1. 다음 보기에서 설명하고 있는 정보보호의 목표로 가장 적절한 것은?

> 가. 정보는 소유자의 인가를 받은 사람만 접근할 수 있다.
> 나. 인가되지 않은 정보는 절대로 공개되어서는 안된다.

① 기밀성(Confidentiality) ② 무결성(Integrity)
③ 가용성(Availability) ④ 인증성(Authentication)

2. 무결성을 위협하는 보안 공격으로 가장 적절하지 <u>않은</u> 것은?

① 스누핑(Snooping)
② 가장(Masquerading)
③ 재연(Replaying)
④ 부인(Repudiation)

3. 다음 중 개인정보보호를 위한 비식별화 기술에 대한 설명으로 가장 적절한 것은?

① 가명처리(Pseudonymization)는 개인식별이 가능한 데이터에 대하여 직접적으로 식별할 수 없는 다른 값으로 대체하는 방법이다.
② 총계 처리(Aggregation)는 개인을 식별하는데 기여할 확률이 높은 주요 개인 식별자에 대해 전체 또는 부분적으로 '*' 등의 대체값으로 변환하는 방법이다.
③ 데이터 삭제(Data Reduction)는 개인정보에 대하여 통계값을 적용하여 특정 개인을 판단할 수 없도록 하는 방법이다.
④ 데이터 마스킹(Data Masking)은 단일 식별 정보를 해당 그룹의 대푯값으로 변환하거나 구간값으로 변환하여 고유정보 추적 및 식별을 방지하는 방법이다.

4. 다음 보기에서 설명하고 있는 패스워드 크랙 공격으로 가장 적절한 것은?

> 해시알고리즘별 패스워드 해시값을 저장시켜 놓은 데이터베이스를 가지고 있다. 크랙하고자 하는 패스워드의 해시값을 알고 있을 때, 기존 해시 데이터베이스와 비교하여 동일한 해시값이 매핑되면, 역으로 그 해시의 원래 평문값인 비밀번호를 추출할 수 있다.

① 무작위 대입 공격
② 레인보우테이블 이용 공격
③ 사전 공격
④ 차분 공격

5. 최근의 정보보호시스템들은 기계학습·인공지능 기술을 적용하여 보안제품을 개발하고 있다. 기계학습은 학습유형에 따라 지도학습, 비지도학습 및 강화학습으로 구분될 수 있다. 다음 중 비지도학습 모델에 해당하는 것으로 가장 적절한 것은?

① Logistic Regression ② k-Means
③ Random Forest ④ Deep Q learning Network

6. 무결성(Integrity), 인증(Authentication)과 부인(Repudiation) 방지를 모두 제공하는 온라인 기술로 가장 적절한 것은?

① HMAC ② 일방향 해시
③ 접근제어 ④ 디지털 서명

7. 메시지 인증 코드(Message Authentication Code) 기술이 제공하는 기능으로 가장 적절한 것은?

① 접근제어와 부인방지
② 무결성 보장과 접근제어
③ 무결성 보장과 인증
④ 인증과 부인방지

8. 인터넷에는 악성코드를 배포하는 네트워크가 존재한다. 인터넷 서핑 중 웹 공격에 의해 악성코드가 감염되는 Drive-by Download가 발생하는데, 그 공격 절차로 가장 적절한 것은?

> 가. 익스플로잇 킷(exploit kit)에 의한 공격 수행
> 나. 경유지를 통해 이동(redirect)
> 다. 악성코드 설치 및 실행
> 라. 악성코드 링크를 통해 악성코드 다운로드
> 마. 공격자가 웹사이트를 변조하여 악성 링크를 심어 넣음

① 마→가→나→라→다 ② 가→마→나→라→다
③ 가→마→라→나→다 ④ 마→나→가→라→다

9. 블록암호화 모드의 복호화 수식으로 가장 적절하지 <u>않은</u> 것은? (단, C_i: i번째 암호문, P_i: i번째 평문, $E_K(P_i)$: Key를 이용한 P_i의 암호화, $D_K(C_i)$: Key를 이용한 C_i의 복호화)

① ECB: $P_i = D_K(C_i)$
② CBC: $P_i = D_K(C_i) \oplus C_{i-1}$
③ CFB: $P_i = D_K(C_{i-1}) \oplus C_i$
④ CTR: $P_i = E_K(Counter) \oplus C_i$

10. 128비트 데이터 블록을 사용한 Rijndael알고리즘을 기반으로 하는 반복 암호로 가장 적절한 것은?

