

BGP라우팅 데이터 분석 LLM 기술 개발 - 최종 발표

20학번 손봉우, 20학번 양준혁

지도 교수님 : 이영석 교수님

팀원



20학번 손봉우

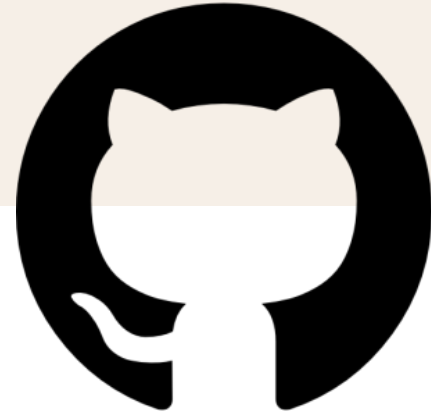
- 백엔드
- 데이터 분석
- 문서 작성
- 발표

- 프론트
- 문서 작성
- 발표

20학번 양준혁



협업 방식



banbakbulga Merge pull request #6 from bgp-llama/docs 43 Commits

week1	chore: 1주차 자료 폴더로 정리	2 months ago
week11	Add files via upload	2 weeks ago
week2	2주차 문서 추가	2 months ago
week3	modify: 발표자료 확장자 수정 pptx -> pdf	2 months ago
week4	4주차 발표자료 재업로드	last month
week6	6주차 발표자료 업로드	last month
week8	8주차 발표자료 업로드	27 days ago
.gitignore	chore: .gitignore에 .DS_Store 추가	2 months ago
README.md	Update README.md	2 weeks ago

README

BGP 라우팅 데이터 분석을 위한 LLM 기반 분석 시스템 개발

프로젝트 개요

- 사용자가 자연어로 BGP 데이터를 질의할 수 있는 AI 기반 분석 챗봇 개발
- 과거 BGP 로그를 쉽게 탐색할 수 있는 타임라인 기반 시각화 도구 구현
- LLM 기반 요약 기능을 통해 방대한 데이터를 빠르게 이해할 수 있도록 지원
- 실시간으로 라우팅 이상 여부를 판단하는 이상 탐지 시스템 설계



6 짬통

공유자료 2025/05/30

의록 2025/05/25

외의록 2025/05/12

회의록 2025/05/11

회의록 2025/04/28

회의록 2025/04/14

회의록 2025/04/06

회의록 2025/04/06

회의록 2025/04/07

회의록 2025/03/30

회의록 2025/03/24

회의록 2025/03/23

회의록 2025/03/10

회의록 2025/02/28

회의록 2025/02/21

회의록 2025/02/20

회의록 2025/02/12

회의록 2025/02/06

회의록 2025/02/05

회의록 2025/01/30

회의록 2025/01/29

회의록 2025/01/23

회의록 2025/04/07

회의 일시

비어 있음

① 유형

교수님 참석 회의

② 작성자

준혁 양

참석자

진효겸 봉우 손

+ 속성 추가

댓글

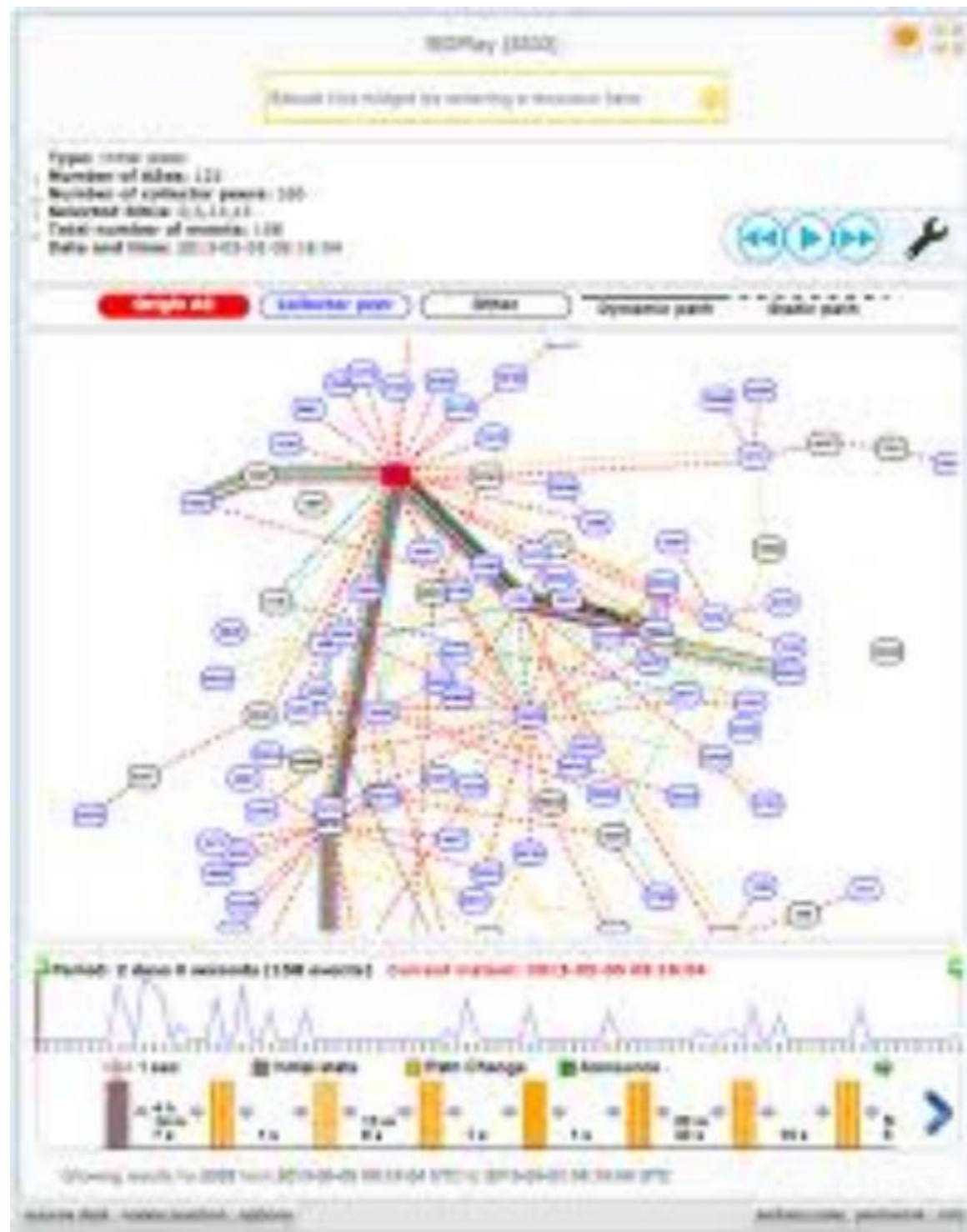
댓글 추가

회의록 (2025.04.07)

