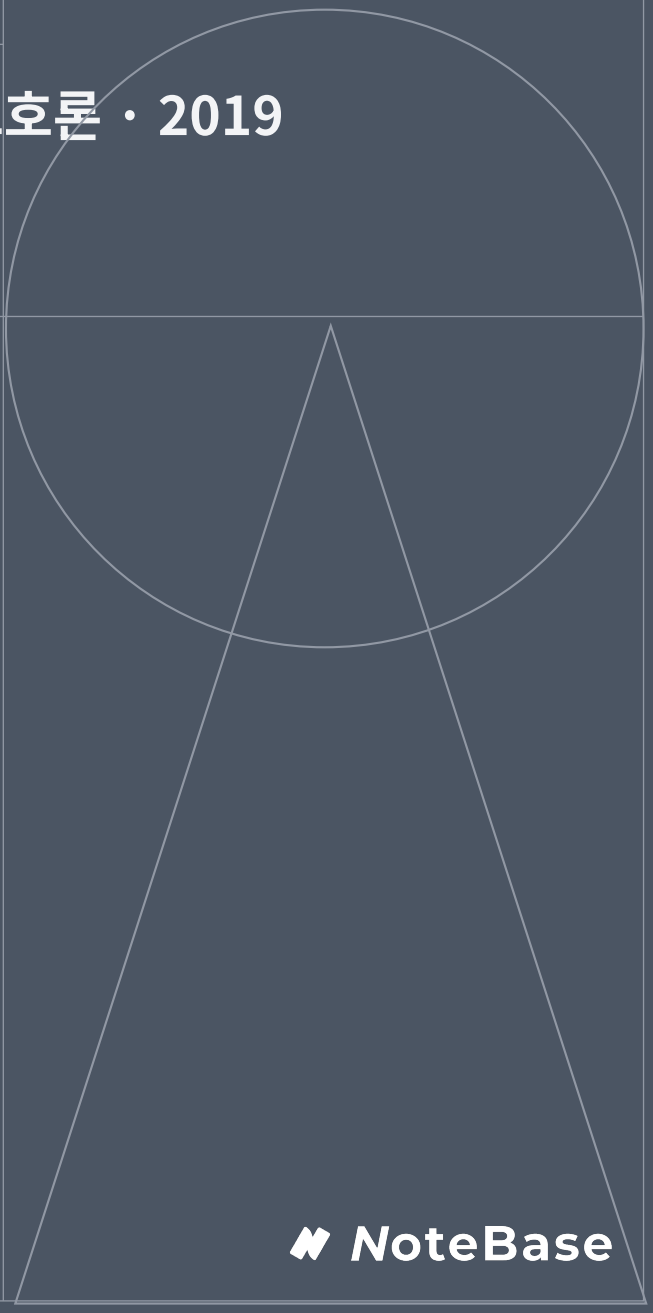
기출OX 해설집

공무원/국가직/9급 · 정보보호론 · 2019



NoteBase

기출OX 해설집

공무원/국가직/9급 · 정보보호론 · 2019

공무원/국가직/9급 · 정보보호론 · 2019

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.

정답 2번

간단한 해설

쿠키는 **실행파일이 아니라 브라우저가 저장하는 데이터**이다. 스스로 디렉터리를 읽거나 파일을 삭제하는 기능은 없다.

선지별 해설

① O: 쿠키는 웹사이트가 이용자를 구별하거나 이전 이용 상태를 기억하도록 돕는다. 예를 들어 로그인 상태나 언어 설정을 유지할 수 있다. 웹사이트는 쿠키에 담긴 식별자를 이용해 **이용 기록을 연결하여 정보를 수집**할 수도 있다.

② X: 쿠키는 이름과 값 등의 형태로 브라우저에 저장되고, 해당 조건에 맞는 웹 요청에 실려 전송되는 **데이터**이다. 실행파일처럼 명령을 수행하지 않으므로, 쿠키 자체가 디렉터리를 읽거나 파일을 지울 수는 없다.

③ O: 웹 응용프로그램 개발자는 서비스 목적에 따라 **쿠키의 이름과 값, 그 값의 의미**를 정할 수 있다. 예를 들어 언어 설정을 나타내는 값이나 서버에서 이용자를 구별하는 식별자를 담도록 설계할 수 있다. 다만 쿠키의 형식과 크기 등에는 브라우저와 규격에 따른 제약이 있다.

④ O: Domain은 쿠키를 전송할 호스트의 범위를, Path는 요청 경로의 범위를 정한다. 따라서 불필요한 곳으로 쿠키가 전달되지 않도록 **도메인과 경로의 범위를 필요한 만큼으로 제한**해야 한다. 다만 이 설정만으로 타인의 접근을 모두 막는다는 뜻은 아니며, 특히 Path는 같은 호스트 안에서 쿠키를 안전하게 격리하는 보안 경계가 아니다.

NoteBase

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.

정답 3번

간단한 해설

프로그램 실행이나 설치 후 자동으로 광고를 표시하는 것은 **애드웨어(Adware)**의 특징이다. NetBus는 공격자가 다른 컴퓨터에 접근해 조작하는 데 악용되는 **원격 제어용 백도어**이다.

