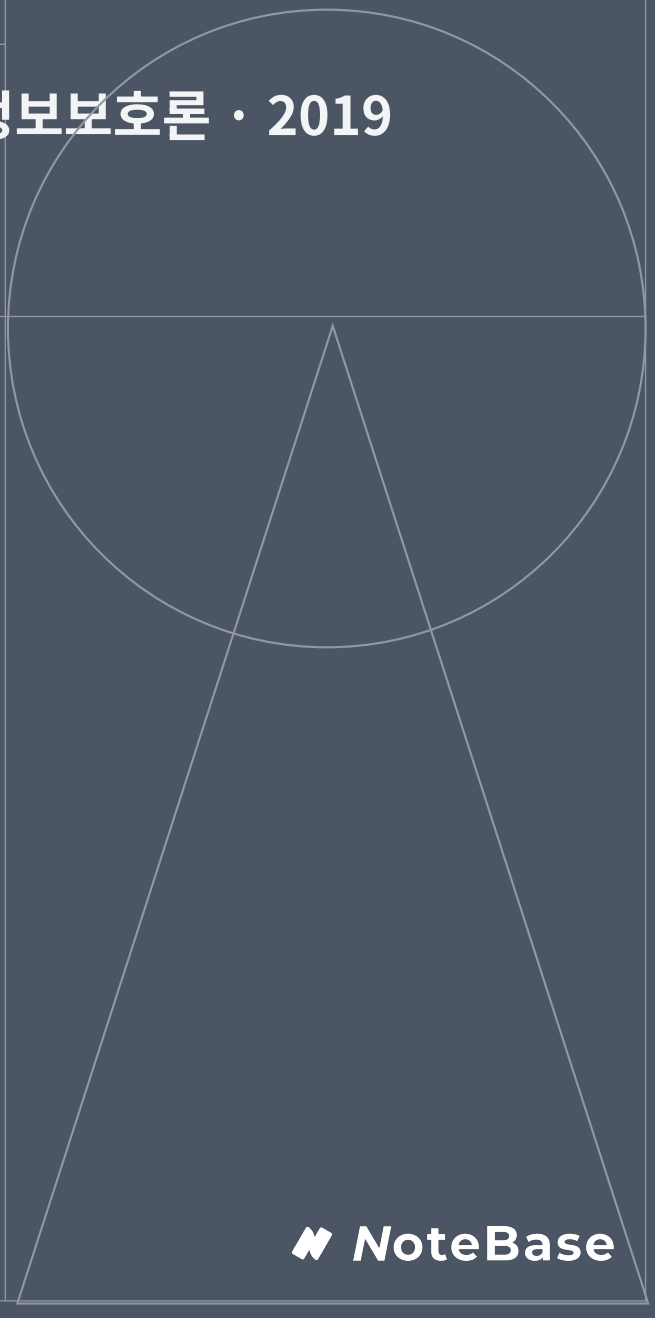
기출OX 해설집

공무원/경찰/공채(경위) · 정보보호론 · 2019



NoteBase

기출OX 해설집

공무원/경찰/공채(경위) · 정보보호론 · 2019

공무원/경찰/공채(경위) · 정보보호론 · 2019

문 1. 정보보호의 목표에 관한 설명 중 옳지 않은 것은?

① 기밀성(Confidentiality)을 보장하기 위한 기술로는 암호화, 접근제어 등이 있다.

② 가용성(Availability)은 사용자가 필요할 때 데이터에 접근할 수 있는 능력을 말한다.

③ 가용성(Availability)을 유지하기 위해 데이터 백업, 위협 요소 제거 등의 기술을 사용할 수 있다.

④ 무결성(Integrity)은 특정한 작업 또는 행위에 대해 책임소재를 확인하는 것이 가능함을 말한다.

정답 4번

간단한 해설

특정 행위를 수행한 주체를 추적하여 책임소재를 확인하는 성질은 **책임추적성**이다. 무결성은 정보가 **허가 없이 변경·훼손되지 않도록 하는 것**을 뜻한다.

선지별 해설

정보보호의 기본 목표인 기밀성·무결성·가용성은 각각 허가되지 않은 공개, 부당한 변경·훼손, 필요한 시점의 이용 불가를 방지하는 것과 관련된다. 행위자와 책임을 연결하는 책임추적성은 이들과 구별되는 개념이다.

① O: 기밀성은 권한 없는 주체가 정보를 알 수 없게 하는 성질이다. **암호화**는 내용을 읽을 수 없게 변환하고, **접근제어**는 누가 정보를 읽을 수 있는지 제한하므로 모두 기밀성 보호에 활용된다.

② O: 가용성은 정당한 사용자가 필요할 때 정보와 서비스를 이용할 수 있는 성질이다. 데이터가 존재하더라도 장애나 공격 때문에 필요한 시점에 접근할 수 없다면 가용성이 훼손된 것이다.

③ O: 백업은 원본 데이터가 손상되거나 사라졌을 때 **복구하여 다시 이용할 수 있게** 하므로 가용성 확보에 기여한다. 장애나 공격을 일으킬 수 있는 위협 요소를 줄이는 조치 역시 서비스 중단 가능성을 낮춘다. 백업 자체가 무중단 운영을 보장한다는 뜻은 아니다.

④ X: 특정 작업이나 행위를 누가 수행했는지 추적하여 책임소재를 확인하는 것은 **책임추적성**에 관한 설명이다. 사용자 식별과 인증, 감사 로그 등이 이를 뒷받침한다. 무결성은 정보가 인가되지 않은 방식으로 변경되거나 훼손되지 않도록 정확성과 완전성을 유지하는 성질이다.

NoteBase

문 2. 암호 해독 공격의 유형에 관한 설명으로 옳지 않은 것은?

① 암호문 단독 공격(Ciphertext Only Attack)은 암호문만을 가지고 평문이나 키를 찾아내는 방법으로, 암호문의 통계적 특성 등을 추정하여 해독하는 방법이다.

② 알려진 평문 공격(Known Plaintext Attack)은 평문에 대응되는 암호문을 약간 알고 있는 상태에서, 나머지 암호문에 대한 공격을 하는 방법이다.

③ 선택 평문 공격(Chosen Plaintext Attack)은 암호 해독자가 암호기에 접근할 수 있어, 적당한 평문을 선택하여 그 평문에 해당하는 암호문을 얻어 키나 평문을 해독하는 방법이다.

④ 선택 암호문 공격(Chosen Ciphertext Attack)은 해독자가 암호기와 복호기에 모두 접근할 수 있어, 선택한 암호문에 대한 평문과 선택한 평문에 대한 암호문을 얻어 키나 평문을 해독하는 방법이다.

정답 4번

간단한 해설

선택 암호문 공격의 구별 기준은 **공격자가 고른 암호문의 복호화 결과를 얻는다**는 점이다. 암호기와 복호기 양쪽에 모두 접근해야 한다는 것을 이 공격의 기본 정의로 삼지는 않는다.

선지별 해설

① O: 암호문 단독 공격에서는 대응하는 평문을 확보하지 못한 채 암호문을 관찰하고 분석한다. 암호문에 남은 빈도나 반복 같은 통계적 특징 등을 이용해 평문 또는 키에 관한 정보를 추정할 수 있다. 이는 공격자가 가진 정보의 범위를 설명하는 것이며, 모든 암호가 통계 분석으로 쉽게 해독된다는 뜻은 아니다.

② O: 알려진 평문 공격은 이미 확보한 평문과 그에 대응하는 암호문 쌍을 이용한다. 알려진 관계를 분석해 키를 추정하거나 다른 암호문을 해독하려는 방식이다. 공격자가 평문을 직접 선택하여 새 암호문을 얻는 것이 필수는 아니라는 점에서 선택 평문 공격과 다르다.

③ O: 선택 평문 공격에서는 공격자가 평문을 고르고 그 평문의 암호화 결과를 얻을 수 있다. 특정한 입력을 넣었을 때 출력이 어떻게 변하는지 관찰하여 암호 체계를 분석한다. **입력을 공격자가 선택할 수 있다는 점**이 단순히 평문·암호문 쌍을 알고 있는 경우와의 차이이다.

④ X: 선택 암호문 공격의 기본 정의는 공격자가 선택한 암호문을 복호화한 평문을 얻어 분석하는 것이다. 선지는 여기에 선택한 평문의 암호화 결과까지 얻는 능력을 함께 묶어, 기본 유형을 구별하는 설명으로는 부정확하다. **선택 암호문을 복호화해 볼 수 있는 능력**이 핵심이며 암호기 접근까지 필수 조건은 아니다. 다만 현대의 형식적 보안 모델에서는 암호화 질의와 복호화 질의를 함께 허용하기도 하므로, 두 능력이 동시에 존재하면 선택 암호문 공격이 될 수 없다는 뜻은 아니다.

NoteBase

문 3. 블록 암호 모드에 관한 설명 중 옳지 않은 것은?

① ECB(Electronic Code Book) 모드는 평문을 동일한 크기의 평문블록으로 나누고, 키로 암호화하여 암호블록을 생성한다.

② CTR(CounTeR) 모드는 평문블록의 암호화를 병렬적으로 처리 가능하다.

③ CBC(Cipher Block Chaining) 모드는 인증을 수행하는 대칭키 암호 시스템의 하나인 Kerberos 버전 5에서도 사용된다.

④ CFB(Cipher Feed Back) 모드에서 이전 블록 값의 최상위 비트에서 발생한 에러는 이후 블록 값에 영향을 미치지 않는다.

정답 4번

간단한 해설

CFB는 **이전 암호문을 다음 처리에 피드백**하므로 암호문의 오류가 뒤 구간의 복호화에도 영향을 줄 수 있다. 최상위 비트의 오류도 이후 구간에 전파될 수 있다.

선지별 해설

① O. ECB는 평문을 암호 알고리즘의 블록 크기에 맞게 나누고, 각 블록을 같은 키로 독립적으로 암호화한다. 같은 키에서 동일한 평문 블록은 동일한 암호문 블록이 되므로 평문의 반복 구조가 드러날 수 있다.

② O. CTR은 서로 다른 카운터 값을 암호화한 결과를 대응하는 평문 블록과 XOR하여 암호문을 만든다. 각 블록의 계산에 이전 암호문이 필요하지 않으므로 **블록별 병렬 처리**가 가능하다. 같은 키에서 카운터 값을 재사용하지 않아야 한다.

③ O. CBC는 이전 암호문 블록을 다음 평문 블록과 XOR한 뒤 암호화하는 연결 방식이다. Kerberos 버전 5의 암호 체계에는 CBC 계열 방식이 사용되어 왔으며, AES 기반 방식도 CBC에 암호문 훔치기(CTS)를 결합한다. 이는 인증 프로토콜 안에서 CBC 계열 암호화가 사용된다는 뜻이지, CBC만으로 사용자 인증이 완성된다는 뜻은 아니다.

④ X. CFB는 이전 암호문을 피드백하여 다음 구간의 복호화에 사용할 값을 만든다. 따라서 피드백되는 암호문에 오류가 생기면 **이후 구간의 복호화에도 영향**을 주며, 최상위 비트의 오류라고 해서 예외가 되지 않는다. 전체 블록 단위 CFB에서 전송 중 한 암호문 블록의 한 비트가 바뀌면 그 평문 블록의 같은 비트와 다음 평문 블록에 오류가 발생할 수 있다. 다른 오류가 없다면 그다음 블록부터 회복하며, 더 작은 세그먼트 단위의 CFB에서는 영향이 이어지는 구간 수가 달라진다.

따라서 오류가 이후 블록에 영향을 미치지 않는다고 한 ④가 옳지 않다.

NoteBase

문 4. 다음 중 AES의 특징이 아닌 것은?

① Feistel 구조의 암호화 알고리즘이다.

② 128비트 블록 단위의 암호화를 수행한다.

③ 사용 가능한 암호키의 길이는 총 3종류로 128비트, 192비트, 256비트가 있다.

④ 암호키 길이가 128비트인 경우 라운드의 횟수는 10회이다.

정답 1번

간단한 해설

AES는 치환·순열망(SPN) 구조이며, 블록 크기는 128비트로 고정된다. 키 길이와 라운드 수는 128비트·10회, 192비트·12회, 256비트·14회로 대응한다.

선지별 해설

① (X) AES는 **치환·순열망(SPN) 구조**의 블록 암호이다. 바이트 치환, 행 이동, 열 혼합, 라운드 키 덧셈 등을 통해 블록 전체를 변환한다. 좌우 부분으로 나누어 한쪽의 함수 출력을 다른 쪽과 결합하는 Feistel 구조라는 설명은 맞지 않는다.

② (O) AES의 **블록 크기는 128비트**로 고정된다. 암호키를 192비트나 256비트로 늘리더라도 한 번에 처리하는 데이터 블록은 128비트이다.

③ (O) AES의 키 길이는 **128·192·256비트**의 세 종류이다. 각각 AES-128, AES-192, AES-256으로 부르며, 이 숫자는 블록 크기가 아니라 키 길이를 나타낸다.

