

AI Agent Backend 최지현

PORTFOLIO

Agent Architect

End-to-End 서비스

Trusted AI 추구

믿음직한

도메인 적응력

 GitHub : <https://github.com/ttoggle918>

 Email : zena101096@naver.com

 Blog: <https://zena1010.tistory.com>
<https://velog.io/@ttoggle918/posts>

★ ABOUT ME ★

구조적 사고 · 넓은 시야

협업 주도 · 소통 능력

가치 중심의 문제 정의

저는 LangGraph 기반의 Agent System 설계 및 오케스트레이션에 강점을 가진 AI Agent 엔지니어입니다.

1. 구조 설계

Agent System Design & Orchestration: LangGraph를 활용하여 다각적으로 비즈니스 문제를 분석하고 Agent Workflow를 설계한 경험.

2. 신뢰성 (믿음직한)

Trusted AI (RAG & Validation): LLM의 환각을 기술적으로 방지하고 교차 검증 및 신뢰도 스코어링을 통해 결과에 대한 믿음을 입증하는 로직을 구현.

3. 도메인 (적응력)

End-to-End Solution & Adaptability: 금융, 무역 등 새로운 도메인 지식을 빠르게 습득하여 Full-Stack AI 서비스를 완성한 역량.

★ SKILL ★

Agent / LLM Ops

LangGraph

GPT-4o

RAG

LangChain

Backend / Infra

Spring Boot

FastAPI (Async)

MSA (지향)

Docker

Redis

AI / ML / NLP

SBERT Fine-tuning

Random Forest

XGBoost

Whisper/DeepFace

★ CAREER & EDUCATION ★



Education

코드스테이츠 (AI 부트캠프)

- ML/DL 기초
- KoBERT 기업 협업

코드스테이츠 (AI 심화 NLP)

- BERT/STS Fine-tuning

#SBERT Fine-tuning
#Random Forest #XGBoost

Career

비상교육 (AI 연구개발 Cell)

- 실제 데이터 기반 AI 서비스 PoC (ML/NLP)
 - 이탈 고객 예측
 - 질문 답변 시스템

Education

KOSA (생성형 AI 통합 과정)

- LangGraph 설계 및 FastAPI E2E 구현 ([KOCRUIT])

KOSA (Spec-up 프로젝트)

- Trusted RAG Agent 아키텍처 ([K-Bridge])

#RAG #LangGraph
#Spring Boot #FastAPI

Career (KOSA (AI 연구개발 Cell))

- AI 개발 교육 보조강사
 - 교강사 대상 보수 교육
 - AI 개발 강의
 - 기술 멘토링
 - 운영 지원

★ EDUCATION & FORMAL BACKGROUND ★

학력 사항	명지대학교 컴퓨터공학과	기술적 관점에서 논리/구조 분석 및 문제 정의 능력 배양
핵심 이수 과정 1	KOSA 생성형 AI 활용 과정 (960시간)	E2E Agent 서비스 아키텍처, LangGraph, FastAPI 집중 학습
핵심 이수 과정 2	코드스테이츠 AI 부트캠프 (1120시간)	ML/DL/NLP 기초 이론 및 기업 협업 프로젝트 기반 학습

