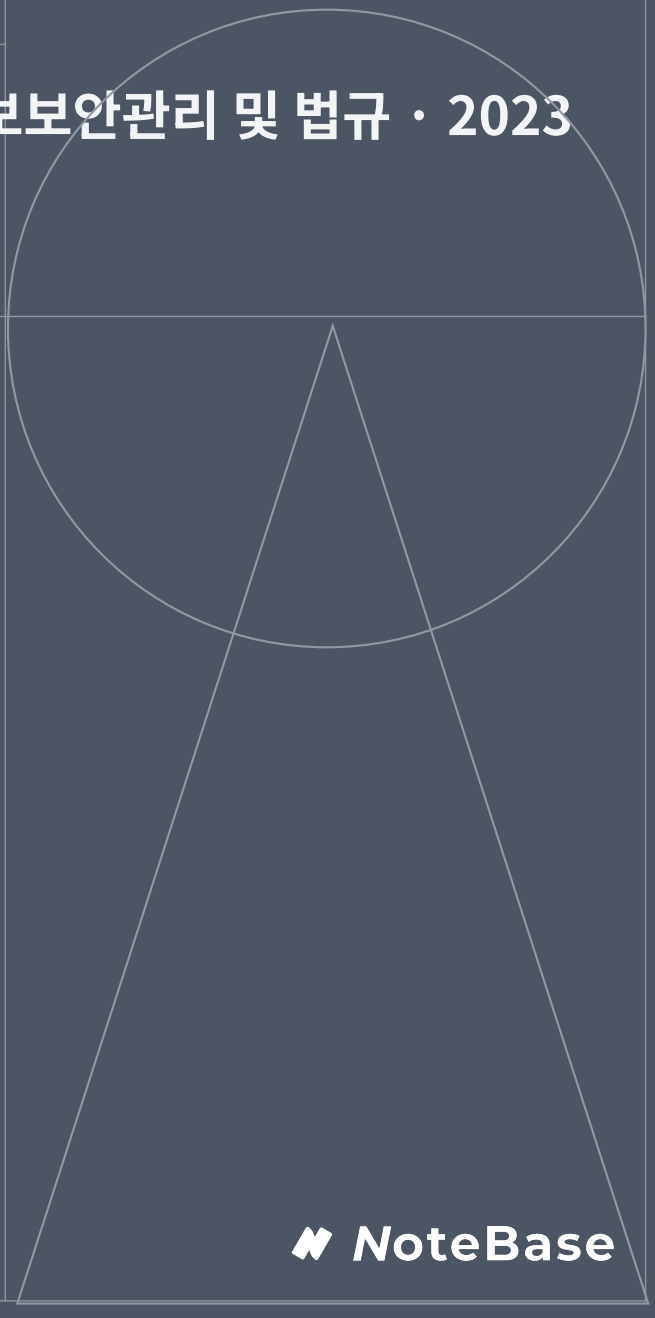
기출OX 해설집

공무원/경찰/경력채용 · 정보보안관리 및 법규 · 2023



NoteBase

기출OX 해설집

공무원/경찰/경력채용 · 정보보안관리 및 법규 · 2023

공무원/경찰/경력채용 · 정보보안관리 및 법규 · 2023

문 1. 정보보호에 관한 설명으로 가장 적절하지 않은 것은?

① 정보보호는 다양한 내·외부 위협으로부터 조직의 정보자산에 대한 기밀성, 무결성, 가용성 등이 보장될 수 있도록 관리적, 기술적, 물리적 보호조치를 마련하는 것이다.

② 기밀성(confidentiality)은 권한있는 자만이 정보자산에 접근하여 그 내용을 알 수 있도록 보장하며 정당하지 않은 자에 의해 정보가 노출되지 않도록 보장하는 것이다.

③ 무결성(integrity)은 권한있는 자만이 위조·변조된 정보를 확인할 수 있도록 보장하며 이를 위해 장비 이중화 구성, 서버 클러스터링 구성, 디스크 RAID 구성의 기법이 활용된다.

④ 가용성(availability)은 권한있는 자의 정보자산 접근 필요 시 언제든지 접근할 수 있도록 보장하며 장애·재해가 발생해도 정상적인 서비스가 가능하도록 보장하는 것이다.

정답 3번

간단한 해설

무결성은 정보의 **부당한 변경·훼손을 방지**하는 성질이다. 장비 이중화와 장애 대응용 클러스터링 등은 주로 가용성을 높이는 대책이므로 ③이 가장 적절하지 않다.

NoteBase

선지별 해설

① O: 정보보호는 조직의 정보자산이 유출되거나 부당하게 변경되거나 사용 불가능해지는 위험을 줄여 기밀성·무결성·가용성을 유지하는 활동이다. 내부자의 오용과 외부 공격 등을 함께 고려하며, 정책·교육 같은 관리적 조치, 접근통제 같은 기술적 조치, 출입통제 같은 물리적 조치를 **함께 마련**한다.

② O: 기밀성은 정보의 열람·공개를 허가된 범위로 제한하여 **비인가자에게 내용이 노출되지 않도록** 하는 성질이다. 정보가 변경되었는지보다 누가 내용을 알 수 있는지가 핵심이며, 접근권한 관리와 암호화 등이 이를 지원한다.

③ X: 무결성은 권한 있는 자만 위조·변조된 정보를 확인하게 하는 것이 아니라, 정보가 **부당하게 변경·훼손되지 않도록** 정확성과 완전성을 유지하는 성질이다. 변경을 예방하거나 탐지하는 통제가 필요하다. 장비 이중화, 장애 대응용 서버 클러스터링, 중복성을 갖춘 RAID는 주로 고장 시에도 서비스를 이어 가게 하는 **가용성 대책**이다. 다만 RAID 0은 중복성이 없어 디스크 장애에 대한 내결함성을 제공하지 않는다.

④ O: 가용성은 권한 있는 사용자가 필요할 때 정보와 서비스를 적시에 안정적으로 이용할 수 있게 하는 성질이다. 장애·재해에 대비한 이중화, 백업·복구, 재해복구 계획 등은 **서비스 중단을 줄이고 이용을 회복**하기 위한 수단이다. 이는 가용성을 확보하려는 목표이며 모든 장애에서 중단이 절대로 없다는 뜻은 아니다.

따라서 무결성의 정의와 가용성 대책을 혼동한 ③이 가장 적절하지 않다.

NoteBase

문 2. 재해복구시스템의 복구 수준별 유형에 관한 설명으로 가장 적절하지 않은 것은?

① 미러사이트 : 관리자가 선택한 데이터만을 별도의 백업디스크에 순차적으로 백업하는 방식으로 많은 복구 시간이 필요하다.

② 핫 사이트 : 주센터와 동일 수준의 시스템을 원격지 사이트에 구축한 후 대기상태로 실시간 미러링(mirroring)을 통해 최신 데이터를 유지하는 방식이며 주센터 재해 발생 시 활성상태로 전환하여 서비스를 제공한다.

③ 웜 사이트 : 주센터의 중요도가 높은 일부 시스템만 원격지 사이트에 구축하여 주센터 재해 발생 시 중요 업무에 대해서만 우선 복구하는 방식이다.

④ 콜드 사이트 : 데이터만 원격지에 보관하고 서비스를 위한 시스템은 확보하지 않거나 전원시설, 통신설비 등만을 최소한으로 확보하는 방식이다.

