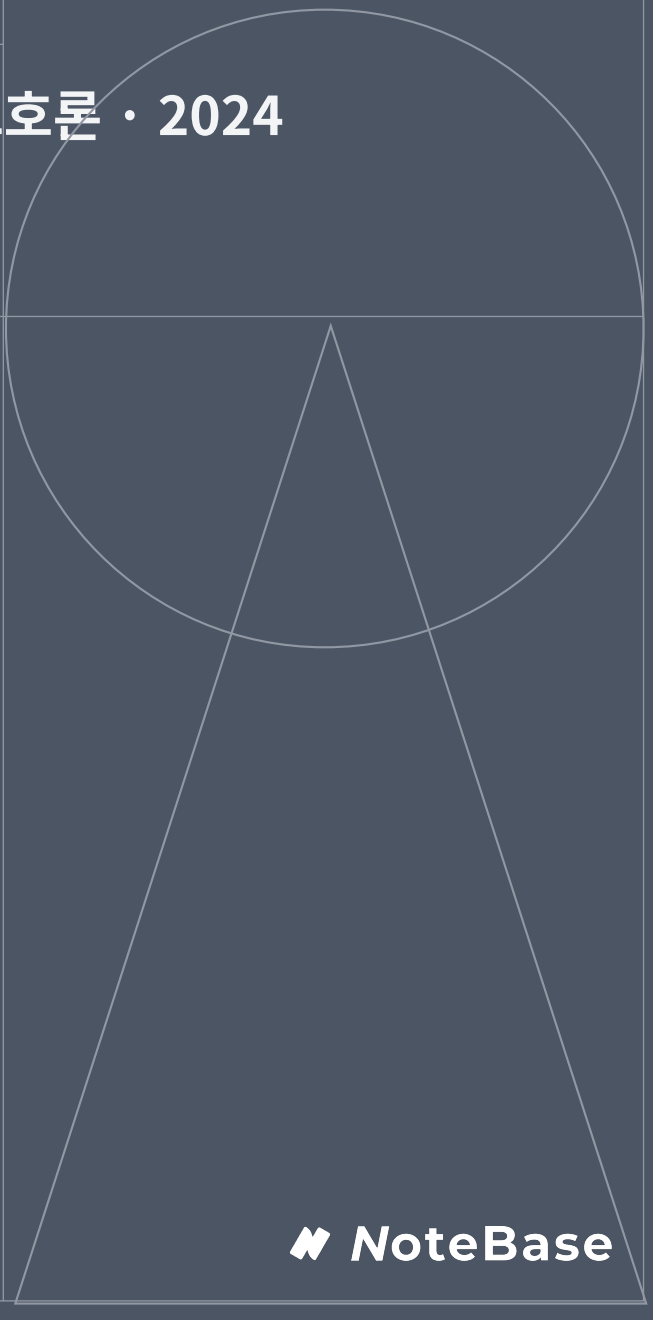
기출OX 해설집

공무원/국가직/9급 · 정보보호론 · 2024



NoteBase

기출OX 해설집

공무원/국가직/9급 · 정보보호론 · 2024

공무원/국가직/9급 · 정보보호론 · 2024

문 1. 사용자 A가 사용자 B에게 보낼 메시지에 대한 전자서명을 생성하는 데 필요한 키는?

① 사용자 A의 개인키

② 사용자 A의 공개키

③ 사용자 B의 개인키

④ 사용자 B의 공개키

정답 1번

간단한 해설

전자서명은 **서명자 A의 개인키**로 생성하고, 이에 대응하는 A의 공개키로 검증한다.

핵심 풀이

전자서명은 메시지의 작성자와 메시지의 변조 여부를 확인하는 데 쓰인다. 이 문제에서 서명자는 메시지를 보내는 A이므로 **A의 개인키로 서명을 생성**한다. 개인키는 서명자가 비밀로 관리하는 키이다. 수신자 B는 A의 개인키가 아니라, 그와 쌍을 이루는 A의 공개키로 메시지와 서명을 검증한다.

메시지의 내용을 B만 읽을 수 있게 하는 공개키 암호화와 구분해야 한다. 이때는 **B의 공개키로 암호화**하고 B의 개인키로 복호화한다. 전자서명 생성에서는 누가 받는지가 아니라 누가 서명하는지가 키 선택의 기준이다.

NoteBase

문 2. 원본 파일에 숨기고자 하는 정보를 삽입하고 숨겨진 정보의 존재 여부를 알기 어렵게 하는 기술은?

① 퍼징(Fuzzing)

② 스캐닝(Scanning)

③ 크립토그래피(Cryptography)

④ 스테가노그래피(Steganography)

정답 4번

간단한 해설

원본 파일에 정보를 삽입하여 **숨겨진 정보의 존재 자체를 알아차리기 어렵게 하는** 기술이 스테가노그래피이다. 정보의 내용을 해독하기 어렵게 하는 암호화와 구별된다.

