# 2014년 국가직 9급 정보보호론 풀이

by 호이호이꿀떡

## 정답 체크

| 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 |
|---|---|---|---|---|---|---|---|---|---|
| ③ | ① | ③ | ③ | ④ | ① | ④ | ② | ④ | ① |
| **11** | **12** | **13** | **14** | **15** | **16** | **17** | **18** | **19** | **20** |
| ④ | ③ | ② | ② | ④ | ③ | ① | ② | ④ | ③ |

**문 1. 서비스 거부(DoS : Denial of Service) 공격 또는 분산 서비스 거부(DDoS : Distributed DoS) 공격에 대한 설명으로 옳지 않은 것은?**

① TCP SYN 이 DoS 공격에 활용된다.
② CPU, 메모리 등 시스템 자원에 과다한 부하를 가중시킨다.
③ 불특정 형태의 에이전트 역할을 수행하는 데몬 프로그램을 변조하거나 파괴한다.
④ 네트워크 대역폭을 고갈시켜 접속을 차단시킨다.

**답 ③**

③ DoS(서비스 거부 공격)는 시스템의 자원을 고갈시켜 제대로 사용하지 못하게 하는 공격으로 시스템을 파괴하지는 않는다(DDoS(분산 서비스 거부 공격)은 다수의 시스템을 이용해 DoS 공격을 하는 것)
데몬 프로그램을 변조하거나 파괴하는 공격은 악성코드나 바이러스 등이다.

**<오답 체크>** ① DoS 는 공격 방법에 따라, TCP SYN 패킷, ICMP echo 메시지, UDP 패킷 등이 사용된다.

②④ DoS 는 시스템 자원과 네트워크 대역폭을 고갈시켜 서버에 접속하려는 사용자가 제대로 서비스를 받지 못하도록 가용성을 떨어뜨리는 공격이다.


**문 2. 보안 프로토콜인 IPSec(IP Security)의 프로토콜 구조로 옳지 않은 것은?**

① Change Cipher Spec
② Encapsulating Security Payload
③ Security Association
④ Authentication Header

**답 ①**

① Change Cipher Spec(암호 사양 변경) 프로토콜은 SSL/TLS 의 프로토콜이다.

**<오답 체크>** ② Encapsulating Security Payload(ESP, 캡슐화 보안 페이로드)
대칭키 암호화를 통해, 기밀성과 무결성과 선택적 인증 제공

③ Security Association(SA, 보안 연계)
데이터의 안전한 전달을 위해 통신의 쌍방 간의 약속
암호 알고리즘, 키 교환 방법, 암호화 키 교환 주기 등 합의되어야 할 요소들의 집합을 의미함

④ Authentication Header(AH, 인증 헤더)
메시지 인증과 무결성 제공

**문 3. DRM(Digital Right Management)에 대한 설명으로 옳지 않은 것은?**

① 디지털 컨텐츠의 불법 복제와 유포를 막고, 저작권 보유자의 이익과 권리를 보호해 주는 기술과 서비스를 말한다.
② DRM 은 파일을 저장할 때, 암호화를 사용한다.
③ DRM 탬퍼 방지(tamper resistance) 기술은 라이센스 생성 및 발급관리를 처리한다.
④ DRM 은 온라인 음악서비스, 인터넷 동영상 서비스, 전자책, CD/DVD 등의 분야에서 불법 복제 방지 기술로 활용된다.

**답 ③**

디지털 저작권 관리(Digital rights management, DRM)는 각종 미디어의 출판자 또는 저작권자가 배포한 디지털 자료나 하드웨어의 사용을 제어하고 불법적인 유통을 방지하도록 사용되는 기술들을 의미한다.

③ 키 관리 및 라이선스 발급 관리를 담당하는 건 클리어링 하우스(Clearing House)이다.
DRM 탬퍼 방지(크랙 방지) 크랙에 의해 라이선스에 정의되지 않은 용도로 콘텐츠가 사용되는 것을 방지하는 기술이다.
DRM 탬퍼 프루핑(Tamper proofing)은 콘텐츠에 승인되지 않은 조작이 가해졌을 때, 위·변조 사항을 감지하여 콘텐츠를 이용하지 못하도록 하는 기술이다.