선지별 해설

① O: 봇(Bot)은 사람의 행동이나 작업을 자동으로 수행하는 프로그램이다. 악성 봇에 감염된 여러 컴퓨터를 공격자가 통제하면서 한 대상에 대량의 요청을 보내면 **분산 서비스 거부(DDoS) 공격**을 수행할 수 있다. 모든 봇이 악성인 것은 아니며, 선지는 공격에 이용되는 악성 봇을 설명한다.

② O: 스파이웨어(Spyware)는 **사용자의 동의 없이 정보를 수집·전송**하는 악성 소프트웨어이다. 금융정보, 신상정보, 암호 등을 몰래 수집해 외부로 유출하므로 사용자의 사생활과 정보의 기밀성을 침해한다.

③ X: NetBus는 원격 컴퓨터에 설치된 구성 요소를 통해 공격자가 해당 컴퓨터를 제어하도록 하는 백도어 프로그램이다. 원격으로 프로그램을 실행하거나 파일을 보내고 가져오는 등의 기능을 제공한다. 선지의 '자동적으로 광고를 표시하는 프로그램'은 **애드웨어(Adware)**에 대한 설명으로 고쳐야 한다.

④ O: 키로깅(Keylogging)은 **키보드로 입력한 내용을 가로채 기록**하는 행위이다. 사용자가 입력하는 계정명이나 암호도 기록될 수 있으므로, 이를 몰래 수행하면 인증정보 등을 탈취하는 수단이 된다.

NoteBase

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.

정답 4번

간단한 해설

④의 '나중에 행위나 이벤트를 부인할 수 없도록 한다'는 **부인방지**의 설명이다. 가용성은 **인가된 사용자가 필요한 때 정보와 서비스를 이용할 수 있도록** 보장하는 성질이다.

선지별 해설

① O: 인증(Authentication)은 **주체의 신원이나 정보의 진위를 확인**하는 서비스이다. 통신 상대가 주장하는 신원이 실제와 일치하는지, 전달된 정보가 주장된 출처에서 나온 것인지 등을 검증한다. 사용자가 제시한 비밀번호를 검증하여 본인인지 확인하는 것이 한 예이다.

② O: 기밀성(Confidentiality)은 **인가되지 않은 상대방에게 정보가 노출되지 않도록** 보호하는 성질이다. 저장된 정보와 전송 중인 정보 모두 보호 대상이므로, 온·오프라인에서 중요정보의 노출을 막는다는 설명에 부합한다.

③ O: 무결성(Integrity)은 정보가 **인가되지 않은 방식으로 생성·변경·삭제되지 않도록** 보호하는 성질이다. 송수신 과정에서 내용을 불법적으로 조작하거나 삭제하는 것을 막아 정보의 정확성과 완전성을 유지한다.

④ X: 행위나 이벤트가 발생했다는 증거를 제공하여 나중에 이를 부인하지 못하게 하는 서비스는 **부인방지(Non-repudiation)**이다. 가용성(Availability)은 인가된 사용자가 필요한 때 정보나 서비스에 접근하여 이용할 수 있도록 보장하는 성질이다. 예를 들어 서비스 거부 공격으로 정상 사용자가 시스템을 이용하지 못하면 가용성이 침해된다.

NoteBase

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

정답 2번

간단한 해설

TCP 플래그를 **하나도 설정하지 않은 패킷**을 보내는 방식은 NULL 스캔이다. 지문의 닫힌 포트는 RST를 보내고 열린 포트는 응답하지 않는 동작은 이 스캔의 기본 응답 규칙에 해당한다.

공통 해설

NULL 스캔은 **모든 TCP 플래그를 0으로 둔 패킷**을 보내 포트 상태를 조사하는 방식이다. 여기서 NULL은 패킷 자체가 없다는 뜻이 아니라 설정된 플래그가 없다는 뜻이다. 따라서 지문의 '모든 플래그가 세트되지 않은 TCP 패킷'이라는 조건이 NULL 스캔을 식별하는 기준이다.

지문과 같은 TCP 응답 규칙을 따르는 호스트에서는 닫힌 포트가 RST 패킷을 반환하고, 열린 포트는 해당 패킷에 응답하지 않는다. RST는 연결을 초기화하거나 거부할 때 사용하는 TCP 플래그이다. 다만 실제 네트워크에서는 방화벽이 패킷을 차단해도 응답이 없을 수 있으므로, **무응답만으로 열린 포트라고 확정할 수는 없다**. 이 경우에는 열림과 필터링을 구별하지 못한다.

NoteBase

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

① ChangeCipherSpec – Handshake 프로토콜에 의해 협상된 암호 규격과 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.

정답 3번

간단한 해설

Alert는 **오류·경고와 연결 종료를 알리는** SSL 프로토콜이다. ③의 보안 연관(SA) 설정과 보안 정책 데이터베이스(SPD) 조회는 **IPsec 관련 기능**이다.

