2019년 경찰간부 정보보호론

-2019년 10월 5일 시행

☑ 만든이 : 지안에듀 조현준

- 성균관대학교 정보공학 전공
- CISA, CISSP, 정보보안기사

☑ 저서

- TopSpot 정보보호론 이론편/문제편
- 알기쉬운 정보보안기사 필기편/실기편(알기사)
- TopSpot 자료구조론 이론편/쪽집게 기출문제

☑ 무료 동영상 안내

- 지안에듀 홈페이지 이용(www.zianedu.com)
  - [빅데이터 3.2] 조현준 정보보호론 연도별 기출문제 풀이강의(전산 전직렬)
- 유튜브 자투리10분 기출20문항정리
  - 유튜브에서 조현준 정보보호론 검색

1. ○△× 19.경간부

정보보호의 3대 목표 중 가용성(Availability)을 위협하는 행위로 옳은 것은 무엇인가?

① 데이터 변조(Modification)
② 서비스 거부(Denial of Service)
③ 신분 위장(Masquerading)
④ 트래픽 분석(Traffic Analysis)

오답피하기 ② 데이터 변조(Modification), 신분 위장(Masquerading)은 무결성에 대한 위협 행위이고, 트래픽 분석(Traffic Analysis)은 기밀성에 대한 위협 행위이다.

정답 ②

2. ○△× 19.경간부

다음 중 수동적 공격(Passive Attack)으로 가장 옳은 것은 무엇인가?

① 분산 서비스 거부(Distributed Denial of Service)
② 세션 하이재킹(Session Hijacking)
③ 스머프 공격(Smurf Attack)
④ 스니핑(Sniffing)

◦ TCP 세션 하이재킹이 스니핑과 다른 점은 명령의 실행이 가능하다는 것이다. 클라이언트와 똑같은 인터페이스가 제공된다. 따라서 TCP 세션 하이재킹을 적극적인(active) 공격이라고 한다.

오답피하기 ④ 분산 서비스 거부(Distributed Denial of Service), 세션 하이재킹(Session Hijacking), 스머프 공격(Smurf Attack)은 적극적 공격이고 스니핑(Sniffing)은 소극적 공격이다.

정답 ④

3. ○△× 19.경간부

다음 설명 중 가장 옳은 것은 무엇인가?

① RC5 암호 알고리즘은 64비트의 고정된 키 길이를 사용한다.
② 3중 DES(Triple DES) 암호 알고리즘은 DES 암호 알고리즘을 개선한 것으로 DES에 비해 처리 속도가 3배 정도 빠르다.
③ IDEA 암호 알고리즘은 16라운드의 암호 방식을 적용하며, 암호화와 복호화에 사용되는 알고리즘이 달라 암호화 강도가 높다.
④ ARIA 암호 알고리즘에 사용되는 키와 블록의 길이는 AES와 동일하다.

◦ ARIA와 AES는 블록의 길이가 128비트로 동일하고, 키는 128비트, 192비트, 256비트의 3종류 키를 사용한다는 면에서는 동일하다. 하지만 라운드 수는 차이가 있다.

오답피하기 ① RC5(Ron's Code 5)는 입출력, 키, 라운드 수가 가변인 블록 알고리즘이다. ② DES가 3DES에 비해 2.5배 정도 빠르다. ③ IDEA는 블록 암호 알고리즘으로써 64비트의 평문에 대하여 동작하며, 키의 길이는 128비트이고, 8라운드의 암호 방식을 적용한다. 또한 암호화와 복호화에 동일한 알고리즘이 사용된다.

정답 ④

4. ○△× 19.경간부

다음 설명 중 가장 옳지 않은 것은 무엇인가?

① 5명이 서로 통신할 경우 대칭키 암호 알고리즘과 공개키 암호 알고리즘에서 필요한 키의 개수가 다르다.
② 일반적으로 대칭키 암호 알고리즘이 공개키 암호 알고리즘보다 암호화 속도가 빠르다.
③ 공개키 암호 알고리즘의 종류로는 RSA, ECC, DSA 등이 있다.
④ 공개키 암호 알고리즘은 인증과 부인 방지를 제공한다.

◦ n명의 사람이 자신 외의 사람과 통신하고 싶을 경우 필요한 대칭키 알고리즘에서 키의 수는 $\frac{n(n-1)}{2}$이고, 공개키 알고리즘에서 키의 수는 $2n$이다.

오답피하기 ① 5명이 서로 통신할 경우 대칭키 암호 알고리즘과 공개키 암호 알고리즘에서 필요한 키의 개수는 10개로 동일하다.

정답 ①

5. ○△× 19.경간부

SPN 구조와 Feistel 구조에 대한 설명 중 가장 옳은 것은 무엇인가?

① SPN 구조는 암호화와 복호화 과정이 동일하여 처리 속도가 빠르다.
② SPN 구조의 종류에는 AES, SEED, BLOWFISH 등이 있다.
③ Feistel 구조의 암호 강도를 결정짓는 요소는 평문 블록의 길이, 키의 길이, 라운드의 수이다.
④ Feistel 구조는 역변환 함수에 제약이 있으며, S-BOX와 P-BOX를 사용한다.

◦ Feistel구조는 3라운드 이상이며 짝수 라운드로 구성된다. 이러한 Feistel 구조는 라운드 함수와 관계없이 역변환이 가능하며, 두 번의 수행으로 블록간의 완전한 확산(diffusion)이 이루어진다. 알고리즘의 수행속도가 빠르고, 하드웨어 및 소프트웨어구현이 용이하고, 아직 구조상에 문제점이 발견되고 있지 않다는 장점을 지니고 있다.
◦ SPN 구조는 라운드 함수가 역변환이 되어야 한다는 제약이 있지만 더 많은 병렬성(parallelism)을 제공하기 때문에 암·복호화 알고리즘의 고속화를 요구하며, 컴퓨터 프로세서(CPU)가 더 많은 병렬성을 지원하게 된 현 추세에 부응하는 방식이라 할 수 있다.

오답피하기 ① SPN 구조는 암호화와 복호화 과정이 다르다. ② AES, SEED, BLOWFISH는 Feistel 구조이다. ④ SPN 구조의 특징이다.

정답 ③

6. ○△× 19.경간부

블록 암호 운영모드 중 OFB(Output FeedBack) 모드에 대한 설명으로 가장 옳지 않은 것은 무엇인가?

① 암호기의 출력과 평문 블록을 XOR 연산하여 암호문 블록을 생성한다.
② 암호문 블록 전송 도중 오류가 발생하더라도 다음 블록의 비트에 영향을 미치지 않는다.
③ CBC(Cipher Block Chaining) 모드나 CFB(Cipher FeedBack) 모드와 마찬가지로 초기화 벡터(IV)를 사용한다.
④ 암호화와 복호화의 구조가 다르고 병렬 처리가 가능하다.

◘ OFB 모드 특징
◦ 초기치가 바뀌면 암호문은 모두 바뀐다.
◦ 암호 알고리즘의 출력은 평문과 무관하다.
◦ 전송 중의 비트 오류가 전파되지 않는다.(C_1에 비트 오류가 발생했다면, 복원된 P_1의 값에만 영향을 미치며, 이후의 복원된 평문에는 아무런 영향도 주지 않는다.)
◦ 암호문 C_i에서 비트 손실이 발생하면 그 다음에 오는 평문은 모두 에러가 발생하기 때문에 동기를 새로 맞추어야 한다.

오답피하기 ④ OFB 모드는 암호화와 복호화의 구조가 동일하다. OFB 모드는 병렬 처리가 불가능하다는 단점을 가지고 있다.

