

PRIDE, PASSION, VISION

PRECURSOR AIS-POTAL

I 제품 소개서

I 제품 개요

AI 도구 접근 통제, 더 안전하게 더 지능적으로

AIS-POTAL (Precursor AI Security) 는 기업의 계정·권한 관리 체계를 기반으로, AI 에이전트가 사용하는 MCP 서버와 Tool에 대한 접근을 통제하고 호출을 탐지·필터링하는 솔루션입니다. 프리커서의 오랜 IAM 구축 경험을 바탕으로 보안성과 운영 효율성을 극대화하여 개발되었습니다.

AI 도구 권한 발급 속도 향상

MCP 서버·Tool 권한 발급 프로세스 자동화로 업무 지연 없이 신속한 처리 가능
사용자 자신의 도구 권한 목록의 명확한 확인으로 관리 효율성 증가
관리자 개입 없이도 사전 승인된 도구 권한 요청 건 자동 처리



HR 연동을 통한 자동화

직원 퇴사 및 휴직 시 계정·권한과 AI 도구 권한 자동 회수로 보안 강화
임시직 및 협력직의 도구 접근 권한 체계적 관리로 불필요한 권한 남용 방지



AI 호출 탐지·필터링으로 위협 차단

프롬프트 인젝션 탐지와 금지어·허용어·스크립트 기반 필터링으로 오·남용 차단
요청·응답 검사로 민감정보 노출을 사전에 방지

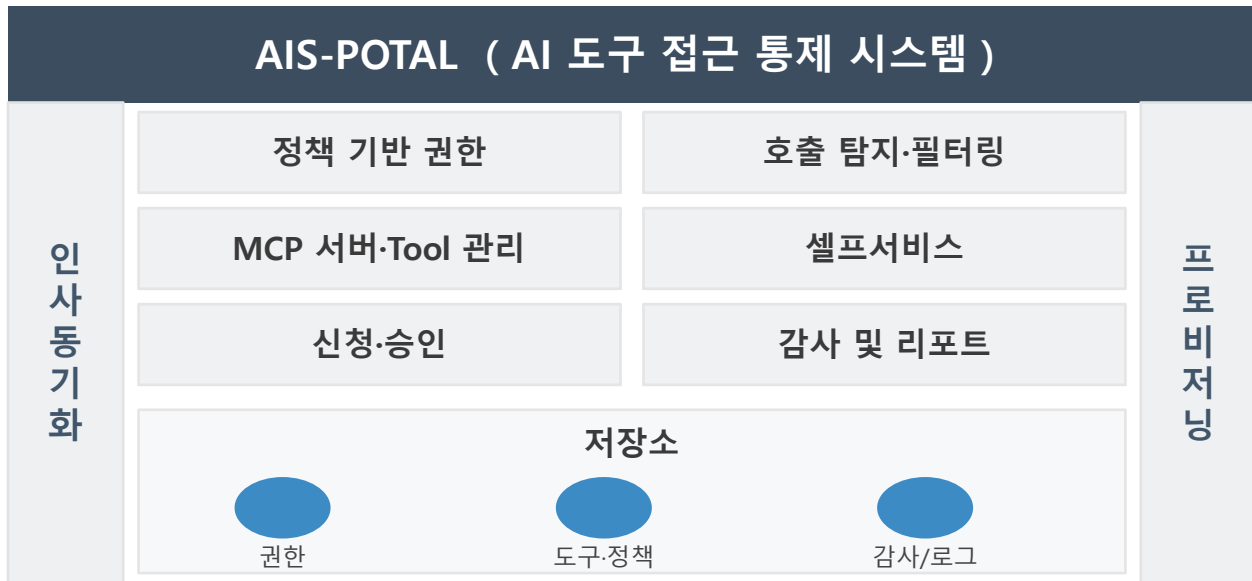


감사 대응력 및 보안성 강화

AI 도구 호출 현황을 실시간으로 모니터링하여 보안 위협을 사전에 방지
계정·권한 및 도구 호출 이력을 체계적으로 기록하여 감사 대응 및 보안 관리 용이



