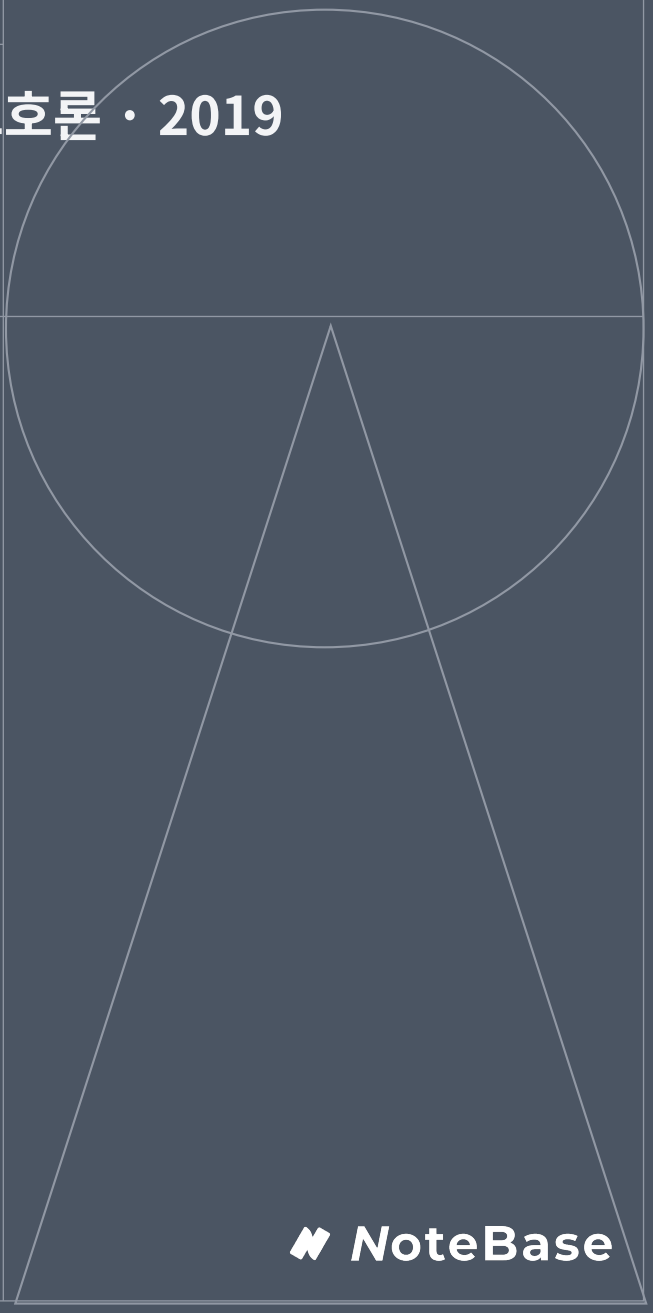
기출OX 해설집

공무원/지방직/9급 · 정보보호론 · 2019



NoteBase

기출OX 해설집

공무원/지방직/9급 · 정보보호론 · 2019

공무원/지방직/9급 · 정보보호론 · 2019

문 1. 정보통신망 등의 침해사고에 대응하기 위해 기업이나 기관의 업무 관할 지역 내에서 침해사고의 접수 및 처리 지원을 비롯해 예방, 피해 복구 등의 임무를 수행하는 조직은?

① CISO

② CERT

③ CPPG

④ CPO

정답 2번

간단한 해설

침해사고의 접수·처리 지원부터 예방과 피해 복구까지 맡는 **전담 대응 조직**이 CERT이다. 사고가 발생한 뒤의 대응뿐 아니라 사고를 줄이기 위한 예방 활동도 수행한다.

공통 해설

CERT(Computer Emergency Response Team)는 기업이나 기관의 관할 범위에서 정보통신망의 침해사고에 대응하는 **침해사고대응팀**이다. 사고 신고를 접수하고 원인과 영향을 분석하여 처리와 피해 복구를 지원하며, 사고 예방 활동도 수행한다. 즉, '접수 및 처리 지원·예방·피해 복구'는 별개의 조직을 뜻하는 단서가 아니라 CERT가 담당하는 업무 범위이다. 이 문항은 개인의 책임자 직위나 자격 명칭이 아니라 **이 업무들을 수행하는 조직**을 묻는다.

NoteBase

문 2. OECD 개인정보보호 8개 원칙 중 다음에서 설명하는 것은?

개인정보 침해, 누설, 도용을 방지하기 위한 물리적·조직적·기술적인 안전조치를 확보해야 한다.

① 수집 제한의 원칙(Collection Limitation Principle)
② 이용 제한의 원칙(Use Limitation Principle)
③ 정보 정확성의 원칙(Data Quality Principle)
④ 안전성 확보의 원칙(Security Safeguards Principle)

정답 4번

간단한 해설

개인정보의 침해·누설·도용을 막기 위해 **물리적·조직적·기술적 안전조치**를 갖추는 것은 **안전성 확보의 원칙**이다.

공통 해설

안전성 확보의 원칙(Security Safeguards Principle)은 개인정보를 분실, 무단 접근, 파괴, 부당한 이용·변경·공개 등의 위험으로부터 보호하도록 합리적인 안전조치를 마련해야 한다는 원칙이다. 지문의 '침해, 누설, 도용을 방지'한다는 설명은 **위험을 막는 보호조치의 확보**를 요구하므로 이 원칙에 해당한다. 판단의 초점은 수집·이용의 범위나 정보 내용의 정확성이 아니라 개인정보를 안전하게 지키는 조치에 있다.

예를 들어 개인정보가 보관된 장소의 출입을 통제하는 것은 물리적 조치, 개인정보 취급자의 권한과 업무 절차를 정하는 것은 조직적 조치, 시스템에서 사용자 인증과 접근 통제를 적용하는 것은 기술적 조치이다. 이처럼 안전조치는 **기술적 수단에만 한정되지 않는다**.