④ (O) 키 길이가 128비트이면 **10라운드**를 수행한다. 192비트이면 12라운드, 256비트이면 14라운드이다. 최초의 라운드 키 덧셈을 별도의 한 라운드로 더 세지 않는다.

따라서 AES의 특징이 아닌 것은 ①이다.

NoteBase

문 5. 비대칭키 암호화 알고리즘으로만 묶인 것은?

① RSA, ElGamal

② FEAL, AES

③ SEED, DES

④ ARIA, IDEA

정답 1번

간단한 해설

비대칭키 암호는 **공개키와 개인키를 한 쌍으로 구분**한다. RSA와 ElGamal은 이 구조를 사용하는 공개키 암호이므로 두 알고리즘 모두 비대칭키 방식에 해당한다.

개념 구분

대칭키 암호는 암호화와 복호화에 같은 비밀키를 공유하여 사용한다. 비대칭키 암호는 공개해도 되는 공개키와 비밀로 유지하는 개인키를 구분하며, 기밀성을 위한 암호화에서는 수신자의 공개키로 암호화한 내용을 수신자의 개인키로 복호화한다.

RSA는 큰 정수의 소인수분해가 어렵다는 성질과 관련된 수학적 구조를 이용하고, ElGamal은 이산로그 문제의 어려움을 이용하는 공개키 암호이다. 두 알고리즘 모두 **서로 대응하는 공개키·개인키**를 사용하므로 비대칭키로 분류한다.

FEAL·AES, SEED·DES, ARIA·IDEA는 각각 모두 대칭키 블록 암호의 묶음이다. 알고리즘마다 내부 구조는 다르지만 암호화와 복호화를 위해 공유한 비밀키를 사용하므로, 이들을 공개키 암호의 묶음으로 고를 수 없다.

따라서 비대칭키 암호화 알고리즘으로만 이루어진 묶음은 ① RSA, ElGamal이다.

NoteBase

문 6. MAC(Message Authentication Code)에 대한 설명 중 옳지 않은 것은?

① MAC에 대한 재전송 공격(Reply Attack)은 순서 번호(Sequence Number) 사용, 타임스탬프(Timestamp), 비표(Nonce) 등을 사용하여 막을 수 있다.

② HMAC(Hashed MAC)은 일방향 해시 함수를 이용하여 메시지 인증 코드를 구성하는 방법이다.

③ MAC은 제3자에 대한 증명, 부인방지를 해결할 수 없다.

④ HMAC(Hashed MAC)에 사용되는 일방향 해시함수는 교체가 어려워 다른 해시함수를 사용할 수 없다.

정답 4번

간단한 해설

HMAC은 **기반 해시함수를 교체할 수 있도록 설계된** 메시지 인증 방식이다. 특정 해시함수에 고정된 것이 아니며, 공유 비밀키와 암호학적 해시함수를 함께 사용한다.

선지별 해설

MAC은 송신자와 수신자가 공유하는 비밀키로 메시지의 인증 값을 만들고 검증하는 방식이다. 메시지의 무결성과 출처 인증에 쓰이지만, 메시지의 최신성이나 제3자에 대한 부인방지가 자동으로 보장되는 것은 아니다.

① O: 공격자가 과거의 정상 메시지와 MAC을 그대로 다시 보내면 MAC 값은 여전히 유효할 수 있다. 따라서 **순서 번호·타임스탬프·비표를 MAC의 보호 대상에 포함**하고, 수신 측에서 중복 여부나 유효 시간, 비표의 일치 여부 등을 확인하여 재전송을 거부한다. 이러한 값을 넣기만 하고 실제로 검사하지 않으면 방어 효과가 없다.

② O: HMAC은 **공유 비밀키와 암호학적 해시함수**를 결합하여 MAC을 구성한다. 키와 메시지를 정해진 내부·외부 해시 구조로 처리하므로, 누구나 계산할 수 있는 단순한 메시지 해시값과는 다르다.

③ O: 일반적인 MAC에서는 송신자뿐 아니라 수신자도 같은 비밀키를 알고 있어 유효한 MAC을 만들 수 있다. 따라서 제3자에게 특정 메시지를 송신자가 생성했다고 독립적으로 입증하기 어렵고, **송신자 고유의 서명에 기반한 부인방지**를 제공하지 못한다.

④ X: HMAC은 기반 해시함수의 세부 구현에 고정되지 않도록 구성되어 있어, 필요하면 적합한 다른 해시함수로 교체할 수 있다. 예를 들어 사용하는 해시함수에 따라 HMAC-SHA-256 등으로 구분한다. 실제 교체 시에는 양쪽이 같은 알고리즘과 매개변수를 사용해야 하므로, 교체 가능하다는 것과 서로 다른 설정으로도 검증된다는 것은 별개이다.

NoteBase

문 7. 전자 서명에 관한 설명 중 옳은 것은?

① 전자 서명의 요구조건으로는 재사용 가능과 서명자 인증이 있다.

② 전자 서명에서 메시지를 송신자의 개인키로 암호화하는 것이 서명 작성에 해당되고, 그 암호문을 송신자의 공개키로 복호화하는 것이 서명 검증에 해당한다.

③ 전자 서명을 통해 메시지의 기밀성이 보장되는 통신을 할 수 있다.

④ 전자 서명으로 부인은 방지할 수 있지만, 내용 변경 행위를 검출할 수는 없다.

정답 2번

간단한 해설

전자서명은 송신자의 개인키로 생성하고, 대응하는 공개키로 검증한다. 서명자 인증·무결성·부인방지를 지원하지만, 메시지를 숨기는 기밀성은 별도의 암호화가 담당한다.

선지별 해설

① (X) 서명자 인증은 요구조건에 해당하지만, **재사용 가능**은 틀리다. 서명은 특정 메시지와 결합되어야 하므로 다른 메시지에 옮겨 붙여 유효한 서명으로 사용할 수 없어야 한다. 같은 원문과 서명을 여러 번 검증할 수 없다는 뜻은 아니다.

② (O) 핵심은 **송신자의 개인키로 서명하고, 송신자의 공개키로 검증**한다는 점이다. 문항의 암호화·복호화 표현은 RSA 방식의 서명 원리를 단순화한 설명으로 이해한다. 실제 RSA 서명은 메시지의 해시와 정해진 인코딩을 이용하며, 모든 전자서명 알고리즘을 메시지 암호화·복호화와 동일시해서는 안 된다.

③ (X) 전자서명 자체는 **기밀성을 제공하지 않는다**. 서명자와 메시지의 진위를 확인할 수 있어도 내용을 숨기지는 않는다. 메시지를 비밀로 전달하려면 별도의 암호화가 필요하다.

④ (X) 전자서명은 부인방지를 지원할 뿐 아니라 **메시지의 변경을 검출**하여 무결성을 확인하게 한다. 서명 후 내용이 달라지면 그 메시지에 대한 서명 검증이 실패한다. 변경 행위를 물리적으로 막는 것과 변경 여부를 검출하는 것은 구별한다.

따라서 옳은 설명은 개인키와 공개키의 역할을 바르게 연결한 ②이다.

NoteBase

문 8. 다음 지문은 윈도우 운영체제의 주요 하이브 레지스트리에 관한 설명이다. 옳은 것은 모두 몇 개인가?

가. HKEY_CURRENT_CONFIG는 시작 프로세스에서 필수적인 소프트웨어 관련 정보를 포함한다.
나. HKEY_LOCAL_MACHINE은 컴퓨터 하드웨어 및 운영체제 정보를 포함한 시스템 설정 정보를 갖고 있다.
다. HKEY_CLASSES_ROOT는 파일 확장자에 대한 정보를 갖고 있다.
라. HKEY_USERS는 시스템에 등록된 모든 사용자들에 대한 정보를 갖고 있다.

① 1개
② 2개
③ 3개
④ 4개

정답 3번

간단한 해설

HKEY_CURRENT_CONFIG가 다루는 것은 **현재 하드웨어 프로필**이며, 시작에 필수적인 소프트웨어 정보라는 설명은 잘못되었다. HKEY_USERS는 사용자별 설정을 다루지만, 실제로 표시되는 범위는 **현재 로드된 사용자 프로필**이라는 점을 구별해야 한다.

NoteBase

보기별 해설

가. X: HKEY_CURRENT_CONFIG는 시스템이 시작할 때 사용하는 **현재 하드웨어 프로필**의 정보를 제공한다. 따라서 '시작 프로세스에서 필수적인 소프트웨어 관련 정보'를 '현재 사용 중인 하드웨어 프로필 정보'로 고쳐야 한다.

나. O: HKEY_LOCAL_MACHINE은 **특정 사용자에 종속되지 않는 컴퓨터 전체의 설정**을 다룬다. 설치된 하드웨어·소프트웨어와 운영체제의 시스템 설정 정보가 여기에 포함되므로 지문의 설명과 일치한다.

다. O: HKEY_CLASSES_ROOT는 파일 형식과 그 속성, 연결 프로그램 등에 관한 정보를 제공한다. 파일 확장자를 통해 어떤 형식의 파일인지, 어떤 프로그램으로 열지를 연결하므로 **파일 확장자에 대한 정보**를 갖는다는 설명은 타당하다.

라. O: 이 문항에서는 HKEY_USERS가 현재 사용자 한 명에 한정되지 않고 **사용자별 프로필 정보를 모아 다루는 키**라는 취지에서 인정한다. 다만 엄밀히는 현재 로드된 사용자 프로필들이 포함되며, 등록된 모든 사용자의 프로필이 항상 로드되어 있다는 뜻은 아니다. HKEY_CURRENT_USER는 이 중 현재 사용자의 설정에 접근하도록 연결된다.

이 문항의 채점 기준에서는 나·다·라를 인정하므로 옳은 설명은 3개이며, ③의 '3개'에 해당한다.

NoteBase

문 9. 쿠키(Cookie)에 관한 설명 중 옳지 않은 것은?

① 쿠키는 사용자가 인터넷 웹 사이트에 방문할 때 생기는 8KB 이상의 파일을 말한다.

② 쿠키는 유효기간, 패스, 도메인 등의 내용을 포함하고 있다.

③ 사용자가 웹 사이트에 방문하면 웹 사이트는 사용자의 컴퓨터에 쿠키를 만든다.

④ 쿠키는 단순히 정보를 담고 있는 텍스트 파일이기 때문에 바이러스를 전파할 수는 없다.

정답 1번

간단한 해설

쿠키는 브라우저가 저장·전송하는 소량의 상태 데이터이며, **8KB 이상의 파일로 정의되지 않는다**. 쿠키가 담아야 하는 최소 크기가 정해져 있는 것도 아니다.

선지별 해설

① X. 쿠키는 사이트가 로그인 상태나 이용 설정 등을 유지하기 위해 브라우저에 저장하는 작은 이름·값 데이터이다. **8KB 이상이어야 한다는 최소 크기 조건은 없다**. 표준의 쿠키당 4096바이트 지원 권고도 브라우저의 처리 능력에 관한 것이지 실제 쿠키가 그만큼 커야 한다는 뜻이 아니다. 저장 가능한 크기는 브라우저 구현의 제한을 받는다.

② O. 쿠키에는 이름과 값 외에 만료 시각이나 유지 기간, 적용할 도메인과 경로 등의 속성을 설정할 수 있다. 다만 모든 속성을 매번 명시해야 하는 것은 아니며, 만료 관련 속성이 없는 세션 쿠키도 있다.

③ O. 웹 서버는 응답의 Set-Cookie 헤더 등으로 쿠키 저장을 요청하고, 브라우저는 이를 사용자의 기기에 저장·관리한다. 이후 조건에 맞는 요청에 쿠키를 함께 보내 상태를 유지한다. 실제 저장 여부는 브라우저의 쿠키 허용 설정 등에 따라 달라질 수 있다.

④ O. 쿠키 자체는 실행 프로그램이 아니라 데이터이므로, 쿠키를 받았다는 사실만으로 바이러스 코드가 실행되는 것은 아니다. 다만 쿠키에 담긴 세션 정보가 탈취되거나 추적에 악용될 위험은 별개의 문제이다. '텍스트 파일'은 데이터라는 성격을 설명하는 말이며 실제 저장 형식은 브라우저마다 다를 수 있다.

따라서 쿠키를 8KB 이상의 파일로 정의한 ①이 옳지 않다.

NoteBase

문 10. 다음의 명령어를 실행한 파일의 접근 권한으로 옳은 것은?

chmod 733 test.txt

① -rwxrwxrwx

② -rwxr--r--

③ -rwx-wx-wx

④ -rwxr-xr-x

정답 3번

간단한 해설

권한값 733은 소유자·그룹·기타 사용자의 순서로 해석한다. **7은 rwx, 3은 읽기 없이 쓰기·실행만 허용하는 -wx**이므로 세 권한 묶음은 rwx, -wx, -wx가 된다.