정답 1번

간단한 해설

미러사이트는 **두 센터가 함께 서비스를 운영**하여 재해에도 신속히 업무를 이어가는 방식이다. 선택 자료를 디스크에 저장하고 오래 복원하는 방식이라는 설명은 이 특성과 맞지 않는다.

선지별 해설

이 문항은 재해 전에 원격지에 마련한 시스템과 데이터의 준비 수준을 구분한다.

① X: 미러사이트는 주센터와 동등한 시스템을 원격지에 갖추고 **양쪽에서 실시간으로 서비스를 운영**한다. 선택한 자료를 별도 디스크에 저장한 뒤 재해 때 복원하는 단순 백업과 다르며, 신속하게 업무를 이어갈 수 있도록 구성한다.

② O: 핫 사이트는 동등한 시스템과 최신 데이터를 준비하되, 원격지 시스템은 평소 **대기 상태**를 유지한다. 재해 때 이를 활성화한다는 점에서 두 센터가 함께 서비스하는 미러사이트와 구별된다.

③ O: 웜 사이트는 중요 자원부터 부분적으로 갖추므로 **핵심 업무를 우선 복구**한다. 전체 업무를 정상화하려면 부족한 자원과 데이터를 추가로 준비해야 한다.

④ O: 콜드 사이트는 백업 데이터와 최소 시설 위주로 준비한다. 서비스를 재개하려면 **장비 조달과 시스템 구축·복원**이 더 필요하므로 준비된 시스템을 전환하는 방식보다 오래 걸린다.

NoteBase

문 3. 시점별 통제에 관한 설명으로 가장 적절하지 않은 것은?

① 통제의 시점에 따라 예방통제, 탐지통제, 교정통제로 구분된다.

② 교정통제는 탐지 전 위협과 취약점에 대응하는 것으로 IDS의 성능을 향상시킨다.

③ 탐지통제는 예방통제를 우회하여 발생하는 문제점을 탐지하려는 활동으로 위협을 탐지한다.

④ 예방통제란 사전에 위협과 취약점에 대처하는 통제를 의미한다.

정답 2번

간단한 해설

교정통제는 **문제를 발견한 뒤 원인과 피해를 시정**하는 통제이다. 탐지 전 대응으로 설명한 ②는 예방통제와 혼동한 것이며, IDS는 탐지통제의 대표 수단이다.

선지별 해설

① O: 통제가 문제의 발생 전·발견 과정·발견 후 어느 시점에 주로 작용하는지를 기준으로 예방통제, 탐지통제, 교정통제로 나눈다. 각각 **발생 방지, 이상 징후 발견, 발견된 문제의 시정**에 초점을 둔 분류이다.

② X: 교정통제는 **문제를 발견한 뒤 원인과 피해를 바로잡는** 통제이다. 감염된 시스템에서 악성코드를 제거하거나 손상된 자료를 복구하는 조치가 여기에 해당한다. 따라서 탐지 전에 위협·취약점에 대응한다는 설명은 예방통제의 성격에 가깝다. 또한 IDS는 침입 징후를 찾아 알리는 탐지통제의 대표 수단이며, IDS의 성능 향상이 교정통제의 정의나 필수 효과인 것은 아니다.

③ O: 예방 조치가 모든 공격을 막는 것은 아니므로, 이를 우회해 발생한 문제나 침입 시도를 **관찰·분석하여 발견**하는 통제가 필요하다. IDS의 경보나 로그 분석이 대표적이다. 탐지통제는 위협의 존재를 알아내어 후속 대응이 시작될 수 있게 한다.

④ O: 예방통제는 문제가 발생하기 전에 위협과 취약점에 대처하여 **사고의 발생 가능성을 줄이는** 통제이다. 예를 들어 접근 권한을 제한하고 인증을 요구하면 비인가자의 접근을 사전에 억제할 수 있다.

따라서 교정통제의 작용 시점과 IDS의 역할을 혼동한 ②가 가장 적절하지 않다.

NoteBase

문 4. 위험분석 방법론에 관한 설명으로 가장 적절하지 않은 것은?

① 델파이법 : 각 분야의 전문적인 지식을 갖춘 전문가 집단을 구성하고 토론을 통해 위험분석을 수행하는 방식이다.

② 퍼지 행렬법 : 자산, 위험, 보안체계 등 위험분석 요소들을 정성적인 언어로 표현된 값을 사용하여 기대 손실을 평가하는 방식이다.

③ 확률 분포법 : 비교 우위 순위 결정표에 의해 위험 항목들의 서술적 순위를 결정하는 방식이다.

④ 시나리오법 : 어떤 사건도 기대대로 발생하지 않는다는 사실에 근거하여 위협에 대한 발생 가능한 결과들을 추정하는 방식이다.

정답 3번

간단한 해설

위험 항목의 비교 우위를 따져 서술적 순서를 정하는 방식은 **순위결정법**이다. 확률 분포법은 위험 발생이나 손실 규모의 확률분포를 이용하므로, 순위를 매기는 방법과 구별해야 한다.

선지별 해설

① O: 델파이법은 **전문가의 판단을 모아** 불확실한 위험을 분석한다. 선지의 '토론'은 전문가 의견을 교환·종합한다는 넓은 취지로 이해해야 한다. 엄밀한 전통 델파이는 대면 자유토론이 아니라 **익명 응답, 반복 설문, 통제된 피드백**으로 판단을 조정하는 방식이므로, 원문의 표현만으로 구체적인 토론 절차를 단정해서는 안 된다.

② O: 퍼지 행렬법은 위험분석 요소를 '높음·보통·낮음'과 같은 **정성적 언어 값**으로 나타내고, 이 값들의 관계를 결합하여 손실·위험 수준을 평가한다. 불확실하고 경계가 모호한 판단을 다룬다는 점이 특징이며, 선지의 기대 손실 평가를 반드시 정확한 금액 산출로 이해할 필요는 없다.

③ X: 비교 우위 순위 결정표로 위험 항목의 서술적 순위를 정하는 것은 **순위결정법**이다. 확률 분포법은 위험의 발생이나 손실 규모를 확률변수와 확률분포로 나타내어 분석한다. 따라서 '확률 분포법'을 '순위결정법'으로 고쳐야 하며, 방법 이름과 설명이 직접 어긋난 이 선지가 가장 적절하지 않다.

④ O: 시나리오법은 위협이 발생했을 때 가능한 전개와 결과를 여러 경우로 구성하여 검토한다. 핵심은 **단일한 예상에 의존하지 않고 가능한 결과들을 추정**하는 것이다. '어떤 사건도 기대대로 발생하지 않는다'는 표현은 미래의 불확실성을 강조한 취지이지, 모든 사건이 반드시 예측과 다르게 일어난다는 사실을 전제로 삼는다는 뜻은 아니다.

NoteBase

문 5. 다음 표준에 관한 설명으로 옳은 것을 모두 고른 것은?

㉠ ISO/IEC 27000은 영국에서 개발된 BSI(British Standards Institute) 인증을 기반으로 만들어진 암호화 프레임워크로 국내 표준이다.
㉡ ISO/IEC 27000은 최적의 보안 관리체계 수립 운영, 정보보호 관리규범 제공을 목적으로 한다.
㉢ ISO/IEC 27001:2013은 통제영역 14개, 통제항목 114개로 구성된다.
㉣ ISO/IEC 27000은 유럽 회원국 공통으로 적용되는 정보보안 조례로 흔히 오렌지 북(orange book)이라고 불린다.

