Deloitte.

Tech Trends 2026

기업의 미래를 결정지을 AI 시대 5대 핵심 동력

: 단순한 AI 도입을 넘어 조직 재구축으로

Deloitte Insights
March 2026

Leader's Message

Deloitte.

"기술의 진화를 넘어, 조직의 '학습 속도'가 격차를 만듭니다"

배재민 대표

AI 통합 서비스(One AI) 그룹 리더 | 컨설팅 부문

02-6676-3700

jaeminbae@deloitte.com

2026년, 우리는 단순한 기술 혁신을 넘어 산업의 작동 방식 자체가 재편되는 전환점에 서 있습니다.
이제 경쟁의 초점은 알고리즘의 우위가 아니라, 기술을 얼마나 빠르게 조직에 흡수하여 비즈니스로 전환하는가에 달려 있습니다.

딜로이트는 현 시점에서 AI를 통해 재편되는 기업 환경 변화를 제시 하고자 합니다.

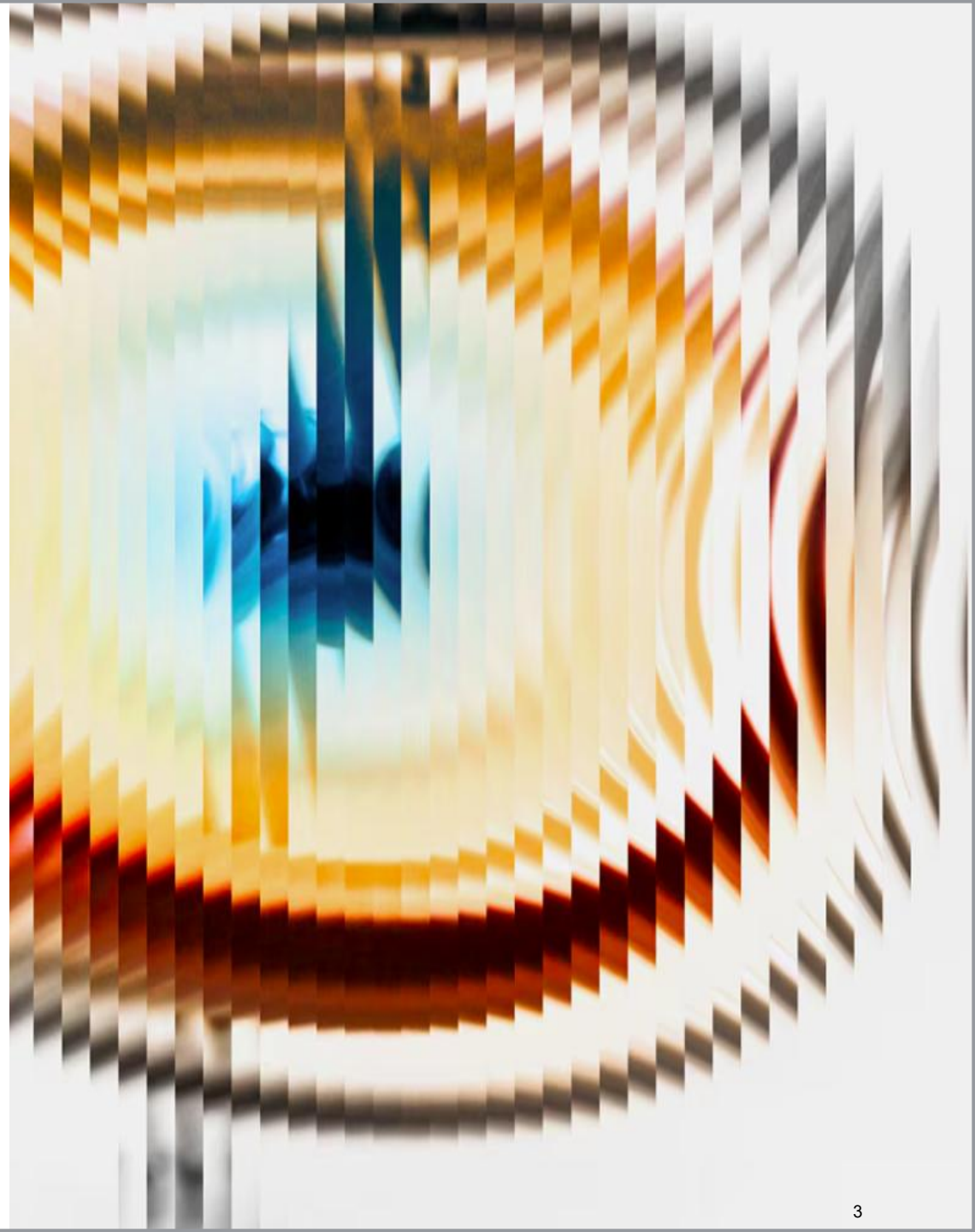
1. 피지컬 AI: 화면을 넘어 물리적 현장에서 직접 행동하는 AI (현장 지능화)
2. 에이전틱 AI의 현실 적용 및 점검 : 에이전틱 AI: 스스로 판단하고 실행하는 자율적 업무 체계 (운영 자율화)
3. AI 인프라 전략: 연산력과 전력 인프라가 곧 기업의 경쟁력 (인프라 최적화)
4. AI 네이티브 조직: 인간과 AI가 협업하는 제품 중심의 민첩한 구조 (조직 재편)
5. 지능형 보안: AI 공격을 AI로 막아내는 전략적 보안 패러다임 (신뢰 확보)

이 다섯 가지 변화는 개별 기술이 아닌, 서로 맞물려 돌아가는 하나의 새로운 운영체제입니다. AI는 물리 세계로 확장되고, 에이전트가 업무를 수행하며, 이를 가능하게 하는 인프라 경쟁이 심화되고, 조직은 이에 맞게 재편되며, 동시에 새로운 보안 과제가 등장합니다.

결국 AI 시대의 경쟁력은 단일 기술의 우수성에서 나오지 않습니다. 기술, 인프라, 조직, 거버넌스를 얼마나 빠르게 통합하고 학습하는가가 기업의 미래를 결정하게 될 것입니다.

본 보고서의 전략적 제언이 귀사의 실질적인 변화와 도약을 이끄는 핵심 시사점이 되기를 기대합니다.

목차



[Executive Summary] 2026년 비즈니스를 재편할 5가지 핵심 동력

딜로이트 Tech Trends 2026은 기업의 근간을 재편하는 5대 핵심 동력을 제시하며, 이제 AI가 단순한 기술적 보완을 넘어 조직 구조의 근본적인 재설계를 요구하고 있음을 보여줍니다.

1 **피지컬 AI: AI와 로보틱스의 결합** (AI Goes Physical)

AI는 디지털 환경을 넘어 로보틱스와 결합하며, 물리적 세계의 복잡한 문제를 자율적으로 해결하는 실행 주체로 진화하고 있다.
(e.g. 아마존: 100만 대의 로봇 배치를 통해 물류 효율 10% 개선, BMW: 생산 라인 내 차량 스스로 주행하는 자율 생산 시스템 구축)

2 **에이전틱 AI의 현실 적용 및 점검** (The agentic reality check: Preparing for a silicon-based workforce)

에이전틱 AI의 성과는 에이전트 자체가 아니라, 기존 업무를 전제로 한 자동화를 넘어 전사적 프로세스를 재설계할 수 있는지에 달려 있다.

3 **AI 인프라 전략의 재정립** (The AI infrastructure reckoning: Optimizing compute strategy in the age of inference economics)

AI 사용량 폭증으로 클라우드 중심 전략은 비용과 성능 한계에 직면하고 있으며, 하이브리드·엣지 기반 인프라로의 전환이 필수적 선택이 되고 있다.

4 **AI 네이티브 조직으로 개편** (The great rebuild: Architecting an AI-native tech organization)

AI 확산은 IT 조직의 운영 모델을 근본적으로 재편하고, CIO를 기술 관리자가 아닌 비즈니스 전환을 이끄는 핵심 전략 리더로 변화시키고 있다.

5 **사이버 보안의 딜레마** (The AI dilemma: Securing and leveraging AI for cyber defense)

AI 시대의 보안은 정적인 통제를 넘어, 지능형 공격에 기계의 속도로 대응하는 AI 기반의 자율적·실시간 방어 체계로 전환되고 있다.

Intro : AI 격차는 기능이 아니라 '조직의 학습 속도'에서 벌어진다

AI 논의의 핵심은 무엇을 어디에 도입할 것인가가 아니라, 실험적 단계에 있는 기술을 얼마나 신속하게 실제 비즈니스 성과로 연결할 수 있는지와 이를 뒷받침할 조직 역량과 운영 체계를 갖추었는지에 있습니다.

AI 도입 과정에서 직면하는 문제

AI 확산 속도와 구조적 변화

- AI 확산 속도는 기존 기술과 비교 불가한 수준
  - 전화(50년), 인터넷(7년), 생성형 AI(수개월)
- 현재 AI 주간 사용자 8억명, 전 세계 인구의 약 10%

핵심 논제

AI로 무엇을 할 수 있나? → 실험 단계를 넘어 실제 성과로 어떻게 연결할 것인가?

