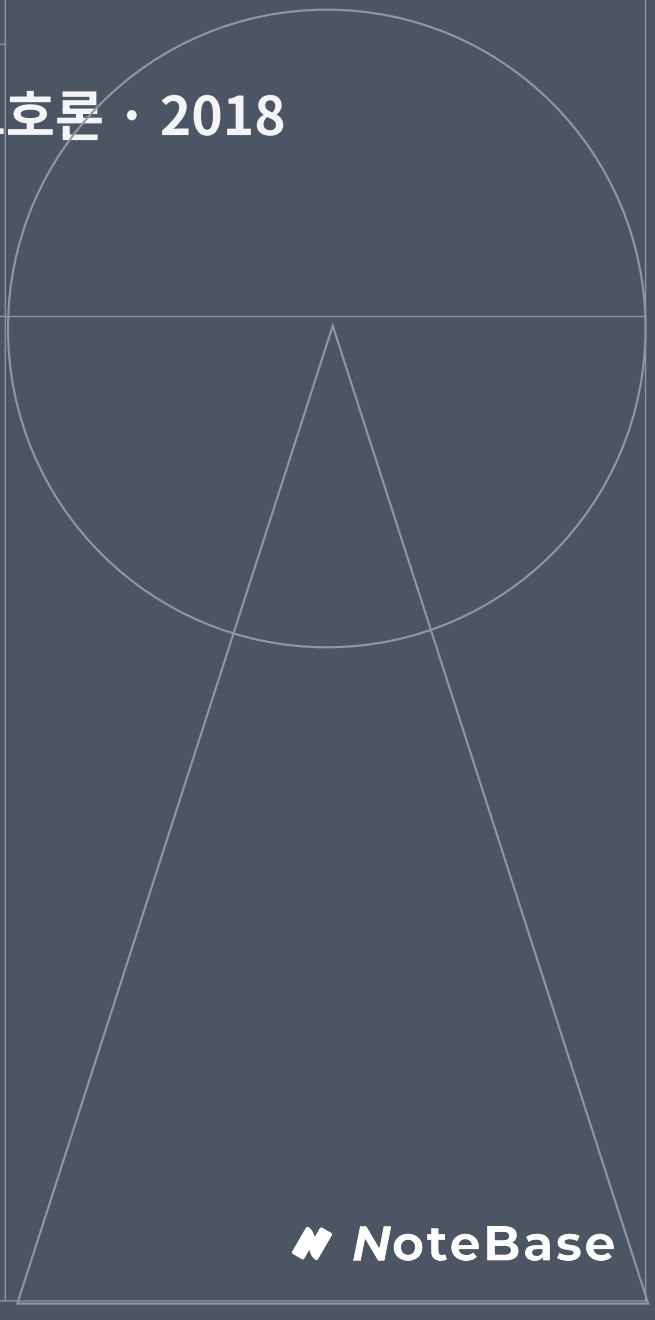
기출OX 해설집

공무원/국가직/9급 · 정보보호론 · 2018



NoteBase

기출OX 해설집

공무원/국가직/9급 · 정보보호론 · 2018

공무원/국가직/9급 · 정보보호론 · 2018

문 1. 전자우편 보안 기술이 목표로 하는 보안 특성이 아닌 것은?

① 익명성

② 기밀성

③ 인증성

④ 무결성

정답 1번

간단한 해설

익명성은 발신자의 신원을 숨기는 특성이다. 일반적인 전자우편 보안은 메시지를 보호하고 발신자를 확인하는 데 목적이 있으며, **익명성을 기본 목표로 삼지는 않는다**.

선지별 해설

① X: 익명성은 통신 주체가 누구인지 드러나지 않게 하는 특성이다. S/MIME 같은 일반적인 전자우편 보안 기술은 내용의 기밀성·무결성과 발신자의 인증성 등을 목표로 하며, **발신자의 신원을 숨기는 것을 기본 목표로 삼지 않는다**.

② O: 기밀성은 **허가받지 않은 사람이 메시지 내용을 알 수 없게** 하는 특성이다. 전자우편 내용을 암호화하여 도청이나 유출로부터 보호한다.

③ O: 인증성은 메시지가 **주장하는 발신자로부터 온 것인지 확인**할 수 있는 특성이다. 발신자의 전자서명을 검증하는 방식으로 발신자 사칭에 대응한다.

④ O: 무결성은 메시지가 **허가 없이 변경되지 않았음**을 확인할 수 있는 특성이다. 전자서명 검증 등을 통해 전송 중 내용이 변조되었는지 확인한다.

NoteBase

문 2. 프로그램이나 손상된 시스템에 허가되지 않는 접근을 할 수 있도록 정상적인 보안 절차를 우회하는 악성 소프트웨어는?

① 다운로더(downloader)

② 키 로거(key logger)

③ 봇(bot)

④ 백도어(backdoor)

정답 4번

간단한 해설

정상적인 보안 절차를 **우회하여 허가되지 않은 접근을 허용**하는 악성 소프트웨어가 백도어이다.

공통 해설

백도어(backdoor)는 프로그램이나 시스템에 정상적인 인증·접근 통제를 거치지 않고 들어갈 수 있는 우회 경로를 제공한다. 예를 들어 공격자가 심어 둔 프로그램을 통해 정상 로그인 절차 없이 시스템에 접속하거나 명령을 실행할 수 있게 하는 방식이다. 문항의 핵심은 악성 소프트웨어가 수행하는 여러 행위 중 **보안 절차를 우회하는 접근 경로를 제공한다**는 기능이며, 이는 백도어의 정의에 해당한다.

NoteBase

문 3. 프로그램을 감염시킬 때마다 자신의 형태뿐만 아니라 행동 패턴까지 변화를 시도하기도 하는 유형의 바이러스는?

① 암호화된(encrypted) 바이러스
② 매크로(macro) 바이러스
③ 스텔스(stealth) 바이러스
④ 메타모픽(metamorphic) 바이러스

정답 4번

간단한 해설

메타모픽 바이러스는 감염·복제할 때 **자신의 코드 자체를 재작성**하여 형태와 구체적인 실행 방식을 바꾼다. 기본 악성 기능을 유지하면서도 코드 패턴을 달리하므로 일정한 패턴에 의존하는 탐지를 어렵게 한다.

공통 해설

메타모픽(metamorphic) 바이러스는 감염·복제 과정에서 **자신의 프로그램 코드를 다시 작성**하는 바이러스이다. 새 복제본은 기존 복제본과 명령어 배열이나 코드 구조가 달라질 수 있어, 알려진 코드의 특정 바이트 패턴을 찾는 탐지를 피하기 쉽다.

