2019년 서울시 9급 정보보호론 풀이

by 호이호이꿀떡

정답 체크

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

1. 해시와 메시지 인증코드에 대한 <보기>의 설명에서 ㉠, ㉡에 들어갈 말을 순서대로 나열한 것은?

> 〈 보 기 〉
> 해시와 메시지 인증코드는 공통적으로 메시지의 (㉠)을 검증할 수 있지만, 메시지 인증코드만 (㉡) 인증에 활용될 수 있다.

㉠	㉡
① 무결성	상호
② 무결성	서명자
③ 비밀성	상호
④ 비밀성	서명자

㉠ 해시와 메시지 인증 코드(MAC)는 무결성을 검증하기 위해 사용한다.

㉡ 메시지 인증 코드 계산에는 비밀키(대칭키)가 들어가기 때문에 통신 상호간의 인증이 가능하다. 여기서 상호간 인증은 보낸 보낸 사람이 누구인지 내가 확인할 수 있다는 의미이다.

단 대칭키를 사용하기 때문에 송신자가 누구인지는 당사자들만 알 뿐, 제3자에게 증명할 수는 없다. 따라서 서명자 인증은 불가능하다. 서명자 인증은 공개키와 개인키를 이용해야 한다.

답 ①

2. 바이러스의 종류 중에서 감염될 때마다 구현된 코드의 형태가 변형되는 것은?

① Polymorphic Virus
② Signature Virus
③ Generic Decryption Virus
④ Macro Virus

◈ 바이러스 발전 단계 요약

▷ 1세대 원시형 바이러스(Primitive Virus)
프로그램 구조가 단순하고 고정 크기를 가지며, 분석이 상대적으로 쉬운 바이러스

▷ 2세대 암호화 바이러스(Encryption Virus)
백신 프로그램이 진단할 수 없도록 바이러스 프로그램의 일부 또는 대부분을 암호화시킨 바이러스

▷ 3세대 은폐형 바이러스(Stealth Virus)
자신을 은폐하고 사용자나 백신 프로그램에 거짓 정보를 제공하기 위해서 다양한 기법을 사용하는 바이러스
감염된 파일의 길이가 증가하지 않은 것처럼 보이게 하고, 백신 프로그램에게 감염되기 전의 내용을 보여줘 바이러스가 없는 것처럼 속인다.

▷ 4세대 갑옷형 바이러스(Armour Virus)
백신 프로그램으로부터 숨기보다는 여러 단계의 암호화와 다양한 기법을 동원하여 바이러스 분석을 어렵게 하고 백신 프로그램 개발을 지연시키며, 암호화를 푸는 부분조차 감염될 때마다 달라진다. 다형성(Polymorphic) 바이러스는 갑옷형 바이러스의 일종

▷ 5세대 매크로 바이러스(Macro virus)
매크로 기능이 있는 MS 사 오피스 제품군(워드, 엑셀, 파워포인트)이외에 비지오(Visio), 오토캐드(AutoCAD) 등 매크로 기능이 있는 응용 소프트웨어 안에서 실행되는 바이러스

① 갑옷형(Armour) 바이러의 일종인 다형성(Polymorphic) 바이러스에 대한 설명이다.

<오답 체크> ②③ 바이러스 시그니처(Virus Signature)는 오용탐지 기법에서 바이러스의 작동방식과 유형들을 수집하여 기록한 정보들을 의미하며, Generic Decryption은 암호화(encryption) 바이러스들을 처리하기 위한 방법들을 의미한다.
둘 다 바이러스의 명칭은 아니다.

답 ①

3. 침입탐지시스템(IDS)에 대한 설명으로 가장 옳지 않은 것은?

① 오용탐지는 새로운 침입 유형에 대한 탐지가 가능하다.
② 기술적 구성요소는 정보 수집, 정보 가공 및 축약, 침입 분석 및 탐지, 보고 및 조치 단계로 이루어진다.
③ 하이브리드 기반 IDS는 호스트 기반 IDS와 네트워크 기반 IDS가 결합한 형태이다.
④ IDS는 공격 대응 및 복구, 통계적인 상황 분석 보고 기능을 제공한다.

◈ 오용 탐지(Misuse Detection)
= 시그니처 기반(Signature Base)
= 지식 기반(Knowledge Base)
이미 발견되고 정립된 공격 패턴을 미리 입력해 두고 그에 해당하는 패턴을 탐지
오탐율이 낮고 비교적 효율적이나 알려진 공격 이외는 탐지 불가능
전문가 시스템(Expert System)의 지식 DB를 이용한 IDS
Zero Day attack(제로 데이 공격)에 취약
◈ 이상 탐지(Anomaly Detection IDS)
= 행위 기반(Behavior)
= 통계적 탐지(Statistical Detection)
정상 패턴을 DB에 등록해두고, 정상에서 벗어나는 행위를 탐지(임계치 설정)
알려지지 않은 공격인 제로 데이 공격(zero day attack) 탐지 가능
오탐율 높고, 임계치 설정이 어려움

① 오용탐지는 새로운 유형의 공격을 탐지하기 부적합하다.
<오답 체크> ③ NIDS(Network IDS, 네트워크 기반 IDS) 네트워크 트래픽을 감시하고 패킷을 분석하는 IDS 시스템으로, 별도의 호스트에 설치한다.
HIDS(Host IDS, 호스트 기반 IDS)는 컴퓨터 시스템의 동작이나 상태 등 컴퓨터 시스템의 내부를 감시하고 분석하는 데 더 중점을 두는 IDS 시스템으로, 기존 서버에 설치되며 별도의 호스트가 필요 없다.
Hybrid Based IDS는 NIDS와 HIDS를 결합한 형태

답 ①

4. <보기>에서 블록암호 모드 중 초기 벡터(Initialization Vector)가 필요하지 않은 모드를 모두 고른 것은?

