2021-해경1차-정보시스템보안-해설-곽후근

1. 다음 중 디지털 포렌식의 기본 원칙에 대한 설명으로 가장 옳지 않은 것은?
① 정당성의 원칙 : 모든 증거는 적법한 절차를 거쳐 획득하여야 하며, 위법한 절차를 거쳐 획득한 증거는 증거 능력이 없다.
② 재현의 원칙 : 증거는 어떤 절차를 통해 정제될 수 없으며 똑같은 환경에서 같은 결과가 한번만 나오면 된다.
③ 신속성의 원칙 : 컴퓨터 내부의 정보는 휘발성을 가진 것이 많기 때문에 가능한 빠르게 획득해야 한다.
④ 연계 보관성의 원칙 : 증거는 획득 후 이송/분석 /보관/법정 제출의 과정이 명확해야 하며, 이러한 과정에 대한 추적이 가능해야 한다.
정답 체크
(2) 증거 자료는 같은 환경에서 같은 결과가 나오도록 재현이 가능해야 한다.
오답 체크
(1) 모든 증거는 적법한 절차를 거쳐서 획득한 것이어야 함을 의미한다. 위법한 절차를 거쳐 획득한 증거는 증거 능력이 없다.
(3) 컴퓨터 내부의 정보는 휘발성을 가진 것이 많기 때문에 신속하게 이뤄져야 함을 의미한다.
(4) 증거는 획득되고 난 뒤 이송/분석/보관/법정 제출이라는 일련의 과정이 명확해야 하고, 이러한 과정에 대한 추적이 가능해야 함을 의미한다.

2. 다음 중 정보자산에 대한 위험분석에서 사용하는 ALE, SLE, ARO 사이의 관계로 가장 옳은 것은?
① ALE=SLE+ARO ② SLE=ALE+ARO ③ ALE=SLE×ARO ④ SLE=ARO×ALE
정답 체크
(3) LE는 보안 투자로부터 얻을 수 있는 최대 편익을 의미한다. ALE를 넘어가는 연간 보안 투자는 비효율적이다. ALE가 20만 달러이고 연간 보안 예산이 25만 달러이면 비효율적이다. ALE는 SLE x ARO로 계산한다.
Tip! ALE를 테이블로 정리하면 다음과 같다.

Concept	Derivation Formula	설명
Exposure Factor(**EF**)	% of Asset loss cuased by threat	위협에 의해 야기될 수 있는 **자산 손실률** (0~100%의 백분율로 표시)
Single Loss Expectancy(**SLE**)	Asset Value × (EF)	단일 위협으로부터 발생되는 조직의 손실 기대치 (**1회 손실액**)(**단일 예산 손실**)
Annualized Rate of Occurrence(**ARO**)	Frequency of threat occurrence per year	위협실현의 연간 빈도 수(**연간 발생 비율**) (역사적 기록, 통계적 분석, 추측 등)
Annualized Loss Expectancy(**ALE**)	(SLE) × (ARO)	**위협에 의한 조직의 연간 재정적 손실** (**연간 예산 손실**)

3. 다음 중 대칭키 암호에 대한 설명으로 가장 옳지 않은 것은?
① DES, AES는 대칭키 암호 알고리즘에 속한다.

② AES는 SPN(Substitution-Permutation Network) 기반 대칭키 암호이다.
③ AES는 128bit 라운드 키를 사용한다.
④ 대칭키 암호는 두 개의 키 값(비밀키, 공개키)이 서로 대칭적으로 존재해야 한다.
정답 체크
(4) 대칭키는 비밀키가 서로 대칭적으로 존재하고, 비대칭키(공개키)는 개인키, 공개키가 비대칭적으로 존재한다.
오답 체크
(1) DES, 3-DES, AES, IDEA, Blowfish 등은 대칭키 암호에 속한다.
(2) AES는 SPN 구조를 가진다. (DES는 Feistel 구조를 가진다.)
(3) AES는 128/192/256비트 라운드 키를 사용한다.

