119 회 정보처리기술사 합격을 위한

118 회 정보관리기술사

기출풀이

- KPC 기술사회-

SMART KPC
한국생산성본부

교육 문의 및 상담 : 한 승 연

- Tel : 02) 724-1831/1223
- Fax : 02) 724-1875
- Email : syhan@kpc.or.kr
- Web Site : www.kpc.or.kr
cafe.naver.com/81th

kpc 기술사회

119 회 합격대비 심화반 신청 안내

[토요일 명품심화반] 5.25.(토) 개강

- O 열정반(박상욱/KPC): cafe.naver.com/81th/134354
- O 공감반(공수재/KPC): cafe.naver.com/81th/134329
- O MP 필통반(구환회/KPC): cafe.naver.com/81th/134384
- O ITPE Makers(박제일/KPC): cafe.naver.com/81th/134386
- O 단합반(SPP 반)(안경환/KPC): cafe.naver.com/81th/134412
- O FB(Future Builders)(강희석/KPC): cafe.naver.com/81th/134330
- O 정주행(서정훈/KPC): cafe.naver.com/81th/134299

[일요일 명품심화반] 5.19.(일) 개강

- O T.O.P 반 (유술사/KPC): https://cafe.naver.com/81th/137407
- O NS 반 (강정배/박주형/강남아지트): https://cafe.naver.com/81th/134237

[유일한 평일 명품심화반] 5.17.(금) 개강

- O 강남평일야간반 (강정배/전일/강남아지트/화,금):

  https://cafe.naver.com/81th/133950

※ 신 청 : KPC 홈페이지에서 신청 가능합니다.

※ 교육비: 9 주 91 만원

국가기술자격 기술사 시험문제

기술사 제 118 회 제 1 교시 (시험시간: 100 분)

분야	정보통신	종목	정보관리기술사	수험번호		성명	

※ 다음 문제 중 10 문제를 선택하여 설명하시오. (각 10 점)

1. 정규화(Normalization)의 의미와 효과
2. 빅데이터 분석 플랫폼이 추구하는 데이터 통합 아키텍처
3. 현실세계에서 모델링(Modeling)의 필요성과 Inside-Out 전략
4. 가상공간(Cyber Space)의 특징과 디지털 트윈(Digital Twin)의 의미
5. SLM(Service Level Management) 프레임워크의 구성요소
6. 디지털 윤리(Digital Ethics)와 개인정보보호(Privacy)
7. 선형회귀모형의 추론에 대한 가정 4 가지
8. 모바일 엣지 컴퓨팅(Mobile Edge Computing)
9. 금융권에서 블록체인 시스템을 도입할 시 고려해야 할 정보보안 이슈
10. 5G 네트워크 슬라이싱(5G Network Slicing)
11. 멀티 모달 인터페이스(Multimodal Interface)의 구성요소
12. 해시값(Hash Value)과 해시함수의 구분, 종류, 용도
13. CMMI(Capability Maturity Model Integration)의 단계적 표현(Staged Representation)과 연속적 표현(Continuous Representation)

1	정규화(Normalization)
문제	정규화(Normalization)의 의미와 효과
도메인	데이터베이스
정의	데이터의 중복성을 최소화, 이상현상 방지, 정보의 일관성을 보장하기 위해 함수 종속성을 이용하여 속성들 간의 종속성을 분석해서 하나의 릴레이션에는 하나의 종속성만 갖도록 분해하는 과정
키워드	중복 최소화, 이상현상 방지, 일관성 보장, 함수 종속성 이용
출제의도분석	DB 정규화 문제의 포괄적 의미 질문 및 효과 파악
답안작성 전략	정규화의 단계적 의미와 효과에 초점을 맞추어 충분한 설명 필요
참고문헌	서브노트
풀이 기술사님	표기수 PE (제 117 회 정보관리기술사 / kisu.pyo@gmail.com)

1. 정규화(Normalization)의 정의 및 단계별 의미

가. 정규화(Normalization)의 정의

- 데이터의 중복성을 최소화, 이상현상 방지, 정보의 일관성을 보장하기 위해 함수 종속성을 이용하여 속성들 간의 종속성을 분석해서 하나의 릴레이션에는 하나의 종속성만 갖도록 분해하는 과정

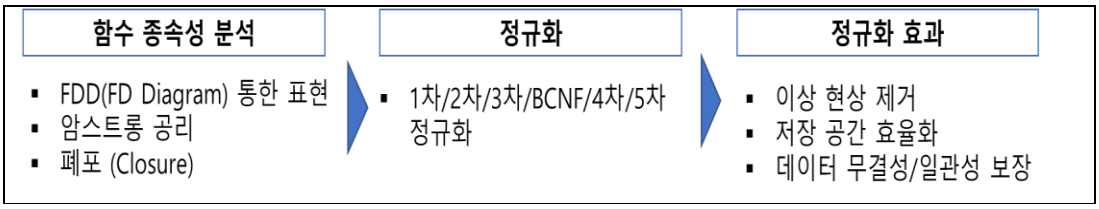
나. 정규화(Normalization)의 단계별 의미

단계	핵심 요소	의미
1 차 정규화	원자성	각 속성에 값이 반복이 없는 원자 값으로만 구성되도록 분해하는 과정
2 차 정규화	부분함수 종속성 제거	주식별자가 아닌 속성들 중에서 주식별자 전체가 아닌 일부 속성에 종속된 속성을 찾아 제거하는 과정
3 차 정규화	이행함수 종속성 제거	기본키 외의 속성들 간에 함수적 종속성을 가지지 않도록 이행함수 종속성을 제거해 가는 과정
BCNF	결정자 함수 종속성 제거	복잡한 식별자 관계에 의한 문제를 해결하기 위해, 후보키가 아닌 결정자를 제거하는 과정
4 차 정규화	다치 종속성 제거	하나의 릴레이션에 두 개 이상의 다치 종속이 발생하는 경우 이를 제거하는 과정
5 차 정규화	조인종속성 제거	조인 종속(JD)이 존재하지 않거나 JD 에 의해 분해되는 Projection 들이 원래 릴레이션의 후보키를 유지하는 과정

- 정규화 원칙인 정보 무손실, 중복성 감소, 분리 원칙에 근거하여 수행

2. 정규화(Normalization)의 효과

가. 정규화 수행 효과 개념도



- 함수 종속성 추론 규칙인 폐포와 암스트롱 공리 활용한 종속성 파악 및 정규화 수행

나. 정규화의 상세 효과

효과	핵심 요소	설명
이상현상 제거	갱신/삽입/삭제 이상	- 데이터의 중복과 종속으로 발생하는 갱신/삽입/삭제 이상현상 제거
저장 공간의 효율화	데이터 중복 최소화	- 불필요한 데이터 중복을 최소화하여 데이터 저장 공간의 효율화 충족
데이터 일관성/무결성 보장	종속성 제거	- 폐포와 암스트롱 공리를 활용하여 함수 종속성 분석 - FDD 를 통해 종속성 표현 - 종속성 제거하는 정규화를 통해 일관성/무결성 유지

- 정규화로 인해 성능이 과도하게 저하되는 경우 업무에 따라 반정규화 수행

3. 정규화(Normalization)의 효과 극대화를 위한 주의점과 해결방안

주의점	해결 방안
- 빈번한 Join 연산이 증가하여 성능이 낮아질 수 있음 - 과도한 테이블 분리로 인해 스키마가 복잡해져 이해하기 힘들고 유지보수 어려움	- 업무 특성에 따라 반정규화를 수행하여 성능 향상 (일관성 문제 발생시 영향범위 파악 필요) - 관계 테이블 설명서 등을 작성시 관련 있는 테이블, 칼럼 간의 관계를 상세히 기술

"끝"

[참고] 통계학 및 데이터 분석 분야의 정규화(Normalization)

데이터 분석 시 데이터의 범위를 일치시키거나 분포를 유사하게 만들어 주기 위해 정규화 작업을 선행한 후 분석을 수행함.

참고 : https://adnoctum.tistory.com/184

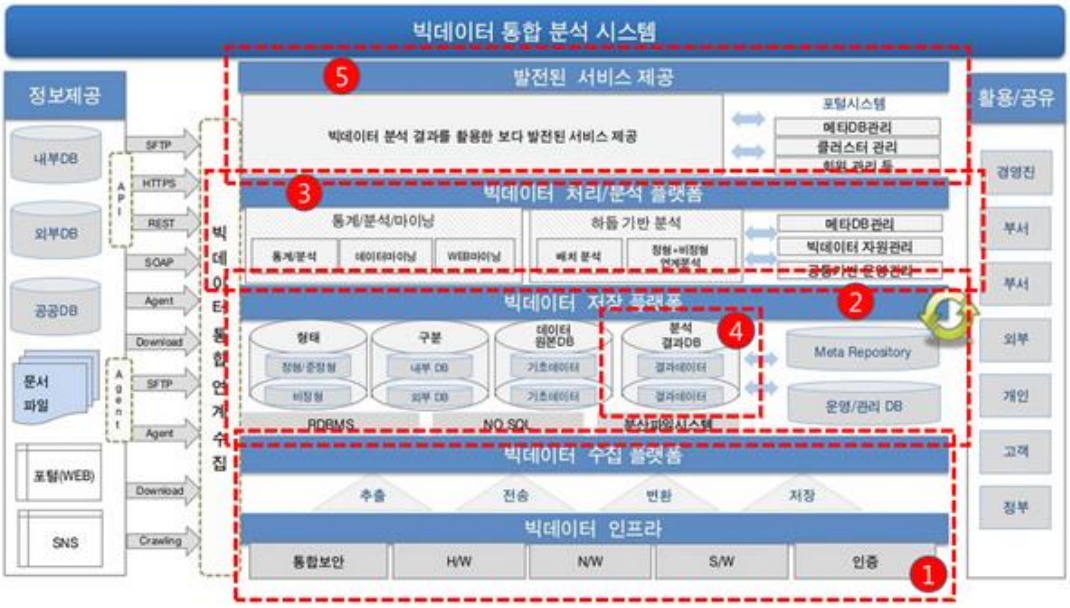
2	데이터 통합 아키텍처
문제	빅데이터 분석 플랫폼이 추구하는 데이터 통합 아키텍처
도메인	데이터베이스
정의	비즈니스 요구사항에 맞는 적절한 분석 방법을 지원하기 위해 데이터 라이프사이클 관리 및 데이터 유형의 변화에 변경없이 적용 가능한 통합 아키텍처
키워드	데이터 라이프사이클, 비정형
출제의도분석	하둡을 비롯한 비정형 데이터를 다루는 데이터 인프라가 가능해지면서 빅데이터 분석/처리 외에 데이터 통합에 대한 이슈도 부상
답안작성 전략	데이터 통합 아키텍처 설계시 레이어 구성별 요소 기술 상세 기술
참고문헌	빅데이터 시대의 데이터 통합 전략: 공공부문 사례 분석 (함유근) https://m.blog.naver.com/PostView.nhn?blogId=samsjang&logNo=220788844868&proxyReferer=https%3A%2F%2Fwww.google.com%2F
풀이 기술사님	표기수 PE (제 117 회 정보관리기술사 / kisu.pyo@gmail.com)

1. 비정형 데이터의 통합, 데이터 통합 아키텍처의 개념

- 비즈니스 요구사항에 맞는 적절한 분석 방법을 지원하기 위해 데이터 라이프사이클 관리 및 데이터 유형의 변화에 변경없이 적용 가능한 통합 아키텍처

2. 데이터 통합 아키텍처 및 요소 기술

가. 데이터 통합 아키텍처



- 기구축된 시스템에 추가 구축하는 경우, 기존 인프라를 최대 활용 및 레이어별 요소 기술 추가

나. 데이터 통합 아키텍처의 요소기술

레이어	요소 기술	설명
빅데이터 수집	로그 수집기 크롤링(Crawling) 스쿱(Sqoop)	- 내부와 외부의 매체로부터 수동/자동으로 데이터 수집 -단순히 데이터를 모으는 것이 아니라 조건에

