AI 표준화 및 시험인증

백성복 인공지능기반기술(PG1005) 부의장, KT 융합기술원 책임연구원

1. 머리말

인공지능 기술이 점차 보편화되면서 인공지능 기반기술 및 응용기술에 대한 표준화와 각 기술의 시험이나 평가, 인증 체계의 중요성과 필요성이 부각되고 있다. 이는 인공지능 기술과 응용이 사회와 개인에 미치는 영향력이 크고 그 범위가 넓어서 해당 시스템의 안전성과 신뢰성을 확인하는 것이 매우 중요하기 때문이다. 하지만 인공지능 및 기계학습 분야의 표준 관련 활동은 대부분 초기 태동 단계에 있으며, 산업계에 실질적인 도움을 줄 표준 체계를 갖추기 위해 극복해야 할 많은 과제가 있다.

인공지능 분야의 표준화가 직면한 가장 큰 문제 중 하나는 인공지능 시스템의 개발 및 배포에 대한 명확하고 일관된 지침이 부족하다는 것이다. 또 다른 문제는 이 분야의 기술이 유례없이 빠른 속도로 진화하고 있다는 것이다. 새로운 인공지능 프레임워크와 알고리즘이 지속적으로 개발되고 있기 때문에 관련된 표준을 최신 상태로 유지하려면 많은 노력이 필요하다.

시험, 평가 및 인증은 인공지능 시스템의 안전과 신뢰성을 보장하는 중요한 구성 요소이다. 이러한 프로세스는 인공지능 시스템이 특정 표준 및 요구 사항을 충족하는지 확인하기 위한 메커니즘을 제공한다. 또한 인공지능 시스템이 내리는 결정이 안전하고 신뢰할만하다는 일정 수준의 보증을 제공하는 수단이 된다.

인공지능 기술의 발전 속도에 맞추어 기업의 실무자들이 인공지능 시스템의 안전과 신뢰성을 보장하기 위해 무엇이 필요한지 쉽게 파악할 수 있도록 지원하며, 규제 및 감독 기관의 담당자들이 새로운 인공지능 시스템을 평가하고 그 사용을 승인하기 위한 적절한 근거를 제시할 수 있도록 실질적인 표준 및 시험 인증 절차를 조속히 구축할 필요가 있다.

이 글에서는 현재 활발히 진행되고 있는 국내외 표준화기구의 인공지능 관련 표준화 및 시험 평가 기준 수립 활동에 대해 살펴보고 해당 단체들이 지향하고 있는 미래 표준화 방향에 대해 검토해 본다.

2. 국내외 표준화 동향

2.1 국내 표준 단체 활동 현황

인공지능을 표준화 주제로 다루고 있는 대표적인 기구와 그들의 주요 수행 내용이 <표 1>에 나열되어 있다. KS 표준에서는 기존에 정의한 인공지능 기본 개념 및 용어에 대한 개정 및 관리 작업이 진행될 것으로 보이며, TTA 산하 프로젝트 그룹별로 인공지능 기반 기술 및 응용에 대한 표준화 작업이 진행 중이다. 지능정보기술포럼 및 산업인공지능표준화 포럼에서는 지도학습 기술 및 관련 데이터를 중심으로 지능정보 기술에 대한 지속적인 표준화 활동이 예상된다.

2.2 국외 표준 단체 활동 현황

인공지능 분야 표준화 주도권 확보를 위한 각국의 경쟁이 국제 표준화 기구를 무대로 치열하게 전개되고 있다. <표 2>에 인공지능 분야의 대표적인 표준화 기구와 각 기구별 활동 내용이 나열되어 있다.

ISO 산하에 조직되어 정보기술 표준을 담당하는 JTC1에서는 예하의 스터디 그룹들이 인공지능 개념, 신뢰성, 윤리성, 평가 등 다양한 표준화 주제를 다루고 있다. ITU-T는 인공지능 기반의 네트워크, IoT, 보안, 멀티미디어 등에 대한 인공지능 접목을 주제로 표준 개발을 수행하고 있

