

AI 가치사슬 전반의 실효적 책임성:

사업자 역할에 상응하는 AI 책임 배분

인공지능(AI)은 경제 전 부문에서 디지털 전환을 이끌고 있습니다. 제조업체는 AI를 활용해 안전하고 지속가능한 제품을 설계하고, 중소기업은 AI 번역 도구를 통해 전 세계 고객에게 다가갑니다. 보건의료 연구자는 AI를 활용해 환자 치료의 질을 높이고 새로운 의학적 성과를 만들어내며, 업종을 막론하고 기업들은 AI 시스템으로 자사 제품의 장애인 접근성을 높일 수 있습니다. 이처럼 AI는 다양한 분야에서 복잡한 문제를 풀어낼 새로운 가능성을 열어가고 있습니다.

AI가 제대로 자리 잡으려면 기술에 대한 신뢰와 확신이 뒷받침되어야 합니다. 이에, 정책 입안자들이 신뢰성과 책임성을 높이기 위한 제도를 설계할 때 짚어야 할 원칙이 하나 있습니다. 기업이 지는 책임은 그 기업이 맡은 역할에 걸맞아야 한다는 것입니다.

AI 가치사슬에서 각 주체의 역할에 맞게 책임을 정하는 것은 서로 구별되면서도 상호 연관된 측면에서 중요합니다. 기업의 관련 정보 접근 권한과 AI 공급망 내 위치를 바탕으로 현실적인 책임을 부여함으로써, 기업이 통제할 수 없는 사항에 대해 이행하기 어려운 의무를 부담하는 것을 방지할 수 있습니다. 둘째, 위험을 식별하고 대응하기에 적합한 위치에 있는 기업을 소비자와 기업 고객을 보호하는 데 필요한 조치를 취할 책임 주체로 지정함으로써, 이들을 보다 효과적으로 보호할 수 있습니다. 셋째, 현장에서 실효성 있게 적용할 수 있는 정책 체계를 마련할 수 있습니다.

AI 생태계의 주요 주체

AI 공급망은 복잡하고 지속적으로 변화하고 있으며, 인공지능 개발사업자(developer), 통합사업자(integrator), 이용사업자(deployer) 등 다양한 기업으로 구성됩니다. 많은 경우 개발사업자가 AI 시스템을 만들고, 이용사업자가 이를 실제 환경에서 사용합니다.

개발사업자 AI 시스템을 설계·코딩·제작



이용사업자 AI 시스템을 사용

예시 AI 시스템을 설계·코딩·제작하는 기업을 개발사업자라고 합니다. 예를 들어, 음성 인식용 AI 시스템을 개발하는 소프트웨어 기업이 이에 해당합니다.

하나의 기업이 개발사업자인 동시에
이용사업자일 수 있습니다

예시 AI 시스템을 사용하는 기업을 이용사업자라고 합니다. 예를 들어, 은행이 자체 개발했거나 제3자가 개발한 AI 시스템을 대출 심사에 활용하는 경우, 은행은 이용사업자에 해당합니다.

예시 사이버보안 기업이 네트워크 트래픽과 고객 거래를 모니터링하는 AI 소프트웨어를 개발한 후 이를 자사 시스템에 직접 사용하는 경우, 해당 기업은 개발사업자이자 이용사업자에 해당합니다.

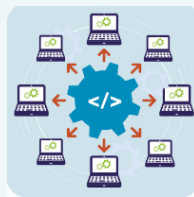
다른 경우에는 한 기업이 AI 모델을 개발하고, 두 번째 기업이 이를 애플리케이션이나 플랫폼(AI 시스템)에 통합하며, 세 번째 기업이 해당 AI 시스템을 활용해 특정 업무를 수행할 수 있습니다. 예를 들어, 기업의 금융 거래 데이터에서 인사이트를 도출하는 콘텐츠 관리 플랫폼을 이용해 문서를 요약하는 업무가 이에 해당합니다.

개발사업자



모델 개발사업자는 텍스트를 요약하거나 이미지를 생성하는 생성형 AI 모델을 개발할 수 있습니다.

통합사업자



통합사업자는 해당 생성형 AI 모델을 자체 소프트웨어 애플리케이션에 통합하여, 화상 커뮤니케이션 플랫폼에서 회의 내용을 기록·요약하거나 문서 관리 소프트웨어를 활용하여 사업 계약서를 분석하는 등의 기능을 제공할 수 있습니다.

