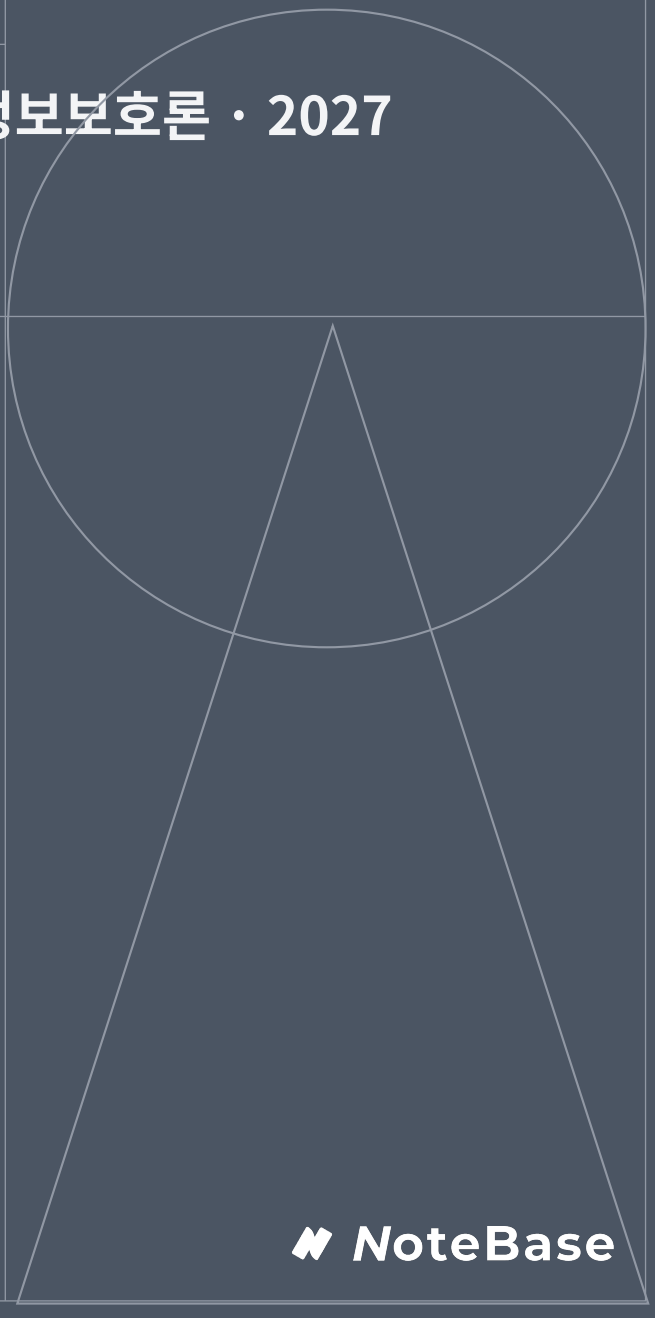
기출OX 해설집

공무원/경찰/공채(경위) · 정보보호론 · 2027



NoteBase

기출OX 해설집

공무원/경찰/공채(경위) · 정보보호론 · 2027

공무원/경찰/공채(경위) · 정보보호론 · 2027

문 1. 시스템 보안 주제와 그 설명으로 가장 적절하지 않은 것은?

① 계정 관리 - 사용자와 시스템 사이 또는 두 시스템 사이의 활성화된 접속 관리

② 접근 제어 - 다른 시스템으로부터 보호할 수 있도록 네트워크 관점에서 접근을 통제

③ 권한 관리 - 각 사용자가 정당한 권한으로 허용된 정보 자산에 접근

④ 로그 관리 - 시스템 내부나 네트워크를 통해 외부에서 시스템에 어떤 영향을 미칠 경우 그 내용을 기록하여 관리

정답 1번

간단한 해설

계정은 사용자 신원과 계정의 수명주기, 세션은 현재 활성화된 접속을 관리하는 대상이다. 활성 접속을 관리한다는 설명은 계정 관리가 아니라 세션 관리에 해당한다.

NoteBase

선지별 해설

① X: 사용자와 시스템 또는 시스템 사이의 **활성화된 접속을 관리하는 것은 세션 관리**이다. 접속의 생성·유지·종료와 세션 만료 등을 다룬다. 계정 관리는 사용자 계정의 생성·변경·비활성화·삭제와 인증정보 등 계정의 수명주기를 관리하므로 구별해야 한다.

② O: 네트워크 관점의 접근 제어는 정책에 따라 시스템에 들어오는 통신을 허용하거나 제한하여 무단 접근을 통제한다. 주소·포트 등의 규칙을 사용할 수 있다. 다만 접근 제어 전체가 네트워크 통제에만 한정되는 것은 아니며, 선지는 그중 네트워크 측면을 설명한 것이다.

③ O: 권한 관리는 사용자나 역할에 어떤 정보 자산과 작업을 허용할지 정한다. 파일 읽기·쓰기·실행 등 **허용된 자산과 행위의 범위**를 관리하여 권한을 벗어난 이용을 막는다. 사용자가 누구인지 확인하는 인증과, 무엇을 할 수 있는지 정하는 권한은 구별된다.

④ O: 로그 관리는 접속·인증·작업·오류 등 시스템에서 발생한 사건을 기록하고 보관·분석하는 활동이다. 기록은 이상 행위 탐지와 사고 원인 추적의 근거가 된다. 기록 자체가 모든 공격을 예방한다는 뜻은 아니며, 필요한 사건이 남도록 설정하고 기록을 보호하는 관리가 필요하다.

따라서 세션 관리의 설명을 계정 관리에 연결한 ①이 가장 적절하지 않다.

NoteBase

문 2. 보안 위협과 이를 방지하기 위한 기술로 가장 적절한 것은?

① 보안 위협: 부인, 기술: 암호화

② 보안 위협: 도청, 기술: 메시지 인증 코드

③ 보안 위협: 위장, 기술: 일방향 해시 함수

④ 보안 위협: 메시지 변경, 기술: 디지털 서명

정답 4번

간단한 해설

디지털 서명은 **메시지의 무결성을 검증하여 변경을 탐지**한다. 암호화는 기밀성, MAC은 키 기반 인증·무결성, 키 없는 해시는 신원 인증과 구별한다.

선지별 해설

① X: 단순 암호화의 기본 목적은 내용을 숨기는 기밀성 보호이다. 메시지를 보낸 사실의 부인에 대응하려면 서명자의 개인키로 생성한 디지털 서명 등 출처를 검증할 증거가 필요하다. 암호화만으로 부인방지가 일반적으로 성립하지 않는다.

② X: 메시지 인증 코드(MAC)는 공유 비밀키를 이용해 메시지의 무결성과 출처 인증을 지원하지만 내용을 숨기지는 않는다. 도청자가 메시지를 읽지 못하게 하는 목적에는 암호화가 대응한다.

③ X: 키 없는 일방향 해시 함수는 누구나 계산할 수 있으므로 그 값만으로 발신자의 신원을 입증하지 못한다. 다른 사람으로 위장하는 공격에 대응하려면 키 기반 메시지 인증이나 디지털 서명 등 인증 수단이 필요하다.

④ O: 디지털 서명은 메시지 내용과 서명을 결합하여 검증하므로 **서명 후 메시지가 바뀌면 유효한 서명 검증이 성립하지 않도록** 무결성을 보호한다. 전송 중의 물리적 변경 자체를 막는다는 뜻이 아니라 변경을 탐지하여 신뢰하지 않게 하는 방식이다.

따라서 메시지 변경 위협에 디지털 서명을 대응시킨 ④가 적절하다.

NoteBase

문 3. 재전송 공격이 가능한 블록 암호 운영 모드로 가장 적절한 것은?

① CBC

② CFB

③ OFB

④ CTR

정답 2번

간단한 해설

CFB는 **암호문을 다음 단계의 입력으로 되먹임**하므로, 같은 키에서 과거의 연속된 암호문을 재사용하면 과거 평문 일부가 다시 복원될 수 있다. 다만 재전송 공격이 CFB에만 가능한 것은 아니다.

개념 구분

재전송 공격은 과거에 전송된 메시지를 가로챘다가 다시 보내 수신자가 처리하도록 하는 공격이다. CFB는 앞서 받은 암호문을 블록 암호의 입력에 반영하고, 그 출력과 현재 암호문을 XOR하여 평문을 복원한다. 이 때문에 **과거 암호문을 되먹임 상태에 다시 반영**하는 방식의 재전송이 가능하다.

블록 전체를 한 번에 되먹임하는 CFB를 예로 들면, 같은 키로 암호화된 과거의 연속된 두 암호문 블록을 현재 통신에 끼워 넣을 수 있다. 삽입한 첫 블록의 평문은 앞선 상태가 달라 잘못 복원될 수 있지만, 둘째 블록에서는 과거 첫 암호문이 입력으로 쓰이므로 과거의 둘째 평문이 다시 복원된다. 별도의 무결성·신선성 검사가 없다면 이를 공격으로 판별하여 거부하는 기능은 CFB 자체에 없다.

CBC는 현재 암호문을 복호화한 값에 이전 암호문을 XOR한다. CFB처럼 이전 암호문을 암호화하여 XOR에 사용할 값을 만드는 구조와 다르다. OFB는 암호문의 영향을 받지 않는 내부 출력값을 되먹임하며, CTR은 카운터를 암호화한 값을 사용한다. 따라서 OFB·CTR에서는 과거 암호문을 끼워 넣는 것만으로 CFB처럼 되먹임 상태가 과거 암호문에 맞춰지는 것은 아니다.

다만 **암호화 모드 자체가 재전송 방지를 보장하지는 않는다**. CBC에도 연속된 과거 암호문을 삽입하여 평문 일부를 재현하는 공격이 가능하고, OFB·CTR도 오래된 메시지를 다시 받아들이지 않도록 하는 별도의 검사가 필요하다. CFB의 재전송 가능성을 설명하는 것과 다른 모드에서는 재전송이 불가능하다고 단정하는 것은 구별해야 한다. 재전송 방지에는 메시지와 순서번호 등을 인증하고, 수신자가 이미 처리한 번호의 재사용을 거부하는 절차가 필요하다.

NoteBase

문 5. 블루투스 보안 취약점에 대한 설명으로 가장 적절하지 않은 것은?

① 블루재킹은 공격 장치와 공격 대상 장치를 연결하여 공격 대상 장치에서 임의의 동작을 실행한다.

② 블루프린팅은 블루투스 공격 장치의 검색 활동을 의미한다.

③ 블루스나핑은 블루투스의 취약점을 이용하여 장비의 임의 파일에 접근하는 공격이다.

④ 블루버깅은 블루투스 장비 간의 취약한 연결 관리를 악용한 공격이다.

정답 1번

간단한 해설

블루재킹은 원치 않는 메시지 전송, 블루스나핑은 정보 탈취, 블루버깅은 기능 제어로 구별한다. 블루프린팅은 장치 특성을 알아내는 탐색 활동이다.

선지별 해설

① X: 블루재킹은 블루투스를 통해 **요청하지 않은 메시지나 전자 명함을 전송**하는 행위이다. 이를 대상 장치의 명령 실행이나 원격 제어와 동일시하면 안 된다. 취약점을 이용해 장치의 기능을 제어하는 설명은 블루버깅에 가깝다.

② O: 블루프린팅은 주변 블루투스 장치의 주소·서비스 정보 등의 특징을 수집하여 제조사나 모델 등을 식별하는 탐색·지문분석 활동이다. 선지의 검색 활동은 공격을 준비하는 장치가 대상을 탐색한다는 의미이다. 단순 검색만으로 모든 취약점이 확정된다는 뜻은 아니다.

