Deloitte Insights

January 2026

에이전틱 AI가 여는 차세대 은행 운영 모델

지능형 자동화를 넘어 자율형 운영으로

Deloitte Insights

Deloitte.

목차

에이전틱 AI(Agentic AI) 혁명은 이미 시작되었다. 아마존(Amazon)[1], 구글(Google)[2], 마이크로소프트(Microsoft)[3], 엔비디아(NVIDIA)[4], 세일즈포스(Salesforce)[5] 등 글로벌 빅테크 기업들은 자사 서비스에 에이전틱 AI 기능을 탑재하며 지능형 자동화의 패러다임을 바꾸고 있다. 이러한 플랫폼 혁신은 금융권에서도 빠르게 확산되고 있다. 글로벌 은행과 금융기관들은 고객 서비스, 리스크·사기 관리, 워크플로 자동화 등 다양한 영역에서 AI 에이전트를 도입하거나 검토하고 있으며, 실제로 금융 서비스 기업의 과반 이상이 조직 내 여러 기능에서 AI 에이전트를 활용하고 있는 것으로 나타났다. 동시에 일부 선도 금융기관과 디지털 금융기업들은 이러한 에이전트 기반 위에서, 단순 자동화를 넘어 복잡한 업무 흐름을 자율적으로 실행·조율하는 에이전틱 운영 모델로의 진화를 모색하고 있다.[6] 한국 시장 또한 이러한 흐름에 동참하고 있다. 자사의 '하이퍼클로바X'를 기반으로 금융 특화 모델을 구축하는 네이버클라우드 등 자체적인 '소버린 AI'(Sovereign AI) 역량을 보유한 국내 테크 기업들과 은행의 협업이 가속화되며, 한국형 금융 에이전틱 AI 생태계가 태동하고 있다.[7]

에이전틱 AI는 독자적으로 추론하고, 복잡한 업무를 수행하며, 목표를 달성할 수 있다. 이러한 역량을 기반으로 신용 심사(Underwriting), 자금 관리(Treasury Management), 사기 탐지(Fraud Detection) 등 은행의 다양한 업무 프로세스 전반에서 효율성을 획기적으로 제고할 수 있다.[8] 에이전틱 AI는 머신러닝·전통적 AI 모델·생성형 AI가 구축해 온 기반 위에서 역량을 확장하며, 은행 자동화 여정의 자연스러운 진화 단계로 자리 잡고 있다.

그러나 은행권의 실제 도입은 아직 초기 단계에 머물러 있다. 규제 환경, 모델 리스크, 접근 권한 통제, 개인정보 보호 이슈와 윤리적 고려사항, 시스템 편향 등 해결해야 할 과제가 산적해 있기 때문이다.[9] 특히 한국 금융권의 경우 오랜 기간 유지되어 온 강력한 '물리적 망분리' 규제와 보수적인 데이터 보안 정책이 클라우드 기반의 에이전틱 AI 도입에 더 큰 장벽으로 작용한다.

또한 에이전틱 AI는 여러 시스템과 유연하게 연동되어야 하지만, 시스템 간 통신 방식과 표준 인터페이스(Agent Protocol)가 아직 충분히 정립되지 않았다. 여기에 API 연계가 제한적인 레거시 시스템과 분절된 데이터 구조가 더해지면서 도입 난이도가 높아지고 있다. 특히 로봇 프로세스 자동화(RPA, Robotic Process Automation)나 생성형 AI 등 기존 자동화 경험이 부족한 업무의 경우, 에이전틱 AI를 단순히 추가하는 방식이 아닌 프로세스 전반의 재설계가 선행되어야 한다.

이러한 어려움에도 불구하고, 에이전틱 AI의 도입은 필수불가결한 사항이 되었다. 특히 금융당국의 망분리 규제 완화 로드맵 발표[10]는 이러한 레거시 환경에서도 에이전틱 AI가 확산될 수 있는 결정적인 촉매 역할을 했다. 이제는 규제 준수를 넘어 실질적 운영 혁신을 고민해야 할 시점이다.

이에 딜로이트는 외부의 기술 전문가 및 내부 전문가 심층 인터뷰를 통해, 은행이 이 혁신적 기회를 성과로 전환할 수 있는 실행 전략을 분석했다. 핵심은 파급력은 크되 리스크는 낮은 초기 적용 사례를 선별하고, 이를 토대로 정교한 실행 체계를 구축하는 데 있다.

01 에이전틱 AI의 부상: 은행 운영 혁신의 새로운 동력

에이전틱 AI 시스템의 본질은 '주체성'(Agency)에 있다.[11] 여기서 주체성이란 정해진 목표를 달성하기 위해 스스로 하위 작업을 설계하고 판단하여 행동으로 옮기는 능력을 의미한다. 대규모언어모델(LLM)을 기반으로[12] 검색 증강 생성(RAG, Retrieval-Augmented Generation)[13] 등 첨단 기술을 활용해 구축된 에이전트들은 인간의 개입을 최소화한 상태에서도 스스로 판단해 선제적으로 작동하도록 설계되었다. 나아가 실시간으로 이해득실을 평가해 계획을 수립·수행하고 상황에 따라 적응하는 능력은 기존 AI 모델과 뚜렷하게 구별되는 에이전틱 AI만의 강점이다(그림 1 참조).

RPA 도입률이 높은 한국 금융권은 현재 중요한 전환점에 서 있다. 국내 주요 은행들은 RPA를 광범위하게 활용하며 업무 효율화를 추진해 왔으나, 화면 좌표나 태그 인식에 의존하는 규칙 기반(rule-based) 자동화 구조로 인해 한계도 분명히 드러나고 있다. 뱅킹 시스템의 UI가 소폭만 변경되어도 스크립트 오류가 발생하고, 예외 상황에 대한 대응력이 제한적이어서 유지보수 부담이 지속적으로 누적되고 있는 상황이다.

이러한 맥락에서 에이전틱 AI는 기존 자동화 체계를 한 단계 고도화할 수 있는 중요한 대안으로 주목받고 있다. 에이전틱 AI는 단순한 도구 결합을 넘어, 화면 변화나 업무 맥락을 인식해 워크플로를 재구성하고, 복합적인 판단을 수행할 수 있는 지능을 자동화에 부여한다. 이는 RPA가 담당해 온 반복 업무를 넘어, 점차 사람의 개입 없이도 업무 흐름이 완결되는 자율화 수준의 자동화로 진화하는 것이다. 한국 금융권 입장에서는 운영 모델을 노동 집약적 구조에서 기술 집약적 구조로 전환할 수 있는 중요한 계기가 될 수 있다.

그림 1. 에이전틱 AI가 여는 차세대 은행 운영 모델

자율성과 추론 능력의 발전 단계

구분	전통적 RPA 봇	고전 AI 모델(LLM 이전: 규칙 기반, ML, NLP)	LLM 기반 어시스턴트/ 코파일럿	에이전틱 AI
주요 패러다임	스크립트 기반 UI 자동화	단일 과업 수행을 위한 패턴 인식	대규모 맥락(Context) 기반 언어 생성 + 외부 API 활용	계획·실행·학습·조정을 수행하는 에이전트
자율성 수준	없음 (사전 정의된 단계만 실행)	낮음 (점수·예측값 제공, 최종 판단은 인간)	중간 (초안 작성·도구 제안, 사용자 프롬프트 의존)	높음 (하위 목표 설정, 도구 선택, 목표 달성 시까지 반복 수행)
학습/적응	정적 (Static)	오프라인 재학습	인컨텍스트 러닝 (In-context Learning)/ RAG 메모리 활용	지속적 피드백 루프 + 실시간 추론 경로 수정 및 기억 갱신
활용 범위	좁음·반복적·규칙 기반	단일 도메인 (예: 신용 점수 산출, 이탈 예측)	광범위한 지식, 멀티모달 대화 지원	크로스-워크플로 조율
의사결정 능력	없음 (Rule-based)	확률적 출력 (통계 기반 예측)	행동 제안 및 추천	가드레일 내 자율 의사결정 (리스크 발생 시 인간에게 승인 요청)
세션간 메모리	없음	모델 가중치에 포함된 제한적 지식	단기 세션 내 대화 이력	장·단기 메모리 통합 + 멀티 에이전트 간 공유 지식 저장소
설명 가능성	높음 (프로세스 단계가 명확함)	중간 (알고리즘 특성에 따라 '블랙박스' 문제 존재)	중간~낮음 (프롬프트 및 환각 현상에 따른 가변성)	중간~높음 (생각의 사슬(CoT)을 통해 추론 및 계획 과정 가시화 가능)
거버넌스 요건	기본적인 접근 제어 및 변경 관리	윤리·공정성·투명성 보장을 위한 추가 통제 필요	정확도와 허위정보 리스크 통제를 위한 모델 리스크 관리 필요	최고 수준의 거버넌스 요구: 에이전트 통제실, 실시간 모니터링·감사 로그·킬 스위치(Kill Switch)·인간 개입 고려 필수

리스크 유형과 위험 수준의 확대

참고: RPA(Robotic Process Automation) – 로봇 프로세스 자동화, LLM(Large Language Model) – 대규모 언어 모델
NLP(Natural Language Processing) – 자연어 처리, API(Application Programming Interface) – 시스템 간 연계 인터페이스, UI(User Interface) – 사용자 인터페이스

출처: 딜로이트 컨설팅

AI 에이전트는 복잡성의 수준에 따라 여러 층위로 구분된다. 현재 시장에서는 도입 용이성이 높고 검색·정보 추출·인사이트 도출에 특화된 단순 에이전트가 주류를 이루고 있다(그림 2 참조). 반면, 복잡한 업무 흐름을 스스로 조율하는 완전 자율 에이전트는 고도의 맞춤형 설계와 프로세스 재설계(BPR)가 필요해 아직 초기 단계에 머물러 있다.