<표 1> 국내 표준화 현황

구분	표준화 기구	주요 내용
국가 (KS)	국가기술표준원/ 국립전파연구원	인공지능 기본 개념 및 전문가 시스템, 기계학습, 신경망 등 용어 표준 제·개정 진행 중
단체 (TTA)	지능형 반도체 PG (PG417)	고성능 인공지능 시스템 구성을 위한 다중 칩 기반 인공지능 반도체의 기능 안전 및 성능에 대한 평가 등이 주요 표준화 이슈로 진행 중
	스마트헬스 PG (PG419)	스마트헬스 서비스를 위한 영상 교환 인공지능 데이터 플랫폼, 진단 보조 인공지능 모델용 학습 데이터 등 진단과 치료의 영역에서 활용될 수 있는 표준화 아이템이 진행 중
	스마트농축수산 PG (PG426)	농·축·수산물의 양육 과정에서 인공지능 기술을 활용하여 장비/기기 및 환경 제어하는 기술의 표준 개발 진행 중
	지능형 CCTV PG (PG427)	인공지능 기술을 이용하여 CCTV 영상의 분석, 복원을 수행하기 위한 인터페이스 및 상호연동 표준 개발 진행 중
	소프트웨어 품질평가 PG (PG604)	인공지능 소프트웨어의 품질평가를 위한 척도를 개발하고 있으며, 인공지능을 소프트웨어 평가의 하나 사례로 개발 진행 중
	메타데이터 PG (PG606)	자연어처리 및 인공지능 연구를 위한 다양한 데이터의 수집/저장/분석/관리 관련 메타데이터 기술 표준화 진행 중
	디지털콘텐츠 PG (PG610)	인공지능 기술을 이용하여 3D 콘텐츠 제작 및 웹서비스 화하는 디지털 콘텐츠 응용기술에 대한 표준화 진행 중
	사물인터넷/ 스마트시티 플랫폼 PG (PG1001)	지능형 재난 상황관리 총괄 시스템, 5G 기반 스마트시티 영상정보 수집 및 지능형 분석 시스템 등 사물인터넷 분야에 인공지능을 접목한 지능형 서비스 기술 표준화 진행 중
	클라우드 컴퓨팅 PG (PG1003)	에지 컴퓨팅 기반의 지능형 우편 종합 물류 프레임워크 등 지능형 에지 컴퓨팅 기반 응용서비스 기술 표준화 진행 중
	인공지능기반기술 PG (PG1005)	지능형 질의응답 시스템을 위한 개체 연결 표준, 설명가능 인공지능 기술과 유즈케이스, 인공지능 학습용 데이터 참조 기준 등 인공지능 기반 기술 및 인공지능 학습용 데이터 분야 표준화 진행 중
포럼	지능정보기술포럼	지도학습을 위한 데이터 품질 평가 지침, 설계/제조 분야 인공지능 데이터 요구사항 등 AI 데이터 분야 표준화 작업 수행 중
	산업인공지능표준화 포럼	인공지능 데이터 축적 방법 및 포맷, 인공지능 신뢰성 평가 기준 및 윤리 가이드라인, 인공지능 적용 산업별 상호운용성 확보를 위한 표준화 추진 중

출처: ICT 표준화 로드맵 Ver 2023

고 ETSI도 인공지능 기반 통신망 운용관리에 초점을 맞춘 표준화 활동을 선도하고 있다. 그 외에도 다양한 사실 표준화 기구에서 인공지능 모델의 호환이나 윤리성, 견고성 등에 대한 논의가 이루어지고 있다.

3. 표준 기구 활동 사례

3.1 국제 표준화 그룹: ITU-T SG13

ITU-T 산하에 조직되어 미래 네트워크 및 이동 통신망의 지능화 관련 제반 표준의 제·개정 작업을 주도적 수행하는 그룹인 SG13은 2016년 딥러닝이 주목받기 시작하자 이듬해 2017년 인공지능 포커스그룹(FG-ML5G, Focus Group on Machine Learning for Future Networks including 5G)을 발족하고 유즈케이스, 아키텍처, 데이터 등을 주제로 인공지능을 통신망 분야에 적용하기 위한 각종 연구와 문서화 작업을 시작하였다.

