총평 : 2020년 국가직 9급 정보보호론 시험은 전반적으로 평이한 문제들로 출제가 되었지만, 몇몇 문제들은 정확하게 자세한 사항을 바탕으로 풀이하여야 되는 문제들이 출제되었습니다. 암호화에 대한 문제가 5문제 출제되면서 가장 많은 출제비중을 보였으며, 애플리케이션 보안 부분의 문제가 출제되지 않았습니다. 네트워크 보안은 3문제가 출제되어 많은 문제가 출제되지는 않았지만 중요하게 다루어야 하는 부분을 출제하였습니다. 앞으로의 시험에서도 전체적인 내용을 학습과 동시에 자주 출제되는 포인트에 대해서는 좀더 상세한 학습이 필요할 것으로 보입니다.

문 1. 정보보호 위험관리에 대한 설명으로 옳지 않은 것은? 2
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.
[해설]
- 위험은 조직 내에서 존재하는 취약점을 이용하는 다양한 보안 위협이나 외부적 요인에 의해 발생할 수 있는 재해, 사고 등으로 볼 수 있으며, 이로 인한 손실 또는 부정적인 영향을 미칠 가능성을 말한다.

문 2. 공개키 암호화에 대한 설명으로 옳지 않은 것은? 3
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.
[해설]
- 전자서명 할 때는 서명하는 사용자의 개인키로 암호화한다.
- 공개키 알고리즘

알고리즘명	발표년도	개발자	안전도 근거
RSA	1978	Rivest, Shamir, Adleman	소인수 분해 문제
Knapsack	1978	R.C.Merkle, M.E.Hellman	부분합 문제
McEliece	1978	McEliece	대수적 부호 이론
ELGamal	1985	ELGamal	이산대수 문제
ECC	1985	N.kObitz, V.Miller	타원곡선 이산대수 문제
RPK	1996	W.M.Raike	이산대수 문제
Lattice	1997	Goldwasser, Goldreich, Halevi	가장 가까운 벡터를 찾는 문제

문 3. X.509 인증서 형식 필드에 대한 설명으로 옳은 것은? 4
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
[해설]
- Issuer name : 인증서 발행자의 이름을 나타내는 정보
- Subject name : 인증서 사용자의 이름을 나타내는 정보
- Signature algorithm ID ; 인증기관이 인증서를 서명하기 위한 알고리즘과 알고리즘 식별자 정보

문 4. 일방향 해시함수를 사용하여 비밀번호를 암호화할 때 salt라는 난수를 추가하는 이유는? 1
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.
[해설]
솔트(salt) 사용
- 솔트는 공개되어 있는 랜덤값으로 패스워드의 해시값 생성시 함께 사용된다.
- 솔트를 사용하면 접근 권한을 얻으려는 공격자가 수행하는 해시 함수 연산 횟수가 증가하여, 보다 안전한 패스워드 인증 방식이 된다.

문 5. 윈도우 운영체제에서 TPM(Trusted Platform Module)에 대한 설명으로 옳지 않은 것은? 1
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.
[해설]
- TPM(Trusted Platform Module)은 신뢰할 수 있는 플랫폼 모듈이며, 암호화 키를 포함하여 외부의 공격이나 내부의 다른 요인에 의해 하드웨어의 변경이나 손상을 방지하는 등의 보안관련 기능을 제공하는 기술이다.
- TPM의 공개키가 아니고, 개인키를 사용하여 플랫폼 설정정보에 서명함으로써 디지털 인증을 생성한다.

문 6. 키 k에 대한 블록 암호 알고리즘 E_k , 평문블록 M_i , Z_0 는 초기벡터, $Z_i = E_k(Z_{i-1})$가 주어진 경우, 이때 i = 1, 2, ..., n에 대해 암호블록 C_i 를 $C_i = Z_i \oplus M_i$ 로 계산하는 운영 모드는? (단, ⊕는 배타적 논리합이다) 3

① CBC ② ECB

③ OFB ④ CTR

[해설]

