이나 권한을 다루지만, 책임추적성은 접근 후 남은 행위 기록을 통해 원인과 책임 소재를 확인한다. 지문의 '기록', '문제 발생 시', '책임 소재'가 책임추적성을 가리키는 결정적 표현이다.

다시 나오면 이렇게 판단

누구인지 제시하면 식별, 그 신원을 검증하면 인증, 허용 범위를 정하면 인가, 행위 기록으로 사후 책임자를 찾으면 책임추적성으로 판단한다.

암기 포인트

식별은 신원 제시, 인증은 신원 확인, 인가는 권한 결정, 책임추적성은 행위 기록과 사후 책임 확인이다.

NoteBase

문 2. ISMS-P 인증체계는 정책기관, 인증기관, 심사기관으로 나누어져 있다. 인증위원회 개최를 통한 인증서 발급 등의 업무를 수행하는 인증기관으로 가장 적절한 것은?

① 한국인터넷진흥원(KISA)

② 한국정보통신진흥협회(KAIT)

③ 한국정보통신기술협회(TTA)

④ 개인정보보호협회(OPA)

정답 1번

쟁점

이 문제는 ISMS-P 인증체계에서 인증기관과 심사기관의 역할을 구별하는 문제이다. 핵심은 인증위원회 운영과 인증서 발급을 담당하는 기관을 찾는 것이다.

용어 풀이

인증기관은 심사 결과를 바탕으로 인증위원회를 운영하고 적합한 신청기관에 인증서를 발급하는 기관이다.
심사기관은 현장 심사 등 인증심사를 수행하고 그 결과를 인증기관에 제출하는 기관이다.

핵심 구분

ISMS-P 공식 인증체계에서 한국인터넷진흥원(KISA)은 법정 인증기관으로서 인증위원회 운영, 인증심사 결과의 심의·의결 요청 및 인증서 발급 업무를 수행한다. 반면 한국정보통신진흥협회(KAIT), 한국정보통신기술협회(TTA), 개인정보보호협회(OPA)는 심사기관이므로 인증기관과 구별된다.

선지별 해설

① O — 한국인터넷진흥원(KISA)은 법정 인증기관이다. 인증위원회의 심의·의결 절차를 거쳐 신청기관에 인증서를 발급한다.
② X — 한국정보통신진흥협회(KAIT)는 심사기관이지 인증기관이 아니다. 틀린 표현은 '인증기관'이며, 올바른 표현은 'ISMS-P 인증심사를 수행하는 심사기관'이다.
③ X — 한국정보통신기술협회(TTA)는 심사기관이지 인증기관이 아니다. 틀린 표현은 '인증기관'이며, 올바른 표현은 'ISMS-P 인증심사를 수행하는 심사기관'이다.
④ X — 개인정보보호협회(OPA)는 심사기관이지 인증기관이 아니다. 틀린 표현은 '인증기관'이며, 올바른 표현은 'ISMS-P 인증심사를 수행하는 심사기관'이다.

오답 포인트

네 기관이 모두 ISMS-P 제도와 관련되어 있다는 점 때문에 역할을 혼동하기 쉽다. '실제 심사를 수행하는 기관'과 '인증위원회를 거쳐 인증서를 발급하는 기관'을 구분해야 한다.

NoteBase

다시 나오면 이렇게 판단

문제에 '인증위원회'와 '인증서 발급'이 제시되면 인증기관을 찾고, '인증심사 수행'이 제시되면 심사기관을 찾는다. 보기 중 한국인터넷진흥원(KISA)은 법정 인증기관에 해당한다.

암기 포인트

KISA는 인증위원회·인증서 발급, KAIT·TTA·OPA는 인증심사를 담당한다.

NoteBase

문 3. 정보보호 시스템 인증에 관한 설명으로 가장 적절하지 않은 것은?

① 정보보호 시스템 평가기준은 정보보호 시스템 제품을 객관적으로 평가하여 신뢰성을 확보하기 위한 인증제도이다.

② TCSEC은 보안 솔루션을 개발할 때 표준이 되는 정보보호 제품 인증으로 가장 등급이 낮은 D부터 A까지 있다.

③ ITSEC은 운영체제와 장치를 평가하기 위한 유럽형 지침으로 기밀성, 무결성, 가용성을 다루며 기능성과 보증을 분리 평가한다.

④ TCSEC과 ITSEC의 단점을 보완하고자 세계 각국에서 사용되는 다양한 평가 지침을 포함한 TOE 인증은 정보보호 제품에 대한 상호인증이다.

정답 4번

출제 포인트

정보보호 시스템 평가기준인 TCSEC·ITSEC·CC의 특징과 TOE·상호인정의 의미를 구별하는 문제이다.

핵심 개념

TCSEC은 미국의 정보보호 시스템 평가기준으로 D에서 A까지 등급을 구분한다. ITSEC은 유럽에서 마련된 평가기준으로 보안 기능과 그 기능이 제대로 구현되었다는 보증을 분리하여 평가한다. CC(Common Criteria)는 여러 국가의 평가기준을 통합한 국제 공통평가기준이다. TOE(Target of Evaluation)는 CC에 따라 평가받는 제품이나 시스템 등 평가대상을 뜻하며, 인증이나 상호인정 제도 자체를 뜻하지 않는다.

선지별 해설

① O — 정보보호 시스템 평가기준은 제품이나 시스템의 보안 기능과 신뢰성을 객관적으로 평가하여 일정 수준을 충족했음을 인증하기 위한 기준이다.
② O — TCSEC은 보안 수준을 가장 낮은 D부터 C·B를 거쳐 가장 높은 A까지 구분한다. 따라서 D부터 A까지의 등급 체계라는 설명은 적절하다.
③ O — ITSEC은 유럽에서 마련된 평가기준으로 기밀성·무결성·가용성과 관련된 보안 기능을 다루고, 기능성 평가와 보증 평가를 분리한다.
④ X — 틀린 표현은 ‘TOE 인증은 정보보호 제품에 대한 상호인증’이다. TOE는 인증제도가 아니라 평가대상 제품·시스템을 뜻한다. 올바르게는 여러 평가기준을 통합한 국제 공통평가기준은 CC이고, CC에 따른 인증서의 국가 간 상호인정은 CCRA에 의해 이루어진다고 표현해야 한다.

오답 포인트

④는 CC, TOE, CCRA를 하나의 개념처럼 섞었다. TOE는 무엇을 평가하는지를 나타내는 말이고, CC는 무엇을 기준으로 평가하는지를 나타내며, CCRA는 인증서를 국가 간에 상호인정하는 협정이다.

NoteBase

다시 나오면 이렇게 판단

평가대상이면 TOE, 국제 공통평가기준이면 CC, CC 인증서의 국가 간 상호인정이면 CCRA로 구분한다.

암기 포인트

TOE는 대상, CC는 기준, CCRA는 상호인정이다.

NoteBase

문 4. 재해복구시스템에 관한 설명으로 가장 적절하지 않은 것은?

① Mirror 사이트는 RTO 및 RPO 측면에서 가장 적절한 사이트로 1차 사이트와 완전 이중화를 수행하고 데이터베이스도 실시간으로 동기화한다.

② Hot 사이트는 주 서버와 백업 서버를 Active-Active 상태로 유지하여 주 서버는 업무를 처리하고 백업 서버는 운영하지 않는 상태로 대기한다.

③ Warm 사이트는 중요한 업무 위주로 백업 사이트를 구성하는 것으로 시스템 복구에 수 일에서 수 주까지 소요된다.

④ Cold 사이트는 전기 시설을 완비하고 재해 발생 시 서버와 소프트웨어를 구매해서 복구하는 방식으로 재해복구 측면에서 가장 부적절하다.

정답 2번

출제 포인트

재해복구 사이트를 복구 자원의 준비 수준과 전환 방식에 따라 Mirror, Hot, Warm, Cold 사이트로 구분할 수 있는지를 묻는 문제이다.

