# 선행기술자진조사보고서

대상 발명: 진입 전 기원증명 및 운동성 평가에 기초한 기능효력 제어 시스템, 방법 및 기록매체 / 기준일: 2026-06-27

## 1. 조사 결론

- 가장 근접한 공개기술군은 AI 에이전트의 pre-action authorization 또는 admission control 계열, OAuth/Keycloak/DPoP/RAR 계열의 정책·토큰 기반 인가, STIR/SHAKEN/PASSporT 계열의 통신 발신자 신뢰, EMV 3DS/SCA 계열의 금융 거래 인증, W3C PROV/Certificate Transparency/Sigstore 계열의 provenance 및 append-only 감사로그이다.
- 조사된 단일 공개문헌은 “대상 입력이 기능적 실제가 되기 전 기원증명값을 생성하고, 원문 비저장 압축 식별정보와 시간 단위 운동성 측정정보, 계보 응집도값, 기원 문맥 특징 벡터, 문맥 특징 결여 상태, 관계 그래프 상태, 기능효력 범위 결속 상태를 결합하여, 존재/표시는 말소하지 않되 실행·승인·반출·신뢰표시·세션 지속·계약상 효력·상태전이의 기능효력만 fail-inert 방식으로 제어하는 구조”를 전요소로 개시하지 않는다.
- 심사에서 조합 논리가 제기될 가능성이 높은 조합은 “OAP/ACP/ARM + OAuth/DPoP/RAR + CT/PROV 감사로그”이다. 이 조합에 대해서는 본건의 차별축을 “권한 토큰/사후 provenance/도구 호출 정책”이 아니라 “기능효력 성립 전 기원증명값과 운동성·관계 그래프·범위 결속을 하나의 효력 성립 조건으로 묶는 기존 시스템 연동형 제어층”으로 고정하는 것이 유리하다.
- 우선심사 제출용 논리에서는 발명의 효과를 보안 일반론이나 위험 점수 향상으로 쓰기보다, 기존 시스템을 대체하지 않으면서 기능효력 부여 직전 지점에서 기능효력 결정을 제공하고, 효력 없음(NO_EFFECT)에서도 원 객체의 존재 자체는 말소하지 않는 기술적 인터록 구조로 설명하는 편이 강하다.

## 2. 청구항 핵심요소 매핑

| 요소 | 기술 내용 | 심사 대응 핵심어 |
|---|---|---|
| A | 기존 기능 체계 안에서 기능적 효력을 획득하려는 대상 입력의 수신 | 기존 시스템 대체가 아닌 연동 |
| B | 기능적 실제가 되기 전 기원증명값 생성, 원문 비저장 | pre-effect origin proof / privacy-preserving commit |
| C | 압축 식별정보 생성 | 원문 없는 참조값 및 컨텍스트 해시 |
| D | 시간 단위 운동성 측정정보 수집 | 0.1초 또는 설정 윈도우 / micro-batch motion |
| E | 계보 응집도값, 기원 문맥 특징 벡터, 문맥 특징 결여 상태 산출 | state of origin continuity, not generic risk score |
| F | 복수 기원증명값의 관계 그래프 상태 산출 | multi-origin relationship graph |
| G | 기능효력 범위 결속 | delete/block 전체가 아닌 effect-scope binding |
| H | 효력 없음(NO_EFFECT)에서도 존재/표시는 말소하지 않고 기능효력만 미부여 | fail-inert interlock |
| I | 감사 영수증 체인 | decision reproducibility, not mere logging |

## 3. 근접 선행기술군별 조사

### 3.1 AI 에이전트 pre-action authorization / admission control

ACP는 에이전트의 intent와 system state mutation 사이에서 행위가 실행되기 전 admission control을 수행하는 계층을 제시한다 [R1]. OAP는 individual tool call 전에 declarative policy를 평가하고 signed audit record를 생성한다 [R2]. ARM은 tool calls, returned data, denied actions를 포함한 provenance graph를 사용한다 [R4].

이 계열은 본건과 가장 가깝다. 그러나 중심은 에이전트 도구 호출의 허가·거부 또는 provenance-aware tool mediation이다. 본건은 AI 도구 호출에 한정되지 않고 API, 통신 세션, 금융 승인, 데이터 반출, 계정 상태전이, 계약상 효력, 관리자 예외를 동일한 기능효력 성립 조건으로 다룬다.

