

# API 설계서

## 1. 기본 정보

- **Base URL:** http://localhost:8080
- 인증 방식: JWT Bearer Token + Refresh Token
- **Content-Type:** application/json
- **API 버전:** v1

## 2. 공통 응답 형식

### 2.1 성공 응답

```
{
  "success": true,
  "data": {},
  "message": "요청이 성공적으로 처리되었습니다.",
  "timestamp": "2024-01-01T12:00:00Z"
}
```

### 2.2 오류 응답

```
{
  "success": false,
  "message": "오류 메시지",
  "errorCode": "ERROR_CODE",
  "timestamp": "2024-01-01T12:00:00Z"
}
```

## 3. 인증 API

### 3.1 로그인

- **POST** /api/v1/auth/signin

요청 본문:

```
{
  "username": "admin",

```

```
"password": "admin123!@#"
}
```

응답:

```
{
  "token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9...",
  "type": "Bearer",
  "refreshToken": "550e8400-e29b-41d4-a716-446655440000",
  "id": 1,
  "username": "admin",
  "email": "admin@company.com",
  "role": "CEO",
  "expiresIn": 86400
}
```

### 3.2 토큰 리프레쉬

- **POST** /api/v1/auth/refreshtoken

요청 본문:

```
{
  "refreshToken": "550e8400-e29b-41d4-a716-446655440000"
}
```

응답:

```
{
  "token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJ1c2VybmFtZSIsImV4cCI6MTcyMDg2NzlwMH0...",
  "type": "Bearer",
  "refreshToken": "your_refresh_token_here",
  "id": 1,
  "username": "testuser",
  "email": "test@example.com",
  "role": "ROLE_USER",
  "expiresIn": 3600
}
```

### 3.3 로그아웃

- **POST** /api/v1/auth/signout

요청 본문:

```
{
  "refreshToken": "550e8400-e29b-41d4-a716-446655440000"
}
```

응답:

```
{
  "message": "로그아웃되었습니다.",
  "success": true
}
```

### 3.4 모든 기기에서 로그아웃

- **POST** /api/v1/auth/signout-all

헤더: Authorization: Bearer {token}

응답:

```
{
  "message": "모든 기기에서 로그아웃되었습니다.",
  "success": true
}
```

## 4. 문서 관리 API

### 4.1 문서 업로드

- **POST** /documents/upload
- **Content-Type**: multipart/form-data
- 헤더: Authorization: Bearer {token}

요청 본문 (**Form Data**):

```
{
  "file": "파일 객체",
  "title": "문서 제목",
  "content": "문서 내용",
  "categoryTypeId": 1,
  "readRoleId": 5
}
```

```
}
```

응답:

```
{
  "id": 1,
  "title": "문서 제목",
  "fileName": "example.pdf",
  "filePath": "550e8400-e29b-41d4-a716-446655440000",
  "fileSize": 1024000,
  "mimeType": "application/pdf",
  "status": "PROCESSING",
  "author": "1",
  "createdRole": "MANAGER",
  "createdAt": "2024-01-01T12:00:00"
}
```

## 4.2 문서 목록 조회

- **GET** /documents
- 헤더: Authorization: Bearer {token}

쿼리 파라미터:

- categoryTypeId: 카테고리 필터링 (선택)
- startDate: 시작일 필터링 (선택)
- endDate: 종료일 필터링 (선택)

응답:

```
[
  {
    "id": 1,
    "fileName": "example.pdf",
    "filePath": "550e8400-e29b-41d4-a716-446655440000",
    "fileSize": 1024000,
    "mimeType": "application/pdf",
    "owner": "1",
    "createdRole": "MANAGER",
    "createdAt": "2024-01-01T12:00:00",
    "status": "COMPLETED",
    "readRole": {
      "id": 5,
      "name": "MANAGER",

```

```

    "description": "과장",
    "level": 5
  },
  "categories": [
    {
      "id": 1,
      "name": "A",
      "description": "Category A"
    }
  ]
}
]

```

#### 4.4 문서 상세 조회

- **GET** /documents/files/{hash}
- 헤더: Authorization: Bearer {token}
- 응답:

```

{
  "id": 123,
  "fileName": "장애 대응매뉴얼.pdf",
  "filePath": "a1b2c3d4-e5f6-7890-abcd-ef1234567890.pdf",
  "fileSize": 2048576,
  "mimeType": "application/pdf",
  "author": "김개발",
  "owner": "이운영",
  "createdRole": "MANAGER",
  "createdAt": "2024-07-12T10:30:00",
  "status": "COMPLETED",
  "readRole": {
    "id": 2,
    "name": "USER",
    "description": "일반 사용자"
  },
  "categories": [
    {
      "id": 5,
      "name": "장애대응",
      "description": "시스템 장애 대응 관련 문서"
    },
    {
      "id": 8,
      "name": "운영매뉴얼",

