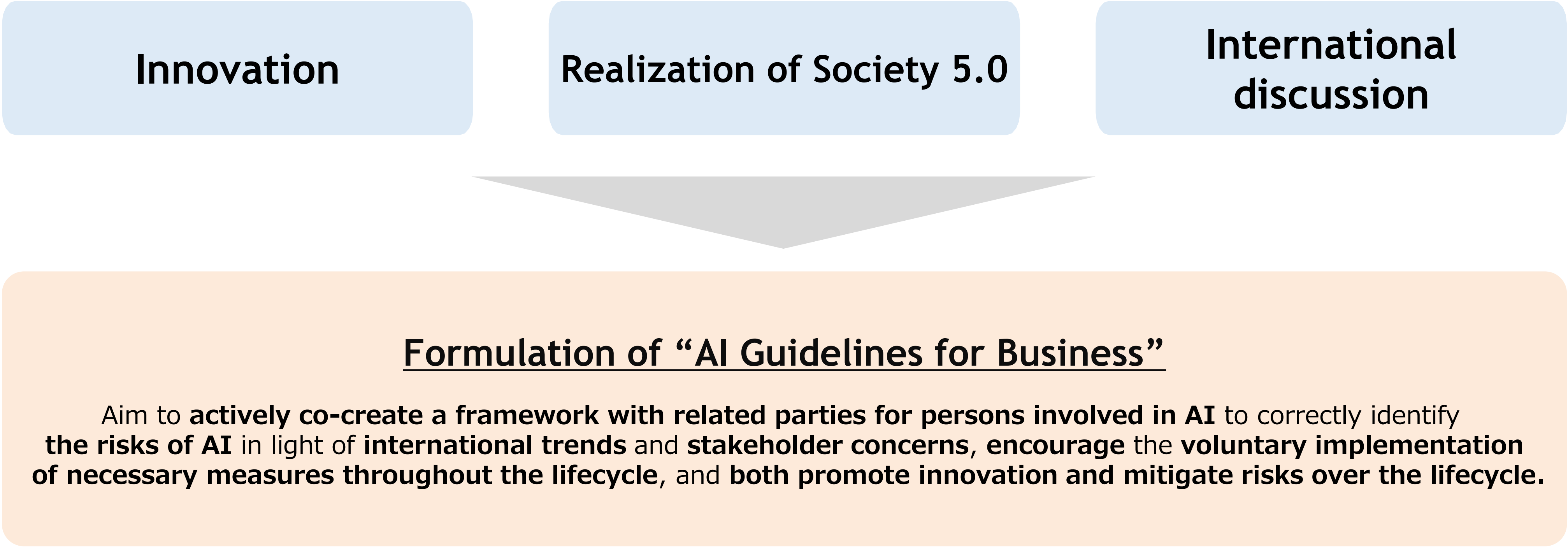
仮訳

Outline of the draft “AI Guidelines for Business”

Ministry of Internal Affairs and Communications
Ministry of Economy, Trade and Industry
(January 2024)

Background and Purpose of Formulating "AI Guidelines for Business"

- AI-related technologies, as represented by generative AI, are developing day by day, and opportunities and possibilities for their use continue to expand, with the aim of creating innovations in industries and resolving social issues.
- In Japan, there are growing expectations of the advanced use of AI for the realization of "Society 5.0".
- Japan has contributed to **international discussions** pioneering with the proposal for AI development principles at G7, and leading discussions at international organizations such as G7, G20, and OECD.
- Given this situation, the aim is to co-create a framework that both promotes innovation and mitigates risks over the lifecycle by providing a unified guiding principle for AI governance in Japan.



Innovation

Realization of Society 5.0

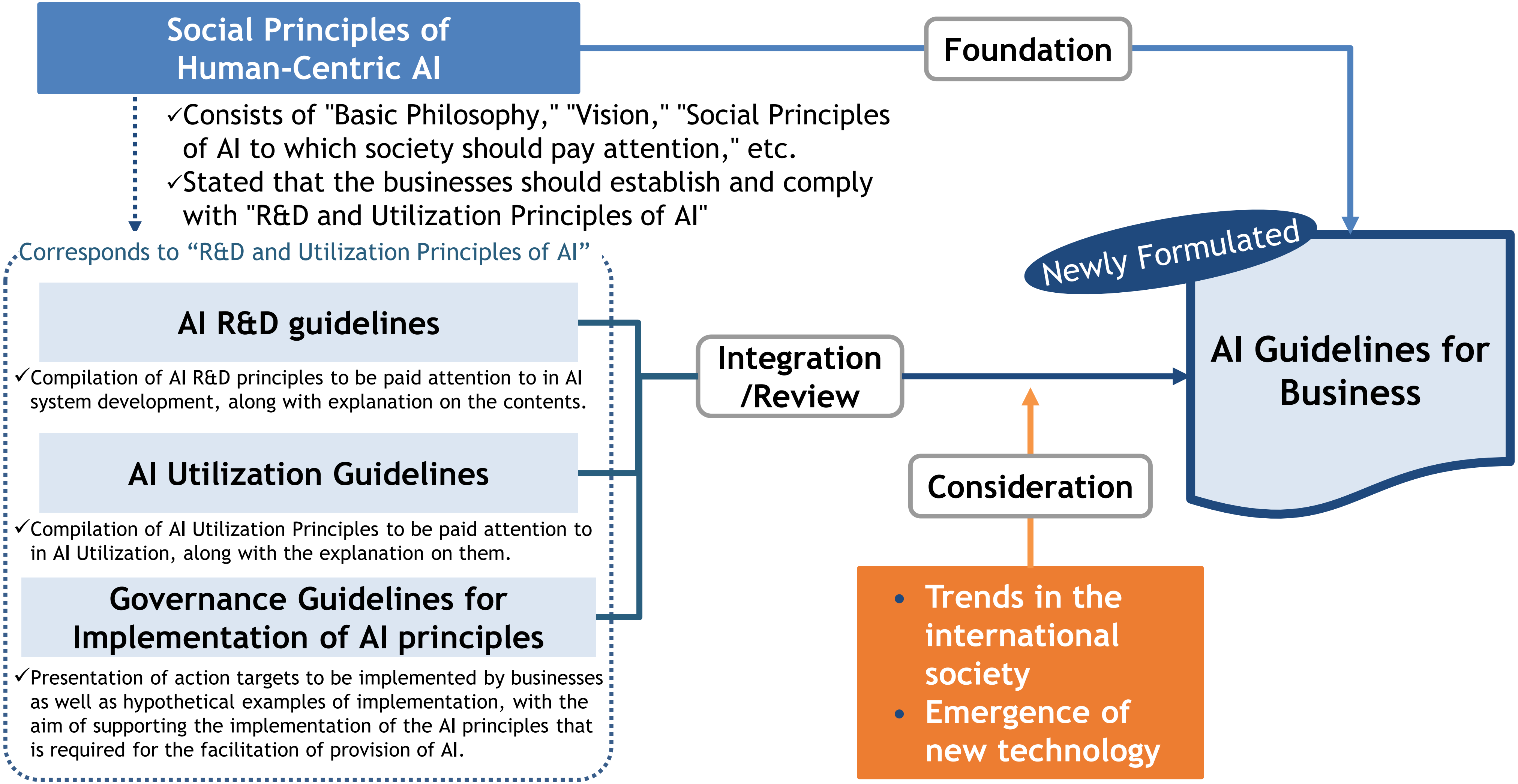
International discussion

Formulation of "AI Guidelines for Business"

Aim to **actively co-create a framework with related parties for persons involved in AI** to correctly identify **the risks of AI** in light of **international trends** and **stakeholder concerns**, **encourage** the **voluntary implementation of necessary measures throughout the lifecycle**, and **both promote innovation and mitigate risks over the lifecycle.**

Policy for Formulating “AI Guidelines for Business”

- "AI Guidelines for Business" is formulated based on the "Social Principles of Human-Centric AI," integrating three guidelines in Japan with consideration for trends in the international society and the emergence of new technologies.
- Ensuring consistency with previous guidelines, it is expected to achieve continuous development as a governance mechanism that supports business activities.



