【정보보안관리 및 법규】

1. 강제적 접근통제(MAC : Mandatory Access Control)의 문제점에 대한 설명으로 가장 적절하지 **않은** 것은?
① 제한적인 사용자 기능과 많은 관리적 부담을 요구하며 비용이 많이 소요된다.
② DAC(Discretionary Access Control) 시스템은 일반적인 목적의 컴퓨터이며, 반면에 MAC 시스템은 매우 특정한 목적을 위해 사용된다.
③ 접근에 대한 레이블링(labeling)을 정의하고 보안 정책을 확인해야하기 때문에 성능저하가 우려된다.
④ 통제의 기준이 주체의 신분에 근거를 두고 있으며, 접근통제 메커니즘이 데이터의 의미에 대해 아무런 지식을 가지고 있지 않다.

2. 다음은 커버로스(Kerberos) 서버, 다수의 클라이언트, 다수의 응용 서버로 구성된 커버로스 공동체 환경을 위한 조건이다. 적절한 것을 모두 고른 것은?

㉠ 커버로스 서버는 반드시 ID와 모든 사용자의 해시된 패스워드를 데이터베이스에 저장하고 있어야 한다. ㉡ 모든 사용자는 커버로스 서버에 등록돼야 한다. ㉢ 커버로스 서버는 각 서버와 비밀키를 공유해야 하고, 모든 서버는 커버로스 서버에 등록돼야 한다. ㉣ 상호 교류하는 각 공동체에 속한 커버로스 서버는 다른 공동체의 서버와 비밀키를 공유하지 않는 대신 두 개의 커버로스 서버는 상호 간에 등록돼야 한다.

① ㉠㉡ ② ㉠㉡㉢
③ ㉢㉣ ④ ㉠㉡㉢㉣

3. 정보보호 관리체계(ISMS : Information Security Management System)의 수행 절차에 대한 설명으로 가장 적절하지 **않은** 것은?
① 정보보호 정책 수립, 경영진 책임 및 조직 구성, 위험 관리, 정보보호 대책 구현, 사후 관리 순서의 수행 절차를 가진다.
② 경영진 책임 및 조직 구성 단계에서는 경영진 참여와 정보보호 조직구성 및 자원할당의 절차가 진행된다.
③ 위험 관리 단계에서는 위험관리 방법 및 계획을 수립하고, 위험 식별 및 평가가 이루어지고, 정보보호 대책 산정 및 이행계획이 수립된다.
④ 정보보호 대책 구현 단계에서는 내부 공유 및 교육이 이루어지고, 조직 전반에 걸친 상위 수준의 정보보호 관리체계 범위가 설정된다.

4. 국제 공통 평가기준(CC : Common Criteria)에 대한 설명으로 가장 적절하지 **않은** 것은?
① 국가마다 서로 다른 정보보호시스템 평가기준을 연동하고 평가결과를 상호인증하기 위해 제정된 평가기준이다.
② 정보보호시스템의 보안등급 평가에 신뢰성을 부여하고 현존하는 평가기준과 조화를 통해 평가결과의 상호인증을 위한 상호인정협정의 목적이 있다.
③ 보안기능과 보호기능으로 나누어 평가하고 보안 등급 체계는 A, B, C의 6등급으로 D는 부적합에 해당된다.
④ 정보보호 시스템의 수출입에 소요되는 인증비용절감으로 국제유통촉진이 가능하다.

5. 다음은 개인정보보호 관리체계(PIMS : Personal Information Management System)에 대한 설명이다. 적절하지 **않은** 것을 모두 고른 것은?

㉠ 국민들에게는 개인정보를 안전하게 관리하는 조직을 객관적으로 식별할 수 있는 기준을 제시한다. ㉡ 통제항목은 정보보호 분야에 개인정보의 특수성을 감안하여 개인정보 수집, 이용, 관리, 파기라는 개인정보 생명주기를 반영한 특징이 있다. ㉢ 인증체계는 과학기술정보통신부가 인정기관 역할을 수행하고 있으며 인증기관으로 한국인터넷진흥원(KISA)이 수행하고 있다. ㉣ 내부 정보 유출 방지를 위해 인증 과정 중에 외부 전문가를 포함하지 않고 기업이 자율 제도로 운영한다.

