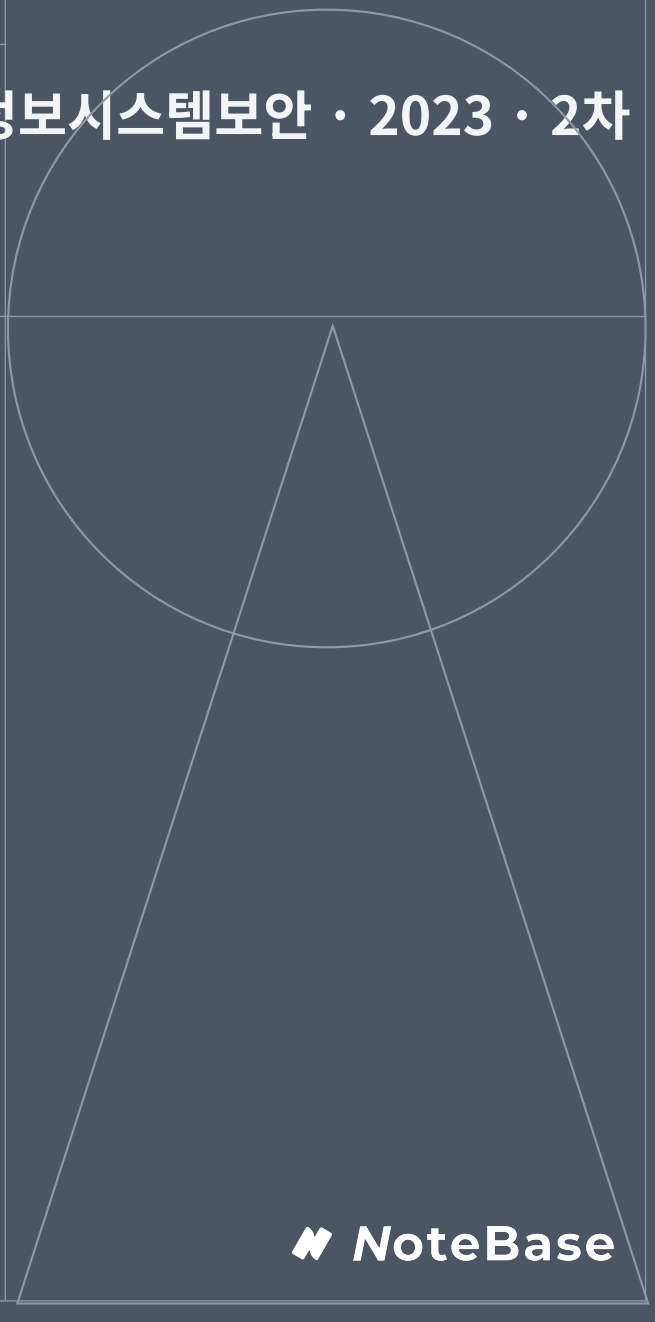
기출OX 해설집

공무원/해경/일반직 9급 · 정보시스템보안 · 2023 · 2차



NoteBase

기출OX 해설집

공무원/해경/일반직 9급 · 정보시스템보안 · 2023 · 2차

공무원/해경/일반직 9급 · 정보시스템보안 · 2023 · 2차

문 1. 다음은 정보시스템에 대해 가용성(Availability)과 보안수준(Security Level)간의 관계를 설명한 것이다. 가장 적합한 설명은?

① 보안수준과 가용성간에는 아무런 관련이 없다.

② 보안수준을 높이면 가용성이 낮아진다.

③ 보안수준을 높이면 가용성도 높아진다.

④ 보안수준을 낮추면 가용성도 낮아진다.

정답 2번

출제 포인트

이 문제는 정보시스템의 보안 통제를 강화할 때 사용자가 시스템과 자원에 접근할 수 있는 정도인 가용성이 어떻게 달라지는지를 묻는다.

핵심 개념

가용성은 인가된 사용자가 필요할 때 정보와 시스템을 사용할 수 있는 성질이다. 보안 수준을 높이기 위해 인증 절차, 접근 통제, 권한 제한 등을 강화하면 무단 접근은 줄지만 정상 사용자의 접근 절차와 제약도 늘 수 있다. 따라서 이 문항이 전제한 일반적인 관계에서는 보안 수준이 높아질수록 가용성이 낮아지는 상충관계가 나타난다.

선지별 해설

① X — '아무런 관련이 없다'는 표현이 틀렸다. 보안 통제를 강화하면 접근 절차와 제한이 늘어 가용성에 영향을 줄 수 있으므로, 두 요소 사이에는 상충관계가 존재한다.
② O — 보안 수준을 높이기 위해 접근 통제와 인증을 강화하면 시스템 이용이 제한되거나 복잡해질 수 있으므로 가용성이 낮아질 수 있다. 이 문항의 일반적 관계에 가장 적합한 설명이다.
③ X — '가용성도 높아진다'는 표현이 틀렸다. 이 문항의 전제에서는 보안 수준을 높이면 이용 제약이 커져 가용성이 낮아진다고 보아야 한다.
④ X — '가용성도 낮아진다'는 표현이 틀렸다. 보안 수준을 낮추면 접근 제한이 완화되므로 일반적으로 가용성은 높아진다고 보아야 한다.

NoteBase

오답 포인트

보안과 가용성이 모두 정보보호의 중요한 목표라는 사실만 보고 두 값이 항상 같은 방향으로 움직인다고 판단하기 쉽다. 이 문항은 목표의 중요도가 아니라 접근 통제를 강화할 때 생기는 이용 제약을 묻는다.

다시 나오면 이렇게 판단

인증·권한·접근 제한이 강화되는 상황이면 정상 사용자의 이용 편의와 즉시 접근 가능성이 줄어드는지를 판단한다. 별도의 장애 대응이나 이중화 조건이 제시되지 않았다면 보안 수준과 가용성의 일반적 상충관계를 적용한다.

암기 포인트

접근 통제 강화는 보안 수준을 높이고, 이용 제약 증가는 가용성을 낮춘다.

NoteBase

문 2. 다음 중 조직내의 정보시스템을 안전하게 보호를 위해 마련해야 할 보호대책이 아닌 것은?

① 관리적 보호대책

② 기술적 보호대책

③ 소프트웨어공학적 보호대책

④ 물리적 보호대책

정답 3번

출제 포인트

정보시스템 보호대책의 기본 분류인 관리적·기술적·물리적 보호대책을 구분하는 문제이다.

핵심 개념

관리적 보호대책은 보안정책, 조직, 인력, 교육, 절차 등 관리 체계를 통해 보안을 확보하는 대책이다.
기술적 보호대책은 접근통제, 인증, 암호화, 방화벽, 침입 탐지 등 정보기술을 이용하는 대책이다.
물리적 보호대책은 출입통제, 잠금장치, 감시 설비, 재해 방지 등 시설과 장비를 물리적으로 보호하는 대책이다.
따라서 보호대책의 기본 분류는 관리적·기술적·물리적 보호대책이다.

선지별 해설

① O — 관리적 보호대책은 조직의 보안정책 수립, 책임과 권한의 배분, 보안교육 및 절차 운영을 포함하는 정식 보호대책이다.
② O — 기술적 보호대책은 인증·접근통제·암호화와 같은 기술로 정보시스템의 기밀성, 무결성, 가용성을 보호하는 정식 보호대책이다.
③ X — 틀린 표현은 '소프트웨어공학적 보호대책'이다. 이는 정보시스템 보호대책의 기본 분류에 해당하지 않는다. 올바르게는 보호대책을 관리적·기술적·물리적 보호대책으로 구분한다. 안전한 소프트웨어 개발 기법은 기술적 보호 활동에 포함될 수 있지만 독립된 기본 분류는 아니다.
④ O — 물리적 보호대책은 전산실 출입통제, 잠금장치, 감시 설비 등으로 시설과 장비에 대한 물리적 접근과 재해 위험을 통제하는 정식 보호대책이다.

