

# 사내 채팅형 AI Agent를 위한 Outlook MCP Gateway 구축 보고서

Multi-tenant 아키텍처, 보안 전략 및 51개 Tool 구현 범위 정의

---

문서 유형

기술검토/배포 설계안 v2.1

작성일

2026-02-18

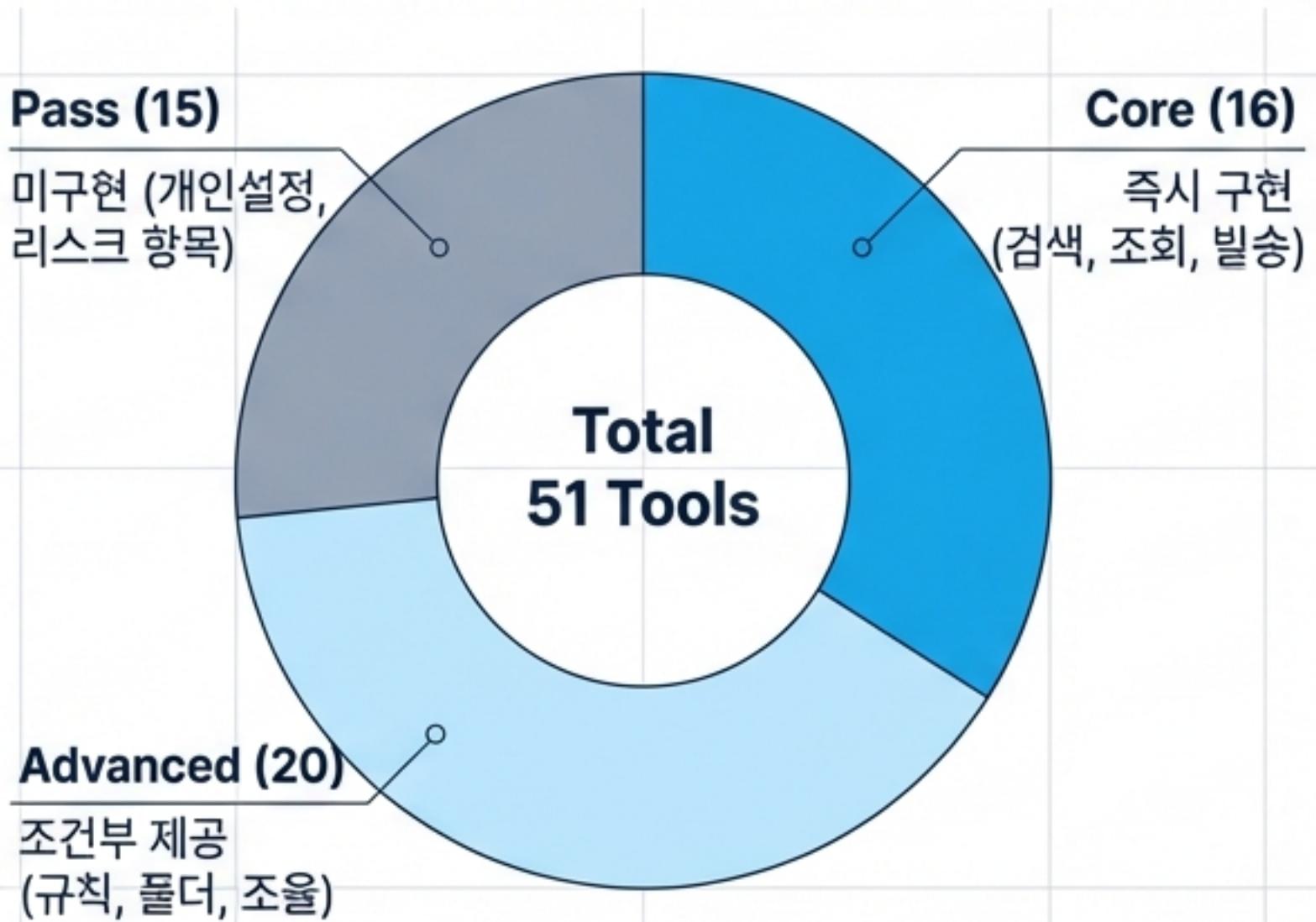
대상

팀장/임원 보고용

# 1. 핵심 요약 (Executive Summary)

## 목표 (Goal)

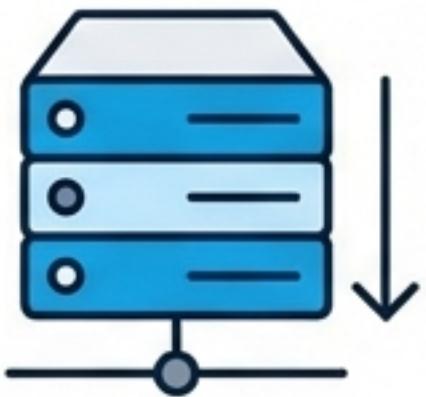
전 임직원이 사내 채팅에서 자연어로 Outlook(메일/일정)을 제어하는 표준 Gateway 구축.  
App-only(테넌트 전권) 권한 확보 후, 사내 Gateway 레벨에서 엄격한 스코프/보안 통제.



