정보보호론	국가 전산 7급	2019년 8월 17일

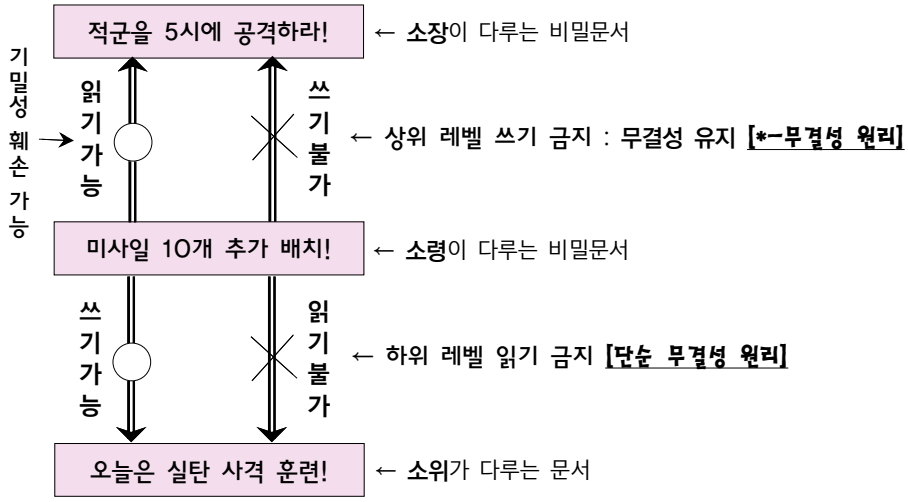
♠ 필기합격인원/합격선(46명/76.66점) - 선발예정인원 33명 ♠

1. Biba 보안 모델에 대한 설명으로 옳은 것은? [2019년 국가 7급]

① 이해가 상충되는 회사들 간의 정보흐름이 일어나지 않도록 고안되었다.
② 자신의 보안 수준보다 낮거나 같은 수준의 객체만 읽을 수 있다.
③ 자신의 보안 수준보다 높거나 같은 수준의 객체에만 쓸 수 있다.
④ 자신의 무결성 수준보다 높거나 같은 수준의 객체만 읽을 수 있다.

♤ Biba 보안 모델 - 무결성 위주

- Biba 보안 모델은 **Biba integrity**(무결성) 모델이라고도 한다.
- Biba 보안 모델은 정보의 불법 변조 방지를 정의한 모델이다. - BLP 모델의 문제점 해결



① 상위레벨 쓰기금지 정책(No-write-up Policy) : [*-무결성 원리]
- 주체는 자신의 무결성 접근등급보다 높은 객체에 쓰기를 할 수 없다.
- 높은 무결성을 가진 정보의 훼손을 방지하기 위한 것이다.
- 자신의 무결성 접근등급보다 높거나 같은 수준의 객체만 읽을 수 있다.

② 하위레벨 읽기금지 정책(No-read-down Policy) : [단순 무결성 원리]
- 주체는 자신의 무결성 접근등급보다 낮은 객체는 읽을 수 없다.
- 자신의 무결성 수준보다 높거나 같은 수준의 객체만 읽을 수 있다.
- 낮은 수준의 문서가 인용되는 것을 방지한다.

정답 : ④

2. IT 재해복구체계 수립 시, 업무영향분석(BIA: business impact analysis) 과정에서 고려하는 항목이 아닌 것은? [2019년 국가 7급]

① MTD(Maximum Tolerable Downtime)
② MTU(Maximum Transfer Unit)
③ RTO(Recovery Time Objective)
④ RPO(Recovery Point Objective)

♤ IT 재해복구체계 수립 시, 업무영향분석(BIA)

- 업무영향분석(BIA)은 재해가 발생했을 때, 복구최소대상인 단위업무를 정의하고, 단위업무의 복구우선순위와 복구목표시간, 복구목표시점 정의를 통해 업무복구에 필요한 자원을 산정하는 과정이다.
- 업무영향분석(BIA)을 이해하기 위해서는 기본적으로 다음 개념을 이해해야 한다.
- RTO / RPO / MTD / MTPD

