지금은
Agentic AI 시대

기술적 진화: Search to Action

LLM의 한계

대규모 언어 모델(LLM)은 뛰어난 자연어 이해 및 문장 생성 능력을 보여주며 비즈니스 혁신의 가능성을 보여주었다. 그러나 초기 LLM은 특정 가상 환경이나 사용자 인터페이스 내에서 인간이 제공하는 입력값(Prompt)에만 기존 학습 데이터를 활용해 수동적으로 대응하는 한계를 가졌다.

이런 정적인 응답 구조는 실시간으로 변화하는 복잡한 업무 프로세스를 스스로 처리하거나 다단계 의사결정을 독자적으로 수행하기에는 어려웠다.

따라서 정보 검색 모듈을 결합한 검색 증강 생성(RAG: 외부 지식 베이스에서 관련 문서를 검색해 LLM에게 전달하고, 이를 바탕으로 답변을 생성하는 방식)이 도입되어 최신 정보 접근성은 보완되었으나, RAG(Retrieval-Augmented Generation) 역시 정보를 수집하고 변환하는 도구적 한계에서 벗어나지 못해 실무 단계의 복잡한 실행 계획 수립에는 미치지 못하였다.

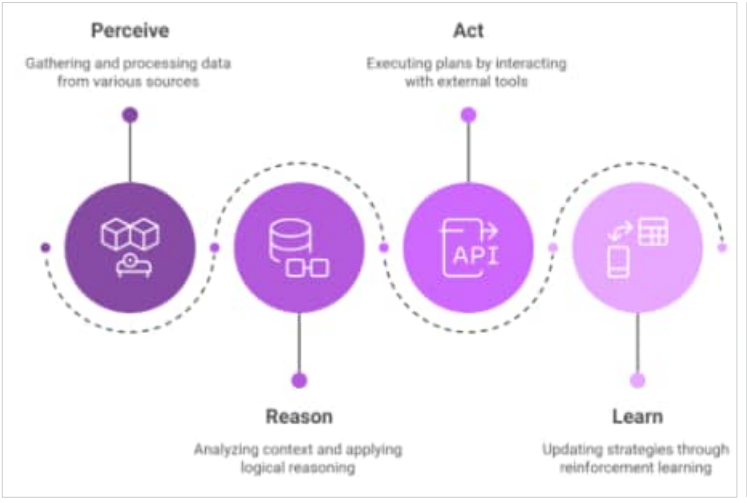
하나증권 리서치센터
미래산업/미드스몰캡
박 찬 솔 연구위원

Agentic은 결과 평가로 셀프 피드백

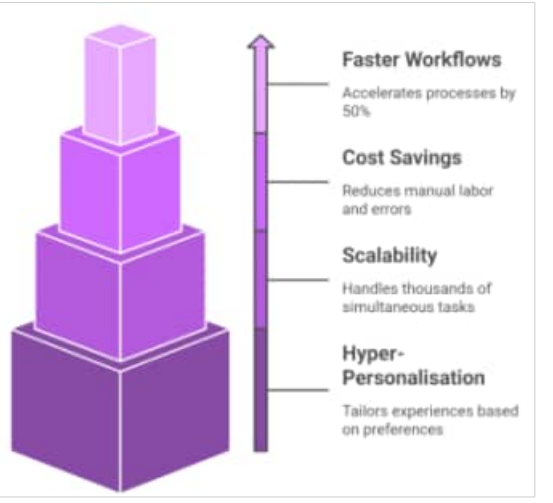
이러한 기술적 공백을 메우며 등장한 Agentic AI는 인공지능이 단순한 텍스트 답변기를 넘어, 사용자가 제시한 고차원적인 목표를 달성하기 위해 독립적으로 판단하고 행동하는 자율 시스템이다.