③ O: 블루스나핑은 취약한 블루투스 구현을 악용하여 사용자 승인 없이 저장된 정보나 파일에 접근하는 공격이다. 전화번호부·일정 등 **정보의 무단 접근과 유출**이 핵심이다. 실제 접근 가능한 범위는 대상 장치와 취약점에 따라 달라지므로 모든 장치의 모든 파일에 항상 접근한다는 뜻은 아니다.

④ O: 블루버깅은 취약한 연결이나 펌웨어 구현을 악용하여 장치의 명령·기능을 비인가 방식으로 제어하는 공격이다. 단순 메시지 전송인 블루재킹, 저장 정보 탈취인 블루스나핑과 달리 **장치 기능의 무단 제어**에 초점이 있다. 해당 취약점이 있는 구현을 전제로 한다.

따라서 임의 동작 실행을 블루재킹의 특징으로 설명한 ①이 가장 적절하지 않다.

NoteBase

문 6. 프로그램의 코드보안에 대한 설명으로 가장 적절하지 않은 것은?

① 소스코드에서 문제를 발생시키는 요인으로 '데이터의 형태와 길이에 대한 불명확한 정의'가 있다.

② strcpy() 함수는 포맷스트링 공격에 취약한 함수이다.

③ 오버플로우가 발생하는 버퍼에 저장되는 공격자의 코드를 셸코드라고 한다.

④ 프로그램 실행 중에 해당 힙 영역이 고갈되면 메모리 부족으로 이상 종료가 된다.

정답 2번

간단한 해설

strcpy()는 문자열을 복사할 때 목적지 버퍼의 크기를 검사하지 않아 **버퍼 오버플로우**를 일으킬 수 있다.
포맷스트링 공격은 printf() 같은 함수에서 **외부 입력을 서식 문자열로 사용**할 때 발생한다.

선지별 해설

① O: 입력 데이터의 형태와 최대 길이가 명확하지 않으면, 어떤 입력을 허용하고 얼마만큼의 저장 공간을 확보해야 하는지 제대로 정하기 어렵다. 이로 인해 잘못된 데이터 처리나 버퍼 범위를 넘는 쓰기가 발생할 수 있으므로 **입력 형식과 허용 길이**를 명확히 정의하고 검사해야 한다.

② X: strcpy()는 원본 문자열을 널 문자까지 목적지에 복사하는 함수이며, 목적지 버퍼의 크기를 인자로 받지 않는다. 따라서 복사할 문자열이 목적지의 용량을 넘으면 **버퍼 오버플로우**가 발생할 수 있다. 포맷스트링 공격은 printf() 등의 서식 처리 함수에 외부 입력을 서식 문자열로 넘겨, 공격자가 넣은 서식 지정자가 해석되도록 하는 공격이다. strcpy()는 서식 문자열을 해석하는 함수가 아니므로 두 취약점을 구분해야 한다.

③ O: 셸코드는 셸 실행 등 공격자가 의도한 동작을 수행하도록 만든 기계어 코드이다. 버퍼 오버플로우 공격에서는 이를 입력 데이터에 포함해 버퍼에 저장하고, 실행 흐름을 조작하여 **저장된 공격 코드를 실행**시키려 한다. 다만 버퍼에 코드가 저장되었다는 사실만으로 곧바로 실행되는 것은 아니다.

④ O: 힙 고갈로 인한 메모리 부족이 프로그램의 이상 종료로 이어질 수 있다는 취지의 설명이다. 힙은 실행 중 필요한 메모리를 동적으로 할당하는 데 사용되며, 공간이 부족하면 추가 할당이 실패할 수 있다. 예를 들어 C의 malloc()은 할당 실패 시 NULL을 반환하므로 이를 확인하고 적절히 처리해야 한다. 엄밀히는 **힙 고갈이 항상 이상 종료를 뜻하지는 않는다**. 할당 실패를 처리하는 방식에 따라 해당 작업만 중단하거나 복구할 수 있으며, 실패를 제대로 처리하지 못하면 이상 동작이나 종료로 이어질 수 있다.

NoteBase

문 7. 치환 암호에 대한 설명으로 가장 적절하지 않은 것은?

① 단일 치환 암호는 다중 치환 암호보다 안전하다.

② 단일 치환 암호는 치환표를 키로 사용할 수 있다.

③ 단일 치환 암호는 빈도 분석법으로 암호문을 해석할 수 있다.

④ 단일 치환 암호는 평문의 특정 문자의 빈도와 이에 대응되는 암호문의 문자 빈도가 일치한다.

정답 1번

간단한 해설

고정된 일대일 치환은 문자 빈도를 보존한다. 이 때문에 단일 치환은 빈도 분석에 취약하며, 여러 치환표로 빈도 대응을 분산시키는 다중 치환보다 안전하다는 설명은 적절하지 않다.

선지별 해설

① X: 단일 치환은 같은 평문 문자를 항상 같은 암호문 문자로 바꾸므로 **문자별 빈도 특성이 남는다**. 여러 치환표를 사용하는 다중 치환은 같은 문자를 위치 등에 따라 다르게 바꾸어 이런 단순한 빈도 대응을 흐리게 하므로, 통상적인 고전 암호 비교에서 단일 치환이 더 안전하다는 설명은 틀리다. 다중 치환도 키 사용 방식에 따라 분석될 수 있어 절대적인 안전성을 뜻하지는 않는다.

② O: 단일 치환의 키는 평문 문자와 암호문 문자 사이의 일대일 대응을 정한 치환표로 표현할 수 있다. 수신자는 그 대응을 역으로 적용하여 원문을 복원한다. 문자의 위치를 옮기는 전치와 달리 **문자 기호 자체를 다른 기호로 대체**한다.

③ O: 단일 치환에서는 언어의 문자 빈도와 반복 패턴이 암호문에 대응되어 남으므로 빈도 분석으로 치환 관계를 추정할 수 있다. 다만 짧거나 특이한 문장은 일반적인 언어 통계와 다를 수 있으므로, 가장 흔한 문자 하나만 보고 항상 즉시 복호화할 수 있다는 뜻은 아니다.

④ O: 평문의 A를 항상 Q로 치환한다고 하면 A가 등장한 횟수만큼 Q가 등장한다. 일대일 치환에서는 전체 문자 수도 유지되므로 **대응하는 두 문자의 출현 횟수와 상대빈도가 같다**. 평문 A와 암호문 A처럼 이름이 같은 문자의 빈도를 비교하는 것이 아니라 치환표로 대응되는 문자를 비교해야 한다.

따라서 단일 치환 암호가 다중 치환 암호보다 안전하다고 한 ①이 가장 적절하지 않다.

NoteBase

문 8. 재해 복구 전략 수립 시 RTO = 0이고 RPO = 0일 경우 결정할 수 있는 재해 복구 시스템으로 가장 적절한 것은?

① Hot Site
② Cold Site
③ Mirror Site
④ Warm Site

정답 3번

간단한 해설

RTO 0·RPO 0은 **중단 없는 서비스와 데이터 손실 없는 복구**를 목표로 한다. 제시된 복구 사이트 분류에서는 Mirror Site가 이에 대응한다.

개념 구분

RTO는 서비스 중단 후 목표로 하는 복구 소요시간이고, RPO는 복구해야 할 데이터의 시점으로 표현하는 허용 데이터 손실 범위이다. 두 값이 모두 0이라는 조건은 **서비스 중단과 데이터 손실을 모두 허용하지 않는 목표**를 뜻한다.

Mirror Site는 주 센터와 대응하는 운영 환경을 실시간으로 동기화하여 유지하고 즉시 업무를 이어받도록 구성하는 방식이다. 이 문항의 분류에서는 동기식 데이터 복제와 지속적인 서비스 연속성을 목표로 하는 미러 사이트가 가장 적합하다.

Hot Site는 주요 장비와 운영 환경이 준비되어 복구가 빠르지만, 일반적인 대기형 구성에서는 전환과 최신 데이터 적용에 시간이 필요할 수 있다.

Warm Site는 일부 환경을 갖추고 추가 준비가 필요하며,

Cold Site는 주로 공간·전원 등 기반 시설부터 준비되어 있어 장비 설치와 데이터 복구가 요구된다.

실제 설계에서 단순히 미러 사이트라는 이름만으로 두 목표가 자동 보장되는 것은 아니다. 동기 복제 방식, 장애 감지와 자동 전환, 네트워크·애플리케이션의 연속성을 함께 검증해야 한다.

따라서 주어진 목표에 가장 적합한 선택지는 ③ Mirror Site이다.

NoteBase

문 9. SHA-512 해시 알고리즘에서 메시지(M)의 길이가 2560비트라면 입력을 위해 추가되어야 할 패딩은 몇 비트인가?

① 256비트

② 384비트

③ 512비트

④ 670비트

정답 2번

간단한 해설

SHA-512는 마지막 128비트를 길이 필드로 남긴다. 25601024=512이므로 896비트 지점까지 붙이는 패딩은 $896 - 512 = 384$비트이다. **128비트 길이 필드는 이 계산에서 제외**한다.

계산 과정

① 기준: SHA-512의 입력 블록은 1024비트이고, 마지막 128비트는 원래 메시지 길이를 기록하는 필드이다. 먼저 1비트의 1과 필요한 수의 0을 붙여 길이가 블록 기준 **896비트 지점**에 이르게 한다. 메시지 길이를 L, 덧붙이는 0의 수를 k라 하면 L+1+k≡896±od1024를 만족하는 최소 음이 아닌 k를 구한다.

② 대입: $2560 = 2 \times 1024 + 512$이므로 현재 마지막 블록에는 512비트가 있다. 따라서 $512 + 1 + k = 896$에서 $k = 383$이다. 길이 필드 앞에 붙이는 1과 0의 총 길이는 $1 + 383 = 384$비트이다.

③ 검산과 범위: 길이 필드를 붙이기 전에는 $2560 + 384 = 2944$비트이고, 128비트 길이 필드까지 붙이면 $3072 = 3 \times 1024$비트가 되어 블록 경계와 맞는다. 이 문항의 인정 정답은 **길이 필드를 제외한 패딩** 384비트이다. 길이 필드까지 포함한 전체 추가 길이를 묻는다면 $384 + 128 = 512$비트이므로 범위를 구별해야 한다.

따라서 길이 필드 앞에 추가하는 패딩은 384비트로 ②에 해당한다.

NoteBase

문 10. 보안솔루션에 대한 설명으로 가장 적절하지 않은 것은?

① VLAN - 인터넷 회선을 임대회선처럼 사용할 수 있게 해주는 솔루션

② NAC - MAC 주소를 기반으로 접근제어 및 인증을 수행하는 솔루션

③ DLP - 사용자 수준에서 정보가 유출되는 것을 막는 솔루션

④ PC 방화벽 - 네크워크상의 웜이나 공격자로부터 PC를 보호하는 솔루션

정답 1번

간단한 해설

공중망을 이용한 사설 연결은 VPN, 논리적 LAN 분리는 VLAN이다. 두 기술의 목적을 바꾸어 설명한 부분을 찾는다.

선지별 해설

① X: 인터넷 등 공중망을 이용해 사설 통신망과 유사한 연결을 제공하는 것은 VPN이다. VLAN은 스위치 네트워크를 **논리적인 브로드캐스트 도메인으로 분리**하는 기술로, 인터넷 회선을 임대회선처럼 쓰게 하는 VPN과 다르다.

② O: NAC는 네트워크에 접속하는 사용자·단말을 식별하고 정책에 따라 접근을 허용하거나 제한한다. 단말의 MAC 주소를 등록·대조하는 방식도 활용할 수 있다. 다만 MAC 주소만 사용하는 것이 NAC의 전부는 아니며, 인증서·사용자 인증·단말 보안 상태 점검 등을 결합할 수 있고 MAC 주소 위조 위험도 고려해야 한다.

