NISC

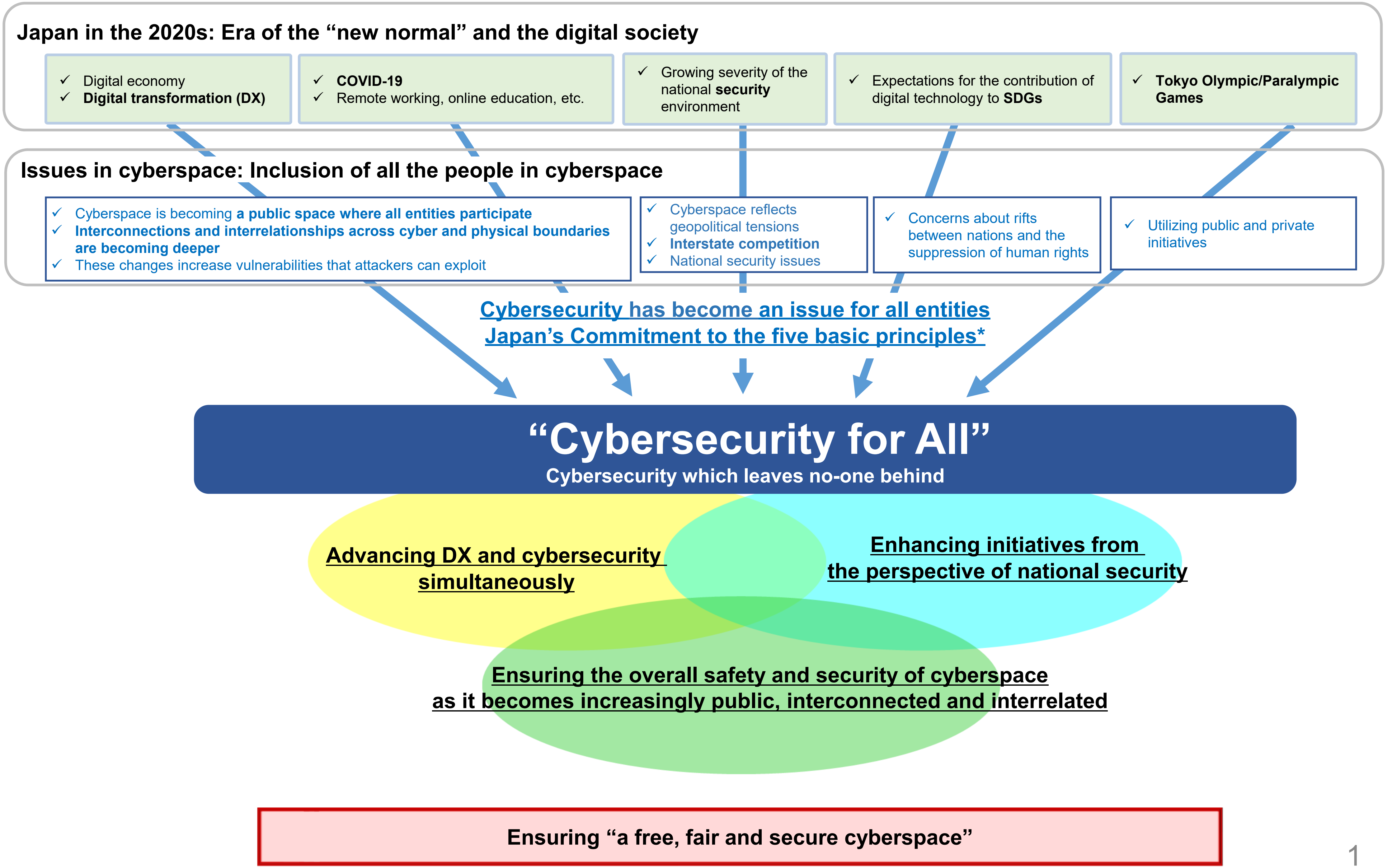
National center of Incident readiness and Strategy for Cybersecurity

Japan's Cybersecurity Strategy 2021 (Overview)

National center of Incident readiness and Strategy for Cybersecurity (NISC)

As of September 28, 2021

Issues and Direction of Japan’s Cybersecurity Strategy 2021



Japan in the 2020s: Era of the “new normal” and the digital society

- ✓ Digital economy
- ✓ **Digital transformation (DX)**

- ✓ **COVID-19**
- ✓ Remote working, online education, etc.

