제39회 ITPE 실전 명품 모의고사 해설집

2025.12.21

제 39 회 ITPE 실전 명품 모의고사

일시 : 2025 년 12 월 21 일 제 4 교시(시험시간: 100 분)

분야	정보통신	자격종목	정보관리 컴퓨터 시스템 응용	수검 번호		성 명	

※ 다음 문제 중 4 문제를 선택하여 설명 하십시오. (각 25 점)

1. 최근 기업 시스템 환경은 온프레미스 방식에서 클라우드 환경으로 빠르게 전환되고 있으며 이에 따라 데이터베이스도 전통적인 방식에서 클라우드 네이티브 방식으로의 전환이 확산되고 있다. 다음에 대해 설명하시오.

   가. 클라우드 네이티브 데이터베이스의 정의

   나. 기존 데이터베이스와의 비교

   다. 클라우드 네이티브 데이터베이스 도입 시 고려사항

2. AI/ML 모델의 성능은 데이터 품질에 의해 좌우되며, 데이터 품질 향상을 위해 데이터의 전처리를 수행하고 있다. 다음에 대해 설명하시오.

   가. 데이터 전처리 설명

   나. 정규화(Normalization)과 표준화(Standardization)

   다. 피처 엔지니어링(Feature Engineering)

3. 최근 기업의 보안사고 증가에 따라 정부에서는 CISO(Chief Information Security Officer)기업 대상으로 자체 취약점 진단을 시행하여 결과를 보고하도록 하였다. 다음을 설명 하시오

   가. 취약점 진단 절차

   나. 애플리케이션 취약점 진단 방법

   다. 인프라 취약점 진단 방법

4. 데이터 마이닝의 이상탐지 기법 중 시계열 데이터 이상탐지는 시스템의 안정성과 신뢰성을 위한 필수 기술이다. 다음을 설명하시오

가. 시계열 데이터 이상탐지의 개념 및 목적

나. 시계열 데이터 이상탐지의 알고리즘

다. 시계열 데이터 이상탐지의 적용사례

5. 디지털 전환이 가속화되고 제조·물류·의료 등 주요 산업에서 자동화와 지능화가 빠르게 확산되면서, AI가 소프트웨어 영역을 넘어 물리적 공간에서 자율적으로 판단·행동하는 '피지컬 AI(Physical AI)'의 중요성이 증가하고 있다. 다음에 대해 설명하시오.

가. 피지컬 AI의 개념과 유형

나. 피지컬 AI의 핵심 기술

다. 피지컬 AI의 도입 시 고려사항

[정보관리기술사 선택문제]

6. FTP(File Transfer Protocol)에 대하여 다음을 설명하시오.

가. FTP 개념

나. Active Mode와 Passive Mode 비교

다. FTP Bounce Attack의 공격원리와 대응방안

[컴퓨터시스템응용기술사 선택문제]

6. CPU 스케줄링 방식에 대해서 다음을 설명하시오.

가. 선점형 스케줄링 기법

나. 비선점형 스케줄링 기법

다. 호위효과(Convey Effect)

01	클라우드 네이티브 데이터베이스(Cloud Native Database)		
문제	최근 기업 시스템 환경은 온프레미스 방식에서 클라우드 환경으로 빠르게 전환되고 있으며 이에 따라 데이터베이스도 전통적인 방식에서 클라우드 네이티브 방식으로의 전환이 확산되고 있다. 다음에 대해 설명하시오. 가. 클라우드 네이티브 데이터베이스의 정의 나. 기존 데이터베이스와의 비교 다. 클라우드 네이티브 데이터베이스 도입 시 고려사항		
도메인	디지털서비스	난이도	상 (상/중/하)
키워드	컨테이너, 자동화, AIOps, 고가용성, 민첩성, 효율화		
출제배경	클라우드 네이티브 확산		
참고문헌	https://payproglobal.com/ko/ https://www.ddaily.co.kr/page/view/2025030207254725832		
출제자	이다연 기술사(제 135회 정보관리기술사 / dlekdusz@naver.com)		

I. 클라우드 환경 최적화 DB, 클라우드 네이티브 데이터베이스(Cloud Native Database)의 정의

가. 클라우드 네이티브 데이터베이스(Cloud Native Database)의 정의

- 클라우드 환경을 기반으로 설계하고 컨테이너, 스토리지, 자동화 기반 운영 등 클라우드의 고유 특성을 활용하여 구현한 데이터베이스

나. 클라우드 네이티브 데이터베이스(Cloud Native Database)의 필요성

클라우드 네이티브 시스템 전략적 대응	- 기업 IT 시스템이 클라우드로 이전함에 따라 클라우드에 최적화된 DB를 활용한 시스템 구축 필요성 증가
고가용성 확보	- 전통DR 센터 대비 비용 절감 - 자동 Fail-over 제공
비즈니스 민첩성 요구	- 신규 DB 구축 시간 및 비용 감소 - DevOps 파이프라인 내 DB로 활용 가능
운영 효율화	- 클라우드 가격 정책 기반 비용 산정 가능 - 자동화된 인프라로 운영 배포 시간 단축

- 기존 데이터베이스와 비교하여 운영 효율성 및 확장성, 고가용성을 제공하여 도입 확산 추세

II. 클라우드 네이티브 데이터베이스(Cloud Native Database)와 기존 데이터베이스와의 비교

가. 기술적 관점에서의 기존 데이터베이스와의 비교

비교 항목	기존 데이터베이스	클라우드 네이티브 데이터베이스
아키텍처	- 단일 인스턴스 중심	- 분산 구조
확장 방식	- Scale-up	- Scale-out
데이터 저장 방식	- 로컬 스토리지	- 분산 스토리지
자동화 수준	- 제한적 자동화	- AIOps 활용 자동화
배포 방식	- 물리환경 기반으로 수동배포	- 컨테이너 활용한 지속적 배포

튜닝 방식	- DBA 분석 후 적용, 수동방식	- AIOps 활용한 자가 진단 및 적용

- 클라우드 기반 기술 활용하여 고가용성 구성 및 자동화 통한 운영 효율성 향상

나. 관리적 관점에서의 기존 데이터베이스와의 비교

비교 항목	기존 데이터베이스	클라우드 네이티브 데이터베이스
비용	- 초기 구축비용 및 구매비용, 유지보수 비용 증가	- 사용량 기반 요금제 활용 가능, CAPEX 최소화
확장성	- 사전 필요 용량 산정 - 용량 증설 시 다운타임 발생	- Autoscaling 적용하여 자동 확장 가능
장애 대응	- 로컬 또는 DRaaS 연계 필요	- Multi-AZ(Ability Zone) 활용 자동 조치
거버넌스/감사대응	- 변경 이력 수동 관리 - 낮은 표준화 수준	- IaC 기반 이력 관리 - 높은 표준화 수준
벤더 종속성	- HW, SW의 종속성 심화	- 다수의 MSP 선택 가능

III. 클라우드 네이티브 데이터베이스 도입 시 고려사항

가. 기술적 측면 고려사항

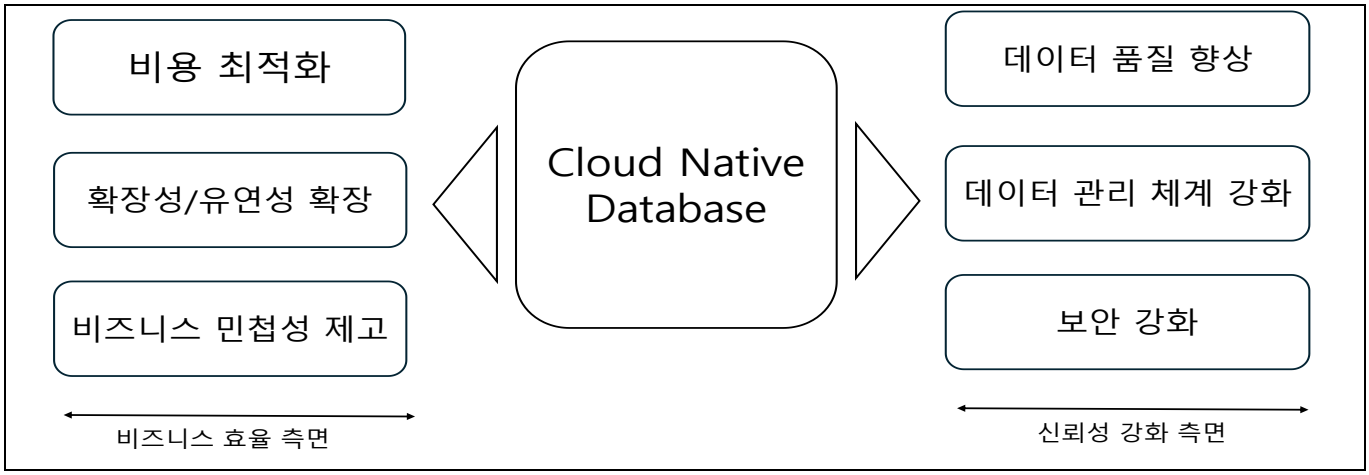
구분	고려사항	설명
DB 전환 측면	- 처리 성능 확인	- 분산 스토리지 구조 따른 트랜잭션 지연 여부 확인
	- SQL 호환 여부	- 온프레미스 환경에서의 SQL 정상 실행 확인 - 쿼리 실행 계획 확인하여 성능 검증
	- 스키마 호환성 확인	- 기존 데이터 마이그레이션 가능 여부 확인 - Procedure, index, column, data type 사용 가능 여부 확인
	- 스토리지 구조 선택	- Shared-nothing, Shared-disk 구조 따른 성능 일관성 영향 검토
협업 기술 측면	- 기존 시스템과의 호환성	- 클라우드 환경에 최적화 되어있지 않은 시스템과 연동 시 성능저하 발생
	- 기술 연계 가능 여부	- Helm, CRI, CRI-O 와 같은 클라우드 기술 연계 가능여부 확인
DB 성능 측면	- 쿼리 성능 최적화	- 분산 옵티마이저, CBO 통한 최적화 수행
	- 시스템 부하 대응	- 쿼리 오프로딩, 샤딩, 파티셔닝 통한 부하 분산
데이터 품질 측면	- 데이터 일관성 모델 선택	- Strong/Weak/Eventual 모델 중 적합 모델 선정
	- 트랜잭션 처리 기술 적용	- 2PC, SAGA 패턴 등과 같은 처리 기술 적용하여 일관성 유지
네트워크 보안 측면	- 네트워크 접근 제어	- 방화벽, WAF 적용하여 네트워크 공격 사전 감지
	- 보안 정책 적용	- 중요 데이터에 대한 접근 권한 분리, 암호화

나. 관리적 측면 고려사항

구분	고려사항	설명
데이터 관리 측면	- 데이터 품질 관리	- 정확성, 일관성 등을 기준으로 메타데이터, 데이터 카탈로그 관리
	- 데이터 이관 계획 수립	- 온프레미스 환경의 데이터를 클라우드로 이관 시 검증, 데이터 연속성 확보 위한 방안 마련
	- 데이터 라이프사이클 관리	- 백업, 아카이빙 기준 마련, 보존주기 정립 통한 수명관리
정책측면	- 도입 목적 명확화	- 조직의 IT 전략과 데이터 거버넌스 방향을 정렬, 일관성있는 운영 가능하도록 기반 마련
	- 거버넌스 체계 수립	- 이해관계자 R&R 명확화, 변경/장애/품질 관리 프로세스 수립
	- 컴플라이언스 준수 확인	- 개인정보보호법, ISMS-P와 같은 관련 규제 준수 여부 점검
보안 /위험관리 측면	- 보안 정책 적용	- 데이터 암호화, 분리보관, 접근제어를 클라우드 환경에도 적용할 수 있는 정책 마련
	- 감사 및 모니터링 실시	- 보안 정책이 제대로 동작하는지 상시 감독 체계 구축 및 피드백
	- 장애 관리	- DRaaS 통한 클라우드 기반 장애 대응 및 백업 체계 마련
	- 벤더 종속성 관리	- 특정 CSP 에 의존하지 않도록 벤더 중립적 설계, 멀티 클라우드 활용
비용 관리 측면	- FinOps 통한 관리	- 클라우드 과금 모델 고려한 비용 산정 - 트래픽 사용 분석 통한 비용 최소화 방안 마련
	- IaC 통한 운영 자동화	- 자동백업/패치 통한 운영 효율성 증가 및 비용 감소 효과

