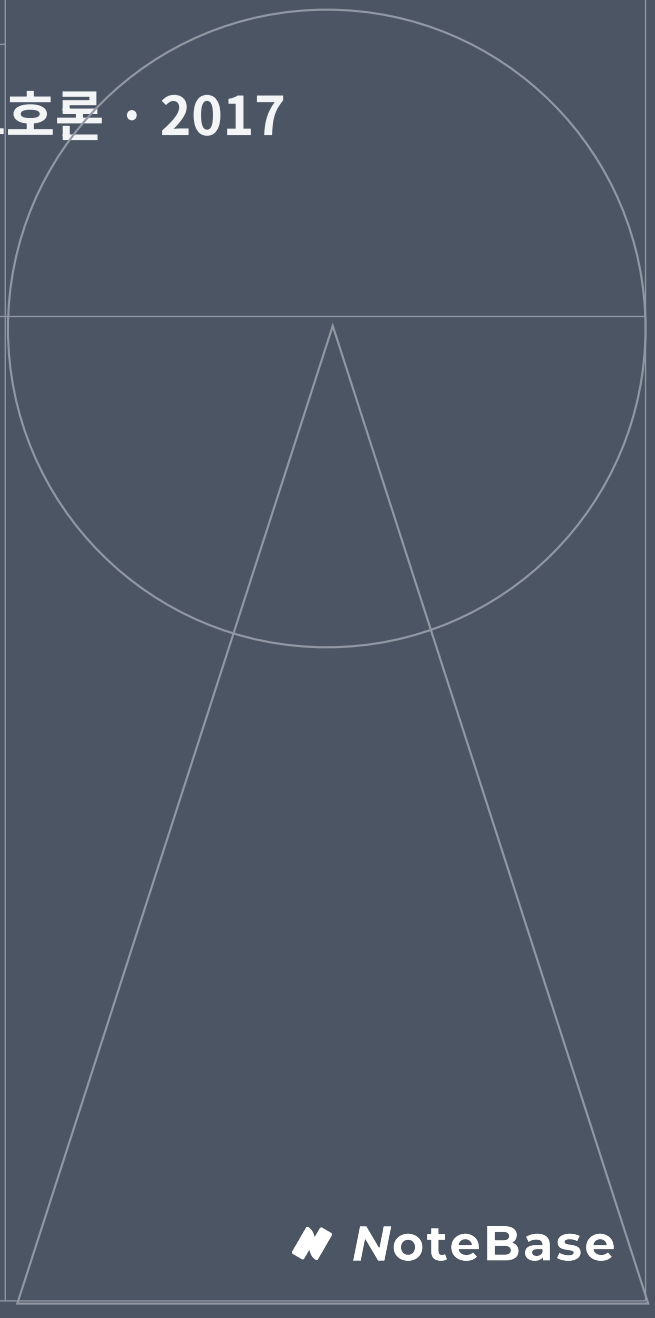
기출OX 해설집

공무원/국가직/7급 · 정보보호론 · 2017



NoteBase

기출OX 해설집

공무원/국가직/7급 · 정보보호론 · 2017

공무원/국가직/7급 · 정보보호론 · 2017

문 1. 다음 대칭키 암호화에서 K값은?

◯ 8비트 정보 P와 K의 배타적 논리합(XOR) 연산의 결과를 Q라 함
◯ P = 11010011
◯ Q = 10000110

① 11010011
② 10000110
③ 01010101
④ 01010100

정답 3번

출제 포인트

대칭키 암호화의 기본 연산인 배타적 논리합(XOR)의 성질을 이용해 미지의 키값을 역산하는 문제이다. XOR은 같은 값을 두 번 적용하면 원래 값으로 돌아오는 자기 역원(self-inverse) 성질을 가지므로, 암호화 결과와 평문을 알면 키를 거꾸로 구할 수 있다는 점이 핵심이다.

조건 정리

평문 P = 11010011, 이 P와 키 K를 XOR 연산한 결과가 Q = 10000110이다. 즉 $P \oplus K = Q$ 관계가 성립하며, 구해야 할 값은 K이다.

사용할 공식

XOR은 결합·자기 역원 성질을 가지므로 $P \oplus K = Q$ 이면 양변에 P를 XOR하여 $K = P \oplus Q$ 를 얻는다. ($P \oplus P = 0$이고 0과의 XOR은 항등이므로 $P \oplus (P \oplus K) = K$가 성립한다.)

NoteBase

계산 과정

K = P ⊕ Q 를 비트별로 계산한다.
P = 1 1 0 1 0 0 1 1
Q = 1 0 0 0 0 1 1 0
비트별 XOR(같으면 0, 다르면 1):
1번째 자리: 1과 1 → 0
2번째 자리: 1과 0 → 1
3번째 자리: 0과 0 → 0
4번째 자리: 1과 0 → 1
5번째 자리: 0과 0 → 0
6번째 자리: 0과 1 → 1
7번째 자리: 1과 1 → 0
8번째 자리: 1과 0 → 1
따라서 K = 01010101이다.

선지 판단

① 11010011(X) → 이는 평문 P 값 그대로이며 계산 결과인 01010101과 다르다.
② 10000110(X) → 이는 Q 값 그대로이며 계산 결과와 다르다.
③ 01010101(O) → P와 Q를 비트별 XOR한 결과와 정확히 일치한다.
④ 01010100(X) → 마지막 자리(8번째)가 0으로 계산되어 있으나, 실제로는 P의 8번째 비트 1과 Q의 8번째 비트 0을 XOR하면 1이 되어야 하므로 마지막 자리가 틀린 값이다.

오답 포인트

이 문제에서 흔히 하는 실수는 P나 Q 자체를 답으로 고르거나(①, ②), 비트별 XOR을 계산할 때 마지막 한두 자리에서 서로 같은 자리끼리 짝을 잘못 맞추어 한 비트를 틀리게 계산하는 것이다(④). XOR은 같은 자리끼리만 비교하며, 같으면 0, 다르면 1이라는 규칙을 8자리 전부에 일관되게 적용해야 한다.

다시 나오면 이렇게 판단

P ⊕ K = Q 형태의 식이 주어지면 미지수를 구하는 방법은 항상 같다. 알고 있는 두 값(P와 Q)을 XOR하면 나머지 미지의 값(K)이 나온다는 것을 먼저 떠올리고, 8비트를 한 자리씩 짝지어 같으면 0, 다르면 1로 채운다. 계산 후에는 선지에서 자신이 구한 값과 정확히 일치하는지 자리 수까지 맞춰 확인한다.

암기 포인트

XOR의 자기 역원 성질: A ⊕ B = C 이면 A = B ⊕ C, B = A ⊕ C 가 모두 성립한다. 즉 세 값 중 두 값을 알면 나머지 한 값은 그 두 값을 XOR하여 바로 구할 수 있다.

NoteBase

문 2. DRM(Digital Right Management)에 대한 설명으로 옳지 않은 것은?

① 문서의 열람, 편집, 프린트 등에 대한 접근 권한을 설정한다.

② 문서 사용에 인가를 부여받은 사용자에게 접근을 허용한다.

③ DRM 모듈로 운영되는 시스템의 하드디스크는 도난당하더라도 정보 유출의 위험이 적다.

④ 사용하기 불편하므로 인증서를 전혀 사용하지 않는다.

정답 4번

출제 포인트

DRM(디지털 저작권 관리)의 기본 개념과 동작 원리, 즉 콘텐츠·문서를 암호화하고 접근 권한을 통제하는 방식을 정확히 이해하고 있는지를 묻는 문제이다. 특히 DRM 운용 과정에서 인증서(공개키 기반의 암호화·복호화 키 관리 수단)가 실제로 사용되는지 여부가 핵심 쟁점이다.

핵심 개념

DRM은 문서나 콘텐츠 원본을 암호화하여 저장하고, 열람·편집·인쇄 등 각 기능 단위로 접근 권한을 부여한 사용자에게만 복호화 키를 제공하는 기술이다. 이 과정에서 사용자·시스템을 식별하고 암호화 키를 안전하게 교환하기 위해 공개키 기반구조(PKI)의 인증서가 활용된다. 콘텐츠 자체가 암호화되어 있으므로 저장매체(하드디스크 등)를 물리적으로 탈취당해도 키 없이는 내용을 열람할 수 없어 정보 유출 위험이 낮아진다.

선지별 해설

① O — DRM은 문서 단위로 열람, 편집, 프린트, 복사 등 세부 기능에 대한 접근 권한을 개별적으로 설정하여 통제하는 것이 핵심 기능이다.
② O — DRM은 사전에 인가(권한 부여)를 받은 사용자만 식별하여 해당 문서에 접근하도록 허용하고, 인가되지 않은 사용자의 접근은 차단한다.
③ O — DRM 모듈로 운영되는 시스템은 문서(콘텐츠)를 암호화된 상태로 저장하므로, 하드디스크 자체를 도난당하더라도 복호화 키 없이는 내용을 확인할 수 없어 정보 유출 위험이 상대적으로 적다.
④ X — 틀린 표현 → 올바른 표현: "사용하기 불편하므로 인증서를 전혀 사용하지 않는다" → DRM은 사용자 인증과 암호화 키 관리를 위해 공개키 기반구조(PKI)의 인증서를 일반적으로 활용한다. 인증서를 전혀 사용하지 않는다는 서술은 DRM의 실제 동작 방식과 맞지 않는다.

오답 포인트

③번과 ④번을 혼동하기 쉬운데, ③은 암호화로 인한 정보 유출 방지 효과를 설명한 옳은 내용이고, ④는 인증서 사용 여부에 대한 사실관계를 틀리게 서술한 문장이다. DRM이 '불편해서 인증서를 안 쓴다'는 서술 자체가 기술적으로 성립하지 않는다는 점을 놓치면 오답을 고르기 쉽다.

NoteBase

다시 나오면 이렇게 판단

DRM 관련 지문에서는 암호화 대상(콘텐츠 자체를 암호화하는지), 권한 통제 단위(열람·편집·인쇄 등 기능별 통제인지), 그리고 인증서·키 관리 수단이 실제로 쓰이는지 세 가지를 축으로 옳고 그름을 판단한다. 'OO을 전혀 사용하지 않는다'처럼 단정적으로 부정하는 선지는 DRM의 핵심 구성요소(암호화, 접근 통제, 인증서 기반 키 관리)와 배치되는지 먼저 의심한다.

암기 포인트

DRM = 콘텐츠 암호화 + 기능별 접근 권한 통제 + 인증서 기반 사용자 인증·키 관리. 매체를 탈취당해도 암호화 덕분에 정보 유출 위험은 낮다.

NoteBase

문 3. 블록암호 알고리즘에 대한 설명으로 옳지 않은 것은?

