1과목 : 시스템 보안

1. 리눅스 운영체제 특수 권한에 대한 설명으로 틀린 것은?

① SetGID가 부여된 파일은 소유 그룹의 실행 권한이 x에서 s로 변경된다.

② SetUID가 부여된 파일은 소유자의 실행 권한이 x에서 s로 변경된다.

❸ Sticky bit이 부여된 디렉터리는 기타 사용자의 실행 권한이 x에서 s로 변경된다.

④ Sticky bit는 /tmp와 같은 777 권한의 공용 디렉터리에서 파일 삭제 통제에 이용된다.

2. 악성코드 유형은 무엇인가?

> - 하드디스크 내에 악성코드 파일을 설치하지 않고, 시스템 메모리에 곧바로 로드되어 실행된다.
> - OS에 내장된 정상적인 도구 PowerShell, WMI(Windows Management Instrumentation)를 이용하여 실행되므로 백신 프로그램을 정상 실행으로 판단한다.
> - E-Mail의 첨부파일, PDF 문서, JPEG 파일 등에 삽입되어 배포된다.

① 루트킷 ② 트로이 목마

③ 스파이웨어 ❹ 파일리스

3. 최근 기관이나 단체를 사칭하는 것부터 이력서나 발주서 등을 사칭해 무의식 중에 열어보도록 하는 방법을 사용하여 이메일에 첨부파일이나 URL을 삽입한 후, 이를 클릭해 악성코드를 실행하도록 하는 등의 공격이 성행하고 있다. 이러한 공격의 차단을 목적으로 하는 가장 적합한 솔루션은?

① WAF(Web Application Firewall)

❷ CDR(Content Disarm &Reconstruction)

③ TMS(Threat Management System)

④ DLP(Data Loss Prevention)

4. 문제 복원 오류로 내용이 없습니다. 정확한 내용을 아시는분께서는 오류신고를 통하여 내용 작성 부탁 드립니다. 정답은 임의로 1번으로 설정하였습니다.

❶ 문제 복원 오류로 내용이 없습니다.

② 문제 복원 오류로 내용이 없습니다.

③ 문제 복원 오류로 내용이 없습니다.

④ 문제 복원 오류로 내용이 없습니다.

5. 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.

❶ exFAT(Extended File Allocation Table)

② ext4(extended file system)

③ HFS(Hierarchical File System)

④ ReFS(Resilient File System)

6. 다음 중 윈도우 운영체제에서 시스템에 대한 비인가 변경을 통제하기 위한 기술에 해당하는 것은?

① 커널 모드 ② 윈도우 디펜더

③ 보안 업데이트 ❹ 사용자 계정 컨트롤

7. OTP(One-Time Password) 사용자 인증방식에 대한 설명으로 틀린 것은?

① OTP는 해시함수 등 암호학적 알고리즘에 의해 패스워드를 생성하기 때문에 다음 생성될 암호를 예측하는 것은 계산상 불가능하다.

② OTP에 의해 생성된 패스워드는 재사용이 불가능한 특징을 보인다.

③ OTP 단말기와 서버는 사전에 공유한 비밀값을 암호학적 알고리즘에 적용하여 패스워드를 생성한다.

❹ 시간 동기화 방식을 사용하는 OTP 시스템에서 OTP 서버와 단말기에 적용되는 시간은 정확한 패스워드 생성을 위해 시간 오차를 전혀 허용하지 않는다.

8. 다음 지문에서 설명하는 파일은?

> 이 파일은 미디어 장치의 루트 디렉터리에 위치하며 미디어(CD/DVD, USB) 연결 시 특정 프로그램이 자동으로 실행되도록 제어한다. 해당 미디어가 악성코드에 감염되었을 때 감염 확산 또는 정보 유출 등의 피해가 발생할 수 있다.

① mediarun.msc ② activerun.inf

❸ autorun.inf ④ execute.inf

9. secure.txt 파일의 소유자에게는 읽기와 실행권한을 부여하고 다른 사용자에게는 읽기 권한을 제거하는 권한 변경 명령으로 알맞은 것은?

① chmod 401 secure.txt ② chmod o+rx, a-r secure.txt

③ chmod 504 secure.txt ❹ chmod u=rx, o-r secure.txt

10. 다음 중 빈칸 ㉠에 들어갈 알맞은 용어는?

> "온라인 소스코드 (㉠) 보안 강화 권고"는 IT 개발 프로젝트에서 사용되는 온라인 소스코드 (㉠)에 대한 취약한 보안설정으로 인해 프로젝트가 외부에 공개되어 공격자가 소스코드를 열람하거나 정보가 탈취되어 공급망 공격 등에 활용될 수 있는 상황을 방지하기 위한 것이다. 소스코드 (㉠)로는 GitHub, GitLab, Bitbucket 등이 있다.

① 클라우드 ❷ 저장소

③ 젠킨스 ④ 빌드

11. 윈도우 시스템 인증 구성요소에서 모든 계정의 로그인에 대한 검증을 하고, 비밀번호 변경을 처리하며 자원 접근 토큰을 생성하는 것은?

❶ LSA(Local Security Authority)

② SAM(Security Account Manager)

③ SRM(Security Reference Monitor)

④ NTLM(NT LAN Manager)

12. 도메인 계정에 대한 로그인 성공, 실패 관련 이벤트 로그를

기록하기 위해 보안설정이 필요한 감사 항목은?

① 계정 관리 감사 ❷ 계정 로그인 이벤트 감사
③ 개체 액세스 감사 ④ 시스템 이벤트 감사

13. 레지스트리에 대한 설명으로 틀린 것은?

① 시스템 구성정보를 저장하는 데이터베이스로 저장되는 위치는 윈도우 운영체제 버전에 따라 다르다.
② 레지스트리의 편집을 위해 사용되는 도구는 regedit.exe 이다.
③ 레지스트리 키는 HKEY_CLASSES_ROOT, HKEY_USERS, HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE, HKEY_CURRENT_CONFIG 등을 포함한다.
❹ 레지스트리 백업 및 복구는 shell.exe를 구동하여 수행한다.

14. ㉠, ㉡, ㉢에 들어갈 내용이 올바르게 짝지어진 것은?

리눅스 서버 관리자 A는 (㉠) 공격에 대응하기 위해 PAM 모듈을 활용하고자 한다.
(계정보안 정책은 패스워드 3회 입력 실패 시, 10분간 계정을 잠금)
auth required pam_tally2.so (㉡) =3 unlock_time = (㉢)

① ㉠ 패스워드 무차별 대입 ㉡ disable ㉢ 10
❷ ㉠ 패스워드 무차별 대입 ㉡ deny ㉢ 600
③ ㉠ 부채널 ㉡ disable ㉢ 10
④ ㉠ 부채널 ㉡ deny ㉢ 600

15. 쿠키(Cookie)에 대한 설명 중 옳지 않은 것은?

