Development and Challenges in Japanese Cybersecurity Policy

2018. 4. 5

Ryozo Hayahsi

Information Security Policy (Early Days)

- 1977: Successful Establishment of Computer& Semiconductor Industry through VLSI project
- Dominance in Semiconductor Industry
- Dominance in Machine Tool Industry
- Prevalence in High-Tech Product
- Vision of 80’s (Information Age)
- Integration of computer and telecommunication(MITI& MPT)
- 1980: Privacy Protection Guideline
- 1988:Privacy Protection Act

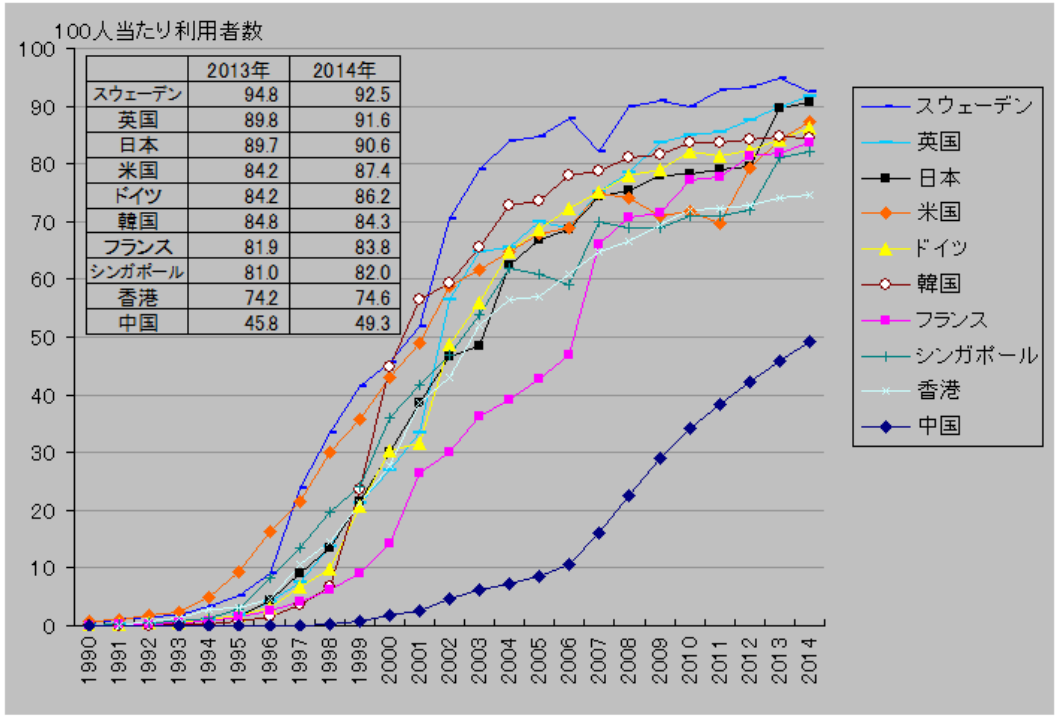
- IT power shifted to US due to software industry and network.
- 1992: OECD Security Guideline
- 1993: Internet Commercial Use
- 1993: IPAComputer Virus Registration System
- 1996 : Establishment of JPCERT/CC

- Major incidents were information leakage by fault or accidents.

- MITI & MPT assume basic responsibility.

Cabinet Headquarter for IT Strategy (2000)

インターネット普及率の推移(国際比較)



(注)人口に占めるインターネット利用者数の割合である。
(資料)世銀 WDI 2016.2.7(原資料はITU(International Telecommunication Union))
日本の値は総務省データ(図録6210参照)とは異なっている。

- Increase of internet user and injury
- 2000: IT Basic Act (MITI and MPT)
- Headquarter for IT Strategy (including security)
- E-Japan Initiative
- 2000: Unauthorized Access Law
- 2001: Electronic Signature Law
- 2001: Common Criteria
- 2002: OECD Cybersecurity Guideline
- 2003: Security Standard for Service

Establishment of NISC (2005)

- Further increase of incidents (Computer Crime & National Security)
- 2005: Cabinet National Information Security Center

1 Development of Strategy

2 Measures for government agencies

3 Response Capacity

4 Critical Infrastructure protection

5 International Strategy

- First National Strategy on Information security (2007)
- Basic Principle: Economy, Society, National Security
- Primary Goal: PPP model
- Priority policy: Government, Critical infrastructure, Business, Individual
- Cross cutting: Technology, Human resources, International, Crime

Enactment of Cybersecurity Basic Act (2015)

- 2007; Estonia
- 2009: Attack against Korea & US
- 2011: Mitsubishi Heavy
- 2011: Sony playstation
- 2011: Citi
- 2012: Nuclear regulation Authority
- 2013: Korean case
- 2013: National Strategies in US & EU
- 2014: Sony Picture Case
- 2015: White House Conference at Stanford

- 2015: Cybersecurity Basic Act (Smart devices, Organized Attack, Bot)
- 2015: New NISC (National center of Incident readiness and Strategy for Cybersecurity)

1 Basic Strategy Group

2 International Strategy group

3 Group for Government safety

4 GSOC & Information Gathering

5 Critical infrastructure

6 Analysis & Response

Cybersecurity Strategy (2015)

