Japanese Policy on AI

June 2024

Shoji Watanabe
Cabinet Office, Japan

Japanese Policy

Compiled from materials by the Cabinet Office

Previous Basic Strategies “AI Strategy 2022”, “Principles for a Human-Centered AI Society”

Changes in technologies such as generative AI

Natural dialogue is possible, elaborate image generation is easy, etc.

! Great benefits and innovation, contribution to Society 5.0

! On the other hand, risks related to AI are more imminent

International Discussions

Common vision and goals agreed at G7 Hiroshima Summit 2023 is "Trustworthy AI”.

G7 leaders agreed on the comprehensive policy framework including international guiding principles. (Hiroshima AI Process)

AI Strategy Council (experts) , AI Strategy Team, AI International Strategy Promotion Team (relevant ministries)

Tentative Discussion Points on AI" (May 26, 2023, compiled by AI Strategy Council)

Basic Approach

(1) Leading role in international rule making, (2) Response to the risk and use of AI,
(3) Prompt and flexible response involving diverse stakeholders

Response to Risks

- Responding to concerns and risks related to generated AI
  - Handling at central ministries (Digital Agency), reminders from the Personal Information Protection Commission (PPC), guidelines for educational institutions (MEXT), discussions on AI and copyright (MEXT), and study on AI and intellectual property (Secretariat for Intellectual Property Strategy Promotion)
  - Guidelines by MOC & METI, consideration on necessary action (Cabinet Office), AI Safety Institute
  - R&D on countermeasure technology, etc.

Optimal use of AI

- Data connection infrastructure, etc. (DA, etc.)
- Pilot use in government (DA, etc.)
- Skills and literacy education for a wide range of generations (MIC, MEXT)

Strengthening AI R&D capabilities

- Securing computational resources (METI), developing training data (MIC), support for model development (METI), fundamental research (MEXT)
- Environment attracting talent (MEXT)
- Promotion of startup (METI, MEXT, etc.)

Cooperation among ministries collaborating with AI Strategy Council, AI Strategy Team, and AI International Strategy Promotion Team

AI-related budget

Compiled from materials by the Cabinet Office

Budget for FY2024 is about 0.8 billion dollar.
Supplemental budget (FY2023-2024) is about 2.1 billion dollars.

Responding to Risk

4.5 million dollars [6.6 million dollar]

- Contribution to G7, Hiroshima AI Process, OECD, GPAI…
- Research on countermeasures against disinformation
- Literacy education

Promotion of AI Use

0.23 billion dollar [0.42 billion dollar]

- Deployment in critical fields such as healthcare, infrastructure, education, and government, etc.
- Support for introduction of AI by small and medium-sized enterprises
- Support for human resource development (reskilling, AI literacy)

Strengthening AI development capabilities

0.25 billion dollar [1.6 billion dollar]

- Securing computational resources
- Expansion of data centers
- R&D on energy effective GPU
- Improvement of training data
- Supporting AI model development
- Enhancement of basic research
- Attractive R&D environment for researchers

- In addition to the above, a portion of the grants to each national R&D agency will be used for AI research and development.

Notation :
amount of draft budget for FY2024 [amount of supplemental budget]

Further Discussion (Requirement for AI Actors)

