

기본상품 규격서

WISE Agent Labs V1(인공지능(AI)소프트웨어)

(대표기능 : LLMOps 기반 모델 최적화 및 No-Code Agent Builder 워크플로우 구축)

1. 상품개요 및 구매조건

1.1 상품개요

WISE Agent Labs V1(와이즈 에이전트 랩스 브이원)은 거대언어모델(LLM)의 관리를 위한 학습·평가·운영(LLMOps) 영역과, 실무에 즉시 투입 가능한 업무용 에이전트를 구축하고 시뮬레이션하는 (Agent Builder)영역이 결합된 AI 에이전트 구축·운영 통합 솔루션입니다.

본 플랫폼은 데이터 준비부터 모델 최적화, 파이프라인 자동화, 그리고 최종 에이전트 서비스 배포에 이르는 AI 개발 전 주기를 단일 환경에서 관리합니다. 특히 코딩 지식이 없는 현업 담당자도 No-Code UI를 통해 고성능 AI 에이전트를 구성할 수 있도록 지원하며, 기업 환경에 필수적인 개인정보 보호(PII), 역할 기반 권한 제어(RBAC)뿐만 아니라 OTP 및 QR코드 기반의 다중 인증 체계와 리소스 관제 및 시스템 장애 자동 알림(SMTP) 체계를 갖추어 안전하고 지속 가능한 AI 운영 환경을 제공합니다.

1.2 규격별 적용대상 및 범위, 사용 기간

구분	물품분류번호	모델명	구매 단위	라이선스 (적용대상)	SW라이선스 (사용기간)	인도 조건	비고
	물품식별번호	제품규격		라이선스 (적용범위)			
1	4323269801	WISE Agent Labs V1	조 (copy)	제한없음	제한없음	현장설치	-
	26411880	WISE Agent Labs V1 1core license		1core			



1.3 규격별 1조(copy)구매시 SW라이선스 사용권리 및 사용기간

구분	물품식별 번호	모델명 및 제품규격	라이선스 적용대상 및 범위, 정책 등 (1조(copy)구매시)	
1	26411880	WISE Agent Labs V1 1core license	라이선스 범위	해당 제품은 1core 구매 단위 라이선스 제품
			규격의 역할	· No-Code 웹 UI 기반 SFT, LoRA 모델 파인튜닝 및 BLEU/ROUGE 정량 지표 평가 · 드래그 앤 드롭 캔버스 환경 기반 지능형 AI 에이전트 워크플로우 설계 및 시뮬레이션 · 정규식 기반 개인정보(PII) 실시간 마스킹 및 RBAC 기반 접근 통제 인프라 제공 · Model Context Protocol(MCP) 표준 채택을 통한 외부 시스템 및 도구 확장 · 25년 기술력이 집약된 자사 검색엔진(Search Formula-1) 연동을 통한 최고 성능의 키워드 및 벡터 검색 지원 · Document AI 및 Docling 라이브러리 기반 비정형 문서 파싱 및 구조화 데이터 추출 · 사용자 지시에 따라 LLM이 복수의 톨을 호출하고 실행 흐름을 제어하는 멀티 톨 에이전트 노드 지원 * 요구사항에 따른 수량 및 추가 옵션 선택 구매 가능
			사용기간	구매 시 사용 기간 제한 없음

사실과상위없음



1.4 구매예시

설치서버	모델명 및 제품규격	권장사양(H/W)	1조(Copy)구매 단위
1	WISE Agent Labs V1 1core license	- OS: 64bit OS (Linux 계열) *GPU 라이브러리 호환성을 위해 Ubuntu 계열 권장 - CPU: 2.0 GHz x 32core 이상 - 메모리: 128GB 이상 - 디스크: SSD 1TB 이상 - Network: 1Gbps Ethernet 이상	32조(Copy)
총 구매 Copy			32조(Copy)구매

