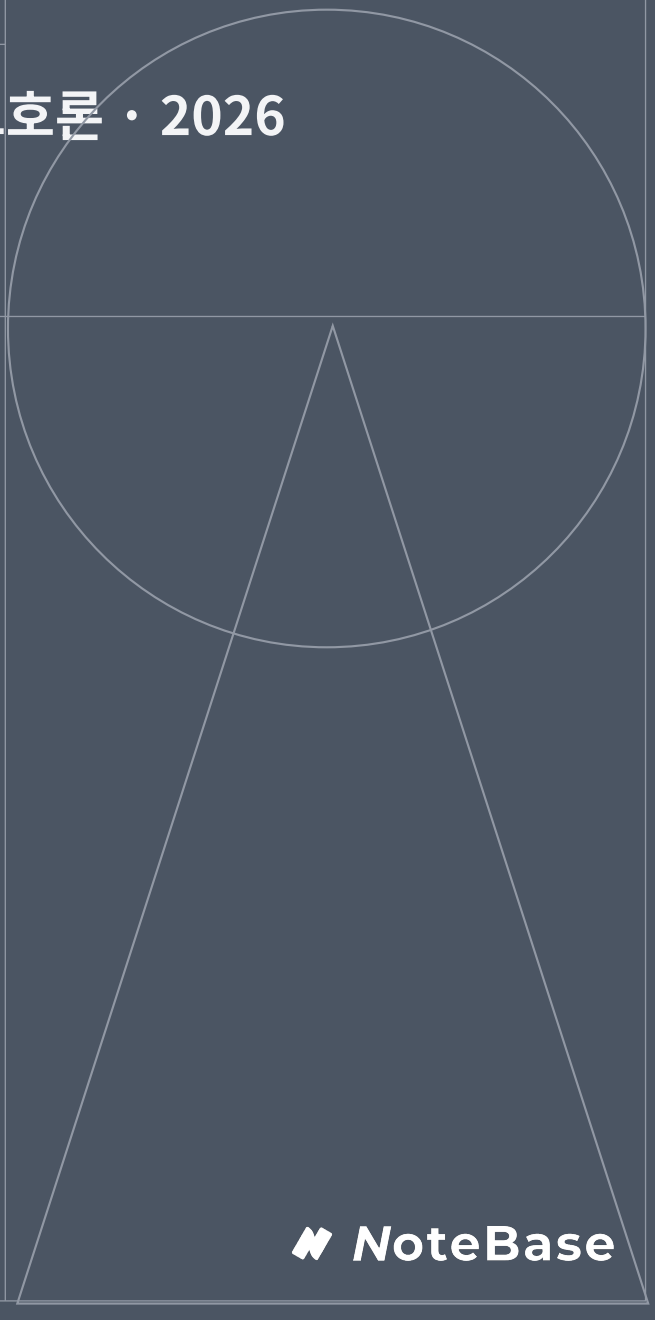
기출OX 해설집

공무원/지방직/9급 · 정보보호론 · 2026



NoteBase

기출OX 해설집

공무원/지방직/9급 · 정보보호론 · 2026

공무원/지방직/9급 · 정보보호론 · 2026

문 1. 악성 코드(malware)에 대한 설명으로 옳지 않은 것은?

① 바이러스는 다른 프로그램에 자신을 복제하여 악의적 목적을 수행한다.

② 랜섬웨어는 사용자의 파일을 암호화하여 자료를 인질로 잡고 금전을 요구한다.

③ 웜은 네트워크를 통해 자신을 복제하고 전파할 수 있는 악성 프로그램이다.

④ 트로이목마는 정상적인 프로그램으로 위장하여 자기 복제를 통해 다른 시스템으로 확산한다.

정답 4번

간단한 해설

트로이목마는 정상적인 프로그램으로 위장하지만, **자기 복제 기능은 없다**. ④의 '자기 복제를 통해 다른 시스템으로 확산한다'는 설명은 네트워크에서 스스로 복제·전파하는 웜의 특징과 혼동한 것이다.

선지별 해설

① O: 바이러스는 **다른 프로그램에 자신의 코드를 삽입**하여 감염시키는 악성 코드이다. 감염된 프로그램이 실행되면 바이러스 코드도 실행되어 다른 프로그램으로 복제되거나 자료 훼손 등의 악의적 동작을 수행할 수 있다.

② O: 랜섬웨어는 파일을 암호화하는 등의 방법으로 **자료를 이용할 수 없게 만든 뒤 금전을 요구**하는 악성 코드이다. 사용자의 자료를 인질로 삼아 복구의 대가를 요구한다는 점에서 선지의 설명에 해당한다.

③ O: 웜은 다른 프로그램에 기생하지 않고 **독립적으로 자기 복제와 전파**를 수행하는 악성 프로그램이다. 네트워크를 통해 다른 시스템으로 퍼질 수 있으므로, 다른 프로그램에 자신의 코드를 삽입하는 바이러스와 구별된다.

④ X: 트로이목마는 정상적이거나 유용한 프로그램처럼 위장하여 사용자의 실행을 유도하고, 실행되면 숨겨 둔 악성 기능을 수행한다. **트로이목마 자체에는 자기 복제 기능이 없으므로**, '자기 복제를 통해 다른 시스템으로 확산한다'는 부분이 잘못되었다. 이 부분은 '사용자가 정상 프로그램으로 믿고 실행하도록 유도하여 악성 기능을 수행한다'로 고쳐야 한다.

NoteBase

문 2. 대칭키 암호 알고리즘에 대한 설명으로 옳지 않은 것은?

① 암호화/복호화 속도는 공개키 암호보다 빠르다.

② 키의 길이가 공개키 암호보다 상대적으로 짧다.

③ 공개키는 암호화에 사용하고 개인키는 복호화에 사용한다.

④ 사용자의 증가에 따라 관리해야 할 키의 수가 비례적으로 늘어난다.