정답 ④

7. ○△× 19.경간부

해시함수에 대한 설명 중 가장 옳지 않은 것은 무엇인가?

① 일방향 해시함수의 경우 입력되는 메시지의 길이가 다르더라도 출력되는 해시 값의 길이는 같다.
② 해시함수의 보안 요구사항 중 강한 충돌 내성은 같은 해시 값을 갖는 두 개의 다른 입력 값을 발견하는 것이 계산상 불가능해야 하는 것을 의미한다.
③ SHA-256의 블록 길이와 출력되는 해시 값의 길이는 256비트로 동일하다.
④ 해시함수에 대한 공격 중 하나인 생일 공격(Birthday

Attack)은 일방향 해시함수의 강한 충돌 내성을 깨고자 하는 공격이다.

◦ 무차별 공격은 일방향 해시함수의 「약한 충돌 내성」을 깨고자 하는 공격이고, 생일 공격(birthday attack)은 일방향 해시함수의 「강한 충돌 내성」을 깨고자 하는 공격이다.

오답피하기 ③ SHA-256은 512비트 블록 길이와 256비트 해시값을 갖는다.

정답 ③

8. ○△× 19.경간부

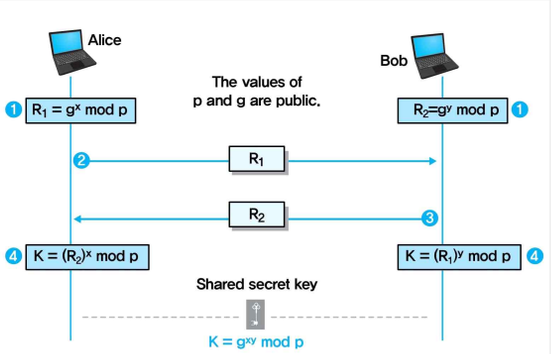
다음은 A와 B가 디피-헬만(Diffie-Hellman) 키 교환 알고리즘을 이용하여 서로 공유할 키를 생성하는 절차에 대한 설명이다. ㉠~㉢에 들어갈 내용으로 올바른 것은?

보기

(1) A는 소수 p와 p의 원시근 g를 선택하여 사전에 B와 공유한다.
(2) A는 p보다 작은 양수 a를 선택하여 K_A=(㉠)를 계산한다.
(3) B도 p보다 작은 양수 b를 선택하여 K_B=(㉡)를 계산한다.
(4) A와 B가 서로 K_A와 K_B를 공유한다.
(5) A가 $K_B^a \bmod p$, B가 $K_A^b \bmod p$를 계산하여 서로 (㉢)라는 공통의 키를 공유하게 된다.

① ㉠: $g^a \bmod p$ ㉡: $g^b \bmod p$ ㉢: $p^{ab} \bmod g$
② ㉠: $g^a \bmod p$ ㉡: $g^b \bmod p$ ㉢: $g^{ab} \bmod p$
③ ㉠: $p^a \bmod g$ ㉡: $p^b \bmod g$ ㉢: $p^{ab} \bmod g$
④ ㉠: $p^a \bmod g$ ㉡: $p^b \bmod g$ ㉢: $g^{ab} \bmod p$

Diffie-Hellman 방법



오답피하기 ② 소수 p와 p의 원시근 g에 대하여 사용자 A는 p보다 작은 양수 a를 선택하고 $g^a \bmod p$를 계산하여 B에게 전달한다. 마찬가지로 사용자 B는 p보다 작은 양수 b를 선택하고, $g^b \bmod p$를 계산하여 A에게 전달한다. 그러면 A와 B는 $g^{ab} \bmod p$를 공유하게 된다.

정답 ②

9. ○△× 19.경간부

전자 서명의 특성에 대한 설명 중 가장 옳지 않은 것은 무엇인가?

① 위조 불가(Unforgeable) : 합법적인 서명자 이외의 다른 사람이 전자 문서에 대한 전자 서명을 생성할 수 없어야 한다.
② 변경 불가(Unalterable) : 서명한 문서의 내용을 변경할 수 없어야 한다.
③ 재사용 불가(Not Reusable) : 전자 문서의 서명은 다른 전자 문서의 서명으로 사용할 수 없어야 한다.
④ 부인 방지(Non-Repudiation) : 누구든지 전자 서명의 서명자를 검증할 수 있어야 한다.

◦ 서명자 인증(User authentication): 전자서명의 서명자를 누구든지 검증할 수 있어야 한다.
◦ 부인방지(Non-repudiation): 서명자는 서명행위 이후에 서명한 사실을 부인할 수 없어야 한다.

오답피하기 ④ 서명자 인증에 대한 설명이다.

정답 ④

10. ○△× 19.경간부

다음 공개키 기반 구조(Public Key Infrastructure)에 대한 설명 중 가장 옳은 것은 무엇인가?

① 공개키 기반 구조는 대칭키 암호시스템에 기초하여 디지털 인증서를 생성하고 관리하는데 필요한 정책 및 절차이다.
② 정책 인증 기관(Policy Certification Authority)은 공개키 기반 구조 전반에 사용되는 정책과 절차를 수립하는 기관이다.
③ 등록 기관(Registration Authority)은 공개키 기반 구조의 필수 구성요소로서 사용자의 신분과 소속을 확인하고 사용자에게 공개키 인증서를 발행하는 기능을 수행한다.
④ 인증서에는 버전, 일련번호, 유효기간 등의 정보가 담겨 있다.

오답피하기 ① 공개키 기반 구조는 공개키 암호시스템에 기초하여 디지털 인증서를 생성하고 관리하는데 필요한 정책 및 절차이다. ② 정책 승인 기관(PAA, Policy Approving Authority)에 대한 설명이다. ③ RA는 선택적인(optional) 요소이다. RA가 없을 때에 인증기관은 RA의 기능을 수행할 수 있다고 가정한다.

정답 ④

11. ○△× 19.경간부

다음 중 강제적 접근 제어(MAC : Mandatory Access Control)에 대한 설명으로 옳은 것은 모두 몇 개인가?

보기

가. 유닉스(UNIX) 운영체제의 기본 접근제어 방식에 적용되었다.
나. 최초 객체에 설정된 강제적 접근 제어 관계는 복사된 객체에도 그대로 적용된다.
다. 부여된 역할에 기반하여 접근이 제어되므로 주로 군사용으로 사용된다.
라. 강제적 접근 제어의 대표적인 구현 형태는 ACL(Active Control List)이다.

① 0개 ② 1개
③ 2개 ④ 3개

MAC의 특징
- MAC정책은 객체의 소유자가 변경할 수 없는 주체들과 객체들 간의 접근통제관계를 정의한다.
- 한 주체가 한 객체를 읽고 그 내용을 다른 객체에게 복사하는 경우에 원래의 객체에 내포된 MAC 제약사항이 복사된 객체에 전파(propagate)된다.
- MAC 정책은 모든 주체 및 객체에 대하여 일정하며, 어느 하나의 주체/객체 단위로 접근 제한을 설정 할 수 없다.

DAC의 특징
- DAC 정책은 허가된 주체(즉, 객체의 소유자)에 의하여 변경 가능한 하나의 주체와 객체간의 관계를 정의한다.
- 한 주체가 어느 한 객체를 읽고 그 내용을 다른 어느 한 객체로 복사하는 경우에 처음의 객체에 내포된 접근통제정보가 복사된 객체로 전파(propagate)되지 않는다.
- DAC정책은 모든 주체 및 객체들 간에 일정하지 않고 하나의 주체/객체 단위로 접근 제한을 설정할 수 있다. 즉, 비록 DAC이 어느 한 주체로 하여금 특정 비밀등급의 한 객체를 접근하지 못하게 할지라도, 그 주체는 다른 주체가 그러한 비밀등급을 갖는 다른 객체들을 접근하는 것을 방지할 수 없다.

