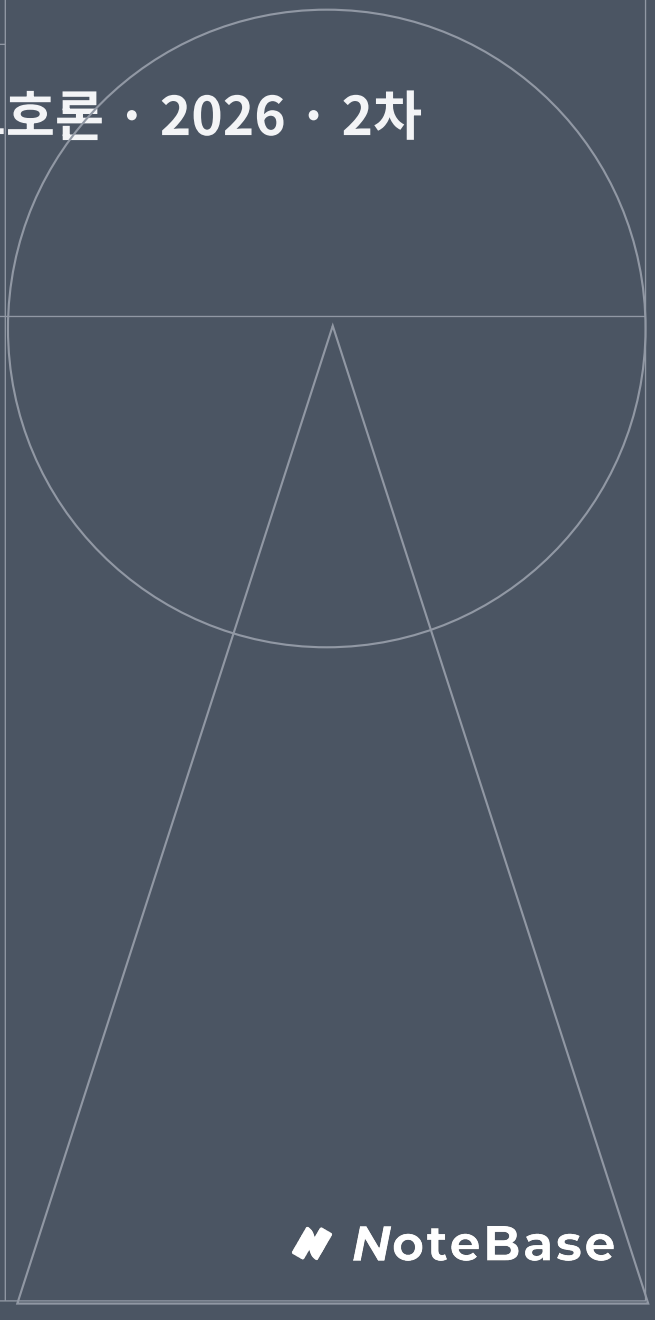
기출OX 해설집

공무원/국가직/7급 · 정보보호론 · 2026 · 2차



NoteBase

기출OX 해설집

공무원/국가직/7급 · 정보보호론 · 2026 · 2차

공무원/국가직/7급 · 정보보호론 · 2026 · 2차

문 1. 다음은 ARP 스푸핑에 대한 설명이다. (가)에 들어갈 용어는?

공격자가 스위치 내의 다른 단말기에 가짜 ARP 응답을 보내어 왜곡하는 공격으로, 공격자의 (가)를 속여서 패킷을 가로채는 공격이다. 이를 통해 클라이언트에서 서버로 가는 패킷이나 서버에서 클라이언트로 가는 패킷이 공격자에게 향하게 하여 로컬 네트워크의 통신 흐름을 왜곡한다.

① MAC 주소

② IP 주소

③ Port 주소

④ email 주소

정답 1번

간단한 해설

ARP 스푸핑은 가짜 ARP 응답으로 **정상 상대의 IP 주소에 공격자의 MAC 주소를 연결**하여 패킷을 공격자에게 보내게 한다. IP 주소와 MAC 주소의 대응 관계를 속여 로컬 네트워크의 통신을 가로채는 방식이다.

빈칸별 해설

(가) MAC 주소: ARP는 로컬 네트워크에서 통신할 상대의 IPv4 주소에 대응하는 MAC 주소를 알아내는 프로토콜이다. 단말은 이 대응 관계를 ARP 캐시에 저장하고, 실제 이더넷 프레임을 보낼 때 목적지 MAC 주소를 사용한다. 공격자는 가짜 ARP 응답에 정상 상대의 IP 주소와 자신의 MAC 주소를 넣어, 다른 단말이 **정상 상대의 MAC 주소 대신 공격자의 MAC 주소를 저장**하도록 유도한다.

예를 들어 클라이언트의 ARP 캐시에서 같은 로컬 네트워크에 있는 서버의 IP 주소가 공격자의 MAC 주소와 연결되면, 클라이언트는 서버로 보낼 패킷을 공격자의 MAC 주소를 목적지로 하는 프레임에 담아 전송한다. 이때 패킷의 목적지 IP 주소는 서버를 가리켜도, 로컬 네트워크에서 프레임을 받는 쪽은 공격자가 된다.

따라서 (가)에 들어갈 용어는 MAC 주소이며, ①에 해당한다.

NoteBase

문 2. 다음에서 설명하는 알고리즘은?

◯ 이산대수 문제를 기반으로 암·복호화를 지원하고 전자서명에 활용될 수 있는 방식이다.
◯ 디피헬만(Diffie-Hellman)의 공용키 분배법의 확장형으로 암호문 길이가 평문 길이의 2배가 되는 단점이 있다.

① RSA
② ElGamal
③ LEA
④ KCDSA

정답 2번

간단한 해설

디피헬만의 키 분배 원리를 확장해 암·복호화에 이용하고, 별도의 전자서명 방식도 제시한 것이 ElGamal이다. 기본 암호화 방식은 평문 하나를 **두 요소로 된 암호문**으로 바꾸므로 길이가 2배가 된다.

핵심 풀이

이산대수·디피헬만 단서: ElGamal은 이산대수 문제의 어려움에 기반한 공개키 암호 방식이다. 디피헬만에서 공유 비밀값을 만드는 원리를 확장하여, 수신자의 공개키로 평문을 암호화하고 수신자의 개인키로 복호화한다. ElGamal에는 암호화 방식과 별도로 전자서명 방식도 있다.

암호문 길이 단서: 기본 ElGamal 암호화에서는 평문을 하나의 군 원소로 나타내고, 암호문을 **임시 난수로 만든 값과 평문을 감춘 값**의 두 요소로 구성한다. 각 요소를 평문 원소와 같은 길이로 표현하므로 암호문 길이가 평문 길이의 2배가 된다.

KCDSA와의 구분: KCDSA도 이산대수 문제에 기반하지만, **전자서명 알고리즘**이다. 따라서 이산대수라는 단서만으로 구별하지 말고, 암·복호화와 암호문 길이 증가라는 단서까지 함께 보아야 한다.

RSA와의 구분: RSA는 큰 정수의 **소인수분해 문제**와 관련된 공개키 암호 방식으로, 이산대수에 기반한 디피헬만 확장 방식이라는 설명과 다르다.

