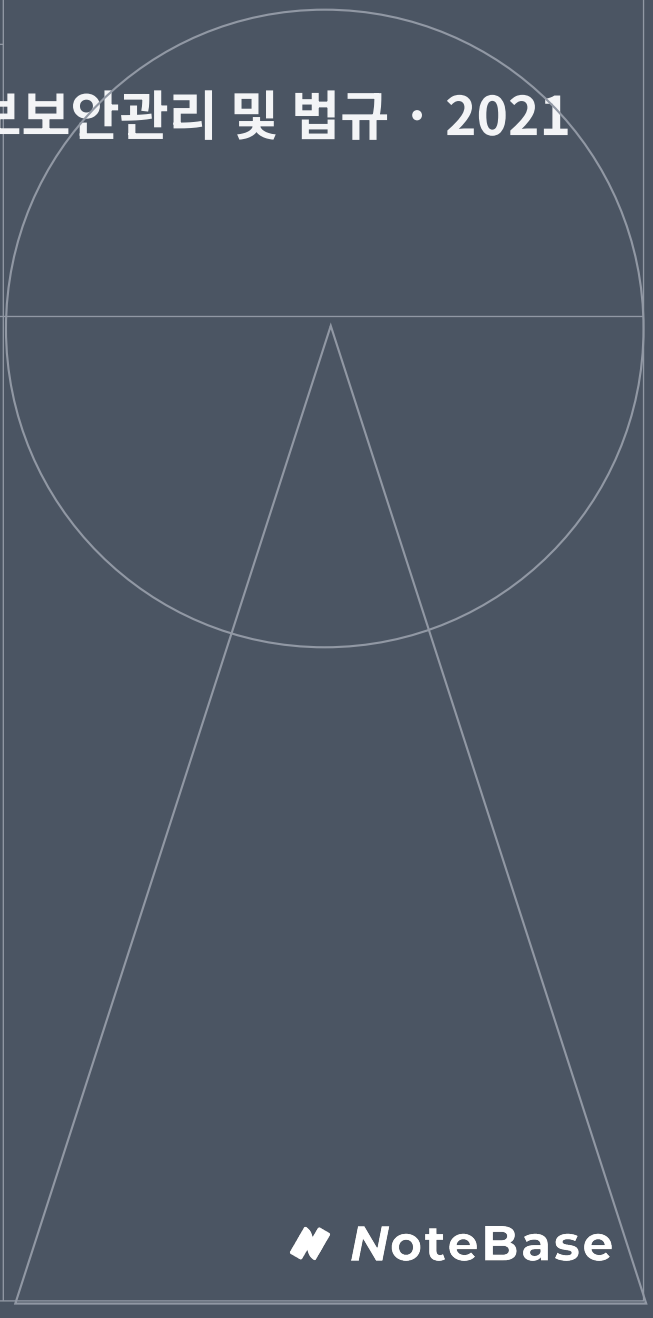
기출OX 해설집

공무원/경찰/경력채용 · 정보보안관리 및 법규 · 2021



NoteBase

기출OX 해설집

공무원/경찰/경력채용 · 정보보안관리 및 법규 · 2021

공무원/경찰/경력채용 · 정보보안관리 및 법규 · 2021

문 1. 정보보호 및 개인정보보호 관리체계(ISMS-P)에 대한 설명으로 가장 적절하지 않은 것은?

① ISMS-P 인증심사 종류에는 '최초심사', '사후심사', '갱신심사'가 있으며, 최초심사를 통해 인증을 취득하면 3년의 유효기간이 부여된다.

② 인증 의무대상자는 ISMS 인증을 받아야 하며, ISMS-P 인증을 받은 경우에도 인증의무를 이행한 것으로 본다.

③ 인증기관인 한국인터넷진흥원(KISA)은 금융 분야 인증위원회를 구성 및 운영하고, 인증심사 및 인증서 발급 업무를 수행한다.

④ 사후심사는 인증발급일 기준으로 매 1년 이전에 심사를 완료해야 하며, 인증유효기간 내 심사를 받지 않을 경우 인증이 취소된다.

정답 3번

간단한 해설

금융 분야의 인증위원회를 운영하고 인증심사·인증서 발급을 담당하는 기관은 **금융보안원(FSI)**이다.
한국인터넷진흥원(KISA)의 인증제도 운영 업무와 금융 분야 담당 기관을 혼동한 설명이다.

NoteBase

선지별 해설

① O: 최초심사는 처음 인증을 취득하기 위한 심사이며, 취득한 인증의 유효기간은 **3년**이다. 사후심사는 그 기간 중 관리체계가 인증기준에 맞게 유지되는지 확인하고, 갱신심사는 유효기간이 끝날 때 인증기간을 연장하기 위한 심사이다.

② O: ISMS는 정보보호 관리체계를, ISMS-P는 여기에 개인정보 처리단계별 보호 요구사항까지 포함한 관리체계를 인증한다. ISMS 의무대상자가 **ISMS-P 인증을 취득해도 인증의무를 이행**한 것으로 인정된다. 모든 의무대상자에게 ISMS-P 취득만을 요구한다는 뜻은 아니다.

③ X: 금융 분야 인증위원회 구성·운영, 인증심사 및 인증서 발급을 담당하는 기관은 **금융보안원(FSI)**이다. 한국인터넷진흥원(KISA)은 인증제도 운영·품질관리, 인증위원회 운영, 신규·특수 분야 심사와 인증서 발급 등의 업무를 수행하지만, 선지에 제시된 금융 분야 담당 기관과는 구별해야 한다.

④ O: 사후심사는 인증기준에 맞는 관리체계가 계속 유지되는지 점검하므로 인증 유효기간 중 매년 1회 이상 실시하며, 인증발급일을 기준으로 **매 1년이 되기 전에 완료**해야 한다. 당시 인증제도 안내서는 유효기간 내 사후심사를 받지 않으면 인증이 취소된다고 설명한다. 이는 사후관리 미이행에 관한 내용이며, 갱신심사를 받지 않아 유효기간 만료로 인증 효력을 잃는 경우와 구별된다.

NoteBase

문 2. 기술적 보호대책에 해당하는 내용으로 가장 적절한 것은?

① 정보시스템, 통신망, 정보를 보호하기 위한 가장 기본적 대책

② 자연재해 및 권한이 없는 외부인에 의한 파괴 등으로부터 정보시스템을 보호하기 위한 대책

③ 법률, 규정, 제도, 교육 등을 통한 보안계획 수립 및 운용 대책

④ 위험분석 및 보안감사를 통한 정보시스템의 신뢰성 확보 대책

정답 1번

간단한 해설

기술적 보호대책은 인증·암호화·접근통제처럼 **시스템에 구현한 보안 기능**으로 정보시스템·통신망·정보를 보호하는 것이므로 ①이 가장 적절하다.

개념 구분

정보보호 대책은 보호 목적만으로 구분하기보다 어떤 수단과 활동을 중심으로 구현하는지 살펴야 한다. 기술적 대책은 시스템의 하드웨어·소프트웨어 등에 구현한 보안 기능을, 물리적 대책은 시설·장비와 주변 환경의 보호를, 관리적 대책은 정책·조직·교육·점검을 중심으로 한다.

