

2 소버린 AI, 모델 확보에서 실행 통제로

➔ AI 공급 집중과 접근 통제 강화, 소버린 AI 논의를 가속

- AI가 국가 핵심 서비스에 결합되며 운영 안정성이 국가 리스크로 부상
 - 생성형 AI가 행정·보건·금융·제조·국방·통신 등 국가 핵심 서비스 전반으로 확산되면서, AI 기능을 안정적으로 구동·유지하는 일이 정부와 기업의 운영 과제로 부상
 - 특히 AI 활용이 업무 자동화와 의사결정 지원을 넘어 필수 서비스의 가동 과정에 직접 연결되면서, 특정 모델이나 플랫폼의 중단 가능성이 새로운 서비스 리스크로 확대
 - 그러나 프런티어 모델, 고성능 반도체, 클라우드 플랫폼, AI 개발 도구가 소수 국가와 글로벌 빅테크에 집중되면서, 대다수 국가는 AI 실행 기반의 핵심 요소를 외부에 의존하는 구조
 - '26년 6월 美 상무부가 Anthropic의 최신 고성능 AI 모델 Fable 5, Mythos 5에 대해 외국인 접근 제한을 지시하면서, 모델 접근권도 정책 통제의 대상이 될 수 있음을 시사
 - 이는 AI 활용의 불확실성이 가격·기능 등 상업적 조건의 변동을 넘어, 공급국 정부와 사업자의 정책 변화에 따라 서비스 접근 자체가 제한될 수 있는 단계로 확대됐음을 의미
- 각국, '소버린 AI'를 국가 전략 의제로 격상하며 AI 실행 기반 확보에 착수
 - 이러한 공급 집중과 접근 통제 우려가 현실로 나타나면서, 각국은 소버린 AI를 단순 기술 확보 차원을 넘어 국가 핵심 서비스의 안정성과 산업 경쟁력 문제로 인식
 - 주요국은 데이터센터, 컴퓨팅 자원, 공공 클라우드, 민감 데이터 처리 체계를 재정비하며, AI를 자국 기준에 따라 실행·운영할 수 있는 기반을 마련하기 시작
 - '26년 기준 가동 중인 정부 지원 소버린 AI 프로젝트가 130여 개에 이르고, '25년 4분기에만 신규 인프라 프로젝트 23건이 추가되는 등 각국의 대응 속도가 빠르게 확대 (CNAS, '26.4.)
 - 다만 대다수 프로젝트는 GPU 클러스터와 데이터센터 구축에 집중되어 있으며, 실제 실행 조건인 전력, 클라우드 운영권, 모델 접근권, 조달 기준까지 포괄하는 전략은 아직 소수에 그치는 상황

- 이에 따라 소버린 AI의 쟁점은 자국 모델 보유 여부를 넘어, AI 실행 기반부터 모델 접근, 운영 권한, 적용 기준을 포괄하는 ‘AI 스택 통제권’ 확보 문제로 이동

➔ 소버린 AI, 자국 모델 보유에서 AI 스택 통제권으로 전환

● AI 주권 논의, 모델 보유에서 실행 조건 통제로 이동

- 초기 소버린 AI 논의는 외국 모델 의존이 자국어·자국 가치 반영을 제약하고 민감 데이터 노출 위험을 키울 수 있다는 우려에서 출발해, 자체 모델 개발을 주권 확보의 핵심 목표로 설정
- 그러나 자국 모델을 확보하더라도 학습·추론에 필요한 컴퓨트, 반도체, 클라우드, 데이터 운영체계를 외부에 의존하면, 실제 구동과 운영 단계에서 통제력이 제한되는 구조 (CNAS, '26.4.)
- 특히 외부 공급자가 접근 조건, 가격, 약관, 기능 제공 범위 등을 조정할 경우, 이를 기반으로 운영되는 공공·산업 서비스의 안정성에 직접적인 부담이 발생할 가능성 상존 (AI Policy Bulletin, '26.4.)
- 결국 소버린 AI의 핵심은 “어떤 모델을 보유했는가”가 아니라, 자국 기준에 따라 “어떤 조건에서 AI를 안정적으로 실행하고 통제할 수 있는가”로 재정의되는 양상

