ICT의 가치를 이끄는 사람들!!

131회

컴퓨터시스템응용기술사 기출풀이 3교시

T 02.724.1831 E kpcitpe@kpc.or.kr H www.kpc.or.kr C cafe.naver.com/kpcitpe

국가기술자격 기술사 시험문제

정보처리기술사 제 131 회 제 3 교시

분야	정보처리	종목	컴퓨터시스템응용	수험번호		성명	

※ 다음 문제 중 4 문제를 선택하여 설명하시오. (각 25 점)

1. 현재의 딥러닝 기술은 사람의 눈으로 식별되지 않을 만큼 작은 노이즈를 추가해서 만든 적대적 예제(Adversarial Example)를 활용한 공격에 취약하다. 이와 관련하여 다음을 설명하시오.
   가. White-box 및 Black-box 적대적 공격에 대한 개념과 장·단점 비교
   나. 적대적 훈련(Adversarial Training) 및 Defense GAN(Generative Adversarial Networks) 방어기법

2. 개인정보 비식별 처리와 관련하여 다음을 설명하시오.
   가. 개인정보 비식별 처리 유형
   나. 비식별 개인정보의 위험 요인

3. 디스크 여러 개를 활용하여 속도를 높이고 안정성을 향상시키는 기술인 RAID(Redundant Array of Inexpensive Disk) 기술 중 RAID5 와 RAID6 에 대하여 설명하고, 최소 디스크 수량 및 고장 허용 측면에서 비교하여 설명하시오.

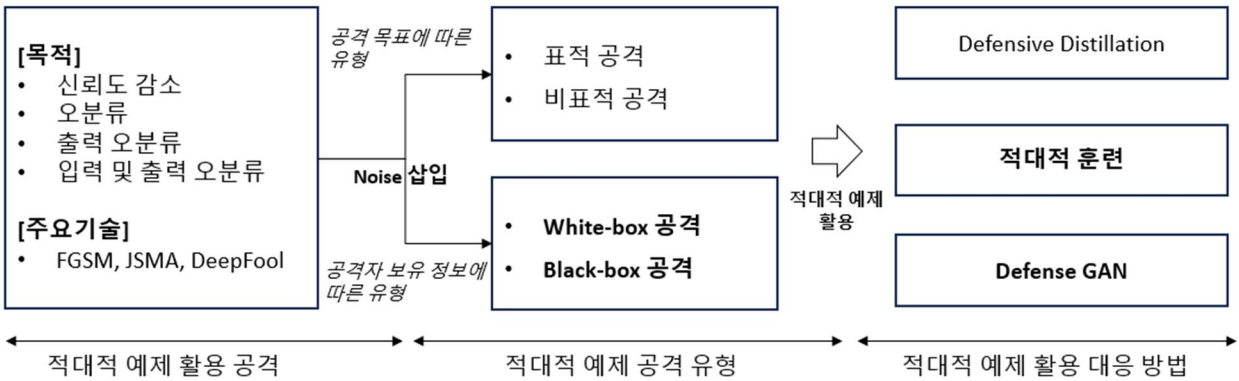
4. 데이터베이스에 사용되는 트랜잭션의 개념과 이를 정의하는 4 가지 중요한 속성을 가리키는 ACID 의 각 요소에 대하여 설명하시오.

5. 공공기관 정보화 사업 추진 시 국가정보원 보안성 검토 절차를 설명하시오.

6. 데이터옵스(DataOps)의 주요 기술을 설명하고, 데브옵스(DevOps)와의 차이점을 설명하시오.

문 제	1. 현재의 딥러닝 기술은 사람의 눈으로 식별되지 않을 만큼 작은 노이즈를 추가해서 만든 적대적 예제(Adversarial Example)를 활용한 공격에 취약하다. 이와 관련하여 다음을 설명하시오. 가. White-box 및 Black-box 적대적 공격에 대한 개념과 장·단점 비교 나. 적대적 훈련(Adversarial Training) 및 Defense GAN(Generative Adversarial Networks) 방어기법
출 제 영 역	인공지능 / 난 이 도 ★★★☆☆
출 제 배 경	- 최근 LLM 등의 인공지능 활용 사례가 늘어나면서 적대적 공격에 따른 위험에 대한 관심도 함께 증가 이중 적대적 예제를 활용한 공격과 대응 방법에 대한 지식 검증 - 130 회 적대적 공격 문제의 확장
출 제 빈 도	130 회 관리, 119 회 응용
참 고 자 료	- KISEC 연구리포트(https://www.kisec.com/rsrh_rpt_det.do?id=221) - 적대적 예제를 활용한 딥러닝에 대한 공격 기술 연구 동향 (DBPia 논문) - 딥러닝 모델에 대한 적대적 예제 공격 기술 동향 연구 (2023 년 한국산학기술학회 춘계 학술발표논문집) - Adversarial Training Methods for Deep Learning(https://www.mdpi.com/1999-4893/15/8/283) - 연구리포트 (https://www.kisec.com/rsrh_rpt_det.do?id=241)
K e y w o r d	- 노이즈 삽입, 모델 내부 정보, 적대적 예제 적용 학습, 노이즈 저항성
풀 이	양재모(130 회 정보관리기술사)

1. 딥러닝 학습의 취약점, 적대적 예제(Adversarial Example)를 활용한 공격의 개요

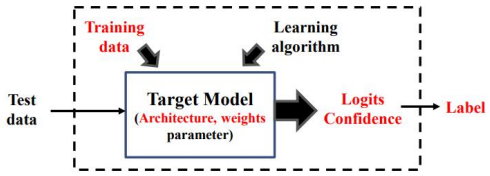


개념	정상적인 입력에 사람이 알아채지 못할 정도로 **작은 노이즈를 추가**해서 딥러닝 모델이 이미지를 올바르게 분류하지 못하도록 **속이거나** 음성을 잘못 인식하도록 **방해하는 공격**

- 적대적 예제를 활용한 공격에는 공격자가 모델에 대한 정보 보유 여부에 따라 **White-box**와 **Black-box** 적대적 공격으로 구분

2. White-box 및 Black-box 적대적 공격에 대한 개념과 장/단점 비교

가. White-box 및 Black-box 적대적 공격에 대한 개념 비교

구분	White-box 적대적 공격	Black-box 적대적 공격
개념	공격자가 모델에 대한 모든 정보를 알고 모델의 구조, 손실 함수, 가중치와 같은 **내부 정보를 이용**한 적대적 공격 기법	공격자가 모델에 대한 정보를 알지 못하고 사전에 제작된 값을 **입력하여 출력되는 결과를 관찰**하며 모델의 취약성을 분석 공격하는 적대적 공격 기법
공격 메커니즘		
공격방식	• 모델 **내부의 손실함수의 기울기**를 따라 올라가는 방향으로 노이즈를 추가	• 질의에 따른 **입력과 출력의 쌍 값**을 분석하여 적대적 모델 생성
활용	• 적대적 예제의 존재를 설명하고 이해하기 위한 연구 활용	• 공격대상 모델의 대체 모델을 학습 연구나 질의 효율성 증가 연구에 활용

- White-box 공격은 성공률이 높지만 정보를 수집하기는 어려워 상대적으로 공격이 용이한 Black-box 공격을 많이 시도

나. White-box 및 Black-box 적대적 공격의 장/단점 비교

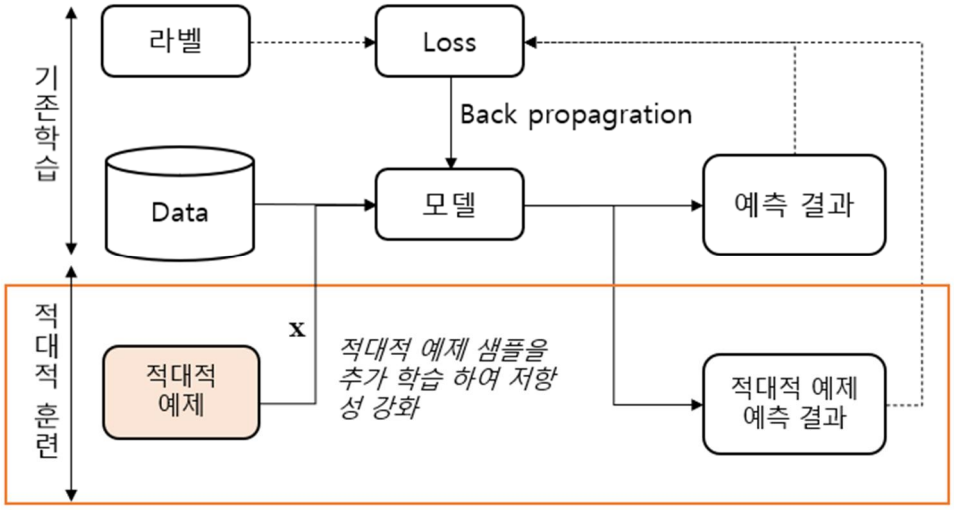
구분	White-box 적대적 공격	Black-box 적대적 공격
장점	• 높은 공격 성공률 • 높은 쿼리(Query) 효율성 • 공격 성공 시 치명적 결과 초래	• 공격을 위한 모델 정보 불필요 • 분류된 라벨만 볼 수 있는 제한된 환경에서도 활용 가능 • 공격 수행 방식이 용이
단점	• 공격하는 과정이 복잡하고 난해 • 높은 공격 난이도 • 현실적으로 어려운 공격 방식	• 공격 성공률이 다소 낮은 한계점 • 낮은 쿼리(Query) 효율성

