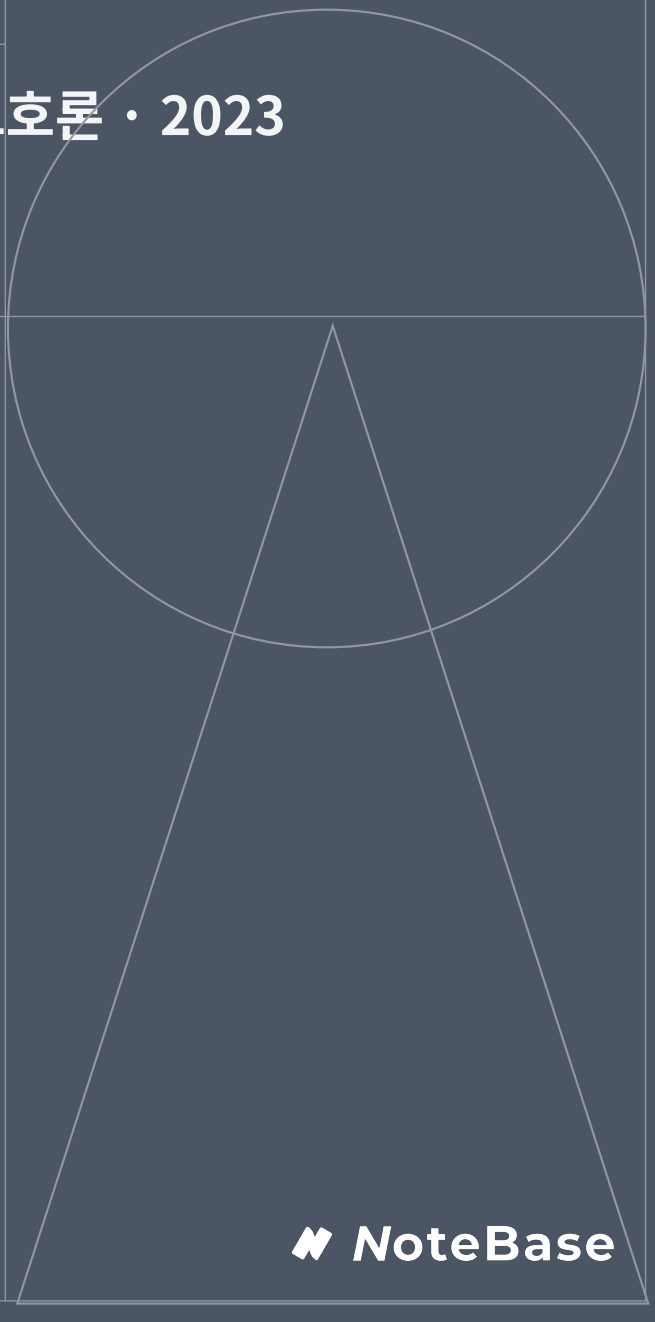
기출OX 해설집

공무원/국가직/9급 · 정보보호론 · 2023



NoteBase

기출OX 해설집

공무원/국가직/9급 · 정보보호론 · 2023

공무원/국가직/9급 · 정보보호론 · 2023

문 1. SSS(Server Side Script) 언어에 해당하지 않는 것은?

① IIS

② PHP

③ ASP

④ JSP

정답 1번

간단한 해설

IIS는 서버 측 스크립트 언어가 아니라 **웹 서버 소프트웨어**이다. 서버 측 스크립트는 서버에서 코드를 실행하여 웹 페이지의 내용을 생성하는 데 사용된다.

선지별 해설

① X: IIS(Internet Information Services)는 마이크로소프트의 **웹 서버 소프트웨어**이다. 클라이언트의 웹 요청을 받아 응답하며, ASP 등의 서버 측 프로그램이 실행될 환경을 제공한다. 스크립트를 실행할 수 있는 서버와 스크립트 언어 자체를 구분해야 한다.

② O: PHP는 **서버 측 스크립트 언어**이다. 서버에서 PHP 코드를 실행하여 데이터베이스 조회 등의 작업을 처리하고, 그 결과로 생성한 HTML 등을 클라이언트에 보낸다.

③ O: ASP(Active Server Pages)는 마이크로소프트의 서버 측 스크립트 기술이다. 웹 페이지에 포함된 **스크립트를 서버에서 실행**하고, 실행 결과로 만든 페이지를 클라이언트에 전달한다.

④ O: JSP(JavaServer Pages)는 **자바 기반의 서버 측 웹 페이지 생성 기술**이다. 서버에서 자바 코드를 이용해 동적인 내용을 처리하고, 생성한 응답을 클라이언트에 보낸다.

NoteBase

문 2. 정보나 정보시스템을 누가, 언제, 어떤 방법을 통하여 사용했는지 추적할 수 있도록 하는 것은?

① 인증성
② 가용성
③ 부인방지
④ 책임추적성

정답 4번

간단한 해설

정보시스템의 사용 이력을 특정 사용자와 연결하여 **누가, 언제, 어떤 방법으로 사용했는지** 확인할 수 있게 하는 성질이 책임추적성이다.

공통 해설

책임추적성은 정보나 정보시스템에서 이루어진 행위를 **그 행위를 한 주체에 연결해 추적할 수 있는 성질**이다. 문항의 '누가'는 사용 주체, '언제'는 사용 시점, '어떤 방법'은 사용 방식을 뜻한다. 이러한 사용 이력을 주체와 연결하면 특정 행위의 책임이 누구에게 있는지 추적할 수 있다.