정답 3번

간단한 해설

공개키로 암호화하고 개인키로 복호화하는 것은 **공개키 암호 방식**이다. 대칭키 암호는 송신자와 수신자가 공유하는 **같은 비밀키**로 암호화와 복호화를 수행한다.

선지별 해설

① O: 대칭키 암호는 일반적으로 공개키 암호보다 연산 부담이 작아 **암호화·복호화 속도가 빠르다**. 따라서 대용량 데이터 자체를 암호화하는 데 적합하다.

② O: **동일한 보안 강도를 기준으로** 비교하면 대칭키 암호는 일반적으로 공개키 암호보다 짧은 키를 사용한다. 두 방식은 공격 방법과 계산 난이도가 다르므로, 키의 비트 수가 같다고 보안 강도까지 같은 것은 아니다.

③ X: 대칭키 암호는 공개키와 개인키를 구분하지 않고, 송신자와 수신자가 공유하는 **동일한 비밀키로 암호화와 복호화**를 수행한다. 수신자의 공개키로 암호화하고 그에 대응하는 수신자의 개인키로 복호화하는 것은 공개키 암호 방식이다.

④ O: 통신하는 사용자 쌍마다 별도의 비밀키를 공유하는 방식에서는 **사용자가 늘수록 관리해야 할 키도 증가**한다. n명의 사용자가 서로 모두 통신한다면 각 사용자는 n − 1개의 키를 보유하고, 전체의 서로 다른 키는 $\frac{n(n-1)}{2}$개이다. 선지의 '비례적으로'는 사용자 증가에 따라 키 수도 늘어난다는 취지이며, 전체 키 수가 사용자 수에 엄밀히 정비례한다는 뜻은 아니다.

NoteBase

문 3. (가) ~ (라)에 들어갈 용어를 바르게 연결한 것은?

구분	메시지 인증 코드	전자서명
송신자	(가)로 MAC값을 계산	(나)로 서명을 작성
수신자	(다)로 MAC값을 계산	(라)로 서명을 검증

① (가): 공유키, (나): 공개키, (다): 공유키, (라): 개인키

② (가): 개인키, (나): 공유키, (다): 공개키, (라): 공유키

③ (가): 공유키, (나): 개인키, (다): 공유키, (라): 공개키

④ (가): 개인키, (나): 공유키, (다): 공유키, (라): 공개키

정답 3번

간단한 해설

메시지 인증 코드(MAC)는 송신자와 수신자가 **같은 공유키**로 계산한다. 전자서명은 **송신자의 개인키로 작성**하고, 그와 짝을 이루는 **송신자의 공개키로 검증**한다.

빈칸별 해설

(가) 공유키: MAC는 메시지와 비밀키를 입력하여 만든 인증값이다. 송신자는 수신자와 **미리 공유한 비밀키**로 MAC값을 계산하고, 메시지와 함께 보낸다.

(나) 개인키: 전자서명은 **송신자만 보유하는 개인키**로 작성한다. 다른 사람이 임의로 송신자의 서명을 만들 수 없도록 서명용 개인키는 비밀로 유지한다.

(다) 공유키: 수신자는 받은 메시지에 대해 **송신자와 동일한 공유키**로 MAC값을 다시 계산한다. 이를 전달받은 MAC값과 비교하여 메시지의 변경 여부와 공유키를 가진 주체가 생성한 메시지인지를 확인한다.

(라) 공개키: 수신자는 서명에 사용된 개인키와 짝을 이루는 **송신자의 공개키**로 전자서명을 검증한다. 수신자 자신의 공개키를 사용하는 것이 아니라, 서명한 송신자의 공개키를 사용한다.

따라서 (가)·(다)는 공유키, (나)는 개인키, (라)는 공개키이며, 이 대응은 ③과 일치한다.

NoteBase

문 4. 디지털 포렌식에 대한 설명으로 옳지 않은 것은?

① 디지털 포렌식 과정에서 획득한 모든 증거는 법적 효력을 가진다.

② 수집된 증거가 결함이 없이 위·변조되지 않았음을 증명할 수 있어야 한다.

③ 동일한 조건과 동일한 상황이라면 디지털 포렌식의 분석 결과는 항상 같은 결과가 나와야 한다.

④ 증거를 획득한 뒤에는 이송, 분석, 보관, 법정 제출이라는 일련의 과정 및 각 과정의 담당자가 명확해야 하며 이에 대한 추적이 가능해야 한다.

정답 1번

①

디지털 포렌식으로 획득했다는 사실만으로 **모든 자료에 증거능력이 인정되는 것은 아니다**. 적법절차 등 증거능력 요건을 충족해야 하며, 위법하게 수집한 증거는 원칙적으로 증거로 사용할 수 없다.

형사소송법 제308조의2
형사소송법 제308조의2(위법수집증거의 배제) 적법한 절차에 따르지 아니하고 수집한 증거는 증거로 할 수 없다.

②

무결성의 원칙은 수집한 디지털 증거가 이송·분석·보관 등의 과정에서 훼손되거나 위·변조되지 않았음을 입증할 수 있어야 한다는 원칙이다.

③

재현성의 원칙에 따라 동일한 증거를 동일한 조건과 절차로 분석하면, 다른 분석자가 수행하더라도 같은 결과를 얻을 수 있어야 한다.

④

보관의 연속성 원칙은 증거의 수집부터 법정 제출까지 각 단계의 처리 내역과 담당자를 기록하여, 증거의 관리·이동 경로를 끊김 없이 추적할 수 있어야 한다는 원칙이다.

NoteBase

문 5. 암호화 알고리즘에 대한 설명으로 옳은 것은?

① DES는 56비트 키를 사용하는 대칭키 암호 알고리즘이다.

② AES는 국내에서 개발된 블록 암호 알고리즘으로 국제 표준이 되었다.

③ SEED는 3개의 키값을 사용하고 DES의 3배인 168비트의 보안 강도를 제공한다.

