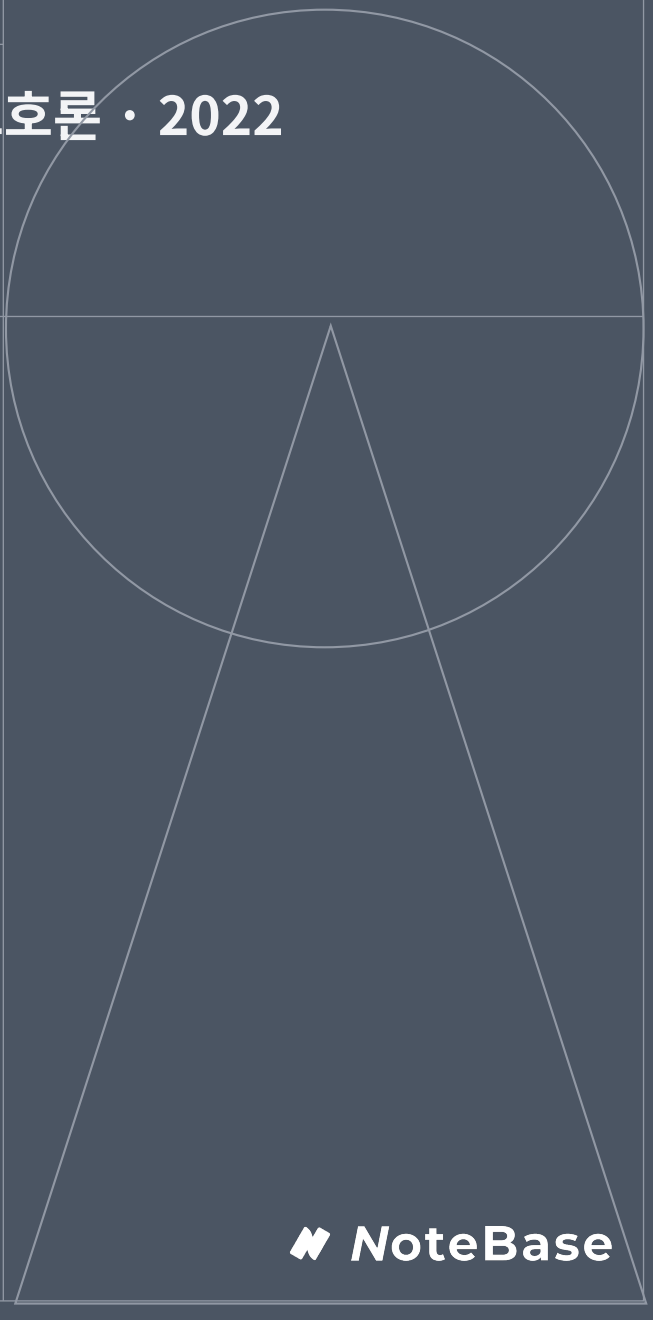
기출OX 해설집

공무원/지방직/9급 · 정보보호론 · 2022



NoteBase

기출OX 해설집

공무원/지방직/9급 · 정보보호론 · 2022

공무원/지방직/9급 · 정보보호론 · 2022

문 1. 송·수신자의 MAC 주소를 가로채 공격자의 MAC 주소로 변경하는 공격은?

① ARP spoofing

② Ping of Death

③ SYN Flooding

④ DDoS

정답 1번

간단한 해설

ARP spoofing은 **IP 주소와 MAC 주소의 대응 정보를 위조**하여 상대방에게 보낼 통신이 공격자에게 향하게 하는 공격이다. 통신 상대의 MAC 주소를 공격자의 것으로 믿게 한다는 점이 핵심이다.

핵심 풀이

ARP spoofing: ARP는 같은 네트워크에서 IP 주소에 대응하는 MAC 주소를 알아내는 프로토콜이다. 공격자는 거짓 ARP 정보를 보내 피해자의 ARP 캐시에 **상대방 IP 주소와 공격자 MAC 주소가 대응하도록** 만든다. 예를 들어 수신자 IP 주소에 대응하는 MAC 주소를 공격자의 것으로 믿게 하면, 송신자가 수신자에게 보내는 프레임이 공격자에게 전달된다. 이때 바뀌는 것은 ARP 캐시에 저장된 IP–MAC 주소 대응 정보이다.

다른 공격과의 구분: Ping of Death, SYN Flooding, DDoS는 **서비스의 정상 이용을 방해하는 서비스 거부 공격**에 해당한다. 이 문항에서처럼 MAC 주소의 대응 정보를 속여 통신이 공격자에게 향하게 하는 것이 이들 공격의 핵심 수법은 아니다.

NoteBase

문 2. 스니핑 공격의 탐지 방법으로 옳지 않은 것은?

① ping을 이용한 방법

② ARP를 이용한 방법

③ DNS를 이용한 방법

④ SSID를 이용한 방법

정답 4번

간단한 해설

SSID는 **무선 LAN을 구별하는 네트워크 이름**이다. SSID를 확인하는 것만으로는 패킷을 몰래 수집하는 호스트를 탐지할 수 없다.

선지별 해설

① O: ping을 이용한 탐지는 같은 이더넷 구간에서 의심 호스트의 IP 주소를 목적지로 지정하되, **목적지 MAC 주소를 그 호스트의 주소와 다르게** 설정한 ICMP Echo Request를 보내는 방식이다. 정상적인 MAC 주소 필터링에서는 이 프레임을 버리지만, 무차별 모드에서 프레임을 받아 운영체제가 처리하면 응답할 수 있다. 이 반응을 스니핑의 징후로 이용한다. 일반적인 ping에 응답한다는 사실만으로 스니핑을 판정하는 것은 아니다.

② O: ARP는 같은 네트워크에서 IP 주소에 대응하는 MAC 주소를 알아내는 프로토콜이다. ARP를 이용한 탐지는 의심 호스트의 IP 주소에 대한 ARP 요청을 **정상적으로는 수신하지 않을 목적지 MAC 주소**로 보내 응답 여부를 관찰한다. 무차별 모드에서는 이런 프레임까지 받아 처리할 수 있으므로, 응답을 해당 모드의 징후로 삼는다. ping 방식과 마찬가지로 운영체제와 드라이버의 필터링 방식에 따라 탐지 결과가 달라질 수 있다.

③ O: 일부 스니퍼는 수집한 패킷의 IP 주소를 호스트 이름으로 표시하려고 **DNS 역방향 조회**를 수행한다. 이를 이용해 사용하지 않는 IP 주소를 넣은 유인 패킷을 흘린 뒤, 그 주소를 조회하는 DNS 요청이 발생하는지 관찰한다. 해당 패킷을 수집한 프로그램이 이름을 알아보려는 동작을 탐지하는 원리이다. 스니퍼가 주소 조회를 하지 않으면 이 방식으로는 탐지하기 어렵다.