- 클라우드 네이티브 데이터베이스 적용 시 클라우드 및 데이터베이스 전환 시 발생할 수 있는 문제들에 대한 대응방안 마련 필

IV. 클라우드 네이티브 데이터베이스 적용 시 기대효과

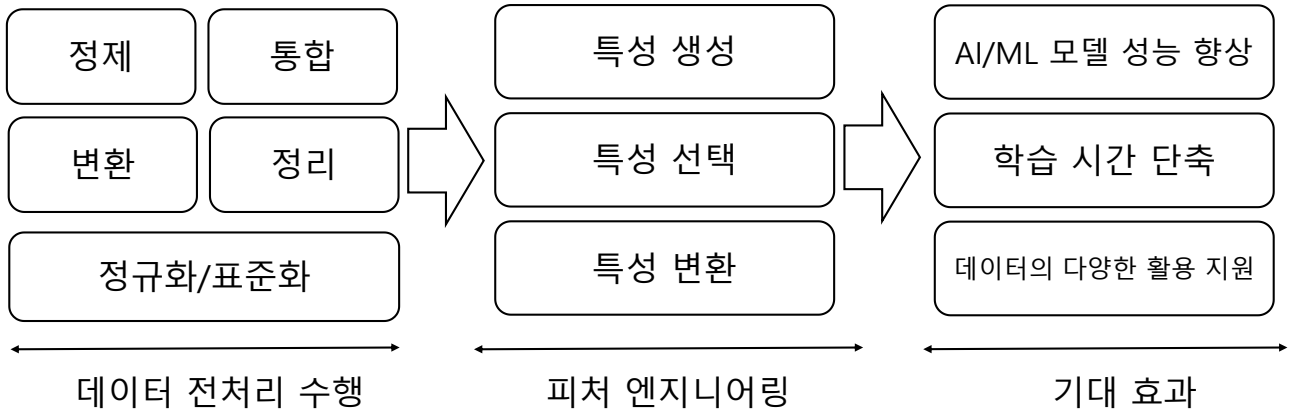


- 클라우드 네이티브 데이터베이스 적용 시 클라우드 최적화된 향상된 성능으로 데이터 처리 및 관리가 가능하여 데이터 신뢰성 및 품질 향상 통한 비즈니스 가치 실현 가능

"끝"

02	데이터 전처리(Data Preparation)		
문제	AI/ML 모델의 성능은 데이터 품질에 의해 좌우되며, 데이터 품질 향상을 위해 데이터의 전처리를 수행하고 있다. 다음에 대해 설명하시오. 가. 데이터 전처리 설명 나. 정규화(Normalization)과 표준화(Standardization) 다. 피처 엔지니어링(Feature Engineering)		
도메인	확률/통계	난이도	중 (상/중/하)
키워드	정제, 통합, 변환, 정리, 정규화, 정규화, 표준화, 특성 선택, 특성 변환, 특성 생성		
출제배경	인공지능 학습 데이터 관리 위한 전처리 기법의 전반적인 이해 확인		
참고문헌	https://m.blog.naver.com/kgitdream/223228828237 https://blog.naver.com/branson_note/223569254978 https://scikit-learn.org/stable/api/sklearn.preprocessing.html https://m.blog.naver.com/femold/223075605378 ITPE 기술사회 서브노트		
출제자	이다연 기술사(제 135회 정보관리기술사 / dlekdusz@naver.com)		

I. AI/ML 모델 성능 향상 위한, 데이터 전처리의 개요

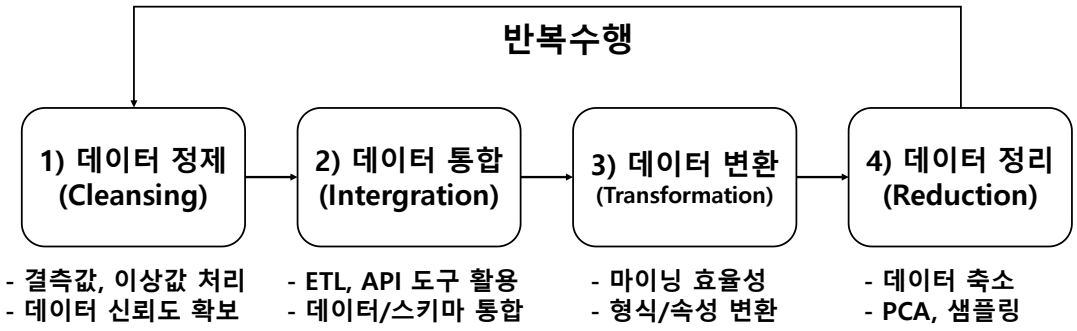


개요	- 우수한 성능의 AI/ML 모델 개발을 위해 데이터 전처리(Data Preparation) 과정을 통해 학습에 필요한 데이터 품질을 검증하고 향상하는 과정이 선행적으로 수행되어야 함

II. 데이터 전처리 설명

가. 데이터 전처리 개념 및 프로세스 설명

구분	설명
개념	- 수집한 데이터의 불완전(incomplete), 불일치(inconsistent) 요소 및 잡음(noisy)를 제거하여 데이터 분석 및 처리에 적합한 형식으로 변환함으로써 자료의 정합성과 가치를 확보하기 위한 데이터 처리 기법

<table>
<tr><td>프로세스</td><td colspan="2"> 
</td></tr>
<tr><td rowspan="4">단계별
상세 설명</td><td>1) 데이터 정제
(Cleansing)</td><td>- 레코드 집합, 테이블, 데이터베이스에서 손상되거나 부정확한 레코드를 검색 및 수정 또는 제거하는 과정</td></tr>
<tr><td>2) 데이터 통합
(Integration)</td><td>- 여러 소스의 데이터를 통합하여 하나의 구조로 합침
- ETL 등과 같은 통합 도구를 활용하여 데이터/스키마 통합</td></tr>
<tr><td>3) 데이터 변환
(Transformation)</td><td>- 하나의 형태에서 다른 형식이나 구조로 데이터 변환</td></tr>
<tr><td>4) 데이터 정리
(Reduction)</td><td>- 차원 축소, 특징 선택, 학습/검증/테스트로 데이터셋 분할</td></tr>
</table>

- 다양한 데이터 전처리 기법을 통해 데이터의 잡음과 불일치를 제거함으로써 품질 향상 가능

나. 데이터 전처리 기법 설명

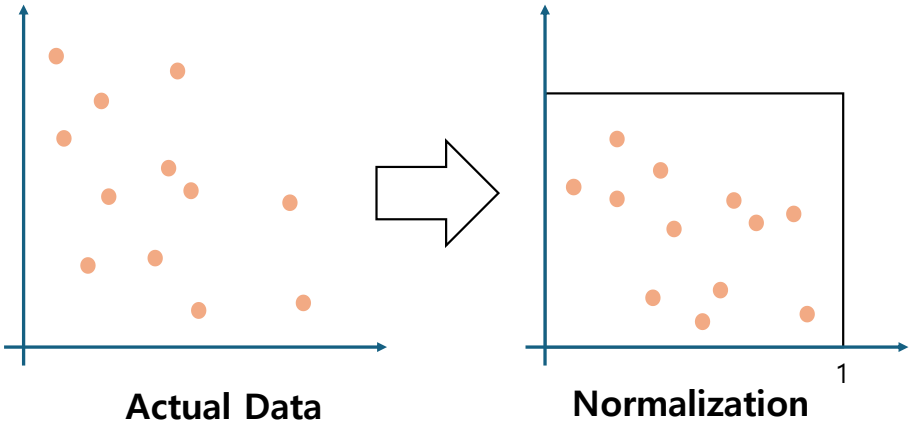
구분	전처리 기법	설명
결측치 처리	- 결측치는 처리 불가능 하기 때문에 결측치를 가진 행 또는 열을 삭제 또는 대체 처리	
	- 결측치 삭제	- 결측치를 포함한 행 또는 열을 삭제
	- 결측치 대체	- 결측치를 최빈값, 중간값, 평균값 등으로 대체
샘플링	- 전체 데이터 중 필요한 일부 데이터만 선택	
	- 단순확률 추출	- 모집단에서 샘플을 균등하게 임의 추출
	- 계통 추출	- 샘플에서 일정 간격을 두고 샘플 추출
	- 층화 확률 추출	- 모집단이 몇 개의 계층으로 구성되어 있을 때 각 계층으로부터 임의 추출
	- 집락(군집) 추출	- 모집단이 여러 군집일 경우, 우선 군집을 선택하고 군집 내에서샘플 추출
범주형 데이터 인코딩	- 알고리즘이 범주형 데이터를 이해할 수 있도록 변환	
	- 원-핫 인코딩(One-Hot Encoding)	- 범주형 벡터를 0과1 벡터로 변환
	- 라벨 인코딩(Label Encoding)	- 명목형 분류 라벨을 정수형으로 변환
피처 선택 /추출	- 학습에 필요한 특성만 선택하여 모델 복잡성 감소 - 오버피팅 감소	
특징	- 특징(Feature) 추출	- PCA(주성분 분석) 등으로 새로운 변수 생성

(Feature) 선택	- 그리드 서치 알고리즘	- 단계별 지역 최적해 도출 후, 문제에 대한 최적해 도출 기법 - 연속형 피처 선택 알고리즘으로 사용
	- 랜덤 포레스트	- 특성의 상대적 중요도를 의사결정 트리로 구성하여 평가
피처 스케일링	- 머신러닝 알고리즘이 최적의 성능을 낼 수 있도록 특징을 동일한 스케일로 변환	
	- 정규화 (Normalization)	- 데이터를 0과 1 범위로 스케일링
	- 표준화 (Standardization)	- 평균 0, 분산 1이 되도록 변환하는 모든 방법 - 표준화 후 특징 열은 정규분표 형태를 가짐

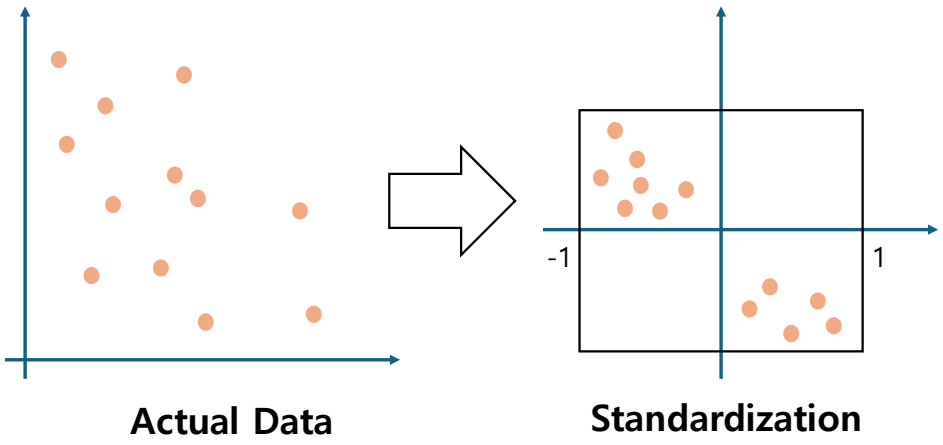
- 피처 스케일링 기법인 정규화와 표준화를 통해 데이터들을 공통된 기준으로 변환 하여 활용 가능

III. 정규화(Normalization)과 표준화(Standardization) 설명

가. 정규화(Normalization) 설명

구분	설명	
개념	- 데이터를 0과 1의 구간 사이의 값으로 변환하는 스케일링 기법	
개념도		
주요 방법	- Min-Max 정규화	- 데이터를 지정된 범위로(주로 0과 1사이) 스케일링 - 이상치에 민감하며 데이터 원본의 분포를 보존하지 않음
	- 소수 스케일링 (Decimal Scaling)	- 데이터를 일정한 자릿수로 나누어 스케일링 - -1~1로 범위를 조정하지만 분포는 보존
	- 로그 변환(Log Transformantion)	- 데이터에 로그를 취하여 분포를 대칭적으로 만드는 방법 - 양의 왜도를 가진 데이터나 지수적으로 증가하는 데이터에 적합

나. 표준화(Standardization) 설명

구분	설명	
개념	- 데이터를 변환하여 평균이 0, 분산이 1인 표준 정규 분포 형태로 변환하여 범위를 조정하는 스케일링 기법	
개념도		
주요 방법	- Z-Score 표준화	- 데이터를 평균 0, 표준편차 1의 분포로 변환 - 가장 널리 쓰이는 전통적인 표준화 방식 - 이상치(Outlier)에 민감
	- Robust 표준화	- 평균 대신 중위수, 표준편차 대신 IQR(Interquartile Range) 사용 - 이상치가 많은 데이터에서 효과적인 방법

