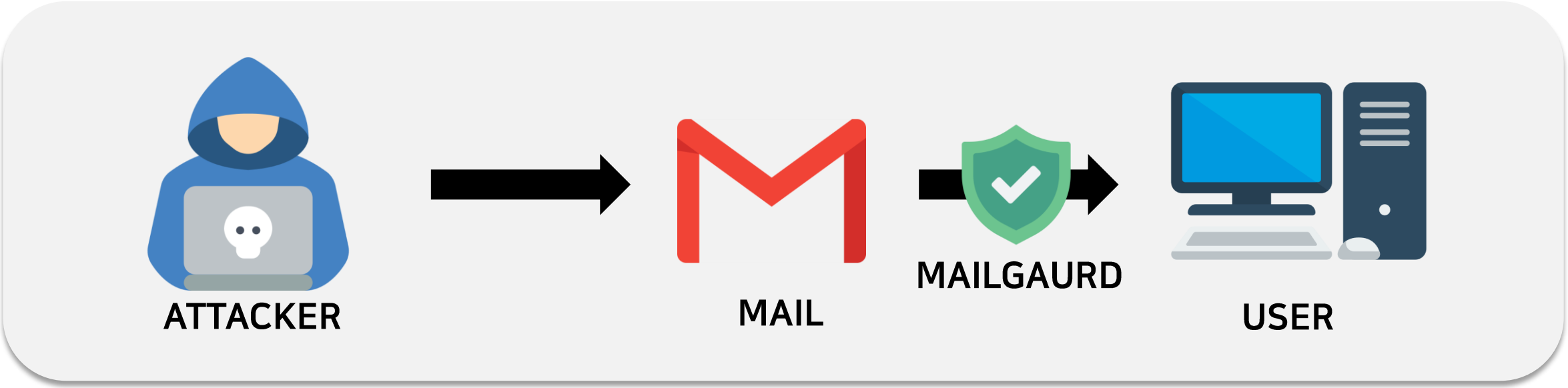
Mail Guard

산학프로젝트 1차 빌드 발표

Genesis 팀
전영우(2021041072)
고재현(2023078075)
심수민(2021041067)