예를 들어 기존 LLM이 정교한 이메일 본문을 작성하는 것에 멈추었다면, Agentic AI는 조직 내 시스템 승인 권한 아래 마케팅 데이터베이스에서 1) 주요 고객 정보를 식별하고, 2) 개인화된 메시지를 구성하여 외부 API망을 통해 메일을 직접 발송하는 등 실행력(Actionability)을 가진다는 것에 차이가 있다

Agentic AI의 자율적 작동 방식은 목표 설정, 계획 수립, 도구 활용 및 실행, 결과 평가 및 보정 등 4단계 프로세스를 순환한다. 순환적 흐름은 예기치 못한 비정상적인 결과가 나왔을 때 스스로 계획을 정정하는 자가 교정 추론(Self-correcting reasoning)이 가능해져, 인간의 개입을 최소화한다.



Agentic AI 문제 해결 Loop



기업이 Agentic AI를 보는 관점

Agentic AI 모델 및 관련 기술

OpenAI vs. Anthropic 모델

Agentic AI 기술 생태계는 글로벌 빅테크 기업들의 독점적인 상용 솔루션과 고도화된 연산 효율성을 지향하는 로컬 소프트웨어, 그리고 이들을 조율하는 다중 에이전트 개발 프레임워크로 발전하고 있다.

OpenAI가 발표한 '오퍼레이터(Operator)'는 자연어 지시를 통해 가상 데스크톱 환경을 직접 조종할 수 있는 대표적인 컴퓨터 활용 에이전트(Computer Using Agent)이다. 오퍼레이터는 가상 브라우저 내에서 웹 화면의 요소를 시각적으로 분석한 뒤 클릭, 입력, 스크롤링과 같은 정교한 행위들을 자율적으로 실행한다. 만약 태스크 진행 도중 차단 페이지나 CAPTCHA 입력 등의 비정상 상태를 마주치면 자체적인 자가 교정 알고리즘을 사용하거나 사용자에게 조작 권한을 일시 양도하는 하이브리드 협업 방식을 취한다. 또한 금융 결제나 로그인 등 민감 정보가 포함된 행위는 사람의 승인 단계를 요구하는 한편, 전용 모니터링 모델이 백그라운드에서 실시간으로 피싱 사이트 유도나 비정상 데이터 추출 시도를 감시하고 작업을 즉각 차단하는 방식으로 보안성을 확보하고 있다.

앤트로픽(Anthropic)은 마우스 픽셀 위치를 계산하여 컴퓨터 운영체제를 제어하는 기능을 클로드에 내장했다. 기존에 많은 AI 에이전트들이 특정 API(응용 프로그램 인터페이스)를 호출해 정해진 기능을 수행하는 것이 일반적이었다면, 앤트로픽의 Claude는 PC 내 내장된 상태로 직접 사람이 컴퓨터를 쓰는

것처럼 화면을 보고, 마우스를 움직이고, 클릭하고, 타이핑한다.

앤트로픽은 Agentic AI를 구현하기 위해 5가지 디자인 패턴을 소개한다.

❶ Reflection(답변 생성 후 스스로 검토해서 최적의 결과물 생성) : 실행하는 방식은 초안 작성 후 사실성/일관성/안정성 등을 점검하고, 응답의 신뢰도를 추정해 후속 행동을 취한다

❷ Tool Use(필요한 도구를 언제 쓸지 모델이 스스로 결정) : 입력 질문을 분석해서 규칙 혹은 학습 기반인지 판단하고, 표준화된 템플릿으로 툴을 호출하고, 툴의 출력을 검산, 교차검증 등으로 검증한다. 여러 툴을 순차나 병렬로 연결해서 복합적인 문제로 해결한다.

❸ Planning(복잡한 목표들은 하위 작업들로 쪼개, 순차적으로 실행 계획 수립) : 작업을 상하위로 분류하고, 병렬 실행 가능 여부를 판단하고, 실패나 예외 상황에 대한 대체 경로를 설계/정의하고, 실행하는 시간과 비용을 고려하며, 실시간 결과에 따라서 계획을 재작성하기도 한다

❹ Multi-Agent(여러 AI가 역할을 나누고, 협력하는 결과 완성) : 작업을 Agent별로 분업해 병렬 처리하는데, 먼저 역할과 책임을 정의하고, 중앙 조정자를 두고 에이전트 간 결과 상호검증, 합의 등 진행하며 작업의 우선순위 등을 두고 처리한다.