① IDEA - 상이한 대수 그룹으로부터의 세 가지 연산을 혼합하는 방식

② Blowfish - 키의 크기가 가변적이므로 안전성과 성능의 요구에 따라 유연하게 사용

③ SEED - 1999년 KISA와 국내 암호전문가들이 개발한 128비트 블록암호

④ ARIA - 국가보안기술연구소 주관으로 64비트 블록 암호로 128비트 암호화키만 지원

정답 4번

출제 포인트

국내외 주요 블록암호 알고리즘(IDEA, Blowfish, SEED, ARIA)의 개발 배경과 구조적 특징(블록 크기, 키 길이, 연산 방식)을 정확히 구분하는지를 묻는다. 특히 ARIA의 블록 크기와 지원 키 길이를 다른 암호와 혼동하지 않는지가 핵심이다.

핵심 개념

블록암호는 고정된 길이의 블록 단위로 평문을 암호화하며, 알고리즘마다 블록 크기와 키 길이, 라운드 함수의 구성 방식이 다르다. IDEA는 XOR·모듈러 덧셈·모듈러 곱셈이라는 서로 다른 대수 구조에서 나온 세 연산을 혼합해 안전성을 높인 방식이다. Blowfish는 64비트 블록암호로 키 길이를 32비트부터 448비트까지 가변적으로 설정할 수 있어 안전성과 속도의 균형을 상황에 맞게 조절할 수 있다. SEED는 1999년 한국정보보호진흥원(KISA)이 국내 암호 전문가들과 함께 개발한 128비트 블록암호이다. ARIA는 국가정보원과 산학연구협력으로 개발되어 국가보안기술연구소가 주관한 128비트 블록암호로, 128·192·256비트의 세 가지 키 길이를 모두 지원한다.

선지별 해설

① IDEA는 실제로 XOR, mod 2^16 덧셈, mod(2^16+1) 곱셈이라는 서로 다른 대수 그룹의 연산 세 가지를 혼합하는 구조가 맞으므로 옳은 설명이다.
② Blowfish는 실제로 32비트에서 448비트까지 키 크기를 가변적으로 설정할 수 있어 안전성과 성능 요구에 따라 유연하게 사용할 수 있으므로 옳은 설명이다.
③ SEED는 실제로 1999년 KISA(당시 한국정보보호진흥원)와 국내 암호 전문가들이 개발한 128비트 블록암호가 맞으므로 옳은 설명이다.
④ ARIA는 블록 크기가 64비트가 아니라 128비트이고, 지원하는 암호화키 길이도 128비트만이 아니라 128·192·256비트를 모두 지원한다. 블록 크기와 지원 키 길이 두 가지 모두 틀린 표현이므로 → 올바른 표현은 "국가보안기술연구소 주관으로 128비트 블록 암호로 128·192·256비트 암호화키를 지원"이다. 따라서 옳지 않은 설명이다.

NoteBase

오답 포인트

ARIA를 SEED와 같은 128비트 블록암호로 알고 있으면서도 정작 지문에서 블록 크기가 64비트라고 제시되면 헷갈릴 수 있다. 또한 AES가 128·192·256비트 키를 지원한다는 사실과 뒤섞여 ARIA가 128비트 키만 지원한다고 착각하기 쉽다. ARIA는 블록 크기와 키 길이 모두 AES와 동일한 구조를 따른다는 점을 명확히 구분해야 한다.

다시 나오면 이렇게 판단

블록암호 문제에서는 각 알고리즘의 블록 크기와 키 길이를 짝으로 묶어 먼저 확인한다. SEED와 ARIA를 같은 128비트 블록암호로 분류하되, ARIA는 키 길이가 128·192·256비트로 다양하다는 점에서 SEED(128비트 고정)와 차이가 있다는 것을 기준으로 선지를 판단한다.

암기 포인트

SEED=128비트 블록·128비트 키(KISA, 1999년), ARIA=128비트 블록·128/192/256비트 키(국가보안기술연구소 주관), Blowfish=64비트 블록·가변 키(32~448비트), IDEA=서로 다른 대수 연산 세 가지 혼합.

NoteBase

문 4. 암호화에 대한 설명으로 옳지 않은 것은?

① AES는 블록 크기가 192비트이며, 키는 192비트와 256비트 두 가지를 사용한다.

② Rabin은 RSA와 같은 원리로 암호화하고, 2차 합동에 근거하고 있다.

③ DES는 대칭키 방식으로서 16개 라운드로 구성되어 있다.

④ One-Time Pad는 암호화를 수행할 때마다 랜덤하게 선택된 키 스트림을 사용한다.

정답 1번

출제 포인트

AES, Rabin, DES, One-Time Pad 등 주요 암호 알고리즘의 블록 크기·키 길이·구조·동작 방식에 대한 사실관계를 정확히 아는지 묻는 문제이다. 특히 AES의 블록 크기와 키 길이를 혼동하지 않는 것이 핵심이다.

핵심 개념

AES(Advanced Encryption Standard)는 블록 크기가 항상 128비트로 고정되어 있고, 키 길이만 128비트·192비트·256비트 세 가지 중 하나를 선택해서 사용하는 대칭키 블록 암호이다. 즉 블록 크기와 키 길이는 서로 다른 값이며, 키 길이가 커진다고 블록 크기가 함께 커지지 않는다.
Rabin 암호는 RSA와 마찬가지로 소인수분해의 어려움에 기반한 공개키 암호로, 평문을 제곱하여 암호화하고 복호화 시 모듈러 제곱근을 구하는 방식이어서 2차 합동(이차잉여) 문제에 근거한다.
DES(Data Encryption Standard)는 56비트 키를 사용하는 대칭키 블록 암호로, Feistel 구조를 기반으로 16라운드의 반복 연산을 수행한다.
One-Time Pad(일회용 패드)는 매 암호화마다 평문과 같은 길이의 완전히 랜덤한 키 스트림을 새로 선택하여 한 번만 사용하는 암호 방식으로, 이론적으로 완전 비밀성(perfect secrecy)을 가진다.

선지별 해설

① X: AES는 키 길이는 128비트·192비트·256비트 세 가지를 사용하지만, 블록 크기는 키 길이와 무관하게 항상 128비트로 고정되어 있다. "블록 크기가 192비트"라는 설명은 틀린 표현이며, 올바른 표현은 "블록 크기는 128비트로 고정, 키는 128·192·256비트 중 선택"이다.
② O: Rabin 암호는 RSA와 같이 소인수분해 문제에 기반한 공개키 암호이며, 암호화 과정이 모듈러 제곱(2차 합동)에 근거하고 있다는 설명은 맞는 내용이다.
③ O: DES는 대칭키 방식이며 16라운드의 Feistel 구조로 구성되어 있다는 설명은 맞는 내용이다.
④ O: One-Time Pad는 사용할 때마다 랜덤하게 선택된 키 스트림을 사용한다는 설명은 맞는 내용이다.

NoteBase

오답 포인트

AES의 블록 크기(128비트 고정)와 키 길이(128·192·256비트 가변)를 같은 값으로 착각하기 쉽다. 키 길이가 192비트나 256비트라고 해서 블록 크기도 함께 커진다고 생각하면 안 되며, AES는 키 길이와 무관하게 블록 크기가 항상 128비트라는 점을 정확히 구분해서 기억해야 한다.

다시 나오면 이렇게 판단

선지에 특정 알고리즘의 블록 크기와 키 길이가 함께 제시되면, 두 수치가 실제로 그 알고리즘의 표준 규격과 일치하는지 각각 따로 확인한다. AES는 "블록 128비트 고정 + 키 128/192/256비트 가변"이라는 구조를 하나의 짝으로 외워 두면 이런 변형 문제에 바로 대응할 수 있다.

암기 포인트

AES = 블록 128비트 고정, 키 128·192·256비트 선택. DES = 키 56비트, 16라운드 Feistel 구조. Rabin = RSA와 같은 소인수분해 기반, 2차 합동(모듈러 제곱근) 이용. One-Time Pad = 매번 새로운 완전 난수 키 스트림 사용, 완전 비밀성 보장.

NoteBase

문 5. 가상화 시스템을 보호하는 방법으로 옳지 않은 것은?

① 게스트 운영체제 사용자들에게 하이퍼바이저에 접근하는 관리권한을 부여해야 한다.

② 원격 감독 기능을 사용할 때에는 적절한 인증과 암호화 메커니즘을 사용해야 한다.

③ 게스트 운영체제와 응용프로그램을 보호하는 것 외에도 가상화 환경과 하이퍼바이저도 보호해야 한다.

④ 하이퍼바이저가 게스트의 활동을 투명하게 감시해야 한다.

정답 1번

출제 포인트

가상화 시스템(하이퍼바이저·게스트 운영체제·가상화 환경) 보호를 위한 보안 원칙을 제대로 아는지 묻는 문항이다. 핵심은 하이퍼바이저가 게스트보다 더 높은 권한을 가지는 계층 구조이므로, 반대로 게스트 쪽 사용자가 하이퍼바이저를 통제하게 해서는 안 된다는 점이다.

핵심 개념

하이퍼바이저는 여러 게스트 운영체제를 관리·격리하는 최상위 관리 계층으로, 게스트 운영체제보다 높은 권한을 가진다. 보안 원칙상 권한은 항상 상위 계층(하이퍼바이저)에서 하위 계층(게스트)으로만 흘러야 하며, 게스트 쪽 사용자가 하이퍼바이저에 대한 관리권한을 갖게 되면 하나의 게스트가 손상되었을 때 전체 가상화 인프라와 다른 게스트들까지 장악될 수 있다. 따라서 최소권한 원칙과 계층 간 격리 원칙에 따라 게스트 운영체제 사용자에게는 하이퍼바이저 관리권한을 부여하지 않는 것이 원칙이다. 반면 원격 관리·감독 기능에 대한 인증·암호화, 게스트뿐 아니라 하이퍼바이저·가상화 환경 자체에 대한 보호, 하이퍼바이저에 의한 게스트 활동의 투명한 감시는 모두 가상화 보안의 정상적인 권장 사항이다.

선지별 해설

① 옳지 않다. 게스트 운영체제 사용자들에게 하이퍼바이저에 접근하는 관리권한을 부여해야 한다는 서술은 틀린 표현이다. → 올바른 표현: 게스트 운영체제 사용자에게는 하이퍼바이저에 대한 관리권한을 부여해서는 안 되며, 하이퍼바이저 관리 기능은 별도의 신뢰된 관리자만 접근할 수 있도록 엄격히 통제해야 한다.
② 옳다. 하이퍼바이저나 가상 머신을 원격으로 감독·관리하는 기능을 사용할 때에는 적절한 인증과 암호화 메커니즘을 통해 통신 채널과 접근을 보호해야 한다.
③ 옳다. 가상화 환경의 보호 대상은 게스트 운영체제와 그 위의 응용프로그램에 그치지 않고, 이를 구동하는 가상화 환경 자체와 하이퍼바이저까지 포함해야 한다.
④ 옳다. 하이퍼바이저는 게스트의 활동을 투명하게(게스트가 인지하지 못하는 방식으로) 감시함으로써 게스트 내부에서 발생할 수 있는 악성 행위나 이상 행위를 탐지할 수 있다.

