Vol.47 2026년

서울대학교
국가미래전략원
Institute for Future Strategy
Seoul National University

IFS 국가 정책 제안

한국 제조업의 AI 전환과 데이터 소버린티

서울대 데이터사이언스대학원 박현우 부교수

9 773058 556003 47
ISSN 3058-5562

1 한국 제조업 전망과 소버린 AI의 세분화

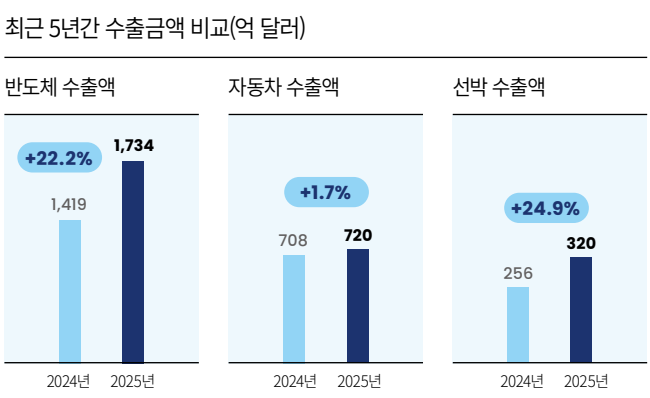
한국 제조업의 현황 및 2025년 슈퍼사이클

- 2025년 반도체, 조선, 방산 등 핵심 주력 산업의 동반 호조로 수출 실적 견인. 미·중 패권 경쟁 속 공급망 재편의 수혜를 입으며 신뢰 가능한 제조 파트너로서 한국의 전략적 위상 재조명
- 세계 최고 수준의 하드웨어 제조 공정 기술과 생산 능력 대비, 이를 통합 제어하고 최적화하는 운영 소프트웨어 및 데이터 관리 역량은 답보 상태. 하드웨어 강국의 위상이 소프트웨어적 한계에 갇힌 상태 지속
- 제조업 디지털 전환 (DX: Digital Transformation) 고도화에 따른 데이터 분석 플랫폼의 외산 의존도 급증. 2025년 제조 호황으로 창출된 부가가치가 국내 생태계 R&D로 환류되지 못하고, 해외 데이터 플랫폼 기업의 라이선스 및 구독 비용으로 유출될 구조적 우려 상존

소버린 AI 패러다임의 세분화: 모델 소버린티와 데이터 소버린티

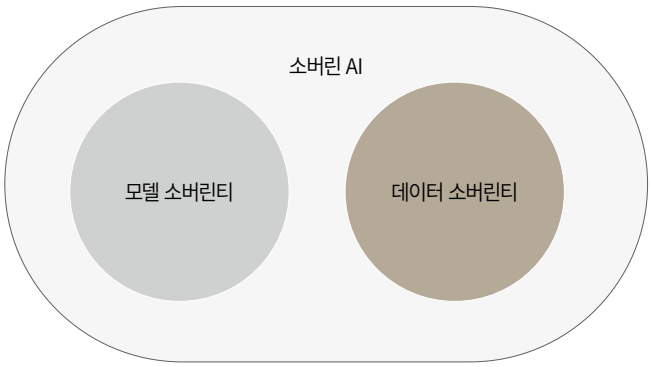
- 기존 소버린 AI 논의는 자국어 LLM 보유 여부인 모델 주권에 집중. 라마3(Llama 3), 큐웬(Qwen), 오픈AI의 gpt-oss 등 고성능 오픈 웨이트 모델의 확산으로 모델 개발 경쟁 지형의 급격한 변화
- 제조 AI 경쟁력의 핵심이 “더 좋은 모델”에서 “양질의 도메인 특화 데이터”로 무게 중심이 이동하면서 모델 소버린티에 더해서 데이터 소버린티에 대한 별도 논의 필요
- 제조업에서 AI 성능은 개별 공장의 설비 특성과 미세 공정 노하우가 담긴 데이터를 학습하는 수준이 결정. 정책 초점을 모델 개발 지원에서 독자적 데이터 인프라 확보 및 보호로 전환 필요
- 제조 AI에 대한 기존 정책적 담론에서는 현장의 구체성이 다소 결여되어 있는데, 데이터 소버린티에 대한 논의를 중심으로 현장의 문제에 연결 가능