예를 들어 사용자 식별정보, 접속 시각과 방식, 수행한 작업을 로그로 남기면 특정 작업을 누가 언제 어떤 방식으로 수행했는지 확인하는 데 활용할 수 있다. 이처럼 사용 행위와 주체를 연결하는 것이 문항에서 묻는 책임추적성의 핵심이다.

NoteBase

문 3. 디지털포렌식의 원칙에 대한 설명으로 옳지 않은 것은?

① 연계성의 원칙: 수집된 증거가 위변조되지 않았음을 증명해야 한다.

② 정당성의 원칙: 법률에서 정하는 적법한 절차와 방식으로 증거가 입수되어야 하며 입수 경위에서 불법이 자행되었다면 그로 인해 수집된 2차적 증거는 모두 무효가 된다.

③ 재현의 원칙: 불법 해킹 용의자의 해킹 도구가 증거 능력을 가지기 위해서는 같은 상황의 피해 시스템에 도구를 적용할 경우 피해 상황과 일치하는 결과가 나와야 한다.

④ 신속성의 원칙: 컴퓨터 내부의 정보는 휘발성을 가진 것이 많기 때문에 신속하게 수집되어야 한다.

정답 1번

간단한 해설

수집한 증거가 위·변조되지 않았음을 보장하는 것은 **무결성의 원칙**이다. 연계성의 원칙은 증거를 누가 언제 수집·보관·분석·인계했는지 그 취급 이력을 끊김 없이 기록하는 것이다.

선지별 해설

① X: 수집된 증거가 위·변조되지 않았음을 증명하는 것은 **무결성의 원칙**이다. 연계성의 원칙은 증거의 수집부터 보관·분석·법정 제출에 이르기까지 취급자, 취급 시각, 인계 과정 등을 기록하여 증거의 이동과 관리 이력을 추적할 수 있게 하는 것이다. 증거 내용이 바뀌지 않았는지와 증거가 누구의 관리를 거쳤는지를 구분해야 한다.

② O: 정당성의 원칙은 **적법한 절차와 방식으로 증거를 수집**해야 한다는 뜻이다. 형사소송법 제308조의2는 적법한 절차에 따르지 않고 수집한 증거를 증거로 할 수 없도록 한다. 위법하게 수집한 증거를 기초로 얻은 2차적 증거도 원칙적으로 유죄 인정의 증거로 사용할 수 없다. 이 문항의 '모두 무효'는 이러한 증거 배제 원칙을 설명한 취지로 이해한다. 다만 실제 법리에서는 위법한 수집과의 인과관계가 희석·단절되었다고 평가되는 예외적인 경우 2차적 증거의 증거능력이 인정될 수 있으므로, 예외 없는 절대적 배제로 확대해서는 안 된다(대법원 2025. 1. 9. 선고 2024도12689 판결).

③ O: 재현의 원칙은 **같은 조건에서 같은 결과가 나오는지** 확인할 수 있어야 한다는 뜻이다. 해킹 도구를 피해 당시와 같은 조건의 시스템에 적용했을 때 동일한 피해 현상이 나타난다면, 그 도구가 해당 피해를 일으킬 수 있다는 분석 결과를 검증할 수 있다. 이는 분석 결과의 신뢰성을 확보하기 위한 것으로, 적법한 수집 등 다른 증거능력 요건도 별도로 충족해야 한다.

④ O: 신속성의 원칙은 시간이 흐르거나 시스템 상태가 바뀌면서 증거가 사라지는 것을 막기 위해 신속히 수집해야 한다는 뜻이다. 특히 메모리에 있는 실행 중인 프로그램이나 접속 상태 등의 정보는 **전원이 꺼지면 사라질 수 있는 휘발성 정보**이므로, 수집이 지연되면 복구하기 어려울 수 있다.

NoteBase

문 4. 다음에서 설명하는 국내 인증 제도는?

◯ 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 의한 정보보호 관리체계 인증과 「개인정보 보호법」에 의한 개인정보보호 관리체계 인증에 관한 사항을 통합하여 한국인터넷진흥원과 금융보안원에서 인증하고 있다.
◯ 한국정보통신진흥협회, 한국정보통신기술협회, 개인정보보호협회에서 인증심사를 수행하고 있다.

① CC
② BS7799
③ TCSEC
④ ISMS-P

정답 4번

간단한 해설

ISMS-P는 **정보보호 관리체계 인증과 개인정보보호 관리체계 인증을 통합**한 국내 인증 제도이다. 지문의 두 관리체계 인증을 함께 다룬다는 조건이 이를 식별하는 핵심이다.

공통 해설

ISMS-P는 '정보보호 및 개인정보보호 관리체계 인증'이다. 기존의 정보보호 관리체계 인증(ISMS)과 개인정보보호 관리체계 인증(PIMS)을 통합하여, 조직이 수행하는 정보보호·개인정보보호 조치와 활동이 인증기준에 적합한지 확인하는 제도이다. 따라서 지문의 **두 관리체계 인증의 통합**이라는 설명은 ISMS-P에 대응한다.

지문에서 한국인터넷진흥원과 금융보안원은 인증을 담당하고,
한국정보통신진흥협회·한국정보통신기술협회·개인정보보호협회는 인증심사를 수행하는 기관으로 제시되어 있다. 이러한 인증기관과 심사기관의 역할 구분도 ISMS-P의 인증체계에 부합한다.

