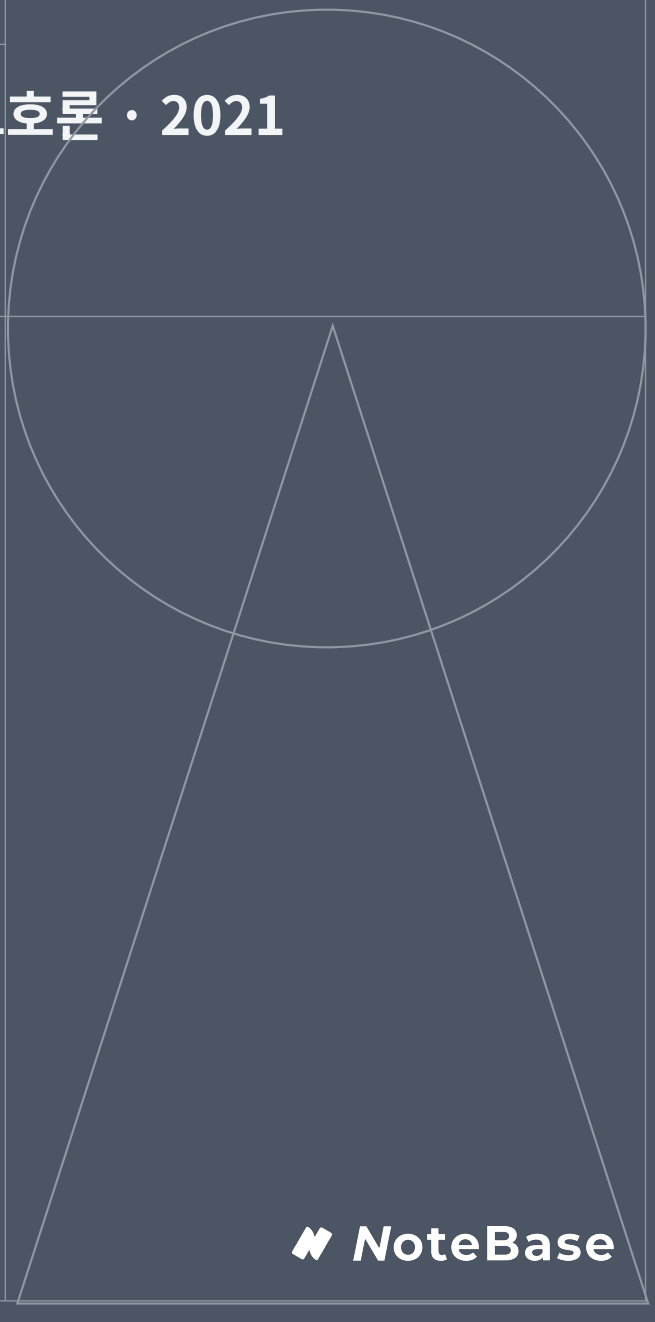
기출OX 해설집

공무원/국가직/9급 · 정보보호론 · 2021



NoteBase

기출OX 해설집

공무원/국가직/9급 · 정보보호론 · 2021

공무원/국가직/9급 · 정보보호론 · 2021

문 1. 겉으로는 유용한 프로그램으로 보이지만 사용자가 의도하지 않은 악성 루틴이 숨어 있어서 사용자가 실행시키면 동작하는 악성 소프트웨어는?

① 키로거

② 트로이목마

③ 애드웨어

④ 랜섬웨어

정답 2번

간단한 해설

유용한 프로그램처럼 위장해 사용자가 실행하도록 유도하고, 내부에 숨겨 둔 악성 기능을 수행하는 것이 **트로이목마**의 특징이다.

공통 해설

트로이목마는 정상적이거나 유용한 프로그램으로 가장하면서 내부에 악성 기능을 숨긴 소프트웨어이다. 여기서 '유용한 프로그램으로 보인다'는 실제로 안전하다는 뜻이 아니라, 사용자가 안전하거나 쓸모 있다고 믿도록 위장한다는 뜻이다. 사용자는 정상적인 기능을 쓰려고 실행하지만, 그 과정에서 의도하지 않은 악성 루틴이 동작한다.

이 문항의 식별 기준은 악성 기능의 구체적인 종류가 아니라 **유용한 프로그램으로 위장하고 악성 기능을 숨기는 방식**이다. 따라서 제시된 설명은 트로이목마에 해당한다.

NoteBase

문 2. 능동적 공격에 해당하는 것만을 모두 고르면?

ㄱ. 도청
ㄴ. 서비스 거부
ㄷ. 트래픽 분석
ㄹ. 메시지 변조

① ㄱ, ㄷ
② ㄴ, ㄷ
③ ㄴ, ㄹ
④ ㄷ, ㄹ

정답 3번

간단한 해설

능동적 공격은 **정보를 변경하거나 정상적인 서비스 이용을 방해**하는 공격이다. 서비스 거부는 이용을 방해하고, 메시지 변조는 전달되는 내용을 바꾼다는 점에서 이에 해당한다.

NoteBase

보기별 해설

소극적 공격은 정보나 통신을 변경하지 않고 관찰하여 정보를 얻는 공격이다. 능동적 공격은 정보를 변경하거나 시스템·통신의 정상적인 작동을 방해하는 공격이다.

ㄱ. 도청 — 소극적 공격: 통신 내용을 몰래 읽거나 듣는 행위이다. **전달되는 내용을 변경하지 않고 정보를 얻는** 공격이므로 소극적 공격에 해당한다.

ㄴ. 서비스 거부 — 능동적 공격: 시스템이나 통신 자원을 고갈시키는 등의 방법으로 정당한 사용자의 **정상적인 서비스 이용을 방해**한다. 메시지 내용을 바꾸지 않더라도 서비스의 가용성을 침해하므로 능동적 공격에 해당한다.

ㄷ. 트래픽 분석 — 소극적 공격: 통신량, 통신 시점, 송수신 관계 등의 **통신 패턴을 관찰**하여 정보를 추론한다. 메시지 내용을 직접 읽지 못해도 분석할 수 있으며, 통신 자체를 변경하거나 방해하지 않으므로 소극적 공격에 해당한다.

ㄹ. 메시지 변조 — 능동적 공격: 전송되는 메시지의 내용을 무단으로 바꾸는 행위이다. **정보의 무결성을 침해**하여 수신자가 원래와 다른 내용을 받게 하므로 능동적 공격에 해당한다.

능동적 공격에 해당하는 것은 ㄴ과 ㄹ이며, 이 조합은 ③에 해당한다.

NoteBase

문 3. 분산 서비스 거부(DDoS) 공격에 대한 설명으로 옳지 않은 것은?

