



제 138 회 대비 ITPE Final Round 해설집

(2일차)

2026.02.01



ICT 기술사, 감리사, PMP, SW No1.

기술사 포탈 <http://itpe.co.kr> | 국내최대 1위 커뮤니티 <http://cafe.naver.com/81th>

ITPE 제138회 대비 Final Round

[2 일차] - 2026. 02. 01(일)

제 2 교시 (시험시간: 100 분)

분야	정보통신 자격 종목	정보관리 컴퓨터 시스템 응용	수검 번호		성명	
----	------------------	--------------------	----------	--	----	--

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

1. 최근 정부에서 '세계 최강의 AI 인프라'를 국가전략으로 제시하며 AI 데이터센터 건설을 통한 'AI 고속도로' 구축을 핵심 국정과제로 추진하고 있어 AI 데이터센터의 중요성이 나날이 증대되고 있다. 다음에 대하여 설명하시오.
 - 가. AI 데이터센터의 정의 및 기존 데이터센터와의 차이점
 - 나. AI 데이터 센터 주요 기술
 - 다. AI 데이터 센터 관련 주요 이슈 및 개선 방안
2. 2025년 12월 국가정보원에서는 공공기관을 대상으로 국가·공공기관 AI 보안 가이드북을 발표하였다. 다음에 대하여 설명하시오.
 - 가. AI 시스템 수명주기에 따른 주요 보안 위협
 - 나. AI 시스템 구축 유형 별 보안 대책 사항"
3. 데이터모델링(Data Modeling)의 개념 및 단계, 각 단계 별 주요 절차에 대하여 설명하시오.
4. 최근 AI의 활용성 증대 기술로 MCP(Model Context Protocol)와 A2A(Agent to Agent) Protocol 도입이 증가하고 있다. 이와 관련하여 다음을 설명하시오.
 - 가. MCP 와 A2A 의 개념
 - 나. MCP 보안위협 및 대응방안
 - 다. A2A 보안위협 및 대응방안

5. 시스템 규모산정은 프로젝트의 일정과 예산을 수립하기 위한 중요한 요소이다.

규모산정과 관련하여 다음을 설명하시오.

- 가. 소프트웨어 규모 산정 방법
- 나. 정보시스템 하드웨어 규모산정 지침 (TTAKIKO-10.0292/R3)에 따른 하드 웨어 규모산정 방법 3 가지
- 다. 인공지능(AI) 도입 방식에 의한 소프트웨어 개발비 대가산정 절차

[정보관리기술사 선택문제]

6. 정보시스템 구축/재구축을 위한 예산 요구를 위해서는 ISP-ISMP 수립 공통가이드에 따라 ISP 또는 ISMP를 사전에 수립하여야 한다. ISP 및 ISMP 수립 공통가이드는 지속적인 개정을 거쳐 2025년 5월 9판이 배포됐고, 12월 일부 개정됐다. 아래 항목에 대해 설명하시오.

- 가. ISP(Information Strategy Plan) 개념과 ISP-ISMP 수립 공통가이드 9판 변경내역
- 나. ISP-ISMP 수립 제외 가능 유형 및 ISP-ISMP 검토 주요 내용
- 다. 소규모 정보시스템 구축 사업계획 수립 절차"

[컴퓨터시스템응용기술사 선택문제]

6. 선점형 CPU 스케줄링 알고리즘인 RR(Round-Robin)에 대하여 설명하고 아래 표에 따른 각 프로세스들의 종료 시간(Finish time)과 응답 시간 (response time, turnaround time)을 계산하시오.

단, Time quantum 은 2 이며, 프로세서가 시간 0에 시작한다고 가정하고 운영체제로 인한 오버헤드는 무시한다.

Process ID	Arrival Time	Processing Time
P1	0	3
P2	1	7
P3	3	2
P4	5	5
P5	6	3

01	AI 데이터센터		
문제	<p>최근 정부에서 '세계 최강의 AI 인프라'를 국가전략으로 제시하며 AI 데이터센터 건설을 통한 'AI 고속도로' 구축을 핵심 국정과제로 추진하고 있어 AI 데이터센터의 중요성이 나날이 증대되고 있다. 다음에 대하여 설명하시오.</p> <p>가. AI 데이터센터의 정의 및 기존 데이터센터와의 차이점 나. AI 데이터 센터 주요 기술 다. AI 데이터 센터 관련 주요 이슈 및 개선 방안</p>		
도메인	디지털서비스	난이도	상 (상/중/하)
키워드	Energy production, AI computing hardware, Support infrastructure, AI cloud services, 연산, 네트워크, 메모리, 스토리지, 전력, 소프트웨어, 데이터 관리, 운영, 보안		
출제배경	전 세계적으로 AI 데이터센터 확보 경쟁이 국가 전략으로 부상함에 따라 토픽 이해 확인		
참고문헌	AI 데이터센터 동향과 시사점 – SPRi(2025.07)		
출제자	정상반멘토 이상현 기술사(제 118회 정보관리기술사 / bluesanta97@naver.com)		

I. AI 워크로드 지원, AI 데이터센터의 정의 및 기존 데이터센터와의 차이점

가. AI 데이터센터의 정의

정의	<ul style="list-style-type: none"> - 대규모 AI 모델의 학습과 추론을 위해 고성능 AI 전용 하드웨어와 초저지연 네트워크, 첨단 냉각 및 전력 관리 시스템을 통합하여 AI 워크로드에 최적화된 고밀도 컴퓨팅 인프라를 갖춘 데이터센터 	
구성요소	Energy production	<ul style="list-style-type: none"> - 소형 모듈 원자로, 핵융합, 지열 에너지, 그리드 저장 공급자 등이 포함되어 AI 데이터센터 운영의 에너지 기반 제공
	AI computing hardware	<ul style="list-style-type: none"> - AI 학습 프로세서, AI 추론 프로세서, 슈퍼컴퓨팅 등 AI 연산에 특화된 하드웨어 포함
	Support infrastructure	<ul style="list-style-type: none"> - 데이터센터 액체 냉각, 데이터센터 냉각, 에너지 최적화 소프트웨어 등 효율적 운영을 위한 첨단 기술과 시스템 포함
	AI cloud services	<ul style="list-style-type: none"> - 클라우드 AI 보안, 클라우드 GPU 등을 통해 최종 AI 서비스와 사용자 경험을 지원

나. 기존 데이터센터와의 차이점

구분	기존 데이터센터	AI 데이터센터
주요 목적	- 일반 IT 서비스 및 웹 애플리케이션 지원	- AI 모델 학습 및 추론 등 고성능 연산 지원
연산 자원	- 주로 CPU 중심	- 고성능 GPU, TPU 등 AI 전용 반도체 중심
전력 밀도	- 상대적으로 낮음	<ul style="list-style-type: none"> - 매우 높음 - 고밀도 GPU 서버 운영에 최적화
냉각 시스템	- 공기 냉각 위주	- 액체 냉각, 물입식 냉각 등 첨단 냉각 기술 적용
네트워크	- 표준 고속 네트워크	- 초저지연 고대역폭 네트워크 필요

운영 최적화	- 일반 서버 및 스토리지 관리	- AI 워크로드 특화 분산처리 및 자원 최적화
- AI 데이터센터는 기존 데이터센터와 달리 AI 워크로드의 특성에 맞추어 고성능 GPU와 전용 냉각·전력 시스템을 갖추어 대규모 연산과 고밀도 작업을 효율적으로 처리		

II. AI 데이터 센터 주요 기술

가. 연산, 네트워크, 메모리·스토리지 측면 주요 기술

구분	핵심 기술	설명
연산	- AI 가속기	- GPU, NPU, TPU, ASIC 기반 대규모 병렬 연산
	- 이기종 컴퓨팅	- 서로 다른 종류의 프로세서들을 하나의 시스템에 통합하여 특정 작업에 가장 적합한 처리 장치를 사용해 성능과 에너지 효율을 최적화하는 기술
	- 병렬 처리 구조	- 여러 개의 프로세서나 코어를 사용해 여러 작업을 동시에 실행하여 컴퓨터 성능을 높이는 구조
네트워크	- 고속 인터커넥트	- NVLink, Infinity Fabric 등 데이터를 빠르고 효율적으로 전달하는 기술
	- 고대역폭 네트워크	- 일정 시간 내에 대량의 데이터를 매우 빠르게 전송할 수 있는 통신 연결 방식. InfiniBand, RoCE 등
	- 저지연 통신	- 데이터 전송 시작부터 수신 완료까지 걸리는 시간이 매우 짧은 통신 환경. RDMA 기반 GPU 간 통신
메모리, 스토리지	- 고대역폭 메모리	- 여러 개의 DRAM을 수직으로 쌓아 올리고 '실리콘 관통 전극 (TSV)' 기술로 연결해 초고속, 대용량 데이터 처리가 가능한 3D 스택(Stack) 방식의 고성능 메모리
	- 계층형 메모리	- 속도, 용량, 가격의 균형을 맞추기 위해 여러 종류의 저장 장치를 층(Layer)처럼 쌓아 올린 메모리(HBM-DRAM-Nvme SSD)
	- 병렬 스토리지	- 대규모 데이터를 여러 저장 장치에 분산하여 동시에 읽고 쓰는 스토리지. Lustre, GPFS, Object Storage 등

나. 전력, SW, 데이터관리, 운영·보안 측면 주요 기술

구분	핵심 기술	설명
전력	- 고전력 밀도 대응	- 열 관리 효율 극대화, 전력 변환 효율 향상, 그리고 첨단 소재 및 설계 기술
	- 냉각 기술	- 고밀도 Rack의 하드웨어 온도 제어를 위해 CPU 등 열 발생 부품 또는 장비에 냉각된 액체를 순환시키는 데이터센터 냉각 방식 - 랙 기반 냉각, 칩 직접 냉각, 액침 냉각, 공기 보조 수랭
	- 전력 스케줄링	- 전력 수요 예측 및 공급 제어를 통해 전력 시스템의 효율성을 최적화하는 기술
소프트웨어	- AI 프레임워크	- AI 모델의 개발, 트레이닝 및 배포를 위한 구조화된 환경을 조성하는 도구, 라이브러리 및 기능의 집합(PyTorch, TensorFlow 등)

	- Kubernetes	- 컨테이너화된 애플리케이션을 자동 배포, 스케일링 및 관리 기술
	- 컴파일 기술	- NVIDIA GPU를 위한 범용 병렬 컴퓨팅 플랫폼 및 프로그래밍 모델 컴파일 기술
데이터 관리	- 데이터 파이프라인	- 여러 소스에서 발생하는 데이터를 자동으로 수집, 변환, 처리하여 분석이나 저장, 활용이 가능한 형태로 만드는 일련의 자동화된 시스템 및 프로세스
	- 고속 데이터 로딩	- 보조 저장 장치에 있는 프로그램이나 대량의 데이터를 주기억장치로 매우 빠른 속도로 옮기는 기술(예: 병렬 I/O, Prefetch..)
	- 데이터 거버넌스	- 조직의 데이터를 안전하고 정확하며 효율적으로 관리하기 위한 정책, 프로세스, 표준을 정의하고 실행하는 체계
운영	- 고가용성 기술	- 시스템 장애 발생 시에도 서비스 중단을 최소화하고 지속적인 운영을 보장하기 위한 기술
	- 운영 자동화	- AIOps 기반 모니터링으로 IT 운영 데이터를 분석하고 IT 인프라 및 애플리케이션 성능 관리 및 문제 해결 자동화
보안	- Zero Trust	- 내부 외부를 구분 없이 모든 접근을 잠재적 위협으로 간주하고 지속적인 인증과 권한 확인을 통해 최소한의 접근 권한만 부여하는 보안 모델

- 간글을 적는 란입니다. 표의 첫 번째 구간은 세로 정렬을 해주시기 바랍니다. 간글도 다른 문장과 마찬가지로 두 번째 줄 이하부터는 한 글자 띄어쓰기를 합니다. 이 부분을 그대로 카피해서 적으셔도 됩니다

III. AI 데이터 센터 관련 주요 이슈 및 개선 방안

가. AI 데이터 센터 관련 주요 이슈

구분	이슈	설명
기술·운영 이슈	- 고전력·고밀도 한계	- 고성능 GPU 처리로 인한 전력 소비 및 발열 급증
	- 공급 병목	- GPU 및 핵심 칩 공급 부족, 데이터센터 임대료 상승
	- 지정학적 리스크	- 미·중 패권 경쟁 및 반도체 수출 규제로 인한 자립성 위기
에너지·환경 이슈	- 탄소 배출 급증	- 전 세계 전력의 2% 소비, 간접 탄소배출 150% 증가 전망
	- 수자원 고갈	- 냉각수 사용량 급증에 따른 지역사회 갈등 및 정책 규제
	- 인허가 제한	- 전력 수요 과부하로 인한 신규 데이터센터 구축 제한
보안·거버넌스 이슈	- 사이버 보안	- 대량의 민감 데이터 및 AI 모델 타깃 공격 위험
	- 데이터 주권	- 국경 간 데이터 이동에 따른 지식재산권 및 개인정보 보호 문제
	- 규제 강화	- EU AI법(AI Act) 등 고위험 AI 서비스에 대한 기술적 통제 요구

- AI 데이터센터는 열과의 전쟁을 해결하기 위한 여러 기술과 전력 해소를 위한 방안, 보안 측면 데이터 영토 확보를 위한 법적 장치 마련에 힘쓰고 있음

나. AI 데이터 센터 개선 방안

구분	방안	설명
전략 및 협력 체계	- 특별구역 지정	- 인프라 접근성 보장 및 계획 승인 절차 완화로 민간투자 유도
	- 삼각 협력 모델(PPP)	- '공공-민간-학계' 협력을 통한 R&D, 실증, 인력양성 통합 추진
	- 전문 인재 양성	- 냉각·에너지 관리 등 융합기술 교육 및 채용 연계형 프로그램 확대
에너지 및 기술 혁신	- 에너지 혁신	- 소형 모듈 원전(SMR), 태양광·풍력 단지와 데이터센터 부지 연계
	- 차세대 냉각 기술	- 액체냉각, 폐열 회수 및 재활용 기술(R&D) 지원 강화
	- 에너지 효율 관리	- PUE(전력효율지수) 기준 도입 및 국가 차원의 배출량 모니터링 체계 구축
투자 및 법·제도	- 인센티브 다양화	- 전기료·지방세 감면 외 '신재생 에너지 사용 인센티브' 신설
	- 법적 틀 마련	- AI 기본법 내 데이터센터 지원 및 데이터 주권 조항 명시
	- 규제 완화	- 신속검토제 도입 및 환경영향평가 간소화, 'AI 데이터센터 지원 컨소시엄' 구성