대응 관계 해설

chmod 733 test.txt는 test.txt의 접근 권한을 숫자 모드 733으로 설정하는 명령이다. 세 자리는 왼쪽부터 소유자, 파일의 그룹에 속한 사용자, 기타 사용자에 대응한다. 각 자리에서 읽기 r은 4, 쓰기 w는 2, 실행 x는 1이며, 허용된 권한의 값을 더해 표시한다.

소유자 7: 7 = 4 + 2 + 1이므로 읽기·쓰기·실행을 모두 허용한다. 따라서 첫 번째 권한 묶음은 **rwx**이다.

그룹 3: 3 = 2 + 1이므로 쓰기와 실행만 허용한다. 읽기의 값 4가 없으므로 r 위치는 하이픈으로 표시하여 **-wx**가 된다.

기타 사용자 3: 그룹과 같은 값이므로 쓰기와 실행만 허용하고 읽기는 허용하지 않는다. 따라서 마지막 권한 묶음도 **-wx**이다.

선지 맨 앞의 하이픈은 일반 파일이라는 유형 표시이고, 그 뒤의 아홉 글자가 접근 권한이다. 이를 이어 쓰면 -rwx-wx-wx가 되어 ③과 일치한다. chmod의 숫자 모드는 이 권한 부분을 지정하며 파일 유형을 바꾸는 것은 아니다.

NoteBase

문 11. 시스템에 상주하는 프로세스 정보를 알려주는 명령어는?

① df

② file

③ find

④ ps

정답 4번

간단한 해설

ps는 **현재 존재하는 프로세스의 상태 정보**를 조회하는 명령어이다. 프로세스 ID와 실행 명령 등의 정보를 통해 시스템에서 어떤 프로그램이 동작하고 있는지 확인한다.

개념 구분

ps는 실행 중이거나 대기 중인 프로세스 등 선택된 프로세스의 정보를 한 시점의 목록으로 보여 준다. 프로세스 ID, 연결된 터미널, CPU 사용 시간, 실행 명령 등을 확인할 수 있으며, 조회 범위와 출력 항목은 옵션에 따라 달라진다. 계속 갱신되는 화면이 아니라 **조회 시점의 프로세스 정보**를 표시한다는 점이 핵심이다.

df는 파일시스템의 전체 용량, 사용량, 남은 공간 등을 보여 준다. 프로세스 상태가 아니라 저장 공간 사용 현황을 조회한다.

file은 파일의 내용과 형식 정보 등을 조사하여 텍스트·실행 파일·이미지 같은 파일 종류를 판별한다. 실행 중인 프로세스 목록을 알려 주는 명령은 아니다.

find는 디렉터리 구조를 탐색하여 이름·종류·크기 등 주어진 조건에 맞는 파일을 찾는다. 시스템에 존재하는 프로세스를 조회하는 기능과 구분된다.

따라서 프로세스 정보를 알려 주는 명령어는 ④ ps이다.

NoteBase

문 12. 다음 괄호 안에 알맞은 것은?

리눅스 시스템에서 관리자(root) 권한이 필요 없는 프로그램에 소유자가 관리자(root)로 되어 있으면서 ( )가 설정된 경우에는 시스템의 보안에 허점을 초래할 수 있다. 실제로 이것이 설정된 파일은 백도어 및 버퍼 오버플로우 등 여러 공격에 이용된다.

① SetGID

② SetUID

③ Sticky Bit

④ umask

정답 2번

간단한 해설

SetUID는 실행 파일의 소유자 권한으로 프로그램이 동작하게 하는 특수 권한이다. root 소유 파일에 불필요하게 설정하면 프로그램의 결함이 관리자 권한 악용으로 이어질 수 있다.

빈칸별 해설

빈칸에는 **SetUID**가 들어간다. 실행 파일에 SetUID가 설정되어 효력이 적용되면, 실행한 프로세스의 유효 사용자 ID가 파일 소유자의 ID로 바뀐다. 따라서 소유자가 root인 실행 파일은 일반 사용자가 실행하더라도 root 권한으로 동작할 수 있다.

관리자 권한이 필요 없는 프로그램에 이 속성을 부여하면 **불필요한 특권**을 주게 된다. 그 프로그램의 취약점이나 악성 기능이 악용되면 높은 권한으로 피해가 확대될 수 있으므로, 지문의 백도어·버퍼 오버플로우 위험과 연결된다. SetUID가 설정되었다는 사실만으로 모든 파일에 취약점이 존재한다는 뜻은 아니다.

SetGID는 실행 시 유효 **그룹 ID**와 관련된다. 실행 파일의 소유 그룹 권한을 사용하는 기능이므로, 소유 사용자가 root라는 단서에 직접 대응하는 SetUID와 구별한다.

Sticky Bit는 디렉터리 안의 파일 삭제·이름 변경을 파일 소유자, 디렉터리 소유자 또는 특권 프로세스로 제한하는 데 쓰인다. 실행 프로그램에 파일 소유자의 사용자 권한을 부여하는 기능은 아니다.

umask는 새 파일이나 디렉터리를 만들 때 허용할 접근 권한을 제한하는 마스크이다. 실행 시 사용자 ID를 root로 바꾸는 속성이 아니다.

따라서 괄호에 알맞은 것은 SetUID인 ②이다.

NoteBase

문 13. 악성코드 중 자기복제 기능은 없지만, 다른 프로그램으로 위장하여 공격하는 악성코드는?

① 바이러스(Virus)

② 웜(Worm)

③ 님다(Nimda)

④ 트로이 목마(Trojan Horse)

정답 4번

간단한 해설

트로이 목마는 **스스로 복제하지 않고 정상 프로그램처럼 위장**하여 악의적인 기능을 수행한다. 자기복제를 통해 감염·전파하는 바이러스나 웜과 구별된다.

개념 구분

판단 기준은 단순히 다른 프로그램처럼 보이는지가 아니라 **자기복제 기능이 없으면서 정상 프로그램으로 위장**한다는 두 조건의 결합이다.

① 바이러스는 다른 프로그램이나 파일 등의 숙주에 자신의 코드를 삽입하여 감염·복제하는 악성코드이다. 자기복제 기능이 없다는 조건과 맞지 않는다.

② 웜은 스스로 복제하여 다른 시스템으로 전파할 수 있는 악성코드이다. 바이러스처럼 반드시 다른 프로그램에 붙어 있어야 하는 것은 아니며, 네트워크 등의 전파 경로를 이용한다.

③ Nimda는 이메일, 웹 취약점, 파일 공유 등 여러 경로를 이용해 복제·전파하는 웜 계열 악성코드이다. 다른 악성 기능을 함께 수행할 수 있더라도 자기복제하지 않는 악성코드라는 조건에는 해당하지 않는다.

④ 트로이 목마는 정상적이거나 유용한 프로그램처럼 가장하지만 실행되면 숨겨진 악의적 동작을 수행하는 악성코드이다. 이 분류의 핵심은 자체 복제에 의한 전파가 아니라 위장과 기만으로 사용자가 실행하도록 유도한다는 점이다.

따라서 두 조건에 해당하는 것은 ④ 트로이 목마이다.

NoteBase

문 14. OSI 7 계층 중 계층과 데이터 전송단위가 바르게 짝지어진 것은?

① Application - Packet

② Transport - Segment

③ Network - Frame

④ Data Link - Data

정답 2번

간단한 해설

전송 계층의 대표적인 데이터 전송단위는 **세그먼트(Segment)**이다. 계층별 대응에서 네트워크 계층은 패킷, 데이터 링크 계층은 프레임으로 구별한다.

선지별 해설

각 계층은 상위 계층에서 받은 데이터에 자기 계층의 제어 정보를 붙여 전달하며, 이를 캡슐화라고 한다. 이 문제는 이러한 계층별 전송단위의 대표 명칭을 묻는다.

① X: 응용 계층(Application)의 전송단위는 일반적으로 **데이터(Data)**라고 부른다. 응용 프로그램이 교환하려는 내용을 처리하는 계층이며, 패킷(Packet)은 네트워크 계층의 전송단위와 연결된다.

② O: 전송 계층(Transport)의 대표 전송단위는 **세그먼트(Segment)**이다. 예를 들어 TCP는 응용 데이터를 나누고 전송 계층 헤더를 붙여 세그먼트로 전달한다. 따라서 Transport와 Segment의 연결이 성립한다.

③ X: 네트워크 계층(Network)의 전송단위는 **패킷(Packet)**이다. 이 계층은 논리 주소를 이용하여 목적지까지 데이터를 전달할 경로를 다룬다. 프레임(Frame)은 그 아래 데이터 링크 계층의 전송단위이다.

④ X: 데이터 링크 계층(Data Link)의 전송단위는 **프레임(Frame)**이다. 상위 계층의 패킷을 하나의 링크에서 전달할 수 있도록 링크 계층의 헤더 등으로 감싼다. Data는 이 문제의 대표 명칭 대응에서 응용 계층 등 상위 계층과 연결된다.

NoteBase

문 15. 다음 무선랜 보안에 관한 설명 중 옳은 것은 모두 몇 개인가?

가. TKIP는 64비트의 확장된 길이의 초기벡터(IV)를 사용한다.
나. WEP 인증은 양방향 인증을 제공하여 보안에 강하다.
다. WPA는 RADIUS, Kerberos 등과 같은 다른 인증서버와 호환 가능하다.
라. WPA2는 2세대 WPA로써, RSA에 기반을 둔 CCMP 암호화 방식을 사용한다.
마. EAP 인증 방식은 WPA에서는 사용할 수 없고, WPA2 이후부터 사용 가능하다.

① 1개
② 2개
③ 3개
④ 4개

정답 1번

간단한 해설

WPA-Enterprise는 802.1X/EAP를 통해 외부 인증 체계와 연동할 수 있으므로 **다만 옳다**. TKIP의 IV는 48비트이고 CCMP는 AES 기반이며, EAP는 WPA에서도 사용한다. 따라서 옳은 것은 **1개로** ①이다.

NoteBase

보기별 해설

가. X: 'TKIP'는 WEP의 24비트 초기벡터를 **48비트로 확장**한다. 패킷별로 증가하는 시퀀스 카운터와 키 혼합을 이용하여 키스트림 재사용과 재전송 공격을 줄인다. 64비트는 TKIP의 메시지 무결성 코드인 'Michael MIC'의 길이와 구별해야 한다.

나. X: WEP의 기본 인증은 접속 단말이 정당한 액세스 포인트인지까지 검증하는 안전한 **상호 인증을 보장하지 않는다**. 공유키 인증도 평문 도전값과 그 암호문이 노출되는 문제가 있으며, WEP 자체에는 짧은 IV와 RC4 키 사용 방식 등의 취약점이 있다. 따라서 양방향 인증으로 보안이 강하다는 설명은 틀리다.

다. O: 'WPA-Enterprise'는 802.1X/EAP를 사용하며, 액세스 포인트가 RADIUS 인증 서버와 연동할 수 있다. EAP의 확장 가능한 인증 구조와 서버의 연동 기능을 통해 Kerberos 같은 기존 인증 체계를 활용하는 구성도 가능하다. 이는 **지원하는 인증 방식과 서버 구성이 갖추어진 경우의 연동 가능성**을 뜻하며, 모든 WPA 장비가 Kerberos를 직접 구현한다는 뜻은 아니다.

라. X: 'WPA2'의 대표적인 데이터 보호 방식인 'CCMP'는 **AES를 기반**으로 한다. 카운터 모드로 기밀성을 제공하고 CBC-MAC으로 무결성과 데이터 출처 인증을 제공한다. RSA는 공개키 암호 알고리즘으로, CCMP의 기반 암호가 아니다.

마. X: EAP는 여러 인증 방법을 운반하는 인증 프레임워크이며, **WPA와 WPA2의 Enterprise 방식 모두**에서 사용할 수 있다. WPA2부터 처음 지원된다는 주장은 틀리다. 사전 공유키를 쓰는 Personal 방식과 구별해야 한다.

옳은 지문은 다 하나이다. 따라서 '1개'인 ①이 정답이며, ②~④는 옳은 지문의 개수와 맞지 않는다.

NoteBase

문 16. 다음 중 DoS 공격의 대응 방안으로 옳은 것은 모두 몇 개인가?

가. UDP Flooding 공격 : 불필요한 서비스를 비활성화 한다.
나. SYN Flooding 공격 : 공격 인정 시간 내에 SYN 개수가 공격 인정 횟수 이상인 IP 주소를 소스로 해서 들어오는 트래픽을 차단한다.
다. Ping of death 공격 : 반복적으로 들어오는 일정 수 이상의 ICMP 패킷을 무시하도록 설정한다.
라. LAND 공격 : 다른 네트워크로부터 자신의 네트워크로 들어오는 IP 브로드캐스트 패킷을 차단한다.

① 1개
② 2개
③ 3개
④ 4개

정답 3번

간단한 해설

LAND 공격은 **출발지와 목적지가 동일한 비정상 패킷**을 차단하여 대응한다. 외부에서 들어오는 IP 브로드캐스트 패킷의 차단은 여러 호스트의 응답을 증폭시키는 Smurf 공격에 대응하는 방법이다.

