International Strategy on Cybersecurity Cooperation
- j-initiative for Cybersecurity -

October 2, 2013

Information Security Policy Council

Japan

Contents

1. Objectives

As 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, which arose from advancements in information and communication technology, has become an essential platform to support national growth. On the other hand, with our heightened reliance on information and communication technology, 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.

In order for countries in the world to coexist in cyberspace and share its benefit to a maximum extent, it is essential to acknowledge different values, build mutual trust and work hand-in-hand to counteract the challenges. To this end, Japan is strongly committed to actively strengthen cooperation and mutual assistance internationally so as to ensure safe and reliable cyberspace.

Japan boasts the world's highest level of telecommunications infrastructure. The increased use and application of information and communication technology means Japan has already faced a variety of cyber threats. In this context, the Japanese government successively prepared and revised strategies, annual plans, sector-specific policies and other measures in pursuit of ensuring cybersecurity, and, based on these strategies and measures, forged cooperation among industry, academia and government stakeholders in addressing these challenges. Japan is dedicated to utilize these extensive experience and knowledge in promoting international cooperation.

This Strategy is based on the Japan Revitalization Strategy and the Cybersecurity Strategy which were developed in June 2013, and summarizes Japan's basic policy and its priority areas for international cooperation and mutual assistance in the field of cybersecurity, so that it can be presented as a package to the stakeholders both in Japan and overseas. Japan will promote initiatives for international cooperation and mutual assistance in cybersecurity based on this Strategy under the common understanding shared among all domestic stakeholders including those from industries, academia and the government. Japan will actively contribute to shaping of safe and reliable cyberspace in which free flow of information is ensured by building relationships of cooperation with countries around the world.

2. Basic Principles

2.1 Ensuring free flow of information

Cyberspace has become a driver for social and economic growth due to its openness and availability to all actors. Excessive administration and regulation of cyberspace diminishes the benefits of cyberspace and could impede social and economic growth.

Therefore, it is imperative to ensure openness and interoperability of cyberspace without excessively administering or regulating it and to maintain and develop safe and reliable cyberspace in which free flow of information is ensured.

This will ensure freedom of expression and vibrant economic activities in cyberspace, facilitate innovation, economic growth and solutions for social issues and provide positive benefits which countries around the world can enjoy.

2.2 Responding to increasingly serious risks

As cyber threats are growing in its severity, existing measures and initiatives are no longer capable of responding to these widespread and globalized risks. Vulnerability of cyberspace to these threats may impede activities in cyberspace and hamper free flow of information.

Therefore, in addition to the existing measures and initiatives, there should be a new mechanism based on enhanced international cooperation in order to appropriately address the risks associated with the revolution in information and communication technology.

2.3 Enhancing risk-based approach

Absolute prevention of cyber attacks is ideal, but has become practically difficult due to expansion of cyberspace and sophistication of cyber threats. A more realistic approach to cyber threats is to assume that certain risks will occur and trigger incidents, but to work toward a rapid recovery from such incident and to prevent any further damage from it through timely and appropriate allocation of resources and international cooperation.

Therefore, one of the most urgent needs for the international community is to establish a mechanism to implement a risk-based approach, whereby risks are quickly and appropriately identified as they evolve and responded to dynamically in accordance with their characteristics.

2.4 Acting in partnership based on social responsibilities

Diverse entities have enjoyed the benefits of the expanding cyberspace. As a result, cyber threats have become a reality, and these threats are spreading far and wide. In this context, it is important that the whole of society participates in “cyberspace hygiene” as a preventive measure against cyber threats, in addition to each entity taking individual measures and actions for their own cybersecurity.

In this regard, all stakeholders in the global cyberspace need to cooperate and assist with each other while fulfilling the responsibilities corresponding to their respective roles in the society.

3. Basic Policies

3.1 Incremental fostering of common global understanding

Vitality of cyberspace has been enhanced by the diversity of entities which make use of it, such as governments, enterprises and individuals, and co-existence of countries with different cultures and values.

For this reason, it is important to build up international cooperation to ensure cybersecurity in a way which recognizes the existence of diverse entities and values in cyberspace, and which maximizes its benefit. Common global understanding needs to be fostered while appreciating diversity.