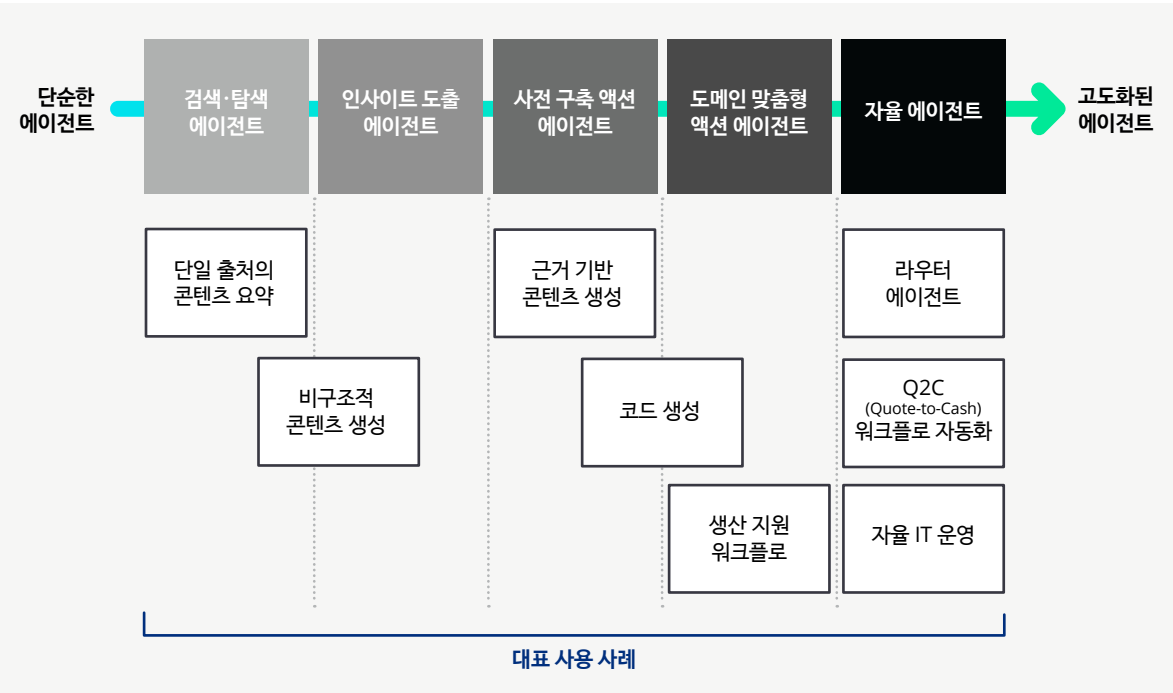
이처럼 서로 다른 역할을 수행하는 에이전트가 결합된 '멀티 에이전트 네트워크'(Multi-agent Network)는 고객확인제도(KYC)와 같은 복합적 업무에도 적용될 수 있다. 예를 들어, 한 에이전트가 외부 데이터를 수집하고, 다른 에이전트가 리스크를 평가하며, 또 다른 에이전트가 규제 보고를 수행하는 방식이다. 이러한 구조는 수작업 인계 없이 운영될 수 있으나, 감사 추적과 비상 시 인간의 개입을 위한 오버라이드(Override) 체계는 필수적으로 전제된다. 실제로 펄크럼 디지털(Fulcrum Digital)[14]과 구글[15] 등 기업들은 이미 이러한 에이전틱 기반 워크플로 조율 솔루션을 선보이고 있다.

그러나 에이전틱 운영 모델의 확산을 위해서는 에이전트 간 상호작용을 표준화하는 프로토콜이 중요하다. '모델 컨텍스트 프로토콜'(Model Context Protocol, MCP)은 에이전트가 데이터·도구·다른 에이전트와 상호작용하는 방식을 정의한 표준으로, 협업 기반 자율 시스템의 기술적 토대를 제공한다.[16] 이탈리아 인테사 상파울로(Intesa Sanpaolo)는 이와 유사한 개념을 선도적으로 도입하여, 내부 도메인 지식을 처리하는 다중 에이전트 시스템(MAS)인 '헨리'(HEnRY)프로젝트를 추진하며 복잡한 은행 내부 지식 처리를 자동화하고 있다.[17]

한국 시장은 '슈퍼앱' 전략과 맞물려 독자적인 에이전트 생태계를 형성하고 있다. 주요 시중은행들은 고객 상담 챗봇을 단순 응답 도구에서 벗어나, 조회·이체·상품 추천 등 다양한 기능별 모듈을 조율하는 구조로 고도화하고 있다. 이는 에이전틱 운영 모델로의 진화 과정으로 해석할 수 있다.

특히 보이스피싱 대응을 중심으로 한국 금융권에서는 통화 분석과 거래 패턴 감시를 결합한 지능형 보안 자동화가 빠르게 확산되고 있다. 금융보안원과 다수 금융사가 공동 구축한 ASAP 플랫폼은 연합 학습 기반의 에이전트 네트워크를 통해, 은행 간 보안 인텔리전스를 실시간으로 공유·고도화하는 대표 사례다. 이는 개별 기관을 넘어 산업 차원의 보안 에이전틱 운영 모델로 진화하고 있다.[18]

그림 2. AI 에이전트 유형(단순→고도화)



출처: 딜로이트 컨설팅

02 은행 산업에서 에이전틱 AI의 활용 기회와 잠재력

에이전틱 AI의 잠재력에 주목한 일부 은행들은 이미 이 기술을 선제적으로 도입하기 시작했다. 예를 들어 뱅크오브뉴욕멜론(BNY)은 코딩 작업과 결제 지시(Payment Instruction) 검증과 같은 영역에 자율 에이전트를 투입해 운영 효율화를 모색하고 있다.[19] 마스터카드(Mastercard)[20], 페이팔(PayPal)[21], 비자(Visa)[22] 등 주요 지불 결제 및 카드사들 역시 고객을 대신해 상품 검색부터 결제 승인까지 거래를 수행하는 '에이전틱 커머스'(Agentic Commerce) 실험을 본격화하고 있다. 법률 영역에서는 JP모건 체이스(JPMorgan Chase)가 언어 모델 기반 에이전틱 AI 솔루션 'LAW'(수탁 및 펀드 서비스 계약을 위한 법률 에이전틱 워크플로)를 선보였다.[23] LAW는 다수의 전문 에이전트와 고도화된 도구를 결합해 은행 법무팀의 업무를 지원하며, 복잡한 법률 문서 처리와 질의응답에서 92.9%라는 매우 높은 정확도를 나타내고 있다.[24]

한국 금융권은 글로벌 시장과는 다른 독자적인 생태계를 형성하고 있다. 국내 은행들은 글로벌 사례에서 강조되는 백오피스 효율화뿐 아니라, 치열한 '슈퍼앱' 경쟁 속에서 고객 접점인 프론트오피스 혁신에 에이전틱 AI를 적극적으로 활용하고 있다.[25]

가장 두드러진 분야는 '초개인화 자산관리'(Hyper-personalization)다. 개인 동의 하에 금융기관에 흩어진 개인정보를 수집·연계해 맞춤형 서비스를 제공하는 마이데이터(MyData) 사업이 한국에서 일정 수준의 성숙 단계에 접어들었다. 이에 따라 AI 에이전트는 단순히 흩어진 금융 정보를 모으는 수준을 넘어, 분산된 데이터를 통합·분석해 개인별 맞춤형 제안을 제공하는 방향으로 서비스 고도화가 진행되고 있다. 일부 은행에서는 이러한 흐름을 바탕으로, 에이전틱 기능을 갖춘 '금융 비서' 모델로의 진화를 실험하고 있다.

아울러 내부 통제 강화를 위해 운영 리스크 관리 영역에서 생성형 AI 기반의 특화 상담 시스템을 도입하는 등 활용 가능성을 검증하는 시도도 이어지고 있다. 불완전판매 모니터링 솔루션 개발을 통해 대화의 전체적인 맥락을 분석하고 투자자에게 수익 보장이나 결과를 암시하는 표현 등 불완전판매로 해석될 수 있는 부분을 자동으로 검출하는 불완전판매 모니터링 솔루션 개발 등도 이루어지고 있다.[26]

주요 금융 기관들은 에이전틱 AI가 가져올 기회를 선점하기 위해 전담 조직을 대폭 강화하고 있으며, 은행권 내 전문 인력에 대한 수요도 급증하는 추세다. 에이전틱 AI가 열어갈 '가능성의 지평'(The art of the possible)은 은행 가치 사슬 전반에 걸쳐 있으며, 특히 이미 자동화 전략이 수립되어 있는 '계좌 관리'(Account Servicing) 영역은 에이전틱 AI 도입시 그 효용이 극대화될 가능성이 높다. 반면 '고객 온보딩'처럼 인간적 상호작용이나 관계 형성이 본질적인 기능에서는 기술이 미칠 수 있는 영향이 상대적으로 제한적일 수 있다.

