Agentic AI 시대의 지급결제 부문 대응 동향 및 시사점

권소연*

* 금융결제원 금융결제연구소 연구역(E-mail: ksy331@kftc.or.kr)

〈요약〉

Agentic AI는 사용자의 의도를 이해하고 다양한 과업을 스스로 계획 · 추론 · 실행하는 AI 시스템으로, 높은 자율성, 장기 메모리 및 도구 활용 능력을 갖춘 점이 특징이다. 특히 개별 AI Agent가 단일 · 정형 업무 수행에 한정되는 것과 달리, Agentic AI는 여러 전문화된 에이전트가 협업하여 복합적 목표를 수행할 수 있어 다양한 영역에서 생산성과 사용자 경험을 크게 개선시킬 잠재력을 지닌다.

Agentic AI 생태계의 확산을 위해서는, 에이전트 간 통신 · 협업을 가능하게 하는 표준화된 프로토콜이 필수적이다. 기존 초기 에이전트 시스템이 사일로 방식으로 운영되면서 협업이 어려웠던 문제를 해소하기 위해, Google · OpenAI · Anthropic 등 빅테크는 외부 도구 접근 방식을 표준화하는 MCP 프로토콜, 에이전트 간 과업 요청 · 소통 · 조율을 가능하게 하는 A2A 프로토콜을 제안하며 에이전트 생태계의 상호운용성을 강화하고 있다.

지급결제 부문에서도 다양한 이해관계자가 참여하여 에이전트를 새로운 거래 주체로 활용하려는 시도가 확산되고 있다. 접근 방식은 상이하지만, 에이전트 기반 지급거래의 표준화와 상용화를 위한 기술 인프라 정비라는 공통된 방향성이 확인된다.

먼저 AP2, ACP, x402 등 Agentic Commerce를 지원하기 위한 결제용 프로토콜이 등장하고 있다. AP2가 에이전트 기반 거래의 신원 검증 · 권한 부여 · 추적 가능성을 확보하는 보안 계층이라면, ACP는 기존 전자상거래 흐름을 에이전트가 이해 · 실행하도록 정형화해 별도 거래시스템 없이 기존 인프라와 연동하는 상거래 운영 계층이다. 또한 x402는 웹 요청 자체에 지급결제 기능을 내장한 실행 계층 프로토콜이라는 점에서 구별된다.

아울러 이러한 기술적 기반을 바탕으로, 주요 지급서비스 제공사들은 Agentic Commerce 환경에 대응하기 위한 지급결제 인프라 정비에 나서고 있다. 카드사는 Visa · Mastercard를 중심으로 에이전트 전용 토큰 · 인증 · 지급 규칙 등을 포함한 프레임워크를 정비하고, 핀테크 업체들은 Agent Toolkit 등을 통해 API 기반의 에이전트 지급거래 환경을 구현하고 있다. 이외에도 스테이블코인 관련사들과 인도 UPI 등 기타 기업들도 Agentic Commerce 생태계 확장에 참여하고 있다.

한편, Agentic AI 기반 지급결제서비스 확산을 위해서는 편의성과 안전성을 동시에 확보할 수 있는 소비자 보호 장치가 뒷받침되어야 한다. 본 고는 AI 신원인증 체계, 구체적 위임 권한 설정, 거래 추적 · 검증 장치 등을 주요 보호 장치로 제시한다. 또한 EU · 영국의 SCA 규제 동향과 소액 · 저위험 거래에 대한 SCA 면제 · 완화 사례를 검토하여, Agentic AI 환경에서도 거래 위험도와 맥락에 따라 인증 강도를 차등화하는 인증체계의 도입이 고려되어야 한다는 점을 제시해본다.

〈설명회 자료〉

1. 들어가며

요청: "내일 저녁에 집 근처에서 영화 주토피아2를 보고 싶다 "

1. 사용자 빈 시간 파악(구글캘린더)
2. 극장 정보 수집(영화예매플랫폼)
3. 집-극장 이동거리, 소요 시간 비교
→ 가장 적합한 **상영관 우선 추천**
4. 맞춤형 **좌석 제안**(과거예매내역)
5. 상영관, 시간, 좌석 최종 선택 시
예매, 결제 자동 완료
6. 극장까지의 최적 이동 경로 안내

기존의 LLM이 정보 제공 중심이었다면, Agentic AI는
실행 및 자동화가 핵심이며, 개인에게 **최적화된 서비스** 제공
→ 다양한 영역에서 생산성 향상, 서비스 경험 개선 가져올 잠재력 有

Agentic AI가 실생활에 자리잡기 위한 조건: 1. 편의성, 2. 안전성

1. 편의성

사용자는 Agentic AI가 제공하는
자동화, 맞춤형 최적화를 통해
에이전트 사용 경험에서 **체감 가능한 효용**을 얻어야 함

편의성 제공 + 보호장치 마련) 균형 필요

2. 안전성

권한을 위임 받은 에이전트가 오작동을 일으키거나
외부 공격에 노출될 경우, 금전적 손실, 개인정보 유출 등
직접적인 피해를 입을 위험 존재

금융결제원 조사연구설명회 자료(2025.12.)

1

2. Agentic AI 개요

가. 개념 및 특징

Agentic AI

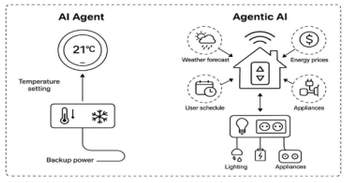
① **(Task Oriented)** 사용자를 대신하여 목표를 추구하고
② **(Autonomous reasoning)** 자율적 의사결정을 내리고
③ **(Action Taking)** 실제 과업을 실행하는 지능형 소프트웨어

<기존 LLM과 Agentic AI 비교>

LLM	Agentic AI
특징: 수동성	**특징: 자율성**
• 명시적 지시가 없는 한 스스로 행위를 개시하지 못함 • 대화 종료 이후에는 상태를 기억하지 못함 • 반응적 시스템	• 사용자가 과업을 일일이 지시·지속적인 개입할 필요 없음 • 대화 종료 후에도 상태 기억 • AI가 사용자의 필요 사항을 선제적으로 감지·행동

AI의 역할이 **지원 → 실행**으로 전환되는 변곡점

AI Agent와 Agentic AI의 비교



AI Agent	• 특정 임무를 수행하도록 설계된 개별 전문가형 시스템 • 특정 작업 단위 내에서 높은 수준의 자율성을 발휘하나, 주로 **단일 작업에 한정**(예: 이메일 필터링 등)
Agentic AI	• **다수의 전문화된 Agent들이 협력**해 복잡한 목표 달성 • 에이전트 간 정보 공유·협업·조율을 통해 업무 진행 • 단순한 합을 넘어서는 창발적 집단 지성 구현

금융결제원 조사연구설명회 자료(2025.12.)

2

2. Agentic AI 개요

나. 주요 에이전트 프로토콜

Agent Protocol

- 초기 에이전트 프로젝트는 **사일로(silo) 방식으로 운영**되어 에이전트 간 도구·메모리 공유하는 Agentic AI 구현 어려웠음
  ⇒ 에이전트 프로토콜 도입으로 이러한 파편화 극복
- **에이전트가 상호 간 원활히 통신**하고, 외부 도구에 접근하며, 더 넓은 생태계와의 **상호 운용성을 확보**할 수 있도록 함

MCP(Model Context Protocol)

ANTHROPIC
OpenAI

- 외부의 도구를 어디서 어떻게 찾고, 어떤 방식으로 사용할지에 대한 절차를 표준화
- AI가 어떤 도구든 빠르고 일괄된 방식으로 활용할 수 있도록 지원

  ⇒ 다양한 애플리케이션* 과의 연결이 가능

  * 협업툴, 메일 서비스, 전자상거래 플랫폼, 생활 앱 등

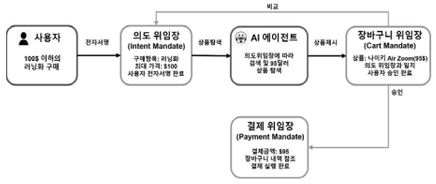
A2A(Agent-to-Agent) Protocol

- 복수의 에이전트 간 과업을 요청·보고 ·협상하는 과정에 필요한 표준화된 소통 방식
- 작업 수행을 위한 비동기적 협업 지원
- "이 일을 어떤 조건으로 언제까지 수행할 것", "작업이 완료되었으니 확인할 것 "등 상호작용 이루어짐

3. 지급결제 관련 대응 동향

가. 주요 결제용 프로토콜

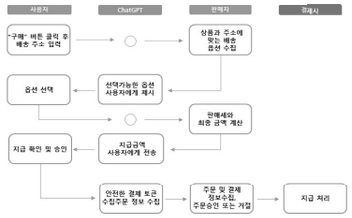
① AP2(Agent Payment Protocol)



- 2025년 9월 Google 주도로 공개한 결제용 프로토콜
- ① Agent에게 지급결제를 안전하게 위임하기 위한 신뢰성, ② 다양한 지급 수단 간 **상호운용성** 확보에 초점
- **디지털 위임장(Mandates)**와 **검증 가능한 자격 증명(VC)**을 적용하여 거래의 진위, 책임소재를 단계적으로 관리
- 모든 실행 과정이 추적·감사 가능, Web3 지급결제 솔루션까지 포괄 지원

② ACP(Agent Commerce Protocol)

OpenAI stripe



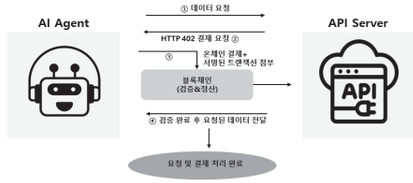
- 2025년 9월 OpenAI와 Stripe가 선보인 결제용 프로토콜
- Agentic AI가 **기존 상거래 인프라 상에서** 구매 과정 전반을 원활하게 연결하도록 하는 개방형 프로토콜
- Agentic AI에서 '상품을 어떻게 보여주고, 장바구니는 어떻게 관리하고, 주문은 어떻게 진행한다.' 식으로 **구매 과정 전반을 표준화**
- 이미 ChatGPT Instant Checkout 환경에 적용됨

3. 지급결제 부문 대응 동향

가. 주요 결제용 프로토콜

③ x402

coinbase CLOUDFLARE



- 2025년 9월 Coinbase와 Cloudflare 주도로 공개한 결제용 프로토콜
- HTTP 402와 ERC-3009 결합하여 **중개 절차 없이 사전 위임·한도에 따라** 웹 상에서 에이전트가 직접 지급거래 실행
- 온체인 스마트 계약이 **거래의 유효성을 자동 검증**하고 USDC 기반으로 즉시 정산
- 모든 거래 과정은 블록체인에 기록되므로 재사용 ·위조 ·변조 위험 없이 자동결제 가능

결제용 프로토콜 간 비교

① AP2	• **보안·컴플라이언스 계층**을 구축하는 데 중점 • 디지털 위임장(Mandates)과 검증가능한 자격증명(VC) 등을 기반으로 에이전트의 지급권한을 사전 정의하고, 자율 거래를 승인·검증하여 **신뢰성 확보에 집중**
② ACP	• 기존 전자상거래 인프라를 에이전트가 쉽게 활용할 수 있도록 표준화한 **상거래 운영 계층** • 쇼핑몰 내 일련의 **상거래 흐름**을 에이전트가 이해하고 실행할 수 있도록 절차를 정형화하고, **기존 지급수단 및 가맹점 시스템을 그대로 활용**하는 실용적인 접근 방식
③ x402	• 웹 요청(HTTP Request) 자체에 지급거래 기능을 내장하는 **실행 계층**의 **온체인 결제용** 프로토콜

3. 지급결제 부문 대응 동향

나. 카드사

Visa- Visa Intelligent Commerce ('25.4月)

