Summary of the Japan's Cybersecurity Strategy (July 27, 2018 Cabinet Decision)

◆ New Cybersecurity Strategy is the second "basic plan for Cybersecurity" under the Basic Act of Cybersecurity. Far-seeing 2020, the Strategy shows basic position and vision on Cybersecurity, and objectives and implementation policies in next 3 years (2018~2021) domestically and internationally.

1 Introduction

- A paradigm shift brought about by cyberspace which no human have experienced before (Society5.0)
- Increasing seriousness of threats with cyberspace and real space unification, necessity of new strategy far-seeing the Tokyo 2020 Games

2 Understanding on Cyberspace

- Knowledge, technologies, and services in cyberspace, such as Artificial Intelligence (AI) and Internet of Things (IoT) are becoming adopted in society and bring about abundance for humanity.
- There is always the latent risk that the providers of these technologies will lose the ability to control them. Attacks directed at IoT, critical infrastructure, supply chains, as well as incidents suspected to have been state-sponsored will increase socio-economic losses exponentially.

3 Visions and Objective of this Strategy

- Adherence to the Basic Position on Cybersecurity (Objectives of the Basic Act on Cybersecurity; Basic Ideals ("free, fair and secure cyberspace"); Basic Principles)
- Basic Vision of Cybersecurity as a Goal: Cybersecurity for sustainable development (Promotion of "Cybersecurity Ecosystem"); Three Approaches (1. Mission Assurance for service providers; 2. Risk Management; 3. Participation, Cooperation and Collaboration)

4 Policy Approaches towards Achieving the Objective

Enabling Socio-Economic Vitality and Sustainable Development

~Advancing Cybersecurity as Value Creation Driver~

- Advancing Cybersecurity as Value Creation Driver
- Achieving a Supply Chain that Creates Values through Diverse Connections
- Building Secure IoT Systems

Building a Safe and Secure Society for the People

~Mission assurance for protecting people and society~

- Measures for the Protection of People and Society
- Protection of Critical Infrastructure through Public and Private Sector Cooperation
- Strengthening and Improving Security in Governmental Bodies and Government-Related Entities
- Ensuring a Safe and Secure Educational and Research Environment at Universities etc.
- Initiatives for the Tokyo 2020 Games and Beyond
- Building an Information Sharing/Collaboration Framework that Extends beyond Traditional Frameworks
- Strengthening the Incident Readiness Against Massive Cyberattacks

Contribution to the Peace and Stability of the Int'l Community and Japan's National Security

~Commitment to a Free, Fair and Secure Cyberspace~

- Commitment to a Free, Fair and Secure Cyberspace
- Strengthening Capabilities for Defense, Deterrence, and Situational Awareness
- International Cooperation and Collaboration

Cross-cutting Approaches to Cybersecurity

- Development and Assurance of Cybersecurity Human Resource
- Advancement of Research and Development
- Cooperation by Everyone who is the Main Player in Cybersecurity

5 Promotion and Implementation of Cybersecurity

The related government bodies will keep working on improving their cybersecurity capabilities under the leadership of National center of Incident readiness and Strategy for Cybersecurity(NISC), and NISC will play its leading role as the focal point in coordinating intra-government collaboration and promoting partnerships between industry, academia, and the public and private sectors.

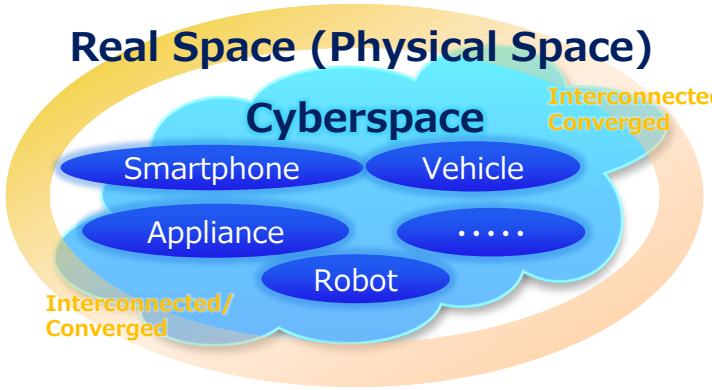
The Current Understanding and the Future Image
(Increasing Seriousness of Threats with Cyberspace and Real Space Unification)