- 세계 주요국 모두 AI 데이터 센터 등 AI 인프라 경쟁에 주도권 확보를 위하여 노력 중임

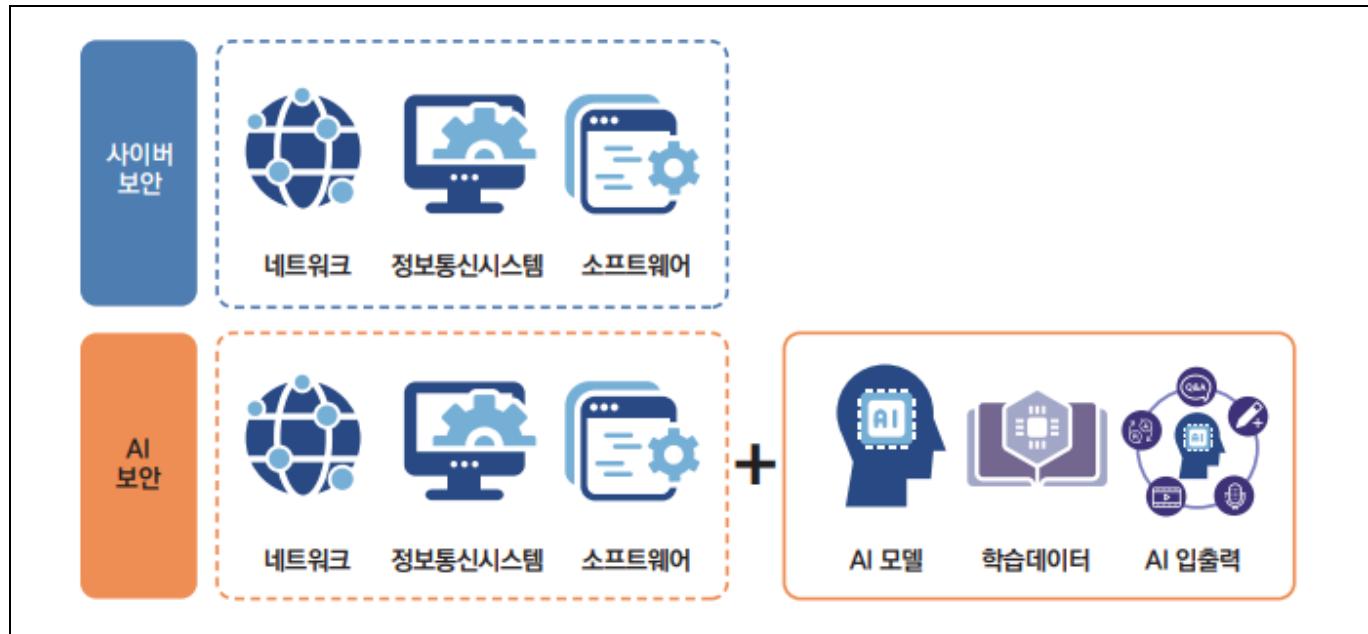
IV. 주요국 AI 데이터센터 관련 정책 동향

구분	동향	설명
미국	- 에너지 자립 가속화	- SMR(소형모듈원전) 및 핵융합 등 차세대 에너지원을 DC 전용 전력망으로 연결하는 프로젝트 세액 공제 제공
	- 인허가 고속도로 구축	- 데이터센터 건설 시 환경 영향 평가 및 각종 행정 절차를 대폭 단축하는 '데이터센터 패스트트랙' 행정명령 시행
EU	- 그린 디지털 전환	- 모든 신규 AI DC에 대해 폐열 재활용 시스템 구축을 의무화, 에너지 효율(PUE) 기준을 미달할 경우 운영을 제한하는 강력한 환경 규제와 보조금 병행
	- 데이터 주권 및 로컬 DC	- 유럽 내 자본과 기술로 구축된 '소버린(Sovereign) AI DC' 유치 시 추가적인 재정 지원 및 세제 혜택 부여
중국	- 동수서산(東數西算) 심화	- 동부 도시의 데이터를 서부의 풍부한 재생에너지(태양광, 풍력) 거점으로 보내 처리하는 국가망을 완성
	- AI 컴퓨팅 자립화	- 국산 GPU 기반의 데이터센터 구축을 공공 부문부터 의무화하고, 자체 컴퓨팅 생태계(화웨이, 바이두 등) 확장을 전폭 지원
한국	- 분산에너지 활성화	- 지역으로 이전하는 DC에 전력 계통 접속 우선권을 부여하고, 지역별 차등 전기요금제를 통해 비수도권 유치 유도
	- K-클라우드 프로젝트	- 국산 AI 반도체(NPU)를 적용한 '저전력·고효율 AI 데이터센터' 실증 사업을 확대하여 외산 GPU 의존도를 낮추고 토종 AI 인프라 경쟁력 강화

"끌"

02	국가 · 공공기관 AI보안 가이드북		
문제	<p>2025년 12월 국가정보원에서는 공공기관을 대상으로 국가 · 공공기관 AI보안 가이드북을 발표하였다. 다음에 대하여 설명하시오.</p> <p>가. AI시스템 수명주기에 따른 주요 보안 위협 나. AI시스템 구축 유형 별 보안 대책 사항</p>		
도메인	보안	난이도	상 (상/중/하)
키워드	데이터 수집, AI 학습, AI시스템 구축, AI시스템 운영, AI시스템 폐기, T01~T15		
출제배경	공공기관 AI 도입에 따른 다양한 보안 위협 대책을 위한 가이드북 이해 확인		
참고문헌	국가 · 공공기관 AI보안 가이드북 – 국가정보원(2025.12)		
출제자	정상반멘토 이상현 기술사(제 118회 정보관리기술사 / bluesanta97@naver.com)		

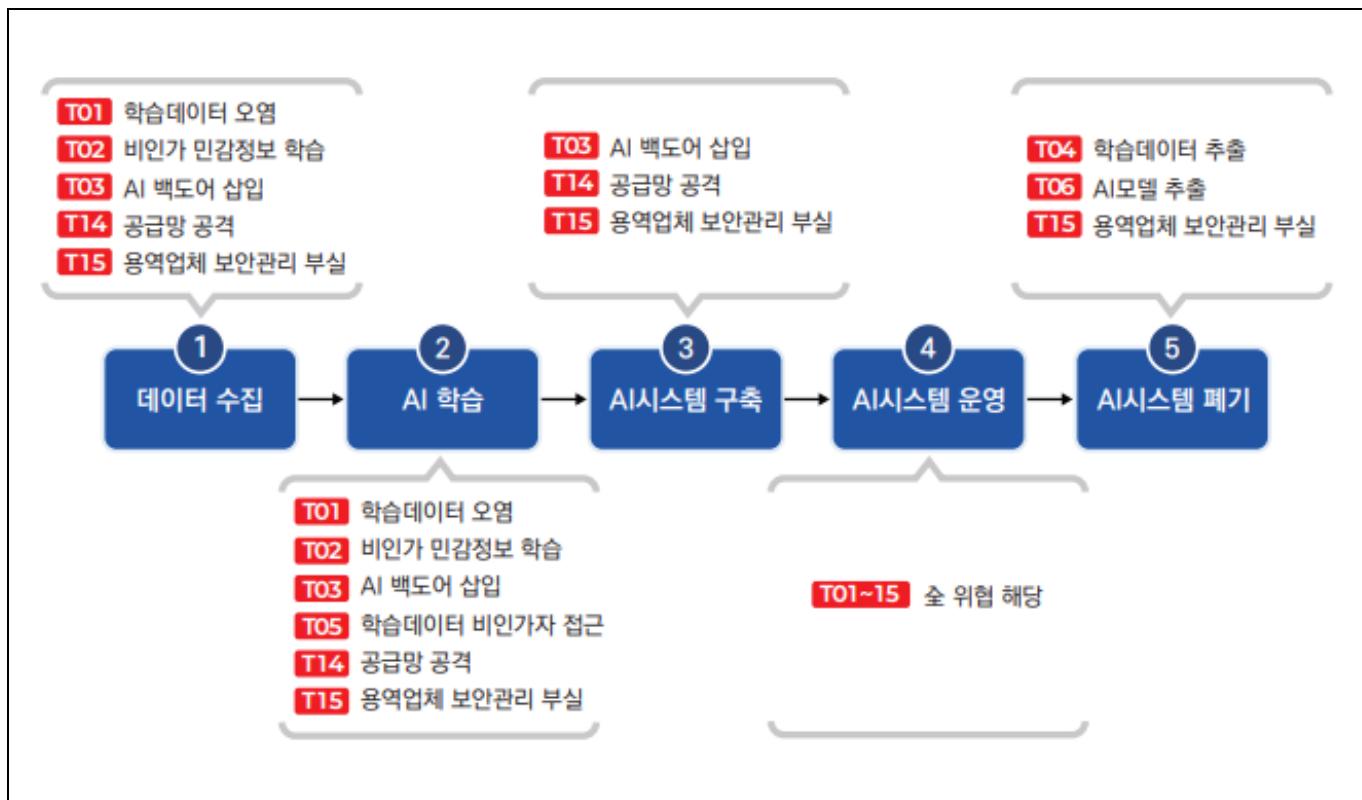
I. 사이버 보안과 AI 보안의 개요



- AI시스템 보안위협은 전통적인 사이버보안 위협과 함께 AI모델, 학습데이터, 입·출력데이터 등에 대한 위협까지 포함
- 모델·데이터에 대한 변조·악성행위가 전체 AI시스템의 보안성·안전성·신뢰성에 심각한 영향, 全 수명주기에 걸친 보안위협을 인지하고 대비 필요

II. AI시스템 수명주기에 따른 주요 보안 위협

가. AI시스템 수명주기에 따른 주요 보안 위협



나. AI시스템 수명주기에 따른 주요 보안 위협 상세 설명

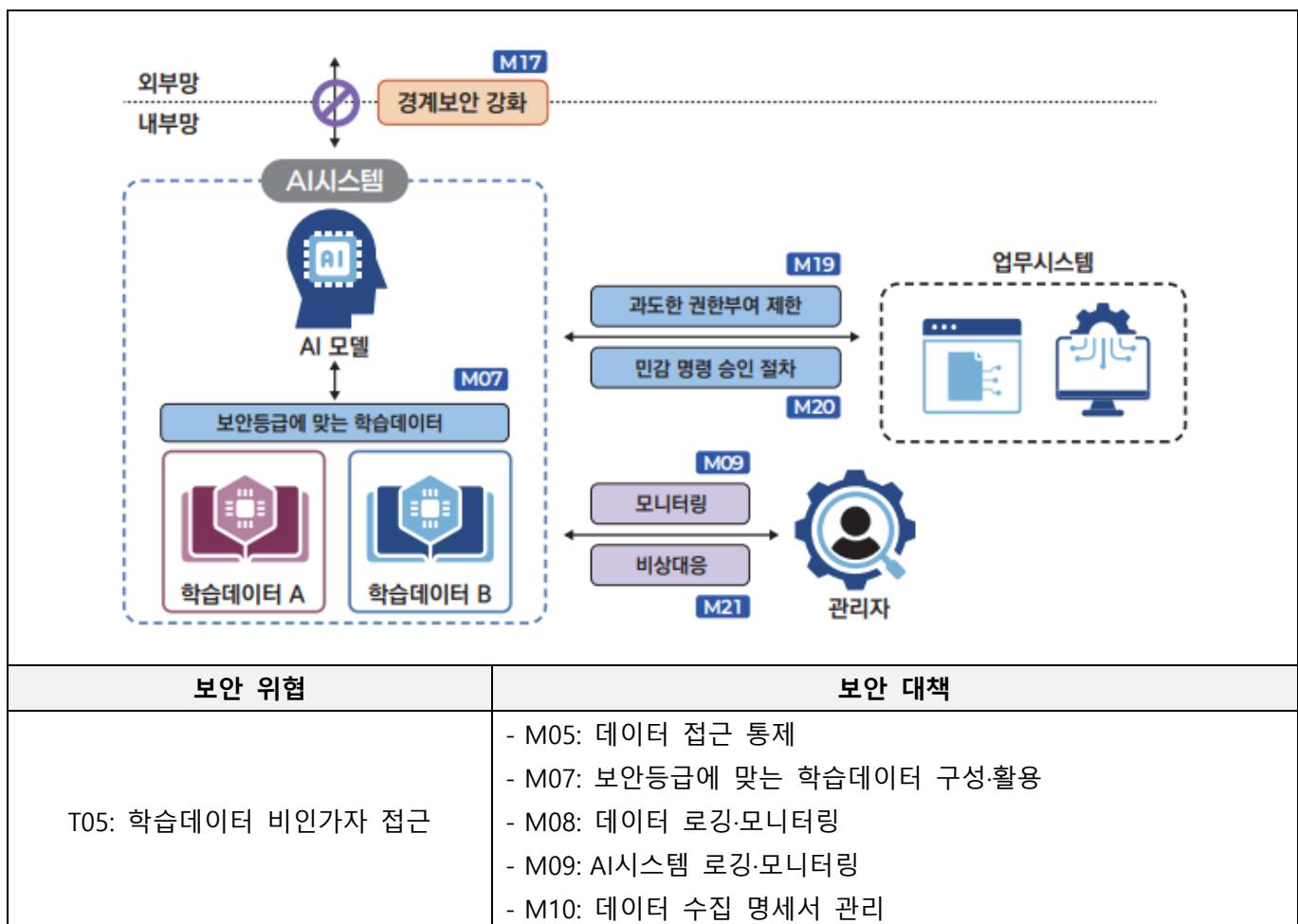
수명주 기	보안위협	설명
데이터 수집	- T01: 학습데이터 오염	- 외부에서 유입된 데이터에 변조된 정보 포함
	- T02: 비인가 민감정보 학습	- 학습데이터에 비인가 민감정보 삽입
	- T03: AI 백도어 삽입	- 학습데이터에 AI 백도어 포함
	- T14: 공급망 공격	- 외부 AI모델, 벡터DB용 데이터에 악성코드 은닉
	- T15: 용역업체 보안관리 부실	- 용역업체를 통한 수집단계 보안위협 발생AI
AI 학습	- T01: 학습데이터 오염	- 외부에서 유입된 데이터에 변조된 정보 포함
	- T02: 비인가 민감정보 학습	- 학습데이터에 삽입된 비인가 민감정보 학습
	- T03: AI 백도어 삽입	- AI가 학습데이터에 포함된 AI 백도어를 학습
	- T05: 학습데이터 비인가자 접근	- 비인가자가 학습데이터에 무단 접근
	- T14: 공급망 공격	- 외부 AI모델, 벡터DB용 데이터에 악성코드 은닉
	- T15: 용역업체 보안관리 부실	- 용역업체를 통한 수집단계 보안위협 발생AI
AI 시스템 구축	- T03: AI 백도어 삽입	- 오픈소스 라이브러리 등에 AI 백도어 은닉
	- T14: 공급망 공격	- 외부 AI모델, 벡터DB용 데이터에 악성코드 은닉
	- T15: 용역업체 보안관리 부실	- 용역업체를 통한 구축단계 보안위협 발생
AI 시스템	- T03: AI 백도어 삽입	- AI모델을 로드·실행하는 단계에 백도어 삽입
	- T04: 학습데이터 추출	- 반복된 질의를 통한 학습데이터를 재구성·추출

