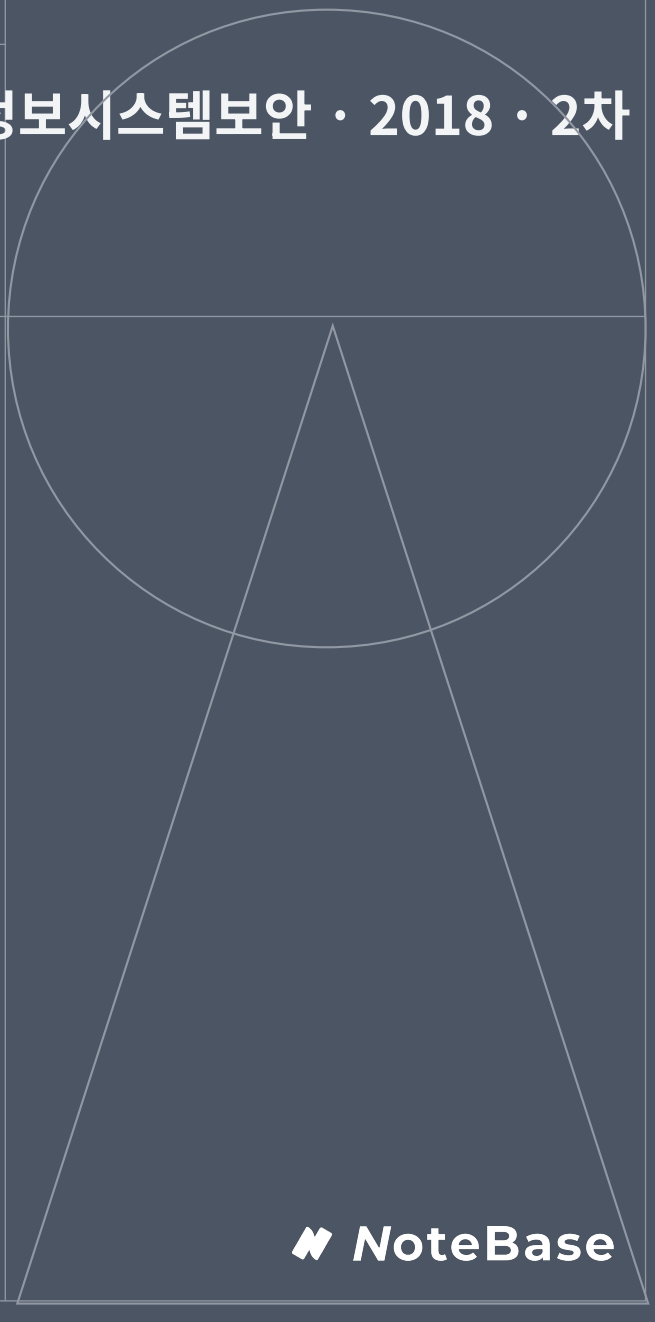
기출OX 해설집

공무원/해경/일반직 9급 · 정보시스템보안 · 2018 · 2차



NoteBase

기출OX 해설집

공무원/해경/일반직 9급 · 정보시스템보안 · 2018 · 2차

공무원/해경/일반직 9급 · 정보시스템보안 · 2018 · 2차

문 1. OECD(경제협력개발기구) 개인정보보안 8원칙 중 정보 정확성 원칙의 구성 요소가 아닌 것은?

① 정확성
② 책임성
③ 완전성
④ 최신성

정답 2번

출제 포인트

OECD 개인정보보호 8원칙 중 정보 정확성 원칙의 구성 요소와 별도의 원칙인 책임성 원칙을 구별하는 문제이다.

핵심 개념

정보 정확성 원칙은 이용 목적에 비추어 개인정보가 정확하고 완전하며 최신 상태로 유지되어야 한다는 원칙이다.
책임성 원칙은 개인정보처리자가 개인정보보호 원칙을 준수할 책임을 진다는 별도의 원칙이다.
따라서 정보 정확성 원칙의 핵심 구성 요소는 정확성·완전성·최신성이다.

선지별 해설

① O — 정확성은 개인정보가 사실과 일치하고 오류가 없어야 한다는 정보 정확성 원칙의 구성 요소이다.
② X — 책임성은 정보 정확성 원칙의 구성 요소가 아니다. 틀린 연결은 '책임성 → 정보 정확성의 구성 요소'이며, 올바르게는 책임성은 개인정보처리자가 원칙 준수의 책임을 지는 별도의 개인정보보호 원칙이다.
③ O — 완전성은 이용 목적에 필요한 정보가 빠짐없이 갖추어져야 한다는 정보 정확성 원칙의 구성 요소이다.
④ O — 최신성은 개인정보가 현재 상태에 맞도록 갱신되어야 한다는 정보 정확성 원칙의 구성 요소이다.

오답 포인트

'책임성'도 OECD 개인정보보호 8원칙에 포함되므로 정보 정확성 원칙의 세부 요소로 착각하기 쉽다. 그러나 정확성·완전성·최신성은 정보의 품질을 설명하고, 책임성은 개인정보처리자의 준수 책임을 설명한다.

NoteBase

다시 나오면 이렇게 판단

정보 자체의 품질을 나타내는 정확성·완전성·최신성은 정보 정확성 원칙으로 묶고, 처리 주체가 원칙 준수의 책임을 진다는 내용은 책임성 원칙으로 구별한다.

암기 포인트

정보 정확성은 '정·완·최', 책임성은 별도 원칙이다.

NoteBase

문 2. 정보보호에 대한 설명과 용어가 바르게 짝지어진 것은?

ㄱ. 자산의 손실을 초래할 수 있는 원하지 않는 사건의 잠재적인 원인이나 행위자
ㄴ. 원하지 않는 사건이 발생하여 손실 또는 부정적인 영향을 미칠 가능성
ㄷ. 자신의 잠재적인 속성으로 위협의 이용 대상이 되는 것
ㄹ. 정보자산에 피해를 주는 주체

① ㄱ: 위협, ㄴ: 취약점, ㄷ: 위험, ㄹ: 위협원
② ㄱ: 위협, ㄴ: 위험, ㄷ: 취약점, ㄹ: 자산
③ ㄱ: 취약점, ㄴ: 위험, ㄷ: 위협, ㄹ: 노출
④ ㄱ: 위협, ㄴ: 위험, ㄷ: 취약점, ㄹ: 위협원

정답 4번

출제 포인트

정보보호의 핵심 용어인 위협, 위험, 취약점, 위협원을 정의의 결정적 표현으로 구별하는 문제이다.

핵심 개념

위협: 자산에 손실을 일으킬 수 있는 원하지 않는 사건의 잠재적 원인이나 행위이다.
위험: 위협으로 인해 원하지 않는 사건과 손실이 발생할 가능성이다.
취약점: 위협에 의해 이용될 수 있는 자산이나 보호대책의 약점이다.
위협원: 정보자산에 피해를 주는 주체 또는 위협을 발생시키는 근원이다.
따라서 잠재적 원인·행위는 위협, 발생 가능성은 위험, 이용 대상이 되는 약점은 취약점, 피해를 주는 주체는 위협원으로 구별된다.

선지별 해설

① X — ㄱ을 위협, ㄹ을 위협원으로 짝지은 것은 맞지만, ㄴ과 ㄷ을 서로 바꾸어 놓았다. ㄴ은 취약점이 아니라 위험이고, ㄷ은 위험이 아니라 취약점이다. 올바르게는 'ㄱ: 위협, ㄴ: 위험, ㄷ: 취약점, ㄹ: 위협원'이다.
② X — ㄱ·ㄴ·ㄷ의 연결은 맞지만, ㄹ의 '자산'이 틀렸다. 정보자산에 피해를 주는 주체는 자산이 아니라 위협원이다. 올바르게는 'ㄱ: 위협, ㄴ: 위험, ㄷ: 취약점, ㄹ: 위협원'이다.
③ X — ㄴ을 위험으로 연결한 것만 맞고 ㄱ·ㄷ·ㄹ이 틀렸다. ㄱ은 취약점이 아니라 위협, ㄷ은 위협이 아니라 취약점, ㄹ은 노출이 아니라 위협원이다. 올바르게는 'ㄱ: 위협, ㄴ: 위험, ㄷ: 취약점, ㄹ: 위협원'이다.
④ O — 잠재적인 원인이나 행위자는 위협, 손실 발생 가능성은 위험, 위협의 이용 대상이 되는 약점은 취약점, 피해를 주는 주체는 위협원이므로 모든 연결이 맞다.