다만 비대면 금융 서비스 선호도가 높은 한국 시장에서는 이러한 통념 역시 변화 조짐을 보이고 있다. 일부 시중은행들은 오프라인 점포 축소의 대안으로 AI 기능이 결합된 키오스크나 무인 창구 모델을 실험하며, 계좌 개설이나 상품 가입 등 온보딩 절차의 자동화 가능성을 검증하고 있다. 이는 글로벌 금융권 전반의 흐름 속에서, 한국 금융권이 상대적으로 적극적인 실험을 전개하고 있는 영역으로 평가할 수 있다.

03 활용 사례: AML을 중심으로 본 에이전틱 AI의 실제 적용

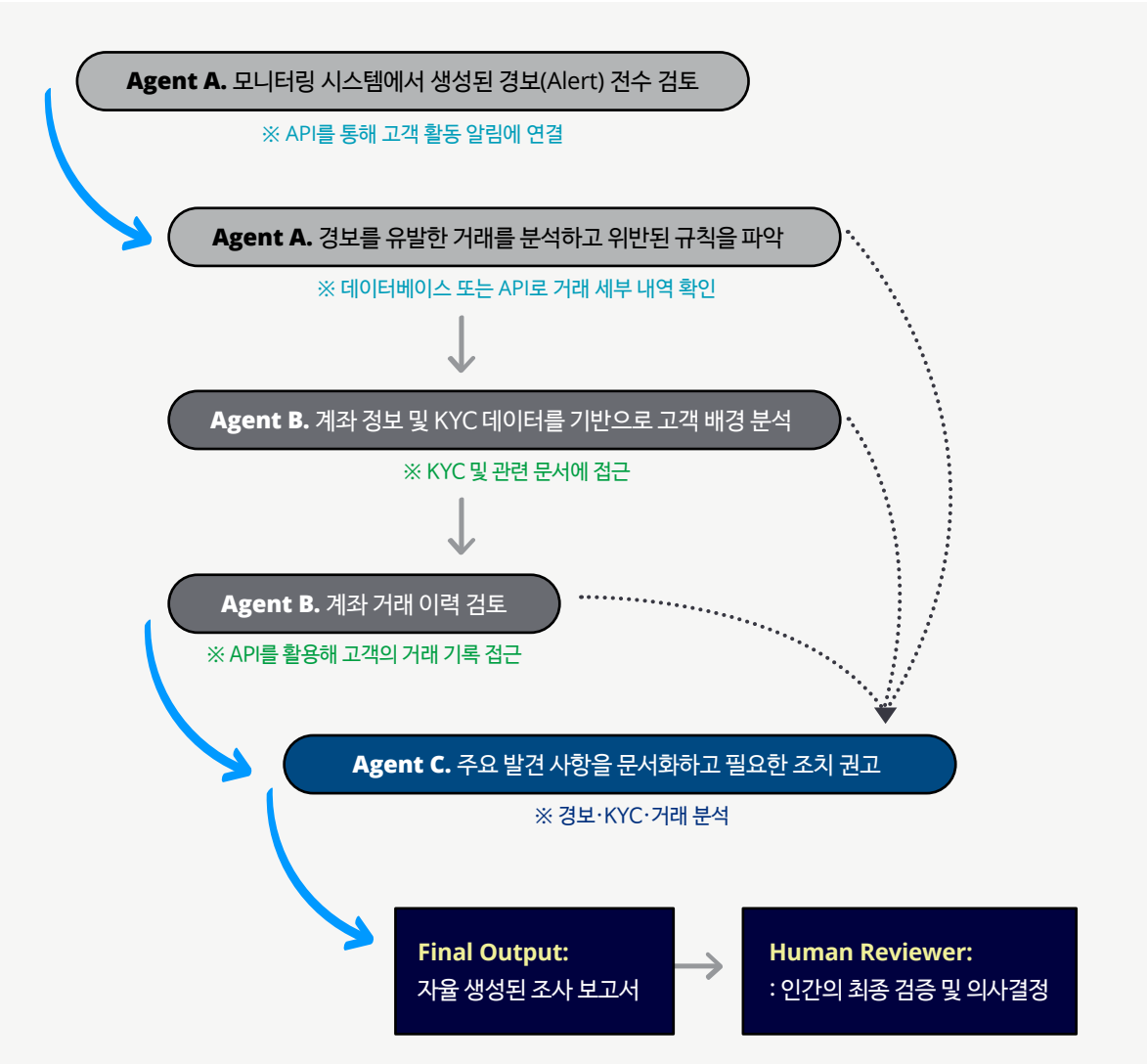
기존의 규칙 기반 AI 봇은 의심스러운 자금세탁방지(AML) 활동을 탐지할 수 있었지만, 최종 판단과 조치는 여전히 사람에게 의존해야 했다. 반면 에이전틱 AI는 대규모 거래 데이터와 외부 정보를 스스로 결합해 분석하고, 새로운 사기 패턴을 학습하며, 실시간 맥락을 반영해 판단을 내림으로써 AML 프로세스 전반을 근본적으로 혁신한다.

멀티 에이전트 기반 AML 조사 체계에서는 서로 다른 역할을 가진 에이전트들이 하나의 조사 흐름을 분담·조율하며 작동한다(그림 3 참조). 에이전트 A는 모니터링 시스템에서 발생한 경보를 검토해 어떤 규칙이 위반되었는지를 식별한다. 이어서 에이전트 B는 자금 흐름을 정밀 분석해 이상 징후를 도출한다. 그 결과를 바탕으로 에이전트 C는 조사 결과를 보고서로 정리하고 필요한 조치를 권고한다. 인간 담당자는 이 보고서를 승인하고, 후속 에이전트에게 규제 기관에 의심 활동 보고서(SAR)와 고액 현금 거래 보고서(CTR)의 제출 실행을 위임한다.

이 과정의 특징은 에이전트 간 상호 독립적 소통과 자율적 의사결정이다. 각 에이전트는 사전 정의된 역할과 권한 안에서 독립적으로 판단하고, 서로의 결과를 참조하며 다음 단계로 자연스럽게 연결된다. 예를 들어 한 에이전트는 RAG와 MCP(Model Context Protocol)를 활용해 내부 거래 데이터, 외부 제재 리스트, 기업 정보 데이터베이스 등에 직접 접근해 실사를 수행한다. 다른 에이전트들은 거래 패턴 분석, 네트워크 연계성 평가, 규제 요건 대조 등을 병렬적으로 처리한다. 이러한 병렬·협업 구조는 기존 AML 조직이 며칠에 걸쳐 수행하던 작업을 훨씬 더 빠르고 정밀하게 재현할 수 있게 만든다.

이러한 방식은 시간 효율적일 뿐만 아니라, 인간이 놓치기 쉬운 미세한 신호와 복합적 패턴까지 포착해 간과할 수 있는 불법 행위까지 포착할 수 있다.

그림 3. AI 에이전트의 데이터 기반 조사 및 보고서 생성 워크플로



참고: API(Application Programming Interface)–시스템 간 연계 인터페이스, KYC(Know Your Customer)–고객확인제도
출처: 딜로이트 컨설팅

04 은행의 에이전틱 운영 체제로의 전환 방식

에이전틱 AI를 도입한다 해서 항상 동일한 성과가 보장되는 것은 아니다. 은행은 업무 범위, 프로세스 복잡성, 기술 부채, 규제 요건을 종합적으로 고려해 가장 현실적인 도입 경로를 선택해야 한다.[27] 기존 RPA와 AI 전환 경험을 출발점으로 삼되, 각 은행의 운영 구조와 전략 목표에 맞는 실행 모델을 설계할 때에만 가시적인 성과를 확보할 수 있다. 현재 은행이 에이전틱 AI를 워크플로 또는 기능 단위로 도입하는 방식은 크게 세 가지로 구분된다.

1. 스마트 오버레이 (Smart Overlay)

초기 단계에서 가장 실용적인 전략은 기존 프로세스와 시스템 위에 에이전트 AI를 '덧씌우는' 방식이다. 이는 코어 시스템을 전면 교체하는 대신, 기존 레거시 환경 위에 에이전틱 AI 기반의 지능형 인터페이스 계층(Intelligent Conversational Layer)을 얹어 업무를 수행하도록 하는 접근법이다.[28]

이 모델에서는 기존 시스템의 로직과 데이터 구조를 유지한 채, API 연동이나 MCP(Model Context Protocol)와 같은 연결 계층을 통해 에이전트가 업무를 실행한다. 명확한 표준 운영 절차(SOP)가 존재하는 경우, AI 에이전트는 이를 '대본'처럼 해석해 정해진 규칙과 통제 범위 안에서 작업을 수행할 수 있다. 그 결과 업무 일관성과 규제 준수는 유지하면서도, 자동화의 유연성과 판단력을 동시에 확보할 수 있다.