NoteBase

문 5. 「개인정보 보호법」 제28조의2(가명정보의 처리 등)의 내용으로서 (가)와 (나)에 들어갈 용어를 바르게 연결한 것은?

제1항 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록 보존 등을 위하여 정보주체의 (가) 가명정보를 처리할 수 있다.
제2항 개인정보처리자는 제1항에 따라 가명정보를 제3자에게 제공하는 경우에는 특정 개인을 알아보기 위하여 사용될 수 있는 정보를 포함 (나).

① (가): 동의를 받아, (나): 할 수 있다
② (가): 동의를 받아, (나): 해서는 아니 된다
③ (가): 동의 없이, (나): 해서는 아니 된다
④ (가): 동의 없이, (나): 할 수 있다

정답 3번

③

통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 개인정보처리자는 **정보주체의 동의 없이** 가명정보를 처리할 수 있다. 이를 제3자에게 제공할 때에는 **특정 개인을 알아보기 위해 사용될 수 있는 정보를 포함해서는 아니 된다**.

개인정보 보호법 제28조의2(가명정보의 처리 등)
① 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있다.
② 개인정보처리자는 제1항에 따라 가명정보를 제3자에게 제공하는 경우에는 특정 개인을 알아보기 위하여 사용될 수 있는 정보를 포함해서는 아니 된다.

NoteBase

문 6. SSL을 구성하는 프로토콜에 대한 설명으로 옳은 것은?

① Handshake는 두 단계로 이루어진 메시지 교환 프로토콜로서 클라이언트와 서버 사이의 암호학적 비밀 확립에 필요한 정보를 교환하기 위한 것이다.

② 클라이언트와 서버는 각각 상대방에게 ChangeCipherSpec 메시지를 전달함으로써 메시지의 서명 및 암호화에 필요한 매개변수가 대기 상태에서 활성화되어 비로소 사용할 수 있게 된다.

③ 송신 측의 Record 프로토콜은 응용 계층 또는 상위 프로토콜의 메시지를 단편화, 암호화, 압축, 서명, 헤더 추가의 순서로 처리하여 전송 프로토콜에 전달한다.

④ Alert 프로토콜은 Record 프로토콜의 하위 프로토콜로서 처리 과정의 오류를 알리는 메시지를 전달한다.

정답 2번

간단한 해설

ChangeCipherSpec는 협상한 보안 매개변수를 **대기 상태에서 현재 사용 상태로 전환**하는 신호이다. 이 메시지 이후의 레코드부터 새로 합의한 알고리즘과 키를 적용한다.

선지별 해설

① X: Handshake가 암호학적 비밀 확립에 필요한 정보를 교환한다는 설명은 맞지만, '두 단계'라는 설명이 틀렸다. 일반적인 전체 Handshake는 **네 단계**, 즉 보안 기능 설정 → 서버 인증 및 키 교환 → 클라이언트 인증 및 키 교환 → 종료로 구분한다. 인증 관련 메시지는 선택한 암호 방식과 인증 요구에 따라 생략될 수 있다.

② O: Handshake에서 협상한 알고리즘과 키 등은 먼저 대기 상태에 저장된다. ChangeCipherSpec를 보내면 송신 측의 대기 쓰기 상태가, 이를 받으면 수신 측의 대기 읽기 상태가 **현재 상태로 전환**된다. 따라서 이후 레코드에 새 보안 매개변수가 적용된다. 다만 선지의 '서명'과 관련된 레코드 무결성 보호는 공개키 전자서명이 아니라 메시지 인증 코드(MAC)를 이용한다.

③ X: 송신 측의 처리 순서는 **단편화 → 압축 → MAC 추가 → 암호화 → 헤더 추가**이다. 압축된 데이터에 무결성 검증용 MAC을 붙인 다음 함께 암호화한다. 선지는 압축과 암호화의 순서를 바꾸었으며, MAC 추가도 암호화보다 앞서야 한다. 압축을 사용하지 않기로 협상하면 압축 단계에서 데이터가 그대로 유지된다.

④ X: Alert는 Record의 하위가 아니라 **상위 프로토콜**이다. 오류나 연결 종료 등을 알리는 Alert 메시지를 Record가 캡슐화하여 운반한다. 즉 Alert는 경고 내용을 정하고, Record는 그 메시지의 전송과 보호를 담당한다.

NoteBase

문 7. 블록체인 기술의 하나인 하이퍼레저 패브릭에 대한 설명으로 옳지 않은 것은?

① 허가형 프라이빗 블록체인의 형태로 MSP(Membership Service Provider)라는 인증 관리 시스템에 등록된 사용자만 참여할 수 있다.

② 체인코드라는 스마트 컨트랙트를 통해서 분산 원장의 데이터를 읽고 쓸 수 있다.

③ 분산 원장은 원장의 현재 상태를 나타내는 월드 스테이트와 원장의 생성 시점부터 현재까지의 사용 기록을 저장하는 블록체인 두 가지로 구성된다.

④ 트랜잭션을 정해진 순서로 정렬하는 과정을 합의로 정의하고, 이를 위해 지분 증명 방식과 BFT(Byzantine Fault Tolerance) 알고리즘을 사용한다.

정답 4번

간단한 해설

④의 '지분 증명 방식을 사용한다'는 설명이 잘못되었다. 패브릭은 **허가된 정렬 노드들이 트랜잭션 순서에 합의**하며, 암호화폐 지분을 기준으로 합의에 참여하는 지분 증명 방식을 사용하지 않는다.