Image

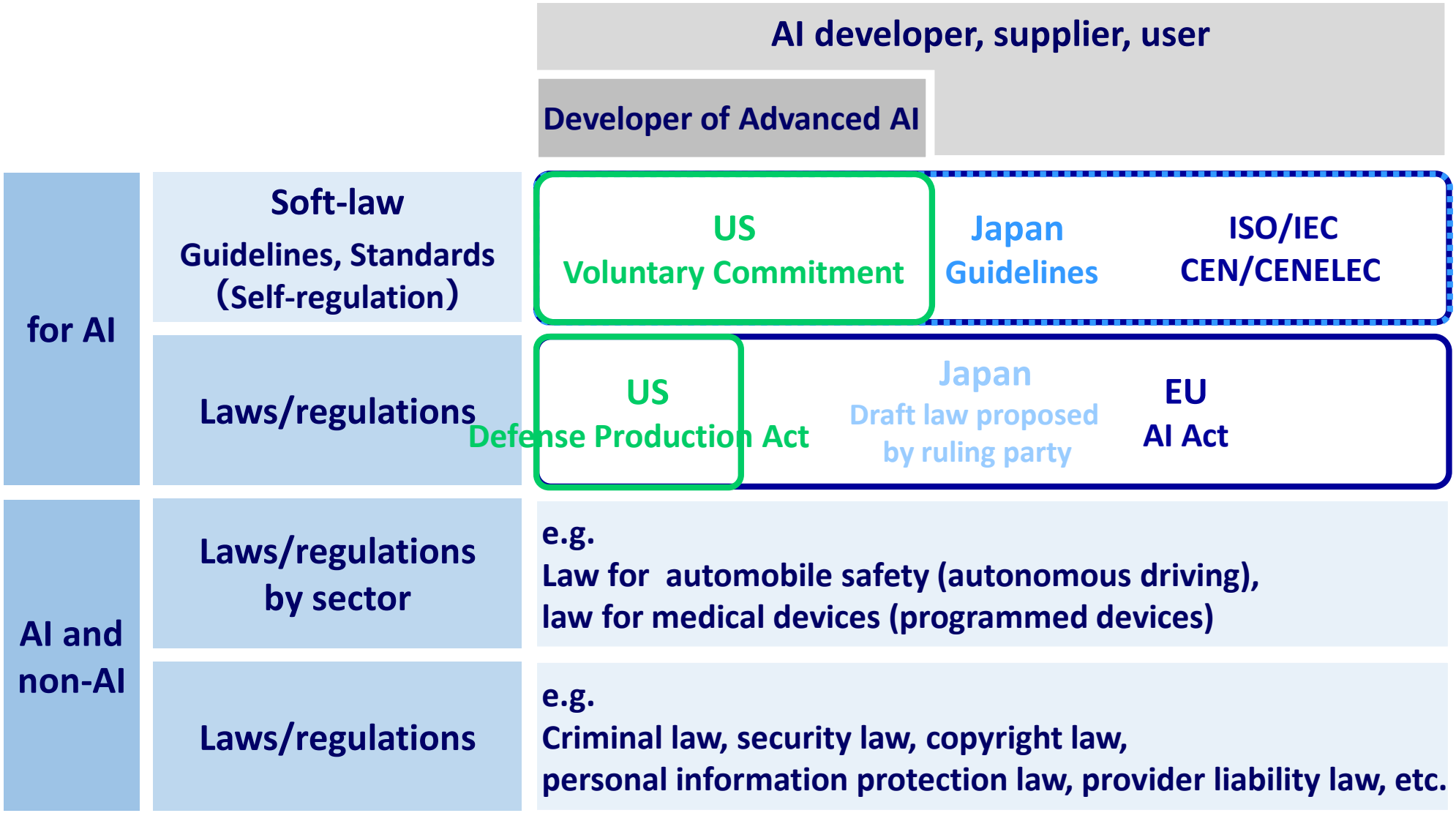
Japan is basically using guidelines (soft-law), which are flexible and useful for rapidly changing technologies.

EU and US are considering to use both soft-law (guideline, standard) and hard-law (law, regulation).

	High risk, influential	Low risk, non-influential
AI developer	**Reliable response to the risks** U.S. Reporting obligation by AI developers of large-scale dual use models EU Law and regulations Third party certification	**Response to the risks** Disclosure of compliance with rules, etc.
AI supplier, user	**Compliance with specific industry regulations, etc.** High-risk equipment, machinery, etc.	**Response to the risks** Development and publication of AI governance policy, etc.
	Procurement and use of appropriate AI by the government **Survey and information sharing on risks**	
Online Platformer	**Response to inappropriate contents** i.e. Digital Service Act (EU)	

Structure of Rule

Image



G7 Leaders' Statement on Hiroshima AI Process (December 2023)

Ⅰ Hiroshima AI Process Comprehensive Policy Framework

(1) OECD's Report towards a G7 Common Understanding on Generative AI

(2) Hiroshima Process **International Guiding Principles for All AI actors**

(3) Hiroshima Process **Code of Conduct for Organizations Developing Advanced AI Systems**

(4) Project-based cooperation on AI

Ⅱ Work Plan to advance Hiroshima AI Process

- expand **outreach to partner governments**
- develop proposal to introduce monitoring tools and mechanisms
- launch a dedicated web site for the Hiroshima AI Process
- dialogue with the multi-stakeholder community
- continuously working together under Italian Presidency

Hiroshima Process
International Guiding Principles for All AI actors (items only)

Ⅰ. measures throughout the development of advanced AI systems, including prior to their deployment.