## 주요 기술 의사결정 (Key Decisions)

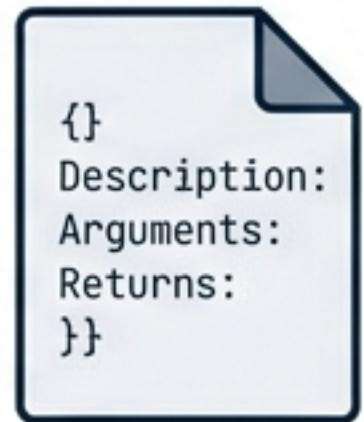
- ✓ 멀티 테넌트 라우팅  
(tenant\_routing\_token 적용)
- ✓ 요청자 검증  
(actor\_email 바인딩으로 Impersonation 방지)
- ✓ 2계층 로깅  
(보안 감사 + 운영 관측)
- ✓ 비즈니스 로직 최소화  
(Thin Server, Thick Context)

## 2. 설계 원칙: Thin Server, Thick Context



### 1. Business Logic Minimization

MCP 서버는 데이터 접근(Data Access)과 액션(Action)만 수행.  
판단, 요약, 추천, 워크플로우  
제어는 AI Agent에게 위임.



### 2. Rich Documentation

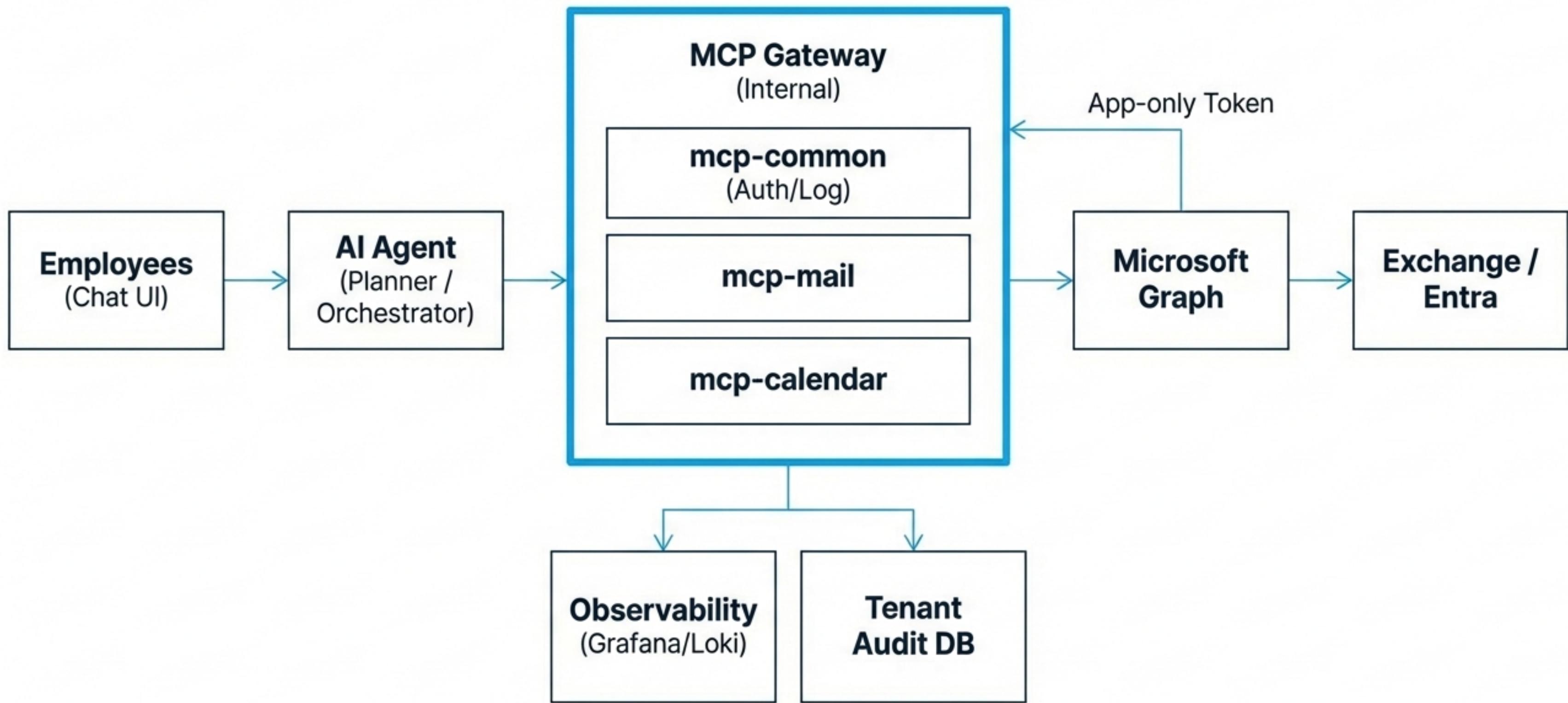
코드 로직 대신 'Description',  
'Arguments', 'Returns' 명세를  
상세화하여 AI의 오호출 방지.  
'언제 사용하는지', '실패 시 대안'을  
프롬프트 레벨에서 가이드.