AI 확산의 핵심은 속도가 아니라 조직 구조

기하급수적으로 확산

- AI 스타트업의 성장 속도는 SaaS 대비 5배
- AI 지식의 유효기간은 '년'이 아닌 '월' 단위
- 기술을 학습하는 속도 보다 기술의 진화 속도가 더 빠름
- 후발 주자는 단순 추격이 아니라 구조적 열세에 직면

구조적 재설계 필요

- 기술 → 활용 → 데이터 정제·통합 → 인프라 투자 → 비용 절감 → 실험 확대
- 모든 요소가 동시·가속되는 플라이휠(연쇄반응) 효과가 일어나는 구조 구축 필요

AI 도입 시 기존 운영 방식의 한계

단순 기술 향상이 아닌 '조직 재구축' 요구

클라우드 중심 인프라 ≠ AI 경제성

- 사용량에 비례해 누적되는 AI 추론 비용을 기존 클라우드 구조로는 감당 불가
- 클라우드 일변도에서 벗어나 비용 최적화 중심의 하이브리드·엣지 인프라로 재설계 필수

인간중심 설계 ≠ 에이전트 병렬처리

- 인간의 순차적 업무 방식은 24/7 가동되는 AI의 처리 속도를 수용 불가
- 에이전트 간 상호작용을 위한 프로세스 재설계 필요

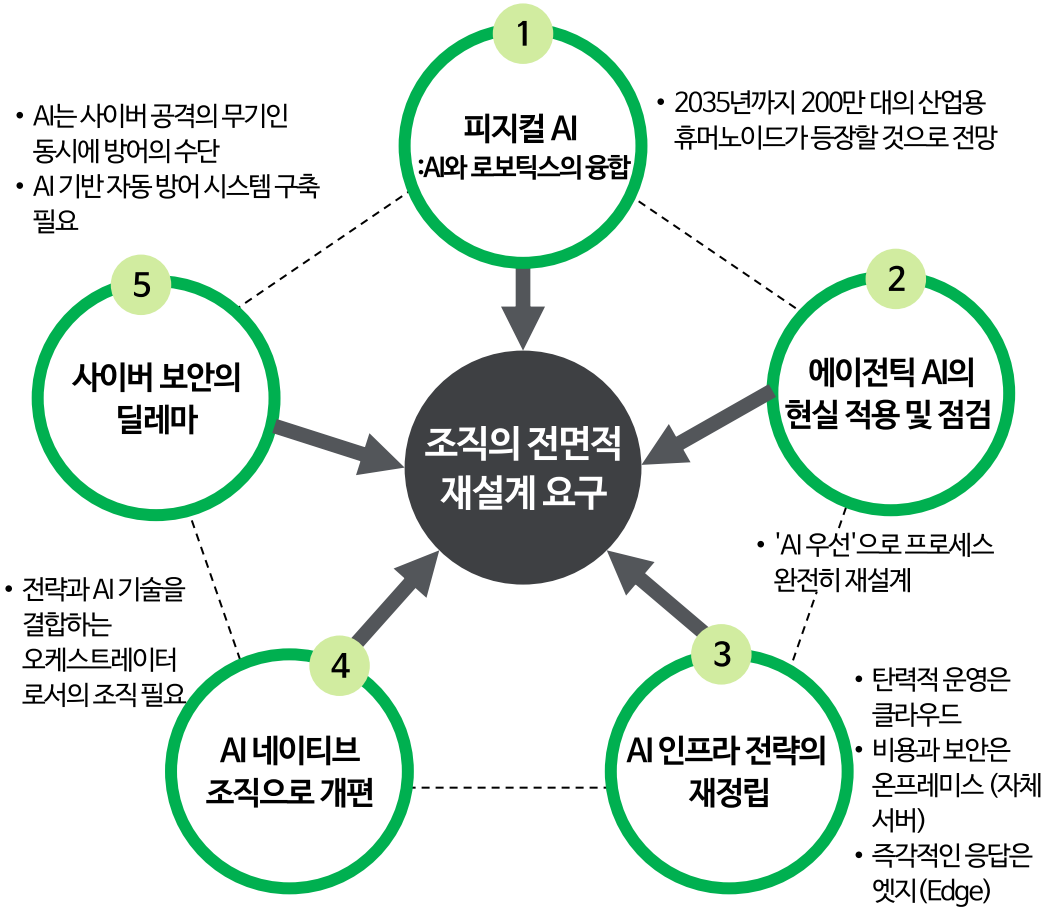
경계형 보안 ≠ 기계 속도 위협

- 전통 보안은 네트워크 경계·인간 탐지 중심
- 데이터·모델·행위 단위 실시간 통제 체계로 전환

서비스 중심 IT ≠ 비즈니스 전환

- 기존 IT 조직은 비즈니스 모델 혁신 주도에 한계
- 비즈니스 전환을 설계·주도하는 전략 조직 필요

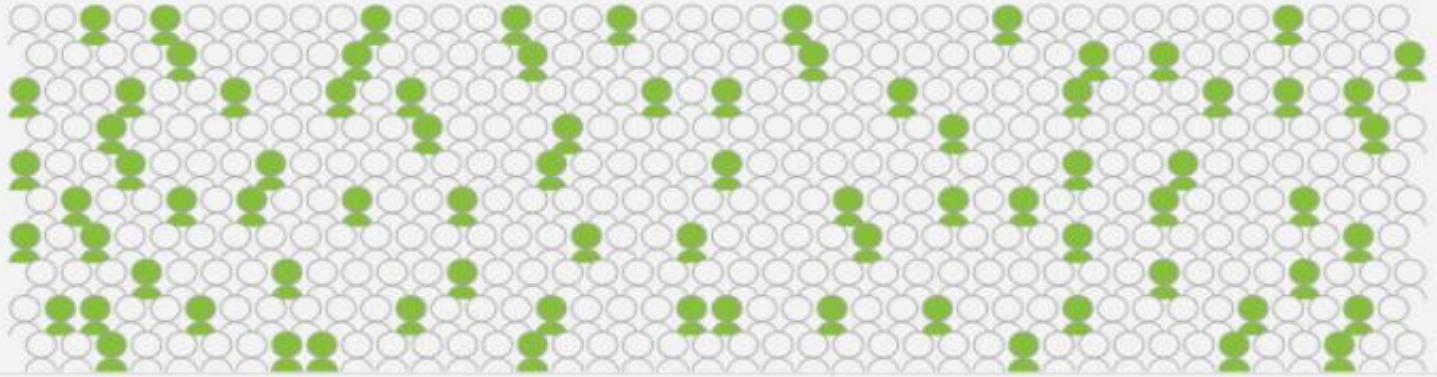
조직 재설계를 요구하는 동인과 과제



[참고] AI 확산 속도

AI는 대중화 · 산업화 되고 있으나, 조직의 전략·운영 체계가 이를 따라가지 못하며 기술과 실행 사이의 격차가 심화되고 있습니다.

주간 AI 사용자는 **약 8억 명**
(전 세계 인구의 10%)



에이전틱 AI 전략은
35% 만이 수립

AI 스타트업은 SaaS 기업보다
매출 100만 달러에서 3천만
달러에 도달하는 시간이
5배 빠르다

11% 의 조직만이 AI 에이전트를
실제 운영 단계 적용

추론 비용은
280배 감소
여전히 수천만 달러 규모의 비용이 발생

투자 불균형
기술에 93%

사람에 7%

운영 모델에 변화가
없다고 답한 리더는
단 **1%**에 불과

Source: Rebecca Bellan, "Sam Altman Says Chat GPT has hit 200M weekly active users,"TechCrunch, Oct 6, 2025; Deloitte Emerging Technology Trend in the Enterprise Survey; Wing Venture Capital, "AI growing faster than SaaS", Stanford Human-Centered AI Institute, "AI index Report 2025 ; Deloitte research on AI investment allocation patterns, 2025 Deloitte 2025 Tech Spending Outlook

CH 1. 피지컬 AI – AI와 로보틱스의 결합

AI는 정보를 생성하는 기술에서 현실을 움직이는 기술로 진화

Screen AI
정보처리 단계

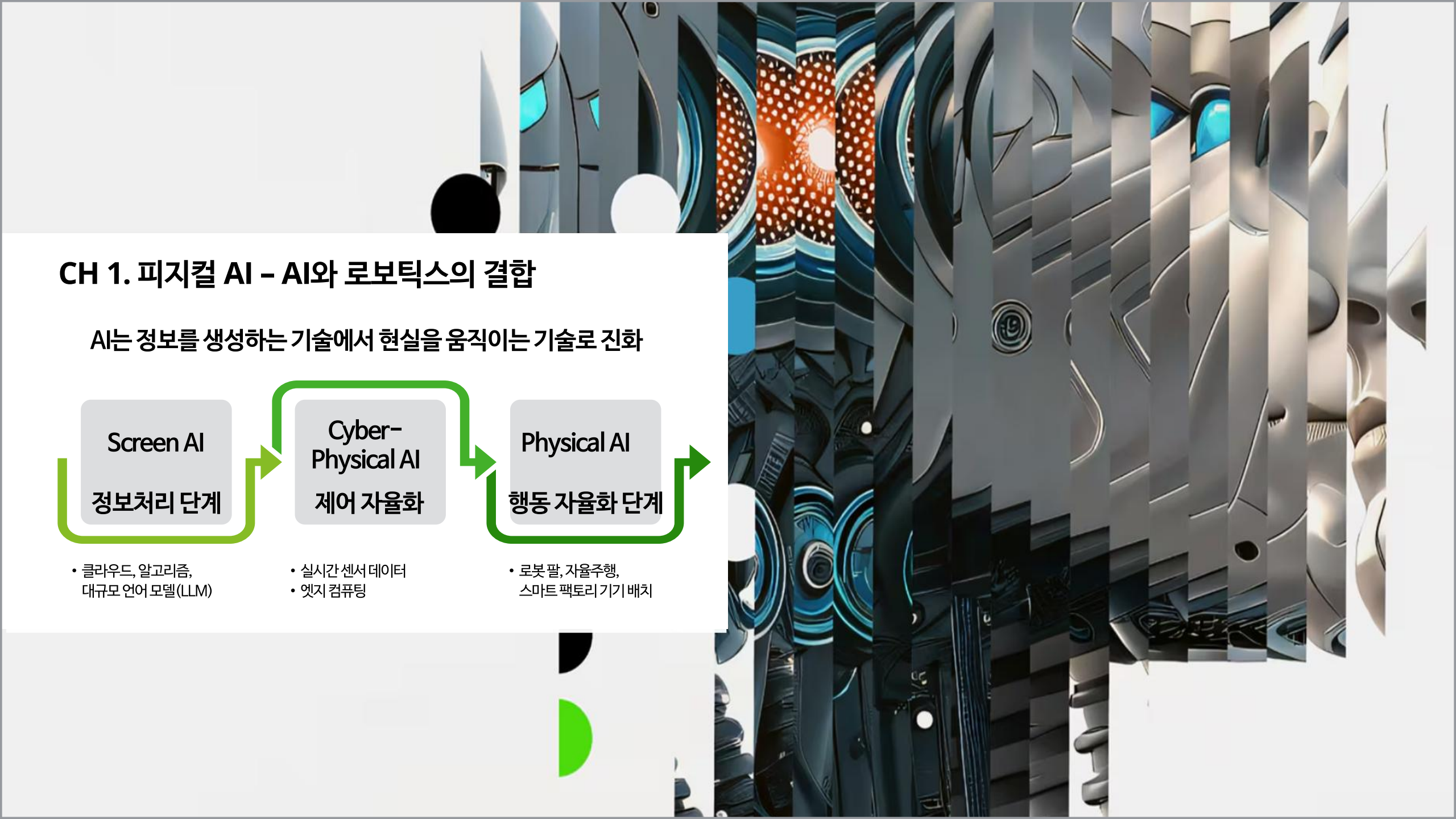
- 클라우드, 알고리즘, 대규모 언어 모델(LLM)