오답 포인트

③의 '소프트웨어공학적'이라는 표현은 보안과 관련 있어 보이지만, 보호대책의 기본 분류 명칭이 아니다. 개발 단계의 보안 기법과 조직 차원의 보호대책 분류를 혼동하면 오답이 된다.

다시 나오면 이렇게 판단

보호대책의 종류를 묻는 문항에서는 사람·정책·절차이면 관리적, 정보기술이면 기술적, 시설·장비·출입이면 물리적으로 판단한다. 이 세 범주 밖의 그럴듯한 명칭은 기본 분류인지 확인한다.

NoteBase

암기 포인트

정보시스템 보호대책의 3대 분류는 관리적·기술적·물리적 보호대책이다.

NoteBase

문 3. 다음 중 정보시스템에 대한 가장 대표적인 가용성(Availability) 공격은?

① 스니핑(Sniffing) 공격

② 변조(Modification) 공격

③ 위장(Masquerading) 공격

④ 분산서비스거부(Distributed Denial of Service) 공격

정답 4번

출제 포인트

정보보안의 핵심 속성인 기밀성·무결성·가용성과 대표 공격의 대응 관계를 묻는 문제이다.

핵심 개념

가용성은 인가된 사용자가 필요할 때 정보와 시스템을 정상적으로 사용할 수 있는 성질이다.
기밀성은 인가되지 않은 자의 정보 열람을 막는 성질이고, 무결성은 정보가 허가 없이 변경되거나 훼손되지 않도록 하는 성질이다.
서비스 거부 공격은 시스템의 자원을 소진하거나 통신을 방해하여 정상적인 이용을 어렵게 하므로 가용성을 침해한다.

선지별 해설

① X — 스니핑은 네트워크상의 데이터를 몰래 엿듣거나 수집하는 공격이므로 대표적으로 기밀성을 침해한다. 틀린 부분은 가용성 공격으로 본 점이며, 올바르게는 기밀성 공격이다.
② X — 변조는 데이터의 내용이나 상태를 허가 없이 바꾸는 공격이므로 대표적으로 무결성을 침해한다. 틀린 부분은 가용성 공격으로 본 점이며, 올바르게는 무결성 공격이다.
③ X — 위장은 공격자가 다른 사용자나 시스템인 것처럼 신분을 속이는 공격이므로 인증 또는 진정성에 대한 위협이다. 틀린 부분은 가용성 공격으로 본 점이며, 올바르게는 신원 확인과 인증을 침해하는 공격이다.
④ O — 분산서비스거부 공격은 다수의 시스템에서 대량의 요청이나 트래픽을 보내 대상의 자원을 고갈시키고 정상 사용자의 서비스 이용을 막는다. 시스템을 필요할 때 사용할 수 없게 하므로 대표적인 가용성 공격이다.

오답 포인트

모든 선지가 정보시스템 공격이라는 공통점 때문에 공격의 대상 속성을 혼동하기 쉽다. 이 문항에서는 ④의 '서비스거부'가 정상적인 서비스 이용 자체를 막는다는 점이 결정적이다.

다시 나오면 이렇게 판단

정보를 몰래 보면 기밀성, 내용을 바꾸면 무결성, 신분을 속이면 인증·진정성, 서비스를 쓰지 못하게 하면 가용성 침해로 판단한다.

NoteBase

암기 포인트

스니핑은 기밀성, 변조는 무결성, 위장은 인증, 서비스 거부는 가용성이다.

NoteBase

문 4. 다음 중 정보시스템 관리자를 속이거나 협박하여 정보시스템에 침입해서 불법적인 행위를 하는 공격은?

① 사회공학적공격(Social Enginnering Attack)

② 소프트웨어 공학적공격(SW Enginnering Attack)

③ 중간공격자 공격(Man In The Middle Attack)

④ 다중수준 보안공격(Multi Level Security Attack)

정답 1번

출제 포인트

이 문제는 사람의 심리와 신뢰를 악용하는 사회공학적 공격을 다른 보안 용어와 구별하는 문제이다.

핵심 개념

사회공학적 공격(Social Engineering Attack)은 시스템의 기술적 취약점보다 사람의 신뢰, 두려움, 호기심 등을 악용하여 비밀번호나 접근 권한 같은 정보를 얻거나 특정 행동을 유도하는 공격이다. 관리자를 속이거나 협박하여 침입에 필요한 도움을 얻는 행위가 대표적인 예이다.
중간자 공격(Man-in-the-Middle Attack)은 통신하는 두 당사자 사이에 공격자가 끼어들어 정보를 도청하거나 변조하는 기술적 공격이다.
다중수준 보안(Multi-Level Security)은 서로 다른 보안등급의 정보를 등급과 권한에 따라 통제하는 보안 모델이다.

선지별 해설

① O — 사회공학적 공격은 관리자의 심리를 이용하여 속이거나 협박하는 등 사람을 조작해 시스템 접근 정보나 권한을 얻는 공격이므로 문제의 설명에 해당한다.
② X — 틀린 표현은 '소프트웨어 공학적 공격'이다. 소프트웨어 공학은 소프트웨어를 체계적으로 개발·운영·유지보수하는 분야이지, 제시된 행위의 공격 유형이 아니다. 올바르게는 '사회공학적 공격'이다.
③ X — 중간자 공격은 공격자가 통신 당사자 사이에 개입하여 통신 내용을 도청하거나 변조하는 공격이다. 관리자를 속이거나 협박하는 공격은 중간자 공격이 아니라 사회공학적 공격이다.
④ X — 틀린 표현은 '다중수준 보안공격'이다. 다중수준 보안은 보안등급과 사용자 권한에 따라 정보 접근을 통제하는 보안 모델이지, 사람을 기만하는 공격 유형이 아니다. 올바르게는 '사회공학적 공격'이다.

오답 포인트

③의 중간자 공격도 정보 탈취와 관련되지만 공격 대상이 사람의 심리가 아니라 통신 경로라는 점이 다르다. 또한 ②와 ④는 보안·소프트웨어 분야의 전문용어처럼 보이지만 제시된 행위를 가리키는 표준 공격 유형이 아니다.

NoteBase

다시 나오면 이렇게 판단

속임수, 협박, 사칭, 회유처럼 사람을 조작하면 사회공학적 공격으로 판단한다. 통신 사이에 개입하면 중간자 공격, 보안등급별 접근 통제라면 다중수준 보안으로 구별한다.

암기 포인트

사람의 심리를 해킹하면 사회공학, 통신의 사이를 가로채면 중간자 공격이다.

NoteBase

문 5. 다음 중 현재 시행중인 보안 관련 인증제와 가장 관계가 먼 것은?

① CC(Common Criteria) 인증제

② GS(Good SW)품질 인증제

③ KCMVP(Korea Cryptographic Module Verification Program) 인증제

④ ISMS(Information Security Management System) 인증제

정답 2번

출제 포인트

이 문제는 인증 대상이 정보보호제품·암호모듈·정보보호 관리체계인지, 소프트웨어의 일반 품질인지 구별하는 문제이다.

핵심 개념

CC는 정보보호제품의 보안 기능과 신뢰성을 평가·인증하는 제도이다. KCMVP는 국가·공공망에서 사용하는 암호모듈의 안전성과 구현 적합성을 검증하는 제도이다. ISMS는 조직의 정보보호 관리체계가 인증기준에 적합한지를 심사하는 제도이다. GS는 소프트웨어의 기능성·신뢰성·사용성 등 제품 품질을 종합적으로 시험·평가하는 제도로서 보안에 한정되지 않는다.

