

# AI Agent Commerce: 글로벌 트렌드와 한국의 대응 전략

에이전틱 커머스 시대의 표준·신뢰 인프라 확보 방안

## SUBJECT

AI Agent Commerce · Standards · Trust Infrastructure

## SCOPE

Global Trends · Korea Position · Policy Recommendations

## DATE

2026년 9월

## 발표 목적 및 핵심 질문

**AI Agent Commerce가 전자상거래 구조 자체를 재편하는 지금,  
한국이 취해야 할 정책적 대응 방향과 실행 방안을 제시한다**

### QUESTION 01

## 구조 변화의 실체

AI Agent Commerce는 어떤 구조 변화이며, 왜 지금 대응해야 하는가.

- 시장 규모와 성장 속도
- 4대 프로토콜의 표준화 경쟁
- 티핑 포인트 통과 증거

### QUESTION 02

## 한국의 위치와 정책 초점

한국의 현재 위치와 문제점은 무엇이며, 정책 초점을 어디로 옮겨야 하는가.

- 파운데이션 모델 vs 활용 인프라
- 결제·인증 인프라 강점 활용
- 프로토콜 종속 리스크 회피

### QUESTION 03

## 실행 가능한 사업 구조

표준·신뢰 인프라 확보를 위한 실행 가능한 사업 구조는 무엇인가.

- 협력형 규제샌드박스
- 중소기업 연대 기반 공동 실증
- Stablecoin 결제 주권 확보

### KEY MESSAGE

**파운데이션 모델 경쟁이 아닌 표준·신뢰 인프라 경쟁이 진정한 승부처다**

## 핵심 요약

# 시장은 이미 티핑 포인트를 지났고, 표준 선점 골든타임은 12~18개월이다

### 01 | 시장 재편 Market Reshuffle

2030년 글로벌 에이전틱 커머스 **3조~5조 달러** 전망. Black Friday 2025 AI 트래픽 전년 대비 **805% 급증**, 사이버위크 주문의 약 **20%가 AI 에이전트 경유**.

### 02 | 표준 선점 경쟁 Standards Race

**MCP · A2A · ACP · UCP/AP2** 4대 프로토콜이 사실상 표준으로 굳어지는 중. 미·EU·중·일이 각기 다른 방식으로 **자국 지분 확보**.

### 03 | 한국의 위치 Korea's Position

파운데이션 모델 확보에 정책 역량 집중. 활용 인프라·표준 참여에서는 **후행**, 해외 프로토콜 **종속 위험** 확대. 중소기업 AI 도입률 **5.3%**로 구조적 한계.

### 04 | 제언

#### Recommendation

정책 초점을 **활용 인프라 중심**으로 이동. **협력형 규제샌드박스**를 통한 실증. **Stablecoin 기반 결제 주권** 확보. 중소기업 **연대 기반 공동혁신 생태계** 구축.

AI Agent Commerce의 정의

단순 챗봇을 넘어, AI가 검색·비교·협상·결제까지 자율 수행하는 차세대 전자상거래

| 구분     | AS-IS   기존 전자상거래<br>Human-Centric | TO-BE   AI 에이전트 커머스<br>Software-Centric |
|--------|-----------------------------------|-----------------------------------------|
| Step 1 | 사람이 직접 상품을 검색                     | 사람은 구매 목적만 제시                           |
| Step 2 | 가격·리뷰·옵션 수동 비교                    | AI가 최적 상품 검색 및 비교                       |
| Step 3 | 장바구니 담기 및 배송지 입력                  | AI 에이전트 간 협상·주문 실행                      |
| Step 4 | 최종 클릭 결제 (본인 확인)                  | AI가 결제까지 대리 수행                          |

핵심 변화

커머스의 주체가 사람의 클릭에서 AI의 실행으로 이동. 남는 것은 권한·한도·책임의 문제다.

패러다임 전환 | SEO → AEO

## 인간이 시각적 UI를 탐색하던 SEO 시대에서 AI가 구조화된 데이터를 판독하는 AEO 시대로 전환

AS-IS

**SEO**

Search Engine Optimization

인간 소비자가 시각적 UI를 탐색

01. HTML 기반 웹페이지 최적화
02. 키워드 중심 검색
03. 사람이 클릭·결정·결제하는 구조

TO-BE

**AEO**

Answer Engine Optimization

AI 에이전트가 구조화된 데이터를 판독

01. Machine Feeds 기반 초경량 API
02. 에이전트가 자율적으로 거래 수행
03. Schema.org 확장, 게임이론 협상

EY ANALYSIS | 브랜드 충성도가 아닌 Machine-Legibility가 경쟁력

브랜드가 에이전트에게 보이지 않으면(invisible), 에이전트는 자동으로 다른 곳으로 수요를 우회한다. 상품 데이터가 **인간용 HTML**에서 **에이전트용 구조화 데이터**로 재편되는 것이 곧 경쟁력이다.