I 주요 기능



인사동기화

HR시스템에서 관리되는 사용자 정보(입사, 이동, 승진, 퇴사 등) 및 조직 정보를 동기화하여 계정·권한을 자동 관리

정책 기반 권한

RBAC 기반으로 사용자그룹·권한그룹을 정의하고 조직·직무·직급 조건에 따라 도구 권한을 자동 부여·회수

MCP 서버·Tool 관리

사내외 MCP 서버와 Tool을 카탈로그로 등록·분류하고 서버·Tool 단위 접근 권한을 관리

신청·승인

사용자·사용자그룹 단위로 도구 권한을 신청하면 다단계 승인 절차를 거쳐 자동 반영

호출 탐지·필터링

AI가 MCP Tool을 호출할 때 요청·응답을 검사하고 프롬프트 인젝션·금지어·스크립트 정책으로 필터링

감사 및 리포트

계정·권한과 AI 도구 호출(허용·차단·필터링) 내역을 분석하여 다양한 감사 보고서 제공

셀프서비스

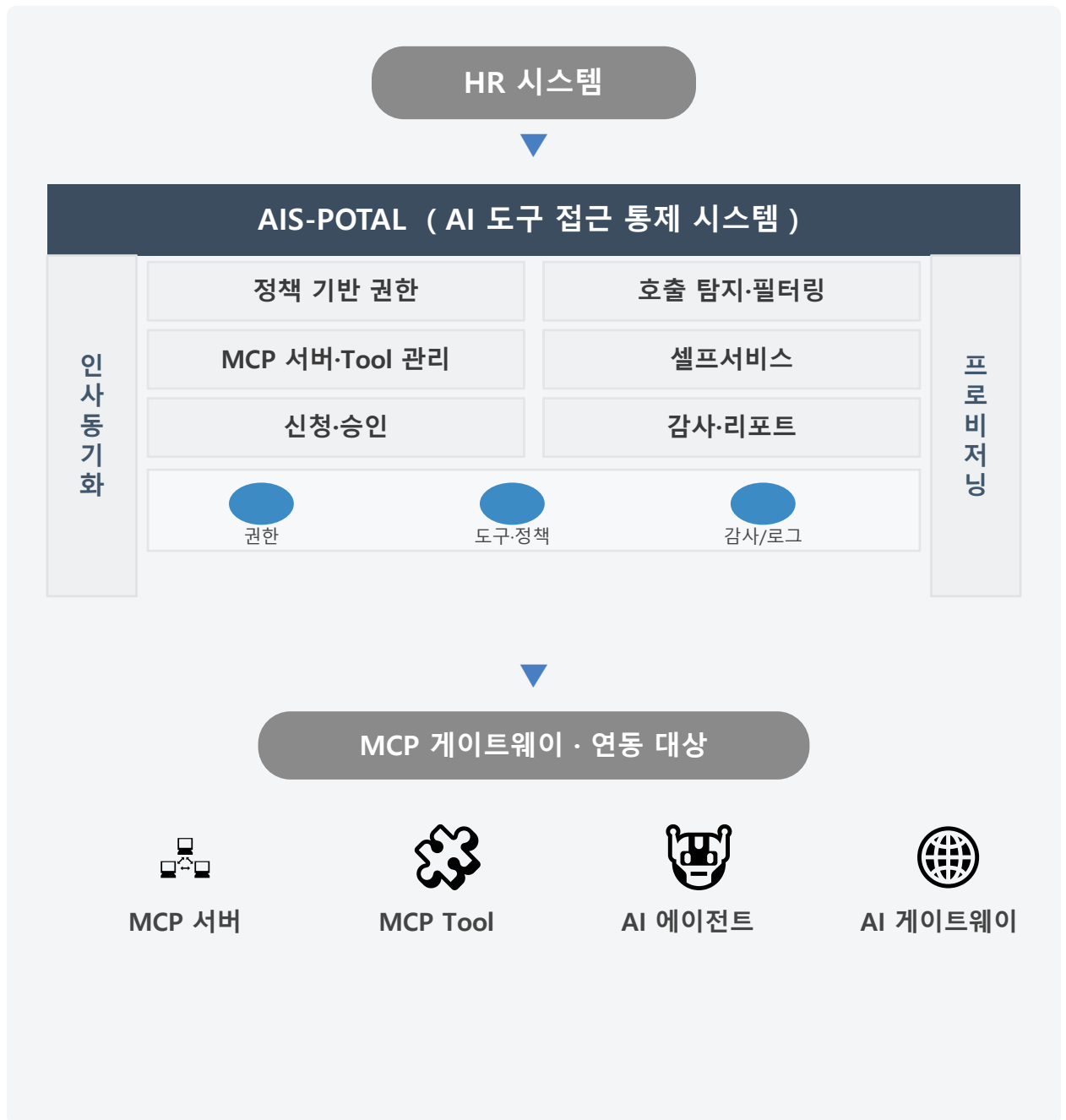
사용자가 스스로 도구 권한 신청·회수, 개인 자격증명 등록 및 도구 권한을 손쉽게 관리