④ X: SSID(Service Set Identifier)는 **무선 LAN을 식별하는 이름**이다. 사용자가 접속할 무선 네트워크를 구별하는 데 쓰이며, 패킷을 몰래 수집하는 동작이나 무차별 모드 여부를 나타내지 않는다. 따라서 SSID를 이용하는 것은 스니핑 탐지 방법에 해당하지 않으며, 스니핑 징후는 ping·ARP에 대한 비정상적인 응답이나 유인 패킷에 뒤따르는 DNS 조회 등으로 확인한다.

NoteBase

문 3. 공격자가 해킹을 통해 시스템에 침입하여 루트 권한을 획득한 후, 재침입할 때 권한을 쉽게 획득하기 위하여 제작된 악성 소프트웨어는?

① 랜섬웨어
② 논리폭탄
③ 슬래머 웜
④ 백도어

정답 4번

간단한 해설

침입 후 다시 접근하기 쉽도록 **정상적인 인증 절차를 우회하는 통로**를 남기는 악성 소프트웨어가 백도어이다. 문제의 '재침입할 때 권한을 쉽게 획득'한다는 목적이 핵심 단서이다.

핵심 풀이

백도어는 정상적인 인증이나 접근 통제를 우회하여 시스템에 접근할 수 있게 하는 숨겨진 통로이다. 루트 권한은 시스템을 관리할 수 있는 최상위 권한이다. 공격자는 이를 획득한 뒤 백도어를 설치하여, 다음 접속 때 같은 침입 과정을 반복하지 않고 시스템에 접근하거나 권한을 확보할 수 있게 한다. 따라서 문제에서 강조하는 것은 최초 침입 자체보다 **침입 후 재접근을 쉽게 만드는 기능**이다.

다른 선택지와의 구분: 랜섬웨어는 파일 암호화 등의 수단으로 사용을 제한하고 금전을 요구하며, 논리폭탄은 **미리 정한 조건이 충족될 때** 악성 동작을 실행한다. 슬래머 웜은 SQL 서버의 취약점을 이용해 네트워크로 빠르게 전파되는 웜이다. 이들의 대표적 특징인 금전 요구·조건부 실행·자기 전파는 문제의 재침입 통로 확보와 구별된다.

NoteBase

문 4. 다음에서 설명하는 용어는?

◯ 한 번의 시스템 인증을 통해 다양한 정보시스템에 재인증 절차 없이 접근할 수 있다.
◯ 이 시스템의 가장 큰 약점은 일단 최초 인증 과정을 거치면, 모든 서버나 사이트에 접속할 수 있다는 것이다.

① NAC(Network Access Control)
② SSO(Single Sign On)
③ DRM(Digital Right Management)
④ DLP(Data Leak Prevention)

정답 2번

간단한 해설

SSO(통합 인증)는 한 번 로그인한 인증 결과를 여러 연계 시스템에서 이용하여 반복 로그인을 줄이는 방식이다. 하나의 인증 수단이 침해되면 여러 서비스로 피해가 확산될 수 있다.

핵심 풀이

SSO(Single Sign On): **한 번의 인증 결과를 여러 연계 시스템에서 이용**하는 통합 인증 방식이다. 예를 들어 통합 포털에 로그인한 뒤 연계된 업무 시스템으로 이동할 때 아이디와 비밀번호를 다시 입력하지 않는 경우가 이에 해당한다. 지문의 '재인증 절차 없이 다양한 정보시스템에 접근'한다는 설명이 결정적인 단서이다.

공통 인증의 위험: SSO 계정이나 로그인 세션이 탈취되면 공격자가 여러 연계 서비스에 접근할 수 있어 피해 범위가 커질 수 있다. 다만 지문의 '모든 서버나 사이트'는 **SSO에 연계되어 해당 사용자에게 접근 권한이 있는 시스템**을 뜻한다. SSO가 개별 시스템의 권한 제한까지 없애는 것은 아니다.

NAC와의 구분: NAC는 사용자나 단말의 인증 상태, 보안 상태 등을 확인하여 **네트워크 접속을 통제**한다. 여러 서비스에서 로그인 절차를 반복하지 않게 하는 SSO와는 통제의 목적이 다르다.

NoteBase

문 5. 보안 공격 유형에는 적극적 공격과 소극적 공격이 있다. 다음 중 공격 유형이 다른 하나는?

① 메시지 내용 공개(release of message contents)

② 신분 위장(masquerade)

③ 메시지 수정(modification of message)

④ 서비스 거부(denial of service)

정답 1번

간단한 해설

메시지 내용 공개는 통신 내용을 바꾸지 않고 몰래 알아내는 **소극적 공격**이다. 공격의 피해가 큰지보다 정보를 관찰하는 데 그치는지, 통신이나 서비스 동작에 개입하는지가 구분 기준이다.

선지별 해설

소극적 공격은 통신 내용을 관찰하거나 수집하는 데 그친다. 적극적 공격은 메시지를 조작하거나 신분을 위장하는 등 통신에 개입하고, 정상적인 서비스 동작을 방해하기도 한다.

① 메시지 내용 공개: 전송되는 메시지를 도청하여 권한 없이 내용을 알아내는 **소극적 공격**이다. 메시지 자체를 변경하지 않으면서 비밀 정보를 노출시키므로 기밀성을 침해한다.

② 신분 위장: 공격자가 다른 사용자나 시스템인 것처럼 행동하는 **적극적 공격**이다. 정당한 사용자인 것처럼 요청이나 메시지를 보내 통신에 개입하므로 단순한 관찰과 구별된다.

③ 메시지 수정: 전송 중인 메시지의 내용을 바꾸는 **적극적 공격**이다. 예를 들어 송금 요청의 금액을 변경하면 수신자가 원래와 다른 내용을 받게 되므로 무결성을 침해한다.

④ 서비스 거부: 정상적인 사용자가 서비스를 이용하지 못하도록 방해하는 **적극적 공격**이다. 메시지 내용을 바꾸지 않더라도 시스템 자원을 고갈시키거나 통신을 방해하여 가용성을 침해한다.

따라서 ①만 소극적 공격이고 ②·③·④는 적극적 공격이므로, 공격 유형이 다른 것은 ①의 메시지 내용 공개이다.

NoteBase

문 6. X.509 인증서 폐기 목록(Certificate Revocation List) 형식 필드에 포함되지 않는 것은?

