Lawmadi OS 공개 기술백서

Public Release v1.0 · Sanitized

법률 의사결정 운영체제 (Legal Decision Operating System, LDOS)

> “불안을 실행 가능한 논리로 전환하다 (Convert Anxiety into Actionable Logic)”

발행일: 2026-02-07 | 저작권자: 최재남

문서 상태: 공개용(보안 등급 조정) — 보안·영업비밀·운영 안전을 위해 일부 내용은 개념 수준으로 추상화되어 있습니다.

목차

1. 개요 (Executive Summary)

Lawmadi OS는 단순한 법률 검색이나 챗봇이 아니라, 공식 근거 기반으로 사건을 구조화하고 검증 가능한 판단 흐름을 생성하는 의사결정 인프라(Decision Infrastructure)입니다.

핵심 철학은 “빠른 답변”보다 “검증 가능한 답변”입니다. 따라서 Lawmadi OS는 입력을 구조화하고, 근거를 확인하고, 검증이 실패하면 결론 생성을 중단하는 Fail-Closed 운영 원칙을 중심에 둡니다.

본 백서는 공개 가능한 범위에서 아키텍처, 런타임 처리 흐름, 보안/신뢰성 원칙, 데이터 정책 및 로드맵을 요약합니다.

2. 핵심 가치 (Core Value Proposition)

Lawmadi OS는 ‘결론을 생성하는 AI’가 아니라 ‘근거에 의해 통제되는 의사결정 지원 시스템’을 지향합니다.

2.1 신뢰 가능한 근거 중심 설계

Lawmadi OS는 권위 있는 공개 법령·판례 API를 근거의 출발점(SSOT)으로 사용합니다.

중요: Lawmadi는 해당 API의 이용조건·정책을 준수하며, 본 문서는 특정 기관과의 제휴/보증 관계를 의미하지 않습니다.

2.2 제로 추론(Zero Inference)

법률 ‘사실’을 임의로 생성하거나 보정하지 않습니다.

모든 법률적 진술은 추적 가능한 근거(Traceable Evidence)를 전제로 합니다.

2.3 Fail-Closed (검증 실패 시 중단)

근거 검증이 실패하면 시스템은 애매한 결론을 내리지 않고 판단 출력을 중단합니다.

이는 법적 리스크 및 오해 가능성을 줄이기 위한 안전 장치입니다.

2.4 실시간 근거(Live Evidence) 우선

법령/판례는 시시각각 변합니다. Lawmadi OS는 저장된 데이터보다 조회 시점의 근거 검증을 우선합니다.

3. 운영 헌법 (Foundational Operating Constitution)

Lawmadi OS는 정책(헌법)에 의해 동작이 통제됩니다. 정책은 내부적으로 규칙 집합으로 관리되며, 공개 문서에는 예시만 제공합니다.

Illustrative Example (Conceptual DSL)

```
RULE Enforce_Source_Integrity
IF evidence.source != OFFICIAL_API
THEN reject_decision
```

위 예시는 개념 설명을 위한 것이며, 실제 규칙 집합/우선순위/예외 처리/스코어 함수는 영업비밀 및 보안상 비공개입니다.

4. 플랫폼 아키텍처 (Layered Platform Architecture)

Lawmadi는 보안과 역할 분리를 위해 3계층 구조를 지향합니다.

4.1 Core Layer (Closed Kernel)

사건 구조화, 근거 검증, 의사결정 흐름 생성 등 핵심 엔진이 위치합니다.

지적재산(IP) 및 운영 헌법이 집행되는 영역입니다.

4.2 Service Layer (User Experience)

사용자 인터페이스(안내형 UX, 질의 흐름, 상담형 대화 UX)를 제공합니다.

Core Layer 내부 로직에 직접 접근하지 않도록 경계를 분리합니다.

4.3 Partner Layer (B2B / 기관 연계)

검증 API, 구조 분석 API 등 기관/기업용 인터페이스 제공이 가능합니다.

접근 제어, 로깅, 레이트리밋 등 통제 하에 운영됩니다.

5. 런타임 처리 흐름 (Deterministic Runtime Flow)

Lawmadi OS는 처리 단계를 명시적으로 정의하여 '블랙박스'를 줄이고 재현성을 높입니다.

High-Level Flow (Sanitized): 입력 검증 → 사건 구조화 → 근거 조회/검증 → 결정 구조 생성 → 결정 토큰 발행 → 응답

5.1 Fail-Closed 동작

근거 검증이 실패하면 시스템은 안전 정지(Stop)하여 결론을 생성하지 않습니다.

사용자는 중단 사유를 이해할 수 있도록 명확한 코드/사유를 받도록 설계됩니다.

