International Journal of Security and Its Applications
Vol. 10, No. 10 (2016) pp.37-46
http://dx.doi.org/10.14257/ijsia.2016.10.10.05

An Analytic Study of Cyber Security Strategies of Japan

Kyoungsik Min[1] and Seung-Woan Chai[2*]

[1,2]*Korea Internet & Security Agency, Seoul, Korea*
[1]*kyoungsik@kisa.or.kr,* [2]*chaisw@kisa.or.kr*

Abstract

Japan has recently enacted the Fundamental Act on Cyber Security, taking prompt actions to reinforce the status of the cyber security policy and to organize the implementation system. This kind of change in policy indicates that cyber space does not remain as a field of information restricted to Internet but has become an international field of discussion about economy, society and politics. This study summarizes the change of cyber security policy of Japan, and analyzes the recent changes.

Keywords*: Cyber Security, Information Security, Security policy of Japan*

1. Introduction

As ICT (information and communication technology) has become more widespread and advanced, and as its use and application has evolved, information communication now provides for a basis for all social, economic and cultural activities. Cyberspace is an artificial domain for the free exchange of ideas without being constrained by national borders; it is an intangible frontier of infinite values generated by intellectual creations and innovations inspired by the ideas globally exchanged. Cyberspace, which arose from advancements in ICT, has become an essential platform to support national growth. On the other hand, with our heightened reliance on ICT, increasingly complex and sophisticated cyber-attack techniques and expansion of cyber-attack targets, the degree of cyber threats have become more and more serious. For example, incidents that would paralyze administrative and social functions in the real world represent a real threat. Cyberspace has continued to expand beyond national borders, and its use and application by various entities have grown rapidly. Consequently, associated risks are becoming more severe, widespread and globalized. Now, cyber threats emerge as urgent global challenge facing the international community as a whole.

Having been selected as the host of the 2020 Summer Olympics, Japan is implementing various policies to enhance cyber security. Especially in November 2014, the government enacted the Fundamental Act on Cyber Security, defining the legal concept of cyber security, clarifying the responsibilities and roles of state and local public entities, and establishing the Cyber Security Strategy Headquarters as the control tower for cyber security strategies under the Cabinet Secretariat's office.

In Japan recently, with propagation of smart devices, such as smart phone and smart car, security incidents occur with these devices, and damages are reported from advanced persistent threats (APT) on government authorities, major infrastructures and heavy chemical industrial facilities. The Great East Japan Earthquake in 2011 raised the necessity of response against cyber security accidents occurring due to natural disasters. The latest incident was the APT attack to Japan Pension Service under the Ministry of Health, Labor and Welfare in July 2015, which caused leakage of personal information of 1250 thousand people [1].

* Corresponding Author

ISSN: 1738-9976 IJSIA

So far, Japan has experienced relatively less cyber security incidents than Korea. With a full-scale proliferation and use of Internet of Things (IoT), cloud computing and big data service, however, large-scale cyber security incidents are increasing rapidly in Japan. In this context, Japan is pushing forward a series of changes to reinforce the cyber security policy.

This study describes the development of cyber security policies of Japan, and analyzes the characteristics of change in security policy represented by the recent enactment of the Fundamental Act on Cyber Security. It also examines the details of global cooperation.

2. An Analysis of Cyber Security Policy

Japan's cyber security policy has been changed for the last 15 years at an interval of about 5 years. In the 1st period (2000~2004) the strategies were focused on response against security incidents. In this period, the Information Security Office was established under the Cabinet Secretariat (corresponding to the Prime Minister's Office). To this point, there had been no separate strategy for information security, but information security policy instructions and guidelines were followed under the informatization policy [2].