## 시장 규모 및 전망

2030년 글로벌 에이전틱 커머스 3조~5조 달러,  
미국 B2C 소매 오케스트레이션만 약 1조 달러 규모

### 2030 GLOBAL MARKET

**\$3—5 T**

글로벌 에이전틱 커머스 시장 규모 (USD)

SOURCE: McKinsey 연구

### US B2C RETAIL ORCHESTRATION

**≈ \$1 T**

미국 B2C 소매 오케스트레이션 매출 예상

SOURCE: McKinsey 연구

### MARKET DEFINITION

AI 에이전트가 사용자의 **선호·예산·구매이력**을 위임받아,  
**검색·비교·협상·결제·사후관리** 전 과정을 자율 또는 반자율  
로 수행한다.

### FUNDAMENTAL SHIFTS

01. 빈번한 API 호출 (초 단위 데이터 요청 반복)
02. 초소액 반복 결제 (기존 카드망 대비 경제성 붕괴)
03. 24/7 실시간 거래 (영업시간·정산주기 없음)

## Black Friday 2025 & Cyber Week 실적

2025년 Black Friday AI 쇼핑 트래픽 805% 급증,  
사이버위크 주문의 약 20%가 AI 에이전트 경유

### BLACK FRIDAY 2025 | AI TRAFFIC

+805%

AI 쇼핑 트래픽 전년 대비 급증

단순 실험이 아닌 상용화 단계 진입을 보여주는 결정적 지표

### CYBER WEEK | AI-ROUTED ORDERS

≈ 20%

사이버위크 전체 주문의 AI 에이전트 중개

5건 중 1건은 이미 AI가 주문 경로를 결정

### TIPPING POINT

티핑 포인트 통과

시장이 **실험 단계**를 지나 **상용화 단계**로 진입. AI 에이전트 커머스는 더 이상 미래의 개념이 아닌 **현재진행형 시장**이다.

## 글로벌 4대 프로토콜 개요

# MCP · A2A · ACP · UCP/AP2, 4대 프로토콜이 사실상 글로벌 표준으로 굳어지고 있다

### MCP

Model Context Protocol

Anthropic | <sup>LEAD</sup>재단 기증

LLM과 외부 도구·DB 간 데이터 접근 표준.  
양방향 컨텍스트 주입 및 실시간 API 연동.

"데이터 접근의 언어"

### ACP

Agentic Commerce Protocol

OpenAI | <sup>LEAD</sup>Stripe

결제·주문 실행·토큰화 담당.  
실제 트랜잭션이 발생하는 구간의 프로토콜.

"상거래의 결제 레일"

### A2A

Agent-to-Agent

<sup>LEAD</sup>Google | Linux Foundation

이기종 에이전트 간 협업·통신 표준.  
상태 동기화·작업 위임·상호운용성 확보.

"에이전트 사회의 대화 규범"

### UCP / AP2

Universal Commerce  
/ Agent Payments

<sup>LEAD</sup>Google · Shopify · Amazon · Meta

상품 탐색·장바구니·결제 전 과정 포괄.  
2026년 4월 Amazon·Meta 합류로 사실상 표준화 완료.

"커머스 가치사슬 전 구간"

4대 프로토콜 상세 비교

각 프로토콜은 커머스 가치사슬의 특정 구간을 담당, 향후 12~18개월이 표준 확정의 골든타임이다

| 프로토콜                                                    | 주도 기업                            | 담당 구간    | 기술적 특징                                                     |
|---------------------------------------------------------|----------------------------------|----------|------------------------------------------------------------|
| <b>MCP</b><br>Model Context Protocol                    | Anthropic                        | 데이터 접근   | LLM-외부 도구 간 인터페이스, 양방향 컨텍스트 주입, 실시간 API 연동                 |
| <b>A2A</b><br>Agent-to-Agent                            | Google                           | 에이전트 협업  | 이기종 에이전트 간 상태 동기화, 작업 위임, 상호운용성 <b>99% 목표</b>              |
| <b>ACP</b><br>Agentic Commerce Protocol                 | OpenAI / Stripe                  | 결제 실행    | 결제·주문 실행·토큰화, 실제 트랜잭션이 발생하는 구간                             |
| <b>UCP / AP2</b><br>Universal Commerce / Agent Payments | Google · Shopify · Amazon · Meta | 상품 탐색·결제 | Machine Feeds 기반 상품 데이터 교환, 동적 재고·가격 협상, <b>게임이론 기반 협상</b> |

GOLDEN TIME

12-18 개월

글로벌 표준이 확정되는 결정적 시기. 이 시기를 놓치면 외산 프로토콜에 종속되어 이후 참여의 의미가 사라진다.