선지별 해설

① O: 패브릭은 참여자의 신원을 확인하고 참여를 허가하는 블록체인이다. MSP는 신뢰할 인증기관과 구성원의 신원·역할을 정의하여, **네트워크에서 인정한 신원인지 확인**하는 기준을 제공한다. 따라서 누구나 익명으로 참여하는 방식과 달리, 인정된 신원을 갖춘 사용자가 권한에 따라 참여한다.

② O: 체인코드는 업무 규칙을 구현한 스마트 컨트랙트를 실행하는 프로그램이다. 이를 호출하여 원장 상태를 조회하거나 변경을 요청할 수 있다. 변경 요청은 체인코드 실행만으로 즉시 확정되는 것이 아니라, **보증·정렬·검증을 거쳐** 유효한 트랜잭션의 결과가 원장에 반영된다.

③ O: 패브릭의 원장은 **현재 값인 월드 스테이트와 거래 이력인 블록체인**으로 구성된다. 월드 스테이트는 각 데이터의 최신 상태를 저장하고, 블록체인은 트랜잭션을 순서대로 블록에 기록한다. 예를 들어 자산 소유자가 A에서 B로 바뀌면 월드 스테이트에는 현재 소유자 B가 나타나고, 블록체인에는 소유권 변경 이력이 남는다.

④ X: 정렬 서비스가 트랜잭션의 공통 순서를 정하도록 합의한다는 취지는 맞지만, **지분 증명(PoS)을 사용한다는 부분**이 잘못되었다. 패브릭은 허가된 정렬 노드 사이에서 Raft 등의 합의 프로토콜을 사용하며, 암호화폐 지분을 기준으로 합의 참여자를 정하지 않는다. Raft는 노드의 중단 장애를 견디는 CFT 방식이다. Fabric 3.0부터는 악의적으로 행동하는 일부 노드에도 대응하는 SmartBFT 기반 정렬 서비스가 지원되므로, BFT 지원 자체를 패브릭에 없는 특성으로 단정해서는 안 된다.

NoteBase

문 9. (가)와 (나)에 들어갈 용어를 바르게 연결한 것은?

악성 코드의 정적 분석은 파일을 (가)하여 상세한 동작을 분석하는 단계로 악성 코드 파일을 역공학 분석하여 그 구조, 핵심이 되는 명령 부분, 동작 방식 등을 알아내는 것을 목표로 한다. 이를 위하여 역공학 분석을 위한 (나)와/과 같은 도구를 활용한다.

① (가): 패킹, (나): OllyDbg
② (가): 패킹, (나): Regshot
③ (가): 디스어셈블링, (나): Regshot
④ (가): 디스어셈블링, (나): OllyDbg

정답 4번

간단한 해설

기계어를 어셈블리 명령어로 바꾸어 코드의 구조와 동작을 읽는 과정이 **디스어셈블링**이다. **OllyDbg**는 이 기능을 갖추어 역공학 분석에 활용된다.

빈칸별 해설

(가) 디스어셈블링: 실행 파일의 기계어를 사람이 읽을 수 있는 **어셈블리 명령어로 변환**하는 과정이다. 변환된 명령어와 분기·함수 호출 등을 살펴 코드의 구조와 동작 방식을 파악하므로, 지문의 역공학 분석에 해당한다. 패킹은 실행 파일을 압축하거나 내부 코드를 감싸는 처리로, 명령어를 읽을 수 있게 풀어 분석하는 디스어셈블링과 구별된다.

(나) OllyDbg: 기계어를 어셈블리 명령어로 보여 주고 코드를 분석하는 기능을 갖춘 역공학 도구이다. OllyDbg는 **실행 제어도 가능한 디버거**이므로 정적 분석 전용 도구라는 뜻은 아니며, 이 문항에서는 디스어셈블링과 코드 분석 기능에 주목한다. 반면 Regshot은 서로 다른 시점의 레지스트리 스냅샷을 비교하는 도구이다. 악성 코드 분석에서는 실행 전후 레지스트리의 변화를 확인하는 데 활용되며, 명령어 자체를 해석하는 도구는 아니다.

따라서 (가)는 디스어셈블링, (나)는 OllyDbg로 연결되며, 이 조합은 ④에 해당한다.

NoteBase

문 10. 프로그램 입력 값에 대한 검증 누락, 부적절한 검증 또는 데이터의 잘못된 형식 지정으로 인해 발생할 수 있는 보안 공격이 아닌 것은?

① HTTP GET 플러딩

② SQL 삽입

③ 크로스사이트 스크립트

④ 버퍼 오버플로우

정답 1번

간단한 해설

HTTP GET 플러딩은 **정상적인 형식의 GET 요청을 대량으로 보내** 서버의 처리 자원을 소모시키는 서비스 거부 공격이다. 입력값의 형식이나 내용에 대한 검증 결함을 이용하는 것이 핵심인 공격과 구별된다.

선지별 해설

각 선지는 입력값의 검증·처리 결함을 이용하는 공격에 해당하는지를 기준으로 판단한다.

① X: HTTP GET 플러딩은 웹 자원을 요청하는 GET 메시지를 대량으로 전송하여 서버의 처리 능력을 소진시키는 공격이다. **요청의 형식과 내용이 정상이어도** 과도한 요청량 때문에 서비스가 지연되거나 중단될 수 있다. 따라서 입력값 검증 누락이나 잘못된 데이터 형식을 이용하는 공격이 아니라, 요청량으로 가용성을 침해하는 서비스 거부 공격으로 구분한다.