NoteBase

오답 포인트

①을 옳다고 잘못 판단하기 쉬운 이유는 '관리권한 부여'라는 표현만 보고 단순히 권한 관리에 관한 좋은 관행처럼 느껴지기 때문이다. 그러나 주체가 누구인지(게스트 운영체제 사용자)와 대상이 무엇인지(하이퍼바이저)를 함께 봐야 한다. 하이퍼바이저는 게스트보다 상위 계층이므로, 하위 계층인 게스트 사용자가 상위 계층을 통제할 권한을 갖는 것은 계층 구조와 최소권한 원칙에 정면으로 위배된다.

다시 나오면 이렇게 판단

가상화 보안 문제에서 '게스트가 하이퍼바이저를 관리·통제·접근한다'는 방향의 서술이 나오면 일단 옳지 않은 선지로 의심한다. 반대로 '하이퍼바이저가 게스트를 감시·통제·보호한다'는 방향이나, 하이퍼바이저·가상화 환경 자체도 보호 대상에 포함된다는 서술, 원격 관리 기능에 인증·암호화를 적용한다는 서술은 옳은 선지로 판단한다.

암기 포인트

권한의 방향은 하이퍼바이저에서 게스트로만 향한다. 게스트 사용자에게 하이퍼바이저 관리권한을 주는 것은 항상 오답이라고 기억해 둔다.

NoteBase

문 6. 정보시스템을 보호하기 위한 미국의 정보보호관리체계로 적합한 것은?

① PIPL

② FISMA

③ JIPDEC

④ NICST

정답 2번

출제 포인트

각국·각 기관의 정보보호관리체계(ISMS) 명칭과 소속 국가·기관을 짝짓는 문제이다. 이름만 보고 어느 나라·어느 분야의 제도인지 구분할 수 있는지를 묻는다.

핵심 정리

FISMA(Federal Information Security Management Act)는 미국 연방정부 기관의 정보시스템 보안을 관리하기 위해 제정된 미국의 정보보호관리체계이다. 미국 연방 행정기관은 이 체계에 따라 정보시스템의 위험을 평가하고 보안대책을 수립·이행한다.
PIPL(Personal Information Protection Law)은 중국의 개인정보보호법으로, 정보시스템 보안관리체계가 아니라 개인정보 보호에 관한 법률이다.
JIPDEC(Japan Institute for Promotion of Digital Economy and Community)는 일본의 기관으로, 프라이버시마크 제도 등 개인정보보호 인증을 관장하는 일본 소속 조직이다.
NICST는 국가정보화전략위원회 등 한국의 정보화 관련 조직을 가리키는 명칭으로, 미국의 제도가 아니다.

선지별 해설

① PIPL: X. 중국의 개인정보보호 관련 법률이며, 미국의 정보보호관리체계가 아니다.
② FISMA: O. 미국 연방정보보안관리법에 근거한 미국의 정보보호관리체계로, 문제에서 요구하는 조건에 정확히 부합한다.
③ JIPDEC: X. 일본의 기관으로 프라이버시마크 인증 등을 담당하며 미국과 무관하다.
④ NICST: X. 한국의 정보화 관련 위원회 명칭이며 미국의 제도가 아니다.

오답 포인트

선지들이 모두 영문 약자로만 제시되어 있어 국가나 분야를 착각하기 쉽다. 특히 PIPL과 JIPDEC은 이름이 생소해 미국 제도로 오인할 수 있으나, PIPL은 중국, JIPDEC은 일본 소속임을 구분해야 한다. NICST 역시 한국의 조직이므로 국가 매칭에 유의한다.

NoteBase

다시 나오면 이렇게 판단

정보보호관리체계 관련 문제는 약자를 국가별로 묶어서 기억해 두면 빠르게 풀 수 있다. 미국=FISMA, 중국=PIPL, 일본=JIPDEC 및 프라이버시마크, 한국=국가정보화 관련 조직(NICST 등)으로 구분해 매칭한다.

암기 포인트

미국 정보보호관리체계는 FISMA(연방정보보안관리법)로 기억해 둔다. PIPL은 중국 개인정보보호법, JIPDEC은 일본 정보보호 인증기관, NICST는 한국 관련 조직이라는 국가별 대응관계를 함께 정리해 둔다.

NoteBase

문 7. 솔라리스 10에서 FTP 파일전송 시 발생되는 /var/log/xferlog 기록 내용에 대한 설명으로 옳지 않은 것은?

Thu Feb 2 16:41:30 2017 1 192.168.10.1 ㉠2870 ㉡/tmp/12-ftp.bmp ㉢b _ o r wish ftp 0 ㉣* c 2870 0

① ㉠ - 응답 포트 번호

② ㉡ - 전송된 파일의 이름

③ ㉢ - 바이너리 파일 전송

④ ㉣ - 인증 서버를 사용하지 않음

정답 1번

출제 포인트

솔라리스(유닉스 계열) FTP 서버가 남기는 /var/log/xferlog 한 줄의 각 필드가 무엇을 의미하는지 순서대로 정확히 알고 있는지를 묻는 문제이다. 로그 한 줄 안에서 위치가 다른 값들에 엉뚱한 명칭을 붙인 선지를 찾아내는 것이 핵심이다.

핵심 개념

표준 xferlog 레코드는 다음 순서로 기록된다. 현재 시각(요일 월 일 시:분:초 연도) - 전송 소요시간(초) - 원격 호스트 주소 - 전송된 파일의 크기(바이트) - 전송된 파일의 이름 - 전송 형태(a=아스키, b=바이너리) - 특수 처리 플래그(압축·묶음 등, 없으면 _) - 전송 방향(o=outgoing, i=incoming, d=delete) - 접속 형태(a=anonymous, g=guest, r=실사용자) - 사용자명 - 서비스명(ftp) - 인증 방식(0=없음, 1=RFC931) - 인증된 사용자 ID(인증을 거치지 않았으면 *) - 완료 상태(c=complete, i=incomplete). 제시된 로그에서 원격 호스트(192.168.10.1) 바로 뒤에 오는 2870이 ㄱ이므로 이는 전송 파일의 크기이고, 그 다음 줄의 /tmp/12-ftp.bmp가 ㄴ(파일명), b가 ㄷ(전송 형태), *가 ㄹ(인증된 사용자 ID)이다.

선지별 해설

① ㄱ - 응답 포트 번호: X. ㄱ(2870)은 원격 호스트 주소 다음 필드로, xferlog 필드 순서상 응답 포트 번호가 아니라 전송된 파일의 크기(바이트 수)를 나타낸다. 포트 번호는 이 로그 형식에 별도 필드로 기록되지 않는다. 이 문항의 정답이다.

② ㄴ - 전송된 파일의 이름: O. ㄴ(/tmp/12-ftp.bmp)은 필드 순서상 파일명 위치에 있으므로 옳은 설명이다.

③ ㄷ - 바이너리 파일 전송: O. ㄷ(b)은 전송 형태 필드이며 b는 바이너리 전송을 의미하므로 옳은 설명이다(아스키 전송이면 a로 표기된다).

④ ㄹ - 인증 서버를 사용하지 않음: O. 인증 방식 필드 값이 0(없음)이고 그 다음 인증된 사용자 ID 필드인 ㄹ이 *로 표시되어 있으므로, 별도 인증 서버를 거치지 않았음을 나타낸다.

NoteBase

오답 포인트

ㄱ의 위치가 원격 호스트 주소 바로 뒤에 있다 보니 통신 관련 값(포트 번호)으로 착각하기 쉽지만, xferlog에서 통신 포트 번호는 기록 대상이 아니며 그 자리는 파일 크기 필드이다. 필드 순서를 암기하지 않은 채 값의 겉모습(숫자라는 이유)만 보고 포트 번호라고 넘겨짚으면 오답을 고르게 된다.

다시 나오면 이렇게 판단

xferlog 문제는 항상 필드 순서표를 먼저 떠올리고, 로그 문자열에서 각 표시(ㄱㄴㄷㄹ 등)가 몇 번째 필드에 해당하는지 위치로 대조한다. 숫자가 있다고 포트 번호나 IP로, 문자 하나(a/b, o/i, r/g/a, c/i)가 있다고 임의로 해석하지 말고 정해진 필드 의미(전송형태/방향/접속형태/완료상태)에 맞춰 판단한다.

암기 포인트

xferlog 필드 순서: 시각 - 소요시간(초) - 원격호스트 - 파일크기 - 파일명 - 전송형태(a/b) - 특수플래그 - 방향(i/o/d) - 접속형태(a/g/r) - 사용자명 - 서비스명(ftp) - 인증방식(0/1) - 인증사용자ID(*) - 완료상태(c/i).

NoteBase

문 8. 생체인식에 대한 특징으로 옳지 않은 것은?

① 생체인식은 사람의 생체적 특징과 행동적 특징을 통한 보편성, 유일성, 영속성, 획득성을 요구한다.

② FRR은 인증 권한이 있는 사람이 인증을 시도했을 때 인증에 실패하는 비율을 말한다.

③ CER은 잘못된 거부율과 잘못된 허용 비율 곡선의 교차점을 말한다.

④ 엄격한 보안이 요구되는 경우는 FAR을 높이고, FRR을 낮춤으로써 보안성을 향상시킬 수 있다.

정답 4번

출제 포인트

생체인식(Biometrics) 인증 방식의 요구 특성과, FAR·FRR·CER 같은 오류율 지표의 정의 및 상호 관계를 정확히 알고 있는지를 묻는다. 특히 보안 수준을 높이기 위해 오류율을 어느 방향으로 조정해야 하는지를 반대로 뒤집어 서술한 선지를 골라내는 것이 핵심이다.

핵심 개념

생체인식이 요구하는 4대 특성은 보편성(누구나 가지고 있음), 유일성(개인마다 다름), 영속성(시간이 지나도 변하지 않음), 획득성(측정과 수집이 용이함)이다. FAR(False Acceptance Rate, 오인식률)은 권한이 없는 사람을 정당한 사용자로 잘못 인증(허용)하는 비율이고, FRR(False Rejection Rate, 오거부율)은 권한이 있는 정당한 사용자를 인증에 실패시켜 잘못 거부하는 비율이다. CER(Crossover Error Rate, 등가오류율)은 FAR 곡선과 FRR 곡선이 만나는 교차점의 값으로, 이 값이 작을수록 인증 시스템의 성능이 우수하다. 보안 수준을 높이려면 잘못된 사람을 들여보내는 FAR을 낮추어야 하며, 그 대가로 정당한 사용자가 거부당하는 FRR은 오히려 높아지는 관계에 있다.

