

ChatGPT 에이전트 초보자 매뉴얼

1. ChatGPT 에이전트란 무엇인가?

ChatGPT 에이전트는 기존 챗봇과 달리 **가상 컴퓨터**를 이용해 사용자를 대신하여 복잡한 작업을 수행하는 인공지능 비서입니다. 이 에이전트는 세 가지 첨단 기능을 결합한 **통합 시스템**으로 이루어집니다. Operator의 웹 사이트 상호작용 능력과 심층 리서치의 정보 분석 능력, 그리고 ChatGPT의 대화·추론 능력이 하나로 합쳐져서 사용자가 요청한 작업을 처음부터 끝까지 자동으로 처리합니다 ¹. 예를 들어 경쟁사 분석 후 슬라이드를 만들거나, 최근 뉴스에 기반해 미팅을 준비하는 것 같은 복잡한 작업도 스스로 수행할 수 있습니다 ².

친구처럼 설명하기

생각보다 간단합니다. 여러분이 “슬라이드쇼 만들어 줘”라고 명확히 지시하면, 이 에이전트는 알아서 웹사이트를 찾아보고, 필요한 정보를 정리하고, 슬라이드까지 만들어 줍니다. 여러분은 중간에 확인하면서 수정 지시를 내릴 수 있고, 원하는 대로 멈추거나 다시 시작할 수도 있죠.

2. 사용 준비

2.1 구독 및 지역 확인

ChatGPT 에이전트는 유료 구독자에게만 제공됩니다. **Plus, Pro, Team** 플랜 사용자라면 바로 사용할 수 있으며, 각 플랜마다 월별 에이전트 메시지 한도가 다릅니다 ³. 현재 **유럽경제지역(EEA)**과 **스위스에서는 사용할 수 없고**, 그 외 대부분 국가에서 사용할 수 있습니다 ⁴.

2.2 기술 요구 사항

- 최신 웹 브라우저(Chrome, Edge, Safari, Firefox 등)와 **안정적인 인터넷 연결**이 필요합니다 ⁵.
- 모바일 앱(iOS/Android) 또는 데스크톱 앱(Windows/macOS)에서 사용할 수 있으며 별도의 하드웨어는 필요하지 않습니다 ⁵.

3. ChatGPT 에이전트 시작하기

3.1 에이전트 모드 활성화

에이전트 모드를 켜는 방법은 두 가지가 있습니다:

1. 도구 드롭다운 사용 ⁶
2. ChatGPT 대화창을 열고 메시지 작성 영역 옆의 **도구 드롭다운**을 클릭합니다.
3. 드롭다운 목록에서 “**에이전트 모드**”를 선택하면 곧바로 활성화됩니다.
4. 명령어 사용 ⁷
5. 입력창에 `/agent` 라고 입력하고 `Enter` 를 누르면 즉시 에이전트 모드로 전환됩니다.

선호하는 방법을 선택하면 되며, 활성화되면 “에이전트 모드가 실행되었습니다”라는 안내 메시지가 나타납니다.

3.2 에이전트 설정

에이전트를 처음 사용할 때 몇 가지 설정을 해주면 작업 효율을 높일 수 있습니다.

1. 커넥터 설정 ⁸

2. 설정 > **데이터 컨트롤** 메뉴에서 Gmail, GitHub, Google Drive 등 연결하고 싶은 서비스를 선택합니다.
3. 각 서비스가 요청하는 권한을 확인한 뒤 동의하면 ChatGPT가 여러분의 데이터에 접근해 자동화 작업을 수행할 수 있습니다.

4. 개인 정보 보호 설정 ⁹

5. “모델 개선을 위해 데이터 사용” 옵션을 켜지 선택합니다. 끄면 대화 기록이 모델 개선에 사용되지 않습니다.
6. **스크린샷 보존**과 **브라우저 데이터 삭제** 설정을 확인하여 원하는 수준의 프라이버시를 유지하세요. 필요할 때 언제든지 변경할 수 있습니다.

팁: 커넥터를 설정해두면 Gmail에서 메일을 가져와 요약하거나, Google Drive 문서를 자동 정리하는 등 업무 자동화의 폭이 크게 넓어집니다 ¹⁰.

4. 작업 생성과 프롬프트 작성

4.1 프롬프트 작성 요령

에이전트에게 일을 시키려면 **구체적이고 단계별 지시**를 주는 것이 중요합니다. 예를 들어 프로젝트 관리 도구를 비교 조사하려면 다음처럼 상세히 지시합니다:

“팀 규모 10~20명이 쓸 수 있는 프로젝트 관리 도구 5개를 조사해 주세요.
각 도구에 대해 **월별 가격**, **핵심 기능**, **Slack/Google Workspace 연동 여부**, **장점과 단점**을 비교표로 만들어 주세요.
무료 평가판을 제공하는 도구에 중점을 두세요.” ¹¹

반대로 “**프로젝트 관리 도구 찾아줘**” 처럼 모호한 지시는 원하는 결과를 얻지 못할 가능성이 큼니다 ¹².