LEA와의 구분: LEA는 암호화와 복호화에 같은 비밀키를 사용하는 **대칭키 블록암호**이다. 공개키와 개인키를 구분하는 ElGamal과 암호 방식이 다르다.

NoteBase

문 3. 정보보호 컴플라이언스에 대한 설명으로 옳지 않은 것은?

① 정보보호 관련 법률과 규정을 준수하는 활동이다.

② 조직의 비즈니스 연속성과 투명성을 높이기 위한 활동의 일환이다.

③ 기술적 조치를 중심으로 구성되며, 인적·제도적 요소는 포함하지 않는다.

④ 외부 규제뿐만 아니라 내부 통제 기능을 대상으로 한다.

정답 3번

간단한 해설

정보보호 컴플라이언스는 법률·규정 등을 준수하기 위한 활동으로, 기술적 조치뿐 아니라 **인적·제도적 요소도 포함**한다. 담당자의 책임과 역할을 정하고 보안교육, 내부 규정, 점검 절차를 운영하는 것도 이에 해당한다.

선지별 해설

① O: 정보보호 컴플라이언스는 조직에 적용되는 **정보보호 관련 법률과 규정의 준수**를 확보하는 활동이다. 준수해야 할 요구사항을 파악하고, 이를 업무 절차와 보호조치에 반영하며, 실제로 지켜지는지 점검한다.

② O: 정보보호 요구사항을 준수하고 이행 상태를 관리하면 보안사고나 규정 위반으로 인한 업무 중단 위험을 줄여 **비즈니스 연속성**을 뒷받침할 수 있다. 또한 준수 여부와 조치 내역을 기록하고 확인하는 과정은 조직 운영의 투명성을 높이는 데 기여한다.

③ X: 정보보호 컴플라이언스에는 **기술적 조치와 인적·제도적 요소가 함께 포함**된다. 접근통제 같은 기술적 조치뿐 아니라 담당자의 역할과 책임 설정, 임직원 보안교육, 내부 보안규정과 점검 절차의 운영도 필요하다. 따라서 '인적·제도적 요소는 포함하지 않는다'는 설명을 '인적·제도적 요소도 포함한다'로 고쳐야 한다.

④ O: 준수 대상에는 법률 등 외부에서 부과한 요구사항뿐 아니라 **조직 내부의 보안정책과 통제 절차**도 포함된다. 내부 규정에 따라 접근권한이 승인되고 정기적으로 검토되는지 확인하는 것처럼, 내부 통제가 제대로 작동하는지를 점검하는 활동도 정보보호 컴플라이언스에 해당한다.

NoteBase

문 4. 「개인정보 보호법」상 고정형 영상정보처리기기의 설치 · 운영 제한에 대한 설명으로 옳지 않은 것은?

① 교통단속을 위하여 정당한 권한을 가진 경우 공개된 장소에 고정형 영상정보처리기기를 설치 · 운영할 수 있다.

② 누구든지 불특정 다수가 이용하는 목욕실, 화장실, 발한실, 탈의실 등 개인의 사생활을 현저히 침해할 우려가 있는 장소의 내부를 볼 수 있도록 고정형 영상정보처리기기를 설치 · 운영하여서는 아니 된다. 다만 대통령령으로 정하는 시설에 대하여는 그러지 아니하다.

③ 고정형영상정보처리기기운영자는 고정형 영상정보처리기기의 설치 목적과 다른 목적으로 고정형 영상정보처리기기를 임의로 조작하거나 다른 곳을 비춰서는 아니 되나, 녹음기능은 사용할 수 있다.

④ 고정형영상정보처리기기운영자는 대통령령으로 정하는 바에 따라 고정형 영상정보처리기기 운영 · 관리 방침을 마련하여야 한다. 다만 「개인정보 보호법」에 따라 개인정보 처리방침을 정할 때 고정형 영상정보처리기기 운영 · 관리에 관한 사항을 포함시킨 경우에는 고정형 영상정보처리기기 운영 · 관리 방침을 마련하지 아니할 수 있다.

정답 3번

①

교통단속을 위하여 정당한 권한을 가진 자는 공개된 장소에 고정형 영상정보처리기기를 설치 · 운영할 수 있다.

개인정보 보호법 제25조(고정형 영상정보처리기기의 설치 · 운영 제한)
① 누구든지 다음 각 호의 경우를 제외하고는 공개된 장소에 고정형 영상정보처리기기를 설치 · 운영하여서는 아니 된다. <개정 2023.3.14>
4. 교통단속을 위하여 정당한 권한을 가진 자가 설치 · 운영하는 경우

②

불특정 다수가 이용하는 목욕실 · 화장실 · 탈의실 등은 **내부를 볼 수 있도록 고정형 영상정보처리기기를 설치 · 운영하는 것이 금지**된다. 다만, 교도소 · 정신보건 시설 등 **법령에 근거하여 사람을 구금하거나 보호하는 시설 중 대통령령으로 정하는 시설**은 예외이다.

개인정보 보호법 제25조(고정형 영상정보처리기기의 설치 · 운영 제한)
② 누구든지 불특정 다수가 이용하는 목욕실, 화장실, 발한실(發汗室), 탈의실 등 개인의 사생활을 현저히 침해할 우려가 있는 장소의 내부를 볼 수 있도록 고정형 영상정보처리기기를 설치 · 운영하여서는 아니 된다. 다만, 교도소, 정신보건 시설 등 법령에 근거하여 사람을 구금하거나 보호하는 시설로서 대통령령으로 정하는 시설에 대하여는 그러하지 아니하다. <개정 2023.3.14>

NoteBase

③

설치 목적과 다른 목적으로 기기를 임의로 조작하거나 다른 곳을 비추는 행위뿐 아니라 **녹음기능의 사용도 금지**된다.

개인정보 보호법 제25조(고정형 영상정보처리기기의 설치 · 운영 제한)
⑤ 고정형영상정보처리기기운영자는 고정형 영상정보처리기기의 설치 목적과 다른 목적으로 고정형 영상정보처리기기를 임의로 조작하거나 다른 곳을 비춰서는 아니 되며, 녹음기능은 사용할 수 없다. <개정 2023.3.14>

④

고정형영상정보처리기기운영자는 운영 · 관리 방침을 마련하여야 한다. 다만, **개인정보 처리방침에 고정형 영상정보처리기기의 운영 · 관리 사항을 포함한 경우**에는 별도의 운영 · 관리 방침을 마련하지 않을 수 있다.

개인정보 보호법 제25조(고정형 영상정보처리기기의 설치 · 운영 제한)
⑦ 고정형영상정보처리기기운영자는 대통령령으로 정하는 바에 따라 고정형 영상정보처리기기 운영 · 관리 방침을 마련하여야 한다. 다만, 제30조에 따른 개인정보 처리방침을 정할 때 고정형 영상정보처리기기 운영 · 관리에 관한 사항을 포함시킨 경우에는 고정형 영상정보처리기기 운영 · 관리 방침을 마련하지 아니할 수 있다. <개정 2023.3.14>

NoteBase

문 5. 해시(Hash) 함수에 대한 설명으로 옳은 것은?

① 해시 함수는 결과값(해시값)으로부터 원래 입력을 쉽게 복원할 수 있다.

② 같은 입력에 대해서는 같은 해시값이 생성된다.

③ 네트워크로 메시지와 메시지의 해시값을 전송하면 메시지의 무결성이 보호된다.