※ MCP 톨의 개수가 증가할수록 권장사양은 증가할 수 있으며,
자사 LLM(WISE LLOA) 사용 시 LLM 별도 구매 및 LLM에서 권장하는 스펙의
서버 필요

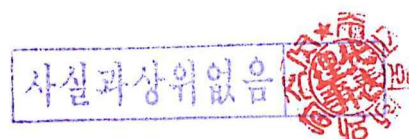
※ 구매예시는 권장사양에 따른 예시이며, 실제 구매 시에는 수요기관과 납품
업체가 상호협의 필요

1.5 해당 규격별 제품은 기본 커스터마이징이 포함된 상품입니다

※기본 커스터마이징 범위는 수요기관과 납품업체가 상호협의

2. 제품 인증내역

분 류	인증 번호	인증 명칭	만료일자
GS 1등급	26-0047	WISE Agent Labs V1 (와이즈 에이전트 랩스 V1)	-



3. 제품 권장사양 및 기능

3.1 구매한 S/W가 설치될 H/W 제품 권장사양

NO	물품식별번호	모델명 및 제품규격	권장사양(H/W)	운영환경 (서버, 사용자)
1	26411880	WISE Agent Labs V1 1core license	- CPU: 32 Core 이상 - Memory: 128GB 이상 - Storage: 1TB 이상 - OS 설치 공간 별도 - 수집 데이터양에 따라 요구 용량은 변동됨 - N/W: 1Gbps Ethernet 이상	☐ OS Linux - Redhat 계열 8 이상 - Ubuntu 22 이상 ☐ Python - 3.10 - 3.13 ☐ Web Browser - MS Edge 16 이상 - Google Chrome 68 이상 ☐ DBMS - PostgreSQL 14 이상



4. SW구매시 제공되는 기능

4.1 다중 인증 기반 계정 보안 체계 (솔루션 공통)

신규 가입 승인, OTP 기반 로그인, 세션 제어, QR 코드 인증 등 다양한 계정 보안 기능을 제공합니다. 보안 강화를 위해 인증 앱을 통한 일회용 OTP 인증번호 입력 절차를 수행하며, 5회 이상 로그인 실패 시 계정 차단과 30분 미활동 시 세션이 만료 처리됩니다. 최초 로그인 및 비밀번호 분실 시 QR 코드로 발급된 인증번호를 검증하여 새 비밀번호를 설정할 수 있습니다.

4.2 RBAC 기반 권한 통제 (솔루션 공통)

역할 기반(RBAC) 제어를 통해 데이터의 관리와 보안 수준을 그룹별로 달리하여 관리합니다. 다양한 그룹을 생성하여 사용자별로 매핑하며, 메뉴 접근 및 행동 단위 권한에 따라 화면 내 버튼/메뉴를 동적으로 노출 또는 차단합니다. 권한에 따라 에이전트 조회·수정·삭제가 가능하며, 개인정보 열람 및 범위 또한 권한에 따라 설정하고 통제할 수 있습니다.

4.3 시스템 통합 관제 및 장애 대응 체계 (솔루션 공통)

CPU, GPU, 메모리 등 자원상태 및 API 호출 통계를 대시보드 그래프로 종합 시각화하고, 고유 식별자를 기반으로 API의 전체 호출 흐름을 연계하여 추적·모니터링합니다.

민감 정보를 탐지해 마스킹 처리하고, 정책 위반 질의는 LLM 전달 전 차단 및 로그를 기록합니다. 접속 이력과 주요 데이터 변경 행위를 수집해 관리자 필터링 분석을 지원하며, 장애 발생 시 등록된 SMTP 정보를 통해 담당자 메일로 서버 장애 정보 및 조치 안내를 자동 발송합니다.



