

선행기술대비표

Prior Art Comparison Table | AAL (Agentic Authorization Layer) 인가 게이트웨이

- 우선심사신청서 첨부자료 -

발명의 명칭	목적 결속형 실행 객체 비생성 제어 기반의 접근·세션·실행·반출 및 도구 호출 통제 시스템 및 그 방법
작성 목적	명세서, 도 1~8, 우선심사신청설명서, AAL 기술자료, 운영 PoC 측정자료 및 선행기술 진보성 자진조사서를 교차 검토하여 심사관이 핵심 차이를 빠르게 확인할 수 있도록 구성요소별 선행기술 대비표를 제공함
검토 기준 문서	① AAL 명세서 및 도 1~8 최신 제출본 ② 선행기술진보성자진조사서.pdf ③ 우선심사신청설명서.pdf ④ AAL기술자료.pdf ⑤ AAL운영PoC측정자료.pdf ⑥ AAL사업행정자료.pdf 및 AAL보조자료.pdf
작성 기준일	2026년 6월 12일
반영 원칙	선행기술대비표_0의 KIPO 제출용 구조·문체·정합성 점검을 기준으로 하고, 선행기술 대비표_1의 AI 에이전트 인가 군집, 최신 우선일·조사일 및 FTO 우선도 정보를 결합함
표현 원칙	전 세계 전수 부존재를 단정하지 않고, 조사 범위 및 기준일 하에서 확인된 선행문헌의 단독 또는 결합으로부터 핵심 구성이 개시·시사되지 않는다는 한정형 표현을 사용함

본 대비표의 핵심 명제

본 발명의 핵심은 이미 존재하는 토큰·세션·파일·도구 호출을 사후 검증·폐기하는 것이 아니라, 목적 객체, 범위 해시, 활성 정책 버전, 감사 사전기록 및 복수 발급 전제조건이 하나의 발급 트랜잭션 내에서 성공하지 않으면 issued_objects 실행 가능 네임스페이스에 후단 실행 가능한 객체 참조값 자체가 생성되지 않는 non_birth 저장구조 상태를 형성하는 데 있다.

1. 제출 전 교차 검토 결론

검토 항목	판단	근거	의견
명세서-도면 정합성	매우 양호	도 1은 요청 수신·목적 결속·범위 해시·정책 버전·감사 사전기록·객체 발생 결정·원자 발급 흐름을 일관되게 표시하고, 도 5/6은 AI 도구 호출 및 데이터 반출 게이트웨이를 분리함	최신 도면군을 그대로 제출 가능. 도 7의 EXPIRED/REVOKED/BR EAK_GLASS 및 감사 이벤트 흐름 도 청구항 33과 정합
명세서-선행기술 조사서 정합성	매우 양호	조사서는 발급 제어 평면, non_birth 7조건, issued_objects/non_birth_events 분리, AI 에이전트 인가 군집 대비를 중심으로 삼음	보고서 본문과 본 대비표를 함께 첨부하면 심사관 파악 속도 향상
도면-운영 PoC 정합성	양호	운영자료는 purpose, scope hash, policy version, pre-audit, born/shadow/non_birth, verify/consume/replay, invariant proof 7/7을 증거화	우선심사신청설명서의 실시준비 논리와 충돌 없음
선행기술대비표_0/_1 통합	완료	_0의 공식 제출 구조와 _1의 AI 에이전트 선행기술 군집을 결합	최종본은 철용성(기준) + moat(추가 최신 조사) 구조로 운용

2. 도면-명세서-보고서 교차 정합성 표

도면/자료	현재 정합성 판단	명세서/보고서 대응	제출 전 조치
도 1 전체 아키텍처	요청 수신부부터 원자적 객체 발급부까지 흐름 명확	목적 객체, 범위 해시, 정책 버전, 감사 사전기록이 발급 전제조건으로 결합	유지 권장
도 2 객체 생애주기	requested/evaluated/minted/verified/consumed/finalized/audited 흐름 안정	후단 강제와 소비 트랜잭션이 연결됨	유지 권장
도 3 상태기계	born, shadow-executable, shadow-review, non_birth 분기 명확	결정상태와 발급 네임스페이스 행 생성 여부를 구분	유지 권장
도 4 소비 트랜잭션	verify -> reserve/lock -> commit/finalize -> backend enforcement 및 blocked audit 흐름 명확	1-7 소비 바인딩과 double-spend/replay 차단 논리 대응	부호 221~224 정합 유지
도 5 AI Agent Gateway	tool call을 실행 객체 발생 요청으로 변환하고 non_birth가 비실행 감사 흐름임을 표시	AI 에이전트 인가 선행기술 군집 대비의 핵심 도면	유지 권장
도 6 Export Gateway	file creation handle/download URL/external transfer handle/BI extract reference 미생성 논리 명확	DLP·PBAC와의 차별점 직접 대응	유지 권장