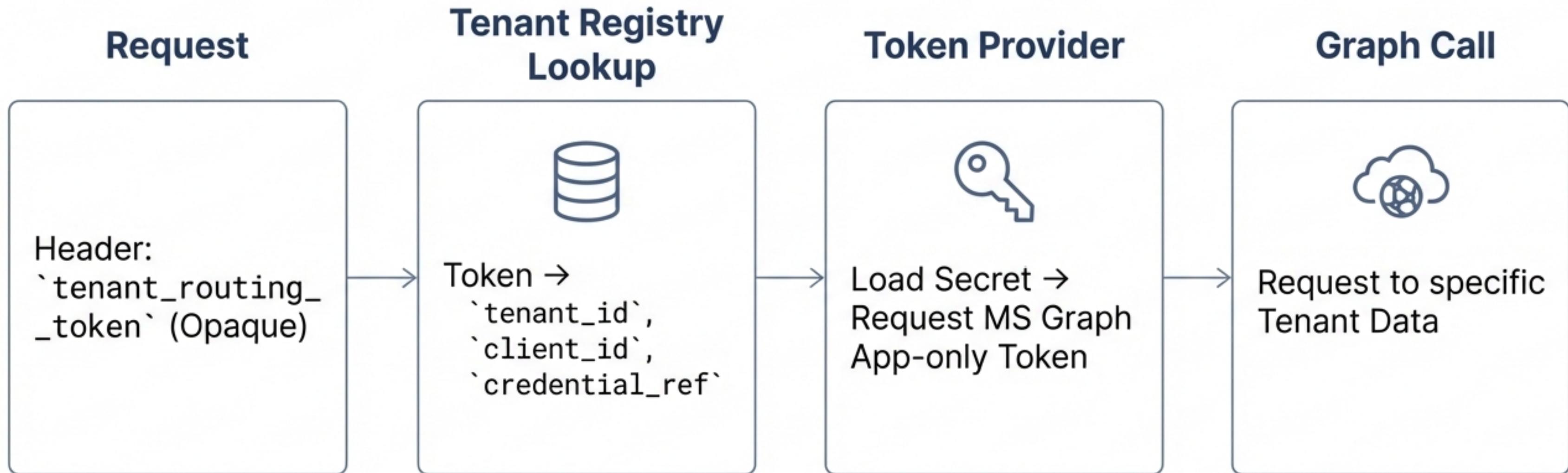
### 3. Safety First

표준 인터페이스로 래핑하여  
필수 공통 기능(인증/라우팅/로깅)  
강제 적용.  
모든 요청에 대한 Audit(감사)  
추적성 확보.

### 3. 전체 아키텍처 (High-Level Architecture)



# 4. 멀티 테넌트 라우팅 전략



Operational Detail: 테넌트별 키 롤오버 지원, 장애 격리(Bulkhead) 적용.

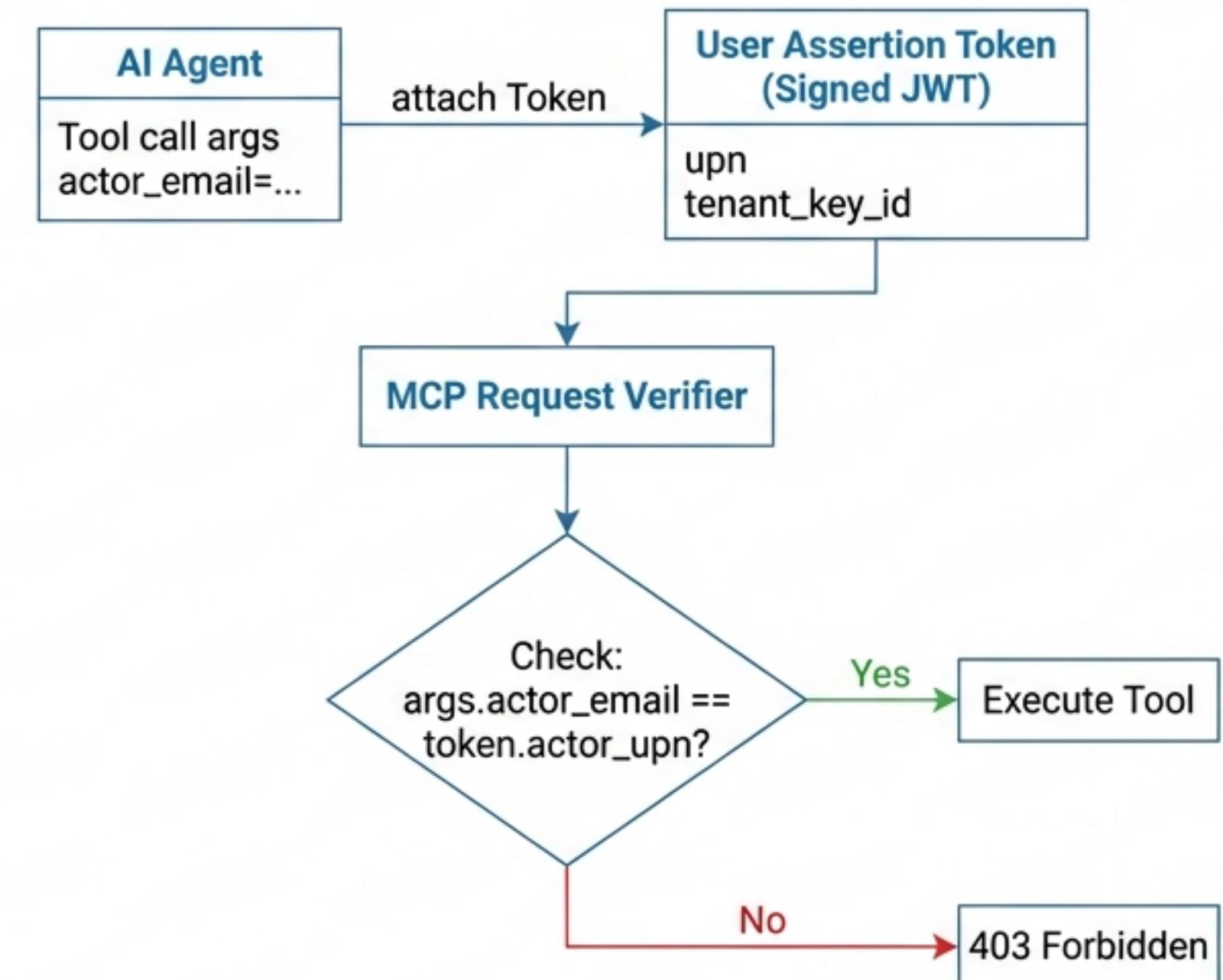
# 5. 보안: 요청자 검증 (Anti-Impersonation)

