Daily 협업일지(02/25)

[1] 오늘 날짜 / 이름 / 팀명

- 날짜: 2026.02.25
- 이름: 김슬기
- 팀명: 6팀

---

[2] 오늘 맡은 역할 및 구체적인 작업 내용

> 오늘 당신이 맡았던 역할은 무엇이었고, 어떤 작업을 수행했나요?
> *(예: 모델 학습 파라미터 조정, 결측치 처리, 발표자료 구성 등)*

✍️ 답변:

```
Tool Execution Gate 및 SSRF 방어:
  - 검색 도구 실행 전 URL을 검사하는 ToolExecutionGate 구현
  - 내부망 IP(127.0.0.1, 192.168.* 등) 및 마스킹된 호스트 접근 차단
감사 로그(Audit Log) 고도화:
  - 로그를 security.log(위협)와 audit.log(정상 이력)로 분리
  - JSON 포맷으로 구조화하여 메타데이터(IP, User, Tenant) 기록 및 Gzip 자동 압축 적용
통합 테스트 슈트 작성 (test_isolation_security.py):
  - 총 13개 항목의 테스트 케이스 작성 (파일 차단, 테넌트 격리, PII 마스킹, SSRF 차단, 로그 적재 확인 등)
  - FakeEmbeddings 및 Mock 객체를 활용하여 API 비용 없이 테스트 가능한 환경 구성
```

---

[3] 오늘 작업 완료도 체크 (하나만 체크)

> 진척 상황을 정량적으로 표시하고, 간단한 근거도 작성하세요.

☐ 🔴 0% (시작 못함)

☐ 🟠 25% (시작은 했지만 진척 없음)

☐ 🟡 50% (진행 중, 절반 이하)

☑ 🔵 ~~75% (거의 완료됨)~~

☐ 🟢 100% (완료 및 점검까지 완료)

📌 간단한 근거:

```
(75%) 핵심 보안 기능 구현과 테스트 코드가 모두 작성되었음. 다만, 실제 운영 환경에서의 대용량 트래픽 테스트와 UI 상에서의 에러 메시지 UX 개선이 일부 남음
```

---

[4] 오늘 협업 중 제안하거나 피드백한 내용이 있다면?

> 오늘 회의나 메시지에서 당신이 제안하거나 팀에 피드백한 내용은 무엇인가요?

✍️ 답변:

```
-
```

---

[5] 오늘 분석/실험 중 얻은 인사이트나 발견한 문제점은?

> EDA, 모델 실험 중 유의미한 점이나 오류가 있었다면 자유롭게 작성하세요.

✍️ 답변:

```
- 보안 로그는 단순히 텍스트로 남기는 것보다 JSON 형태로 남겨야 추후 모니터링 도구(ELK 등)와 연동하기 용이함
- 테스트 코드 작성 중, 실제 LLM을 호출하지 않고도 MagicMock을 통해 가드레일 로직을 검증하는 것이 CI/CD 속도 측면에서 유리함을 확인
```

---

[6] 일정 지연이나 협업 중 어려웠던 점이 있다면?

> 자기 업무 외에도 전체 일정이나 팀 내 협업에서 생긴 문제를 공유해 주세요.

✍️ 답변:

```
- SSRF 테스트 시 실제 내부망으로 요청이 나가지 않도록 Mocking 하는 과정에서 ToolExecutionGate와 RAGChain 간의 의존성 처리가 까다로웠음
```

---

[7] 오늘 발표 준비나 커뮤니케이션에서 기여한 부분은?

> 슬라이드 제작, 발표 연습, 질문 정리 등 발표와 관련된 활동을 썼다면 기록하세요.

✍️ 답변:

```
-
```

---

[8] 내일 목표 / 할 일

> 구체적인 개인 업무나 팀 목표 기반 계획을 간단히 적어주세요.

✍️ 답변:

```
- 팀원 코드 통합 및 추가 작업 분배
```