NoteBase

오답 포인트

①은 위험과 취약점을 맞바꾸어 혼동하게 하고, ②는 피해를 받는 대상인 자산과 피해를 주는 주체인 위협원을 혼동하게 한다. '가능성'과 '약점', '대상'과 '주체'를 구분하는 것이 핵심이다.

다시 나오면 이렇게 판단

정의에서 '원인·행위'가 보이면 위협, '발생 가능성'이면 위험, '이용되는 약점'이면 취약점, '피해를 주는 주체'이면 위협원으로 판단한다.

암기 포인트

위협은 원인, 위험은 가능성, 취약점은 약점, 위협원은 주체이다.

NoteBase

문 3. 중앙집중식 인증 방식인 커버로스(Kerberos)에 대한 다음 설명 중 옳지 않는 것은?

① 커버로스는 시스템을 통해 패스워드를 평문 형태로 전송한다.

② 커버로스는 네트워크 응용 프로그램이 상대방의 신분을 식별할 수 있게 한다.

③ 커버로스 방식에서는 대칭키 암호화 방식을 사용하여 세션을 통신한다.

④ Needham-Schroeder 프로토콜을 기반으로 만들어졌다.

정답 1번

출제 포인트

커버로스가 패스워드 대신 티켓과 세션 키를 이용해 신원을 인증한다는 점을 묻는 문제이다.

핵심 개념

커버로스는 신뢰할 수 있는 제3자인 키 분배 센터를 중심으로 동작하는 네트워크 인증 프로토콜이다.
클라이언트는 패스워드를 네트워크로 직접 보내지 않고, 암호화된 티켓과 세션 키를 이용하여 서버에 자신의 신원을 증명한다.

선지별 해설

① X
틀린 표현은 '패스워드를 평문 형태로 전송한다'이다. 커버로스는 패스워드를 네트워크로 전송하지 않으며, 패스워드에서 얻은 키로 인증 과정의 정보를 처리하고 티켓과 세션 키를 사용한다.

② O
커버로스는 네트워크 환경에서 클라이언트와 서버가 상대방의 신원을 확인할 수 있도록 인증 기능을 제공한다.

③ O
커버로스는 대칭키 암호 방식을 사용하며, 인증 서버가 발급한 세션 키로 클라이언트와 서비스 서버 사이의 인증 및 세션 통신을 지원한다.

④ O
커버로스는 신뢰할 수 있는 제3자가 통신 당사자에게 세션 키를 분배하는 Needham-Schroeder 대칭키 인증 프로토콜을 바탕으로 설계되었다.

NoteBase

오답 포인트

①의 '평문 전송'은 중앙 인증 서버가 패스워드를 직접 받아 확인한다고 오해하게 만드는 표현이다. 중앙집중식 인증이라는 말은 인증 기능이 중앙에 모여 있다는 뜻이지, 패스워드를 네트워크로 보내는 방식이라는 뜻이 아니다.

다시 나오면 이렇게 판단

커버로스 선지는 '패스워드 직접 전송 없음, 티켓 사용, 대칭키 기반, 신뢰할 수 있는 제3자'의 네 기준으로 판단한다. 패스워드를 평문으로 전송한다고 하면 틀린 설명이다.

암기 포인트

커버로스는 패스워드가 아니라 티켓과 세션 키로 인증한다.

NoteBase

문 4. UNIX 시스템에서 각 사용자가 로그인할 때마다 시스템에 의해 자동으로 실행되어야 하는 내용(PATH 변수, 프롬프트 지정 등)을 정의해 놓은 파일은?

① /etc/inittab

② /etc/inetd.conf

③ /etc/profile

④ /etc/rc.local

정답 3번

출제 포인트

이 문제는 UNIX의 시스템 부팅·서비스 설정 파일과 사용자 로그인 환경 설정 파일의 용도를 구별하는 문제이다.

핵심 개념

/etc/profile은 로그인 셸이 시작될 때 적용되는 시스템 공통 환경 설정 파일이다. PATH와 셸 프롬프트 등 사용자의 로그인 환경을 설정할 수 있다. 반면 /etc/inittab과 /etc/rc.local은 시스템 시작 과정에, /etc/inetd.conf는 네트워크 서비스 관리에 관련된다.

NoteBase

선지별 해설

① X
/etc/inittab은 전통적인 System V 계열 UNIX에서 init 프로세스가 시스템 초기화와 실행 수준별 프로세스를 관리하도록 정의하는 파일이다. 틀린 부분은 이를 사용자 로그인 환경 설정 파일로 본 점이며, 로그인 때 PATH와 프롬프트 등을 공통 설정하는 파일은 /etc/profile이다.

② X
/etc/inetd.conf는 inetd가 요청을 받아 실행할 네트워크 서비스와 해당 서버 프로그램 등을 정의하는 설정 파일이다. 틀린 부분은 이를 로그인 시 자동 실행되는 사용자 환경 설정 파일로 본 점이며, 해당 파일은 /etc/profile이다.

③ O
/etc/profile은 사용자가 로그인 셸을 시작할 때 읽혀 시스템 전체에 공통으로 적용할 PATH, 셸 프롬프트 등의 환경을 설정하는 파일이다.

④ X
/etc/rc.local은 전통적으로 시스템 부팅 과정의 마지막 단계에서 관리자가 지정한 명령을 실행하는 데 사용하는 파일이다. 틀린 부분은 실행 시점을 사용자 로그인 때로 본 점이며, 로그인 환경 설정에는 /etc/profile을 사용한다.

오답 포인트

함정은 모두 자동 실행이나 초기 설정과 관련된 파일처럼 보인다는 점이다. 문제의 핵심 표현은 '각 사용자가 로그인할 때'와 'PATH 변수, 프롬프트'이므로 시스템 부팅 파일이나 네트워크 서비스 파일이 아니라 로그인 셸 환경 파일을 골라야 한다.

다시 나오면 이렇게 판단

설정이 적용되는 시점을 먼저 구분한다. 시스템 부팅이면 /etc/inittab 또는 /etc/rc.local, inetd 기반 네트워크 서비스이면 /etc/inetd.conf, 로그인 셸의 공통 환경이면 /etc/profile로 판단한다.

암기 포인트

로그인 환경은 profile, 부팅은 inittab·rc.local, inetd 서비스는 inetd.conf이다.

NoteBase

문 5. 다음 중 SSL 프로토콜에 대한 설명으로 옳지 않은 것은?

① SSL이 적용되었다는 표시로 HTTPS라고 사용한다.

② 보안성과 무결성을 유지하기 위해 마지막에는 HMAC을 붙인다.

③ SSL/TLS를 시작하기 위한 최초의 교신은 암호화와 MAC 없이 시작한다.

④ 110번 포트를 주로 사용한다.

정답 4번

출제 포인트

SSL/TLS가 제공하는 보안 기능, 초기 핸드셰이크의 보호 상태, HTTPS의 기본 포트를 구분하는 문제이다.

핵심 개념

SSL/TLS는 응용 계층의 데이터를 전송 계층 위에서 암호화하고, 상대 인증과 무결성 검증을 제공하는 보안 프로토콜이다. HTTPS는 HTTP에 SSL/TLS를 적용한 통신이며 기본적으로 TCP 443번 포트를 사용한다. 반면 TCP 110번은 암호화되지 않은 POP3의 기본 포트이다.