운영	- T05: 학습데이터 비인가자 접근	- 비인가자가 학습데이터에 무단 접근
	- T06: AI 모델 추출	- AI모델 구조 혹은 가중치 등 AI모델 주요 정보 추출
	- T07: 민감정보 입력·유출	- 사용자가 AI에 민감정보를 입력하여 유출
	- T08: 프롬프트 인젝션	- 악의적인 프롬프트를 입력, AI 출력·동작 변경
	- T09: 회피 공격	- 입력정보를 조작하여 AI의 오판을 유도
	- T10: 통신구간 공격	- 사용자-AI시스템 통신구간에서 정보 탈취
	- T11: 서비스 거부 공격	- AI에 과도한 입력을 발생, 과부하 유발
	- T12: 사고·이상행위 모니터링 체계부재	- 실시간 공격 탐지·모니터링 부재
	- T13: AI시스템 권한관리 부실	- 과도한 권한을 가지고 AI가 임의로 타 시스템 조작
	- T14: 공급망 공격	- 최신 기능·데이터 업데이트 시 악성코드 유입
	- T15: 용역업체 보안관리 부실	- 용역업체를 통한 운영단계 보안위협 발생
	- T04: 학습데이터 추출	- 폐기단계에서 보안관리 부실로 학습데이터 추출
	- T06: AI 모델 추출	- 폐기단계에서 보안관리 부실로 AI모델 추출
	- T15: 용역업체 보안관리 부실	- 용역업체를 통한 폐기단계 보안위협 발생
AI 시스템 폐기	- 운영단계에서 지속적인 데이터 수집 및 재학습을 수행하는 경우 T01, T02의 보안 위협에도 지속 노출	

- 운영단계에서 지속적인 데이터 수집 및 재학습을 수행하는 경우 T01, T02의 보안 위협에도 지속 노출

III. AI시스템 구축 유형 별 보안 대책 사항

가. 내부 전용 AI 시스템 보안 대책



T13: AI시스템 권한관리 부실	<ul style="list-style-type: none"> - M09: AI시스템 로깅·모니터링 - M11: AI시스템 구성요소 명세서 관리 - M17: AI시스템 경계보안 강화 - M19: 과도한 권한 부여 제한 - M20: 민감 명령 승인 절차 마련 - M21: 비상대응 체계 마련 - M22: 설명 가능한 AI 구성 - M23: AI모델 대상 적대적 모의공격 수행 - M24: AI모델에 적대적 공격유형 학습
--------------------	--

- 내부망 전용 AI시스템은 외부망과 연계되지 않은 내부망에서만 운영하여 상대적으로 높은 보안성을 유지하나, 연계등의 목적으로 운영하여 이로 인한 보안위협을 대응해야 함

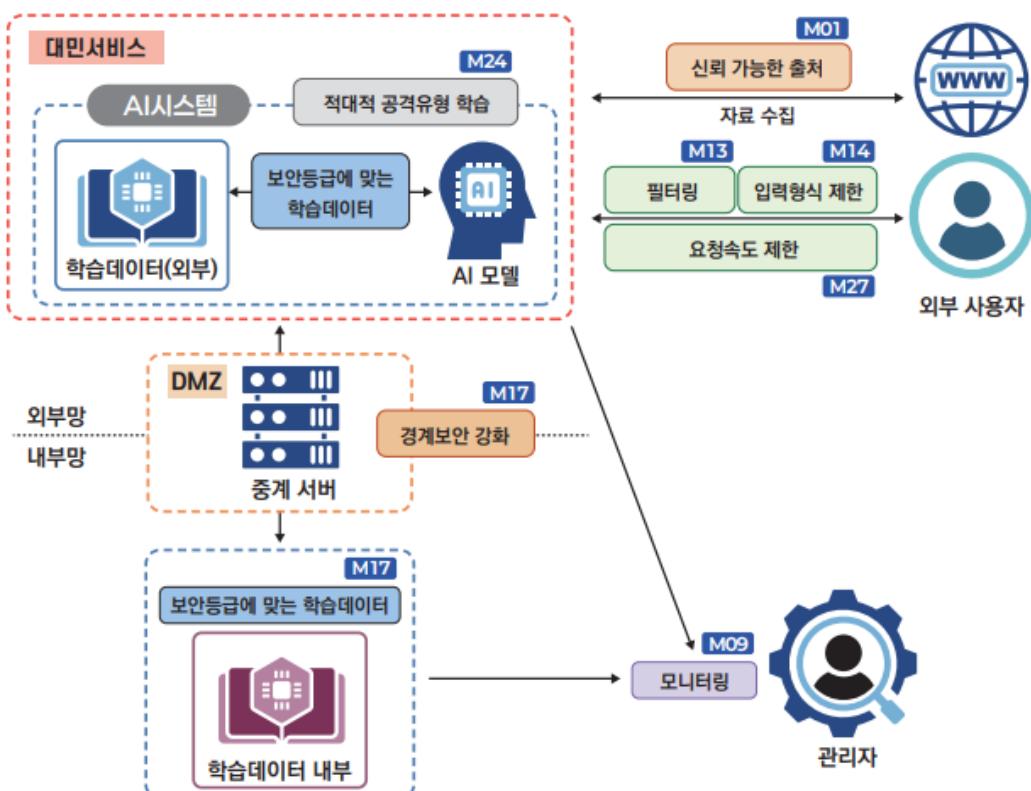
나. 내부업무용 AI시스템의 외부망 연계

보안 위협	보안 대책
T01: 학습데이터 오염	<ul style="list-style-type: none"> - M01: 신뢰할 수 있는 출처의 데이터 활용 - M03: 데이터 검사 / M04: 데이터 암호화 - M05: 데이터 접근통제 / M08: 데이터 로깅·모니터링 - M10 데이터 수집 명세서 관리 / M29: 용역업체 보안관리
T02: 비인가 민감정보 학습	<ul style="list-style-type: none"> - M03: 데이터 검사 / M06: 민감정보 사용 사전 승인 - M07: 보안등급에 맞는 학습데이터 구성·활용 - M29: 용역업체 보안관리

T03: AI 백도어 삽입	- M01: 신뢰할 수 있는 출처의 데이터 활용 - M02: 신뢰할 수 있는 출처의 AI모델 등 활용 / M03: 데이터 검사 - M09: AI시스템 로깅·모니터링 / M10: 데이터 수집 명세서 관리 - M11: AI시스템 구성요소 명세서 관리 - M12: AI시스템 구성요소 무결성 검증 - M22: 설명 가능한 AI 구성 - M23: AI모델 대상 적대적 모의공격 수행 - M26: AI모델 복구 M29 용역업체 보안관리
T06: AI모델 추출	- M16 AI모델 구조·가중치 유출 방지 / M17: AI시스템 경계보안 강화 - M28: AI시스템 구성요소 완전 삭제 / M29: 용역업체 보안관리

- 내부업무용 AI시스템에 최신 데이터를 학습하거나, 기능 확장 및 결과물 활용 등을 목적으로 기관 내부망을 외부망과 연계하는 유형

다. 대민서비스용 AI시스템의 내부망 연계

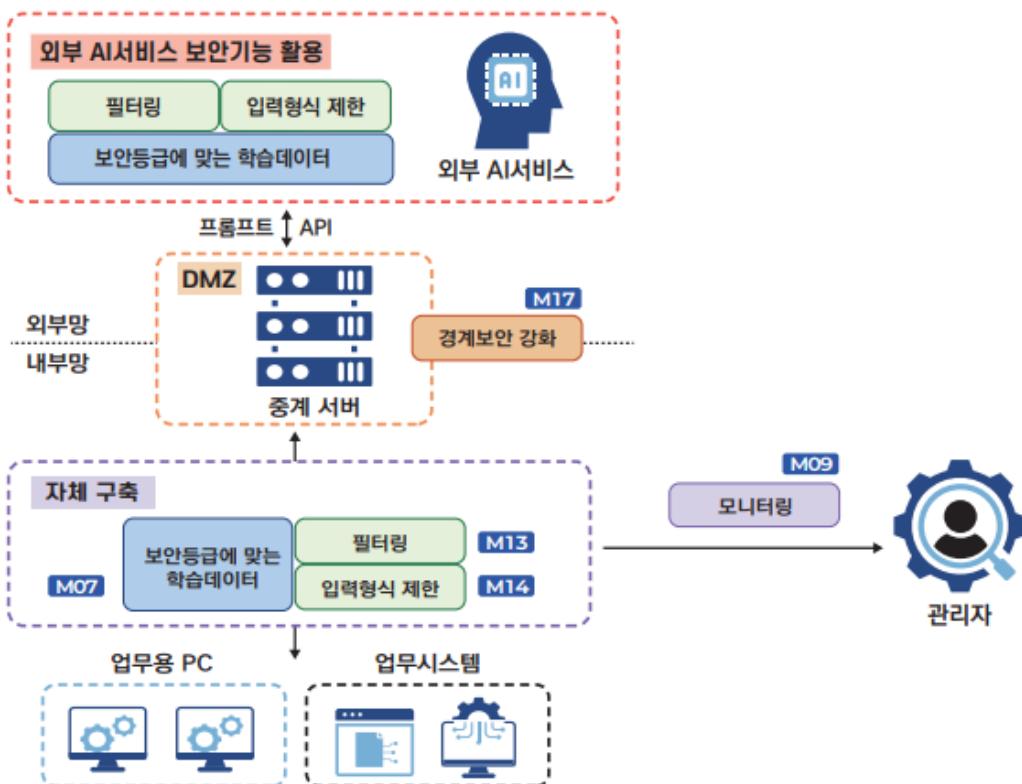


보안 위협	보안 대책
T04: 학습데이터 추출	- M05: 데이터 접근통제 / M08: 데이터 로깅·모니터링 - M09: AI시스템 로깅·모니터링 / M14: 입력 길이·형식 제한 - M15: 가드레일 다중화
T07: 민감정보 입력·유출	- M06: 민감정보 사용 사전 승인 - M07: 보안등급에 맞는 학습데이터 구성·활용 - M09: AI시스템 로깅·모니터링 / M13: 입·출력 필터링

	<ul style="list-style-type: none"> - M14: 입력 길이·형식 제한 / M15: 가드레일 다중화 - M18: AI시스템 통신구간 보호
T08: 프롬프트 인젝션	<ul style="list-style-type: none"> - M09: AI시스템 로깅·모니터링 / M13: 입·출력 필터링 - M14: 입력 길이·형식 제한 / M15: 가드레일 다중화 - M22: 설명 가능한 AI 구성 - M23: AI모델 대상 적대적 모의공격 수행 - M24: AI모델에 적대적 공격유형 학습
T10: 통신구간 공격	<ul style="list-style-type: none"> - M17: AI시스템 경계보안 강화 / M18: AI시스템 통신구간 보호 - M25: AI시스템 구성요소 취약점 점검 및 업데이트
T11: 서비스 거부 공격	<ul style="list-style-type: none"> - M09: AI시스템 로깅·모니터링 / M14: 입력 길이·형식 제한 - M27: 요청 속도 제한

- 불특정 다수의 AI시스템 대상 적대적 공격에 대한 대비가 필요

라. 상용 AI서비스 활용

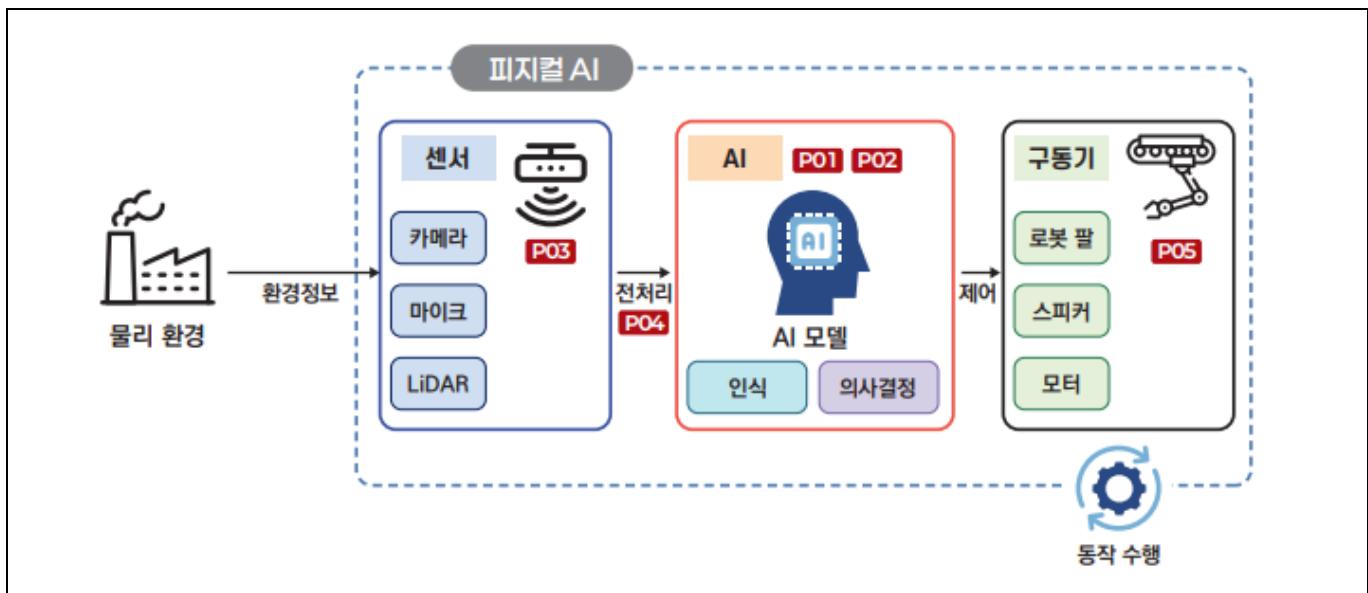


보안 위협	보안 대책
T07: 민감정보 입력·유출	<ul style="list-style-type: none"> - M06: 민감정보 사용 사전 승인 - M07: 보안등급에 맞는 학습데이터 구성·활용 - M09: AI시스템 로깅·모니터링 / M13: 입·출력 필터링 - M14: 입력 길이·형식 제한 / M15: 가드레일 다중화 - M18: AI시스템 통신구간 보호 - M30: 사용자 교육 및 보안정책 수립

T10: 통신구간 공격	- M17: AI시스템 경계보안 강화 / M18: AI시스템 통신구간 보호 - M25: AI시스템 구성요소 취약점 점검 및 업데이트
T15: 용역업체 보안관리 부실	- M29: 용역업체 보안관리