① 발행자 이름(Issuer name)

② 사용자 이름(Subject name)

③ 폐지된 인증서(Revoked certificate)

④ 금번 업데이트 날짜(This update date)

정답 2번

간단한 해설

사용자 이름(Subject name)은 **개별 인증서의 주체를 식별하는 필드**이다. CRL은 사용자 이름을 나열하는 대신 **폐기된 인증서의 일련번호**를 기록한다.

선지별 해설

CRL은 폐기된 인증서의 정보를 담아 서명하여 배포하는 목록이다. 각 선지는 이 목록의 구성 필드에 해당하는지를 판단한다.

① O: 발행자 이름(Issuer name)은 CRL에 서명하고 이를 발행한 주체를 식별한다. 개별 인증서의 소유자가 아니라 **CRL 발행자의 이름**을 나타내는 필드이다.

② X: 사용자 이름(Subject name)은 개별 X.509 인증서에서 그 공개키와 연결된 사람이나 시스템 등의 주체를 식별하는 필드이며, **CRL의 기본 필드가 아니다**. CRL에서는 폐기된 인증서를 사용자 이름이 아니라 인증서 일련번호로 식별한다.

③ O: 폐지된 인증서(Revoked certificate) 목록은 CRL의 구성 필드이다. 각 항목에는 폐기된 인증서의 **일련번호와 폐기 일시**가 기록된다. 폐기된 인증서가 없으면 이 목록은 생략된다.

④ O: 금번 업데이트 날짜(This update date)는 **현재 CRL의 발행 일시**를 나타낸다. 다음 CRL이 발행되어야 할 시한을 나타내는 nextUpdate와 구별된다.

NoteBase

문 7. AES 알고리즘에 대한 설명으로 옳지 않은 것은?

① 블록 암호 체제를 갖추고 있다.

② 128/192/256bit 키 길이를 제공하고 있다.

③ DES 알고리즘을 보완하기 위해 고안된 알고리즘이다.

④ 첫 번째 라운드를 수행하기 전에 먼저 초기 평문과 라운드 키의 NOR 연산을 수행한다.

정답 4번

간단한 해설

④의 'NOR 연산'은 **XOR(배타적 논리합) 연산**으로 고쳐야 한다. AES는 첫 번째 라운드 전에 평문 블록과 초기 라운드 키를 XOR하는 AddRoundKey를 수행한다.

선지별 해설

① O: AES는 데이터를 **128비트 블록 단위**로 처리하는 대칭키 블록 암호이다. 평문 블록을 키에 따라 같은 크기의 암호문 블록으로 변환한다.

② O: AES가 지원하는 키 길이는 **128비트·192비트·256비트**이다. 키 길이가 달라져도 블록 크기는 128비트로 일정하므로, 키 길이와 블록 크기를 구분해야 한다.

③ O: AES는 DES의 56비트 키에 따른 보안 한계 등을 극복하고 **DES를 대체**하기 위해 마련된 암호 표준이다. 선지의 '보완'은 이러한 보안 한계를 개선한다는 의미이다.

④ X: 첫 번째 라운드 전에 평문 블록과 초기 라운드 키를 결합하는 연산은 NOR가 아니라 **XOR를 사용하는 AddRoundKey**이다. XOR는 대응하는 두 비트가 다르면 1, 같으면 0을 출력한다. 이 초기 키 결합을 마친 뒤 첫 번째 라운드의 SubBytes 등 변환을 수행한다.

NoteBase

문 8. 정보기술과 보안 평가를 위한 CC(Common Criteria)의 보안 기능적 요구 조건에 해당하지 않는 것은?

① 암호 지원

② 취약점 평가

③ 사용자 데이터 보호

④ 식별과 인증

정답 2번

간단한 해설

취약점 평가는 제품이 제공할 보안 기능이 아니라, 제품의 취약점과 공격에 대한 저항성을 확인하는 **보안 보증 요구 조건(AVA)**에 속한다. 보안 기능적 요구 조건과 보안 보증 요구 조건을 구분해야 한다.

선지별 해설

CC의 보안 기능적 요구 조건은 평가 대상이 제공해야 할 보안 기능을, 보안 보증 요구 조건은 그 보안성을 평가하고 신뢰할 근거를 확보하기 위한 요구를 규정한다.

① O: 암호 지원(FCS)은 **암호 연산과 암호키 관리**에 관한 보안 기능적 요구 조건이다. 암호 알고리즘을 이용한 데이터 보호와 암호키의 생성·분배·파기 등에 필요한 기능을 규정한다.

② X: 취약점 평가(AVA)는 보안 기능적 요구 조건이 아니라 **보안 보증 요구 조건**이다. 평가 대상에 악용 가능한 취약점이 있는지 분석하고, 침투 시험 등으로 공격에 대한 저항성을 확인한다. 제품이 '어떤 보안 기능을 제공하는가'보다 그 보안성을 '어떻게 확인하는가'에 해당한다.

③ O: 사용자 데이터 보호(FDP)는 접근 통제, 정보 흐름 통제 등으로 **사용자 데이터를 보호하는 기능**에 관한 요구 조건이다. 예를 들어 허가받지 않은 사용자의 데이터 접근을 제한하거나, 데이터가 허용된 경로로만 흐르도록 통제한다.

④ O: 식별과 인증(FIA)은 사용자가 누구인지 구별하고, **주장한 신원이 실제로 맞는지 확인**하는 기능에 관한 요구 조건이다. 사용자 ID로 계정을 식별하고 비밀번호 등으로 그 신원을 확인하는 것이 이에 해당한다.

NoteBase

문 9. 커버로스(Kerberos) 버전 4에 대한 설명으로 옳지 않은 것은?

① 사용자를 인증하기 위해 사용자의 패스워드를 중앙집중식 DB에 저장하는 인증 서버를 사용한다.

② 사용자는 인증 서버에게 TGS(Ticket Granting Server)를 이용하기 위한 TGT(Ticket Granting Ticket)를 요청한다.

③ 인증 서버가 사용자에게 발급한 TGT는 유효기간 동안 재사용할 수 있다.

④ 네트워크 기반 인증 시스템으로 비대칭 키를 이용하여 인증을 수행한다.

정답 4번

간단한 해설

④의 '비대칭 키'는 **대칭키**로 고쳐야 한다. Kerberos 버전 4는 대칭키 암호인 **DES**로 티켓과 인증 정보를 보호하여 인증을 수행한다.