④ RSA는 큰 소수의 곱을 인수분해하기 어렵다는 수학적 원리에 기반한 대칭키 암호 알고리즘이다.

정답 1번

간단한 해설

DES는 암호화와 복호화에 **같은 비밀키**를 사용하는 대칭키 암호이다. 키의 전체 표현은 64비트이지만, 오류 검사용 패리티 8비트를 제외한 **실제 암호 키의 길이는 56비트**이다.

선지별 해설

① O: DES는 같은 비밀키로 암호화와 복호화를 수행하는 대칭키 블록 암호이다. 64비트 단위의 데이터를 처리하며, 키를 표현하는 64비트 중 8비트는 오류 검사용 패리티 비트이다. 따라서 **실제 암호 연산에 쓰이는 키는 56비트**이다.

② X: AES의 기반인 Rijndael은 **벨기에의 암호학자들이 개발**한 알고리즘으로, 미국 국립표준기술연구소(NIST)가 AES로 채택하였다. 국내에서 개발된 블록 암호로는 SEED가 있다. AES가 블록 암호라는 설명은 맞지만 국내에서 개발되었다는 설명이 틀렸다.

③ X: SEED는 **128비트 키와 128비트 블록**을 사용하는 대칭키 블록 암호이다. 서로 독립적인 56비트 키 3개를 사용하여 키 길이가 168비트가 되는 것은 3키 방식의 Triple DES이다. 다만 Triple DES도 알려진 공격을 고려하면 보안 강도는 약 112비트이므로, 키 길이 168비트를 그대로 보안 강도 168비트라고 해서는 안 된다.

④ X: RSA는 **공개키와 개인키를 구분하여 사용하는 비대칭키 암호**이다. 암호화에서는 공개키로 암호화하고 대응하는 개인키로 복호화한다. 큰 소수들을 곱한 수를 소인수분해하기 어렵다는 성질에 기반한다는 설명은 맞지만, 대칭키 암호라는 분류가 틀렸다.

NoteBase

문 6. 국내 국가보안기술연구소 주도로 개발된 암호화 알고리즘은?

① DES

② ARIA

③ RC5

④ IDEA

정답 2번

간단한 해설

ARIA는 국가보안기술연구소 주도로 학계·연구소·정부 기관이 공동 개발한 국산 암호화 알고리즘이다.

핵심 풀이

ARIA는 **국가보안기술연구소 주도로 개발**된 국산 대칭키 블록 암호이다. 2003년에 개발되었으며, 데이터를 128비트 블록 단위로 암호화한다. 이름은 개발에 참여한 학계(Academy), 연구소(Research Institute), 정부 기관(Agency)의 첫 글자에서 따왔다.

다른 후보는 개발 주체가 다르다. DES는 IBM에서 개발했으며, RC5는 로널드 리베스트가, IDEA는 슈에자 라이와 제임스 매시가 개발했다. 따라서 이들은 '국내 국가보안기술연구소 주도 개발'이라는 조건에 해당하지 않는다.

NoteBase

문 7. 사용자가 입력한 키보드 정보를 가로채는 방법은?

① 피싱(phishing)

② 파밍(pharming)

③ 스미싱(smishing)

④ 키로깅(keylogging)

정답 4번

간단한 해설

사용자가 누른 키를 기록하여 입력 정보를 가로채는 방식은 **키로깅(keylogging)**이다. 핵심은 가짜 사이트로 유인하는 것이 아니라 키보드 입력 자체를 수집한다는 점이다.

개념 구분

키로깅: **키보드로 입력한 내용을 기록·수집**하는 방식이다. 예를 들어 사용자가 입력한 아이디와 비밀번호의 키 입력을 기록하면 해당 정보를 탈취할 수 있다. 문제의 '입력한 키보드 정보를 가로채는'이라는 표현이 이 작동 방식을 가리킨다.

다른 공격과의 구분: 피싱은 신뢰할 만한 기관 등을 사칭하여 사용자가 개인정보 등을 제공하도록 속이는 방식이고, 스미싱은 문자메시지를 이용한 피싱이다. 파밍은 정상적인 사이트에 접속하려는 사용자를 가짜 사이트로 연결하는 방식이다. 이들과 구별되는 키로깅의 직접적인 수집 대상은 **사용자의 키 입력**이다.

NoteBase

문 8. 인증에 대한 설명으로 옳지 않은 것은?

① 패스워드는 길이가 길고 대소문자, 숫자, 특수문자를 조합할수록 무차별 대입 공격에 대한 안전성이 높아진다.

② 생체 인증은 신체적 특성을 이용하므로 원천적으로 복제가 불가능하여 별도의 보안 대책이 필요하지 않다.

③ SSO(Single Sign On)는 한 번의 인증으로 다수의 시스템에 접근할 수 있게 하는 인증 시스템이다.

④ OTP(One Time Password)는 한 번 생성되면 그 인증값이 임시적으로 한 번에 한해서만 유효하며, 시간 동기화, 이벤트 동기화, 챌린지·응답 등의 방식으로 생성된다.

정답 2번

간단한 해설

생체 인증에 쓰이는 지문·얼굴 정보도 모방하거나 위조할 수 있으므로 **원천적으로 복제가 불가능한 것은 아니다**. 위조된 생체정보를 이용한 인증 시도를 탐지하고, 저장된 생체정보를 보호하는 보안 대책이 필요하다.

선지별 해설

① O: 무차별 대입 공격은 가능한 패스워드 조합을 차례로 시도하는 공격이다. 다른 조건이 같다면 패스워드가 길고 사용할 수 있는 문자 종류가 많을수록 **공격자가 시도해야 할 후보 수가 증가**한다. 다만 단순한 반복이나 예측 가능한 규칙으로 만든 패스워드는 길이나 문자 종류만으로 안전성을 보장할 수 없다.