프로비저닝

승인된 도구 권한·정책을 AI 게이트웨이에 실시간 또는 배치 방식으로 자동 반영

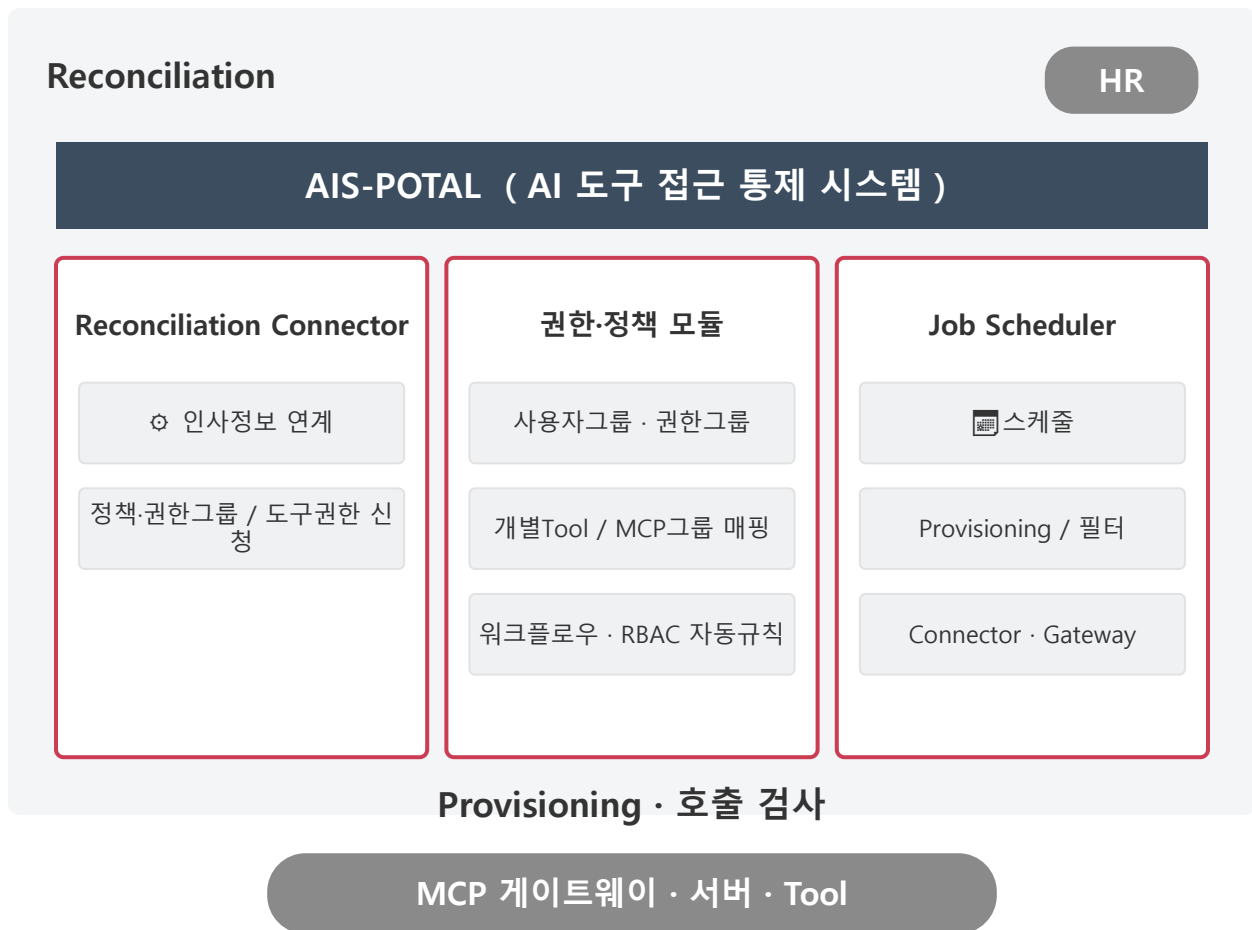
I 전체 구성도

AIS-POTAL는 크게 **외부시스템과 연동**과 **내부 관리** 영역으로 구성됩니다. 외부 연동은 HR 시스템과의 인사정보 동기화 및 MCP 게이트웨이로의 프로비저닝·호출 검사를 포함하며, 내부 관리 는 권한 정책, 신청·승인, 호출 탐지·필터링, 감사 및 리포트 등으로 구성됩니다.



I 논리 구성도

AIS-POTAL는 HR 및 MCP 게이트웨이와 연동하여 AI 도구 권한을 체계적으로 관리합니다. **인사 정보 검증 및 동기화**, UI Console을 활용한 **신청·승인**, 스케줄 기반 **RBAC 자동규칙** 적용 및 **권한 동기화**, 실시간 **Provisioning**과 **호출 탐지·필터링**을 통해 자동화된 도구 통제를 지원합니다.



