

CONNECT 5회차 · 65분

운영과 보안

보안 검토를 위한 한 장, 그리고 증상별 문제 해결

여는 말

- 보안 심사에 들어가는 사람과 운영을 맡는 사람이 대상입니다.
- 앞부분은 심사 자료로 그대로 쓸 수 있게 구성했습니다. 인쇄해서 나눠주셔도 됩니다.

통제 지점은 다섯 개입니다

경계

계정

들어올 사람

워크스페이스

데이터가 섞이지 않는 단위

대화

이 스레드를 볼 사람

자료

답변의 재료가 될 파일

나가는 길

실행 가능한 도구 · 경로

무엇을 정하나 · 누가

계정

✓ 멤버 초대 — owner · admin

워크스페이스

✓ 생성 — 누구나(본인 소유)

대화

✓ 그룹 공개 범위 — owner · admin

자료

✓ 드라이브 폴더 — 올리는 사람

나가는 길

✓ 도구 · 채널 · API 키 · 시스템 (시스템은 owner만)

시스템 등록만 admin 에게도 안 열려 있습니다. 회사 컴퓨터 한 대를 붙이는 가장 무거운 권한이기 때문입니다.

다섯 경계

- 심사에서 가장 먼저 묻는 것이 “격리 단위가 무엇인가”입니다. 워크스페이스라고 답하면 됩니다.
- 네 번째 줄을 눈여겨보세요 — 자료 경계만 관리자가 아니라 올리는 사람 손에 있습니다.

가장 강한 통제

민감도가 다르면 워크스페이스를 나눕니다

01

인사 · 법무 자료

별도 워크스페이스

02

외부 고객 응대

위젯 · 채널이 붙는 곳은 별도로

03

운영 시스템에 닿는 도구

별도 워크스페이스

04

일반 업무

하나로 충분합니다

권한을 잘게 나누는 것은 어느 선을 넘으면 반대가 됩니다 — 개인마다 예외를 만들면 반년 뒤 아무도 설명 못 합니다.

워크스페이스 분리

- 다른 워크스페이스의 자료·도구·대화에는 서로 닿지 않습니다. 이것이 가장 확실한 통제입니다.
- “봐도 되는 사람”과 “물어보면 답에 딸려 나올 사람”은 같습니다 — 자료 경계를 설명할 때 이 한 줄을 쓰세요.
- “비공개 대화”는 다른 멤버에게 안 보인다는 뜻입니다. 데이터베이스 접근이나 법적 요구까지 막는 것이 아닙니다.

심사 · 점검

도입 심사와 분기 점검

- 신원 확인 없는 입력(위젯 · 이메일)이 사내 자료와 같은 워크스페이스에 있나
- 되돌릴 수 없는 도구에 승인 지점이 있나
- 용도를 모르는 API 키가 있나 — 지우고 문제가 생기는지 보기
- 퇴사자가 멤버 목록과 그룹 공개 범위에 남아 있나

분기 1회로 달력에 넣으세요. 도구도 키도 예약도 늘어나기만 하고, 줄이는 절차는 아무도 안 만듭니다.

점검 항목

- 첫 줄이 이 회차에서 가장 중요합니다. 외부 입력이 사내 자료에 닿는 구성이 사고의 전형입니다.
- 그룹 공개 범위는 개인이 아니라 부서로 지정하게 하세요 — 그래야 인사 이동이 자동으로 반영됩니다.
- 시스템을 붙였다면 그 컴퓨터의 작업 폴더 범위도 점검 항목입니다.

증상별로 먼저 볼 곳이 다릅니다

증상

대화

답이 도중에 멈춤

자료

있는 자료인데 못 찾음

도구

켰는데 안 부름

시스템

오프라인으로 표시

예약

계속 밀림

먼저 볼 곳

대화

✓ 새로고침 — 실시간 전달은 손실될 수 있게 설계돼 있습니다

자료

✓ 파일이 텍스트로 읽히나 (스캔 PDF는 못 읽습니다)

도구

✓ 설명에 “언제 부르는지”가 있나

시스템

✓ 주기 신호 기반 — 켜다 켜면 잠깐 그렇게 보입니다

예약

✓ 실행 시간이 주기보다 긴 경우

한 번만 그런 것과 매번 그런 것은 원인이 다릅니다. 문의할 때 이 구분을 함께 적어주세요.

증상별 진단

- 먼저 세 가지 — 새로그침, 워크스페이스가 맞는지, 역할이 맞는지. 두 번째가 의외로 혼합니다.
- 도구 설명은 사람이 아니라 모델이 읽습니다. “무엇을 하는지”만 있고 “언제 쓰는지”가 없으면 안 불립니다.
- MCP 가 연결은 됐는데 도구가 하나도 없으면 연결 실패가 아니라 권한 범위 문제입니다.
- 터널 관련 기능만 막히는 것은 정상 동작입니다 — 주소 관리만 유료 게이트를 탑니다.

비용

사용량이 갑자기 늘었다면

- 실패하고 재시도를 반복하는 예약이 있나 — 가장 큰 사고를 냅니다
- 밖에서 들어오는 길(위젯 · 이메일 · API)에 제한이 걸려 있나
- 판단 없는 작업이 비싼 모델로 돌고 있나
- 끝난 프로젝트의 예약이 아직 도나

총액이 아니라 분포를 보세요. 사람이 아니라 작업을 보는 것이 요령입니다.

비용 급증

- 자동화는 사람보다 훨씬 많이 부릅니다. 새 채널이나 키를 연 뒤 며칠은 사용량을 지켜보세요.
- “누가 제일 많이 썼나”로 접근하면 사용 자체가 줄고 전환도 멈춥니다.

실습 · 30분

감사 로그로 하루를 재구성해보기

1

질문 먼저

로그를 열기 **전에** 네 개를 적습니다

2

로그에서만

기억으로 보충하지 않습니다. 5분 안에 못 찾으면
“못 찾음”

3

사각지대

기록이 없나, 찾는 법을 모르나 — 해결책이 있습니다

로그를 먼저 열면 거기 있는 것에 맞춰 질문을 만들게 됩니다. 그러면 없는 기록, 즉 사각지대가 영영 안 보입니다.

실습 진행

- 질문을 먼저 적게 하는 것이 이 실습의 장치입니다. 순서를 바꾸면 아무것도 안 나옵니다.
- “찾는 법을 모른다”가 대부분이고, 이건 안내 한 줄이면 끝납니다 — 훨씬 싸다고 말해주세요.
- 감사 로그는 무엇이 일어났는지를 남기지 왜 그랬는지는 안 남깁니다. 판단 근거를 어디 적는지 물어보세요.

정리

가져갈 것

- 1 격리 단위는 워크스페이스 — 민감도가 다르면 나눈다
- 2 외부 입력과 사내 자료를 같은 자리에 두지 않는다
- 3 되돌릴 수 없는 동작에 승인, 없으면 그 도구는 붙이지 않는다
- 4 권한 화면이 안 보이는 것은 대개 역할 문제다
- 5 분기 점검을 달력에 넣는다 — 줄이는 절차는 아무도 안 만든다

닫는 말

- Connect 트랙이 끝났습니다. 보안 심사 자료가 필요하다면 이 회차의 앞 세 장을 그대로 쓰시면 됩니다.
- 마지막 회차이므로 남은 질문을 받는 시간을 5분 이상 확보하세요.
- 다음 단계로 각자 워크스페이스에서 분기 점검 항목을 캘린더에 넣게 하면 도입이 유지됩니다.