2021년03월27일년 정보보안기사 필기시험 기출문제 답안

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

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

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

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

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

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. 다음 지문에서 설명하고 있는 공격은 무엇인가?

> 인텔, AMD, ARM의 CPU 제품에서 발견된 보안 취약점 중 하나이다. 인텔 CPU에서 사용하는 비순차 명령 실행 검사 우회 버그를 악용하여 해킹 프로그램이 CPU의 캐시 메모리에 접근하고, 데이터를 유출할 수 있게 되는 취약점이다.

① 스펙터
② 캐시 포이즈닝
③ 멜트다운
④ 미라이

2. 내부 정보 유출 차단을 위한 보안 제품은 무엇인가?

> PC에 에이전트를 설치하여 메일, SNS, 웹사이트 등을 통해 발생할 수 있는 중요 정보 유출을 탐지하여 차단한다.

① DRM
② DLP
③ VDI
④ EDMS

3. 다음 중 Windows에서 사용하는 일반사용자 그룹인 Users 그룹에 대한 설명 중 적합하지 않은 것은?

① User는 시스템 크기의 레지스트리 설정, 운영체제 파일 또는 프로그램 파일을 수정할 수 없다.
② User는 워크스테이션을 종료할 수는 있지만 서버는 종료할 수 없다.
③ Users가 로컬 그룹을 만들 수는 있지만 자신이 만든 로컬 그룹만 관리할 수 있다.
④ Users 그룹의 구성원은 다른 Users 그룹에서 실행할 수 있는 프로그램을 설치할 수 있다.

4. 파일 무결성 점검 도구에 해당하는 것은?

① John the Ripper
② Tripwire
③ Snort
④ Nmap

5. 주체가 주도적으로 자신이 소유한 객체(파일 등)에 대한 접근권한(Read, Write, Execution, Append 등)을 다른 주체(사용자)에게 양도하는 등의 행위가 가능한 접근통제 정책은?

① MAC
② RBAC
③ CBAC
④ DAC

6. 다음 지문이 설명하는 파일 시스템은?

> 마이크로소프트사가 윈도우 CE 6.0 장치와 데스크톱 운영체제인 윈도우 비스타 및 윈도우 7 그리고 윈도우 서버 2008에 도입하기 위해 만들었다. 자료구조의 오버헤드 문제나 파일 크기/디렉터리 제약 문제에 효과적이다.

① exFAT(Extended File Allocation Table)
② ext4(extended file system)
③ HFS(Hierarchical File System)
④ ReFS(Resilient File System)

7. 다음은 윈도우 부팅 순서이다. 올바르게 나열된 것은?

> 가. MBR - 부팅 매체에 대한 기본적인 파일시스템 정보가 들어 있는 MBR 정보를 읽는다.
> 나. POST - 하드웨어 자체가 시스템에 문제가 없는지 기본적인 사항을 체크하는 과정
> 다. NTLDR - 하드디스크의 부팅 파티션에 있는 프로그램으로 윈도우가 부팅될 수 있도록 간단한 파일시스템을 실행하며 boot.ini 파일의 내용을 읽는다.
> 라. NTDETECT.com - 설치된 하드웨어를 검사한다.
> 마. ntoskrnl.exe - HAL.dll을 로드한다.
> 바. CMOS - 사용자가 설정한 기본 사항을 읽어 시스템에 적용한다.

① 바-다-라-가-마-나
② 나-바-가-다-라-마
③ 나-바-다-라-가-마
④ 바-가-마-나-다-라

8. 소유자 외에는 읽기, 쓰기, 실행 등 일체의 접근을 불허하기 위한 umask 설정값으로 알맞은 것은?

① umask 077

② umask 020

③ umask 022

④ umask 066

9. 'last' 명령을 사용하여 정보를 확인할 수 있는 로그파일은?

① wtmp

② utmp

③ pacct

④ lastlog

10. 다음 지문에서 설명하는 파일은 무엇인가?

> 리눅스 /etc 디렉터리 안에 위치하며, IP주소와 호스트 이름을 매핑하는 이 파일에 비인가자 쓰기 권한이 부여된 경우, 공격자는 악의적인 시스템 등록을 통해 정상적인 DNS를 우회하여 악성 사이트로의 접속을 유도하는 파밍 공격 등을 실행할 수 있다.

① hosts.equiv

② hosts

③ inetd.conf

④ shadow

11. 다음 지문에서 설명하는 것은?

> 쿠키와 결합되어 이용자가 웹사이트를 이용하거나 이메일을 보내는 등의 행동을 모니터링하기 위해 사용하는 1픽셀*1픽셀 정도 크기의 임베딩된 이미지를 말한다. 이것은 주로 마케팅 목적으로 사용되며 Web bug, pixel tag, e-mail 트래킹이라는 다양한 이름으로 불리며, 해커에 의해 모니터링용 도구로 사용되기도 한다.

① Session

② Web Beacon

③ Super Cookie

④ History Stealing

12. access log에는 referer라는 필드가 존재한다. 이 필드가 의미하는 것은?

① 서비스에서 발생하는 이벤트 서버와 글로벌 카달로그 사이의 연결문제를 기록한다.

② 사이트를 방문한 사용자가 어떤 경로를 통해 사이트를 방문했는지 알 수 있게 해준다.

③ 시스템 구성요소가 기록하는 이벤트로 시스템 부팅 시 드라이버가 로드되지 않는 경우와 같이 구성요소의 오류를 기록한다.

④ 응용프로그램이 기록한 다양한 이벤트가 저장되며, 저장되는 부분은 소프트웨어 개발자에 의해 결정된다.

13. 루트 사용자 소유로 SUID 권한을 부여한 경우, 이러한 파일로 의심되는 파일을 검색하는 명령어로 알맞은 것은?

① find / -user –perm –1000 -print

② find / -user –perm –2000 -print

③ find / -user –perm –3000 -print

④ find / -user –perm –4000 -print

14. Unix 명령($ ls -l)의 실행 결과에 대한 설명으로 가장 옳은 것은?

```
-rwxr--r-- aaa bbb 98 Aug 7 19:16 ccc
```

① 파일 aaa에 대한 소유자는 bbb이다.

② 파일 bbb에 대한 소유자는 aaa이다.

③ 파일 ccc에 대한 소유자는 aaa이다.

④ 파일 aaa에 대한 소유자는 ccc이다.

