

ChatGPT 시대 정보보호 강화 방안의 고찰 및 제언



MPIS 2023

2023 의료기관 개인정보보호&정보보안 컨퍼런스

Why To Do ?

How To Do ?

What To Do ?

- 3

Why To Do? 왜 해야 할까? 목표정의

- **목표 : 효과적/효율적 정보보호**
- **As-Is (현재)**
 - 관리적/물리적/기술적 보안
 - 우리 기관의 정보보호 인력은? 투자는?
- **To-Be (미래) – 가능할까? 해결될까?**
 - 정보보호 인력 200명? 장비 2000억?
 - 전직원 인식 제고, 보호 인력 효율 극대화

Why To Do? 왜 해야 할까? 목표정의

개인정보 보호 기본계획의 비전 및 전략



개인정보보호위원회
22년 기본계획

비전

안전한 개인정보, 신뢰하는 데이터 시대

추진 전략

- (더 안전해지는) 확실한 개인정보 보호
- (더 편리해지는) 데이터 가치를 높이는 안전한 활용
- (더 튼튼해지는) 컨트롤타워로서 보호와 활용의 조화

추진 과제

확실한 개인정보 보호

- ① 국민의 정보주권을 강화하겠습니다.
- ② 기업의 자율보호 생태계를 조성하겠습니다.
- ③ 공공의 개인정보 보호체계를 고도화하겠습니다.

데이터 가치를 높이는 안전한 활용

- ④ 개인정보를 가장 안전하게 잘 활용하겠습니다.
- ⑤ 디지털 전환 시대에 사각지대를 없애겠습니다.
- ⑥ 연구개발 강화로 더욱 안전한 보호 환경을 만들겠습니다.

컨트롤타워로서 보호와 활용의 조화

- ⑦ 침해사고에 대하여 엄정하고 신속하게 대응하겠습니다.
- ⑧ 국가 개인정보 보호 거버넌스를 구축하겠습니다.
- ⑨ 글로벌 개인정보 협력을 강화하겠습니다.
- ⑩ 일원화된 감독기구로서 리더십을 확립하겠습니다.

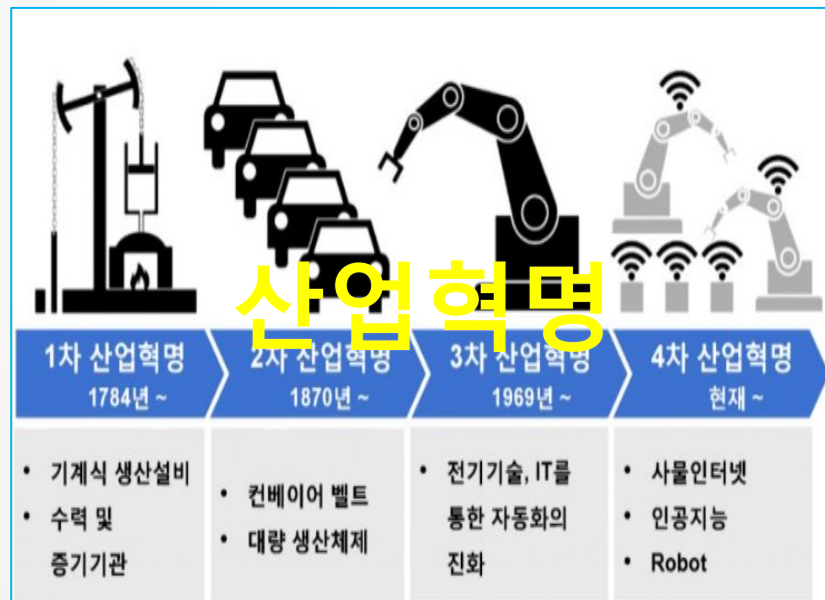
원칙

개인정보 보호 중심 설계(Privacy by Design)



1. ChatGPT

How To Do ?



Openai.com

Generative Pre-trained Transformer 생성형 대화 인공지능

ChatGPT

We've trained a model called ChatGPT which interacts in a conversational way. The dialogue format makes it possible for ChatGPT to answer follow-up questions, admit its mistakes, challenge incorrect premises, and reject inappropriate requests.

우리는 대화 방식으로 상호 작용하는 ChatGPT라는 모델을 훈련했습니다. 대화 형식을 통해 ChatGPT는 후속 질문에 답하고, 실수를 인정하고, 잘못된 전제에 이의를 제기하고, 부적절한 요청을 거부할 수 있습니다.

