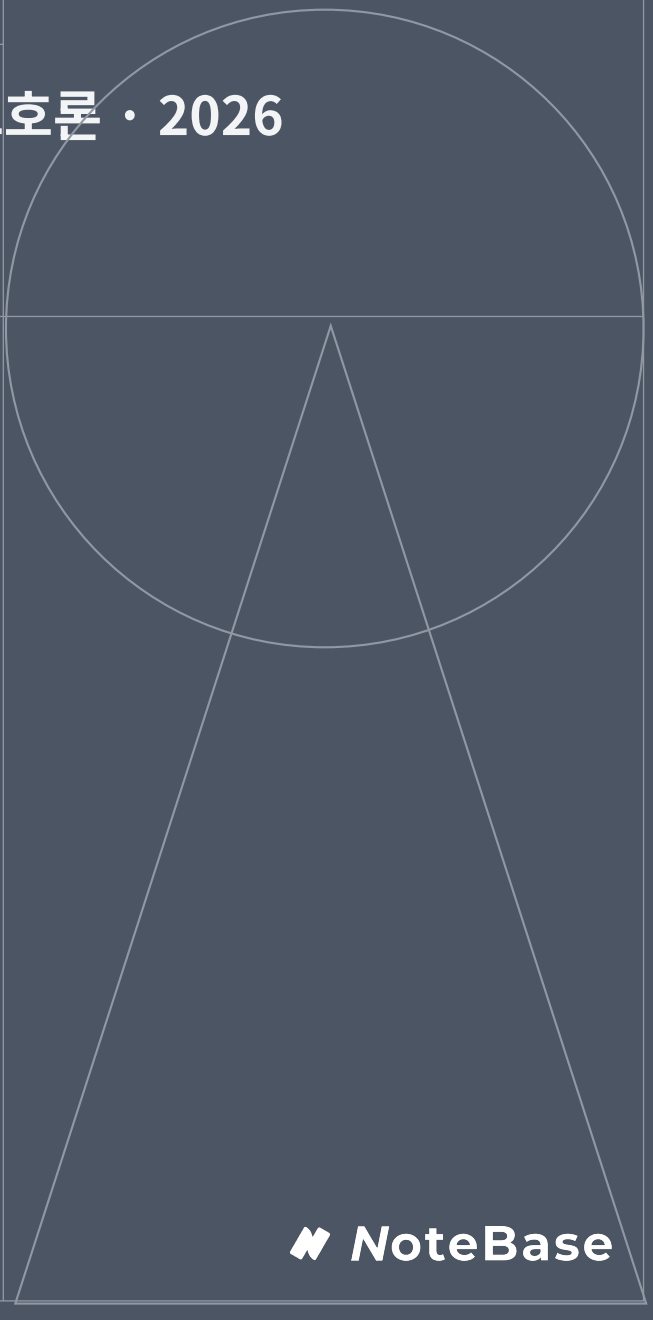
기출OX 해설집

공무원/국가직/9급 · 정보보호론 · 2026



NoteBase

기출OX 해설집

공무원/국가직/9급 · 정보보호론 · 2026

공무원/국가직/9급 · 정보보호론 · 2026

문 1. 일방향 해시 함수의 응용으로 적합하지 않은 것은?

① 전자서명

② 의사난수 생성

③ 데이터 암복호화

④ 소프트웨어 변경 검출

정답 3번

간단한 해설

일방향 해시 함수는 입력을 해시값으로 요약하며, **해시값에서 원문을 복원하기 어렵다**. 원문을 다시 복원해야 하는 데이터 암복호화에는 해시 함수 자체를 사용할 수 없다.

개념 구분

일방향 해시와 데이터 암복호화: 일방향 해시 함수는 임의 길이의 데이터를 일정 길이의 해시값으로 변환한다. 해시값을 계산하기는 쉽지만, 해시값에서 원문을 찾아내기는 계산상 어렵다. 반면 암호화는 데이터를 암호문으로 바꾸고, 정당한 수신자가 적절한 키로 **원문을 복원할 수 있어야 한다**. 해시값에는 이런 복호화 절차가 없으므로 데이터 암복호화에 그대로 사용할 수 없다.

전자서명: 메시지의 해시값을 서명 연산의 입력으로 사용한다. 검증할 때도 메시지의 해시값을 이용하므로, 해시값에서 원문을 복원할 필요가 없다.

의사난수 생성: 해시 함수는 시드와 내부 상태를 바탕으로 예측하기 어려운 비트열을 생성하는 의사난수 생성기의 구성 요소로 쓰일 수 있다. 해시 함수가 스스로 무작위성을 만들어 내는 것은 아니며, 적절한 시드와 생성 절차가 필요하다.

소프트웨어 변경 검출: 신뢰할 수 있는 원본의 해시값과 현재 파일의 해시값을 비교한다. 두 값이 다르면 **파일이 변경되었음**을 알 수 있으므로, 원문 복원 없이 변경 여부를 검출할 수 있다.

NoteBase

문 2. RSA 암호 알고리즘에 대한 설명으로 옳지 않은 것은?

① 공개키 기반 암호 방식이다.

② 개인키는 공개하지 않고 비밀로 유지한다.

③ 큰 수의 소인수분해가 어렵다는 특성을 이용한다.

④ 공개키로 암호화한 메시지는 전자서명 기능을 제공한다.

정답 4번

간단한 해설

공개키로 메시지를 암호화하는 것은 **기밀성**을 위한 처리이며, 누구나 공개키를 사용할 수 있으므로 그것만으로 작성자를 확인할 수는 없다. RSA 전자서명은 **서명자의 개인키로 생성**하고 그에 대응하는 공개키로 검증한다.

선지별 해설

① O: RSA는 서로 대응하는 **공개키와 개인키**를 사용하는 비대칭키 암호 방식이다. 암호화에 사용하는 키와 복호화에 사용하는 키가 서로 다르며, 공개키는 다른 사람에게 공개할 수 있다.