● AI 스택 통제권, 실행·운영·모델·거버넌스 4계층으로 구체화

- AI 통제력은 AI 스택의 한 지점에 집중되지 않고 여러 계층에 분산되어 있어, 각 계층을 누가 어떤 조건으로 통제하느냐가 실질적 주권 수준을 좌우
- 구체적으로 AI 스택은 △AI 실행 기반, △클라우드·운영, △모델·데이터, △적용·거버넌스의 네 계층으로 구분되며, 각 계층은 실행 능력, 운영 관할권, 모델 접근성, 도입 기준을 각각 결정
- 따라서 AI 주권은 특정 계층의 우위만으로 판단하기 어렵고, “어느 계층을 직접 통제하며 어느 계층의 외부 의존은 허용·관리할 것인가”의 조합으로 규정 (WEF·Axon, '26.5·6)

● 전 계층 자립보다 전략 계층 선별 통제와 의존 관리가 현실적 경로

- 다만 프런티어 모델과 클라우드를 주도하는 美조차 반도체 제조·장비 부문에서 외부 의존이 남아, 전 계층의 완전 자립은 어느 국가에도 현실적 목표가 되기 어려운 상황
- 한 계층을 국산화하더라도 이를 떠받치는 다른 계층의 의존이 함께 남기 때문에, 주권 확보의 관건은 의존을 없애는 것이 아니라 의존의 위치와 수준을 파악하는 데 있음

- 이 때문에 각국은 자국의 산업 기반, 민감 업무 범위, 조달 역량을 기준으로 직접 통제할 계층과 외부 의존을 관리할 계층을 구분할 필요 (WEF·Axon, '26.5)
- 동시에 직접 통제하지 않는 계층은 멀티벤더 조달, 기술적 대체 경로, 계약상 접근권 제한, 감사권 확보 등을 통해 공급 변동 리스크를 낮추는 방식이 요구
- 결국, 현실적 AI 주권은 전 계층 자립보다, 핵심 업무에 필요한 통제 범위를 결정하고 나머지 의존을 관리 가능한 조건 안에 두는 설계 역량에 좌우

→ 소버린 AI 실행력, 계층별 통제권 설계에 좌우

(1) AI 실행 기반, GPU 확보에서 전력·유지보수 통제로 확장

● 연산 자원 확보, 소버린 AI 실행의 첫 번째 과제로 부상

- 소버린 AI는 자국 모델 개발에 앞서 학습과 추론을 수행할 연산 환경부터 확보해야 하며, 이 단계가 외부 공급자에 묶이면 이후 운영과 고도화의 선택지도 함께 제한
- 실제로 소버린 AI 투자가 연산 기반 확충으로 확대되는 가운데, 고성능 GPU, AI 서버, 네트워크 장비가 소수 공급자에 집중되면서 각국은 투자 초기부터 핵심 장비 확보 경쟁에 직면
- 이는 소버린 AI가 자국의 모델·데이터 역량을 활용하기 이전에, 해당 모델을 실제로 학습·추론할 수 있는 연산 환경에 접근할 수 있는지부터 외부 공급 여건에 좌우된다는 점을 의미
- 따라서 안정적인 연산 자원 확보는 소버린 AI 전략의 출발점이며, GPU·서버·네트워크 장비의 조달 안정성이 국가 AI 실행력을 좌우하는 기초 조건으로 부상

● 전력·송전망 확보, GPU 투자를 실제 역량으로 전환하는 관문

- 연산 자원을 확보하더라도 실제 가동을 위해서는 안정적 전력, 냉각, 부지, 인허가, 송전망 연결이 함께 뒷받침되어야 하므로, 가동 조건이 별개의 병목으로 부상
- 특히 AI 데이터센터는 대규모 전력을 지속적으로 사용하기 때문에, 장비 구매와 시설 건설보다 전력망 접속과 송전 인프라 확보가 더 큰 제약으로 작용
- 데이터센터 건설은 수개월 단위로 진행될 수 있으나, 송전망 연결과 전력 공급 승인에는 수년이 소요될 수 있어 투자와 가동 사이의 시간 격차가 발생
- Carnegie는 100MW급 데이터센터의 전력 공급이 지연되어 가동 시점이 1년 늦어질 경우, 운영 기간 전체에서 창출 가능한 사업 가치가 약 5.5% 감소할 수 있다고 분석
- 따라서 전력·입지·인허가 병목이 해소되지 않으면 GPU·데이터센터 투자는 실제 AI 역량으로 전환되기 어렵고, 소버린 AI 전략도 선언적 인프라 확충에 머물 가능성



