ISSN 2233-6583

26-4

KISDI

Premium Report

개방형 AI 생태계 구축을 위한 상호운용성 정책방향 및 과제

김 현 수

정보통신정책연구원 선임연구위원

KISDI 정보통신정책연구원

KOREA INFORMATION SOCIETY DEVELOPMENT INSTITUTE

KISDI
26 - 4
2026. 05. 06
Premium Report

개방형 AI 생태계 구축을 위한 상호운용성 정책방향 및 과제

김 현 수
정보통신정책연구원 선임연구위원

요약문

개방형 AI 생태계 구축을 위한 상호운용성 정책방향 및 과제

김 현 수
정보통신정책연구원 선임연구위원
* onlyone@kisdi.re.kr, 043-531-4121
* 고려대학교 법학 박사
* 현 정보통신정책연구원 디지털정책연구실장

요 약 문

독자 AI(Sovereign AI) 구축과 AI 기본사회의 실현을 위해 AI 생태계 개방성이 중요하며, 상호운용성 정책을 통해 개방성을 단순한 선언이 아닌 실질적인 구조로 구현할 수 있다. 이에 본고에서는 상호운용성의 개념과 필요성을 살펴보고, 주요국의 상호운용성 설계 방식을 비교 분석한 결과 등을 바탕으로 우리나라의 정책 추진방향과 과제를 제시하였다.

개방형 AI 생태계를 구현하기 위해서는 상호운용성 확보와 더불어 법/계약, 공급망, 기술, 운영 통제를 유기적으로 결합한 인증 및 조달 체계가 필요하다. 미국, 영국, 유럽연합 등 주요국 사례는 상호운용성을 구현하는 정책 도구가 각기 다르더라도 표준, 시험, 조달, 규범을 결합해 시장 참여자의 행동 변화를 유도한다는 공통점이 있다. 우리나라도 AI 상호운용성 프레임워크를 통해 기술과 데이터 기준을 통합하고, 실질적 호환성을 담보할 시험/인증 체계를 구축하며, 도메인별 데이터 공간을 표준 API 기반으로 설계할 필요가 있다. 또한, 조달 단계에서 데이터 이동성, 클라우드 전환, 모델 포맷 호환성 등 탈 고착 조건을 절차 전반에 반영하고, 필요하다면 전환 권리의 법제화도 검토해야 한다.

이러한 정책 패키지는 특정 사업자/기술에 대한 의존도를 낮추는 동시에 국내 AI 산업의 경쟁력을 제고하여 진정한 기술 주권을 확립하고, 한국형 AI 생태계가 지속 가능한 국가 인프라이자 글로벌 경쟁력을 갖춘 수출 자산으로 자리매김하는 데 기여할 수 있다.

Interoperability Policies for an Open AI Ecosystem

Summary

Openness in the AI ecosystem is crucial for realizing Sovereign AI and an AI basic society, and interoperability policies can transform this openness from a mere declaration into a substantive framework. Accordingly, this paper examines the concept and necessity of interoperability and, based on a comparative analysis of how major countries design their interoperability frameworks, proposes policy directions and key tasks for South Korea.

To realize an open AI ecosystem, a certification and procurement system that organically integrates legal/contractual frameworks, supply chains, technology, and operational controls is necessary, in addition to ensuring interoperability. Case studies from major countries such as the United States, the United Kingdom, and the European Union share a common feature: although the policy tools used to implement interoperability differ, they combine standards, testing, procurement, and regulations to induce behavioral changes among market participants.

Korea must also integrate technology and data standards

through an AI interoperability framework, establish a testing and certification system to ensure practical compatibility, and design domain-specific data spaces based on standard APIs. Furthermore, conditions for breaking lock-in—such as data portability, cloud migration, and model format compatibility—must be incorporated into all procurement procedures, and the legalization of migration rights should be considered if necessary.

This comprehensive policy package will reduce dependence on specific providers or technologies while enhancing the competitiveness of the domestic AI industry. Ultimately, these efforts will help establish true technological sovereignty and ensure that the K-AI ecosystem serves as a sustainable national infrastructure and a globally competitive export asset.