4. 다음 중 Feistel 암호 방식에 대한 설명으로 가장 옳지 않은 것은?
① Feistel 암호 방식의 암호 강도는 평문 블록의 길이, 키의 길이, 라운드의 수에 의하여 결정된다.
② Feistel 암호 방식의 복호화 과정과 암호화 과정은 동일하다.
③ AES 암호 알고리즘은 Feistel 암호 방식을 사용한다.
④ Feistel 암호 방식은 대칭키 암호 알고리즘에서 사용된다.
정답 체크
(3) SPN 암호 방식을 사용한다.
오답 체크
(1) 예를 들면, 평문 블록의 길이는 최소 128비트이고, 키의 길이는 최소 128비트이고, 라운드 수는 16라운드 이상으로 해야 한다.
(2) Feistel은 암호호와 복호화 과정이 동일하고, SPN은 암호호와 복호화 과정이 동일하지 않다.
(4) 대칭키 암호인 DES, Blowfish, SEED 등에서 사용한다.

5. 다음 중 KDC(Key Distribution Center) 없이 양쪽 통신 주체가 대칭 세션 키를 생성할 수 있는 프로토콜로 가장 옳은 것은?
① Otway-Rees 프로토콜
② Needham-Schroeder 프로토콜
③ Kerberos 프로토콜
④ Diffie-Hellman 프로토콜
정답 체크
(4) 공개된 P(소수), G(원시근)와 양쪽 통신 주체의 난수(a, b)가 있으면 대칭 세션 키(P^{ab} mod G)를 생성할 수 있다.
오답 체크
(1) 안전하지 않은 네트워크에서 사용하도록 설계된 컴퓨터 네트워크 인증 프로토콜이다.
(2) 대칭키와 공개키 프로토콜을 정의하고, 이중 대칭키는 커버로스에서 사용된다.
(3) 분산 컴퓨팅 환경에서 대칭키 암호를 이용하여 사용자 인증을 제공하는 중앙 집중형 인증 방식이다.

6. 정부는 사이버테러를 없애기 위하여 2020년 8월「 개인정보 보호법 」개정으로 100만 명 이상 이용자의 개인 정보를 보유 했거나 전년도 정보통신 서비스 매출이 100억 원 이상인 정보통신서비

스 사업자의 경우 망분리를 도입할 것을 법으로 의무화했다. 다음 중 망분리 기술로 가장 옳지 않은 것은?
① DMZ ② OS 커널분리 ③ VDI ④ 가상화기술
정답 체크
(1) 기업의 내부 네트워크와 외부 네트워크 사이에 일종의 중립 지역이 설치되는 호스트 또는 네트워크이다. 외부 사용자가 기업의 정보를 담고 있는 내부 서버에 직접 접근하는 것을 방지하며, 외부 사용자가 DMZ 호스트의 보안을 뚫고 들어오더라도 기업 내부의 정보는 유출되지 않는다.
오답 체크
(2) VDI 방식과는 다르게 운영체제를 이중화시켜 논리적으로 망을 분리하는 OS 커널 분리 솔루션도 많이 이용되고 있다. OS 커널 분리 솔루션의 경우 VDI를 구축하는 것보다 가격이 훨씬 저렴하다. 특히 VDI는 시스템 장애 시 전체 이용자가 피해를 보지만, OS 커널 분리 방식은 하나의 PC만 장애가 발생하기 때문에 위험 관리 측면에서 우수하다(CBC에 해당).
(3) 데스크톱 가상화(VDI, Virtual Desktop Infrastructure)란 물리적으로 존재하진 않지만 실제 작동하는 컴퓨터 안에서 작동하는 또 하나의 컴퓨터를 만들 수 있는 기술이다. 한마디로 컴퓨터 속에 또 다른 가상 컴퓨터를 만들 수 있게 돕는 기술이다(SBC에 해당).
(4) 물리적인 컴퓨터 리소스(자원)의 특징을 다른 시스템, 응용 프로그램, 최종 사용자들이 리소스와 상호 작용하는 방식으로부터 감추는 기술이다. 간단하게 말하면 가상화를 적용하면 하나의 컴퓨터에서 동시에 1개 이상의 운영체제를 가동시킬 수 있다(SBC의 VDI에 해당하고, CBC에서는 별도의 가상화가 필요).

7. 다음 중 유닉스/리눅스 시스템의 로그 파일에 기록 되는 정보에 대한 설명으로 가장 옳지 않은 것은?
① secure - telnet이나 ftp 등 인증과정을 거치는 모든 로그를 저장
② loginlog - 성공한 로그인에 대한 내용
③ pacct - 시스템에 로그인한 모든 사용자가 수행한 프로그램 정보
④ btmp - 5번 이상 실패한 로그인 시도 정보
정답 체크
(2) 실패한 로그인에 대한 내용이다(유닉스).
오답 체크
(1) 사용자/그룹 생성/삭제, 로그인 등의 사용자 인증에 대한 정보를 기록하고 있는 로그 파일이다.
(3) 유닉스에서 시스템에 로그인한 모든 사용자가 수행한 프로그램에 대한 정보 저장하는 로그이다.
(4) 실패한 로그인에 대한 내용이다(리눅스).