15. Crontab을 이용해 정기적으로 매일 오전 1시에 아파치 웹 서버 로그를 백업하고자 한다. 백업 경로는 /backup/logs/ 이며, 파일 이름은 “log-년월일시분” 형식을 따른다. 정상적으로 작동시키기 위해 Crontab에 등록해야할 값으로 올바른 것은? (파일이름 예시: log-201903210019)

① * * * 1 0 cp /etc/httpd/logs/access_log /backup/logs/log-'date +＼%Y＼%m＼%d＼%H＼%M'

② 0 1 * * * cp /etc/httpd/logs/access_log /backup/logs/log-'date +＼%Y＼%m＼%d＼%H＼%M'

③ * * * 0 1 cp /etc/httpd/logs/access_log /backup/logs/log-'date +＼%Y＼%m＼%d＼%H＼%M'

④ 0 1 * * 0 cp /etc/httpd/logs/access_log /backup/logs/log-'date +＼%Y＼%m＼%d＼%H＼%M'

16. 하드웨어 및 소프트웨어를 탑재한 시스템 요소를 의미하는 것은?

① TCB
② EGID
③ PCB
④ CC

17. 윈도우 로그는 무엇인가?

> 이 로그는 윈도우 운영체제의 구성요소가 기록하는 로그이다. 이 로그는 운영체제가 시작될 때, 장치 드라이버의 로드 여부 등을 이벤트로 남긴 것을 말한다.

① 응용 프로그램 로그
② 시스템 로그
③ 보안 로그
④ 설정 로그

18. 파일 공유와 관련된 서비스 포트에 대한 내용으로 적절하지 않은 것은?

① 445(TCP/UDP, Direct Host)
② 139(TCP, NetBIOS Session)
③ 137(UDP, NetBIOS Name)
④ 335(UDP, NetBIOS Datagram)

19. 유닉스 시스템에서 계정과 패스워드에 관련된 설명으로 틀린 것은?

① 유닉스 시스템에서 사용자들은 각각 고유의 아이디를 갖고 있으며, 그 아이디에 대한 정보는 /etc/passwd에 저장된다.
② 유닉스 시스템에서는 각각의 사용자만이 접근 가능한 파일과 디렉터리가 존재할 수 있다.
③ 사용자 패스워드는 /etc/passwd 또는 /etc/shadow 파일에서 관리한다.
④ /etc/shadow 파일에는 사용자의 패스워드가 AES-256 알고리즘에 의해 암호화되어 저장된다.

20. 접근권한을 확인하였더니 'rwSr- -r- -'이었다. 권한 내의 대문자 S에 대한 설명으로 옳은 것은?

① SetUID를 실행 권한이 없는 파일에 설정할 경우 대문자 S로 표기된다.
② SetGID를 실행 권한이 없는 파일에 설정할 경우 대문자 S로 표기된다.
③ 디렉터리에 스티키 비트가 설정되어 대문자 S로 표기하였다.
④ SetGID를 설정하여 대문자 S로 표기하였다.

【2과목】 네트워크 보안 (20문제)

21. 다음은 WEP에 대한 설명이다. 빈칸 ㉠에 들어갈 내용으로 적절한 것은?

> WEP(Wired Equivalent Privacy)는 무선랜 통신을 위한 암호화 기술 중 가장 기본적인 방법이다. 암호화 알고리즘으로는 RC4를 사용하고, 암호화키 길이는 64비트 또는 128비트이다. 무선 단말에서 무선 AP와 통신을 위해 인증 요청을 보내고, 요청을 받은 무선 AP에서는 중간에 키를 계속 가로챌 경우 키 생성 순서를 예측하는 것을 방지하기 위해 랜덤하게 (㉠)를 생성하여 무선 단말기에 보낸다.

① Encryption Key
② Initial Key
③ Initial Vector
④ Encryption Vector

22. 무선랜의 전송 패킷에 덧붙여지는 32bytes 길이의 고유 식별자로서, 무선장치들이 BSS(Basic Service Set)에 접속할 때 패스워드같이 사용되는 코드는 무엇인가?

① 무선 네트워크 아이디(SSID)
② WEP(Wired Equivalent Privacy)
③ MAC(Message Authentication Code)
④ RFID 태그

23. 지문에서 설명하고 있는 것은?

> 이것은 폐쇄적이었던 네트워크 장비들을 열린 구조로 바꾸고 소프트웨어로 제어할 수 있는 기능성을 통해서 네트워크 구조의 새로운 패러다임을 이끌고 있으며 네트워크의 관리적인 측면에서 많은 발전을 이루고 있다. 트래픽의 미세흐름 조정을 통해 네트워크의 효율성을 높이고, 지금까지 어려웠던 QoS 보장 기술을 확보하며, 손쉬운 장비 관리 등 네트워크의 성능과 관리성을 향상시킬 수 있다.

① NFV(Network Function Virtualization)

② MDR(Managed Detection & Response)

③ EDR(Endpoint Detection & Response)

④ SDN(Software Defined Networking)

24. 다음 중 지능형 지속 위협에 대한 설명으로 옳은 것은?

① 공격의 설계부터 침투까지 매우 빠른 시간 내에 이루어진다.

② 다른 형태의 공격들에 비해 대체로 공격자의 비용이 적게 든다.

③ 시스템관리자는 가능한 모든 공격을 고려해야 되기 때문에 방어가 매우 어렵다.

④ 하나의 타깃에 대해서 같은 방법으로 지속적으로 뚫을 때까지 공격하는 것이다.

25. 다음 지문의 빈칸 ㉠, ㉡에 들어갈 용어로 올바르게 짝지어진 것은?

> 무차별 모드로 설정하면 자신의 (㉠) 주소로 오는 패킷이 아닌 것도 전달받을 수 있다. 이를 방어하기 위한 가장 효과적인 대처 방안은 (㉡)이다.

① ㉠ MAC ㉡ 암호화

② ㉠ MAC ㉡ 인증

③ ㉠ 스위치 ㉡ 인증

④ ㉠ 스위치 ㉡ 암호화

26. OSI 7 Layer 중 어느 계층에 대한 설명인가?

> 데이터를 주고 받을 때 데이터의 유실(Loss)이 없도록 보장해주는 계층이며, 신뢰성을 보장하기 위해 데이터를 주고 받는 End-to-End에서 전달받은 데이터의 오류를 검출하고, 만약 오류가 있다고 판단되면 재전송을 요청한다.

① Transport Layer

② Network Layer

③ Session Layer

④ Physical Layer

27. 틀린 것은?(문제 복원 오류로 문제 내용이 정확하지 않습니다. 정확한 문제 내용을 아시는분 께서는 오류신고를 통하여 내용 작성 부탁 드립니다. 정답은 2번 입니다.)