선지별 해설

① O — CC(Common Criteria) 인증제는 정보보호제품의 보안 기능과 보증 수준을 공통평가기준에 따라 평가·인증하므로 보안과 직접 관련된다.
② X — GS(Good Software) 품질 인증제는 사무용·모바일·보안·임베디드 등 소프트웨어 전 분야의 품질을 종합 평가한다. 틀린 부분은 이를 보안 관련 인증제로 본 점이다. 올바르게는 '소프트웨어 전반의 품질 인증제'이다.
③ O — KCMVP는 암호모듈이 정해진 검증기준에 부합하는지 시험하여 안전성과 구현 적합성을 확인하므로 보안과 직접 관련된다.
④ O — ISMS 인증제는 조직이 정보자산 보호를 위한 관리체계를 수립·운영하고 있는지를 심사하므로 보안과 직접 관련된다.

오답 포인트

GS의 품질평가 대상에는 보안 소프트웨어도 포함될 수 있어 보안 인증처럼 보이기 쉽다. 그러나 GS의 핵심은 특정 보안성 검증이 아니라 소프트웨어 제품의 전반적인 품질 평가이다.

NoteBase

다시 나오면 이렇게 판단

인증의 적용 대상을 기준으로 구분한다. 정보보호제품은 CC, 암호모듈은 KCMVP, 조직의 정보보호 관리체계는 ISMS, 소프트웨어 전반의 제품 품질은 GS에 해당한다.

암기 포인트

CC는 보안제품, KCMVP는 암호모듈, ISMS는 보안관리체계, GS는 SW 품질이다.

NoteBase

문 6. 다음 중 하이브리드 암호시스템(Hybrid Cryptography System)에서 대칭키 암호알고리즘을 사용하는 가장 큰 이유는?

① 안전한 대칭키 분배용으로 활용

② 대량의 데이터에 대해 고속 암호화에 활용

③ 생성된 일회용 세션키 암호화에 활용

④ 고속의 공개키 암호시스템 보조용으로 활용

정답 2번

출제 포인트

하이브리드 암호시스템에서 대칭키 암호와 공개키 암호가 각각 맡는 역할을 구분하는 문제이다.

핵심 개념

하이브리드 암호시스템은 공개키 암호의 안전한 키 전달 기능과 대칭키 암호의 빠른 데이터 처리 성능을 결합한 방식이다. 대칭키 암호는 세션키로 대량의 실제 데이터를 빠르게 암호화하고, 공개키 암호는 그 세션키를 안전하게 암호화하여 전달하는 데 사용된다.

선지별 해설

① X
틀린 표현은 '대칭키 분배용'이다. 대칭키 암호는 송신자와 수신자가 같은 비밀키를 미리 공유해야 하므로 그 자체로 안전한 키 분배 문제를 해결하지 못한다. 올바르게는 공개키 암호나 키 합의 방식을 이용하여 대칭 세션키를 안전하게 공유한다.

② O
대칭키 암호는 공개키 암호보다 연산 부담이 작고 처리 속도가 빠르므로 대량의 데이터를 고속으로 암호화하는 데 적합하다. 이것이 하이브리드 암호시스템에서 대칭키 암호를 사용하는 가장 큰 이유이다.

③ X
틀린 표현은 '세션키 암호화에 활용'이다. 생성된 세션키를 암호화하여 전달하는 역할은 수신자의 공개키를 사용하는 공개키 암호가 맡는다. 올바르게는 대칭키 암호가 그 세션키를 사용하여 실제 데이터를 암호화한다.

④ X
틀린 표현은 '고속의 공개키 암호시스템'이다. 공개키 암호는 일반적으로 대칭키 암호보다 느리며, 대칭키 암호는 공개키 암호를 단순히 보조하려는 것이 아니라 실제 대량 데이터의 고속 암호화를 담당한다. 올바르게는 공개키 암호가 세션키의 안전한 전달을 담당하고 대칭키 암호가 데이터의 빠른 암호화를 담당한다.

NoteBase

오답 포인트

①과 ③은 키를 안전하게 전달하는 역할과 전달된 키로 데이터를 암호화하는 역할을 뒤바꾼 선지이다. ④는 공개키 암호 자체가 고속이라는 잘못된 전제를 넣어 두 방식의 결합 목적을 흐린다.

다시 나오면 이렇게 판단

‘실제 데이터·대용량·속도’가 핵심이면 대칭키 암호, ‘세션키 전달·키 분배·공개키로 암호화’가 핵심이면 공개키 암호로 판단한다.

암기 포인트

공개키로 세션키를 안전하게 전달하고, 대칭키로 본문 데이터를 빠르게 암호화한다.

NoteBase

문 7. 다음 <보기> 설명에서 ㉠, ㉡, ㉢에 들어갈 용어를 순서대로 나열한 것은?

<보기>
저작물의 원본을 왜곡하지 않는 범위 내에서 저작권 정보를 삽입하는 기술을 (㉠)이라 하고, 디지털 콘텐츠를 판매할 때 구매자 정보를 삽입하여 불법 배포가 이루어질 경우 최초의 구매자를 추적하는 기술을 (㉡)이라 한다. 또한 디지털콘텐츠의 지적재산권이 안전하게 보호되도록 창작에서 소비까지 전 과정이 적법하게 이루어지도록 하는 기술을 (㉢)이라 한다.

① DRM(Digital Right Management), 워터마킹(Watermarking), 핑거프린팅(Fingerprinting)
② 핑거프린팅(Fingerprinting), DRM(Digital Right Management), 워터마킹(Watermarking)
③ 워터마킹(Watermarking), 핑거프린팅(Fingerprinting), DRM(Digital Right Management)
④ DRM(Digital Right Management), 핑거프린팅(Fingerprinting), 워터마킹(Watermarking)

정답 3번

출제 포인트

이 문제는 워터마킹, 핑거프린팅, DRM을 삽입 정보와 보호 범위에 따라 구별하는 문제이다.

핵심 개념

워터마킹(Watermarking): 콘텐츠에 저작권자 정보 등 식별 정보를 삽입하여 저작권을 표시하고 불법 복제를 억제하는 기술이다. 키워드는 저작권 정보이다.
핑거프린팅(Fingerprinting): 판매되는 콘텐츠마다 구매자 정보를 다르게 삽입하여 불법 배포본의 최초 구매자를 추적하는 기술이다. 키워드는 구매자 정보와 추적이다.
DRM(Digital Rights Management): 디지털 콘텐츠의 생성·유통·이용 전 과정에서 접근과 사용 권한을 관리하여 지적재산권을 보호하는 기술이다. 키워드는 전 과정의 권리 관리이다.

선지별 해설

① X — ㉠에 DRM, ㉡에 워터마킹, ㉢에 핑거프린팅을 배치한 부분이 모두 틀렸다. 올바르게는 ㉠ 워터마킹, ㉡ 핑거프린팅, ㉢ DRM이다.
② X — ㉠의 핑거프린팅, ㉡의 DRM, ㉢의 워터마킹이 각각 정의와 맞지 않는다. 올바르게는 저작권 정보 삽입은 워터마킹, 구매자 정보 삽입과 추적은 핑거프린팅, 전 과정의 권리 관리는 DRM이다.
③ O — 저작권 정보를 삽입하는 ㉠은 워터마킹, 구매자 정보를 삽입하여 최초 구매자를 추적하는 ㉡은 핑거프린팅, 창작부터 소비까지 권리를 관리하는 ㉢은 DRM이다.
④ X — ㉡의 핑거프린팅만 맞고, ㉠의 DRM과 ㉢의 워터마킹이 서로 잘못 배치되었다. 올바르게는 ㉠ 워터마킹, ㉡ 핑거프린팅, ㉢ DRM이다.

NoteBase

오답 포인트

세 기술이 모두 디지털 저작권 보호에 쓰인다는 공통점 때문에 용어를 바꾸어 놓기 쉽다. 특히 ④는 구매자 추적에 해당하는 핑거프린팅을 ㉡에 맞게 두고 ㉠과 ㉢만 바꾸어 놓은 함정이다.

다시 나오면 이렇게 판단

삽입되는 정보의 주체와 보호 범위를 확인한다. 저작권자·저작권 정보이면 워터마킹, 구매자별 정보와 유출자 추적이면 핑거프린팅, 콘텐츠의 생성부터 소비까지 이용 권한을 통제하면 DRM으로 판단한다.

