공식 제출용 - 자진 제출 선제 의견서

선행기술 진보성 자진조사보고서

Prior Art & Inventive-Step Self-Investigation Report

- 우선심사신청 설명서 첨부자료 -

(특허·실용신안 심사기준 제3부 제3장 진보성 판단 기준에 따른 자진 조사 및 의견)

항목	내용
발명의 명칭	목적 결속형 실행 객체 비생성 제어 기반의 접근·세션·실행·반출 및 도구 호출 통제 시스템 및 그 방법
출원인	김철 (KIM CHUL)
특허고객번호	620250807042
문서 종류	선행기술 진보성 자진조사보고서 (자진 제출 의견서 겸용)
작성 기준일	2026년 6월 12일
우선일(기준 절단일)	2026년 6월 12일 (KST) - 이 날짜 이전 공개 = 잠재적 선행기술
조사 범위	KIPRIS(한국), USPTO/EPO/WIPO 공개 DB, arXiv·IETF·IEEE·ACM (국문/영문)
보안 분류	공식 제출용 - KIPO/MOIP 온라인 제출

면책 고지

본 보고서는 출원인이 자진으로 수행한 선행기술 조사의 결과를 정리한 것으로, 법적 구속력 있는 특허성 의견서가 아닙니다. 모든 결론은 등록된 특허 대리인의 최종 검토를 거쳐야 하며, 특히 KIPRIS 정밀 검색 및 FTO(Freedom-to-Operate) 분석은 별도 의뢰가 요구됩니다.

핵심 명제 (본 보고서의 중심축)

본 보고서에 인용된 발명들은 정책 판단, 토큰 활성 여부 확인, 사후 폐기, 감사로그 기록 또는 접근제어를 개별적으로 제공할 뿐, 고위험 행위 요청에 대하여 목적·범위·증거·정책 버전·감사 사전기록을 발급 전제 조건으로 결합하고, 조건 미충족 시 issued_objects 실행 가능 네임스페이스에 후단 실행 가능한 객체 참조값 자체가 생성되지 않는 non_birth 저장구조 상태를 형성하며, 그 감사 식별자도 검증 입력으로 사용되지 않도록 하는 원자적 발급 제어 평면을 개시하거나 시사하지 않는다.

목 차

제0장 조사 방법론·범위·한계 및 기준일

0.1 조사 목적

본 장은 본 보고서가 제시하는 결론의 검증가능성과 한계를 먼저 투명하게 밝힌다. 이는 공식 제출 문서로서 본 보고서가 갖추어야 할 신뢰성의 전제이다.

(1) 본 발명의 청구범위 핵심 구성에 대응하거나 이를 시사할 수 있는 선행기술을 식별하고, (2) 심사관이 진보성 부정을 위해 시도할 개연성이 높은 복수 문헌 결합 시나리오를 미리 도출하여, (3) 각 시나리오에 대한 "결합 동기 부재" 및 "예측 불가능한 효과" 논거를 사전 정리함으로써, 거절이유 통지 시 신속·정확한 대응을 가능하게 함에 있다.

0.2 조사 도구 및 데이터베이스

본 보고서의 선행기술 자료는 다음 공개 출처를 직접 조회·교차 확인하여 수집하였다.

- USPTO 공개 특허·공보 원문(image-ppubs.uspto.gov) 및 Google Patents 서지정보
- 상용 특허정보 색인(RPX Insight, Justia Patents) - 권리자·출원/등록일·법적 상태 교차 확인
- IETF RFC 원문(OAuth 2.0 계열 표준, draft-goswami-agentic-jwt, draft-prakash-aip)
- Model Context Protocol(MCP) 공식 사양 블로그 및 표준 개정 이력
- arXiv cs.CR / cs.AI 공개 학술 프리프린트 (AI 에이전트 인가·격리 분야 2025-2026 군집)
- 권리자 공식 사이트 - 권리 귀속 및 특허 표시 페이지 확인

0.3 검색 전략 및 검색어

핵심 개념을 9개 군으로 분해하고, 각 군별 키워드와 권리자명·특허번호를 조합하여 한국어·영어 병용 검색하였다.

검색 DB	주요 검색어/IPC	비고
KIPRIS	에이전트 인가, 토큰 발급 게이트, 비출생 불변식 IPC: G06F21/33, G06F21/41, G06F21/62	변리사 정밀 검색 필수 - 본 자진조사에 미포함
USPTO/EPO/WIPO	Agentic authorization, capability token, fail-closed issuance, non-existence invariant	공개 DB 검색 수행
arXiv (cs.CR/cs.AI)	Agentic JWT, ASTRA TBAC, IBCT, ILION, PEA model, Trinity gate, non-birth invariant	2025-01 ~ 2026-06 집중
IETF Datatracker	draft-goswami-agentic-jwt, draft-prakash-aip, UCAN, Biscuit token	RFC·인터넷 초안 포함
IEEE/ACM DL	Agent delegation, capability-based authorization, task-scoped token	2022~2026

0.4 조사 기준일 및 시간적 범위

조사 기준일: 2026년 6월 12일. 본 보고서는 다음 원칙을 적용한다.

- 선행기술성(공지) 판단의 핵심은 출원의 우선일(최선 출원일)이다. 우선일 이후에 비로소 공개된 자료는 특허법 제29조의 선행기술이 될 수 없다.
- 본 보고서는 우선일 전에 공개된 것이 명백한 자료(등록·공개 특허, 확정 표준, 우선일 전 발행 논문)를 "선행기술"로 다루고, 우선일 전후가 불분명하거나 우선일 이후로 보이는 자료는 "동시기·후행 기술 동향"으로 명확히 구분하여 기재한다.
- 특히 AI 에이전트·MCP 분야는 2025~2026년에 공개가 가속되는 영역이므로, 해당 자료를 선행기술로 단정하지 않고 시간적 지위를 보수적으로 표기한다.

0.5 조사 범위의 한계 및 표현 원칙

> **주의**
>
> 미공개 출원, 비공개 영업비밀, 색인 누락 문헌, 비영어·비한국어권 일부 문헌, 회색문헌(grey literature) 등은 검색에 포착되지 않을 수 있다. KIPRIS 전수 결과는 본 자동화 검색 범위에서 직접 확정 검증되지 않았다. 따라서 본 보고서는 "전 세계 부존재"를 단언하지 않으며, 결론은 항상 "본 보고서에 기재된 조사 범위 내에서 확인되지 아니함"의 형식으로 한정 진술한다.

표현 원칙: 본 보고서가 "확인되지 아니하였다", "도출되지 아니한다"고 진술하는 경우, 이는 항상 본 보고서의 조사 방법·범위·기준일을 전제로 한 한정적 진술이다. 이러한 한정 표현은 진보성 주장의 설득력을 약화시키지 아니하며, 오히려 심사 실무상 신뢰성과 방어가능성을 높인다.

0.6 인용문헌 검증 상태 표기 원칙

등급	의미
◎ 검증	1차 출처에서 번호·명칭·권리자·법적상태를 직접 확인
○ 확인	개념·표준이 널리 확립된 공지기술로서 1차/권위 출처 확인
△ 미확정	내부 문서 기재 번호가 단일 문헌으로 확정 검증되지 않음 - 대표 문헌으로 대체·대리인 재검증 권고

제1장 본 발명의 기술적 본질

본 발명의 핵심은 정책 평가 결과를 표시(allow/deny)하거나 이미 발급된 토큰을 사후 폐기하는 데 있지 아니하다. 고위험 행위 요청에 대하여 후단에서 실행 가능한 객체 참조값이 발급 저장구조의 실행 가능 네임스페이스에 애초에 생성되지 않도록 하는 비생성 결정상태(non_birth)를, 저장구조와 트랜잭션 경계에서 보장하는 발급 제어 평면(Issuance Control Plane)을 형성하는 것에 있다.