① 하나의 공격 지점에서 대규모 공격 패킷을 발생시켜서 여러 사이트를 동시에 공격하는 방법이다.

② 가용성에 대한 공격이다.

③ 봇넷이 주로 활용된다.

④ 네트워크 대역폭이나 컴퓨터 시스템 자원을 공격 대상으로 한다.

정답 1번

간단한 해설

①의 '하나의 공격 지점'이라는 설명이 잘못되었다. DDoS는 **여러 공격 지점에서 분산하여** 트래픽이나 요청을 보내 대상 서비스의 정상적인 이용을 방해하는 공격이다.

선지별 해설

① X: DDoS의 '분산'은 **공격 트래픽의 발생 지점이 여러 곳**이라는 뜻이다. 여러 장치가 대상 서비스에 동시에 트래픽이나 요청을 보내므로, '하나의 공격 지점에서 여러 사이트를 공격한다'는 설명은 DDoS의 특징을 잘못 설명한 것이다.

② O: 가용성은 정당한 사용자가 필요할 때 정보나 서비스를 이용할 수 있는 성질이다. DDoS는 과도한 부하로 서비스를 지연시키거나 중단시켜 **정상적인 이용을 방해**하므로 가용성에 대한 공격이다.

③ O: 봇넷은 악성코드 등에 감염되어 공격자의 제어를 받는 여러 장치의 집합이다. 공격자가 이 장치들에 공격 명령을 내려 **여러 곳에서 동시에 요청을 발생**시킬 수 있으므로 DDoS에 주로 활용된다.

④ O: 대량의 트래픽으로 **네트워크 대역폭을 포화**시키거나, 과도한 요청으로 서버의 CPU·메모리 등 시스템 자원을 소모시킨다. 그 결과 정상 사용자의 통신이나 요청을 처리할 여력이 부족해진다.

NoteBase

문 4. 부인방지 서비스를 제공하기 위한 전자서명에 대한 설명으로 옳지 않은 것은?

① 서명할 문서에 의존하는 비트 패턴이어야 한다.

② 다른 문서에 사용된 서명을 재사용하는 것이 불가능해야 한다.

③ 전송자(서명자)와 수신자(검증자)가 공유한 비밀 정보를 이용하여 서명하여야 한다.

④ 서명한 문서의 내용을 임의로 변조하는 것이 불가능해야 한다.

정답 3번

간단한 해설

서명자와 검증자가 비밀키를 공유하면 검증자도 같은 인증 정보를 만들 수 있어, 누가 작성했는지 제3자에게 입증하기 어렵다. 부인방지를 위한 전자서명은 **서명자의 개인키로 생성**하고, 대응하는 공개키로 검증한다.

선지별 해설

① O: 전자서명은 **서명 대상 문서의 내용에 의존**하는 비트 패턴이어야 한다. 일반적으로 문서의 해시값을 이용해 서명을 생성하므로, 서명은 특정 문서와 결합된다. 문서와 무관한 고정된 표시만 붙이면 그 표시를 다른 문서에 옮겨도 구별할 수 없다.

② O: 한 문서의 서명을 **다른 문서의 유효한 서명으로 재사용할 수 없어야** 한다. 서명을 복사해 다른 내용의 문서에 붙였을 때 검증이 성공한다면, 서명자가 동의하지 않은 내용까지 서명한 것으로 꾸밀 수 있기 때문이다. 이는 동일한 문서와 서명 쌍을 다시 전송하는 문제와는 구별된다.

③ X: 부인방지를 위한 전자서명은 공유 비밀 정보가 아니라 **서명자만 보유한 개인키**로 생성하고, 대응하는 공개키로 검증한다. 비밀키를 공유하는 메시지 인증 코드(MAC) 방식에서는 수신자도 유효한 인증 코드를 만들 수 있다. 따라서 인증 코드만으로는 제3자에게 송신자가 작성했다는 사실을 입증하기 어려워 부인방지를 제공하지 못한다.

④ O: 서명한 문서는 **변조한 뒤에도 기존 서명이 유효하게 검증되도록 만들 수 없어야** 한다. 문서 내용이 바뀌면 기존 서명과의 대응이 깨져 검증에 실패하므로 무결성 훼손을 확인할 수 있다. 여기서 변조 불가능은 파일의 편집 자체를 막는다는 뜻이 아니라, 변조한 내용을 원래 서명된 내용인 것처럼 통과시킬 수 없어야 한다는 뜻이다.

NoteBase

문 5. 다음은 IT 보안 관리를 위한 국제 표준(ISO/IEC 13335)의 위험 분석 방법에 대한 설명이다. ㉠~㉢에 들어갈 용어를 바르게 연결한 것은?

(㉠)은 가능한 빠른 시간 내에 적정 수준의 보호를 제공한 후 시간을 두고 중요 시스템에 대한 보호 수단을 조사하고 조정하는 것을 목표로 한다. 이 방법은 모든 시스템에 대하여 (㉡)에서 제시하는 권고 사항을 구현하는 것으로 시작한다. 중요 시스템을 대상으로 위험에 즉각적으로 대응하기 위하여 비정형 접근법이 적용될 수 있다. 그리고 (㉢)에 의한 단계별 프로세스를 적절하게 수행한다. 결과적으로 시간이 흐름에 따라 비용 대비 효과적인 보안 통제가 선택되도록 할 수 있다.

① ㉠: 상세 위험 분석, ㉡: 기준선 접근법, ㉢: 복합 접근법

② ㉠: 상세 위험 분석, ㉡: 복합 접근법, ㉢: 기준선 접근법

③ ㉠: 복합 접근법, ㉡: 기준선 접근법, ㉢: 상세 위험 분석

④ ㉠: 복합 접근법, ㉡: 상세 위험 분석, ㉢: 기준선 접근법

정답 3번

간단한 해설

복합 접근법은 기준선 접근법으로 기본적인 보호를 신속히 확보하고, 중요 시스템에는 상세 위험 분석을 적용하여 보호 수단을 보완하는 방식이다. 처음부터 모든 시스템을 정밀하게 분석하는 데 드는 시간과 비용을 줄이면서 필요한 곳에 분석을 집중한다.

빈칸별 해설

㉠ 복합 접근법: 기준선 접근법과 상세 위험 분석 등을 결합하는 전체 전략이다. 지문의 **빠르게 적정 수준의 보호를 제공한 뒤 중요 시스템의 보호 수단을 조사·조정**한다는 설명이 이에 해당한다. 중요 시스템의 긴급한 위험에는 비정형 접근법을 활용할 수도 있으므로, 한 가지 분석 방법만 사용하는 것이 아니다.