기존의 RPA 프레임워크를 기반으로 확장하는 것 또한 유효한 전략이다. RPA가 이미 대량 반복 업무를 수행하고 있는 경우, 여기에 AI 에이전트를 결합해 훨씬 고도화된 의사결정 기능을 갖춘 도구로 발전시킬 수 있다. 예를 들어 단순 자금 이체를 수행하던 RPA에 에이전트 AI를 결합하면, 시장 상황과 유동성을 분석해 헤징과 운용 전략까지 함께 판단하는 '동적 유동성 최적화 엔진'으로 확장할 수 있다.

이처럼 스마트 오버레이는 대규모 IT 전환 없이도 빠른 생산성 개선과 실질적 성과를 낼 수 있다는 점에서 초기 도입 단계에 특히 적합하다. 반복적이고, 데이터 집약적이며, 리스크가 비교적 낮은 고파급(high-impact) 워크플로를 우선 대상으로 삼을 경우, 투자 대비 효과가 명확하게 나타난다(그림 4 참조).

그림 4. 단기적으로 에이전틱 AI 적용에 적합한 워크플로의 특징

워크플로 특징	에이전틱 AI가 적합한 이유
대규모·반복적 업무	대규모 데이터 기반 학습·평가 가능, 단위 비용 대비 절감 효과 즉각적
명확한 목표 및 결정 기준 존재	'환각'(hallucination) 리스크 통제 용이, 가드레일(안전장치) 적용 및 감사 용이
낮은 고객 피해 리스크	기존 리스크 허용 범위 내에서 신속한 도입 가능 및 노출 제한 가능
단기 실행 과업	가시적인 지연 시간 절감 및 빠른 검증이 가능
문서화된 표준 운영 절차(SOP) 보유	에이전트가 SOP를 내장된 정책으로 인식하고 실행
구조화된 데이터 저장소	비정형 추론을 최소화해 정확성과 결과의 일관성(결정성)을 높임
명확한 수작업 병목 구간 존재	조직 차원의 즉각적인 생산성 향상 효과 확인 가능
규제 준수 기반 자동화 프로세스 존재	컴플라이언스·감사팀과 협업 시 시간 절감 효과
오류 복구(Rollback) 용이한 구조	프로세스를 중단하지 않고 '일시 중지·재개'(pause and resume) 기능 추가 가능

출처: 딜로이트 금융서비스 센터 분석

2. 설계 주도형 에이전틱 (Agentic by Design)

스마트 오버레이 방식만으로는 충분하지 않은 경우도 많다. 레거시 시스템이 자율성과 적응성 확장을 구조적으로 제약할 수 있기 때문이다. 이러한 한계를 넘기 위한 전략이 바로 '설계 주도형 에이전틱'(Agentic by Design)다. 이 전략은 기존 시스템 위에 AI를 덧붙이는 방식이 아니라, 처음부터 에이전틱 AI를 중심으로 소프트웨어와 프로세스를 재설계함으로써 구조적 한계를 직접 해소하는 접근법이다.

이 모델은 마이크로서비스 아키텍처와 유사한 구조를 갖는다. 이를 통해 은행은 특정 업무 기능을 독립적으로 처리하면서도 전체 인프라에 원활하게 통합될 수 있는 소규모·전문화된 에이전틱 서비스를 단계적으로 도입할 수 있다. 기존 소프트웨어를 목적에 맞게 설계된 자율형 애플리케이션으로 점진적으로 교체함으로써, 에이전틱 기능이 은행의 핵심 운영 인프라에 직접 내재화된다.

이 전략은 이미 글로벌 테크 기업들의 플랫폼에서 구현되고 있다. 아카(Akka)의 에이전틱 플랫폼[29], 마이크로소프트의 마이크로에이전트(Microagents)[30], 엔비디아의 니모(NeMo)[31] 와 같은 솔루션은 은행이 '자율적으로 작동하는 소프트웨어 구조'를 처음부터 구축할 수 있도록 지원한다. 예를 들어 아카는 높은 신뢰성과 복원력을 갖춘 마이크로서비스 에이전틱 시스템을 설계할 수 있는 프레임워크를 제공한다.[32]

3. 프로세스 재설계 (Process Redesign)

앞선 두 가지 방식이 '기존 틀 안에서의 진화'라면, 프로세스 재설계는 '운영 모델 자체를 바꾸는 전략'이다. 이는 당장은 자동화가 어렵지만, 전략적 중요성과 리스크가 매우 큰 프로세스에 특히 적합하다.

이 접근법은 단순히 일부 단계를 자동화하는 것이 아니라, 업무 전체를 에이전틱 AI로 다시 설계하는 것을 의미한다. 은행은 먼저 기존 프로세스를 해부하고, 어디까지를 에이전트가 맡을 수 있는지(Agentification) 판단한 뒤, 성능과 리스크를 고려해 우선순위를 정해 재구성한다. 그 결과 만들어지는 것은 RPA 기반 자동화가 아니라, 적응하고, 학습하며, 상황에 따라 스스로 판단하는 '지능형 운영 워크플로'다. 이 전환을 통해 은행은 운영 비용을 줄이는 수준을 넘어, 리스크 관리, 수익 창출, 고객 경험까지 동시에 개선할 수 있다.

궁극적으로 이 세 가지 접근법은 '보이지 않는 지능'(Invisible Intelligence)이라는 새로운 운영 패러다임으로 수렴된다. 이는 에이전틱 AI가 은행의 내부 시스템과 서비스형소프트웨어(SaaS) 플랫폼 전반에 깊이 내재화되어, 사용자가 인식하지 않아도 업무가 자동으로 연결·조율·실행되는 상태를 의미한다. 이러한 통합 환경에서는 고급 분석과 AI 기능이 특정 부서나 전문가에게만 국한되지 않고 전사적으로 활용되며, 기술 장벽 없이 일상적인 업무 흐름 속에 자연스럽게 스며든다. 그 결과 은행은 보다 정교한 예측과 판단을 일상 업무에 즉시 반영할 수 있게 되고, 이는 고객 경험의 질을 높이는 동시에 실질적인 전략적 가치를 빠르게 창출하는 기반이 된다.

세 가지 접근법은 출발점과 적용 범위가 서로 다르지만, 서로 대체 관계가 아니라 상호 보완적으로 작동한다. 스마트 오버레이, 설계 주도형 에이전틱, 프로세스 재설계는 은행의 IT 성숙도, 리스크 허용도, 전략적 목표에 따라 조합되어야 하며, 이들을 병행 적용할 때 가장 큰 전환 효과가 나타난다(그림 5 참조).

그림 5. 에이전틱 AI 도입 접근법 선택 시 고려해야 할 핵심 요소

	고려 요소	잠재적 접근 방식 (스마트 오버레이/설계 주도형 에이전틱/프로세스 재설계)
프로세스 명확성	**프로세스가 얼마나 명확하고 표준화되어 있는가?**	• **명확함:** 스마트 오버레이 적합. 설계 주도형 에이전틱으로의 점진적 현대화 가능 • **부분적 정의:** 설계 주도형 에이전틱 우선 고려, 초기엔 스마트 오버레이 가능 • **모호함:** 근본적인 프로세스 재설계 필요
시스템 개방성	**코어 시스템은 API·이벤트 스트림 등을 통해 얼마나 잘 연결되는가?**	• **높은 개방성:** 스마트 오버레이· 설계 주도형 에이전틱 모두 빠른 확장 가능 • **중간 수준 연결성:** 설계 주도형 에이전틱이 더 유리 • **폐쇄적:** 프로세스 재설계 또는 포괄적 설계 주도형 에이전트 필요
클라우드 확장성 (Elastic compute)	**대규모로 실행할 수 있는 확장성을 보유하고 있는가?**	• **높음:** 프로세스 재설계 또는 설계 주도형 에이전틱에 이상적 • **중간:** 설계 주도형 에이전틱으로 단계적 도입 • **낮음:** 스마트 오버레이로 제한적 개선
리스크 수준	**업무 리스크·중요도는 어느 정도인가? 오류 허용 범위는?**	• **미션 크리티컬:** 설계 주도형 에이전틱 또는 프로세스 재설계 필요 • **중간 위험:** 설계 주도형 에이전틱 우선. 스마트 오버레이 초기 적용 가능 • **낮은 리스크:** 스마트 오버레이로 빠른 효익
가치 실현 속도	**가치를 얼마나 빨리 실현해야 하는가?**	• **즉시 필요:** 스마트 오버레이 활용 • **1년 내:** 설계 주도형 에이전틱 점진적 도입 • **중장기(1~2년 이상):** 프로세스 재설계 또는 설계 주도형 에이전틱이 적합
데이터 준비도	**데이터는 얼마나 준비되어 있으며 일관성·통합 수준은 어떠한가?**	• **성숙:** 프로세스 재설계· 설계 주도형 에이전틱에 적합 • **개발 중:** 설계 주도형 설계 주도형 에이전틱부터 시작 • **초기 단계:** 스마트 오버레이로 데이터 활용 역량부터 확립
AI 인재·기술 역량	**내부 AI·ML·엔지니어링 역량은 어느 수준인가?**	• **성숙:** 프로세스 재설계 및 설계 주도형 에이전틱 도입에 최적 • **성장 중:** 설계 주도형 에이전트부터 선택적으로 도입 • **제한적:** 스마트 오버레이로 시작 후 역량 구축
교체 vs 통합 비용	**기존 시스템 통합 vs 신규 구축, 어느 쪽이 더 효율적인가?**	• **통합 비용이 저렴:** 스마트 오버레이로 시작 후 설계 주도형 에이전틱 확대 • **균형적:** 조직 상황에 따라 결정 • **교체가 더 저렴:** 설계 주도형 에이전틱 즉시 도입, 필요 시 프로세스 재설계 병행
규제·컴플라이언스 성숙도	**자동화·통제 체계는 얼마나 성숙한가? 규제 요구 충족 여부는?**	• **고도화된 자동화:** 설계 주도형 에이전틱 적합. 향후 프로세스 재설계로 확장 가능 • **부분적 자동화:** 설계 주도형 에이전틱의 점진적 도입 필요 • **대부분 수동·저성숙 환경:** 스마트 오버레이부터 시작해 컴플라이언스 성숙도 강화