◈ **복구목표시점(RPO, Recovery Point Objective) – 데이터 관점**
- RPO는 어느 시점에 **백업**할 것인지?를 결정하는 지표이다.**(백업시점)**
- RPO는 재해 발생으로 중단된 서비스에 대해 수용 가능한 데이터 손실과 연관된다.
- RPO는 수용 가능한 데이터 손실의 양을 결정하는데 효과적이다.**(손실되어도 무방)**
- 모든 데이터의 완벽한 복구는 현실적으로 어렵다.

◈ **복구목표시간(RTO, Recovery Time Objective) – 업무 관점**
- 간단히 말하면, 복구목표시간(RTO)은 **복구하는데 걸리는 시간**이다.**(업무 관점)**
- RTO는 재해 발생 이후에 원 상태로 복구하는데 소요되는 시간이다.
- RTO는 서비스가 중단되었을 때, 서비스 복구까지 걸리는 최대 허용시간이다.
- RTO는 조직의 핵심 업무를 정상화시키기 위한 목표시간이다.
- RTO는 정성적/정량적 평가를 통해 산정한다.

◈ **한계복구시간(MTD, Maximum Tolerable Downtime)**
- 핵심 프로세스가 중단된 채로 회사가 견딜 수 있는 최장시간
- 조직이 업무처리 중단으로 인한 영향을 감내할 수 있는 시간

◈ **최대허용중단시간(MTPD. Maximum Tolerable Period of Disruption)**
- 회사의 특정 업무 중단 시 회사에서 허용할 수 있는 최대중단기간을 의미
- 업무 중단 발생 시 영향 추정을 위하여 단위업무별 MTPD를 산정한다.
- MTPD는 자사의 주요 재무요소를 적용 후 단위업무별로 산정한다.
- MTPD는 조직으로 하여금 수용 불가한 상태가 되기까지 소요되는 시간을 말한다.

◈ **최대전송단위(MTU, Maximum Transfer Unit)**
- MTU는 네트웍의 물리매체에서 최대로 보낼 수 있는 데이터그램 크기이다.(바이트)
- MTU는 업무영향분석(BIA)과 무관하다.

정답 : ②

3. 다음에서 설명하는 위험분석 접근 방법은? [2019년 국가 7급]

○ 정형화되고 구조화된 프로세스를 사용하는 대신, 분석가 개인의 지식 및 경험을 활용한다.
○ 비교적 비용대비 효과가 우수하며 중·소규모 조직에 적합하다.
○ 개인적인 경험에 의존하므로 정당성이나 일관성이 부족할 수 있다.

---

① 기준선 접근(baseline approach)　② 상세 위험분석(detailed risk analysis)
③ 비형식적 접근(informal approach)　④ 복합 접근(combined approach)

♤ **위험분석 방법**

• 위험분석 방법으로 **기준선 접근, 상세 위험분석, 비형식적 접근, 복합 접근** 등이 있다.
• 비형식적 접근(informal approach)은 비정형 접근이라고도 한다.

◈ **비형식적 접근 / 비정형 접근법(informal approach)**
① **경험자의 지식**을 사용하여 위험분석을 수행하는 것이다.
• 이 방법은 구조적인 방법론에 기반하지 않는다.
• 특정 위험분석 기법을 선정하여 수행하지 않고,
• 수행자의 경험에 따라 중요 위험 중심으로 분석한다.
• 수행자의 경험이 적은 분야는 위험을 놓칠 가능성이 있다.
② 논리적이고 검증된 방법론이 아니다.
• 검토자의 개인적 경험에 지나치게 의존한다.
• **전문성이 높은 인력이 참여하지 않으면 실패할 위험**이 있다.
• 개인적인 경험에 의존하므로 정당성이나 **일관성이 부족**할 수 있다.
③ 작은 규모의 조직에 적합할 수 있다.(중소규모 조직에 적합)