예를 들어 어떤 명령어를 기능이 같은 다른 명령어로 바꾸거나, 실행 결과에 영향을 주지 않는 코드를 끼워 넣을 수 있다. 이렇게 하면 실제로 실행되는 명령어의 조합은 달라져도 **기본적인 악성 기능은 유지**된다. 문제에서 말하는 '형태뿐만 아니라 행동 패턴까지 변화'는 이러한 코드와 구체적 실행 방식의 변형에 연결되며, 악성 기능 자체가 매번 달라져야 한다는 뜻은 아니다.

NoteBase

문 4. 증거의 수집 및 분석을 위한 디지털 포렌식의 원칙에 대한 설명으로 옳지 않은 것은?

① 정당성의 원칙－증거 수집의 절차가 적법해야 한다.

② 연계 보관성의 원칙－획득한 증거물은 변조가 불가능한 매체에 저장해야 한다.

③ 신속성의 원칙－휘발성 정보 수집을 위해 신속히 진행해야 한다.

④ 재현의 원칙－동일한 조건에서 현장 검증을 실시하면 피해 당시와 동일한 결과가 나와야 한다.

정답 2번

간단한 해설

②의 변조 방지 설명은 **무결성의 원칙**에 해당한다. **연계 보관성의 원칙**은 증거를 누가 수집·인계·보관했는지 그 이력을 끊김 없이 기록하여 추적할 수 있어야 한다는 뜻이다.

선지별 해설

① O: 정당성의 원칙은 증거를 **적법한 절차로 수집**해야 한다는 원칙이다. 증거의 내용이 사건과 관련되어 있더라도 수집 절차의 적법성은 별도로 확보해야 한다.

② X: 연계 보관성의 원칙은 증거의 수집부터 이송·분석·보관에 이르기까지 **취급자와 처리 이력을 연속적으로 기록**하여 증거의 이동과 관리 과정을 추적할 수 있어야 한다는 원칙이다. 변조를 방지하는 매체에 저장하여 증거 내용이 바뀌지 않도록 하는 것은 무결성의 원칙과 관련된다. 안전한 매체에 저장했더라도 인계·보관 이력이 빠져 있다면 연계 보관성을 확보했다고 할 수 없다.

③ O: 신속성의 원칙은 디지털 증거가 사라지거나 바뀌기 전에 신속하게 수집해야 한다는 원칙이다. 특히 메모리의 정보처럼 **전원이 꺼지면 소실될 수 있는 휘발성 정보**는 수집이 늦어지면 확보할 수 없으므로 신속한 대응이 필요하다.

④ O: 재현의 원칙은 **동일한 조건에서 검증하면 동일한 결과**를 얻을 수 있어야 한다는 원칙이다. 피해 당시의 환경과 실행 조건을 재구성하여 같은 현상이 나타나는지 확인함으로써 원인에 대한 분석을 검증한다. 이때 조건이 달라진 실험의 결과를 그대로 비교해서는 안 된다.

NoteBase

문 5. 웹 애플리케이션의 대표적인 보안 위협의 하나인 인젝션 공격에 대한 대비책으로 옳지 않은 것은?

① 보안 프로토콜 및 암호 키 사용 여부 확인

② 매개변수화된 인터페이스를 제공하는 안전한 API 사용

③ 입력 값에 대한 적극적인 유효성 검증

④ 인터프리터에 대한 특수 문자 필터링 처리

정답 1번

간단한 해설

보안 프로토콜과 암호 키는 통신·데이터 보호에 쓰이지만, 입력값이 명령으로 해석되는 인젝션을 직접 막지는 못한다. 인젝션을 막으려면 **입력 데이터와 실행할 명령을 분리**해야 한다.

선지별 해설

인젝션은 신뢰할 수 없는 입력값이 SQL 질의나 운영체제 명령 등의 일부로 해석되어, 공격자가 의도한 동작을 일으키는 공격이다. 방어의 핵심은 입력값이 명령의 구조나 의미를 바꾸지 못하게 하는 것이다.

① X: 보안 프로토콜과 암호 키의 사용 여부 확인은 암호화 등 데이터 보호가 적절히 이루어지는지 점검하는 조치이다. 암호화된 통신으로 전달된 입력에도 악성 명령이 포함될 수 있으므로, 이것만으로는 인젝션을 방지할 수 없다. 인젝션 대비책으로는 **명령과 데이터를 분리하는 매개변수화**와 입력값 검증 등을 적용해야 한다.

② O: 매개변수화된 인터페이스는 명령이나 질의의 구조를 먼저 정하고 입력값을 별도의 매개변수로 전달한다. 예를 들어 SQL 질의에 검색어를 문자열로 이어 붙이지 않고 매개변수로 전달하면, 검색어가 **질의 구문이 아닌 데이터**로 처리되도록 할 수 있다.

③ O: 입력값의 자료형·길이·범위·형식 등이 허용된 조건에 맞는지 검증하면 악성 입력이 처리되는 것을 줄일 수 있다. 예를 들어 숫자만 허용하는 항목에는 숫자 이외의 입력을 거부한다. 다만 정상 입력에도 특수 문자가 필요할 수 있으므로, **입력값 검증만으로 모든 인젝션을 막을 수는 없다**.

④ O: 인터프리터에서 명령을 구분하거나 제어하는 특수 문자를 적절히 제한하면 입력값이 명령 구조를 바꾸는 위험을 줄일 수 있다. 동적 질의를 사용해야 한다면 **해당 인터프리터의 문법에 맞는 이스케이프 처리**로 특수 문자가 제어 기호가 아닌 데이터로 해석되도록 해야 한다. 특정 문자 몇 개를 일괄 제거하는 방식만으로 완전한 방어가 되는 것은 아니다.

NoteBase

문 6. 「개인정보 보호법」 상의 개인정보의 수집·이용 및 수집 제한에 대한 설명으로 옳지 않은 것은?

① 개인정보처리자는 정보주체의 동의를 받은 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다.

② 개인정보처리자는 「개인정보 보호법」에 따라 개인정보를 수집하는 경우에는 그 목적에 필요한 최소한의 개인정보를 수집하여야 한다. 이 경우 최소한의 개인정보 수집이라는 입증책임은 개인정보처리자가 부담한다.

③ 개인정보처리자는 정보주체의 동의를 받아 개인정보를 수집하는 경우 필요한 최소한의 정보 외의 개인정보 수집에는 동의하지 아니할 수 있다는 사실을 구체적으로 알리고 개인정보를 수집하여야 한다.