NoteBase

문 3. 취약한 웹 사이트에 로그인한 사용자가 자신의 의지와는 무관하게 공격자가 의도한 행위(수정, 삭제, 등록 등)를 일으키도록 위조된 HTTP 요청을 웹 응용 프로그램에 전송하는 공격은?

① DoS 공격

② 취약한 인증 및 세션 공격

③ SQL 삽입 공격

④ CSRF 공격

정답 4번

간단한 해설

로그인한 사용자의 **인증 상태를 악용해 본인 의사와 무관한 요청**을 보내도록 하는 것이 CSRF(사이트 간 요청 위조)이다. 웹 응용 프로그램이 이 요청을 사용자의 정상적인 요청으로 받아들이면 공격자가 의도한 수정·삭제·등록 등이 실행된다.

공통 해설

CSRF(Cross-Site Request Forgery, 사이트 간 요청 위조)는 이미 인증된 사용자의 브라우저가 공격자가 만든 요청을 대상 웹 응용 프로그램에 보내도록 유도하는 공격이다. 브라우저가 해당 사이트의 세션 쿠키 등 인증정보를 요청에 자동으로 첨부하고, 서버가 요청의 위조 여부를 제대로 확인하지 않으면 **사용자가 로그인했다는 사실을 사용자가 그 행위를 원했다는 뜻으로 잘못 신뢰**하게 된다.

예를 들어, 사용자가 로그인 상태에서 공격자가 만든 페이지에 접근했을 때 브라우저가 대상 사이트로 게시물 등록 요청을 보내도록 할 수 있다. 취약한 사이트가 이를 정상 요청으로 처리하면 사용자가 직접 등록을 의도하지 않았어도 게시물이 등록된다. 문제의 '로그인한 사용자', '자신의 의지와는 무관한 행위', '위조된 HTTP 요청'은 이러한 CSRF의 작동 방식을 설명한다.

NoteBase

문 4. 스테가노그래피에 대한 설명으로 옳지 않은 것은?

① 스테가노그래피는 민감한 정보의 존재 자체를 숨기는 기술이다.

② 원문 데이터에 비해 더 많은 정보의 은닉이 가능하므로 암호화보다 공간효율성이 높다.

③ 텍스트·이미지 파일 등과 같은 디지털화된 데이터에 비밀 이진(Binary) 정보가 은닉될 수 있다.

④ 고해상도 이미지 내 각 픽셀의 최하위 비트들을 변형하여 원본의 큰 손상 없이 정보를 은닉하는 방법이 있다.

정답 2번

간단한 해설

스테가노그래피는 비밀정보를 다른 데이터에 숨기므로 **은닉 용량이 매체의 크기와 허용 가능한 변형 정도에 제한**된다. 일반적으로 비밀정보보다 큰 운반 매체가 필요하므로, 더 많은 정보를 넣을 수 있어 암호화보다 공간효율성이 높다는 설명은 성립하지 않는다.

선지별 해설

① O: 스테가노그래피는 평범해 보이는 텍스트나 이미지 등에 비밀정보를 넣어 **정보가 존재한다는 사실 자체를 숨기는** 기술이다. 암호화가 정보의 내용을 알아보기 어렵게 바꾸는 것과 구별된다.

② X: 스테가노그래피의 은닉 용량은 원문인 운반 매체의 크기와, 눈에 띄지 않게 바꿀 수 있는 부분의 양에 제한된다. 일반적으로 적은 양의 비밀정보를 숨기는 데 그보다 큰 매체가 필요하므로 **암호화보다 공간효율성이 높다고 할 수 없다**. '원문 데이터에 비해 더 많은 정보의 은닉이 가능하다'는 설명은 '운반 매체가 허용하는 제한된 양의 정보를 은닉한다'로 고친다.

③ O: 비밀정보를 0과 1의 비트열로 표현하면 텍스트·이미지 등 디지털 매체에 넣을 수 있다. 매체의 형식에 맞는 은닉 방법을 이용하여, 겉으로는 평범한 파일처럼 보이면서 내부에는 비밀 비트열을 담도록 한다.

④ O: 이미지의 픽셀을 나타내는 값에서 **최하위 비트(LSB)**는 값의 크기에 미치는 영향이 가장 작은 비트이다. 예를 들어 8비트 색상값 100의 최하위 비트를 0에서 1로 바꾸면 값은 101이 되어 변화가 작다. 이런 방식으로 일부 최하위 비트에 비밀정보를 넣으면 눈에 띄는 화질 손상을 줄이면서 정보를 은닉할 수 있다.

NoteBase

문 5. 다음 중 OSI 7계층 모델에서 동작하는 계층이 다른 것은?

① L2TP

② SYN 플러딩

③ PPTP

④ ARP 스푸핑

정답 2번

간단한 해설

SYN 플러딩은 TCP의 연결 설정 절차를 악용하므로 **전송 계층(4계층)** 공격이다. 나머지 항목은 데이터 링크 계층(2계층)의 터널링 또는 주소 해석과 관련된다.

선지별 해설

① L2TP: **데이터 링크 계층(2계층)**의 터널링 프로토콜이다. PPP 프레임을 캡슐화하여 다른 네트워크를 거쳐 전달한다. 터널을 운반하는 하위 프로토콜과 터널링 대상인 PPP의 계층을 구별해야 한다.

② SYN 플러딩: **전송 계층(4계층)** 공격이다. TCP의 3단계 연결 설정 과정에서 SYN 요청을 대량으로 보내고 연결을 완료하지 않아, 서버에 미완료 연결 상태가 쌓이게 한다. 이로 인해 연결 처리 자원이 소모되어 정상적인 연결 요청을 처리하기 어려워진다.

③ PPTP: **데이터 링크 계층(2계층)**의 터널링 프로토콜이다. PPP 프레임을 캡슐화하여 IP 네트워크를 통해 전달하므로, L2TP와 마찬가지로 2계층 터널링에 분류한다.

