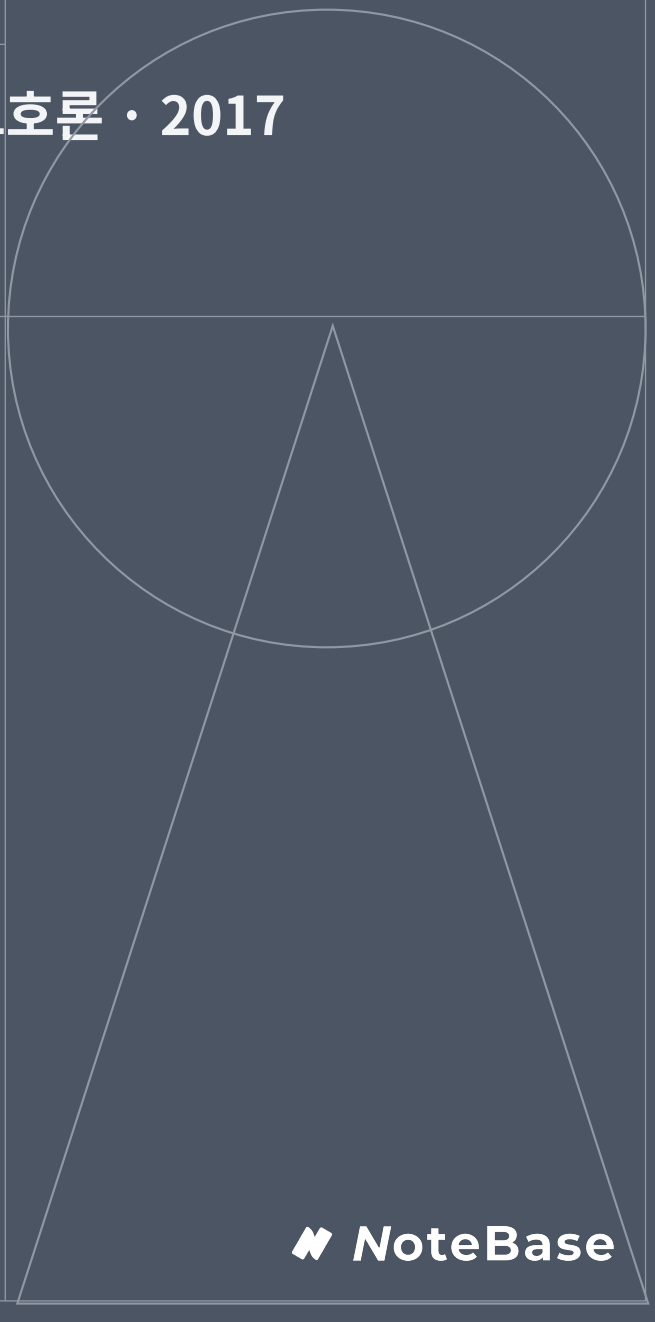
기출OX 해설집

공무원/국가직/9급 · 정보보호론 · 2017



NoteBase

기출OX 해설집

공무원/국가직/9급 · 정보보호론 · 2017

공무원/국가직/9급 · 정보보호론 · 2017

문 1. 컴퓨터 시스템 및 네트워크 자산에 대한 위협 중에서 기밀성 침해에 해당하는 것은?

① 장비가 불능 상태가 되어 서비스가 제공되지 않음

② 통계적 방법으로 데이터 내용이 분석됨

③ 새로운 파일이 허위로 만들어짐

④ 메시지가 재정렬됨

정답 2번

간단한 해설

기밀성은 **인가받지 않은 사람이 정보 내용을 알 수 없도록** 보호하는 성질이다. 통계적 방법으로 비밀 데이터의 내용을 알아내는 것도 정보 노출이므로, 데이터를 변경하지 않아도 기밀성을 침해한다.

공통 해설

기밀성은 정보 내용을 인가받지 않은 사람에게 공개하지 않는 성질이다. 따라서 이 문항의 판단 기준은 **권한 없는 사람이 정보 내용을 알아내는가**이다. 정보를 읽거나 추론하여 알아내는 것만으로도 침해가 성립하며, 원본 데이터가 바뀌어야 하는 것은 아니다.

위협 상황에서 '통계적 방법으로 데이터 내용이 분석됨'은 통계적 특성을 이용해 보호된 정보의 내용을 알아내는 경우이므로 이 기준에 해당한다. 장비 불능으로 서비스가 제공되지 않는 것은 정보나 서비스를 이용할 수 없게 된 상황이고, 허위 파일 생성과 메시지 재정렬은 각각 허위 정보가 추가되거나 정보의 순서가 바뀐 상황이다. 이 세 현상 자체는 비밀 내용이 권한 없는 사람에게 알려졌다는 것을 뜻하지 않으므로, 제시된 위협 중 기밀성 침해에 해당하는 것은 데이터 내용의 분석이다.

