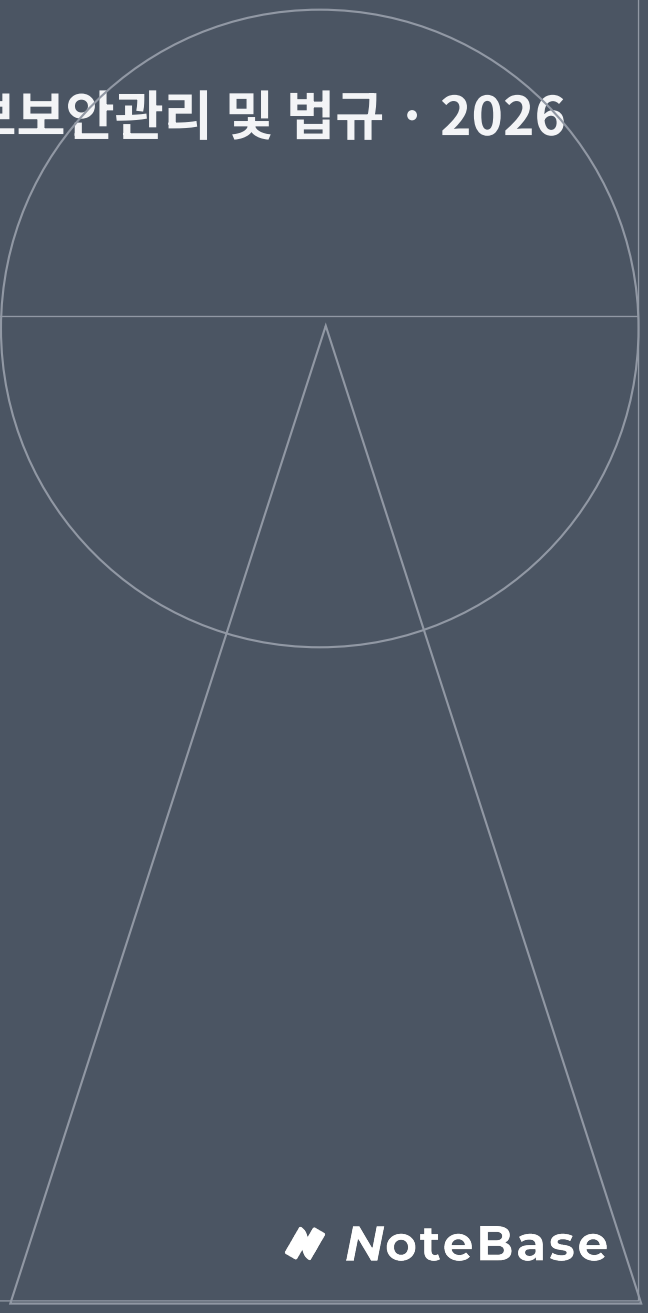
기출OX 해설집

공무원/경찰/경력채용 · 정보보안관리 및 법규 · 2026



NoteBase

기출OX 해설집

공무원/경찰/경력채용 · 정보보안관리 및 법규 · 2026

공무원/경찰/경력채용 · 정보보안관리 및 법규 · 2026

문 1. 접근통제에 관한 설명으로 가장 적절하지 않은 것은?

① 비인가된 사용자의 정보자원 사용 행위를 방지할 수 있어야 한다.

② 인가된 사용자가 비인가된 방식으로 정보 자산을 접근하는 행위는 접근통제 범위에 해당되지 않는다.

③ 보안상의 위협, 변조 등과 같은 위험으로부터 접근 대상이 되는 시스템과 제반 환경을 보호하기 위한 보안대책을 의미한다.

④ 인가된 사용자가 정보 자산을 실수 혹은 의도적으로 잘못 접근하여 정보 자산을 훼손하는 행위도 방지할 수 있어야 한다.

정답 2번

간단한 해설

접근통제는 비인가 사용자의 이용뿐 아니라 **인가된 사용자의 비인가된 방식의 접근**도 막아야 한다. ②는 사용자에게 일부 권한이 있다는 이유로 부적절한 접근을 통제 대상에서 제외했다.

선지별 해설

① O: 접근통제는 사용자 등 주체가 정보자원에 접근할 수 있는지와 어떤 작업을 할 수 있는지를 정책에 따라 결정한다. 따라서 **권한이 없는 사용자의 자원 이용을 차단**하는 것은 기본 목적이다.

② X: 시스템 이용이 허용된 사용자도 모든 자원과 작업에 권한을 갖는 것은 아니다. 접근통제에는 **인가된 사용자의 비인가된 방식의 접근도 포함**된다. 예를 들어 읽기 권한만 가진 사용자의 수정·삭제 요청은 통제해야 한다. 따라서 이를 접근통제 범위에서 제외한 ②가 가장 적절하지 않다.

③ O: 접근통제는 시스템·정보와 관련 시설에 대한 접근을 허용하거나 제한하여 비인가 접근과 변조 등의 위험을 줄이는 보안대책이다. 논리적 접근뿐 아니라 **시설 등 물리적 환경에 대한 접근**도 통제 대상이 될 수 있다. 모든 종류의 위험을 접근통제 하나로 완전히 없앤다는 의미는 아니다.

④ O: 정당한 사용자에게도 업무상 필요한 자원과 작업만 허용하여 과도한 권한으로 인한 훼손을 예방해야 한다. **허용 범위를 벗어난 접근은 고의·실수와 관계없이 통제**하는 것이 원칙이다. 예를 들어 수정 권한이 없는 중요 자료의 변경 요청을 차단하면 우발적 또는 의도적 훼손을 줄일 수 있다.

NoteBase

문 2. 다음의 설명과 같을 때 패스워드 안전성을 표현하는 수식으로 가장 적절한 것은?

· 패스워드의 길이를 S, 패스워드의 사용 기간을 L, 패스워드의 사용 빈도를 R이라고 한다.
· 패스워드 추측 변수 P는 낮을수록 안전하다.

① $P = \frac{L \times R}{S}$
② $P = \frac{S \times R}{L}$
③ $P = \frac{L \times S}{R}$
④ $P = \frac{S}{L \times R}$

정답 1번

간단한 해설

P는 낮을수록 안전하므로 길이 S가 커질 때 P가 작아지는 **분모의** S가 결정적 단서이다. 사용 기간과 사용 빈도는 이 문항의 단순화된 위험 지표에서 분자에 놓으며, 실제 성공 확률을 계산하는 식으로 일반화하지 않는다.

핵심 풀이

이 문항은 P가 낮을수록 안전하다는 조건에서 변수 변화의 방향을 비교한다. S는 원문대로 패스워드 길이이며, 다른 조건이 같을 때 길어질수록 추측하기 어려워지므로 **S가 커지면 P는 작아져야 한다**. 제시된 식 중 S를 분모에 둔 것은 하나뿐이다. 나머지는 S가 분자에 있어 길어질수록 위험 지표가 커지는 방향이 된다.

사용 기간 L과 사용 빈도 R는 이 문항의 단순화된 지표에서 커질수록 노출 위험을 높이는 요인으로 취급한다. 따라서 두 값은 분자에 놓는다. 이는 주어진 선택지의 **증감 방향을 비교하는 모형**이며, 사용 빈도만으로 실제 추측 성공 확률이 정해진다는 뜻은 아니다.

정확한 확률식과는 구별해야 한다. 같은 모양의 전통적인 추측 확률식에서는 S가 **가능한 패스워드 후보의 총수**, R가 **단위 시간당 공격자의 추측 횟수**를 뜻한다. 따라서 두 모형의 변수 정의를 서로 바꾸어 적용할 수 없으며, 원문 정의만으로 정확한 성공 확률을 계산할 수는 없다.

이 문항에서 요구하는 방향성에 맞는 식은 $P = \frac{L \times R}{S}$이므로 ①이다.

NoteBase

문 3. 다음은 시스템을 보호하여 사업환경을 유지하기 위한 방안에 관한 내용이다. ㉠, ㉡에 들어갈 용어로 가장 적절한 것은?

(㉠)는 중요한 사업의 기능들을 비상시에 대비하여 자산(assets)의 우선순위를 평가하거나, 대체 장소를 선택하는 등 재해나 재난 시에 원상 복귀하고자 미리 평가 계획을 하는 단계이다.
(㉡)는 실제 재해나 재난이 발생하는 동안 그리고 재해 발생 후에 조직원들이 취해야 하는 절차와 계획 등을 의미한다.

① ㉠: BCP, ㉡: BIA

② ㉠: BCP, ㉡: DRP

③ ㉠: DRP, ㉡: BIA

④ ㉠: DRP, ㉡: BCP

정답 2번

간단한 해설

지문은 **사업 연속성을 위한 준비 계획**과 재난 시 실행할 복구 절차를 대비한다. 이에 따라 ㉠은 BCP, ㉡은 DRP로 연결하며, 두 계획을 단순히 재난 전·후로 나누지는 않는다.

