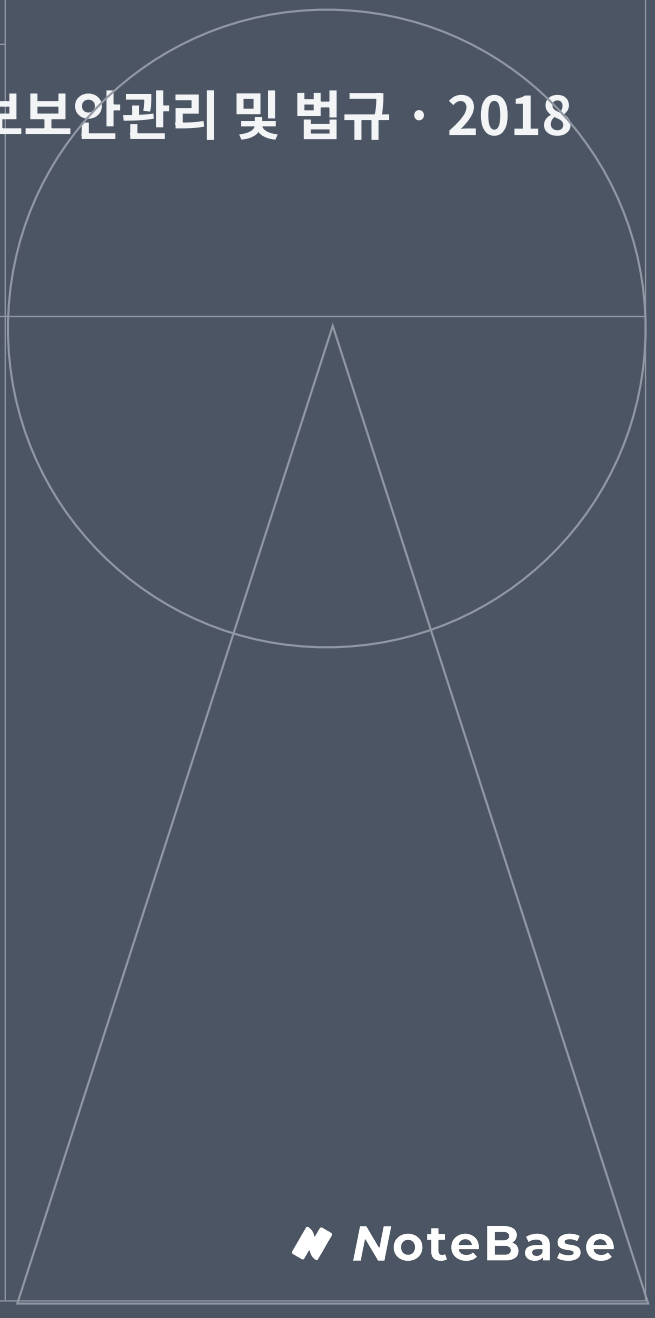
기출OX 해설집

공무원/경찰/경력채용 · 정보보안관리 및 법규 · 2018



NoteBase

기출OX 해설집

공무원/경찰/경력채용 · 정보보안관리 및 법규 · 2018

공무원/경찰/경력채용 · 정보보안관리 및 법규 · 2018

문 1. 강제적 접근통제(MAC : Mandatory Access Control)의 문제점에 대한 설명으로 가장 적절하지 않은 것은?

① 제한적인 사용자 기능과 많은 관리적 부담을 요구하며 비용이 많이 소요된다.

② DAC(Discretionary Access Control) 시스템은 일반적인 목적의 컴퓨터이며, 반면에 MAC 시스템은 매우 특정한 목적을 위해 사용된다.

③ 접근에 대한 레이블링(labeling)을 정의하고 보안 정책을 확인해야하기 때문에 성능저하가 우려된다.

④ 통제의 기준이 주체의 신분에 근거를 두고 있으며, 접근통제 메커니즘이 데이터의 의미에 대해 아무런 지식을 가지고 있지 않다.

정답 4번

간단한 해설

정답은 ④이다. 전통적인 DAC는 **주체의 신원과 소유자가 부여한 권한**을 중심으로 통제하고, 등급 기반 MAC는 **인가 등급과 보안 레이블**에 따라 중앙의 정책을 강제한다.

NoteBase

선지별 해설

① (O) MAC에서는 중앙에서 정한 정책을 사용자가 임의로 바꾸기 어렵다. 따라서 **사용자의 자율성이 제한**되고, 주체·객체의 보안 속성과 정책을 지속적으로 관리하는 데 인력과 비용이 든다.

② (O) 전통적인 적용 환경을 비교한 설명이다. DAC는 소유자가 접근권한을 정하는 방식으로 범용 시스템에 널리 쓰이고, MAC는 군사 기밀처럼 **엄격한 등급별 보호**가 필요한 환경에서 활용되어 왔다. 특정 보안 정책에 맞춘 운용은 유연성을 낮출 수 있다. 다만 MAC가 특정 종류의 컴퓨터에서만 구현된다는 뜻은 아니다.

③ (O) 주체와 객체에 보안 레이블을 부여·관리하고, 접근 시 그 레이블이 정책상 허용되는 관계인지 검사해야 한다. 이 과정에서 **정책 검사에 따른 처리 부담**이 생길 수 있으므로 성능 저하 우려를 들 수 있다. 실제 부담의 크기는 구현에 따라 다르다.

④ (X) 주체의 신원·그룹과 소유자가 정한 권한을 중심으로 통제하는 것은 전통적인 **DAC의 설명**이다. 이 문항의 등급 기반 MAC는 **주체의 인가 등급과 객체의 보안 레이블**을 중앙 정책에 따라 비교한다. 데이터의 민감도가 레이블로 반영된다는 뜻이지, 시스템이 내용의 의미를 스스로 이해한다는 뜻은 아니다. 따라서 MAC의 문제점으로 가장 적절하지 않은 것은 ④이다.

NoteBase

문 2. 다음은 커버로스(Kerberos) 서버, 다수의 클라이언트, 다수의 응용 서버로 구성된 커버로스 공동체 환경을 위한 조건이다. 적절한 것을 모두 고른 것은?

㉠ 커버로스 서버는 반드시 ID와 모든 사용자의 해시된 패스워드를 데이터베이스에 저장하고 있어야 한다.
㉡ 모든 사용자는 커버로스 서버에 등록돼야 한다.
㉢ 커버로스 서버는 각 서버와 비밀키를 공유해야 하고, 모든 서버는 커버로스 서버에 등록돼야 한다.
㉣ 상호 교류하는 각 공동체에 속한 커버로스 서버는 다른 공동체의 서버와 비밀키를 공유하지 않는 대신 두 개의 커버로스 서버는 상호 간에 등록돼야 한다.

① ㉠㉡
② ㉠㉡㉢
③ ㉢㉣
④ ㉠㉡㉢㉣

정답 2번

간단한 해설

공동체 간 인증에서 두 KDC의 **상호 등록만으로 비밀키 공유를 대신할 수는 없다**. 직접 연결된 공동체 사이에는 티켓을 처리할 공동체 간 비밀키가 필요하다.