4.4 API 키 발급 및 인증 보안 관리 (솔루션 공통)

에이전트 및 모델 외부 호출 시 사용되는 API 키의 발급, 관리, 인증 보안 기능을 제공합니다. 학습된 모델과 프롬프트 구성을 하나의 API 서비스 모듈로 구성하고 외부 호출용 고유 엔드포인트를 통해 접근 권한을 통제합니다. 생성된 AI 에이전트를 외부 서비스에 연동하기 위해 독립적인 API 키를 생성, 조회, 삭제할 수 있는 기능을 제공하며, 외부 시스템에서 호출 시 발급된 API키를 통해 유효성 검증 및 접근 제어를 수행하여 안전한 데이터 통신 환경을 지원합니다.

4.5 학습·평가 데이터 관리 (LLMOps 특화)

텍스트, 이미지, 오디오 등 다양한 형태의 데이터셋을 지원하며 비정형 문서를 활용하여 학습 데이터로 사용할 수 있습니다. 모델 성능 평가를 위한 평가용 데이터셋과 검증 데이터셋을 활용하여 모델 동작을 확인합니다. 또한, 사용자 편의를 위해 키워드 시뮬레이션 데이터 작성양식 샘플을 제공합니다.

4.6 모델 생애주기 통합 관리 및 배포 (LLMOps 특화)

외부 모델 등록부터 설정 관리, 버전/이력 추적, 다양한 운영 환경에의 배포까지 모델의 라이프사이클 전반을 통합 관리합니다. 사용자의 로컬 모델 직접 업로드 및 Hugging Face 등 오픈소스 플랫폼의 URL을 이용한 모델 수집/등록을 지원합니다. 각 모델 별 특성에 맞춰 지원되는 파라미터(Top-K, 응답 길이 등)를 UI에서 독립적으로 설정 가능하며, 모델을 다양한 운영환경(On-Premise, Cloud 등)에 손쉽게 배포하고 운영 상태를 모니터링 및 관리할 수 있습니다.



4.7 No-Code 기반 모델 파인튜닝 성능 평가 (LLMOps 특화)

SFT, LoRA, PEFT 등 다양한 기법을 지원하며, 코딩 없이 웹 UI에서 모델(LLM, Retriever 등)을 파인튜닝 할 수 있습니다. Epochs, Batch size 등 학습 조건 설정 기능과 권장 초기값을 제공하며 유효성 검증을 자동으로 수행하여 오류를 예방합니다. 학습 작업의 우선순위와 시작 시간을 대기열에 등록하여 자동실행하거나 수동으로 즉시 취소할 수 있습니다. 또한, BLEU, ROUGE 등 다양한 평가 기법을 제공하고 설정한 기준점수와 평가점수를 비교하여 산출된 평가 지표를 표 형태로 제공합니다.

4.8 모델 파이프라인 관리 (LLMOps 특화)

모델과 데이터 소스를 파이프라인 캔버스에서 시각적으로 연결하여 구성하고, 구성된 파이프라인 흐름을 저장하여 재사용합니다. 변경 이력을 추적하여 일부 설정 교체 후 즉각 재실행하여 결과를 비교할 수 있습니다. 재학습 성공 시 자동 반영(On/Off) 설정에 따라 운영 파이프라인 배포 및 교체가 가능하며, 파이프라인 대기열에 따른 자동 실행 기능과 사용자가 설정한 일시에 실행하는 수동 트리거 기능을 제공합니다.

4.9 프롬프트 관리 및 시뮬레이션 (LLMOps 특화)

요약, 회의록 등 자주 쓰이는 기본 템플릿을 내장하고, 대화 주제 도메인을 인식해 가장 적합한 템플릿을 자동 추천 및 매칭합니다. 시스템에서 사전 등록된 LLM 모델을 선택하여 시뮬레이션 할 수 있으며, 시뮬레이션 중 허용 범위를 검증받은 파라미터를 조정할 수 있습니다.

성공적인 결과 도출 시 프롬프트 원문과 파라미터 조합을 한 세트로 저장 및 재현합니다.