❺ Dynamic Routing(질문/문제 난이도에 따라 적절한 처리 경로 탐색) : 입력값 카테고리 난이도를 정의하고, 비용/지연/신뢰도/리소스 가용성 등 고려한 규칙대로 실행한다.

Claude Agentic Tool 중에서 Claude Code의 흥행이 고무적인데, 미국 개발자 커뮤니티 내에서 대성공을 거두면서 B2B 시장을 장악해 나가고 있는 대표적인 Agentic AI 서비스다. 코딩 성능도 압도적이라는 평가는 받지만 범용 환경이 아니라, Agentic Tool을 가장 효과적으로 쓸 수 있는 개발자들의 맞춤 서비스라는 점에서 OpenAI와는 다른 전략을 선택했기 때문에 폭발적인 성장을 이룰 수 있었다고 생각하고 있다.

모델별 사이즈 vs. SWE 벤치마크 퍼포먼스

국가/기업의 Agentic AI 활용/대응 사례

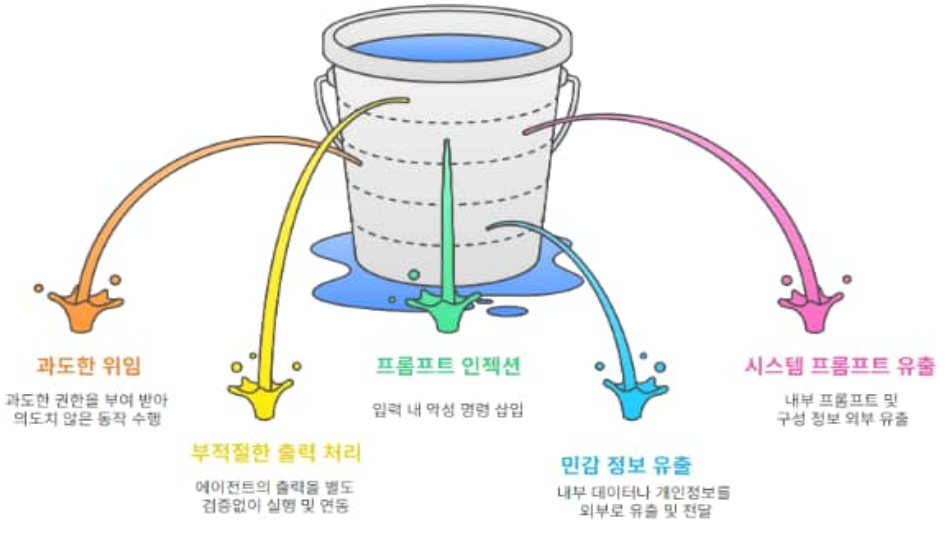
데이터 보안 vs. 생산성

글로벌 차원의 Agentic AI 활용은 실질적인 비즈니스 효율성 증가와 비용 구조 변화를 이끌어내고 있으며, 주요 국가들의 규제 프레임워크 제정 움직임과 함께 가속화되고 있다. 글로벌 선도 기업들은 특정 도메인 내에서 반복되던 전통적인 노동 집약적 업무 방식을 지능형 자율 제어로 대체하고 있다.