1. 검토 배경

◆ AI 모델, 클라우드, 데이터 등이 결합된 'AI 인프라'는 개별 서비스를 넘어 국가 경제, 안보, 산업 경쟁력을 좌우하는 핵심 기반으로 자리 잡음

- 그러나 클라우드, 반도체, 데이터 등 핵심요소를 장악한 소수 글로벌 빅테크 기업이 생태계를 주도하면서 특정 사업자나 플랫폼에 대한 기술적·법제도적 의존도가 심화되고 있음

◆ 이에 따라 국가가 AI 시스템을 독립적으로 개발 · 통제하여 국가 안보와 경제적 이익, 윤리적 가치를 보장하는 '독자 AI'(sovereign AI)가 중요한 정책 어젠다로 부상함

- 다만, 이는 모든 요소를 국산화하는 고립된 자급자족이 아니라 글로벌 협력과 민간 혁신을 유지하며 통제권과 선택권을 확보하는 방향이어야 함
- 개방성이 결여된 독자 AI는 외형상 주권을 표방하더라도 실질적으로는 또 다른 형태의 '고착'(lock-in)을 초래할 수 있음

◆ 생태계 개방성은 AI 기술의 신속한 '확산'(diffusion)을 통해 'AI 기본사회'를 실현하는데 기여함

- AI 기술을 먼저 개발하는 것에 그치지 않고 이를 신속하게 응용하고 확산해야 새로운 일자리와 부가가치를 창출할 수 있음
- 중소기업과 모든 국민이 큰 비용 부담 없이 다양한 인프라를 통해 AI를 활용하여 생산성과 편익을 높일 수 있음

◆ 국내 AI 서비스가 개발 단계부터 글로벌 시장을 겨냥한 수출형 생태계 기반 조성이 필요하다는 점에서도 개방성이 중요한 역할을 함

- 인구 감소와 내수 시장의 포화라는 구조적 한계를 극복하고 지속 가능한 성장을 담보하기 위해 수출형 생태계로의 전환이 시급함
- 글로벌 호환성을 확보해야 별도의 복잡한 변환 과정 없이 즉시 수출이 가능하며, 혁신의 속도와 다양성을 유지할 수 있음

◆ 개방형 AI 생태계 관점에서 '상호운용성' 정책은 생태계 규칙을 설정(rule-setting)함으로써 개방성을 단순한 선언이 아닌 실질적인 구조로 구현하는 역할을 수행함

- 상호운용성은 인프라, 모델, 서비스, 데이터 등 다양한 생태계 구성요소가 유연하게 호환되는 상태를 의미하며, 이는 특정 공급자에 대한 종속을 방지하고, 멀티클라우드 및 멀티모델 전략을 가능하게 하며, 국제 표준 정합성을 확보하기 위한 필수 조건임

● 또한, 단순한 기술적 연결의 차원을 넘어 AI 생태계 내 공정 경쟁과 지속 가능한 혁신을 결정짓는 핵심 기제로 작용함

◆ **이에 본고에서는 AI 상호운용성의 개념과 필요성을 살펴보고, 주요국의 상호운용성 설계 방식을 비교 분석한 결과 등을 바탕으로 우리나라의 정책 추진 방향과 핵심 과제를 제시 하고자 함**

2. AI 상호운용성의 개념과 필요성

◆ AI 생태계의 상호운용성은 다양한 인프라, 모델, 서비스, 데이터가 자유롭게 연결, 조합, 교체될 수 있는 상태를 의미하며, 크게 네 가지 층위로 구분할 수 있음