이용사업자

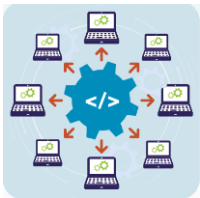


이용사업자는 통합사업자의 소프트웨어 애플리케이션을 활용하여 주요 비즈니스 문서를 검색해 특정 질문에 대한 답변을 찾거나 요약본을 생성하는 등 일반적인 업무를 지원할 수 있습니다.



개발사업자(Developers)

개발사업자에는 AI 시스템과 그 기반이 되는 모델을 개발하고, 해당 AI 시스템 전체를 고객에게 판매하거나 라이선스를 제공하는 기업이 포함됩니다. 기업용 인사관리 소프트웨어나 업무 협업 소프트웨어가 그 예입니다. 범용 AI 영역에서 모델 개발사업자는 매우 다양한 애플리케이션에 활용될 수 있는 AI 모델을 개발합니다. 예를 들어, 한 기업이 다양한 용도에 맞게 조정해 사용할 수 있는 파운데이션 모델을 개발할 수 있습니다. 동일한 파운데이션 모델은 검색 엔진, 챗봇, 스팸 탐지 소프트웨어, 긴 문서를 요약하는 도구 등 다양한 AI 시스템을 구동하는 데 쓰일 수 있으며, 그 밖의 여러 애플리케이션에도 활용될 수 있습니다. 일반적으로 개발사업자는 자사의 AI 모델이나 시스템이 어떻게 개발되었는지에 관한 정보를 갖고 있지만, 다른 기업이 해당 AI 도구를 어떻게 사용하는지에 관한 정보는 부족합니다.



통합사업자(Integrators)

다른 기업, 즉 '통합사업자'는 AI 모델을 특정 애플리케이션에 통합해 다른 기업이 사용할 수 있도록 합니다. 어떤 통합사업자는 AI 모델을 특정 AI 시스템이나 애플리케이션에 연결하기만 할 수도 있지만, 또 다른 통합사업자는 모델을 미세 조정하거나 수정한 뒤 AI 시스템이나 애플리케이션에 통합하기도 합니다. 예를 들어, 한 기업이 하나 이상의 제3자 AI 모델을 통합한 AI 애플리케이션을 개발하는 경우, 그 기업은 통합사업자의 역할을 합니다. 일반적으로 통합사업자는 자신이 AI 모델에 가한 변경 사항에 관한 정보를 갖고 있지만, 모델의 최초 개발 과정이나 이용사업자가 이후 AI 시스템을 어떻게 사용하는지에 대해서는 직접적인 정보를 갖고 있지 않습니다.



이용사업자(Deployers)

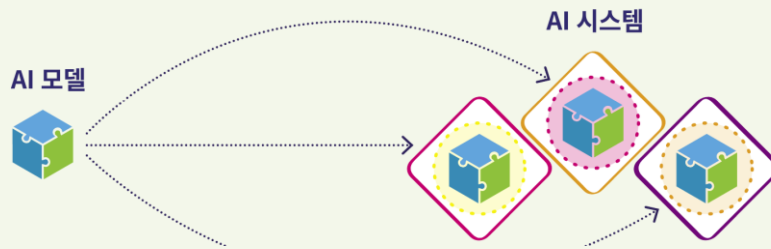
흔히 특정 목적을 위해 AI 도구를 사용하는 기업을 이용사업자라고 부릅니다. 이런 기업은 특정 AI 기술을 언제, 어떻게 사용할지 결정하므로 구체적인 사용 사례와, 관련 사실관계를 파악하고 있습니다. 그러나 이용사업자는 대개 다른 기업으로부터 AI 도구를 제공받는 경우가 많아, 해당 도구의 최초 학습 과정에 대해서는 직접적인 정보를 갖고 있지 않습니다. 대체적으로 이용사업자는 소비자와 직접적인 관계를 맺는 기업인 경우가 많습니다.

효과적인 정책 및 책임 체계는 주체의 유형 차이를 고려해 획일적인 요건의 적용을 피하고, 각 주체의 역할에 맞는 책임을 부여해야 합니다. 이는 AI 공급망에 참여하는 주체 별로 접근할 수 있는 정보의 범위가 상이하고, 고객을 보호하기 위해 관련 위험을 식별하여 이를 대응하는 데 필요한 조치를 취할 수 있는 역량과 위치 또한 서로 다르기 때문에 중요합니다.

