Cyber Security Strategy (Information Security Policy Council, June 10, 2013)

Environmental Change

Merger and Integration of Cyberspace and Real-space
[widespread/sophistication, further progress, global expansion]

Increasing Serious Risk Surrounding Cyberspace
[hugeness, diffusion, globalization]

Vision to aim as a Goal

~Realization of the "Cyber Security Nation"~

For national security/crisis management; social/economic development; and safety/security of public, realizing the society that is strong against cyber attacks, full of innovations and that its public will be proud of, through constructing the world-leading, resilient and vigorous cyberspace

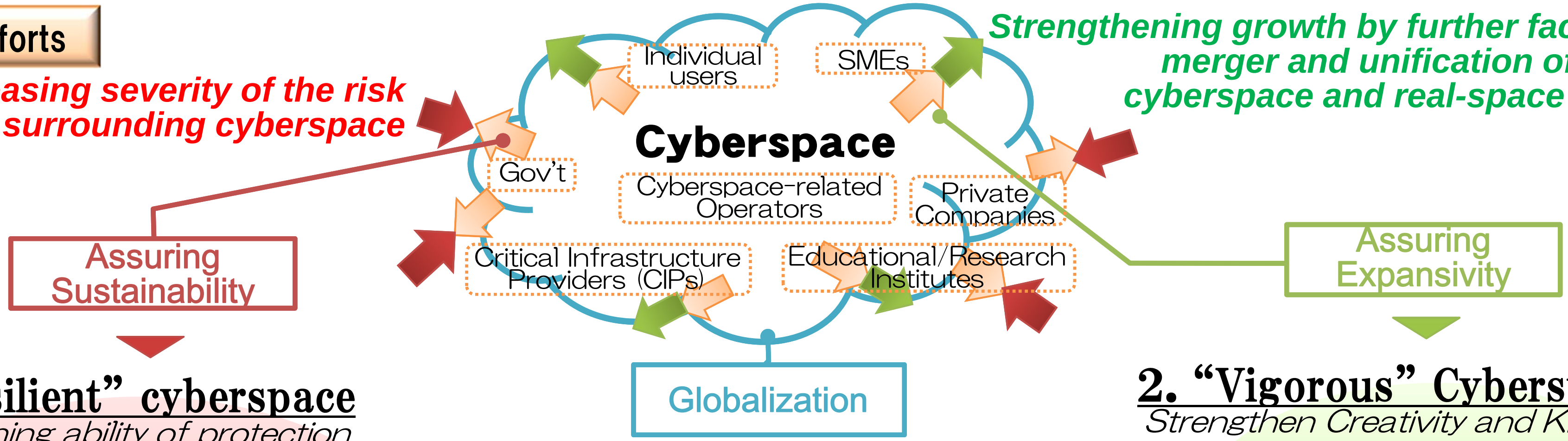
Basic Principles

① Assuring free flow of information
② New measures against increasing serious risk
③ Strengthening of risk based response
④ Actions and mutual cooperation considering shared responsibility

Areas of Efforts

Increasing severity of the risk surrounding cyberspace

Strengthening growth by further facilitating merger and unification of cyberspace and real-space



1. "Resilient" cyberspace

Strengthening ability of protection and recovery

①Measures in Gov't
②Measures in CIP
③Measures in Private companies and Educational/Research Institutes
④Hygiene of Cyberspace
⑤Crime countermeasures of Cyberspace
⑥Defense of Cyberspace

3. "World-leading" Cyberspace

Strengthening ability of contribution and outreach

①Diplomacy
②Global Outreach
③International Cooperation

2. "Vigorous" Cyberspace

Strengthen Creativity and Knowledge

①Activation of Industry
②Research and Development
③Human Resource Development
④Literacy Improvement

Promotion Systems etc.

