10th Anniversary

GISC 2026

Global ICT Standards Conference 2026

AI 에이전트를 위한 DB 가드레일,
DB Governance MCP

특허경영으로 도출한 클라비의 기술 방향

주식회사 클라비 | 이용준 전무

ICT Standards and Intellectual Property:
Shaping the Physical AI

주최 과학기술정보통신부 지식재산처 주관 국립전파연구원 TTA IITP KEA kista ETRI

Index

01 특허경영 전략과 해결 과제

02 핵심 특허와 기술 구현

03 사업화와 표준 연계

Abstract

AI 에이전트의 DB 접근을 실행 전에 심사하는 가드레일

DB Governance MCP

문제	AI 에이전트가 DB에 직접 접속하면 고비용 질의, 민감정보 노출, 감사 공백이 생길 수 있습니다.
해법	에이전트와 DB 사이에서 MCP를 경유하는 요청을 실행 전에 심사합니다. 요청마다 정책·위험·비용을 판단해 허용·보류·거부를 결정합니다.
특징	비용이 높은 질의는 차단에 그치지 않고 재작성 등 대안과 함께 제시하며, 판단 이력은 변조 방지 감사 로그로 남깁니다.
구조	실행 비용 평가·최적화 특허와 실행 정책·감사 특허를 하나의 MCP 처리 파이프라인으로 통합하는 구조로 개발 중입니다.
목표	에이전트 요청이 늘어도 숙련된 DBA가 상시 지키는 DB처럼 안정적인 운영 수준을 유지하는 것을 목표로 합니다.

클라비 특허경영: 발굴부터 활용까지 표준 절차로 운영

2022년 설립 | DX, AX 전문 기업으로 성장

발명 발굴 → 발명제안서 → 기술·권리범위 검토 → 명세서 작성 → 특허법인 검토·출원 → 심사·사후관리

기술 계층별 포트폴리오

- 데이터 수집·정제
- 에이전트 실행·제어 ★
- 검색증강생성·온톨로지
- 모델 학습·평가
- 접근통제·감사기록 ★

기반기술 / 산업응용 구분 관리

기반기술

생성형 AI · SaaS · 데이터 거버넌스 · 자연어 DB 질의 최적화 · 검색증강생성 · 모델 파인튜닝

산업응용

농업 · 업무관리 · 법령정보 · 디지털 트윈 · 멀티모달 위험분석

활용 · 확장

등록특허 6건 통상실시권 제공 협약 (공동기술 개발 협력사)

해외출원 후보 선별 · 국제출원 검토

2026년 신규 발명 13건: 명세서 초안 완료 · 특허법인 검토 중 (연내 출원 목표)

2027년 30건 확보 추진

2026 ICT특허경영대상 부총리 겸 과학기술정보통신부장관 표창 수상

클라비의 기술 방향: 특허 기반 DB 가드레일 개발과 표준 연계

AX 시대의 과제: 데이터의 개방과 통제

데이터 개방과 통제의 트레이드오프를 해결하는 것이 특허 선정의 출발점

업무시스템	AI Agent	필요한 통제
정형화된 화면 / 고정 API / 승인된 업무 절차	업무 목적에 따른 동적 질의 상황별 데이터 조합	누가 · 무엇을 · 왜 · 어떻게 실행 전 심사와 감사

