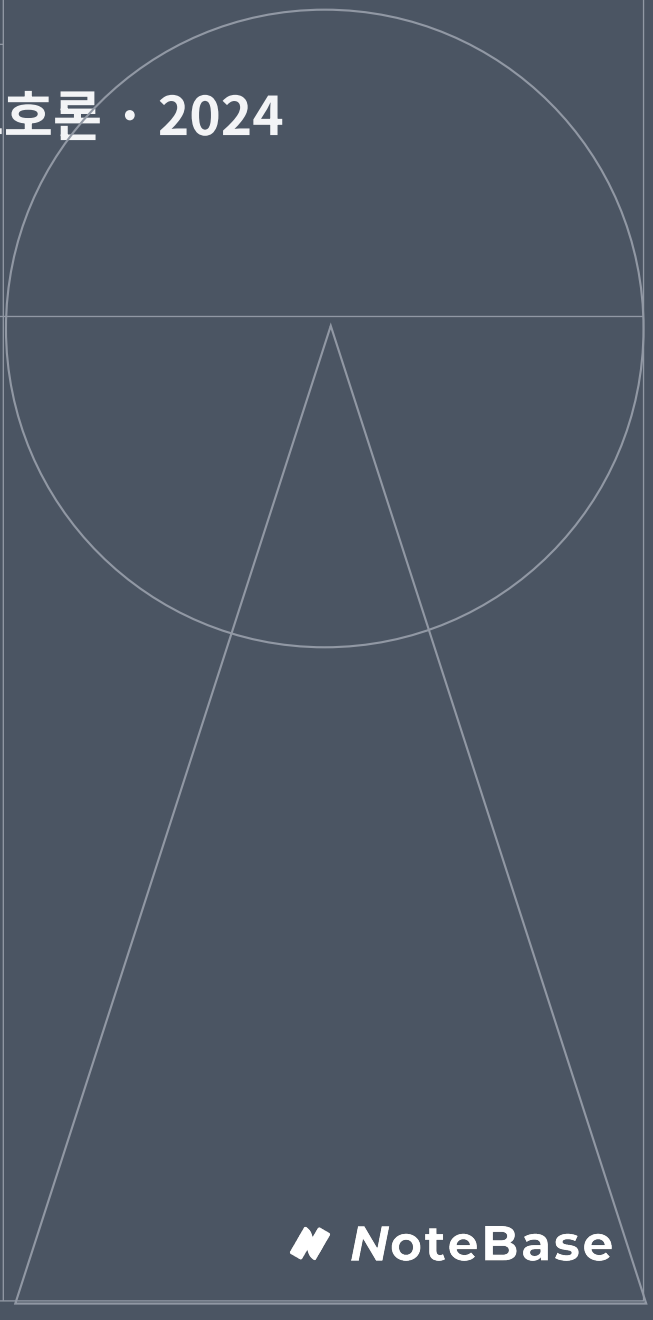
기출OX 해설집

공무원/지방직/9급 · 정보보호론 · 2024



NoteBase

기출OX 해설집

공무원/지방직/9급 · 정보보호론 · 2024

공무원/지방직/9급 · 정보보호론 · 2024

문 1. 사용자 A가 사용자 B에게 보내는 메시지 M의 해시값을 A와 B가 공유하는 비밀키로 암호화하고 이를 M과 함께 보냄으로써 보장하려는 것은?

① 무결성

② 기밀성

③ 가용성

④ 부인방지

정답 1번

간단한 해설

수신자가 직접 계산한 메시지의 해시값과 공유 비밀키로 복호화한 해시값을 비교하면 **메시지의 변경 여부**를 확인할 수 있다. 이는 내용이 위·변조되지 않았음을 확인하는 **무결성**을 위한 방식이다.

핵심 풀이

해시값 대조: A는 메시지 M의 해시값을 계산한 뒤, A와 B만 공유하는 비밀키로 이를 암호화하여 M과 함께 보낸다. B는 받은 M의 해시값을 직접 계산하고, 첨부된 암호문을 같은 비밀키로 복호화하여 얻은 해시값과 비교한다. 안전한 해시함수와 암호화를 사용하고 비밀키가 보호된다는 전제에서, 두 값이 일치하면 전송 중 내용이 변조되지 않았음을 확인할 수 있다. 이처럼 **허가되지 않은 변경을 탐지**하여 데이터의 온전함을 확인하는 성질이 무결성이다.

기밀성·가용성과의 구분: 암호화한 대상은 M 자체가 아니라 해시값이다. 따라서 **M의 내용을 숨기는 기밀성**을 보장하는 방식은 아니다. 또한 필요할 때 정보나 서비스를 이용할 수 있게 하는 가용성도 해시값 대조로 보장되지 않는다.

부인방지와의 구분: 부인방지는 송신자가 나중에 자신이 메시지를 보냈다는 사실을 부인하지 못하도록 하는 성질이다. 이 문제에서는 **A와 B가 같은 비밀키를 공유**하므로 B도 해당 암호화 해시값을 만들 수 있다. 따라서 그 값만으로 제3자에게 A만이 작성자임을 입증할 수 없어 부인방지를 보장하지 못한다.

NoteBase

문 2. 서비스 거부 공격에 해당하지 않는 것은?

① Smurf 공격

② Slowloris 공격

③ Pharming 공격

④ HTTP GET 플러딩 공격

정답 3번

간단한 해설

Pharming은 DNS 정보 등을 변조하여 사용자를 **가짜 웹사이트로 유도하고 정보를 탈취**하는 공격이다. 서버의 자원을 고갈시켜 정상적인 이용을 막는 서비스 거부 공격과 구별된다.

선지별 해설

① O: Smurf 공격은 출발지 IP 주소를 피해자의 주소로 위조한 ICMP Echo Request를 브로드캐스트 주소로 보내는 공격이다. 이에 응답하는 다수 호스트의 **ICMP Echo Reply가 피해자에게 집중**되어 네트워크에 과부하를 일으키므로 서비스 거부 공격에 해당한다.

② O: Slowloris 공격은 HTTP 요청 헤더를 완성하지 않은 채 조금씩 전송하여 서버가 요청의 나머지 부분을 계속 기다리게 한다. 이렇게 **미완성 요청의 연결을 오래 유지**하여 연결 처리 자원을 점유하므로, 정상 사용자가 접속하지 못하는 서비스 거부가 발생한다. 대량의 트래픽을 보내지 않고도 서버 자원을 고갈시킬 수 있다.