	플럼(Flume) 스크라이브(Scribe)	따라 검색하고 원하는 형태로 변환
빅데이터 저장	병행 DBMS Hadoop NoSQL	- 실시간으로 데이터를 원하는 형태로 저장 - 데이터를 빠르고 쉽게 분석할 수 있도록 저장 형태를 미리 정의
빅데이터 정제	분산 병렬처리 인메모리 처리	- 수많은 빅데이터를 분석하라 수 있도록 저장, 전달, 관리
빅데이터 분석	Data Mining Machine Learning Predictive Analysis SNS Analysis	-빅데이터를 비즈니스에 활용하기 위해 활용 분야별로 분석
빅데이터 지식화	Data Visualization Information Visualization	- 분석된 데이터를 의미 있는 정보로 보일 수 있도록 정보화 및 시각화

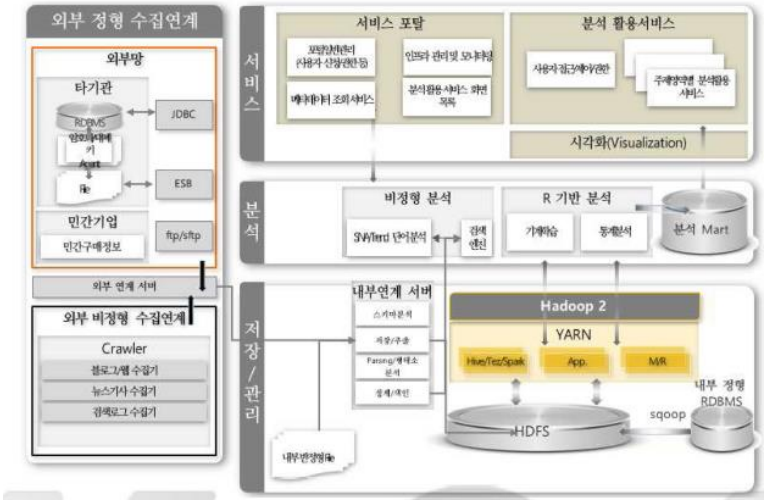
- 기존 데이터 통합의 한계점에 따라 Data Lake 방식 도입

3. 데이터 통합의 한계점과 해결 방안

한계점	해결 방안
• 실시간 분석 위한 통합 한계 • 기존 Data의 물리적 통합 • 기관 간의 Data 접근에 제한적	• Data Lake 방식 : DW, DM과 달리 원본 Data 형태 그대로 제공 • 클라우드 시스템 : Data 규모 확장성 측면의 효율성 • 논리적 Data Warehouse : 데이터 소스별 분산 저장/관리 후 사용자 이용시 가상적 통합/이용

- 데이터 유형 변화 수용 및 데이터 용량 증가에 대응 가능해야 함

[참고] 데이터 통합 아키텍처 사례



"끝"

3	모델링(Modeling) 필요성, Inside-Out 전략
문제	현실세계에서 모델링(Modeling)의 필요성과 Inside-Out 전략
도메인	IT 경영
정의	Inside-Out 전략 : 기업이 기술을 외부로 내보내서 자사의 기존 비즈니스 모델이 아닌 다른 경로의 상업화를 모색하는 개방형 혁신의 전략
키워드	Licensing-Out, Spin-Out, Spin-Off, 프로젝트 공개
출제의도분석	기업의 혁신을 위한 개방형 혁신의 전략과 모델 질문
답안작성 전략	질문이 모델링의 필요성이므로, 관점별 그룹핑으로 상세히 기술 Inside-Out 전략은 개방형 혁신과 연계, 상세 유형과 Outside-In 전략 언급 필요
참고문헌	https://www.slideshare.net/human5804/case-study-64557362 https://brunch.co.kr/@hvnpoet/25 Chesbrough 의 개방형 혁신 이론, 김석관 오픈 이노베이션의 개념과 성공사례, NIPA 정책동향
풀이 기술사님	표기수 PE (제 117 회 정보관리기술사 / kisu.pyo@gmail.com)

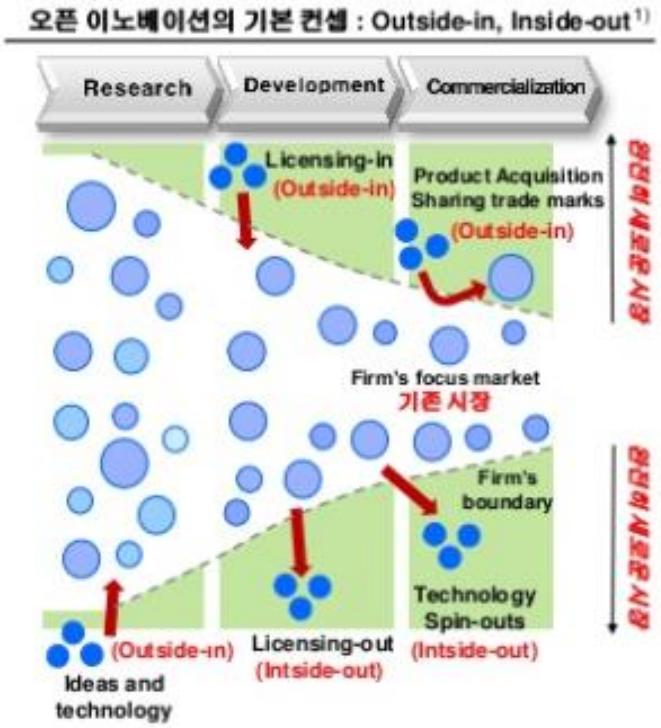
1. 현실세계에서 모델링의 필요성

관점	필요성	설명
사회적 측면의 필요성	의사소통 도구	- 참여자 간의 소통을 위한 도구로서의 역할
	핵심 파악 및 문제 해결	- 모델의 가시화를 통한 현실의 핵심 파악 및 문제 해결책 도출
	R&D / 교육 및 훈련	- 구조화를 통한 연구 및 개발 수행 - 시뮬레이션 통한 교육/훈련 가능
	시뮬레이션 가능	- 가상 시뮬레이션을 통한 이벤트 가상 실현 및 효과 분석 가능
비즈니스 측면의 필요성	가치 제안	- 제공되는 제품이 창출하는 가치를 규정
	목표 시장 규정	- 제공되는 제품이 사용될 사용자 및 시장 규정
	가치 사슬 정의	- 기업이 제품을 만들고 판매하기 위한 가치 사슬 구조 정의 및 필요사항 규정
	비용/편익 구조 추정	- 기업의 매출 창출 위한 절차 규정 및 비용/편익 구조 추정
	가치 네트워크 형성	- 공급자, 소비자, 경쟁자 등으로 구성된 생태계내에서 기업의 위치를 정해줌
	경쟁 전략 수립	- 혁신 기업이 경쟁자들에 대해 우위를 확보하기 위한 경쟁 전략을 포함

- 단순화, 추상화, 구조화, 시각화를 통해 모델링 수행

2. Inside-Out 전략의 개념 및 상세 유형

가. Inside-Out 전략의 개념

개념도	
개념	- 기업이 기술을 외부로 내보내서 자사의 기존 비즈니스 모델이 아닌 다른 경로의 상업화를 모색하는 개방형 혁신의 전략

- 개방형 혁신을 위한 전략으로 Inside-Out 과 Outside-In 전략 존재

나. Inside-Out 의 상세 유형

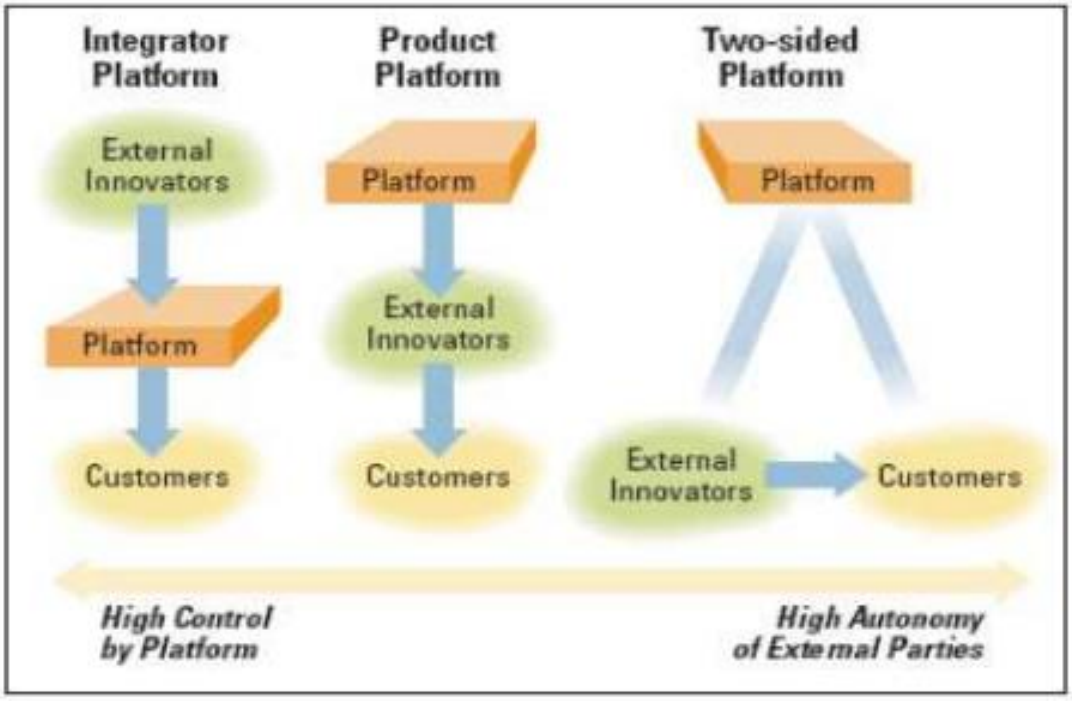
유형	핵심 요소	설명
Licensing-Out	기술 외부 판매	- 자사 기술 외부 판매, 타사 사업모델 통해 사업화 모색
Spin-Out	기업 일부를 전문 회사로 설립	- 기업의 일부 사업부 또는 신규사업을 분리하여 벤처회사 형태로 전문회사를 설립
Spin-Off	별도 조직 통한 사업화	- 기존 조직 내 사업화가 어려운 경우 별도 조직을 통해 사업화
프로젝트 공개	외부 전문가 참여 및 공유 촉진	- 내부 프로젝트를 외부에 공개하여 외부 전문가의 참여 및 공유를 촉진

3. 개방형 혁신의 전략과 Model

구분	전략/유형	설명
전략	Inside-Out 전략	- 기술판매, 스핀오프 등
	Outside-In 전략	- 기술구매, 공동연구, 합작벤처설립, 기업인수 등

모델	Integrated Platform Model	- 플랫폼의 소유자가 외부 개발자와 고객 사이에서 외부 개발자가 개발한 제품을 직접 판매하는 방식
	Product Platform Model	- 외부 개발자가 플랫폼 소유자의 기술을 이용해 제품을 개발하여 직접 고객에게 판매하는 모델
	Two-Sided Platform Model	- 플랫폼 소유자와의 계약된 플랫폼 환경 하에서 활동한다는 조건 하에서 외부 개발자가 자유롭게 고객과 직접 거래를 하는 모델

[참고] 개방형 혁신의 모델



"끝"