1. 프로젝트 개요

1-1. 시스템 개요



목차

1. 프로젝트 개요

1-2. 시스템 사용자 설명

회원관리

1. 회원가입, 탈퇴
2. 로그인, 아웃
3. 사용자 정보 열람, 수정

메일 동기화

1. 메일 동기화
2. 사용자 환경 설정
3. 메일 선택, 열람관리, 검색, 필터링

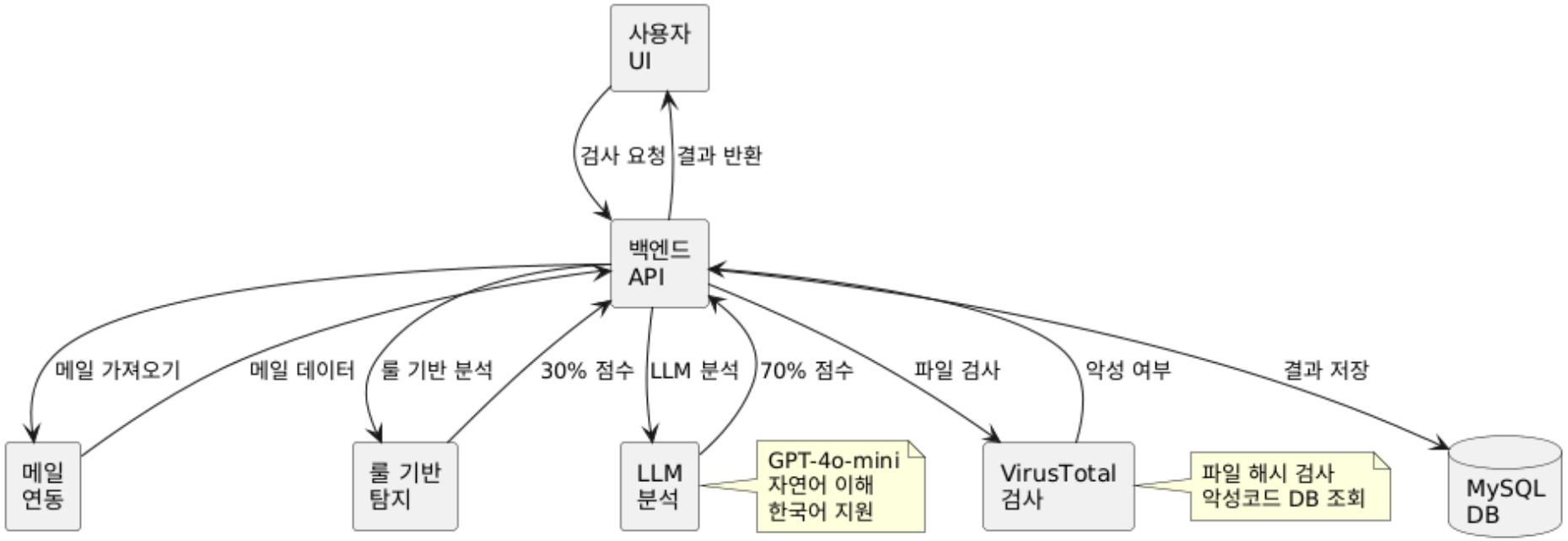
악성메일 검사

1. 피싱 탐지
2. 스미싱 탐지
3. 악성 첨부파일 탐지

1. 프로젝트 개요

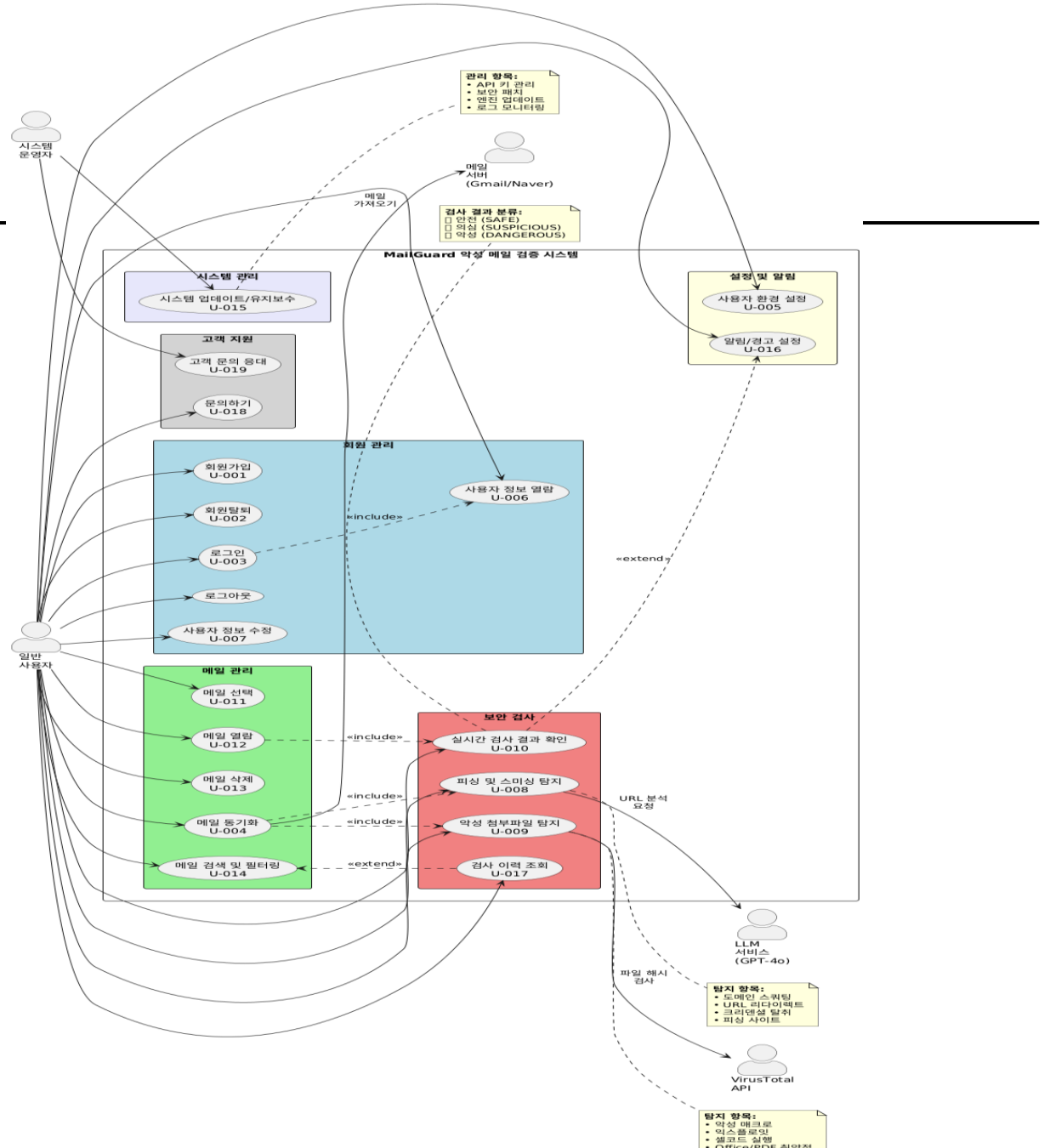
1-3. 운영 개념 및 Flow Chart

브라우저에서 실행가능한 웹 서비스 형태



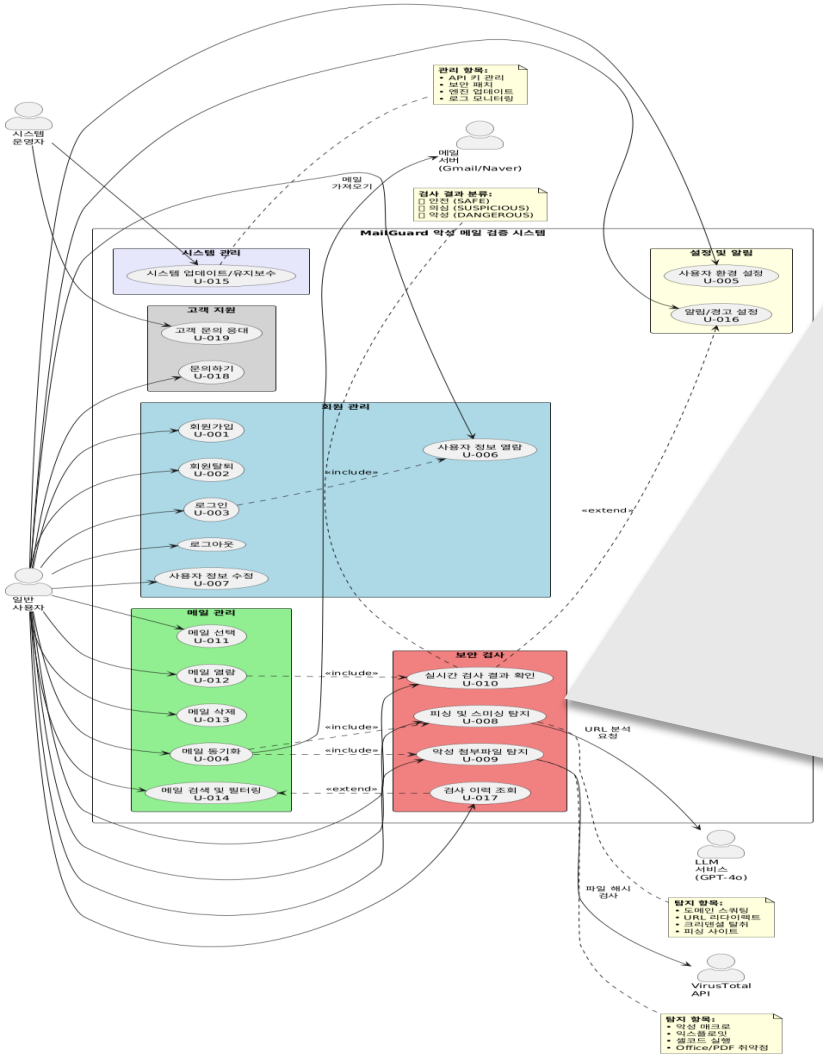
2. 시스템 요구사항

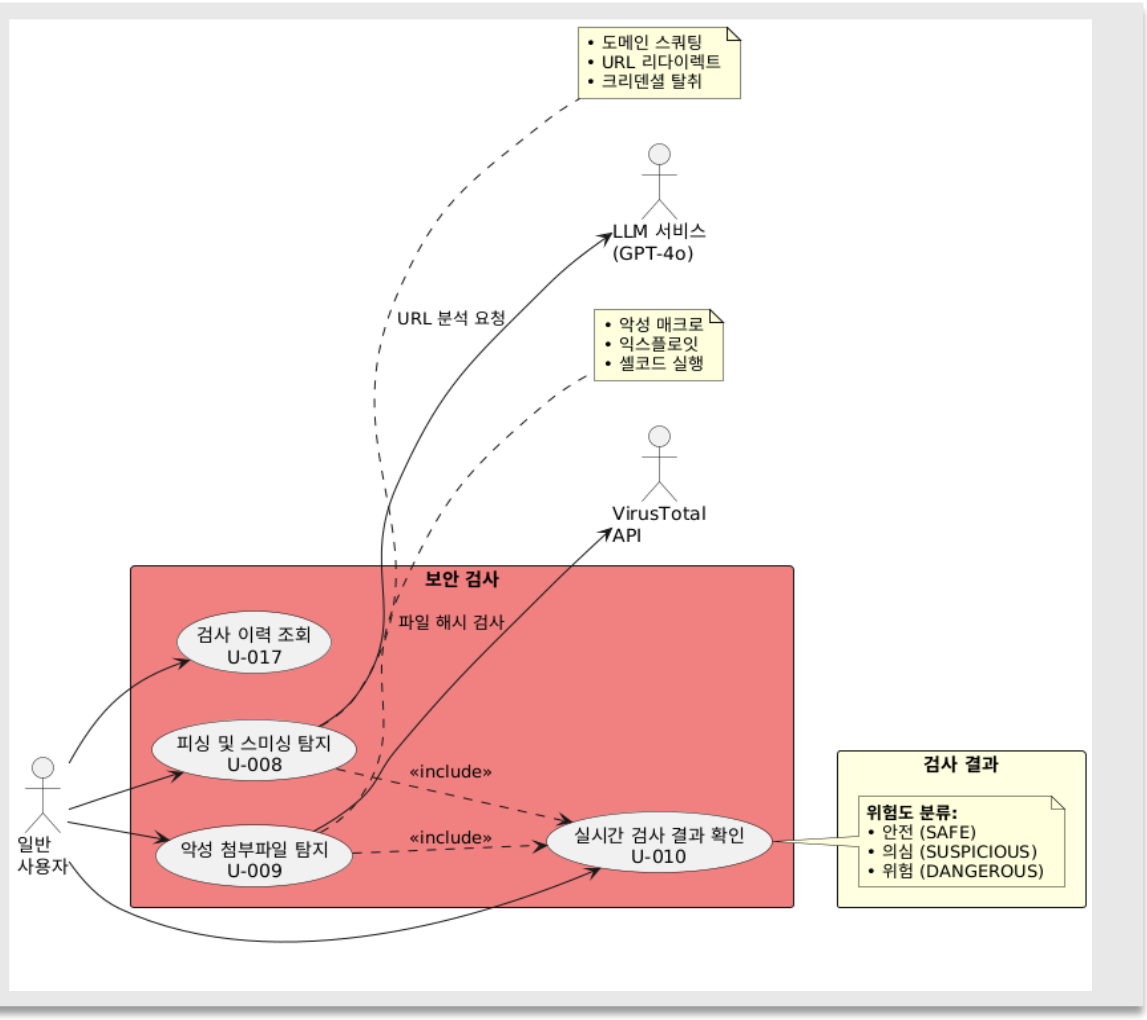
2-1. Use Case Diagram



2. 시스템 요구사항

2-1. Use Case Diagram





2. 시스템 요구사항

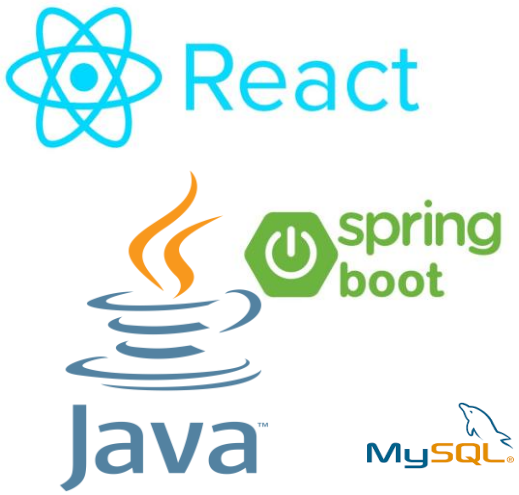
2-2. Product Backlog

주제명	에픽 ID	에픽명	스토리 ID	스토리
피싱/스미싱 탐지	E-1	본문 분석	S1-1	사용자는 이메일 본문 내 URL이 피싱 의심일 경우 자동으로 탐지 및 표기되길 원한다
		실시간 차단	S1-2	시스템은 의심 URL 클릭시 접속을 차단하고 경고 메시지를 제공해야한다.
		외부 연동	S1-3	시스템은 외부 피싱 DB/LLM API와 연동하여 탐지 정확도를 높인다.
악성 첨부 파일 탐지	E-2	메일 선택	S2-1	사용자는 읽고 싶은 메일을 선택한다.
		Hash 연산	S2-2	시스템은 사용자가 선택한 메일의 첨부파일의 Hash값을 계산해야한다.
		외부 API 연동	S2-3	시스템은 Hash값(MD5/SHA256 등)을 Virus Total API에 전송해야한다.
		첨부파일 정보수집	S2-4	Viust Total API에서 첨부파일 해시값에 대응되는 JSON DATA 받아온다.
		GUI제공	S2-5	시스템은 받아온 DATA를 사용자에게 GUI를 통해 제공해야한다.
경고 알림	E-3	피싱/스미싱 탐지	S3-1	시스템은 스미싱, 피싱 여부 가능성을 기준으로 하여 안전, 의심, 경고 표시를 제공한다.
		악성 첨부파일 탐지	S3-2	시스템은 수신한 이메일의 제목, 본문 등을 바탕으로 피싱 혹은 스미싱 / 악성파일 첨부 가능성이 있는지 판단 가능해야 한다.
