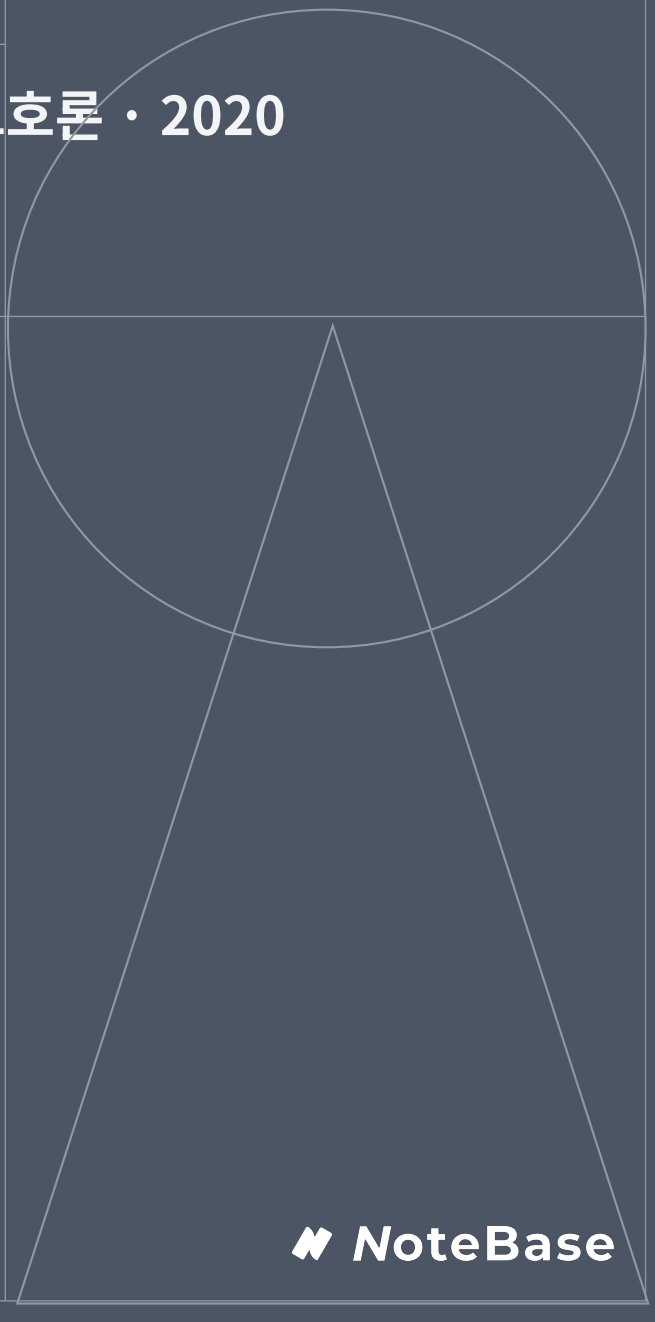
기출OX 해설집

공무원/국가직/9급 · 정보보호론 · 2020



NoteBase

기출OX 해설집

공무원/국가직/9급 · 정보보호론 · 2020

공무원/국가직/9급 · 정보보호론 · 2020

문 1. 정보보호 위험관리에 대한 설명으로 옳지 않은 것은?

① 자산은 조직이 보호해야 할 대상으로 정보, 하드웨어, 소프트웨어, 시설 등이 해당한다.

② 위험은 자산에 손실이 발생할 가능성과 관련되어 있으나 이로 인한 부정적인 영향을 미칠 가능성과는 무관하다.

③ 취약점은 자산이 잠재적으로 가진 약점을 의미한다.

④ 정보보호대책은 위협에 대응하여 자산을 보호하기 위한 관리적, 기술적, 물리적 대책을 의미한다.

정답 2번

간단한 해설

②의 '부정적인 영향을 미칠 가능성과는 무관하다'는 설명이 잘못되었다. 위험은 손실을 일으키는 사건의 **발생 가능성**과 그 사건이 초래할 **부정적 영향의 크기**를 함께 고려한다.

선지별 해설

① O: 자산은 조직에 가치가 있어 **보호해야 할 대상**이다. 정보 자체뿐 아니라 정보를 저장·처리하는 하드웨어와 소프트웨어, 이를 수용하는 시설도 포함한다. 따라서 자산은 디지털 정보에만 한정되지 않는다.

② X: 위험은 위협이 취약점을 이용하여 자산에 손실을 일으킬 가능성과 관련된다. 위험을 평가할 때는 **발생 가능성과 부정적 영향의 크기를 함께 고려**하므로, 부정적 영향과 무관하다는 부분을 고쳐야 한다. 예를 들어 사고가 발생할 가능성이 같더라도 핵심 업무를 중단시키는 사고와 영향이 작은 사고는 위험 수준이 다를 수 있다.

③ O: 취약점은 위협에 의해 악용될 수 있는 **자산이나 보호체계의 약점**이다. 보안 패치가 적용되지 않은 소프트웨어나 미흡한 출입통제 등이 이에 해당한다. 취약점은 약점 자체이고, 이를 악용하여 피해를 줄 수 있는 요인은 위협이라는 점에서 구별된다.

④ O: 정보보호대책은 위협에 대응하여 자산을 보호하고 위험을 줄이기 위한 수단이다. 보안정책 수립과 교육은 **관리적 대책**, 접근통제와 암호화는 **기술적 대책**, 잠금장치와 출입구 경비는 물리적 대책에 해당한다.

NoteBase

문 2. 공개키 암호화에 대한 설명으로 옳지 않은 것은?

① ECC(Elliptic Curve Cryptography)와 Rabin은 공개키 암호 방식이다.

② RSA는 소인수 분해의 어려움에 기초를 둔 알고리즘이다.

③ 전자서명 할 때는 서명하는 사용자의 공개키로 암호화한다.

④ ElGamal은 이산대수 문제의 어려움에 기초를 둔 알고리즘이다.

정답 3번

간단한 해설

전자서명은 **서명자의 개인키로 생성**하고, 대응하는 **공개키로 검증**한다. ③은 서명 생성에 사용하는 키를 공개키로 잘못 설명했다.

선지별 해설

① O: ECC와 Rabin은 공개키와 개인키를 구분하여 사용하는 **비대칭키 암호 방식**이다. ECC는 타원곡선 위의 이산대수 문제를, Rabin은 큰 정수의 소인수분해 문제를 기반으로 한다.