선지별 해설

① O: ChangeCipherSpec은 Handshake에서 협상한 암호 규격과 키를 **이후 레코드부터 적용**하도록 알린다. 협상으로 준비한 보안 매개변수를 실제 송수신에 사용하는 상태로 전환하는 역할이다.

② O: Handshake는 사용할 암호 알고리즘을 협상하고 키 교환과 인증을 수행하여, 양쪽이 통신 보호에 필요한 공유 비밀을 마련하게 한다. **상호인증을 지원**하지만 모든 연결에서 양쪽 인증이 필수인 것은 아니다. 인증서를 이용한 클라이언트 인증은 서버의 요청 등에 따라 선택적으로 수행된다.

③ X: Alert는 SSL 통신 중 발생한 **오류·경고의 종류와 심각도**를 상대방에게 전달하고 연결 종료도 알린다. 치명적 오류를 알리는 Alert는 연결을 즉시 종료하게 한다. 보안 연관(SA)을 협상·설정하는 기능은 IPsec에서 사용하는 IKE와 관련되며, IP 패킷의 보안 정책 데이터베이스(SPD) 조회도 IPsec의 처리에 속한다. SPD는 해당 패킷을 보호할지, 그대로 통과시킬지, 폐기할지 등의 정책을 정하므로 SSL Alert의 기능과 구별된다.

④ O: Record는 Handshake·ChangeCipherSpec·Alert 및 응용계층의 메시지를 받아 **레코드 단위로 나누어** 전달한다. 협상된 방식에 따라 압축할 수 있으며, 압축하지 않는 방식도 허용된다. 이후 현재 적용 중인 보안 매개변수에 따라 MAC과 암호화 등의 보호 처리를 수행한다.

NoteBase

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.

정답 3번

간단한 해설

③의 '뒤에 이어지는 블록은 변경할 필요가 없다'는 설명은 블록 사이의 해시 연결을 무시한 것이다. 앞 블록의 내용이 바뀌면 해시값도 달라지므로, 연결을 유지하려면 **뒤따르는 블록의 이전 블록 해시 정보도 연쇄적으로 수정**해야 한다.

선지별 해설

① O: 블록체인은 거래 등의 기록을 여러 참여자가 나누어 보관하고 검증하는 분산원장 기술이다. 기록을 공유하고 위변조 여부를 확인하는 데 활용할 수 있으므로, **금융 이외의 분야에도 응용**할 수 있다. 예를 들어 물품의 생산·유통 이력을 기록하는 데 사용할 수 있다.

② O: 각 블록의 헤더에는 일반적으로 **이전 블록의 해시값**이 들어 있다. 해시값은 블록의 내용을 바탕으로 계산하는 값으로, 이를 참조하여 블록들이 순서대로 연결된다. 다만 맨 처음 생성되는 제네시스 블록에는 실제로 앞선 블록이 없다.

③ X: 앞 블록의 내용을 변경하면 그 블록의 해시값이 달라져, 다음 블록에 저장된 이전 블록 해시값과 일치하지 않게 된다. 연결을 유지하려면 **뒤따르는 블록의 해시 참조도 연쇄적으로 수정**해야 한다. 예를 들어 A → B → C로 연결된 상태에서 A를 바꾸면 B의 A 해시 참조를 바꾸어야 하고, 그 결과 B의 해시값도 달라지므로 C의 참조 역시 바꾸어야 한다. 이러한 연결 구조 때문에 앞선 기록의 변경을 탐지할 수 있다.

④ O: 블록은 크게 **헤더와 트랜잭션을 담은 본문**으로 구성된다. 트랜잭션은 거래나 상태 변경 등의 기록이며, 본문에는 이러한 트랜잭션의 집합이 들어간다. 헤더에는 이전 블록의 해시값 등 블록을 식별하고 검증하는 데 필요한 정보가 담긴다.

NoteBase

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

정답 2번

간단한 해설

전송 파일의 크기·경로와 함께 'b', 'o', 'ftp' 등이 기록되어 있어 **FTP 파일 전송 내역**임을 알 수 있다. 이 내역을 남기는 로그가 **xferlog**이다.

공통 해설

cat은 지정한 파일의 내용을 화면에 출력하는 명령이다. 모든 후보가 cat을 사용하므로, 제시된 기록을 저장하는 파일을 구별해야 한다. xferlog는 FTP 서버의 파일 전송 내역을 기록하며, 전송 시각·원격 호스트·전송 크기·파일 경로·전송 방식·방향·사용자명 등을 일정한 순서로 남긴다.

제시된 기록에서 198.188.2.2는 원격 호스트이고, 그 뒤의 861486은 전송된 바이트 수이다. 'b'는 바이너리 전송, 'o'는 **FTP 서버에서 외부로 나가는 전송**을 뜻한다. 'freeexam'은 사용자명, 'ftp'는 서비스명이고, 'c'는 전송 완료를 나타낸다. 이러한 필드 배열이 FTP 전송 로그의 특징이므로, 제시된 파일 경로 중 /var/log/xferlog가 해당한다. 이 파일의 내용을 출력하는 명령은 **cat /var/log/xferlog**이다.