〈 보 기 〉
ㄱ. CTR 모드 ㄴ. CBC 모드 ㄷ. ECB 모드

① ㄱ ② ㄷ ③ ㄴ, ㄷ ④ ㄱ, ㄴ, ㄷ

ㄷ. ECB 모드는 다른 키 값이나 블록과는 상관없이 현재의 블록 자체만 암호화하는 방식이기 때문에 초기화 벡터가 필요 없다.
<오답 체크> ㄴ. 블록 암호 알고리즘 중 CBC, CFB 모드는 암호화 과정에서 이전 단계에서 넘어온 값과 XOR 연산을 수행한다. 이때 첫 블록은 이전 단계 블록이 없기 때문에 초기화 벡터(IV, Initialization Vector)라는 값을 생성해 XOR 연산을 한다.
OFB 모드는 키 스트림을 생성하기 위해 초기화 벡터 값을 계속 암호화해 나가는 방식을 사용한다.
ㄱ. CTR 모드의 경우 1씩 증가하는 카운터를 암호화해 키 스트림을 얻는 방식인데, 이 때 초기값으로 사용하는 것을 **nonce** (number used once)라고 한다. CTR 모드에서는 정확히 초기화 벡터라는 표현을 쓰진 않지만, 초기화 벡터와 같은 기능을 하기 때문에 초기화 벡터의 일종으로 보기도 한다. 문제에 따라 융통성 있게 풀어야 한다.

답 ②

◈ **ECB**(electronic codebook, 전자 코드북) 모드
가장 간단한 구조로, 암호화하려는 메시지를 여러 블록으로 나누어 각각 암호화하는 방식이다.
◈ **CBC**(cipher-block chaining, 암호 블록 체인) 모드
평문 블록을 이전 단계의 암호문 블록과 XOR 한 후 암호화한다.
첫 번째 평문 블록의 경우에는 초기화 벡터(IV)와 XOR 한 후 암호화한다.
초기화 벡터가 같은 경우 출력 결과가 같기 때문에, 매 암호화마다 다른 초기화 벡터를 사용해야 한다.
◈ **CFB**(cipher feedback, 암호 피드백) 모드
CBC의 변형으로, 이전 단계의 암호문 블록을 암호화한 후 현재의 평문 블록과 XOR 한다.
첫 번째 평문 블록의 경우에는 초기화 벡터(IV)를 암호화한 것과 XOR 한다.
◈ **OFB**(output feedback, 출력 피드백) 모드
초기화 벡터(IV)를 매 단계마다 암호화해가며 스트림 암호를 생성한 후, 생성한 스트림 암호와 평문 블록을 XOR하여 암호문 블록을 생성한다.
◈ **CTR**(Counter, 카운터) 모드
1씩 증가하는 카운터 값을 암호화하여 스트림 암호를 생성한 후, 생성한 스트림 암호와 평문 블록을 XOR하여 암호문 블록을 생성한다.

5. 스트림 암호(Stream Cipher)에 대한 설명으로 가장 옳지 않은 것은?

① Key Stream Generator 출력값을 입력값(평문)과 AND 연산하여, 암호문을 얻는다.
② 절대 안전도를 갖는 암호로 OTP(One-Time Pad)가 존재한다.
③ LFSR(Linear Feedback Shift Register)로 스트림 암호를 구현할 수 있다.
④ Trivium은 현대적 스트림 암호로 알려져 있다.

◈ 스트림 암호(Stream Cipher)
연속적인 비트, 바이트, 단어들을 순차적으로 암호화하는 방식으로, 유사난수를 연속적으로 생성하여 암호화하려는 자료와 결합한다.
스트림 암호를 위해 생성한 비트열을 키 스트림(KeyStream)이라고 한다.

① 스트림 암호는 키 스트림과 평문을 **XOR** 연산하여 암호문을 출력한다. AND 연산을 할 경우, 평문의 비트가 0이면 암호문은 무조건 0이기 때문에 추정하기가 수월해진다.
<오답 체크> ② OTP(One-Time Pad, 일회성 패드)는 한 번만 사용하는 키 스트림으로, 평문과 동일한 길이를 가진다. 이상적인 스트림 암호라고 하며, 완전 안정성(Perfect Secrecy, 암호문을 보고 암호문에 대응되는 평문을 맞힐 수 있는 확률과 그냥 평문을 맞힐 확률이 같다)을 가진다.
③ 선형 피드백 시프트 레지스터(LFSR, Linear feedback shift register)는 입력되는 값이 이전 상태 값들의 선형 함수로 계산되는 구조의 레지스터이다. LFSR을 이용하면 어느 정도의 안전한 스트림 암호를 구현할 수 있다. 다만, 선형 구조이기 때문에 완벽한 난수 생성은 불가능하며, 생성되는 값들이 일정한 주기에 의해 반복된다.
④ Trivium은 유럽연합의 스트림 암호 공모 프로젝트인 eStream의 하드웨어 애플리케이션 부문에 선정된 암호 중 하나이다.
▷ eStream 선정 암호
소프트웨어 부문: HC-128, Rabbit, Salsa20/12, SOSEMANUK
하드웨어 부문: Grain, MICKEY, trivium

답 ①

6. <보기>에서 설명하는 DRM 구성요소는?

〈 보 기 〉
DRM의 보호 범위에서 유통되는 콘텐츠의 배포 단위로서 암호화된 콘텐츠 메타 데이터, 전자서명 등의 정보로 구성되어 있다. 또한, MPEG-21 DID 규격을 따른다.

① 식별자 ② 클리어링 하우스
③ 애플리케이션 ④ 시큐어 컨테이너

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

④ 시큐어 콘테이너(Secure Container)
DRM의 보호 범위 내에서 유통되는 콘텐츠의 배포 단위로, 아이덴티피어(identifier), 인크립트 콘텐츠(encrypted content), 메타데이터(metadata), 시그니쳐(signature) 등의 정보로 구성돼 있다. 허가되지 않은 사용자로부터 콘텐츠를 안전하게 보호할 수 있도록 할 뿐만 아니라 배포 도중에 발생할 수 있는 위·변조의 위협을 차단하는 역할을 수행한다.
DID(Digital Item Declaration, 디지털 아이템 선언)은 MPEG-21 프레임워크에서 콘텐츠 배포와 거래의 기본단위가 되는 디지털 아이템을 표현하는 방법을 정의한 것이다. 현재 MPEG는 멀티미디어 저작권 보호와 전자상거래를 위해 MPEG-21 표준화를 제정하였고, 따라서 DRM 역시 이 표준화를 따른다.
<오답 체크> ② 클리어링 하우스(Clearing House)는 키(key)와 라이선스(license) 발급을 관리한다.