① DES ② Skipjack
③ AES ④ Blowfish

11. 블록 암호화 과정에서 마지막 평문 블록이 단위 블록 길이에 미치지 못할 경우에 적당한 길이의 비트 열을 추가하여, 단위 블록의 길이에 맞도록 데이터를 채워 넣는 것으로 가장 적절한 것은?

① 패킷 ② 패딩
③ 필드 ④ 패치

12. 하이브리드 암호 시스템으로 가장 적절하지 <u>않은</u> 것은?
① 대칭암호의 암호화에서 사용한 세션 키는 의사난수 생성기로 생성한다.
② 메시지는 대칭 암호로 암호화한다.
③ 대칭암호의 암호화에서 사용한 세션 키는 개인 키 암호로 암호화한다.
④ 공개 키 암호의 암호화에서 사용하는 키는 하이브리드 암호 시스템의 외부로부터 부여된다.

13. RSA 암호알고리즘에서 두 소수 p=3, q=11과 키값 e=3을 선택한 경우, 평문 m=8에 대한 암호문 c로 가장 적절한 것은?
① 15 ② 17
③ 19 ④ 21

14. 일방향 해시함수의 성질로 가장 적절하지 <u>않은</u> 것은?
① 정해진 길이 입력값을 받아 정해진 길이 결과값을 출력한다.
② 해시 알고리즘에는 MD5, SHA-2 등이 있다.
③ 해시는 메시지의 무결성을 확인하기 위해서 사용한다.
④ 결과값으로부터 입력값을 역산할 수 없다.

15. 일방향 해시함수 SHA-3에 대한 설명으로 가장 적절하지 <u>않은</u> 것은?
① 미국의 표준화 기구 NIST는 2012년 KECCAK이라는 알고리즘을 최종 표준으로 선정했다.
② SHA-1과 SHA-2와는 전혀 다른 스펀지구조로 흡수단계와 추출단계를 통해서 해시값을 출력한다.
③ SHA-2의 강한 충돌(Strong Collision) 내성이 깨졌다는 사실을 알고, NIST에서 공모하여 선정했다.
④ 선정조건 중 하나는 “구조를 명확히 하여 해석이 쉬울 것”이다.

16. 주어진 메시지 x에 대해, $H(y) = H(x)$를 만족하면서 $y \neq x$인 y를 찾는 것이 계산적으로는 불가능해야 하는 해시 함수의 특성으로 가장 적절한 것은?
① 의사난수성(Pseudo-randomness)
② 일방향성(Onewayness)
③ 약한 충돌 저항성(Weak Collision Resistance)
④ 강한 충돌 저항성(Strong Collision Resistance)

17. PKI(Public Key Infrastructure)에 대한 설명으로 가장 적절하지 <u>않은</u> 것은?
① PKI의 3가지 구성요소는 사용자, 인증기관, 저장소이다.
② X.509 인증서는 개인키를 포함한다.
③ PKI 환경에서 공개키 암호를 이용할 경우 CA(Certification Authority)는 인증서를 발급한다.
④ 공개키 인증서를 발행하여 무결성, 인증과 부인(Repudiation) 방지를 보장한다.

18. 난수와 PKI에 대한 설명으로 가장 적절하지 <u>않은</u> 것은?
① 난수의 성질에는 무작위성, 예측 불가능성, 재현 불가능성이 있다.
② PKI 환경에서 등록기관은 공개키 인증서를 발급하고, 또 필요에 따라 취소한다.
③ ANSI X9.17에는 의사난수 생성기의 보다 구체적인 구성 방법이 기술되어 있다.
④ 저장소는 인증서와 사용자 관련 정보, 상호 인증서 쌍 및 인증서 취소목록 등을 저장 및 검색하는 장소를 말한다.

19. Biba 보안모델에 대한 설명으로 가장 적절한 것은?
① 시스템 내부 정보의 무결성 유지보다 기밀성을 보장하는 것이 목표이다.
② 정보 주체는 응용 프로그램을 통해서만 정보 객체에 대한 접근이 가능하다.
③ 임의적 접근제어 방식으로 직무 분리를 통해 무결성 침해를 방지한다.
④ 보안등급이 낮은 주체는 보안등급이 높은 객체에 쓰기가 금지된다.