Social Principles of Human-Centric AI

✓Consists of "Basic Philosophy," "Vision," "Social Principles of AI to which society should pay attention," etc.

✓Stated that the businesses should establish and comply with "R&D and Utilization Principles of AI"

Corresponds to “R&D and Utilization Principles of AI”

AI R&D guidelines

✓Compilation of AI R&D principles to be paid attention to in AI system development, along with explanation on the contents.

AI Utilization Guidelines

✓Compilation of AI Utilization Principles to be paid attention to in AI Utilization, along with the explanation on them.

Governance Guidelines for Implementation of AI principles

✓Presentation of action targets to be implemented by businesses as well as hypothetical examples of implementation, with the aim of supporting the implementation of the AI principles that is required for the facilitation of provision of AI.

- Trends in the international society
- Emergence of new technology

Basic Concept of “AI Guidelines for Business”

- The basic concepts of "AI Guidelines for Business" are 1 Support for voluntary efforts by businesses, 2 Coordination with international discussions, and 3 Ease of understanding for readers.
- In addition, the Guidelines will continue to be updated as a "Living Document" through continuous reviews by "multi-stakeholder" and with an emphasis on effectiveness and legitimacy.

Concepts

1 **Support for voluntary efforts by businesses**

Adopt a “risk-based approach” in which the degree of countermeasures corresponds to the magnitude and probability of the risk

2 **Coordination with international discussions**

Ensure consistency with trends and content of relevant domestic and international principles

3 **Ease of understanding for readers**

Allows each "AI developer," "AI provider," and "AI business user" to confirm the risks to be considered in the use of AI and the policies to address them.

＋

Processes

Multi-stakeholder

Formulated by continuous reviews with multi-stakeholder such as academic and research institutions, civil society including general consumers, and private sector companies, with an emphasis on effectiveness and legitimacy.

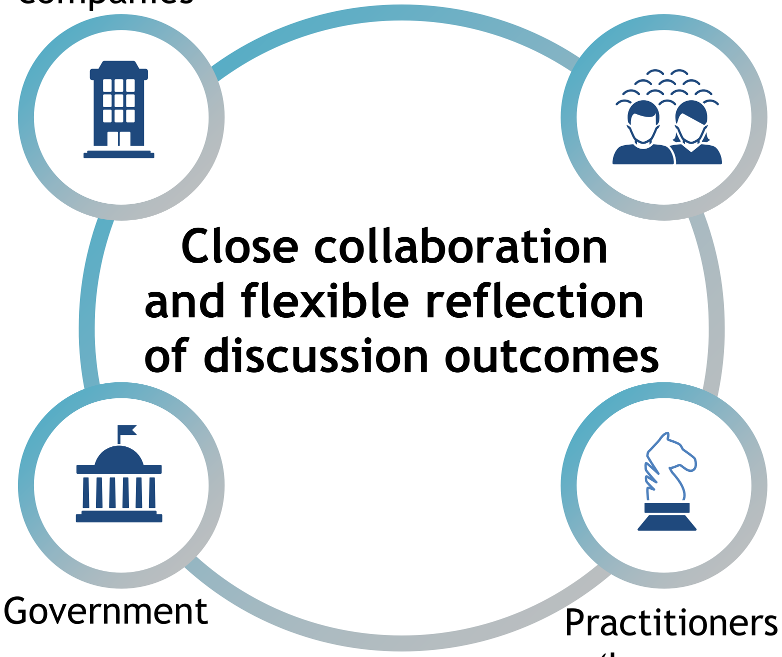
Living Document

Update as appropriate with reference to the philosophy of agile governance for continuous improvement of AI governance

Cooperation with Multi-Stakeholders

- Formulated not solely by the government, but in collaboration with various stakeholders (multi-stakeholder) such as academic and research institutions, civil society including general consumers, and private sector companies, with an emphasis on effectiveness and legitimacy through continuous review and consideration.

Collaborating Actors



Private sector companies

Civic organizations/ General consumers

Close collaboration and flexible reflection of discussion outcomes

Government

Practitioners (lawyers, researchers, consultants, etc.)

Collaboration Method

Numerous opportunities to exchange opinions and engage in discussion

- Review committee composed of the collaborating actors listed on the left
- Working groups primarily composed of practitioners
- Discussions with the private sector companies

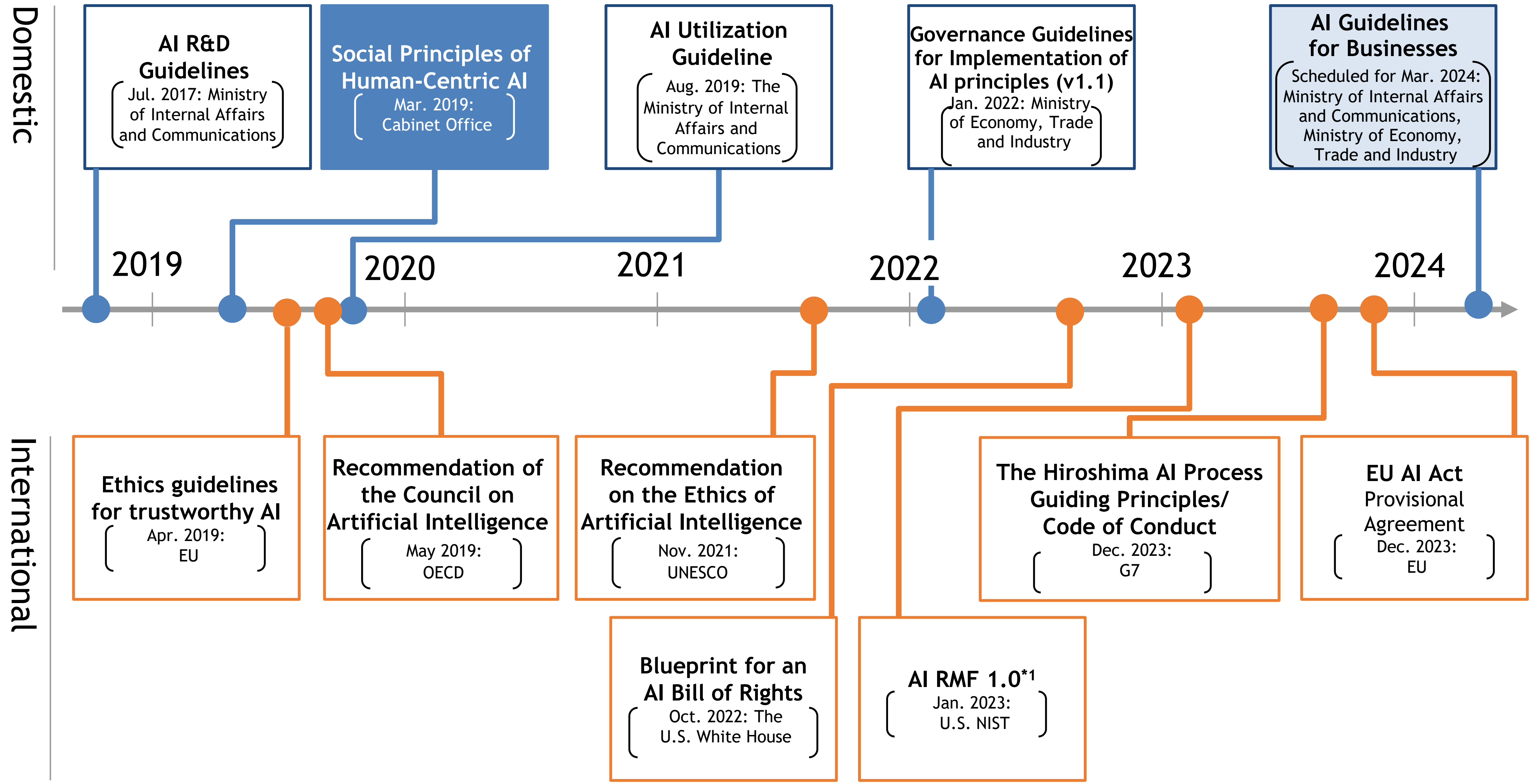
Gathering a wide range of knowledge through inquiries of opinions