[Commerce]- 소비자에게 완결된 상거래 경험을 제공할 수 있도록 하는 **全주기적(End-to-End)** 상거래 표준화 전략

① 개인화
✓ 개인별 소비 성향·선호도를 반영한 맞춤형 추천 가능

② 핵심 보안장치-토큰화, 인증
✓ 플랫폼에 카드 등록 시 다중 보안 절차
✓ 카드번호는 고유 디지털 토큰으로 대체

주체	주체별역할
소비자	• 본인의카드 정보를 Intelligence Commerce 플랫폼에 등록 • AI Agent 승인 및 등록을 통해 쇼핑·결제 자동화 위임 • AI Agent 사용관리 (지급 한도, 결제가능 상점, 거래승인 조건 등)
AI Agent 제공사	• Visa Intelligence Commerce API 및 개발자 도구를 활용한 AI Agent 개발· 등록 • Visa Intelligence Commerce 플랫폼에서 토큰화된 결제VC를 받고 소비자 대리 결제 수행
가맹점	• Visa Intelligence Commerce를 통한 AI Agent와의 결제를 수용
Visa	• 보안 인증 거래 모니터링 분쟁처리 지원

<Visa Intelligent Commerce 화면 예시 >

3. 지급결제 부문 대응 동향

나. 카드사

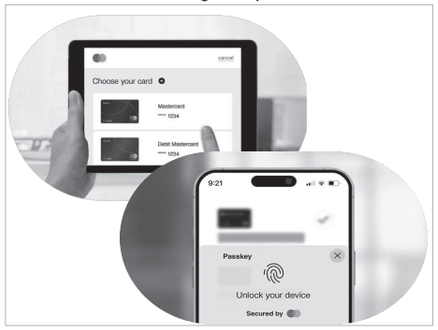
Mastercard- Mastercard Agent Pay ('25.4月)

[Pay]- 지급결제 단계에만 초점, **거래 요청이 발생한 이후의 과정**을 안전하고 효율적으로 수행하는 데 주력

핵심 기술 **Agentic Token**

- 에이전트가 수행하는 모든 거래 요청을 사전 정의된 규칙, 권한으로 추적할 수 있도록 설계된 자격 증명(VC)
- 해당 토큰을 통해 Agentic AI는 **원시 카드 데이터를 노출하지 않고** 안전하게 거래 가능
- 소비자는 **에이전트의 권한 범위를 설정** 가능
  (ex: "매주 일정 금액까지 식료품 주문" 등)
  ⇒ 에이전트의 활동에 대한 통제권 유지

<Mastercard Agent Pay 화면 예시 >



3. 지급결제 부문 대응 동향

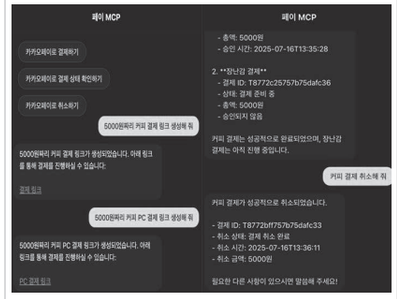
다. 핀테크·빅테크

Stripe·Paypal·Ant·카카오페이

MCP Agent Toolkit 등을 통해 에이전트 결제 환경 구현

Stripe	• 2024년 11월 **Agent Toolkit** 출시 • Stripe Issuing: 일회용 가상 신용카드 번호를 즉시 발급받아 안전하게 거래 처리 • OpenAI와 **ACP 공개**
Paypal	• 2025년 4월 **MCP 서버, Agent Toolkit** 공개 • Perplexity에 Agent Toolkit 적용 • KiteAI 투자: **PYUSD Agentic Commerce에 연계 방안** 모색
Ant	• **MCP 기반** 통합 지급결제 플랫폼 구축 : 자연어 대화 중 결제 실행, 환불 요청 등 직접 수행 가능 • AP2 프로토콜 개발 참여 중
카카오페이	• 자연어로 AI Agent와 지급결제 시스템이 연동될 수 있는 '페이아이(PayAI)'공개 • 2025년 8월 **MCP Agent Toolkit** 발표

<Mastercard Agent Pay 화면 예시 >



3. 지급결제 부문 대응 동향

다. 기타

스테이블코인 관련 기업 및 인도 UPI

[스테이블코인 관련 기업]

스테이블코인

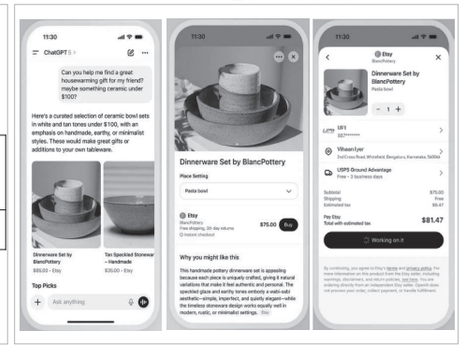
① 가격 변동이 낮아 **가치 안정성**이 높음
② 국경·시간의 제약 없이 **24시간 거래** 가능
③ 스마트 계약과 연동되어 **반복·조건부 지급 자동화** 가능
⇒ Agentic Commerce의 주요 지급수단으로 발전할 가능성 높음

Circle	• OOAK(Object-Oriented Agent Kit) 공개 - Agentic AI가 지갑 생성·키 보안·서명 등 민감한 금융 작업을 안전하게 수행하도록 하는 에이전트 프레임워크 • MCP 기반 수탁형 지갑(Circle Wallet) 제공
Coinbase	• Payment MCP 지원 • X402 Foundation 출범

[인도 UPI]

UPI	• 인도 중앙은행(RBI), 지급결제시스템 운영기관(NPCI)이 OpenAI와 **협력하여 ChatGPT 내 UPI 결제 직접 수행**할 수 있는 기능 테스트 중

<ChatGPT 내 UPI 결제 프로세스(예상)>



4. Agentic Commerce에서의 소비자 보호

에이전트 기반 결제의 제약: "인간이 직접 결제한다"는 가정하에 설계된 기존 인프라

① **(보안·인증 측면)** 기존 결제 시스템은 비인가 자동화를 차단하기 위해 다중 보안 절차(CAPTCHA, 2단계 인증, 안심 결제 등) 적용
⇒ 과거 자동화 시도의 대부분과 연계된 악성 봇을 막기 위한 조치이나, 정작 합법적인 에이전트 결제에도 제약요소로 작용
② **(신원·책임소재 측면)** 현행 제도 하에서 에이전트는 결제 시 대리인이나 법적 주체로 인정되지 않음
⇒ Agentic AI 기반 결제에 문제가 생겨도 해당 문제가 사용자의 지시 오류인지, 에이전트의 오작동인지, 판매자의 과실인지 구분이 어려움
* `25.11월 Amazon, Perplexity 소송제기

소비자 보호 장치

1. 구체적 위임 권한 설정

에이전트가 자율적으로 행사할 수 있는 권한 범위를 명확히 규정하여 의도치 않은 결제를 방지하는 것이 필수적

- (Programmable Limit) 에이전트에게 특정 금액, 가맹점, 업종, 시간대에 **한정된 거래만 수행하도록** 프로그래밍
  - 초기에는 소액·저위험 거래만 허용하고, 이후 안정적으로 운영되면 신뢰 수준에 따라 점차 한도를 확대하는 방식으로 **점진적 조정** 가능
- (Virtual Credit Cards) API 기반으로 **특정 한도가 부여된 가상 카드를 발급**하여 거래 단위별로 권한 분리하여 관리
- 현재 Stripe 등에서 **개념 검증** 단계

2. 거래 추적·검증 장치

에이전트의 결제 실행 과정과 그 근거를 설명할 수 있는 기록으로 남기고, 감사 추적을 체계적으로 기록·관리

- 해당 기록들을 **대시보드 형태의 모니터링 시스템**을 통해 사용자, 관련기관이 실시간으로 확인할 수 있어야 함
- 대시보드는 단순한 거래 내역 모니터링을 넘어 잔여 예산, 승인 상태 등을 종합적으로 표시하며,**분쟁 발생 시 원인 규명·책임 소재 확인 근거**로 활용
- 현재 Skyfire 등에서 **실행 초기** 단계

4. Agentic Commerce에서의 소비자 보호

소비자 보호 장치

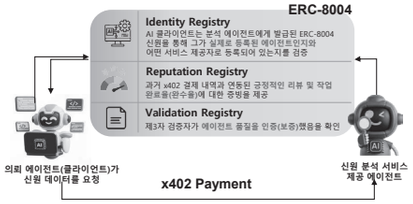
3. AI 신원인증

[KYA(Know Your Agent)]

<KYA 작동방법 예시>

- 기존 레거시 인프라의 **KYC를 보완하기** 위해 제안되는 개념
  * KYC: Know Your Customer
- ① 에이전트가 **실제 사용자에게 귀속**되는가, ② **누가** 해당 에이전트를 **개발· 배포**했는가, ③ 에이전트가 **의도한 방식으로 작동하는가**를 검증하는 절차로 설계
- 금융기관 ·지급결제 네트워크는 에이전트에게 **위 ·변조 불가능한 디지털 증명서** 부여, 거래 시 이를 제시하도록 요구
- 현재 Trulioo 등에서 **개념 검증** 단계

[ERC-8004(Ethereum Request for Comments-8004)]



- **블록체인 생태계**에서의 **AI 신원 표준**
  : 각 에이전트는 고유한 온체인 ID를 부여받아,"Agent-A, 80건 계약 이행, 성공률 96%, 고객 만족도 4.8점"과 같이 **에이전트에 대한 기록을 블록체인상에 등록**할 수 있음
- 해당 평판 기록은 블록체인에 영구 저장되므로 **위조가 불가능**
- 현재 **개념 제안** 단계

5. Agentic AI 기반 지급 시 사용자 인증

"모든 거래에 대해 강력한 인증을 의무해야 한다" VS "거래 위험도에 따라 인증 강도를 차등화해야 한다."

의견① (인증강화): 에이전트가 사용자 대신 결제를 수행하는 과정에서 발생할 수 있는 무단 결제, 의도 왜곡, 책임 불명확성 등 잠재적 리스크를 방지하기 위해, 모든 거래에 대해 일률적인 인증 절차를 적용하고 보안 수준을 강화해야 함

의견② (인증 차등화):
- 거래 금액이나 위험도가 낮은 거래까지 동일한 인증을 요구할 경우 Agentic AI의 핵심 가치인 사용자 편의성이 저하될 수 있다는 점을 지적
- 위험 기반 접근을 통해 저위험 거래에는 간소화된 인증을 적용하고 필요 시에만 강화된 인증을 수행하는 방식이 타당

가. 일반적 전자지급거래 시 사용자 인증 동향

1. EU·영국의 강력한 고객인증(SCA) 정책

[SCA(Strong Customer Authentication)]
- 「PSD2」,「PSR 2017」에 따라 도입된 사용자 인증 정책
- 모든 PSP가 전자지급거래 시 최소 2개 이상의 인증 요소를 이용해 거래자 신원을 확인하도록 의무화한 제도
- 거래리스크, 금액, 반복성, 채널 등에 따라 일정 범위에서 SCA 적용을 면제

→ 소비자 편의성을 해치지 않으면서도, 저위험 거래에 대한 인증 부담을 줄이기 위한 장치

<「PSD2」의 SCA 면제사항>

구분	관련조문	내역
지급계정정보 접근	§10	민감정보에 접근하지 않는 계정정보 조회 시 SCA 면제 허용
비접촉 POS 결제	§11	저액누적한도 내 비접촉 오프라인 결제에 대해 SCA 면제 허용
교통·주차요금 결제	§12	대중교통·주차 등 특정 저위험 결제에 대해 SCA 면제 허용
신뢰하는 수취인	§13	이용자가 사전 등록한 신뢰 수취인에 대한 결제는 SCA 면제 허용
반복 거래	§14	금액이 동일한 정기 반복결제의 후속 거래는 SCA 면제 허용
동일 지연인·법인 계좌 간 임금이체	§15	본인 또는 동일 법인의 계좌 간 내부이체는 SCA 면제 허용
소액거래	§16	단건누적 금액 조건을 충족하는 소액 전자결제에 대해 SCA 면제 허용
비소비자 대상 전용 결제 프로세스 제공 법인	§17	기업공공기관 등 특정 법인의 전용 결제 프로세스에서 SCA 면제 허용
거래리스크 분석	§18	PSP가 저위험으로 판단한 거래에 대해 위험기반으로 SCA 면제 허용

