정보보호론

문 1. 다음 대칭키 암호화에서 K값은?

○ 8비트 정보 P와 K의 배타적 논리합(XOR) 연산의 결과를 Q라 함 ○ P = 11010011 ○ Q = 10000110

① 11010011
② 10000110
③ 01010101
④ 01010100

문 2. DRM(Digital Right Management)에 대한 설명으로 옳지 않은 것은?
① 문서의 열람, 편집, 프린트 등에 대한 접근 권한을 설정한다.
② 문서 사용에 인가를 부여받은 사용자에게 접근을 허용한다.
③ DRM 모듈로 운영되는 시스템의 하드디스크는 도난당하더라도 정보 유출의 위험이 적다.
④ 사용하기 불편하므로 인증서를 전혀 사용하지 않는다.

문 3. 블록암호 알고리즘에 대한 설명으로 옳지 않은 것은?
① IDEA – 상이한 대수 그룹으로부터의 세 가지 연산을 혼합하는 방식
② Blowfish – 키의 크기가 가변적이므로 안전성과 성능의 요구에 따라 유연하게 사용
③ SEED – 1999년 KISA와 국내 암호전문가들이 개발한 128비트 블록암호
④ ARIA – 국가보안기술연구소 주관으로 64비트 블록 암호로 128비트 암호화키만 지원

문 4. 암호화에 대한 설명으로 옳지 않은 것은?
① AES는 블록 크기가 192비트이며, 키는 192비트와 256비트 두 가지를 사용한다.
② Rabin은 RSA와 같은 원리로 암호화하고, 2차 합동에 근거하고 있다.
③ DES는 대칭키 방식으로서 16개 라운드로 구성되어 있다.
④ One-Time Pad는 암호화를 수행할 때마다 랜덤하게 선택된 키 스트림을 사용한다.

문 5. 가상화 시스템을 보호하는 방법으로 옳지 않은 것은?
① 게스트 운영체제 사용자들에게 하이퍼바이저에 접근하는 관리권한을 부여해야 한다.
② 원격 감독 기능을 사용할 때에는 적절한 인증과 암호화 메커니즘을 사용해야 한다.
③ 게스트 운영체제와 응용프로그램을 보호하는 것 외에도 가상화 환경과 하이퍼바이저도 보호해야 한다.
④ 하이퍼바이저가 게스트의 활동을 투명하게 감시해야 한다.

문 6. 정보시스템을 보호하기 위한 미국의 정보보호관리체계로 적합한 것은?
① PIPL
② FISMA
③ JIPDEC
④ NICST

문 7. 솔라리스 10에서 FTP 파일전송 시 발생되는 /var/log/xferlog 기록 내용에 대한 설명으로 옳지 않은 것은?

Thu Feb 2 16:41:30 2017 1 192.168.10.1 ㉠2870 ㉡/tmp/12-ftp.bmp ㉢b _ o r wish ftp 0 ㉣* c 2870 0

① ㉠ – 응답 포트 번호
② ㉡ – 전송된 파일의 이름
③ ㉢ – 바이너리 파일 전송
④ ㉣ – 인증 서버를 사용하지 않음

문 8. 생체인식에 대한 특징으로 옳지 않은 것은?
① 생체인식은 사람의 생체적 특징과 행동적 특징을 통한 보편성, 유일성, 영속성, 획득성을 요구한다.
② FRR은 인증 권한이 있는 사람이 인증을 시도했을 때 인증에 실패하는 비율을 말한다.
③ CER은 잘못된 거부율과 잘못된 허용 비율 곡선의 교차점을 말한다.
④ 엄격한 보안이 요구되는 경우는 FAR을 높이고, FRR을 낮춤으로써 보안성을 향상시킬 수 있다.

문 9. 정보보호관리체계(ISMS)의 정보보호 관리과정에 대한 설명으로 옳지 않은 것은?
① 정보보호정책은 조직이 수행하는 모든 정보보호활동의 근거를 포함할 수 있도록 수립하고, 조직에 미치는 영향을 고려하여 중요한 업무, 서비스, 조직, 자산 등을 포함할 수 있도록 범위를 설정한다.
② 최고경영자는 조직의 규모, 업무 중요도 분석을 통해 정보보호 관리체계의 지속적인 운영이 가능하도록 정보보호 최고책임자, 실무조직 등 정보보호조직을 구성하고 정보보호 관리체계 운영 활동을 수행하는 데 필요한 자원을 확보하여야 한다.
③ 위험관리 방법 및 계획에 따라 정보보호 일부 영역에 대한 위험 식별 및 평가를 2년에 1회 수행하고 그 결과에 따라 조직에서 수용 가능한 위험수준도 설정하여 관리하여야 한다.
④ 정보보호대책 이행 계획에 따라 보호대책을 구현하고 경영진은 이행 결과의 정확성 및 효과성 여부를 확인하여 구현된 정보보호대책을 실제 운영 또는 시행할 부서 및 담당자를 파악하여 관련 내용을 공유하고 교육하여야 한다.

문 10. ISO/IEC JTC 1의 SC 27에서 담당하는 범위가 아닌 것은?
① Management of information and ICT security
② Cards and personal identification
③ Security evaluation criteria and methodology
④ Security requirements capture methodology

문 11. 해킹 수단과 그 공격 방법에 대한 설명으로 옳지 않은 것은?

