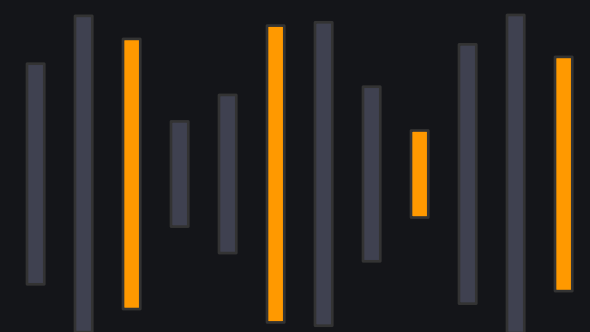




# 에이전트 이코노믹스 (Agent Economics) 자율 AI 시대의 경제 질서

오순영

Amazon Web Services

수석 솔루션즈 아키텍트



# Agenda

6개의 전환으로 보는 에이전트 경제질서

01



## ECONOMICS

지식노동의 한계비용이 낮아진다

02



## ORGANIZATION

부서에서 에이전트 네트워크로

03



## MARKET

에이전트가 거래하면, 가격 단위도 바뀐다

04



## AI SECURITY

보안도 '머신 스피드'로 이동해야 한다

05



## TRUST

신뢰는 윤리 문구가 아니라 거래 인프라다

06



## WORK

일자리가 아니라 '역할의 계약'이 바뀐다

# 에이전트 이코노믹스

소프트웨어가 답변을 넘어 목표, 자원, 거래를 스스로 조정하는 순간, AI는 도구가 아니라 새로운 경제주체가 된다.

< 5% → 40%

2025년에서 2026년 말,  
기업 앱에 통합될 과업형 AI 에이전트가  
통합될 것이라는 전망

Hours / Days

Frontier Agent가  
사람의 지속적 개입 없이  
과업을 수행하는 시간 범위

2M+

프리뷰 후 5개월 동안 기록된  
Amazon Bedrock AgentCore  
SDK 다운로드



# 지식노동의 한계비용이 낮아진다

잠재가치를 실현가치로 바꾸는 것은 모델이 아니라 목표·맥락·검증을 갖춘 운영 구조다.  
경제학적으로 중요한 변화는 시가 “무엇을 할 수 있는가” 보다 “얼마의 비용으로 반복할 수 있는가” 이다.

**\$2.6 ~ 4.4T**

생성형 AI가 매년 창출 가능한  
글로벌 경제가치 추정(McKinsey 추정)

**6명 · 76일**

Bedrock 추론 엔진 재구축을  
수행한 팀과 기간 (Amazon Bedrock팀)

**4.5x ~ 10x+**

Amazon Stores의 50여개 팀  
파일럿 중 새 도구&업무방식 적용한 25개 팀

## 기대와 실행 사이의 간극

Agentic AI가 회사를 바꿀 것이다 **84%**

현재 AI를 매우 효과적으로 활용 **26%**

잠재가치와 실현가치 사이의 격차는 운영에서 발생한다

## AWS frontier team · Bedrock 추론 엔진 재구축

산정

**30명**

12 - 18개월



실제

**6명**

76일

병목은 '실행하는 손'에서 '문제를 정의하고 검증하는 판단'으로 이동

\*\* 출처: McKinsey 생성형 AI 경제 잠재력 · AWS·HBR Analytic Services · AWS frontier teams \*\*

# 🛒 에이전트가 거래하면, 가격의 단위도 바뀐다

기계가 구매하는 시장에서는 비용의 기준이 토큰이 아니라 '완수된 성과(Cost per Successful Action)'로 이동한다.

## ■ 웹 활동의 주체(사람에서 기계로)

51%+

이미 봇이 주도하는 자동화 트래픽 비중  
(웹 트래픽 점유율)



봇 51%      사람 49%

사람만이 아니라  
목적과 예산을 가진 소프트웨어는  
고객이 된다.  
API, 데이터, 콘텐츠가 '기계가  
구매하는 상품'이 된다.