- 적대적 공격에 대한 대응으로는 적대적 예제를 학습 데이터로 적용해 노이즈에 대한 모델 견고성을 높이는 **적대적 훈련** 및 **Defense GAN** 방어 기법을 활용

3. 적대적 훈련 및 Defense GAN 방어기법 설명

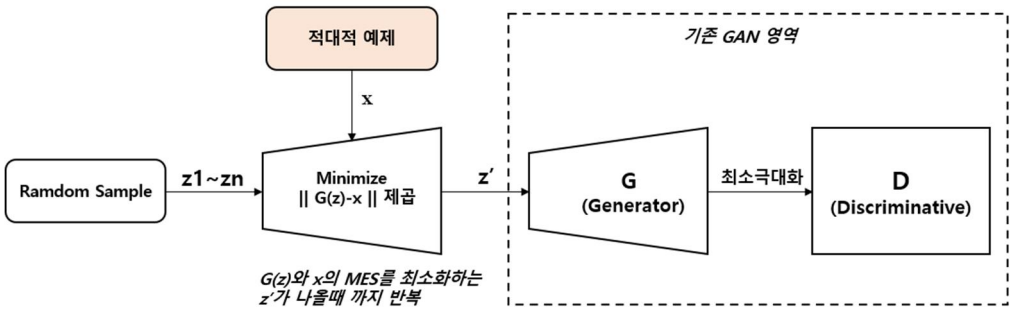
가. 적대적 훈련(Adversarial Training)

개념	모델 학습 시 적대적 예제를 학습 데이터 셋에 포함시켜 모델 학습 진행, **모델의 저항성**을 기르는 적대적 공격 방어 기법

메커니즘		
절차	1. 적대적 예제 생성	• FGSM, JSMA, DeepFool 등 기법 활용
	2. 모델 학습	• 기존 학습에 적대적 예제 샘플을 함께 추가 모델 학습
	3. 모델 강화	• 학습 결과를 역전파하여 모델을 강화
주요 특징	적대적 예제 활용	• 적대적 예제와 깨끗한 샘플을 일반화하도록 모델 훈련
	노이즈 강건성	• 노이즈 기반 적대적인 공격에 대한 모델의 견고성 향상

- GAN 학습 방법에서 적대적 예제를 활용하여 적대적 공격을 방어하는 기법으로 **Defense GAN** 을 활용

나. Defense GAN(Generative Adversarial Networks) 방어기법

개념	최소극대화(Minimax)의 원리로 학습하는 GAN 에 적대적 예제를 추가학습 데이터로 활용 노이즈 제거가 가능한 새로운 생성 데이터로 학습하는 방어 기법	
메커니즘		
절차	1. 적대적 예제 적용	• 램덤 생성 데이터와 적대적 예제간의 MES 최소값
	2. New 생성 데이터(z') 생성	• 생성 이미지와 적대적 예제의 차이를 최소화하는 새로운 생성 데이터(z')후 GAN 수행
주요 특징	다양한 공격에 적용가능	• White-box, Block-box 공격 대응 가능
	기존 분류기 수정 불필요	• 기존 모델의 분류기(Classifier)의 수정 없이 공격에 대한 방어가 가능

- 적대적 예제 공격에 대한 방어 연구와 더불어 적대적 예제를 생성하는 연구 또한 활발하게 진행

4. 최신 적대적 예제 공격 기술

JND-based Attack	GMM(Gaussian Mixture Model)
• 이미지의 형태를 분석하여 JND 프로파일을 만들고, 이를 기반으로 노이즈를 삽입하는 방식	• 픽셀 단위(Pixel-wise) 노이즈가 아니라 인접 픽셀과의 연관성을 고려하여 이미지 전체적으로 부드러운(Global Smooth) 노이즈를 삽입 방식
• 시각적 차이 최소화 공격 기법	• 혼합된 clustering 알고리즘
• JNDp 거리지표 사용	• 이미지 패치(Patch) 간의 유사도를 측정

- 적대적 예제에 대한 연구와 공격 기법이 고도화됨에 따라 이를 대응하기 위한 비지도 학습 기반의 대응 기술 연구 중

또는

5. 추가적 적대적 공격 방어 기법

방어 기법	설명
• Gradient Masking	• 학습 모델의 Gradient 가 출력으로 노출되지 않도록 난독화 처리
• Distillation	• 학습 모델의 결과값들이 학습 방향에 대한 정보를 제공하지 못 하도록 보완

- 인공지능에 모든 프로세스를 전적으로 의지하는 것보다는 인간의 검증 단계를 통해 데이터가 오염되지 않았는지, 모델이 오작동하고 있는지 등 모니터링하고 점검하는 것이 필요

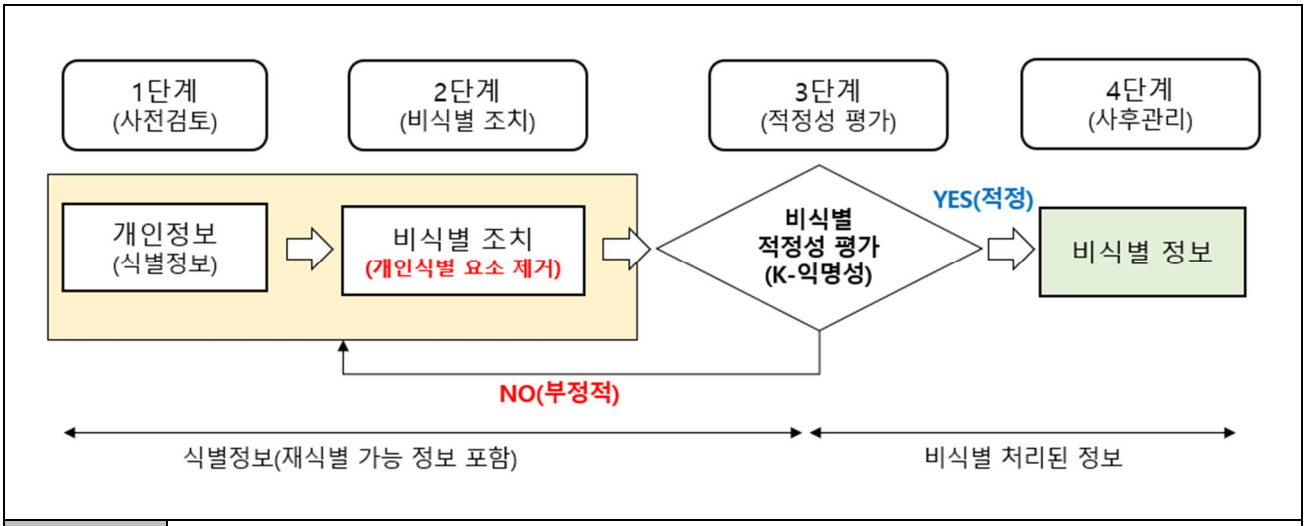
"끝"

기출풀이 의견

1. 문제에서 제시된 적대적 예제를 활용한 공격과 방어 기술 관점으로 논리적인 답안을 작성하면 좋은 점수를 받을 수 있을 것 같습니다.
2. White-box와 Black-box 공격은 유추를 통해 접근이 가능한 문제지만 적대적 훈련과 Defense GAN은 정확한 메커니즘의 제시가 필요합니다. 추가적인 적대적 공격 방어기법이나 최신 공격/방어 기술을 함께 제시한다면 고득점이 가능할 것 같습니다.

