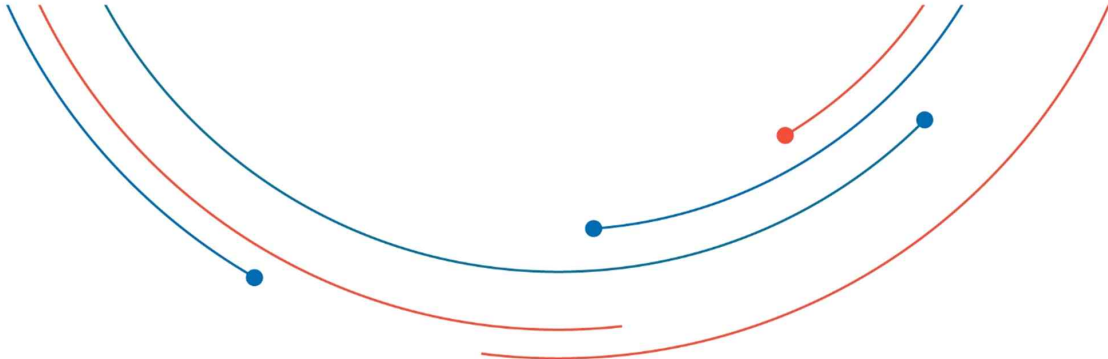




AI.GOV 이슈리포트 2025-2호

공공부문 MCP 도입의 이해와 활용



NIA 한국지능정보원

일러두기 NOTE

「AI.GOV 이슈리포트」는 공공부문의 인공지능 전환 및 디지털정부와 관련된 다양한 이슈를 분석하고 향후 정책 방향을 모색하기 위해 한국지능정보사회진흥원에서 기획하여 발간하는 보고서입니다.

한국지능정보사회진흥원의 사전 승인 없이 본 보고서의 무단전재나 복제를 금하며, 가공·인용할 때는 반드시 출처를 명시하여 주시기 바랍니다.

본 보고서의 내용은 한국지능정보사회진흥원의 공식 견해와 다를 수 있으며, 문의 및 제안은 아래 연락처로 문의해주시기 바랍니다.

- 발행처: 한국지능정보사회진흥원
- 발행인: 황종성
- 작성자: 한국지능정보사회진흥원 김찬우 책임, 이원혁 책임, 윤명근 선임, 윤지영 주임, 강서진 연구원
- 기 획: 한국지능정보사회진흥원 정부만 본부장, 박선주 팀장, 김태원 팀장, 김동희 팀장
- 보고서 온라인 서비스: www.nia.or.kr

목 차 CONTENTS

I. MCP의 기술적 이해	4
1. MCP란?	4
2. MCP의 기술 구조	7
3. MCP 관련 기술적 이슈 사항	10
II. 해외 활용사례 : MCP가 만드는 업무 혁신	11
1. 글로벌 기업의 MCP 도입 확산과 산업별 활용 사례	11
III. 공공부문 MCP 도입 및 적용 방안	14
1. MCP 공공분야 도입의 기술·제도적 제약	14
2. 정부 및 공공부문 적용 시 고려사항	17
3. 적용방안(1): MCP 파일럿 및 테스트 공간 ‘APT(Agent Pilot and Test)’ 마련	22
4. 적용방안(2): MCP 공작소	24
5. 적용방안(3): 공공 서비스 제안	26
6. 공공부문 MCP 적용 전략과 제언	28
참고문헌	30

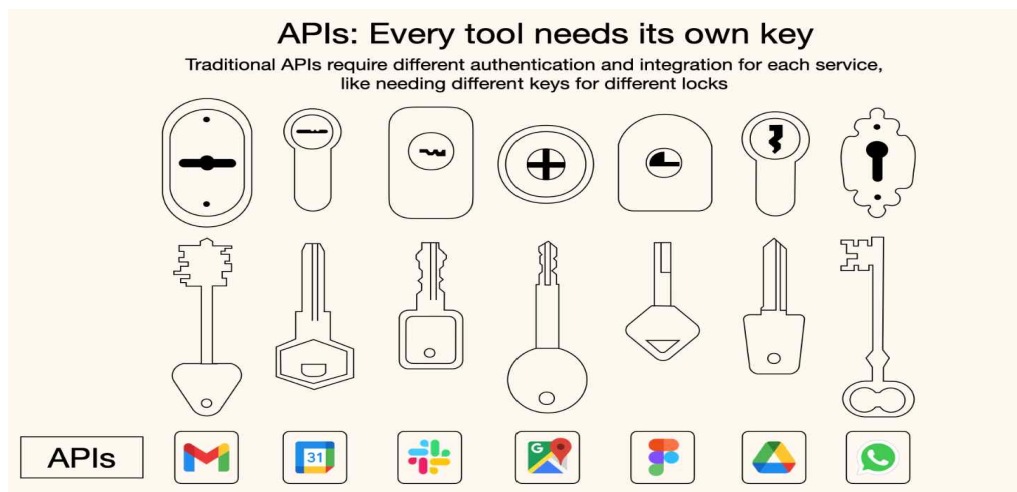
I MCP의 기술적 이해

1 MCP란?

□ MCP(Model Context Protocol), AI와 외부 도구를 연결하는 새로운 표준

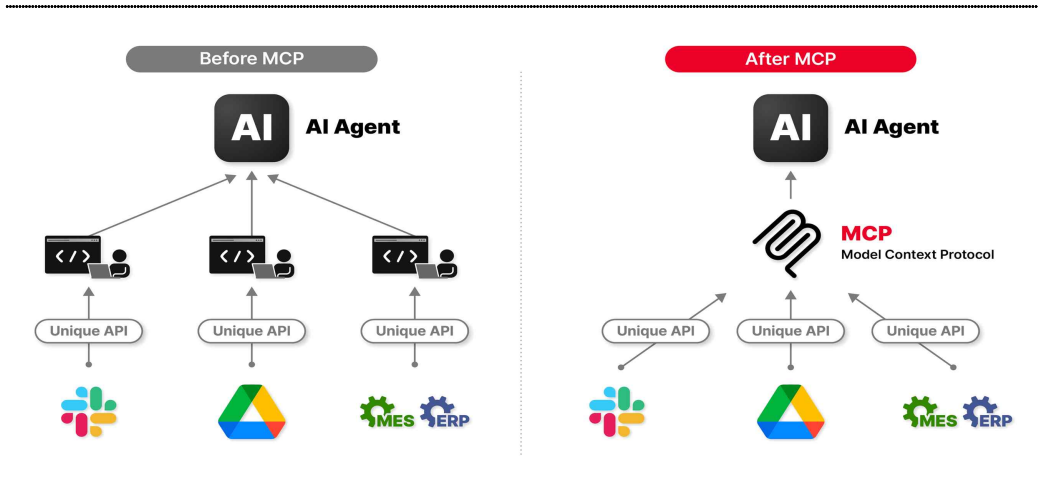
- AI 활용이 확대됨에 따라 데이터 소스와 외부 도구 간의 구조적 연계 필요성이 부각되며, 기존의 API연계 방식의 한계를 넘어서는 새로운 대안의 필요성 증대
- 현재 AI와 외부 도구를 연결하는 표준화된 방식이 부재해, 개발자들은 특정 AI 서비스와 외부 API를 일대일로 연결하는 코드를 직접 작성
- ※ 예) AI Agent를 통해 메일 작성이나 캘린더 등록 등의 작업을 수행할 때, AI와 메일 애플리케이션을 연결하기 위해 개별 API 수정·변경 작업 필요

| 기존의 API 연결 방식 (출처: Anthropic) |



- Anthropic은 '24.12. AI 에이전트가 외부 데이터 및 도구와 통합적으로 상호작용할 수 있는 표준화된 방식을 제공하기 위해 MCP를 최초 발표
- MCP(Model Context Protocol)는 애플리케이션이 대규모 언어모델(LLM)에 컨텍스트(context)를 제공하는 방식을 표준화한 개방형 프로토콜^{*1)}로써,
 - * 프로토콜: 컴퓨터나 통신 장비 간 데이터를 주고받는 방식을 규정한 규칙의 집합
- AI가 보다 정확하고 효율적인 답변을 제시할 수 있도록 각 API를 AI에 맞게 일일이 수정해야 하는 번거로움을 해소하고 효율적인 답변을 유도

| MCP(Model Context Protocol) 도입 전·후 비교 (출처: AHHA LABS) |



- (도입 前) MCP 없이 AI 애플리케이션을 개발할 경우, 특정 데이터베이스나 파일 시스템에 접근하기 위해 각기 다른 API나 라이브러리를 사용
- (도입 後) MCP를 활용하면 다양한 데이터 소스에 대한 접근을 한 번에 표준화 할 수 있어 확장성과 상호운용성을 갖춘 AI 솔루션 구축 가능

| MCP vs. 기존 API 방식 비교 |

기능	역할(내용)	기존 API 방식
통합 노력	한 번의 MCP 통합으로 여러 도구 연결 가능	각 API별로 개별 통합 필요
실시간 데이터 검색	가능	불가능
양방향 통신 지원	가능	요청·응답 방식만 가능
유지보수	상대적으로 간편	API별 개별 유지보수 필요
보안 및 접근 제어	표준화된 방식 적용 가능	API마다 별도 설정 필요