20. 다음 보기에서 강제적 접근제어(MAC, Mandatory Access Control)에 해당하는 것을 모두 고른 것으로 가장 적절한 것은?

가. 비밀성을 갖는 객체에 대하여 주체가 갖는 권한에 근거하여 객체에 대한 접근을 제어하는 방법이다.
나. 주체와 객체의 수에 관계 없이 접근 규칙의 수가 정해지며 개별 주체와 개별 객체 단위의 접근 제한 설정은 불가능하다.
다. 신분 기반의 접근제어 방식으로 접근 권한 관리가 간단하며 보안 관리자의 개입 없이 다른 사용자에게 접근 권한 부여가 가능하다.
라. 사용자는 보호 대상 정보나 자원에 대한 접근 권한을 얻기 위해서는 해당 접근 권한이 배정된 역할의 구성원이 되어야 한다.
마. 접근 권한 주체와 접근 권한 대상이 어떠한 환경에 처해 있는가를 동적으로 분석하여 접근 권한을 부여하는 방법이다.

① 가, 나 ② 나, 다 ③ 나, 라 ④ 다, 마

21. 다음 중 커버로스 프로토콜(Kerberos Protocol)에 대한 설명으로 가장 적절한 것은?
① 인증 서버가 다운되어도 새로운 사용자의 로그인이 가능하다.
② 요청을 주고받는 호스트들 간에 시간 동기화 없이 인증이 가능하다.
③ 커버로스는 세사미(SESAME)의 약점을 보완하기 위해 개발되었다.
④ 대칭키 기반으로 동작하는 컴퓨터 네트워크 인증 프로토콜이다.

22. DB 암호화 방법 중 API 방식에 대한 설명으로 가장 적절한 것은?
① 암복호화 모듈을 애플리케이션 서버 내 설치하여 운영한다.
② 블록 암호화에 적합한 방식으로 고속으로 동작한다.
③ 애플리케이션의 수정이 필요 없어 편리하다.
④ 암복호화할 때 DB 서버의 사용으로 부하가 발생한다.

23. 취약점 데이터베이스로 가장 적절하지 않은 것은?

① Exploit-db ② CVE
③ NIST NVD ④ Shodan

24. ISO 27001의 정보보호 통제 영역으로 가장 적절하지 않은 것은?

① 자산 관리 ② 업무 연속성 관리
③ 컴플라이언스 ④ 품질보증 관리

25. 위험분석 방법 중 정성적 위험분석 유형으로 가장 적절하지 않은 것은?

① 델파이법 ② 시나리오법
③ 순위결정법 ④ 확률분포법

26. 정보보호 위험관리에 대한 설명으로 가장 적절하지 않은 것은?

① 위험분석의 목적은 자산을 식별하고 그 자산의 위험 수준을 측정하여, 그 위험이 허용 가능한 수준인지 아닌지 판단할 수 있는 근거를 마련하는 것이다.
② 자산은 조직이 보호해야 할 대상으로 정보, 하드웨어, 소프트웨어, 시설, 인력, 데이터베이스 등 유형 및 무형자산을 포함한다.
③ 위험분석에서 사용하는 연간예상손실액(ALE)은 단일손실예상액(SLE)과 연간발생빈도(ARO)의 곱으로 계산한다.
④ 정보보안 위험처리 방식 중 위험회피는 위험에 대한 책임을 회피하기 위해 제3자와 공유하는 것으로, 잠재적 손실을 보험 등을 통해 제3자에게 할당하는 것이다.

27. 보안 관제 조직 중 컴퓨터 침해 대응팀(CERT: Computer Emergency Response Team)의 역할로 가장 적절하지 않은 것은?

① 침해 사고 대응 기술 연구
② 이상 트래픽 분석을 통한 침해 여부 판단
③ 침해 사고 시스템의 사용자에 대한 조사
④ 취약점 진단과 침해 사고 예방 활동

28. 다음은 국제공통평가기준(CC)의 구성 요소에 대한 내용이다. 빈칸 ㉠, ㉡에 해당하는 가장 적절한 것은?

