2026.04.03

Memory Watch

이승우_swlee6591@
박재환_jaehwan124@

클로드 코드 소스 유출에 나타난 시사점: AI는 기억 운영 시스템으로 진화 중

❝ **What's New:**

현지 시간 3월 31일 Anthropic의 개발 도구 Claude Code v2.1.88의 배포 과정에서 내부 소스코드가 외부에 노출되는 사건이 발생. 소스는 유출되었지만, 사용자 데이터는 유출되지 않을 것으로 파악됨.
사태 파악 이후 곧 삭제가 진행됐지만, NPM(Node Package Manager) 패키지 내의 512,000라인의 TypeScript 코드가 이미 GitHub를 중심으로 확산되었고, 그 핵심 내용들도 일제히 모두 분석됨.
Claude Code는 코드는 출시 수개월 만에 ARR 25억달러를 달성한 상용화 제품인데, 그 핵심 설계도가 그대로 공개된 사건.

Key Findings & Analysis

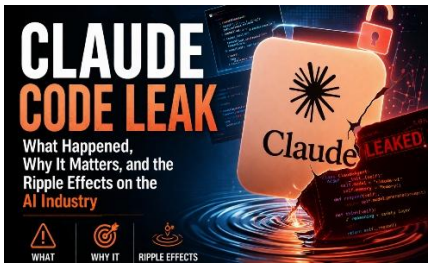
Claude Code의 내부 구조는 우리가 알고 있던 기존의 AI와 달랐다. 아이러니컬하게도 이 시스템은 더 많은 것을 기억하지 않는다. 오히려 기억을 줄이고, 이를 외부에 분산시키며, 필요할 때만 이를 불러오는 구조다.
또한 이 시스템은 자신을 믿지 않는 특성이 있었다. 즉, 기억을 확정된 "사실"로 보는 것이 아니라 "힌트" 또는 "단서"로 취급하며, 이를 항상 다시 검증하며, 틀린 기억은 그대로 비워 버리는 식이다.
또 하나의 중요한 차별점은 "항상 작동하는 AI"라는 점이다. KAIROS라는 구조를 통해 시스템은 사용자가 떠난 이후에도 계속 작동 모드를 유지하며, 정보를 정리하고, 모순을 제거하고, 지식을 재구성한다.

❝ **So What?**

좀 과장되게 말하자면 클로드 코드는 단순한 기억하는 기계를 넘어 기억 운영시스템(OS)으로 진화하고 있는 것처럼 보인다. 이러한 차이는 시간이 지날수록 산업 전체를 뒤흔드는 변화가 될 가능성이 있다. Claude Code에 나타난 AI의 진화 방향을 볼 때, 앞으로 점점 더 다음과 같은 요인들이 중요해질 가능성이 높다.

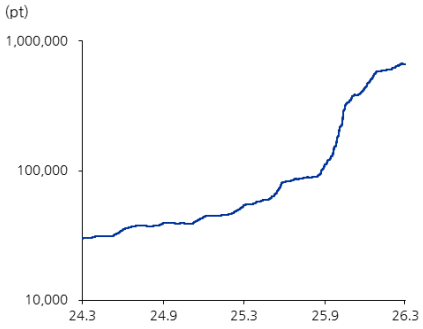
첫째, 단순한 Peak 성능보다 가동률을 높이는 시스템,
둘째, 외부 메모리 및 스토리지 수요 증가,
셋째, 각 디바이스에 대한 고품질 고속 연결성,
넷째, 검증 루프 회로를 위한 SRAM와 온칩 메모리 중요성 증가

Claude Code Leak 사고



자료: linked-in

DXI 지수



자료: DRAM Exchange, 유진투자증권

유진투자증권

Claude Code 소스 유출 사건과 AI 발전 방향의 시사점

보이지 않는 운영체계의 탄생

인류는 오랫동안 도구를 만들어왔다. 돌을 깎아 창을 만들었고, 금속을 녹여 기계를 만들었으며, 전기를 길들여 계산기를 만들었다. 그리고 이제, 우리는 생각하는 도구를 만들었다. 그러나 대부분의 사람들은 여전히 착각하고 있다. 이 새로운 도구의 본질이 '지능'이라고. 이번 Anthropic 의 Claude Code 사건은 그 착각이 얼마나 피상적인지를 드러낸다.

지능은 이미 문제가 아니다

우리는 지난 몇 년 동안 하나의 질문에 집착해왔다. "어떤 모델이 더 똑똑한가?" 더 정확한 답변, 더 자연스러운 문장, 더 빠른 코드 생성. 이 경쟁은 마치 과거 산업혁명 시기, 더 강한 증기기관을 만들기 위한 경쟁과도 같았다. 그러나 이제 상황은 달라졌다. 지능은 더 이상 희소하지 않다. 지능은 점점 범용화되고, 가격은 떨어지고, 접근성은 높아진다. 문제는 더 이상 '얼마나 잘 생각하는가'가 아니다. 문제는, 그 생각이 어떻게 실행되고, 얼마나 통제되는가이다.