② O: 개인키는 키 소유자만 사용하도록 **비밀로 유지**해야 한다. 개인키가 유출되면 해당 공개키로 암호화된 메시지를 복호화하거나 키 소유자를 사칭하여 전자서명을 생성할 수 있다.

③ O: RSA에서는 큰 소수들을 곱한 수를 공개키의 구성 요소로 사용한다. 이 수에서 원래의 소수들을 알아내면 개인키 계산에 필요한 정보를 얻을 수 있으므로, 큰 수의 **소인수분해가 어렵다는 성질**이 RSA의 안전성을 뒷받침한다.

④ X: 수신자의 공개키로 암호화한 메시지는 수신자의 개인키로 복호화하며, 이는 내용을 다른 사람이 읽지 못하게 하는 기밀성을 위한 것이다. 공개키는 누구나 사용할 수 있으므로 공개키로 암호화했다는 사실만으로는 누가 작성했는지 확인할 수 없다. 전자서명은 **서명자의 개인키로 메시지의 해시값에 대한 서명을 생성**하고, 서명자의 공개키로 검증하여 작성자와 메시지의 변조 여부를 확인한다.

NoteBase

문 3. DBMS에서 데이터베이스 객체에 대한 권한 부여를 위해 사용하는 SQL 명령어는?

① ALTER

② GRANT

③ INSERT

④ COMMIT

정답 2번

간단한 해설

데이터베이스 객체에 대한 권한을 부여할 때는 **GRANT**를 사용한다. 특정 사용자나 역할이 해당 객체에서 수행할 수 있는 연산을 허용하는 명령이다.

공통 해설

데이터베이스 객체에 대한 권한은 테이블 등 특정 객체에서 조회·삽입·수정과 같은 연산을 수행할 수 있는 자격이다. **GRANT는 대상 객체의 특정 권한을 사용자나 역할에 부여**하는 SQL 명령이다. 예를 들어 특정 사용자에게 한 테이블의 조회를 허용하려면 GRANT로 그 테이블에 대한 SELECT 권한을 부여한다. 이처럼 문항에서 묻는 것은 객체에 대한 연산을 허용하는 권한 부여이므로 GRANT에 대응한다.

NoteBase

문 4. SSLv3(Secure Sockets Layer version 3)의 레코드 프로토콜에서 응용 프로그램으로부터 획득한 데이터를 송신하기 위해 수행하는 과정을 순서대로 바르게 나열한 것은?

① 압축(옵션) → MAC 추가 → 암호화 → 단편화 → 헤더 추가

② 압축(옵션) → 헤더 추가 → 암호화 → 단편화 → MAC 추가

③ 단편화 → 압축(옵션) → MAC 추가 → 암호화 → 헤더 추가

④ 단편화 → 암호화 → MAC 추가 → 압축(옵션) → 헤더 추가

정답 3번

간단한 해설

응용 데이터를 먼저 **레코드 단위로 단편화**한 뒤 각 단편을 처리한다. 압축을 적용한 데이터에 **MAC을 붙인 후 함께 암호화**하고, 전송할 레코드의 헤더를 추가한다.

올바른 순서

단편화 → 압축(옵션) → MAC 추가 → 암호화 → 헤더 추가

단편화: 응용 프로그램에서 받은 데이터를 레코드가 처리할 수 있는 크기의 조각으로 나눈다. 이후의 압축과 보안 처리는 **각 단편을 단위로** 수행하므로 단편화가 먼저이다.

압축(옵션): 각 단편에 협의된 압축 방식을 적용한다. 데이터를 원래대로 복원할 수 있는 무손실 압축을 사용하며, 압축을 사용하지 않으면 단편을 그대로 다음 단계로 넘긴다. MAC은 이 단계의 출력 데이터를 대상으로 계산한다.

MAC 추가: 비밀키를 이용해 메시지 인증 코드(MAC)를 계산하고 데이터 뒤에 붙인다. 수신 측은 이를 이용해 데이터의 변조 여부를 확인한다. SSLv3에서는 **암호화 전에 MAC을 계산하여 추가**한다.

암호화: **데이터와 MAC을 함께 암호화**하여 내용을 보호한다. 블록 암호를 사용하는 경우에는 암호화할 길이를 블록 크기에 맞추는 패딩도 포함한다.

헤더 추가: 암호화된 결과 앞에 콘텐츠 유형, 프로토콜 버전, 길이를 나타내는 레코드 헤더를 붙인다. 특히 길이는 **암호화된 레코드 내용의 길이**를 나타내므로 암호화 결과가 정해진 뒤 전송 형식을 완성한다.

NoteBase

문 5. 조직의 자산 및 정보를 보호하기 위한 정보보호 관리체계의 국제 인증 규격은?

① CC

② ITSEC

③ TCSEC

④ ISO/IEC 27001

정답 4번

간단한 해설

ISO/IEC 27001은 조직의 **정보보호 관리체계(ISMS)**가 갖추어야 할 요구사항을 정한 국제 규격으로, 관리체계 인증의 기준이 된다.

공통 해설

정보보호 관리체계(ISMS)는 조직의 정보보호 위험을 평가하고, 필요한 보호조치를 수립·운영하며 지속적으로 점검하고 개선하는 체계이다. ISO/IEC 27001은 이러한 관리체계의 수립·운영·유지·개선에 필요한 요구사항을 정한다. 조직은 이 요구사항에 대한 적합성을 심사받아 정보보호 관리체계 인증을 받을 수 있다.

구별 기준은 **평가 대상이 조직의 관리체계인지, IT 제품·시스템의 보안성인지**이다. CC, ITSEC, TCSEC는 IT 제품·시스템의 보안성을 평가하는 기준이다. 반면 ISO/IEC 27001은 조직이 정보와 자산을 보호하기 위해 갖춘 관리체계를 대상으로 하므로, 발문에서 묻는 국제 인증 규격에 해당한다.

NoteBase

문 6. 시스템 보안에서 사용자와 시스템 사이 또는 두 시스템 사이의 활성화된 접속을 관리하는 것은?