문 제	2. 개인정보 비식별 처리와 관련하여 다음을 설명하시오. 가. 개인정보 비식별 처리 유형 나. 비식별 개인정보의 위험 요인		
출 제 영 역	보안	난 이 도	★★★☆☆
출 제 배 경	- 개인정보보호에 대한 요구사항이 꾸준히 늘어나고 있고 '개인정보 비식별 조치 가이드라인'과 ISO 20889 기반으로 하는 비식별 조치 관련 지식 검증		
출 제 빈 도	118 관리, 110 관리		
참 고 자 료	- 개인정보 비식별 조치 가이드라인 (2016, 행정안전부) - 개인정보 비식별 조치를 위한 데이터 상황 기반 위험도 측정 방법 및 타당성 연구 (논문)		
K e y w o r d	- 가명화, 총계, 마스킹, 삭제, 범주화, 암화화, 재현 데이터, 재식별 위험		
풀 이	양재모(130 회 정보관리기술사)		

1. 개인정보 비식별 처리 개요



개념	정보집합물(데이터 셋)에서 개인을 식별할 수 있는 요소를 전부 또는 일부 삭제하거나 대체하는 등의 방법을 활용하여 개인을 알아볼 수 없도록 하는 조치

- **개인정보 비식별 가이드라인**에 따른 **가명**, **총계**, **삭제**, **범주화**, **마스킹**의 개인정보 비식별 처리 유형이 존재

2. 개인정보 비식별 처리 유형

가. 일반적 개인정보 비식별 처리 유형

처리유형	설명	세부기술
가명처리 (Pseudonymization)	• 식별자 데이터를 임의의 데이터로 변환하는 비식별 하는 기법 • 사례) 홍길동, 35 세, 서울 거주, 한국대 재학 -> 임꺽정, 30 대, 서울 거주, 국제대 재학	• 휴리스틱 가명화 • 암호화 • 교환방법

총계 처리 (Aggregation)	• 식별될 수 있는 특징 데이터를 총계나 평균치 등의 계산하여 비식별하는 기법 • 사례) 임꺾정 180cm, 홍길동 170cm, 이콩쥐 160cm, 김팥쥐 150cm -> 물리학과 학생 키 합 : 660cm, 평균키 165cm	• 총계처리 • 부분총계 • 라운딩 • 재배열
데이터 삭제 (Data reduction)	• 식별자 데이터를 삭제하거나 부분 삭제 함으로 특정인을 알 수 없게 하는 기법 • 사례) 주민등록번호 909999-19999999 -> 90 년대 생 남자	• 식별자 삭제 • 식별자 부분삭제 • 레코드 삭제 • 식별요소 전부삭제
데이터 범주화 (Data suppression)	• 식별 데이터를 평준화, 범주화 하여 특정인을 구별할 수 없게 하는 기법 • 사례) 홍길동, 35 세 -> 홍길동, 3~40 세	• 감추기 • 랜덤 라운딩 • 제어 라운딩 • 범위 방법
데이터 마스킹 (Data Masking)	• 특정인임을 추론할 수 있는지 여부를 검토하여 일정 확률 수준 이상 비식별 되도록 하는 기법 • 사례) 홍길동, 35 세, 서울 거주, 한국 대학 재학 -> 홍 OO, 35 세, 서울 거주, OO 대학 재학	• 임의 잡음추가 • 공백과 대체

- 이외에 **ISO 20889** 에서 제시하는 암호화 도구, 해부화, 일반화, 재현 데이터 등의 처리 유형이 존재

나. 비식별 처리 유형

처리유형	설명	세부기술
암호화 도구 (Encryption)	• 암호화 기법을 적용하여 원본 값의 기밀성을 강화한 기법	• 순서보존/형태 보존 암호화 • 동형암호화
해부화 (Anatomization)	• 기존 하나의 데이터셋을 식별성의 유/무에 따른 2 개의 데이터셋으로 분리 기술	• 식별자 컬럼 분할 • 분석 컬럼 분할
재현데이터 (Synthetic data)	• 원본과 최대한 유사한 통계적 성직을 보이는 가상 데이터를 생성	• 완전 재현 데이터 • 부분 재현 데이터
무작위화 (Randomization)	• 개인정보에 임의의 Noise 를 추가하거나 순서 변경, 대체 등의 기법	• 순열, Noise 추가 • 부분 총계
차분 프라이버시 (Differential privacy)	• 질의 결과 변화량을 일정수준 이하로 유지하여 추론에 의한 개인정보 노출 제한 기법	• 라플라스 매커니즘 • 익스퍼넨셜 매커니즘

- 비식별 조치를 해도 공개 정보와 결합해 재식별 가능성이 있으므로 보호모델(**K-익명성, L-다양성, T-근접성**)을 이용하여 재식별 방지
- 비식별 개인정보는 재식별에 대한 위험 요인과 활용 과정에서의 악용 및 관리 조치 미흡 등의 위험 요인 존재

3. 비식별 개인정보의 위험 요인

가. 재식별 가능성 측면의 위험 요인

구분	개인정보 위험 요인	설명
내부요인	• 재식별 우려 정보 수집 • 정보 결합 위험	• 재식별 우려가 있는 추가적인 정보를 수집하였거나 생성된 정보에 의한 결합으로 재식별 위험 발생
	• 낮은 비식별 수준 설정 • 보안체계 취약성	• 비식별 수준을 낮게 유지하거나 비식별 정보의 접근 관리 통제의 보안체계에 이상 위험
외부요인	• 비식별 기법 무력화 기술	• 비식별 기법과 기술을 무력화하는 새로운 기술이 등장하거나 공개
	• 새로운 연계 정보 출현	• 이용 중인 데이터와 새롭게 연계 가능한 정보가 출현하거나 공개

- 비식별 개인정보의 활용 과정에서 불법적 이용이나 관리 조치 위반등의 위험 요인 존재

나. 활용 측면에서의 비식별 개인정보의 위험 요인

활용 단계	위험 요인	설명
수집	• 불법 비식별 개인정보 수집 • 비식별 조치에 따른 정보 변경	• 허가되지 않는 비식별 개인정보 수집 • 데이터 변경에 따른 정보의 변조
보유/이용	• 제 3 자의 불법접근 • 안전조치 위반	• 허가 받지 않는 접근에 의한 정보 유출 • 비식별 개인정보 관리의 안전조치 위반
정보제공	• 재식별 위험 • 비식별 개인정보 유출	• 불특정 다수에게 공개하는 경우 식별 위험 발생 • 해킹에 의한 정보 유출
파기	• 정보 미 파기	• 컴플라이언스 위반

- 비식별 개인정보의 위험 요인을 제거하기 위하여 내부관리계획을 수립하고 기술적, 관리적 보호조치를 수립/시행 필요

4. 비식별 정보 안전 조치 방안

구분	비식별 정보 보호 조치
관리적 보호조치	• 비식별 정보 파일 관리담당자 지정 • 비식별 정보파일 대장 관리 • 원본저장 관리부서와 비식별 정보 관리부서간 비식별 정보 공유 금지 • 이용목적 달성 시 지체 없이 파기 • 비식별 정보파일 유출 시 대응계획 수립
기술적 보호조치	• 비식별 정보 파일에 대한 접근 권한 관리 및 접근통제 • 비식별 정보관리 시스템에 대한 접속기록 관리 • 악성코드 방지 등을 위한 보안프로그램 설치/운영

- 비식별 조치된 정보가 유출되는 경유 다른 정보와 결합하여 식별될 우려가 있으므로 필수적인 보호조치 이행

또는

5. 비식별 위험 최소화를 위한 프라이버시 보호 모델

활용 단계	위험 요인	설명
K-익명성	• 특정인임을 추론할 수 있는지 여부를 검토, 일정 확률수준 이상 비식별 조치	• 동일한 값을 가진 레코드 K개 이상 • 연결공격 방어
L-다양성	• 민감한 정보의 **다양성**을 높여 추론 가능성을 낮추는 기법	• 최소 L개 이상의 다양성 레코드 • 동질성, 배경지식 공격 방어
T-근접성	• 민간함 정보의 **분포**를 낮추어 추론 가능성을 더욱 낮추는 기법	• 전체 데이터 집합의 정보 분포와 특정 정보의 분포 차이를 T이하로 유지 • 쏠림, 유사성 공격 방어