사건의 본질: 코드 유출이 아니라 '설계 철학의 노출'

이번 사건에서 유출된 것은 단순한 코드가 아니다. 그것은 하나의 청사진이다.

- tool orchestration
- permission governance
- memory layering
- agent runtime

이 모든 것은 하나의 메시지를 가리킨다. AI 는 더 이상 질문에 답하는 존재가 아니다. AI 는 이제 환경 속에서 지속적으로 작동하는 행위자(agent)가 된다. 한 번 호출되고 사라지는 것이 아니라, 계속해서 관찰하고, 판단하고, 실행하며, 기억한다. 이것은 단순한 기술적 진보가 아니다. 이것은 "도구"에서 "행위 주체"로의 전환이다.

인간이 만든 또 하나의 운영체계

인류는 이미 두 번의 거대한 운영체계를 만들어낸 적이 있다. 첫 번째는 생물학이다. DNA 는 수십억 년 동안 생명을 운영해온 코드였다. 두 번째는 사회다. 법, 화폐, 국가, 기업은 인간 집단을 운영하는 소프트웨어였다. 그리고 지금, 우리는 세 번째 운영체계를 만들고 있다. 바로 "Agent OS"이다.

Claude Code 의 구조는 그것이 이미 시작되었음을 보여준다. 이 시스템은 단순히 계산하지 않는다. 그것은 작업을 분배하고, 권한을 관리하며, 기억을 유지하고, 행동을 조정한다. 즉, 작은 사회를 내부에 품은 시스템이다.

경쟁의 축이 이동한다

이제 경쟁은 더 이상 모델의 IQ 가 아니다. 경쟁은 보이지 않는 영역으로 이동한다. 누가 더 정교하게 tool 을 호출하는가. 누가 더 안전하게 권한을 통제하는가. 누가 더 효율적으로 memory 를 관리하는가. 누가 더 신뢰 가능한 execution 을 보장하는가? 이것은 기술적 문제이면서 동시에 정치적 문제다. 왜냐하면, 모든 권한 관리 시스템은 결국 "누가 결정권을 가지는가"에 대한 문제이기 때문이다.

기업은 '자동화'가 아니라 '통제'를 산다

일반 사용자는 자동화를 원한다. 버튼 하나로 모든 일이 해결되기를 바란다. 그러나 기업은 다르다. 기업은 묻는다. 누가 이 결정을 승인했는가?, 기록은 남아 있는가? 문제가 생기면 되돌릴 수 있는가? 책임은 누구에게 있는가? 기업은 '통제 가능한 지능'을 돈을 주고 사게 된다. 이것이 바로 Controllable AI 가 프리미엄을 가지는 이유다.

이번 사건의 역설

아이러니하게도, 이 사건은 Anthropic 의 약점을 드러냈다. 그 약점은 모델의 안전성이 아니었다. 그것은 훨씬 더 인간적인 문제였다. build artifact 관리, release pipeline, source map 제거 실패의 문제였다. 즉, 지능은 초월했지만, 운영은 아직 인간 수준에 머물러 있다. 이것은 하나의 중요한 경고다. AI 시대의 신뢰는 더 이상 "이 모델이 안전한가?"로 결정되지 않는다. 앞으로의 질문은 이것이다. "이 시스템은 제대로 운영되고 있는가?"

시장의 재편: 모델에서 운영체계로

우리는 지금 전환점에 서 있다.

과거: Model competition → 미래: Agent OS competition

그리고 그 위에 새로운 계층이 쌓인다.

- governance
- audit
- policy
- memory control

이 계층은 눈에 잘 보이지 않는다. 그러나 매우 높은 가치를 가진다. 이 계층을 잘 컨트롤하고 조화시키는 것이 가장 중요한 키가 될 것이다. 그래서 이제 AI 는 더 이상 단순한 연산 문제가 아니다. 그것은 점점 memory 중심 구조, storage 중심 구조, distributed system 로 이동하고 있다. 즉, AI 는 '계산'이 아니라 "상태(state)를 유지하고 관리하는 문제"가 된다.

새로운 권력의 형태

인류는 항상 새로운 권력을 만들어왔다. 농업은 토지를 권력으로 만들었고, 산업은 자본을 권력으로 만들었으며, 정보화 시대는 데이터를 권력으로 만들었다. 그리고 이제, 통제 가능한 실행 시스템이 권력이 된다

누가 더 똑똑한 AI를 만들었는가가 아니라, 누가 더 안전하게, 더 신뢰 가능하게, 더 지속적으로 그 AI를 '운영'할 수 있는가. 이번 사건은 그것을 보여준다.

AI 가 "저장 + 검색 + 체크 시스템"으로 변하는 순간, 산업의 중심도 함께 이동하게 될 것이다. 더 많은 데이터를 저장하고, 더 빠르게 꺼내고, 더 효율적으로 재구성할 수 있는 지로 말이다, 그리고 이와 관련된 핵심 기술들이 새로운 투자 후보군으로 떠오르게 된다.

