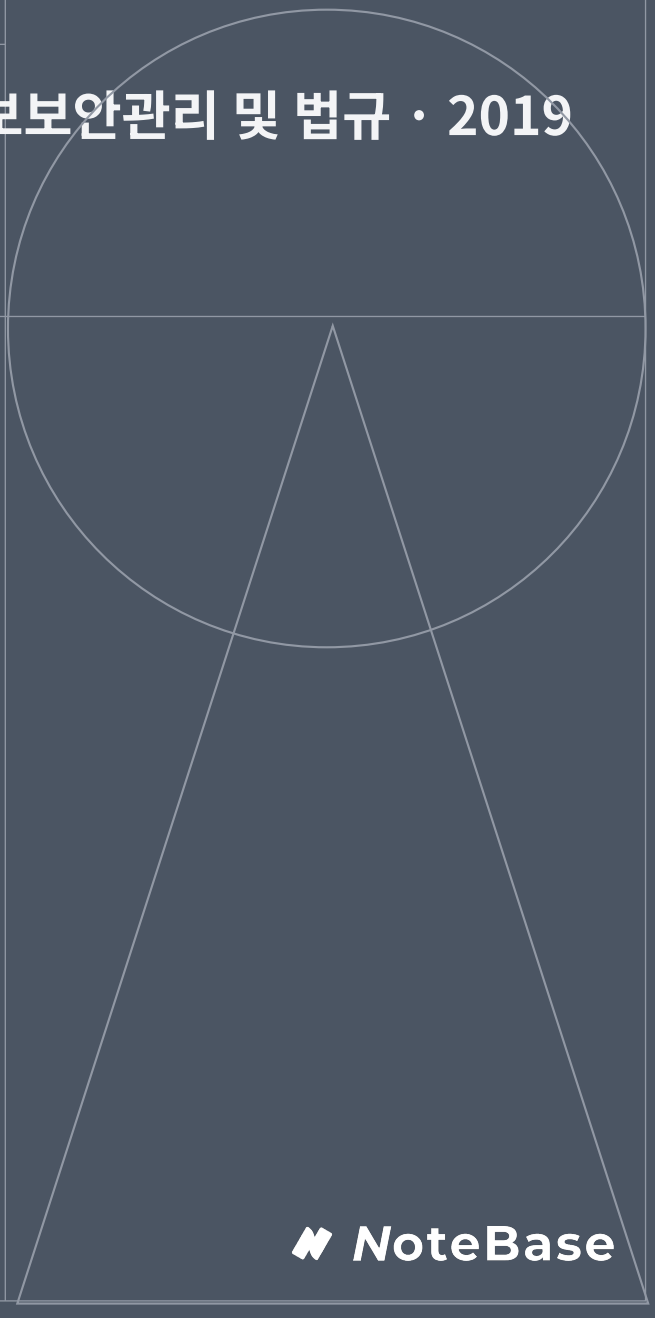
기출OX 해설집

공무원/경찰/경력채용 · 정보보안관리 및 법규 · 2019



NoteBase

기출OX 해설집

공무원/경찰/경력채용 · 정보보안관리 및 법규 · 2019

공무원/경찰/경력채용 · 정보보안관리 및 법규 · 2019

문 1. 사용자 인증 방식에 대한 설명으로 가장 적절하지 않은 것은?

① 지식기반 인증이란 사용자의 기억으로만 인증하는 방식으로 패스워드, PIN(Personal Identification Number) 등이 있으며, 패스워드 방식의 경우 전송 시 암호화하지 않으면 도청 가능성이 있다.

② 소유기반 인증은 보유하고 있는 물건으로 인증하는 방식으로 스마트카드(smart card)나 OTP(One Time Password) 등이 있으며, 스마트카드의 경우 마이크로프로세스 칩과 메모리를 내장한 일종의 소형 컴퓨터로 보안성이 요구된다.

③ 생체기반 인증은 불변의 특성을 지닌 생체적, 행동적 특징을 자동화된 수단으로 등록하여 인증하는 방식으로 존재 특징과 행동 특징으로 분류되고, 평가항목으로는 FRR(False Rejection Rate)과 FAR(False Acceptance Rate) 등이 있다.

④ 행동기반 인증은 개인의 고유한 행동적 특징을 사용해서 인증하는 방식으로 지문, 정맥, 안면, 홍채와 같은 정보를 추출하여 프로파일 정보를 구축하고, 이를 통해서 특징적이고 유일한 정보를 식별해서 인증에 사용한다.

정답 4번

간단한 해설

정답은 ④이다. 지문·정맥·안면·홍채는 **신체적 특징**이며, 행동기반 인증에는 서명 동작·키 입력 리듬·걸음걸이 등이 해당한다.

NoteBase

선지별 해설

① O: 지식기반 인증은 사용자가 **알고 있는 비밀정보**를 확인하는 방식으로 패스워드와 PIN이 대표적이다. 패스워드가 평문으로 전송되면 통신 내용을 엿본 사람이 이를 알아낼 수 있으므로 전송 구간의 기밀성을 보호해야 한다.

② O: 소유기반 인증은 스마트카드나 OTP 생성기처럼 **사용자가 보유·통제하는 인증 수단**을 확인한다. OTP는 생성기 또는 앱에 저장된 비밀값을 이용해 일회용 비밀번호를 생성한다. 스마트카드는 프로세서와 메모리를 갖추어 정보를 저장하고 연산할 수 있으므로 내부 키·데이터를 무단 추출이나 변조로부터 보호해야 한다.

③ O: 생체기반 인증은 등록된 신체적·행동적 특징과 새로 측정한 특징을 비교한다. 신체 구조에 관한 존재 특징과 행동 패턴으로 구분하며, FRR은 본인을 잘못 거부하는 비율, FAR은 타인을 본인으로 잘못 받아들이는 비율이다. 선지의 '불변'은 식별 특징의 **상대적 지속성**을 가리키는 취지이며, 실제 특징이나 측정값이 전혀 변하지 않는다는 뜻은 아니다. 노화·신체 상태와 측정 환경 등에 따라 인식 결과가 달라질 수 있다.

④ X: 지문·정맥·안면·홍채는 신체 구조에 근거한 **생리적·신체적 특징**이다. 행동기반 인증은 서명할 때의 움직임, 키 입력의 시간 간격, 걸음걸이처럼 행동 과정에서 나타나는 패턴을 이용한다. 따라서 신체적 특징의 예를 행동적 특징으로 분류한 부분을 교정해야 한다.

NoteBase

문 2. 커버로스(Kerberos) 인증에 대한 설명으로 가장 적절하지 않은 것은?

① 대칭키 암호화 기법에 바탕을 둔 티켓(ticket) 기반 인증 프로토콜이다.

② 아이디와 패스워드를 통해서만 인증한 후 사용자에 대한 서비스를 제공한다.

③ 인증 서버(Authentication Server)는 실질적인 인증을 수행한다.

④ 재전송 공격(replay attack)을 방지하기 위해 타임스탬프(timestamp) 정보가 필요하다.