① 세션 관리

② 권한 관리

③ 로그 관리

④ 취약점 관리

정답 1번

간단한 해설

사용자와 시스템 사이 또는 두 시스템 사이에 활성화된 접속을 세션이라고 한다. 이 접속의 유지와 종료 등을 다루는 것이 **세션 관리**이다.

공통 해설

세션은 사용자와 시스템 사이 또는 두 시스템 사이에서 통신이나 작업을 위해 활성화된 접속을 뜻한다. 세션 관리는 이러한 **접속의 상태와 수명**을 관리하는 기능으로, 접속을 식별하고 유지하며 필요할 때 종료하는 일을 포함한다. 문제에서 관리 대상으로 제시한 '활성화된 접속'이 바로 세션이므로 세션 관리에 해당한다.

예를 들어 사용자가 로그인한 뒤 서비스를 이용하는 동안 해당 세션을 유지하고, 로그아웃하면 그 세션을 종료하는 것이 세션 관리의 예이다. 핵심은 현재 이어지고 있는 접속 자체를 관리한다는 데 있다.

NoteBase

문 7. 다음 설명에 해당하는 정보보호 위험 분석 방법은?

정성적 위험 분석 방법으로, 시스템에 관한 전문적인 지식을 가진 전문가의 집단을 구성하고 위험을 분석 및 평가하여 정보시스템이 직면한 다양한 위협과 취약성을 토론을 통해 분석하는 방법이다.

① 확률 분포법
② 델파이법
③ 과거 자료 분석법
④ 수학 공식 접근법

정답 2번

간단한 해설

시스템 전문가들의 지식과 판단을 모아 위협과 취약성을 평가한다는 점이 **델파이법**의 단서이다. 정보보호 위험 분석에서는 이를 전문가 의견에 기초한 정성적 방법으로 분류한다.

공통 해설

델파이법은 해당 분야 전문가 집단의 의견을 체계적으로 수렴하여 판단을 형성하는 방법이다. 정보보호 위험 분석에서는 시스템을 잘 아는 전문가들이 위협과 취약성에 관한 의견을 제시하고, 이를 종합하여 위험을 평가하는 정성적 방법으로 활용된다. 지문의 '전문적인 지식을 가진 전문가의 집단'이 이 방법을 가리키는 핵심 단서이다.

기본 절차는 전문가들이 **익명으로 설문에 응답**하고, 집계된 의견을 피드백받아 자신의 판단을 검토하는 과정을 반복하는 것이다. 익명성은 특정인의 권위나 발언에 다른 전문가가 끌려가는 영향을 줄인다. 지문의 '토론'은 전문가 의견을 모아 분석한다는 맥락에서 이해해야 하며, 대면 자유 토론이 델파이법의 필수 절차라는 뜻은 아니다.

확률 분포법·과거 자료 분석법·수학 공식 접근법은 수치 자료나 수학적 모형을 이용해 위험을 추정하는 **정량적 방법**으로 분류된다. 따라서 전문가 집단의 판단을 중심으로 위험을 분석한다는 지문의 정성적 방법과 구별된다.

NoteBase

문 8. CAPTCHA에 대한 설명으로 옳지 않은 것은?

① 컴퓨터와 사람을 구분하기 위한 자동화된 공개 튜링 테스트라 할 수 있다.

② 기밀성을 보장하기 위한 암호의 한 형태이다.

③ 다양한 이미지, 왜곡된 문자, 잡음 섞인 소리를 사용할 수 있다.

④ 대부분의 사람들이 통과하기에는 쉽지만 컴퓨터가 통과하기에는 불가능하거나 어려워야 한다.

정답 2번

간단한 해설

CAPTCHA는 **사람과 자동화 프로그램을 구별**하기 위한 검사이다. 정보를 암호화하여 **기밀성을 보장하는 암호 방식이 아니다**.

선지별 해설

① O: CAPTCHA는 컴퓨터와 사람을 구분하기 위한 완전 자동화된 공개 튜링 테스트이다. 시스템이 문제를 제시하고 응답을 자동으로 판정하여, 접속자가 **사람인지 자동화 프로그램인지** 구별하는 데 사용한다.

② X: 기밀성은 허가받지 않은 사람이 정보의 내용을 알 수 없도록 하는 성질이며, 암호화는 이를 보장하기 위한 수단이다. CAPTCHA의 목적은 정보를 숨기는 것이 아니라 **사람과 자동화 프로그램을 구별하는 것**이므로, 기밀성을 위한 암호의 한 형태라는 설명은 부적절하다.

③ O: CAPTCHA는 사람이 인식할 수 있는 이미지, 왜곡된 문자, 잡음이 섞인 음성 등을 문제로 사용할 수 있다. 예를 들어 왜곡된 문자를 읽어 입력하게 하거나 특정 대상이 있는 이미지를 고르게 하여, **시각·청각 정보의 인식 능력**을 검사한다.

④ O: CAPTCHA의 기본 설계 요건은 **사람에게는 쉽고 자동화 프로그램에는 어려운 과제**를 제시하는 것이다. 사람도 풀기 어렵다면 정상적인 이용을 방해하고, 프로그램도 쉽게 풀 수 있다면 자동 가입이나 자동 게시 같은 행위를 막는 효과가 떨어진다. 이는 설계 목표를 뜻하며, 모든 CAPTCHA를 컴퓨터가 영구적으로 풀 수 없다는 의미는 아니다.

NoteBase

문 9. 다음 설명에 해당하는 보안 솔루션은?

IP 관리 시스템에서 발전한 것으로, MAC 주소를 기반으로 접근 제어 및 인증을 수행하여, 보안 정책에 부합되는 단말기에만 네트워크 자원의 이용을 허용한다.

① NAC
② DLP
③ VPN
④ PIMS

정답 1번

간단한 해설

단말기를 식별·인증하고 **보안 정책을 충족하는 단말기에만 네트워크 접근을 허용**하는 것은 NAC의 기능이다.

공통 해설

NAC(Network Access Control, 네트워크 접근 제어)는 단말기를 식별·인증하고 보안 정책 준수 여부를 확인하여 네트워크 접근을 허용하거나 제한하는 보안 솔루션이다. 단말기의 주소를 관리하는 데서 나아가, 해당 단말기가 실제로 네트워크 자원을 이용해도 되는지까지 통제한다.