5. Agentic AI 기반 지급 시 사용자 인증

가. 일반적 전자지급거래 시 사용자 인증 동향

2. SCA 규제 동향: 거래의 성격과 위험도에 따라 인증 수준을 차등화하는 방향으로 전환

[영국]
- SCA 관련 규정을 기존 PSR(법률)에서 금융감독청(FCA) 규칙 레벨로 이관하여 신속하고 유연하게 규제를 조정

① 비접촉식 결제가 TRA(Transaction Risk Analysis)에서 저위험 거래로 식별된 경우 SCA 면제하는 위험기반 면제로 전환 제안

② AISP 접근 시 적용되던 90일 SCA 재인증 의무를 폐지하고 90일마다 고객 동의만 재확인하도록 절차를 단순화

[EU]
- 「PSD3」및「PSR」개정 논의에서 SCA 규제 일부 유연화 및 제3자 위임(delegation) 일부 포함

① **(AISP)** 기존 90일 은행(ASPSP) 재인증 → 180일 연장 → 이후 AISP의 자체 SCA 분담 수행

② **(패스스루형 디지털지갑 제공사)** 결제사와 아웃소싱 계약을 체결하고, 지갑 내 토큰화 지급수단 사용에 대한 SCA 요소검증 수행(단, 책임은 결제사 부과)

③ **(SCA 면제조항 명확화)** EBA의 해석에 기반해 면제로 운영되던 영역들을 조문화함으로써, SCA 적용 면제 조항을 명확화
(예: MIT(가맹점 개시 거래)· MOTO(우편 주문·전화 주문) 거래)

나. Agentic AI 기반 지급거래 시 사용자 인증 방향

- SCA 유연화: 규제의 목적이 보안 확보 뿐 아니라 이용자 경험과 거래 효율성까지 고려하는 방향으로 확장
- AI가 결제를 수행하는 구조에서는 모든 거래에 동일한 수준의 SCA를 적용하기 어려움
  → 거래의 위험 수준과 맥락에 따라 인증 방식·절차를 달리하는 위험도 기반 차등 인증 구조가 도입될 가능성이 높음
  ① 저위험·일상적 거래에 인증 절차 간소화, ② 최초 거래 개시 시 인증 후 일정 주기마다 동의만 재확인,
  ③ 새로운 수취인이나 고액·비정형 거래의 경우에는 강화된 인증을 요구하는 차등적 방식이 적합할 것

6. 맺으며

향후 전망 및 핵심가치

글로벌 카드사 및 핀테크 기업 등을 중심으로 Agentic AI 기반 지급 서비스 도입이 점차 확대될 것으로 예상

지급 편의성은 이용자 선택을 결정짓는 핵심 요소가 되는 반면, 권한 위임에 따른 오작동·남용 위험에 대비한 안전장치 마련 역시 중요

국내에서의 시사점

거래 처리 시점마다 별도사용자 인증을 요구하는 구조는 Agentic AI 자동화 결제 모델에서 사용자 편익을 저해하는 요소로 작용할 수 있음

① 해외에서 논의되고 있는 추가적인 소비자 보호 장치, 인증방식 차등화 관련 제도·운영 사례 주목할 필요

② Agentic Commerce 환경에서 편의성과 안전성을 균형적으로 확보할 수 있는 인증체계·소비자 보호장치 마련 필요

Ⅰ. 들어가며

A씨는 최근 개봉한 영화 주토피아2를 관람하기 위해 Agentic AI를 활용하였다. A씨가 평소에 사용하던 AI 어시스턴트에게 “내일 저녁에 집 근처에서 영화 주토피아2를 보고 싶다”라고 요청하자, Agentic AI는 먼저 그의 구글 캘린더를 확인해 빈 시간을 파악하였다.

이어서 Agentic AI는 영화 예매 플랫폼을 검색하여 해당 시간대에 주토피아2를 상영 중인 집 근처 극장 정보를 수집하였다. 이후 네이버 지도를 통해 집에서 각 극장까지의 이동 거리와 소요 시간을 비교 · 분석한 뒤, 가장 적합한 상영관을 우선 추천하였다. 또한 선택된 극장의 좌석 배치 데이터를 불러와 A씨의 과거 관람 패턴을 기반으로 맞춤형 좌석을 제안하였다. 마지막으로 A씨가 상영관과 시간, 좌석을 최종 선택하자, Agentic AI는 예매와 결제를 자동으로 완료하고, 극장까지의 최적 이동 경로를 안내하였다.

Agentic AI는 최근 산업 전반에서 가장 주목받는 키워드 중 하나로 부상하고 있다. 기존의 LLM 기반 생성형 AI가 대화와 정보 제공 중심이었던 반면, Agentic AI는 실행과 자동화를 핵심 기능으로 하여 일정 확인, 예약, 구매, 결제 등 개인에게 최적화된 맞춤형 서비스를 제공하기 때문이다. 이에 따라 의사결정 및 업무 처리 과정에 소요되던 사용자의 시간과 노력을 대폭 절감할 수 있어, 금융 · 미디어 · 이커머스 등 다양한 영역에서 생산성 향상과 서비스 경험 개선을 가져올 잠재력이 있다.

다만 Agentic AI가 우리네 실생활에 자리잡기 위해서는 두 가지 전제 조건이 필요하다. 첫째는 편의성이다. 사용자는 Agentic AI가 제공하는 자동화와 맞춤형 최적화를 통해 에이전트 사용 경험에서 체감 가능한 효용을 얻을 수 있어야 한다.

둘째는 안전성이다. 권한을 위임받은 Agentic AI가 예기치 않은 오작동을 일으키거나 외부 공격에 노출될 경우, 금전적 손실이나 개인정보 유출 등 사용자가 직접적인 피해를 입을 위험이 존재한다. 따라서 Agentic AI의 확산을 위해서는 편의성을 제공하면서도 오남용 · 위협을 방지할 수 있는 보호 장치가 함께 마련되어야 한다.

본 고에서는 Agentic AI가 수행할 수 있는 다양한 기능 중 지급결제 분야에서의 활용 동향과 그에 수반되는 소비자 보호 장치에 초점을 맞추어 살펴보고자 한다.

Ⅱ. Agentic AI 개요

1. 개념 및 특징

Agentic AI는 정보 제공 중심의 기존 AI의 단계에서 나아가, 사용자의 의도를 이해하고 실제 행동을 대리 수행하는 자율형 시스템으로 진화한 개념이다. Google, Amazon, IBM 등 글로벌 빅테크 기업들은 Agentic AI를 ① 사용자를 대신하여 목표를 추구하고(Task-oriented), ② 자율적으로 의사결정을 내리며(Autonomous reasoning), ③ 실제 과업을 실행하는(Action-taking) 지능형 소프트웨어로 정의한다.

Agentic AI의 등장은 곧 AI의 역할이 ‘지원(Support)’에서 ‘실행(Execution)’으로 전환되는 변곡점이었다. AI가 단순한 보조 기능을 넘어, 사용자의 일정을 자동으로 예약하고, 필요한 물품을 구매하며, 데이터 관리 업무까지 선제적으로 수행하는 수준으로 발전하고 있다.

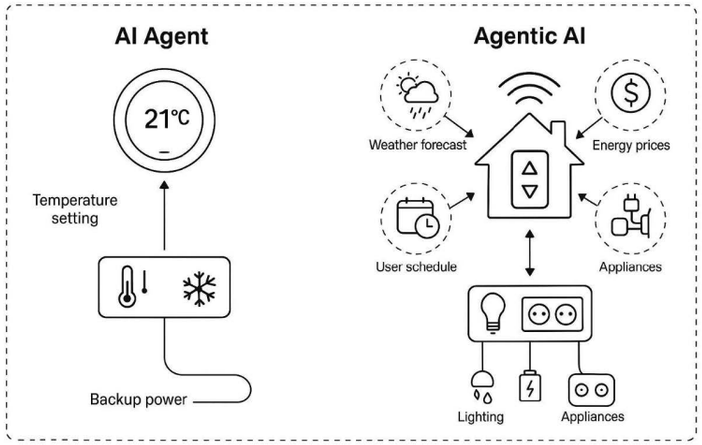
AI Agent와 Agentic AI는 업계에서 두 용어를 혼용하는 경우가 있으나, 실제로는 규모와 구조 측면에서 본질적인 차이를 가진다(그림1 참고).[1)]

AI Agent는 특정 임무를 수행하도록 설계된 개별 전문가형 시스템으로, 이메일 필터링이나 데이터베이스 검색처럼 특정 범위에서 사전 정의된 반복적 과업을 처리하는 데 최적화되어 있다. 이들은 특정 작업 단위 내에서 높은 수준의 자율성을 발휘하나, 주로 단일 과업에 한정되며 학습과 추론 또한 해당 도메인 내에 국한된다.

반면, Agentic AI는 단일 에이전트의 수준을 넘어, 다수의 전문화된 에이전트들이 협력하여 복잡한 목표를 달성하는 시스템이다. 해당 체계에서는 에이전트들이 동적으로 역할을 분담하고, 공동의 메모리 및 계획 자원을 공유함으로써 단순한 합을 넘어서는 창발적 집단 지성(emergent collective intelligence)을 구현한다. Agentic AI는 다단계 · 복합적 과업을 수행할 수 있는 광범위한 자율성을 보유하며, 에이전트 간 정보 공유 · 협업 · 조율을 통해 업무를 진행한다. 학습 및 추론 또한 특정 영역을 넘어 다양한 업무와 환경에 확장되는데, 대표적인 활용 사례로는 공급망 관리, 비즈니스 프로세스 최적화, 가상 프로젝트 매니지먼트 등이 제시된다.

1) Ranjan Sapkota, AI Agents vs. Agentic AI: A Conceptual Taxonomy, Applications and Challenges, 2025. 9.

〈그림1〉 AI Agent와 Agentic AI의 비교



자료: Ranjan Sapkota, Konstantinos, AI Agents vs. Agentic AI: A Conceptual Taxonomy, Applications and Challenges, 2025. 9.

Agentic AI의 핵심적 특징은 자율성(Autonomy)이다. 사용자가 과업을 일일이 지시하거나 지속적으로 개입하지 않더라도, AI가 사용자의 필요 사항을 선제적으로 감지하고 행동하는 실행 주체로 기능한다. 교통 상황을 고려해 회의 일정을 온라인으로 전환하거나, 계좌 잔액 부족을 인지해 대체 결제 수단을 안내하는 등 사용자가 요청하기 전에 먼저 대응할 수 있다.

Agentic AI의 등장은 LLM 패러다임에 근본적 변화를 초래하는 중요한 전환점이었다. LLM은 방대한 텍스트 학습을 통해 인간 수준의 언어 생성 · 이해 능력을 갖춘 강력한 도구이나, 본질적으로 수동적 특성을 가진다. 즉, 명시적 지시가 없는 한 스스로 행위를 개시하지 못하며, 대화 종료 이후에는 상태를 기억하지 않는 반응적 시스템에 머물러 왔다(표1 참조).

〈표1〉 주요 자동화 툴 특징 비교

구분	Traditional RPA bots	고전적 AI 모델(ML, NLP 등)	LLM	Agentic AI
핵심 특징	스크립트 기반 자동화	특정 작업에 대해 훈련된 패턴 인식 모델	대규모 언어모델 + API 기반 기능 수행	계획 · 행동 · 학습 · 협업하는 에이전트
자율성 수준	매우 낮음 (지시된 작업만 실행)	낮음 (제한된 범위에서 인간 지시 수행)	중간 (문맥 · 지시에 따라 텍스트 생성 및 도구 호출)	높음 (고도의 자율성, 목표 달성 중심)
학습 · 적응력	없음	제한적 (재훈련 필요)	제한적 (미세조정 · RAG로 업데이트)	높은 적응력, 지속적 학습 및 자기 개선 가능
사용 용도	반복적 · 규칙 기반 태스크	좁은 범위의 규칙 기반 자동화	텍스트 생성, 검색, 요약, 코드 작성 등 대화 중심	복잡한 여러 단계의 업무를 수행하는 목표 기반 작업
의사결정	없음	예측 기반 기본적 의사결정	단기 · 중간 수준의 의사결정 수행	(인식-추론-행동) 루프 기반 고도의 의사결정
메모리	없음	없음	단기 메모리	장기 메모리 (지속적 맥락 유지 및 축적)
설명가능성	높음 (단순 규칙)	중간 (모델에 따라 다름)	낮음~중간	낮음 → 중간 → 높음으로 발전 중
거버넌스 필요성	기본적인 접근통제 · 보안 필요	모델 공정성 · 품질 평가 필요	데이터 보안 · 사용 정책 · 프롬프트 관리 필요	최고 수준의 거버넌스 필요 (자율적 의도, 행동 추적, 장기적 위험 관리)

자료: Prakul Sharma, How banks can supercharge intelligent automation with agentic AI, Deloitte Insights, 2025. 8.