		결과 제공	S3-3	시스템은 사용자에게 검신 결과를 보고서 형식으로 제공한다.
회원 정보 관리	E-4	회원 정보 입력	S4-1	사용자는 사용할 ID, 비밀번호, 이메일을 작성한다.
		본인인증 메일 발송	S4-2	시스템은 사용자가 입력한 이메일로 본인인증 메일을 발송한다.
		본인인증 확인	S4-3	사용자는 메일로 받은 본인인증 코드를 입력하고 인증받는다.
		새로운 회원 정보 저장	S4-4	시스템은 사용자가 입력한 정보들을 바탕으로 최종적으로 새로운 사용자로 등록한다.
		기존회원 정보 삭제	S4-5	사용자가 등록된 자신의 정보 및 계정을 삭제한다.
		기존 회원 정보 수정	S4-6	시스템은 사용자의 등록된 자신의 정보 수정 요청을 바탕으로 정보 수정을 진행한다.
사용자 정보/환경 관리	E-5	사용자 환경 설정	S5-1	사용자가 기능별 적용 여부를 선택하고 등록한다.
		사용자 정보 열람	S5-2	사용자가 등록된 자신의 정보를 열람한다.
		알림/경고 설정	S5-3	악성 첨부 파일 발견 시 알림 옵션을 설정한다
수신 메일 관리	E-6	메일 선택	S6-1	사용자가 조작하고 싶은 메일을 선택(체크박스와 같은 형태)한다.
		메일 열람	S6-2	사용자가 선택한 메일의 본문과 파일 첨부 여부를 열람한다.
		메일 삭제	S6-3	사용자가 선택한 메일을 시스템에서 삭제한다.
		메일 검색	S6-4	사용자가 특정 메일(보낸사람, 제목 키워드 등)만 입력해서 검사 결과를 확인한다.
		메일 필터링	S6-5	사용자가 선택한 특정 카테고리별로 메일을 분류해 보여준다.
		메일 동기화	S6-6	사용자의 메일 계정에서 메일을 가져와 시스템 DB에 저장한다.
		메일 검사 이력 조회	S6-7	시스템은 특정 메일에 대한 검사 완료 여부에 따른 분류 목록을 제공한다.
시스템 업데이트/유지보수	E-7	보안 패치 관리	S7-1	최신 보안 패치를 적용하여 시스템을 안전하게 유지한다
		외부 API 키 관리	S7-2	외부 API 키를 갱신 및 재발급하여 서비스 중단을 방지한다
		업데이트	S7-3	탐지 엔진(오픈 소스/외부 서비스)을 최신 버전으로 업데이트하여 탐지 정확도를 유지한다
문의 관리	E-8	사용자 문의	S8-1	서비스 이용 중 궁금한 점이나 불편한 사항을 고객센터에 문의한다.
		고객 문의 응대(운영자)	S8-2	접수된 회원 문의에 답변하고 처리한다.

