# 2014년04월05일년 정보보안기사 필기시험 기출문제 답안

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 【1과목 : 20문제】<br>시스템 보안 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| | ② | ④ | ② | ④ | ② | ② | ① | ② | ② | ④ |
| | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| | ① | ④ | ② | ③ | ② | ② | ③ | ① | ④ | ① |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 【2과목 : 20문제】<br>네트워크 보안 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |
| | ④ | ③ | ① | ① | ③ | ④ | ④ | ③ | ④ | ① |
| | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 |
| | ③ | ② | ③ | ③ | ① | ④ | ③ | ② | ③ | ③ |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 【3과목 : 20문제】<br>어플리케이션 보안 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 |
| | ② | ② | ③ | ② | ③ | ① | ④ | ① | ③ | ④ |
| | 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | 60 |
| | ② | ② | ③ | ④ | ③ | ④ | ① | ④ | ③ | ③ |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 【4과목 : 20문제】<br>정보 보안 일반 | 61 | 62 | 63 | 64 | 65 | 66 | 67 | 68 | 69 | 70 |
| | ④ | ② | ③ | ② | ② | ③ | ① | ③ | ③ | ③ |
| | 71 | 72 | 73 | 74 | 75 | 76 | 77 | 78 | 79 | 80 |
| | ③ | ③ | ④ | ③ | ③ | ① | ② | ④ | ④ | ④ |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 【5과목 : 20문제】<br>정보보안 관리 및 법규 | 81 | 82 | 83 | 84 | 85 | 86 | 87 | 88 | 89 | 90 |
| | ④ | ③ | ③ | ② | ③ | ④ | ② | ② | ④ | ① |
| | 91 | 92 | 93 | 94 | 95 | 96 | 97 | 98 | 99 | 100 |
| | ④ | ③ | ④ | ② | ① | ① | ④ | ③ | ③ | ③ |

전자문제집 CBT 홈페이지 : https://www.cbtestpro.kr

최신 수정 자료와 해설(오타・오답・규정변경)은 cbtestpro.kr 웹 및 앱에서 확인하세요.

기출문제의 저작권은 출제기관에 있습니다. cbtestpro.kr 및 관련 앱에서는 편집 및 재구성 작업만 하였음을 밝힙니다.

CBT기출문제

전자문제집 CBT

빠르고 효과적으로 배워 시험 합격을 노려라!

Download on the App Store

GET IT ON Google Play

## 【1과목】 시스템 보안 (20문제)

1. NTFS에서 Sector_per_cluster로 정할 수 없는 것은 무엇인가?

① 1

❷ 6

③ 8

④ 16

2. 가상메모리를 지원하는 운영체제에서 성능은 가상주소를 실주소로 변환하는 DAT(Dynamic Address Translation)에 의해 영향을 받는다. DAT를 빠른 순서에서 느린 순서로 나열한 것은?

① 직접사상 – 연관사상 – 직접/연관사상

② 연관사상 – 직접사상 – 직접/연관사상

③ 직접/연관사상 – 직접사상 – 연관사상

❹ 연관사상 – 직접/연관사상 – 직접사상

3. 다음 설명하고 있는 스케줄링 기법은은 무엇인가?

```
- 작업처리 기준
- CPU 사이클 시간의 길이가 작은 것부터 우선 처리
- 대화식 시스템에는 부적합
```

① 선입선출(FIFO)

❷ SJF

③ 우선순위

④ 다단계큐

4. 다음 중 버퍼 오버플로우 대응책으로 올바르지 못한 것은?

① 버퍼 오퍼플로우 취약점이 생기지 않도록 패치를 정기적으로 한다.

② 문자길이를 검사하지 않는 함수를 사용하지 않고 안전한 프로그래밍을 해야 한다.

③ 함수로부터 복귀할 때 스택의 무결성을 검사한다.

❹ 사용자의 스택 혹은 힙 영역의 쓰기 및 실행권한을 준다.

5. 다음은 리눅스 파일권한에 대한 설명이다. 올바르지 못한 것은?

① ls –al명령어로 권한을 자세히 볼 수 있다.

❷ chmod명령어는 파일, 디렉토리명을 수정할 수 있다.