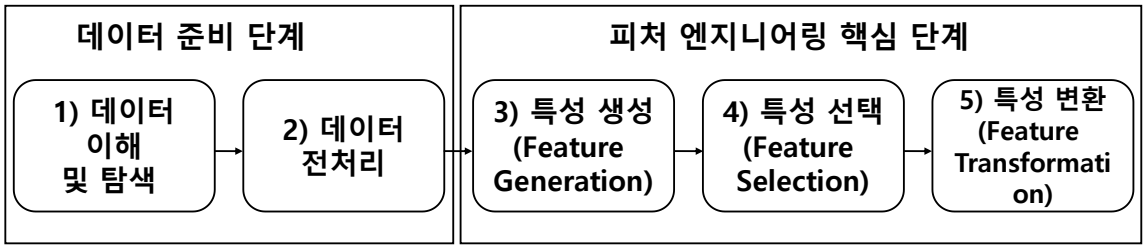
- 표준화와 정규화를 포함한 데이터 전처리 기법을 통해 데이터의 스케일과 분포를 균일하게 조정하여 분석 효율성을 높여 피처 엔지니어링의 후속 과정 수행 가능

IV. 피처 엔지니어링(Feature Engineering) 설명

가. 피처 엔지니어링 (Feature Engineering) 의 개념 및 중요성

개념	- 머신러닝 모델의 성능을 향상시키기 위해 데이터의 특성(Feature)를 변형하거나 선택하는 과정	
중요성	- 모델 성능 향상	- 고품질의 데이터로 학습하여 모델의 결과 정확도 향상
	- 학습 효율 강화	- 변수 간 스케일링 차이를 최소화하여 학습 속도 및 안정성 향상
	- 과적합(Overfitting) 방지	- 불필요 변수, 노이즈를 제거하여 학습 데이터 단순화 - 일반화 성능 증가
	- 다양한 데이터 활용 지원	- 수집한 데이터를 여러가지 형태로의 데이터를 변환하여 의미 있는 정보로 활용 가능

나. 피처 엔지니어링(Feature Engineering)의 프로세스 및 세부 절차 설명

<table>
<tr><td>프로세스</td><td colspan="2"> 
</td></tr>
<tr><td rowspan="5">세부 절차</td><td>1) 데이터 이해 및 탐색</td><td>- 데이터 구조, 변수 유형, 누락값, 이상치 등 파악
- EDA 등을 이용하여 데이터 패턴 및 상관관계 분석</td></tr>
<tr><td>2) 데이터 전처리</td><td>- 누락값 처리, 이상치 제거, 데이터 형식 변환
- 머신러닝 모델이 학습하기 적합한 형태로 변환</td></tr>
<tr><td>3) 특성 생성(Feature Generation)</td><td>- 도메인 지식, 데이터 탐색 결과 기반 특성 설계
- 예) 날짜 정보 -> 요일/계절정보 특성 생성</td></tr>
<tr><td>4) 특성 선택(Feature Selection)</td><td>- 불필요 특성 제거, 중요도 높은 특성만 선택
- 모델 복잡도 감소, 학습시간 단축
- 상관 분석, 모델 기반 특성 선택 등 사용</td></tr>
<tr><td>5) 특성 변환(Feature Transformation)</td><td>- 기존 특성을 변환하여 머신러닝 알고리즘에 적합한 형태로 만드는 과정
- 로그 변환, 스케일링, 원-핫 인코딩 등 사용</td></tr>
</table>

- 피처 엔지니어링을 통해 AI의 학습 데이터를 정제하는 과정을 수행하여 궁극적으로 AI 모델의 성능 및 정확도 향상 달성 가능

"끝"

03	취약점 진단		
문제	최근 기업의 보안사고 증가에 따라 정부에서는 CISO(Chief Information Security Officer)기업 대상으로 자체 취약점 진단을 시행하여 결과를 보고하도록 하였다. 다음을 설명하시오. 가. 취약점 진단 절차 나. 애플리케이션 취약점 진단 방법 다. 인프라 취약점 진단 방법		
도메인	보안	난이도	중 (상/중/하)
키워드	자산식별, 위험도 평가, 사전 예방, SAST, DAST, IAST, 모의해킹(블랙박스, 화이트박스, 그레이박스) OWASP , 인프라 보안점검 자동화 도구 사용		
출제배경	증가하는 보안 사고에 대비하여 IT 자산에 대한 보안 리스크를 사전에 발견, 개선하여 침해사고를 예방하기 위한 절차 확인		
참고문헌	KISA 보안 취약점 가이드 https://cloudimg.ccs.ahnlab.com/img_upload/product/2312222132525346.pdf		
출제자	배미경 기술사(제 135회 정보관리기술사 / hjmom0727@daum.net)		

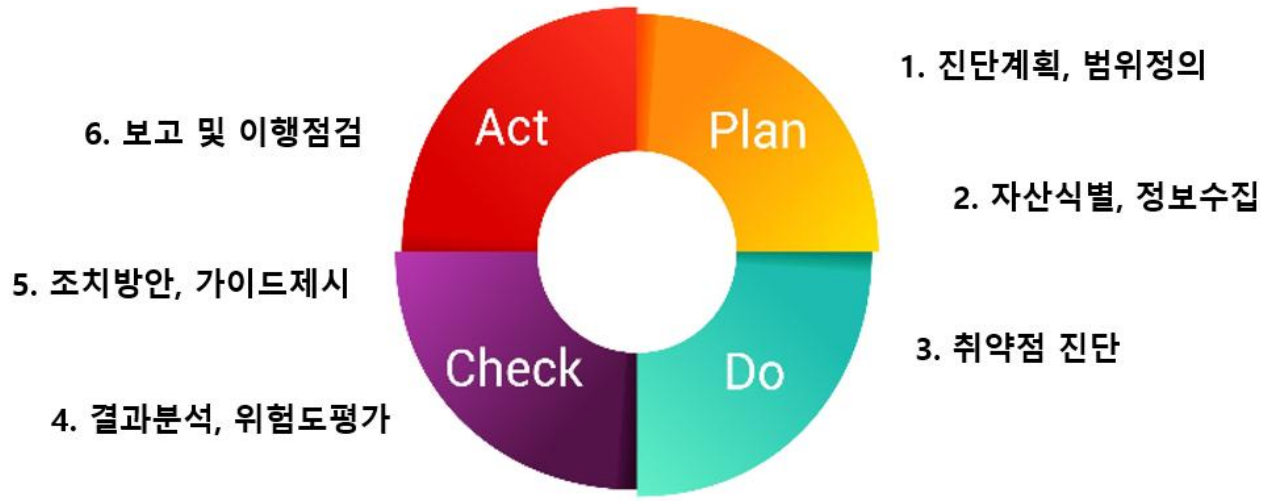
I. 침해사고 예방을 위한 취약점 진단의 개요

개념	- 시스템, 네트워크, 애플리케이션 등 **IT 자산에 존재하는 보안 약점을 식별**하고, 해킹 등 잠재적인 **위협 요소를 분석, 평가**하여 보안 사고를 **사전에 예방**하기 위한 활동

- 날로 진화하는 사이버 위험에 대응하기 위하여, 사전에 잠재적 보안 위험을 발견하고 개선하기 위한 체계적 활동은 기업 생존 전략

II. 취약점 진단의 절차

가. 취약점 진단 절차의 개념도



- 취약점 점검은 PDCA 사이클에 따라 6단계로 진행되며, 정기적으로 수행하여 지속적인 개선이 필요함

나. 취약점 진단의 절차 상세

절차	주요 활동	설명
1. 진단계획 및 범위정의	- 목표 및 범위 설정	- 진단의 목적을 명확히 함 - 진단 **대상** 시스템 및 진단 **방법**을 확정
	- 자원 확보 및 일정 수립	- 진단팀 구성, 필요한 도구 및 계정 정보 확보 - 진단 일정, 소요시간 계획
2. **자산식별** 및 정보수집	- **자산정보**수집	- 시스템 구성도, 아키텍처, 네트워크 구성, 운영체제(OS), 데이터베이스(DB), 웹 서버 종류 등 IT자산에 대한 기술적인 환경 정보를 수집
	- 보안 정책 검토	- 보안 정책 및 내부 통제 절차를 검토, 진단에 반영
3. 취약점진단 수행	- **자동 진단**	- 상용 또는 오픈소스 취약점 스캐닝 도구를 활용, 시스템설정 오류 및 알려진 취약점(CVE) 등을 대량으로 빠르게 스캔
	- **수동 진단** 및 모의 해킹	- 진단 체크리스트 기반으로 설정의 적절성을 수동으로 점검 - 웹/앱의 경우 모의 해킹 기법을 적용, 논리적 취약점을 심층적으로 확인
4. 결과분석 및 **위험도평가**	- 오탐 확인 및 분류	- 자동 진단 결과 중 오탐(False Positive)을 제거 - 발견된 취약점에 대해 정확한 위험도를 평가

	- **위험도 산정**	- 취약점의 심각도(Severity, High/Medium/Low), 악용 가능성(Exploitability), 비즈니스 영향도를 종합적으로 고려, 조치 우선순위를 결정
5. 조치방안 및 가이드라인 제시	- 대응 전략 수립	- 위험도 분류에 따라 즉시 조치, 단기 조치, 중장기 조치 등 단계별 대응 전략을 수립
	- 구체적 **조치 가이드** 제공	- 발견된 취약점을 해결하기 위한 패치, 설정 변경, 코드 수정 등의 구체적이고 실현 가능한 기술적 가이드라인을 수립
6. 보고 및 이행점검	- 보고서 작성 및 결과공유	- 진단 개요, 발견된 취약점 목록, 위험도 평가 결과, 조치 가이드라인 및 전반적인 보안 수준 평가를 포함한 최종 보고서를 작성 - 조치일정 및 책임 범위 등 최종적으로 협의
	- **이행확인** 및 재점검	- 가이드에 따라 취약점 조치를 완료했는지 확인, 재진단을 수행 - 보안 위험의 최종 제거를 검증, 프로세스 완료

- 취약점 진단은 IT 자산 식별이 중요하며, 특히 인터넷 접점의 자산에 대한 취약점 점검을 우선적으로 시행
- 취약점 점검 대상인 애플리케이션, 인프라에 대하여 적합한 점검 기법을 확정하고 진단을 실시함

III. 애플리케이션 취약점 진단 방법

가. 자동분석 방법

방법(기법)	접근방식	장. 단점
SAST (정적분석)	- 실행 없이 소스코드를 분석하여, 코딩 표준 위반, 입력값 검증 누락 등 잠재적 보안 약점을 식별 - OWASP Top 10, 행안부 SW 개발보안가이드 등 적용	[장점] 개발 초기에 적용 가능 모든 코드 경로를 검토
		[단점] 오탐(False Positive)이 많고, 실행환경에서 취약점 찾기 어려움
DAST (동적분석)	- 애플리케이션을 실행상태에서 외부에서 공격을 모의 - HTTP요청/응답 과정에서 발생하는 취약점(XSS, SQL Injection 등)을 탐지	[장점] 실제 공격 환경과 유사, 오탐 적음.
		[단점] 모든 코드 경로를 커버하기 어렵고, 복잡한 로직은 테스트가 어려움
IAST (상호작용분석)	- 애플리케이션 실행 환경 내부에 센서를 설치 - 테스트 시 실시간으로 코드 실행 경로와 취약점을 연동하여 분석	[장점] SAST와 DAST의 장점을 결합하여 높은 정확도로 취약점 발생 지점을 파악
		[단점] 테스트환경에 전용 센서 설치필요

- 애플리케이션 취약점 진단은 SonarQube, Fortify 등 자동화 도구를 이용하여 효율성을 높일 수 있음

나. 수동분석 방법

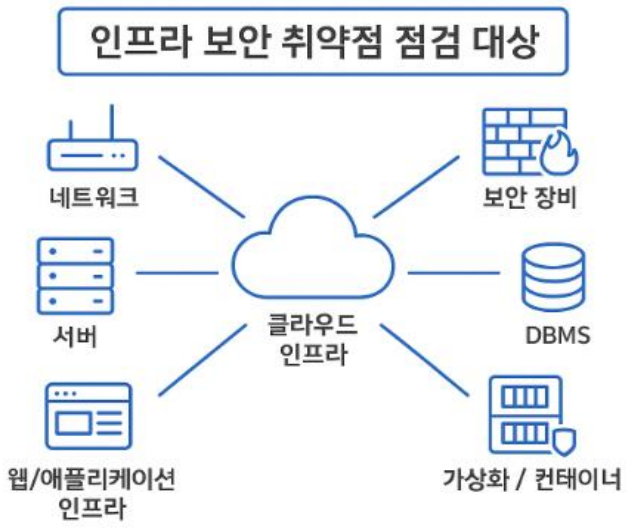
- 수동분석 기법인 모의해킹은 테스트 대상 시스템에 대한 사전정보 수준에 따라 블랙박스, 화이트박스, 그레이박스 세 가지로 분류