핀테크 대기업인 페이팔(PayPal)은 금융 네트워크 내 결제 이상 징후를 자율 수사관 형태로 감시하는 에이전트를 선제 배치하여 사기 피해액 비율을 자사 매출액 대비 0.32% 수준까지 낮추었다. 이는 금융 시장의 평균치 1.32%와 비교해 상당히 낮은 피해금액이다. 독일의 지멘스(Siemens)는 제조 라인의 수천 개 진동 및 열 센서 정보를 예측 진단 에이전트와 자율 연동하여 물리기기 오작동에 따른 다운타임을 기존 대비 40% 절감하는 효과를 보였다. 아마존(Amazon)은 물류센터 자동화를 실현하기 위해 인간 Picker와 실시간 협업하는 이동형 주황색 로봇 드라이브 유닛을 활용하며, 온라인 쇼핑 고객 만족과 가동 효율 향상을 동시에 잡기 위해 전체 매출액의 35%에 영향을 미치는 차세대 에이전틱 추천 매커니즘을 적극 운용하고 있다. 물류 허브를 선도하는 DHL 또한 공급망 경로 지연 방지 및 마지막 인도 지점(Last-mile) 배송 효율화를 실천하기 위해 에이전트를 지능화 도구로 적용하고 있다. 구글의 경우 Agentic Tool을 사용해 회사에서 필요한 코딩의 작년 50%, 올해는 75% 수준으로 AI가 생성하는 것으로 끌어올렸다.

동시에 이러한 고도의 인공지능 확장에 대해 주요 서구 국가들은 보안과 위험 제어를 위한 제도 장치를 도입하기 시작하였다. 미국 국가표준기술연구소(NIST)는 AI 에이전트의 보안적 위험 범위를 제한하기 위해 정부 공공 조달 절차 규격에 에이전트 모니터링 가이드를 설계하였고, 자국 내 주요 공공 조달 사업에 배포되는 인공지능 시스템에 보안 Trail을 최소 90일 동안 보존하게 하는 계약 조건을 도입하고 있다. 유럽연합(EU) 또한 법적 및 도덕적 리스크를 완화하기 위해 2024년 법적 강제성을 지닌 'EU AI Act'를 공식 제정하였다. 특히 고위험군(High-risk AI systems)에 입각한 인력 임용 자격 검수, 개인 신용/금융 평가, 주요 인프라 제어 등 목적의 인공지능 배포 시에는 반드시 고품질 데이터의 훈련 보증/데이터 보존 및 로깅 투명성/인간 감독 시스템 설계가 필요하도록 법률로 규정했다.

Agentic AI 활용의 잠재적인 리스크



국내 기업의 생산성 향상 방향

Make the Loop

국내 기업들이 실질적으로 노동 생산성 혁신을 성취하기 위해서는 비즈니스 프로세스 내에서 에이전트 도입 효과가 가시적으로 나타날 수 있는 가치 지점을 정확히 분류하여 도입해야 한다.

삼성SDS의 세부 사용 통계에 따르면 정기적인 마켓 동향 수집 보고서 집필이나 고객 소통 센터의 인바운드 접수와 같이, 입력과 출력 단계가 규격화되어 있고 일정한 절차대로 수렴되는 반복도가 높은 정형 업무에서 에이전트 사용 빈도수가 집중되고 있으며, 도입 투자자본 대비 효율(ROI) 또한 높게 산출되고 있다.