- ✓ Growing severity of the national **security** environment

- ✓ Expectations for the contribution of digital technology to **SDGs**

- ✓ **Tokyo Olympic/Paralympic Games**

Issues in cyberspace: Inclusion of all the people in cyberspace

- ✓ Cyberspace is becoming **a public space where all entities participate**
- ✓ **Interconnections and interrelationships across cyber and physical boundaries are becoming deeper**
- ✓ These changes increase vulnerabilities that attackers can exploit

- ✓ Cyberspace reflects geopolitical tensions
- ✓ **Interstate competition**
- ✓ National security issues

- ✓ Concerns about rifts between nations and the suppression of human rights

- ✓ Utilizing public and private initiatives

Cybersecurity has become an issue for all entities

Japan’s Commitment to the five basic principles*

“Cybersecurity for All”

Cybersecurity which leaves no-one behind

Advancing DX and cybersecurity simultaneously

Enhancing initiatives from the perspective of national security

Ensuring the overall safety and security of cyberspace as it becomes increasingly public, interconnected and interrelated

Ensuring “a free, fair and secure cyberspace”

* Assuring the free flow of information, the rule of law, openness, autonomy, and collaboration among multi-stakeholders

Enhancing Socio-Economic Vitality and Sustainable Development

Issues and direction—Advancing digital transformation and cybersecurity simultaneously

● The Digital Agency was established in September of this year. This is a great opportunity to advance DX.
To this end, it is important to build trust in cyberspace, which leads to participation and commitment by all the people and businesses.

● As operations, products, and services become increasingly digitalized, ensuring cybersecurity will be directly linked to corporate value. "Security by design" will become ever more important, and digital investments and security measures will likely become increasingly integrated.

⇨ Advance cybersecurity in parallel with digitalization

Specific measures

(1) Raising executive awareness

→Visualize and incentivize initiatives based on the guidelines of cybersecurity management, and further promote such initiatives, by implementing guidelines for digital management.

(2) Advancing DX with Cybersecurity among local regions and SMEs

→Address the shortage of knowledge and human resources required for digitalization, through the development of local regions and the establishment of a registration scheme for services targeting SMEs.

(3) Building a foundation for ensuring trustworthiness of supply chains

→Advance initiatives based on the frameworks which respond to Society5.0.

－ Supply chains: Industry-led consortium
－ Data Flow: Definition of data management, securing the reliability of data with "trust service"
－ Security products/services: Promotion of third-party verification services
－ Advanced technology: Building a common foundation for collecting, accumulating, analyzing, and providing information

(4) Advancing and broadening digital/security literacy with no one left behind

→Advance initiatives which provide assistance in the use of digital technology, along with efforts to drive information education.

Realizing a Digital Society where the People can Live with a Sense of Safety and Security

Issues and direction—Ensuring the overall safety and security of cyberspace as it becomes increasingly public, interconnected and interrelated

● Cyberspace becoming **increasingly public, interconnected and interrelated, and cyberattacks becoming more organized and sophisticated**.

➡ The national government, in cooperation with various stakeholders, will take **a comprehensive and multilayered approach to cybersecurity, which is based on self-help, mutual help and public help**, and which reduces risks and increases resilience for the entire country. This will be done mainly by (1) **creating an environment where risk is managed autonomously** through self-help and mutual help, and by (2) **deploying comprehensive cyber defense** using all available means.

Specific measures (1) Providing a cybersecurity environment which protects the people and society

(1) Ensure safety and security in cyberspace

- Establish guidelines and encourage industry-led efforts for supply chain management, and ensure safety when implementing new technologies (IoT, 5G, etc.)
- Study measures for ensuring safe and reliable telecommunications networks to protect users

(2) Cooperate with new providers of cybersecurity (accommodate cloud services)

- Create security rules for government agencies, critical infrastructure operators, etc. to consider when using cloud
- Promote cloud usage that ensures a measure of security through private-sector efforts, such as the ISMAP initiative
- Advance the development of high-quality cloud that is reliable, open and user friendly