공통 해설

스테가노그래피(Steganography)는 이미지·음성 등의 파일에 비밀 정보를 삽입하여, 겉으로는 평범한 파일처럼 보이게 함으로써 **비밀 정보가 들어 있다는 사실을 숨기는** 기술이다. 예를 들어 사진 파일에 메시지를 넣되 사진을 보는 사람이 메시지의 존재를 알아차리기 어렵게 하는 방식이다. 문제의 '원본 파일에 정보를 삽입'하고 '존재 여부를 알기 어렵게 한다'는 조건이 이 정의에 해당한다.

크립토그래피(Cryptography)의 암호화는 정보를 변환하여 권한 없는 사람이 **내용을 해독하기 어렵게 하는** 방식이다. 암호문이 있다는 사실까지 숨기는 것은 아니므로, 이 문제에서는 내용의 해독 방지와 정보의 존재 은닉을 구별해야 한다.

NoteBase

문 3. 다음에서 설명하는 공격 방법은?

◯ 사람의 심리를 이용하여 보안 기술을 무력화시키고 정보를 얻는 공격 방법
◯ 신뢰할 수 있는 사람으로 위장하여 다른 사람의 정보에 접근하는 공격 방법

① 재전송 공격(Replay Attack)
② 무차별 대입 공격(Brute-Force Attack)
③ 사회공학 공격(Social Engineering Attack)
④ 중간자 공격(Man-in-the-Middle Attack)

정답 3번

간단한 해설

사람의 **심리와 신뢰를 악용**하여 정보를 얻는 방식은 사회공학 공격이다. 신뢰할 수 있는 사람으로 위장하는 것은 상대방이 경계심을 풀고 정보를 제공하도록 유도하는 수단이다.

공통 해설

사회공학 공격은 **사람의 판단과 행동을 조종**하여 정보를 얻거나 보안 절차를 우회하도록 유도하는 공격이다.
지문의 '사람의 심리를 이용'한다는 설명은 공격이 이용하는 취약점을, '신뢰할 수 있는 사람으로 위장'한다는 설명은 상대방의 경계심을 낮추는 수법을 나타낸다. 두 설명 모두 사람을 속여 정보에 접근하는 사회공학 공격의 특징에 해당한다.

예를 들어 공격자가 전산 담당자로 위장하여 계정 점검을 이유로 비밀번호를 알려 달라고 요구할 수 있다.
상대방이 이를 믿고 비밀번호를 제공하면, 공격자는 암호를 직접 해독하지 않고도 정보를 얻는다. 이처럼 사람이 믿고 협조하도록 만드는 과정이 핵심이다.

NoteBase

문 4. 블록 암호의 운영 모드 중 ECB 모드와 CBC 모드에 대한 설명으로 옳은 것은?

① ECB 모드는 블록의 변화가 다른 블록에 영향을 주지 않아 안전하다.

② ECB 모드는 암호화할 때, 같은 데이터 블록에 대해 같은 암호문 블록을 생성한다.

③ CBC 모드는 블록의 변화가 이전 블록에 영향을 주므로 패턴을 추적하기 어렵다.

④ CBC 모드는 암호화할 때, 이전 블록의 결과가 필요하지 않다.

정답 2번

간단한 해설

ECB 모드는 **같은 키로 같은 평문 블록을 암호화하면 같은 암호문 블록**을 생성한다. 각 블록을 독립적으로 처리하므로 다른 블록의 내용이나 처리 결과가 암호화에 반영되지 않는다.

선지별 해설

① X: ECB 모드는 각 블록을 독립적으로 암호화하므로 한 평문 블록이 바뀌어도 다른 블록의 암호화 결과에는 영향을 주지 않는다. 그러나 이러한 독립성이 안전성을 보장하지는 않는다. 같은 키에서 반복되는 평문 블록은 같은 암호문 블록으로 나타나므로 **평문의 반복 패턴이 노출될 수 있다**.

② O: ECB 모드는 같은 키를 사용하여 각 평문 블록에 동일한 블록 암호 연산을 적용한다. 따라서 **같은 평문 블록은 같은 암호문 블록**이 된다. 예를 들어 평문 블록이 A, B, A 순서라면 첫 번째와 세 번째 암호문 블록도 서로 같아 반복 관계가 드러난다.

③ X: CBC 암호화에서는 현재 평문 블록에 직전 암호문 블록을 결합하므로 블록 사이에 의존 관계가 생긴다. 한 평문 블록의 변화는 **해당 블록과 이후 블록의 암호화 결과**에 영향을 주며, 이미 처리한 이전 블록에는 영향을 주지 않는다. 이 연결 때문에 같은 평문 블록도 직전 암호문 블록이 다르면 다른 암호문 블록으로 암호화되어 반복 패턴이 감춰진다.

④ X: CBC 모드는 현재 평문 블록을 **직전 암호문 블록과 배타적 논리합(XOR)**한 뒤 암호화한다. 따라서 두 번째 블록부터는 이전 블록의 암호화 결과가 필요하다. 첫 번째 블록은 직전 암호문 블록이 없으므로 초기화 벡터(IV)와 XOR한 뒤 암호화한다.

