정보보호론 (국가직9급 2022년 4월 2일 시행)

문 1. 사용자의 신원을 검증하고 전송된 메시지의 출처를 확인하는 정보보호 개념은? 3
① 무결성
② 기밀성
③ 인증성
④ 가용성
[해설]
- 인증성(Authentication)
① 정보시스템 상에서 이루어진 어떤 활동이 정상적이고 합법적으로 이루어진 것을 보장하는 것이다.
② 정보에 접근할 수 있는 객체의 자격이나 객체의 내용을 검증하는데 사용하는 것으로 정당한 사용자인지를 판별한다.
③ 인증성이 결여될 경우에는, 사기, 산업스파이 등 부정확한 정보를 가지고 부당한 처리를 하여 잘못된 결과를 가져올 수 있다.

문 2. TCP에 대한 설명으로 옳지 않은 것은? 1
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.
[해설]
- TCP(Transport Control Protocol) : 연결형(connection oriented) 프로토콜이며, 이는 실제로 데이터를 전송하기 전에 먼저 TCP 세션을 맺는 과정이 필요함을 의미한다. (TCP3-way handshaking)

문 3. 암호 알고리즘에 대한 설명으로 옳지 않은 것은? 2
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.
[해설]
- Diffie-Hellman : 1976년에 Diffie와 Hellman이 개발된 최초의 공개키 알고리즘으로써 제한된 영역에서 멱의 계산에 비하여 이산대수 로그 문제의 계산이 어렵다는 이론에 기초를 둔다. 이 알고리즘은 메시지를 암복호화하는데 사용되는 알고리즘이 아니라 암복호화를 위해 사용되는 키의 분배 및 교환에 주로 사용되는 알고리즘이다.

문 4. TCP 세션 하이재킹에 대한 설명으로 옳은 것은? 1

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.
[해설]
TCP 세션 하이재킹
- TCP가 가지는 고유한 취약점을 이용해 정상적인 접속을 빼앗는 방법이다.
- TCP는 클라이언트와 서버간 통신을 할 때 패킷의 연속성을 보장하기 위해 클라이언트와 서버는 각각 시퀀스 넘버를 사용한다. 이 시퀀스 넘버가 잘못되면 이를 바로 잡기 위한 작업을 하는데, TCP 세션 하이재킹은 서버와 클라이언트에 각각 잘못된 시퀀스 넘버를 위조해서 연결된 세션에 잠시 혼란을 준 뒤 자신이 끼어들어가는 방식이다.

문 5. 생체 인증 측정에 대한 설명으로 옳지 않은 것은? 1
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.
[해설]
- FRR(False Rejection Rate) : 잘못된 거부율 (정상적인 사람을 거부함)
- FAR(False Acceptace Rate) : 잘못된 승인율 (비인가자를 정상인가자로 받아들임)

문 6. 블록암호 카운터 운영모드에 대한 설명으로 옳지 않은 것은? 4
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.
[해설]
- CTR(CounTeR) 모드 : 블록을 암호화할 때마다 1씩 증가해가는 카운터를 암호화해서 키스트림을 만든다. 즉, 카운터를 암호화한 비트열과 평문 블록과의 XOR를 취한 결과가 암호문 블록이 된다. 암호화와 복호화가 완전히 같은 구조가 되므로, 프로그램으로 구현하는 것이 간단하다. 블록을 임의의 순서로 암호화/복호화 할 수 있으며, 블록을 임의의 순서로 처리할 수 있다는 것은 처리를 병행할 수 있다는 것을 의미한다.

문 7. AES 알고리즘에 대한 설명으로 옳지 않은 것은? 2
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.
[해설]
- AES 알고리즘에서 각 라운드는 마지막을 제외하고 역연산이 가능한 4개의 변환을 사용하고, 마지막 라운드에서는 3개(SubBytes, ShiftRows, AddRoundKey)의 변환만을 갖는다.

문 8. 비트코인 블록 헤더의 구조에서 머클 루트에 대한 설명으로 옳지 않은 것은? 4
① 머클 트리 루트의 해시값이다.
② 머클 트리는 이진트리 형태이다.
③ SHA-256으로 해시값을 계산한다.
④ 필드의 크기는 64바이트이다.
[해설]
- 머클루트(merkle root)란 머클트리에서 루트 부분에 해당하고, 블록 헤더에 포함된다. 해당 블록에 저장되어 있는 모든 거래의 요약본으로 해당 블록에 포함된 거래로부터 생성된 머클트리의 루트에 대한 해시를 말한다. 거래가 아무리 많아도 묶어서 요약된 머클 루트의 용량은 항상 32바이트이다.
- 블록체인(Blockchain) 기술 : 블록체인은 유효한 거래 정보의 묶음이라 할 수 있다. 블록체인은 쉽게 표현하면 블록으로 이루어진 연결 리스트라 할 수 있다. 하나의 블록은 트랜잭션의 집합(거래 정보)과 블록헤더(version, previousblockhash, merklehash, time, bits, nonce), 블록해쉬로 이루어져 있다.

문 9. SET에 대한 설명으로 옳지 않은 것은? 3
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.
[해설]
- 고객등록에서는 인증기관을 통하여 고객의 등록과 인증서의 생성이 이루어진다.

문 10. 『개인정보 보호법』 제26조(업무위탁에 따른 개인정보의 처리 제한)에 대한 설명으로 옳지 않은 것은? 3
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.
[해설]
- 개인정보 보호법 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. <개정 2015. 7. 24.>
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.

문 11. IPv6에 대한 설명으로 옳지 않은 것은? 4
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.
[해설]
- IPv6는 유니캐스트, 애니캐스트, 멀티캐스트 방식을 사용한다.