- Approximately 100 experts
  - Private company representatives
  - Specialists, researchers
  - Civic organizations, consumer groups, etc.

Gathering a wide range of opinions through public comments

Major Principles Related to AI, etc.

- As the formulation of various regulations and guidelines is actively discussed in other countries, "AI Guidelines for Business" will also be closely aligned with various principles and regulatory trends.



Domestic

AI R&D Guidelines
(Jul. 2017: Ministry of Internal Affairs and Communications)

Social Principles of Human-Centric AI
(Mar. 2019: Cabinet Office)

AI Utilization Guideline
(Aug. 2019: The Ministry of Internal Affairs and Communications)

Governance Guidelines for Implementation of AI principles (v1.1)
(Jan. 2022: Ministry of Economy, Trade and Industry)

AI Guidelines for Businesses
(Scheduled for Mar. 2024: Ministry of Internal Affairs and Communications, Ministry of Economy, Trade and Industry)

International

Ethics guidelines for trustworthy AI
(Apr. 2019: EU)

Recommendation of the Council on Artificial Intelligence
(May 2019: OECD)

Recommendation on the Ethics of Artificial Intelligence
(Nov. 2021: UNESCO)

The Hiroshima AI Process Guiding Principles/ Code of Conduct
(Dec. 2023: G7)

EU AI Act Provisional Agreement
(Dec. 2023: EU)

Blueprint for an AI Bill of Rights
(Oct. 2022: The U.S. White House)

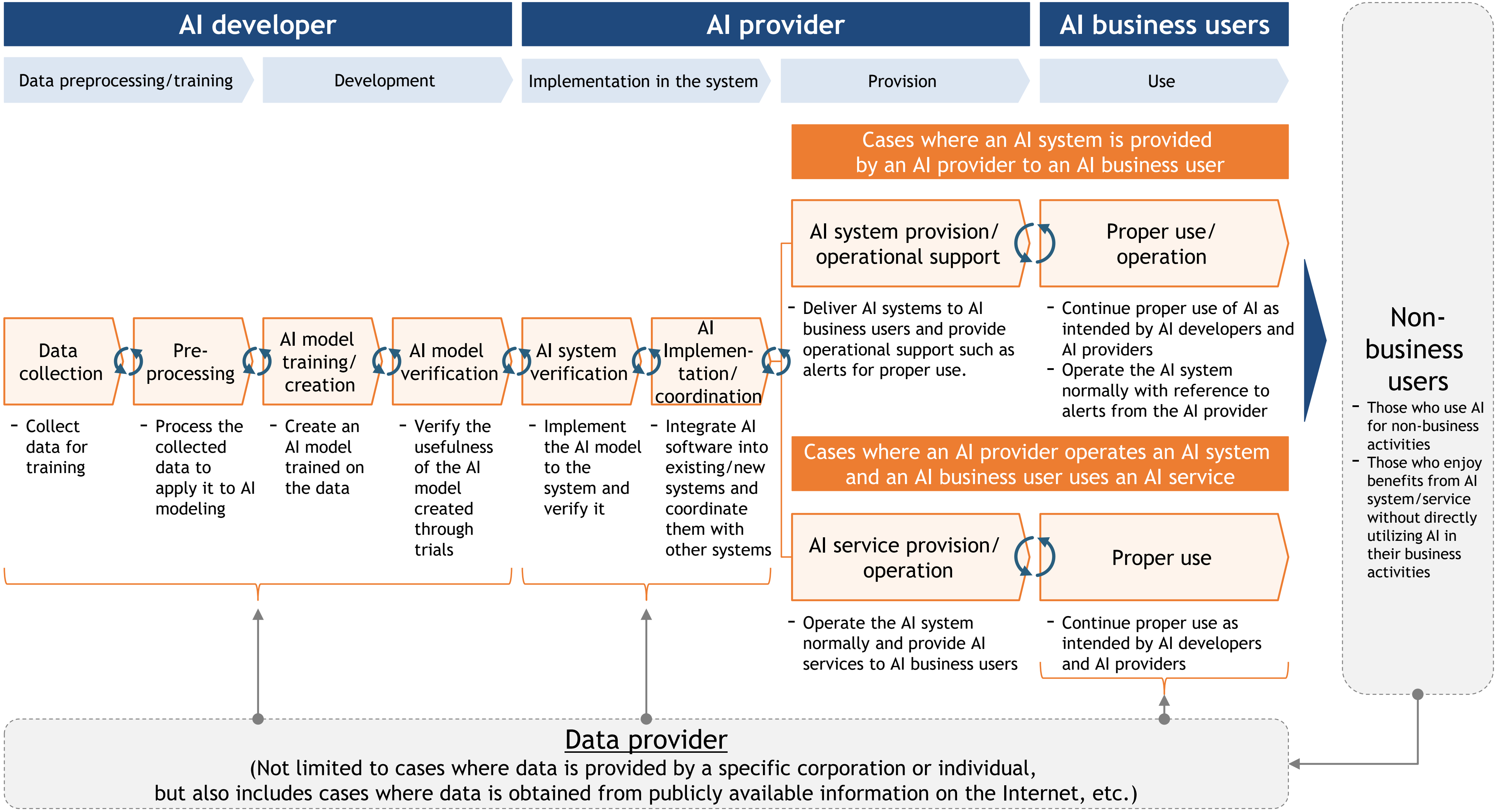
AI RMF 1.0[*1]
(Jan. 2023: U.S. NIST)

[*1] : AI Risk Management Framework 1.0

Actors in General AI Business Activities

- Considering their specific roles in the AI lifecycle, the positions in charge for AI business activities are broadly classified into three categories: "AI developers," "AI providers," and "AI business users."

