2017년 지방직 하반기 9급 정보보호론 풀이

by 호이호이꿀떡

정답 체크

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

문 1. 유닉스(Unix) 운영체제에서 사용자의 패스워드에 대한 해쉬 값이 저장되어 있는 파일은?

① /etc/shadow ② /etc/passwd
③ /etc/profile ④ /etc/group

답 ①

① 패스워드가 암호화되거나 해시값으로 저장되는 파일은 /etc/shadow 파일이다.

<오답 체크> ② /etc/passwd에는 사용자의 기본 정보가 평문 형태로 저장된다.

③ /etc/profile 파일에는 사용자가 로그인했을 때 실행되는 스크립트들이 정의되어 있다.

④ /etc/group 파일에는 그룹에 대한 정보가 들어있다.

문 2. 다음에서 설명하는 것은?

> 평문을 암호화하거나 암호화된 문장을 복호화하는 전기·기계 장치로 자판에 문장을 입력하면 회전자가 돌아가면서 암호화된 문장·복호화된 평문을 만들어낸다.

① 스키테일(Scytale)
② 아핀(Affine)
③ 에니그마(Enigma)
④ 비제니어(Vigenere)

답 ③

③ 에니그마(Enigma)
제2차 세계대전 당시 독일군이 사용한 암호화 장비이다. 회전판을 기반으로 만들어진 전자기계식 암호 장비로, 같은 글자를 눌러도 다른 글자가 튀어나오기 때문에 암호를 해독하기 위해서는 17000여 번을 시도해봐야 하며, 독일군은 한 달에 한 번씩 암호책을 새로 배부하였기 때문에 이론적으로는 해독을 하는 것이 거의 불가능하였다. 하지만 결국 독일군의 허술한 운영으로 암호가 해독되어 연합군의 승리에 큰 기여를 하였다.

<오답 체크> ① 스키테일(Scytale)
고대 그리스에서 고안된 암호화 방식으로, 나무봉에 종이 테이프를 서로 겹치지 않도록 감아 올린 뒤 그 위에 가로로 글씨를 쓰는데, 테이프를 풀어 세로로 길게 늘어선 글을 읽으면 무슨 뜻인지 전혀 알 수 없다는 것을 이용한 암호화 방식이다. 나무봉을 스키테일(scytale)이라 부르며, 이 암호화 방식을 `스키테일 암호`라 부른다.

② 아핀(Affine)
덧셈 암호와 곱셈 암호를 병합한 암호화 방식으로, 문자를 우선 특정 숫자로 치환하여 키(key)와 더하고 곱한 뒤, 그 결과값을 다시 특정 문자로 치환하는 암호화 방식이다.

④ 비제니어(Vigenere)
프랑스 암호학자 비제니어(비즈네르)가 고안한 다중 문자 대치 암호이다. 하나의 문자를 다른 문자로 대치하는 카이사르 암호를 발전시킨 것으로, 특정 문자열을 키로 사용해 평문의 문자와 더하여 암호문을 생성한다. 카이사르 암호는 빈도분석법을 통해 해독이 가능한데, 비즈네르 암호는 키 문자열과 더하기 때문에 빈도분석법으로 해독이 어려워진다.

문 3. RFC 2104 인터넷 표준에서 정의한 메시지 인증 코드를 생성하는 알고리즘은?

① Elliptic Curve Cryptography
② ElGamal
③ RC4
④ HMAC - SHA1

답 ④

④ HMAC(Hash-based Message Authentication Code, 해시 기반 메시지 인증 코드)
해시값을 이용한 메시지 인증 코드로, 1997년 RFC2014로 작성되었다. 패딩 등을 이용하여 MAC보다 더 복잡하고, SHA1은 SHA1의 알고리즘을 이용한다는 걸 의미한다.

문 4. 다음에서 설명하는 디지털 포렌식(Digital Forensics)은?

> 자신에게 불리한 증거 자료를 사전에 차단하려는 활동이나 기술로 데이터 은닉, 데이터 암호화 등이 있다.