③ X: Pharming 공격은 DNS 정보나 사용자 기기의 hosts 파일 등을 변조하여 정상 사이트에 접속하려는 사용자를 가짜 사이트로 유도하는 공격이다. 사용자가 가짜 사이트에 비밀번호 등 민감한 정보를 입력하도록 속이는 **접속 경로 변조·정보 탈취 공격**으로, 자원 고갈을 통해 서비스 이용을 막는 서비스 거부 공격에 해당하지 않는다.

④ O: HTTP GET 플러딩 공격은 웹페이지나 파일 등을 요청하는 **HTTP GET 요청을 대량으로 전송**하여 웹 서버에 과부하를 일으킨다. 서버의 요청 처리 자원이 소모되어 정상 사용자의 요청에 응답하기 어려워지므로 서비스 거부 공격에 해당한다.

NoteBase

문 3. (가)와 (나)에 들어갈 용어를 바르게 연결한 것은?

traceroute 명령어는 (가) 시스템에서 사용되며 (나) 기반으로 구현된다.

① (가): Windows, (나): IGMP
② (가): Windows, (나): TCP
③ (가): Linux, (나): HTTP
④ (가): Linux, (나): ICMP

정답 4번

간단한 해설

traceroute는 Linux에서 사용하는 경로 추적 명령이며, 경유하는 라우터가 보내는 **ICMP 시간 초과 응답**을 이용해 경로를 알아낸다.

빈칸별 해설

(가) Linux: traceroute는 목적지까지 패킷이 거치는 라우터를 확인하는 명령으로, Linux·유닉스 계열에서 사용한다. Windows의 기본 경로 추적 명령 이름은 **tracert**이므로 명령 이름을 구분해야 한다.

(나) ICMP: IP 패킷의 TTL은 라우터를 거칠 때 감소하며, 0이 되면 해당 라우터는 패킷을 폐기하고 ICMP Time Exceeded, 즉 시간 초과 메시지를 보낸다. traceroute는 TTL을 1, 2, 3 등으로 늘려 탐색 패킷을 보내고, 돌아오는 **ICMP 응답의 출발지 주소**로 각 경유 라우터를 확인한다. 다만 탐색 패킷 자체와 라우터의 응답은 구분해야 한다. Linux traceroute는 일반적으로 UDP 탐색 패킷을 사용하며 옵션에 따라 ICMP나 TCP로도 탐색할 수 있지만, 중간 라우터의 확인에는 ICMP 시간 초과 응답을 활용한다.

따라서 (가)는 Linux, (나)는 ICMP로 연결되며 ④의 조합과 일치한다.

NoteBase

문 4. 하이브리드 암호 시스템에 대한 설명으로 옳지 않은 것은?

① 대칭키 암호와 공개키 암호의 장점을 조합한 방법이다.

② 메시지의 기밀성과 세션키의 기밀성을 제공한다.

③ 송신자의 공개키를 이용하여 메시지를 암호화한다.

④ 수신자의 공개키를 이용하여 세션키를 암호화한다.

정답 3번

간단한 해설

③의 '송신자의 공개키로 메시지를 암호화한다'는 설명이 잘못되었다. 하이브리드 암호에서는 메시지를 **대칭키인 세션키**로 암호화하고, 그 세션키를 **수신자의 공개키**로 암호화해 전달한다.

선지별 해설

① O: 하이브리드 암호는 **대칭키 암호의 빠른 처리 속도**와 공개키 암호의 키 전달상 이점을 결합한다. 용량이 큰 메시지는 대칭키로 암호화하고, 그때 사용한 세션키는 공개키 암호로 보호하여 전달하므로 통신 당사자가 미리 같은 비밀키를 공유할 필요가 없다.

② O: 메시지는 세션키로 암호화하고, 세션키는 수신자의 공개키로 암호화한다. 따라서 전송 내용을 가로채더라도 수신자의 개인키가 없으면 세션키를 복원할 수 없고, 세션키가 없으면 메시지를 복호화할 수 없다. 이처럼 **메시지와 세션키를 모두 암호화하여** 각각의 기밀성을 제공한다.

③ X: 메시지를 암호화하는 데 사용하는 키는 송신자의 공개키가 아니라 **대칭키인 세션키**이다. 송신자의 공개키로 암호화한 내용은 그에 대응하는 송신자의 개인키로 복호화해야 하므로, 수신자가 자신의 개인키로 복호화하는 전달 구조에 맞지 않는다. 메시지는 세션키로 암호화하고, 세션키는 수신자의 공개키로 암호화하는 것으로 고쳐야 한다.

④ O: 송신자는 세션키를 **수신자의 공개키로 암호화**하여 암호화된 메시지와 함께 보낸다. 수신자는 자신의 개인키로 세션키를 복원한 다음, 복원한 세션키로 메시지를 복호화한다. 공개키로 보호하는 대상이 메시지 자체가 아니라 세션키라는 점이 핵심이다.

NoteBase

문 5. 암호학적 해시 함수 H에 대한 설명으로 옳은 것은?

① 임의의 크기의 데이터 블록 x에 대해서 가변적 길이의 해시값 $H(x)$를 생성한다.

② 주어진 h로부터 $h = H(x)$인 x를 찾는 것은 계산적으로 불가능하다.

③ 임의의 크기의 데이터 블록 x에 대해 $H(x)$를 구하는 계산은 어려운 연산이 포함되어 계산이 비효율적이다.

④ $H(x) = H(y)$를 만족하는 서로 다른 x, y는 존재하지 않는다.

정답 2번

간단한 해설

암호학적 해시 함수는 주어진 해시값으로부터 그 값을 만들어 내는 입력을 찾기 어렵게 하는 **역상 저항성**을 갖는다. 여기서 '계산적으로 불가능하다'는 수학적으로 불가능하다는 뜻이 아니라, 현실적인 시간과 계산 자원으로는 찾기 어렵다는 뜻이다.

선지별 해설

① X: 입력 데이터의 길이는 달라질 수 있지만, 해시값의 길이는 해당 해시 함수에 정해진 **고정 길이**이다. 따라서 '가변적 길이의 해시값'을 '고정 길이의 해시값'으로 고쳐야 한다.

② O: 주어진 해시값 h에 대해 $H(x) = h$를 만족하는 입력 x를 찾기 어려운 성질을 **역상 저항성**이라고 한다. 처음 사용된 입력을 정확히 복원하는 것뿐 아니라, 그 해시값을 만드는 입력 하나를 찾는 일 자체가 현실적인 시간과 계산 자원으로는 어렵다는 의미이다.

