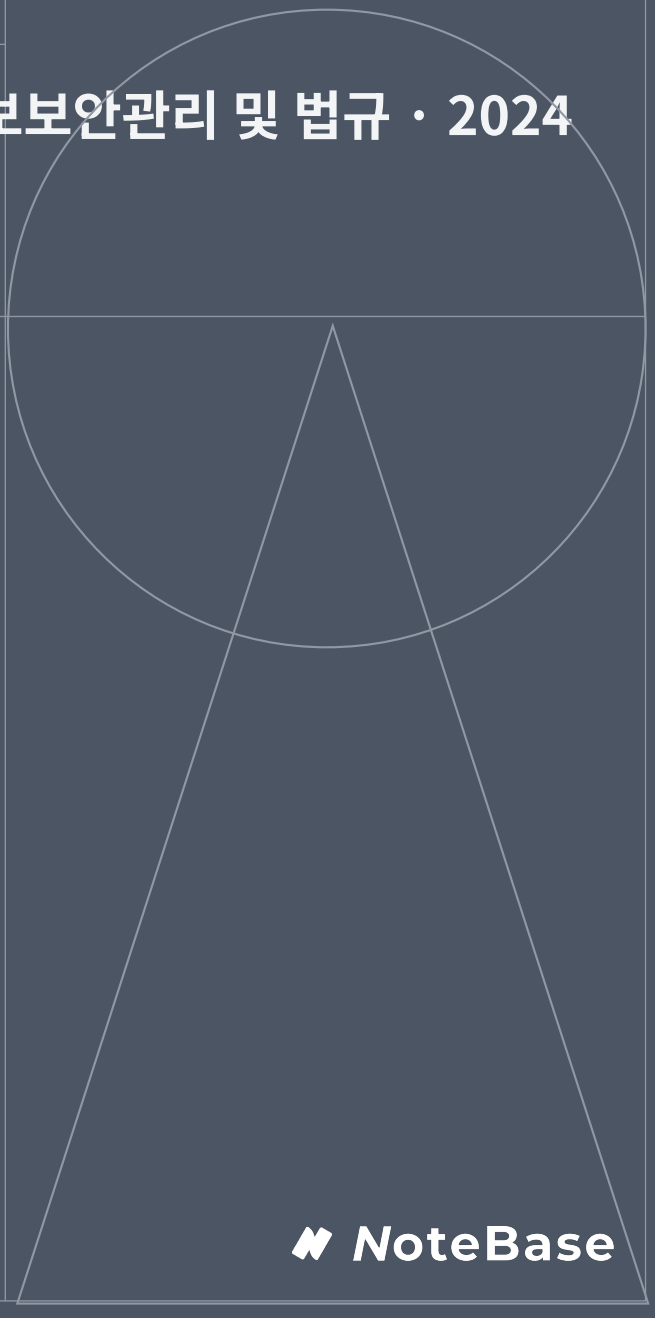
기출OX 해설집

공무원/경찰/경력채용 · 정보보안관리 및 법규 · 2024



NoteBase

기출OX 해설집

공무원/경찰/경력채용 · 정보보안관리 및 법규 · 2024

공무원/경찰/경력채용 · 정보보안관리 및 법규 · 2024

문 1. 다음에서 설명하는 정보보호 목표로 가장 적절한 것은?

정당한 사용자가 서비스를 요청할 때 서비스를 제공할 수 있는 특성으로 정보시스템에 장애가 발생하거나 과부하로 인해 사용할 수 없게 되거나 장시간 기다리게 해서는 안 된다.

① 기밀성
② 무결성
③ 가용성
④ 저장성

정답 3번

간단한 해설

장애나 과부하 때문에 정당한 사용자가 서비스를 이용하지 못하는 상황을 막는 것은 **가용성** 확보이다. 핵심은 정보가 존재하는지보다 필요한 때 실제로 이용할 수 있는지이다.

핵심 풀이

가용성은 정당한 사용자가 필요할 때 정보나 서비스를 **적시에 이용할 수 있는 성질**이다. 지문의 장애·과부하로 인한 이용 불가와 과도한 대기 시간은 모두 서비스의 적시 제공을 방해하므로 가용성 문제이다.

기밀성은 권한 없는 사람에게 정보가 노출되지 않도록 하는 성질이다. 지문의 초점은 정보 유출 여부가 아니라 정당한 사용자의 서비스 이용 가능성이다.

무결성은 정보가 부적절하게 변경되거나 훼손되지 않도록 하는 성질이다. 내용이 변조되지 않았더라도 서비스에 접속할 수 없다면 가용성은 침해될 수 있다.

저장성이라는 표현만으로는 데이터를 보관한 상태와 서비스를 실제로 이용할 수 있는 상태를 구별할 수 없다. 자료가 저장돼 있어도 시스템이 멈추면 요청에 응답하지 못하므로 지문의 목표를 나타내지 못한다.

따라서 지문이 설명하는 목표는 가용성이며 ③에 해당한다.

NoteBase

문 2. 다음은 생체 인식에 이용될 수 있는 이상적인 생체 특징에 관한 내용이다. ㉠~㉣에 해당하는 내용으로 가장 적절한 것은?

㉠ 누구에게나 있는 특성이어야 한다.
㉡ 개인을 구별할 수 있는 고유한 것이어야 한다.
㉢ 시간과 환경의 변화에도 변하지 않고 변경이 불가능한 것이어야 한다.
㉣ 형상을 얻는 것이 용이하고 정량화가 될 수 있어야 한다.

① ㉠: 보편성 (universality), ㉡: 유일성 (uniqueness), ㉢: 영속성 (permanence), ㉣: 획득성 (collectability)

② ㉠: 보편성 (universality), ㉡: 유일성 (uniqueness), ㉢: 획득성 (collectability), ㉣: 영속성 (permanence)

③ ㉠: 유일성 (uniqueness), ㉡: 보편성 (universality), ㉢: 획득성 (collectability), ㉣: 영속성 (permanence)

④ ㉠: 유일성 (uniqueness), ㉡: 보편성 (universality), ㉢: 영속성 (permanence), ㉣: 획득성 (collectability)

정답 1번

간단한 해설

“누구에게나 있음”은 보편성, “개인을 구별함”은 유일성이다. **시간이 지나도 유지되는 성질은 영속성**, 쉽게 얻고 정량화할 수 있는 성질은 획득성이므로 ①의 대응이 맞다.

NoteBase

대응 관계 해설

㉠ 보편성(universality): 생체 인식의 대상이 되는 **누구나 그 특징을 가지고 있어야 한다**는 요구이다. 특징의 존재 여부에 관한 조건이며, 사람마다 특징의 모양이나 값이 같아야 한다는 뜻은 아니다.

㉡ 유일성(uniqueness): 특징에 **사람을 서로 구별할 만큼의 차이**가 있어야 한다는 요구이다. 보편성이 각 사람에게 특징이 있는지를 묻는다면, 유일성은 그 특징으로 다른 사람과 구분할 수 있는지를 묻는다.

㉢ 영속성(permanence): 같은 사람의 특징이 시간이나 환경이 달라져도 **인식에 필요한 안정성을 유지**해야 한다는 요구이다. 지문의 “변하지 않고 변경이 불가능한”은 발문에 명시된 이상적인 성질을 표현한다. 실제 특징이나 측정값이 상처·측정 조건 등에 관계없이 완전히 똑같다는 보장은 아니며, 실무에서는 판별에 충분한 지속성을 본다.

㉣ 획득성(collectability): 센서 등으로 특징을 **쉽게 수집하고 정량적으로 측정**할 수 있어야 한다는 요구이다. 특징이 존재하고 사람마다 달라도 수집하거나 수치화하기 어렵다면 자동 비교에 활용하기 어렵다.

따라서 ㉠ 보편성, ㉡ 유일성, ㉢ 영속성, ㉣ 획득성의 대응이므로 ①과 일치한다.