## The Problem

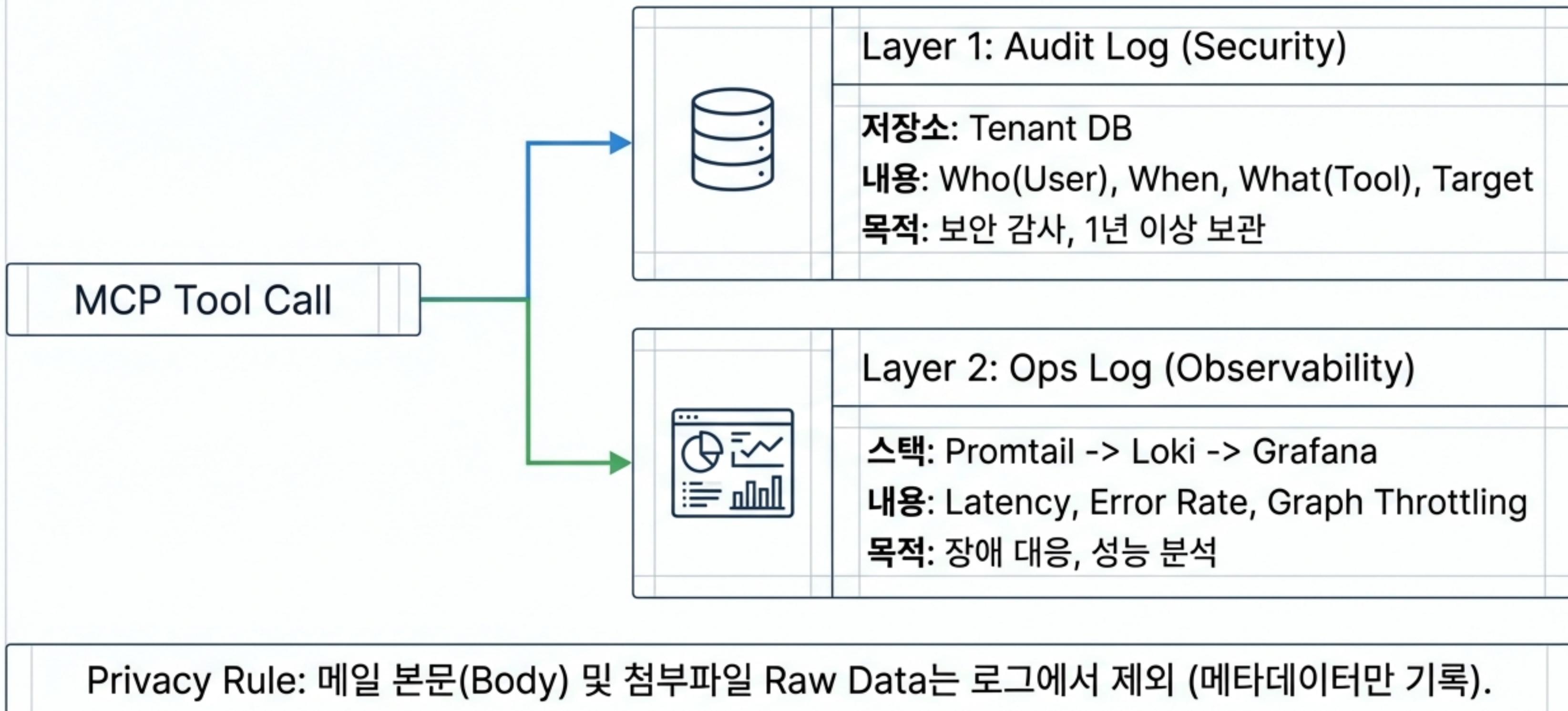
App-only 권한은 강력하므로, 사용자가 `actor\_email` 파라미터를 조작하여 타인의 메일을 훔쳐보는 공격을 방지해야 함.

