제주경찰청 수사과 **Agent [JJ-301-103]** 개발 계획서

1. AI Agent 개발 방법과 절차

1.1 기능 정의 및 역할

- 수사 지원: 수사 계획 수립 및 진행 관리
- 증거 관리: 디지털 증거 수집 및 분석 지원
- 사건 분석: 사건 패턴 분석 및 연관성 도출
- 용의자 추적: 용의자 정보 관리 및 추적 지원
- 수사 협력: 타 기관과의 수사 협력 조정
- 보고서 작성: 수사 보고서 자동 생성 지원

1.2 개발 절차

1. 요구사항 분석 (1주)
    - 수사과 고유 업무 프로세스 분석
    - 수사 관련 법적 요구사항 검토
    - 보안 및 기밀성 요구사항 정의
2. 시스템 설계 (1주)
    - 수사 정보 관리 시스템 설계
    - 증거 체인 관리 시스템 설계
    - 고도 보안 아키텍처 구축
3. 모델 개발 (2주)
    - 수사 특화 AI 모델 구축
    - 패턴 분석 및 추론 엔진 개발
    - 자연어 처리 기반 보고서 생성
4. 통합 테스트 (1주)
    - 수사 시나리오별 기능 검증
    - 보안성 및 기밀성 테스트
    - 법적 요구사항 준수 확인

1.3 핵심 기술 스택

- **LLM**: DeepSeek R1 Distilled (32B 모델)
- 보안: 군사급 암호화, HSM
- 분석: Neo4j, Apache Spark
- 검색: Elasticsearch, Vector DB

- 협업: Secure API Gateway

2. 파인튜닝 데이터셋

2.1 공개 데이터

1. 법령 및 절차
    - 형법 및 형사소송법 (15,000건)
    - 경찰수사규칙 (3,000건)
    - 수사기법 관련 법령 (2,000건)
    - 증거법 관련 판례 (5,000건)
2. 수사 기법 및 매뉴얼
    - 경찰수사매뉴얼 (공개 부분)
    - 디지털 포렌식 가이드
    - 국제수사협력 절차서
    - 과학수사 기법 자료
3. 범죄 유형별 데이터
    - 범죄 통계 및 동향 분석
    - 범죄 수법 분류체계
    - 국제 범죄 동향 보고서
    - 사이버 범죄 분석 자료
4. 학술 연구 자료
    - 범죄학 연구 논문
    - 수사기법 연구 자료
    - 법과학 연구 결과
    - 행동분석 이론서

2.2 비공개 데이터

1. 수사 업무 데이터
    - 수사과 내부 업무 지침 (보안등급: 비밀)
    - 수사 절차 매뉴얼 (내부용)
    - 증거 관리 프로토콜
    - 수사 보고서 양식 및 작성법
2. 사건 처리 사례
    - 고도 익명화된 해결 사건 사례 (500건)
    - 수사 기법별 성공 사례
    - 타 기관 협력 우수 사례
    - 국제 공조 수사 사례
3. 분석 도구 및 기법

    - 범죄 분석 도구 사용법
    - 패턴 분석 알고리즘
    - 용의자 프로파일링 기법
    - 증거 연관성 분석 방법
4. 협력 체계 정보
    - 타 기관 협력 프로토콜
    - 국제 공조 절차 매뉴얼
    - 전문기관 연계 방법
    - 과학수사 의뢰 절차