NoteBase

문 3. 재해발생으로 인해 정상적인 업무가 중단된 경우, 조직 및 기업에 잠재적으로 미치는 영향 및 정량적 피해 규모를 규명하고 비즈니스 측면에서 재해의 위험에 노출되어 있는 정도를 분석하는 것으로 가장 적절한 것은?

① MTD(Maximum Tolerable Downtime)

② RAID(Redundant Array of Inexpensive Disks)

③ BIA(Business Impact Analysis)

④ DRP(Disaster Recovery Planning)

정답 3번

간단한 해설

업무가 중단되었을 때 조직에 어떤 영향과 손실이 생기는지 규명하는 활동은 **업무영향분석(BIA)**이다. 피해 규모와 중요 업무를 파악하여 복구의 우선순위와 필요 수준을 판단하는 근거를 마련한다.

개념 구분

발문의 중심은 재해 자체의 발생 가능성이나 복구 기술이 아니라, **업무 중단이 조직에 미치는 영향과 피해 규모**를 분석하는 데 있다. 이러한 업무영향분석이 ③ BIA이다. 매출 손실처럼 금액으로 평가할 수 있는 피해뿐 아니라 서비스 지연·평판 저하 등도 함께 검토하여 중요 업무와 복구 우선순위를 정하는 근거로 활용한다.

① MTD는 업무 중단이 조직에 중대한 손상을 주기 전까지 감수할 수 있는 **최대 허용 중단시간**이다. 영향 분석 과정에서 판단하는 시간 한계이며, 영향과 손실을 규명하는 분석 활동 자체의 이름은 아니다.

② RAID는 여러 물리 디스크를 배열로 구성하는 **저장장치 기술**이다. 구성 수준에 따라 성능이나 장애 대응 능력을 높일 수 있지만, 기업 전체의 업무 중단 피해를 분석하는 방법은 아니다. 모든 RAID 수준이 장애 복구용 중복성을 제공하는 것은 아니다.

④ DRP는 재해 뒤 정보시스템과 핵심 서비스를 복구할 **절차·자원·역할을 계획**하는 것이다. BIA가 중단의 영향과 복구 필요성을 파악한다면, DRP는 그 결과 등을 바탕으로 실제 복구 방안을 준비한다.

NoteBase

문 4. 다음에서 설명하는 공격으로 가장 적절한 것은?

패스워드별로 생성한 해시값 저장소가 있다. 이 저장소에서 크래킹하고자 하는 해시값을 검색하여 역으로 원래의 패스워드를 찾아내는 방법이다.

① 레이스 컨디션 공격(race condition attack)
② 차분 공격(differential attack)
③ 레인보우 테이블 공격(rainbow table attack)
④ 퍼징 공격(fuzzing attack)

정답 3번

간단한 해설

사전 계산한 해시 자료를 조회하여 대응하는 패스워드 후보를 찾는다는 단서가 핵심이다. 선택지 중 이에 해당하는 것은 ③ 레인보우 테이블 공격이다.

NoteBase

핵심 풀이

핵심 단서: 패스워드 후보에 대한 해시 계산 결과를 미리 준비해 두고 목표 해시에 대응하는 후보를 찾는다는 점이다. 즉, 공격할 때마다 처음부터 모든 후보를 계산하기보다 **사전 계산한 자료를 재사용**한다.

레인보우 테이블의 원리: 해시 함수와 해시값을 다시 패스워드 후보로 바꾸는 환원 함수를 연결해 체인을 만들고, 그 시작점과 끝점 등을 저장하여 검색한다. 중간값을 필요할 때 재계산하므로 **저장 공간과 검색 계산량을 절충**한다. 지문은 이 사전 계산·조회 원리를 간략히 설명한 것으로, 실제 레인보우 테이블을 모든 패스워드와 해시의 쌍을 그대로 저장한 단순 목록과 동일시해서는 안 된다.

해시를 역으로 찾는다는 의미: 해시값에 복호화 함수를 적용하여 원문을 곧바로 되돌리는 것이 아니라, **같은 해시를 만드는 패스워드 후보**를 찾고 확인하는 것이다. 사용한 해시 방식과 후보 범위가 맞아야 하며, 테이블이 다루지 않는 패스워드까지 항상 알아내는 것은 아니다.

다른 선택지와의 구별: ① 레이스 컨디션 공격은 동시 실행의 처리 순서나 시점 차이로 생기는 빈틈을 이용한다.

② 차분 공격은 입력 차이가 출력 차이에 나타나는 통계적 특성을 이용하는 암호 분석이다.

④ 퍼징은 다양하거나 비정상적인 입력을 넣고 오류·충돌 등 반응을 관찰하여 취약점을 찾는 기법이다. 이들은 지문의 사전 계산된 해시 자료 조회와 구별된다.

따라서 제시된 선택지 중 사전 계산 자료를 이용한 패스워드 해시 탐색에 해당하는 것은 ③ 레인보우 테이블 공격이다.

NoteBase

문 5. 위험분석 유형과 접근방법에 관한 설명으로 가장 적절하지 않은 것은?

① 델파이법-분석을 수행하는 개개인들의 지식과 전문성을 활용하여, 토론을 통해 정보시스템이 직면한 다양한 위협과 취약점을 분석하는 방법이다.

② 상세위험분석-비정형화된 프로세스를 사용하여 자산의 식별, 위협 및 취약점 분석을 통해 위험을 분석하는 방법이다.

③ 기준선 접근법-표준화된 보호대책을 체크리스트 형태로 구현하여 보호대책을 식별하는 방법이다.

④ 시나리오법-어떤 사건도 기대대로 발생하지 않는다는 사실에 근거하여 일정 조건하에서 위협에 대한 발생 가능한 결과들을 추정하는 방법이다.

정답 2번

간단한 해설

상세위험분석은 자산·위협·취약점을 **정형화된 절차**로 분석한다. '비정형화된 프로세스'는 비정형 접근법의 특징이므로 상세위험분석에 대한 설명으로 부적절하다.

선지별 해설

① O: 델파이법은 전문가의 지식과 판단을 수렴하여 위협과 취약점 등을 평가하는 방법이다. '토론'은 전문가 사이의 의견 교환이라는 넓은 취지로 이해할 수 있다. 다만 전통적인 델파이법의 특징은 **익명 설문과 반복적인 피드백**이며, 이를 곧바로 대면 자유토론과 같은 뜻으로 이해하면 안 된다.

② X: 상세위험분석은 **정형화된 체계적 절차**에 따라 자산을 식별하고 위협·취약점, 발생가능성과 영향을 분석한다. 비정형화된 프로세스와 분석자의 경험·전문적 판단에 주로 의존하는 것은 비정형 접근법이다. 따라서 자산·위협·취약점을 분석한다는 부분보다 '비정형화된 프로세스'라는 설명이 잘못되었다.

③ O: 기준선 접근법은 표준이나 모범사례에서 제시한 보호대책을 기준으로 삼는다. 이를 체크리스트와 같은 형태로 정리하여 현재 구현된 대책과 비교하고 필요한 대책을 식별하므로, 개별 위험을 처음부터 모두 상세 분석하는 방식과 구별된다.

④ O: 시나리오법은 사건이 반드시 예상대로 전개된다고 가정하지 않고, 일정 조건에서 가능한 사건 전개와 결과를 추정한다. 여기서 핵심은 모든 예상이 반드시 빗나간다는 단정이 아니라 **불확실성을 고려한 조건별 결과 분석**이다.

따라서 가장 적절하지 않은 설명은 ②이다.

NoteBase

문 6. ISMS-P에서 다음 업무를 수행하는 기관으로 가장 적절하지 않은 것은?

인증심사 일정이 확정될 시 한국인터넷진흥원에 심사원 모집을 요청하여 심사팀을 구성하고, 신청기관이 수립·운영하는 정보보호 및 개인정보보호 관리체계를 인증기준에 따라 심사하며, 심사기간에 발견된 결함사항의 보완조치 이행 여부 확인 등의 업무를 수행한다.