## The Solution

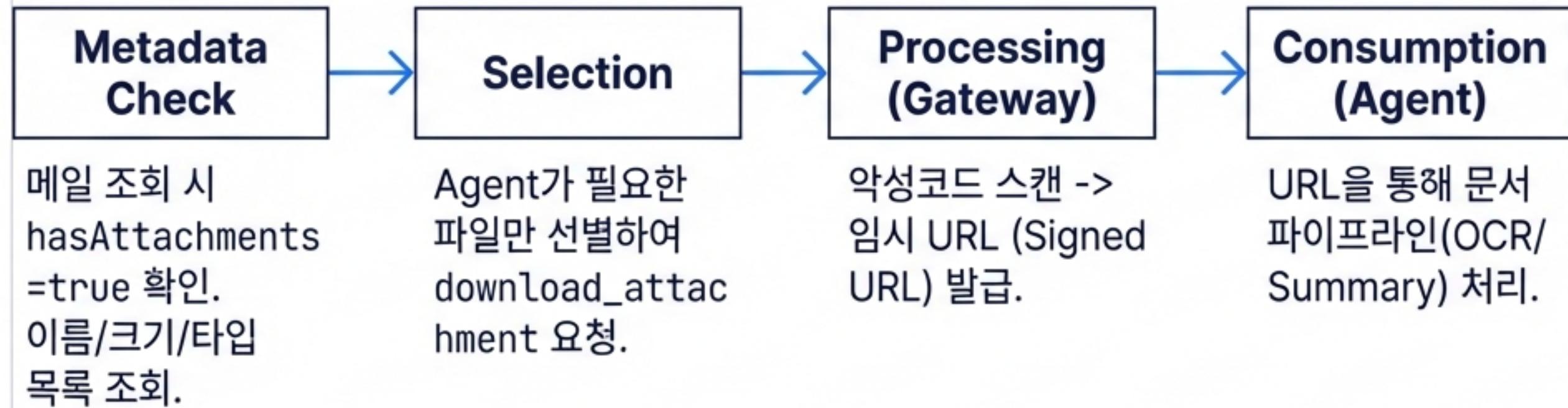
User Assertion Token Binding 적용.  
`actor\_email`은 신뢰 입력이 아니라 검증 대상.