답 ④

7. 이더넷(Ethernet)상에서 전달되는 모든 패킷(Packet)을 분석하여 사용자의 계정과 암호를 알아내는 것은?

① Nessus ② SAINT
③ Sniffing ④ IPS

③ **Sniffing**(스니핑)
다른 상대방들의 패킷 교환을 엿듣고 분석하여, 공격 대상자의 정보를 알아내는 것

<오답 체크> ① **NESSUS**는 네트워크 취약성 분석 도구

② **SAINT**(Security Administrators's Integrated Network Tool)는 미국의 보안컨설팅업체 World Wide DIGITAL SECURITY, Inc. 에서 1998년 6월에 개발한 시스템 관리자용 네트워크 진단도구로, SATAN을 기반으로 개발되었다.

④ **IPS**(Intrusion Prevention Systems, 침입 방지 시스템)
네트워크를 통해서 외부로부터 들어오는 악의적인 세션을 차단하고 세션 기반 탐지를 지원한다. IDS와 달리, 공격의 탐지뿐만 아니라 공격의 수행을 근본적으로 방어하는 것이 주목적이다.

답 ③

8. 리눅스 시스템에서 패스워드 정책이 포함되고, 사용자 패스워드가 암호화되어 있는 파일은?

① /etc/group ② /etc/passwd
③ /etc/shadow ④ /etc/login.defs

③ 패스워드가 암호화되거나 해시값으로 저장되는 파일은 /etc/shadow 파일이다.

<오답 체크> ① /etc/group 파일에는 그룹에 대한 정보가 들어있다.

② /etc/passwd 에는 사용자의 기본 정보가 평문 형태로 저장된다.

④ /etc/login.defs 는 사용자 계정 설정과 관련된 기본값을 정의한 파일이다.

답 ③

9. 타원곡선 암호에 대한 설명으로 가장 옳지 않은 것은?

① 타원곡선 암호의 단점은 보안성 향상을 위하여 키 길이가 길어진다는 것이다.
② 타원곡선에서 정의된 연산은 덧셈이다.
③ 타원곡선을 이용하여 디피-헬먼(Diffie-Hellman) 키 교환을 수행할 수 있다.
④ 타원곡선은 공개키 암호에 사용된다

① 타원곡선 암호는 RSA나 ElGamal 같은 기존의 공개키 암호 알고리즘에 비해 키의 길이가 짧다는 장점이 있다. 이 덕분에 데이터 전송능력과 계산능력이 부족한 무선 통신 환경에서 유용하게 쓰인다.

<오답 체크> ② 타원곡선 암호 연산에서는 덧셈만으로 충분하다.

③ 타원곡선 방식의 디피 헬만 키 교환도 있다 정도만 알아두고, 자세한 과정은 생략해도 된다.

◈ 타원곡선 디피-헬만(Elliptic-curve Diffie-Hellman)

1. 앨리스와 밥은 기준 좌표 g 를 선택해 교환한다.
2. 앨리스는 (d_A, Q_A)의 키쌍을 가진다.
   d는 1부터 n-1 사이의 정수이며, Q는 d×g 값이다.
   (d_A는 개인키, Q_A는 공개키)
3. 밥도 마찬가지 계산을 통해 (dB, QB)의 키쌍을 가진다.
   (d_B는 개인키, Q_B는 공개키)
4. 앨리스는 자신의 개인키와 밥의 공개키를 곱한다.
   $d_A \times Q_B = d_A \times d_B \times g = x_k$
5. 밥 역시 자신의 개인키와 앨리스의 공개키를 곱한다.
   $d_B \times Q_A = d_B \times d_A \times g = x_k$
6. 이로써 둘은 x_k 라는 공통의 비밀키를 갖는다.

④ ◈ 비대칭키 암호(공개키 암호) 알고리즘
RSA : 소인수분해
Rabin : 소인수분해
ElGamal : 이산대수
ECC : 타원곡선 상의 이산대수
Schnorr : 이산대수, ElGamal에 기반, 짧은 키 길이
DSA : 이산대수, Schnorr의 응용
DSS : 이산대수, 전자서명 전용
ECDSA : 내부적으로 타원곡선
Knapsack : 부분집합의 합을 구하는 문제
(NP-complete 문제)
KCDSA : 국산, 국내표준
ECKDSA : 국산, 내부적으로 타원곡선, 소규모, 무선

답 ①

10. 영지식 증명(Zero-Knowledge Proof)에 대한 설명으로 가장 옳지 않은 것은?

① 영지식 증명은 증명자(Prover)가 자신의 비밀 정보를 노출하지 않고 자신의 신분을 증명하는 기법을 의미한다.
② 영지식 증명에서 증명자 인증 수단으로 X.509 기반의 공개키 인증서를 사용할 수 있다.
③ 최근 블록체인상에서 영지식 증명을 사용하여 사용자의 프라이버시를 보호하고자 하며, 이러한 기술로 zk-SNARK가 있다.
④ 영지식 증명은 완정성(Completeness), 건실성(Soundness), 영지식성(Zero-Knowledgeness) 특성을 가져야 한다.

▷ **영지식증명**(Zero-Knowledge Proof)은 증명자(prover)가 자신이 알고 있는 지식과 정보를 공개하지 않으면서, 그 지식을 알고 있다는 사실을 검증자(verifier)에게 증명하는 방식이다.

② X.509 기반의 공개키 인증서는 공개키 기반 구조(PKI) 환경에서 상대방의 공개키가 정당한 것인지 아닌지를 구별하기 위해 사용한다.

<오답 체크> ③ 암호화폐 거래에서 거래의 익명성을 확보하기 위해 영지식 증명을 활용하기도 한다. 영지식 증명을 사용한 대표적인 암호화폐로 지캐시(Zcash)가 있다. 지캐시는 영지식증명을 기술을 기반으로 한 영지식 스나크(zk-SNARKs)라는 알고리즘을 사용하는데, 이는 타원곡선 암호화를 이용하여 보다 빠르고 간결하게 인증을 할 수 있다.