② O: RSA는 **큰 정수의 소인수분해가 어렵다는 성질**에 기초한다. 충분히 큰 두 소수를 곱하여 공개키에 쓰이는 정수를 만드는 것은 쉽지만, 그 정수만으로 원래 두 소수를 알아내기는 어렵다. 두 소수를 알면 개인키를 계산할 수 있으므로 이들을 비밀로 유지해야 한다.

③ X: 전자서명은 **서명자의 개인키로 생성하고 공개키로 검증**한다. 일반적으로 메시지의 해시값에 서명 알고리즘을 적용하며, 검증자는 서명자의 공개키를 이용해 메시지의 변경 여부와 서명자를 확인한다. 따라서 '서명하는 사용자의 공개키로 암호화한다'는 '서명하는 사용자의 개인키로 서명을 생성한다'로 고쳐야 한다. 기밀성을 위한 공개키 암호화에서는 수신자의 공개키로 암호화한다는 점과 구별해야 한다.

④ O: ElGamal은 **이산대수 문제의 어려움**에 기초한다. 정해진 유한한 군에서 거듭제곱의 결과를 구하는 것은 쉽지만, 밑과 결과만으로 지수를 알아내기는 어렵다는 성질을 이용한다. 개인키를 지수로 사용해 공개키를 만들므로, 공개키만으로 개인키를 구하기 어렵다.

NoteBase

문 3. X.509 인증서 형식 필드에 대한 설명으로 옳은 것은?

① Issuer name – 인증서를 사용하는 주체의 이름과 유효기간 정보

② Subject name – 인증서를 발급한 인증기관의 식별 정보

③ Signature algorithm ID – 인증서 형식의 버전 정보

④ Serial number – 인증서 발급 시 부여된 고유번호 정보

정답 4번

간단한 해설

Serial number는 인증기관이 인증서를 발급할 때 부여하는 **인증서 일련번호**이다. 같은 인증기관이 발급한 인증서 사이에서 중복되지 않아 개별 인증서를 구별한다.

선지별 해설

① X: Issuer name은 **인증서를 발급한 인증기관의 이름**을 나타낸다. 인증서의 주체 이름은 Subject name에, 유효기간은 별도의 Validity 필드에 기록한다.

② X: Subject name은 인증서에 담긴 **공개키와 연결된 주체의 이름**을 나타낸다. 인증서를 발급한 인증기관의 식별 정보는 Issuer name에 기록한다. 즉, Subject는 인증 대상이고 Issuer는 발급자이다.

③ X: Signature algorithm ID는 인증기관이 **인증서에 전자서명할 때 사용한 알고리즘의 식별 정보**이다. 인증서 형식의 버전 정보는 Version 필드에 기록한다.

④ O: Serial number는 인증기관이 인증서 발급 시 부여하는 일련번호이다. **같은 인증기관이 발급한 인증서마다 고유**해야 하며, 발급자 이름과 일련번호를 함께 사용하면 개별 인증서를 식별할 수 있다.

NoteBase

문 4. 일방향 해시함수를 사용하여 비밀번호를 암호화할 때 salt라는 난수를 추가하는 이유는?

① 비밀번호 사전공격(Dictionary attack)에 취약한 문제를 해결할 수 있다.

② 암호화된 비밀번호 해시 값의 길이를 줄일 수 있다.

③ 비밀번호 암호화의 수행 시간을 줄일 수 있다.

④ 비밀번호의 복호화를 빠르게 수행할 수 있다.

정답 1번

간단한 해설

salt는 비밀번호와 함께 해시하는 난수로, **미리 계산한 비밀번호 해시 사전을 재사용하기 어렵게** 한다.
사용자마다 다른 salt를 쓰면 공격자는 각 salt에 맞춰 후보 비밀번호의 해시를 다시 계산해야 한다.

핵심 풀이

salt의 역할: 비밀번호를 저장할 때 사용자마다 서로 다른 난수를 비밀번호와 함께 해시한다. 예를 들어 두 사용자의 비밀번호가 모두 'apple'이어도 salt가 다르면 해시 입력이 달라진다. 이렇게 사용자별로 입력을 달리하여 같은 비밀번호의 해시 계산 결과가 여러 계정에 공통으로 이용되는 것을 막는다.

사전공격 방어 원리: 사전공격은 자주 쓰는 단어 등을 비밀번호 후보로 대입하는 공격이다. salt가 없으면 후보별 해시를 미리 계산해 두고 여러 사용자의 저장된 해시와 비교할 수 있다. 서로 다른 salt를 추가하면 **각 salt마다 후보들의 해시를 다시 계산**해야 하므로 기존의 사전 계산표나 레인보 테이블을 그대로 재사용하기 어렵다. ①의 취약점 해결은 이러한 공격 효율을 낮춘다는 의미이다. 다만 salt를 아는 공격자가 후보를 하나씩 대입하는 사전공격까지 완전히 불가능해지는 것은 아니다.

길이·속도·복호화와의 구분: salt는 해시 길이를 줄이거나 해시 수행 시간을 단축하기 위한 수단이 아니다. 같은 해시함수의 출력 길이는 salt를 추가해도 그 함수의 출력 규격을 따른다. 또한 일방향 해시는 **복호화로 원래 비밀번호를 되찾는 방식이 아니다**. 로그인할 때는 입력한 비밀번호와 저장된 salt로 해시를 다시 계산해 저장된 값과 비교한다.

NoteBase

문 5. 윈도우 운영체제에서 TPM(Trusted Platform Module)에 대한 설명으로 옳지 않은 것은?

① TPM의 공개키를 사용하여 플랫폼 설정정보에 서명함으로써 디지털 인증을 생성한다.

② TPM은 신뢰 컴퓨팅 그룹(Trusted Computing Group)에서 표준화된 개념이다.

③ TPM은 키 생성, 난수 발생, 암복호화 기능 등을 포함한 하드웨어 칩 형태로 구현할 수 있다.

④ TPM의 기본 서비스에는 인증된 부트(authenticated boot), 인증, 암호화가 있다.

정답 1번

간단한 해설

플랫폼 설정정보의 무결성을 증명하는 전자서명은 TPM이 보호하는 **개인키로 생성**하고, 대응하는 **공개키로 검증**한다. 공개키로 서명한다는 설명은 두 키의 역할을 바꾼 것이다.