Cyber-Physical AI
제어 자율화

- 실시간 센서 데이터
- 엣지 컴퓨팅

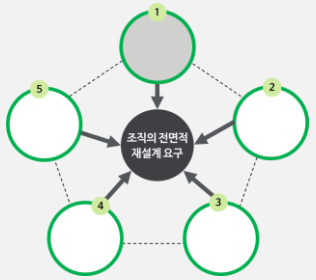
Physical AI
행동 자율화 단계

- 로봇 팔, 자율주행, 스마트 팩토리 기기 배치



1. 피지컬 AI – AI와 로보틱스의 결합 (1/2) – 피지컬 AI 등장과 상용화 사례

AI를 탑재한 기존 로봇들은 복잡한 환경을 스스로 인지, 학습 및 임무를 수행할 수 있는 '적응형 지능(Adaptive Intelligence)'을 갖춘 피지컬 AI로 진화하고 있으며, 현장 배치 단계로 진입해 이전과 다른 수준의 안전성과 정밀도를 실현하고 있습니다.



피지컬 AI의 정의와 본질

- 단순한 작업 자동화가 아니라 인지·추론·적응 기반 시스템
- 적응형 지능(Adaptive Intelligence) 시스템

상용화 및 미래 확산 전망

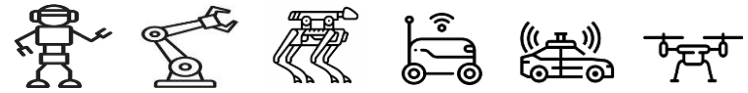
- (초기) 물류·제조·모빌리티 →(중장기) 헬스케어·에너지 등 전(全) 산업에 실전 배치
- 향후 10년 내 휴머노이드 로봇이 주류 기술로 부상
- (인간 개입 지속) Human in the loop 기반 신뢰 구조가 주류 모델

피지컬 AI의 등장

피지컬 AI는 자동화를 고도화 하는 기술이 아니라, 물리 환경을 이해하고 적응하는 시스템으로의 진화

기존 산업 로봇 (Rule Based Act)	피지컬 AI (Perceive-Reason-Act)
• 사전 정의된 동작 수행	• 실시간 인지·추론·행동
• 고정·통제된 환경 전제	• 복잡·비정형 환경 대응
• 반복 작업 중심, 순차적 처리	• 학습·적응 기반 작업
• 사전 정의된 자동화	• 병렬·상황 기반 의사결정

6대 핵심 폼팩터



피지컬 AI의 핵심 구현 기술

- VLA(비전-언어-행동) 모델 → 인식·이해·행동 통합
- 엣지 온보드 컴퓨팅(NPU) → 저지연 실시간 추론
- 센서·배터리·액추에이터·공간 컴퓨팅 발전
- 강화학습 + 모방학습 → 시뮬레이션-현실 학습 루프 연결

산업 확산 동인 및 상용화 사례

프로토 타입에서 실제 운영 단계로 진입 중

실전 배치 단계로 진입

- 전력망 점검, 수술 보조, 도심 자율주행, 스마트 물류창고 등 확산
  - -화면 속 알고리즘이 아니라 물리 공간에서 작동하는 실체
  - -자율·적응·학습 기반 시스템으로 전환 중

대표적 상용화 사례

- (Waymo) 로보택시 서비스로 1,000만 건 이상의 유료 주행 완료
- (Amazon) 100만 대 이상의 로봇을 운영하며, DeepFleet AI로 물류 이동 효율 10% 개선
- (BMW) 공장 내에서 신차가 스스로 조립 라인과 테스트 구간을 이동하는 자율 생산 환경 구축

상용화 촉진 요인

- 제조 인프라 성숙 → 대량 생산 가능, 적용 사례 증가
- 부품 범용화·오픈소스 확산 → 진입 장벽 하락
- 고성능 AI 칩 비용 부담은 여전히 존재하나 자율주행·드론·물류 중심으로 ROI가 검증된 영역부터 상용화 가속

1. 피지컬 AI – AI와 로보틱스의 결합 (2/2) – 피지컬 AI 도입 이슈와 확산 방향

피지컬 AI는 제도적·기술적 제약을 극복하는 과정을 거치면서 산업 전반으로 확산될 것으로 보이며, 휴머노이드와 차세대 로보틱스를 통해 인간 중심 환경의 구조적 변화를 이끌 것으로 예상됩니다.

피지컬 AI 도입 및 확산 과정의 주요 이슈와 과제

기술 자체보다 확장(scale) 과정에서의 문제가 핵심
➡ 전문가들은 Human-in-the-loop 구조가 당분간 필수적임을 강조

7 대 도전 과제

1	시뮬레이션 - 현실 간 성능 격차 (Sim-to-Real Gap)	• 시뮬레이션 학습 모델이 현실의 불확실성을 완전히 반영하지 못하는 구조적 격차
2	초저지연 실시간 처리 한계	• 자율주행차, 수술로봇 등은 밀리초 단위의 응답성 요구
3	안전·신뢰·책임 소재 문제	• 사고 발생 시 책임 주체·설명 가능성 문제
4	국가별 규제 상이성	• 자율주행, 의료 로봇, 드론 등은 국가별로 상이한 인허가 기준과 운영 규정을 적용
5	방대한 실시간 데이터 관리 문제	• 센서·3D·영상 데이터 폭증 → 엣지 클라우드 아키텍처 및 데이터 거버넌스 역량이 경쟁력
6	사이버 - 물리 통합 보안 리스크	• 디지털 침해가 물리적 사고로 연결 → 모델·센서·행위 단위까지 확장된 보안 설계 필요
7	이기종 로봇 플릿 오케스트레이션	• 개별 장비 성능보다 다종 시스템 통합·조율 역량이 핵심→ 플랫폼 중심 통합 제어 구조 필요

피지컬 AI의 확산 방향

안전·정밀·접근성이 중요한 영역에서 인간을 대체하기보다 보완하는 방향으로 확산

확산 방향 (산업 경계 붕괴)

- Physical AI는 물류를 넘어 다양한 산업으로 확장 중
  - 헬스케어: 로봇 수술, 자율 영상 진단 장비
  - 외식업: 조리·서빙·배달 로봇
  - 에너지: 고전압·위험 환경 점검 드론
  - 공공 부문: 교량·도로 점검, 자율 셔틀 서비스

휴머노이드 로봇 시장 전망

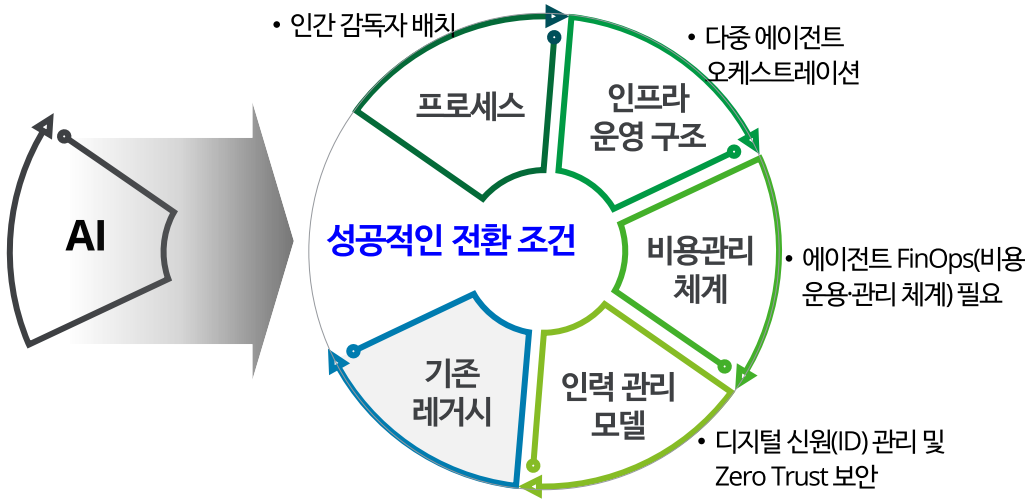
- 휴머노이드는 인간 환경(계단, 문, 작업대 등)에 최적화된 형태
  - 효율성보다 범용성 측면에서 강점
  - 에이전트형 AI와 결합 시 다단계 작업 계획, 실패 복구 및 인간과의 협업 능력 강화
- (UBS 전망) 2035년: 산업 현장 휴머노이드 200만 대 → 2050년: 3억 대
  - 단기적으로는 산업·물류·헬스케어, 장기적으로는 가정·돌봄·소비자 시장이 최대 기회

휴머노이드 이후 전망

- 상용화까지는 시간이 필요하지만, 로봇의 개념 자체를 재정의할 잠재력
  - 생체 조직과 결합한 바이오 하이브리드 로봇
  - 형태를 바꾸는 유동형 로봇
  - 양자 컴퓨팅과 결합한 Quantum Robotics

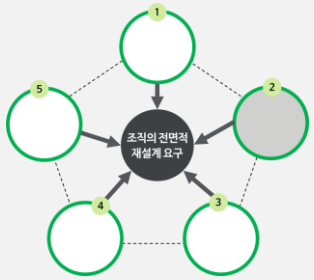
CH 2. 에이전틱 AI의 현실 적용 및 점검

명령(Command) 중심에서 자율적 루프(Loop)



2. 에이전틱 AI의 현실 적용 및 점검 (1/2) – AI 도입 파일럿의 함정

에이전틱 AI 도입의 핵심 과제는 기술 그 자체가 아니라 기존 운영 인프라와의 구조적 부적합에 있으며, 기존 프로세스를 단순히 자동화하는 접근만으로는 에이전틱 AI로의 전환을 성공적으로 달성하기 어렵습니다.