- 상용 AI서비스에 기관의 민감정보가 노출되거나 학습될 수 있는 만큼 주요 위협을 중점 검토하고 대비

IV. 피지컬 AI시스템 보안대책



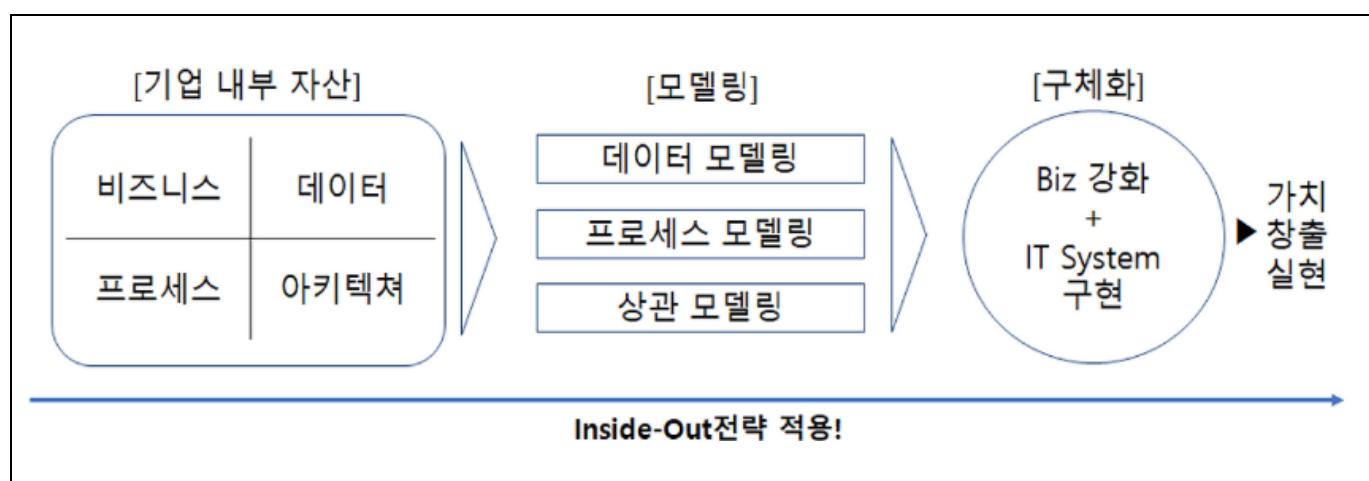
보안 위협	보안 대책
P01: AI 백도어 삽입, 오동작 및 잘못된 행동 수행	- P-M01 데이터 검사 - P-M02 AI모델 대상 적대적 모의공격 수행
P02: 피지컬 AI 과다 연산 유도, 자원 과부하	- P-M05 안전모드 동작 - P-M09 피지컬 AI 로깅·모니터링
P03: 회피 공격	- P-M03 AI모델에 적대적 공격유형 학습 - P-M09 피지컬 AI 로깅·모니터링
P04: 센서정보 전처리 과정 공격, 오동작 유발	- P-M07 센서 입력 범위 설정 - P-M08 피지컬 AI 통신구간 보호
P05: 외부 공격으로 인한 피지컬 AI의 물리적 안전 위협	- P-M04 과도한 권한 부여 제한 - P-M05 안전모드 동작 - P-M06 하드웨어 보안성 강화 - P-M10 비상대응 체계 마련

- 피지컬 AI가 승인되지 않은 행위를 하거나 잘못된 판단으로 인한 안전사고를 유발할 수 있는 만큼, 안전모드 탑재 및 비상대응 체계 마련 등을 통해 보안위협에 대응하여야 함

“끝”

03	데이터모델링(Data Modeling)		
문제	데이터모델링(Data Modeling)의 개념 및 단계, 각 단계 별 주요 절차에 대하여 설명하시오.		
도메인	데이터베이스	난이도	하 (상/중/하)
키워드	요구사항 수집, 개념 모델링, 논리 모델링, 물리 모델링		
출제배경	기본 토픽인 데이터베이스 모델링에 대한 이해 확인		
참고문헌	ITPE 서브노트		
출제자	정상반멘토 이상현 기술사(제 118회 정보관리기술사 / bluesanta97@naver.com)		

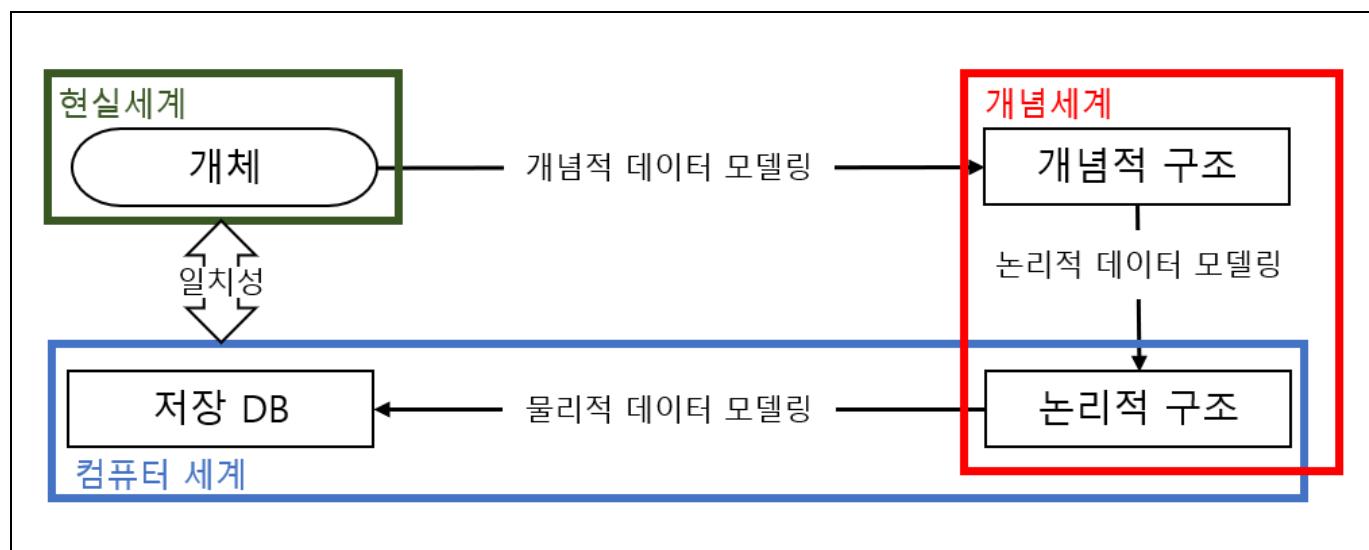
I. 현실세계 비즈니스 모델링의 필요성



- 복잡한 현실세계를 이해하기 쉬운 형태로 변환하기 위해 단순화, 추상화, 구조화, 가시화하는 모델링 이용
- 기업의 비즈니스, 데이터, 프로세스, 아키텍처를 가지고 모델링과정을 거쳐서 구체화함으로써 IT 시스템 구현

II. 데이터모델링(Data Modeling) 개념 및 단계

가. 데이터모델링(Data Modeling) 개념



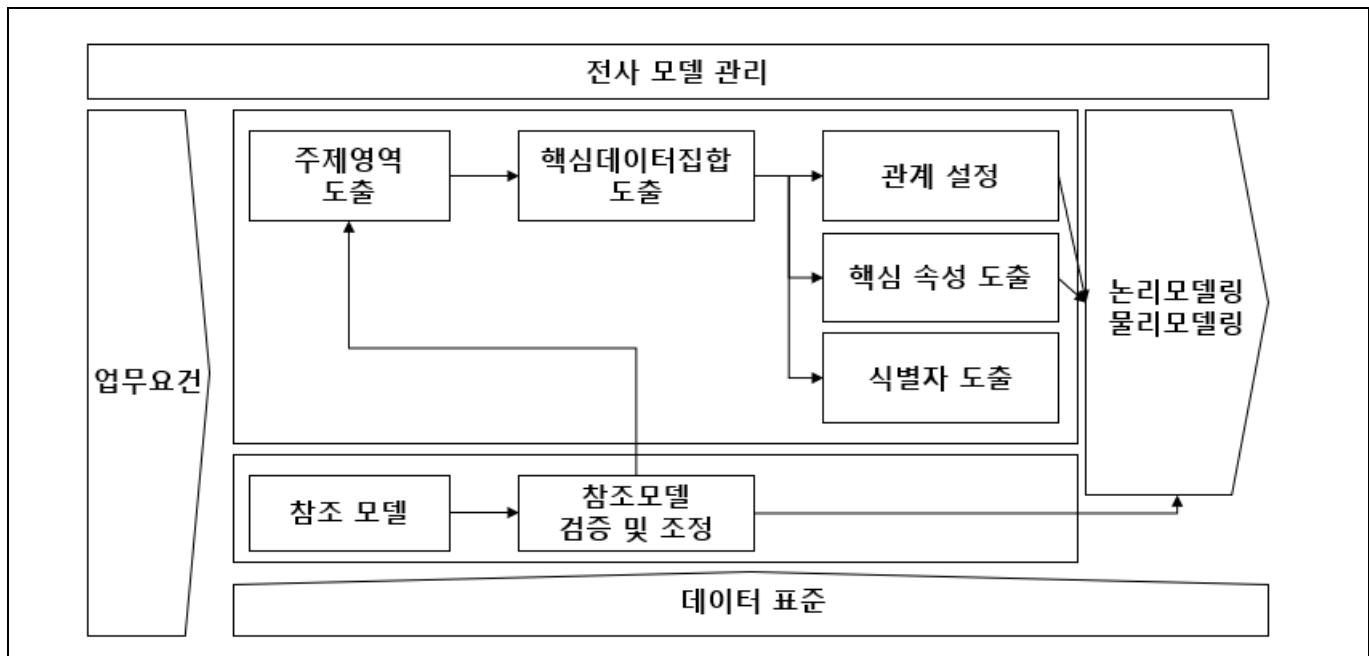
개념	- 현실 세계를 데이터베이스로 표현하기 위해서 추상화하여 정형화된 형태로 표현하기 위한 설계 과정
----	--

나. 데이터모델링(Data Modeling)의 단계

단계	설명	특징
개념 모델링	- 사용자의 요구사항을 분석하여 핵심 엔티티(Entity)와 그들 간의 관계를 정의하는 가장 높은 수준의 추상화 단계 - 비즈니스 흐름을 파악하고 데이터의 전체적인 골격을 설계함.	- 무엇(What)을 관리할지 - 중요 엔티티와 관계 설정
논리 모델링	- 개념 모델링에서 정의한 구조를 데이터베이스 저장 구조에 맞게 상세화하는 단계 - 비즈니스 정보의 논리적 구조를 확정하고 정규화를 통해 데이터 중복을 제거함	- 정규화(Normalization) - 이론적인 구조
물리 모델링	- 논리 모델을 특정 데이터베이스 관리 시스템(DBMS)의 성능과 특성에 맞춰 실제 테이블로 변환하는 단계	- 반정규화 (Denormalization)

III. 데이터모델링(Data Modeling) 각 단계 별 주요 절차

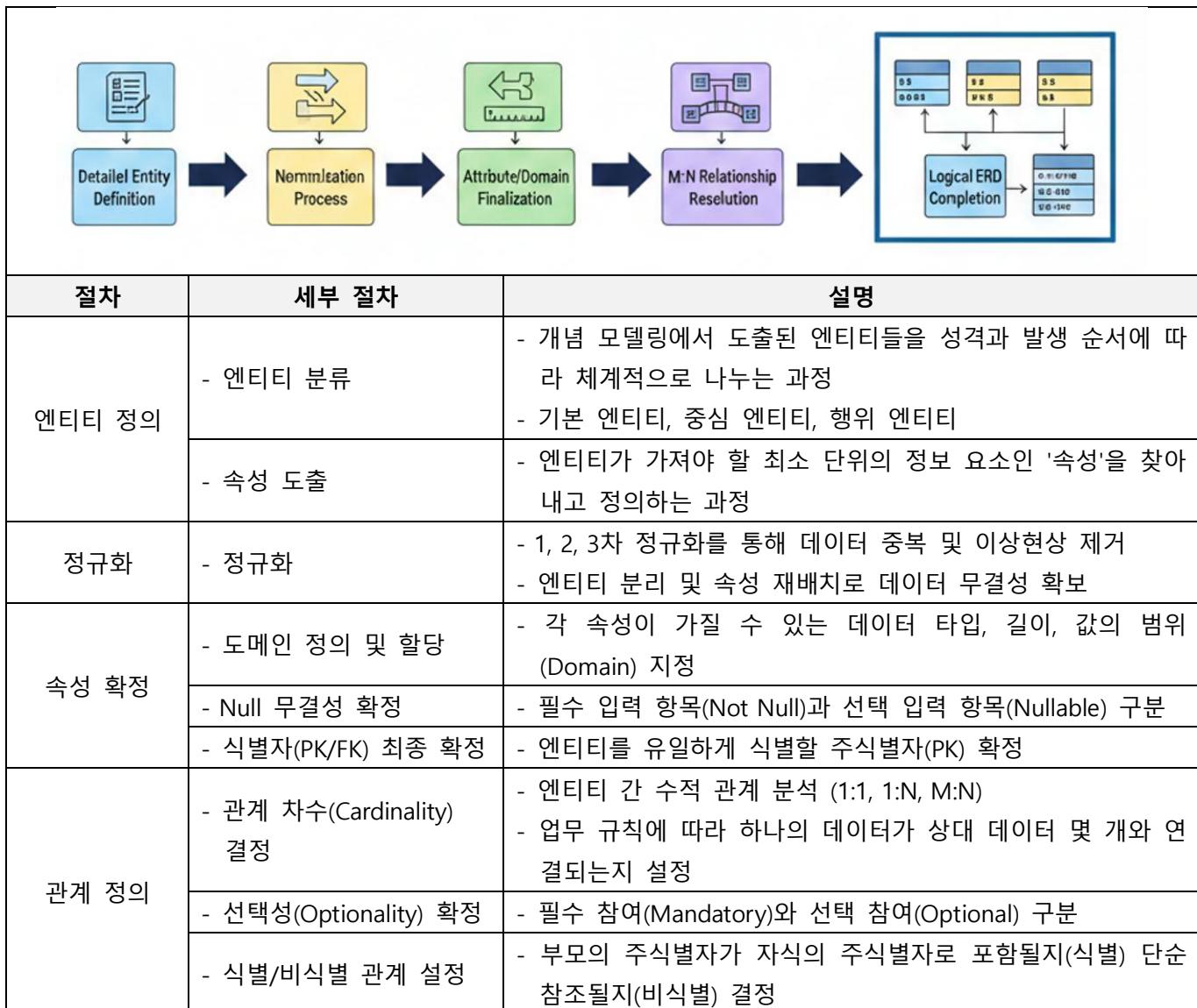
가. 개념적 모델링 주요 절차



절차	주요활동	주요 산출물
주제영역 도출	- 전체 업무 시스템을 데이터 성격에 따라 대분류 - 업무 프로세스와 데이터 간의 관계를 통해 영역 확정	주제영역 분류도
핵심 엔티티 추출	- 각 주제영역 내에서 관리해야 할 핵심 객체 추출 - 유사한 엔티티 통합 및 분리	엔티티 정의서
관계 및 속성 정의	- 엔티티 간의 관계(1:N 등) 및 필수 참여도 설정 - 핵심 속성 및 식별자 정의	개념 ERD

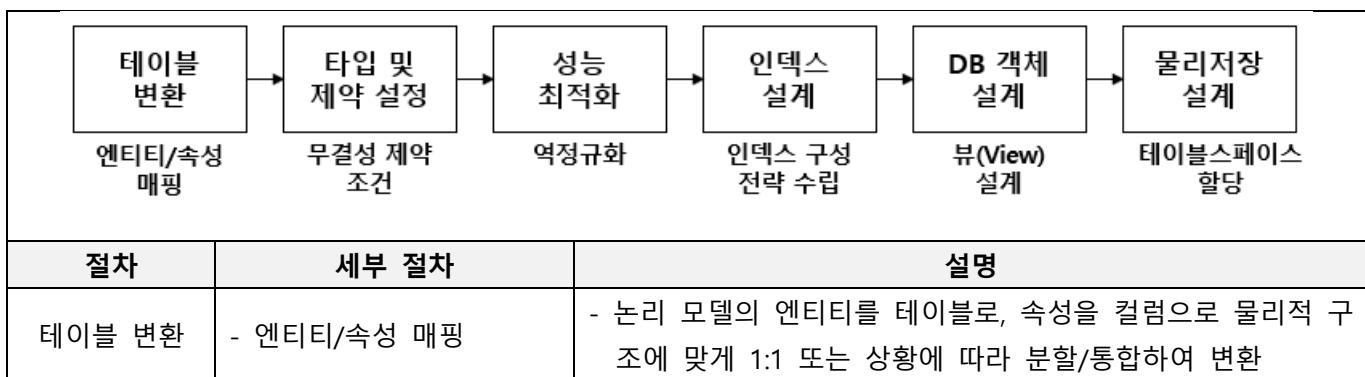
- 주제영역 간의 인터페이스를 명확히 함으로써 모델의 가독성을 높일 수 있으며 의사소통 효율화 가능.