주요국 정책 비교

미·EU·중·일이 서로 다른 방식으로 자국 지분을 확보 중,  
한국은 프로토콜 주도권 부재

| 국가 | 정책 방향         | 주요 내용                                                                                                |
|----|---------------|------------------------------------------------------------------------------------------------------|
| 미국 | 빅테크 사실상 표준 주도 | Anthropic(MCP), Google(A2A/UCP), OpenAI/Stripe(ACP) 등 빅테크 주도 테크 주도. 2026년 4월 Amazon·Meta 합류로 생태계 완성. |
| EU | 규제 프레임워크 선도   | AI Act 기반 규제 프레임워크, 디지털 주권 강화, AI 규제샌드박스 회원국별 운영.                                                    |
| 중국 | 자국 독자 생태계 구축  | 알리바바·텐센트 중심 독자 프로토콜 및 생태계 구축, 국가 주도 산업 정책, 내수 시장 규모 활용.                                              |
| 일본 | 정부 주도 표준화 참여  | 정부 주도 표준화 기구 참여, 상호운용성 확보 전략, 기존 산업과의 통합 중시.                                                         |
| 한국 | 강점 있으나 주도권 부재 | AI 기본법 2026.01 시행(아·태 최초 포괄 입법), 세계적 결제·인증 인프라 보유. 단, 프로토콜 지분 확보 후행.                                 |

한국의 현재 위치 | 강점과 기회

## 세계적 수준의 결제 인프라와 아·태 최초 AI 기본법, 하지만 활용 전략이 뒤처져 있다

### 강점

#### 01 입법적 토대 | AI Basic Act

AI 기본법 2026년 1월 시행, 아시아·태평양 최초의 포괄적 입법

고영향 AI(High-impact AI) 정의를 수용하여 국제 규제 정합성

#### 02 인프라 강점 | Payment & Identity

세계적 수준의 결제·인증 시스템(오픈뱅킹, 한국은행 프로젝트 한강), 풍부한 제조·유통 데이터, 5G/광섬유 기반 초고속 네트워크.

#### 03 기술 역량 | Foundation Model

독자적 파운데이션 모델 개발 역량 보유. 한국어·산업 도메인 특화 모델 확보 진행 중.

### 기회

**\$3–5T**

2030년 시장에서 선점 가능성 존재

결제·입법·기술 역량이 동시에 갖춰진 국가는 소수

### 과제

강점을 활용 인프라로 연결하지 못하는 구조

- 정책 자원 파운데이션 모델에 편중
- 표준·데이터 API 개방 후순위
- 산업별 에이전트 생태계 후행

한국의 3대 구조적 리스크

프로토콜 주도권 부재 · 해외 종속 위험 · 신뢰 인프라 실증 부재의 3중 위기

| 구분      | 리스크             | 현황 (Situation)                                          | 결과 (Consequence)                           |
|---------|-----------------|---------------------------------------------------------|--------------------------------------------|
| RISK 01 | 글로벌 프로토콜 주도권 부재 | 4대 프로토콜(MCP, A2A, ACP, UCP/AP2)에 대한 지분 부족.              | 2026년 4월 UCP에 Amazon·Meta 합류 후 참여 사실상 제한적. |
| RISK 02 | 해외 프로토콜 종속 위험   | 향후 12~18개월 내 지분 확보 실패 시.                                | 국내 판매자의 상품 데이터·결제 흐름·감사 로그가 해외 게이트웨이에 종속.  |
| RISK 03 | 신뢰 인프라 실증 부족    | 비인격 개체 식별(NHI), AP2 Mandate Chain 등 핵심 신뢰 인프라 실증 사례 부족. | 국제 표준화 회의체 의제 채택 실적 저조.                    |

시사점

3중 위기는 개별 대응이 아닌 협력형 규제샌드박스과 연대 기반 실증으로 해결해야 한다.

정책 초점의 이동 | AS-IS → TO-BE

파운데이션 모델은 투입 요소일 뿐,  
진정한 부가가치는 서비스와 활용에서 나온다

| 구분     | AS-IS   현행 정책 초점<br>파운데이션 모델 경쟁 | TO-BE   전환 방향<br>활용 인프라 경쟁      |
|--------|---------------------------------|---------------------------------|
| 전략 방향  | 독자 대형 모델 확보 경쟁                  | 공공 데이터 API 개방 및 표준화             |
| 자원 규모  | 수십조 원 규모 미·중 방식 추종              | 산업별 AI 에이전트 생태계 조성              |
| 중점 대상  | 정책 자원이 파운데이션 모델에 편중             | 중소기업·소상공인 연대 기반 공동 활용 지원        |
| 인프라 전략 | 데이터 API 개방, 산업별 에이전트 생태계 후순위    | 글로벌 프로토콜 상호운용성 확보, KYA 감사 로그 구축 |

핵심포인트

모델 경쟁에서 **활용 인프라(표준·신뢰 인프라)** 경쟁으로 무게중심 이동한다.