오답피하기 ② 가. 유닉스(UNIX) 운영체제의 기본 접근제어 방식에 적용되는 것은 DAC이다. 다. 부여된 역할에 기반하여 접근 제어하는 것은 RBAC이다. 라. DAC의 대표적인 구현 형태는 ACL이다.

정답 ②

12. ○△× 19.경간부

다음 중 커버로스(Kerberos) 인증 프로토콜에 대한 설명으로 옳은 것은 모두 몇 개인가?

보기

가. 커버로스는 개방형 분산 통신망에서 클라이언트와 서버 간의 상호 인증을 지원하는 인증 프로토콜이다.
나. 커버로스를 통해 데이터의 기밀성과 무결성을 보장할 수 있다.
다. 커버로스는 타임 스탬프(Time Stamp)를 이용하므로 다른 사람이 티켓을 복사하여 재사용하는 것을 방지할 수 있다.
라. 커버로스는 세사미(SESAME)의 기능을 확장하고 약점을 보완하기 위해 개발된 것이다.

① 1개 ② 2개
③ 3개 ④ 4개

오답피하기 ③ 라. SESAME(Secure European System for Application in a Multi-vendor Environment) 프로젝트는 Kerberos의 기능을 확장하고 약점을 보완하기 위해 개발된 싱글 사인온 기술이다. SESAME는 대칭 및 비대칭 암호화 기법을 사용하여 인증서비스를 제공한다.

정답 ③

13. ○△× 19.경간부

일회용 패스워드(One Time Password)의 생성 및 인증 방식 중 시간 동기화 방식에 대한 설명으로 가장 옳지 않은 것은 무엇인가?

① OTP 생성 매체와 인증 서버의 시간 정보가 동기화되어 있어야 한다.
② 일정 시간 이상 인증을 받지 못하면 새로운 비밀번호 생성 시까지 기다려야 하는 문제점이 있다.
③ 질의응답 방식보다 사용은 간편하지만, 호환성이 낮다.
④ RSA사에서 만든 Secure ID가 대표적이다.

오답피하기 ③ 시간동기화 방식의 장점은 질의값 입력이 없어 질의 응답 방식보다 사용이 간편하다는 것이다. 또한 질의응답 방식에 비해 호환성이 높다.

정답 ③

14. ○△× 19.경간부

버퍼 오버플로우(Buffer Overflow) 공격에 대응하는 방법으로 가장 옳지 않은 것은 무엇인가?

① 버퍼 오버플로우 공격에 대응하기 위해 변수 타입과 그 타입에 허용되는 연산들에 대해 강력한 표기법을 제공하는 고급 수준의 프로그래밍 언어를 사용한다.
② gets(), scanf(), strcat() 함수 사용을 자제하고 fgets(), fscanf(), strcpy() 함수 사용을 권장한다.

③ 스택 배치를 랜덤하게 설정하고 프로그램 실행 시마다 다른 주소에 배치한다.
④ 스택상에 있는 공격자의 코드가 실행되지 못하도록 한다.

오답피하기 ② gets(), scanf(), strcat(), strcpy() 함수 사용을 자제하고 fgets(), fscanf() 함수 사용을 권장한다.(strncpy() 함수는 권장됨)

정답 ②

15. ○△× 19.경간부

유닉스(Unix) 운영체제에서 명령어 'chmod 752 test.c'를 실행한 파일의 접근 권한에 대한 설명으로 가장 옳은 것은 무엇인가?

① group 권한: 읽기(X) 쓰기(O) 실행(X)
② user 권한: 읽기(O) 쓰기(O) 실행(O)
③ group 권한: 읽기(O) 쓰기(O) 실행(O)
④ user 권한: 읽기(O) 쓰기(X) 실행(O)

오답피하기 ② 숫자로 기술된 접근권한 752를 기호로 기술하면 rwxr-x-w-이 된다. 즉 user는 읽고, 쓰고, 실행이 가능하고, group은 읽고, 실행이 가능하고, other는 쓰기가 가능하다.

정답 ②

16. ○△× 19.경간부

다음에서 설명하는 윈도우 인증의 구성 요소로 가장 옳은 것은 무엇인가?

보기
- 사용자의 계정과 패스워드가 일치하는 사용자에게 고유의 SID(Security Identifier)를 부여한다.
- SID에 기반을 두어 파일이나 디렉터리에 대한 접근의 허용 여부를 결정하고 이에 대한 감사 메시지를 생성한다.

① LSA(Local Security Authority)
② SRM(Security Reference Monitor)
③ SAM(Security Account Manager)
④ SSH(Secure Shell)

◦ SRM은 커널 모드에서 수행되며, 사용자나 프로세스가 어떤 객체를 열려고 시도하면 접근 권한을 확인한다.

오답피하기 ② SAM이 사용자의 계정과 패스워드의 일치 여부를 확인하여 SRM에 알리면, SRM은 사용자에게 SID(Security Identifier)를 부여한다. 또한 SRM은 SID에 기반하여 파일이나 디렉터리에 대한 접근(access)을 허용할지를 결정하고, 이에 대한 감사 메시지를 생성한다.

정답 ②

17. ○△× 19.경간부

유닉스(Unix)와 관련된 설명 중 가장 옳지 않은 것은 무엇인가?

① /etc 디렉터리에는 시스템의 환경 설정 및 주요 설정 파일이 있다.
② pacct는 시스템에 로그인한 모든 사용자가 로그아웃할 때까지 수행한 프로그램 정보와 관련된 로그 파일이다.
③ 파일시스템의 i-Node는 파일의 유형, 파일 수정 시각, 파일의 이름 등의 정보를 가지고 있다.
④ SetUID가 설정된 파일은 실행되는 동안 파일 소유자의 권한으로 실행된다.

오답피하기 ③ 유닉스 파일시스템의 i-Node에는 파일 이름의 정보를 가지고 있지 않다.

정답 ③

18. ○△× 19.경간부

방화벽(Firewall)에 대한 다음 설명 중 옳지 않은 것은 모두 몇 개인가?

보기
가. 패킷 필터링(Packet Filtering) 방화벽은 패킷을 조사하여 허용 여부를 결정하면 되므로 동작 방식이 간단하여 구현하기 쉽다.
나. 스테이트풀 패킷 검사(Stateful Packet Inspection) 방화벽은 종단-대-종단 TCP 연결을 허용하지 않고, 두 개의 TCP 연결을 설정한다.
다. 회로 레벨 프록시(Circuit Level Proxy) 방화벽은 TCP 순서번호를 추적하므로 순서번호를 이용한 세션 하이재킹과 같은 공격을 막을 수 있다.
라. 애플리케이션 게이트웨이(Application Gateway) 방화벽은 프록시 서버를 통해 외부 네트워크와의 직접적인 연결을 피할 수 있다.

① 1개 ② 2개
③ 3개 ④ 4개

오답피하기 ② 나. 회선 수준 프락시 방화벽은 종단-대-종단 TCP 연결을 허용하지 않고, 두 개의 TCP 연결을 설정한다. 다. 상태 추적 방화벽은 TCP 순서번호를 추적하므로 순서번호를 이용한 세션 하이재킹과 같은 공격을 막을 수 있다.

정답 ②

19. ○△× 19.경간부

침입탐지시스템(IDS)에 대한 설명으로 가장 옳은 것은 무엇인가?