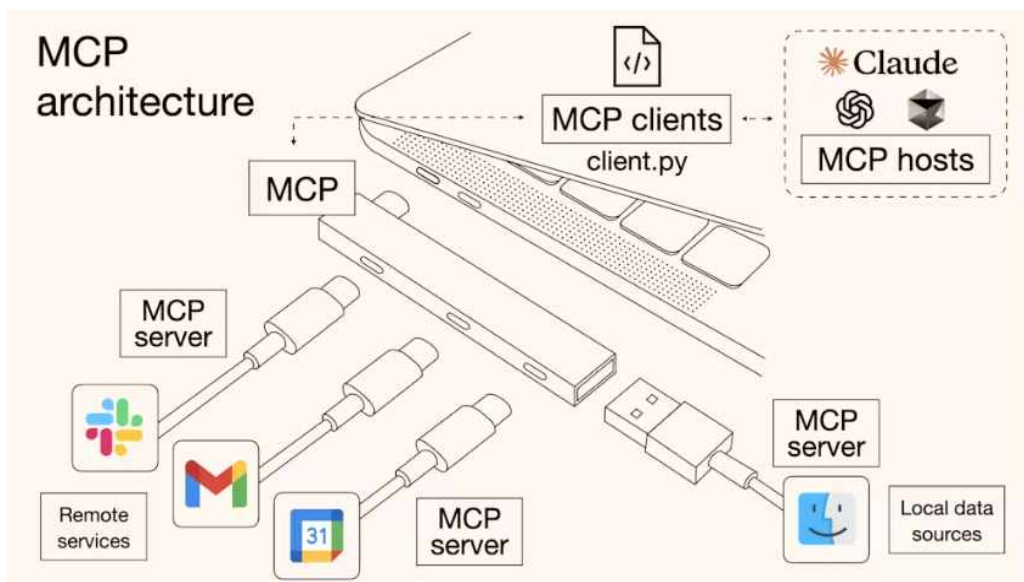
□ Anthropic에서 설명하는 MCP

- Anthropic이 제시한 MCP는 AI 애플리케이션을 외부 시스템에 연결하기 위한 오픈소스 표준 프로토콜로 정의하며,
 - MCP는 AI 어시스턴트가 콘텐츠 저장소, 비즈니스 도구 등 다양한 데이터가 위치한 시스템과 연결될 수 있도록 하는 새로운 표준
 - 각 데이터 소스마다 별도 커스텀 커넥터를 유지하는 대신, 개발자는 단일 표준 프로

토콜을 기반으로 구축할 수 있어 보다 정확한 응답 생성

- MCP를 사용하면 Claude나 ChatGPT 같은 AI 애플리케이션이 데이터 소스(로컬 파일, 데이터베이스), 도구(검색 엔진, 계산기), 워크플로우 시스템 등에 손쉽게 연결 가능하도록 지원
- MCP는 AI 애플리케이션을 위한 'USB-C 포트'와 같은 표준화 역할 수행
USB-C가 전자기기를 연결하는 표준화된 방식을 제공하듯, MCP 역시 AI 애플리케이션을 외부 시스템에 연결하는 표준화된 통합 방법을 제시

| USB-C 포트와 비슷한 MCP (출처: Anthropic) |



- MCP는 개발 도구 생태계 전반에서 프로그래밍 언어 지원 방식을 표준화한 LSP(Language Server Protocol)에서 영감을 받아 개발되었으며,
- LSP가 '하나의 언어 서버 모든 에디터에서 사용 가능'하게 만든 것처럼, MCP는 '하나의 데이터·도구 서버를 모든 AI 애플리케이션에서 사용 가능'하게 함으로써 NxM 문제를 해결

2 MCP의 기술 구조

□ MCP는 Host-Client-Server 구조로 AI와 외부 도구 간 상호운용성을 표준화

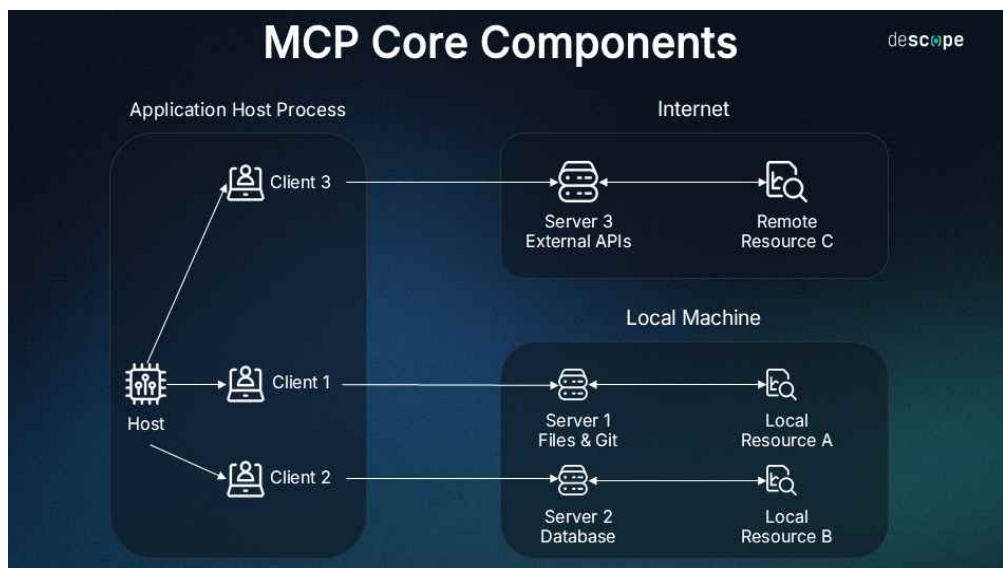
- MCP는 호스트(Host), 클라이언트(Client), 서버(Server)로 구성되어 있으며, MCP 호스트(예: Claude Code, Claude Desktop 등 AI 애플리케이션)가 하나 이상의 MCP 서버에 연결을 설정하는 방식으로 동작

| MCP 구성 요소별 상세 내용 |

구분	역할(내용)	예시
호스트 (Host)	MCP를 통해 데이터를 사용하는 메인 프로그램(AI 애플리케이션)	Claude Desktop, IDE, AI 도구 등
클라이언트 (Client)	MCP 서버와의 연결을 유지하며, MCP 호스트가 사용할 수 있도록 컨텍스트를 가져오는 중간 구성 요소	Claude Agent, IDE 내부의 연결 모듈 등
서버 (Server)	MCP 클라이언트에 컨텍스트를 제공하는 프로그램	파일 서버, 데이터베이스 서버, 번역 서버 등

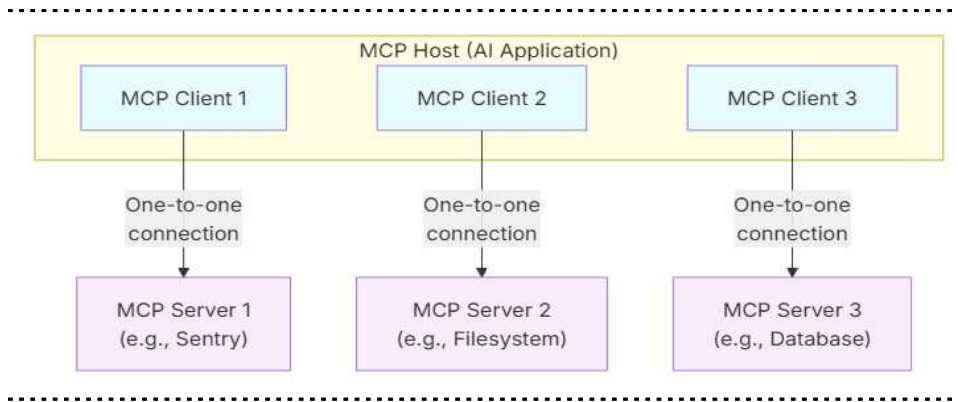
- MCP 호스트는 각 MCP 서버마다 하나의 MCP 클라이언트를 생성하여 통신을 수행하며, MCP 클라이언트는 해당 MCP 서버와 일대일 연결을 유지

| MCP 핵심 구성요소 (출처: descope) |



- MCP 호스트(ex. Visual Studio Code)가 MCP 서버(ex. Sentry MCP 서버)에 연결되면, MCP 호스트는 해당 서버와의 연결을 유지하는 MCP 클라이언트 객체를 생성

| MCP 아키텍처(Host, Client, Server) (출처: Anthropic) |



- MCP 호스트(Host)는 LLM 또는 Agent로서 외부 툴 활용을 지시
 - 사용자의 요청을 받아 분석한 뒤, 특정 작업을 수행하기 위해 외부 툴의 도움이 필요하다고 판단되면 MCP 클라이언트를 통해 해당 툴 서버에 요청을 지시
- MCP 서버(Server)는 도메인별 기능을 캡슐화해 AI 애플리케이션과 연결하는 역할 수행
 - MCP 서버는 표준화된 프로토콜 인터페이스를 통해 AI 애플리케이션에 특정 기능을 제공하는 프로그램으로, 각 서버는 특정 도메인에 특화된 기능을 수행
 - 서버는 클라이언트로부터 MCP 규격에 따른 요청을 수신해 해당 툴을 실행하고, 그 결과를 다시 클라이언트에게 전달

| MCP 서버 핵심기능|

- ① (Tools) LLM이 특정 작업(DB조회, 메일 전송 등)을 수행할 수 있도록 지원하는 기능
- ② (Resources) LLM이 참조할 수 있는 외부 컨텍스트(텍스트, 로그, DB스키마 등) 제공
- ③ (Prompts) LLM과 상호작용하기 위해 사전 정의된 입력 템플릿

