

Movements in AI Standardization and Rule Making and NEC Initiatives

TABE Takashi, MOTONAGA Kazuhiro, SHIMAMURA Toshiya, NAGANUMA Miho, ORTOLAN Francois, FROST Lindsay

Abstract

NEC has participated in efforts to develop standard specifications through organizations like the Institute of Electrical and Electronics Engineers (IEEE), the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), and European Telecommunications Standards Institute (ETSI) for not only the development of AI technologies but also for the social implementation of them. With the advent of generative AI, countries are moving toward stricter regulations regarding AI, and standards related to AI governance are needed. This paper describes policies in Europe, the United States, and Japan; trends in multilateral frameworks such as the G7 Hiroshima AI Process; as well as trends in the development of guidelines and the standardization in line with them. This paper also presents NEC's relevant initiatives.

Keywords



generative AI, AI governance, international standardization, conformity assessment, third party certification, European AI Act, EU AI Act, NIST AI RMF

1. Introduction

With the advent of generative AI, the potential and possibilities of AI have become widely recognized. In the meantime, in addition to existing AI risks such as privacy infringement and discrimination, concerns are increasing about new AI risks such as hallucinations and intellectual property infringement, thereby creating challenges. For example, generative AI has the capability to create new content based on user data, raising issues regarding the respect and protection of personal privacy and intellectual property. It is also necessary to appropriately determine the authenticity of any content generated by AI as well as the appropriate use and transparency of such content.

In response to this, the central governments of various countries are steering toward tighter regulations regarding the governance of AI. They are currently in the stage of putting governance principles and policies into practice, and discussions are progressing in a variety of frameworks.

While a consensus is forming socially and internationally, this paper presents a couple of frameworks for AI

governance and standardization trends and explains NEC's relevant initiatives.

2. Formation of Social Rules on AI Governance

When AI is used for predictions, judgments, and recognition—what humans usually do, issues on transparency, fairness, privacy infringements, security, accountability, etc. may be raised. In addition, with the advent of generative AI and foundation models, other issues such as infringement of intellectual property (copyright etc.), hallucinations (generation of incorrect information), and securing of reliability through value chains have come into new focus.

To safely and securely use AI in society, AI governance to appropriately address these issues is required. Social rules for this purpose are being created in various countries and regions, and each might take different approaches to regulating advanced technologies.

2.1 European AI act

The draft of the European AI Act (EU AI Act), which

was announced in April 2021, is the world's first comprehensive AI regulation in the development of global rules and has drawn attention because of its magnitude of influence on regions outside the European Union (EU), in other words, a Brussels Effect. The EU AI Act is mainly composed of requirements and obligations for providers of high-risk AI systems, and these high-risk AI systems also include some biometric systems.

Through the EU legislative process, it was agreed in December 2023 to include new obligations for foundation model providers and requirements for generative AI. In addition, the European AI Office will be established to oversee governance and create standards for evaluating AI capability. Final agreement on laws is expected in the summer of 2024. Section 3 will detail harmonised standards to be established in association with laws.

2.2 Movements in the USA

While the United States has some of the largest AI companies and has traditionally respected private self-governance, it is also considering the need for regulations. In January 2023, the U.S. National Institute of Standards and Technology (NIST) announced the AI Risk Management Framework (AI RMF) as a document for the risk management of AI technology. Subsequently, the White House clarified guidelines for the use of AI for federal procurement and national defense in the Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (October 2023). Meanwhile, discussions are progressing in Congress about comprehensive AI legislation and stronger regulations, and consideration of the need to introduce federal legislation regarding AI and to establish a regulatory body is progressing while talking with leading AI

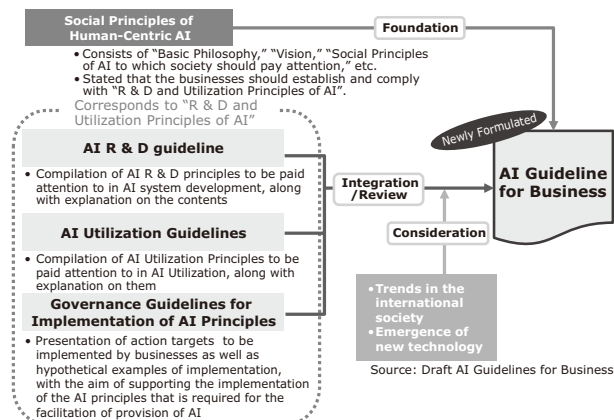


Fig. 1 Outline of initiatives in Japan.

Table 1 International and multilateral frameworks: 11 sets of guiding principles and code of conduct from the G7 Hiroshima AI Process.