① 출발지 211.1.99.1 / 목적지주소 32.15.1.1인 패킷은 규칙 1에 의해 거부된다.

② 출발지 211.1.99.1 / 목적지주소 32.15.6.15인 패킷은 규칙 2에 의해 허용된다.

③ 출발지 211.1.37.15 / 목적지주소 32.15.6.15인 패킷은 규칙 2에 의해 허용된다.

④ 출발지 211.1.37.15 / 목적지주소 32.15.1.1인 패킷은 규칙 3에 의해 차단된다.

28. TCP의 3-Way Handshaking을 통한 서버와의 연결 설정 과정에서, 연결에 성공한 클라이언트 측의 연결 상태 천이 다이어그램상의 상태 변화의 순서를 바르게 나열한 것은?

① CLOSED→SYN_RCVD→ESTABLISHED

② CLOSED→SYN_SENT→ESTABLISHED

③ LISTEN→SYN_RCVD→ESTABLISHED

④ LISTEN→SYN_SENT→ESTABLISHED

29. 보안 솔루션은 무엇인가?

> 다양한 보안 위협에 대한 대응 프로세스를 자동화해 낮은 수준의 보안 이벤트는 사람의 도움 없이 처리하고, 보안사고 발생 시 표준화된 업무 프로세스에 따라 담당자가 쉽게 대응할 수 있는 차세대 솔루션이다.

① SIEM

② SOAR

③ NGFW

④ UTM

30. 다음 지문은 무엇에 대한 설명인가?

> 패킷이 목적지까지 도달하는 동안 거치는 라우터 IP를 확인하는 도구이다. 이 도구는 udp와 icmp, ip의 ttl 값을 이용한다. 상대방의 IP 주소를 알고 있는 상태에서 상대방에게 인터넷 서비스를 제공하고 있는 회사를 알아내는 데 사용할 수 있다.

① traceroute

② ping

③ netstat

④ route

31. NMAP 포트 스캔에 대한 설명으로 올바르지 못한 것은?

① TCP Connect Scan: 대상 포트에 대해 3-Way Handshaking을 정상적으로 통신하는 방식으로 정상적이면 포트가 열려있다고 판단할 수 있다.

② TCP FIN Scan: 대상 포트로 FIN 패킷을 전송하는 방식으로 응답을 받으면 포트가 열려있다고 판단할 수 있다.

③ TCP X-MAS Scan: 대상 포트로 FIN, URG, PSH 플래그가 모두 설정된 패킷을 전송하는 방식으로 응답을 받으면 포트가 닫혀있다고 판단할 수 있다.

④ TCP Null Scan: 대상 포트로 NULL 패킷을 전송하는 방식으로 응답을 받으면 포트가 닫혀있다고 판단할 수 있다.

32. 다음 중 스푸핑 공격의 종류가 아닌 것은?

① ARP

② DNS

③ IP

④ UDP

33. 가장 상위의 계층에서 이루어지는 서비스 거부 공격은 무엇인가?

① ICMP Flooding Attack

② LAND Attack

③ HTTP GET Flooding Attack

④ Teardrop Attack

34. 침입탐지시스템(IDS)에 대한 설명으로 가장 옳은 것은 무엇인가?

① 침입 경로를 찾을 수 있도록 탐지대상으로부터 생성되는 로그를 제공한다.

② Host-IDS는 운영체제에 독립적이다.

③ 오용 침입탐지 기법은 오탐률(False Positive)이 높다.

④ '침입분석 및 탐지→ 데이터수집→데이터 가공 및 축약→보고 및 대응'의 단계로 실행된다.

35. 공격 특징 및 대응방안과 관련성이 가장 높은 것은?

> 웹서버 OS의 TCP 스택(Stack) 자원을 소모하는 특징을 갖는 웹서버 자원 소모 공격으로 사용될 수 있으며, 그 대응방법으로 Anti-DDoS 장비에서 소스 IP별로 PPS 임계치를 설정하거나 패킷 헤더 검사를 통해 정상적인 옵션 필드값을 갖지 않는 비정상 패킷을 차단할 수 있다.

① UDP Flooding

② SYN Flooding

③ ICMP Flooding

④ GET Flooding

36. VPN에 대한 설명으로 올바르지 못한 것은?

① SSL VPN은 웹브라우저만 있으면 언제 어디서나 사용이 가능하다.

② IPSec VPN은 네트워크 계층에서 안전하게 정보를 전송하는 방법이다.

③ IPSec VPN은 운영방식에 따라 트랜스포트 모드만 지원하고 암호화 여부에 따라 ESP, AH 프로토콜을 사용한다.

④ 기본적으로 SSL VPN과 IPSec VPN은 데이터의 기밀성과 무결성이 동일하며, 단지 데이터의 암호화 구현 방식에 차이가 있다.

37. 다음 지문에서 빈칸 ㉠에 해당하는 것은?

> (㉠)는 웹서버를 대신하여 HTTP 요청을 충족시키는 네트워크 개체이다. 자체의 저장 디스크를 갖고 있어 최근 호출된 객체의 사본을 저장 및 보존한다. 브라우저는 사용자의 모든 HTTP 요청이 먼저 (㉠)에 보내지도록 구성될 수 있다. 이렇게 설정되면 객체에 대한 각각의 브라우저 요청들은 가장 먼저 (㉠)에 보내지게 된다.

① Proxy
② Cookie
③ Apache
④ ActiveX

38. 침입탐지시스템(IDS)에 대한 설명으로 가장 적절하지 않은 것은?

① 패킷의 유형에 따라 차단하거나 보내주는 간단한 패킷 필터링 기능을 제공한다.
② 네트워크상의 패킷을 분석하여 침입을 탐지하거나, 내부 사용자들의 활동을 감시하여 해킹 시도를 탐지한다.
③ 네트워크 기반, 호스트 기반, 오용 탐지, 비정상 탐지 등이 있다.
④ 침입 경로를 찾을 수 있도록 탐지대상으로부터 생성되는 로그를 제공한다.

39. 비대면 업무 환경에 대한 설명으로 올바르지 않은 것은?