① ㉠㉡ ② ㉡㉢ ③ ㉢㉣ ④ ㉡㉣

6. 정보보호 관리체계(ISMS)와 개인정보보호 관리체계(PIMS)에 대한 설명으로 가장 적절하지 **않은** 것은?
① ISMS는 범위내 모든 정보자산과 보호대책을 전반적으로 취급하는데 반해, PIMS는 정보자산 중 개인정보에 특화된 보호와 정보보호를 대상으로 한다.
② PIMS는 원칙적으로 기업 또는 조직 전체가 인증 취득 범위로서 인증 범위를 한정시키고 단계적으로 그 범위를 확대하는 방식으로 채택할 수 있다.
③ ISMS에서는 부서, 사업장, 공장, 서비스 등의 장소와 네트워크, 물리적 대책 등 대상 범위에 대해 합리적으로 설명할 수 있는 범위를 한정해 '적용 범위'로서 인증 취득 범위를 선정할 수 있다.
④ PIMS에서는 정보 주체에게 불이익을 입힌 경우 법규 준수의 관점에서 개인정보만을 취급하는 것이며, ISMS는 정보시스템 전체의 정보보호를 취급한다.

7. 다음에서 설명하는 접근 방식에 따른 위험분석 방법으로 가장 적절한 것은?

모든 정보자산에 기업이외의 전문가 지식 및 경험을 활용하는 방법으로 비용 대비 효과가 우수하며 소규모 조직에 적합한 장점이 있지만, 누락하는 경우가 발생하기 쉽고 사업 분야 및 정보보호에 전문성이 높은 인력이 참여하여 수행하지 않으면 실패할 위험이 있다.

① 기준선 접근법(Baseline Approach)
② 비형식적 접근법(Informal Approach)
③ 상세 위험분석 접근법(Detailed Risk Analysis Approach)
④ 복합 접근법(Combined Approach)

8. 재해복구 시스템의 복구 수준별 유형에 대한 설명으로 가장 적절하지 **않은** 것은?
① 미러 사이트(Mirror Site) - 주 센터 재해시 원격지 시스템을 운영(Active) 상태로 전환하며, 서비스 제공 데이터는 동기적 또는 비동기적 방식의 실시간 미러링을 통하여 최신 상태를 유지한다.
② 핫 사이트(Hot Site) - 주 센터와 동일한 수준의 정보기술 자원을 원격지에 구축하여 스탠바이(Stand-by) 상태로 유지하며, 액티브-스탠바이(Active-Standby) 상태로 서비스를 제공함으로써 주기적인 테스트와 구성의 유연성을 제공한다.
③ 웜 사이트(Warm Site) - 중요성이 높은 정보기술 지원만 부분적으로 재해복구센터에 보유하고, 데이터는 수시간에서 1일의 주기로 백업하여 구축 및 유지비용이 핫 사이트에 비해 저렴하다.
④ 콜드 사이트(Cold Site) - 데이터만 원격지에 보관하고, 이의 서비스를 위한 정보자원은 확보하지 않거나 장소 등 최소한으로만 확보하고, 재해시 데이터를 근간으로 필요한 정보자원을 조달하여 정보시스템의 복구를 개시한다.

9. 「개인정보 보호법」에서 개인정보처리자는 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다. 개인정보처리자의 개인정보보호 원칙으로 가장 적절하지 **않은** 것은?
① 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용할 수 있다.
② 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.
③ 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.
④ 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.

10. 「개인정보 보호법」에서 다음 위반 사항에 대한 법정형이 가장 높은 것은?
① 영상정보처리기기의 설치 목적과 다른 목적으로 영상정보처리기기를 임의로 조작하거나 다른 곳을 비추는 자 또는 녹음기능을 사용한 자
② 동법에서 정한 안전성 확보에 필요한 조치를 하지 아니하여 개인정보를 분실·도난·유출·위조·변조 또는 훼손당한 개인정보처리자
③ 업무상 알게 된 개인정보를 누설하거나 권한 없이 다른 사람이 이용하도록 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자
④ 거짓이나 그 밖의 부정한 수단이나 방법으로 개인정보를 취득하거나 개인정보 처리에 관한 동의를 받는 행위를 한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자

11. 「개인정보 보호법」 제21조(개인정보의 파기)에서 개인정보처리자의 개인정보 파기와 관련된 내용으로 가장 적절하지 **않은** 것은?
① 개인정보처리자가 개인정보를 파기하기 전에는 6개월간 임시조치를 하여야 한다.
② 개인정보의 파기방법 및 절차 등에 필요한 사항은 대통령령으로 정한다.
③ 다른 법령에 규정이 없는 한 개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다.
④ 개인정보처리자가 개인정보를 파기하지 아니하고 보존하여야 하는 경우에는 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여서 저장·관리하여야 한다.

