CYBERSECURITY STRATEGY





The Government of Japan

September 2015

OVERVIEW

1 Understanding on Cyberspace

- Cyberspace is an artificial domain as a "frontier generating infinite values" and an essential foundation of Japan's socio-economic activities.
- The emergence of an **"interconnected and converged information society"** where all kinds of "things" are networked and the integration of cyberspace and physical space has become intensified.
- Increasing damage from and social impact of cyber attacks.
- Anticipated further aggravation of cyber threats.

2 Visions and Objective

Ensure a free, fair, and secure cyberspace; and subsequently contribute to:

- Improving socio-economic vitality and sustainable development
- Building a society where the people can live safe and secure lives, and
- Ensuring peace and stability of the international community and national security

3 Basic Principles

(1)Assurance of the Free Flow of Information (2)The Rule of Law
(3)Openness (4)Autonomy (5)Collaboration among Multi-stakeholders

4 Policy Approaches towards Achieving the Objective

(1)Being proactive, not reactive.
(2)Acting as a catalyst, not just a passive player.
(3)Envisaging cyber-physical space, not cyberspace alone.

Improving Socio-Economic Vitality and Sustainable Development

"Cybersecurity is not a cost, but an investment"

- Creation of Secured Internet of Things (IoT) Systems
- Promotion of Enterprise Management with a Security Mindset
- Improvement of Cybersecurity Business Environment

Building a Safe and Secure Society for the People

"Development of cybersecurity infrastructure for 2020 and further"

- Measures for the Protection of the People and Society
- Measures for Critical Information Infrastructure Protection
- Measures for the Protection of Governmental Bodies

Ensuring Peace and Stability of the International Community and National Security

"Proactive contribution to peace in cyberspace"

- Ensuring National Security
- Maintaining Peace and Stability of the International Community
- Cooperation and Collaboration with Countries around the World

Cross-Cutting Approaches to Cybersecurity

- **Advancement of Research and Development (R&D)**
  Promoting R&D to advance detection and defense capabilities against cyber attacks
- **Development and Assurance of Cybersecurity Workforce**
  Developing "hybrid" human resources; conducting practical exercises; discovering the best brains; building long term career paths

5 Promotion and Implementation of Cybersecurity

- Strengthening coordination and collaboration among industries, academia, and the public sector, in addition to relevant governmental bodies.
- Ensuring cybersecurity for the Games of the XXXII Olympiad and the Tokyo 2020 Paralympic Games (Tokyo 2020), etc.

GENERAL ISSUES

Looking towards the Tokyo 2020 and the prospects further ahead for the early 2020s, this strategy outlines the basic directions of Japan's cybersecurity policies for the coming three years approximately.

1 Understanding on Cyberspace

●Significant Benefits:

- Free exchange of ideas without being constrained by national borders
- Infinite values generated by intellectual creations and innovations inspired by the ideas globally exchanged
- Essential foundation for Japan's socio-economic activities

●IT "Diastrophism" Provoked by Information and Communications Technologies Evolution:

With the arrival of the interconnected and converged information society where physical space and cyberspace have become highly integrated, all kinds of physical objects and people have become interconnnected without physical constraints.

●Increasing Cyber Threats:

Cyber threats have become a critical challenge to national security, having caused significant damages on the people's daily lives and economic activities. Japan will be certainly exposed to more serious cyber threats in the future.

2 Visions and Objective

●Ensure a free, fair, and secure cyberspace; and subsequently contribute to:

- ●Improving socio-economic vitality and sustainable development
- ●Building a society where the people can live safe and secure lives, and
- ●Ensuring peace and stability of the international community and national security

3 Basic Principles

Japan affirms the following basic principles in policy planning and its implementation for reaching the strategic objective.

(1) Assurance of the Free Flow of Information
(2) The Rule of Law
(3) Openness
(4) Autonomy
(5) Collaboration among Multi-stakeholders

In line with these five principles, and to protect the people's safety, security, and rights, Japan reserves, as options, all viable and effective measures, i.e. political, economic, technological, legal, diplomatic, and all other feasible means.

SPECIFIC ISSUE 1

Improving Socio-Economic Vitality and Sustainable Development

"Cybersecurity is not a cost, but an investment"

Creation of Secured Internet of Things (IoT) Systems

- Promoting new business harnessing the secured IoT systems with the idea of "Security by Design."
- Improving structural frameworks coordinated by the Cybersecurity Strategy HQs for large scale IoT systems security businesses.
- Establishing comprehensive guidelines for IoT systems security in the energy, automotive, and medical industries, etc.
- Implementing technological development and demonstration in consideration of IoT systems characteristics and hardware authenticity, etc.

Promotion of Enterprise Management with a Security Mindset

- Building a framework for stakeholders, such as the market, to evaluate appropriately enterprises' efforts to address cybersecurity.
- Increasing the variety of layers of intermediators to facilitate communication between senior executives and cybersecurity professional.
- Expanding networks in the private sector and between the public-private sectors to share information on cyber threats and incidents.

Demonstration experiment of self-driving cars

Improvement of Cybersecurity Business Environment

- Promoting cybersecurity-related businesses by using sovereign wealth funds, etc.
- Promoting effective security audit for the utilization of cloud services by SMEs, etc.
- Reexamining the existing mechanisms to promote cybersecurity-related businesses.
- Leading international discussions for establishing international standards and frameworks of mutual recognition.
- Implementing measures to develop a fair business environment, such as advanced intellectual property protection.