Enhancement of the functions of NISC

1. Environmental Changes

Merger and integration of cyberspace and real-space

► widespread/sophistication, further progress, global expansion

Increasing serious risk surrounding cyberspace

► hugeness, diffusion, globalization

2. Basic Policy

(1) Vision to aim as a goal: ‘Realization of the Cyber Security Nation’

For national security/crisis management; social/economic development; and safety/security of public, realizing the society that is strong against cyber attacks, full of innovations and that its public will be proud of, through constructing the world-leading, resilient and vigorous cyberspace,

(2) Basic Principles

① Assuring free flow of information ► Ensure freedom of speech and privacy protection, and enjoy economic development etc.

② New measures against increasing serious risk ► Multi-layered efforts are necessary to respond to the changing risks promptly and precisely

③ Strengthening of risk based response ►Through dynamic response capabilities, strengthening of the response based on the risk characteristics is necessary.

④ Actions and mutual cooperation considering shared responsibility ► Each actor in multi-stakeholder needs to serve its role for proper mutual cooperation and assistance

(3) Roles of Each Actor

① Government ► Diplomacy, defense and crime countermeasures of cyberspace, strengthening the measures and preparations for coping with situations etc.

② Critical infrastructure Providers ► Strengthening the efforts within the current target 10 sectors, providing necessary measures to new sectors etc.
(10 sectors: ICT, Finance, Aviation, Railway, Electricity, Gas, Gov't/Gov't Services (incl. regional municipalities), Medical, Water, Logistics)

③ Private companies, Educational/research institutions ► Collective measures such as information sharing, industry - academia partnership for development advanced technologies and human resources etc.

④ Individual users, Small/medium-sized enterprises ► Fostering recognition of "Do not trouble others", self-governing measures such ad literacy improvement, and information sharing, etc.

⑤ Cyberspace-related operators ► Dealing with vulnerabilities in products etc., recognition and analysis of incidents, increasing the competitiveness in the global market etc.

3. Areas of Efforts

※About details on the efforts, see Cybersecurity Strategy (ISPC, June 10, 2013)

(1) Construction of “Resilient” Cyberspace

※GSOC: Government Security Operation Coordination team
CSIRT: Computer Security Incident Response Team
CYMAT: CYber incident Mobile Assistant Team

① Measures in Government: Strengthening measures in information systems etc. and preparations for coping with cyber attacks.

Ex.

- Construction of system base that is strong against cyber attacks by moving information systems into the government common platform cloud
- Emphasizing measures depending on the degree of importance etc. for information such as state secrets and information systems.
- Strengthening handling of critical info. on national safety by operators other than government, measures by independent administrative institutions etc.
- Increase capabilities of the GSOC to better detect and analyze incidents and share information between government agencies
- Strengthening system to share info. and respond incidents in government by strengthening of cooperation between CYMAT and CSIRT etc.
- Strengthening preparation of coping with situations by implementation of the training every year for large-scale cyber attack situation etc.

② Measures in Critical Infrastructure Providers: Measures in accordance with the ones for government

Ex.

- Promotion of information sharing between critical infrastructure providers and cyberspace-related operators on such matters as cyber attacks
- Establishment of framework for sharing the incident information possessed by GSOC with critical infrastructure providers
- Development of the new "Action Plan" by re-considering the scope of critical infrastructure and measures in such providers etc.

③ Measures in Private Companies and Educational/Research Institutions: Strengthening of recognition and information sharing of incidents, promotion of building CSIRTs and performing exercises

Ex.

- Increase the ability that medium/small-sized companies recognize cyber attacks, by considering incentives to promote investment in security
- Increase the responsive ability against cyber attacks of private companies by performing exercises using a practice test bed
- Increase the responsive ability to counter incidents by promoting the creation of CSIRTs in private companies and research institutions.

④ Hygiene of Cyberspace: Implementation of preventative measures that society as a whole participates

Ex.

- Promotion ensuring hygiene of cyberspace as a national movement by creation of "Cyber Clean Day" (tentative) etc.
- Building framework which ISPs can warn individual users that may access malicious sites.
- Considering flexible ways of operation in related systems, such as possibility of communication analysis for security purpose in consideration to the secrecy of communication etc.

⑤ Crime Countermeasures of Cyberspace: Strengthening of ability to cope with cyber crimes and preparations by utilizing knowledge from private sector etc.

Ex.