포커스그룹에서 작업한 내용은 대부분 상위 조직인 SG13으로 연계되어, 인공지능 관련 주제로 10종 이상의 정식 권고안으로 발표되었다. 주

<표 2> 국외 표준화 현황

구분	표준화 기구		주요 내용
공식	ITU	SG2	(Operational aspects) 인공지능을 활용한 통신 운영 작업 절차 요구사항 및 통신 운영·관리의 지능 레벨 등의 표준화 진행 중
		SG5	(EMF, environment, climate action, sustainable digitalization, and circular economy) 에너지 효율성 관리, 공급 체인 관리, 데이터 센터 구조에서 인공지능 기술 적용 표준 개발 중
		SG11	(Signalling requirements, protocols, test specifications and combating counterfeit telecommunication/ICT devices) 지능형 에지 컴퓨팅 프로토콜, 지능형 네트워크 슬라이싱 관리를 위한 프로토콜 표준 개발 중
		SG12	(Performance, quality of service(QoS) and quality of experience(QoE)) 네트워크 성능, 서비스 품질(QoS) 및 경험 품질(QoE) 분야 인공지능 기술 적용 표준 개발 중
		SG13	(Future networks and emerging network technologies) 미래 네트워크 및 이동 통신망의 지능화 관련 제반 표준의 제·개정 작업 주도적 수행
		SG16	(Multimedia and related digital technologies) 비전, AR, VR 등 멀티미디어 서비스에 인공지능을 활용하기 위한 프레임워크 및 관련 응용 서비스 표준개발
		SG17	(Security) 통신 기반의 다양한 서비스 기술에서 개인정보 보호, 아이디 관리, 침해 대응, 인증서, 인공지능 응용 분야에 대한 보안 표준화 진행 중
		SG20	(Internet of things(IoT) and smart cities and communities(SC&C)) 연합 머신러닝 기반의 IoT 및 스마트시티 커뮤니티 서비스 요구사항, 지능형 IoT 서비스를 위한 분산 기계학습 표준화 진행 중
		FG-AI4NDM	(AI for Natural Disaster Management) 자연재해로부터 구조 및 조기 경보 등의 관리 분야에 인공지능 기술 적용 연구 수행
		FG-AI4 EE	(Environmental Efficiency for AI and other Emerging Technologies) 지속가능한 접근방법과 환경 효율 증진을 위한 기술 분야에 인공지능 기술 적용 연구 수행
		FG-AI4 AD	(AI for autonomous and assisted driving) 자율주행 및 보조 운전에서 인공지능 시스템이 지원하는 서비스 및 애플리케이션에 대한 표준화 활동 지원을 위해 자율주행 인공지능 시스템에 대한 최소 성능 임계값 등에 관한 연구 수행
		FG-AI4H	(Artificial Intelligence for Health) 헬스케어 분야에서 인공지능 적용을 위해 의료 인공지능의 벤치마킹 프레임워크, 건강 알고리즘 프레임워크 등에 대한 평가 및 검증 연구 수행
		FG-AI4A	(Artificial Intelligence(AI) and Internet of Things(IoT) for Digital Agriculture) 디지털 농업 분야 인공지능 기술 적용을 위한 데이터 획득 및 모델링, 윤리·법률·규제 고려사항 등에 관한 연구 수행
	JTC1	SC29	(Coding of audio, picture, multimedia and hypermedia information) 멀티미디어에 인공신경망 기술을 이용한 영상 모델 압축표준과 머신러닝 기반 비디오 부호화 등의 표준을 개발 중
		SC35	(User interfaces) 인공지능 기술기반의 동시통역과 감성 컴퓨팅 표준 등 ICT 환경에서 사용자 시스템 인터페이스 분야의 표준을 개발 중
		SC42	(Artificial intelligence) 인공지능/머신러닝 데이터 품질, 인공지능 신뢰성, 인공지능 시스템 테스팅·품질 평가 등의 표준화 진행 중
		SC43	(Brain-computer interfaces) 뇌-컴퓨팅 연결을 위한 인터페이스 표준으로 뇌와 컴퓨터 사이의 교류와 통신 관련 아이템 개발 예정
	ETSI	ENI	(Experiential Networked Intelligence) 상황인지 기반 망 관리 구조정의 및 인공지능 기반 미래 네트워크 운용·관리 표준화 진행 중
		SAI	(Securing Artificial Intelligence) 인공지능 활용을 위한 보안 아이템으로 인공지능을 활용한 보안, AI 보호, AI 공격 대응에 관한 표준화 진행 중
사실	IEEE		(Institute of Electrical and Electronics Engineers) 의료, 교육, 자율주행차량, 지능형 제조, 로봇 등의 분야에서 인공지능과 관련된 기술표준을 개발 중
	MPAI		(Moving Picture, Audio and Data Coding by Artificial Intelligence) 인공지능 프레임워크 표준 기반 비디오 코딩, 오디오 향상 표준 등 인공지능 기반 및 응용표준을 개발 중
	Khronos Group		인공신경망 호환 포맷(NNEF)을 표준화하기 위해 개방형 API 표준을 개발 중
	W3C	WebML	(Web Machine Learning) 웹브라우저에서 효율적인 머신러닝 추론을 위한 모델 로더, 가속화 로더 API 표준 개발 중

출처: ICT 표준화 로드맵 Ver 2023

요 문서는 다음과 같다.