● 국내 데이터센터 구축, 입지보다 공급망·복구 역량이 관건

- 데이터센터를 국내에 구축하거나 유치하는 것은 AI 실행 기반을 확보하기 위한 중요한 출발점이지만, 시설을 국내에 두는 것과 그 시설을 자국이 운영·통제하는 것은 별개의 문제
- 평소 운영 안정성은 핵심 GPU 서버, 네트워크, 냉각 설비, 관리 소프트웨어의 공급망에 좌우되며, 이를 해외에 의존하면 교체·확충 시점도 외부 조건의 영향을 받음
- 장애 발생 시 복구 역량 역시 펌웨어 업데이트, 보안 패치, 기술 지원 체계에 달려 있어, 해외 사업자 의존이 클수록 국내 인력만으로 신속 대응하기 어려움
- 특히 원격 관리 권한이나 장비 설정 권한이 해외 공급자에게 남아 있을 경우, 데이터센터의 물리적 위치와 무관하게 핵심 설비의 운영 조건이 외부에서 조정될 가능성 상존
- 따라서 AI 실행 기반의 통제력은 단순히 데이터센터 입지와 GPU 확보만으로 판단하기 어렵고, 평소 공급망·유지보수 체계와 비상시 복구 역량까지 함께 확보했는지로 평가할 필요

(2) 클라우드·운영 통제, 시설 입지보다 운영 주체와 적용 법률이 관건

● 클라우드 운영 주체와 접근 권한이 실질 통제 수준을 결정

- 데이터센터와 장비 통제가 물리적 실행 조건을 좌우한다면, 그 위에서 데이터 접근과 서비스 가동을 좌우하는 운영 주체는 별도의 층위이므로, 운영 주체가 입지에 이은 다음 통제 관문으로 부상
- 동일한 데이터센터를 활용하더라도 관리자 권한의 보유 주체, 운영·하청 구조, 장애 시 대응 권한의 소재에 따라 데이터 열람·반출과 서비스 변경 권한이 실질적으로 결정
- 특히 클라우드 운영자는 시스템 설정, 계정 관리, 보안 패치, 장애 복구 과정에서 저장 데이터에 접근하거나 서비스 기능을 제한할 수 있어, 운영 권한의 소재가 설비 보유 여부만큼 중요
- 따라서 클라우드 통제의 핵심 쟁점은 시설을 어디에 두었는지가 아니라, 데이터 접근권과 서비스 가동 권한을 누가 실질적으로 행사하느냐로 이동
- 결국 설비 계층이 물리적 실행 조건을 좌우한다면, 클라우드 계층의 통제는 데이터를 누가 열람·반출하고 서비스를 누가 중단할 수 있는지에 따라 판가름