④ ○ 완전성(completeness): 어떤 문장이 참이면, 정직한 증명자는 정직한 검증자에게 이 사실을 납득시킬 수 있어야 한다.
○ 건실성(soundness): 어떤 문장이 거짓이면, 어떠한 부정직한 증명자라도 정직한 검증자에게 이 문장이 사실이라고 납득시킬 수 없어야 한다.
○ 영지식성(zero-knowledgeness): 어떤 문장이 참이면, 검증자는 문장의 참 거짓 이외에는 아무것도 알 수 없어야 한다.

답 ②

11. 「개인정보 보호법」상 주민등록번호의 처리에 대한 설명으로 가장 옳지 않은 것은?

① 개인정보처리자는 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 암호화 조치를 통하여 안전하게 보관하여야 한다.

② 행정안전부장관은 개인정보처리자가 처리하는 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손된 경우에는 5억원 이하의 과징금을 부과·징수할 수 있으나, 개인정보처리자가 안전성 확보에 필요한 조치를 다한 경우에는 그러하지 아니하다.

③ 개인정보처리자는 정보주체가 인터넷 홈페이지를 통하여 회원으로 가입하는 단계에서는 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하여야 한다.

④ 개인정보처리자로부터 주민등록번호를 제공받은 자는 개인정보 보호 위원회의 심의·의결을 거쳐 제공받은 주민등록번호를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다.

④「개인정보 보호법」제18조(개인정보의 목적 외 이용 · 제공 제한) ②항

제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다. 다만, 제5호부터 제9호까지의 경우는 공공기관의 경우로 한정한다.

5. 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의 · 의결을 거친 경우

개인정보(주민등록번호 포함)을 개인정보보호위원회의 심의·의결을 거쳐 제3자에게 제공할 수는 있으나, 이는 정보주체 또는 제3자의 이익을 부당하게 침해하지 않으며 개인정보를 제공하지 않으면 다른 법률에서 정한 소관 업무를 수행할 수 없는 경우의 공공기관에 한해서만 가능하다.

따라서 ④번처럼 이러한 제한 규정을 언급하지 않고 단순하게 제공할 수 있다고만 표현하면 적절하지 않다.

<오답 체크> ①「개인정보 보호법」제24조의2 ②항

②「개인정보 보호법」제34조의2 ①항

③「개인정보 보호법」제24조의2 ③항

답 ④

제24조의2(주민등록번호 처리의 제한)

① 제24조제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다.

1. 법률·대통령령·국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우
2. 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우
3. 제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 행정안전부령으로 정하는 경우

② 개인정보처리자는 제24조제3항에도 불구하고 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 암호화 조치를 통하여 안전하게 보관하여야 한다. 이 경우 암호화 적용 대상 및 대상별 적용 시기 등에 관하여 필요한 사항은 개인정보의 처리 규모와 유출 시 영향 등을 고려하여 대통령령으로 정한다.

③ 개인정보처리자는 제1항 각 호에 따라 주민등록번호를 처리하는 경우에도 정보주체가 인터넷 홈페이지를 통하여 회원으로 가입하는 단계에서는 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하여야 한다.

④ 행정안전부장관은 개인정보처리자가 제3항에 따른 방법을 제공할 수 있도록 관계 법령의 정비, 계획의 수립, 필요한 시설 및 시스템의 구축 등 제반 조치를 마련·지원할 수 있다.

제34조의2(과징금의 부과 등)

① 행정안전부장관은 개인정보처리자가 처리하는 주민등록번호가 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손된 경우에는 5억원 이하의 과징금을 부과 · 징수할 수 있다. 다만, 주민등록번호가 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손되지 아니하도록 개인정보처리자가 제24조제3항에 따른 안전성 확보에 필요한 조치를 다한 경우에는 그러하지 아니하다.

② 행정안전부장관은 제1항에 따른 과징금을 부과하는 경우에는 다음 각 호의 사항을 고려하여야 한다.

1. 제24조제3항에 따른 안전성 확보에 필요한 조치 이행 노력 정도
2. 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손된 주민등록번호의 정도
3. 피해확산 방지를 위한 후속조치 이행 여부

③ 행정안전부장관은 제1항에 따른 과징금을 내야 할 자가 납부기한까지 내지 아니하면 납부기한의 다음 날부터 과징금을 낸 날의 전날까지의 기간에 대하여 내지 아니한 과징금의 연 100분의 6의 범위에서 대통령령으로 정하는 가산금을 징수한다. 이 경우 가산금을 징수하는 기간은 60개월을 초과하지 못한다.

④ 행정안전부장관은 제1항에 따른 과징금을 내야 할 자가 납부기한까지 내지 아니하면 기간을 정하여 독촉을 하고, 그 지정한 기간 내에 과징금 및 제2항에 따른 가산금을 내지 아니하면 국세 체납처분의 예에 따라 징수한다.

⑤ 과징금의 부과 · 징수에 관하여 그 밖에 필요한 사항은 대통령령으로 정한다.

12. <보기>의 설명에 해당되는 공격 유형으로 가장 적합한 것은?

> SYN 패킷을 조작하여 출발지 IP 주소와 목적지 IP 주소를 일치시켜서 공격 대상에 보낸다. 이때 조작된 IP 주소는 공격 대상의 주소이다.

① Smurf Attack ② Land Attack
③ Teardrop Attack ④ Ping of Death Attack

② **Land 공격**(Land Attack)
패킷의 출발지 IP 주소와 목적지 IP 주소 값을 모두 공격자의 IP 주소 값으로 만들어 전송하는 공격이다. 출발지 주소와 목적지 주소가 같기 때문에 이 패킷의 응답은 공격대상을 떠났다가 그대로 다시 공격대상에게 들어가고, SYN Flooding처럼 동시 사용자 수를 점유해버리며 CPU 자원을 고갈시킨다.