1.1 발급 제어 평면의 3계층 불변 구조

계층	구성	기술적 역할
계층 1 발급 전제 결합	목적 객체(purpose object) + 범위 해시(scope_hash) + 활성 정책 버전 + 감사 사전기록	4개 조건이 하나의 발급 트랜잭션 경계 내에서 동시 충족되지 않으면 발급 연산 자체가 개시되지 않음(fail-closed)
계층 2 3상태 발급 상태기계	born(정상 발급) / shadow-executable(제한 발급) / non_birth(저장구조 행 미생성)	결정 결과가 저장구조의 행 생성 여부와 원자적으로 결합되는 3상태 상태기계
계층 3 후단 강제 소비	verify(객체 검증부) + row-lock consume transaction(소비 트랜잭션)	double-spend·replay 차단; 비생성 감사 ID는 검증 입력으로 사용 시 실행 불가(non_executable) 반환

1.2 비생성 불변식 - non_birth의 7개 동시 조건 (청구항 2 기반)

본 발명에서 결정상태가 non_birth인 경우, 다음 7개 조건이 동시에 성립한다. 이 불변식을 충족하지 못하는 구현은 non_birth를 구현한 것으로 볼 수 없으며, 이는 침해 판단의 리트머스이자 진보성 논증의 중심축이다.

1. 실행 가능한 issued_objects 행(row)이 생성되지 않음 (no executable issued_objects row)
2. 객체 식별자(object_jti)가 부여되지 않음
3. 서명된 권능(signed capability)이 발급되지 않음
4. 검증 참조값(verification_ref)이 존재하지 않음
5. 세션/반출/파일 생성 핸들·BI 추출 참조·도구 호출 식별자(tool invocation id)가 생성되지 않음
6. verify(non_birth audit_id)는 {unknown, inactive, non_executable} 중 하나만 반환
7. 후단 백엔드 실행이 호출되지 않음 (backend execution is NOT invoked)

> **핵심 명제**
>
> "존재하지만 전달되지 않음(deny/revoke)"과 "존재 자체가 없음(non_birth)"은 공격 표면에서 본질적으로 다르다. 후자는 revocation 시간차, 복제 토큰, 캐시/로그/BI 커넥터 경로를 통한 우회 자체가 성립할 객체가 없음을 구조적으로 보장한다.

1.3 청구항 구조 및 도면 대응 개관

청구항군	대상	대표 도면
독립항 1/11/31~40	시스템/방법/저장매체 - 범용 발급 제어 평면	도 1, 도 2, 도 3, 도 7
독립항 20~25	AI 에이전트 실행 게이트웨이 (tool call 정규화·실행 객체화)	도 5, 도 8
독립항 26~30	데이터 반출 게이트웨이 (범위 유효성·정책 평가)	도 6
소비 트랜잭션	reserve→lock→commit→finalize 4단 원자 소비	도 4

제2장 조사된 선행기술 일람

본 장은 본 보고서에서 검토한 선행기술을 서지·핵심개시·검증상태와 함께 일람한다. 권리자·법적상태는 1차/색인 출처에서 확인하였다.

2.1 기존 선행기술 문헌 (보안·인가·감사 영역)

약칭	문헌/표준 (명칭 요지)	권리자/시기	핵심 개시	검
US7519826	Near real-time multiparty task authorization access control	Engedi Technologies 우선2003/등록·만료 2026-12-07	정책 엔진·authorizer 승인 후 authorization agent가 접근 허용	◎
RFC 7662	OAuth 2.0 Token Introspection (토큰 인트로스펙션)	IETF 2015	기발급 토큰의 active 상태·권한 메타데이터를 검증하는 표준	◎
US9338008	Secure release of secret information over a network (trustee 비밀 릴리스)	Cloudera(관련 US9819491) 우선 2012/등록	trustee 정책 적용 결과에 따라 secret을 release 또는 deny	◎
US9047490	Secure execution of workflow tasks in distributed workflow	SAP SE 우선2007/등록	policy/vertex key+onion 구조로 워크플로 실행 완료를 암호 검증	◎
PBAC	US2021/0279355A1 Purpose-based access control(NGAC)	공개 2021	목적(purpose)을 정책/속성으로 모델링·부분 허용 시 가상객체 생성	◎
IDEMP	Idempotence for database transactions (DB 트랜잭션 멱등성)	Oracle(예: US8984170) 우선 2011~2012	논리 트랜잭션 ID로 커밋 1회성 보장, 원자적 all-or-nothing 커밋	◎
ROWLOCK	행 잠금 동시성 제어 (SELECT FOR UPDATE/CAS)	관계형 DB 일반 공지기술	행 단위 잠금으로 동시 갱신 직렬화 - double-spend 방지의 표준 기법	○
PAMAUD	PAM 세션 감사 - 특권 세션 기록·사후 감사	업계 일반/표준 구현	특권 접근 세션을 기록·감사하여 무결성 사후 입증	○
DLP	데이터 손실/반출 방지 - 전송 중 민감데이터 탐지·차단	다수(예: US11405423) 2010s~	문서/전송의 민감데이터를 지문·정책으로 탐지하여 업로드·복사·공유를 차단	◎
AIRIA	Proxy-based secure MCP server access for AI agents (나노샌드박스)	Airia LLC 등록 US12562968 2024	AI 에이전트를 단명 격리 컨테이너에서 실행, 입출력에 보안규칙 적용·차단	◎
MCPAUTH	MCP 인가 사양 (OAuth 2.1, RFC 8707, 감사·동의 경로)	Model Context Protocol 2025~	MCP 서버를 OAuth 리소스 서버로 분류, 토큰 오용 방지·도구 호출 동의·감사 경로	◎

2.2 AI 에이전트 인가 선행기술 군집 (moat - 2025-2026 신규 확인)

아래 문헌은 2025-2026년 공개된 AI 에이전트 인가 분야의 최신 선행기술 군집으로, 우선일(2026-06-12) 기준으로 잠재적 선행기술에 해당하는 문헌이다. 이 군집이 AAL 진보성 스토리의 핵심 약점으로 식별되었으며, FTO 검색의 명시 대상이다.

> **주의**
>
> PEA(arXiv:2605.02682, 2026-05)는 AAL과 개념적으로 가장 인접한 최근접 선행기술이다. 청구범위 작성 시 가장 면밀한 대비가 필요하다.

