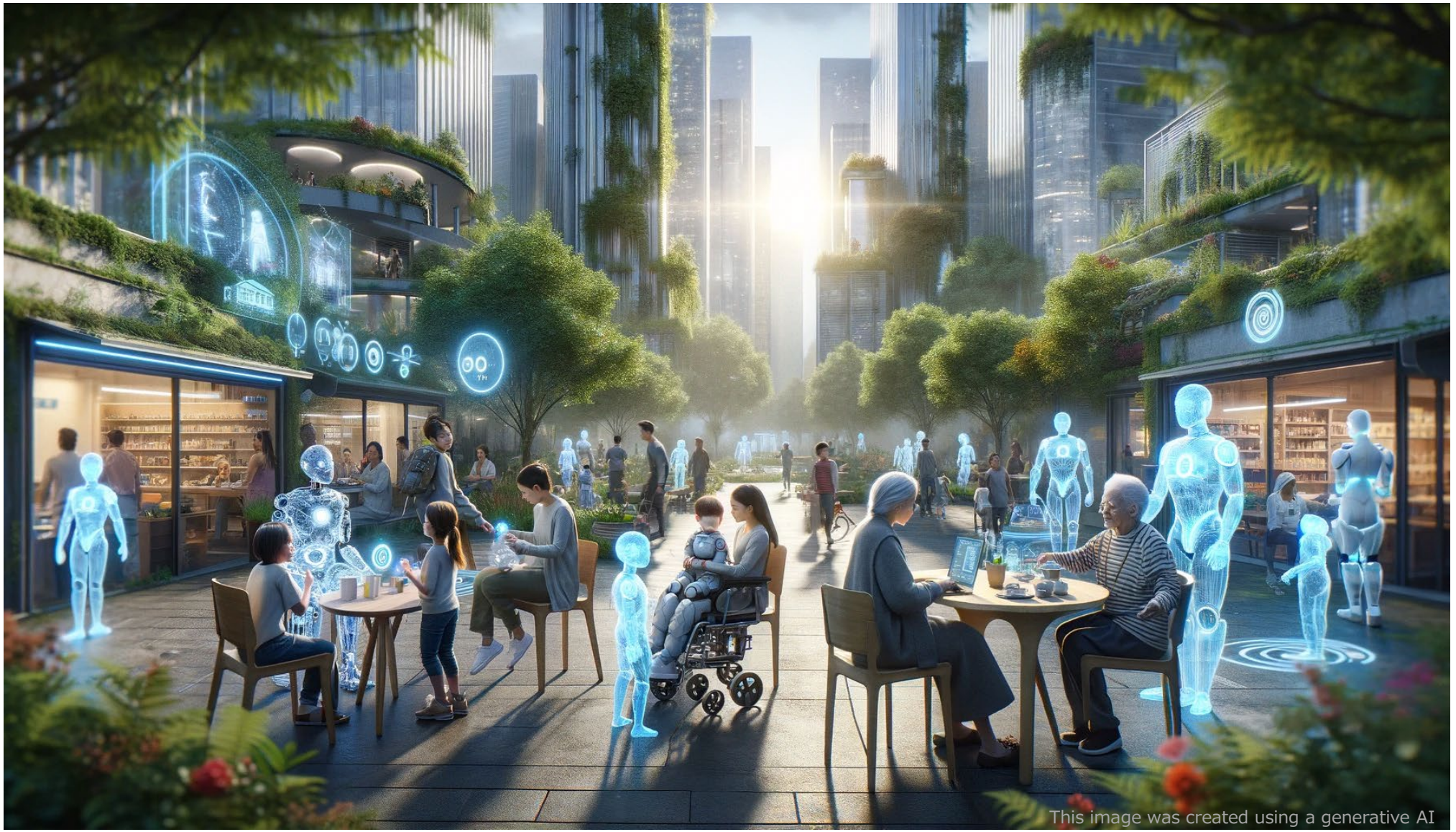
AI White Paper 2024　New Strategies in Stage II

- To the most AI-friendly country in the world -



April 11, 2024

Liberal Democratic Party, Project Team on the Evolution and Implementation of AIs

(Ver.1.0)

Skeleton of AI White Paper 2024

LDP White Paper (2023): It all started. The Big Bang of AI in Japan.

These recommendations have largely been realized or are being implemented.
The world and Japan have progressed at an unprecedented pace over the past year, both in the public and private sectors.

"Stage II": No one can predict specifically and accurately for the year ahead.

New Strategies in Stage II - To the most AI-friendly country in the world

Integrated promotion of competitiveness enhancement and safety assurance

Facilitating R&D and utilization

Strengthening competitiveness

Respond flexibly to take advantage of rapid changes in the environment.