선지별 해설

① O — HTTPS는 HTTP 통신을 SSL/TLS로 보호한다는 뜻이므로, 주소 체계에서 HTTPS는 SSL/TLS가 적용된 웹 통신을 나타낸다.
② O — 전통적인 SSL/TLS 레코드 보호에서는 전송 데이터에 키를 사용하는 MAC을 계산해 덧붙이고 이를 통해 변조 여부를 확인한다. TLS에서는 이 무결성 검증에 HMAC이 사용될 수 있다.
③ O — 최초의 ClientHello 등은 아직 암호 키와 MAC 비밀값이 합의되기 전이므로 암호화와 MAC 보호 없이 시작한다. 이후 핸드셰이크를 통해 키가 설정되면 보호된 통신으로 전환된다.
④ X — 틀린 표현은 '110번 포트를 주로 사용한다'이다. 110번은 POP3의 기본 포트이며, SSL/TLS가 적용된 HTTPS는 기본적으로 TCP 443번 포트를 사용한다.

오답 포인트

SSL/TLS 자체가 하나의 응용 서비스 포트에만 묶이는 것은 아니지만, 시험에서는 HTTPS의 기본 포트인 443번과 POP3의 기본 포트인 110번을 바꾸어 제시하는 함정을 자주 사용한다.

다시 나오면 이렇게 판단

프로토콜 설명 문제에서는 보안 기능과 포트 번호를 나누어 판단한다. SSL/TLS는 암호화·인증·무결성을 제공하고, HTTPS의 기본 포트는 443번이며, POP3의 기본 포트는 110번이다.

NoteBase

암기 포인트

HTTPS는 443, POP3는 110이다. 초기 Hello는 키 합의 전이라 평문으로 시작한다.

NoteBase

문 6. 다음 서버 보안용 취약점 점검 도구에 대한 설명으로 가장 올바르지 못한 것은?

① nmap - 실시간 트래픽 분석과 패킷 로깅이 가능하다.

② SATAN - 네트워크를 통해 리모트 시스템의 보안정도를 조사하고 그 자료를 데이터베이스에 저장한다.

③ Nessus - 유닉스 플랫폼에서 동작하며 클라이언트-서버 구조로 클라이언트의 취약점을 점검한다.

④ SAINT - 유닉스 플랫폼에서 동작하는 네트워크 취약점을 분석한다.

정답 1번

출제 포인트

서버·네트워크 취약점 점검 도구인 nmap, SATAN, Nessus, SAINT의 주된 기능과 동작 방식을 구별하는 문제이다.

핵심 개념

nmap: 네트워크의 호스트를 탐색하고 열린 포트, 서비스, 운영체제 등의 정보를 조사하는 스캐닝 도구이다.
SATAN: 원격 시스템의 보안 취약점을 네트워크를 통해 조사하고 분석 결과를 데이터베이스 형태로 관리하는 도구이다.
Nessus: 클라이언트-서버 구조를 사용하여 서버가 지정된 대상 시스템의 취약점을 검사하는 도구이다.
SAINT: 유닉스 계열 환경에서 네트워크상의 시스템과 서비스에 존재하는 취약점을 분석하는 도구이다.

선지별 해설

① X — nmap의 주된 기능은 호스트 탐색과 포트·서비스 스캔이다. 틀린 표현은 '실시간 트래픽 분석과 패킷 로깅'이며, 올바르게는 '네트워크 호스트와 열린 포트·서비스 등을 탐색한다'이다.
② O — SATAN은 네트워크를 통해 원격 시스템의 보안 상태와 취약점을 조사하고 그 분석 정보를 데이터베이스에 저장·관리한다.
③ O — Nessus는 유닉스 플랫폼에서 개발된 클라이언트-서버 방식의 취약점 점검 도구이다. 클라이언트가 검사를 지시하면 서버가 지정된 대상 시스템을 검사한다.
④ O — SAINT는 유닉스 계열 플랫폼에서 동작하며 네트워크에 연결된 시스템의 취약점을 분석하는 도구이다.

오답 포인트

①의 '실시간 트래픽 분석과 패킷 로깅'은 네트워크 스캐닝과 패킷 캡처·감시 기능을 바꾸어 놓은 표현이다. nmap은 패킷을 이용해 탐색과 스캔을 수행하지만, 그 사실만으로 실시간 트래픽 분석·로깅 도구가 되는 것은 아니다.

NoteBase

다시 나오면 이렇게 판단

도구 이름을 보면 먼저 핵심 동작을 대응시킨다. nmap은 호스트·포트 스캔, SATAN과 SAINT는 네트워크 취약점 분석, Nessus는 클라이언트-서버 방식의 취약점 점검으로 구분한다. 스캔과 패킷 캡처·로깅은 서로 다른 기능으로 판단한다.

암기 포인트

nmap은 맵을 그리듯 호스트와 포트를 찾고, SATAN·SAINT·Nessus는 취약점을 점검한다.

NoteBase

문 7. 다음은 정보보호의 목표와 개념에 관한 설명으로 가장 거리가 먼 것은?

① 정보보호는 정보처리 영역에 있어서 가용성, 기밀성, 무결성을 보장하는 데 있다.

② 가용성이란 승인 또는 허가받은 사람의 경우 언제든지 접근과 이용을 보장 받는 것이다.

③ 최근에는 정보보호영역에서 부인방지, 책임성, 진정성, 신뢰성의 중요성이 날로 커지고 있다.

④ 기밀성이란 승인 또는 허가 받지 아니한 사람이나 프로세스에 의한 데이터의 변경 또는 훼손을 방지하는 것이다.

정답 4번

출제 포인트

정보보호의 기본 목표인 기밀성·무결성·가용성의 정의와 확장된 보안 목표를 구별하는 문제이다.

핵심 개념

기밀성은 승인되지 않은 주체에게 정보가 공개되지 않도록 하는 성질이다. 무결성은 정보가 권한 없이 변경되거나 훼손되지 않도록 정확성과 완전성을 유지하는 성질이다. 가용성은 승인된 사용자가 필요할 때 정보와 시스템에 접근하여 이용할 수 있도록 하는 성질이다. 부인방지·책임성·진정성·신뢰성도 정보보호에서 중요하게 다루는 확장 목표이다.

선지별 해설

① O — 정보보호의 대표적인 기본 목표는 가용성, 기밀성, 무결성을 보장하는 것이며 이를 CIA 3요소라고 한다.
② O — 가용성은 승인되거나 허가받은 사용자가 필요할 때 정보와 시스템에 접근하여 이용할 수 있게 하는 성질이다.
③ O — 정보보호에서는 CIA 3요소 외에도 행위나 전송 사실을 부인하지 못하게 하는 부인방지, 행위의 책임 주체를 추적할 수 있게 하는 책임성, 대상이나 정보가 진짜임을 보장하는 진정성, 시스템이 기대한 대로 일관되게 동작하는 신뢰성이 중요하다.
④ X — 틀린 부분은 '기밀성이란'이다. 승인되지 않은 사람이나 프로세스에 의한 데이터의 변경 또는 훼손을 방지하는 것은 무결성의 설명이다. 기밀성은 승인되지 않은 주체에게 정보가 공개되거나 노출되는 것을 방지하는 성질이다.

오답 포인트

④는 '승인받지 않은 주체'라는 공통 표현을 이용해 기밀성과 무결성을 바꾸어 놓았다. 판단 대상이 정보의 공개·노출이면 기밀성이고, 정보의 변경·훼손이면 무결성이다.

NoteBase

다시 나오면 이렇게 판단

각 선지의 핵심 동사를 확인한다. 공개·노출 방지는 기밀성, 변경·훼손 방지는 무결성, 필요할 때 접근·이용 가능은 가용성으로 판단한다.

암기 포인트

기밀성은 보이지 않게, 무결성은 바뀌지 않게, 가용성은 필요할 때 쓰게 하는 성질이다.

NoteBase

문 8. 다음 보기의 암호 알고리즘 중 키의 길이와 라운드 수가 가장 적은 것을 고르시오?

보기) DES IDEA Rijndael SEED

① 키의 길이 : DES, 라운드 수 : Rijndael
② 키의 길이 : IDEA, 라운드 수 : DES
③ 키의 길이 : DES, 라운드 수 : SEED
④ 키의 길이 : DES, 라운드 수 : IDEA

정답 4번

출제 포인트

DES, IDEA, Rijndael, SEED의 키 길이와 라운드 수를 각각 비교하여 최솟값에 해당하는 알고리즘을 찾는 문제이다.