In the 2nd period (2005~2009), a comprehensive foundation for information security were established. In April 2005, a conference body was established, and the 1st 'Information Security Meeting' was held in July. Also, National Information Security Center (NISC) was established to work out the basic plan for information security and to manage the relevant departments and offices. From this point, the information security policy has been implemented by relevant departments: the Ministry of Internal Affairs and Communications, the Ministry of Economy, Trade and Industry, the Metropolitan Police Department, *etc*. During this period, the goal of Japan's information security policy is to establish the so-called 'Japan Model' of information security based on high quality, reliability, safety and security as the 'global-top establishment of information security' [3].

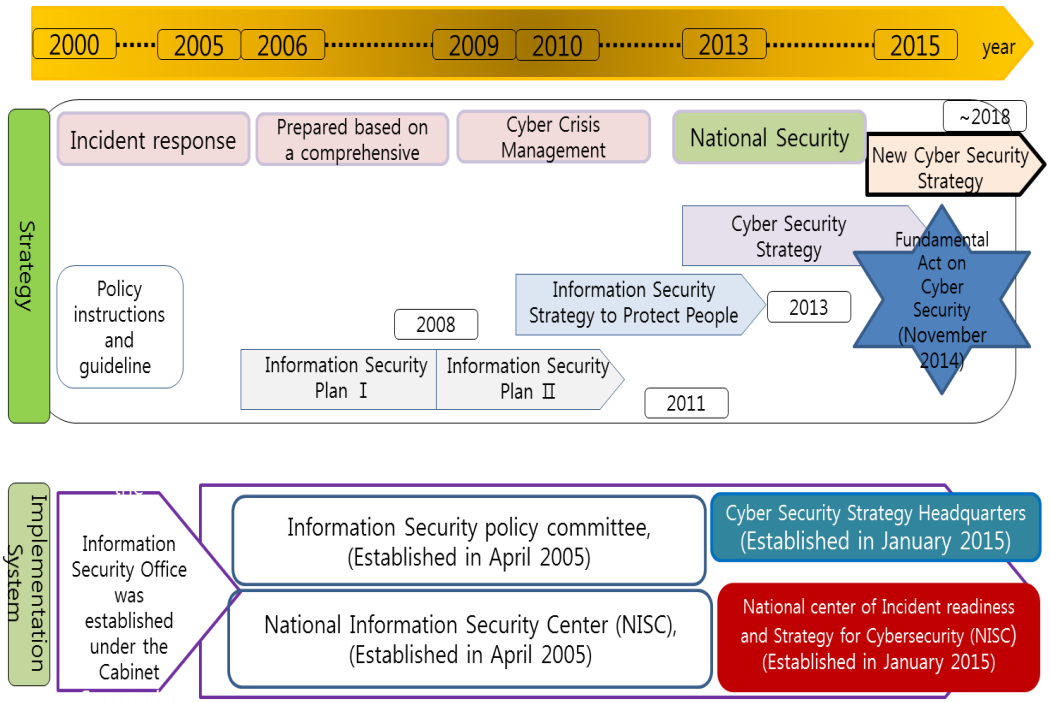

Figure 1. Cyber Security Policy History of Japan

In the 3rd period (2010~2014) the status of the information security policy started to change. Recognizing the increase of influence of information security issues on the overall nation, the Japanese government started to take the national security approach to protection of information. In May 2010, Japan announced the 'Information Security Strategy to Protect People'. With the 'Cyber Security Strategy' released in June 2013, the concept of cyber space started to be discussed. The policy status was reinforced with the establishment of the Fundamental Act on Cyber Security in November 2014.

In the current 4th period (2015~) the Cyber Security Strategy Headquarters was established in accordance with the Fundamental Act on Cyber Security, and the National Information Security Center (NISC) was extended and reorganized to National center of Incident readiness and Strategy for Cybersecurity (NISC). The Japanese government also announced a new reinforced cyber security strategy in September 2015. For this strategy, a safe IoT environment was selected as the key policy goal.