① 한국정보통신진흥협회(KAIT)

② 차세대정보보안인증원(NISC)

③ 개인정보보호협회(OPA)

④ 금융보안원(FSI)

정답 4번

간단한 해설

지문은 ISMS-P의 **심사기관** 역할을 설명하며, 금융보안원은 금융 분야의 **인증기관**으로 구분된다. 금융보안원도 인증심사를 수행하므로, 단순히 심사 업무를 하는지보다 제도상 기관의 구분이 핵심이다.

핵심 풀이

지문은 ISMS-P 추진체계에서 **심사기관**이 맡는 업무를 설명한다. 한국인터넷진흥원에 심사원 모집을 요청해 심사팀을 구성하고, 관리체계의 기준 충족 여부를 심사한 뒤 발견된 결함의 보완조치까지 확인한다는 흐름이 단서이다.

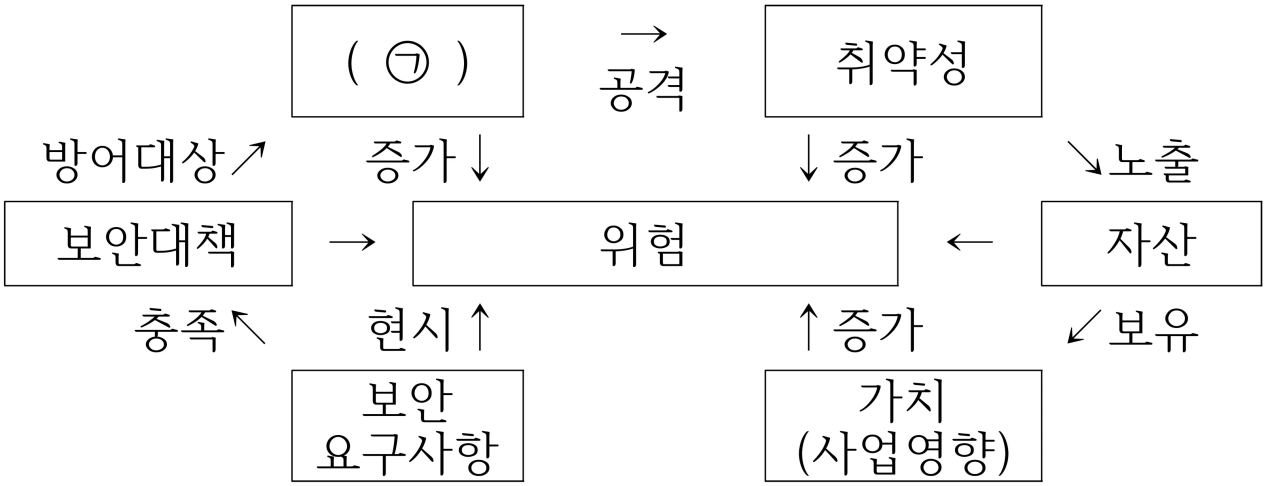
한국정보통신진흥협회(KAIT), 차세대정보보안인증원(NISC), 개인정보보호협회(OPA)는 이 문항의 기준 시점인 2024년의 ISMS-P 심사기관에 해당한다. 따라서 세 기관은 지문이 가리키는 제도상 역할과 연결된다.

금융보안원(FSI)은 금융 분야의 **인증기관**이다. 인증위원회를 구성·운영하고 금융 분야의 인증심사와 인증서 발급을 담당한다. 금융보안원도 심사를 수행하지만, 지문이 설명하는 지정 심사기관이라는 구분과는 다르다.

따라서 지문의 심사기관에 해당하지 않는 기관을 고르면 ④ 금융보안원이다.

NoteBase

문 7. 다음은 정보보호 위험관리(risk management)에서 위험의 구성요소에 관한 설명이다. ㉠에 대한 설명으로 가장 적절한 것은?



(㉠)은(는) 취약점을 공격하여 이용하게 되며 취약점은 자산을 노출시킨다. 또한 자산은 가치를 보유하는데 이러한 (㉠), 취약점, 자산, 가치는 모두 위험을 증가시킨다.
한편 위험을 파악함으로써 보안 요구사항을 파악할 수 있고 보안 요구사항을 만족시키는 정보보호대책을 선정하여 구현함으로써 (㉠)을(를) 방어할 수 있다.

① 조직의 자산을 위험으로부터 보호하기 위한 안전대책으로 자산의 잠재적 속성이다.

② 위험관리를 수행하는 가장 큰 목적으로 조직에 가치가 있는 자원들을 의미한다.

③ 자산을 위험으로부터 보호하기 위한, 또는 위험을 감소시키기 위한 정보보호 조치이다.

④ 자산에 손실을 초래할 수 있는 사건의 잠재적 원인이나 행위자로 정의된다.

정답 4번

간단한 해설

㉠은 취약점을 이용하여 자산에 손실을 초래할 수 있는 **위협**이다. 도식에서 취약성을 공격하고 보안대책의 방어대상이 되는 관계가 결정적 단서이다.

NoteBase

도식 해설

㉠은 위협이다. 도식에서 ㉠은 취약성을 향해 '공격'하고 보안대책의 '방어대상'이 된다. 즉, **취약점을 이용하여 자산에 손실을 일으킬 수 있는 원인**을 뜻한다. 이 문항은 그러한 사건의 잠재적 원인이나 행위자를 포괄하여 설명한다.

취약성은 위협에 이용될 수 있는 약점이며, 취약한 자산을 손실에 노출시킨다. 자산은 조직에 가치가 있는 자원이고, 그 가치가 훼손되면 사업에 영향을 준다. 도식의 '증가' 관계는 위협과 취약성에 따른 **발생 가능성 및 자산 손실의 영향**이 위험을 키운다는 의미이다. 자산의 존재만으로 언제나 동일한 위험이 발생한다는 뜻은 아니다.

보안 요구사항과 보안대책: 위험을 파악하면 어떤 보호가 필요한지 요구사항을 도출할 수 있다. 이를 충족할 대책을 선정·구현하여 위협으로부터 자산을 보호하고 위험을 줄인다. **보안대책은 위험을 줄이는 조치**이므로 손실의 잠재적 원인인 ㉠과 구별된다.

①의 '위험으로부터 보호하기 위한 안전대책'은 보호 조치의 성격을 말하므로 위협의 정의가 될 수 없다. 또한 '자산의 잠재적 속성'이라는 표현만으로 취약성을 정의할 수도 없다. 취약성의 핵심은 **위협에 이용될 수 있는 약점**이라는 점이다.

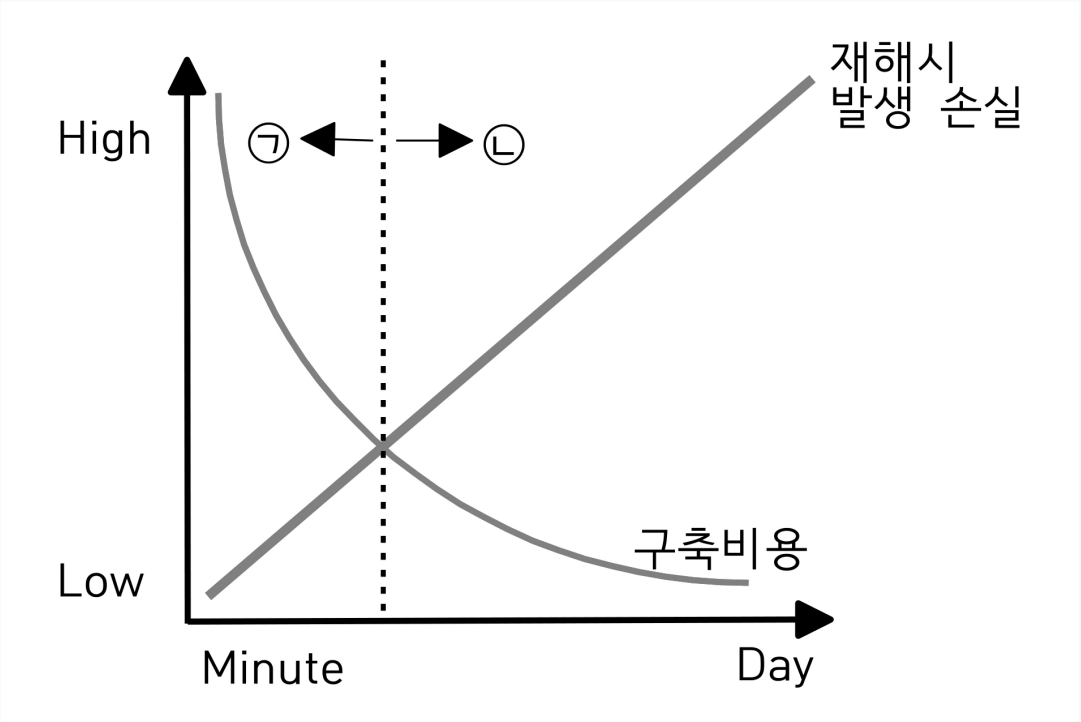
②의 '조직에 가치가 있는 자원들'은 자산이다. 위험관리는 이러한 **보호 대상인 자산**의 손실 위험을 관리하는 활동이며, 자산 자체가 ㉠의 손실 유발 원인을 뜻하지는 않는다.