① ㉠㉡
② ㉡㉣
③ ㉡㉢
④ ㉠㉣

정답 3번

간단한 해설

ISO/IEC 27000 계열은 **정보보호 관리체계의 국제표준군**이다. 27001:2013의 통제는 14개 영역·114개 항목이며, 오렌지 북은 미국의 TCSEC이므로 ㉡과 ㉢이 옳다.

보기별 해설

㉠ (X) ISO/IEC 27000 계열은 **정보보호 관리체계에 관한 국제표준군**이다. 암호화에 한정된 국내 표준이 아니다. 그 발전의 바탕이 된 영국 표준은 BS 7799이며, BSI는 이를 제정한 영국표준협회(British Standards Institution)의 이름이다.

㉡ (O) ISO/IEC 27000 계열은 정보보호 관리체계의 수립·운영·개선과 보안 관리규범을 지원한다. 이 문항은 27000을 표준군의 뜻으로 사용한다. 엄밀히 구분하면 개별 표준 ISO/IEC 27000은 개요와 용어, 27001은 관리체계 요구사항, 27002는 정보보호 통제에 관한 지침을 다룬다.

㉢ (O) ISO/IEC 27001:2013의 부속서 A에 제시된 정보보호 통제는 **14개 영역, 114개 항목**으로 구성된다. 문항이 지정한 2013판을 기준으로 판단해야 하며, 이를 표준 본문 전체의 장 수로 이해해서는 안 된다.

㉣ (X) 오렌지 북은 미국 국방부의 신뢰 컴퓨터 시스템 평가기준(TCSEC)을 가리킨다. ISO/IEC 27000 계열은 국제적인 정보보호 관리체계 표준군이므로, 유럽 회원국의 공통 조례나 오렌지 북이라는 설명은 틀리다.

옳은 보기는 ㉡과 ㉢이므로 정답은 ③이다.

NoteBase

문 6. 국제 공통평가 기준(CC, Common Criteria)의 등급별 보안 수준에 관한 설명으로 가장 적절한 것은?

① EAL1 : 구조시험으로 체계적인 설계·시험 및 검토 단계로 독립적인 취약점 분석

② EAL3 : 방법론적 시험 및 검사로 완전한 범위의 보안 기능 시험

③ EAL5 : 정형화된 설계 검증 및 시험 단계로 포괄적 분석

④ EAL7 : 준정형 검증된 설계 및 시험으로 독립적인 취약점 검사

정답 2번

간단한 해설

EAL3은 **방법론적 시험 및 검사** 수준으로, 보안 기능에 대한 시험 범위와 설계 근거를 확인한다.

선지별 해설

EAL은 보안 기능을 얼마나 엄격하게 평가해 신뢰를 확보했는지를 나타내는 평가보증등급이다.

① X: EAL1은 문서에 제시된 기능의 동작을 확인하는 **기능 시험** 수준이다. 구조 시험은 EAL2, 체계적인 설계·시험·검토는 EAL4의 명칭이므로 선지는 서로 다른 등급을 섞었다.

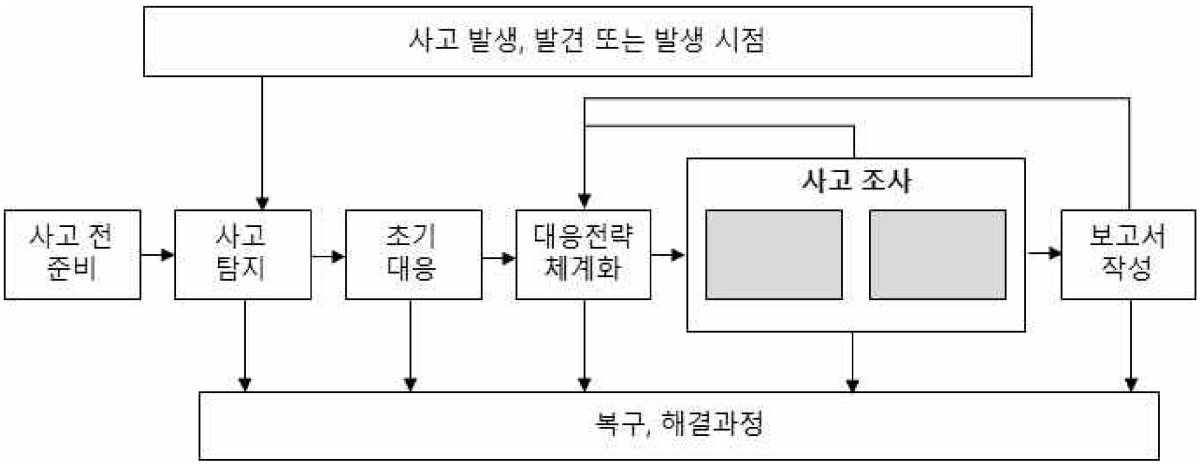
② O: EAL3은 **방법론적 시험 및 검사** 수준이다. 기능 명세와 설계를 토대로 시험하고, 명세의 모든 보안 기능 인터페이스가 시험에 포함되는지 분석한다. 여기서 완전한 범위란 시험 대상의 범위를 말하며, 가능한 모든 입력값을 전수 시험한다는 뜻은 아니다.

③ X: EAL5는 **준정형화된 설계 및 시험** 수준이다. 준정형 설계 기술을 요구하지만, 선지의 정형 설계 검증·시험과 포괄적 분석은 EAL7에 연결해야 한다.

④ X: EAL7은 **정형적으로 검증된 설계 및 시험** 수준으로, 정형 표현과 대응 관계를 이용한 분석을 강화한다. 준정형적으로 검증된 설계 및 시험은 EAL6의 명칭이며, 독립적 취약점 검사를 한다는 사실만으로 이 두 등급을 구별할 수는 없다.

NoteBase

문 7. 한국인터넷진흥원의 침해사고 대응 절차 7단계 그림에서 사고조사 단계에 관한 설명으로 가장 적절하지 않은 것은?



① 데이터 수집 및 분석을 통해 사고조사를 수행하여 언제, 누가, 어떻게 사고가 일어났는지, 피해확산 및 사고 재발을 어떻게 방지할 것인지 결정하는 단계이다.

② 호스트 기반과 네트워크 기반 증거로 나누어 사고를 조사하며 조사과정은 데이터 수집과 데이터 분석(포렌식 분석) 단계로 나뉜다.

③ 호스트 기반 증거 수집은 휘발성 데이터가 사라지기 전에 수집하는 것이 중요하며 그 후에 포렌식 이미징 작업을 수행한다. 휘발성 증거는 사고 의도를 이해하고자 할 때 매우 중요한 정보와 시스템의 스냅샷(snap-shot)을 제공한다.

④ 사고조사 증거 및 결과를 참고해 소송이 필요한 사항인지를 결정하여 사고조사 과정에 수사기관 공조 여부를 판단한다.

정답 4번

간단한 해설

사고 조사의 중심은 증거 수집과 분석이다. 소송 필요성과 수사기관 공조 여부를 정하는 것은 **대응전략 체계화**의 주된 역할이므로 ④가 가장 적절하지 않다.

NoteBase

선지별 해설

그림의 주된 흐름은 사고 전 준비 → 사고 탐지 → 초기 대응 → 대응전략 체계화 → 사고 조사 → 보고서 작성이다. 아래의 복구·해결 과정은 여러 단계와 연결되고, 조사·보고 결과에서 대응전략으로 돌아가는 화살표도 있다. 따라서 단계의 역할은 구분하되 실제 대응은 결과에 따라 조정될 수 있다.