NoteBase

보기별 해설

이 문항은 '해시된 패스워드'라는 표현이 전제하는 **전통적인 패스워드 기반 커버로스 공동체** 모형을 묻는다. 공동체(realm)의 사용자와 응용 서버를 인증하는 중심 서버를 키 배포 센터(KDC)라고 한다.

㉠ O. 위 모형에서는 KDC가 사용자 식별자와 **패스워드에서 유도한 장기 비밀키**를 보유한다. 원문의 '해시된 패스워드'는 이 키를 뜻하는 설명으로 보아야 하며, 평문 패스워드나 단순 비교용 해시만을 뜻하지 않는다. 다만 Kerberos 전체에 패스워드가 반드시 필요하다는 뜻으로 일반화할 수는 없다. 스마트카드 등 패스워드와 독립된 키를 쓰는 방식도 있다.

㉡ O. 해당 공동체의 인증을 받는 사용자는 **KDC에 사용자 주체로 등록**되어야 한다. KDC가 등록된 사용자 식별 정보와 인증 정보를 바탕으로 티켓을 발급하기 때문이다. 여기서 모든 사용자는 그 공동체의 참여 사용자를 가리킨다.

㉢ O. 해당 공동체의 응용 서버도 서비스 주체로 등록되고, **KDC와 서버의 장기 비밀키를 공유**한다. KDC가 서버용 티켓을 그 키로 암호화하면 응용 서버가 복호화하여 티켓의 내용을 확인할 수 있다.

㉣ X. 직접 신뢰를 맺는 두 공동체의 KDC는 상대를 등록하는 것에 더해 **공동체 간 비밀키를 공유**해야 한다. 이 키로 다른 공동체의 티켓을 처리하므로 상호 등록이 키 공유를 대신하지 못한다. 다만 중간 공동체를 거치는 인증 경로도 가능하므로, 교류하는 모든 원격 공동체 쌍이 직접 키를 공유해야 한다는 뜻은 아니다.

따라서 위 모형에서 적절한 보기는 ㉠, ㉡, ㉢이므로 정답은 ②이다.

NoteBase

문 3. 정보보호 관리체계(ISMS : Information Security Management System)의 수행 절차에 대한 설명으로 가장 적절하지 않은 것은?

① 정보보호 정책 수립, 경영진 책임 및 조직 구성, 위험 관리, 정보보호 대책 구현, 사후 관리 순서의 수행 절차를 가진다.

② 경영진 책임 및 조직 구성 단계에서는 경영진 참여와 정보보호 조직구성 및 자원할당의 절차가 진행된다.

③ 위험 관리 단계에서는 위험관리 방법 및 계획을 수립하고, 위험 식별 및 평가가 이루어지고, 정보보호 대책 산정 및 이행계획이 수립된다.

④ 정보보호 대책 구현 단계에서는 내부 공유 및 교육이 이루어지고, 조직 전반에 걸친 상위 수준의 정보보호 관리체계 범위가 설정된다.

정답 4번

간단한 해설

이 문항의 5단계 ISMS 관리과정에서 **관리체계 범위 설정**은 초기의 정보보호 정책 수립 단계에 속한다. ④의 내부 공유 및 교육은 대책 구현 단계에 맞지만, 범위 설정을 이 단계의 업무로 배치한 부분이 틀리다.

선지별 해설

① O: 이 문항이 전제한 종전 ISMS 관리과정은 **정책 수립 및 범위 설정** → 경영진 책임 및 조직 구성 → 위험 관리 → 대책 구현 → 사후 관리의 흐름이다. 보호 방향과 대상을 정한 뒤 추진 조직을 갖추고, 위험에 맞춰 대책을 정하여 실행한 다음 그 운영을 점검·개선하므로 선지의 순서가 맞다.

② O: 경영진 책임 및 조직 구성 단계는 관리체계가 지속적으로 운영되도록 **경영진의 참여와 실행 기반**을 확보하는 과정이다. 의사결정·보고 체계, 정보보호 조직과 책임, 필요한 예산·인력 등의 자원 할당이 여기에 해당한다.

③ O: 위험 관리 단계에서는 평가 방법·계획 수립 → **위험 식별·평가** → 대책 및 이행계획 수립을 수행한다. 무엇이 얼마나 위험한지 판단한 결과를 바탕으로 대책을 정하고 구현 우선순위와 일정 등을 계획하므로 선지의 내용이 맞다.

④ X: **내부 공유 및 교육은 대책 구현 단계**에 해당하지만, 관리체계 범위 설정은 초기의 **정보보호 정책 수립 및 범위 설정 단계**에서 수행한다. 적용할 서비스·조직·자산 등의 범위를 알아야 후속 위험 평가와 대책 마련의 대상을 정할 수 있기 때문이다. 구현 단계는 이미 수립한 이행계획에 따라 대책을 적용하고 관련 부서·담당자에게 공유·교육하는 단계로 고쳐 이해해야 하므로 정답은 ④이다.

NoteBase

문 4. 국제 공통 평가기준(CC : Common Criteria)에 대한 설명으로 가장 적절하지 않은 것은?

① 국가마다 서로 다른 정보보호시스템 평가기준을 연동하고 평가 결과를 상호인증하기 위해 제정된 평가기준이다.

② 정보보호시스템의 보안등급 평가에 신뢰성을 부여하고 현존하는 평가기준과 조화를 통해 평가결과의 상호인증을 위한 상호인정 협정의 목적이 있다.

③ 보안기능과 보호기능으로 나누어 평가하고 보안 등급 체계는 A, B, C의 6등급으로 D는 부적합에 해당된다.

④ 정보보호 시스템의 수출입에 소요되는 인증비용절감으로 국제 유통촉진이 가능하다.

정답 3번

간단한 해설

CC는 보안기능과 보증 요구사항을 구분하며 평가보증등급은 **EAL1~EAL7**이다. A·B·C·D로 구분하는 체계는 TCSEC의 등급이다.

선지별 해설

① O: CC는 국가별로 달랐던 정보보호제품 평가기준을 공통화하여 보안 요구사항과 평가 결과를 비교할 수 있게 한다. 이러한 공통 기준은 국가 간 평가 결과의 상호인정을 뒷받침한다.

② O: 일관된 기준과 평가 절차를 적용하면 평가 결과에 대한 신뢰를 높일 수 있다. CC는 기술적인 평가기준이고, 이를 바탕으로 인증 결과를 상호인정하는 협정은 **CCRA**이다. 선지는 이러한 상호인정의 목적을 설명한다.

③ X: CC는 **보안기능 요구사항과 보증 요구사항**을 구분한다. 보안기능은 제품이 어떤 보안 기능을 제공해야 하는지를, 보증은 그 기능이 요구대로 구현되었다고 신뢰할 근거를 다룬다. 평가보증등급은 EAL1부터 EAL7까지 7단계이다. A1, B1·B2·B3, C1·C2 및 D로 구분하는 체계는 미국의 TCSEC에 해당하며, D는 평가를 받았으나 그보다 높은 등급의 요구사항을 충족하지 못한 경우이다.

