제132회 정보관리기술사 해설집

2024.01.27

국가기술자격 기술사 시험문제

기술사 제 132 회 제 4 교시 (시험시간: 100 분)

분야	정보통신	자격종목	정보관리기술사	수검번호		성명	

※ 다음 문제 중 4 문제를 선택하여 설명하시오. (각 10 점)

1. FIPS(Federal Information Processing Standard) 140-2 에 대하여 다음을 설명하시오.
   가. FIPS 140-2 레벨 분류
   나. 암호화 시스템 설계 시 고려사항
   다. 암호화 시스템의 보안 요소
   라. 보안 위협 대응 전략

2. 행정안전부에서는 고품질의 공공데이터 제공 및 활용의 선제적 대응을 위해 '공공데이터 베이스 표준화 관리 매뉴얼(2023.04.)'을 마련하여 예방적 품질관리 기준을 제시하고 있다. 이와 관련하여 다음을 설명하시오.
   가. 시스템 구축 추진 단계별 예방적 품질관리 활동
   나. 공공데이터 예방적 품질관리 4 개 진단영역과 9 개 진단항목

3. 설비 예지정비(Predictive Maintenance) 시스템 구축 시 LangChain 프레임워크를 활용할 수 있는 방안에 대하여 다음을 설명하시오.
   가. 설비 예지정비의 개념 및 필요성
   나. LangChain 프레임워크와 LLM(Large Language Model)
   다. LangChain 을 이용한 설비 예지정비

4. 소프트웨어 진흥법(시행 2023.10.19)은 소프트웨어 산업의 발전을 위해 시행되어야 할 다양한 활동의 법적 근거를 마련하고 있다. 이와 관련하여 다음을 설명하시오.
   가. 제 5 조(기본계획의 수립 등)의 2 항에 따른 기본계획 내 포함되어야 할 사항
   나. 제 30 조(소프트웨어안전 확보)의 2 항에 따른 소프트웨어안전 확보를 위한 지침 내 포함 되어야 할 사항

5. 소프트웨어 개발에 필요한 규모 산정 방식 종류와 특징을 비교 설명하고, 공공 소프트웨어 사업 규모 산정 방식의 현실적 방안에 대하여 설명하시오.

6. A 기업의 경영진은 임직원들의 증가로 인해 정보보안의 필요성을 인식하고 정보보안 부서의 신설과 정보보안 체계를 수립하고자 한다. 다음을 설명하시오.
   가. 정보보호 정책의 개념
   나. 정보보호 시점 별 보안 활동(Security Action Cycle)
   다. 정보보안 전문가의 역할과 역량

01	FIPS(Federal Information Processing Standard)		
문제	FIPS(Federal Information Processing Standard) 140-2에 대하여 다음을 설명하시오. 가. FIPS 140-2 레벨 분류 나. 암호화 시스템 설계 시 고려사항 다. 암호화 시스템의 보안 요소 라. 보안 위협 대응 전략		
도메인	정보보안	난이도	상(상/중/하)
키워드	암호화 하드웨어 모듈 검증, 레벨1, 레벨2, 레벨3, 레벨4		
출제배경	하드웨어 모듈 암호화를 통한 보안 체계 강화		
참고문헌	https://en.wikipedia.org/wiki/FIPS_140-2		
해설자	강남평일야간반 전일 기술사(제 114회 정보관리기술사 / nikki6@hanmail.net)		

I. 민감한 미분류 정보를 보호하기 위한 표준, FIPS 개요

가. FIPS(Federal Information Processing Standard) 140-2 정의

- 암호화 하드웨어 모듈 검증을 위해 미국 정부가 설정한 컴퓨터 보안 표준 모음

나. FIPS 140 시리즈 분류

시리즈	상세 내용
FIPS 140-1	- 암호화 모듈에 대한 보안 요구 사항
FIPS 140-3	- 암호화 모듈을 검증하는 데 사용되는 최신 버전의 미국 정부 컴퓨터 보안 표준

- FIPS 140-3은 FIPS 140-2를 대체하며 2019년 9월 22일부터 발효되었으며 2020년 9월 22일부터 검증이 시작
- 즉, FIPS 140-2 테스트는 공식적으로 2021년 9월 21일에 종료, NIST는 9월부터 FIPS 140-3 제출 만 허용

II. FIPS 140-2 레벨 분류 상세 설명

가. FIPS 140-2 인증을 위한 프로그램

프로그램	상세 내용
CMVP(Cryptographic Module Validation Program)	- FIPS 140-2/-3 표준 준수를 위해 암호화 모듈을 검증 - CMVP의 목표는 검증된 암호화 모듈의 사용을 촉진하고 검증된 암호화 모듈이 포함된 장비를 조달하는 데 사용할 보안 메트릭을 연방 기관에 제공
CAVP(Cryptographic Algorithm Validation Program)	- 제품이 NIST에서 공식적으로 정의한 알고리즘을 실제로 구현하는지 여부를 검증 - 또한 암호 모듈 유효성 검사의 전제 조건 필요

나. FIPS 140-2 레벨 분류

레벨	주요 내용
레벨 1	- 보안 수준 1은 가장 낮은 수준의 보안을 제공 - 암호화 모듈에 대한 기본 보안 요구 사항이 지정 - 보안 레벨 1 암호화 모듈의 예로는 개인용 컴퓨터(PC) 암호화 보드

레벨 2	- 보안 레벨 2는 일반 텍스트 암호화 키 및 중요한 보안 매개변수 에 물리적으로 접근하기 위해 깨져야 하는 변조 방지 코팅 또는 봉인을 포함하여 변조 증거를 보여주는 기능을 요구함으로써 보안 레벨 1 암호화 모듈의 물리적 보안 메커니즘을 향상
레벨 3	- 보안 레벨 2에서 요구되는 변조 방지 물리적 보안 메커니즘 외에도 보안 레벨 3은 침입자가 암호화 모듈 내에 있는 CSP에 액세스하는 것을 방지
레벨 4	- 보안 수준 4는 가장 높은 수준의 보안 제공

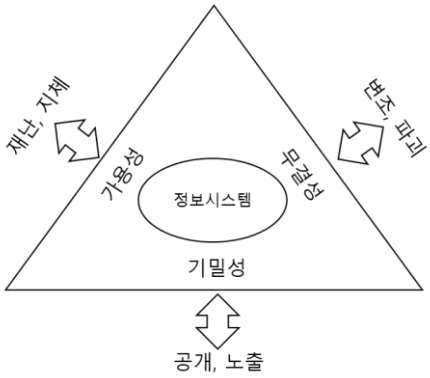
- 조직은 FIPS 140-2 표준을 사용하여 선택한 하드웨어가 특정 보안 요건을 충족하는지 확인 필요