**문 4. 다음 설명에 해당하는 접근제어 모델은?**

> 조직의 사용자가 수행해야 하는 직무와 직무 권한 등급을 기준으로 객체에 대한 접근을 제어한다. 접근 권한은 직무에 허용된 연산을 기준으로 허용함으로 조직의 기능 변화에 따른 관리적 업무의 효율성을 높일 수 있다. 사용자가 적절한 직무에 할당되고, 직무에 적합한 접근 권한이 할당된 경우에만 접근할 수 있다.

① 강제적 접근제어(Mandatory Access Control)
② 규칙 기반 접근제어(Rule-Based Access Control)
③ 역할 기반 접근제어(Role-Based Access Control)
④ 임의적 접근제어(Discretionary Access Control

**답 ③**

③ 역할 기반 접근제어(RBAC, Role Based Access Control)
정보에 대한 사용자의 접근을 개별적인 신분이 아니라 조직 내 개인 역할에 따라 허용 여부를 결정하는 모델

**<오답 체크>** ①② 강제적 접근제어(MAC, Mandatory Access Control)
오직 관리자만이 객체과 자원들에 대한 접근 권한을 부여할 수 있다. 자원에 대한 접근은 주어진 보안레벨에 기반한다.
관리자가 규칙을 작성하기 때문에 규칙 기반 접근제어(Rule Based Access Control)이라고도 한다.

④ 임의적 접근제어(DAC, Discretionary Access Control)
정보의 소유자가 보안 등급을 결정하고 이에 대한 정보의 접근제어도 설정하는 모델이다.

**문 5. 공개키 암호에 대한 설명으로 옳지 않은 것은?**

① 공개키 인증서를 공개키 디렉토리에 저장하여 공개한다.
② 사용자가 증가할수록 필요한 비밀키의 개수가 증가하는 암호 방식의 단점을 해결할 수 있다.
③ 일반적으로 대칭키 암호방식보다 암호화 속도가 느리다.
④ $n$명의 사용자로 구성된 시스템에서는 $\frac{n(n-1)}{2}$ 개의 키가 요구된다.

**답 ④**

④ 대칭키에 해당하는 설명이다.
공개키는 $n$ 명의 사용자로 구성된 시스템에서는 $2n$ 개의 키가 요구된다.

**<오답 체크>** ① 공개키는 누구나 이용할 수 있도록 공개한다.
② 대칭키는 사용자가 증가할수록 필요한 비밀키의 개수는 기하급수적으로 증가하는데, 공개키는 언제나 사용자 한 명당 2 개의 키만 있으면 된다.
③ 공개키 방식은 대칭키 방식보다 키의 길이도 길고 암호화 속도도 느리다.

**문 6. 웹 서버 보안에 대한 설명으로 옳지 않은 것은?**

① 웹 애플리케이션은 SQL 삽입공격에 안전하다.
② 악성 파일 업로드를 방지하기 위하여 필요한 파일 확장자만 업로드를 허용한다.
③ 웹 애플리케이션의 취약점을 방지하기 위하여 사용자의 입력 값을 검증한다.
④ 공격자에게 정보 노출을 막기 위하여 웹 사이트의 맞춤형 오류 페이지를 생성한다.

**답 ①**

① SQL 삽입(SQL 인젝션, SQL injection)은 클라이언트의 입력 값을 조작하여 서버의 데이터베이스를 공격하는 것이다.
데스크톱 응용 프로그램뿐 아니라, 웹 애플리케이션이라도 사용자가 입력하는 SQL 쿼리의 문자열을 점검하지 않는다면, SQL 삽입 공격에 당할 수 있다.

**<오답 체크>** ② XSS(Cross-site Scripting, 크로스 사이트 스크립팅)이나 파일 업로드 취약점 공격에 대한 대응 방법이다.
③ SQL 삽입 공격에 대한 대응 방법이다.
④ 공격자는 서버나 웹 사이트의 에러 메시지의 내용을 분석하여 공격법을 찾는 데 활용한다. 따라서 오류 발생 시 임의로 작성한 오류 페이지를 보여주도록 하면, 정보 노출을 막을 수 있다.

