1과목 : 시스템 보안

1. NTFS 파일 시스템의 메타 파일에 해당하지 않는 것은?

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

① $MFT ② $Logfile
③ $Volume ④ $Bios

2. 다음 지문에서 설명하는 공격은 무엇인가?

두 프로세스 간에 자원을 사용하기 위해서 경쟁하는 것을 이용한 공격으로 시스템 프로그램과 공격 프로그램이 경쟁 상태에 이르게 하여 시스템 프로그램이 갖는 권한으로(set user id가 붙은 경우 root 권한) 파일에 접근을 가능하게 하는 방법을 말한다.

① 힙 오버플로우 공격 ② 레이스 컨디션 공격
③ 스택 오버플로우 공격 ④ 코드 기반 공격

3. 리눅스에서 새로 생성되는 사용자 계정의 홈 디렉터리는 .bashrc 등과 같이 모든 사용자가 필요로 하는 파일들을 만들어줄 필요가 있다. 이러한 공통 파일들을 미리 만들어 특정 디렉터리에 넣어두면 사용자 계정 생성 시 자동복사 되도록 설정할 수 있는데, 이러한 용도의 디렉터리는 무엇인가?

① /etc/init ② /etc/services
③ /etc/login.defs ④ /etc/skel

4. 2016년에 처음 발견되었으며 IP 카메라나 가정용 라우터와 같은 IoT 장치를 주요 공격 대상으로 삼는 DDoS 공격용 봇넷 악성코드는 무엇인가?

① 님다 ② 미라이
③ 스턱스넷 ④ SQL 슬래머

5. 다음 지문에서 설명하는 내용은 스푸핑 공격 중 어떤 공격에 해당하는가?

32bit IP 주소를 48bit의 네트워크 카드 주소(MAC Address)로 대응시켜 주는 프로토콜이고 실제로 IP 주소를 통해 네트워크 연결을 시도하면 TCP/IP에서는 해당 IP주소 해당하는 네트워크 카드 주소를 찾아 연결하게 된다. 이더넷 환경에서 공격대상자의 cache 테이블에 공격자가 원하는 IP에 대한 하드웨어 주소(MAC Address)를 거짓으로 지정하여 업데이트함으로써 공격대상자의 패킷 흐름을 공격자가 원하는 방향으로 조절하여 공격하는 기술이다.

① DHCP 스푸핑 ② IP 스푸핑
③ DNS 스푸핑 ④ ARP 스푸핑

6. 디지털저장매체 중 하드디스크 구조에서 물리적으로는 할당된 공간이지만 논리적으로는 사용할 수 없는 공간을 무엇이라고 하는가?

① 슬랙 ② CHS
③ 클러스터 ④ 확장 공간

7. 윈도우 레지스트리 키 중에서 파일의 각 확장자에 대한 정보와 프로그램의 맵핑 정보가 저장된 키로 옳은 것은?

① HKEY_CLASSES_ROOT ② HKEY_CURRENT_USER
③ HKEY_FILE_EXT ④ HKEY_LOCAL_MACHINE

8. 다음 지문에서 설명하고 있는 시스템 보안은?

- 민감한 암호연산을 하드웨어로 이동함으로써 시스템 보안을 향상시키고자 나온 개념
- 인증된 부트, 인증, 암호화와 같은 기본적인 기능을 제공
- 안전한 입출력에 사용되는 암호 프로세서를 제공

① TPM ② SRM
③ SAM ④ SID

9. 아래 지문의 척도들과 가장 관련성이 높은 보안 서비스는?

- 정보시스템의 가동시간(Up Time)
- 정지시간(Down Time)
- 평균 장애시간(MTTF, Mean Time To Failure)
- 평균 복구시간(MTTR, Mean Time to Repair)

① 기밀성 ② 무결성
③ 가용성 ④ 유지보수성

10. IoT 위협 및 보안에 대한 설명으로 올바르지 않은 것은?

① 홈가전 IoT 제품의 보안 요구사항에는 시큐어 코딩, 알려진 보안약점 및 취약점 제거, 최신 제3자(3rd party) 소프트웨어 사용 등이 있다.

② 홈캠, 네트워크 카메라 등의 네트워크 제품에 대한 주요 보안 위협에는 사진 및 동영상을 공격자의 서버 및 이메일로 전송하는 것이 있다. 이에 대한 원인으로는 접근통제 및 전송 데이터 보호의 부재가 있다.

③ 시큐어 코딩이 적용되지 않은 스마트 홈가전 제품의 경우 입력 데이터 검증 및 표현, 보안 기능, 시간 및 상태, 에러처리 등에서 보안 취약점이 발생할 수 있다.

④ 스마트 홈가전 제품의 데이터 기밀성 및 무결성을 위해 안전한 암호인 MD5, SHA-1 등의 사용이 권장된다.

11. 기존 파일 시스템에 새로운 파일 시스템을 하위 디렉터리로 연결하기 위해 사용하는 명령어는 무엇인가?

① mkfs ② mount
③ fsck ④ mknod

12. ㉠에 들어갈 내용으로 적절한 것은?

유닉스에서는 패스워드 보호를 위해 암호 처리된 패스워드 정보를 공격자가 접근하기 어렵게 일반 사용자 권한으로 접근할 수 없는 (㉠)을 사용하고 있다.

① 해시 암호화 패스워드 파일

② 섀도(Shadow) 패스워드 파일
③ 익명(Anonymity) 패스워드 파일
④ PAM(Pluggable Authentication Module) 패스워드 파일

13. [그림1]은 어떤 리눅스 시스템에 존재하는 특정 /home 디렉터리와 그 아래에 존재하는 디렉터리 및 파일들의 속성 중 name, permission, user, group 등에 대한 정보만 요약한 것이며, [그림2]는 이 시스템에 존재하는 /etc/group 파일의 일부분이다. 이를 통하여 확인할 수 있는 파일 및 디렉터리의 permission에 관한 설명 중 올바르지 않은 것은?

[그림 1]

[name]	[permisson]	[user]	[group]
/home	drwxr-xr-x	root	root
/home/user1	drwxr-x---	user1	security
/home/user1/exam.txt	-rw-rw----	user1	security

[그림 2]

security:x:510:user1,user2,user3:

① user1이란 사용자는 /home/user1 디렉터리로 이동할 수 있다
② user2란 사용자는 exam.txt란 파일의 내용을 읽을 수 있다.
③ user3란 사용자는 exam.txt란 파일을 삭제할 수 있다.
④ 시스템 내에 존재하는 user4란 사용자는 /home/user1 디렉터리로 이동할 수 없다.

14. 로그파일은?

> 다른 로그파일에 비해 많은 정보를 포함하고 있는 로그파일로 동작 중인 서비스에 대한 버퍼 오버플로우 공격의 경우와 같이 시스템 장애에 대한 정보를 로그파일로 저장한다.