정답 2번

간단한 해설

Kerberos는 각 서비스 이용 시 **티켓과 인증자로 신원을 증명**한다. 아이디와 패스워드만으로 인증·서비스 제공이 이루어진다고 한 ②가 적절하지 않다.

선지별 해설

① O: Kerberos는 신뢰하는 키 분배 센터(KDC)와 공유하는 비밀키를 토대로 인증 자격을 발급받는 **대칭키 기반의 티켓 인증** 체계이다. 티켓에는 사용자 신원과 세션키 등의 정보가 담기며, 티켓을 받는 서버가 가진 키로 보호된다.

② X: 아이디와 패스워드만 확인하고 곧바로 각 서비스를 이용하는 방식으로 한정할 수 없다. 일반적인 흐름은 최초 인증으로 티켓 발급 티켓(TGT)을 얻고, 이를 티켓 발급 서버(TGS)에 제시하여 서비스 티켓을 받은 뒤 **서비스 티켓과 인증자**로 서비스 서버에 자신을 증명하는 것이다. 초기 인증에도 공개키를 이용하는 PKINIT 확장이 있으므로 패스워드만 가능하다는 설명도 성립하지 않는다.

③ O: 인증 서버(AS)는 **최초 인증 교환**을 담당하고 일반적으로 TGT를 발급한다. 패스워드 기반 구성에서는 패스워드에서 유도한 비밀키가 인증에 쓰이며, 사전 인증을 요구하는 경우 AS가 그 증거를 확인한다. 이후 서비스 티켓을 발급하는 TGS, 티켓과 인증자를 검증하여 서비스를 제공하는 서비스 서버와 역할을 구별한다.

④ O: 인증자에 담긴 **타임스탬프의 신선도**를 확인하여 오래된 인증 요청의 재전송을 거부하므로 허용 범위 안의 시각 동기화가 필요하다. 다만 타임스탬프만으로 허용 시간 안의 중복 요청까지 막지는 못하므로, 통상 재전송 캐시에 이미 사용된 인증자를 기록하고 중복을 검사한다.

NoteBase

문 3. 다음의 접근 통제 모델(Access Control Model) 중 무결성을 보장하기 위한 모델을 모두 고른 것으로 가장 적절한 것은?

㉠ 벨라파듈라(Bell-LaPadula) 모델
㉡ 비바(Biba) 모델
㉢ 클락 윌슨(Clark-Wilson) 모델

① ㉠
② ㉡
③ ㉠㉡
④ ㉡㉢

정답 4번

간단한 해설

비바와 클락 윌슨 모델은 **무결성** 보호를 목적으로 한다. 벨라파듈라 모델은 정보의 무단 공개를 방지하는 **기밀성** 중심의 모델이다.

보기별 해설

㉠ 벨라파듈라(Bell-LaPadula): X. 정보의 무단 공개를 막는 **기밀성** 중심의 모델이다. 높은 보안 수준의 정보가 낮은 보안 수준으로 유출되지 않도록 정보 흐름을 통제하므로, 무결성 보장 모델로 분류하는 것은 적절하지 않다.

㉡ 비바(Biba): O. 주체와 객체에 무결성 수준을 부여하고, 신뢰도가 낮은 정보가 높은 무결성의 정보나 처리 과정에 영향을 미쳐 **오염시키는 것을 방지**한다. 따라서 정보의 무결성을 보호하는 모델에 해당한다.

㉢ 클락 윌슨(Clark-Wilson): O. 사용자가 보호 대상 데이터를 임의로 변경하지 못하고, 무결성을 유지하도록 검증된 **잘 형성된 트랜잭션**을 통해 변경하게 한다. 또한 **직무 분리**로 한 사람이 업무 전 과정을 임의로 처리하는 것을 제한하여 데이터의 일관성과 무결성을 보호한다.

따라서 무결성을 보장하기 위한 모델은 ㉡과 ㉢이며, 이를 모두 고른 것은 ④이다.

NoteBase

문 4. 위험분석방법에 대한 설명으로 가장 적절한 것은?

① 기준선 접근법(baseline approach): 경험자의 지식을 이용하여 위험분석을 수행하는 방법으로, 조직의 규모가 작은 경우에 적용할 수 있는 방법이다.

② 비형식적 접근법(informal approach): 고위험 영역을 식별하여 이 영역에 대해 상세위험분석을 수행하고, 다른 영역은 베이스라인 접근법을 이용하는 혼합형 방식을 적용한다.

③ 상세 위험분석 접근법(detailed risk analysis approach): 조직의 자산 및 보안 요구사항을 구체적으로 분석하여 적절한 대책을 수립할 수 있으나, 시간과 노력이 많이 소요된다.

④ 복합 접근법(combined approach): 모든 시스템에 표준화된 보안 대책을 체크리스트로 제공하여 분석의 비용과 시간이 절약되지만, 과보호 또는 부족한 보호가 될 가능성이 있다.

정답 3번

간단한 해설

상세 위험분석은 **자산·위협·취약점의 구체적인 분석**을 통해 상황에 맞는 보안 대책을 정한다. 분석의 깊이가 큰 만큼 시간과 노력이 많이 든다.

선지별 해설

① X: 경험자의 지식과 경험에 의존하는 방식은 **비형식적 접근법**이다. 자원이 제한된 소규모 조직에서 활용할 수 있지만, 조직 규모보다 분석 근거가 무엇인지가 구분 기준이다. 기준선 접근법은 표준화된 보안 대책을 공통 기준으로 적용하는 방식이다.

② X: 고위험 영역에는 상세 위험분석을, 나머지 영역에는 기준선 접근법을 적용하는 방식은 **복합 접근법**이다. 비형식적 접근법은 이러한 두 방법의 결합이 아니라 담당자의 지식과 경험을 활용한다.

③ O: 상세 위험분석은 **자산·위협·취약점을 구체적으로 분석**하여 위험과 보안 요구사항에 맞는 대책을 정한다. 개별 상황을 면밀히 조사하므로 적합한 보호조치를 선정할 수 있지만 시간과 노력, 전문성이 많이 필요하다.

④ X: 표준 대책을 체크리스트 등으로 공통 적용해 비용과 시간을 줄이는 것은 **기준선 접근법**이다. 개별 시스템의 위험 차이를 충분히 반영하지 못하면 과도하거나 부족한 보호가 될 수 있다. 복합 접근법은 고위험 영역을 별도로 상세 분석하여 이러한 한계를 보완한다.

따라서 가장 적절한 설명은 ③이다.

NoteBase

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

주 센터와 동일한 수준의 정보기술 지원을 원격지에 구축하고, 상시 운영 가능한 Active-Active 운영 상태를 유지함으로써 주 센터 재해 시 실시간으로 복구가 가능하다.

① Hot Site
② Warm Site
③ Mirror Site
④ Cold Site

정답 3번

간단한 해설

주 센터와 원격 센터를 **상시 Active-Active**로 운영하여 재해 시 서비스를 신속하게 이어가는 것은 미러 사이트의 특징이다. 단순히 복구 장비를 준비하는 것보다 높은 수준의 가동 준비 상태를 뜻한다.