암기 포인트

저작권 표시＝워터마킹, 구매자 추적＝핑거프린팅, 전 과정 권리 관리＝DRM이다.

NoteBase

문 8. 다음 중 대칭키 암호알고리즘과 가장 관련이 없는 것은?

① RSA(Rivest Shamir Adleman)

② ARIA(Academy Research Institute Agency)

③ SPN(Substitution Permutation Network)

④ AES(Advanced Encryption Standard)

정답 1번

출제 포인트

대칭키 암호와 공개키 암호를 구분하고, 대칭키 블록 암호에 사용되는 구조를 판별하는 문제이다.

핵심 개념

대칭키 암호는 암호화와 복호화에 동일한 비밀키를 사용하는 방식이다. 공개키 암호는 공개키와 개인키의 쌍을 사용하는 비대칭키 방식이다.
ARIA와 AES는 대칭키 블록 암호이고, SPN은 치환과 순열을 반복하여 대칭키 블록 암호를 구성하는 대표적 구조이다. RSA는 공개키 암호이므로 나머지와 구별된다.

선지별 해설

① O — RSA는 공개키와 개인키를 사용하는 비대칭키 암호알고리즘이다. 따라서 대칭키 암호알고리즘과 가장 관련이 없다.
② X — ‘ARIA가 대칭키 암호알고리즘과 관련이 없다’는 판단이 틀리다. ARIA는 대칭키 방식의 블록 암호알고리즘이다.
③ X — ‘SPN이 대칭키 암호알고리즘과 관련이 없다’는 판단이 틀리다. SPN은 특정 암호알고리즘의 이름이라기보다 치환과 순열을 반복하는 암호 구조이며, 여러 대칭키 블록 암호의 설계에 사용된다.
④ X — ‘AES가 대칭키 암호알고리즘과 관련이 없다’는 판단이 틀리다. AES는 동일한 비밀키를 사용하는 대표적인 대칭키 블록 암호 표준이다.

오답 포인트

③의 SPN은 개별 암호알고리즘명이 아니라 설계 구조이므로 낯설 수 있다. 그러나 대칭키 블록 암호와 밀접한 구조이므로 ‘가장 관련이 없는 것’이 아니다. 공개키와 개인키의 쌍을 사용하는 ① RSA만 성격이 다르다.

다시 나오면 이렇게 판단

암호 방식의 키 구성을 먼저 확인한다. 같은 비밀키를 사용하면 대칭키, 공개키와 개인키의 쌍을 사용하면 비대칭키로 판단한다. 구조명이 제시되면 치환·순열 구조가 대칭키 블록 암호 설계와 연결되는지도 함께 확인한다.

NoteBase

암기 포인트

RSA는 비대칭키, ARIA와 AES는 대칭키 블록 암호, SPN은 대칭키 블록 암호의 대표적 설계 구조이다.

NoteBase

문 9. 다음 중 대칭키 분배 방법 중에서 중간자공격(Man in The Middle Attack)에 가장 취약한 것은?

① 대칭키를 사전에 공유법

② Diffie-Hellman 키 분배 알고리즘에 의한 분배

③ 키 분배센터(KDC, Key Distribution Cenetr)에 의한 분배

④ PKI(Public Key Infrastructure)기반의 공개키 암호 시스템을 활용한 분배

정답 2번

출제 포인트

대칭키를 전달하거나 합의할 때 통신 상대의 신원을 인증할 수 있는지와 공격자가 키 교환 과정에 개입할 수 있는지를 묻는 문제이다.

핵심 개념

중간자 공격은 공격자가 두 통신자 사이에 끼어 각 통신자와 별도의 키를 만들고 메시지를 중계·변조하는 공격이다. 기본 Diffie-Hellman 키 교환은 비밀값을 직접 보내지 않고 공유 비밀을 합의하지만, 그 자체로는 상대방을 인증하지 않는다. 따라서 전자서명, 인증서, 사전 공유 인증값 등으로 교환 메시지를 인증하지 않으면 중간자 공격에 취약하다.

NoteBase

선지별 해설

① X
대칭키 사전 공유는 통신 전에 안전한 경로로 같은 비밀키를 전달해 두는 방식이다. 이미 안전하게 공유되었다는 전제에서는 키 교환 중 공격자가 공개값을 바꾸어 각 당사자와 별도 키를 만드는 기본 Diffie-Hellman의 취약성이 나타나지 않는다. 틀린 판단은 '사전 공유법이 중간자 공격에 가장 취약하다'는 것이며, 올바르게는 사전 공유 경로의 보안과 키 관리가 핵심 위험이다.

② O
인증되지 않은 기본 Diffie-Hellman에서는 공격자가 양쪽의 공개값을 자신의 공개값으로 바꾸고, 각 당사자와 서로 다른 공유키를 만들 수 있다. 두 당사자는 직접 같은 키를 합의했다고 착각하므로 제시된 방법 중 중간자 공격에 가장 취약하다.

③ X
KDC 방식에서는 신뢰하는 키 분배센터가 각 사용자의 기존 비밀키를 바탕으로 세션키를 안전하게 전달한다. KDC 자체의 침해나 인증 실패는 큰 위험이지만, 정상적인 인증·암호화 절차를 전제로 하면 기본 Diffie-Hellman처럼 상대 인증이 본질적으로 빠진 방식은 아니다. 틀린 판단은 'KDC 방식이 중간자 공격에 가장 취약하다'는 것이며, 올바르게는 KDC의 신뢰성과 장기키 보호가 핵심이다.

④ X
PKI 기반 방식은 인증기관이 발급한 인증서로 공개키와 소유자의 신원을 연결하고, 검증된 공개키를 이용해 대칭키를 보호한다. 인증서를 정상적으로 검증하면 공격자의 공개키 바꿔치기를 막을 수 있다. 틀린 판단은 'PKI 방식이 중간자 공격에 가장 취약하다'는 것이며, 올바르게는 인증서의 유효성 및 신뢰 경로 검증이 필요하다.

오답 포인트

Diffie-Hellman이 도청자에게 비밀키를 노출하지 않는다는 성질을 상대방 인증까지 제공한다는 뜻으로 오해하기 쉽다. 이 문항의 함정은 '키를 안전하게 합의한다'와 '키를 누구와 합의하는지 인증한다'를 혼동하게 하는 데 있다.

다시 나오면 이렇게 판단

키 분배 방식을 비교할 때는 먼저 상대 인증 수단이 있는지를 확인한다. 공개값만 교환하고 서명·인증서·사전 공유 인증값이 없다면 공격자가 공개값을 바꿀 수 있으므로 중간자 공격 취약성을 우선 판단한다.

암기 포인트

기본 Diffie-Hellman은 키 합의는 제공하지만 상대 인증은 제공하지 않으므로, 인증이 없으면 중간자 공격에 취약하다.

NoteBase

문 10. A가 B에게 공개키 암호시스템을 이용하여 메시지를 암호화하여 보내고 싶다. A는 어떻게 암호화해야 하는가?

① A의 공개키로 메시지를 암호화하여 B에게 보낸다.

② A의 개인키로 메시지를 암호화하여 B에게 보낸다.

③ B의 공개키로 메시지를 암호화하여 B에게 보낸다.

④ B의 개인키로 메시지를 암호화하여 B에게 보낸다.

정답 3번

출제 포인트

이 문제는 공개키 암호시스템에서 기밀성을 확보할 때 누구의 공개키로 암호화해야 하는지를 묻는 문제이다.

핵심 개념

공개키 암호시스템에서는 수신자의 공개키로 메시지를 암호화하고, 그 공개키와 쌍을 이루는 수신자의 개인키로 복호화한다. 공개키는 다른 사람에게 알려도 되지만 개인키는 소유자만 보관하므로, B만 읽게 하려면 B의 공개키로 암호화해야 한다.
기밀성은 '수신자의 공개키 → 수신자의 개인키'로 판단한다. 반면 송신자의 개인키를 이용하는 방식은 송신자 확인과 전자서명의 원리에 해당하며 메시지의 기밀성을 위한 방식이 아니다.