그래서 우리는 이제 NAND 와 SSD 를 다시 보고, 기존 DRAM 에 대해서도 재평가를 해야 할 필요가 생겼다. 또한 네트워크에 대해서도 기존과는 다른 각도에서 바라봐야 한다. 이들은 더 이상 GPU 를 위한 보조 부품이 아니다. 그들은 이제 더 진화된 지능을 구축하기 위한 핵심 기반이 된다.

GPU 는 여전히 중요할 것이며 HBM 도 여전히 필수적일 것이지만, GPU 에 집중되어있던 권력은 점차 분산되고 있다. 메모리와 스토리지, 그리고 네트워크가 그 권력을 나누기 시작했다. 이것은 GPU 몰락이 아니다. 새로운 AI 를 위한 새로운 질서의 재편인 것이다. 그리고 그 아래에서, 더 조용한 변화가 진행되고 있다. CXL, 메모리 확장, 분산 메모리 구조. AI 가 하나의 장소에서 작동하는 것이 아니라, 여러 계층의 기억 위에서 움직이기 시작할 때, 이 기술들은 필수가 된다.

AI 시대가 열리면서 우리는 “누가 더 빠르게 많을 것들을 계산하는가”를 물어왔다. 그러나 이제 질문은 바뀐다. “누가 더 잘 기억하고, 더 빠르게 찾고, 더 정확하게 재구성하는가”로 말이다. 그리고 이 질문에 대한 답이 다음 반도체 산업의 승자를 결정할 힌트가 될 것이다. 이제 지능의 중심은 연산에서 기억과 네트워크로 점차 이동하고 있다는 것을 깨닫게 될 것이다.

도표 1. 주요 반도체 분야별 향후 영향 전망

구분	역할	구조 변화 영향	중요도 변화	투자 시사점	핵심 키워드
GPU	AI 연산	always-on agent 로 총 연산 증가	▲ (유지~상승)	피크 성능보다 utilization 중요	지속 연산
HBM	고대역폭 메모리	KV cache 의존도 일부 감소	△ (의존도 둔화)	여전히 핵심이나 절대적 독점 지위 약화	bandwidth
DDR / LPDDR	시스템 메모리	external memory 증가	▲▲ (증가)	steady demand + 구조적 수혜	capacity
NAND / SSD	저장장치	retrieval 기반 구조 확대	▲▲▲ (큰 폭 증가)	AI storage 시장 본격 개화	data access
SRAM / Cache	온칩 메모리	반복 검증 loop 증가	▲▲ (증가)	compute + memory 결합 중요성 증가	latency
Networking (Interconnect)	데이터 이동	distributed memory access	▲▲ (증가)	scale-out 구조의 핵심 인프라	low latency
CXL / Memory Expansion	메모리 확장	memory pooling 수요 증가	▲ (증가 초기)	차세대 메모리 아키텍처 핵심	memory tiering
Storage Controller	데이터 처리	I/O 빈도 증가	▲▲ (상승)	SSD 성능 차별화 핵심	throughput

자료: 유진투자증권

Compliance Notice

당사는 자료 작성일 기준으로 지난 3 개월 간 해당종목에 대해서 유가증권 발행에 참여한 적이 없습니다
당사는 본 자료 발간일을 기준으로 해당종목의 주식을 1% 이상 보유하고 있지 않습니다
당사는 동 자료를 기관투자가 또는 제 3 자에게 사전 제공한 사실이 없습니다
조사분석담당자는 자료작성일 현재 동 종목과 관련하여 재산적 이해관계가 없습니다
동 자료에 게재된 내용들은 조사분석담당자 본인의 의견을 정확하게 반영하고 있으며, 외부의 부당한 압력이나 간섭 없이 작성되었음을 확인합니다
동 자료는 당사의 제작물로서 모든 저작권은 당사에게 있습니다
동 자료는 당사의 동의 없이 어떠한 경우에도 어떠한 형태로든 복제, 배포, 전송, 변형, 대여할 수 없습니다
동 자료에 수록된 내용은 당사 리서치센터가 신뢰할 만한 자료 및 정보로부터 얻어진 것이나, 당사는 그 정확성이나 완전성을 보장할 수 없습니다. 따라서 어떠한 경우에도 자료는 고객의 주식투자의 결과에 대한 법적 책임소재에 대한 증빙자료로 사용될 수 없습니다

투자기간 및 투자등급/투자의견 비율

종목추천 및 업종추천 투자기간: 12 개월 (추천기준일 종가대비 추천종목의 예상 목표수익률을 의미함)		당사 투자의견 비율(%)
· STRONG BUY(매수)	추천기준일 종가대비 +50%이상	0%
· BUY(매수)	추천기준일 종가대비 +15%이상 ~ +50%미만	95%
· HOLD(중립)	추천기준일 종가대비 -10%이상 ~ +15%미만	5%
· REDUCE(매도)	추천기준일 종가대비 -10%미만	0%

(2026.03.31 기준)