<오답 체크> ① **Smurf**(ICMP flooding) 공격
출발지 IP주소를 공격대상의 IP주소로 위장하여 ICMP Echo 메시지를 브로드캐스트함으로써, 공격대상으로 많은 양의 ICMP Echo 응답 패킷이 몰리게 만들어 시스템 자원이 고갈되도록 만드는 공격이다.

③ **Teardrop**
패킷의 순서번호가 중복되도록 조작하는 공격이다.
목표 대상 시스템은 이렇게 보내진 패킷들을 재조합하려고 시도하지만, 계속 실패하여 시스템 자원이 고갈되어 서비스 불능 상태에 빠진다.

④ **Ping of Death**
icmp 패킷을 정상보다 매우 크게 만들어 공격하는 DoS 공격이다.
크게 조작된 icmp 패킷은 라우터를 통과하는 동안 매우 작은 패킷으로 조각화(fragment)되어 공격 대상에 도달하는데, 공격 대상은 조각화된 패킷을 모두 처리하느라 과부하가 걸리게 된다.

답 ②

13. TLS 및 DTLS 보안 프로토콜에 대한 설명으로 가장 옳지 않은 것은?

① TLS 프로토콜에서는 인증서(Certificate)를 사용하여 인증을 수행할 수 있다.
② DTLS 프로토콜은 MQTT 응용 계층 프로토콜의 보안에 사용될 수 있다.
③ TLS 프로토콜은 Handshake · Change Cipher · SpecAlert 프로토콜과 Record 프로토콜 등으로 구성되어 있다.
④ TCP 계층 보안을 위해 TLS가 사용되며, UDP 계층 보안을 위해 DTLS가 사용된다.

▶ **SSL**(Secure Sockets Layer, 보안 소켓 레이어) 또는 **TLS**(Transport Layer Security, 전송 계층 보안)
응용 계층과 전송 계층 사이에서 통신 과정에서 종단간 보안과 클라이언트와 서버 간 상호 인증, 기밀성, 무결성 서비스를 제공하는 보안 프로토콜
인터넷 전자상거래를 위해 넷스케이프사가 개발한 것으로, 웹 브라우저와 웹 서버 간의 전자상거래 정보를 안전하게 전송하기 위한 프로토콜이다. SSL 3.0버전의 업그레이드 버전이 TLS 1.0이 된다.

② **MQTT**(Message Queuing Telemetry Transport)는 경량의 메시지 교환 프로토콜이다. 낮은 전력과 낮은 대역폭 환경에서도 사용할 수 있어, M2M(사물 통신)과 IoT(사물 인터넷) 등에서 사용되고 있다. MQTT는 TCP 기반 프로토콜이기 때문에 SSL/TLS를 적용하며, UDP 기반의 DTLS는 적용할 수 없다.

<오답 체크> ① X.509에서 규정된 공개키 인증서 교환에 의해 상대방에 대한 인증을 수행한다.

④ **DTLS**(Datagram Transport Layer Security, 데이터그램 전송 계층 보안)
UDP 환경에서는 TLS를 사용할 수 없는데, 이러한 문제를 해결하기 위해 TLS를 기반으로 이와 비슷한 보안 수준을 제공하도록 만든 프로토콜

답 ②

◈ **SSL/TLS 구조**

▷ 핸드셰이크 프로토콜(handshake protocol)
서버와 클라이언트가 서로를 인증하고 암호, MAC알고리즘 레코드 데이터 보호에 사용될 암호화 키를 협상

▷ 암호 사양 변경 프로토콜(change cipher spec protocol)
암호 알고리즘을 변경. 핸드셰이크 프로토콜에서 협의된 압축, MAC, 암호화 방식 등을 이후부터 적용하겠다는 것을 상대방에게 알려줌

▷ 경고 프로토콜(alert protocol)
에러 코드를 전송

▷ 애플리케이션 데이터 프로토콜(application data protocol)
HTTP를 포함한 다양한 상위계층의 보안 서비스 제공

▷ 레코드 프로토콜(record protocol)
SSL의 실제 데이터를 다루며, 데이터를 단편화 및 압축하고 MAC을 적용하고 암호화하여 이를 TCP에 전달

14. 무선 통신 보안 기술에 대한 설명으로 가장 옳지 않은 것은?

① 무선 네트워크 보안 기술에 사용되는 WPA2 기술은 AES/CCMP를 사용한다.
② 무선 네트워크에서는 인증 및 인가, 과금을 위해 RADIUS 프로토콜을 사용할 수 있다.
③ 무선 AP의 SSID값 노출과 MAC 주소 기반 필터링 기법은 공격의 원인이 된다.
④ 무선 네트워크 보안 기술인 WEP(Wired Equivalent Privacy) 기술은 유선 네트워크 수준의 보안성을 제공하므로 기존의 보안 취약성 문제를 극복했다.

○ **WEP** 방식
암호화를 위해 RC4 사용하며(암호키 계속 사용)
암호화와 인증에 동일한 키를 사용
○ **WPA** 방식
RC4-TKIP를 통한 암호화(암호키 주기적인 변경)
EAP를 통한 사용자 인증
48비트 길이의 초기벡터(IV) 사용
○ **WPA2** 방식
AES-CCMP 사용
EAP를 통한 사용자 인증

④ WEP는 초창기의 무선랜 보안 프로토콜로 유선 네트워크 수준의 보안성을 제공하기 위해 만들었으나, 현재는 많은 취약점이 드러나 거의 사용하지 않는다.

<오답 체크> ② 801.11i에서는 WiFi 단말기(Station, STA)들을 인증하기 위한 별도의 인증 서버가 존재한다. 인증을 위해 단말과 AP(Access Point) 사이는 802.1x/EAP 프로토콜을 사용하고, AP와 인증서버 사이는 RADIUS 프로토콜을 사용한다.
단말이 AP를 인증 요청을 신호를 보내면, AP는 그 요청을 인증 서버로 전송하여 인증 서버가 단말 인증을 한다.