③ 맨앞에 문자가'-'이면 파일, 'd'이면 디렉토리, 'l'이면 링크이다.

④ chown 명령어는 파일소유자, 파일소유그룹을 수정 할 수 있다.

6. 다음중 레지스트리 키 값에 없는 것은?

① HKEY_CLASSES_ROOT

❷ HKEY_LOCAL_MACHINE_SAM

③ HKEY_USERS

④ HKEY_CURRENT_USER

7. 다음 보여주고 있는 아파치 관련 설정파일은 무엇인가?

```
DocumentRoot /home/abc
  ServerName abc.example.com
```

❶ httpd.conf

② apache.conf

③ virtualhost.conf

④ server.conf

8. 다음중 패스워드로 가장 강력한 것은?

① 123qwe

❷ wJqHdK12!%$

③ ASDqwe

④ qwerasdf

9. 시스템 무결성을 유지하기 위한 명령어는 무엇인가?

① halt

❷ shutdown

③ reload

④ reboot

10. 다음 중 HTTP/1.1 프로토콜에 대한 설명으로 올바르지 않은 것은?

① 클라이언트가 서버에 커넥션을 시도한다.

② HTTP/1.1 GET방식으로 데이터를 요청한다.

③ 서버는 해당 데이터를 검색하여 클라이언트에게 전달한다.

❹ POST는 클라이언트가 정보를 받아들이고 클라이언트에서 동작하도록 요청하는 방식이다.

11. 공유폴더 사용권한의 특징에 대한 설명으로 올바르지 못한 것은?

❶ 공유폴더 사용권한은 파일에도 적용된다.

② NTFS사용권한보다 약한 보안을 제공한다.

③ 네트워크 접근 사용만을 제한하고 로컬접속을 제어할 수 없다.

④ 기본 공유폴더 사용권한은 Everyone 그룹에게 모든 권한이 주어진다.

12. 프로세스 교착상태 발생조건에 해당되지 않는 것은?

① 점유와 대기

② 상호배제

③ 비중단조건

❹ 중단조건

13. 다음 나열된 도구들이 공통적으로 가지고 있는 특징은 무엇인가? CGISCAN, WINSCAN, RPCSCAN

① 다중취약점 스캔

❷ 특정취약점 스캔

③ 은닉스캔

④ 네트워크 구조 스캔

14. 다음중 기본 공유폴더 형태가 아닌 것은?

① C$

② ADMIN$

❸ PRINT$

④ IPC$

15. 다음은 리눅스 시스템 최적화 모니터링 명령어들이다. 무엇을 모니터링 하는 명령어인가? FREE, VMSTAT

① CPU문제점 점검

❷ 메모리 문제점 점검

③ 디스크I/O문제점 점검

④ 네트워크 문제점 점검

16. TCP_WRAPPER 활용시에 로그파일은 일반적으로 ( )과 ( )파일에 기록된다. 괄호안에 순서대로 알맞은 내용은?

① dmessage, secure

❷ message, secure

③ btmp, message

④ wtmp, secure

17. 다음에서 설명하고 있는 스캔탐지도구는 무엇인가?

포트스캔을 실시간으로 탐지하고 tcp_wrapper와 결합하여 hosts.deny 파일에 자동으로 ip를 등록하여 방어해주는 스캔 탐지형 도구이다.

① SARA

② NESSUS

❸ PORTSENTRY

④ NIKTO2

18. 파일이 생성되는 순간부터 로그인가 로그아웃의 정보를 보여주는 로그 파일은 무엇인가?

❶ wtmp

② utmp

③ last

④ secure

19. 다음 중 커널에 대한 설명으로 올바르지 못한 것은?

① 커널은 프로세스, 파일시스템, 메모리 , 네트워크의 관리를 맡는다.

② 컴퓨터 운영체제 핵심으로서 컴퓨터의 가장 기본적인 각 장치들을 관리하고 제어하기 위한 소프트웨어이다.

③ 장치 혹은 시스템의 기능과 관련된 변화가 있을 경우 새로운 커널을 생성해야한다.

❹ 유닉스 계열의 시스템이 부팅될 때 가장 먼저 읽히는 운영체제의 핵심으로 보조기억장치에 상주한다.

*20.* 버퍼오버플로우에 대한 설명으로 올바르지 않은 것은?