3. 개발 일정표 **(20**일간**)**

1주차 **(Day 1-5):** 기초 설계 및 보안 환경 구축

Day 1 (월요일**)**

오전 **(09:00-13:00)**

- 수사과 업무 프로세스 심층 분석
- 수사 관련 법적 요구사항 검토
- 보안 및 기밀성 요구사항 정의

오후 **(14:00-18:00)**

- 고보안 개발 환경 구축
- 접근 권한 관리 시스템 설계
- 데이터 보안 정책 수립

Day 2 (화요일**)**

오전 **(09:00-13:00)**

- DeepSeek R1 32B 모델 보안 설정
- 암호화 통신 환경 구축
- 보안 모니터링 시스템 구축

오후 **(14:00-18:00)**

- 수사 도메인 데이터 수집 계획
- 공개 데이터 보안 검증 후 수집
- 데이터 분류 체계 구축

Day 3 (수요일**)**

오전 **(09:00-13:00)**

- 수사 정보 관리 시스템 설계
- 증거 체인 관리 아키텍처

- 사건 연관성 분석 시스템 설계

오후 **(14:00-18:00)**

- 고보안 데이터베이스 설계
- 암호화 저장소 구축
- 접근 로그 시스템 구현

Day 4 (목요일**)**

오전 **(09:00-13:00)**

- 비공개 데이터 보안 수집
- 데이터 익명화 및 마스킹
- 보안 등급별 데이터 분류

오후 **(14:00-18:00)**

- 훈련 데이터셋 보안 구축
- 수사 시나리오 데이터 생성
- 검증 환경 구축

Day 5 (금요일**)**

오전 **(09:00-13:00)**

- 보안 파인튜닝 환경 준비
- 모델 보안 설정 및 검증
- 암호화 모델 저장소 구축

오후 **(14:00-18:00)**

- 1주차 보안 검토
- 접근 권한 최종 확인
- 보안 정책 문서화

2주차 **(Day 6-10):** 모델 파인튜닝 및 핵심 수사 기능 개발

Day 6 (월요일**)**

오전 **(09:00-13:00)**

- DeepSeek R1 보안 파인튜닝 시작
- 수사 도메인 특화 학습
- 법리 추론 능력 강화

오후 **(14:00-18:00)**

- 사건 접수 및 분류 모듈
- 자동 수사 계획 수립 시스템

- 우선순위 판단 알고리즘

Day 7 (화요일**)**

오전 **(09:00-13:00)**

- 모델 파인튜닝 지속
- 수사 전문 용어 학습 강화
- 법적 추론 정확도 향상

오후 **(14:00-18:00)**

- 증거 관리 시스템 개발
- 디지털 증거 분석 지원
- 증거 체인 추적 기능

Day 8 (수요일**)**

오전 **(09:00-13:00)**

- 모델 성능 평가 및 최적화
- 수사 시나리오 정확도 검증
- 법적 준수성 검토

오후 **(14:00-18:00)**

- 패턴 분석 엔진 개발
- 사건 연관성 도출 알고리즘
- 용의자 프로파일링 지원

Day 9 (목요일**)**

오전 **(09:00-13:00)**

- 보고서 자동 생성 모듈
- 수사 문서 표준화 시스템
- 법적 양식 준수 검증

오후 **(14:00-18:00)**

- 수사 협력 지원 시스템
- 타 기관 연계 인터페이스
- 정보 공유 프로토콜 구현

Day 10 (금요일**)**

오전 **(09:00-13:00)**

- 보안 통신 모듈 구현
- 암호화 메시징 시스템
- 기밀 정보 전송 기능

오후 **(14:00-18:00)**

- 2주차 통합 테스트
- 보안성 검증
- 수사 워크플로우 테스트

3주차 **(Day 11-15):** 고급 분석 기능 및 시스템 연동

Day 11 (월요일**)**

오전 **(09:00-13:00)**

- 고급 범죄 분석 모듈
- 범죄 예측 알고리즘
- 핫스팟 분석 기능

오후 **(14:00-18:00)**

- 용의자 추적 시스템
- 동선 분석 및 예측
- 행동 패턴 분석 기능

Day 12 (화요일**)**

오전 **(09:00-13:00)**

- 디지털 포렌식 지원 도구
- 메타데이터 분석 기능
- 타임라인 재구성 시스템

오후 **(14:00-18:00)**

- 국제 공조 지원 시스템
- 다국어 번역 및 법령 대조
- 국제 범죄 데이터베이스 연동

Day 13 (수요일**)**

오전 **(09:00-13:00)**

- 보안 관제 인터페이스 개발
- 실시간 수사 현황 모니터링
- 권한별 정보 접근 제어

오후 **(14:00-18:00)**

- 모바일 수사 지원 앱
- 현장 수사관용 도구
- 보안 통신 기능 포함

Day 14 (목요일**)**

오전 **(09:00-13:00)**

- 수사 성과 분석 시스템
- KPI 자동 생성 및 추적
- 수사 효율성 측정 도구

오후 **(14:00-18:00)**

- 최고 보안 강화 작업
- 다중 인증 시스템
- 생체인식 연동 기능

Day 15 (금요일**)**

오전 **(09:00-13:00)**

- 3주차 보안 통합 테스트
- 전체 시스템 보안성 검증
- 침투 테스트 실시

오후 **(14:00-18:00)**

- 성능 최적화 및 안정성 확보
- 대용량 데이터 처리 테스트
- 동시 접속 부하 테스트

4주차 **(Day 16-20):** 최종 통합 및 보안 검증

Day 16 (월요일**)**

오전 **(09:00-13:00)**

- 상위 Agent와 보안 연동
- 제주경찰청 Agent와 정보 공유
- 권한별 접근 제어 검증

오후 **(14:00-18:00)**

- 타 수사 기관과 연동 테스트
- 검찰청 Agent와 협업 검증
- 법원 Agent와 정보 연계

Day 17 (화요일**)**

오전 **(09:00-13:00)**

- 실제 수사 시나리오 테스트
- 범죄 유형별 대응 검증

- 긴급 수사 상황 대응 테스트

오후 **(14:00-18:00)**

- 최종 보안 최적화
- 암호화 성능 향상
- 응답 시간 최적화

Day 18 (수요일**)**

오전 **(09:00-13:00)**

- 수사관 교육 자료 작성
- 보안 운영 매뉴얼 작성
- 법적 준수 가이드라인 완성

오후 **(14:00-18:00)**

- 시스템 관리자 보안 가이드
- 장애 대응 및 복구 계획
- 보안 감사 추적 문서화

Day 19 (목요일**)**

오전 **(09:00-13:00)**

- 최종 보안 시스템 검증
- 24시간 연속 보안 모니터링
- 침입 탐지 시스템 테스트

오후 **(14:00-18:00)**

- 배포 환경 보안 설정
- 운영 보안 정책 적용
- 백업 및 복구 보안 검증

Day 20 (금요일**)**

오전 **(09:00-13:00)**

- 보안 시연 시나리오 준비
- 익명화된 실제 사례 데모
- 최종 보안 점검

오후 **(14:00-18:00)**

- 프로젝트 완료 보고서 작성
- 보안 운영 계획 수립
- 지속적 보안 개선 방안 제시

4. 예상 성과

- 수사 계획 수립 시간 60% 단축
- 증거 분석 정확도 85% 이상
- 사건 해결율 25% 향상
- 수사 보고서 작성 시간 70% 단축
- 타 기관 협력 효율성 40% 개선