Issues pertaining to cybersecurity vary widely across a broad spectrum, from socio-economic to national security, and from the easily resolved to the more difficult. There is also an infinite variety of entities that can take part and degrees to which a common understanding can be fostered. Therefore, a common understanding needs to be fostered incrementally, wherever feasible, while appreciating the diverse values.

All platforms will be utilized in promoting this approach, including bilateral, multilateral and regional frameworks as well as the United Nations (U.N.) meetings.

3.2 Japan's contribution to the global community

Japan has developed the world's top-level telecommunications infrastructure containing fiber-optic networks and high-speed wireless networks nationwide, which led to increase in the use and application of cyberspace by various entities of all generations. Consequently, Japan has faced serious cybersecurity issues ahead of other countries. At the same time, relevant entities in both public and private sectors have worked in partnership to implement a wide variety of measures to address these issues and have achieved successes.

Building on these extensive experience and knowledge as a pioneer in cybersecurity, Japan will contribute to the global efforts to address these challenges more efficiently and effectively. We will actively contribute to capacity building activities at the global level, including support for human resources development and support for establishing incident response mechanisms and information-sharing mechanisms.

3.3 Expansion of the technological frontier at the global level

Advanced technology should be employed to the extent possible in order to respond appropriately to the emerging risks and sophistication of cyber attacks. In this regard, Japan has accumulated extensive knowledge and experiences on technical responses to cyber threats, including development of cybersecurity technology and subsequent steps for its practical application.

In order to ensure secure use of cyberspace, Japan values steady development of technology, expansion of technological frontier at the global level, and diffusion of the benefits of advanced yet inexpensive technology.

While information and communication technology can pose a risk depending on the way it may be used, it is of vital importance that we continue developing, using and applying the technology rather than holding back its development or controlling such technology for fear of its potential abuse.

4. Priority Areas

4.1 Implementation of dynamic responses to cyber incidents

In implementing the risk-based approach premised on the possibility of cyber incidents, response needs to be prompt and global, and must minimize the impact of the incident while addressing the ever-changing risks.

As cyber threats are real threats, building a mechanism for international cooperation and partnership is an urgent task. Such mechanism would facilitate quick identification of a cyber incident, accurate analysis of its impact, and global dynamic response to the incident such as prevention of further damage, facilitation of early resolution, research on its causes and prevention of similar incidents.

4.1.1 Enhancing multi-layered mechanism for information sharing

In order to establish a mechanism which can dynamically respond to global cyber incidents, there also needs to be a mechanism for global information-sharing which enables responses based on international information and sharing of countermeasures.

Having a wide range of information sources facilitates quick and accurate judgments on the rapidly-changing situations, given that diverse entities are involved in cyberspace with their own security measures. Thus, it is meaningful to build an information-sharing mechanism that is multi-layered, consisting of multiple layers including technology, law enforcement, policy and diplomacy.

In particular, it is important to forge cooperation among Computer Security Incident Response Teams (CSIRTs), which are responsible for operational responses, such as detecting cyber incidents, analyzing malwares and IP addresses and taking actual responses; cooperation among law enforcement agencies which exercise investigative authorities and are responsible for preventing further damage; cooperation at the policy level which would facilitate quick understanding of the overall picture of an incident and necessary policy responses; information-sharing at the diplomatic level to avoid unexpected escalation into potential conflict; and cooperation among researchers engaged in research and development on leading-edge technology.

Japan will actively work toward establishing a multi-layered global mechanism for information-sharing and will enhance its preparedness for the event of cyber incident.

4.1.2 Appropriate response to cybercrime

International cooperation needs to be strengthened in order to effectively deal with cybercrime which easily transcends national borders.

Japan will continue to exchange information on cybercrime and digital forensics with foreign law enforcement agencies through forums such as the G8 Rome-Lyon Group High-Tech Crime Subgroup and the Counter-cybercrime Technology Investigation Symposium (CTINS). Japan will also dispatch personnel overseas in order to exchange information on the latest cybercrime investigative techniques and to strengthen cooperation with overseas investigation agencies and will actively request mutual legal

assistance to these agencies. Japan will actively participate in the promotion of the Convention on Cybercrime (so-called the Budapest Convention) by assisting countries to become State Parties to the Budapest Convention and by conducting capacity building activities. Through promotion of the Budapest Convention, Japan seeks to contribute to the promotion of international cooperation and formation of international norms in the field of countering cybercrime.

