

# 공무원 대상 생성형 AI & ChatGPT 교육

- 실무 활용 핸드아웃 -

강사: 에브리에이아이코리아 주식회사 육대근, 김주영 / 문의 : [contact@evry.ai](mailto:contact@evry.ai)

교육 목표: 공공업무에서 생성형 AI를 안전하고 효과적으로 활용하는 실무 역량 습득

교육 시간: 3교시 (총 180분) | 대상: 횡성군청

본 자료는 교육 목적으로 작성되었습니다.

© 2025 DECK - 육대근 / 김주영 | 횡성군청 생성형 AI 교육

# 1교시: 생성형 AI & ChatGPT 기초 이론

## A. 생성형 AI란 무엇인가?

### 판별 모델 vs 생성 모델

- 판별 모델: 입력 데이터를 분류하거나 예측 (예: 이미지에서 개/고양이 구분)
- 생성 모델: 학습한 데이터 분포를 바탕으로 새로운 데이터 생성
- 판별 모델 → 정답 맞추기 / 생성 모델 → 새로운 산출물 만들기

### 파운데이션 모델과 지시 튜닝

- 파운데이션 모델: 방대한 데이터로 자그지도 학습한 거대 모델
- 지시 튜닝: 사용자 지시를 따르도록 추가 훈련
- RLHF: 인간 피드백 강화학습으로 인간 가치에 맞게 조율
- 결과: 안전하고 친근한 답변 생성, 다양성 감소하는 트레이드 오프

### 토큰, 임베딩, 문맥길이

- 토큰: 텍스트 처리 단위 (한 글자~부분 단어)
- 임베딩: 토큰의 고차원 벡터 표현, 의미적 유사성 반영
- 문맥 길이: 한 번에 처리 가능한 토큰 수 제한 (GPT-4: 8K~32K)
- 학습된 지식 ≠ 실시간 검색 (훈련 시점까지 데이터만 반영)

⚠ 주의사항 LLM은 최신 정보를 자동으로 검색하지 않습니다. 2023년 이후 정보나 업데이트된 정책은 모델이 알지 못할 수 있습니다.

## B. LLM 동작 원리

### 다음 토큰 예측 방식

- 문맥에 따라 다음에 올 가장 그럴듯한 단어를 예측
- 확률분포에서 토큰을 샘플링하여 문장을 이어감
- 스마트폰 자동완성의 극도로 발전한 형태
- 환각(Hallucination): 사실과 다른 내용도 그럴듯하게 생성

⚠ 실제 사례 2023년 미국 변호사가 ChatGPT의 가짜 판례 6건을 법정에 제출하여 문제가 된 사건 발생

### 주요 생성 파라미터

파라미터	역할	설정 가이드
Temperature	창의적 변동성 조절	보고서: 낮게(0.2) / 브레인스토밍: 높게(0.8)
Top-p	토큰 선택 후보 범위	일관성 원할 때: 낮게 / 다양성 원할 때: 높게
Max Tokens	최대 생성 토큰 수	출력 분량 제한

### 시스템/사용자/어시스턴트 역할

- 시스템 메시지: AI의 기본 성격, 말투, 제한사항 규정
- 사용자 메시지: 사람이 묻거나 요구하는 내용
- 어시스턴트 메시지: AI 응답 내용

## C. 공공업무 활용 시 보안·윤리·법적 고려사항

### 민감정보 및 프라이버시 보호

- LLM에 데이터 입력 = 제3자에게 정보 위탁과 유사
- 입력된 데이터는 모델 개선에 사용될 수 있음
- 원칙: 중요 정보는 애초에 외부 AI에 입력하지 않음
- 가명처리, 총계처리 후 최소한으로 제공

⚠ 삼성전자 사례 (2023) 개발자가 ChatGPT에 소스코드를 문의하다 사내 기밀코드 유출 → 업무용 ChatGPT 사용 일시 금지

### 출처 명시와 최신성 검증

- ChatGPT는 지식의 출처를 밝히지 않음
- "Trust, but verify" - 일단 활용하되 반드시 교차 확인
- 출처 찾아 제시하도록 유도하는 프롬프트 활용
- 최신 법령, 통계는 직접 최신 자료 확인 필요