- MCP 클라이언트(Client)는 서버와 일대일 연결을 유지하며, 서버로부터 받은 컨텍스트를 호스트가 활용할 수 있도록 전달

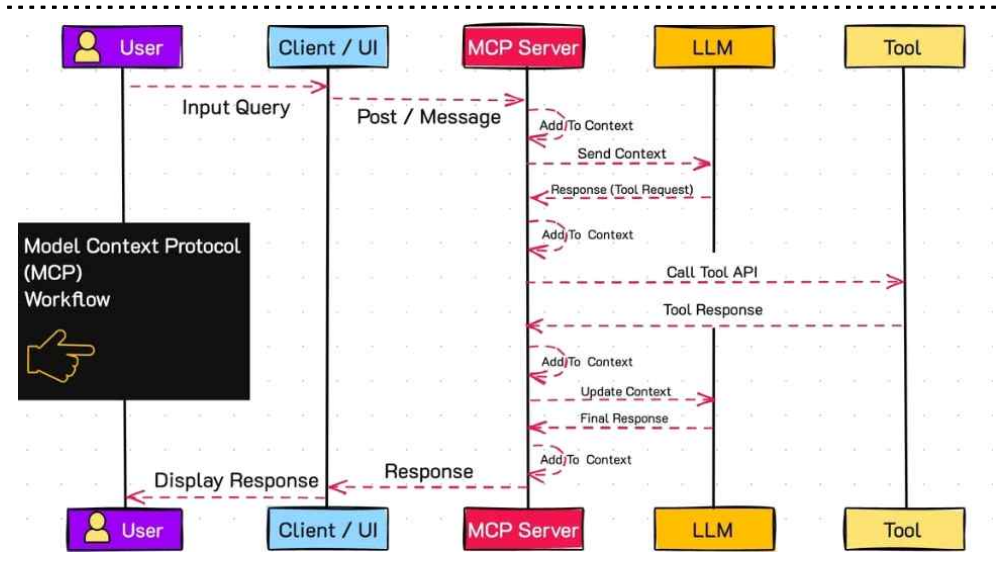
- 클라이언트는 AI가 다양한 도구나 서비스를 사용할 수 있도록 요청을 보내는 역할을 수행

| MCP 클라이언트 핵심 기능 |

- ① (Sampling) MCP 서버가 직접 LLM에 접근하지 않고, MCP 클라이언트를 통해 LLM에 요청과 응답을 처리하는 방식으로 API 없이도 안전하게 LLM 활용 가능
- ② (Root) MCP 서버가 접근할 수 있는 디렉토리의 범위를 정의. 서버는 지정된 Root 아래의 파일만 탐색할 수 있으며, 보안상의 이유로 전체 파일 접근은 제한
- ③ (Elicitation) MCP 서버는 툴 실행 시 모든 입력값을 사전에 받지 않고, 실행 도중 필요한 정보를 대화형으로 확보

- MCP는 표준 메시지 체계를 기반으로 AI와 외부 도구 간 상호작용 절차를 규정
- MCP의 모든 통신은 JSON-RPC 2.0을 기본 메시지 표준을 사용하며, 요청·응답·알림에 대한 표준화된 구조 제공

| MCP User-Client-Server-LLM-Tool 간의 동작 흐름(Work flow) (출처:Medium) |



3 MCP 관련 기술적 이슈 사항

□ MCP 생태계 전반에서 여러 보안 취약점이 확인되었으나 대응은 미흡

| MCP 관련 취약점 사례 및 대응 현황 |

구분	발견 주체	주요 내용	조치 현황
Cursor 원격 코드 실행(RCE) 보안 이슈	Check Point Research	MCP 설정 파일 변경 시 재검증 절차가 없어, 악성 MCP 서버 등록을 통해 원격 코드 실행(RCE) 가능	Cursor가 패치(버전 1.3) 배포('25.7.16.) → MCP 구성 파일 변경 시마다 사용자 승인 절차를 요구하도록 개선
mcp-remote 원격 코드 실행 (RCE) (CVE-2025-6514) 보안 이슈	JFrog 보안팀	신뢰할 수 없는 MCP 서버에 연결할 때, MCP 클라이언트가 원격 MCP 서버와 통신할 수 있는 도구 (mcp-remote)를 통해 공격자가 원격으로 임의의 OS 명령 실행 가능	취약점 공개 직후, mcp-remote 개발팀이 패치(버전 0.1.16) 배포('25.7.9.)
NeighborJack 취약점 및 OS 코드 삽입 이슈	Backslash Security	일부 MCP 서버가 0.0.0.0에 바인딩 되어 인터넷에 노출됨에 따라, NeighborJack 및 OS 코드 삽입 취약점이 발견되어 네트워크 공격자가 인증 없이 시스템을 장악할 수 있는 위험 가능성	연구기관에서 취약점 경고를 발표했으나 MCP 전반에 대한 표준화된 대응책 및 보안 업데이트는 부재
운영·보안 위험 (6대 공격 벡터)	Docker 분석팀	다수 MCP 서버를 분석한 결과, OAuth 취약점, 명령 주입, 무제한 네트워크 접속, 파일 시스템 노출, 토큰 포이즈닝, 자격 증명 탈취 등 다수의 공격 벡터 존재	Docker가 보안 권고 발표 → MCP 운영자·사용자에게 보안 점검 및 강화 권고, 표준 패치나 일괄 대응책은 아직 없음
대규모 MCP 서버 보안 취약점	Palo Alto Networks	악의적 MCP 서버 모방, 동의 피로 (Consent Fatigue), 런타임 격리 부족, 인증 및 자격 증명 관리 부재 등 심각한 보안 리스크 존재	Palo Alto의 위협 인텔리전스 보고서 발표 및 업계 경고 → 보안 아키텍처 개선 권고는 있었으나, 실제 MCP 서버 전반의 구조적 개선은 진행 중

II 해외 활용 사례 : MCP가 만드는 업무 혁신

1 글로벌 기업의 MCP 도입 확산과 산업별 활용 사례

□ Bloomberg: 금융 정보의 신속한 처리와 분석³⁾

- (MCP 표준 연결 규격 도입) Bloomberg는 AI 에이전트가 필요한 기능을 손쉽게 연결할 수 있도록 MCP 표준 연결 규격 도입

기존	개선
새로운 기능을 개발할 때마다 각 시스템과의 개별 연결 필요	MCP 도입으로 개발 시간이 몇 달에서 몇 주로 단축

- (Document Search & Analysis 성공 사례) 금융 전문가들이 방대한 시장 보고서와 뉴스를 실시간 검색 및 요약 가능
 - 최근 반도체 산업 동향 분석 시 Bloomberg 터미널의 뉴스 데이터, 주가 정보, 재무 보고서, 업계 리포트를 동시에 연결해 5분 만에 종합 분석 보고서 생성
 - (조직 전체 개발 문화 혁신) 수백 명의 AI 연구자와 엔지니어가 개발한 도구들을 MCP 표준 규격으로 공유함으로써, 레고 블록 조립 방식으로 신속하게 새로운 서비스 구성 가능
 - 기존 팀별 독립 개발 ‘사일로’ 구조에서 협업 중심의 혁신 생태계로 전환
 - (엔터프라이즈급 보안과 감사 체계) 신원 인지 미들웨어(Identity-aware middleware)를 구축해 모든 AI 도구 호출을 중앙에서 통제
 - SSO(Single Sign-On) 프록시로 사용자 신원 확인 및 권한 부여, 민감한 금융 데이터 접근 전 적절한 권한 검증 등
 - API 키나 인증 토큰 등의 민감 정보는 개발자 컴퓨터에 저장되지 않도록 보안 정보 관리(호텔 키카드 방식으로 체크아웃 시 자동 무효화)
- ※ 모든 인증 정보는 중앙 서버에서 관리하며 필요 시에만 임시 발급

| 구체적 보안 시나리오 |

애널리스트의 고객 포트폴리오 데이터 접근 시:

사용자 신원 확인 → 접근 권한 검증 → 데이터 민감도 평가 → 고위험 데이터는 추가 승인 요구 또는 접근 제한 적용

※ 모든 과정이 자동으로 로그 기록되어 감사 가능

□ Intercom: 고객 상담의 혁신적 자동화⁴⁾

○ (AI 상담원 'Fin') 자동 해결률과 응답 시간의 혁신은 물론, 다국어 지원까지 갖춰 단순한 FAQ 응답을 넘어 복잡한 고객 문의도 실시간 해결

- 평균 51%의 고객 문의를 완전 자동으로 해결, 일부 고객사는 최대 86%까지 자동 해결률을 기록(Anthropic)

- 사람 상담원이 몇 분에서 몇 시간 걸리는 문의를 수초 내 해결하며, 45개 언어를 지원해 다국어 응대도 자동화

※ 예: 지난달 결제 내역 확인 요청에 Fin이 곧바로 결제 시스템에 접속하여 거래 내역 조회·정리해 제공

○ (노코드 설계) 전문 개발 지식이 없는 비개발자도 시각적 인터페이스와 직관적 설정을 통해 손쉽게 활용할 수 있도록 지원하며, 데이터 연계(Data Connectors)와 업무 자동화(Fin Tasks) 등의 기능으로 반복 작업을 간소화

- 비즈니스 담당자는 웹 브라우저에서 간단한 설정 화면을 통해 외부 시스템 연결

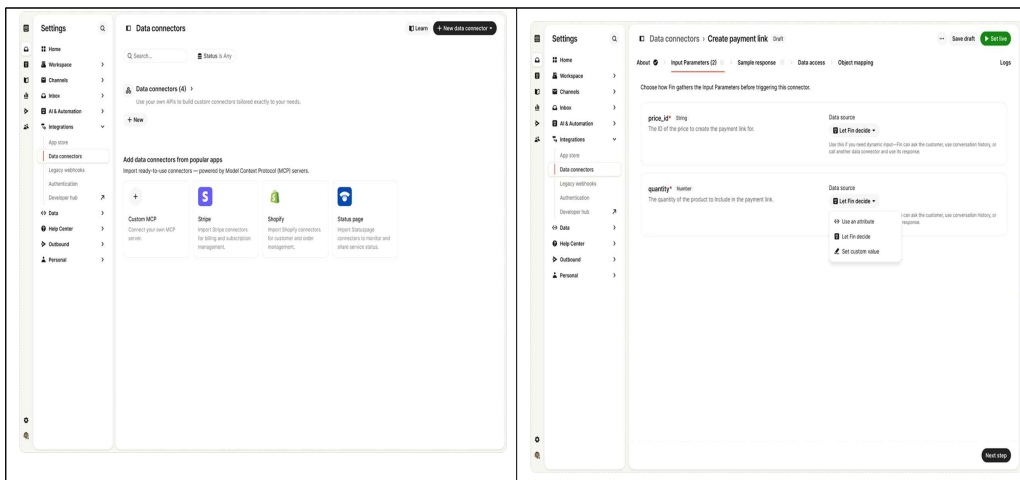
기존	개선
개발자가 API 연동 작업에 며칠씩 소요	비즈니스 담당자가 직접 10분 만에 설정 완료