핵심 개념

DES는 64비트 키 중 패리티 비트 8개를 제외한 유효 키 길이가 56비트이고 16라운드를 사용한다.
IDEA는 128비트 키를 사용하며, 8개의 본 라운드 뒤에 출력 변환을 수행하므로 비교표에서는 통상 8라운드로 센다.
Rijndael은 128·192·256비트 키에 따라 10·12·14라운드를 사용한다.
SEED는 128비트 키와 16라운드를 사용한다.
따라서 키 길이가 가장 짧은 것은 DES이고, 라운드 수가 가장 적은 것은 IDEA이다.

NoteBase

선지별 해설

① X
키 길이의 최솟값을 DES로 고른 것은 맞지만, 라운드 수의 최솟값은 Rijndael이 아니라 IDEA이다. 틀린 표현은 ‘라운드 수: Rijndael’이며, 올바르게는 ‘라운드 수: IDEA’이다.

② X
키 길이는 IDEA의 128비트보다 DES의 유효 56비트가 더 짧고, 라운드 수도 DES의 16라운드보다 IDEA의 8라운드가 더 적다. ‘키의 길이: IDEA, 라운드 수: DES’는 모두 틀렸으며, 올바르게는 ‘키의 길이: DES, 라운드 수: IDEA’이다.

③ X
키 길이의 최솟값을 DES로 고른 것은 맞지만, SEED는 16라운드이므로 라운드 수가 가장 적지 않다. 틀린 표현은 ‘라운드 수: SEED’이며, 올바르게는 ‘라운드 수: IDEA’이다.

④ O
DES의 유효 키 길이 56비트가 가장 짧고, IDEA의 본 라운드 수 8회가 가장 적으므로 두 조건을 모두 충족한다.

오답 포인트

한 알고리즘에서 두 최솟값을 동시에 찾는 문제가 아니라 ‘키 길이’와 ‘라운드 수’를 별도로 비교하는 문제이다. 또한 DES의 키를 표면상 64비트로만 기억하면 유효 키 길이 56비트를 놓치기 쉽고, IDEA의 마지막 출력 변환을 별도의 완전한 라운드로 세면 판단이 흔들릴 수 있다.

다시 나오면 이렇게 판단

먼저 각 알고리즘의 키 길이만 비교하여 DES를 고르고, 그다음 라운드 수만 비교하여 IDEA를 고른다. 두 비교 결과를 결합하면 ‘DES－IDEA’가 된다.

암기 포인트

최소 키는 DES 56비트, 최소 라운드는 IDEA 8라운드이다.

NoteBase

문 9. 다음 중 디바이스 인증기술의 장점이 아닌 것은?

① 책임추적성

② 상호 연동성

③ 보안성

④ 경제성

정답 1번

출제 포인트

디바이스 인증기술의 직접적인 장점과 인증만으로 보장되지 않는 별도의 보안 속성을 구별하는 문제이다.

핵심 개념

디바이스 인증은 통신하거나 서비스에 접속하는 장치가 등록된 정당한 장치인지 확인하는 기술이다. 이를 통해 비인가 장치의 접근을 막아 보안성을 높이고, 표준화된 인증 방식으로 이기종 장치의 상호 연동을 지원하며, 인증·관리를 자동화하여 운영 비용을 줄일 수 있다. 반면 책임추적성은 어떤 주체가 어떤 행위를 했는지를 사후에 확인할 수 있는 성질로, 식별 정보와 감사 로그 등의 기록·관리 수단이 함께 갖추어져야 한다.

선지별 해설

① X — 책임추적성은 디바이스 인증기술 자체의 직접적인 장점으로 보기 어렵다. 인증은 장치의 정당성을 확인하지만, 행위의 주체와 내용을 사후에 추적하려면 감사 로그와 기록 관리가 추가로 필요하다. 올바르게는 '책임추적성은 인증 정보와 감사 기록 등을 결합해 확보하는 별도의 보안 속성이다'라고 표현한다.
② O — 상호 연동성은 서로 다른 디바이스나 서비스가 공통된 인증 체계를 통해 연결되고 인증 정보를 활용할 수 있게 하는 장점이다.
③ O — 보안성은 비인가 디바이스의 접속과 위장을 차단하고 정당한 디바이스만 접근하게 함으로써 향상된다.
④ O — 경제성은 인증 절차와 장치 관리를 표준화·자동화하여 중복 구축과 운영 부담을 줄일 수 있다는 장점이다.

오답 포인트

①의 '책임추적성'도 넓은 의미의 보안 목표이므로 인증의 장점처럼 보이기 쉽다. 그러나 장치의 신원을 확인하는 인증과, 행위자를 사후에 밝혀 책임을 귀속하는 추적·감사는 구별해야 한다.

다시 나오면 이렇게 판단

선지가 인증으로 직접 얻는 효과인지 판단한다. 정당한 장치 확인에 따른 보안성, 표준 기반의 상호 연동성, 관리 효율에 따른 경제성은 직접 효과이다. 사후 행위 추적처럼 별도의 로그·감사 체계가 필요한 속성은 인증 자체의 장점에서 제외한다.

NoteBase

암기 포인트

디바이스 인증의 장점은 보안성·상호 연동성·경제성이고, 책임추적성은 별도의 기록과 감사가 필요하다.

NoteBase

문 10. 다음 중 윈도우 운영체제의 IIS FTP 서버 설정에서 지정할 사항으로 가장 부적절한 것은?

① 운영 포트 변경 및 연결 시간의 제한

② Active/Passive 모드 지원여부

③ 보안계정 사용 및 익명 연결 허용 여부

④ 가상 디렉터리의 사용

정답 2번

출제 포인트

IIS FTP 서버에서 관리자가 지정하는 서버 설정과 FTP 데이터 연결 방식의 차이를 묻는 문제이다.

핵심 개념

IIS FTP 서버 설정은 서비스 포트와 시간 제한, 인증·익명 접속 허용 여부, 디렉터리 구성처럼 서버가 직접 관리하는 항목을 정하는 것이다. 반면 Active/Passive는 FTP의 데이터 연결을 누가 시작하는지에 관한 방식이다. Active 모드에서는 서버가 클라이언트 쪽으로 데이터 연결을 시작하고, Passive 모드에서는 클라이언트가 서버가 알려 준 데이터 포트로 연결한다.

선지별 해설

① O — 운영 포트 변경과 연결 시간 제한은 FTP 서비스의 노출 범위와 유휴 연결을 관리하는 서버 설정이므로 적절하다.
② X — 틀린 표현은 ‘Active/Passive 모드 지원여부’이다. 이는 단순히 어느 모드를 지원할지를 선택하는 일반적인 IIS FTP 사이트 설정 항목이 아니다. 실제로는 클라이언트가 데이터 연결 방식을 선택하고, 서버 관리자는 Passive 연결에 사용할 데이터 포트 범위와 방화벽·외부 IP 관련 사항 등을 구성한다.
③ O — IIS FTP 인증에서는 계정 기반 인증을 사용할지, 익명 인증을 허용할지 등을 정할 수 있으므로 적절하다. 인증 방식과 함께 권한 부여 규칙을 설정해 접근 가능한 사용자를 제한한다.
④ O — 가상 디렉터리는 실제 물리 경로를 FTP 사이트의 논리적 경로에 연결하는 기능이므로 IIS FTP 서버에서 지정할 수 있는 적절한 항목이다.

오답 포인트

②는 Passive 모드 운용을 위해 서버 측 포트 범위나 방화벽을 설정할 수 있다는 사실을 ‘Active/Passive 모드 지원여부를 지정한다’는 표현과 혼동하게 만든다. 연결 환경의 세부 설정과 모드 자체의 지원 여부 선택은 구별해야 한다.

NoteBase

다시 나오면 이렇게 판단

포트·시간 제한·인증·디렉터리처럼 서버가 직접 관리하는 항목인지, 아니면 FTP 프로토콜의 데이터 연결 동작 방식인지 구분한다. Active/Passive가 나오면 모드 지원 여부보다 연결 주체와 Passive용 포트·방화벽 설정을 먼저 판단한다.

암기 포인트

IIS FTP 설정은 포트·시간·인증·경로이고, Active/Passive는 데이터 연결 방식이다.