Ⅱ. identify and mitigate vulnerabilities, incidents and patterns of misuse, after deployment.

Ⅲ. publicly report advanced AI systems' capabilities, etc. to ensure transparency.

Ⅳ. information sharing and reporting of incidents.

Ⅴ. develop, implement and disclose AI governance and risk management policies.

Ⅵ. security controls, including physical security, cybersecurity and insider threat safeguards.

Ⅶ. content authentication and provenance mechanisms to enable users to identify AI-generated content.

Ⅷ. research to mitigate societal, safety and security risks and prioritize investment in effective mitigation measures.

Ⅸ. development of advanced AI systems to address the global problems.

Ⅹ. development and adoption of international technical standards.

Ⅺ. appropriate data input measures and protections for personal data & intellectual property.

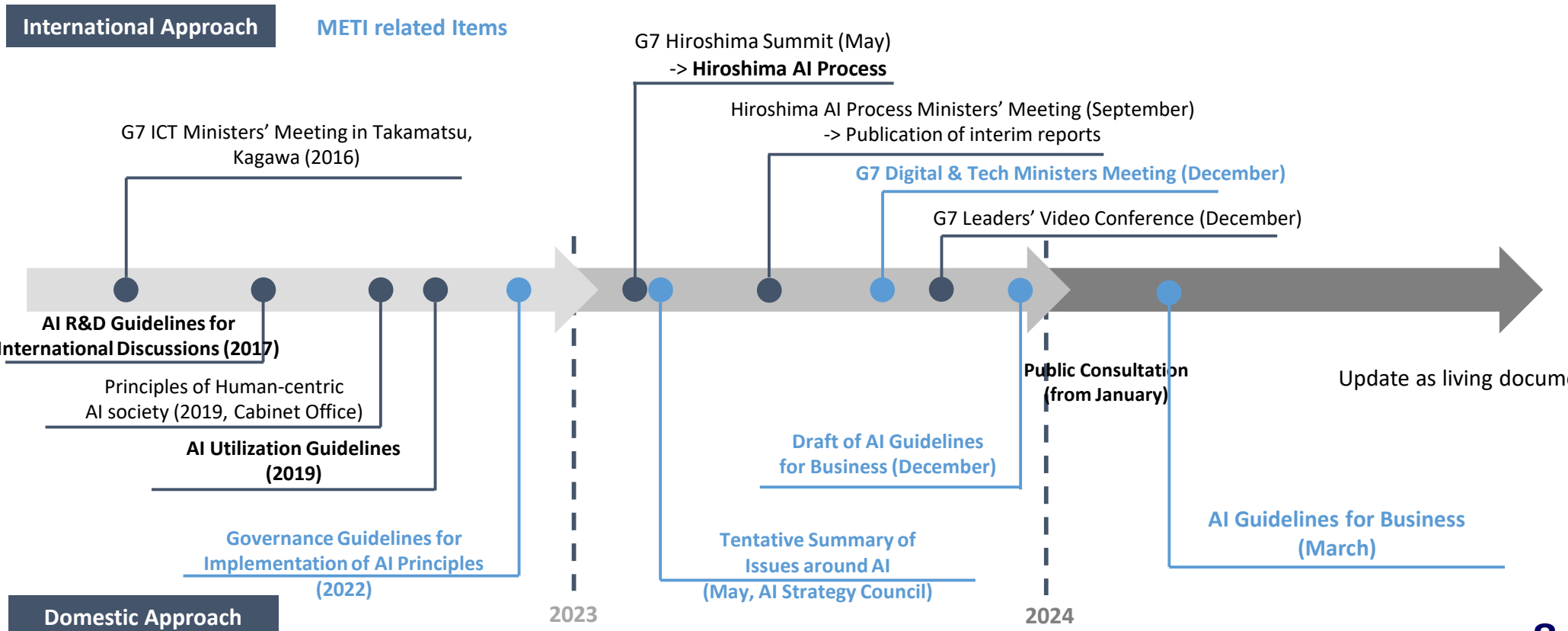
Ⅻ. trustworthy and responsible use of advanced AI systems

Japan's effort in AI governance (Background)

- Initiated AI discussion in the international fora since 2016*. Developed three AI guidelines** since 2017.
- In the international fora: PM Kishida announced to establish '**Hiroshima AI Process**'. MIC leaded discussion to publish deliverables ('**Hiroshima AI Process Comprehensive Policy Framework**')
- On the domestic level: METI and MIC published a draft of '**AI Guidelines for Business**' targeting at all AI-related stakeholders, compiling and updating three existing guidelines.