방법(기법)	접근방식	장. 단점
블랙박스	- **외부공격자 시각** - 시스템 내부정보(소스코드,아키텍처,계정) 없이 외부에 공개된 정보만으로 공격을 시도	[장점] 가장 현실적인 외부해킹 경로 모의하여 외부위협 대응능력을 점검
		[단점] 테스트 커버리지가 낮고, 심층적인 취약점, 코드결함을 찾기 어려움
화이트박스	- 내부 전문가 시각 - 소스코드, 시스템구조, 관리자 계정 등 모든 **정보를 제공**받아 시스템 내부 깊은 곳까지 분석	[장점] 코드레벨의 근본적 결함, 설계오류 등 모든 영역의 취약점을 심층적으로 분석
		[단점] 실제 해커의 공격 방식과는 거리 많은 시간과 비용이 소요
그레이박스	- **제한적 정보** 보유자 시각 - 일반 사용자계정, 제한적인 정보를 제공받아, 내부 사용자나 파트너의 관점에서 권한 상승 등을 시도	[장점] 효율성과 현실성의 균형이 좋으며, 권한 오용이나 내부 유출 시나리오 점검에 효과적
		[단점] 블랙박스만큼 포괄적인 외부 공격 모의나 화이트박스만큼 심층적인 분석은 어려움

- 모의해킹은 전문가에 의한 수동기법으로 자동기법, 도구가 찾기 어려운 논리적 결함을 발견

IV. 인프라 취약점 진단 방법

가. 인프라 취약점 진단 개요

진단 대상	
개념	- 조직의 IT 환경을 구성하는 핵심 요소들을 체계적으로 분류하여 인프라 전체에 대한 보안 설정 오류, 패치 누락, 접근 통제 문제 등을 포괄적으로 점검하는 활동

- 인프라 취약점 진단은 OS, DB, 네트워크 장비 등의 설정이 보안 표준을 준수하고 있는지 확인, 패치 누락 등을 Qualys, OpenVAS 등 **자동 스캐너**를 사용하여 점검

나. 인프라 취약점 진단 상세

진단범위	진단 대상	점검 항목
시스템/서버	- 운영체제(OS)	- 패스워드 정책, 불필요 서비스 제거, 로그관리 설정, 파일 시스템 접근 통제 점검
	- 데이터베이스(DB)	- 접근권한 관리, 기본계정 사용여부, 민감정보 암호화 적용, 감사로그 설정 점검
	- 웹/미들웨어(WAS)	- 기본 페이지 삭제, 버전정보 노출제한, 접근제어 설정, 관리자 인터페이스 보안 점검
네트워크	- 네트워크 장비	- 접근 통제 목록(ACL) 분석 - 방화벽(Firewall)정책 적절성, 불필요한 포트개방 여부, 라우터/스위치 보안 설정 점검
	- 무선 네트워크	- 포트 스캐닝(Port Scanning) 기법 이용 - 무선 보안 설정 점검 : WPA3/WPA2 암호화 적용 여부, 인증 방식의 안전성, 기본 설정 변경 여부
보안시스템, 장비	- 보안 장비, 보안 솔루션	- 관리 설정 점검 및 로그 분석 - IDS/IPS, VPN 등 보안장비의 최신패치 적용, 관리자 접근통제, 정책 적절성 점검
클라우드	- IAM (접근/계정 관리)	- CSPM이용 클라우드 보안설정표준 준수여부 자동점검 - 최소권한(Least Privilege) 원칙준수, MFA(다단계 인증) 적용, API 키 관리의 안전성 점검
	- 클라우드 인프라	- IAM 권한 분석: 최소 권한(Least Privilege) 원칙에 따른 과도한 권한 할당 여부 확인. - VPC/네트워크 설정, 스토리지(S3 등) 접근 제어 및 공개 설정 여부, 보안 그룹 설정 점검

- 제조 공장의 보안사고 증가 등으로 인하여 IT보안 취약점 점검 뿐 아니라, OT 영역의 취약점 점검도 중요해지고 있음

"끝"

04	시계열 이상탐지		
문제	데이터 마이닝의 이상탐지 기법 중 시계열 데이터 이상탐지는 시스템의 안정성과 신뢰성을 위한 필수 기술이다. 다음을 설명하시오. 가. 시계열 데이터 이상탐지의 개념 및 목적 나. 시계열 데이터 이상탐지의 알고리즘 다. 시계열 데이터 이상탐지의 적용사례		
도메인	알고리즘	난이도	중 (상/중/하)
키워드	점이상치, 문맥 이상치, ARIMA, SVM, Autoencoder, LSTM, 예지보전, 이상거래탐지, 공정 품질관리		
출제배경	AI 환경에서 급증하는 대용량 시계열 데이터의 이상 탐지 기술이 필수적으로 활용되고 있어 이에 대한 기술 및 적용사례 등의 이해 필요		
참고문헌	https://meetup.nhncloud.com/posts https://saige.ai/blog/time-series-anomaly-detection/		
출제자	배미경 기술사(제 135회 정보관리기술사 / hjmom0727@daum.net)		

I. 위기예측 과 미래 준비도구, 시계열 데이터 이상탐지의 개념과 목적

가. 시계열 데이터 이상탐지의 개념

구분	설명	
정의	- 시간 흐름에 따라 수집되는 연속적 데이터(시계열 데이터)에서 정상성을 벗어난 비정상적 행동이나 값(Anomaly)을 자동으로 탐지하는 기법	
유형	- **점 이상치** (Point Anomaly)	- 시계열 데이터의 특정시점의 단일데이터 포인트가 나머지 데이터 분포와 현저히 다를 때 발생
	- **문맥적 이상치** (Contextual Anomaly)	- 데이터점 자체의 값은 정상이나, 해당 값 시점 문맥 주변데이터가 이상으로 판단되는 경우 발생
	- **집단 이상치** (Collective Anomaly)	- 데이터 포인트들의 연속적인 부분시퀀스가 전체 시계열의 나머지 부분과 현저하게 다를 때 발생
특징	- **시간 의존성**	- 과거의 정상 패턴과 현재의 데이터 포인트를 비교하여 이상치를 판단, 이상치가 시간흐름 따라 달라짐
	- **순서의 중요성**	- 같은 값이라도 나타난 시점의 전후 맥락에 따라 정상 또는 이상으로 판단될 수 있음
	- **동적(Dynamic)** 특성	- 시계열 데이터의 정상패턴은 지속적으로 변화하므로 이상탐지 모델은 이러한 변화에 적응 필요
	- **희소성**	- 데이터의 희소성으로 불균형한 데이터 문제를 가지며, 이상치 탐지 모델학습 어려움 발생가능

- 시계열 데이터 내에서 비정상적이거나 일반적인 패턴에서 벗어나는 데이터를 식별하여 다양한 산업의 비즈니스에 활용

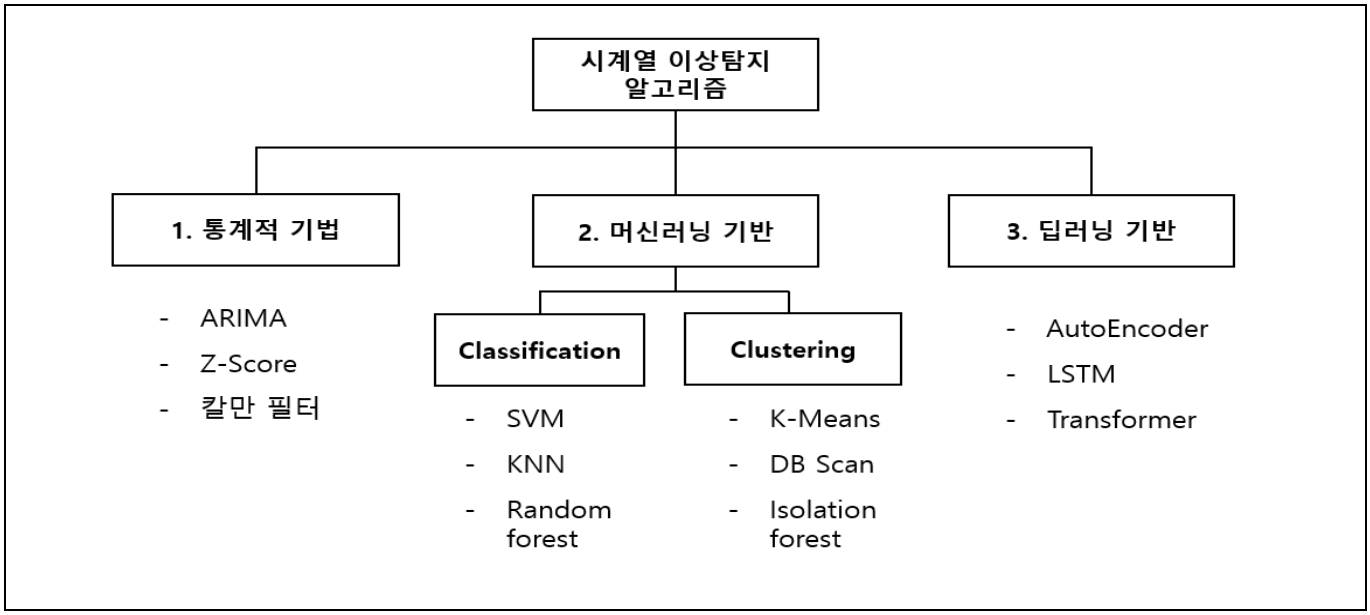
나. 시계열 데이터 이상탐지의 목적

구분	목적	설명
비즈니스 관점	- 사기 및 오용 방지	- 비정상적이거나 악의적인 패턴을 실시간으로 감지, 대규모 손실이 발생 전 차단
	- 수익 손실 최소화 및 효율성 증대	- 제품 불량을 조기에 예측, 예상치 못한 다운타임을 방지하여 생산성을 유지
	- 고객 경험 및 서비스 품질 유지	- 서비스 지연이나 장애를 사전에 파악하여 선제적으로 대응, 서비스품질(QoS) 유지
시스템, 보안관점	- 시스템 장애 및 고장 예측	- 고장으로 이어질 수 있는 미묘한 변화나 이상 징후를 조기에 감지
	- 보안 위협 탐지 및 대응	- 비정상적인 접근, 내부자 위협 등 보안 이상치 식별, 시스템을 보호하고 신속하게 대응
	- 성능 저하의 근본 원인 분석	- 시스템 성능지표에서 이상치 발생시, 연관된 다른 시계열이상치와 연결,성능저하 원인파악
데이터 분석관점	- 데이터 품질 개선 및 전처리	- 분석사용 시계열 데이터에서 오류, 센서고장 등의 잡음(Noise), 잘못된값을 이상치로 식별
	- 새로운 현상 또는 패턴 발견	- 기존 예상패턴과 일치하지 않는 의미있는 이상치 발견 등 미처 인지못한 중요한 정보취득
	- 모델 개발 및 개선을 위한 피드백	- 탐지된 이상치를 분석해 운영중 모델을 재학습, 개선을 위한 중요한 학습 데이터로 활용

- 단순한 수치 변화 뒤에 숨은 위험 요소나 기회 요인을 자동으로 포착해 비즈니스 인사이트를 극대화
- 시계열 이상 탐지 시스템은 통계적 기법, 머신러닝 또는 패턴 인식 알고리즘에 기반하여 운영