4	가상공간 특징, 디지털 트윈 의미
문제	가상공간(Cyber Space)의 특징과 디지털 트윈(Digital Twin)의 의미
도메인	디지털서비스
정의	디지털 트윈 : 현실 세계에서 사람이 쉽게 접근할 수 없는 공간이나 물건 등 여러 부분들에 대해 가상모델링화 하여 지속적인 관찰과 보수가 가능하게끔 하는 기술 모델
키워드	CPS, 시뮬레이션, 디지털 스레드
출제의도분석	가트너 핵심 기술로 선정된 디지털 트윈에 대한 연계 질문
답안작성 전략	디지털 트윈의 의미를 가상공간과 연계하여 작성
참고문헌	위키피디아 https://www.nocutnews.co.kr/news/5046468 KPC 114 회 정보관리기술사 기출풀이
풀이 기술사님	표기수 PE (제 117 회 정보관리기술사 / kisu.pyo@gmail.com)

1. 가상 공간(Cyber Space)의 특징

가. 가상 공간의 생태계 측면 특징

특징	핵심 요소	설명
온라인 상의 DB	정보의 무한 복제 가능	- 가상 공간의 데이터 생산자는 동시에 소비자 역할을 하며 정보의 무한 생산/복제/소비 가능
쌍방향 매체	데이터의 쌍방향 송수신	- 현실 공간에 비해 데이터 제공/소비자 간의 쌍방향 송수신이 자유로움
데이터, 인간 간의 네트워크 형성	Data-Data, Data-인간 간 연결	- 가상 공간 상의 데이터 전달을 통해 데이터 간 혹은 데이터-인간 간의 네트워크 형성
변경 용이성	비마모성	- 신규 요소 적용 및 시뮬레이션 수행 시의 환경 비마모성으로 인해 현실 공간보다 변경이 용이
비즈니스 창출 가능	가상 공간의 신규 비즈니스	- 가상 공간을 통해 쇼핑, 휴식 등 다양한 형태의 비즈니스 가치 창출

- ICT 기술 발전에 따라 현실 공간과 가상 공간의 연결

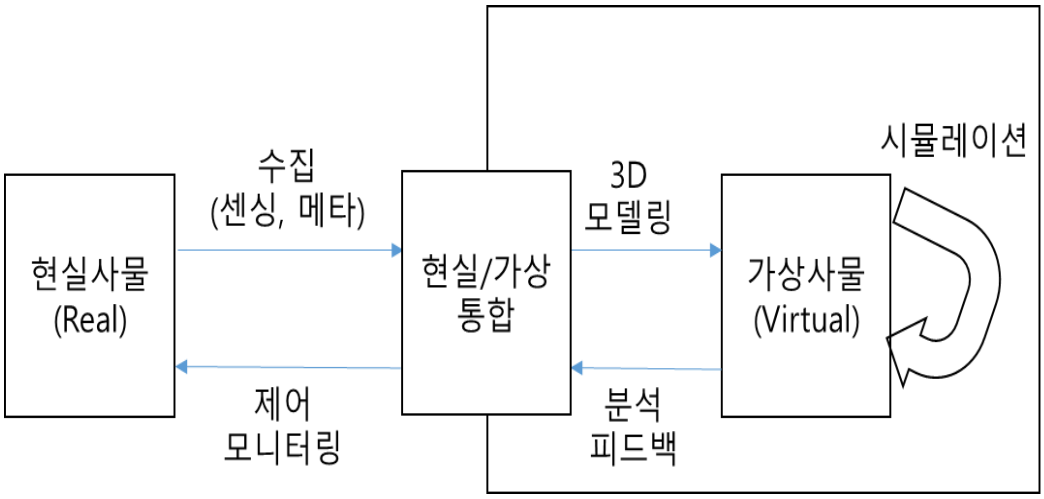
나. 가상 공간의 기술 측면 특징

특징	핵심 요소	설명
VR 기술 활용	입출력, 오감기술, 음향/모션기술	- 몰입감 증대를 위해 가상 현실에 대한 입출력 및 오감, 음향/모션기술 활용
3D 모델링	능동/수동적 모델링	- 동적/정적 객체에 대한 능동/수동적 모델링 수행 - 3 차원 거리 스캐너, 광선 패턴, 깊이 카메라 등 활용
디지털 트윈 기술 활용	시뮬레이션 통한 가상 모델 분석	- 현실세계에 대한 가상 모델 상의 시뮬레이션을 통해 분석 결과 재반영

- 디지털 트윈을 통해서 가상 세계의 정보를 현실세계로 연결 가능

2. 디지털 트윈(Digital Twin)의 의미

가. 디지털 트윈의 개념도



- 현실 세계에서 사람이 쉽게 접근할 수 없는 공간이나 물건 등 여러 부분들에 대해 가상모델링화 하여 지속적인 관찰과 보수가 가능하게끔 하는 기술 모델

나. 디지털 트윈의 의미

관점	핵심요소	의미
비즈니스 관점	IoT 산업 연계 CPS 구현	- 물리적 환경의 디지털화를 통해 현실세계의 특징을 최대한 반영 및 가상 시뮬레이션 가능한 기술 - 스마트 공장, 스마트 시티, 선박 모델링, DTO
기술적 관점	센싱 데이터 수집, 데이터 분석, 시뮬레이션, 디지털 스레드	센서 및 Actuator 에서 수집되는 데이터 기반 모델링을 통해 물리적인 사물을 가상공간에 동일하게 표현하여 모니터링, 제어가 가능하도록 하는 기술

- IoT 를 넘어선 디지털 트윈의 진화로 DTO(Digital Twin of an Organization) 구현

3. 디지털 트윈(Digital Twin)의 활용사례 및 전망

구분	세부항목	설명
활용사례	- 스마트팩토리 - 스마트 시티 - 항공기 엔진 - 선박 모델링	- 사고위험 분석 및 핵심부품 수명주기 관리 - 도시건설 이전에 디지털 트윈을 통한 모델링 - 설계부터 3D 모델링을 통해 고가의 시제품없이 테스트 가능
전망	- IoT 와 융합 - 비용절감 - 생산성 향상	- 현실세계의 정보를 IoT 디바이스를 통해 수집하여 모델링 데이터로 활용 - 지속적인 시뮬레이션 및 실시간 데이터 분석을 통해 고도화된 모델링 가능

- 생산라인에 대한 고장 예측, CAPEX/OPEX 절감, 운영 효율성 향상이 예상되며, 4 차 산업혁명 핵심 기술로 사용 중

"끝"

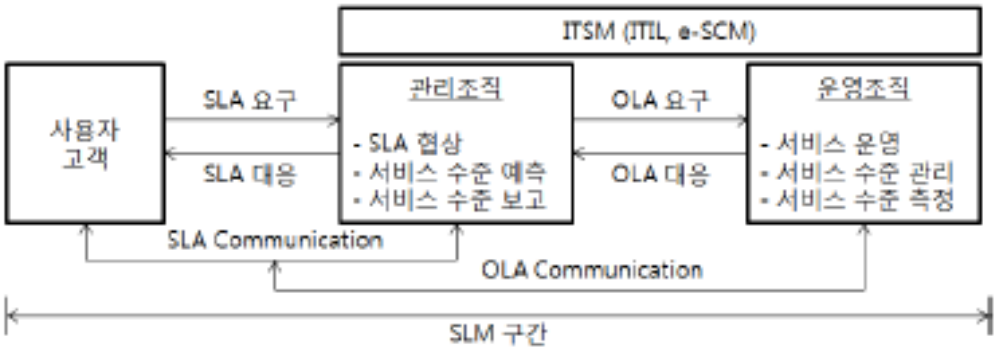
5	SLM 프레임워크
문제	SLM(Service Level Management) 프레임워크의 구성요소
도메인	IT 경영
정의	SLM: SLA 에서 정의한 서비스에 대한 정확한 성과를 측정/평가하고 그 결과를 바탕으로 더 나은 서비스가 이루어지도록 개선방안을 마련하는 일련의 과정
키워드	Service Catalog, SLA, OLA, Quality Plan, Service Report, SLM 엔진
출제의도분석	기업의 전반적 IT 서비스 수준 관리를 위한 전반적 프레임워크 기본 개념 확인
답안작성 전략	SLM 프레임워크 구성요소 설명 및 SLA 지표
참고문헌	기술사 서브노트
풀이 기술사님	표기수 PE (제 117 회 정보관리기술사 / kisu.pyo@gmail.com)

1. SLA 통한 서비스 수준 관리 체계, SLM 의 정의

- IT 서비스 조직에서 사용자의 관점으로 서비스 요구사항을 파악하고, 서비스 수준 개선을 위한 우선순위를 판단하기 위한 도구 및 체계
- SLA 에서 정의한 서비스에 대한 정확한 성과를 측정/평가하고 그 결과를 바탕으로 더 나은 서비스가 이루어지도록 개선방안을 마련하는 일련의 과정

2. SLM 프레임워크의 구성도 및 구성요소

가. SLM 프레임워크의 구성도



- SLA 를 통해 서비스 수준 지표 선정 및 고객에게 일정 수준 이상의 서비스 제공

나. SLM 프레임워크의 구성요소

구성요소	핵심요소	설명
Service Catalog	서비스 내역 목록화	- 고객에게 제공되는 서비스 전체 목록
SLA	서비스 수준 지표 정의	- Service Level Agreement - IT 서비스를 제공하는 업체와 사용하는 업체 간의 서비스 계약서
OLA	세부 운영 관련 협약	- Operation Level Agreement - 내부 조직 간 의사소통 관리 효율성을 위해 서비스 공급자 내부 부서간 협약서
Service Quality Plan	품질 관리 계획	- 합의된 서비스 수준의 보장을 위해 필요한 내용을 기술한 내부 계획

Service Report	서비스 수준 위반 검토	- 주기적인 서비스 수준 위반 여부 검토
SLM 엔진	Reporting, Monitoring	- 서비스 수준 관리 과정에서 관리 지표별 측정치 산출 - 보고서 작성 자동화, 실시간 정보 서비스 모니터링

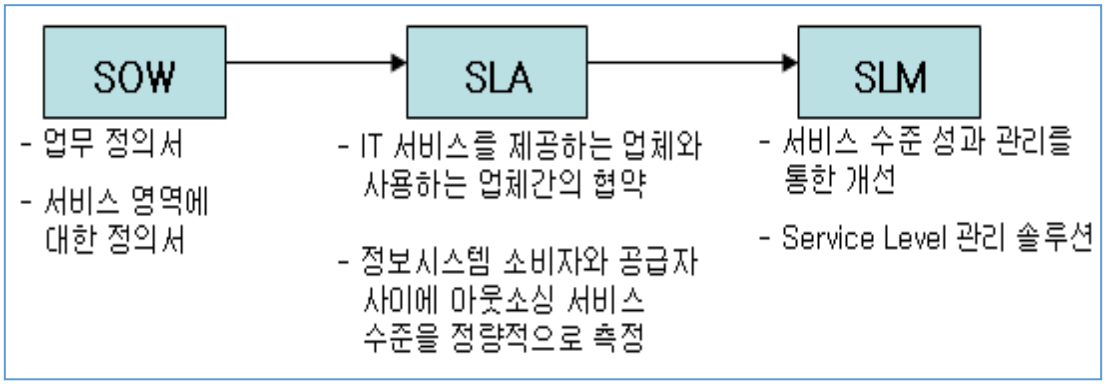
- 산정된 SLA 지표 기반의 서비스 수준 지속적 관리

3. SLA 지표 및 측정방법

구분	측정지표	측정방법(예)
하드웨어	서비스 가동률(%)	서비스 가동률(%)=(1-장애시간/서비스시간)*100
	동일장애발생률(%)	(동일 장애 발생건수 / 총 장애발생건수)*100
소프트웨어	장애 및 오류건수	장애건수 10 건 이하
	SR 적기 처리율(%)	요청한 완료일 이내에 서비스를 제공해준 비율
네트워크	네트워크 가동률(%)	(1-장애시간/네트워크 가동시간)*100
	네트워크 장애건수	장애건수 3 건 이하

