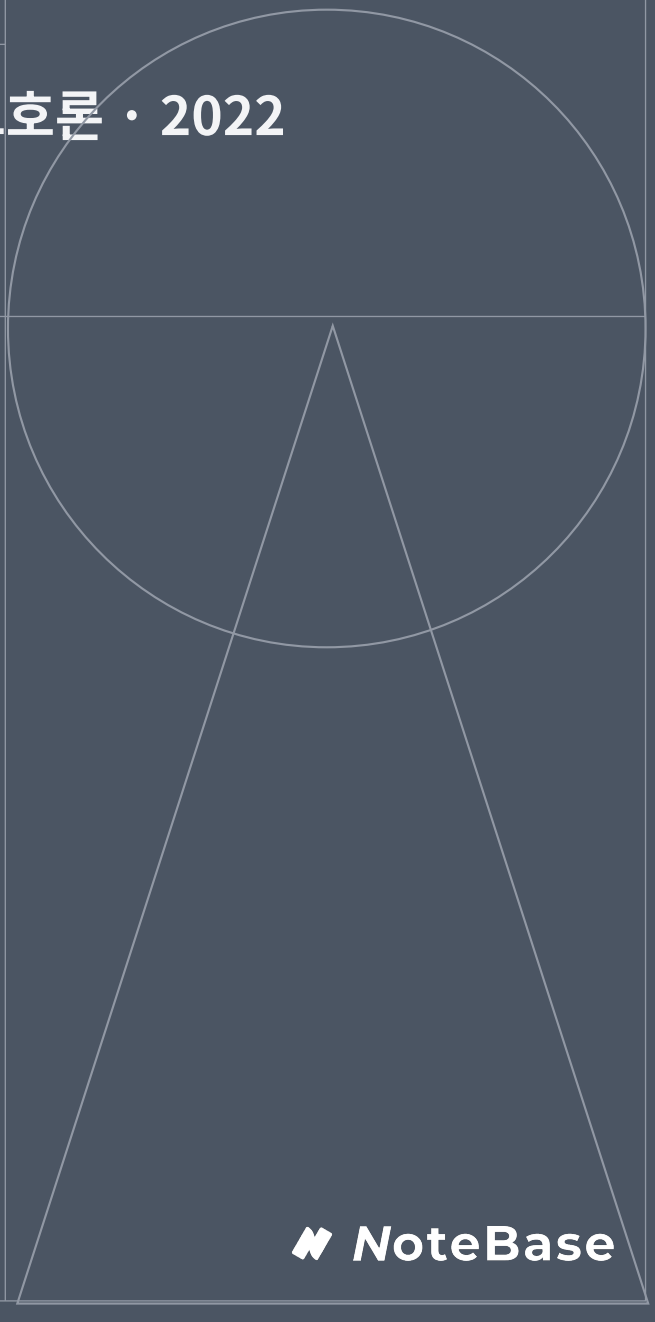
기출OX 해설집

공무원/국가직/9급 · 정보보호론 · 2022



NoteBase

기출OX 해설집

공무원/국가직/9급 · 정보보호론 · 2022

공무원/국가직/9급 · 정보보호론 · 2022

문 1. 사용자의 신원을 검증하고 전송된 메시지의 출처를 확인하는 정보보호 개념은?

① 무결성

② 기밀성

③ 인증성

④ 가용성

정답 3번

간단한 해설

사용자의 신원과 메시지의 출처가 진짜인지 확인하는 것은 **인증성**에 해당한다. 핵심은 주장된 사용자나 송신자가 실제로 그 대상인지를 검증하는 데 있다.

공통 해설

인증성은 사용자나 메시지의 출처가 **주장된 신원과 일치하는지** 확인하는 성질이다. 사용자의 신원을 검증한다는 것은 접속한 사람이 자신이 주장하는 본인인지 확인한다는 뜻이고, 전송된 메시지의 출처를 확인한다는 것은 그 메시지가 주장된 송신자로부터 왔는지 확인한다는 뜻이다. 두 조건은 모두 사용자 또는 송신자의 진위를 확인하므로 인증성에 해당한다.

NoteBase

문 2. TCP에 대한 설명으로 옳지 않은 것은?

① 비연결 지향 프로토콜이다.

② 3-Way Handshaking을 통해 서비스를 연결 설정한다.

③ 포트 번호를 이용하여 서비스들을 구별하여 제공할 수 있다.

④ SYN Flooding 공격은 TCP 취약점에 대한 공격이다.

정답 1번

간단한 해설

TCP는 통신 전에 연결을 설정하는 **연결 지향 프로토콜**이다. '비연결 지향'은 UDP의 특성이다.

선지별 해설

① X: TCP는 **연결 지향 프로토콜**로, 양 끝의 통신 주체가 연결을 설정한 뒤 데이터를 주고받는다. 따라서 '비연결 지향'을 '연결 지향'으로 고쳐야 한다. UDP는 사전 연결 설정 없이 데이터를 보내는 비연결 지향 프로토콜이다.

② O: TCP는 **SYN → SYN+ACK → ACK**의 3-Way Handshaking으로 연결을 설정한다. 클라이언트가 SYN으로 연결을 요청하고, 서버가 SYN+ACK으로 응답한 뒤, 클라이언트가 ACK을 보내 연결 설정을 완료한다.

③ O: TCP 헤더의 **출발지·목적지 포트 번호**는 데이터를 주고받는 응용 프로그램을 구별하는 데 사용된다. 같은 호스트에서도 서비스마다 서로 다른 포트 번호를 사용하면 수신한 데이터를 해당 서비스를 제공하는 프로그램에 전달할 수 있다.

④ O: SYN Flooding은 **TCP 연결 설정 절차를 악용**하는 서비스 거부 공격이다. 공격자가 대량의 SYN을 보내고 마지막 ACK을 보내지 않으면 서버에 연결 설정이 끝나지 않은 상태가 쌓일 수 있다. 이때 연결 대기 공간 등의 자원이 소모되어 정상적인 연결 요청 처리가 방해된다.