지문의 MAC 주소는 접근하려는 단말기를 식별하는 데 쓰이는 정보이다. 이를 바탕으로 인증과 정책 검사를 수행하여 **보안 정책에 부합하는 단말기에만 이용을 허용**한다는 설명이 NAC에 해당한다. 판단 기준은 단말기의 식별 정보 자체가 아니라, 그 단말기에 대한 인증과 정책 검사 결과를 네트워크 접근 통제에 연결한다는 점이다.

NoteBase

문 10. SSH 프로토콜(RFC 4251)의 구성요소에 해당하지 않는 것은?

① 핸드셰이크(Handshake) 프로토콜

② 사용자 인증(User Authentication) 프로토콜

③ 전송 계층(Transport Layer) 프로토콜

④ 연결(Connection) 프로토콜

정답 1번

간단한 해설

RFC 4251에서 SSH의 주요 구성요소는 **전송 계층·사용자 인증·연결 프로토콜**이다. 핸드셰이크 프로토콜은 이 세 구성요소에 포함되지 않는다.

개념 구분

RFC 4251은 SSH를 다음 세 가지 주요 프로토콜로 구성한다. 각 프로토콜은 보안 통신 기반 마련, 사용자 인증, 채널 관리라는 서로 다른 역할을 맡는다.

전송 계층(Transport Layer) 프로토콜: **서버 인증, 기밀성, 무결성**을 제공하여 안전하게 통신할 기반을 마련한다. 여기서 서버 인증은 접속한 서버가 올바른 상대인지 확인하는 것이다.

사용자 인증(User Authentication) 프로토콜: 전송 계층 프로토콜 위에서 동작하며, **클라이언트 측 사용자를 서버에 인증**한다. 전송 계층의 서버 인증과는 인증 대상이 다르다.

연결(Connection) 프로토콜: 사용자 인증 프로토콜 위에서 동작하며, **하나의 암호화된 터널을 여러 논리적 채널로 나누어 사용**하도록 한다. 각 채널을 통해 원격 셸 등의 서비스를 제공할 수 있다.

핸드셰이크(Handshake) 프로토콜: RFC 4251이 구분하는 **SSH의 세 주요 구성요소에는 해당하지 않는다**. SSH의 구성요소를 묻는 이 문항에서는 전송 계층·사용자 인증·연결 프로토콜과 구별해야 한다.

NoteBase

문 11. 「(대검찰청) 디지털 증거의 수집·분석 및 관리 규정」상 전자정보 압수·수색·검증의 기본원칙이 아닌 것은?

① 적법절차의 준수
② 디지털 증거의 신뢰성 유지
③ 디지털 증거의 기밀성 유지
④ 디지털 증거의 원본성 유지

정답 3번

②

디지털 증거는 **신뢰할 수 있는 도구와 방법으로 수집·분석·관리**해야 하며, 이는 신뢰성 유지 원칙에 해당한다.

(대검찰청) 디지털 증거의 수집·분석 및 관리 규정 제7조(2024. 10. 1. 시행, 대검찰청예규 제1449호)
(대검찰청) 디지털 증거의 수집·분석 및 관리 규정 제7조(디지털 증거의 신뢰성 유지) 디지털 증거는 디지털포렌식 전문가에 의해 신뢰할 수 있는 도구와 방법으로 수집 · 분석 및 관리하여야 한다.

전자적 증거의 분석 및 관리 규정 제7조(전자적 증거의 신뢰성 유지) 전자적 증거는 디지털포렌식 분석관이 신뢰할 수 있는 도구와 방법으로 관리 · 분석하여야 한다.

NoteBase

③

기본원칙은 적법절차의 준수, 원본성 유지, 무결성 유지, 신뢰성 유지, 보관의 연속성 유지이다. **기밀성 유지는 이 규정이 정한 기본원칙에 포함되지 않는다.**

(대검찰청) 디지털 증거의 수집·분석 및 관리 규정 제4조(2024. 10. 1. 시행, 대검찰청예규 제1449호)
(대검찰청) 디지털 증거의 수집·분석 및 관리 규정 제4조(적법절차의 준수) 디지털 증거는 수사에 필요한 범위 내에서 적법한 절차를 엄격히 준수하여 수집 · 분석 및 관리되어야 한다.

(대검찰청) 디지털 증거의 수집·분석 및 관리 규정 제5조(2024. 10. 1. 시행, 대검찰청예규 제1449호)
(대검찰청) 디지털 증거의 수집·분석 및 관리 규정 제5조(디지털 증거의 원본성 유지) 디지털 증거는 법정에서 원본과의 동일성을 재현하거나 검증하는데 지장이 초래되지 않도록 수집 · 분석 및 관리되어야 한다.

(대검찰청) 디지털 증거의 수집·분석 및 관리 규정 제6조(2024. 10. 1. 시행, 대검찰청예규 제1449호)
(대검찰청) 디지털 증거의 수집·분석 및 관리 규정 제6조(디지털 증거의 무결성 유지) 디지털 증거는 압수 · 수색 · 검증한 때로부터 법정에 제출하는 때까지 훼손 또는 변경되지 아니하여야 한다.

(대검찰청) 디지털 증거의 수집·분석 및 관리 규정 제7조(2024. 10. 1. 시행, 대검찰청예규 제1449호)
(대검찰청) 디지털 증거의 수집·분석 및 관리 규정 제7조(디지털 증거의 신뢰성 유지) 디지털 증거는 디지털포렌식 전문가에 의해 신뢰할 수 있는 도구와 방법으로 수집 · 분석 및 관리하여야 한다.

(대검찰청) 디지털 증거의 수집·분석 및 관리 규정 제8조(2024. 10. 1. 시행, 대검찰청예규 제1449호)
(대검찰청) 디지털 증거의 수집·분석 및 관리 규정 제8조(디지털 증거의 보관의 연속성 유지) 디지털 증거는 최초 수집된 상태 그대로 어떠한 변경도 없이 보관되어야 하고, 이를 위해 보관 주체들 간의 연속적인 승계 절차를 관리하는 등의 조치를 취해야 한다.

