2022년 국가직 9급 정보보호론 풀이

by 호이호이꿀떡

정답 체크

01	02	03	04	05	06	07	08	09	10
③	①	②	①	①	④	②	④	③	③
11	12	13	14	15	16	17	18	19	20
④	①	②	③	②	②	④	②	①	③

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

① 무결성
② 기밀성
③ 인증성
④ 가용성

③ 인증에 대한 설명이다.

<오답 체크> ① 무결성은 권한이 없는 사용자는 데이터의 수정이 불가능하다는 것을 의미한다.

② 기밀성은 권한이 없는 사용자는 데이터 열람이 불가능하다는 것을 의미한다.

④ 가용성은 정당한 권한이 있는 사용자는 원하는 시간에 서비스를 정상적으로 이용할 수 있어야 하는 것을 의미한다.

답 ③

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.

① TCP는 연결지향형 프로토콜이며, 비연결 지향 프로토콜은 UDP이다.

<오답 체크> ②④ TCP는 **SYN ⇨ SYN+ACK ⇨ ACK**의 3단계를 거쳐 연결을 설정하는데, 이것을 3-way handshaking이라 한다. TCP의 이러한 3-way handshaking 과정의 헛점을 이용한 DoS 공격이 **SYN flooding**(SYN 플러딩)으로, 공격 대상 서버에 존재하지 않는 IP 주소로 위조한 무수히 많은 SYN패킷을 보낸 뒤 서버로부터 오는 SYN+ACK패킷을 무시하여, 서버가 SYN Received 상태로 끊임없이 기다리게 만드는 공격방법이다.

◈ **TCP**의 특징: 연결지향적, 신뢰성 있는 전송, 흐름 제어, 혼잡 제어, 에러 검출 등
◈ **UDP**의 특징: 비연결성, 신뢰성 없음, 흐름 제어 없음, 혼잡 제어 없음, 확인응답 없음, 오류 검출 기능 부족 (최소한의 검사합 기능은 있음)

답 ①

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.

② **디피 헬만 키 교환**(Diffie–Hellman key exchange) 알고리즘은 이산대수 계산의 어려움을 이용하여, 두 송수신자 간 공통의 비밀키(대칭키)를 생성하기 위한 알고리즘이다.
흔히, 디피 헬만 알고리즘을 통해 나와 상대방이 같은 대칭키(비밀키)를 생성하기 때문에, 디피 헬만이 대칭키 암호 알고리즘이라고 오해하는 경우가 있는 것을 이용한 작은 함정 문제이다.
디피 헬만 알고리즘은 '대칭키(비밀키)'를 교환하기 위한 수단일 뿐, 디피 헬만 알고리즘 자체는 공개키를 이용한 비대칭키 암호 알고리즘과 유사하다.

<오답 체크> ① 암·복호화 속도는 대칭키 방식이 훨씬 빠르다.
③ 대표적인 타원 곡선 암호 알고리즘은 ECC, ECDSA가 있으며, 이들은 모두 비대칭키 암호 알고리즘이다.
④ 인증서에는 소유자(발행자)의 공개키가 포함된다.

✠ **대칭키 암호 알고리즘**
DES, 3-DES, IDEA, AES, RC5, RC6, Skipjack, Blowfish
(국산) SEED, HIGHT, ARIA, LEA, LSH

✠ **비대칭키 암호(공개키 암호) 알고리즘**
RSA : 소인수분해
Rabin : 소인수분해
ElGamal : 이산대수
ECC : 타원곡선 상의 이산대수
Schnorr : 이산대수, ElGamal에 기반, 짧은 키 길이
DSA : 이산대수, Schnorr의 응용
DSS : 이산대수, 전자서명 전용
ECDSA : 내부적으로 타원곡선
Knapsack : 부분집합의 합을 구하는 문제
(NP-complete 문제)
KCDSA : 국산, 국내표준
ECKDSA : 국산, 내부적으로 타원곡선, 소규모, 무선

답 ②

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.