※ 지원 시스템: Stripe(결제), Shopify(전자상거래), Linear(프로젝트 관리) 등

- 복잡한 업무 흐름을 시각적으로 설계할 수 있으며, 각 단계마다 조건과 승인 절차 설정 가능

※ 예: 환불 요청 → 주문 내역 확인 → 환불 조건 검토 → 관리자 승인 → 자동 환불 처리의 전체 과정을 한눈에 구성 가능

| Data Connectors 및 Fin Task 화면 (출처: Intercom) |



□ PayPal & Stripe: 결제와 금융 서비스의 완전 자동화⁵⁾

- (PayPal) PayPal은 MCP 서버를 통해 주문 생성, 결제 처리, 인보이스 발행·전송·리마인드·취소·QR코드 생성 등 상거래 전 생명주기 기능을 지원
 - 예를 들어, 온라인 교육 플랫폼에서 수강생이 “강의 연장하고 싶어요” 요청 → AI 에이전트가 PayPal MCP를 통해 현재 수강 상태 확인 → 연장 가격 계산 → 결제 링크 생성 → 고객 전송 → 결제 완료 시 자동으로 수강 기간 연장 및 확인 이메일 발송
- (Stripe) Stripe는 PayPal보다 한 단계 진화한 형태로, Agent Toolkit 기능을 통해 결제 링크 생성, 사용량 기반 과금, 가상카드 발급(Issuing)등 금융 기능 제공
 - 예를 들어, 사용량 기반 과금시 “이번 달 API 호출량이 1만 건이니까 사용료를 자동으로 계산해서 청구해줘” 요청 → Stripe가 실시간 사용량을 추적하고 요금을 계산하여 자동 청구⁶⁾
- PayPal과 Stripe는 개발부터 운영까지 일관된 경험을 제공하며, 로컬-리모트 환경 동일성과 보안 안전장치를 통해 사고 최소화
 - (로컬-리모트 동일성) USB-C 표준이 어떤 기기에서든 동일하게 작동하듯, 개발자 컴퓨터에서 테스트한 기능이 실제 서비스 환경에서도 동일하게 작동
 - (보안 안전장치) Stripe는 ‘제한된 API 키(Restricted Keys)’ 사용을 권장하고, 기능별로 최소한의 권한만 부여하는 ‘최소 권한 원칙’과 은행 카드 일별 한도 설정 등을 통해 보안 사고 발생 시 피해 범위를 최소화

□ Atlassian & Microsoft: 업무 협업의 새로운 표준⁷⁾

- (Atlassian) 원격 MCP 서버 통합을 통해 Jira, Confluence, Compass를 하나의 플랫폼으로 연결하여 회의 노트부터 업무 티켓까지 자동으로 생성
 - ※ 예: 프로젝트 회의 종료 → AI가 회의록을 분석하여 액션 아이템 식별 → 자동 Jira 티켓 생성 → Confluence에 관련 문서 정리 → Compass에서 프로젝트 로드맵 업데이트
 - (대량 작업 처리) 정책 변경으로 관련 문서를 100개를 업데이트해야 할 경우, AI가 개인정보보호 정책 변경과 관련된 문서를 자동으로 식별해 일괄 업데이트를 수행
- (Microsoft) Microsoft Graph MCP를 통해 이메일, 일정, 파일, 연락처를 하나의 흐름으로 연결해 ‘컨텍스트 스위칭(Context Switching)’* 없는 업무 환경 구현
 - * 컨텍스트 스위칭: 업무를 위해 여러 애플리케이션을 오가며 발생하는 시간 낭비와 집중력 저하를 의미
 - (업무 연계 시나리오) 민원 관련 이메일 도착 → OneDrive에 첨부 파일 자동 저장

→ 관련 부서 회의 일정 설정 → 관계자들에게 초대장 발송까지 한 번의 자연어 명령으로 실행

- (협업 극대화) 기획팀에서 프로젝트 제안서를 개발팀으로 이관할 때, AI가 관련 회의록·참고 자료·이해관계자 연락처 등 모든 관련 정보를 자동 정리해 전달하여 부서 간 협업 속도 향상

※ 개발팀 담당자는 별도 정보 수집 과정 없이 즉시 업무 착수 가능

III 공공부문 MCP 도입 및 적용 방안

1 MCP 공공분야 도입의 기술·제도적 제약

□ 보안 : 새로운 기술과 오래된 리스크

○ Wiz, Microsoft, Red Hat 등 주요 전문 기업 조사에 따르면, 악성코드(CVE-2025-6514)를 통한 원격 코드 실행(RCE) 등 보안 취약점 발견^{25.3. 기준}

- MCP를 도입하면 기존 공공서비스의 폐쇄적 환경보다 연결 지점(인터페이스, API, 외부 AI 연계 등)이 급격히 늘어나며, 이에 따른 취약점 확대는 필연적

※ 기존 공공서비스는 중앙집권적 토큰 방식을 사용하므로, MCP 서버가 해킹될 경우 저장된 OAuth 토큰이 탈취되어 대규모 피해로 확산할 수 있는 보안 위험이 존재

○ 국내에서는 아직 MCP와 관련한 보안에 대한 논의가 활발하지 않으나, 보안위험에 대한 정책적 대비는 필요한 시점

- AWS와 A2RS 연구소는 “MCP 기업(산업) 적용을 위한 보안: 프레임워크와 대응전략⁸⁾” 논문을 통해 MCP 환경에서 새롭게 등장할 수 있는 위험을 6가지로 정리

- MCP는 다양한 서버에서 도구를 손쉽게 불러오도록 설계되어 있으므로, 인증 절차가 미흡할 경우 악용될 수 있음

※ (예시) 동일한 도구 목록과 설명을 담은 메니페스트를 제공하면 모델은 이를 진짜로 오인해 가짜 서버에서 도구를 실행하고, 이로 인해 정보 탈취 및 명령어 변조 등 가능

| MCP 보안 위협과 대응 방안 (출처: 「MCP 기업(산업) 적용을 위한 보안」) |

보안 위협 종류	내용
도구 오염(Tool Poisoning)	도구 설명이나 매개변수를 조작해 AI가 의도치 않은 동작을 수행하도록 유도하는 공격

데이터 유출(Data Exfiltration)	손상된 MCP 서버·응답을 악용해 개인정보·금융정보 등 민감 데이터를 무단 추출하는 행위
지휘통제(C2) / 업데이트 메커니즘 타협(Update Mechanism Compromise)	악성 서버를 통해 은밀한 C2 채널을 구축하거나, 업데이트 과정에 백도어를 삽입해 장기 침투를 시도하는 방식
ID 및 접근 제어 문제(Identity/Access Control Subversion)	인증·권한 부여 체계의 결함을 악용해 불법 계정 접근 또는 권한 상승을 획득하는 공격
서비스 거부(Denial of Service, DoS)	과도한 요청으로 MCP 서버와 종속 자원을 과부하 상태로 만들어 정상 서비스 제공을 방해하는 공격
불안정한 구성(Insecure Configuration)	약한 인증, 불필요한 포트 개방 등 잘못된 서버·네트워크 설정을 악용해 무단 접근이나 시스템 손상 초래하는 문제

○ 현재 운영 중인 정부 시스템은 개인정보보호법과 국가정보보호 기본지침을 통해 최소 권한 원칙과 Zero Trust 기반의 접근 통제를 강화

- 그러나 MCP는 다양한 외부 도구와 서버를 손쉽게 연결·활용할 수 있는 구조적 특성을 지녀, 기존 제도 기반의 보안 원칙과 상충하는 부분이 존재

- 따라서 MCP를 도입할 경우, 기존 Zero Trust 아키텍처와의 결합, 인증·접근통제 강화 등 새로운 규제 및 보안 요구를 제도적으로 정립할 필요가 있음

※ '24.12월 통과되어 '26년 시행 예정인 인공지능기본법 역시 MCP 활용과 관련한 구체적 적용 지침 부재

- 모든 접근 요청을 지속적으로 검증하고 행위 기반 접근통제를 적용하는 세밀한 보안 설계가 필수적이며, 이러한 측면에서 MCP 도입의 실효성을 면밀히 검토해야 함

- 정부의 엄격한 보안 요건과 개인정보보호법 준수 의무를 고려할 때, MCP 도입 전 포괄적인 보안 강화 방안 마련 및 Zero Trust 아키텍처 적용 검토 등 선행적 조치가 필요

| 주요 법·제도별 접근통제 및 정보보호 규정 |

구분	관련법	조 문
접근 통제 강화	개인정보보호법 제30조	개인정보처리시스템 접근 권한을 가진 개인정보 취급자는 업무 수행에 필요한 최소한의 범위에서 접근 권한을 관리·통제해야 함
	인사혁신처 정보보안지침 제64조	정보시스템 접근 권한은 최소 인원에게만 부여하며, 직무 변경·퇴직 시 즉시 회수해야 함
정보 보호	개인정보의 안전성 확보조치 기준 제5조	개인정보처리자는 개인정보취급자에게 업무 수행에 필요한 최소 범위로만 시스템 접근 권한을 부여해야 함
	개인정보의 안전성 확보조치 기준 제6조	개인정보처리자는 불법 접근 및 침해사고 방지를 위한 안전조치를 이행해야 함