문법검사나 허용 목록을 통과한 SQL도 실행 위험이 존재합니다

검증 사각 지대

함수/ 뷰 등을 통한 간접 접근이나 분석만으로 확인하기 어려운 동작

데이터 노출 위험

업무 목적을 초과하는 조회, 민감 정보를 포함하는 컬럼 포함

비용 예측의 한계

실행계획/ 통계/ 파라미터에 따른 비용 추정 오차 존재

운영 부하 위험

장시간 실행/ 대량 스캔 및 반복 요청 등 동시 실행

데이터는 더 폭넓게 활용하되, 실행은 검증된 범위에서만 허용

공공·국방 AX 사업 확산, 내부 데이터 접근과 활용이 핵심 과제

2026년 정부 발표 기준 AX 추진 현황

7,540억
범부처 AX-Sprint 지원규모
2026.06 · 중기부

229개
선정 AI 제품·서비스
2026.06 · AX-Sprint

190억
국방 AX 협력센터 예산
2026.06 · 국방부

폐쇄망 · 국가 망 보안체계(N2SF)
보안등급과 기관별 망 정책에 맞춘 접근 설계가 전제

핵심 질문
업무망·폐쇄망 Agent가 기관 내부 데이터를 어떤 권한과 경로로 활용할 것인가?

출처: 중기부(2026.06.19) · 국방부(2026.06.18) · KISA(2026.06.17)

공공·국방 AX의 확산 = 내부 데이터 접근 통제 과제의 확대

특허경영 전략: 데이터 개방과 통제의 트레이드오프를 해결하는 특허

AI·AX 중심 포트폴리오에서, 가장 큰 과제를 해결하는 기술을 핵심 특허로 확보

AI·AX 중심 포트폴리오

- 생성형 AI
- SaaS
- 데이터 거버넌스

출원 10건 · 등록 2건
영역을 병행해 확보 (공적서 기준)