① **세션 하이재킹**(Session Hijacking) 공격
시스템에 접근할 적법한 사용자 아이디와 패스워드를 모를 때, 이미 시스템에 접속되어 세션이 연결되어 있는 사용자의 세션을 가로채기 하는 공격이다.
서버가 기존 클라이언트와 통신을 하고 있는 도중에, 공격자가 서버로 RST 패킷을 보내 강제로 연결을 끊는다. 그리고 재빨리 적당한 순서의 시퀀스 넘버를 생성하여 서버로 보내면, 서버는 공격자가 보낸 시퀀스 넘버를 정상적인 것으로 받아들여 다시 세션을 연결하여 공격자와 서버 간의 연결이 확립된다.

<오답 체크> ② **DoS**(Denial of Service, 서비스 거부 공격)에 대한 설명이다. DoS는 목표 시스템이 정상적으로 처리할 수 있는 것보다 많은 양의 자원을 보내, 시스템 자원을 고갈시켜 마비시키는 공격이다.
③ **버퍼 오버플로우**(Buffer Overflow) 공격에 대한 설명이다.
버퍼 오버플로우란, 입력받은 값이 미리 할당된 버퍼를 초과하여 주변 다른 메모리 영역을 침범하는 현상을 말하는데, 이는 데이터의 길이를 명확히 정의하지 않아 버퍼 영역을 초과하는 데이터를 입력 받아 발생하는 문제이다.
이를 악용하여 강제로 다른 메모리 영역에 데이터를 덮어씌우는 것이 버퍼 오버플로우 공격이다.
④ **랜섬웨어**(Ransomware)에 대한 설명이다.
랜섬웨어는 컴퓨터를 감염시켜 사용자의 파일을 암호화한 뒤 인질로 잡아 금전을 요구하는 악성 프로그램이다.

답 ①

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.

① **FRR**은 정당한 권한이 있는 사용자가 인증에 실패할 확률로, 정당한 사용자인데 판단을 잘못(False)하여 거부(Rejection)하는 것으로 이해하면 된다.

<오답 체크> ③ 생체 인식 정보 기술에 쓰이는 신체적 특성으로는 지문, 홍채, 얼굴, 정맥 등이 있으며 행동적 특성으로는 목소리, 서명 등이 있다.

④ **FAR**은 권한이 없는 사용자가 인증에 성공할 확률로, 정당하지 않은 사용자인데 판단을 잘못(False)하여 승인(Acceptance)하는 것으로 이해하면 된다.

▶ **FRR**(False Rejection Rate, 오거부율): 정당한 권한이 있는 사용자가 인증에 실패할 확률
▶ **FAR**(False Acceptance Rate, 오인식률): 권한이 없는 사용자가 인증에 성공할 확률
▶ **CER**(Crossover Error Rate) 또는 **EER**(Equal Error Rate): FRR과 FAR의 교차점

답 ①

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.

◈ **CTR**(Counter, 카운터) 모드
1씩 증가하는 카운터 값을 암호화하여 스트림 암호를 생성한 후, 생성한 스트림 암호와 평문 블록을 XOR하여 암호문 블록을 생성한다.

④ 카운터 모드는 스트림 암호를 생성할 때나 평문 블록과 결합할 때, 다른 블록과 연관되지 않아 모두 독립적으로 처리가 가능하다. 따라서 순차적으로 암·복호화를 할 필요 없이, 병렬처리가 가능하고 오류 전파가 없다.

<오답 체크> ① 암호화·복호화 모두 생성한 스트림 암호화 평문 블록을 XOR하여 처리하는 방식이다.

② 병렬 처리가 가능하기 때문에 동시에 처리 가능한 블록 개수에 따라 처리속도가 결정된다.

답 ④

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.

◈ AES(Advanced Encryption Standard)
SPN구조
블록 128비트(16바이트) – **라운드 키** 128비트
키 길이 128비트 – 10라운드
키 길이 192비트 – 12라운드
키 길이 256비트 – 14라운드

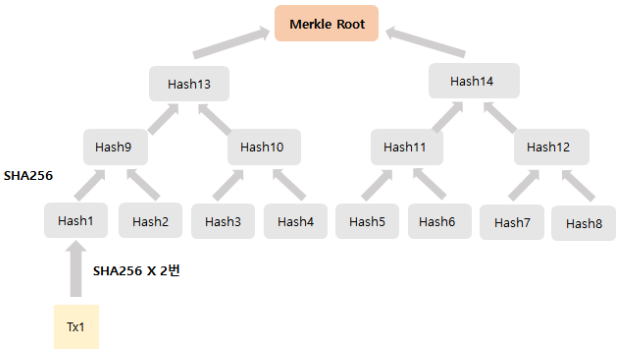
② AES는 각 단계에서 바이트 치환(SubBytes), 행 이동(ShiftRows), 열 혼합(MixColumns), 키 덧셈(AddRoundKey)의 4단계를 거친다.
단, **마지막 단계**에서는 열 혼합을 제외한 **3단계만 수행**한다.