② O: SQL 삽입은 외부 입력에 포함된 SQL 구문이 데이터베이스 질의의 일부로 실행되도록 하는 공격이다. 입력값을 질의문에 부적절하게 결합하면 **단순한 데이터가 명령으로 해석**되어 질의의 조건이나 의미가 바뀔 수 있다. 따라서 입력값을 적절히 검증·처리하지 않은 경우 발생할 수 있다.

③ O: 크로스사이트 스크립트는 공격자가 삽입한 악성 스크립트가 다른 사용자의 브라우저에서 실행되도록 하는 공격이다. 외부 입력을 웹 페이지에 반영하면서 적절히 검증하거나 출력 맥락에 맞게 인코딩하지 않으면, **입력된 문자열이 실행 가능한 코드로 처리**될 수 있다. 예를 들어 게시글의 악성 스크립트가 그대로 페이지에 포함되면 이를 열람한 사용자의 브라우저에서 실행될 수 있다.

④ O: 버퍼 오버플로우는 확보된 메모리 공간인 버퍼의 경계를 넘어 데이터를 기록하는 현상이다. 입력 데이터를 복사하면서 **입력 길이가 버퍼 크기를 넘는지 확인하지 않으면** 인접한 메모리가 덮어써질 수 있다. 공격자는 이를 이용해 프로그램을 비정상 종료시키거나 실행 흐름을 바꿀 수 있으므로, 입력 크기에 대한 검증이 부적절할 때 발생할 수 있는 공격이다.

NoteBase

문 11. 정보의 무결성에 중점을 둔 보안 모델은?

① Biba

② Bell-LaPadula

③ Chinese Wall

④ Lattice

정답 1번

간단한 해설

Biba 모델은 정보가 부적절하게 변경되거나 훼손되는 것을 막는 **무결성** 중심의 보안 모델이다.

공통 해설

무결성은 정보가 허가 없이 변경되거나 훼손되지 않도록 하여 정확성과 완전성을 유지하는 성질이다. 따라서 이 문항에서는 정보의 노출을 막는지보다 **부적절한 변경을 막는지**가 모델을 식별하는 기준이다.

Biba 모델은 주체와 객체의 무결성 등급을 바탕으로 접근을 제한하여, 신뢰도가 낮은 주체나 데이터가 높은 무결성 등급의 정보를 오염시키는 것을 방지한다. 예를 들어 엄격 무결성 정책에서는 낮은 무결성 등급의 프로그램이 높은 등급의 파일에 쓰는 것을 금지한다. 이러한 정보의 변경 통제가 문제에서 묻는 무결성 중심의 보안 모델에 해당한다.

NoteBase

문 12. 허니팟에 대한 설명으로 옳지 않은 것은?

① 공격자가 중요한 시스템에 접근하지 못하도록 실제 시스템처럼 보이는 곳으로 유인한다.

② 공격자의 행동 패턴에 관한 정보를 수집한다.

③ 허니팟은 방화벽의 내부망에는 설치할 수 없다.

④ 공격자가 가능한 한 오랫동안 허니팟에서 시간을 보내도록 하고 그사이 관리자는 필요한 대응을 준비한다.

정답 3번

간단한 해설

허니팟은 **방화벽의 내부망에도 설치할 수 있다**. 내부망에 배치하면 내부 공격이나 이미 침입한 공격자의 활동을 탐지하고 관찰하는 데 활용한다.

선지별 해설

① O: 허니팟은 실제 시스템처럼 보이도록 구성한 유인용 시스템이다. 공격자의 관심과 공격을 **보호 대상에서 유인용 시스템으로 돌려** 중요한 시스템을 보호하는 데 활용한다.

② O: 허니팟에 대한 접속과 공격 과정 등을 기록하면 **공격자의 행동 패턴과 공격 기법**을 파악할 수 있다. 이렇게 수집한 정보는 침입 탐지와 대응 방안을 개선하는 자료가 된다.

③ X: 허니팟의 설치 위치가 방화벽 외부로 한정되는 것은 아니다. 목적에 따라 외부망이나 DMZ뿐 아니라 **방화벽 내부망에도 설치할 수 있다**. 내부망에 설치한 허니팟은 내부자의 공격이나 이미 침입한 공격자의 내부 활동을 탐지하는 데 활용한다.

④ O: 공격자가 실제 시스템으로 여기는 허니팟에 **오랫동안 머물도록 유도**하면 공격 행동을 관찰하고 대응할 시간을 확보할 수 있다. 관리자는 그동안 공격 정보를 분석하고 실제 보호 대상에 대한 차단·격리 등의 대응을 준비한다.

NoteBase

문 13. 다음에 설명하는 위험 분석 방법은?

◯ 구조적인 방법론에 기반하지 않고 분석가의 경험이나 지식을 사용하여 위험 분석을 수행한다.
◯ 중소 규모의 조직에는 적합할 수 있으나 분석가의 개인적 경험에 지나치게 의존한다는 단점이 있다.

① 기준선 접근법
② 비정형 접근법
③ 상세 위험 분석
④ 복합 접근법

정답 2번

간단한 해설

구조적인 방법론 대신 **분석가의 경험과 지식**에 의존하여 위험을 분석하는 방식이 비정형 접근법이다. 개인적 판단에 크게 의존한다는 단점도 이 특징에서 나온다.

공통 해설

비정형 접근법은 **정해진 구조적 방법론에 기반하지 않고** 분석가의 경험과 지식으로 위험을 식별하고 평가하는 방법이다. 제시문의 '구조적인 방법론에 기반하지 않는다'와 '분석가의 경험이나 지식을 사용한다'는 이 방법을 구별하는 두 단서이다.