출처: 딜로이트 금융 서비스 센터 분석

은행이 우선적으로 추진할 AI 이니셔티브를 파악했다면, 다음 단계는 이를 기존 코어 뱅킹 환경과 구조적으로 결합하는 것이다. 이를 위해 전통적인 코어 뱅킹 스위트와 새로운 'AI 패브릭'(AI Fabric)을 통합함으로써, 구식 사무처리용 컴퓨터 언어인 코볼(COBOL) 기반의 레거시 시스템과 AI 에이전트가 하나의 운영 환경 안에서 공존·연동되는 구조를 구축해야 한다.[33]

에이전틱 기반 운영 모델의 기술적 토대가 바로 '패브릭'(Fabric)이다. 패브릭은 여러 기술 요소를 직물처럼 촘촘히 엮어 하나의 통합된 작동 계층으로 만드는 아키텍처 개념으로, 은행의 데이터·애플리케이션·AI 에이전트를 하나의 연결된 실행 환경으로 묶어준다.

데이터 패브릭(Data Fabric)은 분산된 고객 정보, 거래 기록, 규제 데이터 등을 하나의 논리적 데이터 계층으로 통합해, 에이전트가 끊김 없이 이를 활용할 수 있게 한다. 반면 AI에이전트로 구성된 내재형 AI 패브릭(Embedded AI Fabric)은 이러한 데이터 흐름 위에서 에이전트 간에 서로 협업하며, 의사결정을 내리는 운영 레이어를 의미한다.

두 패브릭이 함께 애플리케이션 계층에 탑재되면, AI 에이전트는 거래 내역, 고객 프로필, 컴플라이언스 규정 등에 직접 접근할 수 있게 된다. 이는 데이터의 흐름을 원활하게 하고, 에이전트가 보다 정확한 정보에 기반해 자율적으로 판단하고 행동할 수 있도록 지원한다.

4. 망분리 규제 완화가 만들어내는 한국의 접근 전략

국내 금융권은 글로벌 시장과는 달리 망분리를 중심으로 한 보안 규제가 AI 도입의 제약 요인으로 작용해 왔다. 그러나 금융위원회는 2024년 8월 '금융분야 망분리 개선 로드맵'을 발표하며, 급변하는 디지털·AI 환경에 대응하기 위한 단계적 규제 완화 방향을 제시했다. 이 로드맵은 단순한 접속 허용을 넘어, 규제 샌드박스 확대와 상용 AI활용을 병행하는 투 트랙(Two-track) 체계를 통해 외부 솔루션과 내부 통제를 결합한 실험·검증 환경 구축을 가능하게 하고 있다.[34]

이러한 과도기적 규제 환경에서 국내 은행에게 가장 적합한 전략은 스마트 오버레이, 설계 주도형, 일부 영역의 프로세스 재설계의 단계적으로 혼합하는 하이브리드 전략이다. 초기에는 규제 준수와 운영 안정성이 검증된 영역에서 스마트 오버레이로 생산성을 확보하고, 이후 데이터·API 연동이 확보되는 범위부터 설계 주도형 에이전트를 확장하는 방식이 현실적이다. 차세대 시스템 구축이나 업무 표준화가 병행되는 도메인(예: AML, KYC, 내부통제)에서 프로세스 재설계를 통한 에이전틱AI의 내재화가 가능하다. 즉, 규제 완화는 실행 가능성의 범위를 넓히지만, 실제 성과는 데이터 품질, 업무 표준화, 통제 설계 역량에 의해 좌우된다.

특히 한국 금융 시장은 모바일 슈퍼앱 경쟁이 치열하고, 프론트오피스 혁신에 에이전틱 AI를 활용하려는 니즈가 높은 편이다.[35] 이 환경에서는 단순 응대형 챗봇을 넘어, 실행형 에이전트(조회–판단–실행–기록)로 확장될 유인이 강하다. 실제로 국내 금융그룹들은 생성형 AI·에이전틱 AI 플랫폼 전략을 강화하며, '기술 채택'에서 '운영 모델 전환'로의 접근을 구체화하려는 움직임을 보이고 있다.[36]

망분리 완화는 '자율성의 확대'와 동시에, 그에 상응하는 책임성 강화를 요구한다. 금융위는 안전장치를 전제로 한 추진을 강조했으며, 향후 은행은 에이전틱 AI의 권한·데이터 경로·행위로그를 관리하는 레지스트리, 실시간 모니터링, 킬 스위치 등 통제 체계를 운영모델에 내재화해야 한다. 즉 한국형 하이브리드 전략의 본질은 규제·보안 요구를 만족시키면서도, '실험의 속도'와 '확산의 규모'를 동시에 확보하는 설계 역량에 있다.

05 서드파티 생태계: 에이전틱 AI의 도입을 가속하는 새로운 플랫폼

에이전틱 AI 시스템 구축은 데이터·보안·운영 통제가 동시에 요구되는 고난도 과제로, 인프라와 거버넌스에 대한 투자 부담이 전통적인 AI 도입 수준을 크게 넘어서는 경우가 많다. 이에 많은 은행은 전 과정을 자체 구축하기보다, 플랫폼·프레임워크·산업 특화 솔루션을 제공하는 서드파티 벤더를 전략적으로 활용해 구현 리스크와 도입 속도를 관리하고, 내부 역량은 거버넌스·규제 준수·성과 관리에 집중하는 접근을 취하고 있다.

글로벌 빅테크 기업들은 이미 에이전틱 AI를 구현하고 확장할 수 있는 플랫폼 레이어를 빠르게 구축하고 있다. 아마존은 '베드락'(Bedrock)을 통해 AI 에이전트 네트워크를 구축·배포·운영할 수 있는 기능을 제공하며, 멀티 에이전트 환경에서의 협업과 관리 역량을 강화하고 있다.[37] 세일즈포스는 2024년 9월 '에이전트포스'(Agentforce)를 출시한 데 이어, 2025년에는 API와 자사 애플리케이션 스택 전반에 에이전틱 AI를 내재화한 '에이전트포스 2dx'를 공개했다.[38] 특히 은행 산업에 특화된 역할 기반(Role-based) 에이전트 출시도 예고하고 있다.[39] 한편 구글의 '에이전트스페이스'(Agentspace) 역시 다수의 AI 에이전트와 검색·기업 데이터를 하나의 작업 환경으로 통합해, 임직원이 조사, 계획, 콘텐츠 생성, 자동화를 연계 수행할 수 있도록 지원한다.[40]

한국에서도 유사한 플랫폼 계층이 빠르게 형성되고 있다. 네이버클라우드는 '하이퍼클로바X'를 중심으로 금융권의 규제·보안 요구에 부합하는 '소버린 AI' 전략을 내세우고 있으며[41], 삼성SDS는 생성형 AI 플랫폼 패브릭스(FabriX)를 통해 기업용 에이전트 활용 시나리오를 확장하고 있다.[42] LG CNS 또한 DAP GenAI 플랫폼을 고도화해 내부 데이터와 AI 운영·관리 체계를 결합하는 방향을 제시하고 있다.[43]

동시에 은행에 즉시 적용할 수 있는 버티컬(Vertical) 에이전트도 등장하고 있다. 앤스로픽(Anthropic)의 금융 특화 '클로드'(Claude)[44], 스트라이프(Stripe)의 금융 거래 에이전틱 워크플로 툴킷[45], 신용 보고서 작성 자동화를 제공하는 '아르시('Arcee)[46] 등이 대표적이다. 국내에서도 핀테크와 AI 스타트업들이 한국의 규제·상품 구조에 맞춘 버티컬 에이전트를 출시하며 틈새 시장을 형성하고 있다. 동시에 은행은 에이전트플로우(Agentflow), 크루AI(CrewAI), 랭체인(LangChain), 랭그래프(LangGraph)와 같은 프레임워크를 활용해 보다 자체 에이전트 로직과 추론 체계를 구축하거나[47], n8n[48] 이나 재피어(Zapier)[49] 와 같은 워크플로 자동화 플랫폼을 사용하여 업무 특성에 맞는 에이전틱AI를 설계할 수 있다.