③ O: DLP는 민감한 정보의 외부 전송·복사·반출 등을 탐지하고 통제하여 정보 유출을 방지한다. 사용자 단말의 복사·출력·전송 같은 행위를 통제하는 방식도 포함되며, 네트워크나 저장소 수준에도 적용할 수 있다.

④ O: PC 방화벽은 해당 호스트의 송수신 통신을 정책에 따라 허용하거나 차단하여 네트워크를 통한 비인가 접근과 공격 노출을 줄인다. 모든 웜·악성코드를 단독으로 막는다는 뜻은 아니므로 패치와 악성코드 방어 등도 함께 필요하다.

따라서 VLAN에 VPN의 기능을 연결한 ①이 적절하지 않다.

NoteBase

문 11. 침해 대응 절차의 순서로 가장 적절한 것은?

가. 대응
나. 사고 탐지
다. 사전 대응
라. 제거 및 복구
마. 침해 사고 발생
바. 후속 조치 및 보고

① 나→가→다→라→마→바
② 나→다→라→마→가→바
③ 다→나→마→가→라→바
④ 다→마→나→가→라→바

정답 4번

간단한 해설

준비는 발생 전에, 탐지는 발생 후에 놓는다. 사고를 탐지하면 대응하여 확산을 억제하고, 원인을 제거·복구한 다음 후속 정리와 개선으로 이어진다.

올바른 순서

올바른 순서: 다 → 마 → 나 → 가 → 라 → 바

다. 사전 대응: 사고가 일어나기 전에 대응 조직·연락 체계·절차·도구 등을 준비한다. 여기서 사전 대응은 사고를 탐지한 후의 현장 대응이 아니라 준비 단계이다.

마. 침해 사고 발생 → 나. 사고 탐지: 실제 침해가 발생한 뒤 로그·보안 경보·신고 등을 통해 이를 발견하고 분석한다. 사고 발생과 탐지는 같은 순간일 필요가 없으며, 발생했더라도 일정 시간 발견하지 못할 수 있다.

가. 대응 → 라. 제거 및 복구: 탐지한 사고의 범위와 영향을 파악하여 피해 확산을 억제한 뒤, 침해 원인이나 악성 요소를 제거하고 정상 서비스를 회복한다. 복구에만 급히 착수하고 원인을 남기면 재침해될 수 있다.

바. 후속 조치 및 보고: 처리 결과와 원인을 정리하고 개선책을 반영한다. 이 순서는 문제에 제시된 단계의 대표 흐름이며, 실제 대응에서는 분석·대응·복구가 반복될 수 있고 필요한 중간 보고를 마지막까지 미룬다는 뜻은 아니다.

NoteBase

문 12. RSA의 암호화와 복호화는 다음과 같다. RSA에 대한 공격 방법으로 가장 적절하지 않은 것은?

암호문 = (평문)^E N
평문 = (암호문)^D N
$N = p \times q$ (단, p와 q는 소수)

① p와 q를 추측하는 공격

② E와 N으로부터 D를 구하는 공격

③ 전사 공격

④ 차분 공격

정답 4번

간단한 해설

RSA에서는 **소인수나 개인 지수를 알아내는 시도와 키 후보 전수 탐색**이 공격 방법에 해당한다. 평문·암호문 쌍의 차이를 분석하는 고전적 차분 암호분석은 주로 대칭키 블록암호를 대상으로 한다.

선지별 해설

① O: 공개된 모듈러스 $N = pq$의 소인수인 p, q를 알아내면 개인 지수를 계산하는 데 필요한 수론적 정보를 얻을 수 있다. 통상 두 소수가 서로 다른 RSA에서는 $\lambda(N) = \mathrm{lcm}(p-1, q-1)$을 구하고 ED≡1±odλ(N)을 만족하는 D를 계산한다. 따라서 소인수 추정·분해는 RSA를 겨냥하는 공격이다.

② O: E, N은 공개키 정보이고 D는 비밀로 보호하는 복호화 지수이다. 공개 정보로부터 **개인 지수 도출을 시도**하는 것은 RSA 공격에 해당한다. 공격 목표라는 뜻이지, 적절히 생성된 큰 키에서도 쉽게 계산된다는 뜻은 아니다.

③ O: 전사 공격은 가능한 키 후보를 차례로 시험하는 완전 탐색이다. RSA에도 원리적으로 시도할 수 있지만 충분히 큰 키에서는 탐색량 때문에 현실적으로 어렵다. 적용 가능한 공격 방식과 효율적으로 성공 가능한 공격을 구별해야 한다.

④ X: 여기서 차분 공격은 평문 쌍의 차이와 암호문 쌍의 차이 사이의 통계적 관계를 이용하는 **고전적 차분 암호분석**을 뜻한다. 이는 주로 대칭키 블록암호 분석에 사용되므로 제시된 RSA의 소인수·개인키 탐색 공격과 가장 거리가 멀다. 이름에 차분이 들어가는 전력 분석이나 오류 분석 같은 구현 공격까지 RSA에 불가능하다는 뜻은 아니다.

따라서 문제의 일반적인 암호분석 분류에서 가장 적절하지 않은 것은 ④ 차분 공격이다.

NoteBase

문 13. 평문과 같은 길이의 난수 키를 사용하는 고전적 암호 알고리즘으로, 완전 암호(또는 완벽한 보안)라고도 불리는 암호 알고리즘으로 가장 적절한 것은?

① 버냄(Vernam) 암호

② 시저(Caesar) 암호

③ 플레이페어(Playfair) 암호

④ 힐(Hill) 암호

정답 1번

간단한 해설

버냄 암호를 **평문 길이의 진정한 난수 키를 비밀로 유지하고 한 번만 쓰는 일회용 패드**로 운용하면 완전 비밀성이 성립한다.

대응 관계 해설

조건과 암호의 대응: 평문과 같은 길이의 무작위 키를 평문과 결합하는 버냄 암호를 일회용 패드 방식으로 사용하면 완전 비밀성을 얻는다. 이 문항의 난수 키 길이와 완벽한 보안이라는 두 단서는 이 방식에 대응한다.

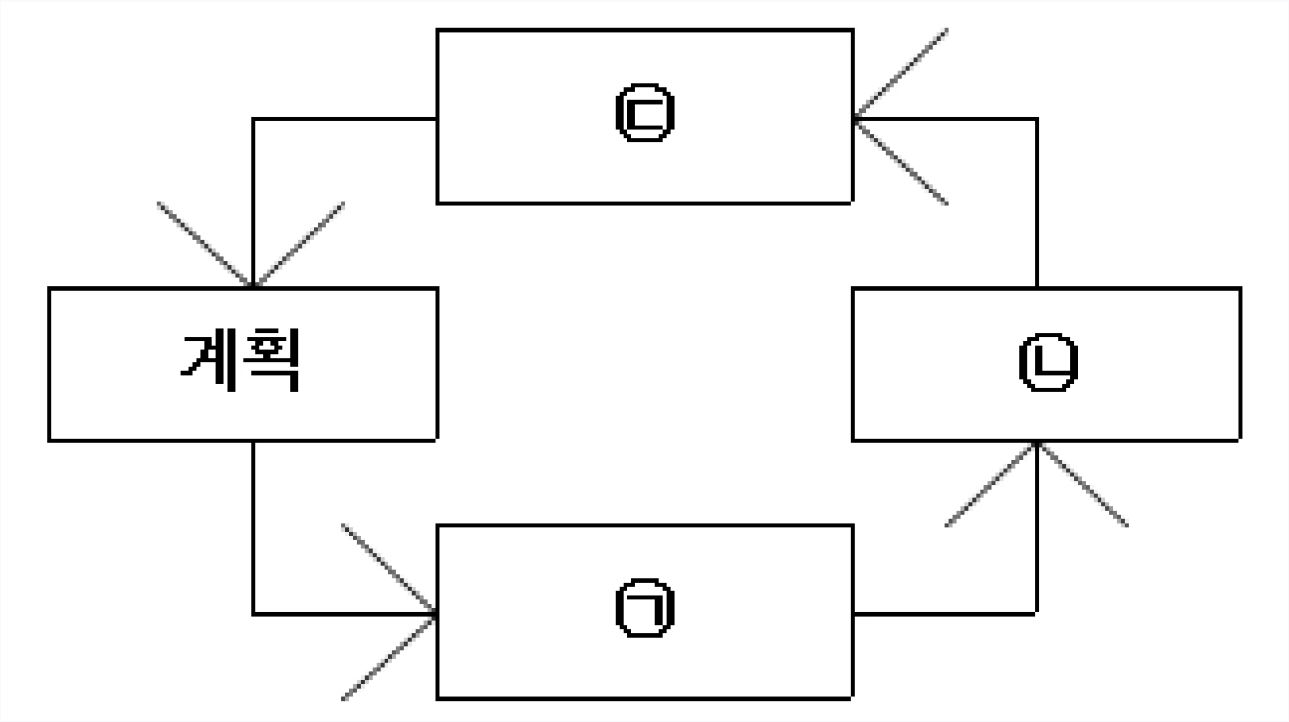
완전 비밀성의 조건: 키는 **평문과 독립적으로 균등·무작위 생성하고 비밀로 유지하며 한 번만 사용**해야 한다. 평문만큼 긴 키라는 조건만으로 충분하지 않고, 의사난수의 반복이나 키 재사용으로 이론적 완전 비밀성이 자동 성립하는 것도 아니다.

시저 암호는 알파벳을 일정 거리 이동시키는 단일 치환 방식이고, 플레이페어 암호는 두 문자씩 묶어 키 표에 따라 치환한다. 힐 암호는 문자 묶음에 키 행렬의 선형 변환을 적용한다. 이들은 문항의 일회용 무작위 키 조건을 특징으로 하는 방식과 다르다.

따라서 제시된 조건에 대응하는 선택지는 ① 버냄(Vernam) 암호이다.

NoteBase

문 14. 다음은 ISO27001의 반복 프로세스로 ㉠, ㉡, ㉢에 들어갈 적절한 용어를 순서대로 나열한 것은?



① ㉠: 처리, ㉡: 점검, ㉢: 실행

② ㉠: 처리, ㉡: 실행, ㉢: 점검

③ ㉠: 실행, ㉡: 점검, ㉢: 처리

④ ㉠: 실행, ㉡: 처리, ㉢: 점검

정답 3번

간단한 해설

제시된 그림은 **PDCA: Plan–Do–Check–Act**의 반복 구조이다. 계획한 내용을 실행하고, 결과를 점검한 뒤, 개선 조치를 다음 계획에 반영한다.

NoteBase

올바른 순서

올바른 순서: 계획 → ㉠ 실행 → ㉡ 점검 → ㉢ 처리·개선 → 계획

계획(Plan): 정보보호의 목표와 방침을 정하고 위험에 대응할 절차와 통제 방안을 마련한다. 그림에서는 왼쪽의 계획에서 아래쪽 ㉠으로 화살표가 이어진다.

㉠ 실행(Do): 계획한 통제와 절차를 실제로 구현하고 운영한다. 계획만 세우는 것이 아니라 업무에 적용하는 단계이다. 아래쪽 ㉠에서 오른쪽 ㉡으로 이어진다.

㉡ 점검(Check): 운영 결과를 모니터링하고 평가하여 목표에 맞는지, 통제가 효과적인지 확인한다. 점검한 결과가 다음의 개선 조치를 위한 근거가 되므로 실행과 처리 사이에 놓인다.