① 항포렌식(Anti Forensic)
② 임베디드 포렌식(Embedded Forensic)
③ 디스크 포렌식(Disk Forensic)
④ 시스템 포렌식(System Forensic)

답 ①

① 항포렌식(Anti Forensic, 안티 포렌식)
디지털 포렌식 기술에 대응하여 자신에게 불리하게 작용할 가능성이 있는 증거물을 훼손하거나 차단하는 일련의 행위를 말한다.
◈ 안티 포렌식 기법
1. 데이터 파괴(Destruction)
2. 데이터 암호화(Encryption)
3. 데이터 은닉(Hiding)
4. 데이터 조작(Manipulation)
5. 풋프린트 최소화(Minimizing the Footprint)
6. 분석 시간 증가(Reducing analyzability)

<오답 체크> ② 임베디드 포렌식(Embedded Forensic)
모바일 포렌식과 임베디드 포렌식을 하나로 묶어 부르기도 하며, 휴대폰, 스마트폰, PDA, 내비게이션 등, 모바일 기기와 임베디드 시스템이 내장된 디지털 기기를 대상으로 증거 획득 및 분석하는 것을 의미

③ 디스크 포렌식(Disk Forensic): 하드디스크나 USB, 플래시 메모리 등 저장매체에서 삭제된 데이터를 찾아내어 법원에 증거자료로 제출하는 과정

④ 시스템 포렌식(System Forensic): 서버나 PC등을 대상으로 하는 디지털 포렌식 전반을 총칭

문 5. 안전한 전자상거래를 구현하기 위해서 필요한 요건들에 대한 설명으로 옳은 것은?

① 무결성(Integrity) - 정보가 허가되지 않은 사용자(조직)에게 노출되지 않는 것을 보장하는 것을 의미한다.
② 인증(Authentication) - 각 개체 간에 전송되는 정보는 암호화에 의한 비밀 보장이 되어 권한이 없는 사용자에게 노출되지 않아야 하며 저장된 자료나 전송 자료를 인가받지 않은 상태에서는 내용을 확인할 수 없어야 한다.
③ 접근제어(Access Control) - 허가된 사용자가 허가된 방식으로 자원에 접근하도록 하는 것이다.
④ 부인봉쇄(Non-repudiation) - 어떠한 행위에 관하여 서명자나 서비스로부터 부인할 수 있도록 해주는 것을 의미한다.

답 ③

③ 허가된 사용자가 자원에 접근한다는 내용을 보고 가용성이라고도 생각할 수 있으나, 허가된 사용자와 허가되지 않은 사용자를 구분하여 자원 접근을 통제하는 것이므로 접근제어가 좀 더 정확하다고 볼 수 있다.
또한 나머지 선지들이 모두 틀렸기 때문에 정답은 ③밖에 되지 않는다.

<오답 체크> ① 기밀성에 대한 설명이다.
무결성은 허가받지 않은 사용자에 의해 데이터가 위·변조되지 않아야 한다는 것을 의미한다.

② **인증**(authentication)은 상대방이 진짜 본인이 맞는지(혹시 신분 위조는 아닌지) 확인하는 것이고, **인가**(authorization)는 그 사용자가 요구하는 권한이 허용된 것인지 아닌지 확인하는 것이다.
문제에서는 '권한이 없는 사용자는 인가받지 않은 상태에서 내용을 확인할 수 없다'고 하였기 때문에 **인가**에 대한 설명이다.

④ 부인방지는 정당하게 이루어진 거래 사실을 부인할 수 없어야 하는 것을 의미한다.

문 6. 무선 인터넷 보안을 위한 알고리즘이나 표준이 아닌 것은?

① WEP ② WPA - PSK
③ 802.11i ④ X.509

답 ④

④ X.509는 공개키를 인증하기 위한 인증서 표준이다. 무선 인터넷 보안과 직접적인 관련은 없다.

<오답 체크> ① **WEP**(Wired Equivalent Privacy)
초창기의 무선랜 보안 프로토콜이며, 암호화를 위해 RC4 사용하며, 암호화와 인증에 동일한 키를 사용

② **WPA**(WiFi Protected Access)
WEP보다 보안성이 강화된 무선 보안 프로토콜로
RC4-TKIP를 통한 암호화(암호키 주기적인 변경)
EAP를 통한 사용자 인증
48비트 길이의 초기벡터(IV) 사용
PSK(Pre Shared Key)는 프로토콜을 운용하는 방식의 하나로, 미리 설정된 키를 사용자와 AP가 공유하여 사용하는 것을 의미한다.