II. 시계열 데이터 이상탐지의 알고리즘

가. 시계열 데이터 이상탐지 알고리즘의 개요



- ML기반의 알고리즘이 대중적으로 사용되고 있으나, 데이터양의 증가, 복잡성으로 딥러닝 기반으로 변화

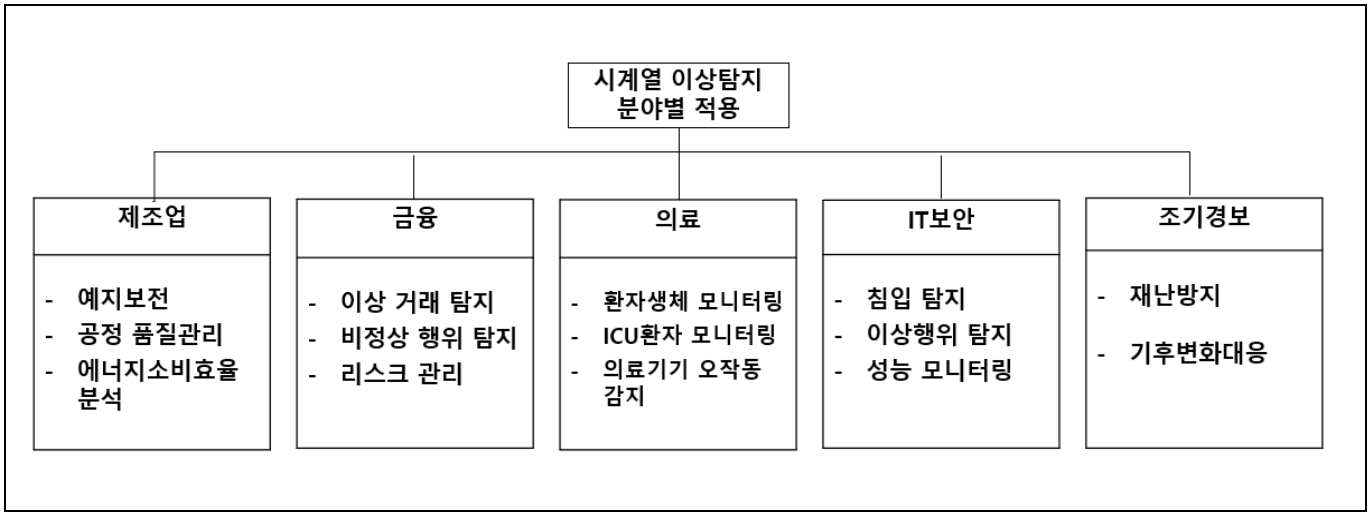
나. 시계열 데이터 이상탐지 알고리즘의 상세설명

구분	알고리즘	특징
통계적 기법	- ARIMA	- 과거 값(AR)과 오차(MA)기반으로 미래 값을 예측, 예측오차를 이용해 이상을 탐지하는 모델 - 예측 기반 이상 탐지 강하나 비선형 패턴에 약함
	- Z-Score	- 데이터가 평균에서 몇 표준편차만큼 떨어져 있는지 기반으로 극단 값을 이상으로 탐지하는 방법 - 가장 단순·빠르나 분포 가정(정규성) 필요
	- 칼만 필터	- 관측 값과 예측 값을 결합해 상태를 추정, 추정오차가 커질 때 이상을 판단하는 상태공간 모델 - 노이즈 강인, 실시간성이나 모델·노이즈 정의 난해
머신러닝 기법	- SVM	- 정상 데이터만 학습, 고차원 공간에서 정상영역을 둘러싸는 경계를 설정하고 경계 밖을 이상치로 분류 - 비선형경계 설정가능하나 대규모 데이터 학습시간 오래걸림
	- KNN	- 데이터포인트와 가장 가까운 k 개의 이웃사이의 거리 측정, 거리가 멀거나 밀도가 낮은 포인트를 이상치로 판단 - 구현간단, 분포가정 불필요, 계산복잡도 높고 k 값 설정 민감
	- Isolation forest	- 데이터를 무작위로 분할해 트리구조를 만들고, 이상치가 정상 데이터보다 더 쉽게 고립된다는 성질을 이용해 탐지 - 계산속도가 빠르고 대규모 데이터에 효율적
딥러닝 기법	- Autoencoder	- 정상데이터를 학습해 잠재공간으로 압축 후 복원, 재구성 오차가 큰 데이터를 이상치로 탐지 - 비지도 학습방식으로 복잡한 패턴 학습
	- LSTM	- 게이트 메커니즘을 통해 장기 의존성을 학습하여 다음 시점 값을 예측, 예측 오차를 기반으로 이상치를 식별 - 시간적 순서와 문맥적 이상치 탐지에 강력하나 학습시간 김
	- Transformer	- 어텐션 메커니즘을 사용하여 시계열의 전역적인 문맥을 병렬적으로 포착하고 예측 오차로 이상치를 탐지 - 긴 시퀀스의 장기 의존성 학습 및 병렬 처리에 유리하나 계산 자원 요구량이 높음

- 시계열 이상탐지를 위한 기법, 알고리즘은 단순한 통계기반 기법부터 복잡한 딥러닝 모델까지 다양하나, 어떤 알고리즘을 사용할지는 데이터 패턴이나 유형, 실시간 탐지여부, 이상치 형태 등에 따라 결정

III. 시계열 데이터 이상탐지의 적용사례

가. 시계열 데이터 이상탐지의 적용분야



- 시계열 이상탐지는 다양한 산업에서 조기대응과 효율개선을 위해 적용되어 비즈니스 인사이트를 극대화 할 수 있도록 지원

나. 시계열 데이터 이상탐지의 적용 사례

구분	적용 사례	설명
제조업	- 예지 보전	- 이상치 예 : 모터진동, 온도센서 값 등이 정상범위를 벗어나거나, 패턴이 급변하는 징후 - 효과 : 고장사전예측, 생산중단 최소화, 유지보수 비용 절감
	- 공정 품질 관리	- 이상치 예 : 공정온도, 압력값이 정상이나, 해당값이 발생한 순서, 지속시간이 비정상적인 경우 - 효과 : 불량률 감소, 공정 안정성 향상
	- 에너지 소비 효율 분석	- 이상치 예 : 시간대 패턴 위반 - 효과 : 에너지 비용 절감, 누수/오작동 조기 발견
금융업	- 이상거래 탐지	- 이상치 예 : 반복결제, 고객 평소패턴 대비 특이 - 효과 : 금융사기 방지, 손실 최소화
	- 알고리즘 거래 오류 탐지	- 이상치 예 : 비정상적인 대량주문, 주문취소율의 급격한 증가 - 효과 : 예기치 않은 금융 손실 위험을 즉시 관리
	- 사용자 이상 행위 탐지	- 이상치 예 : 로그인 급증, 연속 실패 - 효과 : 계좌 탈취 예방, 보안 강화
IT,보안	- 침입 탐지	- 이상치 예 : 비정상적 네트워크 트래픽증가, 특정 포트의 접속시도 빈도 등 공격패턴이 감지 - 효과 : 공격 조기 탐지, 서비스 보호
	- 내부자 이상 행위 탐지	- 이상치 예 : 개인행동 패턴 대비 반복적 의심행위 - 효과 : 내부자 위협 탐지, 계정 남용 방지

	- 성능 모니터링	- 이상치 예 : 지연 급증, 지속적 고부하 - 효과 : 장애 예방, 다운타임 감소

- 다양한 산업 분야에 시계열 이상탐지 기법, 알고리즘 적용하여 비즈니스 손실 최소화, 효율 극대화 기대

IV. 시계열 데이터 이상탐지 도전과제 및 해결방안

문제	도전 과제	해결 방안
데이터 노이즈	- 데이터 품질 개선	- **전처리** : 데이터 평활화, 정규화 - **필터링** : 저역 통과 필터링 - **이동평균** 적용 : 변칙성 완화
느린 연산속도	- 실시간 분석을 위한 연산시간 최적화	- **GPU** 사용 병렬 연산 - **경량화 모델** 설계 : 푸루닝, 지식증류 - **병렬 처리 구조** 도입 (Kafka+Spark구조)
데이터 양의 증가	- 데이터 다양성의 증가	- **Synthetic 증강** : 가상이상데이터로 훈련상황 다양화 - **AutoML** 통한 동적 모델 업데이트 - **가변 임계 값** 설정

- 시계열 이상 탐지는 변화를 감지하는 강력한 도구로, 실제 작업시에 발생하는 문제에 대한 적절한 전처리와 인프라로 극복 가능

"끝"

05	피지컬 AI(Physical AI)		
문제	디지털 전환이 가속화되고 제조·물류·의료 등 주요 산업에서 자동화와 지능화가 빠르게 확산되면서, AI가 소프트웨어 영역을 넘어 물리적 공간에서 자율적으로 판단·행동하는 '피지컬 AI(Physical AI)'의 중요성이 증가하고 있다. 다음에 대해 설명하시오. 가. 피지컬 AI의 개념과 유형 나. 피지컬 AI의 핵심 기술 다. 피지컬 AI의 도입 시 고려사항		
도메인	인공지능	난이도	중 (상/중/하)
키워드	컴퓨터 비전, 센서 퓨전, 강화학습, LAM, 온디바이스 AI, sLLM, LWM, Multi-modality, Synthetic Data , 모델 예측 제어(MPC), SLAM, 에너지 하베스팅, 엣지 컴퓨팅		
출제배경	가트너 2026 10대 전략 기술 '피지컬 AI' 발표에 따른 출제 예상		
참고문헌	피지컬 AI의 기술발전 및 정책적 시사점(2025.09) 피지컬 AI의 현황과 시사점(SPRi, 2025.09) ITPE 기술사회 자료		
출제자	소민호 기술사(제 119회 정보관리기술사 / mhsope@naver.com)		

I. AI의 물리세계로 확장, 피지컬AI(Physical AI)의 개념 및 유형

가. 피지컬AI(Physical AI)의 개념

구분	설명	
개념	- AI가 물리적 실체 안에 구현되어 센서와 액추에이터 등을 통해 **현실 세계를 인식하고, 자율적으로 판단·행동함으로써 환경과 유기적으로 상호작용할 수 있는 시스템**	
특징	대형언어모델 적용	- 디바이스에 대형 언어 모델 적용으로 자연어 기반 의사소통 가능
	물리세계인식	- 실제 현실세계 환경을 인식하고 이해하는 능력 보유
	산업 현장 활용	- 자율주행, 로봇, 병원, 공장 등에서 AI 기반 시스템 운영 지원

- 피지컬 AI는 AI가 센서·액추에이터 기반 물리 환경에서 스스로 인식·판단·행동하며 인간과 자연스럽게 상호작용하는 지능형 시스템

나. 피지컬AI(Physical AI)의 유형

유형	설명
휴머노이드형	- 인간과 유사한 외형과 동작을 수행하며, 고도 통합 AI로 자율 판단·행동이 가능한 지능형 로봇
자율주행차형	- 도로 환경 인식·판단과 경로 해석을 통해 복잡한 주행을 스스로 수행하는 차량 기반 시스템
드론형	- 공중 이동에 특화되어 실시간 공간 인식, 장애물 회피, 자율 비행이 가능한 비행형 AI
AGV	- 사전 정의된 경로를 따라 이동하며 자재를 운반하는 정형 환경 자동화 차량
AMR	- SLAM·비전·LiDAR로 자율 경로 생성·장애물 회피가 가능한 고도 자율 이동 로봇

- 피지컬 AI는 휴머노이드·자율주행차·드론·AGV·AMR 등 다양한 형태로 구현

II. 피지컬 AI의 핵심 기술 설명

가. 피지컬 AI의 인식·추론 기술

구분	기술요소	설명
센서 및 인식	컴퓨터 비전	- 카메라, LiDAR 로 환경 분석(객체 인식, 깊이 추정)
	센서 퓨전	- 다중 센서 데이터 결합하여 측정 정확도 향상
	시공간적 추론	- 물체의 움직임과 시간적 변화 예측
인공지능 및 머신러닝	강화학습	- 보상, 벌점 기반 시행착오를 통한 최적 행동 학습
	진화 연산	- 환경 변화에 따라 지속적으로 최적의 동작을 학습
	LAM	- 행동 계획 및 실행을 최적화하는 모델
	온디바이스 AI	- 디바이스에서 사용 가능한 AI 모델 및 H/W 기술
	모델 경량화 기술	- 양자화, 파라미터 가지치기, 증류학습
	sLLM	- 파라미터 압축을 통한 경량화 대형언어모델
	LWM(Large World Model)	- 가상 세계 생성을 위한 수천조 파라미터 크기의 모델 - 합성데이터 활용한 Physical AI 학습 데이터 생성
	Multi-modality (멀티모달 학습)	- 텍스트, 이미지, 오디오, 센서 데이터를 통합 학습하는 기술. - GPT-4, Gemini와 같은 모델이 다양한 입력 데이터를 처리.
	Synthetic Data (합성 데이터)	- 실제 데이터 부족 문제 해결을 위해 시뮬레이션 데이터를 활용. - 생성형 AI 기반 디지털 트윈의 로봇 훈련을 가속화.