① 기술적 보호대책: 정보시스템·통신망·정보에 직접 적용하는 보안 기능을 가리키는 설명이다. 인증과 접근통제, 암호화, 방화벽, 악성코드 탐지 등이 대표적이며, 핵심은 **기술적 기능으로 접근·통신·데이터를 보호**한다는 점이다. 원문의 “가장 기본적”이라는 표현이 물리적·관리적 대책보다 언제나 우선하거나 그것들 없이 충분하다는 뜻은 아니다.

② 물리적 보호대책: 자연재해나 무단 침입자의 파괴로부터 시설과 장비를 보호하는 내용이다. 출입통제, 잠금장치, 소화설비 등으로 **물리적 접근과 환경 위험**을 관리한다.

③ 관리적 보호대책: 법률·규정·제도·교육을 바탕으로 보안계획을 수립하고 운영하는 내용이다. 보안정책 수립, 역할과 책임 배분, 교육 등 **조직의 관리 체계와 사람의 행동**을 통해 보안을 확보한다.

④ 관리적 보호대책: 위험분석으로 대응 우선순위를 정하고 보안감사로 통제의 적정성과 준수 여부를 점검하는 관리 활동이다. 기술 도구를 활용할 수 있어도 이 설명의 중심은 **위험을 평가하고 보안 운영을 감독**하는 데 있다.

따라서 기술적 보호대책에 가장 적절한 설명은 ①이다.

NoteBase

문 3. 다음 국제 공통 평가기준(CC: Common Criteria)에 해당하는 EAL(Evaluation Assurance Level) 등급으로 가장 적절한 것은?

· TOE(Target of Evaluation) 명세서에 기반한 독립적인 시험 요구
· 구조적 시험(Structurally Tested)
· 낮은 수준에서 중간 수준의 보안이 필요할 경우 실시

① EAL1
② EAL2
③ EAL3
④ EAL4

정답 2번

간단한 해설

구조적 시험은 EAL2를 가리킨다. 낮은 수준에서 중간 수준의 보안 보증을 요구한다는 조건도 이에 부합한다.

핵심 풀이

제시문의 **구조적 시험**은 EAL2의 등급 명칭이다. 낮은 수준에서 중간 수준의 보안 보증을 필요로 하는 경우에 적용한다는 조건도 EAL2의 목적에 해당한다.

TOE는 평가 대상이다. EAL2는 TOE의 명세와 기본 설계 정보를 토대로 독립적인 시험을 수행하며, 개발자의 시험 결과도 활용한다. 다만 **독립적인 시험 자체는 EAL2만의 특징이 아니다**. EAL1에서도 독립 시험을 하므로 나머지 단서와 함께 판단해야 한다.

경쟁 등급을 구분하면 EAL1은 기능적 시험, EAL3은 체계적인 시험과 점검, EAL4는 체계적인 설계·시험·검토에 해당한다. 따라서 구조적 시험을 가리키는 ② EAL2가 정답이다.

NoteBase

문 4. 정보보호 통제의 종류와 설명에 대하여 <보기 1>과 <보기 2>를 가장 적절하게 연결한 것은?

<보기 1>
(가) 행위에 의한 통제
(나) 보안 목표에 의한 통제
(다) 기능에 의한 통제
<보기 2>
㉠ 예방적 통제, 탐지적 통제, 수정적 통제
㉡ 무결성 통제, 기밀성 통제, 가용성 통제
㉢ 관리적 통제, 기술적 통제, 운영적 통제

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

정답 1번

간단한 해설

예방·탐지·수정은 사고에 대한 **통제의 작용**을, 무결성·기밀성·가용성은 **보안 목표**를 구분한다.
관리·기술·운영은 이 문항의 기능별 통제 영역에 해당한다.

NoteBase

대응 관계 해설

(가) 행위에 의한 통제 → ㉠: 사고에 대해 **어떤 작용을 하는지**에 따른 분류이다. 예방적 통제는 사고나 위반의 발생을 미리 막고, 탐지적 통제는 발생한 이상이나 위반을 찾아낸다. 수정적 통제는 발견된 문제를 바로잡고 피해를 줄이거나 정상 상태로 회복시키는 역할을 한다.

(나) 보안 목표에 의한 통제 → ㉡: **보호하려는 보안 속성**을 기준으로 구분한다. 무결성 통제는 정보의 부당한 변경·훼손을 막고, 기밀성 통제는 비인가자의 정보 열람·유출을 방지한다. 가용성 통제는 인가된 사용자가 필요한 때 정보와 서비스를 이용할 수 있게 한다.

(다) 기능에 의한 통제 → ㉢: 이 문항에서는 통제를 수행하는 **관리·기술·운영 영역**에 따른 분류이다. 관리적 통제는 보안정책·계획·위험관리 등 조직의 관리 활동에 중점을 둔다. 기술적 통제는 하드웨어·소프트웨어·펌웨어의 보안 기능으로 구현하며, 운영적 통제는 사람이 일상적인 절차와 업무를 수행하여 보안을 유지하는 데 중점을 둔다.

따라서 (가)는 ㉠, (나)는 ㉡, (다)는 ㉢으로 연결되므로 ①과 일치한다.

NoteBase

문 5. 다음에서 설명하는 재해복구 시스템의 유형으로 가장 적절한 것은?

· 재해복구센터에 주 센터와 동일 수준의 시스템을 대기상태(Stand-by)로 유지
· 동기적 또는 비동기적 방식의 실시간 복제를 통하여 최신 데이터 상태 유지
· 재해 발생 시 재해복구센터의 시스템을 액티브(Active)로 전환하여 복구
· RTO(Recovery Time Objective): 수시간 이내
· 데이터의 업데이트가 많은 경우에 적합

① 미러 사이트(Mirror Site)

② 핫 사이트(Hot Site)

③ 웜 사이트(Warm Site)

④ 콜드 사이트(Cold Site)

정답 2번

간단한 해설

정답은 ② **핫 사이트**이다. 주 센터와 동일 수준의 시스템과 복제 데이터를 준비하고, 재해 시 **대기상태에서 액티브로 전환**한다는 단서가 핵심이다.

NoteBase

핵심 풀이

핵심 단서는 **주 센터와 동일 수준의 시스템을 대기상태로 유지**한다는 점과, 재해가 발생하면 이를 **액티브로 전환**한다는 점이다. 필요한 시스템을 미리 갖추되 평소에는 복구용으로 대기시키고, 장애 시 업무를 넘겨받는 구성은 이 문항의 핫 사이트에 해당한다.

동기적 또는 비동기적 실시간 복제는 주 센터의 데이터 변경을 복구센터에도 계속 반영하여 복구 시 사용할 데이터를 준비하는 방식이다. 그래서 데이터 업데이트가 많은 업무의 복구에 유리하다. 다만 **비동기 복제에는 반영 지연이 생길 수 있으므로**, 최신 상태 유지라는 표현을 모든 순간의 완전한 일치나 데이터 손실이 전혀 없다는 보장으로 해석해서는 안 된다.

제시된 RTO 수시간 이내는 장애 후 업무를 복구하기까지의 **목표 시간**이다. 시스템과 데이터를 미리 준비하므로 장애 후 장비를 새로 확보하는 방식보다 신속한 전환을 목표로 할 수 있다. 이 시간은 문항이 제시한 구성의 목표이며, 모든 핫 사이트에 동일하게 적용되는 고정 기준은 아니다.

미러 사이트와도 실시간 복제라는 특징이 겹칠 수 있지만, 복제 유무만으로 답을 정하면 안 된다. 이 문항에서는 대기상태에서 액티브로 전환한다는 운영 방식과 수시간 이내라는 목표를 함께 읽어 ② **핫 사이트(Hot Site)**를 고른다. 일부 설비만 준비한 웜 사이트나 공간·전력 등 기반시설 중심의 콜드 사이트는 동일 수준의 시스템을 이미 대기시킨다는 조건과 맞지 않는다.