본건 차별 포인트는 “정책 허가” 자체보다, 기능적 실제가 되기 전의 기원증명값, 그 기원증명값의 시간 단위 운동성, 문맥 특징 결여, 관계 그래프 상태, 기능효력 범위 결속을 결합하여 기존 기능 체계의 후단 효력 핸들 생성을 인터록하는 구조이다.

### 3.2 Prompt injection 방어와 capability control

CaMeL은 trusted query에서 control flow와 data flow를 추출하고, untrusted data가 program flow에 영향을 주지 못하도록 capability 기반으로 data exfiltration을 방지한다 [R3].

CaMeL은 prompt injection 문제에 강한 방어 구조를 제시하지만, 원문 프롬프트를 기능효력 판단용 원문 보관 객체로 저장하지 않는 기원증명값, 시간 단위 운동성 측정정보, 계보 응집도 및 관계 그래프 상태를 기능효력의 성립 조건으로 제시하지 않는다.

### 3.3 OAuth / Keycloak / DPoP / RAR 계열

RFC 8693은 token exchange를 통해 OAuth 보안 토큰을 요청·획득하는 STS 구조를 정의하고 [R5], RFC 9396은 authorization_details를 통해 fine-grained authorization data를 전달한다 [R6]. RFC 9449는 DPoP로 token replay를 줄이는 proof-of-possession mechanism을 정의한다 [R7]. Keycloak Authorization Services는 resource server 측 PEP와 정책 평가 구조를 제공한다 [R8].

이 계열은 "권한 범위·토큰·정책 평가"에는 가깝지만, 이미 권한 운반체 또는 정책 평가 대상이 성립한 후의 authorization에 무게가 있다. 본건은 권한 토큰이 아니라 기능효력 획득 전 대상 입력 자체의 기원증명과 운동성 상태를 선행 조건으로 삼는다.

### 3.4 Kubernetes admission control 등 범용 admission 구조

Kubernetes admission webhook은 API 객체가 persistence 되기 전 API 서버가 mutating 또는 validating webhook을 호출하는 확장 지점이다 [R9].

Admission control 자체는 "저장 전 판단"이라는 점에서 가까우나, 본건의 기원증명값, 압축 식별정보, 시간 단위 운동성, 관계 그래프, 기능효력 범위 결속, 존재/표시와 기능효력의 분리라는 결합 구조는 개시하지 않는다.

### 3.5 Provenance, transparency log, audit receipt chain

W3C PROV는 데이터 또는 사물의 생산에 관여한 entity, activity, person에 관한 provenance 정보를 모델링한다 [R10]. RFC 6962 및 RFC 9162의 Certificate Transparency는 append-only Merkle tree log와 consistency proof로 공개 감사를 지원한다 [R11][R12]. Sigstore는 software artifact 서명과 Rekor transparency log 등을 제공한다 [R13].

이 계열은 감사 가능성, 위변조 방지, provenance 표현에는 가깝다. 그러나 기능효력 부여 직전 기원증명값과 운동성·관계 그래프 평가를 수행하고, 그 결과에 따라 후단 기능효력 핸들만 생성되지 않도록 제어하는 active control layer는 아니다.

### 3.6 통신 발신자 신뢰: STIR/SHAKEN/PASSporT

RFC 8224는 SIP originator identity를 cryptographic signature로 검증하는 구조를 정의한다 [R14]. RFC 8225의 PASSporT는 originating identity 또는 telephone number를 signed token으로 검증하고 [R15], RFC 8226은 telephone number authority에 관한 credential 구조를 다룬다 [R16]. RFC 8588은 SHAKEN attestation level과 origination identifier를 PASSporT claim으로 확장한다 [R17].

본건의 통신 실시예와 접점은 전화번호 표시 신뢰 요청 및 세션 지속 요청이다. 그러나 STIR/SHAKEN은 통신 발신자 표시의 신원/권한 검증에 한정되고, 통신과 금융·AI·API·데이터 반출 사이의 관계 그래프 및 기능효력 범위 결속을 다루지 않는다.