② X: 생체 인증은 지문·얼굴 등의 특성을 비교하여 사용자를 확인하지만, 그 특성을 모방한 위조물로 인증 장치를 속이는 공격이 가능하다. 따라서 '원천적으로 복제가 불가능하여 별도의 보안 대책이 필요하지 않다'는 설명은 잘못이다. 실제 사용자의 생체정보인지 확인하는 **위조 생체정보 탐지**와 저장된 생체정보의 유출·변조 방지 대책이 필요하다.

③ O: SSO는 사용자가 **한 번 인증한 결과를 여러 연계 시스템에서 활용**하도록 하는 방식이다. 예를 들어 통합 계정으로 로그인한 뒤 연계된 메일과 업무 시스템을 이용할 때 각각 다시 로그인하지 않도록 구성할 수 있다. 각 시스템의 이용 권한까지 모두 같아진다는 뜻은 아니다.

④ O: OTP는 매번 사용하는 인증값을 바꾸고, 이미 인증에 사용한 값은 다시 받아들이지 않는 방식으로 **인증값의 재사용을 방지**한다. 시간 동기화 방식은 시간을, 이벤트 동기화 방식은 생성 횟수 등의 카운터를 기준으로 값을 만든다. 챌린지·응답 방식은 서버가 제시한 질의값에 대해 비밀정보를 이용하여 응답값을 생성한다.

NoteBase

문 9. 공격자가 공격대상의 IP주소로 위장하여 브로드캐스팅 방식을 통해 ICMP echo request를 다수의 호스트에 전송하는 공격은?

① Smurf
② SYN Flooding
③ ARP Spoofing
④ ICMP Redirect

정답 1번

간단한 해설

공격대상의 IP 주소를 출발지로 위조하고 ICMP echo request를 브로드캐스트하면, 여러 호스트의 응답이 공격대상에 집중된다. 이처럼 **다수 호스트의 응답을 이용하는 반사·증폭 공격**이 Smurf이다.

핵심 풀이

Smurf: 공격자는 ICMP echo request의 출발지 IP 주소를 공격대상의 주소로 위조하고, 목적지를 브로드캐스트 주소로 지정한다. 요청을 받은 여러 호스트가 응답하면, ICMP echo reply는 요청의 출발지로 표시된 **공격대상에 집중**된다. 따라서 공격자가 보낸 요청이 여러 응답으로 증폭되어 공격대상의 네트워크 자원을 소모시킨다. 브로드캐스트 요청에 호스트들이 응답하는 환경을 이용하는 공격이다.

다른 공격과의 구분: SYN Flooding은 TCP 연결 설정 과정의 자원을 소모시키는 공격이고, ARP Spoofing은 IP 주소와 MAC 주소의 대응을 속이는 공격이다. ICMP Redirect는 **경로 변경 메시지**를 악용하는 공격으로, ICMP echo request를 브로드캐스트하여 다수의 응답을 유도하는 Smurf와 구별된다.

NoteBase

문 10. 허니팟(honeypot)에 대한 설명으로 옳지 않은 것은?

① 허니팟은 공격자에게 쉽게 노출되어야 한다.

② 허니팟은 쉽게 해킹이 가능한 것처럼 취약해 보이게 한다.

③ 허니넷(honeynet)은 여러 허니팟을 포함한 네트워크를 의미한다.

④ 허니팟은 시스템을 통과하는 패킷에 대해 일부분만을 샘플링하여 감시한다.

정답 4번

간단한 해설

④의 '일부분만을 샘플링'한다는 설명이 잘못되었다. 허니팟은 공격 행위를 자세히 파악하기 위해 **자신에게 들어오고 나가는 전체 트래픽**을 기록·분석하는 것이 기본이다.

선지별 해설

① O: 허니팟은 공격자를 유인하여 공격 기법과 행위를 관찰하는 미끼 시스템이다. 공격자가 탐색 과정에서 발견하고 접근할 수 있도록 노출되어야 한다. 다만 **공격 대상으로 발견되는 것**과 감시용 허니팟이라는 정체가 드러나는 것은 다르다. 정체를 알아차리면 공격자가 회피하여 관찰 효과가 떨어진다.

② O: 공격자가 공격할 만한 대상으로 여기도록 **취약한 시스템처럼 보이게** 한다. 예를 들어 취약한 서비스를 모방하여 공격자의 접근과 공격 시도를 유도하고, 그 과정에서 사용하는 기법을 관찰한다.

③ O: 허니넷은 **여러 허니팟을 네트워크로 구성**한 환경이다. 개별 미끼 시스템을 연결하여 공격자의 시스템 접근과 네트워크 내 활동을 관찰할 수 있다.

④ X: 허니팟은 일부 패킷만 표본으로 골라 감시하는 방식이 기본이 아니다. **허니팟으로 들어오고 나가는 전체 트래픽과 공격 행위**를 기록·분석하여 공격 과정을 파악한다. 일부 패킷만 수집하면 공격의 흐름이나 사용한 기법을 놓칠 수 있다. 여기서 감시 대상은 허니팟과 관련된 통신이며, 조직의 모든 통신을 허니팟이 통과시킨다는 뜻은 아니다.

NoteBase

문 11. 정보시스템의 접근 제어(access control) 또는 로그 관리에 대한 설명으로 옳지 않은 것은?

① 인증(authentication)은 자신의 신원(identity)을 증명하기 위하여 행하는 과정이다.

② 감사 추적(audit trail)은 시스템의 위험을 평가하고 비용 대비 효과적인 대응책을 수립하는 과정이다.

③ 인가(authorization)는 인증된 주체에게 자원에 대한 접근 권한을 부여하거나 제한하는 과정이다.

④ 책임 추적성(accountability)은 시스템에 접근한 주체가 어떤 행동을 하였는지 기록하여 필요 시 그 행위자를 추적할 수 있게 한다.

정답 2번

간단한 해설

시스템의 위험을 평가하고 비용 대비 효과적인 대응책을 수립하는 것은 **위험 관리**이다. **감사 추적**은 누가 언제 어떤 작업을 했는지 확인할 수 있도록 남긴 기록이다.