❶ 버퍼에 저장된 프로세스 간의 자원 경쟁을 야기해 권한을 획득하는 기법으로 공격하는 방식이다.

② 오버플로우에는 힙오버플로우와 스택오버플로우가 있다.

③ 버퍼오버플로우가 발생하면 데이터는 인접한 포인트 영역까지 침범한다.

④ 대응책은 데이터가 들어가는 배열의 읽기, 쓰기가 배열 범위를 벗어나지 않는지 검사한다.

## 【2과목】 네트워크 보안 (20문제)

*21.* 다음 나열된 장비 중 네트워크 계층에서 이용하는 장비는 무엇인가?

① 리피터

② 허브

③ 브릿지

❹ 라우터

*22.* 다음중 IP클래스 범위로 올바르지 않은 것은?

① A : 0.0.0.0 ~ 127.255.255.255

② B : 128.0.0.0 ~ 191.255.255.255

❸ C: 193.0.0.0 ~ 223.255.255.255

④ D : 224.0.0.0. ~ 239.255.255.255

*23.* 다음은 IPSec 프로토콜에 대한 설명이다. 괄호안에 알맞은 내용으로 연결된 것은?

IPSec은 IP계층에서 데이터를 안전하게 보호하기위하며 인증에 필요한 ( ㄱ )과 암호에 필요한 ( ㄴ )를 이용하고 키 관리에는 ( ㄷ )이 이용된다.

❶ AH-ESP-IKE

② ESP-IKE-AH

③ ESP-AH-IKE

④ IKE-ESP-AH

*24.* 다음과 같은 사이버 공격기법을 무엇이라 하는가?

- A기업 전산망이 외부공격으로 인한 시스템 손상으로 모든 업무마비
- 외주 직원 노트북에 감염된 악성코드를 이용해 내부 시스템에 침입
- 공격자는 p2p프로그램으로 악성코드 유포 이후 7개월 동안 감시 후 공격 집행

❶ APT 공격

② 드라이브 바이 다운로드 공격

③ 워터링 홀 공격

④ 랜섬웨어 공격

*25.* 내부에서 백신설치 여부나 컴퓨터 이름 등으로 pc나 노트북 등 매체등을 제어할 수 있는 솔루션을 무엇이라 하는가?

① ESM

② MDM

❸ NAC

④ SEIM

*26.* 설명하고 있는 네트워크 공격방법은 무엇인가?

스위치에 주소테이블이 가득차게 되면 모든 네트워크 세크먼트로 브로드캐스팅하게 된다. 공격자가 위조된 MAC주소를 지속적으로 네트워크에 내보냄ㅇ로써 스위칭 허브의 주소 테이블을 오버플로우시켜 다른 네트워크 세그먼트의 데이터를 스니핑 할 수 있게 된다.

① ARP 스니핑

② ICMP Redirect

③ ARP 스푸핑

❹ 스위치 재밍

*27.* 스위치 환경에서 나타나는 스니핑 기법이 아닌 것은 무엇인가?

① 스위치 재밍

② ICMP Redirect

③ ARP 스푸핑

❹ 세션하이재킹

28. 라우터는 목적지까지 가는 최단경로를 계산하기 위해 다익스트라 알고리즘을 사용한다. 가장 적합한 라우팅 알고리즘은 무엇인가?

① RIP
② IGRP
❸ OSPF
④ EIGRP

29. 다음에서 설명하는 프로세스 스케줄링 방법은 무엇인가?

CPU를 기다리는 프로세스를 여러 큐에 줄을 세운다는 측면에서 멀티레벨 큐와 동일하나 프로세스가 하나의 큐에서 다른 큐로 이동가능하다는 점이 다르다.

① FIFO
② SJF
③ RR
❹ MLFQ

30. 다음에서 설명하고 있는 것은?

만일 어떤 프로세스가 일정한 시간이 지났는데도 자발적으로 CPU를 내놓지 않을 때는 그 클록이 인터럽트를 발생시켜 운영체제가 CPU의 제어권을 갖게 한다. 이렇게 하여 운영체제가 제어권을 갖게 되면 실행상태에 있던 프로세스는 준비상태로 바뀌고 준비 리스트의 첫 프로세스가 실행 상태로 되는 것이다.

