【정보보안관리 및 법규】

1. 정보보호에 관한 설명으로 가장 적절하지 **않은** 것은?

① 정보보호는 다양한 내·외부 위협으로부터 조직의 정보자산에 대한 기밀성, 무결성, 가용성 등이 보장될 수 있도록 관리적, 기술적, 물리적 보호조치를 마련하는 것이다.

② 기밀성(confidentiality)은 권한있는 자만이 정보자산에 접근하여 그 내용을 알 수 있도록 보장하며 정당하지 않은 자에 의해 정보가 노출되지 않도록 보장하는 것이다.

③ 무결성(integrity)은 권한있는 자만이 위조·변조된 정보를 확인할 수 있도록 보장하며 이를 위해 장비 이중화 구성, 서버 클러스터링 구성, 디스크 RAID 구성의 기법이 활용된다.

④ 가용성(availability)은 권한있는 자의 정보자산 접근 필요 시 언제든지 접근할 수 있도록 보장하며 장애·재해가 발생해도 정상적인 서비스가 가능하도록 보장하는 것이다.

2. 재해복구시스템의 복구 수준별 유형에 관한 설명으로 가장 적절하지 **않은** 것은?

① 미러사이트 : 관리자가 선택한 데이터만을 별도의 백업디스크에 순차적으로 백업하는 방식으로 많은 복구 시간이 필요하다.

② 핫 사이트 : 주센터와 동일 수준의 시스템을 원격지 사이트에 구축한 후 대기상태로 실시간 미러링(mirroring)을 통해 최신 데이터를 유지하는 방식이며 주센터 재해 발생 시 활성상태로 전환하여 서비스를 제공한다.

③ 웜 사이트 : 주센터의 중요도가 높은 일부 시스템만 원격지 사이트에 구축하여 주센터 재해 발생 시 중요 업무에 대해서만 우선 복구하는 방식이다.

④ 콜드 사이트 : 데이터만 원격지에 보관하고 서비스를 위한 시스템은 확보하지 않거나 전원시설, 통신설비 등만을 최소한으로 확보하는 방식이다.

3. 시점별 통제에 관한 설명으로 가장 적절하지 **않은** 것은?

① 통제의 시점에 따라 예방통제, 탐지통제, 교정통제로 구분된다.

② 교정통제는 탐지 전 위협과 취약점에 대응하는 것으로 IDS의 성능을 향상시킨다.

③ 탐지통제는 예방통제를 우회하여 발생하는 문제점을 탐지하려는 활동으로 위협을 탐지한다.

④ 예방통제란 사전에 위협과 취약점에 대처하는 통제를 의미한다.

4. 위험분석 방법론에 관한 설명으로 가장 적절하지 **않은** 것은?

① 델파이법 : 각 분야의 전문적인 지식을 갖춘 전문가 집단을 구성하고 토론을 통해 위험분석을 수행하는 방식이다.

② 퍼지 행렬법 : 자산, 위험, 보안체계 등 위험분석 요소들을 정성적인 언어로 표현된 값을 사용하여 기대 손실을 평가하는 방식이다.

③ 확률 분포법 : 비교 우위 순위 결정표에 의해 위험 항목들의 서술적 순위를 결정하는 방식이다.

④ 시나리오법 : 어떤 사건도 기대대로 발생하지 않는다는 사실에 근거하여 위협에 대한 발생 가능한 결과들을 추정하는 방식이다.

5. 다음 표준에 관한 설명으로 옳은 것을 모두 고른 것은?

㉠ ISO/IEC 27000은 영국에서 개발된 BSI(British Standards Institute) 인증을 기반으로 만들어진 암호화 프레임워크로 국내 표준이다.
㉡ ISO/IEC 27000은 최적의 보안 관리체계 수립 운영, 정보보호 관리규범 제공을 목적으로 한다.
㉢ ISO/IEC 27001:2013은 통제영역 14개, 통제항목 114개로 구성된다.
㉣ ISO/IEC 27000은 유럽 회원국 공통으로 적용되는 정보보안 조례로 흔히 오렌지 북(orange book)이라고 불린다.

① ㉠㉡ ② ㉡㉣ ③ ㉡㉢ ④ ㉠㉣

6. 국제 공통평가 기준(CC, Common Criteria)의 등급별 보안 수준에 관한 설명으로 가장 적절한 것은?