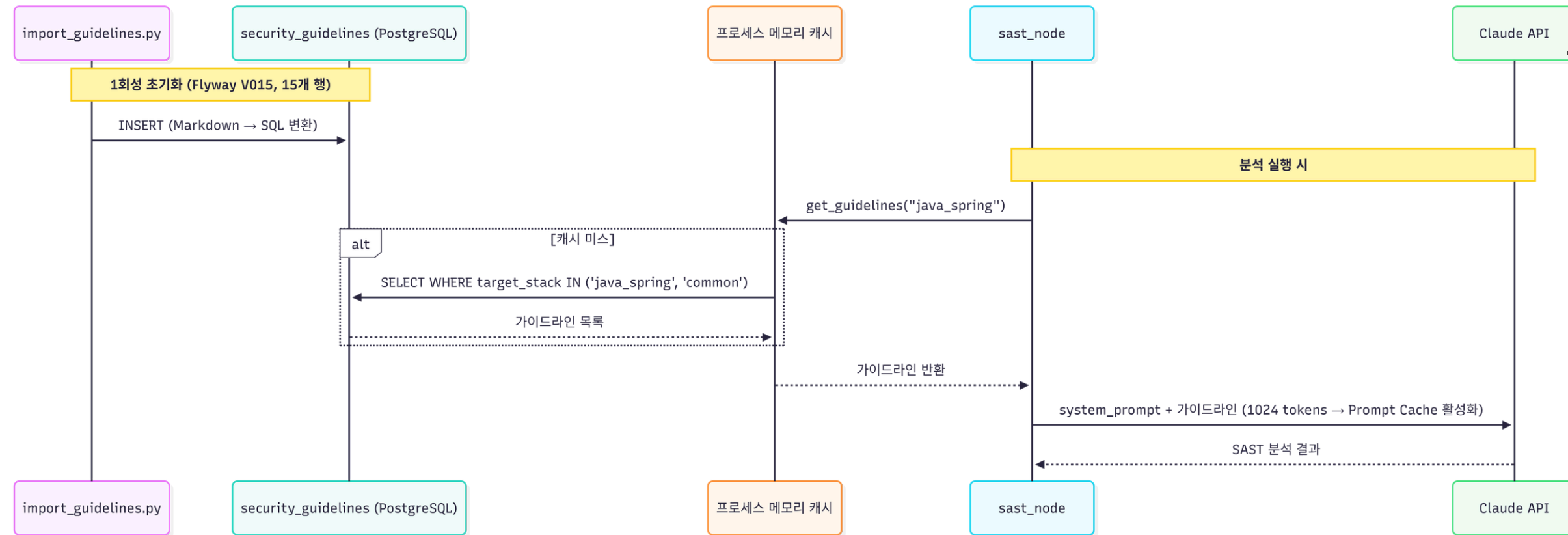
★ CAREER ★

KOSA AI 교육 보조강사 파트타임	2026.03 ~ 현재 (4개월)	교강사 대상 AI 개발 역량강화 교육 실습 멘토링 및 운영 지원 - 기술 멘토링: 수강생 실습 코드 디버깅, 에러 슈팅 및 AI 기술 질의응답 - 운영 지원: 실습 환경 세팅 및 전반적인 교육 행정 업무 수행
비상교육 (AI 연구개발 cell)	2022.09 ~ 2023.03 (6개월)	실제 기업 데이터 기반 AI 서비스 프로토타입 개발 (ML/NLP) <u>이탈 고객 예측</u>: "Random Forest/XGBoost 멀티 모델링으로 이탈 예측 정확도 85.3% 달성" <u>QA 시스템</u>: "SBERT Fine-tuning을 통해 문맥 유사도 정확도 0.90 확보 및 개인정보 익명화 파이프라인 구축"
세코닉스 (인사팀 인턴)	2019.06 ~ 2019.08	비개발 직무 경험 (인사관리 및 행정 지원) <u>이탈 고객 예측</u>  상세 설명 바로가기 <u>QA 시스템</u>  상세 설명 바로가기

★ AI 기반 코드 보안 분석 플랫폼 SECUREAI ENGINE

#TrustworthyAI #DAST교차검증 #FalsePositive감소 #보안원칙수호

신뢰성 확보



해결한 문제

LLM의 코드 분석 시 발생하는 높은 오탐률(False Positive)과 환각으로 인한 신뢰성 부족 및 원칙 우회 리스크.