Japan will build upon the ongoing measures for international cooperation in order to respond to cybercrime incidents more swiftly. For instance, the Japanese government seconds our official as the first Executive Director of the new INTERPOL Global Complex for Innovation (IGCI), which is being established in Singapore to complement the General Secretariat of the International Criminal Police Organization (ICPO).

4.1.3 Establishing framework of cooperation for international security in cyberspace

Cyberspace is a relatively new “domain”, comparable to land, sea, air and space, in which national security activities are also conducted, such as information-gathering, attack and defense. Actively promoting international cooperation and establishing framework of cooperation are important for ensuring stability of the use of cyberspace.

Japan will actively take part in international rulemaking on the use of cyberspace; develop confidence-building measures through dialogues and information-exchange bilaterally and multilaterally including via regional frameworks such as the ASEAN Regional Forum (ARF); and promote capacity building in order not to leave any regions in the international community vulnerable to cybersecurity threats.

Given that cooperation with the United States (U.S.) as our ally bears an extremely significant importance for our national security, Japan will accelerate the dialogues at various levels, such as the Japan-U.S. IT Forum, which is held between Japanese and the U.S. defense authorities, and the Japan-U.S. Cyber Dialogue, which is held between relevant Japanese and U.S. ministries and agencies. In an effort to reinforce deterrence and to enhance effectiveness of the Japan-U.S. Security Arrangements, Japan will continue to further strengthen partnership with the U.S. through various means including close sharing of information and best practices on cyber threats and the responses, more practical joint training exercises, and cooperation to ensure security of the shared systems between the Japanese and the U.S. defense authorities.

Furthermore, Japan will actively work toward establishing a global framework of cooperation for international security in cyberspace. Given that cyberspace is expanding globally, Japan will continue to share information and exchange views on relevant measures through discussions at various levels in order to actively promote cooperation with relevant countries and international organizations. Japan will also make efforts to deepen mutual understanding and develop confidence-building measures.

4.2 Building up “fundamentals” for dynamic responses

It is critical that each country has “fundamentals,” that is, sufficient basic capacity and response mechanisms to respond dynamically to cyber incidents through international cooperation and mutual assistance. Moreover, considering the global nature of cyberspace, raising the cybersecurity standard at the global level and reducing the number of vulnerable nodes in the realm of cyberspace are essential.

Such efforts should also have a consequential deterrent effect on malicious activities carried out in cyberspace.

4.2.1 Support for building a global framework for cyber hygiene

At the basis of international cooperation for dynamic responses to cyber incident is each country’s national mechanism to detect, analyze and respond to cyber incidents. In addressing the globalization of cyber incidents, such mechanism needs to be developed also at a global level.

Drawing on our own experience, Japan will provide support for establishing CSIRTs and developing their operational capacity. Japan will also share information on measures for cleaning bots, detecting malicious sites, dealing with malware, and on information-sharing mechanism for cybersecurity of critical infrastructure.

Japan has experience in establishing CSIRTs in a wide range of regions, such as in the Asia Pacific and in Africa. Japan also have experience in establishing CSIRTs for control systems, which have become increasingly important in recent years, Japan will build upon these experiences and expand support.

Since 2006, ahead of the rest of the world, Japan has been implementing network-based measures to counter bot virus infections in cooperation with internet service providers (ISPs). Bot infection rates decreased dramatically as a result, and Japanese measures are now recognized as a model among developed countries. Going forward, in cooperation with ISPs, Japan plans to commence a new initiative of building a database which stores information on malicious sites and alerts users attempting to access those sites. Japan will actively share the knowledge obtained through this initiative. Furthermore, Japan will promote measures for bot extermination through multilateral cooperation among CSIRTs.

Critical infrastructure systems lie at the basis of our social and economic activities and therefore require a high level of security. In Japan, these systems are built with high security including solid resilience to cyber attacks. Japan will also share these outstanding cybersecurity measures when providing support for building of critical infrastructure systems.

When building a framework for cyber hygiene activities, it is important to have indicators by which actual cyber attacks and cybersecurity initiatives in each country can be quantitatively assessed. Japan will actively cooperate and contribute to initiatives by the Organization for Economic Cooperation and Development (OECD) and other organizations for the formulation and measurement of such indicators.