NoteBase

문 2. 공개키기반구조(PKI)에서 관리나 보안상의 문제로 폐기된 인증서들의 목록은?

① Online Certificate Status Protocol

② Secure Socket Layer

③ Certificate Revocation List

④ Certification Authority

정답 3번

간단한 해설

관리·보안상의 문제로 폐기된 인증서들을 모아 기록한 목록은 **인증서 폐기 목록(CRL)**이다.

공통 해설

인증서는 유효기간이 남아 있어도 개인키 유출 등 관리·보안상의 사유로 폐기될 수 있다. 이런 인증서들을 식별할 수 있도록 **일련번호와 폐기일시 등을 모아 기록한 목록**이 인증서 폐기 목록(CRL, Certificate Revocation List)이다. 인증서를 사용하는 쪽은 해당 목록에 인증서가 등록되어 있는지 확인하여 폐기 여부를 판단한다.

NoteBase

문 3. AES 알고리즘의 블록크기와 키길이에 대한 설명으로 옳은 것은?

① 블록크기는 64비트이고 키길이는 56비트이다.

② 블록크기는 128비트이고 키길이는 56비트이다.

③ 블록크기는 64비트이고 키길이는 128/192/256비트이다.

④ 블록크기는 128비트이고 키길이는 128/192/256비트이다.

정답 4번

간단한 해설

AES는 **블록크기가 128비트로 고정**되며, 키길이는 **128·192·256비트 중 하나**를 사용한다. 키길이가 달라져도 블록크기는 변하지 않는다.

공통 해설

블록크기는 암호 알고리즘이 한 번에 처리하는 데이터 단위의 길이이고, 키길이는 암호화·복호화에 사용하는 비밀키의 길이이다. AES의 규격은 **128비트 블록과 128·192·256비트 중 하나의 키**를 사용하는 것이다. 세 키길이를 동시에 사용하는 것이 아니라 그중 하나를 선택한다.

예를 들어 AES-256은 키길이가 256비트라는 뜻이며, 이때도 블록크기는 128비트이다. 따라서 블록크기를 64비트로 제시하거나 키길이를 56비트로 제시한 설명은 AES 규격에 맞지 않는다. 블록크기 128비트와 키길이 128·192·256비트를 함께 제시한 설명이 AES의 특성에 부합한다.

NoteBase

문 4. 우리나라 국가 표준으로 지정되었으며 경량 환경 및 하드웨어 구현에서의 효율성 향상을 위해 개발된 128비트 블록암호 알고리즘은?

① IDEA

② 3DES

③ HMAC

④ ARIA

정답 4번

간단한 해설

ARIA는 우리나라 국가 표준으로 지정된 **128비트 블록암호**이며, **경량 환경과 하드웨어 구현의 효율성**을 높이도록 설계되었다.

공통 해설

ARIA는 국내에서 개발되어 국가 표준으로 지정된 대칭키 블록암호 알고리즘이다. 데이터를 **128비트 블록 단위**로 암호화·복호화한다는 뜻이며, 이 수치는 암호키의 길이를 뜻하지 않는다.

ARIA는 XOR과 같은 단순한 바이트 단위 연산을 중심으로 구성하여 **경량 환경과 하드웨어에서 효율적으로 구현**할 수 있도록 설계되었다. 따라서 문제에 제시된 국내 국가 표준, 128비트 블록, 경량 환경 및 하드웨어 구현 최적화라는 특성이 가리키는 알고리즘은 ARIA이다.

NoteBase

문 5. '정보시스템과 네트워크의 보호를 위한 OECD 가이드라인' (2002)에서 제시한 원리(principle) 중 "참여자들은 정보시스템과 네트워크 보안의 필요성과 그 안전성을 향상하기 위하여 할 수 있는 사항을 알고 있어야 한다."에 해당하는 것은?

① 인식(Awareness)

② 책임(Responsibility)

③ 윤리(Ethics)

④ 재평가(Reassessment)

정답 1번

간단한 해설

보안의 필요성과 보안을 높이기 위해 자신이 할 수 있는 일을 **알고 있어야 한다**는 것은 **인식(Awareness)** 원리이다.

공통 해설

OECD 가이드라인의 인식(Awareness) 원리는 참여자가 **보안의 필요성과 자신이 취할 수 있는 보호 방법을 이해**해야 한다는 원리이다. 제시문은 보안에 관해 무엇을 알고 있어야 하는지를 설명하므로 이 원리에 해당한다. 인식에는 정보시스템·네트워크에 대한 위험과 이용 가능한 보호 수단을 아는 것이 포함된다. 예를 들어 자신이 사용하는 시스템에 어떤 위험이 있고 어떤 보안 업데이트를 적용할 수 있는지 알아두는 것이 이에 해당한다.