3. 프로젝트 진행현황

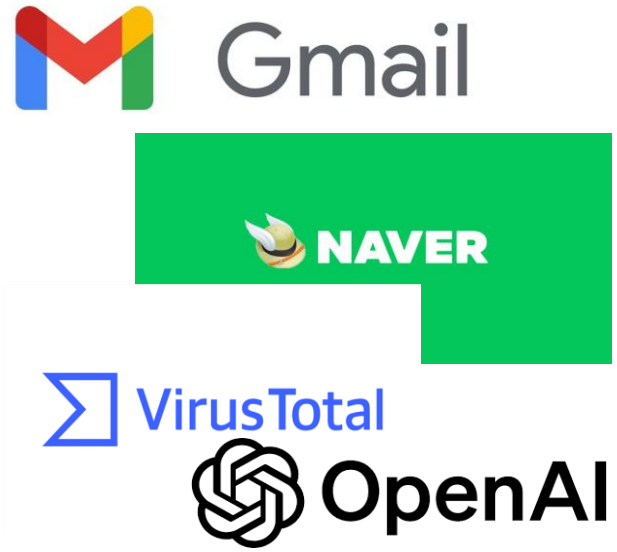
3-1. 개발 환경 및 도구

사용 도구



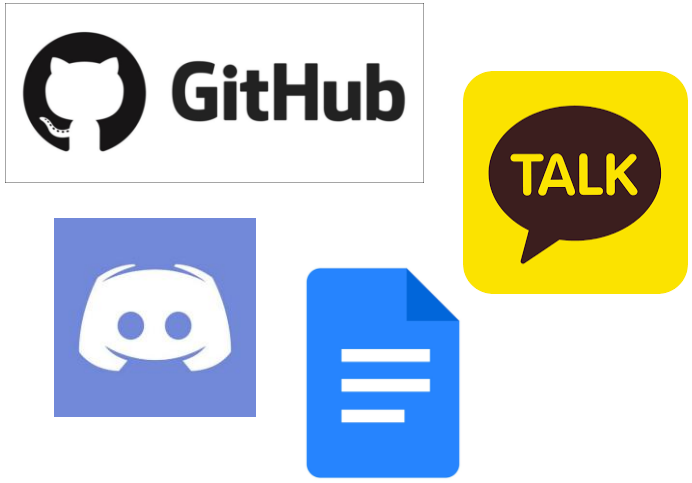
- 프론트 : React
- 백엔드 : SpringBoot
- 로직 구현 : Java
- DB : MySQL

사용 API



- 메일 로딩
  : Naver IMAP / Gmail API
- 악성 메일 판단
- : VirusTotal / OpenAI API

협업 도구



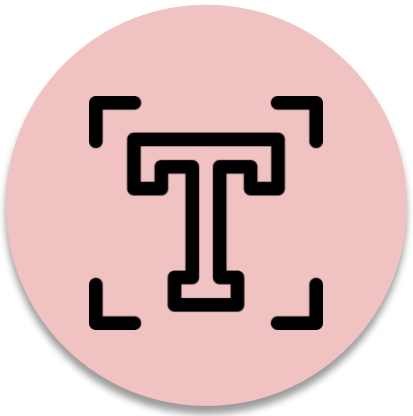
- 의사소통
  : KakaoTalk / Discord
- 프로젝트 관리 : Github
- 문서 작성 : Google Docs

3. 프로젝트 진행현황

3-2. 1차 빌드 구현 목표

기존 구현 목표 : 피싱/스미싱 탐지 기능

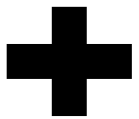
추가 : 유저 정보 관리



제목/본문 분석

본문 URL 분석

첨부파일 분석



회원가입
로그인
...

3. 프로젝트 진행현황

3-3. 태스크 목록(Task 1 ~ Task 2)

번호	태스크명	담당자	소요기간	완료 여부	비고
T1-1	Mail api 연동	고재현	27일	완료	
T1-2	Ui 디자인	고재현	27일	완료	
T1-3	탐지 결과 인터페이스 표시	고재현	35일	완료	
T1-4	관리 루프 구축	고재현	-	미완료	
T2-1	URL 차단 로직 구현	전영우	28일	완료	Black-List기반 도메인 차단 형식
T2-2	경고 메세지 팝업 알림	전영우	28일	완료	
T2-3	URL 의심 여부 판별	전영우	28일	완료	
T2-4	URL 접속 허용	전영우	28일	완료	
T2-5	URL 접속 차단	전영우	28일	완료	

3. 프로젝트 진행현황

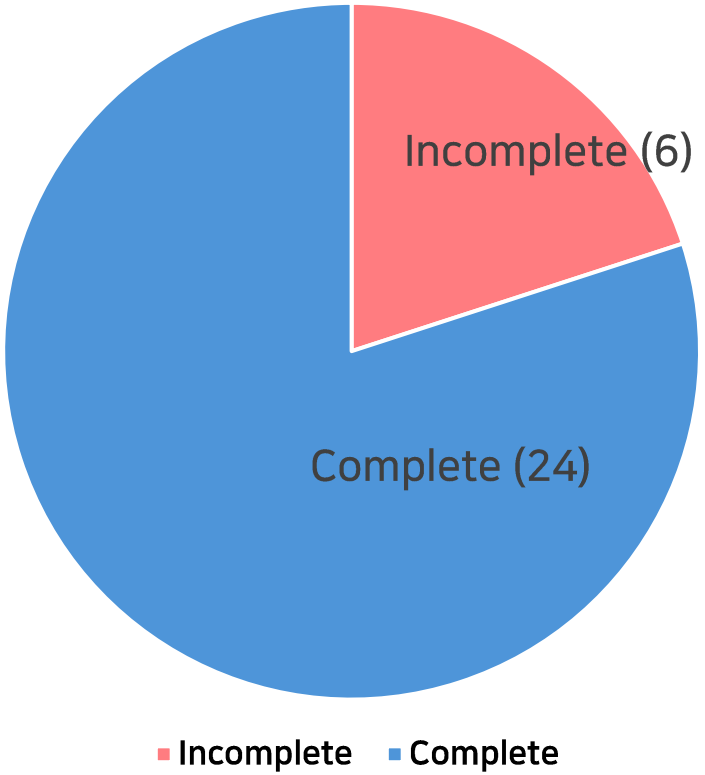
3-3. 태스크 목록(Task 3 ~ Task 9)