❶ 인터럽트 출력
② RTC
③ FSB
④ 오버클럭

31. ICMP에서 TTL=0이 되어 도달할 때 메시지는 무엇인가?

① ICMP unreachable
② echo reply
❸ TTL exceeded
④ echo request

32. 다음 보기에서 설명하고 있는 네트워크 토폴로지는 무엇인가?

- 네트워크 구현이 가장 쉽다
- 중앙 집중식 관리, 오류감지 및 문제 해결이 용이하다.
- 중앙 허브가 고장 나면 전체 네트워크가 마비된다.

① 메시형
❷ 스타형
③ 트리형
④ 버스형

33. 모든IT시스템에서 생성되는 로그와 이벤트를 통합관리래 외부 위험을 사전에 예측하고 내부 정보 유출을 방지할 수 있도록 하는 개념의 보안 솔루션은 무엇인가?

① ESM
② IAM
❸ SIEM
④ DLP

34. 다음 포트스캔 중 공격자가 공격했을 때 포그가 열린 경우 돌아오는 응답이 다른 하나는?

① FIN
② NULL
❸ TCP
④ UDP

35. 다음 설명하고 잇는 공격방식은 무엇인가?

- 출발지와 목적지 IP주소를 공격자 IP로 동일하게 한다.
- 공격 대상이 스스로 계속해서 SYN 패킷을 보내는 공격방법이다.

❶ Land attack
② Ping of Death
③ Tear Drop
④ Smurf Attack

*36.* 스니핑 방지 대책으로 올바르지 않은 것은?

① 원격 접속 시에는 SSH프로토콜을 이용하여 전송간 암호화한다.

② 메일 사용 시에 S/MIME가 적용된 안전한 메일을 이용한다.

③ 전자상거래 이용 시 SSL이 적용된 사이트를 이용한다.

❹ 스위치에서 MAC주소 테이블을 동적으로 지정한다.

*37.* 다음 중 IPSec VPN프로토콜에 대한 설명으로 올바르지 않은 것은?

① IPSec은 3계층 프로토콜이다.

② AH와 ESP기능을 지원한다.

❸ 종단시스템에서 출발하고 종단시스템에서 수신하는 모드를 터널모드라한다.

④ IETF에 의해 IP계층 보안을 위한 개방형 구조로 설계된 VPN기술이다.

*38.* 다음 중 무선 랜 보안대책 수립으로 올바르지 못한 것은?

① AP전파가 건물 내로 한정 되도록 한다.

❷ AP는 외부인이 쉽게 접근하거나 공개된 장소에 설치한다.

③ AP가 제공하는 강력한 키를 설정하고 주기적으로 변경한다.

④ WIPS등을 설치하여 불법접근이나 악의적인 의도 차단을 모니터링한다.

*39.* 시스템에 대한 침임 탐지와 차단을 동시에 할 수 있는 솔루션은 무엇인가?

① SIEM

② ESM

❸ IPS

④ IDS

*40.* 다음에서 설명하고 있는 네트워크 공격 기법은 무엇인가?

| 로컬에서 통신하고 있는 서버와 클라이언트 IP주소에 대한 2계층 MAC주소를 공격자의 MAC주소로 속여 클라이언트가 서버로 가는 패킷이나 서버에서 클라이언트로 가는 패킷을 중간에서 가로채는 공격을 말한다. |
|---|

① 세션하이재킹

② IP스푸핑

❸ ARP스푸핑

④ 스니핑공격

## 【3과목】 어플리케이션 보안 (20문제)

*41.* FTP전송 모드에 대한 설명으로 올바른 것은?

① 기본은 액티브 모드이며, 패시브 모드 변경은 FTP서버가 결정한다.

❷ 기본은 액티브 모드이며, 패시브 모드 변경은 FTP클라이언트가 결정한다.

③ 기본은 패시브 모드이며, 패시브 모드 변경은 FTP서버가 결정한다.

④ 기본은 패시브 모드이며, 패시브 모드 변경은 FTP클라이언트가 결정한다.

*42.* FTP접속 시 PORT 명령으로 보기와 같은 내용을 확인 하였다.

| 208,163,132,1, 9, 17 |
|---|

다음접속 포트는 몇 번인가?