약칭	문헌명 / 출처	저자·소속 / 공개일	핵심 개시	검
A-JWT	Agentic JWT: A Secure Delegation Protocol for Autonomous AI Agents arXiv:2509.13597	Goswami et al. 2025-09-16	이중 측면 의도 토큰 결속, 에이전트 신원 체크섬, 체인 위임 메커니즘; IETF 초안 진행 중	◎
ASTRA	Delegated Authorization for Agents Constrained to Semantic Task-to-Scope arXiv:2510.26702	El Helou et al. (Cisco Systems) 2025-10-30	작업 기반 접근제어(TBAC): 인가 서버가 에이전트 작업 요청을 의미론적으로 검사, 최소 범위 토큰 발급; AgentAuthBench	◎
AIP/IBCT	AIP: Agent Identity Protocol arXiv:2603.24775	Prakash et al. (ISB) 2026-03-31	호출 결합 역량 토큰(IBCT): 신원·권한·범위·출처를 단일 암호화 체인에 결합, append-only 출처 추적; MCP·A2A 바인딩	◎
ILION	ILION: Deterministic Execution Gate for Agentic AI (arXiv)	Chitan 2026 Q1 추정	결정론적 사전 실행 게이트: 기하학적 검증을 통한 다중 안전 계층 의미론적 호환성 검증	△
PEA	Hybrid Inspection and Task-Based Access Control in Zero-Trust Agentic AI arXiv:2605.02682	미상 2026-05 최근접	정책-실행-인가 3계층 분리, 보안 커널 접근법, 단일 사용 서명 역량 토큰(모든 게이트 통과 후 발급)	◎
Trinity	Trinity: Deterministic Command Gate for Zero-Trust Agent Execution	미상 2025~2026 추정	결정론적 명령 게이트: 구문 분석+정책 평가, 정책 위반 도구 호출 차단	△
DM-DCT	Intelligent AI Delegation: Capability Tokens (DeepMind)	Tomasev et al. (DeepMind) 2025~2026 추정	감쇄 우선(attenuation-first) 위임, macaroons 기반 역량 토큰	△
South	Authenticated Delegation and Authorized AI Agents arXiv:2501.09674	South et al. (MIT/ Stanford) 2025-01	AI 에이전트 인증 위임 프레임워크, 권한 범위 바인딩	◎
HIT-ZTAI	Hybrid Inspection and Task-Based Access Control in Zero-Trust Agentic AI arXiv:2605.02682	미상 2026-05	제로트러스트 에이전틱 AI용 혼합 검사+작업 기반 접근제어	◎
UCAN	UCAN Spec v1.0 - User Controlled Authorization Networks	ucan-wg/Fission 2023	체인 위임 역량 토큰, 오프라인 감쇄, JWT 호환	◎
Biscuit	Biscuit: Cryptographic Tokens with Datalog Policies	Delafargue et al. 2023	Datalog 정책 내장 역량 토큰, 감쇄 체인	◎
Macaroons	Macaroons: Cookies with Contextual Caveats (Google) NDSS 2014	Birgisson et al. (Google) 2014	컨텍스트 단서 기반 감쇄 가능 베어러 토큰, offline 검증, HMAC 체인	◎

제3장 단독 문헌 대비 분석 (신규성·구성 차이)

본 장은 각 선행문헌을 단독으로 본 발명과 대비하여, 본 발명의 핵심 구성요소가 해당 문헌에 의해 개시되지 아니함을 구성 차원에서 확인한다.

3.1 US7519826 (다자 실시간 승인 후 접근 허용)

선행문헌의 개시	본 발명의 대응 구성 - 차이
authorizer의 실시간 승인 이후 authorization agent가 자원 접근을 허용/집행. 승인 결과는 접근 허용을 위한 논리적 결정으로 처리됨.	승인은 born 상태로의 전환 "신호"일 뿐이며, 별도로 목적 객체+범위 해시+활성 정책 버전+감사 사전기록이 하나의 발급 트랜잭션 경계에서 성공해야 비로소 실행 가능 행이 생성된다. 승인 결과와 issued_objects 실행 가능 네임스페이스 행 생성 여부의 원자적 결합, 그리고 non_birth(행 미생성) 결정상태는 개시되지 아니한다.

3.2 RFC 7662 (토큰 인트로스펙션)

선행문헌의 개시	본 발명의 대응 구성 - 차이
이미 발급되어 존재하는 토큰의 active 상태·권한 메타데이터를 인가서버에 질의하여 검증.	본 발명은 검증 대상 토큰 자체가 존재하지 않는 상태(non_birth)를 형성한다. "토큰 검증의 강화"와 "토큰 미생성의 보장"은 기술적으로 동치가 아니며, RFC 7662는 미생성 결정상태를 개시하지 아니한다.

3.3 US9338008 (trustee 비밀 릴리스)

선행문헌의 개시	본 발명의 대응 구성 - 차이
server에 보관된 암호화 비밀자료(secret/credential/key)에 대해 trustee 정책으로 release/deny를 결정. deny 시 비밀이 client에 전달되지 않으나, 비밀은 server 내부에 이미 존재.	통제 대상이 "비밀 데이터의 전달 여부"가 아니라 "실행을 가능하게 하는 참조값(execution permit, session handle, tool invocation id)이 발급 저장구조에 생성되는지 여부"이다. "존재하지만 전달 안 됨"이 아니라 "존재 자체가 없음(no row/no handle)"으로, 통제 대상·저장구조·공격 표면이 모두 상이하다.

3.4 US9047490 (분산 워크플로 proof-of-execution)

선행문헌의 개시	본 발명의 대응 구성 - 차이
분산 워크플로의 각 단계가 정확히 완료되었음을 암호학적으로 검증(완료 무결성).	관심사가 "이미 진행 중인 워크플로의 무결성"이 아니라 "객체 발급 트랜잭션을 개시할 것인지 여부"이다. proof-of-execution은 객체 발생 이후의 검증이고, 본 발명은 객체 발생 자체를 저장구조 트랜잭션 경계에서 선행 결정한다.

3.5 PBAC 계열 (목적 기반 접근제어)

선행문헌의 개시	본 발명의 대응 구성 - 차이
목적(purpose)을 정책/속성 요소로 모델링하여 접근요청 허용 여부를 판단. 부분 허용 시 가상객체로 세분화 접근 제공.	목적을 자유 서술 사유 문자열이 아니라 object_type+action+resource_ref+normalized_scope+risk_class+approval_ref+retention_rule+evidence_validity로 기계 결합된 검증 가능 구조체로 정의하고, 이를 발급 네임스페이스 행 생성/미생성 결정과 원자적으로 결합한다. PBAC는 "허용 여부 판단"에 집중하며, 발급 네임스페이스와 소비 트랜잭션의 원자적 결합 및 non_birth_events/issued_objects 네임스페이스 분리를 가르치지 아니한다.

3.6 멱등성/행잠금 계열 (Oracle 등·DB 공지기술)

선행문헌의 개시	본 발명의 대응 구성 - 차이
논리 트랜잭션 ID로 커밋 1회성 보장(멱등성), 행 잠금(SELECT FOR UPDATE)으로 동시 갱신 직렬화.	본 발명은 멱등키 예약과 행 잠금 소비를 채용하되, 이를 목적 결속·범위 해시·감사 사전기록·비생성 결정과 결합한다. 멱등성·행잠금 자체는 범용 신뢰성 기법으로서 "고위험 실행 객체의 비생성 결정상태"라는 과제·효과를 시사하지 아니한다.

3.7 PAM 세션 감사 계열

선행문헌의 개시	본 발명의 대응 구성 - 차이
특권 접근 세션을 기록·감사하여 사후 무결성 입증.	본 발명의 감사는 사후 기록이 아니라 발급의 전제조건이다. 감사 사전기록이 실패하면 발급 자체가 차단(fail-closed)된다. 감사 가용성을 실행 객체 창설의 필수 선행조건으로 구조적으로 결합한 점은 사후 감사 로그와 근본적으로 다르다.