번호	태스크명	담당자	소요기간	완료 여부	비고
T3-1	메일 본문/제목 분석용 LLM 모델 설정	고재현, 전영우	35일	완료	OpenAI API 이용한 분류 방식 사용
T3-2	메일 한국어 데이터셋 확보	고재현, 전영우	35일	완료	
T3-3	LLM 모델 학습	고재현, 전영우	35일	완료	
T3-4	어플리케이션과 상호작용 위한 API 구현	고재현, 전영우	-	미완료	
T4-1	수신된 메일 목록 화면 구현(UI)	심수민	-	미완료	
T4-2	메일 목록에서 클릭 이벤트 구현	심수민	-	미완료	
T4-3	선택한 메일의 정보 (첨부파일 유무, 본문 글)분석 로직 구현	심수민	21일	완료	
...	...	...	...	...	...

3. 프로젝트 진행현황

3-4. 1차 빌드 스프린트 진도율

Task Status Distribution (전체 Task 수 : 30)



계획 대비 진도율 : 80%

전체 task 수 : 30

완료된 task 수 : 24

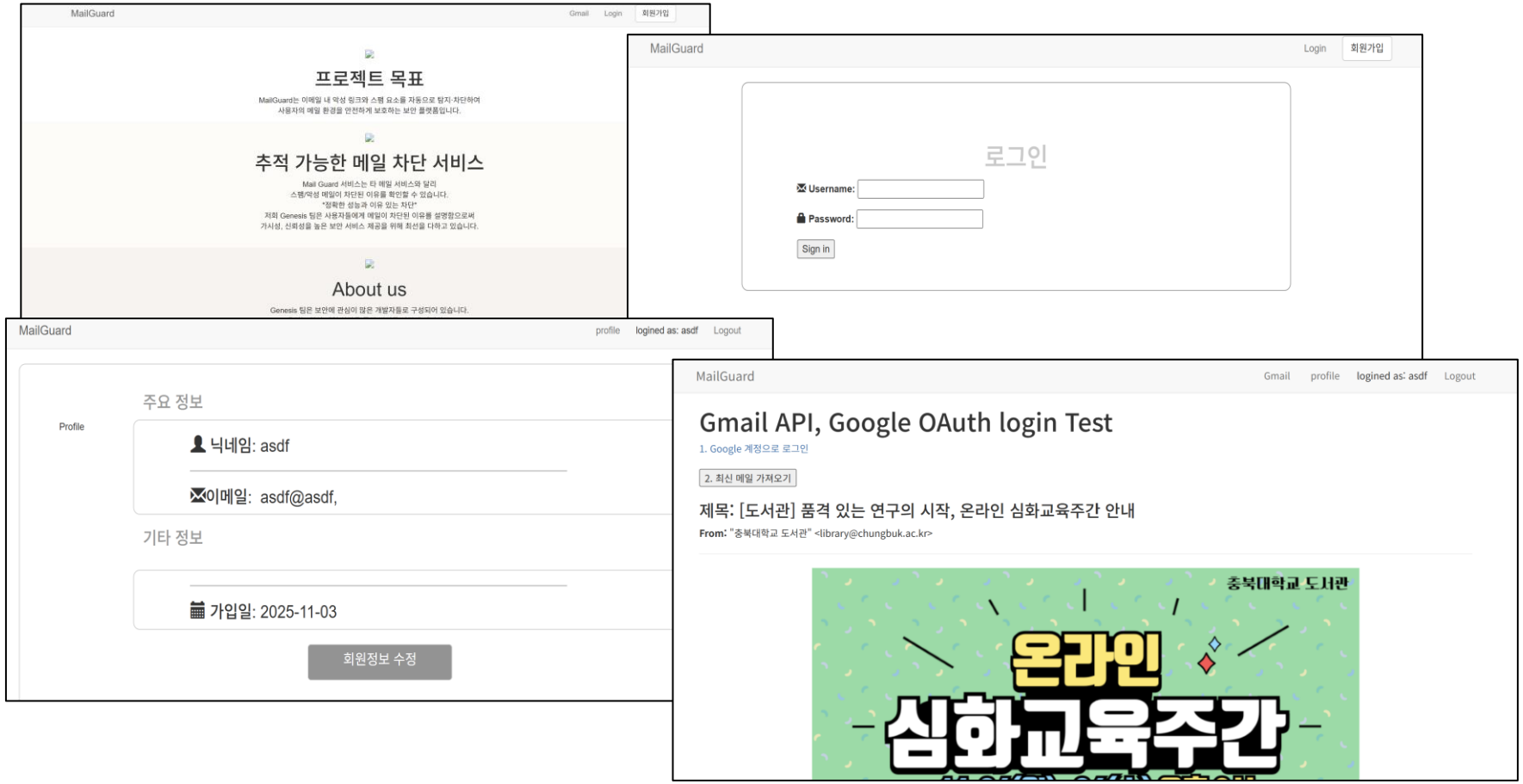
미완료된 task수 : 6

3. 프로젝트 진행현황

3-5. 구현 내용(UI)

구현 GUI

1. Welcome page
2. 로그인 page
3. 회원가입 page
4. mail fetch page

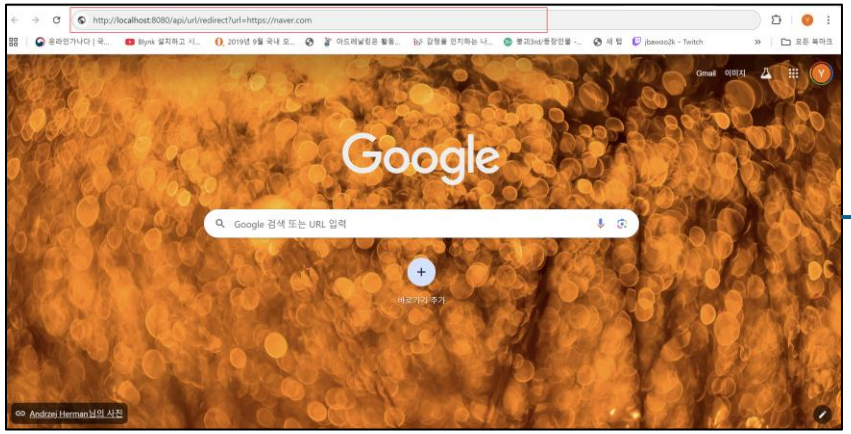


3. 프로젝트 진행현황

3-5. 구현 내용 (URL Blocker)