ChatGPT는 OpenAI가 개발한 대규모 언어 모델입니다. ChatGPT는 트랜스포머 아키텍처를 기반으로 하며 인터넷의 방대한 텍스트 데이터 세트로 능동적인 학습으로 훈련된 모델입니다. ChatGPT는 주어진 프롬프트나 질문에 응답하며 인간의 생각과 유사한 텍스트를 생성하는 데 사용됩니다¹. ChatGPT는 대화 형태로 상호작용을 하며 놀라운 정도로 인간과 대화하는 것과 같은 반응을 제공하는 능력을 가지고 있습니다²³.

¹: ChatGPT 초보 사용자를 위한 사용메뉴얼 : 활용 사례와 관련 자료 ²: 챗gpt란 무엇인가? 원리부터 활용법까지 ³: ChatGPT(챗GPT)란 무엇인가? - 원리, 예시, 활용법 - TBWA 데이터랩

자세한 정보: [1. bing.com](https://www.bing.com) [2. openads.co.kr](https://openads.co.kr) [3. seo.tbwakorea.com](https://seo.tbwakorea.com) [+2 더 보기](#)

1 / 20

MS bing.com



ChatGPT의 활용 사례는 무엇인가요?

ChatGPT의 장점은 무엇인가요?

ChatGPT와 GPT-3의 차이점은 무엇인가요?

• 개인정보 사용 NO!!! / 의료정보 사용 NO!!!



ChatGPT는 인공지능 기반 대화 모델로서, 사용자와 자연스러운 대화를 나눌 수 있습니다. 그러나 다음과 같은 주의사항이 있습니다.

1. **개인정보 유출 가능성**: ChatGPT는 인공지능 모델로서, 사용자가 제공한 정보를 학습하고 저장할 수 있습니다. 그러므로 민감한 개인정보를 대화내용으로 입력하지 않는 것이 좋습니다.
2. 업무 목적으로 사용하지 말 것: ChatGPT는 일반적인 상황에서 사용하는 대화모델이므로, 업무적인 목적으로 사용할 경우 **잘못된 정보나 대화내용을 반환**할 수 있습니다. **이 경우 전문적인 업무 분야에 맞는 대화 모델을 사용하는 것이 바람직합니다.**
3. **전문적인 상담 대응으로 사용하지 말 것**: ChatGPT는 인공지능 모델로서 일반적인 대화를 지원하며, 전문적인 상담 대응으로 사용하는 것은 적절하지 않습니다. **전문적인 상담이 필요한 경우 전문가나 적절한 기관에 상담을 받는 것이 좋습니다.**
4. 자연스러운 대화를 위해 올바른 문장을 입력할 것: ChatGPT는 사용자가 입력한 문장을 학습하여 대답을 반환합니다. 그러므로 올바른 문장, 철자, 문법 등을 사용하여 자연스러운 대화를 이어나가는 것이 좋습니다.
5. 기술적 제한: ChatGPT는 인공지능 기술을 사용하여 작동합니다. 하지만 모든 상황에서 완벽한 대화를 보장할 수는 없으며, 기술적인 문제로 인해 대화가 불가능한 상황이 발생할 수도 있습니다.

- 지식 습득 방식의 변화
 - (As-IS) 검색(구글, 네이버 등) > 문해력
 - (To-Be) 챗GPT(프롬프트) > 진위검증력
- 사람과 IT(정보기술)의 간극 해소
 - (As-IS) ALL > SOME(IT인력) > IT(기술)
 - (To-Be) ALL > IT(기술)
 - ✓ Zero 코딩 !!! No 코딩 !!!
 - 업무자동화/ 업무효율화 극대화

• 지식 습득 방식의 변화. 검색 방식의 변화

Google

부천성모병원 예약방법

전체 뉴스 이미지 동영상 지도 더보기

검색결과 약 500,000개 (0.35초)

진료예약

1. 대표전화 1577-0675.
2. 의과대학 보건의료경영대학원 임상치과대학원 가톨릭인체유래물중앙은행

cmcbucheon.or.kr
https://m.cmcbucheon.or.kr/page/appointment

진료예약 - 가톨릭대학교 부천성모병원

추천 스니펫 정보 사용자 의견

cmcbucheon.or.kr
https://www.cmcbucheon.or.kr

가톨릭대학교 부천성모병원

가톨릭대학교 부천성모병원에서는 환자들이 진료과, 클리닉, 전문센터의 의료진 정보를 통해 진료 예약을 할 수 있으며 예약, 검사, 처방 등의 내역을 볼 수 있는 진료 ...

