2021-군무원-7급-정보보호론-해설-곽후근

1. 정보보호의 요구사항으로서 가용성(availability)에 대한 설명으로 가장 옳지 않은 것은?
① 허락된 사용자가 정보 자산에 접근하려 할 때 방해받지 않도록 하는 것이다.
② 서비스거부(DoS) 공격은 가용성을 해치는 공격이다.
③ 가용성을 유지하려면 다수의 사용자에 대한 동시적 서비스가 이루어지게 해야 한다.
④ 가용성을 위한 네트워크 관리 대책은 현재의 인가 수준을 모든 사람에게 유지시키는 것이다.

정답 체크
(4) 인가 수준을 개별적으로 관리해야 한다(공격자를 차단해야 한다).
오답 체크
(1) 인가된 사용자가 자원이 필요할 때 지체 없이 원하는 객체 또는 자원에 접근하여 사용할 수 있어야 하는 성질을 의미한다.
(2) 적극적 공격이다.
(3) 일반적인 서비스를 하는 사이트를 의미한다.

2. 개인정보처리자의 정보보호 원칙에 대한 설명으로 가장 옳지 않은 것은?
① 개인정보에 관한 개발, 운용 및 정책에 관해서는 비공개 정책을 취해야 한다.
② 개인정보의 익명처리가 가능한 경우에는 익명에 의하여 처리될 수 있도록 해야 한다.
③ 개인정보의 처리 목적에 필요한 범위에서 최소한의 개인정보만을 정당하게 수집해야 한다.
④ 개인정보를 수집하는 것을 원칙적으로 제한하여, 개인정보를 수집할 때는 정보 주체에게 동의를 구해야 한다.

정답 체크
(1) 제3조(개인정보 보호 원칙) ⑤ 개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리를 보장하여야 한다.
오답 체크
(2) 제3조(개인정보 보호 원칙) ⑦ 개인정보처리자는 개인정보를 익명 또는 가명으로 처리하여도 개인정보 수집목적을 달성할 수 있는 경우 익명처리가 가능한 경우에는 익명에 의하여, 익명처리로 목적을 달성할 수 없는 경우에는 가명에 의하여 처리될 수 있도록 하여야 한다.
(3) 제3조(개인정보 보호 원칙) ① 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.
(4) 제15조(개인정보의 수집 · 이용) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다.
1. 정보주체의 동의를 받은 경우

3. 디지털 포렌식에서 연계 보관성의 원칙에 대한 설명으로 가장 옳은 것은?
① 모든 증거는 적법한 절차를 거쳐서 획득한 것이어야 한다.
② 법정에 증거를 제출하기 위해서는 똑같은 환경에서 같은 결과가 나와야 한다.
③ 수집된 정보는 각 단계를 거치는 과정에서 위조·변조되어서는 안 되며, 이런 사항을 매번 확인해

야 한다.
④ 증거를 획득하고 이송·분석·보관·법정 제출 하는 일련의 과정이 명확해야 하고 이런 과정에 대한 추적이 가능해야 한다.

정답 체크
(4) 증거는 획득되고 난 뒤 이송/분석/보관/법정 제출이라는 일련의 과정이 명확해야 하고, 이러한 과정에 대한 추적이 가능해야 함을 의미한다.
오답 체크
(1) 정당성의 원칙이다.
(2) 재현의 원칙이다.
(3) 무결성의 원칙이다.

4. 네트워크형 기반의 공개키 구조 시스템에 대한 설명으로 가장 옳지 않은 것은?
① 유연하며 실질적인 신뢰 관계에 적합하다.
② 루트 인증기관의 비밀키 노출 시 복구가 어렵다.
③ 사용자는 최소한 자신에게 인증서를 발행한 인증기관(CA)을 신뢰한다.
④ 사용자가 공개키 기반 구조의 다른 사용자들에게 서명검증을 보장하는 단일 인증 경로를 제공할 수 없다.

정답 체크
(2) 계층형 기반의 공개키 구조 시스템에 대한 설명이다.
오답 체크
(1) 네트워크형 구조의 장점이다.
(3) 공개키 구조 시스템의 기본 원리이다.
(4) 단일 경로를 보장하는 것은 계층형이다.

