

CONNECT 3회차 · 100분

에이전트와 도구

담당자를 만들고, 도구를 붙이고, 범위를 정하기

여는 말

- 이 회차가 Connect 트랙의 핵심입니다. 실습이 많습니다.
- 100분 중 40분이 실습입니다. 설명이 길어지면 실습이 잘리니 시계를 보세요.
- 참석자가 2회차에서 만든 워크스페이스에 들어와 있는지 먼저 확인하세요.

다섯 종류

언제 무엇을 쓰나

01

서브 에이전트

같은 유형의 요청을 반복할 때

02

MCP 서버

외부 도구 묶음을 통째로

03

HTTP · CLI 액션

API 하나 · 명령 하나

04

시스템

내 컴퓨터의 실제 파일 작업

05

공개 범위

누가 볼 수 있는가

06

활성화

지금 쓸 수 있는가

서브 에이전트부터 시작하세요. 외부 연결 없이 지시문만으로 만들 수 있습니다.

에이전트 종류

- 공개 범위와 활성화는 다른 축입니다 — 비공개+켜짐(다듬는 중), 공개+꺼짐(잠시 내림).
- 지우는 대신 비활성화하면 설정과 이력이 남습니다.

실습 · 15분

서브 에이전트 만들기

1

반복하는 요청 고르기

같은 형식의 문서, 같은 기준의 검토

2

지시문 쓰기

역할 · 규칙(하지 말 것) · 형식

3

비공개로 시험

몇 번 써보고 지시문을 다듬기

4

공개 + 알리기

만들어두고 안 알리면 아무도 모릅니다

결과가 안 좋으면 대화에서 보정하지 말고 지시문 자체를 고치세요. 그래야 다음에도 적용됩니다.

실습

- 20분 잡으세요. “회의록 정리 담당자”를 예시로 함께 만들면 좋습니다.
- 지시문의 규칙은 전부 “하지 말 것”으로 적으라고 하세요.
- 한 에이전트에 여러 가지를 시키지 마세요. 하나에 하나씩입니다.

도구 붙이기

MCP 연결에는 두 방향이 있습니다

- 안에서 밖으로 — 외부 MCP 서버를 워크스페이스에 붙이기 (대부분 이것)
- 밖에서 안으로 — Claude Code 등이 이 워크스페이스를 도구로 쓰기
- 붙인 도구는 에이전트 목록에 APP으로 올라옵니다

토큰은 최소 권한으로 발급하세요. 넓게 주고 좁히는 건 실제로 잘 안 일어납니다.

MCP

- 서버 하나가 도구 25개를 가져올 수 있습니다. 전부 켜둘 필요 없습니다.
- 쓰지 않는 도구를 끄는 것은 절약이자 정확도 개선입니다.

시스템

내 컴퓨터 연결하기

- 시스템 하나가 컴퓨터 한 대입니다
- 설치 → 시스템 등록 → 토큰을 컴퓨터 쪽에 붙여넣기
- 등록 자체는 무료. 터널(외부 주소 노출)이 유료 부가 기능

tt_ 토큰 하나가 그 컴퓨터에 대한 접근 권한입니다. 채팅방에 붙여넣지 마세요.

시스템

- 등록하는 순간 워크스페이스 멤버가 그 컴퓨터에 작업을 시킬 수 있습니다.
- 그 컴퓨터의 작업 폴더 범위를 먼저 확인하라고 반드시 말하세요.

자리와 주소는 별개입니다

무엇

시스템 등록 · 업무 맡기기

몇 대든

첫 1대 연결

자리 하나

두 번째 컴퓨터부터

자리 추가

외부 주소(터널)

서브도메인 / 내 도메인

상태

시스템 등록 · 업무 맡기기

✓ 무료

첫 1대 연결

✓ 무료

두 번째 컴퓨터부터

✓ 유료 — 부족하면 대기로 밀림

외부 주소(터널)

✓ 슬롯 하나가 주소 하나

대기로 밀려도 기록과 설정은 그대로 남습니다. 자리를 늘리면 그 자리에서 이어집니다.

자리와 주소

- 서브도메인 슬롯이 남아 있어도 내 도메인은 못 붙입니다 — 별개의 슬롯입니다.
- 태그는 위치나 사양이 아니라 역할로 묶으세요. 그래야 태그로 업무를 보낼 수 있습니다.
- 안 쓰는 컴퓨터가 자리를 잡고 있으면 그만큼 비용입니다. 분기 점검 항목에 넣으세요.
- 폐쇄망(onprem) 설치본에는 자리도 공개 주소도 없습니다 — 화면 자체가 다릅니다.