12. 「개인정보 보호법」 제23조(민감정보의 처리 제한), 「개인정보 보호법 시행령」 제18조(민감정보의 범위)에서 규정하고 있는 민감정보에 대한 내용으로 가장 적절하지 **않은** 것은?
① 범죄경력자료 ② 성생활에 관한 정보
③ 여권번호 ④ 유전정보

13. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 정보통신서비스 제공자등은 개인정보의 분실·도난·유출 사실을 안 때에는 지체 없이 해당 개인정보를 이용자에게 알리고 해당 기관에 신고해야 한다. 신고해야 할 내용으로 가장 적절하지 **않은** 것은?
① 유출등이 된 개인정보 항목
② 유출등이 발생한 시점
③ 이용자가 상담 등을 접수할 수 있는 부서 및 연락처
④ 이용자의 손해배상액

14. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제44조의7(불법정보의 유통금지 등)에 의거 누구든지 정보통신망을 통하여 불법정보를 유통해서는 안 된다. 이 불법정보에 대한 설명으로 가장 적절하지 **않은** 것은?
① 정당한 사유 없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해하는 내용의 정보
② 총포·화약류를 제조할 수 있는 방법이나 설계도 등의 정보
③ 사람을 비방할 목적이 없는 공공연한 사실 등의 정보
④ 범죄를 목적으로 하거나 교사 또는 방조하는 내용의 정보

15. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 "정보통신서비스제공자는 정보통신서비스의 제공에 사용되는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 하여야 한다"고 규정하고 있다. 정보통신망의 안정성 확보에 관한 정보보호지침 내용으로 가장 적절하지 **않은** 것은?
① 정보통신망의 지속적인 이용이 가능한 상태를 확보하기 위한 기술적·물리적 보호조치
② 정보통신망의 안정성 유지를 위한 법적·행정적 보호조치
③ 정보의 불법 유출·위조·변조·삭제 등을 방지하기 위한 기술적 보호조치
④ 정당한 권한이 없는 자가 정보통신망에 접근·침입하는 것을 방지하거나 대응하기 위한 정보보호시스템의 설치·운영 등 기술적·물리적 보호조치

16. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 및 동 시행령, 「개인정보 보호법」 및 동 시행령에 의거 개인정보 유출 통지 및 신고에 관한 법적 절차가 명시되어 있다. 네 가지 법령에서 "개인정보 유출 통지 및 신고 내용"을 설명한 것으로 가장 적절한 것은?
① 「개인정보 보호법 시행령」에 의하면 대통령령으로 정한 규모 이상의 개인정보란 5천 건 이상의 정보주체를 의미한다.
② 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니 된다고 규정하고 있다.
③ 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」에서 유출 신고 건수는 1만 건 이상을 의미한다.
④ 「개인정보 보호법」에서 개인정보 유출 신고기관은 방송통신위원회와 한국인터넷진흥원이다.

17. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 정보통신서비스 제공자가 이용자의 개인정보를 제3자에게 제공할 때, 이용자에게 동의를 받아야 하는 내용으로 가장 적절하지 **않은** 것은?
① 개인정보를 제공받는 자
② 개인정보를 제공받는 자의 개인정보 이용목적
③ 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간
④ 개인정보를 제공받는 자의 개인정보 침해 이력

18. 「정보통신기반 보호법」에서 국가안전보장에 중대한 영향을 미치는 주요정보통신기반시설에 대한 관리기관의 장이 기술적 지원을 요청한 경우 국가정보원장이 기술적 지원을 수행할 수 **없는** 시설로 가장 적절한 것은?
① 원자력·국방과학·첨단방위산업관련 정부출연연구기관의 연구시설
② 개인정보가 포함된 금융 정보통신기반시설
③ 전력, 가스, 석유 등 에너지·수자원 시설
④ 도로·철도·지하철·공항·항만 등 주요 교통시설

19. 「정보통신기반 보호법」에서 "전자적 침해행위"에 대한 내용으로 가장 적절하지 **않은** 것은?
① 해킹 ② 인터넷사기
③ 컴퓨터바이러스 ④ 고출력 전자기파

20. 「전자서명법」에서 공인인증에 대한 설명으로 가장 적절하지 **않은** 것은?
① "공인인증서"라 함은 공인인증기관이 발급하는 인증서를 말한다.
② "공인인증자"라 함은 전자서명생성정보를 보유하고 자신이 직접 또는 타인을 대리하여 서명을 하는 자를 말한다.
③ "공인인증기관"이라 함은 공인인증역무를 제공하기 위하여 지정된 자를 말한다.
④ "공인인증업무"라 함은 공인인증서의 발급, 인증관련 기록의 관리 등 공인인증역무를 제공하는 업무를 말한다.