5. 침입탐지 유형에서 비정상행위 탐지 방법으로 가장 옳지 않은 것은?
① 신경망 방식
② 통계적 접근 방식
③ 상태 전이 분석 방식
④ 전문가 시스템 방식

정답 체크
(3) 오용탐지 방법이다.
오답 체크
(1), (2) 통계적, 예측 가능 패턴 생성, 신경망 방법은 비정상행위 탐지 방법이다.
(4) 전문가 시스템은 기존 기출에서 오용탐지 방법으로 나왔으나(이의 신청을 했었어야 함) 서적 등에서는 오용탐지와 비정상행위를 보는 견해가 존재한다. 그러므로 가장 틀린 답은 아니다.

6. 커버로스(kerberos) 인증 기술에 대한 설명으로 가장 옳지 않은 것은?
① 대칭키 암호화 체계를 사용한다.

② 각각의 부분들과 키 분배 센터와의 사이에 동등한 관계가 존재한다.
③ 클라이언트가 요구하는 통신망의 다른 객체들에게 그 클라이언트를 인증해 준다.
④ 인증을 위한 패스워드의 사용을 허용하지만 네트워크상에서 패스워드가 전송될 필요가 없다.

정답 체크
(2) KDC에 해당한다.
오답 체크
(1) 공개키를 사용할 여지는 있으나 기출에서 대칭키를 사용한다고 나왔다.
(3) SSO에 활용된다.
(4) 모든 사용자의 패스워드를 인증 서버가 가지고 있다.

7. DoS(Denial of Service)의 공격유형으로 옳지 않은 것은?
① buffer overflow 공격 ② smurf 공격 ③ land 공격 ④ TCP SYN flooding 공격

정답 체크
(1) 스택에는 복귀 주소(return address)가 저장되는데, 오버플로우가 발생하면 복귀 주소가 공격자가 원하는 주소로 바뀌어 공격자가 원하는 코드가 실행된다. (힙 버퍼 오버플로우 공격도 발생한다.)
오답 체크
(2) 희생자의 스푸핑된 원본 IP를 가진 수많은 인터넷 제어 메시지 프로토콜(ICMP) 패킷들이 IP 브로드캐스트 주소를 사용하여 컴퓨터 네트워크로 브로드캐스트하는 분산 서비스 거부 공격이다. 네트워크의 대부분의 장치들은 기본적으로 원본 IP 주소에 응답을 보냄으로써 이에 응답한다. 원본 IP 주소를 컴퓨터는 대량의 ICMP 패킷을 받게 되므로 서비스 거부 상태에 빠지게 된다.
(3) 패킷을 전송할 때 출발지 IP 주소와 목적지 IP 주소를 똑같이 만들어서 공격 대상에게 보내는 공격이다.
(4) 가용성 침해 공격이다. 클라이언트가 SYN 패킷을 보내고 서버는 이에 응답해서 SYN+ACK 패킷을 보낸다. 서버는 클라이언트가 ACK 패킷을 보내올 때까지 SYN Received 상태로 일정 시간을 기다려야 하고, 그동안 공격자는 가상의 클라이언트로 위조한 SYN 패킷을 수없이 만들어 서버에 보냄으로써 서버의 가용 동시 접속자 수를 모두 SYN Received 상태로 만들 수 있다.

8. 다음은 특정 악성소프트웨어에 대한 설명이다. 적절한 악성소프트웨어로 옳은 것은?

공격자의 접근을 허용할 목적으로 컴퓨터에 자기 자신을 설치하는 악성코드로, 통상적으로 공격자가 보안접속 절차를 거치지 않고 컴퓨터에 접속해 로컬 시스템에서 명령어를 실행할 수 있게 한다.

① 좀비(zombie) ② 웜(worm)
③ 백도어(backdoor) ④ 플러더(flooders)

정답 체크
(3) 운영체제나 프로그램을 생성할 때 정상적인 인증 과정을 거치지 않고, 운영체제나 프로그램 등에 접근할 수 있도록 만든 일종의 통로이다.
오답 체크

(1) DDoS에서 악성 코드에 감염된 PC이다.
(2) 인터넷 또는 네트워크를 통해서 컴퓨터에서 컴퓨터로 전파되는 악성 프로그램이다. 윈도우의 취약점 또는 응용 프로그램의 취약점을 이용하거나 이메일이나 공유 폴더를 통해 전파되며, 최근에는 공유 프로그램(P2P)을 이용하여 전파되기도 한다. 바이러스와 달리 스스로 전파되는 특성이 있다.
(4) 출제자가 어떤 의도로 낸 지문인지는 알 수 없으나 통상적으로 해커가 영향을 받는 컴퓨터를 제어 할 수 있게 해주는 일종의 봇 악성 코드로 해석할 수 있다.