① 2,320

❷ 2,321

③ 2,322

④ 2,323

*43.* 전자상거래 프로토콜 중에서 주문정보와 지불정보를 안전하게 이용할 수 있도록 하는 프로토콜은 무엇인가?

① 단체서명

② 단독서명

❸ 이중서명

④ 은닉서명

*44.* 전자투표와 전자화폐의 공통된 요구조건 사항은?

① 양도성

❷ 익명성(비밀성)

③ 단일성

④ 합법성

**45.** 다음 설명하고 있는 보안 전자우편시스템 프로토콜은?

| - RSA Data Security, INC 개발<br>- 전자우편 메세지 표준 기반<br>- 다양한 상용툴킷<br>- X.509 지원 |
|---|

① PEM

② MIME

❸ S/MIME

④ PGP

**46.** 다음 전자투표 방식 중 군중이 밀집한 지역에 투표기가 설치되어 투표할 수 있는 무인투표 시스템방식은 무엇인가?

❶ 키오스크방식

② PSEV방식

③ REV방식

④ LKR방식

**47.** 다음중 가치 저장형 전자화폐 프로토콜이 아닌 것은?

① 몬덱스

② Visa Cash

③ K-Cash

❹ Milicent

**48.** 다음에서 설명하고 있는 OTP(일회용패스워드)생성 방식은 무엇인가?

| 서버와 OTP토큰 간에 동기화된 시각 정보를 기준으로 특정시간마다 변하는 비밀번호를 생성하는 방식이다. 이 방식은 사용자의 인증요청과 상관없이 특정 시간 간격마다 OTP가 매번 바뀌므로 공격자가 해킹에 사용할 수 있는 OTP를 얻어내기 어렵다. |
|---|

❶ 시간동기화 방식

② 이벤트통기화 방식

③ 질문응답방식

④ 조합방식

**49.** 다음 설명하고 있는 DB접근 제어방식은 무엇인가?

| 개별 데이터의 접근은 허용되지 않고 통계함수에 의한 접근만 가능할 때 통계에 의해 얻은 데이터로부터 개별 데이터를 얻어낼 수 있는 경우를 말한다. |
|---|

① 접근통제

② 흐름제어

❸ 추론제어

④ 데이터 제어

**50.** 메일과 관련이 없는 서비스 포트는?

① 109

② 995

③ 993

❹ 163

**51.** 다음 중 OWASP TOP10 2013에 포함되지 않는 것은?

① 인젝션

❷ URL접근제한 실패

③ XSS

④ 크로스사이트 요청변조

**52.** 다음에서 설명하고 있는 웹 공격 방법은 무엇인가?

| 로그인된 피해자의 취약한 웹어플리케이션에 피해자의 세션쿠키와 기타 다른 인증정보를 자동으로 포함하여 위조된 HTTP요청을 강제로 보내도록 하는 것이다. 이것은 취약한 어플리케이션 피해자로부터 정당한 요청이라고 오해 할 수 있는 요청을 강제로 만들 수 있다. |
|---|

① 알려진 취약점 컴포넌트 사용

❷ 크로스사이트 요청변조

③ 민감한 데이터 노출

④ 인증 및 세션관리 취약점

**53.** 소프트웨어 보안약점 중 보안기능을 적절하지 않게 구현했을 때 발생할 수 있는 보안 약점이 아닌 것은?

① 부적절할 인가

② 패스워드 평문저장

❸ 제어문을 사용하지 않는 재귀함수

④ 사용자 중요정보 평문 전송

54. SET프로토콜의 장점이 아닌 것은?

① 전자거래의 사기를 방지한다
② 기존 신용카드 기반 그대로 활용한다.
③ SSL의 단점을 해결한다.
❹ 암호 프로토콜이 너무 복잡하다.

55. 다음 설명 중 SSL프로토콜에 대한 설명으로 올바르지 못한 것은?

① 1994년 네스케이프사에서 처음 제안하였다.
② 1996년 IETF에서 SSL3.0을 제안하였다.
❸ SSL이 적용되었다는 표시로 SHTTP라고 사용한다.
④ SSL프로토콜은 TCP계층과 응용계층 사이에서 동작한다.

