2017-지방직(추가)-정보보호론-A형-해설

대방고시 전산직/계리직, 하이클래스 군무원 곽후근(gobarian@gmail.com)

1. 유닉스(Unix) 운영체제에서 사용자의 패스워드에 대한 해쉬값이 저장되어 있는 파일은?

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

정답 체크)

(1) 패스워드 관련 정보(사용자 계정, 패스워드 해시값, 그 외의 7가지 패스워드 관련 정보)를 저장한 파일이다.

오답 체크)

(2) 사용자 관련 정보(사용자 계정, 패스워드 정보, 사용자 번호, 그룹 번호, 사용자 이름, 사용자 홈 디렉토리, 사용자의 쉘)가 저장된 파일이다.

(3) 사용자가 로그인했을 때 적용되는 스크립트를 정의해놓은 파일이다.

(4) 그룹 관련 정보(그룹, 그룹 비밀번호, 그룹 번호, 그룹 멤버리스트)가 저장된 파일이다.

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)

정답 체크)

(3) 에니그마(enigma)는 독일의 세르비우스(Arthur Scherbius)가 20세기 초에 발명한 암호화/복호화를 수행하는 기계이다. 에니그마는 독일어로 「수수께끼」를 의미이다. 회전하는 원반과 전기회로를 써서 강력한 암호를 만들고자 시도했고, 발명 당시에는 에니그마를 상용으로 사용하였다. 그리고 나치독일 시대에는 군용으로 사용하려고 개량하였다.

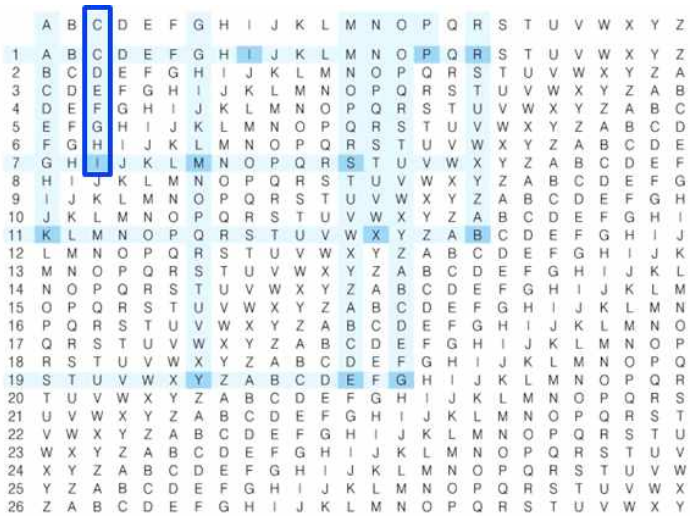
오답 체크)

(1) 예를 들어 HELP ME I AM UNDER ATTACK(도와주세요 공격당하고 있어요)이라는 평문을 전치암호로 바꾸기 위해 가로로 한 줄에 5개씩 알파벳을 배열한다. 그러고 나서 1열부터 5열까지 위에서부터 아래로 순서대로 적으면 HENTEIDTLAEAPMRCMUAK가 된다.

(2) 아핀암호에서는 ax+b(mod 26)로 암호화를 한다. 즉, 평문의 알파벳에 해당하는 수를 a배

하고 b만큼 더한 후 26으로 나눈 나머지에 해당하는 알파벳으로 암호화하는 것이다.
(4) 비게네르 암호에서는 암호화키가 필요한데, 다음이 암호화키라고 해보자.
7, 1, 11, 19
다음 문장을 암호화해보자.
C PROGRAMMING
암호화키가 7, 1, 11, 19라는 의미는 다음 그림과 같이 첫 번째 글자에는 암호표에서 7번째 줄의 암호문을 적용하고, 두 번째 글자에는 1번째 줄의 암호문을, 세 번째 글자에는 11번째 줄의 암호문을, 네 번째 글자에는 19번째 줄의 암호문을 그리고 다섯 번째 글자에는 다시 처음으로 돌아가 7번째 줄의 암호문을 적용한다는 것이다(암호화키에 따라 규칙성에 벗어남).