에이전틱 AI 파일럿 실패 사유

- 인간 중심 프로세스를 등한시
- 에이전트 AI를 자동화 관점으로 도입하면서 한계에 봉착
- 프로세스/운영 재설계, 에이전트 친화적 아키텍처와 거버넌스 동시 구축 필요

에이전틱 AI 운영 모델로 전환

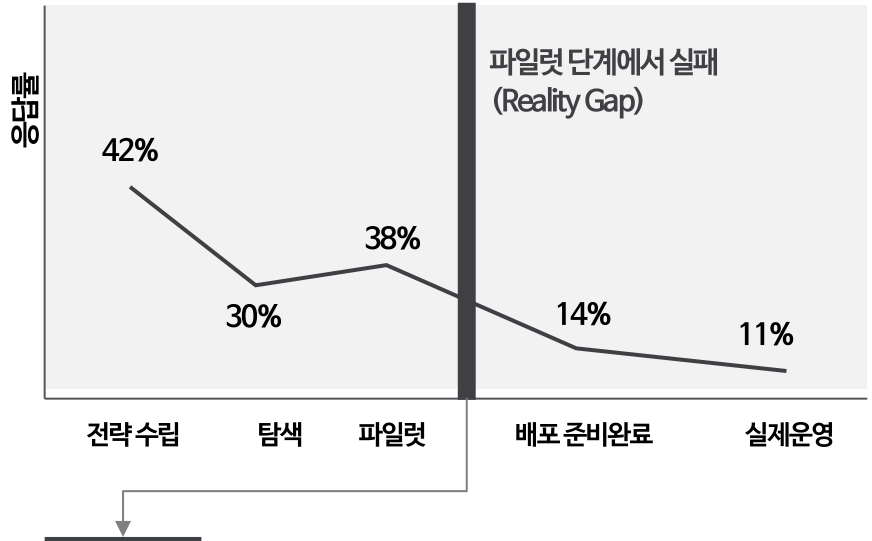
- 에이전트는 인력 대체가 아니라 노동력을 포함하는 운영 모델의 재설계
- 실리콘(에이전틱 AI) + 카본(인간)[1] 기반 혼합 조직이 경쟁력

에이전틱 AI 도입 현황 및 현실 격차

**파일럿에서 단계에서 실패,
실제 운영 단계 진입률은 단 11%에 불과**

- 2028년 업무 의사결정의 15% 자율화, 기업 SW의 33% 에이전트화(Gartner)

에이전틱 AI 도입 기업 현황에 대한 딜로이트 조사 결과[2]



현실 격차

- 전략 로드맵 수립 중 42%, 전략 없음 35%
- 파일럿→운영 간 'Reality Gap'

에이전틱 AI 도입 시 3대 인프라 장애 요인

**레거시 시스템의 한계, 데이터 아키텍처의 제약 및
거버넌스의 부재가 실패의 원인**

시스템	• 기존 엔터프라이즈 시스템은 에이전트 상호작용을 고려해 설계되지 않음 • 실시간 실행, 모듈형 구조, 현대적 API, 보안 ID 관리가 부족 • 가트너는 2027년까지 에이전트 AI 프로젝트의 40% 이상이 레거시 한계로 실패할 것으로 전망
데이터	• 실시간 맥락 파악이 어려운 구식 데이터 처리 방식 ETL[3] 구조→ 지식 그래프/인덱싱 체계로 전환 필요 • 기업의 약 절반이 데이터 검색성과 재사용성을 주요 장애로 지적
거버넌스	• 자율적으로 행동하는 시스템을 전제로 한 거버넌스 부재 • 많은 기업이 프로세스를 재설계하지 않고 단순 자동화에 머무름 • '에이전트 워싱(agent washing)'[4]으로 ROI 악화 • 잘못 설계된 에이전트는 업무를 늘리는 '워크슬롭(workslop)[5]' 유발

1) 인간은 탄소(carbon) 기반 생명체이고, AI 에이전트는 실리콘 기반 반도체 위에서 작동하는 인지 시스템으로, 업무의 기본 단위가 사람 1명이 아니라 사람과 여러 디지털 에이전트가 협업하는 하이브리드 팀으로 전환됨을 은유적으로 표현, 2) Deloitte (2025), Tech trends 2025, A perspective for the investment management sector ; 3) ETL은 데이터 처리의 전통적인 방식으로, Extract · Transform · Load를 의미 ; 4) 기존 자동화·룰 기반 시스템·단순 스크립트·챗봇을 '에이전트 AI'라고 포장하는 행위 ; 5) 더 많은 일·검증·조정·후처리를 만들어내는 현상

2. 에이전틱 AI의 현실 적용 및 점검 (2/2) – AI 에이전트 조직으로의 성공적인 전환 조건

AI 에이전트로의 전환은 단순한 기술 도입이 아니라 조직 전반의 운영 방식에 대한 전환이며, 성공하는 기업은 프로세스·운영·비용·인력 관리 역량을 선제적으로 갖춘 조직입니다.

에이전틱 AI 조직으로의 전환 방향

성공 기업은 '자동화'가 아니라 '운영 재설계' 를 채택

기존 방식	에이전트 네이티브 접근
• 기존 워크플로에 추가 • 단일 에이전트 • IT 거버넌스 • 자동화 도구	• 엔드투엔드 재설계 • 다중 에이전트 오케스트레이션 • 자율 시스템 거버넌스 • 실리콘 기반 노동력[1]

에이전트 중심 운영 체계(Agent-Native Operations) 구축

- 기존 워크플로우에 에이전트를 얹지 않고, 엔드투엔드 프로세스를 에이전트 기준으로 재설계
- 에이전트는 병렬 처리, 상호 협업, 맥락 전달이 가능
- 인간 중심 프로세스를 그대로 유지할 경우 에이전트의 강점을 활용할 수 없음
- (성공 사례) HPE는 내부 성과 평가 프로세스를 전면 재설계해 다중 에이전트로 구성된 'Alfred'를 도입

에이전틱 AI로의 성공적인 전환 조건

에이전트 도입은 '노동' 재 정의이며, 적절한 지점에 '인간 감독자(agent supervisor)' 배치와 프로세스·운영·비용·인력 관리 역량이 성공의 핵심

프로세스	혼합 노동력 (Mixed Workforce) 운영 모델	• **인간의 역할 변화: 단순 실행에서 거버넌스 감독 및 혁신 기획으로 이동** • Hybrid 체계: Moderna 사례 (CHRO-CTO 역할 통합을 통한 업무 계획 재설계) • 신뢰 확보: Mapfre, Moderna 등 사례 (민감 업무에 대한 Human-in-the-loop 상시 유지) → 하이브리드 인간 - 디지털 인력 모델이 실제
인프라 운영	다중 에이전트 오케스트레이션 (Orchestration)	• 구조: 범용 챗봇이 아닌 특화 에이전트들의 마이크로 서비스형 결합 • 표준 프로토콜: MCP, A2A, ACP 등을 통한 '에이전트 간 통신' 체계 구축
비용	에이전트 비용과 FinOps (비용관리체계 전면 재편)	• 에이전트는 상시 작동 → 잘못 설계되면 토큰/리소스 사용이 연쇄적으로 폭증 → 에이전트 FinOps(비용 운용·관리 체계) 필요 – 토큰 기반 비용 구조를 관리하는 에이전트 전용 FinOps(운영체계) 구축 – 실시간 비용 모니터링, 자동 확장·축소 등 AI 지출에 특화된 거버넌스 체계 구축
인력	실리콘 노동력 관리 프레임워크	• HR/운영: 디지털 온보딩 및 수명주기 관리 • 신원/보안: 에이전트 전용 디지털 신원(ID) 관리 및 Zero Trust 보안 • 성과/비용: 성과 관리 로그 및 에이전트 FinOps(토큰 기반 비용 모니터링)