SPECIFIC ISSUE 2

Building a Safe and Secure Society for the People

"Development of cybersecurity infrastructure for 2020 and further"

Measures for the Protection of the People and Society

- Promoting the gathering of information on vulnerabilities as well as the coordination and enhancement of the systems for Internet monitoring and cyber attack detection.
- Promoting security measures for general users, such as security alerts and tips.
- Examining measures for security assurance for expanding public Wi-Fi spots, etc.
- Promoting local community-based outreach and awareness raising activities; awareness raising and assistance for SMEs and local governments.
- Enhancing measures to advance cybercrime response and investigative capabilities.

Measures for Critical Information Infrastructure (CII) Protection

- Conducting constant review on the scope of CII and CII operators.
- Enhancing effective and prompt public-private information sharing; promoting inter-governmental coordination and conducting training and exercises.
- For the smooth introduction and operation of the Social Security and Tax Number System (My Number system), taking necessary measures for local governments; enhancing monitoring and oversight mechanisms; and building a monitoring and detection mechanism to supervise national and local systems as a whole.
- Promoting internationally approved third-party certification schemes for industrial control systems, such as smart meters.

Interactive outreach and awareness raising seminar (Cybersecurity Cafe)

Exercises to improve cyber incident response capabilities (CII cross-sectoral exercises)

Measures for the Protection of Governmental Bodies

- Enhancing security assurance through penetration tests; addressing supply chain risks; improving detection and analysis functions; and advancing defense capabilities through defense-in-depth measures, etc.
- Achieving more resilient organizational mechanisms and response capabilities through management audit, risk assessment, etc.
- Establishing and promoting inter-governmental common measures in view of the features of new IT products and services.
- Comprehensively enhancing measures through monitoring, audit, and examination of incorporated administrative agencies and special corporations performing public functions with the governmental bodies.

SPECIFIC ISSUE 3

Ensuring Peace and Stability of the International Community and National Security

"Proactive contribution to peace in cyberspace"

Ensuring National Security

- Enhancing response capabilities, both in quality and quantity, of relevant governmental bodies, such as law enforcement agencies and the Self-Defense Forces (SDF).
- Ensuring cybersecurity to protect Japan's advanced technology (technologies related to outer space, nuclear energy, equipment of SDF, etc.)
- Strengthening the public-private coordination in terms of information sharing, analysis, and response for sustainable provision of services by the governmental bodies, CII operators, etc.

Building Peace and Stability of the International Community

- Contributing actively to the development of international rules and norms regarding cyberspace at the United Nations and in other international settings.
- Cooperating with the international community to tackle international terrorist organizations maliciously using cyberspace.
- Promoting active cooperation for cybersecurity capacity building of other countries.

Japan-ASEAN Cybersecurity Policy Meeting

Cooperation and Collaboration with Countries around the World

- Asia Pacific: Further strengthening and expanding cooperative relationship with ASEAN, and enhancing cooperation and partnerships with regional strategic partners.
- North America: Enhancing close cooperation at every level (Japan-U.S. Cyber Dialogue, Japan-U.S. Policy Cooperation Dialogue on the Internet Economy, Japan-U.S. Cyber Defense Policy Working Group, etc.)
- Europe, Latin America and the Caribbean, Middle East and Africa: Strengthening partnerships with countries sharing common values with Japan.

Meridian Conference 2014 in Japan

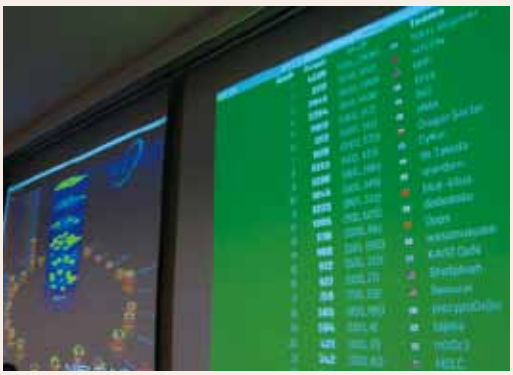
SPECIFIC ISSUE 4

Cross-Cutting Approaches to Cybersecurity

Advancement of Research and Development (R&D)

- Further advancing detection and defense capabilities against cyber attacks by sharing information and data.
- Promoting interdisciplinary research on cybersecurity.
- Protecting cybersecurity core technologies for national security.
- Enhancing R&D in international collaboration by integrating unique technologies of different countries.

Cybersecurity Camp for the youth



Security contest with 58 countries (2014)

Development and Assurance of Cybersecurity Workforce

- Developing multi-talented "hybrid" human resources.
- Promoting industry-academia-public collaboration and practical exercises in higher education.
- Expanding elementary and secondary education for cybersecurity.
- Developing a cloud environment for cyber exercises and supporting educational material development through industry-academia-public partnerships.
- Discovering and acquiring the best brains as global players by supporting international contest events, etc.
- Developing qualification schemes to evaluate practical skills and establishing the standards of basic skills, etc.

Promotion and Implementation of Cybersecurity

- Strengthening detection, analysis, decision-making, and response functions through the further enhancement of NISC's response capabilities and enhanced coordination and collaboration among industries, academia, and the public sector, in addition to relevant governmental bodies.
- Develop close coordination and collaboration among the Cybersecurity Strategic Headquarters, the National Security Council, and a headquarters for emergency response to terrorism, to respond to highly sophisticated cyber attacks that might be state-sponsored.
- Towards the Tokyo 2020, clearly identifying risks; building and maintaining organizations, facilities, and cooperative relationships; and conducting comprehensive training.

The Cybersecurity HQs will formulate an annual plan and an annual report for each fiscal year, and establish a budget prioritization policy.

The Government of Japan