④ 해시 함수는 임의 길이의 입력을 받아 입력마다 서로 다른 길이의 결과값을 만든다.

정답 2번

간단한 해설

해시 함수는 **동일한 입력에 항상 동일한 해시값**을 내는 결정적 함수이다. 같은 해시 함수를 사용하면 실행할 때마다 결과가 임의로 바뀌지 않는다.

선지별 해설

① X: 암호학적 해시 함수는 해시값으로부터 그 값을 만드는 입력을 찾기 어렵도록 설계된다. 이를 **역상 저항성**이라고 한다. 입력의 해시값은 쉽게 계산할 수 있지만, 해시값에서 원래 입력을 쉽게 복원할 수 있는 것은 아니다.

② O: 해시 함수는 **같은 함수에 같은 입력을 넣으면 같은 출력**을 내는 결정적 함수이다. 따라서 동일한 메시지에 동일한 해시 함수를 적용하면 언제 계산하더라도 같은 해시값을 얻는다.

③ X: 메시지와 해시값을 함께 전송하는 것만으로는 공격자에 의한 변조를 막거나 확실히 검출할 수 없다. 공격자가 메시지를 바꾼 뒤 **변경한 메시지의 해시값도 다시 계산해 교체**하면 수신자의 해시값 비교를 통과할 수 있기 때문이다. 무결성을 확인하려면 비교 기준인 해시값을 신뢰할 수 있어야 하며, 악의적 변조에 대응하려면 비밀키를 사용하는 HMAC이나 전자서명 등의 인증 수단이 필요하다.

④ X: 일반적인 암호학적 해시 함수는 임의 길이의 입력을 받아 **정해진 길이의 해시값**을 생성한다. 출력 길이는 입력마다 달라지는 것이 아니라 사용하는 해시 함수에 따라 정해진다. 예를 들어 SHA-256의 출력은 입력 길이와 관계없이 256비트이다.

NoteBase

문 6. 다음에서 설명하는 보안 시스템은?

조직의 IT 인프라 전체에서 발생하는 로그와 이벤트 데이터를 실시간으로 수집·분석하여 보안 위협을 탐지하는 통합 보안 솔루션이다.

① NAC
② DLP
③ VPN
④ SIEM

정답 4번

간단한 해설

조직 전체의 로그와 이벤트를 모아 **실시간으로 통합 분석하여 보안 위협을 탐지**하는 것은 SIEM의 기능이다. 여러 시스템에서 발생한 기록을 연결해 위협을 파악한다는 점이 핵심이다.

핵심 풀이

SIEM(Security Information and Event Management)은 보안 정보 및 이벤트 관리 시스템이다.
서버·네트워크 장비·보안 장비 등에서 발생하는 로그와 이벤트를 수집하고, **서로 관련된 기록을 연계 분석**하여 위협을 탐지한다. 예를 들어 여러 장비에 흩어진 접속 실패 기록을 함께 분석하면 개별 장비의 기록만 볼 때 놓치기 쉬운 공격 징후를 파악할 수 있다. 지문의 'IT 인프라 전체', '로그와 이벤트 데이터', '실시간 수집·분석'이 이 기능을 가리킨다.

NAC는 사용자나 단말의 네트워크 접속을 통제하고, DLP는 중요 정보의 외부 유출을 방지하며, VPN은 암호화된 통신로를 제공한다. 이들과 구별되는 SIEM의 중심 기능은 **여러 시스템의 로그·이벤트를 통합하여 위협을 탐지**하는 것이다.

NoteBase

문 7. 악성코드(Malware)의 종류로만 옳게 짝지어진 것은?

① Worm, Trojan Horse

② IDS, APT

③ SET, IPsec

④ DDoS, IP 스푸핑

정답 1번

간단한 해설

웜(Worm)은 **자기 복제와 전파**를 수행하고, 트로이 목마(Trojan Horse)는 **정상 프로그램으로 위장해 악성 기능을 수행**한다. 둘 다 시스템에 해를 끼치는 프로그램인 악성코드의 종류이다.

선지별 해설

① O: 웜(Worm)은 독립적으로 실행되며 자신을 복제하여 다른 시스템으로 전파되는 악성코드이다. 트로이 목마(Trojan Horse)는 정상적이거나 유용한 프로그램으로 위장하여 사용자의 실행을 유도하고, 실행되면 정보 유출 등 악성 기능을 수행하는 코드이다. 두 용어 모두 **악성 프로그램 자체의 종류**를 가리킨다.

② X: IDS는 시스템이나 네트워크의 활동을 감시하여 침입 징후를 탐지하는 **침입탐지시스템**이다. APT는 특정 대상을 상대로 다양한 수단을 동원하여 장기간 지속하는 지능형 지속 위협을 뜻한다. APT 공격에 악성코드가 활용될 수는 있지만, IDS는 보안 시스템이고 APT는 공격·위협의 개념이므로 악성코드의 종류끼리 묶은 것이 아니다.

③ X: SET는 인터넷 등 개방된 네트워크에서 신용카드 결제를 안전하게 처리하기 위한 프로토콜이다. IPsec은 IP 계층에서 통신 데이터의 인증·무결성·기밀성 등을 제공하는 보안 프로토콜 체계이다. 두 용어는 악성코드가 아니라 **거래나 통신을 보호하는 보안 프로토콜**에 해당한다.

④ X: DDoS는 여러 공격원에서 트래픽이나 요청을 집중시켜 대상 서비스의 정상적인 이용을 방해하는 분산 서비스 거부 공격이다. IP 스푸핑은 IP 패킷의 출발지 주소를 위조하는 기법이다. 악성코드가 이러한 공격에 사용될 수는 있지만, 두 용어 자체는 **악성코드의 종류가 아니라 공격 기법**을 가리킨다.

NoteBase

문 8. 리눅스 운영체제에서 허가권을 변경하는 명령어 사용 형식이 옳지 않은 것은?

① 그룹에 쓰기 권한 부여: chmod g+w

② 사용자의 실행 권한 제거: chmod o-x

③ 사용자, 그룹, 타인의 실행 권한 제거: chmod a-x

④ 타인에게 읽기, 쓰기 권한만 부여: chmod o+rw

정답 2번

간단한 해설

②의 o-x는 **타인의 실행 권한**을 제거한다. 파일 소유자의 실행 권한을 제거하려면 **u-x**를 사용한다.

선지별 해설

① O: g는 파일의 소유 그룹, +는 권한 추가, w는 쓰기 권한을 뜻한다. 따라서 g+w는 **그룹에 쓰기 권한을 추가**하며, 기존 읽기·실행 권한은 유지한다.

② X: o는 파일 소유자와 소유 그룹에 속하지 않는 타인을 뜻한다. 따라서 o-x는 타인의 실행 권한을 제거한다. 선지의 '사용자'를 파일 소유자로 보면 대상 기호는 **o가 아니라 u**이므로, 소유자의 실행 권한을 제거하는 형식은 chmod u-x이다.

③ O: a는 u·g·o를 모두 포함하며, -는 권한 제거, x는 실행 권한을 뜻한다. 따라서 a-x는 **소유자·그룹·타인 모두의 실행 권한을 제거**한다. 읽기·쓰기 권한은 변경하지 않는다.