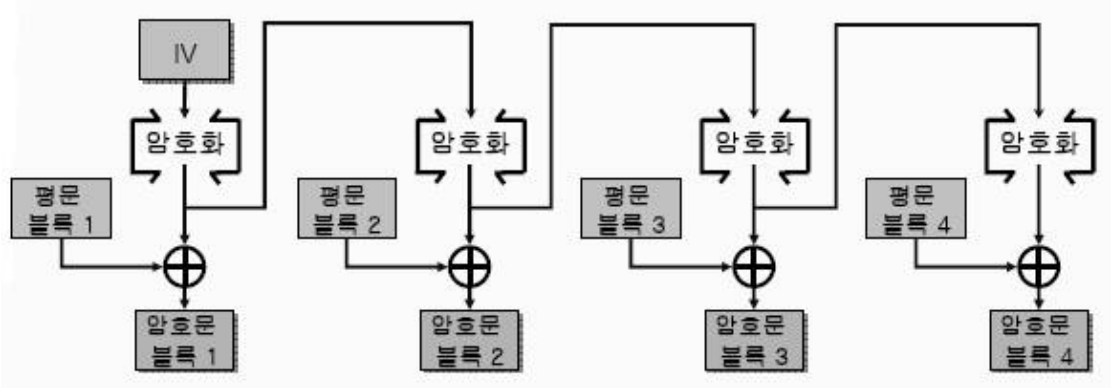
- OFB(Output-FeedBack) 모드

① 암호 알고리즘의 출력을 암호 알고리즘의 입력으로 피드백한다.

② 평문 블록은 암호 알고리즘에 의해 직접 암호화되고 있는 것이 아니며, 평문 블록과 암호 알고리즘의 출력을 XOR해서 암호문 블록을 만들어 낸다.

③ 키 스트림을 미리 준비할 수 있으며, 미리 준비한다면 암호문을 만들때 더 이상 암호 알고리즘을 구동할 필요가 없다. (키 스트림을 미리 만들어 두면 암호화를 고속으로 수행할 수 있으며, 혹은 키 스트림을 만드는 작업과 XOR를 취하는 작업을 병행하는 것도 가능하다.)

- OFB 모드에 의한 암호화



문 7. 정보보호 시스템 평가 기준에 대한 설명으로 옳은 것은? 4

① ITSEC의 레인보우 시리즈에는 레드북으로 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.

[해설]

- TCSEC의 레인보우 시리즈에는 레드북으로 불리는 TNI(Trusted Network Interpretation of the TCSEC, 네트워크용 정보보보호 시스템 평가 기준)가 있다.

- ITSEC의 평가등급은 최하위 레벨의 신뢰도를 요구하는 E0(부적합판정)부터 최상위 레벨의 신뢰도를 요구하는 E6까지 7등급으로 구분한다.

- CC의 EAL2 등급은 구조적 시험을 의미한다.

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? 4

① 세션 ID
② 클라이언트 난수
③ 압축 방법 목록
④ 인증서 목록

[해설]

- Client Hello : 클라이언트는 서버에 처음으로 연결을 시도할 때, Client Hello 메시지를 통해 클라이언트 SSL 버전, 클라이언트에서 생성한 임의의 난수, 세션 식별자(ID), Cipher Suit 리스트, 클라이언트가 지원하는 압축 방법 리스트 등의 정보를 서버에 전송한다.

문 9. 개인정보 보호법 상 기본계획에 대한 조항의 일부이다. ㉠, ㉡에 들어갈 내용을 바르게 연결한 것은? 2

> 제9조(기본계획) ①보호위원회는 개인정보의 보호와 정보 주체의 권익 보장을 위하여 (㉠)년마다 개인정보 보호 기본계획(이하 “기본계획”이라 한다)을 관계 중앙행정기관의 장과 협의하여 수립한다.
> ②기본계획에는 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

[해설]

- 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.
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

③ 국회, 법원, 헌법재판소, 중앙선거관리위원회는 해당 기관(그 소속 기관을 포함한다)의 개인정보 보호를 위한 기본계획을 수립·시행할 수 있다.

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? 3

① 6 ② 8

③ 12 ④ 16

[해설]

- Diffie-Hellman 방법에서 대칭(공유) 키는 K = g^xy mod p이다.