Medium and Long Term

Shift from as of Formulating Current Strategy (Sept. 2015) to Present

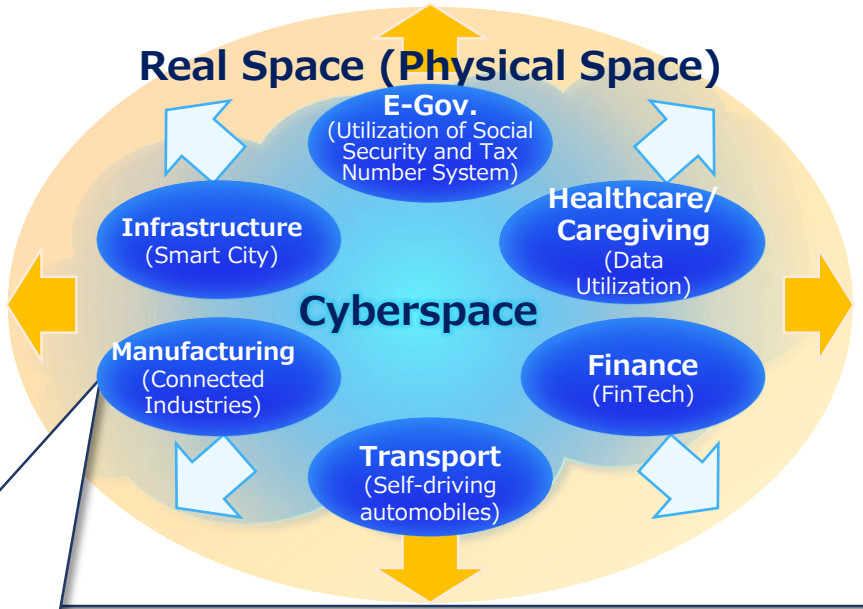
[(As of formulating the strategy2015) Emergence of Interconnected and Converged Information Society]

- People and things in real space have become interconnected to the network, and cyberspace and real space have become highly integrated. -



Unification

[Unification of Cyberspace and Real Space]



Understanding on Cyberspace

・**While knowledge, technologies, and services in cyberspace**, such as AI, IoT, Fintech, robotics, 3D printers, and AR/VR, **are becoming established in society and leading innovations** that are transforming the existing structures in socio-economic activities and the daily lives of Japanese people, **there are always the latent uncertainties**.

Benefits of Cyberspace

- Technologies and services in cyberspace are **controlled and gaining routine use in numerous domains**. **They bring about abundance for humanity**.
- **The evolution of AI** based on deep learning is bringing about changes, it is beginning to be adopted in a wide range of industries.
- New businesses and services are being created to utilize **the data obtained from IoT devices**.

Increasing Threats in Cyberspace

- **There is always the latent risk that the providers** of technologies and services in cyberspace **will lose the ability to control** them, in which case **they can cause immeasurable economic and social loss or damage**.
- **Society will be significantly affected when interruptions occur to numerous businesses, functions, and services** due to the interruption of important infrastructural services or unintended behavior by IoT devices, and situations could even develop to the point of **becoming national security issues**.
- Inadequacies in cybersecurity measures are predicted to **directly cause and expand financial damages and losses**.

Basic Vision and Approaches for Cybersecurity
(Cybersecurity for Sustainable Development –Promotion of "Cybersecurity Ecosystem"-)

○ Japan will aims for sustainable development of cyberspace(Realizing "Cybersecurity Ecosystem") to realize a society(Society5.0*) where new values and services are generated continuously, bringing abundance to the people.
○ Japan will adhere to its basic position on cybersecurity presented in the Strategy 2015 and promote public and private sector initiatives on cybersecurity based on three approaches (1. mission assurance for service providers; 2. risk management; and 3. participation, coordination and collaboration).

* The fifth society in human history following hunting, agriculture, industry and information. New value or service emerge one after another and generate wealth to subjective people of the society (from Future Investment Strategy 2017)

<Basic Vision of Cybersecurity>

1. Mission Assurance
Reliable Execution of Operations & Services

- Understand the operations or services that should be carried out as "missions," and ensure capabilities and resources* to execute such "missions."
- Each organization should proactively work towards securing cybersecurity to conduct its "missions," without just relying on some experts.

