# 2023년 국가직 9급 정보보호론 총평

### 1. 출제경향 분석

시험범위는 계속 넓어져 정보보호직과 정보보안기사를 따라가고 있습니다. 악성코드 정적분석 도구는 정보보호직에서 출제된 적이 있습니다. 쿠키의 처리과정은 요청과 응답 메시지의 형식을 알면 쉽게 풀 수 있는 문제입니다. 이는 정보보안기사에 출제된 적이 있습니다.(알기사, 조현준 저 참조) 향후 정보보호론은 범위는 넓어지고, 난이도는 계속 올라간다고 생각하시면 될 것 같습니다.

### 2. 난이도

전체적인 난이도는 전년도 국가직 시험과 비슷한 수준으로 판단되고, 당락을 결정할 난이도 있는 문제는 5문항 정도로 보입니다. 다만, 옳은 것을 고르라는 문제가 있어 시간이 걸리고, 실수가 좀 있을 것 같습니다. 기본에 충실하고 응용문제(800제, 모의고사 등)를 많이 푸신 분들은 고득점이 나왔을 것 같습니다. 하지만 쉬운 기출문제(시중 기출문제집이 어려운 문제는 빼는 경향이 있음) 위주로만 이론정리를 하신 분들은 어렵게 느껴졌을 것으로 생각됩니다.

### 3. 향후 학습방향

다음 시험을 위해서 본인의 위치를 냉철히 판단해보고 약점을 보완하셔야 합니다. 약간은 주관적일 수 있지만 이번 시험을 기준으로 80점 이상을 받으신 분들은 그 동안의 공부의 방향이 맞다고 보여집니다. 그러나 60점이하로 받으신 분들은 공부방법을 다시 한번 생각해 볼 필요가 있습니다.



## 조 현 준

- 성균관대학교 정보공학 전공
- CISA, CISSP, 정보보안기사
- 前, 데카르트고시학원 전산직 전임강사
- 現, 지안공무원학원 전산직 전임강사
- 現, (주)지안에듀 정보보안(산업)기사 전임강사


- TopSpot 자료구조론 이론편/기출편
- TopSpot 알기사 정보보안기사(산업기사) 필기
- TopSpot 알기사 정보보안기사(산업기사) 실기
- TopSpot 정보보호론
- TopSpot 정보보호론 기출문제집

유튜브 기출해설 강의 목록(링크) : 조현준 정보보호론 검색
https://www.youtube.com/playlist?list=PLaR0eJQDBqV8Mb3h4hdxwnQ_nBhY0qCWB

## 2023년 국가직 9급 정보보호론

2023년 4월 8일 시행

**1.** ○△× 23.국가.9급

**SSS(Server Side Script) 언어에 해당하지 않는 것은?**

① IIS
② PHP
③ ASP
④ JSP

◦ 자바 스크립트와 같은 CSS(Client Side Script) 기반의 언어는 웹 프락시를 통해 웹 브라우저에 전달하기 때문에 웹 프락시를 통해 전달하는 과정에서 변조될 가능성이 있다. 따라서 CSS 기반의 언어로 필터링 할 경우 공격자가 필터링 로직만 파악하면 쉽게 필터링이 무력화된다. 즉, 필터링 로직은 ASP, JSP, PHP 등과 같은 SSS(Server Side Script)로 필터링을 수행해야 한다.

오답피하기 ① 아파치(apache)와 마이크로 소프트 IIS(Internet Information Server)는 웹서버이다.

정답 ①

**2.** ○△× 23.국가.9급

**정보나 정보시스템을 누가, 언제, 어떤 방법을 통하여 사용했는지 추적할 수 있도록 하는 것은?**

① 인증성
② 가용성
③ 부인방지
④ 책임추적성

오답피하기 ④ 책임추적성(accountability)은 시스템 내의 각 개인은 유일하게 식별되어야 한다는 정보 보호 원칙이다. 이 원칙에 따라 정보 처리 시스템은 누가, 언제, 어떠한 행동을 하였는지 기록하여 필요 시 그 행위자를 추적할 수 있게 하여 정보 보호 규칙을 위반한 개인을 추적할 수 있고, 각 개인은 자신의 행위에 대해서 책임을 진다.