8. 다음 〈보기〉 중 리눅스 시스템에서 침해사고 분석 시 wtmp 로그파일에서 확인할 수 있는 정보로 가장 옳은 것을 모두 고른 것은?

〈 보 기 〉
㉠ 재부팅 시간 정보
㉡ 사용자의 로그인/로그 아웃 정보
㉢ 로그인에 실패한 사용자의 IP주소

① ㉠
② ㉠, ㉡

③ ㉡
④ ㉠, ㉡, ㉢
정답 체크
(2) ㄱ. 재부팅 시간 정보: wtmp에서 확인할 수 있다.
ㄴ. 사용자의 로그인/로그아웃 정보: wtmp에서 확인할 수 있다.
오답 체크
(1) ㄴ이 없다.
(3) ㄱ이 없다.
(4) ㄷ. 로그인에 실패한 사용자의 IP 주소: btmp에서 확인할 수 있다.

9. 다음 중 스트림 암호에 대한 설명으로 가장 옳지 않은 것은?
① 통상 한 번에 1비트씩 암호화 및 복호화를 하기 때문에 하드웨어적인 shift register 방식을 많이 사용한다.
② 짧은 주기와 높은 선형 복잡도가 요구되며 주로 LFSR을 이용한다.
③ 스트림 암호는 데이터의 흐름을 순차적으로 처리해가기 때문에 내부상태를 가지고 있다.
④ 블록 암호화 방식보다 매우 빠르지만 암호화 강도는 약하다.
정답 체크
(2) 긴 주기와 낮은 선형 복잡도를 요구한다.
오답 체크
(1) 1비트씩 또는 8비트씩 암호화 및 복호화를 한다.
(3) 내부상태를 저장하기 위해 LFSR를 이용한다.
(4) 속도의 강점을 가지지만 강도는 약하다.

10. 다음은 정보보호 관리 체계(ISMS, Information Security Management System) 5단계 과정을 수립하려고 한다. 가장 옳은 순서는?
① 경영 조직 → 위험 관리 → 정책 수립 및 범위 설정 → 구현 → 사후관리
② 정책 수립 및 범위 설정 → 경영 조직 → 위험 관리 → 구현 → 사후관리
③ 정책 수립 및 범위 설정 → 경영 조직 → 구현 → 위험 관리 → 사후관리
④ 경영 조직 → 정책 수립 및 범위 설정 → 위험 관리 → 구현 → 사후관리
정답 체크
(2) PDCA를 따른다.
Plan : 정책 수립 및 범위 설정, 경영 조직, 위험 관리
Do : 구현
Check, Act : 사후관리

11. 다음 〈보기〉의 ㉠, ㉡에 들어갈 웹 공격 기법으로 가장 옳은 것은?

〈 보 기 〉
(㉠)은(는) 웹 해킹으로 서버 권한을 획득한 후, 해당 서버에서 공격자의 PC로 연결하고 공격자가 직접 명령을 입력하여 개인정보 전송 등의 악의적인 행위를 하는 공격이다. 이 기법은 방화벽의 내부에서 외부로 나가는 패킷에 대한 아웃바운드 필터링을 수행하지 않는 허점을 이용한다.

(㉡)은(는) 공격자가 웹 서버의 게시판 등에 악성 스크립트를 삽입한 후, 사용자의 쿠키와 같은 개인정보를 특정 사이트로 전송하게 하거나 악성파일을 다운로드하여 실행하도록 유도하는 공격이다.

	㉠	㉡
①	디렉토리 리스팅	포맷 스트링
②	디렉토리 리스팅	XSS
③	리버스 텔넷	포맷 스트링
④	리버스 텔넷	XSS

정답 체크

(4) 리버스 텔넷 : 방화벽이 존재하는 시스템을 공격할 때 자주 사용된다. 일반적으로 웹 서버는 방화벽 내부에 존재한다. 그리고 웹 서버는 80번 포트를 이용한 웹 서비스만 제공하면 되기 때문에, 방화벽은 외부 인터넷을 사용하는 사용자에 대해 80포트만을 허용한다. 웹 서버의 텔넷(Telnet)이 열려있어도, 방화벽으로 인해 공격자가 외부에서 접근할 수 없다(방화벽의 인 바운드 정책).