### 3.7 금융 승인: EMV 3DS와 Strong Customer Authentication

EMVCo는 EMV 3DS가 card-not-present fraud 방지와 e-commerce payment security 향상에 쓰이는 기술이라고 설명한다 [R18]. EU Regulation 2018/389는 PSD2 하의 strong customer authentication 및 secure communication standards를 정한다 [R19].

이 계열은 거래 승인 전 인증과 위험평가에 가깝지만, 기원증명값의 운동성 측정, 복수 기원증명값 관계 그래프, 효력 범위 결속, 효력 없음 상태에서의 존재/표시 보존형 제어는 개시하지 않는다.

### 3.8 특허문헌군

US 11,196,560 B2는 정책 검증과 token generating responsibility 확인 후 토큰을 생성하는 authorization framework이다 [R20]. US 11,245,682 B2는 권한 판단 후 rule/condition 정보를 포함한

access token을 생성한다 [R21]. US 8,887,286 B2와 US 10,757,122 B2는 행동 모델 및 사용자 행동 이상탐지에 관한 문헌이다 [R22][R23]. US 9,324,119 B2는 identity/asset risk score와 trend를 계산한다 [R24]. US 2018/0285839 A1은 immutable ledger overlay network를 이용한 data provenance, permissioning, compliance, access control 구조이다 [R25].

특허문헌군은 토큰 기반 권한, adaptive authorization, anomaly detection, risk score, provenance ledger의 개별 요소를 보여준다. 그러나 본건의 “진입 전 기원증명값 + 시간 단위 운동성 + 기원 문맥 특징 결여 + 관계 그래프 상태 + 기능효력 범위 결속 + fail-inert 기능효력 제어 + 감사 영수증 체인” 조합을 전요소로 제시하지 않는다.

## 4. 신규성 및 진보성 주장의 중심축

| 주장축 | 구체 논점 |
|---|---|
| 기원증명값의 위치 | 인증 토큰 또는 로그 이벤트가 아니라 기능적 실제가 되기 전 생성되는 효력 성립 전 기록으로 정의한다. |
| 운동성 측정 | 0.1초 또는 설정 가능 시간 윈도우에서 기원증명값의 상태 변이를 측정한다. 단순 행동 이상탐지가 아니라 기원증명값의 계보·문맥·관계 구조를 판단한다. |
| 기능효력 범위 결속 | 대상 입력 자체를 삭제하거나 파괴하지 않고, 실행/승인/반출/신뢰표시/세션 지속/계약상 효력/상태전이 중 특정 효력 범위만 결속한다. |
| fail-inert 제어 | NO_EFFECT에서도 네트워크 패킷, 표시 문자열, 입력 기록, 요청 기록, 감사 기록의 존재를 부정하지 않으면서 후단 효력 핸들 생성을 막는다. |
| 기존 시스템 연동성 | 기존 인증·인가·승인·세션 처리·감사 절차를 대체하지 않고 기능효력 부여 직전 결정 조회/수신 지점으로 연동한다. |
| 감사 영수증 체인 | 단순 저장 로그가 아니라 기능효력 결정의 재현 가능한 근거를 기원증명값·운동성·상태 평가·관계 그래프·결속 상태와 연결한다. |

## 5. 예상 거절이유별 대응 초안

| 예상 논리 | 대응 논점 |
|---|---|
| AI 에이전트 OAP/ACP 문헌을 근거로 한 신규성·진보성 거절 | OAP/ACP는 tool call 또는 agent action에 대한 deterministic authorization/admission control이다. 본건은 대상 입력의 종류를 AI 도구 호출로 한정하지 않고, 기능효력 성립 전 기원증명값과 그 운동성·관계 그래프·범위 결속을 기능효력 조건으로 결합한다. 또한 NO_EFFECT에서도 객체의 존재 자체를 말소하지 않는 fail-inert 후단 인터록을 명시한다. |
| OAuth/DPoP/RAR 또는 Keycloak과의 조합 | OAuth 계열은 권한 운반체의 발급·교환·범위·proof-of-possession이 중심이다. 본건은 token possession이나 scope evaluation이 아니라 기능효력 세계에 들어가기 전 대상 입력의 기원증명값과 운동성 상태를 판단한다. 권한 토큰을 대체하는 것이 아니라 기존 인가 절차 앞 또는 직전에서 별도 효력 결정을 제공한다. |
| Provenance/CT/Sigstore와의 조합 | Provenance 및 transparency log는 기록·검증·감사에 강점이 있으나, 본건은 감사 영수증을 기능효력 결정의 부속 결과로 생성하고, 그 전에 기원증명값과 운동성·관계 그래프를 active decision gate로 사용한다. 즉 사후 추적 가능성만으로는 본건의 기능효력 부여/미부여 구조가 도출되지 않는다. |
| 행동 이상탐지 또는 risk score 문헌과의 조합 | 행동 모델과 risk score는 이상 여부를 점수화한다. 본건의 계보 응집도값, 기원 문맥 특징 벡터, 문맥 특징 결여 상태, 관계 그래프 상태는 기원증명값의 기능효력 성립 조건으로 사용되며, 결과가 특정 효력 범위 결속과 fail-inert 인터록으로 이어진다. |