**문 7. 「개인정보 보호법」상 개인정보 유출 시 개인정보처리자가 정보 주체에게 알려야 할 사항으로 옳은 것만을 모두 고르면?**

> ㄱ. 유출된 개인정보의 위탁기관 현황
> ㄴ. 유출된 시점과 그 경위
> ㄷ. 개인정보처리자의 개인정보 보관·폐기 기간
> ㄹ. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

① ㄱ, ㄴ ② ㄷ, ㄹ
③ ㄱ, ㄷ ④ ㄴ, ㄹ

**답 ④**

「개인정보 보호법」
제 34 조(개인정보 유출 통지 등)
① 개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 다음 각 호의 사실을 알려야 한다.
1. 유출된 개인정보의 항목
2. **유출된 시점과 그 경위**
3. 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
4. 개인정보처리자의 대응조치 및 피해 구제절차
5. **정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처**

② 개인정보처리자는 개인정보가 유출된 경우 그 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하여야 한다.

**문 8. PGP(Pretty Good Privacy)에 대한 설명으로 옳지 않은 것은?**

① PGP 는 전자우편용 보안 프로토콜이다.
② 공개키 암호 알고리즘을 사용하지 않고, 대칭키 암호화 알고리즘으로 메시지를 암호화한다.
③ PGP 는 데이터를 압축해서 암호화한다.
④ 필 짐머만(Philip Zimmermann)이 개발하였다.

**답 ②**

**PGP**(Pretty Good Privacy)는 전자우편 서비스에 대한 보안 기술로, 인증기관을 사용하지 않고 개개인의 신뢰 관계를 이용하여 인증하는 방식이다.

② PGP 는 대칭키와 공개키를 모두 사용하는 하이브리드 방식으로 메시지를 암호화한다.
대칭키(세션키)로 메시지를 암호화한 후 공개키로 대칭키(세션키)를 암호화한다.
하지만 보기의 설명이 어떻게 읽느냐에 따라 해석이 달라질 수 있어 정확하지는 않은 문장이다.
또한 PGP 는 하이브리드 암호화 방식이 아닌, 대칭키 단독 암호화 방식으로도 이용할 수 있다.
하지만 나머지 보기들이 모두 맞기 때문에 가장 적절하지 않은 답은 ②번뿐이다.

**<오답 체크>** ③ PGP 는 데이터를 먼저 압축을 한 후, 압축된 메시지를 암호화한다.

**문 9. 컴퓨터 바이러스에 대한 설명으로 옳지 않은 것은?**

① 트랩도어(Trapdoor)는 정상적인 인증 과정을 거치지 않고 프로그램에 접근하는 일종의 통로이다.
② 웜(Worm)은 네트워크 등의 연결을 통하여 자신의 복제품을 전파한다.
③ 트로이목마(Trojan Horse)는 정상적인 프로그램으로 가장한 악성프로그램이다.
④ 루트킷(Rootkit)은 감염된 시스템에서 활성화되어 다른 시스템을 공격하는 프로그램이다.

**답 ④**

④ 좀비 PC 에 대한 설명이다.
좀비 PC 는 악성코드에 감염되어 해커의 공격에 사용되는 컴퓨터를 뜻한다. 해커는 다수의 좀비 PC 를 감염시켜 봇넷(botnet)을 구성한 뒤 공격 준비가 완료되면 좀비 PC 를 활성화해 목표 시스템을 공격하는 데 이용한다.
루트킷(Rootkit)은 해커들이 컴퓨터나 또는 네트웍에 침입한 사실을 숨긴 채 관리자용 접근 권한(루트 권한)을 획득하는데 사용하는 도구의 모음이다.

**<오답 체크>** ② 웜(Worm)은 시스템에 직접적인 영향은 미치지 않는 악성 프로그램이다. 다른 파일에 기생하지 않고, 스스로 자가 복제하는 성질을 가졌다.

③ 트로이목마(Trojan Horse)는 정상적인 프로그램으로 가장한 악성 프로그램으로, 다른 시스템으로 전파되지는 않는다. 트로이목마는 보통 해커들이 대상 컴퓨터의 인증이나 백신을 우회하여 시스템 내부에 침투하기 위해 사용한다.