NoteBase

문 6. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상 정보통신서비스 제공자등이 이용자 개인정보의 국외 이전을 위한 동의 절차에서 이용자에게 고지해야 할 사항에 해당하지 않는 것은?

① 이전되는 개인정보 항목

② 개인정보가 이전되는 국가, 이전일시 및 이전방법

③ 개인정보를 이전받는 자의 개인정보 이용 목적 및 보유·이용 기간

④ 개인정보를 이전하는 자의 성명(법인인 경우는 명칭 및 정보관리책임자의 연락처)

정답 4번

간단한 해설

고지해야 하는 신원 정보는 개인정보를 **이전받는 자**의 것이다. ④의 '이전하는 자'는 '이전받는 자'로 고쳐야 하며, 법인이면 그 명칭과 정보관리책임자의 연락처를 알려야 한다.

선지별 해설

구 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제63조제3항은 정보통신서비스 제공자등이 개인정보 국외 이전에 대한 동의를 받으려면 미리 법정 사항 모두를 이용자에게 고지하도록 규정하였다. 이 문항은 그 고지사항을 묻는다.

① O: 이전되는 개인정보 항목은 법정 고지사항이다. 이용자가 **어떤 개인정보가 국외로 넘어가는지** 확인하고 동의할 수 있도록 이전 대상 항목을 미리 알려야 한다.

② O: 개인정보가 이전되는 국가, 이전일시 및 이전방법은 법정 고지사항이다. 국외 이전이 **어디로, 언제, 어떤 방법으로** 이루어지는지를 알려야 한다.

③ O: 개인정보를 이전받는 자의 개인정보 이용 목적 및 보유·이용 기간은 법정 고지사항이다. 국외의 수령자가 개인정보를 **무엇에 사용하고 얼마 동안 보유·이용하는지**를 알려야 한다.

④ X: 구법 제63조제3항제3호가 고지하도록 한 대상은 개인정보를 **이전받는 자의 성명**이다. 이전받는 자가 법인이면 그 명칭 및 정보관리책임자의 연락처를 알려야 한다. 선지는 이 대상을 '이전하는 자'로 바꾸었으므로 법정 고지사항에 해당하지 않는다.

NoteBase

문 7. IPSec에서 두 컴퓨터 간의 보안 연결 설정을 위해 사용되는 것은?

① Authentication Header

② Encapsulating Security Payload

③ Internet Key Exchange

④ Extensible Authentication Protocol

정답 3번

간단한 해설

IPSec의 보안 연결을 설정하려면 통신 상대를 인증하고 사용할 보안 알고리즘과 키를 마련해야 한다. 이 과정을 수행하여 **보안 연관(SA)을 설정**하는 프로토콜이 IKE(Internet Key Exchange)이다.

공통 해설

IPSec의 보안 연관(SA)은 데이터를 어떤 보안 알고리즘과 키로 보호할지 정한 보안 정보의 집합이다.
IKE(Internet Key Exchange)는 통신 상대를 인증하고, 보안 알고리즘을 협상하며, 키 교환을 통해 필요한 키를 생성하여 SA를 설정·관리한다. 따라서 문제에서 묻는 '두 컴퓨터 간의 보안 연결 설정'은 **IKE의 SA 설정 기능**에 해당한다.

구별 기준은 **보안 연결의 조건을 협상·설정하는가**이다. AH(Authentication Header)와 ESP(Encapsulating Security Payload)는 설정된 SA의 알고리즘과 키를 이용하여 실제 IP 패킷을 보호하는 프로토콜이다.
EAP(Extensible Authentication Protocol)는 여러 인증 방법을 지원하는 인증 프레임워크로, IKEv2의 인증 과정에 사용될 수 있지만 그 자체가 IPSec의 SA 설정 전반을 수행하는 프로토콜은 아니다.

NoteBase

문 8. 다음 설명에 해당하는 것은?

PC나 스마트폰을 해킹하여 특정 프로그램이나 기기 자체를 사용하지 못하도록 하는 악성코드로서 인터넷 사용자의 컴퓨터에 설치되어 내부 문서나 스프레드시트, 이미지 파일 등을 암호화하여 열지 못하도록 만든 후 돈을 보내주면 해독용 열쇠 프로그램을 전송해 준다며 금품을 요구한다.

① Web Shell

② Ransomware

③ Honeypot

④ Stuxnet

정답 2번

간단한 해설

파일을 암호화하거나 기기 사용을 막은 뒤 **복구를 대가로 금품을 요구**하는 악성코드가 랜섬웨어(Ransomware)이다.