NoteBase

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

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

정답 2번

간단한 해설

여러 호스트의 ICMP 응답을 피해자에게 집중시키는 것은 **Smurf Attack**이다. SYN 패킷으로 연결 대기 자원을 소모시키는 SYN Flooding Attack과 달리, **Land Attack**은 출발지·목적지 IP 주소와 포트를 각각 같게 조작한다.

대응 관계 해설

ㄱ. Smurf Attack: 공격자는 출발지 IP 주소를 피해자의 주소로 위조하고, 중계 네트워크의 브로드캐스트 주소로 ICMP Echo Request를 보낸다. 요청을 받은 여러 호스트의 Echo Reply가 위조된 출발지인 피해자에게 몰린다. 이처럼 **여러 호스트의 응답을 반사·증폭**하여 피해자의 네트워크와 처리 자원에 부담을 주는 방식이다.

ㄴ. SYN Flooding Attack: TCP 연결은 SYN → SYN+ACK → ACK의 3단계로 설정된다. 위조된 출발지 주소로 SYN을 계속 보내면 서버는 SYN+ACK를 보낸 뒤 마지막 ACK를 기다리게 된다. 이때 **연결이 완료되지 않은 대기 상태**가 대량으로 쌓여 정상적인 연결 요청을 처리하기 어려워진다.

ㄷ. Land Attack: SYN 패킷의 출발지 IP 주소와 목적지 IP 주소를 모두 피해자의 주소로, 출발지 포트와 목적지 포트도 같은 값으로 조작한다. 취약한 시스템에서 자기 자신을 상대로 연결을 처리하도록 하여 장애를 유발하는 공격이다. SYN 패킷을 사용한다는 점보다 **출발지와 목적지의 주소·포트가 각각 동일하다**는 점이 구별 기준이다.

ㄱ–Smurf Attack, ㄴ–SYN Flooding Attack, ㄷ–Land Attack의 대응은 ②의 조합과 일치한다.

NoteBase

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.

정답 1번

간단한 해설

①의 'RC4 알고리즘과 고정 암호키'는 전통적인 WEP의 특성이다. WPA2는 **AES 기반 CCMP**를 표준 암호화 방식으로 사용하며, 사전 공유키를 쓰더라도 이를 데이터 암호화에 그대로 쓰지 않고 **통신용 키를 별도로 생성**한다.

선지별 해설

① X: WPA2의 표준 암호화 방식은 **AES 기반 CCMP**이다. RC4와 고정 공유키를 사용하는 것은 전통적인 WEP의 특성이다. WPA2는 인증으로 얻은 키 또는 사전 공유키를 바탕으로 4-way 핸드셰이크를 수행하여 통신용 키를 생성한다. 따라서 사전 공유키가 고정되어 있을 수 있다는 사실과, 고정된 키를 데이터 암호화에 그대로 사용한다는 설명을 구별해야 한다.

② O: WPA는 **기업용 인증과 개인용 인증**을 지원한다. 기업용은 IEEE 802.1X 환경에서 EAP를 이용해 사용자를 인증하고, 개인용인 WPA-PSK는 단말과 무선 접속 장치가 미리 공유한 비밀키를 이용한다. 선지는 WPA가 지원하는 두 인증 방식을 설명한 것이다.

③ O: WEP는 짧은 초기화 벡터와 RC4 키 구성의 취약점 때문에 수집한 패킷을 분석하여 비밀키를 복구하는 공격에 취약하다. 통상 '64비트 WEP'는 **40비트 비밀키와 24비트 초기화 벡터**를 합한 길이로, 비밀키 자체가 64비트인 것은 아니다. 공격에 필요한 패킷이 충분히 확보되는 조건에서는 수분 내에 키가 복구될 수 있으며, 소요 시간은 트래픽과 공격 환경에 따라 달라진다.

④ O: WPA-PSK는 사전 공유키를 이용하는 WPA의 개인용 인증 방식이다. 원래 WPA의 암호화 방식인 TKIP는 RC4를 사용하면서도 **패킷별 키 혼합과 메시지 무결성 검사**를 도입하여 WEP의 취약점을 보완했다. 따라서 사전 공유키를 사용하더라도 WEP보다 강화된 통신 보호를 제공한다.

NoteBase

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
KS_a: 사용자 A의 개인키, KP_a: 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 $M \| E_{KS_a}[H(M)]$
④ $E_K[M \| E_{KS_a}[H(M)]]$

정답 4번

간단한 해설

메시지의 해시값에 **A의 개인키로 전자서명**하면 송신자 인증과 무결성을 확인할 수 있다. 원문과 서명을 묶어 **공유 비밀키로 전체를 암호화**하면 메시지의 기밀성도 보호된다.