C	P	R	O	G	R	A	M	M	I	N	G
7	1	11	19	7	1	11	19	7	1	11	19



3. RFC 2104 인터넷 표준에서 정의한 메시지 인증 코드를 생성하는 알고리즘은?
① Elliptic Curve Cryptography
② ElGamal
③ RC4
④ HMAC - SHA1
정답 체크)
(4) 일방향 해시 함수(SHA-1)을 이용하여 메시지 인증 코드를 구현한 것이다. 1996년 Mihir Bellare, Ran Canetti, Hugo Krawczyk이 관련 논문을 발표하고, 1997년 RFC 2104를 작성하였다. HMAC은 IPsec과 TLS 등에서 사용한다.
오답 체크)
(1) ECC는 공개키 암호 방식으로 암호문 또는 서명을 생성하는 알고리즘이다.
(2) ElGamal은 공개키 암호 방식으로 암호문 또는 서명을 생성하는 알고리즘이다.
(3) RC4는 대칭키 암호 방식으로 암호문을 생성하는 알고리즘이다.
Tip! 이의 신청을 할 수 없는 답이 정해진 숫자 문제가 자주 출제되므로 정보보호론의 경우 숫자에 민감하기 바란다. 여기서는 RFC 번호가 해당된다.

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

자신에게 불리한 증거 자료를 사전에 차단하려는 활동이나 기술로 데이터 은닉, 데이터 암

호화 등이 있다.

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

정답 체크)
(1) 하드디스크의 경우, '물리적 방식'과 '소프트웨어 방식'이라는 두 가지 형태의 안티포렌식 방식을 사용한다. 물리적 방식은 망치나 파쇄기 등의 공구를 사용하여 하드디스크를 파괴하는 것을 말한다. 강력한 자력을 이용해 하드웨어 자체를 파괴하는 '디가우싱'(Degaussing)도 이에 해당된다. 소프트웨어 방식은 소프트웨어를 사용하여 남아 있는 데이터를 지우거나 기존 데이터에 새로운 데이터를 덮어씌워 해독하지 못하도록하는 방식이다.

오답 체크)
(2) 휴대폰, 스마트폰, PDA, 네비게이션, 라우터 등의 모바일 기기를 대상으로 한다.
(3) 비휘발성 저장매체(HDD, SSD, USB, CD 등)를 대상으로 한다.
(4) 서버나 PC 등을 대상으로 한다.

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.

정답 체크)
(3) 접근 제어는 기밀성 또는 무결성을 위해 사용된다.

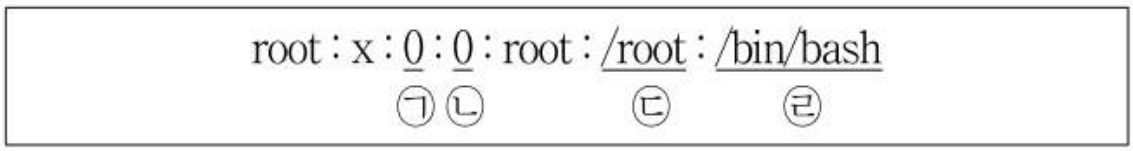
오답 체크)
(1) 해당 설명은 기밀성에 해당하고, 무결성은 정보의 내용이 불법적으로 생성 또는 변경되거나 삭제되지 않도록 보호되어야 하는 성질의 의미한다.
(2) 해당 설명은 기밀성에 해당하고, 인증은 상대방의 신원을 확인시켜주는 것을 의미한다. 예를 들어, 사용자 인증에는 시스템 접근 통제를 사용하고, 데이터 출처 인증에는 MAC을 사용한다.
(4) 어떠한 행위에 관하여 서명자나 서비스로부터 부인할 수 없도록 해주는 것을 의미한다.

6. 무선 인터넷 보안을 위한 알고리즘이나 표준이 아닌 것은?

