

# 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



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

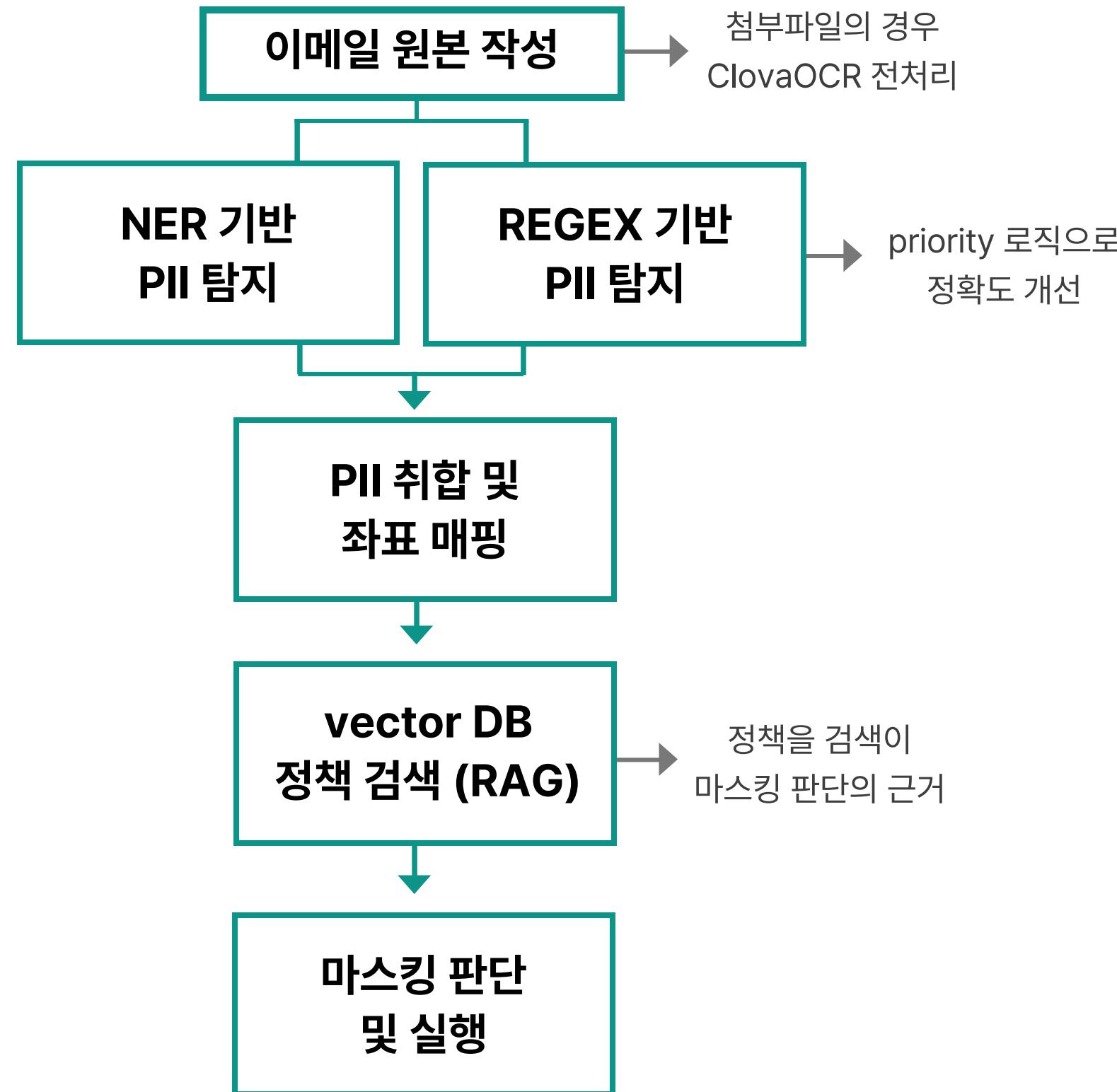
## PII 엔티티 관리

# 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	△(본인 활동만)	△(본인 활동만)	O	△(본인 활동만)
	X	X	O	X
정책 관리	△(본인 활동만)	△(본인 활동만)	O	△(본인 활동만)
	X	X	O	X
사용자 역할 설정	X	X	X	O