  *“Data providers” and “non-business users” are excluded.



AI developer

AI provider

AI business users

Data preprocessing/training

Development

Implementation in the system

Provision

Use

Cases where an AI system is provided by an AI provider to an AI business user

AI system provision/ operational support

- Deliver AI systems to AI business users and provide operational support such as alerts for proper use.

Proper use/ operation

- Continue proper use of AI as intended by AI developers and AI providers
- Operate the AI system normally with reference to alerts from the AI provider

Data collection

- Collect data for training

Pre-processing

- Process the collected data to apply it to AI modeling

AI model training/ creation

- Create an AI model trained on the data

AI model verification

- Verify the usefulness of the AI model created through trials

AI system verification

- Implement the AI model to the system and verify it

AI Implementation/ coordination

- Integrate AI software into existing/new systems and coordinate them with other systems

Cases where an AI provider operates an AI system and an AI business user uses an AI service

AI service provision/ operation

- Operate the AI system normally and provide AI services to AI business users

Proper use

- Continue proper use as intended by AI developers and AI providers

Non-business users

- Those who use AI for non-business activities
- Those who enjoy benefits from AI system/service without directly utilizing AI in their business activities

Data provider

(Not limited to cases where data is provided by a specific corporation or individual, but also includes cases where data is obtained from publicly available information on the Internet, etc.)

Positioning of the "Guidelines for AI Businesses" in the Main Body and in the Appendix

- In the Main Body, we present "what kind of society to aim for (Basic Philosophy = why)" and "what kind of initiatives to take (Common Principles = what)," which are important for businesses to make safe and secure use of AI and maximize the benefits of AI.
- In the Appendix, we present "what approach to take (specific approaches = how)", under the assumption that this will lead to concrete actions by business operators.

Main Body（why, what)

Appendix (how)

What kind of society to aim for?

(Basic Philosophy=why)

What kind of initiatives to take?

(Common Principles=what)

What approach to take?

(Specific approaches=how)

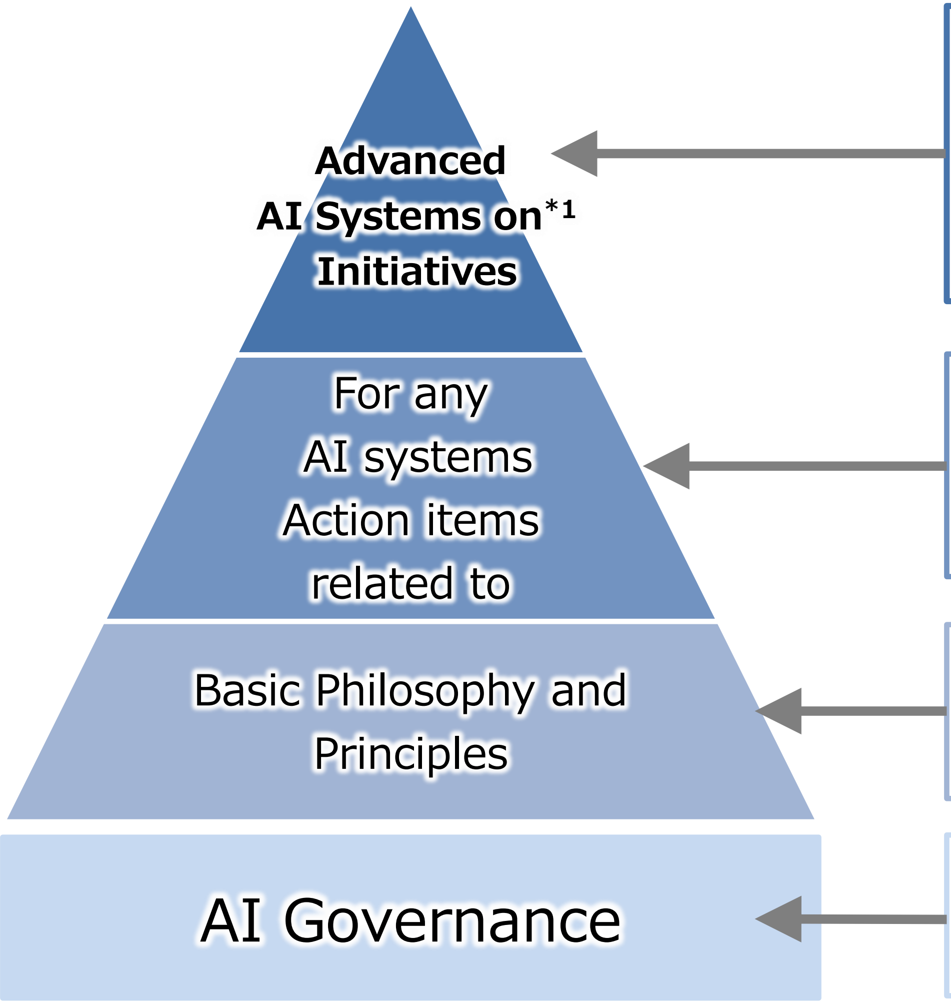
Structure of “AI Guidelines for Business”

- Descriptions in the Appendix correspond to those in the Main Body and serve as a commentary to support the reading of the Main Body and considerations and actions based on it.

	Main Body (why, what)			Appendix (how)	
For all actors	Part 1	Definitions		1. Part 1 Related [About AI]	A. Premises on AI B. Benefits/Risks of AI
	Part 2	The Society to Aim for with AI and What Each Actor Works On	A. Basic Philosophy B. Principles C. Common Guiding Principles D. Common Guiding Principles for businesses involved in advanced AI systems E. Establishing AI Governance	2. Part 2 Related [E. Establishing AI Governance]	A. Establishing AI Governance and Monitoring by Management B. Examples of AI Governance Initiatives by Businesses
Classified by actors	Part 3	Matters Related to AI Developers	※Including "Additional matters in the "Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems"."	3. Part 3 Related [For AI Developers]	A. Commentary on Part 3 B. Commentary on Part 2 C. Common Guiding Principles C. Matters to be complied with in the development of advanced AI systems
	Part 4	Matters Related to AI Providers		4. Part 4 Related [For AI Providers]	A. Commentary on Part 4 B. Commentary on Part 2 C. Common Guiding Principles
	Part 5	Matters Related to AI Business Users		5. Part 5 Related [For AI Business Users]	A. Commentary on Part 5 B. Commentary on Part 2 C. Common Guiding Principles
Other references				6. Major considerations when referring to the "Contract Guidelines on Utilization of AI and Data" 7. Checklist 8. Cross-cutting hypothetical cases 9. Comparative table with international guidelines	

Scope of the AI Guidelines for Businesses

- **Broad coverage of (all possible) AI systems and services, including general AI,** reflecting the international guidelines and international codes of conduct for advanced AI systems compiled by the Hiroshima AI Process
- In actual AI development, provision, and use, it is important for **each business entity** to **voluntarily promote specific efforts, such as establishing appropriate AI governance for compliance with the guidelines,** by referring to these guidelines.



Advanced AI Systems on[*1] Initiatives

For any AI systems Action items related to

Basic Philosophy and Principles

AI Governance

Reflects the outcome of the Hiroshima AI process (Comprehensive Policy Framework)

- Hiroshima Process International Guiding Principles for All AI Actors and for Organizations Developing Advanced AI Systems
- Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems

Part 2 D. "Common Guidance for Businesses on Advanced AI Systems"; Part 3.