2. 주요 에이전트 프로토콜

Agentic AI 생태계 확장을 위해 에이전트 간 통신 · 협업을 가능하게 하는 프로토콜의 필요성이 부각되고 있다.[2)]

초기 에이전트 프로젝트들은 각기 다른 API와 프레임워크를 사용하는 사일로(Silo) 방식[3)]으로 운영되었기 때문에, 에이전트 간 도구 · 메모리를 공유하는 Agentic AI를 구현하기 어려웠다. 이러한 파편화를 극복하기 위해 등장한 것이 바로 에이전트 프로토콜(Agent Protocol)이다. 이는 에이전트가 상호 간 원활히 통신하고, 외부 도구에 접근하며, 더 넓은 생태계와 상호운용성을 확보할 수 있도록 한다.

현재 AI 플랫폼 기업, 연구기관 및 오픈 커뮤니티 등 다양한 영역에서 많은 에이전트 프로토콜이 제안되고 있다. 특히 글로벌 AI 선도 기업인 Google · OpenAI · Anthropic 등이

2) IBM, What are AI agent protocols?, 2025.
3) 사일로(Silo) 방식이란 부서 · 시스템 · 에이전트 등이 서로 단절된 채 독립적으로 운영되어 정보 공유 · 협업이 차단되는 구조를 의미한다.

선보이며 업계 표준으로 자리 잡을 가능성이 높은 MCP · A2A 프로토콜을 먼저 살펴보고, Ⅲ장에서는 지급결제 영역에서 시도되는 결제용 프로토콜인 AP2, ACP, x402를 이어서 살펴보도록 한다.

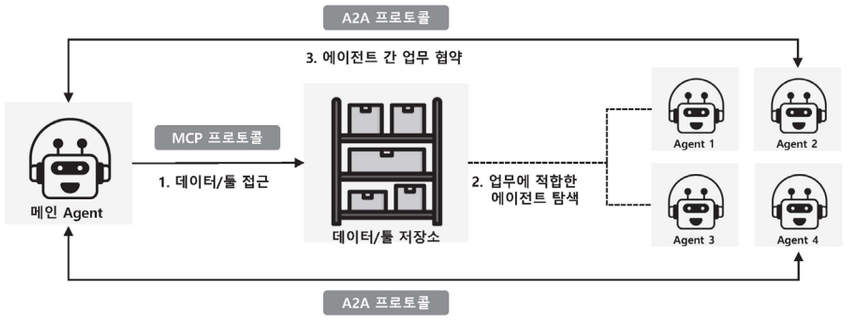
가. MCP와 A2A 프로토콜

Agentic AI가 작업을 원활히 수행하려면 다양한 도구(tool)가 필요하다. 예컨대 여행 일정을 계획할 때는 '항공권 검색 도구', '호텔 예약 도구'와 같은 기능이 요구된다. MCP(Model Context Protocol)는 이러한 외부의 도구를 어디서 어떻게 찾고, 어떤 방식으로 사용할지에 대한 절차를 표준화한 프로토콜이다. 마치 공구함을 열면 드라이버와 망치가 항상 정해진 위치에 있고 사용법도 동일한 것처럼, MCP는 AI가 어떤 도구든 빠르고 일관된 방식으로 활용할 수 있도록 지원한다. 이를 통해 다양한 애플리케이션[4]과의 연결이 가능해진다.

반면, A2A 프로토콜(Agent-to-Agent Protocol)은 복수의 에이전트들 간에 과업을 요청 · 보고 · 협상하는 과정에서 필요한 표준화된 소통 방식을 제공한다. 특히 장기적 관점에서 작업 수행을 위해 비동기적 협업[5]을 지원하는 것이 특징이다. 이를 통해 "이 일을 어떤 조건으로 언제까지 해달라", "작업이 완료되었으니 확인해달라"와 같은 상호작용이 이루어진다.

상기의 두 프로토콜은 상호 보완적인 성격을 갖는다. MCP가 에이전트와 외부 서비스 · 데이터베이스 간 연결을 담당한다면, A2A 프로토콜은 에이전트 간 협력과 조율을 가능하게 한다(그림2 참조). 예컨대 재고 관리 에이전트가 MCP를 통해 내부 데이터베이스에서 재고 부족을 감지하면, 주문 에이전트는 A2A 프로토콜을 통해 외부 공급업체 에이전트와 협력하여 자동으로 주문을 진행할 수 있다.

〈그림2〉 Agentic AI 실제 업무 수행 시 프로세스 예시



자료: 김중한, 이영진, 오동환, 최민하, 김재우, 박준규, 글로벌 AI 바이블: AI 에이전트, 플랫폼의 새로운 지배자, 삼성증권, 2025.10.

4) 애플리케이션의 예로는 구글 드라이브 · 드롭박스 같은 클라우드 저장소, 슬랙 · 노션과 같은 협업 툴, 지메일 등의 메일 서비스, 아마존 · 쿠팡과 같은 전자상거래 플랫폼, 구글 캘린더 · 네이버 지도와 같은 생활 앱 등이 있다.
5) 비동기적 협업이란 여러 에이전트가 동시에 연결되어 있지 않아도, 특정 사건이나 조건이 발생하면 순차적으로 자동 반응 · 처리하는 방식의 협업을 의미한다. 즉, 즉각적 동시 응답이 아닌 지연 · 분산된 형태로 과업을 이어가는 구조이다.

Ⅲ. 지급결제 부문 대응 동향

지급결제 부문에서는 카드사, 핀테크 등 다양한 이해관계자가 참여하여 에이전트를 새로운 거래 주체로 활용하는 시도가 확산되고 있다. 사업자별 접근 방식은 다소 상이하지만, 이들 모두 에이전트 기반 지급결제의 표준화와 상용화를 위한 기술 인프라 정비라는 공통된 방향성을 지닌다.

1. 주요 결제용 프로토콜

AP2와 ACP, 그리고 x402는 모두 에이전트 기반 상거래를 지원하기 위한 표준 프로토콜이지만, 적용 대상과 용도에서 다소 차이가 있다.

AP2(Agent Payment Protocol)는 2025년 9월 Google 주도로 글로벌 결제사들이 협력하여[6] 공개한 개방형 결제 프로토콜로, Agentic AI 기반 결제 과정에서 ① 에이전트에게 결제를 안전하게 위임하기 위한 신뢰성, ② 다양한 지급수단 간 상호운용성 확보에 초점을 둔다(그림3 참조).

AP2는 사용자의 실시간 개입 없이도 에이전트가 독립적으로 결제를 수행할 수 있도록 하기 위해 ① 권한 부여(Authorization), ② 의사 확인(Authenticity), ③ 책임 규명(Accountability)을 명확히 하는 것을 핵심 목표로 한다. 이를 위해 〈표2〉와 같이 디지털 위임장(Mandates)과 검증 가능한 자격 증명(VC, Verifiable Credentials)을 적용하여 거래의 진위와 책임소재를 단계적으로 관리하며, 모든 실행 과정이 추적 · 감사 가능하도록 표준화되어 있다.[7]

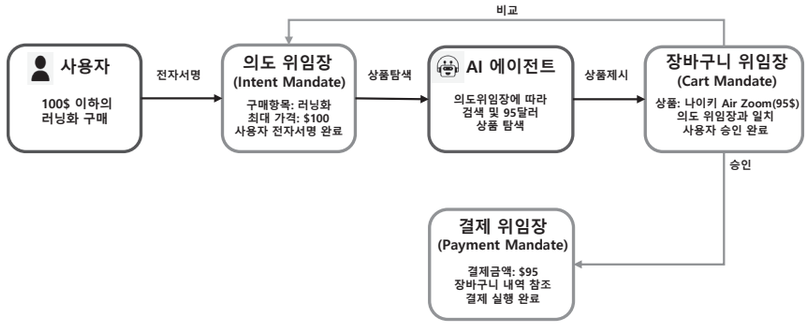
〈표2〉 디지털위임장 및 단계별 검증 가능한 자격 증명(VC)

구분	내역
Intent Mandate (1단계)	AI Agent에서 사용자의 원래 의사를 증명하는 디지털 서명장치
Cart Mandate (2단계)	AI Agent가 실제 결제를 실행하기 직전, 사용자가 장바구니(cart) 내역을 직접 확인 · 증명하였음을 증명하는 디지털 서명장치
Payment Mandate (3단계)	AI Agent가 금융기관(은행 · 카드사 등)과 연결된 유효한 지급수단을 통해 실제 결제를 집행할 권한이 있음을 증명하는 디지털 서명장치

자료: 권소연, AI Agent 결제 지원 프로토콜(AP2) 공개, 해외디지털금융브리프, 2025. 9.

6) Coinbase, Mastercard, American Express, Paypal 등 60개 이상의 기업과 협력하였다.
7) 에이전트의 구매 과정에서 누가(사용자, 에이전트, 판매자, 결제사) 무엇을 승인했는지 명확히 하고 이에 맞춰 결제가 진행된다.

〈그림3〉 Agent Payment Protocol 기반의 상거래 프로세스 예시

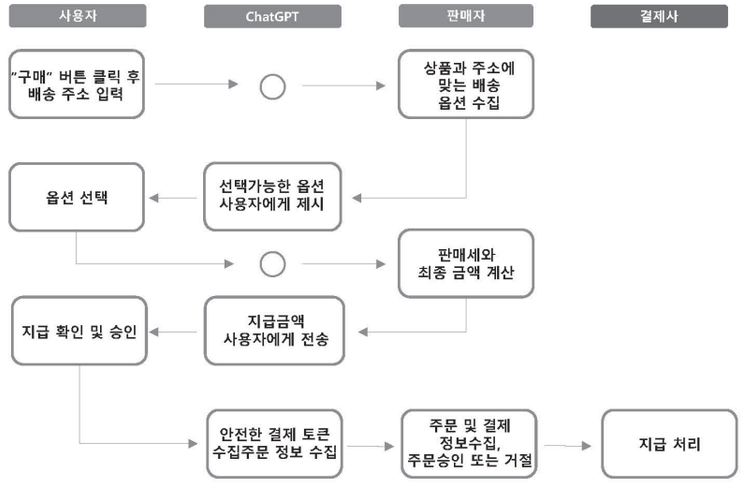


자료: Vishal Mysore, Google Agents Payment Protocol (AP2) : Deep Dive with Live Examples, OpenAI, 2025. 9.20. 재구성

또한 상호운용성을 강화하기 위해 AP2는 오픈 결제 프로토콜인 x402 프로토콜을 연계함으로써, 카드 · 계좌이체 등 기존 지급결제 솔루션 뿐만 아니라 스테이블코인 및 Web3 지급결제 솔루션까지 포괄하는 확장성을 확보하였다.

다음으로 ACP(Agentic Commerce Protocol)는 2025년 9월 OpenAI와 Stripe가 선보인 결제용 프로토콜로, Agentic AI가 기존 상거래 인프라 상에서 구매 과정 전반을 원활하게 연결하도록 하는 개방형 프로토콜이다. 즉, '상품을 어떻게 보여주고, 장바구니는 어떻게 관리하고, 주문은 어떻게 진행한다' 식으로 구매 과정 전반을 정해 놓은 매뉴얼로, 에이전트가 별도의 망을 구축하지 않고 기존 지급결제 시스템과 연계할 수 있도록 하는 데에 초점을 둔다(그림4 참조).