④ O: 상호인정 범위에 포함되는 인증 결과를 다른 참여국에서도 인정하면 **중복 평가 부담**을 줄일 수 있다. 이에 따라 제품의 수출입에 드는 인증 비용과 시간을 줄이고 국제 유통을 촉진할 수 있다.

따라서 CC의 평가 체계와 다른 TCSEC의 등급을 제시한 ③이 가장 적절하지 않다.

NoteBase

문 5. 다음은 개인정보보호 관리체계(PIMS : Personal Information Management System)에 대한 설명이다. 적절하지 않은 것을 모두 고른 것은?

㉠ 국민들에게는 개인정보를 안전하게 관리하는 조직을 객관적으로 식별할 수 있는 기준을 제시한다.
㉡ 통제항목은 정보보호 분야에 개인정보의 특수성을 감안하여 개인정보 수집, 이용, 관리, 파기라는 개인정보 생명주기를 반영한 특징이 있다.
㉢ 인증체계는 과학기술정보통신부가 인정기관 역할을 수행하고 있으며 인증기관으로 한국인터넷진흥원(KISA)이 수행하고 있다.
㉣ 내부 정보 유출 방지를 위해 인증 과정 중에 외부 전문가를 포함하지 않고 기업이 자율 제도로 운영한다.

① ㉠㉡
② ㉡㉢
③ ㉢㉣
④ ㉡㉣

정답 3번

간단한 해설

구 PIMS에서 과학기술정보통신부를 인정기관으로 제시한 ㉢과 외부 전문가를 배제한 기업 자체 제도로 설명한 ㉣이 틀렸다. **정책기관과 인증기관의 역할**, **외부 심사에 의한 인증**을 구분하면 정답은 ③이다.

NoteBase

보기별 해설

이 문항은 ISMS-P로 통합되기 전의 국내 개인정보보호 관리체계(PIMS) 인증제도를 묻는다. 당시 제도와 이후 통합 제도의 담당 기관을 구분하여 판단한다.

㉠ O: PIMS 인증은 조직의 개인정보 보호 활동이 인증기준에 맞게 체계적으로 수행되는지를 외부에서 심사하는 제도이다. 따라서 이용자는 기업의 자체 주장만이 아니라 **객관적인 인증 결과**를 개인정보 관리 수준을 판단하는 기준으로 활용할 수 있다. 인증이 모든 유출 사고의 부재를 보장하는 것은 아니다.

㉡ O: 개인정보는 수집한 뒤 이용·제공하고 보유·관리하다가 필요가 없어지면 파기한다. PIMS는 이러한 **개인정보 생명주기의 각 단계**에 필요한 보호조치를 인증기준에 반영한다. 일반적인 정보보호 대책에 더해 개인정보 처리와 정보주체 권리의 특성을 고려한다는 설명이다.

㉢ X: 문항이 다루는 구 PIMS의 정책·관리 감독 주체는 **방송통신위원회와 행정안전부**이며, 2017년 안내서에서는 개편 전 부처명인 행정자치부로 표기된다. 한국인터넷진흥원이 인증기관을 맡는다는 부분은 맞지만, 과학기술정보통신부를 구 PIMS의 인정기관으로 제시한 부분이 잘못되었다. 정책기관의 제도 관리와 인증기관의 심사·인증 업무를 구분해야 한다.

㉣ X: 인증에는 인증기관의 심사와 분야별 외부 전문가의 참여, 인증위원회의 심의가 포함된다. 따라서 내부 정보 유출 방지를 이유로 외부 전문가를 배제한 기업 자체 인증이라고 설명할 수 없다. **자율적으로 인증을 신청하는 것**과 **기업이 스스로 인증하는 것**은 다르며, 객관성을 갖춘 외부 심사로 인증 여부를 판단한다.

따라서 적절하지 않은 보기는 ㉢과 ㉣이며, 이를 모두 고른 ③이 정답이다.

NoteBase

문 6. 정보보호 관리체계(ISMS)와 개인정보보호 관리체계(PIMS)에 대한 설명으로 가장 적절하지 않은 것은?

① ISMS는 범위내 모든 정보자산과 보호대책을 전반적으로 취급하는데 반해, PIMS는 정보자산 중 개인정보에 특화된 보호와 정보보호를 대상으로 한다.

② PIMS는 원칙적으로 기업 또는 조직 전체가 인증 취득 범위로서 인증 범위를 한정시키고 단계적으로 그 범위를 확대하는 방식으로 채택할 수 있다.

③ ISMS에서는 부서, 사업장, 공장, 서비스 등의 장소와 네트워크, 물리적 대책 등 대상 범위에 대해 합리적으로 설명할 수 있는 범위를 한정해 '적용 범위'로서 인증 취득 범위를 선정할 수 있다.

④ PIMS에서는 정보 주체에게 불이익을 입힌 경우 법규 준수의 관점에서 개인정보만을 취급하는 것이며, ISMS는 정보시스템 전체의 정보보호를 취급한다.

정답 2번

간단한 해설

②의 '기업 또는 조직 전체가 인증 취득 범위'라는 단정이 부정확하다. 당시 PIMS는 **특정 서비스·업무를 구분하여 인증을 신청**하도록 했으며, 인증 범위에 중요한 변경이 있으면 다시 최초심사를 받아야 했다.

NoteBase

선지별 해설

① O: ISMS는 정한 인증 범위 안의 정보자산을 대상으로 기밀성·무결성·가용성을 유지하는 관리체계이다. PIMS는 **개인정보 처리와 정보주체의 권익 보호**에 초점을 맞추며, 개인정보를 처리하는 조직·시스템의 보호조치도 함께 다룬다.

② X: 기업이나 조직 전체를 원칙적인 인증 범위라고 단정한 부분이 부정확하다. 당시 개인정보보호 관리체계 인증 등에 관한 고시 제13조 제2항은 인증 대상을 **특정 서비스·업무로 구분하여 신청**하도록 했다. 또한 제2조 제8호에 따르면 인증 범위에 중요한 변경이 있어 다시 신청할 때에는 최초심사를 실시한다. 범위를 한정하거나 확대하는 것 자체가 무조건 금지되는 것은 아니다. 대상 서비스·업무에 필요한 개인정보 처리 영역을 빠짐없이 포함하고, 중요한 범위 변경에는 다시 심사를 받는 것이 정확하다.

③ O: ISMS는 조직의 서비스와 업무, 물리적 위치, 관련 정보자산 등을 식별하여 적용 범위를 설정한다. 사업장이나 서비스 등 합리적으로 설명되는 범위로 인증을 받을 수 있지만, 그 범위의 정보보호에 필요한 조직·설비·시스템을 임의로 누락해서는 안 된다. 인증 의무대상이라면 법령상 포함해야 할 범위도 지켜야 한다.