[그림 1] 대한민국 주요 산업 수출 동향



출처: 산업통상부 2025년 수출입 동향
(https://www.motir.go.kr/kor/article/ATCL3f49a5a8c/171403/view)

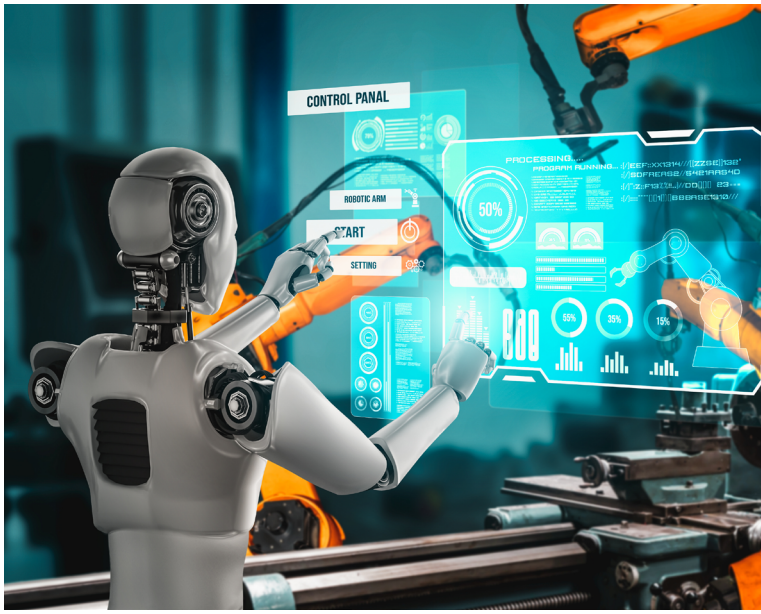
[그림 2] 소버린 AI의 세분화



2 글로벌 빅테크와 플랫폼 기반 기술 종속 메커니즘

팔란티어-SAP 파트너쉽과 제조 AI 플랫폼 시장의 지각변동

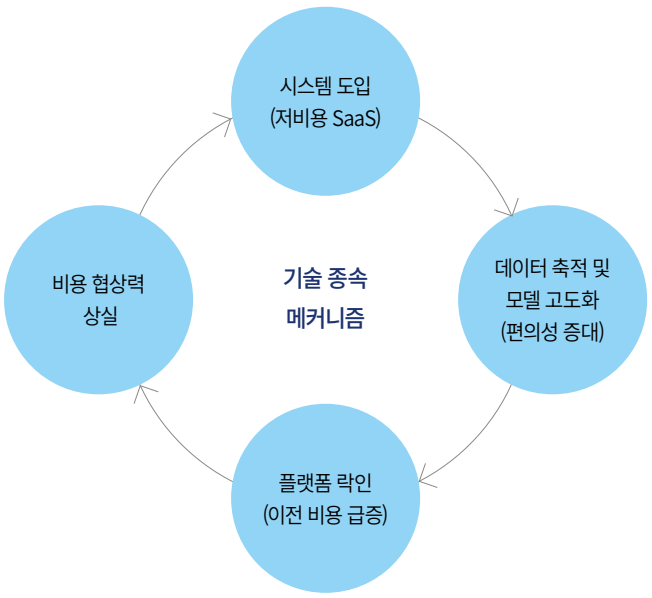
- 미 국방·첩보 분석 기업 팔란티어(Palantir)와 글로벌 ERP 시장을 장악한 독일 SAP의 전략적 제휴 체결. 기업의 핵심 경영 데이터를 담고 있는 ERP와 AI 분석 플랫폼(Palantir Foundry)이 결합된 강력한 통합 솔루션의 등장
- 즉각적 생산 효율화 및 편의성으로 국내 기업 도입 가속화 예상. 이미 SAP 의존도가 절대적인 국내 대기업 및 중견기업이 AI 분석 기능마저 외산에 의존하게 될 경우, 독자적 디지털 생태계 구축이 원천 봉쇄될 우려
- 초기에는 SaaS 모델로 큰 투자 없이 최신 AI 기능 활용 가능. 데이터가 축적되고 AI 모델이 해당 플랫폼 아키텍처에 최적화 되며 타 시스템 이전 비용이 급증. 강력한 락인(lock-in) 효과 발생