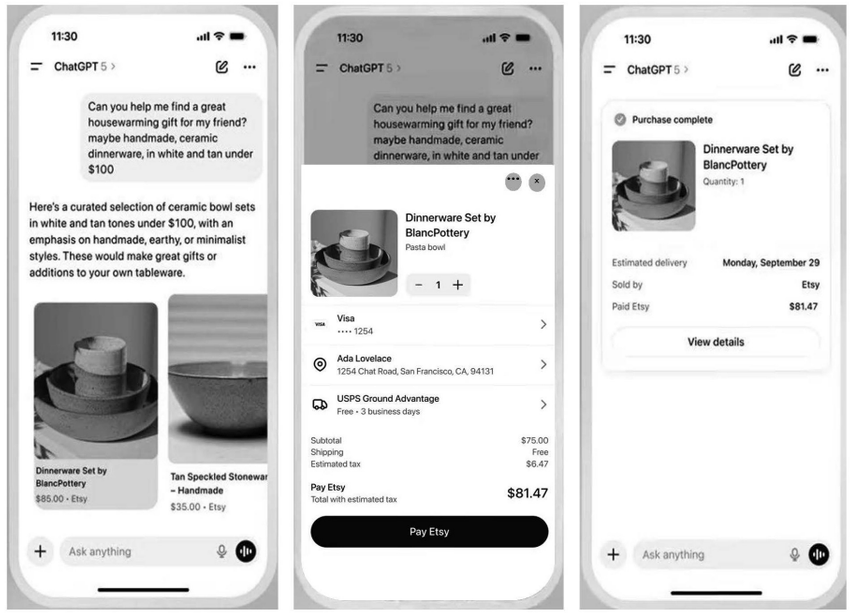
〈그림4〉 Agentic Commerce Protocol 기반 상거래 프로세스



자료: OpenAI, Buy it in ChatGPT: Instant Checkout and the Agentic Commerce Protocol", 2025. 9.30. 재구성

ACP는 이미 ChatGPT Instant Checkout 환경에 적용되어, 사용자가 별도 앱 전환이나 웹페이지 이동 없이 ChatGPT의 대화형 인터페이스 상에서 결제까지 완료할 수 있도록 지원하고 있다(그림5 참조). 이를 통해 기존 전자상거래에서 발생하던 탐색 · 입력 · 확인 과정의 마찰 비용을 줄이고, 대화형 상거래를 실질적으로 구현하는 기반이 될 수 있다.

〈그림5〉 ChatGPT Instant Checkout 실행 화면 예시



자료 : OpenAI(2025. 9.)

상기의 두 프로토콜은 AP2가 에이전트 지급결제 생태계 전반을 뒷받침할 수 있는 신뢰 및 승인 모델이라면, ACP는 지금 즉시 도입할 수 있는 상거래 운영 프로토콜이라는 점에서 구분된다.

먼저 AP2는 Google · Mastercard · Coinbase 등 광범위한 산업군 연합을 바탕으로 "보안 · 컴플라이언스 계층"을 구축하는 데 중점을 둔다. 즉, 디지털 위임장과 검증 가능한 자격 증명 등을 기반으로 AI 에이전트의 지급 권한을 사전에 정의하고 자율 거래를 승인 · 검증함으로써, 에이전트 기반 지급거래의 신뢰성을 확보하는 데 집중한다.

반면 ACP는 기존 전자상거래 인프라를 에이전트가 쉽게 활용할 수 있도록 표준화한 "상거래 운영 계층"으로, 쇼핑몰 내 상품 검색 · 비교 · 장바구니 관리 · 주문 처리와 같은 일련의 상거래 흐름을 에이전트가 이해 · 실행할 수 있도록 절차를 정형화하며, 기존 지급수단 및 가맹점 시스템을 그대로 활용하는 실용적 접근방식이라는 점에서 차별화된다.

이에 따라 개방형 지급결제 생태계 확장성과 투명성 측면에서는 AP2가 보다 근본적 기반을 제공하나, 적용 편의성과 상용화 속도 측면에서는 ACP가 상대적으로 앞서 있는 구조로, 두 프로토콜의 지향점이 분명히 구분된다.

한편 x402는 AP2와 ACP가 각각 에이전트 지급결제의 신뢰 기반과 상거래 절차를 표준화하는 프로토콜인 것과 달리, 웹 요청(HTTP Request) 자체에 결제 기능을 내장하는 "실행 계층"의 온체인 결제용 프로토콜이라는 점에서 구분된다.

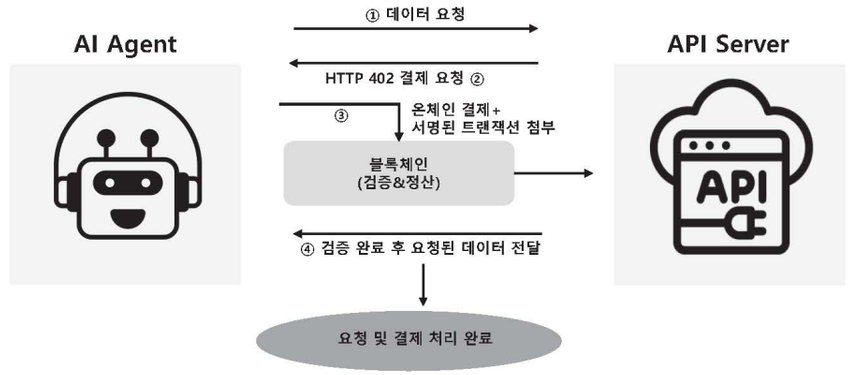
x402는 Coinbase와 Cloudflare가 2025년 9월 공식 발표한 결제용 프로토콜로, 기존의 중앙 지급결제 인프라와 달리 웹 요청(HTTP Request) 자체에 지급거래 기능을 내장하는 것을 핵심으로 한다.

기존 지급결제 시스템은 중앙 금융 중개기관의 개입이 반드시 필요하고, 사용자의 수동 인증을 통해 거래가 완료되었다. 반면 x402는 HTTP 402[8]와 ERC-3009[9]를 결합하여 이러한 중개 절차 없이, 사전 위임 · 한도에 따라 웹 상에서 에이전트가 직접 지급거래를 실행하도록 설계되었다.

x402에서는 결제 승인, 검증, 정산이 더 이상 사람이나 기관에 의해 처리되지 않는다. 대신 온체인 스마트 계약이 거래의 유효성을 자동 검증하고 USDC 기반으로 즉시 정산한다. 모든 과정은 블록체인에 기록되므로 재사용 · 위조 · 변조 위험 없이 자동결제가 가능하며, 계정 생성이나 세션 유지 없이도 API 호출 또는 콘텐츠 요청 시 즉시 비용을 지급할 수 있다.

이러한 구조는 Agent들이 사람의 개입 없이 데이터를 구매하고, 연산 자원 · API · 서비스를 임대 · 교환하며, 사용량 기반 비용을 실시간 정산하는 기계 간 경제(M2M)를 구현한다. 이는 웹의 기능이 지금까지의 "정보 검색 중심 Web 2.0"에서 "가치 이전 · 경제 활동 중심 Web 3.0"으로 확장되는 변화를 촉진하며, 향후 Web 3.0 생태계에서 Agentic Commerce의 기반으로 자리 잡을 가능성이 있다.

〈그림6〉 x402 지급결제 흐름



자료: Ekko an and Ryan Yoon, x402: Coinbase and the Beginning of the AI Agent Era, Tiger Research Reports, 2025.11. 4. 재구성

8) HTTP 402는 웹 표준 '결제 필요' 신호로, 서비스가 결제가 필요함을 알리는 표준 방식이다.
9) ERC-3009는 이더리움 계열 토큰에 적용되는 사전 서명 기반 지급 승인 규격으로, 사용자가 미리 설정한 금액 및 조건 범위 내에서는 추가 인증 없이 지급거래를 수행할 수 있도록 허용하는 표준이다.

2. 카드사

Visa와 Mastercard는 기존 카드 거래 처리 인프라를 확장하여, Agentic AI가 사용자를 대신해 거래를 수행할 수 있도록 솔루션을 공개하였다. Visa는 Intelligence Commerce를, Mastercard는 Agent Pay 솔루션을 각각 선보였는데, 서비스 명칭에서 양사의 접근 방식 차이가 엿보인다.

Visa는 에이전트가 Visa API만 연동해도 소비자에게 완결된 상거래 경험을 제공할 수 있도록 하는 全주기적(End-to-End) Agentic Commerce 표준화 전략을 중심으로 하는 반면, Mastercard는 지급 단계에만 초점을 맞추어 추천 · 탐색 과정은 Agentic AI 개발사에게 맡기고, 지급거래 요청이 발생한 이후의 과정을 안전하고 효율적으로 수행하는 데 주력하고 있다.

가. Visa

Visa는 2025년 4월 연례 행사에서 Agentic AI와 지급거래의 융합을 통한 AI 상거래 비전과 함께 "Intelligent Commerce"라는 솔루션을 공개했다. 해당 솔루션은 Agentic AI가 상품 탐색, 추천, 결제 등 상거래 전 과정을 단일 인터페이스에서 처리할 수 있도록 지원하는 표준 결제용 프레임워크이다.

Intelligent Commerce는 모든 Agentic AI가 활용 가능한 결제용 API 패키지 형태로 제공된다. 기존에는 개별 에이전트가 수많은 쇼핑몰과 각각 다른 결제용 API를 직접 연동해야 하는 복잡한 과정이 필요했으나, Visa는 이를 표준화하여 글로벌 가맹점 데이터를 단일 API로 일괄 제공하는 방식으로 단순화하였다(표3 참조).

〈표3〉 Visa Intelligent Commerce 솔루션 활용 주체별 역할

주체	주체별 역할
소비자	- 본인의 카드 정보를 Intelligence Commerce 플랫폼에 등록 - AI Agent 승인 및 등록을 통해 쇼핑 · 결제 자동화 위임 - AI Agent 사용관리 (지급 한도, 결제 기능 상정, 거래승인 조건 등)
AI Agent 제공사	- Visa Intelligence Commerce API 및 개발자 도구를 활용한 AI Agent 개발 · 등록 - Visa Intelligence Commerce 플랫폼에서 토큰화된 결제 VC를 받고 소비자 대리 결제 수행
가맹점	- Visa Intelligence Commerce를 통한 AI Agent와의 결제를 수용
Visa	- 보안 · 인증 · 거래 모니터링 · 분쟁 처리 지원

1) 개인화

Intelligent Commerce의 핵심은 소비자의 지급거래 데이터를 AI에 적용하여 개인화된 서비스를 구현하는 데 있다. 기존의 생성형 AI가 다수의 사용자 데이터 기반 추천 정도만 제공했다면, Agentic AI는 개인별 소비 성향과 선호도를 반영한 맞춤형 상거래 추천이 가능하다.

동시에 Visa는 이러한 개인화 서비스에 있어 데이터 보호와 이용자 통제권 확보를 중요한 원칙으로 제시한다. Visa는 방대한 거래 데이터를 보유하고 있으나 에이전트에게는 데이터 인사이트[10]만이 요약 · 가공된 형태로 제공되며, 사용자는 언제든 데이터 공유를 철회할 수 있다.

2) 핵심 보안장치- 토큰화, 인증

Visa는 API와 SDK 형태의 개발 도구를 통해 토큰화, 인증 등의 기능을 외부 Agentic AI가 내장할 수 있도록 지원한다. Visa는 사용자가 최초로 Visa Intelligent Commerce 플랫폼에 카드 등록 시 Visa Secure, 3D Secure, 생체 인증 등 다중 보안 절차를 포함시켜, 철저하게 본인 여부를 확인하고 등록을 승인하도록 하고 있다.

또한 등록된 16자리 카드 번호는 고유한 디지털 토큰으로 대체되는데, 해당 토큰은 사용자 거래 은행의 신원확인 후 Agentic AI 전용으로 발급된다. 발급된 토큰은 에이전트에 귀속되지만 사용자가 명시적으로 권한을 부여할 때에만 지급거래에 활용될 수 있다. 이를 통해 실제 카드 정보가 직접 노출되는 위험을 차단하면서도, Agentic AI가 사용자를 대신해 안전하게 거래를 수행할 수 있다.