# 6. 2계층 로깅 전략 (Audit & Operations)

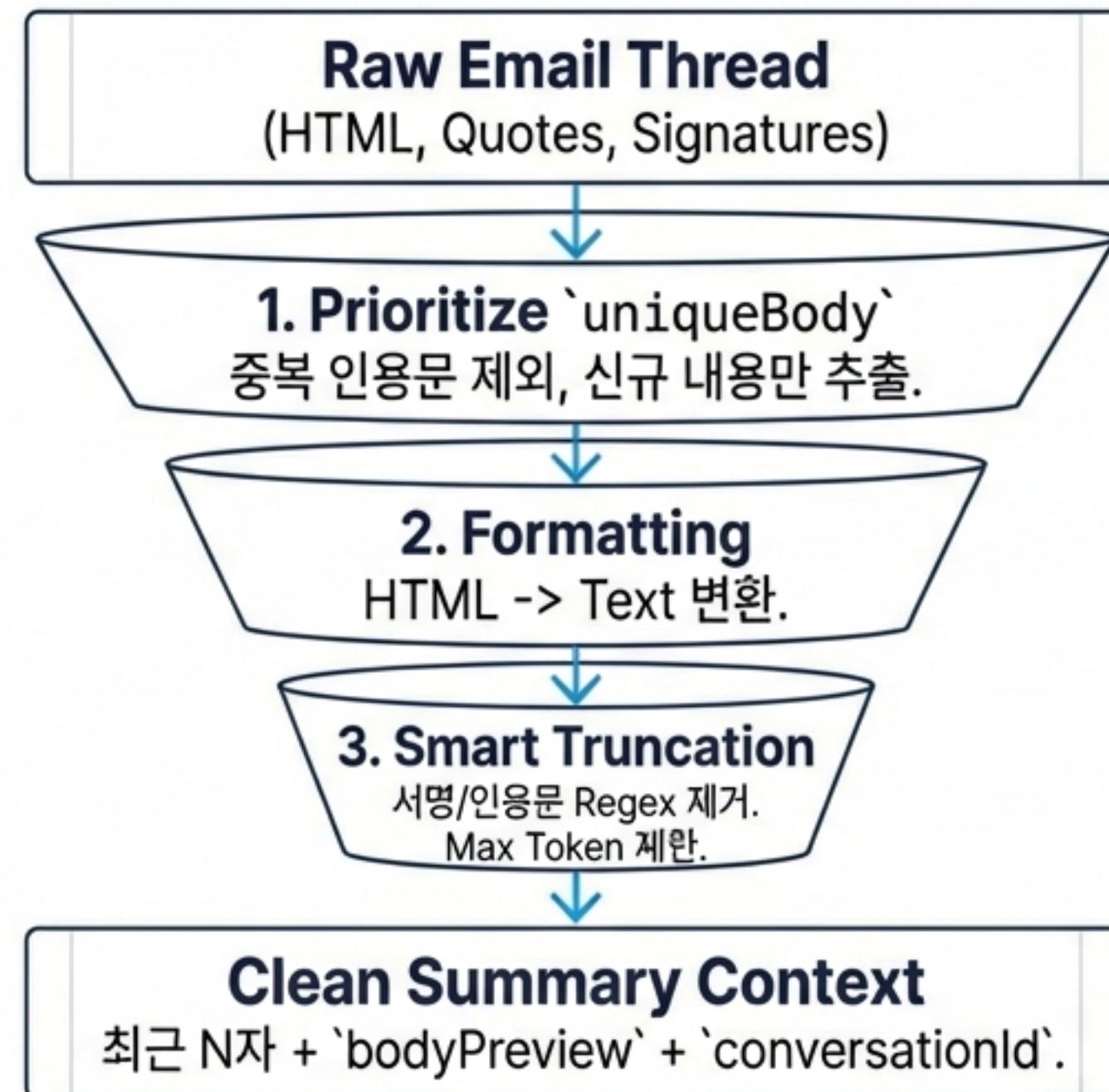


## 7. 예외 처리 가이드: 첨부파일 (Attachments)



<b>Large Files Policy</b> 3MB~150MB 파일은 Upload Session/Streaming 처리 지원.
--

## 8. 예외 처리 가이드: 긴 메일 스레드 (Long Threads)



**Rolling Summary:** 매우 긴 스레드는 `conversationId`로 분할 조회하여 단계적 요약 수행.

## 9. Tool 구현 범위 및 분류 기준 (Total 51 Tools)

### Core (16개)

#### 기본 제공

전사 보편 시나리오 필수.  
매일 사용.

- 메일 검색/조회/발송
- 일정 브리핑/생성
- 첨부 목록 확인

### Advanced (20개)

#### 조건부 제공

특정 조건/역할 필요.  
Core 안정화 후 확장.

- 규칙 생성
- 폴더 이동/정리
- 회의 조율(FindTime)
- 읽음 처리

### Pass (15개)

#### 미구현

저빈도, 고위험(삭제),  
단순 개인설정.

- 캘린더 삭제
- 개인 프로필 변경
- 일괄 요청(Batch)

# 10. [Scope] Mail - Core Tools (핵심 기능)

Tool Name	Arguments	Description / Purpose
get_messages	folder, top, filter	메일 목록 조회. 리스트 확인 후 선별.
get_message	messageId	메일 상세 조회. 요약/답장 판단용 본문 획득.
search_emails	query (OData)	메일 검색. 키워드/발신자/기간 기반.
create_draft	subject, body, to	답장/신규 메일 초안 생성. 발송 전 검토.
send_email	to, subject, body	메일 실 발송. (User Confirm 필수).
reply_to_email	messageId, comment	스레드 유지 회신.
get_attachments	messageId	첨부파일 메타데이터 목록 조회.

# 11. [Scope] Mail - Advanced Tools (심화/정리 기능)

Tool Name	Arguments	Description / Purpose
forward_email	messageId to	메일 전달 (공유/에스컬레이션).
delete_message	messageId	메일 삭제. (Risk 가드 필요/휴지통 이동).
move_message	messageId destFolder	폴더 이동. 분류 자동화.
mark_as_read	messageId isRead	읽음 처리. Triage 큐 관리.
create_mail_rule	conditions actions	메일 규칙 생성. 자동 분류.
get_mail_folders	-	폴더 트리 조회. 이동 대상 선택.

## 12. [Scope] Calendar - Core Tools (일정 핵심)

Tool Name	Arguments	Description / Purpose
list_events	start, end	일정 목록 조회. 오늘의 브리핑/타임라인.
get_event	eventId	일정 상세. 본문/참석자 확인.
create_event	subject, start, end	새 일정 생성. 회의 잡기.
update_event	eventId, updates	일정 변경. 시간/장소 수정.
delete_event	eventId	일정 삭제/취소.

### Usage Context

'오늘 일정  
브리핑해줘',  
'팀 미팅 잡아줘'  
시나리오의 기반.

# 13. [Scope] Calendar - Advanced & App-only Strategy

## App-only Restriction Strategy

MS Graph `findMeetingTimes` API는 Application 권한을 미지원. 따라서 `get\_schedule` (Free/Busy 조회) API를 사용하여 Availability 데이터 수집 후, MCP 내부 로직으로 슬롯을 계산하여 제공.

Tool Name	Arguments		Description / Purpose
get_schedule	schedules	timeRange	참석자 가용성(Free/Busy) 확인.
find_meeting_times	attendees	duration	(Wrapper) 내부 로직으로 구현. Agent 표준 인터페이스.
accept/decline_event	eventId	comment	초대 응답 자동화.

# 14. [Scope] Contacts & Organization (연락처/조직)

Tool Name	Arguments	Description / Purpose
Contactss JetBrains Mono	query (name/email) Inter Regular	연락처 검색. '홍길동에게 보내줘' 처리 시 수신자 식별. Inter Regular
get_organization JetBrains Mono	- Inter Regular	조직 정보 조회. 챗 사용자(SSO)와 Graph 사용자 매핑. Inter Regular
list_contact_folders JetBrains Mono	- Inter Regular	폴더 기반 연락처 그룹 조회. Inter Regular

Pass Items: `list\_people` (Privacy reasons), `create\_contact` (Personal scope excluded). Inter Regular

# 15. 미구현(Pass) 항목 및 제외 사유

Category	Tools (Code)	Reason (제외 사유)
High Risk / Admin	<code>delete_calendar</code> <code>wipe_data</code> JetBrains Mono	오작동 시 복구 불가. 데이터 손실 위험.
Personal Settings	<code>get_user_settings</code> <code>update_user_settings</code> JetBrains Mono	챗봇 프로필로 대체. 개인화 설정은 Graph 범위 제외.
Low Utility	<code>batch_request</code> <code>list_subscriptions</code> JetBrains Mono	백엔드/운영 전용 기능. Agent가 직접 호출할 필요 없음.