```

```
    "description": "운영 가이드 및 매뉴얼"
  }
]
}
```

## 4.5 문서 다운로드

- **GET** /documents/download/{id}
- 헤더: Authorization: Bearer {token}

응답: 파일 스트림 (Content-Disposition: attachment)

## 4.6 문서 상태 조회

- **GET** /documents/{id}/status
- 헤더: Authorization: Bearer {token}

응답:

```
{
  "documentId": 1,
  "status": "COMPLETED"
}
```

# 5. 에러 리포트 API

## 5.1 에러 리포트 목록 조회 (최신순)

- **GET** /api/v1/error-reports/list/latest
- 헤더: Authorization: Bearer {token}

응답:

```
[
  {
    "id": 1,
    "reportTitle": "SQL 인젝션 공격 탐지",
    "reportPreview": "시스템 침해 또는 정보 탈취 목적으로 추정",
    "reportCategory": "ATTACK",
    "reportCategoryDescription": "보안 위협 또는 공격 시도",
    "reportPath": "/app/reports/attack/security_report_20240101_120000.md",
  }
]
```

```
"reportStatus": "NOT_STARTED",
"reportStatusDescription": "시작 안함",
"reportComment": "",
"isDeleted": false,
"createdDt": "2024-01-01T12:00:00",
"deletedDt": null
}
]
```

## 5.2 진행중인 에러 리포트 조회

- **GET** /api/v1/error-reports/list/in-progress
- 헤더: Authorization: Bearer {token}

응답:

```
[
{
  "id": 5,
  "reportTitle": "API 게이트웨이 응답 지연 - 인증 서비스",
  "reportPreview": "인증 서비스 API 응답시간이 평소보다 200% 증가하여 사용자 경험 저하",
  "reportCategory": "VALID",
  "reportCategoryDescription": "정상적인 시스템 오류",
  "reportPath": "/reports/error_report_20240712_005.json",
  "reportStatus": "IN_PROGRESS",
  "reportStatusDescription": "분석 진행 중",
  "reportComment": "로드밸런서 설정 검토 중. 예상 완료시간: 2시간",
  "isDeleted": false,
  "createdDt": "2024-07-12T11:20:00",
  "deletedDt": null
}
]
```

## 5.2 완료된 에러 리포트 조회

- **GET** /api/v1/error-reports/list/completed
- 헤더: Authorization: Bearer {token}
- 응답:

```
[
{
  "id": 3,
  "reportTitle": "SQL 인젝션 공격 차단 완료",
  "reportPreview": "악성 SQL 쿼리 패턴 탐지 후 자동 차단 시스템 작동",
  "reportCategory": "ATTACK",
  "reportCategoryDescription": "보안 공격 의심",

```

```

    "reportPath": "/reports/error_report_20240712_003.json",
    "reportStatus": "COMPLETED",
    "reportStatusDescription": "분석 완료",
    "reportComment": "공격 IP 차단 완료. WAF 규칙 업데이트됨. 추가 모니터링 3일간  
실시",
    "isDeleted": false,
    "createdDt": "2024-07-12T08:45:00",
    "deletedDt": null
  }
]

```

## 5.2 시작되지 않은 리포트 조회

- **GET** /api/v1/error-reports/list/not-started
- 헤더: Authorization: Bearer {token}
- 응답:

```

[
  {
    "id": 25,
    "reportTitle": "DDoS 공격 패턴 의심 - 대량 요청 탐지",
    "reportPreview": "단일 IP에서 초당 1000회 이상의 요청이 10분간 지속됨",
    "reportCategory": "ATTACK",
    "reportCategoryDescription": "보안 공격 의심",
    "reportPath": "/reports/error_report_20240712_025.json",
    "reportStatus": "NOT_STARTED",
    "reportStatusDescription": "분석 대기 중",
    "reportComment": null,
    "isDeleted": false,
    "createdDt": "2024-07-12T12:30:00",
    "deletedDt": null
  }
]