③의 '자산을 보호하거나 위험을 감소시키기 위한 조치'는 정보보호대책이다. ㉠은 대책이 방어하려는 위협이고, 이 선지는 **위협에 대응하는 수단**을 설명한다.

따라서 ㉠에 해당하는 위협을 자산 손실을 초래할 수 있는 사건의 잠재적 원인이나 행위자로 설명한 ④가 가장 적절하다.

NoteBase

문 8. 다음 RTO(Recovery Time Objective)에 관한 설명으로 가장 적절하지 않은 것은?



① 재해로 인해 중단된 서비스 복구시 유실을 감내할 수 있는 데이터의 손실 허용시점이다.

② 구축비용에 반비례하며 재해시 발생 손실에 비례한다.

③ ㉠방향으로 갈수록 재해시 발생 손실을 줄일 수 있지만 구축비용이 높아진다.

④ ㉡방향으로 갈수록 구축비용을 줄일 수 있지만 재해시 발생 손실이 높아진다.

정답 1번

간단한 해설

RTO는 서비스의 **목표 복구시간**, RPO는 복구할 데이터의 **목표 시점**이다. 데이터 손실을 어디까지 허용하는지를 설명한 문장은 RPO에 해당한다.

NoteBase

선지별 해설

① X: 허용할 수 있는 데이터 손실의 범위를 복구할 데이터 시점으로 정하는 것은 **RPO(Recovery Point Objective)**이다. RTO는 중단된 서비스나 시스템을 **얼마나 빠르게 복구할 것인지 정한 목표시간**이다. 따라서 선지의 데이터 손실 허용시점은 RTO가 아니라 RPO로 고쳐야 한다.

② O: 그림의 가로축은 왼쪽 Minute에서 오른쪽 Day로 갈수록 복구시간이 길어진다. 이때 구축비용 곡선은 내려가고 재해 시 발생 손실은 올라가므로, RTO와 구축비용은 **반대 방향**, RTO와 중단 손실은 **같은 방향**으로 변한다. 선지의 비례·반비례는 이 개념도의 증감 관계를 가리키며, 실제 비용이 모든 상황에서 일정한 수학적 비율로 변한다는 뜻은 아니다.

③ O: ㉠은 가로축의 **왼쪽, 더 짧은 RTO**를 향한다. 신속하게 복구할 수 있도록 시스템과 복구 체계를 갖추는 비용은 커지지만, 업무 중단이 길어져 생기는 손실은 줄어드는 방향이다.

④ O: ㉡은 가로축의 **오른쪽, 더 긴 RTO**를 향한다. 빠른 복구를 위한 구축비용은 줄일 수 있지만, 복구까지 업무가 중단되는 시간이 길어져 재해 시 발생 손실은 커지는 방향이다.

NoteBase

문 9. 스마트 카드의 공격 기법으로 가장 적절하지 않은 것은?

① 소프트웨어공격은 애플리케이션, 알고리즘, 프로토콜 등에서 발견되는 취약점을 공격하는 기법이다.

② 도청 기법은 프로세서에서 방사되는 전자기파를 모니터링/도청하는 기법이다.

③ 장애유발 기법은 비정상 환경 조건에서 프로세서가 오동작하도록 만드는 기법이다.

④ 마이크로 프로빙(micro probing)은 사용자가 입력하는 정보를 갈취하는 악성코드를 활용하는 기법이다.

정답 4번

간단한 해설

마이크로 프로빙은 **미세 탐침으로 칩 내부 신호에 직접 접근**하는 물리적 공격이다. 악성코드를 이용한 사용자 입력 정보 탈취와는 다르다.

선지별 해설

① O: 소프트웨어 공격은 애플리케이션의 구현, 암호 알고리즘, 통신 프로토콜 등의 논리적 취약점을 이용한다. 칩 내부 회로에 직접 접촉하는 방식과 달리, 소프트웨어와 인터페이스의 보안 결함을 공격한다.

② O: 스마트 카드에서의 도청은 프로세서가 작동하면서 방사하는 전자기파 등의 신호를 관찰하여 정보를 추정하는 방법이다. 정상 연산 과정에서 새어 나오는 **물리적 부채널 정보**를 이용한다.

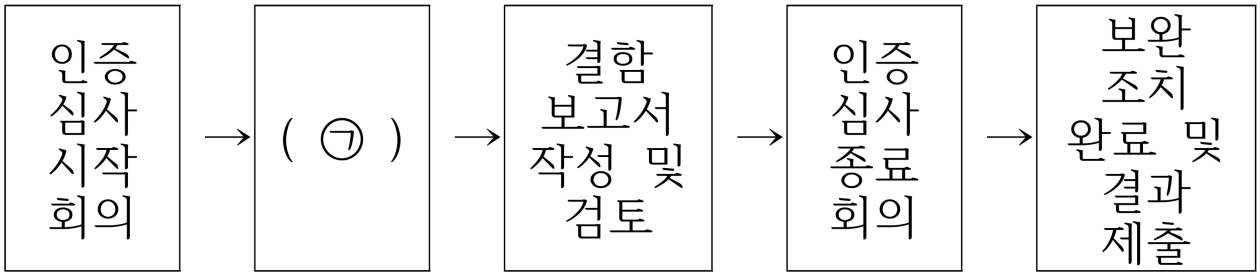
③ O: 장애유발 기법은 전압·클록·온도 등 동작 환경에 비정상 조건을 만들어 프로세서의 오동작을 유도한다. 정상 동작에서 나온 신호를 관찰하는 도청과 달리 **의도적으로 오류를 발생**시킨다는 점이 특징이다.

④ X: 마이크로 프로빙은 **칩 내부 회로에 미세 탐침을 직접 접촉**시켜 신호를 관찰하거나 조작하는 물리적 공격이다. 사용자 입력 정보를 악성코드로 빼내는 방식은 입력 탈취형 악성코드의 설명이며, 마이크로 프로빙의 정의가 아니다.

따라서 공격 기법의 설명으로 가장 적절하지 않은 것은 ④이다.

NoteBase

문 10. 다음은 ISMS-P 인증 심사단계에 관한 내용이다. ㉠에 대한 설명으로 가장 적절한 것은?



① ISMS-P 인증제도 개요, 심사원 소개, 심사 계획 등을 설명하고, 신청기관 담당자는 ISMS-P 구축 및 운영 현황 등에 대하여 간략하게 설명한다.

② 관리체계 수립 및 운영, 보호대책 요구사항 및 개인정보 처리단계별 요구사항의 인증항목에 맞는 체계를 구축하고 적절하게 운영하고 있는지 확인한다.

③ 서면 및 현장심사를 통하여 도출된 문제점에 대해 신청기관 담당자와의 회의를 통해 상호 간 결과를 확인한다.

