사내 메일 PII(개인 식별 정보) 마스킹 AI AGENT

RBAC 권한 분리

시스템의 보안과 안정적인 운영을 위해 사용자 권한을 4개의 역할 기반으로 세분화하여 관리

역할: System Admin(시스템 관리자), Policy Admin(정책 관리자), Auditor(감사자), User(일반 사용자)

SMTP 연결을 통한 즉각 전송

- 메일이 외부로 전송되기 직전, 마스킹 페이지를 거쳐 실시간으로 PII 마스킹을 수행한 후 즉시 다음 목적지로 전달
- 메일 본문 데이터의 서버 체류 시간이 감소하여 데이터 프라이버시 침해 위험 최소화

정책 준수 및 커스텀

- 법적 요구사항, 규정을 준수하기 위한 마스킹 정책을 유연하게 적용
- PII 엔티티, 여러 조건들을 조합하여 다양한 커스텀 정책을 생성, 수정 가능

PII 엔티티 관리

기본 제공 PII 엔티티 외에, 마스킹 대상이 되는 엔티티를 정책 관리자가 사내 시스템에서 사용되는 특정 패턴을 정규 표현식 기반으로 추가/삭제하여 마스킹 정확도를 높이고 사내 환경에 최적화 시킴

Basic: Role-based 권한 분리(RBAC)

4개의 역할로 나눠 책임과 권한 분리

		User	Auditor	Policy Admin	System Admin
이메일 작성 및 마스킹		O	O	O	O
프라이버시 보호 이력 열람		△(본인 활동만)	O	△(본인 활동만)	△(본인 활동만)
엔티티 관리	엔티티 조회	△(본인 활동만)	△(본인 활동만)	O	△(본인 활동만)
	엔티티 추가/수정	X	X	O	X
정책 관리	정책 조회	△(본인 활동만)	△(본인 활동만)	O	△(본인 활동만)
	정책 추가/수정	X	X	O	X
사용자 역할 설정		X	X	X	O

User: 마스킹 자동화 with AI

이메일 원본 작성 → 첨부파일의 경우 ClovaOCR 전처리

NER 기반 PII 탐지

REGEX 기반 PII 탐지 → priority 로직으로 정확도 개선

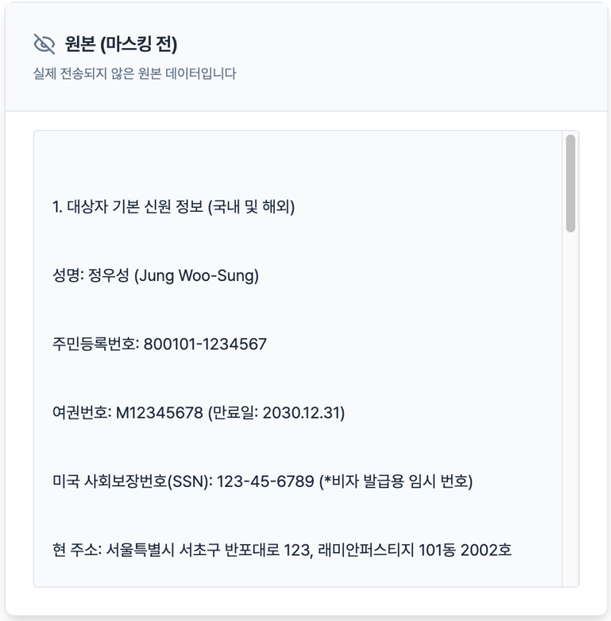
PII 취합 및 좌표 매핑

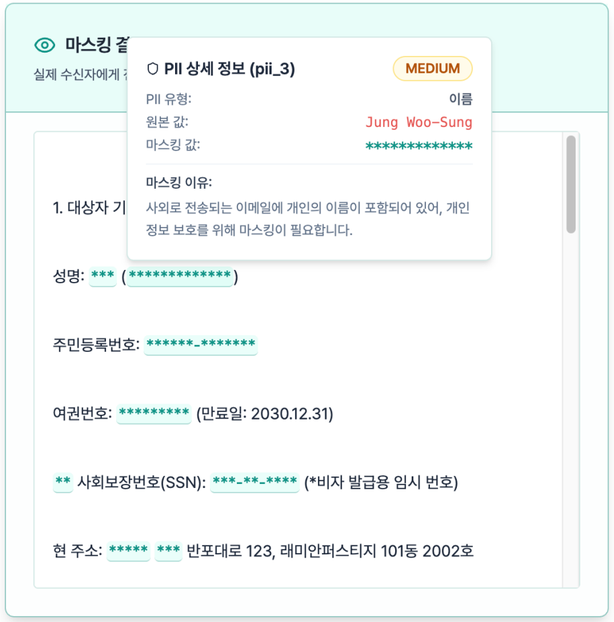
vector DB 정책 검색 (RAG) → 정책을 검색이 마스킹 판단의 근거