## ■ AgentCore Payments 프리뷰 서비스(소액결제 프로토콜)

01 발견      웹 콘텐츠 · API · MCP 서버 · 다른 에이전트

02 인증      AgentCore Identity  
구매 주체와 위임된 동의를 확인

03 결제      x402 기반 소액결제 (Coinbase · Stripe)

04 집행      Policy · Gateway - 허용 도구 · 금액 · 조건

공급 측 - AWS WAF는 요청당 가격을 정해 AI 봇에 과금한다

## ■ Agent P&L

Prompt Caching      - 90%

Intelligent Prompt  
Routing      - 30%

총 원가에 포함되어야 할 것

- 추론 + 데이터·API 사용료
- 실패와 재시도
- 인간 검수
- 보안 · 감사비용

\*\* 출처: AWS Financial Services Symposium 2026 · AWS WAF AI traffic monetization · Bedrock 비용 최적화 \*\*

# 🧩 부서에서 에이전트 네트워크로

오케스트레이터와 전문 에이전트가 MCP·A2A로 연결되면, 조직의 경계가 권한과 프로토콜로 다시 그려진다.

## ■ Allianz Technology SE · 7개의 전문 Agent 보험금 청구 워크플로우 구축



**- 80%**

보험금 처리시간의 단축률  
100일 → 20일

### 새로운 운영 경계

- 어떤 데이터·도구에 접근하는가
- 누구를 대신해 결정하는가

### MCP 도구 연결 · A2A 에이전트 간 능력 발견 · 과업 위임

  
Strands Agents  
SDK

  
AgentCore  
Runtime

  
AgentCore  
Gateway

  
AgentCore  
Memory

  
MCP + A2A  
Protocol

“목표, 권한, 비용, 품질”  
하나의 운영체제로 관리 필요  
에이전트가 많아질수록 책임의  
연결도의 설계 중요.

\*\* 출처 AWS re:Invent 2025 금융서비스 사례 · AWS AgentCore Runtime A2A 지원 · AgentCore FAQs \*\*

# 고성능 AI의 등장으로 보안 전략을 다시 쓰게 한다

프론티어 AI의 익스플로잇 역량은 시작에 불과하다 - 속도·규모·접근성이 동시에 바뀌면 보안의 전제가 무너진다.

2.3년 → 20시간

평균 익스플로잇 소요 시간 변화  
(2018 → 2026)

97%

AI 사고를 경험한 조직에서  
적절한 접근 통제가 결여

94%

임원진이 AI 사용 전  
보안 적용이 중요하다고 응답

■ 업계에 미치는 영향(보안 전략 재설정이 필요한 3가지) → 보안태세는 고성능 AI로부터의 취약점 공격에 대응할 수 있는 상태인가?

COMPLIANCE

규정준수

CSA·NIST·OWASP가 지침을 업데이트 중  
현재의 규정 준수 태세에는 더 이상  
실제 위험이 반영되지 않을 수 있음

VULNERABILITY

취약점 과부하

AI가 여러 결함을 동시에 발견하므로  
Log4J 수준의 이벤트가 더 자주  
발생할 것으로 예상

RISK MODEL

위험 관리

AI 이전의 가정을 기반으로 구축된  
위험 모델은 이제 유효하지 않음  
평균 악용 시간 가정은 폐기 대상

\*\* 출처 IBM Cost of Data Breach 2025 · SailPoint AI Agents Report 2025 · CSA · NIST · OWASP · zerodayclock.com \*\*

# 보안도 Machine Speed로 이동해야 한다

자율성이 높아질수록 보안은 사후 점검이 아니라 에이전트의 행동 경로에 내장된 완결된 보안 루프가 된다.

## Weeks → Hours

에이전트 기반 보안 테스트가 바꾸는  
검증 주기

## 90%+

HENNGE가 AWS Security Agent로  
단축한 테스트 기간

## 4 Stages

AWS Continuum이 운영하는  
완결된 보안 루프

### ■ AWS Continuum · 4단계 완결된 보안 루프

#### DISCOVER

#### 발견

소스코드·아키텍처·앱  
맥락을 이해하고 잠재  
취약점 탐색



#### PRIORITIZE

#### 우선순위

비즈니스 영향과  
공격 가능성 기준으로  
정렬



#### VALIDATE

#### 검증

격리된 샌드박스에서  
실제 공격 체인 재현 ·  
오탐 제거



#### REMEDiate

#### 교정

가드레일 안에서 되돌릴  
수 있는 완화 · 중요 변경  
은 인간 승인

\*\* 출처 AWS frontier agents for security testing · AWS Security Agent GA · AWS Continuum \*\*