정답 ④

**3.** ○△× 23.국가.9급

**디지털포렌식의 원칙에 대한 설명으로 옳지 않은 것은?**

① 연계성의 원칙: 수집된 증거가 위변조되지 않았음을 증명해야 한다.
② 정당성의 원칙: 법률에서 정하는 적법한 절차와 방식으로 증거가 입수되어야 하며 입수 경위에서 불법이 자행되었다면 그로 인해 수집된 2차적 증거는 모두 무효가 된다.
③ 재현의 원칙: 불법 해킹 용의자의 해킹 도구가 증거 능력을 가지기 위해서는 같은 상황의 피해 시스템에 도구를 적용할 경우 피해 상황과 일치하는 결과가 나와야 한다.
④ 신속성의 원칙: 컴퓨터 내부의 정보는 휘발성을 가진 것이 많기 때문에 신속하게 수집되어야 한다.

디지털 포렌식의 기본원칙
- 정당성: 디지털 자료증거는 적법한 절차를 거쳐 획득
- 재현성: 피해 당시와 동일 조건에서 현장 검출 시 동일 결과 도출
- 신속성: 휘발성 정보를 신속한 조치에 의해 수집
- 연계보관성: 디지털 증거물의 획득, 이송, 분석, 보관, 법정 제출의 각 단계를 담당하는 책임자 명시
- 무결성: 획득한 디지털 증거가 위조 또는 변조되지 않았음을 증명

오답피하기 ① 무결성 원칙에 대한 설명이다.

정답 ①

**4.** ○△× 23.국가.9급

**다음에서 설명하는 국내 인증 제도는?**

보기
- ○ 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 의한 정보보호 관리체계 인증과 「개인정보 보호법」에 의한 개인정보보호 관리체계 인증에 관한 사항을 통합하여 한국인터넷진흥원과 금융보안원에서 인증하고 있다.
- ○ 한국정보통신진흥협회, 한국정보통신기술협회, 개인정보보호협회에서 인증심사를 수행하고 있다.

① CC
② BS7799
③ TCSEC
④ ISMS-P

ISMS-P 추진 체계
- 정책기관: 과학기술정보통신부, 개인정보보호위원회
- 인증기관: 한국인터넷진흥원과 금융보안원
- 심사기관: 한국정보통신진흥협회, 한국정보통신기술협회, 개인정보보호협회

오답피하기 ④ CC, TCSEC은 정보시스템 보안평가 기준이고, BS7799는 영국에서 만든 정보보호 관리체계 구축에 대한 표준이다. ISMS-P(Personal Information & Information Security Management System) 인증은 정보보호 및 개인정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 인터넷진흥원 또는 인증기관이 증명하는 제도이다.

정답 ④

**5.** ○△× 23.국가.9급

**「개인정보 보호법」 제28조의2(가명정보의 처리 등)의 내용으로서 (가)와 (나)에 들어갈 용어를 바르게 연결한 것은?**

보기

제1항 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 (가) 가명정보를 처리할 수 있다.

제2항 개인정보처리자는 제1항에 따라 가명정보를 제3자에게 제공하는 경우에는 특정 개인을 알아보기 위하여 사용될 수 있는 정보를 포함 (나).

| | (가) | (나) |
|---|---|---|
| ① | 동의를 받아 | 할 수 있다 |
| ② | 동의를 받아 | 해서는 아니 된다 |
| ③ | 동의 없이 | 해서는 아니 된다 |
| ④ | 동의 없이 | 할 수 있다 |

제28조의2(가명정보의 처리 등)

① 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있다.

② 개인정보처리자는 가명정보를 제3자에게 제공하는 경우에는 특정 개인을 알아보기 위하여 사용될 수 있는 정보를 포함해서는 아니 된다.

오답피하기 ③ 가명정보를 정보주체의 동의 없이 처리할 수 있는 경우와 강행규정과 임의규정의 차이를 알고 있는지를 묻고 있다.

정답 ③

## 6. ○△× 23.국가.9급

**SSL을 구성하는 프로토콜에 대한 설명으로 옳은 것은?**

① Handshake는 두 단계로 이루어진 메시지 교환 프로토콜로서 클라이언트와 서버 사이의 암호학적 비밀 확립에 필요한 정보를 교환하기 위한 것이다.