- SLA 지표는 평가지표와 관리지표로 이원화하여 관리

[참고] SoW, SLA, SLM 의 관계



"끝"

6	디지털 윤리와 개인정보보호
문제	디지털 윤리(Digital Ethics)와 개인정보보호(Privacy)
도메인	보안
정의	- 디지털 윤리 : 디지털 정보를 획득, 처리, 활용하는 과정에서 지켜야 할 프라이버시, 정보 정확성, 정보소유(ownership), 정보접근가능성 등의 규범 - 개인정보보호 : 자신의 개인정보를 수집, 저장, 분석, 제공, 활용 및 파기 등을 결정할 수 있는 권리
키워드	프라이버시, 정확성, 정보소유, 정보접근가능성, '준수'에서 '옳은 일 하는가' 변경, 자발적/적극적
출제의도분석	가트너에서 선정된 토픽이자 빅데이터 분석과 5G 로 인한 초연결 사회에서 부각되는 디지털 윤리와 개인정보보호에 대한 개념 질문
답안작성 전략	윤리와 개인정보보호의 관계를 도식화 및 중요성/필요성을 부각하여 차별화
참고문헌	https://m.blog.naver.com/PostView.nhn?blogId=lugenzhe&logNo=220301249180&proxyReferer=https%3A%2F%2Fwww.google.co.kr%2F 빅데이터 동향과 이슈, NIA (2015.2)
풀이 기술사님	표기수 PE (제 117 회 정보관리기술사 / kisu.pyo@gmail.com)

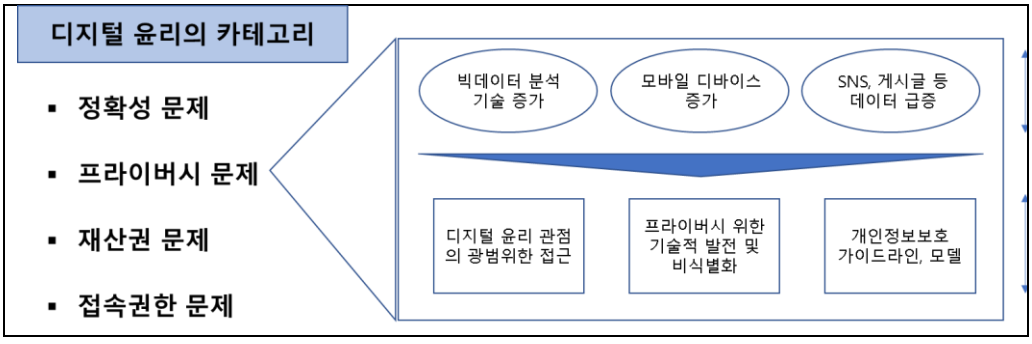
1. 디지털 윤리와 개인정보보호의 개념

디지털 윤리	- 디지털 정보를 획득, 처리, 활용하는 과정에서 지켜야 할 프라이버시, 정보 정확성, 정보소유(ownership), 정보접근가능성 등의 규범
개인정보보호	- 자신의 개인정보를 수집, 저장, 분석, 제공, 활용 및 파기 등을 결정할 수 있는 권리

- 빅데이터 기술의 발전 및 시장 확대로 기업이 수집·보유한 데이터 활용에 대한 윤리적 문제와 데이터 관리에 대한 보안 기술요건에 대한 논의 등 다양한 프라이버시 이슈가 제기
- 개인정보 : 살아있는 개인에 관한 정보로서 성명, 주민등록번호, 영상 등 개인을 알아볼 수 있는 정보 (해당 정보로만 개인을 파악할 수 없더라도 다른 정보와 쉽게 결합하여 파악 가능한 정보를 포함)

2. 디지털 윤리와 개인정보보호의 관계 및 프라이버시 위협과 보호

가. 디지털 윤리와 개인정보보호의 관계



- 빅데이터 산업 활성화에 따라 개인정보보호 및 디지털 윤리에 대한 이슈 부각

나. 프라이버시 위협과 보호

구분	핵심 요소	설명
프라이버시 위협 요소	자료 집합소	- 공개 데이터와 비공개 데이터를 수집, 프로필을 생성하기 위해 데이터를 통합하는 회사
	디지털 프로필	- 개인 관련 정보 및 습관에 대한 정보 집합
	프로파일링	- 개인에 대한 디지털 프로필 생성 행위
	전자 감시	- 개인의 활동을 온라인, 오프라인으로 추적하는 행위
	DB 내 개인정보	- 기업, 은행, 정부기관 등 DB 에 저장된 개인정보 - 개인정보 저장 위치, 정확성, 변경가능성, 보유기간, 공개 조건, 활용 영역 등에 대한 명시 필요
	SNS 게시글	- SNS 상의 연락처, 게시글 및 인적 네트워크 구조
프라이버시 보호	프라이버시 정책 가이드라인	- 데이터 수집 : 합법적 경영 목적을 수행하기 위해 적정한 데이터 수집 및 개인의 동의 필요 - 데이터 정확성 : DB 입력 전에 정확성 입증 및 현재의 상태로 유지 필요 - 데이터 기밀성 : 비합법적인 공개의 금지를 보장할 수 있도록 관리적/물리적/기술적 보호 필요
	Opt-In / Out 모델	- Opt-In 모델 : 고객이 수집에 동의하는 경우에만 수집 가능한 모델 - Opt-Out 모델 : 고객이 수집을 거부할 경우에 수집을 금지하는 모델
	공동 데이터 마이닝	- 기존의 중앙 집중식 대형 DW 에 데이터 수집 및 마이닝 하는 경우 발생하는 개인정보 침해 문제 방지 - 각 Data Set 을 노출하지 않고 글로벌 데이터 마이닝 결과 도출 가능 기술
	ZKPK 프로토콜 활용 생체 인증	- 지각 간섭기술, 분류기술 및 제로지식 증명 프로토콜(ZKPK)을 활용하여, 분산 환경 하에 민감함 생체 정보를 강력하게 보호하는 기술

- ZKPK : Zero-Knowledge Proof of Knowledge

3. 개인정보보호에서 디지털 윤리로의 전환

개인정보보호 (Privacy)	디지털 윤리
▪ '우리는 준수하고 있는가 '	▪ '우리는 옳은 일을 하고 있는가 '
▪ 소극적 수행	▪ 적극적 수행
▪ 강제적 참여	▪ 자발적 참여

- 개인정보보호에 대한 모든 논의는 디지털 윤리와 고객, 구성원 및 직원들의 신뢰에 대한 광범위한 주제에 근거해야 함 "끝"

7	선형회귀모형 추론의 가정
문제	선형회귀모형의 추론에 대한 가정 4 가지
도메인	통계
정의	선형회귀 : 종속변수 y 와 한 개 이상의 독립 변수 x 와의 선형 상관 관계를 모델링하는 기법. (독립변수 개수에 따라 단순/다중 선형 회귀 분석 구분)
키워드	선형성, 독립성, 정규성, 등분산성
출제의도분석	통계 분석 중 대표적 방식인 선형회귀분석의 수식 뿐만 아니라 분석/해석이 가능하게 되는 가정까지 파악하고 있는지를 질문
답안작성 전략	선형회귀모형의 산술식과 4 가지 가정을 정확하게 기입 및 가정이 만족/불만족 되었을 때의 산점도나 잔차 분포를 함께 설명. 연관 토픽인 다중공선성 문제 및 해결 방안을 3 단락에 기술
참고문헌	http://mysas.co.kr/sas_tiptech/i_eg.asp?b_no=2442&cmd=content&bd_no=28 https://kkokkilkon.tistory.com/175 http://www.sigmapress.co.kr/shop/shop_image/g55612_1413878468.pdf https://blog.naver.com/kewnew/220276636749, 위키피디아
풀이 기술사님	표기수 PE (제 117 회 정보관리기술사 / kisu.pyo@gmail.com)

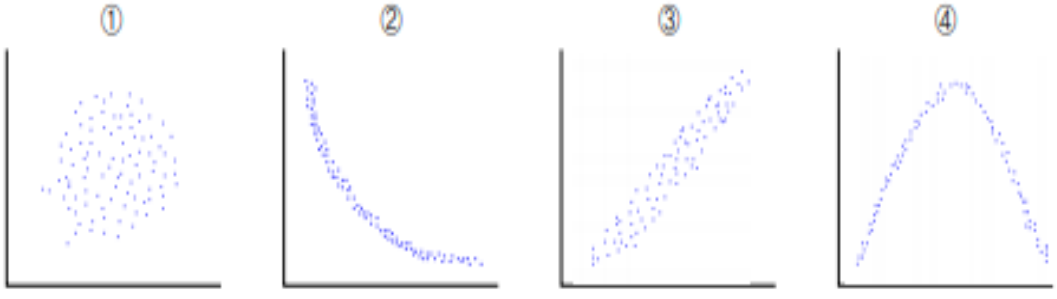
1. 선형회귀모형 추론의 가정 4 가지

구분	가정	설명
모형에 대한 가정	선형성	- 예측하고자 하는 종속변수 y 와 독립변수 x 간에 선형성을 만족한다고 가정
오차에 대한 가정	독립성	- 독립변수 x 간에 상관관계가 없음을 가정
	정규성	- 잔차는 정규분포를 따른다고 가정
	등분산성	- 잔차가 특정한 패턴 없이 고르게 분포한다고 가정

- 오차에 대한 가정의 경우 잔차 분석을 통해 검증
($Y_i = \alpha + \beta X_i + \varepsilon_i$ 에서 ε_i 가 잔차)

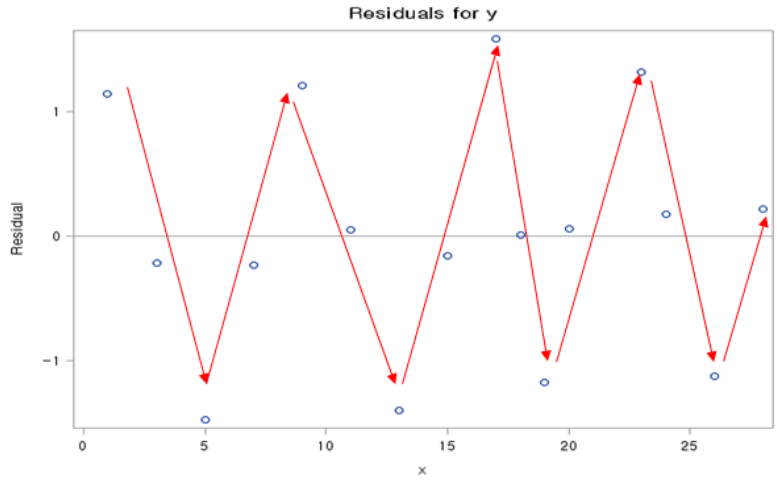
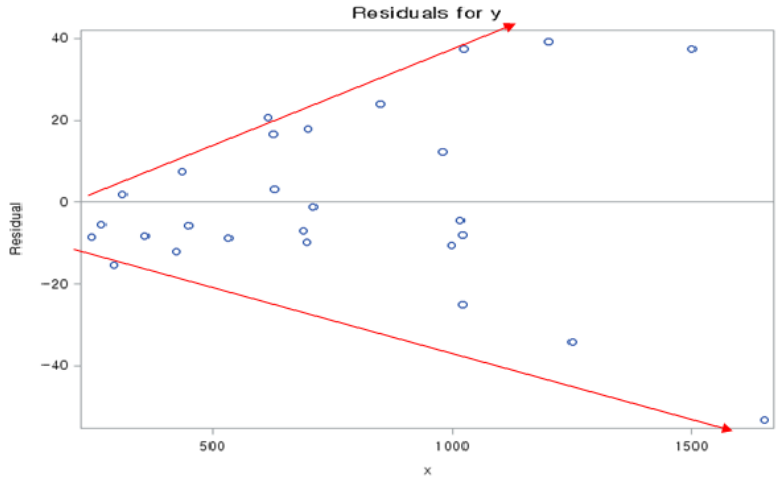
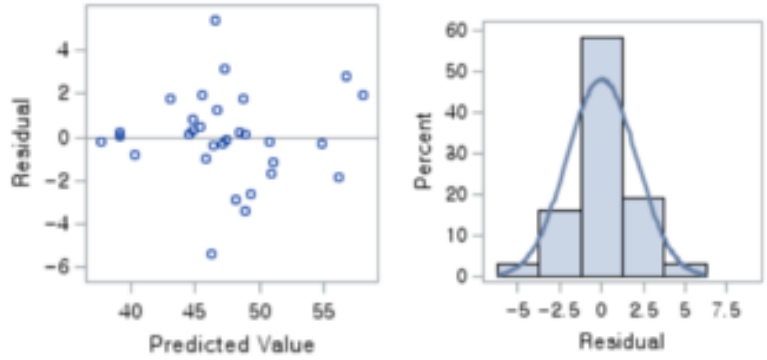
2. 선형회귀모형 추론의 가정 검증 방법