Guiding principles	Code of conduct
1. Ensure risk mitigation throughout AI development	Apply thorough measures during AI development, including diverse internal and external testing methods and risk mitigation strategies. Assess potential risks, maintain traceability, support documentation, and promote research in AI safety and security.
2. Identify and mitigate post-deployment AI vulnerabilities and misuse.	Post-deployment, organizations should monitor and mitigate AI system vulnerabilities and misuse, encourage third-party reporting, maintain documentation and ensure accessible vulnerability reporting mechanisms for diverse stakeholders.
3. Report advanced AI systems' capabilities for accountability	Encourage public transparency reports on new advanced AI systems, detailing evaluations, capacity, limitations, effects on society, and addressing risks like bias and discrimination. Documentation should be clear and updated.
4. Promote incident reporting and information sharing among AI stakeholders.	Promote responsible information sharing among AI stakeholders, including evaluations and security risks, establish shared safety standards, and maintain transparency.
5. Implement and disclose risk-based AI policies	Organizations should establish accountable mechanisms to develop, disclose, and implement risk-based AI governance, including privacy policies, and update them regularly across the AI lifecycle.
6. Implement robust security controls for AI	Implement security safeguards for AI, including physical, cybersecurity, and insider threats. This includes securing data, assessing risks, implementing cybersecurity policies, and maintaining high-standard security measures.
7. Develop reliable content authentication for AI	Where feasible, implement content authentication and provenance mechanisms like watermarking for AI-generated content. Also consider labeling and disclaimers for user-interaction transparency.
8. Prioritize research and investment in AI risk mitigation	Organizations should invest in research focusing on AI safety, security, trust, and key risks mitigation, respect human rights, protect privacy, and confront misinformation. Sharing of best practices is encouraged.
9. Prioritize AI development for global challenges	Prioritize responsible AI development for tackling global challenges like climate crisis and health and education issues. Promote digital literacy, understand technology impact, and innovate solutions.
10. Advance development and adoption of AI standards	Encourage organizations to contribute to and use international technical standards for AI, including watermarking, cybersecurity policies, and public reporting for user benefit.
11. Implement data protection for AI systems	Encourage organizations to safeguard data quality, manage harmful biases, preserve privacy, respect intellectual property and comply with legal copyrights in AI systems.

companies. Discussion points for the introduction of regulations include defense, cybersecurity, worker protection, impact on the electoral system, and risk of human extinction resulting from high-performance AI.

2.3 Initiatives in Japan

Initiatives to regulate AI in Japan have not been based on legal regulations, or so-called hard laws, but rather based on soft laws such as guidelines¹⁾. The Cabinet Office announced the "Social Principles of Human-Centric AI"

(2019), and the Ministry of Internal Affairs and Communications, the Ministry of Economy, Trade and Industry, and other organizations proceeded with the development of multiple AI guidelines. These guidelines will be integrated into the "AI Guidelines for Business" in 2024 while maintaining consistency with the multilateral framework through the G7 Hiroshima AI Process (**Fig. 1**). As trends surrounding AI are changing rapidly, regular updates are expected. The internal governance that NEC implements is also based on these guidelines.

Additionally, the formulation of conformity assessment and certification structures as well as individual rules for eight high-risk sectors (government, finance, energy, transportation, traffic, telecommunications, broadcasting, and medical) are also being considered.

2.4 Multilateral framework

Issues posed by AI are widely recognized and shared, and internationally consistent rules on AI are required.

At the G7 Hiroshima Summit held in May 2023, the importance of interoperable AI governance was agreed. In particular, 11 sets of international guiding principles and corresponding code of conduct targeting AI system developers were established (**Table 1**) at the G7 Hiroshima AI Process, a framework to address risks posed by generative AI such as issues regarding intellectual property and fake information. An agreement on a comprehensive policy framework was also reached at the end of 2023. As such, Japan is leading international discussions.

3. Movements toward AI Governance-Related Standardization

As it is believed that interoperable rules for AI governance are required and those rules may include technical details, standardization is expected to play an important role. This section will provide an overview of the movements toward standardization by European standardization bodies and international standards.

3.1 Development of harmonised standards for EU AI Act

The AI Act of the Parliament of the European Union (EUP) will be published within the format of the new legislative framework (NLF), which is composed of laws referencing harmonised standards, certifications, audits, and market surveys. Suitable technical standards—mainly developed by the European Standards Organizations (ETSI (European Telecommunications Standards Institute), CEN (Comite Europeen de Normalisation), and CENELEC (European Committee for Electrotechnical

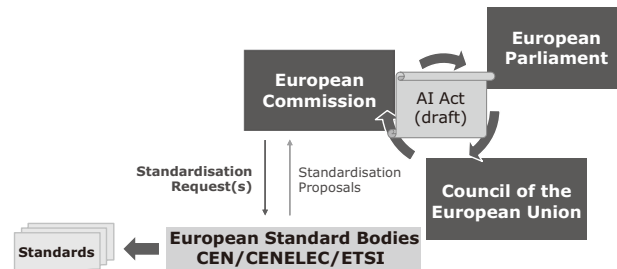


Fig. 2 Development of Harmonised Standards in Europe.