핵심 개념

Mirror 사이트는 주 사이트와 백업 사이트를 완전히 이중화하고 데이터를 실시간으로 동기화하는 방식이다. Hot 사이트는 복구에 필요한 시스템과 데이터를 미리 갖추고 즉시 또는 단시간 안에 업무를 넘겨받을 수 있도록 대기하는 방식이다. Warm 사이트는 핵심 업무 중심의 장비와 데이터를 일부 준비하여 Hot 사이트보다 복구 시간이 길다. Cold 사이트는 장소와 전기·통신 등 기반 시설 위주로 마련하고 재해 후 장비와 소프트웨어를 확보하므로 복구 시간이 가장 길다.

선지별 해설

① O — Mirror 사이트는 주 사이트와 완전 이중화를 구성하고 데이터베이스를 실시간으로 동기화하므로 RTO와 RPO를 가장 짧게 할 수 있다.
② X — 틀린 표현은 ‘Active-Active 상태’와 ‘백업 서버는 운영하지 않는 상태로 대기한다’이다. Active-Active라면 양쪽 서버가 모두 운영되므로 백업 서버가 운영하지 않는다는 설명과 모순된다. Hot 사이트는 백업 시스템이 가동 가능한 상태로 준비되어 장애 시 즉시 또는 단시간 안에 업무를 인계받는 형태이며, 대기 서버가 평상시 업무를 처리하지 않는 구성은 Active-Standby로 표현하는 것이 옳다.
③ O — Warm 사이트는 중요한 업무를 우선하여 필요한 자원을 일부 갖춘 중간 수준의 복구 방식이므로 시스템 복구에 수 일에서 수 주가 걸릴 수 있다.
④ O — Cold 사이트는 전기 등 기반 시설을 마련해 두지만 서버와 소프트웨어는 재해 발생 후 확보·설치하므로 복구 시간이 가장 길고 신속한 재해복구에는 가장 부적절하다.

NoteBase

오답 포인트

②는 ‘Active-Active’라는 용어와 ‘백업 서버를 운영하지 않고 대기’한다는 상태를 한 문장에 섞은 것이 함정이다. Active-Active는 두 시스템이 모두 동작하는 구성이고, 한쪽만 업무를 처리하며 다른 쪽이 대기하는 구성은 Active-Standby이다.

다시 나오면 이렇게 판단

사이트 이름보다 평상시 준비 상태와 장애 후 추가 작업의 양을 확인한다. 실시간 완전 이중화는 Mirror, 즉시 전환 가능한 가동 준비 상태는 Hot, 일부 자원만 준비된 상태는 Warm, 기반 시설만 있고 장비를 사후 확보하는 상태는 Cold로 판단한다.

암기 포인트

복구 속도와 준비 수준은 Mirror → Hot → Warm → Cold 순이며, Active-Active와 비가동 대기는 동시에 성립하지 않는다.

NoteBase

문 5. 파일 소유자가 자신의 파일 권한을 변경하는 접근통제 방법으로 가장 적절한 것은?

① MAC(Mandatory Access Control)

② DAC(Discretionary Access Control)

③ Non-DAC(Non Discretionary Access Control)

④ RBAC(Role-Based Access Control)

정답 2번

출제 포인트

이 문제는 파일 접근 권한의 결정 주체를 기준으로 DAC, MAC, Non-DAC, RBAC를 구별하는 문제이다.

핵심 개념

DAC(임의적 접근통제): 객체의 소유자가 자신의 판단에 따라 해당 객체의 접근 권한을 부여하거나 변경하는 방식이다. 키워드는 '소유자 재량'이다.
MAC(강제적 접근통제): 보안 등급과 보안 정책에 따라 시스템이 접근을 강제하며, 개별 소유자가 임의로 권한을 바꾸지 못하는 방식이다.
Non-DAC(비임의적 접근통제): 권한 결정이 객체 소유자의 재량이 아니라 조직이나 시스템의 정책에 의해 이루어지는 방식이다.
RBAC(역할 기반 접근통제): 사용자에게 직접 권한을 하나씩 주기보다 직무나 역할에 권한을 부여하고 사용자를 역할에 배정하는 방식이다.

선지별 해설

① X — MAC은 보안 등급과 중앙의 강제 정책에 따라 접근을 통제하므로 파일 소유자가 자신의 판단으로 권한을 변경하는 방식이 아니다. 틀린 대응은 '소유자가 자신의 파일 권한을 변경하는 방식 = MAC'이며, 올바르게는 DAC이다.
② O — DAC에서는 파일과 같은 객체의 소유자가 다른 사용자의 접근 권한을 자신의 재량으로 부여하거나 변경할 수 있다. 문제의 '파일 소유자'와 '자신의 파일 권한 변경'이 DAC의 핵심 특징에 해당한다.
③ X — Non-DAC은 권한을 객체 소유자의 재량이 아닌 조직 또는 시스템의 정책으로 결정하는 비임의적 접근통제이므로 제시된 상황과 맞지 않는다. 틀린 대응은 '소유자가 자신의 파일 권한을 변경하는 방식 = Non-DAC'이며, 올바르게는 DAC이다.
④ X — RBAC은 역할에 권한을 묶고 사용자를 그 역할에 배정하는 방식이므로 파일 소유자의 재량을 기준으로 하지 않는다. 틀린 대응은 '소유자가 자신의 파일 권한을 변경하는 방식 = RBAC'이며, 올바르게는 DAC이다.

NoteBase

오답 포인트

‘접근 권한을 변경한다’는 표현만 보고 역할이나 중앙 관리 방식을 고르면 안 된다. 이 문항의 결정적 단서는 권한을 정하는 주체가 ‘파일 소유자’라는 점이며, 이는 DAC의 소유자 재량을 뜻한다.

다시 나오면 이렇게 판단

권한 결정 주체를 먼저 확인한다. 객체 소유자가 정하면 DAC, 보안 등급과 강제 정책이 정하면 MAC, 직무·역할이 정하면 RBAC으로 판단한다.

암기 포인트

소유자 재량은 DAC, 등급에 따른 강제는 MAC, 직무 역할은 RBAC이다.

NoteBase

문 6. 다음 사업 연속성 계획(BCP, Business Continuity Planning)에 관한 절차 중 빈칸 ㉠~㉢에 들어갈 단계로 올바르게 짝지어진 것은?

범위 설정 및 기획 → (㉠) → (㉡) → (㉢) → 수행 테스트 → 계획의 유지 보수

① ㉠: 복구계획 수립, ㉡: 복구전략 개발, ㉢: 사업영향평가

② ㉠: 복구계획 수립, ㉡: 사업영향평가, ㉢: 복구전략 개발

③ ㉠: 사업영향평가, ㉡: 복구계획 수립, ㉢: 복구전략 개발

④ ㉠: 사업영향평가, ㉡: 복구전략 개발, ㉢: 복구계획 수립

정답 4번

출제 포인트

사업 연속성 계획에서 사업영향평가의 결과를 바탕으로 복구전략을 정하고, 그 전략을 실행할 복구계획을 수립한다는 선후관계를 묻는 문제이다.

올바른 순서

범위 설정 및 기획 → 사업영향평가 → 복구전략 개발 → 복구계획 수립 → 수행 테스트 → 계획의 유지 보수

1. 범위 설정 및 기획 — BCP의 대상과 범위, 추진 방향을 정한다.
2. 사업영향평가 — 업무 중단이 조직에 미치는 영향을 분석하고 핵심 업무와 복구 요구를 파악한다.
3. 복구전략 개발 — 사업영향평가 결과에 맞추어 업무와 자원을 어떻게 복구할지 대안을 정한다.
4. 복구계획 수립 — 선택한 복구전략을 실제로 수행할 절차와 역할을 구체화한다.
5. 수행 테스트 — 계획이 실제로 작동하는지 시험한다.
6. 계획의 유지 보수 — 테스트 결과와 환경 변화를 반영하여 계획을 갱신한다.

이 순서가 되는 이유는 사업영향평가에서 확인한 복구 요구가 복구전략 선택의 근거가 되고, 선택된 복구전략이 구체적인 복구계획 수립의 입력이 되기 때문이다.

NoteBase

선지별 해설

① X — '복구계획 수립 → 복구전략 개발 → 사업영향평가'는 필요한 분석과 전략보다 계획을 먼저 세우므로 선후관계가 모두 뒤바뀌었다. 올바르게는 '사업영향평가 → 복구전략 개발 → 복구계획 수립'이다.