㉡ 기준선 접근법: 일반적인 위협에 대응하도록 마련된 보호 대책 목록이나 권고 사항을 바탕으로 기본적인 보안 통제를 적용한다. 개별 시스템의 자산·위협·취약점을 처음부터 정밀하게 분석하지 않아도 **기본적인 보호 대책을 신속히 도입**할 수 있다. 따라서 모든 시스템에 권고 사항을 먼저 구현한다는 부분에 들어간다.

㉢ 상세 위험 분석: 자산을 식별하고 가치를 평가한 뒤, 위협과 취약점을 분석하여 위험을 평가하고 그에 맞는 보호 대책을 선정한다. 기준선 접근법보다 시간과 전문성이 더 필요하지만, **시스템별 위험에 맞는 보호 대책**을 구체적으로 선택할 수 있다. 따라서 초기 보호 이후 중요 시스템의 보호 수준을 단계적으로 보완하는 분석에 해당한다.

㉠은 복합 접근법, ㉡은 기준선 접근법, ㉢은 상세 위험 분석이므로 ③의 연결과 일치한다.

NoteBase

문 6. 다음에서 설명하는 크로스사이트 스크립팅(XSS) 공격의 유형은?

공격자는 XSS 코드를 포함한 URL을 사용자에게 보낸다. 사용자가 그 URL을 요청하고 해당 웹 서버가 사용자 요청에 응답한다. 이때 XSS 코드를 포함한 스크립트가 웹 서버로부터 사용자에게 전달되고 사용자 측에서 스크립트가 실행된다.

① 세컨드 오더 XSS

② DOM 기반 XSS

③ 저장 XSS

④ 반사 XSS

정답 4번

간단한 해설

URL에 포함된 공격 코드가 사용자 요청을 거쳐 **웹 서버의 응답에 실려 되돌아온다**는 점이 반사 XSS의 특징이다. 브라우저는 응답에 포함된 스크립트를 실행한다.

공통 해설

반사 XSS는 요청에 포함된 악성 입력이 웹 서버의 응답에 반영되고, 사용자의 브라우저에서 스크립트로 실행되는 공격이다. '반사'는 **요청으로 보낸 공격 코드가 응답에 실려 돌아온다**는 뜻이다.

지문에서는 공격자가 XSS 코드를 포함한 URL을 보내고, 사용자가 이를 요청하자 서버가 해당 코드를 포함한 스크립트를 응답으로 돌려준다. 이처럼 공격 코드가 요청과 그에 대한 서버 응답을 통해 전달되므로 반사 XSS에 해당한다. 사용자 측에서 스크립트가 실행된다는 사실만으로 DOM 기반 XSS라고 판단하는 것이 아니라, 공격 코드가 응답에 포함되어 돌아오는 경로를 기준으로 구분한다. 서버에 코드를 저장했다가 나중에 사용하는 과정을 추가로 가정할 필요도 없다.

NoteBase

문 7. SHA 알고리즘에서 사용하는 블록 크기와 출력되는 해시의 길이를 바르게 연결한 것은?

① 알고리즘: SHA-1, 블록 크기: 256비트, 해시 길이: 160비트

② 알고리즘: SHA-256, 블록 크기: 512비트, 해시 길이: 256비트

③ 알고리즘: SHA-384, 블록 크기: 1024비트, 해시 길이: 256비트

④ 알고리즘: SHA-512, 블록 크기: 512비트, 해시 길이: 512비트

정답 2번

간단한 해설

SHA-256은 입력 메시지를 **512비트 블록** 단위로 처리하고, 최종적으로 **256비트 해시값**을 출력한다. 블록 크기는 입력 처리 단위이고 해시 길이는 최종 출력의 길이이므로 서로 구분해야 한다.

선지별 해설

블록 크기는 패딩을 마친 입력 메시지를 나누어 처리하는 단위이고, 해시 길이는 전체 메시지를 처리한 뒤 얻는 최종 해시값의 비트 수이다. 입력 메시지가 길어져 처리할 블록 수가 늘어나도, 같은 알고리즘의 해시 길이는 일정하다.

① X: SHA-1의 블록 크기는 **512비트**이고 해시 길이는 160비트이다. 선지의 해시 길이는 맞지만, 블록 크기 256비트를 512비트로 고쳐야 한다.

② O: SHA-256의 블록 크기는 512비트이고 해시 길이는 256비트이므로 두 수치가 모두 맞다. 이름의 **256은 최종 해시 길이**를 뜻하며 입력 블록 크기를 뜻하지 않는다.

③ X: SHA-384의 블록 크기는 1024비트이고 해시 길이는 **384비트**이다. 선지의 블록 크기는 맞지만, 해시 길이 256비트를 384비트로 고쳐야 한다.

④ X: SHA-512의 블록 크기는 **1024비트**이고 해시 길이는 512비트이다. 선지의 해시 길이는 맞지만, 블록 크기 512비트를 1024비트로 고쳐야 한다.

NoteBase

문 8. 데이터베이스 접근 권한 관리를 위한 DCL(Data Control Language)에 속하는 명령으로 그 설명이 옳은 것은?

① GRANT: 사용자가 테이블이나 뷰의 내용을 읽고 선택한다.

② REVOKE: 이미 부여된 데이터베이스 객체의 권한을 취소한다.

③ DROP: 데이터베이스 객체를 삭제한다.

④ DENY: 기존 데이터베이스 객체를 다시 정의한다.

정답 2번

간단한 해설

REVOKE는 **이미 부여된 권한을 취소**하는 DCL 명령이다. 데이터베이스 객체 자체를 삭제하는 것이 아니라, 사용자가 그 객체에 수행할 수 있는 작업의 권한을 회수한다.

선지별 해설

① X: GRANT는 사용자에게 데이터베이스 객체에 대한 **권한을 부여**하는 DCL 명령이다. 테이블이나 뷰의 내용을 조회하는 명령은 SELECT이다. SELECT 권한을 GRANT로 부여하는 것과 SELECT로 실제 데이터를 조회하는 것은 구별해야 한다.