골든타임 | 12~18개월

# 규격이 굳기 전에 참여하는 나라만이 규격의 주인이 된다

| NOW   2026.08                                                                                                                                                                                           | + 12 MONTHS   2027.08                                                     | + 18 MONTHS   2028.02                                                                                                                                                      |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <div>골든타임 시작</div> <div>4대 프로토콜 표준 논의 활성화,<br/>Amazon·Meta UCP 합류로 사실상 표준화 임박</div>                                                                                                                     | <div>표준 초안 확정</div> <div>국제 표준화 기구의 초안 확정, 참여<br/>국가·기업 지분 배분 완료 단계</div> | <div>문 닫힘</div> <div>표준 확정 후 참여는 소비자 지위에<br/>머뭇, 재협상 여지 없음</div>                                                                                                           |
| <div>참여할 경우</div> <div>규격의 주인이 된다</div> <div><div>· 협력형 규제샌드박스를 통한 신속한 실증</div><div>· 글로벌 표준과의 상호운용성 확보</div><div>· ITU-T / IETF / W3C 회의체 의제 채택 실적 축적</div><div>· K-표준이 아·태 시장으로 확산할 여지 확보</div></div> |                                                                           | <div>놓칠 경우</div> <div>규격의 사용자가 된다</div> <div><div>· 외산 프로토콜에 기술 종속</div><div>· 디지털 주권 상실</div><div>· 국내 판매자 데이터·결제 흐름 해외 의존</div><div>· 표준 결정 회의체 참여 자체가 무의미해짐</div></div> |

"지금 참여하지 않으면, 이후에는 참여의 의미가 없다."

결제 인프라의 구조적 한계

기존 카드망은 AI의 초소액 반복 결제 처리에 부적합,  
결제 주체의 변화를 인프라가 따라가지 못한다

| 번호 | 문제 유형                                       | 내용                                                             |
|----|---------------------------------------------|----------------------------------------------------------------|
| 01 | 소액 비경제성<br>Micro-payment Economics          | 카드결제 평균 처리 비용 \$2~5. 소액일수록 수수료가 더 나오는 구조, AI 초소액 결제 시 경제성 붕괴.  |
| 02 | 건별 인증의 한계<br>Per-transaction Authentication | 거래마다 반복되는 본인확인 절차. AI의 초고속 API·데이터 호출 시 인증 요구는 사실상 불가능.        |
| 03 | 대리결제 증명 불가<br>Proof of Delegated Authority  | AI의 결제 권한 위임 여부 기록 체계 부재. 현행법은 사람만 결제 주체로 전제. 감사·분쟁·귀책 판단 불가능. |
| 04 | 법적 지위 부재<br>Legal Status of AI Agent        | AI는 결제 주체로 명시되지 않음. 권한·한도·책임의 정책적 공백 발생. 법 개정 없이 자율결제 상용화 어려움. |

BENCHMARK  
온체인 결제 평균 비용

\$0.2 —카드망의 1/10 ~ 1/25 수준

결제 주권 설계의 필요성

# AI 에이전트 커머스 시대, 결제 주권을 설계하지 않으면 경제 주권을 상실한다

배경  
커머스 주체가 사람의 클릭에서 AI의 실행으로 이동. 결제 주체의 변화를 **법과 인프라가 따라가지 못한다.**

| 공백     | POLICY GAP | 내용                                                          |
|--------|------------|-------------------------------------------------------------|
| GAP 01 | 인증 체계의 한계  | 기본 설계가 <b>본인 인증 중심</b> . AI 대리인의 권한을 증명할 방식이 존재하지 않는다.      |
| GAP 02 | 결제 구조의 충돌  | <b>건별 승인 중심 인프라</b> . 반복·초소액 결제에 대한 대응 자체가 불능.              |
| GAP 03 | 법적 지위의 부재  | 현행법은 <b>사람만 전제</b> . AI는 결제 주체로 명시되지 않고, 권한·한도·책임이 정의되지 않음. |

방치 시 위험

\$64B/연간

연간 약 640억 달러 규모의 스테이블코인이 제도 밖에서 흐르고 있다

방치 시 결제 데이터와 수익이 **해외로 유출**,  
**경제 주권 상실**로 이어질 위험.

Stablecoin | 프로그래머블 결제 인프라

Stablecoin은 단순 결제 수단이 아닌, AI가 자율 경제 활동을 수행할 수 있는 유일한 프로그래머블 인프라이다

| 번호    | 4대 핵심 장점                             | 내용                                              |
|-------|--------------------------------------|-------------------------------------------------|
| 장점 01 | 초소액 결제 지원<br>Micro-payments          | 매우 낮은 수수료로 고빈도·초소액 거래를 무한 반복 처리 가능.             |
| 장점 02 | 24/7/365 가용성<br>Always-on Settlement | 은행 영업시간·주말 정산주기에 구속 없이 실시간 결제·정산. AI 상시 거래에 적합. |
| 장점 03 | 국경 없는 정산<br>Cross-border             | 카드망-매입사-환전-정산은행의 복잡한 중개 단계 제거. 역직구·크크로스보더 최적.   |
| 장점 04 | 감사 가능성<br>Auditability               | 스마트 컨트랙트 기반 투명 거래 기록. 조작 불가 온체인 원장.             |

프로그래밍 가능한 화폐

예산·한도·용도 등 결제 규칙을 스마트 컨트랙트에 사전 설정 가능

자동 규칙 게이트

설정된 조건을 벗어난 결제 시도 시 실시간 자동 차단. 사고 예방형 인프라.