Table 2 Horizontal AI regulatory requirements.

Reference information	
1	European standard(s) and/or European standardisation deliverable(s) on risk management systems for AI systems
2	European standard(s) and/or European standardisation deliverable(s) on governance and quality of datasets used to build AI systems
3	European standard(s) and/or European standardisation deliverable(s) on record keeping through logging capabilities by AI systems
4	European standard(s) and/or European standardisation deliverable(s) on transparency and information provisions for users of AI systems
5	European standard(s) and/or European standardisation deliverable(s) on human oversight of AI systems
6	European standard(s) and/or European standardisation deliverable(s) on accuracy specification for AI systems
7	European standard(s) and/or European standardisation deliverable(s) on robustness specifications for AI systems
8	European standard(s) and/or European standardisation deliverable(s) on cybersecurity specifications for AI systems
9	European standard(s) and/or European standardisation deliverable(s) on quality management systems for providers for AI systems, including post-market monitoring processes
10	European standard(s) and/or European standardisation deliverable(s) on conformity assessment for AI systems

Standardization))—that are recognized in the EU Official Journal as European Norms (EN) and Harmonised Standards [*sic.*] can be cited by manufacturers as part of their pre-market testing and enable products to be marketed as conforming to the requirements of the AI ACT. Thus, the specifications become effective in combination with the legislation (**Fig. 2**).

The European Commission (EC) issued the Standardisation Request on Artificial Intelligence (M/593), demanding development of standards related to the 10 horizontal AI regulatory requirements (**Table 2**).

These include standard specifications for risk management systems to avoid and minimize risks posed by AI, data governance and quality, cyber security, quality management systems, and conformity assessment.

In response, CEN/CENELEC JTC21 first created an architecture of standards to clarify the inherent structure of the 10 standardization items and conducted a gap

analysis to identify the standards needed while considering the utilization of existing standards. ETSI will also cooperate with the standard development process in accordance with the Joint Work Programme created by JTC21. NEC has been working on the necessity of AI standards in the fields of communication and cybersecurity for many years through initiatives such as participating as an ETSI Board member and leading the AI coordination committee.

The deadline for standardization is May 22, 2025. Because many of the necessary standards are not available, and the workload for standardization is substantial, a large number of international standards, such as ISO/IEC standards, are expected to be transposed with minimal change into European Harmonised standard. Besides, a second standardisation request [sic.] from European Commission is expected to cover additional regulation on large language models (LLM), general-purpose AI systems (GPAI), and foundation models (FM). As it is difficult to provide all standards before the AI Act is put in force, a phased release of standard specifications is also being considered, beginning with risk assessment. Additionally, alignment with sectoral legislation, such as in the medical field, is also required.

3.2 Movements in international standardization

Subcommittee 42 (SC42) Artificial Intelligence established under ISO/IEC JTC1 is actively working on international standardization, and standardization for AI governance is leading the way. These initiatives, which were launched earlier than regional standardization efforts such as those in Europe, are drawing attention.

For example, working groups (WG) developed reliability standards, such as the data quality standards developed by WG2 and the AI system quality and test method standards (TS29119-11) by WG3 and JWG2. In addition, JWG4 in collaboration with the IEC TC65 SC65A subcommittee has developed standards for AI safety requirements that are based on Japan's proposed TR5469, which is responsible for standardizing the functionality security of control equipment.

Japan has been actively involved in international standardization since the establishment of SC42 Artificial Intelligence, with the National Institute of Advanced Industrial Science and Technology (AIST) playing a central role. NEC was also active in the SC42 committee as well as its domestic expert committees and contributed by serving as the domestic chief reviewer of WG3 and WG5 and as the AI safety project editor.

In the United States, the utilization of international standards and the participation of experts are required

to effectively address AI risks. As indicated earlier, the EU AI Act indicates that international standards will be adopted. For example, ISO/IEC 42001 is the AI Management System Standard (AI MSS) for managing AI systems and serves as the basis for conformity assessment, which has been identified as necessary in various frameworks. In addition, consideration of a third-party certification system has already begun.

4. NEC's Initiatives

NEC is working not only on technology development but also on the standardization and creation of legal systems and rules. As part of NEC's initiatives related to AI governance, NEC led the U.S. AI ethics project (P7001) at the Institute of Electrical and Electronics Engineers (IEEE) and submitted comments during the development process of NIST's AI risk management framework.