NoteBase

문 6. 다음에서 설명하는 내용으로 가장 적절한 것은?

· 사용자에게 자신의 패스워드를 관리할 수 있는 기능을 제공한다.
· 시스템 및 각종 자원에 대하여 접근제어를 할 수 있다.
· 사용자에 따라 권한을 차등적으로 부여할 수 있다.
· 역할 기반의 사용자 계정 솔루션이다.

① LBS(Location Based System)
② IAM(Identity and Access Management)
③ MPLS(Multi Protocol Label Switching)
④ DS(Differentiated Services)

정답 2번

간단한 해설

패스워드 관리와 역할별 권한 부여는 **사용자 신원과 접근 권한을 통합 관리**하는 IAM의 기능이므로 ②가 정답이다.

NoteBase

핵심 풀이

사용자 패스워드 관리: 사용자가 허용된 범위에서 자신의 비밀번호를 변경·재설정하는 셀프서비스 기능은 **사용자 계정과 인증정보 관리**에 해당한다. 이는 사용자에게 다른 사람의 비밀번호나 권한까지 임의로 바꿀 수 있게 한다는 뜻은 아니다.

시스템·자원 접근제어와 차등적 권한 부여: 사용자를 식별·인증하고 각 사용자에게 허용된 자원과 행위를 판단한다. 예를 들어 같은 문서라도 어떤 사용자는 읽기만, 다른 사용자는 수정까지 가능하도록 **사용자별 접근권한**을 관리한다.

역할 기반 계정 관리: 업무상 역할에 필요한 권한을 묶고 사용자에게 해당 역할을 배정한다. 이처럼 **역할을 통해 권한을 부여·회수**하면 사용자마다 개별 권한을 일일이 설정하는 부담을 줄일 수 있다. IAM은 이러한 역할 기반 접근제어를 지원할 수 있으며, 역할 기반 방식만을 의미하는 용어는 아니다.

① LBS: 위치정보를 활용해 길 안내나 주변 시설 검색 등을 제공하는 위치 기반 시스템·서비스 분야이다. 중심 대상은 위치정보이며, 사용자 계정과 권한을 통합 관리하는 체계의 명칭은 아니다.

③ MPLS: 패킷에 붙인 레이블을 이용해 네트워크에서 패킷을 전달하는 기술이다. **레이블 기반 전달**이 핵심이므로 패스워드와 사용자 계정 관리에 대한 설명과 구별된다.

④ DS: 트래픽을 분류하고 등급별로 서로 다른 전달 처리를 적용하는 차등화 서비스이다. **네트워크 트래픽의 서비스 품질**을 다루며, 사용자의 자원 접근 권한을 차등 부여하는 IAM과는 대상이 다르다.

계정·인증정보 관리와 자원 접근 권한 관리를 함께 다루는 체계는 IAM(Identity and Access Management)이므로 정답은 ②이다.

NoteBase

문 7. <보기 1>의 위험분석 방법론 중 <보기 2>의 설명과 가장 적절하게 연결한 것은?

<보기 1>
(가) 기준선 접근법(Baseline Approach)
(나) 비정형화된 접근법(Informal Approach)
(다) 상세 위험 분석 접근법(Detailed Risk Analysis Approach)
(라) 복합 접근법(Combined Approach)
<보기 2>
㉠
· 고위험 영역을 빠르게 식별하고 처리
· 영역의 구분이 잘못 수행되었을 때, 위험분석 비용이 낭비되거나 부적절한 대응책이 선택될 수 있음
㉡
· 비용 대비 효과가 우수하며 소규모 조직에 적합
· 작은 규모의 조직에는 적합하나, 새롭거나 경험이 적은 위험 영역을 간과할 가능성이 있음
㉢
· 자산가치, 위협, 취약점의 평가에 기초한 위험을 산정하므로 경영상 허용수준까지 위험을 줄이는 근거가 명확
· 조직의 자산 및 보안 요구사항을 구체적으로 분석하여 가장 적절한 대책 수립
㉣
· 비용 및 시간 절약
· 모든 시스템에 대해 표준화된 보호 대책의 세트를 체크리스트 형태로 제공

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

정답 4번

간단한 해설

표준 체크리스트는 기준선 접근법, **경험이 적은 위험의 누락**은 비정형화된 접근법의 특징이다.
자산·위협·취약성을 구체적으로 평가하는 상세 분석과, 고위험 영역을 나누어 분석 수준을 달리하는 복합 접근법도 구별된다.

NoteBase

대응 관계 해설

(가) 기준선 접근법 → ㉣: 미리 마련된 **표준 보호대책 체크리스트**를 기준으로 필요한 조치를 선택한다. 개별 시스템의 위험을 처음부터 모두 상세히 분석하는 부담을 줄여 시간과 비용을 절약할 수 있다. 공통 기준 중심이므로 조직별 차이를 충분히 반영하지 못할 수 있다.

(나) 비정형화된 접근법 → ㉡: 분석자의 **지식과 경험**을 활용하므로 비교적 적은 자원으로 수행할 수 있어 소규모 조직에 적합하다. 그러나 익숙하지 않은 위험을 빠뜨릴 수 있으므로, 비용 측면의 장점과 경험이 적은 영역을 간과한다는 한계가 함께 연결된다.

(다) 상세 위험 분석 접근법 → ㉢: 자산의 가치와 위협·취약성을 **체계적으로 평가**하여 위험을 산정한다. 이 분석 결과를 조직의 허용 가능한 위험 수준과 비교하므로 위험을 얼마나 줄여야 하는지와 어떤 대책이 필요한지 구체적인 근거를 얻는다. 다만 위험이 분석만으로 자동 감소하는 것은 아니며, 선정한 대책을 실제로 시행해야 한다.

(라) 복합 접근법 → ㉠: 먼저 중요한 고위험 영역을 가려내고 그 영역에는 상세 위험 분석을, 나머지에는 기준선 접근법을 적용하는 방식이다. **영역별 분석 수준을 달리**하여 자원을 집중할 수 있지만, 구분을 잘못하면 낮은 위험에 자원을 낭비하거나 높은 위험에 불충분한 대책을 적용할 수 있다.

따라서 (가) ㉣, (나) ㉡, (다) ㉢, (라) ㉠으로 연결되어 ④와 일치한다.

NoteBase

문 8. TCSEC(Trusted Computer System Evaluation Criteria)와 ITSEC(Information Technology Security Evaluation Criteria)의 설명으로 가장 적절하지 않은 것은?

① 기능성과 보증성 측면에서 ITSEC은 분리하여 평가하는 반면, TCSEC은 묶어서 평가한다.

② TCSEC은 ITSEC보다 나은 유연성을 제공하고, ITSEC은 기밀성에 대처하는 반면에 TCSEC은 무결성, 가용성, 기밀성에 모두 대처한다.

③ ITSEC은 유럽 국가들이 평가제품의 상호인정 및 평가기준이 상이함에 따른 불합리함을 보완하기 위하여 작성한 유럽형 보안기준이다.

④ TCSEC은 D~A1(D, C1, C2, B1, B2, B3, A1)까지 총 7개의 세부 보안등급이 있다.