* Including human resource, equipment, facilities, network, information systems, infrastructure and supply chain

Cybersecurity for Sustainable Development
–Realizing "Cybersecurity Ecosystem"-

The image of cyberspace evolving through autonomous initiatives of all stakeholders mutually impacting each other will be called the "Cybersecurity Ecosystem" as compared to a type of ecosystem that develops sustainably.

2.Risk Management
Assessment of Uncertainty & Appropriate Response

- Minimizing risks to an acceptable level by identifying, analyzing, and evaluating them associated with "missions" assigned to organizations.

3. Participation, Coordination,and Collaboration (New Cyber Hygiene)
Measures, Coordination & Cooperation by Individuals & Organization from Peacetime

- Fundamental initiatives implemented by individuals or organizations from peacetime to prevent damages or its escalation possibly caused by threats in cyberspace.
- Sharing information and mutually coordination and collaboration between each other regardless of peacetime or emergency situations should be regarded as new cyber hygiene.

Enabling Socio-Economic Vitality and Sustainable Development

・It is necessary in all industrial sectors that consistent cybersecurity measures are carried out to ensure corporate business continuity and create new value. In doing so, it is important for the companies to implement the measures for which should be handled as part of risk management.

1. Advancing Cybersecurity as Value Creation Driver

- Raising executive awareness (from “cost” to “investment”)
- Promote companies to actively disseminate and disclose information regarding their cybersecurity initiatives
- Promoting the use of insurance in cybersecurity in cooperation with private sectors
- Preparing guidelines to support the challenges towards new value creation, risk analysis, and research & development

2. Achieving a Supply Chain that Creates Values through Diverse Connections

- Clarifying threats in the supply chain and formulating as well as disseminate frameworks that cut across industrial categories for implementing operational-level measures
- Offering specific measures of each sector
- Promoting initiatives by small and medium-sized enterprises

3. Building Secure IoT Systems

- Improving structural framework for IoT systems and international standard
- Establishing models regarding measures for vulnerable IoT devices and expanding them overseas through international coordination and standardization

Mission Assurance for Protecting People and Society

For the realization of society in which the people can live safely and securely, it is important to ensure multi-layered cybersecurity, through the coordination of multi-stakeholders, including governmental bodies, local governments, cyber-related enterprises, critical infrastructure operators, educational and research institutions, and every people themselves. The government will promote initiatives based on the "mission assurance" approach in order to reduce risks to an acceptable level and ensure that these operations and services are provided safely and continuously.

1. Measures for the Protection of the People and Society

- Promoting the policy of "Proactive Cyber Defense "
  (Promoting the sharing and utilization of threat information, Providing information of vulnerabilities)
- Enhancing measures against cybercrimes

2. Protection of Critical Infrastructure through Public and Private Sector Cooperation

- Promoting initiatives based on the Cybersecurity Policy for Critical Infrastructure Protection
- Strengthening security in local governments

3. Strengthening and Improving Security in Governmental Bodies and Government-Related Entities

- Managing the state of information systems in real-time
  (Measures based on new common standards)

4. Ensuring a Safe and Secure Educational and Research Environment at Universities etc.

- Implementing practice for each level, and practical training and exercises

5. Initiatives for the Tokyo 2020 Games and Beyond

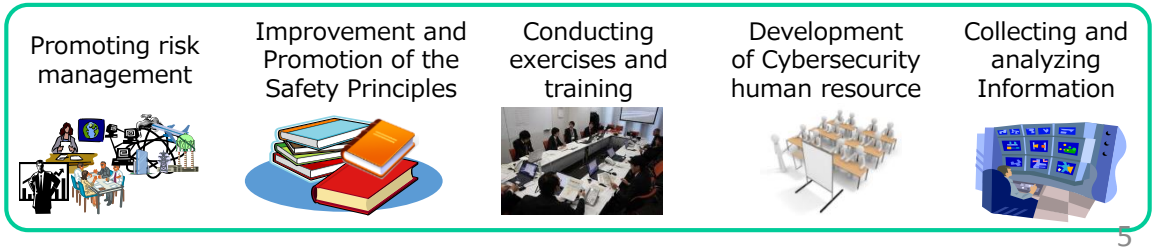
- Promoting the development of the Cyber Security Incident Response Coordination Center

6. Building an Information Sharing/Collaboration Framework that Extends beyond Traditional Frameworks

- Promoting information sharing/collaboration between multi-stakeholders

7. Strengthening the Incident Readiness Against Massive Cyberattacks

- Strengthening the incident readiness against massive cyberattacks in order to work on risk management for both cyberspace and real space



Commitment to a Free, Fair, and Secure Cyberspace

A free, fair, and secure cyberspace is essential to contribute to the peace and stability of the international community and to Japan's national security. In order to safeguard a free, fair, and secure cyberspace, Japan will communicate its position in the international fora, ensure international security and promote international collaboration.