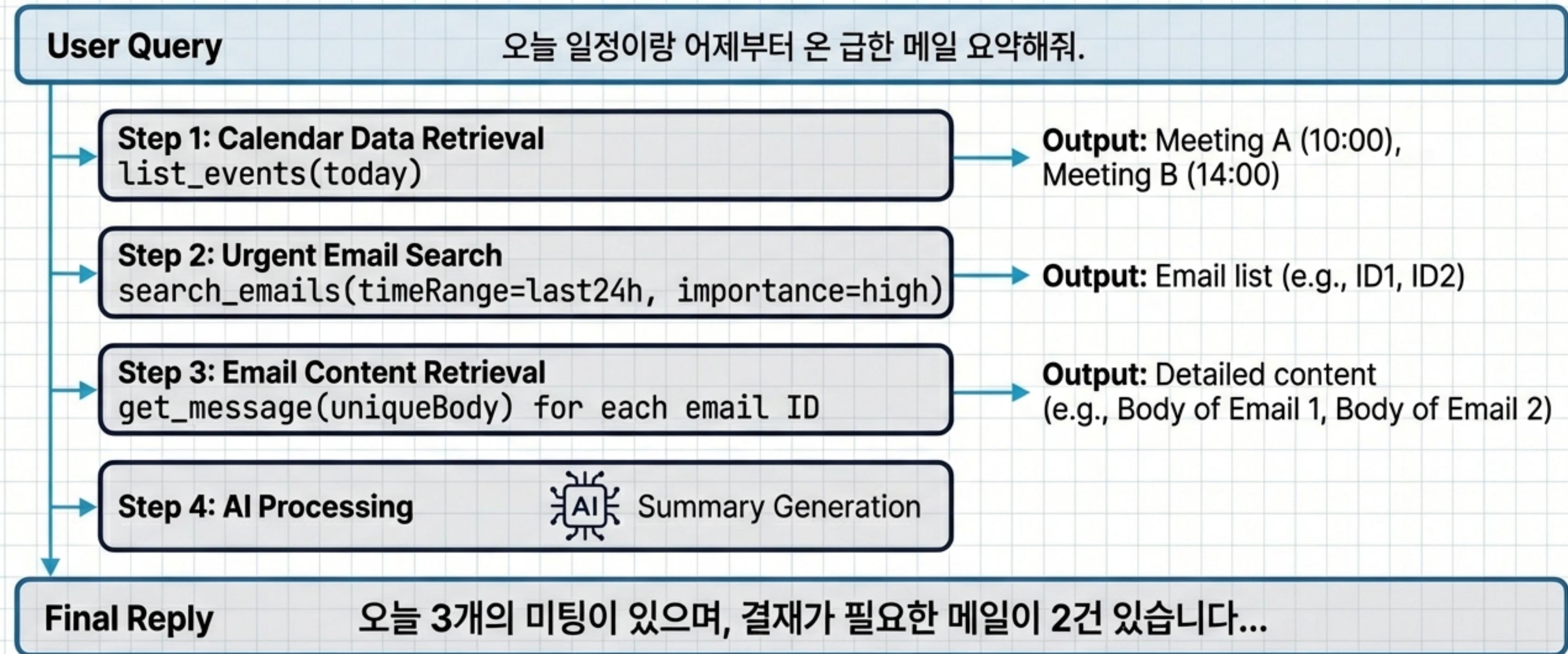
# 16. AI를 위한 문서화(Documentation) 전략

## Tool: search\_emails

```
{  
  "description": "사용자가 특정 메일(주제/발신자/기간)을 찾을 때 사용. 결과가 많으면 `top`으로 제한됨.",  
  "arguments": {  
    "query": {  
      "type": "string",  
      "description": "OData 포맷. 예: 'from:finance@corp.com'"  
    },  
    "timeRange": {  
      "type": "string",  
      "description": "ISO8601 포맷 권장."  
    }  
},  
  "error_codes": ["NOT_FOUND", "THROTTLED"]  
}
```

비즈니스 로직 대신  
상세한 '설명'으로  
Agent 행동 유도.