④ ARP 스푸핑: **데이터 링크 계층(2계층)** 공격이다. 같은 LAN에서 IP 주소에 대응하는 MAC 주소를 알아내는 ARP의 주소 대응 정보를 위조한다. 예를 들어 게이트웨이의 IP 주소에 공격자의 MAC 주소를 연결하도록 속이면, 게이트웨이로 향할 프레임이 공격자에게 전달될 수 있다.

L2TP·PPTP·ARP 스푸핑은 2계층에 해당하는 반면, SYN 플러딩은 TCP의 연결 설정을 공격하는 4계층 공격이므로 동작 계층이 다르다.

NoteBase

문 6. 해시 함수의 충돌에 대한 설명으로 옳은 것은?

① 해시 함수의 입력 메시지가 길어짐에 따라 생성되는 해시 값이 길어지는 것을 의미한다.

② 서로 다른 해시 함수가 서로 다른 입력 값에 대해 동일한 출력 값을 내는 것을 의미한다.

③ 동일한 해시 함수가 서로 다른 두 개의 입력 값에 대해 동일한 출력 값을 내는 것을 의미한다.

④ 동일한 해시 함수가 동일한 입력 값에 대해 다른 출력 값을 내는 것을 의미한다.

정답 3번

간단한 해설

해시 충돌은 **동일한 해시 함수**에 **서로 다른 입력**을 넣었는데 같은 해시 값이 나오는 현상이다. 입력이 다르다는 조건과 출력이 같다는 조건을 함께 만족해야 한다.

선지별 해설

① X: 해시 값의 길이가 늘어나는 것은 충돌의 의미가 아니다. 일반적인 암호학적 해시 함수는 입력 메시지의 길이와 관계없이 **정해진 길이의 해시 값**을 출력한다. 충돌은 출력 길이가 아니라 서로 다른 입력의 출력 값이 같은지에 관한 개념이다.

② X: 충돌은 **동일한 해시 함수 안에서** 서로 다른 입력의 출력이 같아지는 현상이다. 서로 다른 해시 함수의 출력이 같다는 것만으로는 이 정의에 해당하지 않는다.

③ O: 하나의 해시 함수에 서로 다른 두 입력을 넣었을 때 **동일한 해시 값**이 나오면 충돌이다. 해시 함수를 H, 두 입력을 x, y라고 하면 $x \neq y$이면서 $H(x) = H(y)$인 경우이다.

④ X: 동일한 해시 함수는 동일한 입력에 대해 **항상 동일한 출력**을 내는 결정적 함수이다. 충돌에서는 입력이 서로 달라야 하며, 같아지는 것은 출력 값이다.

NoteBase

문 7. 암호화 기법들에 대한 설명으로 옳지 않은 것은?

① Feistel 암호는 전치(Permutation)와 대치(Substitution)를 반복시켜 암호문에 평문의 통계적인 성질이나 암호키와의 관계가 나타나지 않도록 한다.

② Kerckhoff의 원리는 암호 해독자가 현재 사용되고 있는 암호 방식을 알고 있다고 전제한다.

③ AES는 암호키의 길이를 64비트, 128비트, 256비트 중에서 선택한다.

④ 2중 DES(Double DES) 암호 방식은 외형상으로는 DES에 비해 2배의 키 길이를 갖지만, 중간일치공격 시 키의 길이가 1비트 더 늘어난 효과밖에 얻지 못한다.

정답 3번

간단한 해설

③의 '64비트'를 **192비트**로 고쳐야 한다. AES가 지원하는 키 길이는 **128·192·256비트**이다.

선지별 해설

① O: Feistel 암호는 평문 블록을 두 부분으로 나누고, 라운드 함수와 키를 이용한 변환을 반복한다. DES와 같은 Feistel 암호에서는 대치로 키와 암호문의 관계를 복잡하게 하는 **혼돈**을, 전치와 반복으로 평문의 통계적 특성을 암호문 전체에 퍼뜨리는 **확산**을 구현한다. 이를 통해 통계적 특성이나 키와의 관계를 쉽게 분석하지 못하게 한다.

② O: Kerckhoff의 원리는 공격자가 암호 알고리즘을 알고 있어도 암호체계가 안전해야 한다는 원리이다. 보안의 근거는 알고리즘을 감추는 데 있지 않고 **키의 비밀성**에 있으므로, 암호 해독자가 사용 중인 암호 방식을 안다고 전제한다.

③ X: AES가 지원하는 키 길이는 **128비트, 192비트, 256비트**이다. 64비트 키는 지원하지 않으므로 선지의 '64비트'를 '192비트'로 고쳐야 한다. 키 길이와 달리 AES가 한 번에 처리하는 블록의 크기는 항상 128비트이다.

④ O: DES의 유효 키 길이는 56비트이고, 2중 DES는 서로 다른 두 키를 사용하므로 전체 키 길이가 112비트이다. 그러나 중간일치공격은 알려진 평문을 첫 번째 키 후보들로 암호화한 값과, 대응하는 암호문을 두 번째 키 후보들로 복호화한 값을 비교하여 중간값이 일치하는 키 쌍을 찾는다. 일치한 후보는 다른 평문·암호문 쌍으로 확인한다. 충분한 저장 공간을 사용하는 기본 공격의 주요 연산량은 $2^{56} + 2^{56} = 2^{57}$회 수준이며, 약 2^{56}개의 중간값을 저장한다. 따라서 **연산량을 기준으로 한 보안 효과**는 57비트 키 수준으로 설명하며, 실제 키 길이가 57비트로 바뀐다는 뜻은 아니다.

NoteBase

문 8. 디지털 포렌식에 대한 설명에서 ㉠, ㉡에 들어갈 용어는?

(㉠) 공간은 물리적으로 파일에 할당된 공간이지만 논리적으로 사용할 수 없는 낭비 공간이기 때문에, 공격자가 의도적으로 정보를 은닉할 가능성이 있다. 또한, 이전에 저장되었던 데이터가 남아 있을 가능성이 있어 파일 복구와 삭제된 파일의 파편 조사에 활용할 수 있다. 이 때, 디지털 포렌식의 파일 (㉡) 과정을 통해 디스크 내 비구조화된 데이터 스트림을 식별하고 의미 있는 내용을 추출할 수 있다.