```

## 5.2 공격 탐지 리포트 조회

- **GET** /api/v1/error-reports/list/attacks
- 헤더: Authorization: Bearer {token}

응답:

```

[

```



```
{
  "id": 1,
  "reportTitle": "SQL 인젝션 공격 시도 탐지",
  "reportPreview": "사용자 입력 필드에서 악성 SQL 쿼리 패턴 감지",
  "reportCategory": "ATTACK",
  "reportCategoryDescription": "보안 공격 의심",
  "reportPath": "/reports/error_report_20240712_001.json",
  "reportStatus": "COMPLETED",
  "reportStatusDescription": "분석 완료",
  "reportComment": "공격 IP 차단 완료. WAF 규칙 업데이트. 지속 모니터링 중",
  "isDeleted": false,
  "createdDt": "2024-07-12T14:30:00",
  "deletedDt": null
}
```

### 5.3 정상 리포트 조회

- GET /api/v1/error-reports/list/valid
- 헤더: Authorization: Bearer {token}

응답:

```
[
  {
    "id": 3,
    "reportTitle": "데이터베이스 연결 타임아웃",
    "reportPreview": "높은 트래픽으로 인한 DB 연결 지연 발생",
    "reportCategory": "VALID",
    "reportCategoryDescription": "정상적인 시스템 오류",
    "reportPath": "/reports/error_report_20240712_003.json",
    "reportStatus": "COMPLETED",
    "reportStatusDescription": "분석 완료",
    "reportComment": "커넥션 풀 확장 및 쿼리 최적화 완료",
    "isDeleted": false,
    "createdDt": "2024-07-12T11:30:00",
    "deletedDt": null
  }
]
```

### 5.3 비정상 리포트 조회

- GET /api/v1/error-reports/list/invalid

- 헤더: Authorization: Bearer {token}

응답:

```
[
  {
    "id": 9,
    "reportTitle": "잘못된 JSON 형식 요청",
    "reportPreview": "클라이언트에서 파싱 불가능한 JSON 데이터 전송",
    "reportCategory": "INVALID",
    "reportCategoryDescription": "유효하지 않은 요청",
    "reportPath": "/reports/error_report_20240712_009.json",
    "reportStatus": "COMPLETED",
    "reportStatusDescription": "분석 완료",
    "reportComment": "클라이언트팀 수정 요청 완료. API 문서 업데이트",
    "isDeleted": false,
    "createdDt": "2024-07-12T09:45:00",
    "deletedDt": null
  }
]
```

### 5.3 일별 에러 카운트 통계

- **GET** /api/v1/error-reports/analytics/daily-count
- 헤더: Authorization: Bearer {token}

응답:

```
[
  {
    "date": "2024-01-01",
    "count": 15
  }
]
```

### 5.4 리포트 상태별 통계

- **GET** /api/v1/error-reports/analytics/statistics
- 헤더: Authorization: Bearer {token}

응답:

```
{
  "success": true,
  "data": {
    "NOT_STARTED": 25,
    "IN_PROGRESS": 8,
    "COMPLETED": 67
  },
  "message": "리포트 통계 조회 성공"
}
```

## 5.6 카테고리별 통계 조회

- **GET** /api/v1/error-reports/analytics/category-statistics
- 헤더: Authorization: Bearer {token}
- 응답:

```
{
  "success": true,
  "message": "카테고리별 리포트 통계 조회 성공",
  "data": {
    "ATTACK": 45,
    "VALID": 234,
    "INVALID": 12,
    "SYSTEM_ERROR": 78,
    "NETWORK_ERROR": 23,
    "DATABASE_ERROR": 56
  },
  "errorCode": null,
  "timestamp": "2024-07-12T10:30:00Z"
}
```

## 5.6 최근 공격 탐지 건수 조회

- **GET** /api/v1/error-reports/analytics/recent-attacks
- 헤더: Authorization: Bearer {token}

쿼리 파라미터:

- **days** (선택, 기본값: 7): 조회할 일수 (예: 7일, 30일)
- 응답:

```
{
  "success": true,
  "message": "최근 7일간 공격 탐지 건수 조회 성공",
  "data": 45,
}
```

```
"errorCode": null,  
"timestamp": "2024-07-12T10:30:00Z"  
}
```