AI 도입에 있어서 사용자 마인드의 한계

- AI를 비용 절감을 위해 구매하는 도구로만 인식하는 사용자 마인드로는, AI가 데이터를 학습하면서 고도화 되는 과정에서 지능의 소유권이나 파생 데이터의 귀속 문제 간과 우려
- 제조업의 AI 전환에서 초기 비용 절감과 빠른 도입만을 우선하면 최첨단 AI 도입을 통한 AI 전환이 제조업 내부의 내재적 역량으로 축적되지 않음

[그림 3] 기술 종속 메커니즘



3 제조업 블랙박스화와 암묵지 유출

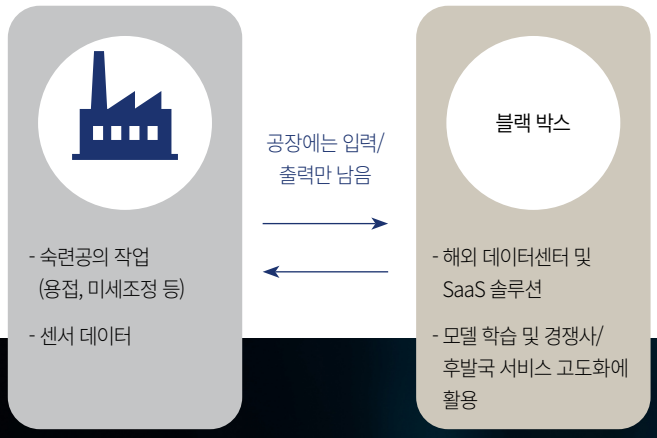
제조업의 본질인 암묵지의 유출 위험

- 한국 제조업 경쟁력의 원천은 매뉴얼화하기 힘든 숙련공의 미세한 감각과 오랜 경험인 암묵지. 이는 후발 주자가 막대한 자본 투자로도 단기간에 모방하기 어려운 핵심 진입 장벽
- AI 전환(AI Transformation, AX)은 암묵지를 명시적 지식과 디지털 데이터로 변환하는 과정. 해외 클라우드 AI를 무비판적으로 사용할 경우, 현장의 암묵지가 데이터로 변환되어 우리의 통제 밖인 해외 서버로 실시간 전송·축적되는 결과를 초래
- 글로벌 플랫폼은 수집된 데이터를 학습해 범용 제조 파운데이션 모델 고도화. 우리의 핵심 노하우가 경쟁사 및 후발국 AI 모델의 성능을 향상시키고 시행착오를 줄여주는 학습 재료로 쓰일 수 있음

제조 공정의 블랙박스화와 통제권 상실

- 고도화된 AI가 공정을 제어하며 공정 의사결정에서 인간 배제 심화. 시스템이 내리는 지시에 수동적으로 따르게 되어 공정 원리에 대한 이해도가 저하되고 기술적 종속 심화
- 해외 플랫폼 AI의 판단 근거를 알 수 없는 블랙박스 상태로 제조 공정 운영. 예기치 못한 공정 트러블 발생 시 자체 원인 규명이 불가능하며, 벤더사의 기술 지원 없이는 공장이 멈추는 위험 노출