① btmp ② wtmp
③ syslog ④ messages

15. 랜섬웨어에 해당하지 않는 것은?
① 페트야(Petya) ② 크립토월(CryptoWall)
③ 워너크라이(WannaCry) ④ 크립토재커(CryptoJacker)

16. 서버의 파일 시스템에 대한 시간 속성이 잘못 기술된 것은?
① mtime: 파일을 생성하거나 내용을 수정한 시간
② atime: 최근 파일을 읽거나 실행시킨 시간
③ ctime: 파일 속성이 변경된 시간
④ rtime: 파일을 실시간 실행시킨 시간

17. 다음에서 설명하고 있는 것은 무엇인가?

> 리눅스에서 시스템 관리자가 응용프로그램들이 사용자를 인증하는 방법을 선택할 수 있도록 해주는 공유라이브러리 묶음으로 이것을 사용하는 응용프로그램을 재컴파일 하지 않고, 인증방법을 변경할 수 있다는 장점이 있다.

① sudo ② PAM
③ Batch file ④ Shell script

18. 윈도우 NTFS 파일 시스템의 특징으로 옳지 않은 것은?
① 파일과 폴더에 개별 권한을 설정할 수 있어 강력한 보안 정책 설정이 가능하다.
② 이벤트 뷰어를 사용하여 MFT(Master File Table)의 내용을 확인할 수 있다.
③ FAT 파일 시스템에 없는 보안 속성(사용자 접근제어) 정보를 내장하고 있다.
④ 파일 압축 및 암호화를 위한 구조를 갖는다.

19. rlogin 접속을 허용하는 설정 파일들로 올바르게 짝지어진 것은?
① /etc/hosts.allow, /etc/exports
② /etc/hosts.allow, /.rhosts
③ /etc/hosts.equiv, /etc/exports
④ /etc/hosts.equiv, /.rhosts

20. 다음 지문에서 설명하고 있는 안전한 보안 인증 방식은?

> - 시스템 관리자가 응용 프로그램들이 사용자를 인증하는 방법을 선택할 수 있도록 해주는 일종의 공유 라이브러리이다.
> - 다양한 형태의 인증방식을 부가적으로 사용할 수 있는 장점이 있다.
> - 시스템 환경에 맞게 설정하여 각 시스템에서 사용 가능한 인증 모듈을 통해 사용자의 인증 요구를 처리한다.

① SSH(Secure Shell)
② SAM(Secure Access Module)
③ SSO(Single Sign On)
④ PAM(Pluggable Authentication Module)

2과목 : 네트워크 보안

21. ㉠에 들어갈 용어로 적절한 것은?

> 스니퍼 탐지 도구는 로컬 네트워크 상의 호스트들에서 네트워크 인터페이스 카드의 (㉠) 여부를 검사함으로써 스니퍼가 수행되고 있는지를 확인할 수 있다.

① Duplex Mode ② MAC 변조
③ Promiscuous Mode ④ ARP

22. 다음 지문에서 설명하는 공격 대응 방법은 무엇인가?

> 악성봇에 감염된 PC를 해커가 제어하지 못하도록 특정 주소로 연결을 시도할 때 실제 해당 주소로 연결되지 않게 하며 해커의 악의적인 명령을 전달받지 못하도록 한다.

① DNS 라우팅 ② DNS 스푸핑
③ DNS 웜홀 ④ DNS 싱크홀

23. Firewall, IDS, IPS의 비교 중 올바른 것으로 짝지어진 것은?

	Firewall	IDS	IPS
㉠ 패킷 차단	○	×	○
㉡ 오용 탐지	×	×	○
㉢ 이상 탐지	×	○	○
㉣ 장점	엄격한 접근통제	실시간 탐지	세션 기반 탐지 기능
㉤ 단점	외부 공격에 취약	변형 패턴 탐지 어려움	오탐 현상 발생 가능

① ㉠, ㉢ ② ㉡, ㉢
③ ㉠, ㉣, ㉤ ④ ㉠, ㉢, ㉣

24. 다음 지문에서 설명하는 용어는 무엇인가?

> 암호화, 복호화, 전자서명 등의 암호 관련 연산을 빠르게 수행하고, 암호키의 생성 및 안전한 보관을 할 수 있는 하드웨어 장치를 의미한다.

① HSM ② 비트라커
③ OTP ④ TCB

25. 침입차단시스템에 대한 설명으로 옳지 않은 것은?

① 패킷 필터링 방화벽은 패킷의 통과여부를 결정하기 위해 프로토콜 종류, 출발지 또는 목적지 IP 주소, TCP/UDP 포트 번호 등을 이용한다.

② 응용 게이트웨이 방식 방화벽은 내부망으로 패킷이 전송되는 것을 방지할 수 있으며 사용자 인증 기능도 제공할 수 있다.

③ 상태 기반 패킷 검사(SPI) 방식 방화벽은 프로토콜 종류, 출발지 또는 목적지 IP 주소, TCP/UDP 포트 번호 외에 패킷의 데이터 부분에 대한 점검도 수행하지만, nmap 도구에 의해 ACK 스캔을 차단하지 못하는 단점이 있다.

④ 심층 패킷 분석(DPI) 방식 방화벽은 패킷의 데이터 부분에 포함된 바이러스 등 악성코드를 검사할 수 있다.

26. 서비스의 가용성과 성능뿐만 아니라 DDoS 공격 대응에도 효과적이서 최근 Anycast DNS가 많이 도입되어 있다. 다음 중 이 기술에 대해 잘못 설명한 것은?

① 사용자가 접속에 사용하는 IP 주소의 패킷은 해당 주소를 갖는 가장 가까운 호스트로 라우팅된다.

② 주요 라우팅 프로토콜로 OSPF가 사용된다.

③ IPv4/IPv6 anycast 모두 적용 가능하다.

④ 1.1.1.1이나 8.8.8.8 등의 Public DNS뿐만 아니라 kr root DNS 등이 대표적인 예이다.

27. 다음 지문에서 설명하는 시스템으로 옳은 것은?

> 정형·비정형 데이터와 보안 로그 속에서 침입자 공격을 빠른 속도로 분석하고 예측해야 한다. 보안 위협 징후를 판단할 수 있는 데이터를 생성하고, 이 데이터로 보안 사고를 분석하고 예방·대응한다. 또한 로그 관리를 통합적으로 수행하며 네트워크 포렌식(Forensic)과 보안 관련 준수성(Compliance)에 중요한 역할을 담당한다.

① SIEM ② UTM
③ EMS ④ ESM

28. ㉠, ㉡, ㉢, ㉣에 들어갈 내용으로 적절한 것은?