선지별 해설

① O: 인증은 접속 주체가 주장하는 **신원이 실제와 일치하는지 확인**하는 과정이다. 비밀번호나 생체정보 등을 검증하여 해당 주체가 본인임을 확인한다.

② X: 위험을 평가하고 비용 대비 효과적인 대응책을 수립하는 것은 **위험 관리**에 대한 설명이다. 감사 추적은 시스템의 접근·작업 내역을 시간 순서대로 남긴 기록으로, 누가 언제 무엇을 했는지 재구성하여 사고 조사나 행위자 추적에 활용한다.

③ O: 인가는 인증된 주체가 자원에 접근하여 **어떤 행위를 할 수 있는지 결정**하는 과정이다. 인증이 사용자의 신원을 확인한다면, 인가는 그 사용자에게 파일 읽기·수정 등의 권한을 허용하거나 제한한다.

④ O: 책임 추적성은 **행위를 특정 주체에게 연결**하여 그 책임을 확인할 수 있는 성질이다. 사용자 식별정보와 작업 내역을 로그에 남기면 사후에 누가 해당 행위를 했는지 추적할 수 있으며, 감사 추적 기록은 이를 뒷받침한다.

NoteBase

문 12. 영국이 제정한 정보보호 관리체계 표준은?

① BS7799

② FISMA

③ PIMS

④ NIST 800-53

정답 1번

간단한 해설

BS7799는 **영국표준협회(BSI)**가 제정한 정보보호 관리체계 표준이다.

개념 구분

BS7799: 영국표준협회(BSI)가 제정한 **영국의 정보보호 관리체계 표준**이다. 정보보호 관리체계는 조직이 정보보호 정책과 책임을 정하고 위험에 맞는 보호대책을 지속적으로 운영·관리하는 체계이다. 따라서 발문의 '영국'과 '정보보호 관리체계 표준'이라는 조건에 대응한다.

FISMA와 NIST 800-53: 둘 다 미국과 관련된다. FISMA는 연방기관의 정보보호 관리를 규율하는 **미국 연방법**이고, NIST 800-53은 미국 국립표준기술연구소(NIST)가 발행한 **정보시스템·조직의 보안통제 지침**이다. 법률과 구체적인 보호조치를 제시하는 지침이라는 차이가 있으며, 어느 것도 영국이 제정한 표준에 해당하지 않는다.

PIMS: 국내에서 운영되었던 **개인정보보호 관리체계 인증제도**이다. 조직의 개인정보보호 관리체계를 심사·인증하는 제도라는 점에서, 영국의 정보보호 관리체계 표준인 BS7799와 구분된다.

NoteBase

문 13. 버퍼 오버플로 공격에 대한 설명으로 옳지 않은 것은?

① 버퍼에 정해진 크기 이상의 데이터를 입력하여 프로그램을 공격하는 행위이다.

② 버퍼 오버플로에 취약한 함수(strcpy(), strcat() 등)는 사용하지 않는 것이 좋다.

③ 메모리 공격을 방어하려고 주소 공간 배치를 난수화하는 기법을 스택 가드(stack guard)라 한다.

④ 세그멘테이션 폴트(segmentation fault)가 발생했을 때 버퍼 오버플로 공격을 의심할 수 있다.

정답 3번

간단한 해설

주소 공간 배치를 난수화하는 기법은 **ASLR(주소 공간 배치 난수화)**이다. 스택 가드는 스택에 둔 **카나리 값의 변조**를 검사하여 버퍼 오버플로를 탐지한다.

선지별 해설

① O: 버퍼 오버플로 공격은 버퍼가 저장할 수 있는 범위를 넘는 데이터를 쓰게 하여 인접한 메모리 내용을 덮어쓰는 공격이다. 이 과정에서 데이터나 복귀 주소 등이 손상되면 **프로그램이 비정상 종료되거나 실행 흐름이 바뀔 수 있다**.

② O: strcpy()와 strcat()는 문자열을 복사하거나 이어 붙일 때 **목적지 버퍼의 크기를 자동으로 검사하지 않는다**. 따라서 입력 문자열이 길면 버퍼 경계를 넘어 쓸 수 있으므로 사용을 피하는 것이 좋다. 문자열 처리 시에는 버퍼 크기와 종료 문자를 고려하여 쓰기 범위를 제한해야 한다.

③ X: 주소 공간 배치를 난수화하는 기법은 **ASLR**이다. 스택·힙·공유 라이브러리 등의 위치를 무작위화하여 공격자가 필요한 메모리 주소를 예측하기 어렵게 한다. **스택 가드**는 스택의 지역 버퍼와 복귀 주소 사이 등에 카나리라는 검사 값을 두고, 함수가 반환되기 전에 그 값이 변했는지 확인하는 기법이다. 주소를 무작위화하는 방식과 스택의 변조를 탐지하는 방식을 구분해야 한다.

④ O: 세그멘테이션 폴트는 프로그램이 허용되지 않은 메모리 영역에 접근하는 등의 경우에 발생한다. 버퍼 오버플로로 포인터나 복귀 주소가 손상되면 잘못된 주소에 접근할 수 있으므로 공격을 의심할 수 있다. 다만 일반적인 프로그램 오류로도 발생하므로 **발생 사실만으로 공격을 확정할 수는 없다**.

NoteBase

문 14. 보안 요소 중 인가된 사용자에게만 정보에 접근할 수 있도록 허용하는 것은?

① 가용성(availability)

② 무결성(integrity)

③ 기밀성(confidentiality)

④ 부인방지(non-repudiation)

정답 3번

간단한 해설

'인가된 사용자에게만 접근을 허용한다'는 **기밀성**의 기준이다. 정보에 접근할 권한이 없는 사람에게 정보가 노출되지 않도록 보호한다는 뜻이다.