• 바이러스(Virus)는 스스로를 복제하여 컴퓨터를 감염시켜 피해를 주는 악성 프로그램으로, 한 시스템에서 다른 시스템으로 전파되는 성질이 있다.

**문 10.「정보보호 관리체계 인증 등에 관한 고시」에 의거한 정보보호 관리체계(ISMS)에 대한 설명으로 옳지 않은 것은?**

① 정보보호관리과정은 정보보호정책 수립 및 범위설정, 경영진 책임 및 조직구성, 위험관리, 정보보호대책 구현 등 4 단계 활동을 말한다.
② 인증기관이 조직의 정보보호 활동을 객관적으로 심사하고, 인증한다.
③ 정보보호 관리체계는 조직의 정보 자산을 평가하는 것으로 물리적 보안을 포함한다.
④ 정보 자산의 기밀성, 무결성, 가용성을 실현하기 위하여 관리적. 기술적 수단과 절차 및 과정을 관리, 운용하는 체계이다

**답 ①**

① 정보보호관리과정은 4 단계가 아니라 5 단계로 구성되어 있다.

「정보보호 관리체계 인증 등에 관한 고시」
제 2 조(용어의 정의)
6. "정보보호관리과정(이하 '관리과정'이라 한다)"이란 정보보호 관리체계를 수립·운영하기 위하여 유지·관리하여야 할 과정으로 다음 각 목의 5 단계 활동을 말한다.
가. 정보보호정책 수립 및 범위설정
나. 경영진 책임 및 조직구성
다. 위험관리
라. 정보보호대책 구현
마. 사후관리

**<오답 체크>** ② 인증기관의 업무
인증심사 결과의 심의
인증서 발급・관리
인증의 사후관리
정보보호 관리체계 인증심사원의 양성 및 자격관리
그 밖에 정보보호 관리체계 인증에 관한 업무

**문 11. 공격자가 자신이 전송하는 패킷에 다른 호스트의 IP 주소를 담아서 전송하는 공격은?**

① 패킷 스니핑(Packet Sniffing)
② 스미싱(Smishing)
③ 버퍼 오버플로우(Buffer Overflow)
④ 스푸핑(Spoofing)

**답 ④**

④ **스푸핑(spoofing)**은 네트워크 상에서 전송하는 패킷의 출발지 주소 등를 조작해 자신의 신분을 숨기고 다른 사용자로 위장해 공격 대상에 불법 접근하여 정보를 빼내는 것이다.

**<오답 체크>** ① **스니핑(sniffing)**은 네트워크 상에서 자신이 아닌 다른 상대방들의 패킷 교환을 엿듣는 것을 말한다.

② **스미싱(Smishing)**
문자 메시지(SMS)와 피싱(Phishing)의 합성어로, 스마트폰 사용자에게 가짜 사이트 주소 링크를 문자 메시지(SMS)로 보내 스마트폰 정보나 소액결제를 유도하는 공격이다.

③ **Buffer Overflow(버퍼 오버플로우)** 공격
프로그램에 미리 할당된 버퍼보다 더 많은 양의 데이터를 집어넣어, 다른 메모리 영역을 침범하여 데이터를 변조시키는 공격이다.

**문 12. 정보보호의 주요 목적에 대한 설명으로 옳지 않은 것은?**

① 기밀성(confidentiality)은 인가된 사용자만이 데이터에 접근할 수 있도록 제한하는 것을 말한다.
② 가용성(availability)은 필요할 때 데이터에 접근할 수 있는 능력을 말한다.
③ 무결성(integrity)은 식별, 인증 및 인가 과정을 성공적으로 수행했거나 수행 중일 때 발생하는 활동을 말한다.
④ 책임성(accountability)은 제재, 부인방지, 오류제한, 침입탐지 및 방지, 사후처리 등을 지원하는 것을 말한다.

**답 ③**

③ 무결성(Integrity)은 허가받지 않은 사용자에 의해 데이터가 위•변조 되지 않아야 하는 것을 말한다.