→

핵심 특허 선정 이유

AX 전환의 현 시점에서 데이터의 개방과 통제라는 트레이드오프를 해결하기 위한 솔루션

→

특허① 등록
SQL 실행 전 비용 평가·
질의 최적화

특허② 등록
Agent 실행정책과
감사 가능한 통제

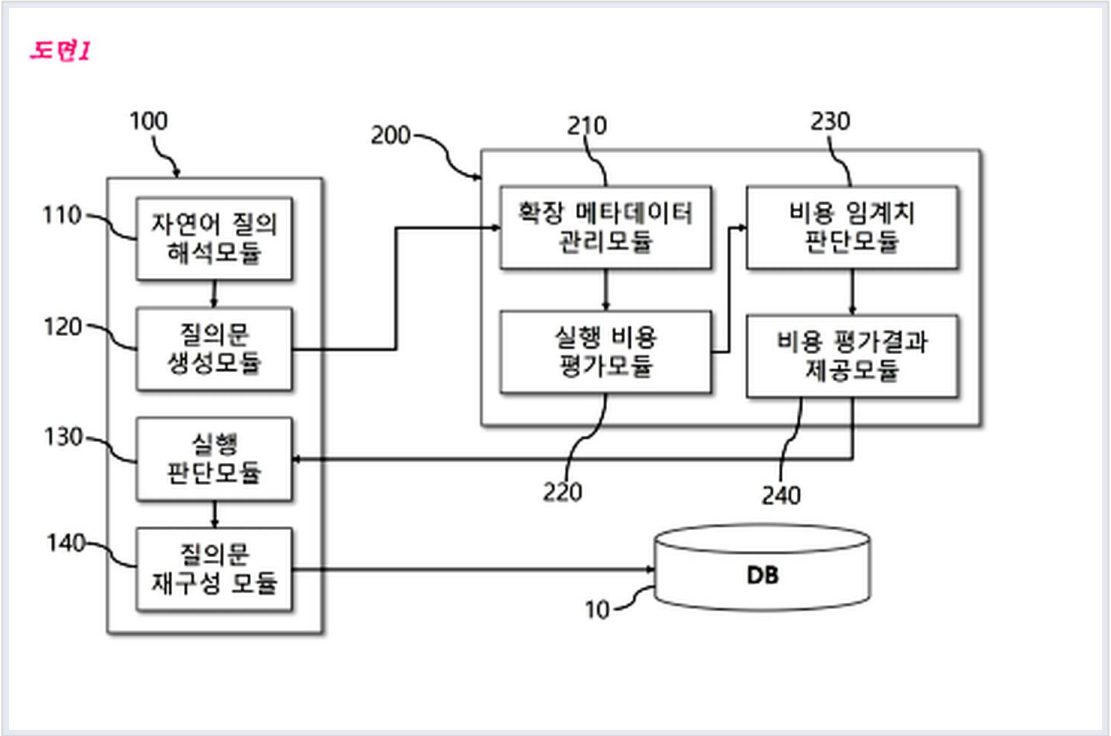
제품화 DB Governance MCP

AX 시대의 핵심 과제를 해결하는 기술을 특허로 확보하고, 제품으로 구현

특허① (등록) SQL 실행 전 비용 평가·질의 최적화

등록특허 10-3022056 · 처리 흐름과 등록공보 도면

1	자연어 질의 해석	110
2	질의문(SQL) 생성	120
3	확장 메타데이터 확인	210
4	실행 비용 평가	220
5	비용 임계치 판단 · 결과 제공	230·240
6	실행 판단 · 질의문 재구성 → DB 실행	130·140



등록특허 10-3022056 도 1 (등록공보)

실행 전에 비용을 예측하고, 임계치를 넘으면 더 효율적인 질의로 재구성

특허② (등록) Agent 실행정책과 감사 가능한 통제

인증 → 위험/ 정책 심사 → 실행 결정 → 감사

AI가 데이터베이스를 실행하기 전, 거버넌스와 감사 가능한 통제

모든 요청은 정책과 위험 검증을 거쳐, 승인된 경우에만 AI가 데이터베이스를 실행합니다.

1 인터페이스
- 웹 포털
- 업무시스템
- API
- AI 챗봇

2 요청 수신/검증
- 요청 수신
- 형식 검증
- 악성 요청 탐지
- 필수 정보 확인

3 정규화/구조화
- 자연어 → 실행 요청 변환
- SQL/파라미터 정규화
- 구조화된 작업 단위로 변환

4 주체 인증
- 사용자/시스템 인증
- 권한 및 역할 확인
- 세션/토큰 검증
- 접근 가능한 데이터 범위 확인

5 위험·비용 예측
- 데이터 영향도 분석
- 실행 비용 예측
- 성능 및 리소스 영향
- 위험도 점수 산출

6 정책 평가
- 보안 정책 검토
- 데이터 접근 정책
- 컴플라이언스 규칙
- 위험도 기반 규칙 평가

7 실행 결정 오케스트레이션
- 평가 결과 종합
- 실행/보류/승인 경로 결정
- 승인 절차 오케스트레이션
- AI 실행을 위한 안전한 명령 생성

8 보류/승인 연계

자동 승인
정책을 충족하고 위험이 낮은 요청

수동 승인
민감 데이터, 고위험 요청 (담당자 검토)

보류
추가 정보 필요 또는 정책 위반 가능성

승인 시 AI 실행

보류 시 담당자 검토

승인자 (업무/보안/데이터)

AI 기반 DB 실행

데이터베이스 안전 실행
- 승인된 명령만 실행
- 권한 내에서 실행
- 실행 결과 반환

9 이후 처리 및 감사(Audit)

10 스키마 정의
- 접근 가능한 DB 스키마 관리
- 테이블/컬럼 메타데이터
- 데이터 분류 및 민감도 정의

11 로그 저장
- 요청 내용, 변환된 명령
- 평가 결과, 승인 이력
- 실행 결과, 소요 자원
- 모든 이벤트를 감사 로그로 저장

12 무결성 보호
- 로그 위변조 방지
- 전자서명/해시 체인
- 보관 기간 관리
- 감사 추적 가능성 확보

13 조회·리포팅
- 요청 이력 조회
- 실행 결과 및 위험도 리포트
- 정책 준수 현황 대시보드
- 감사 대응 리포트 (규제/내부감사)