3. An Analysis of the Act on Cyber Security and Change in Policy

Japan has enacted the fundamental law that institutionally backs up the basis of the cyber security system, clarifying its intention to reinforce the cyber security policy. This law defines the basic concept cyber security, the strategies and the responsibilities of the state. It especially defines, in a legal sense, the cyber security as 'the state in which the required measures have been taken to secure safety and reliability of the information system and the IT network, and the state is maintained appropriately' [4]. Japan started discussion on cyber space regularly since 2013. In its National Security Strategy announced in December 2013, it defined the cyber space as the global commons like ocean and space, and stated that threats to free access and use of them were increasing [5]. Due to increasing threats of cyber-attacks aiming at capture of national secret, destruction of infrastructure and interruption of military system, it is required to implement protection of cyber space in a perspective of national security.

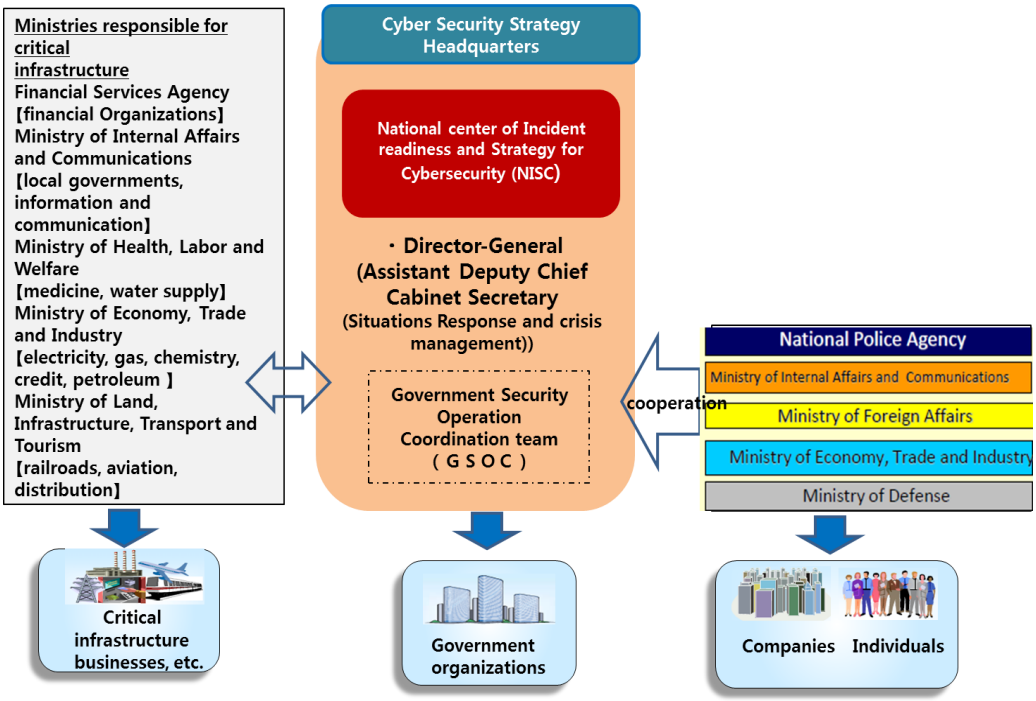

Figure 2. Framework for Cyber Security Policies in Japan

The Fundamental Act on Cyber Security requires the 'Information Security Policy Meeting' which is in charge of cyber security strategy of the Japanese government to be raised to the Cyber Security Strategy Headquarters to play the role of the control tower for cyber security strategies for all the governmental departments. It also requires the National Information Security Center (NISC) which plays the role of secretariat to be reorganized to the National center of Incident readiness and Strategy for Cybersecurity (NISC).

The 2015 cyber security strategy developed based on the Fundamental Act on Cyber Security shows critical changes in policy. Firstly, from countermeasures to proactive approach: This approach requires analysis of social changes or potential hazard, and proactive measures in advance. The philosophy of the information security policy of Japan has been based on the 'society assuming accidents'. This policy is to minimize and localize damages, and to implement the resilient society system, assuming that the information security system is not absolute and that accidents will occur. Japan's information security policy is considered to take a step forward and take more proactive measures.