㉢ 처리·개선(Act): 점검에서 발견한 문제에 시정·개선 조치를 취하고 그 결과를 다음 계획에 반영한다. 위쪽 ㉢에서 왼쪽 계획으로 돌아가는 화살표는 **지속적인 개선의 반복**을 나타낸다. 처리라는 말은 실행을 다시 수행한다는 뜻이 아니라 점검 결과에 따른 개선에 해당한다.

NoteBase

문 15. 하이브리드 암호시스템에 대한 설명으로 옳은 것만을 모두 고른 것으로 가장 적절한 것은?

가. 세션키는 송신자의 공개키로 암호화한다.
나. 세션키는 의사난수 생성기로 생성할 수 있다.
다. 평문과 세션키는 각각 암호화하여 수신자에게 전송한다.
라. 평문은 수신자와 사전 공유된 세션키로 암호화한다.

① 가, 나
② 나, 다
③ 가, 다, 라
④ 나, 다, 라

정답 2번

간단한 해설

전형적인 하이브리드 키 전송에서는 **평문은 세션키로, 세션키는 수신자의 공개키로 암호화**한다. 세션키는 안전하게 새로 생성해 전달하므로 사전 공유가 필수인 구조가 아니다.

보기별 해설

가. X: 세션키는 송신자의 공개키가 아니라 **수신자의 공개키**로 암호화한다. 그래야 대응하는 개인키를 가진 수신자가 세션키를 복원할 수 있다. 송신자의 개인키를 사용하는 서명과 수신자에게 키를 비밀 전달하는 절차를 구별한다.

나. O: 세션키는 적절한 암호학적 의사난수 생성기를 통해 생성할 수 있다. 일반적인 예측 가능한 난수 함수가 아니라 충분한 엔트로피와 예측 저항성을 갖춘 생성 방식이어야 한다.

다. O: 이 문항의 전형적인 키 전송형 하이브리드 구성에서는 평문은 대칭 세션키로 암호화하고, 세션키는 수신자의 공개키로 암호화한다. 두 암호화 결과를 함께 보내 대용량 데이터 처리의 효율성과 키 전달의 편의성을 결합한다.

라. X: 여기서는 송신자가 생성한 세션키를 공개키 암호로 보호해 전달하므로, 수신자와 세션키를 **미리 공유해 두는 것**을 전제로 하지 않는다. 수신자는 전달받은 암호화 세션키를 자신의 개인키로 복원한 뒤 평문을 복호화한다.

따라서 옳은 설명은 나와 다이며, 이에 해당하는 조합은 ②이다.

NoteBase

문 16. 속성기반 접근제어(Attribute-Based Access Control)에서 “정보가 객체 사이를 이동하거나 시스템 상태를 변경하도록 하는 능동적 존재”에 대한 속성 유형으로 가장 적절한 것은?

① 주체 속성

② 객체 속성

③ 관리 속성

④ 환경 속성

정답 1번

간단한 해설

객체 사이의 정보 이동이나 시스템 상태 변화를 일으키는 능동적 존재는 **주체**이다. 그 존재의 특성을 나타내는 것이므로 **주체 속성**에 해당한다.

공통 해설

속성 유형은 그 속성이 설명하는 대상을 기준으로 구분한다. 접근제어에서 주체는 객체에 대한 연산을 요청하거나 수행하여 정보 흐름이나 시스템 상태 변화를 일으키는 **능동적 존재**이다. 따라서 발문에서 설명한 존재에 관한 속성은 '주체 속성'이다.

예를 들어 사용자가 파일의 내용을 수정하는 경우, 수정 행위를 수행하는 사용자는 주체이고 수정 대상인 파일은 객체이다. 이때 사용자를 식별하는 정보는 **행위자에 관한 속성**이므로 주체 속성으로 분류한다. 발문도 이러한 행위자를 설명하므로, 객체나 관리·환경에 관한 속성과 구별된다.

NoteBase

문 17. 강제적 접근제어 모델에 대한 설명으로 옳은 것을 고른 것으로 가장 적절한 것은?

가. 벨 라파둘라 모델에서는 자신의 권한보다 높은 보안 레벨의 문서는 읽을 수 없다.
나. 벨 라파둘라 모델에서는 자신의 권한보다 높은 보안 레벨의 문서에는 쓰기 권한이 없다.
다. 비바 모델에서는 무결성 레벨 2인 사람이 신뢰도가 더 높은 무결성 레벨 1의 정보를 읽을 수 있다.
라. 비바 모델에서는 무결성 레벨 2의 정보를 신뢰도가 더 높은 무결성 레벨 1의 문서에 쓰는 것이 가능하다.

① 가, 다
② 가, 라
③ 나, 다
④ 나, 라

정답 1번

간단한 해설

벨 라파둘라: 상향 읽기·하향 쓰기 금지, 비바: 하향 읽기·상향 쓰기 금지를 구별한다. 이 문항에서는 숫자 크기가 아니라 명시된 신뢰도 관계로 비바의 위·아래를 판단한다.

보기별 해설

가. O: 벨 라파둘라 모델은 기밀성을 보호한다. 단순 보안 속성인 **No Read Up**에 따라 주체는 자신의 허용 보안 등급보다 높은 객체를 읽지 못한다.

나. X: 벨 라파둘라 모델의 별표 속성은 No Write Down, 즉 낮은 보안 등급으로의 쓰기를 금지하여 비밀정보의 하향 유출을 막는다. 높은 등급으로의 쓰기를 금지하는 규칙이 아니다. 다만 이 규칙이 모든 실제 쓰기 권한을 자동 부여한다는 뜻은 아니다.

다. O: 엄격한 비바 무결성 모델은 낮은 신뢰도의 정보가 높은 신뢰도의 처리를 오염시키지 못하도록 No Read Down을 적용한다. 이 문항은 숫자 1이 2보다 신뢰도가 높다고 명시하므로, 레벨 2의 주체가 더 높은 무결성 레벨 1의 정보를 읽는 것은 허용 방향이다.

라. X: 비바 모델의 **No Write Up**은 낮은 무결성의 주체가 더 높은 무결성 객체에 쓰는 것을 막는다. 레벨 2의 정보로 더 신뢰도가 높은 레벨 1의 문서를 변경하게 하면 고무결성 자료가 오염될 수 있으므로 제시된 방향은 금지된다.

따라서 옳은 설명은 가와 다이며, 그 조합은 ①이다.

NoteBase

문 18. NIST SP800-53 보안 통제의 클래스에 포함되는 것으로 가장 적절하지 않은 것은?

① 관리적 통제

② 운영적 통제

③ 기술적 통제

④ 활용적 통제

정답 4번

간단한 해설

문항은 **관리적·운영적·기술적 통제**라는 전통적인 세 클래스의 명칭을 묻는다. 활용적 통제는 여기에 포함되지 않는다. 판본에 따른 분류 표기 변화와 구별해야 한다.

선지별 해설

① O: 관리적 통제는 보안 정책·계획·위험평가 등 **위험을 관리하고 의사결정을 하는 활동**에 초점을 둔다. 문제에서 묻는 전통적인 세 클래스 중 하나이다.

② O: 운영적 통제는 주로 사람이 수행하는 절차와 운영 활동에 초점을 둔다. 교육·훈련, 인적 보안, 사고 대응 활동 등이 대표적인 설명이다. 실제 활동에 기술 도구가 함께 쓰이지 않는다는 뜻은 아니다.

③ O: 기술적 통제는 하드웨어·소프트웨어 등 시스템이 수행하는 보안 기능에 초점을 둔다. 자동화된 인증·접근 통제 등의 기능으로 이해할 수 있다. 관리적·운영적 측면과 완전히 분리된다는 뜻은 아니다.

④ X: 문제의 전통적인 클래스 분류는 **관리적·운영적·기술적 통제**이다. 활용적 통제는 이 세 클래스에 포함되는 명칭이 아니다.

판본 구별: 이 세 클래스는 SP 800-53 Rev.3 등에 제시된 전통적 분류이다. Rev.4에서는 한 통제에 관리적·운영적·기술적 성격이 함께 있을 수 있다는 점을 반영하여 통제 패밀리에 붙이던 특정 클래스 표기를 제거했다. 따라서 이를 최신 판본에서 각 패밀리를 반드시 하나의 클래스로 고정하는 규칙으로 외우면 안 된다.

따라서 이 문항의 전통적인 세 클래스에 해당하지 않는 ④ 활용적 통제가 정답이다.

NoteBase

문 19. 다음은 해시 함수(hash function)의 충돌 내성에 대한 설명이다. 이에 해당하는 공격 방법으로 가장 적절한 것은?

일방향 해시 함수는 어느 메시지의 해시 값이 주어졌을 때 그 해시 값을 갖는 다른 메시지를 발견하는 것이 매우 어렵다.

① 전사 공격
② 시간 공격
③ 사전 공격
④ 중간자 공격

정답 1번

간단한 해설

목표 해시 값과 일치하는 메시지를 찾기 위해 **가능한 후보를 하나씩 대입**하는 방법이 전사 공격이다. 해시 값을 직접 거꾸로 계산하는 대신, 후보의 해시 값을 계산해 목표 값과 비교한다.

핵심 풀이

전사 공격: 가능한 후보를 빠짐없이 시험하는 무차별 대입 방식이다. 이 문제에 적용하면 후보 메시지의 해시 값을 계산하고, 주어진 목표 해시 값과 같은지 확인하는 과정을 반복한다. 원래 메시지가 주어져 있고 그와 다른 메시지를 찾는 경우에는 원래 메시지를 후보에서 제외한다. 해시 함수의 역변환을 구하는 것이 아니라 **후보를 대입하고 결과를 비교**하는 공격이다.

사전 공격과의 구분: 사전 공격은 자주 쓰는 단어나 비밀번호 등 미리 준비한 목록으로 후보를 제한한다. 제시문에는 후보가 그러한 목록에 속한다는 조건이 없으므로, 특정 사전에 의존하지 않고 가능한 후보를 탐색하는 전사 공격이 적절하다.

해시 내성의 구분: 엄밀히는 **해시 값만 주어진 상태**에서 그 값을 만드는 메시지를 찾기 어려운 성질이 역상 내성이다. 특정 메시지가 주어진 상태에서 같은 해시 값을 갖는 다른 메시지를 찾기 어려운 성질은 제2역상 내성이다. 충돌 내성은 어느 한 메시지나 목표 해시 값을 미리 고정하지 않고, 해시 값이 같은 서로 다른 두 메시지를 찾기 어려운 성질이다. 발문의 '충돌 내성'이라는 명칭과 달리, 제시문은 목표 해시 값이 먼저 주어진 조건을 설명한다. 이러한 용어 구분과 별개로, 목표 값에 맞는 후보를 반복해서 시험하는 전사 공격을 적용할 수 있다.

NoteBase

문 20. 능동적 보안 공격으로 옳은 것을 고른 것으로 가장 적절한 것은?

가. 도청
나. 삽입 공격
다. 메시지 변조
라. 트래픽 분석

① 가, 다
② 나, 다
③ 나, 라
④ 다, 라

정답 2번

간단한 해설

흐름을 변경하거나 새 데이터를 추가하는지가 기준이다. 삽입과 메시지 변조는 능동적 공격이고, 내용을 엿듣거나 통신 양상을 관찰하는 것은 수동적 공격이다.

보기별 해설

가. X: 도청은 통신 내용을 몰래 읽는 행위이다. 관찰 대상인 메시지나 데이터 흐름 자체를 변경하지 않으므로 **수동적 공격**으로 분류한다. 기밀성을 침해한다는 피해의 크기와 능동·수동 분류는 별개의 기준이다.

나. O: 삽입 공격은 공격자가 만들어 낸 메시지나 데이터를 흐름에 끼워 넣는 행위이다. 단순히 관찰하는 것이 아니라 **원래 없던 내용을 추가하여 흐름에 개입**하므로 능동적 공격이다.