> (㉠) 공격은 TCP 연결 설정 과정 중 3-Way Handshaking 과정에서의 Half-Open 연결 시도가 가능하다는 취약점을 이용한 공격 방식이다.
> (㉡) 공격은 패킷을 전송할 때 출발지와 목적지 IP 주소를 공격대상의 IP로 동일하게 패킷을 생성하여 전송하는 공격 방식이며, 또한 (㉢) 공격은 ICMP Request 메시지를 이용하여 공격 대상 시스템에 대량의 메시지를 전송하는 공격 방식이다. 이와 같은 방식은 (㉣) 공격에 해당한다.

① ㉠ LAND ㉡ SYN Flooding ㉢ Smurf ㉣ DoS
② ㉠ SYN Flooding ㉡ Smurf ㉢ LAND ㉣ Sniffing
③ ㉠ SYN Flooding ㉡ LAND ㉢ Smurf ㉣ DoS
④ ㉠ LAND ㉡ Smurf ㉢ SYN Flooding ㉣ Sniffing

29. 애플리케이션 계층 취약점을 이용하는 공격유형과 거리가 먼 것은?

① Heartbleed ② Memcached DDoS
③ Meltdown, Spectre ④ Shell Shock

30. 스푸핑 공격에 따른 침해사고 발생 시 네트워크 기반 증거의 출처 장비 중 물리적인 포트와 MAC 주소 간의 매핑을 저장하는 CAM 테이블을 포함하고 있으며, 조사관이 트래픽을 캡처하거나 저장할 수 있는 플랫폼을 갖는 장비는 무엇인가?

① 방화벽 ② 스위치
③ IDS ④ IPS

31. 다음 지문에서 설명하는 ICMP 메시지 타입은?

> 네트워크 상의 통신량이 폭주하여 목적지 또는 라우터 등의 메모리나 버퍼 용량이 초과되어 IP 데이터그램이 유실되는 상태가 되면 해당 에러 메시지를 송신측에 통보함으로써 일종의 흐름제어 및 혼잡제어 등의 역할을 한다.

① Source Quench ② Destination Unreachable
③ Time Exceeded ④ Parameter Problem

32. 다음 중 파일을 안전하게 전송하기 위하여 SSH(Secure Shell)를 사용하는 프로토콜은?

① SFTP(Secure FTP) ② TFTP(Trivial FTP)
③ FTPS(FTP-SSL) ④ HTTPS(HTTP-Secure)

33. 무선 네트워크 보안 프로토콜에 관한 다음 설명 중 틀린 것은?
① WEP, WPA, WPA2 모두 통신 기기들에 대한 인증과 메시지 암호화 기능을 제공한다.
② WEP에서는 암호 강도가 높지 않은 RC4를 암호화 알고리즘으로 사용하였으며, AES 기반의 강력한 암호화 방식을 의무화한 것은 WPA에서부터이다.
③ WEP에서는 인증이나 암호화에 사전 공유키를 사용할 수 있지만, WPA나 WPA2에서처럼 동적으로 암호키를 변경하는 기능을 제공하지는 않는다.
④ WPA, WPA2 등에서는 WEP에는 없는 엔터프라이즈 모드를 제공하며, 엔터프라이즈 모드에서는 인증 및 키 관리 기능을 수행하는 중앙 서버를 이용할 수 있다.

34. 네트워크 방화벽(Firewall)의 주요 기능과 거리가 먼 것은?
① 접근 제어 ② 로깅과 감사 추적
③ 인증 ④ 개인정보 마스킹

35. Smurf 공격은 보통 라우터가 패킷을 받아서 다른 포트로 forwarding할 때 목적지 IP 주소의 네트워크 부분만 참조하고 라우팅 테이블을 검색하여 패킷을 전달하는 점을 이용한 공격 방법이다. Source IP 주소를 자신의 IP 주소가 아닌 공격대상 시스템의 IP 주소로 변조한 후 subnet의 broadcast 주소로 ICMP Echo Request를 보내면 이 패킷은 라우터를 거쳐서 특정 네트워크에 도착하여 모든 시스템이 받게 된다. 그러면 네트워크의 모든 시스템은 위조된 IP 주소로 ICMP Echo Reply 패킷을 전송하게 된다. 결과적으로 시스템은 Congestion 상태에 빠지게 되어 심각한 서비스 장애를 일으킨다. 이러한 공격 방법을 방지하기 위한 설명 중 내용이 적절하지 못한 것은?
① 라우터에서 Direct Broadcast를 Disable시킨다.
② IP Broadcast 주소로 도착한 ICMP 패킷에 대한 Reply를 금지시킨다.
③ 라우터의 Ingress Filtering을 이용하여 Spoof된 패킷을 막는다.
④ 65,535byte보다 큰 ICMP Echo 패킷을 IP Fragmentation을 이용하여 전송한다.

36. VPN을 구현하는 프로토콜과 해당 프로토콜이 속하는 계층이 바르게 연결된 것은?
① L2TP - Data Link Layer ② SSH - Session Layer
③ IPSec - Transport Layer ④ SSL - Network Layer

37. 파일에 숨겨진 악성코드만 골라 막는 콘텐츠 보안 솔루션으로 파일을 분해해 악성파일 혹은 불필요한 파일을 제거하고 콘텐츠는 원본과 동일하게 새로운 파일을 만드는 솔루션은?
① CDR(Content Disarm &Reconstruction)
② WAF(Web Application Firewall)
③ DLP(Data Loss Prevention)
④ 스팸 필터 솔루션

38. 침입 탐지에 대한 설명 중 옳은 것은?
① 침입을 하는 전문적인 집단으로 CERT가 있다.
② Honey pot을 이용하면 공격자의 행동 정보를 수집할 수 있다.
③ 침입을 탐지 못하고, 통과시키는 것을 False Positive라고 한다.
④ 내부 공격자의 위협을 줄이기 위해서는 보안 설정을 Blacklist 방식으로 해야 한다.

39. 올바르지 않은 것은?
① TCP SYN 플러딩 공격은 서버의 시스템 자원에 대한 공격이며, 일반 사용자들이 서버로 접속을 못하도록 하는 공격으로 서버 측의 대기 큐의 크기를 늘리는 방법이 대응 방안이 될 수 있다.
② 스머프 공격은 UDP 플러딩 공격으로 IP 주소의 브로드캐스트 주소대역을 이용한다.
③ Teardrop 공격은 IP 단편들이 서로 중첩되도록 IP 패킷 헤더를 조작해서 수신 측의 IP 패킷의 재조합 과정에서 오류를 발생시키도록 하는 공격이나, 최신 운영체제로의 업데이트로 문제를 해결할 수 있다.
④ HTTP GET 플러딩 공격은 공격자가 에이전트 다수에게 원격에서 명령을 보내어 동시에 특정 웹 페이지를 요청하는 형태로 공격이 이루어질 수 있으며, DDoS 공격 대응 장비에서 임계치 기반 방어 기법을 사용하면 해결에 도움이 된다.