4.2 사용할 수 있는 도구들

에이전트는 작업을 수행하기 위해 여러 도구를 자유롭게 결합해 사용합니다:

- **시각적 브라우저:** 사람처럼 웹사이트를 클릭, 스크롤, 입력하여 양식 작성·예약 등 상호작용을 수행합니다 ¹³.
- **텍스트 기반 브라우저:** 많은 양의 웹 콘텐츠를 빠르게 읽고 추론할 때 사용합니다 ¹⁴.
- **터미널:** 코드 실행이나 파일 처리 등 명령줄 작업이 필요할 때 사용합니다 ¹³.
- **API 호출:** 캘린더, 메일 등 외부 앱의 데이터를 직접 받아올 때 활용합니다 ¹⁰.

이 도구들은 모두 가상 컴퓨터 안에서 작동하며, 에이전트가 상황에 따라 가장 효율적인 조합을 선택합니다. 예를 들어 캘린더 정보는 API로 가져오고, 보고서 작성은 텍스트 브라우저로 조사한 뒤, 결과를 시각적 브라우저로 슬라이드에 편집할 수 있습니다 ¹⁵.

4.3 작업 진행과 개입

에이전트가 작업을 시작하면 **실시간으로 모든 행동이 기록**되고, 브라우저 화면과 진행 상태를 확인할 수 있습니다 ¹⁶. 화면 오른쪽에는 진행률 표시 막대가 나타나며, 어떤 웹사이트를 방문했고 어떤 동작을 했는지 설명이 함께 나타납니다

¹⁶.

작업 도중에는 언제든지 다음과 같은 제어를 할 수 있습니다 ¹⁷ :

- **일시정지(Pause)**: 잠시 멈춰 현재까지의 진행 상황을 확인할 수 있습니다.
- **인터럽트(Interrupt)**: 현재 작업을 중단하고 추가 지시사항을 입력합니다.
- **브라우저 인수(Take over)**: 민감한 정보를 입력하거나 직접 조작하고 싶은 경우에 사용합니다. 인수 중에는 입력한 내용이 기록되지 않으며, 완료 후 “**제어권 반환**” 버튼을 눌러 에이전트에게 다시 작업을 맡길 수 있습니다

¹⁸ .

5. 민감한 정보 처리와 보안

에이전트는 보안을 위해 **암호, 신용카드 번호** 등 민감한 정보를 직접 입력하지 않습니다. 이런 정보가 필요할 때는 반드시 **브라우저 인수** 기능을 사용하여 사용자가 직접 입력해야 합니다 ¹⁹ . 입력한 데이터는 기록되지 않고 바로 전달되므로 안심할 수 있습니다. 또한, ChatGPT 인터페이스에는 개인 정보를 직접 남기지 말고 필요한 경우 항상 인수 기능을 통해 입력하세요 ¹⁹ .

6. 자주 발생하는 문제와 해결법

6.1 에이전트 모드가 보이지 않을 때 ²⁰

1. **구독 확인**: Pro, Plus 또는 Team 플랜인지 확인합니다.
2. **지역 제한 확인**: 현재 EEA나 스위스에 있지 않은지 확인합니다.
3. **메시지 한도 확인**: 월간 에이전트 메시지 한도를 초과하지 않았는지 점검합니다.
4. **브라우저 새로고침** 혹은 **앱 재실행** 후 다시 시도합니다.
5. 문제가 계속되면 브라우저 캐시와 쿠키를 삭제하고 다시 로그인합니다.

6.2 작업이 너무 오래 걸리는 경우 ²¹

- 복잡한 요청일수록 시간이 오래 걸릴 수 있습니다. 작업이 멈춘 것 같으면 **일시정지** 후 상태 업데이트를 요청하세요.
- 작업을 더 작은 단계로 나누어 순차적으로 요청하는 것이 효과적입니다.
- 자동화가 아닌 **RPA 도구**가 적합한지 검토해 볼 수 있습니다.

6.3 로그인 문제 ²²

- 모든 로그인은 **브라우저 인수** 기능을 통해 사용자가 직접 해야 합니다.
- 로그인 후에도 문제가 지속된다면 브라우저 데이터를 지우고 다시 시도해 보세요.
- 커넥터 권한을 올바르게 설정했는지 확인합니다.
- 자동화 방지 정책이 있는 일부 웹사이트는 에이전트 접근을 막을 수 있습니다.

6.4 원하는 결과를 얻지 못할 때 ²³

- 지시를 더 **구체적으로** 작성하고, 필요한 경우 원하는 출력 예시를 함께 제시하세요.
- 복잡한 요청을 여러 단계로 나누어 각각 처리하게 하는 것이 좋습니다.
- AI가 적합하지 않은 작업은 없는지(특정 RPA 도구가 더 적합한지) 검토하세요.