NoteBase

선지별 해설

① X
A의 공개키로 암호화한 메시지는 A의 개인키로 복호화하는 구조이므로, B에게만 안전하게 전달하려는 목적에 맞지 않는다. 틀린 표현은 ‘A의 공개키’이며, 올바르게는 ‘B의 공개키’로 암호화해야 한다.

② X
A의 개인키를 이용하는 것은 A가 만든 메시지임을 확인하는 전자서명의 원리와 관련되며, B만 메시지를 읽게 하는 기밀성 방식이 아니다. 틀린 표현은 ‘A의 개인키’이며, 올바르게는 ‘B의 공개키’로 암호화해야 한다.

③ O
B의 공개키로 암호화하면 그 키와 쌍을 이루는 B의 개인키로만 복호화할 수 있으므로, 수신자인 B에게 메시지의 기밀성을 보장할 수 있다.

④ X
B의 개인키는 B만 비밀리에 보관해야 하므로 A가 암호화에 사용해서는 안 된다. 또한 기밀성 확보의 올바른 구조는 B의 공개키로 암호화하고 B의 개인키로 복호화하는 것이다. 틀린 표현은 ‘B의 개인키’이며, 올바르게는 ‘B의 공개키’이다.

오답 포인트

‘보내는 사람이 A이므로 A의 키를 쓴다’고 생각하기 쉽지만, 기밀성을 위한 암호화 키는 송신자가 아니라 복호화할 수신자를 기준으로 고른다. 특히 ②의 ‘A의 개인키’는 전자서명 원리와 혼동하게 만드는 표현이다.

다시 나오면 이렇게 판단

누구만 평문을 읽어야 하는지 먼저 확인한다. B만 읽어야 한다면 B만 가진 개인키로 복호화할 수 있도록 B의 공개키로 암호화한다. 송신자의 개인키가 제시되면 기밀성이 아니라 서명·인증의 맥락인지 구분한다.

암기 포인트

기밀성은 수신자 공개키로 암호화하고 수신자 개인키로 복호화한다. 서명은 송신자 개인키가 핵심이다.

NoteBase

문 11. 다음 중 재전송 공격(Replay Attack)의 방어법이 아닌 것은?

① 초기벡터(IV, Initial Vector) 사용

② 타임스템프(Timestamp) 사용

③ 비표(Nonce) 사용

④ 순서번호(Sequence Number) 사용

정답 1번

출제 포인트

재전송 공격을 막는 메시지 신선성 확인 수단과 암호화에 쓰는 초기벡터의 역할을 구별하는 문제이다.

핵심 개념

재전송 공격은 공격자가 이전에 전송된 정상 메시지를 가로채 저장한 뒤 다시 보내 인증이나 거래를 반복시키는 공격이다. 방어의 핵심은 타임스탬프, 비표, 순서번호처럼 메시지가 이번 통신에서 새로 생성되었음을 확인하고 이미 처리한 메시지를 거부하는 것이다. 초기벡터는 같은 평문을 암호화하더라도 암호문이 반복되는 것을 줄이는 등 암호화의 안전성을 위한 입력값이며, 그 자체로 과거 메시지의 재사용 여부를 판별하지는 않는다.

선지별 해설

① X

초기벡터 사용 자체는 메시지의 신선성이나 중복 수신 여부를 확인하는 장치가 아니므로 일반적인 재전송 공격 방어법이 아니다. 틀린 표현은 '초기벡터 사용'이며, 재전송 방어에는 타임스탬프·비표·순서번호와 같은 신선성 확인값을 인증 대상에 포함하고 재사용을 거부해야 한다.

② O

타임스탬프를 사용하면 수신 시각과 허용 시간 범위를 비교하여 지나치게 오래된 메시지를 거부할 수 있으므로 재전송을 탐지하는 데 쓰인다.

③ O

비표는 한 번만 사용하는 임의값이다. 요청마다 새 비표를 사용하고 이미 사용한 값을 다시 받아들이지 않으면 과거 응답이나 메시지의 재전송을 차단할 수 있다.

④ O

순서번호를 사용하면 수신자가 기대하는 번호 또는 이미 처리한 번호를 확인하여 중복되거나 과거 순서번호를 가진 메시지를 거부할 수 있다.

NoteBase

오답 포인트

초기벡터와 비표가 모두 반복을 피하기 위한 값처럼 보인다는 점이 함정이다. 비표는 통신의 신선성을 입증하는 데 직접 쓰이지만, 초기벡터는 기본적으로 암호화 결과의 반복을 피하기 위한 값이므로 역할이 다르다.

다시 나오면 이렇게 판단

선지가 과거 메시지인지 판별하거나 중복 사용을 거부하게 만드는 값인지 확인한다. 시간 유효성을 검사하는 타임스탬프, 일회성을 보장하는 비표, 중복과 순서를 확인하는 순서번호는 재전송 방어 수단이고, 암호화 입력을 다양화할 뿐인 초기벡터는 단독 방어 수단이 아니다.

암기 포인트

재전송 방어는 신선성 확인이다. 시간은 타임스탬프, 일회성은 비표, 중복·순서는 순서번호로 확인한다.

NoteBase

문 12. 한번의 시스템 인증을 통해 재인증 절차 없이 정보 시스템들에 대해 접근할 수 있는 통합 로그인 제품은?

① SSO(Single Sign On)

② SAC(Server Access Control)

③ RBAC(Role Base Access Control)

④ TSO(Trust Sign On)

정답 1번

출제 포인트

한 번의 인증으로 여러 정보시스템을 재인증 없이 이용하게 하는 통합 인증 방식이 SSO임을 묻는 문제이다.

핵심 개념

SSO(Single Sign-On)는 사용자가 한 번 인증하면 서로 연계된 여러 시스템이나 서비스에 추가 로그인 없이 접근할 수 있게 하는 통합 인증 방식이다.
SAC는 서버 접근 통제, RBAC는 역할 기반 접근 통제로서 인증 이후의 접근 권한을 관리하는 개념이다.

선지별 해설

① O — SSO(Single Sign-On)는 한 번의 인증 결과를 연계된 여러 정보시스템에서 이용하므로 재인증 없이 접근할 수 있다.
② X — 틀린 표현은 SAC(Server Access Control)이다. SAC는 서버에 대한 사용자의 접속과 행위를 통제하는 접근통제 방식이며, 제시된 통합 로그인 제품은 SSO이다.
③ X — 틀린 표현은 RBAC(Role Base Access Control)이다. 올바른 명칭은 RBAC(Role-Based Access Control)이며, 사용자에게 직접 권한을 주기보다 역할에 권한을 부여하는 접근통제 방식이다. 제시된 통합 로그인 제품은 SSO이다.
④ X — 틀린 표현은 TSO(Trust Sign On)이다. 한 번의 인증으로 여러 시스템에 접속하는 표준적인 통합 로그인 개념은 TSO가 아니라 SSO(Single Sign-On)이다.

오답 포인트

SSO와 SAC·RBAC는 모두 보안과 접근에 관련되지만 기능이 다르다. 문제의 핵심 표현인 '한 번의 인증'과 '재인증 없이 여러 시스템 접근'은 접근 권한 부여가 아니라 통합 로그인을 뜻한다.

다시 나오면 이렇게 판단

한 번 로그인하여 여러 시스템을 이용한다는 문구가 나오면 SSO로 판단한다. 사용자나 역할별로 허용 권한을 나누는 내용이면 접근통제로 구분한다.

NoteBase

암기 포인트

한 번 인증·여러 시스템은 SSO, 역할에 따른 권한 부여는 RBAC이다.