선지별 해설

① O: Kerberos는 신뢰할 수 있는 중앙 인증 서버가 사용자의 인증 정보를 관리한다. 사용자마다 개별 서비스 서버에 패스워드를 등록하는 대신 중앙 DB를 이용한다. 이때 저장하는 인증용 키는 **패스워드에서 유도한 비밀키**이므로, 선지의 패스워드 저장을 평문 패스워드를 그대로 저장한다는 뜻으로 이해해서는 안 된다.

② O: 사용자는 먼저 인증 서버(AS)에 **TGS를 이용하기 위한 TGT**를 요청한다. TGT는 개별 서비스를 바로 이용하는 티켓이 아니라, TGS에서 해당 서비스용 티켓을 발급받을 때 사용자의 신원을 증명하는 티켓이다. 따라서 AS에서 TGT를 받은 뒤, 이를 TGS에 제시하여 필요한 서비스용 티켓을 받는다.

③ O: 발급받은 TGT는 **유효기간 안에서 여러 번 사용**할 수 있다. 사용자는 다른 서비스용 티켓이 필요할 때도 기존 TGT를 TGS에 제시할 수 있어, 매번 AS에서 TGT를 새로 받거나 패스워드를 다시 입력할 필요가 없다. 다만 TGT와 함께 제시하는 인증자에는 현재 시각 등을 넣어 요청마다 새로 생성하므로, 티켓의 재사용과 이전 인증 요청의 재전송은 구별된다.

④ X: Kerberos 버전 4는 네트워크 기반 인증 시스템이지만, 인증에 사용하는 암호 방식은 **DES 기반 대칭키 방식**이다. 대칭키 방식은 같은 비밀키로 암호화와 복호화를 수행한다. AS와 TGS가 공유하는 비밀키로 TGT를 보호하고, 사용자와 서버 사이의 인증에는 분배된 세션키 등을 사용한다. 따라서 '비대칭 키를 이용하여 인증을 수행한다'는 설명은 대칭키 방식으로 고쳐야 한다.

NoteBase

문 10. 다음에서 설명하는 보안 공격은?

◯ 정상적인 HTTP GET 패킷의 헤더 부분의 마지막에 입력되는 2개의 개행 문자(\r\n\r\n) 중 하나(\r\n)를 제거한 패킷을 웹 서버에 전송할 경우, 웹 서버는 아직 HTTP 헤더 정보가 전달되지 않은 것으로 판단하여 계속 연결을 유지하게 된다.
◯ 제한된 연결 수를 모두 소진하게 되어 결국 다른 클라이언트가 해당 웹 서버에 접속할 수 없게 된다.

① HTTP Cache Control
② Smurf
③ Slowloris
④ Replay

정답 3번

간단한 해설

HTTP 헤더의 끝을 알리는 빈 줄을 보내지 않아 서버가 **불완전한 요청을 기다리며 연결을 유지**하게 하는 것은 Slowloris의 특징이다. 이러한 연결이 누적되면 연결 자원이 소진되어 정상 이용자가 접속하지 못한다.

핵심 풀이

헤더 종료 표시: HTTP 요청에서 헤더 영역은 빈 줄로 끝나며, 마지막 헤더 뒤의 \r\n\r\n이 이를 나타낸다. 지문처럼 마지막 \r\n을 보내지 않으면 헤더 영역을 끝내는 빈 줄이 없어 서버는 **헤더 수신이 아직 끝나지 않은 상태**로 보고 나머지 데이터를 기다린다.

연결 자원 소진: Slowloris는 이처럼 불완전한 HTTP 요청으로 여러 연결을 오래 유지하여 웹 서버의 연결 자원을 점유하는 서비스 거부 공격이다. 서버가 기다리는 연결이 늘어나 허용된 연결 수가 소진되면 정상 클라이언트의 새 연결을 받아들이지 못한다. 지문의 핵심은 **HTTP 헤더를 완성하지 않아 연결을 점유**한다는 점이다.

Smurf와의 구분: Smurf는 피해자의 IP 주소로 출발지 주소를 위조한 ICMP 요청을 브로드캐스트하여 여러 호스트의 응답이 피해자에게 몰리게 하는 공격이다. 같은 서비스 거부 공격이라도 Smurf는 응답 트래픽의 증폭을 이용하고, Slowloris는 미완성 HTTP 요청에 따른 연결 점유를 이용한다.

NoteBase

문 11. (가), (나)에 들어갈 접근통제 보안모델을 바르게 연결한 것은?

(가)은 허가되지 않은 방식의 접근을 방지하는 모델로 정보 흐름 모델 최초의 수학적 보안모델이다.
(나)은 비즈니스 입장에서 직무분리 개념을 적용하고, 이해가 충돌되는 회사 간의 정보의 흐름이 일어나지 않도록 접근통제 기능을 제공하는 보안모델이다.

① (가): Bell-LaPadula Model, (나): Biba Integrity Model
② (가): Bell-LaPadula Model, (나): Brewer-Nash Model
③ (가): Clark-Wilson Model, (나): Biba Integrity Model
④ (가): Clark-Wilson Model, (나): Brewer-Nash Model

정답 2번

간단한 해설

Bell-LaPadula 모델은 보안등급에 따른 정보 흐름을 통제하여 **기밀성**을 보호한다. Brewer-Nash 모델은 **이해가 충돌하는 회사 간의 정보 흐름**을 막으므로, (나)는 '직무분리'라는 표현보다 이해상충 방지라는 목적에 주목해야 한다.

빈칸별 해설

(가) Bell-LaPadula Model: 주체와 객체의 보안등급을 비교하여 접근을 통제하는 수학적 보안모델이며, 보호 목표는 **기밀성**이다. 기본 규칙인 '상위 등급 읽기 금지'는 자신의 등급보다 높은 비밀정보를 읽지 못하게 하고, '하위 등급 쓰기 금지'는 읽은 비밀정보를 낮은 등급의 객체에 기록하여 유출하는 것을 막는다. 이처럼 보안등급 사이의 정보 흐름을 제한한다는 점이 지문의 설명과 연결된다. 반면 Clark-Wilson 모델은 인가된 처리 절차와 직무분리를 통해 상업적 시스템의 데이터 무결성을 유지하는 데 초점을 둔다.

(나) Brewer-Nash Model: '만리장성 모델' 또는 'Chinese Wall 모델'이라고 하며, 이해상충 관계에 있는 회사들의 비공개 정보가 한 주체를 통해 섞이거나 전달되는 것을 막는다. **이전에 접근한 회사 정보에 따라** 이후의 접근 허용 범위가 달라진다. 예를 들어 A사와 B사가 경쟁 관계라면, A사의 비공개 정보에 접근한 분석가가 B사의 비공개 정보에도 접근하는 것을 제한한다. '직무분리'만 보면 Clark-Wilson 모델을 떠올릴 수 있지만, 여기서는 경쟁 회사 간 이해상충 방지가 결정적 단서이다. Biba Integrity 모델은 무결성 등급에 따라 접근을 통제하여 데이터가 오염되는 것을 막는 모델이므로, 이러한 회사 간 이해상충을 기준으로 삼는 모델과 구별된다.