9. 다음에서 설명하는 데이터베이스 암호화 방식으로 가장 옳은 것은?

- DBMS에 내장 또는 옵션으로 제공되는 암호화 기능을 이용하는 방식이다. - 응용 프로그램에 대한 수정이 없고 인덱스의 경우 DBMS 자체 인덱스 기능과 연동이 가능하다. - DB 내부에서 암·복호 처리를 하는 방식이다.

① TDE 방식 ② API 방식
③ Plug-In 방식 ④ Hybrid 방식

정답 체크
(1) 일반적으로 어플리케이션 수정이 필요 없고, DB 등 지원 가능 여부에 대한 고려 필요하다.
오답 체크
(2) Plug-in 방식에 비해 DB 서버에 영향을 주지 않으나 구축 시 어플리케이션의 수정 필요하다.
(3) 구축 시 일부 어플리케이션 수정이필요하며 DB 서버의 성능에 대한 검토 필요하다.
(4) Plug-in과 API 방식이 조합된 형식이다.

10. 침입차단 시스템에서 배스천 호스트(bastion host)에 대한 설명으로 가장 옳지 않은 것은?
① 침입차단 시스템의 주 서버로 사용된다.
② 보안 정책에 따라 사용자 계정 설정과 접근 권한 설정 기능 등을 수행한다.
③ 사용자의 접속내역과 사용내역을 기록하여 감사 추적을 위한 근거를 제시한다.
④ 내부 네트워크와 외부 네트워크 사이에서 프로토콜 및 데이터를 중계하는 역할을 수행 한다.

정답 체크
(4) 게이트웨이에 대한 설명이다.
오답 체크
(1) 스크리닝 라우터와 더불어 방화벽의 구성 요소이다.
(2), (3) 접근 제어, 프록시, 인증, 로깅 등의 기능을 수행한다.

11. AES의 내부 구조로 가장 옳지 않은 것은?
① S 박스 계층(S-box layer) ② 확산 계층(diffusion layer)
③ 키 덧셈 계층(key addition layer) ④ 바이트 대치 계층(byte substitution layer)

정답 체크
정답 없음
오답 체크

(1) SubBytes에서 수행한다.
(2) SubBytes, ShiftRows, MixColumns, AddRoundKey를 수행하면 diffusion을 수행한다.
(3) AddRoundKey에서 수행한다.
(4) SubBytes에서 수행한다.

12. 방화벽(Firewall)의 구축 형태 중 Screening Router의 특징에 대한 설명으로 가장 옳지 않은 것은?
① 3계층과 4계층에서 실행되며 IP 주소와 포트에 대한 접근통제가 가능하다.
② 라우터에서 구현된 펌웨어의 수준으로는 제한점이 없고 복잡한 정책을 구현하기 쉽다.
③ 네트워크 수준의 IP 데이터그램에서는 출발지 주소 및 목적지 주소에 의한 스크린 기능이 있다.
④ TCP/UDP 수준의 패킷 에서는 포트 번호에 의한 스크린, 프로토콜별 스크린 기능이 있다.

정답 체크
(2) 제한점이 많고, 복잡한 정책을 구현하기 어렵다.
오답 체크
(1) IP와 포트 주소를 이용하여 접근을 제어한다.
(3) 3계층에서의 접근 제어를 의미한다.
(4) 4계층에서의 접근 제어를 의미한다.

13. 네트워크 해 킹 공격 중 land 공격의 대응책에 대한 설명으로 가장 옳은 것은?
① 타임아웃 시간을 줄인다.
② 일회용 패스워드 시스템을 사용한다.
③ 큰 패킷 전송을 제한하도록 설정된 ping 프로그램의 패치를 설치해야 한다.
④ 네트워크 내의 라우터가 내부 IP 주소를 발신지로 갖는 외부 패킷을 차단하도록 한다.