③ 802.11: 무선 인터넷을 위한 일련의 표준 규격
802.11i는 보안성을 강화한 무선 인터넷 표준으로, WPA/WPA2 방식을 사용

문 7. 다음은 유닉스에서 /etc/passwd 파일의 구성을 나타낸 것이다. ㉠ ~ ㉣에 대한 설명으로 옳은 것은?

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

① ㉠ - 사용자 소속 그룹 GID
② ㉡ - 사용자 UID
③ ㉢ - 사용자 계정 이름
④ ㉣ - 사용자 로그인 쉘

답 ④

root : 사용자 계정 이름
x : 패스워드가 들어갈 자리(패스워드는 /etc/shadow에 암호화된 형태로 저장)
㉠ 0 : 사용자 UID (root인 경우 0)
㉡ 0 : 사용자 소속 그룹 GID (root인 경우 0)
root : 사용자에 대한 정보를 적는 곳
㉢ /root : 사용자 계정 홈 디렉터리
㉣ /bin/bash : 사용자 계정 로그인 쉘

문 8.「국가정보화 기본법」상 ㉠, ㉡에 들어갈 용어가 바르게 연결된 것은?

○ 정부는 국가정보화의 효율적, 체계적 추진을 위하여 (㉠)마다 국가정보화 기본계획을 수립하여야 한다.
○ 국가정보화 기본계획은 (㉡)이 국가와 지방자치단체의 부문계획을 종합하여 정보통신 진흥 및 융합 활성화 등에 관한 특별법 제7조에 따른 정보통신 전략위원회의 심의를 거쳐 수립·확정한다.

㉠	㉡
① 3년	행정안전부장관
② 3년	과학기술정보통신부장관
③ 5년	과학기술정보통신부장관
④ 5년	행정안전부장관

답 ③

「국가정보화 기본법」
제6조(국가정보화 기본계획의 수립) ① 정부는 국가정보화의 효율적, 체계적 추진을 위하여 **5년**마다 국가정보화 기본계획(이하 "기본계획"이라 한다)을 수립하여야 한다.
② 기본계획은 **과학기술정보통신부장관**이 국가와 지방자치단체의 부문계획을 종합하여 「정보통신 진흥 및 융합 활성화 등에 관한 특별법」 제7조에 따른 정보통신 전략위원회(이하 "전략위원회"라 한다)의 심의를 거쳐 수립·확정한다.

문 9. 일정 크기의 평문 블록을 반으로 나누고 블록의 좌우를 서로 다른 규칙으로 계산하는 페이스텔(Feistel) 암호 원리를 따르는 알고리즘은?

① DES(Data Encryption Standard)
② AES(Advanced Encryption Standard)
③ RSA
④ Diffie - Hellma

답 ①

① DES(Data Encryption Standard)
페이스텔(Feistel) 구조의 대칭키 암호 알고리즘
블록 64비트
키 길이 56비트 + 패리티 8비트 = 64비트
16라운드
<오답 체크> ② AES(Advanced Encryption Standard)
SPN구조의 대칭키 암호 알고리즘
(SPN구조는 각 단계에서 치환, 전치, 혼합, 덧셈을 거친다는 표현이 들어간다)
블록 128비트(16바이트)
키 길이 128비트 – 10라운드
키 길이 192비트 - 12라운드
키 길이 256비트 - 14라운드
③ RSA는 소인수분해 계산의 어려움에 기반한 공개키 암호 알고리즘
④ 디피 헬만 키 교환(Diffie–Hellman key exchange) 알고리즘은 두 송수신자 간 공통의 비밀키(대칭키)를 생성하기 위한 방법으로, 이산대수의 어려움에 기반한 알고리즘이다.

문 10. IPSec 표준은 네트워크 상의 패킷을 보호하기 위하여 AH(Authentication Header)와 ESP (Encapsulating Security Payload)로 구성된다. AH와 ESP 프로토콜에 대한 설명으로 옳지 않은 것은?

① AH 프로토콜의 페이로드 데이터와 패딩 내용은 기밀성 범위에 속한다.
② AH 프로토콜은 메시지의 무결성을 검사하고 재연(Replay) 공격 방지 서비스를 제공한다.
③ ESP 프로토콜은 메시지 인증 및 암호화를 제공한다.
④ ESP는 전송 및 터널 모드를 지원한다.