(3) Address cybercrimes

- Actively point out criminals exploiting cyberspace or malicious business operators who provide criminal infrastructure blocking traceability for ensuring a sense of security and safety
- Strengthen police capabilities for responding to cyber incidents

(4) Deploy comprehensive cyber defense

- Enhance the functions of national CERTs/CSIRTs, which handle general coordination of integrated advancement from response to cyberattacks to policy measures, including prevention of recurrence (marshal resources and strengthen collaboration of responsible government agencies, enhance public-private partnership by working with the Cybersecurity Council and other relevant agencies and international collaboration)
- Establish an environment for comprehensive cyber defense (vulnerability handling, technical verification mechanism, and establishing functions for investigating the cause of relevant industrial control system incidents, etc.)

(5) Ensure trustworthiness of cyberspace

- Support stakeholders who possess personal information and intellectual property
- Ensure trustworthiness of IT systems and services from the perspective of economic security (government procurement, critical infrastructure, international submarine cables, etc.)

Realizing a Digital Society where the People can Live with a Sense of Safety and Security

Specific measures (2) Ensuring cybersecurity integral with digital transformation (led by the Digital Agency)

- Propose and implement the basic principle for cybersecurity in the Digital Agency's development policy for the information systems of the national government, etc..
- Plan systems which ensure the authenticity of information and its provider, and promote their utilization. Implement the ISMAP system and encourage its use by the private sector.

Specific measures (3) Promoting efforts by stakeholders which underpin the foundations of the economy and society

(1) Government agencies, etc.

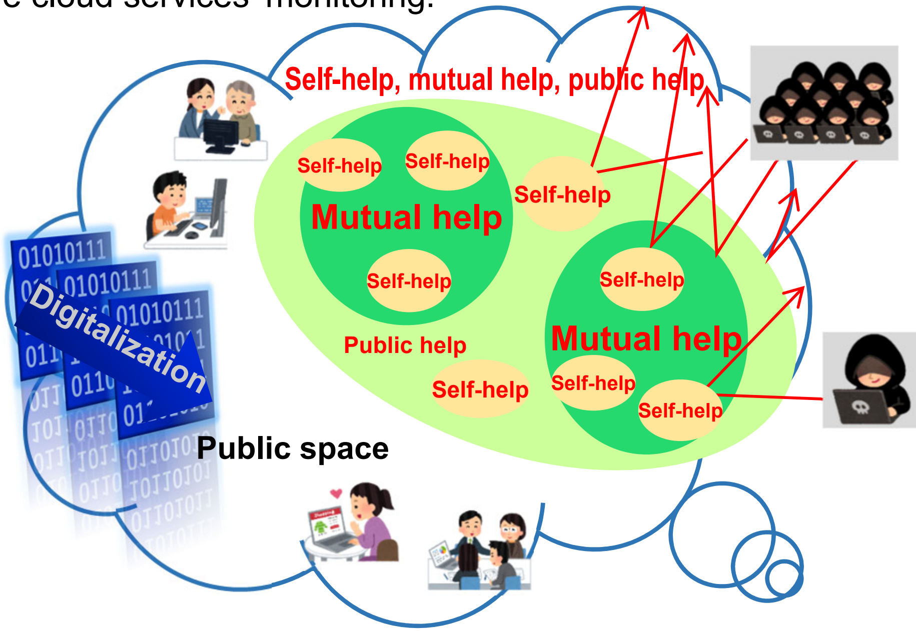
- Advance measures based on the Common standards for Governmental Agencies and Related Agencies, and increase the overall security level of government agencies through efforts including security audits, CSIRT training and monitoring by GSOC.
- Promote the revision and implementation of the Common standards for Governmental Agencies and Related Agencies in accordance with the expanding use of cloud services and enhance the GSOC functions to enable cloud services' monitoring.

(2) Critical infrastructure

- Revise the "Cybersecurity Policy for Critical Infrastructure Protection (4th Edition)," and advance reinforcement and management leadership in response to environmental changes.
- Update guidelines and advance efforts to establish necessary systems in response to standardization of local government information systems, handling administrative procedures online, etc.

(3) Universities, education and research institutions, etc.

- Seminars and training on risk management and incident response, supporting enhanced measures at universities, etc. possessing advanced information, including measures against supply chain risks, and so on.