다. O: 메시지 변조는 전송되는 내용 등을 바꾸는 행위이다. 원래의 데이터를 변경하여 무결성을 침해하므로 능동적 공격에 해당한다.

라. X: 트래픽 분석은 통신량·시간·빈도·송수신 관계 등을 관찰하여 정보를 추론한다. 메시지를 해독하지 못해도 가능하며, 관찰만으로 수행하는 이 분류에서는 **수동적 공격**이다. 공격자가 별도로 트래픽을 삽입하거나 바꾸는 행위와 구별한다.

따라서 능동적 보안 공격은 나·다이므로 ②가 적절하다.

NoteBase

문 21. 디지털 서명에 대한 설명으로 옳은 것을 고른 것으로 가장 적절한 것은?

가. 기밀성 보장이 가능하다.
나. 무결성 검증이 가능하다.
다. 부인하는 것을 방지할 수 있다.
라. 디지털 서명은 공개키로 생성한다.

① 가, 나
② 가, 라
③ 나, 다
④ 다, 라

정답 3번

간단한 해설

디지털 서명은 **개인키로 생성하고 공개키로 검증**하며, 무결성과 부인방지를 지원한다. 내용의 기밀성은 서명만으로 제공되지 않는다.

보기별 해설

가. X: 디지털 서명 자체는 메시지 내용을 숨기지 않으므로 기밀성을 제공하지 않는다. 서명된 평문은 그대로 읽힐 수 있으며, 기밀성이 필요하면 별도의 암호화와 결합해야 한다.

나. O: 서명은 메시지 내용과 연결되어 검증되므로 서명 이후 메시지가 변경되었는지 확인하는 **무결성 검증**을 지원한다. 유효한 서명이 검증되는지는 올바른 공개키와 안전한 알고리즘을 사용하는 등의 전제에 따른다.

다. O: 서명자의 개인키로 생성한 서명은 해당 서명자가 메시지에 서명했다는 증거를 제공하여 **서명 사실의 부인방지**를 지원한다. 이를 위해 개인키 보호와 공개키의 신뢰할 수 있는 신원 연결 등이 필요하다.

라. X: 디지털 서명은 서명자의 개인키로 생성하고 대응하는 공개키로 검증한다. 공개키는 배포될 수 있으므로 공개키만으로 누구나 해당 서명을 생성할 수 있는 구조여서는 안 된다.

따라서 옳은 설명은 나와 다이며, 그 조합은 ③이다.

NoteBase

문 22. 암호모듈 검증제도로 국가·공공기관에서 도입하는 암호모듈의 안전성과 구현 적합성을 검증하는 제도로 가장 적절한 것은?

① CC

② GDPR

③ CCRA

④ KCMVP

정답 4번

간단한 해설

국가·공공기관이 도입하는 암호모듈의 **안전성과 구현 적합성**을 검증하는 국내 제도는 KCMVP이다.

공통 해설

KCMVP(Korea Cryptographic Module Validation Program)는 국가·공공기관에서 도입하는 암호모듈의 안전성과 구현 적합성을 검증하는 제도이다. 암호모듈은 암호화·복호화 등 암호 기능을 수행하도록 구현한 소프트웨어나 하드웨어 구성 요소를 말한다.

검증 대상은 암호 알고리즘의 명칭 자체가 아니라 **암호 기능을 실제로 구현한 모듈**이다. 즉, 암호 기능을 적합하게 구현했는지와 모듈이 안전한지를 확인한다. 발문에 제시된 대상이 국가·공공기관에 도입하는 암호모듈이고, 확인할 사항이 안전성과 구현 적합성이므로 이 설명은 KCMVP에 해당한다.

NoteBase

문 23. 다음 설명에 해당하는 포렌식 종류로 가장 적절한 것은?

운영체제, 서비스, 응용 프로그램을 분석하여 증거를 확보하는 것으로 분석 대상 정보시스템에 따라 윈도우 포렌식, 리눅스 포렌식, 유닉스 포렌식 등으로 분류할 수 있다.

① 디스크 포렌식
② 시스템 포렌식
③ 네트워크 포렌식
④ 데이터베이스 포렌식

정답 2번

간단한 해설

운영체제·서비스·응용 프로그램의 흔적을 분석하고 윈도우·리눅스·유닉스 등으로 구분하는 것은 시스템 포렌식이다.

대응 관계 해설

설명과 개념의 대응: 운영체제와 그 위에서 동작하는 서비스·응용 프로그램의 흔적을 분석하여 증거를 확보하는 것은 시스템 포렌식이다. **윈도우·리눅스·유닉스와 같이 대상 시스템의 운영체제에 따라 구분**한다는 단서가 이를 뒷받침한다.

디스크 포렌식과의 구분: 디스크 등 저장매체의 파일시스템, 파일, 삭제 영역과 저장 흔적을 분석하는 데 초점을 둔다. 시스템 포렌식도 디스크에서 얻은 자료를 활용할 수 있지만 제시문의 분류 기준은 저장매체 자체가 아니라 운영체제·서비스 환경이다.

네트워크 포렌식과의 구분: 패킷, 통신 흐름, 네트워크 장비와 통신 로그 등을 분석하여 송수신 활동과 침입 흔적을 재구성한다.

데이터베이스 포렌식과의 구분: DBMS의 데이터와 트랜잭션·감사 로그, 변경·삭제 흔적 등을 분석한다. 여러 포렌식 분야는 실제 조사에서 결합될 수 있으나 이 문항의 운영체제별 분류 단서와 가장 직접 연결되는 것은 시스템 포렌식이다.

따라서 제시된 설명은 ② 시스템 포렌식에 해당한다.

NoteBase

문 24. 영지식 인증(Zero-Knowledge Authentication)에서 사용되는 프로토콜로 가장 적절하지 않은 것은?

① Fiat-Shamir 프로토콜

② Feige-Fiat-Shamir 프로토콜

③ Guillou-Quisquater 프로토콜

④ Needham-Schroeder 프로토롤

정답 4번

간단한 해설

Fiat–Shamir, Feige–Fiat–Shamir, Guillou–Quisquater는 **비밀의 지식에 대한 증명 기반 식별**에 해당한다. Needham–Schroeder는 암호화 메시지 교환을 통한 인증·키 설정 계열로 구별한다.

선지별 해설

① O: Fiat–Shamir 인증 프로토콜은 난수를 이용한 약속과 도전·응답을 통해 **비밀값을 직접 공개하지 않고 알고 있음을 증명**하는 대표적인 식별 방식이다. 여기서는 인증 프로토콜을 가리키며, 대화형 증명을 해시로 비대화형화하는 동명의 변환과 구별한다.

② O: Feige–Fiat–Shamir는 여러 비밀값에 대한 도전·응답을 사용하는 영지식 식별 프로토콜이다. 검증자가 비밀값 자체를 전달받아 비교하는 방식이 아니라, 응답이 공개 정보와 수학적으로 일관되는지 확인한다.

③ O: Guillou–Quisquater는 RSA형 모듈러 거듭제곱 관계를 이용하는 식별 프로토콜이다. 비밀값을 공개하지 않고 그 보유를 증명하는 도전·응답 방식으로 이 문항의 영지식 인증 계열에 포함된다. 단순히 데이터를 암호화해서 전송하는 것과 구별된다.

④ X: Needham–Schroeder는 암호화된 메시지 교환에 기반한 인증·키 설정 계열의 프로토콜이다. **영지식 증명으로 비밀의 지식을 입증하는 대표 프로토콜로 분류하지 않는다**. 인증에 암호를 사용하고 비밀키를 직접 보내지 않는다는 사실만으로 모든 인증 절차가 영지식 증명이 되는 것은 아니다.

따라서 영지식 인증 프로토콜로 가장 적절하지 않은 것은 ④ Needham–Schroeder이다.

NoteBase

문 25. PKI의 구성 요소 중 인증 기관(CA)에 대한 설명으로 옳은 것만을 모두 고른 것으로 가장 적절한 것은?

가. 인증서를 폐지할 경우 인증서 폐지목록을 작성한다.
나. 이용자의 키 쌍을 생성할 수 있다.
다. 루트 인증 기관은 자신의 공개키에 대해 자신의 개인키로 셀프 서명할 수 있다.
라. 인증 기관의 개인키로 이용자의 디지털 서명을 생성하고 인증서를 발행할 수 있다.

① 가, 다
② 나, 라
③ 나, 다, 라
④ 가, 나, 다, 라

정답 4번

간단한 해설

CA는 **자신의 개인키로 이용자의 인증서에 서명**해 공개키와 이용자의 연결을 보증한다. 라는 이 인증서 서명을 가리킨다고 해석한다. 이용자가 문서에 하는 서명에는 **이용자 자신의 개인키**를 쓴다.

출제 포인트

인증 기관(CA)의 인증서 발급·폐지 기능과 키 생성, 루트 인증서의 자체 서명을 구별하는 문제이다.

핵심 개념

PKI는 공개키와 그 소유자의 신원을 인증서로 연결하는 공개키 기반 구조이다. CA는 이 연결을 보증하는 인증 기관으로, 인증서를 발급하고 폐지 정보를 관리한다.
인증서 서명은 CA가 인증서 내용에 하는 서명이고, 이용자의 문서 서명은 이용자가 자신의 문서에 하는 서명이다. 두 서명은 사용하는 개인키와 서명 대상이 다르다.

NoteBase

보기별 판단

가 O: 인증서를 유효기간 중 폐지하면 CRL(인증서 폐지목록)에 폐지 정보를 반영한다. CRL은 폐지된 인증서를 확인하는 데 쓰인다.
나 O: 키 쌍은 공개키와 개인키의 한 쌍이다. 이용자가 직접 생성할 수도 있고 CA가 생성할 수도 있으므로 '생성할 수 있다'는 설명이 맞다. CA가 반드시 모든 이용자의 키를 생성한다는 뜻은 아니다.
다 O: 루트 CA는 자신의 공개키가 담긴 인증서에 그 공개키와 짝을 이루는 자신의 개인키로 자체 서명할 수 있다. 이를 셀프 서명이라고 한다.
라 O(인증서 서명 문맥): CA는 자신의 개인키로 이용자의 공개키와 신원 정보가 담긴 인증서에 서명하여 발급한다. 제공된 정답에서는 '이용자의 디지털 서명'을 이용자에게 발급하는 인증서에 붙이는 CA의 서명으로 해석한다. 이용자가 문서에 하는 서명 자체를 CA의 개인키로 생성한다는 뜻으로 이해하면 안 된다.

선지별 해설

① X: 가와 다의 기능은 맞지만 CA가 이용자의 키 쌍을 생성할 수 있다는 나와, 인증서 서명 문맥의 라를 빠뜨렸다. 해당 문맥에서는 가·나·다·라를 모두 포함해야 한다.
② X: 나와 라만 고르면 인증서 폐지목록을 작성하는 가와 루트 CA의 자체 서명을 설명한 다가 누락된다. 가와 다도 포함해야 한다.
③ X: 나·다·라에 더해 인증서 폐지목록을 작성한다는 가도 포함해야 한다. 인증서 폐지 정보 관리 역시 CA의 기능이다.
④ O: 가·나·다는 CA의 기능으로 성립하고, 라를 이용자의 인증서에 CA가 서명한다는 의미로 해석하면 네 보기를 모두 포함한 조합이 적절하다.

오답 포인트

나의 '생성할 수 있다'를 '반드시 생성한다'로 읽으면 CA의 가능한 기능을 잘못 제외하게 된다. 라의 '이용자의 디지털 서명'은 표현에 주의가 필요하다. 인증서에는 CA의 개인키로 서명하지만, 이용자의 문서에는 이용자 자신의 개인키로 서명한다.