④ O: 읽기·쓰기 권한을 추가한다는 의미에서 o+rw는 타인에게 해당 권한을 부여하는 형식이다. 다만 선지의 '만'을 최종 권한의 제한으로 해석해서는 안 된다. **+는 기존의 다른 권한을 제거하지 않으므로** 타인에게 실행 권한이 이미 있으면 그대로 남는다. 실행 권한 없이 읽기·쓰기 권한만 갖도록 지정하려면 chmod o=rw를 사용한다.

NoteBase

문 9. 다음은 정보보호의 요구사항에 대한 설명이다. (가)에 들어갈 용어는?

(가)은 비인가된 자에 의한 정보의 변경, 삭제, 생성 등으로부터 보호되어 정보의 정확성, 완전성이 보장되어야 한다는 원칙이다.

① 기밀성
② 인증성
③ 무결성
④ 가용성

정답 3번

간단한 해설

비인가자의 변경·삭제·생성으로부터 정보를 보호하여 **정확성과 완전성**을 유지하는 요구사항은 무결성이다. 정보를 볼 수 있는지를 제한하는 기밀성과는 구별된다.

빈칸별 해설

(가) 무결성: 정보가 허가되지 않은 방식으로 변경·삭제·생성되지 않도록 하여 **정확성과 완전성을 보장**하는 성질이다. 비인가자가 정보의 내용을 바꾸거나 거짓 정보를 추가하면 정확성이, 필요한 정보를 삭제하면 완전성이 훼손된다. 지문은 이러한 훼손으로부터 정보를 보호해야 한다는 원칙을 설명한다.

기밀성은 허가되지 않은 자에게 정보가 공개되지 않도록 하는 성질이고, 인증성은 사용자나 정보의 출처가 주장하는 대상과 일치하는지를 확인하는 성질이다. 가용성은 인가된 사용자가 필요할 때 정보나 서비스를 이용할 수 있는 성질이다. 따라서 정보의 정확성과 완전성을 보장한다는 (가)에는 ③의 무결성이 들어간다.

NoteBase

문 10. 책임 추적성(Accountability)을 보장하기 위한 주요 수단은?

① 암호화

② 백업 및 복구

③ 감사 로그

④ 침입 방지 시스템

정답 3번

간단한 해설

감사 로그는 누가 언제 어떤 작업을 했는지 기록하여 행위자를 확인할 수 있게 한다. 이처럼 시스템의 행위를 해당 주체와 연결하는 것이 책임 추적성이다.

개념 구분

책임 추적성(Accountability)은 시스템에서 발생한 행위를 그 행위를 한 주체까지 추적할 수 있는 성질이다.
감사 로그는 사용자 식별정보, 수행 시각, 수행 작업 등을 남겨 **행위와 행위자를 연결**하는 근거가 된다. 예를 들어 파일 삭제 기록에 사용자 계정과 삭제 시각이 남아 있으면 해당 작업을 수행한 계정을 추적할 수 있다.

암호화는 주로 정보의 내용을 권한 없는 사람이 읽지 못하게 하여 기밀성을 보호한다. 백업 및 복구는 손실되거나 훼손된 데이터를 되살려 가용성을 확보하는 데 쓰인다. 침입 방지 시스템은 공격을 탐지하고 차단하는 수단이다. 이들과 구별되는 감사 로그의 핵심 역할은 **수행된 행위의 기록을 통한 추적**이다.

NoteBase

문 11. SSL(Secure Socket Layer)에 대한 설명으로 옳지 않은 것은?

① TCP/IP 4계층 모델의 네트워크 계층에서 동작하는 프로토콜이다.

② 암호화된 웹 서핑을 가능하게 한다.

③ 서버 인증, 클라이언트 인증, 암호화 세션 기능을 제공한다.

④ SSL을 지원하는 웹 사이트 URL은 'https://'로 시작한다.

정답 1번

간단한 해설

SSL은 IP가 동작하는 네트워크 계층이 아니라 **응용 프로토콜과 전송 계층의 TCP 사이**에서 통신을 보호한다. 웹에서는 HTTP 데이터를 암호화하여 주고받게 한다.

선지별 해설

① X: SSL은 **HTTP 같은 응용 프로토콜과 TCP 사이**에서 동작한다. 응용 데이터를 암호화한 뒤 TCP를 통해 전달하므로, IP가 동작하는 네트워크 계층의 프로토콜이라는 설명은 잘못되었다.

② O: SSL은 브라우저와 웹 서버 사이에 오가는 **HTTP 데이터를 암호화**하여 전송할 수 있게 한다. 따라서 통신 내용을 도청하더라도 원래 내용을 쉽게 알아볼 수 없도록 보호하는 암호화된 웹 서핑을 지원한다.

③ O: SSL은 인증서 등을 이용한 서버 인증과 클라이언트 인증을 지원하며, 핸드셰이크에서 암호 알고리즘과 키를 합의하여 암호화 통신을 위한 세션을 설정한다. 다만 **클라이언트 인증은 선택적**이므로 모든 웹 접속에서 반드시 수행되는 것은 아니다.

④ O: SSL/TLS로 보호되는 HTTP 통신을 HTTPS라고 하며, 이를 사용하는 웹 주소는 **'https://'**로 시작한다. 브라우저는 이 주소 체계에 따라 서버와 보안 연결을 설정한 뒤 HTTP 데이터를 주고받는다.

NoteBase

문 12. 웹 취약점과 대응 방안에 대한 설명으로 옳지 않은 것은?

① 업로드 취약점 공격: 파일 고유의 데이터인 시그니처를 분석하여 특정 파일에 대한 접근제어를 수행한다.

② 인젝션 공격: 파일 확장자를 검증한다.

③ XSS 공격: 웹 브라우저를 업데이트하여 악성 스크립트 실행을 차단하거나 사용자의 입력에 대한 유효성을 검사한다.

④ CSRF 공격: 위조 방지 토큰(요청 검증 토큰)을 추가한다.

정답 2번

간단한 해설

②의 '파일 확장자 검증'은 **파일 업로드 취약점**에 대한 대응이다. 인젝션은 외부 입력이 명령이나 질의의 일부로 실행되는 공격이므로, **입력값 검증과 명령·데이터의 분리**가 필요하다.

선지별 해설

① O: 업로드 취약점 공격은 파일 업로드 기능을 이용하여 악성 파일을 서버에 올리는 공격이다. 파일 시그니처는 **파일 형식을 식별하는 바이트 패턴**이므로, 이를 분석하여 허용한 형식에 맞지 않는 파일을 차단할 수 있다. 확장자만 바꾼 파일도 식별하는 데 도움이 되지만, 시그니처 검사만으로 안전성이 보장되지는 않으므로 확장자 검사와 실행 권한 제한 등을 함께 적용한다.

② X: 인젝션은 검증되지 않은 외부 입력이 SQL 질의나 운영체제 명령 등에 포함되어 공격자가 의도한 동작을 일으키는 공격이다. 파일 확장자 검증은 업로드할 파일의 종류를 제한하는 방법이므로 인젝션의 일반적인 대응 방안과 연결되지 않는다. 인젝션에는 입력값의 허용 형식과 범위를 검증하고, SQL 인젝션의 경우 **매개변수화된 질의로 질의 구조와 입력 데이터를 분리**하는 등의 대책을 적용한다. 이렇게 하면 입력에 SQL 구문이 들어 있어도 명령이 아닌 데이터로 처리된다.

