2019년도 국가직 9급 정보보호론 - 나책형

[2019년 국가직9급 정보보호론]
문 1. 쿠키(Cookie)에 대한 설명으로 옳지 않은 것은? 2
① 쿠키는 웹사이트를 편리하게 이용하기 위한 목적으로 만들어졌으며, 많은 웹사이트가 쿠키를 이용하여 사용자의 정보를 수집하고 있다.
② 쿠키는 실행파일로서 스스로 디렉터리를 읽거나 파일을 지우는 기능을 수행한다.
③ 쿠키에 포함되는 내용은 웹 응용프로그램 개발자가 정할 수 있다.
④ 쿠키 저장 시 타인이 임의로 쿠키를 읽어 들일 수 없도록 도메인과 경로 지정에 유의해야 한다.
[해설]
- 쿠키는 실행파일이 아닌 텍스트 파일이기 때문에 실행되지 않는다. 쿠키는 웹사이트에 접속할 때 자동적으로 만들어지는 임시 파일로 이용자가 본 내용, 상품 구매 내역, 신용카드 번호, 아이디(ID), 비밀번호, IP 주소 등의 정보를 담고 있는 일종의 정보파일로 크기는 4KB 이하로 작다.

[2019년 국가직9급 정보보호론]
문 2. 악성프로그램에 대한 설명으로 옳지 않은 것은? 3
① Bot – 인간의 행동을 흉내 내는 프로그램으로 DDoS 공격을 수행한다.
② Spyware – 사용자 동의 없이 설치되어 정보를 수집하고 전송하는 악성 소프트웨어로서 금융정보, 신상정보, 암호 등을 비롯한 각종 정보를 수집한다.
③ Netbus – 소프트웨어를 실행하거나 설치 후 자동적으로 광고를 표시하는 프로그램이다.
④ Keylogging – 사용자가 키보드로 PC에 입력하는 내용을 몰래 가로채 기록하는 행위이다.
[해설]
※ 공개 해킹도구
1. 트로이목마 S/W
- 일반적으로 서버와 클라이언트 프로그램으로 구성된다.(공격의 대상에는 서버 프로그램, 공격자는 클라이언트 프로그램을 이용)
- 일반적인 기능 : 원격 조정, 캐시된 패스워드 확인, 키보드 입력 확인, 시스템 파일 삭제
- 탐지 방법 : 안티 바이러스 프로그램 사용, 자동실행 설정이 된 레지스트리 확인, 사용 중인 포트 확인, 설치된 프로그램 확인
- 종류 : NetBus, Back Orifice, Ackcmd, School Bus, Rootkit
2. 크래킹 S/W
- 사용자 ID, Password 를 찾는 행위
- 종류 : Chntpw, John the Ripper, Pwdump, Webcrack, LOphtCrack
3. 키로그 S/W
- 설치된 컴퓨터에서 키보드로 입력한 정보를 로그로 남기는 프로그램
- 종류 : Winhawk, Sc-Keylog, Keylog25

[2019년 국가직9급 정보보호론]
문 3. 정보보호 서비스에 대한 설명으로 옳지 않은 것은? 4
① Authentication – 정보교환에 의해 실체의 식별을 확실하게 하거나 임의 정보에 접근할 수 있는 객체의 자격이나 객체의 내용을 검증하는 데 사용한다.
② Confidentiality – 온오프라인 환경에서 인가되지 않은 상대방에게 저장 및 전송되는 중요정보의 노출을 방지한다.
③ Integrity – 네트워크를 통하여 송수신되는 정보의 내용이 불법적으로 생성 또는 변경되거나 삭제되지 않도록 보호한다.
④ Availability – 행위나 이벤트의 발생을 증명하여 나중에 행위나 이벤트를 부인할 수 없도록 한다.
[해설]
- Availability : 정보와 정보시스템의 사용을 인가 받은 사람이 그를 사용하려고 할 때 언제든지 사용할 수 있도록 보장하는 것이다.
- Nonrepudiation : 행위나 이벤트의 발생을 증명하여 나중에 행위나 이벤트를 부인할 수 없도록 한다.