선지별 해설

① O — 생체인식은 사람의 생체적 특징(지문, 홍채, 정맥 등)과 행동적 특징(음성, 서명, 걸음걸이 등)을 이용하며, 인증 수단으로 쓰이기 위해 보편성, 유일성, 영속성, 획득성을 요구한다는 설명은 옳다.
② O — FRR은 인증 권한이 있는 정당한 사용자가 인증을 시도했음에도 인증에 실패(거부)하는 비율을 말한다는 설명은 정의와 일치한다.
③ O — CER은 잘못된 거부율(FRR)과 잘못된 허용 비율(FAR) 두 곡선이 서로 교차하는 지점의 오류율을 의미하며, 인증 시스템의 정확도를 비교하는 지표로 쓰인다는 설명은 옳다.
④ X — 틀린 표현 → 올바른 표현: "FAR을 높이고, FRR을 낮춤" → "FAR을 낮추고, FRR을 높임". 엄격한 보안이 요구되는 환경에서는 권한 없는 사람을 잘못 허용하는 FAR을 낮추는 것이 우선이며, 그 결과 정당한 사용자가 거부당하는 FRR은 높아지게 된다. 선지는 FAR과 FRR의 조정 방향을 서로 반대로 서술하여 틀렸다.

NoteBase

오답 포인트

FAR과 FRR을 이름만 보고 헷갈려서 '보안을 높인다 = 두 오류율을 다 낮춘다'고 잘못 생각하기 쉽다. 그러나 FAR과 FRR은 트레이드오프 관계에 있어 한쪽을 낮추면 다른 쪽은 높아진다는 점을 놓치면 ④번을 옳은 설명으로 착각하게 된다.

다시 나오면 이렇게 판단

'보안을 강화한다'는 문구가 나오면 항상 FAR(잘못된 허용) 감소가 최우선 목표라는 점을 떠올리고, 그 대가로 FRR(잘못된 거부)이 증가한다는 트레이드오프 방향이 선지에서 맞게 서술되었는지부터 확인한다.

암기 포인트

생체인식 4대 요구특성: 보편성·유일성·영속성·획득성. FAR=잘못된 허용(보안 위협), FRR=잘못된 거부(사용자 불편), CER=FAR·FRR 곡선의 교차점(작을수록 우수). 보안↑ → FAR↓, FRR↑.

NoteBase

문 9. 정보보호관리체계(ISMS)의 정보보호 관리과정에 대한 설명으로 옳지 않은 것은?

① 정보보호정책은 조직이 수행하는 모든 정보보호활동의 근거를 포함할 수 있도록 수립하고, 조직에 미치는 영향을 고려하여 중요한 업무, 서비스, 조직, 자산 등을 포함할 수 있도록 범위를 설정한다.

② 최고경영자는 조직의 규모, 업무 중요도 분석을 통해 정보보호 관리체계의 지속적인 운영이 가능하도록 정보보호 최고책임자, 실무조직 등 정보보호조직을 구성하고 정보보호 관리체계 운영 활동을 수행하는 데 필요한 자원을 확보하여야 한다.

③ 위험관리 방법 및 계획에 따라 정보보호 일부 영역에 대한 위험 식별 및 평가를 2년에 1회 수행하고 그 결과에 따라 조직에서 수용 가능한 위험수준도 설정하여 관리하여야 한다.

④ 정보보호대책 이행 계획에 따라 보호대책을 구현하고 경영진은 이행 결과의 정확성 및 효과성 여부를 확인하여 구현된 정보보호대책을 실제 운영 또는 시행할 부서 및 담당자를 파악하여 관련 내용을 공유하고 교육하여야 한다.

정답 3번

쟁점

정보보호관리체계(ISMS)의 '정보보호 관리과정' 5단계(정보보호 정책 수립 및 범위 설정 → 경영진 책임 및 조직 구성 → 위험관리 → 정보보호대책 구현 → 사후관리)에 대한 서술 중 위험관리 단계의 수행 주기와 대상 범위가 기준과 어긋난 선지를 찾는 문제이다. 핵심은 위험 식별·평가를 '얼마나 자주', '어느 범위까지' 해야 하는가이다.

용어 풀이

정보보호관리체계(ISMS)=조직의 정보자산을 보호하기 위한 정책·조직·위험관리·대책·사후관리를 체계적으로 운영하는 종합 관리체계이다.
위험관리=자산에 대한 위협과 취약점을 식별하고 위험을 평가한 뒤, 조직이 수용할 수 있는 위험수준(DoA, Degree of Assurance)을 정해 대응하는 활동이다.
수용 가능한 위험수준=조직이 감수하기로 결정한 잔여 위험의 허용 한계이다.

핵심 구분

위험 식별 및 평가의 대상 범위: '일부 영역'이 아니라 관리체계 범위 내 '전(全) 영역'이 원칙이다.
위험 식별 및 평가의 수행 주기: '2년에 1회'가 아니라 '연 1회 이상' 정기적으로 수행하는 것이 원칙이다.
관리과정 순서: 정책 수립·범위 설정(①) → 경영진 책임·조직 구성(②) → 위험관리(③) → 대책 구현(④) → 사후관리로 이어진다.

NoteBase

선지별 해설

① O — 정책 수립 및 범위 설정 단계의 정확한 서술이다. 정보보호정책이 모든 정보보호활동의 근거가 되도록 수립하고, 조직에 미치는 영향을 고려해 중요한 업무·서비스·조직·자산 등을 포함하도록 범위를 설정한다.
② O — 경영진 책임 및 조직 구성 단계의 정확한 서술이다. 최고경영자가 조직 규모·업무 중요도 분석을 통해 정보보호 최고책임자와 실무조직 등 정보보호조직을 구성하고, 운영에 필요한 자원을 확보하는 내용이다.
③ X — 위험관리 단계의 서술이지만 두 군데가 기준과 다르다. '정보보호 일부 영역'은 틀린 표현으로, 위험 식별 및 평가는 관리체계 범위 내 '전 영역'을 대상으로 해야 한다. 또한 '2년에 1회 수행'도 틀린 표현으로, 위험 식별 및 평가는 '연 1회 이상' 정기적으로 수행해야 한다. 수용 가능한 위험수준을 설정해 관리한다는 뒷부분은 맞다.
④ O — 정보보호대책 구현 단계의 정확한 서술이다. 이행 계획에 따라 보호대책을 구현하고, 이행 결과의 정확성·효과성을 확인하며, 실제 운영·시행 부서와 담당자를 파악해 관련 내용을 공유·교육하는 내용이다.

오답 포인트

③에서 '수용 가능한 위험수준도 설정하여 관리하여야 한다'는 뒷문장은 맞는 서술이라, 뒷부분만 보고 옳다고 넘기기 쉽다. 틀린 부분은 앞쪽의 '일부 영역'과 '2년에 1회'라는 두 표현이다. 반대로 ②의 '자원을 확보하여야 한다', ④의 '공유하고 교육하여야 한다'처럼 의무형 서술은 그 자체로 오류가 아니므로 문구가 길다고 오답으로 몰지 않도록 주의한다.

다시 나오면 이렇게 판단

ISMS 관리과정 문제에서 위험관리 단계가 나오면 두 숫자·범위 표현을 먼저 확인한다. '연 1회 이상'인지(→ '2년에 1회'·'분기 1회' 등은 함정), 대상이 '전 영역'인지(→ '일부 영역'·'주요 영역만'은 함정)를 체크하면 대부분 오답 선지가 걸린다. 선지 뒷부분의 결론이 맞더라도 앞부분의 주기·범위 수치가 틀리면 그 선지가 정답(옳지 않은 것)이다.

암기 포인트

ISMS 위험관리 두 숫자: 위험 식별·평가는 '전 영역, 연 1회 이상'으로 외워 둔다. 관리과정 5단계 순서는 '정책·범위 → 경영진·조직 → 위험관리 → 대책 구현 → 사후관리'로 정리해 둔다.

NoteBase

문 10. ISO/IEC JTC 1의 SC 27에서 담당하는 범위가 아닌 것은?

① Management of information and ICT security
② Cards and personal identification
③ Security evaluation criteria and methodology
④ Security requirements capture methodology

정답 2번

출제 포인트

국제표준화기구 ISO/IEC JTC 1 산하 정보보호 담당 분과위원회인 SC 27의 표준화 범위(scope)를 알고 있는지, 그리고 유사해 보이는 다른 분과위원회의 담당 영역과 혼동하지 않는지를 묻는다. ISO/IEC JTC 1/SC 27은 명칭 그대로 "IT Security techniques"를 다루는 분과로, 정보보호 관리·암호 기술·보안 평가·요구사항 도출 방법론 등을 총괄한다.

핵심 개념

ISO/IEC JTC 1/SC 27의 표준화 범위는 크게 다음과 같이 정리된다. 첫째, 보안 요구사항 도출 방법론(security requirements capture methodology). 둘째, 정보 및 ICT 보안의 관리(management of information and ICT security), 즉 정보보호관리체계(ISMS) 관련 표준. 셋째, 암호 및 기타 보안 메커니즘(cryptographic and other security mechanisms). 넷째, 보안관리 지원 문서. 다섯째, 신원관리·바이오인식 등 프라이버시 관련 보안 측면. 여섯째, 적합성 평가·인정·심사 관련 요건. 일곱째, 보안 평가기준 및 방법론(security evaluation criteria and methodology, 예: 공통평가기준·ISO/IEC 15408 계열). 반면 "카드 및 개인식별(Cards and personal identification)"은 신용카드·IC카드 등 카드의 물리적 규격과 개인식별 방식을 다루는 영역으로, ISO/IEC JTC 1 산하의 별도 분과위원회인 SC 17(카드 및 개인식별)의 담당 범위이며 SC 27의 소관이 아니다.

선지별 해설

① Management of information and ICT security → SC 27의 대표 영역인 정보 및 ICT 보안 관리(ISMS 등)에 해당하므로 SC 27이 담당하는 범위이다. 오답(문제는 아닌 것을 찾는 것이므로 이 선지는 제외 대상이 아님).
② Cards and personal identification → 카드 및 개인식별은 SC 27이 아니라 별도 분과인 SC 17의 담당 범위이다. SC 27이 담당하는 범위가 아니므로 이 선지가 정답이다.
③ Security evaluation criteria and methodology → 보안 평가기준 및 방법론은 SC 27의 핵심 영역(공통평가기준 등 보안성 평가 표준)에 해당하므로 SC 27이 담당하는 범위이다.
④ Security requirements capture methodology → 보안 요구사항 도출 방법론 역시 SC 27의 표준화 범위에 명시적으로 포함되는 영역이다.