③ O: XSS는 웹 페이지에 삽입된 악성 스크립트가 이용자의 브라우저에서 실행되는 공격이다. 입력값의 유효성을 검사하여 허용하지 않은 내용을 걸러내고, 출력 시에는 **출력 위치에 맞게 인코딩**하여 입력 내용이 실행 코드로 해석되지 않도록 한다. 브라우저 업데이트는 알려진 브라우저 취약점을 보완하는 보조 대책이며, 업데이트만으로 웹 애플리케이션의 모든 XSS를 차단할 수 있는 것은 아니다.

④ O: CSRF는 로그인한 이용자의 브라우저가 인증 정보를 자동으로 보내는 점을 이용하여, 이용자가 의도하지 않은 요청을 서버에 보내게 하는 공격이다. 서버가 공격자가 예측하기 어려운 위조 방지 토큰을 발급하고 **요청에 포함된 토큰의 유효성을 검증**하면, 인증 정보만 자동으로 붙은 위조 요청을 거부할 수 있다. 토큰을 추가하는 것뿐 아니라 서버에서 확인하는 절차가 필요하다.

NoteBase

문 13. 포트 스캔(Port Scan)에 대한 설명으로 옳지 않은 것은?

① 공격 대상 시스템의 운영체제 확인이 가능하다.

② 특정 패킷을 보내서 공격 대상 시스템의 어떤 서비스 포트가 열려 있고 닫혀 있는지 확인할 수 있다.

③ 스캐닝 공격 기법 종류에는 TCP Scan, UDP Scan, Fin Scan, XMAS Scan 등이 있다.

④ UDP Scanning은 3-Way Handshaking의 특징을 악용하는 방법이다.

정답 4번

간단한 해설

④의 '3-Way Handshaking'은 **TCP의 연결 설정 절차**이다. UDP는 이 절차를 사용하지 않으며, UDP 스캔은 **UDP 응답이나 ICMP 오류 메시지** 등을 바탕으로 포트 상태를 판단한다.

선지별 해설

① O: 운영체제마다 TCP/IP 패킷을 처리하는 방식에 차이가 있다. 스캔 과정에서 얻은 응답 패킷의 특성을 알려진 운영체제의 특성과 비교하는 **운영체제 지문 분석**으로 대상의 운영체제를 식별하거나 추정할 수 있다. 다만 응답이 제한되거나 변조되면 정확한 식별이 어려울 수 있다.

② O: 포트 스캔은 대상의 포트에 특정 패킷을 보내고 **응답의 종류와 유무**를 분석하여 포트 상태를 조사한다. 예를 들어 TCP SYN 스캔에서는 SYN 패킷에 SYN/ACK가 오면 열린 포트로, RST가 오면 닫힌 포트로 판단한다. 방화벽이 패킷을 차단하면 개방 여부를 확정하지 못할 수도 있다.

③ O: TCP 스캔과 UDP 스캔은 각각 TCP와 UDP 포트를 조사하는 기법이다. FIN 스캔과 XMAS 스캔도 포트 스캔에 속하며, **TCP 헤더의 제어 플래그**를 달리 설정한다. FIN 스캔은 FIN 플래그를, XMAS 스캔은 FIN·PSH·URG 플래그를 설정한 패킷을 보내 응답을 분석한다.

④ X: 3-Way Handshaking은 SYN → SYN/ACK → ACK 순으로 이루어지는 **TCP의 연결 설정 절차**이며, 비연결형 프로토콜인 UDP에는 이 절차가 없다. UDP 스캔은 UDP 패킷을 보낸 뒤 UDP 응답이 오면 열린 포트로, ICMP 'Port Unreachable' 오류가 오면 닫힌 포트로 판단한다. 응답이 없을 때는 열린 포트와 패킷이 차단된 포트를 구별하지 못할 수 있다. 따라서 선지의 연결 설정 절차를 이용한다는 설명은 TCP 스캔에 관한 내용으로 고쳐야 한다.

NoteBase

문 14. OECD의 '개인정보보호 원칙'이 아닌 것은?

① 책임의 원칙(Accountability Principle)
② 이용 제한의 원칙(Use Limitation Principle)
③ 정보 정확성의 원칙(Data Quality Principle)
④ 비공개의 원칙(Closeness Principle)

정답 4번

①

책임의 원칙은 **개인정보관리자가 개인정보보호 원칙을 실현하는 조치의 준수에 책임을 져야 한다**는 원칙이다.

프라이버시 보호 및 개인정보의 국경 간 이전에 관한 가이드라인 제2부 제14항
개인정보관리자는 앞서 규정된 개인정보보호 원칙들을 실현하는 조치를 준수하는 데 책임을 져야 한다.

②

이용 제한의 원칙은 **정보주체의 동의나 법률상 근거가 있는 경우를 제외하고, 명시된 목적 외의 개인정보 공개·제공·이용을 제한**하는 원칙이다.

프라이버시 보호 및 개인정보의 국경 간 이전에 관한 가이드라인 제2부 제10항
개인정보는 제9항에 따라 명시된 목적 외의 목적으로 공개·제공하거나 그 밖의 방식으로 이용하지 않도록 한다. 다만 정보주체의 동의가 있거나 법률의 권한에 따른 경우는 예외로 한다.

③

정보 정확성의 원칙은 개인정보가 이용 목적에 부합하고, **그 목적에 필요한 범위에서 정확성·완전성·최신성을 유지해야 한다**는 원칙이다.

프라이버시 보호 및 개인정보의 국경 간 이전에 관한 가이드라인 제2부 제8항
개인정보는 이용 목적에 부합해야 하며, 그 목적에 필요한 범위에서 정확하고 완전하며 최신 상태로 유지되어야 한다.

NoteBase

④

8원칙에 포함되는 것은 **공개의 원칙(Openness Principle)**이다. 개인정보 처리 정책·관행과 개인정보의 존재·이용 목적 등을 쉽게 확인할 수 있도록 하는 원칙이며, 비공개의 원칙은 포함되지 않는다.

프라이버시 보호 및 개인정보의 국경 간 이전에 관한 가이드라인 제2부 제12항
개인정보와 관련된 발전·관행·정책에 관하여 전반적인 공개 방침을 두어야 한다. 개인정보의 존재와 성격, 주요 이용 목적, 개인정보처리자의 신원과 통상 거주지를 쉽게 확인할 수 있는 수단이 마련되어야 한다.

NoteBase

문 15. 다음 설명의 (가), (나), (다)에 들어갈 용어를 바르게 연결한 것은?

○ (가)은/는 단말기가 회사의 내부 네트워크에 접속을 시도할 때 이를 제어하고 통제한다.
○ (나)은/는 외부 네트워크에서 내부 네트워크로 유입되는 침입을 막는다.
○ (다)은/는 시스템이나 네트워크에 대한 다양한 불법 침입행위를 실시간 탐지, 분석하여 비정상적인 패킷일 때 자동으로 차단한다.

① (가): NAC, (나): 방화벽, (다): IPS
② (가): IPS, (나): DRM, (다): 방화벽
③ (가): NAC, (나): IPS, (다): IDS
④ (가): DRM, (나): IDS, (다): NAC

정답 1번

간단한 해설

(다)의 핵심은 침입을 탐지하는 데 그치지 않고 비정상적인 패킷을 **자동으로 차단**한다는 점이다. 탐지·경보가 중심인 IDS와 달리, IPS는 탐지한 공격을 직접 차단하는 침입방지시스템이다.