I 기능 상세 01

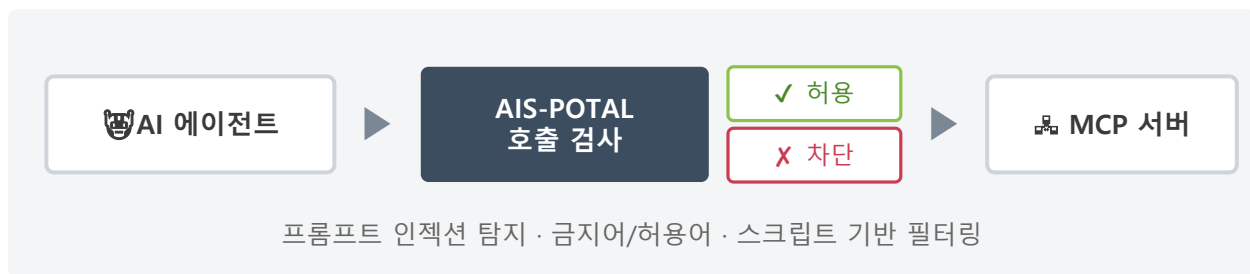
라이프사이클 관리.

HR 시스템에서 인사발령 정보를 동기화하고, 설정된 RBAC 기반 자동 규칙에 따라 MCP 게이트웨이에 도구 권한을 자동 프로비저닝합니다. 또한, 사용자가 도구 권한을 신청하고 결재가 승인되면 해당 권한이 게이트웨이에 자동 반영됩니다.



호출 탐지·필터링.

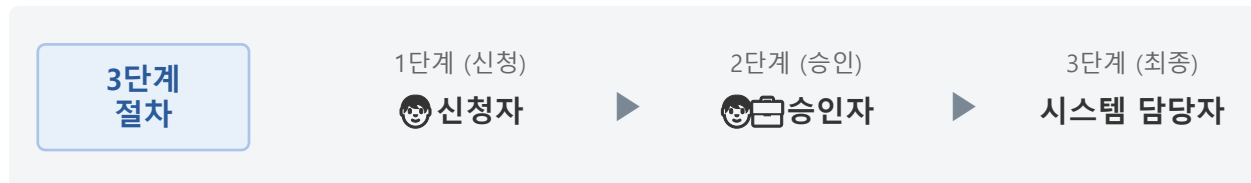
AI 에이전트가 MCP Tool을 호출하는 시점에 사용자 권한을 검증하고, 프롬프트 인젝션 탐지·금지어·허용어·스크립트 기반 정책으로 요청과 응답을 검사하여 허용 또는 차단합니다.