40. 아래의 결과를 보았을 때 이 네트워크는 어떠한 공격에 취약하다고 추측할 수 있는가?

```
# ping 202.102.233.255
PING 202.102.233.255 (202.102.233.255) from
211.13.2.1: 56(84) bytes of data.
64 bytes from 202.102.233.207: icmp_seq=0
ttl=126 time=3345.4 ms
64 bytes from 202.102.233.194: icmp_seq=0
ttl=126 time=3542.7 ms (DUP!)
64 bytes from 202.102.233.193: icmp_seq=0
ttl=126 time=3738.8 ms (DUP!)
64 bytes from 202.102.233.214: icmp_seq=0
ttl=126 time=4053.1 ms (DUP!)
64 bytes from 202.102.233.207: icmp_seq=1
ttl=126 time=3316.3 ms
64 bytes from 202.102.233.194: icmp_seq=1
ttl=126 time=3541.0 ms (DUP!)
```

① Land Attack ② Smurf Attack
③ Syn Flooding Attack ④ Ping of Death Attack

3과목 : 어플리케이션 보안

41. 다음 지문에서 설명하고 있는 API는?

- 사용자 브라우저를 통해 실제 키를 노출하지 않고 암호화/복호화 등을 처리한다.
- 실제 키에 대한 접근 요청을 제외한 전자서명 생성 및 검증, 해싱, 암호화, 복호화, 키 생성, 키 유도, 키 탐색 등을 수행한다.
- 인증서를 사용한 방식은 물론 TLS 클라이언트 인증서와 연동 등으로 보다 나은 인증 방법을 제공한다.

① WebCrypto API ② REST API

③ SOAP API ④ Indexing API

42. 다음 중 DB 암호화 유형 중 애플리케이션의 수정 없이 사용될 수 있는 유형으로 올바르게 짝지어진 것은?
① Plug-In 유형 - API 유형
② TDE 방식 - 파일 암호화
③ API 유형 - TDE 방식
④ Plug-In 유형 - 파일 암호화

43. CAPTCHA에 대한 설명으로 잘못된 것은?
① HIP(Human Interaction Proof) 기술의 일종이다.
② 웹사이트 회원가입 시 자동가입방지 등을 위해 사용된다.
③ 튜링 테스트(Turing Test)라고도 부른다.
④ 인공지능의 한계를 이용한 인증 기법이다.

44. XML 기반의 보안기술에 대한 설명 중 옳지 않은 것은?
① XML Signature - 무결성 및 부인방지 기능
② XKMS - PKI 서비스 기능
③ SAML - 가용성 보장 기능
④ XACML - 접근제어 기능

45. WPKI에 대한 설명으로 적절하지 않은 것은?
① 무선 인터넷 상에서의 인터넷 뱅킹, 사이버 주식 거래 시 외부 침입이나 정보 누출로부터 보호받을 수 있도록 하는 무선 인터넷 공개키 기반 구조이다.
② PKI 기술의 핵심인 비밀성, 무결성 및 신원 확인과 부인방지 같은 서비스를 무선 환경에서 구현함으로써 무선 보안을 가능하게 한다.
③ 모바일의 특성을 고려하지 않은 솔루션으로 무선 인터넷 기기와 주고받는 데이터나 애플리케이션에 보안을 지원한다.
④ 규격 내용은 전자서명, WTLS(Wireless Transport Layer Security) 인증서 프로파일, 인증서 DN(Distinguished Name), 인증서 및 알고리즘 관련 OID(Object Identifier) 등으로 구성되어 있다.

46. 모바일 앱(App) 보안에 관한 내용으로 틀린 것은?
① 서비스 지속성을 위해 루팅이나 탈옥된 단말에서도 서비스가 정상적으로 동작되어야 한다.
② 정상 기능 오동작이나 취약점을 통해 배터리 고갈, 과도한 트래픽 유발, 허가되지 않은 주소로 정보 전송 등이 되어서는 안 된다.
③ 디컴파일 도구를 이용 시 실행파일을 소스코드로 쉽게 변환시킬 수 있으며, 이를 이용하여 앱 위변조 발생이 가능하다. 이를 예방하기 위해 난독화 도구를 사용하여 패키징한 후 배포해야 한다.
④ 앱 설치 시 비정상적인 파일/디렉터리가 생성되지 않아야 하며, 실행 시에는 불필요한 접근 권한이 존재해서는 안된다. 또한 앱 삭제 시에는 관련된 파일이 완전히 삭제되어야 한다.

47. 다음 중 메일 서버의 구성요소로만 이루어진 것은?
① MUA, MTA, SPF ② MUA, URLBL, PGP
③ IMAP, MDA, POP3 ④ SMTP, SPF, MTA

48. 다음은 HTTP 프로토콜 중 Header 옵션에 대한 설명이다. 가장 알맞은 것은?

> 해당 옵션의 설정에 따라서 특정 웹 리소스의 캐싱이 되지 않게 하며, 악용되어 사용될 경우 서버에 부하가 발생하는 공격으로도 사용될 수 있다. 이는 RFC 2616(HTTP 1.1)에 규정되어 있다.

① Cookie ② User-Agent
③ Cache-Control ④ Content-Length

49. FTP Passive 모드에 대한 설명으로 옳지 않은 것은?
① 데이터 전송을 위해 1024번 이전 포트를 사용한다.
② 서버에서 클라이언트를 접속해야 하는 모순을 해결하기 위해 고안된 방식이다.
③ 보안을 위해서는 서버에서 Passive 모드로 사용할 포트를 제한한다.
④ 제어 전송을 위해 서버에서는 21번 포트를 사용한다.

50. DNSSEC의 전자서명과 서명검증 절차를 지원하기 위하여 추가한 신규 리소스 레코드와 관련이 없는 것은?
① DNSCA ② DNSKEY
③ RRSIG ④ NSEC/NSEC3

51. 개발된 소스 코드를 살펴봄으로써 코드 상의 취약점을 찾는 방식은?
① Black Box Testing ② White Box Testing
③ Green Box Testing ④ Brown Box Testing

52. 메일 수신 서버 또는 웹 메일 서버로부터 전자우편 메시지를 자신의 컴퓨터 단말 장치로 전송받는 데 사용되는 프로토콜이 아닌 것은?
① IMAP(Internet Mail Access Protocol)
② RTP(Realtime Transport Protocol)
③ POP(Post Office Protocol)
④ HTTP(HyperText Transfer Protocol)

53. ㉠, ㉡에 들어갈 용어로 올바르게 짝지어진 것은?

> 비트코인의 경우, 블록체인에 새로운 블록을 추가하기 위해서는 대량의 해시(hash) 연산을 통해 조건에 맞는 난수를 찾는 (㉠)이 필요하며, 이렇게 새로운 블록을 추가함으로써 코인을 획득하는 것을 흔히 (㉡)이라고 한다.