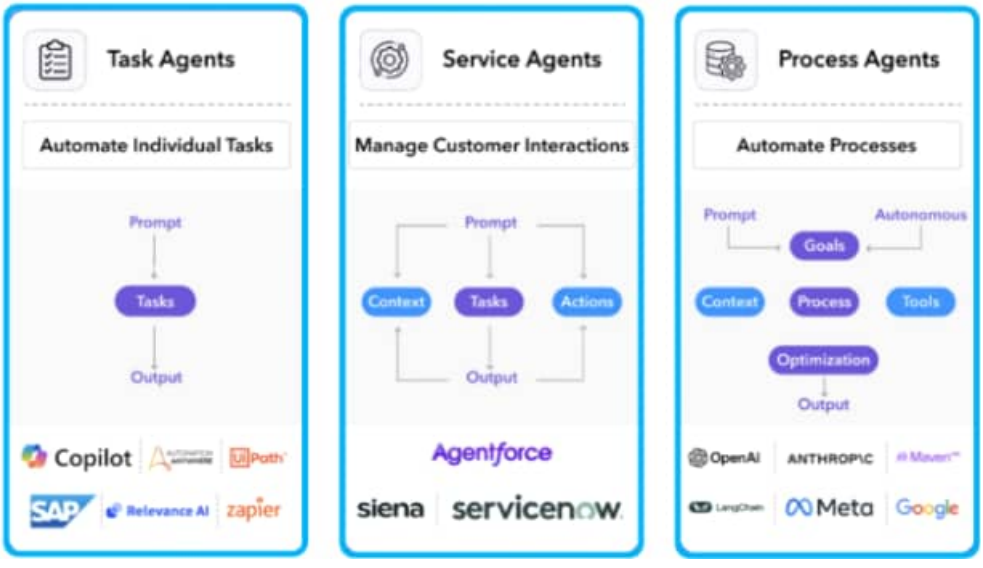
이러한 업무 자동화에 착수할 때 성공적으로 목적을 달성하기 위해 기업이 구축해야 하는 내부 시스템은 '인적 검증 기반 피드백 선순환(Feedback Loop)' 체계이다. 초기 단계에 배포된 지능형 에이전트의 완성도는 약 60% 안팎에 머무를 수 있다. 이때 작동을 멈추는 것이 아니라, 오류가 발생하거나 품질이 미흡한 40% 영역의 데이터를 사람이 직접 잡아 검수 및 수정한 뒤 이를 피드백 데이터로 변환해야 한다. 변환된 데이터를 정제하여 고품질의 재학습 데이터셋으로 가공하고, 이를 다시 모델 가중치에 강화 학습 기법으로 에이전트를 점진적으로 업데이트하는 영구 순환 구조를 구축해야만 기업들은 장기적으로 인력 부담은 최소화하고 업무 완결성은 극대화하는 생산 가치를 얻을 수 있다.

비용 폭발 문제

실제 비즈니스에 Agentic AI를 도입할 때 기업들이 마주하는 문제는 비용 폭발이다. Agentic AI는 챗봇처럼 API를 몇 번 호출하는 것이 아니라, 목표 달성을 위해서 생각-실행-수정을 무한 반복하면서 엄청난 양의 토큰을 소모하게 된다. 특히 Context Window Inflation이라는 과거 기억이 누적되면서 새로운 경로를 탐색할 때마다 토큰 소모량이 크게 누적되어 늘게 되는 현상이 발생한다. 이런 문제를 해결하기 위해

Anthropic의 경우 Prompt Caching을 활용하고 있는데, 이전 프롬프트의 처리 경과를 임시 저장하는 방법이다. 응답속도와 API 비용을 크게 줄일 수 있는 방법으로 각광받고 있다. Agent의 자유도를 Rule Base도 제한하는 방법도 있다. 특정 프레임워크를 활용해 매번 하는 유사한 작업이나 순서가 있는 작업들을 하나로 묶어 같이 저장하고 룰을 세팅해 순서를 따르게 하는 방식이다. 사고가 필요한 부분만 자유도를 부여해서 토큰 낭비를 기계적으로 차단할 수 있다. 또한, Token Cap 방식도 있다. 토큰 범위를 미리 설정하거나, Agent가 문제를 해결하는 과정에서 에러가 몇 차례 나면 인간 개입을 자동으로 요청하도록 세팅하는 방법을 사용할 수 있다.

현장에서 Agentic AI가 가장 많이 활용되는 분야



비즈니스에서의 Agentic AI 활용 사례

Agentic AI 도입 분야 및 전략

Agentic 분야는 성장 초기. 얼마나 어떻게 연결할까?

1단계 - 비정형 고유 지식 인프라 정비 및 저위험 영역 선제 적용: 먼저 기업이 오랫동안 축적해 온 업무 매뉴얼, 설계서, 법률 약관, 고객 문의 로그 등의 사내 고유 데이터를 유기적으로 정제하여 에이전트가 오독 없이 즉각 활용 가능한 벡터 및 지식 인프라로 전면 재정리한다. 초기 단계에는 실패 비용이 극히 낮고 성과 도출이 단순한 자료 수집 및 리포트 초안 구성 등 낮은 위험도의 작업부터 제한적으로 적용하면서 작업을 확장할 필요가 있다고 본다.