기존 카드망 vs 온체인 결제 비교

온체인 결제, 카드망 대비 수수료 1/10~1/25 수준으로  
AI 에이전트 결제에 최적화

| 구분     | 기존 카드·간편결제<br>Human-Centric | 온체인 결제<br>Software-Centric |
|--------|-----------------------------|----------------------------|
| 주요 대상  | 사람의 클릭, 건별 승인               | AI의 실행, 반복·초소액 결제          |
| 평균 비용  | \$2 ~ \$5                   | \$0.2 (1/10~ 1/25 수준)      |
| 인증 방식  | 반복적 본인 확인 절차                | KYA(AI 신원등록) 및 사전 권한 위임    |
| 결제 속도  | 정산 주기 존재 (영업일 기준)           | 24시간 실시간 즉시 결제             |
| 감사 가능성 | 제한적                         | 온체인 원장 기반 무결성 로그           |
| 프로그래밍  | 불가능                         | 스마트 컨트랙트 기반 자동 규칙 게이트      |

결론

AI 에이전트 커머스 환경에서 온체인 결제는 선택이 아닌 필수이다.

KYA 및 권한·한도·책임 해결 방안

KYA(Know Your Agent) 도입으로 AI 에이전트 신원 확인, 권한·한도·책임의 3대 문제 해결

SOLUTION 01

신원 확인 및 권한 검증

- KYA 도입, AI 에이전트에 고유 등록 신원 부여
- 기존 KYC/KYB를 넘어 소프트웨어 신원 특정
- 3단계 서명 체인: 의도 → 장바구니 → 결제

SOLUTION 02

스마트 컨트랙트 사전 예방

- 자동 규칙 게이트 구축
- 예산 초과, 카테고리 위반, 위임 범위 이탈
- 실시간 자동 차단으로 사고 예방

SOLUTION 03

4대 감독 권한 확보

- 결제 주체 식별 (KYA)
- 권한 검증 (위임 범위 확인)
- 실시간 차단 (AML 필터링)
- 사고 시 동결 (규제형 킬 스위치)

3단계 실증 로드맵

| 단계  | 기간       | 핵심 목표         | 주요 활동                                                          |
|-----|----------|---------------|----------------------------------------------------------------|
| 1단계 | 6~12개월   | 샌드박스 기술 검증    | 실증 도메인: 관광, 역직구, B2B 소액결제. KYA·AP2 Mandate Mandate Chain 기술 검증 |
| 2단계 | 통화 주권 유지 | 달러 수취 + 원화 정산 | 달러 스테이블코인 수취 허용, 최종 정산 원화(KRW) 의무화, FX·AML 관리 체계               |
| 3단계 | 국가 표준화   | 한국형 결제 게이트웨이  | KYA 전면 적용, 감사 로그 FIU·금감원 보고 체계 연결, 아·태 K-K-표준 확산               |

중소기업 AI 전환의 구조적 한계

중소기업 AI 도입률 5.3%, 제조업 1%에 불과  
자원·데이터·인력 부족으로 단독 대응 불가

| 출처            | 지표             | 내용                                                            |
|---------------|----------------|---------------------------------------------------------------|
| 중소기업중앙회       | AI 활용 중소기업     | 비중 <b>5.3%</b> , 제조업 분야는 <b>1%</b> 에 머물                       |
| OECD 보고서      | 중소기업 vs 대기업 격차 | 중소기업 <b>20.4%</b> vs 대기업 <b>40.0%</b> — 최근 5년간 2배 증가했으나 격차 지속 |
| OECD D4SME 설문 | 사용법 불확신        | <b>67%</b> 가 생성형 AI 사용법·리스크 평가 불확신                            |
| OECD D4SME 설문 | 데이터·법적 우려      | <b>80%</b> 가 데이터 프라이버시·법적 책임 우려                               |

4대 구조적 장애요인

자원 부족

AI 모델 개발·운영 예산 확보 불가. 개별 기업 단위 투자는 비경제적.

데이터 부족

AI 경쟁력은 데이터 축적에 있음. 개별 중소기업은 데이터 규모가 한계.

인력 부족

AI 전문 인재 채용·육성 불가. 글로벌 비즈니스 대응 역량 부족.

인프라 부족

클라우드·API 개방·구조화 데이터 변환 등 기술 인프라 미비.

단독 대응의 불가능성 | 왜 연대가 필요한가

# AI의 본질은 데이터에 있고, 데이터는 많이 쌓을수록 경쟁력이 생긴다

## 공동 대응이 필수적이다

| 구분         | 과거 IT 혁명                 | AI 혁명                             |
|------------|--------------------------|-----------------------------------|
| 경쟁력의 원천    | 외부 기술 수동적 도입으로 효율성 향상 가능 | 데이터가 경쟁력의 원천, 다양하게 많이 쌓을수록 경쟁력 발생 |
| 중소기업 대응 방식 | 개별 기업 단위 도입 가능           | 공동 대응 필수 — 개별 대응 불가능              |

### EY | Machine-Legibility가 곧 경쟁력

에이전트 커머스에서 브랜드가 **machine-legible**하지 않으면 자동으로 수요가 우회됨. 중소기업이 **단독으로 상품 데이터 구조화, API 구축, 프로토콜 대응**을 수행하는 것은 **사실상 불가능**.