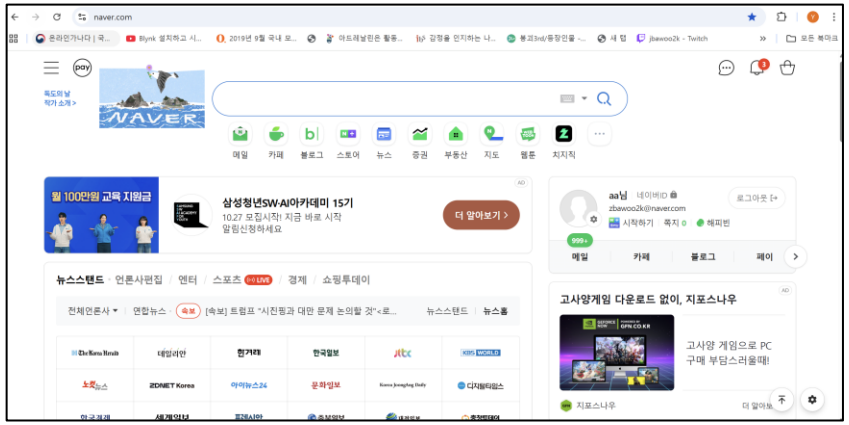
Black-list 기반 도메인 차단 기능 구현

1. 파이썬 이용한 악성 도메인 csv파일 생성
2. csv 파일 DB에 업로드
3. 스프링 부트 실행 후 리다이렉션 차단 확인

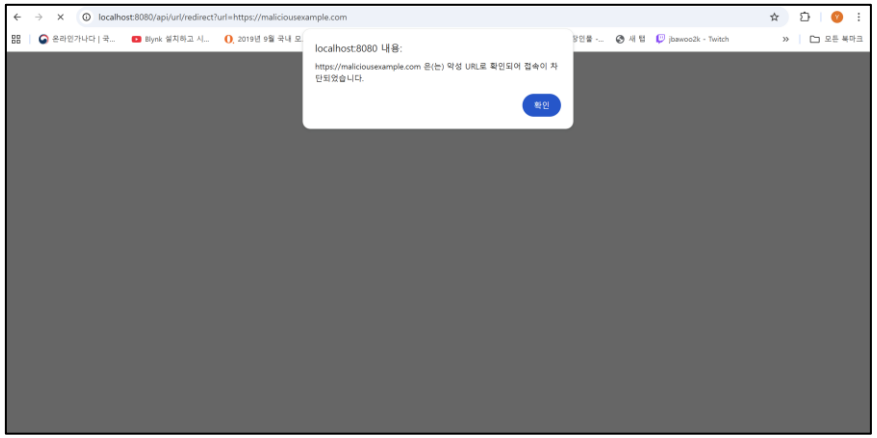


차단 로직

정상



차단



3. 프로젝트 진행현황

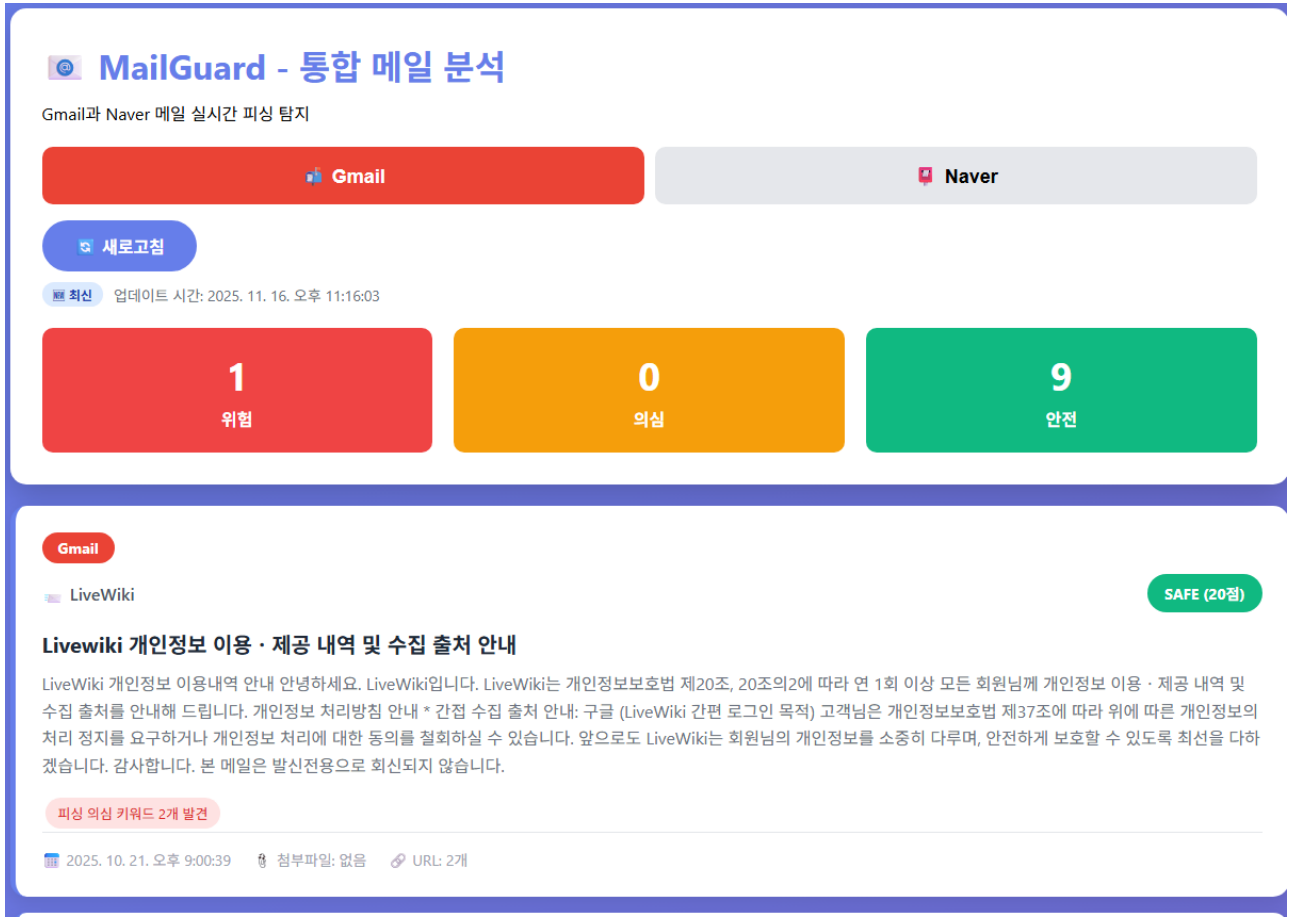
3-5. 구현 내용 (본문,제목 악성 분석)