- 비식별 개인정보의 재식별 위험성을 최소화하기 위한 방안으로 재식별 가능성 검토 보호 모델를 이용

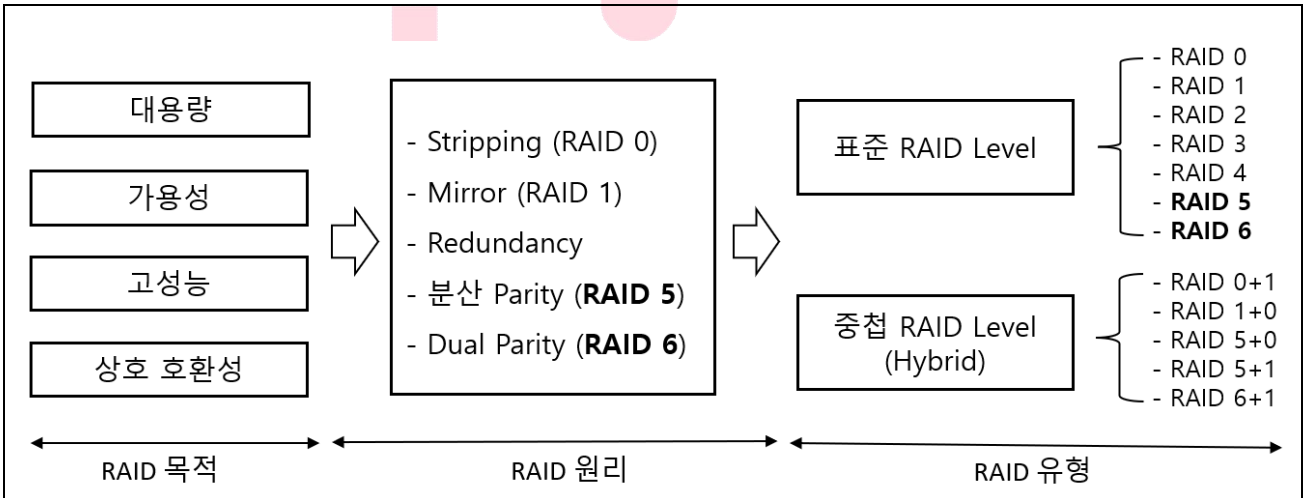
"끝"

기출풀이 의견

1. 비식별 처리 유형은 기본 토픽으로 가능한 많은 처리 유형을 제시하여 차별화를 가져야 할 것 같습니다.
2. '비식별 개인정보의 위험요인'에 대한 작성이 어려웠을 것으로 예상됩니다. 위험요인에 대한 정확한 가이드 문서는 없으므로 일반적인 위험 요인을 다양한 관점에서 제시하고 이에 대한 대응 조치 방안을 함께 제시하면 좋을 것 같습니다.

문 제	**3. 디스크 여러 개를 활용하여 속도를 높이고 안정성을 향상시키는 기술인 RAID(Redundant Array of Inexpensive Disk) 기술 중 RAID5 와 RAID6 에 대하여 설명하고, 최소 디스크 수량 및 고장 허용 측면에서 비교하여 설명하시오.**		
출 제 영 역	CA/OS	난 이 도	★★☆☆☆
출 제 배 경	- 빈출인 RAID 에서 분산 Parity 를 지원하여 내 고장성을 높인 RAID5 와 RAID6 에 대한 심화 지식 검증		
출 제 빈 도	125 응용, 122 응용, 120 관리, 117 응용, 99 관리		
참 고 자 료	- RAID 정리 (https://devocean.sk.com/blog/techBoardDetail.do?ID=163608) - RAID 란? (https://kimhyun2017.tistory.com/17) - 120 회 기출 풀이집		
Keyword	- 고가용성, 단일 볼륨, 안전성, 분산 Pariry, Dual Parity		
풀 이	양재모(130 회 정보관리기술사)		

1. 시스템 고가용성을 위한 RAID 의 개요

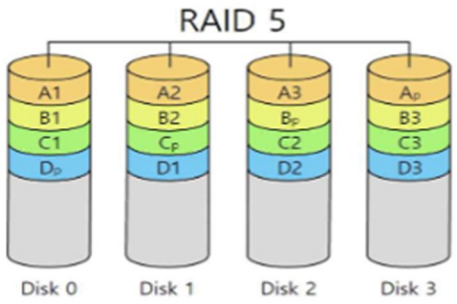


개념	데이터를 여러 개의 디스크에 중복(Mirror), 분산(Stripping) 저장 및 복구 정보를 저장하여 고성능, 고가용성 및 손실 데이터의 복구가 가능한 기술	
기대효과	단인 볼륨 이용	• 대용량의 단일 볼륨을 사용하는 효과
	성능 향상	• 디스크 I/O 병렬화로 인한 성능 향상 (RAID 0, RAID 5, RAID 6)
	안전성 확보	• 데이터 복제로 인한 안정성 향상 (RAID 1, RAID 5, RAID 6)

- 모든 디스크에 Parity 정보를 분산 저장하여 하드 디스크에 문제가 발생해도 **데이터를 복구 가능**한 **RAID 5, RAID 6** 구성 존재

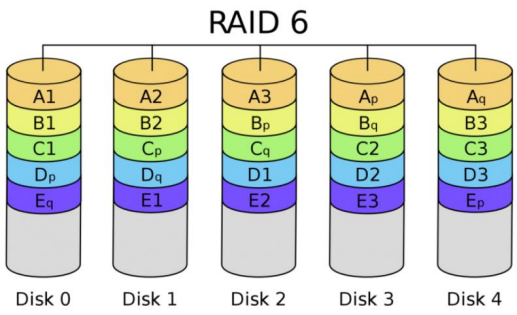
2. RAID 5 와 RAID 6 설명

가. Parity 분산, RAID 5

구분		설 명
개념		• 블록은 모든 디스크에 나누어서 저장하지만 균등하지 않음 • 패리티 정보도 모든 디스크 분산 저장 • 용량: C=(N-1)*D (C: 총 용량, N: Disk 개수, D: HDD 용량)
성능	• 읽기 성능 우수(N-1 배), 쓰기 성능 저하	
장점	• 일반적으로 1 개의 디스크 고장 허용, 읽기 속도 우수	
단점	• 디스크 재구성이 매우 느리고 패리티 정보 갱신으로 인해 쓰기 성능 저하	

- RAID5 보다 공간 효율은 낮은 반면 내 고장성을 높이기 위해 Dual Parity 비트를 사용한 RAID 6 사용

나. Dual Parity 분산, RAID 6

구분	주요 서비스	설 명
개념		• RAID 5 와 유사한 구조로, Block 레벨의 Striping 과 Double Parity 사용(Parity 분산 제공) 하는 RAID
성능	• 읽기 성능은 RAI5 와 유사, 이중 패리티로 인해 쓰기 트랜잭션이 매우 느림	
장점	• 높은 내 고장성, 디스크가 최대 2 개까지 고장나도 데이터 손실이 미 발생	
단점	• Dual Parity 사용으로 내부적인 쓰기 알고리즘이 복잡 해저 RAID 5 보다 조금 낮은 성능 (고장 난 디스크 동기화 속도 저하) • 높은 구현 난이도, 복원시간이 많이 걸림	

- RAID5 는 1 Parity 비트, RAID6 는 2 Parity 비트를 분산 저장하여 각각 3 개, 4 개의 최소 디스크가 필요

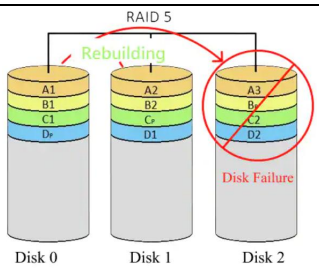
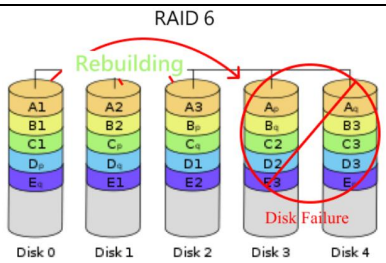
3. RAID 5 와 RAID 6 의 최소 디스크 수량 및 고장 허용 측면 비교

가. 최소 디스크 수량 측면에서의 RAID 5 와 RAID 6 비교

구분	RAID 5	RAID 6
최소 디스크 수량	• **3 개** (권장 5 개 이상)	• **4 개**
공간 효율	• **1-1/n** (n: Disk 수량) • (사례) 10 개의 디스크 구성시 90%	• **1-2/n** (n: Disk 수량) • (사례) 10 개의 디스크 구성시 80%
Parity 수	• 1 개	• 2 개

- RAID6 가 RAID5 에 비해 데이터의 신뢰성을 높일 수 있으나 공간 효율과 성능적 측면으로 RAID5 를 주로 사용

나. 고장 허용 측면의 RAID5 와 RAID6 비교

구분	RAID 5	RAID 6
고장 허용 디스크 수	• Parity 중복 개수(일반적 1 디스크)	• 2 디스크
복구 메커니즘		
복구 원리	• 분산된 Parity bit 의 짝수/홀수를 체크하여 손실된 데이터 복구	• 각각의 분산 Parity bit 의 값을 체크하여 손실된 데이터 복구