마스킹 판단 및 실행

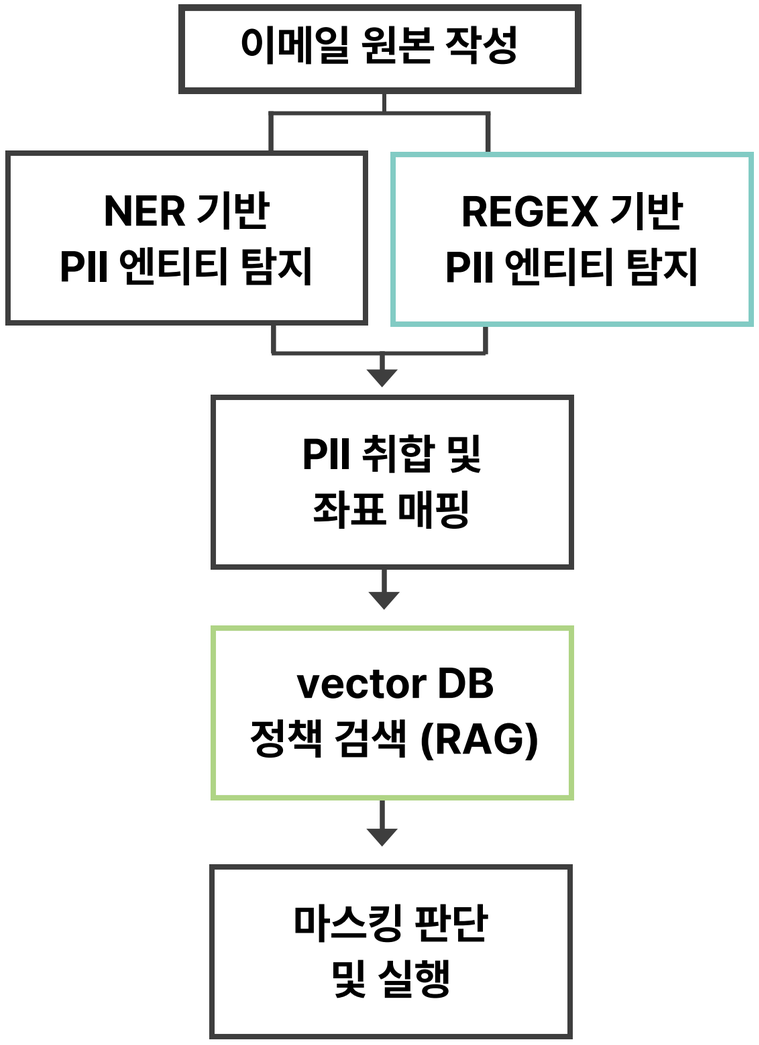
내장 엔티티 목록

이메일	GPS
IP 주소	계좌번호
카드번호	운전면허번호
여권번호	핸드폰/지역 전화번호
MAC 주소	주민번호





Policy: 엔티티, 정책 관리



PII 엔티티 관리

엔티티 관리 페이지에서 REGEX
커스텀 PII 엔티티 추가하여 DB 기반
동적인식기 생성

커스텀 엔티티 추가 기능

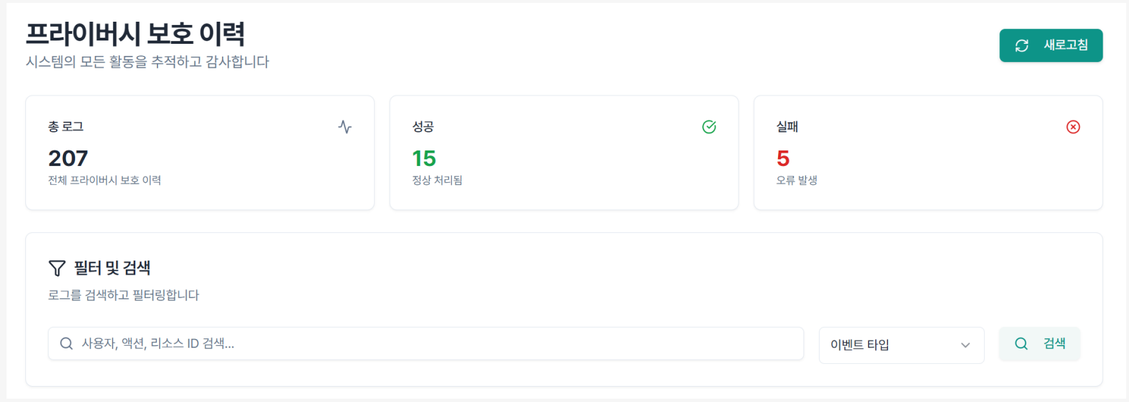
정책 관리

openai vision을 활용하여 내용 인식 후
vectorDB에 알맞은 포맷으로 가이드라인
자동 추출 / 정책 업로드 및 편집 가능

정책 내 추출된 가이드라인

Auditor: 프라이버시 보호 이력

프라이버시 보호 이력 페이지를 통해 개인정보 보호 관련한 모든 로그가 투명하게 기록



프라이버시 보호 이력 헤더 부분

로그 내역

이메일 전송과 마스킹 결정에 관한 로그

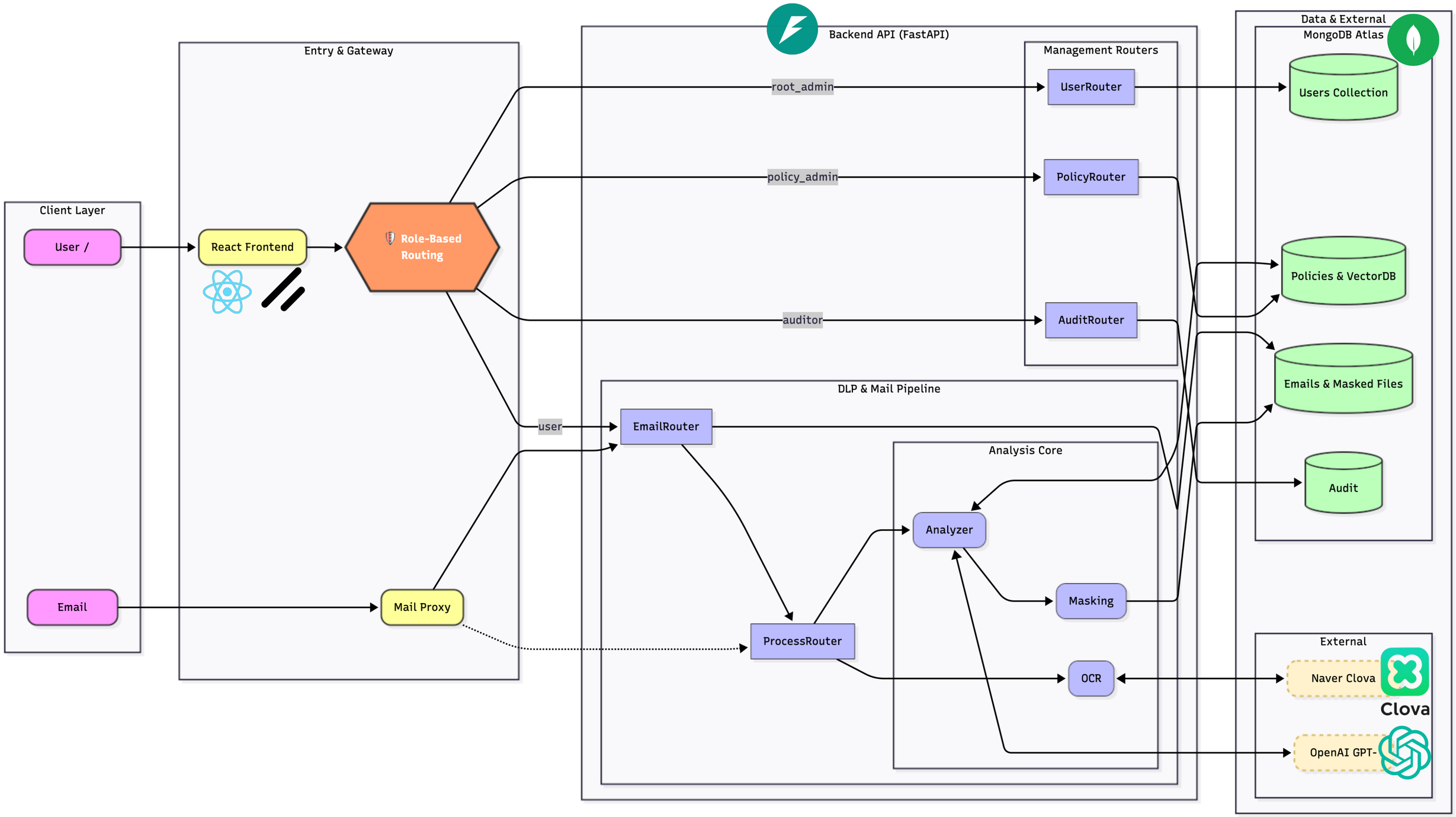
- 메일 송수신 여부와 송신 메일의 마스킹 결정에 대한 기록
- 메일 전송 성공/실패 로그, 전송 성공 메일 마스킹 결정 로그 기록

PII 엔티티 관리 로그

- 정책 관리자가 정규 표현식 엔티티를 변경한 내역 기록
- 생성, 삭제 로그 기록

정책 관리 로그

- 정책 관리자가 마스킹 정책을 변경한 내역 기록
- 생성, 수정, 삭제 로그 기록


Client Layer
User /
Email
Entry & Gateway
React Frontend
Role-Based Routing
Mail Proxy
Backend API (FastAPI)
root_admin
policy_admin
auditor
user
Management Routers
UserRouter
PolicyRouter
AuditRouter
DLP & Mail Pipeline
EmailRouter
ProcessRouter
Analysis Core
Analyzer
Masking
OCR
Data & External
MongoDB Atlas
Users Collection
Policies & VectorDB
Emails & Masked Files
Audit
External
Naver Clova
Clova
OpenAI GPT-