중소 규모 조직에는 적합할 수 있지만, 분석 과정과 판단이 분석가 개인의 역량에 크게 좌우된다. 따라서 분석가가 달라지면 중요하게 보는 위험이나 평가 결과가 달라질 수 있으며, 개인적 경험에 지나치게 의존한다는 한계가 생긴다.

NoteBase

문 14. RSA를 적용하여 7의 암호문 11과 35의 암호문 42가 주어져 있을 때, 알고리즘의 수학적 특성을 이용하여 계산한 245(=7 * 35)의 암호문은? (단, RSA 공개 모듈 n = 247, 공개 지수 e = 5)

① 2

② 215

③ 239

④ 462

정답 2번

간단한 해설

RSA의 **곱셈 성질**에 따라 두 평문의 곱에 대한 암호문은 각 암호문을 곱한 뒤 모듈러 연산을 하여 구한다. 11 × 42 = 462를 247로 나눈 나머지는 215이므로, 245의 암호문은 215이다.

계산 과정

RSA에서 평문 m의 암호문은 E(m)=m^e n이다. 여기서 n은 나머지를 구할 때의 기준인 공개 모듈이고, e는 공개 지수이다. 이 문제에서는 n = 247, e = 5이며, 7과 35를 암호화한 값이 각각 11과 42로 주어져 있다.

구하려는 평문은 245 = 7 × 35이다. **동일한 공개 모듈과 공개 지수**를 적용하면 $(ab)^e = a^e \cdot b^e$이므로 E(ab)≡E(a)E(b)±od n이 성립한다. 따라서 245의 암호문은 주어진 두 암호문 11과 42를 곱한 뒤 247로 나눈 나머지로 구할 수 있다. 공개 지수 5를 적용한 결과가 이미 두 암호문에 반영되어 있으므로, 이 곱에 다시 5제곱을 하지 않는다.

두 암호문의 곱은 11 × 42 = 462이다. 이 값은 아직 모듈러 연산을 하기 전의 값이므로, **247로 나눈 나머지**를 구한다. 462 = 247 × 1 + 215이므로 나머지는 215이다. 따라서 245의 암호문은 215로, ②의 값과 일치한다.

NoteBase

문 15. 사용자 A가 사전에 비밀키를 공유하고 있지 않은 사용자 B에게 기밀성 보장이 요구되는 문서 M을 보내기 위한 메시지로 옳은 것은?

KpuX: 사용자 X의 공개키
KprX: 사용자 X의 개인키
KS: 세션키
H(): 해시 함수
E(): 암호화
||: 연결(concatenation) 연산자

① M \|| E_KprA(H(M))
② E_KprA(M \|| H(M))
③ E_KS(M) \|| E_KpuB(KS)
④ E_KS(M) \|| E_KprA(KS)

정답 3번

간단한 해설

문서 M은 **세션키로 암호화**하고, 그 세션키는 **수신자 B의 공개키로 암호화**하여 함께 보낸다. B는 자신의 개인키로 세션키를 얻을 수 있으므로, 사전에 비밀키를 공유하지 않아도 문서를 복호화할 수 있다.

NoteBase

핵심 풀이

문서 M의 보호: 기밀성은 허가받지 않은 사람이 문서 내용을 알 수 없도록 하는 성질이다. A는 세션키 KS로 문서를 암호화하여 $E_{KS}(M)$을 만든다. 그러나 B와 비밀키를 미리 공유하지 않았으므로, B가 KS를 안전하게 얻을 방법도 필요하다.

세션키 KS의 전달: A는 **B의 공개키로 세션키를 암호화**하여 $E_{KpuB}(KS)$를 만든다. 두 암호문을 연결한 메시지는 E_KS(M) \| E_KpuB(KS)이며, 이를 전자봉투 방식이라고 한다. B는 자신의 개인키 KprB로 세션키를 복원한 다음, 그 세션키로 문서 암호문을 복호화한다. 따라서 사전에 비밀키를 공유할 필요가 없다.

①·②와의 구분: ①은 문서 M을 암호화하지 않고 그대로 보내므로, 해시값에 A의 개인키를 적용한 부분이 있어도 문서의 기밀성을 보장하지 못한다. ②는 문서와 해시값을 A의 개인키로 암호화하지만, **A의 공개키로 복원할 수 있어** B만 내용을 읽도록 제한하지 못한다.

④와의 구분: 문서를 세션키로 암호화한 점은 같지만, 세션키를 A의 개인키로 암호화하였다. A의 공개키를 아는 사람도 세션키를 복원하여 문서를 읽을 수 있으므로, 세션키 보호에는 **A의 개인키가 아니라 B의 공개키**를 사용해야 한다.

NoteBase

문 16. 보안 서비스와 이를 제공하기 위한 보안 기술을 잘못 연결한 것은?

① 데이터 무결성 - 암호학적 해시

② 신원 인증 - 인증서

③ 부인방지 - 메시지 인증 코드

④ 메시지 인증 - 전자 서명

정답 3번

간단한 해설

메시지 인증 코드는 송신자와 수신자가 **같은 비밀키를 공유**하므로 수신자도 유효한 코드를 만들 수 있다. 따라서 제3자에게 송신자가 작성했음을 입증하는 **부인방지를 제공하지 못하며**, 이를 위해서는 전자 서명을 이용한다.