핵심 풀이

지문의 핵심은 주 센터와 동일한 수준의 환경을 원격지에 갖추는 데 그치지 않고, **두 센터를 상시 가동하는 Active-Active** 상태를 유지한다는 점이다. 한쪽이 중단되어도 이미 가동 중인 다른 쪽이 서비스를 이어받을 수 있으므로, 재해 후 장비를 설치하거나 시스템을 새로 가동하는 시간이 거의 필요하지 않다.

Hot Site는 필요한 시스템과 기반 시설을 미리 갖추어 신속한 복구가 가능한 방식이다. 다만 **신속하게 전환할 준비가 되어 있음**만으로 두 센터가 평소부터 함께 서비스를 처리하는 Active-Active 운영까지 뜻하지는 않는다.

Warm Site는 복구에 필요한 환경을 일부 갖춘 방식이다. 재해 후 부족한 구성 요소의 보완이나 데이터 복원 등의 준비가 필요하므로, 지문의 상시 가동·실시간 복구 조건과 차이가 있다.

Mirror Site는 주 센터에 대응하는 환경을 원격지에 중복 구축하고 **데이터를 실시간으로 복제**하는 방식이다. 지문처럼 두 센터를 모두 활성 상태로 운영하면 재해 시 서비스 중단을 최소화할 수 있다. 여기서 실시간 복구는 이러한 준비 상태를 나타내며, 모든 장애에서 지연이나 손실이 절대 없다는 보장은 아니다.

Cold Site는 복구에 사용할 공간과 전력 등 기본 시설을 마련해 두는 방식이다. 재해 후 장비 반입·설치와 데이터 복원 등의 작업이 필요하므로 즉시 서비스를 이어가는 방식과 구별된다.

따라서 동일 수준의 원격 환경, 상시 Active-Active 운영, 실시간 복구라는 단서에 가장 적합한 유형은 ③ Mirror Site이다.

NoteBase

문 6. SSO(Single Sign On)에 대한 설명으로 가장 적절하지 않은 것은?

① 한 번의 시스템 인증을 통하여 접근하고자 하는 다양한 정보 시스템에 재인증 절차 없이 접근할 수 있도록 하는 통합 로그인 솔루션이다.

② 자동 인증을 원하는 시스템에 SSO 에이전트(agent) 소프트웨어를 설치하고 SSO 서버와의 통신을 통해 자동으로 인증을 수행해 준다.

③ 인증 방식은 패스워드, 토큰 또는 공인인증서를 사용하는 PKI(Public Key Infrastructure) 기반 인증 등의 다양한 형태가 존재한다.

④ 사용자 인증 시 고정된 패스워드를 사용하는 것이 아니라 매번 패스워드를 생성하여 사용한다.

정답 4번

간단한 해설

SSO는 한 번의 인증으로 여러 시스템의 로그인을 연계하는 방식이다. 매번 새로운 일회용 비밀번호를 사용하는 설명은 **OTP의 특징**이므로 ④가 적절하지 않다.

선지별 해설

① O: SSO는 한 번 확인한 **인증 결과를 여러 연계 시스템에서 활용**하여 사용자가 시스템마다 반복 로그인하지 않게 하는 방식이다. 여기서 재인증 절차가 없다는 것은 통상 사용자에게 같은 자격 증명을 다시 입력하게 하지 않는다는 뜻이며, 시스템 간 인증 정보 검증까지 생략한다는 뜻은 아니다. 세션 만료나 높은 보안 수준을 요구하는 작업에는 추가 인증이 필요할 수 있다.

② O: **에이전트 방식의 SSO**에서는 연계 시스템에 설치된 에이전트가 SSO 서버와 통신하여 인증 상태를 확인하고 로그인 처리를 연동한다. 이는 SSO의 한 구현 방식이며, 모든 SSO가 각 시스템에 별도 에이전트를 설치해야 한다는 뜻은 아니다.

③ O: SSO는 인증 결과를 연계하는 체계이므로 최초 사용자 인증 수단을 하나로 제한하지 않는다. 패스워드, 인증 토큰, 인증서와 개인키를 사용하는 PKI 기반 인증 등 **여러 인증 수단과 결합**할 수 있다. 공인인증서라는 원문의 예시도 인증서 기반 인증의 한 형태를 가리킨다.

④ X: 매번 달라지는 일회용 비밀번호를 만들어 사용하는 것은 **OTP(One-Time Password)** 방식의 특징이다. SSO의 핵심은 비밀번호 생성 규칙이 아니라 한 번의 인증 결과를 연계 시스템에서 활용하는 데 있다. SSO의 최초 인증에 OTP를 사용할 수는 있지만, SSO 자체가 매번 새 비밀번호를 생성하는 방식은 아니다.

NoteBase

문 7. 위험 분석에서 위험(risk)이란 원하지 않는 사건이 발생하여 부정적인 영향을 미칠 가능성을 말한다. 위험의 유형과 규모를 확인하기 위해서는 위험에 관련된 모든 요소들과 위험의 규모에 미치는 영향을 분석해야 한다. 이러한 위험 분석에 포함되는 핵심적인 구성 요소로 가장 적절하지 않은 것은?

① 취약성(vulnerability)

② 손실(loss)

③ 자산(asset)

④ 위협(threat)

정답 2번

간단한 해설

정답은 ② 손실이다. 이 문항의 기본 구성 요소는 자산·위협·취약성이며, 손실은 이들의 관계에서 발생할 수 있는 **피해의 결과나 규모**를 뜻한다.

개념 구분

이 문항은 위험을 발생시키는 기본 관계를 **자산·위협·취약성**으로 구분하는 틀을 묻는다. 위협이 자산의 취약성을 이용하거나 촉발하면 피해가 발생할 수 있다.

취약성: 위협에 의해 이용되거나 문제가 드러날 수 있는 **자산·통제 수단의 약점**이다. 예를 들어 서버의 미패치 보안 결함은 공격을 가능하게 하는 취약성이다.

손실: 보안사고로 발생하는 **피해의 결과나 규모**이다. 데이터 소실, 업무 중단, 금전적 피해 등이 해당한다. 이는 이 문항에서 구별하는 세 가지 기본 요소와는 역할이 다르다. 다만 예상 손실은 영향 평가에 중요하므로 위험 분석에서 전혀 고려하지 않는다는 뜻은 아니다.

자산: 조직이 가치를 부여하고 **보호해야 하는 대상**이다. 정보, 서버, 소프트웨어, 시설 등이 해당하며, 자산의 중요성과 가치가 피해 규모 판단의 바탕이 된다.

위협: 자산에 피해를 줄 수 있는 **사건·행위 또는 그 원인**이다. 공격뿐 아니라 화재나 사람의 실수도 위협이 될 수 있으므로 악의적인 행위에만 한정하지 않는다.

따라서 자산·위협·취약성이라는 기본 구성 요소와 구별되는 것은 ② 손실이다.

NoteBase

문 8. 다음에서 설명하는 내용으로 가장 적절한 것은?