개념 구분

기밀성(confidentiality): **누가 정보에 접근할 수 있는가**에 관한 보안 요소로, 허용된 사용자만 정보를 열람하도록 하여 비인가자에게 정보가 노출되는 것을 막는다. 예를 들어 급여 자료를 담당자만 열람하도록 제한하는 것은 기밀성을 보호하는 조치이다. 문항의 '인가된 사용자에게만'이라는 조건이 이 개념을 가리킨다.

가용성(availability): 인가된 사용자가 **필요할 때 정보나 서비스를 이용할 수 있도록** 보장하는 성질이다. 접근 대상을 제한하는 기밀성과 달리, 허용된 사용자의 이용이 장애나 공격으로 중단되지 않는지가 핵심이다.

무결성(integrity): 정보가 **허가 없이 변경되거나 훼손되지 않도록** 보호하는 성질이다. 정보의 열람 범위보다 정보 내용의 정확성과 온전함에 초점을 둔다.

부인방지(non-repudiation): 송신이나 거래 등 **행위가 있었다는 사실을 나중에 부인하지 못하도록** 증거를 제공하는 성질이다. 정보 접근을 제한하는 것과는 구별된다.

NoteBase

문 15. 정량적 위험 분석 방법에 해당하는 것은?

① 델파이법

② 시나리오법

③ 순위결정법

④ 과거자료 분석법

정답 4번

간단한 해설

과거자료 분석법은 과거의 사고 발생 기록을 통계적으로 분석하여 **위험의 발생 가능성을 수치로 추정**하므로 정량적 위험 분석에 해당한다.

개념 구분

과거자료 분석법: 정량적 위험 분석은 사고의 발생 가능성이나 예상 손실을 확률·빈도·금액 등의 수치로 나타내는 방식이다. 과거자료 분석법은 축적된 사고 기록에서 **발생 빈도와 손실 규모** 등을 분석하여 앞으로의 위험을 추정한다. 따라서 과거자료 분석법은 정량적 위험 분석 방법에 해당한다. 다만 과거 기록을 미래에 적용하려면 자료가 현재 분석 대상과 관련성이 있는지 살펴야 한다.

델파이법·시나리오법·순위결정법: 이 문항의 분류에서는 정성적 위험 분석 방법이다. 델파이법은 전문가들의 의견을 수렴하여 위험을 판단하고, 시나리오법은 일정한 조건에서 발생 가능한 상황과 그 결과를 추정한다. 순위결정법은 위협들을 상호 비교하여 **상대적인 우선순위**를 정한다. 특히 순위에 숫자를 붙이더라도 그 숫자만으로 사고 발생 확률이나 손실액을 수치적으로 산정한 것은 아니다.

NoteBase

문 16. CSRF(Cross-Site Request Forgery) 공격에 대한 설명으로 옳은 것은?

① 쿠키를 변조한 후 불법적인 인증을 거쳐 권한을 획득하는 공격이다.

② 악성 URL을 보내서 클릭 시 피해자의 정보를 유출하는 공격이다.

③ 입력 값에 대한 유효성을 검증하지 않고 그대로 사용할 때 발생할 수 있는 데이터베이스 공격이다.

④ 로그인된 사용자가 자신의 의지와는 무관하게 공격자가 의도한 행위를 하는 공격이다.

정답 4번

간단한 해설

CSRF는 **이미 로그인된 사용자의 인증 상태를 악용**하여, 사용자가 원하지 않는 요청을 서버에 보내게 하는 공격이다. 서버가 이를 정상적인 사용자 요청으로 받아들이면 공격자가 의도한 행위가 실행된다.

개념 구분

CSRF(사이트 간 요청 위조)는 피해자의 브라우저가 **기존 인증 정보를 동반한 위조 요청**을 보내도록 유도하는 공격이다. 서버가 요청의 진위를 제대로 확인하지 않으면 이를 피해자가 의도한 요청으로 처리할 수 있다. 예를 들어, 로그인 상태에서 공격자가 만든 페이지에 접속했을 때 취약한 사이트로 이메일 주소 변경 요청이 전송되어 피해자의 의사와 무관하게 주소가 바뀌는 경우이다. 이는 ④의 설명에 해당한다.

다른 공격과의 구분: ①의 쿠키 변조와 달리 CSRF는 **쿠키 자체를 변조할 필요가 없다**.

②처럼 악성 URL을 클릭하게 했다는 사실이나 정보 유출이라는 결과만으로는 CSRF를 설명할 수 없으며, 핵심은 피해자의 인증 상태를 이용한 요청 위조이다.

③의 데이터베이스 공격은 입력값이 SQL 명령의 일부로 해석되어 질의가 조작되는 SQL 삽입 공격에 해당한다.

NoteBase

문 17. 「개인정보 보호법」상 개인정보처리자가 제3자에게 개인정보의 처리 업무를 위탁하는 문서에 포함되어야 하는 내용이 아닌 것은?

① 개인정보의 기술적·관리적 보호조치에 관한 사항
② 개인정보의 안전한 관리를 위하여 대통령령으로 정한 사항
③ 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
④ 정보주체의 권리침해에 대한 조사 및 이에 따른 처분에 관한 사항

정답 4번

①

개인정보 처리업무를 위탁하는 문서에는 **개인정보의 기술적·관리적 보호조치에 관한 사항**을 포함해야 한다.

개인정보 보호법 제26조 제1항 제2호
개인정보 보호법 제26조(업무위탁에 따른 개인정보의 처리 제한)
① 개인정보처리자가 제3자에게 개인정보의 처리 업무를 위탁하는 경우에는 다음 각 호의 내용이 포함된 문서로 하여야 한다. <개정 2023.3.14>
2. 개인정보의 기술적 · 관리적 보호조치에 관한 사항

NoteBase

②

개인정보의 안전한 관리를 위하여 대통령령으로 정한 사항도 위탁문서에 포함해야 한다. 여기에는 **위탁업무의 목적·범위, 재위탁 제한, 안전성 확보 조치 등**이 해당한다.