III. 암호화 시스템 설계 시 고려사항 및 암호화 시스템의 보안 요소

가. 암호화 시스템 설계 시 고려사항

구분	고려사항	주요 내용
구축 및 설치	암호 알고리즘의 선택	- 강력한 암호 알고리즘을 선택 - 표준이나 보안 커뮤니티에서 인정받는 알고리즘을 사용하는 것이 중요
	키 관리	- 안전하고 효과적인 키 관리가 핵심 - 키 생성, 저장, 전송, 갱신, 파기 등에 대한 철저한 정책이 필요
	랜덤성	- 무작위성은 암호화에 있어 중요한 요소 - 키 및 초기화 벡터 (IV)를 생성하는 데 안전한 난수 발생기를 사용
	암호화 모드	- ECB, CBC, GCM 등 다양한 암호화 모드가 있으며, 데이터의 특성에 맞는 적절한 모드를 선택
	인증과 무결성	- 암호화된 데이터의 무결성을 보장하고 인증을 위해 해시 함수나 HMAC 등의 기술을 사용
	키 교환 및 프로토콜	- 키 교환을 안전하게 수행하는 방법과 통신 프로토콜에 대한 보안 고려가 필요
	사용자 인증 및 권한	- 시스템 사용자의 신원을 확인하고, 적절한 권한 제어를 구현
	암호화 성능	- 암호화 및 복호화의 성능에 대한 고려가 필요하며, 특히 대량의 데이터 처리 시에도 효율적으로 동작
유지 및 관리	보안 업데이트	- 보안 취약성이 발견되거나 알려진 경우, 시스템을 신속하게 업데이트하여 보안을 강화
	사용자 교육	- 사용자에게 안전한 비밀번호 사용 및 보안 관행에 대한 교육이 필요
	컴플라이언스	- 해당 산업의 규정 및 규제를 준수하도록 시스템을 설계
	로그 및 감사	- 시스템에서 발생하는 모든 보안 이벤트를 기록하고 감사할 수 있는 체계를 구축

나. 암호화 시스템의 보안 요소

개념도	보안 요소	설명
	기밀성	- Confidentiality - 오직 인가된 사람, 인가된 프로세스, 인가된 시스템만이 알 필요성에 근거하여 시스템에 접근해야 한다는 원칙
	무결성	- Integrity - 네트워크를 통하여 송수신되는 정보의 내용이 불법적으로 생성 또는 변경되거나 삭제되지 않도록 보호되어야 하는 성질
	가용성	- Availability - 시스템이 지체 없이 동작하도록 하고, 합법적 사용자가 서비스 사용을 거절당하지 않도록 하는 것

- 보안 요소 강화 뿐만 아니라 새롭고 다양한 보안 위협에 대응할 수 있는 전략과 실행이 필요

IV. 보안 위협 대응 전략

구분	고려사항	주요 내용
기술적 대응력 강화	위험 평가 및 감지	- 조직은 정기적으로 보안 위험을 식별하고 평가
	다층 방어 전략	- 다양한 방어층을 구축하여 여러 보안 레벨을 만듬
	암호화/보안 기술 사용	- 데이터 암호화, 방화벽, 침입 탐지 시스템(IDS), 침입 방지 시스템(IPS), 안티바이러스 프로그램 등과 같은 보안 기술을 활용하여 시스템을 강화
보안 거버넌스 체계 구축	보안 정책 및 교육	- 강력한 보안 정책을 수립하고 모든 직원에게 보안 교육을 제공. 직원이 보안에 대한 인식을 갖고, 적절한 행동을 취할 수 있도록 하는 것이 중요
	접근제어 및 권한 관리	- 시스템에 접근하는 사용자 및 기기를 정확히 식별하고, 필요한 권한만을 부여하는 접근 제어와 권한 관리 체계를 구축
	모니터링 및 이벤트 관리	- 실시간으로 시스템 및 네트워크 활동을 모니터링하고, 이상 징후를 탐지하고 대응할 수 있는 이벤트 관리 시스템을 운영
	사이버 보험 및 예방 계획	- 사이버 보험을 가입하여 발생 가능한 손실에 대비하고, 사전에 예방 계획을 수립하여 신속한 대응을 가능케 해야함
	재해 복구 및 비상 대응 계획	- 시스템이나 네트워크가 공격을 받았을 때의 대응책을 마련하고, 빠르게 복구할 수 있는 계획을 수립
	법규 및 규정 준수	- 관련 법규와 규정을 준수하여 비즈니스 활동이나 개인 정보에 대한 보호를 보장
	보안 업데이트 및 패치 관리	- 시스템 및 소프트웨어의 보안 업데이트 및 패치를 정기적으로 적용하여 알려진 취약점에 대응

- 보안에 대한 전략은 지속적으로 개선되고 적응해야 하며, 새로운 위협이나 기술의 발전에 맞게 조직은 적절한 대응책을 유지해야 함

"끝"

02	공공데이터 베이스 표준화 관리		
문제	행정안전부에서는 고품질의 공공데이터 제공 및 활용의 선제적 대응을 위해 '공공데이터 베이스 표준화 관리 메뉴얼(2023.04)'을 마련하여 예방적 품질관리 기준을 제시하고 있다. 이와 관련하여 다음을 설명하시오. 가. 시스템 구축 추진 단계별 예방적 품질관리 활동 나. 공공데이터 예방적 품질관리 4개 진단영역과 9개 진단항목		
도메인	데이터베이스	난이도	중 (상/중/하)
키워드	계획단계, 발주단계, 정보시스템 컨설팅 단계, 정보시스템 구축 단계 데이터 표준, 데이터 구조, 데이터 값, 데이터 관리체계		
출제배경	2023년 4월 개정고시 내용에 대한 숙지 여부 확인		
참고문헌	ITPE 기술사회 자료집		
해설자	단합반멘토 안경환 기술사(제 110회 정보관리기술사 / akh.itpe@gmail.com)		