각종 재해나 재난 발생에 대비하여 핵심 시스템의 가용성과 신뢰성을 회복하고 업무의 연속성을 유지하기 위한 일련의 계획과 절차를 의미한다. 단순한 데이터의 복구나 원상회복뿐만 아니라 업무의 지속성을 보장하며 이를 통해 조직의 신뢰도를 유지하고, 나아가 전체적인 신뢰성 유지와 가치를 최대화하는 방법이다.

① BCP(Business Continuity Planning)

② BIA(Business Impact Analysis)

③ DRP(Disaster Recovery Planning)

④ MTD(Maximum Tolerable Downtime)

정답 1번

간단한 해설

단순한 시스템·데이터 복구를 넘어 **핵심 업무의 지속**을 준비하는 계획이 BCP이다. 제시문의 업무 연속성과 조직 신뢰 유지라는 설명이 이에 해당한다.

핵심 풀이

제시문은 시스템의 가용성과 신뢰성 회복에 더하여 **업무의 연속성 유지**를 강조한다. BCP(업무연속성계획)는 재난이나 장애 중에도 핵심 업무를 지속하고 정상 업무로 복귀할 수 있도록 자원과 절차를 준비하는 계획이다. 단순한 데이터 복구를 넘어 업무 지속과 조직의 신뢰를 다룬다는 점이 결정적 단서이다.

DRP(재해복구계획)는 **정보시스템과 데이터의 복구**에 초점을 둔다. 시스템을 복구해 업무 재개를 지원하지만, 제시문처럼 업무의 연속성 전반을 설명하는 개념으로는 BCP가 더 적절하다.

BIA(업무영향분석)는 업무 중단이 조직에 미치는 영향을 분석하여 **복구의 우선순위와 요구사항**을 정하는 활동이다. 계획 수립에 필요한 분석이지, 제시문이 말하는 업무 지속을 위한 계획과 절차 전체의 명칭은 아니다.

MTD(최대허용중단시간)는 조직이 업무 중단을 감내할 수 있는 **최대 시간**이다. 계획이나 절차가 아니라 허용 가능한 중단 기간을 나타내는 지표이다.

따라서 제시문에 해당하는 것은 ① BCP이다.

NoteBase

문 9. OTP(One Time Password) 기법은 동기식과 비동기식 방식으로 나뉠 수 있다. 동기식 방식에 대한 설명으로 가장 적절한 것은?

① OTP 생성매체가 일정 시간마다 비밀번호를 자동으로 생성하는 형태로 시간을 기준 값으로 하여 OTP 생성매체와 OTP 인증 서버가 동기화 된다.

② 사용자의 OTP 생성매체와 은행의 OTP 인증 서버 사이에 동기화 되는 기준 값이 없으며 사용자가 직접 임의의 난수를 OTP 생성매체에 입력하여 생성한다.

③ 사용자가 은행의 OTP 인증 서버로부터 받은 질의 값(challenge)을 OTP 생성매체에 직접 입력하면 응답 값(response)이 생성된다.

④ 직접 질의 값을 확인하여 OTP 생성매체에 입력해야 하므로 은행은 별도의 질의 값을 관리해야 한다.

정답 1번

간단한 해설

동기식 OTP는 생성매체와 인증 서버가 **시간이나 카운터라는 공통 기준값**을 맞추어 비밀번호를 생성·검증한다. 일정 시간마다 비밀번호가 바뀌는 방식은 시간 동기식이고, 서버의 질의값을 입력해 응답을 만드는 방식은 질의·응답 방식이다.

선지별 해설

① O: **시간 동기식 OTP**는 생성매체와 인증 서버가 공유한 비밀키와 동일한 시간 구간을 기준으로 일회용 비밀번호를 계산한다. 일정 시간이 지나면 시간 기준값이 바뀌므로 생성되는 비밀번호도 갱신된다. 시간을 기준으로 양쪽이 동기화된다는 이 설명이 적절하다.

② X: **동기화되는 기준값이 없다**는 설명은 동기식 OTP에 해당하지 않는다. 동기식은 시간이나 사용 횟수에 따른 카운터를 공통 기준으로 맞추어 비밀번호를 생성·검증한다. 또한 사용자가 임의로 입력한 난수를 서버가 알지 못한다면 그것만으로 응답을 검증할 수 없으므로, 이 표현을 그대로 표준적인 질의·응답 절차로 이해해서도 안 된다.

③ X: 서버가 제시한 **질의값에 대한 응답**을 생성하는 절차는 이 문제에서 대비하는 비동기식의 질의·응답 방식이다. 동기식에서는 매번 서버의 질의값을 받아 입력하는 대신, 양쪽이 맞춘 시간이나 카운터를 이용하여 OTP를 생성·검증한다.

④ X: 별도의 질의값을 사용자에게 제시하고 그 응답을 확인하는 관리는 **질의·응답 방식**의 특징이다. 동기식의 기본 절차에서는 매 인증마다 별도 질의값을 입력받는 것이 아니라, 비밀키와 함께 시간 또는 카운터의 동기 상태를 관리하여 OTP를 검증한다.

NoteBase

문 10. 정보보호 및 개인정보보호 관리체계(ISMS-P)에 대한 설명으로 가장 적절하지 않은 것은?

① 기존 ISMS 인증 및 ISMS-P 인증으로 구성되며, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」과 「개인정보 보호법」을 근간으로 “정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시”를 확정했다.

② 과학기술정보통신부장관, 행정안전부장관 및 방송통신위원회는 정보보호 및 개인정보보호 관리체계 인증 운영에 관한 정책사항을 협의하기 위하여 정보보호 및 개인정보보호 관리체계 인증 협의회를 운영한다.

③ 한국정보통신진흥협회는 인증위원회를 개최하여 최종 인증을 부여하고 인증심사원 양성을 추진하며, 심사기관은 한국인터넷진흥원이 심사를 수행한다.

④ 인증심사 기준은 관리체계 수립 및 운영과 보호대책 요구사항, 개인정보 처리 단계별 요구사항으로 각 분야별 세부항목을 정의하고 있다.

정답 3번

간단한 해설

인증위원회 운영과 인증심사원 양성은 **한국인터넷진흥원(KISA)**의 역할이다. 한국정보통신진흥협회(KAIT)는 인증심사를 수행하는 심사기관이므로, 선지는 기관별 역할을 잘못 연결했다.

NoteBase

선지별 해설

2019년 시험 당시의 ISMS-P 인증 제도는 조직의 정보보호와 개인정보보호 활동이 인증기준에 맞게 수립·운영되는지를 확인하는 제도이다. 정책을 협의하는 기관, 인증을 부여하는 기관, 실제 심사를 수행하는 기관의 역할을 구별한다.

① O: 통합된 인증 제도에서는 **ISMS 인증과 ISMS-P 인증**을 선택할 수 있다. ISMS는 정보보호 관리체계를 대상으로 하고, ISMS-P는 개인정보 처리 과정의 보호까지 포함한다. 당시 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」과 「개인정보 보호법」에 근거한 공통 고시가 통합 운영 사항을 정했다.

② O: 당시 과학기술정보통신부장관, 행정안전부장관 및 방송통신위원회가 인증 협의회를 운영했다. 협의회는 인증제도 개선과 인증기관·심사기관 지정 등의 **정책 사항을 협의**하는 기구이며, 개별 신청기관의 인증심사 결과를 심의하는 인증위원회와 구별된다.