도면/자료	현재 정합성 판단	명세서/보고서 대응	제출 전 조치
도 7 감사 체인	PRE_DECISION, OBJECT_MINTED, NON_BIRTH, EXPIRED, REVOKED, BREAK_GLASS 등 반영	감사 선행조건 및 감사 이벤트 예시와 정합	유지 권장
도 8 검증 캔버스	decide/verify/consume/audit API와 불변식 증명 대응	운영 PoC 및 침해 판단 리트머스 역할	유지 권장

3. AAL 7대 불변식 기준 핵심 대비

아래 표는 AAL의 7대 핵심 불변식을 선행기술 군집과 비교한 요약이다. ○는 개시 또는 강한 개념 중첩, △는 부분 개시 또는 유사 개념, ×는 본 대비표 기준 개시 확인 없음, △검증은 원문·시간적 지위 재확인 필요를 의미한다.

불변식	AAL 구현	AI 에이전트 인가 군집 대비	기초 토큰군 / 기준 접근제어군
I-1 비출생 저장	사전조건 실패 시 issued_objects 행 미생성	A-JWT × / ASTRA × / AIP·IBCT × / PEA ×	기초 토큰군 × / 기준 접근제어군 ×
I-2 감사 선행 조건	감사 레코드 = 발급 fail-close 선행조건	A-JWT × / ASTRA × / AIP·IBCT △ 사후 출처 / PEA ×	기초 토큰군 × / 기준 접근제어군 △ 사후감사
I-3 목적 결속	purpose object 원자 결합	A-JWT ○ 의도 결속 / ASTRA △ 작업 매핑 / AIP·IBCT ○ 호출 결합 / PEA △ 작업·정책 게이트	기초 토큰군 △ caveat·정책 / 기준 접근제어군 △ PBAC
I-4 발급자 4중 속성	신원 + 권한 + 목적 + 유효기간	A-JWT △ / ASTRA △ / AIP·IBCT △ / PEA △	기초 토큰군 ○/△ / 기준 접근제어군 △
I-5 네임스페이스 분리	issued_objects ↔ non_birth_events 엄격 분리	A-JWT × / ASTRA × / AIP·IBCT × / PEA ×	기초 토큰군 × / 기준 접근제어군 ×
I-6 비우회성	복수 계층 교차 검증	A-JWT △ / ASTRA △ / AIP·IBCT △ / PEA ○	기초 토큰군 △ / 기준 접근제어군 △
I-7 소비 바인딩	verify → consume 원자 쌍, 단일사용	A-JWT × / ASTRA × / AIP·IBCT △ / PEA △	기초 토큰군 △ / 기준 접근제어군 △
전체 핵심 충족	7/7	A-JWT 1~2/7 / ASTRA 1~2/7 / AIP·IBCT 2~3/7 / PEA 2~3/7 최근접	기초 토큰군 2/7 내외 / 기준 접근제어군 1~2/7

요약

검토된 문헌군 중 I-1(비출생 저장 불변식), I-2(감사 선행 조건), I-5(실행/비실행 네임스페이스 분리)의 조합을 동시에 개시하는 문헌은 확인되지 않는다. PEA는 최근접이나 최종적으로 토큰을 발급하는 post-birth 계열이다.