- 피지컬 AI가 환경을 인식하고 학습하며 판단하는 능력을 구현하기 위한 핵심 기술들로 구성

나. 피지컬 AI의 제어·운영 기술

구분	기술요소	설명
로보틱스	모델 예측 제어(MPC)	- 동적환경 최적 제어 신호 생성
	Whole Body Control	- AI, 액추에이터 및 감속기를 통한 정밀 제어 수행
	SLAM	- AI 기반 센서 융합을 통해 로봇이 주변 환경을 실시간으로 인식하고 이동
	Dexterity (정밀 조작)	- 로봇이 인간과 유사한 수준의 손재주와 정밀한 조작을 수행. - MIT의 고정밀 로봇 손, DaVinci 수술 로봇 등의 사례.
에너지 자율성	에너지 하베스팅	- 주변 환경에서 에너지를 수집하여 전력으로 변환
	저전력 AI 칩	- AI 연산을 수행하면서도 소비 전력을 최소화하는 반도체 칩
	지능적 전원관리	- AI 기반 에너지 예측, 배터리 수명 연장 및 전력 소비 절감
분산처리	클라우드 컴퓨팅	- 대규모 데이터 처리 및 AI 모델 훈련
	엣지 컴퓨팅	- 데이터 로컬 처리를 통한 실시간 반응성 향상
운영 & 유지	RaaS(Robots as a Service)	- 구독형 로봇 서비스 모델. - 필요할 때 로봇을 대여하여 운영비 절감.
	자가유지보수 (Upgrade-ability & Self-Maintenance)	- OTA(Over-The-Air) 업데이트를 통해 로봇의 지속적 성능 개선. - 자가 진단 및 자율 유지보수 시스템 도입 증가.

- 피지컬 AI 는 다양한 기술을 결합해 실제 환경에서 자율적으로 인식·판단·동작하는 것을 가능하게 함

III. 피지컬 AI 의 도입 시 고려사항

가. 피지컬 AI 의 기술·운영 측면 고려사항

구분	고려사항	설명
기술적 한계 대응	모델 실시간성·범용성 검증	- 다양한 환경에서 인지·제어 모델이 안정적으로 작동하는지, 실시간 처리 가능성을 사전 검증해야 함
	Sim-to-Real 편차 최소화	- 시뮬레이션만 의존하지 않고 실제 데이터 수집·교차 검증을 통해 현실 적응도를 높여야 함
	에너지 효율 구조 설계	- 배터리 용량, 연산 자원, 경량화 모델 등을 고려해 장시간 운용 가능한 설계를 구축해야 함
비용·통합	도입·운영 비용 산정 및 ROI 분석	- GPU·센서·액추에이터 등 고비용 요소를 고려해 지속가능한 비용 구조와 ROI를 검토해야 함
	모듈형·표준화된 설계	- HW/SW/반도체가 서로 다른 생태계를 갖기 때문에 상호 호환성과 모듈형 플랫폼 구성이 중요
	유지보수·업그레이드 용이성	- 부품 교체, 모델 업그레이드, 연산 자원 확장을 쉽게 할 수 있는 구조를 마련해야 함

- 모델 성능, 에너지 효율, 비용·통합 구조 등 피지컬 AI 도입의 실현 가능성과 안정적 운영을 위한 기술적 기반을 점검해야 함

나. 피지컬 AI 의 사회·제도적 측면 고려사항

구분	고려사항	설명
경제·노동시장	재교육·전환 지원 체계	- 자동화로 인한 일자리 변화에 대비해 재교육과 직무 전환 체계를 마련해야 함
	사회적 수용성 확보	- 서비스 도입 시 근로자·이용자에 대한 영향과 불안 요소를 최소화하는 커뮤니케이션 필요
	일자리 영향 분석	- 특정 산업에서 대체·보조 역할을 구분해 경제적 충격을 완화할 정책적 판단이 필요
윤리·법·규제	책임 소재 명확화 기준 마련	- 사고 발생 시 개발자·운영자·제조사 간 책임 분담을 명확히 정의하는 제도적 기준 필요
	개인정보·감시 데이터 보호	- 영상·음성·위치 등 민감정보 처리에 대한 보안 규정 강화 및 최소 수집 원칙 준수 필요
	인간 존엄성·감정 영향 관리	- 인간형 로봇과의 정서적 관계 형성, 감정 조작 등의 윤리 문제를 예방할 가이드라인 마련
지정학·기술 경쟁	기술 자립성·공급망 확보	- 고성능 반도체·센서·로봇 부품의 해외 의존도를 줄이고 안정적 공급망을 확보해야 함
	국가별 규제·표준 분석	- 미국·EU·중국 등 주요국의 AI·로봇 규제를 분석해 글로벌 시장 진출 전략을 세워야 함

	기술 격차 해소 투자	- 연구개발 투자 확대, 산학연 협력 강화로 장기 경쟁력을 확보해야 함

- 피지컬 AI 도입은 기술적 실시간성·비용·윤리·규제·공급망 등 전반을 종합적으로 검토해 안정적·지속가능한 운영 체계를 마련 필요

IV. 피지컬 AI의 시사점

구분	시사점
국가 전략	- AI·로봇 융합 시대에 대응하여 **산업별 실증·상용화 중심의 국가 전략** 필요. - 한국의 ICT 강점과 제조 기반을 반영한 맞춤형 전략 수립. - **피지컬 AI 전략위원회** 신설을 통해 R&D·규제·국제협력 총괄 거버넌스 구축. - 대규모 투자로 핵심 기술 자립 및 글로벌 경쟁력 확보 필요.
연구개발 강화	- 기반모델·강화학습·액추에이터 등 **핵심 요소기술의 해외 의존도** 탈피 시급. - **온디바이스 AI 반도체**, **월드 모델** 등 실시간 물리 환경 대응 기술 개발 필요. - 휴머노이드·자율주행·드론·AGV 등 다영역 연구 프레임워크 구축. - 실증 중심 R&D, **세제혜택·수요보장·재정지원**을 통한 상용화 촉진.
산업 생태계 및 인력 양성	- 스타트업·중소기업이 자유롭게 실증 가능한 **테스트베드 및 규제 샌드박스 확대**. - **피지컬 AI 얼라이언스** 설립으로 대기업-스타트업 협력 강화 및 기술 확산. - 산업별 수요에 대응하는 **다층형 얼라이언스(Multi-Layered Alliance)** 구성 필요. - 초·중·고·대학 연계 AI·로봇 융합 교육 확대 및 **재교육·전문대 실습 중심 훈련 체계** 마련. - AI·기계·전자·HRI·윤리 등 **다학제 기반 통합 교육과정** 확산.
법·제도 및 국제협력	- 로봇 안전 인증, AI 윤리·안전성, 자율 로봇의 **책임소재 명확화** 필요. - ISO·IEEE 등 **국제 표준화 활동에 적극 참여**하여 글로벌 규제 조화 추진. - 주요국과 협력해 **국제 윤리 기준·보호 체계** 마련 및 글로벌 신뢰 확보.

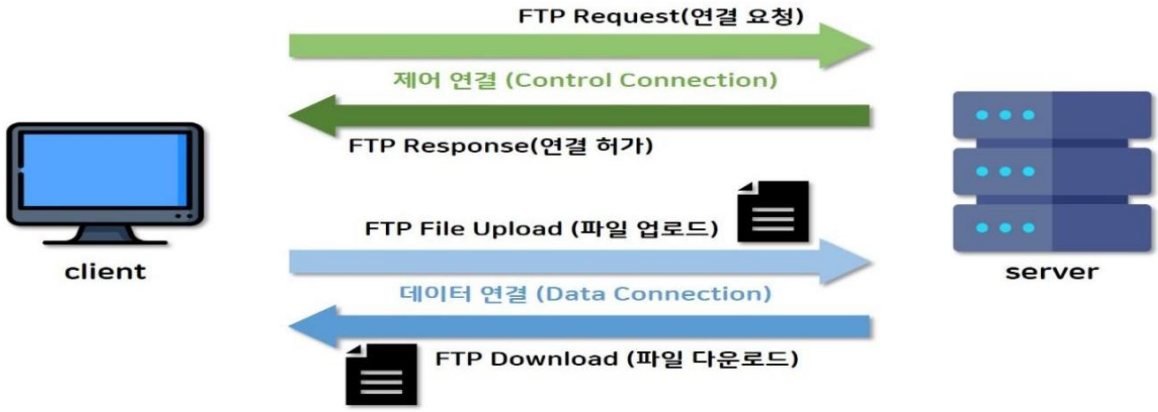
- 피지컬 AI는 국가 전략·R&D·산업 생태계·법·제도 측면에서 기술 자립과 안전한 활용을 위한 종합적 정책·인력·국제협력이 필수적

"끝"

06	FTP(File Transfer Protocol)		
문제	FTP(File Transfer Protocol)에 대하여 다음을 설명하시오. 가. FTP 개념 나. Active Mode와 Passive Mode 비교 다. FTP Bounce Attack의 공격원리와 대응방안		
도메인	보안	난이도	중 (상/중/하)
키워드	제어채널, 데이터채널, 20/tcp 포트, 21/tcp 포트, PORT 명령, LIST 명령, SFTP, FTPS, 최신버전 업데이트, Anonymous FTP		
출제배경	빈출 토픽인 FTP 및 미기출 토픽인 FTP Bounce Attack에 대한 숙지 확인		
참고문헌	ITPE 기술사회 서브노트		
출제자	박서현 기술사(제 131회 정보관리기술사 / mondaysss@naver.com)		

I. 파일 송수신 표준 프로토콜, FTP 개념

가. FTP(File Transfer Protocol) 개념



개념	- TCP/IP 프로토콜을 기반으로 서버와 클라이언트 사이에서 파일 송수신을 하기 위한 표준 네트워크 프로토콜

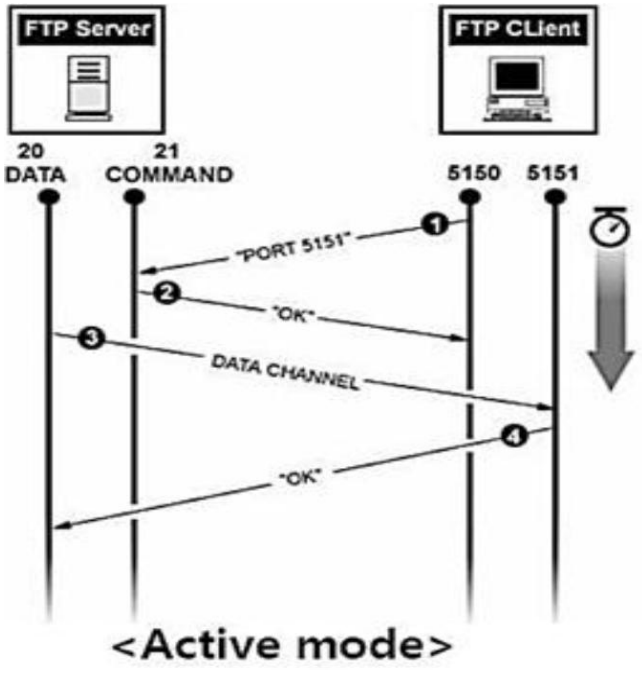
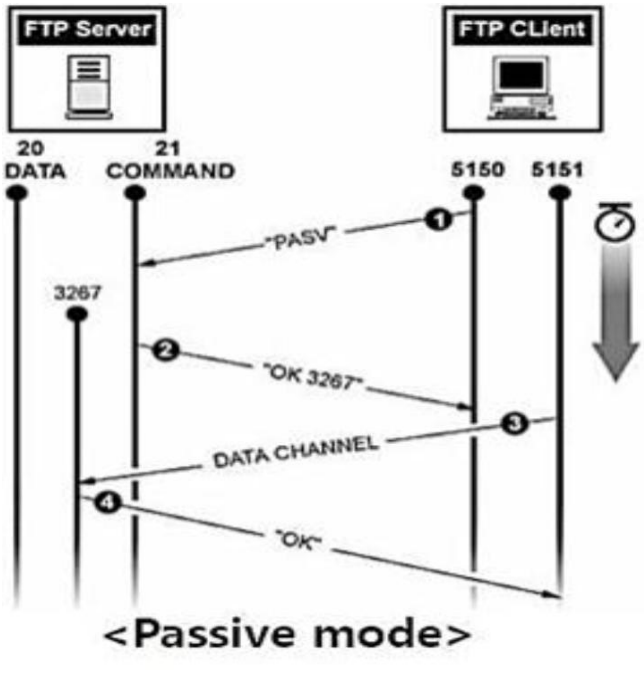
나. FTP(File Transfer Protocol) 구성요소

