정보보호론

문 1. 정보보호의 3대 요소 중 가용성에 대한 설명으로 옳은 것은?

① 권한이 없는 사람은 정보자산에 대한 수정이 허락되지 않음을 의미한다.
② 권한이 없는 사람은 정보자산에 대한 접근이 허락되지 않음을 의미한다.
③ 정보를 암호화하여 저장하면 가용성이 보장된다.
④ DoS(Denial of Service) 공격은 가용성을 위협한다.

문 2. ISO/IEC 27001에서 제시된 정보보안관리를 위한 PDCA 모델에서 ISMS의 지속적 개선을 위해 시정 및 예방 조치를 하는 단계는?

① Plan
② Do
③ Check
④ Act

문 3. 보안 관리 대상에 대한 설명으로 ㉠~㉢에 들어갈 용어는?

> ○ (㉠) – 시스템과 네트워크의 접근 및 사용 등에 관한 중요 내용이 기록되는 것을 말한다.
> ○ (㉡) – 사용자와 시스템 또는 두 시스템 간의 활성화된 접속을 말한다.
> ○ (㉢) – 자산에 손실을 초래할 수 있는 원치 않는 사건의 잠재적 원인이나 행위자를 말한다.

	㉠	㉡	㉢
①	로그	세션	위험
②	로그	세션	위협
③	백업	쿠키	위험
④	백업	쿠키	위협

문 4. 유닉스 시스템에서 파일의 접근모드 변경에 사용되는 심볼릭 모드 명령어에 대한 설명으로 옳은 것은?

① chmod u-w: 소유자에게 쓰기 권한 추가
② chmod g+wx: 그룹, 기타 사용자에게 쓰기와 실행 권한 추가
③ chmod a+r: 소유자, 그룹, 기타 사용자에게 읽기 권한 추가
④ chmod o-w: 기타 사용자에게 쓰기 권한 추가

문 5. 정보가 안전한 정도를 평가하는 TCSEC(Trusted Computer System Evaluation Criteria)의 보안등급 중에서 검증된 설계(Verified Design)를 의미하는 보안등급은?

① A 등급
② B 등급
③ C 등급
④ D 등급

문 6. 다음에서 설명하는 공격 기술은?

> 암호 장비의 동작 과정 중에 획득 가능한 연산시간, 전력 소모량, 전자기파 방사량 등의 정보를 활용하여 암호 알고리즘의 비밀 정보를 찾아내는 기술

① 차분 암호 분석 공격(Differential Cryptanalysis Attack)
② 중간자 공격(Man-In-The-Middle Attack)
③ 부채널 공격(Side-Channel Attack)
④ 재전송 공격(Replay Attack)

문 7. DoS(Denial of Service) 공격의 대응 방법에 대한 설명으로 ㉠, ㉡에 들어갈 용어는?

> ○ 다른 네트워크로부터 들어오는 IP broadcast 패킷을 허용하지 않으면 자신의 네트워크가 (㉠) 공격의 중간 매개지로 쓰이는 것을 막을 수 있다.
> ○ 다른 네트워크로부터 들어오는 패킷 중에 출발지 주소가 내부 IP 주소인 패킷을 차단하면 (㉡) 공격을 막을 수 있다.

	㉠	㉡
①	Smurf	Land
②	Smurf	Ping of Death
③	Ping of Death	Land
④	Ping of Death	Smurf

문 8. 「전자서명법」상 용어의 정의로 옳지 않은 것은?

① '전자서명'이라 함은 서명자를 확인하고 서명자가 당해 전자문서에 서명을 하였음을 나타내는 데 이용하기 위하여 당해 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보를 말한다.
② '인증서'라 함은 전자서명생성정보가 가입자에게 유일하게 속한다는 사실 등을 확인하고 이를 증명하는 전자적 정보를 말한다.
③ '서명자'라 함은 전자서명검증정보를 보유하고 자신이 직접 또는 타인을 대리하여 서명을 하는 자를 말한다.
④ '전자서명생성정보'라 함은 전자서명을 생성하기 위하여 이용하는 전자적 정보를 말한다.

문 9. 「전자정부 SW 개발·운영자를 위한 소프트웨어 개발보안 가이드」상 분석·설계 단계 보안요구항목과 구현 단계 보안약점을 연결한 것으로 옳지 않은 것은?

	분석·설계 단계 보안요구항목	구현 단계 보안약점
①	DBMS 조회 및 결과 검증	SQL 삽입
②	디렉터리 서비스 조회 및 결과 검증	LDAP 삽입
③	웹서비스 요청 및 결과 검증	크로스사이트 스크립트
④	보안기능 동작에 사용되는 입력값 검증	솔트 없이 일방향 해시함수 사용

문 10. 개인정보 보호법령상 영업양도 등에 따른 개인정보의 이전 제한에 대한 내용으로 옳지 않은 것은?