① 침입 경로를 찾을 수 있도록 탐지대상으로부터 생성되는 로그를 제공한다.
② Host-IDS는 운영체제에 독립적이다.
③ 오용 침입탐지 기법은 오탐률(False Positive)이 높다.
④ '침입분석 및 탐지 → 데이터수집 → 데이터 가공 및 축약 → 보고 및 대응'의 단계로 실행된다.

오답피하기 ② Host-IDS는 운영체제에 종속적이다. ③ 오용 침입탐지 기법은 오탐률(False Positive)이 낮다. ④ '데이터수집 → 데이터 가공 및 축약 → 침입분석 및 탐지 → 보고 및 대응'의 단계로 실행된다.

정답 ①

20. ○△× 19.경간부

가상사설망(VPN)에 대한 설명으로 가장 옳지 않은 것은 무엇인가?

① 공중 네트워크를 이용하여 사설 네트워크와 같은 효과를 제공한다.
② VPN에 사용되는 터널링(Tunneling)은 터미널이 형성되는 양 호스트 사이에 전송되는 패킷을 추가 헤더 값으로 인캡슐화 하는 기술이다.
③ L2F(Layer2 Forwarding)는 PPTP(Point-to-Point Tunneling Protocol)와 L2TP(Layer2 Tunneling Protocol)를 결합한 방식이다.
④ VPN은 데이터 암호화, 접근제어 등의 보안 서비스를 제공한다.

오답피하기 ③ L2TP(Layer2 Tunneling Protocol)는 시스코사에서 개발한 L2F(Layer2 Forwarding)와 MS사에서 개발한 PPTP(Point-to-Point Tunneling Protocol)를 결합한 방식이다.

정답 ③

21. ○△× 19.경간부

다음에서 설명하는 시스템으로 가장 옳은 것은 무엇인가?

보기

· 서로 다른 보안장비에서 발생한 로그를 하나의 화면에서 모니터링 할 수 있는 통합 관리 시스템
· 보안 정책 통합 관리와 적용을 통한 보안 운영 관리의 일관성 제공

① NAC(Network Access Control)
② PMS(Patch Management System)
③ BCM(Business Continuity Management)
④ ESM(Enterprise Security Management)

◦ 패치관리 시스템(PMS, Patch Management System): 시스템의 보안 취약점을 보완하기 위해 배포되는 보안 패치 파일을 원격에서 자동으로 설치, 관리해 주는 시스템. 보안 패치의 미설치로 인해 발생할 수 있는 각종 피해를 예방하기 위해 패치 설치를 권고하여 설치를 유도하거나, 필요시 강제적으로 설치할 수 있도록 관리해 주는 시스템이다. 웜 · 바이러스 등 사이버 위협에 대한 효과적인 해결책의 하나로 제시되어 공공기관을 중심으로 도입이 확산되고 있다.

오답피하기 ④ ESM(Enterprise Security Management)은 기업과 기관의 보안 정책을 반영, 다양한 보안 시스템을 관제 · 운영 · 관리함으로써 조직의 보안 목적을 효율적으로 실현하는 시스템이다.

정답 ④

22. ○△× 19.경간부

다음에서 설명하는 블루투스(Bluetooth)의 보안 취약점으로 가장 적절하게 연결된 것은?

보기

㉠: 다른 데이터의 이동이나 변조를 가하는 것이 아니기에 사용자를 귀찮게 하는 문제 외에는 별다른 위험이 없다.
㉡: 블루투스 장치끼리 인증 없이 정보를 간편하게 교환하기 위해 개발된 OPP(OBEX Push Profile) 기능을 사용하여 블루투스 장치로부터 주소록 등의 내용을 요청해 이를 열람하는 등의 공격 방법이다.
㉢: 해커가 모바일 장치를 물리적으로 소유한 것처럼 다른 사람의 모바일 장치가 전화를 걸거나 다른 기능들을 수행하도록 할 수 있다.

	㉠	㉡	㉢
①	블루재킹	블루스나핑	블루버깅
②	블루재킹	블루버깅	블루프린팅
③	블루재킹	블루스나핑	블루프린팅
④	블루버깅	블루스나핑	블루프린팅

블루투스 공격

◦ 블루프린팅(Blueprinting): 블루투스 공격 장치의 검색 활동을 의미한다.
◦ 블루스나핑(bluesnarfing): 블루투스의 취약점을 이용하여 장비의 임의 파일에 접근하는 공격이다.
◦ 블루버깅(bluebugging): 블루투스 장비 간의 취약한 연결 관리를 악용한 공격이다. 공격 장치와 공격 대상 장치를 연결하여 공격 대상 장치에서 임의의 동작을 실행하는 공격이다.
◦ 블루재킹(bluejacking): 블루투스를 이용해 스팸처럼 명함을 익명으로 퍼트리는 것이다. 블루재킹은 다른 데이터의 이동이나 변조를 가하는 것이 아니며, 명함에는 주로 해커 메시지가 들어 있다.

오답피하기 ① 블루투스 공격 유형 중 블루재킹, 블루스나핑, 블루버깅에 대한 설명이다.

정답 ①

23. ○△× 19.경간부

무선 랜 보안과 관련한 설명으로 옳지 않은 것은 모두 몇 개인가?

보기

가. 무선 랜의 취약점을 보완하기 위해 IEEE 802.1x와 RADIUS(Remote Authentication Dial-In User Service) 서버를 이용해 무선 사용자를 인증한다.

나. WPA(Wifi Protected Access)는 WEP(Wired Equivalent Privacy) 암호의 약점을 보완한 CCMP(Counter mode with CBC-MAC Protocol) 암호화 방식을 사용한다.

다. WPA2는 보안 강화를 위해 RC4 대신 AES 알고리즘을 사용한다.

라. KRACK(Key Reinstallation Attacks)은 WPA2의 4-way 핸드셰이크(handshake) 과정에서 메시지를 조작하고 재전송하여 정보를 획득하는 공격이다.

① 0개 ② 1개
③ 2개 ④ 4개

◦ KRACK(Key Reinstallation AttaCK)은 Wi-Fi 클라이언트 디바이스가 보안이 설정된 Wi-Fi 네트워크에 접속할 때 수행하는 4-way 인증 handshake의 세 번째 단계를 대상으로 한다. 세 번째 단계에서 암호화 키는 여러 번 전송될 수 있는데, 만약 공격자가 이 전송 데이터를 특정한 방법으로 모아서 재생하면 Wi-Fi 보안 암호화가 깨질 수 있다.

오답피하기 ② 나. WPA는 WEP 암호의 약점을 보완한 TKIP 암호화 방식을 사용한다.

정답 ②

24. ○△× 19.경간부

네트워크 기반의 공격들과 이에 대한 보안 대책으로 가장 옳지 않은 것은 무엇인가?

① Land Attack - 패킷 필터링 도구를 이용하여 자신의 시스템 주소와 동일한 소스(Source) 주소를 가진 외부 패킷을 필터링 한다.

② ARP Spoofing - ARP 테이블을 ARP reply 메시지에 따라 동적(Dynamic)으로 관리하여 작성한다.

③ DNS Spoofing - 중요한 사이트에 대해서는 IP 주소를 확인해 hosts 파일에 등록해 둔다.

④ TCP Connection Hijacking - TCP 연결설정 과정에서 시작 순서번호(Initial Sequence Number)를 임의의 번호로 할당한다.

◦ 정적 ARP 테이블 대응 방법은 관리자가 직접 ARP 테이블을 작성할 수 있을 정도로 네트워크의 규모가 작은 경우에 적합하다. 그리고 리부팅하면 static 옵션이 사라지므로 계속 사용하려면 배치 파일 형태로 만들어 두고 리부팅 시마다 자동으로 수행되도록 설정해야 한다.