답 ①

① **AH**(Authentication Header, 인증 헤더)는 메시지 무결성과 인증 기능은 제공하지만, 암호화는 보장하지 않는다.
암호화를 통해 기밀성을 제공하는 것은 ESP(Encapsulating Security Protocol, 보안 캡슐 프로토콜)이다.
<오답 체크> ② AH 프로토콜은 무결성과 인증 기능을 제공하며, AH에는 순서 번호 필드가 포함되어 있어 재전송 공격을 방지할 수 있다.
③ **ESP**(Encapsulating Security Payload, 캡슐화 보안 페이로드)는 대칭키 암호화를 통해, 기밀성과 무결성과 선택적 인증을 제공한다.
④ AH와 ESP 둘 다 전송 및 터널 모드를 지원한다.
전송 모드에서는 IP 페이로드와 IP 헤더 일부를 인증·암호화하고, 터널 모드에서는 내부 IP 패킷 전체(헤더+페이로드)를 인증·암호화한다.

문 11. 스마트폰 보안을 위한 사용자 지침으로 옳지 않은 것은?

① 관리자 권한으로 단말기 관리
② 스마트폰과 연결되는 PC에도 백신 프로그램 설치
③ 블루투스 기능은 필요 시에만 활성
④ 의심스러운 앱 애플리케이션 다운로드하지 않기

답 ①

① 관리자 권한은 일반 이용자 권한으로 접근하지 못하는 시스템 설정을 변경하는 권한을 가지기 때문에, 시스템과 보안에 대해 잘 모르는 사용자는 함부로 건들지 않는 게 좋다.
<오답 체크> ③ 블루투스, WIFI 등 무선 네트워크 기능은 단순히 켜놓는 것만으로도 해킹의 통로로 이용될 수 있기 때문에, 사용하지 않을 때는 꺼놓는 것이 좋다.

문 12. 다음에서 설명하는 것은?

> ○ 전달하려는 정보를 이미지 또는 문장 등의 파일에 인간이 감지할 수 없도록 숨겨서 전달하는 기술
> ○ 이미지 파일의 경우 원본 이미지와 대체 이미지의 차이를 육안으로 구별하기 어렵다.

① 인증서(Certificate)
② 스테가노그래피(Steganography)
③ 전자서명(Digital Signature)
④ 메시지 인증 코드(Message Authentication Code)

답 ②

② **스테가노그래피**(steganography)는 보통의 데이터에 또 다른 정보나 데이터를 보이지 않게 삽입하는 기술이다.
<오답 체크> ① **인증서**(Certificate)는 공개키와 그에 관한 정보를 포함하는 전자 증명서로, 주로 X.509 v3 표준 형식에 기반함
④ **메시지 인증 코드**(**MAC**, Message Authentication Code)는 대칭키를 사용하는 해시값으로, 무결성과 출처 인증(발신지에 대한 인증)이 가능하다. 출처 인증은 가능하지만, 부인 방지는 불가능하다.

문 13. 조직의 정보자산을 보호하기 위하여 정보자산에 대한 위협과 취약성을 분석하여 비용 대비 적절한 보호 대책을 마련함으로써 위험을 감수할 수 있는 수준으로 유지하는 일련의 과정은?

① 업무 연속성 계획
② 위험관리
③ 정책과 절차
④ 탐지 및 복구 통제

답 ②

② 위험을 분석·평가하고 적절히 통제하고 관리하는 일련의 과정을 위험관리라고 한다.

<오답 체크> ① 업무 연속성 계획 : 비즈니스 활동에 대한 방해요인에 대응하며 중대한 실패 또는 재난의 영향으로부터 중요한 비즈니스 프로세스를 보호하기 위한 계획

③ 정책과 절차 : 조직이 수행하는 모든 정보보호활동의 근거를 수립하고, 조직에 미치는 영향을 고려하여 중요한 업무, 서비스, 조직, 자산 등을 포함할 수 있도록 범위를 설정

④ 탐지 및 복구 : 정보보호 침해사고가 발생한 것을 탐지하고 시스템을 정상 상태로 복구하는 것

문 14. 「개인정보 보호법」상 다음 업무를 수행하는 자는?