③ X: 입력 x로부터 해시값 $H(x)$를 구하는 **순방향 계산은 효율적**이어야 한다. 계산하기 어려워야 하는 것은 해시값으로부터 입력을 찾는 역방향의 문제이다. 따라서 해시값 계산이 어렵고 비효율적이라는 설명은 잘못되었다.

④ X: 해시값은 고정 길이이므로 가능한 출력의 수가 한정되어 있다. 그보다 많은 서로 다른 입력을 대응시키면 같은 출력에 대응하는 입력이 생기므로, $x \neq y$이면서 $H(x) = H(y)$인 **충돌은 존재한다**. 암호학적 해시 함수에 요구되는 충돌 저항성은 충돌이 전혀 없다는 뜻이 아니라, 충돌하는 서로 다른 두 입력을 계산적으로 찾기 어렵다는 뜻이다.

NoteBase

문 6. 커버로스(Kerberos)에 대한 설명으로 옳지 않은 것은?

① 네트워크를 이용한 인증 프로토콜이다.

② 세션키를 분배하는 데 사용될 수 있다.

③ 세션키를 이용하여 데이터의 기밀성을 제공할 수 있다.

④ 버전 5에서는 비표(nonce)를 사용하지 않기 때문에 재생(replay) 공격에 취약하다.

정답 4번

간단한 해설

④의 '비표(nonce)를 사용하지 않는다'는 설명이 잘못되었다. Kerberos V5는 **nonce로 요청과 응답을 대응**시키며, 인증자의 타임스탬프와 중복 사용 검사로 재생 공격에 대응한다.

선지별 해설

① O: Kerberos는 신뢰할 수 있는 제3자인 키 분배 센터(KDC)를 이용하는 **네트워크 인증 프로토콜**이다. 클라이언트는 발급받은 티켓과 세션키로 만든 인증자를 서버에 제시하여 자신의 신원을 증명한다.

② O: KDC는 클라이언트와 서버가 통신에 사용할 **세션키를 분배**한다. 클라이언트는 암호화된 응답에서 세션키를 얻고, 서버는 자신에게 제시된 티켓을 복호화하여 같은 세션키를 얻는다.

③ O: 클라이언트와 서버가 공유한 **세션키로 데이터를 암호화**하면 제3자가 내용을 읽지 못하도록 기밀성을 제공할 수 있다. 인증을 마쳤다는 사실만으로 모든 데이터가 자동 암호화되는 것은 아니며, 실제 통신에 암호화 기능을 적용해야 한다.

④ X: Kerberos V5는 **nonce를 사용한다**. 클라이언트는 요청에 임의의 nonce를 넣고, 응답의 암호화된 부분에 포함된 nonce가 자신이 보낸 값과 일치하는지 검사하여 이전 응답의 재사용을 탐지한다. 또한 서버는 인증자의 타임스탬프가 허용 시간 범위 안에 있는지 확인하고, 재생 캐시로 이미 사용된 인증자의 중복을 검사하여 재생 공격에 대응한다.

NoteBase

문 7. 포트 스캔 방식 중에서 포트가 열린 서버로부터 SYN+ACK 패킷을 받으면 로그를 남기지 않기 위하여 RST 패킷을 보내 즉시 연결을 끊는 스캔 방식은?

① TCP Half Open 스캔

② UDP 스캔

③ NULL 스캔

④ X-MAS 스캔

정답 1번

간단한 해설

TCP Half Open 스캔은 열린 포트에서 SYN+ACK를 받으면 **마지막 ACK 대신 RST**를 보내 연결 시도를 중단한다. TCP의 3단계 연결 설정을 끝까지 완료하지 않는 것이 핵심이다.

핵심 풀이

TCP Half Open 스캔: 정상적인 TCP 연결은 클라이언트의 SYN 전송, 서버의 SYN+ACK 응답, 클라이언트의 ACK 전송으로 설정된다. TCP Half Open 스캔은 SYN을 보낸 뒤 SYN+ACK를 받으면 포트가 열려 있음을 확인하고, **ACK 대신 RST를 보내 연결 설정을 중단**한다. 3단계 연결 설정을 완료하지 않으므로 Half Open 스캔 또는 SYN 스캔이라고 한다.

UDP 스캔: UDP 패킷을 보내 응답이나 ICMP 오류 메시지 등을 확인하는 방식이다. UDP는 **TCP의 3단계 연결 설정을 사용하지 않으므로** 문제의 SYN+ACK 수신 후 RST 전송 절차에 해당하지 않는다.

NULL 스캔과 X-MAS 스캔: NULL 스캔은 TCP 제어 플래그를 모두 끈 패킷을, X-MAS 스캔은 FIN·PSH·URG 플래그를 켠 패킷을 보낸다. 두 방식 모두 **SYN을 보내 SYN+ACK 응답을 확인하는 방식이 아니다**.

문제의 '로그를 남기지 않기 위하여'는 완전한 TCP 연결을 만들지 않아 탐지 가능성을 줄이려는 취지이다. Half Open 스캔도 방화벽이나 침입 탐지 시스템에 탐지·기록될 수 있으므로, 어떠한 로그도 남지 않는다는 뜻으로 이해해서는 안 된다.

NoteBase

문 8. 패스워드를 저장할 때 솔트(salt)를 사용함으로써 얻을 수 있는 이점이 아닌 것은?

① 시스템 내에 같은 패스워드를 쓰는 사용자가 복수로 존재한다는 것을 발견하지 못하게 한다.

② 오프라인 사전(dictionary) 공격을 어렵게 한다.

③ 사용자가 같은 패스워드를 여러 시스템에서 중복해서 사용하여도 그 사실을 발견하기 어렵게 한다.

④ 패스워드 파일에 솔트가 암호화된 상태로 저장되므로 인증 처리 시간을 단축시킨다.

정답 4번

간단한 해설

솔트는 패스워드와 함께 해시 계산에 사용하는 값으로, **암호화할 필요 없이 해시값과 함께 저장**할 수 있다. 솔트의 목적은 같은 패스워드라도 서로 다른 해시값을 갖게 하여 추측 공격을 어렵게 하는 것이며, **인증 처리 시간 단축이 아니다**.

선지별 해설

솔트는 패스워드에 추가하여 해시 계산에 사용하는 값이다. 사용자나 계정마다 서로 다른 솔트를 사용하면 동일한 패스워드라도 서로 다른 해시값이 저장된다.