도구 정리

안 쓰는 도구를 끄는 것은 정확도 개선입니다

01

~10개

문제 없음

02

10~30개

이름과 설명이 좋으면 괜찮음

03

30개 이상

정리를 권합니다 — 비슷한 게 여럿이면 잘못 고릅니다

04

“언젠가 쓸지도”

끄는 쪽입니다. 필요해지면 그때 켜면 됩니다

설정 → 채널 → MCP에서 정합니다. 켜져 있다는 것은 지금 쓸 수 있다는 뜻입니다.

도구 켜고 끄기

- 비용보다 정확도가 더 아픕니다. 후보가 줄면 잘못 고를 확률이 낮아집니다.
- 내장 도구도 목록에 있습니다 — 웹 · 드라이브 · 웹뷰 · 시스템 작업 폴더 · 스레드 메모 · 위임.
- 결과가 1만 자를 넘으면 앞 2천 자만 남기고 원문은 보관합니다. 버리는 게 아니라 필요하면 다시 읽습니다.
- 분기 점검에서 가장 흔히 나오는 문제는 자격증명이 만료된 연결입니다.

모델의 판단을 빼고 도구만 남긴 자리

대화

도구를 고르는 주체

모델

인자를 정하는 주체

모델

실패했을 때

원인이 섞임

쓰는 목적

일을 시킴

플레이그라운드

도구를 고르는 주체

✓ 나

인자를 정하는 주체

✓ 나

실패했을 때

✓ 도구 문제로 확정

쓰는 목적

✓ 확인

도구를 붙인 직후에는 대화가 아니라 여기서 먼저 시험하세요. 자격증명 만료 확인에도 씁니다.

플레이그라운드

- 인자 입력란은 도구 정의에서 자동으로 만들어집니다. 필수 인자도 표시됩니다.
- 여기서도 실제로 실행되고 사용량에 잡힙니다 — 발송·삭제·결제 도구는 시험이라도 조심하세요.
- 결과 크기를 미리 볼 수 있어서, 덜어내기에 걸릴 도구인지 판단할 수 있습니다.

드라이브

읽히려고 두는 것과 고쳐지려고 두는 것

드라이브

어디에
클라우드

무엇을
참조할 자료

에이전트가
읽어서 답변에 씀

HyperTeams 작업 폴더

어디에
✓ 내 컴퓨터

무엇을
✓ 실제로 고칠 파일

에이전트가
✓ 고치고 만듦

“봐도 되는 사람”과 “물어보면 답에 달려 나올 사람”은 같습니다. 권한은 개인이 아니라 부서로 주세요.

드라이브

- 올린 문서는 조각으로 나뉘어 색인되고 답변의 근거가 됩니다. 단순 저장이 아닙니다.
- 올리기 전 가장 놓치기 쉬운 확인 — 어느 채널에서 이 파일에 닿을 수 있는가.
- 검색 범위는 워크스페이스 기본 · 에이전트별 · 채널별로 따로 정합니다. 채널별이 특히 중요합니다.
- 좋은 후보는 “자주 참조되고 바깥에 나가도 되는 것”입니다.

쌓아두고 떠나는 자리

스레드 여러 개

실행

동시에

내가 할 일
각각 시작

쓰는 때
서로 무관한 일

예약

—

큐

실행

✓ 하나씩 순서대로

내가 할 일

✓ 쌓아두고 떠나기

쓰는 때

✓ 순서가 있거나 한꺼번에 던질 때

예약

✓ 크론 식으로 시간에 맡김 (`0 9 \* \* \*`)

파일을 고쳐야 하면 HyperTeams 예약, 자료를 조회해 정리하는 것이면 Connect 예약입니다.

큐와 예약

- 항목마다 에이전트·모델·그룹·공개 범위·제외할 도구를 따로 정할 수 있습니다. 안 정하면 기본값입니다.
- 재시도에는 반드시 지시를 함께 주세요 — 그냥 재시도하면 같은 방식으로 또 실패합니다.
- 아무도 안 볼 때 도는 것이므로 “틀린 결과를 내는 것보다 안 하고 알리는 게 낫다”를 지시문에 넣으세요.
- 끝난 프로젝트의 예약이 계속 도는 것이 가장 흔한 낭비입니다. 분기마다 정리하세요.