[2019년 국가직9급 정보보호론]
문 4. 다음에서 설명하는 스캔방법은? 2

공격자가 모든 플래그가 세트되지 않은 TCP 패킷을 보내고, 대상 호스트는 해당 포트가 닫혀 있을 경우 RST 패킷을 보내고, 열려 있을 경우 응답을 하지 않는다.

① TCP Half Open 스캔 ② NULL 스캔
③ FIN 패킷을 이용한 스캔 ④ 시간차를 이용한 스캔
[해설]
- Stealth scan : FIN 스캔, XMAS 스캔, NULL 스캔 등으로 구성된다. FIN 스캔은 FIN 플래그를, XMAS 스캔은 모든 플래그를 활성화하며, NULL 스캔은 이와 반대로 모든 플래그를 비활성화한 값을 사용한다. 이 세가지 스캔 방식은 공통적으로 대상 포트가 열려있으면 아무런 응답이 없으며, 닫혀 있으면 해당 호스트는 공격자에게 RST 패킷을 전송한다.

[2019년 국가직9급 정보보호론]
문 5. SSL(Secure Socket Layer) 프로토콜에 대한 설명으로 옳지 않은 것은? 3
① ChangeCipherSpec – Handshake 프로토콜에 의해 협상된 암호규격과 암호키를 이용하여 추후의 레코드 계층의 메시지를 보호할 것을 지시한다.
② Handshake – 서버와 클라이언트 간 상호인증 기능을 수행하고, 암호화 알고리즘과 이에 따른 키 교환 시 사용된다.
③ Alert – 내부적 및 외부적 보안 연관을 생성하기 위해 설계된 프로토콜이며, Peer가 IP 패킷을 송신할 필요가 있을 때, 트래픽의 유형에 해당하는 SA가 있는지를 알아보기 위해 보안 정책 데이터베이스를 조회한다.
④ Record – 상위계층으로부터(Handshake 프로토콜, ChangeCipherSpec 프로토콜, Alert 프로토콜 또는 응용층) 수신하는 메시지를 전달하며 메시지는 단편화되거나 선택적으로 압축된다.
[해설]

- Alert Protocol : 다양한 에러 메시지를 전달한다. 메시지의 암호화 오류, 인증서 오류, 오류 조건 등을 전달하는데 사용된다.

[2019년 국가직9급 정보보호론]
문 6. 블록체인에 대한 설명으로 옳지 않은 것은? 3
① 금융 분야에만 국한되지 않고 분산원장으로 각 분야에 응용할 수 있다.
② 블록체인의 한 블록에는 앞의 블록에 대한 정보가 포함되어 있다.
③ 앞 블록의 내용을 변경하면 뒤에 이어지는 블록은 변경할 필요가 없다.
④ 하나의 블록은 트랜잭션의 집합과 헤더(header)로 이루어져 있다.
[해설]
- 블록체인에서 유효한 거래 정보의 묶음이라 할 수 있다. 하나의 블록은 트랜잭션의 집합(거래 정보)과 블록헤더(version, previousblockhash, merklehash, time, bits, nonce), 블록해쉬로 이루어져 있다. 블록헤더의 previousblockhash 값은 현재 생성하고 있는 블록 바로 이전에 만들어진 블록의 블록 해쉬값이다. 블록은 바로 앞의 블록 해쉬 값을 포함하는 방식으로 앞의 블록과 이어지게 된다. 블록체인은 쉽게 말한다면 블록으로 이루어진 연결 리스트라 할 수 있다. 블록체인의 특징인 추가전용(Append Only) DB는 내용을 추가만 할 수 있고 삭제기능은 없다. 이렇게 추가한 블록을 주기적으로 생성하고 이를 체인으로 연결한다. 블록 안의 데이터를 일정시간동안 모아서 체인으로 연결하는 이유는 P2P 네트워크로서 노드들이 블록을 누가 만들 것인지 합의해야 하기 때문이다.