① 웹사이트에 마지막으로 방문한 시간, 페이지 등 다양한 정보를 기록할 수 있다.
② 웹서버가 웹브라우저에게 보내어 저장했다가 서버의 부가적인 요청이 있을 때 다시 서버로 보내준다.
③ 일정한 기간 동안만 유효하게 할 수 있고, 유효(만료) 기한이 설정되지 않을 경우 웹브라우저 종료 시에 자동 삭제된다.
❹ 웹서버에 저장된 쿠키값은 개인정보보호를 위해 정기적으로 삭제해야 한다.

16. 다음 중 AD(Active Directory) 시스템을 안전하게 관리하기 위한 방안을 잘못 설명한 것은?

① 전용 계정을 별도로 관리하여 일반 업무용 AD 계정과는 분리하여 사용한다.
❷ 관리자 계정은 특수성이 있으므로 비밀번호 갱신주기에 대해서는 예외적용을 하도록 한다.
③ 비밀번호 갱신 정책에는 최근에 사용한 비밀번호들을 재사용하지 못하게 하는 제약조건도 고려되어야 한다.
④ 관리자용 단말은 인터넷과 격리된 망분리 환경으로 구성되어야 한다.

17. 스택상에서 특정 코드 실행을 막기 위해 수정해야 하는 파일은?

❶ /etc/system ② /etc/getty
③ /etc/fsck ④ /etc/conf

18. 시스템 오류를 공격하는 Heap Overflow 공격의 특징 및 원리에 대한 설명으로 틀린 것은?

① 프로그램이 실행되면서 메모리를 동적으로 할당하는 영역을 이용한다.
② 프로그래머가 malloc과 같은 메모리 할당 함수를 이용한다.
③ 힙 영역을 오버플로우 시켜서 특정 코드를 실행하여 공격하는 기술이다.
❹ 버스를 통해 전달되는 중요 정보를 엿보고 가로채는 공격 기술이다.

19. 다음 지문의 설정사항이 의미하는 것은?

[Linux 환경]
"/etc/securetty" 파일에서 pts/0 ~ pts/x 설정 제거 또는 주석 처리

[HP-UX 환경]
vi 편집기를 이용하여 "/etc/securetty" 파일을 연 후 아래와 같이 주석 제거 또는 신규 삽입
(수정 전) #console
(수정 후) console

① root 계정의 패스워드 임계치를 설정하고 있다.
② 모든 계정에 대한 패스워드 임계치를 설정하고 있다.
③ 모든 계정에 대한 암호화 접속을 활성화하기 위한 설정이다.
❹ root 계정의 원격접속을 제한하는 설정이다.

20. 윈도우 시스템에 포함된 원격 접속 프로그램인 터미널 서비스 기능을 이용할 때 사용되는 명령어는?

① vnc ❷ mstsc
③ teamviewer ④ realvnc

2과목 : 네트워크 보안

21. 가상사설망(VPN)의 터널링에 사용되는 프로토콜이 아닌 것은?

① PPTP ② L2F
❸ RSVP ④ IPSec

22. 아래 지문에서 강조(밑줄)된 프로토콜의 기능과 가장 거리가 먼 것은?

- 'DoubleDirect'라고 명명된 공격기법은 iOS, MAC OS X, Android에 이르기까지 상용화 되었던 대부분의 모바일 운영체제를 대상으로 하는 중간자 공격(Man-in-the-Middle attack) 기술이었다. 무선 네트워크 공격에 널리 사용되는 ICMP 프로토콜을 이용했다.
- 공격대상의 DNS 트래픽을 스니핑(Sniffing)하여 IP 주소를 예측하고, 해당 IP를 대상으로 ICMP Redirect 패킷을 이용해 공격대상 기기의 라우팅 테이블을 변경하고 트래픽을 우회시킨다.

① 네트워크 장치의 동적 상황 검사
② Routing Table 변경 요청

③ IP 통신을 위한 진단 데이터 전송
❹ Multi-casting 제어

23. 다음 보기 중 빅데이터의 방대한 정보 속에서 단순한 로그 수집 및 분석이 아닌 사후에 추적 등이 가능하도록 상관분석과 포렌식 기능을 제공해주는 지능적 위협에 대한 조기 경고 모니터링 체계를 의미하는 것은?

① IPS ② TMS
③ UTM ❹ SIEM

24. 다음 지문은 네트워크 공격기술에 대한 설명이다. 적절하지 못한 것으로 짝지어진 것은?

㉠ Boink 공격은 불완전한 IP 단편 처리 로직을 악용하여 시스템 장애를 발생시킨다.
㉡ 랜드(LAND) 공격은 패킷을 전송할 때 출발지 IP 주소와 목적지 IP 주소를 똑같이 만들어 공격 대상에게 보내는 방식이다.
㉢ SYN 플러딩(flooding) 공격은 ICMP 패킷과 네트워크에 존재하는 임의의 시스템을 이용하여 패킷을 증폭함으로써 서비스 거부 공격을 수행한다.
㉣ 스머프(Smurf) 공격은 동시 사용자 수 제한을 이용하는 것으로, 존재하지 않는 클라이언트가 서버별로 한정된 접속 가능 공간에 접속한 것처럼 속여 다른 사용자가 서비스를 제공 받지 못하도록 하는 공격이다.

① ㉠, ㉡ ② ㉠, ㉢
③ ㉡, ㉣ ❹ ㉢, ㉣

25. 다음 지문은 라우팅에 관한 설명이다. 빈칸에 들어갈 내용을 순서대로 나열한 것은?

(가)는 입력된 패킷의 목적지 IP를 바탕으로 (나)에 등록된 서브넷 정보와 일치하는 레코드의 인터페이스 정보와 게이트웨이 정보를 확인하여 패킷을 (나)에 전달한다. (가)에서 패킷을 수신하면 (나)상의 상대방 네트워크 IP 주소를 검색하여 패킷을 어디로 보낼 것인가를 결정하는데 라우터에 (다)가 설정되어 있으면 (나)상에서 등록되어 있지 않은 목적지 IP 주소들에 대해서는 설정된 경로로 전송하게 된다.

① (가) 라우터 (나) 라우팅 테이블 (다) Static Route
❷ (가) 라우터 (나) 라우팅 테이블 (다) Default route
③ (가) 스위치 (나) 목적지 테이블 (다) Static Route
④ (가) 스위치 (나) 목적지 테이블 (다) Default Route

26. 스위칭 환경에서 시도할 수 있는 스니핑 공격 유형과 거리가 먼 것은?

❶ SYN Flooding ② Switch jamming
③ ICMP Redirect ④ ARP Spoofing

27. 지문에서 설명한 공격의 대응 방안으로 옳지 않은 것은?

DDoS 공격의 에이전트 설치상의 어려움을 보완한 공격 기법으로 TCP 프로토콜 및 라우팅 테이블 운영상의 취약성을 이용하며, 정상적인 서비스를 제공 중인 서버를 Agent로 활용하는 공격기법이다.

① 위조된 패킷이 인터넷망으로 인입되지 않도록 ISP의 네트워크 단에서 직접 차단한다.
② 사전 공격에 악용될 소지가 있는 취약한 DNS 서버 등에 대해 보완 조치한다.
③ 악의적으로 이용되지 않기 위해 ICMP 프로토콜을 사용할 필요가 없는 시스템인 경우에는 스위치 또는 서버에서 해당 프로토콜을 차단한다.
❹ 외부 인터넷 서버의 접속이 잦을 경우 클라이언트의 보호를 위해 HTTP 프로토콜을 차단한다.