③ X: **한국인터넷진흥원(KISA)**은 인증위원회 운영과 인증서 발급, 인증심사원 양성·자격관리 등을 담당한다. 한국정보통신진흥협회(KAIT)는 인증심사를 수행하는 **심사기관**의 역할을 하므로, 선지는 인증 부여·심사원 양성의 주체를 잘못 연결했다. KISA나 인증기관도 인증심사를 수행할 수 있으며, KISA의 역할이 심사에만 한정되는 것은 아니다.

④ O: 인증기준은 **관리체계 수립 및 운영, 보호대책 요구사항, 개인정보 처리 단계별 요구사항**의 세 영역으로 구성된다. 각각 조직의 관리 절차, 관리적·기술적·물리적 보호조치, 개인정보의 수집부터 파기까지의 보호를 점검한다. ISMS 인증에는 앞의 두 영역을, ISMS-P 인증에는 세 영역을 적용한다.

따라서 기관별 역할을 잘못 연결한 ③이 가장 적절하지 않다.

NoteBase

문 11. 「개인정보 보호법」에서 공개된 장소에 영상정보처리기기를 설치·운영할 수 있는 경우로 가장 적절하지 않은 것은?

① 범죄의 예방 및 수사를 위하여 필요한 경우

② 시설안전 및 화재 예방을 위하여 필요한 경우

③ 영상정보 저장과 음성 녹음이 동시에 필요한 경우

④ 교통정보의 수집·분석 및 제공을 위하여 필요한 경우

정답 3번

간단한 해설

영상정보처리기기를 설치·운영할 법정 사유가 있어도 **녹음기능은 사용할 수 없다**. 영상 저장과 음성 녹음이 동시에 필요하다는 사정은 설치·운영의 허용 사유가 아니다.

NoteBase

핵심 풀이

이 문항은 2019년 당시 「개인정보 보호법」 제25조의 영상정보처리기기 규정을 기준으로 판단한다. 공개된 장소에 설치·운영하는 것은 원칙적으로 제한되며, 제1항에서 정한 **법정 허용 사유**에 해당해야 한다.

허용 사유의 구분:

① O: 범죄의 예방 및 수사는 제25조제1항제2호에 해당한다.

② O: 시설안전 및 화재 예방은 같은 항 제3호에 해당한다.

④ O: 교통정보의 수집·분석 및 제공은 같은 항 제5호에 해당한다.

따라서 이 세 목적은 법에 열거된 설치·운영 사유이다. 다만 허용 사유에 해당하더라도 장소 제한과 안내 등 다른 법정 요건을 함께 지켜야 한다.

영상 저장과 음성 녹음의 구분:

③ X: 제25조제5항은 영상정보처리기기운영자의 **녹음기능 사용을 금지**한다. 영상과 음성을 동시에 확보할 필요가 있다는 사정은 제1항의 허용 사유가 아니며, 설치·운영 목적이 허용되더라도 녹음까지 허용되는 것은 아니다.

따라서 설치·운영할 수 있는 경우로 가장 적절하지 않은 것은 영상정보 저장과 음성 녹음이 동시에 필요하다는 ③이다.

NoteBase

문 12. 「개인정보 보호법」 및 동 시행령에서 공공기관의 장은 개인정보파일 운용으로 인하여 개인정보 침해가 우려되는 경우, 그 위험요인의 분석과 개선 사항 도출을 위한 "개인정보 영향평가"를 수행해야 한다. 해당 평가 수행에 따른 고려 사항으로 가장 적절하지 않은 것은?

① 개인정보 처리 시스템 수

② 개인정보의 보유기간 및 제3자 제공 여부

③ 정보주체의 권리를 해할 가능성 및 그 위험 정도

④ 민감정보 또는 고유식별정보의 처리 여부

정답 1번

간단한 해설

정답은 ①이다. 법령상 고려사항은 개인정보 처리 시스템의 수가 아니라 **처리하는 개인정보의 수**이다.

핵심 풀이

2019년 출제 당시 「개인정보 보호법」 제33조제2항은 처리하는 개인정보의 수, 제3자 제공 여부, 정보주체의 권리를 해할 가능성과 위험 정도, 대통령령으로 정한 사항을 고려하도록 했다. 같은 법 시행령 제36조는 민감정보 또는 고유식별정보의 처리 여부와 개인정보 보유기간을 추가했다.

① X: 개인정보 처리 시스템 수: 법령이 열거한 항목은 시스템의 개수가 아니라 **처리하는 개인정보의 수**이다. 시스템이 몇 개인지와 그 안에서 처리하는 개인정보의 규모는 서로 다르므로 ①이 제시된 법정 고려사항에 해당하지 않는다.

② O: 개인정보의 보유기간 및 제3자 제공 여부: **보유기간은 시행령, 제3자 제공 여부는 법률**에 각각 규정되어 있으므로 두 내용 모두 고려사항이다. 보관 기간과 외부 제공에 따른 개인정보의 처리 범위를 살펴야 한다.

③ O: 정보주체의 권리를 해할 가능성 및 그 위험 정도: 개인정보 처리로 권리가 침해될 가능성과 그 위험의 정도를 평가하는 **법률에 명시된 항목**이다. 위험요인을 분석하고 개선 사항을 도출하려는 영향평가의 목적과 연결된다.

④ O: 민감정보 또는 고유식별정보의 처리 여부: 개인정보의 종류에 따른 침해 위험을 살피기 위해 **시행령에서 정한 고려사항**이다. 일반적인 처리 규모와 별도로 이러한 정보의 처리 여부를 확인한다.

따라서 법령상 열거된 고려사항과 다른 것은 ① 개인정보 처리 시스템 수이다. 이는 실제 평가에서 시스템 현황을 조사할 필요가 없다는 뜻은 아니다.

NoteBase

문 13. 「개인정보 보호법」에서 개인정보 보호위원회(이하 "보호위원회"라 한다)와 관련된 내용으로 가장 적절하지 않은 것은?

① 중앙행정기관의 장은 소관 법령의 제정 또는 개정을 통하여 개인정보 처리를 수반하는 정책이나 제도를 도입·변경하는 경우에는 보호위원회에 개인정보 침해요인 평가를 요청하여야 한다.

② 보호위원회는 개인정보의 보호와 정보주체의 권익 보장을 위하여 매년 개인정보 보호 내부 관리계획을 관계 중앙행정기관의 장과 협의하여 수립한다.

③ 중앙행정기관의 장은 기본계획에 따라 매년 개인정보 보호를 위한 시행계획을 작성하여 보호위원회에 제출하고, 보호위원회의 심의·의결을 거쳐 시행하여야 한다.

④ 보호위원회는 기본계획을 효율적으로 수립하기 위하여 개인정보 처리자, 관계 중앙행정기관의 장, 지방자치단체의 장 및 관계 기관·단체 등에 개인정보처리자의 법규 준수 현황과 개인정보 관리 실태 등에 관한 자료의 제출이나 의견의 진술 등을 요구할 수 있다.