주요 내용 요약:

1. 프로토타입 진행 상황
 - BGP 플래핑 사례 기반으로 GPT-4-5-mini 모델
 - 로컬 환경에서 사용자 입력을 받아 의심 지점
 - JSONL 형식의 요약 데이터를 생성하여 Mong
2. 데이터 저장 및 처리 문제
 - AS 번호, Prefix 단위의 데이터 양이 방대함. 자
 - 현실적으로 전체 데이터를 다 저장하기보단, 관
 - 저장 단위(5분, 10분, 1시간 등)에 따라 시스템
3. 정답 기반 응답과 모델 성능 평가

프로젝트 개요 : BGP 라우팅 데이터 분석 시스템



기존 문제점

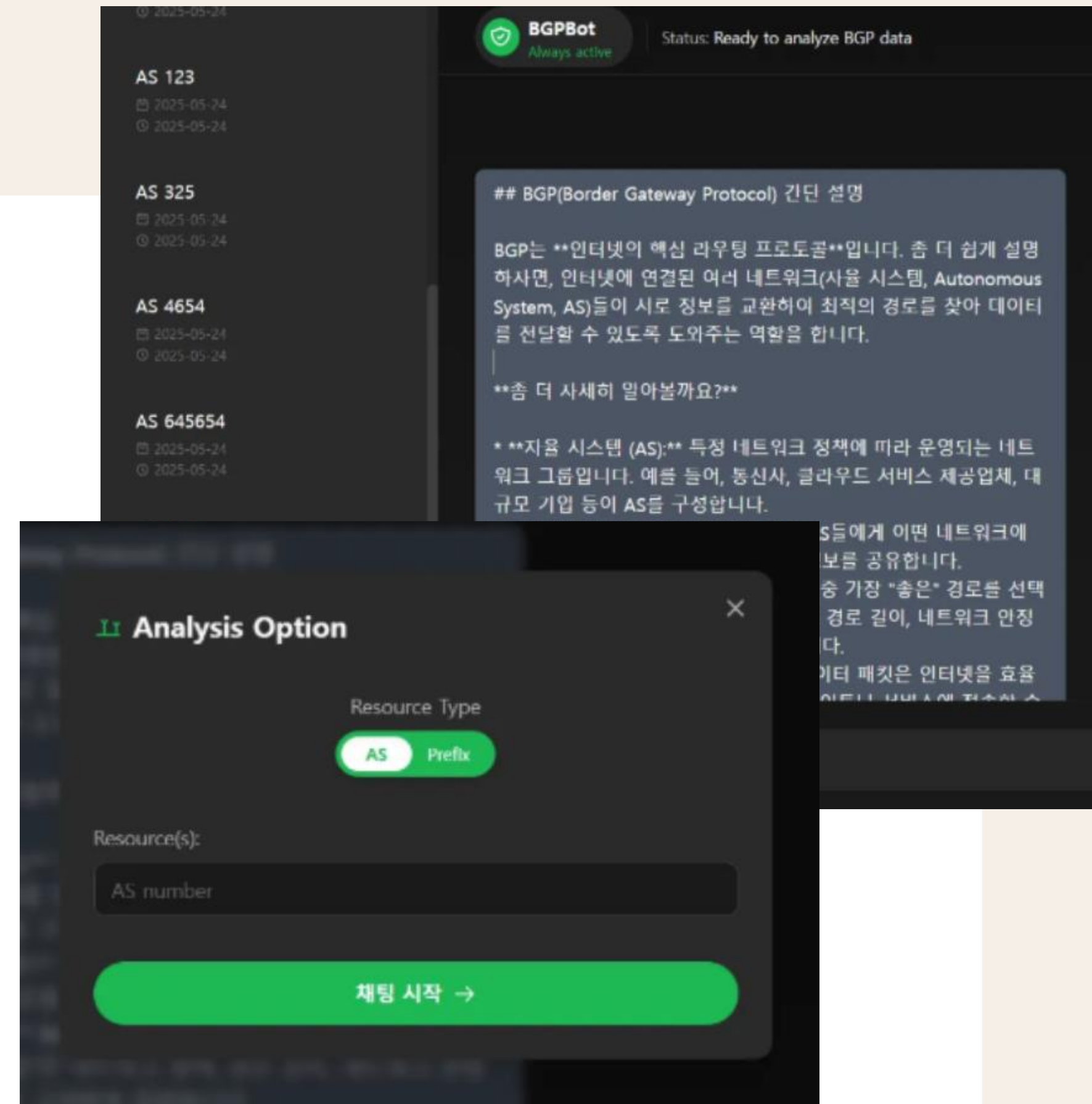
- BGP 데이터를 분석할 때 복잡한 명령어 및 설정 요구됨
- 실시간 라우팅 변화 감지를 위한 자동화 부족
- 과거 데이터를 활용한 분석이 어렵고, 시각화 기능이 제한적
- 보안 위협(BGP 하이재킹, 경로 변경 등) 탐지가 어려움

프로젝트 개요 : BGP 라우팅 데이터 분석 시스템

LLM (Large Language Model) 기술을 활용하여
BGP 데이터의 이상 탐지 및 시각화 기능을 제공

사용자는 웹 인터페이스를 통해 IP/Prefix, 날짜, 수집 서버 등을 설정하고, 자연어나 템플릿으로 분석 명령을 입력할 수 있다. 시스템은 이를 바탕으로 BGP 이상현상을 탐지하고, 시계열 그래프 및 AS 관계 그래프를 생성하여 분석 결과를 직관적으로 제공한다.