가. 산점도(Scatter Plot) 활용한 선형성 검증



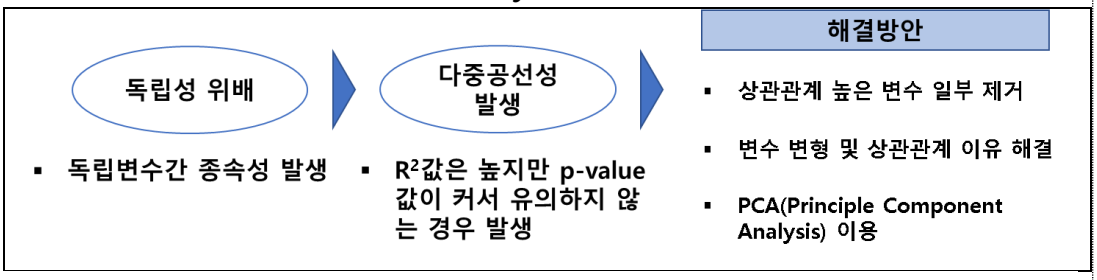
- 두 변수 일 때, 독립변수 x 와 종속변수 y 간의 산점도에서 변수 간 직선 관계가 보임 (③ 해당)
- x 와 y 간의 상관 계수에 대한 p-value 값이 유의수준보다 작게 나와야 함

나. 잔차 분석을 통한 독립성, 정규성, 등분산성 검증

가정	설명
독립성	 - 독립성 : 독립변수 간의 종속 관계가 없어야 함 - 위와 같이 잔차 분포가 일정한 패턴을 보이는 경우 독립성이 위배됨
등분산성	 - x 값이 변함에 따라 잔차의 분산이 일정해야 함 - 위와 같이 x 값이 증가함에 따라 잔차의 분산이 변하면 등분산성이 위배됨
정규성	 - 잔차의 분포가 평균 0 인 정규분포를 따라야 함 - 위와 같이 잔차의 평균이 0 인 정규분포를 따를 경우 정규성 만족

Notes

3. 독립성 위배, 다중공선성(Multicollinearity) 해결 방안



- 독립변수들 간에 강한 상관관계가 나타나는 다중공선성 발생시, 변수 변경 및 PCA 사용하여 해결

"끝"

8	모바일 엣지 컴퓨팅
문제	모바일 엣지 컴퓨팅(Mobile Edge Computing)
도메인	디지털 서비스
정의	초지연 서비스와 부하분산 및 품질 향상 위해 통신 서비스를 이용하려는 사용자와 가까운 곳에 서버를 위치시켜 데이터를 처리하는 기술
키워드	빅데이터, 부하분산, 지연시간 감소, MEC 서버
출제의도분석	5G 의 저지연성 요구 충족을 위한 MEC 기술 및 가트너에 선정된 엣지 컴퓨팅
답안작성 전략	MEC 기술 요소와 최신 적용 사항, 기술적 이슈 기재로 답안 차별화
참고문헌	KPC 114 회 기출풀이, 동기회 114 회 기출풀이, 서브노트 모바일 Edge 컴퓨팅 기술 동향, 윤찬현 5G 를 위한 MEC 기술동향, ETRI
풀이 기술사님	표기수 PE (제 117 회 정보관리기술사 / kisu.pyo@gmail.com)

1. 모바일 엣지 컴퓨팅의 개념

가. 모바일 엣지 컴퓨팅의 정의

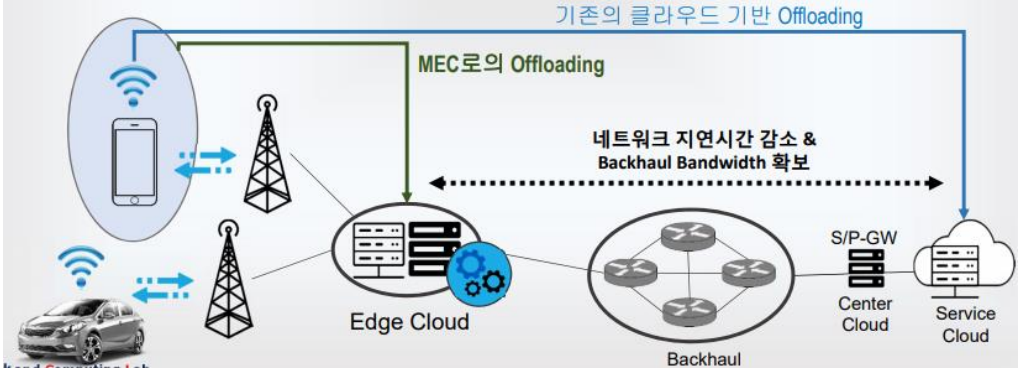
- 초저지연 서비스와 부하분산 및 품질 향상 위해 통신 서비스를 이용하려는 사용자와 가까운 곳에 서버를 위치시켜 데이터를 처리하는 기술

나. 모바일 엣지 컴퓨팅의 특징

특징	설명
부하 분산	- 연산의 분산으로 중앙 프로세싱의 자원절약 및 부하감소
탄력성 제공	- 중앙 시스템 문제시에도 엣지에서 일부 서비스 제공 가능

2. 모바일 엣지 컴퓨팅의 구조 및 기술 요소

가. 모바일 엣지 컴퓨팅의 구조



- 5G 서비스로 인한 초저지연 서비스 부상과 함께 MEC 기술 중요성 증가

나. 모바일 엣지 컴퓨팅의 기술 요소

기술	핵심요소	설명
클라우드 및 가상화 기술	자원의 On-Demand 서비스	- 하나의 플랫폼 상에 복수의 가상머신들을 활용하여 자원 효율화하는 MEC 핵심 기술

대용량 표준 서버 기술	대용량 IT 하드웨어 자원 제공	- 패킷 처리와 같은 막대한 하드웨어 자원을 사용하는 프로그램과 서비스 지원
응용 및 서비스 생태계	API, 사용자 친화적 프로그래밍 모델/도구	- 생태계 조성을 위한 지원 프로그램 - 서로 다른 벤더의 플랫폼 적용을 위한 표준 지원

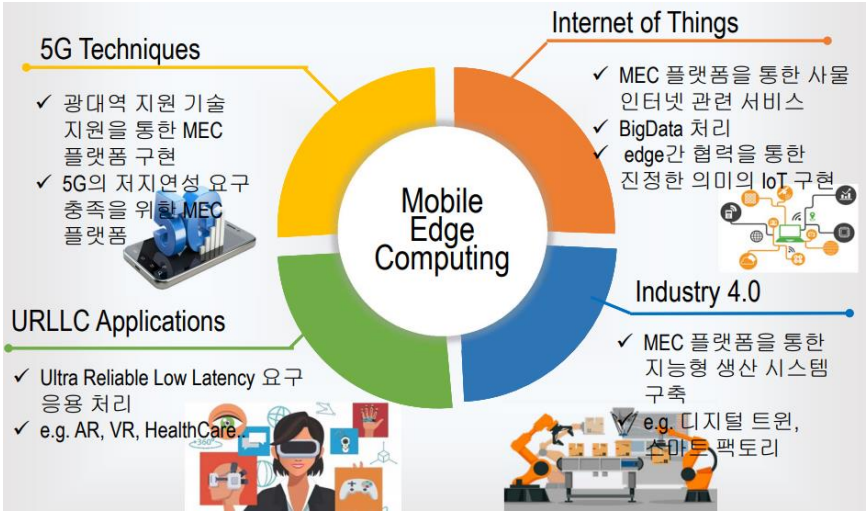
- 5G 네트워크 환경 적용을 위해 이동성, 보안, 상황인지 기술에 대한 해결 필요

3. 모바일 엣지 컴퓨팅의 특징별 적용사항

특징	적용	설명
안정성	자율주행 자동차	자율주행차 시장은 순간의 네트워크 지연이나 데이터 전송 오류가 치명적인 사고로 이어질 수 있음
	항공엔진, 드론	산업기계 자체가 중앙 서버에서 멀리 떨어진 곳에 위치해 있어 중앙서버와의 연결이 어려움
즉시성	증강현실	사람의 시청각 반응 능력은 매우 예민하기 때문에 불과 몇백 ms 차이만으로도 가상현실 몰임감에 영향을 미칠 수 있음
	가상현실	
	생체(음성,안면)인식	
효율성	스마트 팩토리	제조 기업의 스마트 팩토리에서는 대규모의 센서 데이터가 발생하며 이의 효율적인 처리가 필요함

"끝"

[참고]



9	블록체인
문제	금융권에서 블록체인 시스템을 도입할 시 고려해야 할 정보보안 이슈
도메인	디지털서비스
정의	-
키워드	키 관리, 거래 검증 및 합의, 참여자 권한관리, 블록체인 SW / 서비스 보안
출제의도분석	블록체인의 실무 환경 적용시의 발생 가능한 보안이슈를 종합적으로 질문
답안작성 전략	블록체인 거래 발생시의 동작 절차에 따른 보안이슈 및 대응방안 작성
참고문헌	블록체인 기술과 보안 고려사항, 금융보안원
풀이 기술사님	표기수 PE (제 117 회 정보관리기술사 / kisu.pyo@gmail.com)

1. 금융권에서 블록체인 시스템 도입 시 고려할 정보보안 이슈

분류	보안위협	설명
키 관리	키 도난 및 분실	공격자에게 키를 도난 당하거나 분실된 키가 악용될 경우 자산 및 기밀거래 메시지 유출
	취약한 키 생성	취약한 키 생성 알고리즘으로 인해 키 재생성 공격이 가능할 경우 자산 및 기밀거래 메시지가 유출 가능
거래 검증 및 합의	합의 가로채기	참여자 중 과반수(또는 운영주체)를 장악하여 블록체인의 합의 과정을 조작
	사이드 체인 내 비정상 거래 발생	메인 체인에서 유효하지 않은 자산이 사이드 체인에서 거래 가능
참여자 권한관리	개인정보 침해	거래정보에 대한 참여자의 접근권한 관리 부족시 개인정보 침해 가능
	권한 오남용	참여자의 내·외부 권한관리 부족시 금융회사 및 내부직원에 의한 보안사고 등 발생 가능
블록체인 S/W 보안	블록체인 S/W 취약점	블록체인 S/W 에 보안 취약점이 존재할 경우 키 도난, 합의 조작, DDoS 공격 등에 악용가능
	스마트 컨트랙트 취약점	스마트 컨트랙트에 취약점이 존재할 경우 자산 유출, 개인정보 침해, DDoS 공격 등에 악용가능
서비스 보안	분산 서비스 거부 공격	다수 참여자가 악성코드 등을 통해 공격자에게 장악될 경우 대량의 스팸거래를 발생 가능하며 이로 인해 블록체인 서비스가 중단 가능
	가용성 저하	블록체인의 처리속도 한계, 거래정보 급증으로 인해 추가 서비스 개발 및 확대 제한 등의 가용성이 저하
	비정상거래 탐지 불가	비정상거래에 대한 사전 탐지 및 차단 기술이 부족하여 사기거래, 자금세탁, 이중지불 등의 거래가 발생 가능
	상호운용성 미제공	블록체인 간 자산교환, 기능 확장 등 연계 필요시 책임주체 및 표준규격이 명확하지 않아