[그림 4] 제조 공정 암묵지의 디지털 유출 프로세스



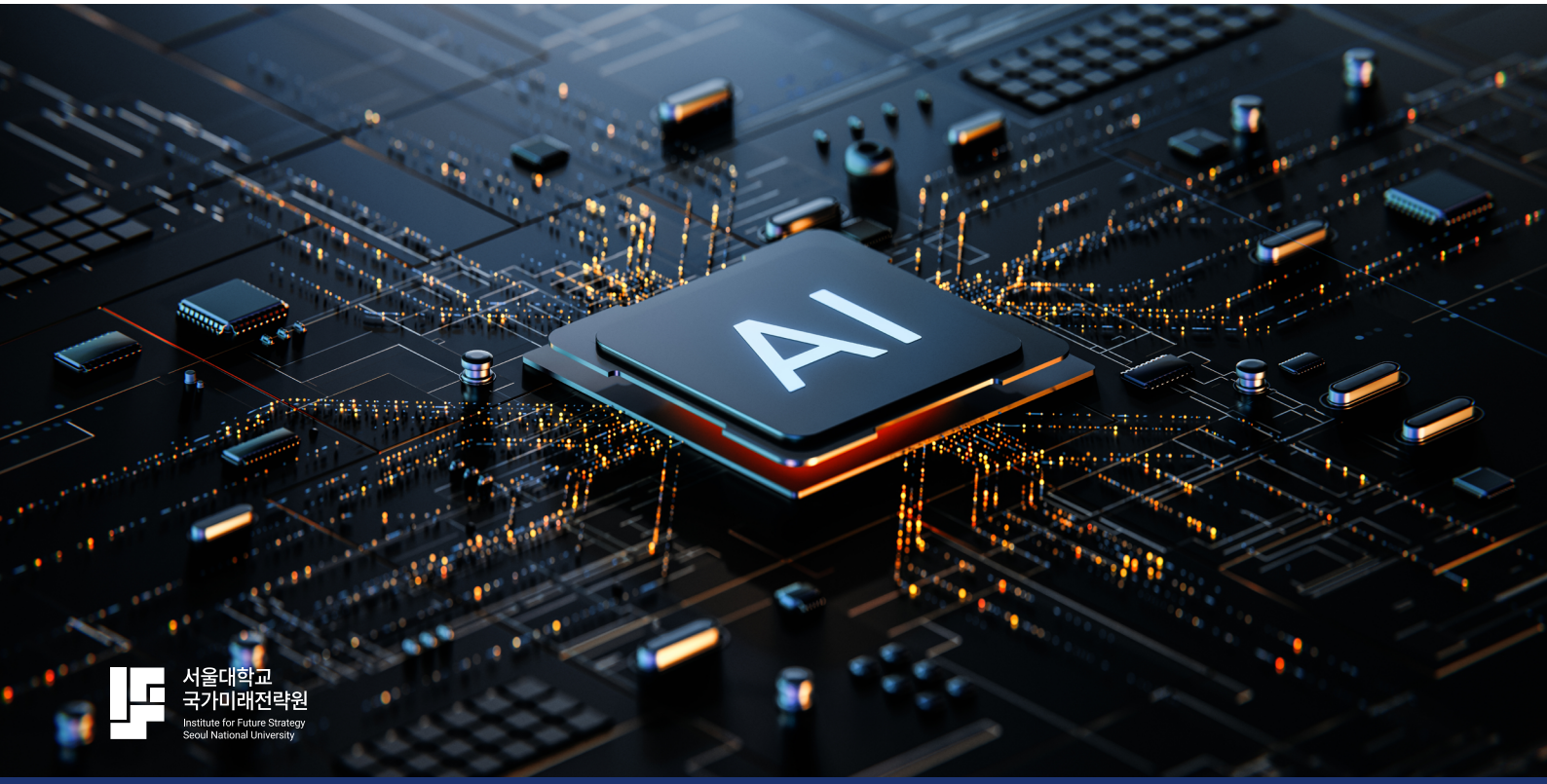
4 전략 자산으로서 제조 데이터

미·중 기술 패권 전쟁과 국가 안보 자산으로서의 데이터

- 미국, EU 등 주요국은 데이터를 국가 안보와 직결된 전략 자산으로 규정하고 자국 산업 데이터의 국외 유출을 통제하는 정책을 강화하며 디지털 국경을 구축
- 데이터는 21세기의 원유를 넘어, AI라는 전략 무기를 구동하는 핵심 자원이자 필수 탄약으로 격상. 국가 차원의 체계적인 보호·관리 부재 시 기술 패권 경쟁 도태 및 안보 위협 직면
- 반도체, 방산, 배터리 등 국가 핵심 전략 산업의 데이터가 해외 서버에 저장될 경우, 잠재적 적국이나 경쟁국 정보기관의 감시 및 분석 대상이 되어 국가 기밀 유출 보안 우려 상존