LLM API 이용한 메일 분석

1. Gmail, naver 메일 연동

2. 룰기반 + gpt 평가

3. 위험도 3단계 분류



3. 프로젝트 진행현황

3-5. 구현 내용 (첨부파일 검사)

Virus Total을 이용한 첨부파일 분석

1. Gmail, naver 메일 첨부파일 연동

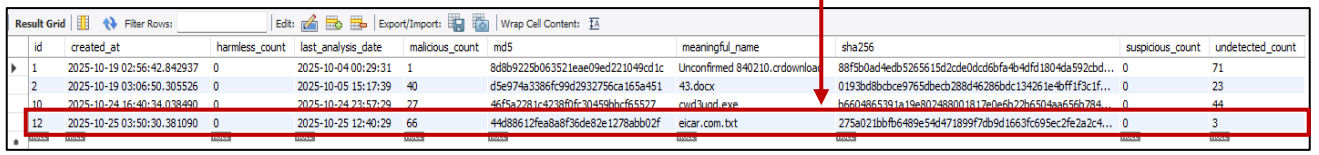
2. 첨부파일 유형별 분류

3. Virus Total을 통한 첨부파일 악성 판별

<로그인&메일 가져오는 페이지>

EICAR test file 테스트

<압축파일 비밀번호 입력&검사>



id	created_at	harmless_count	last_analysis_date	malicious_count	md5	meaningful_name	sha256	suspicious_count	undetected_count
1	2025-10-19 02:56:42.842937	0	2025-10-04 00:29:31	1	8d8b9225b063521eae09ed221049cd1c	Unconfirmed 840210.crdownload	88f5b0ad4edb5265615d2cde0dcd6bfa4b4dfd1804da592cbd...	0	71
2	2025-10-19 03:06:50.305526	0	2025-10-05 15:17:39	40	d5e974a3386fc99d2932756ca165a451	43.docx	0193bd8bcbce9765dbecb288d46286bdc134261e4bff1f3c1f...	0	23
10	2025-10-24 16:40:34.038490	0	2025-10-24 23:57:29	27	46f5a2281c4238f0fc30459bbcf65527	cwd3upd.exe	b6604865391a19e80248800181 7e0e6b22b6504aa656b784...	0	44
12	2025-10-25 03:50:30.381090	0	2025-10-25 12:40:29	66	44d88612fea8a8f36de82e1278abb02f	eicar.com.txt	275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4...	0	3

<검사 결과 DB에 저장>

4. DEMO

DEMO

4. 문제점 및 추후계획

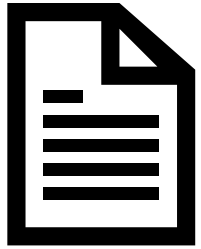
4-1. 문제점

API 키 발급 갱신 필요	API KEY의 사용 기간/API KEY 사용량 제한 API KEY모니터링 및 갱신 필요
OpenAI API - 분석 속도	Open AI API 를 이용해 악성 메일을 판별하는 기능을 구현. 테스팅 결과 – 속도가 예상보다 느림
시스템의 외부 API 의존성	OpenAI API / VirusTotal API 등 구축된 외부 API를 이용해서 구현 외부 API 성능 및 기능에 의해 시스템이 제약을 받음

4. 문제점 및 추후계획

4-2. 추후계획

악성 메일
분석 보고서 생성 기능



스프린트 백로그에 맞춘
추가 기능 구현

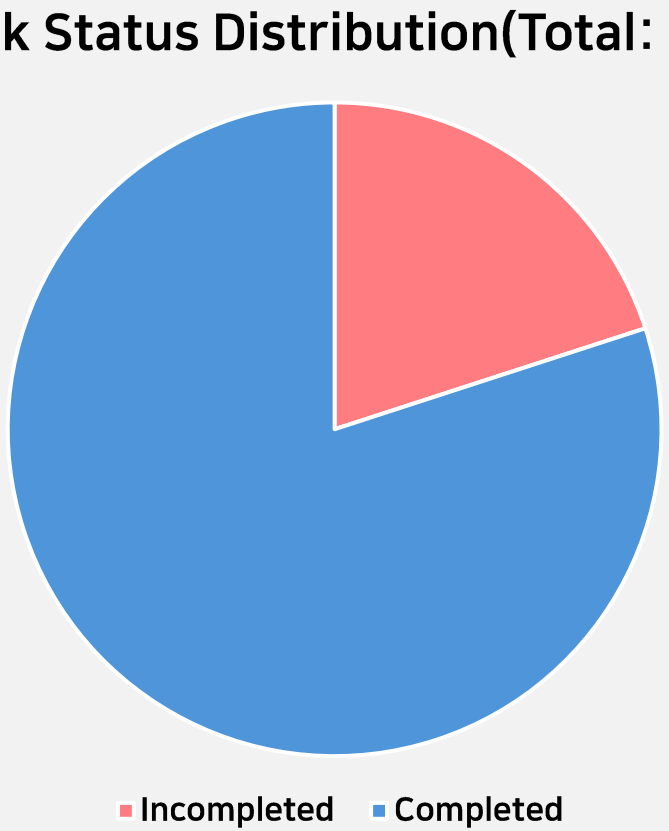
Chrome 확장 프로그램
vs 웹 서비스

Q&A

목차(참고용. 최종본에서는 삭제)