오답피하기 ② ARP 스푸핑 공격에 대한 대응은 동일 네트워크 내의 시스템들에 대한 ARP 캐시 테이블을 ARP reply 메시지와 관계없이 관리자가 직접 정적(static)으로 작성함으로써 ARP 스푸핑 공격이 성립하지 않게 만드는 것이다. 즉, 정적 ARP 테이블을 사용하는 시스템은 ARP reply 메시지를 무시한다.

정답 ②

25. ○△× 19.경간부

네트워크 스캐닝(Scanning)과 관련한 설명으로 가장 옳지 않은 것은 무엇인가?

① 대표적인 스캔 도구로 NMAP(Network Mapper)이 있다.

② 스텔스(Stealth) 스캔의 종류로 플래그(Flag) 값을 모두 설정하여 전송하는 Xmas 스캔과 플래그(Flag) 값을 모두 설정하지 않고 전송하는 NULL 스캔 등이 있다.

③ 스캔하고자 하는 포트를 대상으로 UDP 연결을 시도할 때, 아무런 응답이 없다면 해당 포트의 비활성화를 의미한다.

④ TCP Full Open 스캔은 신뢰성은 높지만, 속도가 느리고 로그가 남는다.

오답피하기 ③ UDP Scan은 ICMP Port Unreachable 에러 메시지가 수신되면 해당 포트의 비활성화를 의미하며, 아무런 응답이 없다면 해당 포트의 활성화를 의미한다.

정답 ③

26. ○△× 19.경간부

인터넷 프로토콜(IP)에 대한 설명으로 가장 옳지 않은 것은 무엇인가?

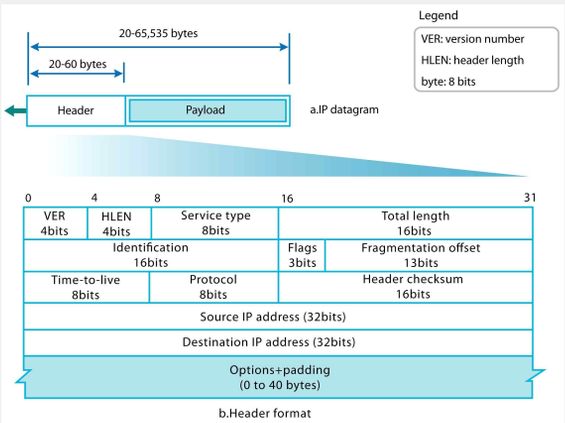
① 클래스 기반 주소 지정에서 처음 세 비트의 값이 '110'으로 시작하는 주소를 클래스 C주소라고 한다.

② IPv4의 데이터그램(Datagram)에서 첫 번째 필드는 선택사항(Option)을 포함한 헤더(header)의 길이 값이다.

③ IPv6에서는 헤더(header)가 40바이트로 고정되어 있어 헤더의 길이 필드가 불필요하다.

④ IPv6에서는 IPv4에서 사용하던 체크섬(Checksum) 필드가 삭제되었다.

IPv4 데이터그램



오답피하기 ② IPv4 데이터그램의 첫 번째 필드는 버전이다.

정답 ②

27. ○△× 19.경간부

FTP(File Transfer Protocol)의 보안 대책에 대한 설명으로 옳은 것을 모두 고른 것은?

보기

가. Bounce Attack을 예방하기 위해 20번 포트를 통한 명령은 제한한다.

나. TFTP가 필요한 경우, Secret Mode로 운영한다.

다. /etc/passwd 파일에서 Anonymous FTP에 불필요한 항목을 제거한다.

라. /etc/ftpusers에 등록된 사용자만이 FTP에 접근할 수 있으므로 root와 같은 중요 계정은 등록하지 않는다.

① 가, 다 ② 나, 라

③ 나, 다 ④ 다, 라

◦ FTP 바운스 공격은 Port 20번과 21번이 분리가 되어 있는 것을 이용하여, 명령채널을 통해 파일 전송을 요청한 클라이언트와 데이터 전송채널을 통해 실제 파일 전송을 받는 클라이언트가 분리될 수 있는 취약점이다. 최근 FTP 서버는 바운스 공격이 불가능 하도록 20번 포트를 통한 명령을 제한하고 있다 .

오답피하기 ① 나. TFTP가 필요한 경우, Secure Mode로 운영한다. 라. ftpusers 파일은 접속을 제한할 계정정보를 담고 있는 설정파일이다. 따라서 root 등 중요 계정을 ftpusers 파일에 명시하여 접속을 제한한다.

정답 ①

28. ○△× 19.경간부

전자우편 보안에 사용되는 기술들에 대한 설명으로 가장 옳지 않은 것은 무엇인가?

① PGP(Pretty Good Privacy)는 전자우편 메시지의 인증과 기밀성 제공을 위해 개발된 전자우편 보안의 표준안이다.

② S/MIME이 제공하는 보안 서비스에는 기밀성, 무결성, 송신 사실 부인방지, 사용자 인증 등이 있다.

③ S/MIME은 X.509 버전3 규정을 준수하여 공개키 인증서를 사용한다.

④ PEM(Privacy Enhanced Mail)은 분산화된 키 인증 방식을 통해 관리가 용이하여 대중적으로 사용되고 있다.

PEM(Privacy Enhanced Mail)

◦ 중앙집중화된 키 인증
◦ 인터넷 표준(안)
◦ 구현의 어려움
◦ 높은 보안성(군사용, 금융계 등)
◦ 이론 중심
◦ 많이 사용되지 않음

오답피하기 ④ PGP에 대한 설명이다.

정답 ④

29. ○△× 19.경간부

데이터베이스 보안 통제에 대한 설명 중 가장 옳지 않은 것은 무엇인가?

① 흐름통제 : 접근 가능한 객체 간의 정보 흐름을 통제하는 것으로 낮은 보안 등급에서 높은 보안 등급으로 정보 흐름 발생 시 기밀성이 위반되지 않도록 통제하는 것이다.

② 추론통제 : 간접적인 데이터 노출로부터 데이터를 보호하는 것으로 비밀 정보의 은폐, 데이터 위장 등의 방법으로 통제할 수 있다.

③ 접근통제 : 인증된 사용자에게 허가된 범위 내에서만 접근을 허용하여 내부의 정보에 대한 접근을 통제하는 것이다.

④ 뷰(View) : 기본 테이블로부터 유도되어 만들어지는 가상 테이블로 데이터의 논리적 독립성을 제공한다.

오답피하기 ① 임의의 객체에 포함되어 있는 정보가 명시적으로 혹은 암시적으로 보다 낮은 보호수준의 객체로 이동하는 것을 검사하여 접근가능한 객체 간의 정보흐름을 조정하는 것이 흐름제어이다.

정답 ①

30. ○△× 19.경간부

다음 웹 서비스 공격 기법에 대한 설명으로 바르게 짝지어진 것은?

보기

(가) 공격자가 게시판에 악성 스크립트를 저장하여 피해자가 해당 글을 읽을 경우 악성 스크립트가 실행되도록 하는 공격 기법

(나) 공격자가 입력 폼 및 URL 입력란에 SQL 문을 삽입하여 정보를 열람하거나 조작하는 공격 기법

(다) 공격자가 의도한 웹사이트 사용행위를 사용자 자신의 의도와는 무관하게 특정 웹사이트에 요청하게 만드는 공격 기법

	(가)	(나)	(다)
①	XSS	SQL Injection	XXE
②	XSS	SQL Injection	CSRF
③	XXE	SQL Injection	CSRF
④	XXE	CSRF	XSS

◦ XML External Entities(XXE): 오래되거나 설정이 미흡한 XML 프로세서는 XML 문서 내에서 외부 개체 참조(external entity references)를 평가한다. 외부 개체는 파일 URI 핸들러, 내부 파일 공유, 포트 검색, 원격 코드 실행 및 서비스 거부 공격을 사용하여 내부 파일을 노출시키는 데 사용될 수 있다.