④ 신청기관 임직원 및 담당자에게 심사 결과를 설명하고 보완조치요청서를 통해 결함사항들에 대한 보완조치를 요청한다.

정답 2번

간단한 해설

㉠은 시작회의와 결함보고서 사이에 있는 **인증심사** 단계이다. 인증기준에 맞게 체계를 구축하고 운영하는지를 확인하는 ②가 해당한다.

NoteBase

도식 해설

㉠의 위치: 그림에서 ㉠은 인증심사 시작회의 뒤, 결함보고서 작성 및 검토 앞에 있다. 결함을 보고서로 정리하려면 먼저 기준 충족 여부를 확인해야 하므로 이 자리는 **실제 인증심사** 단계이다.

인증심사 시작회의: 심사팀이 제도 개요·심사원·계획을 안내하고 신청기관이 관리체계의 구축·운영 현황을 소개한다. 이는 본격적인 확인 작업에 앞서 심사의 진행 방향을 공유하는 단계로, ①의 설명에 해당한다.

㉠ 인증심사: 관리체계 수립 및 운영, 보호대책 요구사항, 개인정보 처리단계별 요구사항에 따라 **체계의 구축과 실제 운영이 기준에 맞는지** 확인한다. 서면으로 정책·절차·운영 증적을 검토하고, 현장에서는 담당자 면담과 시스템 확인 등으로 이행 상태를 살핀다. 기준을 설명하는 데 그치지 않고 적합성을 확인한다는 점이 핵심이다.

결함보고서 작성 및 검토: 서면·현장심사에서 확인된 미흡 사항을 정리하고 신청기관과 그 결과를 대조하여 사실관계를 확인한다. 따라서 ③은 ㉠에서 확인한 내용을 바탕으로 하는 **결과 정리·검토** 단계의 설명이다.

인증심사 종료회의: 신청기관 임직원과 담당자에게 심사 결과를 설명하고, 확인된 결함에 대한 보완조치를 요청한다. ④의 보완조치요청서에 의한 요청은 이 단계에 해당한다.

보완조치 완료 및 결과 제출: 신청기관이 요청받은 결함을 개선하고 그 조치 내역과 증빙을 제출하는 후속 단계이다. 종료회의에서 보완을 요청하는 것과 실제로 보완하여 결과를 제출하는 것을 구별한다.

따라서 ㉠의 인증심사를 설명한 것은 ②이다.

NoteBase

문 11. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제53조 (통신과금서비스제공자의 등록 등)에 따르면 통신과금서비스를 제공하려는 자는 대통령령으로 정하는 바에 따라 필요한 사항을 갖추어 과학기술정보통신부장관에게 등록하여야 한다. 이를 위해 갖추어야 할 사항으로 가장 적절하지 않은 것은?

① 재무건전성

② 사업계획서

③ 통신과금서비스이용자정보

④ 업무를 수행할 수 있는 인력과 물적 설비

정답 3번

①

통신과금서비스를 제공하려는 자는 등록요건으로 **재무건전성을 갖추어야 한다**.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제53조(통신과금서비스제공자의 등록 등)
① 통신과금서비스를 제공하려는 자는 대통령령으로 정하는 바에 따라 다음 각 호의 사항을 갖추어 과학기술정보통신부장관에게 등록하여야 한다. <개정 2008.2.29, 2013.3.23, 2017.7.26>
1. 재무건전성

②

통신과금서비스를 제공하려는 자는 등록에 필요한 사항으로 **사업계획서를 갖추어야 한다**.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제53조(통신과금서비스제공자의 등록 등)
① 통신과금서비스를 제공하려는 자는 대통령령으로 정하는 바에 따라 다음 각 호의 사항을 갖추어 과학기술정보통신부장관에게 등록하여야 한다. <개정 2008.2.29, 2013.3.23, 2017.7.26>
4. 사업계획서

③

등록 시 갖추어야 하는 것은 통신과금서비스이용자정보가 아니라 **통신과금서비스이용자보호계획**이다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제53조(통신과금서비스제공자의 등록 등)
① 통신과금서비스를 제공하려는 자는 대통령령으로 정하는 바에 따라 다음 각 호의 사항을 갖추어 과학기술정보통신부장관에게 등록하여야 한다. <개정 2008.2.29, 2013.3.23, 2017.7.26>
2. 통신과금서비스이용자보호계획

NoteBase

④

통신과금서비스를 제공하려는 자는 **업무를 수행할 수 있는 인력과 물적 설비를 갖추어야 한다**.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제53조(통신과금서비스제공자의 등록 등)
① 통신과금서비스를 제공하려는 자는 대통령령으로 정하는 바에 따라 다음 각 호의 사항을 갖추어 과학기술정보통신부장관에게 등록하여야 한다. <개정 2008.2.29, 2013.3.23, 2017.7.26>
3. 업무를 수행할 수 있는 인력과 물적 설비

NoteBase

문 12. 「정보통신기반 보호법」 제8조(주요정보통신기반시설의 지정 등)에 관한 내용으로 가장 적절하지 않은 것은?

① 주요정보통신기반시설의 지정 및 지정취소 등에 관하여 필요한 사항은 이를 대통령령으로 정한다.

② 중앙행정기관의 장은 소관분야의 정보통신기반시설 중 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정할 수 있다.

③ 관계 중앙행정기관의 장은 관리기관이 해당 업무를 폐지·정지 또는 변경하는 경우에는 직권 또는 해당 관리기관의 신청에 의하여 주요정보통신기반시설의 지정을 취소할 수 있다.

④ 지방자치단체의 장이 관리·감독하는 기관의 정보통신기반시설에 대하여는 과학기술정보통신부장관이 지방자치단체의 장과 협의하여 주요정보통신기반시설로 지정하거나 그 지정을 취소할 수 있다.

정답 4번

①

주요정보통신기반시설의 지정·지정취소 등에 필요한 사항은 **대통령령으로 정한다**.

정보통신기반 보호법 제8조(주요정보통신기반시설의 지정 등)
⑦주요정보통신기반시설의 지정 및 지정취소 등에 관하여 필요한 사항은 이를 대통령령으로 정한다.

②

중앙행정기관의 장은 업무의 국가사회적 중요성 등 법정 사항을 고려하여, 소관분야의 시설 중 **전자적 침해행위로부터 보호할 필요가 있다고 인정되는 시설을 지정할 수 있다**.

정보통신기반 보호법 제8조(주요정보통신기반시설의 지정 등)
①중앙행정기관의 장은 소관분야의 정보통신기반시설중 다음 각호의 사항을 고려하여 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정할 수 있다. <개정 2019.12.10, 2020.6.9>
1. 해당 정보통신기반시설을 관리하는 기관이 수행하는 업무의 국가사회적 중요성
2. 제1호에 따른 기관이 수행하는 업무의 정보통신기반시설에 대한 의존도
3. 다른 정보통신기반시설과의 상호연계성
4. 침해사고가 발생할 경우 국가안전보장과 경제사회에 미치는 피해규모 및 범위
5. 침해사고의 발생가능성 또는 그 복구의 용이성

NoteBase

③

관리기관이 해당 업무를 폐지·정지하거나 변경하면 관계 중앙행정기관의 장은 **직권 또는 해당 관리기관의 신청에 따라 지정을 취소할 수 있다**.

정보통신기반 보호법 제8조(주요정보통신기반시설의 지정 등)
③관계중앙행정기관의 장은 관리기관이 해당 업무를 폐지 · 정지 또는 변경하는 경우에는 직권 또는 해당 관리기관의 신청에 의하여 주요정보통신기반시설의 지정을 취소할 수 있다.

④

지방자치단체의 장이 관리·감독하는 기관의 시설은 **행정안전부장관이 지방자치단체의 장과 협의하여** 지정하거나 지정을 취소할 수 있다.