56. 다음 중 지불브로커 시스템 특징이 아닌 것은 무엇인가?

① 독립적 신용구조를 갖지 않는다.
② 신용카드, 은행을 이용하여 지불하도록 연결하는 구조이다.
③ 현실적 전자 지불 시스템이다.
❹ 실제 화폐를 대치할 수 있다.

57. 다음 중 전자입찰시스템에서 요구하는 안전성에 포함되지 않는 것은?

❶ 단일성
② 비밀성
③ 무결성
④ 공평성

58. 다음 중 ebXML 종류에 포함되지 않는 것은?

① SAML
② XKMS
③ XACML
❹ CALS

59. Mod_security 아파치 모듈 기능에 포함되지 않는 것은?

① Request filtering : 요청이 들어와서 웹서버나 다른 모듈에 의해 사용되기전에 요청을 분석한다.
② Anti-evasion TechnIques : 회피공격에 대응하기 위해 분석 전에경로나 파라미터 값들을 표준화 한다.
❸ Audit Logging : 사후 사고에 대한 분석을 위한 세부 상황 기록기능은 없다.
④ HTTPS Filtering : 웹서버에 모듈로 끼워지기 때문에 요청된 데이터가 복호화 된 후 에 접근이 가능하다.

60. 다음에서 설명하고 있는 DNS공격 방법은 무엇인가?

> 취약한 DNS서버에 조작된 쿼리를 전송하여 DNS 서버가 저장하고 있는 주소 캐시정보를 임으로 변조하는 공격을 말한다.

① DNS DDOS
② DNS하이재킹
❸ DNS 캐시 포이즈닝 공격
④ DNSSEC

## 【4과목】 정보 보안 일반 (20문제)

61. 공개키 기반구조(PKI)의 응용분야가 아닌 것은?

① SET
② S/MIME
③ PGP
❹ 커버로스

62. 다음에서 설명하는 DRM기술은 무엇인가?

> 인간의 감지 능력으로는 검출 할 수 없도록 사용자의 정보를 멀티미디어 콘텐츠 내에 삽입하는 기술로 콘텐츠를 구매한 사용자의 정보를 삽입함으로써 이후에 발생할 될 콘텐츠 불법 배포자를 추적하는데 사용하는 기술이다.

① 워터마킹
❷ 핑거프린팅
③ 템퍼링기술
④ DOI

63. 다음 중 커버로스에 대한 설명으로 올바르지 못한 것은 무엇인가?

① MIT에서 개발한 분산 환경 하에 개체인증 서비스를 제공한다.
② 클라이언트, 인증서버, 티켓서버, 서버로 구성된다.
❸ 커버로스는 공개키 기반으로 만들어 졌다.
④ 커버로스의 가장 큰 단점은 재전송공격에 취약하다는 것이다.

64. 실시간 인증서 상태를 알려주는 프로토콜은 무엇인가?

① CRL
❷ OCSP
③ PCA
④ DPV

65. 다음에서 설명하는 해시함수 성질은 무엇인가?

> X가 주어졌을 때 H(X`)=H(X)인 X`=X가 아닌 것을 찾는 것은 계산적으로 어려워야 한다.

① 강한 충돌회피성
❷ 약한 충돌회피성
③ 일방향성
④ 계산의 용이성

66. 다음 중 임의적 접근통제 (DAC)설명으로 올바르지 않은 것은?

① 객체에 대하여 사용자가 접근권한을 추가 혹은 삭제 할 수 있다.
② 가장 일반적인 구현은 접근통제목록(ACL)을 통해 이루어진다.
❸ ACL은 중앙 집권적 통제방법에 적합하다.
④ 대부분 운영체계에서 지원된다.

67. 블록암호화 모드 중 암호문 블록이 파손되면 2개의 평문블록에 영향을 끼치는 운영모드는 무엇인가?

❶ CBC
② CFB
③ OFB
④ ECB

68. 한 단계 앞의 암호문 블록이 존재하지 않을 때 대신할 비트열을 무엇이라 하는가?