① O: 사용자마다 서로 다른 솔트를 적용하면 같은 패스워드를 사용해도 저장되는 해시값이 달라진다. 따라서 유출된 패스워드 파일에서 **해시값의 일치 여부만으로** 같은 패스워드를 쓰는 사용자를 찾아내기 어렵다.

② O: 솔트가 없으면 공격자는 사전의 패스워드 후보별 해시값을 미리 계산하여 여러 계정에 재사용할 수 있다. 서로 다른 솔트를 사용하면 **솔트별로 후보 해시값을 다시 계산**해야 하므로, 이런 사전 계산 결과를 재사용하는 오프라인 사전 공격이 어려워진다. 다만 공격자가 특정 계정의 솔트와 해시값을 얻으면 후보 패스워드를 대입해 확인하는 시도 자체는 가능하다.

③ O: 여러 시스템에서 같은 패스워드를 사용하더라도 각 시스템이 서로 다른 솔트를 적용하면 해시값이 달라진다. 따라서 여러 시스템의 저장된 해시값을 비교하는 것만으로는 **패스워드의 중복 사용을 알아내기 어렵다**.

④ X: 솔트는 **비밀로 유지하거나 암호화해야 하는 값이 아니다**. 일반적으로 패스워드 해시값과 함께 저장하고, 인증할 때 저장된 솔트와 입력된 패스워드로 해시값을 다시 계산해 비교한다. 솔트를 사용하는 이점은 해시값 비교를 통한 패스워드 중복 탐지와 사전 계산 공격을 어렵게 하는 것이며, 솔트의 암호화나 인증 처리 시간 단축이 아니다.

NoteBase

문 9. 다음에서 설명하는 보안 공격은?

사용자 요청이 웹 서버의 애플리케이션을 거쳐 데이터베이스에 전달되고 그 결과가 반환되는 구조에서 주로 발생하는 것으로, 공격자가 악의적으로 질의에 포함시킨 특수 문자를 제대로 필터링하지 않으면 데이터베이스 자료가 무단으로 유출·변조될 수 있다.

① 버퍼 오버플로우

② SQL 삽입

③ XSS

④ CSRF

정답 2번

간단한 해설

악성 입력이 데이터베이스 질의의 일부로 해석되어 자료를 유출·변조하는 것은 **SQL 삽입**이다. 핵심 단서는 특수 문자를 이용해 **질의의 구조나 의미를 바꾸는 것**이다.

핵심 풀이

SQL 삽입은 애플리케이션이 사용자 입력을 SQL 문에 결합할 때, 공격자가 넣은 문자열이 단순한 데이터가 아니라 **SQL 구문의 일부로 해석**되도록 하는 공격이다. 입력에 포함된 따옴표나 연산자 등이 질의의 조건이나 구조를 바꾸면, 원래 허용하지 않은 자료를 조회하거나 변경할 수 있다. 지문에서 웹 애플리케이션을 거쳐 데이터베이스로 전달되는 질의와 자료의 무단 유출·변조를 설명하므로 SQL 삽입에 해당한다.

다른 공격과는 악성 입력이 작용하는 위치와 방식을 구분한다. XSS는 삽입된 스크립트가 **사용자의 웹 브라우저에서 실행**되게 하는 공격이다.

CSRF는 로그인한 사용자의 인증 상태를 악용해 사용자가 의도하지 않은 요청을 보내게 하는 공격이다.

버퍼 오버플로우는 버퍼의 경계를 넘는 데이터를 기록하여 인접한 메모리를 침범하는 공격이다.

NoteBase

문 10. 「개인정보 보호법 시행령」에서 규정한 민감정보에 해당하지 않는 것은? (단, 공공기관이 관련 규정에 따라 해당 정보를 처리하는 경우는 제외한다)

① 유전자검사 등의 결과로 얻어진 유전정보

② 「형의 실효 등에 관한 법률」 제2조제5호에 따른 범죄경력자료에 해당하는 정보

③ 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 알아보지 못하도록 일정한 기술적 수단을 통해 생성한 정보

④ 인종이나 민족에 관한 정보

정답 3번

①

유전자검사 등의 결과로 얻어진 **유전정보는 민감정보**에 해당한다.

개인정보 보호법 시행령 제18조 제1호
개인정보 보호법 시행령 제18조(민감정보의 범위) 법 제23조제1항 각 호 외의 부분 본문에서 "대통령령으로 정하는 정보"란 다음 각 호의 어느 하나에 해당하는 정보를 말한다. 다만, 공공기관이 법 제18조제2항제5호부터 제9호까지의 규정에 따라 다음 각 호의 어느 하나에 해당하는 정보를 처리하는 경우의 해당 정보는 제외한다.
<개정 2016.9.29, 2020.8.4>
1. 유전자검사 등의 결과로 얻어진 유전정보

②

범죄경력자료에 해당하는 정보는 민감정보에 포함된다.

개인정보 보호법 시행령 제18조 제2호
개인정보 보호법 시행령 제18조(민감정보의 범위) 법 제23조제1항 각 호 외의 부분 본문에서 "대통령령으로 정하는 정보"란 다음 각 호의 어느 하나에 해당하는 정보를 말한다. 다만, 공공기관이 법 제18조제2항제5호부터 제9호까지의 규정에 따라 다음 각 호의 어느 하나에 해당하는 정보를 처리하는 경우의 해당 정보는 제외한다.
<개정 2016.9.29, 2020.8.4>
2. 「형의 실효 등에 관한 법률」 제2조제5호에 따른 범죄경력자료에 해당하는 정보

NoteBase

③

신체적·생리적·행동적 특징에 관한 정보 중 **특정 개인을 알아볼 목적으로 기술적 수단을 통해 생성한 정보**가 민감정보에 해당한다. 선지는 그 목적을 '알아보지 못하도록'이라고 반대로 서술한다.

개인정보 보호법 시행령 제18조 제3호
개인정보 보호법 시행령 제18조(민감정보의 범위) 법 제23조제1항 각 호 외의 부분 본문에서 "대통령령으로 정하는 정보"란 다음 각 호의 어느 하나에 해당하는 정보를 말한다. 다만, 공공기관이 법 제18조제2항제5호부터 제9호까지의 규정에 따라 다음 각 호의 어느 하나에 해당하는 정보를 처리하는 경우의 해당 정보는 제외한다.
<개정 2016.9.29, 2020.8.4>
3. 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 정보

④

인종이나 민족에 관한 정보는 민감정보에 해당한다.