## 5.6 전체 에러 리포트 리스트 조회

- **GET** /api/v1/error-reports/list/all
- 헤더: Authorization: Bearer {token}
- 응답:

```
[  
  {  
    "id": 1,  
    "reportTitle": "데이터베이스 연결 실패 - 서버 응답 지연",  
    "reportPreview": "주요 데이터베이스 연결이 3초 이상 지연되어 서비스 영향 발생",  
    "reportCategory": "ATTACK",  
    "reportCategoryDescription": "보안 공격 의심",  
    "reportPath": "/reports/error_report_20240712_001.json",  
    "reportStatus": "COMPLETED",  
    "reportStatusDescription": "분석 완료",  
    "reportComment": "긴급 대응 완료. 추가 모니터링 진행 중",  
    "isDeleted": false,  
    "createdDt": "2024-07-12T10:30:00",  
    "deletedDt": null  
  },  
  {  
    "id": 2,  
    "reportTitle": "API 응답 시간 초과 - 로그인 서비스",  
    "reportPreview": "로그인 API 응답시간이 5초를 초과하여 타임아웃 발생",  
    "reportCategory": "VALID",  
    "reportCategoryDescription": "정상적인 시스템 오류",  
    "reportPath": "/reports/error_report_20240712_002.json",  
    "reportStatus": "IN_PROGRESS",  
    "reportStatusDescription": "분석 진행 중",  
    "reportComment": "서버 부하 증가로 인한 지연. 스케일링 검토 중",  
    "isDeleted": false,  
    "createdDt": "2024-07-12T09:15:00",  
    "deletedDt": null  
  }  
]
```

## 5.6 리포트 상태 변경

- **PATCH** /api/v1/error-reports/{id}/status/completed
- 헤더: Authorization: Bearer {token}

응답:

```
{
  "success": true,
  "message": "리포트 처리가 완료되었습니다.",
  "data": {
    "id": 123,
    "reportTitle": "SQL 인젝션 공격 시도 탐지",
    "reportPreview": "사용자 입력 필드에서 악성 SQL 쿼리 패턴 감지",
    "reportCategory": "ATTACK",
    "reportCategoryDescription": "보안 공격 의심",
    "reportPath": "/reports/error_report_20240712_123.json",
    "reportStatus": "COMPLETED",
    "reportStatusDescription": "분석 완료",
    "reportComment": "보안 패치 적용 완료",
    "isDeleted": false,
    "createdDt": "2024-07-12T14:30:00",
    "deletedDt": null
  },
  "errorCode": null,
  "timestamp": "2024-07-12T16:00:00Z"
}
```

## 5.7 리포트 코멘트 수정

- **PATCH** /api/v1/error-reports/{id}/comment
- 헤더: Authorization: Bearer {token}

쿼리 파라미터:

- comment: 수정할 코멘트

응답:

```
{
  "success": true,
  "message": "에러 리포트 코멘트가 수정되었습니다.",
  "data": {
    "id": 123,
    "reportTitle": "SQL 인젝션 공격 시도 탐지",
    "reportPreview": "사용자 입력 필드에서 악성 SQL 쿼리 패턴 감지",
    "reportCategory": "ATTACK",

```

```

    "reportCategoryDescription": "보안 공격 의심",
    "reportPath": "/reports/error_report_20240712_123.json",
    "reportStatus": "COMPLETED",
    "reportStatusDescription": "분석 완료",
    "reportComment": "긴급 처리 완료",
    "isDeleted": false,
    "createdDt": "2024-07-12T14:30:00",
    "deletedDt": null
  },
  "errorCode": null,
  "timestamp": "2024-07-12T15:45:00Z"
}

```

## 5.8 리포트 소프트 삭제

- **DELETE** /api/v1/error-reports/{id}
- 헤더: Authorization: Bearer {token}

응답:

```

{
  "success": true,
  "message": "에러 리포트가 삭제되었습니다.",
  "data": null,
  "errorCode": null,
  "timestamp": "2024-07-12T16:30:00Z"
}

```

## 6. HTTP 상태 코드

코드	설명
200	OK - 요청 성공
201	Created - 리소스 생성 성공
400	Bad Request - 잘못된 요청

401	Unauthorized - 인증되지 않음
403	Forbidden - 권한 부족
404	Not Found - 리소스를 찾을 수 없음
409	Conflict - 리소스 충돌
422	Unprocessable Entity - 유효성 검증 실패
500	Internal Server Error - 서버 내부 오류

## 7. 보안 및 제한사항

### 7.1 Rate Limiting

- 로그인 API: 분당 5회
- 일반 API: 분당 100회
- 파일 업로드: 시간당 50회

### 7.2 파일 업로드 제한

- 최대 파일 크기: 50MB
- 허용 MIME 타입: application/pdf, text/plain, image/\*
- 동시 업로드: 사용자당 3개

### 7.3 권한 체크

- 문서 읽기: 사용자 직급  $\geq$  문서 읽기 권한
- 문서 업로드: 자신보다 높은 직급 권한 설정 불가
- CEO 전용 API: JWT 토큰의 role이 CEO인 경우만 접근

### 7.4 토큰 관리

- Access Token 만료시간: 24시간
- Refresh Token 만료시간: 7일
- 기기별 최대 토큰 수: 5개