1. Commitment to a Free, Fair, and Secure Cyberspace

- Communicating the ideas of a free, fair and secure cyberspace
  (Communicating basic approach to cybersecurity, Thwart any efforts that aim to inhibit the development of cyberspace)
- Promoting the rule of law in cyberspace
  (Application of existing international law to cyberspace, Contribution to the development and universalization of norms)

2. Strengthening Capabilities for Defense, Deterrence, and Situational Awareness

- Ensuring national resilience
  (Mission assurance, Defending Japan's advanced technologies and defense related technologies)
- Enhancing deterrence capabilities
  (Measures for effective deterrence, Confidence building measures)
- Strengthening cyber situational awareness
  (Increasing the capabilities of relevant governmental bodies, Threat information sharing)

3. International Cooperation and Collaboration

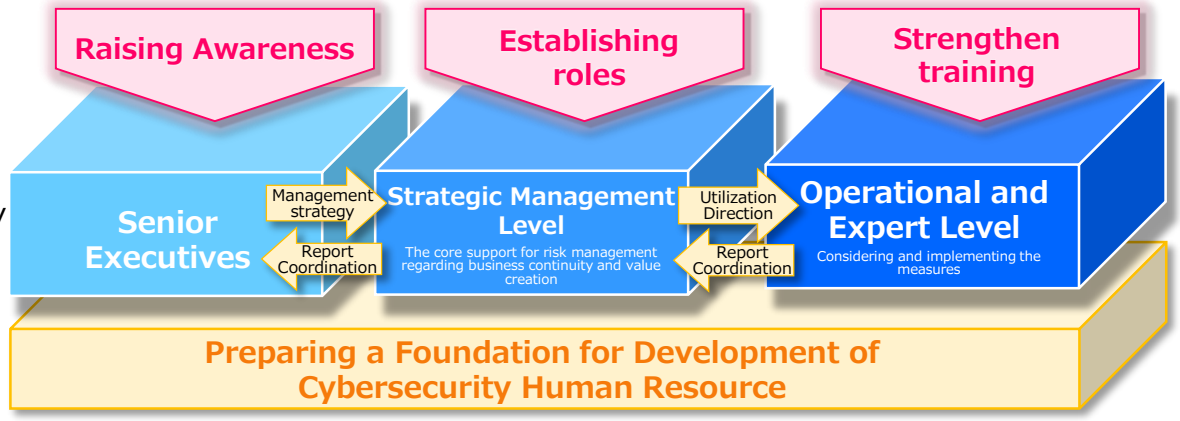
- Sharing expertise and coordinating policy
- International collaboration for incident response
- Cooperating for capacity building

Promoting Measures the Cross-cutting Approaches to Cybersecurity

It is important to work on human resource development and research and development as a foundation for the policy goals from both a cross-cutting and mid- and long-term perspective. Simultaneously, it is also crucial to promote a cooperative approach in which everyone plays a role in working on cybersecurity as an active agent in cyberspace.

1. Development and Assurance of Cybersecurity Human Resource

- Training and adoption at the “strategic management level”
- Training for the operational and expert level
- Preparing a foundation for development of cybersecurity human resource, Promoting international partnership
- Strengthening the assurance and development of cybersecurity human resource at agencies

