

정보보호론

문 1. 보안의 3대 요소 중 적절한 권한을 가진 사용자가 인가한 방법으로만 정보를 변경할 수 있도록 하는 것은?

- ① 무결성(integrity)
- ② 기밀성(confidentiality)
- ③ 가용성(availability)
- ④ 접근성(accessability)

문 2. 스트림 암호에 대한 설명으로 옳지 않은 것은?

- ① 데이터의 흐름을 순차적으로 처리해 가는 암호 알고리즘이다.
- ② 이진화된 평문 스트림과 이진 키스트림 수열의 XOR 연산으로 암호문을 생성하는 방식이다.
- ③ 스트림 암호 알고리즘으로 RC5가 널리 사용된다.
- ④ 구현이 용이하고 속도가 빠르다는 장점이 있다.

문 3. DES(Data Encryption Standard)에 대한 설명으로 옳지 않은 것은?

- ① 1977년에 미국 표준 블록 암호 알고리즘으로 채택되었다.
- ② 64비트 평문 블록을 64비트 암호문으로 암호화한다.
- ③ 페이스텔 구조(Feistel structure)로 구성된다.
- ④ 내부적으로 라운드(round)라는 암호화 단계를 10번 반복해서 수행한다.

문 4. 다음 (가) ~ (다)에 해당하는 악성코드를 옳게 짝 지은 것은?

(가) 사용자의 문서와 사진 등을 암호화시켜 일정 시간 안에 일정 금액을 지불하면 암호를 풀어주는 방식으로 사용자에게 금전적인 요구를 하는 악성코드

(나) 운영체제나 특정 프로그램의 취약점을 이용하여 공격하는 악성코드

(다) 외부에서 파일을 내려받는 다운로드와 달리 내부 데이터로부터 새로운 파일을 생성하여 공격을 수행하는 악성코드

(가) (나) (다)

- ① 트로퍼 익스플로잇 랜섬웨어
- ② 트로퍼 랜섬웨어 익스플로잇
- ③ 랜섬웨어 익스플로잇 트로퍼
- ④ 랜섬웨어 트로퍼 익스플로잇

문 5. ISO 27001의 정보보호영역(통제분야)에 해당하지 않은 것은?

- ① 소프트웨어 품질 보증(Software Quality Assurance)
- ② 접근통제(Access Control)
- ③ 암호화(Cryptography)
- ④ 정보보안 사고관리(Information Security Incident Management)

문 6. 암호화 알고리즘과 복호화 알고리즘에서 각각 다른 키를 사용하는 것은?

- ① SEED
- ② ECC
- ③ AES
- ④ IDEA

문 7. DoS(Denial of Service)의 공격유형이 아닌 것은?

- ① Race Condition
- ② TearDrop
- ③ SYN Flooding
- ④ Land Attack

문 8. 다음에서 설명하는 방화벽 구축 형태는?

- 배스천(Bastion) 호스트와 스크린 라우터를 혼합하여 사용한 방화벽
- 외부 네트워크와 내부 네트워크 사이에 스크린 라우터를 설치하고 스크린 라우터와 내부 네트워크 사이에 배스천 호스트를 설치

- ① Bastion Host
- ② Dual Homed Gateway
- ③ Screened Subnet Gateway
- ④ Screened Host Gateway

문 9. 다음에서 설명하는 보안 기술은?

- 해시 함수를 이용하여 메시지 인증 코드를 구현한다.
- SHA-256을 사용할 수 있다.

- ① HMAC(Hash based Message Authentication Code)
- ② Block Chain
- ③ RSA(Rivest-Shamir-Adleman)
- ④ ARIA(Academy, Research Institute, Agency)

문 10. 스미싱 공격에 대한 설명으로 옳지 않은 것은?

- ① 공격자는 주로 앱을 사용하여 공격한다.
- ② 스미싱은 개인 정보를 빼내는 사기 수법이다.
- ③ 공격자는 사용자가 제대로 된 url을 입력하여도 원래 사이트와 유사한 위장 사이트로 접속시킨다.
- ④ 공격자는 문자 메시지 링크를 이용한다.