[2019년 국가직9급 정보보호론]
문 7. 다음의 결과에 대한 명령어로 옳은 것은? 2

```
Thu Feb 7 20:33:56 2019 1 198.188.2.2 861486 /tmp/12-67-ftp1.bmp b _ o r freeexam
ftp 0 * c 861486 0
```

① cat /var/adm/messages
② cat /var/log/xferlog
③ cat /var/adm/loginlog
④ cat /etc/security/audit_event
[해설]
- xferlog : FTP 서버의 데이터 전송관련 로그
- messages : 부트 메시지 등 시스템의 콘솔에서 출력된 결과를 기록하고 syslog에 의하여 생성된 메시지도 기록
- loginlog : 5번이상 로그인에 실패한 정보 기록
- audit_event : 미리 정의된 audit event들 기록

[2019년 국가직9급 정보보호론]

문 8. 다음 설명에 해당하는 DoS 공격을 옳게 짝 지은 것은? 2

ㄱ. 공격자가 공격대상의 IP 주소로 위장하여 중계 네트워크에 다량의 ICMP Echo Request 패킷을 전송하며, 중계 네트워크에 있는 모든 호스트는 많은 양의 ICMP Echo Reply 패킷을 공격 대상으로 전송하여 목표시스템을 다운시키는 공격 ㄴ. 공격자가 송신자 IP 주소를 존재하지 않거나 다른 시스템의 IP 주소로 위장하여 목적 시스템으로 SYN 패킷을 연속해서 보내는 공격 ㄷ. 송신자 IP 주소와 수신자 IP 주소, 송신자 포트와 수신자 포트가 동일하게 조작된 SYN 패킷을 공격 대상에 전송하는 공격

	ㄱ	ㄴ	ㄷ
①	Smurf Attack	Land Attack	SYN Flooding Attack
②	Smurf Attack	SYN Flooding Attack	Land Attack
③	SYN Flooding Attack	Smurf Attack	Land Attack
④	Land Attack	Smurf Attack	SYN Flooding Attack

[해설]

- Smurf Attack : 발신지 IP 주소가 공격대상의 IP 주소로 위조된 ICMP 패킷을 특정 브로드캐스트 주소로 보내어 공격대상이 다량의 ICMP reply 패킷을 받도록 하는 공격기법이다.
- SYN Flooding Attack : 공격자가 송신자 IP 주소를 존재하지 않거나 다른 시스템의 IP 주소로 위장하여 목적 시스템으로 SYN 패킷을 연속해서 보내는 공격이다.
- Land Attack : 송신자 IP 주소와 수신자 IP 주소, 송신자 포트와 수신자 포트가 동일하게 조작된 SYN 패킷을 공격 대상에 전송하는 공격이다.

[2019년 국가직9급 정보보호론]

문 9. 무선 LAN 보안에 대한 설명으로 옳지 않은 것은? 1

① WPA2는 RC4 알고리즘을 암호화에 사용하고, 고정 암호키를 사용한다.
② WPA는 EAP 인증 프로토콜(802.1x)과 WPA-PSK를 사용한다.
③ WEP는 64비트 WEP 키가 수분 내 노출되어 보안이 매우 취약하다.
④ WPA-PSK는 WEP보다 훨씬 더 강화된 암호화 세션을 제공한다.

[해설]

- WPA2는 암호화에 AES 알고리즘을 사용하며, 가변길이 암호키를 사용한다.

[2019년 국가직9급 정보보호론]
문 10. 사용자 A가 사용자 B에게 해시함수를 이용하여 인증, 전자서명, 기밀성, 무결성이 모두 보장되는 통신을 할 때 구성해야 하는 함수로 옳은 것은? 4

K: 사용자 A와 B가 공유하고 있는 비밀키 KSa: 사용자 A의 개인키, KPa: 사용자 A의 공개키 H: 해시함수, E: 암호화 M: 메시지, ||: 두 메시지의 연결

① $E_K[M \| H(M)]$
② $M \| E_K[H(M)]$
③ $M \| E_K Sa[H(M)]$
④ $E_K[M \| E_K Sa[H(M)]]$
[해설]
- M || E KSa [H(M)] : 전자서명, 부인방지, 무결성 보장
- E K [M || E KSa [H(M)]] : 기밀성 보장

