

에이전틱 AI (Agentic AI) 마스터 가이드

- 기업 교육 및 실무 구현을 위한 종합 교육자료 -

[본 과 정 의 핵 심 목 표]

1. 생성형 AI와 에이전틱 AI의 차이를 이해하고 패러다임 전환을 체득합니다.
2. AI 에이전트를 설계하는 4대 핵심 구성 요소와 작동 메커니즘을 학습합니다.
3. 앤드류 응 교수의 4대 디자인 패턴을 통해 완성도 높은 시스템을 기획합니다.
4. 실습 예제를 분석하여 싱글 및 멀티 에이전트의 구현 능력을 배양합니다.
5. 엔터프라이즈 환경에서의 보안, 비용 제어 및 안전 장치 구축 가이드를 습득합니다.

발행처: 한국키네틱코엔지니어링 AI 교육 담당

발행일: 2026년 5월

차 례

1	제1장: 에이전틱 AI 개요 및 필요성	2
1.1	1.1 에이전틱 AI의 정의	2
1.2	1.2 생성형 AI vs 에이전틱 AI 상세 비교	2
2	제2장: 에이전트의 4대 핵심 구성 요소	3
3	제3장: 앤드류 응(Andrew Ng)의 4대 에이전트 디자인 패턴	4
3.1	3.1 자기 성찰 (Reflection)	4
3.2	3.2 도구 사용 (Tool Use)	4
3.3	3.3 계획 수립 (Planning)	4
3.4	3.4 멀티 에이전트 협업 (Multi-Agent Collaboration)	4
4	제4장: 실무 구현 예시 - CrewAI 프레임워크 실습	5
5	제5장: 엔터프라이즈 도입 시 가드레일 및 보안	6
5.1	5.1 Human-in-the-Loop (HITL) 설계	6
5.2	5.2 프롬프트 인젝션 및 보안 대책	6
5.3	5.3 무한 루프 차단 및 비용 절감 설계	6
6	워크숍 학습 평가 및 디스커션	7

1 제1장: 에이전틱 AI 개요 및 필요성

1.1 1.1 에이전틱 AI의 정의

에이전틱 AI(Agentic AI)는 최소한의 인간 감독 하에 스스로 목표를 설정하고, 계획을 수립하며, 필요한 도구를 사용해 복잡한 다단계 작업을 자율적으로 수행하는 인공지능 시스템을 의미합니다. 기존의 AI가 주어지는 질문에 수동적으로 답변하는 보조였다면, 에이전틱 AI는 목표 지향적이고 독자적인 행동력을 지닌 '동료'의 역할을 수행합니다.

1.2 1.2 생성형 AI vs 에이전틱 AI 상세 비교

기존 생성형 AI와의 명확한 비교를 통해 에이전틱 AI의 특성을 이해하는 것이 중요합니다.

표 1: 생성형 AI와 에이전틱 AI 패러다임 비교

구분	생성형 AI (Generative AI)	에이전틱 AI (Agentic AI)
행동 양식	반응형 (Reactive) 사용자의 지시가 있어야 반응	선제적/자율적 (Proactive/Autonomous) 목표가 설정되면 주도적으로 계획하고 실행
작업 방식	단일 턴 (Single-turn) 일회성 프롬프트-답변 구조	반복 루프 (Iterative Loop) 목표 달성 시까지 '사고-행동-관찰' 반복
주요 결과물	텍스트, 이미지 등 미디어 콘텐츠 생성	최종 목적 달성 및 비즈니스 프로세스 완수
도구 활용	거의 없음 (챗봇 UI 내부 지식 한정)	API, DB 쿼리, 웹 브라우징, 내부 서버 제어
자가 성찰	없음 (잘못된 결과도 수정 없이 출력)	스스로 모순이나 에러를 판별하여 자체 수정

강사 코칭 팁

교육생들에게 "기존 ChatGPT는 훌륭한 작가나 조연자라면, 에이전틱 AI는 목표를 던져주면 대신 일처리를 끝마치고 보고하는 유능한 직원"이라는 비유를 사용하면 이해도를 극대화할 수 있습니다.

2 제2장: 에이전트의 4대 핵심 구성 요소

AI 에이전트가 정상적으로 구동하기 위해서는 두뇌, 기억력, 행동 능력, 개성이 유기적으로 조화를 이루어야 합니다.