● 해외 법률과 원격 관리 권한이 클라우드 통제의 불확실성으로 작용

- 클라우드 운영권이 중요한 이유는 외국 법률, 사업자 정책, 원격 관리 권한이

데이터센터 위치와 무관하게 클라우드 서비스 운영권과 데이터 접근권에 영향을 미치기 때문

- 美 클라우드 법에 따라 美 사업자가 보유·통제하는 데이터는 서버 위치와 무관하게 美 당국의 법적 접근 대상이 될 수 있어, 국내 저장만으로는 역외 관할권 우려 해소에 한계
- 또한 외국 클라우드 사업자는 원격 관리 계층(control plane), 관리자 권한, 운영 정책을 통해 국내에서 제공되는 클라우드 서비스의 기능과 접근 조건을 외부에서 조정 가능
- 따라서 클라우드 통제의 핵심은 데이터를 어디에 저장했는지가 아니라, 필요시 데이터 접근과 서비스 제한, 장애 복구 권한을 누가 실제로 행사할 수 있느냐에 의해 좌우
- 클라우드 주권, 해외 사업자 배제가 아닌 운영 통제 요건의 제도화가 핵심
 - 클라우드 통제력이 시설 위치보다 운영 주체, 접근권, 관할권에 의해 좌우되는 만큼, 통제 확보의 관건은 이를 계약·인증·감사 기준 등 제도적으로 구체화하는 기준 마련으로 이동
 - 따라서 클라우드 주권을 확보하려면 외산 배제나 전면 국산화에만 초점을 맞추기보다, 운영 조건을 사전에 규정하고 이행 여부를 검증하는 제도적 장치 마련이 핵심
 - 실제로 주권형 클라우드 기준은 데이터 저장 위치를 넘어 역외 법률의 영향, 운영 인력의 접근권, 보안 인증, 공급망 통제 가능성을 함께 평가하는 방향으로 구체화
 - 다만 이러한 요건은 모든 업무에 일괄 적용되기보다, 공공·국방·금융·핵심 인프라 등 높은 통제 수준이 필요한 영역부터 우선 적용되는 방식으로 확산
 - 결국 클라우드 주권은 특정 사업자 배제의 문제가 아니라, 업무 민감도에 따라 운영 통제 수준을 검증 가능한 기준으로 규정하는 문제로 전환

(3) 모델·데이터 통제, 접근권 확보와 자국 데이터 활용 역량이 핵심

- 외부 모델 접근권 확보가 모델 계층 통제의 첫 관문으로 부상
 - 실행 기반과 클라우드 통제가 AI 서비스의 하부 조건이라면, 실제 업무에 사용할 모델에 안정적으로 접근하지 못하면 앞서 확보한 인프라 통제의 효과는 제한적
 - 그러나 대다수 국가는 외부 API 모델을 결합해 서비스를 빠르게 구현하고 있어, 사업자 정책이나 공급국 규제에 따른 접근 제한·기능 조정 등 통제하기 어려운 변수에 노출



- 이러한 외부 모델이 공공·금융·제조 등 국가 핵심 업무에 깊게 결합될수록, 접근 차단이나 기능 제한은 단순한 불편을 넘어 서비스 연속성 문제로 확대
- 이에 따라 모델 계층의 주권 기준은 최상위 모델 보유 여부보다, 핵심 업무별로 필요한 모델 접근권을 확보하고 장애·차단 시 대체 경로까지 마련할 수 있는가로 이동
- 오픈웨이트 모델 활용, 접근 안정성을 높이지만 기반 모델 의존은 잔존
 - 외부 API 모델 의존을 줄이기 위해서는 모델을 자체 환경에서 실행·조정할 수 있어야 하나, 프런티어급 모델의 독자 개발은 비용과 인력 부담이 커 단기간에 추진하기 어려움
 - 실제로 다수 국가는 오픈웨이트 모델을 자국 언어·산업·공공 맥락에 맞게 미세 조정하는 방식을 채택하고 있으며, 이 과정에서 美 기업이 공개한 모델이 주요 기반 모델로 활용 (CNAS, '26.4.)
 - 다만 오픈웨이트도 라이선스 조건, 재배포 범위, 업데이트 지속성에 제약을 받을 수 있어, 범용 공개 모델 활용만으로 민감 업무에 필요한 통제력을 온전히 확보하기 어려운 한계가 상존
 - 결국 모델 계층의 주권성은 공개 모델 활용 여부가 아니라, 필요한 모델을 안정적으로 실행하고 국내 데이터로 고도화할 수 있는 역량에 좌우
- 자국 데이터 활용권, 모델 고도화 수준을 결정
 - 도메인 특화·프라이빗 모델의 성능은 어떤 데이터를 학습·검색·추론 과정에 투입할 수 있는지에 좌우되므로, 데이터 활용권이 모델 계층 통제의 핵심 조건으로 부상
 - 특히 행정·의료·금융·제조·통신 등 분야별 업무 데이터는 국가별 제도와 산업 현장의 실제 절차를 반영하므로, 범용 모델을 국내 업무에 맞게 조정하는 기반으로 작용
 - 다만 데이터를 보유하더라도 활용 권한, 법적 근거, 내부 승인 절차 등 데이터 활용 체계가 마련되지 않으면, 데이터가 실제 모델 고도화로 연결되기 어려운 한계가 상존
 - 특히 행정·의료·금융 등 민감 데이터의 경우 활용 가치는 크지만, 개인식별 정보와 기밀성이 높은 정보를 포함할 수 있어 비식별·보안 처리와 접근 권한 설정이 선행될 때에만 활용 가능
 - 결국 데이터 주권은 데이터를 국내에 보관하는 수준을 넘어, 필요한 데이터를 합법적이고 안전하게 AI 개발·운영 과정에 투입할 수 있는 역량으로 판단할 필요