Secondly, supportive role to leading role: The government enforces the policy to promote private sector's voluntary and active response, and plays the leading role as a member of the global society. The Japanese government's domestic and supportive role is to change to more positive and leading role in implementing policies. Thirdly, from cyber space to convergence space: The Japanese government enforces the policy to respond to the changes to the interconnected and converged information society where the cyber space is converged into the real space. In other words, the government enforces systematically the security policy in preparation for the hyper-connected society led by IoT, cloud and big data.

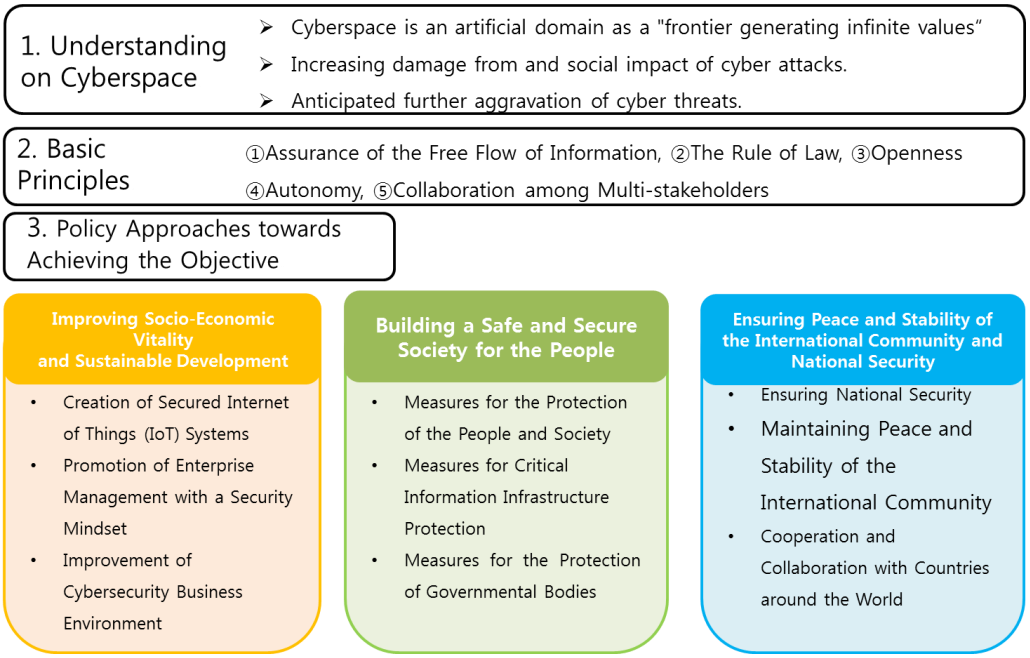

Figure 3. New Cyber Security Strategy of Japan

<Source>: Cyber Security Strategy, The Government of Japan, September 2015.

4. An Analysis of Global Cooperation for Cyber Security

A noticeable point in Japan's cyber security strategy is that the global cooperation was selected as one of the three tasks. In Japan, the necessity of global cooperation was first raised in 2006 with the '1st Basic Plan for Information Security'. It became one of the key tasks in 2013 with the 'Cyber Security Strategy'. Its stature was reinforced with the 'J-initiative for Cybersecurity' announced in the same year. The Japanese government selected the directions of policy for global cooperation: ① Developing the awareness that there are various entities and values coexisting in the cyber space, and that global cooperation is critical in order to secure cyber security (gradual development of global common recognition), ② Contributing positively to fostering of human resources for cyber security and building of information sharing system (reinforcing contribution to the global society), and ③ Utilizing technologies and experience of Japan for countermeasures against cyber-attacks (applying technologies to the global domain).