① O: 사고 조사는 **증거를 수집·분석하여 사고의 실체를 규명**하는 단계이다. 발생 시점, 관련 행위자, 침입 방법과 피해 범위를 파악하고, 그 결과를 피해 확산 차단과 재발 방지에 활용한다. 단순히 이상 징후를 발견하는 사고 탐지와는 조사 깊이가 다르다.

② O: 사고 조사에서는 시스템 내부의 로그·메모리·파일 등 **호스트 기반 증거**와 통신 기록·보안장비 로그 등 **네트워크 기반 증거**를 함께 살핀다. 데이터를 확보하는 수집과 확보된 자료의 의미·상관관계를 밝히는 분석으로 구분한다. 그림의 사고 조사 내부 두 구획은 이러한 수집·분석 기능에 대응한다.

③ O: 메모리, 실행 중인 프로세스, 현재 네트워크 연결 상태 등은 종료나 시간 경과로 사라질 수 있으므로 **휘발성 정보를 먼저 보존**하는 것이 중요하다. 이어서 디스크 등을 포렌식 이미지로 확보해 분석한다. 휘발성 자료는 당시 시스템 상태의 단면을 보여 주므로 공격 행위와 의도를 추론하는 단서가 되지만, 그 자체만으로 의도가 확정되는 것은 아니다.

④ X: 이 절차에서 소송 필요성과 수사기관 공조 여부를 정하는 주된 단계는 **대응전략 체계화**이다. 초기 대응에서 확보한 조사 결과를 바탕으로 대응 방침을 정하고 관리자의 승인을 받아 이후 사고 조사의 방향을 마련한다. 사고 조사는 그 방침에 따라 증거를 수집·분석하는 단계이다. 조사 중 새 사실이 나오면 전략을 재검토할 수 있으므로, 공조 판단이 이후에는 절대로 불가능하다는 뜻은 아니다.

따라서 대응전략 체계화의 역할을 사고 조사 단계의 설명으로 제시한 ④가 가장 적절하지 않다.

NoteBase

문 9. 요구사항에 따른 위험분류에 관한 설명으로 가장 적절하지 않은 것은?

① 베이스라인 접근법은 모든 시스템에 대해 표준화된 보호대책 목록을 체크리스트 형태로 제공한다.

② 비정형 접근법은 정형화되고 구조화된 프로세스를 사용하는 대신 분석가 개인의 지식 및 경험을 활용한다.

③ 상세 위험분석은 경험자의 지식을 토대로 위험분석을 수행하기 때문에 빠르고 분석 비용이 상대적으로 저렴하다.

④ 복합 접근법은 고위험 영역에 대해 상세 위험분석을 수행하고 그 외의 다른 영역은 베이스라인 접근법을 사용한다.

정답 3번

간단한 해설

상세 위험분석은 자산·위협·취약점을 체계적으로 조사하므로 **시간과 비용이 많이 든다**. 경험을 활용한 신속하고 비교적 저렴한 분석은 비정형 접근법의 특징이므로 ③이 부적절하다.

선지별 해설

① O: 베이스라인 접근법은 표준 보호대책 목록을 바탕으로 시스템의 기본 보호 수준을 점검한다. 체크리스트로 공통 대책의 적용 여부를 확인하므로 **표준화된 기준을 여러 시스템에 적용**하기 쉽다. 다만 공통 목록이 모든 시스템의 고유한 위험까지 충분히 해결한다는 뜻은 아니며, 적용 대상과 보호 수준의 적합성을 확인해야 한다.

② O: 비정형 접근법은 정해진 분석 절차에 의존하기보다 **분석가의 지식과 경험**을 활용한다. 비교적 신속하게 판단할 수 있지만, 분석가가 경험하지 못한 위험을 놓치거나 주관에 따라 결과가 달라질 수 있다.

③ X: 상세 위험분석은 자산의 가치, 위협, 취약점 등을 **구조화된 절차로 깊이 있게 분석**하여 위험과 보호대책을 정하는 방식이다. 많은 자료와 전문성이 필요해 보통 시간·노력·비용 부담이 크다. 경험을 활용하여 비교적 빠르고 저렴하게 분석한다는 특징은 비정형 접근법에 가깝다. 상세 분석에도 전문가의 지식은 필요하므로, 전문가가 참여한다는 사실만으로 두 방법을 구별해서는 안 된다.

④ O: 복합 접근법은 먼저 위험과 업무 중요도를 개괄적으로 살펴 **고위험·핵심 영역에 상세 분석을 집중**하고, 나머지 영역에는 베이스라인을 적용한다. 모든 시스템을 같은 깊이로 분석하지 않고 필요한 곳에 분석 자원을 배분하는 방식이다.

따라서 비정형 접근법의 신속성·상대적 저비용을 상세 위험분석의 특징으로 설명한 ③이 가장 적절하지 않다.

NoteBase

문 10. 위험관리 5단계 과정에 관한 설명으로 가장 적절하지 않은 것은?

① 위험관리 전략 및 계획 수립 단계 : 자산, 위협, 취약성, 기존 보호 대책 등을 분석하여 위험의 종류와 규모를 결정한다.

② 위험평가 단계 : 위험분석 결과를 이용하여 최종적으로 위험도를 평가하고, 조직에서 수용 가능한 목표 위험수준을 정하여 이를 기준으로 위험의 대응 여부와 우선순위를 결정한다.

③ 정보보호 대책 선정 단계 : 위험평가 결과를 토대로 수용 가능한 목표 위험수준을 초과하는 위험을 수용 가능한 수준으로 감소시키기 위하여 위험처리 전략을 설정하고 적절한 통제사항을 선택한다.

④ 정보보호 계획 수립 단계 : 선정한 보호 대책을 구현하기 위한 이행계획을 수립하는 단계로 정보보호 대책 및 구현의 우선순위, 일정계획, 예산, 책임, 운영계획 등을 포함한 이행계획을 수립한다.

정답 1번

간단한 해설

자산·위협·취약성과 기존 보호 대책을 분석하여 위험의 종류와 규모를 파악하는 일은 **위험분석**에 해당한다. 전략 및 계획 수립은 그 분석을 수행할 범위·방법·역할 등을 정하는 앞 단계이다.

선지별 해설

① X: 자산·위협·취약성과 기존 보호 대책을 조사하여 위험의 종류와 규모를 파악하는 것은 **위험분석 단계**이다. 위험관리 전략 및 계획 수립 단계에서는 조직의 목표와 요구사항에 맞춰 위험관리 범위, 방법, 담당 조직과 역할, 수행계획 등을 정한다. 따라서 선지의 단계 이름을 '위험분석 단계'로 고쳐야 한다.

② O: 위험평가 단계에서는 **분석한 위험을 수용 기준과 비교**한다. 조직이 감수할 수 있는 목표 위험수준을 기준으로 추가 대응이 필요한 위험과 처리 우선순위를 결정한다. 위험의 종류·규모를 파악하는 분석과, 그 결과를 바탕으로 대응 필요성을 판단하는 평가를 구별해야 한다.

③ O: 정보보호 대책 선정 단계는 위험평가 결과에 따라 **위험처리 전략과 통제사항**을 선택하는 과정이다. 목표 위험수준을 초과한 위험을 수용 가능한 수준으로 낮추도록 적절한 관리적·물리적·기술적 보호 대책을 선정한다.