		예상치 못한 보안위협 발생 가능

- 발생가능한 각 보안위협에 대한 대응방안 필요

2. 금융권에서 블록체인 사용의 보안위협에 대한 대응 방안

보안위협	대응 방안	설명
키 도난 및 분실	보안 가이드 준수 키 복구 기능 적용 다중 서명 용도별 키 할당 암호화 및 사용 후 즉시 삭제	- 공격자에 의해 키가 유출되지 않도록 키를 안전하게 보관하고 키 도난 및 분실에 대응
취약한 키 생성	안전한 키 생성 안전성 검증	- 공격자가 키를 재생성하지 못하도록 키를 안전한 방식으로 생성 및 검증
합의 가로채기	비정상 참여자 모니터링 수수료 부과 및 거래 처리량 제한 참여자 검증	- 내외부 공격자에게 장악된 노드로 인해 거래 유효성이 조작되지 않도록 모니터링 및 차단
사이드 체인 내 비정상 거래 발생	합의 통합	- 메인 체인의 유효하지 않은 자산이 사이드 체인으로 이전되어 정상 거래되는 것을 차단
개인정보 침해	채널 구성 거래정보 삭제 참여자 식별 및 접근통제 거래 암호화	- 블록체인에서 개인정보 침해가 발생하지 않도록 거래와 무관한 제 3 자의 접근을 통제
권한 오남용	스마트 컨트랙트 기반 통제 내부직원 통제	- 금융회사 및 내부직원이 허가되지 않은 거래 및 서비스에 참여하는 것을 차단
블록체인 S/W 취약점	코드 검토 보안 테스트 안전한 개발 방법론	- 블록체인 SW 에 존재할 수 있는 보안 취약점을 악용한 해킹공격 차단
스마트 컨트랙트 취약점	코드 검토 및 악성코드 탐지 검증된 코드 사용	- 스마트 컨트랙트 코드에 존재할 수 있는 보안 취약점을 악용한 비정상거래 등 악성행위를 차단
분산 서비스 거부 공격	스팸거래 차단 거래요청 건수 제한 거래 허용 참여자 관리	- 대량 스팸거래 요청 등의 DDoS 공격으로 인해 블록체인 서비스가 중단되지 않도록 대응
가용성 저하	유효성 검증 참여자 제한 선택적인 거래정보 저장	- 거래 처리속도 저하와 전체 거래정보의 크기 증가 등으로 인한 가용성 저하 문제를 개선
비정상거래	거래 허용 참여자 관리	- 블록체인에서는 자금세탁거래 등

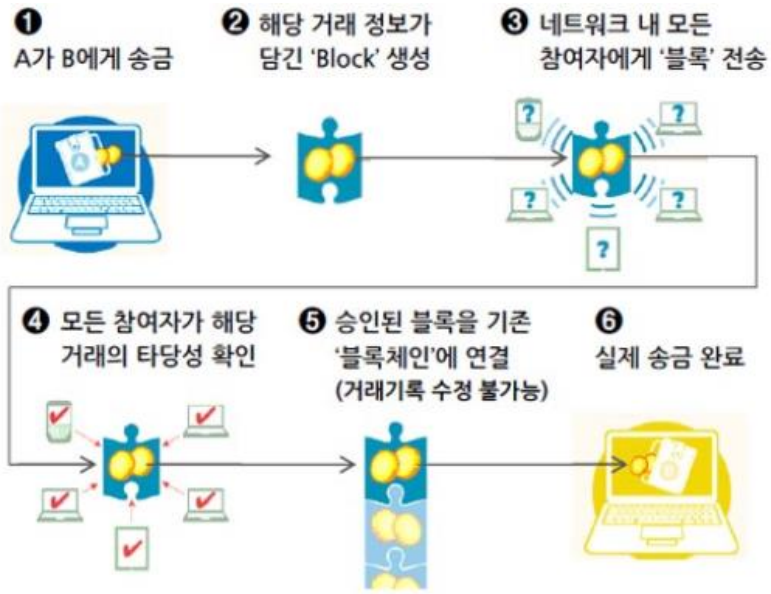
탐지 불가		비정상 거래가 발생하더라도 거래 취소 등의 대응이 어려우므로 사전에 탐지 및 차단
상호운용성 미제공	Pegged 사이드 체인 표준규격 개발	- 블록체인 간의 신뢰 가능한 자산이전 기술 및 표준규격을 개발하여 안전한 서비스 연계가 가능하도록 상호운용성 제공

- 현재 연구되고 있는 기술과 관련된 보안 이슈도 대응체계 마련 필요

3. 보안기술 연구에 따른 금융권 블록체인 정보보안 고려사항

구분	보안 기술	고려사항
최신 연구동향 검토	양자컴퓨팅	- 양자컴퓨팅에도 안전한 키 생성기술 검토
	거래정보 삭제 기술	- 보관기한 만료된 개인정보의 삭제, 비정상거래 취소 등 검토
	보안 표준	- 블록체인 서비스 제공 및 블록체인간 연계 시 안전성 제공을 위한 보안 표준 개발에 대응
평가 기준 마련	평가 항목 및 기준 개발	- 제시된 보안 위협 및 대응방안을 기반으로 금융권 블록체인 시스템에 대한 평가 항목 도출 및 세부 평가기준 개발

[참고] 금융권에서 블록체인 시스템의 동작 프로세스



"끝"

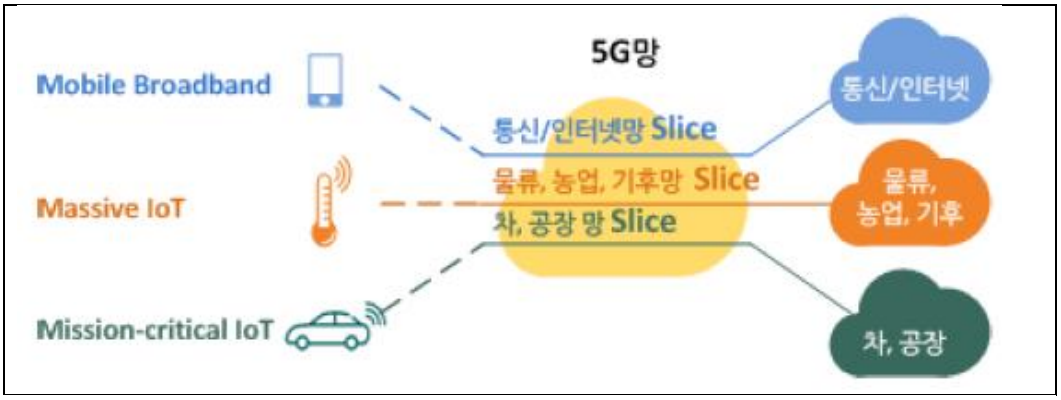
10	네트워크 슬라이싱(Network Slicing)
문제	5G 네트워크 슬라이싱(Network Slicing)
도메인	네트워크
정의	논리적으로 분리된 네트워크를 만들어 서로 다른 특성을 갖는 다양한 서비스들에 제공하는 5G 네트워크 핵심 기술
키워드	SDN, NFV
출제의도분석	5G 의 핵심 기술이자 SDN, NFV 의 기술요소 평가 가능
답안작성 전략	NW Slicing 의 정확한 개념, 기술 요소, 실무적 구성 방법 기재로 차별화
참고문헌	KPC 113 회 컴퓨터시스템응용기술사 기출문제 풀이집, 서브노트
풀이 기술사님	표기수 PE (제 117 회 정보관리기술사 / kisu.pyo@gmail.com)

1. 네트워크 슬라이싱(Network Slicing)의 정의

- 물리적으로 하나의 네트워크를 통해 Device, Access, Transport, Core 를 포함하여 End-to-End 로 논리적으로 분리된 네트워크를 만들어 서로 다른 특성을 갖는 다양한 서비스들에 제공하는 5G 네트워크 핵심 기술

2. 네트워크 슬라이싱의 개념도 및 핵심 기술

가. 네트워크 슬라이싱의 개념도



- 하나의 물리적 망을 논리적 망으로 분할하여(Slicing) 각 슬라이스마다 다른 Service 를 제공

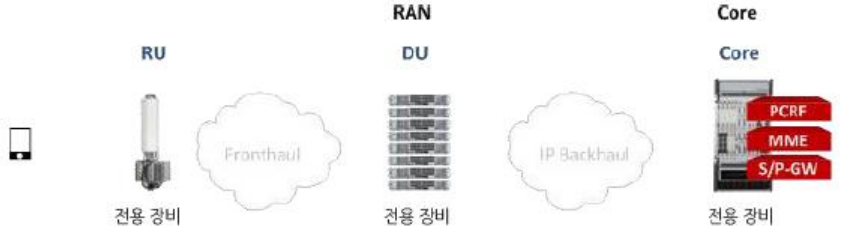
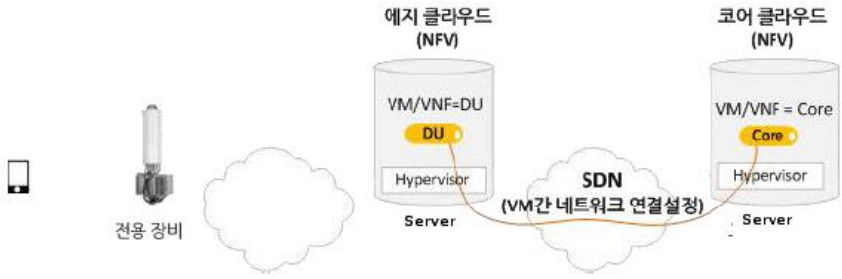
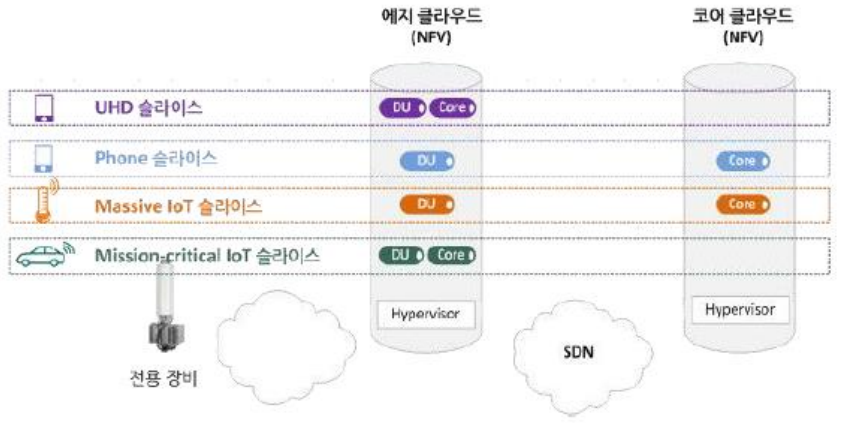
나. 네트워크 슬라이싱(Network Slicing)의 핵심 기술