◈ **베이스라인 접근법(baseline approach)**
① **체크리스트**를 이용한 위험분석 방법이다.
• 모든 시스템에 대한 표준 보호대책을 체크리스트로 제공한다.
• 체크리스트에 있는 보호대책 구현 여부를 조사한다.
• 체크리스트에 있는 구현되지 않은 보호대책을 식별한다.
② 분석 비용과 시간은 절약된다.
• 하지만, 과보호 또는 부족한 보호가 될 가능성이 상존한다.
• 해당 조직에 적합한 체크리스트가 없으면 위험을 분석하지 않는 것과 유사하다.
③ 체크리스트 방식은 담당자에게 **체크리스트에만 집착**하게 할 수 있다.
• 보안 상태 자체보다 체크리스트를 통해 나타나는 점수에 집착한다.
• 보안요구사항에 따른 우선순위보다는 구현 용이성에 따라 정보보호대책을 구현하게 된다.

정답 : ③

4. 다음 수식에 의해 산출되는 것은? [2019년 국가 7급]

수식 : H[(K⁺⊕ opad) || H[(K⁺⊕ ipad) || M]]

H : 해시함수

K⁺: 비밀키 K에 0을 덧붙인 것

M : 메시지

ipad, opad : 특정 상수

⊕ : XOR

|| : 연결(concatenation)

---

① GMAC ② HMAC

③ CMAC ④ 전자서명

♤ **HMAC(Hash-based Message Authentication Code, 해시기반 메시지인증코드)**

- HMAC는 **해시-기반 메시지인증코드**이다.
- HMAC는 송수신자가 메시지 훼손되었는지 여부를 확인하는 데 사용할 수 있다.
- HMAC는 송신자는 원래 데이터의 해시값을 계산하여 데이터와 해시값을 모두 전송한다.
- HMAC에서 전송 메시지는 단일 메시지로 보낸다.(해시값 + 원래 데이터)
- 수신자는 받은 메시지에 대한 해시값을 다시 계산하여 받은 HMAC와 같은지 확인한다.
- HMAC는 다양한 해시함수에 적용하여 메시지인증코드를 생성할 수 있다.

// HMAC는 해시함수 알고리즘에 따라서 메시지인증코드 길이가 다르다.

- HMAC_MD5("", "") = 0x74e6f7298a9c2d168935f58c001bad88
- HMAC_SHA1("", "") = 0xfbdb1d1b18aa6c08324b7d64b71fb76370690e1d
- HMAC_SHA256("", "")
  = 0xb613679a0814d9ec772f95d778c35fc5ff1697c493715653c6c712144292c5ad

수식 : H[(K⁺⊕ opad) || H[(K⁺⊕ ipad) || M]]

↓분석

송수신자가 공유하는 비밀키와 메시지에 대해 해시함수를 적용하여 HMAC를 구한다.

- MAC는 HMAC, CMAC, GMAC, UMAC, VMAC 등으로 구분한다.
- MAC의 기반 기술은 크게 블록암호, 해시함수, 유니버셜 해싱 3가지로 나뉜다.
- HMAC는 송수신자의 공유키와 메시지를 이용하여 해시함수로 MAC를 만드는 것이다.

◈ CMAC
- CMAC는 암호-기반 메시지인증코드이다.
- CMAC는 Cipher-based MAC이다.
- CMAC는 AES와 triple-Des를 주로 이용한다.

◈ UMAC
- UMAC는 Universal-hashing 기반 메시지인증코드이다.
- UMAC는 f(x)=f(y)와 같은 특성을 갖는 해시함수 f를 선택하기 위한 확률적 알고리즘이다.
- UMAC는 해시함수 집합에서 특정 수학적 속성을 통해 해시함수(F)를 선택한다는 것이다.
- 해시함수는 다대일 대응이므로 해시값이 충돌하는 입력값이 반드시 존재한다는 원리이다.
- 유니버셜 해싱은 해시함수의 충돌 확률을 낮추기 위해 등장한 것이다.