NoteBase

문 11. 다음 중 위험관리에 관련된 용어와 그 의미의 연결이 가장 거리가 먼 것은?

① 잔여위험 - 위험처리를 수행하기 이전에 잔여하는 위험

② 위험수준 - 결과와 가능성의 조합으로 표현되는 위험의 크기

③ 통제 - 위험을 변경시키기 위한 대책

④ 위험분석 - 위험의 본질을 이해하고 위험수준을 결정하는 과정

정답 1번

출제 포인트

위험관리 용어의 정의를 정확히 연결하고, 특히 잔여위험이 어느 시점에 남는 위험인지 구별하는 문제이다.

핵심 개념

잔여위험: 위험처리를 수행한 후에도 남아 있는 위험이다. 핵심 키워드는 '처리 후'이다.
위험수준: 위험의 결과와 그 결과가 발생할 가능성의 조합으로 나타낸 위험의 크기이다.
통제: 위험을 변경하기 위한 대책이다.
위험분석: 위험의 본질을 이해하고 위험수준을 결정하는 과정이다.

선지별 해설

① X — '위험처리를 수행하기 이전'이라는 시점이 틀렸다. 잔여위험은 위험처리를 수행한 후에도 남아 있는 위험이다.
② O — 위험수준은 결과와 가능성의 조합으로 표현되는 위험의 크기이므로 올바른 연결이다.
③ O — 통제는 위험을 줄이거나 그 성격을 바꾸는 등 위험을 변경하기 위한 대책이므로 올바른 연결이다.
④ O — 위험분석은 위험의 본질을 이해하고 위험수준을 결정하는 과정이므로 올바른 연결이다.

오답 포인트

①은 '잔여한다'는 말 때문에 위험처리 전부터 존재하는 위험으로 오해하게 만든다. 그러나 잔여위험의 기준 시점은 위험처리 후이며, '이전'과 '이후'를 바꾸어 놓은 것이 함정이다.

다시 나오면 이렇게 판단

위험관리 용어의 정의에서는 먼저 시점을 확인한다. '잔여위험'이 나오면 위험처리 후에도 남는 위험인지 확인하고, 위험수준은 결과와 가능성, 위험분석은 본질의 이해와 수준 결정이라는 짝을 확인한다.

암기 포인트

잔여위험은 처리 후, 위험수준은 결과와 가능성, 위험분석은 이해와 수준 결정이다.

NoteBase

문 12. 다음 중 NTFS 파일 시스템에 대한 설명으로 가장 옳지 않은 것은?

① 이론적인 최대 NTFS 파일 크기는 16EB이다.

② 기본 NTFS 보안을 변경하면 사용자마다 각기 다른 NTFS 보안을 설정할 수 없다.

③ NTFS 구조는 크게 VBR 영역, MTF 영역, Data 영역으로 나눈다.

④ 실제 최대 NTFS 파일 크기는 16TB이다.

정답 2번

출제 포인트

NTFS의 파일 크기 한계, 디스크 구조, 사용자별 접근 권한 설정 기능을 구분하는 문제이다.

핵심 개념

NTFS는 Windows 계열에서 사용하는 파일 시스템으로, 파일과 폴더마다 사용자·그룹별 접근 권한을 설정할 수 있다. 디스크 구조의 핵심은 부트 정보를 담는 VBR, 파일·디렉터리의 메타데이터를 관리하는 MFT, 실제 내용을 저장하는 Data 영역이다.

선지별 해설

① O — NTFS가 주소 체계상 표현할 수 있는 이론적인 최대 파일 크기는 16*EB*이다.
② X — 틀린 부분은 '사용자마다 각기 다른 NTFS 보안을 설정할 수 없다'이다. NTFS는 접근 제어 목록을 이용하므로 기본 권한을 변경하여 사용자나 그룹마다 읽기·쓰기·수정 등 서로 다른 권한을 설정할 수 있다. 올바르게는 '사용자마다 각기 다른 NTFS 보안을 설정할 수 있다'이다.
③ O — NTFS 구조는 크게 VBR, MFT, Data 영역으로 구분한다. VBR은 부트 정보, MFT는 파일과 디렉터리의 메타데이터, Data 영역은 실제 파일 내용을 담당한다. 선지의 'MTF'는 일반적으로 사용하는 명칭인 MFT를 가리키는 표현이다.
④ O — 이 문항이 전제한 NTFS 규격 설명에서 실제로 구현된 최대 파일 크기는 16*TB*이다. 이론적 한계인 16*EB*와 실제 구현 한계를 구분해야 한다.

오답 포인트

②의 '설정할 수 없다'라는 부정 표현이 함정이다. NTFS 보안의 핵심 기능이 바로 사용자·그룹별 세분화된 접근 권한 설정이다. 또한 ③의 'MTF'는 표준 약어 MFT와 글자 순서가 달라 보이지만, 문항에서는 MFT 영역을 뜻하는 표현으로 사용되었다.

다시 나오면 이렇게 판단

NTFS 보안 선지는 사용자·그룹별 권한 설정이 가능한지를 먼저 확인한다. 용량 선지는 이론적 주소 한계와 운영체제에서의 실제 구현 한계를 분리하고, 구조 선지는 VBR·MFT·Data의 역할을 대응시킨다.

NoteBase

암기 포인트

NTFS는 사용자별 권한 설정이 가능하며, 핵심 구조는 VBR·MFT·Data이다.

NoteBase

문 13. AES 알고리즘의 블록 크기와 키 길이에 대한 설명으로 가장 올바른 것은?

① 블록 크기는 128/192/256비트이고, 키 길이는 64비트이다.

② 블록 크기는 128비트이고, 키 길이는 56비트이다.

③ 블록 크기는 64비트이고, 키 길이는 128/192/256비트이다.

④ 블록 크기는 128비트이고, 키 길이는 128/192/256비트이다.

정답 4번

출제 포인트

AES의 고정된 블록 크기와 허용되는 세 가지 키 길이를 구별하는 문제이다.

핵심 개념

AES는 데이터를 128비트 블록 단위로 암호화하는 대칭키 블록 암호이며, 키 길이는 128비트·192비트·256비트 중 하나를 사용한다. 키 길이가 길어지면 라운드 수도 AES-128은 10회, AES-192는 12회, AES-256은 14회로 달라지지만 블록 크기는 항상 128비트이다.

선지별 해설

① X — '블록 크기는 128/192/256비트이고, 키 길이는 64비트'라는 부분이 틀리다. AES의 블록 크기는 128비트로 고정되고, 키 길이는 128/192/256비트이다.
② X — '키 길이는 56비트'라는 부분이 틀리다. 56비트는 DES의 유효 키 길이이며, AES의 키 길이는 128/192/256비트이다. AES의 블록 크기가 128비트라는 부분만 맞는다.
③ X — 블록 크기와 키 길이를 서로 뒤바꾼 설명이다. 올바르게는 블록 크기가 128비트이고, 키 길이가 128/192/256비트이다.
④ O — AES는 128비트의 고정 블록 크기와 128비트·192비트·256비트의 키 길이를 사용하므로 옳다.

오답 포인트

128·192·256이라는 세 수를 블록 크기의 종류로 착각하거나, DES의 56비트 키 길이를 AES에 섞는 것이 함정이다. 특히 ③은 AES의 블록 크기와 키 길이를 정확히 서로 바꾸어 제시한다.

다시 나오면 이렇게 판단

AES에서는 '블록은 128비트로 고정, 키는 128·192·256비트 중 선택'이라는 두 축을 먼저 확인한다. 56비트 키가 나오면 DES의 특징으로 판단한다.

암기 포인트

AES는 블록 128 고정, 키 128·192·256 선택이다.

NoteBase

문 14. <보기 1>의 상황과 개인정보의 안전한 전달을 위해 제공되어야 할 <보기 2>의 정보보호서비스를 가장 바르게 연결한 것은?