3. 프로젝트 진행현황

3-4. 1차 스프린트 진도율



진도율 체크_1차 스프린트

- 전체 task 수 : 30
- 완료된 task 수 : 24
- 미완료된 task수 : 6

계획 대비 진도율 : 80%

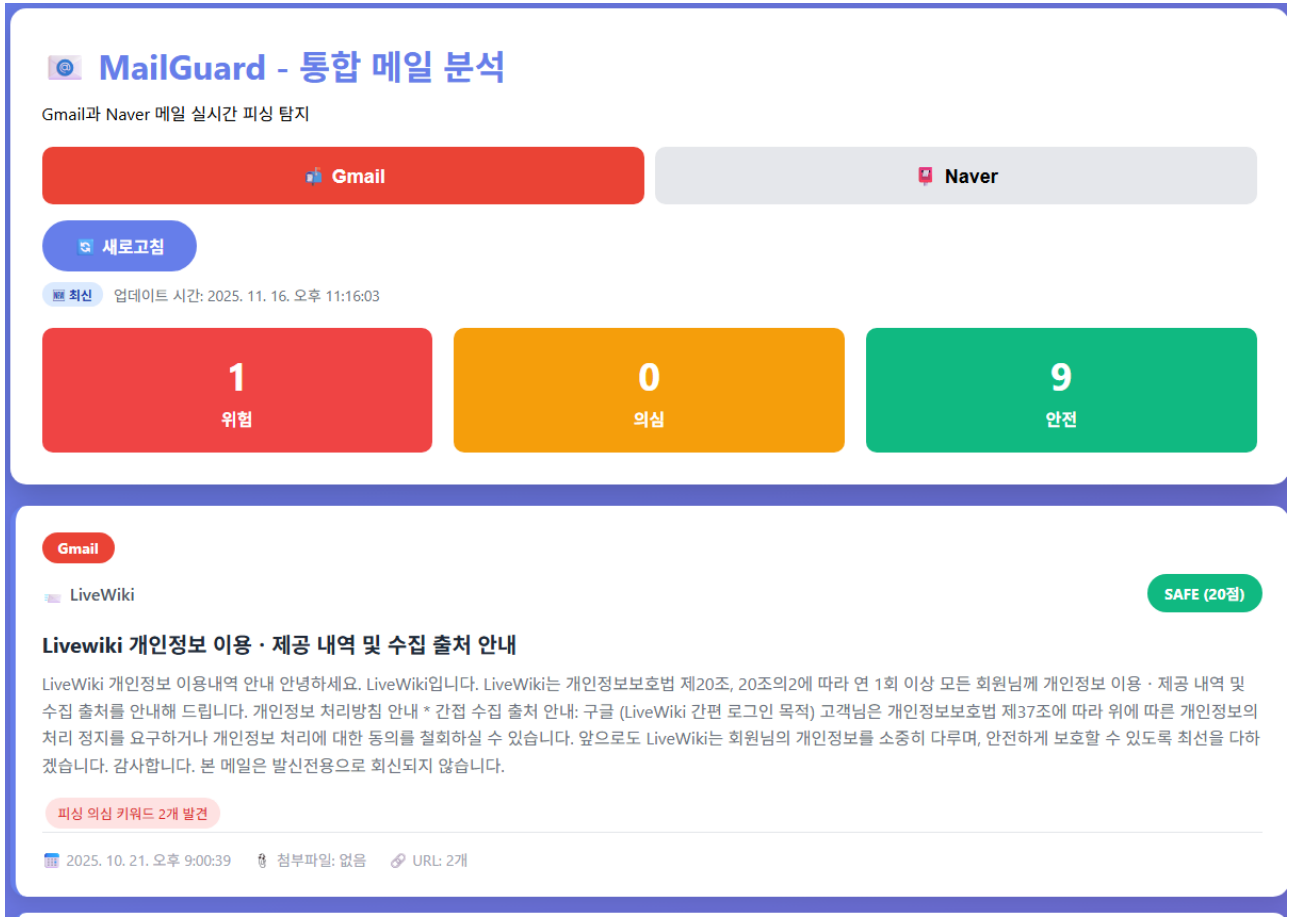
3. 프로젝트 진행현황

3-5. 구현 내용 ()

1.Gmail, naver 메일 연동

2.룰기반 + gpt 평가

3.위험도 3단계 분류



4. 문제점 및 추후계획

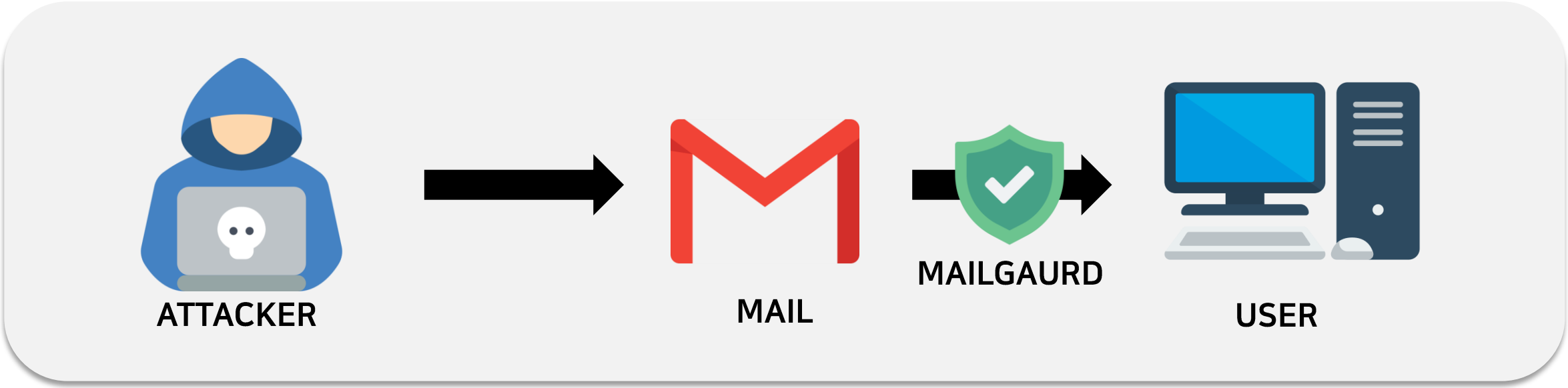
4-1. 문제점

API 의존성

API 키 발급 갱신 필요	API key의 기간이 끝나거나 혹은 api key 사용량을 모두 사용했는지를 지속적으로 모니터링하고 갱신할 필요가 있음.
Open AI API - 분석 속도	Open AI API 를 이용해 악성 메일을 판별하는 기능을 구현. 테스팅 결과 - 속도가 느린 문제점이 발생함.
API 키 발급 갱신 필요	OpenAI API / VirusTotal API 등 API를 이용해서 구현했습니 다만, api key에 사용량에 한계가 있는 단점이 존재함.

1. 프로젝트 개요

1-1. 시스템 개요



4. 문제점 및 추후계획

4-2. 추후계획

악성 메일 분석 보고서 생성 기능

메일이 악성/정상 여부를 검토된 후, 해당 메일이 악성이라면 악성으로 판별된 이유에 대해 문서의 형태로 확인할 수 있는 기능 구현을 목표하고 있습니다.

스프린트 백로그에 맞춘 추가 기능 구현

악성 메일 판별 및 회원 가입 로직 이외 스프린트 백로그에 정의된 기능들의 추가적인 구현을 목표하고 있습니다.

검토중인 사안

Chrome 확장 프로그램 서비스 vs 웹

유저 사용의 편의성 측면 증진을 위해 크롬 확장 프로그램 형식을 활용한 서비스 제공 방식을 검토 중입니다.