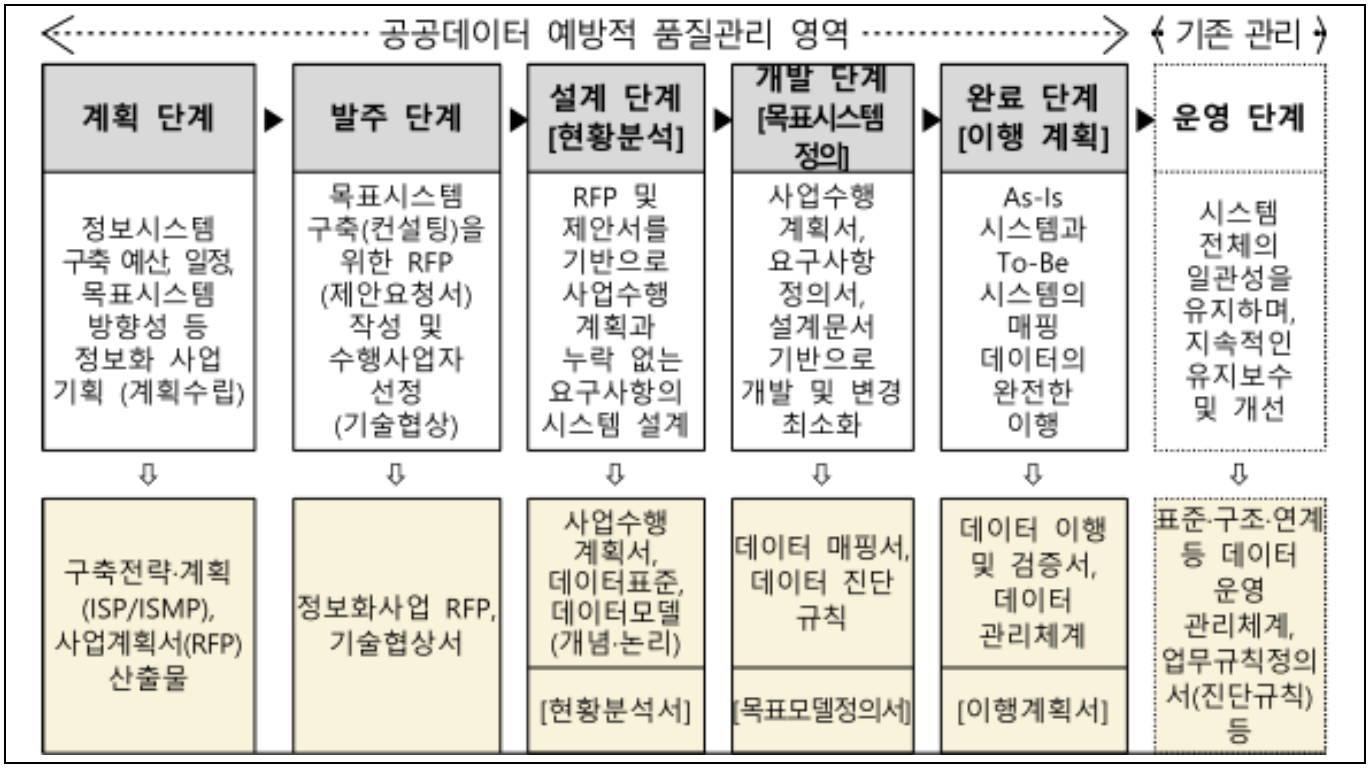
I. 공공기관의 데이터베이스 표준화 지침 개정내용

개정내용	개정사유
관리항목의 유연성 강화 (별표 제1호 및 제2호 신설)	- 데이터 표준 산출물과 별지 및 별표에 포함된 관리항목을 일치시켜 관리항목 등록·관리 유연성 및 편의성 제고함
비표준데이터 관리체계 마련 (제8조 제5항)	- 운영 중인 정보시스템(DB)의 비표준데이터를 표준화된 데이터와 매핑관리할 수 있도록 명시함
메타정보 관리항목 정비 (별표 제4호)	- 중앙 메타데이터 관리시스템, 공동활용시스템 등에서 필요한 공통항목으로 메타정보 관리항목을 정비함 (기존 : 43개 → 조정 : 38개)
용어 정의 추가(제2조)	- 데이터 표준 간 관계 및 상위표준 준용 필요성을 명시함
관리시스템 현행화 (제4조, 제5조, 제6조, 제8조, 제13조)	- 표준관리 통합시스템과 메타데이터 관리시스템이 제공하는 기능에 따른 조항별 문구를 조정함

- 데이터베이스 구축 운영 시 공공기관이 준수해야 할 표준 관련 지침 내용을 보완하고, 메타데이터 표준 관리항목을 조정하는 등 기관의 효율적 데이터 표준화를 지원하고자 함
- 예방적 품질관리는 이러한 데이터 품질관리 활동이 구축 및 운영단계에서 원활히 이루어질 수 있도록 사업 계획을 수립하는 단계에서 데이터 품질관리 4개 영역별 제시된 점검항목을 사전 진단하여 계획에 반영하는 절차를 의미

II. 시스템 구축 추진 단계별 예방적 품질관리 활동

가. 시스템 구축 추진 단계별 예방적 품질관리 활동과 산출물



나. 시스템 구축 추진 단계별 예방적 품질관리 활동 수행 활동

시스템 구축 단계	컨설팅 단계	수행 활동 설명
계획 단계	- 목표, 예산, 서비스 등을 기획하는 단계	- ISP 또는 ISMP 사업을 통해 정보시스템의 기능과 서비스를 정의하고 데이터 품질 관련 개선 과제를 정의하는 단계
발주 단계	- 발주 단계	- 데이터 표준·구조·값·연계 등과 관련한 개선과제를 요구사항으로 도출하고 일정과 예산을 고려하여 사업수행 과업을 확정하는 단계
설계 단계	- 현황분석 단계	- 개발에 앞서 요구사항이 향후 운영단계까지 데이터 품질이 유지될 수 있도록 유지관리가 용이하고 유연한 시스템을 설계하는 단계
개발 단계	- 목표시스템 정의 단계	- 요구사항에 따라 시스템을 개발하고, 다양한 시나리오를 통해 테스트를 거치면서 오류를 확인하고 수정하여 데이터 완성도를 높이는 단계
완료 단계	- 이행 계획(수립) 단계	- 데이터 완결성 확보(데이터 이관이 필요한 경우) 및 데이터 관리체계를 점검하는 정보시스템 구축 최종 완료 단계

- 정보시스템 구축 사업은 계획 단계 → 발주 단계 → 설계 단계 → 개발 단계 → 완료 단계 총 5단계로 이루어지며 완료단계에서 테스트·이행·전환 추진을 통해 정보시스템 구축이 최종 완료되며, 컨설팅사업은 계획

단계 → 발주 단계 → 현황분석 단계 → 목표시스템 정의 단계 → 이행 계획(수립) 단계로 구성

III. 공공데이터 예방적 품질관리 4개 진단영역과 9개 진단항목

가. 진단영역 및 항목 구성도

- ① 예방적 품질관리 수행을 위해 우선되는 표준원칙 준수
- ② 데이터 표준, 구조, 값, 품질 제고를 위한 원칙, 조직, 역할, 절차 등의 지속적인 데이터 관리 체계 유지
- ③ 데이터 모델 설계 준수, 용어 표준 등 고품질 데이터 활용을 위한 표준 정립