4.2.2 Promotion of awareness-raising activities

In order to ensure proper cyber incident responses, relevant entities need to have an appreciation of cybersecurity and basic personnel capacity to deal with the incidents. For example, operational and policy level managers in charge of incident responses need to have certain capabilities, and all entities need to have a certain degree of security awareness and capacity. Japan has continuously implemented various capacity-building and awareness-raising activities, utilizing our own highly capable personnel and advanced technological facilities. Thus, Japan has accumulated sufficient knowledge and experience in this area.

Japan will contribute to raising the level of cybersecurity internationally, by drawing on its knowledge and by taking active part in disseminating capacity-building and awareness-raising activities around the world. Such activities can include conducting cybersecurity trainings targeted at government and corporate cybersecurity managers and CSIRTs.

In particular, Japan runs international campaign for raising awareness on cybersecurity every October. Japan will work closely with countries conducting similar awareness-raising activities and will appeal for expansion of the campaign on a more global level.

4.2.3 Enhanced research and development through international cooperation

In responding to the advancement and sophistication of cyber threats, it is essential to develop advanced countermeasure techniques that correspond to the threat level.

An effective way of developing advanced countermeasures that can appropriately respond to cyber attacks is to combine each country's technological strengths organically and develop them. Japan will actively promote research and development through international cooperation.

It is also important to immediately put these countermeasure techniques into practice and use them for dynamic responses to cyber incidents and for support of development of a cleanup framework.

In particular, Japan promotes PRACTICE (Proactive Response Against Cyber-attacks Through International Collaborative Exchange), a project to build a network of countries to gather information on cyber attacks, malwares and other incidents, and to experiment, research and develop technology which predicts cyber attacks and provides immediate responses. Japan will contribute to improve the prediction and response capacity against cyber attacks at a global level by further extending partners to this project.

4.3 International rulemaking for cybersecurity

In cyberspace, various countries with different values and systems coexist. Moreover, cyberspace is used in a variety of ways by diverse entities. In order to maximize the benefits of cyberspace, it is important to ensure that it can be used in a stable manner. In this regard, international rules need to be made for various activities which make use of cyberspace, while strengthening personnel ties in the medium and long term.

4.3.1 Formulation of international standards of technology

As cybersecurity systems are increasingly traded internationally, maintaining technological standards of such systems is growing in its importance so as to ensure their interoperability and security level.

While various initiatives are underway for international standardization, it is important to formulate and disseminate international standards of cybersecurity technology and to create mutual recognition frameworks. In this regard, public-private partnership is essential since enterprises and other such entities are the main actors to actually use such standards in their business activities.

Japan established the Control System Security Center (CSSC) in 2013, which serves as the basis for setting up evaluation and authentication technology for control system security. Japan will institute an evaluation and authentication organization for promoting the use of such technology and will also contribute to activities of enterprises and organizations participating in the CSSC to propose new international standards using the CSSC. Additionally, as part of the cybersecurity measures, Japan will actively promote the Common Criteria Recognition Arrangement (CCRA) for procurement, which is an international framework for mutual recognition of authentication. Furthermore, Japan has also contributed to formulation of the Cybersecurity Information Exchange Framework (CYBEX) at the International Telecommunications Union (ITU), and will continue to promote this activity in cooperation with other countries.

As for cloud services, Japan is leading the activities for international standardization of cloud security at the International Organization for Standardization (ISO) and ITU so that cloud services can be used safely and securely. In addition to actively contributing to the prompt adoption of international standards, Japan will promote the formulation and dissemination of a concrete manual together with relevant enterprises both in Japan and overseas, and will promote the sharing of knowledge acquired through this process.

It is important to note that, while ensuring cybersecurity remains an important agenda, excessive control over what technology to be used, for instance by giving priority to domestic technology over those from abroad, may result in reduction of domestic security. In the spirit of mutual prosperity of all the relevant countries, Japan seeks consistency with international trade rules taking into consideration transparency and fairness so that regulation does not become excessive.

4.3.2 International rulemaking

In order to ensure stable use of cyberspace, there are ongoing global efforts for international rulemaking on the use of cyberspace. For instance, the Group of Government Experts (GGE) established under the First Committee of the UN General Assembly issued a report in June 2013, which refers to norms for state use of information and communication technology. Japan will continue to make active contributions to such global endeavors and will share our basic principles and policies at every opportunity.