④ 개인정보처리자는 정보주체가 필요한 최소한의 정보 외의 개인정보 수집에 동의하지 아니하는 경우 정보주체에게 재화 또는 서비스의 제공을 거부할 수 있다.

정답 4번

간단한 해설

필요한 최소한의 정보 외의 개인정보 수집에 동의하지 않았다는 이유로 **재화나 서비스의 제공을 거부해서는 안 된다**. 선택적인 정보 수집에 대한 동의를 서비스 이용의 조건으로 강제할 수 없기 때문이다.

선지별 해설

① O: 「개인정보 보호법」 제15조제1항제1호는 정보주체의 동의를 개인정보 수집·이용의 적법한 근거 중 하나로 정한다. 동의를 받아 수집한 개인정보는 **그 수집 목적의 범위에서 이용**할 수 있다.

② O: 같은 법 제16조제1항에 따라 개인정보처리자는 수집 목적에 필요한 최소한의 개인정보를 수집하여야 한다. 수집한 정보가 그 목적에 필요한 최소한의 정보라는 점은 **개인정보처리자가 입증**해야 한다. 정보주체에게 불필요한 수집이라는 점을 증명하도록 책임을 돌릴 수 없다.

③ O: 같은 법 제16조제2항은 동의를 받아 개인정보를 수집할 때, 필요한 최소한의 정보 외의 개인정보 수집에는 **동의하지 않을 수 있다는 사실을 구체적으로 알리도록** 한다. 정보주체가 추가적인 정보 제공을 스스로 선택할 수 있도록 보장하는 규정이다.

④ X: 같은 법 제16조제3항은 필요한 최소한의 정보 외의 개인정보 수집에 동의하지 않는다는 이유로 재화 또는 서비스의 제공을 **거부하는 것을 금지**한다. 따라서 '제공을 거부할 수 있다'는 '제공을 거부하여서는 아니 된다'로 고쳐야 한다. 이는 선택적인 정보 수집에 대한 동의를 강제하지 못하도록 하는 제한이다.

NoteBase

문 7. <보기 1>은 리눅스에서 일반 사용자(hello)가 'ls -al'을 수행한 결과의 일부분이다. <보기 2>의 설명에서 옳은 것만을 모두 고른 것은?

<보기 1>

-rwxr-xr-x 1 hello world 4096 Nov 21 15:12 abc.txt

ⓐ ⓑ

<보기 2>

ㄱ. ⓐ는 파일의 소유자, 그룹, 이외 사용자 모두가 파일을 읽고 실행할 수 있지만, 파일의 소유자만이 파일을 수정할 수 있음을 나타낸다.

ㄴ. ⓑ가 모든 사용자(파일 소유자, 그룹, 이외 사용자)에게 읽기, 쓰기, 실행 권한을 부여하려면 'chmod 777 abc.txt'의 명령을 입력하면 된다.

ㄷ. ⓑ가 해당 파일의 소유자를 root로 변경하려면 'chown root abc.txt'의 명령을 입력하면 된다.

① ㄱ

② ㄱ, ㄴ

③ ㄴ, ㄷ

④ ㄱ, ㄴ, ㄷ

정답 2번

간단한 해설

파일 소유자 hello는 **chmod로 접근 권한을 변경**할 수 있다. 그러나 일반 사용자 권한으로는 chown 명령을 입력해도 **파일 소유자를 root로 변경할 수 없다**.

NoteBase

보기별 해설

ㄱ. O: ⓐ의 '-rwxr-xr-x'에서 맨 앞 '-'는 일반 파일을 뜻하고, 뒤의 아홉 자리는 소유자·그룹·이외 사용자의 권한을 세 자리씩 나타낸다. r은 읽기, w는 쓰기, x는 실행이며 '-'는 해당 권한이 없다는 뜻이다. 소유자는 rwx, 그룹과 이외 사용자는 각각 r-x이므로 모두 읽기·실행 권한이 있지만, 표시된 권한 중 **쓰기 권한은 소유자에게만** 있다.

ㄴ. O: ⓑ의 hello는 abc.txt의 소유자이므로 chmod로 이 파일의 접근 권한을 변경할 수 있다. 숫자 모드에서 읽기는 4, 쓰기는 2, 실행은 1로 표시하므로 7 = 4 + 2 + 1은 세 권한을 모두 부여한다는 뜻이다. 'chmod 777 abc.txt'의 세 숫자는 차례로 소유자·그룹·이외 사용자에게 적용되어 **각각 읽기·쓰기·실행 권한**을 부여한다.

ㄷ. X: 'chown root abc.txt'는 파일 소유자를 root로 바꾸는 명령 형식이다. 그러나 문제의 hello는 일반 사용자이므로, 파일 소유자라는 이유만으로 다른 사용자에게 소유권을 넘길 수는 없다. 소유자 변경에는 **root 등 소유자 변경 권한을 가진 주체의 실행**이 필요하다. 따라서 hello가 일반 사용자 권한으로 이 명령만 입력하면 변경된다는 설명을 고쳐야 한다.

옳은 보기는 ㄱ, ㄴ이며, 이는 ②의 조합에 해당한다.

NoteBase

문 8. 다음은 CC(Common Criteria)의 7가지 보증 등급 중 하나에 대한 설명이다. 시스템이 체계적으로 설계되고, 테스트되고, 재검토되도록 (methodically designed, tested and reviewed) 요구하는 것은?

낮은 수준과 높은 수준의 설계 명세를 요구한다. 인터페이스 명세가 완벽할 것을 요구한다. 제품의 보안을 명시적으로 정의한 추상화 모델을 요구한다. 독립적인 취약점 분석을 요구한다. 개발자 또는 사용자가 일반적인 TOE의 중간 수준부터 높은 수준까지의 독립적으로 보증된 보안을 요구하는 곳에 적용 가능하다. 또한 추가적인 보안 관련 비용을 감수할 수 있는 곳에 적용 가능하다.

① EAL 2

② EAL 3

③ EAL 4

④ EAL 5

정답 3번

간단한 해설

CC의 **EAL 4**는 '체계적으로 설계되고, 테스트되고, 재검토됨'을 뜻하는 보증 등급이다. 상위·하위 설계 명세와 완전한 인터페이스 명세를 검토하고 독립적인 취약점 분석을 수행한다는 지문의 설명이 이에 해당한다.

공통 해설

CC의 평가보증등급(EAL)은 평가 대상인 TOE의 보안 기능을 얼마나 엄격한 근거와 절차로 확인하는지를 나타낸다. 이 중 EAL 4의 명칭은 **'체계적으로 설계되고, 테스트되고, 재검토됨'**(methodically designed, tested and reviewed)이다. 문제는 이 명칭과 그에 해당하는 보증 요구사항을 제시하여 등급을 묻고 있다.