성과

- 취약점을 '찾았다'가 아닌 '증명했다'로 전환하여 실무에 즉시 도입 가능한 수준의 AI 신뢰성 확보

그림 : 보안 가이드라인 DB 주입 (경량 RAG)

설계 포인트 및 신뢰성 확보 (Point)

- ◆ Framework-aware 프롬프트: React 자동 이스케이프 등 프레임워크 특성을 AI에 주입하여 초기 40~50%에 달하던 오탐률 대폭 감소.
- ◆ DAST 샌드박스 교차 검증: SAST가 '의심'한 취약점을 완전 격리된 Docker 샌드박스에서 실제 익스플로잇으로 '증명'하여 무결성 확보
- ◆ 보안 원칙 수호 (ADR-016): MCP의 파라미터 바인딩 미지원(SQL 인젝션 위험) 문제를 인지하고, 편의성 대신 Backend API 경유로 우회하여 핵심 보안 원칙 준수.

★ AI 기반 코드 보안 분석 플랫폼 ★ SECUREAI ENGINE

#DevSecOps #AgentArchitect #컴플라이언스자동화 #비용절감

서비스 가치

해결한 문제

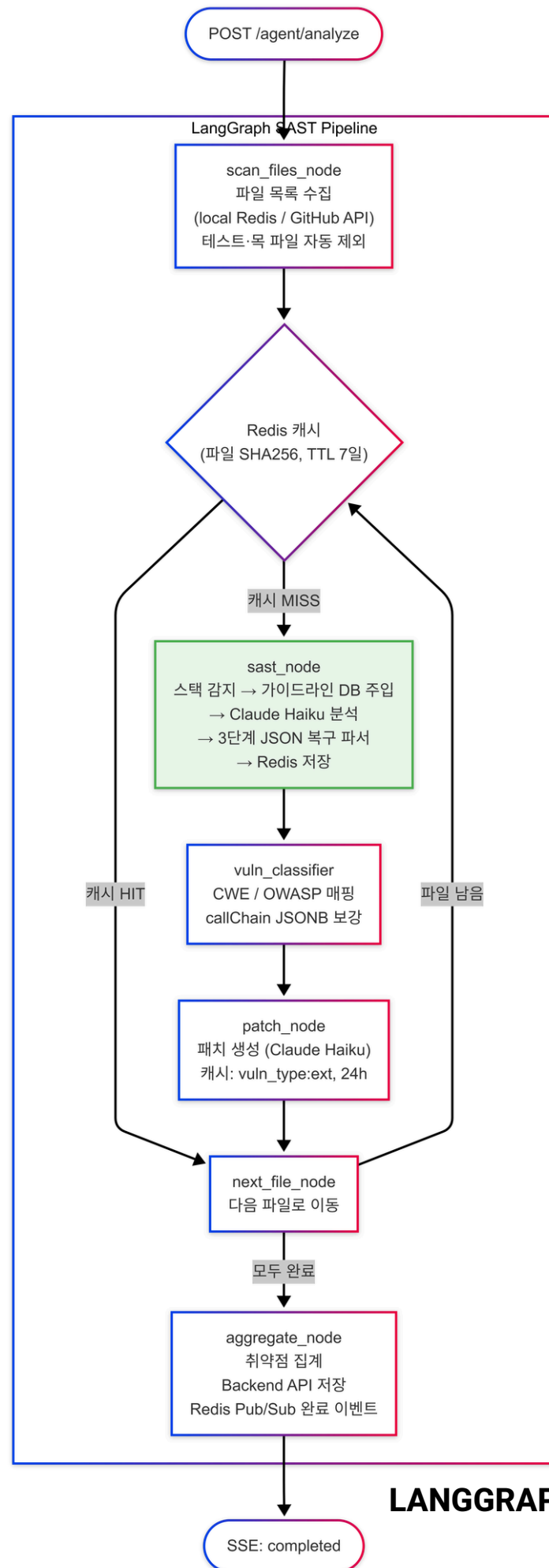
보안 점검 누락 리스크 및 한국형 규제(ISMS-P, 행안부 등) 증적 문서를 일일이 작성해야 하는 리소스 낭비.

제공하는 가치

- ◆ 자동 보안 분석: GitHub 주소 입력 시 파일별 취약점 분석부터 수정 코드까지 자동 생성.
- ◆ 컴플라이언스 증적 자동화: CISO, 행안부, ISMS-P 3종 증적 문서 및 리포트 자동 생성.
- ◆ 비용 및 시간 절감: SHA256 해시 기반 캐싱으로 재분석 시 AI 호출 0회 (비용 대폭 절감).