오답피하기 ② XSS, SQL Injection, CSRF 공격에 대한 설명이다.

정답 ②

31. ○△× 19.경간부

블록체인(Block Chain)에 대한 설명으로 옳은 것은 모두 몇 개인가?

보기

가. 비트코인에서 최초로 구현되었다.

나. 블록체인의 한 블록에는 앞의 블록에 대한 정보가 포함되어 있다.

다. 블록체인 기술에서는 작업 증명이나 지분 증명 등과 같은 합의 알고리즘을 사용한다.

라. 제네시스 블록(Genesis block)은 블록체인의 가장 첫 번째 블록을 말한다.

① 1개 ② 2개

③ 3개 ④ 4개

◦ 비트코인은 2008년에 사토시 나카모토라는 정체불명의 인물이 발표한 논문에서 시작되었다. 비트코인은 P2P 네트워크 상에서 구현한 최초의 암호화폐이다. 또한, 블록체인 기술은 비트코인을 구현하기 위해 만들어졌기 때문에 블록체인과 비트코인은 동시에 탄생했다고 볼 수 있다.

◦ 제네시스 블록(Genesis Block)은 블록체인 네트워크의 시작을 상징하는 첫 번째 블록이다. 첫 번째 블록이 생성된 이후 다음 블록이 지속적으로 연결된다. 블록이 생성된 순서는 높이로 표현하며, 0번 블록은 네트워크가 최초에 시작될 때 만들어진 제네시스 블록이 된다.

오답피하기 ④ 보기는 블록체인에 대한 설명으로 반드시 모두 숙지해야 한다.

정답 ④

32. ○△× 19.경간부

디지털 포렌식의 기본 원칙 중 '무결성의 원칙'에 대한 설명으로 옳은 것은 무엇인가?

① 증거자료는 같은 환경에서 같은 결과가 나오도록 재현이 가능해야 한다.

② 컴퓨터 내부의 정보 획득은 신속하게 이루어져야 한다.

③ 증거가 획득되고 이송, 보관, 분석, 법정 제출 등의 과정이 명확해야 한다.

④ 획득된 정보는 위·변조되지 않았음을 입증할 수 있어야 한다.

오답피하기 ① 재현의 원칙, ② 신속성의 원칙, ③ 연계보관성의 원칙에 대한 설명이다.

정답 ④

33. ○△× 19.경간부

다음 중 ISO 27001:2013의 통제 항목에 해당하지 않는 것은 무엇인가?

① 정보보호 조직(Organization of information security)

② 운영 보안(Operations security)

③ 공급자 관계(Supplier relationship)

④ 모니터링과 검토(Monitoring and review)

➡ ISO 27001:2013 정보보호 통제 항목

요구사항	내용
정보보호 정책	정보보호에 대한 경영방침과 지원사항을 제공하기 위함
정보보호 조직	조직 내에서 보호를 효과적으로 관리하기 위해서는 보호에 대한 책임을 배정
인적 자원 보안	사람에 의한 실수, 절도, 부정수단이나 설비의 잘못사용으로 인한 위험을 감소
자산 관리	조직의 자산에 대한 적절한 보호책 유지
접근 통제	정보에 대한 접근통제를 하기 위함
암호화	기밀성, 인증 또는 정보의 무결성을 보호하기 위해 암호화의 적절하고 효과적인 사용을 보장
물리적 환경적 보안	비인가된 접근, 손상과 사업장 및 정보에 대한 영향을 방지하기 위함
운영 보안	정보 처리 설비의 정확하고 안전한 운영을 보장하기 위함
통신 보안	네트워크 및 지원 정보 처리 시설의 안전한 통신을 보장하기 위함
정보 시스템 개발 유지보수	정보시스템 내에 보안이 수립되었음을 보장하기 위함
공급자 관계	협력업체(공급자)에서 접근가능한 조직 내 정보보호를 보장과 협력업체와의 계약에 따라 정보 보안 및 서비스 제공에 합의된 수준을 유지하기 위함
정보보안 사고 관리	보안사고에 대한 대응 절차의 수립 및 이행을 보장함
정보보호 측면 업무 연속성 관리	사업활동에 방해요소를 완화시키며 주요 실패 및 재해의 영향으로부터 주요 사업 활동을 보호하기 위함
컴플라이언스	범죄 및 민사상의 법률, 법규, 규정 또는 계약 의무사항 및 보호요구사항의 불일치를 방지하기 위함

오답피하기 ④ 모니터링과 검토(monitoring and review)는 ISO 27001:2013 정보보호 통제 항목에 포함되지 않는다.

정답 ④

34. ○△× 19.경간부

위험이 존재하는 프로세스나 사업을 수행하지 않고 포기하는 정보보호의 위험처리 전략으로 가장 옳은 것은 무엇인가?

① 위험 회피 ② 위험 감소
③ 위험 전가 ④ 위험 수용

오답피하기 ① 위험 처리 전략 중 위험 회피(Risk Avoidance)는 위험이 존재하는 프로세스나 사업을 수행하지 않고 포기하는 것이다. 자산 매각이나 설계변경 등 다른 대안을 선택하여 해당 위험이 실현되지 않도록 하는 것이다. 이것은 보통 편리함이나 유용한 기능 수행 능력의 상실을 초래할 수 있다.

정답 ①

35. ○△× 19.경간부

다음에서 설명하는 사이버 위기 경보의 단계로 가장 옳은 것은 무엇인가?

보기

- 침해 사고가 다수 기관에서 발생했거나 대규모 피해로 발전될 가능성 증가
- 복수 정보통신서비스제공자(ISP)망/기간망의 장애 또는 마비

① 관심 ② 주의
③ 경계 ④ 심각

◘ 사이버 위기경보 단계

단계	정의
심각	• 국가적 차원에서 네트워크 및 정보시스템 사용 불가능 • 침해사고가 전국적으로 발생했거나 피해범위가 대규모인 사고 발생 • 시스템 자료 유출 사고 발생 • 국가적 차원에서 공동 대처 필요
경계	• 복수 정보통신서비스제공자(ISP)망·기간망의 장애 또는 마비 • 침해사고가 국지적으로 발생했거나 대규모 피해로 발전될 가능성 증가 • 다수 기관의 공조 대응 필요
주의	• 일부 네트워크 및 정보시스템 장애 • 침해사고가 일부 기관에서 발생했거나 다수기관으로 확산될 가능성 증가 • 국가 정보시스템 전반에 보안태세 강화 필요
관심	• 웜·바이러스, 해킹 등에 의한 피해발생 가능성 증가 • 해외 사이버공격 피해가 확산되어 국내 유입우려 • 사이버위협 징후 탐지활동 강화 필요

오답피하기 ③ 사이버 위기 경보 단계 중 경계 단계에 대한 설명이다.

정답 ③

36. ○△× 19.경간부

「개인정보보호법」에서 사용하는 용어의 뜻으로 가장 옳지 않은 것은 무엇인가?

① 개인정보 – 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.
② 정보주체 – 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.
③ 개인정보파일 – 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물을 말한다.
④ 개인정보처리자 – 개인정보취급자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 임직원, 파견근로자, 시간제근로자 등을 말한다.

◦ “개인정보처리자”란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.
◦ “개인정보 보호책임자”란 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지는 자로서 영 제32조제2항에 해당하는 자를 말한다.
◦ “개인정보취급자”란 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 임직원, 파견근로자, 시간제근로자 등을 말한다.