- 인프라 상호운용성은 클라우드, GPU 등 AI 모델이 구동되는 물리적/가상적 자원의 호환성을 의미함. 예를 들어, 특정 클라우드에서 학습/배포한 모델을 별도의 수정 없이 다른 클라우드 또는 자체 서버로 이전하여 배포할 수 있음
- 모델 상호운용성은 프레임워크나 런타임에 관계없이 AI 모델을 공유하고 실행할 수 있는 능력을 의미함. 공통 규격인 ONNX(Open Neural Network Exchange)를 통해 모델을 공유하거나 다양한 오픈소스 모델을 표준화된 방식으로 호출하여 사용하는 것이 대표적인 예임
- 서비스 상호운용성은 표준 API 프로토콜을 통해 서로 다른 소프트웨어, 데이터베이스, AI 에이전트가 원활하게 협업하는 능력을 의미함. 하나의 AI 서비스 내에서 외부의 다양한 도구와 데이터를 결합해 복합적인 결과물을 생성하거나 AI 에이전트들이 서로의 기능을 호출하고 정보를 주고받을 수 있게 됨
- 데이터 상호운용성은 서로 다른 AI 시스템이 동일한 데이터를 이해하고 가공할 수 있는 상태를 의미함. 데이터의 형식과 의미를 통일함으로써 시스템 간의 자유로운 데이터 이동을 보장함

◆ 상호운용성은 모델/데이터의 고립(silo) 해소, 기술적 종속 방지 및 비용 절감, 스타트업과 중소기업 활성화, 복원력 및 보안 강화 등을 위해 필요함

- 거대 모델과 특정 산업에 특화된 소형 모델이 서로 정보를 주고받을 수 있는 표준 인터페이스가 없다면 전체 시스템의 효율성이 저하됨. 또한, 이용자가 A 기업의 AI 서비스를 쓰다가 B 기업으로 옮기고 싶을 때 자신의 데이터를 손쉽게 추출해 이전할 수 있어야 데이터 주권이 보장되고 시장의 역동성이 유지됨

- 특정 기업의 AI 모델이나 서비스에 고착될 경우 해당 기업이 가격을 인상하거나 서비스 내용을 변경하더라도 유연하게 대응하기 어려움. 반면, 정부나 기업, 개인이 다양한 솔루션을 자유롭게 조합해 이용할 수 있으면 예산과 시간을 크게 절감할 수 있음

- 스타트업과 중소기업이 혁신적인 AI 서비스를 개발했을 때 글로벌 플랫폼과 즉시 연결되어 전 세계 시장에 진출하고, 대기업이 독점한 데이터나 인프라에 접근할 수 있는 표준 통로를 제공함으로써 기술력 중심의 공정한 경쟁 환경을 조성할 수 있음

- 모든 시스템이 하나로 묶여 있는 폐쇄형 구조보다 상호운용성을 갖춘 분산형 구조가 위기에 강함. 특정 AI 서비스에 장애가 발생하는 경우 호환성이 확보된 다른 서비스로 즉시 대체 가능하기 때문임. 또한, 표준화된 규격은 외부 전문가들이 해당 시스템의 편향성이나 보안 취약점을 점검하기 용이하게 만듦

3. 주요국의 AI 상호운용성 정책

(1) 미국

◆ **미국은 보안 인증과 위험관리 표준 등을 통해 비교적 느슨하지만 호환성 있는 기술 · 거버넌스 생태계를 만들고, 이를 국제 표준으로 확장해 자국 기업의 글로벌 영향력을 강화하는 전략을 취함**

- AI 시스템은 단일 소프트웨어처럼 독립적으로 작동하는 것이 아니라 클라우드, 데이터베이스, 외부 API, 다른 AI 모델 및 응용서비스와 지속적으로 연결됨
- 서로 다른 시스템이 안전하게 연동되지 않거나 데이터 이동 과정에서 오류가 발생할 경우 단순한 기술적 불편을 넘어 심각한 보안 및 안전 사고로 이어질 수 있음
- 따라서 AI 상호운용성을 단지 산업 편의성의 문제가 아니라 AI 안전성과 신뢰성을 보장하기 위한 전제 조건으로 인식

◆ **FedRAMP(Federal Risk and Authorization Management Program)는 연방기관이 사용하는 클라우드 서비스에 대해 공통된 보안 평가 및 모니터링 절차를 제공**