NoteBase

문 13. 다음 중 컴퓨터에 침투하여 주요 파일을 암호화하고 컴퓨터 사용자에게 암호화된 파일의 복호화 키를 알려준다는 조건으로 금전 등을 요구하는 악성코드는?

① 웜(Worm)
② 매크로 바이러스(Mecro Virus)
③ 랜섬웨어(Ransomware)
④ 트로이목마(Trojan Horse)

정답 3번

출제 포인트

파일을 암호화한 뒤 복호화를 대가로 금전을 요구하는 악성코드가 랜섬웨어임을 구별하는 문제이다.

핵심 개념

랜섬웨어는 파일이나 시스템을 암호화하거나 사용하지 못하게 만든 뒤, 복구를 조건으로 금전을 요구하는 악성코드이다.
웜은 스스로 복제하여 네트워크로 확산하고, 매크로 바이러스는 문서의 매크로 기능을 이용하며, 트로이목마는 정상 프로그램으로 위장하여 악성 기능을 수행한다.

선지별 해설

① X — 웜(Worm)은 자기 복제와 네트워크 확산이 핵심이다. 파일을 암호화하고 복호화 키를 조건으로 금전을 요구하는 악성코드는 웜이 아니라 랜섬웨어이다.
② X — 매크로 바이러스(Mecro Virus)는 문서 프로그램의 매크로 기능을 이용해 감염·전파되는 바이러스이다. 제시된 행위는 매크로 바이러스가 아니라 랜섬웨어의 특징이다.
③ O — 랜섬웨어(Ransomware)는 주요 파일을 암호화한 뒤 복호화 또는 접근 복구를 대가로 금전을 요구하므로 제시된 설명과 일치한다.
④ X — 트로이목마(Trojan Horse)는 유용하거나 정상적인 프로그램으로 위장해 사용자가 실행하도록 유도하는 악성코드이다. 파일 암호화 후 금전을 요구하는 유형은 트로이목마가 아니라 랜섬웨어이다.

오답 포인트

악성코드라는 공통점만 보고 웜이나 트로이목마를 고르면 안 된다. 이 문항의 결정적 표현은 '파일 암호화', '복호화 키', '금전 요구'이며, 이 세 단서가 랜섬웨어를 가리킨다.

다시 나오면 이렇게 판단

감염 방식보다 공격 목적과 행위를 확인한다. 자기 복제·확산은 웜, 문서 매크로 이용은 매크로 바이러스, 정상 프로그램 위장은 트로이목마, 암호화·접근 차단 뒤 대가 요구는 랜섬웨어로 판단한다.

NoteBase

암기 포인트

암호화 후 몸값 요구는 랜섬웨어이다.

NoteBase

문 14. 다음 중 PKI에 관한 설명 중 가장 옳지 않은 것은?

① PKI란 Public Key Infrastructure의 약어로 공개키 암호 알고리즘을 적용하고 인증서를 관리하기 위한 기반시스템이다.

② 주로 X.509 인증서를 사용하고 있다.

③ 인증서를 발급하는 역할을 하는 기관을 RA라 한다.

④ 인증서의 폐기 여부를 확인하기 위해 사용되는 프로토콜은 OCSP이다.

정답 3번

출제 포인트

이 문제는 PKI의 목적과 인증서 형식, CA·RA의 역할, 인증서 상태 확인 방식을 구별하는 문제이다.

핵심 개념

PKI(Public Key Infrastructure)는 공개키 암호 기술을 바탕으로 인증서를 발급·관리·검증하여 공개키의 소유자를 신뢰할 수 있게 하는 기반 체계이다. CA는 인증서를 발급하고 서명하는 인증기관이며, RA는 신청자의 신원과 등록 정보를 확인하여 인증서 발급 절차를 지원하는 등록기관이다. X.509는 대표적인 공개키 인증서 표준이고, OCSP는 인증서의 현재 폐기 상태를 온라인으로 조회하는 프로토콜이다.

선지별 해설

① O — PKI는 Public Key Infrastructure의 약어이며, 공개키 암호 기술을 이용해 인증서의 발급·관리·검증을 지원하는 기반시스템이다.
② O — PKI에서는 공개키와 소유자 정보를 결합한 인증서의 대표적 표준으로 X.509를 사용한다.
③ X — 틀린 표현은 '인증서를 발급하는 역할을 하는 기관을 RA라 한다'이다. 인증서를 발급하고 전자서명하는 기관은 CA이며, RA는 인증서 신청자의 신원 및 등록 정보를 확인하여 CA의 발급 업무를 지원한다.
④ O — OCSP는 특정 인증서가 폐기되었는지 등 현재 상태를 온라인으로 확인하는 데 사용하는 프로토콜이다.

오답 포인트

③은 CA와 RA의 역할을 바꾸어 제시한 선지이다. RA가 신청자 확인과 등록을 담당한다는 이유만으로 인증서의 실제 발급 주체까지 RA라고 판단하면 틀린다.

다시 나오면 이렇게 판단

PKI 기관의 역할은 'CA는 인증서 발급·서명, RA는 신청자 신원 확인·등록'으로 구분한다. 인증서 형식은 X.509, 인증서의 온라인 상태 조회는 OCSP로 연결하면 된다.

NoteBase

암기 포인트

CA는 발급, RA는 등록 확인, X.509는 인증서 형식, OCSP는 폐기 상태 조회이다.

NoteBase

문 15. 다음 중 시스템 설계자가 서비스 기술자와 유지보수 기술자를 위하여 특정 컴퓨터에 접근을 편리하게 할 수 있도록 고의적으로 만든 악성코드는?

① 애드웨어(Adware)

② 백도어(Backdoor)

③ 매크로 바이러스(Macro Virus)

④ 웜(Worm)

정답 2번

출제 포인트

시스템에 정상적인 인증 절차를 우회하여 접근할 수 있도록 의도적으로 마련한 비밀 접근 통로가 백도어임을 묻는 문제이다.

핵심 개념

백도어는 정상적인 인증·보안 절차를 거치지 않고 시스템에 접근할 수 있게 만든 숨은 통로이다.
개발·유지보수의 편의를 위해 고의로 넣은 접근 수단도 악용될 수 있으므로 백도어에 해당한다.
애드웨어는 광고 노출, 매크로 바이러스는 문서의 매크로 기능을 이용한 감염, 웜은 스스로 복제하여 네트워크로 확산하는 것이 핵심이다.

선지별 해설

① X — '애드웨어'가 틀린 연결이다. 애드웨어는 광고를 표시하거나 광고 목적의 정보를 수집하는 프로그램이다. 올바르게는 제시된 설명에 해당하는 개념은 '백도어'이다.
② O — 백도어는 시스템 설계자나 개발자가 점검·서비스·유지보수 등을 위해 의도적으로 만들어 둔 비밀 접근 경로를 뜻한다. 정상적인 접근 통제를 우회할 수 있다는 점이 문제의 설명과 일치한다.
③ X — '매크로 바이러스'가 틀린 연결이다. 매크로 바이러스는 문서 프로그램의 매크로 기능을 이용하여 문서나 서식 파일을 감염시키는 악성코드이다. 올바르게는 의도적으로 만든 숨은 접근 통로는 '백도어'이다.
④ X — '웜'이 틀린 연결이다. 웜은 다른 파일에 기생하지 않고 스스로 복제하며 주로 네트워크를 통해 확산하는 악성코드이다. 올바르게는 유지보수용으로 만들어 둔 우회 접근 수단은 '백도어'이다.

오답 포인트

'악성코드'라는 넓은 표현만 보고 전파 방식에 초점을 맞추면 매크로 바이러스나 웜을 고르기 쉽다. 이 문항의 결정적 단서는 '특정 컴퓨터에 접근', '편리하게', '고의적으로 만든'이며, 이는 감염·증식이 아니라 접근 통제 우회를 가리킨다.