④ O: 개인정보 관련 법 준수와 정보주체 보호를 중시하는 PIMS와, 인증 범위의 정보자산 전반을 보호하는 ISMS의 주안점을 대비한 취지이다. 다만 원문의 '정보 주체에게 불이익을 입힌 경우'를 피해 발생 뒤에만 PIMS가 적용된다는 뜻으로 받아들이면 부정확하다. PIMS는 **개인정보 침해의 사전 예방과 지속적 보호**도 포함하며, '개인정보만'은 보호 대상의 초점을 가리킬 뿐 관련 시스템의 안전조치를 제외한다는 뜻이 아니다. ISMS의 '정보시스템 전체'도 앞서 정한 인증 범위 안에서 이해해야 한다.

NoteBase

문 7. 다음에서 설명하는 접근 방식에 따른 위험분석 방법으로 가장 적절한 것은?

모든 정보자산에 기업이외의 전문가 지식 및 경험을 활용하는 방법으로 비용 대비 효과가 우수하며 소규모 조직에 적합한 장점이 있지만, 누락하는 경우가 발생하기 쉽고 사업 분야 및 정보보호에 전문성이 높은 인력이 참여하여 수행하지 않으면 실패할 위험이 있다.

① 기준선 접근법(Baseline Approach)

② 비형식적 접근법(Informal Approach)

③ 상세 위험분석 접근법(Detailed Risk Analysis Approach)

④ 복합 접근법(Combined Approach)

정답 2번

간단한 해설

전문가의 지식과 경험에 의존하여 위험을 분석하면서, 체계적인 절차 부족으로 누락이나 개인 역량의 영향을 받는 것은 비형식적 접근법의 특징이다.

핵심 풀이

비형식적 접근법은 정형화된 분석 절차보다 **전문가의 지식과 경험**에 의존하여 위험을 판단한다. 지문의 외부 전문가 활용, 적은 분석 비용과 소규모 조직에서의 활용 가능성은 이 특징과 연결된다. 다만 체계적인 절차가 부족하여 위험 요소를 빠뜨리거나 판단이 전문가의 역량에 좌우될 수 있다. 외부 전문가만 참여해야 하는 방법이라는 뜻은 아니다.

기준선 접근법은 표준이나 지침에 제시된 **기본 보호대책**을 적용한다. 전문가 개인의 경험을 중심으로 위험을 분석한다는 지문의 핵심과 구별된다.

상세 위험분석 접근법은 자산의 가치, 위협과 취약성을 자세히 조사하여 위험을 분석하고 대책을 선정한다. 체계적인 분석에 상당한 시간과 비용이 들어 지문의 방법과 구별된다.

복합 접근법은 개략적인 위험분석으로 중요하거나 위험이 큰 시스템을 가려 상세히 분석하고, 나머지에는 기준선 대책을 적용하는 등 **분석의 깊이를 달리하여 결합**한다. 지문에는 이러한 구분·결합보다 전문가 경험에 의존하는 특성이 제시되어 있다.

따라서 설명에 해당하는 방법은 ② 비형식적 접근법이다.

NoteBase

문 8. 재해복구 시스템의 복구 수준별 유형에 대한 설명으로 가장 적절하지 않은 것은?

① 미러 사이트(Mirror Site) - 주 센터 재해시 원격지 시스템을 운영(Active) 상태로 전환하며, 서비스 제공 데이터는 동기적 또는 비동기적 방식의 실시간 미러링을 통하여 최신 상태를 유지한다.

② 핫 사이트(Hot Site) - 주 센터와 동일한 수준의 정보기술 자원을 원격지에 구축하여 스탠바이(Stand-by) 상태로 유지하며, 액티브-스탠바이(Active-Standby) 상태로 서비스를 제공함으로써 주기적인 테스트와 구성의 유연성을 제공한다.

③ 웜 사이트(Warm Site) - 중요성이 높은 정보기술 지원만 부분적으로 재해복구센터에 보유하고, 데이터는 수시간에서 1일의 주기로 백업하여 구축 및 유지비용이 핫 사이트에 비해 저렴하다.

④ 콜드 사이트(Cold Site) - 데이터만 원격지에 보관하고, 이의 서비스를 위한 정보자원은 확보하지 않거나 장소 등 최소한으로만 확보하고, 재해시 데이터를 근간으로 필요한 정보자원을 조달하여 정보시스템의 복구를 개시한다.

정답 1번

간단한 해설

이 문항의 복구 수준별 분류에서 미러 사이트는 주 센터와 원격 센터를 평상시부터 **액티브-액티브**로 운영한다. 재해가 난 뒤 대기 중인 원격 시스템을 운영 상태로 전환한다는 ①의 설명은 핫 사이트의 특징이다.

NoteBase

선지별 해설

① X: 미러 사이트는 두 센터가 평상시부터 **동시에 운영**되도록 구성하고 데이터를 지속적으로 복제한다. 재해 후 원격 시스템을 대기 상태에서 액티브로 바꾸는 방식은 이 문항에서 구별하는 핫 사이트에 해당한다. 따라서 미러 사이트의 운영 형태를 액티브-액티브로 고쳐야 하므로 정답은 ①이다. 실시간 미러링이라는 데이터 복제 설명만으로 이 잘못된 운영 상태 설명이 옳아지지는 않는다. 또한 비동기 복제에는 지연이 있을 수 있으므로 데이터 손실이 언제나 전혀 없다고 단정해서는 안 된다.

② O: 핫 사이트는 필요한 장비와 환경을 미리 갖추되, 원격 센터를 **대기 상태로 유지**하다가 재해 시 서비스를 넘겨받도록 하는 유형이다. 이 문항의 액티브-스탠바이 구성은 이러한 준비 수준을 뜻하며, 준비된 대체 환경에서 복구 시험과 구성 점검을 할 수 있다.

③ O: 웜 사이트는 복구에 필요한 설비를 **부분적으로 준비**하는 방식이다. 핵심 기능 중심으로 자원을 갖추고 주기적 백업을 이용하므로 모든 자원을 준비한 핫 사이트보다 일반적으로 비용이 적게 들지만 추가 준비·복원 시간이 필요하다. 선지의 수시간에서 1일이라는 백업 간격은 이 문항이 제시한 운용 수준이며, 모든 웜 사이트에 고정된 필수 주기는 아니다.

④ O: 콜드 사이트는 **장소·기반시설 위주**로 최소한의 복구 기반을 준비하고 서비스용 정보기술 장비는 충분히 갖추지 않는 유형이다. 원격 보관한 백업데이터를 이용하되, 재해 후 장비를 조달·설치하고 데이터를 복원해야 하므로 유지비는 낮은 편이고 복구에는 상대적으로 긴 시간이 걸린다.

NoteBase

문 9. 「개인정보 보호법」에서 개인정보처리자는 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다. 개인정보처리자의 개인정보보호 원칙으로 가장 적절하지 않은 것은?

① 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용할 수 있다.

② 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.

③ 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.

④ 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.

정답 1번

간단한 해설

개인정보는 처리 목적에 필요한 범위에서 적합하게 처리하고, 원칙적으로 **목적 외의 용도로 활용하여서는 안 된다**. 이를 허용하는 내용으로 바꾼 ①이 정답이다.

NoteBase

선지별 해설

업무를 위해 개인정보파일을 직접 또는 다른 사람을 통해 운용하는 공공기관·법인·단체·개인 등은 개인정보처리자이다. 이들이 지켜야 할 개인정보 보호법 제3조의 원칙을 기준으로 판단한다.