□ 책임행정과 MCP vs API 비교: 공공부문의 핵심 딜레마

○ 공공부문에서 가장 중요한 원칙인 '책임행정(Accountability)' 관점에서, MCP

와 기존 API 간 근본적 차이점 분석이 MCP 도입 여부를 판단하는 핵심 요소

- MCP는 특정 상황(Context)에 따라 판단을 내리기 위해 여러 개의 알고리즘 모델을 연결하여 실행하는 구조를 가지고 있으며, 이 때문에 최종 판단 결과가 어떤 경로를 통해 도출되었는지 파악하기 어려운 구조
 - 전통적인 행정 판단은 사람이 규정을 해석하고 적용하기 때문에 책임 소재가 명확하지만, MCP는 복수의 맥락 변수(Contextual Variables)에 따라 시스템이 내부적으로 모델을 자동 선택·실행하기 때문에 판단 경로 자체가 고정되지 않음
 - 맥락 구성 로직, 데이터 입력, 모델 자체, 모델 선택, 실행 환경 등 다양한 오류 지점이 존재할 수 있어, 단일 책임 주체를 특정하기 어려움
 - MCP는 기존 API 방식에 비해 책임성·추적성 확보 측면에서 구조적 한계 존재
 - API 방식: 명확한 요청-응답 구조로 이루어져 단계별 로그와 추적이 용이하며, 각 API 호출마다 인증, 권한, 접근 기록이 명시적으로 관리되어 책임 소재 파악 용이
 - MCP 방식: 컨텍스트 유지 및 동적 도구 탐색을 기반으로 AI가 자율적으로 여러 시스템에 접근하기 때문에, “누가, 언제, 왜, 어떤 데이터에 접근했는지” 추적하기가 복잡하고 불투명
 - 특히 정부의 의사결정 과정에서는 “AI가 어떤 근거로 특정 결론에 도달했는가”를 설명할 수 있는 설명가능성(Explainability) 확보가 MCP 환경에서는 구조적으로 어려움
 - MCP는 행정 의사결정의 전제 조건인 맥락(Context)을 자동으로 구성하는 기능을 수행하지만, 그 과정에서 데이터 편향, 알고리즘 편향 등 AI 알고리즘의 편향성이 복합적으로 작용하면서 MCP 환경에서는 기존보다 편향이 증폭될 위험이 존재
 - 맥락(Context)을 통해 어떤 조합을 판단 근거로 사용할지를 결정하는 자동화된 맥락 구성 과정에서 편향이 발생할 경우, 정책 수혜의 형평성이 훼손될 위험이 따름
- ※ MCP는 초기 설계 단계에서부터 공공성과 형평성을 반영한 변수 선택 기준을 마련해야 하며, 시민 참여·전문가 자문·시범 운영 결과 등을 바탕으로 한 지속적인 수정 및 검증 체계가 필요

□ 공공분야 MCP의 도입은 사회적 수용성과 윤리적 정당성 확보가 필수

- MCP는 규정 중심의 행정 체계를 데이터·맥락 기반 자동화 의사결정 구조로 전환
 - 기존 행정은 ‘규정에 따른 일률적 적용’을 중시했으나, MCP는 맥락(Context)에 따라 AI Agent가 동적으로 판단 기준을 적용
 - 공무원의 직관·경험·심의 중심의 판단 구조가 MCP를 통한 데이터 기반의 자

동화된 판단 구조로 대체되며, 사람 개입이 최소화

- MCP의 도입은 단순한 기술 업그레이드가 아니라, 정책 결정과 행정 절차의 자동화 및 재구성을 수반하기 때문에 사회적 합의 기반의 설계와 책임 소재의 명확화 병행이 필요
 - 행정 결정의 기준 설정, 모델 선택, 결과 도출의 전 과정이 기계적 절차로 대체되면서 행정 절차가 기술적으로 재편
 - MCP는 표면적으로 객관적 판단을 수행하는 것처럼 보이지만, 실제로는 정책적 가치와 사회적 선택이 내재된 기술 구조이므로 설계와 운용 단계에서 사회적·윤리적 검토가 필요

2 정부 및 공공부문 적용 시 고려사항

□ MCP 도입은 대체 기술 가능성과 제도적 제약을 고려해 신중한 판단이 필요

- MCP는 어디까지나 하나의 기술적 방법론에 불과하므로 향후 더 효율적인 기술이 등장할 수 있으며, 따라서 공공부문에 MCP를 도입할 때는 법·제도적 기반과 행정 환경 적합성을 함께 검토해야 함
 - 내부적으로 도입 필요성이 확인되고 제약이나 관련 규정이 없는 경우, 새로운 규정을 마련해 AI 에이전트 도입을 추진하는 절차가 필요

| 인공지능 에이전트 도입 필요성 판단 체크리스트 |

분류	체크리스트
내부 환경 검토	단일 부서 내의 업무인가, 다른 부서와 연계되어 있는가? • 단일 시스템을 통제해 단일 결과물을 도출하는 경우, 부서 내부 의사결정으로 진행 가능 • 다른 부서의 시스템을 연동해야 하는 경우, 에이전트 임무 수행 중 발생할 수 있는 오류·문제 대응 시나리오 및 책임 소재를 사전에 명확히 해야 하므로 초기 정책 결정에 시간 소요
	외부망을 사용하지 않는 업무인가? • 보안을 고려하여 내부망 환경에서만 운영되는 업무라면, 외부 데이터를 조회하거나 결괏값을 수신하기 전에 내부 보안 규정을 반드시 확인해야 함 • 외부 서비스를 호출해 결괏값을 받는 기술이 필수인 경우, 에이전트 기술이 필요해도 도입이 어려움

분류	체크리스트
	처리하고자 하는 모든 업무가 전산화되어 있는가? • 에이전트는 여러 단위 업무를 호출하는 역할이므로, 해당 단위 업무가 전산화되어 있지 않다면 단위 절차에 대한 에이전트 도입이 어려울 수 있음 - 예: 회의실 예약 에이전트를 개발하려 해도 기존 회의실 예약 시스템이 없다면 에이전트 도입 불가능 업무 담당자 PC 내의 정보를 활용해야 하는가? • 필수적으로 참조해야 하는 정보가 시스템이 아닌 업무 담당자의 PC 등에 저장된 경우, 이를 에이전트와 연계할 별도 절차가 필요 • 에이전트는 특정 서비스나 정보에 접근하기 위해 네트워크에서의 경로 확보가 전제되어야 함
업무 검토	수행하고자 하는 임무가 정형화되어 있는가? • 정형화된 업무인 경우 에이전트 도입 가능성이 높고, 절차에 따라서 승인받고 처리되어야 하는 업무라면 그에 맞게 절차를 따를 수 있도록 에이전트를 설계할 수 있음 • 반대로 정형화되지 않거나 분기 조건이 많은 업무(특정한 상황에 따라서 분기되어야 하는 임무)의 경우, 에이전트 도입을 위해 관련된 규정이나 규칙을 정교하게 설계해야 함 실시간으로 처리되어야 하는 업무인가? • 실시간 처리가 필요한 업무라도 중간에 다른 시스템의 승인 절차나 권한 동의가 필요한 경우, 실시간 처리가 어려움 • 특정 업무가 지연되는 경우, 에이전트는 전체 업무를 수행하지 못하고 전산 자원을 점유(세션)해야 하므로 효율성이 떨어질 수밖에 없음 • 각 업무가 실시간, 동시에 처리되어도 괜찮은 업무라면 에이전트 도입에 적절할 수 있으나, 앞의 절차가 완료되어야 다음 절차로 넘어갈 수 있는 업무인 경우에는 면밀한 분석 필요 인간에게 실질적으로 영향을 주는 업무인가? • 에이전트의 결과가 직접적으로 인간의 삶에 영향을 미치는 업무 (예: 소득 지원금 결정 등)는 인간의 판단 개입을 포함한 엄격한 검증 과정 요구 • 예: 산사태 예측 에이전트가 100mm 호우에 산사태가 나지 않는다고 예상했는데 실제로는 인명 사고가 발생한 경우, 모델 신뢰성 및 검증 절차를 명확히 해야 함
기술 검토	도입하고자 하는 지능이 어떠한 지능인가? • 식별 지능: 객체 인식, OCR(광학 문자 인식), STT(음성 인식)과 같이 외부의 정보로부터 특정한 물체나 정보를 인식하고 추출할 수 있는 지능 - 예: 화재 감지, 산불(연기), 무역신고서 광학문자인식 등 • 생성 지능: 인간의 질문에 대해 새로운 결과물을 만들어내고 대화를

분류	체크리스트
	하면서 원하는 결과를 생성하는 지능 - 예: HyperClovaX, Exaone, Gemma 등 • 의사결정 지능: 에이전트 호스트 역할로써 업무 절차를 정의하고, 특정 절차가 중단되거나 불가능한 경우에 대체 절차를 수행하도록 하는 지능(초거대 언어모델 기반) • 각 지능은 단위 서비스로 제공되는 형태가 많으며 특히 식별 지능은 HW나 별도의 사업으로 구매된 경우가 많음 • 만약 희망하는 기술에 내부 솔루션 형태로 도입된 것이 없는 경우, 별도의 예산을 확보하여 도입해야 함 계산이나 규칙으로 처리되는 업무는 있는가? • 초거대 언어모델은 확률 방법과 기존 정보를 학습하는 방식으로 계산하므로, 모든 것은 확률에 의해 처리 • 특정 값에 따라서 다음 단계의 에이전트 처리가 여러 갈래로 나누어지는 경우 복잡한 설계 로직이 요구됨 도입하고자 하는 것이 정확한 값을 요구하는가? • 예: 나눗셈 계산 시 소수점 단위 및 각각의 정보가 무엇을 기반으로 계산해야 하는지에 대한 절차 필요 • 정확한 값을 제공해 주어야 하는 클라이언트가 그 값을 도출하기 위해 별도의 계산을 해야 하는 경우, 정확한 값을 산출해야 하는 절차는 별도 설계 필요 능동적인 일을 수행하는가? • 에이전트가 다른 시스템에 명령을 수행하는 경우, 해당 시스템에 주게 되는 영향을 면밀하게 검토해야 함 • 특히 데이터베이스 상으로 수행해야 하는 만들기, 읽기, 갱신하기, 삭제하기(CRUD) 기능의 경우 단위 시스템에 큰 영향을 줄 수 있으므로 능동적 수행 여부는 다른 시스템과의 연계 관점에서 면밀히 검토되어야 함 인간의 의사결정을 무시하고 수행할 수 있는가? • 에이전트가 인간 판단 없이 자율적으로 수행하는 업무라면, 그 결과에 대한 책임 소재를 명확히 규정해야 함 단위 시스템이 희망하는 기능을 모두 보유하고 있는가? • 에이전트가 접근해야 하는 여러 시스템이 요구 정보를 모두 제공하거나 명령 수행이 가능한지 확인해야 함 • 사용자 계정별 권한 차이가 있는 경우, 권한에 따른 정보 제공이 지원되지 않으면 에이전트 도입이 곤란 • 클라이언트별 기능 요구사항을 상세히 설계한 뒤, 단위 시스템의 해당 기능 여부 검토가 필수