- ITU-T Y.3172: 통신망에 인공지능 기술을 적용하기 위한 아키텍처 프레임워크
- Y.Sup55, ITU-T Y.3170-series: 통신망에 인공지능 기술을 적용한 유즈케이스
- ITU-T Y.3173: 통신망의 지능화 수준을 평가하기 위한 프레임워크
- ITU-T Y.3174: 통신망에 인공지능 기술을 적용하기 위한 데이터 처리 프레임워크

요약하면 통신망에 인공지능 기술을 적용할 때 참조할 수 있도록 아키텍처 및 데이터 처리 프레임워크에 관한 권고안이 제시되었고. 네트워크 지능화 수준과 등급을 평가할 때 참고할 수 있는 프레임워크도 게재되었다.

3.2 국내 표준화 그룹: PG1005

2019년 TTA 산하에 조직되어 인공지능 기반 기술 및 인공지능 데이터 관련 국내 표준 개발을 담당하고 있는 PG1005는 2019년 활동을 시작하여 지능형 질의응답 시스템을 위한 개체 연결 표준, 설명가능 인공지능 기술과 유즈케이스, 인공지능 학습용 데이터 참조 기준 등 인공지능 기반기술 및 데이터 분야 표준화 작업을 수행 중이다. 개발한 주요 표준 문건은 다음과 같다.

- 지능형 질의응답 시스템을 위한 메타데이터
- 지능형 질의응답 서비스 프레임워크
- 자율주행 자동차의 객체 인식 기술에 필요한 도로상 데이터의 객체 분류 체계
- 기계학습 기반 구매패턴 분석을 위한 전자상거래 데이터 구성요소
- 유방암 판독 인공지능 모델 개발을 위한 유방촬영술 의료지식베이스 구축방안
- 경량 지능형 소프트웨어 프레임워크
- 서비스형 기계학습 기능 요구사항
- 지도학습을 위한 데이터 품질 관리 요구사항
- 모의 환경 기반 인공지능 게임 에이전트 생성 요구사항
- 지능형 질의응답 시스템 평가 체계
- 지능형 질의응답 시스템을 위한 개체 연결 방법

2023년 현재, 한국어 음성 및 텍스트 데이터, 데이터 품질 평가 지침, AI 신뢰성 확보 가이드라인, 자율주행 AI 학습용 데이터 관리 등에 관한 표준화를 추진 중이다.

4. 시험 및 인증 기준 수립 방향

인공지능 기술 발전이 초기 단계임을 감안하면 인공지능 알고리즘이나 시스템의 성능과 안정성을 시험하고 인증하기 위한 명확한 기준을 제시하기에는 한계가 있다. 인공지능 플랫폼의 안전을 보장함으로써 인공지능 기술과 응용에 대한 신뢰를 구축하는 것이 점점 중요해질 것이므로 표준화된 시험 및 인증 기준 마련이 시급하다. 그러나 현재는 인공지능의 수준과 등급을 분류하기 위한 기준 정도가 제시되고 있으며, 그 외 세부 분야별 연구와 논의가 주로 진행되는 상황이다.

이 절에서는 인공지능 기술의 세부 주제별로 구체적인 시험·인증 기준을 마련하기 위해 진행 중인 논의를 바탕으로 대표적인 요구 사항을 아래와 같이 간단히 살펴본다.

• 학습 데이터 윤리기준

현재 인공지능 알고리즘 및 시스템에 사용되는 학습 데이터의 윤리적 기준 준수를 위한 시험 및 인증 시스템에 대해 공식화된 정의는 없다. 그러나 인공지능에서 윤리의 중요성이 점차 인식되면서 인공지능 기술의 개발과 보급을 위한 윤리적 지침을 마련하려는 논의는 진행 중이다. 여기에는 인공지능 시스템의 공정성, 책임성 및 투명성에 대한 평가뿐만 아니라 데이터의 책임 있는 수집, 저장 및 사용을 보장하는 조치가 포함될 수 있다. 인공지능 학습 데이터의 윤리적 기준 준수를 위한 시험 및 인증 시스템 개발에는 산업계,

정부 및 학계의 이해 관계자 간 합의가 필요하다.