1) 반도체(실리콘) 위에서 구동되는 AI 에이전트가 단순 도구를 넘어 자율적으로 업무를 수행하는 '디지털 노동 주체'로 기능하는 상태

CH 3. AI 인프라 전략의 재정립

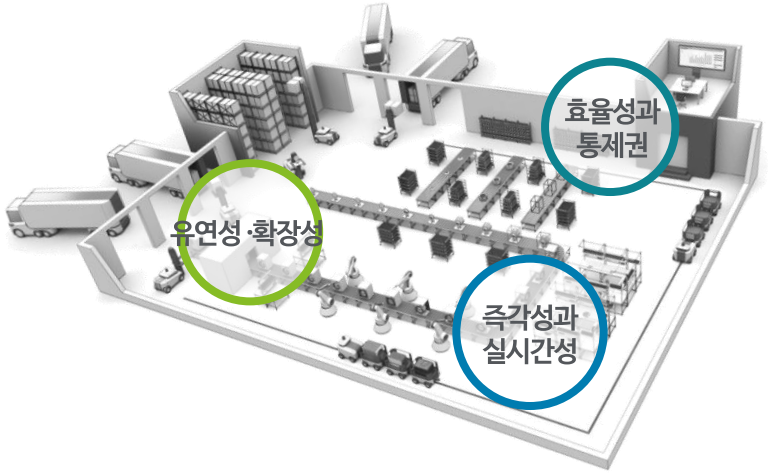
'클라우드 우선' 전략 재고 및 AI 팩토리 구축

하이브리드 AI 인프라 전략

워크로드별 Right-Sizing

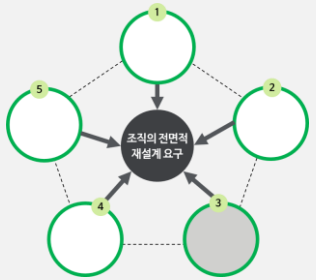
AI 팩토리 구축

AI Factory = AI를 위한 목적형 인프라 스택



3. AI 인프라 전략의 재정립 (1/2) – '클라우드 우선' 전략 재고

AI 확산으로 추론 비용은 급락했지만 '사용량(상시추론)'이 더 폭증하면서, 클라우드 우선 배치보다는 비용·주권·지연 민감도·회복력·IP를 동시에 만족하는 하이브리드 인프라가 필수가 되고 있습니다.



AI 인프라 재배치

- **(추론 비용)** 2년 전 대비 280배 하락, AI 사용량(에이전틱 AI의 상시 추론)급증으로 총 AI 지출 폭증
- **(데이터 센터)** 공냉·범용 워크로드 기준 → 특수 냉각(액체 냉각) 요구
- **(클라우드)** 비용 데이터 주권, 초저지연, IP 이슈로 하이브리드 · 온프레미스로 회귀

워크로드 재배치 및 AI 팩토리 구축 방향

- 3 계층 하이브리드 전략 추진 → 탄력성, 일관성, 즉각성 실현
- AI 전용 '그린필드' 인프라인 AI 팩토리 구축이 속도와 효율면에서 유리
- 운영자동화 및 조직 전환 지속

컴퓨팅 인프라 운영 이슈

AI 가 POC에서 운영으로 전환
→ 기존 인프라와 AI 수요 구조 불일치(mismatch) 발생

인프라 비용의 역설 발생

- PoC → 운영(Production) 전환 단계에서 기존 인프라 전략이 AI 수요(상시 추론·대규모 호출)와 부적합
- AI 워크로드는 반복·상시 추론을 전제로 하며, 클라우드 기반 서비스는 API 호출 증가 → 비용 급증
- 추론 비용은 2년간 280배 하락했지만, 총 AI 지출은 폭발적 증가(사용량 증가가 비용 하락을 압도)
  - 일부 기업은 월 비용이 수천만 달러 수준까지 증가
  - 상시 추론이 발생하는 에이전틱 AI가 가장 큰 비용 요인

워크로드별 전략 수립 요구

- 클라우드 비용이 온프레미스 구축 비용의 60~70% (임계점)를 초과시 전략적 판단 필요
  → 클라우드 일변도에서 탈피, 전략적 하이브리드 모델 채택
- 클라우드를 온프레미스로 옮기는 문제가 아니라, 워크로드별로 최적의 컴퓨팅 플랫폼을 선택하는 전략이 필요

컴퓨팅 인프라 재배치 방향

워크로드 중심의 3계층(Three-Tier) 배치

컴퓨팅 인프라 재고 요인

- **(비용)** 자본 투자(CAPEX)가 운영비(OPEX)보다 유리
- **(데이터 주권)** 소버린 AI가 인프라 투자 가속
- **(지연시간 민감도)** 자율주행 등의 경우는 10밀리초 이하의 응답 시간이 요구 → 클라우드 기반 처리는 한계
- **(회복력 요구)** 미션 크리티컬 업무는 클라우드 장애 대비해 온프레미스 요구
- **(지식재산권 보호)** 민감 정보를 AI에 이전하는 대신 AI 역량을 데이터가 있는 곳으로 이전하는 방식 선호

3계층 하이브리드 접근
(three-tier hybrid)

인프라의 거버넌스 확보 ⬇ 비용과 리스크 상시 평가 실행

1. **퍼블릭 클라우드: 유연성과 확장성 실현**
   - 용도: 워크로드 변동이 큰 AI 학습, 일시적 용량 확장(Bursting), 실험적 단계
   - 강점: 최신 AI 모델 및 서비스에 즉각 접근 가능, 인프라 관리 부담 최소화
2. **온프레미스: 효율성과 통제권 확보**
   - 용도: 대규모·상시 운영되는 프로덕션 추론(Inference)
   - 강점: 비용 예측 가능성 확보, 보안 및 성능에 대한 완전한 통제 및 역량 내재화
3. **엣지: 즉각성과 실시간성 실현**
   - 용도: 제조, 자율 주행 등 초저지연(Low-latency) 의사결정이 필요한 현장
   - 강점: 데이터 발생 지점에서의 로컬 처리를 통해 '찰나의 반응' 가능

3. AI 인프라 전략의 재정립 (1/2) – AI 팩토리 구축과 지능형 인프라 운영 모델

하이브리드 인프라의 본질은 '인프라 이전'이 아니라 '워크로드 배치 최적화'이며, 이를 가능케 하는 것은 AI 팩토리와 이를 운영할 조직의 역량입니다.

AI 전용 '그린필드' 인프라: AI 팩토리

AI Factory = AI를 위한 목적형 인프라 스택
→ 기존 환경 개조(Brownfield)보다 전용 환경 (Greenfield) 구축

목적형 스택		잉여 컴퓨팅
하드웨어 믹스	• GPU/CPU/NPU/TPU 혼합 아키텍처 구성 → 워크로드별 최적화	• (옵션) 서비스화로 수익화
지식 레이어	• 벡터DB·그래프DB·지식그래프 + 컨텍스트/데이터 파이프라인 → AI가 즉시 이해할 수 있는 데이터로 구조화	
네트워크	• GPU-to-GPU 통신(예: 고속 인터커넥트) → 고속화·초저지연 실현	
오케스트레이션	• 멀티모달 워크로드를 이질 플랫폼에서 통합 운영	

조직 역량 전환 (지능형 운영 모델)

워크로드별 Right-Sizing과 지능형 운영 역량의 내재화

조직 역량 전환을 위한 4대 핵심과제

1. AI-Infra Ops:
차세대 인프라 운영 숙련도

GPU 클러스터 관리	• 수천 개의 GPU가 하나처럼 작동하도록 병렬 연산 환경을 최적화하고 장애를 관리하는 기술
특수 냉각 기술 운용	• 고전력 GPU에서 발생하는 열을 제어를 위한 액체 냉각(DLC) 시스템 유지보수 및 열관리 역량
AI 관측 (Observability)	• 단순 서버 가동률을 넘어, 모델 추론 성능과 인프라 간의 상관관계를 실시간 모니터링하는 전문 도구 활용 역량

2. Network 재설계:
AI 중심의 초고속·저지연 설계

AI-First 트래픽 설계	• GPU 간(East-West) 대량 트래픽 패턴 이해 병목 현상을 제거
고대역폭/초저지연	• 인피니밴드(InfiniBand)나 고성능 이더넷을 활용 • 찰나의 지연도 허용하지 않는 네트워크 토폴로지 구축

3. Cost Engineering:
추론 경제 기반의 포트폴리오 최적화

GPU 활용률 극대화	• 워크로드에 따라 자원을 동적으로 할당하는 재무적·기술적 의사결정
하이브리드 비용 모델	• 클라우드와 온프레미스 간의 TCO(총소유비용)를 비교 분석하여 최적의 실행 지점 탐색

4. AI Ops Agents:
운영의 알고리즘화 및 자율화

지능형 장애 대응	• 에이전트가 수많은 알림을 요약하고 근본 원인을 추정한 뒤, 운영자에게 최적의 조치 시나리오를 추천.
실시간 최적화	• 워크로드 수요, 에너지 비용, 탄소 배출량을 알고리즘이 실시간 분석하여 리소스 조달과 배치를 자동화하는 '자율 운영' 단계로 진입

CH 4. AI 네이티브 조직으로 개편

AI는 IT 도입이 아니라 조직 아키텍처 재설계

Traditional IT
(서비스 관리자)

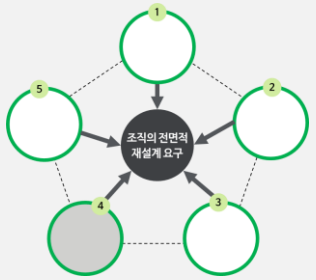
AI-Augmented IT
(자동화 운영)

AI-Orchestrated Enterprise
(인간+AI 에이전트 협업)

AI 중심으로 재설계

4. AI 네이티브 조직으로 개편 (1/2) – 기술 조직의 재편

AI는 단순한 기술 도구를 넘어 조직의 구조와 역할을 재편하는 촉매로 작용하며, 기술 조직을 비용 중심의 운영 기능에서 벗어나 비즈니스 전략과 수익 창출을 주도하는 핵심 조직으로 전환시키고 있습니다.



