정보보호론

〔강평 및 해설 : 임재선 교수〕

총 평

이번 시험은 비교적 고른 출제였다고 생각되며 시대 상황에 맞춰 블록체인과 악성코드를 묻는 문제가 출제되었다. 분야별로 분류하면 시스템 보안: 4문제, 정보보안 일반 : 1문제, 네트워크 보안 : 4문제, 애플리케이션 보안: 1문제, 보안과 암호: 5문제, 정보보안 관리 : 2문제, 정보보호 관련 법규 : 3문제가 출제되었다.

문제에서 보안과 암호 분야에서 인증, 전자서명, 기밀성, 무결성이 모두 보장되는 통신을 구성할 때 구성해야 하는 함수를 고르는 문제는 기존에 암기로 접근하는 방식으로는 어려웠을 문제였다. 기밀성과 무결성의 의미를 이해하고 각각을 보장하는 함수를 구성해야 하는 문제로 앞으로 보안 분야를 어떻게 공부해야 하는지 알려주는 문제라고 생각한다.

많은 학생이 어려워하는 정보보호 관련 법규에서는 개인정보 보호법 시행령의 개인정보 영향 평가의 대상과 정보통신기반 보호법의 내용을 묻는 문제가 출제되었으며 모두 기출문제에서 출제되어 기출문제를 꾸준히 공부한 학생이면 풀 수 있을 문제였다. 앞으로도 법규 관련 문제는 기출문제 위주로 출제될 것으로 예상된다.

기출문제를 중심으로 꾸준히 학습하되 4차 산업혁명과 IoT 분야에서 쟁점이 되고 있는 해킹 및 네트워크 보안 문제를 관심 있게 준비해야 할 것으로 생각된다.

문 1. 쿠키(Cookie)에 대한 설명으로 옳지 않은 것은?

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 인터넷 웹사이트의 방문기록을 남겨 사용자와 웹사이트 사이를 매개해 주는 정보이다

- 쿠키는 웹 서비스 사용자의 PC의 저장소에 저장되는 변수이다.
- 웹 서비스의 세션을 유지하는 데 사용될 수 있다.
- 서버에서 웹 서비스 사용자의 접근 기록을 추적할 수 있다.
- 쿠키는 Java Script 같은 웹 개발언어를 통해 cookie 변수 등을 만들어 접근해 사용할 수 있다.
- 상태정보를 저장하지 않는 HTTP를 보완하기 위한 기술이다.

정답 2

문 2. 악성프로그램에 대한 설명으로 옳지 않은 것은?

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

③ Netbus는 상대방 컴퓨터의 IP를 알아내고 patch프로그램을 설치하면 그 컴퓨터를 마음대로 조정할 수 있는 프로그램이다. 소프트웨어를 실행하거나 설치 후 자동적으로 광고를 표시하는 프로그램은 애드웨어이다.

정답 3

문 3. 정보보호 서비스에 대한 설명으로 옳지 않은 것은?

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

④ 가용성(Availabiltiy): 자원(정보, 시스템, 네트워크, 프린터) 등을 계속해서 사용할 수 있게 한다.

- 부인방지(부인봉쇄: Non-repudiation): 작성자가 거래내역에 대한 부인을 방지한다.

정답 4

문 4. 다음에서 설명하는 스캔방법은?

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

② Null스캔이란 TCP 헤더 내에 플래그 값을 설정하지 않고 전송하는 방법이다.

정답 2

문 5. SSL(Secure Socket Layer) 프로토콜에 대한 설명으로 옳지 않은 것은?

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.

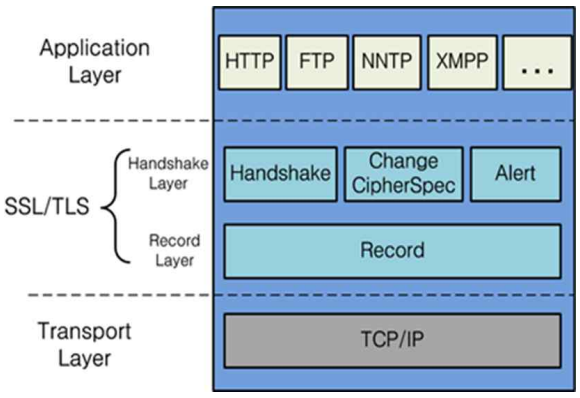
③ Alert – 내부적 및 외부적 보안 연관을 생성하기 위해 설계된 프로토콜이며, Peer가 IP 패킷을 송신할 필요가 있을 때, 트래픽의 유형에 해당하는 SA가 있는지를 알아보기 위해 보안 정책 데이터베이스를 조회한다.