① ㉠: 실린더(Cylinder), ㉡: 역어셈블링(Disassembling)

② ㉠: MBR(Master Boot Record), ㉡: 리버싱(Reversing)

③ ㉠: 클러스터(Cluster), ㉡: 역컴파일(Decompiling)

④ ㉠: 슬랙(Slack), ㉡: 카빙(Carving)

정답 4번

간단한 해설

파일에 할당된 영역 중 실제 파일 내용이 끝난 뒤 남는 공간이 **슬랙(Slack)**이다. 디스크의 데이터 자체에서 파일 형식의 특징을 찾아 의미 있는 내용을 추출하는 기법은 **카빙(Carving)**이다.

빈칸별 해설

㉠ 슬랙(Slack): 파일에 할당된 마지막 저장 단위에서 **실제 파일 내용의 끝과 할당 영역의 끝 사이**에 남는 공간이다. 파일은 클러스터 단위로 공간을 할당받으므로 마지막 클러스터를 모두 채우지 못하면 이런 여유 부분이 생긴다. 클러스터는 할당 단위 자체이고, 슬랙은 그 안에서 파일 내용으로 사용되지 않는 부분이라는 차이가 있다. 이곳에 이전 데이터의 흔적이 남거나 정보가 의도적으로 숨겨질 수 있으므로 디지털 포렌식의 조사 대상이 된다.

㉡ 카빙(Carving): **파일시스템 메타데이터보다 데이터 내용에 근거하여**파일이나 그 일부를 식별하고 추출하는 기법이다. 예를 들어 파일 형식에 고유한 헤더와 푸터 등의 특징을 찾아 데이터의 시작과 끝을 판단한다. 따라서 파일 목록이나 저장 위치 정보가 손상되어도 남아 있는 데이터에서 복구를 시도할 수 있다. 지문의 '비구조화된 데이터 스트림을 식별하고 의미 있는 내용을 추출'한다는 설명이 이에 해당한다.

㉠은 슬랙, ㉡은 카빙이므로 두 용어의 조합은 ④와 일치한다.

NoteBase

문 9. 버퍼 오버플로우 공격 대응 방법 중 ASLR(Address Space Layout Randomization)에 대한 설명으로 옳은 것은?

① 함수의 복귀 주소 위조 시, 공격자가 원하는 메모리 공간의 주소를 지정하기 어렵게 한다.

② 함수의 복귀 주소와 버퍼 사이에 랜덤(Random) 값을 저장하여 해당 주소의 변조 여부를 탐지한다.

③ 스택에 있는 함수 복귀 주소를 실행 가능한 임의의 libc 영역 내 주소로 지정하여 공격자가 원하는 함수의 실행을 방해한다.

④ 함수 호출 시 복귀 주소를 특수 스택에 저장하고 종료 시 해당 스택에 저장된 값과 비교하여 공격을 탐지한다.

정답 1번

간단한 해설

ASLR은 스택·힙·공유 라이브러리 등의 **메모리 배치를 무작위화**하여 공격 대상 주소를 예측하기 어렵게 한다. 따라서 공격자가 복귀 주소를 위조하더라도 원하는 코드나 데이터의 정확한 주소를 지정하기 어려워진다.

선지별 해설

① O: ASLR은 프로그램의 스택·힙·공유 라이브러리 등이 배치되는 주소를 무작위화한다. 함수의 복귀 주소를 위조해 실행 흐름을 바꾸려면 이동할 대상의 주소를 알아야 하므로, **대상 주소의 예측을 어렵게 하는 것**이 ASLR의 방어 원리이다.

② X: 버퍼와 복귀 주소 사이에 검사값을 두는 것은 **스택 카나리** 방식이다. 버퍼를 넘쳐 쓴 데이터가 복귀 주소에 도달하는 과정에서 카나리까지 덮어쓰면, 함수가 복귀하기 전에 검사값의 변화를 확인하여 메모리 훼손을 탐지한다. ASLR은 검사값을 비교하는 대신 메모리 배치를 무작위화한다.

③ X: 복귀 주소를 libc의 함수 주소로 덮어쓰는 것은 **Return-to-libc 공격**의 원리이다. libc는 C 표준 라이브러리이며, 이 공격은 이미 메모리에 있는 라이브러리 코드를 이용해 공격자가 원하는 함수를 실행하도록 유도한다. 따라서 '원하는 함수의 실행을 방해한다'는 설명도 잘못되었다. ASLR은 라이브러리의 적재 주소를 무작위화하여 이러한 공격에 필요한 함수 주소를 예측하기 어렵게 한다.

④ X: 복귀 주소의 사본을 별도 스택에 보관하는 것은 **섀도 스택** 방식이다. 함수 호출 시 정상 복귀 주소를 별도로 저장하고, 복귀 시 일반 스택의 복귀 주소와 비교하여 불일치를 탐지한다. 주소의 위치를 예측하기 어렵게 하는 ASLR과 달리, 저장된 복귀 주소가 변조되었는지를 확인하는 방식이다.

NoteBase

문 10. 국내의 기관이나 기업이 정보 및 개인정보를 체계적으로 보호할 수 있도록 통합된 관리체계 인증제도는?

① PIPL－P

② ISMS－I

③ PIMS－I

④ ISMS－P

정답 4번

간단한 해설

ISMS-P는 정보보호 관리체계(ISMS)와 개인정보보호 관리체계(PIMS)를 하나로 통합한 인증제도이다. 정보보호와 개인정보보호를 함께 다룬다는 점이 핵심이다.