### 중립성과 편향성

- 모델 학습 과정에서 사회적 편향 포함 가능성
- 특정 집단 부정적 일반화나 차별적 표현 주의
- 정책 중립적이고 균형 잡힌 시각 유지
- 과장·홍보성 표현 지양

## D. 한계와 품질관리

### 환각(Hallucination) 대응

- 환각: 그럴듯하지만 사실무근인 정보 생성
- 원인: 지식 암기가 아닌 확률적 단어 연쇄 생성
- 완전 제거 불가능, 사용자 차원에서 줄이는 방법 필요

### 검증 루틴 (3단계 점검)

1. 사실과 수치 대조: 통계, 날짜, 고유명사 원문 데이터와 대조
2. 규정·문체 검사: 기관 형식과 어투 부합성 확인
3. 이해관계·균형성 점검: 편향되거나 일방적 표현 여부

💡 자기 검증 기법 모델에게 "위 답변에서 사실과 다른 부분이나 논리적 비약을 지적하라"는 추가 프롬프트로 2차 검토 가능

## E. 프롬프트 기본기

### Role · Context · Input · Output · Constraint - Tone 구조

요소	설명	예시
ROLE	모델에게 특정 역할 부여	"당신은 ○○부서 보고서 담당자입니다"
CONTEXT	작업 목적, 대상 독자, 양식	"도지사 주재 회의 보고용 1페이지 요약본"
INPUT	활용할 실제 데이터, 문서	CSV 데이터, 정책 요약, 회의 메모
OUTPUT	원하는 출력 구성과 형식	"1) 요약 2) 표 3) 분석 4) 과제"
CONSTRAINT	반드시 지켜야 할 조건	"민감정보 마스킹, 2쪽 이내"
TONE	문체와 어조	"공문서답게 간결·객관적으로"

### 핵심 포인트 정리

- ✓ LLM은 지식 창고가 아니라 확률적 문장 생성기
- ✓ 마스킹 → 요약 → 검증 프로세스 준수
- ✓ 프롬프트의 힘: 역할·맥락·제약이 절반
- ✓ 숫자와 날짜는 반드시 재검산

## 2교시: 실습1 : 데이터 → 보고서 자동화

### Lab 1-1: CSV 데이터로 보고서 뼈대 생성

[역할] 당신은 {{기관명}} {{부서명}}의 정례보고 작성자입니다.

[맥락] 아래 데이터와 문서규정을 반영해 "월간 민원·집행 현황 보고" 초안을 작성합니다.

[입력]

- 민원 데이터(CSV): <<민원\_현황\_샘플.csv 내용>>
- 집행 데이터(CSV): <<사업\_집행\_현황.csv 내용>>
- 기관 문서규정 요약: <<기관\_문서규정\_요약.txt 내용>>
- 표준 목차: <<템플릿\_표준목차.md 내용>>

[출력]

- 1) 1페이지 요약: 핵심지표 3, 위험/이슈 3, 다음달 과제 3
- 2) 표 3개: (a) 민원유형 Top5 (b) 처리기한 임박 건 (c) 집행률 상/하위 3개
- 3) 분석: 추세·원인·시사점 각 3문장
- 4) 다음달 과제/KPI 표: 과제·담당·기한·지표

[제약]

- 표 내 수치는 CSV를 재계산해 제시(추정 시 '추정' 명시)
- 민감정보/개인식별정보는 포함 금지
- 기관 문체·표기 규칙 준수, 총 2쪽 이내

[톤] 공문체, 간결·객관.

## 구조화된 출력 (JSON 형식)

같은 내용을 JSON으로도 출력하세요.

형식:

```
{
  "summary": {"key_points":[...], "issues":[...], "next_actions":[...]},
  "tables": {
    "top5_issue_types":[{"민원유형":"","건수":0,"비율%":0}],
    "due_soon":[{"민원ID":"","처리기한":"","상태":""}],
    "spend_variance":[{"세부사업":"","집행률%":0,"상/하위":"상위|하위"}]
  },
  "analysis":{"trend":"","causes":[],"implications":[""]},
  "kpi_next_month":[{"과제":"","담당":"","마감일":"","KPI":""}]
}
```

제약은 이전과 동일.