2^3*2 mod 13 = 64 mod 13 = 12

문 11. NIST의 AES(Advanced Encryption Standard) 표준에 따른 암호화 시 암호키(cipher key) 길이가 256비트일 때 필요한 라운드 수는? 4

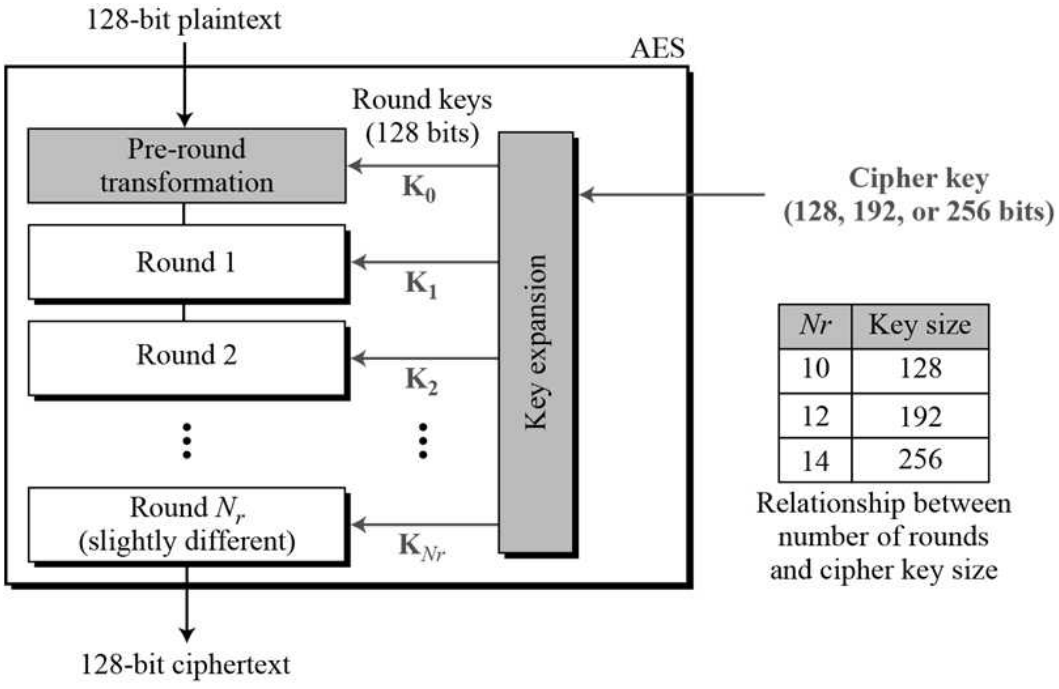
① 8 ② 10

③ 12 ④ 14

[해설]

- AES 알고리즘의 블록크기는 128비트이고 키길이는 128/192/256비트이며, 각 라운드수는 10/12/14이다. SPN(Substitution-Permutation Network) 구조를 사용하고 있다.

- AES 암호의 구조도



Nr	Key size
10	128
12	192
14	256

Relationship between number of rounds and cipher key size

문 12. IPsec의 ESP(Encapsulating Security Payload)에 대한 설명으로 옳지 않은 것은? 4

① 인증 기능을 포함한다.

② ESP는 암호화를 통해 기밀성을 제공한다.

③ 전송 모드의 ESP는 IP 헤더를 보호하지 않으며, 전송계층 으로부터 전달된 정보만을 보호

한다.
④ 터널 모드의 ESP는 Authentication Data를 생성하기 위해 해시 함수와 공개키를 사용한다.
[해설]
- ESP(Encapsulating Security Payload) : 메시지의 암호화를 제공한다. 사용하는 암호화 알고리즘으로는 DES-CBC, 3DES, RC5, IDEA, 3IDEA, CAST, blowfish 가 있다.
- 터널 모드의 ESP는 Authentication Data를 생성하기 위해 해시 함수와 대칭키를 사용한다.