- RAID 6 가 RAID 5 에 비해 데이터의 신뢰성을 높일 수 있으나 공간 효율과 성능적 측면으로 RAID 5 나 RAID 0+1, RAID 1+0 등의 Hybrid 구성을 주로 사용

4. 가용성을 위한 주요 Hybrid RAID 구성

구분	RAID 5+1	RAID 0+1	RAID 1+0
특징	• RAID5 구성 후 RAID1 묶음 • 1 은 Spare	• RAID0 구성 후 RAID1 묶음 • Striping -> Mirroring	• RAID1 구성 후 RAID0 묶음 • Mirroring ->Striping
최소수량	• 6 개	• 4 배수	• 4 배수
공간효율	• 낮은 공간 효율성	• N * 2 / D	• N * 2 / D
고장허용	• 2	• 0 쌍 아닌 2 개	• 1 내에 하나

- 실제 환경에서는 공간 효율과 성능적 측면으로 RAID 5 나 RAID 0+1, RAID 1+0 등의 하이브리드 구성을 주로 사용

"끝"

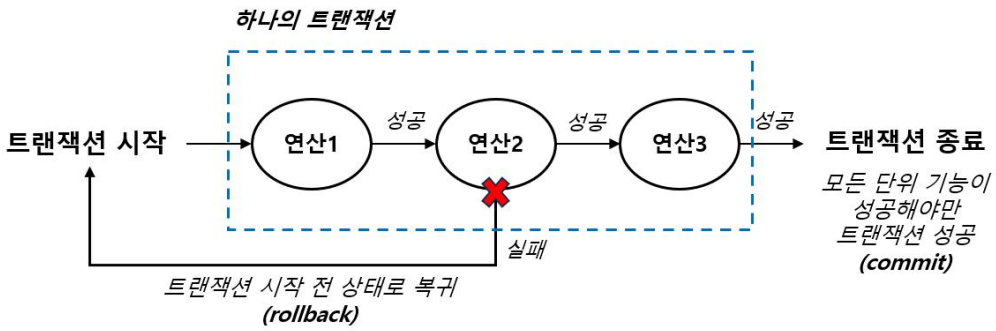
기출풀이 의견

1. RAID는 빈출 항목으로 유형과 각각의 상세 특징까지 꼭 암기해서 정확하게 작성해주는 것이 중요합니다.
2. RAID의 전체적인 개요와 함께 문제에서 요구한 RAID5, RAID6에 대한 Fact를 기술하고 추가적인 RAID에 대해 적어주면 좋은 점수가 기대됩니다.

문 제	4. 데이터베이스에 사용되는 트랜잭션의 개념과 이를 정의하는 4 가지 중요한 속성을 가리키는 ACID 의 각 요소에 대하여 설명하시오.		
출 제 영 역	데이터베이스	난 이 도	★★☆☆☆
출 제 배 경	- 데이터베이스의 기본 토픽인 트랜잭션의 개념과 특성에 대한 지식 검증		
출 제 빈 도	129 관리, 116 응용, 107 관리, 90 회 관리/응용, 81 회 관리		
참 고 자 료	- 도리의 디지털라이프(https://blog.skby.net/) - 위키피디아 (https://ko.wikipedia.org/wiki/ACID)		
K e y w o r d	- 논리적 작업단위, Commit, Rollback, 원자성, 일관성, 고립성, 영속성, 분산 트랜잭션, SAGA		
풀 이	양재모(130 회 정보관리기술사)		

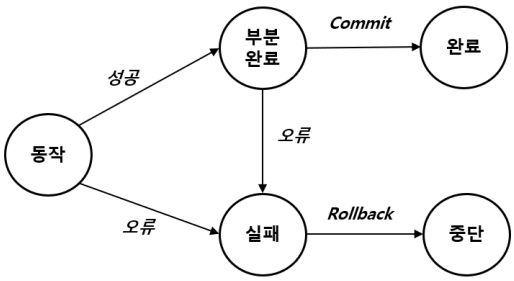
1. 데이터베이스의 논리적 작업 단위, 트랜잭션의 개념

가. 트랜잭션의 개념

분류	설 명	
트랜잭션 매커니즘		
개념	데이터베이스를 조작하기 위한 하나의 **논리적 작업 단위**를 이루는 일련의 **연산의 집합**	
트랜잭션 연산	Commit	• 갱신 연산이 완료되었다고 트랜잭션 관리자에게 알려주고 결과를 최종적으로 데이터베이스에 반영하는 연산
	Rollback	• 트랜잭션이 지금까지 실행한 연산의 결과가 취소되고 트랜잭션 수행 이전의 상태로 돌아가는 연산

- 트랜잭션 완료 시 Commit, 미완료 시 Rollback 을 통해 데이터베이스의 일관성을 유지
- 트랜잭션 수행 중 상태 값의 관리를 통해 실패 시 이전 상태로 복구, 트랜잭션 원자성 유지

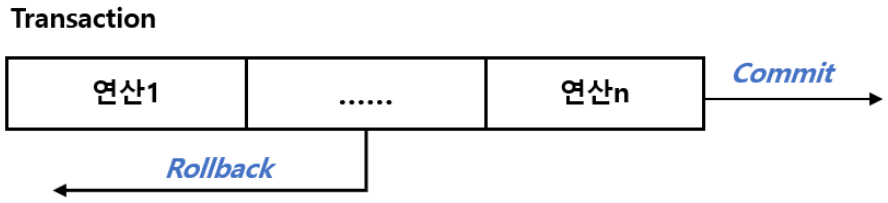
나. 트랜잭션의 상태

상태 Diagram	상태	
	동작	• 트랜잭션 실행 시작, 진행
	부분완료	• 마지막 명령문 실행 직후
	완료	• 트랜잭션 성공적 실행 완료
	실패	• 논리적, 시스템 오류 발생
	중단	• 트랜잭션 시작 전 상태로 환원

- 트랜잭션이 안전하게 수행된다는 것을 보장하기 위해 데이터베이스는 **원자성(Atomicity)**, **일관성(Consistency)**, **고립성(Isolation)**, **영속성(Durability)의** 4 가지 **ACID 속성**을 보장

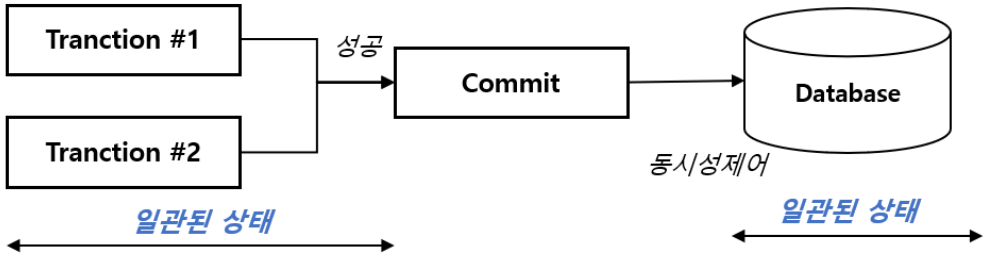
2. 원자성과 일과성 ACID 요소 설명

가. 원자성(Atomicity)

분류	설 명	
개념	분해가 불가능한 수행 단위로 완전히 수행, 수행되지 않는 상태를 유지 트랜잭션을 구성하는 연산은 반드시 모두 실행이 되거나 혹은 아예 실행되지 않아야 하는 속성	
매커니즘		
특징	• All or Nothing	• 모든 트랜잭션은 성공이 아니면 실패
보장기법	• 회복 기법	• Commit or Rollback

- 실행 도중에 오류가 발생하여 작업을 완료하지 못하였다면, 트랜잭션 전체를 취소하여 원자성 유지

나. 일관성(Consistency)

분류	설 명	
개념	트랜잭션이 성공적으로 완료되면 언제나 모순이 없는 상태 유지되는 속성	
매커니즘		
특징	• 동시성 제어를 통한 모순 발생 방지	• 무결성 제약조건, 사용자가 요구하는 논리적 요건의 충족
보장기법	• 동시성 제어 기법	• 무결성 제약 조건, Locking, Timestamp, Validation

- 일관성은 트랜잭션이 실행을 성공적으로 완료하면 언제나 일관성 있는 데이터베이스 상태로 유지

3. 고립성과 영속성 ACID 요소 설명

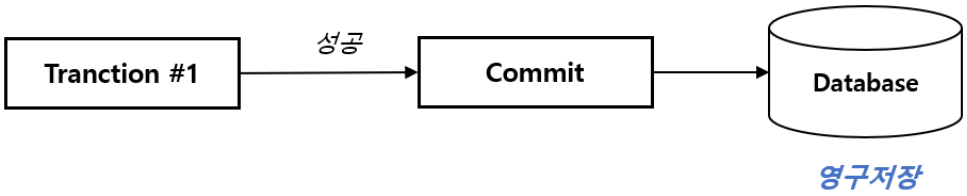
가. 격리성 (Isolation)