빈칸별 해설

㉠ BCP(Business Continuity Plan, 업무연속성계획): 중요한 사업 기능을 유지·재개할 수 있도록 필요한 자원과 대체 수단 등을 준비하는 계획이다. 지문에서 자산의 우선순위를 평가하고 대체 장소를 선택하는 것은 **사업 연속성을 위한 사전 준비**에 해당하므로 BCP로 연결한다.

㉡ DRP(Disaster Recovery Plan, 재해복구계획): 재해로 중단된 시스템과 서비스 등을 복구하기 위해 수행할 절차와 역할을 정한 계획이다. 이 문항에서는 재난 발생 중·후 조직원이 실행할 절차를 앞의 포괄적인 연속성 준비와 대비하여 **실제 복구 실행을 위한 DRP**로 연결한다.

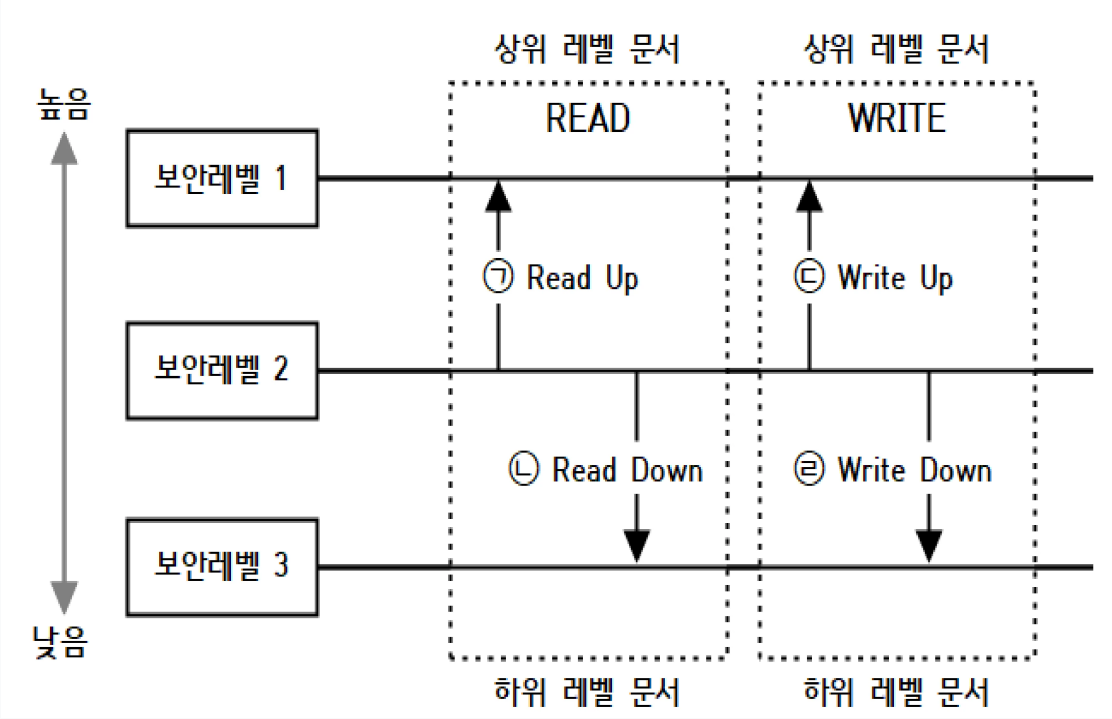
두 계획을 재난 전·후라는 시점만으로 엄격히 구분해서는 안 된다. **DRP도 재난 전에 수립·시험**하며, BCP 역시 재난 중·후의 업무 유지와 재개를 포함한다. 지문은 이러한 범위 전체를 정의하기보다 준비 활동과 복구 실행 절차를 대비한 설명이다.

BIA(Business Impact Analysis, 업무영향분석)는 업무 중단이 조직에 미치는 영향을 분석하여 중요 업무와 복구 우선순위 등을 파악하는 활동이다. 계획 수립의 근거가 되지만 복구 절차를 정한 계획 자체는 아니다.

따라서 ㉠ BCP, ㉡ DRP를 연결한 ②이다.

NoteBase

문 4. 다음은 BLP(Bell-LaPadula) 모델의 접근통제에 관한 그림이다. ㉠~㉣에서 접근을 통제하는 것만으로 옳게 짝지어진 것은?



① ㉠㉢

② ㉠㉣

③ ㉡㉢

④ ㉡㉣

정답 2번

간단한 해설

BLP는 기밀성을 보호하기 위해 **상위 등급 읽기와 하위 등급 쓰기를 금지**한다. 읽기는 대상 정보가 주체에게 들어오고, 쓰기는 주체의 정보가 대상 문서로 나간다는 차이를 기준으로 판단한다.

NoteBase

구성 요소별 해설

BLP는 높은 보안등급의 정보가 낮은 등급으로 유출되는 것을 막는 기밀성 모델이다. 그림은 보안레벨 1이 가장 높고 3이 가장 낮으며, 보안레벨 2를 기준으로 읽기·쓰기 대상 문서가 위인지 아래인지 표시한다. 기본 규칙은 **상위 읽기 금지와 하위 쓰기 금지**이다. 아래의 허용 여부는 이 등급 규칙에 관한 것으로, 별도의 접근 권한까지 자동으로 부여한다는 뜻은 아니다.

㉠ Read Up: **상위 읽기 금지**에 따라 차단한다. 보안레벨 2의 주체가 더 높은 레벨 1의 문서를 읽으면 상위 기밀이 낮은 등급의 주체에게 전달되기 때문이다. 이를 단순 보안 속성이라고 한다.

㉡ Read Down: 등급 규칙상 허용한다. 레벨 2의 주체가 더 낮은 레벨 3의 문서를 읽는 것은 **낮은 등급의 정보를 상위 주체가 받는 것**이므로 상위 기밀의 하향 유출을 일으키지 않는다.

㉢ Write Up: 등급 규칙상 허용한다. 레벨 2의 주체가 더 높은 레벨 1의 문서에 쓰면 정보가 **상위 등급의 저장 대상**으로 이동하므로 하위 등급으로 기밀이 유출되지 않는다.

㉣ Write Down: **하위 쓰기 금지**에 따라 차단한다. 레벨 2의 주체가 더 낮은 레벨 3의 문서에 쓰면 상위 등급의 정보를 하위 등급에서 읽을 수 있도록 내보낼 수 있기 때문이다. 이를 별표 속성이라고 한다.

따라서 차단되는 접근은 ㉠과 ㉣이며, 이에 해당하는 조합은 ②이다.

NoteBase

문 5. 다음에서 설명하는 개인 식별 방안이 만족해야 할 항목으로 가장 적절하지 않은 것은?

· 개인(prover)이 자신만이 가진 비밀 정보를 공개하지 않고 상대방인 확인자(verifier)에게 정보를 알고 있음을 증명할 수 있는 암호화 체계이다.
· 통상의 패스워드 방식에서는 본인임을 증명하기 위해서 비밀 정보를 그대로 표시하게 되므로 항상 위험이 따르게 되는데 이러한 결점을 극복한 것으로, 스마트카드 및 원격지 로그인에서의 사용자 식별에 사용된다.
· 비밀유지의 목적뿐만 아니라, 암호화폐에서 사용자의 익명성과 거래정보의 익명성을 제공하는 데 사용된다.

① 건실성(soundness)
② 완전성(completeness)
③ 영지식성(zero-knowledge)
④ 무작위성(randomness)

정답 4번

간단한 해설

영지식 증명의 기본 성질은 건실성·완전성·영지식성이다. **무작위성은 이 세 기본 성질에 포함되지 않으므로** ④가 답이며, 실제 구현에서 난수를 사용하지 않는다는 뜻은 아니다.

NoteBase

개념 구분

지문은 영지식 증명을 이용한 식별 방안을 설명한다. 핵심은 **비밀 자체를 공개하지 않고 필요한 사실을 증명**하는 것이다. 비밀을 검증자에게 직접 제시하는 방식과 달리, 스마트카드·원격 로그인에서 비밀 보유를 확인하는 데 활용할 수 있다. 암호화폐에서도 거래의 유효성을 확인하면서 참여자나 거래 내용의 노출을 줄이는 데 쓰일 수 있다.

건실성(soundness): 거짓 명제를 주장하는 부정직한 증명자가 정직한 확인자를 쉽게 속일 수 없어야 한다. 즉, **거짓 주장의 수락 가능성을 제한**하는 성질이다. 확률적 증명에서는 허용되는 오류확률을 작게 만들므로, 모든 방식에서 오류가 수학적으로 항상 0이라는 뜻은 아니다.

완전성(completeness): 명제가 참이고 필요한 증거를 가진 증명자와 확인자가 절차를 정직하게 수행하면 확인자가 증명을 받아들일 수 있어야 한다. **정당한 증명이 정상적으로 수락**되는 성질로, 거짓 증명을 막는 건실성과 구별된다.