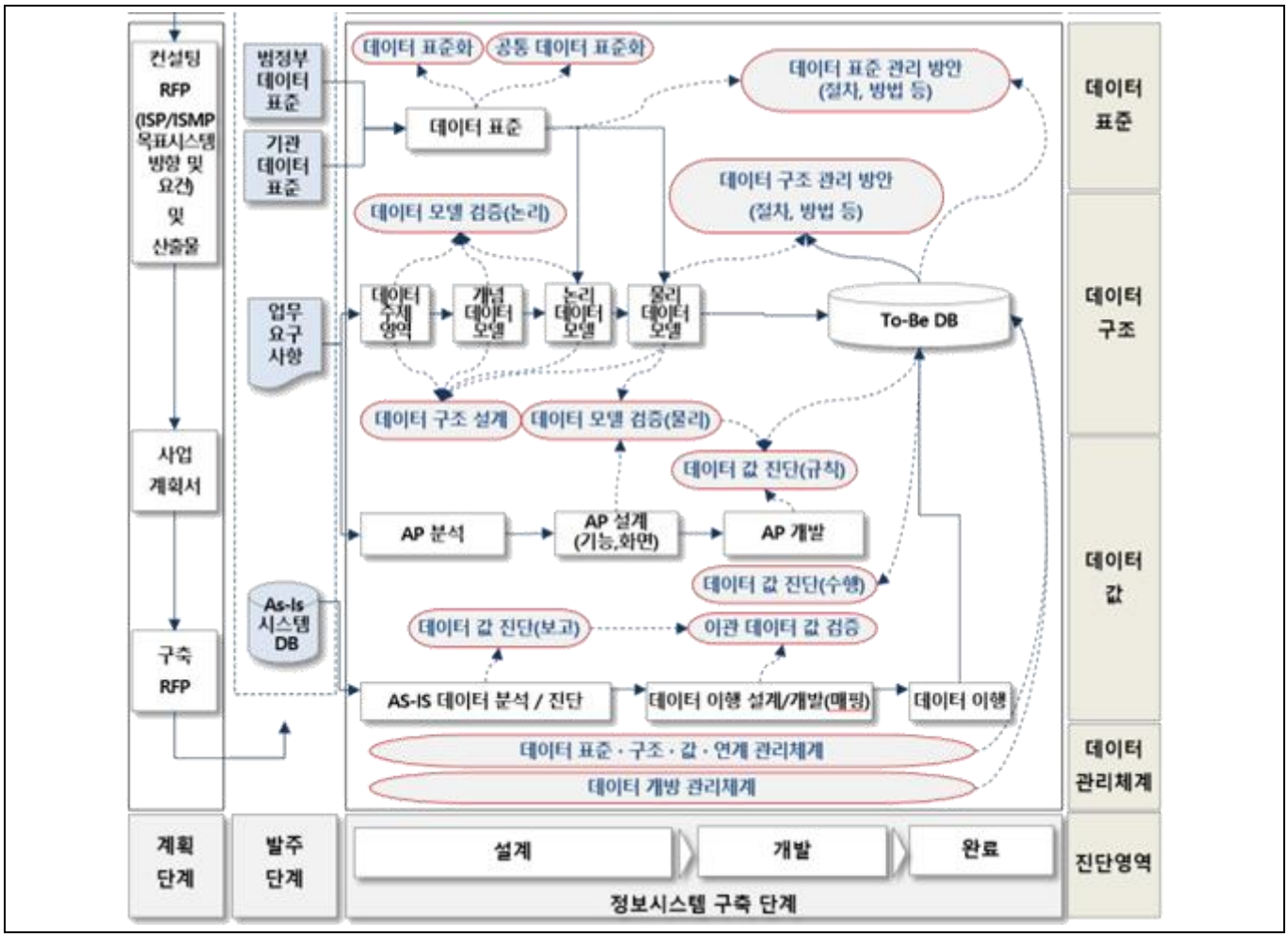
나. 공공데이터 예방적 품질관리 4개 진단영역과 9개 진단항목

진단 영역(4)	진단 항목(9)	진단 기준(18)
1. 데이터 표준	1.1 데이터 표준화 및 상위표준 준수	- 데이터 표준 코드, 용어, 단어, 도메인 등 데이터 표준화 사항 반영 여부
		- 공통표준 및 기관표준 적용·준수 여부
	1.2 데이터 표준 관리	- 데이터 표준 관리방안 반영 여부
		- 데이터 표준 변경이력 관리방안 반영 여부
2. 데이터 구조	2.1 데이터 구조 설계	- 데이터 구조 설계(모델링) 시 준수해야 할 기준 및 규칙, 고려사항 등 반영 여부
		- 데이터 구조(논리·물리) 설계를 위한 주제영역, 개념모델, 논리모델 관련 사항 반영 여부
	2.2 데이터 구조 검증	- 업무 요구사항의 모델 반영과 데이터 구조 정규화 수행 및 검증 계획 반영 여부
		- 데이터 모델링 과정 및 구조 적정성 검증 등에 대한 활동 사항 반영 여부
	2.3 데이터 구조 관리	- 데이터 구조 관리방안 반영 여부
		- 데이터 구조 변경이력 관리방안 반영 여부
3. 데이터 값	3.1 데이터 값 검증	- 데이터(연계데이터 포함) 값 검증 계획 반영 여부

		- 데이터 값 검증 수행 및 검증 결과에 따른 개선활동 반영 여부
	3.2 이관 데이터 값 검증	- 데이터 이관 계획(일정 및 수행방법론 등) 반영 여부
		- 이관 데이터 값 검증 수행 및 검증 결과에 따른 개선활동 반영 여부
4. 데이터 관리체계	4.1 데이터 품질관리 체계	- 데이터 품질관리를 위한 정책, 절차, 조직(담당자) 관련 사항 반영 여부
		- 데이터 품질관리를 위한 필수산출물 등 관련 사항 반영 여부
	4.2 데이터 개방 및 메타데이터 관리체계	- 개방 예정 데이터 목록 등 기관의 공공데이터 개방 계획과 본 사업의 연관성 관련사항 반영 여부
		- 공공데이터베이스의 메타데이터 등록, 관리 및 현행화 관련사항 반영 여부

"끝"

※ 구축 사업 분야에서 예방적 품질관리 활동



03	LangChain		
문제	설비 예지정비(Predictive Maintenance) 시스템 구축 시 LangChain 프레임워크를 활용할 수 있는 방안에 대하여 다음을 설명하시오. 가. 설비 예지정비의 개념 및 필요성 나. LangChain 프레임워크와 LLM(Large Language Model) 다. LangChain을 이용한 설비 예지정비		
도메인	인공지능	난이도	중(상/중/하)
키워드	임베딩, 비상계획, 가동정지, 장비 신뢰성 향상		
출제배경	LLM을 이용한 설비 예지정비 시스템 구축에 대한 이해		
참고문헌	ITPE 24회 모의고사 해설지 Smart Factory 추진의 핵심 기술, AI기반 설비예지정비 솔루션, A&TES (한화시스템) https://www.aitimes.com/news/articleView.html?idxno=138844 https://www.itworld.co.kr/news/216969 설명 가능한 AI를 적용한 기계 예지 정비 방법 (천강민, 양재경) 지능형 IoT를 융합한 장비 운용 시스템의 예지 보전을 위한 연구(이상덕, 김영곤)		
해설자	모멘텀 안수현 기술사(제119회 정보관리기술사 / tino1999@naver.com)		

I. 설비 예지정비의 개념 및 필요성

가. 설비 예지정비의 개념

- 설비의 이상을 사전에 예측하여 설비고장이 더 진행되기 이전에 정비 조치를 통해 대응하게 함으로써, 비계획 가동정지 예방과 설비의 수리비용 절감을 위한 기술

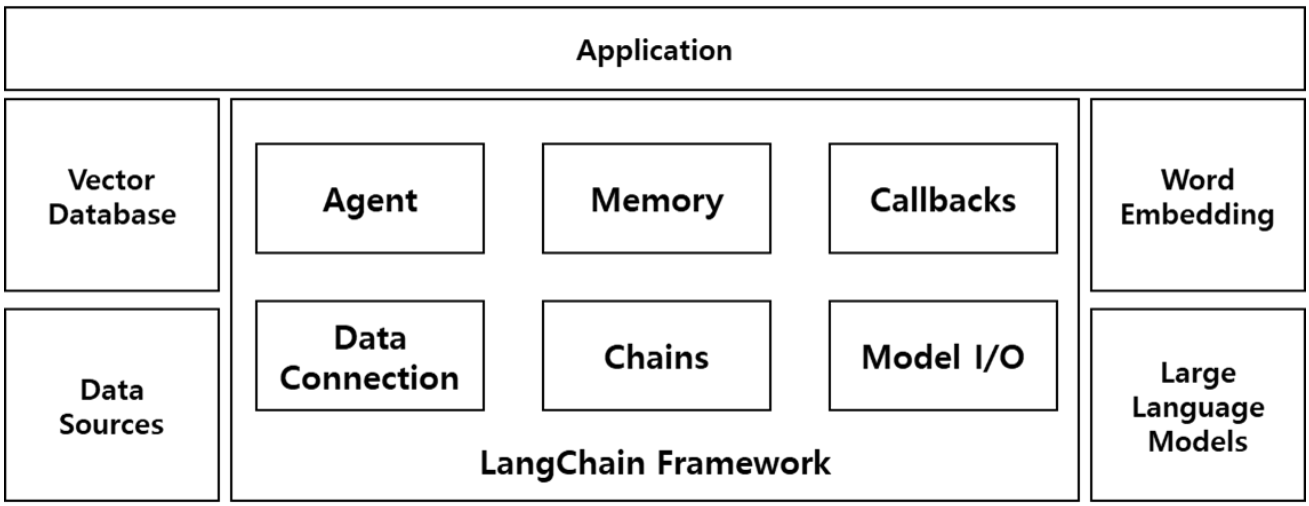
나. 설비 예지정비의 필요성

필요성	설명
장비 신뢰성 향상:	- 설비의 고장 및 장애를 예방하여 장비의 신뢰성을 향상 - 생산 일정을 지키고 생산 불량률을 낮추는 데 기여
생산량 증가	- 설비의 효율성을 최적화하고 고장으로 인한 비계획적인 다운타임을 최소화하여 생산량을 증가
비용 절감	- 계획된 유지보수로 인해 높은 비용의 비계획적인 수리 및 대체를 방지하고 전반적으로 유지보수 비용을 낮출 수 있음
안전성 강화	- 안전 규정 및 규제를 준수하고 작업 환경을 향상시켜 직원들의 안전을 강화하며, 장비의 안전 및 정확한 작동은 사고 발생 가능성을 줄임
에너지 효율성 향상	- 정기적인 점검과 유지보수는 설비의 에너지 효율성을 향상
장비 수명 연장	- 적절한 예지정비는 설비의 수명을 연장시키고 새로운 장비를 구입하는 비용 절감
유지보수 계획 수립	- 유지보수 계획을 세우고 실행함으로써 설비 운영을 체계적으로 관리