나. 논리적 모델링 주요 절차



- 논리적 모델링에서 정의된 관계는 이후 외래키(FK)로 구현되어 데이터베이스의 물리적 구조를 형성하게 됨

다. 물리적 모델링 주요 절차



	- 물리 명명 규칙 적용	- 단어 사전 및 도메인 정의서를 바탕으로 한글명을 표준화된 영문명으로 변환
타입 및 제약 설정	- 데이터 타입/길이 지정	- 데이터의 실제 값 범위와 DBMS 특성을 고려하여 최적의 데이터 타입과 최대 길이를 정의
	- 무결성 제약조건 정의	- 기본키(PK), 외래키(FK) 확정하고 데이터 정합성을 유지하기 위한 물리적 제약사항을 설정
성능 최적화	- 역정규화 수행	- 성능 저하가 예상될 경우, 테이블을 병합하거나 중복 컬럼을 추가하여 조회 속도를 향상시킴
	- 테이블 분할(수직/수평)	- 테이블 파티셔닝을 검토하여 I/O 성능 개선
인덱스 설계	- 대상 컬럼 선정	- 조회 조건(WHERE), 조인 조건, 정렬(ORDER BY)에 자주 사용되는 컬럼을 식별하여 인덱스 생성 후보로 선정
	- 인덱스 구성 전략 수립	- 단일 인덱스, 결합 인덱스 등 유형을 결정 - 결합 인덱스의 경우 컬럼의 순서를 정하여 검색 효율을 극대화
DB 객체 설계	- 뷰(View) 설계	- 복잡한 조인 쿼리를 단순화하거나, 특정 컬럼을 숨겨 보안성을 높이기 위해 사용자에게 보여줄 가상 테이블을 정의
	- 저장 로직 설계	- 저장 프로시저, 트리거, 사용자 정의 함수를 설계
물리 저장 설계	- 테이블스페이스 할당	- 테이블스페이스를 업무별/데이터 성격별로 분리하여 디스크 경합을 방지
	- 파티셔닝 전략 확정	- 데이터를 물리적으로 분할 저장하는 전략 수립

- 데이터베이스 설계 과정에서 무결성, 일관성, 회복, 보안, 효율성, 확장 등의 사항 고려`

IV. 데이터베이스 모델링(Database Modeling)의 고려사항

고려사항	설명
무결성(Integrity)	- 간신, 삽입, 삭제 등 연산 수행한 뒤에도 데이터 값은 주어진 제약조건 만족
일관성(Consistency)	- 두 데이터 값 사이나 특정 질의에 대한 응답들에 모순성이 없이 일치하는 특성
회복(Recovery)	- 시스템 장애가 발생했을 때 장애 발생 직전의 일관된 DB 상태로 복구
보안(Security)	- 불법적인 데이터 변경이나 손실, 노출에 대한 보호(접근제어와 밀접한 관계)
효율성(Efficiency)	- 응답 시간 단축, 저장 공간 최소화, 시스템 생산성
DB 확장(Growth)	- 시스템 운영에 영향을 주지 않으면서 새로운 데이터를 계속적인 추가 기법

- 위의 요건이 모두 원만히 갖춰질 때 완성된 데이터베이스는 건전하게 운용 가능

“꼴”

04	MCP(Model Context Protocol), A2A (Agent to Agent) Protocol		
문제	최근 AI의 활용성 증대 기술로 MCP(Model Context Protocol)와 A2A (Agent to Agent) Protocol 도입이 증가하고 있다. 이와 관련하여 다음을 설명하시오. 가. MCP와 A2A의 개념 나. MCP 보안위협 및 대응방안 다. A2A 보안위협 및 대응방안		
도메인	보안	난이도	상 (상/중/하)
키워드	공격 표면의 급격한 확장 및 공급망 위협, 권한 위임 오용 및 신뢰 문제, Prompt Injection 및 민감정보 유출 위험 증가, 감사 및 추적 불가, AI 고유 신원 부여, 입력 검증		
출제배경	MCP 보안 위협 및 대응방안 137회 출제		
참고문헌	KISA 2025년 상반기 사이버 위협 동향 보고서		
출제자	강북심화 이제이 기술사(제 130회 정보관리기술사 / bwmslove@naver.com)		

I. MCP 와 A2A 의 개념

가. AI 를 위한 USB-C 인터페이스, MCP(Model Context Protocol) 설명

개념	- 대규모 언어 모델(LLM)이 다양한 데이터 소스 및 도구와 안전하고 일관되게 상호작용할 수 있도록 지원하는 개방형 프로토콜	
개념도	<pre> graph LR subgraph Local [Local] direction TB H[Host with MCP Client] <--> MCP Protocol S1[MCP Server A] H <--> MCP Protocol S2[MCP Server B] S1 <--> Web APIs R1[Remote Service B] S2 <--> Web APIs R2[Remote Service C] end subgraph Internet [Internet] direction TB S3[MCP Server C] <--> Web APIs R1 S3 <--> Web APIs R2 end </pre>	
기술요소	- MCP 호스트	- 연결을 수행하는 LLM 어플리케이션(Claude Desktop 또는 IDE)
	- MCP 클라이언트	- 호스트 응용 프로그램 내에서 서버와 1:1 연결 유지
	- MCP 서버	- Context, 도구 및 프롬프트를 클라이언트에 제공
	- Resources	- MCP 서버가 클라이언트에 제공하는 모든 종류의 데이터
	- Prompts	- 모델에게 주어진 Context 를 구조적으로 정의하는 Contents
	- Tools	- LLM 이 작업을 수행하는데 실행 가능한 기능 검색 및 호출
	- JSON-RPC 2.0	- JSON 기반의 원격 프로시저 호출을 수행하는 경량 프로토콜

나. 다중 에이전트 협업 기반의 분산형 생태계 진화, A2A(Agent2Agent) Protocol 설명

개념	<ul style="list-style-type: none"> - 서로 다른 개발자, 프레임워크, 벤더가 만든 AI 에이전트들이 표준화된 방식으로 안전하게 협업하고 소통 가능한 오픈 프로토콜 	
개념도	<pre> graph LR User[User] <--> ClientAgent[Client Agent] ClientAgent -- "A2A" --> RemoteAgent1[Remote Agent 1] ClientAgent -- "A2A" --> RemoteAgent2[Remote Agent 2] </pre>	
기술요소	- Agent Card	- 기능, 입력/출력 포맷, endpoint URL, 보안정책 등을 포함
	- A2A 메시지 포맷	- 요청(request), 응답(response), 상태(status) 등 명확한 포맷 정의
	- SSE 지원	- 작업 진행 중 상태나 중간 결과를 실시간으로 전달

- MCP, A2A 와 같은 Protocols 은 편리한 도구인 동시에, 공격자에게 강력한 공격 표면을 제공하는 양날의 검

II. MCP 보안위협 및 대응방안

가. MCP 보안위협

구분	보안위협	설명
MCP Tool 측면	- Tool Poisoning (툴 중독공격)	- 공격자가 MCP 도구 설명에 악성 코드를 숨겨 넣고, AI 가 이를 실행하도록 유도함
	- Hidden Risks (숨겨진 명령어)	- 사용자에게는 무해한 도구처럼 보이지만, 실제로는 숨겨진 명령어를 AI 가 실행함
	- Rug Pulls	- 설치 이후, 도구가 악의적으로 수정되어 정보 유출 등의 악성

	(가짜 업데이트)	행위를 수행함
MCP 연동 구조 측면	- Cross-Server Attacks (신뢰된 도구 하이재킹)	- 악성 서버가 정상적인 MCP 서버의 도구를 덮어쓰거나 가로채는 공격 수행(사용자 로그에 기록되지 않아 추적의 어려움)
	- 취약한 보호체계	- 사용자가 보안 인식이 부족하거나, 도구변경에 대한 검증 부족
	- 앤드포인트 보안	- 도구의 설명을 신뢰하는 구조로 연쇄적인 감염 가능성 존재
MCP Server 측면	- 프롬프트 인젝션	- 악성 명령이 포함된 입력으로 시스템 오작동 유도
	- 민감 데이터 유출	- 다양한 앱과 도구가 연동되면서 데이터 노출 가능성 증가
MCP Client 측면	- 인증 미흡	- 토큰 유출 시, 인증 우회 및 세션 탈취 가능
	- 무분별한 설치	- MCP 서버 보안 이해 부족 및 묻지마 설치로 인한 위협 증대

- MCP Tool 과 구조적 특성상의 다양한 보안 위협이 존재하며, 이에 대한 체계적인 대응 필요

나. MCP 보안위협 대응방안

구분	대응방안	설명
MCP Tool 측면	- Tool Pinning (도구 고정)	- 신뢰된 버전의 도구만 사용하도록 고정하여, 악성 업데이트가 적용되지 않도록 방지
	- Clear Warnings (명확한 경고 표시)	- 도구가 실행되기 전, 정확히 어떤 작업이 수행될지 명확하게 사용자에게 표시되도록 설정
	- 권한 제한	- 도구가 접근할 수 있는 데이터나 자원은 반드시 업무상 필요한 범위로 제한하여야 함
MCP 연동 구조 측면	- 신뢰되지 않은 서버 사용 금지	- 보안이 검증된 MCP 서버만 사용하며, 강력한 보안 조치를 갖춘 서버를 우선 채택
	- 보안 계층 적용	- 중요한 작업에는 Invariant 와 같은 보안 스택을 포함하여 다중 보안 계층을 적용
	- Wait for Maturity	- 보안 체계와 관리 프로세스가 충분히 정착될 때까지 MCP 전체 도입을 지연시키는 것도 방안이 될 수 있음
MCP Server 측면	- 서버 간 격리	- 한 서버에서 도구가 손상되어도, 다른 서버나 도구에 영향을 주지 않도록 격리 설정 유지
	- 실행 전 투명성 보장	- 사용자가 요청한 도구 실행 직전에, 실제로 수행될 명령어와 동작을 구체적 수준까지 검토
	- 권한 최소화	- 도구 실행에 필요한 데이터, 파일, 시스템 접근 권한은 최소한의 범위로 설정
MCP Client 측면	- 도구 업데이트 모니터링	- 도구의 변경 여부를 주기적으로 검사하여 비인가된 수정이나 악성 코드 삽입을 탐지
	- 로그 기록 및 감사	- 도구 사용 기록을 남기고, 이상 징후나 비정상적 행동을 감지할 수 있도록 감사 체계 유지
	- 사용자 교육	- 내부 사용자 및 운영자를 대상으로 MCP 위험성과 안전한 사용법에 대한 교육 실시

- 단순한 함수를 통해 로그인 정보를 훔치거나 메시지 전송 기능으로 위장하여 해커에게 메시지를 전송하는 등의 Exploit 공격 가능

III. A2A(Agent2Agent) Protocol 보안 위협 및 대응방안

가. A2A(Agent2Agent) Protocol 보안 위협

구분	보안 위협	설명
접근 및 신뢰 문제	- 공격 표면의 급격한 확장 및 공급망 위협	- A2A는 여러 에이전트가 연결된 '체인 구조'를 기본 단위로 사용하여 소프트웨어 공급망 공격 구조와 유사한 위협 내포 - 하나의 에이전트가 침해되면 연결된 전체 시스템에 영향 - 호출 경계(Trust Boundary) 없이 메시지가 순환될 경우 보안 통제 한계
	- 권한 위임 오용 및 신뢰 문제 (Delegation Abuse)	- 요청한 에이전트가 신뢰할 수 있는 대상인가?"와 "요청할 권리 있는가?"가 AI 간 통신의 핵심 쟁점 - 인증 체계 미비나 과도한 인증 위임으로 인해 인가되지 않은 에이전트가 높은 권한 작업을 수행하는 문제 발생 가능
데이터 및 가시성 문제 데이터 및 가시성 문제	- Prompt Injection 및 민감정보 유출 위험 증가	- 에이전트 간 교환되는 메시지에 프롬프트, 내부 문맥(Context) 사용자 의도가 포함되어, Prompt Injection 공격이 다단계로 확산 가능 - 내부 시스템 정보나 PII, 결제 정보 등 민감데이터의 오남용 가능성 존재
	- 감사 및 추적 불가 (Agent Observability 부족)	- AI가 "왜 그런 출력을 하게 되었는지" 또는 "어떤 흐름을 통해 발생했는지"를 추적하는 것이 핵심 - 문맥의 전달 경로가 기록되지 않거나 표준화되지 않으면, 보안 감시 및 사고 대응이 어려워지고 책임추적이 불가능