## 6. 청구항 보강 권고

- 독립항에는 “기능적 실제가 되기 전에”와 “기존 기능 체계가 기능적 효력을 부여하기 전에”를 모두 남겨 pre-effect timing을 이중으로 고정한다.
- 관계 그래프 상태 산출 주체는 관계 그래프 평가부(160)로 고정한다. 상태 평가부(150)는 계보 응집도값, 기원 문맥 특징 벡터, 문맥 특징 결여 상태, 변이지수, 파열 플래그에 집중한다.
- NO_EFFECT 문언은 “존재 자체를 말소하지 않으면서 실행 가능한 핸들 등 후단 효력값이 생성되거나 사용되지 않도록 제어”로 유지한다.
- 감사 영수증은 event_hash 등의 필드명만이 아니라 기능효력 결정의 재현 가능한 근거 연결 구조로 기재한다.
- 도면 및 부호의 설명에서는 801/802/803, 903/904/905를 한글 주표기로 유지하고, 영문 상수명은 본문 괄호 병기로 제한한다.

## 참고문헌

| 번호 | 자료 | 조사상 의미 |
|---|---|---|
| R1 | Marcelo Fernandez, Agent Control Protocol: Admission Control for Agent Actions, arXiv:2603.18829 https://arxiv.org/abs/2603.18829 | 에이전트 행위가 실행되어 시스템 상태를 변경하기 전에 실행 trace의 속성을 검사하는 admission control 계층을 제시한다. |
| R2 | Uchi Uchibeke, Before the Tool Call: Deterministic Pre-Action Authorization for Autonomous AI Agents, arXiv:2603.20953 https://arxiv.org/abs/2603.20953 | 도구 호출 직전 동기식 정책 평가 및 암호학적으로 서명된 감사 기록을 제시한다. |
| R3 | Edoardo Debenedetti et al., Defeating Prompt Injections by Design, arXiv:2503.18813 https://arxiv.org/abs/2503.18813 | 프롬프트 인젝션 방어를 위해 trusted query에서 control flow와 data flow를 분리하고 capability를 사용한다. |
| R4 | Mohammad Hossein Chinaei, Causality Laundering: Denial-Feedback Leakage in Tool-Calling LLM Agents, arXiv:2604.04035 https://arxiv.org/abs/2604.04035 | 도구 호출, 반환 데이터, 거부된 행위까지 포함하는 provenance graph와 runtime reference monitor를 제시한다. |
| R5 | RFC 8693, OAuth 2.0 Token Exchange https://www.rfc-editor.org/info/rfc8693/ | HTTP/JSON 기반 Security Token Service로 토큰 교환, 위임 및 impersonation 시나리오를 다룬다. |
| R6 | RFC 9396, OAuth 2.0 Rich Authorization Requests https://datatracker.ietf.org/doc/html/rfc9396 | OAuth 메시지에서 fine-grained authorization data를 authorization_details 파라미터로 전달한다. |
| R7 | RFC 9449, OAuth 2.0 Demonstrating Proof of Possession https://www.rfc-editor.org/info/rfc9449/ | 애플리케이션 계층 proof-of-possession으로 OAuth 토큰을 sender-constrained token으로 묶어 재전송을 줄인다. |
| R8 | Keycloak Authorization Services Guide https://www.keycloak.org/docs/latest/authorization_services/index.html | 리소스 서버 측 Policy Enforcement Point 및 정책 평가 구조를 제공한다. |
| R9 | Kubernetes Dynamic Admission Control https://kubernetes.io/docs/reference/access-authn-authz/extensible-admission-controllers/ | API 서버가 객체를 저장하기 전 mutating/validating admission webhook을 호출하는 확장 지점을 제공한다. |
| R10 | W3C PROV Overview / PROV-DM https://www.w3.org/TR/prov-overview/ | 데이터 또는 사물의 생산에 관여한 entity, activity, person에 관한 provenance 정보를 모델링한다. |