④ O: 정보보호 계획 수립 단계에서는 선정한 대책을 **누가, 언제, 어떤 자원으로 구현할지** 구체화한다. 구현 우선순위, 일정, 예산, 담당 책임과 운영 방안을 이행계획에 담으므로, 대책 자체를 고르는 선정 단계와 구별된다.

NoteBase

문 11. 「지능정보화 기본법」에서 정의하고 있는 지능정보기술에 관한 내용으로 가장 적절하지 않은 것은?

① 부호, 문자를 제외한 모든 데이터를 전자적으로 처리하는 기술

② 전자적 방법으로 학습·추론·판단 등을 구현하는 기술

③ 물건 상호 간 또는 사람과 물건 사이에 데이터를 처리하거나 물건을 이용·제어 또는 관리할 수 있도록 하는 기술

④ 무선 또는 유·무선이 결합된 초연결지능정보통신기반 기술

정답 1번

①

데이터에는 **부호와 문자도 포함**된다. 이러한 데이터를 전자적으로 수집·분석·가공 등 처리하는 기술은 지능정보기술이다.

지능정보화 기본법 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.
4. "지능정보기술" 이란 다음 각 목의 어느 하나에 해당하는 기술 또는 그 결합 및 활용 기술을 말한다.
나. 데이터(부호, 문자, 음성, 음향 및 영상 등으로 표현된 모든 종류의 자료 또는 지식을 말한다)를 전자적 방법으로 수집 · 분석 · 가공 등 처리하는 기술

②

전자적 방법으로 **학습·추론·판단 등을 구현하는 기술**은 지능정보기술에 포함된다.

지능정보화 기본법 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.
4. "지능정보기술" 이란 다음 각 목의 어느 하나에 해당하는 기술 또는 그 결합 및 활용 기술을 말한다.
가. 전자적 방법으로 학습 · 추론 · 판단 등을 구현하는 기술

③

물건 상호 간 또는 사람과 물건 사이의 **데이터 처리나 물건의 이용·제어·관리를 가능하게 하는 기술**은 지능정보기술에 포함된다.

지능정보화 기본법 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.
4. "지능정보기술" 이란 다음 각 목의 어느 하나에 해당하는 기술 또는 그 결합 및 활용 기술을 말한다.
다. 물건 상호간 또는 사람과 물건 사이에 데이터를 처리하거나 물건을 이용 · 제어 또는 관리할 수 있도록 하는 기술

NoteBase

④

무선 또는 유·무선이 결합된 초연결지능정보통신기반 기술은 지능정보기술에 포함된다.

지능정보화 기본법 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.
4. "지능정보기술" 이란 다음 각 목의 어느 하나에 해당하는 기술 또는 그 결합 및 활용 기술을 말한다.
마. 무선 또는 유 · 무선이 결합된 초연결지능정보통신기반 기술

NoteBase

문 12. 다음 빈칸에 가장 적절한 것은?

( )은/는 개인정보를 활용하는 새로운 정보시스템 도입 및 기존 정보시스템의 변경 시, 기업의 고객은 물론 고객의 프라이버시에 미칠 영향에 대하여 미리 조사, 분석, 평가하는 체계적인 절차이다.

① 정보보호관리체계인증(ISMS)
② 하트블리드(heartbleed)
③ 개인정보영향평가(PIA)
④ 상호인정협정(CCRA)

정답 3번

간단한 해설

시스템 도입·변경이 프라이버시에 미칠 영향을 **사전에 조사·분석·평가**하는 절차는 개인정보영향평가(PIA)이다.

빈칸별 해설

빈칸: 개인정보영향평가(PIA). 개인정보를 처리하는 시스템을 새로 도입하거나 변경할 때, **프라이버시에 미칠 영향을 사전에 평가**하여 침해 위험과 개선 방안을 찾는 절차이다. 지문의 '미리 조사, 분석, 평가'가 이를 가리키는 핵심 단서다.

ISMS는 조직의 정보보호 관리체계가 인증기준에 적합한지를 평가하여 인증하는 제도이다. 특정 시스템의 도입·변경에 따른 개인정보 영향을 사전에 평가하는 PIA와 평가의 초점이 다르다.

하트블리드는 OpenSSL의 하트비트 처리 과정에서 경계 검사가 부족하여 메모리 정보가 노출되는 취약점이다. 개인정보에 미칠 영향을 평가하는 절차의 이름이 아니다.

CCRA는 공통평가기준(CC)에 따른 보안 인증서를 참여국 사이에서 상호 인정하기 위한 협정이다. 개인정보 침해 위험을 사전에 분석하는 PIA와 구별한다.

따라서 빈칸에 들어갈 말은 개인정보영향평가(PIA)이므로 정답은 ③이다.

NoteBase

문 13. 「개인정보 보호법」 제23조(민감정보의 처리 제한)에 관한 설명으로 가장 적절한 것은?

① 민감정보란 개인에 관한 정보로 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보를 의미한다.

② 민감정보란 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보를 의미한다.

③ 개인정보처리자는 정보주체의 개인정보 수집 및 이용 동의를 받은 경우, 민감정보는 별도 동의 없이 사용할 수 있다.

④ 개인정보처리자가 민감정보를 처리하는 경우, 그 민감정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 기술적 조치만 취하면 제3자에게 전달할 수 있다.

정답 2번

①

성명·주민등록번호·영상 등으로 살아 있는 개인을 알아볼 수 있는 정보는 **개인정보에 해당한다**. 민감정보는 그중 사상·신념·건강·성생활 등 **사생활 침해 우려가 큰 법정 범주의 정보**를 말한다.

개인정보 보호법 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다. <개정 2014.3.24, 2020.2.4, 2023.3.14>
1. "개인정보"란 살아 있는 개인에 관한 정보로서 다음 각 목의 어느 하나에 해당하는 정보를 말한다.
가. 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보

개인정보 보호법 제23조(민감정보의 처리 제한)
①개인정보처리자는 사상 · 신념, 노동조합 · 정당의 가입 · 탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보(이하 "민감정보"라 한다)를 처리하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다. <개정 2016.3.29>
1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우
2. 법령에서 민감정보의 처리를 요구하거나 허용하는 경우

NoteBase

②

민감정보는 **사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보**와 그 밖에 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보이다.

개인정보 보호법 제23조(민감정보의 처리 제한)
①개인정보처리자는 사상 · 신념, 노동조합 · 정당의 가입 · 탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보(이하 "민감정보"라 한다)를 처리하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다. <개정 2016.3.29>
1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우
2. 법령에서 민감정보의 처리를 요구하거나 허용하는 경우

③

일반적인 개인정보 수집·이용 동의만으로 민감정보를 처리할 수는 없으며, **다른 개인정보 처리 동의와 별도로 동의**를 받아야 한다. 다만 **법령에서 민감정보 처리를 요구하거나 허용하는 경우**에는 별도 동의 없이 처리할 수 있다.

개인정보 보호법 제23조(민감정보의 처리 제한)
①개인정보처리자는 사상 · 신념, 노동조합 · 정당의 가입 · 탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보(이하 "민감정보"라 한다)를 처리하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다. <개정 2016.3.29>
1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우
2. 법령에서 민감정보의 처리를 요구하거나 허용하는 경우

NoteBase

④

민감정보에는 **기술적·관리적 및 물리적 안전조치**가 필요하다. 이러한 조치를 취했다는 사정만으로 제3자 제공이 허용되는 것은 아니며, **별도 동의나 법령상 허용 등 민감정보 처리의 적법한 근거**도 갖추어야 한다.