성과

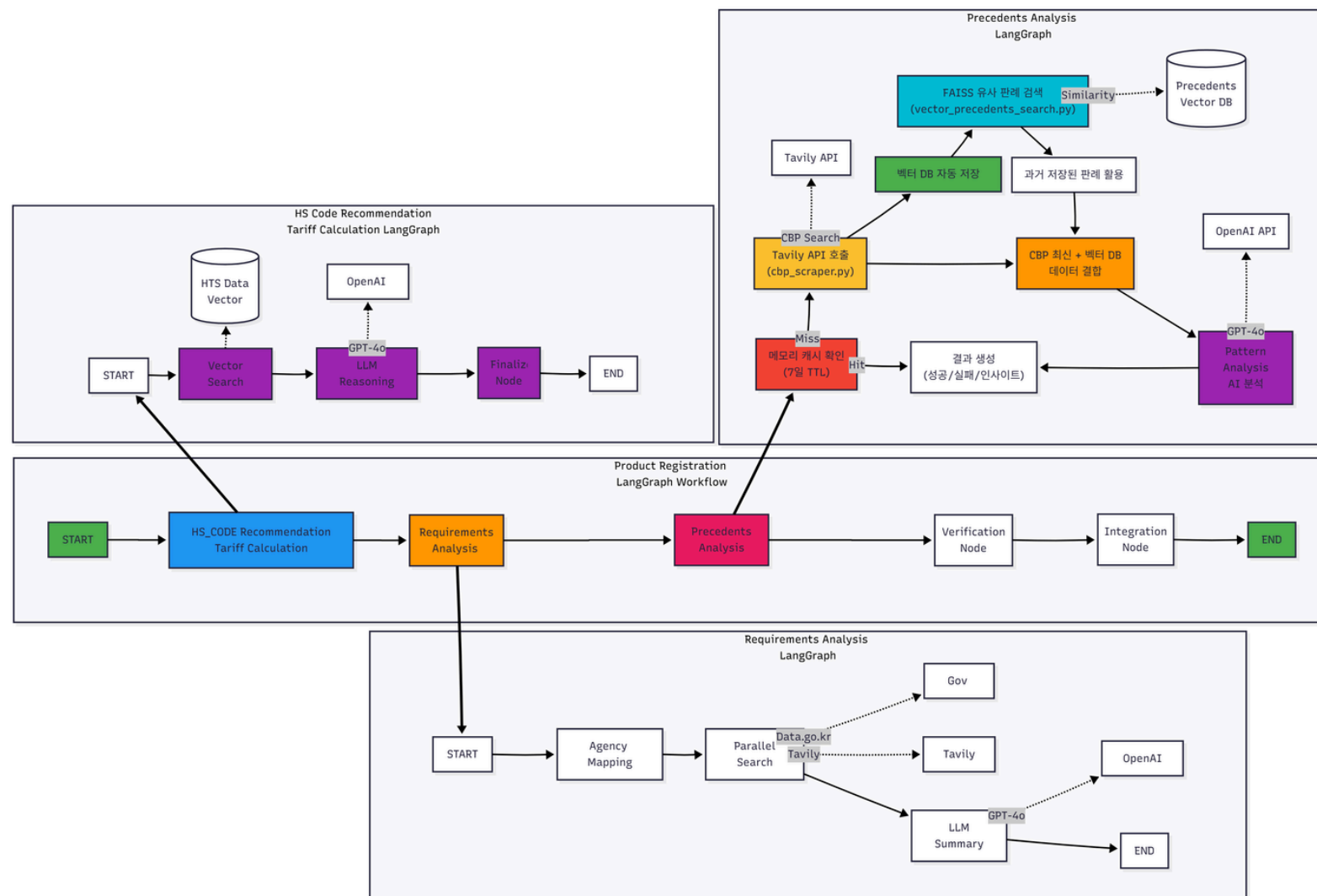
- 규제 대응 리드타임을 획기적으로 단축하여 감사 예산 및 공수 절감
- 기존 SAST 도구를 넘어선 "한국형 컴플라이언스 자동화 플랫폼"으로 비즈니스 해자 구축.