*G7 ICT Ministers' Meeting in Takamatsu, Kagawa

**AI R&D Guidelines for International Discussions (2017, Ministry of Internal Affairs and Communication), AI Utilization Guidelines (2019, Ministry of Internal Affairs and Communication) and Governance Guidelines for Implementation of AI Principles (2022, Ministry of Economy, Trade and Industry)



Japanese AI Guidelines for Business

Main Body

COMMON TO ALL AI BUSINESS ACTORS

Part 1 **Definitions**

Part 2 **Society to aim for with AI and what each AI business actor works on**

A. Basic philosophy
B. Principles
C. Common guiding principles
D. Guiding principles Common to AI Business actors involved in advanced AI systems
E. Establishing AI governance

SPECIFIC TO EACH AI BUSINESS ACTOR

Part 3 **Matters related to AI Developers**

- Pre-processing of data and training
- During AI development
- After AI development
- **Items for advanced AI developers**

Part 4 **Matters related to AI Providers**

- AI system implementation
- After provision of AI systems and services
- **Items for advanced AI providers**

Part 5 **Matters related to AI Business Users**

- Use of AI systems and services
- **Items for advanced AI business users**

Appendix

As commentary to the concise main body, appendix contains;

- Examples of AI systems and services
- Patterns and examples of AI business actors and their relations
- Practical items to build AI governance within each business actor and their concrete examples
- Explanation about each item of main body, examples of concrete measures and other references
- Check list *Existing efforts by AI related actors are also collected in multi-stakeholder consultation and are described in columns

Excerpt from Appendix

(D-5) i. Introduction of mechanisms for security measures: Throughout the process of developing AI systems, take appropriate security measures in light of the characteristics of the technology to be employed (security by design) ("5) Ensuring Security")

[Points] It is expected to pay attention to the security of AI and take reasonable measures to ensure the confidentiality, integrity, and availability of AI systems, in light of the technical level at that time. In addition, measures to be taken in case of a security breach are expected to be organized in advance, taking into account the purpose and characteristics of the AI in question, and the magnitude of the impact of the breach. Security by design" defined by the Cabinet Cyber Security Center (NISC) in the "Direction to incorporate information security from the planning and design phase" should be considered from the early stage of the development process to ensure the security of the system to be developed. Security is to be secured by considering security from the early stages of the development process. Adding security functions after the fact or implementing security tools just before shipment, as in the past, may cause frequent rework and result in high development costs. Implementing security measures at an early stage of development reduces rework and costs and leads to the creation and provision of systems and software with good maintainability.....

[Concrete measures]

- Security by design
  - Threat Assessment: .....
  - Software Bill of Materials: .....
  - .....

[Other references]

- NCSC, "Guidelines for secure AI system development" (November, 2023)
- NIST, "CYBERSECURITY FRAMEWORK" (April, 2018)
- ISO/IEC27000 Series
- NIST, SP800 Series .....

AI Safety Institute

Japanese AI Safety Institute was established at IPA (Information-technology Promotion Agency) in cooperation with related ministries and national laboratories.

Current tasks **are study on AI safety issue (AI safety evaluation, disinformation, etc.)**, **preparation of standards**, **consideration on evaluation method**, and **international collaboration** with UK and US AISI, etc.

Executive Director
Akiko Murakami

Executive Officer, Chief Digital Officer, Sompo Japan Insurance, Inc.
Former researcher of IBM Japan.

Relevant ministries :

Cabinet Office (Secretariat for Science, Technology and Innovation)
Cabinet Cyber Security Center
Digital Agency
Ministry of Foreign Affairs
Culture, Sports, Science and Technology
Trade and Industry
National Security Bureau
National Police Agency
Ministry of Internal Affairs and Communications
Ministry of Education
Ministry of Economy
Ministry of Defense

Related organizations :

National Institute of Information and Communications Technology (NICT)
RIKEN
National Institute of Informatics
National Institute of Advanced Industrial Science and Technology (AIST)