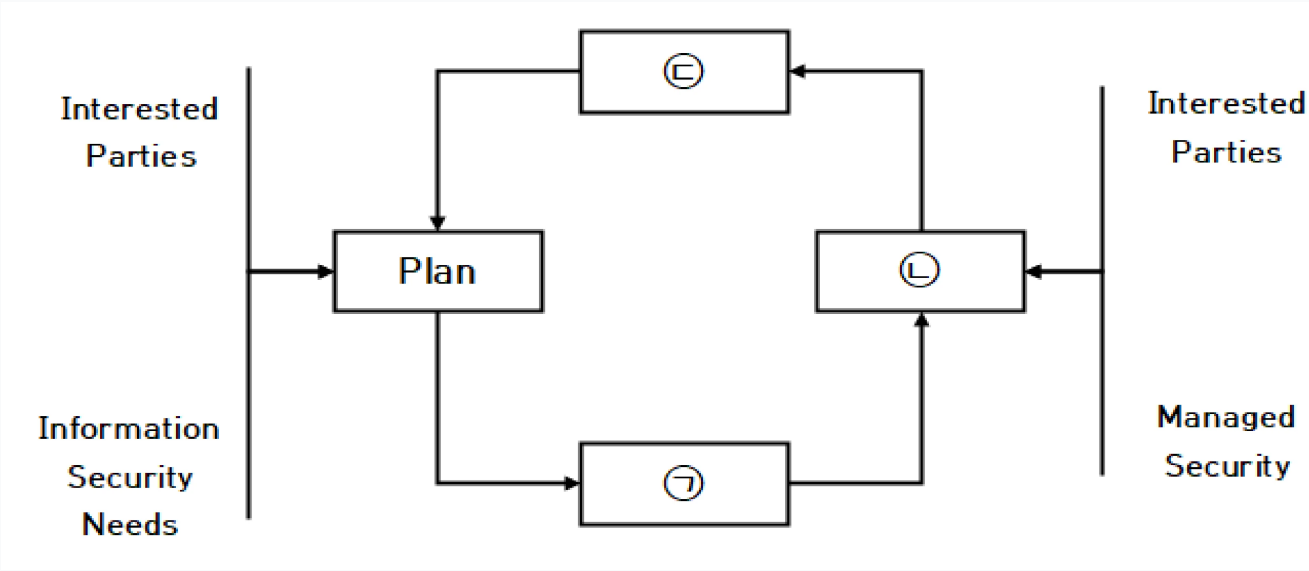
영지식성(zero-knowledge): 확인자가 증명 과정에서 **명제의 참 여부를 넘어서는 비밀 정보를 얻지 못하도록** 해야 한다. 비밀을 감춘 채 검증에 필요한 사실만 확인하게 한다는 지문의 목적에 해당한다.

무작위성(randomness): 난수는 도전값 생성이나 비밀 정보 은닉 등 실제 프로토콜 구현에 활용될 수 있다. 그러나 이 문항이 묻는 영지식 증명의 표준적인 세 기본 성질은 건실성·완전성·영지식성이며, **무작위성은 그 세 성질에 포함되지 않는다**. 난수가 불필요하거나 사용되면 안 된다는 뜻은 아니다.

따라서 기본 성질로 가장 적절하지 않은 항목은 ④ 무작위성이다.

NoteBase

문 6. 다음은 IT 보안관리 프로세스에 관한 그림이다. ㉠~㉢에 해당하는 내용으로 가장 적절한 것은?



① ㉠: 프로세스 성과평가 및 결과 경영자 검토, ㉡: 정보 보안 위험 관리 유지보수 및 개선, ㉢: 위험 처리 계획의 이행

② ㉠: 프로세스 성과평가 및 결과 경영자 검토, ㉡: 위험 처리 계획의 이행, ㉢: 정보 보안 위험 관리 유지보수 및 개선

③ ㉠: 위험 처리 계획의 이행, ㉡: 프로세스 성과평가 및 결과 경영자 검토, ㉢: 정보 보안 위험 관리 유지보수 및 개선

④ ㉠: 위험 처리 계획의 이행, ㉡: 정보 보안 위험 관리 유지보수 및 개선, ㉢: 프로세스 성과평가 및 결과 경영자 검토

정답 3번

간단한 해설

계획 다음에는 **위험 처리 계획을 이행**하고, 그 실행 성과를 평가·검토해야 개선할 부분을 알 수 있다. 개선 결과가 다시 계획에 반영되므로 그림은 지속적으로 순환하는 PDCA 과정을 나타낸다.

NoteBase

올바른 순서

Plan → ㉠ 위험 처리 계획의 이행(Do) → ㉡ 프로세스 성과평가 및 결과 경영자 검토(Check) → ㉢ 정보 보안 위험 관리 유지보수 및 개선(Act)

Plan: 그림 왼쪽의 계획 단계이다. 양옆의 'Interested Parties'는 이해관계자를 뜻하며, 왼쪽의 'Information Security Needs'는 계획에 반영할 정보보안 요구이다. 조직의 요구와 위험을 검토하여 보안 목표와 위험 처리 계획을 세운다. **실행할 목표와 방법을 먼저 정해야** 다음 단계에서 이를 이행할 수 있다.

㉠ Do: Plan에서 아래쪽 ㉠으로 향하는 화살표는 수립한 계획의 실행을 뜻한다. 이에 해당하는 내용은 '위험 처리 계획의 이행'이다. 선정한 보호대책을 실제로 적용·운영하여 **계획을 실행 결과로 바꾸는** 단계이다.

㉡ Check: 아래쪽 ㉠에서 오른쪽 ㉡으로 올라가는 화살표를 따라 실행 이후의 점검 단계가 이어진다. '프로세스 성과평가 및 결과 경영자 검토'가 이에 해당한다. 오른쪽에 표시된 'Managed Security'는 관리되는 보안 상태를 가리키며, 이 단계에서는 **실행 성과를 목표와 비교**하고 그 결과를 경영자가 검토하여 문제점과 개선 필요를 확인한다.

㉢ Act: 오른쪽 ㉡에서 위쪽 ㉢으로 연결되므로 성과 검토 뒤에 이루어지는 '정보 보안 위험 관리 유지보수 및 개선'이다. **점검에서 확인한 문제를 개선에 반영**하고 관리체계를 유지한다. 위쪽 ㉢에서 왼쪽 Plan으로 되돌아가는 화살표는 개선 결과가 다음 계획에 반영되는 지속적 순환을 나타낸다.

NoteBase

문 7. 클라우드보안인증제에 관한 설명으로 가장 적절하지 않은 것은?

① 클라우드서비스 제공자가 제공하는 서비스에 대해 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제23조의2에 따라 정보보호 수준의 향상 및 보장을 위하여 보안인증기준에 적합한 클라우드컴퓨팅서비스에 대하여 보안인증을 수행하는 제도이다.

② 클라우드서비스 보안인증 유형은 IaaS, SaaS, DaaS가 있으며 유효기간은 모두 5년이고, 클라우드서비스 보안인증 등급은 상·중·하로 구분된다. 인증평가 종류는 최초평가, 사후평가, 갱신평가로 나뉜다.

③ 클라우드서비스 보안인증체계에서 정책기관은 한국인터넷진흥원, 인증기관은 과학기술정보통신부, 평가기관은 한국인터넷진흥원 및 과학기술정보통신부에서 지정한 기관, 그리고 공공부문 기술자문기관은 국가보안기술연구소에서 그 역할을 수행한다.

④ 클라우드 인증자 정보유출은 클라우드 서비스를 이용·제공하는 과정에서 관리되는 이용자 관련 정보가 제3자의 악의적인 침입 또는 클라우드 서비스 제공자·이용자의 보안 관리 이슈 등으로 외부에 유출된 경우를 의미한다.

정답 3번

①

클라우드보안인증은 **정보보호 수준의 향상 및 보장**을 목적으로, **보안인증기준에 적합한 클라우드컴퓨팅서비스**에 인증을 부여하는 제도이다.

클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제23조의2(클라우드컴퓨팅서비스의 보안인증)
① 과학기술정보통신부장관은 정보보호 수준의 향상 및 보장을 위하여 보안인증기준에 적합한 클라우드컴퓨팅서비스에 대하여 대통령령으로 정하는 바에 따라 인증(이하 "보안인증"이라 한다)을 할 수 있다.

②

보안인증 유형에는 **IaaS·SaaS·DaaS**가 있으며, **유효기간은 모두 5년**이다. 등급은 **상·중·하**로 구분한다. 처음 인증받을 때의 **최초평가**, 인증 후 매년 실시하는 **사후평가**, 유효기간 만료 전 연장을 위한 **갱신평가**가 있다.

클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 시행령 제15조의7(보안인증의 유효기간 등)
① 법 제23조의2제2항에 따른 보안인증의 유효기간은 5년으로 한다.

NoteBase

③

보안인증체계에서 **정책기관은 과학기술정보통신부, 인증기관은 한국인터넷진흥원**이다. 선지는 두 기관의 역할을 뒤바꾸었다.