개인정보 보호법 제26조 제1항 제3호
개인정보 보호법 제26조(업무위탁에 따른 개인정보의 처리 제한)
① 개인정보처리자가 제3자에게 개인정보의 처리 업무를 위탁하는 경우에는 다음 각 호의 내용이 포함된 문서로 하여야 한다. <개정 2023.3.14>
3. 그 밖에 개인정보의 안전한 관리를 위하여 대통령령으로 정한 사항

개인정보 보호법 시행령 제28조 제1항
개인정보 보호법 시행령 제28조(개인정보의 처리 업무 위탁 시 조치)
① 법 제26조제1항제3호에서 "대통령령으로 정한 사항"이란 다음 각 호의 사항을 말한다.
1. 위탁업무의 목적 및 범위
2. 재위탁 제한에 관한 사항
3. 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
4. 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항
5. 법 제26조제2항에 따른 수탁자(이하 "수탁자"라 한다)가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항

③

위탁문서에는 수탁자가 **위탁업무 수행 목적 외에 개인정보를 처리하는 것을 금지하는 사항**을 포함해야 한다.

개인정보 보호법 제26조 제1항 제1호
개인정보 보호법 제26조(업무위탁에 따른 개인정보의 처리 제한)
① 개인정보처리자가 제3자에게 개인정보의 처리 업무를 위탁하는 경우에는 다음 각 호의 내용이 포함된 문서로 하여야 한다. <개정 2023.3.14>
1. 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항

NoteBase

④

정보주체의 권리침해에 대한 조사 및 이에 따른 처분은 **위탁문서의 법정 필수 기재사항에 해당하지 않는다**.
위탁문서에 포함할 감독 사항은 수탁자가 보유한 개인정보의 관리 현황 점검 등이다.

개인정보 보호법 제26조 제1항
개인정보 보호법 제26조(업무위탁에 따른 개인정보의 처리 제한)
① 개인정보처리자가 제3자에게 개인정보의 처리 업무를 위탁하는 경우에는 다음 각 호의 내용이 포함된 문서로 하여야 한다. <개정 2023.3.14>
1. 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
2. 개인정보의 기술적 · 관리적 보호조치에 관한 사항
3. 그 밖에 개인정보의 안전한 관리를 위하여 대통령령으로 정한 사항

개인정보 보호법 시행령 제28조 제1항
개인정보 보호법 시행령 제28조(개인정보의 처리 업무 위탁 시 조치)
① 법 제26조제1항제3호에서 "대통령령으로 정한 사항"이란 다음 각 호의 사항을 말한다.
1. 위탁업무의 목적 및 범위
2. 재위탁 제한에 관한 사항
3. 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
4. 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항
5. 법 제26조제2항에 따른 수탁자(이하 "수탁자"라 한다)가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항

NoteBase

문 18. 「개인정보 보호법」상 가명정보의 처리에 대한 설명으로 옳지 않은 것은?

① 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 없다.

② 통계작성, 과학적 연구, 공익적 기록보존 등을 위한 서로 다른 개인정보처리자 간의 가명정보의 결합은 개인정보 보호위원회 또는 관계 중앙행정기관의 장이 지정하는 전문기관이 수행한다.

③ 개인정보처리자는 가명정보를 처리하는 과정에서 특정 개인을 알아볼 수 있는 정보가 생성된 경우에는 즉시 해당 정보의 처리를 중지하고, 지체 없이 회수·파기하여야 한다.

④ 개인정보처리자는 가명정보를 처리하는 경우에는 원래의 상태로 복원하기 위한 추가 정보를 별도로 분리하여 보관·관리하는 등 해당 정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.

정답 1번

①

통계작성, 과학적 연구, 공익적 기록보존 등을 위한 가명정보 처리는 **정보주체의 동의 없이 할 수 있다**.

개인정보 보호법 제28조의2 제1항
개인정보 보호법 제28조의2(가명정보의 처리 등)
① 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있다.

②

통계작성, 과학적 연구, 공익적 기록보존 등을 위한 서로 다른 개인정보처리자 간의 가명정보 결합은 **개인정보 보호위원회 또는 관계 중앙행정기관의 장이 지정한 전문기관**이 수행한다.

개인정보 보호법 제28조의3 제1항
개인정보 보호법 제28조의3(가명정보의 결합 제한)
① 제28조의2에도 불구하고 통계작성, 과학적 연구, 공익적 기록보존 등을 위한 서로 다른 개인정보처리자 간의 가명정보의 결합은 보호위원회 또는 관계 중앙행정기관의 장이 지정하는 전문기관이 수행한다.

NoteBase

③

가명정보 처리 중 특정 개인을 알아볼 수 있는 정보가 생성되면 **즉시 해당 정보의 처리를 중지하고, 지체 없이 회수·파기**하여야 한다.

개인정보 보호법 제28조의5 제2항
개인정보 보호법 제28조의5(가명정보 처리 시 금지의무 등)
② 개인정보처리자는 제28조의2 또는 제28조의3에 따라 가명정보를 처리하는 과정에서 특정 개인을 알아볼 수 있는 정보가 생성된 경우에는 즉시 해당 정보의 처리를 중지하고, 지체 없이 회수 · 파기하여야 한다. <개정 2023.3.14>

④

가명정보를 처리할 때에는 **복원에 필요한 추가 정보를 별도로 분리하여 보관·관리**하는 등
분실·도난·유출·위조·변조·훼손을 막기 위한 **기술적·관리적 및 물리적 안전조치**를 하여야 한다.