Specific measures (4) Seamless information sharing and collaboration by multiple stakeholders and enhancement of readiness to respond to massive cyberattacks, etc.

- Actively use findings and know-how obtained through response capabilities and operation at the Tokyo Games to support business operators, etc. nationwide.
- Strengthen seamless and whole of nation response capabilities, keeping in mind even in peacetime the possibility that a minor incident may escalate into a major cyberattack.

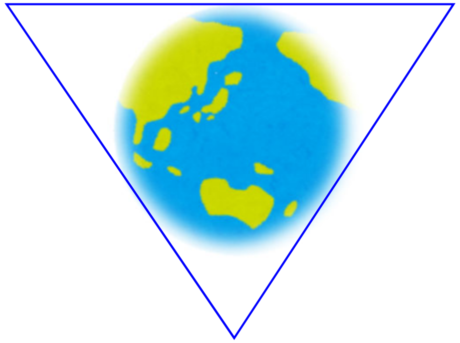
Issues and direction—Enhancing initiatives from the perspective of national security

- Amidst the growing severity of the security environment surrounding Japan, cyberspace has become an realm of interstate competition that reflects geopolitical tensions. China, Russia and North Korea are presumed to be building cyber capabilities and conducting cyberattacks intended to steal information, etc..
- Meanwhile, Japan’s ally and like-minded countries have been accelerating efforts to build the capabilities of their cyber commands and strengthen the ability to respond to cyberattacks, and they are collaborating to address cyber incidents and conflicts over international rules in cyberspace in particular.
- In addition, as national security has been expanding its scope to include economic and technological fields, Japan must also collaborate with its ally and like-minded countries to address conflicts over technological foundation concerning cyberspace and data, on which Japan must also establish international rules in line with its basic principles to ensure “a free, fair and secure cyberspace.”

⇨ To ensure safety and security of cyberspace, Japan will place a higher priority on cyber issues in diplomatic and national security agenda, and Japan also commits to the following.

Ensuring “a free, fair and secure cyberspace”

International cooperation and collaboration



Strengthening Japan’s capabilities for defense, deterrence, and situational awareness

Contribution to the Peace and Stability of the International Community and Japan’s National Security

Specific measures

(1) Ensuring a free, fair and secure cyberspace

- Promoting the rule of law in cyberspace (formulating rules that contribute to Japan’s national security)
  - Promote discussions on the application of international law and the practice of norms, and advance the universalization of the Convention on Cybercrime, etc.
- Formulating rules in cyberspace
  - Formulate international rules in line with Japan’s basic principles, based on the progress of international efforts including Data Free Flow with Trust (DFFT), 5G security, etc.

(2) Strengthening Japan’s capabilities for defense, deterrence, and situational awareness

- Increasing defense capabilities
  - Fundamentally strengthen the cyber defense capabilities of the Ministry of Defense and the Self-Defense Forces (SDF), and conduct exercises and other measures by the SDF and US military to defend infrastructure.
  - Strengthen public-private collaboration and information sharing to ensure security of advanced technology, the defense industry, etc.
- Enhancing deterrence capabilities
  - Employ capabilities to disrupt opponents’ use of cyberspace for attack, use diplomatic means and criminal prosecution, and maintain and strengthen the Japan-US alliance
- Strengthening cyber situational awareness capabilities
  - Advance efforts to further clarify the actual situation of cyberattacks by leveraging the nationwide networks, technical teams and human intelligence

(3) International cooperation and collaboration

- Sharing expertise and coordinating policy
  - Strengthen multi-layered frameworks for international collaboration within and across ministries and agencies, with like-minded countries including the US, Australia, and India as well as ASEAN
- Strengthening international collaboration for incident response
  - Enhance Japan’s international presence by leading international cyber exercises, etc.
- Supporting for capacity building
  - Enhance efforts in the Indo-Pacific region, including ASEAN, such as industry-academia-government collaboration, diplomacy and national security based on the Basic Policy on Cybersecurity Capacity Building for Developing Countries.

Cross-Cutting Approaches to Cybersecurity

Advance DX and cybersecurity simultaneously

Ensure the overall safety and security of cyberspace as it becomes increasingly public, interconnected and interrelated

Enhance initiatives from the perspective of national security

- Taking a cross-cutting, medium- to long-term view, promote R&D, development of human resources, and awareness-raising activities in order to advance the above.

