The approaches to promote critical infrastructure protection in Japan

The approaches to promote critical infrastructure protection in Japan are illustrated below:

1. Coverage of Critical Information Infrastructure

In the "Action Plan on Information Security Measures for Critical Infrastructure" promulgated by the Information Security Policy Council (ISPC) in 2005, critical infrastructure is defined as: Critical infrastructure which offers the highly irreplaceable service in a commercial way is necessary for people's normal lives and economic activities, and if the service is discontinued or the supply is deficient or not available, it will seriously influence people's lives and economic activities. Based on the definition of the action plan, the critical infrastructure contains: telecommunication systems, administration services of the government, finance, civil aviation, railway, logistics, power, gas, water, and medical services

2. Promoted Relevant Policies of The Past

The issues regarding the CIIP are gradually being developed with the norm of information social security policy in Japan. Adopting the Action Plan of the Basic Guidelines Toward the Promotion of an Advanced Information and Telecommunications Society of 1998 proposed by the Japanese government in 1998 as a basis. The Japanese government keeps presenting polices of improvement for the relevant issues in order to acquire the stable development of telematics and telecommunications. Several years later, the Ministry of Economy, Trade, and Industry (METI) announced the Comprehensive Strategy on Information Security in 2003. The formulation of the strategy not only emphasizes the possible telematics-related risks and protection against threats that may be encountered in the information society, but it also enhances the level of information security to the level of national security and presents a comprehensive information security improvement program. Furthermore, the submission of the strategy has identified government's responsibility in the development of information security Therefore, a division which is solely responsible for information security was established in the Cabinet Secretariat and is devoted to the development of it. In 2005, the Ministry of Economy, Trade, and Industry (METI) amended the Comprehensive Strategy on Information Security and announced the First National Strategy on Information Security based on the creation of a policy of a long-term information security task in Japan which is also the foundation for the policy of guidelines and action security concerning critical information infrastructure. This is in addition to being the most important basis for the policy of information security development. The strategy is different from the Comprehensive Strategy on Information Security in connotation. In the range of information security protection, it not only maintains information security from the perspective of the government; for instance, to divide the rights and duties on information security protection practices between the central government and the local government, and to strengthen the capacity of the government to solve emergencies such as cyber attacks, but it also tries to employ the public-private partnership on the CIIP issue to construct an extensive information security protection and to develop a Capability for Engineering of Protection, Technical Operation, Analysis and Response (CEPTOAR): one similar to the ISAC of America, to strengthen the information sharing and analysis of information security of all industry involved. According to the strategy, the METI established the Information Security Policy Council (ISPC) and the National Information Security Center (NISC) under the subordination of the Cabinet Secretariat in order to reach a goal of dependable society of information security.1

Finally, the information security policies more directly related with the CIIP are the Action Plan on Information Security Measures for Critical Infrastructure and the Standards for Information Security Measures for the Central Government Computer Systems, both of which regulate CI-related threats, information security standards, public-private partnership information sharing system, and the levels of information security standards between different governments and critical infrastructures, respectively.

3. Oraganization Framework

Generally speaking, the Cabinet Secretariat is the main division of the CIIP and the information security for the Japanese government, while the ISPC and the NISC established under the Cabinet Secretariat in 2005 are the core organizations for the development of the CIIP policy. In addition, the National Policy Agency (NPA) and the Ministry of Internal Affairs and Communications (MIC) also played an important role in assisting the Cabinet Secretariat with critical infrastructure protection. The part of public-private partnership is covered by the CEPTOAR which takes the responsibility for information sharing and analysis of information security between the government and private organizations.

4. Notification System

For critical infrastructure protection, Japan has set up a warning and notification system in addition to the emphasis on fundamental information security protection. With the concept of public-private partnership, various messages related with information security are analyzed and shared in order to prevent information security incidents from occurring. The network of notification system in Japan mainly consists of several organizations as listed below.