구성 요소별 해설

해시와 전자서명: A는 메시지 M의 해시값 $H(M)$을 구하고, 자신의 개인키 KS_a로 서명한다. 문제에서는 이 서명을 $E_{KS_a}[H(M)]$으로 나타낸다. B는 A의 공개키 KP_a로 서명을 검증하여 **A가 서명한 메시지인지** 확인한다. 수신한 메시지에서 계산한 해시값이 서명으로 확인한 해시값과 일치하는지도 검사하므로 메시지의 무결성을 확인할 수 있다.

메시지와 서명의 연결: 원문과 서명을 $M \| E_{KS_a}[H(M)]$으로 연결한다. B가 원문으로 해시값을 다시 계산하고 서명을 검증할 수 있도록 둘을 함께 보내는 것이다. 다만 **서명만으로는 기밀성이 보장되지 않으므로** 원문을 그대로 전송하는 ③의 구성에는 암호화가 추가로 필요하다.

전체 암호화: 연결한 원문과 서명 전체를 A와 B의 공유 비밀키 K로 암호화한다. 전송할 함수는 $E_K[M \| E_{KS_a}[H(M)]]$이 된다. B는 먼저 공유 비밀키로 복호화하여 원문과 서명을 얻고, 이어 A의 공개키로 서명을 검증한다. **바깥쪽 암호화는 기밀성**을, 안쪽 전자서명은 송신자 인증과 무결성 확인을 담당한다.

이 구성이 ④에 해당한다. ①과 ②는 공유 비밀키를 사용하지만 A의 개인키로 생성한 전자서명이 없다. 공유 비밀키는 B도 알고 있으므로 그 키를 이용한 인증만으로는 A만 생성할 수 있는 전자서명을 대신할 수 없다.

NoteBase

문 11. 다음 알고리즘 중 공개키 암호 알고리즘에 해당하는 것은?

① SEED 알고리즘

② RSA 알고리즘

③ DES 알고리즘

④ AES 알고리즘

정답 2번

간단한 해설

RSA는 **공개키와 개인키를 구분하여 사용하는 비대칭키 암호**이다. 암호화와 복호화에 같은 비밀키를 사용하는 대칭키 암호와 구별된다.

공통 해설

공개키 암호는 서로 수학적으로 연결된 **공개키와 개인키**를 한 쌍으로 사용하는 비대칭키 암호이다. 기밀성을 위한 암호화에서는 송신자가 수신자의 공개키로 암호화하고, 수신자는 자신의 개인키로 복호화한다. 공개키는 다른 사람에게 알려 줄 수 있지만 개인키는 소유자가 비밀로 보관한다. RSA는 이러한 공개키 암호 알고리즘에 해당한다.

SEED, DES, AES는 모두 **대칭키 블록 암호**이다. 이들은 암호화와 복호화에 같은 비밀키를 사용하므로, 송신자와 수신자가 그 키를 안전하게 공유해야 한다. 따라서 공개키와 개인키를 구분하는 공개키 암호에 해당하지 않는다.

NoteBase

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.

정답 4번

간단한 해설

④의 설명은 미리 계산한 해시 정보를 활용하는 **레인보우 테이블 공격**에 해당한다. **차분 공격**은 평문 쌍의 차이가 암호문 쌍의 차이에 미치는 통계적 특성을 분석하여 암호키를 추정하는 방법이다.

선지별 해설

① O: 부인방지는 사용자가 메시지를 보내거나 거래를 수행했다는 사실을 나중에 부인할 수 없도록 **행위의 증거를 제공**하는 보안 성질이다. 전자서명은 서명자의 행위에 대한 증거를 제공하는 대표적인 수단이다.

② O: 최소권한은 계정에 **업무 수행에 필요한 최소한의 권한만 부여**하는 원칙이다. 예를 들어 자료 조회만 필요한 계정에는 수정·삭제 권한을 주지 않아, 계정이 오용되거나 탈취되었을 때의 피해 범위를 줄인다.

③ O: 키 위탁은 암호키를 신뢰할 수 있는 제3자 등에게 맡겨 보관하고, 정해진 조건에서 사용할 수 있도록 하는 방식이다. 사용자가 키를 분실하더라도 **위탁된 키를 통해 암호화된 자료를 복구**할 수 있도록 하는 것이 그 목적 중 하나이다.

④ X: 차분 공격은 같은 키로 암호화한 평문 쌍과 암호문 쌍을 대상으로 **입력 차이와 출력 차이 사이의 통계적 관계**를 분석하여 암호키를 추정한다. 선지처럼 해시 정보를 미리 계산해 두고 저장 공간과 탐색 시간을 절충하여 비밀번호를 찾는 방식은 레인보우 테이블 공격에 해당한다. 이는 해시 테이블을 이용하는 공격과 차분 분석을 혼동한 설명이다.

NoteBase

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, 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.

정답 2번

간단한 해설

②의 '보호프로파일은 보호목표명세서를 수용할 수 있다'는 관계가 잘못되었다. **ST가 PP의 공통 보안 요구사항을 수용하여 특정 평가대상에 맞게 구체화**할 수 있으며, PP가 특정 구현에 종속된 ST를 수용하는 관계는 아니다.