오답피하기 ④ 개인정보처리자는 개인정보취급자를 지휘·감독하며, 개인정보 보호책임자는 총괄 책임을 가진다.

정답 ④

37. ○△× 19.경간부

「개인정보보호법」 제25조 제1항 ‘누구든지 다음 각 호의 경우를 제외하고는 공개된 장소에 영상정보처리기기를 설치·운영하여서는 아니 된다.’의 각 호에 해당하지 않는 것은 모두 몇 개인가?

보기

가. 법령에서 구체적으로 허용하고 있는 경우
나. 범죄의 예방 및 수사를 위하여 필요한 경우
다. 시설안전 및 화재 예방을 위하여 필요한 경우
라. 교통단속을 위하여 필요한 경우
마. 교통정보의 수집·분석 및 제공을 위하여 필요한 경우

① 0개 ② 1개
③ 2개 ④ 3개

제25조(영상정보처리기기의 설치·운영 제한)
① 누구든지 다음 각 호의 경우를 제외하고는 공개된 장소에 영상정보처리기기를 설치·운영하여서는 아니 된다.
1. 법령에서 구체적으로 허용하고 있는 경우
2. 범죄의 예방 및 수사를 위하여 필요한 경우
3. 시설안전 및 화재 예방을 위하여 필요한 경우
4. 교통단속을 위하여 필요한 경우
5. 교통정보의 수집·분석 및 제공을 위하여 필요한 경우

오답피하기 ① 영상정보처리기기를 설치 가능한 경우로 반드시 숙지해야 한다.

정답 ①

38. ○△× 19.경간부

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 의한 형사 처벌 대상이 아닌 것은 무엇인가?

① 이용자의 동의를 받지 아니하고 개인정보를 수집하는 프로그램을 이용자의 컴퓨터나 그 밖에 대통령령으로 정하는 정보처리장치에 설치한 정보통신서비스 제공자
② 정보통신망에 의하여 처리·보관 또는 전송되는 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설한 자
③ 법정대리인의 동의를 받지 아니하거나 법정대리인이 동의하였는지를 확인하지 아니하고 만 14세 미만인 아동의 개인정보를 수집한 정보통신서비스 제공자
④ 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망에 침입한 자

제71조(벌칙)
① 다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.
1. 이용자의 동의를 받지 아니하고 개인정보를 수집한 자
2. 이용자의 동의를 받지 아니하고 개인의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보를 수집한 자
3. 개인정보를 이용하거나 제3자에게 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자
4. 이용자의 동의를 받지 아니하고 개인정보 처리위탁을 한 자
5. 이용자의 개인정보를 훼손·침해 또는 누설한 자
6. 개인정보가 누설된 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자
7. 필요한 조치를 하지 아니하고 개인정보를 제공하거나 이용한 자
8. 법정대리인의 동의를 받지 아니하거나 법정대리인이 동의하였는지를 확인하지 아니하고 만 14세 미만인 아동의 개인정보를 수집한 자
9. 정보통신망에 침입한 자
10. 정보통신망에 장애가 발생하게 한 자
11. 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설한 자

오답피하기 ① 3천만원 이하의 과태료에 해당되고, 나머지는 5년 이하의 징역 또는 5천만원 이하의 벌금에 해당된다.

정답 ①

39. ○△× 19.경간부

다음 빈칸에 들어갈 대상으로 옳은 것은 무엇인가?

보기

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」
제45조의3(정보보호 최고책임자의 지정 등)
① 정보통신서비스 제공자는 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 임원급의 정보보호 최고책임자를 지정하고 (　　)에게 신고하여야 한다. 다만, 자산총액, 매출액 등이 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우에는 정보보호 최고책임자를 지정하지 아니할 수 있다.

① 과학기술정보통신부장관
② 행정안전부장관
③ 국가정보원장
④ 한국인터넷진흥원장

제45조의3(정보보호 최고책임자의 지정 등)
① 정보통신서비스 제공자는 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 임원급의 정보보호 최고책임자를 지정하고 과학기술정보통신부장관에게 신고하여야 한다. 다만, 자산총액, 매출액 등이 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우에는 정보보호 최고책임자를 지정하지 아니할 수 있다.
② 제1항에 따른 신고의 방법 및 절차 등에 대해서는 대통령령으로 정한다.
③ 제1항 본문에 따라 지정 및 신고된 정보보호 최고책임자(자산총액, 매출액 등 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우로 한정한다)는 제4항의 업무 외의 다른 업무를 겸직할 수 없다.

오답피하기 ① 정보통신서비스 제공자는 임원급의 정보보호 최고책임자를 지정하고 과학기술정보통신부장관에게 신고하여야 한다.

정답 ①

40. ○△× 19.경간부

「정보통신기반 보호법」에 관한 설명으로 가장 옳지 않은 것은 무엇인가?

① 전자적 침해행위라 함은 정보통신기반시설을 대상으로 해킹, 컴퓨터바이러스, 논리 · 메일폭탄, 서비스거부 또는 고출력 전자기파 등으로 정보통신기반시설을 공격하는 행위를 말한다.
② 정보통신기반보호위원회의 위원은 위원장 1인을 포함한 25인 이내의 위원으로 구성한다.
③ 정보통신기반보호위원회는 주요정보통신기반시설 보호와 관련된 제도의 개선에 관한 사항 등을 심의한다.
④ 관리기관의 장은 대통령령이 정하는 바에 따라 정기적으로 소관 주요정보통신기반시설의 취약점을 분석 · 평가할 수 있다.

오답피하기 ④ 관리기관의 장은 대통령령이 정하는 바에 따라 정기적으로 소관 주요정보통신기반시설의 취약점을 분석 · 평가하여야 한다.(강행규정)

정답 ④

2020년 빅데이터 기반 합격 커리큘럼 [정보보호론]

전산개발, 정보보호직, 경찰간부

비전공자도 합격 전략 과목으로 만들수 있는 정보보호론!

※ 공무원 시험일정과 학원사정에 의해 변경될 수 있음.

구분		2019.09~2019.10	2019.11~2019.12	2020.01~2020.02	2020.03~2020.04	2020.05~2020.06	2020.07~2020.08
전산개발	이론 1.0	기본+심화	용어+요약 1.1 + 1.2	속성이론 1.4			
	기출+적중 3.0		핵심기출 700선 3.1	최고수준 800제 3.3			
	모의고사 5.0				국가직 9급 5.1	지방직 등 9급 5.2	국가직 7급 5.3
정보보호직+경간부 7.0			정보보안기사 필기 7.1				
교재		2020 탑스팟 이론서	핵심기출 700선	·2020 탑스팟 이론서/ 최고수준 800제	프린트물	프린트물	프린트물
문제난이도		중~중상	중~중상	중상~상	중상~상	중상~상	상
비고		·이론서2권-전2권 구성 ·주3회 이론수업 ·매주 복습 퀴즈 진행	·연도별 기출문제 풀이 3.2 -교재프린트 제공, 동영상 진행 ·핵심기출 700선 (문제편/정답·해설편/용어·요약집) -전3권 구성 ·정보보안기사는 11월 개강	·최고 수준 800제 (제본, 수강생 제공)는 고득점 합격을 목표로 함	·모의고사식 실전 훈련	·모의고사식 실전 훈련 ·최신 정보보안기사 기출문제 포함 모의고사 진행	·모의고사식 실전 훈련 ·국회사무처 등 시험대비 겸합 ·최종 마무리 정리