② X — '복구계획 수립'이 사업영향평가보다 먼저 놓인 부분이 틀렸다. 업무 중단의 영향과 복구 요구를 먼저 파악해야 계획을 세울 수 있다. 올바르게는 '사업영향평가 → 복구전략 개발 → 복구계획 수립'이다.

③ X — '복구계획 수립 → 복구전략 개발'의 순서가 틀렸다. 복구전략을 먼저 선택한 뒤 그 전략을 실행할 구체적인 계획을 수립한다. 올바르게는 '사업영향평가 → 복구전략 개발 → 복구계획 수립'이다.

④ O — 사업영향평가로 복구 요구를 파악하고, 그 결과에 따라 복구전략을 개발한 다음, 전략을 실행할 복구계획을 수립하는 올바른 순서이다.

오답 포인트

'복구전략 개발'과 '복구계획 수립'을 바꾸기 쉽다. 전략은 무엇을 어떤 방식으로 복구할지 정하는 상위 방향이고, 계획은 선택한 전략을 누가 어떻게 실행할지 구체화한 것이므로 전략이 계획보다 앞선다.

다시 나오면 이렇게 판단

절차형 문제에서는 앞 단계의 산출물이 뒤 단계의 입력이 되는지를 확인한다. BCP에서는 영향과 요구를 분석한 뒤 전략을 선택하고, 선택된 전략을 실행 계획으로 구체화한다.

암기 포인트

영향을 평가하고, 전략을 정하고, 계획을 세운다: 영향 → 전략 → 계획.

NoteBase

문 7. FRR(False Rejection Rate)과 FAR(False Acceptance Rate)은 생체인증 기술의 정확성을 나타낸다. 생체인증 시스템에 관한 설명 중 가장 적절하지 않은 것은?

① 사용자 편의성을 요구할 경우 FRR이 낮아진다.

② 사용자 편의성을 요구할 경우 FAR이 높아진다.

③ 시스템의 보안성을 강화할 경우 FRR이 낮아진다.

④ 시스템의 보안성을 강화할 경우 FAR이 낮아진다.

정답 3번

출제 포인트

생체인증의 수용 기준을 완화하거나 강화할 때 FRR과 FAR이 서로 반대 방향으로 변한다는 점을 묻는 문제이다.

핵심 개념

FRR(False Rejection Rate)은 정당한 사용자를 잘못 거부하는 비율이고, FAR(False Acceptance Rate)은 비인가 사용자를 잘못 수용하는 비율이다.
사용자 편의성을 높이려고 수용 기준을 완화하면 FRR은 낮아지고 FAR은 높아진다. 반대로 보안성을 강화하려고 수용 기준을 엄격하게 하면 FAR은 낮아지고 FRR은 높아진다.

선지별 해설

① O — 사용자 편의성을 높이기 위해 수용 기준을 완화하면 정당한 사용자가 거부될 가능성이 줄어 FRR이 낮아진다.
② O — 수용 기준을 완화하면 비인가 사용자까지 잘못 수용할 가능성이 커져 FAR이 높아진다.
③ X — 틀린 표현은 '보안성을 강화할 경우 FRR이 낮아진다'이다. 보안성을 강화하여 수용 기준을 엄격하게 하면 정당한 사용자도 거부될 가능성이 커지므로 FRR은 높아진다.
④ O — 보안성을 강화하여 수용 기준을 엄격하게 하면 비인가 사용자를 잘못 수용할 가능성이 줄어 FAR이 낮아진다.

오답 포인트

③은 보안 강화가 모든 오류율을 함께 낮춘다고 착각하게 만든다. 일반적인 임계값 조정에서는 FRR과 FAR이 상충하므로 보안성을 높이면 FAR은 낮아지지만 FRR은 높아진다.

다시 나오면 이렇게 판단

편의성 강화는 수용 기준 완화로 연결하여 'FRR 하락·FAR 상승'으로 판단하고, 보안성 강화는 수용 기준 엄격화로 연결하여 'FRR 상승·FAR 하락'으로 판단한다.

NoteBase

암기 포인트

편의성은 FRR↓·FAR↑, 보안성은 FRR↑·FAR↓이다.

NoteBase

문 8. 다음 ㉠~㉣에서 설명하는 위험분석 방법이 올바르게 짝지어진 것은?

㉠
· 순위결정표에 위협 항목들의 우선순위를 결정하는 방법이다.
· 분석 시간이 상대적으로 짧고 이해하기가 쉽다.
㉡
· 위협의 발생 빈도를 계산하는 식을 이용하여 위험을 계량하는 방법이다.
· 위험을 정량화하여 매우 간결하게 나타낼 수 있으나, 기대 손실을 추정하는 자료의 양이 적다는 단점이 있다.
㉢
· 전문가 집단을 대상으로 한 설문조사에 의한 위험분석이다.
· 전문가 집단을 통해 정보시스템의 취약성과 위협요소를 추정하여 평가하기 때문에 비용을 절약할 수 있다.
㉣
· 미래에 일어날 수 있는 여러 상황을 이론적으로 예측하는 방법이다.
· 어떤 사건도 기대하는 대로 발생하지 않는다는 사실에 근거하여 일정 조건에서 위협에 대해 발생 가능한 결과들을 예측하며, 적은 정보를 가지고 전반적인 가능성을 추론할 수 있다.

① ㉠: 순위결정법, ㉡: 수학공식접근법, ㉢: 시나리오법, ㉣: 델파이법
② ㉠: 수학공식접근법, ㉡: 순위결정법, ㉢: 델파이법, ㉣: 시나리오법
③ ㉠: 순위결정법, ㉡: 수학공식접근법, ㉢: 델파이법, ㉣: 시나리오법
④ ㉠: 수학공식접근법, ㉡: 순위결정법, ㉢: 시나리오법, ㉣: 델파이법

정답 3번

출제 포인트

위험분석 방법을 설명 속 핵심 단서와 연결하는 문제이다. 순위표, 계산식, 전문가 설문, 미래 상황 예측을 각각 구별해야 한다.

핵심 개념

순위결정법: 순위결정표를 이용해 위협 항목의 우선순위를 정하는 방법이다. 분석 시간이 비교적 짧고 이해하기 쉽다.
수학공식접근법: 위협의 발생 빈도 등을 계산식에 적용하여 위험을 정량화하는 방법이다. 위험을 간결한 수치로 나타낼 수 있다.
델파이법: 전문가 집단을 대상으로 반복적인 설문과 의견 수렴을 실시하여 취약성과 위협요소를 추정·평가하는 방법이다.
시나리오법: 미래에 발생할 수 있는 여러 상황과 그 결과를 이론적으로 예측하는 방법이다. 적은 정보로도 전반적인 가능성을 추론할 수 있다.

NoteBase

선지별 해설

① X — ㉠의 순위결정법과 ㉡의 수학공식접근법은 맞지만, ㉢과 ㉣의 연결이 뒤바뀌었다. 전문가 집단 설문을 이용하는 ㉢은 델파이법이고, 미래의 여러 상황을 예측하는 ㉣은 시나리오법이다.
② X — 네 항목의 연결이 모두 뒤바뀌었다. 순위결정표를 사용하는 ㉠은 순위결정법, 계산식으로 위험을 계량하는 ㉡은 수학공식접근법, 전문가 설문을 이용하는 ㉢은 델파이법, 미래 상황을 예측하는 ㉣은 시나리오법이다.
③ O — ㉠ 순위결정법, ㉡ 수학공식접근법, ㉢ 델파이법, ㉣ 시나리오법으로 모든 설명이 올바르게 연결되어 있다.
④ X — 네 항목의 연결이 모두 뒤바뀌었다. ㉠은 순위결정법, ㉡은 수학공식접근법, ㉢은 델파이법, ㉣은 시나리오법으로 고쳐야 한다.

오답 포인트

①은 앞의 두 항목이 맞아 보이지만 ㉢의 전문가 설문과 ㉣의 미래 상황 예측을 서로 바꾸어 놓았다. 또한 ‘전문가’라는 단서는 델파이법, ‘발생 가능한 여러 결과’라는 단서는 시나리오법에 연결해야 한다.

다시 나오면 이렇게 판단

설명의 대표 단서를 먼저 찾는다. 순위표는 순위결정법, 계산식·계량화는 수학공식접근법, 전문가 설문은 델파이법, 미래의 여러 상황과 결과 예측은 시나리오법으로 판단한다.