정보통신기반 보호법 제8조(주요정보통신기반시설의 지정 등)
④지방자치단체의 장이 관리 · 감독하는 기관의 정보통신기반시설에 대하여는 행정안전부장관이 지방자치단체의 장과 협의하여 주요정보통신기반시설로 지정하거나 그 지정을 취소할 수 있다. <개정 2008.2.29, 2013.3.23, 2014.11.19, 2017.7.26>

NoteBase

문 13. 「개인정보 보호법」 제30조(개인정보 처리방침의 수립 및 공개)에 따를 때, 예외 없이 개인정보 처리방침에 포함되어야 하는 사항이 아닌 것은?

① 개인정보의 처리 목적

② 개인정보의 처리 및 보유 기간

③ 개인정보처리의 위탁에 관한 사항

④ 정보주체와 법정대리인의 권리·의무 및 그 행사방법에 관한 사항

정답 3번

①

개인정보처리자는 처리방침에 **개인정보의 처리 목적**을 반드시 포함해야 한다.

개인정보 보호법 제30조(개인정보 처리방침의 수립 및 공개)
① 개인정보처리자는 다음 각 호의 사항이 포함된 개인정보의 처리 방침(이하 "개인정보 처리방침"이라 한다)을 정하여야 한다. 이 경우 공공기관은 제32조에 따라 등록대상이 되는 개인정보파일에 대하여 개인정보 처리방침을 정한다. <개정 2016.3.29, 2020.2.4, 2023.3.14>
1. 개인정보의 처리 목적

②

개인정보처리자는 처리방침에 **개인정보의 처리 및 보유 기간**을 반드시 포함해야 한다.

개인정보 보호법 제30조(개인정보 처리방침의 수립 및 공개)
① 개인정보처리자는 다음 각 호의 사항이 포함된 개인정보의 처리 방침(이하 "개인정보 처리방침"이라 한다)을 정하여야 한다. 이 경우 공공기관은 제32조에 따라 등록대상이 되는 개인정보파일에 대하여 개인정보 처리방침을 정한다. <개정 2016.3.29, 2020.2.4, 2023.3.14>
2. 개인정보의 처리 및 보유 기간

NoteBase

③

개인정보처리의 위탁에 관한 사항은 **위탁이 있는 경우에만** 처리방침에 정하므로, 위탁이 없는 경우에는 포함할 의무가 없다.

개인정보 보호법 제30조(개인정보 처리방침의 수립 및 공개)
① 개인정보처리자는 다음 각 호의 사항이 포함된 개인정보의 처리 방침(이하 "개인정보 처리방침"이라 한다)을 정하여야 한다. 이 경우 공공기관은 제32조에 따라 등록대상이 되는 개인정보파일에 대하여 개인정보 처리방침을 정한다. <개정 2016.3.29, 2020.2.4, 2023.3.14>
4. 개인정보처리의 위탁에 관한 사항(해당되는 경우에만 정한다)

④

정보주체와 법정대리인의 **권리·의무 및 그 행사방법**은 처리방침에 반드시 포함해야 한다.

개인정보 보호법 제30조(개인정보 처리방침의 수립 및 공개)
① 개인정보처리자는 다음 각 호의 사항이 포함된 개인정보의 처리 방침(이하 "개인정보 처리방침"이라 한다)을 정하여야 한다. 이 경우 공공기관은 제32조에 따라 등록대상이 되는 개인정보파일에 대하여 개인정보 처리방침을 정한다. <개정 2016.3.29, 2020.2.4, 2023.3.14>
5. 정보주체와 법정대리인의 권리 · 의무 및 그 행사방법에 관한 사항

NoteBase

문 14. 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제23조의 2(클라우드컴퓨팅서비스의 보안인증)에 대한 내용으로 가장 적절하지 않은 것은?

① 과학기술정보통신부장관은 정보보호 수준의 향상 및 보장을 위하여 보안인증기준에 적합한 클라우드컴퓨팅서비스에 대하여 대통령령으로 정하는 바에 따라 인증을 할 수 있다.

② 보안인증의 유효기간은 인증 서비스 등을 고려하여 대통령령으로 정하는 3년 내의 범위로 한다.

③ 보안인증의 유효기간을 연장받으려는 자는 대통령령으로 정하는 바에 따라 유효기간의 갱신을 신청하여야 한다.

④ 누구든지 보안인증을 받지 아니한 클라우드컴퓨팅서비스에 대하여 보안인증 표시 또는 이와 유사한 표시를 하여서는 아니 된다.

정답 2번

①

과학기술정보통신부장관은 정보보호 수준의 향상 및 보장을 위해 **보안인증기준에 적합한 클라우드컴퓨팅서비스를 인증할 수 있다**.

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

보안인증의 유효기간은 인증 서비스 등을 고려하여 대통령령으로 정하는 **5년 내의 범위**이다. 3년 내로 제한하지 않는다.

클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제23조의2(클라우드컴퓨팅서비스의 보안인증)
② 보안인증의 유효기간은 인증 서비스 등을 고려하여 대통령령으로 정하는 5년 내의 범위로 하고, 보안인증의 유효기간을 연장받으려는 자는 대통령령으로 정하는 바에 따라 유효기간의 갱신을 신청하여야 한다.

③

보안인증의 유효기간을 연장받으려는 자는 대통령령으로 정하는 바에 따라 **유효기간의 갱신을 신청하여야 한다**.

클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제23조의2(클라우드컴퓨팅서비스의 보안인증)
② 보안인증의 유효기간은 인증 서비스 등을 고려하여 대통령령으로 정하는 5년 내의 범위로 하고, 보안인증의 유효기간을 연장받으려는 자는 대통령령으로 정하는 바에 따라 유효기간의 갱신을 신청하여야 한다.

NoteBase

④

보안인증을 받지 않은 클라우드컴퓨팅서비스에는 누구든지 **보안인증 표시뿐 아니라 이와 유사한 표시도 할 수 없다**.

클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제23조의2(클라우드컴퓨팅서비스의 보안인증)
④ 누구든지 보안인증을 받지 아니한 클라우드컴퓨팅서비스에 대하여 보안인증 표시 또는 이와 유사한 표시를 하여서는 아니 된다.

NoteBase

문 15. 다음 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 대한 내용에서 ㉠에 해당하는 기관으로 가장 적절한 것은?

정부는 정보통신망의 고도화와 안전한 이용 촉진 및 방송통신과 관련한 국제협력·국외진출 지원을 효율적으로 추진하기 위하여 (㉠)을(를) 설립한다.

① 한국인터넷진흥원
② 방송통신위원회
③ 과학기술정보통신부
④ 한국지능정보사회진흥원

정답 1번

공통 해설

정보통신망의 고도화와 안전한 이용 촉진, 방송통신 관련 국제협력·국외진출 지원을 위해 정부가 설립하는 기관은 **한국인터넷진흥원**이다. 다만 정보통신망의 고도화 중 **구축·개선 및 관리에 관한 사항은 제외**한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제52조(한국인터넷진흥원)
① 정부는 정보통신망의 고도화(정보통신망의 구축 · 개선 및 관리에 관한 사항은 제외한다)와 안전한 이용 촉진 및 방송통신과 관련한 국제협력 · 국외진출 지원을 효율적으로 추진하기 위하여 한국인터넷진흥원(이하 "인터넷진흥원"이라 한다)을 설립한다. <개정 2009.4.22, 2020.6.9>

NoteBase

문 16. 다음은 「개인정보 보호법」 제9조(기본계획)에 관한 설명이다. ㉠, ㉤에 들어갈 내용으로 가장 적절한 것은?