① 기업 업무망에 안전하게 접속하기 위해서는 VPN 또는 암호통신이 필수적이다.
② 원격 근무자가 기업 업무망에 VPN을 통해 접속할 경우 다중 인증을 사용하지 않아도 안전하다.
③ 구축형 영상회의 플랫폼을 이용할 경우 참가자는 기업에서 제공하는 VPN을 이용해서 접속해야 한다.
④ 비대면 업무에 사용하는 네트워크 환경이 안전하지 않을 경우 통신 내용 또는 데이터가 유출될 수 있다.

40. traceroute 프로그램은 icmp protocol을 이용하여 패킷의 전송경로를 보여주는 프로토콜이다. 다음 icmp 메시지 중 traceroute와 연관이 있는 것은?

> 가. 시간초과(time exceeded)
> 나. 에코(echo)
> 다. 송신지 억제(source quench)
> 라. 타임스탬프(timestamp)

① 가, 나
② 나, 다
③ 다, 라
④ 가, 라

【3과목】 어플리케이션 보안 (20문제)

41. 다음 지문에서 설명하는 DRM 기술은 무엇인가?

> 디지털 저작권 보호 관리를 위한 정보보호 기술의 하나로서 디지털 이미지, 오디오, 비디오 등 디지털 형식으로 되어 있는 지적재산의 저작권 보호를 위해 자료에 삽입한 비트 패턴을 말한다. 동일한 자료에 삽입되는 비트 패턴은 항상 동일하다.

① DOI
② 핑거프린팅
③ 안티탬퍼링 기술
④ 워터마킹

42. 서버를 점검하던 중 다음과 같은 문장이 포함된 ASP 스크립트가 존재하는 것을 알게 되었다. 의심되는 공격은 무엇인가?

```
<% eval request("cmd") %>
```

① Buffer Overflow
② CSRF
③ 웹셸(WebShell)
④ DoS/DDoS

43. 다음 지문에서 설명하고 있는 DNS 구성요소는?

> 인터넷상에 산재하여 존재하고 있는 네임서버들 가운데에서 특정한 도메인 이름에 대해서 원하는 유형의 리소스 레코드 데이터를 조회하는 기능을 수행하는 역할을 한다.

① whois 클라이언트
② 리소스 레코드 에이전트
③ 도메인 제어기
④ 리졸버

44. HTTP 요청 방식은 무엇인가?

> 이 요청 방식은 게시판 등에 파일 업로드를 위해 주로 사용하는 방식으로서 URL에 요청 데이터를 기록하지 않고, HTTP 바디에 데이터를 전송한다. 따라서 인수값을 URL을 통해 직접 전송하지 않기 때문에 다른 사람이 링크를 통해 해당 페이지를 볼 수 없다.

① GET 방식

② POST 방식

③ HEAD 방식

④ CONNECT 방식

45. FTP 공격 유형 중 어떤 공격 유형인지 고르면?

> FTP 서버가 데이터를 데이터 포트(20/TCP)로 전송할 때 목적지가 어딘지 검사하지 않는 프로토콜의 구조적 문제점을 이용하는 공격 유형이다. 익명 FTP 서버를 이용해 공격자가 자신을 숨기고 PORT 명령을 조작하여 공격대상의 네트워크 및 포트스캔, Fake Mail 전송, 데이터 전송이 가능하며, 또한 방화벽 내부에 FTP 서버가 있으면 방화벽 패킷 필터링을 무시하고 여러 공격이 가능하다.

① FTP 무차별 대입 공격

② FTP 바운스 공격

③ 익명 FTP 공격

④ TFTP 공격

46. 다음 빈칸 ㉠에 들어갈 내용으로 알맞은 것은?

> 웹 세션 동작 메커니즘 중 클라이언트가 세션 토큰을 포함하지 않은 HTTP 요청 메시지를 전송했을 때, 서버는 클라이언트로 응답 메시지를 보내는 경우에 헤더에 (㉠)값을 설정하면 클라이언트에 쿠키를 만들 수 있다.

① Cookie

② Set-Cookie

③ Session

④ Keep-alive

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

47. 전자서명(Digital Signature) 메커니즘에서 제공되는 기능과 가장 거리가 먼 것은?

① 메시지 송신자에 대한 인증

② 전자서명 메시지에 대한 부인방지

③ 전자서명 검증 과정을 통한 메시지 무결성

④ 송수신 메시지에 대한 비밀성

48. 다음 지문에서 설명하는 서명 방식은?

> SET에서 도입된 기술로 상점이 카드 사용자의 계좌번호와 같은 지불정보를 모르게 하는 동시에 상점에 대금을 지불하는 은행은 카드 사용자가 상점에서 산 물건을 모르지만 상점이 요구한 결제 대금이 정확한지 확인할 수 있게 한다.

① 이중 서명

② 은닉 서명

③ 비밀 서명

④ 지불 서명

49. TFTP에 대한 설명으로 옳지 않은 것은?

① RRQ와 WRQ 메시지는 클라이언트가 서버에게 전송하는 요청이다.

② DATA 메시지는 클라이언트와 서버가 모두 사용한다.

③ ACK 메시지는 클라이언트와 서버가 모두 사용한다.

④ TCP 69번 포트를 통해 데이터를 전송한다.

50. PGP는 전자우편 보안 시스템이다. PGP가 제공하지 않는 기능은?

① 전자서명

② 압축

③ 수신 부인방지

④ 단편화와 재조립

51. ㉠, ㉡에 들어갈 내용으로 올바르게 짝지어진 것은?

> FTP 서버가 Passive mode로 동작할 수 있기 위해서는 보안 정책에서 모든 인터넷으로부터 FTP 서버로 목적지 포트 (㉠)/TCP, 모든 인터넷으로부터 FTP 서버로 목적지 포트 (㉡)이상/TCP 허용하는 규칙이 필요하다.

① ㉠ 21 ㉡ 1024

② ㉠ 20 ㉡ 1024

③ ㉠ 21 ㉡ 2048

④ ㉠ 20 ㉡ 2048

52. 인터넷 메일 구조의 핵심요소에 대한 설명으로 옳지 않은 것은?

① MUA－사용자 액터(actor)와 사용자 응용프로그램을 대신하여 동작한다.

② MSA－원격서버로부터 POP3 또는 IMAP를 사용하여 메시지를 추출한다.

③ MDA－메시지를 MHS에서 MS로 메시지를 전달한다.

④ MTA－메시지가 목적지 MDA에 도달할 때까지 중계 역할을 한다.

53. 다음 중 웹(Web) 방화벽이 수행하는 주요 기능이 아닌 것은?