정답 2번

간단한 해설

ITSEC은 기능성과 보증성을 분리해 평가하므로 TCSEC보다 유연하며, 기밀성·무결성·가용성을 다룬다. TCSEC은 **기밀성 중심**이므로 두 기준의 유연성과 보호 범위를 뒤바꾼 설명이 부적절하다.

선지별 해설

① O: 기능성은 어떤 보안 기능을 제공하는지, 보증성은 그 기능이 올바르고 효과적으로 구현되었다고 얼마나 신뢰할 수 있는지를 뜻한다. ITSEC은 **기능성과 보증성을 분리**하여 평가하지만, TCSEC은 정해진 보안등급마다 기능 요구사항과 보증 요구사항을 함께 묶는다.

② X: 유연성과 보호 목표의 설명이 뒤바뀌었다. 기능과 보증을 분리해 요구사항에 맞게 평가할 수 있는 **ITSEC이 더 유연**하며, 기밀성뿐 아니라 무결성·가용성도 다룬다. TCSEC은 군사 기밀의 비인가 공개를 방지하는 **기밀성 중심**의 기준이다. 이는 TCSEC에 무결성과 관련된 요구사항이 전혀 없다는 뜻은 아니다.

③ O: ITSEC은 독일·프랑스·영국·네덜란드 등이 마련한 유럽의 공통 보안평가기준이다. 국가별 기준의 차이를 조정하여 평가 결과를 상호 인정할 수 있는 기반을 마련하려는 목적이 있으므로, 서로 다른 기준으로 인한 중복 평가와 불일치를 줄이는 방향이다.

④ O: TCSEC의 분류는 D, C, B, A의 네 큰 범주이며, 세부 등급은 **D, C1, C2, B1, B2, B3, A1의 7개**이다. D는 평가를 받았으나 상위 등급의 요건을 충족하지 못한 경우에 해당하고, C·B·A는 각각 임의적 보호·강제적 보호·검증된 보호를 중심으로 구분된다.

NoteBase

문 9. 클라우드서비스 보안인증제에 대한 설명으로 가장 적절하지 않은 것은?

① IaaS, SaaS 표준등급, SaaS 간편등급, DaaS의 인증종류를 가진다.

② 서버 가상화 기술은 SaaS의 기술 중 하나이다.

③ 중요한 데이터를 다루는 SaaS 서비스는 표준등급을 받아야 한다.

④ DaaS 서비스는 필수 보안 요건을 만족하여야 하며, 보안장비 등의 영역에서 구성되어야 한다.

정답 2번

간단한 해설

서버 가상화는 **IaaS의 인프라 제공**과 연결되는 기술이다. SaaS는 응용 소프트웨어를 서비스로 제공하므로 서비스 계층을 구분해야 한다.

선지별 해설

2021년 출제 당시의 인증 체계를 기준으로 판단한다.

① O: 출제 당시 인증은 IaaS, SaaS, DaaS로 구분되고, **SaaS는 표준등급과 간편등급**으로 나뉘었다. 따라서 선지의 네 종류는 당시 인증 체계에 부합한다.

② X: 서버 가상화는 물리 서버의 자원을 나누어 가상 서버를 제공하는 **인프라 계층의 기술**로서 IaaS와 연결된다. SaaS는 이용자에게 응용 소프트웨어를 서비스로 제공하는 방식이다. SaaS의 구현 기반에서도 서버 가상화를 활용할 수 있다. 다만 이 문항처럼 서비스 모델을 구분하는 문맥에서는 서버 가상화를 SaaS의 기술로 분류한 것이 인프라 계층과 응용프로그램 제공 모델을 혼동한 설명이다.

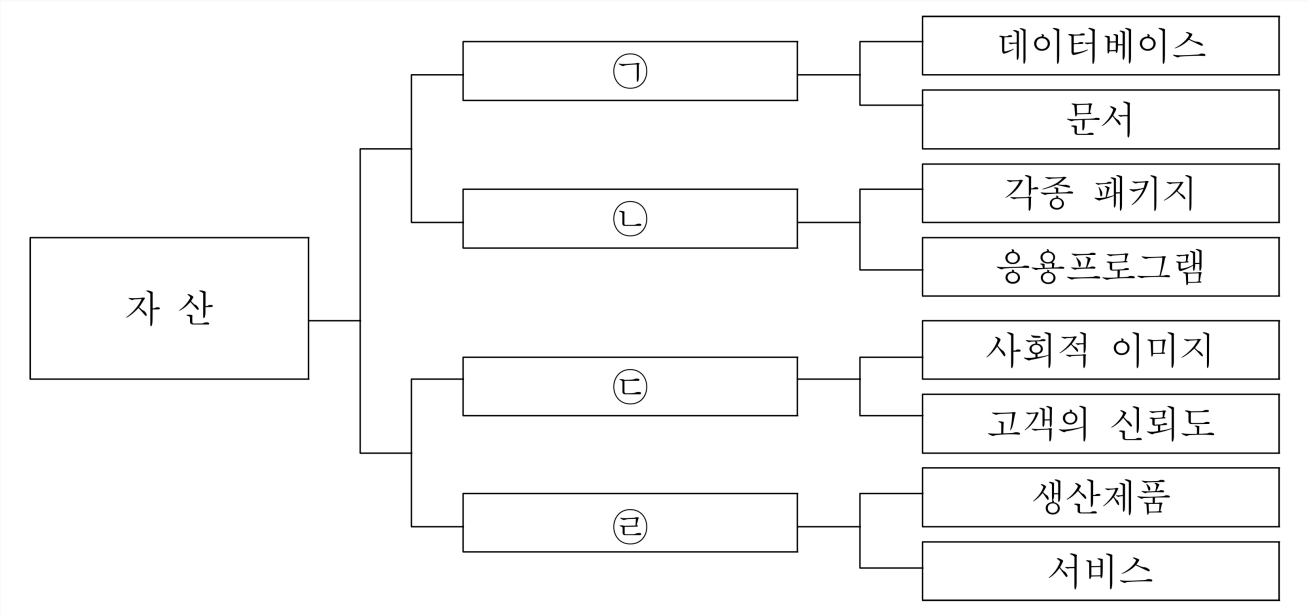
③ O: 전자결재, 인사·회계관리 등 **중요 데이터를 다루는 SaaS**는 표준등급 인증 대상이었다. 중요 데이터 처리에 필요한 보안 수준을 확보하도록 표준등급을 적용한 것이다.

④ O: DaaS는 가상 데스크톱 환경을 원격으로 제공한다. 네트워크·보안장비·하이퍼바이저 등 인프라 영역에 구성하며, 가상자원 초기화와 비인가 접속 차단 등 **필수 보안요건**을 충족해야 한다.

따라서 가장 적절하지 않은 설명은 ②이다.

NoteBase

문 10. 자산의 종류 중 ㉠~㉣에 들어갈 내용으로 가장 적절한 것은?



① ㉠: 소프트웨어 자산, ㉡: 정보 자산, ㉢: 상품 자산, ㉣: 무형 자산

② ㉠: 정보 자산, ㉡: 소프트웨어 자산, ㉢: 상품 자산, ㉣: 무형 자산

③ ㉠: 소프트웨어 자산, ㉡: 정보 자산, ㉢: 무형 자산, ㉣: 상품 자산

④ ㉠: 정보 자산, ㉡: 소프트웨어 자산, ㉢: 무형 자산, ㉣: 상품 자산

정답 4번

간단한 해설

정답은 ④이다. **데이터베이스·문서는 정보 자산**, 패키지·응용프로그램은 소프트웨어 자산, 사회적 이미지·고객 신뢰도는 무형 자산, 생산제품·서비스는 상품 자산에 해당한다.