- 설비 예지정비 기술은 AI의 예측 기술을 통해 다운타임 방지 및 다양한 분석 가능

II. LangChain 프레임워크의 설명

가. LangChain 프레임워크



(개념)- 언어모델을 활용한 서비스 개발 시 여러 언어모델과 통합을 간소화하도록 설계된 SDK(Software Development Kit)이자 다양한 언어모델을 기반으로 하는 애플리케이션 개발을 위한 프레임워크.

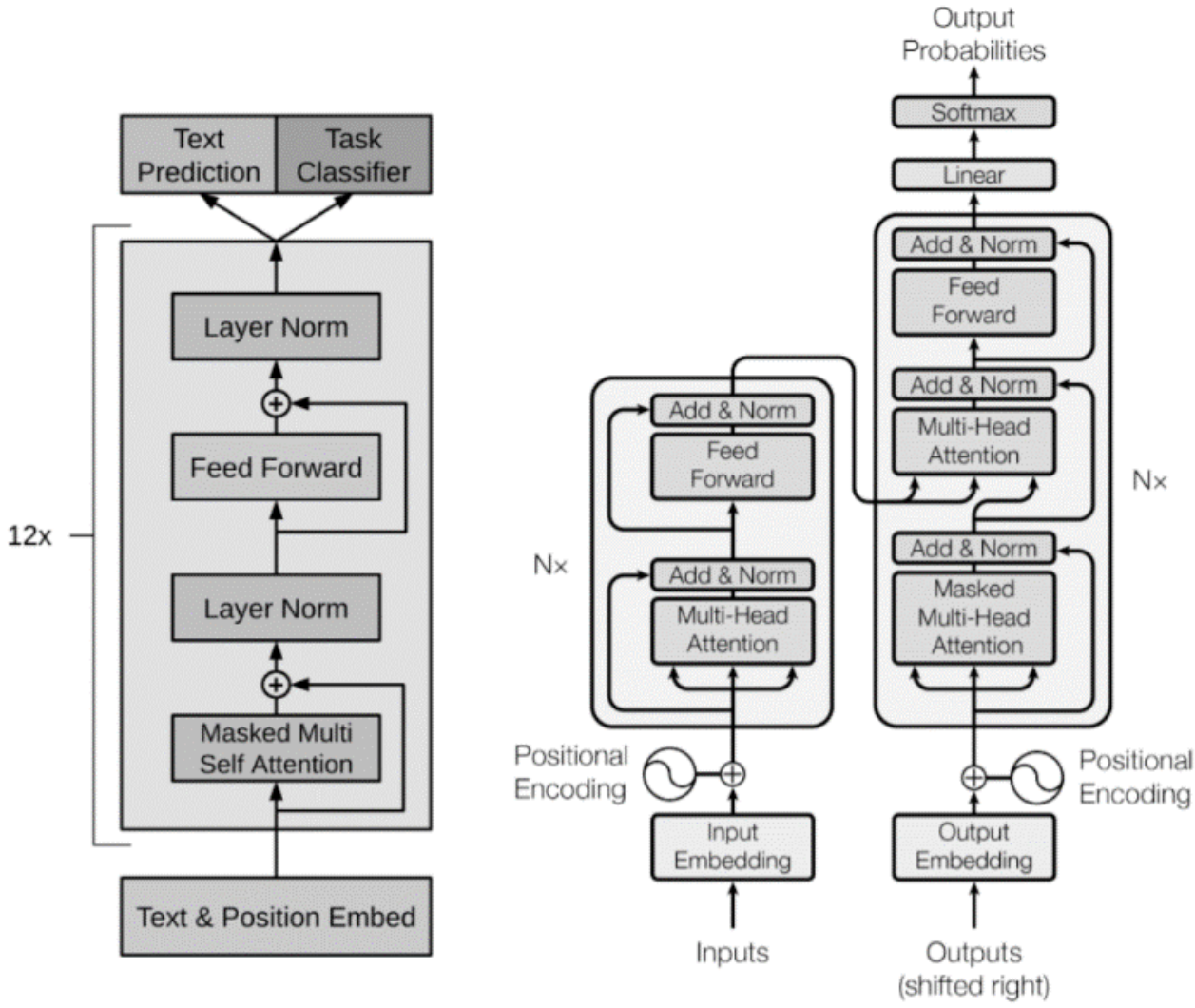
- 여러 모듈로 구성된 LanChain Framework를 활용하여 데이터베이스, 소스, LLM 등 다양한 외부 소스와의 연계를 통해 애플리케이션 개발 수행

나. LangChain 프레임워크의 구성요소

구분	구성요소	설명
메인 모듈	- Model I/O	- 언어모델 인터페이스로 모든 언어모델과 인터페이스 할 수 있는 빌딩 블록을 제공
	- Data Connection (데이터 연결)	- 애플리케이션 별 데이터와의 인터페이스로 모델 훈련세트의 일부가 아닌 사용자별 데이터가 필요, 데이터를 로드, 변환, 저장 및 쿼리할 수 있는 빌딩 블록을 제공
	- Agent(에이전트)	- 체인이 사용할 도구를 선택하여 동작하도록 지원 - 언어모델을 사용하여 수행할 일련의 작업을 선택
추가 모듈	- Chains	- 다양한 기능을 제공하는 컴포넌트를 인터페이스를 이용하여 체인으로 연결
	- Memory(메모리)	- 체인 실행 사시에 이전 상황을 기억하여 애플리케이션 상태 유지
	- Callbacks	- 모든 체인의 중간단계 기록 및 스트리밍 - 로깅, 모니터링, 스트리밍 및 기타작업을 위한 연결

