C30 무료 특강 수업 자료 키트 · 지피티쌤 (본편 6수업 · 총 26분 32초)

AI 비서에게 메일과 결제를 맡기기 전에 알아야 할 점검표 & 안전 지시문

2026-11-13 (03:20~05:47 KST) 단일 위임 기록(대화 DB 108행 · 완료 응답 42건 · 기록 step 합계 321) · 4개 분석 도구 교차 기록 기준

- **강좌명**: `[무료 특강] AI 비서에게 메일과 결제를 맡기기 전 15분 점검 — 42회 실행 실측으로 본 연결·한도·보안 경계` (`C30` · 최종 제목 사용자 확정 전)
- **강사**: 지피티쌤 (본편 6수업 · 총 26분 32초)
- **측정 기준일**: `2026-11-13` (`03:20~05:47 KST`, 한 번의 2시간 27분 연속 위임 기록: 대화 DB 108행 · 완료 응답 42건 · 기록된 `stepN` 합계 321 · 4개 도구 교차 기록 기준)
- **확인 수준 표기 원칙**: 본 자료는 원 시스템 화면·사업자 장부·로컬 DB·공개 코드로 **직접 확인**한 사실, 로컬 수치로 역산한 **추정**, 그날 대화창 속 **피클의 말**(발언 기록 자체만 확인), 네 도구 모두 **확인하지 못한 영역**을 엄격히 구분하여 적습니다.

1. 한눈에 보는 2026-11-13 실측 핵심 지표 요약

구분	측정 항목	실측 수치 및 사실	확인 수준 · 출처 도구
전체 기록 단위	대화 거울 DB · 완료 응답	단일 세션 `108행` (`user 38` · `assistant 65` · `agent_request 5`, `760` · `861` 결번 / `Cursor` · `Antigravity` · `Claude`), 그중 완료 응답 `42건` (`S01~S42`) · 식별자 `stepN` 숫자 합계 `321` (`Codex` 보고서 65단계와는 세는 단위가 다름; 서버 과금 원장 일치 여부는 **미확인**)	직접 확인 (`Antigravity` · `Cursor` · `Claude`)
네트워크 경로	맥 로컬 `Cache.db` (`04:06~05:45`)	총 `242건` — 자격증명 로그 S3 `138건` + 백엔드 API `104건`, 네이버 메일·IMAP 직접 호스트 `0건` (`03:20~04:06` 구간은 캐시 파일 밖)	직접 확인 (`Antigravity` · `Cursor`)
연결 소요	네이버 메일 첫 연결 (`03:20→03:46`)	약 `26분` 소요 — 비밀번호 입력 · 아이폰 알림 허용 · 2단계 인증 승인 · 고객확인제도 실물 아이폰 카메라 촬영 개입	직접 확인 (`Claude` · `Antigravity`)
한도 소모	새벽 4시 초기화 전후 사용량	`03:49` `43~44%` (`115 step` 구간) → `04:00` 초기화 후 `206 step` 누적 시 `05:46` 최종 `53%` 기록 (`04:23` `13%` · `04:38` `34%` 중간 화면은 `Claude` 스틸 근거)	직접 확인 (`Claude` 화면 · `Antigravity` DB)
스텝 당 무게	`04:00` 이후 선형 역산 비율	`206 step = 53%` 기준 `1 step ≈ 0.257%p` (`100% ≈ 385~390 step`). 단, 과금 원장 미열람 및 동일 `50 step`에서 `13%` · `14%` 표시 사례 존재	**추정** (`Antigravity` 역산 · 한계 명시)
장부 오판	본계정 월 30만 원 구독 결제수단	피클은 개인카드로 보고 삭제 후 법인카드 변경을 권유하며 카드 입력창(`835`)을 띄웠으나, 사업자 장부 대조 결과 **이미 법인카드**였음(카드 미입력)	직접 확인 (`Claude` 장부 · `Antigravity` DB)
금고 · 평문 구분	로컬 DB · 공개 코드 · 피클 답변 분리	① 로컬 대화 DB 본문에는 보안 카드 입력 암호 원문 미저장(`Antigravity` **직접 확인**). ② 공개 커밋 (`cff16a34...`)에는 감사 기록 후 비밀 필드를 작업자에게 넘기는 `release` 경로와 최대 `30일` 위임 상한 존재(`Codex` **직접 확인**, 현행 배포 동일성은 **미확인**). ③ `05:05` 입력 프로세스 평문 취급 등 5차례 정정은 대화창 속 **피클의 말**(운영 백엔드 내부 처리를 직접 검증한 것 아님)	직접 확인 / 공개 코드 / 피클의 말 분리
세션 잔존	로그아웃 보고 뒤 원 서비스 확인	`05:20` 로그아웃 완료 보고(**피클의 말**) 뒤에도 `05:26` 구글 `[내 기기]`에 `Linux · Google Chrome` `[로그아웃]` 버튼 생존 → `05:30` 수동 종료	직접 확인 (`Claude` 화면)