지문의 상위 설계 명세는 보안 기능의 전체 구조를, 하위 설계 명세는 내부의 구체적인 설계를 설명한다. EAL 4에서는 이러한 설계 자료와 완전한 인터페이스 명세, 구현의 일부를 바탕으로 보안 기능이 어떻게 동작하는지 분석한다. 또한 보안정책을 명시한 비정형 모델과 개발자의 테스트 자료를 검토하고, **평가자의 독립적인 테스트와 취약점 분석**으로 개발자의 주장만으로는 확인하기 어려운 부분을 점검한다.

따라서 일반적인 평가 대상 제품에서 중간 수준부터 높은 수준까지의 독립적으로 보증된 보안을 원하고, 이를 위한 추가적인 보안 관련 비용을 감수하는 상황에 적용되는 등급이 EAL 4이다.

NoteBase

문 9. 다음에 설명한 Diffie-Hellman 키 교환 프로토콜의 동작 과정에서 공격자가 알지 못하도록 반드시 비밀로 유지해야 할 정보만을 모두 고른 것은?

소수 p와 p의 원시근 g에 대하여, 사용자 A는 p보다 작은 양수 a를 선택하고, x = g^a p를 계산하여 x를 B에게 전달한다. 마찬가지로 사용자 B는 p보다 작은 양수 b를 선택하고, y = g^b p를 계산하여 y를 A에게 전달한다. 그러면 A와 B는 g^ab p를 공유하게 된다.

① a, b

② p, g, a, b

③ a, b, g^ab p

④ p, g, a, b, g^ab p

정답 3번

간단한 해설

a와 b는 각 사용자의 **비밀 지수**이며, 두 사용자가 계산한 **공유 비밀값** g^ab p도 숨겨야 한다. p와 g는 공개해도 되는 계산 매개변수이다.

구성 요소별 해설

p, g: 소수 p와 원시근 g는 두 사용자가 같은 방식으로 계산하기 위한 **공개 매개변수**이다. 비밀로 유지해야 할 대상은 이 매개변수 자체가 아니라 각자의 비밀 지수와 공유 비밀값이다.

a, b: A와 B가 각각 선택한 **비밀 지수**이다. 상대에게 보내는 것은 a와 b 자체가 아니라 이들로 계산한 x와 y이다. a가 노출되면 공격자는 전달되는 y를 이용해 y^a p를 계산할 수 있고, b가 노출되면 x를 이용해 x^b p를 계산할 수 있다. 어느 경우든 두 사용자의 공유 비밀값을 얻으므로 a와 b는 모두 숨겨야 한다.

g^ab p: A가 y^a p를 계산한 결과와 B가 x^b p를 계산한 결과가 일치하는 **공유 비밀값**이다. 이 값은 통신용 키를 만드는 바탕이 되므로, a와 b를 숨겼더라도 공유 비밀값 자체가 노출되면 키 교환의 목적을 달성할 수 없다.

따라서 비밀로 유지해야 할 정보의 조합은 a, b, g^ab p이며, ③의 구성과 일치한다.

NoteBase

문 10. IEEE 802.11i에 대한 설명으로 옳지 않은 것은?

① 단말과 AP(Access Point) 간의 쌍별(pairwise) 키와 멀티캐스팅을 위한 그룹 키가 정의되어 있다.

② 전송되는 데이터를 보호하기 위해 TKIP(Temporal Key Integrity Protocol)와 CCMP(Counter Mode with Cipher Block Chaining MAC Protocol) 방식을 지원한다.

③ 서로 다른 유무선랜 영역에 속한 단말들의 종단간(end-to-end) 보안 기법에 해당한다.

④ 802.1X 표준에서 정의된 방법을 이용하여 무선 단말과 인증 서버 간의 상호 인증을 할 수 있다.

정답 3번

간단한 해설

IEEE 802.11i는 **단말과 AP 사이의 무선 링크**를 보호하는 보안 표준이다. 서로 다른 유무선랜 영역에 있는 단말 사이의 전체 통신 경로를 보호하는 종단간 보안 기법은 아니다.

선지별 해설

① O: 쌍별 키는 특정 단말과 AP 사이의 **유니캐스트 통신**을 보호하고, 그룹 키는 여러 단말이 수신하는 **멀티캐스트·브로드캐스트 통신**을 보호한다. 일대일 통신과 여러 수신자에게 보내는 통신을 구분하여 키를 사용한다.

② O: IEEE 802.11i는 데이터의 기밀성과 무결성을 보호하기 위해 TKIP와 CCMP를 지원한다. TKIP는 기존 WEP 장비의 취약점을 보완하도록 설계되었으며 RC4를 사용한다. CCMP는 **AES 기반**으로 암호화와 메시지 무결성 검증을 수행한다.

③ X: IEEE 802.11i의 보호 범위는 **데이터 링크 계층의 무선 구간**이다. 기반시설 모드에서는 단말과 해당 AP 사이를 보호한다. 예를 들어 무선 단말이 AP를 거쳐 유선망의 서버에 접속하더라도, 무선 구간의 보호가 AP 이후 서버까지 자동으로 이어지지는 않는다. 따라서 '서로 다른 유무선랜 영역에 속한 단말들의 종단간 보안'이 아니라 '무선 링크의 보안'으로 고쳐야 한다.

④ O: IEEE 802.1X의 포트 기반 접근 제어 체계에서 **상호 인증을 지원하는 EAP 방식**을 이용하면 무선 단말과 인증 서버가 서로의 신원을 확인할 수 있다. 이때 AP는 인증자 역할을 하며 단말과 인증 서버 사이의 인증 메시지를 중계한다.

NoteBase

문 11. SSL(Secure Socket Layer)에서 메시지에 대한 기밀성을 제공하기 위해 사용되는 것은?

① MAC(Message Authentication Code)

② 대칭키 암호 알고리즘

③ 해시 함수

④ 전자서명

정답 2번

간단한 해설

SSL은 전송할 메시지를 **대칭키 암호 알고리즘으로 암호화**하여, 비밀키를 모르는 제삼자가 내용을 읽지 못하도록 한다. 이것이 메시지의 기밀성을 제공하는 방식이다.