● 한 번 인증받은 보안 평가 결과를 여러 기관이 재사용하도록 해(do once, use many) 클라우드 서비스 간 비교와 전환을 쉽게 만들고, 결과적으로 다양한 클라우드와 AI 서비스가 공통된 보안 기준 위에서 결합될 수 있는 환경을 조성

● 2024년 공표된 FedRAMP 현대화 방향은 FedRAMP 인증 결과에 대한 '적정성 추정'(presumption of adequacy) 원칙을 강화함으로써 중복 심사를 줄이고, 추가 요구는 예외적 필요가 있을 때에만 허용

◆ 표준기술연구소(NIST)의 「AI 위험관리 프레임워크」(AI Risk Management Framework, 이하 "AI RMF")는 AI 시스템이 제3자 데이터, 소프트웨어, 외부 모델 및 기존 시스템과 결합되는 과정에서 발생할 수 있는 위험을 핵심 관리 대상으로 제시

● Govern 기능은 제3자 소프트웨어와 데이터, 기타 공급망 이슈에서 발생하는 AI 위험과 편익을 관리하기 위한 정책과 절차 수립을 강조

● MAP 기능은 AI 시스템의 사용 맥락, 구성요소, 이해관계자, 위험과 편익을 식별하도록 하며, 제3자 데이터나 소프트웨어가 포함된 경우 해당 요소의 기술적·법적 위험도 함께 파악하도록 함

◆ **NIST는 산하에 정부 · 산업 · 학계가 모여 사이버 보안 실증 및 상호운용성 테스트를 수행하는 사이버보안센터 (National Cybersecurity Center of Excellence, 이하 "NCCoE")를 두고 있음**

- NCCoE는 실제 환경을 모사한 테스트베드에서 여러 기업의 제품과 기술을 연동해 보고, 그 결과를 참조 설계(reference design), 예시 구현(example implementation), 실무 가이드 형태로 공개
- 이는 기업들이 추상적인 표준 문서만 참고하는 것이 아니라 실제로 어떤 방식으로 시스템을 연결하고 보안을 확보해야 하는지를 구체적으로 확인할 수 있게 함

※ 유럽연합은 유럽의 공공 · 민간 IT 시스템이 서로 상호운용될 수 있도록 기술 사양 기반 자동 테스트 환경을 제공하는 '상호운용성 테스트베드'(Interoperability Test Bed) 운영

(2) 유럽연합

◆ **유럽연합은 강력한 법적 규제를 통해 상호운용성을 의무화하고, 가이아-X와 같은 연합형 인프라를 통해 디지털 주권을 수호하며 유럽 기업의 경쟁력을 도모**

◆ **AI법(AI Act)은 고위험 AI 시스템에 대해 안전성, 투명성, 데이터 등 필수 요건을 제시하고, 이를 충족하는지를 적합성 평가를 통해 확인하도록 규정**

● 개별 기업이 제각각 구현하는 것이 아니라 조화 표준(harmonised standards) 또는 공통 사양(common specificstion)을 따를 경우 “적합성 추정”(presumption of conformity) 하여 상호운용 가능한 기술·서비스 구조를 사실상 의무화

◆ 데이터법(Data Act)은 데이터 접근 · 공유 규칙을 명확히 하는 동시에, 특히 클라우드 전환과 상호운용성에 관한 장을 두어 고착 방지와 경쟁 촉진을 목표로 함

● 2025년 9월부터 본격 적용된 클라우드 전환 규정은 클라우드 서비스 제공자에게 표준화된 방식의 데이터 자산 이전, 전환 수수료의 점진적 철폐 및 기술/계약/조직적 전환장벽 제거 의무 부과

● 상호운용성 규정은 클라우드 서비스 제공자 및 ‘공통 유럽 데이터 공간’(Common European Data Spaces) 참여자에게 적용되며, 후자에는 데이터의 의미론적(semantic) 호환성, 데이터 구조 및 인터페이스의 표준화 등의 의무 부과

※ 멀티 클라우드 사용을 위한 상호운용성도 포함하되, 데이터 송신이 전환의 일회적 송신과 달리 지속적 활동이 될 수 있으므로, 비용 이하의 범위에서 수수료를 부과할 수 있음