진료예약 · 진료과 · 의료진 · 주요전화

cmcbucheon.or.kr
https://www.cmcbucheon.or.kr/hospitalguide.total_c...

종합건강검진안내 - 가톨릭대학교 부천성모병원

예약상담안내, 방법, 방문 또는 전화·팩스 및 인터넷 예약 (전화번호 : 032-340-2160, 1 / FAX : 032-340-2163). 시간, 평일 : 08:00 ~ 17:00.

cmcbucheon.or.kr
https://www.cmcbucheon.or.kr/page/department

종합검진센터 - 가톨릭대학교 부천성모병원

가톨릭대학교 부천성모병원에서는 환자들이 진료과, 클리닉, 전문센터의 의료진 정보를 통해 진료 예약을 할 수 있으며 예약, 검사, 처방 등의 내역을 볼 수 있는 진료 ...



Microsoft Bing

검색 채팅

부천성모병원 예약방법을 자세히 알려줘

✓ "부천성모병원 예약방법" 검색 중
✓ 답변을 생성하는 중...

네, 부천성모병원 예약방법을 알려드리겠습니다. 가톨릭대학교 부천성모병원에서는 환자들이 진료과, 클리닉, 전문센터의 의료진 정보를 통해 진료 예약을 할 수 있으며 예약, 검사, 처방 등의 내역을 볼 수 있는 진료차트 서비스를 제공하고 있습니다 1 2 3.

예약방법은 다음과 같습니다.

- 첫 방문 전화예약: 홈페이지에서 이름과 전화번호를 입력하면 전문 상담사가 순차적으로 연락드립니다. 운영시간은 화요일부터 금요일 오전 8시부터 오후 5시까지입니다 1.
- 인터넷 진료예약: 홈페이지에서 회원예약 또는 비회원예약을 선택하고 원하는 진료과와 의료진을 검색하여 예약할 수 있습니다 1.
- 전화예약: 종합건강검진센터 TEL. 032-340-2160으로 전화하여 예약할 수 있습니다 4.

부천성모병원은 소사역 3번 출구나 부천종합운동장역에서 셔틀버스를 이용하거나 시내버스 52, 56, 56-1, 3, 5, 12, 31-7, 71, 60, 95번을 타고 가실 수 있습니다 2. 자세한 찾아오시는 길은 홈페이지에서 확인하실 수 있습니다.

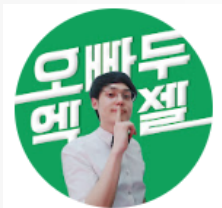
부천성모병원에서 건강한 진료를 받으시길 바랍니다. 😊

자세한 정보: 1. cmcbucheon.or.kr 2. cmcbucheon.or.kr +2 더 보기 1 / 20

업무 방식의 변화



yes24



YouTube KR

오빠두엑셀 | 엑셀 강의 대표채널

@Oppadu · 구독자 110만명

직장인을 위한 PPT 핵심 기능, 20분 족집개 특강

오빠두엑셀 | 엑셀 강의 대표채널

가입

조회수 1.4만회 4일 전 #PPT #파워포인트 #파워포인트강의



엑셀에서 B열에 진료과가 있고, D열에 총진료비가 있어. 진료과별 총진료비를 구하는 함수를 알려줘

- ✓ "엑셀에서 열별로 데이터 합치는 함수" 검색 중
- ✓ 답변을 생성하는 중...

네, 엑셀에서는 SUMIF 함수를 사용하여 진료과별 총진료비를 구할 수 있습니다. SUMIF 함수는 조건에 맞는 셀의 합계를 구하는 함수입니다.

아래와 같이 입력해보세요.

```
=SUMIF(B:B, "진료과", D:D)
```

위 식은 B열에서 "진료과"라는 값을 찾아 D열의 값을 합산합니다.

더 궁금한 점이 있으시면 언제든지 물어보세요!

자세한 정보: [1. bing.com](https://www.bing.com) [2. oppadu.com](https://www.oppadu.com) +3 더 보기

4 / 20

학원? 고수?



