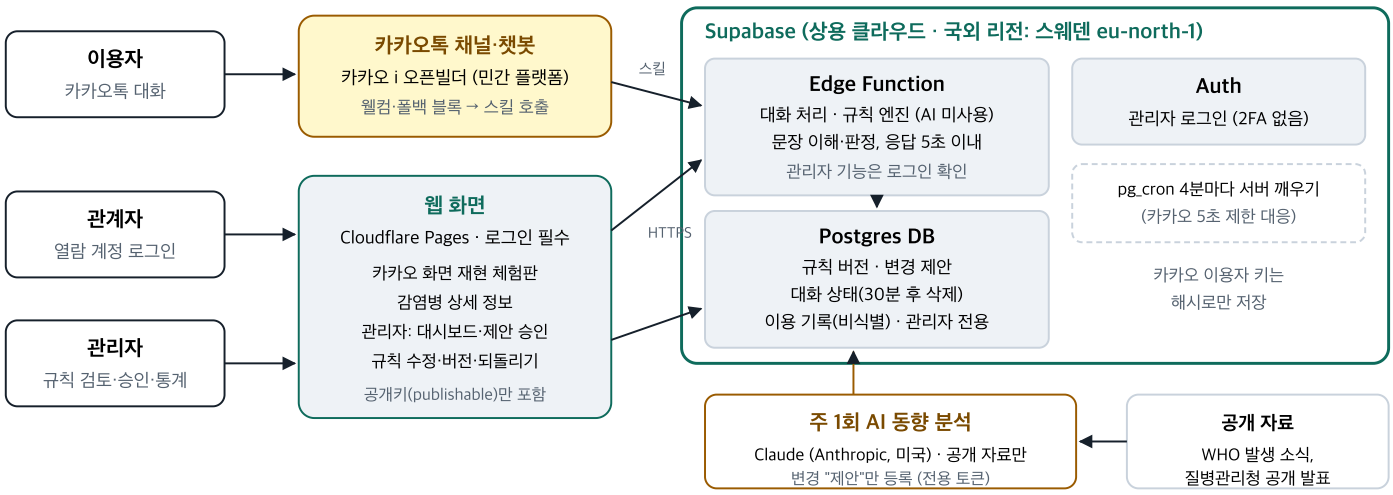
검역감염병 자진신고 지원 챗봇 데모 — 시스템 구성 및 보안 검토 질의서

해외 방문 후 증상이 있는 이용자가 카카오톡에서 증상·방문 정보를 말하면 관련 검역감염병과 상담 창구를 안내하는 시범 구성에 대해 보안 검토 의견을 요청합니다.

시연용 프로토타입
작성 2026-11-02
https://ev-quarantine-chatbot.pages.dev

1. 시스템 구성도



2. 현재 구성 요약

- **입력**: 증상, 방문 국가, 귀국 후 경과 구간. 이름·연락처·정확한 날짜는 받지 않음
- **안내**: 관련 감염병 최대 3개, 참고 정보·상담 권장·즉시 상담 권장. "진단 아님" 명시
- **저장**: 대화 상태 30분 후 삭제, 이용 기록은 증상·국가·결과 등급만 (비식별)
- **규칙 관리**: 버전·승인 이력·되돌리기, 바꾸기 전후 판정 비교 후 승인
- **웹사이트**: 관계자 계정(열람·관리자) 로그인 뒤에만. 일반 이용자는 카카오톡으로만 이용
- **판정**: 승인된 규칙(룰셋)으로만 판정. 이용자 응답에 생성형 AI 미사용
- **상담 연계**: 1339·관할 검역소 안내 (시연에서는 실제 연결 안 함)
- **AI 활용**: 주 1회 공개 자료 조사 → 변경 제안 → 관리자 승인 시에만 반영
- **호스팅**: 카카오(국내), Cloudflare(글로벌), Supabase(스웨덴). CSAP 인증 아님

3. 질의 사항

#	분야	질의	데모 현황 (참고)
1	**민감정보**	증상(건강 정보)을 받는 것이 개인정보보호법상 민감정보 처리에 해당하는지. 이름·연락처 없이 카카오 이용자 키를 해시로만 둘 때도 별도 동의가 필요한지	증상·국가·경과 구간만 저장, 이용자 키는 해시
2	**민간 메신저**	카카오톡 채널을 기관 공식 창구로 운영할 때의 기준(비즈니스 인증, 대외 승인)과 이용자 대화가 민간 플랫폼을 거치는 것의 허용 여부	개인 채널(시연), 검색 비허용
3	**보관·파기**	대화 상태·이용 통계의 보관 기간 기준, 통계를 사업 평가 목적으로 쓸 수 있는 범위	대화 상태 30분, 통계는 무기한 (데모 초기화로 삭제)
4	**원문 수집 (계획)**	인식 개선용으로 못 알아들은 문장 원문을 저장해도 되는지 (숫자·이메일 가림, 30일 후 삭제, 관리자만 열람)	아직 저장하지 않음
5	**생성형 AI**	해외 생성형 AI로 공개 자료만 조사해 규칙 변경을 "제안"하는 방식이 기관 AI 활용 보안 지침상 허용되는지, 추가 조건(입력 금지 정보, 승인 절차)	이용자 데이터는 AI에 넣지 않음, 반영은 관리자 승인 후
6	**클라우드 이용**	국외 리전 상용 클라우드 사용 가능 여부, 실서비스 시 CSAP 인증·국내 리전 필수 여부	Supabase 스웨덴, Cloudflare 글로벌
7	**안내 책임**	안내 등급·문구가 대민 안내로 적절한지, 의료·법무 검토가 필요한지 (오안내 시 책임 범위)	"의료적 진단이 아닌 검역 행정 참고용" 표시
8	**관리자 보안**	규칙을 바꾸는 관리자 화면에 2단계 인증·접근 IP 제한·제안자와 승인자 분리가 필요한지	웹 전체 로그인 필수, 아이디·비밀번호만, 승인 이력·버전 기록
9	**외부 연계**	카카오 스킬 서버 호출 인증 방식(현재 주소에 비밀 키)의 적정성, 실서비스 시 신고 접수(Q-CODE 등) 연계 요건	주소 내 키 확인, 외부 연계 없음
10	**검토 절차**	정보화사업 보안성 검토, 웹 취약점 점검, 개인정보 영향평가 대상 여부와 필요한 산출물	미실시