NoteBase

문 12. 국내 정보보호 관리체계(ISMS)에서 '관리체계 수립 및 운영'의 PDCA 사이클을 바르게 나열한 것은?

(가) 위험관리
(나) 관리체계 운영
(다) 관리체계 기반 마련
(라) 관리체계 점검 및 개선

① P: (가) → D: (나) → C: (라) → A: (다)
② P: (가) → D: (다) → C: (나) → A: (라)
③ P: (다) → D: (가) → C: (나) → A: (라)
④ P: (다) → D: (나) → C: (가) → A: (라)

정답 3번

간단한 해설

위험을 평가하여 보호대책을 선정해야 그 대책을 실제로 운영할 수 있으므로, **위험관리는 관리체계 운영에 앞선다**. 운영 후에는 점검에서 발견한 문제를 개선하고 그 결과를 다음 관리 활동에 반영한다.

NoteBase

올바른 순서

(다) → (가) → (나) → (라)

이 배열은 '관리체계 수립 및 운영'을 구성하는 네 인증영역의 진행 순서이다. PDCA는 계획(Plan)·실행(Do)·점검(Check)·개선(Act)의 반복을 뜻한다. 다만, 네 인증영역을 PDCA의 각 글자와 엄밀하게 일대일 대응시키는 것은 아니다. 관리체계 운영에는 실행이, 마지막 영역에는 점검과 개선이 함께 포함된다.

(다) 관리체계 기반 마련: 경영진의 참여 아래 책임자와 조직을 정하고, 적용 범위·정책·필요한 자원을 마련한다. **관리할 대상과 책임·기준**이 먼저 정해져야 그 범위에 대한 위험을 체계적으로 평가할 수 있다.

(가) 위험관리: 정보자산을 식별하고 현황과 흐름을 분석하여 위험을 평가한 뒤, 그 결과에 따라 보호대책을 선정한다. 실제 운영에 들어가기 전에 **어떤 위험에 어떤 대책을 적용할지** 결정하는 과정이다.

(나) 관리체계 운영: 선정한 보호대책을 구현하고 담당자에게 공유하며 운영현황을 관리한다. 앞 단계에서 정한 대책을 **실제 업무에 적용하고 운영 기록을 남기는** 과정이며, 이 기록은 이후 점검의 근거가 된다.

(라) 관리체계 점검 및 개선: 운영 결과와 관련 요구사항의 준수 여부를 점검하고, 발견한 문제의 원인을 분석하여 개선한다. 개선 결과를 정책·위험관리·운영 활동에 반영하므로 관리체계는 **한 번 구축하고 끝나는 것이 아니라 반복적으로 개선**된다.

NoteBase

문 13. 다음 설명에 해당하는 DoS/DDoS 공격기법은?

순서 번호에 오류가 있게 조작된 IP 패킷 조각(fragments)을 전송하여, 이 패킷 조각을 전달받은 시스템의 IP 패킷 재조합 과정에서 오류가 발생되도록 하는 공격기법

① Smurf
② Teardrop
③ ICMP Flooding
④ Buffer Overflow

정답 2번

간단한 해설

조작된 IP 패킷 조각으로 **재조합 과정의 오류**를 유발하는 것이 Teardrop 공격의 특징이다. 단편을 정상적으로 처리하지 못하는 시스템의 취약점을 이용해 서비스 장애를 일으킨다.

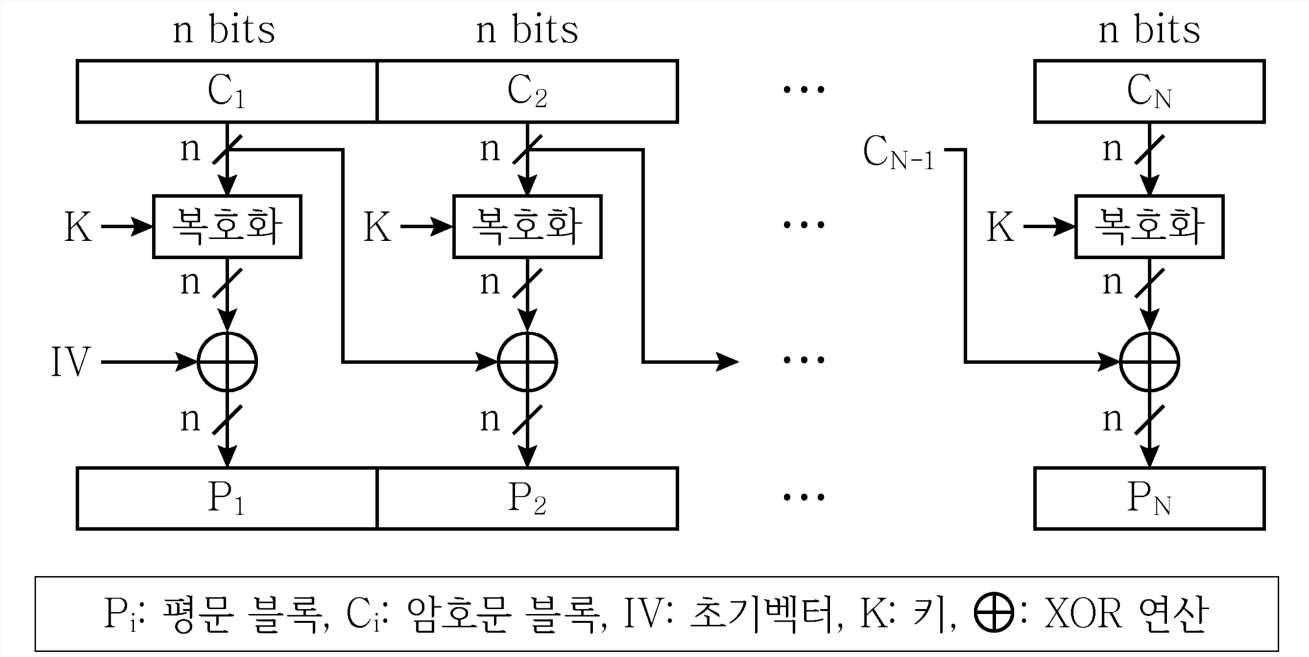
공통 해설

IP 패킷이 여러 조각으로 나뉘어 전송되면 수신 시스템은 각 조각의 위치 정보를 이용해 원래 패킷으로 재조합한다. Teardrop은 조각의 위치 정보인 프래그먼트 오프셋 등을 조작하여 데이터 영역이 겹치게 만들고, 이를 제대로 처리하지 못하는 시스템에서 재조합 오류나 장애를 일으키는 서비스 거부 공격이다.