NoteBase

보기별 해설

가. O: UDP Flooding은 대량의 UDP 패킷으로 네트워크 대역폭이나 시스템의 처리 자원을 소모시키는 공격이다. 불필요한 UDP 서비스를 비활성화하면 공격에 노출된 서비스와 불필요한 응답 처리를 줄일 수 있다. 다만 이것만으로 회선의 대역폭 소진까지 모두 막는 것은 아니다.

나. O: SYN Flooding은 TCP 연결 설정 요청을 대량으로 보내 연결이 완성되지 않은 상태를 누적시키고 서버 자원을 소모시킨다. 일정 시간 동안의 SYN 요청 수를 기준으로 공격 출발지 IP를 탐지하여 그 트래픽을 차단하면 **과도한 연결 요청**을 억제할 수 있다. 출발지 위조나 분산 공격에는 추가적인 방어가 필요하다.

다. O: 반복적으로 들어오는 ICMP 패킷 중 임계치를 넘는 것을 버리면 처리해야 할 공격 트래픽을 줄일 수 있으므로 DoS 완화 방안이 된다. 다만 Ping of death의 핵심은 비정상적으로 큰 패킷의 재조립 과정에서 취약점을 유발하는 것이므로, **수신량 제한만으로 취약점이 제거되는 것은 아니다**. 비정상 패킷 검사·차단과 관련 취약점의 보완도 필요하다.

라. X: 외부에서 유입되는 IP 브로드캐스트 패킷을 차단하는 것은 네트워크 내 여러 호스트가 응답하도록 만드는 Smurf 공격의 증폭을 막는 대응이다. LAND 공격은 출발지와 목적지 주소·포트를 같게 조작한 패킷을 이용하므로, **출발지와 목적지가 같은 비정상 패킷을 차단**하는 것이 대응의 핵심이다.

옳은 보기는 가·나·다의 3개이므로 ③에 해당한다.

NoteBase

문 17. 스니핑(Sniffing) 공격을 수행하는 스니퍼를 탐지하는 기법에 관한 설명 중 옳은 것은 모두 몇 개인가?

가. 유인(Decoy)을 이용한 탐지: 관리자가 가짜 ID와 패스워드를 네트워크에 계속 뿌리고, 공격자가 이 ID와 패스워드를 이용하여 접속을 시도할 때 스니퍼를 탐지하는 방법
나. ARP를 이용한 탐지: 정상적인 ARP Request를 보냈을 때 위조된 ARP Response를 되돌려 보내는 것을 모니터링하여 탐지하는 방법
다. ping을 이용한 탐지: 네트워크에 존재하지 않는 MAC 주소로 위장하여 ping을 보냈을 때, ICMP Echo Reply를 되돌려 보내는지를 모니터링하여 탐지하는 방법
라. ARP Watch를 이용한 탐지: MAC 주소와 IP 주소의 매칭 값을 초기에 저장하고 ARP 트래픽을 모니터링하여, 이를 변하게 하는 패킷이 탐지되면 알려주는 툴인 ARP Watch를 이용하여 탐지하는 방법

① 1개
② 2개
③ 3개
④ 4개

정답 3번

간단한 해설

ARP·ping 기반 스니퍼 탐지는 정상적으로 받지 않아야 할 프레임에 응답하는지를 살피는 방식이다. 유인 계정의 사용과 IP·MAC 대응 변화도 도청을 의심할 단서가 된다.

NoteBase

보기별 해설

가. (O) 유인 탐지는 **미끼로 흘린 인증정보의 사용**을 관찰한다. 정상 사용자가 이용하지 않는 가짜 ID·패스워드를 공격자가 가로채 접속에 쓰면, 그 시도가 도청을 의심할 단서가 된다. 조용히 수집만 하는 행위 자체를 항상 발견하는 방식은 아니다.

나. (X) 스니퍼를 찾는 ARP 탐지는 일반적인 ARP 요청에 위조 응답이 오는지를 확인하는 방식이 아니다. **대상에게 정상 수신되지 않아야 할 목적지 MAC 주소**로 ARP 요청을 보내고, 이를 받아 응답하는 특이 동작을 통해 무차별 모드 사용을 의심한다. 위조된 ARP 응답을 감시하는 것과, 비정상 목적지 프레임에 대한 응답으로 스니퍼를 탐지하는 것은 구별해야 한다.

다. (O) ping 탐지도 **목적지 MAC 주소와 대상 IP 주소를 다르게 취급**하는 원리를 이용한다. 대상의 IP 주소를 지정하되 정상적으로 수신하지 않을 MAC 주소로 프레임을 보내고, ICMP Echo Reply가 오는지를 살핀다. 무차별 모드와 운영체제의 패킷 처리 방식에 따라 응답할 수 있으므로 모든 스니퍼에 통하는 확정 검사는 아니다.

라. (O) ARP Watch는 **IP·MAC 주소 대응 관계의 변화**를 감시한다. 이전에 관찰한 대응과 ARP 트래픽을 비교하여 변경을 알리므로, ARP 스푸핑을 이용한 도청의 징후를 발견하는 데 활용할 수 있다. 정상적인 장비 교체도 변경을 일으킬 수 있으므로 경고만으로 공격을 확정하지 않는다.

따라서 옳은 보기는 가·다·라의 3개이므로 ③이다.

NoteBase

문 18. 다음 설명에 해당하는 공격은?

> 개인 단체, 정치 단체, 국가, 산업체 등 목표 조직을 타깃으로 하여 다양한 보안 위협을 만들어 침해에 성공해 정보를 유출하거나 장기간의 접속 권한을 획득하기 위해 또는 장기간의 접근을 위해 지속적으로 수행되는 공격이다.

① APT(Advanced Persistent Threat)

② DDoS(Distributed Denial of Service)

③ Ransomware

④ Zero-Day Attack

정답 1번

간단한 해설

특정 조직을 표적으로 삼아 장기간 지속적으로 접근을 유지하고 정보를 유출하려는 특징은 APT의 핵심이다.
하나의 취약점이나 일회성 공격 방식이 아니라 목표 달성을 위한 지속적인 공격 활동을 뜻한다.

NoteBase

개념 구분

지문에는 목표 조직을 정해 공격한다는 표적성, 다양한 보안 위협을 활용한다는 수단의 복합성, 장기간 접속 권한을 유지한다는 지속성이 함께 제시되어 있다. 이 단서들을 묶어서 공격의 성격을 판단한다.

APT(Advanced Persistent Threat): **특정 표적에 대한 지속적인 침투와 접근 유지**를 특징으로 하는 지능형 지속 위협이다. 공격자는 여러 수단을 활용하고 방어에 맞추어 방법을 바꾸면서 정보 유출 등 장기적인 목적을 추구한다. 지문의 '목표 조직', '장기간의 접속 권한', '지속적으로 수행'이라는 내용이 모두 이에 연결된다.

DDoS(Distributed Denial of Service): 여러 출발지에서 공격 트래픽이나 요청을 보내 자원을 소모시키고, 정당한 사용자의 **서비스 이용을 방해**하는 공격이다. 장기간 은밀한 접근을 유지하여 정보를 유출한다는 설명보다는 가용성을 떨어뜨리는 데 초점이 있다.

Ransomware: 파일을 암호화하거나 시스템 사용을 제한한 뒤 복구를 대가로 금전을 요구하는 악성코드이다. 지문에는 이러한 복구 대가 요구가 없으며, 중심 단서는 장기적인 표적 침투와 접근 유지이다.

Zero-Day Attack: 알려지지 않았거나 대응 패치가 마련되지 않은 취약점을 악용하는 공격이다. **취약점의 공개·대응 시점**과 관련된 개념이며, 공격이 특정 조직을 상대로 장기간 지속된다는 뜻은 아니다. APT에서 제로데이 공격을 수단으로 사용할 수는 있지만 두 용어가 같은 범위의 개념은 아니다.

따라서 지문의 설명은 APT이며, ①과 연결된다.

NoteBase

문 19. 다음 중 DDoS 공격에 관한 설명으로 옳은 것은 모두 몇 개인가?

가. DDoS 공격에 사용된 좀비 PC는 악성코드의 흔적을 지우기 위해 스스로 하드디스크를 손상시킬 수도 있다.
나. DDoS 공격의 구성 요소로는 공격자, 마스터, 핸들러 프로그램, 에이전트 등이 있다.
다. 트리누(Trinoo), TFN 등이 대표적인 공격 유형이다.
라. DDoS 공격에서 악성코드에 감염된 좀비 PC끼리 형성된 네트워크를 봇넷(Botnet)이라고 한다.
마. 라우터의 Egress 필터링 기능을 이용하여 대응할 수 있다.

① 2개
② 3개
③ 4개
④ 5개

정답 4번

간단한 해설

DDoS는 여러 감염 호스트가 함께 공격하는 방식으로, 제어 프로그램·봇넷·공격 도구가 사용되고 감염 PC의 데이터 파괴가 동반될 수도 있다. Egress 필터링도 내부에서 나가는 공격 트래픽을 줄이는 대책이므로 **가~마 모두 옳아 5개인** ④이다.

NoteBase

보기별 해설

가. O: DDoS에 동원된 좀비 PC의 악성코드에 **자기 삭제나 디스크 데이터 파괴 기능**이 포함될 수 있다. 공격 뒤 분석·추적에 필요한 흔적을 없애기 위해 파일이나 부팅 정보를 손상시키는 방식이다. 모든 좀비 PC가 반드시 파괴 동작을 수행한다는 뜻은 아니며, 디스크의 물리적 부품이 스스로 부서진다는 뜻도 아니다.

나. O: 전통적인 DDoS의 계층적 제어 구조에는 공격자, 명령을 전달하는 마스터와 그 위에서 실행되는 핸들러 프로그램, 실제 공격 트래픽을 만드는 에이전트가 있다. **공격자 → 마스터의 핸들러 → 다수 에이전트 → 피해 시스템**의 관계로 이해할 수 있다. 구현에 따라 제어 구조는 달라질 수 있다.

다. O: 'Trinoo'와 'TFN'은 다수의 감염 시스템을 제어하여 공격 트래픽을 발생시키는 대표적인 **DDoS 공격 도구 계열**이다. 지문의 '공격 유형'은 이러한 도구와 그 공격 방식을 가리키는 표현이다. 이들이 사용하는 구체적인 트래픽 방식과 도구의 이름은 구별한다.

라. O: 악성코드에 감염되어 공격자의 명령을 받는 봇들이 이루는 네트워크를 **'봇넷'**이라고 한다. 그 구성 호스트를 좀비 PC라고 부를 수 있으며, 다수의 봇이 함께 DDoS 공격에 동원된다. 봇넷은 중앙 제어형일 수도 있고 P2P형일 수도 있으므로 모든 좀비 PC가 서로 직접 연결되어 있어야 하는 것은 아니다.

마. O: 'Egress 필터링'은 내부 네트워크에서 외부로 나가는 트래픽을 통제한다. 경계 라우터에서 허용되지 않은 출발지 주소를 사용한 패킷이나 비정상적인 송신 트래픽을 차단하면 **내부 좀비 PC가 외부 공격에 참여하는 것을 줄일 수 있다**. 실제 출발지 주소를 쓰는 공격이나 외부에서 유입되는 모든 DDoS까지 이것만으로 막는 것은 아니다.

가·나·다·라·마의 다섯 지문이 모두 옳다. 따라서 정답은 '5개'인 ④이며, ①~③의 개수는 이에 맞지 않는다.

NoteBase

문 20. 다음 중 세션 하이재킹(Session Hijacking)에 관한 설명으로 옳은 것은 모두 몇 개인가?

가. 정당한 절차로 인증을 받은 사용자의 세션을 가로채는 공격이다.
나. 패킷의 유실과 재전송이 증가해 서버와의 응답시간이 길어진다.
다. 공격자는 클라이언트와 서버 사이의 기존 세션을 동기화시킨다.
라. 암호화, 지속적인 인증 등을 통해 대응할 수 있다.

① 1개
② 2개
③ 3개
④ 4개

정답 3번

간단한 해설

이 문항의 TCP 세션 탈취에서는 기존 클라이언트와 서버를 **비동기화**시키므로 '동기화시킨다'는 다가 틀리다. 인증된 세션의 탈취, 통신 지연 가능성, 암호화와 지속적인 인증을 통한 대응을 설명한 가·나·라는 옳다.

NoteBase

보기별 해설

가. O. 세션 하이재킹은 정상 사용자가 이미 인증받아 사용 중인 세션을 탈취하여 그 사용자처럼 통신하거나 서비스를 이용하는 공격이다. 인증 절차를 처음부터 통과하지 않고도 인증 이후의 연결이나 세션 식별자를 악용할 수 있다는 점이 핵심이다.