<오답 체크> ① 미국 상무성(NIST)에서 주최한 알고리즘 공모에서 대먼과 리즈먼이 제출한 Rijndael이 최종 선정되었다.

답 ②

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.



【머클 트리 구조】

머클 트리(Merkle Tree)는 이진 트리 구조로 되어있으며, 최하위 노드는 각 거래의 해시(hash)값으로 구성되어 있으며, 상위 노드는 하위 노드 두 개를 합친 데이터의 해시값을 가진다.
위 그림을 예로 들면, 거래1(Tx1)을 SHA-256으로 변환한 해시값이 Hash1이 되고, 거래2의 해시값은 Hash2가 된다.
그리고 Hash1과 Hash2를 합친 데이터의 해시값은 상위노드 Hash9가 되고, 이렇게 반복 계산하여 나오는 최상위 노드의 값을 **머클 루트**(Merkle Root)라고 한다.
머클트리는 SHA-256 알고리즘을 통해 해시값을 계산한다.

④ 비트코인의 블록 헤더 구조는 버전, 해시 포인터, 머클 루트, 타임스탬프, 난이도 목표, 넌스(nonce) 값으로 구성되어 있다.
버전, 타임스탬프, 난이도 목표, 넌스 값의 필드 크기는 4비트이고, 해시 포인터, 머클 루트의 필드 크기는 32비트이다.

답 ④

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.

③ 고객등록 단계는 고객이 상품 구매를 위해 구매정보를 전송하는 단계이다.(주문 내역이 담긴 **주문정보**, 결제수단 정보가 담긴 **지불정보**, 자신을 증명할 **인증서**)
이 때, 고객이 구매정보를 보내는 상대방은 지불 게이트웨이가 아니라, 판매자이다. 고객은 주문정보, 지불정보, 인증서를 모두 판매자에게만 전송한 뒤, 판매자가 지불정보와 인증서를 다시 지불 게이트웨이에 전달하는 방식이다.

답 ③

✠ **SET**(Secure Electronic Transaction) 절차
① 인증서 수신(고객)
고객은 판매자를 검증하기 위해 판매자와 지불 게이트웨이(PG, Payment Gateway)의 인증서 수신
② 구매요청(고객)
고객은 자신의 주문정보, 지불정보, 인증서를 판매자에게 전송하여 구매 요청
고객의 주문정보는 판매자의 공개키(하이브리드 암호 방식)를 이용해 암호화하여 은행은 보지 못하게 하고, 지불정보는 은행의 공개키(하이브리드 암호 방식)를 이용해 암호화하여 판매자가 보지 못하게 한다.
③ 지불정보와 인증서 PG에 전송(판매자)
판매자는 고객인증서를 확인한 후 주문정보는 자신이 보유하고 고객의 지불정보와 고객 및 판매자 인증서를 PG에 전송
이때 고객의 지불정보는 암호화되어 있기 때문에 판매자는 알 수 없음
④ 신용카드 결제 승인 요청(PG)
PG는 고객과 판매자의 인증서를 확인 후, 지불정보를 해당 금융기관이 이용 가능하도록 복호화하여 신용카드 결제 승인 요청
⑤ 승인여부 PG에 전송(금융기관)
금융기관은 고객의 신용한도를 고려하여 승인 여부 전송
⑥ 승인여부 판매자에 전송(PG)
PG는 승인 여부를 판매자에게 전송
⑦ 주문처리(판매자)
판매자는 PG의 응답에 따라 고객 주문 처리

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.