④ Record – 상위계층으로부터(Handshake 프로토콜, ChangeCipherSpec 프로토콜, Alert 프로토콜 또는 응용층) 수신하는 메시지를 전달하며 메시지는 단편화되거나 선택적으로 압축된다.

해설

SSL은 웹브라우저와 웹서버 간에 안전한 정보 전송을 위해 사용되는 암호화 방법이다.

③ Alert Protocol: 다양한 에러 메시지를 전달한다. SA(Security Association)는 IPSec 프로토콜로 통신전에 카 교환방법, 키 교환주기 등의 합의를 이루는 프로토콜이다.



정답 3

문 6. 블록체인에 대한 설명으로 옳지 않은 것은?

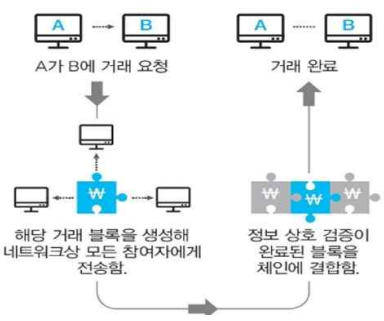
① 금융 분야에만 국한되지 않고 분산원장으로 각 분야에 응용할 수 있다.

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

블록체인 특징
- 비트코인 거래 요청이 발생할 경우 해당 블록에 대한 검증을 거쳐 승인이 이루어져야 거래가 완성된다.
- 거래가 발생할 때마다 분산 저장된 데이터를 대조하기 때문에 안전성이 더 높아진다.
- 블록체인은 공공거래장부(원장)를 서로 비교하여 동일한 내용만 공공거래장부(원장)로 인정한다. 즉 네트워크 참여 인원이 전부 보안에 조금씩 기여하게 된다.
- 