개인정보 보호법 시행령 제18조 제4호
개인정보 보호법 시행령 제18조(민감정보의 범위) 법 제23조제1항 각 호 외의 부분 본문에서 "대통령령으로 정하는 정보"란 다음 각 호의 어느 하나에 해당하는 정보를 말한다. 다만, 공공기관이 법 제18조제2항제5호부터 제9호까지의 규정에 따라 다음 각 호의 어느 하나에 해당하는 정보를 처리하는 경우의 해당 정보는 제외한다.
<개정 2016.9.29, 2020.8.4>
4. 인종이나 민족에 관한 정보

NoteBase

문 11. DNS 스푸핑 공격에 대한 설명으로 옳지 않은 것은?

① 위조된(spoofed) DNS 응답을 보내 공격자가 의도한 웹 사이트로 사용자의 접속을 유도하는 공격이다.

② 일반적으로 DNS 질의는 TCP 패킷이므로 공격자는 로컬 DNS 서버가 인터넷의 DNS 서버로부터 응답을 얻기 위해 설정한 TCP 세션을 하이재킹해야 한다.

③ 위조된 응답이 일반적으로 로컬 DNS 서버에 의해 캐시되므로 손상이 지속될 수 있는데 이를 DNS 캐시 포이즈닝이라고 한다.

④ 디지털 서명으로 DNS 데이터의 진위 여부를 확인하는 DNSSEC는 DNS 캐시 포이즈닝에 대처하도록 설계되었다.

정답 2번

간단한 해설

②의 '일반적으로 DNS 질의는 TCP 패킷'이라는 전제가 잘못되었다. 일반적인 DNS 질의·응답은 **UDP**를 사용하므로, DNS 스푸핑에 **TCP 세션 하이재킹이 필수인 것은 아니다**.

선지별 해설

① O: DNS 스푸핑은 **위조된 DNS 응답을 정상 응답으로 받아들이게 하는** 공격이다. 도메인 이름에 대응하는 IP 주소를 공격자가 원하는 주소로 속이면 사용자는 의도한 사이트 대신 공격자가 지정한 사이트에 접속할 수 있다.

② X: 일반적인 DNS 질의·응답에는 TCP가 아니라 **UDP**를 사용한다. UDP는 TCP처럼 세션을 설정하지 않으므로, 공격자는 질의 식별자와 포트 등 응답 수락 조건에 맞는 위조 응답을 정상 응답보다 먼저 도착시켜 공격할 수 있다. DNS에서 TCP도 사용할 수 있지만, DNS 스푸핑을 하려면 반드시 TCP 세션을 하이재킹해야 한다는 설명은 잘못되었다.

③ O: 로컬 DNS 서버는 같은 질의에 재사용할 수 있도록 DNS 응답의 정보를 캐시에 저장한다. 위조된 정보가 정상 정보로 받아들여져 저장되면, 캐시가 만료되거나 제거될 때까지 다른 사용자에게도 잘못된 정보를 제공할 수 있다. 이처럼 **DNS 캐시에 거짓 정보를 주입하는** 공격이 DNS 캐시 포이즈닝이다.

④ O: DNSSEC는 DNS 데이터에 대한 **디지털 서명을 검증**하여 데이터의 출처와 무결성을 확인한다. 신뢰할 수 있는 키를 바탕으로 서명을 검증하면 공격자가 위조한 데이터를 정상 데이터로 받아들이는 것을 막을 수 있으므로, DNS 캐시 포이즈닝에 대응하는 수단이 된다.

NoteBase

문 12. (가)와 (나)에 들어갈 내용을 바르게 연결한 것은?

하트블리드(Heartbleed)는 (가)를 구현한 공개 소프트웨어인 OpenSSL의 심각한 보안 취약점으로, 수신한 요청 메시지의 실제 (나)을/를 제대로 확인하지 않은 것에 기인한 것이다.

① (가): SSH, (나): 길이
② (가): SSH, (나): 유형
③ (가): TLS, (나): 길이
④ (가): TLS, (나): 유형

정답 3번

간단한 해설

하트블리드는 OpenSSL의 **TLS 하트비트 처리**에서 발생한 취약점이다. 요청에 적힌 데이터 길이를 실제 수신한 데이터의 길이와 대조하지 않아, 데이터 범위를 넘어선 메모리 내용까지 응답에 포함될 수 있었다.

빈칸별 해설

(가) TLS: OpenSSL은 통신 내용을 보호하는 SSL/TLS를 구현한 공개 암호 라이브러리이다. 하트블리드는 그중 **TLS 하트비트 확장 기능의 구현 오류**로 발생했다. 하트비트는 상대방이 응답하는지 확인하기 위해 요청과 응답을 주고받는 기능이다. SSH는 안전한 원격 접속 등에 사용하는 별도의 프로토콜이므로 이 빈칸에 해당하지 않는다.

(나) 길이: 하트비트 요청에는 되돌려 받을 데이터와 그 길이가 들어가며, 수신 측은 요청의 데이터를 응답에 그대로 복사해 보낸다. 취약한 구현은 **요청에 표시된 길이가 실제 수신 데이터의 범위 안인지 확인하지 않았다**. 공격자가 실제 데이터보다 큰 길이를 적어 보내면, 그 길이만큼 복사하는 과정에서 데이터 뒤의 메모리까지 읽어 응답에 포함할 수 있었다. 따라서 원인은 메시지 유형의 확인 누락이 아니라 길이에 대한 경계 검사 누락이다.

(가)에 TLS, (나)에 길이를 넣은 조합은 ③에 해당한다.

NoteBase

문 13. 정보보호제품 평가·인증제도에 대한 설명으로 옳지 않은 것은?

① 정보보호제품 평가·인증제도는 「지능정보화 기본법」 제58조 (정보보호시스템에 관한 기준 고시 등)에 근거한다.

② 인증기관은 국가보안기술연구소이다.

③ 「정보보호시스템 공통평가기준」은 최고의 평가보증등급인 EAL 1부터 최저의 평가보증등급인 EAL 7까지 보증등급을 정의하고 있다.

④ 보호 프로파일은 정보보호시스템이 사용될 환경에서 필요한 보안 기능 및 보증 요구사항을 공통평가기준에 근거하여 서술한 것이다.

정답 3번

①

정보보호제품 평가·인증제도는 **정보보호시스템의 성능과 신뢰도에 관한 기준을 정하여 고시하도록 하는 규정**에 근거한다.