다시 나오면 이렇게 판단

서명 주체, 개인키의 소유자, 서명 대상을 함께 확인한다. CA의 인증서 서명과 이용자의 문서 서명을 구별하고, 조합형 문제에서는 성립하는 보기가 누락되었는지도 확인한다.

암기 포인트

인증서 서명은 CA의 개인키, 이용자 문서 서명은 이용자의 개인키. 루트 CA는 자체 서명, 폐지 정보는 CRL.

NoteBase

문 26. 공통평가기준(CC)에 대한 설명으로 옳은 것만을 모두 고른 것으로 가장 적절한 것은?

가. 평가 결과는 가입국 간 상호 인정된다.
나. EAL4는 방법론적 설계, 시험, 검토에 대한 평가보증등급이다.
다. IT 제품이나 정보시스템의 보안성 평가를 위한 국제 표준이다.
라. 구성 요소에는 평가대상, 보호 프로파일, 보안목표 명세서, 평가보증등급이 있다.

① 가, 다
② 나, 라
③ 나, 다, 라
④ 가, 나, 다, 라

정답 4번

간단한 해설

CC는 **TOE·PP·ST와 보증 요구사항으로 IT 보안성을 평가**하는 공통 기준이다. EAL4는 방법론적 설계·시험·검토 수준이고 상호인정은 협정의 정해진 범위에서 이루어진다.

보기별 해설

가. O: CC 평가·인증 결과는 CCRA 등 상호인정 협정의 범위에서 참여국 사이에 인정될 수 있다. 이는 모든 등급과 모든 결과를 무제한 인정한다는 뜻은 아니며, 협정의 보증 수준과 보호 프로파일 등 적용 조건을 따른다.

나. O: EAL4의 명칭은 **Methodically Designed, Tested, and Reviewed**로, 방법론적으로 설계·시험·검토되었음을 평가하는 보증 수준이다. EAL은 제품이 제공하는 보안 기능의 종류 자체가 아니라 평가의 엄격성과 보증 수준을 구별한다.

다. O: CC는 IT 제품·시스템의 보안 기능과 보증 요구사항을 공통 기준으로 명세하고 평가하기 위한 국제 기준으로, ISO/IEC 15408과 연결된다.

라. O: TOE는 평가대상, PP는 특정 구현과 독립된 공통 보안 요구사항을 담는 보호 프로파일, ST는 특정 TOE의 보안 요구사항과 주장 등을 담는 보안목표 명세서이다. EAL은 평가보증등급으로 이들 개념과 함께 CC 평가 체계를 구성한다.

따라서 상호인정의 적용 범위를 전제로 가·나·다·라가 모두 옳으며, 조합은 ④이다.

NoteBase

문 27. 다음 설명에 해당하는 난수의 성질로 가장 적절한 것은?

“과거에 출력한 의사난수열이 공격자에게 알려져도 다음에 출력하는 의사난수를 공격자는 알아낼 수 없다.”는 성질을 말하며 이러한 의사난수를 강한 의사난수라고 한다.

① 규칙성
② 무작위성
③ 예측 불가능성
④ 재현 불가능성

정답 3번

간단한 해설

이미 알려진 과거 출력으로도 **다음 출력값을 예측할 수 없는 성질**이 예측 불가능성이다. 지문의 핵심은 공격자가 이전 의사난수열을 알고 있어도 다음 값을 알아낼 수 없다는 데 있다.

공통 해설

예측 불가능성은 공격자가 지금까지 출력된 의사난수열을 알고 있어도 **다음 출력값을 현실적인 계산 자원으로 알아내기 어려운 성질**이다. 지문은 과거 출력이 공개된 상황에서도 다음 의사난수를 알아낼 수 없다고 했으므로 이 정의에 해당한다. 여기서 '알아낼 수 없다'는 말은 우연히 한 번 맞힐 수 없다는 뜻이 아니라, 과거 출력을 이용하여 다음 값을 효과적으로 예측할 수 없다는 뜻이다.

판단 기준은 **과거 출력으로부터 다음 값을 예측할 수 있는지**이다. 무작위성은 출력값의 분포나 값들 사이의 통계적 관계에 관한 성질이므로, 겉으로 무작위처럼 보인다는 것만으로 예측 불가능성까지 보장되지는 않는다. 규칙성의 유무나 같은 수열을 다시 만들 수 있는지도 지문에서 묻는 다음 값의 예측 가능성과는 구별된다.

NoteBase

문 28. 다음 설명에 해당하는 공격 방법으로 가장 적절하지 않은 것은?

사람들 사이의 신뢰 관계를 바탕으로 사람들을 속여 정상적인 보안 절차를 무시하고 비기술적인 수단으로 정보를 탈취하는 행위를 말하며, 공격 대상에게 어떤 방식으로 접근하는가에 따라 '인간 기반 공격'과 '컴퓨터 기반 공격'으로 구분할 수 있다.

① 피싱

② 파밍

③ 스미싱

④ 서비스 거부 공격

정답 4번

간단한 해설

제시문은 신뢰와 판단을 악용하는 사회공학적 기만을 가리킨다. **서비스 거부 공격은 서비스 가용성을 떨어뜨리는 공격**이라는 점에서 구별된다.

선지별 해설

① O: 피싱은 신뢰할 만한 사람이나 기관을 사칭하여 사용자가 민감한 정보를 제공하거나 위험한 행동을 하도록 유도한다. 사람의 신뢰와 판단을 악용하는 사회공학적 공격의 대표적 예이다.

② O: 파밍은 정상 사이트로 접속한다고 믿는 사용자를 위조 사이트로 유도하여 정보를 입력하게 만드는 공격이다. DNS·호스트 설정 변조 등 기술적 경로 조작이 결합될 수 있지만, 이 문항에서는 위조 사이트를 신뢰하게 하여 정보를 탈취하는 기만의 측면으로 포함한다. 모든 파밍 과정이 비기술적이라는 뜻은 아니다.

③ O: 스미싱은 문자 메시지를 수단으로 사용하는 피싱이다. 배송·결제·공지 등으로 가장한 문자를 믿게 하여 링크 접속이나 정보 제공 등의 행동을 유도한다.

④ X: 서비스 거부 공격의 주된 목적은 자원을 고갈시키거나 처리를 방해하여 **정상 사용자가 서비스를 이용하지 못하게 하는 것**이다. 사람의 신뢰를 이용해 비밀정보를 직접 얻는 사회공학적 기만과 중심 목표·수단이 다르다.

따라서 제시된 사회공학적 공격의 설명과 가장 거리가 먼 것은 ④ 서비스 거부 공격이다.

NoteBase

문 29. 정보보호 관리체계(ISMS)에 대한 설명으로 옳은 것을 고른 것으로 가장 적절한 것은?

가. ISMS 인증 유효기간은 5년이다.
나. 사후심사는 연 1회 이상 수행한다.
다. 최초심사 인증을 받으면 2년 후 사후 심사를 시행한다.
라. 한국인터넷진흥원은 인증서를 발급하고 인증심사원을 양성할 수 있다.

① 가, 나
② 가, 다
③ 나, 라
④ 다, 라

정답 3번

간단한 해설

인증 유효기간 3년과 매년 1회 이상의 사후심사를 구분한다. 한국인터넷진흥원은 인증서 발급과 인증심사원 양성 업무를 수행할 수 있다.

보기별 해설

가. X: ISMS 인증의 유효기간은 **3년**이다. 5년이 아니며, 인증 취득 이후에도 관리체계를 계속 유지하고 사후심사를 받아야 한다.

나. O: 사후심사는 인증받은 관리체계가 지속적으로 유지되는지를 확인하기 위해 **매년 1회 이상** 실시한다. 최초심사에 통과한 것만으로 유효기간 동안의 심사가 모두 면제되는 것은 아니다.

다. X: 인증을 받은 뒤 2년을 기다렸다가 처음 사후심사를 받는 것이 아니다. **매년 1회 이상**이라는 주기에 따라 최초 인증 후에도 첫해부터 사후심사를 받으며, 이후에도 유지 여부를 확인한다.

라. O: 한국인터넷진흥원은 인증기관으로서 인증서 발급 업무를 수행하며, 인증심사원 양성과 자격 관리에도 관여한다. 인증서의 발급과 심사를 수행할 전문인력의 양성은 구별되는 업무이지만, 한국인터넷진흥원이 수행할 수 있는 업무에 모두 포함된다.

따라서 옳은 설명은 나·라이므로 ③이 적절하다.

NoteBase

문 30. 다음 중 국내 블록 암호 알고리즘으로 옳은 것을 고른 것으로 가장 적절한 것은?

가. AES 나. SEED 다. ARIA 라. RC5
마. IDEA 바. HIGHT 사. LEA

① 가, 나, 마, 사
② 나, 다, 바, 사
③ 다, 라, 마, 바
④ 라, 마, 바, 사

정답 2번

간단한 해설

국내 개발 블록 암호는 **SEED·ARIA·HIGHT·LEA**이다. 국내 사용 여부가 아니라 개발 출처를 기준으로 구분한다.

보기별 해설

가. X: AES는 벨기에 연구자들이 개발한 Rijndael을 바탕으로 미국 표준으로 채택된 블록 암호이다. 국내에서 사용하는지와 국내에서 개발했는지를 구분한다.

나. O: SEED는 국내에서 개발한 블록 암호 알고리즘으로 한국인터넷진흥원에서 관련 규격·구현 자료를 제공한다.

다. O: ARIA는 국내에서 개발한 범용 블록 암호 알고리즘이다. 국내 개발 알고리즘을 고르는 기준에 해당한다.

라. X: RC5는 로널드 리베스트가 설계한 블록 암호로 국내 개발 알고리즘이 아니다.

마. X: IDEA는 스위스 취리히 연방공과대학교의 연구진이 개발한 블록 암호로 국내 개발 알고리즘이 아니다.

바. O: HIGHT는 제한된 자원을 갖는 환경을 고려하여 국내에서 개발한 경량 블록 암호 알고리즘이다.

사. O: LEA는 소프트웨어 환경에서 효율적인 처리를 지향하여 국내에서 개발한 블록 암호 알고리즘이다.

따라서 국내 개발 블록 암호는 나(SEED)·다(ARIA)·바(HIGHT)·사(LEA)이며, 해당 조합은 ②이다.

NoteBase

문 31. 다음 설명에 해당하는 위험 분석 방법으로 가장 적절하지 않은 것은?

손실 크기를 화폐가치로 측정할 수 없어 위험을 기술 변수로 표현하는 경우 주관적이며, 근거가 제공되지 않지만 시간, 노력, 비용이 적게 든다.

① 델파이법
② 순위결정법
③ 확률분포법
④ 브레인스토밍

정답 3번

간단한 해설

제시문은 서술·판단 중심의 정성적 위험 분석을 가리킨다. **확률분포를 이용한 수치 모형은 정량적 분석**이라는 점에서 다르다.

선지별 해설

① O: 델파이법은 전문가의 판단을 반복적으로 수렴하여 위험을 평가하는 데 사용할 수 있다. 자료가 부족한 상황에서 정성적 판단을 얻는 방법으로 분류된다.

② O: 순위결정법은 위험이나 대안의 상대적 중요도를 비교하여 우선순위를 매긴다. 손실을 반드시 화폐액으로 계산하지 않고 서열로 표현할 수 있어 정성적 분석의 예에 해당한다.

③ X: 확률분포법은 손실이나 발생 가능성을 확률분포 등의 수치 모형으로 표현하는 **정량적 위험 분석**에 해당한다. 제시문의 서술적 변수와 주관적 판단 중심이라는 정성적 분석 특징과 구별된다.