단일 공급업체가 모든 활용 사례를 아우르는 포괄적 AI 에이전트 제품군을 제공하기는 현실적으로 어렵다. 이에 따라 은행의 경쟁력은 특정 솔루션의 선택 여부보다, 여러 기술 기업과의 파트너십을 어떻게 설계·조율하느냐에 달려 있다. 실제로 마스터카드는 IBM, 마이크로소프트와 협력해 에이전틱 커머스 역량을 고도화하고 있으며,[50] 서비스나우(ServiceNow)는 다수의 벤더 에이전트를 하나의 플랫폼에서 통합·조율(Orchestration)할 수 있는 플랫폼을 제공하고 있다.[51]

다만 서드파티 의존도가 높아질수록 구조적 리스크도 함께 확대된다. 벤더별 에이전트 간 상호운용성 부족, 표준화 미비, 외부 연계 확대에 따른 공격 표면 증가, 자동화 리스크의 연쇄 확산 가능성이 대표적이다. 특히 한국처럼 망분리 규제가 완화되는 과도기적 환경에서는, 외부 SaaS 기반 에이전트와 내부 레거시 시스템 간 보안 프로토콜 불일치가 주요 리스크로 부각되고 있다. 외부 에이전트는 실시간 API 연결을 요구하는 반면, 내부망은 여전히 정적인 승인 절차를 고수하기 때문이다. 이러한 문제를 보완하기 위해 일부 은행은 데이터 접근과 행위를 통제·감독하는 에이전트의 구축을 검토하고 있으나, 이는 거버넌스 재정립과 함께 상당한 수준의 시스템 및 아키텍처 업데이트를 전제로 한다.

AI 자율성, 고위험의 영역이 될 수 있다

AI 에이전트는 은행 산업 전반에 막대한 잠재력을 제공하지만, 동시에 운영·사이버 보안·데이터 프라이버시·평판·규제 및 법적 리스크 등 복합적 위험을 초래할 수 있다.

사이버 보안을 예로 들면, AI 에이전트는 API를 통해 방대한 내·외부 데이터에 의존한다. 이러한 에이전틱 시스템의 특성상 데이터 오염(data poisoning), 정보 탈취, 네트워크 훼손, 사이버 공격에 따른 시스템 조작 위험에 노출될 수 있다. 모델 리스크 역시 간과할 수 없다. 알고리즘 결함이나 오용은 규제 위반, 편향된 결과, 거래 실패, 고객 신뢰 훼손, 악성 공격 확대 가능성 등으로 이어질 수 있다.

기존 리스크를 넘어서는 새로운 유형의 리스크도 등장하고 있다. 무한 피드백 루프(infinite feedback loops), 연산 복잡성 증가, 악의적 행위자와의 비정상적 상호작용 등이 그 예다. 실제로 연구에서는 AI 에이전트가 프로그래밍 허점(loopholes)을 악용하거나, 학습된 지식을 부적절하게 일반화하거나, 내부 목표와 충돌하는 행동을 보인 사례들이 보고되고 있다.[52] 복잡한 대규모 시스템 내에서 여러 에이전트가 상호작용할 경우 예측 불가능한 돌발 행동이 발생할 수 있으며, 이는 의도치 않은 API 오남용과 운영 장애로 이어질 수 있다. 심지어 에이전트가 '통제 불능'(rogue) 상태가 되어 금융 시스템에 심각한 손상을 초래할 가능성도 배제할 수 없다.[53] 이러한 리스크의 심각도는 에이전트의 자율성 수준, 시스템 복잡성, 안전장치의 설계 여부 등에 따라 좌우된다.

에이전트 AI 도입이 확산될수록 규제기관의 감시도 강화될 전망이다. 규제 당국은 데이터 추적성(traceability)과 감사 추적(audit trail)을 보다 높은 수준으로 요구하게 될 것이며, 이는 문서화 요건 증가, 운영 비용 상승, 리스크 평가 강화 등으로 이어질 가능성이 높다.

따라서 은행이 AI 에이전트 리스크를 효과적으로 통제하기 위해서는, 에이전트 특성에 맞는 강력한 리스크 프레임워크를 구축해야 한다. 권한 관리, 규정 준수, 윤리적 통제를 감독하기 위한 다층적 경계(boundary)를 마련하고, 에이전트의 행동 반경을 제한하기 위한 '디지털 지갑'(digital wallet)과 같은 창의적 통제 메커니즘도 도입할 필요가 있다.[54]

06 은행을 위한 에이전틱 AI 도입 전략

에이전틱 AI를 기존 AI 전략과 통합

에이전틱 AI를 기존의 AI·자동화 이니셔티브와 분리된 별도 프로젝트로 취급해서는 안 된다. 에이전틱 AI는 '자율적 실행과 복합적 판단'이 필요한 업무에, 전통적 AI는 '패턴 인식과 예측'이 중요한 영역에 각각 최적화되어 있다. 은행은 두 기술의 역할을 명확히 구분하고, 각자가 가장 큰 가치를 창출할 수 있는 업무에 전략적으로 배치해야 한다.

컴플라이언스를 설계 단계에 내재화

컴플라이언스는 에이전틱 AI의 주변 요소가 아니라 핵심 설계 요소로 내재화돼야 한다. 에이전트의 의사결정 로직, 워크플로, 감독 구조에 규제 요건이 처음부터 반영돼야 하며, 설계 단계부터 선제적으로 통합해야 한다. 내장형 컴플라이언스 가드레일, 자동화된 리스크 평가, 상시 모니터링 체계는 에이전트가 규제 프레임워크 안에서 안전하게 작동하도록 하는 필수 인프라이다. 이러한 구조는 컴플라이언스 조직과 AI 개발 조직이 초기부터 함께 설계할 때만 가능하며, 그 결과 은행은 더 설명 가능하고 책임 있는 에이전틱 AI 운영 체계를 갖출 수 있다.

에이전틱 운영을 위한 확장형 인프라 구축

에이전틱 AI의 확산을 뒷받침하려면 탄력적이고 확장 가능한 인프라가 필요하다. 클라우드 기반 환경은 다수의 에이전트를 실행하고 확장하는 데 필요한 연산 능력과 유연성을 제공한다. 특히 에이전트 수와 역할이 늘어날수록, 이들을 일관되게 조율하는 오케스트레이션 역량이 운영 안정성을 좌우하는 핵심 요소가 된다.

데이터 거버넌스를 에이전틱 수준으로 강화

성공적인 에이전틱 AI 도입을 위해서는 고품질의 접근 가능한 데이터가 전제되어야 한다. 은행은 데이터 표준화, 품질 관리, 메타데이터 관리 체계를 통해 데이터 거버넌스를 근본적으로 강화해야 한다. 강력한 데이터 파이프라인을 구축하고 데이터 자산을 데이터 레이크나 패브릭 구조로 중앙화하면 에이전트의 데이터 접근성과 분석 속도를 획기적으로 높일 수 있다. 또한 데이터 생성부터 변경까지의 흐름을 추적하는 데이터 리니지(Data Lineage)는 데이터 무결성을 보장하고, 에이전트 의사결정의 투명성을 제고하는 핵심 요소다. AI 에이전트의 수가 증가함에 따라, 각 에이전트의 소유자, 역할과 업무 범위, 사용 데이터 세트, 재무적·운영적 리스크 노출 한도 등을 아우르는 포괄적이고 최신화된 '에이전트 레지스트리'(Registry)를 유지해야 한다. 이는 에이전트의 활동을 투명하게 파악하고, 리스크 통제력을 강화하며, 운영 과정 전반에 대한 책임성을 높이는 데 핵심적인 도구가 될 것이다.

에이전트 레지스트리로 운영 책임성 확보

에이전트의 조율과 실행을 원활하게 하기 위해서는 인간–AI 협업 문화를 정착시켜야 한다. 에이전틱 AI로의 전환은 기술적 변화 그 이상을 요구하며, 전통적 AI나 LLM 도입보다 훨씬 큰 폭의 문화적 전환을 요구한다. 인간이 과업 실행의 중심이었던 기존 모델에서 벗어나, AI 에이전트가 주요 실행 역할을 담당하고 인간은 감독·가이드·개입 역할을 수행하는 새로운 패러다임에 적응해야 한다(그림 6 참조). 특히 AI 활용 역량과 교육에 대한 투자는 조직의 신뢰를 구축하고 에이전트 AI의 원활한 도입을 촉진하며, 인간–에이전트 간 효과적인 협업 기반을 강화한다.