AI 로 인한 기술 조직의 핵심 변화 내용

- **우선순위** : 기술 예산 중 AI 비중 증가
- **인재:** AI 아키텍트, 인간-AI 협업 디자이너 등 신규 역할 급증
- **조직의 역할**: 비즈니스 전략을 이끄는 성장·수익 실현을 선도

기술 조직의 핵심 설계 원칙

- 레거시 패치 구조 탈피
- 디지털 문해력 전 직무 기본 역량화
- CIO - CFO - CSO 삼각 리더십 체계 조성
- 기술 소유보다 기술 조율 우선시
- 대담한 목표 설정 (POC 함정 탈피)

조직의 재설계 동인

AI는 도구가 아니라 조직 재설계의 촉매제
AI 확산은 기술 조직의 구조·역할·권한을 재정의 요구 증가

기술 조직의 전환 신호

- 아키텍처 수준의 통합 (78%)
  - -향후 5년 내 78%의 기술 리더가 아키텍처 워크플로에 AI 에이전트를 광범위하게 통합 의견
  - ➡AI를 추가 기능이 아리나 프로세스 설계 요소로 인식
- 투자 우선순위의 구조적 이동 (64%)
  - -64%의 기업이 향후 2년간 AI 투자를 확대할 계획
  - ➡전사 운영 모델을 AI 중심으로 재편
- 기술 예산 구조의 변화 (8% → 13%)
  - -기술 예산 중 AI 비중은 평균 8%에서 13%로 상승
  - ➡PoC 단계에서 핵심 전략 투자 영역으로 인식
- CIO 위상의 격상 (65%)
  - -CIO의 65%가 CEO에게 직접 보고하는 구조로 전환
  - ➡기술 조직은 지원 조직에서 전략 조직으로 변모

3대 핵심 변화 (AI가 재편하는 테크 조직)

조직의 구조 자체를 AI 중심으로 재설계

우선 순위 (Priorities)

- 단순 운영(IT)에서 비즈니스 전략 주도로 전환
- AI/데이터가 기술 조직 아젠다 최상단

인재 (People)

- 생성형 AI 대응 인력 확대 (약 70%)
- AI Architect 수요 30% → 58%
- Human-AI 협업 중심 직무 확대

존재 목적 (Purpose)

- 비용 센터에서 '수익 창출원(Revenue Generator)'으로 진화
- CIO는 점점 CEO의 전략 파트너로 이동

조직 재편 전략

- Problem-First: 기술 업그레이드가 아닌 '실제 비즈니스 문제 해결'에서 시작
- Modular Architecture: 변화에 즉각 대응 가능한 모듈형 및 관측 가능한 시스템 구축
- Human-Machine Synergy: 인간의 창의성과 AI의 속도를 결합한인재 전략 수립

4. AI 네이티브 조직으로 개편 (2/2) – AI 네이티브 조직의 설계 원칙

AI 네이티브 조직은 기술 구조, 운영 모델, 거버넌스 등 전 영역에 AI를 내재화함으로써, 인간의 창의성과 에이전트의 수행력이 결합된 '상시 진화형' 조직으로 전환하는 것을 목표로 합니다.

조직·아키텍처·리더십의 6대 전환 방향

01. 아키텍처: 모듈화 및 관측 가능성

- **레거시 패치 구조에서 AI 내재형 구조로의 전환**
  - 고정된 시스템이 아니라, 필요에 따라 부품처럼 교체 가능한 '모듈형 설계'
  - 시스템 내부 상태를 실시간으로 파악하는 '관측 가능성' 확보

02. 운영 모델: 프로젝트에서 제품 중심

- **일회성 과제 중심에서 가치 흐름 중심 조직으로의 전환**
  - Cross-functional Squad 운영 (개발·데이터·비즈니스 통합)
  - Forward-deployed Engineer 도입으로 현장 밀착 실행
  - AI 기반 지속적 계획·테스트·피드백 루프 구축

03. 인간과 에이전트의 협업 팀

- **인간과 AI의 협업이 기본 단위가 되는 조직**
  - AI Prompt Engineer, Synthetic Data Specialist 등 신 직무 등장
  - AI Architect, Edge AI Engineer 등 전문직 확대
  - 전 직무의 디지털 문해력(Digital Fluency) 기본 역량화

04. 거버넌스: 3M 프레임워크

- **사후 통제 방식이 아닌, 내재형 거버넌스**
  - Map: 활동과 의사결정 흐름 가시화
  - Measure: 성과·ROI·리스크 정량 측정
  - Monitor: 품질·윤리·보안 지속 모니터링
- 설명 가능성(Explainability)과 감사 가능성(Auditability) 설계 단계 내재화

05. 기술 조율 및 생태계 구성

- **내부 IT 공급자에서 생태계 오케스트레이터로의 진화**
  - 스타트업, Hyperscaler, 학계, 규제기관과의 협업 확대
  - 플랫폼 기반 파트너십 모델 확산
  - 개방형 혁신(Open Innovation) 강화

06. 상시 진화 및 베타 정신

- **변화가 일상이 되는 상시 학습 조직**
  - 변화는 이벤트가 아니라 상시 역량
  - "Fail fast, learn faster" 문화 정착
  - 소규모 POC에 머무르지 않고 대담한 목표 설정

미래 기술 조직의 공통적 특징

기술 조직은 비용 센터를 넘어 전사 전략·프로세스·운영·인재 역량 관리를 주도하는 조직으로 전환

전략	• 생태계 조율하고 변화의 일상화
프로세스	• AI가 아키텍처에 내재화
운영	• 운영 모델이 제품 중심으로 재편
인재	• 인간과 에이전트가 협업 단위

리더를 위한 Action Plan

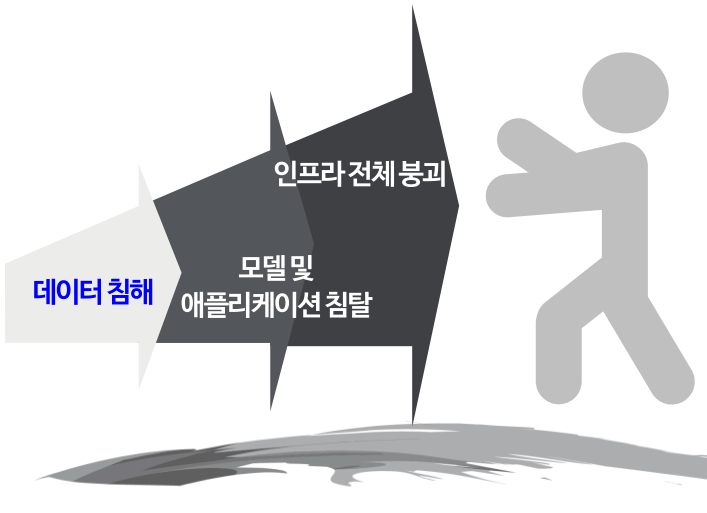
- Vibe Shift (인식 전환): AI 거부 대신 학습을 통한 '자율적 팀' 구축
- Role Shift (역할 변화): 인프라 관리자에서 'AI 오케스트레이터'*로 진화
- Now is the Time (즉시 실행): 성능 고도화 대기보다 '현재 기술로 즉시 성과' 창출

CH 5. 사이버 보안의 딜레마

공격도 방어도 AI의 기계적 속도로

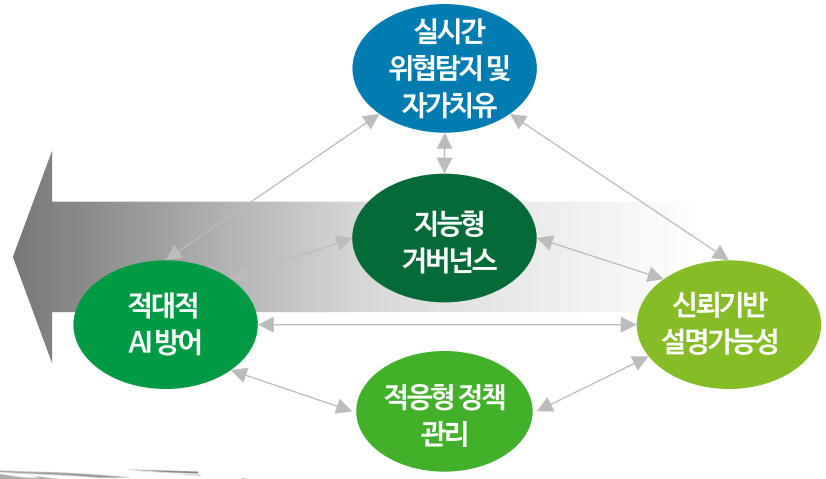
AI 를 활용한 사이버 공격

인프라 전 계층의 붕괴



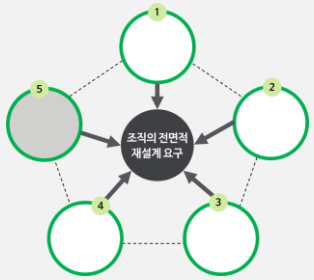
AI 위협에 대한 핵심 방어 전략

AI-네이티브 보안과 고도화된 거버넌스



5. 사이버 보안의 딜레마 (1/2) – 사이버 위협의 식별

AI 보안의 문제는 '새로운 위협'이 아니라, 기존 보안 방식이 AI를 전제로 설계되지 않았다는 데 있습니다.