개인정보 보호법 제23조(민감정보의 처리 제한)
①개인정보처리자는 사상 · 신념, 노동조합 · 정당의 가입 · 탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보(이하 "민감정보"라 한다)를 처리하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다. <개정 2016.3.29>
1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우
2. 법령에서 민감정보의 처리를 요구하거나 허용하는 경우
② 개인정보처리자가 제1항 각 호에 따라 민감정보를 처리하는 경우에는 그 민감정보가 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손(이하 "유출등"이라 한다)이 되지 아니하도록 제29조에 따른 안전성 확보에 필요한 조치를 하여야 한다. <신설 2016.3.29, 2026.3.10>

개인정보 보호법 제29조(안전조치의무) 개인정보처리자는 개인정보가 유출등이 되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적 · 관리적 및 물리적 조치를 하여야 한다. <개정 2015.7.24, 2026.3.10>

NoteBase

문 14. 「개인정보의 안전성 보호조치 기준」 제5조(접근권한의 관리)에 관한 설명으로 가장 적절한 것은?

① 개인정보처리자는 개인정보처리 시스템에 대한 접근권한을 업무수행에 필요한 최대한의 범위로 업무 담당자마다 동일하게 부여하여야 한다.

② 개인정보처리자는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우, 지체없이 개인정보처리 시스템의 접근권한을 변경 또는 말소하여야 한다.

③ 개인정보처리자는 권한 부여, 변경 또는 말소에 대한 내역을 기록하고 그 기록을 최소 7년간 보관하여야 한다.

④ 개인정보처리자는 개인정보처리 시스템에 접속할 수 있는 사용자 계정을 발급하는 경우, 사용자 그룹에 발급된 계정을 공유하고 그룹 내에서만 사용하도록 권한을 설정한다.

정답 2번

①

개인정보처리시스템의 접근권한은 **업무 수행에 필요한 최소한의 범위로 차등 부여**하여야 한다.

개인정보의 안전성 확보조치 기준 제5조(접근 권한의 관리)
① 개인정보처리자는 개인정보처리시스템에 대한 접근 권한을 업무 수행에 필요한 최소한의 범위로 차등 부여하여야 한다.

②

전보·퇴직 등으로 개인정보취급자가 바뀌면 개인정보처리자는 **지체 없이 접근권한을 변경하거나 말소**하여야 한다.

개인정보의 안전성 확보조치 기준 제5조(접근 권한의 관리)
② 개인정보처리자는 개인정보취급자 또는 개인정보취급자의 업무가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근 권한을 변경 또는 말소하여야 한다.

③

접근권한의 부여·변경·말소 내역은 기록하여 **최소 3년간 보관**하여야 한다. 7년이 아니다.

개인정보의 안전성 확보조치 기준 제5조(접근 권한의 관리)
③ 개인정보처리자는 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.

NoteBase

④

정당한 사유가 없는 한 개인정보취급자별로 계정을 발급하고 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

개인정보의 안전성 확보조치 기준 제5조(접근 권한의 관리)
④ 개인정보처리자는 개인정보처리시스템에 접근할 수 있는 계정을 발급하는 경우 정당한 사유가 없는 한 개인정보취급자 별로 계정을 발급하고 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

NoteBase

문 15. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조(정보보호 관리체계의 인증)에 관한 설명으로 가장 적절한 것은?

① 정보보호 최고책임자는 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계를 수립·운영하고 있는 자에 관하여 인증을 할 수 있다.

② 주요정보통신서비스 제공자 중 연간 매출액 또는 세입 등이 1,500억 원 이상이거나 정보통신 서비스 부문 전년도 매출액이 10억 원 이상 또는 7개월간의 일일 평균 이용자 수가 100만 명 이상에 해당하는 자는 인증을 받아야 한다.

③ 한국인터넷진흥원, 정보보호관리체계 인증기관 및 정보보호관리체계 심사기관은 정보보호 관리체계의 실효성 제고를 위하여 연 2회 이상 사후관리를 실시하고 그 결과를 경찰청장에게 통보하여야 한다.

④ 정보보호 관리체계 인증의 유효기간은 3년으로 하고 정보보호 관리등급을 받은 경우 그 유효기간 동안 인증을 받은 것으로 본다.

정답 4번

①

정보보호 관리체계의 인증 권한자는 정보보호 최고책임자가 아니라 **과학기술정보통신부장관**이다.

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

NoteBase

②

매출액·이용자 수 기준은 **정보통신서비스 부문 전년도 매출액 100억 원 이상 또는 전년도 일일평균 이용자 수 100만 명 이상**이며, 이 두 기준에서는 금융회사를 제외한다. **주요정보통신서비스 제공자는 이 수치 기준과 별도로 인증 의무**를 진다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제47조(정보보호 관리체계의 인증)
② 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자로서 다음 각 호의 어느 하나에 해당하는 자는 제1항에 따른 인증을 받아야 한다. <신설 2012.2.17, 2015.12.1, 2018.12.24, 2020.6.9, 2024.1.23, 2026.3.31>
1. 주요정보통신서비스 제공자
3. 전년도 매출액 또는 세입 등이 1,500억원 이상이거나 정보통신서비스 부문 전년도 매출액이 100억원 이상 또는 전년도 일일평균 이용자수 100만명 이상으로서, 대통령령으로 정하는 기준에 해당하는 자

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제49조(정보보호 관리체계 인증 대상자의 범위)
② 법 제47조제2항제3호에서 "대통령령으로 정하는 기준에 해당하는 자"란 다음 각 호의 어느 하나에 해당하는 자를 말한다. <개정 2016.5.31, 2024.7.23>
2. 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 자. 다만, 「전자금융거래법」 제2조제3호에 따른 금융회사는 제외한다.
3. 전년도 일일평균 이용자 수가 100만명 이상인 자. 다만, 「전자금융거래법」 제2조제3호에 따른 금융회사는 제외한다.

③

한국인터넷진흥원, 정보보호 관리체계 인증기관 및 심사기관은 **연 1회 이상** 사후관리를 실시하고, 그 결과를 **과학기술정보통신부장관**에게 통보하여야 한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제47조(정보보호 관리체계의 인증)
⑧ 한국인터넷진흥원, 정보보호 관리체계 인증기관 및 정보보호 관리체계 심사기관은 정보보호 관리체계의 실효성 제고를 위하여 연 1회 이상 사후관리를 실시하고 그 결과를 과학기술정보통신부장관에게 통보하여야 한다. 이 경우 사후관리는 현장심사와 서면심사의 방법을 병행하여 실시한다. <신설 2012.2.17, 2013.3.23, 2015.12.1, 2017.7.26, 2026.3.31>

NoteBase

④

정보보호 관리체계 인증은 **3년간 유효**하며, **정보보호 관리등급을 받으면 그 등급의 유효기간 동안 인증을 받은 것으로 본다**.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제47조(정보보호 관리체계의 인증)
⑤ 제1항에 따른 정보보호 관리체계 인증의 유효기간은 3년으로 한다. 다만, 제47조의5제1항에 따라 정보보호 관리등급을 받은 경우 그 유효기간 동안 제1항의 인증을 받은 것으로 본다. <신설 2012.2.17, 2015.12.1>

NoteBase

문 16. 「개인정보 보호법」 제16조(개인정보의 수집 제한)에 관한 설명으로 가장 적절하지 않은 것은?