◈ VMAC
- VMAC는 블록암호-기반 메시지인증코드이다.
- VMAC는 block cipher-based MAC이다.
- VMAC는 보편적 해시 알고리즘을 사용한다.
- VMAC는 CBC-MAC를 기반으로 발전하고 있다.
- CBC-MAC은 잘 알려진 알고리즘인 CBC 모드를 이용하여 MAC를 생성한다.

◈ GMAC
- GMAC는 Galois/Counter Mode(GCM) 모드의 변종으로 인증에 특화된 알고리즘이다.
- GMAC는 Garter-Wegman 설계 기반으로 고안된 GHASH를 이용하여 MAC를 생성한다.
- GHASH 함수는 이진 Galois체 상에서 곱셈 연산을 수행하는 함수이다.
- GHASH 함수는 키 의존인 Look-Up Table(LUT)을 이용하여 곱셈 연산을 수행한다.
- 체론에서, 갈루아체(Galois field)는 유한개의 원소를 가지는 체이다.
- 갈루아체(Galois field)는 유한체(有限體, finite field)라고도 한다.

◈ PMAC
- PMAC는 Rogaway가 제안한 병렬(parallelizable) MAC 알고리즘이다.
- 최초 PMAC는 그레이코드(gray code) 기반 PMAC를 제안하다.
- 그레이코드 기반 PMAC는 구현의 어려움으로 인해 개량한 PMAC1을 다시 제안하였다.
- PMAC1은 가변길이 블록암호를 이용하여 구현한 것으로 효율성을 향상시켰다.
- PMAC1의 연산 비용과 안성은 기존 CMAC과 유사하다.

정답 : ②

5. 정보보호 및 개인정보보호 관리체계(ISMS-P)의 인증 등에 관한 고시 상의 인증심사 기준 중에서 '개인정보 처리단계별 요구사항'에 포함되지 않는 것은? [2019년 국가 7급]

① 사용자 계정 관리
② 이용자 단말기 접근 보호
③ 영상정보처리기기 설치·운영
④ 개인정보처리방침 공개

♤ **정보보호 및 개인정보보호 관리체계(ISMS-P) - 한국인터넷진흥원 참조**

영역	분야	항목
3. 개인정보 처리단계별 요구사항 (22)	3.1 개인정보 수집 시 보호조치(7)	3.1.1 개인정보 수집 제한
		3.1.2 개인정보 수집 동의
		3.1.3 주민등록번호 처리 제한
		3.1.4 민감정보 및 고유식별정보의 처리 제한
		3.1.5 간접수집 보호조치
		3.1.6 영상정보처리기기 설치·운영
		3.1.7 홍보 및 마케팅 목적 활용 시 조치
	3.2 개인정보 보유 및 이용 시 보호조치(5)	3.2.1 개인정보 현황관리
		3.2.2 개인정보 품질보장
		3.2.3 개인정보 표시제한 및 이용 시 보호조치
		3.2.4 이용자 단말기 접근 보호
		3.2.5 개인정보 목적 외 이용 및 제공
	3.3 개인정보 제공 시 보호조치(3)	3.3.1 개인정보 제3자 제공
		3.3.2 업무 위탁에 따른 정보주체 고지
		3.3.3 영업의 양수 등에 따른 개인정보의 이전
		3.3.4 개인정보의 국외이전
	3.4 개인정보 파기 시 보호조치(4)	3.4.1 개인정보의 파기
		3.4.2 처리목적 달성 후 보유 시 조치
		3.4.3 휴면 이용자 관리
	3.5 정보주체 권리보호(3)	3.5.1 개인정보처리방침 공개
		3.5.2 정보주체 권리보장
		3.5.3 이용내역 통지

• 참고로, 사용자 계정 관리는 **보호대책 요구사항**에 있다.

정답 : ①