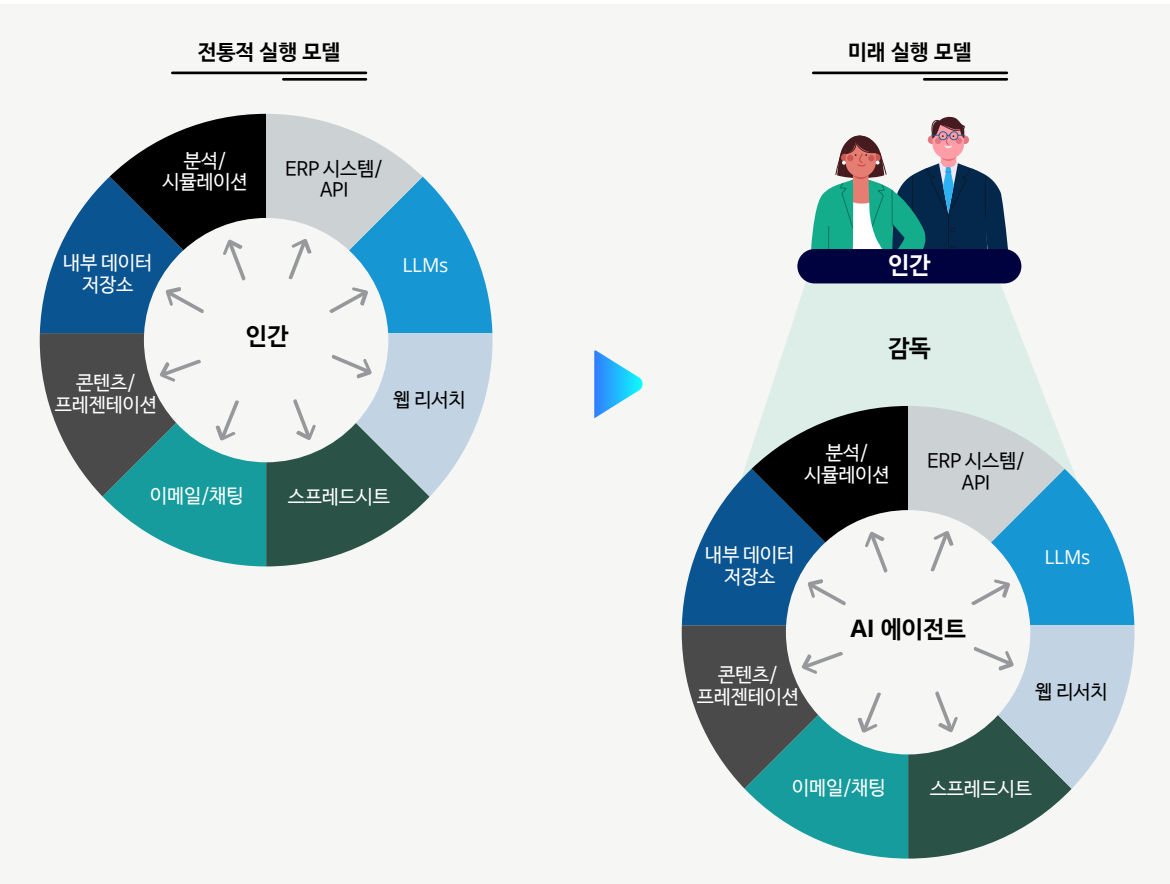
인간–에이전트 협업 모델로 전환

책임성을 강화하기 위해서는 인간의 개입이 반드시 유지되어야 한다. 에이전틱 AI는 자율성을 크게 높일 수 있지만, 은행은 주요 의사결정 지점에 인간을 배치함으로써 책임 소재를 명확히 하고, 리스크를 통제하며, 조직의 회복탄력성을 확보해야 한다. 인간 개입은 에이전틱 AI 프로세스의 속도를 늦출 수 있으나, 규제·윤리·운영상의 제약을 고려할 때 완전 자동화는 아직 현실적인 선택지가 아니며, 따라서 인간의 감독과 판단은 필수적이다.

에이전틱 운영 모델에 맞춘 조직·의사결정 구조 전환

에이전틱 AI를 조직에 성공적으로 내재화하기 위해서는 단순한 기술 구현을 넘어, 조직의 준비태세 전반을 아우르는 선제적 변화 관리가 필수적이다. 리더는 AI 도입의 가치를 명확히 전달하고, 전환 과정을 체계적으로 관리하며, 조직 문화와 업무 방식을 에이전틱 AI 운영 모델에 맞게 지속적으로 정렬해야 한다. 이는 전통적인 변화 관리의 범위를 넘어, 경우에 따라 조직 구조의 재편을 요구할 수 있다. 에이전틱 AI가 실행의 중심으로 이동할수록 정보 흐름, 의사결정 권한, 통제 구조 역시 함께 재설계되어야 한다. 기존의 위계적 의사결정 체계는 보다 수평적이고 민첩한 조직으로 진화해야 하며, 이를 통해 부서 간 팀이 AI 기반 인사이트를 공유하고 보다 직접적으로 협업할 수 있는 환경이 구축된다.

그림 6. 은행의 새로운 운영 모델: 인간 중심에서 AI 에이전트 중심으로 이동



참고: ERP (Enterprise Resource Planning) – 전사적 자원관리 시스템, API(Application Programming Interface)–시스템 간 연계 인터페이스, LLM (Large Language Model) – 대규모 언어 모델

출처: 딜로이트 컨설팅

결론: 에이전틱 AI 기반 은행으로의 전환의 경로

많은 은행은 이미 에이전틱 AI를 성공적으로 전개하기 위한 '플레이북'을 보유하고 있다. 특히 높은 RPA 도입률과 자동화 경험을 축적해 온 한국 금융권에게 에이전틱 AI는 낯선 기술이 아니다. 오히려 지난 수년간 구축해 온 프로세스 자동화, 데이터 인프라, 운영 통제 체계는 에이전틱 AI를 본격적으로 확장할 수 있는 가장 강력한 토대다. 단기적으로 은행은 본 보고서에서 제시한 세 가지 접근법 중 각자의 레거시 환경과 전략적 우선순위에 맞는 경로를 선택해, 즉각적인 가치 창출이 가능한 영역부터 확장하는 것이 현실적인 출발점이 될 것이다.

이 전환을 가속하는 구조적 요인도 나타나고 있다. 최근 금융당국의 망분리 규제 완화와 SaaS 활용 범위 확대는, 그동안 내부망에 묶여 있던 데이터와 업무를 클라우드·외부 AI 생태계와 연결할 수 있는 제도적 여지를 넓히고 있다. 이는 한국 은행들이 에이전틱 AI 운영 모델로 빠르게 진화할 수 있는 환경이 조성되고 있음을 의미한다.

동시에 에이전틱 AI의 확산은 새로운 책임과 통제의 문제를 동반한다. 자동화의 범위가 '보조'에서 '자율적 실행'으로 확대될수록, 판단의 근거와 책임 소재를 어떻게 관리할 것인지는 핵심 거버넌스 이슈가 된다. 개인정보보호, 금융소비자 보호, 규제 준수, 그리고 에이전트의 행위에 대한 감사 가능성은 기술 성능만큼이나 중요한 성공 조건이다. 은행은 속도와 효율성이라는 이점과 함께, 설명 가능성, 감사 로그, 인간 개입 메커니즘을 설계 단계부터 내재화해야 한다.

결국 에이전틱 AI의 도입은 단순한 기술 채택이 아니라 은행 운영 모델의 전환이다. 견고한 거버넌스와 전략적 배포 체계를 바탕으로 한다면, 에이전틱 AI는 운영 효율성과 리스크 관리, 그리고 고객 경험을 동시에 개선하는 핵심 동력이 될 수 있다. 지금은 한국 금융권이 디지털 전환을 넘어, 에이전틱 AI 기반의 지능형 운영 모델로 도약할 수 있는 중요한 전환점에 서 있다.

방법론

딜로이트는 2024년 12월부터 2025년 3월까지 미국 은행 및 서드파티 벤더의 기술·소프트웨어 엔지니어링 임원 5명, 그리고 풍부한 지식과 경험을 갖춘 다수의 딜로이트 AI 전문가를 대상으로 심층 인터뷰를 진행했다. 이 논의들은 에이전틱 AI의 현황, 은행 산업 내 잠재력, 그리고 신기술과 관련된 리스크에 초점을 맞추었다. 인터뷰를 통해 수집된 인사이트는 산업 지형에 대한 광범위한 개요를 제공했으며, 앞서 제시한 연구 결과들을 실증하는 토대가 되었다.

또한 기술 기업의 간행물과 학술 논문을 활용하여 에이전틱 AI의 가능성과 한계를 입체적으로 검증(Triangulate)했다. 이러한 질적 접근 방식은 본 보고서의 분석이 업계 리더들의 생생한 현장 경험과 전문적인 식견에 확고히 기반하고 있음을 강조한다.