XSS : 웹사이트 관리자가 아닌 이가 웹 페이지에 악성 스크립트를 삽입할 수 있는 취약점이다. 주로 여러 사용자가 보게 되는 전자 게시판에 악성 스크립트가 담긴 글을 올리는 형태로 이루어진다. 이 취약점은 웹 애플리케이션이 사용자로부터 입력 받은 값을 제대로 검사하지 않고 사용할 경우 나타난다. 이 취약점으로 해커가 사용자의 정보(쿠키, 세션 등)를 탈취하거나, 자동으로 비정상적인 기능을 수행하게 할 수 있다. 주로 다른 웹사이트와 정보를 교환하는 식으로 작동하므로 사이트 간 스크립팅이라고 한다.

오답 체크

(1), (2), (3) 디렉토리 리스팅 : 웹 브라우저에서 웹 서버의 특정 디렉토리를 열면, 그 디렉토리에 있는 파일과 디렉토리 목록이 모두 나열되는 것이다. 공격자는 디렉토리 리스팅을 통해 여러 정보를 획득할 수 있다. 우선 화면에 보이지 않는 여러 웹 페이지를 클릭 하나만으로도 직접 접근할 수 있다.

포맷 스트링 : printf() 사용된 %s와 같은 문자열을 가리켜 포맷 스트링이라 한다. 포맷 스트링을 조작하면(%n을 사용) 임의의 메모리 주소의 쓰기 혹은 복귀 주소를 변경할 수 있다.

12. 인터넷망에서 안전하게 정보를 전송하기 위하여 사용되고 있는 네트워크 계층 보안 프로토콜인 IPSec(IP Security Protocol)에 대한 설명 중 가장 옳지 않은 것은?

① 네트워크 계층의 보안을 위하여 인증 헤더 (AH, Authentication Header) 프로토콜과 ESP(Encapsulating Security Payload) 프로토콜을 사용하여 보안연계(SA, Security Association) 서비스를 제공한다.

② 강력한 암호화와 인증 방식을 가지며, 두 컴퓨터 사이의 터널화 된 통신을 가능하도록 한다.

③ 비연결 무결성은 메시지가 위·변조되지 않았음을 보장해준다.

④ ESP 프로토콜은 암호화를 지원하지 않으며 AH 프로토콜만 암호화를 지원한다.

정답 체크

(4) AH는 인증, 무결성, 재전송 방지를 제공하고, ESP는 인증, 무결성, 기밀성(암호화), 재전송 방지를 제공한다.

오답 체크

(1) AH, ESP, IKE(SA를 위한 SPI를 전송)를 제공한다.

(2) 전송 모드와 터널 모드를 제공한다.

(3) AH, ESP를 통해 무결성을 제공한다.

13. 다음 〈보기〉의 접근 제어 정책으로 가장 옳은 것은 무엇인가?

〈 보 기 〉
ㅇ 한 주체가 어느 한 객체를 읽고 그 내용을 다른 어느 한 객체로 복사하는 경우에 처음의 객체에 내포된 접근 통제 정보가 복사된 객체로 전달되지 않는다.
ㅇ 특정 객체에 대해 특정 주체가 다른 주체에 대해 임의적으로 접근 제어가 가능하여 매우 유연한 접근 제어 서비스를 제공할 수 있다.

① Access Control List ② RBAC ③ DAC ④ MAC

정답 체크

(3) 객체에 대한 소유권(ownership)에 기초해서 소유권을 가진 주체가 객체에 대한 권한의 전부 혹은 일부를 다른 주체에게 부여한다. 유닉스 혹은 관계형 데이터베이스(RDBMS)에서 사용한다.

오답 체크

(1) 주체의 관점에서 객체들에 대한 권한을 다루거나 객체의 관점에서 주체들의 권한을 다룬다.

(2) 기업 환경에서는 사용자가 기업 내에서 어떤 역할(Role)을 수행하고 있는가에 따라 권한이 정해진다. 이를 모델화한 것이 역할 기반 접근 제어이다.

(4) 주체와 객체에 적절한 보안 등급(레이블)을 부여하고, 접근 제어시 이 등급을 비교함으로써 접근의 허용 여부를 판단하게 된다. 군사 환경과 같은 엄격한 보안이 요구되는 분야에 적합하다.

14. 다음 〈보기〉에서 설명하는 블록암호 운용 모드는?