1. Promotion of R&D

Build a government-industry-academia ecosystem, and pursue practical R&D using that as a foundation.
Take medium- to long-term technological trends into consideration.

(2) Advance practical R&D

(1) Address supply chain risks

(2) Cultivate/develop domestic industries

(3) Foundations for monitoring, analyzing, and sharing attacks

(4) Advance research of cryptography, etc.

(1) Strengthen international competitiveness Build a government-industry-academia ecosystem

- Leverage measures to promote research and government-industry-academia collaboration
- Enhance research environment, etc.

(3) Take medium- to long-term technological trends into consideration

(1) Advancement of AI technology
AI for Security
Security for AI

(2) Advancement of quantum technology
Post-quantum cryptography
Quantum communications/cryptography

2. Recruitment, development, and active use of human resources

Maintain the quality and quantity of initiatives by public and private sectors, with a focus on efforts to address environmental changes. Create an environment that enables career development spanning both public and private sectors.

(1) Advance DX with Cybersecurity

- Create an environment where people can gain additional security knowledge
- Promote practices which encourage function building and staff mobility, etc. (xSIRT, side/concurrent business, etc.)

(2) Address increasingly sophisticated and complex threats

- Strengthen human resources development programs
SecHack365/CYDER/enPiT
ICSCoE Core Human Resource Development Program, etc.
- Build a common foundation for human resources development and make it available to industry and academia
- Promote the use of qualification systems, etc.

Create an environment that enables talented human resources to develop careers which span the private sectors, municipalities, and national government agencies

(3) Pursue government agency initiatives

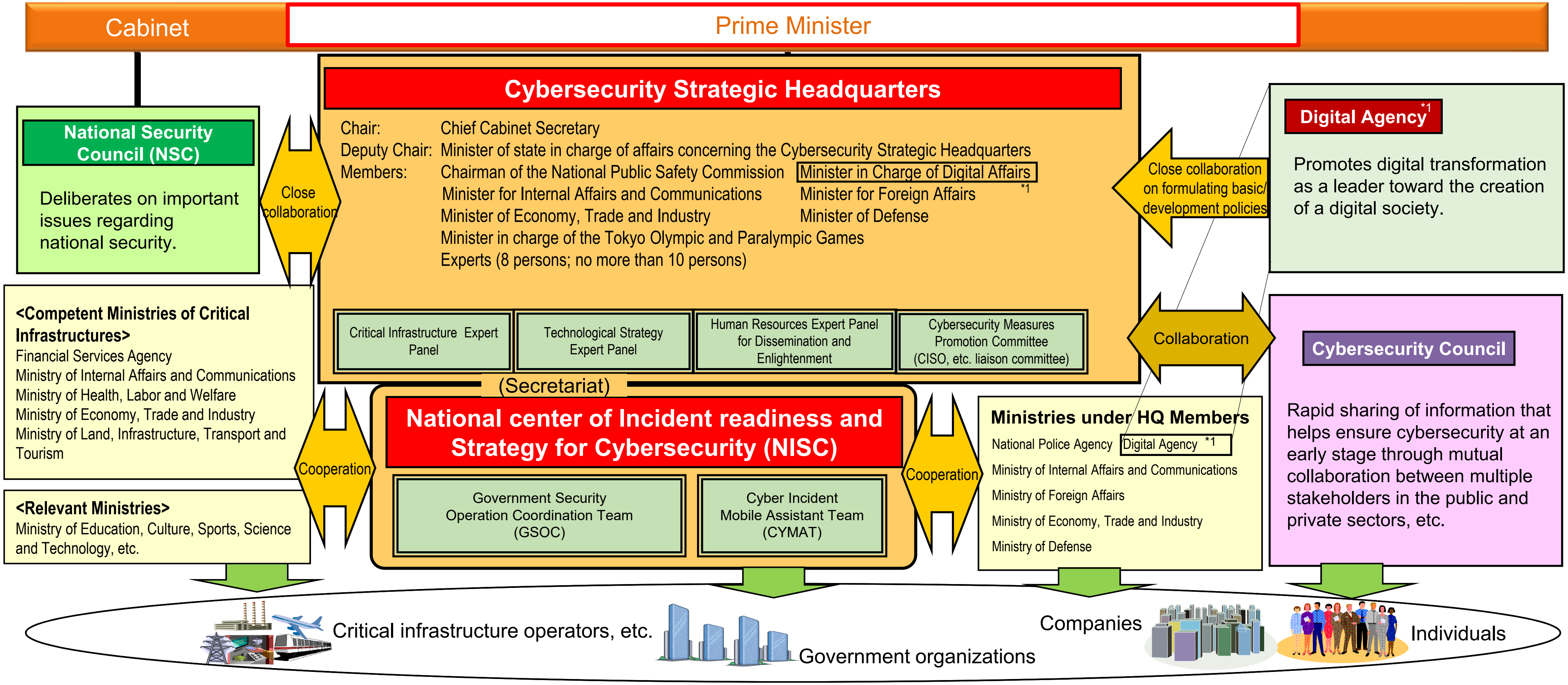
- Strengthen systems for enlisting the help of advanced outside experts
- Promote recruitment of successful candidates from the “digital division” experts
- Enhance training