NoteBase

문 5. 컴퓨터 보안의 3요소가 아닌 것은?

① 무결성(Integrity)

② 확장성(Scalability)

③ 가용성(Availability)

④ 기밀성(Confidentiality)

정답 2번

간단한 해설

확장성은 **사용자 수나 처리량 증가에 대응하여 시스템의 처리 능력을 확대하는 성질**이다. 컴퓨터 보안의 3요소는 기밀성·무결성·가용성이다.

개념 구분

컴퓨터 보안의 3요소는 기밀성·무결성·가용성이다. 기밀성은 인가되지 않은 사람에게 정보가 공개되지 않도록 하는 성질이고, 무결성은 정보가 허가 없이 변경되거나 훼손되지 않도록 하는 성질이다. 가용성은 인가된 사용자가 **필요할 때 정보나 서비스를 이용할 수 있도록 하는 성질**이다.

확장성은 사용자 수나 처리량이 늘어날 때 시스템의 처리 능력을 확대하여 대응할 수 있는 성질이다. 가용성이 필요한 시점의 이용 가능성을 뜻한다면, 확장성은 **증가하는 부하에 대응하는 능력**을 뜻하므로 컴퓨터 보안의 3요소에 포함되지 않는다.

NoteBase

문 6. 로컬에서 통신하고 있는 서버와 클라이언트의 IP 주소에 대한 MAC 주소를 공격자의 MAC 주소로 속여, 클라이언트와 서버 간에 이동하는 패킷이 공격자로 전송되도록 하는 공격 기법은?

① SYN 플러딩

② DNS 스푸핑

③ ARP 스푸핑

④ ICMP 리다이렉트 공격

정답 3번

간단한 해설

IP 주소에 대응하는 MAC 주소를 공격자의 것으로 위조하는 것은 ARP 스푸핑이다. 상대방에게 보낼 패킷을 공격자의 MAC 주소로 전송하게 만들어 통신을 가로챈다.

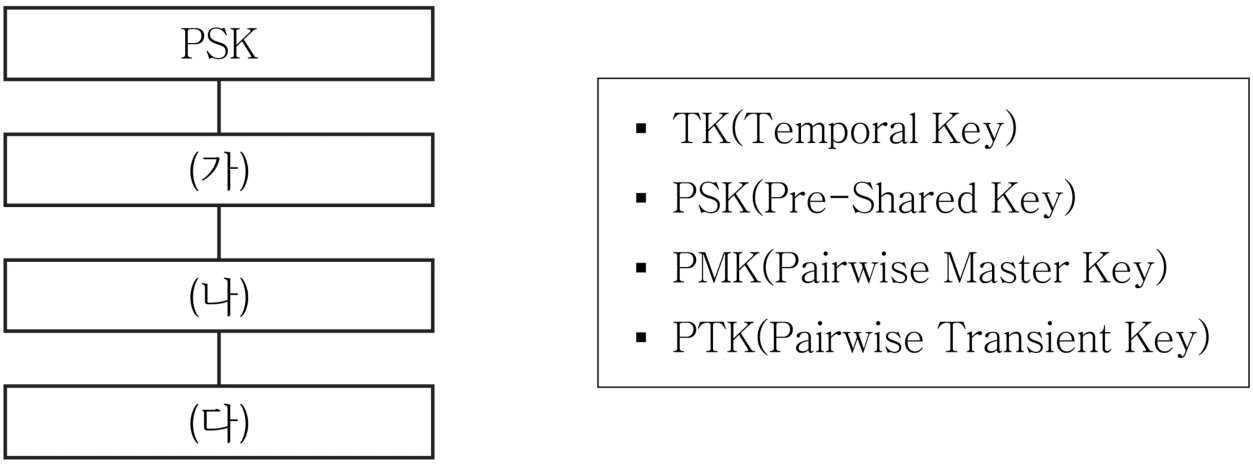
공통 해설

ARP는 로컬 네트워크에서 IPv4 주소에 대응하는 MAC 주소를 알아내는 프로토콜이다. 호스트는 이 대응 정보를 ARP 캐시에 저장하고, 같은 로컬 네트워크의 상대방에게 데이터를 보낼 때 목적지 MAC 주소를 정하는 데 사용한다.

ARP 스푸핑은 **거짓 ARP 정보로 IP 주소와 MAC 주소의 대응 관계를 바꾸는** 공격이다. 문제에서는 클라이언트가 서버의 IP 주소를 공격자의 MAC 주소에 대응시키고, 서버도 클라이언트의 IP 주소를 공격자의 MAC 주소에 대응시키도록 속인다. 그 결과 패킷의 목적지 IP 주소가 원래 상대방의 것이어도, 이를 담은 프레임의 목적지 MAC 주소는 공격자의 것이 되어 양쪽에서 보내는 패킷이 공격자에게 전달된다.

NoteBase

문 7. IEEE 802.11i 키 관리의 쌍별 키 계층을 바르게 나열한 것은?