③ **SSID**(Service Set Identifier, 무선 네트워크 이름)는 무선랜을 통해 전송되는 패킷들을 구별하기 위해 덧붙여지는 32바이트 길이의 고유 식별자로, 각각의 무선랜들을 구분해주는 일종의 무선 네트워크 중개기(공유기)의 주소이다.
특정 무선랜에 접속하려는 무선 장치들은 동일한 SSID를 사용해야 하며, SSID를 알지 못하면 접속할 수 없다.
그렇기 때문에 SSID를 불필요하게 노출시켜 공격자의 관심을 끌 필요는 없다.
MAC 주소 필터링은 유선 네트워크의 라우터처럼, 무선랜에서 신뢰할 수 있는 기기만 접속을 허용하도록 MAC 주소로 구별하여 접근을 통제하는 기법이다.
하지만 무선 네트워크 분석 도구를 이용하여 전파를 스캔하면, 어렵지 않게 무선 라우터와 AP, 여기 연결된 디바이스의 MAC 주소를 획득할 수 있어 스푸핑(spoofing)을 통해 MAC 주소를 변경할 수 있다. 오히려 MAC 필터링 과정으로 인해 새로운 기기를 추가하는 등 정상적인 사용자가 이용하기만 더 번거로워질 뿐이다.

다만, ③번은 문장이 굉장히 애매하게 쓰였다.
SSID 값 노출과 MAC 필터링이 공격의 원인이 된다고 하였는데, SSID 값 노출은 그 자체로 공격의 원인이 되며, MAC 필터링은 그 자체로는 공격의 원인이 되지 않으나 별 효과는 없는 대응책에 해당하기 때문이다.
또한 SSID 노출이 공격의 원인이라고 쓰였으나, SSID 값을 숨기는 것 역시 요즘에는 별 도움이 되지 않는 대응책으로 받아들여지고 있다.
차라리 '무선 AP의 SSID 값 노출과 필터링 미적용이 공격의 원인이 된다' 또는 '무선 AP의 SSID 값 숨김과 MAC 주소 기반 필터링 기법만으로는 공격을 방어하기 부족하다'라고 고치는 것이 더 올바른 표현이라 생각된다.
다만 ④번이 확실하게 틀린 내용이기 때문에 답을 고르는 데 어려움은 없고 복수정답 가능성도 없다.

답 ④

15. 서비스 거부 공격(DoS)에 대한 설명으로 가장 옳지 않은 것은?

① 공격자가 임의로 자신의 IP 주소를 속여서 다량으로 서버에 보낸다.
② 대상 포트 번호를 확인하여 17, 135, 137번, UDP 포트 스캔이 아니면, UDP Flooding 공격으로 간주한다.
③ 헤더가 조작된 일련의 IP 패킷 조각들을 전송한다.
④ 신뢰 관계에 있는 두 시스템 사이에 공격자의 호스트를 마치 하나의 신뢰 관계에 있는 호스트인 것처럼 속인다.

▶ DoS 공격(Denial of Service, 서비스 거부 공격)
목표 시스템이 정상적으로 처리할 수 있는 것보다 많은 양의 자원을 보내, 시스템 자원을 고갈시켜 제대로 사용하지 못하게 하는 공격

④ 스푸핑(Spoofing)에 대한 설명이다.

<오답 체크> ①③ DoS 공격자는 기본적으로 자신의 추적을 피하기 위해 패킷의 IP 주소를 속인다.
또한 DoS 공격 중 SYN flooding(SYN 플러딩) 공격처럼 서버의 대기열 점유하기 위해 IP 패킷을 조작하는 경우도 있다.
SYN 플러딩은 TCP 3-way handshaking을 이용한 DoS공격인데, 공격 대상 서버에 존재하지 않는 IP 주소로 위조한 무수히 많은 SYN패킷을 보낸 뒤 서버로부터 오는 SYN+ACK패킷을 무시하여, 서버가 SYN Received 상태로 끊임없이 기다리게 만드는 공격방법이다.

② UDP Flooding에 대한 탐지 방법이며, UDP Flooding은 UDP 패킷을 이용한 DoS 공격이다.

답 ④

16. 윈도우 운영체제에서의 레지스트리(Registry)에 대한 설명으로 가장 옳은 것은?

① 레지스트리 변화를 분석함으로써 악성코드를 탐지할 수 있다.
② 레지스트리는 운영체제가 관리하므로 사용자가 직접 조작할 수 없다.
③ 레지스트리 편집기를 열었을 때 보이는 다섯 개의 키를 하이브(Hive)라고 부른다.
④ HKEY_CURRENT_CONFIG는 시스템에 로그인하고 있는 사용자와 관련된 시스템 정보를 저장한다.

① 악성코드는 부팅 후 자동 실행되거나 은닉하여 백신 탐지를 피하기 위해 레지스트리 값을 오염시키는 경우가 많다. 그러므로 레지스트리를 분석하면 악성코드를 발견하고 제거하는 것이 가능하며, 대다수의 백신 프로그램이 시스템을 검사할 때 레지스트리 값을 같이 검사한다.

<오답 체크> ② 레지스트리 편집기(regedit.exe)를 이용해 사용자가 직접 편집하는 것도 가능하다.

③ **하이브**(Hive)는 레지스트리 정보를 실제로 저장하고 있는 데이터베이스 파일이며, 키, 하위키, 값들을 논리적으로 분류한 그룹이다.
C:₩WINDOWS₩System32₩config 폴더에 저장된다.
그런데 레지스트리 편집기를 열면 보이는 다섯 개의 최상위 폴더 역시 레지스트리 하이브(Registry Hive)라고 한다. 이것은 key라기보다는 폴더 또는 하위 트리의 개념에 가깝다.
하지만 이 역시 정확히 틀린 표현이라고 하긴 애매한데, ①번의 설명이 가장 옳으므로 그냥 출제자의 의도를 따라야 한다.

④ HKEY_CURRENT_USER에 대한 설명이다.