NoteBase

다시 나오면 이렇게 판단

숨은 통로·인증 우회·개발자나 유지보수 담당자의 비밀 접근이라는 단서가 나오면 백도어로 판단한다. 광고 노출은 애드웨어, 문서 매크로 감염은 매크로 바이러스, 자기 복제와 네트워크 확산은 웜으로 구분한다.

암기 포인트

백도어는 정상 문을 거치지 않는 숨은 접근 통로이다.

NoteBase

문 16. 다음 중 패스워드를 저장할 때 해시를 이용하는데, 안전도를 높이기 위해 무작위 문자열을 추가한다. 이렇게 추가되는 문자열을 무엇이라 하는가?

① Nonce

② Plaintext

③ Salt

④ Cipher

정답 3번

출제 포인트

패스워드를 해시하기 전에 덧붙이는 무작위 값인 솔트(Salt)의 의미와 유사 보안 용어를 구별하는 문제이다.

핵심 개념

솔트(Salt)는 각 패스워드에 서로 다른 무작위 문자열을 더한 뒤 해시하여 같은 패스워드도 서로 다른 해시값을 갖게 하는 값이다. 미리 계산된 해시표를 이용한 공격을 어렵게 하며, 일반적으로 솔트 자체는 해시값과 함께 저장할 수 있다.
Nonce는 한 번만 사용하는 값, Plaintext는 암호화되지 않은 원문, Cipher는 암호화·복호화에 쓰는 알고리즘을 뜻한다.

선지별 해설

① X — Nonce는 통신이나 암호 프로토콜에서 한 번만 사용하여 값의 재사용이나 재전송을 막는 값이다. 틀린 표현은 ‘Nonce’이며, 패스워드 해시 전에 추가하는 무작위 문자열은 Salt이다.
② X — Plaintext는 암호화되기 전의 평문 데이터이다. 틀린 표현은 ‘Plaintext’이며, 해시 안전도를 높이려고 패스워드에 추가하는 값은 Salt이다.
③ O — Salt는 패스워드마다 생성하여 패스워드와 함께 해시하는 무작위 문자열이다. 동일한 패스워드의 해시값이 같아지는 것을 막고 사전 계산 공격의 효율을 낮춘다.
④ X — Cipher는 데이터를 암호화하거나 복호화하는 암호 알고리즘을 뜻한다. 틀린 표현은 ‘Cipher’이며, 패스워드 해시에 추가하는 무작위 문자열은 Salt이다.

오답 포인트

Nonce와 Salt가 모두 임의성이나 유일성을 활용한다는 점이 함정이다. ‘한 번만 사용하여 재사용을 방지’하면 Nonce이고, ‘패스워드에 덧붙여 해시값을 다르게 생성’하면 Salt이다.

NoteBase

다시 나오면 이렇게 판단

패스워드 저장과 해시가 함께 나오고 무작위 문자열을 추가한다고 하면 Salt로 판단한다. 프로토콜에서 한 번만 쓰는 값이면 Nonce, 암호화 전 원문이면 Plaintext, 암호화 방식이면 Cipher로 구별한다.

암기 포인트

Salt는 패스워드 해시에 섞는 값, Nonce는 한 번만 쓰는 값이다.

NoteBase

문 17. 국가안전보장에 중대한 영향을 미치는 주요정보통신기반시설에 대한 보호대책의 미흡으로 국가안전보장이나 경제사회전반에 피해가 우려될 수 있으므로 기반시설을 지정하여야 한다. 다음 중 주요정보통신기반시설이 아닌 것은 무엇인가?

① 전력, 가스, 석유 등 에너지·수자원 시설

② 인터넷포털, 전자상거래 등 인터넷시설

③ 도로, 철도, 지하철, 공항, 항만 등 주요 교통시설

④ 방송중계, 국가지도통신망 시설

정답 2번

쟁점

이 문제는 국가안전보장에 중대한 영향을 미치는 주요정보통신기반시설의 법정 범위를 구별하는 문제이다. 핵심은 「정보통신기반 보호법」 제7조 제2항에 열거된 시설인지 확인하는 것이다.

용어 풀이

주요정보통신기반시설은 국가·사회적으로 중요한 정보통신기반시설 가운데 전자적 침해행위로부터 특별히 보호할 필요가 있어 지정된 시설이다.

핵심 구분

「정보통신기반 보호법」 제7조 제2항은 국가안전보장에 중대한 영향을 미치는 시설로 주요 교통시설, 에너지·수자원 시설, 방송중계·국가지도통신망 시설, 원자력·국방과학·첨단방위산업 관련 정부출연연구기관의 연구시설을 열거한다. 인터넷포털·전자상거래 등 인터넷시설은 이 열거에 포함되지 않는다.

NoteBase

선지별 해설

① O
전력·가스·석유 등 에너지·수자원 시설은 법에서 열거한 대상이다.

② X
인터넷포털·전자상거래 등 인터넷시설은 해당 열거 대상이 아니다.
틀린 표현: 인터넷포털, 전자상거래 등 인터넷시설
올바른 표현: 원자력·국방과학·첨단방위산업 관련 정부출연연구기관의 연구시설 등이 법정 열거 대상이다.

③ O
도로·철도·지하철·공항·항만 등 주요 교통시설은 법에서 열거한 대상이다.

④ O
방송중계·국가지도통신망 시설은 법에서 열거한 대상이다.

오답 포인트

인터넷을 이용하는 서비스라는 이유만으로 모든 인터넷 관련 시설이 국가안전보장에 중대한 영향을 미치는 시설의 법정 열거에 포함된다고 판단하기 쉽다. ②의 '인터넷포털, 전자상거래'는 열거 문구에 없다는 점이 함정이다.

다시 나오면 이렇게 판단

교통, 에너지·수자원, 방송중계·국가지도통신망, 원자력·국방 관련 정부출연연구시설인지 순서대로 대조한다. 단순한 인터넷 서비스 유형은 별도의 법적 근거 없이 이 열거에 포함시키지 않는다.

암기 포인트

교통-에너지·수자원-방송·국가지도망-원자력·국방 연구시설은 포함되고, 포털·전자상거래는 제외된다.

NoteBase

문 18. 다음 보기에서 설명하는 유닉스 시스템 명령어는?

<보기>
시스템의 파일 또는 디렉토리(Directory)가 만들어질 때의 허가권(Permission)의 기본값을 정하기 위해서 사용한다. 해당 설정값은 모든 계정 사용자들에게 존재하는 값으로써 각 계정 사용자들이 생성하는 파일 또는 디렉토리(Directory)의 허가권(Permission)을 결정하기 위한 값이다.

① chmod
② umask
③ chown
④ touch

정답 2번

출제 포인트

이 문제는 파일이나 디렉터리를 새로 만들 때 기본 권한에서 제외할 권한 비트를 지정하는 umask의 기능을 묻는다.

핵심 개념

umask는 새 파일이나 디렉터리의 기본 권한을 정할 때 부여하지 않을 권한 비트를 지정하는 값이다. 일반적인 최대 기본 권한은 파일이 666, 디렉터리가 777이며, 실제 권한은 이 값에서 umask로 지정한 비트를 제거하여 결정된다.
chmod는 권한 변경, chown은 소유자·소유 그룹 변경, touch는 시간 정보 갱신이 핵심 기능이다.

선지별 해설

① X — chmod는 기존 파일이나 디렉터리의 접근 권한을 변경하는 명령어이다. 틀린 표현은 chmod이며, 새로 생성되는 파일이나 디렉터리의 기본 권한을 결정하는 설정은 umask이다.
② O — umask는 파일이나 디렉터리를 생성할 때 기본 권한에서 제외할 권한 비트를 지정하므로 보기의 설명에 해당한다.
③ X — chown은 파일이나 디렉터리의 소유자 또는 소유 그룹을 변경하는 명령어이다. 틀린 표현은 chown이며, 생성 시 기본 권한을 결정하는 설정은 umask이다.
④ X — touch는 파일의 접근·수정 시간을 갱신하며, 파일이 없으면 빈 파일을 만들 수 있는 명령어이다. 틀린 표현은 touch이며, 생성 시 적용할 기본 권한의 제외 비트를 정하는 설정은 umask이다.