□ MCP 도입은 정교한 권한 정의와 보안 통제가 선행이 필수

- 조직 내부에서 도입 필요성에 대한 공감대가 형성되더라도, MCP는 LLM을 기반으로 여러 에이전트를 활용하는 구조이기 때문에 사용자의 접근 권한에 따라 적합한 클라이언트를 호출하기가 어려워, 시스템 간 보안 권한 정의가 우선적으로 요구됨
- LLM 모델은 학습한 데이터를 바탕으로 어떤 질문에든 답변을 제공할 수 있다는 장점이 있지만, 보안이 중요한 환경에서는 모델이 언제든지 답을 해주는 특성이 보안에 영향을 줌
 - 사용자 권한별로 LLM을 MCP 호스트로 분리해 별도로 운영하는 방법도 있으나, 비용과 시간이 많이 들 뿐 아니라 권한이 변경될 때마다 지속적인 관리가 필요함
 - 로그인한 사용자의 권한을 위임받아 에이전트가 여러 단위 시스템에 접근해야 하며, 이 과정에서 각 시스템의 권한 관리자가 에이전트와 안정적으로 연동되어야 함
- 호스트의 임무 요청을 받아 실행하는 각 클라이언트는 서로 다른 관리 주체와 데이터 권한 체계를 가지고 있으며, 만약 클라이언트마다 다른 권한을 가지고 있다면 해당 임무는 수행이 불가능
- SSO(Single Sign On)와 같은 단일 접근키를 가진다고 하더라도, MCP는 에이전트가 능동적으로 정보를 탐색하고 실행하는 구조이기 때문에 그보다 더 정교한 권한 정의가 필요
 - MCP가 ‘읽기’ 기능을 수행할 때에도 사용자 권한에 따라 제공 가능한 정보는 제한되어야 하며, 특히 공공부문의 경우 개인정보 조치가 포함될 수 있으므로 엄격한 기준 필요

□ 기존 서비스 대비 MCP 도입의 이익과 한계 측정

- MCP를 도입할 때에는 업무 담당자의 역할 변화와 프로세스 차이를 충분히 고려하며, 도입 전·후 변화를 비교·분석하는 내부 검토와 합의 선행이 필요
 - 업무 담당자 인터뷰를 통해 반복적·기계적 업무(조회, 탐색, 보고 등)를 파악하고, MCP가 해당 업무를 얼마나 줄일 수 있는지 확인

- MCP 도입이 사람의 일자리와 직접적으로 연결되는 경우, 근로기준법 등 관련 법령을 검토하여 MCP가 대체할 수 있는 업무 범위를 정의하고, 그에 따른 비용 효과를 분석 검토
 - 단순히 예산 대비 효과가 아니라, 사람이 수행하기 어려운 방대한 정보 탐색이나 데이터 연결 업무를 MCP가 줄여줄 수 있는지 여부 평가

□ 기존 시스템과 데이터 활용 가능 영역 분석

- 오랜 기간 운영되어 온 행정 시스템에는 이미 다양한 기능이 구현되어 있으므로, MCP와의 중복 여부를 면밀히 검토하고 기존 시스템 기능과의 비교 분석 필요
- 단순히 스프레드시트나 간단한 프로그램으로 해결 가능한 업무라면, MCP 적용을 무리하게 추진할 필요 없음
 - MCP는 단순 자동화 도구가 아니라, 여러 시스템과 데이터를 연결해 새로운 부가 가치를 창출하는 영역에 우선적으로 적용하는 것이 적함

□ 신뢰성과 정보의 사실 여부를 검증하는 구조 확립

- MCP는 사람의 권한을 위임받아 다양한 외부 도구와 데이터를 연결하므로, 신뢰성 확보가 도입의 전제 조건
- MCP가 연결한 결괏값은 주기적으로 검증 절차를 거치고, 내부 감사 및 외부 검증을 통해 오류 여부 확인
 - 특히 통계 및 정보분석처럼 동일한 데이터라도 해석이 달라질 수 있는 영역에서는, MCP가 제공한 분석 결과를 인간의 판단으로 보강하고 최종 결론은 반드시 인간 검증을 통해 확정

□ 조직 내 업무의 권한과 책임을 명확하게 정의

- MCP 도입 시 내부 규정에서 권한 위임과 책임 소재가 명확히 구분되지 않은 경우, 전결 규정과 문제 발생 시의 책임 범위를 제도적으로 정의
- 부서 간 협업 과정에서 MCP가 다른 부서의 시스템과 연계되는 경우, 오작동이 다른 부서 시스템에 피해를 주지 않도록 사전 규정 마련

- 특히 MCP는 여러 클라이언트와 서버를 연결하는 구조이므로, 권한 관리 체계와 역할 분담에 대한 세밀한 설계 요구

3 적용방안(1): MCP 파일럿 및 테스트 공간 ‘APT(Agent Pilot and Test)’ 마련

□ 공공부문의 MCP 도입 효과성에 대한 사전 검증 필요

- MCP를 빠르게 도입하려 해도 MCP 클라이언트와 서버가 실제 데이터에 접근하여 임무를 수행하기 때문에 위험도가 높고, 오동작 발생 시 원인 파악 및 안정화 작업 필요
- 실제 운영 중인 서비스(API 등)에 에이전트를 적용하기 전, 에이전트가 접근하고 특정 임무를 수행하며, 이의 결과물을 사람이 직접 확인할 수 있는 환경 필요
- 중복 투자 방지를 위해, 각 업무 담당자가 인공지능과의 대화를 통해 자신의 업무에 적합한 에이전트 서비스를 미리 탐색, 제안, 추천받을 수 있는 별도의 에이전트 구성 필요

□ 범정부 포털 내 에이전트 테스트 환경 마련

- 주요 기관별 담당 업무를 세분화하고, MCP 클라이언트로 구축 가능한 시스템 API 현황을 조사하여 종합적인 마켓플레이스 형태의 정보를 제공
 - 각 기관은 기존 업무 시스템 중 에이전트 활용이 가능한 부분을 분리하고, 이를 기반으로 MCP 서버 테스트가 가능한 복제본 형태의 시스템 구역 마련
 - 분리된 영역에는 상세한 설명과 함께, 에이전트 서버를 검색하여 찾아볼 수 있는 공통 저장소 및 인가된 접근 권한 발급 기능을 제공
- 기관의 업무 담당자가 해당 기관의 업무적 난점과 해소 방안을 입력하면, 인공지능이 해당 문제를 해결할 수 있는 적절한 MCP 클라이언트-서버 연계 지점을 추천하도록 설계
 - 기관 사용자는 인가받은 MCP 클라이언트와 MCP 서버를 이용해 필요한 정보 또는 활동을 입력하고, MCP 클라이언트가 기대한 결과를 도출하는지 확인
 - 원하는 결과가 도출되지 않는 경우, 해당 데이터를 제공하는 타 기관·시스템의 MCP 서버 담당자와 협의하여 실제 활용 가능성을 검토하고, MCP 서버 기능 보강 요청
 - MCP 클라이언트가 MCP 서버의 데이터를 입력·수정·삭제·외부 전송하는 등

직접 영향을 미치는 경우, 기관 간 법적 책임 여부에 관한 협약을 별도로 수립

- 해당 기관에서는 이를 별도의 MCP 호스트로 구성하여 파일럿 테스트를 수행하고, 그 결과를 바탕으로 효과성을 검증·실무 적용 계획을 수립해 안정적인 인공지능 에이전트 도입
 - 테스트 환경을 마련해 MCP 호스트를 구성하고, 호스트가 MCP 클라이언트를 통해 여러 MCP 서버를 적절히 호출하는지 기능 확인
 - 테스트 환경에서 오류 없이 충분히 구동되는지를 확인하기 위한 체크리스트를 작성하고, 실제 구동 환경으로 이관하기 위한 일정, 체크리스트, 추가개발 영역, 법적인 권리와 책임 확정
 - 테스트 환경을 토대로 MCP 호스트, MCP 클라이언트, MCP 서버에 대한 명세서, 테스트 결과서, 법적 대응 방안, 운영 예산 등을 마련하여 기관별 의사결정 단계로 이관

□ MCP APT를 통한 MCP 데이터 활용성 극대화

- 데이터 부재를 이유로 에이전트 도입이 지연되는 사례 감소
- 충분한 파일럿 테스트를 통해 에이전트의 안정성을 확보한 뒤 실제 업무 환경에 적용함으로써, 인공지능 시스템에 대한 신뢰성 확보
- 인공지능이 자율적으로 업무의 절차 및 중요도 등을 판단할 수 있는 ‘에이전틱 인공지능’ 단계로 나아가는 초석 마련
 - MCP 호스트의 기능과 요구사항이 분야별로 정교화되고, AI가 분석·판단해야 할 범위가 늘어날수록 기능이 개선

예시 시나리오

- 특정 지자체에서 사회보장정보원의 방대한 데이터를 MCP 호스트를 통해 조회하고, 사회복지 사각지대 정보를 다각적으로 분석하여 담당자에게 명세서 형태로 전달
- 지자체마다 상이한 판단 준거 및 적용 기준을 MCP 호스트에 지시문으로 입력
- MCP 호스트는 이에 따라 MCP 클라이언트를 호출해, 사회보장정보원 외에 지자체 내부의 관할 정보를 조회
- MCP 호스트의 지시에 따라 MCP 클라이언트는 사회복지 사각지대 대상 가구를 추천하고, 담당자에게 이메일 보고 등으로 검토를 자동으로 의뢰