LANGGRAPH SAST 파이프라인

★ HS코드/규제 자동 분석 RAG AGENT 플랫폼 ★

#도메인적응력 #가치중심의문제정의 #무역행정자동화 #AgentArchitect 비즈니스가치 중심



LangGraph 워크플로우

문제 정의

복잡하고 방대한 수출입 규제 문서를 사람이 일일이 확인해야 하는 법적/시간적 리스크.

해결 방법

- HS코드 하나로 끝내는 스마트 규제 분석
- Multi-Stage CoT Agent: 규제-절차-리스크-사후 관리 4단계를 순차 분석하는 LangGraph 파이프라인 설계.

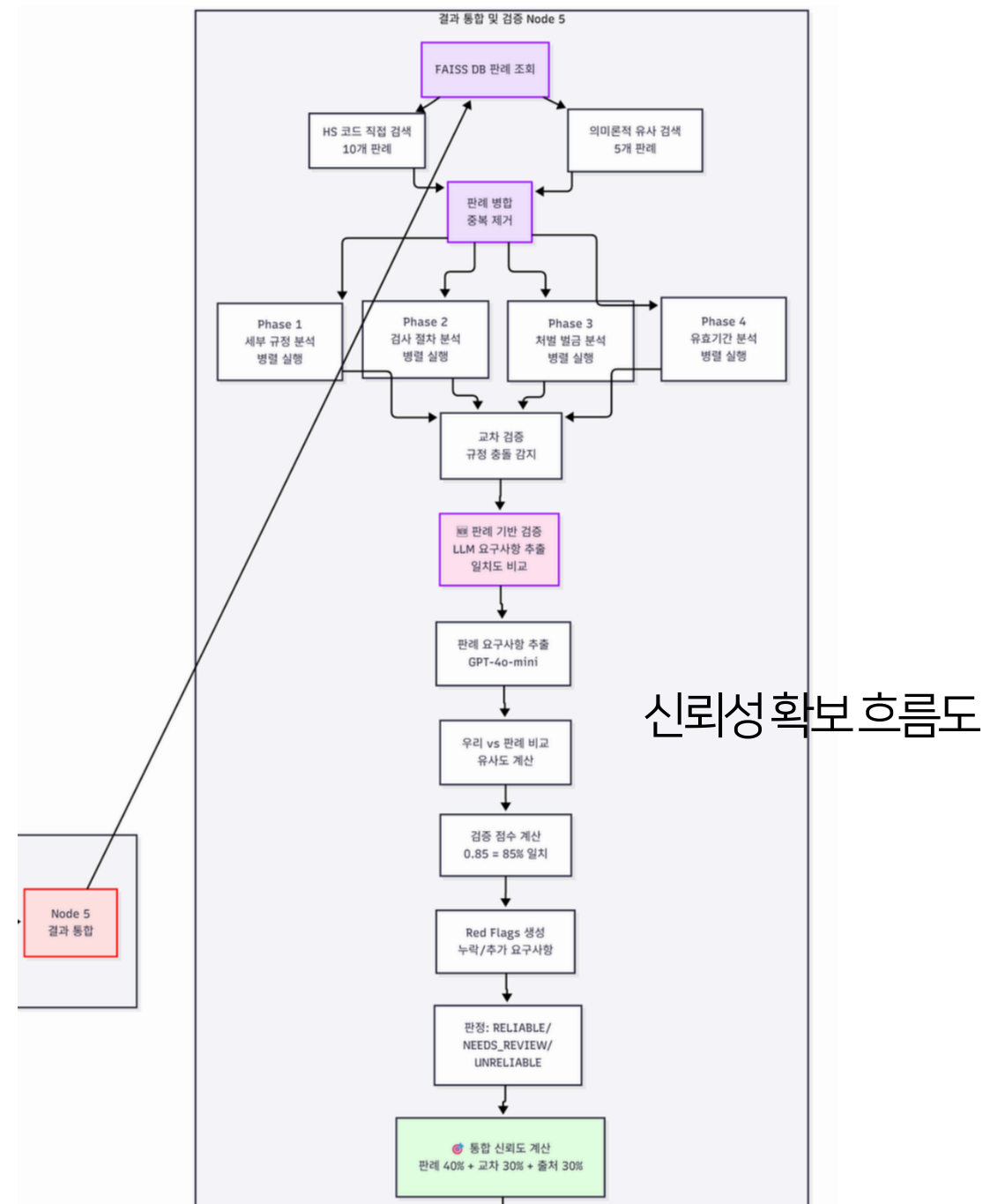
성과 (Impact)