- BGP 데이터에 대한 자연어 질의 처리
- 이상 탐지 결과 요약 및 시각적 대시보드 제공
- Node Graph, Statistics 등 다양한 분석 시각화 제공
- 과거 데이터와 최신 데이터 모드 지원



기존 시스템 관찰 결과

- 시각화 그래프의 부족
 - 기존 시스템은 이상 징후만 로그 형태로 제공 빠른 의사결정에 한계
- 명령어 기반의 불편함
 - 초보자나 관리자 모두 직관적인 대시보드와 UI를 선호
- 반복적인 복원 요청
 - 과거 데이터에 대한 복원 기능이 없거나 제한적 업무 부담 증가

핵심 아이디어

- LLM 기반 자연어 질의 및 명령어 처리
 - 복잡한 명령어 대신 자연어 입력으로 이상 탐지, 데이터 분석 명령을 직관적으로 수행
- 자동화된 이상 탐지 및 결과 시각화
 - 실시간 라우팅 변화 탐지 및 자동화된 이상 징후 분석, 직관적인 시각화 제공
- 과거 데이터 복원 및 최신 데이터 동시 지원
 - 반복 업무 감소, 특정 시간대 복원 기능으로 실무자 효율성 강화
- BGP 데이터 및 AS 관계 시각화 기능
 - 시계열 그래프 및 AS 관계 네트워크 그래프를 통해 분석 결과를 직관적으로 표현