구분	구성요소	설명
포트	- 제어 포트(21번)	- 클라이언트와 서버 사이의 명령, 제어 등을 송수신 담당
	- 데이터 포트(20번)	- 클라이언트와 서버 사이의 직접적인 파일 송수신 담당
모드	- Active Mode	- 클라이언트가 서버에게 연결할 데이터 포트를 알려주는 모드
	- Passive Mode	- 서버가 클라이언트에게 연결할 데이터 포트를 알려주는 모드
보안	- 인증	- 사용자 인증을 위해 ID와 비밀번호를 요청 - Anonymous(익명) 접속 모드도 지원하나 보안상 취약
	- 암호화	- 보안 강화 위한 FTPS, SFTP와 같은 프로토콜 사용

- FTP 전송 모드의 Active mode와 Passive mode의 동작 차이점 존재

II. Active Mode와 Passive Mode 비교

가. Active Mode와 Passive Mode 개념 비교

Active Mode	Passive Mode
	
- 일반적인 FTP 사용 방식으로 서버에서 클라이언트의 특정 포트에 접속하여 데이터를 전송하는 모드	- 보안 설정된 클라이언트에서 FTP 사용방식으로 클라이언트에서 서버의 특정 포트에 접속하여 데이터를 전송하는 모드

- 데이터 채널을 만들 때 연결 주체가 서버이면 Active Mode, 연결주체가 클라이언트면 Passive Mode

나. Active Mode와 Passive Mode 상세 비교

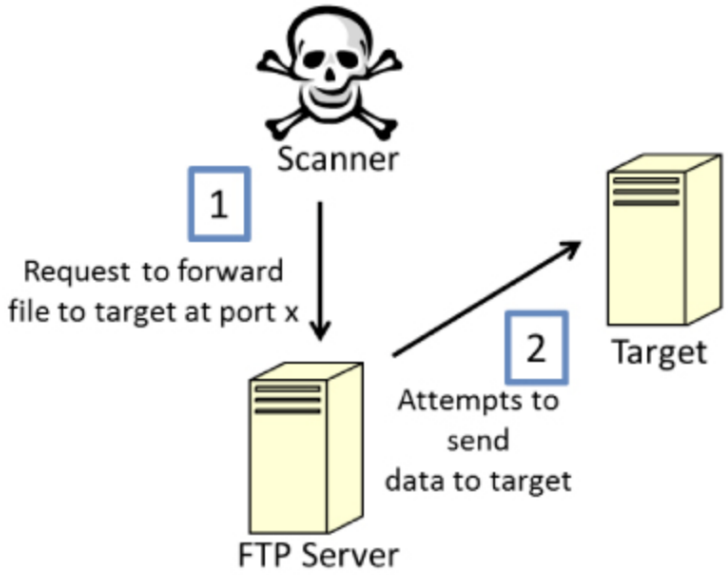
구분	Active Mode	Passive Mode
연결 구조	(1)클라이언트→서버 : 제어채널(21포트) - 서버가 접속할 임의포트(5151)를 전송 (2)서버→클라이언트 : 데이터채널(임의포트) - 서버가 클라이언트의 임의포트(5151)에 connect 요청한 후 file list 전송	(1)클라이언트→서버 : 제어채널(21포트) - 접속요청(PASV) 수락한 서버는 클라이언트가 접속할 임의포트(3267) 전송 (2)클라이언트→서버: 데이터채널(임의포트) - 클라이언트가 임의포트(3267)로 connect 요청한 후 연결되면 서버가 file list 전송
특징	- 서버의 20/tcp 포트를 이용하여 클라이언트의 임의포트에 접속	- 서버의 임의포트에 접속
데이터채널 접속방향	- 서버→클라이언트	- 클라이언트→서버
데이터채널 서버포트	- 20/tcp 포트	- 임의 생성한 포트(1024/tcp 이상)
데이터채널 클라이언트포트	- 임의 생성한 포트(1024/tcp 이상)	- 임의 생성한 포트(1024/tcp 이상)

문제점	- 서버가 접속시도(클라이언트 방화벽차단)	- 서버의 1024 이상 모든 포트 open 필요
사용도	- 낮음	- 높음

- FTP의 Active Mode에서 제어 채널과 데이터 채널을 별도로 사용하고, 데이터 채널 생성 시 목적지를 확인하지 않는 설계 허점을 이용한 FTP Bounce Attack 발생

III. FTP Bounce Attack의 공격원리와 대응방안

가. FTP Bounce Attack의 공격원리



단계	절차	설명
1단계	- 공격자→FTP서버 접속	- 공격자는 FTP 서버에 Active Mode로 접속 - 데이터채널의 목적지를 공격대상 서버 IP, Port로 지정하는 PORT 명령 전송
2단계	- FTP서버→공격대상 서버 데이터채널 접속 시도	- FTP 서버는 공격대상 서버로 데이터 채널 생성을 시도 - 데이터 채널 생성에 성공하면 LIST 명령의 결과를 데이터 채널로 전송(FTP 서버를 스캐닝 도구처럼 사용)
3단계	- FTP서버→공격대상 서버 데이터 전송	- 공격자의 IP는 숨겨지고 FTP 서버가 공격대상 서버에 접속하는 프록시 역할을 수행

- FTP 프로토콜의 Active Mode('PORT'명령)를 악용하여 공격자가 FTP 서버를 우회 프록시처럼 사용해 공격 대상 서버에 TCP 연결을 생성, 공격자는 자신의 IP를 드러내지 않고 공격 대상 서버 포트 스캐닝 또는 악성코드를 전송하는 등의 공격 가능

나. FTP Bounce Attack의 대응방안

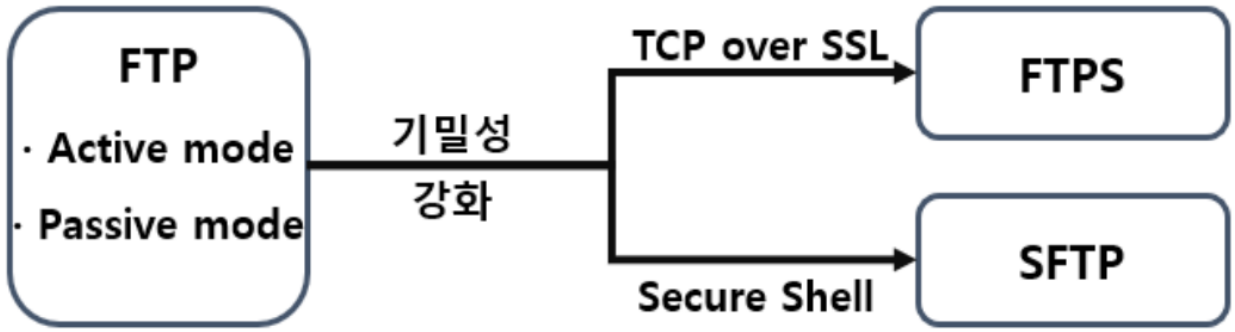
구분	대응방안	설명
프로토콜 변경	- SFTP 또는 FTPS 사용	- 인증정보와 데이터가 암호화하여 송수신되는 SFPT, FPTS 프로토콜을 사용하여 안정성 강화

서버보안	- FTP 서버 업데이트	- FTP 서버 소프트웨어를 항상 최신 버전으로 유지하고 보안 패치를 적용하여 알려진 취약점을 해결
	- Anonymous FTP비활성화	- 기본으로 제공되는 Anonymous FTP 기능을 사용하지 않도록 설정, 만약 필요하다면 업로드 권한을 제한하고 특정 디렉토리만 허용하는 등 접근 제어를 엄격히 설정
	- PORT 명령 제한	- FTP 서버가 PORT 명령을 통해 원격 호스트에 연결 시도 시 요청 클라이언트의 IP와 동일한 IP 주소로만 연결하도록 제한
네트워크 보안	- 불필요한 포트 차단	- 불필요한 포트에 대한 외부 접근을 차단
	- 네트워크 모니터링	- FTP 서버의 로그를 모니터링하고 의심스러운 활동(ex. 비정상적 PORT 명령 시도) 감지 시 즉시 대응 가능한 시스템 구축

- FTP 서버 취약점을 이용하는 보안 취약점을 사전에 제거 및 강회된 보안 프로토콜인 FTPS, SFTP 적용

IV. FTP, FTPS, SFTP 비교

가. FTP, FTPS, SFTP의 개념 비교



FTP	FTPS	SFTP
- TCP/IP 프로토콜을 기반으로 서버, 클라이언트 사이에서 파일 송수신 하기 위한 프로토콜	- 보안 기능을 제공하기 위하여 SSL/TLS 암호화 프로토콜 기반에서 동작하도록 설계된 FTP 프로토콜	- SSH(Secure Shell)를 통해 동작하는FTP 로, TCP 보안 채널(터널링)을 형성하여 데이터의 안전한 전송을가능하게 하는 FTP 프로토콜

나. FTP, FTPS, SFTP의 상세 비교

구분	FTP	FTPS	SFTP
프로토콜	- TCP	- TCP Over SSL	- TCP + Secure Shell
사용 포트	- 21	- 21 or 990	- 22
데이터 형식	- Readable	- Readable	- 이진 형식
기밀성	- 평문	- 암호화	- 암호화
암호화	- 평문	- 인증 관련 부분 데이터	- 인증 관련된 부분 데이터 패킷까지 암호화하지 않음

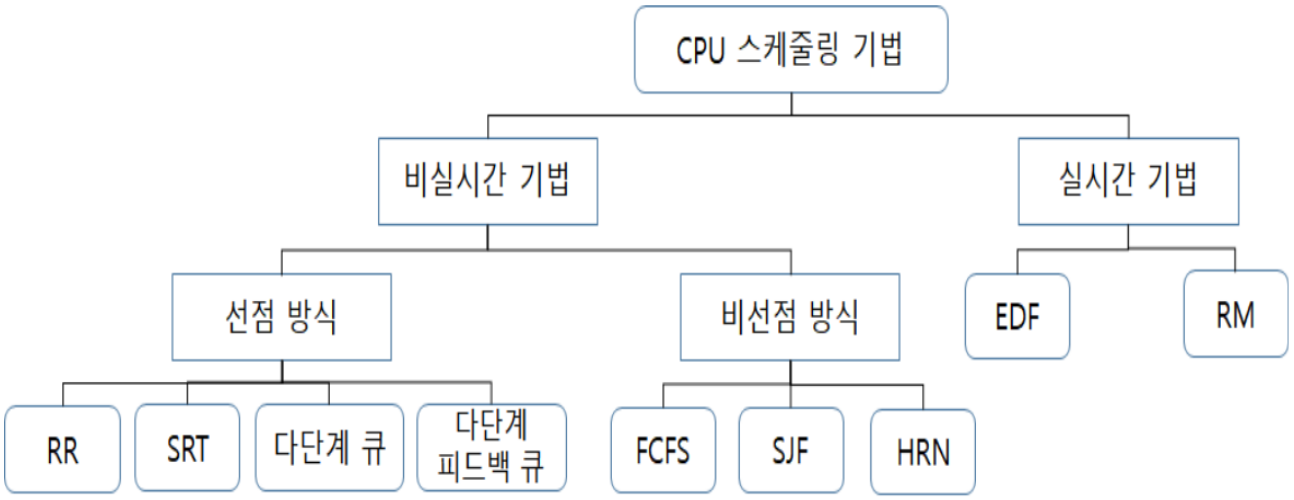
기능	- 파일 전송	- FTP 기능 + 분할 압축,	- FTP 기능+ 인증, 암호화, 무결성, 압축, 터널링
장점	- 형식 간단 유연	- 보안 우수	- 보안 좋음, 설정 공유, 간편
단점	- 보안 취약점	- 복잡	- 해킹 가능성 존재
표준	- RFC 959, 1123	- RFC 959, 1123, 4127, 2228	- 없음

- FTP 서비스 사용시에는 보안성을 고려하여 SFTP, FTPS 프로토콜 사용을 권장

"끝"

06	CPU 스케줄링		
문제	CPU 스케줄링 방식에 대해서 다음을 설명하시오. 가. 선점형 스케줄링 기법 나. 비선점형 스케줄링 기법 다. 호위효과(Convey Effect)		
도메인	운영체제	난이도	하 (상/중/하)
키워드	Round Robin, SRT, MLQ, MLFQ, FCFS, SJF, HRN		
출제배경	빈출 토픽에 대한 숙지 확인		
참고문헌	ITPE 기술사회 서브노트		
출제자	박서현 기술사(제 131회 정보관리기술사 / mondaysss@naver.com)		

I. CPU의 효율적 운용을 위한, CPU 스케줄링 기법의 개요



개념	CPU를 효율적으로 사용하기 위해 다중 프로그래밍을 가능하도록 운영체제에서 프로세스를 대상으로 CPU 자원을 할당하는 순서를 정하는 방법 및 기법