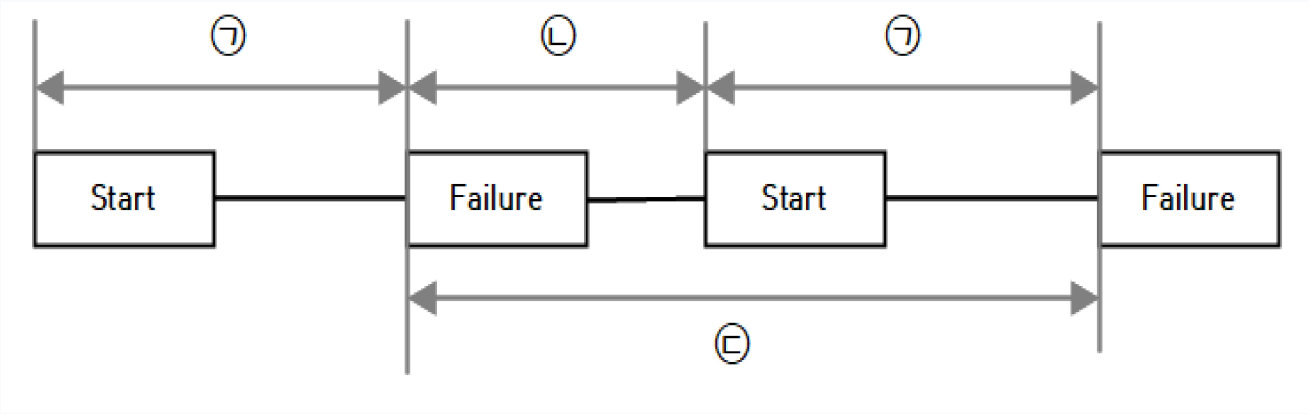
클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제23조의2(클라우드컴퓨팅서비스의 보안인증)
⑤ 과학기술정보통신부장관은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제52조에 따른 한국인터넷진흥원 또는 대통령령에 따라 과학기술정보통신부장관이 지정한 기관(이하 "인증기관"이라 한다)으로 하여금 보안인증에 관한 업무로서 다음 각 호의 업무를 수행하게 할 수 있다.
1. 보안인증기준에 적합한지 여부를 확인하기 위한 평가(이하 "인증평가"라 한다)
2. 인증평가 결과의 심의
3. 보안인증서의 발급 · 관리
4. 보안인증의 사후관리
5. 보안인증평가원의 양성 및 자격관리
6. 그 밖에 보안인증에 관한 업무

④

클라우드 인증자 정보유출에는 **외부 침입에 따른 유출뿐 아니라 제공자·이용자의 보안 관리상 문제로 발생한 유출**도 포함된다. 유출 대상은 개인정보에 한정되지 않고 클라우드에서 생산·저장·관리하는 이용자 정보 전반이다.

NoteBase

문 8. 다음은 하드웨어 백업 관리를 위한 가용성에 관한 그림이다. ㉠~㉢에 해당하는 용어로 가장 적절한 것은?



① ㉠: MTTR, ㉡: MTTF, ㉢: MTBF

② ㉠: MTTR, ㉡: MTBF, ㉢: MTTF

③ ㉠: MTTF, ㉡: MTBF, ㉢: MTTR

④ ㉠: MTTF, ㉡: MTTR, ㉢: MTBF

정답 4번

간단한 해설

Start에서 Failure까지는 **고장 전 정상 가동 시간**, Failure에서 다음 Start까지는 **고장 후 수리 시간**이다. 두 Failure 사이를 잇는 긴 화살표는 이 두 구간을 합한 고장 간격을 나타낸다.

NoteBase

도식 해설

Start는 가동 시작 또는 수리 후 재가동, Failure는 고장 발생 시점이다. 그림의 화살표가 어느 두 시점을 잇는지 구분하면 된다. 각 용어의 Mean은 여러 관측에서 구한 평균을 뜻하며, 그림은 그 평균의 대상이 되는 구간을 보여준다.

㉠: Start에서 Failure까지의 **정상 가동 구간**이다. 가동을 시작한 뒤 고장에 이르기까지의 평균 시간이므로 MTTF(Mean Time To Failure, 평균 고장 도달 시간)에 해당한다. 고장 난 뒤 복구하는 구간과 구별한다.

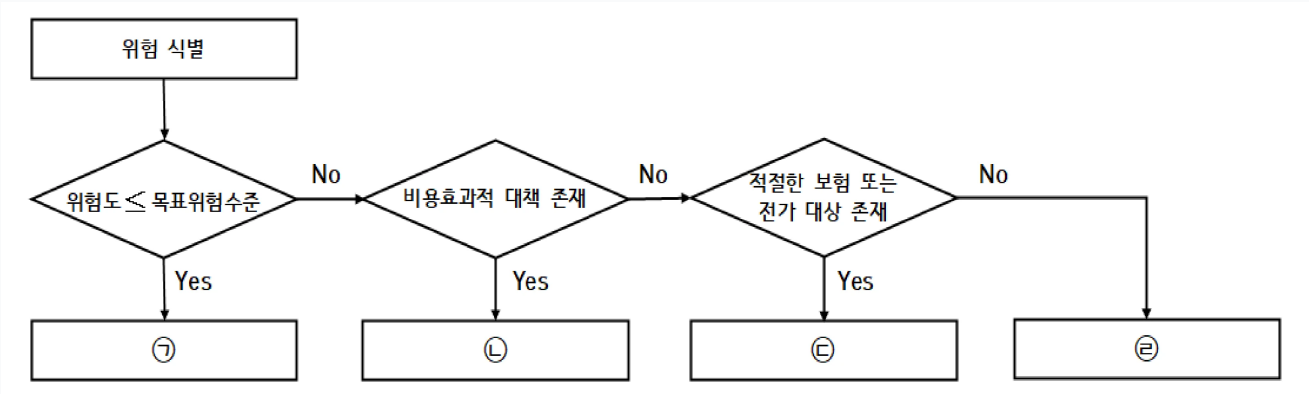
㉡: Failure에서 다음 Start까지의 **고장 후 수리·복구 구간**이다. 고장을 고쳐 정상 가동 상태로 되돌리는 데 걸리는 평균 시간이므로 MTTR(Mean Time To Repair, 평균 수리 시간)에 해당한다.

㉢: 한 Failure에서 다음 Failure까지 이어지는 구간으로, 중간의 **수리 시간과 재가동 후 정상 가동 시간**을 모두 포함한다. 이 그림처럼 고장 사이의 전체 경과 시간을 쓰는 정의에서는 MTBF(Mean Time Between Failures, 평균 고장 간격)이며, MTBF = MTTR + MTTF의 관계가 성립한다.

따라서 ㉠은 MTTF, ㉡은 MTTR, ㉢은 MTBF로 대응되는 ④이다.

NoteBase

문 9. 다음은 위험처리 방법에 관한 그림이다. ㉠~㉣에 해당하는 내용으로 가장 적절한 것은?



① ㉠은 현재의 위험을 받아들이고 잠재적 손실 비용을 감수하는 것이다.

② ㉡은 위험이 존재하는 프로세스나 사업을 수행하지 않고 포기하는 것이다.

③ ㉢은 위험 수준을 낮추는 대책으로 위험 결과를 낮추는 대책과 위험 발생 가능성을 낮추는 대책으로 나눌 수 있다.

④ ㉣은 위험에 대비하여 보험을 들거나, 다른 기관과 계약을 맺거나, 또는 위협이 발생시키는 위험과 비용을 공유하는 협력 관계나 공동 벤처 구조를 활용하는 것이다.

정답 1번

간단한 해설

그림에서 위험도가 **목표위험수준 이하**이면 위험 수용인 ㉠으로 간다. 이후 분기는 비용효과적인 대책이 있으면 감소, 보험·전가 대상이 있으면 전가, 모두 없으면 회피를 나타낸다.

NoteBase

선지별 해설

① O: ㉠은 위험 수용이다. 그림에서 **위험도가 목표위험수준 이하**이면 이 경로로 가므로, 현재 위험을 받아들이고 발생할 수 있는 손실 비용을 감수한다.

② X: ㉡은 **비용효과적인 대책이 존재**할 때 선택하는 위험 감소이다. 대책을 적용해 사고 가능성이나 피해 규모를 낮춘다. 사업이나 프로세스를 포기하는 것은 위험 회피로, 그림의 ㉣에 해당한다.

③ X: ㉢은 **적절한 보험 또는 전가 대상이 존재**할 때 선택하는 위험 전가이다. 보험이나 계약 등을 통해 위험에 따른 부담을 다른 주체에게 이전한다. 발생 가능성이나 결과를 낮추는 대책은 위험 감소로, ㉡에 해당한다.

④ X: ㉣은 그림에서 목표위험수준을 넘는 위험에 대해 비용효과적인 대책도, 적절한 보험·전가 대상도 없는 경로이므로 위험 회피에 해당한다. **위험을 유발하는 활동을 중단하거나 포기**하는 방식이다. 선지의 보험·계약·비용 공유는 전가 또는 공유에 관한 설명으로, 그림에서는 ㉢에 대응한다.

따라서 그림의 ㉠을 위험 수용으로 설명한 ①이다.

NoteBase

문 10. 정보보호등급제에 관한 설명으로 가장 적절하지 않은 것은?

① 정보보호 관리체계(ISMS)를 유지하는 기업 대상으로 정보보호 수준을 측정하여 '우수', '최우수' 등급을 부여하는 제도이다.