| 번호 | 자료 | 조사상 의미 |
|---|---|---|
| R11 | RFC 6962, Certificate Transparency<br>https://www.rfc-editor.org/info/rfc6962/ | TLS 인증서의 존재를 append-only Merkle tree log에 기록하고 inclusion/consistency proof로 감사한다. |
| R12 | RFC 9162, Certificate Transparency Version 2.0<br>https://www.rfc-editor.org/info/rfc9162/ | Certificate Transparency v2.0으로 공개 로그와 감사 가능한 Merkle consistency proof 구조를 정의한다. |
| R13 | Sigstore / OpenSSF Sigstore<br>https://openssf.org/community/sigstore/ | Cosign, Fulcio, Rekor transparency log 등을 통해 software artifact 서명과 추적을 제공한다. |
| R14 | RFC 8224, Authenticated Identity Management in SIP<br>https://www.rfc-editor.org/info/rfc8224/ | SIP 요청 발신자 식별을 cryptographic signature로 검증하기 위한 Identity header 메커니즘을 정의한다. |
| R15 | RFC 8225, PASSporT: Personal Assertion Token<br>https://www.rfc-editor.org/info/rfc8225 | 개인 통신의 발신 identity 또는 telephone number를 cryptographically signed token으로 검증한다. |
| R16 | RFC 8226, Secure Telephone Identity Credentials<br>https://www.rfc-editor.org/info/rfc8226/ | 전화번호에 대한 authority를 certificate로 주장하는 STIR credential 구조를 다룬다. |
| R17 | RFC 8588, PASSporT Extension for SHAKEN<br>https://www.rfc-editor.org/info/rfc8588/ | SHAKEN 프레임워크의 attestation level과 origination identifier를 PASSporT claim으로 확장한다. |
| R18 | EMVCo, EMV 3-D Secure<br>https://www.emvco.com/emv-technologies/3-d-secure/ | 카드 비대면 거래에서 fraud 감소와 e-commerce payment security 강화를 위한 EMV 3DS를 제공한다. |
| R19 | Commission Delegated Regulation (EU) 2018/389<br>https://eur-lex.europa.eu/eli/reg_del/2018/389/oj/eng | PSD2의 strong customer authentication 및 common and secure open standards of communication 관련 RTS. |
| R20 | US 11,196,560 B2, Policy and token based authorization framework for connectivity<br>https://patents.google.com/patent/US11196560B2/en | 정책 검증 후 token generating responsibility를 확인하고 token을 생성하는 connectivity authorization framework. |
| R21 | US 11,245,682 B2, Adaptive authorization using access token<br>https://patents.google.com/patent/US11245682B2/en | protected resource 접근 권한 판단 후 rule/condition 정보를 포함한 access token을 생성한다. |

| 번호 | 자료 | 조사상 의미 |
|---|---|---|
| R22 | US 8,887,286 B2, Continuous anomaly detection based on behavior modeling and heterogeneous information analysis https://patents.google.com/patent/US8887286B2/en | 다차원 behavior modeling과 heterogeneous information analysis에 기반한 continuous anomaly detection. |
| R23 | US 10,757,122 B2, User behavior anomaly detection https://patents.google.com/patent/US10757122B2/en | user behavior module을 통해 network user behavior anomaly를 탐지하는 구조. |
| R24 | US 9,324,119 B2, Identity and asset risk score intelligence and threat mitigation https://patents.google.com/patent/US9324119B2 | identity 및 asset의 risk score/trend를 계산하여 threat mitigation에 활용한다. |
| R25 | US 2018/0285839 A1, Data provenance, permissioning, compliance, and access control using immutable ledger overlay network https://patents.google.com/patent/US20180285839A1/en | 데이터 저장 시스템에 immutable ledger overlay network를 이용해 provenance, permissioning, compliance, access control을 제공한다. |