NoteBase

문 3. 암호 알고리즘에 대한 설명으로 옳지 않은 것은?

① 일반적으로 대칭키 암호 알고리즘은 비대칭키 암호 알고리즘에 비하여 빠르다.

② 대칭키 암호 알고리즘에는 Diffie-Hellman 알고리즘이 있다.

③ 비대칭키 암호 알고리즘에는 타원 곡선 암호 알고리즘이 있다.

④ 인증서는 비대칭키 암호 알고리즘에서 사용하는 공개키 정보를 포함하고 있다.

정답 2번

간단한 해설

Diffie-Hellman은 대칭키 암호 알고리즘이 아니라 **비대칭키 기반의 키 합의 방식**이다. 합의한 공유 비밀을 이용해 대칭키를 마련할 수 있다는 점과, Diffie-Hellman 자체가 대칭키로 데이터를 암호화한다는 것은 구별해야 한다.

선지별 해설

① O: 대칭키 암호는 암호화와 복호화에 같은 비밀키를 사용하며, 일반적으로 비대칭키 암호보다 **연산 부담이 작고 처리 속도가 빠르다**. 따라서 대용량 데이터를 암호화하는 데 적합하다. 비대칭키 암호는 서로 다른 공개키와 개인키를 사용하며, 일반적으로 더 복잡한 수학적 연산이 필요하다.

② X: Diffie-Hellman은 **비대칭키 기반의 키 합의 알고리즘**이다. 각 참여자는 자신의 개인키와 상대방의 공개값을 이용하여 같은 공유 비밀을 계산한다. 이 공유 비밀로부터 대칭키를 도출할 수 있지만, Diffie-Hellman 자체는 대칭키로 평문을 암호화하고 복호화하는 알고리즘이 아니다. 대칭키 암호 알고리즘의 예로는 AES가 있다.

③ O: 타원 곡선 암호(ECC)는 타원 곡선 위의 점에 대한 수학적 연산을 이용하는 **비대칭키 암호 기술**이다. 개인키로부터 공개키를 계산할 수 있지만, 공개키로부터 개인키를 알아내기는 어렵다는 성질을 이용한다. 타원 곡선 기반의 전자서명이나 키 합의가 이에 해당한다.

④ O: 공개키 인증서는 **인증 대상의 신원과 공개키를 연결**하는 전자 문서이다. 인증 대상의 공개키 및 관련 알고리즘 정보 등을 포함하며, 인증기관의 전자서명을 통해 그 연결을 확인할 수 있게 한다. 공개키에 대응하는 개인키는 비밀로 관리하며 인증서에 포함하지 않는다.

NoteBase

문 4. TCP 세션 하이재킹에 대한 설명으로 옳은 것은?

① 서버와 클라이언트가 통신할 때 TCP의 시퀀스 넘버를 제어하는 데 문제점이 있음을 알고 이를 이용한 공격이다.

② 공격 대상이 반복적인 요구와 수정을 계속하여 시스템 자원을 고갈시킨다.

③ 데이터의 길이에 대한 불명확한 정의를 악용한 덮어쓰기로 인해 발생한다.

④ 사용자의 동의 없이 컴퓨터에 불법적으로 설치되어 문서나 그림 파일 등을 암호화한다.

정답 1번

간단한 해설

TCP 세션 하이재킹은 **시퀀스 번호 처리의 취약점**을 악용하여 이미 연결된 서버와 클라이언트 사이의 통신을 가로채는 공격이다. 통신에 맞는 번호를 가진 위조 패킷을 끼워 넣어 정상 통신 상대처럼 행세한다.

선지별 해설

① O: TCP의 시퀀스 번호는 전송하는 데이터의 순서를 나타내며, 수신 측이 데이터를 올바른 순서로 처리하는 데 사용된다. TCP 세션 하이재킹은 연결 정보를 알아내고 **수신 측이 받아들일 수 있는 시퀀스 번호**에 맞춘 위조 패킷을 주입하여 기존 통신에 끼어드는 공격이다. 선지는 이러한 시퀀스 번호 처리의 취약점을 이용하는 방식을 설명한다.

② X: 반복적인 처리로 시스템 자원을 고갈시켜 정상 이용자가 서비스를 이용하지 못하게 하는 것은 **서비스 거부(DoS) 공격**의 방식이다. 핵심은 CPU·메모리 등의 처리 자원을 소진하는 데 있다. TCP 세션 하이재킹의 핵심은 기존 연결에 끼어들어 통신 상대를 가장하는 데 있다.

③ X: 입력 데이터의 길이를 충분히 검사하지 않아 할당된 저장 공간을 넘어서 데이터를 쓰고 인접한 메모리를 덮어쓰는 것은 **버퍼 오버플로 공격**이다. 이는 메모리 경계를 넘는 쓰기 문제이며, TCP 시퀀스 번호를 이용해 기존 연결에 끼어드는 세션 하이재킹과 구별된다.

④ X: 사용자 몰래 실행되어 문서나 그림 파일 등을 암호화하고 사용할 수 없게 만드는 것은 **랜섬웨어**의 특징이다. 랜섬웨어는 보통 복호화를 대가로 금전을 요구한다. TCP 세션 하이재킹은 파일 암호화가 아니라 이미 성립한 통신 연결의 탈취에 초점을 둔다.

NoteBase

문 5. 생체 인증 측정에 대한 설명으로 옳지 않은 것은?

① FRR는 권한이 없는 사람이 인증을 시도했을 때 실패하는 비율이다.

② 생체 인식 시스템의 성능을 평가하는 지표로는 FAR, EER, FRR 등이 있다.

③ 생체 인식 정보는 신체적 특징과 행동적 특징을 이용하는 것들로 분류한다.