② 산업계, 학계 등 관련 전문가 10명 이내로 인증위원회를 구성하여 인증결과를 심의하고, 인증심사팀은 ISMS 인증심사원 양성교육을 수료하고 자격요건을 갖춘 자들로 구성한다.

③ 인증제도의 객관성 및 신뢰성 확보를 위해 정책기관과 인증위원회를 통합하여 운영하고, 인증제도를 관리·감독하는 정책기관은 한국인터넷진흥원이 직접 수행한다.

④ 정보보호등급제는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 및 동법 시행령, 그리고 「정보보호 관리등급 부여에 관한고시」의 법적 근거를 갖는다.

정답 3번

①

정보보호 관리체계 인증을 연속 3년간 유지한 기업의 정보보호 수준을 평가하여 **우수·최우수 등급을 부여**한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제47조의5(정보보호 관리등급 부여)
① 제47조에 따라 정보보호 관리체계 인증을 받은 자는 기업의 통합적 정보보호 관리수준을 제고하고 이용자로부터 정보보호 서비스에 대한 신뢰를 확보하기 위하여 과학기술정보통신부장관으로부터 정보보호 관리등급을 받을 수 있다. <개정 2013.3.23, 2017.7.26>

②

인증결과를 심의하는 위원회는 **산업계·학계 등의 관련 전문가 10명 이내**로 구성한다. 심사팀은 **ISMS 인증심사원 양성교육을 수료하고 필요한 자격요건을 갖춘 사람**으로 구성한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제55조의3(정보보호 관리등급 부여의 방법 및 절차)
③ 제2항에 따른 심사는 인증심사원만 수행할 수 있다.

NoteBase

③

객관성과 신뢰성을 확보하기 위해 **정책기관과 인증위원회를 분리**하여 운영한다. 정책기관은 **과학기술정보통신부**이고, 한국인터넷진흥원은 인증기관으로서 등급제 운영과 심사를 수행한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제47조의5(정보보호 관리등급 부여)
① 제47조에 따라 정보보호 관리체계 인증을 받은 자는 기업의 통합적 정보보호 관리수준을 제고하고 이용자로부터 정보보호 서비스에 대한 신뢰를 확보하기 위하여 과학기술정보통신부장관으로부터 정보보호 관리등급을 받을 수 있다. <개정 2013.3.23, 2017.7.26>
② 과학기술정보통신부장관은 한국인터넷진흥원으로 하여금 제1항에 따른 등급 부여에 관한 업무를 수행하게 할 수 있다. <개정 2013.3.23, 2017.7.26>

④

정보통신망법이 정보보호 관리등급 부여의 근거를 두고, **시행령과 정보보호 관리등급 부여에 관한 고시가 심사기준·방법·절차를 구체화**한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제47조의5(정보보호 관리등급 부여)
① 제47조에 따라 정보보호 관리체계 인증을 받은 자는 기업의 통합적 정보보호 관리수준을 제고하고 이용자로부터 정보보호 서비스에 대한 신뢰를 확보하기 위하여 과학기술정보통신부장관으로부터 정보보호 관리등급을 받을 수 있다. <개정 2013.3.23, 2017.7.26>
⑤ 제1항에 따른 등급 부여의 심사기준 및 등급 부여의 방법 · 절차 · 수수료, 등급의 유효기간, 제4항에 따른 등급취소의 방법 · 절차, 그 밖에 필요한 사항은 대통령령으로 정한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제55조의2(정보보호 관리등급 부여의 심사기준)
② 제1항에 따른 심사기준별 세부 평가기준 및 평가방법 등에 관하여 필요한 사항은 과학기술정보통신부장관이 정하여 고시한다. <개정 2013.3.23, 2017.7.26>

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제55조의3(정보보호 관리등급 부여의 방법 및 절차)
⑤ 제1항부터 제4항까지에서 규정한 사항 외에 정보보호 관리등급 부여의 신청 · 심사 및 정보보호 관리등급 증명서의 발급 등에 필요한 세부사항은 과학기술정보통신부장관이 정하여 고시한다. <개정 2013.3.23, 2017.7.26>

NoteBase

문 11. 「정보통신기반 보호법 시행령」 제9조의3(주요정보통신기반시설보호대책 이행 여부 확인 결과 보고 등)에 따를 때 주요정보통신기반시설보호대책의 이행 여부 확인 결과를 정보통신기반보호위원회에 보고하여야 하는 주체에 해당하는 것만을 모두 고른 것은?

㉠ 국방부장관
㉡ 국가정보원장
㉢ 행정안전부장관
㉣ 한국인터넷진흥원장
㉤ 과학기술정보통신부장관

① ㉠㉡㉤
② ㉠㉡㉢
③ ㉡㉣㉤
④ ㉢㉣㉤

정답 1번

㉠

국방부장관은 주요정보통신기반시설보호대책의 이행 여부 확인 결과를 **정보통신기반보호위원회에 보고해야 하는 주체**이다.

정보통신기반 보호법 시행령 제9조의3(주요정보통신기반시설보호대책 이행 여부 확인 결과 보고 등)
① 과학기술정보통신부장관, 국가정보원장 및 국방부장관은 법 제5조의2에 따른 주요정보통신기반시설보호대책의 이행 여부 확인 결과를 위원회에 보고하여야 한다. <개정 2013.3.23, 2017.7.26>

㉡

국가정보원장은 주요정보통신기반시설보호대책의 이행 여부 확인 결과를 **정보통신기반보호위원회에 보고해야 하는 주체**이다.

정보통신기반 보호법 시행령 제9조의3(주요정보통신기반시설보호대책 이행 여부 확인 결과 보고 등)
① 과학기술정보통신부장관, 국가정보원장 및 국방부장관은 법 제5조의2에 따른 주요정보통신기반시설보호대책의 이행 여부 확인 결과를 위원회에 보고하여야 한다. <개정 2013.3.23, 2017.7.26>

NoteBase

㉣

이행 여부 확인 결과의 보고 의무자는 **과학기술정보통신부장관·국가정보원장·국방부장관**이며,
행정안전부장관은 포함되지 않는다.

정보통신기반 보호법 시행령 제9조의3(주요정보통신기반시설보호대책 이행 여부 확인 결과 보고 등)
① 과학기술정보통신부장관, 국가정보원장 및 국방부장관은 법 제5조의2에 따른
주요정보통신기반시설보호대책의 이행 여부 확인 결과를 위원회에 보고하여야 한다. <개정 2013.3.23, 2017.7.26>

㉤

이행 여부 확인 결과의 보고 의무자는 **과학기술정보통신부장관·국가정보원장·국방부장관**이며,
한국인터넷진흥원장은 포함되지 않는다.

정보통신기반 보호법 시행령 제9조의3(주요정보통신기반시설보호대책 이행 여부 확인 결과 보고 등)
① 과학기술정보통신부장관, 국가정보원장 및 국방부장관은 법 제5조의2에 따른
주요정보통신기반시설보호대책의 이행 여부 확인 결과를 위원회에 보고하여야 한다. <개정 2013.3.23, 2017.7.26>

㉥

과학기술정보통신부장관은 주요정보통신기반시설보호대책의 이행 여부 확인 결과를
정보통신기반보호위원회에 보고해야 하는 주체이다.

정보통신기반 보호법 시행령 제9조의3(주요정보통신기반시설보호대책 이행 여부 확인 결과 보고 등)
① 과학기술정보통신부장관, 국가정보원장 및 국방부장관은 법 제5조의2에 따른
주요정보통신기반시설보호대책의 이행 여부 확인 결과를 위원회에 보고하여야 한다. <개정 2013.3.23, 2017.7.26>

NoteBase

문 12. 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 시행령」 제17조(통지의 내용 및 방법)에 따를 때, 클라우드컴퓨팅 서비스를 제공하는 자는 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제25조 제1항의 침해사고 등이 발생한 경우 지체 없이 사용자에게 해당 내용을 통지해야 하지만 ( )을/를 바로 알기 어려운 경우에는 나머지 사항을 먼저 알리고 ( )이/가 확인되면 지체 없이 해당 이용자에게 통지해야 한다. ( )에 공통으로 들어갈 것으로 가장 적절한 것은?

① 발생 원인

② 발생 내용

③ 담당부서 및 연락처

④ 클라우드컴퓨팅서비스 제공자의 피해 확산 방지 조치 현황

정답 1번

공통 해설

침해사고 등의 발생 원인을 바로 알기 어려운 경우에도 통지를 미룰 수 없으며, **나머지 사항을 먼저 알리고 원인이 확인되면 지체 없이 추가 통지**해야 한다.

클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 시행령 제17조(통지의 내용 및 방법)
① 클라우드컴퓨팅서비스를 제공하는 자(이하 "클라우드컴퓨팅서비스 제공자"라 한다)는 법 제25조제1항 각 호의 어느 하나에 해당하는 경우에는 지체 없이 다음 각 호의 사항을 해당 이용자에게 알려야 한다. 다만, 제2호의 발생 원인을 바로 알기 어려운 경우에는 나머지 사항을 먼저 알리고, 발생 원인이 확인되면 지체 없이 해당 이용자에게 알려야 한다.
1. 발생 내용
2. 발생 원인
3. 클라우드컴퓨팅서비스 제공자의 피해 확산 방지 조치 현황
4. 클라우드컴퓨팅서비스 이용자(이하 "이용자"라 한다)의 피해 예방 또는 확산 방지 방법
5. 담당부서 및 연락처

NoteBase

문 13. 다음은 「가명정보의 결합 및 반출 등에 관한 고시」 제2조 (정의)의 일부 내용이다. ㉠, ㉡에 들어갈 내용으로 가장 적절한 것은?