① 패딩
② 스트림
❸ 초기벡타(IV)
④ 블록모드

69. KDC(신뢰분배센터)에 사용자 수가 증가 될 때 영향으로 올바르지 못한 것은?

① 가입자 n의 증가에 따른 키 관리가 복잡해진다.
② 장기간 사용 시 세션 키가 노출 될 위험성이 발생한다.
❸ KDC 키가 늘어나지 않는다.
④ 가입자 수 N에 따라 한 가입자마다 상대가입자수(N-1)만큼의 상호 세션키를 비밀리에 보관해야 한다.

70. 생일역설(Birthday attack)에 한전한 해시함수 비트는?

① 64비트
② 32비트
❸ 180비트
④ 128비트

71. 다음 중 암호 운영모드 중 스트림 암호와 같은 역할을 하는 운영모드는?

① ECB, CBC
② CBC, OFB
❸ OFB, CFB
④ CTR, OFB

72. 생체인식 기술에서 요구하는 사항에 포함되지 않는 것은?

① 보편성
② 구별성
❸ 일시성
④ 획득성

73. 해시함수의 특징으로 올바르지 못한 것은?

① MAC와 달리 키를 사용하지 않는다.
② 에러 탐색기능을 제공한다.
③ 해쉬함수 자체는 비밀이 아니기 때문에 해시값을 포함한 암호가 필요하다.
❹ 메시지 한 비트 변화가 해시코드의 일부의 변화만 가져온다.

74. 커버로스 프로토콜에서 티켓에 포함되는 사항이 아닌 것은?

① 서버ID
② 클라이언트ID
❸ 서버의 네트워크주소
④ 티켓의 유효기간

75. 다음 중 접근통제정책에 포함되지 않는 것은?

① DAC
② MAC
❸ NAC
④ RBAC

76. 무결성에 기반 한 접근통제 모델로 낮은 무결성 등급의 데이터는 읽을 수 없고, 높은 등급의 데이터는 수정 할 수 없는 접근 통제 모델은?

❶ 비바모델
② 벨-라파듈라모델
③ 클락윌슨모델
④ 접근통제모델

77. 다음과 같은 특성을 가지는 접근통제 모델은 무엇인가?

```
- no read up
- no write down
```

① 클락윌슨모델
❷ 벨-라파듈라 모델
③ 비바모델
④ 내부접근통제 모델

78. 공개키 인증서에 포함되지 않는 내용은 무엇인가?

① 버전
② 일련번호
③ 유효기간
❹ 개인키 정보

79. 인증서 취소사유에 해당되지 않는 것은?

① 인증서 발행 조직에서 탈퇴
② 비밀키 손상
③ 비밀키의 유출의심
❹ 공개키의 공유

80. 다음 공개키 암호알고리즘 중에서 이산대수에 기반 한 알고리즘이 아닌 것은?

① Diffi-Hellman
② El Gamal
③ DSA
❹ RSA

## 【5과목】 정보보안 관리 및 법규 (20문제)

81. 다음 중 법에 따른 암호화 대상이 아닌 것은?

① 주민등록번호
② 바이오정보
③ 비밀번호
❹ 전화번호

82. 위험의 구성요소가 아닌 것은?

① 자산
② 위협
❸ 손실
④ 취약성

83. 다음 중 CCTV를 설치할 수 있는 곳이 아닌 것은?

① 교도소
② 교통단속을 위한 도로
❸ 범죄 예방을 위한 발열 실(목욕탕, 사우나)
④ 병원

84. 다음에서 설명하는 위험처리 방식은?

위험이 존재하는 프로세스나 사업을 수행하지 않고 포기하는 것을 말한다.

① 위험수용
❷ 위험회피
③ 위험전가
④ 위험감소

85. 다음 중 정량적 위험분석 방법론에 속하지 않는 것은?

① 과거자료 분석법
② 확률분포법
❸ 순위결정법
④ 수학공식접근법

**86.** 다음 중 정성적 위험평가 방법에 대한 설명으로 올바르지 못한 것은?

① 계산에 대한 노력이 적게 든다.

② 위험분석과정이 지극히 주관적이다.

③ 측정결과를 화폐로 표현하기 어렵다.

❹ 위험관리 성능평가가 용이하다.