기존 해결 방법의 한계 및 개선점

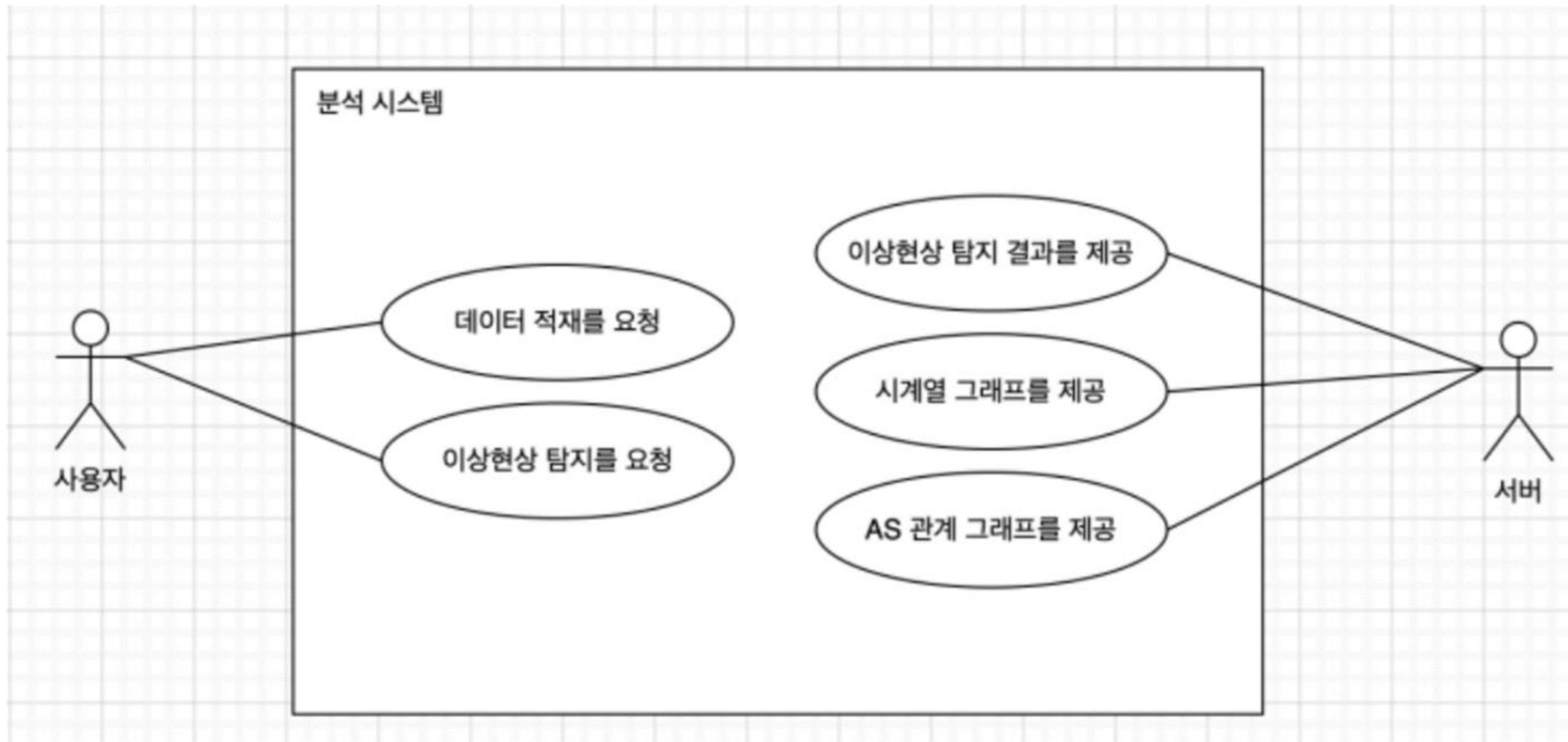
기존 방법

- 복잡한 명령어 기반, 사용자 진입 장벽 높음
- 실시간 탐지 및 시각화 기능 부재
- 과거 데이터 복원 기능 미흡

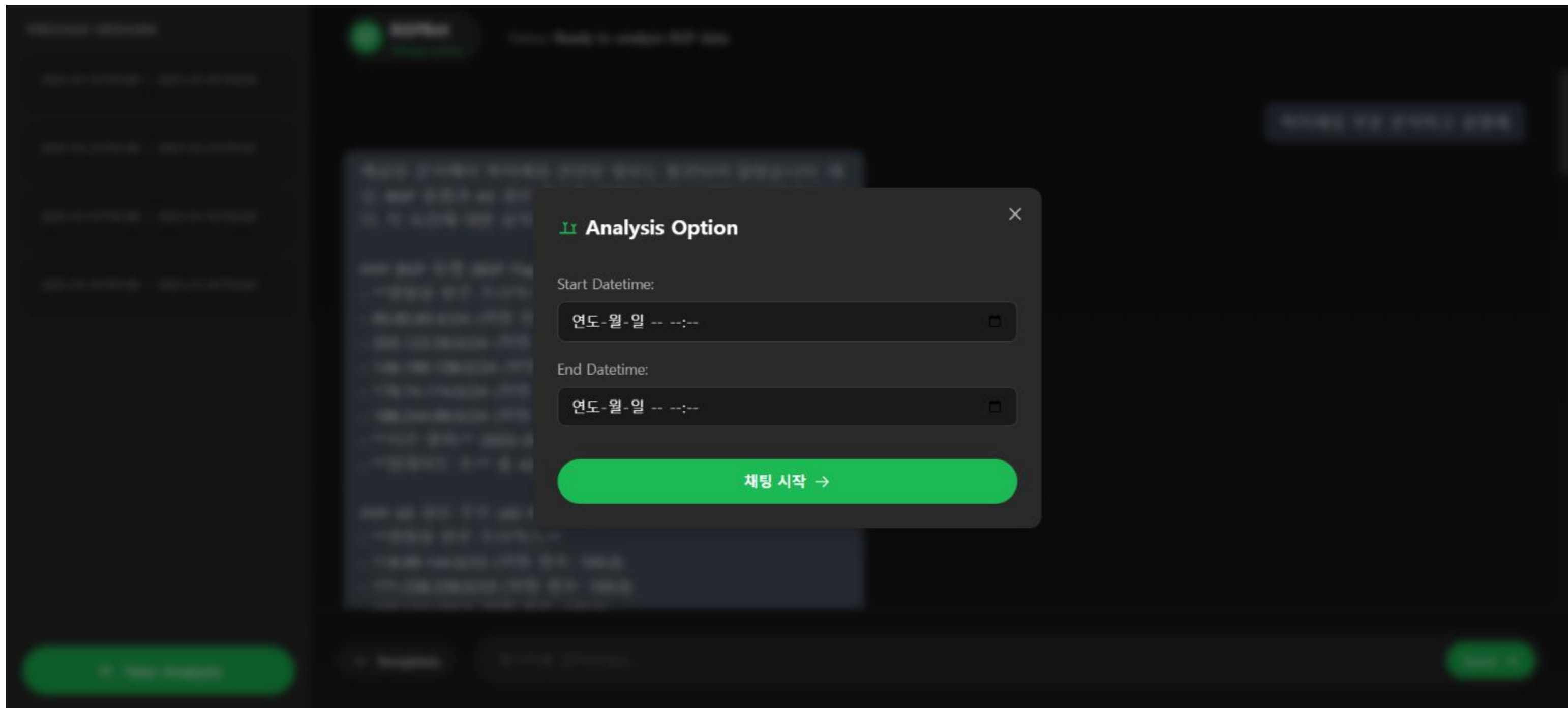
제안된 개선점

- LLM을 통한 자연어 기반 분석으로 접근성 향상
- 실시간 탐지 + 직관적 시각화 대시보드 제공
- 특정 시간대 복원, 반복 업무 자동화 기능 강화