① 파일 업로드 제어 및 검사 기능

② HTTP 공격 패킷 탐지 및 차단

③ 웹 서버 오류 필터링 및 기밀 정보 유출 차단

④ IP 주소와 포트 기반 패킷 탐지 및 차단

54. 다음 지문에서 설명하고 있는 원칙으로 적절한 것은?

> 증거는 획득, 이송, 분석, 보완, 법정제출이라는 일련의 과정이 명확해야 하고 이런 과정에 대한 추적이 가능해야 한다.

① 재현의 원칙

② 무결성의 원칙

③ 정당성의 원칙

④ 연계보관성의 원칙

55. 웹 보안 취약점은 무엇인가?

> 세션 쿠키, SSL 인증서, 윈도우 도메인 인증과 같이 자동으로 입력된 신뢰 정보를 기반으로 한 웹 애플리케이션에서 사용자의 요청을 변조함으로써 해당 사용자의 권한으로 악의적인 공격을 수행한다. 공격 대상은 클라이언트가 아니라 서버이며, 웹 2.0 환경에서 매우 효과적인 공격 기법이다.

① XSS

② CSRF

③ WebShell

④ Injection Flaws

56. 다음 중 OTP에 대한 설명으로 틀린 것은?

① OTP는 전송계층에서 동작한다.

② 정적인 일반 패스워드와 달리 단방향 암호 기반의 해시를 매번 다르게 계산하여 패스워드로 사용한다.

③ OTP 생성 및 인증 방식에는 S/KEY 방식, 시간 동기화 방식 등이 있다.

④ 온라인 뱅킹, 전자상거래, 온라인 게임 등에 사용된다.

57. 다음에 제시된 <보기 1>의 사용자 인증방법과 <보기 2>의 사용자 인증도구를 바르게 연결한 것은?

<보기 1>
ㄱ. 지식 기반 인증
ㄴ. 소지 기반 인증
ㄷ. 생체 기반 인증
<보기2>
A. OTP 토큰 B. 패스워드 C. 홍채

	[ㄱ]	[ㄴ]	[ㄷ]
①	A	B	C
②	A	C	B
③	B	A	C
④	B	C	A

① ①

② ②

③ ③

④ ④

58. DNS 공격 유형은 무엇인가?

> 해커가 DNS 서버를 해킹하거나, 패킷을 조작하여 특정 도메인에 대응하는 IP 주소를 해커가 원하는 IP 주소로 위조하는 기법이다.

① DNS 터널링

② DNS 스푸핑

③ DNS 하이재킹

④ NXDOMAIN 공격

59. 다음 중 유일하게 HTTP(HyperText Transfer Protocol) 응답(response)에 body data가 없는 메소드는?

① HEAD

② GET

③ TRACE

④ POST

60. 전자상거래 SET 보안 프로토콜의 송신측 암호화 절차이다. 빈칸 ㉠, ㉡, ㉢, ㉣에 들어갈 용어로 적절한 것은?

> 가. 송신자는 메시지를 압축하고, 압축된 메시지를 다시 송신자의 (㉠)로 암호화하여 전자서명을 만든다.
> 나. 원문 메시지에 전자서명을 첨부한 다음 이를 (㉡)로 암호화한다.
> 다. 그 다음 사용된 (㉢)를 다시 수신자의 RSA (㉣)로 암호화한 후 암호문과 함께 전송한다.

① ㉠ 공개키 ㉡ 대칭키 ㉢ 대칭키 ㉣ 개인키

② ㉠ 개인키 ㉡ 공개키 ㉢ 대칭키 ㉣ 공개키

③ ㉠ 공개키 ㉡ 대칭키 ㉢ 공개키 ㉣ 공개키

④ ㉠ 개인키 ㉡ 대칭키 ㉢ 대칭키 ㉣ 공개키

【4과목】 정보 보안 일반 (20문제)

61. 다음 지문에서 BLP 모델에 대한 설명으로 옳지 않은 것은?

① No-write-down 정책은 인가받은 보안등급 이하의 정보를 수정하지 못하게 하는 정책이다.

② BLP 모델에서는 정보를 Top Secret, Secret, Unclassified 등과 같은 보안 등급에 따라 분류하고 있으며 정보의 기밀성 보장에 초점을 두고 있다.

③ BLP 모델에서 주체와 객체의 보안등급은 각각 취급등급(clearance), 비밀등급(security label)을 사용한다.

④ No-read-up 정책은 낮은 보안등급을 인가받은 주체가 보안등급이 높은 객체에 대한 읽기/쓰기 접근을 허용하지 않음으로 정보의 기밀성을 보장하게 된다.

62. 다음 해시함수 설명 중 잘못된 것은?

① 해시함수는 임의의 유한 길이의 비트 스트링을 고정된 길이의 비트 스트링으로 변환하는 함수이다.

② 효율적 전자서명 생성을 위해 전자서명 생성 과정에서 해시함수가 사용된다.

③ 일방향 특성으로서 해시함수 h에 대해 해시값 y로부터 h(x)=y가 되는 입력값 x를 찾는 것이 계산상 불가능해야 한다.

④ 강한 충돌방지 특성으로서 해시함수 h에 대해 h(y)=h(x)가 되는 입력값 쌍 y와 x(단, $y \neq x$)를 찾는 것이 어렵지 않아야 한다.

63. RSA 암호화 방식에서 공개키가 (7,33), 개인키가 (3,33)일 경우, 공개키로 암호화 한 값이 3이라고 할 때 이를 복호화 한 값은 무엇인가?

① 99

② 27

③ 2,187

④ 343

64. CRL에 포함되어야 하는 기본 필드에 속하지 않는 것은?

① 버전(Version)

② 서명 알고리즘(Signature)

③ 다음 발급일자(Next Update)

④ 인증서 효력정지 및 폐지 목록 번호(CRL Number)

65. RADIUS 프로토콜의 기본 기능과 가장 거리가 먼 것은?

① 인증

② 계정 관리

③ 권한 부여

④ 책임추적성

66. 한국형 암호 알고리즘은 무엇인가?

> 국가보안기술연구소에서 2013년 개발한 경량 블록 암호 알고리즘으로 2019년 국제표준으로 제정되었다. 특징으로는 AES 암호알고리즘에 대비하여 경량 암호로 높은 처리량, 낮은 전력소비로 사물인터넷 암호화에 적합한 알고리즘이다.

① SEED

② ARIA

③ HIGHT

④ LEA

67. 해시함수 h의 성질에 관한 설명 중 틀린 것은?