4. 구성요소별 종합 대비

구성요소	AAL 핵심	선행기술 대비
목적 객체	object_type, action, resource_ref, normalized_scope, risk_class, approval_ref, retention_rule, evidence_validity를 포함하는 기계 검증 구조체	PBAC/A-JWT/ASTRA가 목적·의도·작업을 다루나 발급 결정과 행 생성/미생성 원자 결합은 없음
범위 해시(scope_hash)	요청 범위와 정책 범위를 해시화하여 발급 전 제조건으로 결합	범위 최소화(ASTRA) 또는 토큰 caveat(UCAN/Biscuit)는 있으나 저장구조 미생성의 선행조건으로 결합되지 않음
활성 정책 버전	발급 시점의 정책 버전이 객체 발생 결정에 결합	일반 정책엔진 문헌은 정책 적용을 개시하나 active policy version이 객체 출생 조건으로 실패 폐쇄하는 구조는 아님
감사 사전기록	pre-audit 레코드 생성 실패 시 발급 불가	PAM/출처 추적/AIP는 사후 감사 또는 append-only 기록. 발급 차단 선행조건은 아님
객체 발생 결정	born/shadow-executable/shadow-review/non_birth 상태기계	기존 allow/deny, sandbox block, token grant와 달리 행 생성 여부를 상태기계와 결합
원자적 객체 발급	조건 충족 시에만 issued_objects에 실행 가능 참조값 생성	PEA는 게이트 후 토큰 발급. 실패 시 non_birth_events와 분리된 비실행 상태를 저장하는 구조 없음
AI tool call 통제	tool call을 실행 객체 발생 요청으로 정규화하고 tool invocation id 비생성을 포함	A-JWT/ASTRA/AIP는 에이전트 권한 결속이나 호출 참조값 자체의 비출생을 개시하지 않음
데이터 반출 통제	file handle/download URL/BI extract reference 비생성	DLP는 전송 탐지·차단 중심. 참조값 출생 전 제어 아님
소비 바인딩	verify -> reserve/lock -> commit/finalize 원자 쌍	기초 토큰군의 단일사용 또는 만료와 달리 DB 행 잠금/후단 강제까지 결합

5. 선행기술별 상세 대비 - 기준 문헌군

문헌	분야	개시 요지	AAL 차별점
US7519826	다자 승인 후 접근 허용	승인 후 authorization agent가 접근을 집행	승인 결과와 issued_objects 행 생성의 원자 결합, non_birth 행 미생성 상태가 없음
RFC 7662	토큰 인트로스펙션	기발급 토큰의 active 상태 조회	검증 대상 토큰 자체가 존재하지 않는 non_birth와 다름
US9338008	trustee 비밀 릴리스	비밀자료의 release/deny	비밀 전달 제어이지 실행 가능 참조값의 출생 전 제어 아님
US9047490	워크플로 proof-of-execution	실행 완료 무결성 증명	객체 발생 이후 검증. 발급 저장구조 미생성 제어와 시점이 다름
PBAC	목적 기반 접근제어	목적을 정책 속성으로 처리	목적 구조체와 발급 네임스페이스 행 생성/미생성의 원자 결합 없음
IDEMPO/ROWLOCK	커밋 1회성/행잠금	동시성·역등성 제어	AAL은 이를 목적·감사·비생성 불변식과 결합하여 실행 객체 공격면 제거
PAM/DLP	사후 감사/반출 차단	세션 기록, 전송 탐지·차단	감사가 발급 선행조건으로 fail-closed하지 않고, 파일/반출 참조값 미생성 보장 없음
Airia/MCP-AUTH	샌드박스 및 OAuth/MCP 인가	격리 실행·자원 지시자·동의·감사	격리·인가 표준이지 issued_objects/non_birth_events 분리 불개시

6. 선행기술별 상세 대비 - AI 에이전트 인가 군집

문헌군	선행기술 개시	검치는 부분	AAL 차별 요소
A-JWT	의도 결속 JWT, 에이전트 신원 체크섬, 위임 연쇄	목적/의도 결속(I-3)	토큰 생성 후 결속. 비출생 저장(I-1), 감사 선행(I-2), 네임스페이스 분리(I-5), 소비 바인딩(I-7) 없음
ASTRA/TBAC	자연어 작업 요청의 의미론적 분석과 최소 scope 토큰 발급	작업 기반 권한 최소화	발급 scope 최적화이지 행 미생성 보안 경계가 아님
AIP/IBCT	호출 결합 역량 토큰, 신원·권한·범위·출처 체인	호출 결합 및 출처 추적	존재 후 감쇄·사후 출처 기록. 감사가 발급 물리적 선행조건이 아님

문헌군	선행기술 개시	겹치는 부분	AAL 차별 요소
PEA/HIT-ZTAI	정책-실행-인가 분리, 결정론적 다중 게이트, 통과 후 단일사용 토큰	최근점: 게이트 후 발급, 비우회성 일부	게이트 실패 시 issued_objects 행 자체 미생성, non_birth_events 분리, audit fail-closed 선행조건 불개시
ILION/Trinity	결정론적 실행/명령 게이트	실행 전 차단	저장구조상 객체 출생 제어인지 원문 확인 필요. 현 단계에서 I-1/I-2/I-5 결합 확인 안 됨
South/UCAN/Biscuit/Macaroons	인증 위임·오프라인 감쇄·Datalog 정책·caveat	발급된 역량의 감쇄·위임	토큰 존재 전제. 비출생 패러다임으로 전환할 결합 동기 부족