〈 보 기 〉
ㅇ 암·복호화 모두 병렬 처리가 가능하다.
ㅇ 블록 암호 알고리즘의 암호화 로직만 사용한다.
ㅇ 암호문의 한 비트 오류는 복호화되는 평문의 한 비트에만 영향을 준다.

① CTR ② CFB ③ CBC ④ ECB

정답 체크

(1) 암호화/복호화 병렬 처리가 가능하다(이전 단계의 영향을 받지 않는다). 암호화/복호화시에 암호화 로직만 사용한다(즉, 복호화 로직을 사용하지 않는다). 암호문의 한 비트 오류는 복호화되는 평문의 한 비트에만 영향을 준다(즉, 에러가 전파되지 않는다).

오답 체크

(2) 복호화는 병렬 처리가 가능하지만 암호화는 병렬 처리가 가능하지 않다(즉, 이전 단계의 영향을 받는다). 암호화/복호화시에 암호화 로직만 사용한다(즉, 복호화 로직을 사용하지 않는다). 암호문의 한 비트 오류는 복호화되는 평문의 한 비트와 다음 복호화되는 평문에 영향을 준다(즉, 에러가 전파된다).

(3) 복호화는 병렬 처리가 가능하지만 암호화는 병렬 처리가 가능하지 않다(즉, 이전 단계의 영향을 받는다). 암호화시에 암호화 로직을 사용하고 복호화시에 복호화 로직을 사용한다. 암호문의 한 비트 오류는 복호화되는 평문의 한 비트와 다음 복호화되는 평문에 영향을 준다(즉, 에러가 전파된다).

(4) 암호화/복호화 병렬 처리가 가능하다(이전 단계의 영향을 받지 않는다). 암호화시에 암호화 로직을 사용하고 복호화시에 복호화 로직을 사용한다. 암호문의 한 비트 오류는 복호화되는 평문의 한 비트에만 영향을 준다(즉, 에러가 전파되지 않는다).

15. 다음 〈보기〉에서 설명하는 기법으로 가장 옳은 것은?

〈 보 기 〉
높은 등급의 인가를 가진 주체가 낮은 등급의 인가를 가진 주체에게 정보를 보내는 방법으로 비밀 정보를 다른 사람이 알지 못하게 전달하는 방법이다.

① 터널링
② 은닉채널
③ 송신채널
④ 이중채널
정답 체크
(2) 기본 채널의 대역폭을 축소하여 보내는 은닉 메시지는 다른 사람이 눈으로는 볼 수 없다.
오답 체크
(1) 데이터 스트림을 인터넷 상에서 가상의 통로를 통해 전달시키는 기술이다.
(3) 보내는 쪽은 채널을 의미한다. 반대는 수신채널이다.
(4) 통상적으로 사용하는 용어는 아니나 전송 채널이 2개인 것을 의미한다.

16. 다음 〈보기〉는 사이버 침해사고 대응절차에 대한 설명이다. 침해사고 대응 1단계부터 6단계까지 순서를 가장 옳게 나열한 것은?

〈 보 기 〉
㉠ 침해사고의 인식 및 신고
㉡ 긴급 조치
㉢ 침해사고 결과 분석 및 보고서 작성
㉣ 분석
㉤ 재발방지 조치
㉥ 침해사고 분석 및 대응 결과 승인

① ㉠-㉡-㉣-㉤-㉢-㉥ ② ㉠-㉡-㉢-㉣-㉤-㉥ ③ ㉠-㉡-㉢-㉤-㉥-㉣ ④ ㉢-㉣-㉤-㉥-㉡-㉠
정답 체크
(1) 침해사고의 인식 및 신고 : 침해가 발생했음을 확인하다.
긴급 조치 : 랜선을 제거한다.
분석 : 문제를 분석한다.
재발방지 조치 : 해커가 설치한 백도어 등을 제거한다.
침해사고 결과 분석 및 보고서 작성 : 보고서를 작성한다.
침해사고 분석 및 대응 결과 승인 : 보고서를 확인한다.

17. 다음 중 커버로스(Kerberose)에 대한 설명으로 가장 옳지 않은 것은?
① 커버로스는 모든 사용자의 패스워드를 알고 있고, 중앙집중식 데이터베이스에 그 패스워드를 저장하고 있는 인증 서버를 이용한다.
② 커버로스는 사용자에게 동일한 계정 정보로 여러 가지 서비스를 받을 수 있게 한다.
③ 커버로스는 패스워드 사전공격(Dictionary Attack)에 강하다.
④ 대칭키를 사용하여 도청으로부터 보호한다.
정답 체크
(3) AS는 패스워드를 가지고 있고, 사전공격에 약하다.

