



금융감독원

보 도 자 료

금융은 **통통**하게 소비자는 **행복**하게

보도	2024.3.18.(월) 조간	배포	2024.3.15.(금)		
담당부서	디지털혁신국 디지털혁신총괄팀	책임자	국 장	곽범준	(02-3145-7160)
		담당자	팀 장	심은섭	(02-3145-7162)

금융권 AI 활용 활성화를 위한 세미나 개최

- 정부의 AI 정책방향을 금융권과 공유하고 금융권의 건전한 AI 활용 확산을 지원 -

I . 개 요

- 금융감독원은 '24.3.15.(금) 금융회사 AI 담당 임원 등 약 250명이 참석한 가운데 '금융권 AI 활용 활성화를 위한 세미나'를 개최하였음
- 이번 세미나는 금융권의 건전한 AI 활용 환경 조성을 위해 마련되었으며,
 - 정부(과기정통부)의 AI 정책 추진방향을 금융권에 소개하고 학계와 산업계, 금융권 전문가들과 함께 AI 활용 활성화 및 책임성 확보 방안을 논의하였음

금융권 AI 활용 활성화를 위한 세미나 개요

- ☑ 일 시 : '24.3.15.(금) 15:00~17:20
- ☑ 장 소 : 금융감독원 2층 대강당
- ☑ 인사말 : 금융감독원 김병철 전략감독 부원장보
- ☑ 주제발표 : ① AI 일상화 등 2024년도 AI 정책방향(과학기술정보통신부)
② 생성형 AI 기술 진화에 따른 산업변화 트렌드(LG AI연구원)
③ 안전한 AI 활용을 위한 고려사항(연세대학교 정보대학원)
- ☑ 패널토론 : (금감원) 곽범준 디지털혁신국장
(금융권) 조영서 KB 금융지주 부사장, 안성희 신한카드 상무,
김성수 교보생명 상무
(학계·산업계) 권태경 연세대 교수, 이화영 LG AI연구원 상무

II. 주요 내용

- 김병철 금융감독원 부원장보는 AI가 우리 일상에 빠르게 침투하고 있는 가운데 해외 주요국들의 AI 우위(AI Supremacy) 선점을 위한 국가간 경쟁도 더욱 심화되고 있다고 평가하면서,
 - 금융권의 AI 경쟁력 제고를 위해 금융데이터와 다양한 산업군이 보유한 양질의 데이터가 융합·활용될 수 있는 방안을 검토하겠다고 밝힘
 - 또한, 산·학·연 전문가와 소통을 강화하여 AI 혁신의 저해요인을 발굴·개선하고 AI 활용시 발생할 수 있는 정보유출 등 리스크 요인에 대한 감독방안도 균형감 있게 검토해 나가겠다고 밝힘

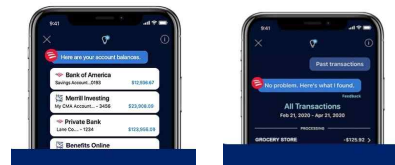
< 일상생활 속 AI 활용 · 악용사례 >

① (AI 비서) **뱅크오브아메리카(BoA)**의 AI 금융비서는 소비자의 금융·비금융 정보를 학습해 일 평균 150만명의 이용자에게 음성 계좌조회 및 자금이체 등 다양한 금융서비스를 제공

- **모건스탠리**는 내부 자산관리직원에게 AI 비서를 제공하여 시장조사, 투자전략 등 대고객 정보제공에 소요되는 시간을 단축하여 **업무효율성**을 제고

모든 계정의 잔액 보기

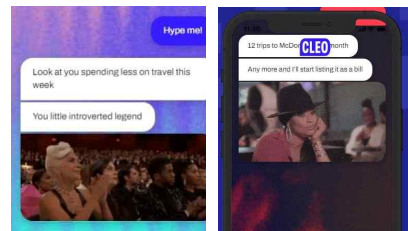
여러 계정에서 과거 거래 찾기



* 출처(bankofamerica.com)

② (AI 자산관리) 영국의 핀테크기업 **클레오(Cleo)**는 생성형 AI를 활용하여 **초개인화된 금융조언**을 제공하는 **자산관리 서비스**를 제공

- 챗봇을 통해 **Z세대의 언어와 밈(meme)**을 적극 활용하고 어려운 금융전문용어 대신 친구와 대화하는 편안한 방식으로 금융서비스를 제공



* 출처(web.meetcleo.com)

③ (AI 금융사기) 홍콩의 금융사 직원은 **딥페이크 기술**에 속아 거액(340억원)을 송금하는 금융사기 피해를 입었으며, 해외 각국에서는 **딥보이스**를 악용한 **피싱범죄**가 지속 발생

④ (비금융 AI 적용사례) LG AI연구원은 생성형 AI 기술을 활용하여 **알츠하이머와 암의 발병원인**을 분석하고 **치료제 효과까지 예측**하는 **AI 모델 개발**을 추진

- **메타버스엔터테인먼트사**는 AI를 활용한 **케이팝 가상 아이돌**을 제작하여 음원을 발표하고 팬들과 쌍방향 소통을 위한 챗봇 서비스를 제공 중

(1부. 정부의 AI 정책방향 및 국내·외 산업환경 변화)