3. Collaboration based on full participation and awareness raising

Improve and review action plans considering progress of digitalization, including support for the elderly.

Implementation Framework

- A concerted effort by the whole of government is needed to promote and implement cybersecurity policy in order to ensure a free, fair and secure cyberspace in line with Japan's cybersecurity policies. Further efforts will be made to strengthen the capabilities and collaboration of relevant agencies so that they can contribute to the digital transformation led by the Digital Agency, and leverage their limited resources to fulfill their roles.
- NISC and relevant ministries and agencies must work together to actively communicate this strategy to stakeholders both in Japan and abroad, in order to encourage each stakeholder to take practical actions, and further understanding by foreign governments of Japan's stance and enhance deterrence against attackers with the importance of international cooperation in mind.
- To enable comprehensive response by the whole of government against cyberattacks, the Cybersecurity Strategic Headquarters will improve a national CERTs/CSIRTs framework.
- Annual reports and plans should be discussed in an integrated manner, and activities for the next year aligned with the results and evaluation of the previous year's activities, in order to develop a cohesive flow of activity which is in line with the strategy.



Cabinet

Prime Minister

Cybersecurity Strategic Headquarters

Chair: Chief Cabinet Secretary

Deputy Chair: Minister of state in charge of affairs concerning the Cybersecurity Strategic Headquarters

Members: Chairman of the National Public Safety Commission; Minister in Charge of Digital Affairs [*1]; Minister for Internal Affairs and Communications; Minister for Foreign Affairs; Minister of Economy, Trade and Industry; Minister of Defense; Minister in charge of the Tokyo Olympic and Paralympic Games; Experts (8 persons; no more than 10 persons)

Critical Infrastructure Expert Panel

Technological Strategy Expert Panel

Human Resources Expert Panel for Dissemination and Enlightenment

Cybersecurity Measures Promotion Committee (CISO, etc. liaison committee)

National Security Council (NSC)

Deliberates on important issues regarding national security.

Close collaboration

Digital Agency[*1]

Promotes digital transformation as a leader toward the creation of a digital society.

Close collaboration on formulating basic/development policies

Collaboration

Cybersecurity Council

Rapid sharing of information that helps ensure cybersecurity at an early stage through mutual collaboration between multiple stakeholders in the public and private sectors, etc.

(Secretariat)

National center of Incident readiness and Strategy for Cybersecurity (NISC)

Government Security Operation Coordination Team (GSOC)

Cyber Incident Mobile Assistant Team (CYMAT)

Cooperation

Cooperation

<Competent Ministries of Critical Infrastructures>

Financial Services Agency

Ministry of Internal Affairs and Communications

Ministry of Health, Labor and Welfare

Ministry of Economy, Trade and Industry

Ministry of Land, Infrastructure, Transport and Tourism

<Relevant Ministries>

Ministry of Education, Culture, Sports, Science and Technology, etc.

Ministries under HQ Members

National Police Agency

Digital Agency [*1]

Ministry of Internal Affairs and Communications

Ministry of Foreign Affairs

Ministry of Economy, Trade and Industry

Ministry of Defense

Critical infrastructure operators, etc.