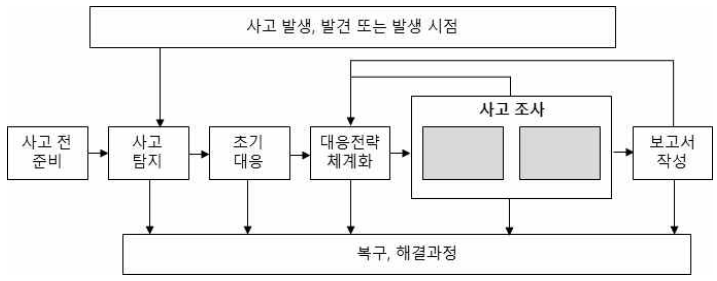
① EAL1 : 구조시험으로 체계적인 설계·시험 및 검토 단계로 독립적인 취약점 분석

② EAL3 : 방법론적 시험 및 검사로 완전한 범위의 보안 기능 시험

③ EAL5 : 정형화된 설계 검증 및 시험 단계로 포괄적 분석

④ EAL7 : 준정형 검증된 설계 및 시험으로 독립적인 취약점 검사

7. 한국인터넷진흥원의 침해사고 대응 절차 7단계 그림에서 사고조사 단계에 관한 설명으로 가장 적절하지 **않은** 것은?



① 데이터 수집 및 분석을 통해 사고조사를 수행하여 언제, 누가, 어떻게 사고가 일어났는지, 피해확산 및 사고 재발을 어떻게 방지할 것인지 결정하는 단계이다.

② 호스트 기반과 네트워크 기반 증거로 나누어 사고를 조사하며 조사과정은 데이터 수집과 데이터 분석(포렌식 분석) 단계로 나뉜다.

③ 호스트 기반 증거 수집은 휘발성 데이터가 사라지기 전에 수집하는 것이 중요하며 그 후에 포렌식 이미징 작업을 수행한다. 휘발성 증거는 사고 의도를 이해하고자 할 때 매우 중요한 정보와 시스템의 스냅 샷(snap-shot)을 제공한다.

④ 사고조사 증거 및 결과를 참고해 소송이 필요한 사항인지를 결정하여 사고조사 과정에 수사기관 공조 여부를 판단한다.

8. 다음 중 클라우드컴퓨팅에 관한 설명으로 옳은 것을 모두 고른 것은?

㉠ 클라우드컴퓨팅이란 집적·공유된 정보통신기기, 정보통신설비, 소프트웨어 등의 정보통신자원을 가상으로 결합하거나, 분할하여 사용하는 기술로 대량의 정보를 복수의 정보통신자원으로 분산하여 처리한다.
㉡ 클라우드컴퓨팅의 보안인증 유효기간은 인증 서비스 등을 고려해 경찰청장이 정하는 3년 내의 범위로 하고 연장을 하려는 자는 유효기간의 갱신을 신청하여야 한다.
㉢ PaaS의 경우, 이용자가 직접 구축하지 않고 이미 구축된 소프트웨어 및 애플리케이션만을 이용하는 서비스를 말한다.
㉣ 클라우드컴퓨팅 서비스 이용 시 서비스 유형에 따른 보안 위험을 평가하여 비인가 접근·설정오류 등을 방지할 수 있도록 보안 통제 정책을 수립·이행하여야 한다.

① ㉠㉡ ② ㉡㉢ ③ ㉢㉣ ④ ㉠㉣

9. 요구사항에 따른 위험분류에 관한 설명으로 가장 적절하지 **않은** 것은?

① 베이스라인 접근법은 모든 시스템에 대해 표준화된 보호대책 목록을 체크리스트 형태로 제공한다.

② 비정형 접근법은 정형화되고 구조화된 프로세스를 사용하는 대신 분석가 개인의 지식 및 경험을 활용한다.

③ 상세 위험분석은 경험자의 지식을 토대로 위험분석을 수행하기 때문에 빠르고 분석 비용이 상대적으로 저렴하다.

④ 복합 접근법은 고위험 영역에 대해 상세 위험분석을 수행하고 그 외의 다른 영역은 베이스라인 접근법을 사용한다.

10. 위험관리 5단계 과정에 관한 설명으로 가장 적절하지 **않은** 것은?