나. O. TCP 세션의 순서 번호와 확인 응답 번호가 어긋나는 비동기화 방식에서는 정상 패킷이 수신 측의 기대 범위와 맞지 않아 버려지고 재전송이 늘 수 있다. 확인 응답이 반복되는 ACK 폭풍까지 생기면 네트워크 부하가 커져 응답이 지연된다. 이는 이 문항의 TCP 세션 탈취 문맥에서 설명하는 현상이며, 쿠키 탈취 등 모든 형태의 세션 하이재킹에서 반드시 나타나는 증상은 아니다.

다. X. 기존 클라이언트와 서버의 세션을 동기화시키는 것이 아니라 **기존 양 끝의 통신 상태를 비동기화**시키는 것이 해당 공격 방식의 특징이다. 공격자가 위조 패킷의 순서 번호를 수신 측이 받아들일 값에 맞추는 것과, 원래 클라이언트·서버 사이의 동기 상태를 유지하는 것은 다르다.

라. O. 인증된 암호화 통신으로 도청·변조를 막고, 세션의 유효성과 사용자 상태를 계속 확인하며 필요한 시점에 재인증하는 방식으로 위험을 줄일 수 있다. 웹에서는 로그인 순간뿐 아니라 세션 전체에 TLS를 적용하는 것이 중요하다. 다만 암호화만으로 단말에서 유출된 세션 토큰의 재사용까지 모두 막는 것은 아니므로 세션 관리와 인증 통제를 함께 적용한다.

따라서 옳은 보기는 가·나·라의 3개이므로 정답은 ③이다.

NoteBase

문 21. 다음 설명에 해당하는 기술은?

과거 IP 관리 시스템에서 발전한 솔루션을 말한다. 이 기술은 클라이언트가 네트워크에 접근하는 것을 통제할 뿐만 아니라, IP가 무질서하게 사용되는 것을 막아, 가용 IP를 쉽게 확인할 수 있게 해주고 IP 충돌로 인한 문제를 막아준다.

① NAT(Network Address Translation)

② NAC(Network Access Control)

③ VLAN(Virtual Local Area Network)

④ VPN(Virtual Private Network)

정답 2번

간단한 해설

NAC는 사용자·단말의 네트워크 접근을 정책에 따라 통제하는 기술이다. 지문은 여기에 IP 사용 현황과 충돌 관리 기능을 결합한 솔루션을 설명한다.

핵심 풀이

결정적인 단서는 **클라이언트의 네트워크 접근을 통제**한다는 점이다. NAC는 접속하는 사용자·단말을 식별하고, 정해진 정책에 따라 접근 허용·제한·격리 등을 적용하는 네트워크 접근 제어 기술이다.

지문은 IP 관리 기능에서 발전한 NAC 솔루션을 설명한다. IP 사용 현황을 관리하여 가용 주소를 확인하고 무단 사용이나 주소 충돌을 줄이는 기능을 접근 통제와 함께 제공한다는 뜻이다. **IP 관리만이 아니라 접속 통제까지 한다**는 점을 함께 읽어야 한다.

NAT는 내부·외부 통신에서 IP 주소 등을 변환하는 기술이다. IP라는 용어가 등장하더라도, 사용자나 단말의 접속 자격을 심사하는 NAC와는 기능이 다르다.

VLAN은 물리적인 연결과 별개로 네트워크를 논리적인 브로드캐스트 영역으로 나누는 기술이다. NAC가 접근 정책을 적용할 때 VLAN 분리를 활용할 수는 있지만, 두 기술이 같은 개념은 아니다.

VPN은 공중망 등을 통해 사설망처럼 통신할 수 있도록 논리적인 연결을 제공하는 기술이다. 지문의 중심인 단말 접근 통제와 IP 사용 관리를 가리키는 명칭은 아니다.

따라서 설명에 해당하는 기술은 NAC인 ②이다.

NoteBase

문 22. IPS(Intrusion Prevention System)와 IDS(Intrusion Detection System)에 관한 설명 중 옳지 않은 것은?

① IPS는 침입 공격에 대하여 방지하는 것을 목표로 하는 시스템이다.

② IPS는 호스트의 IP 주소, 포트번호, 사용자 인증에 기반을 두고 외부 침입을 차단한다.

③ IDS는 침입 공격에 대하여 탐지하는 것을 목표로 하는 시스템이다.

④ IDS는 해커의 공격이나 정보유출이 탐지되면 해당 기능을 차단하도록 되어 있다.

정답 4번

간단한 해설

IDS의 기본 역할은 침입 징후를 **탐지하여 기록·경보**하는 것이고, 탐지된 공격을 직접 차단하는 기능은 IPS의 핵심이다. 따라서 IDS가 탐지 즉시 해당 기능을 차단한다고 일반화한 **④가 옳지 않다**.

선지별 해설

① O: 'IPS'는 침입 탐지 결과를 바탕으로 공격 패킷을 폐기하거나 연결을 끊는 등 **공격을 차단·방지하는 것**을 목표로 한다. 네트워크형 IPS는 보통 통신 경로에 설치되어 지나가는 트래픽을 검사한다. 예방을 목표로 한다는 말이 모든 공격을 반드시 막는다는 뜻은 아니다.

② O: IPS는 공격 관련 IP 주소와 포트번호를 이용하여 차단 대상을 정할 수 있고, 사용자 인증 정보와 연계되는 구성에서는 사용자별 접근도 통제할 수 있다. 여기서 열거한 정보는 **정책 적용과 차단에 활용할 수 있는 기준**이다. IPS의 탐지가 이 정보에만 의존한다는 뜻은 아니며, 공격 서명·이상행위·프로토콜 분석 등도 활용한다. IP·포트 중심의 단순 허용·차단은 방화벽에서도 제공하는 기능이다.

③ O: 'IDS'는 네트워크 트래픽이나 호스트의 활동을 관찰하여 침입 징후를 **탐지하고 기록·경보하는 것**을 주된 목표로 한다. 알려진 공격 패턴과의 일치 여부나 평소 행동과의 차이 등을 분석하여 관리자에게 이상 상황을 알린다.

④ X: 공격이나 정보유출을 탐지했다는 이유만으로 **해당 활동을 자동 차단하는 것이 기본 IDS의 역할은 아니다**. 탐지에 더해 공격을 중단시키는 기능은 IPS의 핵심 차이이다. IDS가 다른 방화벽·대응 장비와 연동하여 차단을 유도하는 구성은 가능하지만, 그러한 추가 연동을 일반적인 IDS 자체의 필수 기능으로 설명하면 안 된다.

이 문항은 기본 기능을 기준으로 IDS와 IPS를 구분한다. IDS에 직접 차단 기능을 일반적으로 부여한 ④가 인정 정답과 대응한다.

NoteBase

문 23. IPSec의 프로토콜 구조로 옳지 않은 것은?

① Encapsulating Security Payload

② Security Association

③ Internet Group Management Protocol

④ Authentication Header

정답 3번

간단한 해설

IGMP는 IPv4 멀티캐스트 그룹의 가입 정보를 관리하는 프로토콜이다. IPSec의 패킷 보호 프로토콜인 AH·ESP나 보안 매개변수를 관리하는 SA와는 기능이 다르다.

개념 구분

IPSec은 IP 계층에서 통신을 보호하는 보안 구조이다. 실제 패킷을 보호하는 AH·ESP와, 이들을 적용할 때 사용할 키·알고리즘 등의 정보를 담는 보안 연관 SA를 구별하여 이해해야 한다.

Encapsulating Security Payload(ESP): IPSec의 패킷 보호 프로토콜이다. 암호화 기능을 사용하면 **데이터의 기밀성**을 제공하며, 선택된 구성에 따라 무결성·데이터 출처 인증과 재전송 방지 기능도 제공한다.

Security Association(SA): 통신 보호에 필요한 **알고리즘·키·수명 등의 보안 매개변수**를 연결하여 관리하는 보안 연관이다. AH나 ESP와 같은 패킷 형식의 이름은 아니지만, IPSec의 동작을 규정하는 핵심 구성 요소이므로 이 문제의 IPSec 구조에 포함된다.

Internet Group Management Protocol(IGMP): IPv4 호스트가 자신이 가입하려는 **멀티캐스트 그룹 정보를 인접한 멀티캐스트 라우터에 알리는** 프로토콜이다. 그룹 수신자 관리가 목적이며, IP 패킷을 인증·암호화하거나 IPSec 보안 연관을 설정하는 구성 요소가 아니다.

Authentication Header(AH): IPSec에서 패킷의 무결성과 데이터 출처 인증을 제공하는 프로토콜이다. 순서 번호 검사를 통한 재전송 방지도 지원하지만, 데이터 본문을 암호화하여 기밀성을 제공하지는 않는다.

따라서 IPSec 구조의 구성 요소로 적절하지 않은 것은 IGMP이며, ③과 연결된다.

NoteBase

문 24. 다음 중 네트워크 스캔(Network Scan)에 관한 설명으로 옳은 것은 모두 몇 개인가?

가. TCP FIN 스캔은 TCP 헤더 내에 FIN 플래그(flag)를 설정하여 전송하는 방식으로 Half-open 스캔 방식에 속한다.
나. TCP Full Open 스캔은 포트가 열려 있는 경우, 대상시스템으로부터 SYN+ACK 패킷을 수신하면 RST 패킷을 보내 연결 과정을 중단한다.
다. XMAS 스캔은 스텔스(Stealth) 스캔에 속한다.
라. XMAS 스캔은 패킷의 모든 플래그를 NULL로 설정하여 전송한다.
마. NULL 스캔의 대상이 포트가 닫혀 있을 경우 RST 패킷이 돌아온다.

① 1개
② 2개
③ 3개
④ 4개

정답 2번

간단한 해설

TCP Half-open 스캔은 **SYN+ACK를 받은 뒤 RST로 연결 설정을 중단**하는 방식이다. Full Open 스캔은 ACK를 보내 연결을 완성하며, FIN·NULL·XMAS 스캔은 전송하는 플래그 조합으로 구별한다.

NoteBase

보기별 해설

가. X: FIN 플래그만 설정하여 전송한다는 부분은 맞지만, 이를 Half-open 스캔으로 분류한 부분이 틀렸다. FIN 스캔은 정상적인 연결 설정을 시작하지 않고 포트의 응답 차이를 이용하는 스텔스 스캔이다. 통상 Half-open 스캔은 **TCP SYN 스캔**을 가리킨다.

나. X: SYN+ACK를 받은 뒤 RST를 보내 연결 설정을 중단하는 것은 Half-open 스캔이다. Full Open 스캔은 SYN → SYN+ACK → ACK의 **3방향 핸드셰이크를 완성**하여 연결 성립 여부를 확인한다.

다. O: XMAS 스캔은 정상적인 TCP 연결을 완성하지 않고 특수한 플래그 조합에 대한 응답으로 포트 상태를 추정하므로 스텔스 스캔에 속한다. 다만 '스텔스'라는 명칭이 탐지 장비에 절대로 발견되지 않는다는 뜻은 아니다.

라. X: 플래그를 모두 0으로 비워 두는 것은 NULL 스캔이다. XMAS 스캔은 통상 **FIN·PSH·URG 플래그를 설정**하여 전송한다.

마. O: NULL 스캔은 TCP 플래그가 모두 0인 패킷을 보낸다. 표준적인 TCP 동작을 따르는 시스템에서 닫힌 포트는 이에 RST로 응답한다. 열린 포트는 통상 응답하지 않지만, 필터링으로도 무응답이 생기므로 무응답만으로 열림을 단정할 수는 없다.

옳은 보기는 다·마의 2개이므로 ②에 해당한다.

NoteBase

문 25. 메일의 헤더 정보, 제목, 메시지 내용의 특정 단어 및 문장 패턴을 검색하여 스팸 메일을 탐지 및 차단하는 기술적 대응 방안은?

① 콘텐츠 필터링
② 발송량 기준 차단
③ 송신자 필터링
④ 시간대별 차단

정답 1번

간단한 해설

메일에 담긴 특정 단어나 문장 패턴을 검사하는 방식은 콘텐츠 필터링이다. 판단 기준이 발송자·발송량·시간대가 아니라 메일의 정보 내용에 있다.

핵심 풀이

지문은 메일의 헤더·제목·본문에서 **특정 단어와 문장 패턴**을 찾아 스팸 여부를 판단한다. 이처럼 메일에 담긴 정보를 규칙이나 패턴과 대조하는 방법이 콘텐츠 필터링이다. 본문만 검사하는 것으로 범위를 좁혀서는 안 된다.

발송량 기준 차단은 일정 시간에 발송되는 메일의 수나 빈도처럼 **발송 규모**를 기준으로 한다. 제목이나 본문의 단어를 해석하는 방식과 구별된다.

송신자 필터링은 보낸 사람의 이메일 주소·도메인·발송 서버 IP 등 **송신자 정보**를 허용·차단 기준과 대조한다. 헤더를 활용할 수는 있지만, 이 문제는 제목과 메시지 내용까지 포함한 단어·문장 패턴 검색을 설명한다.

시간대별 차단은 메일이 발송되거나 유입되는 시간대를 기준으로 차단 여부를 정한다. 특정 문구가 포함되었는지를 검사하는 콘텐츠 필터링과는 판단 기준이 다르다.