2. 단계별 15분 실전 점검 체크리스트 (Before · During · After)

[Before] 계정 연결 전 3분 준비 — 26분 병목 예방

☐ **휴대폰 시스템 알림 + 메일 앱 내부 알림 동시 ON 확인**: 둘 중 하나라도 꺼져 있으면 2단계 인증 푸시가 오지 않아 AI와 재발송 대화를 반복하며 스텝을 소모합니다.

☐ **2단계 인증 활성화 및 앱 비밀번호 발급 경로 사전 숙지**: 포털 메일(네이버 등)은 외부 IMAP 연결 시 2단계 인증이 선행되어야 합니다.

☐ **실물 스마트폰 손옆 대기**: 맥북 아이폰 미러링 화면에서는 카메라 권한이 차단됩니다(`iPhone camera is not available from Mac`). 신분증 촬영(고객확인제도 등)이 뜨면 즉시 실물 기기로 전환하세요.

☐ **연결 직후 자동 스캔 범위 인지**: 메일 연결 직후 AI가 최근 메일을 읽어 안건을 요약하므로(`03:46` 연결 직후 `READ 16건` 확인, *Codex·Antigravity*), 민감한 편지함이라면 연결 전 계정을 분리합니다.

[During] 업무 지시 중 쿼터 방어 & 원천 장부 대조

☐ **공식 커넥터 조회와 무거운 웹 브라우저 탐색을 분리해 지시**: 연결된 메일 인덱스 요약(`1~4 step`)이나 단일 정기결제 점검(`S18 7 step`)은 가볍지만, 보안메일 복호화(`S15 46 step`)나 외부 웹 계정 전환·검증(`S16 51 step`)은 한 번에 하루 한도의 약 12~13%(추정) 안팎을 소모합니다.

☐ **카드 삭제·변경 권유를 받으면 금고 입력 전에 원천 장부 끝 4자리부터 대조**: AI는 메일 영수증 일부만 보고 이미 법인카드인 구독을 개인카드로 단정할 수 있습니다.

☐ **세무·회계 처리 발언은 참고 의견으로만 취급**: 대화창에서 AI가 말한 정산 방법(개인 지출 후 법인 정산 등)은 적부가 검증되지 않은 설명이므로 사업자 기준 문서를 먼저 대조합니다.

[After] 업무 종료 후 3중 퇴거 프로토콜

☐ **1단계 — 원 서비스 `[내 기기 / 로그인 활동]` 직접 로그아웃**: AI가 브라우저 창을 닫고 "열린 세션 0개"라고 답해도 원 서비스 서버의 세션 토큰(`Linux · Google Chrome` 등)은 살아 있을 수 있습니다. 구글·네이버 보안 설정에서 직접 `[로그아웃]` 을 눌러 `로그아웃됨` 을 눈으로 확인하세요.

☐ **2단계 — 앱 `Connections` (연결된 서비스) 목록 점검**: 일회성 점검이 끝난 계정은 공식 연결 목록에서 해제되었는지 확인합니다 (`Connections` 가 남아 있으면 백그라운드 캘린더·메일 조회가 이어질 수 있음, *Codex 확인*).