① Ransomware – 파일을 암호화한 후 복호화를 조건으로 금전을 요구함

② Rootkit – 스택에 할당된 버퍼보다 큰 코드를 삽입하여 오동작을 일으킴

③ SQL Injection – 데이터베이스에 질의어를 변조하여 공격함

④ Cross-site Scripting – 웹 페이지에 악성 스크립트를 삽입하여 정보를 획득함

문 12. 암호모듈을 KS X ISO/IEC 19790에 따라 검증하고 암호모듈의 안전성을 보증하는 국내 제도는?

① KCMVP

② TCSEC

③ ITSEC

④ METI

문 13. 사용자가 무선랜 보안을 위하여 취할 수 있는 방법이 아닌 것은?

① MAC 주소 필터링의 적용

② SSID(Service Set Identifier) 브로드캐스팅의 금지

③ 무선 장비 관련 패스워드의 주기적인 변경

④ WPA, WPA2, WEP 중에서 가장 안전한 보안 방법인 WEP를 이용한 무선랜의 통신 보호

문 14. ISO 27001의 통제 영역별 주요 내용에 대한 설명으로 옳지 않은 것은?

① 자산 관리 영역은 자산을 파악하고, 이를 적절히 분류하고 보호하는 데 활용하는 것이다.

② 사업 연속성 관리 영역은 형법과 민법, 법령, 규정 또는 계약 의무 및 보안 요구 사항에 대한 위반을 피하기 위한 기준을 제시한 것이다.

③ 정보시스템 획득, 개발, 유지 보수 영역은 정보시스템 내에 보안이 수립되어 있음을 보장하기 위한 것이다.

④ 통신 및 운영 관리 영역은 정보처리 설비의 정확하고 안전한 운영을 보장하기 위한 내용을 포함하고 있다.

문 15. 정수의 소인수분해를 기반으로 한 RSA 암호 알고리즘에서 공개키 (e, n) = (7, 33)을 이용하여 생성된 암호문 C 값이 7일 때, 이를 다시 복호화한다면 원문 메시지 값은?

① 11

② 13

③ 17

④ 19

문 16. 리눅스 파일의 접근 제어에 대한 설명으로 옳지 않은 것은?

① 모든 종류의 파일은 inode라는 파일 관리 수단으로 운영체제에 의해서 관리된다.

② passwd 명령으로 패스워드를 설정하면, 패스워드에 대한 암호화나 해시된 값이 /etc/passwd에 저장된다.

③ superuser 계정은 시스템의 모든 권한이 가능하므로 외부에 노출되지 않도록 주의해야 한다.

④ 어떤 권한을 가지고 있는가에 대한 UID, GID가 별도로 존재한다.

문 17. 블루투스에 대한 설명으로 옳지 않은 것은?

① 페어링 과정은 한 장치가 그 지역에 있는 다른 장치들을 찾아 BD_ADDR이나 논리적 이름에 근거해 파트너가 될 장치를 선택하는 것이다.

② 장치 간 종류를 식별하기 위해서 SDP(Service Discovery Protocol)를 보내고 받는다.

③ 블루투스의 취약점을 이용하여 장비의 임의 파일에 접근하는 공격은 BlueBug이다.

④ OPP(OBEX Push Profile)는 블루투스 장치끼리 인증 없이 정보를 간편하게 교환하기 위해 개발되었다.

문 18. 방화벽의 보안 기능에 대한 설명으로 옳은 것은?

① 방화벽은 내부의 불만이 있는 사용자 또는 외부 공격자와 무의식적으로 협력하는 사용자를 완벽히 차단할 수 있다.

② 방화벽을 설치하게 되면 외부로부터의 모든 무선랜 통신을 안전하게 보호할 수 있다.

③ 랩톱, PDA와 같은 이동형 저장장치가 감염되는 경우에도 방화벽을 설치하여 내부 네트워크를 안전하게 보호할 수 있다.

④ 내부 보안 정책을 만족하는 트래픽만이 방화벽을 통과할 수 있다.

문 19. 재해복구 시스템의 복구 수준별 유형에 대한 설명으로 옳지 않은 것은?

① Mirror Site – 주 센터와 동일한 수준의 정보기술 자원(하드웨어, 소프트웨어, 기타 부대 장비 등)을 원격지에 구축하여 모두 액티브 상태에서 실시간으로 동시에 서비스하는 방식

② Hot Site – 주 센터와 동일한 수준의 정보기술 자원을 대기 상태(standby)로 원격지에 구축하여 동기적 혹은 비동기적 미러링을 통해 데이터의 최신을 유지하고 있다가 주 센터 재해 시 액티브로 전환하여 서비스하는 방식

③ Down Site – 웹 애플리케이션 서비스 등 데이터의 업데이트 빈도가 높은 정보시스템을 액티브로 전환하여 서비스하는 방식

④ Cold Site – 기계실, 전원 시설, 통신 설비, 공조 시설, 온도 조절 시스템 등을 갖추어 놓고, 주 센터 재해 시 정보기술 자원을 설치하여 서비스하는 방식

문 20. 정보보안 관리 규격 중 IT 보호 및 통제부문의 모범적인 업무 수행 방법에 적용 가능한 ISACA(Information Systems Audit and Control Association)에서 개발된 프레임워크는?

① COBIT

② BS 7799

③ BSI

④ HIPAA