4.10 외부 AI 모델 연동 (LLMOps 특화)

신규 모델 추가 시 기존 시스템의 구조 변경 없이 API 연동 로직을 플러그인 또는 모듈 단위로 분리하여 유연한 확장성을 확보합니다. 다양한 AI 모델의 응답 포맷 차이를 흡수하여 공통된 출력 구조로 변환하여 처리합니다. AI 모델에 대한 정보(호출 URL, 인증 토큰, 파라미터 형식 등)를 설정 파일 또는 관리도구를 통해 등록 및 관리하며, 해당 설정 값을 기반으로 모델을 호출합니다.

4.11 에이전트 관리 (Agent Builder 특화)

신규 에이전트 생성 시 빈 캔버스에서 시작하거나, 기존 에이전트의 구성을 복제할 수 있으며, 목적별로 사전 정의된 샘플을 활용하여 빠르게 구성할 수 있습니다. 이름, 설명, 생성자, 마지막 수정일이 포함된 표 형태의 에이전트 목록 조회와 필터 검색 기능을 제공합니다.

동일 서버 내 기존 설정을 유지한 채 에이전트 복사 및 일괄 삭제가 가능하나, API 키가 연결된 에이전트는 시스템 보호를 위해 삭제할 수 없도록 제한합니다.

4.12 캔버스 작업 환경 및 시뮬레이션 (Agent Builder 특화)

카테고리(Input, Output, Data Sources, Model 등) 기반 메뉴에서 노드를 드래그 앤 드롭하여 캔버스에 즉시 배치하고 연결선 생성 및 매핑 기능을 지원합니다. 특정 노드에 프리즈(Freeze) 적용 시 재실행을 방지하고 이전 결과값을 고정하여 사용할 수 있습니다. Chat Input/Output 노드 포함 시 스트리밍 응답 출력이 지원되는 세션 기반 대화형 시뮬레이션 환경을 제공합니다.



4.13 멀티 툴 연동 Agent 노드 (Agent Builder 특화)

사용자 지시에 따라 외부 및 로컬 LLM이 판단하여 복수의 툴을 호출하고 실행 흐름을 자율적으로 제어하는 노드를 제공합니다. LLM이 MCP 기반 툴을 선택·호출 할 수 있도록 지원하며, 에이전트 노드 자체도 ‘툴 모드’를 활성화하여 다른 에이전트의 툴로 연결 및 사용이 가능합니다.

외부 LLM 호출 실패, MCP 서버 연결 실패 등 오류 발생 시 에러 메시지를 반환하고, 툴 실행 결과와 에이전트 호출 이력을 로그로 기록하여 확인합니다.

4.14 다양한 노드 지원 (Agent Builder 특화)

언어 모델(상용 또는 자사 모델)을 연결하여 텍스트 응답을 추론하고 생성하며, 동적 변수 지원 프롬프트 작성 및 임베딩 모델을 통한 벡터 변환을 지원합니다. Document AI를 통해 PDF, 이미지 문서에서 텍스트, 표, 이미지를 구조화하여 추출하고, Docling 라이브러리 기반 고급 문서 파싱을 지원합니다. 또한 호환 DB 쿼리 실행, if-Else 분기 라우팅, 커스텀 임베딩 및 커스텀 리랭커 노드를 지원하여 검색 결과와 RAG 응답 품질을 향상시킵니다.

4.15 당사 검색엔진 솔루션(Search Formula-1) 연동을 통한 키워드 및 벡터 검색 (Agent Builder 특화)

강력한 성능의 당사 검색 엔진 솔루션(Search Formula-1)을 연동하여 키워드 기반 검색 노드 및 벡터 검색 노드를 제공합니다.

동의어, 오타 교정, 금칙어, 카테고리 부스팅 등 다양한 검색 사전을 통합 관리하며, 기존 SF-1 V5/V6 버전의 사전데이터 이전 기능을 제공합니다.