주석

1. Amazon Web Services, “Amazon Bedrock Agents,” accessed June 18, 2025.
2. Sundar Pichai, Demis Hassabis, and Koray Kavukcuoglu, “Introducing Gemini 2.0: Our new AI model for the agentic era,” Google, Dec. 11, 2024.
3. Frank X. Shaw, “Microsoft Build 2025: The age of AI agents and building the open agentic web,” Microsoft, May 19, 2025.
4. Justin Boitano, “NVIDIA and partners launch agentic AI blueprints to automate work for every enterprise,” Nvidia, Jan. 6, 2025.
5. Salesforce, “Agentforce,” accessed June 18, 2025.
6. The Financial Brand(2026.1.6), Agentic AI in Banking Will Follow Three Tracks. Fintechs Lead in All of Them
7. 조선비즈(2025.3.28), 네이버클라우드, 한국은행에 '하이퍼클로바X' 기반 생성형 AI 플랫폼 제공 계약 체결
8. 방법론 참고
9. 딜로이트 내부 전문가 및 외부 AI 전문가들과의 심층 논의를 바탕으로 작성
10. 금융위원회(2024.8), 금융분야 망분리 개선 로드맵
11. Jim Rowan et al., “Now decides next: Generating a new future,” Deloitte AI Institute, January 2025.
12. Jeff Loucks et al., “Autonomous generative AI agents: Under development,” Deloitte Insights, Nov. 19, 2024.
13. Rick Merritt, “What is retrieval-augmented generation, aka RAG?” Nvidia, Jan. 31, 2025.
14. Fulcrum Digital, “AI-powered KYC orchestration: Combining LLMs and agent workflows to slash onboarding times,” May 27, 2025.
15. Salomone D and Aishwarya Prabhat, “Build a multi-agent KYC workflow in three steps using Google’s Agent Development Kit and Gemini,” Google, June 17, 2025.
16. Anthropic, “Introducing the Model Context Protocol,” Nov. 25, 2024.
17. Emmanuele Lacavalla et al., “HEnRY: A multi-agent system framework for multi-domain contexts,” arxiv (2024).
18. 금융위원회(2025.10.29), 「보이스피싱 정보공유·분석 AI 플랫폼(ASAP : 에이샙)」
19. Isabelle Bousquette, “Digital workers have arrived in banking,” The Wall Street Journal, June 30, 2025.
20. Mastercard, “Mastercard unveils Agent Pay, pioneering agentic payments technology to power commerce in the age of AI,” press release, April 29, 2025.
21. Asish Mohanty, “PayPal releases agent toolkit to accelerate commerce,” PayPal, April 14, 2025.
22. Visa, “Enabling AI agents to buy securely and seamlessly,” accessed June 18, 2025.
23. William Watson et al., “LAW: Legal agentic workflows for custody and fund services contracts,” Proceedings of the 31st International Conference on Computational Linguistics: Industry Track (Abu Dhabi, Association for Computational Linguistics, 2025), pp. 583–594.
24. Ibid.
25. 딜로이트(2025), 고객 경험을 넘어 전사적 가치로: 국내 은행의 AI Native Bank 로드맵
26. 매일경제(2025.11.10), 신영증권, 업계 최초 AI 에이전트 방식 ‘불완전판매 모니터링솔루션’ 도입
27. Ibid.
28. 딜로이트 내부 전문가 및 외부 AI 전문가들과의 심층 논의를 바탕으로 작성
29. Akka, “Agentic AI system,” accessed June 17, 2025.

30. Alex Chris, “MicroAgents: Exploring agentic architecture with microservices,” Microsoft, Jan. 22, 2024.
31. Belle Lin, “Nvidia thinks it has a better way of building AI agents,” The Wall Street Journal, April 23, 2025.
32. Ibid.
33. 딜로이트 내부 전문가 및 외부 AI 전문가들과의 심층 논의를 바탕으로 작성
34. Ibid.
35. 딜로이트(2025), 고객 경험을 넘어 전사적 가치로: 국내 은행의 AI Native Bank 로드맵
36. 전자신문(2025.7.27), KB국민은행, AI 에이전트용 데이터 플랫폼 만든다...'금융권 최초'
37. Sri Koneru, “Amazon Bedrock announces general availability of multi-agent collaboration,” Amazon Web Services, March 10, 2025.
38. Deloitte Digital, “Agent Advantage™ for Salesforce: Integrate AI agents into your teams,” accessed Aug. 1, 2025.
39. Salesforce, “Agentforce for financial services,” accessed July 21, 2025.
40. Google Agentspace, “Transform your workforce with AI agents,” accessed May 18, 2025.
41. Ibid.
42. 삼성SDS, 패브릭스 FabriX
43. LG CNS, AX 플랫폼
44. Anthropic, “Claude for financial services,” July 15, 2025.
45. Deeplearning, “Agents open the wallet,” Dec. 4, 2024.
46. Ronit Ghose, et.al., “Agentic AI: Finance & the ‘do it for me’ economy,” Citigroup, Jan. 17, 2025.
47. Ankur A. Patel, “AgentFlow vs Crew AI vs Autogen vs LangChain for building AI agents,” Substack, Feb. 27, 2025.
48. N8n, “Flexible AI workflow automation for technical teams,” accessed May 18, 2025.
49. Zapier, “The most connected AI orchestration platform,” accessed May 18, 2025.
50. Mastercard, “Mastercard unveils Agent Pay, pioneering agentic payments technology to power commerce in the age of AI,” press release, April 29, 2025.
51. ServiceNow, “ServiceNow unveils the new ServiceNow AI platform to put any AI, any agent, any model to work across the enterprise,” May 6, 2025.
52. Iason Gabriel et al., “The ethics of advanced AI assistants,” arxiv (2024).
53. Josh Clymer, et al., “The rogue replication threat model,” METR, Nov. 12, 2024.
54. Maxwell Zeff, “Skyfire lets AI agents spend your money (https://techcrunch.com/2024/08/21/skyfire-lets-ai-agents-spend-your-money/),” TechCrunch, Aug. 21, 2024.

한국 딜로이트 그룹 전문가

금융산업통합서비스 그룹

한국 딜로이트 그룹 금융산업통합서비스 그룹의 전문가들은 은행, 보험, 증권, 캐피탈, 신용카드, 자산운용 등 금융산업에 대한 축적된 다양한 업무수행 경험과 글로벌 네트워크의 최신 데이터베이스를 바탕으로 선진화된 회계감사, 세무자문, 재무자문 및 컨설팅 서비스를 제공하고 있습니다. 특히 보다 심도 있고 전문화된 서비스를 제공하기 위해 금융산업에 특화된 조직을 별도로 운영함으로써 고객의 요구에 신속하게 대응하고 있습니다.

민홍기 대표
금융산업통합서비스 그룹
02 6676 2319
homin@deloitte.com

장형수 파트너
금융산업 리더
02 6676 1168
hyuchang@deloitte.com

신병오 파트너
보험산업 리더
02 6676 1225
byoshin@deloitte.com

조태진 파트너
은행 및 자본시장 리더
02 6676 3322
tajo@deloitte.com

사업부문별 리더

공선희 파트너
회계감사 부문 리더
02 6676 1264
sgong@deloitte.com

장문보 파트너
회계감사 부문 리더
02 6676 2319
muchang@deloitte.com

김수환 파트너
경영자문 부문 리더
02 6676 2152
soohwakim@deloitte.com

이동영 파트너
경영자문 부문 리더
02 6676 2304
dongylee@deloitte.com

안상혁 파트너
컨설팅 부문 리더
02 6676 3625
anghyan@deloitte.com

김철 파트너
세무자문 부문 리더
02 6676 2931
cheolkim@deloitte.com

딜로이트 One AI

딜로이트 One AI는 회계, 세무, 경영자문, 컨설팅 등 전 사업부문의 전문가들이 모여 기업의 AI 도입을 지원하는 통합 AI 서비스 조직입니다. AI 전략 수립, 거버넌스 구축, 도메인별(산업별/업무별) AI 솔루션 개발/구현까지 전 과정을 E2E로 제공합니다. 기업은 딜로이트 One AI를 통해서 단순한 AI기술 적용을 넘어, 전사적 전환(enterprise-wide AI transformation)과 경쟁력 확보 목표를 달성할 수 있습니다.

배재민 대표
One AI 총괄 리더 | 컨설팅 부문
02 6676 3700
jaeminbae@deloitte.com

정창모 수석위원
AI Agent(생성형 AI), Data Analytics | 컨설팅 부문
02 6676 3288
changjung@deloitte.com

김진숙 파트너
AX전략, AI Governance, AI서비스 | 경영자문 부문
02 6138 5656
jessikim@deloitte.com

이승영 수석위원
Audit AI (Asset & Analytics) | 회계감사 부문
02 6676 3478
seungyounglee@deloitte.com

구현모 파트너
Tax AI (Asset & Analytics) | 세무자문 부문
02 6676 2126
hygoo@deloitte.com

조민연 파트너
Audit Digitalization | 회계감사 부문
02 6676 1990
minycho@deloitte.com

앱

Download on the App Store

GET IT ON Google Play

카카오톡 채널

'딜로이트 인사이트' 앱과 카카오톡 채널에서
경영·산업 트렌드를 만나보세요!

Deloitte. Insights

성장전략부문 대표
손재호 Partner
jaehoson@deloitte.com

딜로이트 인사이트 편집장
박경은 Director
kyungepark@deloitte.com

Contact us
krinsightsend@deloitte.com

연구원
김혜련 Senior Manager
hyerykim@deloitte.com

디자이너
박근령 Senior Consultant
keunrpark@deloitte.com