문 13. 네트워크나 컴퓨터 시스템의 자원 고갈을 통해 시스템 성능을 저하시키는 공격에 해당하는 것만을 모두 고르면? 1

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
[해설]
- 서비스 거부공격 (DoS attack) : DoS공격은 인터넷을 통하여 장비나 네트워크을 목표로 공격한다. DoS공격의 목적은 정보를 훔치는것이 아니라 장비나 네트워크를 무력화 시켜서 사용자가 더 이상 네트워크 자원을 접근할 수 없게 만든다.
- Ping of death : 네트워크의 연결 상태를 점검하기 위한 ping 명령을 보낼 때, 패킷을 최대한 길게하여 (최대 65,500바이트) 공격 대상에게 보내면 패킷은 네트워크에서 수백 개의 패킷으로 잘게쪼개져 보내진다. 네트워크의 특성에 따라 한 번 나뉜 패킷이 다시 합쳣서 전송되는 일은 거의 없으며, 공격 대상 시스템은 결과적으로 대량의 작은 패킷을 수신하게 되어 네트워크가 마비된다.
- Smurf 공격 : Ping of Death처럼 ICMP 패킷을 이용한다. ICMP Request 를 받은 네트워크는 ICMP Request 패킷의 위조된 시작 IP 주소로 ICMP Reply 를 다시 보낸다. 결국 공격 대상은 수많은 ICMP Reply 를 받게 되고 Ping of Death 처럼 수많은 패킷이 시스템을 과부하 상태로 만든다.

문 14. 다음 설명에 해당하는 위험분석 및 평가 방법을 옳게 짝 지은 것은? 3

ㄱ. 전문가 집단의 토론을 통해 정보시스템의 취약성과 위협 요소를 추정하여 평가하기 때문에 시간과 비용을 절약할수 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.

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

[해설]
- 델파이법 : 전문가 집단의 토론을 통해 정보시스템의 취약성과 위협 요소를 추정하여 평가하기 때문에 시간과 비용을 절약할수 있지만, 정확도가 낮다.
- 과거자료 분석법 : 이미 발생한 사건이 앞으로 발생한다는 가정하에 수집된 자료를 통해 위험 발생 가능성을 예측하며, 자료가 많을수록 분석의 정확도가 높아진다.
- 시나리오법 : 어떤 사건도 기대하는 대로 발생하지 않는다는 사실에 근거하여 일정 조건에서 위협에 대해 발생 가능한 결과들을 예측하며, 적은 정보를 가지고 전반적인 가능성을 추론할 수 있다.

문 15. 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제19조 (국내대리인 지정 대상자의 범위)에 명시된 자가 아닌 것은? 1
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 방송 통신위원회로부터 관계 물품.서류 등을 제출하도록 요구받은 자
[해설]
- 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.
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. 전년도 말 기준 직전 3개월간 그 개인정보가 저장ㆍ관리되고 있는 이용자 수가 일일평균 100만명 이상인 자
4. 이 법을 위반하여 개인정보 침해 사건ㆍ사고가 발생하였거나 발생할 가능성이 있는 경우로서 법 제64조제1항에 따라 방송통신위원회로부터 관계 물품ㆍ서류 등을 제출하도록 요구받은 자
② 제1항제1호 및 제2호에 따른 매출액은 전년도(법인인 경우에는 전 사업연도를 말한다) 평균환율을 적용하여 원화로 환산한 금액을 기준으로 한다.

문 16. 다음 설명에 해당하는 악성코드 분석도구를 옳게 짝지은 것은? 1

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.

	ㄱ	ㄴ
①	Sandbox	Process Explorer
②	Sandbox	Burp Suite
③	Blackbox I	DA Pro
④	Blackbox	OllyDBG

[해설]
- Sandbox : 보호된 영역 내에서 프로그램을 동작시키는 것으로, 외부 요인에 의해 악영향이 미치는 것을 방지하는 보안 모델이다. '아이를 모래밭(샌드 박스)의 밖에서 놀리지 않는다'라고 하는 말이 어원이라고 알려져 있다. 이 모델에서는 외부로부터 받은 프로그램을 보호된 영역, 즉 '상자' 안에 가두고 나서 동작시킨다. '상자'는 다른 파일이나 프로세스로부터는 격리되어 내부에서 외부를 조작하는 것은 금지되고 있다. 가상화 기술 기반으로 악성코드의 비정상 행위를 유발하는 실험과정에서 발생할 수 있는 분석시스템으로의 침해를 방지하여 통제된 환경과 분석 기능을 제공한다.
- Process Explorer : 프로세스를 관리할 수 있는 프로그램으로 악성코드의 행위를 추출하기 위해 실제로 해당 코드를 실행함으로써 발생하는 비정상 행위 혹은 시스템 동작 환경의 변화를 살펴볼 수 있는 동적 분석 기능을 제공한다.