3.8 DLP / 데이터 반출 탐지 계열

선행문헌의 개시	본 발명의 대응 구성 - 차이
전송 중(data-in-motion) 또는 단말에서 민감 데이터를 탐지·차단(detect-then-block).	본 발명은 파일 생성 핸들·반출 참조값 자체를 발급 단계에서 non_birth로 봉쇄한다. "파일이 생성된 후 전송을 탐지"하는 것이 아니라 "파일/반출 핸들이 생기기 전에 차단"하는 시점·구조의 차이가 명확하다.

3.9 Airia AI 에이전트 MCP 게이트웨이 특허군 (US12562968 등)

선행문헌의 개시	본 발명의 대응 구성 - 차이
AI 에이전트의 MCP 서버를 단명 격리 컨테이너(nano sandbox)에서 실행하고, 게이트웨이가 입력(명령)·출력에 보안규칙을 적용하여 비준수 시 차단하며, 도구/서버 정의 변경 시 자동 차단.	제어 계층이 인프라/프로세스 격리+I/O 가드레일인 반면, 본 발명은 애플리케이션·DB 트랜잭션 레벨에서 tool invocation id 등 실행 참조값 자체의 비생성(non_birth)을 보장한다. 나노 샌드박스는 컨테이너 탈출을 막더라도 실행 참조값이 DB에 생성된 이후라면 캐시·로그·BI 경로 우회가 가능한 반면, 본 발명은 그 참조값이 저장구조에 부존재함을 보장한다. 두 발명은 충돌하지 않고 병렬·보완 관계이며, 본 발명의 "참조값 부존재 보장"은 독립적·추가적 진보성을 형성한다.

제3-A장 AI 에이전트 인가 선행기술 군집 심층 분석 (moat)

본 장은 2025-01~2026-06 공개된 AI 에이전트 인가 선행기술 군집을 심층 분석한다. 이 군집은 AAL 진보성 스토리의 핵심 약점으로 식별되었으며, FTO 검색의 명시 대상이다.

3-A.1 Agentic JWT (A-JWT) - arXiv:2509.13597

저자: Goswami et al. | 공개일: 2025-09-16 | ◎

핵심 개시: A-JWT는 에이전트 동작을 사용자 의도에 암호화적으로 결속하는 이중 측면 의도 토큰(dual-faceted intent token)을 제안한다. 에이전트 신원 체크섬(agent identity checksum)과 체인 위임 메커니즘을 통해 위임 연쇄 전반에 걸친 의도 무결성을 보장한다. IETF 초안(draft-goswami-agentic-jwt)으로도 표준화가 진행 중이다.

핵심 차이: "의도(purpose) 토큰 결속"은 AAL I-3(목적 결속)과 개념이 겹친다. 핵심 차이: A-JWT는 토큰을 먼저 발급한 후 의도를 결속(post-issuance binding)하는 방식인 반면, AAL은 purpose 파라미터를 발급 결정과 원자적으로 결합함으로써 토큰 자체가 issued_objects 네임스페이스에 존재하지 않는 상태(non-existence)를 사전조건으로 강제한다. A-JWT에는 비출생 저장 불변식(I-1)·감사 선행 조건(I-2)·네임스페이스 분리(I-5)·소비 바인딩(I-7)에 해당하는 메커니즘이 없다.

3-A.2 ASTRA / TBAC (Cisco) - arXiv:2510.26702

저자: El Helou et al. (Cisco Systems) | 공개일: 2025-10-30 | ◎

핵심 개시: Task-Based Access Control(TBAC)은 인가 서버가 에이전트의 자연어 작업 요청을 의미론적으로 분석하여 최소 필요 권한 범위(minimal scope)의 토큰을 발급하는 방식이다.

핵심 차이: ASTRA/TBAC는 토큰 자체를 발급하되 그 범위를 의미론적으로 최소화한다. 발급 여부를 결정하는 비출생 불변식(I-1), 감사 선행 조건(I-2), 네임스페이스 분리(I-5), 소비 바인딩(I-7)을 포함하지 않는다. TBAC가 "어떤 범위의 토큰을 발급할 것인가"를 다루는 데 비해, AAL은 "토큰(행)이 아예 생성되지 않는 것이 보안 경계"라는 근본적으로 다른 설계 원리를 채택한다.

3-A.3 AIP / IBCT (ISB) - arXiv:2603.24775

저자: Prakash et al. (Indian School of Business) | 공개일: 2026-03-31 | ◎

핵심 개시: 호출 결합 역량 토큰(Invocation-Bound Capability Token, IBCT)은 신원·권한 감쇄·범위 제약·출처 기록을 단일 암호화 체인에 결합한다. compact(JWT/Ed25519) 및 체인(Biscuit/Datalog) 두 가지 구현 방식을 제공하며, MCP 및 A2A 프로토콜 바인딩과 append-only 출처 추적을 지원한다.

핵심 차이: IBCT는 토큰을 생성하여 체인으로 결합하는 방식이다(존재 후 감쇄). AAL의 issued_objects 네임스페이스 비생성 불변식(I-1)과 감사 선행 조건(I-2)에 해당하는 메커니즘이 없다. IBCT의 "append-only 출처 레코드"는 사후 감사이지 발급 차단 선행조건이 아니다.

3-A.4 ILION - 결정론적 실행 게이트

저자: Chitan | 공개일: 2026 Q1 추정 (△ - 대리인 재검증 필수)

핵심 개시: ILION은 에이전틱 AI 시스템이 실행 전 여러 안전 계층에 걸쳐 의미론적 호환성을 기하학적 방식으로 검증하는 결정론적 사전 게이트를 제안한다는 간접 확인이 있다.

핵심 차이: ILION은 실행 허가/차단 게이트(execution-time gate)이며, 저장소 네임스페이스에 실행 가능 행을 생성하지 않는 비출생 불변식(I-1)이나 감사 선행 조건(I-2)을 구현하지 않는 것으로 파악된다. △ 등급이므로 FTO 검색 시 원문 확인 필수.

3-A.5 PEA 모델 - arXiv:2605.02682 (최근접 선행기술)

> **주의**
> PEA는 AAL과 개념적으로 가장 인접한 선행기술이다. 청구범위 해석 시 가장 면밀한 대비가 필요하다.

핵심 개시: Policy-Execution-Authorization(PEA) 3계층 분리 아키텍처. 인가 계층이 결정론적 다중 게이트 파이프라인을 실행하는 보안 커널로 동작하며, 단일 구성요소가 결정과 실행을 동시에 담당하지 못하게 한다. 모든 게이트 통과 후에만 단일 사용 서명 역량 토큰을 발급한다.

반증 논거: PEA도 최종적으로는 토큰(역량 자격증명)을 생성한다. AAL의 차별점은 (a) 사전조건 실패 시 issued_objects 행 자체의 비생성이 물리적·트랜잭션 수준 보안 경계라는 점, (b) 감사 레코드가 단순 사후 기록이 아니라 발급 트랜잭션을 차단하는 fail-closed 물리적 선행조건이라는 점, (c) 네임스페이스 분리(I-5)와 소비 바인딩(I-7)의 결합에 있다. "게이트 통과 후 발급" vs "게이트 실패 시 행 미생성" - 이 공격 면 차이가 진보성 핵심 논거이다.