① 개인정보처리자는 개인정보를 수집하는 경우에 그 목적에 필요한 최소한의 개인정보를 수집하여야 한다. 이 경우 최소한의 개인정보 수집이라는 입증책임은 개인정보처리자가 부담한다.

② 개인정보처리자는 그 목적에 필요한 최소한의 범위를 벗어난 개인정보는 선택정보로서 필수정보 동의 시에 일괄 동의를 얻어야 하며 정보주체가 동의하여도 수집하지 못한다.

③ 개인정보처리자는 정보주체의 동의를 받아 개인정보를 수집하는 경우, 필요한 최소한의 정보 외의 개인정보 수집에는 동의하지 아니할 수 있다는 사실을 구체적으로 알려야 한다.

④ 개인정보처리자는 정보주체가 필요한 최소한의 정보 외의 개인정보 수집에 동의하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 아니된다.

정답 2번

①

개인정보는 **수집 목적에 필요한 최소한의 범위**로 수집하여야 하며, 그 범위가 최소한이라는 **입증책임은 개인정보처리자**가 부담한다.

개인정보 보호법 제16조(개인정보의 수집 제한)
① 개인정보처리자는 제15조제1항 각 호의 어느 하나에 해당하여 개인정보를 수집하는 경우에는 그 목적에 필요한 최소한의 개인정보를 수집하여야 한다. 이 경우 최소한의 개인정보 수집이라는 입증책임은 개인정보처리자가 부담한다.

NoteBase

②

선택정보는 필수정보와 **동의 사항을 구분**하여 동의를 받아야 한다. 필요한 최소한의 정보 외의 개인정보는 **수집에 동의하지 않을 수 있음을 구체적으로 알리고, 정보주체가 동의하면 수집할 수 있다**.

개인정보 보호법 제16조(개인정보의 수집 제한)
② 개인정보처리자는 정보주체의 동의를 받아 개인정보를 수집하는 경우 필요한 최소한의 정보 외의 개인정보 수집에는 동의하지 아니할 수 있다는 사실을 구체적으로 알리고 개인정보를 수집하여야 한다. <신설 2013.8.6>

개인정보 보호법 제22조(동의를 받는 방법)
① 개인정보처리자는 이 법에 따른 개인정보의 처리에 대하여 정보주체(제22조의2제1항에 따른 법정대리인을 포함한다. 이하 이 조에서 같다)의 동의를 받을 때에는 각각의 동의 사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 알리고 동의를 받아야 한다. 이 경우 다음 각 호의 경우에는 동의 사항을 구분하여 각각 동의를 받아야 한다. <개정 2017.4.18, 2023.3.14>
1. 제15조제1항제1호에 따라 동의를 받는 경우
2. 제17조제1항제1호에 따라 동의를 받는 경우
3. 제18조제2항제1호에 따라 동의를 받는 경우
4. 제19조제1호에 따라 동의를 받는 경우
5. 제23조제1항제1호에 따라 동의를 받는 경우
6. 제24조제1항제1호에 따라 동의를 받는 경우
7. 재화나 서비스를 홍보하거나 판매를 권유하기 위하여 개인정보의 처리에 대한 동의를 받으려는 경우
8. 그 밖에 정보주체를 보호하기 위하여 동의 사항을 구분하여 동의를 받아야 할 필요가 있는 경우로서 대통령령으로 정하는 경우

③

동의를 받아 개인정보를 수집할 때에는 **필요한 최소한의 정보 외의 개인정보 수집에는 동의하지 않을 수 있다는 사실**을 구체적으로 알려야 한다.

개인정보 보호법 제16조(개인정보의 수집 제한)
② 개인정보처리자는 정보주체의 동의를 받아 개인정보를 수집하는 경우 필요한 최소한의 정보 외의 개인정보 수집에는 동의하지 아니할 수 있다는 사실을 구체적으로 알리고 개인정보를 수집하여야 한다. <신설 2013.8.6>

NoteBase

④

정보주체가 **필요한 최소한의 정보 외의 개인정보 수집에 동의하지 않았다는 이유로 재화나 서비스 제공을 거부할 수 없다**.

개인정보 보호법 제16조(개인정보의 수집 제한)
③ 개인정보처리자는 정보주체가 필요한 최소한의 정보 외의 개인정보 수집에 동의하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 아니 된다. <개정 2013.8.6>

NoteBase

문 17. 「개인정보의 기술적·관리적 보호조치 기준」 제6조(개인정보의 암호화)에 관한 설명으로 가장 적절하지 않은 것은?

① 정보통신서비스 제공자는 비밀번호가 복호화되지 않도록 양방향 암호화 알고리즘(해시함수)을 사용하여 암호화한다. 이때 암호화한 해시값을 크래킹하기 위해 첨가값(salt), 반복횟수(iteration count) 등을 추가하도록 하는 것이 가능하다.

② 정보통신서비스 제공자는 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호, 신용카드번호, 계좌정보, 생체인식정보에 대해서는 안전한 알고리즘으로 암호화하여 저장한다.

③ 정보통신서비스 제공자는 정보통신망을 통해 이용자의 개인정보 및 인증정보를 송·수신할 때 안전한 보안서버 구축 등의 조치를 통해 이를 암호화해야 한다.

④ 정보통신서비스 제공자는 이용자의 개인정보를 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때 이를 암호화해야 한다.

정답 1번

①

비밀번호는 복호화되지 않도록 **일방향 암호화하여 저장**해야 한다. 해시함수는 양방향 암호화가 아니며, 솔트와 반복횟수는 **해시값의 크래킹을 어렵게 하기 위한** 수단이다.

개인정보의 안전성 확보조치 기준 제7조(개인정보의 암호화)
① 개인정보처리자는 비밀번호, 생체인식정보 등 인증정보를 저장 또는 정보통신망을 통하여 송 · 수신하는 경우에 이를 안전한 암호 알고리즘으로 암호화하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

②

이용자의 주민등록번호·여권번호·운전면허번호·외국인등록번호·신용카드번호·계좌번호·생체인식정보는 **안전한 암호 알고리즘으로 암호화하여 저장**해야 한다. 선지의 계좌정보는 암호화 대상 항목을 열거한 문맥에서 **계좌번호**를 가리킨다.

개인정보의 안전성 확보조치 기준 제7조(개인정보의 암호화)
② 개인정보처리자는 다음 각 호의 해당하는 이용자의 개인정보에 대해서는 안전한 암호 알고리즘으로 암호화하여 저장하여야 한다. 1. 주민등록번호 2. 여권번호 3. 운전면허번호 4. 외국인등록번호 5. 신용카드번호 6. 계좌번호 7. 생체인식정보

NoteBase

③

보안서버로 이용자와 개인정보를 주고받는 **인터넷망 전송 구간은 안전한 암호 알고리즘으로 암호화**해야 한다. 비밀번호·생체인식정보 등 **인증정보는 정보통신망 송수신 시 암호화**해야 하며, 보안서버 구축은 이러한 전송 암호화를 위한 조치이다.

개인정보의 안전성 확보조치 기준 제7조(개인정보의 암호화) ① 개인정보처리자는 비밀번호, 생체인식정보 등 인증정보를 저장 또는 정보통신망을 통하여 송 · 수신하는 경우에 이를 안전한 암호 알고리즘으로 암호화하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.
④ 개인정보처리자는 개인정보를 정보통신망을 통하여 인터넷망 구간으로 송 · 수신하는 경우에는 이를 안전한 암호 알고리즘으로 암호화하여야 한다.