① WEP
② WPA - PSK
③ 802.11i
④ X.509

정답 체크)
(4) 암호학에서 공개키 인증서와 인증알고리즘의 표준 가운데에서 공개 키 기반(PKI)의 ITU-T 표준이다.
오답 체크)
(1) 1997년 재정된 802.11 표준에서 도입되었던 WEP는 전통적인 유선 네트워크와 비슷한 데이터 보안성을 제공하기 위해 만들어졌다. 64비트 또는 128비트 키값을 사용하는 WEP는, 한때 매우 보편적으로 사용되었으며 라우터의 보안 설정에서 가장 우선적으로 표시되는 옵션이었다. 2001년 초, 암호학자들이 몇 가지 치명적인 취약점을 발견하였으며, 이를 이용하면 누구나 구할 수 있는 소프트웨어를 사용해 몇 십 분만에 WEP 연결을 크랙할 수 있다.
(2) WEP처럼 AP와 통신해야 할 클라이언트에 암호화키를 기본으로 등록해 두고 있다. 암호화키를 이용해 128비트인 통신용 암호화키를 생성하고, 이 암호화키를 10,000개 패킷마다 바꾼다. WPA는 WPA-Personal(개인용)과 WPA-Enterprise(기업용)로 나뉘는데 WPA-PSK는 WPA-Personal에 속한다.
(3) 802.11i는 WPA2를 나타내고, WPA2는 CCMP(암호키 동적 변경)과 AES 등 강력한 블록 암호 알고리즘을 사용한다.

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



① ㉠ - 사용자 소속 그룹 GID
② ㉡ - 사용자 UID
③ ㉢ - 사용자 계정 이름
④ ㉣ - 사용자 로그인 쉘
정답 체크)
(4) 사용자의 로그인 쉘을 나타낸다.
오답 체크)
(1) 사용자 UID를 나타낸다.
(2) 사용자 소속 그룹 GID를 나타낸다.
(3) 사용자의 홈 디렉토리를 나타낸다.
Tip! 나머지 내용을 정리하면 다음과 같다.
- 첫 번째 root : 사용자 계정을 나타낸다.
- 두 번째 x : 패스워드가 암호화되어 shadow 파일에 저장되어 있음을 나타낸다.
- 다섯 번째 root : 사용자의 이름이다. 시스템 설정에 별다른 영향이 없는 설정으로 자신의 이름을 입력해도 된다.

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

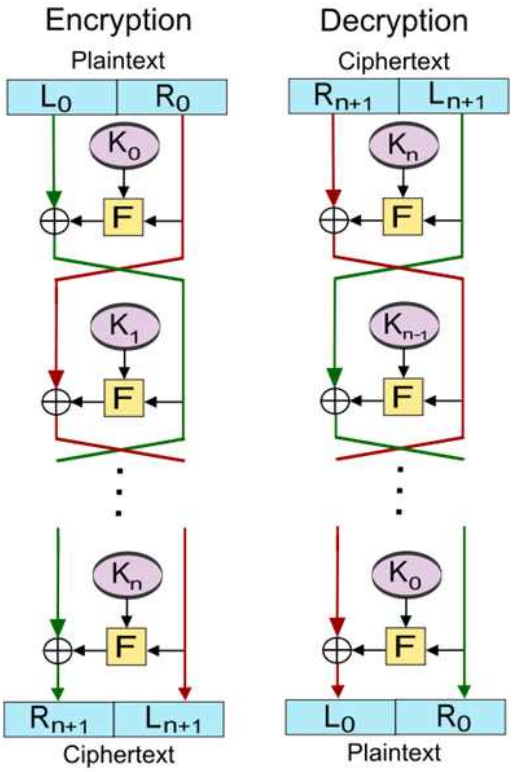
○ 정부는 국가정보화의 효율적, 체계적 추진을 위하여 (㉠)마다 국가정보화 기본계획을

수립하여야 한다.
○ 국가정보화 기본계획은 (㉡)이 국가와 지방자치단체의 부문계획을 종합하여 정보통신진흥 및 융합 활성화 등에 관한 특별 법 제7조에 따른 정보통신 전략위원회의 심의를 거쳐 수립·확정한다.