3-A.6 기초 역량 토큰 선행기술 계보 분석

AAL의 역량 토큰 관련 불변식(I-3, I-4, I-7)에 대한 진보성 판단에는 아래 기초 문헌이 통상기술자 수준의 기준점이 된다.

문헌	핵심 개시	AAL 관련성
Macaroons (Google, 2014)	컨텍스트 단서 기반 감쇄 가능 베어러 토큰, offline 검증, HMAC 체인	토큰 감쇄 기초 개념 - I-7 소비 바인딩의 원거리 선행
UCAN v1.0 (2023)	체인 위임 역량 토큰, 오프라인 감쇄, JWT 호환, 도메인 위임	체인 위임 구조 - A-JWT·IBCT의 직접 선행, AAL I-3·I-4 비교 기준
Biscuit Token (2023)	Datalog 정책 내장 역량 토큰, 오프라인 정책 평가, 검증 가능 체인	Datalog 정책 체인 - AIP/IBCT Biscuit 모드의 직접 선행
RFC 7662 (2015)	토큰 인트로스펙션: 인가 서버에 토큰 상태 실시간 조회	토큰 존재 후 조회 패러다임 - AAL 비출생 패러다임과 대조

3-A.7 AI 에이전트 군집 7대 불변식 대비 매트릭스

아래 표는 AAL의 7대 핵심 불변식을 행으로, 주요 선행기술 문헌을 열로 배치한 매트릭스이다. 어느 단일 문헌도 AAL의 핵심 불변식 I-1·I-2·I-5 조합을 동시에 개시하지 않는다.

불변식	AAL 구현	A-JWT	ASTRA	AIP	PEA	ILION	South	UCAN	Biscuit	Mac.
I-1 비출생 저장 불변식	사전조건 실패 시 issued_objects 행 미생성	×	×	×	×	×	×	×	×	×
I-2 감사 선행 조건	감사 레코드 = fail-closed 발급 선행 조건	×	×	△	×	×	×	×	×	×
I-3 목적 결속	purpose 원자 결합	○	△	○	△	△	△	△	△	△
I-4 발급자 4중 속성	신원+권한+목적+유효기간	△	△	△	△	×	△	○	○	△
I-5 네임스페이스 분리	issued_objects↔non_birth_events 엄격 분리	×	×	×	×	×	×	×	×	×
I-6 비우회성	7계층 교차 검증, 단일 계층 우회 불가	×	△	△	○	○	×	×	×	×
I-7 소비 바인딩	verify→consume 원자 쌍, 단일 사용 강제	×	×	△	△	×	×	△	△	△
★ 전체 충족	7/7	1/7	1/7	2/7	2/7	2/7	1/7	2/7	2/7	1/7

매트릭스 결론

I-1(비출생 저장 불변식), I-2(감사 선행 조건), I-5(네임스페이스 분리)는 검토된 모든 선행기술에서 개시되지 않음. 이 세 불변식의 조합이 AAL의 핵심 신규·진보 요소임.

제4장 결합발명 진보성 방어 - 시나리오별 3축 논거

4.0 진보성 판단 법리 요약

- 결합의 동기(TSM): 통상의 기술자가 인용발명들을 결합할 만한 교시·시사·동기 또는 합리적 성공의 기대가 선행기술 자체에 존재해야 한다.
- 사후적 고찰 금지: 본원 발명을 청사진으로 삼아 인용발명을 사후적으로 재구성하는 판단은 허용되지 않는다.
- 구성요소의 대응: 결합하더라도 청구항의 각 구성요소가 모두 도출되어야 한다.
- 예측 불가능한 효과: 결합으로부터 예측되는 효과를 넘는 이질적·현저한 효과가 있으면 진보성이 뒷받침된다.

시나리오 A - 다자 승인 + 토큰 인트로스펙션 + 정책 기반 감사

가상 심사관 주장: US7519826(다자 실시간 승인) + RFC7662(기발급 토큰 활성 검증) + 정책 기반 감사/토큰 발급류 문헌을 결합하면 본 발명에 도달한다.

① 결합 동기의 부재 - US7519826과 RFC7662는 모두 "이미 생성·발급된 접근권 또는 토큰의 유효성을 사후 제어"하는 과제에 속한다. 양 문헌은 "발급 트랜잭션 경계 내에서 실행 가능 행을 생성하지 않는 결정상태"라는 과제를 인식하지 못하므로, 이를 향한 결합의 교시·시사·동기가 선행기술 어디에도 없다.

② 결합하여도 결여되는 청구 구성요소 - 세 문헌을 결합하여도 (가) non_birth 결정상태, (나) 목적·범위·정책 버전·감사 사전기록의 4중 동시 충족, (다) 감사 사전기록 실패 시 발급의 fail-closed 차단, (라) 비생성 감사 ID의 검증 입력 불가(non_executable)는 도출되지 아니한다.

③ 비생성 불변식의 예측 불가능한 효과 - 비생성 불변식(7조건 동시 성립)은 revocation 시간차 공격, 복제 토큰 공격, 캐시/로그/BI 경로 우회를 "통제 대상 객체의 부존재"로 원천 제거한다. 이는 "발급 후 검증을 강화"하는 결합으로부터 예측되는 효과와는 이질적인, 공격 표면의 구조적 소거라는 현저한 효과이다.

시나리오 B - 비밀 릴리스 + 분산 워크플로 실행 증명

가상 심사관 주장: US9338008(trustee secret release/deny) + US9047490(proof-of-execution)을 결합하면 "trustee deny ≈ non_birth"이고 "proof-of-execution = verify/consume"이므로 본 발명에 도달한다.

① 결합 동기의 부재 - US9338008의 통제 대상은 "비밀 데이터의 전달", US9047490의 관심은 "진행 중 워크플로의 완료 무결성"이다. 두 문헌 모두 "실행 가능 참조값의 발급 네임스페이스 내 생성 여부를 트랜잭션 경계에서 결정"한다는 과제를 공유하지 않으며, 양자를 결합할 기술적 동기가 제시되지 않는다.

② 결합하여도 결여되는 청구 구성요소 - 결합하여도 (가) "전달 차단"이 아닌 "발급 행 미생성"이라는 저장구조적 부존재, (나) 범위 해시의 결정론적 산출과 발급 객체·검증·소비 트랜잭션으로의 반복 결합, (다) born/shadow-executable/non_birth 3상태 발급 상태기계는 도출되지 아니한다.

③ 비생성 불변식의 예측 불가능한 효과 - "존재하지만 전달 안 됨(secret deny)"과 "존재 자체가 없음(non_birth)"의 차이는 공격 표면에서 본질적이다. 전자는 server 내부에 비밀이 존재하여 내부 유출·복제 위험이 잔존하나, 후자는 통제 대상 참조값이 저장구조에 부존재하여 그러한 위험 자체가 성립하지 않는다.

시나리오 C - PBAC + PAM 세션 감사 + 멱등성/행잠금

가상 심사관 주장: PBAC(목적 기반 접근제어) + PAM 세션 감사 + 멱등성/행잠금을 결합하면 "목적 기반 판단 + 감사 + 원자적 트랜잭션"으로 본 발명에 도달한다.