① 역상저항성은 주어진 임의의 출력값 y에 대해 y =h(x)를 만족하는 입력값 x를 찾는 것이 계산적으로 불가능한 성질이다.

② 두 번째 역상 저항성은 주어진 입력값 x에 대해 h(x)=h(x')를 만족하는 다른 입력값 x'을 찾는 것이 계산적으로 불가능한 성질이다.

③ 충돌 저항성은 h(x)=h(x')를 만족하는 두 입력값 x와 x'을 찾는 것이 계산적으로 불가능한 성질이다.

④ 충돌 저항성은 역상 저항성을 보장한다.

68. 암호 알고리즘 공격 방법은 무엇인가?

> 암호 해독자가 사용된 암호기에 접근할 수 있어 평문에 해당하는 암호문을 얻을 수 있는 상황에서 키를 추정하여 암호를 해독하는 방법이다.

① 암호문 단독 공격

② 기지 평문 공격

③ 선택 평문 공격

④ 선택 암호문 공격

69. Kerberos 키 분배 프로토콜의 기반 기술에 해당하는 것은?

① Needham-Schroeder 프로토콜

② Challenge-Response 프로토콜

③ Diffie-Hellman 프로토콜

④ RSA 이용 키 분배 프로토콜

70. 다음 지문이 설명하는 해시(Hash) 함수에 해당하는 것은?

> - 128비트 출력
> - 512비트 블록단위로 처리
> - 4라운드 64단계로 구성

① MD4

② MD5

③ SHA-1

④ SHA-256

71. 전자서명이 갖추어야 할 조건이 아닌 것은?

① 개인키를 알고 있는 서명자만 서명을 생성할 수 있다.

② 서명자를 누구든지 검증할 수 있다.

③ 문서의 해시값에 서명하므로 생성된 서명은 다른 문서에 재사용할 수 있다.

④ 서명자는 자신의 서명 사실을 부인할 수 없다.

72. 다음 지문이 설명하는 키 교환 방식은?

> 양자 간에 완성된 키를 교환하지 않고, 서로가 주고받은 특정 정보로 양자가 동일한 키를 계산하여 키를 분배한다.

① KDC 교환 방식

② RSA 키 교환방식

③ Diffie-Hellman 키 교환방식

④ 사전공유 키 교환방식

73. 전자서명의 요구사항으로 가장 적절하지 않은 것은?

① 전자서명을 위조하는 것이 계산적으로 실행 불가능해야 한다.

② 전자서명 생성이 비교적 용이해야 한다.

③ 기억장소에 전자서명의 복사본을 유지하는 것이 실용적이어야 한다.

④ 위조와 부인을 방지하기 위하여 수신자에 대한 정보를 사용해야 한다.

74. 블록암호 모드는 무엇인가?

> 초기값을 암호화한 값과 평문 블록을 XOR하여 암호문 블록을 생성하고, 그 암호문을 입력으로 사용하여 다시 암호화한 값과 평문 블록을 XOR하여 암호문 블록을 생성하는 작업을 반복하는 방식이다. 암호화에서는 특정 평문 블록이 이후의 모든 암호문 블록에 영향을 미치지만, 복호화에서는 특정 암호문 블록 오류의 영향이 국지적이라는 특성을 갖는다.

① 암호 블록체인 모드(Cipher Block Chaining Mode)

② 암호 피드백 모드(Cipher Feedback Mode)

③ 출력 피드백 모드(Output Feedback Mode)

④ 카운터 모드(Counter Mode)

75. 공개키 암호화 방식에 대한 설명으로 옳은 것은?

① 고급 데이터 암호화 기법

② DES(Data Encryption Standard)

③ 부인방지 및 인증 지원

④ 암호화 속도가 빠름

76. 해시함수에 대한 내용으로 옳지 않은 것은?

① 정보의 무결성을 확인하기 위한 목적으로 사용한다.

② 해시함수는 일방향성, 충돌 회피, 효율성의 특징이 있다.

③ SHA-1 함수는 MD5보다 조금 느리지만 보안성 측면에서 좀 더 안전하다.

④ 인증에서 증명 용도로 사용될 수 있다.

77. ㉠, ㉡, ㉢에 들어갈 내용으로 적절한 것은?

> 정보시스템에 백신 프로그램을 설치한 후, 최신으로 유지하지 않는다면 해당 시스템은 바이러스에 (㉠)을 가지고 있는 것이다. 여기서 바이러스는 시스템을 공격하는 (㉡)이 되고, 바이러스 공격으로 발생하는 해당 시스템의 피해 가능성을 (㉢)이라고 한다.

① ㉠ 취약점 ㉡ 위협 ㉢ 위험

② ㉠ 위험 ㉡ 위협 ㉢ 취약점

③ ㉠ 위험 ㉡ 취약점 ㉢ 위험

④ ㉠ 취약점 ㉡ 위험 ㉢ 위협

78. 생체인증 기술의 정확성을 나타내는 FRR(False Rejection Rate)과 FAR(False Acceptance Rate)에 대해서 잘못 설명한 것은?

① 시스템에 접근하려 할 때 FRR이 낮으면 사용자 편의성이 증대된다.

② 시스템에 접근하려 할 때 FAR이 높으면 사용자 편의성이 증대된다.

③ 시스템의 생체인증 보안성을 강화하게 되면 FRR이 높아진다.

④ 시스템의 생체인증 보안성을 강화하게 되면 FAR이 높아진다.

79. 공격과 이를 방어하는 기술로 알맞게 짝지어진 것은?

> 메시지 인증 및 무결성을 보장하고자 송신자는 메시지와 함께 그 메시지의 MAC(Message Authentication Code)을 수신자에게 보낸다. 이때 공격자가 중간에 이 메시지와 MAC을 가로채서 보관한다. 그리고 송신자를 가장하여 보관 메시지 및 MAC을 그대로 수신자에게 반복해서 보내면 수신자는 송신자로부터 온 것으로 판단하고, 이를 반복해서 처리하는 공격을 받게 된다.

① 키 추측공격 – 의사난수 알고리즘, 키 길이 확대

② 중간자공격 – 대칭암호, 공개키 암호

③ 재전송공격 – 순서번호, 타임스탬프, 비표

④ 위조공격 – 일방향 해시함수, 메시지 인증 알고리즘

80. 다음 지문은 Diffie-Hellman 키 사전 분배에 대한 내용을 설명한 것이다. ㉠~㉣에 들어가야 할 단어로 옳은 것은?