선지별 해설

① O: 암호학적 해시는 데이터로부터 일정한 길이의 해시값을 계산한다. 데이터를 변경하면 일반적으로 해시값도 달라지므로, 현재 데이터의 해시값을 **신뢰할 수 있는 원본 해시값과 비교**하여 무결성을 확인할 수 있다. 다만 공격자가 데이터와 비교용 해시값을 함께 바꿀 수 있다면 해시값 비교만으로는 변조를 탐지할 수 없다.

② O: 인증서는 인증기관의 전자 서명을 통해 **신원 정보와 공개키의 연결**을 보증한다. 인증서의 유효성을 확인하고 상대방이 해당 공개키에 대응하는 개인키를 보유했는지 검증하면 신원 인증에 활용할 수 있다. 인증서 파일을 제시했다는 사실만으로 신원 인증이 완성되는 것은 아니다.

③ X: 메시지 인증 코드(MAC)는 메시지와 공유 비밀키로 생성하며, 메시지의 무결성과 인증에 사용한다. 그러나 송신자와 수신자가 같은 키를 알기 때문에 **수신자도 동일한 메시지 인증 코드를 생성**할 수 있다. 따라서 제3자에게 송신자의 작성 사실을 입증하는 부인방지 수단으로 사용할 수 없다. 부인방지에는 서명자의 개인키로 생성하고 공개키로 검증하는 전자 서명을 연결해야 한다.

④ O: 전자 서명은 서명자의 개인키로 생성하고 대응하는 공개키로 검증한다. 검증을 통해 **메시지가 서명 후 변경되지 않았는지**와 해당 개인키로 서명되었는지를 확인하므로 메시지 인증에 활용할 수 있다. 서명자의 신원까지 확인하려면 인증서 등으로 공개키와 서명자의 연결도 신뢰할 수 있어야 한다.

NoteBase

문 17. 웹 서버와 클라이언트 간의 쿠키 처리 과정으로 옳지 않은 것은?

① HTTP 요청 메시지의 헤더 라인을 통한 쿠키 전달

② HTTP 응답 메시지의 상태 라인을 통한 쿠키 전달

③ 클라이언트 브라우저의 쿠키 디렉터리에 쿠키 저장

④ 웹 서버가 클라이언트에 관해 수집한 정보로부터 쿠키를 생성

정답 2번

간단한 해설

②의 '상태 라인'은 '헤더 라인'으로 고쳐야 한다. 서버는 HTTP 응답의 **Set-Cookie 헤더**로 쿠키를 전달하며, 상태 라인은 상태 코드 등 응답의 처리 결과를 나타낸다.

선지별 해설

① O: 브라우저는 저장된 쿠키 중 전송 조건에 맞는 것을 골라 HTTP 요청의 **Cookie 헤더**에 담아 서버로 보낸다. 서버는 이를 이용해 이전 요청과 이어지는 사용자 상태를 식별할 수 있다.

② X: 서버가 브라우저에 쿠키를 전달하는 위치는 HTTP 응답의 **Set-Cookie 헤더**이다. 상태 라인은 HTTP/1.1에서 'HTTP/1.1 200 OK'처럼 프로토콜 버전, 상태 코드와 사유 구절을 나타내는 첫 줄이며, 쿠키를 전달하는 부분이 아니다.

③ O: 서버가 전달한 쿠키는 **클라이언트 측에서 브라우저가 저장·관리**한다. 선지의 '쿠키 디렉터리'는 이러한 저장 공간을 가리킨다. 다만 구체적인 저장 방식은 브라우저와 쿠키 종류에 따라 달라지므로, 모든 쿠키가 반드시 별도의 디스크 파일로 저장된다는 뜻은 아니다.

④ O: 웹 서버는 클라이언트에 관해 얻은 정보나 서비스 처리 결과를 바탕으로 **쿠키의 이름과 값**을 정해 생성할 수 있다. 예를 들어 사용자가 선택한 언어를 쿠키 값으로 보내면, 브라우저가 이를 저장했다가 이후 요청에 포함해 서버가 해당 언어 설정을 유지하도록 할 수 있다.

NoteBase

문 18. 「개인정보 보호법」 제15조(개인정보의 수집·이용)에서 개인정보 처리자가 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있는 경우에 해당하지 않는 것은?

① 정보주체의 동의를 받은 경우
② 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
③ 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우
④ 공공기관과의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우

정답 4번

①

개인정보처리자는 **정보주체의 동의를 받은 경우** 개인정보를 수집하고 수집 목적의 범위에서 이용할 수 있다.

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>
1. 정보주체의 동의를 받은 경우

②

개인정보처리자는 **법률에 특별한 규정이 있거나 법령상 의무 준수를 위해 불가피한 경우** 개인정보를 수집하고 수집 목적의 범위에서 이용할 수 있다.

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>
2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우

③

공공기관이 법령 등에서 정한 소관 업무 수행을 위해 불가피한 경우에는 개인정보를 수집하고 수집 목적의 범위에서 이용할 수 있다.

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>
3. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우

NoteBase

④

계약을 근거로 수집·이용하려면 **정보주체와 체결한 계약의 이행** 또는 **계약 체결 과정에서 정보주체의 요청에 따른 조치의 이행**에 필요해야 한다. 공공기관과의 계약이라는 사유만으로는 해당하지 않는다.

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>
4. 정보주체와 체결한 계약을 이행하거나 계약을 체결하는 과정에서 정보주체의 요청에 따른 조치를 이행하기 위하여 필요한 경우

NoteBase

문 19. 함수 P에서 호출한 함수 Q가 자신의 작업을 마치고 다시 함수 P로 돌아가는 과정에서의 스택 버퍼 운용 과정을 순서대로 바르게 나열한 것은?