NoteBase

오답 포인트

카드 관련 표준이라고 해서 무조건 보안 관련 위원회인 SC 27 소관이라고 생각하기 쉬우나, 카드의 규격·개인식별 방식은 ISO/IEC JTC 1 내에서 SC 27과는 별개인 SC 17이 전담한다는 점을 놓치면 오답을 고르게 된다. 나머지 세 선지(관리, 평가기준, 요구사항 도출)는 모두 SC 27의 이름(IT Security techniques)에 부합하는 핵심 업무이므로 소거법으로도 ②가 남는다.

다시 나오면 이렇게 판단

선지에 등장하는 표준화 대상이 정보보호의 관리·암호·평가·요구사항처럼 보안 기술 자체를 다루면 SC 27, 카드·개인식별처럼 특정 매체·기기의 물리적 규격을 다루면 SC 17로 구분해서 판단한다.

암기 포인트

SC 27 = IT Security techniques(관리·암호·평가기준·요구사항 도출 등 보안 기술 전반), SC 17 = Cards and personal identification(카드 및 개인식별 전담)으로 짝지어 기억해 둔다.

NoteBase

문 11. 해킹 수단과 그 공격 방법에 대한 설명으로 옳지 않은 것은?

① Ransomware - 파일을 암호화한 후 복호화를 조건으로 금전을 요구함

② Rootkit - 스택에 할당된 버퍼보다 큰 코드를 삽입하여 오동작을 일으킴

③ SQL Injection - 데이터베이스에 질의어를 변조하여 공격함

④ Cross-site Scripting - 웹 페이지에 악성 스크립트를 삽입하여 정보를 획득함

정답 2번

출제 포인트

대표적인 해킹 수단과 공격 기법의 이름을 그 동작 방식 설명과 정확히 짝짓는 문제이다. 이름은 익숙해도 설명이 다른 기법의 것과 뒤바뀌어 제시되면 틀린 선지가 된다. 이 문제에서는 Rootkit이라는 이름에 실제로는 버퍼 오버플로우 공격의 동작 방식이 붙어 있어, 이름과 설명의 매칭이 어긋난 것을 찾아내야 한다.

핵심 개념

Ransomware(랜섬웨어)는 사용자의 파일이나 시스템을 암호화하여 사용할 수 없게 만든 뒤, 이를 복호화해 주는 대가로 금전을 요구하는 악성코드이다. Rootkit(루트킷)은 공격자가 시스템에 침입한 후 관리자 권한을 획득·유지하면서 자신의 존재(프로세스, 파일, 네트워크 연결 등)를 운영체제와 관리자로부터 숨기기 위한 도구 모음이다. 반면 스택에 할당된 버퍼의 크기보다 큰 데이터나 코드를 입력하여 반환 주소 등 인접 메모리 영역을 덮어써 프로그램의 오동작이나 임의 코드 실행을 유발하는 공격은 버퍼 오버플로우(Buffer Overflow) 공격이다. SQL Injection(SQL 삽입)은 웹 애플리케이션이 사용자 입력값을 제대로 검증하지 않을 때, 입력값에 SQL 질의문을 조작하는 구문을 끼워 넣어 데이터베이스에 질의어를 변조된 형태로 실행시켜 데이터를 탈취·조작하는 공격이다. Cross-site Scripting(XSS, 크로스 사이트 스크립팅)은 신뢰된 웹 페이지에 악성 스크립트를 삽입해 두었다가, 다른 사용자가 그 페이지를 열람할 때 사용자의 브라우저에서 악성 스크립트가 실행되도록 하여 쿠키나 세션 정보 등을 탈취하는 공격이다.

NoteBase

선지별 해설

① Ransomware - 파일을 암호화한 후 복호화를 조건으로 금전을 요구함: O. 랜섬웨어의 정의와 정확히 일치하는 설명이다.
② Rootkit - 스택에 할당된 버퍼보다 큰 코드를 삽입하여 오동작을 일으킴: X. 이 설명은 루트킷이 아니라 버퍼 오버플로우 공격의 동작 방식이다. 루트킷은 침입 후 자신의 존재와 활동 흔적을 숨기고 관리자 권한을 유지하기 위한 도구이지, 버퍼 크기를 초과하는 코드를 삽입하는 공격 기법 자체를 가리키지 않는다. 틀린 표현 → 올바른 표현: "Rootkit" → "Buffer Overflow"로 바꾸어야 옳은 설명이 된다.
③ SQL Injection - 데이터베이스에 질의어를 변조하여 공격함: O. SQL 인젝션의 정의와 정확히 일치하는 설명이다.
④ Cross-site Scripting - 웹 페이지에 악성 스크립트를 삽입하여 정보를 획득함: O. XSS의 정의와 정확히 일치하는 설명이다.

오답 포인트

①③④는 각 공격 기법의 이름과 설명이 정확히 일치하므로 옳지 않은 것을 고르는 이 문제에서는 정답이 될 수 없다. 이름만 보고 익숙한 개념이라 지나치기 쉬운데, 반드시 뒤에 붙은 설명 문장이 그 이름이 가리키는 동작과 실제로 맞는지 하나씩 대조해야 한다. 특히 루트킷처럼 이름 자체가 자주 등장하는 용어일수록 설명이 다른 공격 기법(버퍼 오버플로우)의 것으로 바뀌어 제시되는 함정에 유의해야 한다.

다시 나오면 이렇게 판단

해킹 수단·공격 기법 이름과 동작 방식이 짝지어 제시되는 문제는 이름을 먼저 떠올리지 말고, 설명 문장이 묘사하는 동작(무엇을 대상으로, 무엇을 변조·삽입·암호화하는지)을 먼저 분석한 뒤 그 동작에 맞는 정확한 명칭을 떠올려 선지의 이름과 비교한다. 스택 버퍼 초과 삽입이라는 키워드가 나오면 곧바로 버퍼 오버플로우를 떠올리고, 은닉·권한 유지라는 키워드가 나오면 루트킷을 떠올리는 식으로 키워드와 명칭을 1대1로 연결해 둔다.

암기 포인트

랜섬웨어=파일 암호화+금전 요구, 루트킷=침입 흔적·존재 은닉+권한 유지, 버퍼 오버플로우=스택 버퍼 크기 초과 코드 삽입으로 오동작·임의 코드 실행, SQL 인젝션=질의어 변조로 DB 공격, XSS=웹 페이지에 악성 스크립트 삽입으로 정보 탈취로 각각 한 줄로 정리해 암기해 둔다.

NoteBase

문 12. 암호모듈을 KS X ISO/IEC 19790에 따라 검증하고 암호모듈의 안전성을 보증하는 국내 제도는?

① KCMVP

② TCSEC

③ ITSEC

④ METI

정답 1번

출제 포인트

국내 암호모듈 검증 제도의 명칭과 근거 표준을 알고 있는지, 그리고 이를 국외 보안평가 기준들과 혼동하지 않는지를 묻는다. KS X ISO/IEC 19790은 암호모듈의 보안 요구사항을 규정한 표준이며, 이 표준에 따라 암호모듈을 검증하고 안전성을 보증하는 국내 제도의 이름을 찾는 문제이다.

핵심 개념

KCMVP(Korea Cryptographic Module Validation Program, 암호모듈 검증제도)는 국가정보원과 국가보안기술연구소가 운영하는 국내 제도로, 암호모듈이 KS X ISO/IEC 19790(국제표준 ISO/IEC 19790을 국내 표준으로 채택한 것)에서 정한 보안 요구사항을 만족하는지 검증하여 안전성을 보증한다. 공공기관 등에 도입되는 암호모듈은 이 검증을 통과해야 한다. 반면 TCSEC(오렌지북)과 ITSEC은 각각 미국과 유럽에서 만들어진 정보시스템·운영체제 전반의 보안 등급 평가 기준이며, METI는 일본 경제산업성(경제산업부에 해당하는 행정부처)의 명칭으로 암호모듈 검증 제도 자체가 아니다.

선지별 해설

① KCMVP: 옳다. 국내에서 KS X ISO/IEC 19790에 따라 암호모듈을 검증하고 안전성을 보증하는 제도이다.
② TCSEC: 틀린 표현이다. TCSEC은 미국 국방부가 만든 컴퓨터 시스템 자체의 보안 등급을 평가하는 기준(오렌지북)으로, 암호모듈 검증 제도가 아니며 국내 제도도 아니다 → 국내 암호모듈 검증 제도는 KCMVP이다.
③ ITSEC: 틀린 표현이다. ITSEC은 유럽 여러 나라가 공동으로 만든 정보기술 제품의 보안성 평가 기준으로, 역시 암호모듈 전용 검증 제도가 아니며 국내 제도도 아니다 → 국내 암호모듈 검증 제도는 KCMVP이다.
④ METI: 틀린 표현이다. METI는 일본의 경제산업성을 가리키는 명칭일 뿐 암호모듈 검증 제도 자체가 아니며, 국내 제도도 아니다 → 국내 암호모듈 검증 제도는 KCMVP이다.

오답 포인트

TCSEC·ITSEC은 암호모듈 하나만이 아니라 시스템·제품 전반의 보안 등급을 평가하는 국외의 일반 보안평가 기준이라는 점에서 암호모듈 전용 검증 제도인 KCMVP와 성격이 다르다. METI는 평가 기준의 명칭이 아니라 일본의 행정부처 명칭이라는 점에서 선택지 구성 자체가 다른 셋과 층위가 다르다는 점에 유의한다.

NoteBase

다시 나오면 이렇게 판단

발문에 KS X ISO/IEC 19790, 암호모듈 검증, 국내 제도라는 키워드가 함께 나오면 곧바로 KCMVP를 떠올린다. TCSEC·ITSEC·CC(공통평가기준) 같은 이름이 선지에 섞여 나오면 이들은 시스템·제품 전반의 보안평가 기준이지 암호모듈 전용 검증 제도가 아니라는 점으로 소거한다.

암기 포인트

KCMVP = 국내, 암호모듈 전용 검증 제도(근거 표준 KS X ISO/IEC 19790). TCSEC = 미국, 오렌지북, 시스템 보안등급. ITSEC = 유럽, 정보기술 제품 보안성 평가.

NoteBase

문 13. 사용자가 무선랜 보안을 위하여 취할 수 있는 방법이 아닌 것은?

① MAC 주소 필터링의 적용

② SSID(Service Set Identifier) 브로드캐스팅의 금지

③ 무선 장비 관련 패스워드의 주기적인 변경

④ WPA, WPA2, WEP 중에서 가장 안전한 보안 방법인 WEP를 이용한 무선랜의 통신 보호

정답 4번

출제 포인트

무선랜(Wi-Fi) 보안을 강화하기 위해 사용자가 실제로 취할 수 있는 조치와, 잘못된 보안 방식(취약한 암호화 프로토콜)을 구분할 수 있는지를 묻는다. 특히 WEP·WPA·WPA2의 상대적 안전성 순서를 정확히 알고 있는지가 핵심이다.