III. LLM(Large Language Model)의 설명

가. LLM(Large Language Model)의 구성



개념	- GPT, BERT 모델과 같이 대량의 텍스트 데이터를 학습하여 인간과 유사한 언어 이해 및 생성 능력을 갖춘 초거대 언어 AI 모델

- LLM을 대표할 수 있는 GPT-3(왼쪽)와 Transformer(오른쪽)의 아키텍처

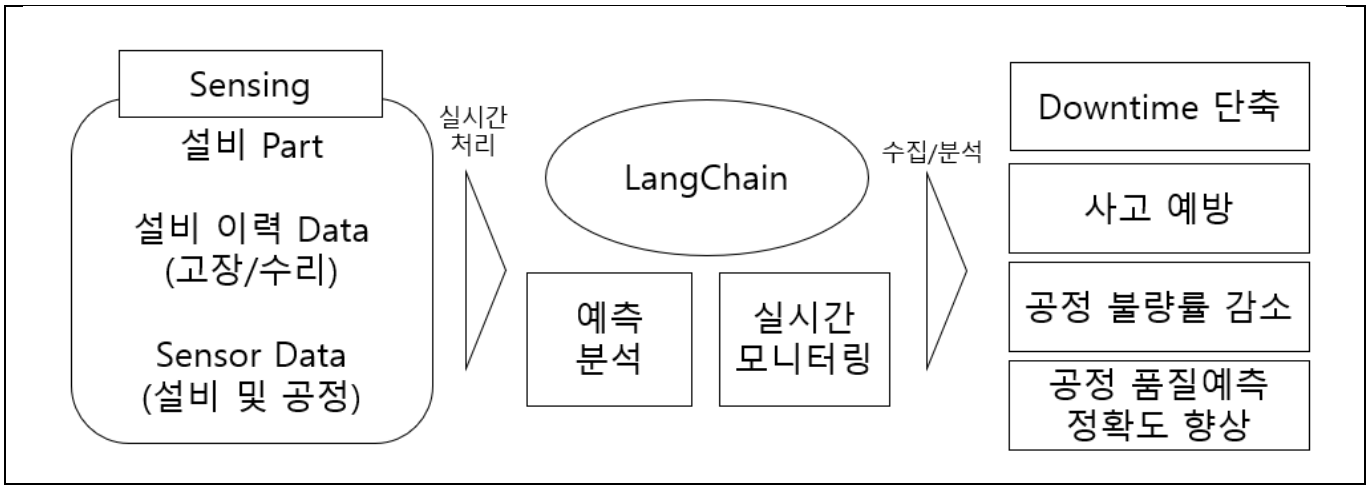
나. LLM(Large Language Model)의 설명

구분	항목	설명
주요 모델	GPT	트랜스포머의 디코더 구조로 구성되어 few shot Learning 된 순방향 자연어 처리 모델
	BERT	트랜스포머의 인코더 구조로 구성되어 file turning된 양방향 자연어 처리 모델
구성요소	임베딩 레이어 (embedding layer)	입력 텍스트로부터 임베딩을 생성. 대규모 언어 모델의 이 부분은 입력의 의미론적이고 구문론적 의미를 포착하므로 모델이 컨텍스트를 이해할 수 있음

	순환 레이어 (recurrent layer)	입력 텍스트의 단어를 순서대로 해석하며, 문장 내 단어 간의 관계를 해석.
	어텐션 메커니즘 (attention mechanism)	언어 모델이 현재 작업과 관련된 입력 텍스트의 단일 부분에 집중하는 레이어로, 모델이 가장 정확한 출력을 생성할 수 있도록 하는 기술

- LangChain을 이용해 다양한 LLM을 통합하여 설비 예지정비 시스템 구축가능

IV. LangChain을 이용한 설비 예지정비

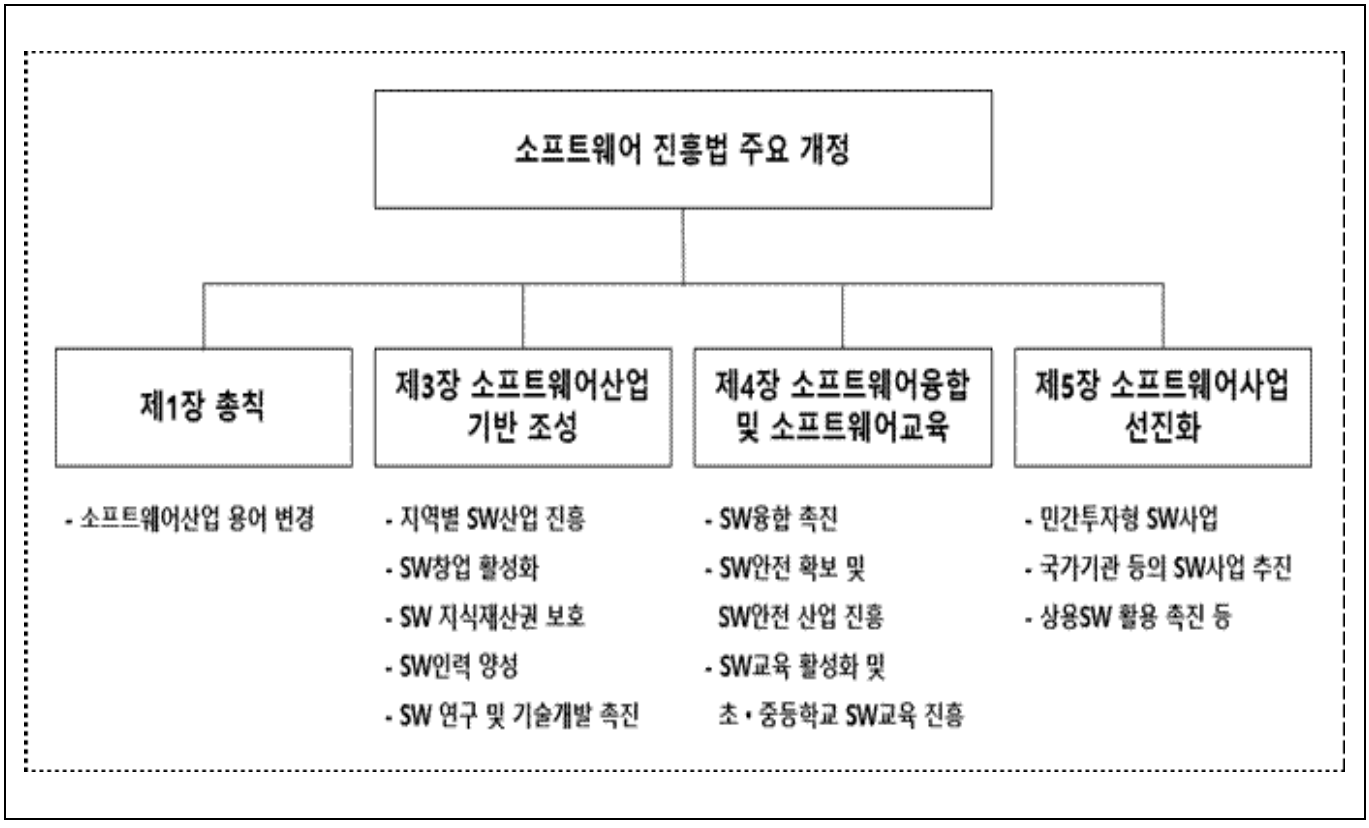


- 각종 센서 및 AIoT를 통해 수집된 데이터를 Langchain을 이용해 예측 및 분석하고 모니터링하여, 다운타임을 단축하고 사고 및 불량률 감소 등 고도화된 스마트 팩토리 구축 가능

"끝"

04	소프트웨어 진흥법		
문제	소프트웨어 진흥법(시행 2023.10.19)은 소프트웨어 산업의 발전을 위해 시행되어야 할 다양한 활동의 법적 근거를 마련하고 있다. 이와 관련하여 다음을 설명하시오. 가. 제5조(기본계획의 수립 등)의 2항에 따른 기본계획 내 포함되어야 할 사항 나. 제30조(소프트웨어안전 확보)의 2항에 따른 소프트웨어안전 확보를 위한 지침 내 포함되어야 할 사항		
도메인	소프트웨어공학	난이도	상(상/중/하)
키워드	위험분석, 안전 설계 및 구현, 소프트웨어 기반 조성, 인력 양성 등		
출제배경	소프트웨어 진흥법 시행령		
참고문헌	소프트웨어 진흥법		
해설자	BP반 김찬일 기술사(제 130회 정보관리기술사 / s2carey@naver.com)		

I. 소프트웨어 산업의 발전 위한, 소프트웨어 진흥법의 개요



- 소프트웨어 진흥에 필요한 사항을 정하여 국가 전반의 소프트웨어 역량을 강화하고 소프트웨어산업 발전의 기 반을 조성함으로써 국가경쟁력의 확보, 국민생활의 향상 및 국민경제의 건전하고 지속적인 발전에 이바지하기 위 한 법률

II. 제5조(기본계획의 수립 등)의 2항에 따른 기본계획 내 포함되어야 할 사항

제2장 소프트웨어 진흥시책

☐ **제5조(기본계획의 수립 등)** ① 과학기술정보통신부장관은 소프트웨어 진흥을 위하여 관계 중앙행정기관의 장과 협의를 거쳐 소프트웨어 진흥 기본계획(이하 "기본계획"이라 한다)을 수립 · 시행하여야 한다.