**문 13. 네트워크 각 계층별 보안 프로토콜로 옳지 않은 것은?**

① 네트워크 계층(network layer) : IPSec
② 네트워크 계층(network layer) : FTP
③ 응용 프로그램 계층(application layer) : SSH
④ 응용 프로그램 계층(application layer) : S/MIME

**답 ②**

② FTP(File Transfer Protocol, 파일 전송 프로토콜)는 서버와 클라이언트 사이의 파일을 전송하기 위한 프로토콜로, 네트워크 계층이 아니라 응용 프로그램 계층에 속한다.
또한 FTP 는 보안 프로토콜도 아니다.
응용 프로그램 계층에서 FTP 를 암호화하는 보안 프로토콜은 SSH(Secure Shell)이다.

계층별 보안 프로토콜
PPTP - 2 계층
L2F - 2 계층
L2TP - 2 계층
IPSec - 3 계층
SSL/TLS - 4 계층
SOCKSv5 - 5 계층
SSH(Secure Shell) - 7 계층

**문 14. 방화벽(firewall)에 대한 설명으로 옳지 않은 것은?**

① 패킷 필터링 방화벽은 패킷의 출발지 및 목적지 IP 주소, 서비스의 포트 번호 등을 이용한 접속제어를 수행한다.
② 패킷 필터링 기법은 응용 계층(application layer)에서 동작하며, WWW 와 같은 서비스를 보호한다.
③ NAT 기능을 이용하여 IP 주소 자원을 효율적으로 사용함과 동시에 보안성을 높일 수 있다.
④ 방화벽 하드웨어 및 소프트웨어 자체의 결함에 의해 보안상 취약점을 가질 수 있다.

**답 ②**

② 패킷 필터링 방화벽이 적용된 라우터를 스크리닝 라우터(Screening Router)라고 하며, 3 계층인 네트워크 계층과 4 계층인 전송 계층 사이에서 동작한다.

**<오답 체크>** ③ NAT(Network Address Translation)는 공인 IP 주소를 다수가 함께 공유하여 사용할 수 있도록 주소 변환을 해주는 서비스다.
NAT 환경에서는 여러 사용자들이 공인된 하나의 외부 IP 주소를 공유하기 때문에 내부 주소가 드러나지 않아 보안성을 높이는 효과가 있다.

**문 15. 해시 함수(hash function)에 대한 설명으로 옳지 않은 것은?**

① 임의 길이의 문자열을 고정된 길이의 문자열로 출력하는 함수이다.
② 대표적인 해시 함수는 MD5, SHA-1, HAS-160 등이 있다.
③ 해시 함수는 메시지 인증과 메시지 부인방지 서비스에 이용된다.
④ 해시 함수의 충돌 회피성은 동일한 출력을 산출하는 서로 다른 두 입력을 계산적으로 찾기 가능한 성질을 나타낸다.

**답 ④**

④ 충돌 회피성(collision resistance)은 출력 해시값이 같은 임의의 서로 다른 두 입력을 계산적으로 찾기 불가능한 성질을 말한다(= 강한 충돌 내성)

**<오답 체크>** ① 해시 함수는 가변 길이의 입력을 받아, 고정 길이의 값을 출력한다.
HAVAL 해시 함수처럼 가변 길이 출력하는 경우도 있지만, 일반적으로 해시 함수의 특징을 얘기할 땐 고정 길이를 출력한다고 말한다.

③ 해시 함수와 대칭키를 이용하여 메시지 인증 코드(MAC: Message Authentication Code)를 생성해 무결성과 출처 인증(송신자에 대한 인증)이 가능하다. (MAC 은 부인 방지는 불가능하다)
전자 서명에도 해시를 사용하며 이를 통해 부인 방지 기능을 제공할 수 있다. 대개 메시지가 아닌 해시값에 전자 서명을 한다.