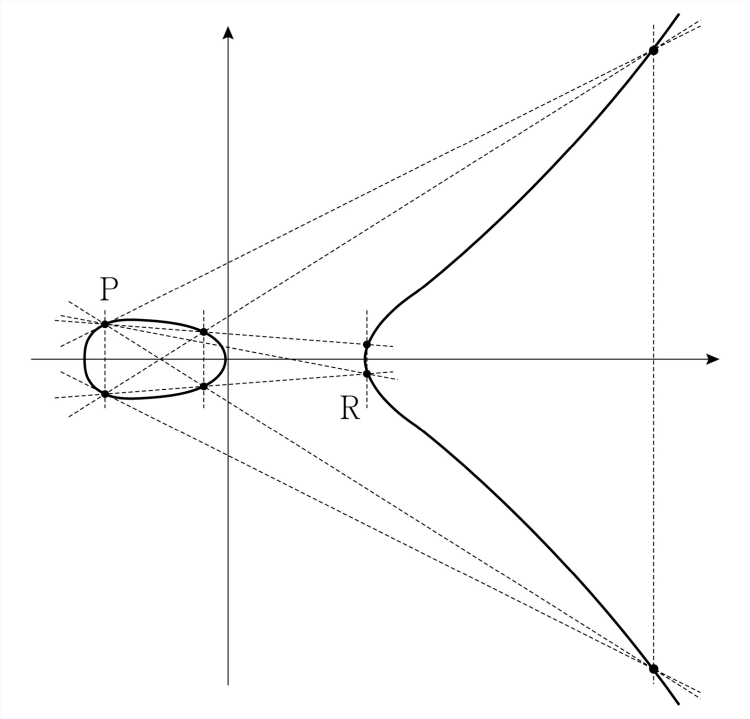
② O: REVOKE는 사용자에게 **이미 부여된 권한을 취소**하는 DCL 명령이다. 예를 들어 테이블의 조회 권한을 부여한 뒤 이를 회수할 때 사용한다. 객체를 없애는 것이 아니라 그 객체에 대한 권한을 취소한다.

③ X: DROP이 데이터베이스 객체를 삭제한다는 설명 자체는 맞다. 다만 객체의 구조를 정의하거나 삭제하는 **DDL(데이터 정의어)**에 속하므로, 접근 권한을 관리하는 DCL 명령이라는 문제의 조건에 맞지 않는다.

④ X: DENY는 이를 지원하는 DBMS에서 사용자에게 특정 권한을 **명시적으로 거부**하는 명령이다. 기존 데이터베이스 객체의 정의를 변경하는 명령은 DDL에 속하는 ALTER이다.

NoteBase

문 9. 타원곡선 암호시스템(ECC)은 타원곡선 이산대수의 어려움을 이용한다. 그림과 같이 실수 위에 정의된 타원곡선과 타원곡선상의 두 점 P와 R이 주어진 경우, R = kP를 만족하는 정수 k의 값은? (단, 점선은 타원곡선의 접선, 점을 연결하는 직선 또는 수직선을 나타낸다)



① 2

② 3

③ 4

④ 5

정답 3번

간단한 해설

타원곡선의 점 덧셈은 직선의 교점을 찾은 뒤 **x축에 대칭시켜** 구한다. 그림에서 이 규칙으로 P를 거듭 더하면 R은 $4P$가 되므로 k = 4이다.

NoteBase

계산 과정

kP는 타원곡선의 덧셈으로 P를 k번 더한 점이다. 두 점을 잇는 직선이 곡선과 만나는 세 번째 점을 C라 하면, 두 점의 합은 C를 **x축에 대칭시킨 점**이다. 같은 점을 두 번 더할 때는 그 점에서의 접선을 사용한다.

1. $2P = P + P$: P에서의 접선을 오른쪽 위로 연장하면 곡선의 맨 오른쪽 위 점과 만난다. 이 교점을 x축에 대칭시킨 맨 오른쪽 아래 점이 $2P$이다.

2. $3P = P + 2P$: P와 맨 오른쪽 아래의 $2P$를 잇는 직선은 왼쪽의 닫힌 곡선에서 y축 바로 왼쪽 아래 점을 지난다. 이 세 번째 교점을 x축에 대칭시킨 y축 바로 왼쪽 위 점이 $3P$이다.

3. $4P = P + 3P$: P와 방금 구한 $3P$를 잇는 완만한 직선은 오른쪽 곡선의 R 바로 위 점을 지난다. 이 세 번째 교점을 x축에 대칭시키면 R이므로 $P + 3P = R$, 즉 $R = 4P$이다.

따라서 k = 4이며, 선택지 ③의 값과 일치한다.

NoteBase

문 10. 「개인정보 보호법」상 가명정보의 처리에 관한 특례에 대한 사항으로 옳지 않은 것은?

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

② 개인정보처리자는 가명정보를 처리하는 과정에서 특정 개인을 알아볼 수 있는 정보가 생성된 경우에는 내부적으로 해당 정보를 처리·보관하되, 제3자에게 제공해서는 아니 된다.

③ 개인정보처리자는 가명정보를 처리하고자 하는 경우에는 가명정보의 처리 목적, 제3자 제공 시 제공받는 자 등 가명정보의 처리 내용을 관리하기 위하여 대통령령으로 정하는 사항에 대한 관련 기록을 작성하여 보관하여야 한다.

④ 통계작성, 과학적 연구, 공익적 기록보존 등을 위한 서로 다른 개인정보처리자 간의 가명정보의 결합은 개인정보 보호위원회 또는 관계 중앙행정기관의 장이 지정하는 전문기관이 수행한다.

정답 2번

①

통계작성, 과학적 연구, 공익적 기록보존 등을 위한 가명정보 처리는 **정보주체의 동의 없이도 허용**된다.

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

②

가명정보 처리 과정에서 특정 개인을 알아볼 수 있는 정보가 생성되면 **즉시 해당 정보의 처리를 중지하고 지체 없이 회수·파기**해야 하므로, 내부적으로 계속 처리·보관할 수 없다.

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>

NoteBase

③

가명정보 처리 특례에 따라 가명정보를 처리하려는 개인정보처리자는 **처리 목적·제3자 제공 시 제공받는 자 등 법정 사항에 관한 기록을 작성·보관**해야 한다.

개인정보 보호법 제28조의4(가명정보에 대한 안전조치의무 등)
③ 개인정보처리자는 제28조의2 또는 제28조의3에 따라 가명정보를 처리하고자 하는 경우에는 가명정보의 처리 목적, 제3자 제공 시 제공받는 자, 가명정보의 처리 기간(제2항에 따라 처리 기간을 별도로 정한 경우에 한한다) 등 가명정보의 처리 내용을 관리하기 위하여 대통령령으로 정하는 사항에 대한 관련 기록을 작성하여 보관하여야 하며, 가명정보를 파기한 경우에는 파기한 날부터 3년 이상 보관하여야 한다. <개정 2023.3.14>

④

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

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

문 11. 시스템 내 하드웨어의 구동, 서비스의 동작, 에러 등의 다양한 이벤트를 선택·수집하여 로그로 저장하고 이를 다른 시스템에 전송할 수 있도록 해 주는 유닉스의 범용 로깅 메커니즘은?