암기 포인트

순위표는 순위결정, 계산식은 수학공식, 전문가 설문은 델파이, 미래 상황은 시나리오이다.

NoteBase

문 9. GDPR(General Data Protection Regulation) 인증에 관한 설명으로 가장 적절하지 않은 것은?

① 유럽 위원회가 제안한 것으로 유럽연합(EU) 내의 개인정보(personal data) 보호 기능을 강화하고 통합하는 개인정보에 대한 EU 규정이다.

② 적용 기업은 지점, 판매소, 영업소 등 EU 내 사업장을 운영하는 기업으로 전자상거래 등을 통해 EU 내에서 개인정보를 처리하는 기업은 제외된다.

③ 적법성, 공정성, 투명성의 원칙, 목적 제한의 원칙, 개인정보처리의 최소화, 정확성의 원칙, 보관기간제한의 원칙, 무결성 및 기밀성, 책임성을 기본 원칙으로 한다.

④ 정보주체의 명시적 동의가 있는 경우 또는 회원국 법률에 따른 경우 등을 제외하고는 민감정보(special categories of personal data)의 처리는 원칙적으로 금지된다.

정답 2번

쟁점

이 문제는 GDPR의 성격, 역외 적용범위, 개인정보 처리 원칙 및 민감정보 처리의 원칙과 예외를 구별하는 문제이다. 핵심은 EU 안에 사업장이 있는지 여부만으로 적용대상을 판단해서는 안 된다는 점이다.

용어 풀이

역외 적용 = 기업이 EU 밖에 설립되어 있어도 EU 내 정보주체에게 재화·서비스를 제공하거나 그 행동을 모니터링하는 개인정보 처리에는 GDPR이 적용될 수 있다는 의미이다.
민감정보 = 인종·민족, 정치적 견해, 종교·철학적 신념, 노동조합 가입, 유전·생체·건강 및 성생활·성적 지향 등에 관한 특별한 범주의 개인정보이다.

핵심 구분

GDPR 제3조는 EU 내 사업장의 활동과 관련된 개인정보 처리뿐 아니라, EU 밖의 개인정보처리자·수탁처리자가 EU 내 정보주체에게 재화·서비스를 제공하거나 EU 내 행동을 모니터링하는 경우에도 적용될 수 있도록 정한다. 제5조는 적법성·공정성·투명성, 목적 제한, 개인정보 최소화, 정확성, 보관기간 제한, 무결성·기밀성 및 책임성의 원칙을 규정한다. 제9조는 민감정보 처리를 원칙적으로 금지하면서 명시적 동의, 일정한 법률상 근거 등 예외를 둔다.

NoteBase

선지별 해설

① O
유럽위원회가 개인정보 보호체계의 개혁을 제안했고, GDPR은 자연인의 개인정보 보호와 개인정보의 자유로운 이동에 관한 EU 규정으로 제정되었다. EU 전역의 개인정보 보호 규칙을 통일하고 정보주체의 보호를 강화하려는 취지라는 설명은 적절하다.

② X
GDPR은 EU 내 사업장을 운영하는 기업에만 적용되는 것이 아니다. EU 밖에 설립된 기업도 EU 내 정보주체에게 전자상거래 등으로 재화·서비스를 제공하거나 그 행동을 모니터링하는 개인정보 처리에는 적용될 수 있다.
틀린 표현: '전자상거래 등을 통해 EU 내에서 개인정보를 처리하는 기업은 제외된다.'
올바른 표현: 'EU 밖의 기업이라도 EU 내 정보주체에게 재화·서비스를 제공하거나 그 행동을 모니터링하는 개인정보 처리에는 GDPR이 적용될 수 있다.'

③ O
열거된 내용은 GDPR 제5조의 개인정보 처리 원칙에 해당한다. 제5조 제1항의 여섯 원칙에 제2항의 책임성 원칙을 함께 제시한 설명이다.

④ O
GDPR 제9조는 민감정보의 처리를 원칙적으로 금지하지만, 정보주체가 특정 목적의 처리에 명시적으로 동의한 경우나 EU 또는 회원국 법률에 근거한 일정한 경우 등에는 예외적으로 처리를 허용한다. 따라서 원칙과 예외를 올바르게 설명한 선지이다.

오답 포인트

②의 함정은 GDPR의 적용범위를 'EU 내 사업장 보유 기업'으로만 좁힌 표현이다. GDPR은 기업의 설립 장소만이 아니라 EU 내 정보주체를 대상으로 한 재화·서비스 제공과 행동 모니터링이라는 처리 활동도 기준으로 삼는다.

다시 나오면 이렇게 판단

GDPR 적용범위 문제에서는 먼저 EU 내 사업장 관련 처리를 확인하고, 사업장이 없더라도 EU 내 정보주체를 대상으로 재화·서비스를 제공하거나 행동을 모니터링하는지를 추가로 확인한다. 'EU 밖 기업은 제외된다'처럼 역외 적용을 전면 부정하는 표현은 틀린 것으로 판단한다.

암기 포인트

GDPR 적용범위는 'EU 내 사업장 + EU 내 정보주체 대상 제공·모니터링'으로 기억한다.

NoteBase

문 10. Bell-Lapadula 접근통제 모델의 설명 중 가장 적절하지 않은 것은?

① 무결성을 보장할 수 있는 모델로 주체에 의한 객체 접근의 항목으로 무결성을 다룬다.

② 최초의 수학적 모델로서 보안 등급과 범주를 이용한 강제적 정책에 의한 모델이다.

③ 미 국방성(DoD)의 지원을 받아 설계된 모델로 TCSEC의 근간이 되었다.

④ 정보 구분은 Top Secret, Secret, Confidential, Unclassified로 구분된다.

정답 1번

출제 포인트

Bell-LaPadula 모델의 보호 목표가 무결성이 아니라 기밀성이라는 점과 다단계 보안 모델의 주요 특징을 구별하는 문제이다.

핵심 개념

Bell-LaPadula 모델은 보안 등급이 있는 주체와 객체 사이의 정보 흐름을 통제하여 기밀성을 보호하는 강제적 접근통제 모델이다. 핵심 규칙은 상위 등급 객체를 읽지 못하게 하는 단순 보안 속성(no read up)과 하위 등급 객체에 쓰지 못하게 하는 *-속성(no write down)이다. 반면 무결성 보호를 대표하는 모델로는 Biba 모델이 있다.

선지별 해설

① X — 틀린 표현은 '무결성을 보장'한다는 부분이다. Bell-LaPadula 모델은 주체의 객체 접근을 통제하여 기밀성을 보장하는 모델이다.
② O — Bell-LaPadula 모델은 최초의 수학적·형식적 다단계 보안 모델로 알려져 있으며, 보안 등급과 범주가 부여된 보안 레이블에 따라 강제적 접근통제를 수행한다.
③ O — Bell-LaPadula 모델은 미국 국방성의 지원 아래 개발되었고, 다단계 보안의 기밀성 원칙을 정립하여 TCSEC의 이론적 기반이 되었다.
④ O — 이 모델에서 사용하는 대표적인 정보 보안 등급은 Top Secret, Secret, Confidential, Unclassified의 순서로 구분된다.

오답 포인트

①의 '주체에 의한 객체 접근'이라는 표현만 보면 접근통제 모델의 일반 설명처럼 보이지만, 보호 목표를 '무결성'이라고 바꾼 것이 함정이다. Bell-LaPadula는 기밀성, Biba는 무결성을 중심으로 한다.

다시 나오면 이렇게 판단

모델 이름과 최우선 보호 목표를 먼저 연결한다. Bell-LaPadula는 기밀성이므로 상향 읽기와 하향 쓰기를 제한하고, Biba는 무결성이므로 그 반대 방향의 오염을 제한한다.

NoteBase

암기 포인트

Bell-LaPadula는 기밀성: 위로 읽기 금지, 아래로 쓰기 금지이다.

NoteBase

문 11. 「개인정보 보호법」 제2조(정의)에 관한 설명으로 가장 적절하지 않은 것은?

① “처리”란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기, 그 밖에 이와 유사한 행위를 말한다.

② “정보주체”란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.

③ “개인정보파일”이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물을 말한다.