선지별 해설

① X: 플랫폼 설정정보에 대한 전자서명은 TPM이 보호하는 서명용 **개인키로 생성**한다. 검증자는 대응하는 공개키로 서명을 확인하여 정보의 출처와 무결성을 검증한다. TPM은 플랫폼 구성 레지스터(PCR)에 기록된 측정값을 바탕으로 서명된 증명 정보를 제공하므로, 선지의 '공개키를 사용하여 … 서명'은 '개인키를 사용하여 … 서명'으로 고쳐야 한다.

② O: TPM은 **신뢰 컴퓨팅 그룹(TCG)이 표준화**한 보안 모듈이다. TCG는 TPM의 구조, 명령, 암호 기능 등의 규격을 정하여 서로 다른 제조사의 구현에서도 공통된 보안 기능을 사용할 수 있도록 한다.

③ O: TPM은 암호 연산을 수행하는 **하드웨어 칩 형태로 구현할 수 있다**. 암호키 생성과 보호, 난수 발생, 암호화·복호화 등의 기능을 제공하며, 보호된 환경에서 키를 사용하는 것이 핵심이다.

④ O: TPM은 **인증된 부트, 인증, 암호화**를 지원한다. 인증된 부트에서는 부팅 과정에서 실행되는 구성요소의 측정값을 TPM에 기록하여 부팅 상태를 확인할 근거를 남긴다. 인증에서는 키와 전자서명으로 장치의 신원이나 플랫폼 상태를 증명하고, 암호화에서는 키를 보호하고 암호 연산을 지원하여 데이터의 기밀성을 지키는 데 사용된다.

NoteBase

문 6. 키 k에 대한 블록 암호 알고리즘 E_k, 평문블록 M_i, Z_0는 초기벡터, $Z_i = E_k(Z_{i-1})$가 주어진 경우, 이때 $i = 1, 2, \ldots, m$에 대해 암호블록 C_i를 $C_i = Z_i \oplus M_i$로 계산하는 운영모드는? (단, $\oplus$는 배타적 논리합이다)

① CBC

② ECB

③ OFB

④ CTR

정답 3번

간단한 해설

블록 암호의 **이전 출력값을 다음 입력으로 되돌려** 키스트림을 만들고, 이를 평문과 XOR하여 암호문을 얻는 방식은 **OFB(출력 피드백)**이다. 피드백되는 값은 평문과 결합하기 전의 암호화 출력이다.

구성 요소별 해설

초기벡터 Z_0: 키스트림 생성을 시작하는 입력이다. 이를 키 k로 암호화하여 첫 출력 블록 $Z_1 = E_k(Z_0)$를 얻는다.

출력 피드백 $Z_i = E_k(Z_{i-1})$: 직전 출력 블록을 다시 암호화하여 다음 출력 블록을 만든다. 예를 들어 $Z_2 = E_k(Z_1)$이므로 첫 암호블록 C_1이 아니라 **암호화 출력** Z_1 **자체**가 다음 입력으로 쓰인다. 이 과정에는 평문이 들어가지 않아 평문과 독립적으로 키스트림을 생성한다.

평문과의 결합 $C_i = Z_i \oplus M_i$: 생성한 키스트림 블록과 같은 위치의 평문블록을 XOR하여 암호블록을 만든다. 즉, 블록 암호는 키스트림을 생성하고 **평문과의 XOR은 그 뒤에** 수행된다.

이러한 구성은 출력 피드백 모드인 OFB이며, ③에 해당한다. ECB는 평문블록을 직접 암호화하고, CBC는 평문과 이전 암호블록을 XOR한 결과를 암호화한다. CTR은 키스트림을 생성할 때 이전 출력 대신 카운터 블록을 암호화한다.

NoteBase

문 7. 정보보호 시스템 평가 기준에 대한 설명으로 옳은 것은?

① ITSEC의 레인보우 시리즈에는 레드 북으로 불리는 TNI (Trusted Network Interpretation)가 있다.

② ITSEC은 None부터 B2까지의 평가 등급으로 나눈다.

③ TCSEC의 EAL2 등급은 기능시험 결과를 의미한다.

④ TCSEC의 같은 등급에서는 뒤에 붙는 숫자가 클수록 보안 수준이 높다.

정답 4번

간단한 해설

TCSEC에서는 같은 문자로 구분되는 범주 안에서 **뒤에 붙는 숫자가 클수록 보안 요구 수준이 높다**. C1보다 C2가, B1보다 B2·B3가 더 높은 수준이다.

선지별 해설

① X: 레인보우 시리즈는 ITSEC이 아니라 **TCSEC과 그 관련 문서**를 가리킨다. 이 가운데 TNI(Trusted Network Interpretation)는 TCSEC을 네트워크 환경에 적용하여 해석한 문서이며, 표지 색에 따라 '레드 북'으로 불린다.

② X: ITSEC의 평가 등급은 None부터 B2까지가 아니라 **E0부터 E6까지**이다. ITSEC은 보안 기능과 보증을 구분하며, E 등급은 평가 대상이 요구한 대로 올바르게 구현되었는지에 대한 신뢰 수준을 나타낸다.

③ X: EAL은 TCSEC이 아니라 **공통평가기준(CC)의 평가보증등급**이다. CC에서 기능 시험을 의미하는 등급은 EAL1이며, EAL2는 구조적 시험을 의미한다. 따라서 평가 기준의 명칭과 등급의 의미가 모두 잘못 연결되어 있다.

④ O: TCSEC은 D·C·B·A의 큰 범주로 나누고, 일부 범주를 숫자로 세분한다. **같은 문자 범주에서는 숫자가 커질수록** 더 높은 보안 요구를 충족해야 하므로 C1보다 C2가 높고, B1·B2·B3 순으로 수준이 높아진다. 선지의 '같은 등급'은 이러한 같은 문자 범주를 뜻한다.

NoteBase

문 8. SSL(Secure Socket Layer)의 Handshake 프로토콜에서 클라이언트와 서버 간에 논리적 연결 수립을 위해 클라이언트가 최초로 전송하는 ClientHello 메시지에 포함되는 정보가 아닌 것은?

① 세션 ID

② 클라이언트 난수

③ 압축 방법 목록

④ 인증서 목록

정답 4번

간단한 해설

인증서 목록은 ClientHello가 아니라 **별도의 Certificate 메시지**에 포함된다. ClientHello는 보안 연결에 사용할 조건을 협의하기 위한 정보를 먼저 보내는 메시지이다.