I 기능 상세 02

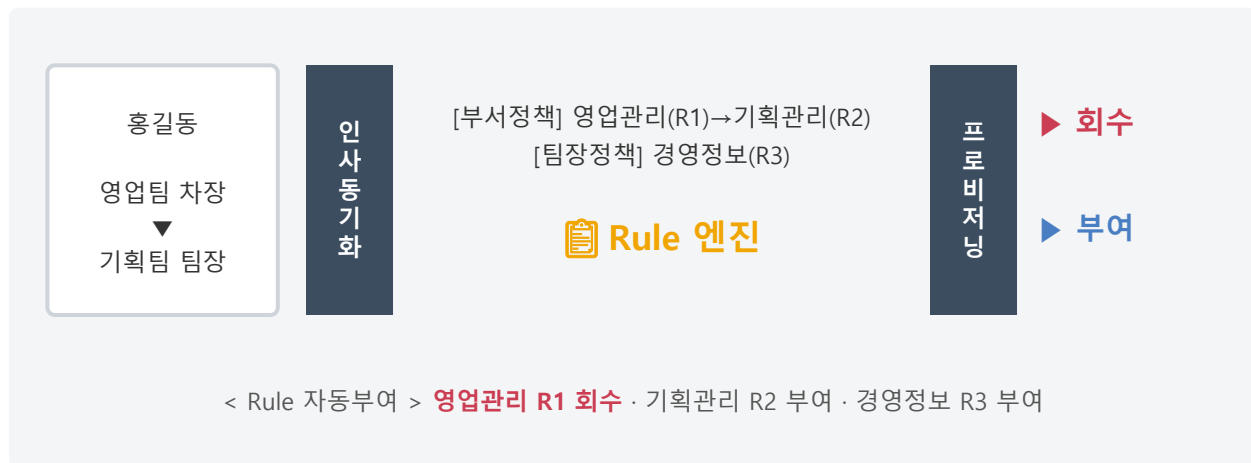
워크플로우.

사용자는 도구 권한의 신청, 회수 등 여러 업무를 하나의 워크플로우에서 처리할 수 있으며, 신청 → 승인 → 최종 승인 3단계 절차를 거쳐 자동 반영됩니다. 또한, 복수의 도구 권한을 여러 사용자에게 동시에 부여할 수 있어 효율성과 편리성을 제공합니다.



Rule 관리.

RBAC(역할 기반 접근 제어) 통제 기능을 구현하여, 기업의 조직·직무·직책 등에 따라 사용자가 해당 조건을 충족하면 별도의 신청 없이 자동으로 도구 권한이 부여되거나 회수됩니다.



I 기능 상세 03

외부 도구. 자격증명.

GitHub 등 외부 MCP 서버 이용 시, 각 사용자가 "내 연결" 화면에서 개인 자격증명(개인 키·토큰)을 등록하면 해당 사용자의 호출에 자동으로 실려 나갑니다. 관리자는 서버 등록 시 백엔드 인증 방식만 정의하고, 실제 키는 사용자별로 안전하게 관리됩니다.



사용자

AIS-POTAL
내 연결



백엔드 인증
토큰 치환



외부 MCP
(GitHub 등)

외부 도구 등록 및 개인 자격증명 발급 완료 시 해당 MCP 서버 접근 가능

감사/통제.

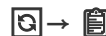
전사 차원에서 모든 사용자 유형(정규직, 임시직, 협력직 등)에 대해 어떤 MCP 서버·Tool에 접근 권한을 가지고 있는지, 그리고 실제 호출 내역을 감사 및 통제할 수 있습니다.

외부 도구·자격증명의 체계적인 관리

RBAC·정책 기반 접근 제어로 오·남용 원천 차단

불필요한 도구 권한을 식별하고 제거

호출 이력 관리로 책임 추적성 확보



라이프사이클 · Rule 엔진



3단계 승인 워크플로우



도구 호출 감사 및 리포트

감사합니다

전화 문의 | 010-6668-0101

제품 문의 | sales@precursor.co.kr

홈페이지 | precursor.co.kr