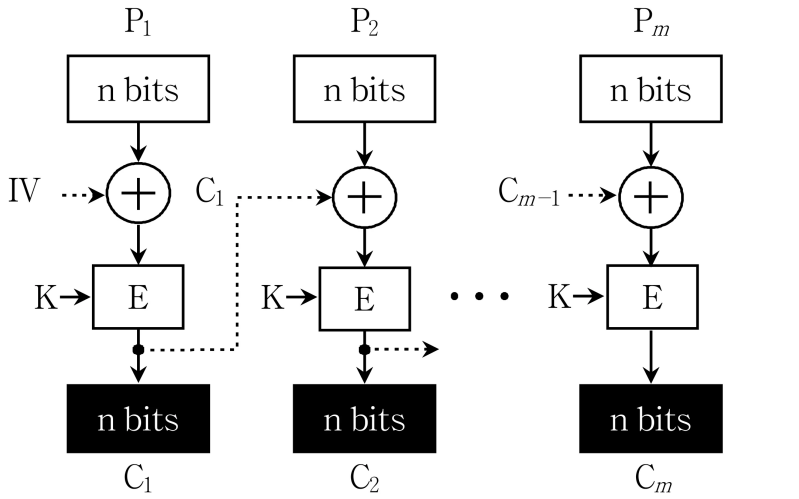
공통 해설

ISMS-P의 명칭은 '정보보호 및 개인정보보호 관리체계 인증'이다. 기관이나 기업이 정보와 개인정보를 보호하기 위한 관리체계를 갖추고 운영하는지를 심사하여 인증한다.

기존에 따로 운영되던 정보보호 관리체계 인증(ISMS)과 개인정보보호 관리체계 인증(PIMS)을 **하나의 인증체계로 통합**한 것이 ISMS-P이다. 따라서 문항의 '정보 및 개인정보'와 '통합된 관리체계'라는 조건은 ISMS-P에 대응한다.

NoteBase

문 11. 다음의 블록 암호 운용 모드는?



① 전자 코드북 모드(Electronic Code Book Mode)

② 암호 블록 연결 모드(Cipher Block Chaining Mode)

③ 암호 피드백 모드(Cipher Feedback Mode)

④ 출력 피드백 모드(Output Feedback Mode)

정답 2번

간단한 해설

이전 암호 블록을 현재 평문 블록과 **XOR한 뒤 암호화**하는 구조는 암호 블록 연결(CBC) 모드이다. 첫 블록에는 이전 암호 블록 대신 초기화 벡터(IV)를 사용한다.

NoteBase

도식 해설

첫 블록: 그림에서 평문 P_1과 IV가 XOR 기호로 들어가고, 그 결과가 암호화 상자 E에 입력된다. XOR는 대응하는 두 비트가 다르면 1, 같으면 0을 만드는 연산이다. 키 K를 사용하는 암호화 함수를 E_K라 하면 첫 암호 블록은 $C_1 = E_K(P_1 \oplus IV)$이다. 첫 블록에는 앞선 암호 블록이 없으므로 **IV가 연결의 시작값**이 된다.

후속 블록: 점선 화살표는 앞에서 생성한 C_1이 다음 평문 P_2의 XOR 입력으로 들어감을 나타낸다. 따라서 $C_2 = E_K(P_2 \oplus C_1)$이며, 이후에도 같은 방식으로 이전 암호 블록과 현재 평문 블록을 결합한다. 이처럼 **이전 암호 블록을 평문과 XOR한 결과를 암호화**하는 방식이 암호 블록 연결(CBC) 모드이다.

다른 모드와의 구분: ECB는 각 평문 블록을 독립적으로 암호화하므로 그림과 같은 이전 암호 블록의 연결이 없다. CFB와 OFB는 암호화 함수의 출력과 평문을 XOR하여 암호문을 만들므로, 그림과 달리 **평문과의 XOR가 암호화 상자 뒤**에 놓인다. 이때 CFB는 암호문을, OFB는 평문과 XOR하기 전의 암호화 함수 출력을 다음 암호화 입력으로 되돌린다.

NoteBase

문 12. 무결성을 위협하는 공격이 아닌 것은?

① 스누핑 공격(Snooping Attack)

② 메시지 변조 공격(Message Modification Attack)

③ 위장 공격(Masquerading Attack)

④ 재전송 공격(Replay Attack)

정답 1번

간단한 해설

스누핑은 정보를 바꾸지 않고 몰래 읽는 공격이므로 **기밀성**을 위협한다. 정보의 무단 변경이나 삽입을 막는 무결성과는 구별된다.

공통 해설

무결성은 정보가 **권한 없는 방식으로 변경되거나 삽입되지 않도록** 하는 성질이다. 공격이 정보를 읽는 데 그치는지, 수신자가 처리할 정보의 내용·출처·전달 순서를 조작하는지를 기준으로 구별한다. 스누핑은 통신 내용이나 저장된 정보를 몰래 열람하는 공격으로, 정보 자체를 변경하지 않는다. 따라서 무결성보다 **허가받지 않은 정보 열람을 막는 기밀성**을 위협하는 공격으로 분류한다.

메시지 변조는 전달되는 내용을 무단으로 바꾸고, 위장은 다른 사람이나 시스템인 것처럼 속여 그 명의의 메시지를 받아들이게 한다. 재전송은 이전에 전송된 유효한 메시지를 가로채 다시 보내는 공격이다. 이때 메시지 내용이 그대로여도 수신자가 이를 새로운 요청으로 처리하면 부당한 중복 처리가 발생할 수 있다. 예를 들어 이미 처리된 송금 요청을 다시 보내 중복 송금을 유도하는 경우이다. 이들은 각각 내용의 변경, 출처의 위조, 과거 메시지의 부당한 재삽입을 통해 정상적인 정보 처리를 훼손하므로 무결성을 위협한다.

NoteBase

문 13. 다음에서 설명하는 접근 제어 모델은?