(4) 적용·거버넌스 통제, 업무 분류와 조달 기준이 국내 수요를 형성

- 업무 민감도 분류가 소버린 AI 적용 범위와 통제 수준을 결정
 - 모델·데이터 통제는 AI 활용의 기반을 제공하지만, 실제 도입 단계에서는 업무별 위험도와 민감도에 따라 적용 요건을 달리 설계할 필요성이 증대
 - AI 활용 업무는 보안 수준, 서비스 연속성, 오판 시 피해 규모, 책임 소재가 서로 다르기 때문에, 일률적 소버린 AI 요건은 비용 증가와 현장 적용 부담으로 이어질 가능성
 - 따라서 소버린 AI 적용은 장애, 오판, 정보 유출이 발생했을 때 국민 안전과 공공서비스에 미치는 영향을 기준으로 업무를 분류하는 데서 출발
 - 국민 안전, 민감 정보, 핵심 인프라와 연결된 업무는 국내 운영, 사용 기록 관리, 접근권 통제, 사후 감사 등 높은 수준의 검증 요건이 필요
 - 반면 일반 행정 지원이나 내부 문서 초안 작성처럼 위험도가 낮은 업무는 글로벌 클라우드와 국내 인프라를 함께 활용하는 방식도 가능
 - 결국 업무 민감도 분류는 모든 AI 활용을 동일하게 규제하기 위한 장치가 아니라, 위험 수준에 따라 국내 통제와 외부 활용의 경계를 정하는 기준이자 이후 조달 설계의 출발점으로 기능
- 분류 기준이 공공 조달에 반영될 때 국내 사업자의 공급 기회가 형성
 - 소버린 AI는 정부의 통제 기준에 더해 해당 기준을 충족하는 AI를 민감 업무에 공급할 국내 사업자가 있어야 하므로, 공공 조달이 그러한 국내 공급자를 키우는 핵심 연결 고리로 작용
 - 다만 공공 조달이 국내 운영, 데이터 보호, 사용 기록 관리 등 민감 업무 수행 요건을 평가 기준에 명시하지 않으면, 사업자가 이를 충족하는 제품을 개발하여 공급할 유인이 부족
 - 나아가 보안 평가, 모델 사용 기록 관리, 제3자 감사, 책임 소재 등 운영 신뢰성 검증 요건이 구체화 될수록, 국내 사업자도 공공 납품 실적으로 기술력을 객관적으로 입증할 기회를 확보
 - 이러한 납품 실적이 축적되면 공공 조달은 단순 구매를 넘어, 시장 기반이 좁은 국내 사업자에게 초기 공급 실적과 운영 사례를 제공하고 민간 확산으로 이어지는 첫 수요처로 작동
- 조달·감사 기준의 실제 집행 여부가 국내 AI 공급 기반을 좌우
 - 다만 조달이 국내 사업자의 참여와 납품으로 이어지려면 기준이 선언에 그치지 않고 발주·평가·계약·운영 점검 전 과정에 일관되게 적용되어야 가능



- 그러나 주요국에서도 AI 도입은 빠르게 확산되는 반면, 도입 이후 성능·편향·보안·책임성을 점검하는 사후 거버넌스는 아직 충분히 정착되지 못한 상황
- 이처럼 도입 후 점검 장치가 미흡하면 국내 사업자는 운영 신뢰성을 입증할 기회를 확보하기 어렵고, 공공 AI 계약도 실적을 갖춘 기존 글로벌 사업자 중심으로 고착될 가능성
- 결국 업무 분류 기준이 구매·평가·계약·사후 점검 전 단계에서 실제로 집행될 때, 공공 조달은 국내 사업자의 납품 기회와 소버린 AI 시장 형성으로 연결 가능