[2019년 국가직9급 정보보호론]
문 11. 다음 알고리즘 중 공개키 암호 알고리즘에 해당하는 것은? 2
① SEED 알고리즘 ② RSA 알고리즘
③ DES 알고리즘 ④ AES 알고리즘
[해설]
- 대칭키 암호화 알고리즘 : DES, 3DES, AES, SEED, IDEA, ARIA, Blowfish, RC5, RC6 등
- 비대칭키 암호화 알고리즘 : RSA, ElGamal, ECC, RABIN 등

[2019년 국가직9급 정보보호론]
문 12. 정보보안 관련 용어에 대한 설명으로 옳지 않은 것은? 4
① 부인방지(Non-repudiation) – 사용자가 행한 행위 또는 작업을 부인하지 못하는 것이다.
② 최소권한(Least Privilege) – 계정이 수행해야 하는 작업에 필요한 최소한의 권한만 부여한다.
③ 키 위탁(Key Escrow) – 암호화 키가 분실된 경우를 대비하여 키를 보관하는 형태를 의미한다.
④ 차분 공격(Differential Attack) – 대용량 해쉬 테이블을 이용하여 충분히 작은 크기로 줄여 크랙킹 하는 방법이다.
[해설]
– 차분 암호분석 공격(Differential cryptanalysis Attack) : chosen plaintext cryptanlysis의 일종으로 블록 암호에서 입력쌍의 차이(Input difference)와 해당 출력쌍에 대한 차이(Output difference) 값들의 확률 분포가 균일하지 않다는 사실을 이용하여 공격하는 방법이다. 입력에 따른 출력의 변화를 이용하여 암호를 공격하는 방법이다.

[2019년 국가직9급 정보보호론]

문 13. 공통평가기준은 IT 제품이나 특정 사이트의 정보시스템의 보안성을 평가하는 기준이다. '보안기능 요구사항'과 '보증요구사항'을 나타내는 보호프로파일(PP), 보호목표명세서(ST)에 대한 설명으로 옳지 않은 것은? 2

① 보호프로파일은 구현에 독립적이고, 보호목표명세서는 구현에 종속적이다.

② 보호프로파일은 보호목표명세서를 수용할 수 있고, 보호목표명세서는 보호프로파일을 수용할 수 있다.

③ 보호프로파일은 여러 시스템·제품을 한 개 유형의 보호프로파일로 수용할 수 있으나, 보호목표명세서는 한 개의 시스템·제품을 한 개의 보호목표명세서로 수용해야 한다.

④ 보호프로파일은 오퍼레이션이 완료되지 않을 수 있으나, 보호목표명세서는 모든 오퍼레이션이 완료되어야 한다.

[해설]

- PP(보호프로파일)와 ST(보호목표명세서)의 차이점

구분	PP	ST
구현의 독립성	구현에 독립적	구현에 종속적
범위	제품군 ex) IDS	특정제품 ex) A사의 IDS
시스템/제품별 적용방법	여러 시스템/베품들이 하나의 동일한 유형의 보호프로파일을 수용할 수 있음	하나의 시스템/제품은 하나의 보안모표명세서로 작성됨
수용여부	보호프로파일은 보안목표명세서를 수용할 수 없읍	보안목표명세서는 보호 프로파일을 수용할 수 있음
표현방법	사용자 측면의 "What I want?"	개발자 측면의 "What I have?"

[2019년 국가직9급 정보보호론]

문 14. 방화벽 구축 시 내부 네트워크의 구조를 외부에 노출하지 않는 방법으로 적절한 것은? 1

① Network Address Translation ② System Active Request

③ Timestamp Request ④ Fragmentation Offset

[해설]

- NAT(Network Address Translation) : 사설 IP주소를 공인 IP주소로 바꿔주는 주소 변환기이다. 인터넷의 공인 IP주소를 절약할 수 있고, 인터넷과 연결되는 사용자들의 고유한 사설망을 침입자들로부터 보호할 수 있다.