Government organizations

Companies

Individuals

(*1) Basic Act on Creation of a Digital Society (Act No. 35 of 2021), Act for Establishment of the Digital Agency (Act No. 36 of 2021). (effective since September 1, 2021)

Outline of the Cybersecurity Strategy 2021

Medium and Long Term

1 Japan in the 2020s

1-1 Establishment of the digital economy and promotion of digital transformation, expectations for contribution to SDGs, changing national security environment, impact and experience of COVID-19, and application of efforts toward the Tokyo Games.

2 Basic principles of the strategy

2-1 Ensuring a cyberspace which is “free, fair and secure”

2-2 The basic principles adhere to the 5 principles set forth in the previous strategies (assurance of the free flow of information, the rule of law, openness, autonomy, and collaboration among multiple stakeholders)

3 Issues surrounding cyberspace

Risks from the perspective of environmental changes, risks from the perspective of international affairs, and recent trends of threats in cyberspace

Strategy Period

4 Policy approaches

<Three directions> (1) Advancing digital transformation and cybersecurity simultaneously
(2) Ensuring the overall safety and security of cyberspace as it becomes increasingly public, interconnected and interrelated
(3) Enhancing initiatives from the perspective of Japan’s national security

Enhancing Socio-Economic Vitality and Sustainable Development

1. Raising executive awareness
2. Advancing DX with Cybersecurity among local regions and SMEs
3. Building a foundation for ensuring trustworthiness of supply chains that support new value creation
4. Advancing digital/security literacy with no one left behind

Realizing a Digital Society where the People can Live with a Sense of Safety and Security

1. Providing a cybersecurity environment which protects the people and society
2. Ensuring cybersecurity integral with digital transformation (led by the Digital Agency)

3, 4, 5. Promoting efforts by stakeholders which underpin the foundations of the economy and society
(1) Government agencies, etc.
(2) Critical infrastructure
(3) Universities, education and research institutions, etc.

6. Seamless information sharing and collaboration by multiple stakeholders and application of knowledge gained through efforts toward the Tokyo Games, etc.
7. Enhancement of readiness to respond to massive cyberattacks, etc.

Contribution to the Peace and Stability of the International Community and Japan’s National Security

1. Ensuring “a free, fair and secure cyberspace”
2. Strengthening Japan’s capabilities for defense, deterrence, and situational awareness
3. International cooperation and collaboration