In order to reinforce the multilateral partnership, Japan holds the regular conference for cyber security policy with USA, UK, India, EU and ASEAN. Security Arrangements is of essential importance for Japan. The Japan-U.S. have built a cooperative relationship to promote various efforts in the areas of policy consultation, information sharing and cyber incident response through such platforms as the Japan-U.S. Cyber Dialogue and the Policy Cooperation Dialogue on the Internet Economy. As for European countries, Japan has also built cooperative relationship to promote various efforts with shared values. For instance, Japan held the bilateral Japan-UK Cyber Dialogue and the Japan-EU Internet Security Forum. Japan also concluded the Convention on Cybercrime adopted by the Council of Europe.

In regions such as South America and Africa, the use and application of cyberspace has also rapidly progressed. As a consequence, a number of cybersecurity issues have surfaced including an increase in malware infections and other cyber threats. Japan has extended cooperation to countries in these regions, such as through provision of support for the establishment of CSIRTs (Computer Security Incident Response Team).

Japan has a close relationship with the Asia Pacific region due to its geographical proximity and close economic ties. Close cooperation with the Asia Pacific region in countering cyber threats is crucial for the region to make united efforts [6].

Within the Asia Pacific region, Japan's relationship with the ASEAN is particularly important given its existing close ties and increased investment by Japanese enterprises in ASEAN countries. ASEAN and Japan have cooperated in ongoing initiatives through the ASEAN-Japan Information Security Policy Meeting, as well as the ASEAN-Japan Ministerial Policy Meeting on Cybersecurity Cooperation. Japan is very enthusiastic in cooperation with ASEAN. This can be understood in the same context that Japan started to classify the East Asian countries as the main cooperation objects since 2005. The East Asian region represented by ASEAN has a close economical relationship with Japan, and is recognized to require reinforcement of strategic relationship in terms of competition with Korea and China [7].

The cyber security policy cooperation conference with ASEAN was started in 2009. The cooperation conference consists of the 'high-level policy conference' for directors and the 'network security workshop' and 'information security practice' for managers and practitioners. In the ministerial conference on cyber security held in September 2013, a mutual agreement was announced for joint measures against cyber-attacks. Japan and ASEAN have agreed on the following cooperative measures [8]:

1) Creating a secure business environment

- Enhancing the level of cyber security in the private sector through the

Information Security Management System (ISMS)
-Promoting cooperation and solidarity between relevant departments through the Computer Security Incident Response Team (CSIRT)

2) Building a secure Information and communication network

-Enhancing the network security through sharing of information on the measures against botnet and spam
-Reinforcing technical cooperation for security through the 'Proactive Response Against Cyber-attacks Through International Collaborative Exchange (PRACTICE)' and 'Direct Alert Environment for Darknet and Livenet Unified Security (DAEDALUS)'

3) Enhancing capacity for cyber security

-Promoting cooperation based on the cyber strategy (including protection of infrastructure, private-public corporation, ICT business sustainability plan, protection of the weak on Internet, cloud computing security and smartphone security)
-Enacting 'Japan-ASEAN Cyber Security Personnel Fostering Initiatives'
-Building the network to promote prompt response and information sharing against security incidents (cyber training, *etc*.)
-Enhancing joint recognition between Japan and each member state of ASEAN