빈칸별 해설

(가) NAC: 네트워크 접근제어(Network Access Control)는 **단말기의 네트워크 접속 허용 여부**를 통제한다. 사용자·단말기의 인증 정보나 보안 상태 등을 확인하여 내부 네트워크에 접속할 수 있는지를 결정하므로, 단말기의 접속 시도를 제어한다는 설명에 해당한다.

(나) 방화벽: 내부 네트워크와 외부 네트워크 사이에서 **보안 정책에 따라 통신을 허용하거나 차단**한다. 외부에서 내부로 들어오는 트래픽 중 허용되지 않은 통신을 차단하여 내부 네트워크를 보호하므로, 외부로부터 유입되는 침입을 막는다는 설명에 해당한다.

(다) IPS: 침입방지시스템(Intrusion Prevention System)은 시스템이나 네트워크의 트래픽을 실시간으로 탐지·분석하고, 공격으로 판단한 패킷을 **자동으로 차단**한다. IDS가 침입 탐지와 경보에 중점을 두는 것과 달리 차단까지 수행하므로, 제시문의 '비정상적인 패킷일 때 자동으로 차단'이 IPS를 가리키는 결정적인 단서이다.

따라서 (가) NAC, (나) 방화벽, (다) IPS의 연결은 ①과 일치한다.

NoteBase

문 16. 다음에서 설명하는 네트워크 공격은?

출발지와 목적지의 IP 주소를 동일하게 공격 대상의 IP 주소로 변조하여 전송한다. 출발지 IP 주소가 자신의 IP 주소이므로 스스로 응답하고, 이 과정을 반복하여 과부하를 유발한다.

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

정답 4번

간단한 해설

출발지와 목적지 IP 주소를 모두 **공격 대상 자신의 IP 주소**로 설정하는 것이 Land 공격의 핵심이다. 대상이 자기 자신을 통신 상대로 처리하게 하여 과부하를 유발한다.

핵심 풀이

Land 공격: 패킷의 출발지와 목적지 IP 주소를 모두 공격 대상의 IP 주소로 위조하는 서비스 거부 공격이다.
목적지 주소 때문에 패킷은 공격 대상에게 전달되고, 출발지 주소도 자기 주소이므로 응답 상대 역시 자기 자신이 된다. 취약한 시스템은 이러한 패킷을 처리하는 과정에서 자원을 소모하거나 정상적인 통신 처리를 방해받는다.
지문의 **'출발지와 목적지의 IP 주소를 동일하게'**라는 조건과 '스스로 응답'한다는 설명이 이 공격을 가리킨다.

Smurf 공격과의 구분: Smurf 공격도 출발지 IP 주소를 공격 대상의 주소로 위조하지만, 요청의 목적지는 **브로드캐스트 주소**이다. 요청을 받은 여러 호스트의 ICMP 응답이 공격 대상에게 몰리게 한다. 따라서 대상이 자기 자신을 응답 상대로 처리하는 Land 공격과는 응답을 발생시키는 방식이 다르다.

NoteBase

문 17. 암호에 대한 설명으로 옳지 않은 것은?

① 공개키 암호 알고리즘은 트랩도어 단방향 함수에 기반을 둔다.

② 대칭키 암호 알고리즘은 공개키 암호 시스템에 비해서 암호화 및 복호화 속도가 빠르다.

③ 공개키 암호 알고리즘의 대표적인 알고리즘은 DES이다.

④ 공개키 암호는 전자서명에 사용된다.

정답 3번

간단한 해설

DES는 암호화와 복호화에 같은 비밀키를 사용하는 **대칭키 블록 암호**이다. 대표적인 공개키 암호 알고리즘으로는 RSA가 있다.

선지별 해설

① O: 트랩도어 단방향 함수는 정방향 계산은 쉽지만 역방향 계산은 어렵고, **특별한 비밀정보를 알면 역방향 계산도 쉽게 할 수 있는 함수**이다. 공개키 암호는 이러한 성질을 이용하여 공개키로 암호화할 수 있게 하면서도 대응하는 개인키를 가진 수신자만 효율적으로 복호화할 수 있게 한다.

② O: 대칭키 암호는 비교적 단순한 연산을 반복하여 데이터를 처리하므로, 큰 수에 대한 복잡한 수학적 연산을 이용하는 공개키 암호보다 **일반적으로 암호화·복호화 속도가 빠르다**. 따라서 대용량 데이터의 암호화에는 주로 대칭키 암호를 사용한다.

③ X: DES는 공개키 암호가 아니라 **대칭키 블록 암호**이다. 송신자와 수신자가 같은 비밀키를 공유하고 그 키로 암호화와 복호화를 수행한다. 공개키와 개인키라는 서로 다른 키를 사용하는 대표적인 공개키 암호 알고리즘으로는 RSA가 있다.

④ O: 공개키 암호 기술은 전자서명에 사용된다. 서명자는 **개인키로 서명을 생성**하고 검증자는 서명자의 **공개키로 서명을 검증**한다. 이를 통해 서명자의 신원을 확인하고 서명된 데이터의 변경 여부를 검증할 수 있다.

NoteBase

문 18. 「정보보호산업의 진흥에 관한 법률 시행령」에 따른 정보보호 공시에 대한 설명으로 옳지 않은 것은?

① 정보기술부문 투자 현황 대비 정보보호부문 투자 현황은 정보보호 공시 내용에 포함된다.

② 공공기관은 정보보호공시의무자에서 제외된다.

③ 공시 주체의 정보보호 최고책임자가 주관하여 공시하여야 한다.

④ 「전자금융거래법」에 따른 금융회사는 정보보호공시의무자에 포함된다.

정답 4번

①

정보보호 공시에는 **정보기술부문 투자 현황 대비 정보보호부문 투자 현황**을 포함해야 한다.

정보보호산업의 진흥에 관한 법률 시행령 제8조(정보보호 공시)
③ 정보통신망을 통하여 정보를 제공하거나 정보의 제공을 매개하는 자가 법 제13조제1항 또는 제2항에 따라 정보보호 공시를 하는 경우에는 다음 각 호의 내용을 포함해야 한다. <개정 2021.12.9>
1. 정보기술부문 투자 현황 대비 정보보호부문 투자 현황

②

공공기관은 정보보호공시의무자에서 제외한다.

정보보호산업의 진흥에 관한 법률 시행령 제8조(정보보호 공시)
② 제1항에도 불구하고 다음 각 호의 어느 하나에 해당하는 자는 정보보호공시의무자에서 제외한다. <신설 2021.12.9, 2025.10.1>
1. 공공기관

③

정보보호 공시는 **공시 주체의 정보보호 최고책임자가 주관**하며, 공시내용은 미리 최고경영자의 확인을 거쳐야 한다.

정보보호산업의 진흥에 관한 법률 시행령 제8조(정보보호 공시)
④ 법 제13조제1항 또는 제2항에 따라 정보보호 공시를 하는 경우에는 공시 주체의 정보보호 최고책임자가 주관하여 공시하여야 하며, 공시내용에 대해서는 미리 최고경영자의 확인을 거쳐야 한다. <개정 2021.12.9>

NoteBase

④

「전자금융거래법」에 따른 **금융회사는 정보보호공시의무자에서 제외**한다.