NoteBase

도식 해설

㉠은 **정보 자산**이다. 연결된 데이터베이스와 문서는 조직이 저장·활용하는 정보의 집합 또는 정보가 담긴 자료이다. 여기서 데이터베이스는 저장된 정보에 초점을 맞춘 것이며, 이를 관리하는 프로그램인 데이터베이스 관리 시스템(DBMS)과 구별한다.

㉡은 **소프트웨어 자산**이다. 각종 패키지와 응용프로그램은 데이터를 처리하거나 업무 기능을 실행하는 프로그램이다. ㉠의 정보 내용과 달리 정보를 처리하는 도구라는 점이 구분 기준이다.

㉢은 **무형 자산**이다. 사회적 이미지와 고객의 신뢰도는 물리적 실체가 없어도 조직의 평판과 지속적인 거래에 영향을 주는 가치이다. 이 도식에서는 이러한 평판·신뢰의 가치를 별도의 자산 범주로 묶고 있다.

㉣은 **상품 자산**이다. 생산제품과 서비스는 조직이 고객에게 제공하는 산출물이라는 공통점이 있다. 서비스가 물리적 형태를 갖지 않더라도, 이 도식은 제공하는 상품이라는 역할에 따라 ㉣에 분류한다.

따라서 ㉠ 정보 자산, ㉡ 소프트웨어 자산, ㉢ 무형 자산, ㉣ 상품 자산의 순서가 맞으므로 정답은 ④이다. 각 칸의 분류명만 외우기보다 오른쪽에 연결된 사례의 공통 성격을 기준으로 대응시키면 된다.

NoteBase

문 11. 「개인정보 보호법」상 정보주체가 자신의 개인정보 처리와 관련하여 가질 수 있는 권리로 가장 적절하지 않은 것은?

① 개인정보의 처리에 관한 정보를 제공받을 권리
② 개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리
③ 개인정보의 처리 여부를 확인하고 이를 저장한 시스템의 정보를 요구할 권리
④ 개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리

정답 3번

①

정보주체는 자신의 **개인정보 처리에 관한 정보를 제공받을 권리**를 가진다.

개인정보 보호법 제4조(정보주체의 권리) 정보주체는 자신의 개인정보 처리와 관련하여 다음 각 호의 권리를 가진다. <개정 2023.3.14>
1. 개인정보의 처리에 관한 정보를 제공받을 권리

②

정보주체는 자신의 개인정보 처리에 관한 **동의 여부와 동의 범위 등을 스스로 선택하고 결정할 권리**를 가진다.

개인정보 보호법 제4조(정보주체의 권리) 정보주체는 자신의 개인정보 처리와 관련하여 다음 각 호의 권리를 가진다. <개정 2023.3.14>
2. 개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리

③

정보주체는 개인정보의 처리 여부를 확인하고 **개인정보 자체의 열람(사본 발급 포함) 및 전송을 요구할 권리**를 가진다. 선지는 요구 대상을 개인정보를 저장한 시스템의 정보로 바꾸었다.

개인정보 보호법 제4조(정보주체의 권리) 정보주체는 자신의 개인정보 처리와 관련하여 다음 각 호의 권리를 가진다. <개정 2023.3.14>
3. 개인정보의 처리 여부를 확인하고 개인정보에 대한 열람(사본의 발급을 포함한다. 이하 같다) 및 전송을 요구할 권리

NoteBase

④

정보주체는 개인정보 처리로 발생한 피해를 **신속하고 공정한 절차에 따라 구제받을 권리**를 가진다.

개인정보 보호법 제4조(정보주체의 권리) 정보주체는 자신의 개인정보 처리와 관련하여 다음 각 호의 권리를 가진다. <개정 2023.3.14>
5. 개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리

NoteBase

문 12. 「개인정보 보호법」상 개인정보 분쟁조정위원회의 설치 및 구성에 대한 설명으로 가장 적절하지 않은 것은?

① 분쟁조정위원회는 위원장 1명을 포함한 20명 이내의 위원으로 구성하며, 위원은 당연직위원과 위촉위원으로 구성한다.

② 위원장은 위원 중에서 공무원이 아닌 사람으로 보호위원회 위원장이 위촉한다.

③ 분쟁조정위원회 또는 조정부는 재적위원 과반수의 출석으로 개의하며 출석위원 3분의 2 이상 찬성으로 의결한다.

④ 위원장과 위촉위원의 임기는 2년으로 하되, 1차에 한하여 연임할 수 있다.

정답 1, 3번

①

분쟁조정위원회는 위원장 1명을 포함한 **30명 이내**의 위원으로 구성한다. 위원은 당연직위원과 위촉위원으로 구성한다.

개인정보 보호법 제40조(설치 및 구성)
② 분쟁조정위원회는 위원장 1명을 포함한 30명 이내의 위원으로 구성하며, 위원은 당연직위원과 위촉위원으로 구성한다. <개정 2015.7.24, 2023.3.14>

②

위원장은 위원 중 **공무원이 아닌 사람**으로 **개인정보 보호위원회 위원장이 위촉**한다.

개인정보 보호법 제40조(설치 및 구성)
④ 위원장은 위원 중에서 공무원이 아닌 사람으로 보호위원회 위원장이 위촉한다. <개정 2013.3.23, 2014.11.19, 2015.7.24>

③

분쟁조정위원회 또는 조정부는 **재적위원 과반수의 출석**으로 개의하고, **출석위원 과반수의 찬성**으로 의결한다. 의결에 3분의 2 이상의 찬성을 요구하지 않는다.

개인정보 보호법 제40조(설치 및 구성)
⑦ 분쟁조정위원회 또는 조정부는 재적위원 과반수의 출석으로 개의하며 출석위원 과반수의 찬성으로 의결한다.

NoteBase

④

위원장과 위촉위원의 임기는 **2년**이며, **1차에 한하여 연임**할 수 있다.

개인정보 보호법 제40조(설치 및 구성)
⑤ 위원장과 위촉위원의 임기는 2년으로 하되, 1차에 한하여 연임할 수 있다. <개정 2015.7.24>

NoteBase

문 13. 다음은 「전자정부법」 제2조(정의)의 일부이다. <보기 1>의 뜻과 <보기 2>의 용어를 연결한 것으로 가장 적절한 것은?

<보기 1>
· (가)란 행정기관등이 직무상 작성하거나 취득하여 관리하고 있는 자료로서 전자적 방식으로 처리되어 부호, 문자, 음성, 음향, 영상 등으로 표현된 것을 말한다.
· (나)란 컴퓨터 등 정보처리능력을 지닌 장치에 의하여 전자적인 형태로 작성되어 송수신되거나 저장되는 표준화된 정보를 말한다.
· (다)란 종이문서와 그 밖에 전자적 형태로 작성되지 아니한 문서를 정보시스템이 처리할 수 있는 형태로 변환한 문서를 말한다.

<보기 2>
㉠ 행정정보 ㉡ 전자문서 ㉢ 전자화문서

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

정답 1번

가

행정정보는 **행정기관등이 직무상 작성·취득하여 관리하는 자료** 중 전자적으로 처리되어 문자·음성·영상 등으로 표현된 것이다.