6. 주요 엔진 개요 (Key Engine Overview)

6.1 사건 구조 파서 (Case Structuring)

비정형 문장을 사실/관계/쟁점 구조로 변환하여 시스템 처리가 가능하게 합니다.

목표: 사실관계의 구조화 → 검증 가능한 요청 생성

6.2 라우팅/스웜 협업 (Swarm Routing)

사건 유형과 쟁점 특성에 따라 적절한 모듈(리더/전문 프로필)로 경로를 결정합니다.

라우팅은 도메인 적합성, 내부 신뢰 점수, 근거 의존성 등 개념적 요소를 활용할 수 있습니다.

구체 스코어링 수식/가중치는 영업비밀로 비공개입니다.

6.3 시간적 유효성 (Temporal Validity)

법은 시간에 따라 효력이 달라집니다. Lawmadi는 시행/폐지 여부 등 유효성 체크를 고려합니다.

정책상 불확실하면 Fail-Closed 또는 Reference-Only로 처리할 수 있습니다.

7. 보안 및 신뢰성 (Security & Trust, Sanitized)

본 절은 설계 목표 및 경계(Boundary) 원칙을 설명합니다.

7.1 입력/출력 경계 (Gateway Protection)

입력 스키마 검증, 인증/인가(IAM 등) 연동, 로깅 및 모니터링(민감정보 마스킹), 레이트리밋 및 악성 요청 방어를 포함합니다.

7.2 무결성(Integrity) 설계 목표

근거 데이터의 무결성을 확인하기 위한 해시(예: SHA-256) 구조를 활용할 수 있습니다.

의사결정 결과는 '결정 토큰(Decision Token)' 형태로 추적 가능하게 구성될 수 있습니다.

7.3 서명(Signature) 경계 설계

핵심 원칙: 서명은 커널 내부에 키를 두지 않고, 외부 신뢰 시스템(KMS/HSM 등)으로 분리합니다.

공개 문서/샘플 구현에는 서명 값은 placeholder로 제공됩니다.

8. 데이터 정책 (Data Governance)

8.1 근거 데이터(법령/판례) 취급 원칙

공식 공개 API 기반 SSOT를 지향합니다.

데이터 최신성/정합성/정책 준수를 위해 자체 DB 복제 모델을 지양합니다.

8.2 성능을 위한 임시 캐시(가능)

성능 최적화를 위해 단기 TTL 캐시(예: 10~30분)는 허용될 수 있습니다.

단, 캐시는 '성능 목적'이며 근거의 출처/진실성을 대체하지 않습니다.

8.3 감사 로그(Audit) 및 개인정보

감사 목적 로그는 최소한으로 수집하며, 민감정보는 마스킹/분리 저장을 지향합니다.

본 문서는 개인정보 처리의 법적 고지를 대체하지 않으며, 실제 서비스 공개 시 별도 고지가 필요합니다.

9. 비공개 자산 (Non-Public Assets)

공개 백서에는 다음을 포함하지 않습니다.

1) 라우팅 스코어링 함수의 상세(가중치·룰 우선순위·예외처리)

2) 운영용 설정(config), 엔드포인트, 키/토큰, 호출 패턴

3) 배포 인프라(IaC/CI/CD), 보안 정책 상세, 관측(로그) 정책 상세

4) 외부 공급자(LLM 등) 라우팅 로직 상세

5) 실제 운영 데이터/사용자 데이터 및 내부 평가 데이터

10. 로드맵 (Roadmap, Public View)

Lawmadi는 단계적으로 확장됩니다. 본 로드맵은 공개 범위 내 요약이며 상세 일정과 구현 범위는 변경될 수 있습니다.

Phase 1

의사결정 커널 MVP 정립(구조화·흐름·토큰·Fail-Closed)

Phase 2

근거 검증 엔진 및 시간적 유효성 강화

Phase 3

사용자 경험(UX) 고도화 및 기관용 인터페이스(Partner API) 설계/적용

Phase 4

교육·시각화·워크플로우 기반 플랫폼 확장

11. 용어 (Glossary)

LDOS: Legal Decision Operating System (법률 의사결정 운영체제)

SSOT: Single Source of Truth (단일 진실 공급원)

Fail-Closed: 검증 실패 시 결론 생성을 중단하는 안전 정책

Decision Token: 입력·근거·흐름을 추적 가능하게 묶는 결과 식별 토큰(개념)

Temporal Validity: 시행/폐지/효력 등 시간에 따른 유효성 고려

12. 저작권 및 면책 (Copyright & Disclaimer)

본 문서는 정보 제공 목적의 공개 기술 개요입니다. 실제 구현 세부(알고리즘/정책/보안 설정)는 영업비밀 및 보안상 비공개입니다.

본 문서는 법률자문이 아니며, 변호사-의뢰인 관계를 형성하지 않습니다. 중요한 의사결정 전에는 전문가 상담을 권장합니다.