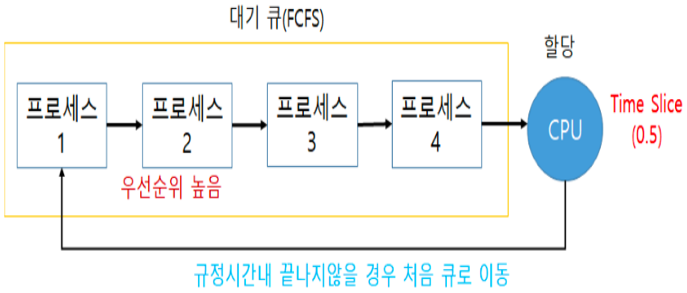
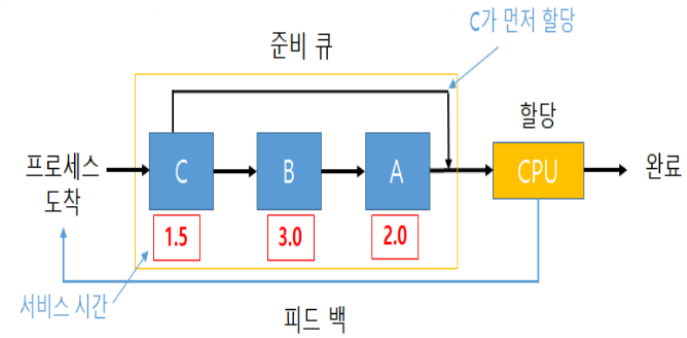
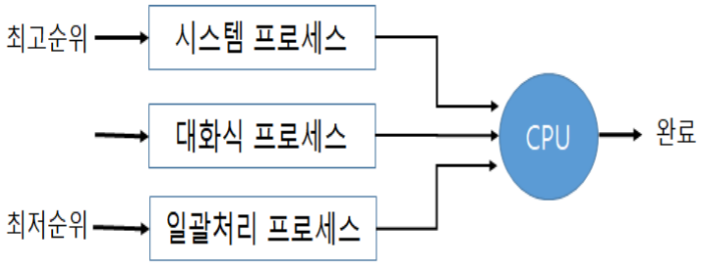
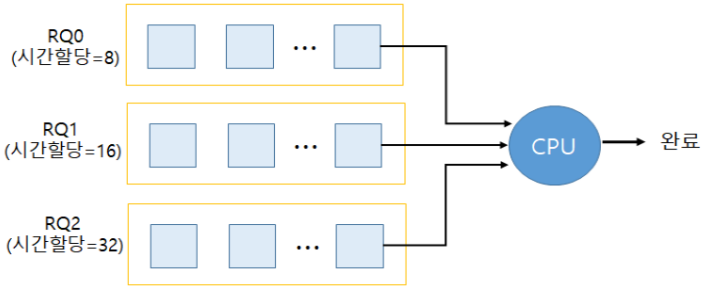
- 프로세스가 실행 상태일 때 우선 순위가 높은 다른 프로세스가 현재 프로세스를 중단시키고 CPU를 차지할 수 있다면 선점, 없다면 비선점형 스케줄링으로 구분하고 프로세스가 요청되었을 때 제한시간 안에 처리여부에 따라 실시간, 비실시간 알고리즘으로 구분

II. 선점형 스케줄링 기법 설명

가. 선점형 스케줄링 기법 개념

- 하나의 프로세스가 CPU를 차지하고 있을 때 우선순위가 높은 다른 프로세스가 현재 프로세스를 중단시키고 CPU를 차지할 수 있는 기법

나. 선점형 스케줄링 기법 상세 설명

유형	개념도	설명
Round Robin		- 타임 퀀텀(Time Quantum)을 사용하여 각 프로세스가 고정된시간 동안 CPU를 할당 받고, 해당 시간이 지나면 다음 프로세스에게CPU를 넘기는 방식의 선점형 스케줄링 알고리즘
SRT (Shortest Remaining Time First)		- 실행시간이 가장 짧은 프로세스를 먼저 실행, 새로운 프로세스가 도착하면 현재 실행중인 프로세스와 비교하여 남은 실행 시간이 더 짧은 프로세스가 CPU 할당
MLQ (Multi-Level Queue)		- 프로세스들을 여러 개의 큐로 나누고, 각 큐는 다른 우선순위와 스케줄링 알고리즘을 사용하여 운영하는 방식
MLFQ (Multi-Level Feedback Queue)		- Multi-Level Queue의 확장형으로, 프로세스가 큐들 사이를 이동 할 수 있게 하여 동적으로 우선순위를 조정하는 방식

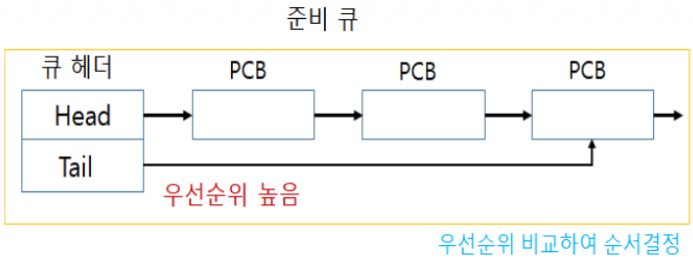
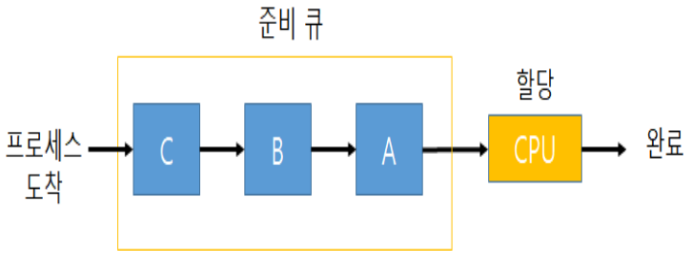
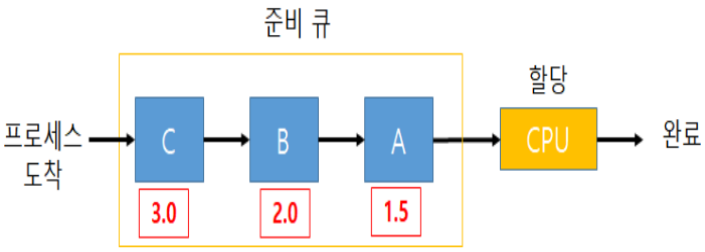
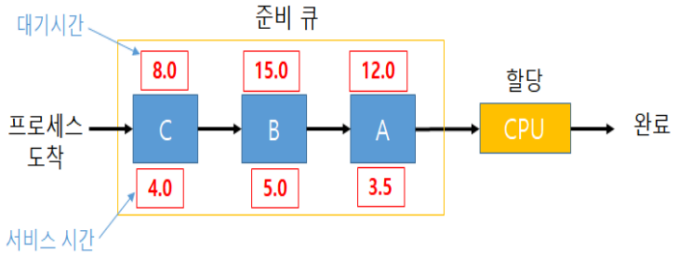
- 선점 방식은 CPU를 사용 중인 프로세스를 강제로 중단하고 교체하여 응답성이 빠르고 실시간 처리에 유리

III. 비선점형 스케줄링 기법 설명

가. 비선점형 스케줄링 기법 개념

- 한 프로세스가 CPU를 할당 받으면 작업 종료 후 CPU 반환 시까지 다른 프로세스는 CPU 점유 불가한 CPU 스케줄링 방법

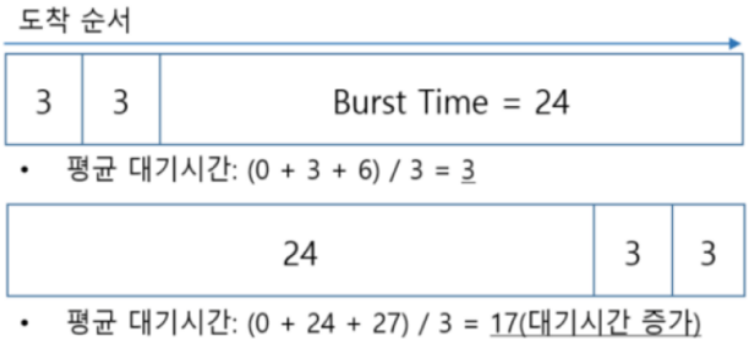
나. 비선점형 스케줄링 기법 상세 설명

유형	개념도	설명
우선순위 (Priority)		- 프로세스에 우선순위를 부여하고 우선순위가 높은 프로세스에 CPU를 먼저 할당하는 방식
FCFS (First Come First Service)		- 프로세스가 대기큐에 도착한 순선대로 CPU 할당 - 가장 간단한 스케줄링 알고리즘으로 FIFO(First Input First Out) 알고리즘
SJF (Shortest Job First)		- 대기큐에 있는 프로세스들 중에 실행시간(Burst Time)이 가장 짧은 프로세스에게 CPU를 먼저 할당하는 기법
HRN (Highest Response Ratio Next)		- 대기 프로세스 중 우선순위(Response Ratio)가 높은 작업을 먼저 수행하는 알고리즘 - 대기큐에 있는 프로세스들 중 우선순위가 높은 프로세스에게 먼저 CPU를 할당하는 기법

- 비선점 방식은 프로세스가 CPU를 자발적으로 반환까지 다른 프로세스가 대기하며, 처리 순서가 보장되지만 응답시간이 느리거나 호위효과 등 발생우려

IV. 호위효과(Convey Effect) 설명

가. 호위효과(Convey Effect)의 개념



개념	CPU 스케줄링에서 긴 작업이 CPU를 장시간 점유할 때, 짧은 작업들이 그 뒤를 따라 대기하면서 시스템의 전체 처리 성능이 저하되는 현상

- 호위 현상은 대표적으로 FCFS(First-Come First-Served) 스케줄링 기법에서 나타나며, 긴 작업이 CPU를 장시간 점유해 짧은 작업들이 대기하면서 시스템 처리 성능이 저하 문제

나. 호위효과(Convey Effect) 해결방안

구분	해결방안	설명
선점	선점형 스케줄링	- 긴 작업 중간에 짧은 작업이 CPU를 사용할 수 있도록 선점 방식으로 스케줄링해 긴 작업이 짧은 작업을 방해 금지
	라운드로빈 스케줄링	- Time Slice 단위로 CPU를 공정하게 분배하여 Burst Time이 긴 작업이 CPU를 독점하는 것을 예방
	MLFQ(Multi-Level Feedback Queue)스케줄링	- Burst Time이 긴 작업은 우선순위가 낮은 큐로 이동 - 짧은 CPU Burst 프로세스를 상위 큐에서 처리
비선점	SJF(Shortest Job First)	- 짧은 CPU Burst 프로세스를 우선 처리 - Burst Time이 긴 작업은 계속 우선순위에서 밀리는 기아 현상
	HRN (Highest Response Ratio Next)	- 짧은 CPU Burst와 대기시간이 긴 프로세스를 우선 처리 - 대기시간을 우선순위 선정 시 반영하여 기아 현상을 방지
	우선순위 스케줄링	- 짧은 CPU Burst 프로세스에 높은 우선순위 부여 - 우선순위 역전 문제 발생할 수 있어 에이징으로 해결

- 호위현상 문제 해결하기 위해 선점형 스케줄링, SJF, 라운드 로빈, 멀티 레벨 큐 같은 방식을 적용

"끝"

제 39 회 ITPE
실전 명품 모의고사 해설집

대 상 정보관리기술사, 컴퓨터시스템응용기술사, 정보통신기술사, 정보시스템감리사 시험
발행일 2025년 12월 21일
집 필 강정배 PE, 전일 PE, 이상헌 PE, 소민호 PE, 현수 PE, 박서현 PE, 배미경 PE
출 판 **ITPE(Information Technology Professional Engineer)**
주 소 ITPE 대치점 서울시 강남구 선릉로 86길 17 선릉엠티빌딩 7층
ITPE 선릉점 서울시 강남구 선릉로 86길 15 3층 IT교육센터 아이티피이
ITPE 강남점 서울시 강남구 테헤란로 52길 21 파라다이스벤처타워 3층 303호
ITPE 영등포점 서울시 영등포구 당산동2가 하나비즈타워 7층 ITPE
ITPE 을지로점 서울시 중구 삼일대로 363, 2615호(장교동 장교빌딩)
ITPE 강북점 서울 종로구 수표로 96, 7층 (관수동,국일관드림팰리스)
연락처 070-4077-1267 / itpe@itpe.co.kr