따라서 해당하는 방안은 콘텐츠 필터링인 ①이다.

NoteBase

문 26. 다음 설명에 해당하는 DNS 보안 위협은?

보안이 취약한 DNS 서버에 조작된 쿼리를 전송하여 DNS 서버가 저장하고 있는 주소 캐시(Cache) 정보를 위·변조하는 공격이다.
이 공격을 통해 사용자는 자신이 의도하지 않은 다른 사이트로 접속되는 문제가 발생한다.

① DNS Cache Poisoning 공격

② Bind DNS 서비스 방해 공격

③ DNS Spoofing

④ DNS Sinkhole

정답 1번

간단한 해설

DNS 서버의 **캐시에 거짓 주소 정보를 저장**하여 정상 도메인 질의에도 잘못된 주소를 돌려주게 하는 공격은 'DNS Cache Poisoning'이다. 저장된 캐시의 위·변조가 핵심 단서이므로 ①이다.

NoteBase

개념 구분

'DNS 캐시 포이즈닝'의 결정적인 단서는 **DNS 서버가 저장해 둔 주소 캐시의 위·변조**이다. DNS 서버는 한 번 얻은 이름과 주소의 대응 정보를 일정 시간 보관하여 반복 질의에 이용한다. 이 캐시에 거짓 정보가 들어가면 정상 도메인을 질의한 사용자에게도 공격자가 의도한 주소를 응답할 수 있다.

지문의 '조작된 쿼리'는 취약한 서버가 잘못된 정보를 받아들이도록 유도하는 공격 과정을 나타낸다. 핵심은 질의 자체의 존재가 아니라 **위조·오염된 이름 해석 정보가 캐시에 저장되어 이후 응답에 재사용되는 것**이다. 그 결과 사용자는 원래 접속하려던 사이트 대신 다른 사이트로 연결될 수 있다.

'DNS Spoofing'은 DNS 응답이나 이름·주소 대응을 속이는 공격을 넓게 가리키며, 캐시 포이즈닝과 겹쳐 쓰이기도 한다. 다만 위조 응답 하나로 사용자를 속이는 경우까지 모두 캐시 오염을 필요로 하는 것은 아니다. 이 문항처럼 **서버의 저장된 캐시 변조**를 명시하면 'DNS Cache Poisoning'이 더 구체적으로 대응한다.

'Bind DNS 서비스 방해 공격'은 DNS 서버의 자원 소진이나 서비스 장애를 일으켜 이름 해석의 가용성을 저해하는 공격이다. 응답 불가·지연과 잘못된 주소 정보로의 유도는 구별된다.

'DNS Sinkhole'은 보안 대응에서 악성 도메인의 질의를 관리되는 주소로 유도하여 악성 통신을 차단하거나 감염 호스트를 파악하는 기법이다. 지문은 방어 목적의 싱크홀 운용이 아니라 취약한 서버의 캐시를 오염시키는 공격을 설명한다.

따라서 지문의 두 단서인 '주소 캐시 변조'와 '의도하지 않은 사이트로의 접속'에 가장 구체적으로 대응하는 것은 ① DNS Cache Poisoning 공격이다.

NoteBase

문 27. 다음 설명에 해당하는 것은?

응용 프로그램이 실행될 때 일종의 가상머신 안에서 실행되는 것처럼 원래의 운영체제와 완전히 독립되어 실행되는 형태를 말한다 또한, 컴퓨터 메모리에서 애플리케이션 호스트 시스템에 해를 끼치지 않고 작동하는 것이 허락된 보호받는 제한구역을 가리킨다.

① Sandbox

② Bluebox

③ Middlebox

④ Whitebox

정답 1번

간단한 해설

샌드박스는 프로그램을 격리된 제한 환경에서 실행하여 호스트의 파일·메모리·네트워크 등 자원에 대한 접근을 통제한다. 지문의 '보호받는 제한구역'이 이를 가리키는 결정적 단서이다.

NoteBase

개념 구분

지문은 응용 프로그램이 호스트 시스템에 미치는 영향을 제한하도록 실행 환경을 분리하는 방식을 설명한다. 핵심은 단순히 가상머신을 사용하는지 여부가 아니라, 프로그램에 허용한 자원과 권한만 사용하게 하는 격리와 통제이다.

Sandbox: 신뢰하기 어려운 프로그램도 **제한된 권한과 자원 범위 안에서 실행**하게 하는 보호 환경이다. 파일 변경이나 네트워크 접근 등을 통제하여 호스트에 대한 영향을 줄인다. 가상머신으로 구현할 수 있지만, 모든 샌드박스가 별도의 운영체제를 실행하는 완전한 가상머신인 것은 아니다.

Bluebox: 전통적으로 전화망의 제어 신호를 악용하는 데 사용된 장치를 가리킨다. 컴퓨터 응용 프로그램을 안전하게 격리하여 실행하는 제한 환경과는 다른 개념이다.

Middlebox: 통신의 송신자와 수신자 사이에서 일반적인 라우팅 이외의 처리를 수행하는 중간 장치이다. 방화벽이나 NAT 장치 등이 예이며, **네트워크 경로에서의 중간 처리**가 핵심이다.

Whitebox: 내부 구조나 동작을 알고 분석하는 관점에서 쓰이는 용어이다. 예를 들어 화이트박스 테스트는 프로그램 내부의 코드 구조와 실행 경로를 고려하여 검사한다. 지문의 실행 권한 제한·격리를 뜻하는 환경의 명칭은 아니다.

따라서 응용 프로그램을 보호받는 제한구역에서 실행하게 하는 방식은 Sandbox이며, ①과 연결된다.

NoteBase

문 28. 웹 취약점 및 공격에 대한 설명 중 옳지 않은 것은?

① 명령 삽입 취약점 : 클라이언트의 요청을 처리하기 위해 전송 받은 인수에 특정 명령을 실행하는 코드를 포함시켜 웹서버에 전송하는 것

② XSS(Cross Site Scripting) 취약점 : 공격자에 의해 작성된 스크립트가 다른 웹사용자에게 전달되어 수행되는 것

③ CSRF(Cross Site Request Forgery) 취약점 : 브라우저를 통해 디렉터리에 있는 파일과 목록을 나열하는 것

④ SQL Injection 공격 : 데이터베이스와 연동되어 있는 애플리케이션의 입력값을 조작하여 DBMS가 의도되지 않은 결과를 반환하도록 하는 공격 기법

정답 3번

간단한 해설

파일과 디렉터리 목록의 노출은 **디렉터리 리스팅**이다. CSRF는 인증된 사용자의 브라우저를 통해 사용자가 의도하지 않은 요청을 보내게 하는 공격이므로 두 개념을 구별해야 한다.

NoteBase

선지별 해설

① O. 명령 삽입은 외부에서 받은 입력을 운영체제 명령 등에 안전하지 않게 결합할 때, 입력 속 내용이 단순한 데이터가 아니라 실행할 명령으로 해석되는 취약점이다. 요청 인수에 삽입된 명령이 서버 측에서 실행되는 것이므로 선지의 설명은 적절하다. 단순히 문자열을 전송했다는 사실만으로 성공하는 것은 아니며, 서버의 부적절한 입력 처리와 명령 실행이 전제된다.

② O. XSS는 공격자가 넣은 스크립트가 정상 웹페이지의 내용처럼 전달되거나 처리되어 다른 사용자의 브라우저에서 실행되는 공격이다. 웹서버가 데이터를 안전하게 출력하지 않거나 클라이언트 코드가 위험하게 처리할 때 발생할 수 있다. 핵심 실행 위치는 피해 사용자의 브라우저이며, 서버의 운영체제 명령을 실행하는 ①과 구별된다.

③ X. 브라우저에서 디렉터리의 파일 이름과 하위 목록을 볼 수 있게 노출하는 것은 **디렉터리 리스팅**에 관한 설명이다. CSRF는 인증된 사용자의 브라우저가 그 사용자의 의사와 무관하게 웹 애플리케이션에 요청을 보내도록 유도하는 공격이다. 서버가 세션 쿠키 등으로 사용자를 식별하더라도 해당 요청이 사용자의 진짜 의도에서 나왔는지 확인하지 못하는 점을 악용한다.

④ O. SQL Injection은 입력값이 SQL 문장의 구조나 의미를 바꾸도록 삽입되어 데이터베이스가 개발자의 의도와 다른 질의를 실행하게 하는 공격이다. 의도하지 않은 조회 결과뿐 아니라 권한과 질의 구성에 따라 데이터 변경·삭제 등의 영향도 생길 수 있다. 입력값을 SQL 명령과 분리하여 처리하지 못하는 것이 핵심 원인이다.

따라서 CSRF를 디렉터리 리스팅으로 잘못 설명한 ③이 정답이다.

NoteBase

문 29. 다음 사례에 해당하는 WEB 공격 유형은?

입사 지원을 위한 채용 사이트에서는 지원자의 성명, 주민등록번호, 주소 등 입사 지원 정보에 대한 확인 방법을 숫자로 된 단순 아이디 값으로 검증하고 있다. 이로 인해 공격자는 지원자 별로 할당된 숫자 아이디 파라미터 값을 순차적으로 증가시켜 타인의 입사지원서를 열람할 수 있는 자동화 프로그램을 제작하여 개인정보를 유출하였다.

① SQL Injection 공격
② 사회공학 기법
③ 파라미터 변조 취약점
④ 파일 다운로드 취약점

정답 3번

간단한 해설

숫자 아이디를 바꾸었을 때 서버가 요청자의 열람 권한을 확인하지 않아 타인의 자료가 노출되었다. 이는 **파라미터 변조와 대상 자료별 접근 권한 검증의 결여**가 결합한 취약점이다.

핵심 풀이

사례에서는 입사지원서를 가리키는 숫자 아이디가 요청 파라미터로 사용된다. 공격자는 SQL 문장을 넣거나 담당자를 속인 것이 아니라 그 값을 바꾸어 다른 지원자의 자료를 요청했다. 서버가 요청자에게 해당 지원서의 열람 권한이 있는지 검증하지 않았으므로, ③ 파라미터 변조 취약점에 해당한다. 이러한 객체 식별자 변경을 통한 무단 접근은 안전하지 않은 직접 객체 참조와도 연결된다.

① SQL Injection 공격: 입력값에 SQL 구문을 끼워 넣어 데이터베이스 질의의 의미나 실행을 바꾸는 공격이다. 사례에는 SQL 구문의 삽입·변경이라는 단서가 없다.

② 사회공학 기법: 사람의 신뢰나 심리적 약점을 이용하여 정보를 얻거나 행동을 유도하는 방법이다. 사례는 사람을 기만한 것이 아니라 요청 파라미터를 직접 변경했다.

④ 파일 다운로드 취약점: 다운로드 대상 파일이나 경로에 대한 검증·접근 통제가 부족하여 허용되지 않은 파일을 가져올 수 있는 문제이다. 사례의 결정적 단서는 파일 경로 변경이 아니라 **지원자 식별자 변경에 따른 타인 자료 열람**이다.

방어의 핵심은 서버가 매 요청마다 **요청자와 대상 자료 사이의 접근 권한**을 검증하는 것이다. 아이디를 추측하기 어렵게 바꾸는 것은 보조 수단일 뿐이며, 권한 검증을 대신할 수 없다.

NoteBase

문 30. 전자상거래에서 사용되는 SET 프로토콜에 관한 설명 중 옳지 않은 것은?

① RSA 암호화를 사용하여 속도가 빠르고, 강력한 보안을 제공한다.

② 기존의 신용카드 기반을 그대로 활용할 수 있다.

③ 신용카드 소지자에게 전자지갑 소프트웨어를 요구한다.

④ 신용카드 트랜잭션을 보호하기 위해 기밀성, 인증 및 메시지 무결성 등의 서비스를 제공한다.

정답 1번

간단한 해설

SET는 기존 신용카드 결제를 암호화·인증서·전자서명으로 보호하는 프로토콜이다. RSA 사용이 빠른 처리 속도를 뜻하지 않으며, 복잡한 인증과 암호 연산은 처리 부담을 만든다.

선지별 해설

① (X) SET가 RSA 등 암호 기술로 거래를 보호한다는 취지는 맞지만, **RSA를 사용하므로 속도가 빠르다**는 설명은 틀리다. 공개키 연산과 인증서·전자서명 검증에는 처리 부담이 있으며, SET의 복잡한 인증 절차도 비용을 더한다. 데이터의 대량 암호화에는 상대적으로 빠른 대칭키 방식을 결합한다.

② (O) SET는 **기존 신용카드 결제 기반**을 이용하여 온라인 거래를 보호하도록 설계되었다. 카드 소지자·가맹점·금융기관의 기존 결제 관계를 활용한다는 뜻이며, 별도의 인증서나 SET 지원 소프트웨어가 전혀 필요 없다는 뜻은 아니다.