28. 다음 지문에서 설명하는 것은?

윈도우의 소프트웨어 취약점을 악용하는 것으로 NSA가 개발한 것으로 추정되는 공격도구로서 섀도 브로커스에 의해 2017년도에 공개되었다. 이는 미국 볼티모어시 정부에 대한 랜섬웨어 공격에서 다시금 부상하게 되었다. 문제는 많은 컴퓨터가 구식의 윈도우 운영체제를 계속 사용하고 있다는 것이다. 마이크로소프트의 SMB 구현의 취약점을 공격한다.

① 페트야 공격(Patya Attack)
❷ 이터널블루 공격(EternalBlue Attack)
③ 공급망 공격(Supply Chain Attack)
④ 갠드크랩 공격(GandCrab Attack)

29. 다음 괄호 안에 들어갈 수 있는 적절한 용어는?

라우터를 활용하여 네트워크 보안을 강화하기 위한 방법으로 access-list와 함께 유용하게 사용할 수 있는 기법으로는 ( )이 있다. 이는 access-list와 비슷한 효과를 내면서도 더욱 간편하게 사용할 수 있는데, 다음과 같은 경우를 생각해보자. 만약 시스템이나 네트워크를 모니터링 하던 중 특정 ip 또는 특정 대역에서 비정상적인 시도가 감지되었을 경우, 해당 ip를 차단하기 위해 매번 기존 access-list를 지우고 새롭게 ip를 추가하여 작성하는 것은 여간 번거로운 일이 아닐 수 없다. 이 필터링은 이때 사용될 수 있는데 명령어 자체는 특정한 목적지 ip 또는 ip 대역에 대하여 라우팅 테이블을 생성하는 방식과 동일하다. 다만 특정한 ip 또는 ip 대역에 대해 Null이라는 가상의 쓰레기 인터페이스로 보냄으로써 패킷의 통신이 되지 않도록 하는 것이다.

❶ Blackhole 필터링
② Unicast RPF를 이용한 필터링
③ Ingress filtering

④ Multicast RPF를 이용한 필터링

30. 다음 지문에서 설명하는 용어는?

> 이것은 사이버 공격을 프로세스 상으로 분석해 각 공격 단계에서 조직에 가해지는 위협 요소들을 파악하고 공격자의 목적과 의도, 활동을 분쇄 완화해 조직의 회복 탄력성을 확보하는 전략이다. 한마디로 공격자의 관점에서 사이버 공격 활동을 파악, 분석해 공격 단계별로 조직에 가해지는 위협 요소를 제거하거나 완화하자는 것이다.

① 멀버타이징(Malvertising)
② 익스플로잇(Exploit)
❸ 사이버 킬 체인(Cyber Kill Chain)
④ 사이버 위협 인텔리젼스(CTI)

31. 다음 지문에서 설명하는 용어는?

> 라우터나 스위치에서 DDoS 또는 DoS를 차단하는 경우 패킷이 특정 인터페이스로 보내져 패킷이 필터링 될 때마다 패킷의 출발지 ip로 ICMP Unreachable이라는 에러 메시지를 보내게 되는데, 필터링 하는 패킷이 많을 경우에는 라우터나 스위치에 과부하를 유발할 수 있기 때문에 ICMP 에러 메시지를 보내지 않도록 이것을 설정하는 것이 좋다.

① HA(High Availability) ❷ Null Routing
③ Cut-Through ④ Load Balancing

32. 다음 중 nmap의 TCP Half Open 스캔과 TCP FIN/NULL/XMAS 스캔에 대한 특징으로 옳지 않은 것은?

① TCP Half Open 스캔과 TCP FIN/NULL/XMAS 스캔은 대상 호스트에 로그를 남기지 않는다.
② nmap 사용 시, TCP Half Open 스캔은 -sS 옵션, TCP FIN/NULL/XMAS 스캔은 각각 -sF, -sN, -sX 옵션을 사용한다.
③ 공격대상의 닫힌 포트에 대한 TCP Half Open 스캔과 TCP FIN/NULL/XMAS 스캔은 각각 RST + ACK, RST 응답이 온다.
❹ 공격대상의 열린 포트에 대한 TCP Half Open 스캔과 TCP FIN/NULL/XMAS 스캔 시 둘 모두 SYN + ACK 응답이 온다.

33. 무선랜의 보안 취약점에 대한 설명으로 잘못된 것은 무엇인가?

① 무선랜은 유선처럼 물리적으로 랜케이블을 연결할 필요가 없기 때문에 관리자의 눈을 피해 불법침입자가 접속하기 용이하다.
② 기존의 AP를 제거하고 불법으로 AP를 교체하거나, 임의의 장소에 불법으로 AP를 설치하는 방법으로 내부 네트워크를 해킹할 수 있다.
❸ 무선망에서의 트래픽은 기존의 유선망과 동일한 패킷 프레임 구조로 구성되어 유선망에서의 해킹공격과 동일한 형식의 공격이 가능하다.
④ 단말기에 대한 인증과 무선 구간의 암호화를 위해 WEP/WPA 프로토콜 등을 사용하여 보안기능을 일부 강화할 수 있다.

34. 다음 중 모바일 기기를 통한 애플리케이션 배포, 데이터 및 환경설정 변경, 모바일 분실 및 장치 관리를 통합적으로 해주는 시스템은?

❶ MDM ② ESM
③ NAC ④ DLP

35. 다음 무선통신 보안에 관한 설명 중 틀린 것은?

① MAC 주소 인증은 사전에 미리 등록을 하여야 하는 번거로움이 있다.
② WEP 인증은 데이터 암호화와 사용자 인증 기능을 제공한다.
❸ SSID는 AP가 브로드캐스팅하지 않으면 접속할 방법이 없다.
④ EAP 인증을 통해 공격자의 패킷 도청을 방어할 수 있다.

36. 방화벽 장비에 대한 설명으로 가장 부적절한 것은?

❶ Transport Mode의 IPSec VPN이 구현될 수 있다.
② 보호하고자 하는 네트워크에 허가받지 않은 사용자들의 접근을 통제할 수 있는 시스템이다.
③ 주요 기능으로 IP, PORT 차단 기능이 있다.
④ 내부 네트워크 주소와 인터넷 주소를 변환시켜주는 기능을 설치하여 운영할 수 있다.

37. US-CERT는 크랙(KRACK)이라 부르는 WPA2(Wi-Fi Protected Access II) 프로토콜 내 취약점에 대한 내용을 공개하였으며, 키 재설정 공격인 크랙(Key Reinstallation Attack, KRACK)은 와이파이 인증 표준인 WPA2의 키 관리 취약점을 공격하는 것이다. 다음 중 이 취약점을 이용하는 공격과 거리가 먼 것은?