공통 해설

랜섬웨어(Ransomware)는 파일을 암호화하거나 시스템 사용을 제한하여 피해자가 데이터나 기기를 이용하지 못하게 하고, 이를 복구해 주겠다며 금품을 요구하는 악성코드이다. 지문에서는 문서·스프레드시트·이미지 파일을 암호화해 열지 못하게 한 뒤, 돈을 보내면 해독용 열쇠 프로그램을 주겠다고 요구한다. 여기서 암호화는 데이터를 보호하려는 수단이 아니라 **피해자의 파일 접근을 막아 금품을 요구하는 수단**으로 쓰인다. 따라서 지문의 행위는 랜섬웨어의 특징에 해당한다.

NoteBase

문 9. 「개인정보 보호법 시행령」상 개인정보처리자가 하여야 하는 안전성 확보 조치에 해당하지 않는 것은?

① 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행

② 개인정보가 정보주체의 요구를 받아 삭제되더라도 이를 복구 또는 재생할 수 있는 내부 방안 마련

③ 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치

④ 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치

정답 2번

간단한 해설

②의 '복구 또는 재생할 수 있는'은 삭제의 취지와 반대이다. 정보주체의 요구에 따라 개인정보를 삭제할 때에는 **복구 또는 재생되지 않도록** 조치해야 한다.

선지별 해설

① O: 「개인정보 보호법 시행령」 제30조제1항은 안전성 확보 조치로 내부 관리계획을 수립하고 시행하도록 한다. 개인정보취급자에 대한 교육·감독과 보호조치의 이행 기준을 정해 **조직 내부에서 개인정보를 일관되게 관리**하기 위한 조치이다.

② X: 「개인정보 보호법」 제36조제3항에 따라 정보주체의 요구로 개인정보를 삭제할 때에는 **복구 또는 재생되지 않도록** 해야 한다. 삭제한 정보를 다시 되살릴 수 있는 방안을 마련하라는 의무는 없다. 선지의 '복구 또는 재생할 수 있는'은 '복구 또는 재생할 수 없도록 하는'으로 고쳐야 한다.

③ O: 「개인정보 보호법 시행령」 제30조제1항은 개인정보를 저장·전송할 때 암호화 등으로 보호하도록 한다. 암호화는 정보를 알아보기 어려운 형태로 바꾸어, 저장매체나 전송 내용이 노출되더라도 **권한 없는 사람이 내용을 읽기 어렵게** 하는 기술적 보호조치이다.

④ O: 「개인정보 보호법 시행령」 제30조제1항은 침해사고에 대응할 수 있도록 접속기록을 보관하고 위조·변조를 막도록 한다. 접속기록에는 누가 언제 접속하여 어떤 처리를 했는지에 관한 정보가 남으므로 사고 경위를 조사하는 데 쓰인다. 기록의 위조·변조를 방지해야 **조사에 필요한 증거의 신뢰성**을 유지할 수 있다.

NoteBase

문 10. 공개키 암호시스템에 대한 설명 중 ㉠~㉢에 들어갈 말로 옳게 짝지어진 것은?

○ (㉠)의 안전성은 유한체의 이산대수 계산의 어려움에 기반을 둔다.
○ (㉡)의 안전성은 타원곡선군의 이산대수 계산의 어려움에 기반을 둔다.
○ (㉢)의 안전성은 소인수분해의 어려움에 기반을 둔다.

① ㉠: ElGamal 암호시스템, ㉡: DSS, ㉢: RSA 암호시스템
② ㉠: Knapsack 암호시스템, ㉡: ECC, ㉢: RSA 암호시스템
③ ㉠: Knapsack 암호시스템, ㉡: DSS, ㉢: Rabin 암호시스템
④ ㉠: ElGamal 암호시스템, ㉡: ECC, ㉢: Rabin 암호시스템

정답 4번

간단한 해설

같은 이산대수 문제라도 ElGamal은 **유한체**, ECC는 **타원곡선군**에서의 계산 난도를 이용한다. Rabin은 **소인수분해의 어려움**에 기반을 둔다.

빈칸별 해설

㉠ ElGamal 암호시스템: 유한체에서 거듭제곱한 결과와 밑을 알아도 지수를 구하기는 어렵다는 **이산대수 문제**를 이용한다. 공개키로부터 비밀 지수를 알아내기 어렵다는 점이 핵심이다.

㉡ ECC: 타원곡선 위의 점을 반복해서 더하는 연산을 이용한다. 기준점과 그 기준점을 여러 번 더한 결과를 알아도 몇 번 더했는지 구하기 어려운 **타원곡선군의 이산대수 문제**에 기반을 둔다. ㉠과는 이산대수를 계산하는 군이 다르다.

㉢ Rabin 암호시스템: 두 큰 소수의 곱을 공개하고, 이를 법으로 하는 제곱 연산으로 암호화한다. 복호화에는 모듈러 제곱근을 구하는 과정이 필요하며, 이 문제는 **소인수분해 문제와 계산상 동등**하다. 소인수분해로 두 소수를 알면 이를 이용해 제곱근을 구할 수 있다. RSA도 소인수분해의 어려움과 관련되므로, ㉢의 단서만으로 고르지 않고 앞의 두 빈칸까지 함께 확인해야 한다.