③ (O) 신용카드 소지자는 SET 거래를 처리하는 **전자지갑 소프트웨어**를 사용한다. 전자지갑은 카드 관련 정보와 인증서 등을 다루고, 구매자가 거래에 필요한 서명·암호 처리를 수행하도록 돕는다.

④ (O) SET는 신용카드 거래정보의 **기밀성·참여자 인증·메시지 무결성**을 제공한다. 암호화로 정보 노출을 제한하고, 인증서와 전자서명 등을 통해 참여자의 신원 및 거래내용의 변조 여부를 확인한다.

따라서 옳지 않은 설명은 처리 속도를 잘못 설명한 ①이다.

NoteBase

문 31. 다음 설명에 해당하는 전자서명 방식은?

고객의 지불정보가 판매자를 통하여 해당 지급정보 중계기관으로 전송됨에 따라 고객의 지불정보가 판매자에게 노출될 가능성과 판매자에 의한 결제 정보의 위·변조 가능성을 제거한다.

① 부인불가 서명
② 이중 서명
③ 은닉 서명
④ 위임 서명

정답 2번

간단한 해설

주문정보와 지불정보를 각각 필요한 상대에게만 공개하면서 두 정보가 같은 거래에 속함을 확인하는 단서는 **이중 서명**을 가리킨다. SET에서는 두 정보의 해시값을 결합한 서명과 지불정보 암호화를 함께 이용하여 내용 노출과 변조에 대응한다.

NoteBase

개념 구분

지문의 핵심은 판매자가 지불정보를 중계하되 그 내용은 알 수 없고, 주문과 결제의 연결 관계를 임의로 바꿀 수도 없게 한다는 것이다. SET에서 사용하는 **이중 서명**은 주문정보와 지불정보의 해시값을 함께 묶어 고객이 서명함으로써 두 정보가 같은 거래에 속함을 확인하게 한다.

판매자는 주문정보와 지불정보의 해시값을, 지급정보 중계기관은 지불정보와 주문정보의 해시값을 이용하여 서명을 확인한다. 서로에게 공개하지 않는 정보의 원문 대신 해시값을 사용하므로 각자가 필요한 정보만 보면서도 두 정보의 결합을 검증할 수 있다.

지불정보의 내용이 판매자에게 보이지 않는 것은 중계기관만 복호화할 수 있도록 하는 암호화와 결합하여 달성한다. 이중 서명은 그 정보와 주문의 연결 및 무결성을 검증하는 역할을 한다. 따라서 서명 그 자체가 데이터를 암호화한다거나 변조 시도 자체를 물리적으로 막는다고 이해해서는 안 되며, 변조한 내용을 정상 거래로 검증받기 어렵게 하는 구조로 이해해야 한다.

① 부인불가 서명은 서명을 검증하는 과정에 서명자의 협력이 필요한 방식이다. 검증에 대한 서명자의 관여가 특징이며, 주문정보와 지불정보를 분리하여 결합하는 것이 핵심인 지문과 다르다.

③ 은닉 서명은 서명받을 내용을 가린 상태에서 서명을 받아, 서명자가 그 원문을 알지 못하게 하는 방식이다. 여기서 가리는 대상은 서명자가 서명할 메시지이며, 고객이 자신의 주문·지불정보를 결합해 서명하는 이중 서명과 구별된다.

④ 위임 서명은 원래 서명자가 다른 주체에게 서명 권한을 위임하고 대리 서명자가 그 권한에 따라 서명하는 방식이다. 지문에는 서명 권한을 다른 사람에게 넘기는 과정이 제시되어 있지 않다.

따라서 주문정보와 지불정보의 비공개 분리 및 거래 결합을 설명하는 방식은 ② 이중 서명이다.

NoteBase

문 32. 재해복구 시스템은 복구 수준에 따라 4가지 유형으로 구분된다. 다음 중 콜드 사이트(Cold Site) 복구 시스템에 관한 설명으로 적합한 것은?

① 주 센터와 동일한 수준의 정보기술자원을 원격지에 구축하고, 주 센터와 재해복구센터 모두 운영(Active) 상태로 동시에 서비스를 제공하는 방식

② 주 센터와 동일한 수준의 정보기술자원을 대기 상태로 원격지에 구축하여 주 센터 재해 발생 시 재해복구센터의 정보 시스템을 운영(Active) 상태로 서비스를 제공하는 방식

③ 데이터만 백업하여 원격지에 보관하고, 업무 재개를 위한 정보기술자원은 확보하지 않거나 또는 장소 등 최소한의 자원만 확보한 후, 재해 시 백업된 데이터를 활용하여 정보 시스템을 복구하는 방식

④ 핫 사이트와 유사하나, 주 센터와 동일한 정보기술자원을 보유하는 대신에 중요성이 높은 자원만 부분적으로 재해복구센터에 보유하는 방식

정답 3번

간단한 해설

콜드 사이트는 백업 데이터와 장소 등 최소한의 기반을 확보하되, **즉시 업무를 운영할 정보기술자원은 갖추지 않는 방식**이다. 재해 후 장비 확보·설치와 데이터 복구가 필요하므로 업무 재개에 시간이 걸린다.

선지별 해설

① X: 주 센터와 재해복구센터가 모두 운영 상태로 동시에 서비스를 제공하는 것은 미러 사이트이다. 두 센터에 동일 수준의 자원을 두어 서비스 연속성을 높이는 방식으로, 최소한의 자원만 준비하는 콜드 사이트와 다르다.

② X: 동일 수준의 정보기술자원을 원격지에 준비해 두고 재해 시 운영 상태로 전환하는 것은 핫 사이트이다. 핵심은 **운영에 필요한 자원을 미리 갖춘 대기 상태**라는 점이다.

③ O: 콜드 사이트는 원격지에 백업 데이터를 보관하고 장소 등 최소한의 기반만 확보하거나, 업무 재개용 정보기술자원은 재해 후 마련한다. 따라서 장비 설치와 시스템·데이터 복구에 시간이 필요하다. 평상시 구축·유지 비용은 상대적으로 낮지만 **복구에 필요한 준비 작업이 많다**.

④ X: 중요성이 높은 정보기술자원을 중심으로 일부만 확보해 두는 것은 웜 사이트이다. 자원을 완비한 핫 사이트와 최소 기반만 마련한 콜드 사이트 사이의 방식으로, 재해 시 부족한 자원과 데이터를 보충하여 서비스를 복구한다.

NoteBase

문 33. 다음 괄호 안에 해당하는 국제 표준은?

( )은(는) 과거 BS7799 Part01에서 ISO/IEC17799를 거쳐 현재는 국제 표준이 되었다.
정보보호 관리체계(ISMS)를 수립, 구현 및 유지하기 위해 공통적으로 적용할 수 있는 실무적인 지침 및 일반적인 원칙을 규정하고 있다.

① ISO/IEC 27000

② ISO/IEC 27002

③ ISO/IEC 27004

④ ISO/IEC 27006

정답 2번

간단한 해설

BS7799 Part 1과 ISO/IEC 17799를 계승한 실무 지침은 ISO/IEC 27002이다. 정보보호 통제를 선택·구현·관리하는 데 필요한 원칙과 지침을 제공한다.

NoteBase

개념 구분

지문은 ISMS 관련 표준 중 실무적인 통제 지침을 묻는다. 특히 BS7799 Part 1에서 ISO/IEC 17799를 거쳐 온 연혁이 결정적인 단서이다. ISO/IEC 27001이 관리체계의 요구사항을 다루는 것과, ISO/IEC 27002가 통제의 실무 지침을 다루는 것을 구별한다.

ISO/IEC 27000: ISMS에 대한 **개요와 공통 용어**를 설명하는 표준이다. 관련 표준을 이해하기 위한 기본 개념과 정의를 제공하며, 지문이 말하는 통제 실무 지침의 번호는 아니다.

ISO/IEC 27002: 조직이 정보보호 통제를 선택하고 구현·관리할 때 참고할 **실무 지침과 원칙**을 제공한다. BS7799 Part 1을 토대로 발전한 ISO/IEC 17799가 ISO/IEC 27002로 번호를 변경한 계보를 가지므로, 지문의 연혁과 역할이 모두 일치한다.

ISO/IEC 27004: 정보보호 성과와 ISMS의 효과성을 **모니터링·측정·분석·평가**하는 데 필요한 지침을 다룬다. 통제를 어떻게 측정하고 효과를 판단할 것인지에 중점을 두므로, 지문의 실무 통제 지침과 구별된다.

ISO/IEC 27006: 당시 ISMS의 심사와 인증을 수행하는 **인증기관의 요구사항**을 다루는 표준이다. 인증을 받으려는 조직에 적용할 실무 통제 목록 자체보다, 인증기관의 역량과 신뢰성 등 심사·인증 수행 조건에 관한 표준이다.

따라서 괄호에 들어갈 표준은 ISO/IEC 27002이며, ②와 연결된다.

NoteBase

문 34. 정보보호 관리체계(ISMS)에 관한 설명 중 옳은 것은?

① ISMS 인증 제도는 「정보통신기반 보호법」에 근거를 두고 2002년부터 시행해오고 있다.

② 인증 심사 기준은 정보보호관리과정과 정보보호대책의 두 가지로 구성되어 있다.

③ 모든 기업이 자율적으로 심사를 신청하는 자율 제도로 운영된다.

④ 국가정보원이 평가하여 인증하며, 인증의 유효기간은 3년이다.

정답 2번

간단한 해설

문항의 기존 ISMS 심사기준은 **정보보호 관리과정과 정보보호대책**으로 나뉜다. 근거 법률은 정보통신망법이고 법정 인증 의무 대상도 있으며, 국가정보원이 인증을 부여한다는 설명은 틀리다.

선지별 해설

① X. ISMS 인증의 근거는 **「정보통신망 이용촉진 및 정보보호 등에 관한 법률」**이다. 이 법의 정보보호 관리체계 인증 제도와 「정보통신기반 보호법」의 주요정보통신기반시설 보호 제도를 혼동해서는 안 된다. 선지는 시행 시기에 관한 표현과 별개로 근거 법률을 잘못 연결했으므로 틀리다.

② O. 문항이 사용하는 종전 ISMS 인증 심사기준은 **정보보호 관리과정과 정보보호대책**의 두 축으로 구성된다. 관리과정은 정책 수립, 조직의 책임, 위험관리, 보호대책의 구현과 사후관리처럼 관리체계를 운영하는 절차를 살핀다. 정보보호대책은 접근통제, 물리적 보안, 운영보안 등 실제 보호조치를 살핀다. 이는 해당 문항의 기존 ISMS 기준에 대한 설명이며, 이후 통합·개편된 ISMS-P의 세부 영역 명칭과 항목을 그대로 대입해서는 안 된다.

③ X. 자율적으로 인증을 신청할 수 있는 경우도 있지만, 법에서 정한 일정한 대상에게는 인증 의무가 있다. 따라서 '모든 기업'이 오직 자율 신청으로만 참여한다는 설명은 틀리다. 자율 신청 대상과 법정 의무 대상을 구분해야 한다.

④ X. 인증 유효기간이 3년이라는 부분은 맞지만, 국가정보원이 이 인증을 평가·부여한다는 부분은 틀리다. ISMS 인증 업무는 한국인터넷진흥원(KISA)과 지정된 인증기관 등이 법령상 역할에 따라 수행한다. 유효기간 중에도 사후심사를 통해 관리체계의 유지 여부를 확인하므로 3년 동안 아무런 점검을 받지 않는다는 뜻도 아니다.

따라서 기존 ISMS 인증 심사기준의 두 구성 부분을 적절하게 설명한 ②가 정답이다.

NoteBase

문 35. 다음 중 OWASP(Open Web Application Security Project)에서 발표한 OWASP TOP 10 - 2017에 해당되는 항목은 모두 몇 개인가?

가. 인젝션
나. 취약한 인증
다. 민감한 데이터 노출
라. XML 외부 개체(XXE)
마. 크로스 사이트 요청 변조(CSRF)
바. 안전하지 않은 역직렬화

① 2개
② 3개
③ 4개
④ 5개

정답 4번

간단한 해설

2017년 OWASP Top 10에는 인젝션·취약한 인증·민감한 데이터 노출·XXE·안전하지 않은 역직렬화가 포함된다. CSRF는 이 판의 독립 항목에 포함되지 않는다.

NoteBase

보기별 해설

이 문항은 OWASP Top 10의 **2017년 판**에 포함된 항목을 묻는다. 다른 연도의 명칭이나 순위로 판단하지 않는다.

가. 포함: 인젝션은 **A1:2017**이다. 신뢰할 수 없는 입력이 명령이나 질의의 일부로 해석되어 의도하지 않은 동작을 일으키는 위험이다.

나. 포함: 취약한 인증은 **A2:2017**이다. 인증이나 세션 관리의 결함으로 다른 사용자의 신원을 도용할 수 있는 문제를 다룬다.

다. 포함: 민감한 데이터 노출은 **A3:2017**이다. 중요한 데이터를 적절히 보호하지 못해 노출되는 위험을 말한다.