> Diffie-Hellman 키 사전 분배 방식은 Diffie-Hellman의 키 교환 방식을 응용한 방식으로 (㉠)를 기반으로 구성된다. 키 분배 센터는 (㉡) p를 선정하고 Zp위에서 원시근 g를 찾아 공개한다. 가입자는 (㉢)를 선정하여 (㉣)를 계산하여 공개한다.

① ㉠ 이산대수문제 ㉡ 큰 정수 ㉢ 공개키 ㉣ 개인키

② ㉠ 이산대수문제 ㉡ 큰 소수 ㉢ 개인키 ㉣ 공개키

③ ㉠ 소인수분해문제 ㉡ 큰 정수 ㉢ 개인키 ㉣ 공개키

④ ㉠ 소인수분해문제 ㉡ 큰 소수 ㉢ 공개키 ㉣ 개인키

【5과목】 정보보안 관리 및 법규 (20문제)

81. BCP의 접근 5단계 방법론을 순차적으로 올바르게 나열한 것은?

① 프로젝트의 범위 설정 및 기획 → 복구전략 개발 → 사업영향평가 → 복구계획 수립 → 프로젝트의 수행 테스트 및 유지보수

② 프로젝트의 범위 설정 및 기획 → 사업영향평가 → 복구전략 개발 → 복구계획 수립 → 프로젝트의 수행 테스트 및 유지보수

③ 프로젝트의 범위 설정 및 기획 → 복구계획 수립 → 사업영향평가 → 복구전략 개발 → 프로젝트의 수행 테스트 및 유지보수

④ 프로젝트의 범위 설정 및 기획 → 복구계획 수립 → 복구전략 개발 → 사업영향평가 → 프로젝트의 수행 테스트 및 유지보수

82. '사이버위기경보'의 등급 중 복수 정보통신서비스제공자(ISP) 망에 장애 또는 마비가 발생하였을 경우, 발령하는 경보의 단계는 무엇인가?

① 심각 단계

② 경계 단계

③ 주의 단계

④ 관심 단계

83. 정보통신기반보호법에 따르면 관리기관의 장은 대통령령이 정하는 바에 따라 정기적으로 소관 주요정보통신기반시설의 취약점을 분석·평가하여야 한다. 이때 관리기관의 장은 특정 기관으로 하여금 소관 주요정보통신기반시설의 취약점을 분석·평가하게 할 수 있는데, 그에 속하지 아니 하는 기관은?

① 한국인터넷진흥원

② 국가정보원

③ 대통령령이 정하는 기준을 충족하는 정보공유·분석센터

④ 정부출연 연구기관 등의 설립·운영 및 육성에 관한법률의 규정에 의한 한국전자통신연구원

84. A기업은 정보보호관리체계 수립을 위한 일환으로 보호해야 할 정보자산을 식별하고 식별된 정보자산에 대한 가치평가를 하려고 한다. 이때 정보자산의 가치평가에 사용하는 평가항목으로 적절하지 않은 것은?

① 무결성 평가

② 가용성 평가

③ 기밀성 평가

④ 부인방지 평가

85. 「정보보호산업의 진흥에 관한 법률」에 따른 '정보보호 공시제도'에 관한 설명이다. 가장 거리가 먼 것은?

① 정보보호 공시제도는 정보보호에 대한 기업의 투자 현황 및 활동을 공개하여 주주의 알권리를 확보하고, 투자자들에게 투자정보를 제공하기 위한 제도이다.

② 정보보호 공시제도는 이용자들에게 정보보호에 대한 기업의 투자 현황과 활동을 공개하여 정보보호에 대한 기업의 투자를 촉진하기 위한 제도이다.

③ 정보보호 공시제도는 기업의 책임 하에 제공되는 정보이지만 공시내용의 투명성 확보를 위해 정부는 모니터링 점검단을 통해 정기적으로 공시내용에 대한 정확성을 검증한다.

④ 정보보호 공시제도를 통해 해당 기업의 정보보호 관련 투자현황, 전문인력현황, 인증현황, 정보보호 위반 관련 행정처분 내역 등을 알 수 있다.

86. 정보통신기반보호법상 중앙행정기관의 장은 소관분야의 정보통신기반시설 중 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정할 수 있는데, 이 경우에 고려할 사항으로 명시되지 않은 것은?

① 당해정보통신기반시설을 관리하는 기관이 수행하는 업무의 국가 사회적 중요성

② 침해사고가 발생할 경우 국제적으로 미칠 수 있는 피해의 범위

③ 다른 정보통신기반시설과의 상호 연계성

④ 침해사고의 발생가능성 또는 그 복구의 용이성

87. 다음은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상 정보통신망에 유통되어서는 안 되는 불법정보 관련 조항을 나열한 것이다. 실제 내용과 다른 것은 무엇인가?

① 음란한 부호·문언·음향·화상 또는 영상을 배포·판매·임대하거나 공공연하게 전시하는 내용의 정보

② 법령에 따라 금지되는 사행행위에 해당하는 내용의 정보

③ 사람을 비방할 목적으로 공공연하게 사실이나 거짓의 사실을 드러내어 타인을 모욕하는 내용의 정보

④ 공포심이나 불안감을 유발하는 부호·문언·음향·화상 또는 영상을 반복적으로 상대방에게 도달하도록 하는 내용의 정보

88. 다음 중 「개인정보 보호법」의 개인정보 보호 원칙이 아닌 것은 무엇인가?

① 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.

② 개인정보의 처리 목적에 필요한 범위에서 개인정보의 독립성, 객관성 및 공정성이 보장되도록 하여야 한다.

③ 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.

④ 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리를 보장하여야 한다.

89. 조직의 위험평가 수립 및 운영에 대한 사항으로 가장 적절하지 않은 것은?

① 위험관리 계획에 따라 위험평가를 연 1회 이상 정기적으로 또는 필요한 시점에 수행하여야 한다. 매년 위험평가 대상에 변동이 없어도 위험평가는 수행되어야 한다.

② 위험관리를 위한 수행인력, 기간, 대상, 방법, 예산 등의 방법 및 절차를 구체화한 위험관리 계획을 수립하여야 하며, 위험평가 참여자는 위험관리를 운영하는 IT 부서 또는 정보보호 부서 인력으로 구성된다.

③ 위험관리를 위한 위험평가 방법 선정은 베이스라인 접근법, 상세위험 분석법, 복합 접근법, 위협 및 시나리오 기반 등의 다양한 방법론 중에서 해당 조직에 맞는 방법론을 선정하고 유지하여야 한다. 선정한 방법론을 운영하는 과정에서 해당 조직에 적절하지 않다고 판단하여 위험분석 방법론을 변경하여도 상관없다.