채널

밖에서 들어오는 길은 넷입니다

01

이메일 에이전트

메일만 쓰는 사람. 주소를 아는 누구나 보낼 수 있습니다

02

채팅 위젯

우리 사이트 방문자. 사이트에 온 누구나

03

API 키

다른 시스템·스크립트

04

MCP

외부 도구 / 외부 AI가 이 워크스페이스를 도구로

팀원에게는 채널이 필요 없습니다. 채널은 계정이 없는 사람과 시스템을 위한 것입니다.

채널

- 공통 설정이 같습니다 — 담당 에이전트 · 기본 그룹 · 쓸 수 있는 도구 · 추가 지시문 · 모델 · 컴/꿈.
- “쓸 수 있는 도구”를 반드시 좁히세요. 바깥에서 들어오는 길이라 워크스페이스의 모든 도구가 열려 있으면 위험합니다.
- 열기 전 확인 — 이 워크스페이스에 사내 문서가 연결돼 있나. 있으면 채널용 워크스페이스를 나누세요.

열기 전에 반드시 거는 제한

이메일 에이전트

누가 보내나

주소를 아는 누구나

1순위 제한

보낸 사람 · 도메인 허용 목록

처음 설정

자동 답장 끄고 시작

개인정보

첨부에 달려 옵니다

채팅 위젯

누가 보내나

✓ 사이트에 온 누구나

1순위 제한

✓ 허용 도메인 (키는 소스에 노출됩니다)

처음 설정

✓ 분당 요청 제한 걸기

개인정보

✓ 이메일 수집을 켜면 보관 책임이 생깁니다

공개 창구의 지시문에는 약속하는 말을 막으세요 — 할인·계약 조건. 나간 말은 회사가 한 말이 됩니다.

밖으로 여는 두 창구

- 이메일 주소는 ``<핸들>.<에이전트>@...`` 형태라 핸들을 바꾸면 기존 주소가 끊깁니다.
- 자동 답장을 처음에 꺼두면 어떤 메일이 들어오고 에이전트가 어떻게 답하려 하는지 먼저 볼 수 있습니다.
- 용도별로 에이전트를 나누세요 — 계약서 담당에 웹 검색은 필요 없습니다.
- 결과 스레드는 별도 그룹으로 모으세요. 사내 대화와 섞이면 공개 범위 사고가 납니다.

데이터베이스 붙이기

PostgreSQL · MySQL · SQLite · MongoDB — 연결 문자열의 스킴으로 종류를 판별합니다

01

읽기

db_list_tables · db_describe_table · db_select

02

원시 질의

db_query — 받은 SQL 을 그대로 실행합니다. 조회 전용이 아닙니다

03

되돌릴 수 없음

db_insert · db_update · db_delete

04

연결

db_connect — 마지막 사용 후 30분에 정리됩니다

쓰기 도구를 다 꺼도 db_query 하나면 쓰기가 됩니다. 막는 것은 도구 설정이 아니라 읽기 전용 계정입니다.

데이터베이스

- 가장 중요한 한 줄: 도구를 끄는 것보다 읽기 전용 계정이 확실합니다. 지키는 주체가 다릅니다.
- 운영 DB 대신 복제본을 붙이라고 권하세요.
- 외부 입력 경로(위젯·채널·메일)가 같은 워크스페이스에 있으면 읽기 전용은 선택이 아니라 조건입니다.
- 연결 문자열에는 비밀번호가 들어 있습니다 — 대화창에 붙여넣지 않게 하세요.

실습 · 25분

예약을 하나 걸어보기

1

대기로 먼저

한 번만 도는 것으로. 실행 시각이
의도한 시각인지

2

반복으로

일시 정지가 삭제가 아님을
눌러서 확인

3

일부러 실패

없는 자료를 가리키게 하고 무엇이
남는지 봅니다

4

정리

실패 시 동작을 지시에 넣고
연습용은 끝니다

빈 표를 만들어 정상 완료로 처리하거나 숫자를 지어내면, 사람이 보는 작업과 달리 아무도 못 잡습니다.

실습 진행

- 첫 예약은 밖으로 나가지 않는 업무로 잡게 하세요. 시각이나 범위가 어긋나는 게 첫 예약의 기본값입니다.
- 3단계를 건너뛰면 이 실습은 한 게 아닙니다.
- “사람이 볼 때는 사람이 멈춥니다. 예약은 그럴 사람이 없습니다” — 이 문장을 그대로 쓰세요.