- 규제 데이터의 복잡성 해결
- Hybrid 구조: 공공 API + 검색엔진 결합으로 정보 최신성 확보
- 규제 불확실성 해소 및 통관 사전 준비 시간 획기적 단축

★ HS코드/규제 자동 분석 RAG AGENT 플랫폼 ★

#RAG #TrustworthyAI #CrossValidation #LangGraph #CoT

신뢰성 확보 Agent



신뢰성 확보 흐름도

문제 정의

"LLM의 법률 데이터 할루시네이션(Hallucination)으로 인한 결과 신뢰성 부족"

해결 방법: 병렬 추론 및 Cross-Validation 아키텍처

- LangGraph를 활용해 '요건 분석'과 '판례 검증' 노드를 비동기 병렬로 실행.
- 두 결과의 논리적 모순을 체크하는 재검증(Re-verification) 노드 설계.
- Vibe Coding 활용: AI 어시스턴트를 활용해 복잡한 에이전트 상태 전이 로직을 신속히 검증하고 TDD 적용.

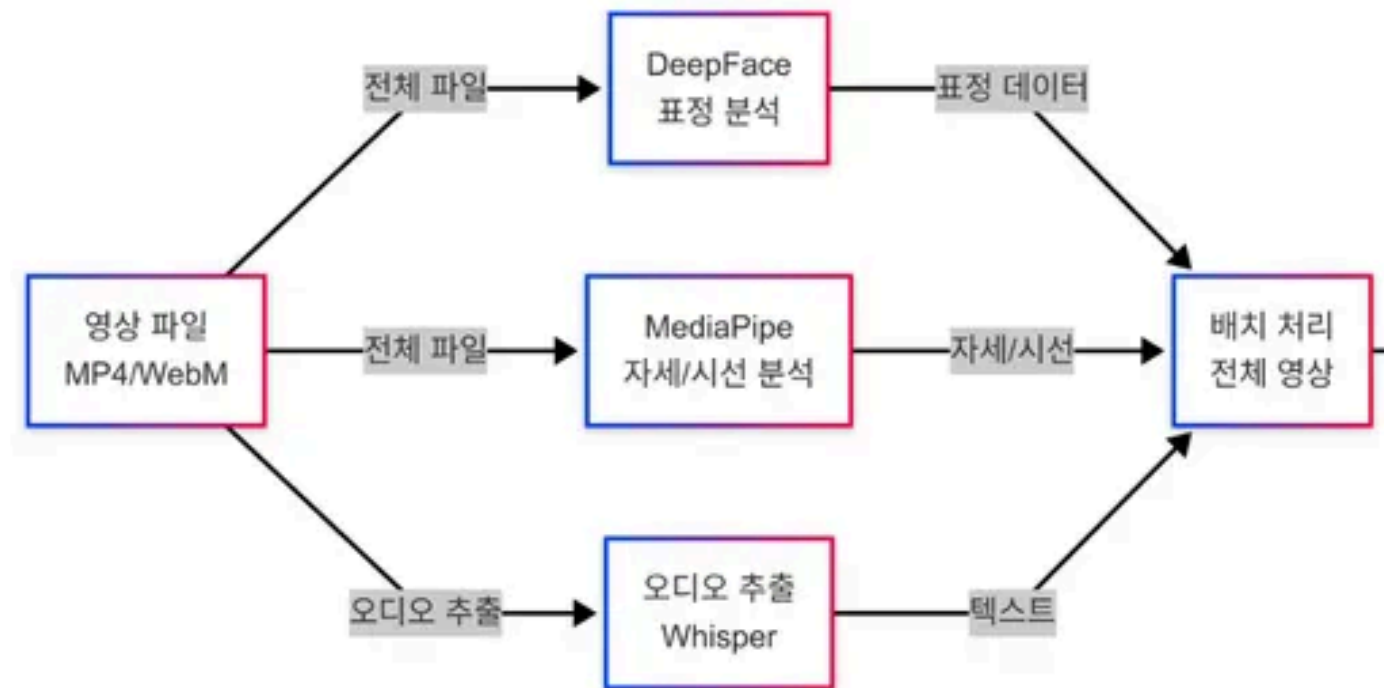
성과 (Impact)