나. A2A(Agent2Agent) Protocol 대응 방안

구분	대응방안	설명
접근 및 신뢰	- 엄격한 인증 및 권한 관리 (Zero Trust 적용)	- AI 간 통신에서도 Zero Trust 모델 적용 - 모든 에이전트, 서버, 도구에 대해 OAuth, mTLS 등 강력한 인증을 시행
	- AI 에이전트에게 고유 신원 부여	- 권한 상승(privilege escalation)이나 포렌식 조사의 어려움을 해소하기 위해, AI 에이전트에게 검증 가능한 고유의 비인간 신원(non-human identity)을 부여
데이터 및 가시성 문제	- 입력 검증 및 데이터 최소화	- 모든 입력값(프롬프트, API 요청, 외부 문맥)에 대해 철저한 검증 수행 - 외부와 공유되는 문맥에 포함될 데이터를 최소화하고, 민감 데이터는 공유 전 필터링 또는 마스킹
	- 감사 및 추적 표준화 (Observability 확보)	- 모든 요청, 응답, 문맥 전달 및 권한 변경 이력을 표준화된 감사 로그로 기록

- 보안 위험에 대응하기 위해서는, 제로 트러스트 보안 전략 원칙하에 모든 통신에 대해 강력한 인증과 최소

권한 원칙을 적용하고, 프롬프트 및 응답의 무결성을 보장하며, 전 과정의 추적 가능성을 확보하는 것이 필요

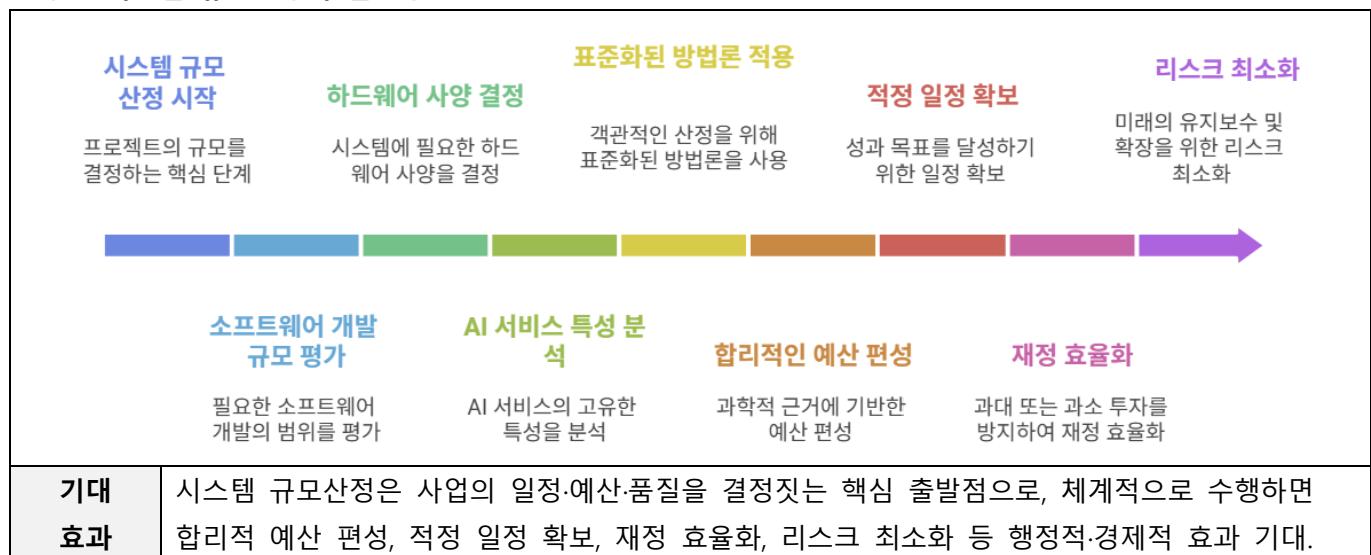
VI. AI 모델간 통신 프로토콜 비교

항목	MCP	A2A	ACP	ANP
개념	LLM과 외부 리소스/툴 간 "표준 연결선".	다양한 에이전트가 "서로 소통하고 협업"하는 언어	여러 프레임워크/플랫폼의 에이전트 "상호 운용"을 위한 통합 규격	"탈중앙·P2P" 기반의 차세대 분산형 에이전트 네트워크 표준
주요 목적	LLM↔도구·외부데이터 연결	에이전트↔에이전트 소통 및 협업	에이전트 상호 운용성 /통합	분산형 에이전트 네트워킹
구조 모델	클라이언트-서버	Peer/클라-리모트	브로커·등록소 기반 클라이언트-서버	탈중앙, 완전 P2P
인증 방식	Token 혹은 DID (옵션)	DID/헤더/핸드셰이크 등	Bearer/JWT/TLS 다양	W3C DID, End-to-End 암호화
에이전트 검색	수동, URL 혹은 등록	Agent Card/HTTP 통해 동적 탐색	Registry 기반	well-known/agent 및 P2P 탐색
메시지 형식	JSON-RPC+프롬프트/툴/리소스/컨텍스트	태스크+아티팩트, 상태, 메시지	구조적 메시지 (멀티파트, MIME)	JSON-LD/스키마, ADP/Meta-protocol
확장성/분산성	중간(실습에 집중)	높음(동적)	높음(API로 확장 용이)	매우 높음(P2P, 분산, 메타규약 협상)
주 사용 사례	LLM 기반 앱, 지식 베이스, 플러그인	멀티-에이전트 협동, 상호 태스크 위임	대형 프로젝트/플랫폼, 에이전트 통합	메타버스·IoT·탈중앙 네트워크

“끌”

05	규모산정		
문제	<p>정보 시스템 규모산정은 프로젝트의 일정과 예산을 수립하기 위한 중요한 요소이다. 규모산정과 관련하여 다음을 설명하시오.</p> <p>가. 소프트웨어 규모 산정 방법 나. 정보시스템 하드웨어 규모산정 지침 (TTAKIKO-10.0292/R3)에 따른 하드웨어 규모산정 방법 다. 인공지능(AI) 서비스 도입 사업유형과 사업비 산정 절차 (단, "소프트웨어 사업 대가산정 가이드 2025년 개정판"을 기준으로 한다.)</p>		
도메인	소프트웨어공학	난이도	상 (상/중/하)
키워드	전문가 감정, 델파이 방식, LOC 기법, MM, FP, COCOMO, CPU, 메모리, 디스크, 스토리지, 수식 계산법, 참조법, 시뮬레이션법, 사전준비, 이용료 계산, 커스터마이징 작업비용 계산, 구축·개발 비용 계산, 사업비 산정		
출제배경	정보관리, 컴시응 빈출, 필수(기본) 토픽 재점검		
참고문헌	ITPE 서브노트		
해설자	강북심화 이제이 기술사(제 130회 정보관리기술사 / bwmslove@naver.com)		

I. 정보 시스템 규모산정의 필요성



II. SW의 적정한 비용산정 방식, SW 규모산정 개요

개념	개발에 소요되는 인원, 자원, 기간 등으로 소프트웨어의 규모를 확인하여 개발 계획 수립에 필요한 비용을 산정하는 기법	
대상	사전 비용 분석	소프트웨어 개발에 필요한 비용을 사전에 예측하기 위한 활동
	개발기간 산정	프로젝트 전체 수행 기간 및 공수 산정
	프로젝트 관리 및 추적	실제 진행사항과 예상 진행사항 비교하여 프로젝트 상태 모니터링
	위험 관리	일정과 예산의 위험을 감지하고 대응책 마련

- SW 규모산정 방법에는 상향식, 하향식, 수학적 방법으로 분류되며 각 방법별 세부 산정기법이 존재

나. SW 규모산정 방법

산정방법	기법	내용
하향식 (Top Down)	- 전문가 감정 - 델파이 방식	- 경험적 단언, 개발자 합의(인력, 시스템 크기, 예산)
상향식 (Bottom Up)	- LOC 기법 - Man/Month	- 업무분류구조 정의, 각 구성요소에 대한 독립적 산정, 집계
수학적	- 기능점수(FP) - COCOMO	- 소프트웨어 비용산정의 자동화, 수치화에 의한 비용을 산정

- 재사용을 중요시하는 SW방법론의 진화에 따라 초기 LOC 방식에서 COCOMO 및 FP 등의 방식이 대두됨

III. 하드웨어 규모산정 개념 및 산정방법

가. 규모산정 개념

개념	기본적인 용량과 성능 요구사항이 제시되었을 때, 그것을 시스템 요구사항으로 변환하는 방법		
대상	CPU	해당업무를 처리하기 위한 CPU의 전체규모를 계산한 후, 적정한 성능을 지닌 서버 기종을 선정	
	메모리	CPU 규모산정에 따른 서버 구성방안에 의거하여, 서버별 시스템 S/W, 응용프로그램 등의 메모리 사용량을 산정	
	디스크	CPU 규모산정에 따른 서버 구성방안에 의거하여, 서버별 OS, 시스템 S/W, DB의 데이터, DB의 아카이브(Archive) 및 백업영역 등의 디스크 사용량을 산정	
	스토리지	CPU를 기준으로 산정된 서버 규모에 따라 필요한 스토리지의 규모를 산정	

- 일반적으로 규모산정에 대한 대상은 하드웨어 뿐만 아니라 소프트웨어나 네트워크를 포함하지만, 해당 지침에서의 규모산정 대상은 하드웨어로 PC나 기타 주변 장비가 아닌 서버 장비로 규정함

나. 하드웨어규모 산정의 3가지 방법

방법	개념	개념도
수식계산법	사용자 수 등 규모산정을 위한 요소를 토대로 용량 수치를 계산하고, 보정치를 적용하는 방법	<p>총 사용자수 * 보정치 = CPU 2 Core</p>
참조법	업무량(사용자 수, DB 크기)에 따라, 기본 데이터를 토대로 대략적인 시스템 규모를 비교하여 비슷한 규모를 산정	<p>유사 시스템 → 참조 → B 시스템</p>
시뮬레이션법	대상 업무에 대한 작업부하를 모델링하고 이를 시뮬레이션하여 규모를 산정	<p>기본 규모산정 (보정) → 시뮬레이션 (부하, 성능)</p>

- 정보시스템 하드웨어 규모선정 방법들의 장단점이 존재하여, 정보시스템의 특징을 고려하여 방법 선택 필요

IV. 인공지능(AI) 서비스 도입 사업유형 및 산정 절차

가. 인공지능(AI) 서비스 도입 사업유형

〈AI 서비스 도입 사업유형과 비용 및 작업요소 간 관계〉						
비용항목	사업유형	단순 도입형	커스터마이징형			시스템 통합형
			기본	데이터	모델	
커스터마이징 작업비용	서비스 이용료	○	○	○	○	△
	요구사항분석/설계		○	○	○	△
	데이터 구축			○	○	
	모델 구현 및 학습				○	
검증 및 안정화			○	○	○	
구축개발비용						○

유형	설명
단순 AI 서비스 도입형	- 공공 도입이 가능한 AI 서비스를 개발 또는 변형 없이 정기 이용료(구독료)를 지불하고 사용하는 사업유형
커스터 마이징형	- 기본 커스터마이징
	- AI 데이터 구축 커스터마이징
	- AI 모델 커스터마이징
시스템 통합형	- 공공 도입이 가능한 AI 서비스를 도입하면서 발주기관의 도입 목적에 따라 커스터마이징 작업과 추가적인 소프트웨어 개발 및 시스템통합 작업이 병행되는 사업유형

- 서비스 도입 사업비 = 서비스 총 이용료 + 커스터마이징 작업비용 + 구축개발비용

나. 인공지능(AI) 서비스 도입 사업비 산정 절차

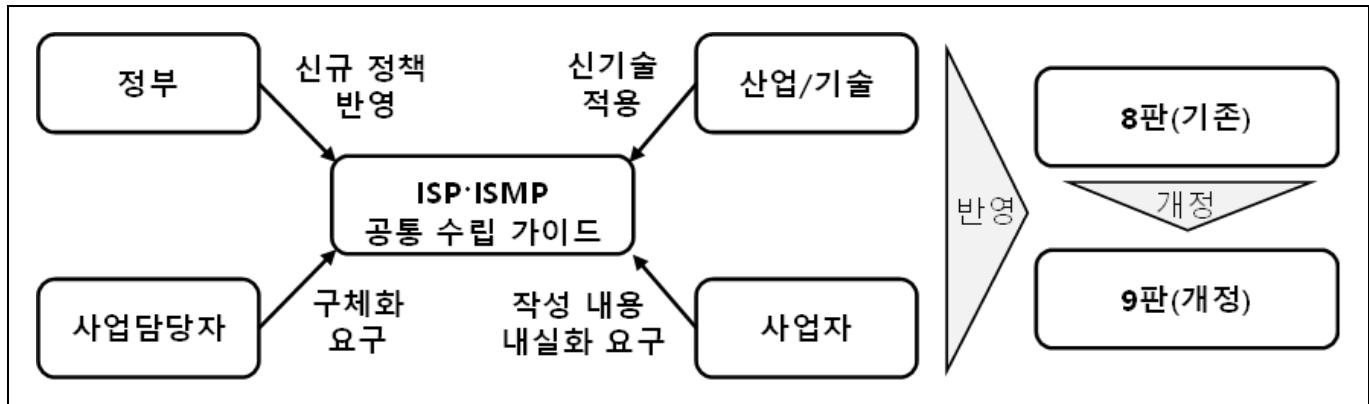
절차	추가활동	산출물
1. 사전준비	- 도입 대상 서비스 식별 - 세부 도입 서비스 항목과 서비스 도입 유형 결정 산출물 서비스 도입 사업비 대상 서비스 및	- 대상 서비스 및 추가 활동 항목
2. 서비스 이용료 계산	- 서비스 특성을 고려하여 사용기간 결정 - 해당 서비스 가격표 또는 견적서 참고하여 이용료 계산	- 서비스 이용료

3. 커스터마이징 작업비용 계산	<ul style="list-style-type: none"> - 서비스 도입 시 필요한 커스터마이징 작업비용 항목 식별 - 해당 서비스 가격표 또는 견적서, 유사 서비스 가격표 또는 견적서를 참고하여 커스터마이징 작업비용 계산 	- 커스터마이징 작업 비용
4. 구축·개발 비용 계산	<ul style="list-style-type: none"> - 서비스 도입 시 필요한 소프트웨어 개발 및 시스템통합 작업비용 항목 식별 - 기존 소프트웨어 개발비 산정 방식에 따라 기능점수 또는 투입 공수 방식으로 구축·개발 비용 계산 	- 구축·개발 비용
5. AI 서비스 도입 사업비 산정	<ul style="list-style-type: none"> - 서비스 도입 사업비 산정 - 서비스 이용료 + 커스터 마이징 작업비용 + 구축·개발 비용 	- 서비스 도입 사업비

“끝”