문 12. SSH를 구성하는 프로토콜에 대한 설명으로 옳은 것은? 1
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.

[해설]
- SSH는 보통 TCP상에서 수행되는 3개의 프로토콜로 구성된다.
- SSH 사용자 인증 프로토콜(User Authentication Protocol) : 클라이언트 측 사용자를 서버에게 인증
- SSH 연결 프로토콜(Connection Protocol) : 암호화된 터널을 여러 개의 논리적 채널로 다중화
- SSH 전송 계층 프로토콜(Transport Layer Prtocol) : 서버 인증, 기밀성, 무결성을 제공하고, 옵션으로 압축을 제공

문 13. 유럽의 국가들에 의해 제안된 것으로 자국의 정보보호 시스템을 평가하기 위하여 제정된 기준은? 2
① TCSEC
② ITSEC
③ PIMS
④ ISMS-P
[해설]
- ITSEC (Information Technology Security Evaluation Criteria)
① 1991년 독일, 프랑스, 네덜란드, 영국 등 유럽 4개국이 평가제품의 상호 인정 및 평가기준이 상이함에 따른 불합리함을 보완하기 위하여 작성한 것이다.
② 평가등급은 최하위 레벨의 신뢰도를 요구하는 E0(부적합판정)부터 최상위 레벨의 신뢰도를 요구하는 E6까지 7등급으로 구분한다.

문 14.『개인정보 보호법』제3조(개인정보 보호 원칙)에 대한 설명으로 옳지 않은 것은? 3
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.
[해설]
- 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 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. <개정 2020. 2. 4.>
⑧ 개인정보처리자는 이 법 및 관계 법령에서 규정하고 있는 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력하여야 한다.

문 15. ISO/IEC 27001의 통제영역에 해당하지 않은 것은? 2
① 정보보호 조직
② IT 재해복구
③ 자산 관리
④ 통신 보안
[해설]
- ISO/IEC 27001의 통제영역 : 정보보호 정책, 준거성, 정보보호 조직, 인적자원 보호, 자산 관리, 정보시스템 도입.개발 및 유지보수, 업무연속성 관리, 접근 통제, 암호화, 물리적 정보보호, 운영관리, 통신 보안, 위탁관리, 정보보호 사고관리

문 16. 접근제어 모델에 대한 설명으로 옳지 않은 것은? 2
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.
[해설]
- 임의적 접근 통제(DAC : Discretionary Access Control) : 주체가 속해 있는 그룹의 신원에 근거하여 객체에 대한 접근을 제한하는 방법으로 객체의 소유자가 접근 여부를 결정한다.
- 강제적 접근 통제(MAC : Mandatory Access Control) : 주체와 객체의 등급을 비교하여 접근 권한을 부여하는 접근 통제이며, 모든 객체는 기밀성을 지니고 있다고 보고 객체에 보안 레벨을 부여한다.
- 역할 기반 접근통제(RBAC : Role Based Access Control) : 주체와 객체 사이에 역할을 부여하여 임의적, 강제적 접근통제 약점을 보완한 방식이다. 사용자가 적절한 역할에 할당되고 역할에 적합한 접근권한(허가)이 할당된 경우만 사용자가 특정한 모드로 정보에 접근할 수 있는 방법이다.

문 17. 운영체제에 대한 설명으로 옳지 않은 것은? 4
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.
[해설]
- 프로세스 관리자 : 프로세스 생성 및 삭제, 중앙처리장치 할당을 위한 스케줄링 결정
- 파일 관리자 : 컴퓨터 시스템의 모든 파일 관리. 파일의 접근 제한 관리.

문 18.『정보통신망 이용촉진 및 정보보호 등에 관한 법률』의 용어에 대한 설명으로 옳지 않은 것은? 2
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.
[해설]
- 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제2조(정의) ① 이 법에서 사용하는 용어의 뜻은 다음과 같다.
3. “정보통신서비스 제공자”란 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다.
4. “이용자”란 정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하는 자를 말한다.
5. “전자문서”란 컴퓨터 등 정보처리능력을 가진 장치에 의하여 전자적인 형태로 작성되어 송수신되거나 저장된 문서형식의 자료로서 표준화된 것을 말한다.
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
나. 정보통신망의 정상적인 보호ㆍ인증 절차를 우회하여 정보통신망에 접근할 수 있도록 하는 프로그램이나 기술적 장치 등을 정보통신망 또는 이와 관련된 정보시스템에 설치하는 방법
12. “통신과금서비스이용자”란 통신과금서비스제공자로부터 통신과금서비스를 이용하여 재화

등을 구입ㆍ이용하는 자를 말한다.

문 19. 스니핑 공격에 대한 설명으로 옳지 않은 것은? 1
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.
[해설]
- ARP Spoofing은 스위칭 환경의 랜상에서 패킷의 흐름을 바꾸는 공격 방법이다. 공격자가 서버와 클라이언트의 통신을 스니핑하기 위해 ARP 스푸핑 공격을 시도한다.

문 20. 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」에서 인증심사원에 대한 설명으로 옳지 않은 것은? 3
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.
[해설]
- 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 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 인정할 수 있다.
④ 인터넷진흥원은 인증정보를 제공하는 홈페이지에 제2항의 보수교육 운영에 관한 세부내용을 공지하여야 한다.
⑤ 인터넷진흥원은 제2항의 요건을 충족한 인증심사원에 한하여 별지 제8호서식의 정보보호 및 개인정보보호 관리체계 인증심사원 자격 증명서를 갱신하여 발급하고 자격 유효기간을 3년간 연장한다.