(1) National Incident Response Team

The National Incident Response Team (NIRT) which is the information security office under the Cabinet Secretariat in the organization framework belongs to the Computer Emergency Response Team (CERT)2 and is first in line in the government to handle internet emergencies. According to the Action Plan for Ensuring e-Government's IT Security, the NIRT which consists of 17 experts from the government and the private organizations is responsible to (1) accurately understand and analyze emergencies, (2) develop technical

strategies to solve and rehabilitate emergencies to prevent incidents from reoccurrence, (3) provide other governmental organizations the assistance to solve the information security issue, (4) collect and analyze information or intelligence so that effective solutions and strategies may be provided when an incident happens, (5) provide the governmental organization with professional knowledge and information, and (6) enhance and improve all knowledge pertinent to information security.

The Japan Computer Emergency Response Team Coordination Center (JPCERT/cc) is the first Computer Security Incident Response Team (CSIRT) established in Japan. It consists of internet service suppliers, security products/service suppliers, governmental agencies, and associations of industry & commerce. The JPCERT/CC is also a member of the Asia Pacific Computer Emergency Response Team (APCERT) and a member of the Forum of Incident Response and Security Teams (FIRST). It coordinates and integrates prevention measures pertinent to information security and is consistent with other CSIRTs.

(3) Telecom Information Sharing and Analysis Center

In Japan, besides the mechanism responsible to notify the government, which functions as a bridge for communication between it and all those outside of it, the mechanism of information sharing and notification is also established among industries to provide each with a channel for information exchange and consultation. In 2001, Japan established the Telecom Information Sharing and Analysis Center Japan (Telecom-ISAC Japan). In addition to real-time inspection for computer intrusion incidents and conducting information collection and analysis, the Telecom-ISAC Japan proposes to e-government many suggestions related with the Transact-SQL issue as well. The reasons for launching the Telecom-ISAC are to instantaneously detect a computer intrusion incident, and to instantaneously gather and analyze its information, and then exchange this with other telecom carriers and offer them relevant countermeasures for precaution; so that in can reach the goal of ensuring telecom security since it is an important infrastructure concerning social economy.

(4) Cyber Force

The reasons for launching the Cyber Force are to maintain the security to use the internet by regularly "patrolling" it, searching for evidence of internet crime, and to notify the critical infrastructure operators about any unusual internet use so as to prevent the occurrence of cyber terror attacks. The Cyber Force also assists operators to solve and diminish the damage and influences when an incident occurs.

(5) Portal Site of National Police Agency

The National Police Agency owns the portal site "@police". It exists to prevent large-scale cyber emergencies and to provide gathered information concerning information security to government. In addition to providing the techniques related with the safe use of computer networks, @police is also dedicated to educating internet users about the concept of information security and to increase security awareness.

(6) Ministry of Economy, Trade and Industry

Since 1990, the Ministry of Economy, Trade and Industry (METI) has cooperated with the JPCERT/CC and the Information Technology Promotion Agency (IPA) to provide reports on virus, intrusion, and the damage caused by them, to remind the public to pay attention.

5. Legal Norms

The laws regarding critical infrastructure protection in Japan are illustrated as follows:

(1) Unauthorized Computer Access Law of 1999

The Unauthorized Computer Access Law includes various conducts such as cyber intrusion, and data thefts, into the norms of criminal punishment to deter cyber crimes from spreading in order to ensure the safety of the critical information infrastructure.

(2) Act on Electronic Signatures and Certification Business of 2000

With the formulation of the Act on Electronic Signatures and Certification Business, the smooth promotion of the electronic signature system is ensured and the circulation and process of electronic communication can be fostered further.

(3) Basic Law on Formation of an Advanced Information and Telecommunication Network Society of 2001

Through the formulation of the Basic Law on Formation of an Advanced Information and Telecommunication Network Society, the legal basis to execute an information technology policy is enhanced, and the direction and job content for the government to execute this policy is explicitly stated.

1.http://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf(last accessed date: 2009/07/20).
2.http://www.nisc.go.jp/en/sisaku/h1310action.html(last accessed date: 2009/07/20).

Release : 2013/04