② 클라이언트와 서버는 각각 상대방에게 ChangeCipherSpec 메시지를 전달함으로써 메시지의 서명 및 암호화에 필요한 매개변수가 대기 상태에서 활성화되어 비로소 사용할 수 있게 된다.

③ 송신 측의 Record 프로토콜은 응용 계층 또는 상위 프로토콜의 메시지를 단편화, 암호화, 압축, 서명, 헤더 추가의 순서로 처리하여 전송 프로토콜에 전달한다.

④ Alert 프로토콜은 Record 프로토콜의 하위 프로토콜로서 처리 과정의 오류를 알리는 메시지를 전달한다.

ChangeCipherSpec 메시지

◦ ChangeCipherSpec 메시지는 바로 직전에 협상된 CipherSpec과 키에 의하여 보호될 후속 레코드를 상대에게 알리기 위하여 클라이언트 또는 서버에 의해 전송된다.

◦ 종단 간에 협상된 보안 파라미터를 이후부터 적용/변경함을 알리기 위해 사용하는 프로토콜이다. 예를 들어 이 메시지를 받으면 수신자측에서는 보류된 읽기 상태를 현재 읽기 상태로 변경한다.

오답피하기 ① Handshake 과정은 크게 초기협상단계, 서버인증단계, 클라이언트인증단계, 종료단계로 분류된다.(크게 4단계, 세부적으로 13단계) ③ Record 프로토콜은 단편화, 압축, MAC 추가, 암호화, 레코드 헤더 추가의 과정으로 이루어진다. ④ Alert 프로토콜은 Record 프로토콜의 상위 프로토콜이다.

정답 ②

## 7. ○△× 23.국가.9급

**블록체인 기술의 하나인 하이퍼레저 패브릭에 대한 설명으로 옳지 않은 것은?**

① 허가형 프라이빗 블록체인의 형태로 MSP(Membership Service Provider)라는 인증 관리 시스템에 등록된 사용자만 참여할 수 있다.

② 체인코드라는 스마트 컨트랙트를 통해서 분산 원장의 데이터를 읽고 쓸 수 있다.

③ 분산 원장은 원장의 현재 상태를 나타내는 월드 스테이트와 원장의 생성 시점부터 현재까지의 사용 기록을 저장하는 블록체인 두 가지로 구성된다.

④ 트랜잭션을 정해진 순서로 정렬하는 과정을 합의로 정의하고, 이를 위해 지분 증명 방식과 BFT(Byzantine Fault Tolerance) 알고리즘을 사용한다.

하이퍼레저 패브릭

◦ 기업형 블록체인이며 폐쇄형(프라이빗) 블록체인이다.

◦ MSP(Membership Service Provider)를 통해 채널(Channel)의 관리 권한이나 접근 권한을 관리한다.

◦ 체인코드는 이더리움과 같은 분산 플랫폼에 있는 스마트 컨트랙트에 해당한다. 체인코드는 자산과 자산을 변경하기 위한 트랜잭션 명령을 인코딩하는데 사용한다.

◦ 분산 원장

– 월드 스테이트(World State): 현재 상태를 저장해 놓은 데이터베이스

– 블록체인(Blockchain): 상태변화에 대한 모든 로그 기록이 저장

◦ 프라이빗 블록체인의 합의 알고리즘

– Paxos: 가장 일반적인 합의 알고리즘이다.

– PBFT(Practical Byzantine Fault Tolerance): 비잔틴 장군 문제를 해결하고자 고안된 합의 알고리즘이다.

– Raft: Paxos를 보완한 형태이다.

오답피하기 ④ 공개형 블록체인의 합의 알고리즘은 작업증명과 지분증명이 있으며, 폐쇄형 블록체인의 합의 알고리즘은 Paxos, PBFT 등이 있다.