• 설명 가능 인공지능

설명 가능 인공지능의 평가 기준으로는 인공지능 기반 의사 결정 프로세스의 설명 가능성, 제공된 설명의 정확성 및 일관성, 인공지능 시스템의 견고성과 신뢰성에 대한 평가 등이 있다. 또한 투명성, 책임 및 공정성에 대한 요구 사항도 추가될 수 있다. 시험 및 인증 시스템은 해당 분야의 진화 내용을 지속적으로 반영할 수 있어야 한다.

• 인공지능 탑재 시스템

인공지능 기반 시스템에 대한 시험 및 인증 시스템에 대한 보편적 기준은 마련되지 않은 상태이다. 그러나 인공지능 기반 시스템의 시험 및 인증에는 일반적으로 시스템 전체뿐만 아니라 이러한 시스템에 사용되는 인공지능 알고리즘과 모델의 성능, 정확성 및 안전성 평가가 포함될 것이다. 여기에는 학습 데이터의 공정성 및 편향, 다양한 시나리오에서 의도한 대로 작동하는 시스템의 기능, 환경의 예기치 않은 입력 또는 변경에 응답하는 시스템의 기능과 같은 항목에 대한 시험도 포함될 수 있다. 또한 시스템의 보안 및 개인 정보 보호는 물론 관련 규정 및 표준 준수를 인증하는 것도 포함될 필요가 있다.

• 강화학습

보상, 정책 알고리즘 및 모델을 포함하여 강화학습을 위한 객관적인 성능 테스트 지침을 제공하는 것이 중요하다. 이러한 기준에 따라 쉽게 시험을 수행할 수 있도록 표준 기반의 성능 시험 지침을 수립해야 한다. 또한 표준 기반의 성능시험 가이드라인에 따라 시험을 쉽게 수행할 수 있도록 효율적인 시험 환경과 시험 시스템을 구축해야 한다.

• 멀티모달

멀티모달 모델에 대한 성능 시험 및 인증 체계 구축이 필요하다. 멀티모달 모델 기반의 서비스에 대해 성능시험체계를 구축하는 한편, 관련 서비스 전반에도 인증체계를 갖추어야 한다. 인간과 기계의 복합적 상호작용 요구사항에 대한 기준을 수립하고 이를 시험인증 기준에 반영할 필요가 있다.

• 그래프 신경망

그래프 기반 인공지능 모델은 신뢰성과 정확성을 보장하기 위해 성능 테스트가 필요하다. 그래프 모델 구조의 안정성을 보장하기 위해서는 이에 특화된 성능 테스트 및 인증에 대한 표준이 수립되어야 한다.

5. 맺음말

인공지능 표준화 및 시험 인증 기준의 마련에 앞서 현재 진행 중인 인공지능 분야 표준 단체의 활동 현황과 시험 인증 기준과 관련해 논의되는 사항에 대해 살펴보았다. 인공지능 표준화 및 시험 인증 기준은 인공지능 기반 기술 및 응용의 진화와 발전을 효율적으로 지속시키기 위한 핵심 요소이다. 인공지능 기술 개발자들이 보다 안정적인 기술을 개발할 수 있고, 사용자들은 보다 안정적이고 신뢰성 있는 인공지능 시스템을 이용할 수 있도록 인공지능 표준화와 시험 인증 기준의 마련을 조속히 진행해야 하며, 이를 위해 산업계와 정부, 과학기술 단체 등의 긴밀한 협업이 필요하다.

참고문헌

[1] TTA, ICT 표준화 로드맵 인공지능 Ver.2023, 2022.10.

[2] TTA, ICT 표준화 전략맵 지능형 네트워크 Ver.2023, 2022.10

[3] 신성필, 이강찬, 인공지능 기술 국제 표준화 동향 분석, 정보와 통신 Vol38, No.05, pp.0011~0017, 2021

[4] 조영임, 인공지능(Artificial Intelligence) 이슈와 국제 표준화 동향, 소프트웨어 정책연구소, 20201

[5] ITU-T SG13, https://www.itu.int/en/ITU-T/studygroups/2017-2020/13/Pages/default.aspx

[6] 정보통신표준화위원회 지능정보기반 기술위원회 인공지능기반기술 프로젝트그룹 (PG1005), https://committee.tta.or.kr/standard/general.jsp?commit_code=PG1005