위협의 진화와 대응 프레임워크

- AI를 전제로 한 보안 체계 재 수립
- 내 · 외부 위협 및 시스템에 내재된 리스크 관리 필요성 증가
- 4대 보안 영역(데이터, 모델, 앱, 인프라)별 리스크 관리 요소 식별

AI 를 활용한 사이버 전략 증강

- AI 기반의 능동적 방어 (AI-Native Defense) 체계 구축
- 미래 위협 시나리오 및 대비책 (Future Outlook) 마련

AI가 만든 새로운 보안 역설

AI는 생산성과 혁신을 가속화 하지만
새로운 보안 사각지대 발생

AI 확산

- LLM
- 에이전틱 시스템
- 멀티모달 AI

보안 체계 설계 시 고려사항

공격 표면 확대 ⬇ 기존 보안 경계 무력화	• LLM·에이전틱 시스템 확산 → 데이터 집중 지점 증가 • 멀티모달 AI (텍스트·음성·영상) → 새로운 공격 벡터 생성
AI가 만든 취약성을 AI가 다시 방어	• 자동화된 공격 확산 가능성 • 적응형 지속 공격 (Adaptive Persistent Threat) • 모델 조작·프롬프트 인젝션 리스크
사후 대응 (reactive security) 무용	• AI는 학습·적응·확산 → 대응 지연 시 피해 규모 기하급수 확대 • 자율 에이전트 확산 → 통제 복잡성 증가 • 단일 취약점이 전사·산업·물리 인프라까지 파급 가능

AI로 인해 확대되는 주요 보안 위험 영역

AI 보안 위험은 데이터 – 모델 – 애플리케이션 – 인프라
전 계층의 붕괴로 확산 가능

데이터	• LLM 학습·추론 과정에서 민감정보 노출 • 학습 데이터 조작을 통한 모델 왜곡
모델	• 모델 조작 (Model Manipulation) → 파라미터 변조·프롬프트 인젝션 • 적대적 공격 (Adversarial Attacks) → 입력값 교란, 오판 유도 • 모델 드리프트 (Model Drift) → 시간이 지남에 따라 성능 저하 및 오판 • 설명 가능성 부족 (Opacity Risk) → 규제 대응 어려움 • 모델 탈취 (Model Extraction) → API 호출을 통한 모델 복제
어플리케이션	• 프롬프트 인젝션 공격, API 남용 및 무단 접근 • 에이전틱 시스템 오남용 및 권한 관리 실패
인프라	• GPU·고성능 컴퓨팅 자원 집중화, 클라우드/온프레미스 하이브리드 복잡성 → 단일 인프라 침해가 다중 시스템 붕괴로 확산 가능 • 공급망 공격 (Supply Chain Attack) 시 위성·통신·전력 인프라 연계 리스크로 확산

5. 사이버 보안의 딜레마 (2/2) – 미래 방어 전략 : AI-네이티브 보안과 고도화된 거버넌스

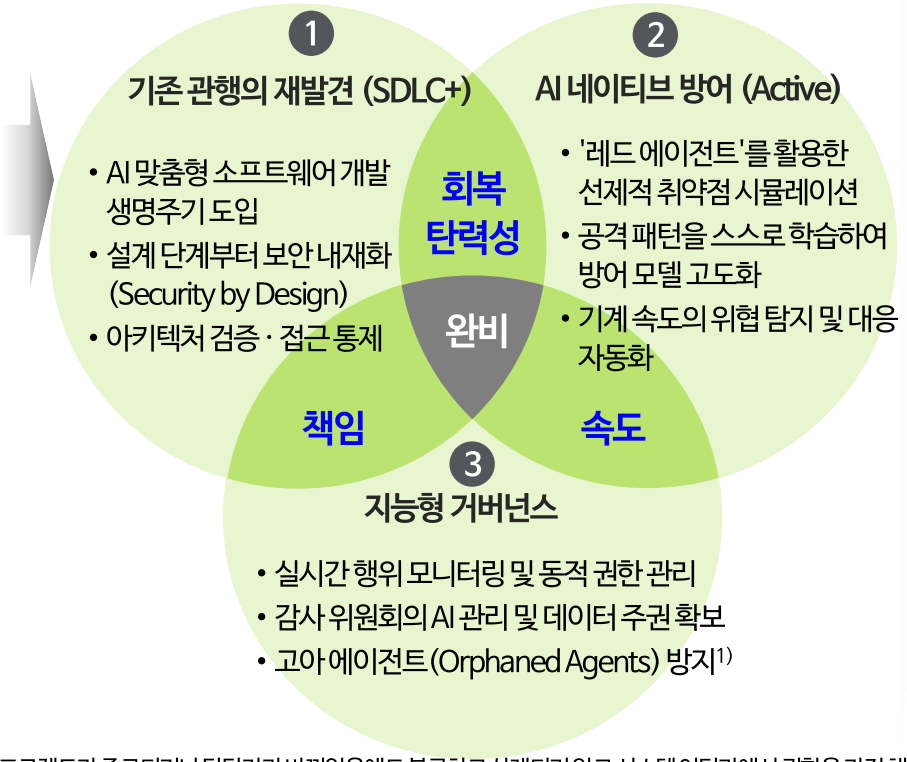
AI 위협에는 AI 기반의 자동화된 방어로 맞서되, 그 이면의 신뢰와 책임은 설계 단계부터 내재화된 정교한 거버넌스를 통해 확보해야 합니다.

AI 위협에 대한 핵심 방어 전략

AI 위협 대응의 핵심은 개별 기술의 도입이 아니라,
회복 탄력성(Proactive Resilience)·속도(Velocity)·책임(Accountability)의 유기적 통합

AI 위협의 본질

- **보호의 난제:** AI는 데이터와 연산이 결합된 구조로, 표준 트래픽과 유사해 탐지가 난해 (by 산미 코예조 스탠퍼드대 교수)
- **기존 방식의 한계:** 기존 보안 원칙으로 기계의 속도와 대규모 영향력에 대응하기에는 한계
- **AI의 역설:** AI는 새로운 취약점을 생성하는 동시에, 배가된 방어력 (Force Multiplier)
  - – 탐지 역량의 배가: 초당 수백만 개의 데이터를 분석해 위협
  - – 대응 속도의 가속 및 레버지지 효과 : 밀리초(ms) 단위로 즉각 처리



미래 리스크 전망 및 대응 로드맵

AI 보안 설계는 회복력, 자율통제 시스템,
거버넌스 신뢰 구조 확보로 실현

1 단계 — 인프라 회복 탄력성 확보

- **선제적 회복 탄력성 → 인프라 파괴 방어**
  - –AI 인프라의 설계 단계(SDLC+)부터 수동 제어 백업이라는 회복 탄력성(복원력) 마련 및 유지
  - ➡위협 현실화 전 '예측'과 '사전 대응 ' 및 사후 '복원력 '

3 단계 — 초고속 자율 통제 시스템 구축

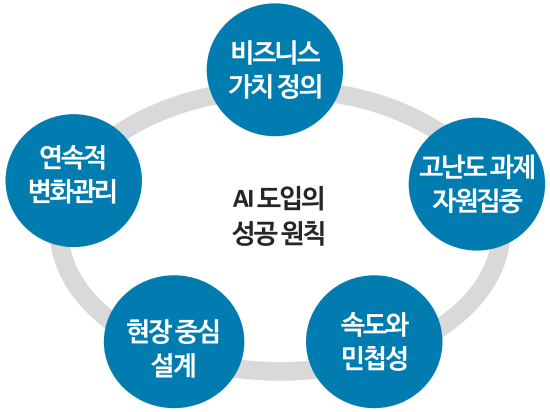
- **기계의 속도에 대응하는 지능형 방어 시스템 구축 → 사이버 공격에 자율 교전 및 압도**
  - –사람이 아닌 '적응형 방어 아키텍처'가 스스로 의사결정
  - –시스템이 시스템을 감시하는 Automated Guardrails(자동화된 통제) 역량 확보

3 단계 — 거버넌스 신뢰(책임) 구조 조성

- **보안 체계를 지속 유지 시키는 거버넌스 모델 구축 지속 → 지속적·내재형 거버넌스**
  - –이사회·감사위원회의 AI 감독 역할 강화
  - –국경 간 AI 운영 시 데이터 주권과 규제 대응 필수

1)특정 목적(예: 데이터 분석, 고객 응대)을 위해 생성되었으나, 프로젝트가 종료되거나 담당자가 바뀌었음에도 불구하고 삭제되지 않고 시스템 어딘가에서 권한을 가진 채 방치된 AI 에이전트를 의미

결론: AI 진화에 따라 추적해야 할 기술
– 딜로이트 제언: 성공 하는 리더들의 5가지 실천 원칙



[결론] AI 진화에 따라 추적해야 할 기술 (1/2) : 모델의 정체와 하드웨어의 진화

모델 중심에서 운영·데이터·엣지 중심으로, AI 경쟁력의 핵심이 이동하고 있습니다.

[결론] AI 진화에 따라 추적해야 할 기술 (2/2) : AI 인터페이스와 보안의 진화

변화의 확실한 예측보다, 신호를 감지(Sense)하고 즉각 평가(Evaluate)하여 AI의 기계적인 속도로 대응(Respond)하는 조직 역량이 성패를 결정할 것입니다.

AI 인터페이스: 새로운 폼팩터와 '에이전트'의 등장

AI 네이티브 웨어러블의 도전

- (시장 규모) 2026년 기준 2,654억 달러 규모로 급성장
- 스마트폰 기능의 확장 VS. 독립 AI 기기 (펜던트, 안경 등)의 탄생에 대한시장 검증 중

성공 여부는 미정, 프라이버시·차별성 관건

AI 에이전트와 '동의의 역설 (Consent Paradox)'

- 초개인화된 편의성을 위해 '과거 이력, 위치, 금융' 등 민감 데이터를 필수적으로 개방해야 하는 구조
- 학습 모델에 데이터의 '영구적인 흔적' 으로 데이터 삭제권(Right to erasure) 실현이 불가능

기능을 위해 허용 vs 프라이버시 위해 거부 논쟁 심화

보안 및 마케팅: 신뢰 기반의 새로운 질서

생체 인증 중심의 신뢰 보안 (Trust Security)

- AI가 복제하는 목소리·문서(딥페이크)가 정교해지며 '디지털 증명' 무력화
- CISO 92%가 패스워드 없는 하이브리드 인증 체계로 전환 중

생체 인증 '단독'이 아닌 하이브리드(보완형) 접근이 유력

SEO[1]에서 GEO로의 이동 (Generative Engine Optimization)