정답 ④

**8.** ○△× 23.국가.9급

**「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제23조의3(본인확인기관의 지정 등)에 의거하여 다음의 사항을 심사하여 대체수단의 개발 · 제공 · 관리 업무(이하 "본인확인업무"라 한다)를 안전하고 신뢰성 있게 수행할 능력이 있다고 인정되는 자를 본인확인기관으로 지정할 수 있는 기관은?**

보기

1. 본인확인업무의 안전성 확보를 위한 물리적 · 기술적 · 관리적 조치계획
2. 본인확인업무의 수행을 위한 기술적 · 재정적 능력
3. 본인확인업무 관련 설비규모의 적정성

① 과학기술정보통신부
② 개인정보보호위원회
③ 방송통신위원회
④ 금융위원회

제23조의3(본인확인기관의 지정 등)
① 방송통신위원회는 다음 각 호의 사항을 심사하여 대체수단의 개발 · 제공 · 관리 업무를 안전하고 신뢰성 있게 수행할 능력이 있다고 인정되는 자를 본인확인기관으로 지정할 수 있다.
1. 본인확인업무의 안전성 확보를 위한 물리적 · 기술적 · 관리적 조치계획
2. 본인확인업무의 수행을 위한 기술적 · 재정적 능력
3. 본인확인업무 관련 설비규모의 적정성
② 본인확인기관이 본인확인업무의 전부 또는 일부를 휴지하고자 하는 때에는 휴지기간을 정하여 휴지하고자 하는 날의 30일 전까지 이를 이용자에게 통보하고 방송통신위원회에 신고하여야 한다. 이 경우 휴지기간은 6개월을 초과할 수 없다.
③ 본인확인기관이 본인확인업무를 폐지하고자 하는 때에는 폐지하고자 하는 날의 60일 전까지 이를 이용자에게 통보하고 방송통신위원회에 신고하여야 한다.

오답피하기 ③ 본인확인기관의 지정은 방송통신위원회에서 하고, 정보보호 관리체계의 인증은 과학기술정보통신부에서 한다.

정답 ③

**9.** ○△× 23.국가.9급

**(가)와 (나)에 들어갈 용어를 바르게 연결한 것은?**

보기

악성 코드의 정적 분석은 파일을 [ (가) ]하여 상세한 동작을 분석하는 단계로 악성 코드 파일을 역공학 분석하여 그 구조, 핵심이 되는 명령 부분, 동작 방식 등을 알아내는 것을 목표로 한다. 이를 위하여 역공학 분석을 위한 [ (나) ]와/과 같은 도구를 활용한다.

| | (가) | (나) |
|---|---|---|
| ① | 패킹 | OllyDbg |
| ② | 패킹 | Regshot |
| ③ | 디스어셈블링 | Regshot |
| ④ | 디스어셈블링 | OllyDbg |

◦ Regshot은 오픈 소스 레지스트리 비교 유틸리티로 새로운 소프트웨어 설치 및 시스템 변경 등의 작업 시 레지스트리 스냅샷을 통해 변경된 레지스트리를 확인 · 비교 할 수 있다.
◦ OllyDbg(만든이인 Oleh Yuschuk의 이름을 땀)는 바이너리 코드 분석을 위한 x86 디버거로서, 소스 코드가 없을 때 유용하게 사용된다.
◦ 정적 분석이란 악성코드를 실행하지 않고 그 자체가 갖고 있는 내용들을 통해 진단하는 것이다. 비교적 쉽고 빠르며, 별도의 지식 없이 정보를 수집할 수 있다.
◦ 악성코드 파일을 실행하지 않는 정적 분석과는 다르게 동적 분석은 해당 파일을 실행하여 나타나는 변화를 모니터링하여 어떠한 기능을 수행하는지 확인하는 분석 방법이다. 악성코드 파일이 실제 악성 행위를 할 수 있으므로 가상 환경에서 동적 분석을 수행한다.

오답피하기 ④ 악성 코드 정적 분석은 디스어셈블링 과정을 통해 이루어지며, IDA, OllyDbg 등과 같은 도구를 이용한다.