핵심 풀이

ClientHello: 클라이언트가 연결에 사용할 조건을 알리는 메시지로, SSL 버전, 클라이언트 난수, 세션 ID, 암호 스위트 목록, 압축 방법 목록을 포함한다. 세션 ID는 기존 세션의 재개를 요청할 때 사용하며, 새 세션을 만들 때는 이 필드를 비워 둘 수 있다. 압축 방법 목록은 이미 확정된 한 가지 방법이 아니라 **클라이언트가 지원하는 방법들의 목록**이다.

Certificate: 인증에 필요한 인증서 목록을 전달하는 별도의 Handshake 메시지이다. 서버 인증을 수행하는 경우 서버는 ServerHello 다음에 자신의 인증서를 보낸다. 따라서 ④의 인증서 목록은 **ClientHello의 구성 정보가 아니다**. 보안 조건을 제안하는 ClientHello와 인증서를 전달하는 Certificate의 역할을 구분해야 한다.

NoteBase

문 9. 「개인정보 보호법」 상 기본계획에 대한 조항의 일부이다. ㉠, ㉡에 들어갈 내용을 바르게 연결한 것은?

제9조(기본계획) ① 보호위원회는 개인정보의 보호와 정보주체의 권익 보장을 위하여 (㉠)년마다 개인정보 보호 기본계획(이하 “기본계획”이라 한다)을 관계 중앙행정기관의 장과 협의하여 수립한다.
② 기본계획에는 다음 각 호의 사항이 포함되어야 한다.
1. 개인정보 보호의 기본목표와 추진방향
2. 개인정보 보호와 관련된 제도 및 법령의 개선
3. 개인정보 침해 방지를 위한 대책
4. (㉡)
5. 개인정보 보호 교육·홍보의 활성화
6. 개인정보 보호를 위한 전문인력의 양성
7. 그 밖에 개인정보 보호를 위하여 필요한 사항

① ㉠: 1, ㉡: 개인정보 보호 자율규제의 활성화

② ㉠: 3, ㉡: 개인정보 보호 자율규제의 활성화

③ ㉠: 1, ㉡: 개인정보 활용·폐지를 위한 계획

④ ㉠: 3, ㉡: 개인정보 활용·폐지를 위한 계획

정답 2번

㉠

보호위원회가 관계 중앙행정기관의 장과 협의하여 **3년마다** 개인정보 보호 기본계획을 수립한다.

개인정보 보호법 제9조(기본계획)
① 보호위원회는 개인정보의 보호와 정보주체의 권익 보장을 위하여 3년마다 개인정보 보호 기본계획(이하 "기본계획"이라 한다)을 관계 중앙행정기관의 장과 협의하여 수립한다. <개정 2013.3.23, 2014.11.19, 2015.7.24>

NoteBase

ㄴ

기본계획에는 **기본목표·추진방향, 제도·법령 개선, 침해 방지 대책**뿐 아니라 **자율규제 활성화, 교육·홍보 활성화, 전문인력 양성** 및 그 밖에 개인정보 보호에 필요한 사항도 포함해야 한다.

개인정보 보호법 제9조(기본계획)
② 기본계획에는 다음 각 호의 사항이 포함되어야 한다.
1. 개인정보 보호의 기본목표와 추진방향
2. 개인정보 보호와 관련된 제도 및 법령의 개선
3. 개인정보 침해 방지를 위한 대책
4. 개인정보 보호 자율규제의 활성화
5. 개인정보 보호 교육 · 홍보의 활성화
6. 개인정보 보호를 위한 전문인력의 양성
7. 그 밖에 개인정보 보호를 위하여 필요한 사항

NoteBase

문 10. 소수 $p = 13$, 원시근 $g = 2$, 사용자 A와 B의 개인키가 각각 3, 2일 때, Diffie-Hellman 키 교환 알고리즘을 사용하여 계산한 공유 비밀키는?

① 6

② 8

③ 12

④ 16

정답 3번

간단한 해설

공유 비밀키는 **상대방의 공개값을 자신의 개인키만큼 거듭제곱한 뒤 p로 나눈 나머지**이다. 두 사용자는 모두 2^3· 2 13을 얻게 되므로 공유 비밀키는 12이다.

계산 과정

주어진 값은 소수 p = 13, 원시근 g = 2이며, A와 B의 개인키를 각각 a = 3, b = 2로 둔다. Diffie-Hellman에서는 공개된 p와 g를 이용하여 거듭제곱을 계산하고, mod p 연산으로 p로 나눈 나머지를 구한다.

공개값 계산: 각 사용자는 g를 자신의 개인키만큼 거듭제곱한 나머지를 상대방에게 보낸다. A의 공개값은 Y_A=g^a p=2^3 13=8, B의 공개값은 Y_B=g^b p=2^2 13=4이다. 이 8과 4는 **교환하는 공개값**이며, 아직 공유 비밀키가 아니다.

공유 비밀키 계산: A는 B에게 받은 공개값 4에 자신의 개인키 3을 지수로 적용한다. 따라서 K=Y_B^a p=4^3 13이다. 64 = 13 × 4 + 12이므로 K = 12이다. B도 Y_A^b p=8^2 13=12를 얻는다. 두 계산은 모두 g^ab p이므로 **같은 공유 비밀키**가 만들어진다.

계산한 공유 비밀키 12는 ③의 값과 일치한다.

NoteBase

문 11. NIST의 AES(Advanced Encryption Standard) 표준에 따른 암호화 시 암호키(cipher key) 길이가 256비트일 때 필요한 라운드 수는?

① 8

② 10

③ 12

④ 14

정답 4번

간단한 해설

AES는 암호키 길이에 따라 라운드 수가 달라지며, **256비트 키에는 14라운드**를 적용한다.

핵심 풀이

AES 표준은 암호키 길이가 128비트이면 10라운드, 192비트이면 12라운드, 256비트이면 14라운드로 정한다. 문제에서 주어진 암호키는 256비트이므로 **AES-256의 14라운드**를 적용한다.

암호키 길이와 블록 길이는 구별해야 한다. 암호키 길이는 비밀키의 크기이고, 블록 길이는 한 번에 암호화하는 데이터 묶음의 크기이다. AES의 블록 길이는 키 길이와 관계없이 **128비트로 고정**되므로, 블록 길이를 기준으로 10라운드를 선택해서는 안 된다.

NoteBase

문 12. IPsec의 ESP(Encapsulating Security Payload)에 대한 설명으로 옳지 않은 것은?

① 인증 기능을 포함한다.