④

이용자의 개인정보를 개인정보취급자의 컴퓨터·모바일 기기·보조저장매체 등에 저장할 때에는 **안전한 암호 알고리즘으로 암호화한 후 저장**해야 한다.

개인정보의 안전성 확보조치 기준 제7조(개인정보의 암호화)
⑤ 개인정보처리자는 이용자의 개인정보 또는 이용자가 아닌 정보주체의 고유식별정보, 생체인식정보를 개인정보취급자의 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 안전한 암호 알고리즘을 사용하여 암호화한 후 저장하여야 한다.

NoteBase

문 18. 「정보통신기반 보호법」 제3조(정보통신기반보호위원회)에 관한 설명으로 가장 적절하지 않은 것은?

① 주요정보통신기반시설 보호에 관한 사항을 심의하기 위하여 국가정보원장 소속하에 정보통신기반보호위원회(위원회)를 둔다.

② 위원회의 위원은 위원장 1인을 포함한 25인 이내의 위원으로 구성한다.

③ 위원회의 위원장은 국무조정실장이 되고 위원회의 위원은 대통령령으로 정하는 중앙행정기관의 차관급 공무원과 위원장이 위촉하는 사람으로 한다.

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

정답 1번

①

주요정보통신기반시설 보호에 관한 사항을 심의하는 정보통신기반보호위원회는 **국무총리 소속**으로 둔다.
국가정보원장 소속이 아니다.

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>

②

정보통신기반보호위원회는 **위원장 1명을 포함하여 25명 이내**의 위원으로 구성한다.

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

③

위원장은 **국무조정실장**이다. 위원은 **대통령령으로 정하는 중앙행정기관의 차관급 공무원과 위원장이 위촉하는 사람**으로 한다.

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>

NoteBase

④

위원회의 효율적인 운영을 위해 **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 19. 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제25조(침해사고 등의 통지 등), 제26조(이용자 보호 등을 위한 정보 공개), 제27조(이용자 정보의 보호)에 관한 설명으로 가장 적절하지 않은 것은?

① 클라우드컴퓨팅 서비스 제공자는 이용자 정보가 유출되었을 때 사고 원인을 규명한 보고서가 작성·완료될 때까지 이용자에게 알리지 못한다.

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

③ 클라우드컴퓨팅 서비스 제공자는 법원의 제출명령이나 법관이 발부한 영장에 의하지 아니하고는 이용자의 동의 없이 이용자 정보를 제3자에게 제공할 수 없다.

④ 클라우드컴퓨팅 서비스 제공자는 사업을 종료하려는 경우에 이용자에게 사업종료 사실을 알리고 사업 종료일 전까지 이용자 정보를 반환해야 한다.

정답 1번

①

이용자 정보가 유출되면 사고 원인 보고서의 작성·완료를 기다리지 않고 **지체 없이 그 사실을 해당 이용자에게 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 **이용자 정보가 저장되는 국가의 명칭**을 알려 줄 것을 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.

NoteBase

③

법원의 제출명령이나 법관이 발부한 영장에 의한 경우가 아니면 이용자의 동의 없이 이용자 정보를 제3자에게 제공할 수 없다.

클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제27조(이용자 정보의 보호)
① 클라우드컴퓨팅서비스 제공자는 법원의 제출명령이나 법관이 발부한 영장에 의하지 아니하고는 이용자의 동의 없이 이용자 정보를 제3자에게 제공하거나 서비스 제공 목적 외의 용도로 이용할 수 없다.
클라우드컴퓨팅서비스 제공자로부터 이용자 정보를 제공받은 제3자도 또한 같다.

④

사업을 종료하려면 이용자에게 그 사실을 알리고 **사업 종료일 전까지 이용자 정보를 반환**하며 보유 정보를 파기하는 것이 원칙이다. 다만 사실상 반환이 불가능하면 정보를 파기하고, 이용자와 특별히 다르게 정한 계약이 있으면 그에 따른다.

클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제27조(이용자 정보의 보호)
④ 클라우드컴퓨팅서비스 제공자는 사업을 종료하려는 경우에는 그 이용자에게 사업 종료 사실을 알리고 사업 종료일 전까지 이용자 정보를 반환하여야 하며 클라우드컴퓨팅서비스 제공자가 보유하고 있는 이용자 정보를 파기하여야 한다. 다만, 이용자가 사업 종료일 전까지 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 20. 「위치정보의 보호 및 이용 등에 관한 법률」 제15조(위치정보의 수집 등의 금지)에 관한 설명으로 가장 적절하지 않은 것은?

① 누구든지 개인위치정보주체의 동의를 받을 경우, 개인위치정보의 수집·이용이 가능하다.

② 긴급구조기관의 긴급구조요청이 있는 경우에도 개인위치정보주체의 동의 없이는 개인위치정보의 수집·이용은 불가능하다.

③ 위치정보를 수집할 수 있는 장치가 부착된 물건을 판매하거나 대여·양도하는 자는 위치정보 수집장치가 부착된 사실을 구매하거나 대여·양도받는 자에게 알려야 한다.

④ 누구든지 타인의 정보통신기기를 복제하거나 정보를 도용하는 방법으로 개인위치정보사업자 및 위치기반서비스사업자를 속여 타인의 개인위치정보를 제공받아서는 아니된다.

정답 2번

①

개인위치정보는 **정보주체의 동의를 받아 수집·이용하는 것이 원칙**이다.

위치정보의 보호 및 이용 등에 관한 법률 제15조(위치정보의 수집 등의 금지)
①누구든지 개인위치정보주체의 동의를 받지 아니하고 해당 개인위치정보를 수집 · 이용 또는 제공하여서는 아니 된다.

②

긴급구조기관의 긴급구조요청은 **동의 없는 개인위치정보 수집·이용 금지의 예외**에 해당한다.

위치정보의 보호 및 이용 등에 관한 법률 제15조(위치정보의 수집 등의 금지)
①누구든지 개인위치정보주체의 동의를 받지 아니하고 해당 개인위치정보를 수집 · 이용 또는 제공하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다. <개정 2012.5.14, 2018.4.17>
1. 제29조제1항에 따른 긴급구조기관의 긴급구조요청 또는 같은 조 제7항에 따른 경보발송요청이 있는 경우

③

위치정보 수집장치가 붙여진 물건을 판매·대여·양도하는 자는 **장치가 붙여진 사실을 상대방에게 알려야** 한다.

위치정보의 보호 및 이용 등에 관한 법률 제15조(위치정보의 수집 등의 금지)
③위치정보를 수집할 수 있는 장치가 붙여진 물건을 판매하거나 대여 · 양도하는 자는 위치정보 수집장치가 붙여진 사실을 구매하거나 대여 · 양도받는 자에게 알려야 한다. <개정 2018.4.17, 2020.6.9>

NoteBase

④

정보통신기기를 복제하거나 정보를 도용하여 개인위치정보사업자나 위치기반서비스사업자를 속이고 **타인의 개인위치정보를 제공받는 행위는 금지**된다.

위치정보의 보호 및 이용 등에 관한 법률 제15조(위치정보의 수집 등의 금지)
②누구든지 타인의 정보통신기기를 복제하거나 정보를 도용하는 등의 방법으로 개인위치정보사업자 및 위치기반서비스사업자(이하 "개인위치정보사업자등"이라 한다)를 속여 타인의 개인위치정보를 제공받아서는 아니된다. <개정 2018.4.17>

NoteBase