④ “개인정보처리자”란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인 및 단체를 제외한 개인을 말한다.

정답 4번

쟁점

이 문제는 「개인정보 보호법」 제2조에 규정된 처리, 정보주체, 개인정보파일, 개인정보처리자의 정의에 관한 문제이다. 핵심은 개인정보처리자의 범위에 공공기관, 법인, 단체 및 개인 등이 모두 포함된다는 점이다.

용어 풀이

개인정보처리자 = 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통해 개인정보를 처리하는 주체이다.

핵심 구분

현행 「개인정보 보호법」 제2조는 개인정보처리자의 범위를 공공기관, 법인, 단체 및 개인 등으로 정한다. 따라서 개인정보처리자를 개인으로 한정하거나 공공기관·법인·단체를 제외하는 설명은 틀리다.

선지별 해설

① O — ‘처리’는 개인정보의 수집·생성부터 이용·제공·공개·파기까지 개인정보에 가하는 일련의 행위와 그 밖의 유사한 행위를 말하므로 조문의 정의와 일치한다.
② O — ‘정보주체’는 처리되는 정보로 알아볼 수 있고 그 정보의 주체가 되는 사람을 말하므로 조문의 정의와 일치한다.
③ O — ‘개인정보파일’은 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물을 말하므로 조문의 정의와 일치한다.
④ X — 개인정보처리자에는 개인뿐 아니라 공공기관, 법인 및 단체도 포함되므로 ‘공공기관, 법인 및 단체를 제외한 개인’이라는 부분이 틀리다. 틀린 표현: ‘공공기관, 법인 및 단체를 제외한 개인’. 올바른 표현: ‘공공기관, 법인, 단체 및 개인 등’.

NoteBase

오답 포인트

④는 개인정보처리자의 업무 목적과 개인정보파일 운용 요건을 앞부분에서 정확히 제시한 뒤, 주체의 범위를 개인으로 축소한 선지이다. 정의 조항에서는 문장 끝의 주체 범위까지 확인해야 한다.

다시 나오면 이렇게 판단

정의 조항 문제에서는 행위, 대상, 목적, 주체를 나누어 조문과 대조한다. 개인정보처리자의 주체는 '공공기관·법인·단체·개인 등'이라는 전체 범위로 판단한다.

암기 포인트

개인정보처리자는 개인만이 아니라 공공기관·법인·단체·개인 등을 모두 포함한다.

NoteBase

문 12. 「정보통신기반 보호법」 제6조(주요정보통신기반시설보호계획의 수립 등)에 포함되어야 하는 사항으로 가장 적절하지 않은 것은?

① 주요정보통신기반시설의 취약점 분석·평가에 관한 사항

② 주요정보통신기반시설의 설치 및 사용자 서비스에 관한 사항

③ 주요정보통신기반시설의 보호에 관하여 필요한 사항

④ 주요정보통신기반시설 및 관리 정보의 침해사고에 대한 예방, 백업, 복구대책에 관한 사항

정답 2번

쟁점

이 문제는 「정보통신기반 보호법」 제6조 제3항이 주요정보통신기반시설보호계획의 필수 포함 사항으로 열거한 내용을 묻는다. 핵심은 기반시설의 보호에 관한 사항과 시설의 설치·사용자 서비스에 관한 사항을 구별하는 것이다.

용어 풀이

주요정보통신기반시설보호계획은 관계중앙행정기관의 장이 소관 분야의 주요정보통신기반시설을 보호하기 위하여 수립·시행하는 계획이다.

핵심 구분

법 제6조 제3항은 ① 취약점 분석·평가, ② 주요정보통신기반시설 및 관리 정보의 침해사고에 대한 예방·백업·복구대책, ③ 그 밖에 주요정보통신기반시설의 보호에 필요한 사항을 보호계획의 내용으로 규정한다. 시설의 설치 및 사용자 서비스는 이 조항의 열거 사항이 아니다.

선지별 해설

① O — 주요정보통신기반시설의 취약점 분석·평가에 관한 사항은 법 제6조 제3항 제1호에 규정된 보호계획의 필수 내용이다.

② X — '주요정보통신기반시설의 설치 및 사용자 서비스에 관한 사항'은 법 제6조 제3항에 열거되어 있지 않다. 틀린 표현은 '설치 및 사용자 서비스'이며, 올바르게는 '주요정보통신기반시설 및 관리 정보의 침해사고에 대한 예방, 백업, 복구대책에 관한 사항'이다.

③ O — 주요정보통신기반시설의 보호에 관하여 필요한 사항은 법 제6조 제3항 제3호의 포괄 항목에 해당한다.

④ O — 주요정보통신기반시설 및 관리 정보의 침해사고에 대한 예방, 백업, 복구대책은 법 제6조 제3항 제2호에 규정된 보호계획의 필수 내용이다.

NoteBase

오답 포인트

②의 '설치 및 사용자 서비스'는 정보통신시설과 관련되어 보여 그럴듯하지만, 보호계획의 법정 항목은 취약점 분석·평가와 침해사고의 예방·백업·복구 등 보호 활동을 중심으로 구성된다.

다시 나오면 이렇게 판단

선지의 핵심어가 '취약점 분석·평가', '침해사고 예방·백업·복구', '그 밖의 보호 필요 사항' 중 하나에 해당하는지 확인한다. 시설의 설치나 일반 사용자 서비스처럼 보호 활동과 직접 관련되지 않은 내용은 제외한다.

암기 포인트

보호계획의 세 축은 '취약점 분석·평가 — 침해사고 예방·백업·복구 — 그 밖의 보호 필요 사항'이다.

NoteBase

문 13. 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제2조(정의)에 관한 설명으로 가장 적절하지 않은 것은?

① “클라우드컴퓨팅”이란 집적·공유된 정보통신기기, 정보통신설비, 소프트웨어 등 정보통신자원을 이용자의 요구나 수요 변화에 따라 정보통신망을 통하여 신축적으로 이용할 수 있도록 하는 정보처리체계를 말한다.

② “클라우드컴퓨팅기술”이란 클라우드컴퓨팅의 구축 및 이용에 관한 정보통신기술로서 가상화 기술, 분산처리 기술 등 대통령령으로 정하는 것을 말한다.

③ “클라우드컴퓨팅서비스”란 클라우드컴퓨팅을 활용하여 상용으로 타인에게 정보통신자원을 제공하는 서비스로서 대통령령으로 정하는 것을 말한다.

④ “이용자 정보”란 클라우드컴퓨팅서비스 이용자가 클라우드컴퓨팅서비스를 이용하여 클라우드컴퓨팅서비스를 제공하는 자의 정보통신자원에 저장하는 정보로서 클라우드컴퓨팅서비스 제공자가 소유 또는 관리하는 정보를 말한다.

정답 4번

쟁점

이 문제는 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제2조의 법정 정의에 관한 문제이다. 핵심은 정보통신자원의 제공·관리 주체와 그 자원에 저장된 이용자 정보의 소유·관리 주체를 구별하는 것이다.

용어 풀이

이용자 정보 = 이용자가 클라우드컴퓨팅서비스를 이용하여 서비스 제공자의 정보통신자원에 저장하는 정보로서, 이용자가 소유하거나 관리하는 정보이다.

핵심 구분

현행 법률 제2조는 클라우드컴퓨팅, 클라우드컴퓨팅기술, 클라우드컴퓨팅서비스 및 이용자 정보를 각각 정의한다. 저장 장소인 정보통신자원은 클라우드컴퓨팅서비스 제공자의 것이지만, 그곳에 저장되는 이용자 정보는 이용자가 소유 또는 관리한다.

NoteBase

선지별 해설

① O
집적·공유된 정보통신자원을 이용자의 요구나 수요 변화에 따라 정보통신망을 통하여 신축적으로 이용할 수 있게 하는 정보처리체계라는 설명은 클라우드컴퓨팅의 법정 정의에 해당한다.

② O
클라우드컴퓨팅의 구축 및 이용에 관한 정보통신기술 중 가상화 기술, 분산처리 기술 등 대통령령으로 정하는 기술이라는 설명은 클라우드컴퓨팅기술의 법정 정의에 해당한다.