① ㉠ 작업증명 ㉡ 채굴 ② ㉠ 작업증명 ㉡ 송금
③ ㉠ 지분증명 ㉡ 채굴 ④ ㉠ 지분증명 ㉡ 송금

54. HWP, TXT, PDF, 도면 등 업무에 사용하는 파일을 암호화하여, 외부자는 물론 허가된 내부자에 의한 주요 정보유출을 원천 차단함으로써 기업 정보 유출을 막는 솔루션은?
① IPS(Intrusion Prevention System)
② DRM(Digital Rights Management)
③ ESM(Enterprise Security Management)
④ VPN(Virtual Private Network)

55. 다음 중 SSO에 대한 설명으로 적절하지 못한 것은?
① 하나의 아이디로 여러 사이트를 이용할 수 있는 시스템이다.

② 싱글사인온(SSO)을 사용하면 응용서비스 로그인 시간을 줄여준다.
③ SSO를 이용하면 개별 애플리케이션 단위로 동일한 암호를 설정하게 되므로 편리하기는 하지만 보안의 입장에서는 권장하지 않는다.
④ SSO 솔루션을 통해 직원이 어디서 어떤 응용서비스에 접속하여 무엇을 하는지에 대한 로그정보 저장이 가능하다.

56. 디지털 포렌식의 원칙 중 어느 원칙에 대한 설명인가?

> 증거가 획득된 다음 증거에 대한 이송, 분석, 보관, 법정 제출이라는 일련의 과정 및 각 과정마다 담당자가 명확해야 하며 이에 대한 추적이 가능해야 한다.

① 연계보관성의 원칙 ② 정당성의 원칙
③ 무결성의 원칙 ④ 재현의 원칙

57. 다음 지문이 설명하는 소프트웨어 보안 약점을 고르면?

> 특정 웹사이트에 대해서 사용자가 인지하지 못한 상황에서 사용자의 의도와는 무관하게 공격자가 의도한 행위(수정, 삭제, 등록 등)를 요청하게 하는 공격을 말한다. 웹 응용프로그램이 사용자로부터 받은 요청에 대해서 사용자가 의도한 대로 작성되고 전송된 것인지 확인하지 않을 경우 발생 가능하고 특히 해당 사용자가 관리자인 경우 사용자 권한 관리, 게시물 삭제, 사용자 등록 등 관리자 권한으로만 수행 가능한 기능을 공격자의 의도대로 실행시킬 수 있게 된다.

① 크로스사이트 요청 위조 공격(CSRF)
② 크로스 사이트 스크립트(XSS)
③ 경로 조작 및 자원 삽입
④ SQL 삽입

58. 다음 지문에서 설명하는 것은?

> 결제자의 다양한 정보를 수집해 패턴을 만든 후 패턴과 다른 이상 결제를 잡아내고, 결제 경로를 차단하는 보안 방식으로 보안 솔루션에 의존하던 기존 보안과 달리, 빅데이터를 바탕으로 적극적인 보안 개입을 하는 것이 특징이다.

① 이상행위 탐지시스템(FDS)
② 침입탐지시스템(IDS)
③ 블록체인(Blockchain)
④ SET(Secure Electronic Transaction)

59. 다음 지문의 빈칸 ㉠, ㉡에 들어갈 내용이 올바르게 짝지어진 것은?

> SET에서는 대칭키 방식의 암호화를 위해 송·수신자 간에 비밀키 교환이 이루어진다. 비밀키 교환을 위해 A가 B에게 전자봉투를 생성하여 전송할 때 전자봉투 생성에 필요한 것은 (㉠)와 (㉡)이다.

① A의 공개키, B의 개인키 ② 비밀키, A의 개인키
③ 비밀키, B의 공개키 ④ A의 개인키, B의 공개키

60. 다음 지문에서 설명하는 보안 기술은 무엇인가?

> SOA, SIRP, TIP를 폭넓게 포함하는 개념으로 보안 운영에 있어 유입되는 위험에 대해 대응 레벨을 자동으로 분류하고, 표준화된 업무 프로세스에 따라 사람과 기계가 유기적으로 협력할 수 있도록 지원하는 대응 플랫폼을 말한다. 수집된 모든 로그 및 이벤트를 바탕으로 위협 인텔리전스와 능동적 탐지를 통해 침해정보와 영향도를 도출하고 이를 개선하기 위한 시스템 변경을 자동화할 수 있다.

① SOAP(Security Orchestration Automation Platform)
② SOAR(Security Orchestration Automation and Response)
③ SIEM(Security Information and Events Management)
④ UEBA(User and Entity Behavior Analytics)

4과목 : 정보 보안 일반

61. 다음 지문이 설명하고 있는 암호 공격방식은?

> 암호 해독자가 사용된 암호기에 접근할 수 있어 평문 P를 선택하여 그 평문 P에 해당하는 암호문 C를 얻은 다음 키나 평문을 추정하여 암호를 해독하는 방법

① 암호문 단독 공격 ② 기지 평문 공격
③ 선택 평문 공격 ④ 선택 암호문 공격

62. 수동적, 능동적 공격 방식의 예가 올바르게 짝지어진 것은?

	[수동적 공격]	[능동적 공격]
①	트래픽 분석	삽입공격
②	재생공격	삭제공격
③	메시지 변조	재생공격
④	메시지 변조	도청

① ① ② ②
③ ③ ④ ④

63. 블록 암호 알고리즘을 사용하여 메시지 인증 코드(MAC)를 생성할 때 가장 적합한 블록 암호 모드는 무엇인가?

① CBC 모드 ② ECB 모드
③ OFB 모드 ④ CTR 모드

64. 인증 수단으로는 일반적으로 알고 있는 것, 자신의 모습, 가지고 있는 것, 위치하는 곳 등의 방식을 사용한다. 다음 인

증 방식의 예로 옳지 않은 것은?

① 알고 있는 것(something you know) - 사용자 아이디, 아이디에 해당하는 패스워드, OTP(One Time Password) 생성기

② 자신의 모습(something you are) - 지문, 망막, 홍채

③ 가지고 있는 것(something you have) - 스마트 카드, 신분증

④ 위치하는 곳(somewhere you are) - 사용자 IP 주소, 콜백(call back)

65. 다음 중 사용자 인증 및 개인 식별에 대한 설명으로 옳지 않은 것은?

① 사용자 인증 기술은 A가 B에게 자신이 A임을 확인시켜 줄 수 있는 기술이다.

② 개인 식별 기술은 B가 C에게 자신이 B가 아니라고 확인시켜 줄 수 있는 기술이다.

③ 개인을 식별하는 방법으로 지문(생체정보), 보안 토큰(사용자 소유), 비밀번호(사용자 지식) 등이 사용될 수 있다.