## 17. 활용 시나리오 1: 모닝 브리핑 (Morning Briefing)

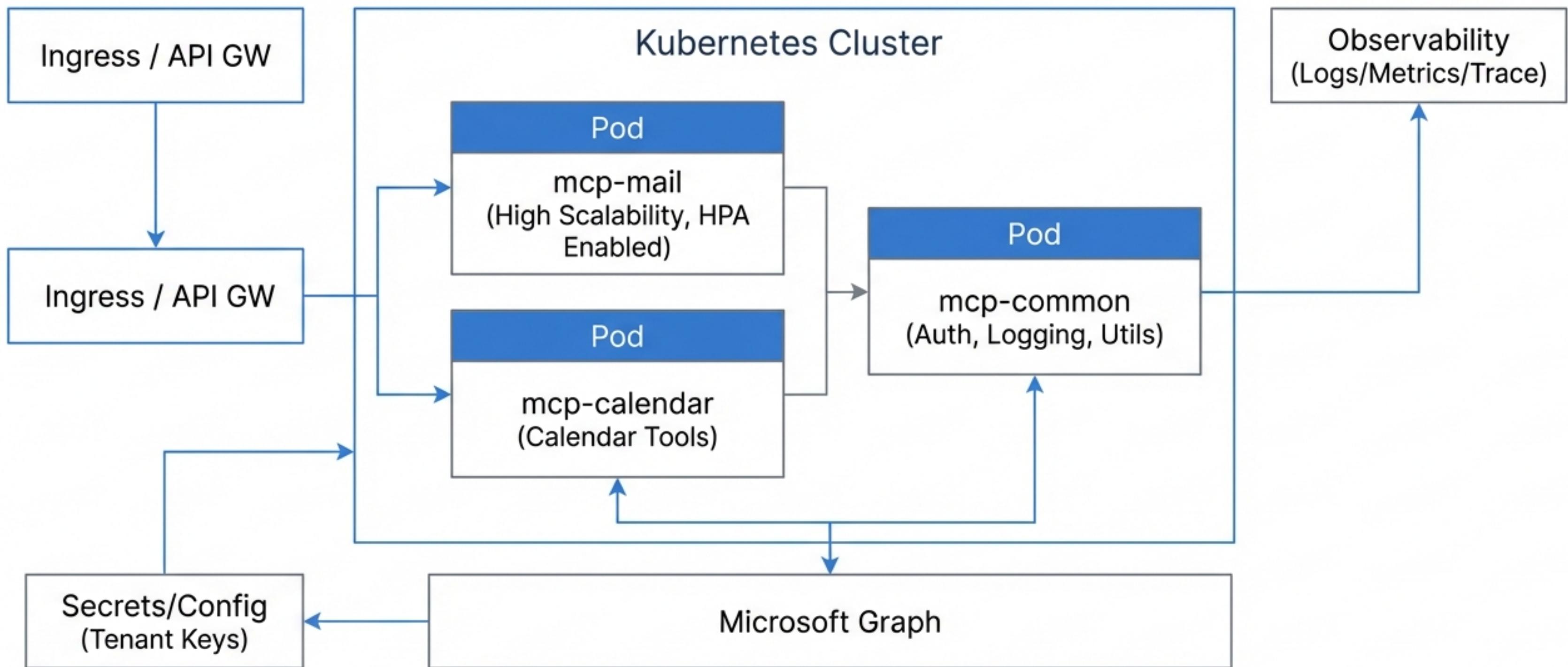


# 18. 활용 시나리오 2: 스마트 답장 (Smart Reply)

**User Query:** 이 메일 스레드 정리하고 긍정적으로 답장 초안 써줘.

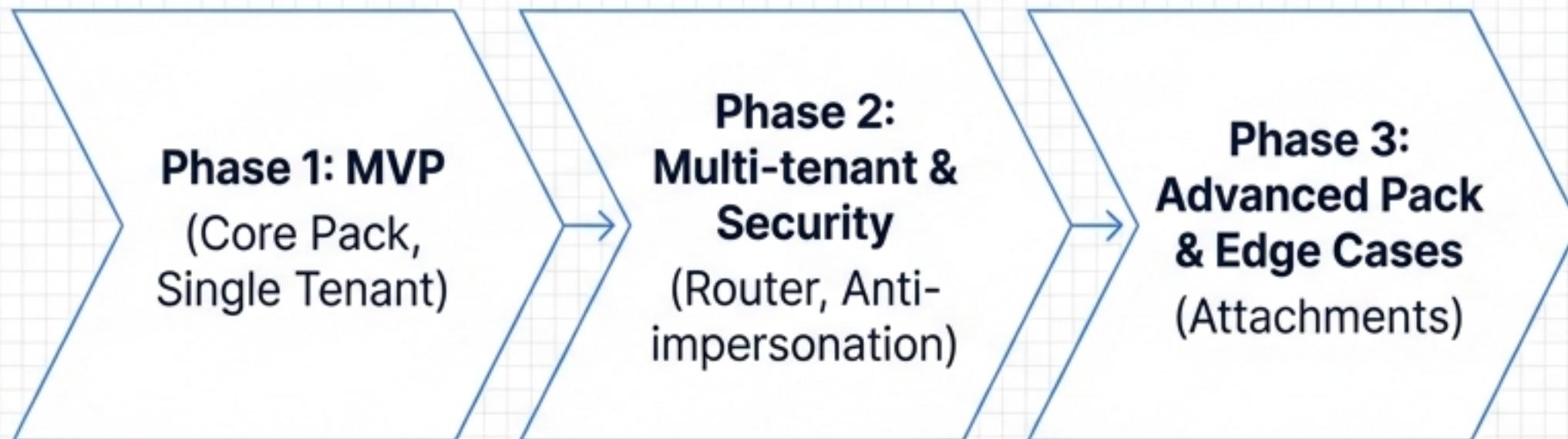


# 19. 배포 및 인프라 구조 (Implementation)



# 20. 구현 로드맵 및 운영 체크리스트

## Implementation Roadmap



## Operational Checklist

- Tenant Key Rotation Policy
- Graph API Throttling Monitor
- Audit Log Access Control
- Latency Dashboard Setup