① utmp

② syslog

③ history

④ pacct

정답 2번

간단한 해설

여러 하드웨어·서비스의 이벤트를 모아 로그로 저장하고 **다른 시스템으로 전송**할 수 있는 유닉스의 범용 로깅 메커니즘이 syslog이다.

공통 해설

syslog는 커널과 여러 서비스에서 발생한 이벤트 메시지를 공통 방식으로 수집·처리하는 유닉스의 범용 로깅 메커니즘이다. 메시지의 발생 분야와 심각도 등을 기준으로 필요한 메시지를 선택하고, 설정에 따라 로그 파일에 저장하거나 원격 로그 수집 시스템으로 전송한다. 예를 들어 각 서버에서 발생한 서비스 오류 메시지를 한 로그 서버로 모아 관리할 수 있다. 문제에서 제시한 **다양한 이벤트의 선택·수집, 로그 저장, 다른 시스템으로의 전송**이라는 기능이 syslog의 역할에 해당한다.

NoteBase

문 12. 공개키 암호시스템에 대한 설명으로 옳은 것만을 모두 고르면?

ㄱ. 한 쌍의 공개키와 개인키 중에서 개인키만 비밀로 보관하면 된다.
ㄴ. 동일한 안전성을 가정할 때 ECC는 RSA보다 더 짧은 길이의 키를 필요로 한다.
ㄷ. 키의 분배와 관리가 대칭키 암호시스템에 비하여 어렵다.
ㄹ. 일반적으로 암호화 및 복호화 처리 속도가 대칭키 암호시스템에 비하여 빠르다.

① ㄱ, ㄴ
② ㄱ, ㄹ
③ ㄴ, ㄷ
④ ㄷ, ㄹ

정답 1번

간단한 해설

공개키 암호는 **공개키를 배포하고 개인키만 비밀로 보관**하므로, 통신 상대와 비밀키를 미리 공유해야 하는 부담을 줄인다. 또한 동일한 안전성을 얻는 데 필요한 키 길이는 암호 방식에 따라 달라지며, **ECC는 RSA보다 짧은 키**를 사용한다.

NoteBase

보기별 해설

ㄱ. O: 공개키 암호시스템은 서로 연관된 공개키와 개인키를 사용한다. 공개키는 다른 사람에게 알려 주어도 되지만, **개인키는 소유자만 비밀로 보관**해야 한다. 예를 들어 공개키 암호화에서는 송신자가 수신자의 공개키로 암호화하고, 수신자가 자신의 개인키로 복호화한다.

ㄴ. O: ECC는 타원곡선 암호이며, RSA와는 안전성을 뒷받침하는 수학적 문제와 알려진 공격 방법이 다르다. 따라서 키의 비트 수가 같다고 안전성도 같은 것은 아니다. 기존 컴퓨터를 이용한 공격에 대해 같은 안전성을 비교하면 **ECC가 RSA보다 짧은 키**를 필요로 한다. 예를 들어 약 128비트의 보안 강도에 대응하는 키 길이는 ECC 약 256비트, RSA 3072비트이다.

ㄷ. X: 대칭키 방식은 통신 당사자가 같은 비밀키를 공유하므로, 그 키를 상대방에게 안전하게 전달해야 한다. 공개키 방식은 **개인키를 전달하지 않고 공개키를 배포**할 수 있어 비밀키 분배의 부담이 줄고 키 관리가 상대적으로 용이하다. 따라서 '어렵다'는 '상대적으로 쉽다'로 고쳐야 한다. 다만 배포받은 공개키가 실제 상대방의 것인지 확인하는 인증은 필요하다.

ㄹ. X: 공개키 암호는 일반적으로 대칭키 암호보다 복잡한 수학적 연산을 수행하므로 **암호화·복호화 처리 속도가 느리다**. '빠르다'는 '느리다'로 고쳐야 한다. 이 때문에 실제 통신에서는 공개키 방식으로 대칭키를 안전하게 공유하고, 대량의 데이터는 처리 속도가 빠른 대칭키 방식으로 암호화하는 구성을 사용한다.

옳은 보기는 ㄱ, ㄴ이며, 이를 묶은 선택지는 ①이다.

NoteBase

문 13. 이메일의 보안을 강화하기 위한 기술이 아닌 것은?

① IMAP

② S/MIME

③ PEM

④ PGP

정답 1번

간단한 해설

IMAP의 기본 목적은 서버에 저장된 **이메일의 조회·관리**이다. 메시지 암호화나 전자서명을 통해 이메일 자체를 보호하는 보안 기술과 구별된다.

선지별 해설

① X: IMAP은 메일 클라이언트가 서버에 저장된 이메일을 읽고 검색하며 폴더와 읽음 상태 등을 관리하는 **메일 접근 프로토콜**이다. 이메일 메시지 자체의 암호화·전자서명을 위한 기술은 아니다. TLS와 함께 사용하여 통신 구간을 보호할 수 있다는 점과 IMAP의 기본 용도는 구별해야 한다.

② O: S/MIME은 MIME 형식의 이메일에 **암호화와 전자서명**을 적용하는 보안 기술이다. 암호화는 허가받지 않은 사람이 내용을 읽지 못하도록 기밀성을 보호하고, 전자서명은 발신자 인증과 메시지 무결성 확인에 쓰인다.

③ O: PEM은 이메일에 암호화와 인증 절차를 적용하여 **기밀성·무결성·발신자 인증** 등을 제공하는 보안 기술이다. 메일을 단순히 조회하는 기능이 아니라 송신자와 수신자 사이에서 메시지 내용을 보호하는 데 목적이 있다.

④ O: PGP는 공개키 암호와 대칭키 암호를 결합하여 이메일 등을 보호하는 보안 기술이다. 메시지는 대칭키로 암호화하고 그 대칭키는 수신자의 공개키로 보호하며, **전자서명으로 발신자와 내용의 변조 여부**를 확인할 수 있다.

NoteBase

문 14. 국제 정보보호 표준(ISO 27001:2013 Annex)은 14개 통제 영역에 대하여 114개 통제 항목을 정의하고 있다. 통제 영역의 하나인 물리적 및 환경적 보안에 속하는 통제 항목에 대한 설명에 해당하지 않는 것은?

① 보안 구역은 인가된 인력만의 접근을 보장하기 위하여 적절한 출입 통제로 보호한다.

② 자연 재해, 악의적인 공격 또는 사고에 대비한 물리적 보호를 설계하고 적용한다.

③ 데이터를 전송하거나 정보 서비스를 지원하는 전력 및 통신 배선을 도청, 간섭, 파손으로부터 보호한다.

④ 정보보호에 영향을 주는 조직, 업무 프로세스, 정보 처리 시설, 시스템의 변경을 통제한다.