☐ **3단계 — 금고(`Vault`)에 비밀번호를 넣었다면 원 서비스 비밀번호 변경**: 맥 앱 결제수단 화면(`Cards`)이 비어 있어도 비밀번호 목록이 0건인지, 클라우드 서버·백업 스냅샷까지 파기되었는지는 외부에서 확인할 수 없습니다(**4개 도구 공통 미확인**). 비밀번호를 직접 새 값으로 바꾸면 과거 저장본의 효력을 즉시 끊을 수 있습니다.

---

3. 상황별 복붙 안전 지시문 (Prompt Guardrails) 4선

프롬프트 1 — 메일함 기반 가벼운 구독·청구서 조사 (쿼터 절약형)

```
외부 웹사이트에 새로 로그인하거나 작업 브라우저를 띄우지 말고,
현재 공식 연결된 메일함 안에서만 최근 90일 동안 '결제', '청구서', '영수증', '구독'이 포함된 메일을 찾아
[날짜 / 서비스명 / 결제 금액 / 메일에 적힌 결제수단 표기] 표로만 정리해 줘.
메일 본문에 카드 종류(개인/법인)가 명시되지 않았다면 추측하지 말고 '원문 미표기'라고 적어 줘.
```

프롬프트 2 — 외부 페이지 확인 전 스텝·인증 사전 브리핑 요청

```
작업을 바로 실행하지 말고 먼저 계획을 한 줄씩 알려 줘.
1) 공식 연결된 커넥터만 쓰는지, 별도 작업 브라우저 로그인이 필요한지
2) 내 로그인 비밀번호나 2단계 인증(OTP), 실물 카메라 촬영이 필요한 단계가 있는지
내가 계획과 범위를 확인하고 '진행해'라고 답한 뒤에만 실행해 줘.
```

프롬프트 3 — 결제 수단 변경·삭제 제안 시 원천 대조 보류 지시

```
결제 수단 삭제나 새 카드 입력 카드를 띄우지 마.
먼저 네가 확인한 화면에서 현재 등록된 결제 수단의 [카드사명 / 끝 4자리 / 다음 결제일]만 그대로 적어서 알려 줘.
내 사업자 결제 장부와 대조한 뒤 내가 직접 변경 여부를 결정할게.
```

프롬프트 4 — 일회성 위임 종료 및 잔여 연결 점검 지시

```
방금 진행한 작업과 관련해 열려 있는 작업 브라우저를 닫고,
현재 내 계정에 남아 있는 공식 연결(Connections) 목록과 금고(Vault) 저장 항목 종류를 있는 그대로 나열해 줘.
원 서비스 서버의 기기 세션 폐기와 비밀번호 변경은 내가 직접 원 서비스 보안 설정에서 진행할게.
```

---

4. 투명한 한계 고지 — 이번 실측에서 네 도구 모두 확인하지 못한 8가지

사실 확인 수준을 지키는 원칙에 따라, 아래 8가지는 관찰 도구가 임의로 단정하지 않고 **확인되지 않은 영역(모름)**으로 남깁니다:

1. 현재 운영 중인 피클 서버가 공개 저장소 커밋(`cff16a34...`)과 동일한 코드로 돌아가는지 여부
2. 금고(`Vault`)에 구글 로그인·비밀번호가 실제로 0건인지 보여주는 직접 목록 (`05:45` 맥 빈 화면은 결제 카드 `Cards` 목록임)
3. 클라우드 서버·복제본·백업 스냅샷에서 자격증명 데이터가 실제로 지워졌는지 여부
4. 피클 작업 브라우저의 구체적 구동 인프라 실체 (위치 정보 없이 `Linux` 로 표시된 이유 등)
5. `05:17~05:18` 금고 잠금 해제(`Unlock`) 팝업이 뜬 확정 원인
6. 네이버페이 외부 자동결제 등록의 현재 유지 상태
7. 피클이 대화 중 설명한 세무 처리 방식의 적부
8. 로컬 대화 DB 결번 `760` 구간의 화면 상태 (`861` 구간은 화면 이상이 없었으나 결번 원인은 미상)

강사: 지피티쌤 · 본 문서는 직접 확인 사실, 역산 추정, AI 답변(피클의 말), 미확인 영역을 구분하여 표기합니다.