① X: 처리 목적에 필요한 범위에서 적합하게 처리해야 한다는 앞부분은 맞지만, 목적 외의 용도로 활용할 수 있다는 뒷부분은 목적 제한 원칙에 반한다. 제3조 제2항에 따라 **그 목적 외의 용도로 활용하여서는 안 된다**고 고쳐야 한다. 법에서 정한 예외적인 목적 외 이용·제공은 별도의 요건 충족 여부를 판단할 문제이며, 선지처럼 일반적인 허용 원칙으로 바꿀 수 없다.

② O: 제3조 제1항은 처리 목적을 분명히 정하고 **그 목적에 필요한 최소한의 정보**만 적법하고 정당하게 수집하도록 한다. 목적을 막연하게 정하거나 나중에 쓸 수도 있다는 이유만으로 불필요한 정보를 더 수집하는 것은 이 원칙에 맞지 않는다.

③ O: 제3조 제3항은 처리 목적에 필요한 범위에서 **정확성·완전성·최신성**이 보장되도록 요구한다. 정보가 사실에 맞고, 목적에 필요한 내용이 빠지지 않으며, 필요한 경우 변화한 내용을 반영해야 한다는 뜻이다. 완전성이 모든 정보를 빠짐없이 수집하라는 뜻은 아니므로 최소 수집 원칙과 함께 적용한다.

④ O: 제3조 제6항은 **사생활 침해를 최소화하는 방법**으로 개인정보를 처리하도록 한다. 수집의 목적과 범위만 적절하면 되는 것이 아니라, 같은 목적을 달성하더라도 정보주체의 사생활에 미치는 영향을 줄이는 처리 방법을 선택해야 한다.

따라서 목적 외 활용을 일반적으로 허용한 ①이 가장 적절하지 않다.

NoteBase

문 10. 「개인정보 보호법」에서 다음 위반 사항에 대한 법정형이 가장 높은 것은?

① 영상정보처리기기의 설치 목적과 다른 목적으로 영상정보처리기기를 임의로 조작하거나 다른 곳을 비추는 자 또는 녹음기능을 사용한 자

② 동법에서 정한 안전성 확보에 필요한 조치를 하지 아니하여 개인정보를 분실·도난·유출·위조·변조 또는 훼손당한 개인정보처리자

③ 업무상 알게 된 개인정보를 누설하거나 권한 없이 다른 사람이 이용하도록 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자

④ 거짓이나 그 밖의 부정한 수단이나 방법으로 개인정보를 취득하거나 개인정보 처리에 관한 동의를 받는 행위를 한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자

정답 3번

간단한 해설

2018년 출제 당시 업무상 알게 된 개인정보의 누설·무권한 제공에는 **5년 이하의 징역 또는 5천만원 이하의 벌금**이 규정되어 있었다. 다른 선지의 법정형 상한은 3년·3천만원 또는 2년·2천만원으로 이보다 낮다.

NoteBase

선지별 해설

2018년 출제 당시 「개인정보 보호법」의 징역형 상한과 벌금형 상한을 같은 기준으로 비교한다.

① 영상정보처리기기를 설치 목적과 다르게 임의로 조작하거나 다른 곳을 비추는 행위, 녹음기능을 사용하는 행위는 당시 제72조제1호에 해당한다. 법정형은 **3년 이하의 징역 또는 3천만원 이하의 벌금**이다.

② 안전성 확보에 필요한 조치를 하지 않아 개인정보의 분실·도난·유출·위조·변조·훼손이 발생한 경우는 당시 제73조제1호에 해당한다. 법정형은 **2년 이하의 징역 또는 2천만원 이하의 벌금**이다. 이 선지는 단순한 안전조치 미이행에 그치지 않고 그로 인한 침해 결과까지 전제한다.

③ 업무상 알게 된 개인정보를 누설하거나 권한 없이 다른 사람이 이용하도록 제공한 행위는 당시 제71조제5호에 해당한다. 그 사정을 알면서 영리 또는 부정한 목적으로 제공받은 자도 포함되며, 법정형은 **5년 이하의 징역 또는 5천만원 이하의 벌금**이다.

④ 거짓이나 부정한 방법으로 개인정보를 취득하거나 처리 동의를 받은 행위는 당시 제72조제2호에 해당한다. 그 사정을 알면서 영리 또는 부정한 목적으로 제공받은 자도 포함되며, 법정형은 **3년 이하의 징역 또는 3천만원 이하의 벌금**이다.

징역형 상한은 ③이 5년, ①·④가 3년, ②가 2년이고, 벌금형 상한도 같은 순서이다. 따라서 제시된 행위 중 법정형이 가장 높은 것은 ③이다.

NoteBase

문 11. 「개인정보 보호법」 제21조(개인정보의 파기)에서 개인정보 처리자의 개인정보 파기와 관련된 내용으로 가장 적절하지 않은 것은?

① 개인정보처리자가 개인정보를 파기하기 전에는 6개월간 임시조치를 하여야 한다.

② 개인정보의 파기방법 및 절차 등에 필요한 사항은 대통령령으로 정한다.

③ 다른 법령에 규정이 없는 한 개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다.

④ 개인정보처리자가 개인정보를 파기하지 아니하고 보존하여야 하는 경우에는 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여서 저장·관리하여야 한다.

정답 1번

간단한 해설

개인정보가 불필요해지면 다른 법령상 보존 의무가 있는 경우를 제외하고 **지체 없이 파기**해야 한다. 파기 전 6개월간 임시조치를 해야 한다는 규정은 없다.

선지별 해설

① X: 개인정보 보호법 제21조에는 파기 전에 **6개월간 임시조치를 하라는 의무가 없다**. 보유기간이 지났거나 처리 목적을 달성하는 등 개인정보가 불필요해지면, 다른 법령에 따른 보존 의무가 있는 경우를 제외하고 지체 없이 파기해야 한다. 파기할 때에는 복구하거나 재생할 수 없도록 조치해야 한다(제1항·제2항).

② O: 제21조 제4항은 개인정보의 구체적인 파기방법과 절차 등에 필요한 사항을 **대통령령에 위임**한다. 법률이 파기의 기본 의무를 정하고, 그 시행에 필요한 세부사항을 대통령령에서 정하도록 한 것이다.

③ O: 제21조 제1항은 보유기간 경과나 처리 목적 달성 등으로 불필요해진 개인정보를 지체 없이 파기하도록 한다. 다만 예외는 다른 법령이 단순히 관련되어 있는 경우가 아니라, **다른 법령에 따라 보존해야 하는 경우**이다.

④ O: 다른 법령에 따른 보존 의무 때문에 개인정보를 파기하지 못하는 경우에는 해당 개인정보나 개인정보파일을 **다른 개인정보와 분리하여 저장·관리**해야 한다(제21조 제3항). 보존 의무가 있다는 이유로 기존 개인정보와 섞어 계속 관리해도 된다는 뜻은 아니다.

따라서 파기 전 6개월의 임시조치 의무를 제시한 ①이 가장 적절하지 않다.