지급 시점에도 추가적인 인증 절차가 반드시 요구된다. 사용자가 토큰을 Agentic AI가 사용할 수 있도록 승인하면, 에이전트는 결제 시점마다 Visa API를 통해 지문 · 얼굴 인식과 같은 생체 인증, 일명 패스키(Passkey)를 통해 인증한다. 이를 통해 무허가 결제 시도가 차단되며, 사용자의 동의 하에서만 대리 결제가 진행될 수 있다. 결국 에이전트는 사용자의 명확한 동의와 인증을 거쳐야만 Visa 카드 토큰을 활용할 수 있는 권한을 갖게 된다.

나. Mastercard

Mastercard는 2025년 4월, Agent Pay라는 AI 지급결제 인프라 솔루션을 공개하며 Agentic Commerce 경쟁에 본격적으로 참여하였다. Agent Pay는 사용자가 설정한 조건에 따라 최적의 지급 수단을 자동 선택하고, 동시에 악의적인 에이전트를 판별할 수 있도록 설계된 지급결제

10) Visa가 보유한 방대한 원시 거래 데이터를 분석해 도출된 인사이트로, 소비자의 선호 브랜드, 호텔 유형, 식사 취향 등이 해당된다. 예를 들어, "사용자는 저가형 호텔보다 부티크 호텔을 선호한다."는 수준의 요약 정보만 Agentic AI에 전달되며, 구체적 거래 내역은 노출되지 않는다.

프레임워크다.

Agent Pay의 중심에는 Agentic Token이 있다. 이는 에이전트가 수행하는 모든 거래 요청을 사전 정의된 규칙과 권한으로 추적할 수 있도록 설계된 자격 증명(VC)이다. 이 토큰을 통해 Agentic AI는 원시 카드 데이터를 노출하지 않고 안전하게 거래할 수 있으며, 소비자는 에이전트의 권한 범위를 설정할 수 있다. 예를 들어 사용자는 에이전트에게 “매주 일정 금액까지 식료품 주문”과 같은 제한적 권한을 부여할 수 있고, 고액의 재량 구매는 차단할 수 있다.

이러한 구조를 통해 사용자는 에이전트가 언제, 어디서, 어떤 조건으로 활동하는지에 대한 통제권을 유지하며, 모든 주문 · 구매 · 배송 내역은 안전하게 기록되어 분쟁 발생 시 신속한 검증이 가능하다.

Mastercard는 Agent Pay를 Citibank, US Bank 고객을 대상으로 시범적으로 제공하고 있으며, 연말까지 미국 내 모든 Mastercard 카드 소유자에게 서비스를 확대할 계획이다.

3. 핀테크 · 빅테크

Agentic AI가 상거래 전반에 확산되면서 국내외 핀테크 · 빅테크도 이에 대응한 기술 · 플랫폼 고도화를 추진하고 있다.

가. Stripe

Stripe는 2024년 11월 Agent Toolkit[11]을 출시하며, Agentic AI가 Stripe API 호출만으로 지급거래 · 송금 · 청구 · 구독 등 다양한 기능을 수행할 수 있도록 지원하고 있다. 특히 Agentic AI는 Stripe Issuing 기능을 통해 일회용 가상 신용카드 번호를 즉시 발급받아 안전하게 거래를 처리할 수 있으며, 2025년 4월부터는 이를 간단한 LLM 함수 호출만으로도 생성할 수 있게 되었다.

이후 Stripe는 2025년 9월 OpenAI와 공동으로 ACP를 공개하여, Agentic AI가 기존 상거래 인프라 상에서 구매 과정을 원활히 연결할 수 있도록 하는 개방형 결제 표준을 제시하였다. 해당 프로토콜은 Stripe의 결제 인프라를 기반으로 ChatGPT 내 “Instant Checkout” 기능에 적용되어, 앞선 〈그림5〉에서와 같이 사용자가 별도 앱 전환이나 웹페이지 이동 없이 대화형 인터페이스 내에서 결제와 주문을 즉시 완료할 수 있도록 구현하였다.

11) Agent Toolkit이란 일종의 개발자들을 위한 라이브러리로, 개발자들이 에이전트에 결제 · 송장 발행 · 환불 처리 등 다양한 결제 관련 기능을 적용할 수 있게 해주는 도구이다.

나. Paypal

PayPal은 2025년 4월 MCP 서버와 Agent Toolkit을 공개하며 Agentic Commerce 시장 참여를 본격화하였으며, 5월에는 Perplexity에 Agent Toolkit을 적용해 AI 인터페이스에서 Paypal 결제 기능을 구현하였다.

이를 통해 이용자는 Agent에 특정 상품이나 서비스의 결제를 자연어 · 음성 명령으로 요청할 수 있으며, 결제부터 영수증 · 송장 발급까지의 모든 과정이 PayPal과 Venmo를 통해 백엔드에서 자동 처리된다. 또한 PayPal은 2025년 7월 Kite AI에 대한 투자를 통해 자사 스테이블코인(PYUSD)을 Agentic Commerce와 연계할 수 있는 기반을 마련하며, 향후 Agentic Commerce 환경에서 디지털 자산 활용을 확대하는 방안을 모색하고 있다.

다. Ant International

중국 Ant Group의 글로벌 결제 · 핀테크 사업을 총괄하는 Ant International은 MCP 기반 통합 지급결제 플랫폼을 구축하였다. 해당 플랫폼은 Agentic AI가 자연어 대화 중에 결제 실행, 상태 확인, 환불 요청 등을 직접 수행할 수 있도록 설계되었으며, 대체 지급 방식(APM)[12]과 신용카드 기반 대행 결제를 모두 지원한다. 또한 Ant는 AP2 프레임워크 내 APM 기반 프로토콜 개발에 참여하고 있으며, 이를 통해 AI 지급거래의 표준화 · 토큰화 · 지급 위임 모델 고도화를 추진하고 있다.

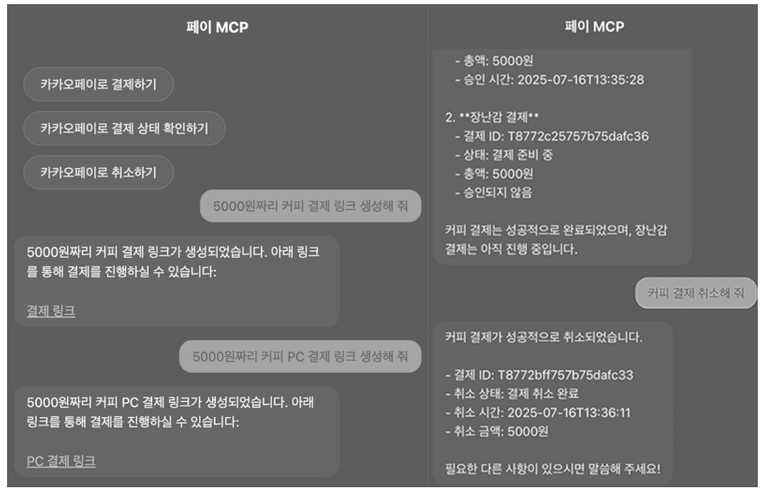
라. 카카오페이

국내에서는 카카오페이가 자연어로 AI Agent와 지급결제 시스템이 연동될 수 있는 ‘페이아이(PayAI)’를 공개하며 Agentic AI 분야에 대한 시도를 본격화하고 있다. 카카오페이는 2025년 8월 Agentic AI와 카카오페이 결제 기능 API를 연동하기 위한 MCP Agent Toolkit을 선보이고, 이를 실제로 활용하는 시연 영상을 공개했다. 해당 영상에서는 ChatGPT와 같은 LLM이 카카오페이 결제 API와 연동되어 결제 링크 생성, 결제 상태 확인, 결제 취소 등 다양한 기능을 자동화하는 과정이 시연되었다.

이번 Toolkit은 결제 준비 · 승인 요청 · 상태 조회 · 취소 처리 등 총 8개의 모듈형 Tool 기능을 제공하며, 이를 통해 개발자는 자연어 인터페이스에서 결제 기능을 호출할 수 있다.

12) 대체 지급 방식(APM, Alternative Payment Method)은 전통적인 카드 기반 결제 방식이 아닌 모든 지급수단을 통칭하는 표현이다.

〈그림 7〉 카카오페이 MCP 결제(생성 · 조회 · 취소) 화면 예시



자료: 카카오페이, AI 에이전트와 카카오페이 결제 오픈 API 연동하기: MCP Agent Toolkit 개발기, 2025. 8. 6.

카카오페이의 경우 현시점에서는 결제 링크 생성 · 상태 확인 · 취소 요청 등 결제 보조 기능을 중심으로 제공하고 있으나, 향후에는 최종 결제 실행까지 자율적으로 수행하는 Agentic AI 형태로 고도화될 가능성이 높을 것으로 전망된다.

4. 기타

가. 스테이블코인 관련 기업

스테이블코인은 ① 가격 변동이 적어 가치 안정성이 높고, ② 국경과 시간의 제약 없이 24시간 거래가 가능하며, ③ 스마트 계약과 연동되어 반복적 · 조건부 지급거래를 자동화할 수 있다는 장점을 지닌다. 이러한 특성은 에이전트 간 API 호출, 데이터 접근, 서비스 이용 등이 실시간으로 이루어지며 소액 거래가 빈번히 발생하는 환경에서 특히 유용하다. 이처럼 스테이블코인은 향후 Agentic AI 상거래의 주요 지급수단으로 발전할 가능성이 높은 만큼, 관련 기업의 행보와 기술 동향에 주목할 필요가 있다.

Circle은 2025년 1월 Agentic AI가 지갑 생성 · 키 보안 · 서명 등 민감한 금융 작업을 안전하게 수행할 수 있도록 하는 에이전트 실행 프레임워크인 OOAK(Object-Oriented Agent Kit)를 공개하였다. 또한 MCP 기반 멀티체인 수탁형[13] 지갑(Circle Wallet)을 제공하여 에이전트가 자금을 직접 충전 · 보관 · 지급할 수 있도록 하였으며, Crossmint와의 협력을 통해 AI가 독립적으로 거래를 수행할 수 있는 스테이블코인 지급결제 솔루션을 제공하고 있다.

Coinbase는 Payments MCP를 통해 LLM이 API 키 없이도 자연어를 활용하여 지갑 생성, 온램프[14], 스테이블코인 결제를 실행할 수 있도록 지원하였다. 또한 Cloudflare[15]와 공동으로 x402 Foundation을 출범하여, 기존에 사실상 사용하지 않던 HTTP 402 상태 코드를 부활시키고 웹 요청 자체에 결제 기능을 내장하였다.[16]

나. 인도 UPI

인도에서는 중앙은행(RBI)과 지급결제시스템 운영기관(NPCI)[17]이 Razorpay[18], OpenAI와 협력하여 ChatGPT 내에서 UPI[19] 결제를 직접 수행할 수 있는 기능을 테스트 중이다. 이는 국가 지급결제인프라 차원에서 Agentic AI 기반 지급서비스 실증을 추진하는 첫 사례로, 향후 상용화를 목표로 하고 있다.

13) 복수 블록체인 네트워크를 단일 지갑에서 동시에 지원하고(멀티체인), 사용자가 직접 개인 키를 관리하지 않고, 지갑 서비스 제공자가 대신 관리해주는(수탁형) 지갑이다.
14) 법정화폐(예: 원화 · 달러)를 디지털 자산(코인, 스테이블코인 등)으로 전환하는 것을 의미한다.
15) Cloudflare는 웹 인프라 제공업체로, x402를 웹 규모에서 지연을 최소화하여 안정적으로 처리하기 위한 글로벌 네트워크 인프라를, Coinbase는 결제 및 보안 프로토콜 설계를 담당한다.
16) 이 경우 결제 과정이 별도의 결제 페이지로 분리되지 않고, HTTP 요청 내부에 통합되기 때문에, 결제가 웹 요청 단계 속에 자연스럽게 녹아들게 된다.
17) NPCI(National Payment Corporation of India)는 인도 내 소액 지급결제시스템을 구축 · 운영하는 기관으로, UPI, IMPS 등 A2A(Account-to-Account) 기반 지급결제 인프라를 운영한다.
18) Razorpay는 인도의 핀테크 기업으로, 온라인 PG, 카드, UPI, A2A결제 등을 제공하는 종합 지급 서비스 사업자이다.
19) UPI(Unified Payments Interface)는 NPCI가 구축한 인도 국가 표준 계좌 기반 지급결제 인프라로, 은행 간 실시간 송금 · 결제를 단일 인터페이스에서 처리하도록 한 실시간 결제 시스템이다.