① (가): PMK, (나): TK, (다): PTK

② (가): PMK, (나): PTK, (다): TK

③ (가): PTK, (나): TK, (다): PMK

④ (가): PTK, (나): PMK, (다): TK

정답 2번

간단한 해설

PMK는 **PTK를 생성하는 기준 키**이고, TK는 **PTK에 포함되어 사용자 데이터를 보호하는 키**이다. 따라서 실제 데이터 보호에 쓰는 TK가 이를 포함하는 PTK보다 아래 계층에 놓인다.

NoteBase

올바른 순서

PSK → (가) PMK → (나) PTK → (다) TK

PSK: 사전 공유 키로, 무선 단말과 액세스 포인트(AP)가 미리 공유하는 비밀 키이다. 그림에서는 이 키를 출발점으로 쌍별 키 계층을 구성한다.

(가) PMK(Pairwise Master Key): 쌍별 마스터 키로, 하위 키를 생성하는 기준이 된다. 사전 공유 키 방식에서는 **PSK를 PMK로 사용한다**. 따라서 PSK 다음 칸은 PMK이며, 별도의 새 키 값을 반드시 생성한다는 뜻은 아니다.

(나) PTK(Pairwise Transient Key): 4단계 핸드셰이크 과정에서 PMK와 양측의 MAC 주소, 각자가 만든 난수인 nonce를 이용해 생성하는 쌍별 일시 키이다. **PMK를 바탕으로 생성**되므로 PMK보다 아래 계층에 놓인다.

(다) TK(Temporal Key): **PTK를 구성하는 키 중 하나**로, 단말과 AP 사이의 유니캐스트 사용자 데이터를 암호화하는 데 사용한다. PTK에서 데이터 보호에 필요한 부분을 취하므로 그림의 마지막 칸에 놓인다.

NoteBase

문 8. CC(Common Criteria)의 보증 요구사항(Assurance Requirements)에 해당하는 것은?

① 개발

② 암호 지원

③ 식별과 인증

④ 사용자 데이터 보호

정답 1번

간단한 해설

CC의 '개발(ADV)'은 설계·구현 자료를 근거로 보안기능이 올바르게 구현되었는지 확인하는 **보증 요구사항**에 속한다.

개념 구분

보증 요구사항: 제품의 보안기능이 요구된 대로 구현되었다는 신뢰를 얻기 위해 필요한 증거와 평가 활동을 규정한다. **개발(ADV)**은 여기에 속하며, 보안기능의 명세·설계·구현에 관한 자료를 통해 요구된 보안기능이 제품에 어떻게 구현되어 있는지 평가할 수 있게 한다.

기능 요구사항: 제품이 **어떤 보안 동작을 수행해야 하는지**를 규정한다. 암호 지원(FCS)은 암호키 관리와 암호 연산, 식별과 인증(FIA)은 사용자 식별과 신원 확인, 사용자 데이터 보호(FDP)는 접근통제 등 사용자 데이터를 보호하는 기능에 관한 요구사항이다. 이들은 보안기능의 구현을 뒷받침하는 평가 증거에 관한 '개발'과 구별된다.

NoteBase

문 9. 다음 /etc/passwd 파일 내용에 대한 설명으로 옳지 않은 것은?

root : x : 0 : 0 : root : /root : /bin/bash
㉠ ㉡ ㉢ ㉣

① ㉠은 사용자 ID이다.

② ㉡은 UID 정보이다.

③ ㉢은 사용자 홈 디렉터리 경로이다.

④ ㉣은 패스워드가 암호화되어 /bin/bash 경로에 저장되어 있음을 의미한다.

정답 4번

간단한 해설

㉣의 /bin/bash는 **로그인 셸의 실행 파일 경로**이다. 패스워드 저장 위치를 뜻하지 않으며, 두 번째 필드의 x가 패스워드 해시를 /etc/shadow에서 관리함을 나타낸다.

선지별 해설

/etc/passwd의 각 행은 한 계정의 정보를 담으며, 콜론(:)으로 필드를 구분한다. 그림의 밑줄 친 값은 필드의 위치에 따라 의미가 달라진다.

① O: ㉠의 root는 첫 번째 필드에 있는 **사용자 계정명**으로, 로그인할 때 사용하는 사용자 ID이다. 숫자로 사용자를 식별하는 UID와 구별한다.

② O: ㉡의 0은 세 번째 필드에 있는 **UID**이다. UID는 운영체제가 사용자를 식별하는 숫자이며, UID 0은 슈퍼유저 권한을 나타낸다. 바로 뒤의 네 번째 필드에 있는 0은 기본 그룹을 식별하는 GID이다.

③ O: ㉢의 /root는 여섯 번째 필드에 있는 **홈 디렉터리 경로**이다. 이 계정의 개인 파일과 설정 등을 두는 기본 디렉터리를 지정한다. 첫 번째 필드의 계정명 root와 달리 /root는 파일 시스템상의 경로이다.