① TCP 연결 하이재킹 ② HTTP 컨텐츠 인젝션
③ Wi-Fi 패킷 재전송 ❹ SSID 브로드캐스팅

38. TCP SYN Flooding 공격은 대량의 패킷을 생성하여 공격하는 방식이다. 다음 중 TCP SYN Flooding 공격과 관련이 없는 것은?

① Half Open Connection 공격 ② 분산 DoS 공격
③ Reflector 공격 ❹ Teardrop 공격

39. Snort 탐지 옵션 정의 중 틀린 것은?

① sid : 규칙을 분류·식별하기 위한 ID 옵션이다.
② nocase : 대소문자 구분 없이 탐지하는 옵션이다.
❸ offset : content 옵션 명령이 검사할 byte 수를 지정하는 옵션이다.
④ distance : 이전 content 옵션으로 찾은 패턴의 끝부분 이후 몇 byte부터 검색할지 정하는 옵션이다.

40. 다음 중 로드 밸런싱을 제공하는 장비는?

① L2 스위치 ② L3 스위치
❸ L4 스위치 ④ 허브

3과목 : 어플리케이션 보안

41. SSO에 대한 설명 중 적절하지 못한 것은?

① SSO는 한번의 인증으로 여러 서비스에 대한 이용을 지원하는 사용자 인증 시스템이다.

② SSO를 도입하면 여러 응용 프로그램의 로그인 처리가 간소화되어 사용자들의 편의성이 증진될 수 있다.

③ SSO를 도입하면 최초 로그인 대상이 되는 응용 프로그램 또는 운영체제에 대한 보안 강화가 요구될 수 있다.

❹ SSO를 도입하면 사이트별로 각각의 사용자 인증 시스템을 운영하는 방식에 비하여 보안이 강화된다.

42. 다음은 여러 공격 유형에 대해 DNSSEC이 방어 기능을 제공할 수 있는지를 보여주는 분석표이다. 분석이 잘못된 공격유형은?(문제 오류로 분석표가 없습니다. 정확한 내용을 아시는분 께서는 오류신고를 통하여 내용 작성 부탁 드립니다. 정답은 4번 입니다.)

① 파밍

② 피싱

③ DDos 공격

❹ 웜바이러스에 의한 hosts 파일 안의 정보변조

43. 다음은 KISA의 리눅스 Wi-Fi 보안취약성에 대한 보안권고문 중 일부이다. 빈칸 ㉠에 공통적으로 들어갈 용어는?

리눅스의 특정 드라이버에서 발생하는 (㉠) 취약점 (CVE-2019-17666) ▶ 취약점 내용 - 리눅스 커널의 "rtlwifi" 드라이버에서 경계값 체크가 미흡하여 (㉠) 발생 ※ rtlwifi 드라이버 : 특정 Realtek Wi-Fi 모듈이 리눅스OS 시스템과 통신할 수 있도록 허용해 주는 컴포넌트 - 공격자가 경계값을 넘어서는 길이의 "NoA" 패킷을 전송하면 (㉠)로 인해 시스템 장애(crash) 발생

① XML injection

② Brute force

③ SSRF(Server-Side Request Forgery)

❹ Buffer Overflow

44. 인터넷과 같은 공용 통신망에서 안전한 데이터 전달과 사용자 인증 기능을 수행하는 SSL 보안 프로토콜 중 전송되는 데이터에 대한 암호화 및 복호화, 메시지 인증 코드의 생성과 검증을 수행하는 프로토콜은?

① Handshake 프로토콜 ② Alert 프로토콜

③ Change Cipher Spec 프로토콜 ❹ Record 프로토콜

45. MS SQL 서버는 윈도우 인증과 SQL 서버 인증이라는 두 가지 인증 방법을 제공하고 있다. 이에 대한 설명으로 잘못된 것은?

① SQL Server의 기본 인증 모드는 윈도우 인증이다.

② 윈도우 인증 모드가 적용되어 있을 경우 SQL 서버 인증을 이용할 수 없다.

③ 혼합 인증 모드가 적용되어 있을 경우 윈도우 인증과 SQL 서버 인증 모두 사용될 수 있다.

❹ 윈도우 인증과 SQL 서버 인증 중 보안성이 높은 안전한 인증 방법은 SQL 서버 인증이다.

46. 쿠키에 대한 설명 중 가장 부적절한 것은?

① 웹사이트에 마지막으로 방문한 시간, 페이지 등 다양한 정보를 기록할 수 있다.

② 쿠키의 유효 기간을 설정할 수 있으며, 유효(만료) 기간이 설정되지 않을 경우 웹브라우저 종료 시에 자동 삭제된다.

③ 웹서버가 웹브라우저에게 보내어 저장했다가 해당 사이트를 다시 방문할 때 서버에게 전달된다.

❹ 웹 서버에 저장된 쿠키값은 개인정보보호를 위해 정기적으로 삭제해야 한다.

47. DRM 구성 요소 중에서 콘텐츠를 이용하는 사용자에 대해 정해진 정책에 따라 사용 권한을 결정하고, 부여된 사용 권한에 따라 라이선스의 발급 및 그 내역을 관리하는 시스템을 무엇이라고 하는가?

① 패키저(Packager)

❷ 클리어링 하우스(Clearing House)

③ 시큐어 컨테이너(Secure Container)

④ DRM 제어기(DRM Controller)

48. 버퍼 오버플로우 공격을 막는 가장 중요한 방법으로 프로그래밍 시 권장하는 함수가 아닌 것은?

① strncat() ② fgets()

③ snprintf() ❹ strcpy()

49. 다음 디지털 포렌식에 대한 설명 중 옳지 않은 것은?

① 디지털 증거는 현실적으로 손상되기 쉽고, 분석 중에 훼손 및 변경, 조작될 수 있다.

❷ 정당성의 원칙은 수집 증거가 위변조 되지 않았음을 증명하는 것이다.

③ 디지털 증거는 증거 식별, 수집, 획득, 보존, 분석 등의 과정을 거친다.

④ 연계보관성의 원칙은 증거물 획득, 이송, 분석, 법정 제출의 각 단계에서 담당자 및 책임자를 명확히 하는 것이다.

50. 전자메일의 실제 발송자를 추적하기 위해 사용되는 메일 헤더의 항목은?

① Message-ID ② Content-Type

③ From ❹ Received

51. 데이터베이스의 보안 유형과 거리가 먼 것은?

① 접근 제어(Access Control)

❷ 데이터 집계연산(Aggregation)

③ 가상 테이블(Views)

④ 암호화(Encryption)

52. 전자 금융거래에서 사용되는 단말 정보, 접속 로그, 거래 정보 등을 분석하여 이상 금융거래 또는 부정 거래 행위를 탐지 및 예방하는 시스템은?

① IDS(Intrusion Detection System)

❷ FDS(Fraud Detection System)

③ POS(Point Of Sale System)

④ HDS(Hitachi Data System)

53. 다음 지문에서 설명하는 보안 솔루션은?

> 잠재적인 데이터 또는 정보(데이터)의 유출 전송을 감지하며, 사용 중 또는 이동 중 정지 상태에 있는 민감한 데이터 또는 정보를 모니터링 하거나 감지, 차단함으로써 이를 방지한다.

① DRM(Digital Rights Management)
❷ DLP(Data Loss Prevention)
③ NAC(Network Access Control)
④ MLS(Multi-Level Security)

54. 다음 지문에서 설명하는 공격 기법은 무엇인가?