2. “결합키”란 결합 대상인 가명정보의 일부로서 해당 정보만으로는 특정 개인을 알아볼 수 없으나 다른 결합 대상 정보와 구별할 수 있도록 조치한 정보를 말한다.
3. “결합키연계정보”란 결합키가 (㉠) 정보를 결합할 수 있도록 (㉡) 결합신청자의 결합키를 연계한 정보를 말한다.

① ㉠: 동일한, ㉡: 동일한

② ㉠: 동일한, ㉡: 서로 다른

③ ㉠: 서로 다른, ㉡: 동일한

④ ㉠: 서로 다른, ㉡: 서로 다른

정답 2번

③

결합키연계정보는 **결합키가 동일한 정보**를 결합할 수 있도록 **서로 다른 결합신청자의 결합키를 연계한 정보**이다.

가명정보의 결합 및 반출 등에 관한 고시 제2조(정의) 이 고시에서 사용하는 용어의 정의는 다음과 같다.
3. "결합키연계정보"란 결합키가 동일한 정보를 결합할 수 있도록 서로 다른 결합신청자의 결합키를 연계한 정보를 말한다.

NoteBase

문 14. 다음은 「개인정보 보호법 시행령」 제30조(개인정보의 안전성 확보 조치)의 일부 내용이다. ㉠~㉤ 중 적절하지 않은 것만을 모두 고른 것은?

2. 개인정보에 대한 접근 권한을 제한하기 위한 다음 각 목의 조치
가. ㉠ 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템(이하 “개인정보처리시스템”이라 한다)에 대한 접근 권한의 부여·변경·말소 등에 관한 기준의 수립·시행
나. ㉡ 정당한 권한을 가진 자에 의한 접근인지 를 확인하기 위해 필요한 인가수단 적용 기준의 설정 및 운영
다. 그 밖에 개인정보에 대한 접근 권한을 제한하기 위하여 필요한 조치
3. 개인정보에 대한 접근을 통제하기 위한 다음 각 목의 조치
가. ㉢ 개인정보처리시스템에 대한 침입을 탐지하고 차단하기 위하여 필요한 조치
나. ㉣ 개인정보처리시스템에 접속하는 정보주체의 컴퓨터 등으로서 보호위원회가 정하여 고시하는 기준에 해당하는 컴퓨터 등에 대한 인터넷망의 차단. 다만, ㉤ 전년도 말 기준 직전 3개월 간 그 개인정보가 저장·관리되고 있는 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제2조제1항제4호에 따른 이용자 수가 일일평균 100만명 이상인 개인정보처리자만 해당한다.
다. 그 밖에 개인정보에 대한 접근을 통제하기 위하여 필요한 조치
4. 개인정보를 안전하게 저장·전송하는데 필요한 다음 각 목의 조치
가. ㉥ 비밀번호의 양방향 암호화 저장 등 인증정보의 암호화 저장 또는 이에 상응하는 조치

① ㉠㉡㉤
② ㉠㉢㉣
③ ㉡㉣㉥
④ ㉢㉤㉥

정답 3번

㉠
개인정보에 대한 접근 권한을 제한하기 위해 **개인정보처리시스템 접근 권한의 부여·변경·말소 등에 관한 기준을 수립·시행**해야 한다.

개인정보 보호법 시행령 제30조(개인정보의 안전성 확보 조치)
① 개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 해야 한다. <개정 2023.9.12>
2. 개인정보에 대한 접근 권한을 제한하기 위한 다음 각 목의 조치
가. 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템(이하 "개인정보처리시스템"이라 한다)에 대한 접근 권한의 부여 · 변경 · 말소 등에 관한 기준의 수립 · 시행

NoteBase

㉡

정당한 권한을 가진 자의 접근인지를 확인하기 위해 설정·운영해야 하는 것은 인가수단이 아니라 **인증수단의 적용 기준**이다.

개인정보 보호법 시행령 제30조(개인정보의 안전성 확보 조치)
① 개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 해야 한다. <개정 2023.9.12>
2. 개인정보에 대한 접근 권한을 제한하기 위한 다음 각 목의 조치
나. 정당한 권한을 가진 자에 의한 접근인지를 확인하기 위해 필요한 인증수단 적용 기준의 설정 및 운영

㉢

개인정보에 대한 접근을 통제하기 위해 **개인정보처리시스템에 대한 침입을 탐지하고 차단하는 데 필요한 조치**를 해야 한다.

개인정보 보호법 시행령 제30조(개인정보의 안전성 확보 조치)
① 개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 해야 한다. <개정 2023.9.12>
3. 개인정보에 대한 접근을 통제하기 위한 다음 각 목의 조치
가. 개인정보처리시스템에 대한 침입을 탐지하고 차단하기 위하여 필요한 조치

㉣

인터넷망 차단 대상은 정보주체의 컴퓨터가 아니라, **개인정보처리시스템에 접속하는 개인정보취급자의 컴퓨터 등 중 보호위원회 고시 기준에 해당하는 것**이다.

개인정보 보호법 시행령 제30조(개인정보의 안전성 확보 조치)
① 개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 해야 한다. <개정 2023.9.12>
3. 개인정보에 대한 접근을 통제하기 위한 다음 각 목의 조치
나. 개인정보처리시스템에 접속하는 개인정보취급자의 컴퓨터 등으로서 보호위원회가 정하여 고시하는 기준에 해당하는 컴퓨터 등에 대한 인터넷망의 차단. 다만, 전년도 말 기준 직전 3개월 간 그 개인정보가 저장 · 관리되고 있는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제4호에 따른 이용자 수가 일일평균 100만명 이상인 개인정보처리자만 해당한다.

NoteBase

ⓓ

이 인터넷망 차단 의무는 **전년도 말 기준 직전 3개월간 해당 개인정보가 저장·관리되는 정보통신망의 이용자 수가 일일평균 100만명 이상인 개인정보처리자**에게만 적용된다.

개인정보 보호법 시행령 제30조(개인정보의 안전성 확보 조치)
① 개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 해야 한다. <개정 2023.9.12>
3. 개인정보에 대한 접근을 통제하기 위한 다음 각 목의 조치
나. 개인정보처리시스템에 접속하는 개인정보취급자의 컴퓨터 등으로서 보호위원회가 정하여 고시하는 기준에 해당하는 컴퓨터 등에 대한 인터넷망의 차단. 다만, 전년도 말 기준 직전 3개월 간 그 개인정보가 저장 · 관리되고 있는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제4호에 따른 이용자 수가 일일평균 100만명 이상인 개인정보처리자만 해당한다.

ⓑ

비밀번호는 양방향이 아닌 **일방향 암호화로 저장**하는 등 인증정보의 암호화 저장 또는 이에 상응하는 조치를 해야 한다.

개인정보 보호법 시행령 제30조(개인정보의 안전성 확보 조치)
① 개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 해야 한다. <개정 2023.9.12>
4. 개인정보를 안전하게 저장 · 전송하는데 필요한 다음 각 목의 조치
가. 비밀번호의 일방향 암호화 저장 등 인증정보의 암호화 저장 또는 이에 상응하는 조치

NoteBase

문 15. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제4조의2 (합성영상등으로 인한 피해 예방을 위한 시책)에 따를 때 인공지능 기술을 이용하여 사람의 얼굴·신체 또는 음성을 대상으로 한 촬영물·영상물 또는 음성물을 대상자의 의사에 반하여 편집·합성 또는 가공한 정보의 무분별한 유통으로 인한 성범죄, 명예훼손 또는 사기 등의 피해를 예방하기 위하여 시책을 마련해야 하는 주체에 해당하는 것만을 모두 고른 것은?