감사합니다.

SUMIF 함수가 무엇인지 알려주세요.

SUMIF 함수를 사용하여 다른 데이터도 계산할 수 있나요?

1. 창의성

: 빠르게 주어진 조건을 충족하며 만들어낸다 (문학, 시, 논문 등)

예> A~Z까지 모든 알파벳이 들어가는 최소한의 문장을 만들어줘

예> '부천성모' 4글자로 사행시를 만들어줘

2. 인식능력

: 풍선 100개가 줄로 묶여 있고,

이 풍선을 가지고 있는 아이 사진을 보여주고,

이 풍선의 줄을 자르면 어떻게 될까?

아이는 어떤 마음을 가질까 라고 질문하면?

: 풍선 100개가 날라갑니다 아이가 슬퍼하겠네요

라고 답을 합니다.

3. 언어능력(번역 능력)

: 전세계의 꽤 많은 언어가 잘 변환된다고 합니다.

체감은

MS bing(www.bing.com) 사이트에서

(일반사용자가 무료 이용 가능한 최신 버전 ChatGPT)

(그래서 ChatGPT를 시작할때는 '빙~~~신~~~' 으로)

(신을 닮고 싶은 빙? 쿨~~력~~ T.T)

한국어로 질문/명령

(이런걸 프롬프트 라고 합니다)

해도 잘 대답해 주는 이유입니다.

4. 추론 능력

: 추리 문장을 주고 질문하면 답을 찾을 수 있습니다.

주어진 단서 조건을 몇 개 주고

범인은 누구지? 라고 묻는다면

범인은... 바로 당신 이군요... (뭐 이런 느낌?)

ChatGPT 의 특징

Writing

01. Chatsonic
02. ChatABC
03. JasperAI
04. Quillbot

Coding

01. Copilot
02. Tabnine
03. MutanleAI
04. Safurai
05. 10web

Research

01. PaperPal
02. Perplexity
03. YouChat
04. Elicit

Twitter

01. Tweetmonk
02. TribeScaler
03. Postwise
04. Tweetify

Productivity

01. Synthesia
02. Otter
03. Bardeen
04. Copy AI

Content Creation

01. WriteSonic
02. Tome
03. CopySmith
04. TextBlaze

Images

01. StockImg
02. Midjourney
03. NightCafe
04. Photosonic

Videos

01. Steve AI
02. Pictory
03. DeepBrain
04. Lumen 5

AI Audio

01. Murf AI
02. Specify
03. Lovo AI
04. Media AI

Music

01. Boomy AI
02. Soundraw
03. Beatoven
04. Soundful

Presentations

01. Beautiful AI
02. Simplified
03. SlideGo
04. Sendsteps

Resume Builder

01. Kickresume
02. Rezi AI
03. Resume AI
04. Enhance CV

1. 암호해제 관제

- .[방안] 년 1회 의사포함 각 부서장에게 1년간 암호해제 내역을 메일로 보내줌으로 해당부서에서 암호해제를 부서장이 모니터링 후 이상유무를 문서로 받습니다.
- .[효과] 전체 교직원이 암호해제 위험성(최소한 내가 해제한 내용이 관제되고 있음을 인지) 인식 제고,
실질적으로 필요한 문서만 암호해제 하였는지 부서장이 관제 위임함

2. 관제(모니터링)

- .[방안1] SIEM에서 관측되는 로그 중 임계치 초과(5분 내 다수 암호해제, V3 바이러스 다수 관제) 시
C-talk 메신저 혹은 메일로 위험 경고 (이걸 챗GPT가 자동으로 시행)
- .[방안2] SIEM에 각 장비(방화벽, NAC, V3 등) 로그를 파이썬으로 결측치/이상치 제거 후
봐야 할 로그만 남겨 모니터링 효율화 (관제 레포팅을 담당자에게 메일로 발송)
- .[효과] 실제 관제를 실시함으로, 사용자에게 위험 경고, 담당자는 업무부하 경감하고 실질 모니터링

- 18

- AI가 인간을 대체할 것인가?

그렇지 않을 것이다.