> 익명 FTP 서버를 이용하며 공격 대상의 네트워크를 포트 스캐닝하는 데 사용하는 공격 기법으로서 FTP 서버가 데이터 포트로 데이터를 전송할 때 목적지가 어디인지 검사하지 않는다는 취약점을 이용한다.

❶ Bounce 공격 ② XSS 공격
③ Anonymous FTP 공격 ④ 디렉터리 리스팅 공격

55. WPKI 구성요소의 역할을 잘못 기술한 것은?

① 인증기관(CA) : 인증서 발급
❷ 등록기관(RA) : 인증서 폐지
③ 사용자(Client) : 인증서 발급 및 관리에 대한 요청
④ 디렉터리(Directory) : CA가 발행한 인증서 정보 저장

56. XML 조회를 위한 질의문(XPath, XQuery 등) 생성 시 사용되는 입력값과 조회 결과에 대한 검증 방법(필터링 등)을 설계하고 유효하지 않은 값에 대한 처리방법을 설계할 때 고려해야 할 사항 중 잘못된 것은?

① 공통 검증 컴포넌트를 이용한 입력값 필터링
② 필터 컴포넌트를 이용한 입력값 필터링
③ 개별 코드에서 입력값을 필터링하도록 시큐어코딩 규칙 정의
❹ 필터를 이용한 출력값 검증

57. TLS에 대한 공격대상과 공격방법의 쌍이 올바르지 못한 것은?

① DHE export Key - Logjam
② CBC mode encryption - BEAST
❸ CBC mode encryption + padding - FREAK
④ OpenSSL(SSL 3.0) - Heartbleed

58. 다음 중 SSL이 제공하는 보안 기능과 거리가 먼 것은?

① 암호화 세션 ② 서버 인증
③ 클라이언트 인증 ❹ 부인 방지

59. 다음 지문에서 웹 로그파일에 저장되는 내용을 모두 고른 것은?

> 가. 클라이언트 IP
> 나. 클라이언트 접속시간
> 다. 클라이언트 ID
> 라. 클라이언트 요청내용
> 마. 클라이언트 요청종류

① 가, 나, 다 ② 다, 라, 마
❸ 가, 나, 다, 마 ④ 나, 다, 라, 마

60. OTP(One-Time Password)는 고정된 패스워드 대신 랜덤하게 생성되는 일회성 패스워드를 말하며 동일한 패스워드를 사용할 경우 발생할 수 있는 보안상 취약점을 극복하여 일회성의 서로 다른 패스워드를 생성함으로써 안전한 전자상거래를 진행할 수 있게 한다. 다음 중 OTP의 생성 및 인증 방식이 아닌 것은?

① 이벤트 동기화 방식 ❷ 캡차(CAPTCHA) 방식
③ 질의/응답 방식 ④ 시간 동기화 방식

4과목 : 정보 보안 일반

61. 다음 중 Needham-Schroeder 키 분배에 대한 설명으로 옳지 않은 것은?

① 키 분배 센터를 이용하는 키 분배 방법이다.
② 질의-응답(Challenge-Response) 방식을 이용하여 설계되었다.
❸ Kerberos 프로토콜의 취약점을 개선한 프로토콜이다.
④ 재전송 공격(Replay attack)에 취약하다.

62. 다음 지문에서 공유 폴더에 적용된 접근통제 방식은?

> IT 팀장이 직원으로부터 공유 폴더에 접근할 수 없다는 보고를 받은 후 조사를 했더니 다음과 같은 사실을 발견하였다.
> - 해당 직원 또는 직원이 속한 그룹에게 공유 폴더에 대한 접근 권한이 부여되어 있지 않았다.
> - 다른 직원 또는 그룹에게 공유 폴더에 대한 접근 권한이 부여되어 있었다.
> - IT팀 내 다른 직원이 최근에 공유 폴더에 대한 접근 권한을 갱신하였다.

① 강제적 접근통제 ❷ 임의적 접근통제
③ 역할기반 접근통제 ④ 규칙기반 접근통제

63. 다음 중 Kerberos 프로토콜에 대한 설명으로 옳지 않은 것은?

① 비밀키 암호작성법에 기초를 둔 온라인 암호키 분배방법이다.
❷ Kerberos 프로토콜의 목적은 인증되지 않은 클라이언트도 서버에 접속할 수 있도록 하는 것이다.
③ Kerberos 프로토콜은 데이터의 기밀성과 무결성을 보장한다.
④ 키 분배 센터에 오류 발생 시, 전체 서비스를 사용할 수 없게 된다.

64. 다음은 커버로스 프로토콜의 세션키 전송 절차에 필요한 단계이다. 이 단계의 순서가 올바르게 나열된 것은?

㉠ 클라이언트는 티켓을 이용하여 서버에 접속
㉡ 티켓 발급서버는 인증된 클라이언트에게 티켓을 발급
㉢ 서버는 티켓을 확인 후 클라이언트를 인증하여 접속을 허락
㉣ 클라이언트는 서버에 접속하기 위해 인증서버와 인증(패스워드)
㉤ 인증서버는 인증된 클라이언트에게 티켓 발급 서버로부터 티켓 발급을 허용

① ㉣ → ㉢ → ㉤ → ㉡ → ㉠
② ㉠ → ㉣ → ㉡ → ㉢ → ㉤
❸ ㉣ → ㉤ → ㉡ → ㉠ → ㉢
④ ㉤ → ㉡ → ㉠ → ㉢ → ㉣

65. 다음은 특정 블록 암호 운영 모드의 암호화 과정이다. 해당 모드는?(문제 오류로 운영모드 이미지가 없습니다. 정확한 내용을 아시는분 께서는 오류신고를 통하여 내용 작성 부탁드립니다. 정답은 2번 입니다.)

① ECB 모드 ❷ CBC 모드
③ CFB 모드 ④ OFB 모드

66. 스트림 암호에 대한 설명으로 가장 부적절한 것은?

① 일회성 패드를 실용적으로 구현할 목적으로 개발되었다.
❷ 짧은 주기와 높은 선형 복잡도가 요구되며 주로 LFSR을 이용한다.
③ 블록단위 암호화 대비 비트단위로 암호화하여 암호화 시간이 더 빠르다.
④ 블록 암호의 OFB 모드는 스트림 암호와 유사하게 동작한다.

67. 다음 중 전자서명에 대한 설명으로 옳지 않은 것은?

❶ 서명문에 공개키 암호화 방식(혹은 비대칭 암호화 방식)을 이용하여 서명자의 개인키로 생성한 정보
② 전자서명은 서명문의 위조 불가, 서명한 행위의 부인 방지를 제공할 수 있다.
③ 은닉서명은 서명자가 서명문의 내용을 알지 못하는 상태에서 서명하도록 한 방식으로 서명자의 익명성이 보장된다.
④ DSA 알고리즘은 이산대수 문제의 어려움에 기반을 두고 있는 대표적인 전자서명 알고리즘이다.

68. 다음 중 KDC(Key Distribution Center)에 대한 설명으로 옳지 않은 것은?