(가)에 Bell-LaPadula Model, (나)에 Brewer-Nash Model을 연결한 조합은 ②이다.

NoteBase

문 12. 리눅스 시스템에서 umask값에 따라 새로 생성된 디렉터리의 접근 권한이 ‘drwxr-xr-x’일 때 기본 접근 권한을 설정하는 umask의 값은?

① 002

② 020

③ 022

④ 026

정답 3번

간단한 해설

umask는 새 디렉터리에서 **제거할 권한**을 지정한다. 'rwxr-xr-x'는 소유자의 권한은 그대로 두고 그룹과 기타 사용자의 쓰기 권한만 제거한 상태이므로 umask는 022이다.

공통 해설

umask의 세 자리는 왼쪽부터 소유자·그룹·기타 사용자에 대해 제거할 권한을 나타낸다. 읽기(r)는 4, 쓰기(w)는 2, 실행(x)은 1에 대응하며, 0은 제거할 권한이 없다는 뜻이다. umask에 지정된 권한은 생성 시 요청한 권한에서 제외된다. 이 문항은 디렉터리의 일반적인 생성 권한인 'rwxrwxrwx'(777)에 umask를 적용하는 경우이다.

'drwxr-xr-x'에서 맨 앞의 d는 디렉터리라는 뜻이며 권한 숫자에는 포함하지 않는다. 뒤의 권한을 세 자리씩 나누면 소유자는 'rwx', 그룹과 기타 사용자는 각각 'r-x'이다. 따라서 소유자의 권한은 제거하지 않고, **그룹과 기타 사용자의 쓰기 권한만 제거**해야 한다. umask의 각 자리는 소유자 0, 그룹 2, 기타 사용자 2가 되어 022이다.

NoteBase

문 13. (가), (나)에 해당하는 침입차단시스템 동작 방식에 따른 분류를 바르게 연결한 것은?

(가) 각 서비스별로 클라이언트와 서버 사이에 프록시가 존재하며 내부 네트워크와 외부 네트워크가 직접 연결되는 것을 허용하지 않는다.
(나) 서비스마다 개별 프록시를 둘 필요가 없고 프록시와 연결을 위한 전용 클라이언트 소프트웨어가 필요하다.

① (가): 응용 계층 게이트웨이 (application level gateway), (나): 회선 계층 게이트웨이 (circuit level gateway)
② (가): 응용 계층 게이트웨이 (application level gateway), (나): 상태 검사 (stateful inspection)
③ (가): 네트워크 계층 패킷 필터링 (network level packet filtering), (나): 상태 검사 (stateful inspection)
④ (가): 네트워크 계층 패킷 필터링 (network level packet filtering), (나): 회선 계층 게이트웨이 (circuit level gateway)

정답 1번

간단한 해설

응용 계층 게이트웨이는 **서비스별 프록시**가 응용 프로토콜을 처리하고, 회선 계층 게이트웨이는 서비스마다 별도 프록시를 두지 않고 **연결을 중계**한다. (나)의 전용 클라이언트 소프트웨어는 이 중계 기능을 이용하기 위한 것이다.

대응 관계 해설

(가) 응용 계층 게이트웨이: 프록시는 클라이언트와 서버 사이에서 통신을 대신 처리하는 중계자이다. 응용 계층 게이트웨이는 **서비스별 응용 프로토콜을 이해하는 프록시**를 사용한다. 클라이언트와 프록시 사이의 연결, 프록시와 서버 사이의 연결을 따로 맺으므로 내부와 외부 호스트가 직접 연결되지 않는다. 네트워크 계층 패킷 필터링은 IP 주소·포트 번호 등의 헤더 정보를 기준으로 패킷 통과 여부를 결정하므로, 서비스별 프록시가 통신을 대신한다는 설명과 구별된다.

(나) 회선 계층 게이트웨이: 개별 서비스의 명령이나 내용을 해석하기보다 **서비스와 무관하게 연결을 중계**하므로 서비스마다 별도 프록시를 둘 필요가 없다. 대표적인 SOCKS 방식에서는 클라이언트가 프록시에 접속하여 목적지와 연결 중계를 요청한다. 따라서 이러한 요청 절차를 지원하는 클라이언트 소프트웨어가 필요하다. 상태 검사는 연결 상태를 추적하여 패킷이 허용된 통신에 속하는지 판단하는 방식이므로, 전용 클라이언트로 프록시 중계를 요청한다는 설명과 구별된다.

(가)는 응용 계층 게이트웨이, (나)는 회선 계층 게이트웨이로 대응하며 ①의 조합과 일치한다.

NoteBase

문 14. IPSec에 대한 설명으로 옳지 않은 것은?

① AH는 인증 기능을 제공한다.

② ESP는 암호화 기능을 제공한다.

③ 전송 모드는 IP 헤더를 포함한 전체 IP 패킷을 보호한다.

④ IKE는 Diffie-Hellman 키 교환 알고리즘을 기반으로 한다.

정답 3번

간단한 해설

③의 'IP 헤더를 포함한 전체 IP 패킷을 보호한다'는 **터널 모드**의 설명이다. 전송 모드는 주로 **IP 헤더 뒤의 페이로드**를 보호한다.

선지별 해설

① O: AH는 데이터의 **출처 인증과 무결성**을 제공한다. 수신자는 인증 정보를 검사하여 송신 출처와 전송 중 데이터의 변조 여부를 확인한다. 데이터 내용을 암호화하는 기밀성 기능은 제공하지 않는다.

② O: ESP는 **암호화를 통한 기밀성**을 제공할 수 있어 제3자가 데이터 내용을 읽지 못하도록 한다. 인증과 무결성 기능도 지원하므로 암호화만을 위한 프로토콜로 한정되지는 않는다.

③ X: 전송 모드는 주로 IP 헤더 뒤의 페이로드, 즉 TCP·UDP 등의 헤더와 그 데이터를 보호한다. 원래 IP 헤더를 포함한 전체 IP 패킷을 보호하는 방식은 **터널 모드**이다. 터널 모드는 원래 패킷 전체를 내부에 넣고 바깥에 새 IP 헤더를 붙인다. 다만 전송 모드에서도 AH는 기존 IP 헤더의 일부 필드까지 인증하므로, IP 헤더가 전혀 보호되지 않는다고 단정해서는 안 된다.