정답 2번

간단한 해설

보호위원회는 관계 중앙행정기관의 장과 협의하여 **3년마다 개인정보 보호 기본계획**을 수립한다. 매년 작성하는 것은 각 중앙행정기관의 시행계획이므로 계획의 명칭과 수립 주기를 함께 구별해야 한다.

NoteBase

선지별 해설

① O: 중앙행정기관의 장이 법령의 제정·개정을 통해 개인정보 처리를 수반하는 정책이나 제도를 도입·변경하면, 보호위원회에 **개인정보 침해요인 평가를 요청**해야 한다. 법 제8조의2 제1항에 따른 의무로, 새 제도에 개인정보 침해 위험이 있는지 검토하도록 하는 절차이다.

② X: 보호위원회가 관계 중앙행정기관의 장과 협의하여 수립하는 것은 **3년마다의 개인정보 보호 기본계획**이다. 법 제9조 제1항에 따라 “매년”은 “3년마다”로, “개인정보 보호 내부 관리계획”은 “개인정보 보호 기본계획”으로 각각 고쳐야 한다.

③ O: 법 제10조 제1항에 따라 중앙행정기관의 장은 기본계획에 맞추어 **매년 시행계획**을 작성한다. 보호위원회에 제출하고 그 심의·의결을 거쳐 시행하는 것으로, 보호위원회의 3년 단위 기본계획을 연도별로 구체화하는 절차이다.

④ O: 보호위원회는 기본계획을 효율적으로 수립하기 위해 **자료 제출이나 의견 진술을 요구**할 수 있다. 법 제11조 제1항의 대상에는 개인정보처리자, 관계 중앙행정기관의 장, 지방자치단체의 장 및 관계 기관·단체 등이 포함되며, 법규 준수 현황과 개인정보 관리 실태 등이 요구할 수 있는 내용이다.

따라서 가장 적절하지 않은 것은 ②이다.

NoteBase

문 14. 「개인정보 보호법」에서 공공기관의 장이 개인정보파일을 운용하는 경우 행정안전부장관에게 이를 제32조(개인정보파일의 등록 및 공개)에서 규정하는 바에 따라 등록하여야 한다. 동 조항에서 규정하고 있는 개인정보파일 중 등록 제외대상에 대한 내용으로 가장 적절하지 않은 것은?

① 국가 안전, 외교상 비밀, 그 밖에 국가의 중대한 이익에 관한 사항을 기록한 개인정보파일

② 범죄의 수사, 공소의 제기 및 유지, 형 및 감호의 집행, 교정처분, 보호처분, 보안관찰처분과 출입국관리에 관한 사항을 기록한 개인정보파일

③ 「조세범처벌법」에 따른 범칙행위 조사 및 「관세법」에 따른 범칙행위 조사에 관한 사항을 기록한 개인정보파일

④ 공공기관에서 불특정 다수를 대상으로 하는 단기적 업무처리만을 위하여 사용되는 개인정보파일

정답 4번

간단한 해설

법에서 정한 제외대상은 공공기관의 **내부적 업무처리만을 위한 파일**이다. 불특정 다수를 대상으로 단기간 사용하는 파일이라는 이유만으로 등록 의무가 제외되지는 않는다.

NoteBase

선지별 해설

2019년 시험 당시 「개인정보 보호법」 제32조는 공공기관의 장이 운용하는 개인정보파일의 명칭·운영 목적·개인정보 항목 등을 행정안전부장관에게 등록하도록 정했다. 다만 제2항에 열거된 파일에는 이 등록 의무가 적용되지 않는다.

① O: **국가 안전·외교상 비밀·국가의 중대한 이익**에 관한 사항을 기록한 파일은 제32조제2항제1호에 명시된 등록 제외대상이다. 단순히 공공기관이 보유한다는 사실이 아니라, 기록된 사항이 해당 국가적 이익에 관한 것인지가 기준이다.

② O: 범죄 수사와 공소 제기·유지, 형 및 감호의 집행, 교정·보호·보안관찰처분, 출입국관리에 관한 사항을 기록한 파일은 제32조제2항제2호의 제외대상이다. 수사에 관한 파일뿐 아니라 **열거된 형 집행·처분 및 출입국관리** 관련 파일도 포함된다.

③ O: 「조세범처벌법」과 「관세법」에 따른 **범칙행위 조사**에 관한 사항을 기록한 파일은 제32조제2항제3호에 해당한다. 모든 조세·관세 행정 자료가 일괄 제외되는 것이 아니라, 선지에 제시된 법률에 따른 범칙행위 조사라는 범위를 충족해야 한다.

④ X: 제32조제2항제4호가 정한 제외대상은 공공기관의 **내부적 업무처리만을 위하여 사용되는** 개인정보파일이다. 불특정 다수를 대상으로 한다거나 업무처리 기간이 짧다는 이유만으로 이 제외사유에 해당하지 않는다. 선지는 '내부적 업무처리만'이라는 용도 요건을 '불특정 다수 대상의 단기적 업무처리'로 잘못 바꾸었다.

따라서 등록 제외대상의 요건을 잘못 설명한 ④가 가장 적절하지 않다.

NoteBase

문 15. 「개인정보 보호법」에서 개인정보 처리와 관련한 정보주체의 권리로 가장 적절하지 않은 것은?

① 개인정보처리자가 개인정보의 처리를 통해 취득한 이익에 관한 정보를 제공받을 권리

② 개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리

③ 개인정보에 대하여 열람, 처리 정지, 정정·삭제 및 파기를 요구할 권리

④ 개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리

정답 1번

간단한 해설

정보주체에게 보장되는 것은 **개인정보의 처리에 관한 정보**를 제공받을 권리이다. 이를 개인정보처리자가 취득한 이익에 관한 정보를 제공받을 권리로 바꾸면 법이 정한 권리의 내용과 달라진다.

선지별 해설

① X: 개인정보 보호법 제4조제1호가 정한 것은 **개인정보의 처리에 관한 정보를 제공받을 권리**이다. 선지처럼 개인정보처리자가 처리로 취득한 이익에 관한 정보를 제공받을 권리로 규정한 것이 아니다. 정보 제공의 대상을 처리자의 이익으로 바꾼 이 설명이 적절하지 않다.

② O: 개인정보 보호법 제4조제2호는 개인정보 처리에 관한 **동의 여부와 동의 범위를 선택·결정할 권리**를 규정한다. 자신의 개인정보 처리에 동의할지, 어디까지 동의할지를 정보주체가 결정한다는 설명에 해당한다.

③ O: 개인정보 보호법 제4조제3호의 **열람 요구권**과 같은 조 제4호의 **처리 정지·정정·삭제·파기 요구권**을 함께 설명한 것이다. 정보주체가 자신의 개인정보를 확인하고 필요한 조치를 요구하는 권리이며, 구체적인 행사는 법에서 정한 요건과 절차에 따른다.

④ O: 개인정보 보호법 제4조제5호는 개인정보 처리로 발생한 피해를 **신속하고 공정한 절차로 구제받을 권리**를 규정한다. 따라서 개인정보 처리로 인한 피해에 대해 절차적 구제를 요구할 수 있다는 설명은 적절하다.