② 기본계획에는 다음 각 호의 사항이 포함되어야 한다.

1. 소프트웨어산업 진흥을 위한 시책의 기본방향
2. 소프트웨어산업 부문별 육성시책
3. 소프트웨어산업 기반 조성
4. 소프트웨어교육 및 인력 양성
5. 소프트웨어 기술의 연구개발 및 보급
6. 소프트웨어의 이용 촉진 및 유통 활성화
7. 소프트웨어사업 또는 소프트웨어융합 사업의 창업(이하 "소프트웨어창업"이라 한다) 지원
8. 소프트웨어산업의 국제협력 및 해외시장 진출
9. 소프트웨어 자산관리 활성화
10. 소프트웨어융합의 활성화
11. 지역별 특성에 기반한 소프트웨어산업의 진흥 및 지역 산업과의 융합 촉진
12. 소프트웨어안전 관리
13. 그 밖에 소프트웨어 진흥을 위하여 필요한 사항

③ 과학기술정보통신부장관은 기본계획에 따라 소프트웨어 진흥 시행계획(이하 "시행계획"이라 한다)을 수립 · 시행하여야 한다.

④ 제1항부터 제3항까지에서 규정한 사항 외에 기본계획 및 시행계획의 수립 · 시행에 필요한 사항은 대통령령으로 정한다.

1. 소프트웨어산업 진흥을 위한 시책의 기본방향
2. 소프트웨어산업 부문별 육성시책
3. 소프트웨어산업 기반 조성
4. 소프트웨어교육 및 인력 양성
5. 소프트웨어 기술의 연구개발 및 보급
6. 소프트웨어의 이용 촉진 및 유통 활성화
7. 소프트웨어사업 또는 소프트웨어융합 사업의 창업(이하 "소프트웨어창업"이라 한다) 지원
8. 소프트웨어산업의 국제협력 및 해외시장 진출
9. 소프트웨어 자산관리 활성화
10. 소프트웨어융합의 활성화
11. 지역별 특성에 기반한 소프트웨어산업의 진흥 및 지역 산업과의 융합 촉진
12. 소프트웨어안전 관리

13. 그 밖에 소프트웨어 진흥을 위하여 필요한 사항

III. 제30조(소프트웨어안전 확보)의 2항에 따른 소프트웨어안전 확보를 위한 지침 내포함되어야 할 사항

제30조(소프트웨어안전 확보) ① 정부는 소프트웨어안전 확보를 위한 시책을 마련할 수 있다.

② 과학기술정보통신부장관은 다음 각 호의 사항을 포함하는 소프트웨어안전 확보를 위한 지침을 정하여 고시하여야 한다.

1. 소프트웨어안전 관련 위험 분석
2. 소프트웨어안전 확보를 위한 설계 및 구현 방법
3. 소프트웨어안전 검증 방법
4. 운영 단계의 소프트웨어안전 확보 방안
5. 그 밖에 소프트웨어안전 확보에 필요하다고 인정되는 사항

③ 중앙행정기관의 장은 소관 분야의 소프트웨어안전에 관한 기술기준을 수립하는 경우 제2항에 따른 지침 또는 국제표준 등을 고려하여야 한다.

1. 소프트웨어 안전 관련 위험 분석
2. 소프트웨어 안전 확보를 위한 설계 및 구현 방법
3. 소프트웨어 안전 검증 방법
4. 운영 단계의 소프트웨어 안전 확보 방안
5. 그 밖에 소프트웨어안전 확보에 필요하다고 인정되는 사항

"끝"

05	소프트웨어 규모산정		
문제	소프트웨어 개발에 필요한 규모산정 방식 종류와 특징을 비교 설명하고, 공공 소프트웨어 사업 규모 방식의 현실적 개선 방안에 대하여 설명하시오.		
도메인	소프트웨어공학	난이도	중(상/중/하)
키워드	FP, LOC, COCOMO, 스토리포인트, 투입자원, 소요기간 파악		
출제배경	소프트웨어공학 기본토픽 이해 확인		
참고문헌	ITPE 기술사회 자료집		
해설자	정상반 정상 기술사(제 124회 정보관리기술사 / itpe_peak@naver.com)		

I. SW의 적정한 비용산정 방식, SW 규모산정 개요

가. SW 규모산정의 정의

- 소프트웨어 규모파악(양적 크기, 질적 수준) 통한 소요공수와 투입자원 및 소요기간 파악하여 실행 가능한 계획 수립하기 위한 비용 산정하는 과정

나. SW 규모산정의 의의

구분	설명
낮게 산정 시	- 품질문제 발생, 납기문제, 개발자 부담 가중
높게 산정 시	- 예산낭비(개발비, 유지보수비), 일의 효율성 저하

II. SW 규모산정 방식 종류와 종류별 특징 비교

가. 규모산정 방식 종류

산정 방식	설명
LOC 산정	- SW의 각 기능의 원시코드 라인수의 비관치, 낙관치, 기대치를 측정하여 예측치를 구하여 비용을 산정하는 방식
COCOMO	- 원시 프로그램의 규모에 의한 방법으로 시스템을 구성하고 있는 모듈과 서브 시스템의 비용 합계를 계산하여 비용 산정하는 방식
FP(기능점수)	- 사용자 관점에서 SW 개발 규모를 측정하기 위해 기능을 정량화하고 계수적 측정을 통해 나타낸 기법
스토리포인트	- 팀이 특정 기능을 개발하는데 필요한 노력의 양을 추정하기 위한 편리하고 표율적인 측정 기법

나. 규모산정 방식 종류별 특징 비교

구분	LOC	COCOMO	FP	스토리포인트
개념적 특징	프로그램 코드량, 1인당 월평균 생산 코드를 기반으로 비용산정	프로젝트 데이터에 기초하여 비용산정	복잡도, 가중치 적용으로 구성하여 비용산정	요구사항 기반에서 규모 및 비용 산정
산정 방식	개발 소스의 라인을 카운트	모드에 따른 파라미터 사용	ILF, EIF, EI, EQ, EO 요소 활용	복잡도 추정하여 규모를 설정

기법	소스코드 라인수 측정	정해진 공식을 활용한 측정	데이터 트랜잭션 기능으로 분류	유저 스토리 사용
활용	구조적 프로그래밍 방식에 활용	프로젝트 규모에 따라 모드 분류 활용	사업초기 개발 비용 예측 가능	애자일 개발방법론에서 활용

III. 소프트웨어 규모 산정 방식의 현실적인 개선 방안

가. 프로젝트 측면 현실적 개선 방안

구분	개선방안	설명
문제 복잡도	난이도 조절	- 비즈니스의 문제와 기술적 프로젝트 구현 문제의 적절한 난이도 조절 필요
	요구사항 맞춤 유형 적용	- 발주자의 요구사항에 맞는 유형의 BP, 또는 개발 방법론 확인 필요
	프로젝트 개발언어 고려	- 구체적인 프로젝트에 적용되어야 할 개발언어 확인 및 적용 고려
시스템 크기	트랜잭션 크기 확인	- 시스템의 트랜잭션 크기를 사전에 확인 하여 적용
	데이터 연계 고려	- 외부 연계, 시스템 간의 데이터 연계를 고려한 규모 산정 필요