라. 포함: XML 외부 개체(XXE)는 **A4:2017**이다. 외부 개체 처리가 허용된 XML 파서가 신뢰할 수 없는 입력을 처리하여 정보 노출 등을 일으킬 수 있는 위험이다.

마. 미포함: 크로스 사이트 요청 변조(CSRF)는 **2017년 Top 10의 독립 항목이 아니다**. 인증된 사용자의 브라우저가 의도하지 않은 요청을 보내게 하는 공격으로, 목록에서 빠졌다고 위험 자체가 사라진 것은 아니다.

바. 포함: 안전하지 않은 역직렬화는 **A8:2017**이다. 신뢰할 수 없는 직렬화 데이터를 객체로 복원하는 과정에서 악성 동작이나 데이터 변조 등이 발생할 수 있는 문제이다.

따라서 포함되는 항목은 가·나·다·라·바의 5개이므로 ④이다.

NoteBase

문 36. 「정보통신기반 보호법」에서 명시한 주요정보통신기반시설의 취약점을 분석·평가하는 전담반에 속하지 않는 것은?

① 한국인터넷진흥원

② 한국전자통신연구원

③ 「정보통신기반 보호법」 제16조의 규정에 의한 정보공유·분석센터

④ 「정보보호산업의 진흥에 관한 법률」 제23조에 따라 지정된 정보보호 컨설팅 전문기업

정답 4번

간단한 해설

법률에 열거된 지정 기업의 명칭은 **'정보보호 전문서비스 기업'**이다. '정보보호 컨설팅 전문기업'이라는 표현은 해당 법정 명칭과 일치하지 않는다.

개념 구분

시험 당시 「정보통신기반 보호법」 제9조제2항은 관리기관이 취약점 분석·평가를 위한 자체 전담반을 구성하도록 하고, 제3항은 외부 전문기관으로 하여금 분석·평가하게 할 수 있도록 구분했다. 외부 전문기관에 맡기는 경우에는 자체 전담반을 구성하지 않을 수 있다. 따라서 발문의 '전담반에 속하는 기관'이라는 표현과 법률의 **자체 전담반·외부 수행기관 구분**을 혼동하지 않아야 한다. 제시된 기관 목록은 외부 분석·평가기관의 법정 명칭과 대조하여 판단한다.

① 한국인터넷진흥원: 당시 제9조제3항제1호에 열거된 기관으로, 주요정보통신기반시설의 취약점 분석·평가를 수행하게 할 수 있다.

② 한국전자통신연구원: 당시 제9조제3항제4호에 열거된 기관이다. 법률이 정한 외부 분석·평가기관에 포함된다.

③ 정보공유·분석센터: 당시 제9조제3항제2호는 제16조에 따른 정보공유·분석센터 중 **대통령령이 정하는 기준을 충족하는 센터**를 대상으로 한다. 명칭만 갖추면 모두 해당하는 것은 아니다.

④ 정보보호 컨설팅 전문기업: 당시 제9조제3항제3호의 정확한 명칭은 「정보보호산업의 진흥에 관한 법률」 제23조에 따라 지정된 **정보보호 전문서비스 기업**이다. 따라서 법정 명칭과 일치하지 않는 ④가 제시된 선택지 중 답에 해당한다. 이는 적법하게 지정된 정보보호 전문서비스 기업이 취약점 분석·평가를 수행할 수 없다는 뜻은 아니다.

NoteBase

문 37. 「개인정보 보호법」 제31조(개인정보 보호책임자의 지정)에서 개인정보 보호책임자의 업무에 속하지 않는 것은?

① 개인정보 보호 인증 취득

② 개인정보 보호 교육 계획의 수립 및 시행

③ 개인정보 처리와 관련한 불만의 처리 및 피해 구제

④ 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선

정답 1번

간단한 해설

제31조는 개인정보 보호책임자에게 교육 계획, 고충·피해 구제, 처리 실태의 조사·개선 등의 업무를 맡긴다. **개인정보 보호 인증 취득 자체는 이 조의 업무 항목이 아니므로** ①이다.

선지별 해설

① X: '개인정보 보호 인증 취득'은 제31조가 열거한 **개인정보 보호책임자의 고유한 법정 업무에 포함되지 않는다**. 인증은 개인정보처리자의 처리·보호 조치가 법에 부합하는지 별도 기준과 절차에 따라 심사하는 제도이다. 보호책임자가 조직의 인증 준비에 관여할 수는 있지만, 그 사실만으로 인증 취득 자체가 제31조의 업무 항목이 되는 것은 아니다.

② O: 개인정보 보호책임자의 업무에는 **개인정보 보호 교육 계획의 수립 및 시행**이 포함된다. 개인정보를 취급하는 구성원이 보호 원칙과 절차를 알고 준수하도록 교육을 계획하고 실행하는 업무이다.

③ O: **개인정보 처리와 관련한 불만의 처리 및 피해 구제**는 보호책임자의 법정 업무이다. 정보주체의 고충을 접수·처리하고 개인정보 처리로 인한 피해에 대응하는 역할을 뜻한다.

④ O: **개인정보 처리 실태 및 관행의 정기적인 조사 및 개선**도 보호책임자의 법정 업무이다. 조직에서 실제로 개인정보를 어떻게 처리하는지와 반복되는 업무 관행을 점검하고 문제점을 바로잡는 역할이다.

따라서 제31조에 규정된 보호책임자의 업무에 속하지 않는 것은 ①이다. 보호책임자의 일상적인 보호·관리 업무와 별도의 인증 취득 제도를 구별해야 한다.

NoteBase

문 38. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제22조 (개인정보의 수집·이용 동의 등)에서 정의하는 정보통신서비스 제공자가 이용자의 개인정보를 이용하려고 수집하는 경우 이용자에게 알리고 동의 받아야 할 사항이 아닌 것은?

① 개인정보의 수집·이용 목적

② 수집하는 개인정보의 항목

③ 개인정보처리의 위탁기관명

④ 개인정보의 보유·이용 기간

정답 3번

간단한 해설

당시 정보통신망법 제22조의 고지·동의 사항은 **수집·이용 목적, 수집 항목, 보유·이용 기간**이다.
개인정보처리의 위탁기관명은 이 조항의 열거 사항에 포함되지 않는다.

선지별 해설

2019년 출제 당시 정보통신망법 제22조제1항은 정보통신서비스 제공자가 이용자의 개인정보를 이용하려고 수집할 때 고지하고 동의를 받아야 할 사항을 정했다. 이는 이용자가 정보 수집의 내용과 범위를 알고 동의하도록 하는 규정이다.

① O: 개인정보의 수집·이용 목적은 **왜 정보를 수집하고 어디에 사용하는지**를 나타낸다. 제22조제1항의 고지·동의 사항에 해당한다.

② O: 수집하는 개인정보의 항목은 성명·연락처 등 **어떤 정보를 수집하는지**를 나타낸다. 목적만 알리고 항목을 생략해서는 이용자가 수집 범위를 알 수 없으므로 고지·동의 사항에 포함된다.

③ X: 개인정보처리의 위탁기관명은 **제22조제1항의 세 가지 고지·동의 사항이 아니다**. 개인정보의 수집·이용에 관한 고지 사항과 처리업무를 다른 자에게 맡기는 위탁에 관한 사항을 구분해야 한다. 당시 개인정보 처리위탁은 제25조에서 별도로 규율했으므로, 이 선지를 고르더라도 위탁에 관한 고지 의무가 전혀 없다는 뜻은 아니다.

④ O: 개인정보의 보유·이용 기간은 **얼마나 오래 정보를 보유하고 이용하는지**를 나타낸다. 이용자가 정보 처리의 시간적 범위를 알고 동의하도록 하기 위한 고지·동의 사항이다.

NoteBase

문 39. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제27조의3(개인정보 유출등의 통지·신고)에서 통지 및 신고 시에 필수로 포함되어야 할 사항은 모두 몇 개인가?

가. 유출등이 된 개인정보 항목
나. 유출등의 공격에 대한 분석 내용
다. 유출등이 발생한 시점
라. 이용자가 취할 수 있는 조치
마. 정보통신서비스 제공자등의 대응 조치

① 1개
② 2개
③ 3개
④ 4개

정답 4번

간단한 해설

당시 제27조의3은 유출된 항목·발생 시점·이용자의 조치·제공자의 대응·상담 부서 및 연락처를 통지·신고 사항으로 정했다. 공격 분석 내용은 이 열거 항목에 해당하지 않는다.

NoteBase

보기별 해설

2019년 시험 당시 정보통신망법 제27조의3 제1항이 정한 **통지·신고 항목**을 기준으로 판단한다.

가. 포함: **유출등이 된 개인정보 항목**은 제1호에 규정되어 있다. 어떤 종류의 개인정보가 분실·도난·유출되었는지를 알리는 사항이다.

나. 미포함: **공격에 대한 분석 내용**은 해당 조항이 열거한 필수 통지·신고 항목이 아니다. 사고 조사에 필요한 정보일 수 있다는 점과, 이 조항의 열거 사항에 해당하는지는 구별해야 한다.

다. 포함: **유출등이 발생한 시점**은 제2호에 규정되어 있다. 발생한 때를 알리는 사항으로, 공격 기법에 대한 분석 내용과는 다르다.

라. 포함: **이용자가 취할 수 있는 조치**는 제3호에 규정되어 있다. 이용자 자신이 피해를 줄이기 위해 할 수 있는 대응을 안내하는 사항이다.

마. 포함: **정보통신서비스 제공자등의 대응 조치**는 제4호에 규정되어 있다. 이용자가 할 일과 구분하여 서비스 제공자 측의 대응을 알리는 사항이다.

조문에는 이 밖에 제5호인 '이용자가 상담 등을 접수할 수 있는 부서 및 연락처'도 있다. 그러나 이 항목은 제시된 보기에 없으므로 보기의 개수에 더하지 않는다.

따라서 제시된 보기 중 필수 항목은 가·다·라·마의 4개이므로 ④이다.

NoteBase

문 40. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 정의하는 용어에 관한 설명으로 옳은 것은 모두 몇 개인가?

가. “정보통신서비스”란 「전기통신사업법」 제2조 제6호에 따른 전기통신역무와 이를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 것을 말한다.
나. “침해사고”란 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태를 말한다.
다. “전자적 전송매체”란 정보통신망을 통하여 부호·문자·음성·화상 또는 영상 등을 수신자에게 전자문서 등의 전자적 형태로 전송하는 매체를 말한다.
라. “통신과금서비스이용자”란 정보보호제품을 개발·생산 또는 유통하는 사람이나 정보보호에 관한 컨설팅 등과 관련된 사람을 말한다.
마. “전자문서”란 컴퓨터 등 정보처리능력을 가진 장치에 의하여 전기적인 형태로 작성되어 송수신되거나 저장된 문서형식의 자료로서 정형화된 것을 말한다.

① 2개
② 3개
③ 4개
④ 5개

정답 2번

간단한 해설

통신과금서비스이용자는 보안업 종사자가 아니라 그 서비스를 이용해 재화·용역을 구매하는 자이다. 또한 전자문서의 법정 정의는 **전자적인 형태로 작성된 표준화된 자료**를 말하므로 라·마가 틀리고 가·나·다가 옳다.

NoteBase

보기별 해설

가. O. 당시 정보통신망법은 정보통신서비스에 전기통신역무 자체뿐 아니라, 그 역무를 이용하여 정보를 제공하거나 정보 제공을 매개하는 활동도 포함한다. 따라서 통신을 직접 제공하는 기능에만 한정하지 않은 보기의 정의는 적절하다.

나. O. 당시 법률의 침해사고 정의는 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부, 고출력 전자기파 등의 방법으로 정보통신망이나 관련 정보시스템을 공격하여 발생한 사태를 가리킨다. 보기는 그 공격 방법과 대상을 정확하게 설명한다.

다. O. 전자적 전송매체는 정보통신망을 통해 부호·문자·음성·화상·영상 등을 수신자에게 전자문서 등의 전자적 형태로 보내는 매체이다. 전송되는 정보의 종류와 전송 형태를 함께 제시한 보기의 정의는 법률상 내용과 부합한다.

라. X. 통신과금서비스이용자는 **통신과금서비스를 이용하여 재화나 용역을 구입·이용하는 자**이다. 통신요금과 함께 대금을 청구·징수하는 등의 통신과금서비스를 제공받아 구매·이용하는 사람을 뜻한다. 보안제품의 개발·생산·유통이나 보안 컨설팅에 종사한다는 사실로 정의되는 사람이 아니다.

마. X. 당시 법률은 전자문서를 정보처리능력이 있는 장치로 **전자적인 형태**로 작성하여 송수신하거나 저장한 문서형식의 자료 중 **표준화된 것**으로 정의한다. 보기의 '전기적인 형태'와 '정형화된 것'은 법률이 정한 표현과 다르므로, 법정 정의를 정확하게 제시한 설명으로 볼 수 없다.

따라서 옳은 보기는 가·나·다의 3개이므로 정답은 ②이다.

NoteBase