# Security Agent - 통합 기능과 고객 적용 효과

보안 에이전트 = 코드의 생애주기 전체에 내장된 머신 스피드 보안

설계 검토

수 분

지정한 보안 요구사항에  
기반하여 문서를 검토 및 평가

코드 검토

준 실시간

PR과 S3 코드를 보안  
요구사항 기반으로 소스코드 분석

침투 테스트

수 시간

다중 공격 시나리오로  
검증된 취약점 식별·상관 분석

위협 모델링

수 십분

제공된 소스를 기반으로  
위협 모델링 수행

## LG CNS · Security Agent 도입 효과

SPEED

속도

점검시간의 제약이 적어  
빠르게 취약점을 식별하고  
제거 가능하여 보안 프로세스  
속도 향상

EXPERTISE

전문성

인력 확대 없이 전문가의  
역량을 활용할 수 있어  
서비스 제공 고객 확대 가능

COST

비용

점검 수행에 필요한 비용이  
절감되어 더 자주 점검을  
수행할 수 있게 됨

INTEGRATION

통합

소스코드 변경 시 사람이  
관여하지 않고 파이프라인  
연계를 통한 자동 점검 수행

\*\* 출처 AWS Security Agent GA · LG CNS Security Agent 도입 사례 \*\*

# 신뢰는 윤리 문구가 아니라 거래 인프라다

높은 자율성 = 통제를 없애는 것이 아니라, 목적, 권한, 예산, 중단조건을 코드와 정책으로 명확하게 만드는 것

## Agentic AI 준비도 (AWS·HBR)

데이터가 충분히 준비됨 13%

거버넌스가 충분히 준비됨 11%

인력이 매우 충분히 준비됨 5%

명확한 성공지표가 없음 95%

준비되지 않은 자율성은 결국 사람의 재확인 비용을 키운다

## Amazon Bedrock AgentCore 기능

**Identity** 사용자와 에이전트의 신원을 연결

**Gateway** 도구 접근의 공통 경계를 생성

**Policy** Cedar 기반 결정론적 규칙으로 권한·입력값·지출 한도를 집행

**Observability** CloudWatch·OpenTelemetry로 추론과 도구 호출의 경로 추적

**Evaluations** 13개 기본 평가기로 완수·정확성·안전·도구 선택 검증

\*\* 출처 AWS·HBR Analytic Services · AgentCore Evaluations & Policy · AWS Docs - AgentCore Policy \*\*

# 일자리가 아니라 '역할의 계약'이 바뀐다

반복 실행은 에이전트로, 목적·판단·책임은 인간으로 이동한다.

## 인간 역할의 이동



**Do**

직접 수행한다



**Delegate**

목표와 맥락을 위임한다



**Verify**

결과와 예외를 검증한다



**Own**

최종 결과를 책임진다

사라지는 것은 직업 전체가 아니라 '사람이 직접 수행해야 했던 과업의 경계'다

**~40%**

AI 변화에 노출된 전 세계 일자리 비중

IMF

**2× & 2.5×**

요구 역량의 변화 속도 & 새 과업이 인간  
역량(공감·판단·창의성)을 요구할 가능성

PwC 2026

**7×**

AI 노출도가 높은 주니어 직무가  
시니어 역량을 요구할 가능성

PwC 2026

\*\* 출처 IMF - New Skills and AI · PwC 2026 AI Jobs Barometer · Werner Vogels 2026 predictions \*\*

# 자율 AI 시대의 새 경제질서는 목적·권한·책임이다

AI가 더 많이 일하는 시대가 아니라, 에이전트의 수가 아닌 인간의 의도를 얼마나 정확하게 확장하는가가 경쟁력이 되는 시대를 연다.

## HUMAN INTENT

기술의 속도보다  
방향의 선명함



목적  
PURPOSE

무엇을 위해  
행동하는가



권한  
AUTHORITY

어디까지 스스로 결정하고  
언제 인간에게 돌아오는가



책임  
ACCOUNTABILITY

결과를 누가 설명하고  
끝까지 책임지는가

자율성은 시스템에 부여할 수 있지만 책임은 조직과 인간에게 남는다.  
가장 많은 에이전트를 가진 조직이 아니라, 무엇을 위해 행동해야 하는지 가장 선명하게 정의하는 조직이 새로운 경제질서를 주도한다.

# Thank you!