- 프로젝트 뿐만이 아닌 자원, 생산성 측면에서의 개선 방안도 고려할 필요 있음

나. 자원, 생산성 측면 현실적인 개선방안

구분	개선방안	내용
자원 요소	인적 자원 고려한 배치	- 관리자, 개발자, 지원체계 등의 투입되는 인적 요소 확인 필요
	소프트웨어 자원 고려	- 개발지원 도구, 테스트 툴과 같은 최적의 SW 툴의 배치 적용
생산성 요소	개발자 능력 확인	- 경험, 전문지식 습득 정도 투입되는 전문적인 개발자의 능력 확인
	개발 방법론	- 최신기법, 개발 방법론, 관리 방법론 등의 프로젝트에 적용될 방법론 확인

- 개발 방법론, 조직원 역량, 시스템 복잡도 등 다양한 요소 고려하여 규모 산정 필요

"끝"

06	정보보안 체계		
문제	A 기업의 경영진은 임직원들의 증가로 인해 정보보안의 필요성을 인식하고 정보보안 부서의 신설과 정보보안 체계를 수립하고자 한다. 다음을 설명하시오. 가. 정보보호 정책의 개념 나. 정보보호 시점별 보안 활동(Security Action Cycle) 다. 정보보안 전문가의 역할과 역량		
도메인	보안	난이도	중(상/중/하)
키워드	예방, 탐지, 저지, 교정		
출제배경	정보보안 중요성에 따른 기본적인 개념 확인		
참고문헌	ITPE 기술사회 자료		
해설자	모멘텀 안수현 기술사(제119회 정보관리기술사 / tino1999@naver.com)		

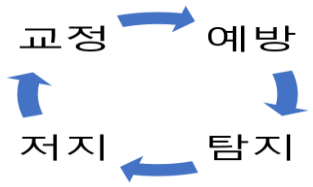
I. 정보보호 정책의 개념

구분	설명
정의	조직이나 기업이 정보자산을 보호하고 안전하게 관리하기 위해 수립하고 시행하는 일련의 원칙, 규정, 지침, 절차 등의 체계적인 정책
목적	조직의 정보자산을 보호하고 기밀성, 무결성, 가용성을 유지
활동	리스크 관리, 교육 및 훈련, 기술적 보안조치, 사고 대응 및 복구

- 정보보안 체계는 정보보호의 시점별 보안활동을 분석하고, 전문가의 의견을 수렴하여 효율적으로 수립

II. 정보보호 시점별 보안활동

가. 정보보호 사이클(Security Action Cycle)

개념도	단계	통제활동	설명
	사전	예방	알려진 보안위협의 발생을 사전에 대비 및 방어
	발생중	탐지	보안위협 및 침해사고의 발생을 인지
	발생중	저지	미비한 통제조치를 보완하거나 위험발생을 저지
	사후	교정	문제의 원인을 식별/분석하여 보완조치

나. 정보보호 시점별 보안활동

통제유형	기술적	관리적	물리적
예방(Preventive)	방화벽, 암호화, WIPS, DRM, IAM, AAA	보안 정책수립, 보안서약, 업무분리, 보안경비	출입통제, 자물쇠
탐지(Detective)	IDS, 감사로그, ESM, DLP, 무결성 검증	감사, 모니터링	센서, 경보, CCTV
저지(Deterrent)	DLP, USB보안, IPS, 필터링	법/제도화, 모의훈련	CCTV, 담장, 경보
교정(Corrective)	백신, NAC, Check point	BCP 수립, 백업/복구	DR센터 구축, UPS, 항온항습, 전력이중화

III. 정보보안 전문가의 역할과 역량

가. 정보보안 전문가의 역할

역할	설명
시스템 보안 구현 및 관리	방화벽, 침입탐지 시스템 등을 구현하고 유지보수하는 역할
암호화 기술 이해	기밀성을 유지하기 위한 데이터 및 통신 암호화 기술을 이해하고 구현하는 역할
접근 통제 및 식별 관리	사용자의 접근을 통제하고 식별 관리 시스템을 구현하는 역할
취약점 관리	시스템 취약점을 식별하고 관리하여 보안을 유지하는 역할
사이버 위협 대응	사이버 공격에 대응하여 시스템을 보호하고 복구하는 역할
보안 정책 및 규정 준수	관련된 법규와 규정에 따라 보안 정책을 수립하고 이행하는 역할
교육 및 인식 확대	보안 인식을 높이기 위한 교육 및 훈련 프로그램을 개발하고 실시하는 역할
포렌식 및 사고 대응	사고 발생 시 빠른 대응 및 조사를 위한 포렌식 기술을 활용하는 역할
신기술 및 트렌드 추적	보안 기술 및 트렌드를 추적하고 조직에 적용할 수 있는 새로운 기술을 도입하는 역할

나. 정보보안 전문가의 역량

역할	설명
기술적 지식	다양한 보안 기술과 도구에 대한 깊은 이해
전략적 사고	보안 문제를 비즈니스 목표와 연계시키는 전략적 사고 능력
커뮤니케이션 능력	비전문가에게도 이해되도록 기술 용어를 명확히 전달하는 능력
규정 준수 이해	보안 규정과 법률에 대한 이해와 준수 능력
문제 해결 능력	복잡한 보안 문제에 대한 신속하고 효과적인 해결책 마련 능력
교육 및 훈련 능력	교육 및 훈련 프로그램을 설계하고 실행할 수 있는 능력
컨설팅 및 협상 능력	이해관계자와의 협력 및 보안 컨설팅을 제공하는 능력
윤리적 행동	고객과 조직의 신뢰를 유지하기 위해 윤리적 행동을 지향하는 태도

"끝"

[참고] SDLC 별 보안활동

순번	분류	통제 활동
개발	계획 및 분석	- 보안위험, 위협에 대한 계획 수립한다. Ex. 사이버 보안 지수 계획
	보안 설계	- 위협에 대한 방어라인 설계, 위협에 대한 전방위적인 방어 설계, 미래 사이버보안 환경 강화 연계 설계
	시스템 구축	- 관리적, 물리적, 기술적 보안 관제 시스템 구축한다. Ex) 한국수력원자력 자료 유출 위협에 대한 인프라 시스템 구축
	보안 테스트	- 보안 테스트 시나리오, 테스트 케이스 작성 및 수행.
	릴리즈	- ESM, SIEM 구축 및 Release
운영	시스템 운영	- 관리적 운영 보안 사항 적용: ISO 27001, ISMS, PIMS 적용. - 기술적 보안: APT 공격에 대한 IDS, IPS기술적 보안 운영 적용. - 물리적 보안: CCTV, 출입카드, 기업정보, VDI, SBC, 망분리 적용.
유지 보수	정기/비정기 훈련	- 1년 2회 정기 비정기 훈련 및 Simulation Test를 통해, 문제점 및 개선사항을 체크리스트 중심으로 적용한다. (공격자 마인드 점검)
	문제점 개선단계	- 체크리스트의 사이버 보안 위협 및 취약점을 개선한다. - 보안 위협 및 취약점을 개선 보안과 관련된 위험을 분석한다.

ITPE 기술사회
제132회 정보처리기술사 기출문제 해설집

대 상 정보관리기술사, 컴퓨터시스템응용기술사, 정보통신기술사, 정보시스템감리사 시험
발행일 2024년 01월 27일
집 필 강정배PE, 전일PE, 안경환PE, 안수현PE, 오준식PE, 김훈찬PE
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
연락처 070-4077-1267 / itpe@itpe.co.kr