추천과정	
전산개발(9급)	입문과정(무료B)→이론 1.1 + 1.2 + 1.3 →기출 3.1 , 3.2 ☒ 택1→최고수준 800제 3.3 →9급 대비 모의고사 5.1 + 5.2
군무원(9급, 7급)	입문과정(무료B)→이론 1.1 + 1.2 + 1.3 →기출 3.1 , 3.2 ☒ 택1→최고수준 800제 3.3 →정보보안기사 필기 7.1 →9급 대비 모의고사 5.1 + 5.2
전산개발(7급)	입문과정(무료B)→이론 1.1 + 1.2 + 1.3 →기출 3.1 , 3.2 ☒ 택1→최고수준 800제 3.3 →9급 대비 모의고사 5.1 + 5.2 → 7급 대비 모의고사 5.3
정보보호직	입문과정(무료B)→이론 1.1 + 1.2 + 1.3 →기출 3.1 , 3.2 ☒ 택1→최고수준 800제 3.3 →정보보안기사 필기 7.1
사이버, 경찰간부	입문과정(무료B)→이론 1.1 + 1.2 + 1.3 →기출 3.1 , 3.2 ☒ 택1→최고수준 800제 3.3 →정보보안기사 필기 7.1 →9급 대비 모의고사 5.1 + 5.2 7급 대비 모의고사 5.3

빅데이터 1.0 / 이론

- 1.1 기본+심화 통합이론
- 1.2 핵심 용어 정리 200선(용어집)
- 1.3 핵심 요약집 정리
- 1.4 속성 이론

빅데이터 3.0 / 기출+적중

- 3.1 핵심기출 700선
- 3.2 연도별 기출문제 풀이
- 3.3 최고수준 800제(학원 내부교재)

빅데이터 5.0 / 모의고사

- 5.1 국가직 9급 대비 모의고사
- 5.2 지방직, 교육청, 서울시, 군무원 대비 모의고사
- 5.3 7급 대비 모의고사

빅데이터 7.0 / 정보보호직+경간부

- 7.1 정보보안기사 필기(알기사)

기타 무료 강의

- A 정보보호론 학습 전략
- B 정보보호론 기초 입문 과정
- C 계리직 대비 정보보호론

[전산직 공채 총정리 (3년간)]

시험종류			2017년				2018년				2019년				시험과목	비고
구분	직류	급수	인원	접수기간	시험일	필기 합격선	인원	접수기간	시험일	필기 합격선	인원	접수기간	시험일	필기 합격선		
해경	정보보호	9급	2	2.8~2.22	3.11	90~	3	3.5 ~ 3.15	4.14	70점후	-				컴일,네트워크보안,시스템보안	필기 합격선이 2016년, 2017년 모두 90점이상 공무원기출+정보보안기사필기 문제집에서 다수 출제
해경	전산	7급					1	3.5 ~ 3.15	4.14	-	-				서류전형	
국가직	전산개발	9급	35	2.1 ~ 2.6	4.8	84	50	2.20 ~ 2.23	4.7	73	83	2.20~2.23	4.6	83	국,영,한,컴일,정보	전산개발, 정보보호직 동시 접수 불가
국가직	정보보호	9급	7	2.1 ~ 2.6	4.8	83	5	2.20 ~ 2.23	4.7	69	8	2.20~2.23	4.6	75	국,영,한,네트워크보안,시스템보안	전산개발, 정보보호직 동시 접수 불가
지방직	전산개발	9급	시도별	4.17~4.21	6.17	시도별	시도별	3.12 ~ 3.16	5.19	시도별	시도별	4.8~4.12	6.15	시도별	국,영,한,컴일,정보	지방직, 교육청 동시 접수 가능, 동시 응시는 불가
교육청	전산개발	9급	시도별	4.17~4.21	6.17	시도별	시도별	3.26 ~ 3.30	5.19	시도별	시도별	4.15~4.19	6.15	시도별	국,영,한,컴일,정보	거주지 제한 있음, 2019년부터 지방직과 시험지 동일
서울시	전산개발	9급	7	3.13~3.17	6.24	86	13	3.12 ~ 3.16	6.23	88	18	3.12~3.18	6.15	76	국,영,한,컴일,정보	거주지 제한 없음, 2019년부터 지방직 시험일자와 동일
군무원	국방부	7급					2	6.7 ~ 6.12	8.11	77	14	4.12~4.17	6.22	74	국,자구,DB,정보	영어와 한국사는 공인시험으로 대체 2018년부터 프로그래밍언어론→정보보호론 교체
군무원	국방부	9급	11	4.17~4.21	7.1	72	13	6.7 ~ 6.12	8.11	77.33	8	4.12~4.17	6.22	78.67	국,컴일,정보	영어와 한국사는 공인시험으로 대체 2018년부터 프로그래밍언어론→정보보호론 교체
군무원	육군	9급	24	4.24~4.28	7.1	68	18	6.7 ~ 6.12	8.11	74.67	56	4.12~4.17	6.22	77.33	국,컴일,정보	상동
군무원	해군	9급	8	4.24~4.28	7.1	67	9	6.7 ~ 6.12	8.11	73.33	19	4.12~4.17	6.22	73.33	국,컴일,정보	상동
군무원	공군	9급	2	4.24~4.28	7.1	66	3	6.7 ~ 6.12	8.11	73.33	21	4.12~4.17	6.22	76	국,컴일,정보	상동
국회사무처	전산개발	9급	1	5.8~5.15	7.22	80	1	5.21~5.25	8.25	83	3	5.20~5.24	8.24		국,영,한,컴일,정보	객관식 5지 선다형 출제
국가직	전산개발	7급	26	6.5~6.9	8.26	75.83	29	7.14~7.17	8.18	74.16	30	7.14~7.17	8.17		국,한,정보,자구,DB,소공	2017년부터 영어는 공인시험으로 대체
해경	전산	순경	14	7.31~8.11	9.2	-	10	7.11~7.30	8.11	-	10	5.24~6.3	7.2		실기시험(서술, 약술)	실기시험→서류전형→면접→최종합격, 경력채용
경찰	사이버(보안)	경장					135	7.20~7.31	9.1	시도별	79	7.12~7.22	8.10		필기(2): 정보보호론,시스템네트워크보안 선택(1): 정보보호관리및법규,디지털포렌식개론, 데이터베이스론	객관식 과목별 20문항, 경력채용 필기시험(50%)→신체,적성,체력(25%)→면접(25%)
지방직(서울)	전산개발	7급					3	3.12~3.16	6.23	80	4	8.6~8.9	10.12		국,영,한,정보,자구,DB,소공	영어는 공인시험 대체 아님, 거주지 제한 없음
지방직(경기)	전산개발	7급	2	6.26~6.29	9.23	81.42	3	7.16~7.20	10.13	76.42	2	8.5~8.7	10.12		국,영,한,정보,자구,DB,소공	영어는 공인시험 대체 아님, 거주지 제한 있음
경찰간부	사이버	간부	5	8.14~8.23	9.23	332.5(1차) 463(2차)	5	8.7~8.16	9.15	312.5(1차) 463.5(2차)	5	8.20~8.29	10.5		필수 : 정보보호론(객), 시스템네트워크보안㈜ 선택 : DB, 통신이론, 소공 중 택1	정보보호론은 전 범위에서 출제 시스템네트워크보안은 해당 범위에서만 서술식으로 출제
국가직(추가)	전산개발	9급	10	8.14~8.17	10.21	80									국,영,한,컴일,정보	2017년 하반기 추가 채용
지방직(추가)	전산개발	9급	시도별	10.20~10.26	12.16	시도별									국,영,한,컴일,정보	2017년 하반기 추가 채용

※ 만든이 : 지안에듀-조현준 선생(정보보호론, 자료구조론, 정보보안기사 담당), 최신 자료는 지안에듀(www.zianedu.com) 조현준 교수방 참조