③ O
클라우드컴퓨팅을 활용하여 상용으로 타인에게 정보통신자원을 제공하는 서비스로서 대통령령으로 정하는 것이라는 설명은 클라우드컴퓨팅서비스의 법정 정의에 해당한다.

④ X
이용자 정보의 소유 또는 관리 주체를 클라우드컴퓨팅서비스 제공자로 바꾸어 서술했으므로 틀리다.
틀린 표현: 클라우드컴퓨팅서비스 제공자가 소유 또는 관리하는 정보
올바른 표현: 클라우드컴퓨팅서비스 이용자가 소유 또는 관리하는 정보

오답 포인트

④는 정보가 저장되는 정보통신자원의 주체와 저장된 정보의 소유·관리 주체를 뒤바꾼 선지이다. 제공자의 정보통신자원에 저장된다는 사실만으로 그 정보까지 제공자가 소유하거나 관리하는 것은 아니다.

다시 나오면 이렇게 판단

법정 정의 문제에서는 대상, 행위, 주체를 나누어 확인한다. 이용자 정보에 관해서는 '제공자의 정보통신자원에 저장'과 '이용자가 소유 또는 관리'를 서로 다른 요소로 구분하면 된다.

암기 포인트

저장 자원은 제공자, 저장 정보의 소유·관리는 이용자이다.

NoteBase

문 14. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제45조의3 (정보보호 최고책임자의 지정 등)에서 정한 정보보호 최고책임자 업무 중 가장 적절하지 않은 것은?

① 정보보호 계획의 수립·시행 및 개선

② 정보보호 실태와 관행의 정기적인 감사 및 개선

③ 정보보호 협회의 설립과 운영 및 개선

④ 정보보호 위험의 식별 평가 및 정보보호 대책 마련

정답 3번

쟁점

이 문제는 정보보호 최고책임자가 총괄하는 법정 업무와 정보통신서비스 제공자가 구성·운영할 수 있는 협의회를 구별하는 문제이다.

용어 풀이

정보보호 최고책임자(CISO)는 조직의 정보보호 업무를 총괄하는 책임자이다. 정보보호 최고책임자 협의회는 침해사고의 공동 예방·대응과 정보 교류 등을 위하여 정보통신서비스 제공자가 구성·운영할 수 있는 협의체이다.

핵심 구분

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제45조의3은 정보보호 계획의 수립·시행 및 개선, 정보보호 실태와 관행의 정기적인 감사 및 개선, 정보보호 위험의 식별 평가 및 대책 마련 등을 정보보호 최고책임자의 업무로 정한다. 반면 정보보호 최고책임자 협의회의 구성·운영은 정보통신서비스 제공자가 할 수 있는 사항이지, 정보보호 최고책임자 개인의 법정 업무가 아니다.

선지별 해설

① O — 정보보호 계획의 수립·시행 및 개선은 정보보호 최고책임자가 총괄하는 법정 업무이다.
② O — 정보보호 실태와 관행을 정기적으로 감사하고 개선하는 것도 법정 업무이다.
③ X — '정보보호 협회의 설립과 운영 및 개선'은 정보보호 최고책임자의 법정 업무로 열거되어 있지 않다. 틀린 표현: 정보보호 협회의 설립과 운영 및 개선. 올바른 표현: 정보보호 교육과 모의 훈련 계획의 수립 및 시행 등이 정보보호 최고책임자의 업무이며, 정보보호 최고책임자 협의회는 정보통신서비스 제공자가 구성·운영할 수 있다.
④ O — 정보보호 위험을 식별·평가하고 그에 따른 정보보호 대책을 마련하는 것은 법정 업무이다.

NoteBase

오답 포인트

③은 같은 조에 등장하는 '정보보호 최고책임자 협의회'와 '정보보호 최고책임자의 업무'를 섞은 선지이다. 협의회를 구성·운영할 수 있는 주체는 정보통신서비스 제공자이며, 협의회 관련 사항을 최고책임자의 업무 목록으로 볼 수 없다.

다시 나오면 이렇게 판단

법령형 선지에서는 업무의 내용뿐 아니라 그 업무의 주체를 함께 확인한다. 계획 수립, 감사, 위험 식별·평가, 교육·훈련은 최고책임자의 업무이고, 협의회 구성·운영은 정보통신서비스 제공자에게 허용된 사항으로 구분한다.

암기 포인트

CISO 업무는 계획·감사·위험·교육이고, 협의회 구성·운영의 주체는 정보통신서비스 제공자이다.

NoteBase

문 15. 「개인정보 보호법」 제15조(개인정보의 수집·이용)에서 정한 개인정보처리자가 정보주체에게 동의를 받을 때 정보주체에게 알려야 하는 사항으로 가장 적절하지 않은 것은?

① 개인정보의 수집·이용 목적

② 수집하려는 개인정보의 항목

③ 개인정보의 보유 및 이용 기간

④ 수집기관의 명칭 및 기관 현황

정답 4번

쟁점

이 문제는 개인정보처리자가 정보주체의 동의를 받아 개인정보를 수집·이용할 때 고지해야 하는 사항에 관한 문제이다. 핵심은 「개인정보 보호법」 제15조 제2항의 고지사항과 법에서 요구하지 않는 사항을 구별하는 것이다.

용어 풀이

고지사항은 정보주체가 동의 여부를 판단할 수 있도록 개인정보처리자가 동의를 받기 전에 알려야 하는 법정 사항이다.

핵심 구분

「개인정보 보호법」 제15조 제2항은 수집·이용 목적, 수집하려는 개인정보의 항목, 개인정보의 보유 및 이용 기간, 동의를 거부할 권리와 거부에 따른 불이익이 있는 경우 그 내용을 고지하도록 정한다. 수집기관의 명칭 및 기관 현황은 이 조항이 열거한 고지사항이 아니다.

선지별 해설

① O — 개인정보의 수집·이용 목적은 정보주체에게 알려야 하는 사항이다. 정보주체는 자신의 정보가 어떤 목적으로 처리되는지를 알고 동의해야 한다.
② O — 수집하려는 개인정보의 항목은 고지사항이다. 어떤 정보가 수집되는지를 구체적으로 알려야 동의의 대상이 명확해진다.
③ O — 개인정보의 보유 및 이용 기간은 고지사항이다. 정보가 언제까지 보유·이용되는지를 알려야 한다.
④ X — '수집기관의 명칭 및 기관 현황'은 제15조 제2항이 정한 고지사항이 아니다. 틀린 표현: 수집기관의 명칭 및 기관 현황. 올바른 표현: 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우 그 불이익의 내용.

NoteBase

오답 포인트

기관을 식별하는 정보가 필요해 보인다는 이유만으로 법정 고지사항이라고 판단하기 쉽다. 그러나 제15조 제2항의 네 항목은 처리 목적·수집 항목·보유 및 이용 기간·동의 거부권과 불이익이다.

다시 나오면 이렇게 판단

개인정보 수집·이용 동의의 고지사항을 묻는 문제에서는 '왜 수집하는가, 무엇을 수집하는가, 언제까지 쓰는가, 거부할 수 있는가'를 차례로 대조한다. 이 네 범주에 들어가지 않는 기관 현황 등의 표현은 제외한다.

암기 포인트

수집·이용 동의 고지는 '목적·항목·기간·거부권과 불이익'이다.

NoteBase

문 16. 「정보통신기반 보호법」 제8조(주요정보통신기반시설의 지정 등)에서 주요정보통신기반시설을 지정할 때 주요 고려사항으로 가장 적절하지 않은 것은?

① 기관이 수행하는 업무의 개인정보 보유 건수

② 다른 정보통신기반시설과의 상호연계성

③ 해당 정보통신기반시설을 관리하는 기관이 수행하는 업무의 국가사회적 중요성

④ 침해사고가 발생할 경우 국가안전보장과 경제사회에 미치는 피해규모 및 범위

정답 1번

쟁점

이 문제는 「정보통신기반 보호법」상 주요정보통신기반시설을 지정할 때 고려하는 사항에 관한 문제이다. 핵심은 시설의 국가사회적 중요성·의존도·상호연계성·침해사고 위험 및 파급효과와 개인정보 보유 건수를 구별하는 것이다.

용어 풀이

주요정보통신기반시설은 전자적 침해행위로부터 보호할 필요가 있어 중앙행정기관의 장 등이 법에 따라 지정하는 중요한 정보통신기반시설이다.