㉠ ElGamal 암호시스템, ㉡ ECC, ㉢ Rabin 암호시스템을 모두 충족하는 조합은 ④이다.

NoteBase

문 11. 가상사설망에서 사용되는 프로토콜이 아닌 것은?

① L2F

② PPTP

③ TFTP

④ L2TP

정답 3번

간단한 해설

TFTP는 **간단한 파일 전송**을 위한 프로토콜이며, 가상사설망의 통신 경로를 구성하는 **터널링 프로토콜이 아니다**.

공통 해설

가상사설망(VPN)의 터널링은 원래의 통신 데이터를 다른 프로토콜의 패킷 안에 넣어 공중망을 통과시키는 방식이다. 수신 측은 바깥쪽 정보를 제거하여 원래 데이터를 꺼내므로, 떨어진 지점 사이에 논리적인 통신 경로를 구성할 수 있다. L2F·PPTP·L2TP는 모두 이러한 **터널링 기능**을 제공하며, PPP 프레임 등을 망을 통해 운반하는 데 사용된다.

TFTP(Trivial File Transfer Protocol)는 UDP를 이용하여 원격 장치의 파일을 읽거나 쓰는 **파일 전송 프로토콜**이다. 파일을 주고받는 기능을 제공할 뿐 VPN 터널을 구성하지 않으므로, 이 문항에서 묻는 VPN용 프로토콜에 해당하지 않는다.

NoteBase

문 12. 메모리 영역에 비정상적인 데이터나 비트를 채워 시스템의 정상적인 동작을 방해하는 공격 방식은?

① Spoofing

② Buffer overflow

③ Sniffing

④ Scanning

정답 2번

간단한 해설

버퍼 오버플로(Buffer overflow)는 **버퍼의 용량을 넘는 데이터를 기록**하여 인접한 메모리 영역을 손상시키는 공격이다. 이로 인해 프로그램이 비정상적으로 종료되거나 정상적인 실행 흐름이 바뀔 수 있다.

공통 해설

버퍼는 프로그램이 데이터를 임시로 저장하는 메모리 공간이다. 버퍼 오버플로(Buffer overflow)는 입력 길이를 제대로 검사하지 않아 **할당된 버퍼의 경계를 넘어 데이터가 기록**되는 현상이며, 공격자는 이를 악용하여 주변 데이터나 실행 흐름에 영향을 주는 정보를 덮어쓸 수 있다. 그 결과 프로그램이 중단되거나 의도하지 않은 동작을 하게 된다.

예를 들어 8바이트 크기의 버퍼에 경계 검사 없이 12바이트를 기록하면, 용량을 초과한 4바이트가 인접한 메모리에 기록되어 기존 내용을 손상시킬 수 있다. 문제에서 메모리 영역에 비정상적인 데이터를 채워 정상 동작을 방해한다는 설명은 이러한 버퍼 오버플로의 작동 방식에 해당한다.

NoteBase

문 13. 시스템과 관련한 보안기능 중 적절한 권한을 가진 사용자를 식별하기 위한 인증 관리로 옳은 것은?

① 세션 관리

② 로그 관리

③ 취약점 관리

④ 계정 관리

정답 4번

간단한 해설

사용자별 계정과 인증정보를 관리하여 시스템 이용자의 신원을 확인하는 기능은 **계정 관리**이다. 사용자 ID로 계정을 식별하고 비밀번호 등의 인증정보로 본인 여부를 확인한다.

공통 해설

시스템에서 사용자를 인증하려면 **사용자를 구별하는 계정과 그 계정에 연결된 인증정보**가 필요하다. 계정 관리는 사용자 계정의 생성·변경·삭제와 함께 인증정보 및 계정별 권한을 관리하는 기능이다. 발문에서 묻는 사용자 식별과 인증은 이러한 계정을 바탕으로 이루어진다.

예를 들어 로그인할 때 ID는 어떤 계정을 사용하는지 식별하는 데 쓰이고, 비밀번호는 그 계정의 사용자 본인인지 확인하는 데 쓰인다. 이처럼 사용자와 인증정보를 연결하여 관리하는 계정 관리가 발문의 인증 관리에 해당한다.

NoteBase

문 14. 무선랜을 보호하기 위한 기술이 아닌 것은?

① WiFi Protected Access Enterprise

② WiFi Rogue Access Points

③ WiFi Protected Access

④ Wired Equivalent Privacy

정답 2번

간단한 해설

WiFi Rogue Access Points는 **허가되지 않은 무선 접속점**을 뜻한다. 무선랜을 보호하는 보안 방식이 아니라 무단 접속이나 통신 탈취를 초래할 수 있는 위협 요소이다.