7. 에이전트를 잘 사용하는 팁

7.1 반복 작업 자동화

에이전트는 **정기적인 작업을 자동으로 예약**할 수 있습니다 ²⁴ . 예를 들어 주간 실적 보고서 작성, 경쟁 정보 수집, 일정 분석 등 반복되는 업무를 매주 일정한 시간에 실행하도록 설정해두면 큰 도움이 됩니다.

7.2 커넥터 활용

Gmail, Google Drive, Slack 등과 연결하면 업무·개인 생활에서 다양한 자동화가 가능합니다. 예를 들어 Gmail과 연동해 **24시간 이내 긴급 이메일 요약**을 하거나, Google Drive에서 특정 스프레드시트를 모아 **요약 레포트**를 만드는 등 생산성이 크게 향상됩니다 ²⁴.

7.3 안전한 사용과 주의사항

- ChatGPT 에이전트는 사용자 확인 없이 중요한 행위를 하지 않으며, **프롬프트 인젝션**과 같은 악성 공격을 감지하고 위험을 안내합니다 ²⁵.
- 민감한 업무에는 단계별 승인 절차가 필요하며, 거래나 법적 상호작용 등 위험도가 높은 작업은 거부될 수 있습니다 ²⁶.
- 원격 브라우저 데이터를 서버에 저장하지 않으며, 세션 제어권과 데이터 삭제 권한은 사용자에게 있습니다 ²⁷.

8. 활용 예시

8.1 업무용

상황	에이전트 사용 방법
프레젠테이션 생성	“우리 회사의 3분기 매출 데이터를 분석하여 슬라이드 5장으로 요약해줘. 그래프는 2개 이상 포함하고, 파란색 테마를 사용해줘.”라고 지시하면, 에이전트가 데이터를 분석하고 시각적으로 깔끔한 프레젠테이션을 만들어 줍니다 ²⁸ .
일정 조정	“다음 주 월요일 팀 회의를 오후 3시에서 오후 4시로 변경해 줘. 모든 참석자에게 이메일 공지를 보내줘.”라고 요청하면 캘린더와 이메일을 연동해 일정을 조정하고 참석자에게 자동 공지 메일을 발송합니다 ²⁸ .
재무 데이터 업데이트	“구글 드라이브의 ‘재무자료.xlsx’ 파일을 열어 각 항목의 수익을 합산하고, 새 시트에 요약표를 만들어줘.”라고 지시하면 수치 계산과 표 작성까지 완료합니다 ²⁸ .

8.2 개인 생활

상황	에이전트 사용 방법
여행 계획 및 예약	“9월 말 3박 4일로 도쿄 여행을 계획해줘. 항공과 숙소를 예약하고, 가족친화적인 관광 일정과 맛집을 추천해줘.”라고 요청하면 교통편 검색, 숙소 예약, 일정 정리까지 진행합니다 ²⁹ .
이벤트 기획	“다음 달 친구 생일 파티를 기획해줘. 10명 규모의 식사 장소와 케이크 예약, 그리고 초대 메시지를 작성해줘.”라고 지시하면 에이전트가 장소 예약과 일정 조율, 초대장 작성까지 대신합니다 ²⁹ .

9. 마무리 조언

ChatGPT 에이전트는 **자동화된 개인 비서**이지만, 사용자의 감독과 책임 아래에서 가장 잘 작동합니다. 에이전트가 모든 것을 알아서 할 수 있지만, 여러분이 원하는 방향으로 정확히 수행하려면 **명확하고 세부적인 지시**가 필요합니다. 또한 민감한 정보는 직접 입력해야 하며, 진행 상황을 수시로 확인하여 필요할 때 수정 지시를 내려야 합니다.

정리하면, 구독과 기술 요건을 확인하고, 도구 드롭다운 혹은 `/agent` 명령으로 에이전트를 활성화한 뒤, 명확한 지시와 커넥터 설정을 통해 복잡한 작업을 자동화해보세요. 에이전트가 제공하는 실시간 모니터링과 안전 제어 기능을 활용하면 더 안전하고 효율적으로 일을 처리할 수 있습니다.

1 3 4 5 6 7 8 9 11 12 16 17 18 19 20 21 22 23 24 OpenAI의 ChatGPT 에이전트 사용 방법:

단계별 가이드 - Unite.AI

<https://www.unite.ai/ko/how-to-use-openais-chatgpt-agent-a-step-by-step-guide/>

2 25 26 27 28 29 ChatGPT 에이전트, 리서치와 액션을 연결합니다 | GeekNews

<https://news.hada.io/topic>

10 13 14 15 ChatGPT 에이전트 소개: 연구와 실행의 연결 | AI 한국어 자료 도서관 by 공부하우

<https://library.gongbuhow.com/docs/openai/news/introducing-chatgpt-agent/>