④ O: 브레인스토밍은 참여자의 경험과 아이디어를 모아 위험요인과 영향을 파악하는 방법으로, 정성적 위험 분석에 활용할 수 있다.

제시문의 정성적 분석이라는 방향은 화폐 측정 대신 서술·서열 등으로 위험을 표현한다는 점에서 판단한다. 다만 정성적 분석에도 자료와 판단 근거를 기록할 수 있으므로 근거가 전혀 없다는 표현을 일반 원칙으로 받아들이지는 않는다. 시간·비용이 항상 적다는 보장도 아니다.

따라서 정성적 분석과 가장 거리가 먼 것은 ③ 확률분포법이다.

NoteBase

문 32. 무선랜 보안 기술에 대한 설명으로 가장 적절하지 않은 것은?

① WPA는 TKIP를 사용한다.

② WEP는 양방향 인증 메커니즘을 제공한다.

③ WPA2는 AES 기반 CCMP를 사용한다.

④ EAP는 인증 서버와 무선 단말기 사이에 상호 인증을 제공한다.

정답 2번

간단한 해설

WPA의 TKIP와 WPA2의 AES 기반 CCMP를 구분한다. **WEP 자체는 상호 인증을 제공하지 않는다**. EAP의 상호 인증 여부는 구체적인 인증 방식에 달려 있다.

선지별 해설

① O: WPA는 WEP를 보완하기 위해 **TKIP**를 도입하였다. 패킷별 키 혼합, 재전송 방지 및 메시지 무결성 검사 등을 추가하지만, TKIP의 암호화 기반은 RC4이다. 역사적 기술 구분이며 현재 사용을 권장한다는 뜻은 아니다.

② X: WEP의 공유키 인증은 접근점이 단말기를 확인하는 방식으로, **단말기와 접근점의 신원을 서로 검증하는 상호 인증을 제공하지 않는다**. 같은 공유키를 사용한다는 사실만으로 양방향 인증이 성립하지 않는다.

③ O: WPA2의 대표적인 암호화·무결성 보호 프로토콜은 **AES 기반 CCMP**이다. TKIP와 CCMP를 각각 WPA와 WPA2의 주요 보호 방식으로 구분한다. 호환 모드 등 구현상의 선택지를 모두 부정하는 의미는 아니다.

④ O: 무선랜 보안에서 사용하는 상호 인증 지원 EAP 방식은 인증 서버와 단말기가 서로를 확인하게 한다. 대표적으로 EAP-TLS가 있다. 다만 **EAP는 인증 방법을 수용하는 프레임워크**이므로 모든 EAP 방식이 상호 인증을 제공하는 것은 아니다. EAP-MD5 같은 단방향 방식과 구별해야 하며, 이 선지는 무선랜 보안에 적합한 EAP 방식의 기능을 설명한 것으로 이해한다.

따라서 WEP가 양방향 인증을 제공한다고 설명한 ②가 가장 적절하지 않다.

NoteBase

문 33. 다음은 Elgamal 디지털 서명의 키 생성단계를 보인다. 이 단계에서 사용된 기호에 대한 설명으로 가장 적절하지 않은 것은?

단계1. p는 Z_p^* 안에서 이산대수를 풀 수 없을 정도로 충분히 큰 값을 선택한다.
단계2. Z_p^* 안의 e_1을 선택한다.
단계3. $p-1$보다 작은 d를 선택한다.
단계4. e_2=e_1^d(p)를 계산한다.

① p는 소수이다.
② e_1은 원시근이다.
③ d는 개인키이다.
④ e_2는 공개키이다.

정답 4번

간단한 해설

e_2는 **공개키의 구성요소**이며 공개키 전체는 (p, e_1, e_2)이다. 공개키 전체를 뜻할 때 e_2 하나만으로 표현하면 부정확하다.

출제 포인트

ElGamal 디지털 서명에서 소수 p, 원시근 e_1, 개인키 d, 공개키 (p, e_1, e_2)의 역할을 구분한다.

핵심 개념

개인키는 서명자가 비밀로 보관하며 서명 생성에 사용하는 값이고, 공개키는 다른 사람이 서명을 검증하도록 공개하는 정보이다.
p는 나머지 연산의 기준인 큰 소수이다. e_1은 p로 나눈 나머지를 기준으로 거듭제곱했을 때 1부터 $p-1$까지의 모든 0이 아닌 나머지를 생성하는 원시근이다.
d는 비밀로 선택하는 지수이다. e_2는 e_1을 d제곱한 뒤 p로 나눈 나머지이며, 공개키에 포함된다. p, e_1, e_2를 알아도 d를 구하기 어렵다는 이산대수 문제의 어려움을 이용한다.

NoteBase

선지별 해설

① O
p는 큰 소수이다. 소수 p를 법으로 하는 0이 아닌 나머지들은 곱셈군을 이루며, ElGamal 키 생성에 이 구조를 사용한다.

② O
e_1은 이 곱셈군의 생성자인 원시근이다. 단순히 집합 안의 임의의 원소라는 뜻이 아니라, 거듭제곱으로 군의 모든 원소를 생성하는 값을 선택한다.

③ O
d는 서명자가 비밀로 보관하는 개인키이다. d로부터 e_2를 계산하지만 d 자체는 공개하지 않는다.

④ X
공개키 전체의 구성을 기준으로 보면, e_2 하나를 공개키 전체라고 설명한 부분이 부정확하다. 공개키는 (p, e_1, e_2)이고, e_2는 그 구성요소라고 고친다. e_2는 공개되는 값이므로 개인키로 바꾸어 이해해서는 안 된다. p와 e_1을 공통 공개 매개변수로 미리 정한 경우에는 e_2를 공개키라고 부르기도 하므로, 공개키 전체와 그 성분을 구분하는 것이 이 문항의 판단 기준이다.

오답 포인트

④의 'e_2는 공개키이다'를 판단할 때, 공개되는 값과 공개키 전체를 혼동하기 쉽다. e_2가 개인키가 되어서 틀린 것이 아니라, 공개키 전체에는 p와 e_1도 포함된다는 구분이 필요하다.

다시 나오면 이렇게 판단

비밀로 선택한 지수 d와, 그 지수로 계산해 공개하는 e_2를 먼저 구분한다. 이어 공개키의 전체 구성을 묻는지, 공통 매개변수를 제외한 공개 성분을 묻는지 확인한다.

암기 포인트

p는 소수, e_1은 원시근, d는 개인키, (p, e_1, e_2)는 공개키 전체이다.

NoteBase

문 34. 블록 암호 운영 모드 중 CFB(Cipher FeedBack)의 설명으로 가장 적절하지 않은 것은?

① CBC모드처럼 블록 단위의 패턴이 유지되지 않는다.

② 키 스트림이 암호문에 의존하는 비동기식 스트림 암호이다.

③ 암호문의 한 비트의 오류는 단지 대응되는 평문의 한 비트에만 영향을 준다.

④ 두 개 이상의 메시지를 같은 키로 암호화 한다면, 각 메시지는 서로 다른 IV(초기 벡터) 값을 사용해야 한다.

정답 3번

간단한 해설

CFB는 **암호문을 다음 키 스트림 생성에 피드백**한다. 이 때문에 암호문의 비트 오류가 현재 대응 비트뿐 아니라 이후 평문 구간에도 영향을 준다.

선지별 해설

① O: CFB는 앞선 암호문을 내부 상태에 반영하여 다음 키 스트림을 만든다. 따라서 동일한 평문 블록을 독립적으로 동일한 암호문으로 바꾸는 ECB와 달리, **평문의 반복 패턴이 그대로 드러나지 않는다**. CBC도 이전 블록과의 연쇄로 이런 패턴 노출을 줄인다.

② O: CFB의 키 스트림은 앞서 수신한 암호문에 의존한다. 이러한 **암호문 피드백**으로 내부 상태를 갱신하는 방식을 자기동기식, 또는 비동기식 스트림 암호 방식이라고 한다. 블록 암호를 구성 요소로 사용하면서 스트림 방식으로 처리하는 것이다.

③ X: 현재 암호문 구간의 한 비트 오류는 현재 평문 구간의 대응 비트를 뒤집고, 오류가 포함된 암호문이 피드백되므로 **뒤따르는 평문 구간에도 영향을 준다**. 오류 전파 범위는 피드백 구간의 크기에 따라 달라진다. 블록 전체를 피드백하는 경우에는 다음 평문 블록이 영향을 받고, 그 이후에는 정상 암호문으로 상태가 회복된다. 대응 비트만 바뀌는 OFB·CTR의 성질과 혼동하면 안 된다.

④ O: 같은 키로 여러 메시지를 암호화할 때 IV를 재사용하면 처음의 키 스트림도 반복되어 평문 간 관계가 노출된다. 따라서 메시지마다 새로운 IV를 사용한다. CFB의 IV는 단순히 서로 다르기만 하면 되는 것이 아니라 **예측 불가능해야 한다**는 조건도 중요하다.

따라서 오류의 영향을 대응 평문 한 비트로만 한정한 ③이 가장 적절하지 않다.

NoteBase

문 35. 블록 암호 운영 모드 중 암호화와 복호화할 때 병렬처리가 가능한 운영 모드로 옳은 것을 고른 것은?

가. OFB 나. CBC 다. CFB
라. CTR 마. ECB

① 가, 다
② 나, 라
③ 다, 라
④ 라, 마

정답 4번

간단한 해설

CTR과 ECB는 블록 간 처리 결과에 의존하지 않아 암호화와 복호화를 모두 병렬화할 수 있다. CBC·CFB는 복호화만, OFB는 키 스트림 생성이 순차적이다.

보기별 해설

가. X: OFB는 이전 블록 암호 출력이 다음 키 스트림 블록의 입력이므로, 키 스트림 생성이 순차적으로 연결된다. 미리 생성한 스트림과의 XOR은 병렬화할 수 있어도 전체 블록 암호 연산을 독립적으로 병렬화할 수는 없다.

나. X: CBC 암호화는 직전 암호문이 있어야 다음 블록을 계산하므로 순차적이다. 복호화에서는 이미 주어진 암호문 블록 각각에 역변환을 적용할 수 있어 병렬 처리가 가능하지만, 두 과정 모두라는 조건에는 해당하지 않는다.

다. X: CFB 암호화는 앞에서 생성한 암호문을 다음 입력에 반영하므로 순차적이다. 복호화에서는 수신한 암호문으로 각 입력을 구성할 수 있으므로 병렬화가 가능하나 암호화까지 병렬인 것은 아니다.

라. O: CTR은 각 카운터 블록을 독립적으로 암호화하여 키 스트림을 만든다. 앞 블록의 처리 결과를 기다릴 필요가 없어 암호화와 복호화 모두 병렬 처리가 가능하다.

마. O: ECB는 각 평문 블록의 암호화와 각 암호문 블록의 복호화가 다른 블록에 의존하지 않는다. 따라서 두 과정 모두 병렬 처리가 가능하다. 다만 이러한 독립성이 동일 평문의 패턴 노출 문제를 없애 주지는 않는다.

암호화와 복호화 모두 병렬 처리 가능한 것은 라(CTR)·마(ECB)이므로 ④이다.

NoteBase

문 36. MAC(Message Authentication Code)의 일종으로 CCM의 핵심적인 구성요소로 가장 적절하지 않은 것은?

① SHA 알고리즘

② AES 알고리즘

③ CTR 운영모드

④ CBC-MAC 인증 알고리즘

정답 1번

간단한 해설

CCM은 **CTR과 CBC-MAC을 결합한 인증 암호화 방식**이며 AES를 기반 블록 암호로 사용한다. SHA 해시 알고리즘을 핵심 요소로 사용하는 구조가 아니다.