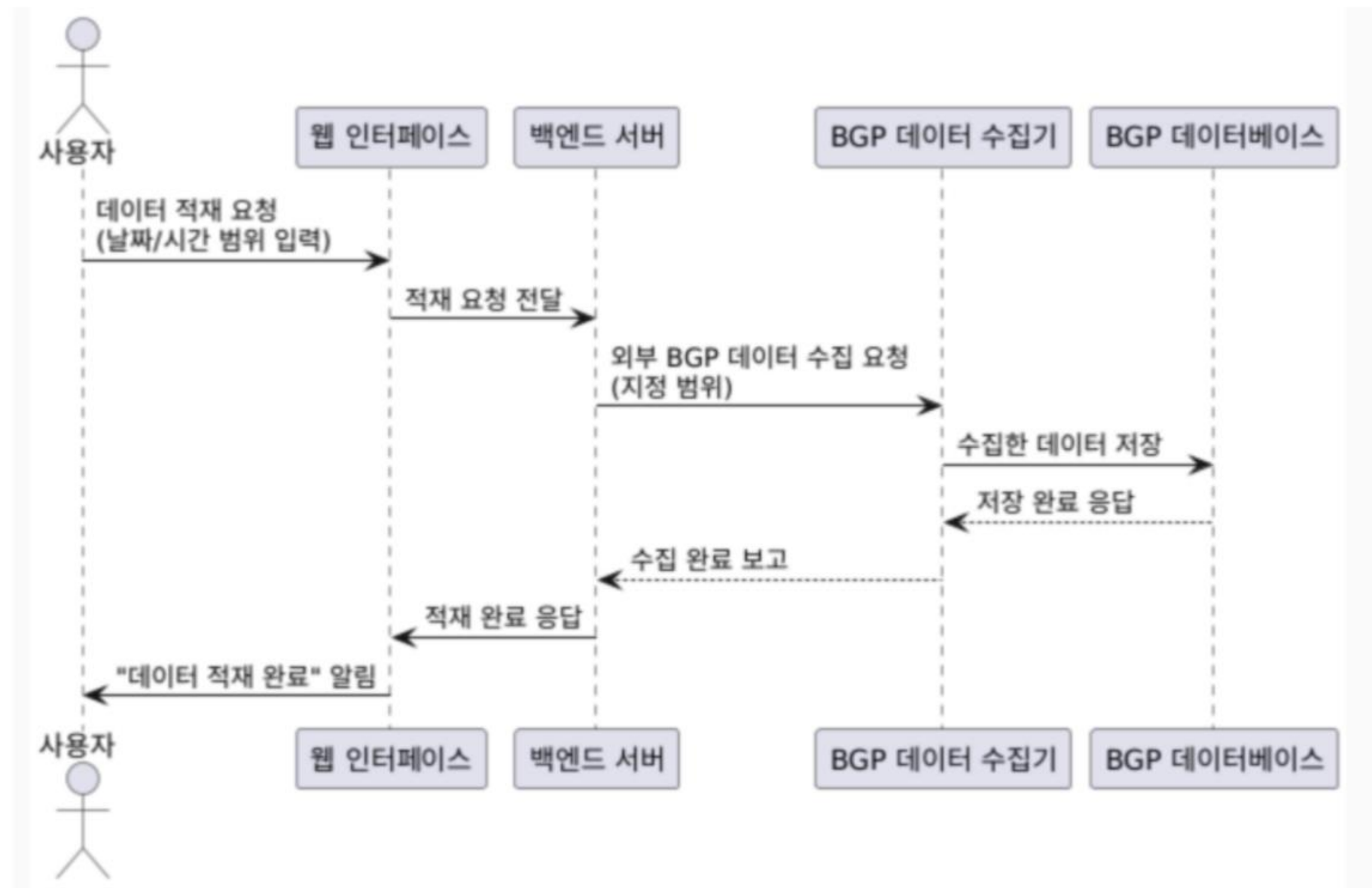
데모 : 유스케이스



데모 : 데이터 적재를 요청



데모 : 시퀀스 다이어그램 1 - 데이터 적재를 요청



데모 : 이상현상 탐지 요청

PREVIOUS SESSIONS

2025-01-01T01:00 ~ 2025-01-01T02:00


2025-05-25T01:00 ~ 2025-05-25T01:02

2025-01-01T01:00 ~ 2025-01-01T02:00

2025-01-01T01:00 ~ 2025-01-01T03:00

2025-05-25T01:00 ~ 2025-05-25T02:00

+ New Analysis

 **BGPBot**
Always active

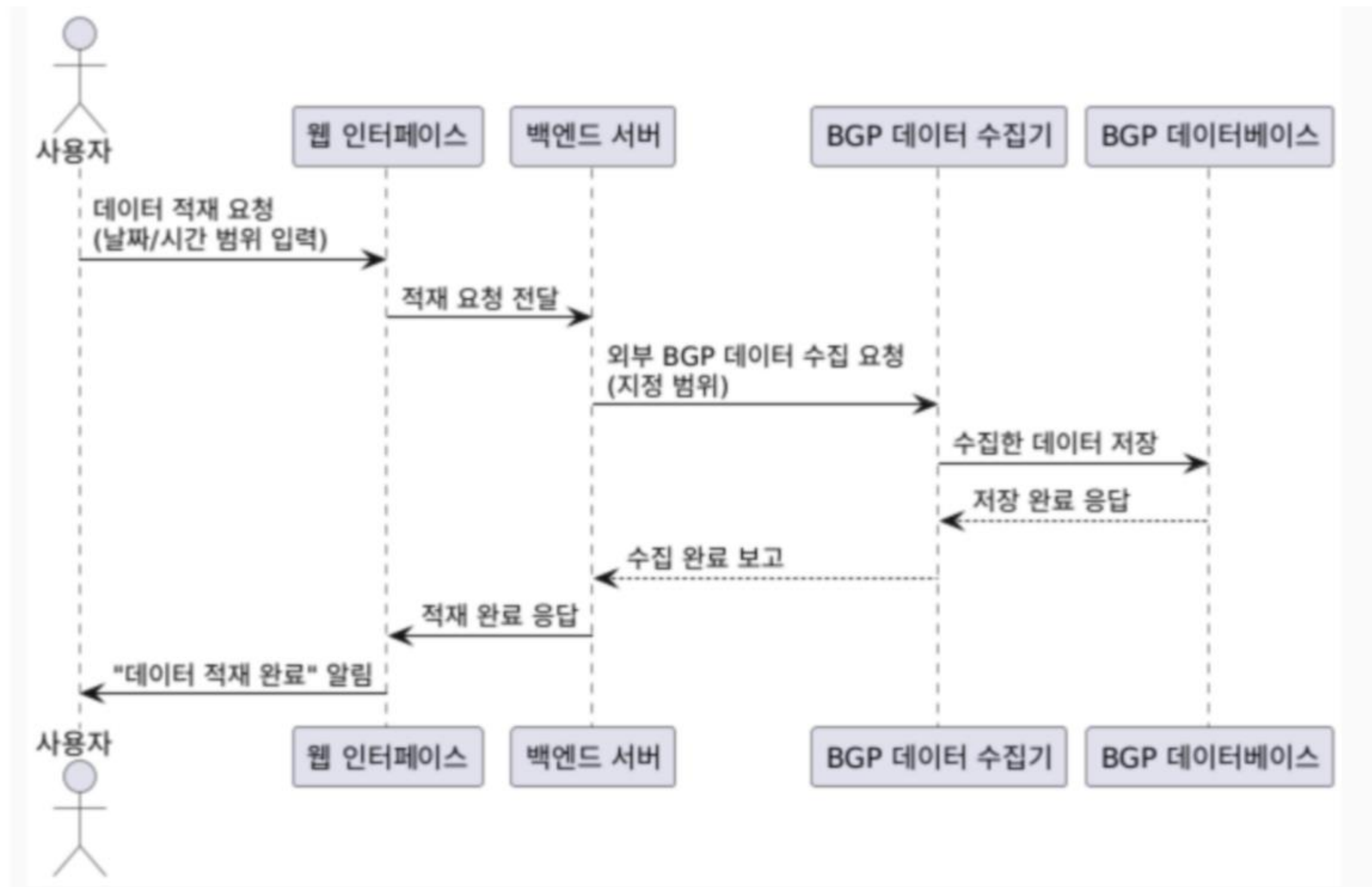
Status: Ready to analyze BGP data

▼ Templates

하이재킹 현상을 분석해줘

Send →

데모 : 시퀀스 다이어그램 2 - 이상현상 탐지를 요청



데모 : 이상현상 탐지 결과를 제공

PREVIOUS SESSIONS


2025-01-01T01:00 ~ 2025-01-01T02:00

2025-05-25T01:00 ~ 2025-05-25T01:02

2025-01-01T01:00 ~ 2025-01-01T02:00

2025-01-01T01:00 ~ 2025-01-01T03:00

2025-05-25T01:00 ~ 2025-05-25T02:00

 **BGPBot**
Always active

Status: Ready to analyze BGP data

플래핑 부분 분석하고 설명해

제공된 문서에서 플래핑(BGP Flap)과 관련된 정보를 분석한 결과는 다음과 같습니다.
|
플래핑(BGP Flap) 분석

- **플래핑 발생 시간:**
- 2025-05-25T19:00:00부터 2025-05-25T19:10:00까지
- 2025-05-25T17:00:00부터 2025-05-25T17:10:00까지
- 2025-05-25T11:00:00부터 2025-05-25T11:10:00까지
- 2025-05-25T12:40:00부터 2025-05-25T12:50:00까지
- 2025-05-25T16:40:00부터 2025-05-25T16:50:00까지
- 2025-05-25T20:30:00부터 2025-05-25T20:40:00까지
- 2025-05-25T02:50:00부터 2025-05-25T03:00:00까지
- 2025-05-25T11:50:00부터 2025-05-25T12:00:00까지
- 2025-05-25T12:20:00부터 2025-05-25T12:30:00까지
- 2025-05-25T10:00:00부터 2025-05-25T10:10:00까지
- 2025-05-25T08:50:00부터 2025-05-25T09:00:00까지
- 2025-05-25T08:30:00부터 2025-05-25T08:40:00까지
- 2025-05-25T06:10:00부터 2025-05-25T06:20:00까지
- 2025-05-25T05:00:00부터 2025-05-25T05:10:00까지