<보기 1>
ㄱ. 甲은 송신하는 개인정보를 도청당하는 일이 없이 乙에게 전달하기 원한다.
ㄴ. 甲은 송신하는 개인정보가 조작당하는 일이 없이 乙에게 전달되기 원한다.
ㄷ. 甲은 통신 상대의 웹 서버가 乙의 진짜 서버라는 것을 확인하고 싶다.
ㄹ. 甲은 乙의 서버에 적절한 시간에 접속하여 정상적으로 요청된 내용을 수행하고 싶다.
<보기 2>
A. 무결성
B. 인증
C. 기밀성
D. 가용성

① ㄱ: B, ㄴ: A, ㄷ: C, ㄹ: D
② ㄱ: A, ㄴ: D, ㄷ: C, ㄹ: B
③ ㄱ: C, ㄴ: A, ㄷ: B, ㄹ: D
④ ㄱ: B, ㄴ: A, ㄷ: D, ㄹ: C

정답 3번

출제 포인트

이 문제는 정보보호의 핵심 서비스인 기밀성·무결성·인증·가용성을 상황별 요구와 연결하는 문제이다.

핵심 개념

기밀성(C): 허가받지 않은 사람이 정보를 보거나 알아내지 못하게 하는 성질이다. 도청 방지가 핵심 단서이다.
무결성(A): 정보가 허가 없이 변경·삭제·조작되지 않았음을 보장하는 성질이다. 조작 방지가 핵심 단서이다.
인증(B): 통신 상대방이나 시스템의 신원이 진짜인지 확인하는 서비스이다. 진짜 서버인지 확인한다는 표현이 핵심 단서이다.
가용성(D): 정당한 사용자가 필요할 때 시스템과 정보에 접근하여 서비스를 이용할 수 있게 하는 성질이다. 적절한 시간의 정상 접속이 핵심 단서이다.
따라서 ㄱ은 C, ㄴ은 A, ㄷ은 B, ㄹ은 D에 해당한다.

NoteBase

선지별 해설

① X
ㄴ-A와 ㄹ-D는 맞지만, ㄱ-B와 ㄷ-C가 틀렸다. 도청되지 않게 전달하는 ㄱ은 인증(B)이 아니라 기밀성(C)이고, 진짜 서버인지 확인하는 ㄷ은 기밀성(C)이 아니라 인증(B)이다. 올바른 연결은 ㄱ-C, ㄴ-A, ㄷ-B, ㄹ-D이다.

② X
ㄱ-A, ㄴ-D, ㄷ-C, ㄹ-B가 모두 틀렸다. 도청 방지는 기밀성(C), 조작 방지는 무결성(A), 진짜 서버 확인은 인증(B), 적절한 시간의 정상 접속은 가용성(D)이다. 올바른 연결은 ㄱ-C, ㄴ-A, ㄷ-B, ㄹ-D이다.

③ O
ㄱ-C는 도청 방지이므로 기밀성, ㄴ-A는 조작 방지이므로 무결성, ㄷ-B는 진짜 서버 확인이므로 인증, ㄹ-D는 필요할 때 정상 이용하는 것이므로 가용성에 해당한다. 네 연결이 모두 정확하다.

④ X
ㄴ-A는 맞지만, ㄱ-B, ㄷ-D, ㄹ-C가 틀렸다. ㄱ은 인증(B)이 아니라 기밀성(C), ㄷ은 가용성(D)이 아니라 인증(B), ㄹ은 기밀성(C)이 아니라 가용성(D)이다. 올바른 연결은 ㄱ-C, ㄴ-A, ㄷ-B, ㄹ-D이다.

오답 포인트

①과 ④는 ㄴ-A를 맞게 제시하면서 기밀성·인증·가용성을 서로 바꾸어 놓았다. 특히 '정보를 누가 보지 못하게 하는가'는 기밀성이고, '상대가 진짜인가'는 인증이라는 차이를 구분해야 한다.

다시 나오면 이렇게 판단

상황의 동사를 기준으로 판별한다. 엿보기·도청 방지는 기밀성, 변경·조작 방지는 무결성, 신원·진위 확인은 인증, 필요할 때 접속·이용 가능은 가용성으로 연결한다.

암기 포인트

도청은 기밀성, 조작은 무결성, 진짜 확인은 인증, 제때 이용은 가용성이다.

NoteBase

문 15. 보기에서 설명하는 특징을 가진 보안 모델은?

ㄱ. 무결성 중심의 상업적 모델로 비인가자의 수정과 인가자의 부적절한 수정을 방지한다.
ㄴ. 정보의 특성에 따라 비밀 노출 방지보다 자료의 변조 방지가 더 중요할 때 적합하며 직무분리를 반영하였고, 접속에 대한 로그를 남긴다.
ㄷ. 군사적 보안 요구사항과 상용보안 요구사항 간의 차이점을 강조한다.
ㄹ. 무결성을 집행하기 위한 일반적인 메커니즘

① Clark - Wilson 모델
② Biba 모델
③ HRU(Harrison - Ruzzo - Ullman) 모델
④ BLP(Bell & La Padula) 모델

정답 1번

출제 포인트

상업 환경의 무결성 보호, 직무분리, 감사 로그를 핵심으로 하는 Clark-Wilson 모델을 다른 보안 모델과 구별하는 문제이다.

핵심 개념

Clark-Wilson 모델은 잘 구성된 트랜잭션과 직무분리, 감사 추적을 통해 데이터 무결성을 보장하는 상업적 보안 모델이다. 비인가자의 수정뿐 아니라 인가자가 정해진 절차를 벗어나 부적절하게 수정하는 것도 방지한다.
Biba 모델은 정보 무결성을 보호하기 위한 다단계 모델로, 낮은 무결성 정보의 유입과 높은 무결성 정보의 하향 변경을 통제한다.
HRU 모델은 접근통제 행렬에서 권한의 부여·회수와 특정 권한의 유출 가능성인 안전성 문제를 다룬다.
BLP 모델은 군사 보안의 기밀성을 중심으로 상위 등급 정보의 누출을 방지한다.

선지별 해설

① O — Clark-Wilson 모델은 상업 환경에서 자료의 무결성을 중시하며, 직무분리와 감사 로그를 사용해 비인가 수정과 인가자의 부적절한 수정을 모두 통제한다. 보기의 ㄱ~ㄹ과 일치한다.
② X — Biba 모델은 무결성 모델이라는 점에서는 관련되지만, 보기의 핵심인 상업적 모델, 직무분리, 잘 구성된 트랜잭션 및 감사 추적을 직접 나타내는 모델은 아니다. 올바르게는 Clark-Wilson 모델이다.
③ X — HRU 모델은 접근통제 행렬에서 권한이 어떻게 변하는지와 권한 안전성 문제를 분석하는 모델이다. 보기의 무결성 중심 상업 모델에 해당한다는 표현은 잘못이며, 올바르게는 Clark-Wilson 모델이다.
④ X — BLP 모델은 군사 환경의 기밀성 보호를 중심으로 하는 모델이다. 자료 변조 방지와 직무분리를 중심으로 한다는 설명은 잘못이며, 올바르게는 Clark-Wilson 모델이다.

NoteBase

오답 포인트

② Biba도 무결성을 다루므로 혼동하기 쉽다. 그러나 보기의 '상업적 모델', '직무분리', '로그'가 함께 제시되면 Clark-Wilson을 가리킨다. ④ BLP는 군사 보안과 연관되지만 보호 목표가 무결성이 아니라 기밀성이라는 점이 결정적이다.

다시 나오면 이렇게 판단

보호 목표와 운영 키워드를 함께 본다. 상업 환경·무결성·직무분리·감사 추적이면 Clark-Wilson, 무결성 등급 통제이면 Biba, 접근통제 행렬의 권한 안전성이면 HRU, 군사 환경·기밀성이면 BLP로 판단한다.

암기 포인트

Clark-Wilson은 상업적 무결성·직무분리·감사 로그, Biba는 무결성 등급, HRU는 권한 안전성, BLP는 군사적 기밀성이다.

NoteBase

문 16. 기존에 알려진 침입 방법에 기초한 오용 침입탐지(Misuse Detection)의 특징이 아닌 것은?

① 알려진 공격법이나 보안정책을 위반하는 행위에 대한 패턴을 지식데이터베이스로부터 찾아서 특정 공격들과 시스템 취약점에 기초한 계산된 지식을 적용하여 탐지해 내는 방법으로 지식 기반(Knowledge-Base)탐지라고도 한다.