NoteBase

문 16. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제27조의3 (개인정보 유출 등의 통지·신고)의 일부내용이다. 빈칸 ㉠부터 ㉤까지 들어갈 것으로 가장 적절하게 짝지어진 것은?

정보통신서비스 제공자등은 개인정보의 분실·도난·유출 사실을 안 때에는 지체 없이 관련 침해사고 사항을 (㉠)에 알리고 (㉡) 또는 (㉢)에 신고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 (㉤)을 경과하여 통지·신고해서는 아니 된다. 다만, 이용자의 연락처를 알 수 없는 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다.

① ㉠: 정보보호 책임자, ㉡: 행정안전부, ㉢: 국가정보원, ㉤: 12시간

② ㉠: 해당 이용자, ㉡: 행정안전부, ㉢: 한국인터넷진흥원, ㉤: 24시간

③ ㉠: 정보보호 책임자, ㉡: 방송통신위원회, ㉢: 국가정보원, ㉤: 12시간

④ ㉠: 해당 이용자, ㉡: 방송통신위원회, ㉢: 한국인터넷진흥원, ㉤: 24시간

정답 4번

간단한 해설

당시 조문은 **해당 이용자에게 통지**하고 방송통신위원회 또는 한국인터넷진흥원에 신고하도록 정했다. 지체 없이 이행해야 하며, 정당한 사유 없이 유출등을 안 때부터 **24시간을 넘길 수 없다**.

NoteBase

빈칸별 해설

이 문항은 2019년 당시 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제27조의3을 묻는다. 개인정보 유출등을 안 정보통신서비스 제공자등은 이용자에게 하는 통지와 관계 기관에 하는 신고를 각각 이행해야 한다.

㉠ 해당 이용자: 통지의 상대방은 유출등의 영향을 받는 **해당 이용자**이다. 이용자가 피해에 대응할 수 있도록 사고 관련 사항을 알리는 의무이므로 내부 정보보호 책임자에게 보고하는 것으로 대신할 수 없다. 다만 연락처를 알 수 없는 등 정당한 사유가 있으면 대통령령에서 정하는 통지 대체 조치를 할 수 있다.

㉡ 방송통신위원회: 당시 조문이 정한 신고 기관 중 하나는 **방송통신위원회**이다. 이 조항의 빈칸에 행정안전부를 넣으면 당시 정보통신서비스 제공자등에 적용된 신고 기관과 달라진다.

㉢ 한국인터넷진흥원: 다른 신고 기관은 **한국인터넷진흥원**이며 국가정보원이 아니다. 원문의 연결어가 ‘또는’이므로 방송통신위원회나 한국인터넷진흥원 중 한 기관에 신고한다. 이 기관 신고와 해당 이용자에게 하는 통지는 별개의 의무이다.

㉣ 24시간: 기산점은 사고가 발생한 때가 아니라 **유출등의 사실을 안 때**이다. 지체 없이 통지·신고해야 하고, 정당한 사유 없이 그때부터 24시간을 넘길 수 없다. 24시간이 될 때까지 자유롭게 미뤄도 된다는 뜻은 아니다.

따라서 ㉠ 해당 이용자, ㉡ 방송통신위원회, ㉢ 한국인터넷진흥원, ㉣ 24시간으로 연결되는 ④가 정답이다.

NoteBase

문 17. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 정보통신서비스 제공자등이 영업의 전부 또는 일부의 양도·합병 등으로 그 이용자의 개인정보를 타인에게 이전하는 경우에 인터넷 홈페이지 게시, 전자우편, 전화 등의 방법에 따라 서비스 이용자에게 반드시 알려야 하는 내용으로 가장 적절하지 않은 것은?

① 개인정보를 이전하려는 사실

② 개인정보를 이전하는 보호책임자의 성명 또는 개인정보보호 업무 및 관련 고충사항을 처리하는 부서의 명칭과 그 전화번호 등 연락처

③ 개인정보를 이전받는 자의 성명·주소·전화번호 및 그 밖의 연락처

④ 이용자가 개인정보의 이전을 원하지 아니하는 경우 그 동의를 철회할 수 있는 방법과 절차

정답 2번

간단한 해설

②의 보호책임자 또는 고충처리 부서 연락처는 **개인정보 처리방침의 기재사항**이며, 영업 양도·합병에 따른 개인정보 이전 시의 필수 고지사항에는 포함되지 않는다.

핵심 풀이

2019년 출제 당시 정보통신망법 제26조 제1항은 영업의 양도·합병 등으로 이용자의 개인정보를 타인에게 이전할 때 미리 알려야 할 사항을 세 가지로 정하고 있었다. 각 항목이 이 목록에 해당하는지 구별한다.

① 이전하려는 사실: 이용자가 자신의 개인정보가 다른 주체에게 넘어간다는 점을 알 수 있도록 **개인정보 이전 자체의 사실**을 알려야 한다.

② 보호책임자 또는 고충처리 부서의 연락처: 이는 **개인정보 처리방침에 포함할 사항**에 해당하는 내용으로, 영업 양도·합병에 따른 이전 시의 세 가지 필수 고지사항에는 포함되지 않는다. 당시 제27조의2 제2항 제7호는 개인정보 보호책임자의 성명 또는 개인정보보호 업무와 관련 고충사항을 처리하는 부서의 명칭 및 전화번호 등 연락처를 처리방침에 포함하도록 정했다. 따라서 이러한 연락처를 전혀 공개할 필요가 없다는 뜻은 아니다.

③ 이전받는 자의 성명·주소·전화번호 및 그 밖의 연락처: 이용자가 **누구에게 개인정보가 이전되는지** 확인하고 연락할 수 있어야 하므로 필수 고지사항이다. 이전받는 자가 법인이면 성명 대신 법인의 명칭을 알린다.

④ 동의를 철회할 수 있는 방법과 절차: 이용자가 이전을 원하지 않을 때 선택권을 행사할 수 있도록 **동의 철회의 방법과 절차**를 알려야 한다.

따라서 이전하려는 사실, 이전받는 자의 인적 사항·연락처, 이전을 원하지 않을 때의 동의 철회 방법·절차에 해당하지 않는 ②가 정답이다.

NoteBase

문 18. 「정보통신기반 보호법」 및 동 시행령에서 정보통신기반시설에 대한 침해사고 발생에 따른 피해의 효율적인 수습을 위하여 대책본부장이 소집한 대책본부회의를 반드시 거쳐야 하는 사항이 명시되어 있다. 해당하는 사항으로 가장 적절하지 않은 것은?

① 피해시설에 대한 복구조치

② 피해확산 방지에 필요한 조치

③ 피해자 구제를 위한 법적 조치

④ 유사한 침해사고의 방지를 위한 예방대책

정답 3번

간단한 해설

대책본부회의를 반드시 거칠 사항에는 시설 복구, 피해확산 방지, 피해액 산정 기준, 재발 예방대책이 포함된다. **피해자 구제를 위한 법적 조치**는 이 필수 회의 사항에 열거되어 있지 않다.