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

정답 체크)
(3) 제6조(국가정보화 기본계획의 수립) ① 정부는 국가정보화의 효율적, 체계적 추진을 위하여 5년마다 국가정보화 기본계획(이하 "기본계획"이라 한다)을 수립하여야 한다.
② 기본계획은 과학기술정보통신부장관이 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.

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 - Hellman
정답 체크)
(1) Feistel 구조는 다음과 같다.



오답 체크)

(2) SPN 구조에 기반한다.

(3) 소인수분해 문제에 기반한다.

(4) 이산 대수 문제에 기반한다.

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.

정답 체크)

(1) 해당 설명은 ESP에 해당하고, AH에는 페이로드와 패딩 포함되지 않는다(다음 그림 참조).

Authentication Header format																															
Offsets	$Octet_{16}$	0								1								2								3					
$Octet_{16}$	Bit_{10}	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	*Next Header*								*Payload Len*								*Reserved*															
4	32	*Security Parameters Index (SPI)*																															
8	64	*Sequence Number*																															
C	96	*Integrity Check Value (ICV)*																															
...	...	...																															

오답 체크)

(2) AH는 인증, 무결성, 재연(replay) 공격 방지 서비스를 제공한다.
(3) ESP는 인증, 무결성, 기밀성(암호화), 재연 공격 방지 서비스를 제공한다.
(4) AH와 ESP는 전송(기존 패킷) 및 터널(새로운 패킷) 모드를 지원한다.

11. 스마트폰 보안을 위한 사용자 지침으로 옳지 않은 것은?
① 관리자 권한으로 단말기 관리
② 스마트폰과 연결되는 PC에도 백신 프로그램 설치
③ 블루투스 기능은 필요시에만 활성
④ 의심스러운 앱 애플리케이션 다운로드하지 않기
정답 체크)
(1) 단말기는 일반 사용자 권한으로 사용하는 것이 좋다(관리자 권한이 공격자에게 탈취될 가능성을 염두에 두어야 함).
오답 체크)
(2) PC를 통해서 스마트폰에 감염이 가능하므로 PC에도 백신 프로그램을 설치해야 한다.
(3) 블루투스를 이용한 공격이 가능하므로 필요시에만 활성화를 한다.
(4) 트로이 목마 형태의 공격이 가능하므로 의심스러운 앱은 다운로드하지 않는다.

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)
정답 체크)
(2) 메시지의 내용을 읽지 못하게 하는 것이 아니라, 메시지의 존재 자체를 숨기는 기법이다. 메시지를 숨겨 넣는 방법을 알게 되면 메시지의 내용은 금방 노출된다.
오답 체크)
(1) 사용자 공개키의 정당성을 증명하기 위해 사용한다(인증기관이 서명함).
(3) 인증, 무결성, 부인 방지를 제공하기 위해 사용한다.
(4) 인증과 무결성을 제공하기 위해 사용한다.

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 업무연속성 계획
② 위험 관리
③ 정책과 절차
④ 탐지 및 복구 통제
정답 체크)

(2) 위험 관리는 위험 분석과 위험 평가라 나눠진다. 위험 분석은 위험을 분석하고 해석하는 과정으로 자산의 취약점을 식별하고 발생 가능한 위험의 내용과 정도를 결정하는 과정이고, 위험 평가는 조직에서 발생할 수 있는 손실에 대비한 보안 대책에 드는 비용 효과 분석을 통해 적은 비용으로 가장 효과적인 위험관리를 수행하기 위한 과정이다(경제학).
오답 체크)
(1) 각종 재해나 재난의 발생을 대비하여 핵심 시스템의 가용성과 신뢰성을 회복하고 사업의 연속성을 유지하기 위한 일련의 사업지속성계획과 절차를 의미한다.
(3) 보안 정책은 규칙으로서 지켜져야 할 정책(regulatory), 하려는 일에 부합하는 정책이 없을 때 참고하거나 지키도록 권유하는 정책(advisory), 어떠한 정보나 사실을 알리는 데 목적이 있는 정책(informative)의 특징을 가지고 실행을 위한 절차를 가진다.
(4) CERT에서 수행하는 침입에 대한 탐지 및 복구를 의미한다.