④ FAR는 권한이 없는 사람이 인증을 시도했을 때 성공하는 비율이다.

정답 1번

간단한 해설

FRR는 **권한이 있는 사람을 잘못 거부하는 비율**이다. 권한이 없는 사람의 인증이 실패하는 것은 정상적인 거부이므로 FRR에 해당하지 않는다.

선지별 해설

① X: FRR(False Rejection Rate, 본인거부율)는 **권한이 있는 사람의 인증 시도 중 잘못 거부된 비율**이다. 따라서 '권한이 없는 사람'을 '권한이 있는 사람'으로 고쳐야 한다. 권한이 없는 사람의 인증을 거부한 것은 정상적인 처리이며, 오인 거부가 아니다.

② O: FAR와 FRR는 각각 잘못된 인증 허용과 잘못된 인증 거부가 얼마나 발생하는지를 나타내는 성능 지표이다. EER(Equal Error Rate, 등가오류율)은 인증 판단 기준을 조정했을 때 **FAR와 FRR가 같아지는 지점의 오류율**로, 두 오류를 함께 고려하는 평가 지표이다.

③ O: 생체 인식은 개인의 **신체적 특징과 행동적 특징**을 이용한다. 신체적 특징에는 지문·홍채·얼굴 등이 있고, 행동적 특징에는 서명하는 습관이나 키보드를 입력하는 리듬 등이 있다.

④ O: FAR(False Acceptance Rate, 타인수락률)는 **권한이 없는 사람의 인증 시도 중 잘못 허용된 비율**이다. 시스템이 타인을 정당한 사용자로 잘못 인식하여 인증을 성공시키는 오류를 측정한다.

NoteBase

문 6. 블록암호 카운터 운영모드에 대한 설명으로 옳지 않은 것은?

① 암호화와 복호화는 같은 구조로 구성되어 있다.

② 병렬로 처리할 수 있는 능력에 따라 처리속도가 결정된다.

③ 카운터를 암호화하고 평문블록과 XOR하여 암호블록을 생성한다.

④ 블록을 순차적으로 암호화·복호화 한다.

정답 4번

간단한 해설

CTR 모드는 각 블록의 카운터값을 독립적으로 암호화하므로 **암호화와 복호화 모두 병렬 처리**할 수 있다. 따라서 블록을 반드시 순차적으로 처리해야 한다는 설명은 잘못되었다.

선지별 해설

① O: CTR 모드는 암호화와 복호화에서 모두 **블록암호의 암호화 함수**로 카운터값을 처리한다. 암호화할 때는 그 출력값을 평문과 XOR하고, 복호화할 때는 같은 출력값을 암호문과 XOR한다. 같은 값을 두 번 XOR하면 원래 값으로 돌아오므로 두 과정의 구조가 같다.

② O: 각 카운터값의 암호화에는 **앞 블록의 처리 결과가 필요하지 않다**. 따라서 여러 블록을 동시에 처리할 수 있으며, 구현에서 병렬 처리 능력을 높이면 여러 블록을 처리하는 시간을 줄일 수 있다.

③ O: 블록마다 서로 다른 카운터값을 암호화하여 출력 블록을 만들고, 이를 대응하는 평문 블록과 **XOR**하여 암호문 블록을 생성한다. 평문 블록 자체를 블록암호의 입력으로 넣는 방식과 구별된다.

④ X: CTR 모드는 블록을 반드시 순차적으로 암호화·복호화하는 방식이 아니다. 각 블록은 해당 카운터값과 키만 있으면 앞 블록의 결과를 기다리지 않고 처리할 수 있으므로, **암호화와 복호화 모두 병렬 처리**가 가능하다.

NoteBase

문 7. AES 알고리즘에 대한 설명으로 옳지 않은 것은?

① 대먼과 리즈먼이 제출한 Rijndael이 AES 알고리즘으로 선정되었다.

② 암호화 과정의 모든 라운드에서 SubBytes, ShiftRows, MixColumns, AddRoundKey 연산을 수행한다.

③ 키의 길이는 128, 192, 256 bit의 크기를 사용한다.

④ 입력 블록은 128 bit이다.

정답 2번

간단한 해설

AES의 **마지막 라운드에서는 MixColumns를 생략**하고 SubBytes, ShiftRows, AddRoundKey만 수행한다. 따라서 네 연산을 '모든 라운드'에서 수행한다는 설명은 잘못되었다.

선지별 해설

① O: 대먼(Joan Daemen)과 리즈먼(Vincent Rijmen)이 제출한 **Rijndael**이 미국 국립표준기술연구소(NIST)의 AES 선정 절차에서 채택되었다. AES는 이를 바탕으로 정한 대칭키 블록 암호 표준이다.

② X: 일반 라운드는 SubBytes → ShiftRows → MixColumns → AddRoundKey 순으로 수행하지만, **마지막 라운드에서는 MixColumns를 생략**한다. 마지막에는 SubBytes → ShiftRows → AddRoundKey만 수행하므로, '모든 라운드'라는 표현을 '마지막 라운드를 제외한 라운드'로 고쳐야 한다. 또한 첫 라운드에 들어가기 전에는 초기 AddRoundKey를 수행한다.

③ O: AES가 지원하는 **키 길이는 128, 192, 256 bit**이다. AES-128, AES-192, AES-256이라는 명칭의 숫자는 각각 사용하는 키의 비트 길이를 뜻한다.

④ O: AES는 데이터를 **128 bit 블록 단위**로 암호화한다. 키 길이가 128, 192, 256 bit 중 어느 것이든 입력 블록 크기는 128 bit로 일정하다. 따라서 AES-256에서도 한 블록의 크기는 256 bit가 아니라 128 bit이다.

NoteBase

문 8. 비트코인 블록 헤더의 구조에서 머클 루트에 대한 설명으로 옳지 않은 것은?

① 머클 트리 루트의 해시값이다.