정보보호산업의 진흥에 관한 법률 시행령 제8조(정보보호 공시)
② 제1항에도 불구하고 다음 각 호의 어느 하나에 해당하는 자는 정보보호공시의무자에서 제외한다. <신설 2021.12.9, 2025.10.1>
3. 「전자금융거래법」에 따른 금융회사

NoteBase

문 19. 다음에서 설명하는 접근제어 과정은?

◯ 자신의 신분 또는 위변조를 증명하는 과정
◯ 지문, 홍채, 정맥을 이용한 확인 과정

① Identification
② Authorization
③ Authentication
④ One-Time Password

정답 3번

간단한 해설

지문·홍채·정맥 같은 생체정보로 **본인임을 검증**하는 과정은 인증(Authentication)이다. 사용자가 누구라고 밝히는 것과 그 주장이 사실인지 확인하는 것은 구별된다.

개념 구분

인증(Authentication): 주장한 신원이나 대상의 진위를 검증하는 과정이다. 접근제어에서는 사용자가 주장한 신원이 실제 본인의 것인지 확인한다. 지문·홍채·정맥 같은 **생체적 특징으로 본인임을 확인**하는 과정이 이에 해당한다. 인증은 정보의 출처와 무결성을 확인하는 의미로도 쓰이므로, 첫 단서의 '위변조'는 정보의 진위 검증과 연결해 이해할 수 있다.

식별(Identification): 접근제어에서 아이디 등을 제시하여 **자신이 누구인지 밝히는** 과정이다. 예를 들어 아이디를 입력하는 것은 식별이고, 그 아이디의 실제 사용자임을 지문으로 검증하는 것은 인증이다.

인가(Authorization): 사용자에게 어떤 자원이나 행위에 대한 접근 권한을 부여하거나 허용 여부를 결정하는 과정이다. 본인인지 확인하는 인증과 달리, **무엇을 할 수 있는지**를 다룬다.

일회용 비밀번호(One-Time Password): 한 번만 사용할 수 있는 비밀번호로 인증에 이용된다. 인증을 수행하는 **수단의 하나**이며, 지문·홍채·정맥을 이용한 생체인증까지 포괄하는 과정의 명칭은 아니다.

NoteBase

문 20. 암호 알고리즘에 대한 설명으로 옳은 것은?

① AES는 다에먼(Daemen)과 레이먼(Rijmen)이 제안한 Rijndael을 기반으로 제정된 미국 표준 알고리즘이다.

② SEED는 미국 NIST가 표준으로 선정한 대칭키 알고리즘이다.

③ ARIA는 스트림 암호 방식으로 동작하는 알고리즘이다.

④ IDEA는 리베스트(Rivest)가 개발한 알고리즘으로 블록, 키, 라운드 크기가 모두 가변적이다.

정답 1번

간단한 해설

AES는 다에먼(Daemen)과 레이먼(Rijmen)이 설계한 **Rijndael을 기반으로 제정된 미국 표준 대칭키 암호**이다. 개발자의 국적과 그 알고리즘을 표준으로 채택한 국가는 구별해야 한다.

선지별 해설

① O: AES는 벨기에의 Joan Daemen과 Vincent Rijmen이 제안한 Rijndael을 기반으로 미국 NIST가 선정하고 FIPS 197로 제정한 표준이다. 따라서 **벨기에 연구자가 개발한 알고리즘을 미국 표준으로 채택**했다는 관계가 성립한다.

② X: SEED는 **한국의 KISA가 개발한 대칭키 블록 암호**이다. 미국 NIST가 AES로 선정한 알고리즘은 SEED가 아니라 Rijndael이다. SEED가 대칭키 알고리즘이라는 부분은 맞지만, 표준 선정 기관과 알고리즘의 대응이 잘못되었다.

③ X: ARIA는 스트림 암호가 아니라 **128비트 블록 단위로 암호화하는 대칭키 블록 암호**이다. 스트림 암호가 키스트림을 생성해 평문과 결합하는 방식인 데 비해, ARIA는 정해진 크기의 데이터 블록에 암호 변환을 적용한다.

④ X: IDEA는 리베스트가 아니라 **라이(Lai)와 매시(Massey)가 개발**한 대칭키 블록 암호이다. 블록 크기는 64비트, 키 길이는 128비트이며, 8회의 라운드 뒤에 출력 변환을 수행한다. 이 출력 변환을 반 라운드로 세어 8.5라운드라고도 한다. 따라서 개발자뿐 아니라 블록·키·라운드가 모두 가변적이라는 설명도 잘못되었다.

NoteBase

문 21. 국가정보원장이 중앙행정기관의 사이버보안 업무 수행을 위한 조직, 인력, 예산, 직무교육 및 사이버보안에 대한 자체 진단·점검 등을 평가하는 제도는?

① 개인정보 보호수준 평가

② 보안적합성 검증

③ 사이버보안 실태평가

④ 개인정보 침해요인 평가

정답 3번

②

보안적합성 검증은 도입·운영하거나 이용하는 **정보보호시스템 등과 클라우드컴퓨팅서비스가 보안대책에 적합한지 확인**하는 제도이다. 제시된 조직·인력·예산 등의 평가는 **사이버보안 실태 평가**에 해당한다.

사이버안보 업무규정 제9조(사이버보안 예방 조치 등)
③ 국가정보원장은 중앙행정기관등이 도입 · 운영하거나 이용하는 정보보호시스템등 및 클라우드컴퓨팅서비스가 제2항에 따른 보안대책에 적합한지 검증할 수 있다. <개정 2024.3.5>

사이버안보 업무규정 제13조(사이버보안 실태 평가)
① 국가정보원장은 중앙행정기관등의 사이버보안 업무 수행을 위한 조직, 인력, 예산, 직무교육 및 사이버보안에 대한 자체 진단 · 점검 등 사이버보안 실태를 평가할 수 있다. <개정 2024.3.5>

③

사이버보안 실태 평가는 국가정보원장이 중앙행정기관 등의 **사이버보안 조직·인력·예산·직무교육 및 자체 진단·점검 등 업무 수행 실태를 평가**하는 제도이다.

사이버안보 업무규정 제13조(사이버보안 실태 평가)
① 국가정보원장은 중앙행정기관등의 사이버보안 업무 수행을 위한 조직, 인력, 예산, 직무교육 및 사이버보안에 대한 자체 진단 · 점검 등 사이버보안 실태를 평가할 수 있다. <개정 2024.3.5>

NoteBase

문 22. CC 인증은 시스템에 대한 보안을 평가하기 위하여 EAL(Evaluation Assurance Level)의 1⊠7단계를 두어 평가한다. '정형화된 설계 검증 및 시험' 단계에 해당하는 것은?

① EAL4

② EAL5

③ EAL6

④ EAL7

정답 4번

간단한 해설

'정형화된 설계 검증 및 시험'은 **EAL7**의 명칭이다. 여기서 정형화는 수학적으로 엄밀한 표현과 증명을 활용해 설계를 검증한다는 뜻이다.

공통 해설

EAL은 평가 대상의 보안 기능을 얼마나 엄격하게 분석·검증·시험했는지를 나타내는 평가보증등급이다. 이 중 EAL7은 **'정형화된 설계 검증 및 시험'**(Formally verified design and tested) 단계이다. 정형적 검증은 수학적으로 엄밀한 명세와 증명을 이용해 설계가 보안 요구사항에 부합하는지 확인하는 방식으로, 실제 동작을 확인하는 시험과 함께 보증의 근거가 된다.