정책·위험 기반 실행 통제와 판단·실행 이력의 감사 추적

DB Governance MCP: 특허를 API와 공존하는 통제 경로로 구현

업무 변경은 승인 API, 탐색형 조회는 정책 기반 DB 접근 — 직접 DB 계정은 Agent에 제공하지 않음



Agent는 DB 자격증명을 직접 보유하지 않으며, 기존 API·접근통제를 대체하지 않고 공존

상용화를 위한 기술 개발·내부 검증 단계

공공 및 국방 등 폐쇄망 환경의 AX 전환에 활용하기 위한 기술 개발

완료

핵심 특허 확보
특허① 등록 · 특허② 등록결정

제품 요구사항 정의
SRS v1.0 (2026. 03)
SRS v1.3 (2026. 10) 업데이트

진행 중 · 내부 검증

프로토타입 구현
PostgreSQL 환경 DB MCP

내부 검증
MCP 프로토콜 경유 Agent 질의의 비용 통제·수행 기본 동작 확인

예정

정량 측정
심사 시간 · 추정-실측 오차 · 차단 오탐/미탐

추가 시험
우회 차단 · DBMS 확장 적합성 · 공공·폐쇄망 PoC

정량 측정과 외부 PoC 를 통한 실증

향후 계획: 공공기관·폐쇄망 AX 솔루션 공급

기존 접근제어·API·보안 운영과 공존하는 방식으로 시장 진입

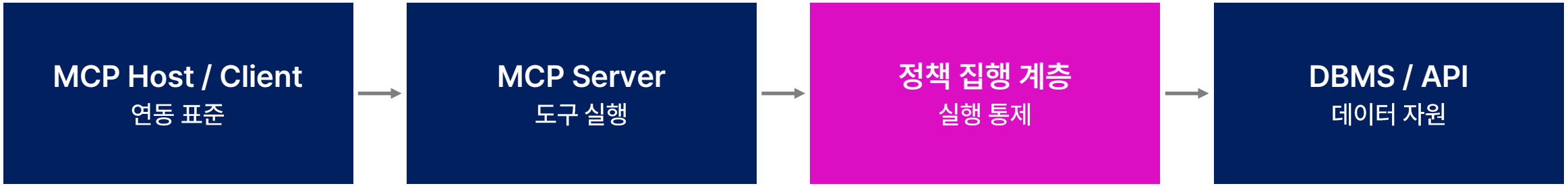
상용화 준비	공공 · 폐쇄망 AX	해외 진출 준비
DB MCP 상용화를 위한 UX 설계 전문 DBA 사용성 검토 GS 인증 준비	내부 업무 데이터 기반 Agent 접근 검증 (PoC)	PCT(국제출원) 검토 중

DBMS 확장 순서

PostgreSQL 우선 검증 → **MySQL** 우선 검증 → **Oracle** 확장 검증 → **DB MCP 지원 확대**

표준 연계: 개방 프로토콜(MCP) 기반 실행 통제 계층 구현

MCP 공식 구조와 NIST 2026 Agent 표준화 이니셔티브를 바탕으로 Clabi 관점에서 재구성



NIST 2026

Agent의 상호운용성 · 보안 · 신원/인증에 대한 표준화 논의가 시작되었습니다

열린 질문

Agent의 DB 실행 통제는 어느 계층에서 표준화되어야 하는가?

개방 프로토콜(MCP) 위에서 동작하는 실행 통제 계층

10th Anniversary

GISC 2026

Global ICT Standards Conference 2026

데이터를 안전하게 열어야
AI가 제대로 활용합니다.

특허로 보호하고 · 제품으로 구현하고 · 공공·폐쇄망 AX로 확장하겠습니다.

주식회사 클라비 | 문의 [yjlee@clabi.ai]

ICT Standards and Intellectual Property:
Shaping the Physical AI

주최 과학기술정보통신부 지식재산처 주관 국립전파연구원 TTA IITP KEA Kista ETRI