공통 해설

기밀성은 허가받지 않은 사람이 메시지 내용을 알 수 없도록 하는 성질이다. SSL에서는 핸드셰이크를 통해 마련한 비밀키를 이용하여 전송 데이터를 **대칭키 암호 알고리즘으로 암호화**한다. 송신자가 평문을 암호문으로 바꾸어 보내면 수신자는 같은 비밀키로 복호화하여 원문을 얻는다. 따라서 메시지 내용을 숨기는 데 직접 사용되는 수단은 대칭키 암호 알고리즘이다.

MAC·해시 함수·전자서명은 메시지의 검증에 사용할 값을 만들지만, **그 자체로 메시지 내용을 숨기지는 않는다**. 원문에 이러한 검증값만 덧붙여 전송하면 원문은 여전히 읽을 수 있으므로, 이들만으로는 문제에서 요구하는 기밀성이 제공되지 않는다.

NoteBase

문 12. 메시지 인증에 사용되는 해시 함수의 요건으로 옳지 않은 것은?

① 임의 크기의 메시지에 적용될 수 있어야 한다.

② 해시를 생성하는 계산이 비교적 쉬워야 한다.

③ 다양한 길이의 출력을 생성할 수 있어야 한다.

④ 하드웨어 및 소프트웨어에 모두 실용적이어야 한다.

정답 3번

간단한 해설

③의 '다양한 길이의 출력'은 **고정 길이의 출력**으로 고쳐야 한다. 이 문항에서 다루는 해시 함수는 입력 메시지의 길이가 달라도 일정한 길이의 해시값을 생성한다.

선지별 해설

① O: 메시지는 짧은 문자열부터 긴 문서까지 크기가 다양하므로, 해시 함수는 **입력 길이가 서로 다른 메시지**를 처리할 수 있어야 한다. 입력의 길이가 출력 해시값의 길이와 같을 필요는 없다.

② O: 송신 측에서 해시값을 만들고 수신 측에서도 이를 다시 계산해야 하므로, **해시값을 구하는 계산은 효율적**이어야 한다. 이는 해시값으로부터 원래 메시지를 찾아내는 계산이 쉬워야 한다는 뜻은 아니다.

③ X: 이 문항에서 다루는 해시 함수는 메시지의 길이에 관계없이 **고정된 길이의 해시값**을 출력한다. 따라서 '다양한 길이의 출력을 생성'한다는 설명은 '고정된 길이의 출력을 생성'하는 것으로 고쳐야 한다. 예를 들어 SHA-256은 짧은 메시지와 긴 메시지 모두에서 256비트의 해시값을 생성한다.

④ O: 실제 시스템에서 사용할 수 있도록 **하드웨어와 소프트웨어 모두에서 효율적으로 구현**할 수 있어야 한다. 계산에 지나치게 많은 시간이나 자원이 필요하면 메시지 인증 과정에서 반복적으로 사용하기 어렵다.

NoteBase

문 13. 사용자 A가 사용자 B에게 보낼 메시지 M을 공개키 기반의 전자서명을 적용하여 메시지의 무결성을 검증하도록 하였다. A가 보낸 서명이 포함된 전송 메시지를 다음 표기법에 따라 바르게 표현한 것은?

PUx: X의 공개키
PRx: X의 개인키
E(K,M): 메시지 M을 키 K로 암호화
H(M): 메시지 M의 해시
// : 두 메시지의 연결

① $E(PU_B, M)$
② $E(PR_A, M)$
③ $M \| E(PU_B, H(M))$
④ $M \| E(PR_A, H(M))$

정답 4번

간단한 해설

문제의 표기법에서는 메시지의 **해시값을 송신자 A의 개인키로 서명**하고, 그 서명을 원문과 함께 전송한다. B는 A의 공개키로 서명을 검증하여 메시지의 무결성을 확인한다.

구성 요소별 해설

해시값: 먼저 원문 M의 해시값 $H(M)$을 구한다. 해시값은 메시지의 내용을 요약한 값으로, 전자서명에서는 **원문 전체 대신 해시값**을 서명 대상으로 삼는다.

서명: 서명을 만드는 사람은 A이므로 **A의 개인키** PR_A를 사용한다. 문제의 표기법에 따라 해시값에 서명한 결과는 $E(PR_A, H(M))$이다. 수신자 B의 공개키 PU_B로 암호화하는 것은 B만 복호화하도록 하는 기밀성 보호에 해당하며, A의 서명을 만드는 연산이 아니다.

전송 메시지: 원문 M에 서명을 연결하므로 $M \| E(PR_A, H(M))$이 되며, 이는 ④의 표현이다. B는 수신한 원문에서 해시값을 다시 계산하고, **A의 공개키로 서명이 그 해시값에 대해 유효한지** 검증한다. 원문이 변조되어 해시값이 달라지면 기존 서명은 검증에 실패하므로 무결성을 확인할 수 있다.

NoteBase

문 14. 대칭키 블록 암호 알고리즘의 운영 모드 중에서 한 평문 블록의 오류가 다른 평문 블록의 암호 결과에 영향을 미치는 오류 전이(error propagation)가 발생하지 않는 모드만을 묶은 것은? (단, ECB: Electronic Code Book, CBC: Cipher Block Chaining, CFB: Cipher Feedback, OFB: Output Feedback)

① CFB, OFB

② ECB, OFB

③ CBC, CFB

④ ECB, CBC

정답 2번

간단한 해설

ECB는 각 평문 블록을 **독립적으로 암호화**하고, OFB는 **평문과 무관하게 생성한 키 스트림**을 사용한다. 따라서 한 평문 블록에 오류가 있어도 다른 평문 블록의 암호화 결과에는 영향을 주지 않는다.

구성 요소별 해설

이 문항은 암호화 전 평문에 생긴 오류가 다른 평문 블록의 암호화 결과까지 바꾸는지를 묻는다.

ECB: 각 평문 블록에 블록 암호를 독립적으로 적용한다. 앞 블록의 평문이나 암호문을 다음 블록의 암호화에 사용하지 않으므로, 평문 오류는 **해당 블록의 암호문에만 영향**을 미친다.

CBC: 현재 평문 블록과 직전 암호문 블록을 XOR한 뒤 암호화한다. 첫 블록에는 직전 암호문 대신 초기화 벡터(IV)를 사용한다. 한 평문 블록이 바뀌면 그 암호문도 바뀌고, **바뀐 암호문이 다음 블록의 입력에 포함**되므로 오류의 영향이 이후 암호화 결과로 전파된다.

CFB: IV 또는 이전 암호문이 반영된 값을 블록 암호로 처리하고, 그 출력의 필요한 부분을 평문과 XOR하여 암호문을 만든다. 이때 **생성한 암호문을 다음 처리에 되먹임**하므로, 평문 오류로 암호문이 달라지면 이후 평문의 암호화에도 영향을 줄 수 있다.