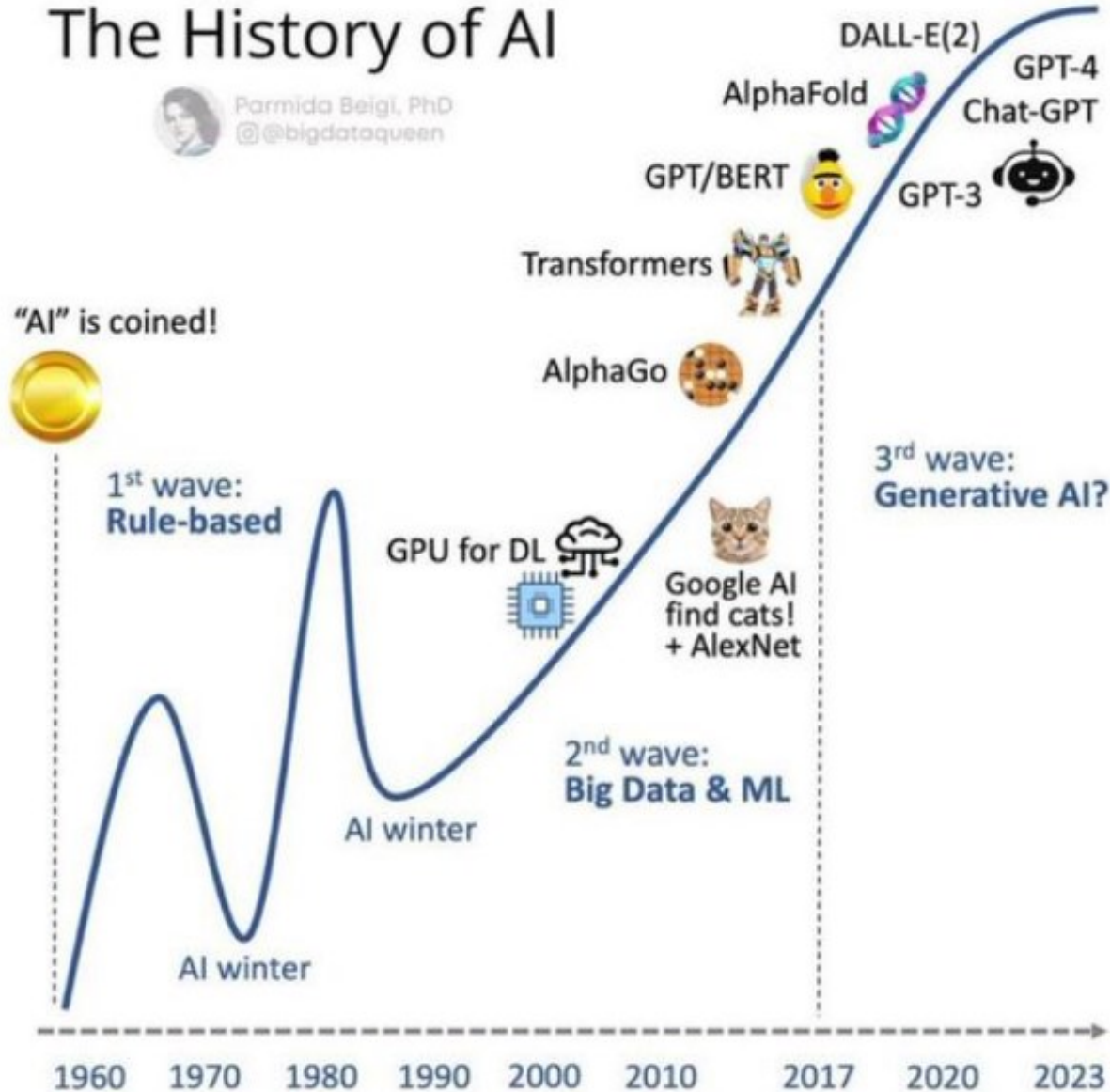
다만, AI를 잘 활용하는 인간이

잘 활용하지 않는 인간의 일까지

빼앗을 수 있다.....