정답 3

문 7. 다음의 결과에 대한 명령어로 옳은 것은?

```
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

② xferlog : FTP 파일 전송 내역 기록

정답 2

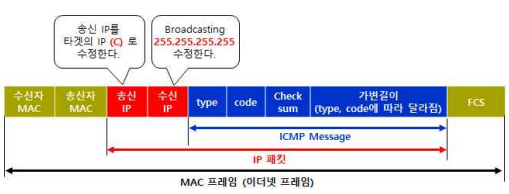
문 8. 다음 설명에 해당하는 DoS 공격을 옳게 짝 지은 것은?

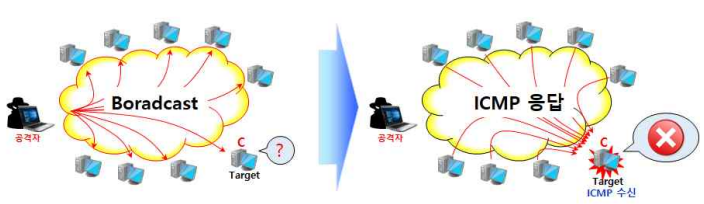
ㄱ. 공격자가 공격대상의 IP 주소로 위장하여 중계 네트워크에 다량의 ICMP Echo Request 패킷을 전송하며, 중계 네트워크에 있는 모든 호스트는 많은 양의 ICMP Echo Reply 패킷을 공격 대상으로 전송하여 목표시스템을 다운시키는 공격
ㄴ. 공격자가 송신자 IP 주소를 존재하지 않거나 다른 시스템의 IP 주소로 위장하여 목적 시스템으로 SYN 패킷을 연속해서 보내는 공격
ㄷ. 송신자 IP 주소와 수신자 IP 주소, 송신자 포트와 수신자 포트가 동일하게 조작된 SYN 패킷을 공격 대상에 전송하는 공격

	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

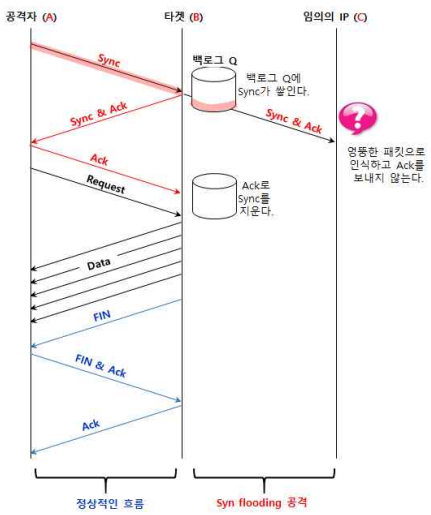
해설

- Smurf Attack : 목표 사이트에 응답 패킷의 트래픽이 넘쳐서 다른 사용자로부터 접속을 받아들일 수 없게 만드는 것이다.

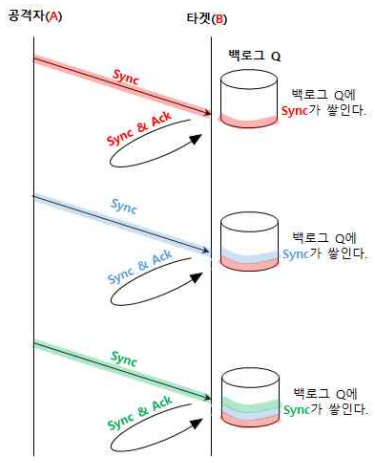




- SYN Flooding Attack : TCP 3-way handshaking 과정 중 Listen 상태에서 SYN을 받은 서버가 SYN/ACK를 전달한 후 ACK를 무한정 기다리게 하는 공격으로 TCP의 연결 방식의 구조적 문제점을 이용한 방법이다.



- Land Attack : Land(랜드) 공격은 패킷을 전송할 때 출발지 IP주소와 목적지 IP주소 값을 똑같이 만들어서 공격 대상에게 보내는 것이다.



정답 2

문 9. 무선 LAN 보안에 대한 설명으로 옳지 않은 것은?

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

① WPA2 방식은 AES 암호화 방법을 사용하여 액세스 포인트에 연결할 브라더 무선 시스템을 가능하게 하여 좀 더 강력한 보안을 제공한다.

정답 1

문 10. 사용자 A가 사용자 B에게 해시함수를 이용하여 인증, 전자서명, 기밀성, 무결성이 모두 보장되는 통신을 할 때 구성해야 하는 함수로 옳은 것은?

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 EK[M || H(M)]
② M || EK[H(M)]
③ M || EKSa[H(M)]
④ EK[M || EKSa[H(M)]]

해설

1) 무결성을 보장하기 위하여 해시함수를 이용하여 해시값을 만들고 이 해시값을 KSa로 암호화 한다. EKSa[H(M)]]
2) 메시지와 암호화된 해시값을 연결한다. M || EKSa[H(M)
3) 기밀성을 보장하기 위해 메시지와 해시값을 공유비밀키K로 암호화 한다. EK[M || EKSa[H(M)]]

정답 4

문 11. 다음 알고리즘 중 공개키 암호 알고리즘에 해당하는 것은?

① SEED 알고리즘 ② RSA 알고리즘
③ DES 알고리즘 ④ AES 알고리즘

해설

공개키 암호 알고리즘에는 디프헬만, RSA, DSA, ECC, Rabin, ElGamal 등이 있다.

정답 2

문 12. 정보보안 관련 용어에 대한 설명으로 옳지 않은 것은?

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

- 차분공격(Differental Crptanalysis): 1990년 Biham과 Shamir에 의하여 개발된 선택된 평문공격법으로, 두 개의 평문 블록들의 비트 차이에 대하여 대응되는 암호문 블록들의 비트 차이를 이용하여 사용된 암호열쇠를 찾아내는 방법이다

정답 4

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

① 보호프로파일은 구현에 독립적이고, 보호목표명세서는 구현에 종속적이다.

② 보호프로파일은 보호목표명세서를 수용할 수 있고, 보호목표 명세서는 보호프로파일을 수용할 수 있다.

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

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

해설

구분	구분보호 프로파일(Protection Profile)	보안목표명세서(Security Target)
개념	• 동일한 제품이나 시스템에 적용할 수 있는 일반적인 보안기능 요구사항 및 보증 요구 사항 정의	• 특정 제품이나 시스템에 적용할 수 있는 일반적인 보안기능 요구사항 및 보증 요구사항 정의
독립성	• 구현에 독립적	• 구현에 종속적
적용성	• 제품군(생체인식시스템) • 여러 제품/시스템에 동일한 PP를 수용 가능	• 특정제품(A사의 지문감식시스템) • 하나의 제품/시스템에 하나의 ST를 수용해야 한다.
관계성	• PP는 ST를 수용할 수 없다.	• ST는 PP를 수용할 수 있다.