답 ①

◈ **Registry Hive 종류**(레지스트리 편집기에 보이는 5개)
○ HKEY_CLASSES_ROOT는 시스템에 등록된 파일 확장자와 그것을 열 때 사용할 어플리케이션에 대한 맵핑 정보 등을 갖고 있다.
○ HKEY_CURRENT_USER는 현재 로그온되어 있는 사용자에 대한 구성 정보(사용자 프로필)를 갖고 있다.
○ HKEY_LOCAL_MACHINE은 시스템에 있는 하드웨어, 소프트웨어, 서비스 및 보안에 대한 정보를 갖고 있다.
○ HKEY_USERS는 시스템에 있는 모든 계정과 그룹에 관한 정보를 저장하고 있다.
○ HKEY_CURRENT_CONFIG는 현재 시스템이 시작되면서 사용하고 있는 하드웨어 프로파일 정보를 갖고 있다.
▷ 레지스트리 편집기에는 나타나지 않지만, 이 외에도 HKEY_CURRENT_USER_LOCAL_SETTING, HKEY_PERFORMANCE_DATA 등이 있다.

17. 침입차단시스템에 대한 설명으로 가장 옳은 것은?

① 스크린드 서브넷 구조(Screened Subnet Architecture)는 DMZ와 같은 완충 지역을 포함하며 구축 비용이 저렴하다.
② 스크리닝라우터 구조(Screening Router Architecture)는 패킷을 필터링하도록 구성되므로 구조가 간단하고 인증 기능도 제공할 수 있다.
③ 이중 네트워크 호스트 구조(Dual-homed Host Architecture)는 내부 네트워크를 숨기지만, 베스천 호스트가 손상되면 내부 네트워크를 보호할 수 없다.
④ 스크린드 호스트 게이트웨이 구조(Screened Host Gateway Architecture)는 서비스 속도가 느리지만, 베스천 호스트에 대한 침입이 있어도 내부 네트워크를 보호할 수 있다.

③ 듀얼 홈드 게이트웨이(Dual homed gateway) 또는 듀얼 홈드 호스트(Dual-homed Host)
두개의 네트워크 인터페이스를 가진 베스천 호스트를 말하며, 하나의 네트워크 인터페이스는 인터넷 등 외부 네트워크에 연결되고, 다른 하나의 네트워크 인터페이스는 내부 네트워크에 연결된다. 이렇게 분리된 각각의 네트워크로, 양 네트워크 간의 직접적인 접근은 허용되지 않는다.
베스천 호스트가 손상되면 당연히 내부 네트워크를 보호할 수 없다.

<오답 체크> ① 스크린드 서브넷 게이트웨이(Screened Subnet Gateway)
외부 네트워크와 내부 네트워크 사이에 서브넷(Subnet)이라는 완충지대를 두며, 서브넷에는 주로 DMZ와 방화벽이 위치한다.
내부 네트워크와 서브넷 사이에 스크리닝 라우터 1개, 외부 네트워크와 서브넷 사이에도 스크리닝 라우터 1개, 총 2개의 스크리닝 라우터가 들어간다.
상당히 안전한 편이지만, 관리 및 설치가 어렵고 속도가 느리며, 구축 비용이 많이 들어간다.

① 스크리닝 라우터(Screening Router)
가장 저렴하고 간단한 방화벽으로, 외부 네트워크와 내부 네트워크의 경계에 놓인다. 일반 라우터에 패킷 필터링 규칙을 적용하는 방식이며, 인증 기능은 제공하지 않는다.

④ 스크린드 호스트 게이트웨이(Screened Host Gateway)
스크리닝 라우터와 듀얼 홈드 게이트웨이의 조합
외부에서 내부로 들어오는 트래픽을 외부 네트워크와 연결된 스크리닝 라우터에서 패킷 필터링을 함으로써 1차 방어를 한 뒤, 내부 네트워크와 연결된 베스천 호스트에서 2차 방어를 함
베스천 호스트가 침입을 당하면 내부 네트워크를 보호할 수 없다.

답 ③

18. 최근 알려진 Meltdown 보안 취약점에 대한 설명으로 가장 옳은 것은?

① CPU가 사용하는 소비 전력 패턴을 사용하여 중요한 키 값이 유출되는 보안 취약점이다.
② CPU의 특정 명령어가 실행될 때 소요되는 시간을 측정하여 해당 명령어와 주요한 키 값이 유출될 수 있는 보안 취약점이다.
③ SSL 설정 시 CPU 실행에 영향을 미쳐 CPU 과열로 인해 오류를 유발하는 보안 취약점이다.
④ CPU를 고속화하기 위해 사용된 비순차적 명령어 처리(Out-of-Order Execution) 기술을 악용한 보안 취약점이다.

▶ Meltdown(멜트다운) 취약점
인텔 x86 CPU와 일부 ARM 기반 프로세서(애플, 닌텐도 스위치 등), IBM의 일부 POWER CPU에서 발견된 하드웨어 취약점. 멜트다운 취약점을 악용하면 공격자는 운영체제의 보안 정책을 모두 무시하고 컴퓨터의 모든 메모리 정보를 들여다볼 수 있다.
CPU는 보다 처리 속도를 보다 향상시키기 위해 순차 실행이 아닌, 예측 실행(Speculative Execution)과 분기 예측(Indirect Branch Prediction) 등 비순차 실행 방식으로 작동한다. 단순히 프로그램을 위에서부터 차례로 *실행하는* 것보다, 다음에 어떤 명령어가 실행될지 예측할 수 있다면 중간에 불필요한 부분은 건너뛰고 필요한 부분만 실행하여 속도를 높일 수 있기 때문이다.
만약 예측이 실패할 경우(분기를 잘못 예측했거나 실행 권한이 없을 경우 등)에는 현재 로드해 놓았던 명령어와 데이터를 버리고, 제대로 된 명령어를 찾아 다시 실행해야 한다. 그런데 이 때 CPU가 잘못 적중해서 불러왔던 데이터는 캐시에 그대로 남게 된다. 일반적인 상황에서는 그 데이터가 보여지지 않을 뿐.
멜트다운 취약점은 이 부분을 공략하는 것이다. 정상적인 데이터 접근이라면 운영체제가 접근을 차단하겠지만, 이렇게 방치된 캐시 메모리에는 특별한 권한이 없어서 접근이 가능하게 된다.
현재는 MS와 리눅스 측에서 패치를 배포하였다.