정답 4번

간단한 해설

조직·업무 프로세스·시설·시스템의 변경을 통제하는 것은 **운영 보안 영역의 변경 관리**이다. 물리적 및 환경적 보안은 출입 통제나 재해 대비, 배선 보호처럼 시설과 장비를 물리적 위협으로부터 보호하는 통제를 다룬다.

선지별 해설

① O: A.11.1.2의 '물리적 출입 통제'에 해당한다. 보안 구역에 들어오는 사람의 인가 여부를 확인하고 출입을 제한하여 **인가되지 않은 사람의 물리적 접근을 방지**한다.

② O: A.11.1.4의 '외부 및 환경적 위협으로부터의 보호'에 해당한다. 자연재해뿐 아니라 악의적인 공격이나 사고로 시설과 장비가 피해를 입는 것도 물리적 위협이므로, 이에 대비한 보호 조치를 설계하고 적용한다.

③ O: A.11.2.3의 '배선 보안'에 해당한다. 전력 및 통신 배선은 정보 서비스를 뒷받침하는 물리적 설비이므로 **도청·간섭·파손으로부터 보호**해야 한다. 통신과 관련된 내용이라도 여기서 보호하는 대상은 배선 자체이므로 물리적 및 환경적 보안에 속한다.

④ X: 정보보호에 영향을 주는 조직·업무 프로세스·정보 처리 시설·시스템의 변경 통제는 A.12.1.2의 '변경 관리'로, **A.12 운영 보안**에 속한다. 변경으로 보안상 문제가 생기지 않도록 관리하는 통제이며, 시설이 언급되었다는 이유로 A.11 물리적 및 환경적 보안으로 분류하지 않는다.

NoteBase

문 15. 대칭키 암호시스템에 대한 암호 분석 방법과 암호 분석가에게 필수적으로 제공되는 모든 정보를 연결한 것으로 옳지 않은 것은?

① 암호문 단독(ciphertext only) 공격 - 암호 알고리즘, 해독할 암호문

② 기지 평문(known plaintext) 공격 - 암호 알고리즘, 해독할 암호문, 임의의 평문

③ 선택 평문(chosen plaintext) 공격 - 암호 알고리즘, 해독할 암호문, 암호 분석가에 의해 선택된 평문과 해독할 암호문에 사용된 키로 생성한 해당 암호문

④ 선택 암호문(chosen ciphertext) 공격 - 암호 알고리즘, 해독할 암호문, 암호 분석가에 의해 선택된 암호문과 해독할 암호문에 사용된 키로 복호화한 해당 평문

정답 2번

간단한 해설

기지 평문 공격에는 '임의의 평문'이 아니라, **이미 알고 있는 평문과 그에 대응하는 암호문의 쌍**이 필요하다. 이 암호문은 해독 대상과 같은 키로 생성된 것이어야 한다.

선지별 해설

① O: 암호문 단독 공격은 암호 알고리즘과 가로챈 암호문을 바탕으로 키나 평문을 추정한다. **알려진 평문·암호문 쌍은 제공되지 않는** 공격이므로, 알고리즘과 해독할 암호문을 연결한 설명에 맞는다.

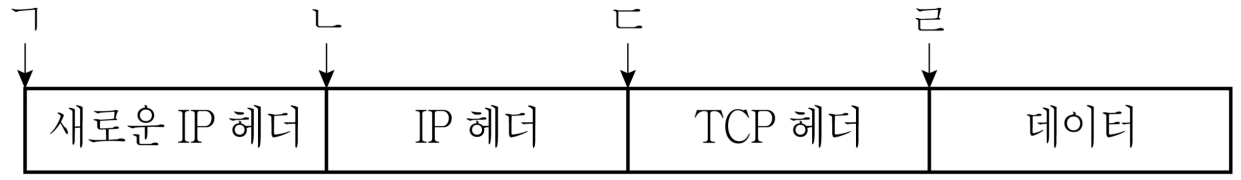
② X: 기지 평문 공격은 이미 알고 있는 평문과, 그 평문을 해독 대상과 같은 키로 암호화한 암호문을 함께 이용한다. 두 자료의 대응 관계를 분석해야 하므로 **'임의의 평문'을 '알려진 평문과 그에 대응하는 암호문의 쌍'**으로 고쳐야 한다. 대응 암호문 없이 평문만 주어지는 것은 필요한 정보를 모두 제공한 것이 아니다.

③ O: 선택 평문 공격에서는 분석가가 **평문을 직접 선택하고 그에 대응하는 암호문을 얻는다**. 해독 대상과 같은 키를 사용하는 암호화 기능을 이용해 원하는 평문의 암호화 결과를 분석할 수 있다. 이미 확보된 평문·암호문 쌍을 이용하는 기지 평문 공격과 달리, 분석할 평문을 선택할 수 있다는 점이 특징이다.

④ O: 선택 암호문 공격에서는 분석가가 **암호문을 직접 선택하고 그에 대응하는 평문을 얻는다**. 해독 대상과 같은 키를 사용하는 복호화 기능을 이용해 선택한 암호문의 복호화 결과를 분석한다. 선택 평문 공격이 암호화 결과를 얻는 방식이라면, 선택 암호문 공격은 복호화 결과를 얻는 방식이다.

NoteBase

문 16. IPv4 패킷에 대하여 터널 모드의 IPSec AH(Authentication Header) 프로토콜을 적용하여 산출된 인증 헤더가 들어갈 위치로 옳은 것은?



① ㄱ

② ㄴ

③ ㄷ

④ ㄹ

정답 2번

간단한 해설

터널 모드는 원래 IP 패킷 전체를 감싸며, AH는 **새 IP 헤더 뒤, 원래 IP 헤더 앞**에 삽입된다. 그림에서 이 경계가 ㄴ이다.

선지별 해설

터널 모드에서는 원래 IP 헤더·TCP 헤더·데이터를 하나의 내부 IP 패킷으로 유지하고, 그 바깥에 새로운 IP 헤더를 붙인다. AH를 적용한 패킷은 '새로운 IP 헤더 → AH → 원래 IP 헤더 → TCP 헤더 → 데이터' 순서로 구성된다.

① X: ㄱ은 새로운 IP 헤더 앞이다. 새로운 IP 헤더는 터널 구간에서 패킷을 전달하기 위한 바깥쪽 헤더이므로 AH보다 먼저 와야 한다. AH는 **새로운 IP 헤더 뒤**의 ㄴ에 삽입한다.

② O: ㄴ은 새로운 IP 헤더와 원래 IP 헤더 사이이다. 터널 모드의 AH는 **원래 IP 패킷 전체의 앞**에 놓이며, 원래 IP 헤더를 포함한 내부 패킷 전체의 무결성과 출처를 인증한다. 따라서 그림의 ㄴ이 AH가 들어갈 위치이다.