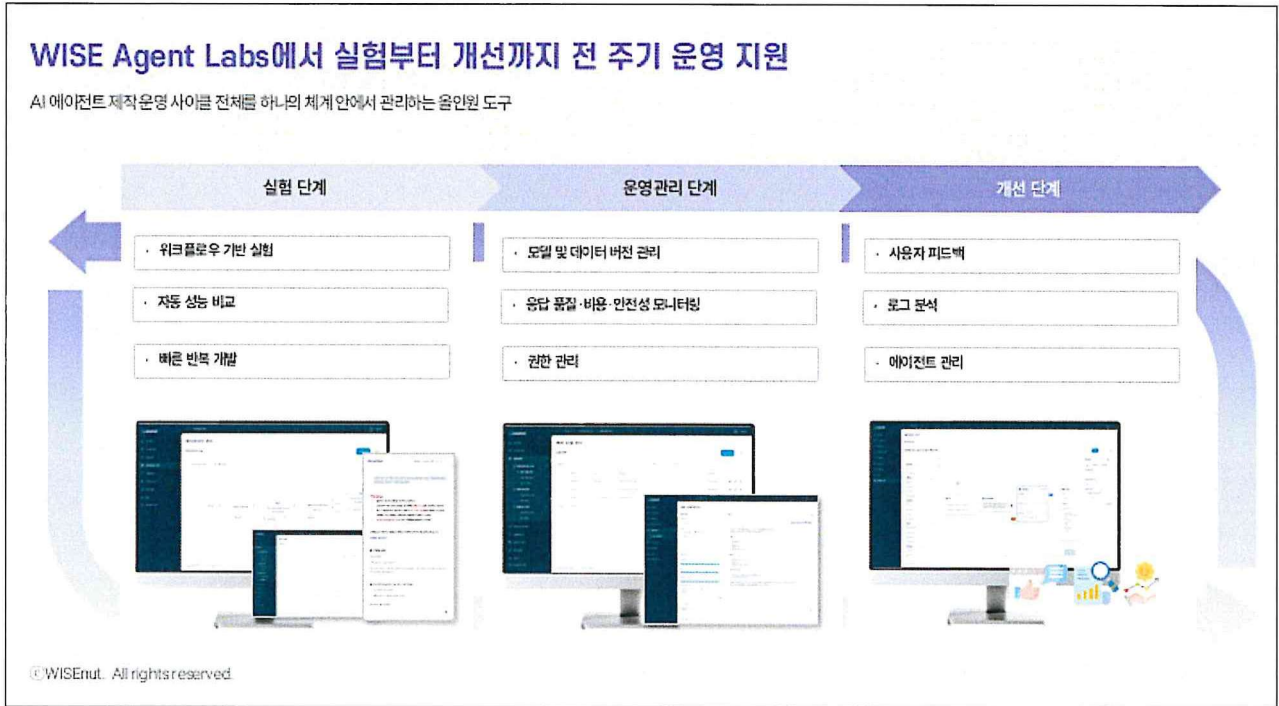
4.16 외부 도구 연동 - MCP 서버 관리 (Agent Builder 특화)

외부 도구 확장을 위한 Model Context Protocol (MCP) 서버 등록을 위해 JSON, STUDIO, Streamable HTTP 3가지 방식을 지원합니다.

자동 유효성 검증을 거친 후 필수 항목 기반으로 등록되며, 서버별 연결된 툴의 개수 현황을 파악할 수 있습니다. Agent 노드 하위에 다수의 툴 노드를 동시 연결하여 복합적인 문제를 해결하며, 툴 실행 결과를 LLM의 컨텍스트로 반환하여 최종 응답의 정확성을 향상시킵니다.



5. 서비스 구성 개념도



6. 공급 및 설치, 타 시스템과의 연계 지원방안

- 1) 공급 및 설치 : 계약 후, 30일 이내 제품 공급 및 설치 지원
- 2) 설치 지원 : 현장 설치, 원격 등을 통한 설치
- 3) 교육 및 운영방안 : 개발자, 운영자 교육 지원
- 4) 연계지원방안 : 별도 협의를 통한 지원

7. 제품 구성 및 납품 방법

7.1 제품 구성

구분	종류	수량	비고
CD	WISE Agent Labs V1 설치용 CD	1장	
제품인증서	소프트웨어 사용인증서	1부	
매뉴얼	운영자 매뉴얼	1부	
제품박스	CD, 제품인증서 첨부된 패키지박스	1EA	

7.2 납품 방법

납품 일정 및 장소, 방법 등은 구매 기관과 협의하여 진행합니다.