제시문의 핵심은 **조작된 IP 단편을 재조합할 때 오류가 발생한다**는 점이다. 이처럼 IP 단편 재조합 처리의 취약점을 이용한다는 작동 방식이 Teardrop을 식별하는 기준이다.

NoteBase

문 14. 복호화 과정이 다음 그림에 해당하는 블록 암호 운영 모드는?



① ECB(Electronic CodeBook)

② CBC(Cipher Block Chaining)

③ CFB(Cipher FeedBack)

④ CTR(CounTeR)

정답 2번

간단한 해설

암호문 블록을 복호화한 뒤 **이전 암호문 블록과 XOR**하여 평문을 얻는 구조는 CBC 모드이다. 첫 블록에는 이전 암호문이 없으므로 초기벡터 IV를 사용한다.

NoteBase

도식 해설

첫 블록: 그림에서 암호문 C_1은 키 K를 사용하는 복호화 상자를 거친 뒤 IV와 XOR되어 평문 P_1이 된다. 키 K로 블록을 복호화하는 함수를 D_K라 하면, 이 관계는 $P_1 = D_K(C_1) \oplus IV$이다. IV는 **첫 블록에서 이전 암호문을 대신**한다.

두 번째 이후 블록: C_1에서 갈라진 화살표가 두 번째 블록의 XOR 지점으로 이어진다. 따라서 C_2를 복호화한 결과에 C_1을 XOR하여 P_2를 얻는다. 일반적으로 $P_i = D_K(C_i) \oplus C_{i-1}$이며, 마지막 블록도 같은 방식으로 처리한다. 이처럼 **직전 암호문을 현재 블록의 복호화 결과와 결합**하는 것이 CBC(Cipher Block Chaining)의 복호화 구조이다.

CFB와의 구분: CFB도 이전 암호문을 이용하지만, 이전 암호문을 **암호화 함수**에 넣어 얻은 출력과 현재 암호문을 XOR한다. 그림은 현재 암호문 자체를 **복호화 함수**에 넣고, 그 뒤에 이전 암호문을 XOR하므로 CFB와 구별된다.

NoteBase

문 15. RSA 암호 알고리즘은 키를 생성하는 과정에서 법(modulus) 연산의 곱셈에 대한 역원(multiplicative inverse)을 찾아야 한다. 법 26에 관한 완전잉여계 집합 $Z_{26} = \{0, 1, \cdots, 25\}$에 속한 원소 중에서 곱셈에 대한 역원이 존재하지 않는 것은?

① 7

② 11

③ 13

④ 23

정답 3번

간단한 해설

법 26에서 곱셈의 역원이 존재하려면 그 수가 **26과 서로소**여야 한다. 13은 26과 공약수 13을 가지므로 곱셈의 역원이 존재하지 않는다.

공통 해설

법 26에서 a의 곱셈에 대한 역원은 ab ≡ 1 ±od26을 만족하는 원소 b이다. 즉, a와 b를 곱하여 26으로 나눈 나머지가 1이 되어야 한다. 이러한 b가 존재할 필요충분조건은 **a와 26의 최대공약수가 1**인 것, 곧 두 수가 서로소인 것이다.

26 = 2 × 13이므로 2나 13으로 나누어떨어지는 수는 이 조건을 만족하지 못한다. 7, 11, 23은 모두 2와 13 어느 것으로도 나누어떨어지지 않아 26과 서로소이므로 역원이 존재한다. 반면 13은 26과 공약수 13을 갖는다. 13에 어떤 정수를 곱해도 13의 배수이므로 26으로 나눈 나머지는 0 또는 13이며, 1이 될 수 없다. 따라서 이 문제에서 곱셈의 역원이 존재하지 않는 원소는 13이다.

NoteBase

문 16. ISMS-P의 '보호대책 요구사항' 분야에 해당하지 않는 것은?

① 정보주체 권리보호

② 재해 복구

③ 외부자 보안

④ 정책, 조직, 자산 관리

정답 1번

간단한 해설

정보주체 권리보호는 **'개인정보 처리 단계별 요구사항'**에 속한다. ISMS-P 인증기준의 한 항목이지만, 문제에서 묻는 '보호대책 요구사항' 분야에는 포함되지 않는다.

개념 구분

ISMS-P 인증기준은 '1. 관리체계 수립 및 운영', '2. 보호대책 요구사항', '3. 개인정보 처리 단계별 요구사항'으로 구분된다. 이 문제는 ISMS-P 전체에 포함되는지를 묻는 것이 아니라, **'2. 보호대책 요구사항'의 하위 분야인지**를 묻는다.

정보주체 권리보호는 자신의 개인정보에 관한 정보주체의 권리 행사를 보장하기 위한 분야로, **'3.5 정보주체 권리보호'**에 해당한다. 따라서 '3. 개인정보 처리 단계별 요구사항'에 속한다.

나머지 항목은 '2. 보호대책 요구사항'에 속한다. 재해 복구는 2.12, 외부자 보안은 2.3, 정책, 조직, 자산 관리는 2.1에 해당한다. 특히 정책·조직·자산을 관리한다는 표현 때문에 '1. 관리체계 수립 및 운영'으로 혼동할 수 있지만, 인증기준에서의 분류는 **'2.1 정책, 조직, 자산 관리'**이다.

NoteBase

문 17. (가), (나)에 들어갈 용어를 바르게 연결한 것은?