③ X: ㄷ은 원래 IP 헤더와 TCP 헤더 사이이다. 원래 IP 헤더 뒤, TCP 헤더 앞에 AH를 넣는 것은 **전송 모드의 배치**이다. 터널 모드에서는 원래 IP 헤더까지 내부 패킷에 포함하므로 AH를 그 앞의 ㄴ에 둔다.

④ X: ㄹ은 TCP 헤더와 데이터 사이이다. AH는 TCP 헤더 뒤에 붙는 헤더가 아니라 **IP 계층의 인증 헤더**이다. 터널 모드에서는 원래 IP 패킷의 내부를 나누지 않고 새로운 IP 헤더와 원래 IP 헤더 사이인 ㄴ에 삽입한다.

NoteBase

문 17. 정보보호 관련 법률과 소관 행정기관을 잘못 짝 지은 것은?

① 「전자정부법」 - 행정안전부
② 「신용정보의 이용 및 보호에 관한 법률」 - 금융위원회
③ 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 - 개인정보보호위원회
④ 「정보통신기반 보호법」 - 과학기술정보통신부

정답 3번

①

중앙행정기관과 그 소속 기관 및 지방자치단체에 관한 전자정부 업무의 중앙사무관장기관은 **행정안전부**이다.

전자정부법 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다. <개정 2013.3.23, 2014.1.28, 2014.11.19, 2017.7.26, 2025.1.7>
4. "중앙사무관장기관"이란 국회 소속 기관에 대하여는 국회사무처, 법원 소속 기관에 대하여는 법원행정처, 헌법재판소 소속 기관에 대하여는 헌법재판소사무처, 중앙선거관리위원회 소속 기관에 대하여는 중앙선거관리위원회사무처, 중앙행정기관 및 그 소속 기관과 지방자치단체에 대하여는 행정안전부를 말한다.

②

신용정보회사 등의 법령 준수 여부를 감독하는 소관 행정기관은 **금융위원회**이다.

신용정보의 이용 및 보호에 관한 법률 제45조(감독 · 검사 등)
① 금융위원회는 신용정보회사등(데이터전문기관을 포함하며, 다음 각 호에 해당하는 자 외의 자로서 대통령령으로 정하는 자는 제외한다. 이하 이 조 및 제45조의2에서 같다)에 대하여 이 법 또는 이 법에 따른 명령의 준수 여부를 감독한다. <개정 2020.2.4>
1. 신용정보회사 및 채권추심회사
2. 본인신용정보관리회사
3. 신용정보집중기관
4. 신용정보제공 · 이용자로서 「금융위원회의 설치 등에 관한 법률」 제38조 각 호의 어느 하나에 해당하는 자
5. 제4호 외의 자로서 대통령령으로 정하는 금융업 또는 보험업을 하는 자

NoteBase

③

소관 행정기관은 **과학기술정보통신부와 방송미디어통신위원회**이다. 이들 기관이 정보통신망의 이용촉진·안정적 관리·운영 및 이용자 보호 시책을 마련한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제4조(정보통신망 이용촉진 및 정보보호등에 관한 시책의 마련)
① 과학기술정보통신부장관 또는 방송미디어통신위원회는 정보통신망의 이용촉진 및 안정적 관리 · 운영과 이용자 보호 등(이하 "정보통신망 이용촉진 및 정보보호등"이라 한다)을 통하여 정보사회의 기반을 조성하기 위한 시책을 마련하여야 한다. <개정 2011.3.29, 2013.3.23, 2017.7.26, 2020.2.4, 2025.10.1>

④

소관 행정기관은 **과학기술정보통신부**이다. 과학기술정보통신부장관은 관계 중앙행정기관의 장 및 국가정보원장과 협의하여 주요정보통신기반시설의 취약점 분석·평가 기준을 정한다.

정보통신기반 보호법 제9조(취약점의 분석 · 평가)
⑤과학기술정보통신부장관은 관계중앙행정기관의 장 및 국가정보원장과 협의하여 제1항 및 제2항에 따른 취약점 분석 · 평가에 관한 기준을 정하고 이를 관계중앙행정기관의 장에게 통보하여야 한다. <개정 2008.2.29, 2013.3.23, 2017.7.26, 2019.12.10>

NoteBase

문 18. 침입탐지시스템의 비정상(anomaly) 탐지 기법에 대한 설명으로 옳지 않은 것은?

① 상대적으로 급격한 변화나 발생 확률이 낮은 행위를 탐지한다.

② 정상 행위를 예측하기 어렵고 오탐률이 높지만 알려지지 않은 공격에도 대응할 수 있다.

③ 수집된 다양한 정보로부터 생성한 프로파일이나 통계적 임계치를 이용한다.

④ 상태전이 분석과 패턴 매칭 방식이 주로 사용된다.

정답 4번

간단한 해설

상태전이 분석과 패턴 매칭은 알려진 공격의 진행 과정이나 특징을 기준으로 하는 **오용(misuse) 탐지**의 대표 방식이다. 비정상 탐지는 **정상 행위의 기준에서 벗어나는 정도**로 침입을 탐지한다.

선지별 해설

① O: 비정상 탐지는 정상적인 사용자나 시스템의 행위와 비교하여 **평소와 크게 다른 행위**를 찾아낸다. 따라서 활동량의 급격한 변화나 정상 행위 모델에서 발생 확률이 낮은 행위를 침입 징후로 탐지할 수 있다.

② O: 정상 행위는 사용자와 운영 환경에 따라 달라 정확히 예측하기 어렵다. 이 때문에 정상적인 작업도 평소와 다르면 공격으로 판단하는 **오탐**이 발생하기 쉽다. 반면 공격 패턴이 미리 등록되어 있지 않아도 정상 기준에서 벗어나면 탐지할 수 있으므로 알려지지 않은 공격에도 대응할 수 있다.

③ O: 접속 시각, 접속 횟수, 네트워크 사용량 등 수집된 정보로 정상 행위의 특성을 나타내는 **프로파일**을 만든다. 관측된 행위가 이 프로파일에서 얼마나 벗어나는지 비교하거나, 통계적으로 정한 임계치를 초과하는지 확인하여 이상 여부를 판단한다.

④ X: 상태전이 분석과 패턴 매칭은 **오용 탐지**의 대표 방식이다. 상태전이 분석은 알려진 공격 시나리오를 시스템의 상태 변화 과정으로 표현한 뒤 실제 행위가 그 과정에 해당하는지 확인한다. 패턴 매칭은 관측된 데이터가 미리 정의한 공격 특징과 일치하는지 대조한다. 비정상 탐지의 대표 방식은 정상 행위 프로파일이나 통계적 임계치를 이용하여 정상 범위에서 벗어나는 행위를 찾는 것이다.