- 신뢰도 확보: 판례/규정 Cross-Validation으로 신뢰도 스코어링 로직 구현

★ AI AGENT 기반 기업용 채용 관리 시스템 ★

#End-to-End서비스 #Multimodal #AgentOrchestration #TeamLead

서비스 혁신 중심



[Multimodal Analysis] 영상 및 음성 처리 파이프라인

문제 정의

단순 반복 업무(서류/일정)로 인한 비효율
채용 과정의 리소스 낭비 및 면접관의 주관적 평가 개입.

해결 방법 (Agent)

1. 멀티모달 분석: Whisper(음성) + DeepFace(표정)를 통한 6차원 정량 평가 리포트 제공.

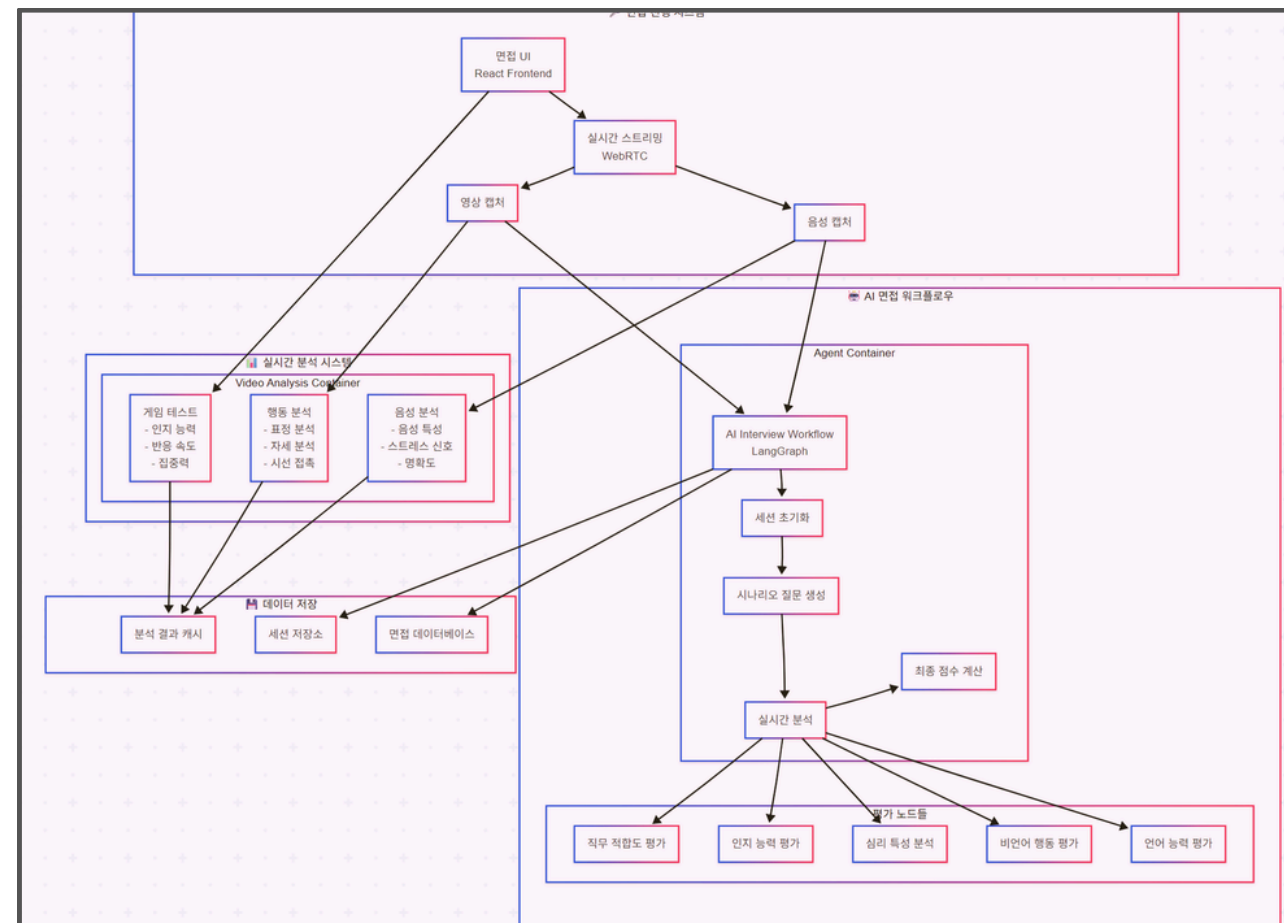
성과 (Impact)