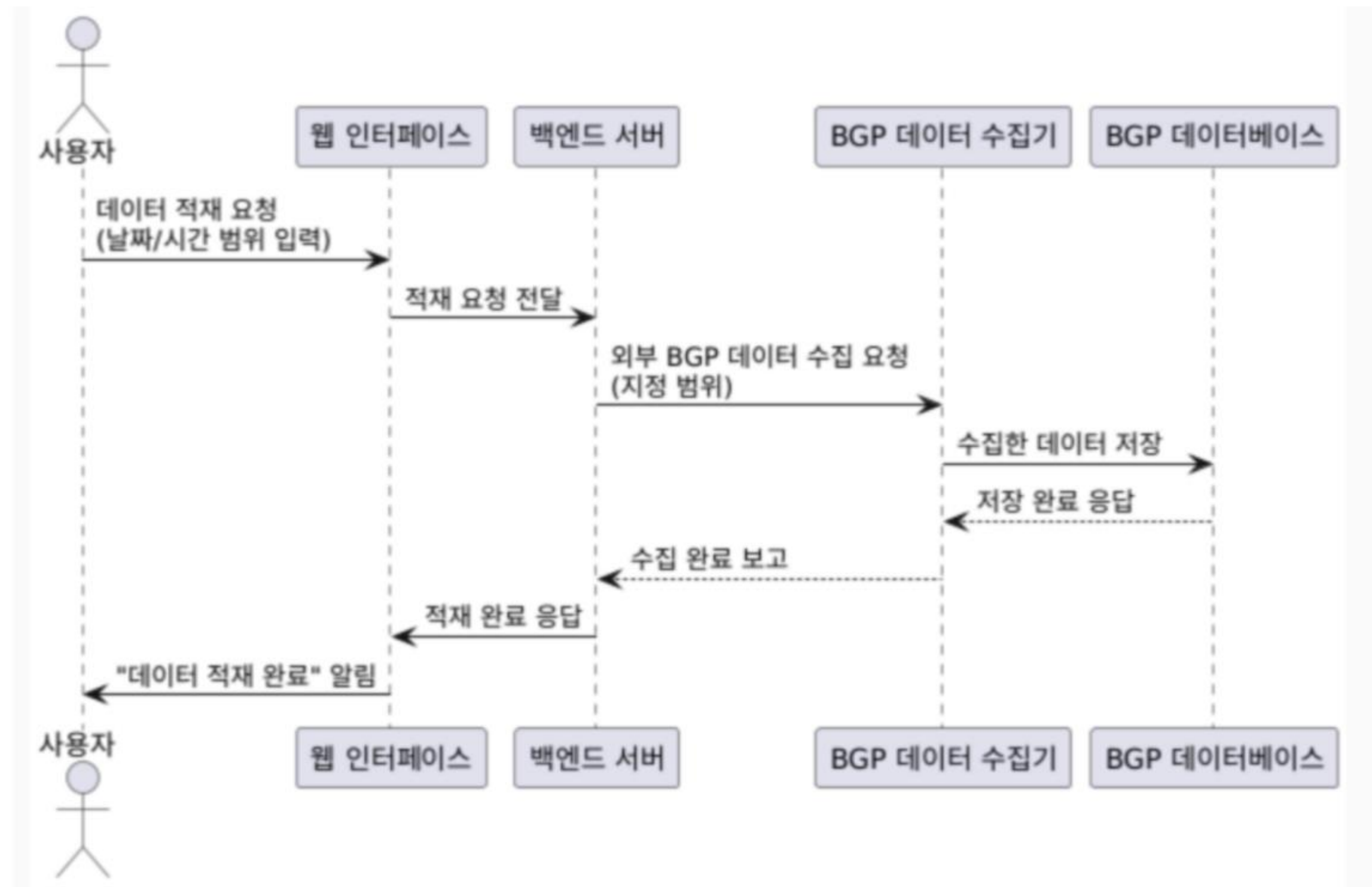
+ New Analysis

▼ Templates

하이재킹 현상을 분석해줘

Send →

데모 : 시퀀스 다이어그램 3 - 이상현상 탐지 결과를 제공



테스트 범위

- 데이터 적재: 외부 BGP 데이터 소스에서 지정 기간의 데이터를 수집하고 데이터베이스에 적재하는 기능.
- 이상현상 탐지: BGP Hijack, Route Leak 등의 이상 현상을 탐지하는 알고리즘의 정확성 및 안정성 검증.
- 탐지 결과 제공: 이상 탐지 결과를 LLM 기반 요약 기능을 통해 사용자에게 직관적으로 전달하는 기능.
- 시각화 기능: 시계열 그래프, AS 관계 그래프 등 다양한 형태의 결과 시각화 기능의 정확성.
- UI 상호작용 흐름: 사용자의 질의, 탐지 결과 요청, 결과 확인까지의 흐름에서 오류나 이슈 없이 일관성 있게 작동하는지 여부.
- 예외 처리: 잘못된 입력값(예: 잘못된 기간, 이상 탐지 조건 등)에 대한 오류 처리 및 사용자 안내 기능.

테스트 결과 개요

- 본 테스트는 6개의 주요 항목(데이터 적재, 이상현상 탐지, 탐지 결과 요약, 시각화, 예외 처리, UI 상호작용 기능)을 대상으로 수행.
- 각 항목별로 정상 동작, 데이터 정확성, UI의 일관성을 평가하였으며, 기능의 정상 작동과 오류 처리의 적정성을 검증.
- 시각화 출력 관련 일부 결함이 발견되었음. 이러한 결함은 상세히 기록되었고, 개선 방안과 함께 목록으로 정리됨.
- 이 테스트 결과 개요는 이후 상세 결과와 결정 근거의 기초 자료로 활용될 예정.