② 머클 트리는 이진트리 형태이다.

③ SHA-256으로 해시값을 계산한다.

④ 필드의 크기는 64바이트이다.

정답 4번

간단한 해설

머클 루트 필드의 크기는 **32바이트(256비트)**이다. 이를 16진수로 나타내면 64자가 되지만, 실제 필드 크기가 64바이트가 되는 것은 아니다.

선지별 해설

① O: 머클 루트는 블록에 포함된 거래들의 해시값을 바탕으로 만든 **머클 트리의 최상위 해시값**이다. 하위 해시들을 차례로 결합하여 하나의 값으로 요약하므로, 블록 헤더에 모든 거래의 해시를 각각 저장할 필요가 없다.

② O: 비트코인의 머클 트리는 **두 해시값을 한 쌍으로 묶어** 상위 해시값을 만드는 이진트리 구조이다. 각 단계에서 해시값 개수가 홀수이면 마지막 값을 복제하여 쌍을 만든 뒤 상위 해시값을 계산한다.

③ O: 비트코인의 머클 트리는 SHA-256을 사용한다. 구체적으로는 하위 해시값 두 개를 이어 붙인 데이터에 **SHA-256을 두 번 적용**하여 상위 해시값을 만든다. 두 번 적용해도 최종 출력 길이는 SHA-256의 출력 길이인 256비트이다.

④ X: 머클 루트 필드는 64바이트가 아니라 **32바이트**이다. 1바이트는 8비트이므로 32바이트는 256비트에 해당한다. 이 값을 16진수 문자열로 표시하면 한 글자가 4비트를 나타내어 64자가 되는데, 이 표시 길이와 블록 헤더에 저장되는 필드의 바이트 크기를 구별해야 한다.

NoteBase

문 9. SET에 대한 설명으로 옳지 않은 것은?

① 인터넷에서 신용카드를 지불수단으로 이용하기 위한 기술이다.

② 인증기관은 SET에 참여하는 모든 구성원의 정당성을 보장한다.

③ 고객등록에서는 지불 게이트웨이를 통하여 고객의 등록과 인증서의 처리가 이루어진다.

④ 상점등록에서는 인증 허가 기관에 등록하여 자신의 인증서를 만들어야 한다.

정답 3번

간단한 해설

③의 '지불 게이트웨이를 통하여'가 잘못되었다. 고객 등록과 인증서 발급은 **고객용 인증기관(CA)**을 통해 이루어지며, 지불 게이트웨이는 상점의 결제 승인 요청을 금융기관에 중계한다.

선지별 해설

① O: SET(Secure Electronic Transaction)은 **인터넷에서 신용카드 결제를 안전하게 수행**하기 위한 보안 프로토콜이다. 암호화와 전자서명, 인증서를 이용하여 결제정보를 보호하고 거래 참여자를 인증한다.

② O: 인증기관은 고객·상점·지불 게이트웨이 등 SET 참여자에게 인증서를 발급하여 **참여자의 신원과 공개키의 연결**을 보증한다. 거래 상대방은 인증서를 검증하여 그 참여자가 정당한 거래 주체인지 확인한다. 여기서 정당성 보장은 거래 상대방의 모든 행위나 상품 품질을 보장한다는 뜻은 아니다.

③ X: 고객은 **고객용 인증기관(CCA)에 등록하고 인증서를 발급**받는다. 인증기관은 카드 발급기관을 통해 고객의 등록정보를 확인한 뒤 인증서를 발급한다. 지불 게이트웨이는 상점의 결제 승인 요청과 금융기관의 응답을 중계하는 역할이므로, 고객 등록과 인증서 처리를 담당하는 주체로 설명한 부분을 고객용 인증기관으로 고쳐야 한다.

④ O: 상점은 SET 거래에 참여하기 위해 **상점용 인증기관(MCA)에 등록하여 인증서를 발급**받아야 한다. 인증기관은 카드 매입기관 등의 확인을 거쳐 상점의 공개키가 포함된 인증서를 발급한다. 선지의 '자신의 인증서를 만들어야 한다'는 상점이 스스로 인증하는 것이 아니라 인증기관이 발급한 상점 인증서를 갖추어야 한다는 의미이다.

NoteBase

문 10. 「개인정보 보호법」 제26조(업무위탁에 따른 개인정보의 처리 제한)에 대한 설명으로 옳지 않은 것은?

① 위탁자가 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 대통령령으로 정하는 방법에 따라 위탁하는 업무의 내용과 수탁자를 정보주체에게 알려야 한다.

② 위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리 현황 점검 등 대통령령으로 정하는 바에 따라 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.

③ 수탁자는 개인정보처리자로부터 위탁받은 해당 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공할 수 있다.

④ 수탁자가 위탁받은 업무와 관련하여 개인정보를 처리하는 과정에서 「개인정보 보호법」을 위반하여 발생한 손해배상책임에 대하여 수탁자를 개인정보처리자의 소속 직원으로 본다.

정답 3번

①

재화나 서비스의 홍보 또는 판매 권유 업무를 위탁할 때에는 **위탁 업무의 내용과 수탁자를 정보주체에게 알려야 한다**.

개인정보 보호법 제26조(업무위탁에 따른 개인정보의 처리 제한)
③ 위탁자가 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 대통령령으로 정하는 방법에 따라 위탁하는 업무의 내용과 수탁자를 정보주체에게 알려야 한다. 위탁하는 업무의 내용이나 수탁자가 변경된 경우에도 또한 같다.

NoteBase

②

위탁자는 개인정보의 분실·도난·유출·위조·변조·훼손을 방지하기 위해 **수탁자를 교육하고 개인정보의 안전한 처리 여부를 감독하여야 한다**.

개인정보 보호법 제26조(업무위탁에 따른 개인정보의 처리 제한)
④ 위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 유출등이 되지 아니하도록 수탁자를 교육하고, 처리 현황 점검 등 대통령령으로 정하는 바에 따라 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다. <개정 2015.7.24, 2026.3.10>

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>

③

수탁자는 **위탁받은 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공할 수 없다**.