선지별 해설

① X: SHA는 해시 알고리즘 계열이다. CCM은 해시 기반 HMAC을 사용하는 구조가 아니라 **블록 암호 기반 CBC-MAC과 CTR을 결합**하므로 SHA는 핵심 구성요소가 아니다.

② O: AES는 CCM의 기반 블록 암호로 사용된다. AES의 암호화 연산을 CTR의 키 스트림 생성과 CBC-MAC의 연쇄 계산에 활용한다. AES 자체와 그 활용 방법인 운영 모드는 서로 다른 층위의 개념이다.

③ O: CTR은 카운터 블록을 암호화하여 얻은 키 스트림을 평문과 XOR하여 **기밀성**을 제공한다. CCM에서는 인증 태그를 보호하는 처리에도 카운터 방식이 사용된다.

④ O: CBC-MAC은 형식에 맞춰 구성한 메시지와 부가 인증 데이터 등을 연쇄 처리하여 **무결성과 데이터 출처 인증**을 위한 인증값을 만든다. 부가 인증 데이터는 인증 대상이지만 반드시 암호화되는 데이터는 아니다.

개념 구별: 문제는 CCM의 구성요소를 묻지만, CCM 전체를 단순한 MAC 하나로만 이해하면 안 된다. CCM은 CTR 암호화와 CBC-MAC 인증을 결합한 **인증 암호화 방식**이다.

따라서 CCM의 핵심 구성요소에 해당하지 않는 것은 ① SHA 알고리즘이다.

NoteBase

문 37. 다음에서 설명하고 있는 보안을 위한 네트워크 구성요소로 가장 적절한 것은?

웹서버 앞단에 설치되며 HTTP 트래픽을 분석, 모니터링, 보호하는 보안 장치이다. 들어오는 HTTP 트래픽을 검사해 SQL 인젝션, 크로스사이트 스크립팅 같은 해킹공격을 탐지하고 방어한다. 또한, 정보유출 방지, 부정 로그인 방지, 웹사이트 위·변조 방지 등으로 활용된다.

① IDS(Intrusion Detection System)

② IPS(Intrusion Prevention System)

③ NAC(Network Access Control)

④ WAF(Web Application Firewall)

정답 4번

간단한 해설

HTTP 요청의 내용을 검사하여 SQL 인젝션·크로스사이트 스크립팅 같은 웹 공격을 차단하는 장치는 **웹 방화벽(WAF)**이다.

공통 해설

WAF(Web Application Firewall)는 웹 애플리케이션을 보호하기 위해 **HTTP 트래픽의 내용을 검사하고 필터링**하는 보안 장치이다. 웹서버 앞에서 요청을 검사하여, 보안 규칙에 따라 악성으로 판단한 요청이 웹 애플리케이션에 도달하지 못하도록 차단한다.

지문의 SQL 인젝션과 크로스사이트 스크립팅은 HTTP 요청에 담긴 공격 내용을 검사하여 대응할 수 있는 대표적인 웹 공격이다. 따라서 '웹서버 앞단', 'HTTP 트래픽 검사', '웹 공격 탐지·방어'라는 단서들은 웹 애플리케이션 보호에 특화된 WAF의 기능을 설명한다. 단순히 침입을 탐지하거나 방지한다는 일반적인 기능보다 **보호 대상이 웹 애플리케이션이라는 점**이 명칭을 식별하는 기준이다.

NoteBase

문 38. 「개인정보보호법 시행령」 제29조(영업양도 등에 따른 개인정보 이전의 통지)에 대한 내용이다. 빈칸 ㉠, ㉡에 해당하는 내용으로 가장 적절한 것은?

② 법 제27조제1항에 따라 개인정보를 이전하려는 자(이하 이 항에서 “영업양도자등”이라 한다)가 과실 없이 제1항에 따른 방법으로 법 제27조제1항 각 호의 사항을 정보주체에게 알릴 수 없는 경우에는 해당 사항을 인터넷 홈페이지에 (㉠) 이상 게재하여야 한다. 다만, 인터넷 홈페이지에 게재할 수 없는 정당한 사유가 있는 경우에는 다음 각 호의 어느 하나의 방법으로 법 제27조제1항 각 호의 사항을 정보주체에게 알릴 수 있다. <개정 2020. 8. 4.>
1. 영업양도자등의 사업장등의 보기 쉬운 장소에 (㉡) 이상 게시하는 방법
2. 영업양도자등의 사업장등이 있는 시·도 이상의 지역을 주된 보급지역으로 하는 「신문 등의 진흥에 관한 법률」 제2조제1호가목·다목 또는 같은 조 제2호에 따른 일반일간신문·일반주간신문 또는 인터넷신문에 싣는 방법

① ㉠: 30일, ㉡: 30일
② ㉠: 30일, ㉡: 60일
③ ㉠: 60일, ㉡: 30일
④ ㉠: 60일, ㉡: 60일

정답 1번

②

영업양도자등이 과실 없이 서면등의 방법으로 이전 사항을 알릴 수 없으면 **인터넷 홈페이지에 30일 이상 게재**해야 한다. 홈페이지에 게재할 수 없는 정당한 사유가 있으면 **사업장등의 보기 쉬운 장소에 30일 이상 게시**하거나, **사업장등이 있는 시·도 이상의 지역을 주된 보급지역으로 하는 일반일간신문·일반주간신문 또는 인터넷신문에 게재**할 수 있다.

개인정보 보호법 시행령 제29조(영업양도 등에 따른 개인정보 이전의 통지)
② 법 제27조제1항에 따라 개인정보를 이전하려는 자(이하 이 항에서 "영업양도자등"이라 한다)가 과실 없이 제1항에 따른 방법으로 법 제27조제1항 각 호의 사항을 정보주체에게 알릴 수 없는 경우에는 해당 사항을 인터넷 홈페이지에 30일 이상 게재하여야 한다. 다만, 인터넷 홈페이지에 게재할 수 없는 정당한 사유가 있는 경우에는 다음 각 호의 어느 하나의 방법으로 법 제27조제1항 각 호의 사항을 정보주체에게 알릴 수 있다. <개정 2020.8.4>
1. 영업양도자등의 사업장등의 보기 쉬운 장소에 30일 이상 게시하는 방법
2. 영업양도자등의 사업장등이 있는 시 · 도 이상의 지역을 주된 보급지역으로 하는 「신문 등의 진흥에 관한 법률」 제2조제1호 가목 · 다목 또는 같은 조 제2호에 따른 일반일간신문 · 일반주간신문 또는 인터넷신문에 싣는 방법

NoteBase

문 39. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」 제9조의4(본인확인기관의 지정절차)에 대한 내용이다. 빈칸 ㉠, ㉡에 해당하는 내용으로 가장 적절한 것은?

① 법 제23조의3제1항에 따라 본인확인기관으로 지정을 받으려는 자는 본인확인기관지정신청서(전자문서로 된 신청서를 포함한다)에 다음 각 호의 서류(전자문서를 포함한다)를 첨부하여 방송미디어통신위원회에 제출하여야 한다. <개정 2025. 10. 1.>

<중략>

④ 방송미디어통신위원회는 제1항에 따른 신청을 받은 경우에는 신청을 받은 날부터 (㉠) 이내에 제9조의3에 따른 심사사항별 세부 심사기준의 충족 여부를 심사하여 그 심사결과를 신청인에게 통지하여야 한다. 다만, 부득이한 사유가 있는 경우에는 그 사유를 알리고 (㉡)의 범위에서 그 기간을 연장할 수 있다. <개정 2025. 10. 1.>

① ㉠: 30일, ㉡: 30일

② ㉠: 60일, ㉡: 30일

③ ㉠: 60일, ㉡: 60일

④ ㉠: 90일, ㉡: 30일

정답 4번

NoteBase

공통 해설

본인확인기관 지정신청서와 첨부서류는 방송미디어통신위원회에 제출하며, 전자문서도 포함한다. 위원회는 **신청을 받은 날부터 90일 이내**에 세부 심사기준 충족 여부를 심사하고 결과를 통지해야 한다. 다만, **부득이한 사유가 있으면 그 사유를 알리고 30일의 범위에서 연장**할 수 있다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제9조의4(본인확인기관의 지정절차)
① 법 제23조의3제1항에 따라 본인확인기관으로 지정을 받으려는 자는 본인확인기관지정신청서(전자문서로 된 신청서를 포함한다)에 다음 각 호의 서류(전자문서를 포함한다)를 첨부하여 방송미디어통신위원회에 제출하여야 한다. <개정 2025.10.1>
1. 조직 · 인력 및 설비 등의 현황을 기재한 사업계획서
2. 제9조의3에 따른 심사사항별 세부 심사기준이 충족됨을 증명할 수 있는 서류
3. 법인의 정관 또는 단체의 규약(법인 또는 단체인 경우에만 해당한다)
4. 그 밖에 본인확인업무 수행의 전문성과 재무구조의 건전성 등을 확인하기 위하여 필요한 서류로서 방송미디어통신위원회가 정하여 고시하는 서류
④ 방송미디어통신위원회는 제1항에 따른 신청을 받은 경우에는 신청을 받은 날부터 90일 이내에 제9조의3에 따른 심사사항별 세부 심사기준의 충족 여부를 심사하여 그 심사결과를 신청인에게 통지하여야 한다. 다만, 부득이한 사유가 있는 경우에는 그 사유를 알리고 30일의 범위에서 그 기간을 연장할 수 있다. <개정 2025.10.1>

NoteBase

문 40. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」 제14조(운영·관리 실태점검의 대상)에 대한 내용이다. 빈칸 ㉠, ㉡에 해당하는 내용으로 가장 적절한 것은?

법 제23조의6제3항에 따른 실태점검(이하 “실태점검”이라 한다)의 대상이 되는 본인확인기관 및 연계정보 이용기관은 다음 각 호의 구분에 따른 자로 한다.
1. 본인확인기관의 경우: 법 제23조의5제1항에 따라 연계정보를 생성 또는 처리한 자로서 연계정보를 생성 또는 처리한 건수가 (㉠) 이상인 자
2. 연계정보 이용기관의 경우: 법 제23조의5제1항에 따라 본인확인기관으로부터 연계정보를 (㉡) 이상 제공받은 자
[본조신설 2025. 5. 20.]

① ㉠: 1,000건, ㉡: 1,000건

② ㉠: 1,000건, ㉡: 3,000건

③ ㉠: 3,000건, ㉡: 1,000건

④ ㉠: 3,000건, ㉡: 3,000건

정답 1번

①

본인확인기관 중 연계정보를 생성 또는 처리한 자로서 **생성 또는 처리 건수가 1,000건 이상인 자**가 실태점검 대상이다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제14조(운영 · 관리 실태점검의 대상) 법 제23조의6제3항에 따른 실태점검(이하 "실태점검"이라 한다)의 대상이 되는 본인확인기관 및 연계정보 이용기관은 다음 각 호의 구분에 따른 자로 한다.
1. 본인확인기관의 경우: 법 제23조의5제1항에 따라 연계정보를 생성 또는 처리한 자로서 연계정보를 생성 또는 처리한 건수가 1,000건 이상인 자

②

연계정보 이용기관은 **본인확인기관으로부터 연계정보를 1,000건 이상 제공받은 경우** 실태점검 대상이 된다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제14조(운영 · 관리 실태점검의 대상) 법 제23조의6제3항에 따른 실태점검(이하 "실태점검"이라 한다)의 대상이 되는 본인확인기관 및 연계정보 이용기관은 다음 각 호의 구분에 따른 자로 한다.
2. 연계정보 이용기관의 경우: 법 제23조의5제1항에 따라 본인확인기관으로부터 연계정보를 1,000건 이상 제공받은 자

NoteBase