기술 영역	세부 기술	설명
SDN	Application	- Network OS 상에서 사용자 서비스를 지원하는 프로그램
	Network OS	- 전체 망에 대한 Global View 를 갖고 전체 망을 제어 - Openflow Controller 는 Openflow protocol 을 통해 Data plane 에 있는 네트워크 장비의 Flow Table 제어
	Data Plane	- 단순 패킷 포워딩, 스위칭 기능만 구현 - 기존 스위치 또는 Layer2(스위칭), Layer3(라우팅) 기능 지원 스위치에 OpenFlow 의 기능을 추가
NFV	NFVI	- 컴퓨팅, 저장소, 네트워크 기능을 지원하는 물리적 하드웨어 지원, 가상화 지원 기능 및 VNF 실행을 지원하는 기능 제공
	NFVs	- 여러 응용 프로그램을 지원하기 위한 SW 로 개발된 네트워크 기능들의 집합

	MANO	- 물리적 그리고 소프트웨어적 자원관리, 전달, VNF 관리 기능 제공
	E2E Networking	- NFV 인프라에서 제공하는 여러 VNF 들을 실행 로직에 맞게 연결한 포워딩 그래프(NFV 서비스 네트워크 체인 기반)

- 주요 기술인 SDN 과 NFV 를 이용하여 네트워크 슬라이싱 구성

3. SDN 과 NFV 를 이용한 네트워크 슬라이싱(Network Slicing) 구성

단계	설명
현재망 파악	 현재의 이동통신 망은 단말은 폰이고, RAN(DU, RU)과 Core 가 RAN 벤더의 전용 Network 장비로 구성
Virtual Network 생성	 1) Network 장비가 아닌 가상화된 Server 에 Network Function SW 를 Virtual Machine 에 탑재(NFV 구성) 2) RAN 은 Edge Cloud 로 되고, Core 는 Core Cloud 로 구성 3) Edge Cloud 와 Core Cloud 에 있는 VN 들 간 Network 연결을 SDN 으로 구성
Slicing	 Service 별로 Slicing 하여 Network Slicing 구성

"끝"

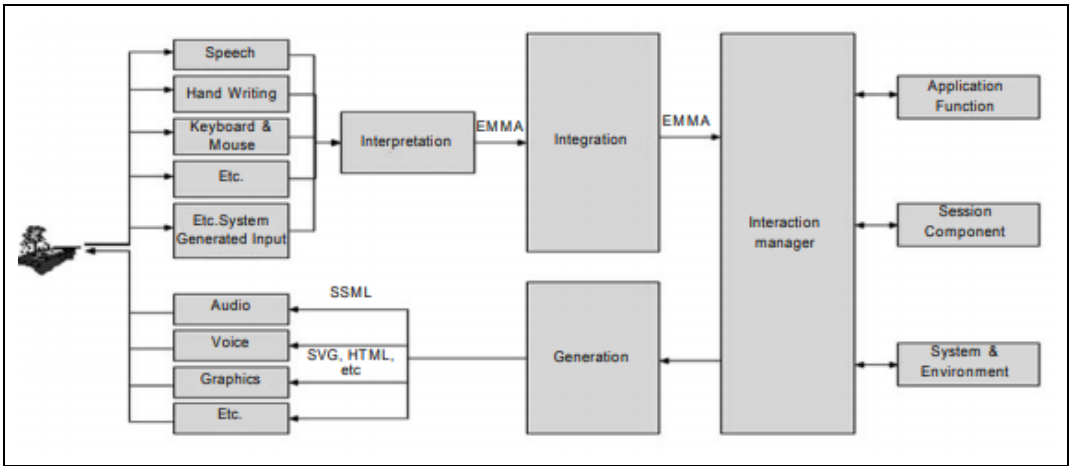
11	멀티 모달 인터페이스
문제	멀티 모달 인터페이스(Multimodal Interface)의 구성요소
도메인	디지털 서비스
정의	전통적인 키보드/마우스 등의 입력 장치뿐만 아니라 다양한 입력 요소를 통하여 I/F 하는 인간 중심형 기술
키워드	입력, 출력, 인터렉션/세션 관리, 시스템환경 관리
출제의도분석	다양한 입력 신호를 처리하는 기술의 상세 구성 요소 질문
답안작성 전략	여러 입력 신호를 받아 처리하는 상세 구성요소 기술
참고문헌	멀티모달 상황인지 인터페이스의 최신 기술동향, 안세열 외 3 인 http://www.tta.or.kr/data/weekly_view.jsp?news_id=850 KPC 101 회 정보관리 기술사 기출문제풀이집
풀이 기술사님	표기수 PE (제 117 회 정보관리기술사 / kisu.pyo@gmail.com)

1. 멀티모달 인터페이스의 개념

- 전통적인 키보드/마우스 등의 입력 장치 뿐만 아니라 다양한 입력 요소를 통하여 I/F 하는 인간 중심형 기술

2. 멀티모달 인터페이스의 구성도 및 구성요소

가. 멀티모달 인터페이스의 구성도



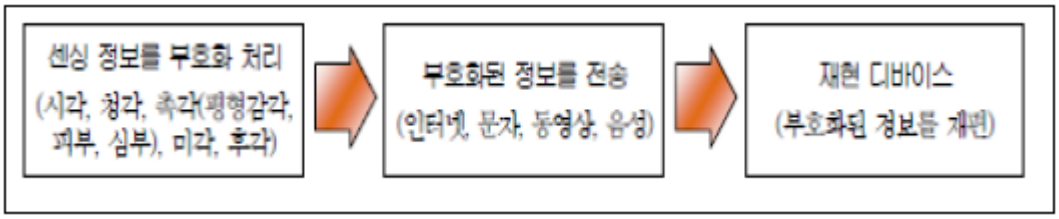
- 재공학과 역공학의 활용 통해 생애주기를 연장 및 효율성 높은 운영/유지보수가 가능

나. 멀티모달 인터페이스의 구성요소

구성요소	핵심 역할	설명
인식/해석/통합 모듈	Multi Modal Input 처리	다양한 입력 요소로부터 인식하여 해당 I/F 가능한 형태로 변환
생성/랜더링 모듈	Multi Modal Output 처리	원하는 형태의 결과물을 해당 스펙에 맞게 변환하여 출력
Interaction Management	인터랙션 관리	입력 요소로부터 얻은 정보를 이용하여 실제 응용서비스 실행을 수행한 후 해당 결과를 출력 요소에 제공

Session Management	세션 관리	다양한 단말 사용시 세션이 연속성을 유지하도록 멀티모달 응용서비스와 지속적인 연결 및 다양한 단말 출력 위한 싱크 기능
시스템 환경 관리	환경 관리	주변 상황에 따라 다양한 단말을 변화할 수 있도록 시스템 환경을 표현
Application Service Module	응용서비스 실행요소	시스템의 구현상에서 서비스가 가능한 형태로의 실행을 위한 기능 제공
상황인지 및 개인화 엔진	사용자 의도 파악	여러 입력 정보가 갖는 부분 정보를 통합하여 사용자 의도 파악
SMMD (Single Media Multi Device)	의사소통 효율성 제고	다양한 형태의 입출력 수단 통한 의사소통 효율성 제고
EMMA (Extensible Multi Modal Annotation)	입력 요소와 인터랙션 관리기 간의 표준 언어	사용자가 키보드, 필기체 및 음성을 사용할 때 그것을 처리한 결과를 표현해 주는 마크업 언어

3. 멀티모달 정보 전달 및 처리 방법



- 순공학으로 생산된 시스템에 대해 역공학과 재공학을 통해 유지보수성 향상 가능

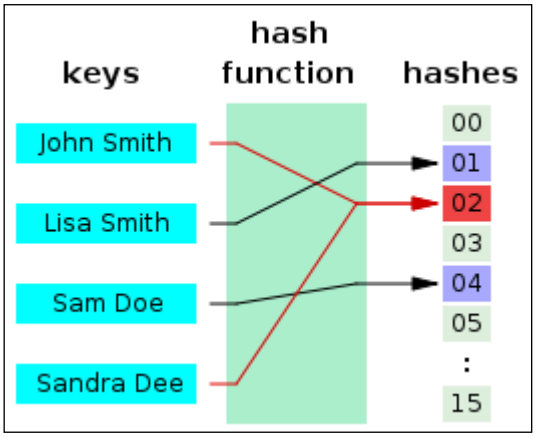
[참고] 멀티모달 인터페이스의 종류

종류		설명	기술
기본	음성 I/F	- 음성입력 : 음성으로 기계를 명령 음성입력 기능, - 음성출력 : 기계의 출력을 음성으로 들려주는 기능	음성인식기술 음성합성기술
	키보드 I/F	키보드를 통한 인식 기술	키보드 기술
	잉크 I/F	펜으로 글을 쓰거나, 그림으로 표시하는 기능	펜 필기체인식 기술
확장	NUI	인공적인 제어장치 없이 사람의 감각, 행동, 인지 능력을 통해 직접 교감하는 방식	디지털기기제어 기술
	TUI	실세계의 사물을 이용하여 디지털 정보와 자연스러운 상호작용 구현	제함경 인터페이스 기술
	Wearable HCI	작용감, 항시성, 안정성, 사회성이 반영된 착용형 컴퓨팅에 사용자와 컴퓨터간 Interaction 통한 기능	HMD, 포스쳐, 모션, 아이트래킹
	감성 유저 인터페이스	사용자의 시각, 청각, 촉각을 자극하여 사용자가 모바일 가전기기와 교감할 수 있는 기능	패더스, 컴저트봇&웨이트봇
	HRI	로봇이 인간의 의도를 판단하고 적합 반응과 행동수행기술	얼굴인식,표정,제스처인식,TTS
	음성인식	마이크나 전화를 통하여 얻어진 음향학적 신호를 단어나 단어의 집합 또는 문장으로 변환 처리하는 기술	끝점추출, 특징추출, 잡음처리, 발화검증

"끝"

12	해시값, 해시함수 구분, 종류, 용도
문제	해시값(Hash Value)과 해시함수의 구분, 종류, 용도
도메인	보안
정의	임의 길이 메시지를 고정길이 메시지(Message digest)로 변환 시 사용하는 단방향 함수인 해시 함수의 결과값
키워드	MAC, MDC, MD5, SHA
출제의도분석	빈출되는 해시 함수에 대한 기본 개념 확인
답안작성 전략	정확한 개념과 종류 기술 및 용도에 대한 상세 기술로 차별화
참고문헌	https://middleware.tistory.com/entry/%ED%95%B4%EC%8B%9C-%ED%95%A8%EC%88%98Hash-Function, 서브노트
풀이 기술사님	표기수 PE (제 117 회 정보관리기술사 / kisu.pyo@gmail.com)