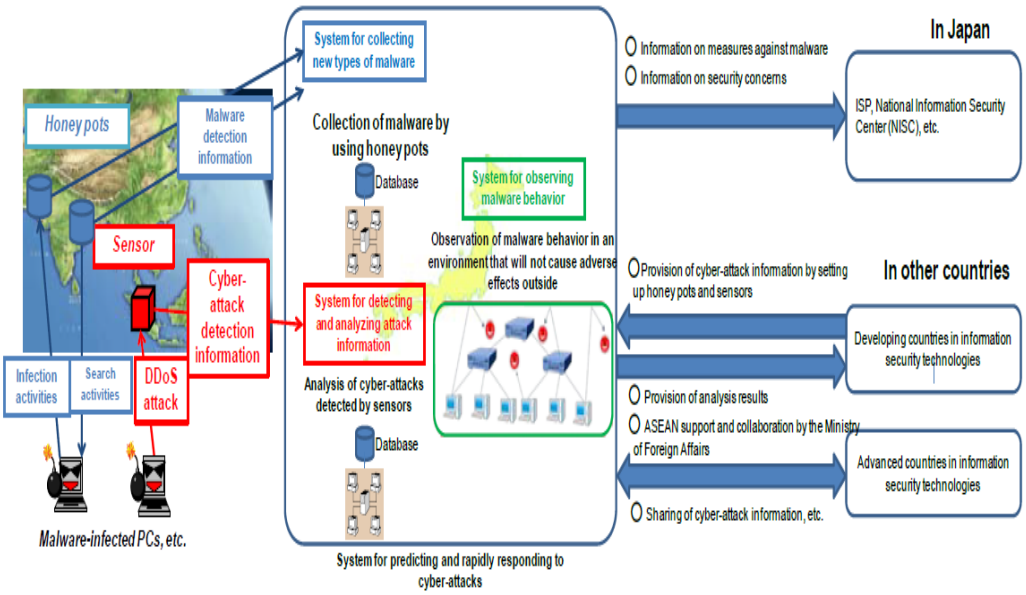

Figure 4. PRACTICE Project Overview

<Source>: International Strategy on Cybersecurity Cooperation: j-initiative for Cybersecurity, Information Security Policy Council, October 2, 2013.

Especially, PRACTICE is the effort to collect, analyze and share information on cyber-attacks. The Japanese Ministry of International Affairs and Communications pushed forwarded this project for 5 years between 2011 and 2015 to establish the technologies to detect and response immediately against cyber-attacks. Japan collects the observation data on cyber-attacks from Indonesia, Thailand, Malaysia and etc. In relation with fostering of human resources for cyber security, Japan provides the training for about 1,000 public officials from ASEAN member countries for 5 years in

link with the technical cooperation project of Japan International Cooperation Agency (JICA).

5. An Analysis of Trend of Cyber Security Budget

Since 2004 when the budget for information security was first opened, the budget has been increased steadily with variant year-on-year rate of change. Until 2010, the budget for information security had been planned and managed by the IT Strategy Headquarters, but from 2012, the 'Information Security Policy Meeting (currently the Cyber Security Strategy Headquarters) takes charge of the budget. The budget of 2011 was planned separately for each department, and no total budget has been opened. Since 2012, the budget has risen substantially every two years. In 2012, the budget for security measures increased as the after-effect of the 2011 Great East Japan Earthquake. In 2014, the budget increased as the venue of the 2020 Summer Olympics was determined. The budget for cyber security in 2016 is 74,280 million Yen, which is more than twice of the budget of the previous year.