→ 국가별 전략: EU·프랑스·일본의 계층 선택과 의존 관리

- 각국의 소버린 AI 전략은 우선 강화 계층과 의존 관리 방식의 차이로 구분
 - 앞선 분석에서 AI 스택은 실행 기반·클라우드 운영·모델 데이터·적용 거버넌스의 네 계층으로 구성되며, 각국의 AI 주권 수준은 어느 계층을 우선 강화하느냐에 따라 달라짐
 - EU는 적용·거버넌스 계층을 중심으로 외부 기술의 활용 조건을 규범으로 설정하는 경로를, 프랑스는 모델·데이터와 실행 기반 계층을 국가 차원에서 직접 확보하는 경로를 선택
 - 일본은 실행 기반과 모델·데이터 계층을 반도체·HPC·제조 데이터 기반으로 보완하며, 산업 현장 중심의 AI 내재화에 집중
 - 세 국가 사례는 소버린 AI가 전 계층 자립의 문제가 아니라, 자국 강점에 맞춰 우선 강화할 계층을 선택하고 남는 의존을 관리하는 문제임을 보여줌

(1) EU, 규범 주도권과 공동 인프라를 결합한 초국가형 소버린 AI 추진

- 적용·거버넌스 계층: AI Act·CADA로 외부 기술의 도입 조건을 설정
 - EU의 소버린 AI 전략에서 가장 높은 수준의 통제가 이루어지는 계층은 적용·거버넌스로, AI Act와 AI Office를 통해 고위험·범용 AI의 감독 체계를 제도화
 - 공공 클라우드의 주권 수준을 4단계로 구분하는 CADA 제정안을 발표하며, 민감 업무에 사용되는 AI 서비스의 도입 기준을 유럽 차원에서 규정 (EU 집행위, '26.6.)
 - Apply AI Strategy를 통해 공공부문 'AI 우선 정책'과 유럽산 오픈소스 AI 우선 구매를 권고하며, 조달 단계에서도 유럽 AI 생태계를 견인하는 구조를 설계
 - 따라서 EU 전략은 외부 AI 기술을 전면 배제하기보다, 유럽 시장과 공공부문에 들어오는 AI 서비스가 어떤 기준을 충족해야 하는지를 규범과 조달 기준으로 설정하는 방식

- 실행 기반·클라우드·모델 계층: 공동 인프라로 격차를 줄이되 외부 의존은 관리
 - 실행 기반 계층에서는 AI 팩토리·AI 기가팩토리를 통해 회원국이 공동 활용할 수 있는 연산 자원을 확충하고, 연구기관·스타트업의 접근성을 높이는 구조를 설계 (EU 집행위, '26.6.)
 - 다만 첨단 GPU·AI 서버는 여전히 美 공급자 의존이 지속되고, 유럽 내 AI 연산 자원은 전 세계의 5% 미만으로 비중이 낮아 실행 기반의 자립에는 한계 (Bruegel, '26.6.)
 - 클라우드·모델 계층에서도 美 하이퍼 스케일러의 시장 영향력이 크고, 유럽 AI 기업 역시 주요 글로벌 클라우드를 활용해 모델을 배포·운영하는 구조가 병존
 - 결국 EU 모델은 실행 기반과 모델을 모두 독자적으로 확보하는 경로라기보다, 규범·조달·공동 인프라를 통해 외부 기술의 활용 조건을 유럽 기준으로 설정·검증하는 거버넌스 주도형 경로로 평가