# User: 마스킹 자동화 with AI



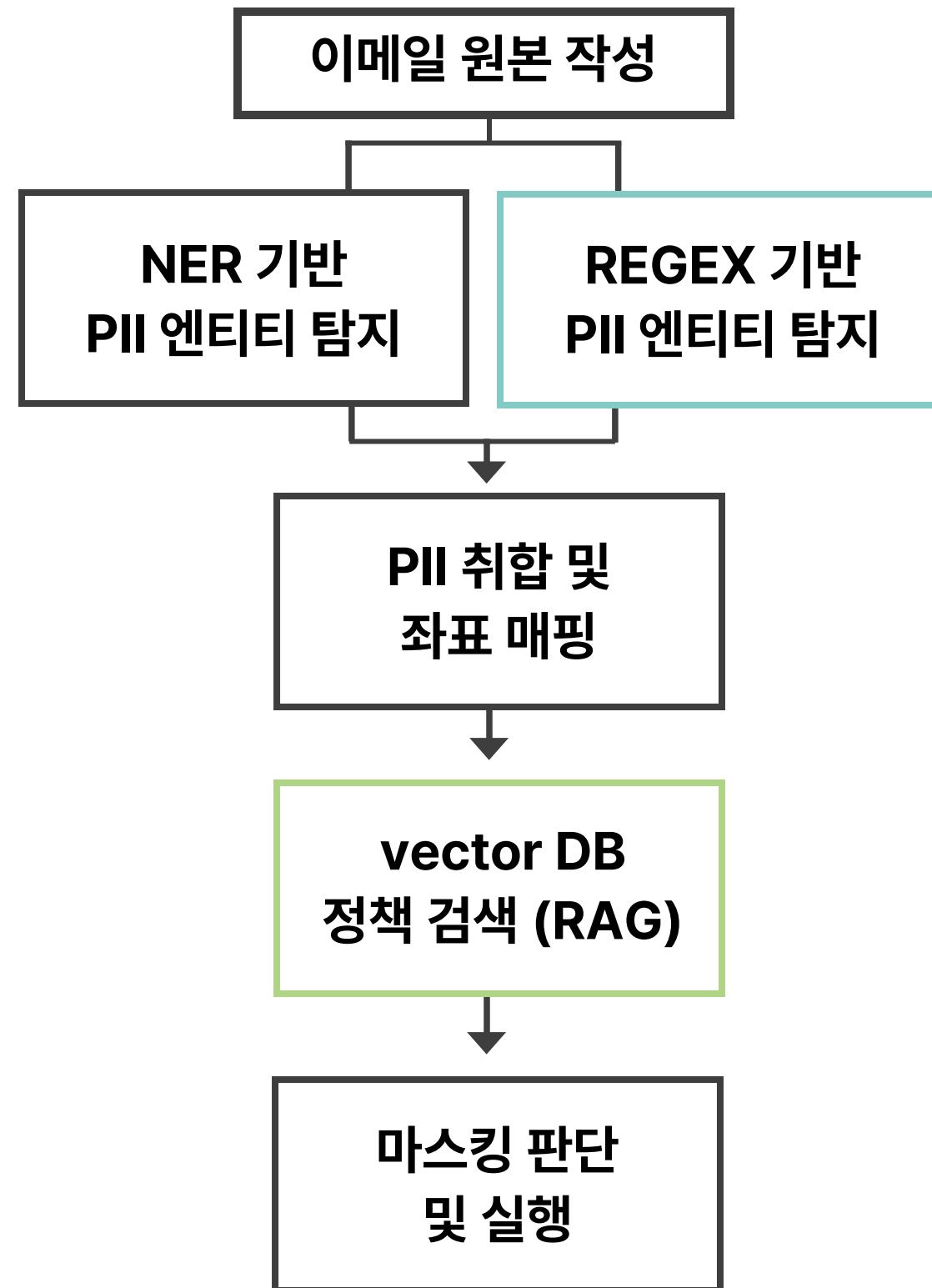
내장 엔티티 목록	
이메일	GPS
IP 주소	계좌번호
카드번호	운전면허번호
여권번호	핸드폰/지역 전화번호
MAC 주소	주민번호