IPSec(RFC 2401)에서 (가)는 기밀성(confidentiality), 데이터 발신 인증(data origin authentication), 비연결 무결성(connectionless integrity) 등을 제공하는 프로토콜이다. 이 프로토콜은 기밀성을 제공하기 위해 (나) 암호 알고리즘을 사용하여 데이터를 암호화한다.

① (가): AH, (나): 공개키

② (가): AH, (나): 대칭키

③ (가): ESP, (나): 공개키

④ (가): ESP, (나): 대칭키

정답 4번

간단한 해설

IPSec에서 인증·무결성과 함께 **기밀성도 제공하는 프로토콜은 ESP**이다. ESP는 데이터를 암호화할 때 송수신자가 비밀키를 공유하는 **대칭키 암호**를 사용한다.

빈칸별 해설

(가) ESP: ESP(Encapsulating Security Payload)는 데이터를 암호화하여 권한 없는 사람이 내용을 읽지 못하게 하는 기밀성을 제공할 수 있다. 설정에 따라 데이터가 해당 발신자에게서 왔는지 확인하는 데이터 발신 인증과, 개별 패킷의 데이터가 변조되지 않았는지 확인하는 비연결 무결성도 제공한다. AH는 인증과 무결성을 제공하지만 **데이터를 암호화하여 기밀성을 제공하지는 않는다**. 따라서 지문의 '기밀성'이 두 프로토콜을 구별하는 단서이다.

(나) 대칭키: ESP의 데이터 암호화에는 **암호화와 복호화에 같은 비밀키를 사용하는** 대칭키 암호 알고리즘을 사용한다. 송신자가 공유된 비밀키로 데이터를 암호화하면 수신자가 같은 키로 복호화한다. 공개키와 개인키를 구분하여 사용하는 공개키 암호 방식과 구별된다. 이 문항은 키를 교환하는 방법이 아니라 실제 데이터를 암호화하는 방식을 묻는다.

(가)는 ESP, (나)는 대칭키이므로 두 용어를 연결한 조합은 ④이다.

NoteBase

문 18. 「개인정보 보호법」상 개인정보 보호위원회의 위원 자격 요건에 해당하지 않는 사람은?

① 공공기관 또는 단체로부터 추천받은 사람으로서 개인정보 보호 업무를 3년 이상 담당하였던 사람

② 개인정보 보호 업무를 담당하는 3급 이상 공무원의 직에 있었던 사람

③ 판사·검사·변호사의 직에 10년 이상 있었던 사람

④ 대학 부교수 이상으로 3년 이상 재직하였던 사람

정답 4번

①

공공기관 또는 단체의 **추천을 받고 개인정보 보호 업무를 3년 이상 담당한 경력**이 있으면 위원의 경력 요건에 해당한다.

개인정보 보호법 제7조의2(보호위원회의 구성 등)
② 보호위원회의 위원은 개인정보 보호에 관한 경력과 전문지식이 풍부한 다음 각 호의 사람 중에서 위원장과 부위원장은 국무총리의 제청으로, 그 외 위원 중 2명은 위원장의 제청으로, 2명은 대통령이 소속되거나 소속되었던 정당의 교섭단체 추천으로, 3명은 그 외의 교섭단체 추천으로 대통령이 임명 또는 위촉한다.
3. 공공기관 또는 단체(개인정보처리자로 구성된 단체를 포함한다)에 3년 이상 임원으로 재직하였거나 이들 기관 또는 단체로부터 추천받은 사람으로서 개인정보 보호 업무를 3년 이상 담당하였던 사람

②

개인정보 보호 업무를 담당하는 **3급 이상 공무원의 직에 있거나 있었던 사람**은 위원 자격 요건에 해당한다.

개인정보 보호법 제7조의2(보호위원회의 구성 등)
② 보호위원회의 위원은 개인정보 보호에 관한 경력과 전문지식이 풍부한 다음 각 호의 사람 중에서 위원장과 부위원장은 국무총리의 제청으로, 그 외 위원 중 2명은 위원장의 제청으로, 2명은 대통령이 소속되거나 소속되었던 정당의 교섭단체 추천으로, 3명은 그 외의 교섭단체 추천으로 대통령이 임명 또는 위촉한다.
1. 개인정보 보호 업무를 담당하는 3급 이상 공무원(고위공무원단에 속하는 공무원을 포함한다)의 직에 있거나 있었던 사람

NoteBase

③

판사·검사·변호사로 **10년 이상 재직 중이거나 재직한 경력**이 있으면 위원의 경력 요건에 해당한다.

개인정보 보호법 제7조의2(보호위원회의 구성 등)
② 보호위원회의 위원은 개인정보 보호에 관한 경력과 전문지식이 풍부한 다음 각 호의 사람 중에서 위원장과 부위원장은 국무총리의 제청으로, 그 외 위원 중 2명은 위원장의 제청으로, 2명은 대통령이 소속되거나 소속되었던 정당의 교섭단체 추천으로, 3명은 그 외의 교섭단체 추천으로 대통령이 임명 또는 위촉한다.
2. 판사 · 검사 · 변호사의 직에 10년 이상 있거나 있었던 사람

④

대학 부교수 이상의 재직기간은 **3년이 아니라 5년 이상**이어야 하며, **개인정보 관련 분야의 전문지식**도 갖추어야 한다.

개인정보 보호법 제7조의2(보호위원회의 구성 등)
② 보호위원회의 위원은 개인정보 보호에 관한 경력과 전문지식이 풍부한 다음 각 호의 사람 중에서 위원장과 부위원장은 국무총리의 제청으로, 그 외 위원 중 2명은 위원장의 제청으로, 2명은 대통령이 소속되거나 소속되었던 정당의 교섭단체 추천으로, 3명은 그 외의 교섭단체 추천으로 대통령이 임명 또는 위촉한다.
4. 개인정보 관련 분야에 전문지식이 있고 「고등교육법」 제2조제1호에 따른 학교에서 부교수 이상으로 5년 이상 재직하고 있거나 재직하였던 사람

NoteBase

문 19. 「개인정보 보호법」상 정보주체의 개인정보 열람 요구 시에, 개인정보 처리자가 정보주체에게 그 사유를 알리고 열람을 제한하거나 거절할 수 있는 경우가 아닌 것은?