㉠ 행정안전부장관
㉡ 개인정보보호위원회
㉢ 방송미디어통신위원회
㉣ 과학기술정보통신부장관

① ㉠㉡
② ㉠㉣
③ ㉡㉢
④ ㉢㉣

정답 4번

㉠

합성영상등의 무분별한 유통으로 인한 피해 예방 시책을 마련할 주체는 **과학기술정보통신부장관과 방송미디어통신위원회**이다. 행정안전부장관은 이 시책의 마련 주체에 포함되지 않는다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제4조의2(합성영상등으로 인한 피해 예방을 위한 시책)
① 과학기술정보통신부장관과 방송미디어통신위원회는 인공지능 기술을 이용하여 사람의 얼굴 · 신체 또는 음성을 대상으로 한 촬영물 · 영상물 또는 음성물을 대상자의 의사에 반하여 편집 · 합성 또는 가공한 정보(이하 이 조에서 "합성영상등"이라 한다)의 무분별한 유통으로 인한 성범죄, 명예훼손 또는 사기 등의 피해를 예방하기 위하여 시책을 마련하여야 한다. <개정 2025.10.1>

NoteBase

ㄴ

합성영상등의 무분별한 유통으로 인한 피해 예방 시책을 마련할 주체는 **과학기술정보통신부장관과 방송미디어통신위원회**이다. 개인정보보호위원회는 이 시책의 마련 주체에 포함되지 않는다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제4조의2(합성영상등으로 인한 피해 예방을 위한 시책)
① 과학기술정보통신부장관과 방송미디어통신위원회는 인공지능 기술을 이용하여 사람의 얼굴 · 신체 또는 음성을 대상으로 한 촬영물 · 영상물 또는 음성물을 대상자의 의사에 반하여 편집 · 합성 또는 가공한 정보(이하 이 조에서 "합성영상등"이라 한다)의 무분별한 유통으로 인한 성범죄, 명예훼손 또는 사기 등의 피해를 예방하기 위하여 시책을 마련하여야 한다. <개정 2025.10.1>

ㄷ

방송미디어통신위원회와 과학기술정보통신부장관은 합성영상등의 무분별한 유통으로 인한 성범죄·명예훼손·사기 등의 피해를 예방하기 위한 시책을 마련하여야 한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제4조의2(합성영상등으로 인한 피해 예방을 위한 시책)
① 과학기술정보통신부장관과 방송미디어통신위원회는 인공지능 기술을 이용하여 사람의 얼굴 · 신체 또는 음성을 대상으로 한 촬영물 · 영상물 또는 음성물을 대상자의 의사에 반하여 편집 · 합성 또는 가공한 정보(이하 이 조에서 "합성영상등"이라 한다)의 무분별한 유통으로 인한 성범죄, 명예훼손 또는 사기 등의 피해를 예방하기 위하여 시책을 마련하여야 한다. <개정 2025.10.1>

ㄹ

과학기술정보통신부장관과 방송미디어통신위원회는 합성영상등의 무분별한 유통으로 인한 성범죄·명예훼손·사기 등의 피해를 예방하기 위한 시책을 마련하여야 한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제4조의2(합성영상등으로 인한 피해 예방을 위한 시책)
① 과학기술정보통신부장관과 방송미디어통신위원회는 인공지능 기술을 이용하여 사람의 얼굴 · 신체 또는 음성을 대상으로 한 촬영물 · 영상물 또는 음성물을 대상자의 의사에 반하여 편집 · 합성 또는 가공한 정보(이하 이 조에서 "합성영상등"이라 한다)의 무분별한 유통으로 인한 성범죄, 명예훼손 또는 사기 등의 피해를 예방하기 위하여 시책을 마련하여야 한다. <개정 2025.10.1>

NoteBase

문 16. 다음은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제22조의2(접근권한에 대한 동의)의 일부 내용이다. ㉠, ㉡에 들어갈 용어로 가장 적절한 것은?

제3항 이동통신단말장치의 기본 운영체제(이동통신단말장치에서 소프트웨어를 실행할 수 있는 기반 환경을 말한다)를 제작하여 공급하는 자와 이동통신단말장치 제조업자 및 이동통신단말장치의 소프트웨어를 제작하여 공급하는 자는 (㉠) 제공자가 이동통신단말장치 내에 저장되어 있는 정보 및 (㉡)에 설치된 기능에 접근하려는 경우 접근권한에 대한 이용자의 동의 및 철회방법을 마련하는 등 이용자 정보 보호에 필요한 조치를 하여야 한다.

① ㉠: 정보통신서비스, ㉡: 정보통신서비스

② ㉠: 정보통신서비스, ㉡: 이동통신단말장치

③ ㉠: 이동통신단말장치, ㉡: 정보통신서비스

④ ㉠: 이동통신단말장치, ㉡: 이동통신단말장치

정답 2번

공통 해설

정보통신서비스 제공자가 접근하려는 대상은 이동통신단말장치에 저장된 정보와 **이동통신단말장치에 설치된 기능**이다. 운영체제 공급자·단말장치 제조업자·소프트웨어 공급자는 이용자가 접근권한에 동의하고 이를 철회할 수 있는 방법을 마련하는 등 정보 보호에 필요한 조치를 해야 한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제22조의2(접근권한에 대한 동의)
③ 이동통신단말장치의 기본 운영체제(이동통신단말장치에서 소프트웨어를 실행할 수 있는 기반 환경을 말한다)를 제작하여 공급하는 자와 이동통신단말장치 제조업자 및 이동통신단말장치의 소프트웨어를 제작하여 공급하는 자는 정보통신서비스 제공자가 이동통신단말장치 내에 저장되어 있는 정보 및 이동통신단말장치에 설치된 기능에 접근하려는 경우 접근권한에 대한 이용자의 동의 및 철회방법을 마련하는 등 이용자 정보 보호에 필요한 조치를 하여야 한다.

NoteBase

문 17. 「위치정보의 보호 및 이용 등에 관한 법률 시행령」 제20조(위치정보의 관리적·기술적 보호조치)에 따른 관리적 조치로 가장 적절하지 않은 것은?

① 위치정보 보호조치에 대한 정기적인 자체 검사의 실시

② 위치정보 제공사실 등을 기록한 취급대장의 운영·관리

③ 위치정보시스템에 대한 접근사실의 전자적 자동 기록·보존장치의 운영

④ 위치정보 취급자의 의무와 책임을 규정한 취급·관리 절차 및 지침 마련

정답 3번

①

위치정보 보호조치에 대한 정기적인 자체 검사는 **관리적 조치**에 포함된다.

위치정보의 보호 및 이용 등에 관한 법률 시행령 제20조(위치정보의 관리적 · 기술적 보호조치)
① 법 제16조제1항에 따른 관리적 조치에는 다음 각 호의 내용이 포함되어야 한다. <개정 2018.10.16>
5. 위치정보 보호조치에 대한 정기적인 자체 검사의 실시

②

위치정보 제공사실 등을 기록한 취급대장의 운영·관리는 **관리적 조치**에 포함된다.

위치정보의 보호 및 이용 등에 관한 법률 시행령 제20조(위치정보의 관리적 · 기술적 보호조치)
① 법 제16조제1항에 따른 관리적 조치에는 다음 각 호의 내용이 포함되어야 한다. <개정 2018.10.16>
4. 위치정보 제공사실 등을 기록한 취급대장의 운영 · 관리

③

위치정보시스템의 접근사실을 전자적으로 자동 기록·보존하는 장치의 운영은 **기술적 조치**이며, 관리적 조치에 해당하지 않는다.

위치정보의 보호 및 이용 등에 관한 법률 시행령 제20조(위치정보의 관리적 · 기술적 보호조치)
② 법 제16조제1항에 따른 기술적 조치에는 다음 각 호의 내용이 포함되어야 한다. <개정 2022.4.19, 2025.10.1>
3. 위치정보시스템에 대한 접근사실의 전자적 자동 기록 · 보존장치의 운영

NoteBase

④

위치정보 취급자의 의무와 책임을 정한 취급·관리 절차 및 지침 마련은 **관리적 조치**에 포함된다.

위치정보의 보호 및 이용 등에 관한 법률 시행령 제20조(위치정보의 관리적 · 기술적 보호조치)
① 법 제16조제1항에 따른 관리적 조치에는 다음 각 호의 내용이 포함되어야 한다. <개정 2018.10.16>
3. 위치정보 취급자의 의무와 책임을 규정한 취급 · 관리 절차 및 지침 마련

NoteBase

문 18. 「위치정보의 보호 및 이용 등에 관한 법률 시행령」 제30조의 4(국회에의 보고) 제2항에 따를 때 위치정보사업자가 국회 과학기술정보방송통신위원회에 제출해야 하는 자료로 가장 적절하지 않은 것은?

① 개인위치정보를 요청한 긴급구조기관 및 경찰관서

② 긴급구조기관 및 경찰관서의 요청 및 제공의 근거가 되는 해당 규정

③ 긴급구조기관 및 경찰관서에 대하여 개인위치정보를 제공한 건수 및 일시

④ 긴급구조기관 및 경찰관서에 대하여 제공한 개인위치정보의 대상이 되는 전화번호

정답 2번

①

위치정보사업자는 **개인위치정보를 요청한 긴급구조기관 및 경찰관서**에 관한 자료를 국회 과학기술정보방송통신위원회에 제출해야 한다.

위치정보의 보호 및 이용 등에 관한 법률 시행령 제30조의4(국회에의 보고)
② 법 제30조제2항에 따라 위치정보사업자는 국회 과학기술정보방송통신위원회에 다음 각 호의 자료를 매 반기가 종료된 날부터 30일 이내에 제출하여야 한다. <신설 2015.8.3, 2018.10.16>
3. 개인위치정보를 요청한 긴급구조기관 및 경찰관서

②

기관 간 개인위치정보 요청·제공의 근거 규정은 **긴급구조기관 및 경찰관서가 국회 행정안전위원회에 제출하는 자료**이며, 위치정보사업자의 제출 항목에는 포함되지 않는다.