문 17. 윈도우 운영체제의 계정 관리에 대한 설명으로 옳은 것은? 2
① 'net accounts guest /active:no' 명령은 guest 계정을 비활성화 한다.
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.
[해설]
- 'net user guest /active:no' 명령은 guest 계정을 비활성화 한다.
- 'net group' 명령은 서버에서 글로벌 그룹을 추가, 표시 또는 수정한다.
- 컴퓨터/도메인에 모든 접근권한을 가진 관리자 그룹인 'Administrators'이 기본적으로 존재한다.

문 18. 커버로스(Kerberos) 프로토콜에 대한 설명으로 옳지 않은 것은? 2
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.
[해설]

커버로스(Kerberos)
- 커버로스는 MIT 아테네 프로젝트에서 개발된 신뢰할 수 있는 제 3자 인증 프로토콜로서, 인증과 메시지 보호를 제공하는 보안 시스템의 이름이다.
- 대칭키 암호 방식을 사용하여 분산 환경에서 개체 인증 서비스를 제공한다.

문 19. 임의적 접근 통제(Discretionary Access Control) 모델에 대한 설명으로 옳은 것은? 1
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 범위내 임의 객체의 접근을 제한한다.
[해설]
- 임의적 접근 통제(DAC : Discretionary Access Control) : 주체가 속해 있는 그룹의 신원에 근거하여 객체에 대한 접근을 제한하는 방법으로 객체의 소유자가 접근 여부를 결정한다.
- 강제적 접근 통제(MAC : Mandatory Access Control) : 주체와 객체의 등급을 비교하여 접근 권한을 부여하는 접근 통제이며, 모든 객체는 기밀성을 지니고 있다고 보고 객체에 보안 레벨을 부여한다.
- 역할 기반 접근통제(RBAC : Role Based Access Control) : 주체와 객체 사이에 역할을 부여하여 임의적, 강제적 접근통제 약점을 보완한 방식이다. 사용자가 적절한 역할에 할당되고 역할에 적합한 접근권한(허가)이 할당된 경우만 사용자가 특정한 모드로 정보에 접근할 수 있는 방법이다.

문 20. 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제45조 (정보통신망의 안정성 확보 등)에 정보보호조치에 관한 지침에 포함되어야 할 보호조치로 명시되지 않은 것은? 2
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
[해설]
제45조(정보통신망의 안정성 확보 등) ① 다음 각 호의 어느 하나에 해당하는 자는 정보통신서비스의 제공에 사용되는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 하여야 한다. <개정 2020. 6. 9.>
1. 정보통신서비스 제공자
2. 정보통신망에 연결되어 정보를 송·수신할 수 있는 기기·설비·장비 중 대통령령으로 정하는 기기·설비·장비(이하 "정보통신망연결기기등"이라 한다)를 제조하거나 수입하는 자
② 과학기술정보통신부장관은 제1항에 따른 보호조치의 구체적 내용을 정한 정보보호조치에

관한 지침(이하 "정보보호지침"이라 한다)을 정하여 고시하고 제1항 각 호의 어느 하나에 해당하는 자에게 이를 지키도록 권고할 수 있다. <개정 2012. 2. 17., 2013. 3. 23., 2017. 7. 26., 2020. 6. 9.>

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

④ 과학기술정보통신부장관은 관계 중앙행정기관의 장에게 소관 분야의 정보통신망연결기기등과 관련된 시험·검사·인증 등의 기준에 정보보호지침의 내용을 반영할 것을 요청할 수 있다. <신설 2020. 6. 9.>

[전문개정 2008. 6. 13.]

[시행일 : 2020. 12. 10.] 제45조