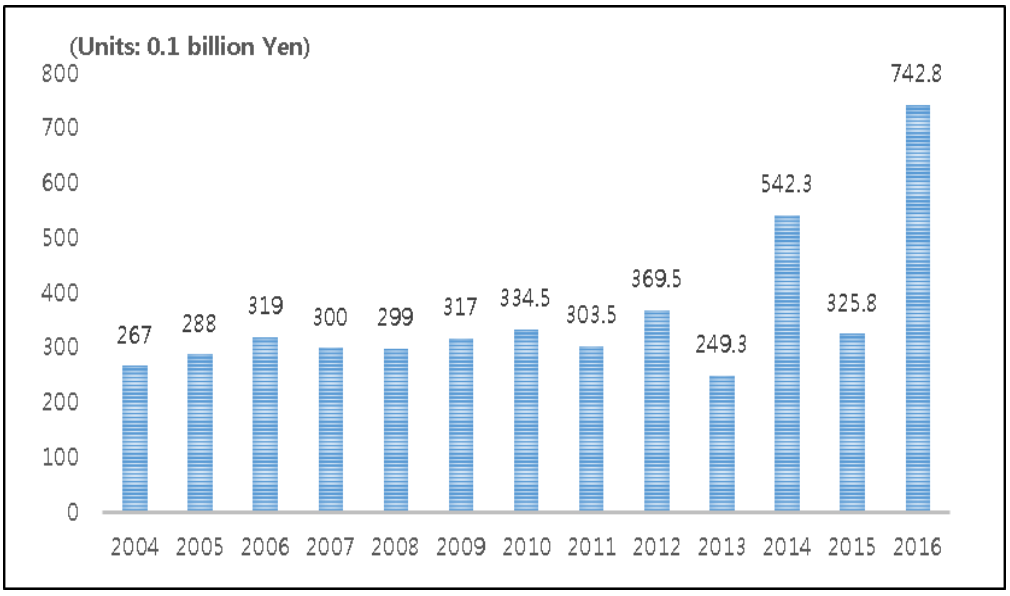

Figure 5. The Trend of Budget for Cyber Security in Japan

<Source>: Data released by IT Strategy Headquarters (2004~2010) and the Cyber Security Strategy Headquarters (2012~2016) of Cabinet Office of Japan
Note) the budget of 2011 is the average of budget between 2004 and 2010.

In the 2016 budget for cyber security [9], the operating budget increased by five times from 1,650 million Yen in 2015 to 8,300 million Yen in 2016 due to the overall policy control function of the National center of Incident readiness and Strategy for Cybersecurity (NISC) under the Cabinet Secretariat reinforced after enactment of the Fundamental Act on Cyber Security in 2014. In addition to the increase of personnel by 20 in 2015, NISC requests increase of personnel. Also the budget for the Government Security Operation Coordination team (GSOC) which controls and responds for government departments increased substantially from 650 million Yen in 2015 to 6,850 million Yen. GSOC has been in operation since 2007.

To break down the budget of each department, the Ministry of Internal Affairs and Communications implements the Future-oriented Network Security Infrastructure Project (1,300 million Yen) and the Local Government Information Security Emergency Measures Project (440 million Yen) as new projects in 2016. The Future-

oriented Network Security Infrastructure Project is planned to enhance the cyber security capacity in preparation for 2020 Summer Olympics. This project is composed of fostering of human resources, large-scale simulation, analysis and sharing of attack information, IoT security and etc. The Local Government Information Security Emergency Measures Project is composed of the measures to respond against cyber threats in relation with the resident number (My Number) system enacted in January 2016.

The Ministry of Economy, Trade and Industry demanded increase of budget for the Infrastructure Security Promotion and IT Project Certification Project from 3,610 million Yen in 2015 to 5,320 million Yen in 2016, and for the Cyber Security Economy Base Building Project from 1,770 million Yen in 2015 to 2,360 million Yen in 2016. The security budget of the Ministry of Defense will increase substantially. The budget for the Information Collection, Examination and Analysis Function Enhancement Project is asked to increase from 2,980 million Yen in 2015 to 6,100 million Yen in 2016. The Ministry of Health, Labor and Welfare, which experienced the large-scale information leakage accident in 2015, plans the budget of 6,210 million Yen for the information security measures of the ministry and the Japan Pension Service.

6. Conclusion

While cyberspace has brought significant benefits to our lives, malicious activities to harm these benefits are increasing. Cyberspace, which anyone can utilize without geographic and time constraints, gives advantages asymmetrically to malicious attackers, not defenders. At the same time, the increasing dependency of socioeconomic activities on cyberspace and the evolution of organized and highly sophisticated methods, or modus operandi, of cyber-attacks that might be state-sponsored have caused grave damages and exerted negative impacts on the people's daily lives and socio-economic activities, and consequently, threats against national security have become more serious year after year.

Additionally, due to the arrival of the interconnected and converged information society, malicious activities in cyberspace will cause extensive impact on all kinds of connected physical objects and services, and the damage caused by cyber-attacks will spread more rapidly and widely in physical space; therefore, it is anticipated that the people's living will be exposed to more immense cyber threats in the future.