❶ 사용자가 아무리 많더라도 KDC에서 관리하여야 할 키의 수는 동일하다.
② 사용자는 상대방과의 암호 통신에 사용될 키를 생성할 필요가 없다.
③ 키의 관리는 KDC에서 이루어지기 때문에 사용자의 키 관리가 요구되지 않는다.
④ KDC에서 많은 키를 관리하기 때문에 해커에 의한 공격 위험이 높다.

69. 공개키 기반 구조(PKI)에서 등록기관(RA)이 수행하는 기능이 아닌 것은?

① 인증서 발급 대행 ② 사용자 신분 확인
③ 인증 요청서 보관 ❹ 인증서 폐지 목록 저장

70. 아래 지문은 긴 메시지에 전자서명하는 방법에 대한 설명이다. 이렇게 하는 가장 근본적인 이유는?

긴 메시지의 해시값을 생성하고, 이를 자신의 개인키로 전자서명 한다. 검증자는 수신된 긴 메시지로부터 해시값을 계산하고, 전자서명자의 공개키로 전자서명된 해시값으로부터 해시값을 복원한다. 이렇게 얻어진 2개의 해시값을 비교하여 동일성 여부로 전자서명을 검증한다.

❶ 전자서명 알고리즘의 특성상 전자서명 및 검증속도가 데이터량에 따라 많은 영향을 받기 때문이다.
② 국제표준으로 규정된 것이기 때문이다.
③ 해시함수로 생성된 해시값이 안전한 전자서명을 보장하기 때문이다.
④ 전자서명에 대칭암호시스템이 사용되기 때문이다.

71. 256 비트 키 길이의 AES 알고리즘의 라운드의 개수는?

① 10 ② 12
❸ 14 ④ 16

72. 다음 설명 중 틀린 것은?

❶ 사용자의 인증서에 인증기관의 올바른 전자서명이 붙어 있고 인증서의 유효기간이 유효하면 인증서를 신뢰한다.
② 개인키가 제대로 관리되고 있어도 인증서는 폐지될 수 있다.
③ 인증서가 폐지되면 CRL에 추가되고 폐지 대상 인증서 목록에 인증기관이 전자서명을 한다.
④ 인증서에 포함되어 있는 공개키가 바른지를 알아보기 위해서는 인증기관의 공개키가 필요하다.

73. 다음 중 HMAC에 대한 설계 목적의 설명으로 올바르지 않은 것은?

① 내장된 해시함수를 손쉽게 교체할 수 있어야 한다.
❷ 사용되는 해시함수를 손쉽게 구할 수 있어야 한다.
③ 제공되는 해시함수를 목적에 맞게 변경하여 사용할 수 있어야 한다.
④ 해시함수의 원래의 성능을 거의 유지할 수 있어야 한다.

74. 다음 블록 암호 운영 모드 중 메시지 인증에 사용될 수 있는 것들로 올바르게 짝지어진 것은?

㉠ ECB ㉡ CBC ㉢ CFB ㉣ CTR

① ㉠ - ㉡ ② ㉠ - ㉢
③ ㉡ - ㉢ ❹ ㉡ - ㉣

75. 다음 중 CRL(Certificate Revocation List)에 대한 설명으로 옳지 않은 것은?

① 인증서 폐지 사유로는 인증 발생 조직에서의 탈퇴, 개인키의 침해, 개인키의 유출 의심 등이 있다.
② 인증서 폐지 메커니즘은 X.509에 정의된 인증서 폐지 목록(CRL)으로 관리한다.
❸ 인증서의 폐지는 인증서 소유자 본인만 가능하다.
④ 폐지된 인증서의 목록은 디렉터리에 보관하여 공개하고 네트워크를 통해 접속하여 확인할 수 있다.

76. 무선 네트워크 보안을 위한 WPA, WPA2 등에서는 순방향 기밀성(forward secrecy)을 지원하지 않고 있지만, 2018년 Wi-Fi Alliance에서는 순방향 기밀성을 지원하는 WPA3을 발표하였다. 다음 중 순방향 기밀성의 의미를 올바르게 설명하고 있는 것은?

① 보안 프로토콜이 적용된 이후의 트래픽에 대해서는 기밀성이 보장된다.

② 중간자 공격을 통해 암호키를 탈취하는 공격에 대한 방어 메커니즘을 갖추고 있다.

❸ 현재 사용되는 세션키나 마스터키가 노출되더라도 예전에 암호화된 트래픽의 기밀성에 영향을 미치지 않는다.

④ 192비트 이상의 암호 강도를 갖는 AES-256, SHA-384 등의 고강도 암호 알고리즘의 채택을 의무화하고, 취약한 비밀번호 사용을 차단한다.

77. 다음 지문의 괄호 안에 들어갈 용어를 순서대로 나열한 것은?

> 공개키 알고리즘으로 정보화 서비스와 전자서명 서비스를 제공할 때 암호화에 사용하는 키는 수신자의 ( )이고, 서명 검증에 사용하는 키는 송신자의 ( )이다.

① 개인키, 개인키 ② 개인키, 공개키

③ 공개키, 개인키 ❹ 공개키, 공개키

78. 공개키 기반구조와 인증서에 대한 다음 설명 중 적절치 않은 것은?

① 인증서란 사용자의 공개키에 대해 인증기관이 인증해 주는 전자문서이다.

② 등록기관이란 공개키와 인증서 소유자 사이의 관계를 확인해주고 인증서 발급을 대행해 주는 기관이다.

❸ 인증서에는 평문 상태의 공개키와 암호문 상태의 개인키가 포함된다.

④ X.509 인증서의 확장영역은 CRL 배포지점 등 사용자나 공개키에 연계된 여러 가지 속성들에 해당하는 선택정보를 담고 있는 부분으로 X.509 버전 3에서 도입되었다.

79. 다음 중 암호공격 방식에 대한 설명이 틀린 것은?

❶ 트래픽 분석 : 불법적인 공격자가 전송되는 메시지를 도중에 가로채어 그 내용을 외부로 노출시키는 공격

② 재생 공격 : 공격자가 이전에 특정 송신자와 수신자 간에 행해졌던 통신내용을 캡처하여 보관하고 있다가 나중에 다시 전송하는 공격

③ 삽입 공격 : 불법적인 공격자가 정당한 송신자로 가장하여 특정 수신자에게 위조된 메시지를 보내어 불법적인 효과를 발생시키는 공격

④ 메시지 변조 : 전송되는 메시지들의 순서를 바꾸거나 메시지의 일부분을 다른 메시지로 대체하여 불법적인 효과를 발생시키는 공격

80. 해시함수 h와 주어진 입력값 x에 대해 h(x)=h(x')을 만족하는 x'(≠x)를 찾는 것이 계산적으로 불가능한 것을 무엇이라고 하는가?

① 압축성 ② 일방향성

❸ 두 번째 역상저항성 ④ 강한 충돌 저항성

5과목 : 정보보안 관리 및 법규

81. 빈칸 ㉠, ㉡에 들어갈 용어를 순서대로 나열한 것은 무엇인가?