구별할 기준은 단순히 시험을 수행하는지가 아니라 **설계 검증의 정형성**이다. EAL4의 체계적인 설계·시험·검토, EAL5의 준정형화된 설계·시험, EAL6의 준정형화된 설계 검증·시험과 구별하여, 문제에서 제시한 정형화된 설계 검증·시험은 EAL7에 대응한다.

NoteBase

문 23. 기업망을 보호하기 위해 네트워크 경계를 신뢰 판단의 전제로 삼지 않고, 위치와 관계없이 모든 접근을 지속적으로 검증하고, 최소 권한만 부여하는 보안 방식은?

① 다중 인증(Multi-factor Authentication)

② 챌린지 핸드셰이크 인증 프로토콜(Challenge Handshake Authentication Protocol)

③ 제로 트러스트 보안 모델(Zero Trust Security Model)

④ 임의적 접근 통제 모델(Discretionary Access Control Model)

정답 3번

간단한 해설

제로 트러스트는 내부망에 있다는 이유만으로 접근을 신뢰하지 않는다. 위치와 관계없이 접근의 적절성을 지속적으로 검증하고, 업무에 필요한 **최소 권한**만 부여한다.

핵심 풀이

제로 트러스트 보안 모델은 **네트워크 위치에 따른 암묵적 신뢰를 배제**한다. 사용자 신원, 단말 상태, 접근하려는 자원 등을 확인하여 접근 허용 여부를 판단하고, 접근 중에도 위험이나 상태 변화에 따라 권한을 재평가한다. 또한 필요한 자원과 작업에 한정해 최소 권한을 부여한다. 예를 들어 내부망의 직원이라도 특정 문서를 읽는 데 필요한 권한만 부여받았다면 그 문서를 수정할 수는 없다. 발문의 경계에 의존하지 않는 신뢰 판단, 지속적 검증, 최소 권한은 이 모델을 가리킨다.

다중 인증과 CHAP는 사용자의 신원을 확인하는 인증 방식이다. 다중 인증은 서로 다른 유형의 인증 요소를 함께 사용하며, CHAP는 도전값에 대한 응답을 검증한다. 이들은 **인증을 수행하는 수단**이며, 발문처럼 접근 전반의 신뢰 판단과 권한 부여 원칙을 포괄하는 보안 모델과 구별된다.

임의적 접근 통제는 **자원 소유자의 재량**에 따라 다른 사용자의 접근 권한을 정하는 방식이다. 누가 권한을 부여하는지가 구분 기준이며, 네트워크 위치와 무관하게 지속적으로 검증한다는 제로 트러스트의 원칙과는 다르다.

NoteBase

문 24. 검증필 암호모듈(KCMVP)의 검증대상 암호알고리즘이 아닌 것은?

① ARIA

② RC5

③ AES

④ LEA

정답 2번

간단한 해설

RC5는 암호알고리즘이지만 **KCMVP의 검증대상에는 포함되지 않는다**. 암호알고리즘이라는 사실과 검증대상으로 지정되었다는 사실은 구별해야 한다.

선지별 해설

KCMVP는 암호모듈의 구현 적합성과 안전성 등을 검증하는 제도이다. 이 문항은 각 알고리즘이 검증대상으로 지정되어 있는지를 묻는다. 검증대상 알고리즘을 사용했다는 사실만으로 해당 암호모듈 자체가 검증을 마쳤다는 뜻은 아니다.

① O: ARIA는 128비트 블록암호로, KCMVP의 **검증대상 블록암호**에 포함된다.

② X: RC5는 KCMVP의 검증대상 암호알고리즘에 포함되지 않는다. 검증대상 블록암호에는 ARIA·SEED·LEA·HIGHT·AES가 있으며, **RC5는 이 지정 목록에 없다**.

③ O: AES는 KCMVP의 검증대상 블록암호에 포함된다. 검증대상 여부를 **국산 알고리즘인지 여부만으로 판단해서는 안 된다**.

④ O: LEA는 128비트 블록암호로, KCMVP의 검증대상 블록암호에 포함된다.

NoteBase

문 25. 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 시행령」에 따른 클라우드컴퓨팅서비스의 보안인증 절차 등에 대한 설명으로 옳지 않은 것은?

① 한국인터넷진흥원은 클라우드컴퓨팅서비스에 대한 보안인증기관의 하나이다.

② 국가기관 등이 이용하는 클라우드컴퓨팅서비스의 보안인증 기준은 국가정보원장이 정한다.

③ 보안인증의 유효기간은 5년이다.

④ 보안인증의 유효기간은 연장할 수 있다.

정답 2번

①

한국인터넷진흥원은 보안인증 업무를 수행하며, 보안인증을 받으려는 자의 인증 신청서와 첨부서류를 접수한다.

클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 시행령 제15조의6(클라우드컴퓨팅서비스의 보안인증 절차 등)
① 법 제23조의2제1항에 따라 클라우드컴퓨팅서비스에 대한 보안인증(이하 "보안인증"이라 한다)을 받으려는 자는 과학기술정보통신부령으로 정하는 인증 신청서에 다음 각 호의 서류를 첨부하여 보안인증에 관한 업무를 수행하는 한국인터넷진흥원 또는 같은 조 제5항에 따라 지정된 기관(이하 "인증기관"이라 한다)에 제출해야 한다.
1. 법 제23조제2항에 따른 클라우드컴퓨팅서비스의 정보보호에 관한 기준(관리적 · 물리적 · 기술적 보호조치를 포함한다. 이하 "보안인증기준"이라 한다)에 적합한지 여부를 확인할 수 있는 서류
2. 보안인증 대상 목록
3. 그 밖에 보안인증에 필요한 사항으로서 과학기술정보통신부장관이 고시하는 사항에 관한 서류

②

국가기관 등이 이용하는 클라우드컴퓨팅서비스의 보안인증기준은 **과학기술정보통신부장관이 국가정보원장과 미리 협의하여 정하고 고시**한다. 국가정보원장이 정하는 것이 아니다.

클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 시행령 제15조의6(클라우드컴퓨팅서비스의 보안인증 절차 등)
⑧ 제1항부터 제7항까지에서 규정한 사항 외에 보안인증에 필요한 사항은 과학기술정보통신부장관이 정하여 고시한다. 다만, 국가기관등이 이용하는 클라우드컴퓨팅서비스의 보안인증기준은 국가정보원장과, 이용 안전성 확보에 관한 사항은 행정안전부장관과 미리 협의해야 한다.

NoteBase

③

보안인증의 유효기간은 **5년**이다.

클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 시행령 제15조의7(보안인증의 유효기간 등)
① 법 제23조의2제2항에 따른 보안인증의 유효기간은 5년으로 한다.

④

보안인증의 유효기간은 **연장할 수 있으며, 연장받으려는 자는 유효기간 만료 6개월 전까지 신청**해야 한다.

클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 시행령 제15조의7(보안인증의 유효기간 등)
② 제1항에 따른 유효기간을 연장받으려는 자는 보안인증의 유효기간이 만료되기 6개월 전까지 보안인증의 유효기간 연장을 신청해야 한다.

NoteBase