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>
6. "행정정보"란 행정기관등이 직무상 작성하거나 취득하여 관리하고 있는 자료로서 전자적 방식으로 처리되어 부호, 문자, 음성, 음향, 영상 등으로 표현된 것을 말한다.

NoteBase

나

전자문서는 정보처리장치로 **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.

다

전자화문서는 종이문서 등 **비전자적 문서를 정보시스템이 처리할 수 있는 형태로 변환한 문서**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>
8. "전자화문서"란 종이문서와 그 밖에 전자적 형태로 작성되지 아니한 문서를 정보시스템이 처리할 수 있는 형태로 변환한 문서를 말한다.

NoteBase

문 14. 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」상 클라우드컴퓨팅서비스의 신뢰성 향상 및 이용자 보호에 대한 설명으로 가장 적절하지 않은 것은?

① 클라우드컴퓨팅서비스 제공자는 이용자 정보가 유출된 때 지체 없이 그 사실을 해당 이용자에게 알려야 한다.

② 이용자는 클라우드컴퓨팅서비스 제공자에게 이용자 정보가 저장되는 국가의 명칭을 알려 줄 것을 요구할 수 있다.

③ 클라우드컴퓨팅서비스 제공자는 클라우드컴퓨팅서비스의 품질·성능 및 정보보호 수준을 향상시키기 위하여 노력하여야 한다.

④ 클라우드컴퓨팅서비스 제공자는 이용자와의 계약이 종료되었을 때에는 이용자에게 이용자 정보를 반환하여야 하고 클라우드컴퓨팅서비스 제공자가 보유하고 있는 이용자 정보를 따로 저장하여야 한다.

정답 4번

①

이용자 정보가 유출되면 클라우드컴퓨팅서비스 제공자는 **지체 없이 해당 이용자에게 유출 사실을 알려야 한다**.

클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제25조(침해사고 등의 통지 등)
① 클라우드컴퓨팅서비스 제공자는 다음 각 호의 어느 하나에 해당하는 경우에는 지체 없이 그 사실을 해당 이용자에게 알려야 한다.
2. 이용자 정보가 유출된 때

②

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

③

클라우드컴퓨팅서비스 제공자는 서비스의 **품질·성능 및 정보보호 수준을 향상시키기 위하여 노력할 의무**를 부담한다.

클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제23조(신뢰성 향상)
① 클라우드컴퓨팅서비스 제공자는 클라우드컴퓨팅서비스의 품질 · 성능 및 정보보호 수준을 향상시키기 위하여 노력하여야 한다.

NoteBase

④

계약이 종료되면 이용자 정보를 반환하고 제공자가 보유한 정보는 **따로 저장하는 것이 아니라 파기하여야 한다**. 사실상 반환이 불가능한 경우에도 파기하며, 당사자 간 계약으로 특별히 다르게 정한 경우에는 그에 따른다.

클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제27조(이용자 정보의 보호)
③ 클라우드컴퓨팅서비스 제공자는 이용자와의 계약이 종료되었을 때에는 이용자에게 이용자 정보를 반환하여야 하고 클라우드컴퓨팅서비스 제공자가 보유하고 있는 이용자 정보를 파기하여야 한다. 다만, 이용자가 반환받지 아니하거나 반환을 원하지 아니하는 등의 이유로 사실상 반환이 불가능한 경우에는 이용자 정보를 파기하여야 한다.
⑤ 제3항 및 제4항에도 불구하고 클라우드컴퓨팅서비스 제공자와 이용자 간의 계약으로 특별히 다르게 정한 경우에는 그에 따른다.

NoteBase

문 15. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제46조의2(집적정보통신시설 사업자의 긴급대응)에서 집적정보통신시설 사업자가 이용약관으로 정하는 바에 따라 해당 서비스의 전부 또는 일부의 제공을 중단할 수 있는 경우로 가장 적절하지 않은 것은?

① 시설이용자의 정보시스템에서 발생한 이상현상으로 다른 시설 이용자의 정보통신망에 심각한 장애를 발생시킬 우려가 있다고 판단되는 경우

② 중대한 침해사고가 발생하여 과학기술정보통신부장관이 요청하는 경우

③ 중대한 침해사고가 발생하여 한국인터넷진흥원이 요청하는 경우

④ 침해사고가 발생하지는 않았지만, 집적된 정보통신시설에 심각한 장애가 발생할 우려가 있다고 판단되어 국무총리가 요청하는 경우

정답 4번

①

시설이용자의 정보시스템 이상으로 **다른 시설이용자의 정보통신망에 심각한 장애가 발생할 우려**가 있다고 판단되면, 이용약관에 따라 서비스의 전부 또는 일부를 중단할 수 있다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제46조의2(집적정보통신시설 사업자의 긴급대응)
① 집적정보통신시설 사업자는 다음 각 호의 어느 하나에 해당하는 경우에는 이용약관으로 정하는 바에 따라 해당 서비스의 전부 또는 일부의 제공을 중단할 수 있다. <개정 2009.4.22, 2013.3.23, 2017.7.26>
1. 집적정보통신시설을 이용하는 자(이하 "시설이용자"라 한다)의 정보시스템에서 발생한 이상현상으로 다른 시설이용자의 정보통신망 또는 집적된 정보통신시설의 정보통신망에 심각한 장애를 발생시킬 우려가 있다고 판단되는 경우

②

중대한 침해사고가 발생하여 과학기술정보통신부장관이 요청하면, 집적정보통신시설 사업자는 이용약관에 따라 서비스의 전부 또는 일부를 중단할 수 있다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제46조의2(집적정보통신시설 사업자의 긴급대응)
① 집적정보통신시설 사업자는 다음 각 호의 어느 하나에 해당하는 경우에는 이용약관으로 정하는 바에 따라 해당 서비스의 전부 또는 일부의 제공을 중단할 수 있다. <개정 2009.4.22, 2013.3.23, 2017.7.26>
3. 중대한 침해사고가 발생하여 과학기술정보통신부장관이나 한국인터넷진흥원이 요청하는 경우

NoteBase

③

중대한 침해사고가 발생하여 한국인터넷진흥원이 요청하면, 집적정보통신시설 사업자는 이용약관에 따라 서비스의 전부 또는 일부를 중단할 수 있다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제46조의2(집적정보통신시설 사업자의 긴급대응)
① 집적정보통신시설 사업자는 다음 각 호의 어느 하나에 해당하는 경우에는 이용약관으로 정하는 바에 따라 해당 서비스의 전부 또는 일부의 제공을 중단할 수 있다. <개정 2009.4.22, 2013.3.23, 2017.7.26>
3. 중대한 침해사고가 발생하여 과학기술정보통신부장관이나 한국인터넷진흥원이 요청하는 경우

④

외부 침해사고에 따른 심각한 장애 우려가 있거나, **중대한 침해사고가 발생하여 과학기술정보통신부장관이나 한국인터넷진흥원이 요청**한 경우는 서비스 중단 사유이다. 침해사고 없이 **국무총리가 요청한 경우는 법정 중단 사유가 아니다**.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제46조의2(집적정보통신시설 사업자의 긴급대응)
① 집적정보통신시설 사업자는 다음 각 호의 어느 하나에 해당하는 경우에는 이용약관으로 정하는 바에 따라 해당 서비스의 전부 또는 일부의 제공을 중단할 수 있다. <개정 2009.4.22, 2013.3.23, 2017.7.26>
2. 외부에서 발생한 침해사고로 집적된 정보통신시설에 심각한 장애가 발생할 우려가 있다고 판단되는 경우
3. 중대한 침해사고가 발생하여 과학기술정보통신부장관이나 한국인터넷진흥원이 요청하는 경우

NoteBase

문 16. 「전자금융거래법」 제2조(정의)에 대한 내용으로 가장 적절한 것은?