[2019년 국가직9급 정보보호론]
문 15. 「개인정보 보호법 시행령」상 개인정보 영향평가의 대상에 대한 규정의 일부이다. ㉠, ㉡에 들어갈 내용으로 옳은 것은? 1

> 제35조(개인정보 영향평가의 대상) 「개인정보 보호법」 제33조제1항에서 "대통령령으로 정하는 기준에 해당하는 개인정보파일"이란 개인정보를 전자적으로 처리할 수 있는 개인정보파일로서 다음 각 호의 어느 하나에 해당하는 개인정보파일을 말한다.
> 1. 구축·운용 또는 변경하려는 개인정보파일로서 (㉠) 이상의 정보주체에 관한 민감정보 또는 고유식별정보의 처리가 수반되는 개인정보파일
> 2. 구축·운용하고 있는 개인정보파일을 해당 공공기관 내부 또는 외부에서 구축·운용하고 있는 다른 개인정보파일과 연계하려는 경우로서 연계 결과 50만 명 이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일
> 3. 구축·운용 또는 변경하려는 개인정보파일로서 (㉡) 이상의 정보주체에 관한 개인정보파일

	㉠	㉡
①	5만 명	100만 명
②	10만 명	100만 명
③	5만 명	150만 명
④	10만 명	150만 명

[해설]
- 제35조(개인정보 영향평가의 대상) 법 제33조제1항에서 "대통령령으로 정하는 기준에 해당하는 개인정보파일"이란 개인정보를 전자적으로 처리할 수 있는 개인정보파일로서 다음 각 호의 어느 하나에 해당하는 개인정보파일을 말한다. <개정 2016. 9. 29.>
1. 구축·운용 또는 변경하려는 개인정보파일로서 5만명 이상의 정보주체에 관한 민감정보 또는 고유식별정보의 처리가 수반되는 개인정보파일
2. 구축·운용하고 있는 개인정보파일을 해당 공공기관 내부 또는 외부에서 구축·운용하고 있는 다른 개인정보파일과 연계하려는 경우로서 연계 결과 50만명 이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일
3. 구축·운용 또는 변경하려는 개인정보파일로서 100만명 이상의 정보주체에 관한 개인정보파일
4. 법 제33조제1항에 따른 개인정보 영향평가(이하 "영향평가"라 한다)를 받은 후에 개인정보 검색체계 등 개인정보파일의 운용체계를 변경하려는 경우 그 개인정보파일. 이 경우 영향평가 대상은 변경된 부분으로 한정한다.

[2019년 국가직9급 정보보호론]
문 16. 버퍼 오버플로우(Buffer Overflow) 공격에 대한 대응으로 해당하지 않는 것은? 4
① 안전한 함수 사용 ② Non-Executable 스택
③ 스택 가드(Stack Guard) ④ 스택 스매싱(Stack Smashing)
[해설]
- 버퍼 오버플로우 공격에 대한 대응 방법 : 스택 가드(Stack Guard), Non-Executable 스택, DEP(Data Execution Prevention), ASLR(Address Space Layout Randomization), 안전한 함수 사용 등

- 스택 스매싱(Stack Smashing) : 콜 스택(the call stack) 상에서 호출된 함수의 리턴 주소가 덮어써졌을 때(overwritten) 발생한다. 이 때 프로그램 컨트롤이 불법 주소로 점프를 시도하면 함수 리턴에서 프로그램이 크래시가 일어 날 수 있다.

[2019년 국가직9급 정보보호론]
문 17. 블록체인(Blockchain) 기술과 암호화폐(Cryptocurrency) 시스템에 대한 설명으로 옳지 않은 것은? 3
① 블록체인에서는 각 트랜잭션에 한 개씩 전자서명이 부여된다.
② 암호학적 해시를 이용한 어려운 문제의 해를 계산하여 블록체인에 새로운 블록을 추가할 수 있고 일정량의 암호화폐로 보상받을 수도 있다.
③ 블록체인의 과거 블록 내용을 조작하는 것은 쉽다.
④ 블록체인은 작업증명(Proof-of-work)과 같은 기법을 이용하여 합의에 이른다.
[해설]
- 블록체인에서 유효한 거래 정보의 묶음이라 할 수 있다. 하나의 블록은 트랜잭션의 집합(거래 정보)과 블록헤더(version, previousblockhash, merklehash, time, bits, nonce), 블록해쉬로 이루어져 있다. 블록헤더의 previousblockhash 값은 현재 생성하고 있는 블록 바로 이전에 만들어진 블록의 블록 해쉬값이다. 블록은 바로 앞의 블록 해쉬 값을 포함하는 방식으로 앞의 블록과 이어지게 된다. 블록체인은 쉽게 말한다면 블록으로 이루어진 연결 리스트라 할 수 있다. 블록체인의 특징인 추가전용(Append Only) DB는 내용을 추가만 할 수 있고 삭제기능은 없다. 이렇게 추가한 블록을 주기적으로 생성하고 이를 체인으로 연결한다. 블록 안의 데이터를 일정시간동안 모아서 체인으로 연결하는 이유는 P2P 네트워크로서 노드들이 블록을 누가 만들것인지 합의해야 하기 때문이다.