(2) 프랑스, 국가 챔피언 육성과 원전 기반 전력 입지를 결합한 소버린 AI 추진

- 모델·데이터 계층: Mistral 육성과 공공 전환으로 접근권을 강화
 - EU가 거버넌스 계층에서 외부 기술의 활용 조건을 설정하는 데 집중한 반면, 프랑스는 모델·데이터 계층에서 자국 기업과 공공 수요를 결합해 통제력을 높이는 경로를 선택
 - 프랑스 Mistral AI를 국가 챔피언으로 육성하며 정부 투자와 공공 조달을 통해 초기 수요를 형성하고, 공공서비스·군사 영역에 자국 모델 도입을 추진 (Oxford Insights, '26.3.)
 - '26.6월에는 국내정보총국(DGSI)의 데이터 분석 도구를 美 Palantir에서 佛 ChapsVision으로 교체하는 방침을 발표하며, 민감 업무의 모델·데이터 의존을 줄이는 방향을 구체화
- 실행 기반 계층: 원전 전력과 데이터센터 입지로 가동 조건을 강화
 - 실행 기반 계층에서는 원전 기반 저탄소 전력을 활용해 AI 데이터센터 유치 경쟁력을 높이고, 인허가 기간 단축을 통해 대규모 인프라 구축 속도를 높이는 방향을 추진
 - 이는 AI 실행 기반의 핵심 병목이 GPU 확보에만 있는 것이 아니라, 안정적 전력과 부지, 인허가, 가동 시점을 함께 확보하는데 있음을 보여주는 사례
 - 다만 Mistral 모델도 주요 글로벌 클라우드를 통해 배포·활용되고 있어, 자국 모델 기업 보유 여부가 곧 클라우드·인프라 계층의 완전한 자립을 의미하지는 않음



- 따라서 프랑스 모델은 자국 모델 기업, 공공 수요, 전력 입지를 결합해 모델·데이터와 실행 기반 계층을 우선 강화하되, GPU·클라우드 의존은 병존하는 산업정책 주도형 경로로 평가

(3) 일본, 반도체·HPC·산업 데이터 기반을 결합한 현장 내재화형 소버린 AI 추진

● 실행 기반 계층: 반도체·HPC로 AI 연산 인프라를 보완

- 프랑스가 모델·데이터 계층의 직접 통제를 우선한 반면, 일본은 AI를 구동하는 물리적 실행 기반 자체를 자국 내에서 확보해 해외 칩·장비 공급 변동에 대한 의존을 줄이는 데 집중
- Rapidus를 통해 2nm급 첨단 로직 반도체 양산을 추진하고 정부 R&D 지원을 확대하며, AI 연산에 필요한 핵심 부품의 해외 조달 의존을 줄이려는 기반을 마련
- FugakuNEXT·ABCI-Q 등 슈퍼컴퓨팅 인프라를 구축해 학습·추론 워크로드를 자국 내에서 처리할 수 있는 환경을 확보, 이를 해외 클라우드 의존을 줄이는 실행 기반으로 활용
- 다만 GPU와 클라우드 공급에서는 여전히 글로벌 기업 의존이 남아 있어, 일본의 실행 기반 전략은 완전 자립보다 핵심 연산자원과 대체 경로를 확보하는 보완 전략에 가까움

● 모델·데이터 계층: 제조 현장 데이터로 범용 모델 의존을 보완

- 일본은 아직 글로벌 최상위 프런티어 모델을 독자 생태계로 운영하는 단계는 아니나, 정부 주도로 기업·연구기관을 연결해 국내 기반 모델 개발 역량을 끌어올리는 방향을 병행
- 경제산업성·NEDO는 GENIAC을 통해 기반 모델 개발 기업에 계산 자원 확보를 지원하고 있으며, '26.6월에는 AI 기반 모델 개발 과제를 선정해 자국 생성형 AI 개발 역량 확충을 추진
- 이는 외부 오픈웨이트 모델을 자국 산업 맥락에 맞게 조정하는 단기 대응을 넘어, 중장기적으로 프런티어 AI 개발 역량을 국내에 축적하려는 시도로 해석
- 범용 모델의 외부 의존을 보완하는 핵심 자산은 제조업 현장 데이터이며, GENIAC 프로젝트는 제조 데이터를 AI 학습에 활용할 수 있는 형태로 정비하는 데 초점 (METI, '26.5.)
- 나아가 로봇틱스 기반 모델 R&D까지 확대하며, 다른 국가가 쉽게 확보하기 어려운 제조 공정·장비·현장 데이터를 산업 특화 AI 역량으로 연결하려는 시도도 병행
- 따라서 일본 모델은 외부 기반 모델 활용과 국내 프런티어 AI 개발 지원을 병행하면서,