핵심 구분

「정보통신기반 보호법」 제8조 제1항은 관리기관 업무의 국가사회적 중요성, 그 업무의 정보통신기반시설 의존도, 다른 정보통신기반시설과의 상호연계성, 침해사고 발생 시 피해규모 및 범위, 침해사고의 발생가능성 또는 복구 용이성을 지정 고려사항으로 규정한다. 개인정보 보유 건수는 이 조항이 열거한 고려사항이 아니다.

선지별 해설

① X — '기관이 수행하는 업무의 개인정보 보유 건수'는 제8조 제1항이 정한 지정 고려사항이 아니다. 틀린 표현은 '개인정보 보유 건수'이며, 올바르게는 '기관이 수행하는 업무의 정보통신기반시설에 대한 의존도'가 고려사항이다.

② O — 다른 정보통신기반시설과의 상호연계성은 한 시설의 침해가 다른 시설로 확산될 가능성과 관련되므로 법정 고려사항이다.

③ O — 해당 시설을 관리하는 기관이 수행하는 업무의 국가사회적 중요성은 제8조 제1항이 명시한 고려사항이다.

④ O — 침해사고 발생 시 국가안전보장과 경제사회에 미치는 피해규모 및 범위는 사고의 파급효과를 판단하는 법정 고려사항이다.

NoteBase

오답 포인트

개인정보 보호의 중요성 때문에 ①도 그럴듯해 보이지만, 이 문항은 일반적인 보안 중요성이 아니라 제8조 제1항에 열거된 지정 기준을 묻는다. '개인정보 보유 건수'와 법정 기준인 '정보통신기반시설에 대한 의존도'를 바꾸어 놓은 것이 함정이다.

다시 나오면 이렇게 판단

주요정보통신기반시설의 지정 기준은 업무의 중요성과 기반시설 의존도, 시설 간 연계성, 사고의 발생·복구 가능성, 피해의 규모·범위라는 구조로 판단한다. 개인정보의 수량처럼 이 구조에 포함되지 않는 별도 지표는 법정 열거사항인지 확인한다.

암기 포인트

주요정보통신기반시설 지정은 '중요성·의존도·연계성·피해·발생 및 복구'를 본다. 개인정보 보유 건수는 해당 조문의 지정 기준이 아니다.

NoteBase

문 17. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제45조의3(정보보호 최고책임자의 지정 등)에서 정한 정보보호 최고책임자의 겸직 가능한 업무로 가장 적절하지 않은 것은?

① 「정보보호산업의 진흥에 관한 법률」 제13조에 따른 정보보호 공시에 관한 업무

② 「정보통신기반 보호법」 제5조제5항에 따른 정보보호책임자의 업무

③ 「전자금융거래법」 제21조의2제4항에 따른 정보보호최고책임자의 업무

④ 「개인정보 보호법」 제31조제2항에 따른 조직관리 인사총괄책임자의 업무

정답 4번

쟁점

이 문제는 정보보호 최고책임자가 본래의 정보보호 업무와 함께 맡을 수 있는 법정 겸직 업무의 범위를 묻는다. 핵심은 다른 법률상의 정보보호·개인정보 보호 업무와 일반적인 조직·인사 업무를 구별하는 것이다.

용어 풀이

정보보호 최고책임자 = 조직의 정보보호 계획, 위험 관리, 감사, 교육 등 정보보호 업무를 총괄하는 책임자이다.

핵심 구분

정보보호 최고책임자는 법에서 열거한 정보보호 관련 업무를 겸할 수 있다. 여기에는 정보보호 공시 업무, 주요정보통신기반시설의 정보보호책임자 업무, 전자금융 분야의 정보보호최고책임자 업무, 개인정보 보호책임자 업무가 포함된다. 반면 일반적인 조직관리·인사총괄 업무는 열거된 겸직 업무가 아니다.

선지별 해설

① O — 「정보보호산업의 진흥에 관한 법률」에 따른 정보보호 공시 업무는 정보보호 최고책임자가 겸할 수 있는 업무로 열거되어 있다.

② O — 「정보통신기반 보호법」에 따른 정보보호책임자의 업무는 정보보호 최고책임자가 겸할 수 있는 업무이다.

③ O — 「전자금융거래법」에 따른 정보보호최고책임자의 업무도 정보보호와 직접 관련된 법정 겸직 가능 업무이다.

④ X — 「개인정보 보호법」이 정한 직책은 '조직관리 인사총괄책임자'가 아니라 '개인정보 보호책임자'이다.
틀린 표현: 조직관리 인사총괄책임자의 업무
올바른 표현: 개인정보 보호책임자의 업무

NoteBase

오답 포인트

④는 조문 번호와 법률명은 그럴듯하게 제시하면서 책임자의 명칭만 바꾼 선지이다. 개인정보 보호법상의 법정 직책은 개인정보 보호책임자이며, 조직관리 인사총괄책임자는 이 조문이 허용하는 겸직 업무가 아니다.

다시 나오면 이렇게 판단

겸직 가능 여부는 업무가 보안과 막연히 관련되는지만 보지 않고, 법이 열거한 직책·업무의 정확한 명칭과 대조하여 판단한다. 특히 개인정보 보호법과 연결되는 직책은 개인정보 보호책임자이다.

암기 포인트

정보보호 최고책임자의 겸직 업무는 정보보호 공시·기반시설 보호·전자금융 보호·개인정보 보호이고, 일반 조직·인사 총괄은 아니다.

NoteBase

문 18. 「위치정보의 보호 및 이용 등에 관한 법률」 제16조(위치정보의 보호조치 등) 및 동법 시행령 제20조(위치정보의 관리적·기술적 보호조치)에서 정한 내용으로 가장 적절하지 않은 것은?

① 위치정보의 수집·이용·제공·파기 등 각 단계별 접근 권한자 지정 및 권한의 제한

② 위치정보시스템의 원활한 사용을 위한 사용자 인터페이스의 설치 및 운영

③ 위치정보시스템에의 권한 없는 접근을 차단하기 위한 방화벽 설치 등의 조치

④ 위치정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용이나 이에 상응하는 조치

정답 2번

쟁점

이 문제는 위치정보를 안전하게 보호하기 위해 요구되는 관리적·기술적 보호조치의 내용을 구별하는 문제이다. 핵심은 업무 담당자와 권한을 통제하는 관리적 조치와 시스템 접근·저장·전송을 보호하는 기술적 조치를 구분하는 것이다.

용어 풀이

관리적 보호조치는 책임자·접근권한·취급절차처럼 사람과 업무 절차를 통제하는 조치이고, 기술적 보호조치는 인증·방화벽·접근기록·보안프로그램·암호화처럼 정보시스템을 기술적으로 보호하는 조치이다.

핵심 구분

현행 「위치정보의 보호 및 이용 등에 관한 법률 시행령」 제20조는 단계별 접근 권한자의 지정과 권한 제한을 관리적 조치로 정하고, 권한 없는 접근을 막는 방화벽과 안전한 저장·전송을 위한 암호화 등을 기술적 조치로 정한다. 사용자 편의를 위한 인터페이스 설치·운영은 위치정보 보호를 위한 관리적·기술적 조치에 해당하지 않는다.

선지별 해설

① O — 위치정보의 수집·이용·제공·파기 단계별로 접근 권한자를 지정하고 권한을 제한하는 것은 관리적 보호조치에 해당한다.

② X — '위치정보시스템의 원활한 사용을 위한 사용자 인터페이스의 설치 및 운영'은 법령이 정한 보호조치가 아니다. 틀린 표현은 '사용자 인터페이스의 설치 및 운영'이며, 올바르게는 위치정보시스템의 침해사고 방지를 위한 보안프로그램의 설치 및 운영 등이 기술적 보호조치에 해당한다.

③ O — 위치정보시스템에 대한 권한 없는 접근을 차단하기 위한 방화벽 설치 등의 조치는 기술적 보호조치에 해당한다.

④ O — 위치정보를 안전하게 저장·전송할 수 있도록 암호화 기술을 적용하거나 이에 상응하는 조치를 하는 것은 기술적 보호조치에 해당한다.