핵심 개념

무선랜 보안 강화 방법에는 MAC 주소 필터링, SSID 브로드캐스팅 금지, 패스워드 주기적 변경, 안전한 암호화 프로토콜(WPA2) 사용 등이 있다. 무선랜 암호화 프로토콜의 안전성 순서는 WEP < WPA < WPA2이다. WEP(Wired Equivalent Privacy)는 초기 암호화 방식으로 고정된 키와 취약한 초기화 벡터(IV) 구조 때문에 짧은 시간 안에 키가 해독될 수 있어 이미 취약성이 널리 알려진 방식이고, WPA2는 AES 기반 암호화를 사용해 셋 중 가장 안전한 방식으로 평가된다.

선지별 해설

① MAC 주소 필터링의 적용: O. 허용된 기기의 MAC 주소만 접속을 허용하여 인가되지 않은 단말의 접근을 차단하는 보안 조치로, 사용자가 취할 수 있는 유효한 방법이다.
② SSID(Service Set Identifier) 브로드캐스팅의 금지: O. SSID를 숨겨 무선랜의 존재를 외부에 쉽게 노출하지 않도록 하는 조치로, 사용자가 취할 수 있는 유효한 방법이다.
③ 무선 장비 관련 패스워드의 주기적인 변경: O. 접속 암호나 관리자 패스워드를 주기적으로 변경하면 유출된 패스워드로 인한 침해 위험을 줄일 수 있으므로 유효한 방법이다.
④ WPA, WPA2, WEP 중에서 가장 안전한 보안 방법인 WEP를 이용한 무선랜의 통신 보호: X. 틀린 표현 → 올바른 표현: 'WEP가 가장 안전하다' → 'WPA2가 가장 안전하고 WEP가 가장 취약하다'. WEP는 셋 중 가장 오래되고 취약한 암호화 방식이므로 이를 '가장 안전한 방법'이라고 전제한 것 자체가 잘못이며, 사용자가 취해야 할 올바른 보안 방법이 아니다.

NoteBase

오답 포인트

①②③은 모두 실제로 권장되는 무선랜 보안 조치라서 정답에서 제외된다. ④를 정답으로 고르지 못하는 경우는 WEP·WPA·WPA2의 안전성 순서를 반대로 암기했기 때문이다. WEP는 이름에 'Privacy'가 들어가 안전할 것 같은 인상을 주지만, 실제로는 셋 중 가장 취약한 방식이라는 점을 혼동하지 않아야 한다.

다시 나오면 이렇게 판단

무선랜 보안 문제에서 WEP, WPA, WPA2가 함께 제시되면 먼저 안전성 순서(WEP < WPA < WPA2)부터 확정한 뒤 각 선지를 판단한다. 'OO를 이용해 통신을 보호한다'는 선지가 나오면 그 프로토콜이 실제로 안전한 방식인지를 반드시 확인한다.

암기 포인트

무선랜 암호화 안전성: WEP(취약) < WPA < WPA2(가장 안전). 이 외 보안 강화 조치로 MAC 주소 필터링, SSID 브로드캐스팅 금지, 패스워드 주기적 변경을 함께 기억해 둔다.

NoteBase

문 14. ISO 27001의 통제 영역별 주요 내용에 대한 설명으로 옳지 않은 것은?

① 자산 관리 영역은 자산을 파악하고, 이를 적절히 분류하고 보호하는 데 활용하는 것이다.

② 사업 연속성 관리 영역은 형법과 민법, 법령, 규정 또는 계약 의무 및 보안 요구 사항에 대한 위반을 피하기 위한 기준을 제시한 것이다.

③ 정보시스템 획득, 개발, 유지 보수 영역은 정보시스템 내에 보안이 수립되어 있음을 보장하기 위한 것이다.

④ 통신 및 운영 관리 영역은 정보처리 설비의 정확하고 안전한 운영을 보장하기 위한 내용을 포함하고 있다.

정답 2번

출제 포인트

ISO/IEC 27001(2005년판 기준 11개 통제 영역 체계)에서 각 통제 영역이 실제로 다루는 목적과 범위를 정확히 구분할 수 있는지를 묻는 문제이다. 영역의 이름만 보고 내용을 짐작하면 안 되고, 각 영역이 대응하는 위협·목표가 무엇인지를 구분해야 한다.

핵심 개념

자산 관리(Asset Management)는 조직의 정보자산을 식별·목록화하고 중요도에 따라 분류하여 그에 맞는 보호 수준을 적용하는 영역이다. 사업 연속성 관리(Business Continuity Management)는 정전, 재해, 시스템 장애 등 업무 중단 사고가 발생했을 때 핵심 업무 프로세스가 중단되지 않도록 하거나 신속히 복구할 수 있도록 대비하는 영역이다. 준거성(Compliance) 영역은 형법·민법 등 법률, 법령, 규정, 계약상 의무 및 보안 요구 사항 위반을 피하기 위한 기준을 제시하는 영역이다. 정보시스템 획득·개발·유지보수 영역은 신규 개발이나 기존 시스템 유지보수 시 정보시스템 내에 보안이 설계·구축되어 있도록 보장하는 영역이다. 통신 및 운영 관리 영역은 정보처리 설비의 정확하고 안전한 운영(운영 절차, 매체 관리, 네트워크 보안 등)을 보장하는 영역이다.

선지별 해설

① O — 자산 관리 영역은 자산을 식별·분류하고 그에 맞게 보호 대책을 적용하는 데 활용되는 영역이므로 설명이 옳다.

② X — 형법과 민법, 법령, 규정 또는 계약 의무 및 보안 요구 사항에 대한 위반을 피하기 위한 기준을 제시하는 것은 사업 연속성 관리 영역이 아니라 준거성(Compliance) 영역의 내용이다. 사업 연속성 관리 영역은 업무 중단 사고에 대비하여 핵심 업무의 지속성을 확보하는 것이 목적이므로, 이 설명은 사업 연속성 관리 영역에 대한 설명으로는 옳지 않다.

③ O — 정보시스템 획득, 개발, 유지 보수 영역은 정보시스템 내에 보안이 수립·반영되어 있음을 보장하기 위한 영역이므로 설명이 옳다.

④ O — 통신 및 운영 관리 영역은 정보처리 설비가 정확하고 안전하게 운영되도록 보장하는 내용을 포함하므로 설명이 옳다.

NoteBase

오답 포인트

이 문제의 함정은 '사업 연속성'이라는 이름만 보고 재해·장애 대응이라는 감을 잡더라도, 선지에 나온 '형법·민법·법령·규정·계약 의무 위반 회피'라는 문구가 준거성 영역의 정의와 그대로 겹친다는 점을 놓치기 쉽다는 데 있다. 영역명과 설명 문구를 서로 바꿔치기하는 방식의 오답 구성이므로, 각 영역명이 나오면 그 영역의 목적(무엇을 막기 위한 것인지)을 먼저 떠올리고 선지 설명과 대조해야 한다.

다시 나오면 이렇게 판단

ISO 27001 통제 영역 문제는 영역명과 목적을 1:1로 짝지어 암기해 두고, 선지에서 영역명과 설명이 실제로 대응하는지부터 확인한다. 법·규정·계약 위반 회피라는 표현이 나오면 곧바로 준거성(Compliance) 영역을 떠올리고, 재해·장애로부터 업무를 지속·복구한다는 표현이 나오면 사업 연속성 관리 영역임을 확인한다.

암기 포인트

자산 관리=자산 식별·분류·보호, 사업 연속성 관리=업무 중단 대비·복구, 준거성=법·규정·계약 위반 회피 기준, 정보시스템 획득·개발·유지보수=시스템 내 보안 내재화, 통신 및 운영 관리=정보처리 설비의 정확·안전한 운영.

NoteBase

문 15. 정수의 소인수분해를 기반으로 한 RSA 암호 알고리즘에서 공개키 $(e, n) = (7, 33)$을 이용하여 생성된 암호문 C 값이 7일 때, 이를 다시 복호화한다면 원문 메시지 값은?

① 11

② 13

③ 17

④ 19

정답 2번

출제 포인트

RSA 공개키 암호 알고리즘에서 공개키로부터 개인키(복호화 지수)를 구하고, 이를 이용해 암호문을 실제로 복호화하는 계산 과정을 정확히 수행할 수 있는지를 묻는다. n의 소인수분해, 오일러 피 함수 $\varphi(n)$ 계산, 모듈러 지수 연산까지 전 과정을 다룬다.

조건 정리

공개키 $(e, n) = (7, 33)$이고 암호문 $C = 7$이다. $n = 33 = 3 \times 11$이므로 $p = 3$, $q = 11$이다. 구해야 할 것은 복호화 지수 d와 이를 이용해 얻어지는 원문 M이다.

사용할 공식

오일러 피 함수: $\varphi(n) = (p - 1)(q - 1)$. 개인키 d는 e · d ≡ 1 ±od(n)을 만족하는 값이다. 복호화는 M ≡ C^d ±odn으로 이루어진다.

계산 과정

$\varphi(33) = (3 - 1)(11 - 1) = 2 \times 10 = 20$이다. $e = 7$이므로 7d ≡ 1 ±od20을 만족하는 d를 찾는다. $d = 3$일 때 $7 \times 3 = 21 \equiv 1$ ±od20이 성립하므로 $d = 3$이다. 이제 M ≡ C^d ±odn = 7^3 ±od33을 계산한다. 7^2 = 49 ≡ 16 ±od33이고, 7^3 = 7^2 × 7 ≡ 16 × 7 = 112 ±od33이다. $112 = 33 \times 3 + 13$이므로 112 ≡ 13 ±od33이다. 따라서 원문 메시지 $M = 13$이다.

선지 판단

① 11: 계산 결과인 13과 다르므로 틀린 값이다.
② 13: 7^3 33 = 13으로 계산 결과와 일치하므로 옳다.
③ 17: 계산 결과인 13과 다르므로 틀린 값이다.
④ 19: 계산 결과인 13과 다르므로 틀린 값이다.

NoteBase

오답 포인트

가장 흔한 실수는 개인키 d를 구하는 식에서 $\varphi(n)$ 대신 n 자체를 모듈러스로 사용하는 것이다. d는 반드시 e · d ≡ 1 ±od(n)에서 구해야 하며, 복호화 연산인 C^d n에서만 n을 모듈러스로 사용한다. 또한 7^3을 계산할 때 343을 그대로 33으로 나누지 않고 중간에 실수로 다른 수로 나누면 값이 틀어지므로, 거듭제곱을 단계별로 모듈러 축소하며 계산하는 습관이 필요하다.