### PAYPAL / OECD 제언

SME가 agentic commerce에서 소외되지 않기 위해서는 **정책 프레임워크, 혁신 허브, 교육 지원**이 필요. 개별 기업 지원이 아닌 **생태계 단위 지원**이 핵심.

**결론**  
중소기업·소상공인은 자원·인력·데이터가 없어 혼자 AI 에이전트 커머스 대응 불가. **업종별 연대·협력 구조 구축**이 유일한 해법이다.

협력형 전략 01 | 협동조합 기반 공동 AX 모델

업종별 협동조합이 공통 AI 수요 발굴부터 성과 확산까지 연결하는  
AX 확산 모델의 축이 된다

MODEL STRUCTURE | 중소벤처기업연구원 제언

| 단계     | 구성 요소          | 활동 내용                                       |
|--------|----------------|---------------------------------------------|
| STEP 1 | 공통 AX 수요 발굴    | 생산 공정과 현장 애로(Pain Point)가 유사한 업종 생태계 중심     |
| STEP 2 | AI 모델 공동 개발·실증 | 협동조합 단위로 <b>공동 AI 모델 개발</b> , 비용 분산, 리스크 분산 |
| STEP 3 | 성과 확산·사후관리     | <b>성공 모델을 업종 내 확산</b> , 지속적 개선              |

BENCHMARK | 북이탈리아 에밀리아-로마냐 모델

- **PICO**(현장 밀착형 기술 중개 조직) 통해 개별 기업 기술 수요 해결
- **공용 디지털 플랫폼** 활용으로 가상 규모의 경제 실현
- **당기순이익 3%**를 상호기금으로 의무 출당 → 데이터 인프라·클라우드 구축 투자
- 인구 400만, 1인당 GDP **4만 달러**, 대기업 없이 중소기업 중심으로 달성

한국형 적용

- **연대 혁신 기금** 조성 및 세제 지원
- 한국형 현장 밀착형 기술 중개 체계 **K-PICO** 구축
- **공동 활용 가능한 디지털 거점** 마련
- 협동조합 단위 데이터·클라우드·API 게이트웨이 공동 구축

협력형 전략 02 | 네트워크 협력형 모델

중핵기업 중심으로 사전 계약 기반 공동 에이전트 서비스 개발,  
위험 분산과 성과 공유를 동시에 달성한다

MODEL CONCEPT | 모델 개념

- 중핵기업(Leading Company)을 중심으로 여러 중소기업이 협력하여 공동 AI 에이전트 서비스 개발
- 사업 시작 전 권리·의무·지분 구조·역할·성과 배분 규칙을 사전 계약으로 확정
- 투명한 성과 공유 구조로 위험 분산과 수익 배분을 동시에 달성

APPLICATION | AI Agent Commerce 적용 방식

| 영역         | 중핵기업 역할                      | 중소기업 역할                             |
|------------|------------------------------|-------------------------------------|
| 플랫폼 인프라    | 커머스 플랫폼·결제 인프라 제공            | 상품 데이터 구조화·응용 서비스 개발                |
| 공동 AEO 전환  | Machine Feeds 표준 및 통합 스키마 설계 | 상품 카탈로그 통합 구조화, Machine Feeds 공동 구축 |
| 공동 프로토콜 참여 | 글로벌 표준화 협상 주도                | MCP/A2A/UCP 컨소시엄 공동 진입, 협상력 확보      |

EY FRAMEWORK 연계 | Orchestrator × Participant × Commercial Truth

Orchestrator 역할을 중핵기업이 담당, 중소기업은 Participant로 통합. 상업적 진실(Commercial Truth) 공동 구축: 상품 데이터·가격·재고·정책을 기계 판독 가능 구조로 통합 관리.

협력형 전략 03 | 동반성장 생태계 모델

기업·업종·지역·산학연이 각자의 자원을 공유하는  
공동혁신 생태계로 확장한다

ECOSYSTEM COMPOSITION | 생태계 구성 4대 축

| 협력 축    | 역할 및 활동                               |
|---------|---------------------------------------|
| 기업 간 협력 | 업종별 협동조합 중심 데이터 공유, 공동 AI 모델 개발       |
| 업종 간 연계 | 이종 산업 간 데이터 융합, 크로스 도메인 AI 에이전트 서비스   |
| 지역 간 연계 | 지역 주도형 AX 대전환, 공동 디지털 거점 활용           |
| 산학연 협력  | 학계·연구소가 코어 알고리즘·온톨로지 설계, 기업이 실증 환경 제공 |

CORE INFRASTRUCTURE | 핵심 인프라 3대 요소

|                                                       |                                                         |                                               |
|-------------------------------------------------------|---------------------------------------------------------|-----------------------------------------------|
| <b>데이터 협력 체계</b><br>영업비밀 노출 우려 해소를 위한 데이터 공유 가이드라인 마련 | <b>공동 디지털 인프라</b><br>클라우드·API 게이트웨이·구조화 데이터 변환 도구 공동 구축 | <b>연대 혁신 자금</b><br>협동조합 디지털 혁신 촉진 전용 기금·세제 지원 |
|-------------------------------------------------------|---------------------------------------------------------|-----------------------------------------------|

중소벤처기업연구원

"AI 정책은 기술 보급에 머물지 않고 데이터 활용과 인프라 실증을 통해 실제 성과로 이어져야 한다."