## Lab 1-2: AI 보고서 품질 보정

### 1단계 - AI 리뷰 프롬프트

다음 보고서 초안의 품질을 아래 기준으로 평가하고, 수정 제안을 표로 만드세요.

[기준]

- 수치/계산 오류 여부
- 근거 없는 단정/추정 라벨링 여부
- 기관 문체/표기 준수 여부
- 표·목차 구조 일관성
- KPI 측정가능성/명확성

출력: "항목/문제/근거/수정제안" 4열 표 + 총평(불릿 5)

자료: <<방금 생성된 보고서 초안 붙여넣기>>

### 2단계 - 개정 프롬프트

위 점검표의 수정제안을 반영해 보고서를 개정하세요.

- 변경사항 요약(불릿 5) 포함
- 표·숫자 재검산
- 문체/표기 규정 확실히 적용

입력: (원본 초안 + 점검표)

출력: 개정본(문서) + "변경사항 요약"

## Lab 1-3: 민감정보 자동 마스킹

다음 텍스트에서 개인식별 가능 정보(성명, 전화, 이메일, 주민번호, 주소, 차량/계좌 등)를 마스킹하세요.

[규칙]

- 성명 → [성명]
- 휴대전화/유선 → [연락처]
- 이메일 → [이메일]
- 주소 → [주소-동 단위]
- 차량/계좌/식별코드 → [식별정보]

출력:

- 1) 마스킹 규칙표(예시 2개씩)
- 2) 마스킹 적용본(원문 구조 유지)

자료: <<민원 원문/메모 등 붙여넣기>>

제약: 의미 변형 없이 최소 마스킹, 수치/일자 보존

## 3교시: 실습2 : 민원 응대, 회의록 정리, 보도자료 초안

### Lab 2-1: 반복 민원 응대 및 FAQ 생성

[역할] 당신은 {{기관명}} 민원 응대 담당자입니다.

[맥락] 기관 정책 요약과 실제 민원 원문을 반영해, 사실확인→정책 안내→대안 제시 순서로 답변 초안을 작성하세요.

[입력]

- 정책 요약: <<정책 요약 붙여넣기>>
- 민원 원문: <<민원 텍스트 붙여넣기>>

[출력]

- 1) 답변 초안(5문장 이내, 친절하고 중립적)
- 2) 추가 확인이 필요한 정보 리스트(불릿 3~5)
- 3) 같은 유형에 재사용 가능한 FAQ 3개 (Q/A 형식)
- 4) 안내 문구(개인정보 최소수집·처리 절차)

[제약] 법적 판단 단정 금지, 과장 표현 금지, 내부 확인 필요 시 '확인 후 회신' 명시, 날짜·절차는 근거와 함께.

[톤] 공손·명료, 민원인 관점에서 이해하기 쉽게.

### 정책 변경 시 업데이트

위 응답 초안을 유지하되, 다음 변경사항을 반영해 업데이트하세요:

- 변경 포인트: <<개정 조문/시행일/적용범위 붙여넣기>>

출력: (a) 개정본 답변 (b) 바뀐 점 요약(불릿 3) (c) FAQ 업데이트 1~2개

## Lab 2-2: 회의록 → 업무지시/액션 아이템 도출

[역할] 주간회의 서기입니다.

[입력] 회의 원문: <<회의 메모 붙여넣기>>

[출력]

- 1) 액션아이템 표(CSV로도 제공): "업무, 책임자, 마감일(YYYY-MM-DD), 성과지표(KPI), 의존관계, 리스크, 비고"
  - 2) 결정사항과 보류사항(각 3줄)
  - 3) 후속일정 제안(주/월간 3개안) — 제목/목적/예상 소요시간 포함
- [제약] 모호 표현→측정가능 표현으로 치환, 중복 제거, 기한 없는 업무 금지.

[톤] 간결·실무형.

### 일정화·호출형 추가 프롬프트

위 액션아이템 표에서 "마감일이 일주일 내"인 항목만 필터링하여,  
캘린더 등록에 적합한 간단 문장(제목 | 일자 | 담당 | 장소/비고) 리스트로  
변환하세요.