개인정보 보호법 제26조(업무위탁에 따른 개인정보의 처리 제한)
⑤ 수탁자는 개인정보처리자로부터 위탁받은 해당 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공하여서는 아니 된다.

④

위탁 업무와 관련한 개인정보 처리 중 법 위반으로 발생한 손해배상책임에 대해서는 **수탁자를 개인정보처리자의 소속 직원으로 본다**.

개인정보 보호법 제26조(업무위탁에 따른 개인정보의 처리 제한)
⑦ 수탁자가 위탁받은 업무와 관련하여 개인정보를 처리하는 과정에서 이 법을 위반하여 발생한 손해배상책임에 대하여는 수탁자를 개인정보처리자의 소속 직원으로 본다. <개정 2023.3.14>

NoteBase

문 11. IPv6에 대한 설명으로 옳지 않은 것은?

① IP주소 부족 문제를 해결하기 위하여 등장하였다.

② 128 bit 주소공간을 제공한다.

③ 유니캐스트는 단일 인터페이스를 정의한다.

④ 목적지 주소는 유니캐스트, 애니캐스트, 브로드캐스트 주소로 구분된다.

정답 4번

간단한 해설

IPv6의 주소 유형은 유니캐스트·애니캐스트·**멀티캐스트**이며, **브로드캐스트 주소는 없다**. 브로드캐스트의 기능은 멀티캐스트가 대신한다.

선지별 해설

① O: IPv4는 32비트 주소를 사용하므로 할당할 수 있는 주소 수에 한계가 있다. IPv6는 **주소 공간을 확대**하여 IP 주소 부족 문제를 해결하기 위해 등장하였다.

② O: IPv6 주소의 길이는 **128비트**이다. IPv4의 32비트보다 주소 길이가 길어 훨씬 많은 주소를 표현할 수 있다.

③ O: 유니캐스트 주소는 **단일 인터페이스를 식별**한다. 인터페이스는 장치가 네트워크 링크에 연결되는 접점이며, 유니캐스트 주소로 보낸 패킷은 그 주소가 가리키는 인터페이스에 전달된다.

④ X: IPv6의 주소 유형은 유니캐스트·애니캐스트·멀티캐스트이므로, '브로드캐스트'를 **멀티캐스트**로 고쳐야 한다. IPv6에는 브로드캐스트 주소가 없으며, 그 기능을 멀티캐스트가 대신한다. 멀티캐스트는 해당 그룹의 모든 인터페이스에 패킷을 전달하고, 애니캐스트는 같은 주소를 공유하는 인터페이스들 중 라우팅 기준으로 가장 가까운 하나에 전달한다.

NoteBase

문 12. SSH를 구성하는 프로토콜에 대한 설명으로 옳은 것은?

① SSH는 보통 TCP상에서 수행되는 3개의 프로토콜로 구성된다.

② 연결 프로토콜은 서버에게 사용자를 인증한다.

③ 전송계층 프로토콜은 SSH 연결을 사용하여 한 개의 논리적 통신 채널을 다중화한다.

④ 사용자 인증 프로토콜은 전방향 안전성을 만족하는 서버인증만을 제공한다.

정답 1번

간단한 해설

SSH는 보통 TCP 위에서 동작하며, **전송계층·사용자 인증·연결의 세 프로토콜**로 구성된다. 이들은 각각 안전한 통신 기반 마련, 사용자 인증, 논리 채널 다중화를 맡는다.

선지별 해설

① O: SSH는 **전송계층 프로토콜, 사용자 인증 프로토콜, 연결 프로토콜**의 세 구성 요소로 이루어진다. 전송계층 프로토콜은 보통 TCP 연결 위에서 동작하고, 사용자 인증 프로토콜과 연결 프로토콜은 그 위에서 차례로 동작한다.

② X: 서버에게 사용자를 인증하는 것은 연결 프로토콜이 아니라 **사용자 인증 프로토콜**이다. 이는 접속하려는 클라이언트 측 사용자의 신원을 서버가 확인하도록 한다. 연결 프로토콜은 사용자 인증 후 논리 채널을 구성하고 관리한다.

③ X: 논리 채널을 다중화하는 것은 전송계층 프로토콜이 아니라 **연결 프로토콜**이다. 또한 한 개의 논리 채널을 다중화하는 것이 아니라, 하나의 암호화된 SSH 연결을 여러 논리 채널로 나누어 사용한다. 전송계층 프로토콜은 서버 인증과 통신의 기밀성·무결성 보호를 담당한다.

④ X: 사용자 인증 프로토콜은 **서버에 사용자를 인증**하며, 서버 인증은 전송계층 프로토콜의 역할이다. 전송계층 프로토콜은 서버 인증뿐 아니라 기밀성·무결성도 제공한다. 전방향 안전성은 장기 비밀키가 나중에 노출되어도 과거 세션의 통신 비밀이 보호되는 성질로, 전송계층의 키 교환과 관련된다.

NoteBase

문 13. 유럽의 국가들에 의해 제안된 것으로 자국의 정보보호 시스템을 평가하기 위하여 제정된 기준은?

① TCSEC

② ITSEC

③ PIMS

④ ISMS-P

정답 2번

간단한 해설

ITSEC는 **유럽 국가들이 공동으로 마련한 정보기술 보안 평가 기준**으로, 정보기술 제품이나 시스템의 보안성을 평가하는 데 사용된다.

공통 해설

ITSEC(Information Technology Security Evaluation Criteria)는 영국·프랑스·독일·네덜란드가 공동으로 마련한 정보기술 보안 평가 기준이다. 정보기술 제품이나 시스템의 보안성을 평가하기 위한 것이므로, 문제의 **'유럽 국가들이 제안한 시스템 평가 기준'**이라는 설명에 해당한다.