With respect to norms for state use of information and communication technology, given the rapid progress of cyber technology, we consider it more realistic to promptly develop legally non-binding soft norms covering various acts in cyberspace, without creating a room for excessive state control. Japan is of the view that existing international law, including the U.N. Charter and international humanitarian law, naturally applies to acts in cyberspace. Japan will further examine how specific legal norms can apply to certain specific acts, taking into account the distinctive characteristics of information and communication network technology. As Japan actively took part in discussions at the U.N. GGE as an expert in drafting the abovementioned report Japan intends to lead international discussion further on the specifics of how existing international law should be applied to acts in cyberspace.

On the other hand, given the imminence of cyber threats and difficulty of identifying perpetrators of cyber attacks, it is important to improve the predictability of each country / region’s cyberspace actions and to promote confidence-building measure in order to avoid unexpected escalation that are not intended by parties, for instance as a result of misidentification of attackers. As measures to build confidence with various countries, Japan will continue to publicly announce its various strategies, strengthen cooperation among CSIRTs and establish information-sharing systems, among others.

Efforts are also underway to build a policy framework for cybersecurity with an emphasis on the social and economic aspect of cyberspace, such as the review of OECD’s Guidelines for the Security of Information Systems and Networks. Such efforts also form part of international rulemaking. Japan has participated proactively in the discussions at the OECD, and will continue to robustly promote these initiatives in cooperation with various countries.

5. Regional Initiatives

5.1 Asia Pacific

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.

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 will further strengthen these ties, by promoting initiatives such as capacity building for human resources development and for the creation of frameworks for information sharing and critical infrastructure protection. Moreover, Japan will comprehensively promote cooperation on cybersecurity technology with the ASEAN, by promoting the JASPER (Japan-ASEAN Security PartnERship) Project which combines the PRACTICE Project with warnings to computers infected with malware. In addition, under the TSUBAME Project, by cooperating with CSIRTs within the Asia region and installing sensors in CSIRTs, trends of cyber attacks within the Asia region are identified at an early stage and warning and response measures are taken quickly, thereby strengthening the cleanup of the cyber environment. Furthermore, in the area of countering cybercrime, Japan will strengthen cooperation with ASEAN and conduct capacity building and sharing of knowledge and best practices through frameworks such as the ASEAN-Japan Ministerial Meeting and the Senior Officials Meeting on Transnational Crime (AMMTC+Japan, SOMTC+Japan).

Japan will also deepen relations with non-ASEAN countries as important partners, and will seek to address cybersecurity issues through cooperation and mutual assistance. Among others, Japan will continue to strengthen partnership with India, building on the existing initiatives such as the bilateral Japan-India Cyber Dialogue.

5.2 U.S. and Europe

Partnership between Japan and the U.S. as our ally centered on the Japan-U.S. Security Arrangements is of essential importance for Japan. The two countries 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 Japan-U.S. Policy Cooperation Dialogue on the Internet Economy. Japan will continue to deepen this partnership.

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. Japan will continue to strengthen these partnerships.

5.3 Other regions

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. Going forward, Japan will further expand these efforts.

5.4 Multilateral frameworks

Efforts for making safe and reliable cyberspace have also been actively pursued in multilateral frameworks.

With respect to international rulemaking and capacity building for cybersecurity, active discussions take place at various forums such as the U.N., G8, ARF, OECD, the Asia-Pacific Economic Cooperation (APEC) and NATO (North Atlantic Treaty Organization). With respect to policies for critical infrastructure protection and rapid incident response, global initiatives have also been undertaken at the Meridian and the IWWN (International Watch and Warning Network), which are for government agencies, as well as at such meetings as the FIRST (Forum of Incident Response and Security Teams), the APCERT (Asia Pacific Computer Emergency Response Team), which is a community of CSIRTs from the Asia Pacific region, and follow-up meetings to the London Conference on Cyberspace, each of which is attended by a broad range of entities from both the public and private sectors. In addition, with respect to cybercrimes, efforts are being undertaken to deepen international cooperation in criminal investigations through frameworks such as the ICPO.