**문 16. 「정보통신기반 보호법」에 대한 설명으로 옳지 않은 것은?**

① 주요정보통신기반시설을 관리하는 기관의 장은 침해사고가 발생하여 소관 주요정보통신기반시설이 교란·마비 또는 파괴된 사실을 인지한 때에는 관계 행정기관, 수사기관 또는 한국인터넷진흥원에 그 사실을 통지하여야 한다.
② "전자적 침해행위"라 함은 정보통신기반시설을 대상으로 해킹, 컴퓨터 바이러스, 서비스 거부 또는 고출력 전자기파 등에 의한 공격행위를 말한다.
③ 관리기관의 장은 소관분야의 정보통신기반시설 중 전자적 침해행위로부터의 보호가 필요하다고 인정되는 시설을 주요 정보통신기반시설로 지정할 수 있다.
④ 주요정보통신기반시설의 취약점 분석·평가 방법 등에 관하여 필요한 사항은 대통령령으로 정한다.

**답 ③**

③ 관리기관의 장(X) -> 중앙행정기관의 장(○)
제 8 조(주요정보통신기반시설의 지정 등) 제 1 항
**중앙행정기관의 장**은 소관분야의 정보통신기반시설중 다음 각호의 사항을 고려하여 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정할 수 있다.

**<오답 체크>** ① 제 13 조(침해사고의 통지) 제 1 항
관리기관의 장은 침해사고가 발생하여 소관 주요정보통신기반시설이 교란·마비 또는 파괴된 사실을 인지한 때에는 관계 행정기관, 수사기관 또는 인터넷진흥원(이하 "관계기관등"이라 한다)에 그 사실을 통지하여야 한다. 이 경우 관계기관등은 침해사고의 피해확산 방지와 신속한 대응을 위하여 필요한 조치를 취하여야 한다.

② 제 2 조(정의)의 2
"전자적 침해행위"라 함은 정보통신기반시설을 대상으로 해킹, 컴퓨터바이러스, 논리·메일폭탄, 서비스거부 또는 고출력 전자기파 등에 의하여 정보통신기반시설을 공격하는 행위를 말한다.

③ 제 8 조(주요정보통신기반시설의 지정 등) 제 1 항
중앙행정기관의 장은 소관분야의 정보통신기반시설중 다음 각호의 사항을 고려하여 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정할 수 있다.

④ 제 9 조(취약점의 분석·평가) 제 5 항
주요정보통신기반시설의 취약점 분석·평가의 방법 및 절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

**문 17. 「개인정보 보호법」상 공공기관에서의 영상정보처리기기 설치 및 운영에 대한 설명으로 옳지 않은 것은?**

① 공공기관의 사무실에서 민원인의 폭언·폭행 방지를 위해 영상정보처리기기를 설치 및 녹음하는 것이 가능하다.
② 영상정보처리기기의 설치 목적과 다른 목적으로 영상정보 처리기기를 임의로 조작하거나 다른 곳을 비춰서는 안 된다.
③ 영상정보처리기기운영자는 영상정보처리기기의 설치·운영에 관한 사무를 위탁할 수 있다.
④ 개인정보 보호법 에서 정하는 사유를 제외하고는 공개된 장소에 영상정보처리기기를 설치하는 것은 금지되어 있다.

**답 ①**

① 녹음기능은 사용할 수 없다.

「개인정보 보호법」
제 25 조(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

④ 다음 각 호의 사항이 포함된 안내판을 설치하는 등 필요한 조치를 하여야 한다.
1. 설치 목적 및 장소
2. 촬영 범위 및 시간
3. 관리책임자 성명 및 연락처
4. 그 밖에 대통령령으로 정하는 사항

⑤ 영상정보처리기기운영자는 영상정보처리기기의 설치 목적과 다른 목적으로 영상정보처리기기를 임의로 조작하거나 다른 곳을 비춰서는 아니 되며, 녹음기능은 사용할 수 없다.

⑧ 영상정보처리기기운영자는 영상정보처리기기의 설치·운영에 관한 사무를 위탁할 수 있다. 다만, 공공기관이 영상정보처리기기 설치·운영에 관한 사무를 위탁하는 경우에는 대통령령으로 정하는 절차 및 요건에 따라야 한다.