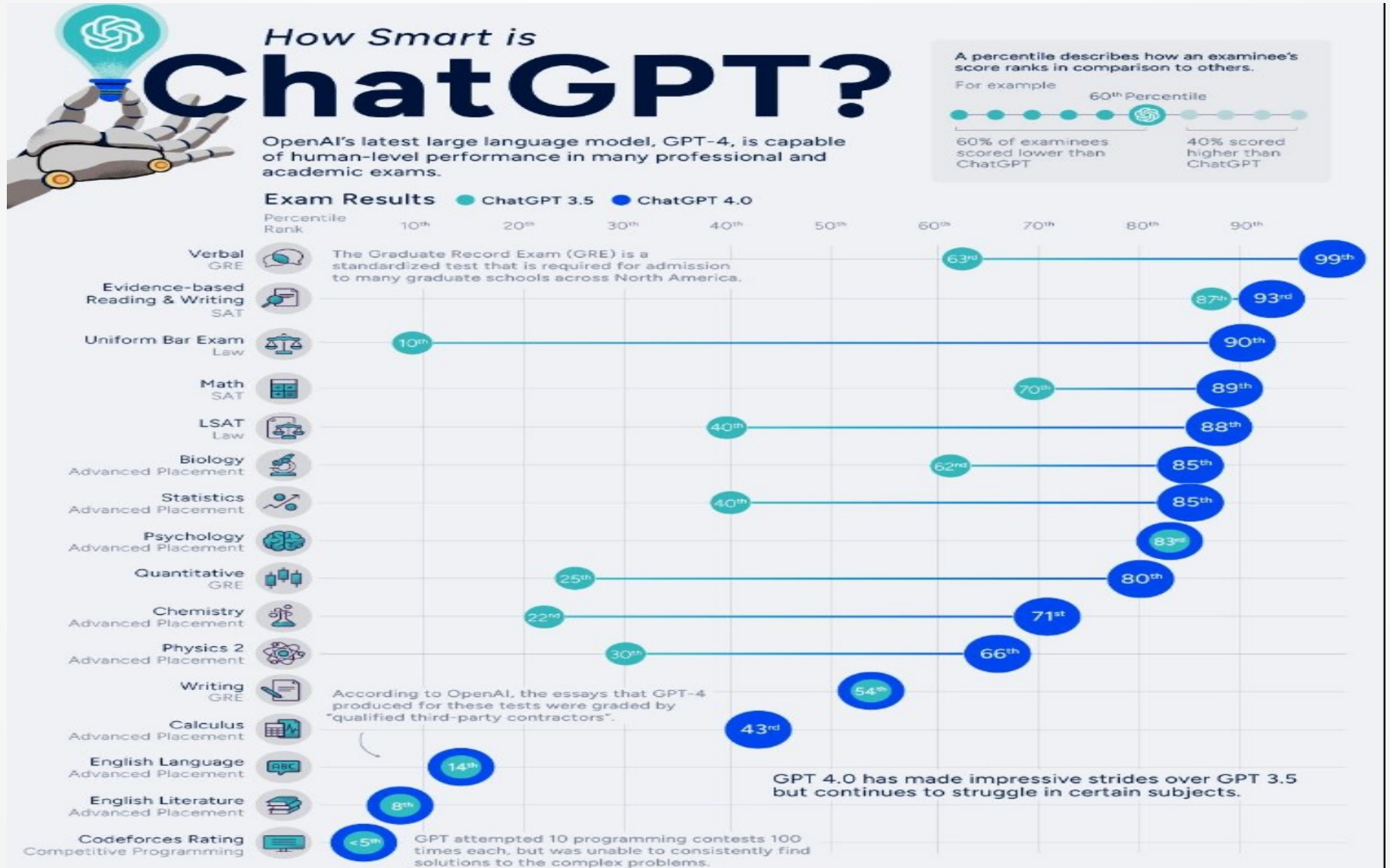
The History of AI

Parmida Beigi, PhD
@bigdataqueen



항목	인공지능 기술	원자력 기술
파괴력	낮음: 인공지능 자체는 즉각적인 파괴력을 가지고 있지 않지만, 무기나 시스템에 적용될 경우 위험할 수 있음	높음: 원자력 발전소 사고, 핵무기 등 원자력 기술의 오용이 큰 파괴력을 발휘할 수 있음
사회적 영향력	높음: 일자리 감소, 사회적 불평등, deepfake, 편견/편향 증폭, 개인정보 침해 등 다양한 사회적 문제를 야기할 수 있음	중간: 에너지 공급, 핵 안보, 전략적 이슈 등 원자력 기술이 사회 전반에 영향을 주는 분야가 있으나, 범위가 제한적임
파급력	중간~높음: 인공지능의 영향은 다양한 분야에 걸쳐 점진적으로 나타날 수 있으며, 시간이 지날수록 더 광범위해질 수 있음	중간: 원자력 발전소를 통한 전력 공급, 의료 및 과학 연구 등에서 활용되지만 파급력이 인공지능에 비해 제한적임
책임성	낮음~중간: 인공지능을 사용함에 따라 인간의 책임이 모호해지거나 회피되는 경우가 발생할 수 있음	중간~높음: 원자력 기술과 관련된 사고 발생 시, 발전소 운영자와 국가에 책임이 명확하게 귀속될 수 있음
시스템 오작동 위험	중간~높음: 인공지능 알고리즘의 오류, 데이터 조작, 해킹 등으로 인한 시스템 오작동 위험이 존재함	중간: 원자력 기술의 안전 시스템은 엄격한 표준과 규제를 따르지만, 설계 결함 인적 실수, 자연재해 등으로 인한 시스템 오작동 위험이 존재함
미확인 위험성 수준	중간~높음: 인공지능의 빠른 발전으로 인해 아직 예측하지 못한 새로운 위험 요소들이 발생할 수 있음	낮음~중간: 원자력 기술의 위험 요소들은 대부분 잘 알려져 있으나, 핵 사고나 방사능 누출 등의 위험 요소가 존재함
위험 요소	다양함: 개인정보 침해, 무기화, 불평등 증대, 일자리 손실 등 다양한 위험 요소가 존재함	제한적: 방사능 누출, 핵폐기물 처리, 원자재 고갈 등 주요 위험 요소가 명확함
자동화 수준	높음: 인공지능 기술은 많은 작업들을 자동화하며, 자율주행, 제조, 서비스 등 다양한 분야에 활용되고 있음	중간: 원자력 기술의 일부 작업들은 자동화되어 있지만, 전반적으로 인간의 감독 및 관리가 필요한 상황 많음