③ 수탁자는 개인정보처리자로부터 위탁받은 해당 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 **제공하여서는 아니 된다.** (「개인정보 보호법」 제26조 ⑤항)

<오답 체크> ①「개인정보 보호법」 제26조 ③항

②「개인정보 보호법」 제26조 ④항

④「개인정보 보호법」 제26조 ⑥항

제26조(업무위탁에 따른 개인정보의 처리 제한)

① 개인정보처리자가 제3자에게 개인정보의 처리 업무를 위탁하는 경우에는 다음 각 호의 내용이 포함된 문서에 의하여야 한다.

1. 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
2. 개인정보의 기술적·관리적 보호조치에 관한 사항
3. 그 밖에 개인정보의 안전한 관리를 위하여 대통령령으로 정한 사항

② 제1항에 따라 개인정보의 처리 업무를 위탁하는 개인정보처리자(이하 "위탁자"라 한다)는 위탁하는 업무의 내용과 개인정보 처리 업무를 위탁받아 처리하는 자(이하 "수탁자"라 한다)를 정보주체가 언제든지 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다.

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.

④ 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.

⑤ 수탁자는 개인정보처리자로부터 위탁받은 해당 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공하여서는 아니 된다.

⑥ 수탁자가 위탁받은 업무와 관련하여 개인정보를 처리하는 과정에서 이 법을 위반하여 발생한 손해배상책임에 대하여는 수탁자를 개인정보처리자의 소속 직원으로 본다.

⑦ 수탁자에 관하여는 제15조부터 제25조까지, 제27조부터 제31조까지, 제33조부터 제38조까지 및 제59조를 준용한다.

답 ③

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.

④ IPv6에는 기존 IPv4에 있던 브로드캐스트 주소 방식 대신 애니캐스트 주소 방식이 도입되었다.
유니캐스트, 멀티캐스트 주소 방식은 IPv4, IPv6 모두 사용
<오답 체크> ② IPv6는 16bit씩 8자리, 총 128bit(16byte)의 길이를 가진다.

▷ **유니캐스트** 주소(Unicast Address) 1 대 1로 데이터 전송
▷ **멀티캐스트** 주소(Multicast Address) 1 대 다수로, 특정한 여러 노드로 데이터 전송
▷ **브로드캐스트** 주소(Broadcast Address) 1 대 다수로, 불특정한 여러 노드로 또는 해당 네트워크의 모든 노드로 데이터를 전송 (IPv4에서만 사용)
▷ **애니캐스트** 주소(Anycast Address) 같은 서비스를 하는 여러 개의 서버가 같은 애니캐스트 주소를 가질 수 있으며, 가장 효율적으로 서비스할 수 있는 또는 가장 근접한 서버가 데이터를 전송 (IPv6에서만 사용. 일부 IPv4에서 가능하기는 하나, 시험 이론에서는 IPv6에서 도입된 것으로 알고 있자.)

답 ④

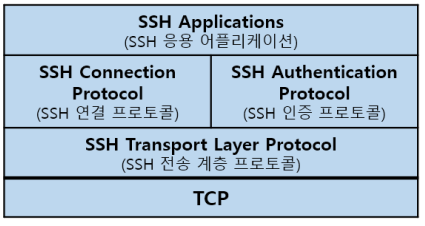
문 12. SSH를 구성하는 프로토콜에 대한 설명으로 옳은 것은?

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.

① SSH는 연결, (사용자)인증, 전송 계층의 3개의 프로토콜로 구성된다.
<오답 체크> ② 사용자 인증 프로토콜에 대한 설명
③ 연결 프로토콜에 대한 설명
④ 전송 계층 프로토콜에 대한 설명
전방향 안전성(forward-secrecy)이란 사용자와 서버들의 비밀키가 노출되더라도 그 이전에 전송된 암호문을 쉽게 복호화할 수 없도록 하는 것을 의미한다.