지정학적 리스크와 디지털 소작농 전락 위기

- 외교적 마찰이나 무역 분쟁 발생 시 상대국 정부의 제재로 인한 클라우드 접근 차단 가능성 상존. 해외 서버의 물리적 장애나 해킹 공격 시 국내 공장 가동이 연쇄적으로 중단되는 치명적인 연쇄 반응 결과에 대한 위험 인지 필요
- 최근 발생한 소비자 개인정보 유출이 사회적 리스크를 넘어서 국가 안보적인 리스크로도 인식됨. 국가 기간 산업인 제조업 데이터가 유사한 리스크에 노출되는 것은 국가 산업 경쟁력의 근간을 흔드는 안보 위협이 될 수 있음
- 경제적인 측면에서도 하드웨어 생산으로 벌어들인 이익의 상당 부분이 소프트웨어 및 플랫폼 사용료 명목으로 해외 빅테크 기업에 영구적으로 유출되는 디지털 소작농 구조 고착화 우려
- 플랫폼에 종속된 상태에서는 독자적인 혁신이 어렵고 거대 플랫폼 기업의 생태계 확장에 봉사하는 하부 구조로 전락. 데이터 주권 확보는 단순한 비용 절감이 아닌 국가 산업의 독립성을 지키기 위한 생존 전략



5 데이터 소버린티 확보를 위한 국가 전략

제조 AI 생태계 육성 및 법적 거버넌스 정비

- 팔란티어, SAP 등 글로벌 독과점 플랫폼에 대항하기 위해 국내 제조 AI 컨소시엄(국내 ERP 기업+AI 전문 기업+제조 대기업)을 지원. 공공 조달 및 국책 사업 발주 시 국산 AI 플랫폼 도입에 가점 부여. 초기 시장 수요 견인

- 국가첨단전략산업법 및 산업기술유출방지법 내 AI 학습 데이터 관련 조항 신설로 핵심 기술 데이터의 무분별한 국외 전송 제한. 데이터 중요도에 따른 등급 분류 체계를 도입하고 최상위 등급의 물리적 망 분리

- 기업의 데이터 소유권, 파생 데이터 및 학습된 모델과 지능에 대한 권리, 계약 종료 시 데이터 반환/삭제 의무를 명확히 보장하는 AI 데이터 주권 표준 계약서 개발 및 보급. 법무 역량이 부족한 중소기업을 위한 법률 자문 지원 시스템 마련

온프레미스 소버린 AI 인프라 구축 대폭 지원

- 보안과 기밀 유지가 생명인 제조 데이터의 특성을 고려하여 퍼블릭 클라우드 중심 지원에서 탈피. 기업 내부 서버 구축 및 자체 데이터 레이크 형성을 위한 구축형 AI 지원 강화

- 개별 구축 여력이 부족한 중소·중견기업을 위해 주요 국가산단 내 공동 활용 가능한 프라이빗 클라우드 센터 구축 고려. 외부와 차단된 폐쇄망 환경에서도 원활하게 구동 가능한 제조 특화 경량화 모델 개발 등 R&D 투자로 제조 AI 관련 기술 자립 유도

- 큐웬, 라마, gpt-oss 등 최신 오픈 웨이트 모델을 기업 내부망에서 안전하게 파인튜닝하여 사용할 수 있도록 기술 가이드라인 및 표준 아키텍처 보급. 기업들이 해외 클라우드에 의존하지 않고도 자체적인 AI 역량을 축적할 수 있는 환경 및 생태계 조성

[그림 5] 데이터 소버린티를 위한 제조 AI 아키텍처

거버넌스	- 표준 계약서 개발 및 보급 - 중소기업을 위한 법률 자문 지원 시스템
데이터	- AI 학습 데이터 관련 법률 규정 제정 및 정비 - 데이터 보안 등급 분류
모델	- 오픈 웨이트 모델 - 경량 sLLM
인프라	- 기업 내부 온프레미스 서버 구축 - 국가산단 공동 활용 프라이빗 클라우드