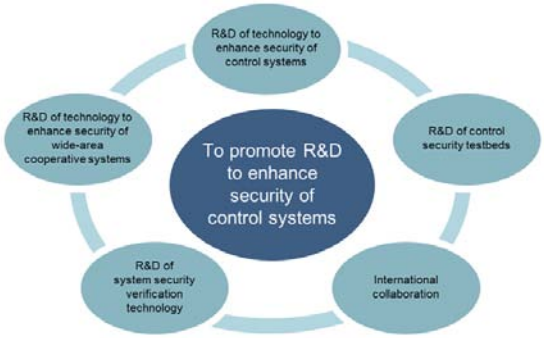
Japan has actively participated in these forums and will make further contributions to the discussion at all opportunities in order to contribute to building safe and reliable cyberspace. Our enhanced contribution needs to be tangible. In this regard, Japan will actively host international conferences to be held in Japan, including the Meridian in 2014.

APPENDIX

Control System Security Center (CSSC)

- Cyber attacks aimed at social infrastructure have increased globally and, as a result, risks which may cause serious damage to society have emerged. In March 2012, infrastructure manufacturers and other companies formed a technology research association in response to increasing demand to secure the safety of information and communication technology systems controlling infrastructure. As of September 2013, 18 organizations are members of the association.
- In April 2013, the Control System Security Center began its operation at CSSC Headquarters (called CSSC-Base6) in Tagajo City in the Tohoku region. The headquarters is equipped with security verification facilities for industrial control systems. Members of the technology research association conduct activities such as development of technology to enhance security of control systems, and capacity building for control system security personnel.
- CSSC has developed small-scale mock plants to simulate electric power system, gas system, building automation, automaker, sewage treatment, smart community and chemical process automation. In fiscal year 2013, these plants will be utilized for hands-on simulation exercises in order to raise awareness for cyber attacks.
- CSSC plans to accept visits from stakeholders abroad, to provide training courses, and to organize international conferences.

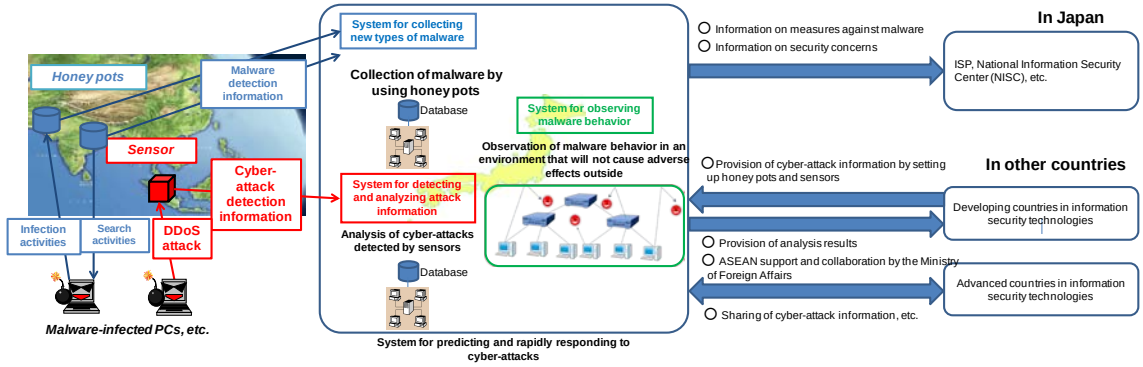
CSSC






PRACTICE (Proactive Response Against Cyber-attacks Through International Collaborative Exchange)

- The project has been implemented since the fiscal year 2011 with the aim of countering and reducing the risks of cyber attacks (distributed denial of service attacks, malware infection activities, etc.) which produce growing damages in recent years.
- We will internationally build a network to gather information related to cyber attacks and malware, etc. through cooperation with Internet service providers and universities in Japan and other countries, and collaborate with other countries to conduct research, development, and field trial for technology that makes it possible to predict the occurrence of cyber attacks and quickly respond to them.
- We will utilize international conferences (bilateral and multilateral) and call upon organizations (Internet service providers, universities, etc.) of various countries to collaborate in sharing information such as cyber attack monitoring data and analysis results and in conducting research and development.