OFB: IV를 암호화한 출력을 다시 암호화하는 과정을 반복하여 키 스트림을 만들고, 이를 평문과 XOR한다. 되먹임되는 것은 평문과 XOR하기 전의 출력이므로 **키 스트림 생성에 평문이나 암호문이 관여하지 않는다**. 평문의 한 비트가 바뀌어도 대응하는 암호문 비트만 바뀌고 다른 블록에는 전파되지 않는다.

따라서 오류 전이가 발생하지 않는 모드의 조합은 ECB와 OFB이며, ②의 조합과 일치한다.

NoteBase

문 15. 유닉스/리눅스 시스템의 로그 파일에 기록되는 정보에 대한 설명으로 옳지 않은 것은?

① utmp - 로그인, 로그아웃 등 현재 시스템 사용자의 계정 정보

② loginlog - 성공한 로그인에 대한 내용

③ pacct - 시스템에 로그인한 모든 사용자가 수행한 프로그램 정보

④ btmp - 실패한 로그인 시도

정답 2번

간단한 해설

loginlog는 성공한 로그인이 아니라 **실패한 로그인 시도**를 기록하는 파일이다. 따라서 '성공한 로그인에 대한 내용'은 '실패한 로그인에 대한 내용'으로 고쳐야 한다.

선지별 해설

① O: utmp는 **현재 시스템을 사용하는 사용자의 접속 상태**를 관리한다. 사용자명, 접속 단말, 로그인 시각 등이 들어 있으며 로그인과 로그아웃에 따라 기록이 갱신된다. 과거의 로그인·로그아웃 이력을 누적하는 wtmp와는 구별된다.

② X: Solaris의 loginlog는 **로그인 실패 내역**을 기록한다. 기록 기능이 활성화된 상태에서 연속 실패가 설정된 횟수에 이르면 실패한 시도의 사용자명, 단말, 시각 등을 남긴다. 따라서 '성공한 로그인'을 '실패한 로그인'으로 고쳐야 한다.

③ O: pacct는 사용자가 수행한 프로그램의 실행 정보를 남기는 프로세스 회계 파일이다. **프로세스 회계 기능이 활성화되어 있으면** 각 프로세스가 종료될 때 실행 명령명, 사용자 ID, CPU 사용 시간 등이 기록된다. 누가 접속했는지를 나타내는 접속 기록과 달리, 어떤 프로그램을 수행했는지를 확인하는 자료이다.

④ O: 리눅스의 btmp에는 **실패한 로그인 시도**가 기록되며, lastb 명령으로 조회할 수 있다. loginlog와 btmp는 모두 로그인 실패를 다루지만, 대표적으로 사용되는 운영체제와 기록 방식이 다르다.

NoteBase

문 16. 「개인정보 보호법」상 개인정보처리자가 개인정보가 유출되었음을 알게 되었을 때에 지체 없이 해당 정보주체에게 알려야 할 사항에 해당하지 않는 것은?

① 유출된 개인정보의 항목

② 유출된 시점과 그 경위

③ 조치 결과를 행정안전부장관 또는 대통령령으로 정하는 전문기관에 신고한 사실

④ 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

정답 3번

간단한 해설

③의 '기관에 신고한 사실'은 **정보주체에게 알려야 할 법정 통지사항이 아니다**. 유출 내용과 피해 대응 방법 등을 정보주체에게 알리는 통지의무와, 일정 규모 이상의 유출에 대해 관계 기관에 통지·조치 결과를 알리는 신고의무는 구분된다.

선지별 해설

구 「개인정보 보호법」 제34조제1항은 개인정보처리자가 개인정보 유출을 알게 되면 지체 없이 해당 정보주체에게 유출 내용과 피해 대응에 필요한 사항을 알리도록 규정한다.

① O: 구 「개인정보 보호법」 제34조제1항제1호는 **유출된 개인정보의 항목**을 통지사항으로 정한다. 정보주체가 자신의 어떤 정보가 유출되었는지 파악할 수 있도록 알려야 한다.

② O: 같은 항 제2호에 따라 **유출된 시점과 그 경위**를 알려야 한다. 유출이 언제, 어떤 과정으로 발생했는지에 관한 정보이다.

③ X: 구법 제34조제3항은 대통령령으로 정한 규모 이상의 개인정보가 유출되면 통지 및 조치 결과를 지체 없이 행정안전부장관 또는 대통령령으로 정하는 전문기관에 신고하도록 규정하였다. 이는 **관계 기관에 대한 신고의무**이며, 신고했다는 사실 자체가 정보주체에게 알려야 할 법정 통지사항은 아니다. 정보주체에게는 같은 조 제1항제4호의 **개인정보처리자의 대응조치 및 피해 구제절차** 등을 알려야 한다.

④ O: 같은 조 제1항제5호에 따라 피해가 발생한 경우 신고 등을 접수할 수 있는 **담당부서 및 연락처**를 알려야 한다. 정보주체가 피해를 신고하고 구제를 요청할 창구를 알 수 있도록 하기 위한 사항이다.

NoteBase

문 17. 인증서를 발행하는 인증기관, 인증서를 보관하고 있는 저장소, 공개키를 등록하거나 등록된 키를 다운받는 사용자로 구성되는 PKI(Public Key Infrastructure)에 대한 설명으로 옳지 않은 것은?

① 인증기관이 사용자의 키 쌍을 생성할 경우, 인증기관은 사용자의 개인키를 사용자에게 안전하게 보내는 일을 할 필요가 있다.

② 사용자의 공개키에 대해 인증기관이 전자서명을 해서 인증서를 생성한다.

③ 사용자의 인증서 폐기 요청에 대하여 인증기관은 해당 인증서를 저장소에서 삭제함으로써 인증서의 폐기 처리를 완료한다.

④ 한 인증기관의 공개키를 다른 인증기관이 검증하는 일이 발생할 수 있다.

정답 3번

간단한 해설

인증서 폐기는 **저장소에서 삭제하는 것만으로 완료되지 않는다**. 이미 배포된 인증서를 더 이상 신뢰하지 않도록 **인증서 폐기 목록(CRL)** 등을 통해 폐기 사실을 알려야 한다.

선지별 해설

① O: 인증기관이 사용자의 공개키·개인키 쌍을 대신 생성했다면, 사용자가 개인키를 사용할 수 있도록 전달해야 한다. 개인키가 유출되면 타인이 사용자를 사칭하거나 암호문을 복호화할 수 있으므로, **개인키의 기밀성을 보장하는 안전한 전달**이 필요하다.