표준화 수준	낮음: 인공지능 분야는 계속 발전 중이며, 기술 및 규제 표준이 완전히 정립되지 않았음	높음: 원자력 기술은 국제 기구와 국가 간 협약, 규제 및 안전 표준이 잘 정립되어 있음
규제 정도	낮음~중간: 인공지능 기술의 발전 속도를 따라잡지 못하는 법률과 규제가 존재함. 국제적인 협력과 표준화가 필요함	높음: 원자력 기술은 국제 기구와 국가 간 협약, 규제 및 안전 표준이 잘 정립되어 있음
활용성	높음: 인공지능은 다양한 분야에서 활용 가능하며, 효율적인 서비스, 의료 진단, 연구 개발 등에서 인류의 삶의 질 향상에 기여할 수 있음	중간: 원자력 기술은 원자력 발전을 통해 지속 가능한 에너지를 제공할 수 있고, 의료 및 과학 연구 등의 특정 분야에서 활용됨
사고 발생 빈도	비교적 낮음: 인공지능 사고는 대체로 개인정보 침해, 알고리즘 오류, 시스템 오작동 등의 형태로 발생함	비교적 낮음: 원자력 사고는 드물게 발생하나, 발생 시 큰 규모의 파괴와 영향을 가져옴 (예: 체르노빌, 후쿠시마 사고)
기술 개발 주체	다양함: 정부, 기업, 학계 등 다양한 주체들이 인공지능 기술 개발에 참여하고 있음	제한적: 주로 정부 및 대형 에너지 회사가 원자력 기술 개발에 참여하고 있음
통제 주체	다양함: 각국의 정부, 기업 및 시민 사회가 통제 주체로 작용할 수 있으나, 국제적인 협력과 통제 기구가 더욱 필요함	국가 및 국제 기구: 원자력 기술의 통제는 주로 정부 및 국제 기구에 의해 이루어짐
규제 형태	소프트 규제: 인공지능 기술에 대한 법률 및 규제가 아직 미흡하며, 윤리 가이드라인 등 소프트 규제가 주를 이룸	하드 규제: 원자력 기술에 대한 국제적인 협약, 규제 및 검증 체계가 강력하게 존재하며, 원자력 발전 및 핵 무기에 대한 엄격한 통제가 이루어짐
기술 발전 속도	빠름: 인공지능 기술은 빠르게 발전하고 있으며, 법률과 규제가 기술 발전 속도를 따라잡지 못하는 상황이 발생하고 있음	상대적으로 느림: 원자력 기술은 일정 수준의 발전 속도를 유지하고 있으나, 인공지능에 비해 상대적으로 느림

전종홍, 2023



감사합니다