- Create Japanese NCFTA, and strengthening of the framework for information sharing with anti-virus vendors
- Considering ways of saving logs such as communication ones and measures to promote digital forensics by related operators and organizations

※NCFTA: National Cyber-Forensics and Training Alliance

(1) Construction of “Resilient” Cyberspace (cont.)

⑥ Defense of Cyberspace: Strengthening capabilities to defend Japan-related cyberspace from state-level cyber attacks

Ex.

- Organizing the roles of related organizations such as JSDF in such emergency situations as information systems of critical infrastructures are attacked, establishing of organizational structure and systems etc. that handle those situations, and arranging application of specific international laws.
- Strengthening capability and preparation of JSDF etc. to counter cyber attacks implemented as part of armed attacks.

(2) Construction of “Vigorous” Cyberspace

① Activation of Industry: Strengthening the global competitiveness of cybersecurity industry in Japan that is highly dependent on foreign products etc.

Ex.

- Participating proactively in the formation of international framework for international standardization, mutual recognition in assessment and certifications, and establishing an organization that assesses and certifies industrial control systems
- Aggressively procuring products etc. that utilize cutting edge technologies within government

② Research and Development: Creation of security technologies that are creative and imaginative to counter the changing risks

Ex

- Accelerating research and development of technologies for detection and advanced analysis for cyber attacks to hold and develop cutting-edge research and development
- Developing cutting-edge technologies to establish groundbreaking countermeasures against increasingly diverse and sophisticated cyber attacks such as hidden malware

③ Human Resource Development: Development of security professionals that are high-quality and with international talent

Ex

- Conducting by public-private cooperation training camps and competition contests of practical skills in order to explore individuals with great skills in software development, etc,
- Supporting the attending of international conferences and studying at graduate schools abroad in order to develop human resources that can compete globally

④ Literacy Improvement: Increase the literacy of the public

Ex

- Promote practical initiatives at elementary and secondary schools such as teaching information morals including information security and software programming, use of digital textbooks. Development of supporters to increase security awareness to the elderly
- Developing framework where individual users can recognize risks and determine its use on their own for smartphone applications

(3) Construction of “World-leading” Cyberspace

① Diplomacy: Multilaterally constructing and strengthening partnerships with such nations as share the same basic values

Ex.

- Continuously deliberating on how to apply specific international laws such as the Charter of the United Nations, International Humanitarian Laws for conducts in cyberspace.
- Deepening on discussions about details on how to deal with cyber sector and establishing international codes of conducts with the other countries such as the US.

② Global Outreach: Developing relationships that can grow together with such partners as ASEAN member states, and supporting responsive capabilities against cyber attacks

Ex

- Developing a network to collect information about cyber attacks by collaborating with other nations, then implementing research and development on methods for prediction and quick response of cyber attacks .
- Introducing success cases of botnet countermeasure projects that were conducted through public-private partnership, and conducting tabletop exercises, joint projects

③ International Cooperation: Strengthening to deal with incidents related to cyber attacks across borders in cooperation

Ex.

- Continuously exchanging information about cyber crime with foreign agencies, and sending officers for such purpose as strong collaboration
- Internationally communicate the basic stance of our nation in order to avoid contingency due mutual distrust, and building from peacetime contact channels, and implementing collaborative research projects and cyber exercises among plurilateral nations.

4. Promotion Systems etc.

- As for NISC (National Information Security Center), the necessary organizational structure such as authority will be developed and reorganized to establish "Cyber Security Center" (tentative) around FY2015.
- Developing framework that promotes the sharing of information related to cyber attacks between government agencies and critical infrastructure providers.
- Properly managing the specific mid and long term goals (FY2015 and 2020) to promote the efforts.

  Ex.

  - By FY2015, increase the coverage of cyber attacks related information sharing network in government agencies etc., decrease malware infection rates and citizen concerns, and increase the number of such nations as participating in international incident coordination
  - By 2020, double the size of domestic information security market, and decrease the lack of proportion in security professionals
- Targeting three years until FY2015, and Implementing development and assessment of annual action plans.
- Developing international strategy for cybersecurity.