7. 결합 발명 방어 시나리오 요약

시나리오	결합 문헌	가상 주장	반증 논거	강도
E 핵심	A-JWT + ASTRA + AIP/IBCT + ILION/PEA	결합 시 AAL의 기술적 효과 달성 가능	군집 전체가 존재 후 토큰·역량 제어 패러다임. I-1 비출생, I-2 감사 선행, I-5 네임스페이스 분리, I-7 소비 바인딩의 결합 없음	★★ ★★ ★
F	PEA + South et al.	게이트 + 인증 위임으로 AAL 자명	두 문헌 모두 자격증명 발급 전제. 결합 귀결은 인증 위임 + 다중 게이트 발급이 지행 미생성 아님	★★ ★★ ☆
G	Macaroons + UCAN + Biscuit	기초 역량 토큰 진화로 AAL 자명	오프라인 감쇄·최소 발급자 신뢰 계보. 감사 선행조건 및 실행 가능 행 미생성 방향 변형 동기 없음	★★ ★★ ☆
H	RFC7662 + PBAC + Airia	토큰 조회 + 목적 정책 + 샌드박스 결합	각각 토큰 존재, 정책 판단, 실행 격리를 전제로 함. 실행 객체 출생 전 저장구조 제어가 아님	★★ ★★ ☆
A-D 기준	US751/PBAC/DLP/PAM/D B 행잠금 등	일반 접근제어·감사·DLP·트랜잭션 조합	일반 구성요소는 개별적으로 알려져 있으나 목적·범위·정책·감사 선행조건을 행 미생성과 원자 결합하는 동기와 효과 없음	★★ ★★ ☆

8. 시간적 지위 및 FTO 검색 우선도

약칭	공개/출원일	우선일 대비	핵심 개시	FTO 우선도	검증
South	2025-01	선행	인증 위임·권한 범위 결합	★★★★★	◎

약칭	공개/출원일	우선일 대비	핵심 개시	FTO 우선도	검증
A-JWT	2025-09-16	선행	의도 토큰 결속, 에이전트 신원 체크	★★★★★	◎
ASTRA/TBAC	2025-10-30	선행	작업-범위 의미론적 매핑, 최소 범위 발급	★★★★★	◎
AIP/IBCT	2026-03-31	선행	호출 결합 역량 토큰, 출처 체인	★★★★★	◎
PEA/HIT-ZTAI	2026-05	선행, 최근접	3계층 분리, 결정론적 다중 게이트, 단일사용 서명 역량	★★★★★	◎
ILION	2026 Q1 추정	선행 추정	결정론적 실행 게이트	★★★★☆	△ 원문 필요
Trinity/DM-DC T	2025~2026 추정	선행 추정	명령 게이트·감쇄 우선 위임	★★★★☆	△ 원문 필요
Airia	2024	선행	나노샌드박스 AI 보안, 실행 격리	★★★★☆	◎
UCAN/Biscuit/Macaroons/RFC 7662	2014~2023/2015	선행	기초 역량 토큰 및 토큰 인트로스펙션	★★★★~★★★	◎
KIPRIS 국내 문헌	별도 검색	미확정	국내 선행기술 가능성	최우선	대리인 검색

9. 종합 결론

본 대비표는 _0의 공식 제출용 구조를 기준으로 하되, _1의 최신 AI 에이전트 인가 군집을 모두 흡수하여 최종 제출용으로 재정렬하였다. 결론적으로, 검토된 선행문헌은 AAL의 일부 주변 요소인 목적/의도 결속, 작업 기반 범위 최소화, 호출 결합 역량 토큰, 샌드박스 격리, 토큰 인트로스펙션, 사후 감사, DLP 및 DB 행잠금을 각각 개시할 수 있다.

그러나 어느 단일 문헌도, 그리고 확인된 결합 시나리오도, 목적·범위·활성 정책 버전·감사 사전기록을 발급 트랜잭션의 선행조건으로 결합하고, 조건 미충족 시 issued_objects 실행 가능 네임스페이스에 후단 실행 가능한 객체 참조값 자체가 생성되지 않으며, non_birth_events와 issued_objects를 분리하고, verify -> consume 원자 소비와 후단 강제까지 연결하는 구성을 개시·시사하지 않는 것으로 정리된다.

심사관 검토 포인트

AAL은 allow/deny, token introspection, purpose attribute, sandbox, DLP, audit log가 아니다. AAL은 execution-object birth control plane이며, 실패 조건에서는 실행 가능한 객체가 태어나지 않는다.