NoteBase

문 12. 「개인정보 보호법」 제23조(민감정보의 처리 제한), 「개인정보 보호법 시행령」 제18조(민감정보의 범위)에서 규정하고 있는 민감정보에 대한 내용으로 가장 적절하지 않은 것은?

① 범죄경력자료

② 성생활에 관한 정보

③ 여권번호

④ 유전정보

정답 3번

간단한 해설

여권번호는 민감정보가 아니라 시행령 제19조의 **고유식별정보**이다. 범죄경력자료, 성생활 정보, 유전자검사 등으로 얻은 유전정보는 민감정보에 해당하므로 정답은 ③이다.

개념 구분

민감정보는 사생활을 현저히 침해할 우려가 있어 법 제23조와 시행령 제18조에서 별도로 정한 정보이다. 고유식별정보는 법령에 따라 개인을 고유하게 구별하기 위해 부여된 식별정보로서 법 제24조와 시행령 제19조에서 정한다. **중요하게 보호해야 한다는 점이 같아도 법적 분류는 다르다**.

범죄경력자료·유전정보: 시행령 제18조는 「형의 실효 등에 관한 법률」 제2조 제5호에 따른 범죄경력자료와 **유전자검사 등의 결과로 얻어진 유전정보**를 민감정보 범위에 둔다. 따라서 ①과 ④는 문항에서 묻는 민감정보에 해당한다.

성생활에 관한 정보: 법 제23조가 **직접 열거한 민감정보**이다. 개인의 내밀한 생활에 관한 내용이므로 ②도 민감정보에 해당한다.

여권번호: 시행령 제19조 제2호에 규정된 **고유식별정보**이다. 민감정보 항목으로 분류하는 것이 아니라 개인 식별을 위한 번호로 구분하며, 민감정보에 포함되지 않는다고 해서 자유롭게 처리할 수 있다는 뜻은 아니다.

따라서 민감정보의 범위에 해당하지 않는 여권번호를 고른 ③이 정답이다.

NoteBase

문 13. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 정보통신서비스 제공자등은 개인정보의 분실·도난·유출 사실을 안 때에는 지체 없이 해당 개인정보를 이용자에게 알리고 해당 기관에 신고해야 한다. 신고해야 할 내용으로 가장 적절하지 않은 것은?

① 유출등이 된 개인정보 항목

② 유출등이 발생한 시점

③ 이용자가 상담 등을 접수할 수 있는 부서 및 연락처

④ 이용자의 손해배상액

정답 4번

간단한 해설

이 문항의 당시 법령상 개인정보 유출 통지·신고 사항에는 피해 대응에 필요한 항목·시점·조치·연락처가 포함된다. **이용자의 손해배상액**은 이러한 필수 사항에 포함되지 않으며, 배상책임과 금액의 판단은 별개의 문제이다.

선지별 해설

2018년 문항이 전제한 구 정보통신망법 제27조의3제1항은 개인정보 유출등을 안 정보통신서비스 제공자등에게 이용자 통지와 관계 기관 신고를 요구하였다. 대상 사항은 유출된 개인정보 항목, 발생 시점, 이용자가 취할 수 있는 조치, 제공자등의 대응 조치, 상담 접수 부서 및 연락처였다. 아래 O/X는 이 필수 사항에 포함되는지를 뜻한다.

① O: **유출된 개인정보 항목**은 제1호의 통지·신고 사항이다. 어떤 종류의 개인정보가 유출되었는지 알아야 이용자가 노출 범위와 예상 피해를 판단하고 적절한 대응을 할 수 있다.

② O: **유출등이 발생한 시점**은 제2호의 사항이다. 사고가 언제 발생했는지 알리는 내용으로, 제공자가 사고 사실을 인지한 시점과 구별된다.

③ O: **상담 접수 부서 및 연락처**는 제5호의 사항이다. 이용자가 유출 사고에 관하여 문의하거나 필요한 도움을 요청할 수 있는 창구를 알리는 것이다.

④ X: 손해배상액은 **필수 통지·신고 사항이 아니다**. 법정 사항은 유출 정보와 발생 시점, 이용자·제공자의 대응 조치, 상담 창구이며, 이용자별 배상액의 확정을 포함하지 않는다. 선지는 손해배상액 대신 “이용자가 취할 수 있는 조치” 또는 “정보통신서비스 제공자등의 대응 조치”와 같은 사항으로 바꾸어야 한다. 따라서 정답은 ④이며, 이는 이용자의 손해배상청구 자체가 부정된다는 뜻은 아니다.

NoteBase

문 14. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제44조의7 (불법정보의 유통금지 등)에 의거 누구든지 정보통신망을 통하여 불법정보를 유통해서는 안 된다. 이 불법정보에 대한 설명으로 가장 적절하지 않은 것은?

① 정당한 사유 없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해하는 내용의 정보

② 총포·화약류를 제조할 수 있는 방법이나 설계도 등의 정보

③ 사람을 비방할 목적이 없는 공공연한 사실 등의 정보

④ 범죄를 목적으로 하거나 교사 또는 방조하는 내용의 정보

정답 3번

쟁점

정보통신망법 제44조의7에서 유통을 금지하는 불법정보의 유형과 명예훼손 정보의 요건을 구별하는 문제이다.

용어 풀이

비방할 목적은 다른 사람의 평판이나 명예를 해치려는 목적이다. 공공연하게는 불특정인 또는 여러 사람이 알 수 있는 상태를 뜻한다. 교사는 다른 사람에게 범죄를 저지르도록 하는 것이고, 방조는 범죄 실행을 돕는 것이다.

핵심 구분

명예훼손 유형의 불법정보는 사람을 비방할 목적으로 사실이나 거짓의 사실을 공공연하게 드러내어 타인의 명예를 훼손하는 내용의 정보이다. 사실이 진실인지 거짓인지뿐 아니라 비방 목적과 명예훼손 내용이 있는지를 함께 판단한다. 비방 목적 없이 사실을 공개했다는 설명만으로 이 유형에 해당한다고 볼 수 없다.

선지별 해설

① O: 정당한 사유 없이 시스템·데이터·프로그램을 훼손하거나 그 운용을 방해하는 내용의 정보는 유통금지 대상이다. 시스템에 대한 부당한 파괴나 운영 방해를 내용으로 한다는 점이 핵심이다.
② O: 총포·화약류를 제조할 수 있는 방법이나 설계도 등의 정보는 유통금지 대상이다. 실제 제조에 이용될 수 있는 방법·설계도라는 정보의 내용이 판단 기준이다.
③ X: “사람을 비방할 목적이 없는”이라는 표현이 틀렸다. 올바르게는 “사람을 비방할 목적으로 공공연하게 사실이나 거짓의 사실을 드러내어 타인의 명예를 훼손하는 내용의 정보”이다. 선지는 비방 목적을 부정하고 명예훼손이라는 내용도 빠뜨려 해당 불법정보의 요건을 충족하지 못한다.
④ O: 범죄를 목적으로 하거나 범죄를 교사 또는 방조하는 내용의 정보는 유통금지 대상이다. 직접 범죄 실행을 목적으로 하는 내용뿐 아니라 다른 사람의 범죄를 유발하거나 돕는 내용도 포함한다.