Strengthening competitiveness through integrated R&D and utilization

R&D of new convenience technologies

Strengthening R&D capabilities

Virtuous circles

Promoting AI utilization

Increase in data and AI-related investments

Upgrading the infrastructure of computing resources, etc.

New technology to improve safety

Minimizing Risk
Maximizing Profit

Ensuring safety promotes AI R&D and utilization

Safety and Security

Ensuring safety

A multi-layered approach (soft law and minimum necessary hard law) based on voluntary responses to develop the environment of safe and secure use and promote innovation.

Responding to risks

Literacy improvement, human resource development, copyright and intellectual property, handling of personal information, etc.

International collaboration and coordination, international consistency

AI White Paper 2024 Key Recommendations

Chapter 1 **Japan in Stage II**	**Stage II Strategies - To the most AI-friendly country in the world -**	• To realize the **"world's most AI-friendly country"** with the best understanding of AI and the easiest AI R&D and implementation. • **Maximizing profits while minimizing risks to the public** from AI. • **Promote strengthening competitiveness and safety in an integrated manner.** • Japan **continues to lead international rulemaking** on safe, secure, and reliable AI, based on the **achievements of the Hiroshima AI Process.** • **Strengthen cooperative relationships with Asian countries and the Global South**, and **demonstrate strong leadership in the world in promoting international joint research and utilization of AI**.
Chapter 2 **Strategies for strengthening Japan's competitiveness through the use of AI:** **Flexible responses that take advantage of rapid environment changes**	**Promotion of utilization**	• To promote **further utilization in public administration, new guidelines will be established** based on the handling of confidential information, etc. • **Disseminate "AI Guidelines for Business" widely to promote appropriate use of AI by** each organization, so that business operators can promptly respond to environmental changes on a risk-based basis against AI risks.
	Strengthening R&D capabilities	• **To utilize data for AI development,** establish a plan for providing data held by the Government and others, share examples of the use of private-sector data, and develop new data useful for development. • **Synergistic efforts in the public and private sectors to collect, maintain and update data, and develop and utilize AI**, so that the development and utilization of AI can be firmly promoted **in fields where Japan can make use of its strengths**, such as automobiles, robotics and materials development, and **in fields that are also important for security**, such as medicine, finance and agriculture. • Based on the discussions and recommendations of the LDP, the Government will **compile a support program for AI start-ups.** • In order to dramatically strengthen competitiveness in cutting-edge AI technologies, including AI for Science, the Government will **develop a data infrastructure for national research institutes, etc.**
	Upgrading infrastructure	• The Government will **provide financial and other policy support** to ensure data centers and other infrastructure to become the world's most AI-friendly country and **encourage necessary private investment**. • **Expand and upgrade the "AI Bridging Cloud Infrastructure (ABCI)"** and begin development of the **next generation of "Fugaku"** with AI capabilities.
Chapter 3 **Strategies to ensure safety**	**Appropriate governance**	• **The basis of AI governance in Japan is for operator and others to voluntary and continuously assess and reduce risks based on "AI Guidelines for Business," etc.** • Based on the concept of the "Basic Law for the Promotion of Responsible AI (tentative name)" by the WG volunteers of this PT, etc., the Government will **develop the minimum necessary legal framework for AI models with extremely high risks.**
	Countermeasures against false and misinformation using generative AI	• **Comprehensive measures**, including institutional measures, will be compiled by the end of this summer to deal with **false and misleading information by using generative AI.** • **In order to appropriately respond to negative impacts on elections,** relevant operators will **implement the same efforts as the Munich Accord in Japan.**
	Further efforts to ensure the safe use of AI	• Establish a **high-level network of AISIs in Japan and other countries,** for international coordination to ensure the safety of AI. • AISI will **serve as Japan's nodal point** for AI safety assessment.
	Relationship with copyright and other intellectual property	• **Regarding intellectual property rights such as copyright**, the Government **will respect these rights** while taking measures in line with the AI era and **promoting appropriate AI utilization.**

Overview of computational resources and training data

Overview of computing resources

In Japan, there are problems such as an insufficient number of data centers, a lack of power grids and high construction costs.

Large-scale computing infrastructure

Cloud server

Cloud Service
Data storage, web services, etc.

CPU
Memory
Storage

Supercomputer

Computation
Scientific and technical calculation, simulation, etc.

CPU
Memory
Storage

Deep learning

Training
(AI development)

GPU
Memory (HBM)
Storage

Inference
(AI utilization)

Potential for progress in small-scale decentralization

CPU/GPU
Memory
Storage

An oligopoly by a few companies

Overview of training data

Data that can be used for domain-specific AI training
AI used within the organization that is not disclosed to the public, e.g.