② 비교적 탐지의 정확도가 높으나 알려진 공격에 대한 정보수집이 어려우며 새로운 취약성에 대한 최신 정보를 유지하기 어렵다.

③ 정상적인 혹은 유효한 행동 모델은 다양한 방법으로 수집된 참조 정보들로부터 생성되며 현재 활동과 행동 모델을 비교하여 탐지한다.

④ 오용 침입탐지 종류로는 전문가시스템(Expert System), 시그니처 분석(Signature Analysis), 상태전이분석(State Transition Analysis)등이 있다.

정답 3번

출제 포인트

오용 침입탐지와 이상 침입탐지를 구별하는 기준을 묻는 문제이다. 알려진 공격 패턴을 기준으로 삼으면 오용 탐지이고, 정상 행동 모델에서 벗어났는지를 기준으로 삼으면 이상 탐지이다.

핵심 개념

오용 침입탐지: 이미 알려진 공격의 시그니처·규칙·상태전이 등 공격 지식을 데이터베이스화하고 현재 행위와 대조하여 침입을 찾는 방식이다. 알려진 공격에는 정확도가 높지만 새로운 공격을 탐지하기 어렵고 지식데이터베이스를 계속 갱신해야 한다.
이상 침입탐지: 정상적인 사용자·시스템 행동 모델을 만들고 현재 활동이 정상 범위를 벗어나는지를 비교하여 침입을 찾는 방식이다. 알려지지 않은 공격도 탐지할 가능성이 있지만 정상 행동을 침입으로 판단하는 오탐이 생길 수 있다.

선지별 해설

① O — 알려진 공격법이나 보안정책 위반 패턴을 지식데이터베이스에서 찾아 대조하는 것은 오용 침입탐지의 핵심 원리이다. 공격에 관한 지식을 이용하므로 지식 기반 탐지라고도 한다.
② O — 오용 탐지는 등록된 공격 패턴과 일치하는 알려진 공격을 비교적 정확하게 탐지한다. 다만 공격 정보를 수집하여 규칙이나 시그니처로 만들고, 새 취약점과 공격 수법에 맞게 이를 지속적으로 갱신하기 어렵다.
③ X — 틀린 부분은 '정상적인 혹은 유효한 행동 모델'을 만들고 현재 활동과 비교한다는 설명이다. 이는 오용 침입탐지가 아니라 정상 행동에서 벗어난 정도를 판단하는 이상 침입탐지의 특징이다. 오용 침입탐지는 알려진 공격 패턴이나 규칙과 현재 활동을 비교한다.
④ O — 전문가시스템, 시그니처 분석, 상태전이분석은 모두 알려진 공격 지식이나 공격 진행 규칙을 이용하므로 오용 침입탐지의 방식에 해당한다.

NoteBase

오답 포인트

③도 '참조 정보와 현재 활동을 비교한다'는 점 때문에 오용 탐지처럼 보일 수 있다. 그러나 비교 기준이 공격 패턴이 아니라 정상 행동 모델이라는 표현이 결정적인 함정이다.

다시 나오면 이렇게 판단

선지에서 무엇을 기준으로 비교하는지 확인한다. 알려진 공격·시그니처·공격 규칙이면 오용 탐지이고, 정상 프로파일·행동 모델·통계적 정상 범위이면 이상 탐지이다.

암기 포인트

오용 탐지는 '공격을 아는 탐지', 이상 탐지는 '정상을 아는 탐지'이다.

NoteBase

문 17. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 상 정보통신 서비스 제공자는 임원급의 정보보호 최고책임자를 지정할 수 있도록 정하고 있다. 이 법에서 정하고 있는 정보통신서비스 제공자의 정보보호 최고책임자가 총괄하는 업무에 해당하지 않는 것은?

① 정보보호 관리체계 수립 및 관리·운영

② 정보보호 취약점 분석·평가 및 개선

③ 주요 정보통신 기반시설의 지정

④ 정보보호 사전 보안성 검토

정답 3번

쟁점

이 문제는 정보통신서비스 제공자의 정보보호 최고책임자가 총괄하는 업무의 범위를 묻는 문제이다. 핵심은 사업자 내부의 정보보호 관리 업무와 국가가 수행하는 주요정보통신기반시설 지정 업무를 구별하는 것이다.

용어 풀이

정보보호 최고책임자(CISO)는 조직의 정보보호 정책과 위험 관리 등 정보보호 업무를 총괄하는 책임자이다.

핵심 구분

문항 출제 당시 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제45조의3은 정보보호 관리체계의 수립 및 관리·운영, 정보보호 취약점 분석·평가 및 개선, 정보보호 사전 보안성 검토 등을 정보보호 최고책임자의 총괄 업무로 규정하였다. 반면 주요정보통신기반시설의 지정은 「정보통신기반 보호법」에 따라 소관 분야의 중앙행정기관의 장이 수행하는 업무이다.

선지별 해설

① O — 정보보호 관리체계의 수립 및 관리·운영은 문항 출제 당시 정보보호 최고책임자가 총괄하는 업무에 포함된다.
② O — 정보보호 취약점의 분석·평가와 그 결과에 따른 개선은 정보보호 최고책임자의 총괄 업무에 포함된다.
③ X — 주요정보통신기반시설의 지정은 정보통신서비스 제공자 내부의 정보보호 최고책임자가 총괄하는 업무가 아니다. 틀린 표현: '주요 정보통신 기반시설의 지정'이 정보보호 최고책임자의 총괄 업무라는 부분이다. 올바른 표현: 주요정보통신기반시설은 「정보통신기반 보호법」에 따라 소관 분야의 중앙행정기관의 장이 지정할 수 있다.
④ O — 정보보호 사전 보안성 검토는 문항 출제 당시 정보보호 최고책임자가 총괄하는 업무에 포함된다.

NoteBase

오답 포인트

③의 '정보통신'과 '기반시설'이라는 표현 때문에 일반적인 정보보호 업무처럼 보이게 한 것이 함정이다. 정보보호 최고책임자는 사업자 내부의 정보보호 업무를 총괄하지만, 주요정보통신기반시설의 지정은 국가의 지정 권한에 속한다.

다시 나오면 이렇게 판단

선지가 조직 내부의 정보보호 체계 수립, 취약점 관리, 보안성 검토에 관한 것이면 정보보호 최고책임자의 업무로 판단한다. 특정 시설을 법정 기반시설로 지정하는 것처럼 공권력 행사에 해당하면 중앙행정기관 등 법정 지정 주체의 업무인지 구별한다.

암기 포인트

CISO는 내부 정보보호를 총괄하고, 주요정보통신기반시설은 중앙행정기관의 장이 지정한다.

NoteBase

문 18. 다음 중 윈도우 로그 종류와 설명이 가장 바르게 짝지어진 것은?

① 계정 관리 감사 — 사용자 권한 할당 정책, 감사 정책, 신뢰 정책의 변경과 관련된 사항을 로깅한다.

② 정책 변경 감사 — 권한 설정 변경이나 관리자 권한이 필요한 작업을 수행할 때 로깅한다.

③ 개체 액세스 감사 — 특정 파일이나 디렉터리, 레지스트리 키 등과 같은 객체에 대한 접근을 시도하거나 속성 변경 등을 탐지한다.

④ 로그인 이벤트 감사 — 시스템의 시작과 종료, 보안 로그 삭제 등 시스템의 주요한 사항에 대한 이벤트를 남긴다.

정답 3번

출제 포인트

윈도우 감사 정책의 각 범주가 어떤 보안 사건을 기록하는지 구별하는 문제이다.

핵심 개념

계정 관리 감사는 사용자·그룹 계정의 생성, 변경, 삭제와 같은 계정 관리 활동을 기록한다. 정책 변경 감사는 사용자 권한 할당 정책, 감사 정책, 신뢰 정책 등의 변경을 기록한다. 권한 사용 감사는 관리자 권한 등 사용자 권한의 사용을 기록한다. 개체 액세스 감사는 감사가 설정된 파일, 디렉터리, 레지스트리 키 등의 접근을 기록한다. 로그인 이벤트 감사는 로그온과 로그오프 등의 인증 관련 사건을 기록하고, 시스템 이벤트 감사는 시스템 시작·종료와 보안 로그에 영향을 주는 사건을 기록한다.