다시 나오면 이렇게 판단

RSA 계산 문제는 항상 같은 순서로 접근한다. 먼저 n을 소인수분해해 p, q를 구하고, $\varphi(n) = (p-1)(q-1)$을 계산한다. 그다음 공개키 지수 e와 $\varphi(n)$을 이용해 ed ≡ 1 ±od(n)을 만족하는 d를 작은 수부터 대입해 찾는다. 마지막으로 암호화는 C ≡ M^e ±odn, 복호화는 M ≡ C^d ±odn 공식에 그대로 대입해 계산한다.

암기 포인트

RSA 4단계: $n = pq$ 소인수분해 → $\varphi(n) = (p-1)(q-1)$ → ed ≡ 1 ±od(n)로 d 도출 → 암호화 C = M^e n / 복호화 M = C^d n. d를 구할 때의 모듈러스는 $\varphi(n)$, 암복호화 연산의 모듈러스는 n이라는 점을 구분해 기억해 둔다.

NoteBase

문 16. 리눅스 파일의 접근 제어에 대한 설명으로 옳지 않은 것은?

① 모든 종류의 파일은 inode라는 파일 관리 수단으로 운영체제에 의해 관리된다.

② passwd 명령으로 패스워드를 설정하면, 패스워드에 대한 암호화나 해시된 값이 /etc/passwd에 저장된다.

③ superuser 계정은 시스템의 모든 권한이 가능하므로 외부에 노출되지 않도록 주의해야 한다.

④ 어떤 권한을 가지고 있는가에 대한 UID, GID가 별도로 존재한다.

정답 2번

출제 포인트

리눅스에서 파일과 계정의 접근 제어가 어떤 요소로 관리되는지 정확히 알고 있는지를 묻는다. inode, 패스워드 저장 위치, superuser 권한, UID/GID의 역할을 구분할 수 있어야 한다.

핵심 개념

inode=파일마다 부여되는 관리 정보 구조체로 파일의 소유자, 권한, 크기, 타임스탬프, 데이터 블록 위치 등을 저장하며 모든 종류의 파일(일반 파일, 디렉터리, 특수 파일 등)에 대해 운영체제가 이를 통해 관리한다. 패스워드 저장=사용자가 passwd 명령으로 암호를 설정하면 그 해시값은 /etc/passwd가 아니라 /etc/shadow 파일에 저장되는 것이 현재 리눅스 시스템의 표준 방식이다(섀도 패스워드 체계). /etc/passwd에는 사용자 계정명, UID, GID, 홈 디렉터리, 로그인 셸 등 계정 정보만 담기고 패스워드 필드는 실제 해시 대신 'x'와 같은 표시로 채워진다. superuser(root)=시스템의 모든 자원과 명령에 대한 무제한 권한을 가지므로 계정 노출이나 탈취 시 피해가 가장 크기 때문에 각별히 보호해야 한다. UID/GID=각 사용자와 그룹에 부여되는 식별 번호로, 파일이나 프로세스에 대해 어떤 권한을 가지는지 판단하는 기준이 된다.

선지별 해설

① O: 리눅스의 모든 파일 종류는 inode를 통해 운영체제가 관리한다.
② X: 틀린 표현 → 올바른 표현. 패스워드에 대한 암호화·해시된 값은 /etc/passwd가 아니라 /etc/shadow에 저장된다. /etc/passwd에는 계정 정보만 저장되고 패스워드 해시값은 담기지 않는다.
③ O: superuser 계정은 시스템의 모든 권한을 가지므로 외부에 노출되지 않도록 각별히 주의해야 한다.
④ O: 파일이나 자원에 대한 권한 판단 기준으로 UID와 GID가 별도로 존재한다.

오답 포인트

/etc/passwd라는 이름 때문에 패스워드 해시가 그 안에 저장된다고 착각하기 쉽지만, 보안 강화를 위해 섀도 패스워드 체계가 도입된 이후에는 실제 해시값은 /etc/shadow에 분리 저장되고 /etc/passwd는 일반 사용자도 읽을 수 있는 계정 정보 파일로만 쓰인다는 점을 혼동하면 안 된다.

NoteBase

다시 나오면 이렇게 판단

리눅스 접근 제어 문항에서 '패스워드 해시가 /etc/passwd에 저장된다'는 서술이 나오면 즉시 틀린 선지로 의심한다. 파일명이 passwd라고 해서 실제 암호 정보가 그 안에 있다고 단정하지 않는다.

암기 포인트

계정 정보는 /etc/passwd, 패스워드 해시값은 /etc/shadow — 이 분리 저장 구조를 한 쌍으로 기억해 둔다.

NoteBase

문 17. 블루투스에 대한 설명으로 옳지 않은 것은?

① 페어링 과정은 한 장치가 그 지역에 있는 다른 장치들을 찾아 BD_ADDR이나 논리적 이름에 근거해 파트너가 될 장치를 선택하는 것이다.

② 장치 간 종류를 식별하기 위해서 SDP(Service Discovery Protocol)를 보내고 받는다.

③ 블루투스의 취약점을 이용하여 장비의 임의 파일에 접근하는 공격은 BlueBug이다.

④ OPP(OBEX Push Profile)는 블루투스 장치끼리 인증 없이 정보를 간편하게 교환하기 위해 개발되었다.

정답 3번

출제 포인트

블루투스 동작 과정(페어링, SDP)과 블루투스 관련 공격 기법(BlueBug, BlueSnarf 등) 및 프로파일(OPP)의 명칭과 실제 동작을 정확히 구분할 수 있는지를 묻는다. 특히 공격 기법의 이름과 그 공격이 실제로 하는 일을 짝짓는 부분에서 혼동을 유도한다.

핵심 개념

블루투스 공격은 이름과 동작이 서로 짝을 이루는데, 이 짝을 바꿔치기하면 오답 선지가 된다. 블루재킹은 상대 장치에 익명의 메시지나 명함을 보내는 장난성 공격이고, 블루스나핑(블루스나프)은 취약점을 이용해 상대 장치에 저장된 연락처·파일 등 임의의 데이터에 무단으로 접근하는 공격이다. 블루버그는 상대 장치의 무선 인터페이스를 장악해 AT 명령을 실행함으로써 통화 연결, 문자 발송 등 장치의 기능 자체를 원격으로 조종하는 공격이다. 즉 파일 접근은 블루스나핑의 특징이지 블루버그의 특징이 아니다.

선지별 해설

① 페어링은 한 장치가 주변의 다른 블루투스 장치를 검색하여 장치 주소(BD_ADDR)나 장치에 설정된 논리적 이름을 근거로 연결할 파트너 장치를 선택하는 과정이 맞다. 페어링 과정에 대한 설명으로 옳다.
② SDP(Service Discovery Protocol)는 블루투스 장치들이 서로 어떤 서비스와 프로파일을 지원하는지, 즉 장치의 종류와 제공 기능을 식별하기 위해 질의와 응답 메시지를 주고받는 프로토콜이 맞다. 옳은 설명이다.
③ 블루투스의 취약점을 이용해 장비에 저장된 임의의 파일(연락처, 일정, 문자 등)에 무단으로 접근하는 공격은 블루버그가 아니라 블루스나핑(블루스나프)이다. 블루버그는 파일 접근이 아니라 상대 장치의 통신 채널을 장악해 전화 걸기, 문자 전송 등 장치의 기능을 원격으로 조종하는 공격이므로, 이 선지는 공격 이름과 실제 동작이 서로 뒤바뀐 틀린 설명이다. → 옳지 않은 것은 이 선지이다.
④ OPP(OBEX Push Profile)는 명함이나 파일 같은 객체를 블루투스 장치 간에 별도의 인증 절차 없이 간편하게 주고받기 위해 만들어진 프로파일이 맞다. 옳은 설명이다.

NoteBase

오답 포인트

블루투스 공격 이름을 외울 때 '무엇을 할 수 있는 공격인가'까지 함께 묶어서 외우지 않으면, 이름은 알아도 동작 설명이 바뀐 선지를 걸러내지 못한다. 이 문제처럼 '임의 파일 접근'이라는 동작 설명에 이름만 블루버그로 바꿔치기하는 방식이 자주 출제된다.

다시 나오면 이렇게 판단

선지에서 공격 기법 이름과 그 공격의 구체적 동작(파일 접근인지, 기능 원격 조종인지, 단순 메시지 전송인지)이 함께 제시되면, 이름보다 동작 설명을 먼저 확인하고 그 동작에 맞는 공격 이름이 실제로 맞는지 대조한다.

암기 포인트

블루재킹=메시지·명함 스팸 전송, 블루스나핑(블루스나프)=파일·정보 무단 접근, 블루버그=원격 기능 조종(통화·문자 등 AT 명령 실행)으로 세 가지를 짝지어 암기한다.

NoteBase

문 18. 방화벽의 보안 기능에 대한 설명으로 옳은 것은?

① 방화벽은 내부의 불만이 있는 사용자 또는 외부 공격자와 무의식적으로 협력하는 사용자를 완벽히 차단할 수 있다.

② 방화벽을 설치하게 되면 외부로부터의 모든 무선랜 통신을 안전하게 보호할 수 있다.

③ 랩톱, PDA와 같은 이동형 저장장치가 감염되는 경우에도 방화벽을 설치하여 내부 네트워크를 안전하게 보호할 수 있다.

④ 내부 보안 정책을 만족하는 트래픽만이 방화벽을 통과할 수 있다.

정답 4번

출제 포인트

방화벽이 실제로 할 수 있는 기능과 할 수 없는 한계를 구분하는 문제이다. 방화벽은 내부 네트워크와 외부 네트워크의 경계에서 사전에 정의된 보안 정책(접근 통제 규칙)에 따라 트래픽을 허용하거나 차단하는 장비이며, 그 이상의 역할(내부자 행위 통제, 무선 통신 보호, 내부에서 이미 감염된 장치 통제)은 수행하지 못한다는 점이 핵심이다.

핵심 개념

방화벽의 기본 동작 원리는 화이트리스트 방식의 트래픽 필터링이다. 즉 내부 보안 정책에서 허용하도록 정의한 트래픽만 통과시키고 그 외의 트래픽은 모두 차단한다. 방화벽은 네트워크 경계(내부-외부 사이)에 위치하므로 경계를 통과하지 않는 통신(예: 무선랜을 통한 직접 통신, 이미 내부에 들어온 이동형 저장장치의 감염)이나 이미 내부 네트워크에 접속 권한을 가진 사용자의 오·남용에 대해서는 통제력이 없다.