② ESP는 암호화를 통해 기밀성을 제공한다.

③ 전송 모드의 ESP는 IP 헤더를 보호하지 않으며, 전송계층으로부터 전달된 정보만을 보호한다.

④ 터널 모드의 ESP는 Authentication Data를 생성하기 위해 해시 함수와 공개키를 사용한다.

정답 4번

간단한 해설

④의 '공개키'는 **공유 비밀키**로 고쳐야 한다. ESP에서 HMAC으로 인증 데이터를 생성할 때는 해시 함수와 통신 양쪽이 공유하는 비밀키를 사용하며, 터널 모드에서도 이 원리는 같다.

선지별 해설

① O: ESP는 암호화뿐 아니라 **데이터 출처 인증과 무결성**을 제공하는 기능도 포함한다. 인증을 적용하면 수신자는 공유 비밀키를 이용해 패킷이 통신 상대가 보낸 것인지, 전송 중 변조되지 않았는지 확인한다. 실제 제공되는 서비스는 보안 연관(SA)을 설정할 때 선택한 옵션에 따라 달라진다.

② O: ESP는 **암호화를 통해 기밀성**을 제공한다. 기밀성은 권한 없는 사람이 데이터 내용을 알아보지 못하게 하는 성질이다. 암호화 서비스를 선택하면 보호할 데이터를 암호문으로 바꾸어 전송하므로, 복호화에 필요한 키가 없는 제삼자는 원래 내용을 읽기 어렵다.

③ O: 전송 모드에서는 원래 IP 헤더 뒤에 ESP 헤더를 삽입하고, TCP·UDP 헤더와 데이터 등 그 뒤의 내용을 보호한다. 따라서 **원래 IP 헤더는 ESP의 보호 범위에 포함되지 않는다**. 이와 달리 터널 모드에서는 원래 IP 헤더를 포함한 내부 IP 패킷 전체를 감싸서 보호하고, 그 바깥에 전달용 IP 헤더를 붙인다.

④ X: 해시 기반 인증 데이터를 생성할 때는 HMAC처럼 **해시 함수와 공유 비밀키**를 결합하는 방식을 사용한다. 송신자는 비밀키로 인증값을 계산하고, 수신자는 같은 키로 다시 계산한 값과 수신한 값을 비교하여 변조 여부를 검사한다. 공개키를 사용하는 방식이 아니며, 전송 모드와 터널 모드의 차이는 보호 대상의 범위에 있다.

NoteBase

문 13. 네트워크나 컴퓨터 시스템의 자원 고갈을 통해 시스템 성능을 저하시키는 공격에 해당하는 것만을 모두 고르면?

ㄱ. Ping of Death 공격
ㄴ. Smurf 공격
ㄷ. Heartbleed 공격
ㄹ. Sniffing 공격

① ㄱ, ㄴ
② ㄱ, ㄷ
③ ㄴ, ㄷ
④ ㄴ, ㄹ

정답 1번

간단한 해설

Ping of Death는 비정상적으로 큰 패킷의 처리 오류를, Smurf는 대량의 ICMP 응답으로 인한 자원 소모를 이용하여 **서비스의 가용성**을 침해한다.

NoteBase

보기별 해설

서비스 거부(DoS) 공격은 정상적인 이용자가 네트워크나 시스템의 서비스를 이용하지 못하게 하여 가용성을 침해하는 공격이다.

ㄱ. Ping of Death 공격: **서비스 거부(DoS) 공격**이다. 조각난 IP 패킷을 재조립한 크기가 IPv4의 최대 패킷 크기인 65,535바이트를 초과하도록 조작한다. 취약한 시스템은 이를 처리하는 과정에서 오류나 장애가 발생하여 정상적인 서비스를 제공하지 못할 수 있다.

ㄴ. Smurf 공격: **ICMP 응답을 증폭시키는 서비스 거부 공격**이다. 출발지 IP 주소를 피해자의 주소로 위조한 ICMP Echo Request를 브로드캐스트 주소로 보내면, 이에 응답하는 여러 호스트의 Echo Reply가 피해자에게 집중된다. 이 응답 트래픽이 대역폭과 처리 자원을 소모하여 서비스 성능을 떨어뜨린다.

ㄷ. Heartbleed 공격: **메모리의 정보를 유출하는 공격**이다. OpenSSL의 TLS/DTLS 하트비트 처리에서 길이 검증이 부족한 취약점을 이용하여, 실제로 보낸 데이터의 범위를 넘어 메모리 내용을 응답받는다. 비밀번호나 개인키 같은 민감한 정보가 노출될 수 있으며, 자원 고갈을 통한 성능 저하를 일으키는 서비스 거부 공격으로 분류하지 않는다.

ㄹ. Sniffing 공격: 네트워크를 흐르는 패킷을 수집하여 내용을 엿보는 **도청 공격**이다. 통신 내용을 몰래 알아내어 기밀성을 침해하는 것이므로, 자원을 고갈시켜 서비스를 방해하는 공격과 구별된다.

서비스 거부 공격에 해당하는 것은 ㄱ, ㄴ이며, ①의 조합과 일치한다.

NoteBase

문 14. 다음 설명에 해당하는 위험분석 및 평가 방법을 옳게 짝 지은 것은?

ㄱ. 전문가 집단의 토론을 통해 정보시스템의 취약성과 위협요소를 추정하여 평가하기 때문에 시간과 비용을 절약할 수 있지만, 정확도가 낮다.
ㄴ. 이미 발생한 사건이 앞으로 발생한다는 가정하에 수집된 자료를 통해 위험 발생 가능성을 예측하며, 자료가 많을수록 분석의 정확도가 높아진다.
ㄷ. 어떤 사건도 기대하는 대로 발생하지 않는다는 사실에 근거하여 일정 조건에서 위협에 대해 발생 가능한 결과들을 예측하며, 적은 정보를 가지고 전반적인 가능성을 추론할 수 있다.

① ㄱ: 순위 결정법, ㄴ: 과거자료 분석법, ㄷ: 기준선 접근법
② ㄱ: 순위 결정법, ㄴ: 점수법, ㄷ: 기준선 접근법
③ ㄱ: 델파이법, ㄴ: 과거자료 분석법, ㄷ: 시나리오법
④ ㄱ: 델파이법, ㄴ: 점수법, ㄷ: 시나리오법

정답 3번

간단한 해설

ㄴ은 평가 항목에 점수를 매기는 방법이 아니라, **과거에 발생한 사건 자료**를 근거로 앞으로의 위험 발생 가능성을 예측하는 과거자료 분석법이다. ㄷ은 과거 기록의 반복을 전제하기보다 **일정 조건에서 가능한 결과**를 가정하는 시나리오법이다.