정답 ④

**10.** ○△× 23.국가.9급

**프로그램 입력 값에 대한 검증 누락, 부적절한 검증 또는 데이터의 잘못된 형식 지정으로 인해 발생할 수 있는 보안 공격이 아닌 것은?**

① HTTP GET 플러딩
② SQL 삽입
③ 크로스사이트 스크립트
④ 버퍼 오버플로우

입력데이터 검증 및 표현
◦ 정의: 프로그램 입력값에 대한 검증 누락 또는 부적절한 검증, 데이터의 잘못된 형식지정으로 인해 발생할 수 있는 보안약점이다.
◦ 종류: SQL 삽입, 경로 조작 및 자원 삽입, 크로스사이트 스크립트, 운영체제 명령어 삽입, 위험한 형식 파일 업로드, 신뢰되지 않은 URL 주소로 자동 접속 연결, XPath 삽입, XQuery 삽입, 크로스사이트 요청 위조, HTTP 응답분할, 메모리 버퍼 오버플로우, 포맷 스트링 삽입

오답피하기 ① HTTP GET Flooding은 최신 DDoS 공격과 관련되어 있으며, 프로그램 입력 값에 대한 검증 누락, 부적절한 검증 또는 데이터의 잘못된 형식 지정으로 인해 발생할 수 있는 보안 공격과는 거리가 멀다.

정답 ①

**11.** ○△× 23.국가.9급

**정보의 무결성에 중점을 둔 보안 모델은?**

① Biba
② Bell-LaPadula
③ Chinese Wall
④ Lattice

오답피하기 ① Biba는 무결성, Bell-LaPadula는 기밀성, Chinese Wall은 기밀성과 무결성에 중점을 둔 보안 모델이다.

정답 ①

**12.** ○△× 23.국가.9급

**허니팟에 대한 설명으로 옳지 않은 것은?**

① 공격자가 중요한 시스템에 접근하지 못하도록 실제 시스템처럼 보이는 곳으로 유인한다.
② 공격자의 행동 패턴에 관한 정보를 수집한다.
③ 허니팟은 방화벽의 내부망에는 설치할 수 없다.
④ 공격자가 가능한 한 오랫동안 허니팟에서 시간을 보내도록 하고 그사이 관리자는 필요한 대응을 준비한다.

◦ 허니팟은 다양한 곳에 위치할 수 있다. 방화벽 앞에 설치할 경우 내부 네트워크 보호에 우수한 장점이 있다. 하지만 쓸데없는 데이터가 많이 쌓여 효율성이 저하될 수 있다. 방화벽 뒤에 허니팟을 설치하면 효율성은 높아지나 내부 네트워크의 위험도가 증가할 수 있다. 허니팟은 DMZ에도 설치할 수 있다.

오답피하기 ③ 허니팟은 방화벽 앞 또는 뒤와 DMZ 등에 설치할 수 있다.

정답 ③

**13.** ○△× 23.국가.9급

**다음에 설명하는 위험 분석 방법은?**

보기

○ 구조적인 방법론에 기반하지 않고 분석가의 경험이나 지식을 사용하여 위험 분석을 수행한다.
○ 중소 규모의 조직에는 적합할 수 있으나 분석가의 개인적 경험에 지나치게 의존한다는 단점이 있다.

① 기준선 접근법
② 비정형 접근법
③ 상세 위험 분석
④ 복합 접근법

오답피하기 ② 비정형 접근법은 구조적인 방법론에 기반하지 않고, 경험자의 지식을 사용하여 위험분석을 수행하는 것이다. 이 방식은 상세 위험분석보다 빠르고 비용이 덜 든다. 특정 위험분석 방법론과 기법을 선정하여 수행하지 않고 수행자의 경험에 따라 중요 위험 중심으로 분석한다. 이러한 방식은 작은 규모의 조직에는 적합할 수 있으나 새로이 나타나거나 수행자의 경험분야가 적은 위험 영역을 놓칠 가능성이 있다. 논리적이고 검증된 방법론이 아닌, 검토자의 개인적 경험에 지나치게 의존하므로 사업분야 및 보안에 전문성이 높은 인력이 참여하여 수행하지 않으면 실패할 위험이 있다.

정답 ②

**14.** ○△× 23.국가.9급

**RSA를 적용하여 7의 암호문 11과 35의 암호문 42가 주어져 있을 때, 알고리즘의 수학적 특성을 이용하여 계산한 245(= 7 * 35)의 암호문은? (단, RSA 공개 모듈 n = 247, 공개 지수 e = 5)**

① 2
② 215
③ 239
④ 462

◘ 모듈러 연산의 성질
◦ (성질1): (a + b) mod n = ((a mod n) + (b mod n)) mod n
◦ (성질2): (a − b) mod n = ((a mod n) − (b mod n)) mod n
◦ (성질3): (a x b) mod n = ((a mod n) x (b mod n)) mod n

오답피하기 ② 모듈러 연산의 성질을 이용하여 풀면 다음과 같다.