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 개인정보 취급자
④ 개인정보 보호책임자
정답 체크)
(4) 개인정보의 처리에 관한 업무를 총괄해서 책임진다(개인정보보호법 제31조).
오답 체크)
(1) 개인정보 처리 업무를 위탁받아 처리하는 자이다(개인정보보호법 제26조).
(2) 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다(정보통신망법 제2조).
(3) 임직원, 파견근로자, 시간제근로자 등 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 자이다(개인정보보호법 제28조).

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 웹페이지의 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 웹서버를 이용하여 데이터베이스로 전송한 후 데이터베이스의 반응을 이용하여 기밀 정보를 취득하는 공격 기법이다.
정답 체크)
(2) 저장 XSS 공격이다.
오답 체크)
(1) 파일 다운로드 취약점 공격이다.
(3) 중간자 공격이다(MITM).

(4) DB 인젝션(injection) 공격이다.

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
정답 체크)
(4) 1991년 5월 유럽 국가들이 발표한 공동 보안 지침서이다. TCSEC이 기밀성만을 강조한 것과 달리 무결성과 가용성을 포괄하는 표준안을 제시하였다.
오답 체크)
(1) CC라는 기준으로 TCSEC과 ITSEC은 통합되었다. 1996년에 초안이 나와 1999년에 국제 표준으로 승인되었다. PP, ST, TOE라는 인증 과정을 거친다.
(2) 1983년에 미국에서 제정되었고, 표지가 오렌지색이라 오렌지북이라 불린다. 보안등급은 크게는 A, B, C, D 4단계, 세부적으론 A1, B3, B2, B1, C2, C1, D 총 7단계로 나뉜다.
(3) 1987년에 설립된 ISO와 IEC의 첫째 합동 기술 위원회이다. ISO의 정보 기술 표준안과 IEC의 정보 기술 표준안의 충돌을 막음으로 정보 기술의 표준화를 보다 효율적으로 추진하는 것이 주목적이다.

17. 다음에서 설명하는 것은?

개인정보 처리자의 자율적인 개인정보 보호활동을 촉진하고 지원하기 위한 인증 업무이며, 공공 기관, 민간기업, 법인, 단체 및 개인 등 모든 공공 기관 및 민간 개인정보 처리자를 대상으로 개인정보보호 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)
정답 체크)
(2) 공공기관이나 민간기업이 개인정보 유출사고 등을 예방하기 위해 추진 중인 개인정보보호 활동들이 체계적이고 지속적으로 이행될 수 있도록 촉진하는 지원체계로서, 개인정보보호 활동에 대해 객관적이고 공신력 있는 검증을 통해 개선 및 보완이 이루어질 수 있도록 자율적인 환경을 조성하는데 그 목적을 두고 있다.
오답 체크)
(1) 기업의 통합적인 정보보호 수준을 향상시키기 위하여 정보보호 준비도 수준을 자율적ㅈ으로 진단 및 평가받을 수 있는 제도이다. “정보보호 준비도 평가” 등급을 해당 기업 전체 등급으로 부여하여 이용자에게는 기업 선택의 기준을 제공하고, 정보보호 활성화 및 투자 확대를 유도한다.
(3) CC가 가지는 7개의 보증 등급을 의미한다. 보증 등급은 기능 시험(EAL-1), 구조 시험(EAL-2), 방법론적 시험과 점검(EAL-3), 방법론적 설계, 시험, 검토(EAL-4), 준정형적 설계

및 시험(EAL-5), 준정형적 검증된 설계 및 시험(EAL-6), 정형적 검증(EAL-7)으로 나눠진다.
(4) 정보통신망의 안전성 및 정보의 신뢰성을 확보하고, 조직의 정보보호 수준 제고를 위하여 관리적·기술적·물리적 보호조치를 종합한 것으로, 조직의 관리체계를 효과적으로 수립하도록 2001년 모델을 개발하여 국내 표준으로 제정되었으며 관리체계의 기본 틀이자 공통 프레임워크로 활용되고 있다.