NoteBase

오답 포인트

②의 '원활한 사용'과 '사용자 인터페이스'는 시스템 편의성과 사용성을 높이는 표현일 뿐, 위치정보의 접근 통제나 유출·침해 방지를 위한 보호조치가 아니다. '설치 및 운영'이라는 형식만 보고 보안프로그램과 혼동하기 쉽다.

다시 나오면 이렇게 판단

선지의 목적이 접근권한 통제, 무단 접근 차단, 접근기록 보존, 침해사고 방지, 암호화 등 위치정보 보호에 직접 연결되는지를 확인한다. 단순한 이용 편의성이나 원활한 사용을 위한 기능은 보호조치에서 제외한다.

암기 포인트

사람과 절차는 관리적 조치, 인증·방화벽·기록·보안프로그램·암호화는 기술적 조치이다. 사용자 인터페이스는 보호조치가 아니다.

NoteBase

문 19. 다음 중 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 시행령」 제3조(클라우드컴퓨팅서비스)에서 정한 서비스를 고른 것으로 가장 적절한 것은?

㉠ 서버, 저장장치, 네트워크 등을 제공하는 서비스
㉡ 응용프로그램 등 소프트웨어를 제공하는 서비스
㉢ 로컬 장치에 응용프로그램의 데이터를 저장하는 서비스
㉣ 응용프로그램 등 소프트웨어의 개발·배포·운영·관리 등을 위한 환경을 제공하는 서비스

① ㉠㉡㉢
② ㉠㉡㉣
③ ㉠㉢㉣
④ ㉡㉢㉣

정답 2번

쟁점

이 문제는 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 시행령」 제3조가 정한 클라우드컴퓨팅서비스의 범위에 관한 문제이다. 핵심은 기반 자원 제공, 소프트웨어 제공, 소프트웨어 개발·배포·운영·관리 환경 제공을 로컬 장치의 데이터 저장과 구별하는 것이다.

용어 풀이

클라우드컴퓨팅서비스는 클라우드컴퓨팅을 활용하여 타인에게 정보통신자원을 제공하는 서비스이다. 시행령 제3조는 제공 대상에 따라 기반 자원, 소프트웨어, 소프트웨어 개발·운영 환경 및 이들의 복합 서비스를 열거한다.

핵심 구분

시행령 제3조는 ㉠ 서버·저장장치·네트워크 등을 제공하는 서비스, ㉡ 응용프로그램 등 소프트웨어를 제공하는 서비스, ㉣ 소프트웨어의 개발·배포·운영·관리 등을 위한 환경을 제공하는 서비스를 포함한다. 또한 이들 서비스를 둘 이상 복합한 서비스도 포함한다. 반면 ㉢ 로컬 장치에 응용프로그램의 데이터를 저장하는 서비스는 제3조가 열거한 유형이 아니다. 따라서 옳은 조합은 ㉠㉡㉣이다.

NoteBase

선지별 해설

① X — ㉠과 ㉡은 맞지만 ㉢이 포함되고 ㉣이 빠져 있다. 틀린 표현: ㉠㉡㉢. 올바른 표현: ㉠㉡㉣이다.
② O — ㉠은 기반 자원 제공, ㉡은 소프트웨어 제공, ㉣은 소프트웨어 개발·배포·운영·관리 환경 제공으로서 모두 시행령 제3조에 열거된 서비스이다.
③ X — ㉠과 ㉣은 맞지만 ㉢이 포함되고 ㉡이 빠져 있다. 틀린 표현: ㉠㉢㉣. 올바른 표현: ㉠㉡㉣이다.
④ X — ㉡과 ㉣은 맞지만 ㉢이 포함되고 ㉠이 빠져 있다. 틀린 표현: ㉡㉢㉣. 올바른 표현: ㉠㉡㉣이다.

오답 포인트

㉢의 '로컬 장치에 데이터 저장'도 일반적인 컴퓨팅 기능이므로 클라우드 서비스처럼 보이는 것이 함정이다. 그러나 이 문항은 일반적 기능이 아니라 시행령 제3조가 열거한 서비스인지 묻는다. 로컬 장치 저장은 열거된 유형이 아니고, ㉣의 개발·배포·운영·관리 환경 제공은 명시된 유형이다.

다시 나오면 이렇게 판단

제공 대상을 기준으로 구분한다. 서버·저장장치·네트워크는 기반 자원, 응용프로그램은 소프트웨어, 개발·배포·운영·관리 도구는 환경 제공에 해당한다. '로컬 장치 저장'이 제시되면 법령의 열거 문구가 아니므로 제외한다.

암기 포인트

클라우드 서비스의 세 축은 자원 제공, 소프트웨어 제공, 개발·운영 환경 제공이다. 로컬 저장은 제외한다.

NoteBase

문 20. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조(정의)에 관한 설명으로 가장 적절하지 않은 것은?

① “정보통신서비스”란 「전기통신사업법」 제2조제6호에 따른 전기통신역무와 이를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 것을 말한다.

② “전자문서”란 컴퓨터 등 정보처리능력을 가진 장치에 의하여 전자적인 형태로 작성되어 송수신되거나 저장된 문서형식의 자료로서 표준화된 것을 말한다.

③ “게시판”이란 그 명칭과 관계없이 정보통신망을 이용하여 저장장치에 저장할 목적으로 부호·문자·음성·화상·동영상 등의 정보를 이용자가 로컬 저장장치에 저장할 수 있는 컴퓨터 프로그램이나 기술적 장치를 말한다.

④ “전자적 전송매체”란 정보통신망을 통하여 부호·문자·음성·화상 또는 영상 등을 수신자에게 전자문서 등의 전자적 형태로 전송하는 매체를 말한다.

정답 3번

쟁점

이 문제는 정보통신망법 제2조의 법정 용어 정의에 관한 문제이다. 핵심은 각 선지의 문언이 법률에 규정된 목적·행위·대상과 일치하는지를 구별하는 것이다.

용어 풀이

게시판 = 명칭과 관계없이, 이용자가 정보통신망을 이용하여 일반에게 공개할 목적으로 정보를 게재할 수 있게 하는 컴퓨터 프로그램이나 기술적 장치이다.

핵심 구분

정보통신망법 제2조 제1항은 정보통신서비스, 전자문서, 게시판, 전자적 전송매체를 각각 정의한다. 게시판은 정보를 로컬 저장장치에 저장하는 수단이 아니라, 이용자가 정보를 일반에게 공개할 목적으로 게재할 수 있게 하는 수단이다.

NoteBase

선지별 해설

① O
정보통신서비스는 전기통신사업법상 전기통신역무와, 그 역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 것을 말한다. 법정 정의와 일치한다.

② O
전자문서는 정보처리능력을 가진 장치에 의하여 전자적 형태로 작성되어 송수신되거나 저장된 문서형식의 자료로서 표준화된 것을 말한다. 법정 정의와 일치한다.

③ X
게시판의 핵심은 이용자가 정보를 일반에게 공개할 목적으로 게재할 수 있다는 점이다. 선지처럼 이용자가 정보를 로컬 저장장치에 저장하는 프로그램이나 장치를 뜻하지 않는다.
틀린 표현: 저장장치에 저장할 목적으로, 이용자가 로컬 저장장치에 저장할 수 있는
올바른 표현: 일반에게 공개할 목적으로, 이용자가 정보를 게재할 수 있는

④ O
전자적 전송매체는 정보통신망을 통하여 부호·문자·음성·화상 또는 영상 등을 수신자에게 전자문서 등의 전자적 형태로 전송하는 매체를 말한다. 법정 정의와 일치한다.

오답 포인트

③은 실제 정의의 '일반에게 공개'와 '게재'를 '저장장치에 저장'과 '로컬 저장'으로 바꾸었다. 게시판의 공개·게재 기능을 개인 장치의 저장 기능과 혼동하게 하는 함정이다.

다시 나오면 이렇게 판단

법정 정의 문제에서는 목적과 핵심 동사를 먼저 대조한다. 게시판은 '일반에게 공개할 목적'과 '이용자가 게재'가 함께 있어야 하며, 로컬 저장을 중심으로 설명하면 게시판의 정의가 아니다.

암기 포인트

게시판은 로컬 저장이 아니라 일반 공개를 위한 정보 게재 수단이다.

NoteBase