개인정보 보호법 제28조의4 제1항
개인정보 보호법 제28조의4(가명정보에 대한 안전조치의무 등)
① 개인정보처리자는 제28조의2 또는 제28조의3에 따라 가명정보를 처리하는 경우에는 원래의 상태로 복원하기 위한 추가 정보를 별도로 분리하여 보관 · 관리하는 등 해당 정보가 유출등이 되지 아니하도록 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적 · 관리적 및 물리적 조치를 하여야 한다. <개정 2023.3.14, 2026.3.10>

개인정보 보호법 제23조 제2항
개인정보 보호법 제23조(민감정보의 처리 제한)
② 개인정보처리자가 제1항 각 호에 따라 민감정보를 처리하는 경우에는 그 민감정보가 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손(이하 "유출등"이라 한다)이 되지 아니하도록 제29조에 따른 안전성 확보에 필요한 조치를 하여야 한다. <신설 2016.3.29, 2026.3.10>

NoteBase

문 19. 「개인정보 보호법」상 영업양도 등에 따른 개인정보의 이전 시 해당 정보주체에게 미리 알려야 하는 사항에 해당하지 않는 것은?

① 개인정보의 수집 출처
② 개인정보를 이전하려는 사실
③ 개인정보를 이전받는 자의 성명(법인의 경우에는 법인의 명칭을 말한다), 주소, 전화번호 및 그 밖의 연락처
④ 정보주체가 개인정보의 이전을 원하지 아니하는 경우 조치할 수 있는 방법 및 절차

정답 1번

①

영업양도 등에 따른 사전 통지사항은 이전 사실, 이전받는 자의 신원·연락처, 이전을 원하지 않는 경우의 조치 방법·절차이다. **개인정보의 수집 출처는 이 사전 통지사항에 포함되지 않는다.**

개인정보 보호법 제27조 제1항
개인정보 보호법 제27조(영업양도 등에 따른 개인정보의 이전 제한)
① 개인정보처리자는 영업의 전부 또는 일부의 양도 · 합병 등으로 개인정보를 다른 사람에게 이전하는 경우에는 미리 다음 각 호의 사항을 대통령령으로 정하는 방법에 따라 해당 정보주체에게 알려야 한다.
1. 개인정보를 이전하려는 사실
2. 개인정보를 이전받는 자(이하 "영업양수자등"이라 한다)의 성명(법인의 경우에는 법인의 명칭을 말한다), 주소, 전화번호 및 그 밖의 연락처
3. 정보주체가 개인정보의 이전을 원하지 아니하는 경우 조치할 수 있는 방법 및 절차

②

영업양도 등으로 개인정보를 다른 사람에게 이전하는 개인정보처리자는 **개인정보를 이전하려는 사실을 해당 정보주체에게 미리 알려야 한다.**

개인정보 보호법 제27조 제1항 제1호
개인정보 보호법 제27조(영업양도 등에 따른 개인정보의 이전 제한)
① 개인정보처리자는 영업의 전부 또는 일부의 양도 · 합병 등으로 개인정보를 다른 사람에게 이전하는 경우에는 미리 다음 각 호의 사항을 대통령령으로 정하는 방법에 따라 해당 정보주체에게 알려야 한다.
1. 개인정보를 이전하려는 사실

NoteBase

③

영업양도 등에 따른 사전 통지사항에는 **이전받는 자의 성명 또는 법인 명칭과 주소·전화번호 및 그 밖의 연락처**가 포함된다.

개인정보 보호법 제27조 제1항 제2호
개인정보 보호법 제27조(영업양도 등에 따른 개인정보의 이전 제한)
① 개인정보처리자는 영업의 전부 또는 일부의 양도 · 합병 등으로 개인정보를 다른 사람에게 이전하는 경우에는 미리 다음 각 호의 사항을 대통령령으로 정하는 방법에 따라 해당 정보주체에게 알려야 한다.
2. 개인정보를 이전받는 자(이하 "영업양수자등"이라 한다)의 성명(법인의 경우에는 법인의 명칭을 말한다), 주소, 전화번호 및 그 밖의 연락처

④

영업양도 등으로 개인정보를 이전할 때에는 **정보주체가 이전을 원하지 않는 경우 조치할 수 있는 방법과 절차**도 미리 알려야 한다.

개인정보 보호법 제27조 제1항 제3호
개인정보 보호법 제27조(영업양도 등에 따른 개인정보의 이전 제한)
① 개인정보처리자는 영업의 전부 또는 일부의 양도 · 합병 등으로 개인정보를 다른 사람에게 이전하는 경우에는 미리 다음 각 호의 사항을 대통령령으로 정하는 방법에 따라 해당 정보주체에게 알려야 한다.
3. 정보주체가 개인정보의 이전을 원하지 아니하는 경우 조치할 수 있는 방법 및 절차

NoteBase

문 20. 다음에서 설명하는 네트워크 공격 기술은?

신뢰 관계에 있는 두 개의 호스트 사이에서 하나의 시스템을 마비시킨 후 마치 자신이 신뢰관계에 있는 호스트인 것처럼 속이는 것이다.

① DNS Spoofing
② IP Spoofing
③ Switch Jamming
④ Teardrop

정답 2번

간단한 해설

신뢰받는 호스트인 것처럼 보이도록 **출발지 IP 주소를 위조**하는 IP Spoofing이다. 지문에서 한 시스템을 마비시키는 것은 그 호스트의 정상 응답이 위장을 방해하지 못하게 하기 위한 과정이다.

핵심 풀이

IP Spoofing은 IP 패킷의 **출발지 IP 주소를 신뢰받는 호스트의 주소로 위조**하는 공격이다. 상대를 IP 주소에 근거하여 신뢰하는 환경에서, 공격자는 위조한 패킷을 보내 자신을 신뢰받는 호스트로 오인하게 한다. 지문에서 한 시스템을 마비시키는 것은 사칭 대상 호스트의 정상 응답을 막아 위장이 방해받지 않게 하는 과정이다. 따라서 이 설명의 핵심은 시스템 마비 자체보다 호스트 사이의 신뢰관계를 이용한 출발지 위장에 있다.

DNS Spoofing은 **도메인 이름에 대한 IP 주소 응답을 속여** 사용자를 잘못된 목적지로 유도하는 공격이다. 지문은 도메인 이름의 해석 결과를 바꾸는 것이 아니라 신뢰받는 호스트를 사칭하는 상황이므로 IP Spoofing과 연결된다.

NoteBase