에이전트 4대 구성 아키텍처

- **1. 프로필 (Profile / Persona):** 에이전트에게 역할(Role)과 성격, 책임 범위를 규정합니다. 프롬프트의 지침(Instruction)에 녹아들며, 에이전트의 페르소나를 명확히 할수록 출력의 일관성이 극대화됩니다.
- **2. 계획 및 추론 (Planning & Reasoning):** 당면한 큰 목표를 하위 목표(Sub-goals)로 쪼개고 실행 순서를 판단하는 능력입니다. *Chain-of-Thought (CoT)*와 *ReAct (Reason + Act)* 기법이 주로 사용됩니다.
- **3. 기억 장치 (Memory):**
 - **단기 기억:** 대화 컨텍스트 내의 정보 교환 기록.
 - **장기 기억:** 외부 벡터 DB나 히스토리 저장을 통해 수 주일, 혹은 수 개월 후에도 핵심 정보와 지식을 유지하고 검색하는 시스템.
- **4. 도구 및 실행 (Tools & Action):** LLM의 내부 매개변수 지식에 의존하지 않고, 외부 검색 엔진, API, 이메일 시스템, 로컬 코드 인터프리터 등 외부 환경과 능동적으로 통신하게 하는 수단입니다.

3 제3장: 앤드류 응(Andrew Ng)의 4대 에이전트 디자인 패턴

세계적인 AI 석학 앤드류 응 교수는 기존 고성능 LLM의 파라미터를 늘리는 대신, 아래 4가지 설계 패턴을 활용하는 것만으로도 성능이 비약적으로 향상된다고 강조하였습니다.

3.1 3.1 자기 성찰 (Reflection)

한 모델이 결과물을 도출하면, 그것으로 끝내지 않고 자가 성찰(Self-Criticism) 프롬프트를 가동하여 도출된 소스코드나 문서의 버그, 어조, 정확성을 재평가합니다. 평가 결과를 반영해 최종 아웃풋을 업데이트하는 과정으로 품질을 수배 이상 증가시킵니다.

3.2 3.2 도구 사용 (Tool Use)

계산기, 지도, 데이터베이스 조회, 파이썬 인터프리터 등 특정 연산이나 외부 조회가 필요할 때 이를 직접 수행할 도구를 호출합니다. LLM이 도구 사용 권한을 판단하고 인자값(Arguments)을 구조화해 넘겨주면, 시스템 백엔드가 이를 실행하여 다시 입력으로 피드백합니다.

3.3 3.3 계획 수립 (Planning)

"A기업의 리스크 요소를 종합 진단해 줘"라는 요청을 분석하여, 다음과 같이 단계별 계획을 스스로 작성하고 순서대로 문제를 해결해 나갑니다. 1단계: A사 최근 뉴스 검색 → 2단계: 재무제표 DB 쿼리 실행 → 3단계: 두 결과 대조 후 요약 보고서 작성. 실행 단계에서 오류가 감지되면 즉시 우회 경로를 수립(Dynamic Replanning)합니다.

3.4 3.4 멀티 에이전트 협업 (Multi-Agent Collaboration)

서로 다른 프로필과 도구를 지닌 에이전트들이 공용 대화창이나 작업 파이프라인에서 데이터를 소통하며 일하는 패턴입니다. 가장 큰 장점은 개별 LLM이 맡은 고유 도메인 범위가 좁혀져 환각 현상(Hallucination)이 극적으로 제어되고 성능이 향상된다는 점입니다.

학습 포인트

과거에는 한 대의 고성능 모델(GPT-4 등)을 잘 학습시키려 노력했으나, 현재 트렌드는 가볍고 저렴한 여러 모델을 앤드류 응 교수의 4가지 에이전트 아키텍처 패턴으로 결합하여 저비용 고성능을 추구하는 방향으로 선회하고 있습니다.