Ⅳ. Agentic Commerce에서의 소비자 보호

Ⅲ장에서 살펴본 바와 같이 국내외 많은 기업들을 중심으로 Agentic AI의 활용 영역이 상거래 및 결제까지 확장되고 있다. 그러나 이러한 시도가 본격적으로 확산되어 지속가능한 Agentic Commerce 생태계가 조성되기 위해서는 현행 지급결제 인프라의 제약 요인 및 이에 대한 해소 방안을 고민할 필요가 있다.

1. 주요 이슈

Agentic AI 기반 지급거래의 제약은 기존 지급결제 인프라가 "인간이 직접 결제한다."는 전제를 기반으로 설계되어 있다는 점에서 비롯된다.

우선 보안 · 인증 측면에서, 기존 지급결제 시스템은 비인가 자동화를 차단하기 위해 CAPTCHA, 2단계 인증, 안심 결제 등 다중 보안 절차를 적용하고 있다. 이는 과거 자동화 시도의 대부분이 악성 봇(bot)과 연계되어 있었기 때문이지만, 에이전트의 자동화 · 대리 결제에는 상당한 제약요소로 작용한다.

또한 신원 및 책임소재 측면에서도 제약이 존재한다. 현행 제도 하에서 에이전트는 지급거래 시 일종의 대리인으로, 법적 주체로서 인정되지 않는다. 이로 인해 Agentic AI가 잘못된 품목을 주문하거나 배송 오류가 발생할 경우, 해당 문제가 사용자의 지시 오류인지, 에이전트의 오작동인지, 아니면 판매자의 과실인지를 구분하기 어려운 상황이 발생한다.

결국 보안 · 인증 장치와 신원 · 책임 체계 모두가 사람의 별도 행위를 기준으로 설계되어 있어, 에이전트 기반 자동화 결제가 확산되기에는 제약이 존재한다.

따라서 Agentic AI 기반 지급거래의 확산을 위해서는 신뢰성과 안전성 측면에서의 보완이 필요하다. ① 해당 에이전트가 합법적으로 승인된 주체임을 확인할 수 있어야 하고, ② 사용자가 거래 품목 · 판매자 · 금액 등 구체적인 권한을 명확하게 위임해야 하며, ③ 거래 과정에서 문제가 발생할 경우 원인을 추적 · 검증할 수 있는 장치가 마련되어야 한다.

2. 소비자 보호 장치

가. AI 신원인증

AI 신원인증은 금융기관과 가맹점이 해당 에이전트가 합법적으로 승인된 주체임을 검증하는 것을 말한다. 이를 통해 신뢰할 수 있는 에이전트의 지급거래만이 처리되도록 하여, 무분별한 자동화나 악의적 봇(bot)에 의한 거래를 효과적으로 차단할 수 있다.

1) KYA(Know Your Agent)

기존 레거시 지급결제 인프라는 KYC(Know Your Customer)를 중심으로 하는 비밀번호, 생체인식 등 사용자의 신원 확인에 기반한다. 그러나 Agentic Commerce 환경에서는 거래의 실행 주체가 '사용자 본인'이 아닌 '에이전트'가 됨에 따라, 기존의 사용자 인증만으로는 거래의 정당성을 보증하기 어렵다는 한계가 드러난다. 별도의 검증 체계가 없을 경우, 악의적 행위자가 합법적 에이전트를 사칭하거나, 권한을 부여받지 않은 에이전트가 무단으로 지급거래를 개시하는 위험이 존재한다.

이를 보완하기 위해 제안되는 개념이 KYA(Know Your Agent)이다(그림8 참조). KYA는 "① 에이전트가 실제 사용자에게 귀속되는가, ② 누가 해당 에이전트를 개발 · 배포했는가, ③ 에이전트가 의도된 방식으로 작동하는가"를 검증하는 절차로 설계된다.

KYA의 일례로서 금융기관 또는 지급결제 네트워크는 에이전트에게 위 · 변조가 불가능한 디지털 증명서를 부여하고, 거래 시 이를 제시하도록 요구할 수 있다. 해당 증명서는 VC(Verifiable Credential)[20] 프레임워크를 기반으로 발급 · 갱신 · 폐기될 수 있으며, 사용자 동의 변경이나 기업 리스크 점수 변화 등이 발생할 경우 실시간으로 반영된다.

일부 연구에서는 에이전트의 신뢰도를 정량화한 소프트웨어 신용점수(Software Credit Score) 개념이 논의되고 있는데, 이는 가맹점이 에이전트의 신용점수에 따라 자동 승인 · 조건부 승인 · 거절을 선택할 수 있도록 한다. 이러한 KYA 체계를 통해 가맹점과 금융기관은 검증된 에이전트가 수행하는 지급결제를 신뢰 가능한 거래로 식별하여 처리할 수 있으며, 비인가 자동화나 악의적 봇에 의한 거래를 효과적으로 차단할 수 있다.

〈그림8〉 KYA 작동방식 예시

자료: Trulioo, Know Your Agent(KYA): An Identity Framework for Trusted Agentic Commerce, 2025. 7.

20) 검증 가능한 자격 증명(Verifiable Credential, VC)은 디지털 환경에서 신원, 권한, 자격 등을 안전하고 위 · 변조 불가능하게 증명할 수 있도록 만든 표준화된 디지털 증명서이다.

2) ERC-8004 (Ethereum Request for Comments-8004)

KYA가 기존 금융기관 중심의 AI 신원인증 체계라면, ERC-8004는 2025년 8월 이더리움 재단의 AI팀이 제안한 블록체인 생태계에서의 AI 신원 표준이다. ERC-8004는 일종의 AI Agent의 주민등록증 역할을 한다. 각 에이전트는 고유한 온체인 ID를 부여받아, "나는 AI Agent-A다."와 같이 자신의 존재를 블록체인 상에 등록할 수 있다.

블록체인 위에는 "Agent-A, 80건 계약 이행, 성공률 96%, 고객 만족도 4.8점"처럼, 해당 AI가 과거 계약을 얼마나 잘 이행했는지에 대한 평판 기록이 투명하게 쌓인다. 이 평판 기록은 블록체인에 영구 저장되므로 위조가 불가능하다. 따라서 다른 에이전트나 일반 사용자는 해당 기록을 근거로 "해당 에이전트는 신뢰할 수 있다."라고 판단할 수 있다. 현재 상용화 초기 단계인 ERC-8004는 퍼블릭 블록체인 상에서 글로벌 상호운용성을 보장하며, 탈중앙화 시스템의 신뢰 기반 역할을 수행할 것으로 평가된다.

나. 구체적 위임 권한 설정

Agentic AI 기반 지급거래에서는 에이전트가 자율적으로 행사할 수 있는 권한의 범위를 명확히 규정하여 의도치 않은 결제 행위를 방지하는 것이 필수적이다.[21]

대표적으로 에이전트에 특정 금액, 가맹점, 업종, 시간대에 한정된 거래만 수행하도록 프로그래밍(Programmable Limits)할 수 있다. 초기에는 소액 · 저위험 거래만 허용하고, 이후 일정 기간 안정적으로 운영되면 신뢰 수준에 따라 점차 한도를 확대하는 방식으로 점진적 조정이 가능하다.

또한 가상 신용카드(Virtual Credit Cards, VCCs)를 활용하면, 사용자는 API 기반으로 특정 한도가 부여된 가상카드를 발급하여 거래 단위별로 권한을 분리하여 관리할 수 있다. VCC는 일회성 · 특정 판매자 대상 · 소액 전용 등 다양한 조건을 부여하여 거래 단위별로 권한을 세분화할 수 있으며, 탈취나 오남용 발생 시 즉시 폐기할 수 있다는 장점이 있다.[22]

다. 거래 추적 · 검증 장치

Agentic AI 기반 상거래 결제가 신뢰성을 확보하기 위해서는 투명성(transparency)과 감사 가능성(accountability)이 전제되어야 한다. 이를 위해 에이전트는 지급 실행 과정과 그 근거를 설명할 수 있는 기록으로 남기고, 동시에 에이전트 ID, 사용자 동의 상태 등이 포함된 감사 추적(Audit Trail)을 체계적으로 기록 · 관리해야 한다.

21) David Paluy, Enabling Autonomous AI Agents to Make Payments: Challenges and Solutions, 2025. 4. 3.
22) 현재 Stripe 등의 기업에서 해당 기술의 개념 검증 단계에 있다.

이러한 기록들은 대시보드 형태의 모니터링 시스템을 통해 사용자와 관련기관이 실시간으로 확인할 수 있어야 한다. 대시보드는 단순한 거래 내역 모니터링을 넘어 잔여 예산, 승인 상태 등을 종합적으로 표시하며, 분쟁 발생 시 원인 규명과 책임 소재 확인의 근거로 활용된다.[23]

Ⅴ. Agentic AI 기반 지급 시 사용자 인증

1. 현황

Agentic AI 기반 지급결제시장은 아직 태동 단계로, 사용자 인증 체계에 대한 별도의 확정된 방향은 없는 실정이다. 모든 거래에 대해 강력한 인증을 의무화해야 한다는 견해와 거래 위험도에 따라 인증 강도를 차등화해야 한다는 견해가 병존하고 있다.

전자는 에이전트가 사용자를 대신하여 지급 행위를 수행하는 과정에서 발생할 수 있는 무단 지급, 의도 왜곡, 책임 불명확성 등 잠재적 리스크를 방지하기 위해, 모든 거래에 대해 일률적인 인증 절차를 적용하고 보안 수준을 강화해야 한다는 입장이다.

반면 후자는 거래 금액이나 위험도가 낮은 거래까지 동일한 인증을 요구할 경우 Agentic AI의 핵심 가치인 사용자 편의성이 저하될 수 있다는 점을 지적하며, 위험 기반 접근을 통해 저위험 거래에는 간소화된 인증을 적용하고 필요 시에만 강화된 인증을 수행하는 방식이 타당하다는 의견을 제시한다(표4 참조).

신뢰는 사용자 편의를 위해 훼손되어서는 안되나, 동시에 모든 거래를 반드시 일일이 수동 승인하도록 강제하는 것도 적절하지 않다. 특히 에이전트 경제 활성화를 위해서는 인증 절차의 간소화를 통한 이용자 편의성 제고가 핵심 과제로 부각되고 있는 만큼, 전자지급거래 전반의 인증 · 보안 동향을 참고하여 향후 Agentic AI 기반 지급거래에 적합한 인증체계와 안전장치의 방향을 모색할 필요가 있다.

〈표4〉 Agentic AI에게 위임하는 단계(Delegation Level) 분류

구분(level)	정의	예시
Manual (수동승인)	거래마다 사용자의 명시적 승인을 요구	-
Pre-approved (사전승인)	단일 · 정형화된 조건 내 자동 승인	특정 가맹점 월 $200 이하 자동 승인

23) 현재 Skyfire 등의 기업에서 해당 기술의 실행 초기 단계에 있다.

Custom/Hybrid (맞춤형 · 혼합형)	복수 조건 조합 및 상황 맥락 기반 맞춤형 위임 설계	시간대+금액+가맹점 조건 결합
Always-on (상시 위임)	신뢰된 에이전트가 사전 조건 없이 상시 자동 수행	반복 · 정기적 결제 완전 자동화

자료: Sardine, PayOS, Building Trust in Agentic Commerce, 2025.

2. 일반적 전자지급거래 시 사용자 인증 동향

가. EU · 영국의 강력한 고객인증(SCA) 정책

SCA(Strong Customer Authentication)은 「PSD2(Payment Service Directive)」에 따라 도입된 사용자 인증 정책으로, 모든 지급서비스제공사업자(PSP)가 전자지급거래 시 최소 2개 이상의 인증 요소를 이용해 거래자 신원을 확인하도록 의무화한 제도이다(표5 참조).