공통 해설

무선랜 보호 기술은 무선 구간의 데이터를 암호화하거나 접속 사용자를 인증하여 도청과 무단 이용을 막기 위한 방식이다. WiFi Protected Access(WPA), 그 기업용 방식인 WPA Enterprise, Wired Equivalent Privacy(WEP)는 모두 이러한 **보호 목적으로 마련된 보안 방식**에 속한다. WEP는 보안상 취약점이 있지만, 취약하다는 사실이 보호 기술이라는 분류 자체를 바꾸지는 않는다.

반면 WiFi Rogue Access Points의 'rogue'는 관리자의 허가를 받지 않았다는 뜻이며, AP는 단말이 무선으로 접속하는 접속점이다. 따라서 Rogue AP는 **허가되지 않은 무선 접속점**을 가리킨다. 공격자가 정상 접속점처럼 꾸민 Rogue AP에 사용자가 연결하면, 공격자는 그 통신을 가로채거나 변조할 수 있다. 이는 보호 기능을 제공하는 보안 방식이 아니라 탐지하고 차단해야 할 위협 요소이다.

NoteBase

문 15. 다음 정보통신 관계 법률의 목적에 대한 설명으로 옳지 않은 것은?

① 「정보통신기반 보호법」은 전자적 침해행위에 대비하여 주요정보통신기반시설의 보호에 관한 대책을 수립·시행함으로써 동 시설을 안정적으로 운영하도록 하여 국가의 안전과 국민 생활의 안정을 보장하는 것을 목적으로 한다.

② 「전자서명법」은 전자문서의 안전성과 신뢰성을 확보하고 그 이용을 활성화하기 위하여 전자서명에 관한 기본적인 사항을 정함으로써 국가사회의 정보화를 촉진하고 국민생활의 편익을 증진함을 목적으로 한다.

③ 「통신비밀보호법」은 통신 및 대화의 비밀과 자유에 대한 제한은 그 대상을 한정하고 엄격한 법적절차를 거치도록 함으로써 통신비밀을 보호하고 통신의 자유를 신장함을 목적으로 한다.

④ 「정보통신산업 진흥법」은 정보통신망의 이용을 촉진하고 정보통신서비스를 이용하는 자의 개인정보를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성하여 국민생활의 향상과 공공복리의 증진에 이바지함을 목적으로 한다.

정답 4번

간단한 해설

④에 제시된 정보통신망 이용 촉진·개인정보 보호·안전한 이용환경 조성은 **구 정보통신망법의 목적**이다. 정보통신산업 진흥법은 **산업 진흥의 기반 조성과 경쟁력 강화**를 통해 국민경제의 발전에 이바지하려는 법이다.

선지별 해설

① O: 정보통신기반 보호법 제1조는 전자적 침해행위에 대비한 **주요정보통신기반시설의 보호**를 규정한다. 보호대책을 수립·시행하여 시설을 안정적으로 운용하고, 이를 통해 국가의 안전과 국민생활의 안정을 보장하려는 것이다.

② O: 전자서명법 제1조는 **전자문서의 안전성과 신뢰성 확보 및 이용 활성화**를 위해 전자서명에 관한 기본 사항을 정한다. 이를 통해 국가와 사회의 정보화를 촉진하고 국민생활의 편익을 증진하는 것이 목적이므로, 선지의 법률과 목적이 올바르게 연결되어 있다.

③ O: 통신비밀보호법 제1조는 통신·대화의 비밀과 자유를 제한할 때 **대상을 한정하고 엄격한 법적 절차를 거치도록** 한다. 제한의 범위와 절차를 엄격히 통제함으로써 통신비밀을 보호하고 통신의 자유를 신장하려는 것이다.

④ X: 정보통신산업 진흥법 제1조의 목적은 **정보통신산업의 진흥을 위한 기반을 조성**하여 산업의 경쟁력을 강화하고 국민경제의 발전에 이바지하는 것이다. 선지의 정보통신망 이용 촉진·이용자 개인정보 보호·건전하고 안전한 이용환경 조성은 구 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제1조의 목적이다. 따라서 선지의 법률명을 해당 정보통신망법으로 바꾸어야 한다.

NoteBase

문 16. 위험분석 및 평가방법론 중 성격이 다른 것은?

① 확률 분포법

② 시나리오법

③ 순위결정법

④ 델파이법

정답 1번

간단한 해설

확률 분포법은 발생 가능성과 손실 규모 등을 확률분포로 나타내어 위험을 수치로 추정하는 **정량적 분석방법**이다. 다른 방법들은 상황에 대한 판단, 상대적 우선순위, 전문가 의견을 중심으로 평가하는 정성적 분석방법에 속한다.