완전성	• 불완전한 오퍼레이션 가능	• 모든 오퍼레이션은 완전해야 한다.

정답 2

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

① Network Address Translation

② System Active Request

③ Timestamp Request

④ Fragmentation Offset

해설

- NAT란 Network Address Translation의 약자로 '네트워크 주소 변환' 기술이다. IPv4의 공인 IP를 절약할 수 있고, 인터넷이란 공공망과 연결되는 사용자들의 고유한 사설망을 침입자로부터 보호할 수 있다.

정답 1

문 15. 개인정보 보호법 시행령 상 개인정보 영향평가의 대상에 대한 규정의 일부이다. ㉠, ㉡에 들어갈 내용으로 옳은 것은?

> 제35조(개인정보 영향평가의 대상) 개인정보 보호법 제33조 제1항에서 “대통령령으로 정하는 기준에 해당하는 개인정보 파일”이란 개인정보를 전자적으로 처리할 수 있는 개인정보 파일로서 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

1. 구축·운용 또는 변경하려는 개인정보 파일로서 5만 명 이상의 정보주체에 관한 민감정보 또는 고유식별정보의 처리가 수반되는 개인정보 파일
3. 구축·운용 또는 변경하려는 개인정보 파일로서 100만 명 이상의 정보주체에 관한 개인정보 파일

정답 1

문 16. 버퍼 오버플로우(Buffer Overflow) 공격에 대한 대응으로 해당하지 않는 것은?

① 안전한 함수 사용
② Non-Executable 스택
③ 스택 가드(Stack Guard)
④ 스택 스매싱(Stack Smashing)

해설

- 버퍼 오버플로 공격은 할당된 메모리 경계에 대한 검사를 하지 않는 프로그램의 취약점을 이용해서 공격자가 원하는 데이터를 덮어쓰는 방식이다. 만약 실행 코드가 덮어써진다면 공격자가 원하는 방향으로 프로그램이 동작하게 할 수 있다.
- 스택 스매싱은 스택 버퍼 오버플로우 공격 방법이다.

정답 4

문 17. 블록체인(Blockchain) 기술과 암호화폐(Cryptocurrency) 시스템에 대한 설명으로 옳지 않은 것은?

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

- 비트코인 거래 요청이 발생할 경우 해당 블록에 대한 검증을 거쳐 승인이 이루어지며, 조작은 매우 어렵다.

정답 3

문 18. 정보통신기반 보호법 상 주요정보통신기반시설의 보호체계에 대한 설명으로 옳지 않은 것은?

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 정보통신 기반시설을 주요정보통신기반시설로 지정할 필요가 있다고 판단하면 중앙행정기관의 장에게 해당 정보통신기반시설을 주요정보통신기반시설로 지정하도록 권고할 수 있다.

해설

- 중앙행정기관의 장은 소관분야의 정보통신 기반시설 중 다음 각 호의 사항을 고려하여 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신 기반시설을 주요 정보통신 기반시설로 지정할 수 있다.

정답 3

문 19. 업무연속성(BCP)에 대한 설명으로 옳지 않은 것은?

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

미러사이트(Mirror Site)
- 주 센터와 동일한 수준의 정보기술자원을 원격지에 구축하여 두고, 주 센터와 재해복구센터 모두 액티브상태로(Active-Active) 실시간에 동시 서비스하는 방식이다.
- 재해 발생 시 복구까지의 소요시간(RTO)은 즉시('0')이다.
- 초기 투자 및 유지보수에 높은 비용이 소요된다.

핫 사이트(Hot Site)
- 재해복구센터에 주 센터와 동일한 수준의 시스템을 대기상태(Standby)로 원격지 사이트에 보유하면서(Active-Standby), 동기적(Synchronous) 또는 비동기적 (Asynchronous) 방식으로 실시간 복제를 통하여 최신의 데이터 상태(Up-to-date)를 유지하고 있다가, 재해 시 재해복구센터의 시스템을 활성화(Active) 상태로 전환하여 복구하는 방식이다.

웜 사이트(Worm Site)
- Hot Site와 유사하나 메인 센터와 동일한 수준의 정보기술 자원을 보유하는 대신 중요성이 높은 기술 자원만 부분적으로 보유하는 방식으로 실시간 미러링을 수행하지 않는다.
- 실시간 미러링을 수행하지 않으며 데이터의 백업 주기가 수시간~1일 정도로 Hot site에 비해 다소 길다(데이터 백업 주기가 수시간~1일 정도 소요되며, 재해 발생 시 복구까지의 소요시간(RTO)은 수일~수주이다).

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

정답 3

문 20. 개인정보 보호법 시행령 의 내용으로 옳지 않은 것은?

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 관리 하여야 한다.

해설

- 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.

정답 1