Cross-Cutting Approaches to Cybersecurity

Promotion of R&D

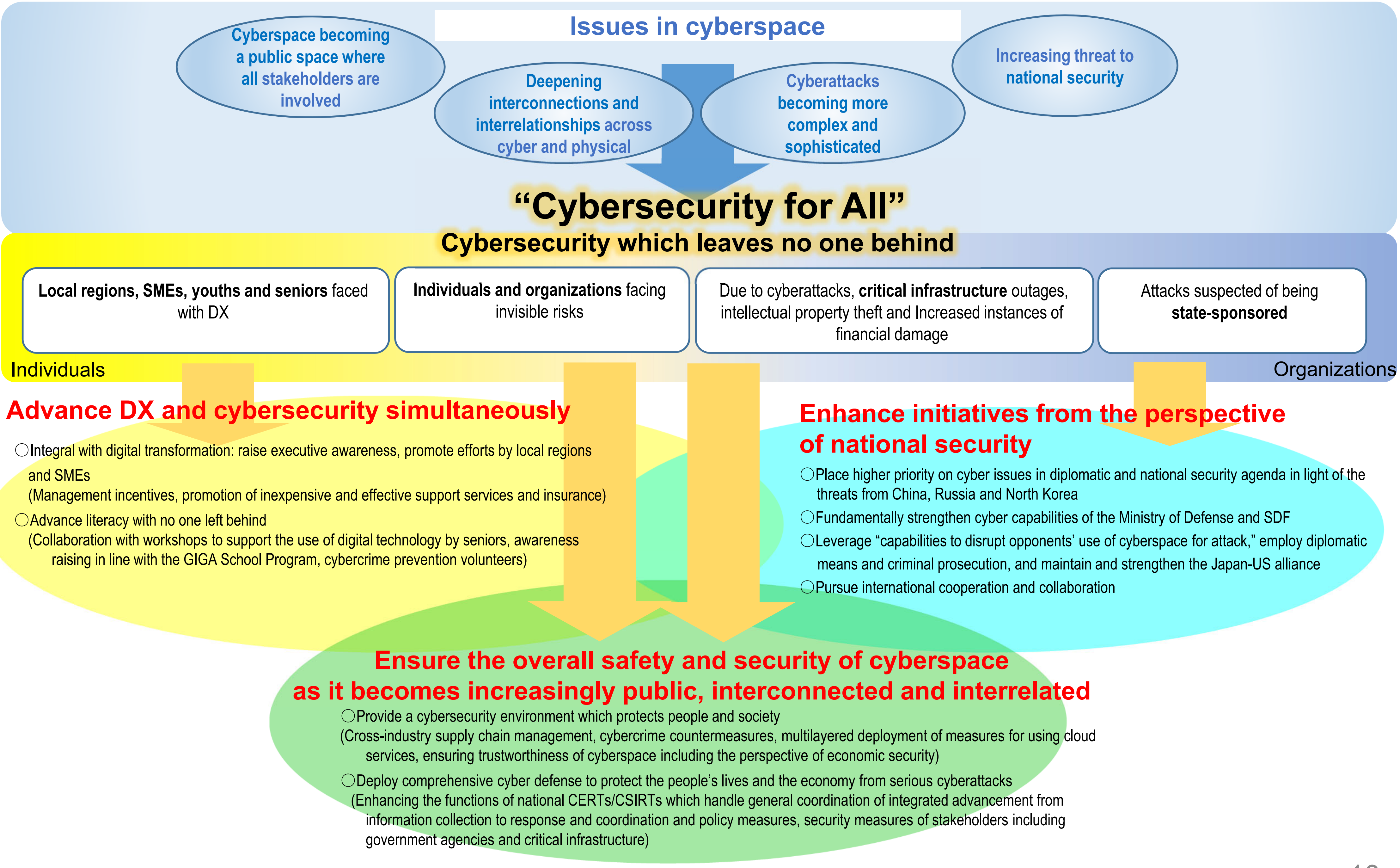
Recruitment, development, and active use of human resources

Collaboration based on full participation and awareness raising

5 Implementation Framework

A concerted effort by the whole of government to ensure “a free, fair and secure cyberspace”

Enhancement of Efforts to Achieve “Cybersecurity for All”



Issues in cyberspace

- Cyberspace becoming a public space where all stakeholders are involved
- Deepening interconnections and interrelationships across cyber and physical
- Cyberattacks becoming more complex and sophisticated
- Increasing threat to national security

“Cybersecurity for All”

Cybersecurity which leaves no one behind

- **Local regions, SMEs, youths and seniors** faced with DX
- **Individuals and organizations** facing invisible risks
- Due to cyberattacks, **critical infrastructure** outages, intellectual property theft and Increased instances of financial damage
- Attacks suspected of being **state-sponsored**

Advance DX and cybersecurity simultaneously

〇Integral with digital transformation: raise executive awareness, promote efforts by local regions and SMEs
(Management incentives, promotion of inexpensive and effective support services and insurance)

〇Advance literacy with no one left behind
(Collaboration with workshops to support the use of digital technology by seniors, awareness raising in line with the GIGA School Program, cybercrime prevention volunteers)

Enhance initiatives from the perspective of national security

〇Place higher priority on cyber issues in diplomatic and national security agenda in light of the threats from China, Russia and North Korea

〇Fundamentally strengthen cyber capabilities of the Ministry of Defense and SDF

〇Leverage “capabilities to disrupt opponents’ use of cyberspace for attack,” employ diplomatic means and criminal prosecution, and maintain and strengthen the Japan-US alliance

〇Pursue international cooperation and collaboration

Ensure the overall safety and security of cyberspace as it becomes increasingly public, interconnected and interrelated

〇Provide a cybersecurity environment which protects people and society
(Cross-industry supply chain management, cybercrime countermeasures, multilayered deployment of measures for using cloud services, ensuring trustworthiness of cyberspace including the perspective of economic security)

〇Deploy comprehensive cyber defense to protect the people’s lives and the economy from serious cyberattacks
(Enhancing the functions of national CERTs/CSIRTs which handle general coordination of integrated advancement from information collection to response and coordination and policy measures, security measures of stakeholders including government agencies and critical infrastructure)