선지별 해설

① O: PP는 제품 유형에 공통으로 필요한 보안 요구사항을 기술하므로 **특정 구현에 독립적**이다. ST는 특정 평가대상(TOE)을 식별하고 그 대상의 보안 요구사항과 이를 충족하는 보안기능을 기술하므로 구현에 종속적이다.

② X: PP는 공통 보안 요구사항의 기준이고, ST는 특정 평가대상에 관한 명세이다. 따라서 **ST가 PP를 수용하여 해당 PP에 대한 적합성을 주장**할 수 있지만, PP가 ST를 수용하는 것은 아니다. PP는 다른 PP를 바탕으로 작성할 수 있다. 선지의 앞부분은 '보호프로파일은 다른 보호프로파일을 수용할 수 있다'로 고친다.

③ O: 하나의 PP는 **같은 유형의 여러 평가대상에 공통으로 적용**될 수 있다. 반면 하나의 ST는 특정한 하나의 평가대상을 기술한다. 예를 들어 방화벽 유형의 PP는 여러 방화벽 제품에 적용할 수 있지만, 각 제품의 ST는 해당 제품의 평가 범위와 보안 요구사항을 구체적으로 정한다. 이때 하나의 평가대상은 여러 구성요소로 이루어진 시스템일 수도 있다.

④ O: 오퍼레이션은 보안 요구사항의 매개변수를 정하거나 제시된 항목 중 필요한 것을 선택하는 등 요구사항을 구체화하는 작업이다. PP는 여러 구현에 적용되므로 할당·선택 사항을 미완료 상태로 남길 수 있다. ST는 특정 평가대상을 실제로 평가할 기준이므로 **미완료된 할당·선택 없이 필요한 오퍼레이션을 완료**해야 한다.

NoteBase

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

정답 1번

간단한 해설

NAT는 외부로 나가는 패킷의 **내부 IP 주소를 외부용 IP 주소로 변환**한다. 외부에는 변환된 주소가 보이므로 내부 호스트의 실제 주소 체계를 직접 노출하지 않을 수 있다.

공통 해설

Network Address Translation(NAT)은 서로 다른 주소 영역 사이에서 IP 주소를 변환하는 기술이다. 내부에서 사설 IP 주소를 사용하는 경우, 방화벽이나 경계 라우터가 외부로 나가는 패킷의 **출발지 주소를 공인 IP 주소로 바꾸어** 전달할 수 있다. 외부 상대는 변환된 주소를 보므로 내부 호스트의 사설 주소와 주소 구성을 직접 알기 어렵다.

예를 들어 내부 호스트 192.168.0.10이 외부 서버에 접속하면, NAT 장비는 출발지 주소를 외부 통신에 사용하는 공인 주소로 변환한다. 응답 패킷이 돌아오면 주소 대응 정보를 이용해 목적지 주소를 내부 주소로 되돌려 해당 호스트에 전달한다. 이처럼 **내부 주소와 외부에 보이는 주소를 분리**하는 방식이 문제에서 요구하는 내부 네트워크 구조의 노출 방지에 해당한다.

NoteBase

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

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

정답 1번

간단한 해설

민감정보 또는 고유식별정보의 처리가 수반되는 개인정보파일은 **5만 명 이상**, 별도의 정보 종류 조건 없이 규모를 기준으로 하는 개인정보파일은 **100만 명 이상**이 기준이다.

NoteBase

빈칸별 해설

「개인정보 보호법 시행령」 제35조는 개인정보를 전자적으로 처리할 수 있는 개인정보파일을 전제로 영향평가 대상의 기준을 정한다. 제시된 각 호는 모두 충족해야 하는 누적 조건이 아니라 어느 하나에 해당하는지를 판단하는 별도의 기준이다.

㉠ 5만 명: 제35조제1호는 구축·운용 또는 변경하려는 개인정보파일에서 5만 명 이상의 정보주체에 관한 **민감정보 또는 고유식별정보의 처리**가 수반되는 경우를 정한다. 이 정보 종류에 관한 조건이 붙은 기준은 10만 명이 아니라 5만 명이다.

㉡ 100만 명: 제35조제3호는 구축·운용 또는 변경하려는 개인정보파일에 관하여 **민감정보나 고유식별정보라는 별도 조건 없이** 정보주체의 수가 100만 명 이상인 경우를 정한다. 따라서 150만 명이 기준이 아니다. 제2호의 50만 명은 다른 개인정보파일과 연계한 결과에 적용되는 별도 기준이다.

㉠ 5만 명, ㉡ 100만 명의 조합은 ①에 해당한다.

NoteBase

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)

정답 4번

간단한 해설

스택 스매싱은 스택의 버퍼 오버플로우를 이용해 복귀 주소 등을 훼손하는 **공격 기법**이므로 대응책에 해당하지 않는다. 이를 탐지하는 방어 기법인 스택 가드와 구별한다.

선지별 해설

① O: 안전한 함수 사용은 **버퍼 크기에 맞게 입력·복사 길이를 제한**하여 버퍼의 경계를 넘어 데이터가 기록되는 것을 예방하는 방법이다. 크기 제한 기능이 있는 함수를 사용하더라도 실제 버퍼 크기에 맞는 제한값을 지정해야 한다.