답 ④

19. <보기>는 TCSEC(Trusted Computer System Evaluation Criteria)에 의하여 보안 등급을 평가할 때 만족해야 할 요건들에 대한 설명이다. 보안 등급이 높은 것부터 순서대로 나열된 것은?

〈 보 기 〉
ㄱ. 강제적 접근 제어가 구현되어야 한다.
ㄴ. 정형화된 보안 정책을 일정하게 유지하여야 한다.
ㄷ. 사용자가 자신의 파일에 대한 접근 권한을 설정할 수 있어야 한다.

① ㄱ-ㄴ-ㄷ ② ㄱ-ㄷ-ㄴ
③ ㄴ-ㄱ-ㄷ ④ ㄴ-ㄷ-ㄱ

ㄱ. 강제적 접근 제어는 각 데이터와 사용자에 보안 등급을 부여하는 방식으로, **B1**에 해당한다.
ㄴ. 정형화된 보안 정책은 **B2**에 해당한다.
ㄷ. 사용자가 임의로 자신의 파일에 대한 접근 권한을 설정할 수 있는 것은 임의적 접근 제어인 **C1**에 해당한다.
따라서 보안 등급이 높은 순서는 ㄴ-ㄱ-ㄷ 이다.

답 ③

◈ **TCSEC 보안 등급** ◈
▷ **A1** Verified Design(검증된 설계)
수학적으로 완벽한 시스템
▷ **B3** Security Domains(보안 영역)
운영체제에서 보안에 불필요한 부분을 모두 제거
모듈에 따른 분석 및 테스트가 가능
시스템 파일 및 디렉터리에 대한 접근 방식을 지정하고, 위험 동작을 하는 사용자의 활동에 대해서는 백업까지 자동으로 이루어짐
▷ **B2** Structured Protection(계층 구조화된 보호)
시스템에 정형화된 보안 정책이 존재
일부 유닉스 시스템이 B2인증에 성공
▷ **B1** Labeled Security(레이블된 보호)
시스템 내의 보안 정책을 적용할 수 있으며 각 데이터에 대해 보안 레벨 설정이 가능
시스템 파일이나 시스템에 대한 권한을 설정
▷ **C2** Controlled Access Protection(통제된 보호)
각 계정별 로그인이 가능하며 그룹 ID에 따라 통제가 가능한 시스템
보안 감사가 가능하며 특정 사용자의 접근을 거부할 수 있음
윈도우NT 4.0과 현재 사용되는 대부분의 유닉스 시스템이 이 등급에 해당
상용 프로그램을 위한 최소한의 요구 등급
▷ **C1** Discretionary Security Protection(임의적 보호)
일반적인 로그인 과정이 존재하는 시스템.
사용자간 침범이 차단되어 있고 모든 사용자가 자신이 생성한 파일에 대해 권한을 설정할 수 있으며, 특정 파일에 대해서만 접근이 가능
초기의 유닉스 시스템이 C1등급
▷ **D** Minimal Protection(최소한의 보호)
보안 설정이 이루어지지 않은 단계

20. 정보보호 및 개인정보보호 관리체계인증(ISMS-P)에 대한 설명으로 가장 옳지 않은 것은?

① 정보보호 관리체계 인증만 선택적으로 받을 수 있다.
② 개인정보 제공 시뿐만 아니라 파기 시의 보호조치도 포함한다.
③ 위험 관리 분야의 인증기준은 보호대책 요구사항 영역에서 규정한다.
④ 관리체계 수립 및 운영 영역은 Plan, Do, Check, Act의 사이클에 따라 지속적이고 반복적으로 실행되는지 평가한다.

◈ **ISMS-P**(정보보호 및 개인정보보호 관리체계 인증)
기존의 ISMS와 PIMS를 통합한 것으로, 정보보호 및 개인정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 인터넷진흥원 또는 인증기관이 증명하는 제도로, 2018년 말부터 시행되었다. 2019년 5월 삼성증권이 최초로 ISMS-P인증을 취득하였으며, 2019년 7월 16일 롯데면세점이 면세업계 최초로 취득하였다.

⇨ 정책기관: 과학기술정보통신부, 방송통신위원회, 행정안전부
⇨ 인증기관: 한국인터넷증흥원(KISA) (+ 금융보안원 신규 지정)

③ 위험관리 영역은 '관리체계 수립 및 운영' 영역에서 규정한다.

<오답 체크> ① ISMS-P 의무대상자는 ISMS-P와 ISMS 중 선택하여 받을 수 있다. ISMS-P는 정보보호와 개인정보보호를 통합하여 인증하며 ISMS는 정보보호 관리체계만 인증한다.

② ISMS-P의 '개인정보 처리 단계별 요구사항' 영역은 개인정보 생명주기에 따른 개인정보의 수집, 보유, 이용, 제공, 파기 시 보호조치와 정보주체 권리보호를 포함하여 5개 분야 22개의 인증기준으로 구성되어 있다.

답 ③

구분		통합인증	분야(인증기준 개수)
ISMS-P	ISMS	1 관리체계 수립 및 운영 (16)	1.1 관리체계 기반 마련(6) 1.2 위험관리(4) 1.3 관리체계 운영(3) 1.4 관리체계 점검 및 개선(3)
		2 보호대책 요구사항 (64)	2.1 정책, 조직, 자산 관리(3) 2.2 인적보안(6) 2.3 외부자 보안(4) 2.4 물리보안(7) 2.5 인증 및 권한 관리(6) 2.6 접근통제(7) 2.7 암호화 적용(2) 2.8 정보시스템 도입 및 개발 보안(6) 2.9 시스템 및 서비스 운영관리(7) 2.10 시스템 및 서비스 보안관리(9) 2.11 사고 예방 및 대응(5) 2.12 재해복구(2)
	-	3 개인정보 처리단계별 요구사항(22)	3.1 개인정보 수집 시 보호조치(7) 3.2 개인정보 보유 및 이용 시 보호조치(5) 3.3 개인정보 제공 시 보호조치(3) 3.4 개인정보 파기 시 보호조치(4) 3.5 정보주체 권리보호(3)