06	ISP/ISMP		
문제	<p>정보시스템 구축/재구축을 위한 예산 요구를 위해서는 ISP-ISMP 수립 공통가이드에 따라 ISP 또는 ISMP를 사전에 수립하여야 한다. ISP 및 ISMP 수립 공통가이드는 지속적인 개정을 거쳐 2025년 5월 9판이 배포됐고, 12월 일부 개정됐다. 아래 항목에 대해 설명하시오.</p> <p>가. ISP(Information Strategy Plan)개념과 ISP-ISMP 수립 공통가이드 9판 변경내역 나. ISP-ISMP 수립 제외 가능 유형 및 ISP-ISMP 검토 주요 내용 다. 소규모 정보시스템 구축 사업계획 수립 절차</p>		
도메인	IT경영전략	난이도	하 (상/중/하)
키워드	<p>환경분석, 현황분석(AS-IS), 정보화 비전 및 전략수립, 목표모델설계(TO-BE), 통합 이행 계획 프로젝트 착수 및 참여자 결정, 정보시스템 방향성 수립, 업무 및 정보기술 요건 분석, 정보시스템 구조 및 요건 정의, 정보시스템 구축 사업 이행방안 수립</p> <p>소규모 정보시스템 사업, 클라우드 우선 적용, 사업계획서 작성(보완) 및 검토요청, 사업계획서 사전검토, 사업계획서 검토 및 기재부 제출</p>		
출제배경	기본 토픽인 ISP/ISMP의 지식 이해 및 9판 변경내역 숙지 여부 확인		
참고문헌	ISP-ISMP 수립 공통가이드 9판(25년 12월 일부 개정 사항 포함)		
출제자	강북심화 이제이 기술사(제 130회 정보관리기술사 / bwmslove@naver.com)		

I. 정보시스템 구축 전략 수립, ISP/ISMP 개정 배경



- ISP/ISMP 수립 공통가이드와 관련된 이해관계자들의 요구사항을 가이드에 지속 반영
- 지속적인 개정을 거쳐 2025년 5월 9판이 배포, 12월 일부 개정

II. ISP(Information Strategy Plan)개념과 ISP-ISMP 수립 공통가이드 9판 변경내역

가. ISP(Information Strategy Plan) 개념

개념	<ul style="list-style-type: none"> - 조직 내의 전략적 정보 요구를 식별하고, 업무활동과 이에 대한 자료 영역을 기술하며, 정보시스템 개발을 위한 통합된 프레임워크를 제공하고, 이의 구현을 위한 통합 정보시스템 계획 		
단계	활동	세부내용	산출물
환경분석	경영환경분석	<ul style="list-style-type: none"> - 외부환경 요인과 경영전략 분석을 통해 변화를 유발하는 요인에 대응하기 위한 시사점 도출 	<ul style="list-style-type: none"> - 경영환경 분석서

	법령, 제도 분석	- 관련 법/제도 분석을 통해 사업에 영향을 미칠 수 있는 요구사항을 도출하여 목표모델 설계시 반영	- 법·제도 분석서
	정보기술(IT) 환경분석	- 최신 정보기술 추세와 기술환경 변화를 검토하여 최신 정보기술의 적용가능성 및 적용 사례 분석 - [국민중심] 정보기술 도입 분석 결과	- 정보기술 동향 분석서
현황분석 (As-Is 분석)	업무현황분석	- 업무절차맵(Process Modeling), 업무기능(Activity) 정의서 등을 작성하여 현행 조직과 업무체계상의 문제점 및 개선 요구사항을 도출	- 업무현황 분석서 (인터뷰 결과 포함)
	정보기술(IT) 현황분석	- (업무시스템 분석) 업무시스템 현황을 분석/진단하여 문제점 및 개선요구사항을 도출 - (데이터분석) 데이터 현황 분석/진단하여 문제점 및 개선 요구사항 도출 - (인프라분석) 하드웨어, 소프트웨어, 네트워크, 스토리지 등 현행 인프라를 분석/진단하여 문제점 및 개선요구사항 도출 - (IT거버넌스 분석) IT업무(관리) 프로세스를 분석/진단하여 문제점 및 개선요구사항을 도출	- 정보기술 업무현황 분석서
	벤치마킹	- 현황분석(업무&정보기술)을 통해 도출된 문제점 및 개선요구사항을 바탕으로 벤치마킹 대상(항목)을 선정한 후, 선진사례 조사/분석을 진행	- 선진사례 동향 파악서
	차이(Gap)분석	- 선진사례의 업무절차 및 정보기술 요건을 도출한 후, 기도출된 정보화 요건과의 차이를 분석, 과제의 보완작업 및 개선	- 차이분석서
	이슈통합 및 개선과제 도출	- 도출된 이슈를 종합, 연관성 높은 이슈사항 그룹화 - 근본원인 분석 후 개선과제 도출 - [국민중심] 사용자 편의성 향상 과제 도출 결과	- 요구사항 및 개선 과제 분석서
	정보화비전 및 전략 수립	- 환경분석/현황분석 결과를 연계하여 비전, 목표, 단계별 실행전략 등을 수립 - [민관협력] 민관협력 대상, 분야, 방식 등 협력 전략 수립 - [클라우드 기술 우선 적용 권고] 민간 클라우드 및 디지털서비스 전문 계약제도 이용 방향	- 정보화 전략 정의서
(To-Be Model)	To-Be 개선 과제 상세화	- 현황분석시 도출된 개선과제의 상세화(과제 개요, 추진 범위, To-Be 개선방향, 적용사례 등) - [AI·데이터기반] AI·데이터 기술기반 의사결정 활용 계획	- To-Be 과제 상세 정의서
	To-Be 업무 프로세스 설계	- 개선과제 내역, 선진사례, IT 개선방향을 종합적으로 고려하여 최적화된 To-Be 업무프로세스 재설계 - To-Be 업무프로세스 내 요건 상세 정의	- To-Be 업무프로세스 설계서
	To-Be 정보 시스템 구조	- 전략적 정보시스템 구축을 위한 이상적 응용서비스 구조를 정립	- To-Be 정보시스템 구조 설계서

	설계	- [국민중심] 통합인증체계 도입 계획 - [국민중심] 사용자 이용환경을 고려한 설계	
	To-Be 데이터 구조 설계	- 정립된 정보시스템을 효율적으로 운용할 정보자원(데이터) 관리 체계를 정리 - [하나의정부] 법정부 시스템연계, 개방형 표준 적용 계획	- To-Be 데이터 구조 설계서
	To-Be 기술 및 보안 구조설계	- 전략적 정보시스템 구축을 위한 필요 기술 요소 및 기반(인프라) 구조를 정립	- To-Be 기술 및 보안 구조 설계서
통합 이행 계획	통합 이행계획 수립	- 과제별 우선순위 평가 및 전략적 특성, 연관성 바탕으로 추진 체계 및 시행일정 수립	- 통합 이행계획 수립서
	총구축비 산출	- (SW 개발비) 기능점수(FP) 산정 후, 개발비 도출 - (장비비) SW구매, HW구매 등 항목별 규격, 수량, 금액 내역	
	효과 분석	- 타당한 기대효과 분석	

- ISP 최종산출물에는 ISP 기본 구성 내용의 결과물이 포함되어야 하며, 기본구성 내용 간의 연관성을 기술

나. ISP-ISMP 수립 공통가이드 9판 변경내역

항목	기존(제8판)	현행(제9판)	변경 사유
신규제도	-	- 소규모 정보시스템 구축 사업계획수립 안내	- 제도개선 사항 반영
일부 개정 ('25.12)	- DPG 기본원칙 적용 우선 검토	- 클라우드 기술 적용 우선 검토	- DPG 위원회 폐지

- ISP-ISMP 수립 공통가이드 9판 개정으로 ISP-ISMP 수립 제외 가능 유형 및 ISP-ISMP 검토 주요 내용에
변경사항 존재

III. ISP-ISMP 수립 제외 가능 유형 및 ISP-ISMP 검토 주요 내용

가. ISP-ISMP 수립 제외 가능 유형

제외 유형	설명	예시
1. 단순시스템 도입	- 입력, 조회, 출력 등의 단순 기능을 적용하여 개발하는 시스템	- 기관 홍보용 홈페이지 - 언론모음 홈페이지 - 설문 시스템 등
2. 단순기능 개발	- 기존 시스템에 일부 기능을 개선 또는 추가하는 사업, 내부 업무처리의 효율화를 목적으로 개발하는 사업	- 일부 소규모 기능 개선 - 단순 반복 업무 효율화를 위한 RPA 도입 사업 등
3. 운영/유지	- 기존 시스템을 운영·유지하는 사업	- 정보시스템 운영 및 유지 관리 사업
4. 단순물품 구매	- 사무기기(전산장비), 소프트웨어 등 장비구매 위주의 사업	- 서버, PC, 노트북, 프린터 등 구매 사업, - 사무용 SW 구입 등 별도

		개발이 필요없는 상용 SW 구매 사업
5. 시설 구축	- 정보시스템이 아닌 시설 구축 및 특수장비를 도입(구매)하는 사업	- 회선 증설, UPS·항온항습기 설치, 전기·통신공사 등 전산실 구축 - 특수장비(전파 측정기 등) 구매 사업 등
6. DB구축	- 시스템 구축 없이 인력 투입을 통해 지식정보자원을 디지털(온라인)화 하는 사업	- off-line 자료를 디지털 파일로 변환하는 사업
7. 민간투자형 SW사업	- 소프트웨어진흥법 시행령 제33조에 따라 ISP 기본 구성항목을 갖춘 사업계획 등을 수립한 민간부문이 제안한 민간투자형 소프트웨어 사업 단, 정부고시형 민간투자형 SW 사업은 ISP 또는 ISMP를 수립하여야 함	-
8. 소규모 정보시스템 사업	<p style="color: red;">- 총구축비 20억원 미만의 정보시스템 구축·재구축 사업 단, 구체적인 사업계획을 수립한 후 기획재정부장관에게 제출하여야 함</p> <p style="color: red;">* 개발비, 장비비(HW, SW), 기타(PMO, 감리비 등) 포함</p>	-

- ISP-ISMP 수립 공통가이드 9판에서 소규모 정보시스템 사업에 대한 수립 제외 가능 유형 추가

나. ISP-ISMP 검토 주요 내용

분야	구성 항목	주요내용
1. 사업 타당성	- 필요성	- 현행 업무 수행 상에 문제점이나 개선하고자 하는 사유를 제시 - 이행과제(세부사업)를 사업목표와 일관성 있도록 작성
	- 시급성	- 차년도에 추진해야 하는 시급한 사유를 제시
	- 중복성	- 기관 내·외부 타 시스템과의 중복가능성을 점검하고 통합·연계 결과를 기술
2. 실현 가능성	- 사업추진 여건	- 사업 추진 및 신규 서비스 운영을 위한 조직 구성과 인력 확보방안을 기술 - 유관기관과 연계·통합이 필요한 경우, 각 기관별 역할과 수행업무 등 협조체계를 기술 - 신규 서비스 시행을 위한 단계별 법·제도 정비방안을 사업계획과 연계하여 제시
	- 기술 적정성	- 적용된 기술이 사업목표 달성을 위한 필수 요소 여부 및 적용가능성을 분석 - 적용된 기술의 실용화 사례를 조사·분석
3. 클라우드 우선 적용		- 사업 추진 시 클라우드 기술 우선 적용 방안을 분석하고 검토 결과를 제시
4. 규모 적정성		- 총구축비의 모든 구성요소를 「SW사업 대가산정 가이드」 등을 활용하

	<p>여 빠짐없이 산출하고, 모든 이행과제들의 비용 합과 일치하도록 작성</p> <ul style="list-style-type: none"> - 「정보시스템 하드웨어 규모산정 지침」(TTA)을 준수하여 시스템 용량 산정
--	--