① 전자지급거래는 금융회사 또는 전자금융업자가 전자적 장치를 통하여 금융상품 및 서비스를 제공하고, 이용자가 금융회사 또는 전자금융업자의 종사자와 직접 대면하거나 의사소통을 하지 아니하고 자동화된 방식으로 이를 이용하는 거래를 말한다.

② 전자금융거래는 자금을 주는 자가 금융회사 또는 전자금융업자로 하여금 전자지급수단을 이용하여 자금을 받는 자에게 자금을 이동하게 하는 거래를 말한다.

③ 전자적 장치는 전자자금이체, 직불전자지급수단, 선불전자지급수단, 전자화폐, 신용카드, 전자채권 그 밖에 전자적 방법에 따른 지급수단을 말한다.

④ 전자지급결제대행은 전자적 방법으로 재화의 구입 또는 용역의 이용에 있어서 지급결제정보를 송신하거나 수신하는 것 또는 그 대가의 정산을 대행하거나 매개하는 것을 말한다.

정답 4번

①

금융회사 또는 전자금융업자가 제공하는 금융상품·서비스를 종사자와 직접 대면하거나 의사소통하지 않고 자동화된 방식으로 이용하는 거래는 **전자금융거래**이다.

전자금융거래법 제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다. <개정 2007.4.27, 2008.2.29, 2012.3.21, 2012.6.1, 2013.5.22, 2020.6.9, 2023.9.14, 2025.12.16>
1. "전자금융거래"라 함은 금융회사 또는 전자금융업자가 전자적 장치를 통하여 금융상품 및 서비스를 제공(이하 "전자금융업무"라 한다)하고, 이용자가 금융회사 또는 전자금융업자의 종사자와 직접 대면하거나 의사소통을 하지 아니하고 자동화된 방식으로 이를 이용하는 거래를 말한다.

②

지급인이 금융회사 또는 전자금융업자로 하여금 전자지급수단으로 수취인에게 자금을 이동하게 하는 전자금융거래는 **전자지급거래**이다.

전자금융거래법 제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다. <개정 2007.4.27, 2008.2.29, 2012.3.21, 2012.6.1, 2013.5.22, 2020.6.9, 2023.9.14, 2025.12.16>
2. "전자지급거래"라 함은 자금을 주는 자(이하 "지급인"이라 한다)가 금융회사 또는 전자금융업자로 하여금 전자지급수단을 이용하여 자금을 받는 자(이하 "수취인"이라 한다)에게 자금을 이동하게 하는 전자금융거래를 말한다.

NoteBase

③

열거된 것은 **전자지급수단**이다. 전자적 장치는 현금자동지급기·컴퓨터·전화기 등 **전자금융거래정보를 전송하거나 처리하는 장치**를 말한다.

전자금융거래법 제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다. <개정 2007.4.27, 2008.2.29, 2012.3.21, 2012.6.1, 2013.5.22, 2020.6.9, 2023.9.14, 2025.12.16>
8. "전자적 장치"라 함은 전자금융거래정보를 전자적 방법으로 전송하거나 처리하는데 이용되는 장치로서 현금자동지급기, 자동입출금기, 지급용단말기, 컴퓨터, 전화기 그 밖에 전자적 방법으로 정보를 전송하거나 처리하는 장치를 말한다.
11. "전자지급수단"이라 함은 전자자금이체, 직불전자지급수단, 선불전자지급수단, 전자화폐, 신용카드, 전자채권 그 밖에 전자적 방법에 따른 지급수단을 말한다.

④

전자지급결제대행에는 재화·용역 거래에서 **지급결제정보의 송수신 또는 대가 정산의 대행·매개**가 포함된다.

전자금융거래법 제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다. <개정 2007. 4. 27., 2008. 2. 29., 2012. 3. 21., 2012. 6. 1., 2013. 5. 22., 2020. 6. 9., 2023. 9. 14.>
19. “전자지급결제대행”이라 함은 전자적 방법으로 재화의 구입 또는 용역의 이용에 있어서 지급결제정보를 송신하거나 수신하는 것 또는 그 대가의 정산을 대행하거나 매개하는 것을 말한다.

NoteBase

문 17. 「정보통신기반 보호법」상 정보통신기반보호위원회와 관련된 내용으로 가장 적절하지 않은 것은?

① 위원회의 위원은 위원장 1인을 포함한 25인 이내의 위원으로 구성한다.

② 주요정보통신기반시설의 보호에 관한 사항을 심의하기 위하여 과학기술정보통신부장관 소속하에 정보통신기반보호위원회를 둔다.

③ 위원회의 위원장은 국무조정실장이 된다.

④ 위원회의 효율적인 운영을 위하여 위원회에 공공분야와 민간분야를 각각 담당하는 실무위원회를 둔다.

정답 2번

①

정보통신기반보호위원회는 **위원장 1인을 포함한 25인 이내**의 위원으로 구성한다.

정보통신기반 보호법 제3조(정보통신기반보호위원회)
②위원회의 위원은 위원장 1인을 포함한 25인 이내의 위원으로 구성한다.

②

주요정보통신기반시설의 보호에 관한 사항을 심의하는 정보통신기반보호위원회는 **국무총리 소속**으로 둔다.

정보통신기반 보호법 제3조(정보통신기반보호위원회)
①제8조에 따라 지정된 주요정보통신기반시설(이하 "주요정보통신기반시설"이라 한다)의 보호에 관한 사항을 심의하기 위하여 국무총리 소속하에 정보통신기반보호위원회(이하 "위원회"라 한다)를 둔다. <개정 2020.6.9>

③

정보통신기반보호위원회의 위원장은 **국무조정실장**이다.

정보통신기반 보호법 제3조(정보통신기반보호위원회)
③위원회의 위원장은 국무조정실장이 되고, 위원회의 위원은 대통령령으로 정하는 중앙행정기관의 차관급 공무원과 위원장이 위촉하는 사람으로 한다. <개정 2007.12.21, 2008.2.29, 2013.3.23, 2020.6.9>

④

위원회의 효율적인 운영을 위하여 **공공분야와 민간분야를 각각 담당하는 실무위원회**를 둔다.

정보통신기반 보호법 제3조(정보통신기반보호위원회)
④위원회의 효율적인 운영을 위하여 위원회에 공공분야와 민간분야를 각각 담당하는 실무위원회를 둔다. <개정 2007.12.21>

NoteBase

문 18. 「위치정보의 보호 및 이용 등에 관한 법률」 제11조(위치기반서비스사업자의 휴업·폐업 등)의 일부분이다. ㉠~㉢에 들어갈 내용으로 가장 적절한 것은?

· 위치기반서비스사업자가 사업의 전부 또는 일부를 휴업하고자 하는 때에는 휴업기간을 정하여 휴업하고자 하는 날의 (㉠)일 전까지 이를 개인위치정보주체에게 통보하고 방송통신위원회에 신고하여야 한다. 이 경우 휴업기간은 (㉡)을 초과할 수 없다.
· 위치기반서비스사업자가 사업의 전부 또는 일부를 폐업하고자 하는 때에는 폐업하고자 하는 날의 (㉢)일 전까지 이를 개인위치정보주체에게 통보하고 방송통신위원회에 신고하여야 한다.