① 법률에 따라 열람이 금지되거나 제한되는 경우
② 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우
③ 공공기관이 조세의 부과·징수 또는 환급에 관한 업무를 수행할 때 중대한 지장을 초래하는 경우
④ 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우

정답 4번

①

법률에 따라 열람이 금지되거나 제한되는 경우에는 개인정보처리자가 정보주체에게 그 사유를 알리고 열람을 제한하거나 거절할 수 있다.

개인정보 보호법 제35조(개인정보의 열람)
④ 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체에게 그 사유를 알리고 열람을 제한하거나 거절할 수 있다.
1. 법률에 따라 열람이 금지되거나 제한되는 경우

②

열람으로 **다른 사람의 재산이나 그 밖의 이익을 부당하게 침해할 우려가 있는 경우**에는 정보주체에게 그 사유를 알리고 열람을 제한하거나 거절할 수 있다.

개인정보 보호법 제35조(개인정보의 열람)
④ 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체에게 그 사유를 알리고 열람을 제한하거나 거절할 수 있다.
2. 다른 사람의 생명 · 신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우

NoteBase

③

열람으로 **공공기관의 조세 부과·징수 또는 환급 업무 수행에 중대한 지장을 초래하는 경우**에는 정보주체에게 그 사유를 알리고 열람을 제한하거나 거절할 수 있다.

개인정보 보호법 제35조(개인정보의 열람)
④ 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체에게 그 사유를 알리고 열람을 제한하거나 거절할 수 있다.
3. 공공기관이 다음 각 목의 어느 하나에 해당하는 업무를 수행할 때 중대한 지장을 초래하는 경우
가. 조세의 부과 · 징수 또는 환급에 관한 업무

④

이 사유는 **개인정보의 수집·이용을 허용하는 근거**이며, 그 자체로 열람을 제한하거나 거절할 수 있는 사유는 아니다. 수집·이용도 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 않는 경우에 한한다.

개인정보 보호법 제15조(개인정보의 수집 · 이용)
① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다. <개정 2023.3.14>
6. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다.

개인정보 보호법 제35조(개인정보의 열람)
④ 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체에게 그 사유를 알리고 열람을 제한하거나 거절할 수 있다.
1. 법률에 따라 열람이 금지되거나 제한되는 경우
2. 다른 사람의 생명 · 신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우
3. 공공기관이 다음 각 목의 어느 하나에 해당하는 업무를 수행할 때 중대한 지장을 초래하는 경우
가. 조세의 부과 · 징수 또는 환급에 관한 업무
나. 「초 · 중등교육법」 및 「고등교육법」에 따른 각급 학교, 「평생교육법」에 따른 평생교육시설, 그 밖의 다른 법률에 따라 설치된 고등교육기관에서의 성적 평가 또는 입학자 선발에 관한 업무
다. 학력 · 기능 및 채용에 관한 시험, 자격 심사에 관한 업무
라. 보상금 · 급부금 산정 등에 대하여 진행 중인 평가 또는 판단에 관한 업무
마. 다른 법률에 따라 진행 중인 감사 및 조사에 관한 업무

NoteBase

문 20. 「보안관제 전문기업 지정 등에 관한 공고」상 보안관제 전문기업 지정기준으로 옳지 않은 것은?

① 법인 설립 이후 5년 이상일 것

② 자기 자본이 20억원 이상일 것

③ 보안관제 수행능력 평가기준에 따라 실시한 심사에서 70점 이상을 받을 것

④ 자격기준을 갖춘 기술인력을 15명 이상 보유할 것(고급기술자 3명 이상, 중급기술자 6명 이상을 포함하여야 한다)

정답 1번

①

보안관제 전문기업의 지정기준은 기술인력·자기자본·보안관제 수행능력 요건이다. **법인 설립 후 5년 경과를 요구하는 기준은 없다.**

보안관제 전문기업 지정 등에 관한 공고 제7조 (보안관제 전문기업 지정기준)
① 보안관제 전문기업 지정기준은 다음 각 호와 같다. 1. 별표 1에서 정한 자격을 갖춘 기술인력을 15명 이상 보유할 것(고급기술자 3명 이상, 중급기술자 6명 이상을 포함하여야 한다) 2. 자기 자본이 20억원 이상일 것(기업 재무제표의 자본총계를 의미한다.) 3. 별표 2의 보안관제 수행능력 평가기준에 따라 실시한 심사에서 70점 이상을 받을 것

②

자기자본은 **기업 재무제표의 자본총계가 20억원 이상**이어야 한다.

보안관제 전문기업 지정 등에 관한 공고 제7조 (보안관제 전문기업 지정기준)
① 보안관제 전문기업 지정기준은 다음 각 호와 같다.
2. 자기 자본이 20억원 이상일 것(기업 재무제표의 자본총계를 의미한다.)

③

보안관제 수행능력 평가기준에 따른 지정심사에서 **70점 이상**을 받아야 한다.

보안관제 전문기업 지정 등에 관한 공고 제7조 (보안관제 전문기업 지정기준)
① 보안관제 전문기업 지정기준은 다음 각 호와 같다.
3. 별표 2의 보안관제 수행능력 평가기준에 따라 실시한 심사에서 70점 이상을 받을 것

NoteBase

④

자격기준을 갖춘 **기술인력 15명 이상**을 보유해야 하며, 그 안에 **고급기술자 3명 이상과 중급기술자 6명 이상**이 포함되어야 한다.

보안관제 전문기업 지정 등에 관한 공고 제7조 (보안관제 전문기업 지정기준)
① 보안관제 전문기업 지정기준은 다음 각 호와 같다.
1. 별표 1에서 정한 자격을 갖춘 기술인력을 15명 이상 보유할 것(고급기술자 3명 이상, 중급기술자 6명 이상을 포함하여야 한다)

NoteBase