멀티테넌시와 RLS: 고객 데이터 경계를 설계하는 법

여러 조직이 하나의 서비스를 사용하면서도 데이터와 권한이 섞이지 않도록 테넌트 경계, 서버 권한, RLS를 함께 설계하는 원칙을 다룹니다.

어떤 상황에서 활용하나요?

고객사 공간을 처음 준비하거나 로그인·멤버 접근 문제를 확인하는 운영 담당자에게 필요한 안내입니다. 계정 설정과 테넌트 소유권을 구분해 점검하고, 다른 고객 자료에 접근하는 방식으로 문제를 해결하지 않습니다.

SAG(새그)는 더크림유니언이 운영하는 GEO·AEO·SEO 분석 및 최적화 플랫폼입니다. 검색엔진과 생성형 AI가 브랜드와 웹사이트 콘텐츠를 어떻게 발견하고 이해하는지 분석하고, 경쟁사 비교·개선 우선순위·실행 결과·재검증을 관리합니다. 플랫폼 구독과 전문 운영 지원을 제공하며, 콘텐츠 제작·사이트 코드 수정 등 대행 실행 범위는 별도 계약에서 정합니다.

멀티테넌시는 화면 구분이 아니라 데이터 계약입니다

구독형 서비스에서는 여러 고객 조직이 같은 애플리케이션과 데이터베이스를 사용합니다. 이때 조직 이름을 화면에 표시하는 것만으로는 격리가 완성되지 않습니다. 모든 조회와 변경이 어느 테넌트의 요청인지 확인하고, 권한이 없는 행은 데이터베이스 단계에서도 접근할 수 없게 해야 합니다.

SAG는 조직을 나타내는 테넌트와 사용자의 역할을 분리해 다룹니다. 사용자가 로그인하면 서버가 세션과 멤버십을 확인하고, 요청한 리소스가 해당 테넌트에 속하는지 검증합니다. 브라우저가 보낸 조직 식별자를 그대로 신뢰하지 않습니다.

콘텐츠·기술 개선 작업을 관리하는 SAG 운영 예시

> 이 화면은 방법 설명을 위한 SAG 공개 예시이며, 특정 고객사의 성과나 색인·검색·AI 추천을 보장하지 않습니다.

서버 권한과 RLS를 함께 두는 이유

서버 권한 검사는 업무 규칙을 이해하기 쉽고 명시적으로 표현합니다. RLS(Row Level Security)는 쿼리에 실수가 생겨도 다른 조직의 행이 노출되지 않도록 데이터베이스에서 한 번 더 경계를 세웁니다. 두 층을 함께 사용하면 한쪽의 누락이 바로 고객 데이터 노출로 이어질 가능성을 낮출 수 있습니다.

핵심 원칙은 다음과 같습니다.

- 테넌트가 필요한 테이블에는 명확한 테넌트 식별자를 둡니다.
- 읽기와 쓰기 모두 같은 소유권 검증을 적용합니다.
- 플랫폼 관리자와 고객 운영자 권한을 분리합니다.
- 감사 로그에는 누가 어떤 리소스를 바꾸었는지 남깁니다.
- API 키와 비밀번호 같은 비밀 값은 일반 운영 레코드에 저장하지 않습니다.

공유 데이터와 고객 전용 데이터를 구분하기

경쟁사 도메인처럼 여러 고객이 관측할 수 있는 대상도 있고, 고객 질문·개선안·승인 기록처럼 조직별로 보호해야 하는 데이터도 있습니다. 전자를 무조건 복제하면 운영 비용이 커지고, 후자를 섣불리 공유하면 보안 문제가 됩니다. SAG는 데이터의 소유권과 공개 범위를 먼저 정의한 뒤 저장 구조를 결정합니다.

검증해야 할 실패 시나리오

정상 조회만 통과해서는 충분하지 않습니다. 다른 테넌트의 ID를 넣었을 때 404 또는 권한 오류가 나는지, 역할이 낮은 사용자가 변경 API를 호출할 수 없는지, 오래된 버전으로 덮어쓰려 할 때 충돌을 감지하는지까지 확인해야 합니다. 데이터 경계는 문서에 적힌 약속이 아니라 반복 가능한 테스트로 증명되는 운영 조건입니다.

RLS가 적용되는 실행 역할까지 확인하기

RLS 정책이 있어도 테이블 소유자나 BYPASSRLS 역할은 정책을 우회할 수 있습니다. SAG의 서버 멤버십·테넌트 조건 검사는 이와 별개로 유지합니다. 데이터베이스 접속 역할과 정책 적용을 함께 확인해야 격리 범위를 판단할 수 있습니다.

주제별 기술 참고

- PostgreSQL 행 보안 정책

이 기술을 이어서 읽는 방법

테넌트 권한, 작업 재시도, 캐시와 승인 이력을 살펴봅니다.

- 안정적인 고객 공간 설계
- 기능 안내 FAQ