분류	설 명
개념	트랜잭션은 다른 트랜잭션에 간섭을 주거나 받지 않고 독립적으로 수행되는 속성

매커니즘		
특징	• 트랜잭션 간의 Commit 전의 참조 방지	• 수행 중 다른 트랜잭션의 간섭 방지
보장기법	• 동시성 제어	• Locking, Isolation Level, 상호배제

- 고립성은 어떤 트랜잭션도 다른 트랜잭션의 Commit 이 완료되기 전까지 부분 참조 불가 특성

나. 영속성 (Durability)

분류	설 명	
개념	트랜잭션이 성공적으로 완료되었을 때 그 결과는 영구적으로 반영되는 속성	
매커니즘		
특징	• 장애 발생 시 복구를 위한 방안 제공	• 완료 후 DB 반영 보장
보장기법	• 회복 기법	• Archive, 로그, Redo/Undo 기반 회복, Checkpoint

- 영속성은 시스템의 장애가 발생하더라도 결과는 데이터베이스에 그대로 남아있어야 하며, 지속성을 보장하기 위해서 회복 기능이 필요
- 트랜잭션은 ACID 특성을 기반으로 무결성과 직렬성, 회복성을 보장받음

4. 데이터베이스 트랜잭션 수행 보장 기법

분류	보장기법	설 명
단일 트랜잭션 원자성 보장 측면	Log 기록	- 트랜잭션 및 데이터 식별자, 갱신 전/후 데이터 값 등 관리
	Commit	- 트랜잭션 내 모든 개별연산 성공 시 DB 영구 저장
	Rollback	- 트랜잭션 수행 실패 시 변경 내역 폐기
	Redo	- 장애로 인해 디스크에 기록되지 않은 커밋 트랙잭션 회복
멀티 트랜잭션 동시 수행 보장 측면	직렬화 검사	- 충돌 직렬성 검사 통한 일관성 검증. 우선순위 그래프 활용
	Locking	- Lock 소유 기반 접근 제어. Shared/Exclusive Lock 활용
	Timestamp	- 고유 Timestamp 부여. 시스템 클락/논리적 계수기 활용
	Snapshot	- 동시성 향상 위한 변경 데이터 버전 관리. MVCC

- 최근 확산되는 MSA(Micro Service Architecture) 환경의 Polyglot 구조에 대한 트랜잭션 관리는 SAGA 패턴 활용

"끝"

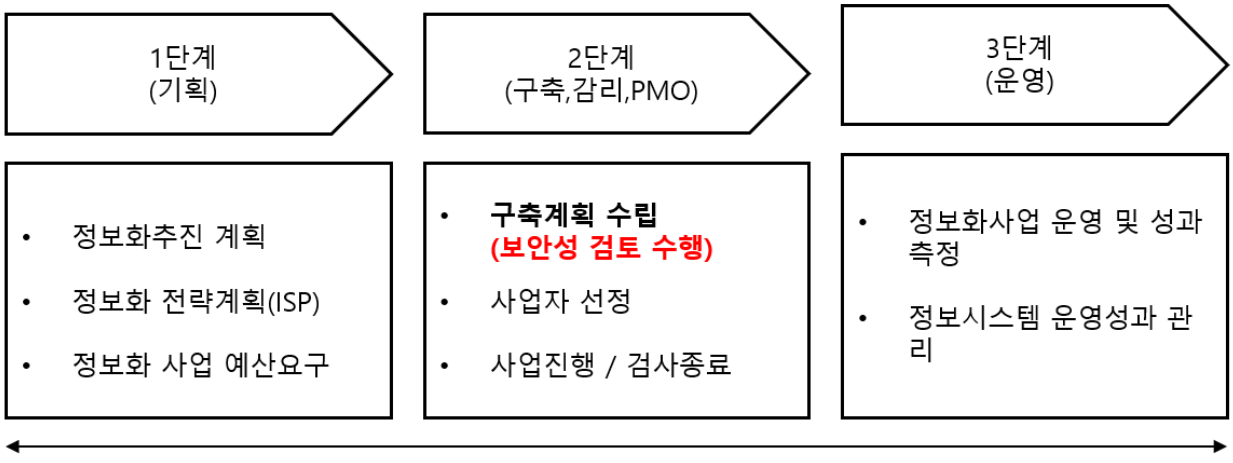
기출풀이 의견

1. 트랜잭션은 DB 기본 토픽으로 최근 자주 출제되기 때문에 개념, ACID 특성, 상태 전이도, 동시성 제어, 보장 기법 등을 학습 내재화가 필요합니다.
2. 트랜잭션의 개념에서는 관련된 정보를 가능한 많이 압축해서 제시하고 ACID는 주요 특징들이 잘 구별되도록 그림과 함께 관련 키워드들을 작성해 주면 좋은 점수가 나올 것 같습니다.

문 제	5. 공공기관 정보화 사업 추진 시 국가정보원 보안성 검토 절차를 설명하시오.		
출 제 영 역	보안	난 이 도	★★★★☆
출 제 배 경	- 공공기관 정보화 사업 추진 시 수행하는 보안성 검토 절차에 대한 지식 검증		
출 제 빈 도	- 미출제		
참 고 자 료	- 국가 정보보안 기본지침 (국가정보원) (https://www.ncsc.go.kr:4018/main/cop/bbs/selectBoardArticle.do?bbsId=InstructionGuide_main&nttId=18588&pageIndex=1#LINK) - 공공정보화사업 단계별 사업관리 가이드(2023.2) - SI 프로젝트 보안성 검토를 위한 점검항목 기준 개선 연구 (논문) - [기고] 보안성 검토 (https://www.comworld.co.kr/news/articleView.html?idxno=49506)		
Keyword	- 사업 계획단계, 검토요청, 검토의뢰, 검토/결과 통보, 검토결과 반영		
풀 이	양재모(130 회 정보관리기술사)		

1. 공공기관 정보화 사업에서의 보안성 검토 개요

가. 국가정보원 보안성 검토의 개념 및 필요성



개념	정보화사업을 수행하고자 할 경우 정보화사업과 관련한 **보안대책의 적절성을 평가**하기 위하여 **사업 계획단계**(사업 공고 전)에서 **국가정보원**을 통해 이행하여야 하는 보안 확인 절차	
필요성	사전 위험관리	• 자산, 위협, 취약점과 같은 위험 구성요소에 대한 사전 보호대책수립
	침해 대응	• 잠재적 위협을 사전에 제거 DDoS 나 랜섬웨어 등 보안사고 대응
	개인정보보호	• 개인정보 유출 및 오용을 방지 및 개인정보보호 강화

- 보안성 검토는 **사업계획 단계(해당 사업 공고일 최소 5 일 이전)**에 국가정보원에 보안성 검토 의뢰

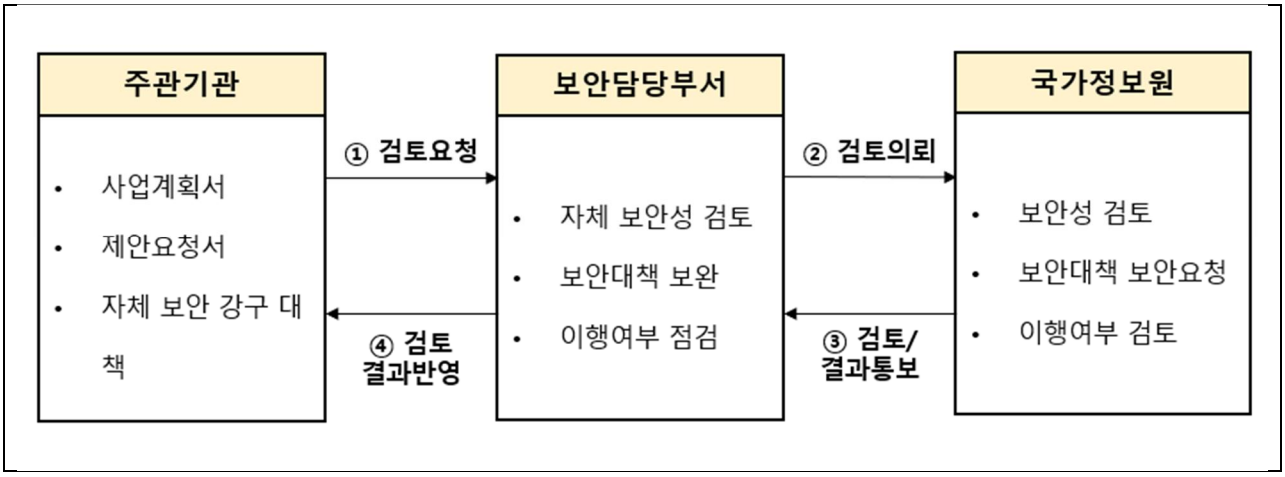
나. 국가정보원 보안성 검토 대상 사업

대상 사업	주요 사업 사례
비밀, 국가안보, 정부정책 관련 사업	• 비밀·대외비를 유통·관리하기 위한 정보통신망 또는 정보시스템
대규모 크기와 다량의 DB 자료 처리 사업	• 다량의 개인정보(100 만 명 이상)를 처리하는 정보시스템 구축
외부기관간 망 연동 및 보안 취약 사업	• 내부망 또는 폐쇄망을 인터넷 또는 다른 정보통신망과 연동하는 사업
보안정책 과제 및 최신 IT 기술 적용	• 첨단 정보통신기술을 활용하는 정보화사업으로 안전성 확인 필요 사업