① 보호위원회는 개인정보의 보호와 정보주체의 권익 보장을 위하여 3년마다 개인정보 보호 기본계획(이하 “기본계획”이라 한다)을 (㉠)과 협의하여 수립한다.
② 기본계획에는 다음 각 호의 사항이 포함되어야 한다.
1. 개인정보 보호의 기본목표와 추진방향
2. 개인정보 보호와 관련된 제도 및 법령의 개선
3. 개인정보 침해 방지를 위한 대책
4. (㉤)
5. 개인정보 보호 교육·홍보의 활성화
6. 개인정보 보호를 위한 전문인력의 양성
7. 그 밖에 개인정보 보호를 위하여 필요한 사항

① ㉠: 관계 중앙행정기관의 장, ㉤: 개인정보 오용·남용 방지를 위한 계획
② ㉠: 관계 중앙행정기관의 장, ㉤: 개인정보 보호 자율규제의 활성화
③ ㉠: 지방자치단체의 장, ㉤: 개인정보 보호 자율규제의 활성화
④ ㉠: 지방자치단체의 장, ㉤: 개인정보 오용·남용 방지를 위한 계획

정답 2번

①

개인정보보호위원회는 **3년마다 관계 중앙행정기관의 장과 협의하여** 개인정보 보호 기본계획을 수립한다.

개인정보 보호법 제9조(기본계획)
① 보호위원회는 개인정보의 보호와 정보주체의 권익 보장을 위하여 3년마다 개인정보 보호 기본계획(이하 "기본계획"이라 한다)을 관계 중앙행정기관의 장과 협의하여 수립한다. <개정 2013.3.23, 2014.11.19, 2015.7.24>

NoteBase

②

기본계획에는 기본목표·추진방향, 제도·법령 개선, 침해 방지 대책, 자율규제 활성화, 교육·홍보 활성화, 전문인력 양성 및 그 밖의 개인정보 보호 필요 사항이 **필수적으로 포함되어야 한다**.

개인정보 보호법 제9조(기본계획)
② 기본계획에는 다음 각 호의 사항이 포함되어야 한다.
1. 개인정보 보호의 기본목표와 추진방향
2. 개인정보 보호와 관련된 제도 및 법령의 개선
3. 개인정보 침해 방지를 위한 대책
4. 개인정보 보호 자율규제의 활성화
5. 개인정보 보호 교육 · 홍보의 활성화
6. 개인정보 보호를 위한 전문인력의 양성
7. 그 밖에 개인정보 보호를 위하여 필요한 사항

NoteBase

문 17. 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제27조 (이용자 정보의 보호)에 따르면 클라우드컴퓨팅서비스 제공자가 이용자 정보를 제3자에게 제공하거나 서비스 제공 목적 외의 용도로 이용할 경우 이용자에게 알리고 동의를 받아야 한다. 이용자에게 알리고 동의를 받아야 할 사항으로 가장 적절하지 않은 것은?

① 이용자 정보의 이용 목적

② 이용자 정보의 보유 및 이용 기간

③ 이용 또는 제공하는 이용자 정보의 항목

④ 이용 또는 제공하는 담당부서 및 연락처

정답 4번

①

제3자 제공 또는 서비스 제공 목적 외 이용 시에는 **이용자 정보의 이용 목적**을 알리고 동의를 받아야 한다.
제3자에게 제공하는 경우에는 **제공받는 자의 이용 목적**을 뜻한다.

클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제27조(이용자 정보의 보호)
② 클라우드컴퓨팅서비스 제공자는 이용자 정보를 제3자에게 제공하거나 서비스 제공 목적 외의 용도로 이용할 경우에는 다음 각 호의 사항을 이용자에게 알리고 동의를 받아야 한다. 다음 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다.
2. 이용자 정보의 이용 목적(제공 시에는 제공받는 자의 이용 목적을 말한다)

②

이용자에게 **정보의 보유 및 이용 기간**을 알리고 동의를 받아야 하며, 제3자 제공 시에는 **제공받는 자의 보유 및 이용 기간**이 대상이다.

클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제27조(이용자 정보의 보호)
② 클라우드컴퓨팅서비스 제공자는 이용자 정보를 제3자에게 제공하거나 서비스 제공 목적 외의 용도로 이용할 경우에는 다음 각 호의 사항을 이용자에게 알리고 동의를 받아야 한다. 다음 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다.
4. 이용자 정보의 보유 및 이용 기간(제공 시에는 제공받는 자의 보유 및 이용 기간을 말한다)

NoteBase

③

이용자에게 **이용 또는 제공하는 이용자 정보의 항목**을 알리고 동의를 받아야 한다.

클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제27조(이용자 정보의 보호)
② 클라우드컴퓨팅서비스 제공자는 이용자 정보를 제3자에게 제공하거나 서비스 제공 목적 외의 용도로 이용할 경우에는 다음 각 호의 사항을 이용자에게 알리고 동의를 받아야 한다. 다음 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다.
3. 이용 또는 제공하는 이용자 정보의 항목

④

담당부서 및 연락처는 법정 고지·동의 사항에 포함되지 않는다. 고지·동의 대상은 제공받는 자, 이용 목적, 정보 항목, 보유·이용 기간, 동의 거부권 및 거부에 따른 불이익이다.

클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제27조(이용자 정보의 보호)
② 클라우드컴퓨팅서비스 제공자는 이용자 정보를 제3자에게 제공하거나 서비스 제공 목적 외의 용도로 이용할 경우에는 다음 각 호의 사항을 이용자에게 알리고 동의를 받아야 한다. 다음 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다.
1. 이용자 정보를 제공받는 자
2. 이용자 정보의 이용 목적(제공 시에는 제공받는 자의 이용 목적을 말한다)
3. 이용 또는 제공하는 이용자 정보의 항목
4. 이용자 정보의 보유 및 이용 기간(제공 시에는 제공받는 자의 보유 및 이용 기간을 말한다)
5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

NoteBase

문 18. 다음은 「위치정보의 보호 및 이용 등에 관한 법률」 제2조(정의)에 대한 설명이다. ㉠~㉣에 해당하는 용어로 가장 적절한 것은?

㉠ 특정 개인의 위치정보(위치정보만으로는 특정 개인의 위치를 알 수 없는 경우에도 다른 정보와 용이하게 결합하여 특정 개인의 위치를 알 수 있는 것을 포함한다)를 말한다.
㉡ 위치정보의 수집요청인, 수집일시 및 수집방법에 관한 자료(위치정보는 제외한다)를 말한다.
㉢ 위치정보를 이용한 서비스를 제공하는 것을 사업으로 영위하는 것을 말한다.
㉣ 위치정보를 제공받는 자, 취득 경로, 이용·제공일시 및 이용·제공방법에 관한 자료(위치정보는 제외한다)를 말한다.

① ㉠: 위치정보, ㉡: 위치정보 이용·제공사실 확인자료, ㉢: 위치기반서비스사업, ㉣: 위치정보 수집사실 확인자료
② ㉠: 위치정보, ㉡: 위치정보 수집사실 확인자료, ㉢: 위치정보사업, ㉣: 위치정보 이용·제공사실 확인자료
③ ㉠: 개인위치정보, ㉡: 위치정보 수집사실 확인자료, ㉢: 위치기반서비스사업, ㉣: 위치정보 이용·제공사실 확인자료
④ ㉠: 개인위치정보, ㉡: 위치정보 이용·제공사실 확인자료, ㉢: 위치정보사업, ㉣: 위치정보 수집사실 확인자료

정답 3번

㉠
개인위치정보는 특정 개인의 위치정보이며, **다른 정보와 용이하게 결합하여 특정 개인의 위치를 알 수 있는 정보도 포함**한다.

위치정보의 보호 및 이용 등에 관한 법률 제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다. <개정 2010.3.22, 2015.2.3, 2020.6.9, 2021.10.19>
2. "개인위치정보"라 함은 특정 개인의 위치정보(위치정보만으로는 특정 개인의 위치를 알 수 없는 경우에도 다른 정보와 용이하게 결합하여 특정 개인의 위치를 알수 있는 것을 포함한다)를 말한다.

㉡
위치정보 수집사실 확인자료는 **수집요청인·수집일시·수집방법에 관한 자료**이며, **위치정보 자체는 제외**한다.

위치정보의 보호 및 이용 등에 관한 법률 제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다. <개정 2010.3.22, 2015.2.3, 2020.6.9, 2021.10.19>
4. "위치정보 수집사실 확인자료"라 함은 위치정보의 수집요청인, 수집일시 및 수집방법에 관한 자료(위치정보는 제외한다)를 말한다.