④ X: ㉣의 /bin/bash는 일곱 번째 필드에 있는 **로그인 셸의 실행 파일 경로**로, 이 계정이 로그인할 때 사용할 명령 해석기가 Bash임을 나타낸다. 패스워드가 이 경로에 저장된다는 설명은 잘못이다. 패스워드 관련 표시는 두 번째 필드의 x이며, 이는 패스워드 해시를 별도 파일인 /etc/shadow에서 관리함을 뜻한다.

NoteBase

문 10. 리눅스에서 설정된 umask 값이 027일 때, 생성된 디렉터리의 기본 접근 권한으로 옳은 것은?

① drw-r-----

② d---r--rw-

③ drwxr-x---

④ d---r-xrwx

정답 3번

간단한 해설

umask는 새로 부여할 권한이 아니라 **제거할 권한**을 지정한다. 디렉터리의 기준 권한 777에서 027에 해당하는 권한을 제거하면 750이 되어, 접근 권한은 drwxr-x---로 표시된다.

계산 과정

디렉터리를 생성할 때의 기준 권한은 8진수 777이다. 각 자리는 차례로 소유자·그룹·기타 사용자의 권한을 나타내며, 읽기 r은 4, 쓰기 w는 2, 실행 x는 1로 표현한다. 따라서 각 자리의 7은 rwx를 모두 허용한다는 뜻이다. umask 027은 이 기준에서 **제거할 권한 비트**를 지정한다.

소유자: umask의 첫 자리가 0이므로 제거할 권한이 없다. 7 − 0 = 7이므로 rwx가 유지된다.

그룹: umask의 둘째 자리가 2이므로 **쓰기 권한 w만 제거**한다. 7 − 2 = 5이며, 5는 읽기 4와 실행 1의 합이므로 r-x가 된다.

기타 사용자: umask의 셋째 자리가 7이므로 읽기·쓰기·실행 권한을 모두 제거한다. 7 − 7 = 0이므로 ---가 된다. 이 자리별 뺄셈은 기준 권한 777에 모든 권한 비트가 들어 있으므로 사용할 수 있다.

남은 권한을 순서대로 합치면 8진수 750, 즉 rwxr-x---이다. 맨 앞에 디렉터리를 뜻하는 d를 붙이면 drwxr-x---가 되어 ③과 일치한다.

NoteBase

문 11. 역공학을 위해 로우레벨 언어에서 하이레벨 언어로 변환할 목적을 가진 도구는?

① 디버거(Debugger)

② 디컴파일러(Decompiler)

③ 패커(Packer)

④ 어셈블러(Assembler)

정답 2번

간단한 해설

저수준 코드로부터 고수준 언어 형태의 코드를 재구성하는 작업이 **디컴파일**이며, 이를 수행하는 도구가 디컴파일러이다.

공통 해설

디컴파일러(Decompiler)는 기계어 등 저수준 표현으로 된 프로그램을 분석하여 **고수준 언어의 코드 형태로 재구성**하는 도구이다. 예를 들어 기계 명령의 연산과 분기 흐름을 분석하여 C 언어의 변수·조건문·반복문과 같은 구조로 나타낸다. 이렇게 얻은 코드는 역공학에서 프로그램의 동작을 이해하는 데 쓰인다.

문제에서 요구하는 '로우레벨 언어에서 하이레벨 언어로'의 변환은 이러한 디컴파일에 해당한다. 후보를 구별하는 기준은 저수준 프로그램을 고수준 코드로 재구성하는 기능이며, 이 목적에 대응하는 도구가 디컴파일러이다.

NoteBase

문 12. 위험 평가 방법에 대한 설명으로 옳지 않은 것은?

① 정성적 위험 평가는 자산에 대한 화폐가치 식별이 어려운 경우 이용한다.

② 정량적 분석법에는 델파이법, 시나리오법, 순위결정법, 브레인스토밍 등이 있다.

③ 정성적 분석법은 위험 평가 과정과 측정기준이 주관적이어서 사람에 따라 결과가 달라질 수 있다.

④ 정량적 위험 평가 방법에 의하면 연간 기대 손실은 위협이 성공했을 경우의 예상 손실액에 그 위협의 연간 발생률을 곱한 값이다.

정답 2번

간단한 해설

델파이법·시나리오법·순위결정법·브레인스토밍은 **정성적 분석법**에 속한다. 손실액과 발생률을 수량으로 산정하는 정량적 분석과 달리, 전문가의 의견이나 상대적 중요도 등의 판단을 이용한다.

선지별 해설

① O: 정성적 위험 평가는 위험을 '높음·보통·낮음' 등의 등급이나 상대적 중요도로 표현한다. 따라서 평판이나 신뢰처럼 **자산의 가치를 화폐로 환산하기 어려운 경우**에도 위험을 평가할 수 있다.

② X: 나열된 기법은 정량적 분석법이 아니라 **정성적 분석법**이다. 델파이법은 전문가의 의견을 반복적으로 수렴하고, 시나리오법은 가능한 사건의 전개와 영향을 예상한다. 순위결정법은 위험의 상대적 중요도를 비교하여 순위를 정하며, 브레인스토밍은 참여자들이 자유롭게 의견을 제시하여 위험 요인을 도출한다. 이들은 손실액과 발생률을 직접 수량화하기보다 의견과 판단을 활용한다.