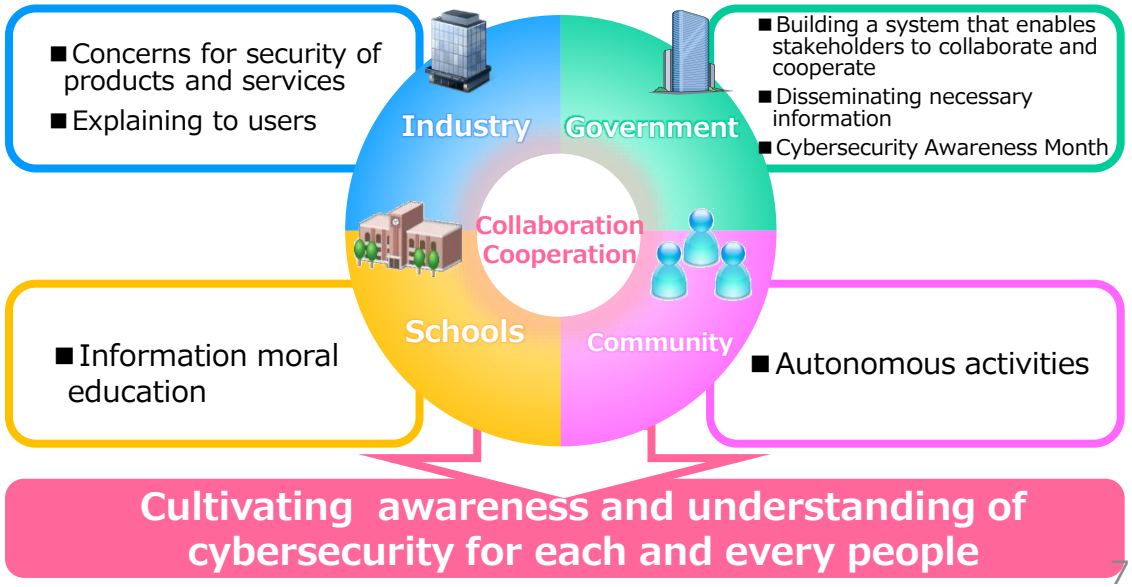


2. Advancement of Research and Development

- Promoting practical R&D (Increasing ability to detect and analyze cyberattacks, and developing a system for carrying out the necessary technical inspections of malicious programs)
- Responses with a view to the mid- and long-term evolution of technology and society

3. Collaboration by Everyone who is the Main Player in Cybersecurity

- Developing action plan for public awareness on cybersecurity and coordination/collaboration
- Disseminating necessary information (enhancing Cybersecurity Awareness Month)



Implementation Framework

○The Government has been promoting a policy of improving cybersecurity measures to secure the use and application of information and communications technologies and data as the socio-economic foundation of society and to ensure Japan's national security. the related government bodies will keep working on improving their cybersecurity capabilities under the leadership of NISC, secretariat of the Cybersecurity Strategy Headquarters, and NISC will play its leading role as the focal point in coordinating intra-government collaboration and promoting partnerships between industry, academia, and the public and private sectors.
○ The Headquarter will seek to secure and execute the budget necessary for the government so that the measures are steadily and effectively executed. The Cybersecurity Strategic Headquarters will set forth annual plans including the list of Agencies in charge.

Cabinet

Prime Minister

IT Strategic Headquarters

IT Strategic Headquarters swiftly and thoroughly introduces the measures for the formation of an advanced information and telecommunications network society.

Cooperation

Cybersecurity Strategic Headquarters

Chair: Chief Cabinet Secretary
Deputy Chair: Minister in charge of the Tokyo Olympic and Paralympic Games
Members:
Chairman of the National Public Safety Commission
Minister for Internal Affairs and Communications
Minister for Foreign Affairs
Minister of Economy, Trade and Industry
Minister of Defense
Minister in charge of Information Technology Policy
Experts (7 persons)

- Critical Infrastructure Expert Panel
- Technological Strategy Expert Panel
- Human Resources Expert Panel for Dissemination and Enlightenment
- Cybersecurity Measures Promotion committee

Cooperation

National Security Council (NSC)

NSC deliberates on important issues regarding national defense.

Competent Ministries of Critical Infrastructures

・Financial Services Agency
・Ministry of Internal Affairs and Communications
・Ministry of Health, Labour and Welfare
・Ministry of Economy, Trade and Industry
・Ministry of Land, Infra, Transport and Tourism

Cooperation

Secretariat

National Center of Incident Readiness and Strategy for Cybersecurity (NISC)

・Director-General ・Deputy Director-General

- GSOC
- CYMAT

Cooperation

Ministries under HQ Members

・National Police Agency
・Ministry of Internal Affairs and Communications
・Ministry of Foreign Affairs
・Ministry of Economy, Trade and Industry
・Ministry of Defense

Relevant Ministries

・Ministry of Education, Culture, Sports, Science and Technology (Security education)

Critical infrastructure businesses, etc. 

Government organizations (Ministries, IAAs, Designated Special Corporations) 

Companies  Individuals