① ㉠: 30, ㉡: 1년, ㉢: 30
② ㉠: 30, ㉡: 2년, ㉢: 60
③ ㉠: 60, ㉡: 1년, ㉢: 30
④ ㉠: 60, ㉡: 2년, ㉢: 60

정답 1번

간단한 해설

제시된 규정은 휴업과 폐업 모두 **30일 전까지 통보·신고**하도록 하고, **휴업기간은 1년을 초과할 수 없도록** 정한다. 통보·신고의 사전 기한과 휴업할 수 있는 최대 기간을 구별해야 한다.

빈칸별 해설

2021년 문항에 제시된 위치기반서비스사업자의 휴업·폐업 규정을 기준으로 한다.

㉠ 30: 제시된 위치정보법 제11조제1항에서 위치기반서비스사업자가 사업의 전부 또는 일부를 휴업하려면, 휴업기간을 정하고 **휴업하려는 날의 30일 전까지** 개인위치정보주체에게 통보하고 방송통신위원회에 신고해야 한다. 휴업한 뒤 30일 이내에 신고한다는 뜻이 아니며, 빈칸 뒤에 '일'이 있으므로 30이 들어간다.

㉡ 1년: 같은 항이 정한 **휴업기간의 상한은 1년**이다. 휴업은 사업을 일시적으로 중단하는 것이므로 그 기간을 정해야 하며, 2년까지 휴업할 수 있다는 내용으로 채울 수 없다. 이는 사전 통보·신고 기한인 30일과 별개의 기간이다.

㉢ 30: 제11조제2항은 사업의 전부 또는 일부를 폐업하려는 때에도 **폐업하려는 날의 30일 전까지** 개인위치정보주체에게 통보하고 방송통신위원회에 신고하도록 한다. 폐업은 사업을 종료하는 것이지만 사전 통보·신고 기한은 휴업과 동일하므로 60이 아닌 30이 들어간다.

따라서 ㉠ 30, ㉡ 1년, ㉢ 30의 조합인 ①과 일치한다.

NoteBase

문 19. 「전자정부법」 제43조(정보주체의 열람청구권)에서 정보주체가 공동이용센터를 통하여 공동이용한 행정정보 중 본인에 관한 행정정보에 대하여 행정안전부장관 또는 해당이용기관의 장에게 신청할 수 있는 열람 사항으로 가장 적절하지 않은 것은?

① 공동이용센터 행정정보 책임자 정보
② 공동이용의 목적
③ 공동이용한 행정정보의 종류
④ 이용기관

정답 1번

①

열람 대상은 이용기관, 공동이용의 목적, 공동이용한 행정정보의 종류와 시기, 공동이용의 법적 근거이다.
공동이용센터 행정정보 책임자 정보는 열람 사항에 포함되지 않는다.

전자정부법 제43조(정보주체의 열람청구권)
① 정보주체는 공동이용센터를 통하여 공동이용한 행정정보 중 본인에 관한 행정정보에 대하여 다음 각 호의 사항에 대한 열람을 행정안전부장관 또는 해당 이용기관의 장에게 신청할 수 있다. <개정 2013.3.23, 2014.11.19, 2017.7.26>
1. 이용기관
2. 공동이용의 목적
3. 공동이용한 행정정보의 종류
4. 공동이용한 시기
5. 해당 행정정보를 공동이용할 수 있는 법적 근거

②

정보주체는 공동이용센터를 통하여 공동이용한 본인의 행정정보에 관하여 **공동이용의 목적**에 대한 열람을 신청할 수 있다.

전자정부법 제43조(정보주체의 열람청구권)
① 정보주체는 공동이용센터를 통하여 공동이용한 행정정보 중 본인에 관한 행정정보에 대하여 다음 각 호의 사항에 대한 열람을 행정안전부장관 또는 해당 이용기관의 장에게 신청할 수 있다. <개정 2013.3.23, 2014.11.19, 2017.7.26>
2. 공동이용의 목적

NoteBase

③

정보주체는 공동이용센터를 통하여 공동이용한 본인의 행정정보에 관하여 **공동이용한 행정정보의 종류**에 대한 열람을 신청할 수 있다.

전자정부법 제43조(정보주체의 열람청구권)
① 정보주체는 공동이용센터를 통하여 공동이용한 행정정보 중 본인에 관한 행정정보에 대하여 다음 각 호의 사항에 대한 열람을 행정안전부장관 또는 해당 이용기관의 장에게 신청할 수 있다. <개정 2013.3.23, 2014.11.19, 2017.7.26>
3. 공동이용한 행정정보의 종류

④

정보주체는 공동이용센터를 통하여 공동이용한 본인의 행정정보에 관하여 **그 정보를 공동이용한 이용기관**에 대한 열람을 신청할 수 있다.

전자정부법 제43조(정보주체의 열람청구권)
① 정보주체는 공동이용센터를 통하여 공동이용한 행정정보 중 본인에 관한 행정정보에 대하여 다음 각 호의 사항에 대한 열람을 행정안전부장관 또는 해당 이용기관의 장에게 신청할 수 있다. <개정 2013.3.23, 2014.11.19, 2017.7.26>
1. 이용기관

NoteBase

문 20. 경찰관 A는 불특정 다수가 이용하는 장소에 영상정보처리기기가 설치되었다는 신고를 받고 현장에 도착하여 신고인에게 「개인정보 보호법」 제25조(영상정보처리기기의 설치·운영 제한)에 제한되지 않는 장소임을 설명하였다. 경찰관 A가 출동했었던 현장으로 가장 적절한 곳은?

① 목욕실

② 발한실

③ 정신보건 시설

④ 탈의실

정답 3번

③

정신보건 시설 중 **수용시설을 갖춘 정신의료기관, 정신요양시설 및 정신재활시설**은 사생활 침해 우려 장소 내부의 **고정형 영상정보처리기기 설치·운영 금지의 예외**에 해당한다.

개인정보 보호법 제25조(고정형 영상정보처리기기의 설치 · 운영 제한)
다만, 교도소, 정신보건 시설 등 법령에 근거하여 사람을 구금하거나 보호하는 시설로서 대통령령으로 정하는 시설에 대하여는 그러하지 아니하다. <개정 2023.3.14>

개인정보 보호법 시행령 제22조(고정형 영상정보처리기기 설치 · 운영 제한의 예외)
② 법 제25조제2항 단서에서 "대통령령으로 정하는 시설"이란 다음 각 호의 시설을 말한다. <개정 2017.5.29, 2020.8.4, 2023.9.12>
2. 「정신건강증진 및 정신질환자 복지서비스 지원에 관한 법률」 제3조제5호부터 제7호까지의 규정에 따른 정신의료기관(수용시설을 갖추고 있는 것만 해당한다), 정신요양시설 및 정신재활시설

④

불특정 다수가 이용하는 탈의실은 사생활을 현저히 침해할 우려가 있는 장소이므로, **내부를 볼 수 있도록 고정형 영상정보처리기기를 설치·운영할 수 없다**.

개인정보 보호법 제25조(고정형 영상정보처리기기의 설치 · 운영 제한)
② 누구든지 불특정 다수가 이용하는 목욕실, 화장실, 발한실(發汗室), 탈의실 등 개인의 사생활을 현저히 침해할 우려가 있는 장소의 내부를 볼 수 있도록 고정형 영상정보처리기기를 설치 · 운영하여서는 아니 된다.

NoteBase