③ O: 정성적 분석에서는 위험의 크기와 등급을 정할 때 평가자의 경험이나 판단이 개입한다. 같은 위험도 어떤 영향을 중요하게 보는지에 따라 등급이 달라질 수 있으므로, **평가자에 따라 결과가 달라질 수 있다**. 공통 평가기준을 마련하면 이런 차이를 줄일 수 있다.

④ O: 정량적 위험 평가에서 연간 기대 손실(ALE)은 **1회 발생 시 예상 손실액(SLE) × 연간 발생률(ARO)**로 구한다. 여기서 연간 발생률은 해당 손실 사건이 1년 동안 발생할 것으로 예상되는 횟수이다. 한 번의 손실액에 연간 예상 횟수를 곱하면 1년 동안의 평균적인 예상 손실액이 된다.

NoteBase

문 13. 「개인정보 보호법」 제30조(개인정보 처리방침의 수립 및 공개)에 따라 개인정보처리자가 정해야 하는 '개인정보 처리방침'에 포함되는 사항이 아닌 것은?

① 개인정보의 처리 목적

② 개인정보의 처리 및 보유 기간

③ 정보주체와 법정대리인의 권리·의무 및 그 행사방법에 관한 사항

④ 개인정보처리자의 성명 또는 개인정보를 활용하는 부서의 명칭과 전화번호 등 연락처

정답 4번

①

개인정보 처리방침에는 개인정보를 **어떤 목적으로 처리하는지**를 포함하여야 한다.

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

개인정보 처리방침에는 **개인정보의 처리 및 보유 기간**을 포함하여야 한다.

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>
2. 개인정보의 처리 및 보유 기간

③

개인정보 처리방침에는 **정보주체와 법정대리인의 권리·의무 및 그 행사방법**을 포함하여야 한다.

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>
5. 정보주체와 법정대리인의 권리 · 의무 및 그 행사방법에 관한 사항

NoteBase

④

기재 대상은 **개인정보 보호책임자의 성명** 또는 **개인정보 보호업무 및 관련 고충사항을 처리하는 부서의 명칭과 전화번호 등 연락처**이다. 개인정보처리자나 개인정보를 활용하는 부서를 뜻하지 않는다.

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>
6. 제31조에 따른 개인정보 보호책임자의 성명 또는 개인정보 보호업무 및 관련 고충사항을 처리하는 부서의 명칭과 전화번호 등 연락처

NoteBase

문 14. 「개인정보 보호법」 제4조(정보주체의 권리)에 따른 정보주체의 권리가 아닌 것은?

① 개인정보의 처리에 관한 정보를 제공받을 권리
② 개인정보의 처리 정지, 정정·삭제 및 파기를 요구할 권리
③ 개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리
④ 완전히 자동화된 개인정보 처리에 따른 결정을 승인하거나 그에 대한 회복 등을 요구할 권리

정답 4번

①

정보주체는 자신의 개인정보가 어떻게 처리되는지에 관한 **정보를 제공받을 권리**를 가진다.

개인정보 보호법 제4조(정보주체의 권리) 정보주체는 자신의 개인정보 처리와 관련하여 다음 각 호의 권리를 가진다. <개정 2023.3.14>
1. 개인정보의 처리에 관한 정보를 제공받을 권리

②

정보주체는 자신의 개인정보에 대해 **처리 정지, 정정·삭제 및 파기**를 요구할 권리를 가진다.

개인정보 보호법 제4조(정보주체의 권리) 정보주체는 자신의 개인정보 처리와 관련하여 다음 각 호의 권리를 가진다. <개정 2023.3.14>
4. 개인정보의 처리 정지, 정정 · 삭제 및 파기를 요구할 권리

③

개인정보 처리로 피해를 입은 정보주체는 **신속하고 공정한 절차에 따라 구제받을 권리**를 가진다.

개인정보 보호법 제4조(정보주체의 권리) 정보주체는 자신의 개인정보 처리와 관련하여 다음 각 호의 권리를 가진다. <개정 2023.3.14>
5. 개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리

NoteBase

④

완전히 자동화된 개인정보 처리에 따른 결정에 대해서는 **거부하거나 설명 등을 요구할 권리**가 인정된다. 선지의 '승인'과 '회복'은 규정된 권리의 내용과 다르다.

개인정보 보호법 제4조(정보주체의 권리) 정보주체는 자신의 개인정보 처리와 관련하여 다음 각 호의 권리를 가진다. <개정 2023.3.14>
6. 완전히 자동화된 개인정보 처리에 따른 결정을 거부하거나 그에 대한 설명 등을 요구할 권리

NoteBase

문 15. 증거물의 “획득 → 이송 → 분석 → 보관 → 법정 제출” 과정에 대한 추적성을 보장하기 위하여 준수해야 하는 원칙은?