위치정보의 보호 및 이용 등에 관한 법률 시행령 제30조의4(국회에의 보고)
① 법 제30조제2항에 따라 긴급구조기관 및 경찰관서는 국회 행정안전위원회에 다음 각 호의 구분에 따른 자료를 매 반기가 종료된 날부터 30일 이내에 제출하여야 한다. <개정 2015.8.3>
2. 법 제29조제11항에 따른 자료
라. 요청 또는 제공의 근거가 되는 해당 규정
② 법 제30조제2항에 따라 위치정보사업자는 국회 과학기술정보방송통신위원회에 다음 각 호의 자료를 매 반기가 종료된 날부터 30일 이내에 제출하여야 한다. <신설 2015.8.3, 2018.10.16>
1. 긴급구조기관 및 경찰관서에 대하여 개인위치정보를 제공한 건수 및 일시
2. 긴급구조기관 및 경찰관서에 대하여 제공한 개인위치정보의 대상이 되는 전화번호
3. 개인위치정보를 요청한 긴급구조기관 및 경찰관서

NoteBase

③

위치정보사업자는 긴급구조기관 및 경찰관서에 **개인위치정보를 제공한 건수 및 일시**를 국회 과학기술정보방송통신위원회에 제출해야 한다.

위치정보의 보호 및 이용 등에 관한 법률 시행령 제30조의4(국회에의 보고)
② 법 제30조제2항에 따라 위치정보사업자는 국회 과학기술정보방송통신위원회에 다음 각 호의 자료를 매 반기가 종료된 날부터 30일 이내에 제출하여야 한다. <신설 2015.8.3, 2018.10.16>
1. 긴급구조기관 및 경찰관서에 대하여 개인위치정보를 제공한 건수 및 일시

④

위치정보사업자는 긴급구조기관 및 경찰관서에 **제공한 개인위치정보의 대상이 되는 전화번호**를 국회 과학기술정보방송통신위원회에 제출해야 한다.

위치정보의 보호 및 이용 등에 관한 법률 시행령 제30조의4(국회에의 보고)
② 법 제30조제2항에 따라 위치정보사업자는 국회 과학기술정보방송통신위원회에 다음 각 호의 자료를 매 반기가 종료된 날부터 30일 이내에 제출하여야 한다. <신설 2015.8.3, 2018.10.16>
2. 긴급구조기관 및 경찰관서에 대하여 제공한 개인위치정보의 대상이 되는 전화번호

NoteBase

문 19. 「정보보호산업의 진흥에 관한 법률 시행령」 제10조(성능평가의 방법 및 성능평가기관의 지정) 제1항에 따를 때 정보보호제품에 관한 성능평가에 포함되어야 할 사항으로 가장 적절하지 않은 것은?

① 정보보호제품의 시간 및 자원 관련 효율성

② 정보보호제품 평가업무 수행을 위한 운영절차

③ 정보보호제품 운영 시 정보보호 기능 외의 일반기능 처리 성능

④ 정보보호제품의 보안기능 외의 정보보호 관련 주요기능 구현 여부

정답 2번

①

정보보호제품의 **시간 및 자원 관련 효율성**은 성능평가에 반드시 포함되는 사항이다.

정보보호산업의 진흥에 관한 법률 시행령 제10조(성능평가의 방법 및 성능평가기관의 지정)
① 법 제17조제1항에 따른 정보보호제품에 관한 성능평가(이하 "성능평가"라 한다)에는 다음 각 호의 사항에 대한 평가가 포함되어야 한다.
4. 정보보호제품의 시간 및 자원 관련 효율성

②

평가업무 수행을 위한 운영절차는 제품의 성능평가 항목이 아니라 **성능평가기관으로 지정받으려는 법인이 갖추어야 할 요건**이다.

정보보호산업의 진흥에 관한 법률 시행령 제10조(성능평가의 방법 및 성능평가기관의 지정)
① 법 제17조제1항에 따른 정보보호제품에 관한 성능평가(이하 "성능평가"라 한다)에는 다음 각 호의 사항에 대한 평가가 포함되어야 한다.
1. 정보보호제품 보안기능 처리 성능
2. 정보보호제품의 보안기능 외의 정보보호 관련 주요기능 구현 여부
3. 정보보호제품 운영 시 정보보호 기능 외의 일반기능 처리 성능
4. 정보보호제품의 시간 및 자원 관련 효율성
② 과학기술정보통신부장관은 다음 각 호의 기관 또는 단체를 법 제17조제2항에 따른 평가기관(이하 "성능평가기관"이라 한다)으로 지정할 수 있다. <개정 2017.7.26>
2. 다음 각 목의 요건을 모두 갖춘 법인
라. 성능평가대상 정보보호제품의 평가업무 수행을 위한 운영절차

NoteBase

③

정보보호제품 운영 시 **정보보호 기능 외의 일반기능 처리 성능**도 성능평가에 포함된다.

정보보호산업의 진흥에 관한 법률 시행령 제10조(성능평가의 방법 및 성능평가기관의 지정)
① 법 제17조제1항에 따른 정보보호제품에 관한 성능평가(이하 "성능평가"라 한다)에는 다음 각 호의 사항에 대한 평가가 포함되어야 한다.
3. 정보보호제품 운영 시 정보보호 기능 외의 일반기능 처리 성능

④

정보보호제품의 **보안기능 외의 정보보호 관련 주요기능 구현 여부**도 성능평가에 포함된다.

정보보호산업의 진흥에 관한 법률 시행령 제10조(성능평가의 방법 및 성능평가기관의 지정)
① 법 제17조제1항에 따른 정보보호제품에 관한 성능평가(이하 "성능평가"라 한다)에는 다음 각 호의 사항에 대한 평가가 포함되어야 한다.
2. 정보보호제품의 보안기능 외의 정보보호 관련 주요기능 구현 여부

NoteBase

문 20. 다음은 「지능정보화 기본법」 제40조(데이터센터의 구축 및 운영 활성화)의 일부 내용이다. ㉠~㉢에 들어갈 용어로 가장 적절한 것은?

제1항 (㉠)은/는 지능정보서비스의 제공을 위하여 다수의 초연결 지능정보통신기반을 일정한 공간에 집적시켜 통합 운영·관리하는 시설(이하 “데이터센터”라 한다)의 안정적인 운영과 효율적인 제공 등을 위하여 데이터센터의 구축 및 운영 활성화 시책을 수립·시행할 수 있다.
제2항 (㉡)은/는 민간 데이터센터의 구축 및 운영 활성화 시책을 수립·시행하고 이에 필요한 지원을 할 수 있다.
제3항 (㉢)은/는 정부 및 공공 부문의 데이터센터의 구축 및 운영 활성화 시책을 수립·시행하고, 민간 데이터센터를 이용하는 공공기관의 지능정보서비스의 안정성과 신뢰성 등을 높이기 위하여 필요한 지원을 할 수 있다.
제4항 제1항부터 제3항까지의 규정에 따른 시책의 수립·시행과 지원 대상·방법 등에 관하여 필요한 사항은 대통령령으로 정한다.

① ㉠: 정부, ㉡: 과학기술 정보통신부장관, ㉢: 행정안전부장관
② ㉠: 정부, ㉡: 행정안전부장관, ㉢: 과학기술 정보통신부장관
③ ㉠: 과학기술 정보통신부장관, ㉡: 정부, ㉢: 행정안전부장관
④ ㉠: 행정안전부장관, ㉡: 정부, ㉢: 과학기술 정보통신부장관

정답 1번

㉠
데이터센터의 안정적인 운영과 효율적인 제공 등을 위한 구축 및 운영 활성화 시책은 **정부가 수립·시행할 수 있다**.

지능정보화 기본법 제40조(데이터센터의 구축 및 운영 활성화)
① 정부는 지능정보서비스의 제공을 위하여 다수의 초연결지능정보통신기반을 일정한 공간에 집적시켜 통합 운영 · 관리하는 시설(이하 "데이터센터"라 한다)의 안정적인 운영과 효율적인 제공 등을 위하여 데이터센터의 구축 및 운영 활성화 시책을 수립 · 시행할 수 있다.

㉡
과학기술정보통신부장관은 민간 데이터센터의 구축·운영 활성화 시책을 수립·시행하고 필요한 지원을 할 수 있다.

지능정보화 기본법 제40조(데이터센터의 구축 및 운영 활성화)
② 과학기술정보통신부장관은 민간 데이터센터의 구축 및 운영 활성화 시책을 수립 · 시행하고 이에 필요한 지원을 할 수 있다.

NoteBase

ⓒ

행정안전부장관은 정부·공공 부문 데이터센터의 구축·운영 활성화 시책을 수립·시행하며, 민간 데이터센터를 이용하는 공공기관의 지능정보서비스 안정성·신뢰성을 높이기 위한 지원을 할 수 있다.

지능정보화 기본법 제40조(데이터센터의 구축 및 운영 활성화)
③ 행정안전부장관은 정부 및 공공 부문의 데이터센터의 구축 및 운영 활성화 시책을 수립 · 시행하고, 민간 데이터센터를 이용하는 공공기관의 지능정보서비스의 안정성과 신뢰성 등을 높이기 위하여 필요한 지원을 할 수 있다.

NoteBase