NoteBase

오답 포인트

③의 “공공연한 사실”에만 주목하면 사실 공개 자체를 불법정보로 오해하기 쉽다. 결정적인 함정은 “비방할 목적이 없는”이라는 표현으로 필수 요건을 뒤집은 데 있다. 반대로 진실한 사실이라는 이유만으로 이 명예훼손 유형에서 제외되는 것도 아니다.

다시 나오면 이렇게 판단

먼저 선지가 유통금지 유형의 요건을 그대로 갖추었는지 확인한다. 명예훼손 정보는 비방 목적, 공공연한 사실 또는 거짓 사실의 공개, 타인의 명예훼손을 함께 확인한다. 다른 유형의 위법성까지 비방 목적의 유무만으로 판단하지 않는다.

암기 포인트

명예훼손 정보: 비방 목적 + 공공연한 사실·거짓 사실 공개 + 타인의 명예훼손.

NoteBase

문 15. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 "정보통신서비스제공자는 정보통신서비스의 제공에 사용되는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 하여야 한다"고 규정하고 있다. 정보통신망의 안정성 확보에 관한 정보보호지침 내용으로 가장 적절하지 않은 것은?

① 정보통신망의 지속적인 이용이 가능한 상태를 확보하기 위한 기술적·물리적 보호조치

② 정보통신망의 안정성 유지를 위한 법적·행정적 보호조치

③ 정보의 불법 유출·위조·변조·삭제 등을 방지하기 위한 기술적 보호조치

④ 정당한 권한이 없는 자가 정보통신망에 접근·침입하는 것을 방지하거나 대응하기 위한 정보보호시스템의 설치·운영 등 기술적·물리적 보호조치

정답 2번

간단한 해설

정보통신망의 안정성 유지를 위한 인력·조직·경비 확보와 관련 계획 수립은 **관리적 보호조치**에 해당한다. 정보보호지침의 해당 항목을 법적·행정적 보호조치로 바꾸면 틀린 설명이 된다.

선지별 해설

① O: 정보통신망을 계속 이용할 수 있도록 하는 **기술적·물리적 보호조치**는 정보보호지침에 포함된다. 망의 지속적인 이용 가능 상태를 확보하는 조치로, 법 제45조 제3항 제3호에 해당한다.

② X: 법 제45조 제3항 제4호는 정보통신망의 안정성 유지를 위한 **관리적 보호조치**를 규정한다. 구체적으로 인력·조직·경비 확보 및 관련 계획 수립 등이 이에 해당하므로, 선지의 "법적·행정적 보호조치"를 이 내용으로 고쳐야 한다.

③ O: 정보의 불법 유출·위조·변조·삭제 등을 방지하기 위한 **기술적 보호조치**는 법 제45조 제3항 제2호에 해당한다. 정보가 권한 없이 유출되거나 부당하게 만들어지거나 변경·삭제되는 것을 막는 조치이다.

④ O: 정당한 권한이 없는 자의 접근·침입을 방지하거나 이에 대응하는 **기술적·물리적 보호조치**는 법 제45조 제3항 제1호에 해당한다. 정보보호시스템의 설치·운영은 이러한 보호조치에 포함된다.

따라서 가장 적절하지 않은 것은 ②이다.

NoteBase

문 16. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 및 동 시행령, 「개인정보 보호법」 및 동 시행령에 의거 개인정보 유출 통지 및 신고에 관한 법적 절차가 명시되어 있다. 네 가지 법령에서 "개인정보 유출 통지 및 신고 내용"을 설명한 것으로 가장 적절한 것은?

① 「개인정보 보호법 시행령」에 의하면 대통령령으로 정한 규모 이상의 개인정보란 5천 건 이상의 정보주체를 의미한다.

② 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니 된다고 규정하고 있다.

③ 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」에서 유출 신고 건수는 1만 건 이상을 의미한다.

④ 「개인정보 보호법」에서 개인정보 유출 신고기관은 방송통신위원회와 한국인터넷진흥원이다.

정답 2번

간단한 해설

정답은 ②이다. 2018년 당시 정보통신망법은 정당한 사유 없이 개인정보 분실·도난·유출 사실을 안 때부터 **24시간을 넘겨 통지·신고할 수 없도록** 규정했다.

NoteBase

선지별 해설

2018년 출제 당시 시행되던 법령을 기준으로 판단한다.

① X: 2018년 당시 「개인정보 보호법 시행령」 제39조제1항의 신고 기준은 **1천 명 이상의 정보주체**에 관한 개인정보이다. 5천 건이 아니며, 정보의 항목 수나 건수가 아니라 개인정보가 유출된 정보주체의 수를 기준으로 한다.

② O: 당시 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제27조의3제1항은 개인정보의 분실·도난·유출 사실을 알면 지체 없이 이용자에게 통지하고 방송통신위원회 또는 한국인터넷진흥원에 신고하도록 했다. 특히 정당한 사유 없이 **그 사실을 안 때부터 24시간을 넘겨서는 안 된다**고 규정했다. 이는 언제나 24시간까지 기다려도 된다는 뜻이 아니다.

③ X: 당시 정보통신망법과 그 시행령의 유출 통지·신고 의무에는 **1만 건 이상이라는 최소 수량 조건이 없다**. 정보통신서비스 제공자등은 개인정보의 분실·도난·유출 사실을 알게 되면 그 규모와 관계없이 법정 사항을 통지·신고해야 했다. 개인정보 보호법령의 일정 규모 이상 유출 신고 기준과 혼동하면 안 된다.

④ X: 당시 「개인정보 보호법」 제34조제3항과 같은 법 시행령 제39조제2항에 따른 신고 대상 기관은 **행정안전부장관 또는 한국인터넷진흥원**이다. 방송통신위원회 또는 한국인터넷진흥원에 신고하도록 한 것은 당시 정보통신망법의 규정이다.

NoteBase

문 17. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 정보통신서비스 제공자가 이용자의 개인정보를 제3자에게 제공할 때, 이용자에게 동의를 받아야 하는 내용으로 가장 적절하지 않은 것은?

① 개인정보를 제공받는 자

② 개인정보를 제공받는 자의 개인정보 이용목적

③ 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간

④ 개인정보를 제공받는 자의 개인정보 침해 이력

정답 4번

간단한 해설

당시 정보통신망법의 제3자 제공 동의 고지사항은 제공받는 자, 이용 목적, 제공 정보 항목, 보유·이용 기간이다. **제공받는 자의 개인정보 침해 이력**은 여기에 포함되지 않으므로 정답은 ④이다.

핵심 풀이

문항은 2018년 당시 정보통신망법 제24조의2 제1항의 제3자 제공 동의를 묻는다. 동의를 받기 위해 알려야 하는 사항은 **제공받는 자, 이용 목적, 제공하는 개인정보 항목, 보유 및 이용 기간**의 네 가지이다. 이는 이용자가 자신의 정보가 누구에게, 무슨 목적으로, 어느 범위까지, 얼마나 오래 넘어가는지 알고 결정하도록 하는 기준이다.