[2019년 국가직9급 정보보호론]
문 18. 「정보통신기반 보호법」상 주요정보통신기반시설의 보호체계에 대한 설명으로 옳지 않은 것은? 3
① 주요정보통신기반시설 관리기관의 장은 정기적으로 소관 주요정보통신시설의 취약점을 분석·평가하여야 한다.
② 중앙행정기관의 장은 소관분야의 정보통신기반시설을 필요한 경우 주요정보통신기반시설로 지정할 수 있다.
③ 지방자치단체의 장이 관리·감독하는 기관의 정보통신기반시설은 지방자치단체의 장이 주요정보통신기반시설로 지정한다.
④ 과학기술정보통신부장관과 국가정보원장등은 특정한 정보통신기반시설을 주요정보통신기반시설로 지정할 필요가 있다고 판단하면 중앙행정기관의 장에게 해당 정보통신기반시설을 주요정보통신기반시설로 지정하도록 권고할 수 있다.
[해설]
- 제8조(주요정보통신기반시설의 지정 등) ①중앙행정기관의 장은 소관분야의 정보통신기반시설중 다음 각호의 사항을 고려하여 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정할 수 있다.
1. 당해 정보통신기반시설을 관리하는 기관이 수행하는 업무의 국가사회적 중요성

2. 제1호의 규정에 의한 기관이 수행하는 업무의 정보통신기반시설에 대한 의존도
3. 다른 정보통신기반시설과의 상호연계성
4. 침해사고가 발생할 경우 국가안전보장과 경제사회에 미치는 피해규모 및 범위
5. 침해사고의 발생가능성 또는 그 복구의 용이성

②중앙행정기관의 장은 제1항의 규정에 의한 지정 여부를 결정하기 위하여 필요한 자료의 제출을 해당 관리기관에 요구할 수 있다.

③관계중앙행정기관의 장은 관리기관이 해당 업무를 폐지·정지 또는 변경하는 경우에는 직권 또는 해당 관리기관의 신청에 의하여 주요정보통신기반시설의 지정을 취소할 수 있다.

④지방자치단체의 장이 관리·감독하는 기관의 정보통신기반시설에 대하여는 행정안전부장관이 지방자치단체의 장과 협의하여 주요정보통신기반시설로 지정하거나 그 지정을 취소할 수 있다. <개정 2008. 2. 29., 2013. 3. 23., 2014. 11. 19., 2017. 7. 26.>

⑤중앙행정기관의 장이 제1항 및 제3항의 규정에 의하여 지정 또는 지정 취소를 하고자 하는 경우에는 위원회의 심의를 받아야 한다. 이 경우 위원회는 제1항 및 제3항의 규정에 의하여 지정 또는 지정취소의 대상이 되는 관리기관의 장을 위원회에 출석하게 하여 그 의견을 들을 수 있다.

⑥중앙행정기관의 장은 제1항 및 제3항의 규정에 의하여 주요정보통신기반시설을 지정 또는 지정 취소한 때에는 이를 고시하여야 한다. 다만, 국가안전보장을 위하여 필요한 경우에는 위원회의 심의를 받아 이를 고시하지 아니할 수 있다.

⑦주요정보통신기반시설의 지정 및 지정취소 등에 관하여 필요한 사항은 이를 대통령령으로 정한다.

[2019년 국가직9급 정보보호론]

문 19. 업무연속성(BCP)에 대한 설명으로 옳지 않은 것은? 3

① 업무연속성은 장애에 대한 예방을 통한 중단 없는 서비스 체계와 재난 발생 후에 경영 유지·복구 방법을 명시해야 한다.