지능정보화 기본법 제58조 제1항
지능정보화 기본법 제58조(정보보호시스템에 관한 기준 고시 등)
① 과학기술정보통신부장관은 관계 기관의 장과 협의하여 정보보호시스템의 성능과 신뢰도에 관한 기준을 정하여 고시하고, 정보보호시스템을 제조하거나 수입하는 자에게 그 기준을 지킬 것을 권고할 수 있다.

NoteBase

②

인증기관은 **한국전자통신연구원 부설 국가보안기술연구소**이며, IT보안인증사무국이 평가결과의 승인과 인증서 발급 업무를 수행한다.

정보보호시스템 평가·인증 등에 관한 고시(과학기술정보통신부고시 제2022-61호) 2.2.1 제22항
2.2.1 인증기관
22인증기관은 한국전자통신연구원 부설 국가보안기술연구소로 하며, 다음 각 호의 업무를 수행한다.
1. 평가기관의 평가업무 감독
2. 인증보고서 작성 및 인증서 발급
3. 신청인과 평가기관간의 분쟁조정
4. 인증제품 소개책자 발간
5. 국제상호인정협정 관련 정책결정
6. 인증제품에 대한 사후관리
7. 인증업무 수행에 관한 규정수립 및 시행
8. 인증받은 보호프로파일 등록 및 관리
9. 관계 국제협약에서 정한 기준에 맞는 기관을 평가기관으로 승인하는 업무

③

평가보증등급은 **EAL1이 최저이고 EAL7이 최고**이다. 숫자가 커질수록 평가의 엄격성·범위·깊이 등에 따른 보증 수준이 높아지며, 선지는 최고와 최저를 뒤바꾸었다.

④

보호프로파일은 정보보호시스템의 사용 환경에서 필요한 **보안기능 및 보증 요구사항을 공통평가기준에 근거하여 서술한 문서**이다. 특정 제품의 구현방법에 종속되지 않고 제품군이 충족해야 할 보안 요구사항을 정리한다는 점이 핵심이다.

정보보호시스템 평가·인증 등에 관한 고시(과학기술정보통신부고시 제2022-61호) 1.3 제6항
1.3 용어 정의
6"보호프로파일"이라 함은 정보보호시스템이 사용될 환경에서 필요한 보안기능 및 보증 요구사항을 공통평가기준에 근거하여 서술한 문서를 말한다.

NoteBase

문 14. 소켓은 통신의 한 종점을 추상화한 것으로, 통신 상대를 식별하기 위한 것이다. TCP 연결을 위한 소켓 정의에 사용되는 것은?

① MAC 주소, IP 주소

② IP 주소, Port 번호

③ Port 번호, URL

④ URL, MAC 주소

정답 2번

간단한 해설

TCP 통신의 한 종점은 **IP 주소와 Port 번호의 조합**으로 식별한다. IP 주소가 통신할 호스트를 가리키고, 포트 번호가 그 호스트 안의 통신 지점을 구분한다.

개념 구분

IP 주소와 Port 번호: TCP 소켓의 주소는 **IP 주소와 포트 번호를 함께** 사용한다. IP 주소는 통신할 호스트의 네트워크상 주소를 나타내고, 포트 번호는 그 호스트에서 데이터를 전달할 응용 프로그램의 통신 지점을 구분한다. 따라서 같은 IP 주소에서도 포트 번호가 다르면 서로 다른 통신 종점을 구별할 수 있다.

MAC 주소와 URL: MAC 주소는 데이터 링크 계층에서 네트워크 인터페이스를 식별하는 주소이고, URL은 응용 계층에서 자원의 위치와 접근 방법을 나타낸다. 둘은 **TCP 소켓의 주소를 구성하는 요소가 아니다**. URL에 호스트 이름이나 포트가 포함될 수는 있지만, TCP가 사용하는 종점의 주소는 IP 주소와 포트 번호의 조합이다.

NoteBase

문 15. 개인정보 보호위원회의 「가명정보 처리 가이드라인」(2024. 2.)에 있는 정형데이터 가명처리 기술로 다음에서 설명하는 암호화 기법은?

◯ 암호화된 상태에서의 연산이 가능한 암호화 방식으로 원래의 값을 암호화한 상태로 연산 처리를 하여 다양한 분석에 이용 가능한 기술이다.
◯ 암호화된 상태의 연산값을 복호화하면 원래의 값을 연산한 것과 동일한 결과를 얻을 수 있는 4세대 암호화기법이다.

① 동형 암호화(homomorphic encryption)
② 다형성 암호화(polymorphic encryption)
③ 순서보존 암호화(order-preserving encryption)
④ 형태보존 암호화(format-preserving encryption)

정답 1번

간단한 해설

동형 암호화는 데이터를 복호화하지 않고 암호화된 상태로 연산할 수 있게 한다. 암호문 연산 결과를 복호화하면 **원래 데이터에 대응 연산을 수행한 결과**를 얻는다는 점이 결정적인 단서이다.

핵심 풀이

동형 암호화는 **평문을 드러내지 않고 암호문에 대해 연산**할 수 있는 암호화 방식이다. 지원되는 연산을 암호문에 수행하면 결과도 암호문으로 나오며, 이를 복호화하면 원래 평문에 대응 연산을 수행한 결과를 얻는다. 예를 들어 덧셈을 지원하는 방식에서 2와 3을 각각 암호화한 뒤 동형 덧셈을 수행하면, 그 결과를 복호화하여 5를 얻는다. 따라서 제시문의 두 설명은 모두 동형 암호화의 성질을 가리킨다.

순서보존 암호화는 **평문 값의 대소관계**가 암호화 후에도 유지되는 방식이다. 암호화된 값으로 순서를 비교할 수 있다는 성질과, 암호문 연산 결과를 복호화하여 평문 연산 결과를 얻는 성질은 구별된다.

형태보존 암호화는 **데이터의 형식과 길이**를 암호화 후에도 유지하는 방식이다. 예를 들어 정해진 길이의 숫자열을 같은 길이의 숫자열로 암호화하는 성질이며, 제시문의 핵심인 암호문 상태의 연산을 뜻하지 않는다.

NoteBase

문 16. 「개인정보 보호법」에서 규정하고 있는 사항이 아닌 것은?

① 개인정보의 수집·이용

② 위치정보사업자의 개인위치정보 제공

③ 고정형 영상정보처리기기의 설치·운영 제한

④ 개인정보 처리방침의 수립 및 공개

정답 2번

①

개인정보 보호법은 **개인정보의 수집 요건과 수집 목적 범위에서의 이용**을 규정한다.