◆ 데이터법 상의 데이터 공간은 2020년 유럽 표준을 준수하는 상호운용 가능하고 안전한 데이터 인프라 구축을 목표로 시작된 ‘가이아-X’ 프로젝트와 관련이 있음

- 이 프로젝트는 의료, 에너지, 모빌리티 등의 분야에서 부문별 데이터 공간 개발을 장려하여 데이터 관리가 투명성, 가역성, 이동성 원칙에 부합하도록 하는 것을 목표로 함
- 2025년 파일럿 단계에서 실제 운영 단계로 전환하면서 15개 이상 공급자의 600여개 서비스를 카탈로그에서 비교 선택 가능하게 하고, 최상위 등급인 Level 3은 항공우주, 국방, 에너지망 등 국가 안보 및 고도의 기밀이 요구되는 용례에 적합하도록 설계

◆ 가이아-X는 다양한 클라우드와 데이터 서비스가 공통의 신원/보안/상호운용성 규칙을 따를 경우 '가이아-X 호환 서비스'로 인정하는 연합형 인프라를 지향

- 데이터 소유자가 언제든지 데이터 공유를 허용 및 철회할 수 있고, 개방형 표준과 오픈소스를 활용한 데이터/서비스 상호운용 인프라이며, 규정 준수 수준에 따라 서비스 라벨을 부여하여 이용자가 목적에 맞는 서비스를 선택할 수 있도록 지원
- 이러한 데이터 공간은 장기적으로 독자 AI 인프라와 결합되어 공공/산업 데이터가 특정 플랫폼에 종속되지 않고, 여러 AI 시스템에서 동일한 규칙 아래 공유되는 것을 지향

◆ 디지털시장법(Digital Markets Act)은 핵심 플랫폼 서비스를 제공하는 게이트키퍼 사업자에게 강력한 상호운용성 의무를

부과하고 있으며, AI 서비스와 클라우드도 핵심 플랫폼 서비스에 포함됨

- EC는 2026년 4월 27일 구글이 안드로이드 핵심 기능에 대한 서드파티(특히, AI 서비스 제공사업자)의 접근과 상호운용성을 보장하도록 의무를 구체화하는 내용의 심사보고서를 발송하고 의견 수렴 절차를 개시함
- 2026년 4월 28일 공표된 디지털시장법 첫번째 검토 보고서에서 향후 법 적용에 있어 AI 및 클라우드 부문에 대한 심층 검토가 우선순위가 될 것이라고 밝힘

(3) 영국

◆ **영국은 '오픈 스탠다드'와 'API-by-default' 원칙을 정부 기술 정책의 중심에 두고, 조달 체계를 통해 공공 구매력을 레버리지로 삼아 시장의 표준화를 유도**

◆ **2020년 「국가 데이터 전략」에서 데이터 표준의 개발과 활용을 통해 서로 다른 부문과 조직 간에 데이터 호환성을 보장하고, 정부 서비스 전반에 'API-by-default' 방식을 채택해 데이터 · 서비스가 API를 통해 연계되도록 하는 방향을 제시**

◆ 2021년 「기술 실무지침」(Technology Code of Practice, 이하 "TCoP") 및 2018년 「오픈 스탠다드 원칙」(Open Standards Principles)에서 '오픈 스탠다드 사용'을 정부 IT의 기본 원칙으로 명시

- TCoP는 정부가 기술 서비스를 설계·구축·구매할 때 준수해야 할 13개 원칙을 제시하는데, 그 중 '오픈 스탠다드 사용' 원칙에서 정부 기술이 다른 기술과 호환되고 쉽게 업그레이드 및 확장될 수 있도록 개방형 표준을 사용해야 한다고 명시하면서 「오픈 스탠다드 원칙」을 따르도록 규정

- 「오픈 스탠다드 원칙」은 정부 IT 분야에서 소프트웨어 상호운용성, 데이터 및 문서 형식에 대한 개방형 표준을 선정하는 방법 및 개방형 표준을 오픈소스 및 독점 소프트웨어에 구현하는 방법에 대한 지침을 제공