8. 검사 및 시험

8.1 로드맵 논의 및 기능 개발

로드맵 논의를 통하여 개발이 결정된 기능들에 대해 개발 부서에서 기능 개발 진행

8.2 단위/모듈 테스트

- 개발 완료 후 테스트 수행
- 개발자가 구축된 솔루션 도는 모듈에 대하여 테스트를 수행하여 고객 시스템 내부 운영이 정상적으로 운영됨을 확인

8.3 납품 및 검수

- 구매 기관 담당자의 입회하에 기관이 지정하는 방법에 따라 검수 실시
- 상품 설치 완료 후, 소프트웨어 기능별 작동 유무 등을 검사
- 규격서 상의 구입내역과 동일한 사양이 충족되고, 테스트 후 이상이 없을 때를 설치가 완료되는 시점으로 규정



9. 유지관리 서비스

- 구매 후 1년간 아래와 같이 무상유지관리 서비스 및 후속으로 유상 유지관리 서비스를 제공합니다.

유지관리 내용				설 명
항 목	세부항목	무상지원범위	유상지원범위	
기술 지원	장애발생 후 복구(응답시간)	4시간 이내 (상호협약후 정함)		- 시스템 장애 시 대응 시간, 장애 처리 절차 등
	정기점검	온라인 지원 또는 별도 협의	방문 또는 온라인 지원 (매월/분기/반기) ※구매자↔공급자간 비용 별도 협의	- 시스템의 장애를 사전에 예방하기 위하여 정기적으로 지원하는 정기점검, 정기성능 조율 서비스 - 제품의 점검 및 유지관리 이력관리, 시스템 사용자 관리지원 - 유지관리 작업 보고서 작성, 시스템 운영 보고서 작성
	일상지원	전화,e-mail, 온라인 원격지원 및 방문 지원		- 콜센터 운영, 사이트운영, 전화/email 등을 통한 장애접수, 질의응답
	이전 설치	-		- 제품의 이전 설치 유상 지원(비용 별도 협의)
	추가/변경작업	-	기본 M/D 제공	- 1회 요청시, 연속 3일 이하 작업 가능
제품 지원	업데이트 및 패치	원격지원	원격 및 방문지원	- 기존 SW 제품의 기능을 보완 및 새로운 기술의 적용이나 운영체제의 변화 등으로 발생하는 불일치 조정
	마이너 업그레이드	원격 및 방문지원	원격 및 방문지원	- 기존 SW 제품을 향상시키기 위하여 새로운 버전으로 교체하는 서비스(2.0→2.1, 버전의 소수점 변화)
교육 지원	상설 교육 (운영자/사용자)	연 2회		- 제품 운영/사용을 위한 운영자/사용자 교육 (와이즈넷 정기 상설교육 운영)

※ 유상유지관리 지원 범위는 선택형에 따라 지원 범위가 확장/축소 될 수 있음

사실과상위없음

사실과상위없음

10. 보안 준수

제품 설치 등을 위해 구매 기관 방문 시에는 구매 기관의 보안 규정을 준수합니다.

11. 저작권 및 사용권

공급된 소프트웨어의 저작권은 기본적으로 공급사에 있으며 구매 기관은 해당 소프트웨어에 대한 사용권만을 가집니다.

12. 담당자 연락처

홈페이지	www.wisenut.com
이메일 상담	sales@wisenut.com
고객센터	Tel. 02-3404-6100
팩스	Fax. 02-3404-6109
주소	경기도 성남시 분당구 대왕판교로 644번길 49 DTC타워 5,6층