- 보안성 검토는 서면 검토를 원칙으로 하며 보안성 검토 기관의 장의 판단에 따라 현장 확인을 병행 실시

2. 국가정보원 보안성 검토 절차 설명

가. 국가정보원 보안성 검토 절차도



- 보안성 검토 대상 사업은 국가정보원에 보안성 검토를 의뢰하고 검토 이행 후 보완 조치사항을 사업에 반영

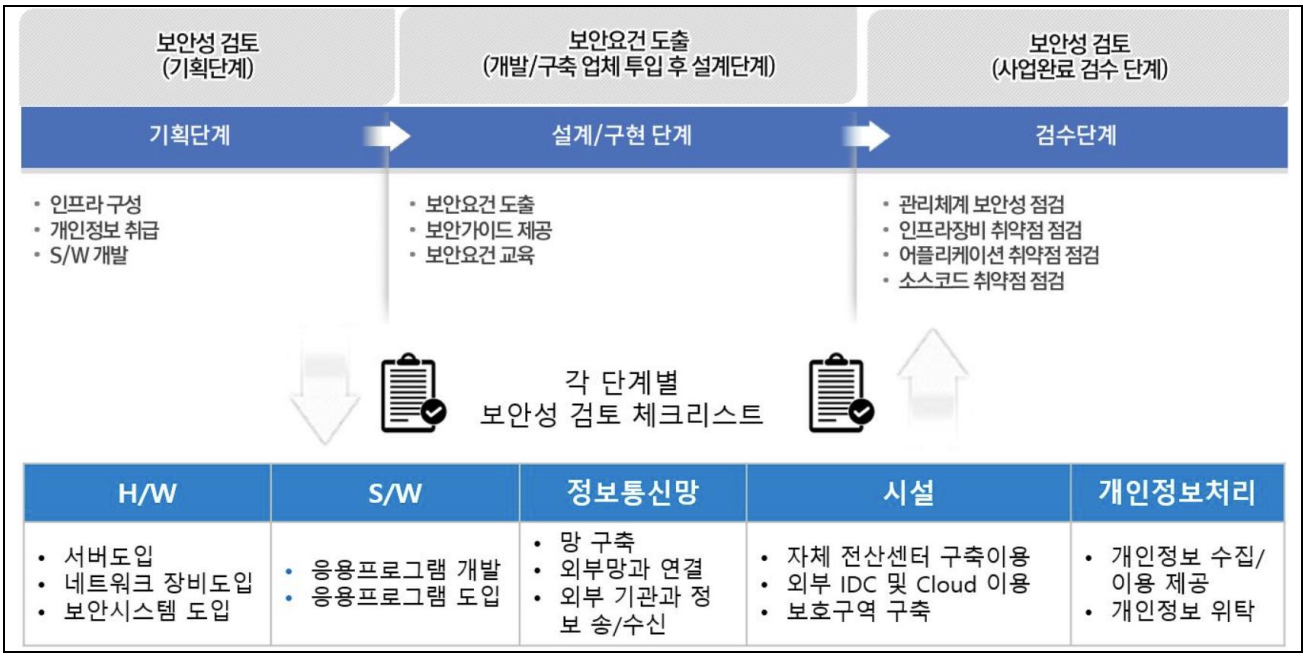
나. 국가정보원 보안성 검토 절차 상세

절차	수행 내용	상세설명
1. 검토요청	• 보안대책 수립	• 사업 계획 단계에서 보안대책 수립
	• 보안성 검토 요청	• 보안담당부서에 보안성 검토 필요성 여부 확인 요청
2. 검토의뢰	• 자체 보안성 검토	• 자체적으로 보안성 검토 및 보안대책 보완
	• 국가정보원에 검토 의뢰	• 보안성 검토 필요시 국가정보원에 검토 의뢰
3. 검토/결과통보	• 보안성 검토 수행	• 정의한 계획에 따라 취약점 스캔, 코드 리뷰 등을 이용하여 보안취약점 탐지
	• 보안성 검토 결과 통보	• 취약점, 위험평가, 추진 사항, 개선방안을 상세히 기술
4. 검토결과 반영	• 보완 사항 반영	• 취약점에 대해 보안 패치, 업데이트, 보안정책 변경
	• 이행여부 점검	• 검토결과 반영 여부 확인을 위해 현장 점검 실시

- 공공 상급기관은 하급기관의 정보화사업에 대한 보안성 검토결과 현황을 매년 국가정보원에 제출

3. 정보화사업 수행 단계별 국가정보원 보안성 검토와 주요 체크 항목

가. 정보화사업 수행 단계별 국가정보원 보안성 검토



- 사업 분야에 따른 보안성 검토 체크리스트 작성해 보안성 검토를 수행

나. 국가정보원 보안성 검토 주요 체크 항목

구분	주요 체크 항목	상세 체크 내용
물리적 시설 보안	• 장비 설치 위치의 안전성	• 시스템운영실 별도 운영
	• 외부인 출입통제	• 지문, IC 카드, CCTV 설치
정보시스템 보안 대책	• 중요시스템 파일 접근제어	• 네트워크 설정, CRON, 디파이스 파일 등
	• 국가정보원에 검토 의뢰	• 보안성 검토 필요시 국가정보원에 검토 의뢰
네트워크 보안	• 전송 데이터 암호화	• 암호화 비도, TLS, DTLS, SSL
	• 네트워크 분리 운영	• 내부망, 공개망, DMZ 등
애플리케이션 보안	• 애플리케이션 소스통제	• 형상관리, 접근 권한 제어
	• 암호통신	• 통신방법, 프로토콜, 알고리즘, 키관리

- 보안성 검토를 효율적으로 수행하기 위하여 사전 검토 체계와 체크리스트 최적화 고려

4. 국가정보원 보안성 검토 시 고려사항

고려사항	내용
• 분야에 맞는 보안성 검토 체계 만들기	• 정보화 사업마다 시스템에 따른 보안적 요소들이 상이 • 사업 분야에 따른 검토 체계를 구성
• 보안성 검토 체크리스트 항목 선정	• 체크 항목 중복 최소화 • 점검 항목 누락이 발생하지 않도록 체크 항목 검증

- 공공기관 정보화 사업은 국가정보원 보안성 검토와 행정안전부 사전협의 결과를 사업계획서에 반영하여 최종 사업계획서를 확정

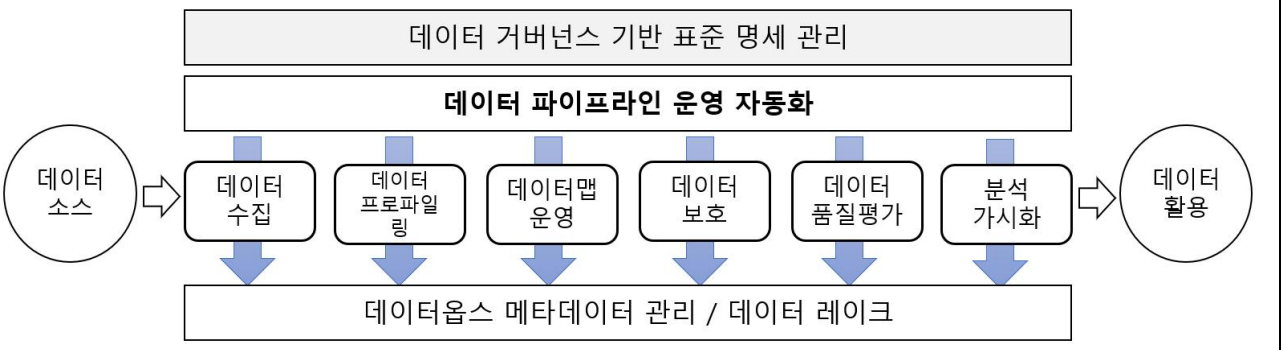
"끝"

기출풀이 의견

1. 공공정보화사업 단계별 사업관리 가이드(2023.2)에 제시된 국가정보원 보안성 검토 절차 내용을 물어본 문제로 정확한 절차 내용의 기술이 중요합니다.
2. 정확한 절차를 기술하고 추가적으로 국가정보원 보안성 검토 관련 정보를 함께 기술한 경우 고득점이 가능하지만 잘 모르는 경우 선택하지 않는게 좋겠습니다.