- 문 11. 디지털 포렌식을 통해 획득한 증거가 법적인 효력을 갖기 위해 만족해야 할 원칙이 아닌 것은?
- ① 정당성의 원칙
 - ② 재현의 원칙
 - ③ 무결성의 원칙
 - ④ 기밀성의 원칙
- 문 12. 「개인정보 보호법」상의 개인정보에 대한 설명으로 옳지 않은 것은?
- ① 개인정보 보호위원회의 위원 임기는 3년이다.
 - ② 개인정보는 가명처리를 할 수 없다.
 - ③ 개인정보 보호위원회의 위원은 대통령이 임명 또는 위촉한다.
 - ④ 개인정보처리자는 개인정보파일의 운용을 위하여 다른 사람을 통하여 개인정보를 처리할 수 있다.
- 문 13. DoS 및 DDoS 공격 대응책으로 옳지 않은 것은?
- ① 방화벽 및 침입 탐지 시스템 설치와 운영
 - ② 시스템 패치
 - ③ 암호화
 - ④ 안정적인 네트워크 설계
- 문 14. 국제 공통 평가기준(Common Criteria)에 대한 설명으로 옳지 않은 것은?
- ① CC는 국제적으로 평가 결과를 상호 인정한다.
 - ② CC는 보안기능수준에 따라 평가 등급이 구분된다.
 - ③ 보안목표명세서는 평가 대상에 해당하는 정보보호 시스템의 보안 요구 사항, 보안 기능 명세 등을 서술한 문서이다.
 - ④ 보호프로파일은 보안 문제를 해결하기 위해 작성한 제품군별 구현에 독립적인 보안요구사항 등을 서술한 문서이다.
- 문 15. 생체인증(Biometrics)에 대한 설명으로 옳지 않은 것은?
- ① 생체 인증은 불변의 신체적 특성을 활용한다.
 - ② 생체 인증은 지문, 홍채, 망막, 정맥 등의 특징을 활용한다.
 - ③ 얼굴은 행동적 특성을 이용한 인증 수단이다.
 - ④ 부정허용률(false acceptance rate)은 인증되지 않아야 할 사람을 인증한 값이다.
- 문 16. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제45조의3 (정보보호 최고책임자의 지정 등)에 따른 정보보호 최고책임자의 업무가 아닌 것은?
- ① 정보보호 사전 보안성 검토
 - ② 정보보호 취약점 분석·평가 및 개선
 - ③ 중요 정보의 암호화 및 보안서버 적합성 검토
 - ④ 정보통신시설을 안정적으로 운영하기 위하여 대통령령으로 정하는 바에 따른 보호조치

- 문 17. 정보보호 및 개인정보보호 관리체계 인증에 대한 설명으로 옳은 것은?

- ① 인증기관 지정의 유효기간은 2년이다.
- ② 사후심사는 인증 후 매년 사후관리를 위해 실시된다.
- ③ 인증심사 기준은 12개 분야 92개 통제 사항이다.
- ④ 인증심사원은 2개 등급으로 구분된다.

- 문 18. PGP(Pretty Good Privacy)에 대한 설명으로 옳지 않은 것은?

- ① RSA를 이용하여 메시지 다이제스트를 서명한다.
- ② 세션 키는 여러 번 사용된다.
- ③ 수신자는 자신의 개인키를 이용하여 세션 키를 복호화한다.
- ④ 세션 키를 이용하여 메시지를 암호·복호화한다.

- 문 19. 다음에서 설명하는 블록암호 운영 모드는?

- 단순한 모드로 평문이 한 번에 하나의 평문 블록으로 처리된다.
- 각 평문 블록은 동일한 키로 암호화된다.
- 주어진 하나의 키에 대하여 평문의 모든 블록에 대한 유일한 암호문이 존재한다.

- ① CBC(Cipher Block Chaining Mode)
- ② CTR(Counter Mode)
- ③ CFB(Cipher-Feed Back Mode)
- ④ ECB(Electronic Code Book Mode)

- 문 20. BCP(Business Continuity Planning)에 대한 설명으로 옳지 않은 것은?

- ① BCP는 사업의 연속성을 유지하기 위한 업무지속성 계획과 절차이다.
- ② BCP는 비상시에 프로세스의 운영 재개에 필요한 조치를 정의한다.
- ③ BIA는 조직의 필요성에 의거하여 시스템의 중요성을 식별한다.
- ④ DRP(Disaster Recovery Plan)는 최대허용중단시간(Maximum Tolerable Downtime)을 산정한다.