같은 기준으로 후보를 구별하면, TCSEC는 미국에서 마련한 시스템 보안 평가 기준이라는 점에서 제안 지역이 다르다. PIMS와 ISMS-P는 국내 조직의 개인정보보호 또는 정보보호·개인정보보호 **관리체계 인증**에 관한 제도이므로, 유럽의 시스템 보안 평가 기준이라는 조건에 해당하지 않는다.

NoteBase

문 14. 「개인정보 보호법」 제3조(개인정보 보호 원칙)에 대한 설명으로 옳지 않은 것은?

① 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.

② 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.

③ 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 비공개로 하여야 하며, 열람청구권 등 정보주체의 권리를 보장하여야 한다.

④ 개인정보를 익명 또는 가명으로 처리하여도 개인정보 수집목적을 달성할 수 있는 경우 익명처리가 가능한 경우에는 익명에 의하여, 익명처리로 목적을 달성할 수 없는 경우에는 가명에 의하여 처리될 수 있도록 하여야 한다.

정답 3번

①

개인정보처리자는 처리 목적을 명확히 하고, **그 목적에 필요한 최소한의 개인정보만** 적법하고 정당하게 수집하여야 한다.

개인정보 보호법 제3조(개인정보 보호 원칙)
① 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.

②

개인정보처리자는 처리 목적에 필요한 범위에서 **개인정보의 정확성·완전성·최신성을 보장**하여야 한다.

개인정보 보호법 제3조(개인정보 보호 원칙)
③ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.

③

개인정보 처리방침 등 개인정보의 처리에 관한 사항은 **공개하여야 하며**, 열람청구권 등 정보주체의 권리를 보장하여야 한다. 선지의 '비공개'가 틀리다.

개인정보 보호법 제3조(개인정보 보호 원칙)
⑤ 개인정보처리자는 제30조에 따른 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리를 보장하여야 한다. <개정 2023.3.14>

NoteBase

④

익명 또는 가명으로 처리하여도 수집목적을 달성할 수 있다면 **익명처리를 우선**하고, **익명처리로 목적을 달성할 수 없는 경우에는 가명처리**를 하도록 하여야 한다.

개인정보 보호법 제3조(개인정보 보호 원칙)
⑦ 개인정보처리자는 개인정보를 익명 또는 가명으로 처리하여도 개인정보 수집목적을 달성할 수 있는 경우 익명처리가 가능한 경우에는 익명에 의하여, 익명처리로 목적을 달성할 수 없는 경우에는 가명에 의하여 처리될 수 있도록 하여야 한다. <개정 2020.2.4>

NoteBase

문 15. ISO/IEC 27001의 통제영역에 해당하지 않은 것은?

① 정보보호 조직

② IT 재해복구

③ 자산 관리

④ 통신 보안

정답 2번

간단한 해설

ISO/IEC 27001:2013에서 IT 재해복구는 **독립된 통제영역 명칭이 아니다**. 재해 상황에서도 정보보호를 유지하는 요구사항은 '업무연속성 관리의 정보보호 측면'에서 다룬다.

개념 구분

ISO/IEC 27001:2013 부속서 A에서 정보보호 조직(A.6), 자산 관리(A.8), 통신 보안(A.13)은 각각 **독립된 통제영역**이다. 정보보호 조직은 보안 역할과 책임 등의 조직 체계를, 자산 관리는 자산 식별과 보호 책임 등을, 통신 보안은 네트워크와 정보 전송의 보호 등을 다룬다.

IT 재해복구는 재해로 중단된 IT 시스템과 서비스를 복구하는 활동이다. 이와 관련된 통제영역은 **'업무연속성 관리의 정보보호 측면'(A.17)**이며, 위기나 재해 중에도 필요한 수준의 정보보호를 유지하도록 계획과 절차를 마련하는 내용을 포함한다. 따라서 IT 재해복구가 정보보호와 무관한 것이 아니라, 'IT 재해복구' 자체가 별도의 통제영역 명칭으로 열거되어 있지 않다는 점을 구분해야 한다.

NoteBase

문 16. 접근제어 모델에 대한 설명으로 옳지 않은 것은?

① 접근제어 모델은 강제적 접근제어, 임의적 접근제어, 역할기반 접근제어로 구분할 수 있다.

② 임의적 접근제어 모델에는 Biba 모델이 있다.

③ 강제적 접근제어 모델에는 Bell-LaPadula 모델이 있다.

④ 역할기반 접근제어 모델은 사용자의 역할에 권한을 부여한다.

정답 2번

간단한 해설

Biba 모델은 임의적 접근제어가 아니라 **무결성을 보호하는 강제적 접근제어 모델**이다. 객체 소유자가 접근 권한을 정하는 임의적 접근제어와 달리, 무결성 등급에 따른 정책으로 정보의 오염을 막는다.

선지별 해설

① O: 접근제어 모델은 접근 허용 여부를 결정하는 기준에 따라 강제적 접근제어, 임의적 접근제어, 역할기반 접근제어로 구분할 수 있다. 강제적 접근제어는 보안 등급과 시스템 정책을, 임의적 접근제어는 객체 소유자의 권한 설정을, 역할기반 접근제어는 **사용자에게 부여된 역할**을 기준으로 접근을 통제한다.

② X: Biba 모델은 **무결성을 보호하는 강제적 접근제어 모델**이다. 주체와 객체의 무결성 등급에 따라 접근을 제한하여 신뢰도가 낮은 정보가 신뢰도가 높은 정보를 오염시키는 것을 막는다. 따라서 '임의적 접근제어 모델'을 '강제적 접근제어 모델'로 고쳐야 한다.

③ O: Bell-LaPadula 모델은 **기밀성을 보호하는 강제적 접근제어 모델**이다. 주체의 보안 등급과 객체의 비밀 등급에 따른 접근 규칙을 적용하여 높은 비밀 등급의 정보가 낮은 등급으로 유출되는 것을 막는다. 무결성 보호를 목적으로 하는 Biba 모델과 보호 목표가 다르다.