$7^5 \bmod 247 = 11$
$35^5 \bmod 247 = 42$
$245^5 \bmod 247 = (7\times35)^5 \bmod 247$
$= ((7^5 \bmod 247)\times(35^5 \bmod 247)) \bmod 247$
$= (11\times42) \bmod 247 = 462 \bmod 247 = 215$

정답 ②

## 15. ○△× 23.국가.9급

**사용자 A가 사전에 비밀키를 공유하고 있지 않은 사용자 B에게 기밀성 보장이 요구되는 문서 M을 보내기 위한 메시지로 옳은 것은?**

보기

KpuX: 사용자 X의 공개키
KprX: 사용자 X의 개인키
KS: 세션키
H(): 해시 함수
E(): 암호화
||: 연결(concatenation) 연산자

① M || EKprA(H(M))
② EKprA(M || H(M))
③ EKS(M) || EKpuB(KS)
④ EKS(M) || EKprA(KS)

오답피하기 ③ 하이브리드 암호시스템의 개념을 이용한다. 세션키로 메시지를 암호화하고(EKS(M)), 세션키는 수신자의 공개키로 암호화해서 보낸다(EKpuB(KS)).

정답 ③

## 16. ○△× 23.국가.9급

**보안 서비스와 이를 제공하기 위한 보안 기술을 잘못 연결한 것은?**

① 데이터 무결성 – 암호학적 해시
② 신원 인증 – 인증서
③ 부인방지 – 메시지 인증 코드
④ 메시지 인증 – 전자 서명

오답피하기 ③ 부인방지 서비스는 전자 서명을 통해 이룰 수 있다. 메시지 인증 코드는 무결성과 인증 서비스를 제공한다.

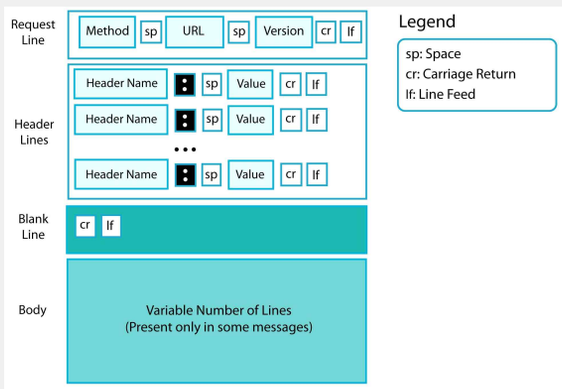
정답 ③

## 17. ○△× 23.국가.9급

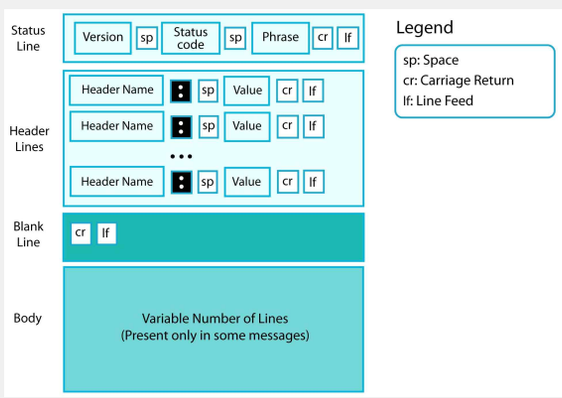
**웹 서버와 클라이언트 간의 쿠키 처리 과정으로 옳지 않은 것은?**

① HTTP 요청 메시지의 헤더 라인을 통한 쿠키 전달
② HTTP 응답 메시지의 상태 라인을 통한 쿠키 전달
③ 클라이언트 브라우저의 쿠키 디렉터리에 쿠키 저장
④ 웹 서버가 클라이언트에 관해 수집한 정보로부터 쿠키를 생성

요청 메시지의 형식




응답 메시지의 형식




오답피하기 ② 쿠키는 요청, 응답 메시지 모두 헤더 라인을 통해 전달한다.