## Lab 2-3: 정책 보도자료 및 브리핑 초안 생성

[역할] {{기관명}} 보도자료 작성자입니다.

[맥락] 아래 정책자료 요약을 기반으로 도민 체감 핵심 메시지 3가지를 중심으로  
보도자료 초안을 만드세요.

[입력] 정책자료 요약: <<정책 요약 붙여넣기>>

[출력]

- 제목 3안(각 25자 내외)
- 리드 2문단(왜 지금? 누가? 무엇을? 어떻게? 효과?)
- 본문: 배경/주요내용/기대효과/도민 혜택/문의처
- Q&A 5개(오해 가능 지점 중심)
- 시각자료 제안 3개(그래픽/도표/사진 아이디어)

[제약] 수치·일정·절차는 근거와 함께, 과장 금지, 내부 승인 전 배포 금지 문구 포함.

[톤] 중립·명료·사실 중심.

### 브리핑 카드 요약

위 보도자료를 1페이지 브리핑 카드로 축약하세요.

구성: "핵심 메시지 3, 핵심 수치 3, 현장 Q&A 3, 다음 행동 3"

형식: 불릿 리스트 + 2행 요약표('무엇/언제/어디/담당/문의')

# 부록: 공통 검수 체크리스트 & 참고자료

## 공통 검수 체크리스트

### 1. 정확성

- • 수치, 날짜, 대상, 범위가 원 자료와 일치하는가?
- • 잘못된 사실 인용이나 허위 정보는 없는가?
- • 관련 법조항이나 통계 원문을 대조했는가?

### 2. 정책 적합성

- • 기관의 문체·표기 규정에 부합하는가?
- • 비밀 유지가 필요한 내용이 노출되지 않았는가?
- • 경어/존칭 사용, 전문용어 표기가 적절한가?

### 3. 중립성

- • 특정 지역, 계층, 성별 등을 편향되게 표현하지 않았는가?
- • 균형 잡힌 시각을 유지하고 있는가?
- • 과장되거나 홍보성 표현이 포함되지 않았는가?

### 4. 프라이버시

- • 개인 이름, 연락처, 주민번호 등이 완벽히 마스킹되었는가?
- • 민원 사례나 회의 내용의 민감한 발언이 비식별화되었는가?
- • 추가 마스킹이나 가명처리가 필요한 부분은 없는가?

### 5. 재사용성


- • 템플릿화 또는 FAQ화하여 향후 반복 활용이 가능한가?
- • 생성된 산출물을 체계적으로 축적·관리할 방안이 있는가?
- • 지식베이스 구축에 활용할 수 있는 형태인가?


## 주요 파라미터 설정 가이드

업무 유형	Temperature	Max Tokens	권장 설정
정례보고서	0.1-0.3	1000-1500	정확성 우선, 일관성 중시
민원 응대	0.2-0.4	500-800	친근함과 정확성 균형
보도자료	0.3-0.5	1200-2000	다양한 표현, 명료한 전달
아이디어 회의	0.6-0.8	800-1200	창의성과 다양성 중시

## 참고 사이트 & 도구

- OpenAI ChatGPT: <https://chat.openai.com>
- 프롬프트 엔지니어링 가이드: <https://www.promptingguide.ai>
- AI 활용 보안 가이드라인: 행정안전부 AI 도입 가이드라인 참조
- 개인정보 마스킹 도구: 각 기관 보안담당부서 문의

 **최종 확인사항** • 생성된 모든 산출물은 담당자가 검토 후 사용 • 대외 발표자료는 반드시 승인 절차 거쳐야 함 • AI 활용 사실을 필요시 명시 (투명성 원칙) • 지속적인 모니터링과 피드백으로 품질 개선

 **효과적 활용 팁** • 처음부터 완벽한 결과를 기대하지 말고 반복 개선 • 프롬프트는 구체적이고 명확하게 작성 • 여러 번 시도해보며 최적 프롬프트 찾기 • 동료들과 좋은 프롬프트 공유하여 조직 역량 향상

- 공무원 대상 생성형 AI & ChatGPT 교육 ·

문의 : [contact@evry.ai](mailto:contact@evry.ai)