② 재해복구시스템의 백업센터 중 미러 사이트(Mirror Site)는 백업센터 중 가장 짧은 시간 안에 시스템을 복구한다.

③ 콜드 사이트(Cold Site)는 주전산센터의 장비와 동일한 장비를 구비한 백업 사이트이다.

④ 재난복구서비스인 웜 사이트(Warm Site)는 구축 및 유지비용이 콜드 사이트(Cold Site)에 비해서 높다.

[해설]

- 콜드 사이트(Cold Site) : 데이터만 원격지에 보관하고, 이의 서비스를 위한 정보자원은 확보하지 않거나 장소 등 최소한으로만 확보하고 있다가, 재해시에 데이터를 근간으로 하여 필요한 정보자원을 조달하여 정보시스템의 복구를 개시하는 방식이다.

[2019년 국가직9급 정보보호론]
문 20. 「개인정보 보호법 시행령」의 내용으로 옳지 않은 것은? 1
① 공공기관의 영상정보처리기기는 재위탁하여 운영할 수 없다.
② 개인정보처리자가 전자적 파일 형태의 개인정보를 파기하여야 하는 경우 복원이 불가능한 형태로 영구 삭제하여야 한다.
③ 개인정보처리자는 개인정보의 처리에 대해서 전화를 통하여 동의 내용을 정보주체에게 알리고 동의 의사표시를 확인하는 방법으로 동의를 받을 수 있다.
④ 공공기관이 개인정보를 목적 외의 용도로 이용하는 경우에는 '이용하거나 제공하는 개인정보 또는 개인정보파일의 명칭'을 개인정보의 목적 외 이용 및 제3자 제공 대장에 기록하고 관리하여야 한다.
[해설]
- ①번 보기 관련
제26조(공공기관의 영상정보처리기기 설치·운영 사무의 위탁) ① 법 제25조제8항 단서에 따라 공공기관이 영상정보처리기기의 설치·운영에 관한 사무를 위탁하는 경우에는 다음 각 호의 내용이 포함된 문서로 하여야 한다.
1. 위탁하는 사무의 목적 및 범위
2. 재위탁 제한에 관한 사항
3. 영상정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
4. 영상정보의 관리 현황 점검에 관한 사항
5. 위탁받는 자가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항
- ②번 보기 관련
제16조(개인정보의 파기방법) ①개인정보처리자는 법 제21조에 따라 개인정보를 파기할 때에는 다음 각 호의 구분에 따른 방법으로 하여야 한다. <개정 2014. 8. 6.>
1. 전자적 파일 형태인 경우: 복원이 불가능한 방법으로 영구 삭제
- ③번 보기 관련
제17조(동의를 받는 방법) ① 개인정보처리자는 법 제22조에 따라 개인정보의 처리에 대하여 다음 각 호의 어느 하나에 해당하는 방법으로 정보주체의 동의를 받아야 한다.
1. 동의 내용이 적힌 서면을 정보주체에게 직접 발급하거나 우편 또는 팩스 등의 방법으로 전달하고, 정보주체가 서명하거나 날인한 동의서를 받는 방법
2. 전화를 통하여 동의 내용을 정보주체에게 알리고 동의의 의사표시를 확인하는 방법
3. 전화를 통하여 동의 내용을 정보주체에게 알리고 정보주체에게 인터넷주소 등을 통하여 동의 사항을 확인하도록 한 후 다시 전화를 통하여 그 동의 사항에 대한 동의의 의사표시를 확인하는 방법
4. 인터넷 홈페이지 등에 동의 내용을 게재하고 정보주체가 동의 여부를 표시하도록 하는 방법
5. 동의 내용이 적힌 전자우편을 발송하여 정보주체로부터 동의의 의사표시가 적힌 전자우편을 받는 방법
- ④번 보기 관련
제15조(개인정보의 목적 외 이용 또는 제3자 제공의 관리) 공공기관은 법 제18조제2항 각 호에 따라 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우에는 다음 각 호의 사항을 행정안전부령으로 정하는 개인정보의 목적 외 이용 및 제3자 제공 대장에 기록하고 관리하여야 한다