오답 체크
(1) 패스워드를 이용하여 키를 만들어낸다.
(2) SSO(Single Sing On)에 활용된다.
(4) 사전에 공유된 비밀키와 세션키를 사용한다.

18. 암호 해독자가 일정량의 평문 P에 대응하는 암호문 C를 알고 있는 상태에서 해독하는 방법이며, 암호문 C와 평문 P의 관계로부터 키 K나 평문 P를 추정하여 해독하는 공격방법은 무엇인가?
① KPA ② CPA ③ COA ④ CCA
정답 체크
(1) 암호 해독자는 일정량의 평문(P)에 대응하는 암호문(C) 쌍을 이미 알고 있는 상태에서 암호문(C)과 평문(P)의 관계로부터 키(K)나 평문(P)을 추정한다.
오답 체크
(2) 해독자가 사용된 암호화기에 접근할 수 있어 평문(P)을 선택하여 평문에 대응하는 암호문(C)을 얻어 키(K)나 평문(P)을 해독하는 방법이다.
(3) 해독자는 단지 암호문 C만을 갖고 이로부터 평문(P)이나 키(K)를 찾아내는 방법이다.
(4) 해독자가 암호 복호화기에 접근할 수 있어 암호문(C)에 대응하는 평문(P)을 얻어내어 해독하는 방법이다.

19. 다음 중 위험(Risk)에 대한 정의 및 구성요소에 대한 내용으로 가장 옳지 않은 것은?
① 위험이란 원하지 않는 사건이 발생하여 손실 또는 부정적인 영향을 미칠 가능성을 말한다.
② 위험은 자산, 위협, 취약성으로 표현한다.
③ 위험은 손실을 끼치는 사건 발생 가능성에는 비례하나 발생 손실의 정도에 반비례한다.
④ 위협 주체가 취약점을 활용할 수 있는 가능성과 그와 관련된 비즈니스 영향을 가리킨다.
정답 체크
(3) 발생 손실의 정도에 비례한다.
오답 체크
(1) 자산의 취약한 부분에 위협요소가 발생하여 자산에 발생한 손실 또는 손상을 유발할 잠재성(가능성)이다.
(2) AVT(자산, 취약점, 위협)의 함수이다.
(4) 기업이 보호하고자 하는 유·무형의 자산과 그에 따른 위협 요소의 상관관계 속에서 발생한다.

20. 다음 중 위험분석 방법에 대한 설명으로 가장 옳지 않은 것은?
① 과거자료 분석법 : 과거 자료가 많을수록 분석의 정확도가 높아진다. 과거에 일어났던 사건이 미래에도 일어난다는 가정이 필요하며 과거의 사건 중 발생 빈도가 낮은 자료에 대해서는 적용이 어렵다.
② 확률분포법 : 미지의 사건을 추정하는데 사용되는 방법이다. 미지의 사건을 확률적(통계적) 편차를 이용하여 최저, 보통, 최고의 위험평가를 예측 할 수 있다. (정확성이 낮다)
③ 시나리오법 : 어떤 사건도 기대대로 발생하지 않는다는 사실에 근거하여 일정 조건하에서 위협에 대한 발생 가능한 결과들을 추정하는 방법이다.
④ 순위 결정법 : 시스템에 관한 전문적인 지식을 갖춘 전문가의 집단을 구성하고 위험을 분석 및 평가하여 정보시스템이 직면한 다양한 위협과 취약성을 토론을 통해 분석하는 방법이다.

정답 체크
(4) 델파이법에 해당되고, 순위결정법은 비교 우위 순위 결정표에 위험 항목들의 서술적 순위를 결정하는 방법이다.
오답 체크
(1) 미래 사건의 발생 가능성을 예측하는 방법으로, 과거의 자료를 통해 위험 발생 가능성을 예측한다.
(2) 미지의 사건을 추정하는데 사용되는 방법이다. 이 방법은 미지의 사건을 확률적(통계적)편차를 이용하여 최저, 보통, 최고의 위험 평가를 예측한다.
(3) 어떤 사건도 기대대로 발생하지 않는다는 사실에 근거하여, 일정 조건 하에서 위협에 대한 발생 가능한 결과들을 추정(시나리오)하는 방법이다.