Non-personal data used for AI training
AI that may be released to the public

	Important secret, etc.	Personal data, Organization data, Membership Data, etc.	Website information (documents, images, videos, etc.)	Open bibliographic information (documents, images, videos, books, figures and tables from papers, numbers, biological and material data)	Machine-readable data	All data
Data held by national and public organizations						
Data held by private institutions and individuals		Exp: Diagnostic info. Customer info. Research info. Product info. etc			Digital converted paper media by OCR, etc.	Data that is not suitable for AI training, such as machine-unreadable or not well-formatted

(Source: Compiled from materials of National Institute of Advanced Industrial Science and Technology (AIST).

LDP Project Team on the Evolution and Implementation of AIs
Volunteer WG (February 16, 2024, excerpted document (translated))

Overview of the Basic Law for the Promotion of Responsible AI

Legislative purpose

Purpose of Legislation: To promote the development of an open environment that enables the design, development and introduction of safe, secure and responsible AI and the human-centered use of AI. The law aims to maximize the benefits of the sound development of AI, including innovation by AI, while minimizing the risk of violations of fundamental human rights and other rights and interests of the public through the utilization of generative AI and other AI.

1. Promote the Responsible Use of AI

State: Promote the use of AI among public and private sectors to address social issues.
Measure: Build and strengthen public-private partnerships to promote AI technological innovation

State: Develop and attract human resources in AI sector and strengthen R&D capabilities
Measures: Provide subsidies and grants for AI related R&D

State: Strengthen the capacity of research institutions regarding the safety of advanced AI
Measures: Strengthen the capacity of the Japan AI Safety Institute (AISI) recently established

2. Designation of Advanced AI Foundation Model Developers

State: Designate AI Foundation Model Developers of a certain size/objective as an "Advanced AI Foundation Model Developer"
Issues TBD
- ✓ Justification and necessity to regulate developers of foundation models as a target of the regulation
- ✓ How to evaluate/classify based on "size" and "purpose" (e.g. number of parameters, training data, general purpose or not)
- ✓ Should the designation be made unilaterally or notifications be required beforehand? In the case of designating unilaterally, whether or not the State should be authorized to conduct investigations for the purpose of designation
- ✓ Whether or not to impose penalties against business entities who do not report?
- ✓ Geographical scope of regulation (whether to limit scope to models used for services provided in Japan)

Private sector: If a notification obligation is imposed, the target business entity shall submit a notification.

3. Obligation to Develop Systems by Advanced AI Foundation Model Developers

State: Designated developers shall develop business structures/systems including the following:
- ☐ Conduct internal and external safety verification, such as Red team testing, for AI in particularly high-risk areas.
- ☐ Share risk information among companies and governments
- ☐ Invest in cybersecurity to protect unreleased model weights
- ☐ Incentivize detection and reporting of vulnerabilities by third parties
- ☐ Adopt a mechanism to inform users when generative AI is used for a particular content
- ☐ Publicly report AI capabilities, limitations, etc.
- ☐ Prioritize research on social risks brought about by AI

3. Obligation to develop systems by Advanced AI Foundation Model Developers (continued)

Private sector: Formulate and publicize standards and codes of conduct that embody the aforementioned obligations by each business entity or industry association.
Issues
- ✓ Whether to entrust the private sector with establishing standards for AI quality-assurance, as in the case of the harmonized standards set forth in the EU AI Act?
- ✓ Whether to incorporate discussions with stakeholders in establishing specific codes of conduct (e.g. in EU Digital Services Act, the European Commission invites stakeholders to formulate codes of conduct)
- ✓ Should private organizations establish a new certification system, etc.?

4. Reporting Obligation and Supervision

State: Advanced AI Foundation Model Developers shall regularly report their status of compliance regarding the requirements set forth in Section 3 to the national government or to third parties (e.g., AI Safety Institute)
Issues
- ✓ Whether or not public disclosure of such report should be required

State and private sector: State shall monitor and review specific Advanced AI Foundation Model Developers based on the above status report. State may seek the opinions of relevant parties in the private sector.

State: State shall publish the findings of assessments and, in certain cases, request Advanced AI Foundation Model Developers to implement remedies.

State: State may request reports and conduct on-the-spot inspections in the event that any Advanced AI Foundation Model Developers fail to comply with obligations, or cause an incident.

5. Penalty, etc.

State: Surcharge or penalty for breach of obligation/order

Private sector: Revocation or suspension of certification, etc.