① 연계 보관성의 원칙

② 정당성의 원칙

③ 재현의 원칙

④ 무결성의 원칙

정답 1번

간단한 해설

증거물을 누가 언제 인수하고 어떻게 처리했는지 전 과정을 끊김 없이 기록하여 추적할 수 있게 하는 것이 **연계 보관성의 원칙**이다.

공통 해설

연계 보관성(chain of custody)의 원칙은 증거물을 획득한 때부터 법정에 제출할 때까지 **보관·이동·처리 이력이 끊김 없이 이어지도록** 관리하는 원칙이다. 각 단계에서 증거물을 취급한 사람, 인계·인수 시점, 처리 내용 등을 기록하여 누가 언제 어떤 상태로 증거물을 넘겨받아 처리했는지 확인할 수 있어야 한다. 문제의 '획득 → 이송 → 분석 → 보관 → 법정 제출'은 이러한 관리 이력을 추적해야 하는 전 과정이므로, 이를 보장하는 원칙은 연계 보관성이다.

NoteBase

문 16. 128비트 키를 이용한 AES 알고리즘 연산 수행에 필요한 내부 라운드 수는?

① 10

② 12

③ 14

④ 16

정답 1번

간단한 해설

AES는 키 길이가 **128비트일 때 10라운드**를 수행하도록 정해져 있다.

핵심 풀이

AES의 라운드는 데이터를 암호화하기 위한 변환을 반복하는 단위이며, 라운드 수는 **키 길이**에 따라 정해진다. 128비트 키는 10라운드, 192비트 키는 12라운드, 256비트 키는 14라운드를 수행한다. 따라서 주어진 128비트 키에 대응하는 내부 라운드 수는 10이다.

AES의 블록 크기는 키 길이와 관계없이 **항상 128비트**이다. 블록 크기는 한 번에 처리하는 데이터의 크기이고, 이 문제에서 라운드 수를 결정하는 조건은 키 길이 128비트이다.

NoteBase

문 17. SSL에서 기밀성과 메시지 무결성을 제공하기 위해 단편화, 압축, MAC 첨부, 암호화를 수행하는 프로토콜은?

① 경고 프로토콜

② 레코드 프로토콜

③ 핸드셰이크 프로토콜

④ 암호 명세 변경 프로토콜

정답 2번

간단한 해설

SSL에서 **단편화·압축·MAC 첨부·암호화**는 레코드 프로토콜의 데이터 보호 처리이다. MAC은 메시지 변조를 검출하고, 암호화는 메시지 내용의 노출을 막는다.

공통 해설

SSL 레코드 프로토콜은 상위 계층에서 받은 데이터를 레코드 단위로 가공하여 보호하는 프로토콜이다. 데이터를 처리 가능한 크기로 나누는 단편화, 데이터 크기를 줄이는 압축, MAC 첨부, 암호화를 담당한다. 압축은 합의된 압축 방식에 따라 수행하며, 압축하지 않는 방식이 선택될 수도 있다.

MAC(메시지 인증 코드)은 공유 비밀값을 이용하여 계산한 값으로, 수신 측이 이를 검증하여 전송 중 메시지가 변조되었는지 확인한다. 암호화는 키가 없는 제삼자가 메시지 내용을 읽지 못하게 한다. 즉, **MAC으로 메시지 무결성을, 암호화로 기밀성을 제공**하는 레코드 계층의 처리라는 점이 제시된 기능 묶음을 식별하는 기준이다.

NoteBase

문 18. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제45조(정보통신망의 안정성 확보 등)에서 정보보호지침에 포함되어야 하는 사항으로 명시적으로 규정한 것이 아닌 것은?

① 정보통신망연결기기등의 정보보호를 위한 물리적 보호조치
② 정보의 불법 유출·위조·변조·삭제 등을 방지하기 위한 기술적 보호조치
③ 정보통신망의 지속적인 이용이 가능한 상태를 확보하기 위한 기술적·물리적 보호조치
④ 정보통신망의 안정 및 정보보호를 위한 인력·조직·경비의 확보 및 관련 계획수립 등 관리적 보호조치

정답 1번

①

정보보호지침에 명시된 정보통신망연결기기등의 정보보호조치는 **기술적 보호조치**이다. 선지는 이를 물리적 보호조치로 바꾸었다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제45조(정보통신망의 안정성 확보 등)
③ 정보보호지침에는 다음 각 호의 사항이 포함되어야 한다. <개정 2016.3.22, 2020.6.9>
5. 정보통신망연결기기등의 정보보호를 위한 기술적 보호조치

②

정보보호지침에는 **정보의 불법 유출·위조·변조·삭제 등을 방지하기 위한 기술적 보호조치**가 포함되어야 한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제45조(정보통신망의 안정성 확보 등)
③ 정보보호지침에는 다음 각 호의 사항이 포함되어야 한다. <개정 2016.3.22, 2020.6.9>
2. 정보의 불법 유출 · 위조 · 변조 · 삭제 등을 방지하기 위한 기술적 보호조치