② O: 인증서는 사용자의 신원과 공개키의 연결을 인증기관이 보증하는 전자문서이다. 인증기관은 사용자의 공개키와 신원 정보 등이 포함된 인증서 내용에 **인증기관 자신의 개인키로 전자서명**한다. 이용자는 인증기관의 공개키로 이 서명을 검증하여 인증서의 발급 주체와 내용의 변조 여부를 확인한다.

③ X: 저장소에서 인증서를 삭제해도 다른 사용자가 이미 내려받은 사본까지 없어지지는 않는다. 따라서 **단순 삭제가 아니라 폐기 사실의 공지**가 필요하다. 대표적으로 인증서 폐기 목록(CRL)에 해당 인증서의 일련번호와 폐기 시각 등을 기록하여 공개하고, 이용자는 이를 확인해 인증서를 계속 신뢰할 수 있는지 판단한다.

④ O: 인증기관의 공개키도 그 소유자가 해당 인증기관인지 확인할 필요가 있다. **교차인증**에서는 한 인증기관이 다른 인증기관의 공개키를 인증하는 인증서를 발급할 수 있다. 이를 통해 서로 다른 인증기관 사이에 신뢰 관계를 연결한다.

NoteBase

문 18. 암호학적으로 안전한 의사(pseudo) 난수 생성기에 대한 설명으로 옳은 것은?

① 생성된 수열의 비트는 정규분포를 따라야 한다.

② 생성된 수열의 어느 부분 수열도 다른 부분 수열로부터 추정될 수 없어야 한다.

③ 시드(seed)라고 불리는 입력 값은 외부에 알려져도 무방하다.

④ 비결정적(non-deterministic) 알고리즘을 사용하여 재현 불가능한 수열을 생성해야 한다.

정답 2번

간단한 해설

암호학적으로 안전한 의사난수는 수열의 일부가 알려져도 **다른 부분을 예측하기 어려워야 한다**. 여기서 예측 불가능하다는 것은 현실적인 계산 자원으로 우연한 추측보다 유의미하게 높은 확률로 알아낼 수 없다는 뜻이다.

선지별 해설

① X: 비트에 요구되는 것은 정규분포가 아니라 **0과 1이 같은 확률로 나타나는 균등성**이다. 정규분포는 평균을 중심으로 종 모양을 이루는 연속확률분포이므로 개별 비트의 분포 조건과 다르다. 다만 유한한 출력에서 0과 1의 개수가 항상 정확히 같아야 한다는 뜻은 아니다.

② O: 암호학적으로 안전한 의사난수는 **출력 일부로부터 다른 부분을 예측하기 어려워야 한다**. 예를 들어 앞부분의 비트를 관찰했더라도 다음 비트를 우연한 추측보다 유의미하게 높은 확률로 알아내기 어려워야 한다. 이는 추측 자체가 불가능하다는 뜻이 아니라, 현실적인 계산 자원으로 예측에 유용한 규칙을 찾아낼 수 없어야 한다는 뜻이다.

③ X: 시드는 의사난수 생성기의 초기 상태를 결정하는 입력이므로 **외부에 노출되지 않도록 보호해야 한다**. 시드가 알려지면 공격자가 같은 알고리즘을 실행하여 출력 수열을 재현하거나 예측할 수 있기 때문이다. 시드는 비밀로 유지할 뿐 아니라 공격자가 쉽게 추측할 수 없도록 충분한 무작위성도 갖추어야 한다.

④ X: 의사난수 생성기는 시드를 바탕으로 **결정적 알고리즘**을 실행하여 수열을 만든다. 따라서 동일한 시드와 동일한 동작 조건에서는 같은 수열을 재현할 수 있다. 비결정적 물리 현상 등을 이용해 난수를 얻는 방식과 구별되며, 암호학적 안전성은 재현 자체의 불가능성이 아니라 시드를 모르는 공격자의 예측이 어렵다는 데 있다.

NoteBase

문 19. 사용자 워크스테이션의 클라이언트, 인증서버(AS), 티켓발행서버(TGS), 응용서버로 구성되는 Kerberos에 대한 설명으로 옳은 것은? (단, Kerberos 버전 4를 기준으로 한다)

① 클라이언트는 AS에게 사용자의 ID와 패스워드를 평문으로 보내어 인증을 요청한다.

② AS는 클라이언트가 TGS에 접속하는 데 필요한 세션키와 TGS에 제시할 티켓을 암호화하여 반송한다.

③ 클라이언트가 응용서버에 접속하기 전에 TGS를 통해 발급받은 티켓은 재사용될 수 없다.

④ 클라이언트가 응용서버에게 제시할 티켓은 AS와 응용서버의 공유 비밀키로 암호화되어 있다.

정답 2번

간단한 해설

AS는 클라이언트와 TGS가 사용할 **세션키와 티켓발급티켓(TGT)**을 클라이언트에게 암호화하여 보낸다. 클라이언트는 이를 이용해 패스워드를 다시 보내지 않고 TGS에 응용서버용 티켓을 요청할 수 있다.

선지별 해설

① X: Kerberos 버전 4에서는 인증 요청에 사용자 ID 등을 보내지만, **패스워드 자체는 전송하지 않는다**. 패스워드는 클라이언트에서 키를 유도하여 AS가 보낸 암호화 응답을 복호화하는 데 사용한다. 따라서 ID와 패스워드를 함께 평문으로 보낸다는 설명은 잘못이다.