In Europe, NEC utilizes its position at ETSI to work on advocacy activities regarding standardization, which are referred to in the European AI White Paper and in the EU AI Act. In Japan, NEC's experts have participated in and contributed to the development of a variety of public guidelines. NEC also works to create draft Japanese Industry Standards (JIS) based on international standards. In addition, NEC participates in the creation of AIST's "Machine Learning Quality Management Guidelines," which is a systematic and comprehensive framework for quality requirements, as part of AI quality management (AIQM). It also participates in UN and EU events and are focusing on global awareness activities.

5. Conclusion

NEC possesses advanced underlying technologies such as generative AI, biometric authentication, and cybersecurity measures and is working to solve social issues by combining these technologies. For this reason, NEC has also been actively working on global standardization activities. Standardization, which forms the basis of interoperable social rules, plays a key role in effectively controlling AI risks and forming global markets. For society to utilize AI safely and securely, it is essential to develop governance mechanisms and technologies.

References

- 1) Tagui Ichikawa, Institute of Innovation Research Hitotsubashi University: Evolutionary Mechanism of AI Governance in the World-institutional innovation caused by regional diversity as a part of co-evolution of technology and institution (Japanese).
<https://hermes-ir.lib.hit-u.ac.jp/hermes/ir/re/79802/070iirWP23-01.pdf>

Authors' Profiles

TABE Takashi

Senior Professional
Global Innovation Strategy Department

MOTONAGA Kazuhiro

Director
Global Innovation Strategy Department

SHIMAMURA Toshiya

General Manager
Digital Trust Business Strategy Department

NAGANUMA Miho

Senior Executive Professional
Digital Trust Business Strategy Department

ORTOLAN Francois

Senior Standardisation Engineer
NEC Laboratories Europe

FROST Lindsay

NEC Laboratories Europe

The details about this paper can be seen at the following.

Related URL:

European Commission: Proposal for a Regulation laying down harmonised rules on artificial intelligence.

<https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence>

European Commission: Standardisation Request M/593 on Artificial Intelligence.

[https://ec.europa.eu/transparency/documents-register/detail?ref=C\(2023\)3215&lang=e](https://ec.europa.eu/transparency/documents-register/detail?ref=C(2023)3215&lang=e)

The Cabinet Office of Japan: The AI Strategy Council (Japanese).

https://www8.cao.go.jp/cstp/ai/ai_senryaku/ai_senryaku.html

Information about the NEC Technical Journal

Thank you for reading the paper.

If you are interested in the NEC Technical Journal, you can also read other papers on our website.

Link to NEC Technical Journal website

Japanese

English

Vol.17 No.2 Special Issue on Revolutionizing Business Practices with Generative AI

– Advancing the Societal Adoption of AI with the Support of Generative AI Technologies

Remarks for Special Issue on Revolutionizing Business Practices with Generative AI
Approaches to Generative AI Technology: From Foundational Technologies to Application Development and Guideline Creation

Papers for Special Issue

Market Application of Rapidly Spreading Generative AI

NEC Innovation Day 2023: NEC's Generative AI Initiatives
Streamlining Doctors' Work by Assisting with Medical Recording and Documentation
Using Video Recognition AI x LLM to Automate the Creation of Reports
Understanding of Behaviors in Real World through Video Analysis and Generative AI
Automated Generation of Cyber Threat Intelligence
NEC Generative AI Service (NGS) Promoting Internal Use of Generative AI
Utilization of Generative AI for Software and System Development
LLMs and MI Bring Innovation to Material Development Platforms
Disaster Damage Assessment Using LLMs and Image Analysis

Fundamental Technologies that Enhance the Potential of Generative AI

NEC's LLM with Superior Japanese Language Proficiency
NEC's AI Supercomputer: One of the Largest in Japan to Support Generative AI
Towards Safer Large Language Models (LLMs)
Federated Learning Technology that Enables Collaboration While Keeping Data Confidential and its Applicability to LLMs
Large Language Models (LLMs) Enable Few-Shot Clustering
Knowledge-enhanced Prompt Learning for Open-domain Commonsense Reasoning
Foundational Vision-LLM for AI Linkage and Orchestration
Optimizing LLM API usage costs with novel query-aware reduction of relevant enterprise data

For AI Technology to Penetrate Society

Movements in AI Standardization and Rule Making and NEC Initiatives
NEC's Initiatives on AI Governance toward Respecting Human Rights
Case Study of Human Resources Development for AI Risk Management Using RCModel

NEC Information

2023 C&C Prize Ceremony



Vol.17 No.2

June 2024

Special Issue TOP