4 적용방안(2): MCP 공작소

□ 희망하는 업무 기술 시 사용 가능한 MCP 클라이언트와 서버 간 조합 추천

- 일상 업무 담당자가 직접 MCP를 구축하거나 호스트를 구현하는 것은 어려움
 - 실제 업무를 가장 잘 이해하는 사람은 현업 담당자이지만, 이들은 인공지능 관련 개발 기술이 없으므로 개발자에게 희망사항을 개별적으로 설명
 - 이 과정에서 사업의 필요성, 예산 확보, 수행, 관리와 같은 SW 용역사업 형태의 문제가 기획되고 많은 행정력 및 예산 투입
 - 이미 상당 부분의 서비스가 전산화된 공공업무는 단위 시스템들이 MCP 서버 역할을 수행할 수 있으며, 업무 담당자의 필요에 따라 유연하게 조율될 수 있음
- 사용자가 본인이 구현하고자 하는 업무를 생성형 언어 모델에 입력하면, 해당 업무에 적합한 MCP 클라이언트-서버 조합을 업무 담당자에게 제시

□ 생성형 AI와 MCP 클라이언트-서버의 설명 정보를 활용, 업무 해결 방법 제시

- 조직 내 각 레거시 시스템 또는 담당자가 관리 중인 데이터의 API, 접근 권한에 대해서 MCP 서버용 설명 자료를 명세화하고 세부적으로 적용
 - 업무 담당자는 자신이 주로 사용하거나 중요하다고 판단되는 공유 정보를 특정 저장소에 저장하고 주기적으로 판올림 작업 진행
 - 해당 업무나 정보에 대한 MCP 클라이언트 접속 가능 검색 정보 및 접근 방법 등을 기술하여 이를 내부 MCP 공작소 환경에 제공
 - 읽기 기능만을 제공하여 본인의 담당 업무에 영향이 없도록 구성
- MCP 호스트 구성을 위해 업무 담당자의 질문을 유기적으로 분석하고 MCP 호스트 추천 내역을 검색하여 제시할 수 있는 언어 모델 마련
 - 내부에 최적화된 언어 모델을 MCP 호스트로 구성하여, 사용자가 희망하는 업무를 입력하고 그 결과에 따라 MCP 호스트가 다른 사용자들의 공유 정보를 조회
 - 질문에 따른 결괏값을 사용자가 판단하고 피드백하여 질의-답변 개선

□ MCP를 통한 행정 업무 자동화와 조직 역량 강화

- MCP를 통해 업무 담당자가 사업화가 어려운 업무상의 불편함과 개선점을 직접 구현·적용할 수 있도록 지원함으로써, 업무 역량을 강화

- MCP 호스트가 반복적인 업무를 파악·개선함으로써, 담당자는 시간과 자원의 한계로 수행하지 못했던 업무까지 수행 가능
- MCP가 조회·정리·보고 등 시간 소요가 큰 업무를 절감함으로써, 공공부문은 대국민 서비스 제공을 더욱 확대

○ 효율성이 높은 MCP 호스트는 기관 내 승인된 단위 업무 담당자들과 공유되어 전체적인 업무 효율성 개선

- MCP가 수행하는 업무를 통해 단순 반복 업무를 줄이고, 이미 타 담당자가 처리한 업무를 쉽게 파악하여 업무 중복 감소

| MCP 기반 복지 사각지대 행정 지원 시나리오 |

예시 시나리오
• MCP APT가 전달한 복지 사각지대 관련 담당자 정보를 인계받음 • 지자체 또는 관내 복지 지원 이력에 대해 내부 MCP 호스트에 질의 • 내부 MCP 호스트는 과거 복지 대응 관련 담당자의 기록을 조회하여 현황 파악 • 담당자는 이 정보를 기반으로 희망하는 새로운 MCP 공작소에서 호스트 시나리오 질의 및 업무지시(일자별 방문 계획을 수립하고, 주의 사항을 체크리스트로 구성) • 담당자는 지정된 일정에 따라 방문하고 취약계층 복지 업무를 지원한 뒤, MCP 호스트에 업무를 적절히 분산, 정리, 저장토록 지정 • MCP 호스트는 담당자의 방문 결과를 요약 정리하여 라이브러리화, 추후 담당자 변경 시에도 응용

□ MCP APT와 MCP 공작소 차이점

○ 두 사업은 목적과 범위에서는 다르지만, 공통된 기술 기반과 GPU를 활용함

| MCP APT와 MCP 공작소 비교 |

항목	MCP APT	MCP 공작소
목적	기관 업무 MCP 기획 PoC	개인 업무의 어려운 점 개선
타 공공기관 연동	연동 가능	내부 업무에 국한
보안의 범위	승인되고 제한된 사용자	개인 데이터, 환경에 제한
MCP 서버의 역할	능동적(자료의 입출력 등)	수동적(조회 등)

5 적용방안(3): 공공 서비스 제안

□ 민원 서비스 혁신: “24시간 똑똑한 공무원”

○ (Intercom 사례에서 배우는 민원 자동화) 효과적인 민원 자동화를 위해서는 단계별로 지능적으로 분류하는 체계 필요

- MCP가 AI 에이전트의 ‘USB-C 포트’ 역할을 수행하여, 다양한 정부 시스템을 하나의 지능형 민원 처리 시스템으로 연결 가능

※ 예: 병원 트리아지(응급도 분류) 시스템과 유사한 방식으로 민원 복잡도와 유형을 분석하여 적절한 처리 경로 결정

| 민원처리 자동화 시나리오 |

단순 정보 제공	“사업자등록증 발급받으려면 어떻게 해야 하나요?” → AI가 필요 서류, 절차, 수수료, 소요 시간 등을 체계적으로 안내 → “지금 바로 신청하시겠어요?” → 온라인 신청 페이지 연결 또는 필요 서류 체크리스트를 카카오톡으로 전송
중간 복잡도 민원	“전입신고 처리 상태를 확인하고 싶어요” → AI가 MCP를 통해 주민등록 시스템에 접속하여 처리 상태를 실시간으로 조회 → 문제 발견 시 담당 공무원에게 자동 알림

- 지능형 라우팅 시스템 효과로 국민은 빠른 서비스를 제공받을 수 있고, 공무원은 반복적·단순 업무에서 벗어나 중요 행정 업무에 집중 가능

※ Intercom 검증 자료 : 51% 자동 해결률로 공무원 업무 효율성 대폭 향상

| MCP 활용 행정 서비스 자동화 시나리오 |

구분	내용
주민등록등본 발급 자동화	○ 시민 요청: “주민등록등본이 필요해요” (카카오톡·정부24) ○ AI 처리: MCP를 통해 본인 인증 시스템에 연결 → 신원 확인 → 발급 목적 확인 → 전자문서 자동 생성 → 이메일 또는 카카오톡으로 발송 ○ 소요 시간: 약 5분 내 처리 완료
세금 납부 안내 및 처리	○ 요청: “재산세 납부하고 싶어요” ○ AI 처리: MCP를 통해 지방세 시스템에 접속 → 납세자 정보 조회 → 미납 세액 확인 → 납부 방법 안내 → PayPal/Stripe 연동으로 즉시 온라인 결제 → 영수증 자동 발행 → 다음 납부 일정 안내
복지 혜택 맞춤 안내	○ 시민 정보 종합 분석: 나이, 소득, 가족 구성, 거주지 등 ○ AI 처리: MCP 통해 복지·고용·건강보험 시스템에 동시 접속 → 종합적 혜택 정보 제공 → 신청 절차 자동 진행

□ MCP 기반 행정 혁신: “대국민 서비스와 내부 업무의 동시 고도화”

- 현행 국세청 홈택스(국세), 행안부 위택스(지방세) 등 분리된 공과금 납부 시스템을 MCP를 활용한 통합 납부 체계로 전환

| 통합 납부 시스템 시나리오 |

- 시민 질의: “이번 달 내야 할 세금 있나요?”
- AI 처리: MCP를 통해 국세청, 지자체, 공기업 등 관련 시스템에 동시 접속 → 납부 현황 종합 조회 → “재산세 5만 원은 다음 주 납부 예정, 자동차세 3만 원은 연체 중입니다.”와 같이 결과 요약 안내 → 통합 결제 링크 제공

※ Stripe 사용량 기반 과금 모델을 적용하여 사용량 기반 정부 서비스 과금

(AI가 MCP를 통해 API 사용 로그 실시간 추적 → 월말 사용료 자동 계산 → 전자세금계산서 발행)

- 문서 관리와 일정 관리 등 내부 행정 업무의 효율성을 높여, 공무원과 국민 모두에게 편리한 전자정부 서비스 제공

| MCP를 활용한 문서관리 혁신 |

구분	내용
자료 검색 및 요약	○ 공무원 검색: “코로나19 관련 경제 정책” ○ AI 처리: MCP를 통해 정부 문서 시스템, 법령 데이터베이스, 회의록 아카이브에 동시 접속 → 수만 건 문서에서 관련 내용 시간순 정리 → 핵심 내용 요약 제공 → 유사 해외 사례나 관련 연구 자료까지 함께 제시
지능형 문서 분류와 태깅	○ 새로운 공문 또는 정책 문서 작성 시, AI가 자동으로 내용 분석 후 적절한 카테고리 분류 및 관련 키워드 태깅 - 예: “청년 일자리 창출을 위한 스타트업 지원 방안” 문서 → AI 자동 태깅(“청년정책”, “일자리”, “스타트업”, “창업지원”) → 관련 부처(고용부, 중기부, 과기정통부) 연결 → 과거 유사 정책 찾아 중복성 검토 결과 제공
회의록 정리와 후속 조치 관리	○ 정부 회의 종료 시 AI가 자동으로 회의록 정리 → 논의 안건별 담당 부서와 처리 기한 정리 → 각 담당자에게 업무 자동 배정 → 진행 상황 실시간 추적 - 예: 국정현안점검회의에서 “부동산 정책 개선안을 다음 달까지 마련” 결정 → AI가 자동으로 국토부에 해당 업무 배정 → 진행 상황 주기적 체크 → 자연 위험 시 사전 일침

| MCP를 활용한 일정 관리 혁신 |

구분	내용
부처 간 회의 일정 자동 조율	○ 요청: “교육부, 복지부, 기재부와 함께 아동 정책 회의를 잡아줘” ○ AI 처리: MCP를 통해 각 부처 담당자 일정 확인 → 모두 참석 가능한 시간대 찾아 회의 설정 → 정부청사 회의실 예약 시스템과 연동해 회의실 자동 배정 → 참석자 초대 및 관련 자료 공유
업무 관련 파일과 이메일의 통합 관리	○ 특정 정책이나 프로젝트 관련 모든 이메일, 파일, 회의록 자동 연결 관리 ○ 담당자 변경이나 인수인계 시 관련 자료가 체계적으로 정리되어 일정 지연 없이 업무 연속성 보장