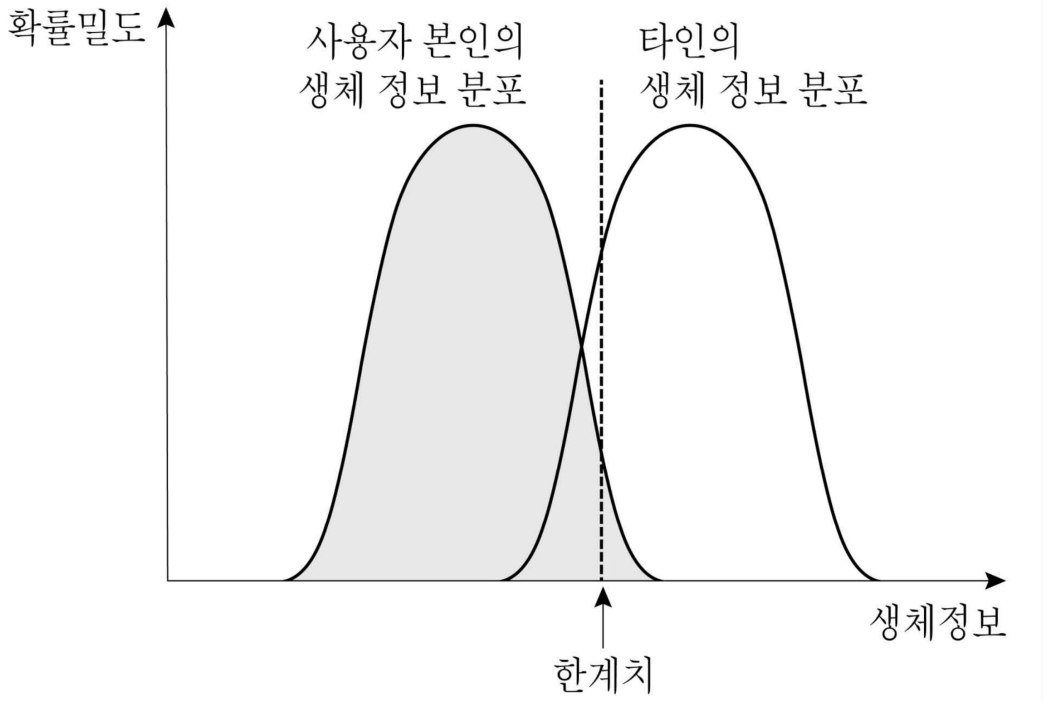
② O: AS는 클라이언트와 TGS 사이에서 사용할 세션키를 생성하고, TGS에 제시할 티켓발급티켓(TGT)을 발급한다. TGT 자체는 AS와 TGS가 공유하는 비밀키로 암호화하며, **세션키와 TGT를 포함한 응답**은 사용자의 패스워드에서 유도한 키로 암호화하여 클라이언트에게 보낸다. 클라이언트는 응답을 복호화하여 세션키를 얻고, TGT는 암호화된 상태로 TGS에 전달한다.

③ X: TGS가 발급한 응용서버용 티켓은 **유효기간 안에서 같은 클라이언트가 해당 응용서버에 반복하여 사용**할 수 있다. 다만 티켓과 함께 제시하는 인증자는 요청할 때마다 새로 생성한다. 인증자에는 시각 정보 등이 포함되므로, 티켓을 재사용하는 것과 과거의 인증 요청을 그대로 재전송하는 것은 구별된다.

④ X: 응용서버용 티켓은 TGS가 발급하며, **TGS와 응용서버가 공유하는 응용서버의 장기 비밀키**로 암호화한다. 응용서버는 자신의 키로 티켓을 복호화하여 클라이언트 정보와 클라이언트·응용서버 간 세션키를 얻는다. 따라서 이 단계의 티켓 암호화 키를 AS와 응용서버 사이의 공유키로 설명한 부분을 고쳐야 한다.

NoteBase

문 20. 생체 인식 시스템은 저장되어 있는 개인의 물리적 특성을 나타내는 생체 정보 집합과 입력된 생체 정보를 비교하여 일치 정도를 판단한다. 다음 그림은 사용자 본인의 생체 정보 분포와 공격자를 포함한 타인의 생체 정보 분포, 그리고 본인 여부를 판정하기 위한 한계치를 나타낸 것이다. 그림 및 생체 인식 응용에 대한 설명으로 옳은 것만을 고른 것은?



ㄱ. 타인을 본인으로 오인하는 허위 일치의 비율(false match rate, false acceptance rate)이 본인을 인식하지 못하고 거부하는 허위 불일치의 비율(false non-match rate, false rejection rate)보다 크다.
ㄴ. 한계치를 우측으로 이동시키면 보안성은 강화되지만 사용자 편리성은 저하된다.
ㄷ. 보안성이 높은 응용프로그램은 낮은 허위 일치 비율을 요구한다.
ㄹ. 가능한 용의자를 찾는 범죄학 응용프로그램의 경우 낮은 허위 일치 비율이 요구된다.

① ㄱ, ㄷ
② ㄱ, ㄹ
③ ㄴ, ㄷ
④ ㄴ, ㄹ

정답 1번

간단한 해설

그림에서 타인 분포의 한계치 왼쪽 면적이 본인 분포의 한계치 오른쪽 면적보다 커 **허위 일치 비율이 더 높다**.
높은 보안성이 필요한 경우에는 타인을 본인으로 받아들이지 않도록 **허위 일치 비율을 낮춰야 한다**.

NoteBase

보기별 해설

그림은 본인의 생체 정보 분포가 왼쪽, 타인의 분포가 오른쪽에 있다. 한계치 왼쪽을 본인으로 받아들이고 오른쪽을 거부하는 영역으로 읽는다. 세로축이 확률밀도이므로 오류 비율은 곡선의 특정 지점 높이가 아니라 해당 영역의 면적으로 판단한다.

ㄱ. O: 허위 일치 비율은 타인을 본인으로 받아들이는 비율로, 타인 분포에서 한계치 왼쪽 면적에 해당한다. 허위 불일치 비율은 본인을 거부하는 비율로, 본인 분포에서 한계치 오른쪽 면적에 해당한다. 그림에서는 **타인 분포의 한계치 왼쪽 면적이 더 크므로** 허위 일치 비율이 허위 불일치 비율보다 크다.

ㄴ. X: 한계치를 오른쪽으로 이동시키면 **본인으로 받아들이는 영역이 넓어진다**. 타인까지 받아들이는 허위 일치 비율은 증가하고, 본인을 거부하는 허위 불일치 비율은 감소한다. 따라서 이 그림에서는 보안성이 낮아지고 사용자 편리성은 높아진다. 보안성을 강화하려면 한계치를 왼쪽으로 이동시켜야 하며, 이때 본인이 거부되는 불편이 늘어난다.

ㄷ. O: 허위 일치는 공격자를 포함한 타인이 본인으로 인증되는 오류이다. 보안성이 높은 응용프로그램은 **타인의 부정한 인증 성공을 억제**해야 하므로 낮은 허위 일치 비율을 요구한다.

ㄹ. X: 가능한 용의자를 찾는 후보 검색 단계에서는 실제 대상이 후보에서 빠지는 오류를 줄이는 것이 중요하다. 따라서 우선 요구되는 것은 **낮은 허위 불일치 비율**이다. 허위 일치만 줄이려고 판정 기준을 엄격하게 하면 실제 대상까지 후보에서 제외될 수 있다. 검색된 후보는 추가 확인을 거쳐야 하므로 후보에 포함되었다는 사실만으로 범인이라고 확정하지 않는다.

옳은 보기는 ㄱ, ㄷ이며, 이 조합은 ①에 해당한다.

NoteBase