◆ 조달 체계 전반에 TCoP와 「오픈 스탠다드 원칙」을 필수 적용하여 표준 API 도입, 데이터 호환성, 클라우드 전환 용이성 등을 입찰 및 계약의 핵심 요건으로 명시

- 명확한 이유가 없는 한 개방형 표준을 입찰 요건에 포함해야 하며, 미사용 시 경제성 평가 후 오픈 스탠다드 위원회에 예외 허용 신청

◆ **2025년 제정된 「데이터 이용·접근법」(Data Use and Access Act)은 기존의 개인정보 보호 중심에서 벗어나 데이터를 경제 성장의 핵심 자산으로 활용하려는 전략이 집약된 법으로서 'API-by-default'를 법제화**

- 특정 산업군에 대해 API 기반 데이터 공유를 의무화할 수 있으며, 이를 관리할 인터페이스 기구를 설립할 수 있음
- 유럽연합이 데이터법을 별도로 제정한 것과 달리, 개인정보보호법을 개정하는 방식을 택하여 규제 혼선을 줄이면서도 기존의 개인정보 보호 프레임워크 안에 스마트 데이터와 상호운용성이라는 혁신 엔진을 장착하려는 실용적인 선택으로 분석됨
- 다만, 개인정보보호법이 개인정보에만 적용되어 산업데이터를 포괄할 수 없는 한계를 극복하기 위해 '사업 데이터' (business data) 개념을 도입하여 非개인정보를 포함

(4) 시사점

◆ **미국은 혁신 및 시장 중심의 인증/표준 모델, 영국은 오픈 스탠다드와 공공 조달로 시장 구조를 바꾸는 모델, 유럽연합은 디지털 주권과 기본권 보호 중심의 강한 규범 모델의 특징을 가지고 있음**

◆ 상호운용성은 단순한 기술 규격이 아니라 국가 주권과 산업 경쟁력을 결정짓는 전략적 인프라로서 인증(표준), 조달(시장 동인), 규범(법적 강제)이 상호보완적으로 작동하는 패키지형 정책 설계가 필요함

- 데이터 공간 및 클라우드 인프라 구축의 초기 단계부터 상호운용성을 핵심 요건으로 반영해야 향후 발생할 시스템 통합 비용과 사회적 마찰을 최소화할 수 있음
- 전담 기구 설치, 서비스 라벨링, 표준 카탈로그 제공 등을 통해 시장 참여자의 자발적 행동을 유도할 수 있는 기제를 마련해야 함

4. 정책 제언

◆ **우리나라는 AI 전 영역을 아우르는 통합적 상호운용성 프레임워크가 미흡하고, 시험 · 인증 체계 또한 보안과 품질 위주에 머물러 있음**

● 이에 모델, 서비스, 데이터 전반의 공통 표준 수립과 시험/인증을 통해 조합과 교체를 가능하게 하고, 이를 조달 제도와 연계하여 기술 종속을 방지하면서 통제력과 글로벌 확장성을 동시에 확보할 것을 제안함

(1) AI 상호운용성 프레임워크 구축

◆ **현재 전자정부 표준프레임워크에 행정 데이터 및 시스템 간 상호운용성 기준은 마련되어 있으나, 모델, API, 클라우드, 데이터 전 영역을 포괄하는 'AI 상호운용성'은 명시적으로 설계되어 있지 않음**

● 미국 AI RMF에서 상호운용성을 핵심 위험 요인 및 관리 항목의 하나로 포함하고, 유럽연합 AI법 및 데이터법에서 조화표준을 따를 경우 규정을 준수한 것으로 추정한다는 점 등을 참고할 필요가 있음

◆ **향후 AI 전용 부문을 추가하여 모델, 서비스, 데이터별 표준을 정의하고, 글로벌 규범(미국 AI RMF, 유럽연합 조화표준, ISO/IEC 표준 등)과 정합성을 확보해야 함**