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.
정답 체크)
(2) PIMS 인증 후, 3년간의 유효 기간이 있다.
오답 체크)
(1) 한국인터넷진흥원(KISA)은 PIMS와 ISMS의 인증기관이다.
(3) 인증 대상은 개인정보보호 활동을 체계적이고 지속적으로 수행하기 위하여 필요한 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계를 수립·운영하고 있는 개인정보 수집·취급 사업자로서 인증 신청은 자율에 맡긴다.
(4) “개인정보 보호법”에 근거하여 PIMS에 따른 안정성 확보에 필요한 조치를 다한 경우에는 과징금 및 과태료를 경감 받을 수 있다.

19. 다음은 침입탐지시스템의 탐지 분석 기법에 대한 설명이다. ㉠ ~ ㉣ 에 들어갈 내용이 바르게 연결된 것은?

침입탐지시스템에서 (㉠)은 이미 발견 되고 정립된 공격 패 턴 을 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 낮은일이 발생하면 침입탐지로 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

정답 체크)
(3)
(ㄱ) 오용탐지기법 : 이미 발견되고 정립된 공격 패턴을 미리 입력해두었다가 해당하는 패턴이 탐지되면 알려주는 것이다.
(ㄴ) False Negative : 실제로는 거짓(true)인 것이 참(false)으로 잘못 판정되는 검사 결과의 오류이다(새로운 공격은 거짓임에도 참으로 판별함).
(ㄷ) 이상탐지기법 : 정상적이고 평균적인 상태를 기준으로 급격한 변화를 일으키거나 확률이 낮은 일이 발생하면 알려주는 것이다.

(ㄹ) False Positive : 실제로는 참(true)인 것이 거짓(false)으로 잘못 판정되는 검사 결과의 오류이다(통계에 기반하기 때문에 정상적인 패킷임에도 거짓으로 구분할 가능성이 존재).

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

① 델파이법
② 퍼지 행렬법
③ 순위 결정법
④ 과거자료 접근법

정답 체크)

(4) 과거자료 접근법은 정량적 분석 방법이다.

오답 체크)

(1), (2), (3) 다음의 표는 정량적 분석과 정성적 분석 방법을 정리한 것이다.

비교	정량적 분석법	정성적 분석법
개념	위협발생확률과 손실크기를 곱해서 계산하는 기대가치분석인 경우 계산이 복잡하고 시간, 노력이 많이 들지만, 신뢰도가 있고 화폐로 표시되며 객관적임	손실크기를 화폐가치로 측정할 수 없어 위험을 기술변수로 표현하는 경우 주관적이며, 근거가 제공되지 않지만 시간, 노력, 비용이 적게듦
유형	수학공식 접근법, 확률분포 추정법, 연간예상손실(ALE), 점수법, 과거자료접근법 등(확률 지배, 몬테카를로 시뮬레이션)	델파이법, 시나리오법, 순위결정법, 질문서법, 브레인스토밍, 스토리보딩 등(퍼지 행렬법)
장점	위험 분석결과가 금전적 가치로 표시, 정보보호대책의 비용을 정당화, 위험 분석의 결과를 이해 용이, 자동화된 과정을 거쳐 일정한 객관적 결과를 산출	정보 평가에 용이, 쉽게 위험 분석을 수행가능하며 위험의 우선 순위를 파악이 용이
단점	-많은 데이터의 입력이 필요하며 복잡한 계산 필요 -완전한 정량적인 위험 분석은 불가능 -정보보호대책의 비용을 정당화 -위험 분석 결과를 이해하기 용이 -일정한 객관적 결과를 산출 -복잡한 계산으로 인한 분석시간 소요	-산정된 위험의 객관적 검증이 어려움 -위험 분석을 수행하는 사람에 따라 결과가 달라질 수 있음(주관적) -비용 효과적인 분석의 근거를 제공할 수 없음