테스트 결과

Id	테스트 대상	테스트 데이터	예상 결과	Pass / Fail / Inconclusive
TC-01	데이터 적재 기능	BGP Update 데이터 수집지: route-views2, 2025-05-25 00:00 ~ 2025-05-25 23:59	데이터가 DB에 정상 적재됨	Pass
TC-02	이상현상 탐지 기능	상동	Hijacking 탐지 결과가 정확히 출력됨	Pass
TC-03	탐지 결과 요약 (LLM)	상동	요약 내용이 자연스럽게 표시됨	Pass
TC-04	시계열 그래프 제공 기능	상동	시계열 그래프가 정확히 생성됨	Fail
TC-05	AS 관계 그래프 제공 기능	상동	AS 관계 네트워크 그래프가 정확히 출력됨	Fail
TC-06	예외 처리 기능 (잘못된 입력)	미래 날짜 입력	오류 메시지가 발생함	Pass

테스트 결과 TC-01

PREVIOUS SESSIONS

2025-05-25T01:00 ~ 2025-05-25T01:02

 **BGPBot**
Always active

Status: Ready to analyze BGP data

2025-05-25T01:00부터 2025-05-25T01:02까지의 데이터가 적재되었습니다.

+ New Analysis

▼ Templates

메시지들 입력하세요...

Send →

테스트 결과 TC-02

제공된 문서에서 하이재킹 현상에 대한 정보는 확인되지 않았습니
다. 그러나 BGP 플랩 현상과 관련된 여러 사건이 보고되었습니다.
아래는 해당 사건에 대한 요약입니다.

BGP 플랩 현상

- **영향을 받은 프리픽스**:
 - 41.89.249.0/24 (위험 점수: 106.0)
 - 41.75.222.0/24 (위험 점수: 78.2)
 - 41.75.221.0/24 (위험 점수: 78.1)
- **시간 범위**: 2025-05-25T01:00:00 - 2025-05-25T01:10:00
- **업데이트 수**: 22510
- **플랩 수**: 3110

이 외에도 여러 시간대에 걸쳐 다양한 프리픽스에서 플랩 현상이
발생했으나, 하이재킹과 관련된 정보는 발견되지 않았습니다. 추가
적인 정보가 필요하시다면 다른 질문을 해주시면 감사하겠습니다.

=> 질의 : 하이재킹 현상 분석해줘

테스트 결과 제대로 된 이상현상 분석
결과를 출력하는 것을 확인할 수 있었음

테스트 결과 TC-03

PREVIOUS SESSIONS

2025-01-01T01:00 ~ 2025-01-01T02:00

2025-05-25T01:00 ~ 2025-05-25T01:02

2025-01-01T01:00 ~ 2025-01-01T02:00

2025-01-01T01:00 ~ 2025-01-01T03:00

BGPBot

Always active

Status: Ready to analyze BGP data

하이재킹 부분 분석하고 설명해

제공된 문서에서 하이재킹 관련된 정보는 발견되지 않았습니다. 대신, BGP 플랩과 AS 경로 루프와 관련된 여러 사건이 보고되었습니다. 각 사건에 대한 요약은 다음과 같습니다.

BGP 플랩 (BGP Flap)

- **영향을 받은 프리픽스:**

- 95.85.85.0/24 (위험 점수: 102.4)

- 203.123.56.0/24 (위험 점수: 101.8)

- 146.196.108.0/24 (위험 점수: 101.2)

- 178.74.174.0/24 (위험 점수: 100.9)

- 188.244.99.0/24 (위험 점수: 100.6)

- **시간 범위:** 2025-05-25T19:00:00 ~ 2025-05-25T19:10:00

- **업데이트 수:** 총 42,289 업데이트, 3,940 플랩

AS 경로 루프 (AS Path Loop)

- **영향을 받은 프리픽스:**

- 116.99.144.0/22 (위험 점수: 103.0)

- 171.238.226.0/23 (위험 점수: 103.0)

- 103.150.100.0/24 (위험 점수: 102.0)

+ New Analysis

▼ Templates

메시지를 입력하세요...

Send →

결정에 대한 근거

- 각 테스트 케이스의 실제 수행 결과를 예상 결과와 비교하여 Pass 또는 Fail을 판정하였다.
- 정상적으로 기능이 수행되어 예상 결과가 정확히 출력된 경우 Pass로, 일부 오류나 누락으로 결과가 불완전했던 경우 Fail로 결정되었다.
- 모든 테스트 항목은 명확히 판별되었으며, 판단이 불확실한 항목은 없었다.

결론 및 추천 사항

결론

- 데이터 적재, 이상 탐지, 결과 요약, UI 흐름은 안정적으로 구현됨
- 일부 시각화 기능에서 데이터 누락 및 오류가 발견됨 보완 필요

추천 사항

- AS 관계 그래프와 시계열 그래프 출력 오류를 보완하고, 데이터 완전성을 검증하는 테스트를 추가 수행
- 시각화 기능의 데이터 처리 문제를 개선하여 누락 현상을 방지
- 결함이 수정된 이후 재테스트를 통해 안정성 및 정확성을 확인

=> 이를 기반으로 시스템의 최종 품질을 확보해 나갈 것이 권장됨

사용자 테스트(A/B 테스트)