Organize guidelines and matters to be addressed by each entity based on the principles.
Also incorporate AI R&D Guidelines and AI utilization guidelines (Ministry of Internal Affairs and Communications).

Part 2 C. "Common Guidelines", Parts 3-5

The Basic Philosophy and Principles are built on the Basic Philosophy of the Social Principles of Human-Centric AI and based on the OECD AI Principles and other principles.

Part 2 A. "Basic Principles" B. "Principles"

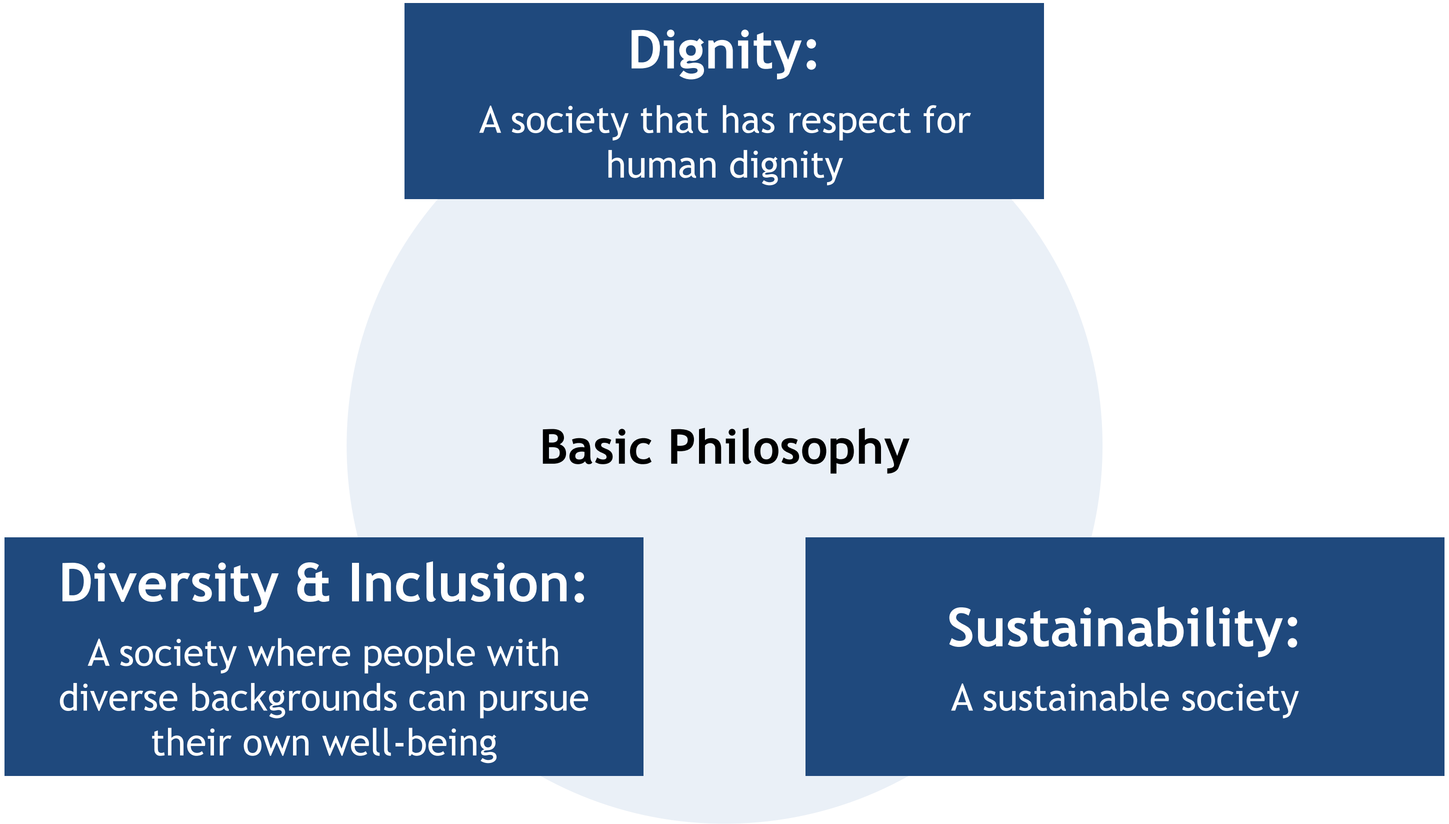
Organized based on the Governance Guidelines for Implementation of AI Principles (Ministry of Economy, Trade and Industry)

Part 2 E. "Establishing AI Governance"

[*1] : The most advanced AI systems, including the most advanced foundation models and generative AI systems

Basic Philosophy

- In the "Social Principles of Human-Centric AI," there is an emphasis on the importance of AI's contribution to the realization of Society 5.0, and its use as a public good for humanity, leading to global sustainability through qualitative changes in the nature of society and true innovation.
- In addition, the following three values are respected as the "Basic Philosophy", and "a society should be built in a way that can pursue the realization of these three values ". This universal concept continues to be the philosophy that should be aimed for in the future.