□ AI 정책 주무부처인 과학기술정보통신부 이은규 인공지능확산팀장은 AI 일상화 등 2024년도 AI 정책방향을 소개하고,

- AI 발전과 신뢰성 확보를 균형있게 달성하기 위해 마련 중인 인공지능법(안)의 주요내용*과 향후 제도정비 과제**를 금융권에 공유하였음

* 고위험 AI의 정의 및 사업자 책무, AI 위원회 구성 및 윤리원칙 등을 포함

** 고위험 AI 판단기준 및 신뢰성 확보조치, 민간 자율 AI 윤리위원회 표준 등

- 또한, 금융권과 질의·응답을 통해 AI 정책관련 현장의견을 수렴하고 규제 불확실성 해소를 통한 AI 산업 활성화를 추진하겠다고 밝힘



□ 이화영 LG AI연구원 상무는 생성형 AI가 다양한 입력형태(멀티모달AI*)를 이해하고 스스로 데이터를 수집·가공(액서너블AI**)하면서 전문지식이 필요한 업무까지 수행이 가능해져 생산성을 높이는데 기여할 것으로 예측하고,

* 텍스트, 이미지, 음성, 영상 등 다양한 입력을 이해하고 처리하는 기술

** AI가 스스로 데이터를 수집·가공하여 모델을 만들고 인간에게 직접 추천하는 기술

- 클라우드 기반의 초거대 언어모델 대비 데이터 보안에 강점이 있는 온-프레미스*(On-premise) 기반의 생성형 AI 시스템 활용이 매우 중요해질 것으로 전망하였음

* 클라우드 환경이 아닌 자체 데이터 설비를 기업 내 구축하여 운용하는 환경

(2부. 건전한 AI 활용방안 및 금융권 AI 활용사례 공유)

- 권태경 연세대 교수는 국내·외 대규모 언어모델(LLM)의 기술적 특성과 데이터 흐름 중심의 AI 동작방식을 소개하고,
 - 언어모델의 악용, 플러그인 취약점 등 대규모 언어모델의 7대 주요 보안위협 및 발생원인을 진단하였으며,
 - 접근계정 보안강화, 올바른 언어모델 확장 프로그램 사용 등을 통한 생성형 AI의 안전한 활용방안을 제시하였음

생성형 대규모 언어모델
AI 기술의 대표적인 보안 위협

개요

연세대학교 정보대학원
정보보호/사이버안전연구소

• 언어모델의 7가지의 대표적 보안 위협과 주 원인

보안 위협	주 원인
잘못된 정보	<ul style="list-style-type: none"> • 편향 • 환각 현상 • 최신 데이터 학습 부족
언어모델 악용	<ul style="list-style-type: none"> • 적대적 시스템 메시지
악성 언어모델을 통한 사기 행위	<ul style="list-style-type: none"> • IT 취약계층의 오용
데이터 유출	<ul style="list-style-type: none"> • 훈련 데이터 합성 및 추론 • 훈련 데이터 암기 및 유출 • 대화중 개인정보 및 민감 정보 작성

보안 위협	주 원인
플러그인 취약점	<ul style="list-style-type: none"> • 언어모델의 적용 범위 확장 • 안정성 확인 미흡 • 해커 역량 강화 • 취약점이 있는 서비스와 연결
확장 프로그램 취약점	<ul style="list-style-type: none"> • 확장 프로그램 내부의 악성 서비스 설치 • 서비스 제공 업체의 보안 조치 미흡
API 취약점	<ul style="list-style-type: none"> • 미흡한 API 키 관리 • 데이터와 명령 사이의 불분명한 경계

- 패넬토론에 참석한 조영서 KB 지주 부사장은 생성형 AI 기술검증 사례*에 기반한 AI 거버넌스 구축 경험을 공유하였으며,
 - * 19개 업무에 대한 자체 AI 기술검증 결과 기존 대비 약 20~50% 수준의 생산성 개선
 - 안전한 AI 활용을 위한 KB 윤리기준 및 AI 위험도 분류기준 등 위험관리 정책, 통제 프로세스 수립방향을 소개하였음
- 안성희 신한카드 상무는 9개 분야* 170여개 AI 모델 운영현황과 AI 트랜스포메이션 추진방안을 소개하였음

* 고객상담, 마케팅 지원, 리스크관리, 데이터분석, 업무효율화, FDS, 경영관리 등

- 김성수 교보생명 상무는 파일럿으로 진행한 교보GPT와 챗봇 등 다양한 AI 활용서비스를 소개하고 향후 추진계획*을 설명하였음

* 보험금지급심사 및 대출심사지원, 챗봇 고도화, 내근사원 업무지원 등

Ⅲ. 향후 계획

- 금융감독원은 AI가 금융혁신의 촉매가 될 수 있도록 학계, 업계, 글로벌 금융감독기구 등과 적극적으로 소통하고 협력할 예정이며,
 - 안전성과 신뢰성을 기반으로 금융권의 AI 활용이 활성화될 수 있도록 합리적 규율방안을 마련해 나갈 계획임

☞ 본 자료를 인용하여 보도할 경우에는 출처를 표기하여 주시기 바랍니다. (<http://www.fss.or.kr>)