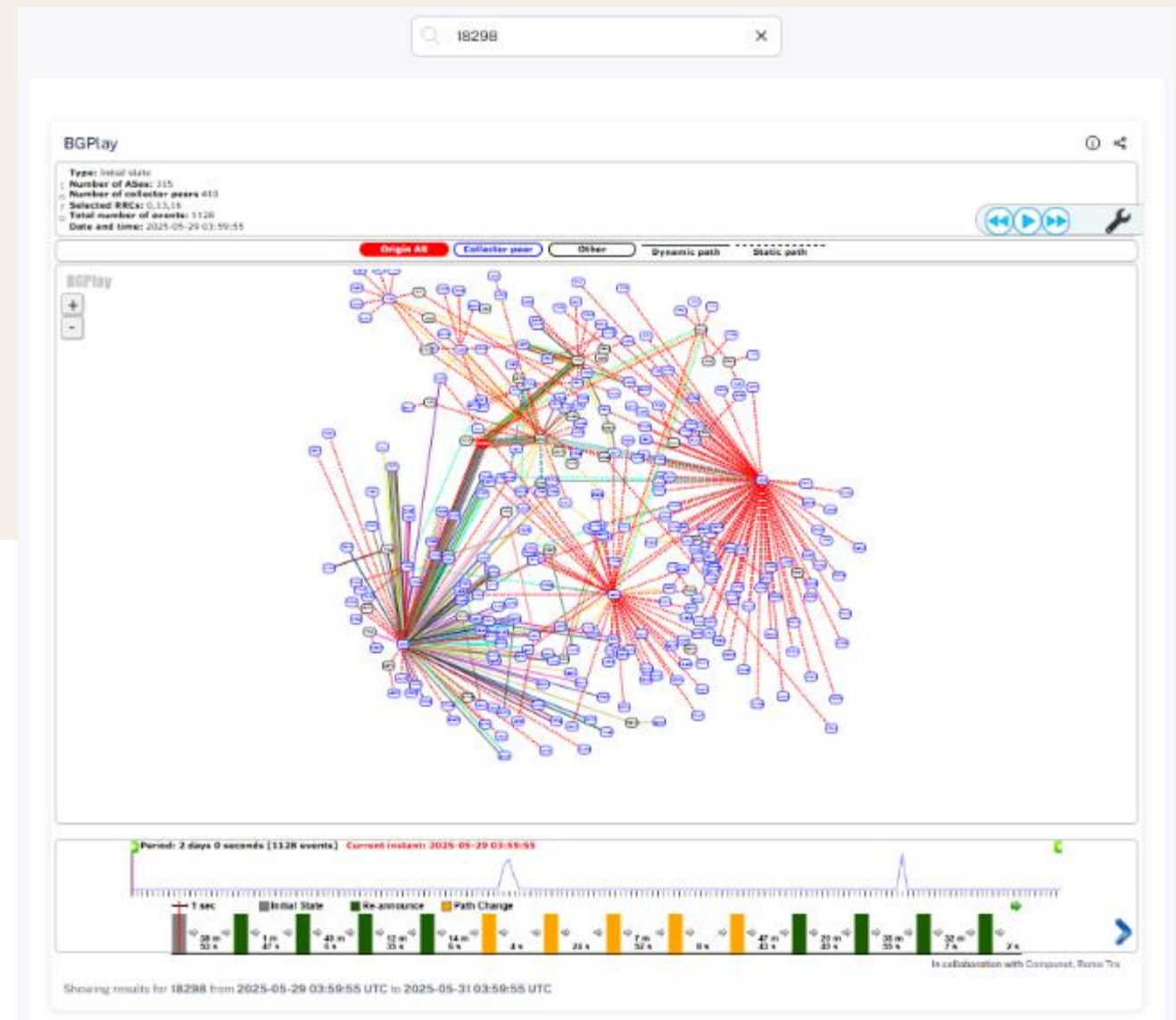
기존 BGPlay 시스템(A)과 자연어 기반 새 시스템(B) 비교
목표: 자연어 입력의 편의성 및 사용자 만족도/재사용 의향 검증

기존 시스템(A):

- 명령어 기반, 입력 복잡, 사용자 진입 장벽 높음

새 시스템(B):

- 자연어로 질의/분석 명령 가능
- 사용자 친화적, 직관적, 빠른 학습곡선



PREVIOUS SESSIONS

2025-05-25T01:00 ~ 2025-05-25T01:02

BGPBot
Always active

Status: Ready to analyze BGP data

있습니다.

하이재킹 현상 분석해줘

제공된 문서에서 하이재킹 현상에 대한 정보는 확인되지 않았습니다. 그러나 BGP 플럼 현상과 관련된 여러 사건이 보고되었습니다. 아래는 해당 사건에 대한 요약입니다.

BGP 플럼 현상

- **영향을 받은 프리픽스**:
- 41.89.249.0/24 (위험 점수: 106.0)
- 41.75.222.0/24 (위험 점수: 78.2)
- 41.75.221.0/24 (위험 점수: 78.1)
- **시간 범위**: 2025-05-25T01:00:00 - 2025-05-25T01:10:00
- **업데이트 수**: 22510
- **플럼 수**: 3110

이 외에도 여러 시간대에 걸쳐 다양한 프리픽스에서 플럼 현상이 발생했으나, 하이재킹과 관련된 정보는 발견되지 않았습니다. 추가적인 정보가 필요하시다면 다른 질문을 해주시면 감사하겠습니다.

+ New Analysis

Templates

하이재킹 현상 분석해줘

Send →

사용자 테스트(A/B 테스트)

- 자연어 기반 분석이 가능해진 새 시스템은, 명령어 진입장벽이 낮아져서 편리하다는 긍정적 평가를 받음.
- 현업 적용 시에도 효율성과 생산성을 크게 높일 수 있을 것으로 기대됨.

=> 자연어 기반 입력으로 사용자 경험을 개선하여 만족도와 재사용 의향을 크게 높인 결과를 확인

추가 계획 및 기대효과

- 데이터 적재 처리 로직과 병렬화 방식을 개선하여, 고객이 느꼈던 속도 저하 문제를 해소할 계획이다. 또한, 데이터베이스 인덱싱 및 캐싱 기법을 적용해 적재 시간을 단축할 예정이다.
- LLM 요약 결과의 길이 조정 및 세부 항목 포함 여부를 고객 맞춤형 옵션으로 제공할 수 있도록 기능을 확장할 예정이다. 또한, 요약 문서의 품질을 높이기 위해 요약 프롬프트와 알고리즘을 지속적으로 보완할 계획이다.
- 고객 피드백을 반영한 후 재테스트를 진행하고, 새로운 의견을 수렴하여 시스템의 품질을 지속적으로 개선해 나갈 예정이다.

기대효과

- 데이터 적재 속도와 품질이 향상되어 사용자 경험을 강화
- 탐지 및 요약 기능의 유연성이 높아져 고객 맞춤형 분석 제공 가능
- 피드백을 바탕으로 한 지속적인 개선으로 고객 만족도와 재사용 의향이 한층 강화될 것으로 기대됨

감사합니다.

20학번 손봉우, 20학번 양준혁