> 개인정보파일의 보호 및 관리·감독하는 임원(임원이 없는 경우에는 개인 정보를 담당하는 부서의 장)을 말한다.

① 수탁자
② 정보통신서비스 제공자
③ 개인정보취급자
④ 개인정보 보호책임자

답 ④

「개인정보 보호법」 제31조(개인정보 보호책임자의 지정) ① 개인정보처리자는 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호책임자를 지정하여야 한다.

② 개인정보 보호책임자는 다음 각 호의 업무를 수행한다.

1. 개인정보 보호 계획의 수립 및 시행
2. 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
3. 개인정보 처리와 관련한 불만의 처리 및 피해 구제
4. 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
5. 개인정보 보호 교육 계획의 수립 및 시행
6. 개인정보파일의 보호 및 관리·감독
7. 그 밖에 개인정보의 적절한 처리를 위하여 대통령령으로 정한 업무

<오답 체크> ① 제26조(업무위탁에 따른 개인정보의 처리 제한)의 2항: 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.

② 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조(정의) ①의 3. "**정보통신서비스 제공자**"란 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다.

③ **「개인정보 보호법」** 제2조(정의)의 5. "**개인정보처리자**"란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.

제28조(개인정보취급자에 대한 감독) ① 개인정보처리자는 개인정보를 처리함에 있어서 개인정보가 안전하게 관리될 수 있도록 임직원, 파견근로자, 시간제근로자 등 개인정보처리자의 지휘·감독을 받아 **개인정보를 처리하는 자**(이하 "**개인정보취급자**"라 한다)에 대하여 적절한 관리·감독을 행하여야 한다.

문 15. XSS 공격에 대한 설명으로 옳은 것은?

① 자료실에 올라간 파일을 다운로드할 때 전용 다운로드 프로그램이 파일을 가져오는데, 이때 파일 이름을 필터링하지 않아서 취약점이 발생한다.
② 악성 스크립트를 웹 페이지의 파라미터 값에 추가하거나, 웹 게시판에 악성 스크립트를 포함시킨 글을 등록하여 이를 사용자의 웹 브라우저 내에서 적절한 검증 없이 실행되도록 한다.
③ 네트워크 통신을 조작하여 통신 내용을 도청하거나 조작하는 공격 기법이다.
④ 데이터베이스를 조작할 수 있는 스크립트를 웹 서버를 이용하여 데이터베이스로 전송한 후 데이터베이스의 반응을 이용하여 기밀 정보를 취득하는 공격 기법이다.

답 ②

② **XSS**(Cross-site Scripting, 크로스 사이트 스크립팅)
웹 사이트에 악성 스크립트를 삽입한 뒤 다른 사용자의 접근을 유도하여, 사용자의 클라이언트에서 악성 프로그램이 실행되도록 하여 개인정보를 유출시키는 공격이다.

<오답 체크> ① **직접 객체 참조**로 인한 웹 취약점 중 디렉터리 탐색에 대한 설명이다.
디렉터리 탐색은 웹 브라우저에서 확인 가능한 경로의 상위로 탐색하여 특정 시스템 파일을 다운로드할 수 있는 취약점이다. 자료실에 올라간 파일을 다운로드할 때 전용 다운로드 프로그램이 파일을 가져오는데, 이때 파일 이름을 필터링하지 않아서 취약점이 발생한다.

③ 스푸핑을 통한 **중간자 공격**(**MITM**, man in the middle attack)에 대한 설명이다. 중간자 공격은 네트워크 통신을 조작하여 통신 내용을 도청하거나 조작하는 공격 기법이다.

④ SQL 삽입(**SQL 인젝션**, SQL injection) 공격은 데이터베이스로 보내는 클라이언트의 입력값을 조작하여 관리자가 예상하지 못한 명령을 실행하거나, 정당한 권한을 획득하지 않고 부정한 방법으로 데이터베이스에 접근하는 공격이다.

문 16. 영국, 독일, 네덜란드, 프랑스 등의 유럽 국가가 평가 제품의 상호 인정 및 정보보호평가 기준의 상이함에서 오는 시간과 인력 낭비를 줄이기 위해 제정한 유럽형 보안 기준은?