Dignity:
A society that has respect for human dignity

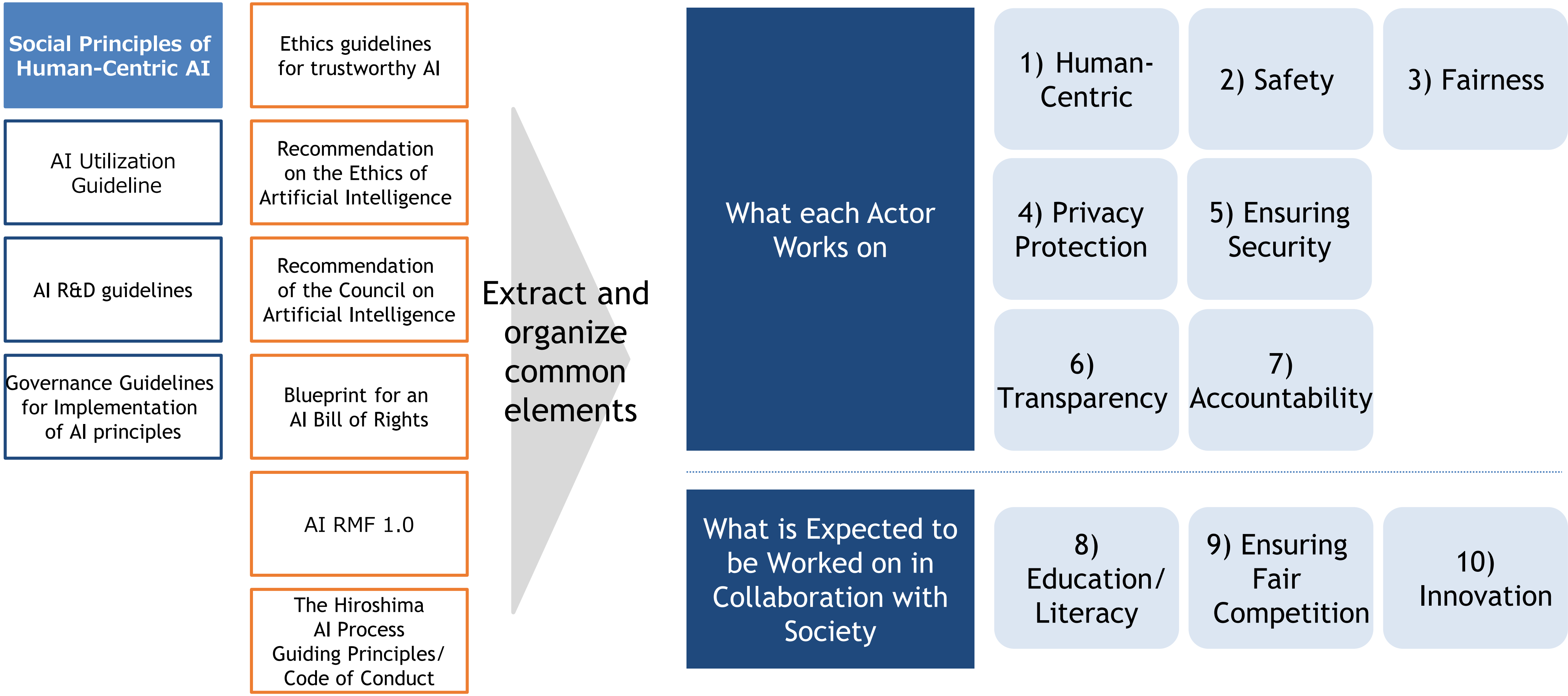
Basic Philosophy

Diversity & Inclusion:
A society where people with diverse backgrounds can pursue their own well-being

Sustainability:
A sustainable society

Guiding Principles Common to All Actors

- The "Common Guiding Principles" outlines what each actor works on in collaboration to achieve the society aimed for through the use of AI.
- The "Common Guiding Principles" is formulated based on the "Social Principles of Human-Centric AI", integrating three guidelines in Japan with consideration for trends in other countries and the emergence of new technologies.
- As a result, it is organized into what each actor works on and what is expected to be worked on in collaboration with society.



Social Principles of Human-Centric AI

AI Utilization Guideline

AI R&D guidelines

Governance Guidelines for Implementation of AI principles

Ethics guidelines for trustworthy AI

Recommendation on the Ethics of Artificial Intelligence

Recommendation of the Council on Artificial Intelligence

Blueprint for an AI Bill of Rights

AI RMF 1.0

The Hiroshima AI Process Guiding Principles/ Code of Conduct

Extract and organize common elements

What each Actor Works on

1) Human-Centric

2) Safety

3) Fairness

4) Privacy Protection

5) Ensuring Security

6) Transparency

7) Accountability

What is Expected to be Worked on in Collaboration with Society

8) Education/ Literacy

9) Ensuring Fair Competition

10) Innovation

Guiding Principles Common to All Actors [1/2]

- Each actor develops, provides, and uses AI systems and services with respect for the rule of law, human rights, democracy, diversity, and a fair and just society in light of the philosophy of 1) Human-Centric, and complies with the Constitution, relevant laws and regulations including the Act on the Protection of Personal Information, Acts on Intellectual Property Protection, and other existing laws and regulations in individual fields related to AI.
- Each actor establishes AI governance and operates it continuously (while taking into account the degree of risk of AI and the resource constraints of each actor).

Guiding Principles		Contents (excerpts of main points)
What each Actor Works on	1) Human-Centric	✓ Act in a way that AI expands abilities of people and enables them to pursue their diverse well-being. ✓ Recognize the increasing risk of AI-generated **disinformation, misinformation, and biased information** destabilizing and disrupting society, and take necessary countermeasures. ✓ Be mindful to facilitate the **use of AI by the socially vulnerable** so that more people can enjoy its benefits
	2) Safety	✓ Conduct appropriate risk analysis and take **measures to address risks**. ✓ Avoid harm caused by the provision and use of AI that deviates from the intended purpose within the scope of the control of each actor. ✓ Consider the accuracy, etc. of data used for training, etc., based on the characteristics and applications of AI system/service, and appropriately implement **support for data transparency, compliance with legal frameworks**, and AI model updating, etc. to the extent reasonable.
	3) Fairness	✓ Strive to **minimize unfair and harmful biases and discrimination** against specific individuals or groups by virtue of their race, gender, nationality, age, political beliefs, religion, or other diverse backgrounds. ✓ Develop, provide, and use AI systems and services with **attention to unconscious and potential bias**, considering the use of AI systems and services that involve with human judgment rather than having AI make judgments solely on its own, to ensure that the outputs of AI systems and services do not lack fairness.
	4) Privacy Protection	✓ **Comply with relevant laws and regulations** such as the Act on the Protection of Personal Information and **develop and publish a privacy policy of each actor** to ensure that the privacy of stakeholders, including each actor, is respected and protected, taking into account the social context and reasonable expectations of people, and respond in accordance with the importance of such privacy.
	5) Ensuring Security	✓ Take reasonable measures in light of the technological level at the time to **maintain the confidentiality, integrity, and availability** of AI systems and services, and to ensure the secure use of AI at all times. ✓ **Identify considerations for dealing with risks from external attacks** on AI systems and services, as new methods of attack are emerging every day.

Guiding Principles Common to All Actors [2/2]

- Each actor develops, provides, and uses AI systems and services with respect for the rule of law, human rights, democracy, diversity, and a fair and just society in light of the philosophy of 1) Human-Centric, and complies with the Constitution, relevant laws and regulations including the Act on the Protection of Personal Information, Acts on Intellectual Property Protection, and other existing laws and regulations in individual fields related to AI.
- Each actor establishes AI governance and operates it continuously (while taking into account the degree of risk of AI and the resource constraints of each actor).

Guiding Principles		Contents (excerpts of main points)
What each Actor Works on	6) Transparency	✓ **Provide appropriate information to stakeholders** to the extent necessary, reasonable, and technically feasible, while ensuring the verifiability of AI systems and services, taking into account the social context in which AI is utilized. (e.g., the fact that AI is being used, data collection and annotation methods, capabilities and limitations of the AI system/service, appropriate/inappropriate use by the provider, etc.)
	7) Accountability	✓ Provide information and explanations to stakeholders regarding traceability, compliance with common guiding principles, etc. ✓ **Establish** and publicly report **AI governance policies, privacy policy, etc**. for each actor. ✓ Document and store relevant information, and make it available for reference when and where needed, in a form that is accessible and suitable for use.
What is Expected to be Worked on in Collaboration with Society	8) Education /Literacy	✓ It is expected to take necessary steps to **ensure** that those involved in AI have **a sufficient level of AI literacy** for their involvement. ✓ It is expected to **educate stakeholders**, taking into account the characteristics of AI, such as complexity and misinformation, as well as the possibility of intentional misuse.
	9) Ensuring Fair Competition	✓ It is expected to make efforts to **maintain a fair competitive environment for AI** in order to create new businesses and services that utilize AI, maintain sustainable economic growth, and present solutions to social issues.
	10) Innovation	✓ It is expected to promote internationalization and diversification, **industry-academia-government partnerships**, and open innovation. ✓ It is expected to ensure interconnectivity and interoperability of own AI systems/services with other AI systems/services. ✓ It is expected to conform to standard specifications.