NoteBase

문 19. 「전자서명법」상 과학기술정보통신부장관이 정하여 고시하는 전자서명인증업무 운영기준에 포함되어 있는 사항이 아닌 것은?

① 전자서명 관련 기술의 연구·개발·활용 및 표준화

② 전자서명 및 전자문서의 위조·변조 방지대책

③ 전자서명인증서비스의 가입·이용 절차 및 가입자 확인방법

④ 전자서명인증업무의 휴지·폐지 절차

정답 1번

①

전자서명 관련 기술의 연구·개발·활용 및 표준화는 **전자서명의 이용 촉진을 위한 지원 대상**이며, 운영기준의 법정 포함사항이 아니다.

전자서명법 제5조(전자서명의 이용 촉진을 위한 지원) 과학기술정보통신부장관은 전자서명의 이용을 촉진하기 위하여 다음 각 호의 사항에 대한 행정적 · 재정적 · 기술적 지원을 할 수 있다.
1. 전자서명 관련 기술의 연구 · 개발 · 활용 및 표준화

전자서명법 제7조(전자서명인증업무 운영기준 등)
② 과학기술정보통신부장관은 다음 각 호의 사항이 포함된 전자서명인증업무 운영기준(이하 "운영기준"이라 한다)을 정하여 고시한다. 이 경우 운영기준은 국제적으로 인정되는 기준 등을 고려하여 정하여야 한다. <개정 2021.10.19>
1. 전자서명 및 전자문서의 위조 · 변조 방지대책
2. 전자서명인증서비스의 가입 · 이용 절차 및 가입자 확인방법
3. 전자서명인증업무의 휴지 · 폐지 절차
4. 전자서명인증업무 관련 시설기준 및 자료의 보호방법
5. 가입자 및 이용자의 권익 보호대책
6. 장애인 · 고령자 등의 전자서명 이용 보장
7. 그 밖에 전자서명인증업무의 운영 · 관리에 관한 사항

NoteBase

②

전자서명인증업무 운영기준에는 **전자서명과 전자문서의 위조·변조 방지대책**이 포함된다.

전자서명법 제7조(전자서명인증업무 운영기준 등)
② 과학기술정보통신부장관은 다음 각 호의 사항이 포함된 전자서명인증업무 운영기준(이하 "운영기준"이라 한다)을 정하여 고시한다. 이 경우 운영기준은 국제적으로 인정되는 기준 등을 고려하여 정하여야 한다. <개정 2021.10.19>
1. 전자서명 및 전자문서의 위조 · 변조 방지대책

③

전자서명인증서비스의 **가입·이용 절차와 가입자 확인방법**은 전자서명인증업무 운영기준에 포함된다.

전자서명법 제7조(전자서명인증업무 운영기준 등)
② 과학기술정보통신부장관은 다음 각 호의 사항이 포함된 전자서명인증업무 운영기준(이하 "운영기준"이라 한다)을 정하여 고시한다. 이 경우 운영기준은 국제적으로 인정되는 기준 등을 고려하여 정하여야 한다. <개정 2021.10.19>
2. 전자서명인증서비스의 가입 · 이용 절차 및 가입자 확인방법

④

전자서명인증업무를 **휴지하거나 폐지하는 절차**는 전자서명인증업무 운영기준에 포함된다.

전자서명법 제7조(전자서명인증업무 운영기준 등)
② 과학기술정보통신부장관은 다음 각 호의 사항이 포함된 전자서명인증업무 운영기준(이하 "운영기준"이라 한다)을 정하여 고시한다. 이 경우 운영기준은 국제적으로 인정되는 기준 등을 고려하여 정하여야 한다. <개정 2021.10.19>
3. 전자서명인증업무의 휴지 · 폐지 절차

NoteBase

문 20. 안드로이드 보안 체계에 대한 설명으로 옳지 않은 것은?

① 모든 응용 프로그램은 일반 사용자 권한으로 실행된다.

② 기본적으로 안드로이드는 일반 계정으로 동작하는데 이를 루트로 바꾸면 일반 계정의 제한을 벗어나 기기에 대한 완전한 통제권을 가질 수 있다.

③ 응용 프로그램은 샌드박스 프로세스 내부에서 실행되며, 기본적으로 시스템과 다른 응용 프로그램으로의 접근이 통제된다.

④ 설치되는 응용 프로그램은 구글의 인증 기관에 의해 서명·배포된다.

정답 4번

간단한 해설

④의 '구글의 인증 기관에 의해 서명·배포된다'는 설명이 잘못되었다. 안드로이드 앱은 **개발자가 자체 서명한 인증서**를 사용할 수 있으며, 구글 인증 기관의 서명이나 구글을 통한 배포가 필수는 아니다.

선지별 해설

① O: 안드로이드의 기본 보안 모델에서 응용 프로그램은 **루트가 아닌 일반 사용자 권한**으로 실행된다. 앱에 사용자 식별자(UID)를 부여하여 해당 권한 범위에서만 자원에 접근하도록 하므로, 앱을 설치했다고 해서 시스템 전체를 관리할 권한이 생기지는 않는다.

② O: 루트(root)는 리눅스의 최고 관리자 권한을 뜻한다. 루팅은 이러한 **루트 권한을 얻는 것**으로, 일반 사용자에게 제한된 시스템 파일이나 설정을 변경하는 등 기기를 폭넓게 제어할 수 있게 한다. 이는 모든 앱이 기본적으로 루트로 실행된다는 뜻은 아니다.

③ O: 샌드박스는 앱의 실행 환경과 자원을 격리하여 시스템과 다른 앱을 보호하는 장치이다. 안드로이드는 UID와 프로세스별 접근 통제를 이용하므로, 앱은 기본적으로 **다른 앱의 데이터에 임의로 접근할 수 없다**. 예를 들어 앱 A가 앱 B의 비공개 파일을 읽으려 해도 필요한 권한이나 허용된 공유 경로가 없으면 접근이 차단된다.

④ X: 안드로이드 앱은 설치를 위해 전자서명이 필요하지만, **중앙 인증 기관의 서명은 필수가 아니다**. 개발자가 외부 인증 기관의 승인 없이 자체 서명 인증서를 만들어 앱에 서명할 수 있다. 서명은 앱의 서명 주체와 업데이트의 연속성을 확인하는 데 쓰이며, 구글이 모든 앱의 안전성을 인증한다는 뜻이 아니다. 배포 역시 구글 플레이에 한정되지 않고 다른 앱 마켓이나 직접 배포 방식으로도 이루어질 수 있다.

NoteBase