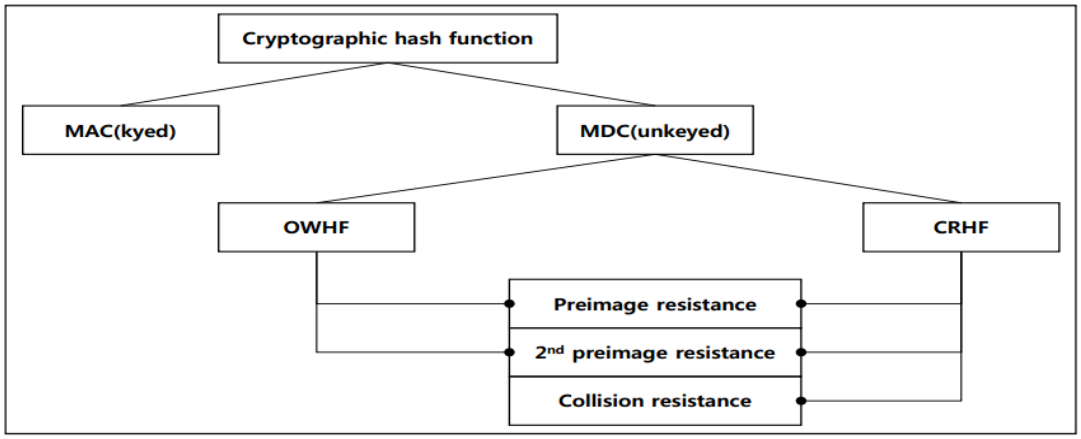
1. 단방향 해시함수의 결과값, 해시값의 개념



- 임의 길이 메시지를 고정길이 메시지(Message digest)로 변환 시 사용하는 단방향 함수인 해시 함수의 결과값

2. 해시함수의 구분 및 종류

가. 해시함수의 구분

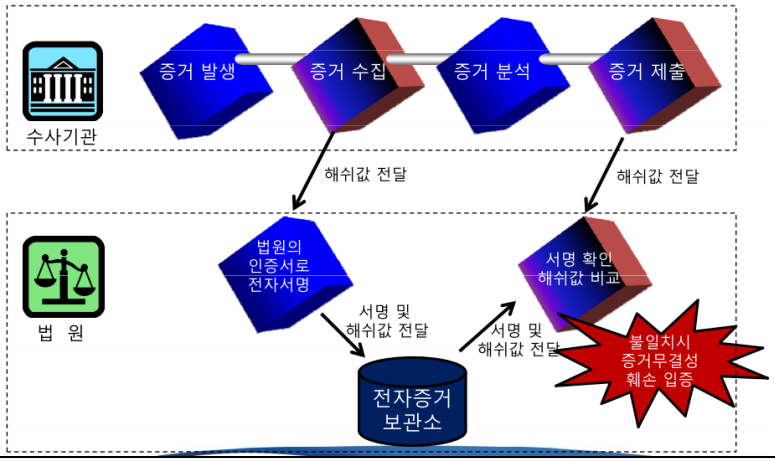
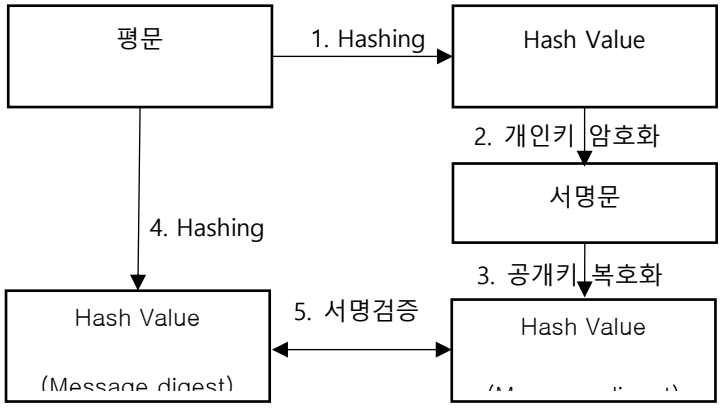


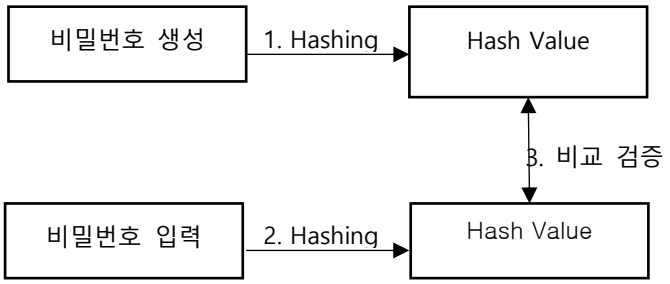
- 해시 함수는 해시 알고리즘을 통해 나온 메시지 다이제스트 값을 대칭적으로 암호화하고 키 값을 비대칭적으로 암호화해서 전송하는 Keyed 방식과 단지 무결성만 체크하고, 해시 알고리즘을 통해 나온 값 만을 같이 전송하는 Unkeyed Hash 로 분류 가능

나. 해시함수의 종류

종류	핵심 내용	설명
MD5	MD4 대체 무결성 검사	- 128 비트 암호화 해시 함수 - 보안 관련 용도 사용은 권장하지 않음
SHA	SHA1, SHA256, SHA384, SHA512	- MD5 대체하여 SHA-1 이 주로 쓰임 - 보안 프로토콜/프로그램 사용
HAS-160	160 비트 출력	- 입력 메시지를 512 비트 블록 단위 처리 후 160 비트 고정 길이 출력

3. 해시함수의 용도

<table>
<tr><th>활용분야</th><th colspan="2">내용</th></tr>
<tr><td rowspan="2">증거
위변조
방지
(포렌식)</td><td>개
념
도</td><td> 
</td></tr>
<tr><td>활
용
방
법</td><td>- 비트스트림 복제 방식으로 저장매체를 전체 복사하여 디스크 드라이브 이미지 생성 후 해시함수 적용
- 원본데이터를 1-bit 만 바꿔도 해시함수의 결과 값이 전혀 다른 출력값을 생성하므로 증거 무결성에 활용</td></tr>
<tr><td rowspan="2">전자서명</td><td>개
념
도</td><td> 
</td></tr>
<tr><td>활
용
방
법</td><td>- 평문을 해싱 후 해시값을 개인키로 암호화 하여 평문과 함께 전송
- 수신측에서 서명문을 공개키로 복호화 한 값과 원문의 해시값을 비교하여 서명검증
- 공인인증서의 데이터 무결성 검증 및 발신자 신원확인에 활용</td></tr>
</table>

시점확인	개념도	
	활용방법	- 임의의 디지털 데이터가 특정한 시점에 존재하였으며, 특정 시점이후 데이터의 내용이 변경되지 않았음을 증명 - 디지털 데이터와 객관적 시각 정보를 결합한 뒤 제 3 자 서명을 거쳐 시점 확인 토큰(TSA: Time Stamping Authority)을 생성 및 검증
단방향 암호화	개념도	
	활용방법	- 비밀번호생성 시 비밀번호를 해싱하여 보관 - 비밀번호입력 값을 해싱하여 저장된 해쉬값과 비교를 통한 인증 - 개인정보보호 안전조치의무의 비밀번호 단방향 암호화 시 적용

[참고] 해시 종류

알고리즘	출력길이	블럭의 크기	라운드 수
MD5	128	512	64
SHA1	160	512	80
SHA256	256	512	64
SHA384	384	1024	80
SHA512	512	1024	80
RMD128	128	512	128
RMD160	160	512	160
RMD256	256	512	128
RMD320	320	512	160
HAS160	160	512	80
TIGER	192	512	56

"끝"

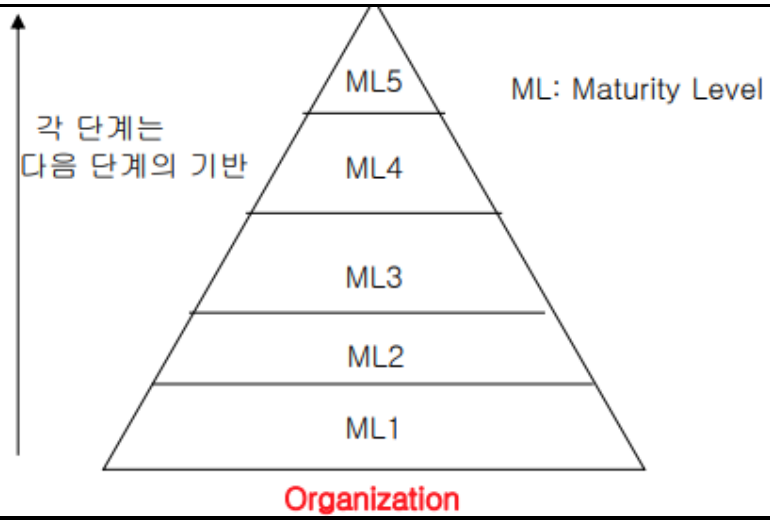
13	CMMI
문제	CMMI(Capability Maturity Model Integration)의 단계적 표현(Staged Representation)과 연속적 표현(Continuous Representation)
도메인	소프트웨어공학
정의	SW 개발 능력/성숙도 평가 및 프로세스 개선 활동의 지속적인 품질 개선 모델
키워드	Initial-Managed-Defined-Quantitatively Managed-Optimizing Incomplete-Performed-Managed-Defined
출제의도분석	CMMI2.0 발표 이후 재조명 받는 CMMI 에 대한 기본적 표현 질문
답안작성 전략	단계적/연속적 표현의 개념 및 단계
참고문헌	기술사 서브노트
풀이 기술사님	표기수 PE (제 117 회 정보관리기술사 / kisu.pyo@gmail.com)

1. CMMI 의 개념

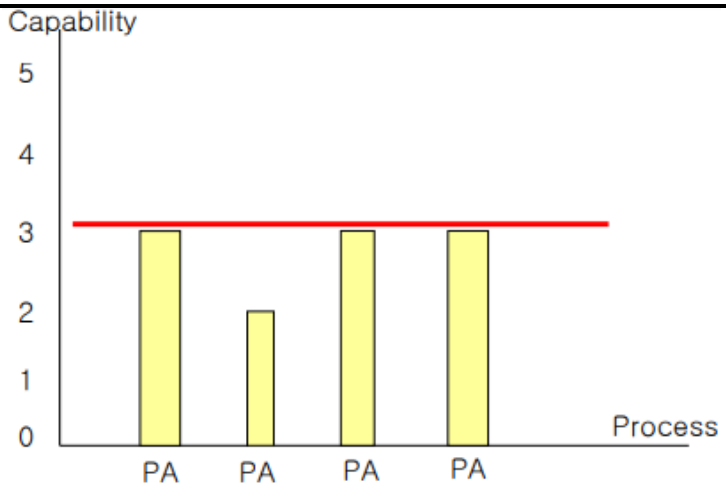
- 시스템과 SW 영역을 하나의 프로세스 개선 툴로 통합시켜 기업의 프로세스 개선활동에 광범위한 적용성을 제공하는 모델
- 기존 CMM 모델을 통합하고 SPICE 를 준수하는 SW 개발 능력/성숙도 평가 및 프로세스 개선 활동의 지속적인 품질 개선 모델

2. CMMI 의 단계적 표현과 연속적 표현

가. CMMI 의 단계적 표현(Staged Representation)

<table>
<tr><td>개념도</td><td colspan="2"> 
</td></tr>
<tr><td>개념</td><td colspan="2">- 가장 기초적인 관리 절차 로부터 상위 수준으로 향상되기 위해 필요한 실무까지 수행되어야 할 프로세스를 단계별로 제시
- 조직 간 비교를 가능하게 하는 단일한 등급 체계 제공</td></tr>
<tr><td rowspan="5">단계</td><td>Level1. Initial</td><td>- 개인의 역량에 따라 프로젝트 성패 좌우</td></tr>
<tr><td>Level2. Managed</td><td>- 프로젝트를 위한 프로세스 관리</td></tr>
<tr><td>Level3. Defined</td><td>- 조직의 프로세스 표준화</td></tr>
<tr><td>Level4. Quantitatively Managed</td><td>- 정량적인 관리</td></tr>
<tr><td>Level5. Optimizing</td><td>- 지속적인 프로세스 개선</td></tr>
</table>

나. CMMI 의 연속적 표현(Continuous Representation)

개념도		
개념	- 조직의 비즈니스 목적을 충족시키고, 위험 요소를 완화시키는데 중요한 개선 사항의 순서를 정하여 적용시킬 수 있음 - Capability Level 을 이용하여 프로세스 영역(PA) 별로 성숙도 평가 가능	
단계	Level0. Incomplete	- 활동이 수행 안됨
	Level1. Performed	- 작업자 능력에 따라 성과 좌우됨
	Level2. Managed	- 특정 프로젝트 내의 프로세스가 정의되고 수행
	Level3. Defined	- 표준화, 일관된 프로세스 정의

3. Staged Representation 과 Continuous Representation 의 비교

비교	Staged Representation	Continuous Representation
활용	성숙도 수준으로 조직간 비교 모델	능력 수준을 프로세스에 적용
Process Area	Maturity Level 로 그룹화	Capability Level 로 그룹화
성숙도	1~5 단계	0~3 단계
예제모델	SW-CMM	SE-CMM

"끝".