선지별 해설

비교 기준은 위험을 수치로 계량하는 정량적 방법인지, 판단과 상대적 평가를 중심으로 하는 정성적 방법인지이다. 단순히 숫자를 사용한다는 사실만으로 정량적 방법이 되는 것은 아니다.

① 확률 분포법: **정량적 분석방법**이다. 사건의 발생 가능성이나 손실 규모의 불확실성을 확률분포로 표현하고, 이를 이용하여 예상 손실과 위험의 범위 등을 수치로 추정한다.

② 시나리오법: 정성적 분석방법이다. 특정 조건에서 위협이 발생했을 때 어떤 결과가 이어질지 가능한 상황을 구성하여 평가한다. 이 문항에서의 분류 기준은 **발생 가능한 상황과 결과에 대한 판단**을 중심으로 한다는 점이다.

③ 순위결정법: 정성적 분석방법이다. 위협이나 위험 항목들을 서로 비교하여 **상대적 우선순위**를 정한다. 1위·2위처럼 번호를 붙여도 그것은 순서를 나타낼 뿐, 손실 규모나 발생확률 자체를 계량한 값은 아니다.

④ 델파이법: 정성적 분석방법이다. 관련 전문가들의 의견을 반복하여 수집하고 그 결과를 피드백하여 위험에 대한 판단을 수렴한다. 평가의 중심이 확률모형에 따른 계량보다 **전문가의 지식과 경험에 근거한 판단**에 있다.

따라서 나머지 세 방법과 달리 정량적 분석방법에 해당하는 것은 ①의 확률 분포법이다.

NoteBase

문 17. 보안 침해 사고에 대한 설명으로 옳은 것은?

① 크라임웨어는 온라인상에서 해당 소프트웨어를 실행하는 사용자가 알지 못하게 불법적인 행동 및 동작을 하도록 만들어진 프로그램을 말한다.

② 스니핑은 적극적 공격으로 백도어 등의 프로그램을 사용하여 네트워크상의 남의 패킷 정보를 도청하는 해킹 유형의 하나이다.

③ 파밍은 정상적으로 사용자들이 접속하는 도메인 이름과 철자가 유사한 도메인 이름을 사용하여 위장 홈페이지를 만든 뒤 사용자로 하여금 위장된 사이트로 접속하도록 한 후 개인 정보를 빼내는 공격 기법이다.

④ 피싱은 해당 사이트가 공식적으로 운영하고 있던 도메인 자체를 탈취하는 공격 기법이다.

정답 1번

간단한 해설

크라임웨어는 **사용자 몰래 범죄 행위를 수행하도록 만든 악성 프로그램**이다. 로그인 정보나 금융정보를 훔치는 프로그램이 대표적인 예이다.

선지별 해설

① O: 크라임웨어는 정보 탈취나 금융 사기 등 **온라인 범죄를 수행하기 위해 제작된 악성 프로그램**을 말한다. 사용자가 모르는 사이에 입력한 계정 정보를 수집해 공격자에게 보내는 프로그램이 이에 해당한다.

② X: 스니핑은 네트워크를 흐르는 패킷을 가로채 내용을 엿듣는 행위이다. 통신 내용을 변경하지 않고 수집하는 도청 자체는 **소극적 공격**으로 분류한다. 패킷 수집에는 스니퍼를 사용하며, 비인가 접근 통로를 만드는 백도어가 필수인 것은 아니다.

③ X: 정상 사이트와 철자가 비슷한 도메인으로 위장 사이트를 만들고 개인정보를 입력하도록 속이는 것은 **피싱에 이용되는 방식**이다. 파밍은 DNS 정보나 사용자 컴퓨터의 hosts 파일 등을 조작하여, 사용자가 정상 주소를 입력해도 가짜 사이트로 연결되게 하는 공격이다. 주소의 유사성으로 속이는 것과 주소에 대응하는 접속 목적지를 바꾸는 것을 구별해야 한다.

④ X: 피싱은 신뢰할 수 있는 기관이나 사이트를 사칭하여 개인정보·인증정보 등을 제공하도록 속이는 공격이다. 정상 사이트가 사용하던 **도메인 자체의 통제권을 빼앗는 행위는 도메인 하이재킹**이다. 피싱은 유사 도메인의 위장 사이트나 사칭 메시지로도 이루어지므로, 기존 도메인의 탈취를 뜻하지 않는다.

NoteBase

문 18. 다음 설명에 해당하는 것은?

◯ 응용 프로그램이 실행될 때 일종의 가상머신 안에서 실행되는 것처럼 원래의 운영체제와 완전히 독립되어 실행되는 형태를 말한다.
◯ 컴퓨터 메모리에서 애플리케이션 호스트 시스템에 해를 끼치지 않고 작동하는 것이 허락된 보호받는 제한 구역을 가리킨다.