② O: Non-Executable 스택은 **스택 영역의 코드 실행을 금지**하는 방법이다. 버퍼 오버플로우로 스택에 악성 코드가 삽입되더라도 그 코드의 실행을 차단한다. 메모리 덮어쓰기 자체를 막는 방법은 아니지만, 이를 이용한 코드 실행 공격에 대한 대응책이다.

③ O: 스택 가드는 스택의 버퍼와 복귀 주소 사이에 카나리라는 검사값을 두고, 함수가 복귀하기 전에 **카나리 값의 변조 여부를 검사**한다. 버퍼 오버플로우로 이 값이 달라졌다면 프로그램을 종료하는 등의 조치를 취해 변조된 복귀 주소가 사용되는 것을 막는다.

④ X: 스택 스매싱은 스택의 버퍼 경계를 넘어 데이터를 기록하여 복귀 주소 등 인접한 정보를 덮어쓰고, 프로그램의 실행 흐름을 바꾸려는 **공격 기법**이다. 버퍼 오버플로우를 방어하는 방법이 아니라 이를 악용하는 방법에 해당한다.

NoteBase

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.

정답 3번

간단한 해설

과거 블록의 내용을 바꾸면 **해시 연결이 달라져 변조가 드러난다**. 작업증명 방식에서는 변경한 블록과 이후 블록들의 작업증명까지 다시 수행하고 정상 체인의 누적 작업량을 따라잡아야 하므로, 과거 기록을 쉽게 조작할 수 없다.

NoteBase

선지별 해설

① O: 기본적인 암호화폐 송금에서는 송신자가 개인키로 거래에 전자서명을 하고, 다른 참여자는 공개키로 이를 검증한다. 이를 통해 **거래를 승인할 권한과 서명 대상 데이터의 무결성**을 확인한다. 다만 '한 개씩'은 단순한 거래 구조를 전제로 한 설명이며, 실제로는 여러 입력이나 다중서명 조건 때문에 한 거래에 여러 서명이 필요할 수 있다. 모든 블록체인 거래의 서명 수가 반드시 하나로 고정되는 것은 아니다.

② O: 작업증명 방식에서는 블록의 해시값이 정해진 목표값보다 작아지도록 논스 등의 값을 바꾸며 반복 계산한다. 조건을 충족하는 값을 찾기는 어렵지만 결과를 검증하기는 쉽다. 유효한 블록이 네트워크에서 받아들여지면 채굴자는 **프로토콜이 정한 블록 보상**을 받을 수 있다. 해시를 이용한 어려운 계산으로 블록을 추가하고 암호화폐를 보상받을 수 있다는 설명은 이러한 채굴 과정을 뜻한다.

③ X: 블록은 이전 블록의 해시값을 포함하여 연결된다. 과거 블록의 거래 내용을 바꾸면 해당 블록의 해시가 달라져 이후 블록과의 연결이 맞지 않게 된다. 작업증명 체인에서 변경한 기록을 받아들여지게 하려면 해당 블록과 뒤따르는 블록의 작업증명을 다시 수행하고, 계속 성장하는 정상 체인의 누적 작업량도 따라잡아야 한다. 따라서 과거 블록의 내용을 조작하는 것은 **쉽지 않다**. 이는 조작이 논리적으로 절대 불가능하다는 뜻이 아니라, 정상 참여자가 충분한 연산 능력을 유지하는 조건에서 조작에 막대한 비용이 든다는 뜻이다.

④ O: 분산된 참여자들이 동일한 거래 기록을 유지하려면 어떤 블록과 체인을 받아들일지 정하는 **합의 규칙**이 필요하다. 작업증명 방식에서는 거래와 블록의 유효성을 확인하고, 유효한 체인 가운데 누적 작업량이 가장 큰 체인을 선택하는 규칙으로 기록을 일치시킨다. 작업증명은 이러한 합의를 구현하는 대표적인 기법이며, 모든 블록체인이 반드시 작업증명을 사용하는 것은 아니다.

NoteBase

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

정답 3번

간단한 해설

③의 지정 주체는 지방자치단체장이 아니라 **행정안전부장관**이다. 지방자치단체장이 관리·감독하는 기관의 시설은 행정안전부장관이 **지방자치단체장과 협의하여 지정할 수 있다**.

선지별 해설

① O: 취약점 분석·평가는 시설의 보안상 약점을 찾아 위험을 평가하는 절차이다. 「정보통신기반 보호법」 제9조제1항에 따라 관리기관의 장은 대통령령으로 정하는 바에 따라 소관 주요정보통신기반시설의 취약점을 **정기적으로 분석·평가하여야 한다**. 사고가 발생한 뒤에만 실시하는 임의적 조치가 아니다.

② O: 법 제8조제1항은 **중앙행정기관의 장**에게 소관 분야 시설의 지정 권한을 부여한다. 업무의 국가사회적 중요성, 정보통신기반시설에 대한 의존도, 침해사고의 피해규모와 범위 등을 고려하여 전자적 침해행위로부터 보호할 필요가 있다고 인정되는 시설을 주요정보통신기반시설로 지정할 수 있다.