① 결합 동기의 부재 - PBAC는 "속성·목적 기반 허용 여부 판단"에, PAM 감사는 "특권 세션의 사후 기록"에, 멱등성/행잠금은 "트랜잭션의 신뢰성·1회성"에 각각 집중한다. 세 문헌은 서로 다른 과제 영역에 속하며, 이들을 결합하여 "발급 네임스페이스 행의 생성/미생성을 감사 전제조건과 원자적으로 결합"하도록 이끄는 교시·시사·동기가 어디에도 없다.

② 결합하여도 결여되는 청구 구성요소 - 결합하여도 (가) non_birth_events와 issued_objects의 네임스페이스 분리, (나) 감사 사전기록 실패 시 fail-closed 발급 불가, (다) 목적 객체의 기계 결합 구조체+범위 해시의 결정론적 산출과 후단 재검증 강제, (라) born/shadow-executable/non_birth 3상태 상태기계가 도출되지 아니한다.

③ 비생성 불변식의 예측 불가능한 효과 - 비생성 불변식은 "목적 판단을 통과하더라도 전제절차(감사 사전기록 등) 실패 시 객체가 미생성"되도록 하여, 판단 통과와 객체 존재를 분리한다. 이는 PBAC의 "판단=허용" 도식과 달리 "판단 통과 ≠ 객체 존재"라는 비직관적 결과를 낳으며, revocation 시간차·복제·캐시 우회 표면을 구조적으로 제거하는 예측 불가능한 효과를 제공한다.

시나리오 D - AI 에이전트 MCP 격리·게이트웨이 (Airia 특허군 등)

가상 심사관 주장: Airia US12562968(나노 샌드박스+게이트웨이 I/O 가드레일) + MCP 인가 사양(OAuth 2.1, 자원 지시자)을 결합하면 본 발명의 AI 에이전트 실행 게이트웨이(청구항 20~25)에 도달한다.

① 결합 동기의 부재 - Airia 특허군은 "실행 환경의 분리(프로세스/컨테이너 격리)"와 "I/O 가드레일"이라는 인프라 계층의 과제에, MCP 인가 사양은 "토큰 기반 인증·인가 및 동의·감사 경로"에 집중한다. 어느 것도 "DB 트랜잭션 레벨에서 tool invocation id 등 실행 참조값을 생성하지 않는 결정상태"라는 과제를 인식하지 않으므로, 그 방향으로의 결합 동기가 없다.

② 결합하여도 결여되는 청구 구성요소 - 결합하여도 (가) tool call을 실행 객체 발생 요청으로 정규화하여 arguments_hash+prompt_context_hash+tool_registry_version+destination_class를 범위 해시에 결합하는 구성, (나) 비생성 결정상태에서 tool invocation id 자체를 DB 트랜잭션 레벨에서 생성하지 않는 구성, (다) destination_class 불일치 시 즉시 non_birth로 차단하는 구성은 도출되지 아니한다.

③ 비생성 불변식의 예측 불가능한 효과 - 나노 샌드박스가 컨테이너 탈출을 차단하더라도, tool invocation id가 DB에 생성된 후라면 캐시·로그·BI 커넥터 경로를 통한 우회가 가능하다. 본 발명의 non_birth는 그 참조값이 저장구조에 부존재함을 보장하여 이러한 잔존 우회 경로 자체를 제거한다.

시나리오 E - AI 에이전트 인가 군집 전체 결합

가상 심사관 주장: "A-JWT(의도 결속) + ASTRA/TBAC(작업 범위 최소화) + AIP/IBCT(호출 결합 체인) + ILION/PEA(결정론적 게이트)를 결합하면 AAL의 기술적 효과를 달성할 수 있다."

① 결합 동기의 부재 - A-JWT, ASTRA, AIP/IBCT, PEA는 모두 토큰·역량·자격증명을 먼저 생성(birth)하고 이후 제약하는 "존재 후 제어(post-birth control)" 패러다임을 공유한다. 이들의 단순 결합은 "더 많은 속성을 가진 토큰"을 생성할 뿐이며, 실행 가능 행이 issued_objects 네임스페이스에 생성되지 않는 것 자체를 보안 경계로 삼는 비출생 패러다임(AAL I-1)으로 수렴하지 않는다.

② 결합하여도 결여되는 청구 구성요소 - 감사 레코드를 발급 트랜잭션의 fail-closed 물리적 선행조건으로 만드는 구조는 A-JWT, ASTRA, AIP/IBCT, ILION, PEA 어디에도 존재하지 않는다(I-2). issued_objects↔non_birth_events 네임스페이스의 엄격한 분리와 verify→consume 원자 쌍의 동시 적용도 군집 내 어느 단일 또는 결합 문헌에도 개시되지 않는다(I-5, I-7).

③ 비생성 불변식의 예측 불가능한 효과 - Biscuit/UCAN/Macaroons 계열의 역량 토큰 기초 기술과 PEA/ILION의 결정론적 게이트를 결합하더라도, 기초 역량 토큰 문헌들은 오프라인 감쇄(offline attenuation)와 최소 발급자 신뢰(minimal issuer trust)를 설계 목표로 삼으므로, issued_objects 행 미생성을 목표로 하는 방향으로 변형할 동기가 문헌 자체에 존재하지 않는다.

시나리오 F - PEA + South et al. 결합

가상 심사관 주장: "PEA의 게이트 파이프라인 + South의 인증 위임을 결합하면 AAL이 자명하다."

① 결합 동기의 부재 - 두 문헌 모두 토큰/자격증명의 발급을 전제로 하며, 비출생 불변식(I-1)·감사 선행 조건(I-2)·네임스페이스 분리(I-5) 개시가 없다.

② 결합하여도 결여되는 청구 구성요소 - 결합의 귀결은 "인증된 위임 + 다중 게이트 검증 후 발급"이지 "행 미생성"이 아니다.

③ 비생성 불변식의 예측 불가능한 효과 - 결합으로부터 예측 불가능한 효과: 두 문헌의 결합이 비출생 패러다임으로 수렴하지 않는다.

> **결합발명 방어의 공통 귀결**
> 본 보고서에 인용된 발명들은 정책 판단, 토큰 활성 여부 확인, 사후 폐기, 감사로그 기록 또는 접근제어를 개별적으로 제공할 뿐, 고위험 행위 요청에 대하여 목적·범위·증거·정책 버전·감사 사전기록을 발급 전제조건으로 결합하고, 조건 미충족 시 issued_objects 실행 가능 네임스페이스에 후단 실행 가능한 객체 참조값 자체가 생성되지 않는 non_birth 저장구조 상태를 형성하며, 그 감사 식별자도 검증 입력으로 사용되지 않도록 하는 원자적 발급 제어 평면을 개시하거나 시사하지 않는다.

제5장 최근 5년(2021-2026) 기술 동향과 본 발명의 위치

5.1 정책 외부화·ABAC/PBAC·정책 엔진

정책 결정점(PDP)과 정책 집행점(PEP)의 분리(NIST SP 800-162 계열), 정책 엔진에 의한 런타임 허용/거절 평가, 속성·목적 기반 접근제어(ABAC/PBAC)는 최근 폭넓게 확립되었다. 이들은 "요청에 대한 허용/거절"을 출력하는 데 집중하며, 결정 결과를 발급 저장구조 행의 생성/미생성과 원자적으로 결합하거나 감사 사전기록을 발급 전제조건으로 배치하는 구성에는 이르지 않는다.