반도체·HPC·제조 데이터라는 기존 산업 자산을 활용해 AI를 현장에 내재화하는 경로로 평가

➔ 국가별 전략 비교: 강점 계층과 취약 계층의 조합

- 세 국가의 전략은 자국 강점에 기반한 우선 강화 계층에서 차이
 - EU는 적용·거버넌스 계층에서 규범과 조달 기준을 강화하고, 프랑스는 모델·데이터와 실행 기반 계층을 국가 챔피언·전력 입지와 결합하는 데 집중
 - 일본은 반도체·고성능 컴퓨팅·제조 데이터 기반을 활용해 실행 기반과 모델·데이터 계층을 보완하며, 산업 현장 중심의 AI 내재화 경로를 선택
 - 세 사례는 소버린 AI 전략이 동일한 경로로 수렴하기보다, 각국이 보유한 산업 기반과 정책 수단에 따라 우선 강화 계층이 달라진다는 점을 보여줌
- 공통 취약 계층을 클라우드·운영이며, 다음 경쟁은 운영권 설계로 이동
 - 반면 클라우드·운영 계층에서는 세 국가 모두 미국 하이퍼 스케일러와 글로벌 클라우드 생태계의 영향권 안에 있어, 시설·모델보다 운영권 설계가 공통 과제로 부상
 - 이는 소버린 AI 전략의 다음 쟁점이 GPU·모델 확보를 넘어, 관리자 접근권, 원격 관리 권한, 장애 대응책임, 법적 관할권을 어떻게 계약·인증·감사 기준에 반영하느냐로 이동하고 있음을 시사
 - 따라서 국가별 사례 비교는 한국도 모든 계층을 같은 강도로 추진하기보다, 강점 계층은 산업 전략으로 키우고 취약 계층은 운영 기준과 조달 제도로 보완해야 함을 보여줌



출처 : Le Monde 외(2026.5.)

https://www.lemonde.fr/en/economy/article/2026/05/29/mistral-ai-aims-for-full-value-chain-presence-to-challenge-us-dominance_6753922_19.html

<https://axonpartnersgroup.com/axon2023/wp-content/uploads/2026/06/Axon-The-Sovereignty-Paradox-Building-Sovereign-AI-Across-the-Full-Value-Chain-v1.1.pdf>

https://reports.weforum.org/docs/WEF_AI_Infrastructure_in_the_Age_of_Sovereignty_Requirements_Strategies_and_a_Trusted_Framework_for_Digital_Embassies_2026.pdf

https://www.oecd.org/en/publications/digital-government-outlook_0496b2bc-en/full-report/adopting-and-governing-ai-in-government_7ef312a9.html

<https://interactives.cnas.org/reports/sovereign-ai-index/>
<https://carnegieendowment.org/research/2026/06/early-lessons-in-the-pursuit-of-sovereign-ai>

<https://carnegieendowment.org/research/2026/06/the-compute-coalition-how-to-build-the-future-of-ai-in-the-free-world>

<https://www.aipolicybulletin.org/articles/ai-access-is-not-enough-middle-powers-need-strategic-reserves>

<https://digital-strategy.ec.europa.eu/en/policies/apply-ai>

<https://digital-strategy.ec.europa.eu/en/policies/cloud-and-ai-development-act>

<https://www.bruegel.org/first-glance/achieve-tech-sovereignty-europe-must-not-mimic-its-rivals>

<https://www.bruegel.org/analysis/europe-needs-strategy-close-artificial-intelligence-compute-gap>

<https://www.techpolicy.press/europes-ai-sovereignty-problem-runs-far-deeper-than-frontier-access/>

<https://www.techpolicy.press/eu-unveils-sweeping-tech-sovereignty-push-balancing-autonomy-with-openness/>

<https://www.atlanticcouncil.org/blogs/geotech-cues/europe-must-address-the-digital-sovereignty-triad/>

<https://sciencebusiness.net/news/sovereignty/european-sovereignty-ai-requires-ugly-trade-offs-say-experts>