> 가. 같은 부류에 속하는 정보시스템은 (㉠)을(를) 새로 작성할 필요 없이 기존에 작성된 (㉠)을(를) 활용할 수 있음
> 나. 작성자는 정보시스템의 기술적인 구현 가능성을 고려하여 (㉡)을(를) 작성하고, 같은 부류의 제품이라도 개별적으로 정의함

① ㉠ 보호프로파일(PP) ㉡ 보안목표명세서(ST)
② ㉠ 보안목표명세서(ST) ㉡ 보호프로파일(PP)
③ ㉠ 평가보증등급(EAL) ㉡ 평가대상(TOE)
④ ㉠ 평가대상(TOE) ㉡ 평가보증등급(EAL)

29. TCSEC 보안등급에 대한 설명으로 가장 적절하지 않은 것은?

① A1등급은 가장 높은 보안등급으로 엄격한 인증, 제한 및 감사를 요구한다.
② B1등급은 레이블된 보안 보호, 보안정책을 적용할 수 있다.
③ C1등급은 통제적 접근 보호, 각 계정별 로그인이 가능하고, 그룹 ID로 통제 가능하다.
④ D등급은 가장 낮은 등급으로 최소한의 보호만을 요구한다.

30. 디지털 증거의 특성으로 가장 적절하지 않은 것은?

① 복제 용이성 ② 비가독성
③ 대량성 ④ 변조 난해성

31. 다음 보기에서 설명하는「형사소송법」조항과 가장 관련성이 깊은 디지털포렌식의 원칙은?

> 제308조의2(위법수집증거의 배제) 적법한 절차에 따르지 아니하고 수집한 증거는 증거로 할 수 없다.

① 정당성의 원칙 ② 무결성의 원칙
③ 재현성의 원칙 ④ 신속성의 원칙

32. 다음은「형사소송법」제106조(압수)에 대한 내용이다. 빈칸 ㉠, ㉡에 해당하는 가장 적절한 것은?

> ③ 법원은 압수의 목적물이 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체인 경우에는 기억된 정보의 범위를 정하여 출력하거나 복제하여 제출받아야 한다. 다만, 범위를 정하여 출력 또는 복제하는 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란하다고 인정되는 때에는 정보저장매체등을 압수할 수 있다.
> ④ 법원은 제3항에 따라 정보를 제공받는 경우 (㉠) 제2조 제3호에 따른 (㉡)에게 해당 사실을 지체 없이 알려야 한다.

① ㉠ 개인정보보호법 ㉡ 정보주체
② ㉠ 경찰관의 정보수집 및 처리등에 관한 규정 ㉡ 보관자
③ ㉠ 개인정보보호법 ㉡ 보관자
④ ㉠ 경찰관의 정보수집 및 처리등에 관한 규정 ㉡ 정보주체

33. OECD의 개인정보보호 원칙에 대한 설명으로 가장 적절하지 않은 것은?

① 개인 참가의 원칙: 정보주체가 제공한 개인정보에 대해 열람, 정정, 삭제를 요구할 수 있는 절차를 마련해야 한다.
② 안전성 보호의 원칙: 개인정보의 분실, 불법적인 접근, 훼손, 사용, 변조, 공개 등의 위험에 대비하여 합리적인 보호조치를 마련해야 한다.
③ 목적 명확성의 원칙: 개인정보는 그 이용목적에 부합되는 것이어야 하며 이용목적에 필요한 범위 내에서 정확하고 완전하며 최신의 상태를 유지해야 한다.
④ 공개의 원칙: 개인정보 관리자의 주소 등을 비롯하여 개인정보의 이용목적, 관련된 정책 등에 대한 내용이 포함된 공개방침이 있어야 한다.

34. 「개인정보보호법」 상 개인정보 보호책임자의 업무로 가장 적절하지 <u>않은</u> 것은?

① 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
② 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
③ 개인정보의 처리와 관련한 고충처리·권리구제 및 개인정보에 관한 분쟁의 조정
④ 개인정보 보호 교육 계획의 수립 및 시행

35. 「개인정보보호법」 제23조(민감정보의 처리 제한)과 그 시행령 제18조(민감정보의 범위)에서 규정하는 민감정보로 가장 적절하지 <u>않은</u> 것은?

① 사상·신념에 관한 정보
② 교육 이력에 관한 정보
③ 정치적 견해에 관한 정보
④ 건강·성생활에 관한 정보

36. 다음은 「개인정보보호법」 제34조의2(과징금의 부과 등)에 대한 내용이다. 빈칸 ㉠, ㉡에 해당하는 가장 적절한 것은?