- 8판 ISP-ISMP 검토 주요 내용의 디지털플랫폼 정부 기본원칙 적용 중 클라우드 우선 적용 원칙만 남기고, 다른 검토 주요 내용 삭제

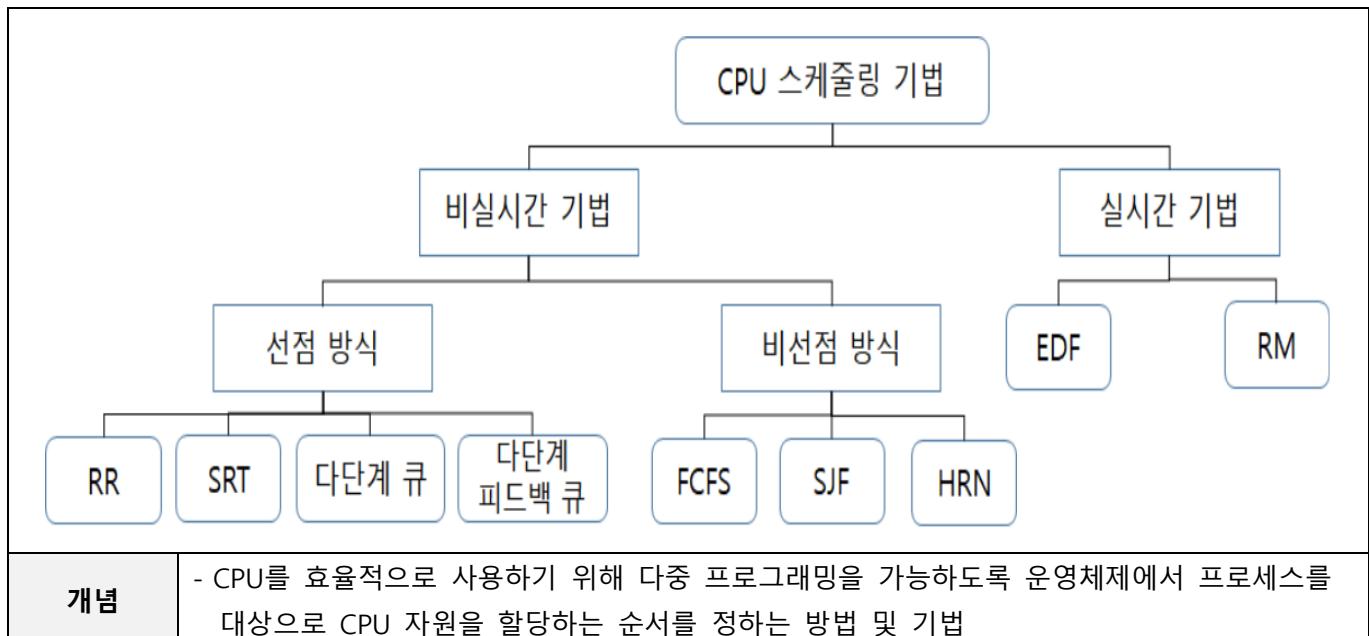
IV. 소규모 정보시스템 구축 사업계획 수립 절차

개념	<ul style="list-style-type: none"> - 각 중앙관서에서 추진하는 총구축비* 20억원 미만의 정보시스템 구축·재구축 사업 																								
대상 및 비용	<ul style="list-style-type: none"> - (대상) 각 중앙관서에서 추진하는 총구축비*20억원 미만의 정보시스템 구축·재구축 사업 * 정보시스템 개발비, 장비비(HW, SW), 기타(감리비 등) 포함 - (수립비) 연구용역비, 자체 예산 등 활용 가능 																								
주요 절차 흐름도	<pre> graph LR A[부처] -- ① 사업계획서 수립(보완) 및 검토요청 --> B[NIA(5일)] B -- ② 사업계획서 사전검토 --> C{사업 계획서 충실히} C -- 부적합 --> A C -- 적합 --> D[NIA(10일)] D -- ③ 검토의견서 작성 및 기획재정부 제출 --> E[기획재정부] E -- ④ 예산편성시 검토의견서 참작 --> F[기획재정부] </pre> <p>※ 검토기간 : 최대 15일(사전검토, 검토의견서 작성 포함)</p>																								
주요 절차	<table border="1"> <tr> <td style="color: red;">사업계획서 작성(보완) 및 검토요청</td> <td colspan="4"> <ul style="list-style-type: none"> - 각 중앙관서에서는 시스템 개요, 현황분석, 목표 모델 설계, 이행계획 4단계 절차로 구성된 사업계획서 작성 </td> </tr> <tr> <td style="color: red;">사업계획서 사전검토</td> <td colspan="4"> <ul style="list-style-type: none"> - 접수된 사업계획서의 품질이 검토가 가능한 수준으로 충실히 작성되었는지 등에 대해 사전 검토하고 필요시 보완 요청 </td> </tr> <tr> <td style="color: red;">사업계획서 검토 및 기재부 제출</td> <td colspan="4"> <ul style="list-style-type: none"> - 소규모 정보시스템 구축 사업계획서 검토 신청 시, 총 6개 항목에 대해 검토 * 정책 연계성, 문제해결의 시급성, 이행과제 타당성, 민간 클라우드 활용, 기술 적합성, 규모 적정성 </td> </tr> <tr> <td>예산편성 시 검토의견서 참작</td> <td colspan="4"> <ul style="list-style-type: none"> - 기획재정부 예산 편성 시 내용 참고 </td> </tr> </table>					사업계획서 작성(보완) 및 검토요청	<ul style="list-style-type: none"> - 각 중앙관서에서는 시스템 개요, 현황분석, 목표 모델 설계, 이행계획 4단계 절차로 구성된 사업계획서 작성 				사업계획서 사전검토	<ul style="list-style-type: none"> - 접수된 사업계획서의 품질이 검토가 가능한 수준으로 충실히 작성되었는지 등에 대해 사전 검토하고 필요시 보완 요청 				사업계획서 검토 및 기재부 제출	<ul style="list-style-type: none"> - 소규모 정보시스템 구축 사업계획서 검토 신청 시, 총 6개 항목에 대해 검토 * 정책 연계성, 문제해결의 시급성, 이행과제 타당성, 민간 클라우드 활용, 기술 적합성, 규모 적정성 				예산편성 시 검토의견서 참작	<ul style="list-style-type: none"> - 기획재정부 예산 편성 시 내용 참고 			
사업계획서 작성(보완) 및 검토요청	<ul style="list-style-type: none"> - 각 중앙관서에서는 시스템 개요, 현황분석, 목표 모델 설계, 이행계획 4단계 절차로 구성된 사업계획서 작성 																								
사업계획서 사전검토	<ul style="list-style-type: none"> - 접수된 사업계획서의 품질이 검토가 가능한 수준으로 충실히 작성되었는지 등에 대해 사전 검토하고 필요시 보완 요청 																								
사업계획서 검토 및 기재부 제출	<ul style="list-style-type: none"> - 소규모 정보시스템 구축 사업계획서 검토 신청 시, 총 6개 항목에 대해 검토 * 정책 연계성, 문제해결의 시급성, 이행과제 타당성, 민간 클라우드 활용, 기술 적합성, 규모 적정성 																								
예산편성 시 검토의견서 참작	<ul style="list-style-type: none"> - 기획재정부 예산 편성 시 내용 참고 																								
개념	<ul style="list-style-type: none"> - 각 중앙관서에서 추진하는 총구축비* 20억원 미만의 정보시스템 구축·재구축 사업 																								
대상 및 비용	<ul style="list-style-type: none"> - (대상) 각 중앙관서에서 추진하는 총구축비*20억원 미만의 정보시스템 구축·재구축 사업 * 정보시스템 개발비, 장비비(HW, SW), 기타(감리비 등) 포함 - (수립비) 연구용역비, 자체 예산 등 활용 가능 																								
주요 절차 흐름도	<pre> graph LR A[부처] -- ① 사업계획서 수립(보완) 및 검토요청 --> B[NIA(5일)] B -- ② 사업계획서 사전검토 --> C{사업 계획서 충실히} C -- 부적합 --> A C -- 적합 --> D[NIA(10일)] D -- ③ 검토의견서 작성 및 기획재정부 제출 --> E[기획재정부] E -- ④ 예산편성시 검토의견서 참작 --> F[기획재정부] </pre> <p>※ 검토기간 : 최대 15일(사전검토, 검토의견서 작성 포함)</p>																								
주요 절차	<table border="1"> <tr> <td style="color: red;">사업계획서 작성(보완) 및 검토요청</td> <td colspan="4"> <ul style="list-style-type: none"> - 각 중앙관서에서는 시스템 개요, 현황분석, 목표 모델 설계, 이행계획 4단계 절차로 구성된 사업계획서 작성 </td> </tr> <tr> <td style="color: red;">사업계획서 사전검토</td> <td colspan="4"> <ul style="list-style-type: none"> - 접수된 사업계획서의 품질이 검토가 가능한 수준으로 충실히 작성되었는지 등에 대해 사전 검토하고 필요시 보완 요청 </td> </tr> <tr> <td style="color: red;">사업계획서 검토 및 기재부 제출</td> <td colspan="4"> <ul style="list-style-type: none"> - 소규모 정보시스템 구축 사업계획서 검토 신청 시, 총 6개 항목에 대해 검토 * 정책 연계성, 문제해결의 시급성, 이행과제 타당성, 민간 클라우드 활용, 기술 적합성, 규모 적정성 </td> </tr> <tr> <td>예산편성 시 검토의견서 참작</td> <td colspan="4"> <ul style="list-style-type: none"> - 기획재정부 예산 편성 시 내용 참고 </td> </tr> </table>					사업계획서 작성(보완) 및 검토요청	<ul style="list-style-type: none"> - 각 중앙관서에서는 시스템 개요, 현황분석, 목표 모델 설계, 이행계획 4단계 절차로 구성된 사업계획서 작성 				사업계획서 사전검토	<ul style="list-style-type: none"> - 접수된 사업계획서의 품질이 검토가 가능한 수준으로 충실히 작성되었는지 등에 대해 사전 검토하고 필요시 보완 요청 				사업계획서 검토 및 기재부 제출	<ul style="list-style-type: none"> - 소규모 정보시스템 구축 사업계획서 검토 신청 시, 총 6개 항목에 대해 검토 * 정책 연계성, 문제해결의 시급성, 이행과제 타당성, 민간 클라우드 활용, 기술 적합성, 규모 적정성 				예산편성 시 검토의견서 참작	<ul style="list-style-type: none"> - 기획재정부 예산 편성 시 내용 참고 			
사업계획서 작성(보완) 및 검토요청	<ul style="list-style-type: none"> - 각 중앙관서에서는 시스템 개요, 현황분석, 목표 모델 설계, 이행계획 4단계 절차로 구성된 사업계획서 작성 																								
사업계획서 사전검토	<ul style="list-style-type: none"> - 접수된 사업계획서의 품질이 검토가 가능한 수준으로 충실히 작성되었는지 등에 대해 사전 검토하고 필요시 보완 요청 																								
사업계획서 검토 및 기재부 제출	<ul style="list-style-type: none"> - 소규모 정보시스템 구축 사업계획서 검토 신청 시, 총 6개 항목에 대해 검토 * 정책 연계성, 문제해결의 시급성, 이행과제 타당성, 민간 클라우드 활용, 기술 적합성, 규모 적정성 																								
예산편성 시 검토의견서 참작	<ul style="list-style-type: none"> - 기획재정부 예산 편성 시 내용 참고 																								

- 소규모 정보시스템 구축 사업에 대해 ISP/ISMP 수립 의무 면제로 사업기간 단축 및 자원 투입 절감 가능

06	RR(Round-Robin)		
문제	선점형 CPU 스케줄링 알고리즘인 RR(Round-Robin)에 대하여 설명하고 아래 표에 따른 각 프로세스들의 종료 시간(Finish time)과 응답 시간(response time, turnaround time)을 계산하시오. 단, Time quantum은 2이며, 프로세서가 시간 0에 시작한다고 가정하고 운영체제로 인한 오버헤드는 무시한다.		
도메인	운영체제	난이도	하 (상/중/하)
키워드	선점 스케줄링, Time Quantum(Time Slice), 시분할방식		
출제배경	OS 기본 토픽인 CPU 스케줄링 중 RR 이해 확인		
참고문헌	ITPE 서브노트		
출제자	정상반멘토 이상현 기술사(제 118회 정보관리기술사 / bluesanta97@naver.com)		

I. CPU의 효율적 운용을 위한, CPU 스케줄링 기법의 개요



- 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, RR(Round-Robin) 설명

가. RR(Round-Robin)의 개념

	<p>준비 상태 큐</p> <p>프로세스 도착 → C → B → A → 할당 → CPU → 완료</p> <p>피드백</p>
개념	<ul style="list-style-type: none"> - 할당된 시간 내에 작업을 완료하기 못하면 다음 프로세스로 교체하고 실행 중이던 프로세스는 대기 큐로 이동하는 기법

나. RR(Round-Robin)의 상세 설명

구분	설명	
동작방식	<ul style="list-style-type: none"> - FIFO의 변형으로 사전에 정의된 할당 시간을 프로세스에 할당하는 방법 - 선점형 방식으로 할당 시간이 만료되면 대기 큐(Queue)에 대기하며 자신의 차례를 기다림. 	
할당시간	<ul style="list-style-type: none"> - 할당시간이 작은 경우 	<ul style="list-style-type: none"> - 할당시간이 작으면 프로세스 교체가 자주 발생하게 됨 - 즉, 잦은 문맥교환 발생으로 오버헤드 발생
	<ul style="list-style-type: none"> - 할당시간이 큰 경우 	<ul style="list-style-type: none"> - 할당시간이 무한대로 커지면 FIFO 스케줄링과 동일하게 동작
특징	<ul style="list-style-type: none"> - 기아상태(Starvation), 무한봉쇄(Indefinite blocking) 미발생 - 모든 프로세스가 공평하게 다뤄짐 - 할당시간의 크기가 시스템의 동작에 절대적인 영향을 미침. 	
적용환경	<ul style="list-style-type: none"> - 시분할 방식 시스템 	

III. RR(Round-Robin) 스케줄링 계산

가. RR(Round-Robin) 스케줄링

P1	P2	P3	P4	P5														
0	1	3	5	6														
P1					10													
P2						12												
P3							17											
P4								20										
P5																		

시점	수행 Task	Queue	설명
0초	없음	없음	- P1 Task 진입
1초	P1	없음	- P1 Task 수행
2초	P1	P2	- P2 Task Queue 적재
3초	P2	P1	- P1 Queue 이동 후 P2 Task 수행
4초	P2	P1, P3	- P3 Task Queue 적재
5초	P1	P3, P2	- P2 Queue 이동 후 P1 Task 수행
6초	P3	P2, P4	- P1 Task 완료로 P3 Task 수행 및 P4 Queue 적재
7초	P3	P2, P4, P5	- P5 Queue 적재
8초	P2	P4, P5	- P3 Task 완료, P2 수행
9초	P2	P4, P5	- P2 수행
10~11초	P4	P5, P2	- P2 Queue 이동, P4 수행
12~13초	P5	P2, P4	- P4 Queue 이동, P5 수행
14~15초	P2	P4, P5	- P5 Queue 이동, P2 수행
16~17초	P4	P5, P2	- P2 Queue 이동, P4 수행
18초	P5	P2, P4	- P4 Queue 이동, P5 수행
19초	P2	P4	- P5 Task 완료, P2 Task 수행
20초	P4	-	- P2 Task 완료, P4 Task 수행

나. RR(Round-Robin) 스케줄링 프로세스 별 종료시간 및 응답 시간

Process ID	종료 시간	응답 시간
P1	5	5 (5-0)
P2	19	18 (19-1)
P3	7	4 (7-3)
P4	20	15 (20-5)
P5	18	12 (18-6)

- 스케줄링 평균 응답 시간은 $(5+18+4+15+12)/5 = 10.8$ 임

IV. 선점형 스케줄링과 비선점형 스케줄링의 비교

비교 항목	선점형 스케줄링	비선점형 스케줄링
특징	<ul style="list-style-type: none"> - 특수 하드웨어(Timer 등) 필요 - 공유 데이터 프로세스 동기화 필요 	<ul style="list-style-type: none"> - 특수 하드웨어 불필요 - 작업종료까지 CPU 점유
장점	<ul style="list-style-type: none"> - 비교적 빠른 응답 - 시분할 시스템에 적합 	<ul style="list-style-type: none"> - 응답시간 예상 용이 - 프로세스 요구를公正하게 처리
단점	<ul style="list-style-type: none"> - 높은 우선순위 프로세스 빈번 시 프로세스 교체 부하 	<ul style="list-style-type: none"> - 작업시간이 긴 프로세스에 의한 기아현상 발생 가능
기법	- RR, SRT, MLQ, MLFQ 등	- FCFS, SJF, HRN, Priority 등
활용	- 실시간, Deadline 응답 환경 등	- 프로세스의 처리시간 편차가 적은 환경

- 활용 목적에 따라 선점형, 비선점형 스케줄링을 통해 시스템의 안정성을 확보하여 프로세스 구성.

“끝”



ITPE

ICT 온라인, 오프라인 융합 No 1

PMP 자격증 정보관리기술사/컴퓨터시스템응용기술사
IT전문가과정 정보시스템감리사
정보통신기술사 애자일

오프라인 명품 강의

제136회 대비 ITPE Final Round 해설집 (2일차)

대상 정보관리기술사, 컴퓨터시스템응용기술사, 정보통신기술사, 정보시스템감리사 시험

발행일 2026년 02월 01일

집필 강정배 PE, 서O욱 PE, 조재원 PE, 이상현 PE, 이제이 PE, 전일 PE, 김찬일 PE, 강진우 PE
장O호 PE, 백현 PE, 정상 PE

출판 **ITPE(Information Technology Professional Engineer)**

주소 ITPE 대치점 서울시 강남구 선릉로 86길 17 선릉엠티빌딩 7층

ITPE 선릉점 서울시 강남구 선릉로 86길 15 3층 IT교육센터 아이티피아

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

본 저작물은 **ITPE(아이티피아)**에 저작권이 있습니다.

저작권자의 허락없이 **본 저작물을 불법적인 복제 및 유통, 배포**하는 경우

법적인 처벌을 받을 수 있습니다.