③ X: 법 제8조제4항에 따라 지방자치단체장이 관리·감독하는 기관의 정보통신기반시설은 **행정안전부장관이 지방자치단체장과 협의하여** 주요정보통신기반시설로 지정하거나 그 지정을 취소할 수 있다. 지방자치단체장은 협의 상대방이며, 해당 시설을 직접 지정하는 주체가 아니다.

④ O: 법 제8조의2제1항에 따라 과학기술정보통신부장관과 국가정보원장등은 지정 필요성이 있다고 판단하면 중앙행정기관의 장에게 해당 시설을 주요정보통신기반시설로 **지정하도록 권고할 수 있다**. 여기서 권고는 지정 필요성을 제시하는 행위이며, 지정 자체와는 구별된다.

NoteBase

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.

정답 3번

간단한 해설

콜드 사이트는 주전산센터와 동일한 장비를 미리 갖추는 방식이 아니라, **공간·전원 등 기반시설을 확보**해 두는 방식이다. 재난 발생 후 장비를 반입·설치하고 데이터를 복원해야 하므로 복구에 시간이 오래 걸린다.

선지별 해설

① O: 업무연속성계획(BCP)은 장애나 재난에도 핵심 업무를 유지하고 복구하기 위한 계획이다. 따라서 **평상시의 중단 예방과 재난 후의 업무 유지·복구**를 함께 다룬다. 예비 설비 등 예방 대책뿐 아니라 대체 업무 수행 방법과 복구 절차도 마련해야 한다.

② O: 미러 사이트는 주전산센터에 대응하는 시스템을 갖추고 **데이터를 실시간으로 복제**하는 백업센터이다. 재난 후 장비를 새로 설치하거나 오래된 백업을 복원하는 작업을 최소화할 수 있어, 콜드·웜·핫 사이트와 비교할 때 가장 짧은 시간에 서비스를 전환·복구할 수 있다.

③ X: 콜드 사이트는 복구에 필요한 공간, 전원, 냉방 등 **기반시설 위주로 준비한 장소**이다. 주전산센터와 동일한 장비를 미리 구비하는 방식이 아니며, 재난 발생 후 필요한 장비를 반입·설치하고 소프트웨어와 데이터를 복원해야 한다. 필요한 시스템 장비를 미리 갖추는 것은 핫 사이트의 특징이고, 여기에 실시간 데이터 복제까지 갖추면 미러 사이트에 해당한다.

④ O: 웜 사이트는 기반시설 외에 **일부 시스템 장비도 미리 갖추는** 방식이다. 기반시설 위주로 준비하는 콜드 사이트보다 장비 확보와 관리에 드는 비용이 추가되므로 구축·유지비용이 높다. 대신 재난 후 준비해야 할 작업이 줄어 복구 시간은 짧아진다.

NoteBase

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 관리하여야 한다.

정답 1번

간단한 해설

공공기관의 영상정보처리기기 운영에 관한 **재위탁이 일률적으로 금지되는 것은 아니다**. 시행령은 위탁 문서에 '재위탁 제한에 관한 사항'을 포함하도록 규정한다.

선지별 해설

① X: 재위탁은 위탁받은 업무를 다시 다른 자에게 맡기는 것이다. 「개인정보 보호법 시행령」 제26조제1항제2호는 공공기관이 영상정보처리기기의 설치·운영 사무를 위탁할 때 문서에 **재위탁 제한에 관한 사항**을 포함하도록 한다. 재위탁을 전면 금지하는 규정이 아니라, 위탁 문서에 재위탁의 제한을 정하도록 한 규정이므로 '재위탁하여 운영할 수 없다'고 단정할 수 없다.

② O: 시행령 제16조는 전자적 파일 형태의 개인정보를 파기하는 방법으로 **복원이 불가능한 방법으로 영구 삭제**하는 것을 규정한다. 파일이 화면에서 보이지 않게 하는 데 그치는 것이 아니라, 삭제한 개인정보를 복원할 수 없도록 해야 한다는 것이 파기의 원칙이다.

③ O: 시행령 제17조는 전화를 이용한 동의를 허용한다. 이때에는 **동의 내용을 알리고 동의의 의사표시를 확인**해야 한다. 전화로 내용을 전달하기만 하는 것으로는 부족하며, 정보주체가 그 내용에 동의하는지도 확인해야 한다.

④ O: 시행령 제15조제1호에 따라 공공기관이 법에서 허용한 사유로 개인정보를 목적 외로 이용하거나 제3자에게 제공할 때에는 **개인정보 또는 개인정보파일의 명칭**을 목적 외 이용 및 제3자 제공 대장에 기록·관리해야 한다. 이는 어떤 개인정보를 이용하거나 제공했는지 식별하기 위한 기록이며, 같은 조에 따라 이용 목적과 법적 근거 등도 함께 관리한다.

NoteBase