This study describes the development and changes of cyber security policies of Japan. Japan started to establish the information security policy in 2005, and is pushing forward to change critical policies based on its 10-year experience. The cyber security policy of Japan can be summarized as follows:

Firstly, the policy aims at establishment of concept of cyber security. The cyber security strategy of Japan starts from awareness of problems that the cyber space is global commons and the source of infinite economic value, and that with the advent of the interconnected and converged information society where the cyber space is converged into the real space, the cyber threats to nations and economic society. This shows that Japan breaks from the defensive and domestic policy. As mentioned in the ‘Cyber Security Strategy’ established after enactment of the Fundamental Act on Cyber Security, the “accident-assumed” countermeasure policy is changing to the proactive policy with the enhanced foresight and immediate response capability.

Secondly, the role of the government is strengthened. Japanese government expresses its will to play the leading role of the global society in implementing the policies. To prove its intention, the government established the Cyber Security Strategy Headquarters under the Cabinet Secretariat, and expanded and reorganized the National center of Incident readiness and Strategy for Cybersecurity (NISC). Since

2010, the axis of the ICT policy of Japan has moved from informatization to cyber security.

Thirdly, the status of cyber security in the national policy is strengthened. Since 2011, the cyber security has been recognized as a major task in Japan's national growth strategy and national security strategy.

After the Great East Japan Earthquake in March 2011, cyber security has been utilized as the means to stimulate the national economy and to strengthen the national status. Japan's positive commitment in the global cooperation with ASEAN is based on this background.

The cyber space has already become the 2nd living space, and the society is changing rapidly to the hyper-connected society where the cyber space is converged with the real space. The cyber security becomes the major issue of the global cooperation, and the competition for the initiative has already started between the advanced countries, including USA, EU and Japan.

References

[1] Media Report, http://economy.hankooki.com/lpage/worldecono/201506/e2015060217510169760.htm
[2] K. Min, "Strategic Direction and Trend of Information Security in Japan", Information Security Issue Report, Korea Internet & Security Agency, **(2005)**.
[3] K. Min, "Present Conditions and Implications of Recent Information Security in Japan", Information Security Issue Report, Korea Internet & Security Agency, **(2008)**.
[4] Fundamental Act on Cyber Security (House of Representatives of Japan), http://www.shugiin.go.jp/internet/itdb_gian.nsf/html/gian/honbun/houan/g18601035.htm
[5] Japanese Cabinet Secretariat's National Security Strategies, http://www.cn.emb-japan.go.jp/fpolicy_j/nss_j.pdf
[6] International Strategy on Cybersecurity Cooperation; j-initiative for Cybersecurity, Information Security Policy Council Japan, **(2013)**.
[7] Japanese Cabinet Secretariat's Cyber Security Center Data, http://www.jssm.net/jssm/security_day/2011/20110226_1.pdf
[8] Japanese Cabinet Meeting on Japan-ASEAN Cooperation for Cyber Security, Japanese Ministry of Internal Affairs and Communications, http://www.soumu.go.jp/main_content/000249127.pdf
[9] Cabinet Secretariat's Cyber Security Center Data, http://www.nisc.go.jp/conference/cs/dai05/pdf/05shiryou03.pdf

Authors

Kyoungsik Min, he is a Ph.D. and Senior Researcher at Korea Internet & Security Agency, Seoul, Korea. He received M.S. and Ph.D. in Economics degree from Meiji University, Tokyo, Japan.

He is a Guest Researcher of Institute for Hyper Network Society, Oita, Japan. He research interests are cyber security policy, security

Economic, and Hyper-connected Society.

Seung-Woan Chai, Ph.D. he is a Senior Researcher at Korea Internet & Security Agency, Seoul, Korea. He received M.S degree in Economics from Dankook University, Seoul, Korea and Ph.D. Degree in economics from Niigata University, Niigata, Japan. He research interests are cyber security policy, security

Economic, and Personnal data protection.