정답 체크
(4) 발신지가 내부 IP 주소라는 것은 land 공격 말고 있을 수 없다.
오답 체크
(1) syn flooding의 대응책이다.
(2) 인증 시스템에서 패스워드 공격에 대한 대응책이다.
(3) ping of death의 대응책이다.

14. APT(Advanced Persistent Threat)에 대한 설명으로 가장 옳지 않은 것은?
① 정보를 수집한 후 공격 대상을 정한다.
② 기존에 알려지지 않았던 취약점을 다양하게 활용하여 이루어진다.
③ 공격자가 다양한 첨단 보안 위협을 이용해 특정 기업의 네트워크에 공격을 가한다.
④ 특정 조직 내부 직원의 컴퓨터를 장악한 후 그 컴퓨터를 통해 다른 컴퓨터나 서버의 중요 정보를 빼온다.

정답 체크
(1) 공격 대상을 정한 후 정보를 수집한다.

오답 체크
(2) 제로 데이 공격을 수행한다.
(3) 사회공학과 루트킷을 이용한다.
(4) 은닉과 적응 과정을 거친다.

15. 정보통신기반 보호법에서 명시한 주요정보통신 기반시설의 취약점을 분석·평가할 수 있는 기관으로 옳지 않은 것은?
① 한국인터넷진흥원
② 한국전자통신연구원
③ 정보통신기반 보호법 제16조의 규정에 의한 정보공유·분석센터
④ 정보보호산업의 진흥에 관한 법률 제23조에 따라 지정된 정보공유·분석센터

정답 체크
(4) 정보보호 전문서비스 기업이다.
오답 체크
(1), (2), (3) 제9조(취약점의 분석 · 평가) ④관리기관의 장은 제1항 또는 제2항에 따라 취약점을 분석 · 평가하고자 하는 경우에는 다음 각호의 1에 해당하는 기관으로 하여금 소관 주요정보통신기반시설의 취약점을 분석 · 평가하게 할 수 있다. 다만, 이 경우 제3항에 따른 전담반을 구성하지 아니할 수 있다.
1.「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제52조의 규정에 의한 한국인터넷진흥원(이하 “인터넷진흥원”이라 한다)
2. 제16조의 규정에 의한 정보공유 · 분석센터(대통령령이 정하는 기준을 충족하는 정보공유 · 분석센터에 한한다)
3.「정보보호산업의 진흥에 관한 법률」제23조에 따라 지정된 정보보호 전문서비스 기업
4.「정부출연연구기관 등의 설립 · 운영 및 육성에 관한 법률」제8조의 규정에 의한 한국전자통신연구원

16. 다음은 SSL(Secure Socket Layer)의 프로토콜 스택에 대한 설명이다. 해당하는 SSL 프로토콜로 옳은 것은?

- 기밀성과 메시지 무결성 제공을 위하여 클라이언트와 서버 간의 약속된 절차에 따라 메시지에 대한 단편화, 압축, 메시지 인증코드 생성 및 암호화 과정 등을 수행한다. - 메시지 단편화 및 압축 시 상대와 합의한 알고리즘을 사용한다. - 압축한 단편과 메시지 인증코드를 합치고 그것을 대칭 암호화한다.

① alert protocol ② record protocol
③ handshake protocol ④ change cipher spec protocol

정답 체크
(2) 대칭 암호를 사용해서 메시지를 암호화하고 통신하는 부분이다. 대칭 암호와 메시지 인증 코드를 이용한다. 알고리즘과 공유 키는 핸드쉐이크 프로토콜을 사용해서 서버와 클라이언트가 상담하여 결정한다.
오답 체크

(1) 뭔가 에러가 발생했다는 것을 통신 상대에게 전달한다.
(3) 클라이언트와 서버가 암호 통신에 사용할 알고리즘과 공유 키를 결정한다. 인증서를 이용한 인증을 수행한다.
(4) 암호 방법을 변경하는 신호를 통신 상대에게 전달한다.