개인정보 보호법 제15조 제1항
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. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
3. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우
4. 정보주체와 체결한 계약을 이행하거나 계약을 체결하는 과정에서 정보주체의 요청에 따른 조치를 이행하기 위하여 필요한 경우
5. 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
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.
7. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우

②

위치정보사업자의 개인위치정보 제공은 **「위치정보의 보호 및 이용 등에 관한 법률」에서 별도로 규정**한다.

위치정보의 보호 및 이용 등에 관한 법률 제20조 제1항
위치정보의 보호 및 이용 등에 관한 법률 제20조(위치정보사업자의 개인위치정보 제공 등)
①제19조제1항 또는 제2항에 따라 개인위치정보주체의 동의를 얻은 위치기반서비스사업자는 제19조제1항 또는 제2항의 이용 또는 제공목적을 달성하기 위하여 해당 개인위치정보를 수집한 위치정보사업자에게 해당 개인위치정보의 제공을 요청할 수 있다. 이 경우 위치정보사업자는 정당한 사유없이 제공을 거절하여서는 아니된다. <개정 2020.6.9>

NoteBase

③

개인정보 보호법은 **공개된 장소의 고정형 영상정보처리기기 설치·운영을 법정 허용 사유가 있는 경우로 제한**한다.

개인정보 보호법 제25조 제1항
개인정보 보호법 제25조(고정형 영상정보처리기기의 설치 · 운영 제한)
① 누구든지 다음 각 호의 경우를 제외하고는 공개된 장소에 고정형 영상정보처리기기를 설치 · 운영하여서는 아니 된다. <개정 2023.3.14>
1. 법령에서 구체적으로 허용하고 있는 경우
2. 범죄의 예방 및 수사를 위하여 필요한 경우
3. 시설의 안전 및 관리, 화재 예방을 위하여 정당한 권한을 가진 자가 설치 · 운영하는 경우
4. 교통단속을 위하여 정당한 권한을 가진 자가 설치 · 운영하는 경우
5. 교통정보의 수집 · 분석 및 제공을 위하여 정당한 권한을 가진 자가 설치 · 운영하는 경우
6. 촬영된 영상정보를 저장하지 아니하는 경우로서 대통령령으로 정하는 경우

NoteBase

④

개인정보 보호법은 개인정보처리자가 **개인정보 처리방침을 수립하고, 수립·변경 시 정보주체가 쉽게 확인할 수 있도록 공개**하도록 규정한다.

개인정보 보호법 제30조 제1항, 개인정보 보호법 제30조 제2항
개인정보 보호법 제30조(개인정보 처리방침의 수립 및 공개)
① 개인정보처리자는 다음 각 호의 사항이 포함된 개인정보의 처리 방침(이하 "개인정보 처리방침"이라 한다)을 정하여야 한다. 이 경우 공공기관은 제32조에 따라 등록대상이 되는 개인정보파일에 대하여 개인정보 처리방침을 정한다. <개정 2016.3.29, 2020.2.4, 2023.3.14>
1. 개인정보의 처리 목적
2. 개인정보의 처리 및 보유 기간
3. 개인정보의 제3자 제공에 관한 사항(해당되는 경우에만 정한다)
3의2. 개인정보의 파기절차 및 파기방법(제21조제1항 단서에 따라 개인정보를 보존하여야 하는 경우에는 그 보존근거와 보존하는 개인정보 항목을 포함한다)
3의3. 제23조제3항에 따른 민감정보의 공개 가능성 및 비공개를 선택하는 방법(해당되는 경우에만 정한다)
4. 개인정보처리의 위탁에 관한 사항(해당되는 경우에만 정한다)
4의2. 제28조의2 및 제28조의3에 따른 가명정보의 처리 등에 관한 사항(해당되는 경우에만 정한다)
5. 정보주체와 법정대리인의 권리 · 의무 및 그 행사방법에 관한 사항
6. 제31조에 따른 개인정보 보호책임자의 성명 또는 개인정보 보호업무 및 관련 고충사항을 처리하는 부서의 명칭과 전화번호 등 연락처
7. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치 · 운영 및 그 거부에 관한 사항(해당하는 경우에만 정한다)
8. 그 밖에 개인정보의 처리에 관하여 대통령령으로 정한 사항
② 개인정보처리자가 개인정보 처리방침을 수립하거나 변경하는 경우에는 정보주체가 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다.

NoteBase

문 17. 다음은 「OECD 프라이버시 프레임워크」(2013)에서 제시한 개인정보 보호 원칙을 설명한 것이다. (가)와 (나)에 해당하는 것을 A ~ D에서 바르게 연결한 것은?

(가) 개인 데이터의 수집에는 제한이 있어야 하고 그러한 정보는 적법하고 공정한 방법에 의해 얻어져야 하며, 정보주체의 적절한 인지 또는 동의가 있어야 한다.
(나) 개인 데이터는 사용목적과 관계가 있어야 하고 그 목적에 필요한 한도 내에서 정확하고, 완전하며, 최신의 것이어야 한다.
A. 수집 제한의 원칙(collection limitation principle)
B. 목적 명확화의 원칙(purpose specification principle)
C. 데이터 품질 원칙(data quality principle)
D. 개인 참여의 원칙(individual participation principle)

① (가): A, (나): B
② (가): A, (나): C
③ (가): D, (나): B
④ (가): D, (나): C

정답 2번

가

수집 제한의 원칙은 **개인정보의 수집 범위를 제한하고 적법하고 공정한 방법으로 수집**하도록 하는 원칙이다. 적절한 경우 정보주체의 인지 또는 동의를 요구한다.

나

데이터 품질 원칙은 **사용목적과의 관련성**을 요구하고, 그 목적에 필요한 범위에서 **정확성·완전성·최신성**을 유지하도록 하는 원칙이다.

NoteBase

문 18. ISMS-P의 보호대책 요구사항 중 '외부자 보안' 인증 항목에 해당하지 않는 것은?

① 보호 구역 지정

② 외부자 현황 관리

③ 외부자 보안 이행 관리

④ 외부자 계약 변경 및 만료 시 보안

정답 1번

간단한 해설

'보호 구역 지정'은 중요한 정보와 시설을 보호할 구역을 정하는 **물리 보안** 항목이다. 외부자 보안은 외부 위탁이나 외부 서비스 이용에 따른 위험과 보안조치를 관리한다.