4 제4장: 실무 구현 예시 - CrewAI 프레임워크 실습

이 장에서는 Python 환경에서 멀티 에이전트를 조율하는 대표적인 오픈소스 프레임워크인 **CrewAI**를 사용하여, '시장 조사 및 기술 콘텐츠 뉴스레터 작성' 작업을 자율 수행하는 소스코드를 살펴봅니다.

```
1 import os
2 from crewai import Agent, Task, Crew, Process
3 from crewai_tools import SerperDevTool
4
5 # 1. API ( )
6 os.environ["OPENAI_API_KEY"] = "your-openai-api-key"
7 os.environ["SERPER_API_KEY"] = "your-serper-api-key"
8
9 search_tool = SerperDevTool()
10
11 # 2.
12 researcher = Agent(
13     role=" (Senior Market Researcher)",
14     goal="IT .",
15     backstory=""" .
16     , .""",
17     verbose=True,
18     allow_delegation=False,
19     tools=[search_tool]
20 )
21
22 writer = Agent(
23     role=" (Tech Content Writer)",
24     goal=" .",
25     backstory=""" IT .
26     .""",
27     verbose=True,
28     allow_delegation=False
29 )
30
31 # 3. (Task)
32 research_task = Task(
33     description=""" 6 AI 3 .""",
34     expected_output=" , , ()",
35     agent=researcher
36 )
37
38 write_task = Task(
39     description=""" .""",
40     expected_output=" , ( ), ()",
41     agent=writer
42 )
43
44 # 4. (Crew)
45 tech_news_crew = Crew(
46     agents=[researcher, writer],
47     tasks=[research_task, write_task],
48     process=Process.sequential,
49     verbose=True
50 )
51
52 if __name__ == "__main__":
53     result = tech_news_crew.kickoff()
54     print(result)
```

Listing 1: CrewAI 기반 시장 조사 및 콘텐츠 발행 자동화 코드

5 제5장: 엔터프라이즈 도입 시 가드레일 및 보안

실무 및 상용 비즈니스 환경에 에이전트를 연동할 때 주의해야 하는 엄격한 보안과 통제 가이드라인을 학습합니다.

5.1 5.1 Human-in-the-Loop (HITL) 설계

에이전트에게 완전한 자율성을 주었을 때 발생할 수 있는 사고를 최소화하기 위해 결제, 발송, 데이터 영구 삭제 등 되돌릴 수 없는 결정(Irreversible Actions)에 임하기 전에는 반드시 인간 감독관의 승인을 거치게 설계해야 합니다.

추론 및 초안 작성(AI) → 검증 및 확인(AI) → 최종 승인(Human) → 실행 및 배포(AI)

5.2 5.2 프롬프트 인젝션 및 보안 대책

* 최소 권한 원칙 (Principle of Least Privilege): 에이전트에 연동하는 API Key와 데이터베이스 계 정에는 절대 Admin/Write 권한을 일괄 부여하지 말고, 오직 필요한 목적에 부합하는 최소 권한(예: 특정 테이블의 Read-only 권한)만 할당합니다. * 샌드박스 인프라: 에이전트가 로컬 파일에 접근하거나 임의의 코드를 실행해야 하는 경우, 무조건 격리된 도커(Docker) 컨테이너 내부 환경에서만 구동되도록 물리적인 통제 레이어를 배치합니다.

5.3 5.3 무한 루프 차단 및 비용 절감 설계

* 토큰 버스트 방지: 자가 성찰 루프나 에러 복구 구문에서 논리적 모순으로 인해 에이전트가 종료되지 않고 계속 연산을 요구하는 무한 루프에 빠질 수 있습니다. * 해결 방안: API 호출 시 반드시 최대 반복 제한(Max Iterations) 수치를 설정하고 타임아웃(Timeout) 및 단기 세션 한도 예산을 하드코딩 형태로 이중 제어해야 합니다.

6 워크숍 학습 평가 및 디스커션

본 교육을 마무리하며 아래 질문을 바탕으로 팀별 토론 및 발표를 진행합니다.

1. **[토론 주제 1]** 여러분의 현재 현업 워크플로우(예: 인사팀 채용 검토, 영업 지원, 서버 장애 대처 등) 중에서 가장 먼저 에이전틱 AI로 전환했을 때 투자 대비 가치(ROI)가 높은 영역은 어디이며, 그 이유는 무엇입니까?
2. **[토론 주제 2]** 해당 업무에 멀티 에이전트 시스템을 적용한다고 가정했을 때, 필요한 개별 에이전트의 역할(Profile)은 무엇이며, 어떤 외부 도구(Tools)가 정의되어야 할지 아키텍처를 스케치해 보세요.
3. **[퀴즈]** 앤드류 응 교수가 제시한 4대 디자인 패턴 중 에이전트가 도출한 코드나 아웃풋의 버그와 결함을 스스로 검수하여 답변의 완성도를 자체적으로 끌어올리는 기술 패턴의 명칭은 무엇입니까?
(정답: 자기 성찰 / Reflection)

- 에이전틱 AI 완벽 가이드 교육 과정 이수를 축하드립니다. -