(Reference) Project overview

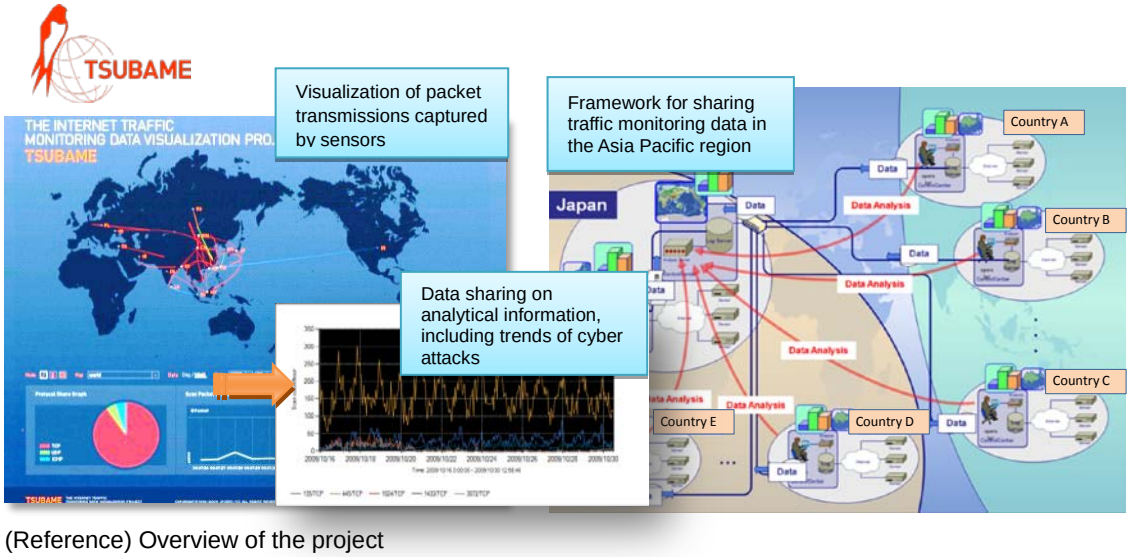
- The project will be implemented together with Telecom-ISAC Japan, which is an ISP association for network security, NICT (National Institute of Information and Communications Technology), which is a research organization, and partner companies, etc.
- Research and development for several elemental technologies is currently being conducted in order to predict attacks. We are aiming to establish the technologies by 2015 and contribute to improvement of abilities to quickly respond.

※ JASPER (Japan-ASEAN Security Partnership)

- This is a collaborative project between Japan and ASEAN aimed at strengthening technical cooperation for network security between Japan and ASEAN
- JASPER is composed of PRACTICE and malware infection alert
- The launch of JASPER project was confirmed at the “ASEAN-Japan Ministerial Policy Meeting on Cybersecurity Cooperation” that was held in September 2013.

TSUBAME (International network traffic monitoring project)

- TSUBAME is a project for monitoring and visualizing Internet traffic, and has been implemented since 2007. The project was developed under the framework of the Asia Pacific Computer Emergency Response Team (APCERT), which is a community of Computer Security Incident Response Teams (CSIRT*) in the Asia Pacific region. The project was initiated and is led by JPCERT/CC.
- This project installs monitoring sensors in the national CSIRTs of the Asia Pacific region (as of September 2013, sensors have been installed in 23 teams in 20 economic regions), and visualizes the monitoring results in the region. The project is aimed at strengthening collaboration among CSIRTs (cooperation in responding to cross-border security incidents, and sharing threat information and analysis capabilities) through the process of gathering and visualizing malicious Internet activities detected by each sensor, sharing this information among all members, and responding to them together.



(Reference) Overview of the project

- This project enables incident responses and other cooperative activities at the operational level by sharing the data collaboratively monitored by CSIRTs in each country/region and creating an analysis platform for situation assessment and swift responses.
- Participating members of the project share the results of the analyzed data. These data are used for incident responses through such measures as issuance of analysis reports. An annual TSUBAME workshop is also held to share analysis methods, to improve analysis capabilities, and to enhance incident response skills.
- Participating members analyze and exchange information on trends of worm infection and scanning activities to search weak points. Members also carry out joint research on such themes as methods for threat visualization in order to efficiently understand the trends of worm infection and scanning activities to search for weak points.

* Abbreviation of Computer Security Incident Response Team. It serves as a point of contact when cyber attacks occur and is also an expert organization that responds to these cyber attacks.