Common guidelines for businesses involved in advanced AI systems

- In addition to the Common Guiding Principles, the following should be complied. [*1] However, since some of the contents of I) through XI) apply only to AI developers, each entity is required to comply with them to the appropriate extent.

I. Take appropriate measures throughout the development of advanced AI systems, including prior to and throughout their deployment and placement on the market, to identify, evaluate, and mitigate risks across the AI lifecycle.

II. Identify and mitigate vulnerabilities, and, where appropriate, incidents and patterns of misuse, after deployment including placement on the market.

III. Publicly report advanced AI systems' capabilities, limitations and domains of appropriate and inappropriate use, to support ensuring sufficient transparency, thereby contributing to increase accountability.

IV. Work towards responsible information sharing and reporting of incidents among organizations developing advanced AI systems including with industry, governments, civil society, and academia.

V. Develop, implement and disclose AI governance and risk management policies, grounded in a risk-based approach – including privacy policies, and mitigation measures, in particular for organizations developing advanced AI systems.

VI. Invest in and implement robust security controls, including physical security, cybersecurity and insider threat safeguards across the AI lifecycle.

VII. Develop and deploy reliable content authentication and provenance mechanisms, where technically feasible, such as watermarking or other techniques to enable users to identify AI-generated content.

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

IX. Prioritize the development of advanced AI systems to address the world's greatest challenges, notably but not limited to the climate crisis, global health and education.

X. Advance the development of and, where appropriate, adoption of international technical standards.

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

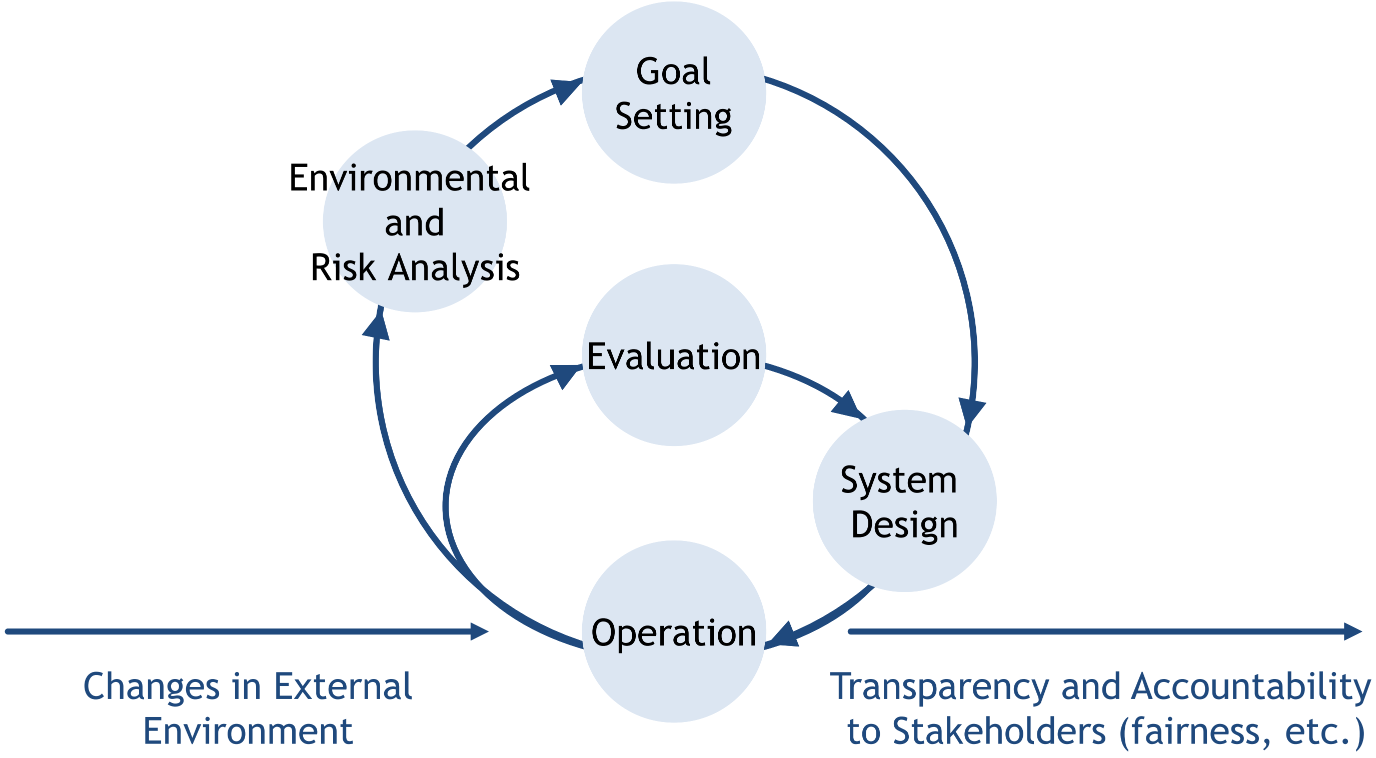
XII. Promote and contribute to trustworthy and responsible use of advanced AI systems.

[*1] :For details, see "Hiroshima AI Process Comprehensive Policy Framework, II Hiroshima Process International Guiding Principles for All AI Actors and for Organizations Developing Advanced AI Systems" in the "Hiroshima AI Process G7 Digital &Tech Minister's Statement" (December 2023)

Establishing AI Governance

- In order to utilize AI safely and securely, it is important to manage risks by establishing appropriate governance under the leadership of management, paying attention to the following:
  - Ensure collaboration between actors from the perspective of value chain/risk chain for issues that involve multiple actors
  - Consider appropriate governance to ensure free cross-border transfer of data when the above issues involve multiple countries
  - Integrate into each organization's strategy as well as corporate structure and permeate into the culture through management's commitment

Establishing Appropriate Governance


Goal Setting
Environmental and Risk Analysis
Evaluation
System Design
Operation
Changes in External Environment
Transparency and Accountability to Stakeholders (fairness, etc.)

+

Ensuring collaboration between multiple actors

Ensure collaboration between actors from the value chain/risk chain perspective

Appropriate cross-border data transfer

Appropriate risk management/ governance implementation in case of multi-country scenarios

Management commitment

Integrate into strategies/structure and permeate into the culture of each organization

Matters Related to AI Developers [1/2]

- It is especially important to consider as much as possible in advance how AI will affect when it is provided/used, and to take measures to deal with it, since AI developers can directly design and modify AI models

During data Preprocessing/ training	D-2) i.	Proper Training of Data	- Handle data appropriately in accordance with laws and regulations through Privacy by Design, etc., when confidential information, personal data, and data protected by intellectual property rights that require attention are included. - **Implement appropriate safeguards**, such as considering the introduction of data management and restriction functions, etc.
	D-3) i.	Consideration for Bias in Data	- Take reasonable measures to **manage data quality** by paying attention that bias can be included in the process of training data and model. - Develop based on a variety of methods, recognizing that bias cannot be completely eliminated.
During AI development	D-2) ii.	Development in Consideration of Human Life, Mind, Body, and Property, as well as the Environment	- Consider performance requirements for use in a variety of situations, including unanticipated environments, and ways to **minimize risk**.
	D-2) iii.	Development Contributing to Proper Use	- Select trained AI models appropriately when developing with a safe range of availability settings and performing post-training on the AI models.
	D-3) ii.	Consideration for Bias in AI Model Algorithms, etc.	- Consider even the possibility of bias contained within each of the technical components of the AI model
	D-5) i.	Implementation of Mechanisms for Security Measures	- **Take appropriate security measures** in light of the characteristics of the technology employed (Secure by Design).
	D-6) i.	Ensuring of Verifiability and Maintenance of Work Records	- Maintain and improve the quality of AI while **preserving work records for post-verification**, based on the characteristics that the predictive performance and quality of AI may significantly fluctuate after utilization and may not reach the expected system.