군사용 보안구조의 요구사항을 충족시키기 위해 개발된 최초의 수학적 모델로 알려져 있다. 불법적 파괴나 변조보다는 정보의 기밀성 유지에 초점을 두고 있다. '상위레벨 읽기금지 정책(No-Read-Up Policy)'을 통해 인가받은 비밀 등급이 낮은 주체는 높은 보안 등급의 정보를 열람할 수 없다. 또한, 인가받은 비밀 등급 이하의 정보 수정을 금지하는 '하위레벨 쓰기금지 정책(No-Write-Down Policy)'을 통해 비밀 정보의 유출을 차단한다.

① DAC(Discretionary Access Control) 모델

② Bell-LaPadula 모델

③ Biba 모델

④ RBAC(Role-Based Access Control) 모델

정답 2번

간단한 해설

기밀성을 지키기 위해 상위 등급의 정보는 읽지 못하게 하고, 하위 등급의 객체에는 쓰지 못하게 하는 것이 Bell-LaPadula 모델의 핵심이다. 두 제한은 비밀 정보가 낮은 보안 등급으로 유출되는 것을 막는다.

공통 해설

Bell-LaPadula 모델은 군사적 다단계 보안 환경에서 주체와 객체의 보안 등급을 비교하여 기밀성을 유지하는 모델이다. 주체는 접근을 요청하는 사용자나 프로세스이고, 객체는 파일처럼 접근 대상이 되는 자원이다. 지문의 두 정책은 **높은 등급의 정보가 낮은 등급으로 흘러가는 것을 차단**한다는 공통 원칙에 따른다.

상위레벨 읽기금지(No Read Up)는 주체가 자신보다 높은 보안 등급의 정보를 읽지 못하게 하는 규칙이다. 낮은 등급의 사용자가 높은 등급의 파일을 읽어 비밀을 알아내는 것을 막는다.

하위레벨 쓰기금지(No Write Down)는 주체가 자신보다 낮은 보안 등급의 객체에 쓰지 못하게 하는 규칙이다. 높은 등급의 사용자가 비밀 내용을 낮은 등급의 파일에 옮겨 적으면 낮은 등급의 사용자에게 정보가 노출될 수 있기 때문이다. 여기서 하위레벨은 **자신의 등급보다 낮은 등급**을 뜻하며, 같은 등급에 대한 쓰기까지 이 규칙으로 금지되는 것은 아니다.

NoteBase

문 14. 유럽의 일반개인정보보호법(GDPR)에 대한 설명으로 옳은 것은?

① EU 회원국들 간 개인정보의 자유로운 이동을 금지하기 위한 목적을 갖는다.

② 그 자체로는 EU의 모든 회원국에게 직접적인 법적 구속력을 갖지 않는다.

③ 중요한 사항 위반 시 직전 회계연도의 전 세계 매출액 4% 또는 2천만 유로 중 높은 금액이 최대한도 부과금액이다.

④ 만 19세 미만 미성년자의 개인정보 수집 시 친권자의 동의를 얻어야 한다.

정답 3번

간단한 해설

GDPR의 중대한 위반에 대한 과징금 상한은 기업의 경우 **직전 회계연도 전 세계 연간 매출액의 4%와 2천만 유로 중 더 큰 금액**이다. 이는 반드시 부과되는 금액이 아니라 부과할 수 있는 최대한도이다.

선지별 해설

① X: GDPR 제1조는 개인정보 보호와 함께 **EU 내 개인정보의 자유로운 이동**을 목적으로 한다. 개인정보 보호를 이유로 EU 내 이동을 제한하거나 금지해서는 안 되므로, 자유로운 이동을 금지하려는 목적이라는 설명은 반대이다.

② X: GDPR은 EU의 규정(Regulation)으로서 **모든 회원국에 직접 적용되고 법적 구속력을 갖는다**. 별도의 국내법 전환을 거쳐야만 적용되는 것은 아니다.

③ O: GDPR 제83조 제5항은 개인정보 처리의 기본원칙이나 정보주체의 권리 등 중대한 사항을 위반하면, 기업의 경우 직전 회계연도 전 세계 연간 매출액의 4%와 2천만 유로 중 **더 큰 금액을 과징금 상한**으로 정한다. 실제 부과액은 위반의 성격·중대성·기간 등 개별 사정을 고려하여 결정한다.

④ X: GDPR 제8조 제1항의 기준은 만 19세 미만이 아니라 **원칙적으로 만 16세 미만**이다. 아동에게 직접 제공하는 정보사회서비스에서 동의를 근거로 개인정보를 처리할 때, 해당 연령 미만이면 친권자의 동의 또는 승인이 필요하다. 회원국은 이 기준연령을 법률로 낮출 수 있지만 만 13세보다 낮출 수는 없다.

NoteBase

문 15. IPsec의 캡슐화 보안 페이로드(ESP) 헤더에서 암호화되는 필드가 아닌 것은?

① SPI(Security Parameter Index)

② Payload Data

③ Padding

④ Next Header

정답 1번

간단한 해설

SPI는 수신 패킷에 적용할 보안 연관(SA)을 식별하므로, 수신자가 복호화 전에 읽을 수 있도록 **암호화하지 않는다**.

공통 해설

기밀성을 위해 ESP 암호화를 적용할 때, **Payload Data와 Padding·Pad Length·Next Header**는 암호화 범위에 포함된다. 반면 이들보다 앞에 놓인 SPI와 순서번호(Sequence Number)는 암호화 범위에서 제외된다. 따라서 제시된 필드 중 Payload Data, Padding, Next Header는 암호화 대상이고 SPI는 암호화 대상이 아니다.

SPI는 수신자가 패킷에 적용할 보안 연관(SA)을 식별하는 32비트 값이다. 보안 연관에는 해당 통신에 사용할 암호 알고리즘과 키 등의 보안 정보가 연결되어 있다. 수신자는 **SPI를 읽어 보안 연관을 찾은 뒤** 그 정보로 암호문을 복호화해야 하므로 SPI 자체는 평문으로 전송한다.

NoteBase

문 16. SSL 프로토콜에 대한 설명으로 옳지 않은 것은?

① 서버와 클라이언트 간 양방향 통신에 동일한 암호화 키를 사용한다.