④ O: IKE는 IPsec 통신에 필요한 보안 설정과 키를 협상·관리하는 프로토콜이다. **Diffie-Hellman 키 교환**으로 양측이 공유 비밀값을 만들고, 이를 키 생성에 활용한다. 공유 비밀값 자체를 그대로 전송하지 않고도 양측이 같은 값을 얻을 수 있다.

NoteBase

문 15. 보안 공격에 대한 설명으로 옳지 않은 것은?

① Land 공격은 패킷을 전송할 때 출발지와 목적지 IP를 동일하게 만들어서 공격 대상에게 전송한다.

② UDP Flooding 공격은 다수의 UDP 패킷을 전송하여 공격 대상 시스템을 마비시킨다.

③ ICMP Flooding 공격은 ICMP 프로토콜의 echo 패킷에 대한 응답인 reply 패킷의 폭주를 통해 공격 대상 시스템을 마비시킨다.

④ Teardrop 공격은 공격자가 자신이 전송하는 패킷을 다른 호스트의 IP 주소로 변조하여 수신자의 패킷 조립을 방해한다.

정답 4번

간단한 해설

Teardrop 공격은 IP 주소를 다른 호스트의 것으로 바꾸는 공격이 아니라, **IP 단편의 오프셋을 조작해 데이터 영역이 겹치게** 하여 수신자의 재조립 과정에서 오류를 일으키는 공격이다. 출발지 IP 주소를 다른 호스트의 주소로 위조하는 것은 IP 스푸핑이다.

선지별 해설

① O: Land 공격은 **출발지와 목적지 IP 주소를 모두 공격 대상의 주소로** 설정한 패킷을 보낸다. 전형적으로 출발지·목적지 포트도 같게 만든 TCP SYN 패킷을 이용한다. 취약한 시스템은 자신을 통신 상대방으로 처리하는 과정에서 자원을 소모하거나 오류를 일으켜 서비스가 중단될 수 있다.

② O: UDP Flooding 공격은 **대량의 UDP 패킷**을 보내 대상의 네트워크 대역폭이나 패킷 처리 자원을 소모시킨다. 그 결과 정상적인 요청을 처리하기 어려워져 서비스 거부 상태에 이를 수 있다.

③ O: ICMP 패킷이 대량으로 몰리면 대역폭과 처리 자원이 소모되어 정상적인 통신이 방해받는다. 선지의 **Echo Reply 패킷이 대상에 집중되는 방식**은 대표적으로 Smurf 공격에서 나타난다. 공격 대상의 IP를 출발지로 위조한 Echo Request를 브로드캐스트로 보내면 여러 호스트의 응답이 공격 대상에 몰린다. 다만 ICMP Flooding이 응답 패킷만 이용하는 것은 아니며, Echo Request를 직접 대량으로 보내는 방식도 있다.

④ X: Teardrop 공격의 핵심은 IP 주소 위조가 아니라 **IP 단편의 오프셋 조작**이다. 오프셋은 원래 데이터에서 각 단편이 놓일 위치를 나타낸다. 공격자는 단편들의 데이터 영역이 겹치도록 조작하여, 이를 제대로 처리하지 못하는 수신 시스템의 재조립 과정에서 오류나 장애를 일으킨다. 따라서 '다른 호스트의 IP 주소로 변조하여'는 '단편의 오프셋을 조작하여'로 고쳐야 한다. 출발지 IP 주소를 다른 호스트의 것으로 위조하는 행위는 IP 스푸핑에 해당한다.

NoteBase

문 16. 다음은 「지능정보화 기본법」 제6조(지능정보사회 종합계획의 수립)의 일부이다. (가), (나)에 들어갈 내용을 바르게 연결한 것은?

제6조(지능정보사회 종합계획의 수립) ① 정부는 지능정보사회 정책의 효율적·체계적 추진을 위하여 지능정보사회 종합계획(이하 “종합계획”이라 한다)을 (가) 단위로 수립하여야 한다.
② 종합계획은 (나)이 관계 중앙행정기관(대통령 소속 기관 및 국무총리 소속 기관을 포함한다. 이하 같다)의 장 및 지방자치단체의 장의 의견을 들어 수립하며, 「정보통신 진흥 및 융합 활성화 등에 관한 특별법」 제7조에 따른 정보통신 전략위원회(이하 “전략위원회”라 한다)의 심의를 거쳐 수립·확정한다. 종합계획을 변경하는 경우에도 또한 같다.

① (가): 3년, (나): 과학기술정보통신부장관
② (가): 3년, (나): 행정안전부장관
③ (가): 5년, (나): 과학기술정보통신부장관
④ (가): 5년, (나): 행정안전부장관

정답 1번

공통 해설

종합계획은 **3년 단위**로 수립한다. 과학기술정보통신부장관이 관계 중앙행정기관장과 지방자치단체장의 의견을 듣고 **정보통신 전략위원회의 심의**를 거쳐 수립·확정하며, 변경할 때도 같은 절차를 따른다.

지능정보화 기본법 제6조 제1항, 지능정보화 기본법 제6조 제2항
지능정보화 기본법 제6조(지능정보사회 종합계획의 수립)
① 정부는 지능정보사회 정책의 효율적 · 체계적 추진을 위하여 지능정보사회 종합계획(이하 "종합계획"이라 한다)을 3년 단위로 수립하여야 한다.
② 종합계획은 과학기술정보통신부장관이 관계 중앙행정기관(대통령 소속 기관 및 국무총리 소속 기관을 포함한다. 이하 같다)의 장 및 지방자치단체의 장의 의견을 들어 수립하며, 「정보통신 진흥 및 융합 활성화 등에 관한 특별법」 제7조에 따른 정보통신 전략위원회(이하 "전략위원회"라 한다)의 심의를 거쳐 수립 · 확정한다. 종합계획을 변경하는 경우에도 또한 같다.

NoteBase

문 17. 「개인정보 영향평가에 관한 고시」상 용어의 정의로 옳지 않은 것은?

① “대상시스템”이란 「개인정보 보호법 시행령」 제35조에 해당하는 개인정보파일을 구축 · 운용, 변경 또는 연계하려는 정보시스템을 말한다.

② “대상기관”이란 「개인정보 보호법 시행령」 제35조에 해당하는 개인정보파일을 구축 · 운용, 변경 또는 연계하려는 공공기관 및 민간기관을 말한다.

③ “개인정보 영향평가 관련 분야 수행실적”이란 「개인정보 보호법 시행령」 제37조제1항제1호에 따른 영향평가 업무 또는 이와 유사한 업무, 정보보호 컨설팅 업무 등을 수행한 실적을 말한다.