① 영업양수자등은 영업의 양도·합병 등으로 개인정보를 이전받은 경우에는 이전 당시의 본래 목적으로만 개인정보를 이용하거나 제3자에게 제공할 수 있다.

② 영업양수자등이 과실 없이 서면 등의 방법으로 개인정보를 이전받은 사실 등을 정보주체에게 알릴 수 없는 경우에는 해당 사항을 인터넷 홈페이지에 10일 이상 게재하여야 한다.

③ 개인정보처리자는 영업의 전부 또는 일부의 양도·합병 등으로 개인정보를 다른 사람에게 이전하는 경우에는 미리 개인정보를 이전하려는 사실 등을 서면 등의 방법에 따라 해당 정보주체에게 알려야 한다.

④ 영업양수자등은 개인정보를 이전받았을 때에는 지체 없이 그 사실을 서면 등의 방법에 따라 정보주체에게 알려야 한다. 다만, 개인정보처리자가 「개인정보 보호법」 제27조제1항에 따라 그 이전 사실을 이미 알린 경우에는 그러하지 아니하다.

문 11. 대칭키 암호 알고리즘에 대한 설명으로 옳은 것만을 모두 고르면?

ㄱ. AES는 128/192/256 비트 키 길이를 지원한다.
ㄴ. DES는 16라운드 Feistel 구조를 가진다.
ㄷ. ARIA는 128/192/256 비트 키 길이를 지원한다.
ㄹ. SEED는 16라운드 SPN(Substitution Permutation Network) 구조를 가진다.

① ㄱ, ㄹ
② ㄴ, ㄷ
③ ㄱ, ㄴ, ㄷ
④ ㄱ, ㄴ, ㄹ

문 12. 다음에서 설명하는 프로토콜은?

○ 무선랜 통신을 암호화하는 프로토콜로서 IEEE 802.11 표준에 정의되었다.
○ 암호화를 위해 RC4 알고리즘을 사용한다.

① AH(Authentication Header)
② SSH(Secure SHell)
③ WAP(Wireless Application Protocol)
④ WEP(Wired Equivalent Privacy)

문 13. 기밀성을 제공하는 암호 기술이 아닌 것은?

① RSA
② SHA-1
③ ECC
④ IDEA

문 14. SSL 프로토콜에 대한 설명으로 옳지 않은 것은?

① 전송계층과 네트워크계층 사이에서 동작한다.
② 인증, 기밀성, 무결성 서비스를 제공한다.
③ Handshake Protocol은 보안 속성 협상을 담당한다.
④ Record Protocol은 메시지 압축 및 암호화를 담당한다.

문 15. DSA(Digital Signature Algorithm)에 대한 설명으로 옳지 않은 것은?

① 기밀성과 부인방지를 동시에 보장한다.
② NIST에서 발표한 전자서명 표준 알고리즘이다.
③ 전자서명의 생성 및 검증 과정에 해시함수가 사용된다.
④ 유한체상의 이산대수문제의 어려움에 그 안전성의 기반을 둔다.

문 16. 무의미한 코드를 삽입하고 프로그램 실행 순서를 섞는 등 악성코드 분석가의 작업을 방해하는 기술은?

① 디스어셈블(Disassemble)
② 난독화(Obfuscation)
③ 디버깅(Debugging)
④ 언패킹(Unpacking)

문 17. 윈도우즈용 네트워크 및 시스템 관리 명령어에 대한 설명으로 옳은 것은?

① ping – 원격 시스템에 대한 경로 및 물리 주소 정보를 제공한다.
② arp – IP 주소에서 물리 주소로의 변환 정보를 제공한다.
③ tracert – IP 주소, 물리 주소 및 네트워크 인터페이스 정보를 제공한다.
④ ipconfig – 원격 시스템의 동작 여부 및 RTT(Round Trip Time) 정보를 제공한다.

문 18. 정보자산에 대한 위험분석에서 사용하는 ALE(Annualized Loss Expectancy, 연간예상손실액), SLE(Single Loss Expectancy, 1회손실예상액), ARO(Annualized Rate of Occurrence, 연간발생빈도) 사이의 관계로 옳은 것은?

① ALE = SLE + ARO
② ALE = SLE × ARO
③ SLE = ALE + ARO
④ SLE = ALE × ARO

문 19. 「개인정보 보호법」상 개인정보 보호 원칙으로 옳지 않은 것은?

① 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.

② 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.

③ 개인정보처리자는 개인정보의 익명처리가 가능한 경우에는 익명에 의하여 처리될 수 있도록 하여야 한다.

④ 개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 비밀로 하여야 한다.

문 20. 다음에서 설명하는 블록암호 운용 모드는?

○ 암·복호화 모두 병렬 처리가 가능하다.
○ 블록 암호 알고리즘의 암호화 로직만 사용한다.
○ 암호문의 한 비트 오류는 복호화되는 평문의 한 비트에만 영향을 준다.

① ECB
② CBC
③ CFB
④ CTR