5.2 AI 에이전트·MCP 인가 표준의 진화 (2025-2026)

MCP 인가 사양은 2025년 다수 개정을 거쳐 MCP 서버를 OAuth 리소스 서버로 분류하고, 자원 지시자(RFC 8707)로 토큰 오용을 제한하며, 도구 호출에 대한 동의·감사 경로를 정비하는 방향으로 발전하였다. 이는 "토큰의 발급·검증·동의·감사"라는 표준 보안 모델의 강화이며, "실행 참조값의 저장구조 미생성 결정상태"라는 본 발명의 제어 평면과는 계층과 목표가 다르다.

5.3 AI 에이전트 사전인가·격리 연구 및 특허 동향

2025~2026년 공개 학술·기술 자료에서 (가) 도구 호출 이전의 결정적(deterministic) 사전인가, fail-closed, 비우회성(non-bypassability)을 강조하는 접근, (나) 마이크로 VM·gVisor·컨테이너 등 에이전트 격리 패턴, (다) 나노 샌드박스형 MCP 게이트웨이 특허(권리자 Airia 특허군)가 확인된다. 이들은 "실행 전 인가 판단"과 "실행 환경 격리·가드레일"에 해당하며, 본 발명의 핵심인 "실행 참조값을 DB 트랜잭션 경계에서 생성하지 않는 비생성 결정상태 및 그 7개 불변식"을 직접 개시하지는 않는다. 다만 인접·동시기 활동이 활발한 영역이므로 본 발명의 구별점을 명세서·청구범위에서 반복 명시하는 것이 바람직하다.

5.4 시간적 구별 - 우선일 이후 공개물의 비-선행기술성

> **주의**
>
> 본 보고서가 동향으로 언급한 일부 자료(예: 2026년 중반 이후 표준 개정 후보, 우선일 이후 발표된 논문 등)는 본 출원의 우선일 이후 공개된 것으로 보이는 바, 특허법 제29조의 선행기술에 해당하지 아니한다. 본 보고서는 이들을 진보성 부정의 근거로 사용하지 않으며, 기술 분야의 활성도를 보이기 위한 맥락으로만 인용한다.

5.5 본 발명의 위치

인접 기술의 발전 방향은 (가) 더 정교한 허용/거절 판단(정책 엔진·PBAC), (나) 발급 후 토큰의 검증·동의·감사(OAuth/MCP), (다) 실행 환경의 격리·가드레일(샌드박스·게이트웨이)로 수렴한다. 본 발명은 이 세 방향 어디에도 속하지 않는 제4의 축 - "실행 가능 참조값이 발급 저장구조 네임스페이스에 생성되는지 여부 자체를, 감사 사전기록을 전제조건으로 하여 트랜잭션 경계에서 결정"하는 발급 제어 평면에 위치한다. 이 위치는 확인된 선행기술의 단독 또는 결합으로부터 용이하게 도출되지 아니한다.

제6장 진보성 종합 결론

진보성 논거	핵심 내용
① 과제 재정의의 비자명성	"이미 발급된 객체를 어떻게 제어할 것인가"에서 "실행 가능 객체의 발생 자체를 저장 구조 레벨에서 차단한다"로의 과제 재정의는 확인된 선행기술 조합으로부터 도출되지 아니함(수동적 사후 제어 → 능동적 원천 차단의 전환).
② 저장구조 물리적 부존재 보장	non_birth 불변식(7조건 동시 성립)은 논리적 거절 응답·토큰 폐기와 구조적으로 구별되며, 확인된 어떤 선행문헌도 "no executable row / no handle"의 저장구조적 부존재를 청구하지 아니함.
③ 감사 사전기록의 전제조건 배치	감사 가용성을 실행 객체 창설의 fail-closed 전제조건으로 결합한 구성은 사후 감사 로그·PAM 세션 감사와 근본적으로 상이함.
④ 상호의존 원자적 제어 흐름	목적·범위·정책·감사·발급·검증·소비를 하나의 상호의존 트랜잭션 흐름으로 결합하여, 개별 요소의 단순 조합으로 도출 불가능한 복잡성과 결합 동기 부재를 형성함.
⑤ AI tool call 실행 객체화	prompt_context_hash + arguments_hash + tool_registry_version + destination_class를 실행 객체 발생 요청으로 정규화하고, 비생성 시 tool invocation id를 DB 트랜잭션 레벨에서 미생성. 인프라 격리·I/O 가드레일과 계층·목표가 상이한 보완적 진보성.

종합 결론

이상을 종합하면, 본 발명은 확인된 선행기술의 단독 또는 그 결합으로부터 통상의 기술자가 용이하게 발명할 수 있는 것으로 보기 어렵고, 각 결합 시나리오에 대하여 결합 동기의 부재와 예측 불가능한 효과가 인정될 수 있다. 따라서 본 발명은 특허법 제29조 제2항의 진보성 요건을 충족할 것으로 판단된다.

제7장 조사 기준일 현재의 차별성 선언

차별성 선언 (한정적·검증가능 형식)

출원인은 본 보고서에 기재된 조사 방법·범위·기준일(2026년 6월 12일) 하에서, 합법적으로 열람 가능한 공개 자료를 조사한 결과, 다음 핵심 구성을 단일 문헌으로 개시하거나 복수 문헌의 결합으로 용이하게 시사하는 자료를 확인하지 못하였음을 밝힌다.

> **차별성 핵심 선언**
>
> 본 보고서에 인용된 발명들은 정책 판단, 토큰 활성 여부 확인, 사후 폐기, 감사로그 기록 또는 접근제어를 개별적으로 제공할 뿐, 고위험 행위 요청에 대하여 목적·범위·증거·정책 버전·감사 사전기록을 발급 전제조건으로 결합하고, 조건 미충족 시 issued_objects 실행 가능 네임스페이스에 후단 실행 가능한 객체 참조값 자체가 생성되지 않는 non_birth 저장구조 상태를 형성하며, 그 감사 식별자도 검증 입력으로 사용되지 않도록 하는 원자적 발급 제어 평면을 개시하거나 시사하지 않는다.

본 선언이 포괄하는 핵심 구성:

- (가) "non_birth = 발급 저장구조의 실행 가능 네임스페이스에 실행 가능 참조값 행이 생성되지 않는 결정 상태"(7개 불변식 동시 성립)
- (나) "감사 사전기록이 발급의 fail-closed 전제조건으로 작동하는 원자적 발급 제어 구조"

본 선언은 절대적·전칭 부존재의 단언이 아니라, 위 조사 전제 하의 한정적 진술이다(제0.5절). 미공개 출원·색인 누락 문헌 등에 대한 한계가 있으며, 국내 KIPRIS 정밀 검색은 대리인을 통한 별도 확인을 권고한다.