(가) 스택에 저장되어 있는 복귀 주소(return address)를 pop한다.
(나) 스택 포인터를 프레임 포인터의 값으로 복원시킨다.
(다) 이전 프레임 포인터 값을 pop하여 스택 프레임 포인터를 P의 스택 프레임으로 설정한다.
(라) P가 실행했던 함수 호출(function call) 인스트럭션 다음의 인스트럭션을 실행한다.

① (가) → (나) → (다) → (라)
② (가) → (다) → (라) → (나)
③ (나) → (가) → (라) → (다)
④ (나) → (다) → (가) → (라)

정답 4번

간단한 해설

함수 Q의 지역 변수 공간을 먼저 정리해야 저장된 정보를 올바르게 꺼낼 수 있다. 이어서 **이전 프레임 포인터를 복원**한 뒤 **복귀 주소**를 꺼내면, 함수 P의 호출 명령 다음부터 실행을 이어 갈 수 있다.

올바른 순서

(나) → (다) → (가) → (라)

(나) 스택 포인터 복원: 스택 포인터는 현재 스택의 맨 위를, 프레임 포인터는 현재 함수의 스택 프레임 기준 위치를 가리킨다. Q의 프레임 포인터 값을 스택 포인터에 대입하면 Q의 지역 변수 등에 사용한 공간을 한꺼번에 정리하고, **저장된 이전 프레임 포인터를 꺼낼 위치**로 스택 포인터를 되돌린다.

(다) 이전 프레임 포인터 복원: pop은 스택 맨 위의 값을 꺼내고 스택 포인터를 다음 항목의 위치로 옮기는 연산이다. 저장되어 있던 P의 프레임 포인터 값을 pop하여 프레임 포인터에 넣으면 **P의 스택 프레임 기준 위치**가 복원되고, 스택 맨 위에는 복귀 주소가 남는다.

(가) 복귀 주소 꺼내기: 이전 프레임 포인터를 꺼낸 다음에 스택 맨 위의 복귀 주소를 pop한다. 이 주소는 **P에서 Q를 호출한 명령 바로 다음 명령의 주소**이며, 실행 위치를 이 주소로 옮겨 Q에서 P로 제어를 돌려준다.

(라) P의 실행 재개: 복귀 주소로 제어가 이동했으므로 P가 실행했던 함수 호출 명령 다음 명령을 실행한다. 호출 명령 자체로 돌아가면 Q를 다시 호출하게 되므로, 실행을 이어 갈 위치는 **호출 명령 다음**이다.

NoteBase

문 20. 무선 네트워크 보안에 대한 설명으로 옳은 것은?

① 이전에 사용했던 WEP의 보안상 약점을 보강하기 위해서 IETF에서 WPA, WPA2, WPA3를 정의하였다.

② WPA는 TKIP 프로토콜을 채택하여 보안을 강화하였으나 여전히 WEP와 동일한 메시지 무결성 확인 방식을 사용하는 약점이 있다.

③ WPA2는 무선 LAN 보안 표준인 IEEE 802.1X의 보안 요건을 충족하기 위하여 CCM 모드의 AES 블록 암호 방식을 채택하고 있다.

④ WPA-개인 모드에서는 PSK로부터 유도된 암호화 키를 사용하는 반면에, WPA-엔터프라이즈 모드에서는 인증 및 암호화를 강화하기 위해 RADIUS 인증 서버를 두고 EAP 표준을 이용한다.

정답 4번

간단한 해설

WPA-개인 모드는 미리 공유한 비밀키인 **PSK를 바탕으로 통신용 암호화 키를 유도**한다. 엔터프라이즈 모드는 **802.1X·EAP와 RADIUS 인증 서버**를 이용해 사용자나 단말을 인증하고 통신 키를 설정한다.

선지별 해설

① X: WPA, WPA2, WPA3를 도입하고 인증 프로그램을 운영한 주체는 **Wi-Fi Alliance**이다. WEP의 보안상 약점을 보완했다는 취지는 맞지만, IETF가 이들을 정의했다는 부분이 틀렸다.

② X: WPA가 TKIP를 채택했다는 부분은 맞지만, WEP와 무결성 확인 방식이 같지는 않다. WEP는 CRC-32 기반의 무결성 검사값인 ICV를 사용하고, WPA의 TKIP는 **Michael 알고리즘의 MIC를 추가**하여 메시지 변조에 대한 보호를 강화한다.

③ X: WPA2의 AES-CCMP 채택과 연결되는 무선 LAN 보안 표준은 **IEEE 802.11i**이다. CCMP는 AES의 CCM 모드를 이용해 기밀성과 무결성을 제공한다. IEEE 802.1X는 사용자나 단말의 인증을 바탕으로 네트워크 접속을 제어하는 표준이므로 두 표준을 구별해야 한다.

④ O: WPA-개인 모드는 사전에 공유한 비밀키인 PSK를 바탕으로 실제 통신에 사용할 암호화 키를 유도한다. WPA-엔터프라이즈 모드는 **802.1X·EAP 기반 인증**을 수행하며, 일반적으로 RADIUS 인증 서버가 인증을 처리한다. 인증 과정에서 얻은 키 재료를 바탕으로 통신용 암호화 키를 유도하므로, EAP 자체가 데이터를 암호화하는 알고리즘이라는 뜻은 아니다.

NoteBase