▶ SSH의 구성

● **SSH 프로토콜 구조**



▷ SSH 연결 프로토콜
암호화된 터널들 각각에 다수 논리채널들을 다중화 (1:N) 가능
▷ SSH (사용자) 인증 프로토콜
해당 서버에 대한 사용자 인증(User Authentication) 제공
▷ SSH 전송 계층 프로토콜
서버 인증, 기밀성, 무결성, 압축(옵션) 제공
주요 협상 대상 : 키 교환 방식, 공개 키 방식, 대칭 키 방식, 메세지 인증 방식, 해시 알고리즘 등이 클라이언트,서버 간에 협상되어짐
● SSH 응용 어플리케이션 : TELNET,RLOGIN,SMTP 등

답 ①

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

① TCSEC
② ITSEC
③ PIMS
④ ISMS-P

② **ITSEC**(Information Technology Security Evaluation Criteria)
유럽의 정보보호 시스템 평가 제도
기밀성, 무결성, 가용성을 다룬다.
보안등급을 E6(최고)~E1(최저)까지 6등급으로 구분하며, E0은 부적합에 해당한다.

<오답 체크> ① **TCSEC**(Trusted Computer System Evaluation Criteria)
미국의 정보보호 시스템 평가 제도
컴퓨터시스템의 구축과 평가 등에 관한 지속적인 연구 결과로 미국 국방부 내 NCSC(미국 컴퓨터 보안 센터) 주도하에 1983년에 제정되었으며, 소위 'Orange Book'으로 불린다.

③ **PIMS**(개인정보보호 관리체계인증)
개인정보를 보호하는 것에 중점을 둔 관리체계 인증제도.
기관 및 기업이 개인정보보호 관리체계를 갖추고 체계적 · 지속적으로 보호 업무를 수행하는지에 대해 객관적으로 심사하여 기준 만족 시 인증을 부여한다.

④ **ISMS-P**(정보보호 및 개인정보보호 관리체계 인증)
기존의 ISMS와 PIMS를 통합한 것으로, 정보보호 및 개인정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 인터넷진흥원 또는 인증기관이 증명하는 제도로, 2018년 말부터 시행되었다.

답 ②

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.

③ 개인정보 처리방침 등 개인정보의 처리에 관한 **사항을 공개하여야 하며**, 열람청구권 등 정보주체의 권리를 보장하여야 한다. (「개인정보 보호법」 제3조 ⑤항

<오답 체크> ①「개인정보 보호법」 제3조 ①항
②「개인정보 보호법」 제3조 ③항
④「개인정보 보호법」 제3조 ⑦항

제3조(개인정보 보호 원칙)
① 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.
② 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.
③ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.
④ 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리하여야 한다.
⑤ 개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리를 보장하여야 한다.
⑥ 개인정보처리자는 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.
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.
⑧ 개인정보처리자는 이 법 및 관계 법령에서 규정하고 있는 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력하여야 한다.

답 ③

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

① 정보보호 조직
② IT 재해복구
③ 자산 관리
④ 통신 보안

통제 영역	항목 수	내용
정보보안 정책 (Information security policies)	2	정보보호에 대한 경영방침과 지원 사항을 제공하기 위함
정보보안 조직 (organizing information security)	7	조직 내에서 보호를 효과적으로 관리하기 위해서는 보호에 대한 책임을 배정
인원 보안 (Human resource policity)	6	사람에 의한 실수, 절도, 부정수단이나 설비의 잘못 사용으로 인한 위험을 감소
자산 관리 (Asset management)	10	조직의 자산에 대한 적절한 보호책 유지
접근 통제 (Access control)	13	정보에 대한 접근통제를 하기 위함
암호화 (Cryptography)	2	기밀성, 인증 또는 정보의 무결성을 보호하기 위해 암호화의 적절하고 효과적인 사용을 보장
물리적 환경적 보안 (Physocal & environmental security)	15	비인가된 접근, 손상과 사업장에 대한 영향을 방지하기 위함
운영 보안 (Operation security)	15	정보처리 설비의 정확하고 안전한 운영을 보장하기 위함
통신 보안 (Communication security)	7	네트워크 및 지원 정보처리 시설의 안전한 통신을 보장하기 위함
시스템 취득, 개발, 유지보수 (System acquisition, development & maintenance)	13	정보시스템 내에 보안이 수립되었음을 보장하기 위함
협력업체(공급자) 관리 (Supplier relationships)	5	협력업체(공급자)에게 접근가능한 조직 내 정보보호 보장과 협력업체와의 계약에 따라 정보보안 및 서비스 제공에 합의된 수준을 유지하기 위함
보안사고 관리 (Information security incident management)	7	보안사고에 대한 대응 절차의 수립 및 이행을 보장
사업연속성 관리의 정보보안 측면 (Information security aspects of business continuity management)	4	사업활동에의 방해요소를 완화시키며 주요 실패 및 재해의 영향으로부터 주요 사업 활동을 보호하기 위함
준거성 (Compliance)	8	범죄 및 민사상의 법률, 법규, 규정 또는 계약 의무사항 및 보보흉구사항의 불일치를 방지하기 위함

답 ②

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.