중소기업 AI Agent Commerce 참여 모델

협력을 통해 중소기업이 에이전트 커머스 생태계의 주축이 되는  
3단계 참여 모델

| 단계                  | 목표                         | 핵심 활동                                                                                                                                                                                              |
|---------------------|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1단계<br>DISCOVERABLE | 발견 가능<br>에이전트가 찾을 수 있는 상태  | <ul style="list-style-type: none"><li>· 협동조합 단위 상품 데이터 구조화, <b>Machine Feeds</b> 공동 구축</li><li>· AEO 전환: 인간용 HTML에서 에이전트용 초경량 API로 전환</li><li>· <b>Schema.org 확장</b> 기반 공동 상품 온톨로지 구축</li></ul>    |
| 2단계<br>TRUSTED      | 신뢰 가능<br>에이전트가 신뢰할 수 있는 상태 | <ul style="list-style-type: none"><li>· <b>MCP/A2A/UCP 컨소시엄</b> 공동 진입</li><li>· KYA 체계 도입: 협동조합 단위 AI 에이전트 신원 등록, 위임 권한 관리</li><li>· <b>Stablecoin 기반 공동 결제 인프라</b>: 초소액·실시간 결제, 수수료 분산</li></ul>  |
| 3단계<br>EXECUTABLE   | 실행 가능<br>자율결제까지 완결되는 상태    | <ul style="list-style-type: none"><li>· 자율 결제 역량 확보: <b>AP2 Mandate Chain</b> 공동 구축</li><li>· 크로스보더 에이전트 커머스: 협동조합 단위 해외 에이전트 플랫폼 연동</li><li>· 성과 배분: <b>사전 계약 기반 수익 공유, 연대 혁신 기금 환원</b></li></ul> |

EY 5대 실행 과제 연계

Commercial Truth 구축 · 에이전트 친화적 상품 데이터 · 자율성 스펙트럼 정의 · 거버넌스 설계 · 3-horizon 로드맵

협력형 규제샌드박스 | 개념과 필요성

개별 기업 실증이 아닌, 컨소시엄·협동조합 단위의  
협력형 규제샌드박스로 전환해야 한다

| 구분    | 기존 규제샌드박스<br>개별 기업 단위 실증                          | 협력형 규제샌드박스<br>컨소시엄·협동조합 단위 단체 실증  |
|-------|---------------------------------------------------|-----------------------------------|
| 실증 주체 | 중소기업은 규제 대응 역량·비용 부족으로 참여 자체가 어려움                 | 컨소시엄·협동조합·업종별 연대체를 단위로 한 단체 실증 특례 |
| 지속성   | 단발성 실증, 사업화·확산 단계로 연결되지 않음                        | 규제 유예를 민간 자율 실증과 경쟁 유도에 활용        |
| 검증 범위 | 개별 기술 검증에 그침 (프로토콜·결제·신뢰 인프라 등 생태계적 요소는 개별 검증 불가) | 실증 결과를 국가 표준화로 직접 연결, 생태계 전체 검증   |

협력형이 필수인 3대 이유

REASON 01

중소기업 단독 대응 불가

중소기업이 단독으로 규제 대응·실증 수행 불가. 연대체 단위 실증이 유일한 해법.

REASON 02

상호운용성이 핵심

프로토콜·결제 인프라는 상호운용성이 핵심. 개별 기업 단위 검증은 의미 없음.

REASON 03

생태계 단위 지원 필요

협력형 모델이 정책의 핵심. 개별 지원원이 아닌 생태계 단위 지원이 요구됨.

협력형 규제샌드박스 | 3종 규제혁신 세트

신속 확인 · 실증 특례 · 임시 허가 3종 규제혁신을  
컨소시엄 단위로 적용한다

| 규제혁신                                                                                                                                                                                           | 개념               | 협력형 적용 방식                                                                                                                                                                                                    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 신속 확인                                                                                                                                                                                          | 30일 내 규제 유무 확인   | 컨소시엄 단위 일괄 확인 — 협동조합이 대표 신청                                                                                                                                                                                  |
| 실증 특례                                                                                                                                                                                          | 법령 부재 시 시장 실증 허용 | 업종별 연대체 공동 실증 — 프로토콜·결제 상호운용성 검증                                                                                                                                                                             |
| 임시 허가                                                                                                                                                                                          | 안전성 확인 시 우선 출시   | 협동조합 단위 임시 허가 — 성과 공유 및 확산 촉진                                                                                                                                                                                |
| <div>협력형 적용 3원칙</div> <div><div>· 컨소시엄 구성: 협동조합·업종별 연대체가 주체, 대기업·학계·금융사 참여</div><div>· 단체 실증: 개별 기업이 아닌 연대체 전체 대상으로 규제 특례 부여</div><div>· 공동 성과 관리: 실증 결과 연대체 공동 소유, 국가 표준 후보안으로 활용</div></div> |                  | <div>REGULATORY DOMAINS   규제 대상 영역</div> <div><div>· AI 에이전트 결제 자율성 (전자금융거래법)</div><div>· 비인간 신원(NHI) 인증 체계 (AI 기본법)</div><div>· Stablecoin 기반 초소액 결제 (가상자산법)</div><div>· 크로스보더 에이전트 커머스 (외환거래법)</div></div> |