2026년 6월 12일

출원인　김 철　(KIM CHUL)　(인)

특허고객번호: 620250807042

지식재산처장　귀중

부속서 A 인용·참조 문헌 서지 및 검증 출처

No	문헌 (요지)	서지·확인 출처 (요지)	검증
A1	US 7,519,826 B2 Near real-time multi-party task authorization access control	Engedi Technologies / 법적상태 Active(만료 2026-12-07) - USPTO 원문 및 특허정보 색인 확인	◎
A2	RFC 7662 OAuth 2.0 Token Introspection	IETF(2015) - IETF 표준 문서	◎
A3	US 9,338,008 B1 Secure release of secret information over a network	Cloudera(관련 US 9,819,491 B2) - USPTO 원문 및 권리자 특허 표시 페이지 확인	◎
A4	US 9,047,490 B2 Secure execution of workflow tasks in a distributed workflow	SAP SE / 우선 2007 - 특허정보 색인 확인	◎
A5	US 2021/0279355 A1 Methods and systems for purpose-based access control(PBAC)	Google Patents / USPTO 확인	◎
A6	US 8,984,170 B2 Idempotence for database transactions(LTXID)	Oracle - USPTO·색인 확인	◎
A7	행 잠금(SELECT FOR UPDATE)/CAS	관계형 DB 동시성 제어의 확립된 공지기술	○
A8	PAM 세션 감사	특권 접근관리 세션 기록·사후 감사의 업계 일반 구현	○
A9	US 11,405,423 B2 등 Metadata-based DLP for cloud resources	데이터 손실/반출 방지(전송 중 탐지) - USPTO 확인	◎
A10	US 12,562,968 (관련 US12,549,574, US12,568,091) Proxy-based secure MCP server access for AI agents	Airia LLC - USPTO 원문 확인	◎
A11	MCP 인가 사양 / RFC 8707	Model Context Protocol 인가(OAuth 2.1, 자원 지시자) 및 도구 호출 감사·동의 경로 - 공식 사양 확인	◎
A12	Agentic JWT (A-JWT) arXiv:2509.13597	Goswami et al. / 2025-09-16 - arXiv 원문 직접 확인	◎
A13	ASTRA / TBAC arXiv:2510.26702	El Helou et al. (Cisco Systems) / 2025-10-30 - arXiv 원문 직접 확인	◎
A14	AIP / IBCT arXiv:2603.24775	Prakash et al. (ISB) / 2026-03-31 - arXiv 원문 직접 확인	◎
A15	PEA 모델 arXiv:2605.02682	미상 / 2026-05 - arXiv 원문 직접 확인 (최근접 선행기술)	◎
A16	South et al. arXiv:2501.09674	South et al. (MIT/Stanford) / 2025-01 - arXiv 원문 직접 확인	◎
A17	UCAN Spec v1.0	ucan-wg/Fission / 2023 - github.com/ucan-wg/spec 확인	◎
A18	Biscuit Token	Delafargue et al. / 2023 - biscuitsec.org 확인	◎
A19	Macaroons (NDSS 2014)	Birgisson et al. (Google) / 2014	◎
A20	IETF draft-goswami-agentic-jwt	Goswami, S. / 2025 진행 중 - IETF Datatracker 확인	◎
A21	IETF draft-prakash-aip	Prakash, R. / 2026 진행 중 - IETF Datatracker 확인	◎

부속서 B 검색 로그 요약

검색 군	대표 검색어 (요지)	확인 결과
다자 승인 인가	US7519826 / authorization agent / policy engine / authorizer	A1 확인
토큰 인트로스펙션	OAuth token introspection / active state	A2(RFC7662) 확인
비밀 릴리스	US9338008 / trustee secret release deny / Cloudera	A3 확인
분산 워크플로 실행증명	US9047490 / proof-of-execution / SAP distributed workflow	A4 확인
목적 기반 접근제어	purpose-based access control / PBAC patent / NGAC	A5 확인
DB 멱등성·행잠금	idempotency key database transaction / LTXID / SELECT FOR UPDATE	A6·A7 확인
데이터 반출/DLP	data loss prevention sensitivity / cloud DLP	A9 확인
AI 에이전트 MCP	Airia nano sandbox MCP / proxy secure MCP server / 2024~2026	A10 확인
MCP 인가 표준	MCP authorization specification OAuth resource indicators 2025/2026	A11 확인
Agentic JWT	arXiv:2509.13597 / dual-faceted intent token / agentic delegation	A12 확인
ASTRA/TBAC	arXiv:2510.26702 / task-based access control / Cisco	A13 확인
AIP/IBCT	arXiv:2603.24775 / invocation-bound capability token / ISB	A14 확인
PEA 모델	arXiv:2605.02682 / policy-execution-authorization / deterministic gate	A15 확인
South et al.	arXiv:2501.09674 / authenticated delegation / authorized AI agents	A16 확인
UCAN/Biscuit/ Macaroons	capability token delegation / attenuation / Datalog policy	A17-A19 확인
ILION/Trinity/DM-DCT	deterministic execution gate / DeepMind capability delegation	△ 원문 확인 요

검색은 한국어·영어 병용, USPTO 원문·특허정보 색인·표준 발행기관·권위 출처를 교차 확인하는 방식으로 수행하였다.

부속서 C 검증 상태 및 대리인 재검증 권고 항목

아래 항목은 출원인 내부 전략문서에 특정 번호로 기재되었으나 본 자동화 검색에서 단일 문헌으로 확정 검증되지 않았거나, 정밀 확인이 별도로 필요한 사항이다. 공식 제출 전 변리사/대리인의 1차 출처 재검증을 권고한다.

항목	상태	권고
US8370913 (정책 기반 감사 토큰 발급)	△ 미확정	번호·청구범위 재확인 또는 "정책 기반 감사 토큰 발급류 공지기술"로 일반화 인용
US10091222B1 (데이터 반출 탐지)	△ 미확정	DLP 대표 문헌(예: US11405423B2)으로 대체 인용 검토
US10581924B2 (데이터 민감도 추가 인증)	△ 미확정	번호 재확인 필요 - 미확인 시 일반 DLP/민감도 인증 공지로 처리
US11449490 (멱등성/행잠금)	△ 미확정	Oracle 멱등성(A6) + 행잠금 공지(A7)로 대체 인용
US12353579 (PBAC)	△ 미확정	PBAC 대표 문헌(A5, US2021/0279355A1 및 등록 패밀리)으로 대체 인용
EP2807560 (PAM 감사)	△ 미확정	PAM 세션 감사 공지기술(A8)로 일반화 인용
ILION (arXiv, Chitan, 2026 Q1)	△ 미확정 - 원문 미확인	원문 1차 출처 확인 필수; 확인 전 진보성 주장 확정 불가
Trinity (2025~2026)	△ 미확정 - 원문 미확인	원문 확인 필수
DM-DCT (DeepMind, 2025~2026)	△ 미확정 - 원문 미확인	원문 확인 필수
국내(KIPRIS) 유사 발명	미수행	대리인 KIPRIS 정밀 검색 별도 수행 권고 IPC G06F21/33·G06F21/41·G06F21/62

최종 권고

- 출원: non_birth(저장구조 행 미생성)와 fail-closed 감사 원자성을 시스템/방법/저장매체 전 카테고리 독립항에 반복 명시.
- 실시: purpose-bound issuance + verify/consume 강제를 일관되게 청구·기재.
- FTO: US7519826·US9338008·US9047490·A-JWT·PEA 등에 대한 claim chart 재검증 및 회피 설계 확인.
- KIPRIS: 국내 선행기술 정밀 검색은 대리인을 통해 최우선으로 수행.
- 본 보고서의 모든 진보성 판단은 변리사/대리인의 최종 검토를 전제로 한다.

문서 식별

선행기술 진보성 자진조사보고서 (우선심사신청 첨부자료)
발명 명칭: 목적 결속형 실행 객체 비생성 제어 기반의 접근·세션·실행·반출 및 도구 호출 통제 시스템 및 그 방법
출원인: 김철 (KIM CHUL) | 특허고객번호: 620250807042 | 작성 기준일: 2026. 6. 12.