NoteBase

대응 관계 해설

ㄱ. 델파이법: **전문가 집단의 지식과 판단**을 모아 정보시스템의 취약성과 위협요소를 추정하는 방법이다. ㄱ에서 전문가 집단의 토론을 평가 근거로 삼는다는 점이 결정적인 단서이다. 제시문은 전문적 판단을 활용해 시간과 비용을 절약할 수 있지만, 추정에 의존하므로 정확도에 한계가 있다는 특성을 설명한다.

ㄴ. 과거자료 분석법: **과거에 발생한 사건이 앞으로도 발생할 수 있다**는 가정 아래, 수집한 사고 기록으로 위험 발생 가능성을 예측한다. 과거 사건의 발생 양상을 판단 근거로 삼으므로 분석에 활용할 자료가 많아질수록 예측의 정확도를 높일 수 있다. 평가 항목에 점수를 부여하는 점수법과 달리, 여기서 핵심은 이미 발생한 사건 자료를 이용한다는 점이다.

ㄷ. 시나리오법: **일정 조건에서 발생 가능한 위협과 결과**를 가정하여 위험을 추론하는 방법이다. 사건이 예상한 대로만 전개되지는 않는다는 점을 고려하여 여러 가능한 상황을 검토한다. 따라서 충분한 과거 자료가 없더라도 제한된 정보로 전반적인 가능성을 살펴볼 수 있으며, 과거 사건의 반복을 근거로 예측하는 과거자료 분석법과 구별된다.

ㄱ은 델파이법, ㄴ은 과거자료 분석법, ㄷ은 시나리오법으로 대응하므로 ③의 조합과 일치한다.

NoteBase

문 15. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」 제19조(국내대리인 지정 대상자의 범위)에 명시된 자가 아닌 것은?

① 전년도(법인인 경우에는 전(前) 사업연도를 말한다) 매출액이 1,000억 원 이상인 자

② 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억 원 이상인 자

③ 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만 명 이상인 자

④ 이 법을 위반하여 개인정보 침해 사건·사고가 발생하였거나 발생할 가능성이 있는 경우로서 법 제64조제1항에 따라 방송통신위원회로부터 관계 물품·서류 등을 제출하도록 요구받은 자

정답 1, 3, 4번

①

국내대리인 지정 대상의 전년도 매출액 기준은 **1조원 이상**이다. 법인은 전 사업연도 매출액을 기준으로 한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제19조(국내대리인 지정 대상자의 범위)
① 법 제32조의5제1항에서 "대통령령으로 정하는 기준에 해당하는 자"란 다음 각 호의 어느 하나에 해당하는 자를 말한다. <개정 2020.8.4, 2025.10.1>
1. 전년도[법인인 경우에는 전(前) 사업연도를 말한다] 매출액이 1조원 이상인 자

②

정보통신서비스 부문의 전년도 매출액이 100억원 이상인 자는 국내대리인 지정 대상에 해당한다. 법인은 전 사업연도를 기준으로 한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제19조(국내대리인 지정 대상자의 범위)
① 법 제32조의5제1항에서 "대통령령으로 정하는 기준에 해당하는 자"란 다음 각 호의 어느 하나에 해당하는 자를 말한다. <개정 2020.8.4, 2025.10.1>
2. 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 자

NoteBase

③

개인정보 보유 이용자 수가 일일평균 100만명 이상이라는 기준은 정보통신망법상 국내대리인 지정 기준에 포함되지 않는다. 개인정보 보호법상 별도 기준은 전년도 말 직전 3개월간 개인정보를 저장·관리하는 **국내 정보주체의 수가 일일평균 100만명 이상**인 경우이다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제19조(국내대리인 지정 대상자의 범위)
① 법 제32조의5제1항에서 "대통령령으로 정하는 기준에 해당하는 자"란 다음 각 호의 어느 하나에 해당하는 자를 말한다. <개정 2020.8.4, 2025.10.1>
1. 전년도[법인인 경우에는 전(前) 사업연도를 말한다] 매출액이 1조원 이상인 자
2. 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 자
3. 삭제<2020.8.4>
4. 이 법을 위반하여 정보통신서비스 이용의 안전성을 현저히 해치는 사건 · 사고가 발생하였거나 발생할 가능성이 있는 경우로서 법 제64조제1항에 따라 방송미디어통신위원회로부터 관계 물품 · 서류 등을 제출하도록 요구받은 자

개인정보 보호법 시행령 제32조의3(국내대리인 지정 대상자의 범위 등)
① 법 제31조의2제1항 각 호 외의 부분 전단에서 "대통령령으로 정하는 자"란 다음 각 호의 어느 하나에 해당하는 자를 말한다.
2. 전년도 말 기준 직전 3개월 간 그 개인정보가 저장 · 관리되고 있는 국내 정보주체의 수가 일일평균 100만명 이상인 자

④

정보통신망법상 사고 요건은 **정보통신서비스 이용의 안전성을 현저히 해치는 사건·사고가 발생했거나 발생할 가능성이 있는 경우**이다. 이 경우 **방송미디어통신위원회로부터 관계 물품·서류 등의 제출을 요구받은 자**가 국내대리인 지정 대상에 해당한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제19조(국내대리인 지정 대상자의 범위)
① 법 제32조의5제1항에서 "대통령령으로 정하는 기준에 해당하는 자"란 다음 각 호의 어느 하나에 해당하는 자를 말한다. <개정 2020.8.4, 2025.10.1>
4. 이 법을 위반하여 정보통신서비스 이용의 안전성을 현저히 해치는 사건 · 사고가 발생하였거나 발생할 가능성이 있는 경우로서 법 제64조제1항에 따라 방송미디어통신위원회로부터 관계 물품 · 서류 등을 제출하도록 요구받은 자

NoteBase

문 16. 다음 설명에 해당하는 악성코드 분석도구를 옳게 짝 지은 것은?

ㄱ. 가상화 기술 기반으로 악성코드의 비정상 행위를 유발하는 실험과정에서 발생할 수 있는 분석시스템으로의 침해를 방지하여 통제된 환경과 분석 기능을 제공한다.
ㄴ. 악성코드의 행위를 추출하기 위해 실제로 해당 코드를 실행함으로써 발생하는 비정상 행위 혹은 시스템 동작 환경의 변화를 살펴볼 수 있는 동적 분석 기능을 제공한다.