문 제	6. 데이터옵스(DataOps)의 주요 기술을 설명하고, 데브옵스(DevOps)와의 차이점을 설명하시오.		
출제영역	디지털서비스	난 이 도	★★☆☆☆
출제배경	- 130 회 정보관리에 출제된 문제의 교차 출제 - 데이터옵스에 대한 기술적 이해와 데브옵스와의 차이에 대한 이해 검증		
출제빈도	- 130 회 정보관리		
참고자료	- 데이터옵스(DataOps) (https://itpenote.tistory.com/729) - 데이터옵스(DataOps) 프레임워크를 개발하고 적용하는 방법(논문, DBPia)		
Keyword	- 데이터 파이프라인/기술/프로세스, 운영 자동화, 자동 배포, 데이터 가상화, 데이터 품질		
풀 이	양재모(130 회 정보관리기술사)		

1. 데이터중심 기업을 위한, 데이터옵스의 개요



개념	데브옵스 팀과 데이터 엔지니어, 데이터 과학자 역할을 결합해 데이터 중심 기업을 지원하는 도구, 프로세스, 조직체계	
주요요소	데이터 파이프라인	• 데이터 수집, 데이터 엔지니어링, 데이터 분석
	데이터 기술	• 데이터 캡처, 데이터 통합, 데이터 준비, 데이터 분석
	데이터 프로세스	• 개발 및 배포, 오케스트레이션, 지속적 테스트

- 데이터를 생산·수집·가공·분석하는 체계인 데이터 플랫폼을 통해 신속한 배포 및 부가가치가 높은 고품질의 가치 창출

2. 데이터옵스의 주요 기술

가. 데이터옵스의 데이터 처리 기술

구분	주요기술	설명
데이터 관리 기술	• 데이터 카탈로그	• 데이터에 대한 중앙 집중화된 메타 데이터 저장소
	• 데이터 가상화	• 물리적 데이터에 독립적으로 통합 수집, 저장, 조회, 분석
	• 데이터 파이프라인	• 수집, 전처리, 통합, 변환, 저장과 분석의 자동화 시스템
지원도구	• 데이터 버전 관리	• 변경 추적과 관리로 데이터 무결성과 신뢰성 유지 도구
	• 테스트 및 배포 자동화	• 데이터 및 응용소프트웨어의 개발, 테스트 배포의 자동화
데이터 지능화	• 데이터 모델링용 AI	• 비즈니스 요구 적합한 모델생성과 통찰력 획득 지원도구

플랫폼 기술	• 클라우드 및 가상화	• 스토리지 가상화, 멀티/하이브리드 클라우드 기술 요소
	• 플랫폼 보안과 통제	• ZeroTrust, SIEM 및 플랫폼의 보안기술과 통합제어 기술

- 데이터옵스 기술로 수동작업의 큰 감소와 데이터파이프 라인 개발과 데이터 분석의 가속화

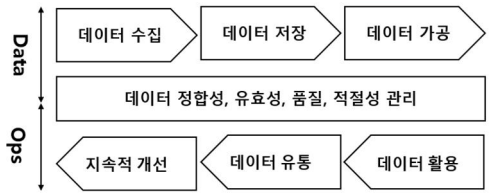
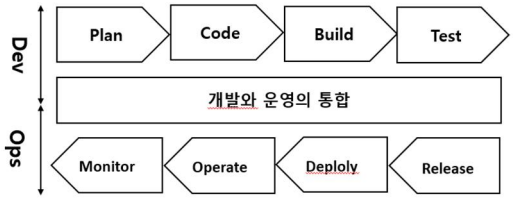
나. 데이터옵스의 운영 기술

구분	주요기술	설명
운영/관리 기술	• 개발 및 자동 배포	• 프로덕션 환경으로 코드/구성을 이동, Jenkins, CircleCI
	• 오케스트레이션	• 파이프라인이 실행되는 동안 관련된 모든 도구를 오케스트레이션, Grafana
환경 관리	• 이력 및 메타 데이터	• 시스템 및 활동 로그 관리, ModgoDB, Logback
	• 환경 생성 및 관리	• 데이터옵스 환경에 대한 접근 제어, OAuth2.0
보안 기술	• 접근 제어 및 통제	• 환경내 도구 및 리소스에 대한 역할 기반 접근, Vault
	• 인증 및 권한	• 환경에 대한 접근 제어, OAuth2.0, MFA

- 데이터옵스는 프로세스 자동화 측면에서 데브옵스와 유사하지만 목적과 주요 활동에 차이점 존재

3. 데이터옵스와 데브옵스의 차이점

가. 데이터옵스와 데브옵스의 개념 차이점

구분	데이터옵스	데브옵스
개념	사용자에게 신뢰할 수 있는 고품질 데이터를 빠르게 제공하기 위해 사람, 프로세스 및 기술을 융합하여 데이터 흐름의 통합과 자동화를 개선하는 방법론	개발팀과 운영팀을 제품 또는 서비스를 담당하는 단일 유닛으로 통합해 시스템 개발 생애주기 동안 지속적인 전달, 배포를 제공하는 소프트웨어 개발 방법론
프레임워크		

- 데이터옵스는 데브옵스를 포함하며 데이터 활용을 개선하려는 기술적 문화적 변화

나. 데이터옵스와 데브옵스의 상세 차이점

구분	데이터옵스	데브옵스
목적	• 데이터 파이프라인 최적화로 의사결정 지원	• 개발과 운영의 협업과 통합 강화
주요 활동	• 데이터 수집, 전처리, 통합, 모델링, 테스트 배포 포함한 데이터 파이프라인 관리	• 개발, 테스트, 빌드, 배포, 모니터링 포함한 SW 생명주기 파이프라인 관리
가치제공	• 데이터 엔지니어링, 분석, 데이터 과학, BI	• 소프트웨어 엔지니어링
품질보증	• 데이터 거버넌스 • 데이터 프로세스 제어	• 코드 릴리즈 • 지속적 테스트 및 모니터링

적용범위	• 조직 전체	• 개발팀과 운영팀
주요이점	• 데이터 서비스 기반 정책결정 지능화 • 데이터 분석 최적화	• 빠른 개발과 지속적 배포 및 팀 협업 • 개발과 운영의 Silo 제거
주요 관계자	• 데이터 엔지니어, 데이터 과학자 • 데이터 분석가, 데이터 전문가	• 소프트웨어 엔지니어 및 개발자 • 시스템 관리자와 운영자, 테스터

- 데이터옵스의 데이터 관리와 가치 실현을 위하여 데브옵스가 조직내 선행 필요

4. 데이터옵스의 성공요소와 고려사항

구분	핵심 요소	설명
핵심 성공 요소	• 메타데이터 관리 확장	• 다크데이터의 최소화와 기업의 데이터 컴플라이언스 연계
	• 자동화 확장	• 복잡한 작업의 정렬과 연결로 자동화된 파이프라인 구축
	• 정책기반 제어와 구성	• 시스템은 데이터 관리 정책과 인프라 구조에 따라 통제
고려사항	• 사용자 교육과 지원	• 단순 도구가 아닌 기업 문화의 변화가 가능한 인식 개선
	• 법적 규정 준수	• 데이터 통합과 관리를 위한 법적 영향 사전 조사 및 분석

- 데이터 거버넌스 기반위에 기업의 데이터와 애플리케이션 개발의 협력이 데이터옵스 성공의 핵심

"끝"

기출풀이 의견

1. 전 회차 기출로 데이터옵스의 배경이나 일반적인 내용보다는 기술적 특징이 드러나도록 프레임워크, 아키텍처, 기술 특징 등을 상세하게 적어주면 좋겠습니다.
2. 데이터옵스와 데브옵스의 차이점이 한눈에 잘 드러나도록 구성도를 포함하여 설명하고 4단락에 성공을 위한 고려사항 등 추가 내용을 함께 적어주면 고득점이 가능할 것 같습니다.