③

정보보호지침에는 **정보통신망의 지속적인 이용을 확보하기 위한 기술적·물리적 보호조치**가 포함되어야 한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제45조(정보통신망의 안정성 확보 등)
③ 정보보호지침에는 다음 각 호의 사항이 포함되어야 한다. <개정 2016.3.22, 2020.6.9>
3. 정보통신망의 지속적인 이용이 가능한 상태를 확보하기 위한 기술적 · 물리적 보호조치

NoteBase

④

정보보호지침에는 정보통신망의 안정 및 정보보호를 위한 **인력·조직·경비의 확보와 관련 계획수립 등 관리적 보호조치**가 포함되어야 한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제45조(정보통신망의 안정성 확보 등)
③ 정보보호지침에는 다음 각 호의 사항이 포함되어야 한다. <개정 2016.3.22, 2020.6.9>
4. 정보통신망의 안정 및 정보보호를 위한 인력 · 조직 · 경비의 확보 및 관련 계획수립 등 관리적 보호조치

NoteBase

문 19. 다음에서 설명하는 ISMS-P의 단계는?

◯ 조직의 업무특성에 따라 정보자산 분류기준을 수립하여 관리체계 범위 내 모든 정보자산을 식별·분류하고, 중요도를 산정한 후 그 목록을 최신으로 관리하여야 한다.
◯ 관리체계 전 영역에 대한 정보서비스 및 개인정보 처리 현황을 분석하고 업무 절차와 흐름을 파악하여 문서화하며, 이를 주기적으로 검토하여 최신성을 유지하여야 한다.
◯ 위험 평가 결과에 따라 식별된 위험을 처리하기 위하여 조직에 적합한 보호대책을 선정하고, 보호대책의 우선순위와 일정·담당자·예산 등을 포함한 이행계획을 수립하여 경영진의 승인을 받아야 한다.

① 위험 관리
② 관리체계 운영
③ 관리체계 기반 마련
④ 관리체계 점검 및 개선

정답 1번

간단한 해설

정보자산과 업무 흐름을 파악하고, 위험 평가 결과에 따라 보호대책과 이행계획을 정하는 활동은 **위험 관리**에 속한다. 대책을 선정하고 계획하는 것과 선정한 대책을 실제로 구현하는 것을 구분해야 한다.

구성 요소별 해설

첫 번째 ◯ — 정보자산 식별(1.2.1): 업무특성에 맞는 분류기준을 정하고 관리체계 범위 내 모든 정보자산을 식별·분류하여 중요도를 산정한다. 그 목록은 최신으로 유지해야 한다. 이는 **무엇을 보호해야 하며 얼마나 중요한지** 파악하여 위험 평가의 기초를 마련하는 활동이다.

두 번째 ◯ — 현황 및 흐름분석(1.2.2): 관리체계 전 영역의 정보서비스와 개인정보 처리 현황, 업무 절차와 흐름을 분석하여 문서화한다. 이를 주기적으로 검토하고 최신성을 유지해야 한다. 자산 목록만으로 알기 어려운 **정보의 처리 과정과 이동 경로**를 파악하여 위험을 찾아낼 근거를 마련한다.

세 번째 ◯ — 보호대책 선정(1.2.4): 위험 평가에서 식별된 위험을 처리할 수 있도록 조직에 적합한 보호대책을 선정한다. 우선순위·일정·담당자·예산 등을 포함한 이행계획을 수립하고 경영진의 승인을 받아야 한다. 이 항목은 **대책을 선정하고 실행을 계획하는 활동**이다. 선정한 대책을 이행계획에 따라 실제로 구현하는 것은 '관리체계 운영'의 보호대책 구현(1.3.1)에 해당한다.

세 구성 요소는 모두 ISMS-P 인증기준의 '1.2. 위험 관리'에 속하므로 ①의 위험 관리에 대응한다.

NoteBase

문 20. 디지털 콘텐츠의 불법 복제와 유포를 막고 저작권 보유자의 이익과 권리를 보호해 주는 기술은?

① PGP(Pretty Good Privacy)

② IDS(Intrusion Detection System)

③ DRM(Digital Rights Management)

④ PIMS(Personal Information Management System)

정답 3번

간단한 해설

디지털 콘텐츠의 이용과 복제를 허용된 범위로 제한하여 저작권자의 권리를 보호하는 기술이 **DRM(디지털 저작권 관리)**이다.

공통 해설

DRM(Digital Rights Management)은 디지털 콘텐츠의 이용 권한을 관리하여 무단 복제와 유포를 억제하고 저작권자의 권리를 보호하는 기술이다. 콘텐츠 암호화와 이용 허가 정보 등을 활용하여 **누가 어떤 범위에서 콘텐츠를 이용할 수 있는지**를 통제한다. 예를 들어 전자책을 허가된 계정에서만 열게 하거나 인쇄·복사 가능 범위를 제한하는 방식으로 콘텐츠의 무단 이용을 막는다.

NoteBase