① ㄱ: Sandbox, ㄴ: Process Explorer
② ㄱ: Sandbox, ㄴ: Burp Suite
③ ㄱ: Blackbox, ㄴ: IDA Pro
④ ㄱ: Blackbox, ㄴ: OllyDBG

정답 1번

간단한 해설

Sandbox는 악성코드를 **격리된 환경에서 실행**하도록 하고, Process Explorer는 **실행 중인 프로세스의 상태**를 관찰하여 악성 행위 분석을 돕는다. 실행 환경을 통제하는 역할과 실행 결과를 살펴보는 역할을 구별한다.

대응 관계 해설

ㄱ. Sandbox: 악성코드를 실행하면서 분석 시스템을 보호하려면 악성코드가 동작하는 공간을 호스트 시스템과 분리해야 한다. 문항의 샌드박스는 **가상화 기술로 격리된 실행 환경**을 마련하여 악성코드의 행위를 관찰할 수 있게 한다. 따라서 통제된 실험 환경과 분석 기능을 제공한다는 설명에 대응한다.

ㄴ. Process Explorer: 동적 분석은 코드를 실제로 실행한 뒤 나타나는 행위나 시스템 상태를 살펴보는 방식이다. Process Explorer는 **실행 중인 프로세스와 그 프로세스가 불러온 DLL, 열어 둔 핸들** 등을 보여 준다. 이를 통해 악성코드 실행 후 생긴 프로세스나 사용 중인 자원 등을 확인하며 동적 분석을 수행할 수 있다. Burp Suite는 웹 애플리케이션의 취약점 점검에 사용하는 도구이므로, 이 문항의 프로세스 관찰 도구와 구별된다.

ㄱ은 Sandbox, ㄴ은 Process Explorer로 대응하므로 ①의 조합과 일치한다.

NoteBase

문 17. 윈도우 운영체제의 계정 관리에 대한 설명으로 옳은 것은?

① ‘net accounts guest /active:no’ 명령은 guest 계정을 비활성화한다.

② ‘net user’ 명령은 시스템 내 사용자 계정정보를 나열한다.

③ ‘net usergroup’ 명령은 시스템 내 사용자 그룹정보를 표시한다.

④ 컴퓨터/도메인에 모든 접근권한을 가진 관리자 그룹인 ‘Admin’이 기본적으로 존재한다.

정답 2번

간단한 해설

'net user'는 사용자 계정을 관리하는 명령으로, 인수 없이 실행하면 현재 컴퓨터의 사용자 계정 목록을 표시한다.

선지별 해설

① X: 'net accounts'는 암호의 최소 길이·유효 기간 등 계정 정책을 조회하거나 설정하는 명령이다. 개별 계정의 활성 상태는 'net user'로 관리하므로, guest 계정을 비활성화하려면 **'net user guest /active:no'**를 사용한다. 여기서 '/active:no'는 지정한 계정을 사용할 수 없게 하는 옵션이다.

② O: **인수 없이 'net user'를 실행하면** 현재 컴퓨터의 사용자 계정 이름 목록이 표시된다. 특정 계정의 소속 그룹이나 활성 상태 등 상세 정보를 확인하려면 'net user guest'처럼 계정 이름을 덧붙인다.

③ X: 'net usergroup'은 윈도우의 표준 net 하위 명령이 아니다. 시스템의 로컬 그룹 목록을 표시하는 명령은 **'net localgroup'**이다. 'net localgroup Administrators'처럼 그룹 이름을 지정하면 해당 그룹의 구성원을 확인할 수 있다.

④ X: 윈도우의 기본 관리자 그룹 이름은 **'Administrators'**이며, 'Admin'이 아니다. 이 그룹의 구성원은 해당 컴퓨터를 관리하는 광범위한 권한을 가진다. 'Administrator'는 기본 관리자 사용자 계정의 이름이므로 그룹 이름인 'Administrators'와 구별한다.

NoteBase

문 18. 커버로스(Kerberos) 프로토콜에 대한 설명으로 옳지 않은 것은?

① 양방향 인증방식의 문제점을 보완하여 신뢰하는 제3자 인증 서비스를 제공한다.

② 사용자의 패스워드를 추측하거나 캡처하지 못하도록 일회용 패스워드를 제공한다.

③ 버전 5에서는 이전 버전과 달리 DES가 아닌 다른 암호 알고리즘을 사용할 수 있다.

④ 클라이언트는 사용자의 식별정보를 평문으로 인증 서버(Authentication Server)에 전송한다.

정답 2번

간단한 해설

커버로스의 기본 인증 수단은 **티켓과 세션 키**이며, 일회용 패스워드를 발급하는 방식이 아니다. 패스워드 자체를 네트워크로 보내지 않더라도 약한 패스워드에 대한 추측 공격까지 막아 주지는 않는다.

선지별 해설

① O: 커버로스는 클라이언트와 서비스 서버가 공통으로 신뢰하는 **키 분배 센터(KDC)**를 이용하는 제3자 인증 방식이다. KDC가 티켓과 세션 키를 발급하므로, 통신 당사자들이 상대마다 장기 비밀키를 직접 공유·관리해야 하는 부담을 줄일 수 있다.

② X: 커버로스는 기본적으로 **일회용 패스워드가 아니라 티켓과 세션 키**를 이용해 인증한다. 사용자의 패스워드 자체는 네트워크로 전송하지 않으며, 서비스 이용 시에는 티켓과 세션 키로 만든 인증자를 제시한다. 또한 약한 패스워드를 사용하면 이를 바탕으로 암호화된 메시지에 오프라인 사전 공격을 할 수 있으므로, 패스워드 추측을 불가능하게 한다는 설명도 부정확하다.

③ O: 버전 4는 DES에 의존했지만, 버전 5는 **특정 암호 알고리즘에 한정되지 않도록** 설계되었다. 메시지에 사용한 암호 유형을 표시하므로 DES 외에 AES 같은 암호 알고리즘도 사용할 수 있다.

④ O: 클라이언트는 최초 인증 요청에서 **사용자 식별정보를 평문으로** 인증 서버(AS)에 보낸다. AS는 이 정보로 요청한 사용자를 식별한다. 평문으로 보내는 식별정보는 사용자 이름과 같은 정보이며, 비밀정보인 패스워드 자체를 평문으로 보낸다는 뜻은 아니다.