④ O: 역할기반 접근제어는 **역할에 권한을 부여하고 사용자에게 역할을 할당**하는 방식이다. 사용자는 자신에게 할당된 역할을 통해 필요한 권한을 얻는다. 예를 들어 인사 담당 역할에 인사자료 조회 권한을 부여하면, 그 역할을 맡은 사용자가 해당 권한을 사용할 수 있다.

NoteBase

문 17. 운영체제에 대한 설명으로 옳지 않은 것은?

① 윈도 시스템에는 FAT, FAT32, NTFS가 있다.

② 메모리 관리는 프로그램이 메모리를 요청하면 적합성을 점검하고 적합하다면 메모리를 할당한다.

③ 인터럽트는 작동 중인 컴퓨터에 예기치 않은 문제가 발생한 것이다.

④ 파일 관리는 명령어들을 체계적이고 효율적으로 실행할 수 있도록 작업스케줄링하고 사용자의 작업 요청을 수용하거나 거부한다.

정답 4번

간단한 해설

④의 작업 스케줄링과 작업 요청의 수용·거부는 **작업 관리**의 기능이다. **파일 관리**는 파일의 생성·삭제·읽기·쓰기와 저장 공간 및 접근 권한 등을 관리한다.

선지별 해설

① O: FAT, FAT32, NTFS는 윈도에서 사용하는 **파일 시스템**이다. 파일 시스템은 저장 장치에 파일과 디렉터리를 구성하고, 파일의 저장 위치와 관련 정보를 관리하는 방식이다.

② O: 메모리 관리는 프로그램의 메모리 요청에 대해 할당 가능한 공간과 접근 권한 등을 확인하고, 적합하면 **필요한 메모리를 할당**한다. 사용이 끝난 메모리를 회수하여 다른 프로그램이 이용할 수 있게 하는 것도 메모리 관리에 포함된다.

③ O: 인터럽트는 실행 중인 작업 외에 **처리가 필요한 사건이 발생했음을 알리는 신호**로, 이를 처리할 때는 현재 실행 흐름을 잠시 멈추고 해당 처리 루틴으로 제어를 옮긴다. 선지에서 말하는 예기치 않은 문제에 대응하는 경우가 이에 포함된다. 다만 인터럽트가 반드시 고장을 뜻하는 것은 아니며, 입출력 완료처럼 정상적인 사건에 의해서도 발생한다.

④ X: 작업의 실행 순서를 정하는 스케줄링과 사용자의 작업 요청을 수용하거나 거부하는 것은 **작업 관리**의 기능이다. 파일 관리는 파일의 생성·삭제·읽기·쓰기, 디렉터리 구성, 저장 공간과 접근 권한 등을 관리한다. 즉, 선지의 '파일 관리'를 '작업 관리'로 고쳐야 한다.

NoteBase

문 18. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」의 용어에 대한 설명으로 옳지 않은 것은?

① “정보통신서비스 제공자”란 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다.

② “통신과금서비스이용자”란 정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하는 자를 말한다.

③ “전자문서”란 컴퓨터 등 정보처리능력을 가진 장치에 의하여 전자적인 형태로 작성되어 송수신되거나 저장된 문서형식의 자료로서 표준화된 것을 말한다.

④ 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위로 인하여 발생한 사태는 “침해사고”에 해당한다.

정답 2번

①

정보통신서비스 제공자에는 **전기통신사업자**뿐 아니라 **영리 목적으로 그 전기통신역무를 이용해 정보를 제공하거나 제공을 매개하는 자**도 포함된다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제2조(정의)
① 이 법에서 사용하는 용어의 뜻은 다음과 같다. <개정 2004.1.29, 2007.1.26, 2007.12.21, 2008.6.13, 2010.3.22, 2014.5.28, 2020.6.9, 2026.1.6>
3. "정보통신서비스 제공자"란 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다.

②

통신과금서비스이용자는 통신과금서비스제공자로부터 **통신과금서비스를 이용하여 재화나 용역을 구입·이용하는 자**이다. 단순히 정보통신서비스를 이용하는 ‘이용자’와 구별된다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제2조(정의)
① 이 법에서 사용하는 용어의 뜻은 다음과 같다. <개정 2004.1.29, 2007.1.26, 2007.12.21, 2008.6.13, 2010.3.22, 2014.5.28, 2020.6.9, 2026.1.6>
4. "이용자"란 정보통신서비스 제공자가 직접 제공하거나 게재자를 통하여 제공되는 정보통신서비스 또는 정보를 이용하는 자를 말한다.
12. "통신과금서비스이용자"란 통신과금서비스제공자로부터 통신과금서비스를 이용하여 재화등을 구입 · 이용하는 자를 말한다.

NoteBase

③

전자문서는 정보처리능력을 가진 장치로 전자적으로 작성되어 송수신되거나 저장된 문서형식의 자료 중 **표준화된 자료**를 말한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제2조(정의)
① 이 법에서 사용하는 용어의 뜻은 다음과 같다. <개정 2004.1.29, 2007.1.26, 2007.12.21, 2008.6.13, 2010.3.22, 2014.5.28, 2020.6.9, 2026.1.6>
5. "전자문서"란 컴퓨터 등 정보처리능력을 가진 장치에 의하여 전자적인 형태로 작성되어 송수신되거나 저장된 문서형식의 자료로서 표준화된 것을 말한다.