> 보호위원회는 개인정보처리자가 처리하는 (㉠)가 분실·도난·유출·위조·변조 또는 훼손된 경우에는 (㉡)의 과징금을 부과·징수할 수 있다. 다만, (㉠)가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 개인정보처리자가 제24조제3항에 따른 안전성 확보에 필요한 조치를 다한 경우에는 그러하지 아니하다.

① ㉠ 주민등록번호 ㉡ 5억원 이하
② ㉠ 주민등록번호 ㉡ 10억원 이하
③ ㉠ 개인정보 ㉡ 5억원 이하
④ ㉠ 개인정보 ㉡ 10억원 이하

37. 「개인정보보호법」 제3절 가명정보의 처리에 관한 특례에 관한 설명으로 가장 적절하지 <u>않은</u> 것은?

① 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있다.
② 개인정보처리자는 가명정보를 처리하는 과정에서 특정 개인을 알아볼 수 있는 정보가 생성된 경우에는 즉시 해당 정보의 처리를 중지하고, 지체 없이 회수·파기하여야 한다.
③ 개인정보처리자는 가명정보를 제3자에게 제공하는 경우에는 특정 개인을 알아보기 위하여 사용될 수 있는 정보를 포함해서는 아니 된다.
④ 개인정보처리자는 가명 정보 결합을 수행한 기관 외부로 결합된 정보를 반출하려는 경우에는 소속기관의 장의 승인을 받아야 한다.

38. 다음은 「개인정보보호법」 제28조의6(가명정보 처리에 대한 과징금 부과 등)에 대한 내용이다. 빈칸 ㉠, ㉡, ㉢에 해당하는 가장 적절한 것은?

> ① 보호위원회는 개인정보처리자가 제28조의5제1항을 위반하여 특정 개인을 알아보기 위한 목적으로 정보를 처리한 경우 전체 매출액의 (㉠) 이하에 해당하는 금액을 과징금으로 부과할 수 있다. 다만, 매출액이 없거나 매출액의 산정이 곤란한 경우로서 대통령령으로 정하는 경우에는 (㉡) 또는 자본금의 (㉢) 중 큰 금액 이하로 과징금을 부과할 수 있다.

① ㉠ 100분의 3 ㉡ 2억원 ㉢ 100분의 3
② ㉠ 100분의 5 ㉡ 2억원 ㉢ 100분의 5
③ ㉠ 100분의 3 ㉡ 4억원 ㉢ 100분의 3
④ ㉠ 100분의 5 ㉡ 4억원 ㉢ 100분의 5

39. 다음 보기에서 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조의 정보보호 관리체계 인증(ISMS) 의무 대상자를 모두 고른 것으로 가장 적절한 것은?

> 가. 집적정보통신시설 사업자
> 나. 전기통신사업법 제6조 1항에 따른 등록을 한 자로서 대통령령으로 정하는 바에 따라 정보통신망서비스를 제공하는 자
> 다. 연간 매출액 1000억 이상의 상급 종합병원
> 라. 정보통신서비스 부문 전년도(법인의 경우 전 사업연도를 말한다) 매출액이 50억원 이상인 자
> 마. 정보통신서비스 부문 3개월 간의 일일평균 이용자수가 100만명 이상인 자

① 가, 나, 다
② 가, 나, 마
③ 나, 다, 마
④ 나, 라, 마

40. 다음은 「정보통신기반보호법」 제3조 정보통신기반보호위원회에 대한 내용이다. 빈칸 ㉠, ㉡에 해당하는 가장 적절한 것은?

> ① 제8조에 따라 지정된 주요정보통신기반시설의 보호에 관한 사항을 심의하기 위하여 국무총리 소속하에 정보통신기반보호위원회(이하 '위원회'라 한다)를 둔다.
> ② 위원회의 위원은 위원장 1인을 포함한 (㉠)인 이내의 위원으로 구성한다.
> ③ 위원회의 위원장은 (㉡)이 되고, 위원회의 위원은 대통령령으로 정하는 중앙행정기관의 차관급 공무원과 위원장이 위촉하는 사람으로 한다.

① ㉠ 20 ㉡ 국무조정실장
② ㉠ 25 ㉡ 국무조정실장
③ ㉠ 20 ㉡ 과학기술정보통신부 장관
④ ㉠ 25 ㉡ 과학기술정보통신부 장관