④ 사용자 인증서 보안 요구사항으로는 식별과 인증, 인가 및 책임추적성 등을 들 수 있다.

66. 다음 중 인증서 폐지 목록의 기본 영역에 포함되지 않는 것은?

① 서명 알고리즘 ② 발급자

③ 버전 ④ 유효 기간

67. 다음은 접근통제가 이루어지는 과정을 설명한 것이다. 빈칸 ㉠에 공통적으로 들어갈 용어는?

- 주체가 특정 객체에 접근을 요청하면 (㉠)은(는) 이를 가로챈다.
- (㉠)은(는) 자신이 가지고 있는 기본규칙에 따라 접근권한(조직이 정의한 정책에 따라 설정됨)을 결정한다.
- (㉠)은(는) 정의된 접근규칙에 따라 접근을 허가 혹은 거부한다.
- (㉠)에서 처리되는 모든 접근 요청은 이후의 추적 및 분석을 위해 기록된다.

① 상주엔진 ② 접근통제 API

③ 시스템호출 ④ 보안커널

68. 생체인식 기술이 가져야 할 보안 요구조건과 거리가 먼 것은?

① 보편성(Universality) ② 구별성(Uniqueness)

③ 일시성(Temporality) ④ 획득성(Collectability)

69. 다음 중 전자서명의 요구사항으로 가장 적절하지 않은 것은?

① 전자서명 생성이 비교적 용이해야 한다.

② 전자서명을 위조하는 것이 계산적으로 실행 불가능해야 한다.

③ 기억장소에 전자서명의 복사본을 유지하는 것이 실용적이어야 한다.

④ 위조와 부인을 방지하기 위하여 수신자에 대한 정보를 사용해야 한다.

70. 다음 중 해시함수가 적용되는 분야를 모두 고른 것은?

가. 전자서명	나. 메시지인증
다. 데이터 압축	라. 패스워드기반 암호화

① 가, 나 ② 가, 나, 라

③ 가, 나, 다, 라 ④ 나, 라

71. 다음은 메시지 인증 절차를 설명한 것이다. 괄호 안에 들어갈 단어가 순서대로 나열된 것은?

- 송신자가 메시지를 생성한다.
- 해시함수를 통해 메시지의 해시값을 생성한 후 이를 (a)의 (b)를 이용하여 암호화한다.
- 암호화된 값을 메시지에 덧붙이고 압축한 후 수신자에게 전송한다.
- 수신자가 파일을 수신하며 압축을 푼다.
- 전자서명 부분을 분리한 후 (c)의 (d)로 복호화한다.
- 해시함수를 통해 메시지 부분에 대한 해시값을 얻는다.
- 두 결과의 값이 동일하면 메시지가 인증된다.

① a 송신자 - b 개인키 - c 송신자 - d 공개키

② a 송신자 - b 개인키 - c 송신자 - d 개인키

③ a 수신자 - b 개인키 - c 수신자 - d 공개키

④ a 송신자 - b 공개키 - c 수신자 - d 개인키

72. 공개키 암호방식에 이용되는 이론적으로 풀기 어려운 수학 문제들은 대부분 소인수 분해 문제, 이산대수 문제, NP-complete 문제 등으로 분류할 수 있다. 다음 중 이산대수 문제에 기반한 공개키 알고리즘과 가장 거리가 먼 것은?

① ECC ② Knapsack

③ DSA ④ ElGamal

73. 패스워드는 사용자 인증에 흔히 사용되는 기법이지만 보안에 매우 취약한 문제가 있다. 다음 지문의 빈칸 ㉠에 들어갈 용어로 적절한 것은?

사용자는 기억하기 쉬운 단어를 패스워드로 사용할 가능성이 높다. 이런 이유로 공격자는 패스워드로 사용될 가능성이 높은 단어를 적절히 선별할 경우 패스워드 공격의 성공 확률을 높일 수 있으며, 이렇게 선별된 단어 모음을 흔히 (㉠)이라고 부른다.

① 핀(PIN) ② 패스프레이즈(Passphrase)

③ 풀(Pool) ④ 사전(Dictionary)

74. 자신의 비밀을 노출하지 않으면서 자신이 비밀을 알고 있다는 것을 증명하는 인증 방법은?

① 패스워드 ② 영지식 인증

③ 바이오매트릭스 ④ 시도-응답 인증

75. 다음 지문에서 설명하는 암호방식은?

> 평문에 대한 연산을 수행하여 암호화한 결과와 암호문에 대한 연산을 수행한 결과가 동일한 암호방식으로, 암호화된 데이터를 복호화하지 않고 데이터에 대한 연산이 가능하다. 금융, 의료분야에서 개인정보에 대한 빅데이터 처리를 위해 유용한 암호화 방식이다.

① 동형(Homomorphic) 암호화
② 형태보존(Format Preserving) 암호화
③ 순서보존(Order Preserving) 암호화
④ 블록체인(Block Chain) 암호화

76. MAC에 대한 설명 중 잘못된 것은?
① 메시지 인증은 메시지 송수신자 사이에 문서의 위·변조 공격에 대한 대응 방안으로 활용한다.
② MAC 생성에 키를 사용하는 해시함수가 널리 사용된다.
③ MAC 자체만으로는 재전송 공격에 취약하다.
④ 메시지 인증은 송신자와 수신자의 안전하고 훼손되지 않는 Key 관리가 목표이다.

77. 다음 중 정보자원에 접근하기 위한 3단계 절차에 해당하지 않는 보안 요구사항은 무엇인가?
① 식별(Identification) ② 인증(Authentication)
③ 인가(Authorization) ④ 책임추적성(Accountability)

78. 메시지 인증 코드의 구조적 제약사항에 따른 재전송 공격을 막는 방법과 거리가 먼 것은?
① Sequence Number ② Hash
③ Nonce ④ Timestamp

79. 다음 지문에서 설명하는 것은?

> 인터넷 애플리케이션에서 사용자 인증에 사용되는 공개 API로 구현된 표준 인증 방법이다. 매시업(Mashup) 서비스로 만들어진 애플리케이션이나 트위터, 페이스북과 같은 SNS 서비스를 다른 애플리케이션 또는 기기(PC, 스마트폰 등)에서 사용자 정보에 접근할 때 사용할 수 있도록 한다. 2010년 IETF에서 공식 표준안(RFC 5849)이 발표되었다.

① SSO(Single Sign On)
② OAuth
③ OpenID
④ OIDC(OpenID Connect)

80. 다음 지문에서 설명하는 용어는 무엇인가?

> Shannon은 순환과 대치를 반복적으로 사용하여 평문과 암호문 사이의 관계 파악을 어렵게 만드는 합성암호를 소개하며, 암호문의 각각의 비트나 문자가 평문의 모든 비트나 특정 비트에 종속적으로 결정되어 암호문에 대한 통계적인 테스트를 통하여 평문을 찾고자 하는 공격자를 좌절시키는 개념을 소개하였다.