> 위험관리의 정보자산 식별 활동에서는 조직의 (㉠)에 따라 정보자산 분류기준을 수립하여 관리체계 범위 내 모든 정보자산을 식별/분류하고, (㉡) 산정한 후 그 목록을 최신으로 관리하여야 한다.

① ㉠ 목표 ㉡ 위협 수준을

② ㉠ 업무특성 ㉡ 위협 수준을

③ ㉠ 목표 ㉡ 중요도를

❹ ㉠ 업무특성 ㉡ 중요도를

82. 다음 중 정보보호 교육 및 훈련에 대한 설명으로 적절하지 않은 것은 무엇인가?

① 위험분석을 통해 구현된 정보보호 대책을 실제 운영 또는 시행할 부서 및 담당자를 파악하여 관련 내용을 공유하고 교육한다.

❷ 정책, 지침 및 절차 등이 개정된 사항에 대해서는 모두 모이기 어렵기 때문에 집합 또는 온라인 교육보단 게시판 등을 통해서 알리는 것이 보다 효과적이다.

③ 타사의 침해사고 사례, 최근 발생한 보안위험 등에 대한 최근 동향을 지속적으로 교육함으로써 보안인식 제고를 위해 노력한다.

④ 출장, 휴가 등의 사정으로 정기 정보보호 교육을 받지 못한 인력에 대해서 전달교육, 추가교육, 온라인 교육 등의 방법으로 정보보호 교육을 수행한다.

83. 다음 지문이 설명하는 것은?

> 이것은 정보자산의 기밀성, 무결성, 가용성을 실현하기 위한 절차와 과정을 체계적으로 수립, 문서화하고 지속적으로 관리, 운영하는 시스템을 말한다.

① 업무연속성관리체계 ② 재난복구체계

③ 보안성평가체계 ❹ 정보보호관리체계

84. 다음 중 정량적 위험분석의 장점이 아닌 것은?

① 위험관리 성능평가가 용이하다.

② 위험평가 결과가 금전적 가치, 백분율, 확률 등으로 표현되어 이해가 쉽다.

③ 정보자산의 가치가 논리적으로 평가되고 화폐로 표현되어 이해가 쉽다.

❹ 위험분석 작업을 위한 시간과 비용이 절약된다.

85. 개인정보 영향평가를 하는 경우에 고려할 사항이 아닌 것은?

① 처리하는 개인정보의 수

② 개인정보의 제3자 제공여부

❸ 개인정보처리의 위탁 여부

④ 정보주체의 권리를 해할 가능성 및 그 위험의 정도

86. 인터넷 기업이 사물인터넷(Internet of Things, IoT)을 이용한 비즈니스를 구상하고 있다. 사물인터넷은 이종 장치들과 유무선 네트워크 기술 그리고 지능화 플랫폼을 기반으로 개

발되어야 한다. 서비스 제공자와 사용자가 IoT 장치의 전 주기 세부단계에서 고려해야 하는 공통 보안 요구사항 중에서 'IoT 장치 및 서비스 운영/관리/폐기 단계의 보안요구사항'으로 가장 부적절한 것은?

① IoT 침해사고 대응체계 및 책임추적성 확보 방안 마련

② 안전한 운영·관리를 위한 정보보호 및 프라이버시 관리 체계 마련

❸ 안전한 소프트웨어 및 하드웨어 개발 기술 적용 및 검증

④ IoT 제품·서비스의 취약점 보안패치 및 업데이트 지속 이행

87. 다음 중 「개인정보보호법」에 따른 국무총리 소속의 개인정보보호위원회의 기능이 아닌 것은?

❶ 개인정보보호 관련 법령, 정책 등을 수립하거나 집행

② 개인정보보호에 관한 법령의 해석·운영에 관한 사항 심의

③ 개인정보의 처리에 관한 공공기관 간의 의견조정에 관한 사항 의결

④ 관계 기관 등에 대한 자료제출이나 사실조회 요구

88. 정보통신서비스 제공자가 이용자에 대한 정보를 이용하려고 수집하는 경우 이용자에게 알리고 동의 받아야 할 사항이 아닌 것은?

① 개인정보의 수집· 이용 목적

❷ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

③ 수집하는 개인정보의 항목

④ 개인정보의 보유·이용 기간

89. 업무연속성관리 및 재난복구계획을 위하여 수행하는 내용 중에서 올바르지 않은 것은 무엇인가?

❶ 재난복구서비스 중에 웜사이트는 재난 발생 시 새로운 컴퓨터를 설치할 수 있는 컴퓨터실을 미리 준비해 둔 것으로 별다른 장비는 가지고 있지 않은 것을 의미한다.

② 업무연속성계획의 접근5단계 방법론에는 프로젝트의 범위 설정 및 기획, 사업영향평가, 복구전략 개발, 복구계획 수립, 프로젝트의 수행 테스트 및 유지 보수로 나눌 수 있다.

③ 재해복구테스트 종류는 체크리스트 방법, 구조적 점검 테스트, 시뮬레이션, 병렬테스트, 전체 시스템 중단 테스트 등이 있다.

④ 업무영향분석의 목적은 운영의 전부 혹은 일부 그리고 컴퓨터서비스가 작동하지 않을 때, 조직을 보호하기 위한 핵심 업무를 파악하는 것이며, 핵심 업무의 정지로 인해 조직에 발생되는 잠재적인 손해 혹은 손실을 파악하는 것이다.

90. 공공기관에서 개인정보파일을 운용하는 경우에 보호위원회에 등록해야 하는 사항에 포함되지 않는 것은?

① 개인정보파일의 명칭

② 개인정보파일에 기록되는 개인정보 항목

❸ 개인정보를 일시적으로 제공하는 경우 그 제공받는 자

④ 개인정보파일로 보유하고 있는 개인정보의 정보주체 수

91. 위험분석 결과 식별된 위험에 대한 처리 전략과 위험별 위험처리를 위한 적절한 (개인)정보보호 대책을 선정한 내용 중에서 올바르지 않은 것은?

① 위험감소: 비밀번호 도용의 위험을 줄이기 위해 개인정보처리시스템 등 중요한 시스템의 로그인 비밀번호 복잡도 길이를 3가지 문자조합, 8글자 이상 강제 설정하도록 비밀번호 설정 모듈을 개발하여 적용한다.

❷ 위험수용: 유지보수 등 협력업체, 개인정보 처리 수탁자 중에서 직접 모두 관리·감독할 수 없어 개인정보를 대량으로 처리하고 있는 IT 수탁사를 대상으로 관리·감독하고 나머지 수탁자는 이슈가 발생될 경우에만 관리·감독한다.

③ 위험전가: 중요정보 및 개인정보 유출 시 손해 배상 소송 등에 따른 비용 손실을 줄이기 위해 관련 보험에 가입한다.

④ 위험회피: 회사 홍보용 인터넷 홈페이지에서는 회원관리에 따른 위험이 존재하므로 회원 가입을 받지 않는 것으로 변경하고 기존 회원 정보는 모두 파기 처리한다.

92. 경영진 참여에 대한 사항으로 가장 부적절한 것은?

❶ 경영진 참여가 이루어질 수 있도록 보고, 의사 결정 등의 책임과 역할을 문서화하지 않았지만 정기적으로 보고하고 있다.