② 웹 서비스 이외에 다른 응용 프로그램에도 적용할 수 있다.

③ 단편화, 압축, MAC 추가, 암호화, SSL 레코드 헤더 추가의 과정으로 이루어진다.

④ 암호화 기능을 사용하면 주고받는 데이터가 인터넷상에서 도청되는 위험성을 줄일 수 있다.

정답 1번

간단한 해설

SSL은 데이터를 대칭키로 암호화하지만, **클라이언트→서버와 서버→클라이언트의 암호화 키를 구분**한다. 한 방향의 암호화와 복호화에는 같은 키를 쓰되, 양방향 전체에 하나의 동일한 키를 쓰는 것은 아니다.

선지별 해설

① X: SSL은 **통신 방향별로 서로 다른 암호화 키**를 사용한다. 클라이언트가 보낼 때 쓰는 키는 서버가 해당 데이터를 복호화할 때 사용하고, 서버가 보낼 때는 별도의 키를 사용하여 클라이언트가 복호화한다. 대칭키 방식이라는 것은 각 방향에서 암호화 키와 복호화 키가 같다는 뜻이며, 양방향의 키까지 같다는 뜻은 아니다.

② O: SSL은 TCP와 같은 신뢰성 있는 전송 프로토콜 위에서 동작하며, **특정 응용 프로토콜에 종속되지 않는다**. 따라서 HTTP를 사용하는 웹 서비스뿐 아니라 다른 응용 프로그램의 통신도 보호할 수 있다.

③ O: SSL 레코드 프로토콜의 송신 처리는 **단편화 → 압축 → MAC 추가 → 암호화 → 레코드 헤더 추가**의 순서로 설명한다. 데이터를 적절한 크기로 나누고, 압축된 데이터에 변조 검출을 위한 MAC을 붙인 뒤 암호화한다. 마지막으로 레코드의 종류·버전·길이 등을 나타내는 헤더를 붙인다. 압축 방식으로 null이 선택되면 실제 압축으로 데이터가 바뀌지는 않는다.

④ O: 암호화는 전송할 평문을 암호문으로 바꾸어 **기밀성**을 제공한다. 제삼자가 전송 중인 데이터를 가로채더라도 적절한 키 없이는 내용을 알아보기 어렵게 하므로, 도청에 따른 정보 노출 위험을 줄인다.

NoteBase

문 17. KCMVP에 대한 설명으로 옳은 것은?

① 보안 기능을 만족하는 신뢰도 인증 기준으로 EAL1부터 EAL7까지의 등급이 있다.

② 암호 알고리즘이 구현된 프로그램 모듈의 안전성과 구현 적합성을 검증하는 제도이다.

③ 개인정보 보호활동을 체계적·지속적으로 수행하기 위한 관리체계의 구축과 이행 여부를 평가한다.

④ 조직의 정보자산을 효과적으로 보호하고 있는지 평가하여 일정 수준 이상의 기업에 인증을 부여한다.

정답 2번

간단한 해설

KCMVP는 **암호 알고리즘을 구현한 암호모듈의 안전성과 구현 적합성**을 검증하는 제도이다. 암호 기능이 정해진 요구사항에 맞게 구현되어 안전하게 동작하는지를 확인한다.

선지별 해설

① X: EAL1부터 EAL7까지의 등급은 **공통평가기준(CC)의 평가보증등급**이다. IT 제품의 보안성을 평가할 때 보증 수준을 구분하는 것으로, 암호모듈을 검증하는 KCMVP의 등급에 관한 설명이 아니다.

② O: KCMVP는 암호모듈 검증제도로, 암호 알고리즘을 구현한 모듈의 **안전성과 구현 적합성**을 검증한다. 구현 적합성은 암호 기능이 정해진 요구사항에 맞게 구현되었는지를 뜻하므로, 선지의 프로그램 모듈에 대한 설명이 이에 해당한다.

③ X: 개인정보 보호활동을 체계적·지속적으로 수행하기 위한 관리체계의 구축과 이행 여부를 평가하는 것은 **개인정보보호 관리체계 인증(PIMS)**에 관한 설명이다. KCMVP의 검증 대상은 이러한 조직의 개인정보보호 관리체계가 아니라 암호모듈이다.

④ X: 조직의 정보자산을 보호하기 위한 관리체계를 평가하여 인증하는 것은 **정보보호 관리체계 인증(ISMS)**에 관한 설명이다. 정보보호를 위한 관리체계가 수립·운영되고 인증기준에 적합한지를 살피는 제도로, 암호모듈의 안전성과 구현 적합성을 검증하는 KCMVP와 평가 대상이 다르다.

NoteBase

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

① 분쟁조정위원회는 위원장 1명을 포함한 20명 이내의 위원으로 구성한다.

② 위원장은 행정안전부·방송통신위원회·금융위원회 및 개인정보보호위원회의 고위공무원단에 속하는 일반직공무원 중에서 위촉한다.

③ 분쟁조정위원회는 재적위원 과반수의 출석으로 개의하며 출석위원 과반수의 찬성으로 의결한다.

④ 위원은 자격정지 이상의 형을 선고받거나 심신상의 장애로 직무를 수행할 수 없는 경우를 제외하고는 그의 의사에 반하여 면직되거나 해촉되지 아니한다.

정답 2번

간단한 해설

위원장은 **위원 중 공무원이 아닌 사람**으로 정한다. 따라서 고위공무원단에 속하는 현직 일반직공무원 중에서 위원장을 위촉한다는 설명은 위원장 자격에 어긋난다.

선지별 해설

① O: 구 「개인정보 보호법」 제40조제2항은 위원장 1명을 포함하여 **20명 이내**의 위원으로 구성하도록 정하였다. 위원장도 전체 정원에 포함되므로 별도로 더하는 것이 아니다. 이 문항은 개정 전 규정을 기준으로 하며, 개정 후에는 위원장 1명을 포함한 30명 이내로 확대되었다.