① 혼돈 ② 확산
③ 차분(Differential) ④ 선형(Linear)

5과목 : 정보보안 관리 및 법규

81. 정보를 전송하는 과정에서 송신자와 수신자가 해당 자원에 대한 사용이 정당한지를 확인하기 위한 절차를 무엇이라고 하는가?
① 인증 ② 인가(Authorization)
③ 감사(Auditing) ④ 관리

82. 다음 중 주요정보통신기반시설 관리기관이 취약점 분석·평가를 의뢰할 수 없는 기관은?
① 「국가정보화기본법」 에 의한 한국정보화진흥원
② 「정보통신기반보호법」 에 의한 정보공유·분석센터
③ 「정보보호산업의 진흥에 관한 법률」 에 따라 지정된 정보보호 전문서비스 기업
④ 「정부출연연구기관 등의 설립·운영 및 육성에 관한 법률」 에 의한 한국전자통신연구원

83. 이것은 영국표준협회(BSI)에서 만든 정보보호관리체계에 대한 표준으로, 최상의 정보보호관리를 위한 포괄적인 일련의 관리 방법에 대하여 요건 별로 해석해 놓은 규격으로, 기업이 고객 정보의 기밀성, 무결성, 가용성을 보장한다는 것을 공개적으로 확인하는 것이 목적이다. 이것은 현재 국제표준기구인 ISO에 의해 ISO 27000 시리즈로 발전하였다. 이것은 무엇인가?
① ITSEC(Information Technology Security Evaluation Criteria)
② TCSEC(Trusted Computer System Evaluation Criteria)
③ CC(Common Criteria)
④ BS7799(British Standard 7799)

84. 사이버 폭력의 특징이 아닌 것은?
① 사이버 폭력 행위는 빠르게 확산된다.
② 익명성으로 인해 사이버 폭력 행위를 쉽게 하게 된다.
③ 가해자를 찾아내기 쉽다.
④ 자신도 모르는 사이에 사이버 폭력 행위를 할 수 있다.

85. 개인정보보호법에서 정한 '민감정보'에 해당하지 않는 것은?
① 장애 등급
② 지문 인증 방식에 사용되는 지문 정보
③ 인종에 관한 정보
④ 혈액형

86. 위험분석 방법론으로 적절히 짝지은 것은?

㉠: 어떤 사건도 예상한 대로 발생하지 않는다는 사실에 근거하며 일정 조건하에서 위험에 대한 발생 가능한 결과들을 추정하는 방법
㉡: 시스템에 관한 전문적인 지식을 가진 전문가의 집단을 구성하고 위험을 분석 및 평가하며 정보시스템이 직면한 다양한 위협과 취약성을 토론을 통해 분석하는 방법

① ㉠ 확률분포법 ㉡ 순위결정법
② ㉠ 시나리오법 ㉡ 델파이법
③ ㉠ 델파이법 ㉡ 확률분포법
④ ㉠ 순위결정법 ㉡ 시나리오법

87. 개인정보의 가명정보 처리에 대한 설명으로 틀린 것은?
① 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있다.
② 누구든지 특정 개인을 알아보기 위한 목적으로 가명정보를 처리해서는 아니 된다.
③ 가명정보 및 가명정보를 원래의 상태로 복원하기 위한 추가 정보에 대하여 안전성 확보 조치는 개인정보처리자가 임의로 처리하여야 한다.
④ 개인정보처리자는 가명정보를 처리하는 과정에서 특정 개인을 알아볼 수 있는 정보가 생성된 경우에는 즉시 해당 정보의 처리를 중지하고 지체 없이 회수·파기하여야 한다.

88. '위치정보'란 이동성 있는 물건 또는 개인이 특정한 시간에 존재하거나 존재하였던 장소에 관한 정보를 말한다. 다음 중 「위치정보보호를 위한 관리적·기술적 보호조치 권고」와 관련한 설명으로 적절하지 않은 것은?
① 관리적·기술적 보호조치에 의해 보호되어야 하는 위치정보의 범위는 개인위치정보뿐 아니라 이동성 있는 물건의 위치정보를 포함한다.
② 위치 좌표값이 그 자체만으로는 특정인의 위치를 나타내지 못하나 통신단말기 번호 또는 단말기 소지자의 이름 등과 결합하여 특정인의 위치를 알 수 있을 때에는 개인위치정보로 볼 수 있다.
③ 결합 가능한 정보들이 여러 DB로 분산되어 있거나 제휴회사 등이 별도로 보유하고 있더라도 서비스 제공을 위해 상호 결합될 가능성이 많다면 개인위치정보에 해당될 수 있다.
④ 법인이나 단체 등의 위치정보도 개인위치정보 보호대상에 포함된다.

89. 개인정보의 안전성 확보조치 기준에서 사용되는 용어 정의이다. 올바르지 않은 것은?
① '개인정보파일'이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물을 말한다.
② '개인정보처리시스템'이란 개인정보를 처리할 수 있도록 데이터베이스시스템에 직접 접속하는 단말기를 말한다.
③ '바이오정보'란 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.
④ '내부망'이란 물리적 망분리, 접근통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.

90. 다음은 개인정보보호법상 개인정보의 처리기준 및 정보주체의 권리에 관한 설명이다. 설명이 가장 올바른 것은?
① 주소불명 등으로 정보주체의 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우에 동의 없이 개인정보를 수집·이용할 수 있다.
② 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우에는 정보주체의 동의 없이 개인정보를 제3자에게 제공할 수 있다.
③ 정보주체에게 재화나 서비스를 홍보하거나 판매를 권유하기 위하여 개인정보처리위탁에 대한 동의를 받으려는 때에는 정보주체가 이를 명확하게 인지할 수 있도록 알리고 동의를 받아야 한다.
④ 개인정보보호법상 바이오정보(생체정보)는 민감정보에 해당하므로 건강정보와 마찬가지로 별도의 동의를 받아야 한다.

91. 개인정보취급자 등의 금지행위에 관한 설명이다. 가장 부적절한 것은?
① 정보보호 관리체계 인증 업무에 종사했던 자가 그 직무상 알게 된 비밀을 학생들에게 인증 업무 사례로 소개한 경우 형사처벌을 받을 수 있다.
② 보험회사의 직원이 친구의 부탁을 받고 친구에게 돈을 빌려간 채무자의 주소, 전화번호 등 연락처를 알려준 경우 형사처벌을 받을 수 있다.
③ 회사의 개발업무에 종사하고 있는 직원이 학위논문 연구를 위해 고객의 개인정보의 일부를 노트북에 내려받아 실험한 것은 유출로 간주되지 않는다.
④ 개인정보를 처리하던 자가 위계의 방법으로 개인정보처리에 관한 동의를 받는 경우 형사처벌을 받을 수 있다.