NoteBase

선지별 해설

① X
계정 관리 감사는 사용자 또는 그룹 계정의 생성·변경·삭제 등을 기록한다. 선지의 '사용자 권한 할당 정책, 감사 정책, 신뢰 정책의 변경'은 정책 변경 감사에 해당한다.

② X
정책 변경 감사는 감사 정책, 사용자 권한 할당 정책, 신뢰 정책 등의 변경을 기록한다. 선지의 '권한 설정 변경이나 관리자 권한이 필요한 작업을 수행할 때 로깅한다'는 설명 중 권한의 실제 사용에 초점을 둔 부분은 권한 사용 감사에 해당한다.

③ O
개체 액세스 감사는 파일, 디렉터리, 레지스트리 키 등 감사 대상 개체에 대한 접근 시도와 관련 변경을 탐지·기록하므로 올바른 짝이다.

④ X
로그인 이벤트 감사는 사용자의 로그온·로그오프와 같은 인증 관련 사건을 기록한다. 선지의 '시스템의 시작과 종료, 보안 로그 삭제 등'은 시스템 이벤트 감사에 해당한다.

오답 포인트

①과 ②는 정책의 변경과 권한의 사용을 서로 바꾸어 놓았고, ④는 사용자 로그인 사건과 시스템 자체의 주요 사건을 혼동하게 만든다. 특히 '정책을 바꿈'과 '부여된 권한을 실제로 씀'을 구분해야 한다.

다시 나오면 이렇게 판단

선지의 동작 대상을 먼저 확인한다. 계정을 만들거나 바꾸면 계정 관리, 감사·권한 할당 등의 정책을 바꾸면 정책 변경, 권한을 실제로 행사하면 권한 사용, 파일·레지스트리 등에 접근하면 개체 액세스, 사용자가 접속하거나 종료하면 로그인 이벤트, 운영체제의 시작·종료나 보안 로그 관련 사건이면 시스템 이벤트로 판단한다.

암기 포인트

계정은 계정 관리, 정책은 정책 변경, 권한 행사는 권한 사용, 파일·레지스트리는 개체 액세스, 사용자 접속은 로그인, 시스템 시작·종료는 시스템 이벤트이다.

NoteBase

문 19. 위험분석 및 평가방법론 중 성격이 가장 다른 것은?

① 확률분포법

② 순위결정법

③ 과거자료 분석법

④ 수학공식 접근법

정답 2번

출제 포인트

위험분석 방법을 수치로 위험을 산정하는 정량적 방법과 전문가의 판단·서열에 의존하는 정성적 방법으로 구분하는 문제이다.

핵심 개념

정량적 위험분석은 발생 가능성이나 손실 규모를 수치로 계산하는 방법이다. 확률분포법, 과거자료 분석법, 수학공식 접근법이 이에 속한다.
정성적 위험분석은 정확한 수치보다 전문가의 경험과 판단을 이용하여 위험의 등급이나 우선순위를 정하는 방법이다. 순위결정법이 이에 속한다.

선지별 해설

① X — 확률분포법은 예상 손실을 확률분포에 따라 추정하는 정량적 위험분석 방법이므로 성격이 다른 방법이 아니다. 틀린 판단은 '확률분포법이 가장 다르다'는 부분이며, 올바르게는 순위결정법이 가장 다르다.
② O — 순위결정법은 전문가가 위험 항목의 상대적 중요도와 우선순위를 정하는 정성적 위험분석 방법이다. 나머지 세 방법이 정량적 방법이므로 성격이 가장 다르다.
③ X — 과거자료 분석법은 과거의 손실·사고 자료를 이용해 위험의 발생 가능성이나 손실을 수치로 추정하는 정량적 위험분석 방법이므로 성격이 다른 방법이 아니다. 틀린 판단은 '과거자료 분석법이 가장 다르다'는 부분이며, 올바르게는 순위결정법이 가장 다르다.
④ X — 수학공식 접근법은 위협의 발생빈도나 손실을 공식으로 계산해 위험을 계량하는 정량적 위험분석 방법이므로 성격이 다른 방법이 아니다. 틀린 판단은 '수학공식 접근법이 가장 다르다'는 부분이며, 올바르게는 순위결정법이 가장 다르다.

오답 포인트

'순위'도 숫자로 표시할 수 있다는 이유로 순위결정법을 정량적 방법으로 오인하기 쉽다. 그러나 순위결정법의 핵심은 계산된 손실액이나 확률이 아니라 전문가의 주관적 판단에 따른 상대적 서열이다.

NoteBase

다시 나오면 이렇게 판단

과거 수치·확률·공식으로 위험을 계산하면 정량적 방법이고, 전문가의 판단으로 등급·순위·시나리오를 정하면 정성적 방법으로 판단한다.

암기 포인트

확률·과거자료·수학공식은 정량, 순위결정은 정성이다.

NoteBase

문 20. 다음 중 IPSec(Internet Protocol Security)에 대한 설명으로 가장 올바르지 못한 것은?

① 네트워크 계층에서 보안성을 제공해주는 표준화된 기술로 송수신자에게 인증 및 암호화 서비스를 제공한다.

② SA(Security Association)는 보안성 있는 데이터를 교환하기 위해 암호화, 키 교환 등에 대한 합의 사항들을 담고 있다.

③ AH(Authentication Header)는 인증 부분과 암호화 부분 모두를 포함한다.

④ 보안서비스를 위하여 AH(Authentication Header)와 ESP(Encapsulating Security Payload)의 두 프로토콜을 사용한다.

정답 3번

출제 포인트

IPSec의 계층, SA의 역할, AH와 ESP가 제공하는 보안 서비스의 차이를 묻는 문제이다.

핵심 개념

IPSec는 IP 계층에서 통신 당사자 인증, 무결성 보호, 기밀성 등의 보안 서비스를 제공하는 기술이다.
SA(Security Association)는 IPSec 통신에 사용할 프로토콜, 암호 알고리즘, 키, 수명 등의 보안 매개변수를 정한 단방향 논리적 연결이다.
AH는 출처 인증과 무결성 및 재전송 방지 기능을 제공하지만 데이터를 암호화하지 않으므로 기밀성을 제공하지 않는다. ESP는 데이터 암호화를 통한 기밀성을 제공하며 인증 기능도 선택적으로 제공할 수 있다.

선지별 해설

① O — IPSec는 네트워크 계층에서 동작하는 표준 보안 기술이다. AH 또는 ESP를 이용해 인증·무결성 서비스를 제공하고, ESP를 이용해 암호화에 의한 기밀성도 제공할 수 있다.
② O — SA에는 안전한 데이터 교환에 적용할 보안 프로토콜과 암호 알고리즘, 키 등 합의된 보안 매개변수가 담긴다. 이러한 SA와 키의 협상·설정에는 일반적으로 IKE가 사용된다.
③ X — 틀린 표현은 'AH는 인증 부분과 암호화 부분 모두를 포함한다'이다. 올바르게는 AH는 데이터 출처 인증과 무결성을 제공하지만 암호화를 수행하지 않으며, 기밀성이 필요할 때는 ESP를 사용한다.
④ O — IPSec의 핵심 보안 프로토콜은 인증과 무결성을 담당하는 AH와, 암호화 및 선택적 인증을 제공하는 ESP이다.

오답 포인트

③은 AH의 이름에 'Authentication'이 들어간다는 점은 맞지만, 여기에 암호화 기능까지 있다고 덧붙인 것이 함정이다. 인증·무결성과 암호화·기밀성을 같은 기능으로 보아서는 안 된다.

NoteBase

다시 나오면 이렇게 판단

AH가 나오면 인증·무결성은 제공하지만 암호화·기밀성은 제공하지 않는다고 판단한다. 암호화나 기밀성이 언급되면 ESP의 기능인지 확인한다.

암기 포인트

AH는 인증·무결성, ESP는 암호화·기밀성이다.

NoteBase