핵심원칙: 개별 규제 대응이 아닌, 연대체 단위의 단체 실증이 프로토콜·결제·신뢰 인프라 표준화의 전제조건

연차별 실행 로드맵 | 협력형 실증

3년간 협력형 실증에서 확장, 검증을 거쳐 국가 표준화로 전환한다

| 연차  | 단계     | 주요 활동                                                                                                                                                                                            |
|-----|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1년차 | 실증 개시  | <div><div>· 업종별 협동조합 대상 협력형 규제샌드박스 개시</div><div>· 4대 프로토콜 국내 어댑터 구축 (컨소시엄 단위) · DID/VC 기반 비인간 신원(NHI) 인증 인프라 실증</div><div>· 공동 상품 데이터 구조화 (AEO 전환) 파일럿, <b>표준 기고서 4건 이상</b> 국제 기구 제출</div></div> |
| 2년차 | 실증 확장  | <div><div>· <b>크로스보더 상호운용성 확보</b> (업종 간 연계)</div><div>· Stablecoin 기반 결제 실증 (협동조합 단위 공동 결제), 개인정보영향평가(PIA) 완료</div><div>· <b>연대 혁신 기금 본격 가동</b>, K-PICO 현장 중개 체계 확대, 데이터 공유 가이드라인 확정</div></div> |
| 3년차 | 검증·제도화 | <div><div>· <b>대국민 상용 서비스 실증</b> (업종별 협동조합 참여), 레드팀 보안 검증</div><div>· <b>국가 표준화 전환</b> — 실증 결과를 K-표준으로 제도화</div><div>· 아·태지역 K-표준 확산 추진</div></div>                                              |

핵심 성과 지표

3,000+ TPS

프로토콜 처리량

≤ 200ms

평균 응답시간

100,000+ 에이전트

동시 접속

0건

자율결제 사고

5.3% → 20%+

중소기업 AI 도입률

정부 정책 패키지 | 4대 핵심 정책

연대 혁신 기금 · K-PICO · 공동 디지털 거점 · 협력형 규제샌드박스의  
4대 정책 패키지

POLICY 01

FUND

연대 혁신 기금

- 협동조합 디지털 혁신 촉진을 위한 **전용 기금 조성**
- 세제 지원: 협동조합 내 AI 투자에 대해 **세액공제**
- 북이탈리아 모델 벤치마크: **당기순이익 일부 의무 출당제**

POLICY 03

DIGITAL HUB

공동 디지털 거점

- 공동 활용 가능한 디지털 인프라 (**클라우드·API 게이트웨이·데이터 변환**)
- 업종별 협동조합이 공동으로 활용하는 **디지털 거점** 마련
- 데이터 협력 체계 구축: 영업비밀 보호 가이드라인, 규제 대응 비용 완화

POLICY 02

TECHNOLOGY BROKERAGE

K-PICO | 한국형 현장 밀착형 기술 중개 체계

- 현장 밀착형 기술 중개 조직 구축, **개별 기업 기술 수요 직접 해결**
- 업종별 전문가 파견, 맞춤형 AI 전환 솔루션 제공
- **공용 디지털 플랫폼** 통해 가상 규모의 경제 실현

POLICY 04

REGULATORY SANDBOX

협력형 규제샌드박스

- **컨소시엄·협동조합 단위 단체 실증 특례**
- **3종 규제혁신** (신속 확인·실증 특례·임시 허가) 적용
- 실증 결과를 **국가 표준화로 직접 연결**

핵심 메시지 및 기대효과

규격이 굳기 전에 참여하는 나라만이 규격의 주인이 된다

기대효과

| 영역 | 기대효과                                                |
|----|-----------------------------------------------------|
| 산업 | 중소기업 연대 기반 AI 에이전트 생태계 주축 육성, AI 도입률 5.3% → 20%로 향상 |
| 표준 | 글로벌 프로토콜 지분 확보, ITU-T·IETF·W3C 기고 채택, K-표준 아·태 확산   |
| 정책 | 디지털 주권 수호, Stablecoin 기반 결제 주권 확보, KYA 표준 선점        |
| 시장 | 협력형 규제샌드박스를 통한 실증 선도, 2030년 \$3~5조 시장에서 주도권 확보      |

결론

- 01. "파운데이션 모델 경쟁이 아닌 표준·신뢰 인프라 경쟁이 진정한 승부처다."
- 02. "중소기업이 단독으로 대응할 수 없는 시대, 연대와 협력이 유일한 해법이다."
- 03. "협력형 규제샌드박스"로 한국이 에이전틱 커머스 표준의 주인이 되어야 한다."