예를 들어, 일반적으로 파운데이션 모델 개발사업자는 자사 모델의 설계와 학습에 관한 사항을 설명할 수 있지만, 통합사업자가 해당 모델을 특정 애플리케이션에 맞게 조정하는 방식이나 이용사업자가 이후 해당 AI 시스템을 실제로 어떻게 사용하는지에 대해서는 알지 못합니다. 반면, 해당 AI 시스템을 사용하는 이용사업자는 시스템이 어떻게 활용되고 있는지, 그 사용이 당초 의도된 용도에 부합하는지, 운영 과정에 인적 감독을 어떻게 적용할 수 있는지를 파악하기에 가장 적합한 위치에 있습니다. 또한 AI 시스템이 생성한 결과물을 검토하고, 최종 이용자의 불만을 접수하며, 시스템 성능에 영향을 미칠 수 있는 실질적 환경 요인을 평가하기에도 가장 적합한 위치에 있습니다.

다른 분야에서와 마찬가지로, AI 시스템을 설계하고 사용하는 기업에 의무를 부과하는 법률이나 정책 체계는 이러한 역할의 차이를 반영해 적절한 책임을 배분해야 합니다.

AI 모델과 AI 시스템



AI 모델이란?

AI 모델은 대량의 데이터를 학습하여 패턴을 인식하거나 예측하고, 콘텐츠를 생성하는 등의 기능을 수행하도록 개발된 소프트웨어입니다.

다음과 같이 비유할 수 있습니다.

- » 수많은 사례를 통해 학습했거나 경험을 통해 꾸준히 학습하는 **숙련된 전문가**
- » 언어, 이미지, 숫자를 처리할 수 있는 **두뇌**

모델이 할 수 있는 일의 예시:

- » 문장에서 다음에 올 단어 예측
- » 이미지 속 사물 인식
- » 텍스트, 이미지, 코드 생성

모델 그 자체만으로는 일반적으로 **사용자가 편리하게 이용하기 어렵습니다**. 사용자 인터페이스나 버튼, 화면, 작업 흐름 등의 기능이 갖춰져 있지 않기 때문입니다.

AI 시스템이란?

AI 시스템은 하나 이상의 AI 모델을 활용해 특정 작업을 수행하거나 문제를 해결할 수 있도록 구성된 완전한 형태의 도구 또는 제품입니다.

다음과 같이 비유할 수 있습니다.

- » 엔진(모델)뿐 아니라 운전대, 좌석, 각종 조작 장치까지 갖춘 **자동차**.

AI 애플리케이션에는 채팅 인터페이스, 버튼, 메뉴, 음성 입력뿐 아니라 규칙과 안전장치, 이메일, 캘린더, 데이터베이스 등과의 연동 기능도 포함될 수 있습니다.

AI 시스템의 예는 다음과 같습니다:

- » 고객의 질문에 답변하는 챗봇
- » 이미지를 보정하는 사진 어플리케이션
- » 이메일 초안 작성을 지원하는 글쓰기 도우미

역할 기반 정책 접근의 선례

역할에 따라 의무를 설정하는 것은 전 세계 개인정보 보호 및 보안 법제에서 모범적인 입법 관행으로 여겨집니다. 예를 들어, 미국을 비롯한 세계 각국의 개인정보 보호법은 데이터 처리 방식과 목적을 결정하는 컨트롤러(controller)와 컨트롤러를 대신해 그 지시에 따라 데이터를 처리하는 프로세서(processor)의 역할을 구분하고 있습니다. 마찬가지로 여러 관할권의 사이버보안 법제에서도 일반적으로 기업과 그 기업의 서비스 제공업체(service provider)를 구분해 규율하고 있습니다.

개인정보 보호 및 보안 법제가 소비자의 개인정보를 처리하는 기업을 역할에 따라 구분하듯, AI 공급망을 구성하는 다양한 주체를 구분한다면 법적 체계는 AI 생태계 내 각 주체의 역할에 맞는 적절한 의무를 부여할 수 있을 것입니다. 이를 통해 해당 주체는 부여된 의무를 실질적으로 이행하고, 소비자를 보다 효과적으로 보호할 수 있습니다.