6 공공부문 MCP 적용 전략 및 제언

□ MCP 도입은 기존 업무·조직 구조 분석과 효율성 검토를 전제로 해야 함

- MCP를 도입하기 전, 조직의 업무를 MCP 관점에서 재정의해야 함
 - 기존 업무 프로세스가 규칙적·체계적이지 않은 상태일 경우 MCP를 도입하면, 잘못된 맥락(Context) 처리로 오히려 오류가 발생할 수 있음
 - 조직과 부서별 업무를 명확히 분석한 뒤, MCP의 맥락 자동화 및 도구 연결 효율성을 적용할 수 있는 영역을 검토해야 함
 - 특히 규정·지침 기반 행정 업무는 MCP와 조화롭게 운영할 방법을 우선 고려하고 MCP 기반 에이전트 위임 가능성을 검토해야 함
- MCP 도입 시 사람·조직·부서 간 관계를 고려해야 함
 - MCP는 여러 시스템과 도구를 연결하므로, 부서 간 권한과 역할에 따라 맥락 제공 방식이 달라질 수 있음
 - 따라서 부서·기관 간 업무 관계와 권한 체계를 면밀히 분석해야 하며, MCP는 인간의 업무를 보완하는 수단이지, 대체 수단이 아님을 명확히 인식해야 함
- MCP 도입의 실효성을 기존 업무 방식과 비교해야 함
 - 이미 효율적으로 운영 중인 업무라면, MCP를 무리하게 도입할 필요는 없음
 - MCP가 절차를 복잡하게 하거나 관리 부담을 증가시킬 경우, 도입을 지양하고 실질적 업무 효율성 제고 여부를 명확히 판단해야 함

□ MCP 활용은 보조적 맥락 제공 도구이며, 최종 의사결정 권한은 인간에 귀속

- MCP는 효율성을 보완하는 보조 도구일 뿐, 독립적 의사결정 주체가 아님
 - MCP는 다양한 외부 도구와 시스템을 연결해 AI가 임무를 수행하도록 지원하지만, 그 과정에서 생성되는 맥락(Context)과 결과물에는 여전히 오류 가능성이 존재
 - MCP의 결과물은 인간 업무의 일부를 보완하는 수준으로 활용해야 하며, 최종 의사결정 권한은 사람에게 귀속되어야 함
 - 특히 추상적 지시가 내려질 경우 MCP가 잘못된 맥락을 형성할 수 있어 오류 가능성이 높아지므로, 결과 검증 책임은 반드시 인간에게 있음
- MCP 활용 과정에서는 인간 검증과 책임이 필수
 - MCP는 인간의 권한을 위임받아 여러 시스템에 접근하는 구조이므로, “인간의 권한 위임”이라는 대전제가 반드시 유지되어야 함
 - MCP가 연결한 시스템과 도구에서 도출한 결과는 반드시 인간의 보고·검증 과정을 거쳐야 하며, 이를 통제할 제도적·기술적 장치가 필요
 - 잘못된 맥락 연결이나 오작동으로 인한 결과(예: 금융 데이터 처리 오류, 행정 기록 오류 등)는 원상 복구할 수 있는 기술적·제도적 장치 마련이 필수

참고문헌

- 1) 대통령직속 디지털플랫폼정부, 「공공부문 초거대AI 도입·활용 가이드라인(2.0)」, (2025.4).
- 2) 디지털공간의 보안 및 규제에 관한 법률(LOI n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique).
https://world.moleg.go.kr/web/wli/lgsllInfoReadPage.do?CTS_SEQ=54019&AST_SEQ=105, (2025.7.30).
- 3) 임영모·김리나·안성원, 2024년 공공부문 AI 도입현황 연구, 소프트웨어정책연구소, (2025.4).
https://spri.kr/posts/view/23866?code=data_all&study_type=&board_type=research.
- 4) Avi Perera, "AI Governance Frameworks: A Comparative Analysis", (November 2, 2024).
<https://aviperera.com/ai-governance-frameworks-a-comparative-analysis/>
- 5) Digital Gov Hub, "OMB M-25-22 Driving Efficient Acquisition of Artificial Intelligence in Government,"
<https://digitalgovernmenthub.org/examples/omb-m-25-22-driving-efficient-acquisition-of-artificial-intelligence-in-government/>
- 6) EU 「Artificial Intelligence Act」, EU Official Journal (12 July 2024).
- 7) European Commission, INSPIRE Directive
https://knowledge-base.inspire.ec.europa.eu/legislation/inspire-directive_en
- 8) FedRAMP, <https://www.fedramp.gov>, (2025.7.30. 방문).
- 9) G-Cloud 14, <https://www.crowncommercial.gov.uk/agreements/RM1557.14>, (2025.7.30. 방문).
- 10) Geoawesome, The INSPIRE Directive Explained: Simplifying Geospatial Data Sharing Across Europe,

- <https://geoawesome.com/the-inspire-directive-explained-simplifying-geo-spatial-data-sharing-across-europe/>, (2025.9.3.방문).
- 11) GOV.UK, National AI Strategy, (2021.9.22 공표, 2022.12.18. 최종 개정), <https://www.gov.uk/government/publications/national-ai-strategy>,(2025.9.6.방문).
 - 12) Govtrack.US, H.R. 353 (115th): Weather Research and Forecasting Innovation Act of 2017, <https://www.govtrack.us/congress/bills/115/hr353/summary>, (2025.9.3.방문).
 - 13) IMDA, "Singapore proposes framework to foster trusted Generative AI development," <https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2024/public-consult-model-ai-governance-framework-genai>,(2025.9.6.방문).
 - 14) KEG Lawyers, "Revenge Porn Laws in California – Penal Code 647(J)(4) PC," <https://www.keglawyers.com/revenge-porn-penal-code-647j4>, (2025.9.3.방문).
 - 15) Legislation.gov.uk, Flood and Water Management Act 2010, <https://www.legislation.gov.uk/ukpga/2010/29/contents>, (2025.9.3.방문).
 - 16) Legislation.gov.uk, Voyeurism (Offences) Act 2019, <https://www.legislation.gov.uk/ukpga/2019/2>, (2025.9.3.방문).
 - 17) Niam Yaraghi, 'Transforming health care for older adults, Innovations, equity, and economics,'(August 2, 2023), <https://www.brookings.edu/articles/transforming-healthcare-for-older-adults/>, (2025.9.3.방문)
 - 18) Pair 공식 웹사이트, "Solutions for Public Good," <https://pair.gov.sg/pages/about>; GovTech, "Explore Pair, a government AI chatbot that helps public officers in Singapore conduct research, generate

ideas, and compose messages.” (Last updated 8 July 2025),
<https://www.tech.gov.sg/products-and-services/for-government-agencies/productivity-and-marketing/pair>, (2025.7.29.방문).

- 19) Singapore Infocomm Media Development Authority & Personal Data Protection Commission, "AI Governance Framework 2nd Edition (PDPC)," <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/SGModelAIGovFramework2.pdf>, (2025.9.6.방문).
- 20) The Ministry of Health and Prevention, France, "Digital Health Roadmap" (2023–2027), (May 2023),
https://extranet.who.int/countryplanningcycles/sites/default/files/public_file_rep/FRA_France_Digital-Health-Roadmap_2023-2027.Pdf, (2025.9.3.방문).
- 21) The White House, "Executive Order 14110: Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence", (2023.10.30.),
<https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/>, (2024.6.30.방문).
- 22) U.S. Department of Justice, The Fair Housing Act,
<https://www.justice.gov/crt/fair-housing-act-1>, (2025.9.3.방문).
- 23) US Congress.GOV, AI LEAD Act(S.2293),
<https://www.congress.gov/bill/118th-congress/senate-bill/2293/text>, (2025.9.6.방문).
- 24) US Office of Personnel Management, "The Artificial Intelligence Classification Policy and Talent Acquisition Guidance: The AI in Government Act of 2020," (2024.4.29.).

미주

- 1) Model Context Protocol. (2024.). What is Model Context Protocol(MCP)?.
<https://modelcontextprotocol.io/docs/getting-started/intro>
- 2) Descope. (2025. 09. 05.). What Is the Model Context Protocol (MCP) and How It Works.
<https://www.descope.com/learn/post/mcp>
- 3) Bloomberg. (2025. 07. 14.). Closing the Agentic AI productionization gap: Bloomberg embraces MCP.
<https://www.bloomberg.com/company/stories/closing-the-agentic-ai-productionization-gap-bloomberg-embraces-mcp/>
- 4) Intercom. (2025. 05. 01.). Introducing MCP: A new way to connect Fin and your customer data to your business tools.
<https://www.intercom.com/blog/introducing-model-context-protocol-fin/>
- 5) Paypal. (2025. 07. 03.). Meet the MCP Server Quickstart Guide: Your Fast Track to Building AI with PayPal.
<https://developer.paypal.com/community/blog/mcp-server-quickstart-guide/>
- 6) Stripe. (2025.) Add Stripe to your agentic workflows.
<https://docs.stripe.com/agents?locale=ja-JP>
- 7) Atlassian. (2025.). Getting started with the Atlassian Remote MCP Server.
<https://support.atlassian.com/atlassian-rovo-mcp-server/docs/getting-started-with-the-atlassian-remote-mcp-server/>
- 8) AWS, A2RS. (2025. 05. 02.). Enterprise-Grade Security for the Model Context Protocol (MCP): Frameworks and Mitigation Strategies.
<https://arxiv.org/pdf/2504.08623>