선지별 해설

① X: 방화벽은 경계를 통과하는 트래픽을 정책에 따라 필터링할 뿐, 정상적인 접근 권한을 가진 내부의 불만 있는 사용자나 외부 공격자와 무의식적으로 협력하는(사회공학 등에 속아 내부 정보를 유출하는) 사용자의 행위까지 완벽히 차단하지는 못한다. '완벽히 차단'은 방화벽의 한계를 벗어난 과장된 설명이다.
② X: 방화벽은 일반적으로 유선 네트워크 경계에서 동작하는 장비로, 무선랜(WLAN) 통신 자체를 방화벽이 직접 보호하지는 않는다. 무선 구간의 보안은 별도의 무선 보안 대책(암호화, 인증 등)이 필요하며, 방화벽 설치만으로 외부로부터의 모든 무선랜 통신이 안전해지는 것은 아니다.
③ X: 랩톱, PDA와 같은 이동형 저장장치가 이미 감염된 상태로 내부 네트워크에 물리적으로 연결되거나 반입되는 경우, 이는 방화벽이 감시하는 경계(내부-외부 트래픽 경로)를 우회하는 경로이므로 방화벽으로는 이러한 감염 확산을 막을 수 없다.
④ O: 방화벽의 본질적 기능은 미리 설정된 내부 보안 정책(접근 통제 규칙)에 부합하는 트래픽만 통과시키고 그렇지 않은 트래픽은 차단하는 것이다. 이는 방화벽의 가장 기본적이고 정확한 정의에 해당한다.

NoteBase

오답 포인트

①·②·③은 모두 방화벽의 보호 범위를 실제보다 넓게 확장하여 '완벽히', '모든', '이동형 저장장치가 감염되어도 안전' 등으로 과장한 표현이다. 방화벽은 네트워크 경계를 통과하는 트래픽을 정책 기반으로 통제하는 장비일 뿐, 내부자의 의도적·비의도적 행위, 무선 구간 통신, 이미 내부에 들어온 감염 매체까지 막아주는 만능 보안 솔루션이 아니라는 점을 혼동하면 오답을 고르게 된다.

다시 나오면 이렇게 판단

선지에 '완벽히', '모든', '어떤 경우에도 안전' 같은 절대적 표현이 나오면 방화벽의 한계를 벗어난 과장 설명일 가능성이 높다고 의심한다. 반대로 '내부 보안 정책을 만족하는 트래픽만 통과' 처럼 방화벽의 필터링 동작을 있는 그대로 서술한 선지가 정답일 확률이 높다.

암기 포인트

방화벽=경계에서 정책 기반 트래픽 필터링 장비. 방화벽이 막지 못하는 것: 내부자의 의도적·비의도적 협조 행위, 무선랜 등 경계를 우회하는 통신, 이미 감염된 이동형 저장장치의 내부 반입.

NoteBase

문 19. 재해복구 시스템의 복구 수준별 유형에 대한 설명으로 옳지 않은 것은?

① Mirror Site - 주 센터와 동일한 수준의 정보기술 자원(하드웨어, 소프트웨어, 기타 부대 장비 등)을 원격지에 구축하여 모두 액티브 상태에서 실시간으로 동시에 서비스하는 방식

② Hot Site - 주 센터와 동일한 수준의 정보기술 자원을 대기 상태(standby)로 원격지에 구축하여 동기적 혹은 비동기적 미러링을 통해 데이터의 최신을 유지하고 있다가 주 센터 재해 시 액티브로 전환하여 서비스하는 방식

③ Down Site - 웹 애플리케이션 서비스 등 데이터의 업데이트 빈도가 높은 정보시스템을 액티브로 전환하여 서비스하는 방식

④ Cold Site - 기계실, 전원 시설, 통신 설비, 공조 시설, 온도 조절 시스템 등을 갖추어 놓고, 주 센터 재해 시 정보기술 자원을 설치하여 서비스하는 방식

정답 3번

출제 포인트

재해복구 시스템(DRS)에서 원격지 백업센터를 구축 수준에 따라 미러 사이트, 핫 사이트, 웜 사이트, 콜드 사이트로 구분하는 표준 분류와 각 유형의 정의를 정확히 아는지 묻는 문제이다. 특히 실제로는 존재하지 않는 용어를 끼워 넣어 정의의 진위를 가리는 방식이 출제 포인트이다.

핵심 개념

미러 사이트(Mirror Site)는 주 센터와 동일한 자원을 원격지에 두고 두 곳 모두 액티브 상태로 실시간 동시 서비스하여 데이터 손실이 없고 복구 시간이 가장 짧다. 핫 사이트(Hot Site)는 동일 수준의 자원을 대기 상태로 원격지에 구축해 두고 동기 또는 비동기 미러링으로 데이터를 최신으로 유지하다가 재해 발생 시에만 액티브로 전환하는 방식이다. 웜 사이트(Warm Site)는 핫 사이트와 콜드 사이트의 중간 단계로, 중요도가 높지 않거나 데이터 업데이트 빈도가 낮은 시스템 위주로 자원을 부분적으로 준비해 두고 재해 시 나머지를 보완하여 가동한다. 콜드 사이트(Cold Site)는 기계실, 전원, 통신, 공조 등 기반 시설만 미리 갖추어 놓고 데이터는 백업 매체로 보관하다가 재해 발생 후 하드웨어를 설치하여 복구하므로 복구 시간이 가장 오래 걸린다.

NoteBase

선지별 해설

① Mirror Site에 대한 설명은 옳다. 주 센터와 동일한 정보기술 자원을 원격지에 구축하고 두 사이트 모두 액티브 상태에서 실시간으로 동시에 서비스하는 방식이 미러 사이트의 정의와 일치한다.
② Hot Site에 대한 설명은 옳다. 동일한 수준의 자원을 대기 상태로 원격지에 두고 동기적 혹은 비동기적 미러링으로 데이터를 최신으로 유지하다가 재해 시 액티브로 전환하는 방식은 핫 사이트의 정의와 일치한다.
③ 옳지 않다. 이 선지는 '데이터의 업데이트 빈도가 높은 정보시스템'을 대상으로 한다고 설명하고 있으나, 이러한 부분적·단계적 자원 준비 방식은 웜 사이트(Warm Site)에 해당하며, 웜 사이트는 오히려 중요도나 데이터 업데이트 빈도가 낮은 시스템 위주로 자원을 준비해 두는 방식이다. 또한 'Down Site'라는 명칭 자체가 재해복구 수준 분류에 존재하지 않는 용어이므로 명칭과 설명 모두 옳지 않다.
④ Cold Site에 대한 설명은 옳다. 기계실, 전원 시설, 통신 설비, 공조 시설 등만 갖추어 놓고 재해 발생 시 정보기술 자원을 설치하여 서비스하는 방식은 콜드 사이트의 정의와 일치한다.

오답 포인트

Down Site라는 용어에 이끌려 이것이 실제 존재하는 유형이라고 착각하면 안 된다. 재해복구 수준별 유형은 미러, 핫, 웜, 콜드의 네 단계로 정리되며 다운 사이트라는 표준 명칭은 없다. 또한 웜 사이트의 특징인 '업데이트 빈도가 낮은 시스템 위주 준비'를 '업데이트 빈도가 높은 시스템'으로 뒤바꾸어 설명하는 함정에 유의한다.

다시 나오면 이렇게 판단

선지에서 사이트 명칭과 설명을 따로 떼어 보고, 먼저 그 명칭이 미러·핫·웜·콜드 네 가지 중 하나인지 확인한다. 낯선 명칭(Down Site 등)이 등장하면 그 자체를 의심하고, 이어서 설명 내용이 어느 표준 유형의 정의와 실제로 일치하는지 역으로 대조하여 오류를 찾는다.

암기 포인트

복구 속도가 빠른 순서로 미러 사이트, 핫 사이트, 웜 사이트, 콜드 사이트를 기억해 둔다. 미러=원격지도 항상 액티브, 핫=대기하다 전환, 웜=중요도·업데이트 빈도 낮은 시스템 위주 부분 준비, 콜드=기반 시설만 준비 후 재해 시 설치라는 네 문장으로 정리해 둔다.

NoteBase

문 20. 정보보안 관리 규격 중 IT 보호 및 통제부문의 모범적인 업무 수행 방법에 적용 가능한 ISACA(Information Systems Audit and Control Association)에서 개발된 프레임워크는?

① COBIT

② BS 7799

③ BSI

④ HIPAA

정답 1번

출제 포인트

정보보호·정보시스템 감사 관련 국제 프레임워크와 그 개발 주체를 정확히 매칭할 수 있는지를 묻는 문제이다. 특히 ISACA(정보시스템감사통제협회)가 개발한 IT 거버넌스·통제 프레임워크가 무엇인지 구분하는 것이 핵심이다.

핵심 정리

COBIT(Control Objectives for Information and related Technology)은 ISACA와 ITGI(IT 거버넌스 연구소)가 개발한 IT 거버넌스 및 통제 프레임워크로, IT 보호 및 통제부문의 모범적인 업무 수행 방법(모범관행)을 제시한다. BS 7799는 영국표준협회(BSI)가 제정한 정보보호관리체계 표준으로 이후 ISO/IEC 27001의 모태가 되었다. BSI는 영국표준협회 자체를 가리키는 표준화 기관 명칭이다. HIPAA는 미국의 의료정보 보호에 관한 법률이다.

선지별 해설

① COBIT: O. ISACA에서 개발한 IT 거버넌스·통제 프레임워크로, IT 보호 및 통제부문의 모범적인 업무 수행 방법을 정의한다.
② BS 7799: X. 영국표준협회(BSI)가 제정한 정보보안관리체계 표준으로 ISACA가 개발한 것이 아니다.
③ BSI: X. 프레임워크가 아니라 영국의 표준화 기관(British Standards Institution) 명칭이다.
④ HIPAA: X. 미국의 의료정보 보호 관련 법률로 ISACA와 무관하다.

오답 포인트

BS 7799와 BSI를 혼동하기 쉬운데, BS 7799는 표준의 이름이고 BSI는 그 표준을 제정한 기관의 이름이다. 두 선지 모두 개발 주체가 ISACA가 아니라 영국표준협회라는 점에서 오답이다. HIPAA는 정보보안 표준이 아니라 미국의 법률이라는 점에서 성격 자체가 다르다.

NoteBase

다시 나오면 이렇게 판단

문제에 개발 기관(ISACA, ISO, BSI 등)이 명시되면 프레임워크 이름보다 먼저 그 기관이 실제로 만든 것이 무엇인지부터 짝짓는다. ISACA는 COBIT, 영국표준협회는 BS 7799(ISO 27001의 전신), 미국 법률은 HIPAA(의료)·SOX(회계) 등으로 구분해 두면 빠르게 소거할 수 있다.

암기 포인트

ISACA → COBIT(IT 거버넌스·통제 모범관행), BSI(영국표준협회) → BS 7799(→ISO/IEC 27001), 미국 의료정보 보호 법률 → HIPAA로 기관과 산출물을 짝지어 외워 둔다.

NoteBase