① 위험관리 전략 및 계획 수립 단계 : 자산, 위협, 취약성, 기존 보호 대책 등을 분석하여 위험의 종류와 규모를 결정한다.
② 위험평가 단계 : 위험분석 결과를 이용하여 최종적으로 위험도를 평가하고, 조직에서 수용 가능한 목표 위험수준을 정하여 이를 기준으로 위험의 대응 여부와 우선순위를 결정한다.
③ 정보보호 대책 선정 단계 : 위험평가 결과를 토대로 수용 가능한 목표 위험수준을 초과하는 위험을 수용 가능한 수준으로 감소시키기 위하여 위험처리 전략을 설정하고 적절한 통제사항을 선택한다.
④ 정보보호 계획 수립 단계 : 선정한 보호 대책을 구현하기 위한 이행계획을 수립하는 단계로 정보보호 대책 및 구현의 우선순위, 일정계획, 예산, 책임, 운영계획 등을 포함한 이행계획을 수립한다.

11. 「지능정보화 기본법」에서 정의하고 있는 지능정보기술에 관한 내용으로 가장 적절하지 **않은** 것은?

① 부호, 문자를 제외한 모든 데이터를 전자적으로 처리하는 기술
② 전자적 방법으로 학습·추론·판단 등을 구현하는 기술
③ 물건 상호 간 또는 사람과 물건 사이에 데이터를 처리하거나 물건을 이용·제어 또는 관리할 수 있도록 하는 기술
④ 무선 또는 유·무선이 결합된 초연결지능정보통신기반 기술

12. 다음 빈칸에 가장 적절한 것은?

(　　)은/는 개인정보를 활용하는 새로운 정보시스템 도입 및 기존 정보시스템의 변경 시, 기업의 고객은 물론 고객의 프라이버시에 미칠 영향에 대하여 미리 조사, 분석, 평가하는 체계적인 절차이다.

① 정보보호관리체계인증(ISMS)
② 하트블리드(heartbleed)
③ 개인정보영향평가(PIA)
④ 상호인정협정(CCRA)

13. 「개인정보 보호법」 제23조(민감정보의 처리 제한)에 관한 설명으로 가장 적절한 것은?

① 민감정보란 개인에 관한 정보로 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보를 의미한다.
② 민감정보란 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보를 의미한다.
③ 개인정보처리자는 정보주체의 개인정보 수집 및 이용 동의를 받은 경우, 민감정보는 별도 동의 없이 사용할 수 있다.
④ 개인정보처리자가 민감정보를 처리하는 경우, 그 민감정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 기술적 조치만 취하면 제3자에게 전달할 수 있다.

14. 「개인정보의 안전성 보호조치 기준」 제5조(접근권한의 관리)에 관한 설명으로 가장 적절한 것은?

① 개인정보처리자는 개인정보처리 시스템에 대한 접근권한을 업무수행에 필요한 최대한의 범위로 업무 담당자마다 동일하게 부여하여야 한다.
② 개인정보처리자는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우, 지체없이 개인정보처리 시스템의 접근권한을 변경 또는 말소하여야 한다.
③ 개인정보처리자는 권한 부여, 변경 또는 말소에 대한 내역을 기록하고 그 기록을 최소 7년간 보관하여야 한다.
④ 개인정보처리자는 개인정보처리 시스템에 접속할 수 있는 사용자 계정을 발급하는 경우, 사용자 그룹에 발급된 계정을 공유하고 그룹 내에서만 사용하도록 권한을 설정한다.

15. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조(정보보호 관리체계의 인증)에 관한 설명으로 가장 적절한 것은?

① 정보보호 최고책임자는 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계를 수립·운영하고 있는 자에 관하여 인증을 할 수 있다.
② 주요정보통신서비스 제공자 중 연간 매출액 또는 세입 등이 1,500억 원 이상이거나 정보통신 서비스 부문 전년도 매출액이 10억 원 이상 또는 7개월간의 일일 평균 이용자 수가 100만 명 이상에 해당하는 자는 인증을 받아야 한다.
③ 한국인터넷진흥원, 정보보호관리체계 인증기관 및 정보보호 관리체계 심사기관은 정보보호 관리체계의 실효성 제고를 위하여 연 2회 이상 사후관리를 실시하고 그 결과를 경찰청장에게 통보하여야 한다.
④ 정보보호 관리체계 인증의 유효기간은 3년으로 하고 정보보호 관리등급을 받은 경우 그 유효기간 동안 인증을 받은 것으로 본다.

16. 「개인정보 보호법」 제16조(개인정보의 수집 제한)에 관한 설명으로 가장 적절하지 **않은** 것은?