2단계 - 규제는 기술 샌드박스부터: 망분리라는 견고한 보안 규제를 적용받는 한국의 주요 산업군은 물리망 단절 중심의 단순 대처에서 벗어나 무중단 정밀 데이터 활용이 가능한 보안 체계로 전환될 필요성이 부각되고 있다. 정부의 규제 샌드박스 정책을 활용해, 실시간 데이터의 안전한 접근 권한을 에이전트에게 한시적으로 제한된 범위에서 승인한다는 논리를 단계별로 테스팅해 볼 필요가 있다.

3단계 - Human in the Loop: 에이전트 자율성이 아무리 고도화되더라도 예상치 못한 오작동에 따른 책임 한계를 정립하기 위해 인간 관리자의 감시와 승인 절차(Human-in-the-loop)를 기본 프로세스로 정립해야 한다.

4단계 – 인터페이스 연동: 가상 환경에서 동작하는 에이전트들이 외부 3rd Party 소프트웨어들과 법적 및 규격적인 마찰 없이 소통할 수 있도록 사전에 약속된 전용 연동 인터페이스(API)의 규격을 사내 시스템에 마련해야 한다. 에이전트에게 허용되는 데이터 접근 범위를 세밀하게 제어 및 회수할 수 있는 공간으로 통제 가능성을 확보해야 한다.

미국 주요 선도 기업의 Agentic AI 활용 실증 사례

주로 엔터프라이즈 소프트웨어 플랫폼이 자사 제품군에 Agentic AI를 이식하면서 실질적인 매출액 성장과 고정비(대부분 인건비) 절감을 이뤄내고 있다. 사내 축적된 비정형 데이터의 무결성을 선제적으로 극복하고, 안전한 거버넌스 가이드라인 하에 사내 비즈니스 시스템인 ERP 및 CRM과 에이전트를 긴밀하게 결합하는 방식으로 비즈니스 구조를 개선하려고 노력 중이다.

❶ Salesforce: Agentforce라는 Agentic Tool로 자율 에이전트와 데이터 클라우드를 통합했다. 사용자의 질문에 요구사항을 분석하고, 필요한 데이터를 찾아 어떤 행동을 취할지 스스로 판단하고 계획을 세운다. 에이전트가 하지 말아야 할 행동이나 보안 규정을 명확히 설정해서, 민감 정보 접근, 환각 현상 등을 차단한다. 또 실시간 외주 데이터 연동으로 가장 정확하고 최신 데이터를 기반으로 고객에게 정보를 전달한다. Customer Relationship Management 분야인 영업지원/이커머스 전략/마케팅 등에서 혁신적인 서비스라는 평가를 받고 있다.

❷ ServiceNow: 외부 고객 접점 보다는 기업의 내부 관리에 초점을 맞춘 Agentic Service를 출시했다. 기업 내 여러 부서가 공유할 수 있는 데이터베이스를 구축하고 자동화 가능한 업무를 자동화하고 있다. 시스템 장애를 자동 복구, 보안 사고 대응, 앱 생성, 인사 지원 등 여러 분야에서 동시 다발적으로 백엔드 워크플로우 오케스트레이션을 진행하고 있다.

❸ Microsoft: Office와 Window 생태계와 Agent 기능을 통합하고 업무 문서와 메일 기반의 범용적 자율성을 부여한 Agent를 추구한다. 회사의 부서별 전문 Agent, 개발자들을 위한 전용 Agent Builder 등 폭 넓게 Agentic AI 분야를 확장하고 있다.

기업별로 Agentic AI 활용 사례는 생각보다 많이 다르다. 아직 매일 변화하고 발전할 수 있는 분야다. 또 일종의 범용툴로 어떤 분야에서 가장 많은 생산성을 창출할지 시험하는 단계이기 때문에 그렇다고도 본다. 최근 많은 Agentic AI의 영역들이 인간을 돕는 것을 넘어 인간의 루틴한 업무를 대체하면서 Agentic Tool 시장이 커지면 커질수록 사용해줄 고객이 줄어든다는 것은 이 분야의 아이러니이자 숙제로 남을 것으로 본다.