17. 개인정보보호법 제30조(개인정보 처리방침의 수립 및 공개)에 명시된 개인정보 처리방침의 필수 항목으로 옳지 않은 것은?
① 개인정보의 처리 목적
② 개인정보의 처리 및 보유 기간
③ 개인정보의 제3자 제공에 관한 사항
④ 정보주체의 권리·의무 및 그 행사방법에 관한 사항

정답 체크
(3) 필수 항목이 아니다.
오답 체크
(1), (2), (4) 제30조(개인정보 처리방침의 수립 및 공개) ① 개인정보처리자는 다음 각 호의 사항이 포함된 개인정보의 처리 방침(이하 “개인정보 처리방침”이라 한다)을 정하여야 한다. 이 경우 공공기관은 제32조에 따라 등록대상이 되는 개인정보파일에 대하여 개인정보 처리방침을 정한다.
1. 개인정보의 처리 목적
2. 개인정보의 처리 및 보유 기간
3. 개인정보의 제3자 제공에 관한 사항(해당되는 경우에만 정한다)
3의2. 개인정보의 파기절차 및 파기방법(제21조제1항 단서에 따라 개인정보를 보존하여야 하는 경우에는 그 보존근거와 보존하는 개인정보 항목을 포함한다)
4. 개인정보처리의 위탁에 관한 사항(해당되는 경우에만 정한다)
5. 정보주체와 법정대리인의 권리·의무 및 그 행사방법에 관한 사항
6. 제31조에 따른 개인정보 보호책임자의 성명 또는 개인정보 보호업무 및 관련 고충사항을 처리하는 부서의 명칭과 전화번호 등 연락처
7. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항(해당하는 경우에만 정한다)
8. 그 밖에 개인정보의 처리에 관하여 대통령령으로 정한 사항

18. 이메일 보안을 위해 사용되는 보안 기술로만 묶인 것으로 가장 옳은 것은?
① SET, S/MIME ② PEM, PGP
③ S/MIME, IDS ④ PGP, SSO

정답 체크
(2) S/MIME, PEM, PGP는 이메일 보안을 위해 사용된다.
오답 체크
(1) SET은 전자상거래용 프로토콜이다.
(3) IDS는 탐지만을 수행하는 수동적 보안 장비이다.
(4) SSO는 모든 인증을 하나의 시스템에서 한다는 의미이다. 시스템이 몇 대가 되어도 하나의 시스

템에서 인증에 성공하면, 다른 시스템에 대한 접근 권한도 모두 얻는다. 이러한 접속 형태의 대표적인 인증 방법으로는 커버로스(Kerberos)를 이용한 윈도우의 액티브 디렉토리(Active Directory)가 있다.

19. 다음에서 설명하는 데이터베이스 접근통제 방법으로 가장 옳은 것은?

- 데이터베이스 서버에 접근제어를 설치하는 방식이다. - 데이터베이스에 직접 접근하는 전용 클라이언트를 포함해 모든 접근 루트를 제어할 수 있다. - 데이터베이스 서버에 트래픽을 발생시켜 서버의 성능 저하가 우려된다.

① 에이전트 방법 ② 게이트웨이 방법
③ 스니핑 방법 ④ 하이브리드 방법

정답 체크
(1) 서버 자체에 접근제어 및 로깅 기능을 포함하는 에이전트 이식한다. DB에 직접 접근하는 전용 클라이언트를 포함해 모든 접근 루트를 제어할 수 있는 가장 강력한 보안 방법이다.
오답 체크
(2) 프록시 방법은 DB 서버로 접속하는 모든 IP를 DB 보안 서버(프록시 서버)를 통하도록 설정 변경한다. 인라인 방법은 타깃 DB 서버와 클라이언트 네트워크 사이에 인라인 보안시스템 구성한다.
(3) 네트워크 선로상의 패킷들을 TAP 방식과 패킷 미러링 방식을 통해 패킷을 분석 및 로깅하는 방법으로 사후 감사의 의미에 비중을 두는 보안 방식이다.
(4) “에이전트+스니핑”, “게이트웨이+스니핑”, “게이트웨이+에이전트+스니핑”을 결합한다.

20. 사용자의 X.509 인증서 생성 시, 인증기관이 사용자 인증서 내의 사용자 공개키에 대한 신뢰성을 제공하기 위해 서명에 사용하는 키는?
① 사용자의 개인키 ② 사용자의 공개키 ③ 인증기관의 개인키 ④ 인증기관의 공개키

정답 체크
(3) 사용자의 공개키에 인증기관의 개인키로 서명한다.
오답 체크
(1), (2), (4) 다른 방법이 있을 수 없다.