② 경영진이 직접 정보보호 활동에 참여도 가능하지만 정보보호 위원회 등을 구성하여 중요한 의사결정 등을 결정할 수 있다.

③ 조직의 규모 및 특성에 맞게 보고 및 의사결정 절차, 대상, 주기 등을 결정할 수 있다.

④ 경영진 참여가 원칙이나, 내부 위임전결 등의 규정이 있는 경우에는 정보보호를 담당하고 있는 책임자가 경영진의 의사결정을 대행할 수 있다.

93. 다음 중 법률에 근거하여 운영되고 있는 정보보호 및 개인정보보호 관련 제도 중에서 자율제도가 아닌 의무제도에 해당하는 것은?

① 정보보호 준비도 평가

② 클라우드 보안인증제

③ 정보보호 공시제도

❹ 주요정보통신기반시설 취약점의 분석·평가

94. 개인정보처리자는 다음 지문의 사항이 포함된 것을 정하고 이를 정보주체가 쉽게 확인할 수 있게 공개하도록 되어 있다. 다음 지문의 사항이 포함된 문서의 법률적 명칭은 무엇인가?

> 개인정보의 처리 목적
> 개인정보의 처리 및 보유 기간
> 개인정보의 제3자의 제공에 관한 사항(해당되는 경우에만 정한다.)
> 개인정보처리의 위탁에 관한 사항(해당되는 경우에만 정한다.)
> 정보주체의 권리의무 및 그 행사방법에 관한 사항
> 그 밖에 개인정보의 처리에 관하여 대통령령으로 정한 사항

① 개인정보 보호정책 ② 표준 개인정보 보호지침

③ 개인정보 보호지침 ❹ 개인정보 처리방침

95. 정보통신망을 통해 이용자가 원하지 않음에도 불구하고 일방적으로 전송되는 영리목적의 광고성 정보인 스팸에 관련된 내용 중에서 잘못된 것은?

❶ 휴대전화 등의 앱 푸시 알람 ON/OFF 기능은 광고성 정보 수신 동의와 동일하므로 푸시 알람을 승인한 경우에는 광고성 정보를 전송하는 것이 가능하다.

② 전송자가 제공하는 재화 또는 서비스에 대한 조건 또는 특징에 대한 변경 안내 정보(회원 등급 변경·포인트 소멸 안내 등)는 영리 목적 광고성 정보의 예외이다.

③ 광고성 정보를 전송하려면 사전에 문서(전자문서 포함) 또는 구술 등의 방법으로 수신자에게 명시적으로 수신 동의를 받아야 한다.

④ 오후 9시부터 그 다음 날 오전 8시까지 전자적 전송매체를 이용하여 광고성 정보를 전송하려는 자는 수신자에게 별도의 사전 동의를 받아야 한다.

96. 다음은 개인정보보호법상 개인정보처리 위탁에 관한 설명이다. 가장 거리가 먼 것은?

① 개인정보처리자가 제3자에게 개인정보의 처리 업무를 위탁하는 경우에는 일정한 내용이 포함된 문서에 의하여야 한다.

❷ 개인정보처리자가 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 위탁에 대해 정보주체의 동의를 받아야 한다.

③ 위탁자는 업무위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리 현황 점검 등 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.

④ 수탁자가 위탁받은 업무와 관련하여 개인정보를 처리하는 과정에서 이 법을 위반하여 발생한 손해배상책임에 대해서는 수탁자를 개인정보처리자의 소속 직원으로 본다.

97. 「정보통신기반 보호법」에 관련된 사항으로 적절하지 않은 것은?

① 주요정보통신기반시설보호계획에는 주요정보통신 기반시설의 취약점 분석·평가에 관한 사항이 포함되어 있다.

② 주요정보통신기반시설보호대책의 미흡으로 국가 안전보장이나 경제사회 전반에 피해가 우려된다고 판단하여 그 보완을 명하는 경우 주요정보통신 기반시설의 침해사고 예방 및 복구 등의 업무에 대한 기술적 지원을 요청할 수 있다.

③ 침해사고가 발생하여 소관 주요정보통신기반시설이 교란·마비 또는 파괴된 사실을 인지한 때에는 관계 행정기관, 수사기관 또는 인터넷진흥원에 그 사실을 통지하여야 한다.

❹ 금융·통신 등 분야별 정보통신기반시설을 위하여 취약점 및 침해요인과 그 대응방안에 관한 정보 제공, 침해사고가 발생하는 경우 실시간 경보·분석체계 운영 업무를 수행하는 사이버안전센터를 구축·운영할 수 있다.

98. 다음은 개인정보처리시스템을 기획하는 단계에서 개인정보보호를 위해 검토하고 확인하여야 할 기본원칙에 관한 설명이다. 잘못된 것끼리 묶은 것은?

가. 개인정보보호 관련 법령 및 지침 등 관련 규정을 세부적으로 검토
나. 개인정보 수집 최소화를 위해 개인정보 처리 목적을 명확히 하고 수집
다. 개인정보 목적 달성 시 파기 방법은 사업진행 상황에 따라 결정
라. 주민등록번호 인증을 통한 회원가입 방법 제공
마. 개인정보처리시스템에 대한 접근권한 등 기본적인 보안대책 마련
바. 개인정보 전송 및 저장 시 적용할 암호화 알고리즘과 방식 결정
사. 개인정보처리시스템과 관련된 개인정보 처리방침 수립
아. 공공기관 개인정보처리시스템과 관련하여서는 개인정보 영향평가 고려

① 가, 나 ❷ 다, 라
③ 마, 바 ④ 사, 아

99. 개인정보보호법 상 개인정보 유출 시 개인정보 처리자가 정보 주체에게 알려야 할 사항으로 옳은 것만을 모두 고르면?

㉠ 유출된 개인정보의 위탁 현황
㉡ 유출된 시점과 그 경위
㉢ 개인정보 보관 폐기 기간
㉣ 정보 주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당 부서 및 연락처

① ㉠, ㉡ ② ㉢, ㉣
③ ㉠, ㉢ ❹ ㉡, ㉣

100. 정보통신서비스 제공자 등은 개인정보의 분실·도난·누출 사실을 안 때에는 지체 없이 다음 각 호의 모든 사항을 해당 이용자에게 알리고 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니 된다. 이때 정당한 사유에 관하여 잘못 설명된 것은?

① 단전, 홍수, 폭설 등의 천재지변으로 인해 24시간 내에 신고가 불가능한 경우, 방송통신위원회 또는 한국인터넷진흥원에 대한 신고지연의 정당한 사유가 될 수 있다.

② 경찰이 이용자 통지에 대해 보류를 요청한 경우, 수사상의 이유로 이용자에 대한 통지 지연의 정당한 사유가 될 수 있다.

③ 물리적·기술적·관리적인 사유로 통지가 불가능한 경우, 이용자에 대한 통지지연의 정당한 사유가 될 수 있다.

❹ 누출 등이 된 개인정보 항목이나 누출 등이 발생한 시점에 대한 파악이 24시간 내에 불가능한 경우, 통지·신고 지연의 정당한 사유가 될 수 있다.

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