① CC(Common Criteria)
② TCSEC(Orange Book)
③ ISO/IEC JTC 1
④ ITSEC

답 ④

④ **ITSEC**(Information Technology Security Evaluation Criteria)
유럽의 정보보호 시스템 평가 제도

<오답 체크> ① **CC**(Common Criteria, 국제공통평가기준)은 국가마다 서로 다른 정보보호시스템 평가기준을 연동하고 평가결과를 상호인증하기 위해 제정된 평가기준

② **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 **ISO/IEC JTC1** (Joint Technical Committee)은 ISO와 IEC가 정보기술 분야의 표준을 공동 제정하기 위해 설립한 표준화 기관이다.

문 17. 다음에서 설명하는 것은?

> 개인정보처리자의 자율적인 개인정보 보호활동을 촉진하고 지원하기 위한 인증 업무이며, 공공기관, 민간기업, 법인, 단체 및 개인 등 모든 공공기관 및 민간 개인정보처리자를 대상으로 개인정보 보호 관리체계 구축 및 개인정보 보호 조치 사항을 이행하고 일정한 보호 수준을 갖춘 경우 인증마크를 부여하는 제도이다.

① SECU - STAR(Security Assessment for Readiness)
② PIPL(Personal Information Protection Level)
③ EAL(Evaluation Assurance Level)
④ ISMS(Information Security Management System)

답 ②

② **PIPL**(Personal Information Protection Level, 개인정보 보호 인증)
개인정보 처리기관의 개인정보보호 조치와 활동에 대한 인증으로, 국내 인증제도이다. PIPL은 공공기관은 물론, 개인정보를 처리하는 민간기업, 법인, 단체 및 중소기업과, 소상공인까지 인증받을 수 있다.
한국정보화진흥원(KISA)이 인증기관 역할을 한다.

<오답 체크> ① **SECU-STAR**(정보보호 준비도 평가)
기존의 정부 주도가 아닌, 민간이 자율적으로 정보보호 등급을 매기고 이를 공개하는 평가 제도이다. 기존의 대기업 위주의 평가 제도에서 벗어나 중소·영세 업체까지 모든 기업의 정보보호 수준을 진단하고 위한 도입되었다.

③ **EAL**(평가보증등급)
국제공통평가기준인 **CC**(Common Criteria, 국제공통평가기준)에서 정의한 제품의 보증등급으로, EAL1에서 EAL7까지 7단계로 구분

④ **ISMS**(Information Security Management System)
2004년에 BS7799를 기반으로 국내 실정에 맞춘 정보보호관리체계로 KISA(구 한국정보보호진흥원)에서 국내 표준을 만들었다. 현재 이 제도는 방송통신위원회 소관으로 "정보통신망이용촉진 및 정보보호 등에 관한 법률"에 명시되어 있고 인증기관은 한국인터넷진흥원(KISA)이다. BS7799의 국제 표준화가 이뤄진 ISO27001와 비교하여, KISA ISMS에서 요구하는 인증기준 및 심사절차가 좀더 엄격하다고 할 수 있다.

문 18. 개인정보보호 관리체계(PIMS) 인증에 대한 설명으로 옳지 않은 것은?

① 한국인터넷진흥원이 PIMS 인증기관으로 지정되어 있다.
② PIMS 인증 후, 2년간의 유효 기간이 있다.
③ PIMS 인증 신청은 민간 기업 자율에 맡긴다.
④ PIMS 인증 취득 기업은 개인정보 사고 발생 시 과징금 및 과태료를 경감 받을 수 있다.

답 ②

② PIMS 인증의 유효기간은 3년이다.

◈ **PIMS**(Personal Information Management System, 개인정보보호 관리체계)
· 기업이 개인정보보호 관리체계를 수립하여 운영하고 있는 서비스 범위가 인증심사 기준에 적합한지 여부를 인증기관이 평가하여 인증을 부여하는 제도이다
· 인증대상: 개인정보를 처리하는 모든 공공기관 및 민간 개인정보처리자
· 인증의 유효기간은 인증서 발급일로부터 3년
· 정책기관: 행정자치부, 방송통신위원회
· 인증기관: 한국인터넷진흥원

문 19. 다음은 침입 탐지 시스템의 탐지분석 기법에 대한 설명이다.

㉠ ~ ㉣에 들어갈 내용이 바르게 연결된 것은?