- AI 모델 측면에서는 공통 모델 포맷 및 모델 메타데이터 표준을 정의하고, 모델 버전, 변경 이력, 학습 데이터 범주를 기록하는 공통 구조를 마련하며, 고영향/공공용 모델에 대해 모델 이력 및 출처 추적 가능성을 확보
- AI 서비스 측면에서는 LLM, 멀티모달, 추천·검색, 예측 모델 등 주요 서비스 유형별 공통 API 규격(입·출력 구조, 오류 코드, 안전 필터링 인터페이스 등)을 정하고, 이 규격을 해외 수출 시 한국형 레퍼런스로 활용할 수 있도록 설계
- 데이터 측면에서는 도메인별 데이터 공간을 전제로 하는 공통 데이터 스키마, 메타데이터, 식별자 표준을 정하고, 규제 및 위험관리 대응을 위한 로그, 이벤트 데이터 포맷 및 제공 방식을 정함

(2) 상호운용성 시험/인증 체계 구축

◆ **상호운용성은 선언이 아니라 시험 가능한 규격으로 만들어야 시장에서 작동함**

- 미국과 유럽연합에서 AI 상호운용성 테스트베드를 운영하고 있다는 점을 참고할 필요가 있음

◆ **우리나라도 별도의 전담기관 또는 기존 인증기관 내 전담 조직으로 'AI/클라우드 상호운용성 시험/인증 센터'를 설립하는 방안을 검토해야 함**

● 모델 호환성, API 규격 준수, 데이터 이동성과 클라우드 전환, 로그 및 감사데이터 표준 준수 등을 검증하며, 의료, 교육, 교통 등 핵심 공공 분야부터 시범 운영 후 단계적으로 확대

(3) 도메인별 데이터 공간 설계

◆ **현재 공공데이터 개방 및 표준화 사업은 활발히 진행되고 있으나, 도메인별 데이터 및 서비스의 상호운용성을 중시하는 유럽연합식 데이터 공간 개념은 초기 단계에 머물고 있음**

◆ **향후 데이터 공간 설계는 단순 개방이 아닌 '통제 가능한 공유'를 목표로 해야 함**

● 의료, 교육, 교통, 제조 등 주요 분야에서 데이터 공간을 설계할 때 각 데이터 공간의 데이터 구조, 접근 및 공유 API, 메타데이터 규칙을 상호운용성 프레임워크와 일치시키고, AI 모델이 이 표준 API를 통해서만 접근/학습하도록 설계하면 향후 모델이나 클라우드를 변경하여도 데이터 자산은 유지할 수 있음

● 즉, 데이터 자산은 국가가 안전하게 통제하면서도 상단의 AI 모델이나 클라우드는 필요에 따라 유연하게 교체하거나 조합할 수 있는 구조가 가능해짐

(4) 조달 제도와의 연계 강화

◆ **현재 AI/클라우드 조달 체계에서 보안 인증, 품질 기준 등은 존재하지만, 데이터 이동성, 클라우드 전환, 모델 포맷 호환성 등을 입찰과 평가에 체계적으로 반영하는 구조는 미흡**

- 일부 감사·보안 지침에 '소스코드/데이터 인계' 정도는 있지만, 전략적인 탈 고착 설계 수준에는 미치지 못함
- 영국이 오픈 스탠다드 원칙을 정부 기술정책의 중심에 두고, 조달 체계를 통해 상호운용성을 촉진하는 것을 참고할 필요가 있음

◆ **우리나라도 AI/클라우드/데이터 플랫폼 조달 시 상호운용성 조건을 입찰 요건, 평가 기준 및 계약조항에 반영해야 함**

- 예를 들어, 표준 포맷 지원, 계약 종료 시 합리적인 이전 가능성 보장, 독점적인 비공개 API 의존 지양, 상호운용성 시험/인증 센터의 인증/라벨을 보유한 경우 가점을 부여하는 방식을 고려할 수 있음
- 특정 사업자 종속을 방지하기 위해 일정 규모 또는 일정 기간 이상의 대규모 공공사업은 멀티클라우드 구조를 원칙으로 함