21. ARIA 암호 알고리즘에 대한 설명으로 가장 옳지 않은 것은?
① 128 비트 블록 암호 알고리즘이다.
② 페이스텔 암호(feistel cipher) 구조를 따른다.
③ 키의 길이는 128, 192, 256 비트를 지원한다.
④ 키의 길이로 128 비트를 사용하면 라운드 수는 12이다.

정답 체크
(2) SPN 구조를 가진다.
오답 체크
(1) AES와 마찬가지로 128비트이다.
(3) AES와 마찬가지로 128, 192, 256비트이다.

(4) AES와 다르게 12/14/16 라운드이다.

22. 개인정보보호법에 명시된 개인정보 보호책임자의 수행 업무에 대한 설명으로 옳지 않은 것은?
① 개인정보 처리와 관련한 불만의 처리 및 피해 구제
② 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
③ 정보보호 및 개인정보보호 관리체계 인증(ISMS-P) 취득
④ 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축

정답 체크
(3) 해당 업무를 수행하지 않는다.
오답 체크
(1), (2), (4) 제31조(개인정보 보호책임자의 지정) ① 개인정보처리자는 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호책임자를 지정하여야 한다.
② 개인정보 보호책임자는 다음 각 호의 업무를 수행한다.
1. 개인정보 보호 계획의 수립 및 시행
2. 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
3. 개인정보 처리와 관련한 불만의 처리 및 피해 구제
4. 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
5. 개인정보 보호 교육 계획의 수립 및 시행
6. 개인정보파일의 보호 및 관리·감독
7. 그 밖에 개인정보의 적절한 처리를 위하여 대통령령으로 정한 업무

23. 접근 통제 보안 모델에서 비바(biba) 모델에 대한 설명으로 가장 적절한 것은?
① 허가되지 않은 방식의 접근을 방지한다.
② 시스템 내의 활동에 관계없이 시스템이 스스로를 보호하고 불안정한 상태가 되지 않도록 한다.
③ 무결성에 초점을 두고 비인가자들의 데이터 변형 방지만 취급한다.
④ 한 보안 수준에서 실행된 명령과 활동은 타 보안 수준의 주체와 객체에 영향을 주지 않음을 보장한다.

정답 체크
(3) BLP의 단점을 보완한 무결성을 보장하는 최초의 모델이다. 비바의 속성은 BLP의 반대 개념인 No Read Down(높은 등급의 주체는 낮은 등급의 객체를 읽을 수 없음), No Write Up(낮은 등급의 주체는 상위 등급의 객체를 수정할 수 없음)이다.
오답 체크
(1) BLP 모델이다.
(2) 상태 기계(state machine) 모델이다.
(4) 비간섭(non interface) 모델이다.

24. 다음 그림이 나타내는 블록암호 운영 모드로 옳은 것은?

① ECB(Electronic CodeBook) ② CFB(Cipher FeedBack)
③ CBC(Cipher Block Chaining) ④ CTR(Counter)

정답 체크
(3) 암호화를 나중에 한다.
오답 체크
(1) 1:1로 암호화와 복호화가 수행된다.
(2) 비슷한 구조에서 암호화를 먼저한다.
(4) Counter가 있어야 한다.

25. 다음은 특정 무선 네트워크 보안 프로토콜에 대한 설명이다. 적절한 무선 네트워크 보안 프로토콜로 옳은 것은?

- WEP 방식의 보안 취약점을 해결하기 위한 대안으로 만들어진 프로토콜이다. - WEP 보다 훨씬 강화된 암호화 세션을 제공한다. - AP에 접속하는 사용자 마다 같은 암호화키를 사용한다는 점이 보안상 미흡하다.

① EAP ② TKIP
③ IEEE 802.11i ④ WPA-PSK

정답 체크
(4) WPA-Personal을 의미한다.
오답 체크
(1) 인증 프레임워크를 의미한다(WPA-Enterprise).
(2) WPA에 사용되는 동적 암호키 변경 알고리즘에 해당한다.
(3) WPA2에 해당한다.