개념 구분

「정보통신기반 보호법 시행령」 제23조제2항은 대책본부회의를 반드시 거칠 사항으로 피해시설 복구, 피해확산 방지, 피해액 산정 기준, 유사 사고 예방대책을 정한다.

① 피해시설에 대한 복구조치: 침해사고로 손상되거나 기능이 중단된 시설을 복구하는 조치로, 회의를 반드시 거칠 사항에 포함된다.

② 피해확산 방지에 필요한 조치: 사고의 영향이 다른 시설이나 업무로 번지는 것을 막기 위한 조치이므로 회의 대상에 포함된다.

③ 피해자 구제를 위한 법적 조치: 피해자의 권리 구제를 위한 조치는 위 조항에 열거된 필수 회의 사항이 아니다. 법령이 별도로 열거한 것은 **피해액 산정의 기준**이다. 두 사항을 혼동해서는 안 된다.

④ 유사한 침해사고의 방지를 위한 예방대책: 같은 유형의 사고가 다시 발생하지 않도록 하는 대책으로, 회의 대상에 포함된다.

따라서 법령에 명시된 필수 회의 사항에 해당하지 않는 것은 ③이다. 이는 피해자 구제 자체가 불필요하거나 금지된다는 뜻은 아니다.

NoteBase

문 19. 「정보통신기반 보호법」 제12조(주요정보통신기반시설 침해행위 등의 금지)에서 주요정보통신기반시설을 대상으로 금지하고 있는 침해행위에 관한 일부내용이다. 빈칸 ㉠부터 ㉢까지 들어갈 것으로 ⓐ부터 ⓒ까지 내용이 가장 적절하게 짝지어진 것은?

1. 접근권한을 가지지 아니하는 자가 주요정보통신기반시설에 접근하거나 접근권한을 가진 자가 그 권한을 초과하여 (㉠)
2. 주요정보통신기반시설에 대하여 데이터를 파괴하거나 주요정보통신기반시설의 운영을 방해할 목적으로 (㉡)
3. 주요정보통신기반시설의 운영을 방해할 목적으로 일시에 대량의 신호를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 (㉢)

ⓐ 컴퓨터바이러스·논리폭탄 등의 프로그램을 투입하는 행위
ⓑ 저장된 데이터를 조작·파괴·은닉 또는 유출하는 행위
ⓒ 정보처리에 오류를 발생하게 하는 행위

① ㉠: ⓐ, ㉡: ⓑ, ㉢: ⓒ
② ㉠: ⓒ, ㉡: ⓑ, ㉢: ⓐ
③ ㉠: ⓑ, ㉡: ⓐ, ㉢: ⓒ
④ ㉠: ⓒ, ㉡: ⓐ, ㉢: ⓑ

정답 3번

간단한 해설

접근권한을 벗어난 행위는 **저장된 데이터 침해**, 파괴·운영 방해 목적의 프로그램 투입은 **컴퓨터바이러스·논리폭탄**, 대량 신호나 부정한 명령의 처리는 **정보처리 오류**와 연결된다. 각 조항의 행위 주체·목적·수단을 함께 읽으면 빈칸을 구별할 수 있다.

NoteBase

빈칸별 해설

㉠에는 ⓑ의 **저장된 데이터를 조작·파괴·은닉 또는 유출하는 행위**가 들어간다. 정보통신기반 보호법 제12조제1호는 접근권한이 없는 사람이 시설에 접근하거나, 권한이 있는 사람이 그 권한을 초과하여 이러한 데이터 침해행위를 하는 경우를 금지한다. 단서는 접근권한의 유무·범위와 저장된 데이터에 대한 행위이다.

㉡에는 ⓐ의 **컴퓨터바이러스·논리폭탄 등의 프로그램을 투입하는 행위**가 들어간다. 제12조제2호는 데이터를 파괴하거나 주요정보통신기반시설의 운영을 방해할 목적으로 해당 프로그램을 투입하는 행위를 금지한다. 목적을 나타내는 앞부분과 프로그램 투입이라는 수단을 연결해야 한다.

㉢에는 ⓒ의 **정보처리에 오류를 발생하게 하는 행위**가 들어간다. 제12조제3호는 시설 운영을 방해할 목적으로 일시에 대량의 신호를 보내거나 부정한 명령을 처리하도록 하는 등의 방법을 사용하여 정보처리 오류를 일으키는 행위를 금지한다. 앞에 제시된 방해 방법에 이어 그 결과인 오류 발생이 연결된다.

따라서 ㉠–ⓑ, ㉡–ⓐ, ㉢–ⓒ로 연결한 ③이 맞다.

NoteBase

문 20. 「전자서명법」 제22조의2(공인인증서의 관리 등)에서 공인인증기관이 제공하는 수단을 통해 이용자가 공인인증서에 의하여 확인할 수 있는 사항으로 가장 적절하지 않은 것은?

① 공인인증기관의 명칭 등 공인인증기관임을 확인할 수 있는 정보

② 가입자의 의사에 반해 부정한 방법으로 자신의 공인인증서가 유출된 사실

③ 가입자가 당해 공인인증서가 발행된 당시에 전자서명생성정보를 지배·관리하고 있는 사실

④ 공인인증서의 발행 전에 전자서명생성정보가 유효한 사실

정답 2번

간단한 해설

정답은 ②이다. 구 「전자서명법」 제22조의2 제2항의 확인 사항은 발급기관의 정보, 발행 당시 가입자의 지배·관리 사실, 발행 전 전자서명생성정보의 유효성이다. **공인인증서 유출 사고의 발생 사실**은 여기에 포함되지 않는다.

선지별 해설

① O. 공인인증기관의 명칭 등 **발급기관을 확인할 수 있는 정보**는 구 「전자서명법」 제22조의2 제2항 제1호의 확인 사항이다. 이용자는 어느 공인인증기관이 발급한 인증서인지를 확인할 수 있어야 한다.

② X. 가입자의 의사에 반하여 공인인증서가 유출되었다는 **사고 발생 사실은 제2항의 확인 사항이 아니다**. 이 조항이 열거한 것은 발급기관의 정보, 발행 당시 가입자의 전자서명생성정보 지배·관리 사실, 발행 전 전자서명생성정보의 유효성이다. 따라서 유출 사실을 이 목록에 넣은 설명을 바로잡아야 한다. 유출 사고의 발생 여부에는 별도의 사실 확인이 필요하므로 가장 적절하지 않은 것은 ②이다.

③ O. 제2항 제2호는 **공인인증서가 발행된 당시**에 가입자가 전자서명생성정보를 지배·관리하고 있었다는 사실을 확인하도록 규정한다. 이는 발행 시점의 지배·관리 관계에 관한 것이며, 발행 이후 모든 시점에도 그 상태가 계속된다고 보증하는 뜻은 아니다.

④ O. 제2항 제3호는 **공인인증서 발행 전**에 전자서명생성정보가 유효하였다는 사실을 확인 사항으로 규정한다. 선지의 시간 조건도 조문과 일치한다. 인증서가 발행되었다는 이유로 전자서명생성정보가 이후에도 무기한 유효하다는 의미로 확대해서는 안 된다.

NoteBase