**문 18. 국제공통평가기준(Common Criteria)에 대한 설명으로 옳지 않은 것은?**

① 정보보호 측면에서 정보보호 기능이 있는 IT 제품의 안전성을 보증·평가하는 기준이다.
② 국제공통평가기준은 소개 및 일반모델, 보안기능요구사항, 보증요구사항 등으로 구성되고, 보증 등급은 5 개이다.
③ 보안기능요구사항과 보증요구사항의 구조는 클래스로 구성된다.
④ 상호인정협정(CCRA:Common Criteria Recognition Arrangement)은 정보보호제품의 평가인증 결과를 가입 국가 간 상호 인정하는 협정으로서 미국, 영국, 프랑스 등을 중심으로 시작되었다.

**답 ②**

국제공통평가기준(CC, Common Criteria)은 국가마다 서로 다른 정보보호시스템 평가기준을 연동하고 평가결과를 상호인증하기 위해 제정된 평가기준이다.
② 국제 공통평가기준(CC)에서 정의한 제품의 보증등급은 EAL1 에서 EAL7 까지 7 단계이다.

**문 19. 위험관리 요소에 대한 설명으로 옳지 않은 것은?**

① 위험은 위협 정도, 취약성 정도, 자산 가치 등의 함수관계로 산정할 수 있다.
② 취약성은 자산의 약점(weakness) 또는 보호대책의 결핍으로 정의할 수 있다.
③ 위험 회피로 조직은 편리한 기능이나 유용한 기능 등을 상실할 수 있다.
④ 위험관리는 위협 식별, 취약점 식별, 자산 식별 등의 순서로 이루어진다.

**답 ④**

위험관리 단계
1 단계 자산(Asset) 식별: 나에게 소중한 대상은 무엇인가
2 단계 위협(Threat) 분석: 소중한 대상(자산)에 해를 끼칠 수 있는 요소는 무엇인가
3 단계 취약성(Vulnerability) 분석: 위협에 대한 약점은 무엇인가
4 단계 위험(Risk) 평가: 얼마나 위험한 것인가
5 단계 위험대응전략: 어떻게 위험에 대응할 것인가

**문 20. 다음 설명에 해당하는 컴퓨터 바이러스는?**

> 산업 소프트웨어와 공정 설비를 공격 목표로 하는 극도로 정교한 군사적 수준의 사이버 무기로 지칭된다. 공정 설비와 연결된 프로그램이 논리제어장치(Programmable Logic Controller)의 코드를 악의적으로 변경하여 제어권을 획득한다. 네트워크와 이동저장매체인 USB 를 통해 전파되며, SCADA (Supervisory Control and Data Acquisition) 시스템이 공격 목표이다.

① 오토런 바이러스(Autorun virus)
② 백도어(Backdoor)
③ 스턱스넷(Stuxnet)
④ 봇넷(Botnet)

**답 ③**

③ **스턱스넷**(Stuxnet)
독일 지멘스(SIEMENS)사의 스카다(SCADA) 시스템을 목표로 개발된 악성 소프트웨어로, 스카다 시스템을 감염시켜 장비를 제어하고 감시하는 특수한 코드를 내부에 담고 있다.
(스카다 시스템은 원자력 발전소와 송·배전망, 화학 공장, 송유·가스관과 같은 산업 기반 시설에 사용되는 제어 시스템으로 작업공정을 감시하고 제어하는 역할을 한다.)

**<오답 체크>** ① **오토런 바이러스**(Autorun virus)
'autorun.inf' 파일이나, 시스템의 레지스트리에 등록돼 자동 실행되도록 설정된 악성코드로, 주로 USB 같은 이동형 저장 장치에 복사되어 전파된다. 폴더를 숨기거나 더블 클릭을 방해하는 등의 악성 행위를 한다.

② **백도어**(Backdoor)는 인증 과정을 거치지 않고, 접근할 수 있도록 만든 비밀 통로이다. = 트랩도어(Trapdoor)

④ **봇넷**(Botnet)
악성코드에 감염되어 공격자에게 권한이 양도된 좀비 PC 들의 집합을 가리킨다.
공격자는 다수의 좀비 PC 를 감염시켜 구성한 봇넷(botnet)을 이용하여 목표 시스템을 공격하는데, 자신의 존재를 숨기고 동시다발적으로 공격하는 효과를 얻을 수 있다.