④ “개인정보 영향평가”란 「개인정보 보호법」 제33조제1항에 따라 공공기관의 장이 「개인정보 보호법 시행령」 제35조에 해당하는 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에 그 위험요인의 분석과 개선 사항 도출을 위한 평가를 말한다.

정답 2, 3번

①

대상시스템은 영향평가 대상 개인정보파일을 **구축·운용, 변경 또는 연계하려는 정보시스템**이다.

개인정보 영향평가에 관한 고시 제2조 제4호
개인정보 영향평가에 관한 고시 제2조(정의) 이 고시에서 사용하는 용어의 뜻은 다음과 같다.
4. "대상시스템"이란 영 제35조에 해당하는 개인정보파일을 구축 · 운용, 변경 또는 연계하려는 정보시스템을 말한다.

②

대상기관은 영향평가 대상 개인정보파일을 구축·운용, 변경 또는 연계하려는 **공공기관으로 한정되며 민간기관은 포함되지 않는다**.

개인정보 영향평가에 관한 고시 제2조 제2호
개인정보 영향평가에 관한 고시 제2조(정의) 이 고시에서 사용하는 용어의 뜻은 다음과 같다.
2. "대상기관"이란 영 제35조에 해당하는 개인정보파일을 구축 · 운용, 변경 또는 연계하려는 공공기관을 말한다.

NoteBase

③

관련 분야 수행실적에는 영향평가·유사업무·정보보호 컨설팅 업무 등이 포함된다. 다만 현행 고시가 인용하는 조항은 **「개인정보 보호법 시행령」 제36조 제1항 제1호**이다. 선지는 이를 제37조 제1항 제1호로 제시하여 인용 조문이 틀렸다.

개인정보 영향평가에 관한 고시 제2조 제5호
개인정보 영향평가에 관한 고시 제2조(정의) 이 고시에서 사용하는 용어의 뜻은 다음과 같다.
5. "개인정보 영향평가 관련 분야 수행실적(이하 "영향평가 관련 분야 수행실적"이라 한다)"이란 영 제36조제1항제1호에 따른 영향평가 업무 또는 이와 유사한 업무, 정보보호 컨설팅 업무 등을 수행한 실적을 말한다.

④

개인정보 영향평가는 공공기관의 장이 대상 개인정보파일의 운용으로 개인정보 침해가 우려되는 경우 실시하는 **위험요인 분석과 개선 사항 도출을 위한 평가**이다.

개인정보 영향평가에 관한 고시 제2조 제1호
개인정보 영향평가에 관한 고시 제2조(정의) 이 고시에서 사용하는 용어의 뜻은 다음과 같다.
1. "개인정보 영향평가(이하 "영향평가"라 한다)"란 법 제33조제1항에 따라 공공기관의 장이 영 제35조에 해당하는 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에 그 위험요인의 분석과 개선 사항 도출을 위한 평가를 말한다.

NoteBase

문 18. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제23조의4 (본인확인업무의 정지 및 지정취소)상 본인확인업무에 대해 전부 또는 일부의 정지를 명하거나 본인확인기관 지정을 취소할 수 있는 사유에 해당하지 않는 것은?

① 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제23조의3 제4항에 따른 지정기준에 적합하지 아니하게 된 경우

② 거짓이나 그 밖의 부정한 방법으로 본인확인기관의 지정을 받은 경우

③ 본인확인업무의 정지명령을 받은 자가 그 명령을 위반하여 업무를 정지하지 아니한 경우

④ 지정받은 날부터 3개월 이내에 본인확인업무를 개시하지 아니하거나 3개월 이상 계속하여 본인확인업무를 휴지한 경우

정답 4번

①

본인확인기관이 **지정기준을 충족하지 못하게 되면** 업무정지 또는 지정취소의 사유가 된다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제23조의4 제1항 제4호
정보통신망 이용촉진 및 정보보호 등에 관한 법률 제23조의4(본인확인업무의 정지 및 지정취소)
① 방송미디어통신위원회는 본인확인기관이 다음 각 호의 어느 하나에 해당하는 때에는 6개월 이내의 기간을 정하여 본인확인업무의 전부 또는 일부의 정지를 명하거나 지정을 취소할 수 있다. 다만, 제1호 또는 제2호에 해당하는 때에는 그 지정을 취소하여야 한다. <개정 2025.10.1>
4. 제23조의3제4항에 따른 지정기준에 적합하지 아니하게 된 경우

NoteBase

②

거짓이나 부정한 방법으로 지정을 받았다면 **반드시 지정을 취소해야 한다**.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제23조의4 제1항 단서, 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제23조의4 제1항 제1호
정보통신망 이용촉진 및 정보보호 등에 관한 법률 제23조의4(본인확인업무의 정지 및 지정취소)
① 방송미디어통신위원회는 본인확인기관이 다음 각 호의 어느 하나에 해당하는 때에는 6개월 이내의 기간을 정하여 본인확인업무의 전부 또는 일부의 정지를 명하거나 지정을 취소할 수 있다. 다만, 제1호 또는 제2호에 해당하는 때에는 그 지정을 취소하여야 한다. <개정 2025.10.1>
1. 거짓이나 그 밖의 부정한 방법으로 본인확인기관의 지정을 받은 경우
2. 본인확인업무의 정지명령을 받은 자가 그 명령을 위반하여 업무를 정지하지 아니한 경우
3. 지정받은 날부터 6개월 이내에 본인확인업무를 개시하지 아니하거나 6개월 이상 계속하여 본인확인업무를 휴지한 경우
4. 제23조의3제4항에 따른 지정기준에 적합하지 아니하게 된 경우

③

업무정지명령을 어기고 업무를 계속하면 **반드시 지정을 취소해야 한다**.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제23조의4 제1항 단서, 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제23조의4 제1항 제2호
정보통신망 이용촉진 및 정보보호 등에 관한 법률 제23조의4(본인확인업무의 정지 및 지정취소)
① 방송미디어통신위원회는 본인확인기관이 다음 각 호의 어느 하나에 해당하는 때에는 6개월 이내의 기간을 정하여 본인확인업무의 전부 또는 일부의 정지를 명하거나 지정을 취소할 수 있다. 다만, 제1호 또는 제2호에 해당하는 때에는 그 지정을 취소하여야 한다. <개정 2025.10.1>
1. 거짓이나 그 밖의 부정한 방법으로 본인확인기관의 지정을 받은 경우
2. 본인확인업무의 정지명령을 받은 자가 그 명령을 위반하여 업무를 정지하지 아니한 경우
3. 지정받은 날부터 6개월 이내에 본인확인업무를 개시하지 아니하거나 6개월 이상 계속하여 본인확인업무를 휴지한 경우
4. 제23조의3제4항에 따른 지정기준에 적합하지 아니하게 된 경우