정답 ②

## 18. ○△× 23.국가.9급

**「개인정보 보호법」 제15조(개인정보의 수집 · 이용)에서 개인정보처리자가 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있는 경우에 해당하지 않는 것은?**

① 정보주체의 동의를 받은 경우
② 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
③ 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우
④ 공공기관과의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우

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
2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
3. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우

4. 정보주체와 체결한 계약을 이행하거나 계약을 체결하는 과정에서 정보주체의 요청에 따른 조치를 이행하기 위하여 필요한 경우
5. 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
6. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다.
7. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우

오답피하기 ④ 공공기관과의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우는 해당하지 않는다.

정답 ④

## 19. ○△× 23.국가.9급

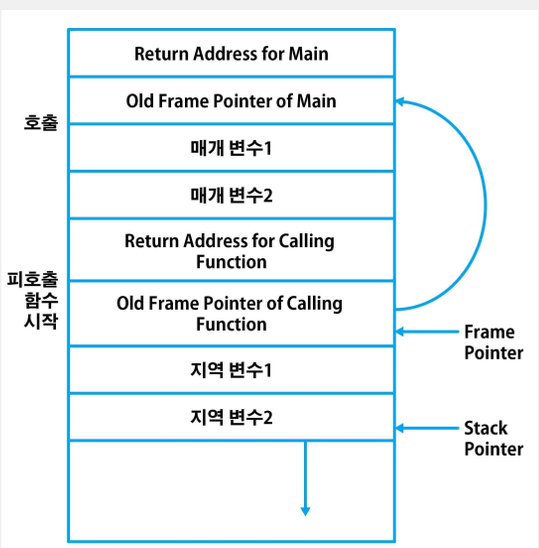
**함수 P에서 호출한 함수 Q가 자신의 작업을 마치고 다시 함수 P로 돌아가는 과정에서의 스택 버퍼 운용 과정을 순서대로 바르게 나열한 것은?**

보기

(가) 스택에 저장되어 있는 복귀 주소(return address)를 pop한다.
(나) 스택 포인터를 프레임 포인터의 값으로 복원시킨다.
(다) 이전 프레임 포인터 값을 pop하여 스택 프레임 포인터를 P의 스택 프레임으로 설정한다.
(라) P가 실행했던 함수 호출(function call) 인스트럭션 다음의 인스트럭션을 실행한다.

① (가) → (나) → (다) → (라)
② (가) → (다) → (라) → (나)
③ (나) → (가) → (라) → (다)
④ (나) → (다) → (가) → (라)

스택 프레임 구조




오답피하기 ④ 스택 프레임 구조를 통해 함수 호출과정을 이해할 수 있다.

정답 ④

## 20. ○△× 23.국가.9급

**무선 네트워크 보안에 대한 설명으로 옳은 것은?**

① 이전에 사용했던 WEP의 보안상 약점을 보강하기 위해서 IETF에서 WPA, WPA2, WPA3를 정의하였다.
② WPA는 TKIP 프로토콜을 채택하여 보안을 강화하였으나 여전히 WEP와 동일한 메시지 무결성 확인 방식을 사용하는 약점이 있다.
③ WPA2는 무선 LAN 보안 표준인 IEEE 802.1X의 보안 요건을 충족하기 위하여 CCM 모드의 AES 블록 암호 방식을 채택하고 있다.
④ WPA-개인 모드에서는 PSK로부터 유도된 암호화 키를 사용하는 반면에, WPA-엔터프라이즈 모드에서는 인증 및 암호화를 강화하기 위해 RADIUS 인증 서버를 두고 EAP 표준을 이용한다.

◦ 소규모 네트워크에서는 PSK(PreShared Key) 방식의 사용자 인증이, 대규모 네트워크인 경우에는 별도의 인증서버를 활용한 802.1x 방식의 사용자 인증이 많이 활용된다.

오답피하기 ① WPA, WPA2, WPA3는 IETF가 아닌 IEEE 802.11i 작업 그룹과 Wi-Fi Alliance에 의해 개발되었다. ② WPA는 TKIP 프로토콜을 채택하여 무결성 서비스 등을 강화하였으나 여전히 WEP와 동일한 RC4 암호화 알고리즘을 사용하는 약점이 있다. ③ IEEE 802.1x는 802.11b의 사용자 인증 취약성을 보완한 프레임워크로, EAP를 통해 다양한 사용자 인증 메커니즘을 지원한다.

정답 ④