NoteBase

오답 포인트

chmod도 권한을 다루므로 혼동하기 쉽다. chmod는 이미 존재하는 대상의 권한을 직접 바꾸고, umask는 앞으로 생성할 대상의 기본 권한에서 빠질 비트를 미리 정한다.

다시 나오면 이렇게 판단

문장에 '생성할 때의 기본 권한'이 나오면 umask를, '기존 파일의 권한 변경'이 나오면 chmod를 판단 기준으로 삼는다. 소유자 변경은 chown, 시간 정보 갱신은 touch에 대응한다.

암기 포인트

umask는 생성 권한의 마스크, chmod는 기존 권한의 변경이다.

NoteBase

문 19. 다음 중 지능형 지속 위협(APT, Advanced Persistent Threat)에 대한 설명으로 가장 옳은 것은?

① 공격의 설계부터 침투까지 매우 빠른 시간 내에 이루어진다.

② 다른 형태의 공격들에 비해 대체로 공격자의 비용이 적게 든다.

③ 시스템관리자는 가능한 모든 공격을 고려해야 되기 때문에 방어가 매우 어렵다.

④ 하나의 타깃에 대해서 같은 방법으로 지속적으로 뚫을 때까지 공격하는 것이다.

정답 3번

출제 포인트

지능형 지속 위협(APT)의 표적성·지속성·고도화 특성과 방어가 어려운 이유를 구별하는 문제이다.

핵심 개념

APT는 특정 조직이나 시스템을 목표로 삼아 충분한 자원과 다양한 공격 기법을 동원하고, 장기간 은밀하게 침투와 내부 활동을 이어 가는 위협이다. '지속적'이라는 말은 하나의 기법만 반복한다는 뜻이 아니라 목표 달성을 위해 공격 경로와 수법을 바꾸면서 계속 시도한다는 뜻이다. 공격자는 여러 경로 중 하나만 성공해도 되지만 방어자는 가능한 침투 경로를 폭넓게 막아야 하므로 방어가 어렵다.

선지별 해설

① X

틀린 표현은 '설계부터 침투까지 매우 빠른 시간 내에 이루어진다'이다. APT는 일반적으로 표적을 분석하고 공격을 준비한 뒤 여러 단계에 걸쳐 은밀하게 침투하므로, 반드시 매우 짧은 시간 안에 이루어지는 공격이 아니다.

② X

틀린 표현은 '공격자의 비용이 적게 든다'이다. APT는 특정 표적을 장기간 공격하기 위해 전문 인력, 시간, 도구 등 상당한 자원을 투입하는 고도화된 공격이므로 대체로 비용이 적게 드는 공격이라고 보기 어렵다.

③ O

공격자는 다양한 공격 경로 가운데 하나의 취약점만 찾아도 침투할 수 있지만, 시스템 관리자는 가능한 여러 침투 경로를 모두 고려하여 방어해야 한다. 이러한 비대칭성 때문에 APT 방어는 매우 어렵다.

④ X

틀린 표현은 '같은 방법으로 지속적으로'이다. APT의 지속성은 동일한 방법만 되풀이한다는 의미가 아니다. 실제로는 하나의 표적을 장기간 겨냥하면서 탐지를 피하고 상황에 맞게 여러 공격 기법과 경로를 조합하거나 변경한다.

NoteBase

오답 포인트

④는 '지속 위협'이라는 명칭을 이용해 같은 공격 방법을 계속 반복하는 것으로 오인하게 한다. APT에서 지속되는 것은 특정 목표를 달성하려는 공격 활동이며, 공격 수법은 방어 상황에 따라 달라질 수 있다.

다시 나오면 이렇게 판단

APT 관련 선지는 특정 표적, 장기·은밀한 활동, 다양한 고도화 기법, 많은 자원 투입이라는 기준으로 판단한다. '단시간', '저비용', '동일 수법만 반복'이라는 표현은 APT의 일반적 특성과 맞지 않는다.

암기 포인트

APT는 특정 표적을 향해 오래, 은밀하게, 여러 수법으로 이어 가는 고도화된 공격이다.

NoteBase

문 20. 다음 중 「개인정보보호법」 제25조에 따라 공개된 장소에서의 영상정보처리기기 설치가 예외적으로 허용되는 경우가 아닌 것은?

① 법령에서 구체적으로 허용하고 있는 경우

② 범죄의 예방 및 수사를 위하여 필요한 경우

③ 교통정보의 수집·분석 및 제공을 위하여 필요한 경우

④ 통계작성·과학적 연구·공익적 기록보전 등을 위하여 필요한 경우

정답 4번

쟁점

이 문제는 공개된 장소에 고정형 영상정보처리기기를 설치·운영할 수 있는 「개인정보 보호법」상 예외 사유에 관한 문제이다. 핵심은 영상정보처리기기의 설치 목적과 가명정보의 처리 목적을 구별하는 것이다.

용어 풀이

고정형 영상정보처리기기는 일정한 공간에 지속적으로 설치되어 사람이나 사물의 영상을 촬영하는 장치를 말한다. 공개된 장소에서는 사생활 침해 위험이 크므로 법에서 정한 예외 사유가 있어야 설치·운영할 수 있다.

핵심 구분

「개인정보 보호법」 제25조 제1항은 공개된 장소에서의 고정형 영상정보처리기기 설치·운영을 원칙적으로 금지하고, 법령의 구체적 허용, 범죄 예방·수사, 시설 안전·관리 및 화재 예방, 교통단속, 교통정보 수집·분석·제공, 촬영 영상정보를 저장하지 않는 대통령령상 경우를 예외로 둔다. 반면 통계작성·과학적 연구·공익적 기록보존 등은 같은 법 제28조의2에서 정보주체의 동의 없이 가명정보를 처리할 수 있는 목적이다. 이 목적 자체는 제25조 제1항의 설치·운영 예외가 아니다.

NoteBase

선지별 해설

① O — 법령에서 공개된 장소의 고정형 영상정보처리기기 설치·운영을 구체적으로 허용한 경우는 제25조 제1항의 예외에 해당한다.
② O — 범죄의 예방 및 수사를 위하여 필요한 경우는 제25조 제1항에 열거된 예외 사유이다.
③ O — 교통정보의 수집·분석 및 제공을 위하여 정당한 권한을 가진 자가 설치·운영하는 경우는 제25조 제1항의 예외 사유이다.
④ X — 통계작성·과학적 연구·공익적 기록보존 등이 필요하다는 사정만으로 공개된 장소에 고정형 영상정보처리기기를 설치·운영할 수 있는 것은 아니다.
틀린 표현: 통계작성·과학적 연구·공익적 기록보전 등을 위하여 필요한 경우에는 공개된 장소의 영상정보처리기기 설치가 허용된다.
올바른 표현: 통계작성·과학적 연구·공익적 기록보존 등을 위해서는 정보주체의 동의 없이 가명정보를 처리할 수 있지만, 그 목적 자체는 공개된 장소의 고정형 영상정보처리기기 설치·운영 예외가 아니다.

오답 포인트

④의 목적은 개인정보 활용에 관한 제28조의2의 가명정보 처리 사유이므로 그럴듯해 보인다. 그러나 이 문항은 제25조 제1항의 영상정보처리기기 설치·운영 예외를 묻고 있으므로 서로 다른 제도의 목적을 섞으면 안 된다.

다시 나오면 이렇게 판단

공개된 장소의 고정형 영상정보처리기기 문제에서는 먼저 제25조 제1항의 열거 사유인지 확인한다.
통계작성·과학적 연구·공익적 기록보존이라는 묶음이 나오면 가명정보 처리 규정과의 혼동을 의심한다.

암기 포인트

영상기기 예외는 범죄·안전·교통 중심이고, 통계·연구·기록보존은 가명정보 처리 목적이다.

NoteBase