92. 위험 처리 방안 중 보안 솔루션을 도입하여 보안 통제를 수립하는 방안에 해당하는 것은?
① 위험 감소 ② 위험 수용
③ 위험 회피 ④ 위험 전가

93. 다음 중 조직의 정보보호 조직체계와 역할 및 책임에 대한 사항으로 가장 부적절한 것은?
① 정보보호 최고책임자 및 개인정보 보호책임자는 예산, 인력 등 자원을 할당할 수 있는 임원급으로 지정하고 관련 법령에 따른 자격요건을 충족하여야 한다.
② 모든 정보통신서비스제공자는 정보보호 최고책임자를 지정 및 신고하여야 한다.
③ 조직 전반에 걸쳐 중요한 정보보호 및 개인정보 보호 관련사항에 대한 검토, 승인 및 의사결정(위험평가 결과, 내부감사 결과 등)을 할 수 있는 위원회를 구성하여 운영하여야 한다.
④ 주요 직무를 수행하는 임직원 및 외부자를 주요 직무자로 지정하고, 주요 직무자를 최소한으로 지정하여 그 목록을 최신으로 관리하여야 한다.

94. 위험관리 절차를 순서대로 배열한 것을 고르면?

㉠ 위험 식별	㉡ 위험 처리
㉢ 위험 평가	㉣ 위험 분석
㉤ 위험 감시 및 재검토	

① ㉠ - ㉡ - ㉢ - ㉣ - ㉤ ② ㉠ - ㉣ - ㉢ - ㉡ - ㉤
③ ㉠ - ㉡ - ㉣ - ㉢ - ㉤ ④ ㉠ - ㉣ - ㉡ - ㉢ - ㉤

95. 다음은 업무연속성 5단계 방법론 중 특정 단계를 설명한 것이다. 어떤 단계를 설명한 것인가?

> 업무연속성 계획 수립 과정에서 수행하는 업무로 주요 업무 프로세스 식별, 우선순위화, 프로세스별 복구 목표시간, 복구 목표수준 산출 등 각 사업단위가 받게 될 재정적인 손실의 영향도 등을 파악하는 단계이다.

① 사업영향평가 ② 위험분석
③ 복구계획 수립 ④ 정보보호 대책 구현

96. 조직이 수행하는 모든 정보보호 활동의 근거가 되는 최상위 수준의 정보보호 정책 수립 시, 포함하여야 할 사항과 가장 거리가 먼 것은?

① 조직의 정보보호 활동을 실행하기 위한 절차, 주기, 수행 주체 등에 관한 사항
② 조직의 정보보호에 대한 최고경영자 등 경영진의 의지 및 방향
③ 조직의 정보보호를 위한 역할과 책임, 대상과 범위에 관한 사항
④ 조직이 수행하는 관리적, 기술적, 물리적 정보보호 활동의 근거

97. 용어에 대한 설명으로 옳지 않은 것은?

① '침해사고'란 정보통신망 또는 이와 관련된 정보 시스템을 공격하는 행위로 인하여 발생한 사태를 말한다.
② '정보통신기반시설'이라 함은 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 및 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 따른 정보통신망을 말한다.
③ '개인위치정보'라 함은 특정 개인의 위치정보(위치정보만으로는 특정 개인의 위치를 알 수 없는 경우에도 다른 정보와 용이하게 결합하여 특정 개인의 위치를 알 수 있는 것을 포함한다)를 말한다.
④ '개인신용정보'란 기업 및 법인에 관한 정보를 제외한 생존 여부와 상관없는 개인에 관한 신용정보로서 해당 정보의 성명, 주민등록번호 및 영상 등을 통하여 특정 개인을 알아볼 수 있는 정보만 말한다.

98. 인증제도는?

> 현재 사용되는 IT 보안제품에 대해 보안성을 평가하는 제도로 제품유형별 PP(Protection Profile)를 정의하고, 8개 군의 평가항목을 대상으로 평가가 이루어진다. 평가결과는 IT 보안제품의 보안위협 및 자산가치의 정도에 따라 EAL1(Evaluation Assurance Level 1) - EAL7(Evaluation Assurance Level 7)까지 7단계로 부여하며 인증서가 제공된다.

① ISO 27001 ② ITSEC
③ CC ④ TCSEC

99. 업무연속성 5단계 방법론 중 특정 단계를 설명한 것이다. 어떤 단계를 설명한 것인가?

> 업무연속성 계획 수립 과정에서 수행하는 업무로 주요 업무 프로세스 식별, 우선순위화, 프로세스별 복구 목표시간, 복구 목표수준 산출 등 각 사업단위가 받게 될 재정적인 손실의 영향도 등을 파악하는 단계이다.

① 사업영향평가 ② 위험분석
③ 정보보호 대책 구현 ④ 복구계획 수립

100. "개인정보보호법"상의 "개인정보처리자의 개인정보 보호 원칙"에 관한 설명 중 가장 부적절할 것은?

① 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집한다.
② 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.
③ 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.
④ 개인정보는 반드시 실명으로 처리되어야 한다.

전자문제집 CBT PC 버전 : www.comcbt.com
전자문제집 CBT 모바일 버전 : m.comcbt.com
기출문제 및 해설집 다운로드 : www.comcbt.com/xe

전자문제집 CBT란?
종이 문제집이 아닌 인터넷으로 문제를 풀고 자동으로 채점하며 모의고사, 오답 노트, 해설까지 제공하는 무료 기출문제 학습 프로그램으로 실제 시험에서 사용하는 OMR 형식의 CBT를 제공합니다.
PC 버전 및 모바일 버전 완벽 연동
교사용/학생용 관리기능도 제공합니다.

오답 및 오탈자가 수정된 최신 자료와 해설은 전자문제집 CBT에서 확인하세요.

1	2	3	4	5	6	7	8	9	10
④	②	④	②	④	①	①	①	③	④
11	12	13	14	15	16	17	18	19	20
②	②	③	④	④	④	②	②	④	④
21	22	23	24	25	26	27	28	29	30
③	④	④	①	③	②	①	③	①	②
31	32	33	34	35	36	37	38	39	40
①	①	②	④	④	①	①	②	②	②
41	42	43	44	45	46	47	48	49	50
①	②	③	③	③	①	③	③	①	①
51	52	53	54	55	56	57	58	59	60
②	②	①	②	③	①	①	①	③	②
61	62	63	64	65	66	67	68	69	70
③	①	①	①	②	④	④	③	④	②
71	72	73	74	75	76	77	78	79	80
①	②	④	②	①	④	④	②	②	②
81	82	83	84	85	86	87	88	89	90
②	①	④	③	④	②	③	④	②	①
91	92	93	94	95	96	97	98	99	100
③	①	②	②	①	①	④	③	①	④