> 침입 탐지 시스템에서 (㉠)은 이미 발견되고 정립된 공격 패턴을 미리 입력해 두었다가 해당하는 패턴이 탐지되면 알려주는 것이다. 상대적으로 (㉡)가 높고, 새로운 공격을 탐지하기에는 부적합하다는 단점이 있다. (㉢)은 정상적이고 평균적인 상태를 기준으로 하여, 상대적으로 급격한 변화를 일으키거나 확률이 낮은 일이 발생하면 침입 탐지로 알려주는 것이다. 정량적인 분석, 통계적인 분석 등이 포함되며, 상대적으로 (㉣)가 높다.

㉠	㉡	㉢	㉣

① 이상탐지기법 False Positive 오용탐지기법 False Negative
② 이상탐지기법 False Negative 오용탐지기법 False Positive
③ 오용탐지기법 False Negative 이상탐지기법 False Positive
④ 오용탐지기법 False Positive 이상탐지기법 False Negative

답 ③

이 문제에서 나오는 False Negative·False Positive를 인증에 나오는 오거부율(FRR)·오승인률(FAR)과 같은 의미로 생각하면 반대가 되어버리니 주의해야 한다.

False Negative는 실제 침입을 침입이 아니라고 판단하는 것
(원래는 차단해야 할 것을 차단을 하지 않는 것)

오거부율(FRR, False Rejection Rate)은 정당한 사용자를 정당하지 않다고 판단하는 것
(원래는 차단하지 않아야 할 사용자를 차단해버리는 것)

㉠ **오용 탐지**(Misuse Detection)
= 시그니처 기반(Signature Base)
= 지식 기반(Knowledge Base)
이미 발견되고 정립된 공격 패턴을 미리 입력해 두고 그에 해당하는 패턴을 탐지
오탐율이 낮고 비교적 효율적이나 알려진 공격 이외는 탐지 불가능
Zero Day attack(제로 데이 공격)에 취약

㉡ **False Negative**(거짓 음성, 제2종 오류)
실제 상태는 ○인데 X라고 진단하는 오류로서, 실제로는 침입(O)인데 침입이 아니라고(X) 오진을 하는 것이다.
오용 탐지는 알려지지 않은 공격은 탐지하지 못하기 때문에 실제 침입을 침입이 아니라고 오진하는 경우가 높다.

㉢ **이상 탐지**(Anomaly Detection IDS)
= 행위 기반(Behavior)
= 통계적 탐지(Statistical Detection)
정상 패턴을 DB에 등록해두고, 정상에서 벗어나는 행위를 탐지(임계치 설정)
알려지지 않은 공격인 제로 데이 공격(zero day attack) 탐지 가능
오탐율 높고, 임계치 설정이 어려움

㉣ **False Positive**(거짓 양성, 제1종 오류)은 실제 상태는 X인데 ○라고 진단하는 오류로서, 실제로는 침입이 아닌(X)데 침입이라고(O) 오진을 하는 것이다.
이상 탐지는 정상에서 벗어나는 행위를 탐지하기 때문에 실제로는 침입이 아닌데 침입이라고 오진하는 경우가 높다.

문 20. 위험 분석 방법 중 손실 크기를 화폐가치로 측정할 수 없어서 위험을 기술 변수로 표현하는 정성적 분석 방법이 아닌 것은?

① 델파이법
② 퍼지 행렬법
③ 순위 결정법
④ 과거자료 접근법

답 ④

④ 과거자료 접근법은 정량적 분석에 해당한다. 용어에서 자칫 정성적 분석법으로 오인할 수 있으니 주의한다.

◈ 정량적 위험 분석: 위험의 크기를 수치로 계산
ALE(연간 예상 손실) 계산법
과거 자료 분석법
수학 공식 접근법
확률 분포법
몬테칼로 시뮬레이션
점수법
◈ 정성적 위험 분석: 위험의 크기를 개략적으로 판단
델파이법
시나리오법
순위 결정법
퍼지 행렬법
질문서법

〈오답 체크〉 ① 델파이법 : 전문가 집단으로 구성된 위험 분석팀의 분석과 평가를 통한 위험 분석 방법
② 퍼지행렬법은 '행렬'이라는 단어를 통해 수학적인 정량적 분석으로 오인할 수 있으나, 정성적인 분석법에 해당하므로 주의한다.