NoteBase

④

업무 미개시의 기준은 **지정일부터 6개월 이내**이며, 계속 휴지의 기준은 **6개월 이상**이다. 선지는 두 기간을 모두 3개월로 잘못 제시했다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제23조의4 제1항 제3호
정보통신망 이용촉진 및 정보보호 등에 관한 법률 제23조의4(본인확인업무의 정지 및 지정취소)
① 방송미디어통신위원회는 본인확인기관이 다음 각 호의 어느 하나에 해당하는 때에는 6개월 이내의 기간을 정하여 본인확인업무의 전부 또는 일부의 정지를 명하거나 지정을 취소할 수 있다. 다만, 제1호 또는 제2호에 해당하는 때에는 그 지정을 취소하여야 한다. <개정 2025.10.1>
3. 지정받은 날부터 6개월 이내에 본인확인업무를 개시하지 아니하거나 6개월 이상 계속하여 본인확인업무를 휴지한 경우

NoteBase

문 19. 메일 보안 기술에 대한 설명으로 옳지 않은 것은?

① PGP는 중앙 집중화된 키 인증 방식이고, PEM은 분산화된 키 인증 방식이다.

② PGP를 이용하면 수신자가 이메일을 받고서도 받지 않았다고 발뺌할 수 없다.

③ PGP는 인터넷으로 전송하는 이메일을 암호화 또는 복호화하여 제3자가 알아볼 수 없게 하는 보안 프로그램이다.

④ PEM에는 메시지를 암호화하여 통신 내용을 보호하는 기능, 메시지 위·변조, 검증 및 메시지 작성자를 인증하는 보안 기능이 있다.

정답 1, 2번

간단한 해설

PGP는 **분산형 신뢰망**을, PEM은 **인증기관 중심의 계층형 구조**를 이용하므로 키 인증 방식이 뒤바뀌었다. PGP의 전자서명은 발신자가 메시지를 작성·서명했다는 증거가 될 수 있지만, **수신자가 메일을 받았다는 사실까지 증명하지는 않는다**.

선지별 해설

① X: PGP는 사용자들이 서로의 공개키와 신원 사이의 연결을 확인하고 서명하는 **분산형 신뢰망(Web of Trust)**을 이용한다. 반면 PEM은 인증기관이 발급한 공개키 인증서를 상위 인증기관으로 이어지는 인증 경로에 따라 검증하는 **계층형 인증 구조**를 이용한다. 따라서 두 기술의 키 인증 방식을 서로 바꾸어야 한다.

② X: 발신자가 PGP로 전자서명한 메일은 발신자의 공개키로 서명을 검증하여 작성자와 내용의 무결성을 확인할 수 있다. 이는 발신자가 자신이 서명한 메시지임을 부인하는 데 대응하는 송신 부인방지와 관련된다. 그러나 발신자의 서명에는 **수신 사실을 입증하는 수신자의 확인 증거가 없다**. 따라서 PGP를 이용했다는 이유만으로 수신자가 메일을 받지 않았다고 부인할 수 없다고 할 수는 없다. 수신 부인방지를 위해서는 수신자가 서명한 수신 확인 등 별도의 증거가 필요하다.

③ O: PGP는 이메일과 파일에 암호화 및 전자서명 기능을 제공하는 보안 기술이다. 메일 내용을 암호화해 전송하고 수신자가 복호화하도록 하여, 권한 없는 제3자가 내용을 읽지 못하게 하는 **기밀성**을 제공한다.

④ O: PEM은 메시지 암호화로 통신 내용의 기밀성을 보호한다. 또한 메시지의 무결성 검증으로 **내용의 위·변조를 탐지**하고, 인증 기능으로 메시지 작성자를 확인한다. 암호화에 의한 내용 보호와 작성자 인증·무결성 검증은 서로 구별되는 보안 기능이다.

NoteBase

문 20. (가)~(다)에 해당하는 트리형 공개키 기반 구조의 구성 기관을 바르게 연결한 것은? (단, PAA는 Policy Approval Authorities, RA는 Registration Authority, PCA는 Policy Certification Authorities를 의미한다)

(가) PKI에 대한 정책을 결정하고 하위 기관의 정책을 승인하는 기관
(나) Root CA 인증서를 발급하고 CA가 준수해야 할 기본 정책을 수립하는 기관
(다) CA를 대신하여 PKI 인증 요청을 확인하고, CA 간 인터페이스를 제공하는 기관

① (가): PAA, (나): RA, (다): PCA
② (가): PAA, (나): PCA, (다): RA
③ (가): PCA, (나): RA, (다): PAA
④ (가): PCA, (나): PAA, (다): RA

정답 2번

간단한 해설

PAA는 PKI 전체의 **정책 결정·승인**을 맡고, PCA는 CA가 따를 기본 정책과 인증 체계를 담당한다. RA는 정책을 승인하는 기관이 아니라 **인증 요청과 신청자 정보를 확인하는 등록기관**이다.

대응 관계 해설

(가) PAA: 정책 승인기관이다. PKI 전체에 적용할 정책을 결정하고 하위 기관의 정책을 승인하므로, 판단 기준은 **전체 정책에 대한 결정·승인 권한**이다. CA가 따라야 할 구체적인 기본 정책을 마련하는 PCA의 역할과 구별된다.

(나) PCA: 정책 인증기관이다. 이 문제의 트리형 PKI 구분에서는 Root CA 인증서 발급과 CA가 준수할 기본 정책 수립을 담당한다. PAA가 전체 정책을 승인한다면, PCA는 그 정책 아래에서 **인증기관이 따를 정책과 인증 체계**를 마련한다는 점이 다르다.

(다) RA: 등록기관이다. CA를 대신하여 인증 요청을 확인하고 신청자의 신원 등 인증서 발급에 필요한 정보를 검증한다. 원문의 'CA 간 인터페이스'는 RA의 일반적인 역할을 정확히 나타내는 표현은 아니다. RA는 보통 신청자와 CA 사이에서 요청과 확인 정보를 전달하므로, 여기서는 'CA를 대신하여 인증 요청을 확인한다'는 단서로 RA를 연결한다. **요청 정보의 확인은 RA**가 맡지만, 인증서에 서명하여 발급하는 업무는 CA가 맡는다.

이 역할에 따라 (가)는 PAA, (나)는 PCA, (다)는 RA로 연결되며, ②의 조합과 일치한다.

NoteBase