② X: 「개인정보 보호법」 제40조제4항에 따르면 위원장은 **위원 중 공무원이 아닌 사람**으로 정한다. 선지에 열거된 기관의 고위공무원단 소속 일반직공무원은 현직 공무원이므로 이 자격을 충족하지 못한다.
'고위공무원단에 속하는 일반직공무원 중에서'라는 부분을 '위원 중에서 공무원이 아닌 사람으로'로 고쳐야 한다.

③ O: 「개인정보 보호법」 제40조제7항에 따라 재적위원 과반수가 출석해야 회의를 열 수 있고, 출석위원 과반수가 찬성해야 의결할 수 있다. **개의는 재적위원, 의결은 출석위원**을 기준으로 한다는 차이를 구별해야 한다. 과반수는 해당 인원의 절반을 넘는 수이다.

④ O: 「개인정보 보호법」 제41조는 위원이 자격정지 이상의 형을 선고받거나 심신상의 장애로 직무를 수행할 수 없는 경우를 제외하고는 **본인의 의사에 반하는 면직·해촉을 금지**한다. 이는 위원이 외부의 압력 때문에 직위를 잃지 않고 독립적으로 분쟁조정 업무를 수행하도록 하는 신분보장 규정이다.

NoteBase

문 19. 전자화폐 및 가상화폐에 대한 설명으로 옳지 않은 것은?

① 전자화폐는 전자적 매체에 화폐의 가치를 저장한 후 물품 및 서비스 구매 시 활용하는 결제 수단이며, 가상화폐는 전자화폐의 일종으로 볼 수 있다.

② 전자화폐는 발행, 사용, 교환 등의 절차에 관하여 법률에서 규정하고 있으나, 가상화폐는 별도로 규정하고 있지 않다.

③ 가상화폐인 비트코인은 분산원장기술로 알려진 블록체인을 이용한다.

④ 가상화폐인 비트코인은 전자화폐와 마찬가지로 이중 지불(Double Spending)문제가 발생하지 않는다.

정답 4번

간단한 해설

이중 지불은 같은 자금을 두 번 사용하는 문제이다. 비트코인은 **블록체인과 작업증명 기반 합의로 이중 지불을 억제**하지만, 미확정 거래나 블록체인 재구성을 이용한 공격 위험까지 없어지는 것은 아니다.

NoteBase

선지별 해설

① O: 전자적 매체에 가치를 저장하여 재화·서비스의 지급에 사용하는 수단을 전자화폐라고 넓게 부르면, 가상화폐도 그 범주에 포함하여 설명할 수 있다. 이 문항은 이러한 **넓은 기술적 의미**를 사용한다. 비트코인이 현금·예금으로의 교환 보장 등 요건을 갖추어야 하는 「전자금융거래법」상 전자화폐에 해당한다는 뜻은 아니다.

② O: **출제 당시의 국내 제도**를 전제로 한 설명이다. 「전자금융거래법」 제16조는 전자화폐의 발행·사용·환금을 규정하지만, 당시에는 가상화폐를 직접 규율하는 별도의 법체계가 마련되지 않았다는 취지이다. 이를 현재도 가상화폐에 적용되는 법률이 전혀 없다는 뜻으로 일반화해서는 안 된다. 이후 가상자산사업자 신고제가 도입되었고, 2024년 7월 19일부터는 「가상자산 이용자 보호 등에 관한 법률」도 시행되었다.

③ O: 비트코인은 거래를 블록으로 묶고 앞선 블록의 해시값을 다음 블록에 포함하여 연결하는 **블록체인**을 사용한다. 여러 노드가 거래 기록을 보관·검증하므로, 단일 관리자가 원장을 독점적으로 관리하는 방식과 구별되는 분산원장기술에 해당한다.

④ X: 이중 지불은 동일한 자금을 서로 다른 거래에 중복하여 사용하는 문제이다. 중앙 관리 방식의 전자화폐는 관리기관이 사용 기록을 확인하여 중복 지급을 통제한다. 비트코인은 중앙기관 대신 작업증명과 합의 규칙으로 거래 이력을 정하고, 채택된 체인에서는 같은 자금을 중복 사용한 거래를 모두 유효한 것으로 인정하지 않는다. 그러나 미확정 거래를 성급히 지급 완료로 받아들이거나 공격으로 체인이 재구성되면, 수취인이 믿었던 지급이 뒤집힐 위험이 있다. 따라서 '이중 지불 문제가 발생하지 않는다'가 아니라 **'이중 지불 위험을 합의 절차와 후속 블록의 누적으로 억제한다'**로 고쳐야 한다.

NoteBase

문 20. X.509 인증서(버전 3)의 확장(Extensions) 영역에 포함되지 않는 항목은?

① 인증서 정책(Certificate Policies)

② 기관 키 식별자(Authority Key Identifier)

③ 키 용도(Key Usage)

④ 서명 알고리즘 식별자(Signature Algorithm Identifier)

정답 4번

간단한 해설

서명 알고리즘 식별자는 인증기관이 인증서에 서명할 때 사용한 알고리즘을 나타내는 **기본 인증서 필드**이다. 버전 3에서 추가된 확장 영역에 속하지 않는다.

공통 해설

X.509 버전 3의 확장 영역은 기본 필드에 더하여 인증서의 정책이나 키 관련 정보 등을 담는 영역이다. 인증서 정책(Certificate Policies), 기관 키 식별자(Authority Key Identifier), 키 용도(Key Usage)는 모두 이 **표준 확장 항목**에 속한다. 이들은 확장 영역 안에 정의된 항목으로 저장된다.

서명 알고리즘 식별자(Signature Algorithm Identifier)는 인증기관이 해당 인증서에 전자서명할 때 사용한 알고리즘을 알려 주는 **기본 필드**이다. 인증서의 서명을 검증하는 데 필요한 정보로, 버전 3의 확장 영역 밖에 별도로 정의되어 있다. 따라서 확장 영역에 포함되지 않는 항목에 해당한다.

NoteBase