NoteBase

문 19. 임의적 접근 통제(Discretionary Access Control) 모델에 대한 설명으로 옳은 것은?

① 주체가 소유권을 가진 객체의 접근 권한을 다른 사용자에게 부여할 수 있으며, 사용자 신원에 따라 객체의 접근을 제한한다.

② 주체와 객체가 어떻게 상호 작용하는지를 중앙 관리자가 관리하며, 사용자 역할을 기반으로 객체의 접근을 제한한다.

③ 주체와 객체에 각각 부여된 서로 다른 수준의 계층적인 구조의 보안등급을 비교하여 객체의 접근을 제한한다.

④ 주체가 접근할 수 있는 상위와 하위의 경계를 설정하여 해당 범위 내 임의 객체의 접근을 제한한다.

정답 1번

간단한 해설

임의적 접근 통제(DAC)는 **객체 소유자가 다른 사용자에게 접근 권한을 부여**할 수 있는 방식이다. 접근 여부는 사용자 신원과 그 사용자에게 부여된 권한을 기준으로 결정한다.

선지별 해설

① O: 임의적 접근 통제(DAC)에서는 파일 등의 객체를 소유한 주체가 **누구에게 어떤 접근 권한을 줄지** 정할 수 있다. 접근을 요청한 사용자의 신원을 확인하고, 그 사용자에게 부여된 읽기·쓰기 등의 권한에 따라 접근을 허용한다. 예를 들어 파일 소유자 A가 사용자 B에게 읽기 권한만 주면, B는 그 파일을 읽을 수 있지만 수정할 수는 없다.

② X: 사용자 역할을 기준으로 접근을 제한하는 것은 **역할 기반 접근 통제(RBAC)**의 설명이다. 관리자는 직무에 맞는 역할에 권한을 연결하고 사용자에게 역할을 부여한다. 사용자는 그 역할을 통해 권한을 얻는다. DAC에서는 개별 사용자의 신원과 객체 소유자가 부여한 권한이 접근 판단의 기준이다.

③ X: 주체와 객체의 보안등급을 비교하여 접근을 제한하는 것은 **강제적 접근 통제(MAC)**의 설명이다. 주체의 보안 인가 수준과 객체의 보안등급에 시스템의 보안정책을 적용하므로, 객체 소유자가 임의로 권한을 주어 그 제한을 바꿀 수 없다. DAC의 기준은 이러한 보안등급 비교가 아니라 사용자 신원과 소유자가 부여한 접근 권한이다.

④ X: 상·하위 경계와 보안 수준의 관계로 접근 범위를 정하는 것은 **격자 기반 접근 통제(LBAC)**에 관한 설명이다. 이 방식은 보안 수준 사이의 지배 관계를 격자 구조로 나타내어 허용되는 접근이나 정보 흐름을 판단한다. DAC의 '임의적'은 정해진 범위 안의 임의 객체에 접근한다는 뜻이 아니라, 객체 소유자가 다른 사용자에게 줄 접근 권한을 재량으로 정할 수 있다는 뜻이다.

NoteBase

문 20. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제45조(정보통신망의 안정성 확보 등)에 정보보호조치에 관한 지침에 포함되어야 할 보호조치로 명시되지 않은 것은?

① 정보의 불법 유출·위조·변조·삭제 등을 방지하기 위한 기술적 보호조치

② 사전 정보보호대책 마련 및 보안조치 설계·구현 등을 위한 기술적 보호조치

③ 정보통신망의 지속적인 이용이 가능한 상태를 확보하기 위한 기술적·물리적 보호조치

④ 정보통신망의 안정 및 정보보호를 위한 인력·조직·경비의 확보 및 관련 계획수립 등 관리적 보호조치

정답 2번

①

정보보호지침에는 정보의 **불법 유출·위조·변조·삭제 등을 방지하기 위한 기술적 보호조치**가 포함되어야 한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제45조(정보통신망의 안정성 확보 등)
③ 정보보호지침에는 다음 각 호의 사항이 포함되어야 한다. <개정 2016.3.22, 2020.6.9>
2. 정보의 불법 유출 · 위조 · 변조 · 삭제 등을 방지하기 위한 기술적 보호조치

②

정보보호지침에는 정보의 불법 유출·위조·변조·삭제 방지 등의 기술적 보호조치가 명시되어 있다. 사전 정보보호대책 마련 및 보안조치 설계·구현은 **지침의 필수 포함 사항으로 열거되어 있지 않다**.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제45조(정보통신망의 안정성 확보 등)
③ 정보보호지침에는 다음 각 호의 사항이 포함되어야 한다. <개정 2016.3.22, 2020.6.9>
1. 정당한 권한이 없는 자가 정보통신망에 접근 · 침입하는 것을 방지하거나 대응하기 위한 정보보호시스템의 설치 · 운영 등 기술적 · 물리적 보호조치
2. 정보의 불법 유출 · 위조 · 변조 · 삭제 등을 방지하기 위한 기술적 보호조치
3. 정보통신망의 지속적인 이용이 가능한 상태를 확보하기 위한 기술적 · 물리적 보호조치
4. 정보통신망의 안정 및 정보보호를 위한 인력 · 조직 · 경비의 확보 및 관련 계획수립 등 관리적 보호조치
5. 정보통신망연결기기등의 정보보호를 위한 기술적 보호조치

NoteBase

③

정보보호지침에는 **정보통신망을 지속적으로 이용할 수 있는 상태를 확보하기 위한 기술적·물리적 보호조치**가 포함되어야 한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제45조(정보통신망의 안정성 확보 등)
③ 정보보호지침에는 다음 각 호의 사항이 포함되어야 한다. <개정 2016.3.22, 2020.6.9>
3. 정보통신망의 지속적인 이용이 가능한 상태를 확보하기 위한 기술적 · 물리적 보호조치

④

정보통신망의 안정과 정보보호를 위한 **인력·조직·경비의 확보 및 관련 계획수립은 관리적 보호조치**이며, 정보보호지침에 포함되어야 한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제45조(정보통신망의 안정성 확보 등)
③ 정보보호지침에는 다음 각 호의 사항이 포함되어야 한다. <개정 2016.3.22, 2020.6.9>
4. 정보통신망의 안정 및 정보보호를 위한 인력 · 조직 · 경비의 확보 및 관련 계획수립 등 관리적 보호조치

NoteBase