선지별 해설

① X: '보호 구역 지정'은 외부자 보안이 아니라 **2.4 물리 보안의 2.4.1 보호구역 지정**에 해당한다. 중요한 정보·문서·시설 등을 보호하기 위해 보호구역을 지정하고 구역별 보호대책을 마련하는 항목이다.

② O: '외부자 현황 관리'는 2.3.1 항목이다. 업무를 외부에 위탁하거나 외부 시설·서비스를 이용하는 현황을 식별하고, 관련 법적 요구사항과 **외부 조직·서비스로부터 발생하는 위험**을 파악하여 보호대책을 마련한다.

③ O: '외부자 보안 이행 관리'는 2.3.3 항목이다. 계약서·협정서·내부정책에 명시된 보안 요구사항에 따라 외부자가 보호대책을 실제로 이행하는지 **주기적인 점검이나 감사로 관리·감독**한다.

④ O: '외부자 계약 변경 및 만료 시 보안'은 2.3.4 항목이다. 계약 만료, 업무 종료 또는 담당자 변경 시 제공한 정보자산의 반납, 정보시스템 접근계정 삭제, 중요정보 파기, 비밀유지 확약서 징구 등의 조치를 이행한다. 이는 **업무 관계가 끝나거나 바뀐 뒤에도 정보나 접근수단이 남는 위험**을 관리하기 위한 것이다.

NoteBase

문 19. NIST 표준(FIPS 186)인 전자서명 표준(DSS)에 대한 설명으로 옳지 않은 것은?

① DSA(Digital Signature Algorithm)는 DSS에서 명세한 알고리즘으로 ElGamal과 Schnorr에 의해 제안된 기법을 기반으로 한다.

② 서명자는 공개키와 개인키의 쌍을 생성하고 검증에 필요한 매개변수들을 공개해야 한다.

③ 서명 과정을 거치고 나면 두 개의 요소로 이루어진 서명이 생성되는데 서명자는 이를 메시지와 함께 수신자(검증자)에게 보낸다.

④ 검증 과정에서 검증자는 서명으로부터 추출한 값과 수신한 메시지로부터 얻은 해시값을 비교하여 일치하는가를 확인함으로써 서명을 검증한다.

정답 4번

간단한 해설

DSA는 수신한 메시지의 해시값을 검증 연산에 사용하지만, 그 해시값 자체를 서명에서 추출한 값과 직접 비교하지 않는다. 메시지의 해시값·서명·공개키로 계산한 **검증값 v와 서명 요소 r**이 일치하는지 확인한다.

선지별 해설

① O: DSA는 DSS에 명세된 전자서명 알고리즘이며, ElGamal과 Schnorr의 서명 기법을 바탕으로 한다. 이들은 **이산대수 문제의 어려움**을 이용하는 서명 기법으로, 공개된 정보만으로 개인키를 알아내기 어렵다는 성질을 이용한다.

② O: 서명자는 공개키와 개인키의 쌍을 생성한다. **개인키는 비밀로 유지**하여 서명 생성에 사용하고, 공개키와 공통 매개변수 p, q, g는 검증자가 이용할 수 있도록 제공한다. 검증자는 이 정보로 서명자를 확인하므로 공개키와 매개변수는 신뢰할 수 있는 방식으로 전달되어야 한다.

③ O: DSA의 서명은 **두 수 r과 s의 쌍**으로 구성된다. 서명자는 메시지의 해시값, 개인키, 서명마다 생성하는 비밀 난수 등을 이용해 서명을 만들고, 메시지와 함께 검증자에게 보낸다. 메시지 자체와 서명은 서로 구별되는 데이터이다.

④ X: DSA는 서명에서 해시값을 복원하여 수신 메시지의 해시값과 비교하는 방식이 아니다. 검증자는 먼저 서명 요소 r과 s가 허용 범위에 있는지 확인하고, 수신 메시지의 해시값·서명·서명자의 공개키·공통 매개변수로 검증값 v를 계산한다. 마지막에 **v와 수신한 서명 요소 r이 일치하는지** 확인하여 서명을 검증한다. 해시값은 검증값을 계산하는 입력이며, 최종 비교 대상은 v와 r이다.

NoteBase

문 20. 「개인정보 보호법」 제31조(개인정보 보호책임자의 지정 등)에서 규정한 개인정보 보호책임자의 수행 업무가 아닌 것은?

① 개인정보 보호 계획의 수립 및 시행

② 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선

③ 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축

④ 정보주체의 권리침해에 대한 조사 및 이에 따른 처분에 관한 사항

정답 4번

①

개인정보 보호책임자는 **개인정보 보호 계획을 수립하고 시행**하는 업무를 수행한다.

개인정보 보호법 제31조 제4항 제1호
개인정보 보호법 제31조(개인정보 보호책임자의 지정 등)
④ 개인정보 보호책임자는 다음 각 호의 업무를 수행한다. <개정 2023.3.14, 2026.3.10>
1. 개인정보 보호 계획의 수립 및 시행

②

개인정보 보호책임자는 **개인정보 처리 및 보호의 실태와 관행을 정기적으로 조사하고 개선**하는 업무를 수행한다.

개인정보 보호법 제31조 제4항 제4호
개인정보 보호법 제31조(개인정보 보호책임자의 지정 등)
④ 개인정보 보호책임자는 다음 각 호의 업무를 수행한다. <개정 2023.3.14, 2026.3.10>
4. 개인정보 처리 및 보호의 실태와 관행에 대한 정기적인 조사 및 개선

③

개인정보 보호책임자는 **개인정보 유출 및 오용·남용을 방지하기 위한 내부통제시스템을 구축**하는 업무를 수행한다.

개인정보 보호법 제31조 제4항 제6호
개인정보 보호법 제31조(개인정보 보호책임자의 지정 등)
④ 개인정보 보호책임자는 다음 각 호의 업무를 수행한다. <개정 2023.3.14, 2026.3.10>
6. 개인정보 유출 및 오용 · 남용 방지를 위한 내부통제시스템의 구축

NoteBase

④

정보주체의 권리침해에 대한 조사 및 이에 따른 처분은 **개인정보 보호위원회의 소관 사무**이다. 개인정보 보호책임자의 수행 업무에 해당하지 않는다.

개인정보 보호법 제7조의8 제3호
개인정보 보호법 제7조의8(보호위원회의 소관 사무) 보호위원회는 다음 각 호의 소관 사무를 수행한다. <개정 2023.3.14>
3. 정보주체의 권리침해에 대한 조사 및 이에 따른 처분에 관한 사항

NoteBase