① 개인정보처리자는 개인정보를 수집하는 경우에 그 목적에 필요한 최소한의 개인정보를 수집하여야 한다. 이 경우 최소한의 개인정보 수집이라는 입증책임은 개인정보처리자가 부담한다.
② 개인정보처리자는 그 목적에 필요한 최소한의 범위를 벗어난 개인정보는 선택정보로서 필수정보 동의 시에 일괄 동의를 얻어야 하며 정보주체가 동의하여도 수집하지 못한다.
③ 개인정보처리자는 정보주체의 동의를 받아 개인정보를 수집하는 경우, 필요한 최소한의 정보 외의 개인정보 수집에는 동의하지 아니할 수 있다는 사실을 구체적으로 알려야 한다.
④ 개인정보처리자는 정보주체가 필요한 최소한의 정보 외의 개인정보 수집에 동의하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 아니된다.

17. 「개인정보의 기술적·관리적 보호조치 기준」 제6조(개인정보의 암호화)에 관한 설명으로 가장 적절하지 **않은** 것은?

① 정보통신서비스 제공자는 비밀번호가 복호화되지 않도록 양방향 암호화 알고리즘(해시함수)을 사용하여 암호화한다. 이때 암호화한 해시값을 크래킹하기 위해 첨가값(salt), 반복횟수(iteration count) 등을 추가하도록 하는 것이 가능하다.
② 정보통신서비스 제공자는 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호, 신용카드번호, 계좌정보, 생체인식정보에 대해서는 안전한 알고리즘으로 암호화하여 저장한다.
③ 정보통신서비스 제공자는 정보통신망을 통해 이용자의 개인정보 및 인증정보를 송·수신할 때 안전한 보안서버 구축 등의 조치를 통해 이를 암호화해야 한다.
④ 정보통신서비스 제공자는 이용자의 개인정보를 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때 이를 암호화해야 한다.

18. 「정보통신기반 보호법」 제3조(정보통신기반보호위원회)에 관한 설명으로 가장 적절하지 **않은** 것은?

① 주요정보통신기반시설 보호에 관한 사항을 심의하기 위하여 국가정보원장 소속하에 정보통신기반보호위원회(위원회)를 둔다.
② 위원회의 위원은 위원장 1인을 포함한 25인 이내의 위원으로 구성한다.
③ 위원회의 위원장은 국무조정실장이 되고 위원회의 위원은 대통령령으로 정하는 중앙행정기관의 차관급 공무원과 위원장이 위촉하는 사람으로 한다.
④ 위원회의 효율적인 운영을 위하여 위원회에 공공분야와 민간분야를 각각 담당하는 실무위원회를 둔다.

19. 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제25조(침해사고 등의 통지 등), 제26조(이용자 보호 등을 위한 정보 공개), 제27조(이용자 정보의 보호)에 관한 설명으로 가장 적절하지 **않은** 것은?

① 클라우드컴퓨팅 서비스 제공자는 이용자 정보가 유출되었을 때 사고 원인을 규명한 보고서가 작성·완료될 때까지 이용자에게 알리지 못한다.

② 이용자는 클라우드컴퓨팅 서비스 제공자에게 이용자 정보가 저장되는 국가의 명칭을 알려 줄 것을 요구할 수 있다.

③ 클라우드컴퓨팅 서비스 제공자는 법원의 제출명령이나 법관이 발부한 영장에 의하지 아니하고는 이용자의 동의 없이 이용자 정보를 제3자에게 제공할 수 없다.

④ 클라우드컴퓨팅 서비스 제공자는 사업을 종료하려는 경우에 이용자에게 사업종료 사실을 알리고 사업 종료일 전까지 이용자 정보를 반환해야 한다.

20. 「위치정보의 보호 및 이용 등에 관한 법률」 제15조(위치정보의 수집 등의 금지)에 관한 설명으로 가장 적절하지 **않은** 것은?

① 누구든지 개인위치정보주체의 동의를 받을 경우, 개인위치정보의 수집·이용이 가능하다.

② 긴급구조기관의 긴급구조요청이 있는 경우에도 개인위치정보주체의 동의 없이는 개인위치정보의 수집·이용은 불가능하다.

③ 위치정보를 수집할 수 있는 장치가 부착된 물건을 판매하거나 대여·양도하는 자는 위치정보 수집장치가 부착된 사실을 구매하거나 대여·양도받는 자에게 알려야 한다.

④ 누구든지 타인의 정보통신기기를 복제하거나 정보를 도용하는 방법으로 개인위치정보사업자 및 위치기반서비스사업자를 속여 타인의 개인위치정보를 제공받아서는 아니된다.