◆ **기관별 각기 다른 기준을 적용하지 않도록 보안 인증을 재사용 가능한 인가 패키지 개념으로 전환해야 함**

- 동일한 통제 항목에 대해서는 주평가자를 지정하여 단일 평가를

수행하고, 다른 절차에서는 그 결과를 인정하는 구조로 개편

- 변경사항이 발생한 특정 항목만 부분적으로 갱신하도록 하여 기업의 재심사 부담을 줄이면서도 통제력을 유지

(5) 상호운용성의 법제화 검토

◆ 조달 기준은 공공과 거래할 경우에만 적용되므로, 민간 영역의 대기업 종속 해소를 위한 법적 근거는 부족함

- 영국이 「데이터 이용·접근법」을 통해 데이터 이동성을 의무화하고, 유럽연합이 「데이터법」을 통해 클라우드 전환을 용이하게 한 것을 참고할 수 있음

◆ 우리나라도 데이터 이동성과 클라우드 전환 권리를 법률에 명시해서 상호운용성을 선택이 아닌 시장 전체의 기본 규칙으로 정립하는 방향도 검토 가능

- 개인정보보호법에 따라 2025년 3월 의료, 통신 분야를 중심으로 개인정보 전송요구권이 본격 시행되었으며, 2026년 8월부터 전 분야로 본인전송요구권이 확대됨
- 하지만 개인정보에 국한되는 한계가 있어 산업데이터를 포함하는 데이터 이동성 법제화 및 클라우드 전환권 법제화에 대한 검토 필요

5. 마치며

◆ **개방형 AI 생태계를 구현하기 위해서는 상호운용성 확보와 더불어 법/계약, 공급망, 기술, 운영 통제를 유기적으로 결합한 인증 및 조달 체계가 필요함**

- 미국, 영국, 유럽연합 등 주요국 사례는 상호운용성을 구현하는 정책 도구가 각기 다르더라도 표준, 시험, 조달, 규범을 결합해 시장 참여자의 행동 변화를 유도한다는 공통점이 있음
- 우리나라도 AI 상호운용성 프레임워크를 통해 기술과 데이터 기준을 통합하고, 실질적 호환성을 담보할 시험/인증 체계를 구축하며, 도메인별 데이터 공간을 표준 API 기반으로 설계할 필요가 있음
- 또한, 조달 단계에서 데이터 이동성, 클라우드 전환, 모델 포맷 호환성 등 탈 고착 조건을 절차 전반에 반영하고, 필요하다면 전환 권리의 법제화도 검토해야 함

◆ **이러한 정책 패키지는 특정 사업자/기술에 대한 의존도를 낮추는 동시에 국내 AI 산업의 경쟁력을 제고하여 진정한 기술 주권을 확립하고, 한국형 AI 생태계가 지속 가능한 국가 인프라이자 글로벌 경쟁력을 갖춘 수출 자산으로 자리매김하는 데 기여할 수 있음**

참 고 문 헌

EC (2023), Introducing the Interoperability Test Bed.

Gaia-X European Association for Data and Cloud AISBL (2025.11), Gaia-X Enters Season 2.0 of Data Spaces and Digital Ecosystems with Summit 2025.

Government of Canada (2025.11), Digital Sovereignty: A Framework to improve digital readiness of the Government of Canada.

NIST (2025), NIST National Cybersecurity Center of Excellence Overview.

NIST (2023), AI Risk Management Framework.

UK Government (2023), G-Cloud Framework Guidance.

US OMB (2024), Modernizing the Federal Risk and Authorization Management Program.

〈웹사이트〉

EC Interoperability Test Bed
https://interoperable-europe.ec.europa.eu/collection/interoperability-test-bed-repository/solution/interoperability-test-bed

UK National Data Strategy
https://www.gov.uk/guidance/national-data-strategy

UK Open Standard Principles
https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles

US FedRAMP
https://www.fedramp.gov/archive/2020-05-07-how-agencies-can-reuse-a-fedramp-authorization/

US NIST NCCoE
https://www.nist.gov/itl/applied-cybersecurity/national-cybersecurity-center-excellence-nccoe