① Whitebox
② Sandbox
③ Middlebox
④ Bluebox

정답 2번

간단한 해설

프로그램을 **격리된 제한 환경**에서 실행하여 호스트 시스템에 대한 접근과 영향을 통제하는 것이 샌드박스(Sandbox)이다.

공통 해설

샌드박스(Sandbox)는 응용 프로그램을 격리하여 실행하고, 프로그램이 접근할 수 있는 메모리·파일 등의 자원을 제한하는 환경이다. 핵심은 프로그램의 동작 범위를 **허용된 영역 안으로 제한**하여 호스트 시스템을 보호하는 데 있다. 예를 들어 파일 접근을 특정 영역으로 제한하면 프로그램이 그 밖의 호스트 파일을 임의로 변경하지 못하게 할 수 있다. 지문의 '가상머신 안에서 실행되는 것처럼'은 실행 환경의 격리를, '보호받는 제한 구역'은 자원 접근의 제한을 나타내므로 두 설명은 모두 샌드박스의 특징이다.

NoteBase

문 19. 각 주체가 각 객체에 접근할 때마다 관리자에 의해 사전에 규정된 규칙과 비교하여 그 규칙을 만족하는 주체에게만 접근 권한을 부여하는 기법은?

① Mandatory Access Control
② Discretionary Access Control
③ Role Based Access Control
④ Reference Monitor

정답 1번

간단한 해설

관리자가 사전에 정한 규칙을 시스템이 강제하여, 조건을 충족한 주체에게만 접근을 허용하는 방식은 **강제적 접근 통제(MAC)**이다. 핵심은 개별 사용자의 재량이 아니라 **중앙에서 정한 보안 정책**에 따라 접근 여부가 결정된다는 점이다.

개념 구분

강제적 접근 통제(Mandatory Access Control, MAC): 주체는 접근을 요청하는 사용자나 프로세스이고, 객체는 파일처럼 보호할 자원이다. MAC은 중앙의 관리 권한으로 정한 보안 정책을 주체와 객체에 일관되게 적용한다. 일반 사용자는 자신의 재량으로 접근 규칙을 바꾸거나 다른 사용자에게 권한을 넘길 수 없다. 문제의 '관리자에 의해 사전에 규정된 규칙'은 이러한 **중앙 정책의 강제 적용**을 가리킨다.

임의적 접근 통제(Discretionary Access Control, DAC): 객체의 소유자 등 접근 권한을 관리할 권한이 있는 사람이 **자신의 재량으로 접근 권한을 설정**한다. 소유자가 다른 사용자에게 파일 읽기 권한을 부여하는 경우가 이에 해당하며, 중앙 정책이 사용자의 재량을 제한하는 MAC과 구별된다.

역할 기반 접근 통제(Role Based Access Control, RBAC): 권한을 역할에 연결하고, 사용자가 맡은 **역할에 따라 권한을 부여**한다. 관리자도 역할과 권한을 설정할 수 있지만, 이 방식을 특정하려면 직무나 역할에 따른 권한 배정이라는 단서가 필요하다. 문제는 역할 배정보다 사전에 정한 규칙의 강제 적용을 설명한다.

참조 모니터(Reference Monitor): 주체의 객체 접근을 매번 중재하여 보안 정책을 집행하는 추상적 보안 메커니즘이다. '접근할 때마다 검사한다'는 부분과 관련되지만, **정책을 집행하는 메커니즘**과 접근 권한을 결정하는 정책 방식은 구별해야 한다. 문제에서 관리자가 미리 정한 규칙에 따라 권한을 부여하는 정책 방식은 MAC이다.

NoteBase

문 20. 임의로 발생시킨 데이터를 프로그램의 입력으로 사용하여 소프트웨어의 안전성 및 취약성 등을 검사하는 방법은?

① Reverse Engineering
② Canonicalization
③ Fuzzing
④ Software Prototyping

정답 3번

간단한 해설

임의로 만든 데이터를 프로그램에 입력하여 오류나 비정상 종료가 발생하는지 검사하는 방법은 **퍼징(Fuzzing)**이다.

공통 해설

퍼징(Fuzzing)은 **임의로 생성하거나 변형한 입력 데이터**를 프로그램에 넣고 실행 결과를 관찰하여 결함과 보안 취약점을 찾는 시험 기법이다. 입력을 처리하는 과정에서 예외, 비정상 종료, 메모리 오류 등이 발생하는지 살핀다. 문제의 핵심은 프로그램을 실제로 실행하면서 임의의 입력에 대한 반응을 검사한다는 점이다.

예를 들어 파일을 읽는 프로그램에 내용이나 길이를 임의로 바꾼 파일을 입력하고, 프로그램이 오류를 적절히 처리하는지 또는 비정상 종료하는지 확인할 수 있다. 이처럼 예상하지 못한 입력에 대한 처리 결함을 드러내는 방식이 퍼징이다.

NoteBase