✠ **강제적 접근 제어**(MAC, Mandatory Access Control)
오직 관리자만이 객체과 자원들에 대한 접근 권한을 부여할 수 있다. 자원에 대한 접근은 주어진 보안레벨에 기반한다.
관리자가 규칙을 작성하기 때문에 **규칙 기반 접근 제어**(Rule Based Access Control)이라고도 한다.
BLP(BELL-LaPadula, 벨 라파듈라) 모델, **Biba**(비바) 모델, **클락-윌슨**(Clark-Wilson) 모델, **만리장성** 모델 등이 있다.
✠ **임의적 접근 제어**(DAC, Discretionary Access Control)
정보의 소유자가 보안 등급을 결정하고 이에 대한 정보의 접근 제어를 설정하는 모델로, 접근 권한을 객체의 소유자가 임의로 지정하는 방식이다
✠ **역할 기반 접근 제어**(RBAC, Role Based Access Control)
정보에 대한 사용자의 접근을 개별적인 신분이 아니라 조직 내 개인 역할에 따라 허용 여부를 결정하는 모델

② 비바(Biba) 모델은 강제적 접근 제어 모델이다.

답 ②

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.

④ 명령어들을 작업스케줄링하고 사용자의 요청을 수용·거부하는 건 프로세스 관리에 관한 설명이다.
파일 관리는 파일과 디렉터리를 생성 관리하고, 각 파일과 디렉터리에 대해 사용자별로 접근권한을 부여 및 관리하는 것을 말한다.

<오답 체크> ③ 작동중인 컴퓨터에 예기치 않은 문제가 발생하였다는 말이, 반드시 시스템 장애 발생이나 외부의 물리적인 충격만 의미하는 것은 아니다. 다른 작업 처리 도중 새로운 요청이 발생하여 처리되도록 프로그래밍된 것들까지 모두 포함하는 개념이다.
"예기치 않은 문제가 발생"이라는 표현이 전혀 적절하지는 않지만, 국내 이론서에는 그렇게 정의되어 있으니 그냥 그렇다고 알고 넘어가자.

● **윈도우의 파일 시스템**
FAT(File Allocation Table, **파일 할당 테이블**)과 NTFS(New Technology File System)는 **윈도우에서 사용하는 파일 시스템 종류**
FAT는 FAT12와 FAT16, FAT32가 있는데, 뒤의 숫자는 **클러스터를 표현하는 비트 수를 의미한다.**
클러스터(cluster)란 컴퓨터 하드디스크에서 사용하는 논리적 단위로, 파일은 클러스터 여러 개로 이루어진다.
FAT12의 12비트로 클러스터를 표현하므로, 최대 클러스터 수는 4,084개 ($2^{12}-12$)
FAT16는 65,524개 ($2^{16}-12$)
FAT32는 268,435,444개 ($2^{28}-12$)
(FAT32에서 28비트만 사용하는 이유는 4비트가 사전에 예약되어 다른 용도로 사용되기 때문이다.)
NTFS(New Technology File System) 방식은 대용량 하드, 압축, 보호, 백업, 로그 등의 기능을 지원하며, 파일과 폴더 별로 개별 관리가 가능하다.

답 ④

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

① "정보통신서비스 제공자"란 「전기통신사업법」 제2조 제8호에 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, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위로 인하여 발생한 사태는 "침해사고"에 해당한다.

⇨ 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 약칭 「정보통신망법」이라 부르겠다.