5 Basic Principles

- Free Flow,
- Rule of Law
- Openness
- Autonomy
- Collaboration among Multiple Stakeholders

Policy Approach

1 Socio-economic Vitality & Sustainability(IoT, Business)

2 Secure Society for people (Cyber crime, Critical infrastructure, Government)

3 Peace & Stability of International Community(Law enforcement , Selfdefence Force, International Cooperation)

4 Cross cutting issues (R&D, Human Resource)

New Threat & Necessary Response

Threat

- Wider Target
- Bigger Damages
- Smart Devices, Censor,
- More Sophisticated
- Critical Infrastructure
- More Global
- More Organized including State Sponsored
- Serious National Security Threat

Response

- Necessity of Holistic Approach
- Information Sharing Mechanism
- From Protection to Detection
- Swift Response
- Risk Management Approach
- NIST Framework
- Human Resource
- Global Response & International Cooperation

Evaluation of Response

General observation

- Japan was relatively quiet, but
- 2015.5 Japan Pension Organization
- 2015 US Public Service
- 2016.2 Swift Bangladesh
- 2016.5 ATM, Convenience Store case

Comparison with UK Strategy

- Strategy itself is built on bottom-up consensus of each ministry.
- Strong Economic Policy Centrism
- Few Strategic Taste
- Independent Ministries
- Segmentation Inside
- Japanese Government Culture
- Survived through Administrative Reform

Challenge Ahead

Effective Critical Infrastructure protection

- Vulnerability of Control System
- Use of common software platform
- Remote maintenance service
- Unprepared except Financial Sector
- Difficulty in Information Sharing
- Business, Regulatory, Legal
- Japanese Organizational Culture

Enhancing Preparedness of Business

- Management Unfamiliarity with IT
- Avoid Business Decision
- Shortage of Skilled Engineer
- Life time Employment
- Japanese way of Promotion
- Japanese Business Organization

Towards Future

Future Trend

- Speed of New Technology (IoT, Autonomous driving etc.)
- Continued Internet Vulnerability
- Basic Structure of Internet
- Economic Incentives
- Difficulty of Attribution
- Seamless Global Network
- Asymmetry between attackers and defenders

What is required?

- Holistic & Systematic Approach
- Crime or Terrorism or War (Investigation & Intelligence)
- Solid and Well Structured National Security Policy
- Balancing National Security and Economic Prosperity

Towards Establishing Effective Strategy

Cooperation & Leadership in Government

- Meiji Foundation of Japanese Government Structure
- Independent Ministry & Weak Prime minister
- Lifetime Employment & Turf
- Value of Information in Turf Battle : Control & Manipulation
- Few Experience in National Security Policy Coordination

Challenge

- Qualification for Cybersecurity Strategy
- Defense, Intelligence, Police
- Segmentation within Ministry
- Balancing economic consideration and National Security consideration
- Weakness of Japanese Defense Ministry (Segmentation & Self-Defense Principle)

Japan-ASEAN Cybersecurity Policy Meeting

- Establishment 2009
- Purpose: Increase Japanese FDI to ASEAN
- Capacity Building in ASEAN
- Building National CERT
- Low key
- Ministerial Meeting 2013

Country	GDP(mm&)	PerCapita
Burunei	114	26,939
Cambodia	200	1,270
Indonesia	9,323	3,570
Lao	159	2,353
Maleysia	2,964	9,503
Miyamer	674	1,275
Philipine	3,049	2,951
Singapore	2,970	52,961
Thailand	4,068	5,908
Vietnam	2,026	2,186

Collaboration Framework

- **1. Creating a secure business environment in the knowledge economy**
- **1.1. Sharing experience and establishing common methodology**
- **1.2. Pursuing policy research**
- **1.3. Strengthening emergency response capability in the private sector**
- **1.4. Support of human resource development**
- **1.5. Sharing experience in privacy protection**
- **1.6. Policy discussion toward increase of FDI and cross border business activities by creating secure business environment**

- **2. Building an environment for secure ICT use**
- **2.1. Building fundamental strengths to ensure ICT security**
- **2.2. Countermeasure against cyber threats**
- **2.3. Producing competitive and secure ICT products and services for the global market**
-
- **3. Government driven Information Security Strategy**
- **3.1. Government driven Information Security Strategy**
- **3.2. Strengthening alliance**

Japan-ASEAN Meetings

(Plenary)

- New Trend (Key note)
- Country Update
- Cooperation Report
- WG Report
- Summary Record

(Working Group)

- Joint Awareness Raising WG
- Critical Infrastructure Protection WG
- Capacity Building WG
- Cyber Exercise WG

(Others)

- CSIRTs

Observation & Insight

Characteristics

- Wide Difference of Economic development among ASEAN countries
- Different value System
- Different Structure of Government, Different Mandate
- Secretariat is weak
- “ASEAN minus” Approach
- Some countries are at war each other.
- Low key and economic policy approach

Towards Effective Cooperation

- Continuation of Pragmatic Approach
- Multiple Stakeholders Process
- Necessity of Deepened Cooperation
- Various Forum : Defense, Police, Intelligence, Regulatiory
- Maturity Model
- Economic Research Institute of ASEAN and Asia