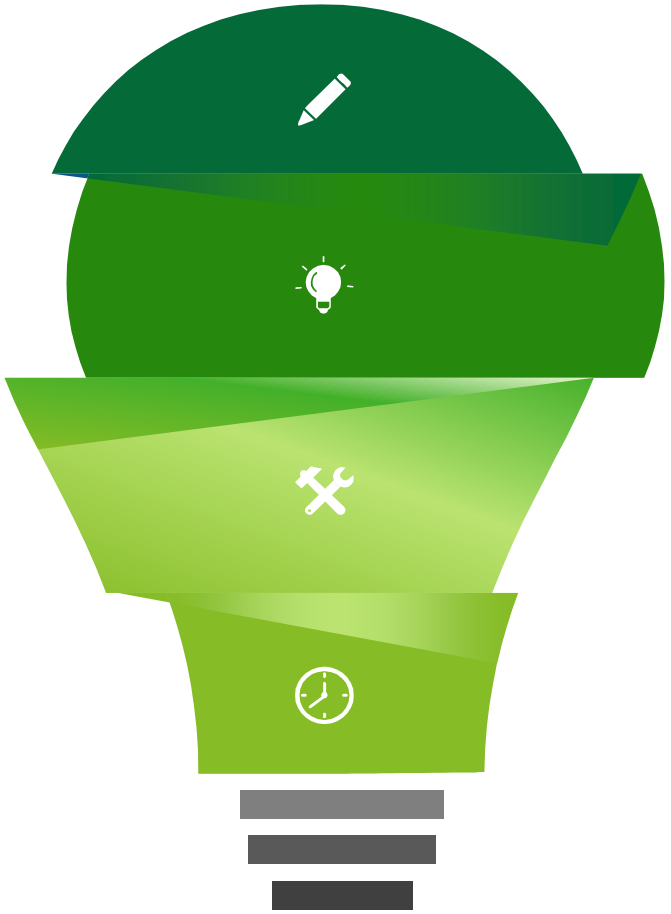
- 사용자는 전통 검색보다 AI 챗봇/AI 답변으로 이동
  - AI 생성 답변 확산으로 기존 웹사이트 클릭률이 1/3 이상 감소
  - AI 플랫폼으로 유입하는 오가닉 트래픽[2] 6.5% → 1년 내 14.5% 전망

기존 웹사이트 클릭률(CTR) 급락에 따른 마케팅 재설계 필요

1) SEO는 Search Engine Optimization로, '검색 엔진 최적화' 의미 ; 2) 광고비를 내지 않고 '자연스럽게' 유입되는 방문자 트래픽을 의미, 반대개념으로 Paid Traffic: 광고(검색 광고, 배너, SNS 광고 등)로 들어오는 트래픽

딜로이트 제언 – 성공하는 리더들의 5가지 실천 원칙

AI 를 성공적으로 도입하고 있는 선도사들에게는 5가지 공통된 패턴이 발견되고 있습니다. 특징은 가장 정교한 기술을 보유한 곳이 아니라 기존 프로세스를 과감히 재설계할 용기와 실행할 속도를 가진 조직이 승자의 반열에 오른다는 점입니다.



01

- **기술 과잉을 경계하고 비즈니스 본질에 집중 (Focusing on Business Essence over Technology)**
  - 혁신의 진정한 동력은 화려한 기술의 도입이 아닌, 해결해야 할 '비즈니스 페인 포인트 (Pain Point)' 로부터 시작
  - 명료한 가치 제안 (Value Proposition) 과 기대 성과에 대한 정의가 결여된 투자는 매몰 비용으로 귀결

02

- **고난도 핵심 난제에 대한 전략적 자원 집중 (Strategic Concentration on Critical Challenges)**
  - 단기성 소규모 PoC (개념 증명) 의 반복적 수행에서 벗어나, 기업의 경쟁 우위를 결정지을 수 있는 전략적 핵심 과제에 자원을 집중
  - 비즈니스 임팩트가 미미한 과제보다는 조직의 성장을 가로막는 고난도 난제를 해결할 때 비로소 진정한 혁신의 동력이 확보

03

- **속도와 민첩성 중심의 실행력 확보 (Prioritizing Agility over Theoretical Perfection)**
  - 완벽한 이론적 정립보다 신속한 실행과 시장 진입 (Time-to-Market) 을 채택
  - 실패의 리스크를 원천 차단하기보다, '빠른 학습 (Fast Learning)' 을 거쳐 리스크 해소

04

- **현장 경험과 결합된 사용자 중심의 솔루션 설계**
  - 기술의 효용성은 현장 실무자의 실제 워크플로우 내에서 증명되어야 함
  - 설계 단계부터 사용자의 수용성 (Adoption) 을 최우선으로 고려할 때 기술은 비로소 현장의 성과로 치환

05

- **필요 (Needs) 중심의 연속적 변화 관리 (Needs-Driven Continuous Transformation)**
  - 변화를 일회성 과업이 아닌 끊임없는 진화의 과정으로 내재화
  - 무엇을 할 수 있는가 라는 기술 중심의 사고에서 무엇을 해야 하는가 라는 필요 중심 사고로 전환

Deloitte.

딜로이트 인사이트 카카오 채널 & 앱

전 세계 경제·산업·경영 트렌드와 인사이트를

실시간으로 확인하세요!

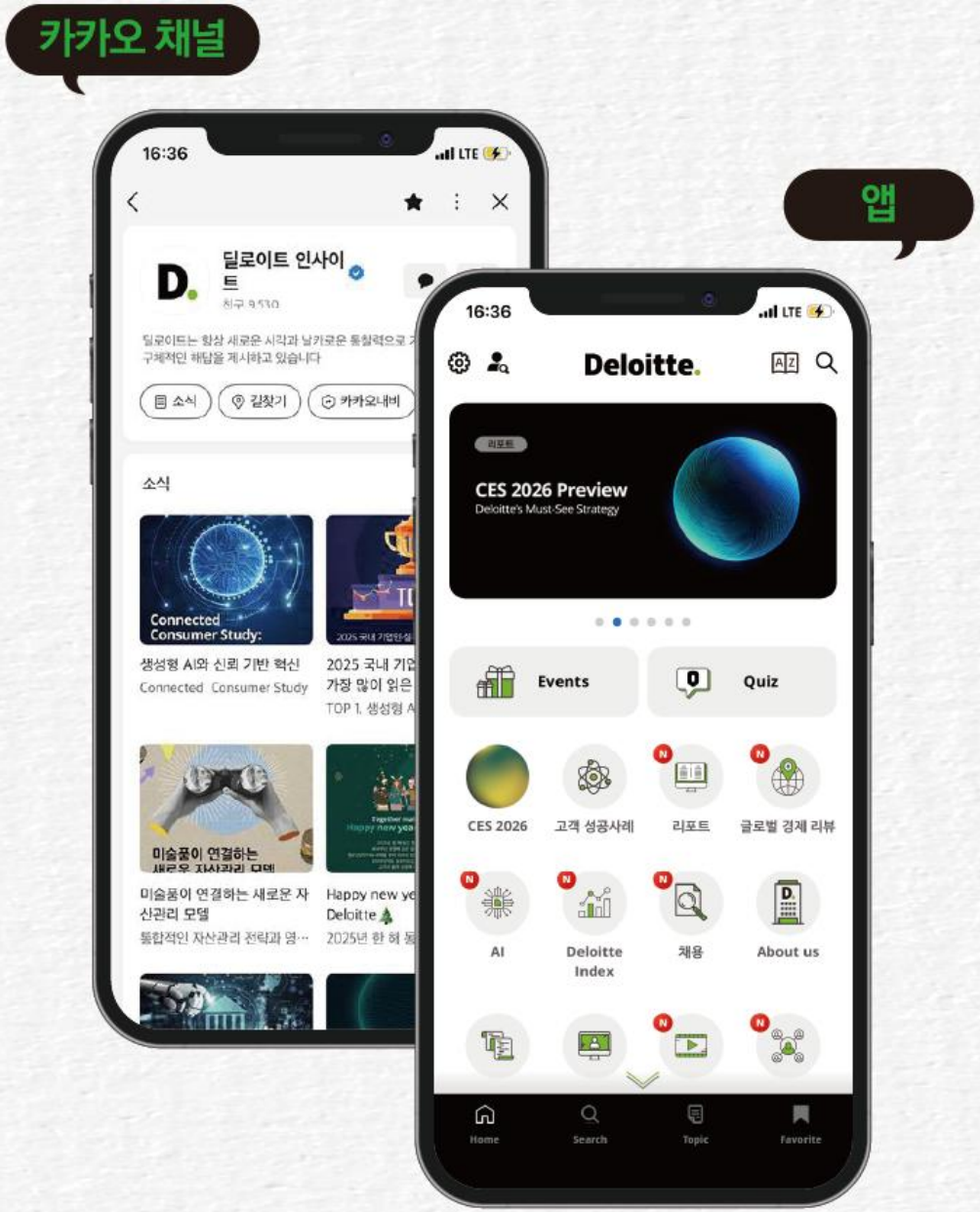
- AI 시대의 전략과 리스크, 산업별 핵심 이슈를 다룬 **분석 리포트**
- 소비심리지수·자동차 구매의향 등 실물경제의 향방을 보여주는 **Deloitte Index**
- 딜로이트 전문가의 인사이트와 글로벌 행사의 현장을 담은 **영상 콘텐츠**
- 글로벌 프로젝트에서 검증된 실행 인사이트를 담은 **고객 성공 사례**

카카오채널

앱

Download on the App Store

GET IT ON Google Play



앱스토어, 구글플레이/카카오톡에서 **'딜로이트 인사이트'** 를 검색해보세요.
더욱 다양한 소식을 만나보실 수 있습니다.

Deloitte. Insights

성장전략부문 대표	딜로이트 인사이트 편집장	연구원	Contact us
손재호 Partner	박경은 Director	배순한 Director	krinsightsend@deloitte.com
jaehoson@deloitte.com	kyungepark@deloitte.com	soobae@deloitte.com	