NoteBase

ⓒ

위치기반서비스사업은 **위치정보를 이용한 서비스를 제공하는 것을 사업으로 영위**하는 것이다.

위치정보의 보호 및 이용 등에 관한 법률 제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다. <개정 2010.3.22, 2015.2.3, 2020.6.9, 2021.10.19>
7. "위치기반서비스사업"이라 함은 위치정보를 이용한 서비스(이하 "위치기반서비스"라 한다)를 제공하는 것을 사업으로 영위하는 것을 말한다.

ⓔ

위치정보 이용·제공사실 확인자료는 **제공받는 자, 취득 경로, 이용·제공일시 및 이용·제공방법**에 관한 자료이다. **위치정보 자체는 제외**한다.

위치정보의 보호 및 이용 등에 관한 법률 제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다. <개정 2010.3.22, 2015.2.3, 2020.6.9, 2021.10.19>
5. "위치정보 이용 · 제공사실 확인자료"라 함은 위치정보를 제공받는 자, 취득경로, 이용 · 제공일시 및 이용 · 제공방법에 관한 자료(위치정보는 제외한다)를 말한다.

NoteBase

문 19. 「지능정보화 기본법」 제60조(안전성 보호조치)에 따르면 과학기술정보통신부장관은 행정안전부장관 등 관계 기관의 장과 협의하여 지능정보기술 및 지능정보서비스의 안전성을 확보하기 위하여 필요한 최소한도의 보호조치의 내용과 방법을 정하여 고시할 수 있다. 고시에 포함되어야 할 내용으로 가장 적절하지 않은 것은?

① 지능정보기술 및 지능정보서비스 이용자의 안전보장 및 피해구제 등에 관한 사항

② 지능정보기술 및 지능정보서비스에 대한 권한 없는 자의 접근, 조작 등 전자적 침해행위의 방지에 관한 사항

③ 지능정보기술 및 지능정보서비스의 접속기록, 운용·활용기록의 저장·관리 및 제공 등에 관한 사항

④ 지능정보기술의 동작 및 지능정보서비스 제공을 외부에서 긴급하게 정지하는 것(이하 “비상정지”라 한다)과 비상정지에 필요한 알고리즘의 제공에 관한 사항

정답 1번

①

안전성 보호조치 고시는 **오작동 방지, 전자적 침해행위 방지, 기록의 저장·관리·제공, 비상정지 및 관련 알고리즘 제공** 등을 대상으로 한다. 이용자의 안전보장·피해구제는 이 고시사항으로 명시되어 있지 않다.

지능정보화 기본법 제60조(안전성 보호조치)
① 과학기술정보통신부장관은 행정안전부장관 등 관계 기관의 장과 협의하여 지능정보기술 및 지능정보서비스의 안전성을 확보하기 위하여 다음 각 호와 같은 필요한 최소한도의 보호조치의 내용과 방법을 정하여 고시할 수 있다.
1. 지능정보기술과 지능정보서비스의 오작동 방지에 관한 사항
2. 지능정보기술 및 지능정보서비스에 대한 권한 없는 자의 접근, 조작 등 전자적 침해행위의 방지에 관한 사항
3. 지능정보기술 및 지능정보서비스의 접속기록, 운용 · 활용기록의 저장 · 관리 및 제공 등에 관한 사항
4. 지능정보기술의 동작 및 지능정보서비스 제공을 외부에서 긴급하게 정지하는 것(이하 "비상정지"라 한다)과 비상정지에 필요한 알고리즘의 제공에 관한 사항
5. 기타 지능정보기술 및 지능정보서비스의 안전성 확보를 위해 필요한 사항

NoteBase

②

권한 없는 자의 **접근·조작 등 전자적 침해행위의 방지**는 지능정보기술·서비스의 안전성을 위한 보호조치 고시사항이다.

지능정보화 기본법 제60조(안전성 보호조치)
① 과학기술정보통신부장관은 행정안전부장관 등 관계 기관의 장과 협의하여 지능정보기술 및 지능정보서비스의 안전성을 확보하기 위하여 다음 각 호와 같은 필요한 최소한도의 보호조치의 내용과 방법을 정하여 고시할 수 있다.
2. 지능정보기술 및 지능정보서비스에 대한 권한 없는 자의 접근, 조작 등 전자적 침해행위의 방지에 관한 사항

③

지능정보기술·서비스의 **접속기록과 운용·활용기록의 저장·관리 및 제공**에 관한 사항은 안전성 보호조치 고시에 포함된다.

지능정보화 기본법 제60조(안전성 보호조치)
① 과학기술정보통신부장관은 행정안전부장관 등 관계 기관의 장과 협의하여 지능정보기술 및 지능정보서비스의 안전성을 확보하기 위하여 다음 각 호와 같은 필요한 최소한도의 보호조치의 내용과 방법을 정하여 고시할 수 있다.
3. 지능정보기술 및 지능정보서비스의 접속기록, 운용 · 활용기록의 저장 · 관리 및 제공 등에 관한 사항

④

안전성 보호조치 고시에는 **외부에서 기술의 동작과 서비스 제공을 긴급히 정지하는 조치와 이에 필요한 알고리즘의 제공**에 관한 사항이 포함된다.

지능정보화 기본법 제60조(안전성 보호조치)
① 과학기술정보통신부장관은 행정안전부장관 등 관계 기관의 장과 협의하여 지능정보기술 및 지능정보서비스의 안전성을 확보하기 위하여 다음 각 호와 같은 필요한 최소한도의 보호조치의 내용과 방법을 정하여 고시할 수 있다.
4. 지능정보기술의 동작 및 지능정보서비스 제공을 외부에서 긴급하게 정지하는 것(이하 "비상정지"라 한다)과 비상정지에 필요한 알고리즘의 제공에 관한 사항

NoteBase

문 20. 다음 「개인정보 보호법」 관련 조문에서 ㉠에 들어갈 내용으로 가장 적절한 것은?

제20조의2(㉠) ① 대통령령으로 정하는 기준에 해당하는 개인정보처리자는 이 법에 따라 수집한 개인정보의 이용·제공 내역이나 이용·제공 내역을 확인할 수 있는 정보시스템에 접속하는 방법을 주기적으로 정보주체에게 통지하여야 한다. 다만, 연락처 등 정보주체에게 통지할 수 있는 개인정보를 수집·보유하지 아니한 경우에는 통지하지 아니할 수 있다.
② 제1항에 따른 통지의 대상이 되는 정보주체의 범위, 통지 대상 정보, 통지 주기 및 방법 등에 필요한 사항은 대통령령으로 정한다.

① 개인정보 이용·제공 내역의 통지

② 개인정보의 목적 외 이용·제공 제한

③ 개인정보를 제공받는 자의 이용·제공 제한

④ 정보주체 이외로부터 수집한 개인정보의 수집 출처 등 통지

정답 1번

공통 해설

개인정보의 이용·제공 내역이나 이를 확인할 정보시스템의 접속 방법을 정보주체에게 주기적으로 알리는 규정이므로, 제목은 **개인정보 이용·제공 내역의 통지**이다.

개인정보 보호법 제20조의2(개인정보 이용 · 제공 내역의 통지)
① 대통령령으로 정하는 기준에 해당하는 개인정보처리자는 이 법에 따라 수집한 개인정보의 이용 · 제공 내역이나 이용 · 제공 내역을 확인할 수 있는 정보시스템에 접속하는 방법을 주기적으로 정보주체에게 통지하여야 한다. 다만, 연락처 등 정보주체에게 통지할 수 있는 개인정보를 수집 · 보유하지 아니한 경우에는 통지하지 아니할 수 있다.
② 제1항에 따른 통지의 대상이 되는 정보주체의 범위, 통지 대상 정보, 통지 주기 및 방법 등에 필요한 사항은 대통령령으로 정한다.

NoteBase