② 단어 그대로, (정보통신서비스)이용자에 대한 설명이다.
통신과금서비스이용자는 **통신과금서비스를 이용**하는 자를 말한다.
▶ "이용자"란 정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하는 자를 말한다. (「정보통신망법」 제2조 제①항 제4호)
▶ "통신과금서비스이용자"란 통신과금서비스제공자로부터 통신과금서비스를 이용하여 재화등을 구입 · 이용하는 자를 말한다. (「정보통신망법」 제2조 제①항 제12호)

<오답 체크> ①「정보통신망법」 제2조 제①항 제3호
③「정보통신망법」 제2조 제①항 제5호
④「정보통신망법」 제2조 제①항 제7호

답 ②

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.

▷ **스니핑**(sniffing)
다른 상대방들의 패킷 교환을 엿듣는 것으로, 소극적 공격에 해당한다.

① 문장 표현이 좀, 아니 많이 이상하다.
스위치에서 ARP 스푸핑 기법을 이용하여 스니핑 공격을 막겠다는 건지, 스위치에 접근하여 ARP 스푸핑을 이용하더라도 스니핑 공격이 불가능하다는 건지 말 뜻이 이해가 잘 안 간다.
단, 스위치와 그 하위 네트워크에서 ARP 스푸핑 기법을 이용하여 스니핑 공격이 가능하므로 어떻게 해석해도 틀린 표현이긴 하다.

▶ **ARP Spoofing**(ARP 스푸핑)
공격자가 자신의 MAC 주소를 공격 대상의 MAC 주소로 바꾸어 마치 자신이 공격 대상인 척 속이는 공격이다.
공격자는 클라이언트와 서버 사이의 패킷을 읽고 확인한 후 정상적인 목적지로 향하도록 다시 돌려보내 연결이 유지되도록 한다.
스위치 장비에는 각 클라이언트들의 MAC 주소와 IP 정보를 담고 있으므로, 스위치에 입력되어 있는 MAC 주소를 조작하여 스니핑 공격이 가능하다.

<오답 체크> ② **모니터링 포트**(Monitoring Port)란 스위치 장비에서 제공하는 포트로, 본래는 관리 목적으로 스위치를 통화하는 모든 패킷의 내용을 복제해 전달하여, 네트워크 사용량, 응답 시간 등 장비 성능을 관리하기 위한 포트이다.
그런데 이 포트를 악용해, 공격자가 모니터링 포트에 접근할 수 있다면 모든 패킷에 대한 스니핑이 가능해진다.

③ 스니핑은 네트워크에 흐르는 패킷을 몰래 염탐하는 것으로, 암호화를 확실히 한다면 예방할 수 있다.

④ **스위치 재밍**(jamming)
위조된 MAC 주소를 지속적으로 보내 스위치가 관리하는 매핑 테이블을 넘치게 만드는 스니핑 기법이다.
스위치는 매핑 테이블이 가득 차게 되면, 스위치는 브로드캐스팅(broadcasting) 모드로 전환하게 되어 스니핑이 가능해진다.

답 ①

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 보수교육시간 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.

③ 교육시간 전부가 아닌 **일부**를 이수한 것으로 인정할 수 있다.

제15조(인증심사원 자격 유지 및 갱신)
② 인증심사원은 자격유지를 위해 자격 유효기간 만료 전까지 인터넷진흥원이 인정하는 보수교육을 수료하여야 한다.
③ 인터넷진흥원은 자격 유효기간 동안 1회 이상의 인증심사를 참여한 인증심사원에 대하여 제2항의 **보수교육 시간 중 일부를 이수한 것으로 인정**할 수 있다.

<오답 체크> ①「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」제15조 제①항
②「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」제16조 제①항 제4호
④ 제12조(인증심사원의 자격 요건 등) 인증심사원은 심사원보, 심사원, 선임심사원으로 구분하며 등급별 자격 요건은 **별표 3**과 같다.

별표3 (인증심사원 등급별 자격 요건)
▷ **심사원보** : 인증심사원 자격 신청 요건을 만족하는 자로서 인터넷진흥원이 수행하는 인증심사원 양성과정 통과하여 자격을 취득한 자
▷ **심사원** : 심사원보 자격 취득자로서 인증심사에 4회 이상 참여하고 심사일수의 합이 20일 이상인 자
▷ **선임심사원** : 심사원 자격 취득자로서 정보보호 및 개인정보보호 관리체계 인증심사를 3회 이상 참여하고 심사일수의 합이 15일 이상인 자

답 ③