①의 제공받는 자는 정보가 전달될 상대방을, ②의 이용 목적은 그 상대방이 정보를 사용할 용도를, ③의 보유 및 이용 기간은 그 상대방이 정보를 보유·이용할 기간을 뜻한다. 세 항목 모두 해당 조문에 규정되어 있다. 선택지에 나오지 않은 **제공하는 개인정보의 항목**도 법정 고지사항에 포함된다.

④의 개인정보 침해 이력은 제공받는 자의 과거 사고·위반 관련 정보로, 위 조문이 정한 제3자 제공 동의의 고지사항에 포함되지 않는다. 보안상 참고할 수 있는 정보라는 점과 **해당 조문의 필수 고지사항인지**는 구분해야 한다. 따라서 가장 적절하지 않은 것은 ④이다.

NoteBase

문 18. 「정보통신기반 보호법」에서 국가안전보장에 중대한 영향을 미치는 주요정보통신기반시설에 대한 관리기관의 장이 기술적 지원을 요청한 경우 국가정보원장이 기술적 지원을 수행할 수 없는 시설로 가장 적절한 것은?

① 원자력·국방과학·첨단방위산업관련 정부출연연구기관의 연구시설

② 개인정보가 포함된 금융 정보통신기반시설

③ 전력, 가스, 석유 등 에너지·수자원 시설

④ 도로·철도·지하철·공항·항만 등 주요 교통시설

정답 2번

간단한 해설

국가정보원장은 금융 정보통신기반시설 등 **개인정보가 저장된 모든 정보통신기반시설**에 기술적 지원을 할 수 없다. 관리기관의 요청이 있어도 이 금지는 적용된다.

핵심 풀이

「정보통신기반 보호법」 제7조제2항은 국가안전보장에 중대한 영향을 미치는 일정한 주요정보통신기반시설에 대해 기술적 지원이 필요한 경우 **국가정보원장에게 우선 요청**하도록 정한다. 그러나 같은 조 제3항에 따른 지원 금지 대상인지는 별도로 확인해야 한다.

지원 금지 기준: 제7조제3항은 금융 정보통신기반시설을 포함하여 **개인정보가 저장된 모든 정보통신기반시설**에 대한 국가정보원장의 기술적 지원을 금지한다. 따라서 관리기관의 장이 요청했다는 사정만으로 이 금지가 해제되지 않는다.

경쟁 시설의 구분: 원자력·국방과학·첨단방위산업 관련 정부출연연구기관의 연구시설은 제2항제4호, 에너지·수자원 시설은 제2항제2호, 주요 교통시설은 제2항제1호에 열거되어 있다. 이들은 **우선 지원 요청 대상의 시설 유형**이며, 해당 시설에 개인정보가 저장되어 있다면 제3항의 금지 규정도 적용된다는 점은 같다.

결국 명시적으로 개인정보가 포함되어 있어 국가정보원장의 기술적 지원이 금지되는 시설은 ②이다.

NoteBase

문 19. 「정보통신기반 보호법」에서 “전자적 침해행위”에 대한 내용으로 가장 적절하지 않은 것은?

① 해킹

② 인터넷사기

③ 컴퓨터바이러스

④ 고출력 전자기파

정답 2번

간단한 해설

전자적 침해행위는 **정보통신기반시설 자체를 공격**하는 행위를 말한다. 인터넷사기는 인터넷을 이용해 사람을 속이는 행위이므로, 그 자체만으로 이러한 시설 공격에 해당하지 않는다.

개념 구분

전자적 침해행위의 기준은 **정보통신기반시설을 공격하는 행위**인지 여부이다. 출제 당시 「정보통신기반 보호법」 제2조 제2호는 그 방법으로 해킹, 컴퓨터바이러스, 논리·메일폭탄, 서비스거부, 고출력 전자기파 등을 규정하였다.

① 해킹과 ③ 컴퓨터바이러스는 법에서 명시한 공격 방법이다. ④ 고출력 전자기파도 명시되어 있으므로, 전자적 침해행위를 인터넷을 통한 침입이나 악성 프로그램 공격만으로 좁혀 이해해서는 안 된다.

② 인터넷사기는 인터넷을 이용해 상대방을 속여 재산상 이익을 얻는 행위이다. **인터넷을 사기의 수단으로 이용**한다는 것만으로 정보통신기반시설 자체에 대한 공격이 되는 것은 아니다. 예를 들어 물품을 판매할 것처럼 속여 대금만 받는 행위는 시설 공격과 구별된다.

따라서 전자적 침해행위에 대한 내용으로 가장 적절하지 않은 것은 ②이다.

NoteBase

문 20. 「전자서명법」에서 공인인증에 대한 설명으로 가장 적절하지 않은 것은?

① “공인인증서”라 함은 공인인증기관이 발급하는 인증서를 말한다.

② “공인인증자”라 함은 전자서명생성정보를 보유하고 자신이 직접 또는 타인을 대리하여 서명을 하는 자를 말한다.

③ “공인인증기관”이라 함은 공인인증역무를 제공하기 위하여 지정된 자를 말한다.

④ “공인인증업무”라 함은 공인인증서의 발급, 인증관련 기록의 관리 등 공인인증역무를 제공하는 업무를 말한다.

정답 2번

간단한 해설

전자서명생성정보를 보유하고 직접 또는 대리하여 서명하는 사람의 법정 명칭은 **서명자**이다. 이를 ‘공인인증자’라고 한 부분이 잘못되었다.

선지별 해설

2018년 시험 당시의 구 「전자서명법」상 공인인증 제도를 기준으로, 인증서를 발급하는 기관과 실제 전자서명을 하는 사람을 구별한다. 전자서명생성정보는 전자서명을 만드는 데 사용하는 전자적 정보이다.

① O: 공인인증서는 법에 따라 **공인인증기관이 발급하는 인증서**이다. 인증서는 전자서명생성정보가 가입자에게 유일하게 속한다는 사실 등을 확인하여 증명하는 전자적 정보이므로, 발급 주체가 누구인지가 공인인증서의 구별 기준이 된다.

② X: 전자서명생성정보를 보유하고 직접 또는 타인을 대리하여 서명하는 사람은 **서명자**이다. 선지는 서명자의 정의에 ‘공인인증자’라는 잘못된 명칭을 붙였다. 공인인증기관에서 전자서명생성정보를 인증받은 사람을 뜻하는 ‘가입자’와도 구별된다.

③ O: 공인인증기관은 **공인인증역무를 제공하도록 지정된 자**이다. 단순히 서명하는 사람이 아니라, 법에서 정한 지정을 받아 인증서를 발급하는 등 인증 서비스를 담당하는 주체이다.

④ O: 공인인증업무는 공인인증서의 발급과 인증 관련 기록의 관리 등 **인증 서비스를 제공하는 업무**이다. 공인인증기관이 업무의 주체이고, 공인인증업무는 그 기관이 수행하는 활동을 가리킨다.

따라서 서명자의 정의를 다른 명칭에 연결한 ②가 가장 적절하지 않다.

NoteBase