〈표5〉 SCA의 인증요소

구분	내역
지식기반 (knowledge)	고객이 알고 있는 정보(패스워드, PIN)
소유기반 (posession)	고객이 보유하고 있는 정보(카드, 기기생성 인증번호 등)
속성기반 (inherence)	고객의 신원에 관한 정보(지문, 음성인식 등)
기타	거래와 연계된 특정한 인증 코드

「PSD2」 제97조(인증)에 따르면, 지급인이 ① 온라인으로 지급 계좌에 접근하는 경우, ② 전자적 지급거래를 개시하는 경우, ③ 지급사기 또는 오남용 리스크가 내포된 원격 채널을 통한 거래행위인 경우 SCA를 적용할 것을 명문화하고 있다.

또한 유럽은행감독청(EBA)이 「PSD2」 제98조(인증 및 통신에 관한 규제기술표준)에 근거하여 제정, 2019년 9월부터 시행 중인 규제기술표준(RTS, Regulatory Technical Standards)에서는 SCA의 적용 범위, 인정되는 요소, 예외 사항, 거래 당사자 간 통신방식 안전성 확보 등을 세부적으로 정하고 있다.

특히 거래 리스크, 금액, 반복성, 채널 등에 따라 일정 범위에서 SCA 적용을 면제하고 있는 점에 주목할 만하다. 이는 소비자 편의성을 해치지 않으면서도, 저위험 거래에 대한 인증 부담을 줄이기 위한 장치이다(표6 참조).

〈표6〉 「PSD2」의 SCA 면제사항

구분	관련조문	내역
지급계정정보 접근	§10	민감정보에 접근하지 않는 계정정보 조회 시 SCA 면제 허용
비접촉 POS 결제	§11	소액 · 누적한도 내 비접촉 오프라인 지급에 대해 SCA 면제 허용
교통 · 주차요금 결제	§12	대중교통 · 주차 등 특정 저위험 지급에 대해 SCA 면제 허용
신뢰하는 수취인	§13	이용자가 사전 등록한 신뢰할 수 있는 수취인에 대한 지급을 SCA 면제 허용
반복 거래	§14	금액이 동일한 정기 반복지급의 후속 거래는 SCA 면제 허용
동일 지연인 · 법인 계좌 간 입금이체	§15	본인 또는 동일 법인의 계좌 간 내부이체는 SCA 면제 허용
소액거래	§16	단건 · 누적 금액 조건을 충족하는 소액 전자결제에 대해 SCA 면제 허용
비소비자 대상 전용 결제 프로세스 제공 법인	§17	기업 · 공공기관 등 특정 법인의 전용 지급 프로세스에서 SCA 면제 허용
거래리스크 분석	§18	PSP가 저위험으로 판단한 거래에 대해 위험기반으로 SCA 면제 허용

자료: Regulation(EU) 2018/389, Chapter Ⅲ (Exemptions from Strong Customer Authentication) §10~§18, 재구성

영국도 EU 회원국이던 2017년 당시 EU 「PSD2」를 자국법으로 이행하기 위한 「PSR 2017(Payment Services Regulations 2017)」을 제정하여 SCA 의무를 포함하였다. 하지만 브렉시트 이후에 EU와는 차별화된 규제정책 행보를 보이고 있으며, 이러한 움직임은 SCA 정책에서도 나타난다. 영국은 관련 규정을 금융감독청(FCA) 규칙(Handbook)으로 이관하여 기술 발전과 시장 환경 변화에 따라 신속하고 유연하게 규제를 조정할 수 있도록 하고 있다.

이러한 방향 하에, FCA는 ① 2025년 3월 기존의 고정 금액 한도 중심의 「PSD2」 SCA RTS 제11조[24] 면제 규정을 대체하여, 비접촉식 결제가[25] TRA(Transaction Risk Analysis)를 통해 저위험 거래로 식별된 경우 SCA를 면제할 수 있도록 하는 위험 기반 면제로의 전환을 제안하였으며, ② 2022년 개편에서는 AISP 접근 시 적용되던 90일 SCA 재인증 의무를 폐지하고 90일마다 고객 동의만 재확인하도록 절차를 단순화하였다. 이를 통해 초기 지급 계좌 접근 시에는 SCA가 요구되지만, 반복 접근에서는 간소화된 절차가 허용되어 사용자 편의성이 개선되었다.

한편, EU도 최근 「PSD3」및 「PSR」 개정 논의에서 SCA 규제의 일부 유연화 및 제3자 위임(delegation)을 포함하고 있다. 먼저 AISP의 지급 계좌 접근 시 은행(ASPSP)에게 적용되던 기존의 90일 SCA 재인증 의무 주기를 최초 SCA 이후 180일 동안 추가 인증 없이 접근을 허용하도록 연장하고, 이후 접근 시에는 ASPSP가 아닌 AISP가 자체 SCA를 분담 수행하도록 한다.[26] 또한 디지털지갑 내 토큰화 지급수단의 결제 사용 시 SCA 요소를 검증하는 패스스루형 지갑 사업자에 대해서는 결제사와 아웃소싱 계약을 체결하되, 결제사 책임은 강화함으로써,

24) 「PSD2」 SCA RTS 11조는 POS 비접촉 결제 시 소액 · 누적 · 연속 사용 금액 한도 조건 하에서 SCA를 면제할 수 있도록 허용하는 규정이다.
25) 비접촉식 결제(Contactless payment) 는 카드 또는 모바일 기기를 결제 단말기에 접촉 없이 가까이 가져다 대는 방식으로 이루어지는 NFC 기반 결제이다.
26) 2023년 제안된 PSR §86 (4)에 근거한다.

SCA 위임과 소비자보호 간 접점을 모색하였다.[27]

개정안은 인증 요소의 구성 요건도 완화하였다. 기존에는 지식 · 소유 · 고유성이라는 서로 다른 범주에서 두 가지 이상의 요소를 결합해야 했지만, 「PSR」 개정 논의 하에서는 독립성이 보장된다면 동일 범주의 요소 조합도 허용된다.[28]

또한 유럽은행감독청(EBA, European Banking Authority)의 해석에 기반해 면제로 운영되던 영역들을 조문화함으로써, SCA 적용 면제 조항을 명확화하고 있다.

대표적으로 MIT(Merchant-Initiating -Transaction) · MOTO(Mail Order/Telephone-Order) 거래에 대해 SCA 수행 의무를 유연화하는 구조로 법제화될 예정이다(표7 참고).

〈표7〉「PSD2」,「PSD3」,「PSR」간 주요 SCA 면제 유형 비교

구분	「PSD2」 적용 방식	「PSD3」 / 「PSR」 개정 방향
1) MIT (가맹점 개시 거래)	- 조문상 명시하지 않음 - 단, 지급인이 직접 개시하지 않는 거래로 SCA 의무 범위(§97) 외 해석 - 최초 거래 시 SCA 수행, 이후 계약 범위 내 반복거래 면제	- PSR 조문 내 “merchant initiated or recurring transactions” 명시 예정 - 최초위임(mandate) 시 SCA 수행, 이후 동일 계약 내 거래 면제
2) MOTO (우편주문 · 전화 주문)	- 조문 상 언급하지 않음 - 전자거래가 아니므로 「PSD2」 SCA 의무 범위(§97) 적용 제외	- PSR에서 ‘non-electronic, payer-non-initiated transactions (MOTO)’ 명문화

3. Agentic AI 기반 지급거래 시 사용자 인증 방향

앞서 살펴본 전자지급거래 시 SCA 규제 동향은 거래의 성격과 위험도에 따라 인증 수준을 차등화하는 방향으로 사용자 인증 제도가 전환되고 있음을 보여준다. 이는 규제의 목적이 보안 확보뿐 아니라 이용자 경험과 거래 효율성까지 고려하는 방향으로 확장되고 있음을 시사한다.

이러한 변화는 향후 Agentic AI 기반 결제 환경에도 중요한 함의를 갖는다. AI가 사용자를 대신해 지급거래를 수행하는 구조에서는 모든 거래에 동일한 수준의 SCA를 적용하기 어렵기 때문이다. 따라서 거래의 위험 수준과 맥락에 따라 인증 방식 · 절차를 달리하는 위험도 기반 차등 인증 구조가 도입될 가능성이 높다.

예를 들어, 저위험 · 일상적 거래에는 인증 절차를 간소화하고 최초 거래 개시시 인증 후 일정 주기마다 동의만 재확인하는 방식으로 지속성을 확보하되, 새로운 수취인이나 고액 · 비정형 거래의 경우에는 강화된 인증을 요구하는 차등적 방식이 적합할 것이다.

이 같은 위험 기반 인증체계의 확립은 지급거래 자동화가 확대되는 환경에서도 편의성과 이용자 보호 간의 균형을 유지하기 위한 기반으로 작용할 것으로 전망된다.

27) 2023년 제안된 PSR §87에 근거한다.
28) 2023년 제안된 PSR §85 (12)에 근거한다.

Ⅵ. 맺으며

본 고에서 살펴본 바와 같이, 지급결제 부문에서 글로벌 카드사 및 핀테크 기업 등을 중심으로 Agentic AI 기반 지급결제 서비스 도입이 점차 확대될 것으로 예상된다. 또한 사용자 관점에서 Agentic AI는 우리네 상거래 및 거래 경험을 완전히 새롭게 할 것으로도 기대된다. 하지만 이 과정에서 지급 편의성은 이용자 선택을 결정짓는 핵심 요소가 되는 반면, 권한 위임에 따른 오작동 · 남용 위험에 대비한 안전장치 마련 역시 필수적이다.

국내 상거래의 경우, 오픈뱅킹 등을 활용한 직 · 선불형 계좌 간편결제가 증가하는 가운데, 계좌출금 등 거래 처리 시점마다 별도의 사용자 인증을 요구하는 구조를 따르고 있다. 그런데 이는 향후 에이전트가 사용자를 대신하여 반복적 · 정기적으로 계좌출금을 통한 지급거래를 실행하는 Agentic AI 결제 모델에서 사용자 편익을 저해하는 요소로 작용할 수 있다.

따라서 향후 Agentic AI 기반 지급거래의 확산 가능성을 고려할 때, 해외에서 논의되고 있는 추가적인 소비자 보호 장치, 인증방식 차등화 관련 제도 · 운영 사례를 주목할 필요가 있다. 이를 토대로 국내에서도 Agent Commerce 환경에서 편의성과 안전성을 균형적으로 확보할 수 있는 인증체계 · 소비자 보호장치의 마련함으로써, 개화하는 Agentic AI 시대에 대비해야 할 것이다.

〈참고문헌〉

[1] 권소연, AI Agent 결제 지원 프로토콜(AP2) 공개, 해외디지털금융브리프, 2025.09.

[2] 김중한, 이영진, 오동환, 최민하, 김재우, 박준규, 글로벌 AI 바이블: AI 에이전트, 플랫폼의 새로운 지배자, 삼성증권, 2025.10.

[3] 카카오페이, AI 에이전트와 카카오페이 결제 오픈 API 연동하기: MCP Agent Toolkit 개발기, 2025.08.06.

[4] Amias Gerety, AI Agents have brains, but where are their wallets?, 2025.10.10.

[5] David Paluy, Enabling Autonomous AI Agents to Make Payments: Challenges and Solutions, 2025.04.03.

[6] Ekko an and Ryan Yoon, x402: Coinbase and the Beginning of the AI Agent Era, Tiger Research Reports, 2025.11.04.

[7] IBM, What are AI agent protocols?, 2025.

[8] Manu Sporny, Verifiable Credentials Data Model v2.0, 2025.03.15.

[9] OpenAI, Buy it in ChatGPT: Instant Checkout and the Agentic Commerce Protocol, 2025.09.30.

[10] Prakul Sharma, How banks can supercharge intelligent automation with agentic AI, Deloitte Insights, 2025.08.

[11] Ranjan Sapkota, AI Agents vs. Agentic AI: A Conceptual Taxonomy, Applications and Challenges, 2025.09.

[12] Sardine, PayOS, Building Trust in Agentic Commerce, 2025.

[13] Trulioo, Know Your Agent(KYA): An Identity Framework for Trusted Agentic Commerce, 2025.07.

[14] Vishal Mysore, Google Agents Payment Protocol (AP2) : Deep Dive with Live Examples, OpenAI, 2025.09.20.