Matters Related to AI Developers [2/2]

- It is especially important to consider as much as possible in advance how AI will affect when it is provided/used, and to take measures to deal with it, since AI developers can directly design and modify AI models

After development	D-5) ii.	Attention to the Latest Trends	- **Identify what to pay attention to** in each development process in order to respond to the risks as new attack methods against AI systems are emerging every day.
	D-6) ii.	Provision of Information to Relevant Stakeholders	- **Provide information** on the technical characteristics and safety assurance mechanisms of AI systems, foreseeable risks and mitigation measures, and causes of and response to defects.
	D-7) i.	Explanation of the Status of Compliance with Common Guiding Principles for AI Providers	- **Provide information and explanations** to AI providers on the possible fluctuations in AI quality and **the resulting risks**, etc.
	D-7) ii.	Documentation of Development-Related Information	- **Document** the development process of the AI system, data collection, labeling, and used algorithms, etc. that impact decision making.
	D-10) i.	Contribution to the Creation of Innovation Opportunities	- Conduct **research on quality, reliability, and development methodologies**, etc. - Contribute to maintaining **sustainable economic growth and solving social issues** - Internationalize, diversify, and promote industry-academia-government partnerships by referencing trends in international discussions such as DFFT, participating in AI developer communities and academic societies, etc. - **Provide information to society as a whole**.

See "Matters to be complied with in the development of advanced AI systems" for AI developers who develop advanced AI systems, including the most advanced foundation models and generative AI systems.

Matters Related to AI Providers [1/2]

- It is important for AI providers to achieve the provision of AI systems and services on the basis of the operation and proper use of AI

During AI system implementation	P-2) i.	Development in Consideration of Human Life, Mind, Body, and Property, as well as the Environment	- Ensure that the system maintains performance levels under a variety of conditions and consider ways to **minimize risk**.
	P-2) ii.	Development Contributing to Proper Use	- **Consider whether there is any difference between the anticipated use environment of the AI developer and that of the AI business user**, while making efforts to ensure the accuracy of the data, etc.
	P-3) i.	Considerations for Bias in AI System Configurations and Data	- **Consider bias** in reference information, external services, and outputs to ensure fairness of data. - **Regularly evaluate** the inputs and outputs of AI models and **the basis for decisions**, and monitor for inappropriate bias. - Consider the possibility that AI systems etc. that receive the output results of AI models may contain biases that arbitrarily limit the judgment of users.
	P-4) i.	Implementation of Mechanisms and Measures to Protect Privacy	- **Take privacy protection measures** such as the implementation of mechanisms to control and restrict access to personal data in an appropriate manner in light of the characteristics of the technology employed (Privacy by Design).
	P-5) i.	Implementation of Mechanisms for Security Measures	- **Take appropriate security measures** in light of the characteristics of the technology employed (Secure by Design).
	P-6) i.	Documentation of System Architecture, etc.	- **Document** the system architecture, data processing processes, etc. that influence the decision-making of the AI system.

Matters Related to AI providers [2/2].

- It is important for AI providers to realize the provision of AI systems and services based on the operation and proper use of AI

AI System Service After Provision

P-2) ii.	Provisions that contribute to appropriate use	- Regularly verify that AI systems and services are being used for **appropriate** purposes
P-4) ii.	Countermeasures Against Privacy Violations	- **Gather information on** privacy violations in AI systems and services **as appropriate, and** consider **ways to prevent recurrence**
P-5) ii.	Vulnerability Response	- Identify trends in what needs to be taken care of in each process of provisioning to address the latest risks and **consider eliminating vulnerabilities**
P-6) ii.	Provide information to Relevant Stakeholders	- Be able to explain information about the technical characteristics of the AI system, foreseeable risks and mitigation measures, possible output or program changes, causes of failures and response status and incident cases, data collection policies and their learning methods and implementation systems, etc. - **Providing information and explanations on the fact that AI is being used, appropriate/inappropriate use, updates and the reasons for them**, etc., in light of the nature of AI and the purpose of its use
P-7) i.	Explanation of the state of compliance with common guidelines for AI users	- **Promote the appropriate use** of AI and **providing AI users with information on** the use of data whose accuracy and, where necessary, up-to-dateness are guaranteed, warnings against learning inappropriate models through in-context learning, and **points to keep in mind when entering personal information** - Alerting the public about inappropriate input of personal data into AI systems and services
P-7) ii.	Documentation of Terms of Service, etc.	- **Create terms of service** for AI users **and clearly state the privacy policy**

AI providers dealing with advanced AI systems should, with respect to "Part 2 D. Guidelines Common to Entities Involved with Advanced AI Systems, I) to XI) should be complied with to the appropriate extent, and XII) should be complied with with respect to

Matters related to AI users

- It is important for AI users to acquire the knowledge necessary for more effective use of AI, in addition to continuous appropriate use and operation of AI systems as needed, within the scope intended by AI providers.

AI System Service when using	U-2) i.	Appropriate use with safety considerations	- **Use AI within the scope assumed by the AI provider in its design,** in compliance with the usage considerations set forth by the AI provider - Understand the degree of accuracy and risk with respect to AI output and **identify various risk factors before use**
	U-3) i.	Consideration of bias in input data and prompts	- **Make business use decisions on AI output results** responsibly, with data input that ensures fairness, and with attention to bias in the prompts
	U-4) i.	Measures against improper input of personal data and breaches of privacy	- Take care not to inappropriately enter personal information into AI systems and services - **Gather information on privacy violations in** AI systems and services, **as appropriate,** and consider preventing them
	U-5) i.	Implementation of security measures	- Comply **with security considerations by** AI providers
	U-6) i.	Provide Information to Relevant Stakeholders	- **Obtain output results** by inputting data that ensures fairness, being mindful of bias in the prompts, and **disseminating the results to relevant stakeholders who need to know when the results are used to make business decisions**
	U-7) i.	Briefing relevant stakeholders	- **Provide information** on the means and format of data provision in **a plain and accessible manner to the relevant stakeholders** in advance, taking into account the characteristics and uses of AI, points of contact with the recipient, privacy policy, etc. - Provide an opportunity to seek human judgment to a reasonable extent as necessary, when AI output results are used to evaluate of a specific individual or group - **Establish a point of contact to respond to inquiries from relevant stakeholders**, and accept explanations and requests in cooperation with AI providers
	U-7) ii.	Use of documents provided and compliance with terms & conditions	- **Maintain and utilize documentation about** the system provided by the AI provider - **Comply with the terms of service** set forth by the AI provider

AI users dealing with advanced AI systems should comply with I) - XI) to the appropriate extent with regard to "Part 2 D. Guidelines common to operators involved in advanced AI systems" and comply with XII)

総務省

MIC

Ministry of Internal Affairs and Communications

経済産業省

Ministry of Economy, Trade and Industry