**87.** 다음 중 개인정보보호법 의한 암호화 대상을 고르면?

주민등록번호, 계좌번호, 카드번호, 여권번호

① 주민등록번호

❷ 주민등록번호, 여권번호

③ 주민등록번호, 계좌번호, 카드번호

④ 주민등록번호, 계좌번호, 여권번호, 카드번호

**88.** 공인인증서에 포함하지 않는 것은 무엇인가?

① 가입자 이름

❷ 주소

③ 일련번호

④ 유효기간

**89.** 다음 중 공인인증서 소멸 요건이 아닌 것은?

① 공인인증서 유효기간이 경과된 경우

② 공인인증기관의 지정이 취소가 된 경우

③ 공인인증서 효력이 정지된 경우

❹ 공인인증서 훼손이 된 경우

**90.** 공인인증서 폐지요건으로 올바르지 못한것은?

❶ 공인인증서 효력이 정지된 경우

② 사기 기타 부정한 방법으로 발급받은 사실을 인지한 경우

③ 사망•실종선고 또는 해산 사실을 인지한 경우

④ 전자서명생성정보가 분실•훼손 또는 도난•유출된 사실을 인지한경우

**91.** 개인정보 누출시 통지해야 할 사항으로 올바르지 못한 것은?

① 개인정보 누출항목

② 개인정보 누출 발생시점과 사유

③ 개인정보 2차 피해를 최소화하기 위한 방안

❹ 정보서비스 제공자의 법적 대리인 및 연락처

**92.** 다음 중 공인인증 업무로 적절한 것은 무엇인가?

① 행정자치부장관은 공인인증업무를 안전하고 신뢰성 있게 수행할 능력이 있다고 인정되는 자를 공인인증기관으로 지정할 수 있다.

② 공인인증기관으로 지정 받을 수 있는 자는 국가기관지방자치단체에 한한다.

❸ 공인인증기관 가입자 또는 인증무역 이용자를 부당하게 차별하여서는 아니 된다.

④ 공인인증기관이 인증업무를 폐지하고자 하는 때에는 폐지하고자 하는 날의 30일전까지 이를 가입자에게 통보하고 미래창조과학부 장관에게 신고하여야 한다.

**93.** 개인정보보호법에서 개인정보 수집 시 고지 항목으로 올바르지 못한 것은?

① 이용목적

② 이용항목

③ 이용기간

❹ 파기방법

**94.** 개인정보보보험에 의한 대리인의 권한 행사 나이는?

① 만13세 이상

❷ 만14세 미만

③ 만16세 이상

④ 만18세 미만

**95.** 개인정보보호법에 따른 사내 개인정보보호 교육의 주기는?

❶ 1년에 1회

② 1년에 2회

③ 1년에 3회

④ 1년에 6회

**96.** 다음 중 주요통신기반시설 취약성 평가/분석 기관이 아닌 것은?

❶ 한국정보화진흥원

② 한국인터넷진흥원

③ 지식정보보안컨설팅전문업체

④ 한국전자통신연구원

97. 개인정보 3자 위탁(제공시 동의) 설명으로 올바르지 못한 것은?

① 동의를 받은 경우

② 개인의 불이익 항목을 고지(알린다)한다.

③ 법률에 정한경우

❹ 정보서비스보다 개인의 이익이 상당한 때

98. 지식정보보안 컨설팅 전문업체 지정 결격사유에 해당하지 않는 것은?

① 파산선고를 받고 복권되지 않는 사람

② 미성년자, 금치산자 또는 한정치산자

❸ 금고 이상의 실형을 선고받고 면제된 날로부터 1년이 지나지 않는 사람

④ 금고이상의 형의 집행유예 선고나 그 유예기간에 있는 사람

99. 지식정보보안 컨설팅 전문업체 지정에 대한 근거 법은 무엇인가?

① 전자서명법

② 정보통신기반 보호법

❸ 정보통신산업진흥법

④ 정보통신망 이용촉진 및 정보보호 등에 관한법률

Download on the App Store 전자문제집 CBT(App Store) :[다운로드]
GET IT ON Google Play 전자문제집 CBT(Google Play) :[다운로드]

100. 개인정보처리자가 시스템에 접속한 기록을 최소한 보관해야 하는 기간은 얼마인가?(2019년 06월 07일 개정된 규정 적용됨)

① 3개월

② 6개월

❸ 1년

④ 2년