원본 (마스킹 전)  
실제 전송되지 않은 원본 데이터입니다

1. 대상자 기본 신원 정보 (국내 및 해외)  
성명: 정우성 (Jung Woo-Sung)  
주민등록번호: 800101-1234567  
여권번호: M12345678 (만료일: 2030.12.31)  
미국 사회보장번호(SSN): 123-45-6789 (\*비자 발급용 임시 번호)  
현 주소: 서울특별시 서초구 반포대로 123, 래미안퍼스티지 101동 2002호

마스킹 결  
실제 수신자에게 보여줄 정보입니다  
○ PII 상세 정보 (pii\_3)  
PII 유형: MEDIUM  
원본 값: Jung Woo-Sung  
마스킹 값: \*\*\*\*\*  
마스킹 이유:  
사외로 전송되는 이메일에 개인의 이름이 포함되어 있어, 개인정보 보호를 위해 마스킹이 필요합니다.  
성명: \*\*\* (\*\*\*\*\*)  
주민등록번호: \*\*\*\*\*-\*\*\*\*\*  
여권번호: \*\*\*\*\* (만료일: 2030.12.31)  
\*\* 사회보장번호(SSN): \*\*\*-\*\*\*-\*\*\* (\*비자 발급용 임시 번호)  
현 주소: \*\*\*\*\* \*\*\* 반포대로 123, 래미안퍼스티지 101동 2002호

# Policy: 엔티티, 정책 관리



## PII 엔티티 관리

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

**새 엔티티 추가**  
커스텀 엔티티를 생성하여 민감 정보를 감지할 수 있습니다

엔티티 ID \*  
예: business\_id

엔티티 이름 \*  
예: 사업자등록번호

카테고리 \*  
예: 사업자정보

설명  
엔티티 설명

Regex 패턴 \*  
예: \d{3}-\d{2}-\d{5}

커스텀 엔티티 추가 가능

## 정책 관리

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

**추출된 가이드라인 (8개)**  
AI가 정책 문서에서 추출한 실무 가이드라인

> #1 신뢰도 80%  
주민등록번호 처리 시  
  
지침: 주민등록번호는 앞 6자만 유지하고 뒤 7자는 '\*'로 마스킹한다.

> #2 신뢰도 80%  
휴대전화 번호 처리 시  
  
지침: 휴대전화 번호는 가운데 4자리를 '\*\*\*\*'로 마스킹한다.

정책 내 추출된 가이드라인

# Auditor: 프라이버시 보호 이력

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

**프라이버시 보호 이력**  
시스템의 모든 활동을 추적하고 감사합니다

총 로그 **207** (전체 프라이버시 보호 이력)

성공 **15** (정상 처리됨)

실패 **5** (오류 발생)

**필터 및 검색**  
로그를 검색하고 필터링합니다

사용자, 액션, 리소스 ID 검색... | 이벤트 타입 | 검색

**프라이버시 보호 이력 헤더 부분**

날짜	액션	이메일	내용	상태	상세보기
11월 30일 오후 08:55	이메일 전송	yes0823bs@swu.ac.kr user	이메일 전송: test 6	성공	상세보기
11월 30일 오후 08:52	엔티티 생성	policyadmin@naver.com policy_admin	엔티티 create: 건강보험증 번호	성공	상세보기
11월 30일 오전 03:28	정책 수정	policyadmin@naver.com policy_admin	정책 텍스트 수정: 긴급 상황 시 개인정보 처리 및 보...	성공	상세보기
11월 30일 오전 03:28	엔티티 삭제	policyadmin@naver.com policy_admin	엔티티 delete: time	성공	상세보기

**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