- 업무 시간 단축 (자동화).
- 면접 자동화 시스템 구축 및 멀티모달 기반 6차원 정량 평가 리포트 제공.

★ AI AGENT 기반 기업용 채용 관리 시스템 ★

#Backend #LangGraph #AgentOrchestration #FastAPI

아키텍처 의사결정



LangGraph 워크플로우 다이어그램 이미지

문제 정의

"기존 Java 환경에서 Python 기반 AI 모델 연동 시 발생하는 성능 병목 및 비동기 처리 한계"

해결 방법 : FastAPI 마이그레이션 및 상태 기반 에이전트 설계

- Spring Boot → FastAPI 전환: Whisper, LLM 등 Python 기반 모델과의 최적 호환성 및 비동기 스트리밍 성능 확보.
- LangGraph Orchestration: '분석-전략-생성-검토'로 이어지는 인간의 사고 프로세스를 모듈화된 노드로 구현.
- Redis Caching: 반복적인 AI 분석 요청에 대한 응답 속도 최적화.

FUTURE PLANS



대체 불가능한

AI Service Architect

FUTURE PLANS: End-to-End AI Service Architect를 목표합니다.

1. 고성능 Agent-Backend 통합 아키텍처 구축

향후 3년 내, LangGraph의 상태 관리와 FastAPI의 비동기 처리를 결합하여 대규모 트래픽에서도 견고하게 동작하는 에이전트 시스템 전문가로 성장하겠습니다.

2. 신뢰성 보장을 위한 LLMOps 파이프라인 설계

단순 구현을 넘어, 에이전트의 답변 품질을 정량화하고 지속적으로 개선할 수 있는 자동화 평가 및 모니터링(LLMOps) 환경을 구축하는데 집중할 계획입니다.

3. 비즈니스 문제를 해결하는 Multi-Agent Ecosystem 리더

궁극적으로는 다수의 특화 에이전트가 외부 툴 및 DB와 유연하게 상호작용하는 High-Scalability 시스템을 주도적으로 설계하여, 기술로 실질적인 비즈니스 가치를 창출하는 솔루션 아키텍트가 되겠습니다.

★ CONTACT ★

 Portfolio: <https://notion.site/Portfolio...>

 GitHub : <https://github.com/ttogle918>

 Email : zena101096@naver.com

 Blog: <https://zena1010.tistory.com>

 Phone : [010-9077-9318](tel:010-9077-9318)

THANK YOU

가치 중심의 문제 정의

협업 주도·소통 능력

AI Service Architect

믿음직한

도메인 적응력