④ 조직에서 수용 가능한 목표 위험수준을 정하고 그 수준을 초과하는 위험을 식별하여야 한다. 수용 가능한 목표 위험수준(DoA, Degree of Assurance)을 정보보호 최고책임자 등 경영진 의사결정에 의하여 결정하여야 한다.

90. 디지털 저작권에 관련된 사항 중 적절하지 않은 것은?

① 본인이 촬영하고 편집한 동영상은 저작물에 따로 등록하지 않아도 저작권이 적용될 수 있다.

② 온라인 비대면 수업과 회의 참가자의 사진을 허락없이 촬영하여 업로드한 경우 초상권 침해가 될 수 있다.

③ 공공 데이터포털에서 공개하고 있는 데이터의 경우 저작권자는 공개한 공공기관이므로 공공데이터는 별도의 저작권자의 이용 허락 없이 활용할 수 있다.

④ 비영리적 목적으로 사용하도록 승인한 공개 소프트웨어는 개인, 기업 모두 자유롭게 사용할 수 있다.

91. 개인정보 보호책임자의 책임 및 역할로 가장 적절하지 않은 것은 무엇인가?

① 개인정보 처리와 관련한 불만의 처리 및 피해 구제

② 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축

③ 개인정보파일의 현행화 작성

④ 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선

92. 「정보통신망법」 제44조의9에 의거하여 일정 규모 이상의 정보통신서비스제공자가 운영 및 관리하는 정보통신망을 통하여 일반에게 공개되어 유통되는 정보의 유통을 방지하기 위한 불법촬영물 등 유통 방지 책임자를 지정하도록 되어 있는 기준에 해당되지 않는 것은 무엇인가?

① 「영유아보육법」 제15조의4제3호에 따른 영상정보

② 「아동·청소년의 성보호에 관한 법률」 제2조제5호에 따른 아동·청소년성착취물

③ 「성폭력범죄의 처벌 등에 관한 특례법」 제14조의2에 따른 편집물·합성물·가공물 또는 복제물

④ 「성폭력범죄의 처벌 등에 관한 특례법」 제14조에 따른 촬영물 또는 복제물

93. 「정보통신망법」 제22조의2에 의거하여 해당 서비스를 제공하기 위하여 반드시 필요한 접근권한이 아닌 경우에 고지해야 할 사항이다. 다음 중 가장 적절하지 않은 것은?

> 「정보통신망 이용촉진 및 정보보호등에 관한 법률」 제22조의2(접근권한에 대한 동의) ① 정보통신서비스제공자는 해당 서비스를 제공하기 위하여 이용자의 이동통신단말장치 내에 저장되어 있는 정보 및 이동통신단말장치에 설치된 기능에 대하여 접근할 수 있는 권한이 필요한 경우 이용자가 명확하게 인지할 수 있도록 알리고 이용자의 동의를 받아야 한다.

① 접근권한이 필요한 이유

② 접근권한이 필요한 정보 및 기능의 항목

③ 접근권한이 필요한 기간

④ 접근권한 허용에 대하여 동의하지 아니할 수 있다는 사실

94. 개인정보 영향평가 시 고려할 사항으로 가장 거리가 먼 것은?

① 처리하는 개인정보의 수

② 개인정보의 제3자 제공 여부

③ 정보주체의 권리를 해할 가능성 및 그 위험 정도

④ 개인정보의 위탁 관리 여부

95. 다음 중 개인정보보호법에서 정의하는 개인정보를 수집할 있는 경우에 해당되지 않는 것은?

① 정보주체의 동의를 받는 경우

② 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우

③ 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우

④ 정보주체의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 개인정보처리자의 권리보다 우선하는 경우

96. 「개인정보 보호법」에 의해 정보주체는 자신의 개인정보처리와 관련하여 권리를 가지는데, 다음 중 정보주체의 권리로 적절하지 않은 것은 무엇인가?

① 개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리

② 개인정보의 처리 정지, 정정 삭제 및 파기를 요구할 권리

③ 개인정보의 처리에 관한 정보를 제공할 권리

④ 개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리

97. 침해사고 발생 대응 방법론의 일반적인 수행과정의 순서로 올바른 것은?

① 사고 전 준비 → 초기대응 → 사고탐지 → 대응전략 체계화 → 보고서 작성 → 사고조사

② 사고 전 준비 → 사고탐지 → 초기대응 → 대응전략 체계화 → 사고조사 → 보고서 작성

③ 사고 전 준비 → 사고탐지 → 초기대응 → 사고조사 → 대응전략 체계화 → 보고서 작성

④ 사고 전 준비→ 사고탐지 → 대응전략 체계화 → 초기대응 → 사고조사 → 보고서 작성

98. 정보보호 최고책임자가 수행하는 정보보호 업무와 관련 없는 것은?

① 정보보호 관리체계의 수립 및 관리·운영

② 개인정보보호 업무

③ 침해사고의 예방 및 대응

④ 중요 정보의 암호화 및 보안서버의 적합성 검토

99. 정보보안의 위험 관리 과정에서 조직의 보안 요구사항에 대한 효과적인 식별 및 효율적인 위험의 감소를 실현하기 위해 세부적인 위험 분석 방법들이 존재한다. <보기>에서 설명하는 (가)에 해당하는 위험 분석 방법으로 가장 옳은 것은?

> (가)는 모든 시스템에 대하여 표준화된 보안 대책을 제시하며 체크리스트 형태로 보안 대책이 있는지 없는지를 판단하여 적용되어 있지 않은 보안대책을 적용하는 방법으로 수행하는 위험 분석 방법

① 비정형 접근법

② 복합 접근법

③ 상세위험 분석

④ 베이스라인 접근법

100. 개인정보 보호법에 따르면 정보주체의 동의 외에도 당초 수집 목적과 합리적으로 관련된 범위 내에서 개인정보를 추가 활용할 수 있도록 허용하고 있다. 다음 중 그 합리성을 판단하는 기준과 거리가 먼 것은?

① 당초 개인정보를 수집한 목적과 관련성이 있는지 여부

② 정보주체의 이익을 부당하게 침해하는지 여부

③ 개인정보의 추가적인 이용 또는 제공에 대한 예측 가능성이 있는지 여부

④ 개인정보처리자의 정당한 이익을 달성하기 위해 필요한 경우로 명백히 정보주체 권리보다 우선하는 경우인지 여부