④

해킹·컴퓨터바이러스·논리폭탄·메일폭탄·서비스거부·고출력 전자기파 등의 방법으로 **정보통신망 또는 관련 정보시스템을 공격하여 발생한 사태**가 침해사고이다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제2조(정의)
① 이 법에서 사용하는 용어의 뜻은 다음과 같다. <개정 2004.1.29, 2007.1.26, 2007.12.21, 2008.6.13, 2010.3.22, 2014.5.28, 2020.6.9, 2026.1.6>
7. "침해사고"란 다음 각 목의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위로 인하여 발생한 사태를 말한다.
가. 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스거부 또는 고출력 전자기파 등의 방법

NoteBase

문 19. 스니핑 공격에 대한 설명으로 옳지 않은 것은?

① 스위치에서 ARP 스푸핑 기법을 이용하면 스니핑 공격이 불가능하다.

② 모니터링 포트를 이용하여 스니핑 공격을 한다.

③ 스니핑 공격 방지책으로는 암호화하는 방법이 있다.

④ 스위치 재밍을 이용하여 위조한 MAC 주소를 가진 패킷을 계속 전송하여 스니핑 공격을 한다.

정답 1번

간단한 해설

ARP 스푸핑은 **IP 주소와 MAC 주소의 대응 관계를 속여** 다른 호스트로 갈 트래픽을 공격자에게 유도하는 기법이다. 따라서 스위치 환경에서도 이를 이용한 **스니핑이 가능하다**.

선지별 해설

① X: ARP는 같은 네트워크에서 IP 주소에 대응하는 MAC 주소를 알아내는 프로토콜이다. ARP 스푸핑은 위조된 ARP 정보를 보내 피해자의 ARP 캐시에 상대방 IP 주소와 공격자 MAC 주소가 대응하도록 만드는 기법이다. 그러면 상대방에게 보낼 트래픽이 공격자에게 전달되어 내용을 엿볼 수 있다. 따라서 '스니핑 공격이 불가능하다'는 **'스니핑 공격이 가능하다'**로 고쳐야 한다.

② O: 스위치의 모니터링 포트는 지정한 포트나 VLAN을 지나는 **트래픽의 복사본을 받는 포트**이다. 이 포트에 연결된 장비는 다른 호스트의 통신을 수집할 수 있으므로, 공격자가 이를 이용하면 스니핑이 가능하다.

③ O: 통신 내용을 암호화하면 공격자가 패킷을 수집하더라도 복호화에 필요한 키 없이는 원래 내용을 알아내기 어렵다. 암호화는 **패킷 수집 자체를 막기보다 내용의 노출을 방지**하므로 스니핑 피해를 줄이는 대책이다.

④ O: 스위치 재밍은 서로 다른 위조 출발지 MAC 주소를 가진 프레임을 대량으로 보내 스위치의 MAC 주소 테이블을 가득 채우는 공격이다. 정상 주소를 충분히 학습하지 못하면 **목적지 MAC 주소를 모르는 프레임**이 같은 VLAN의 다른 포트들로 플러딩될 수 있다. 공격자는 자신의 포트로도 전달되는 트래픽을 수집하여 스니핑할 수 있다.

NoteBase

문 20. 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」에서 인증심사원에 대한 설명으로 옳지 않은 것은?

① 인증심사원의 자격 유효기간은 자격을 부여 받은 날부터 3년으로 한다.

② 인증심사 과정에서 취득한 정보 또는 서류를 관련 법령의 근거나 인증신청인의 동의 없이 누설 또는 유출하거나 업무목적 외에 이를 사용한 경우에는 인증심사원의 자격이 취소될 수 있다.

③ 인증위원회는 자격 유효기간 동안 1회 이상의 인증심사를 참여한 인증심사원에 대하여 자격유지를 위해 자격 유효기간 만료 전까지 수료하여야하는 보수 교육시간 전부를 이수한 것으로 인정할 수 있다.

④ 인증심사원의 등급별 자격요건 중 선임심사원은 심사원 자격취득자로서 정보보호 및 개인정보보호 관리체계 인증심사를 3회 이상 참여하고 심사일수의 합이 15일 이상인 자이다.

정답 3번

①

인증심사원 자격은 **자격을 부여받은 날부터 3년간** 유효하다.

정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시 제15조(인증심사원 자격 유지 및 갱신)
① 인증심사원의 자격 유효기간은 자격을 부여 받은 날부터 3년으로 한다.

②

심사 중 취득한 정보·서류를 법령상 근거나 인증신청인의 동의 없이 누설·유출하거나 업무 목적 외에 사용하면, 한국인터넷진흥원은 **인증심사원 자격을 취소할 수 있다**.

정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시 제16조(인증심사원 자격 취소)
① 인터넷진흥원은 다음 각 호의 어느 하나에 해당하는 사유를 발견한 경우 인증심사원의 자격을 취소할 수 있다.
4. 인증심사 과정에서 취득한 정보 또는 서류를 관련 법령의 근거나 인증신청인의 동의 없이 누설 또는 유출하거나 업무목적 외에 이를 사용한 경우

③

보수교육 이수 인정의 주체는 **한국인터넷진흥원**이다. 자격 유효기간 중 인증심사에 1회 이상 참여한 경우, **보수교육 시간 중 일부**를 이수한 것으로 인정할 수 있다.

정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시 제15조(인증심사원 자격 유지 및 갱신)
③ 인터넷진흥원은 자격 유효기간 동안 1회 이상의 인증심사를 참여한 인증심사원에 대하여 제2항의 보수교육 시간 중 일부를 이수한 것으로 인정할 수 있다.

NoteBase

④

선임심사원은 **심사원 자격을 취득한 뒤 정보보호 및 개인정보보호 관리체계 인증심사에 3회 이상 참여**하고, **심사일수의 합이 15일 이상**이어야 한다.

[별표 3]

인증심사원 등급별 자격 요건(제12조 관련)

https://d2u7om5rih5x7z.cloudfront.net/ox-images/drive-repair/1ot-uzsr61uPfDcGz1y59xfBrVRMmxY5l.webp

※ 인터넷진흥원은 인증심사원의 인증심사 능력에 따라 매년 책임심사원을 지정할 수 있다.

NoteBase