KDDI Research Institute

Cybersecurity Strategy
&
Public privacy cooperation in Japan

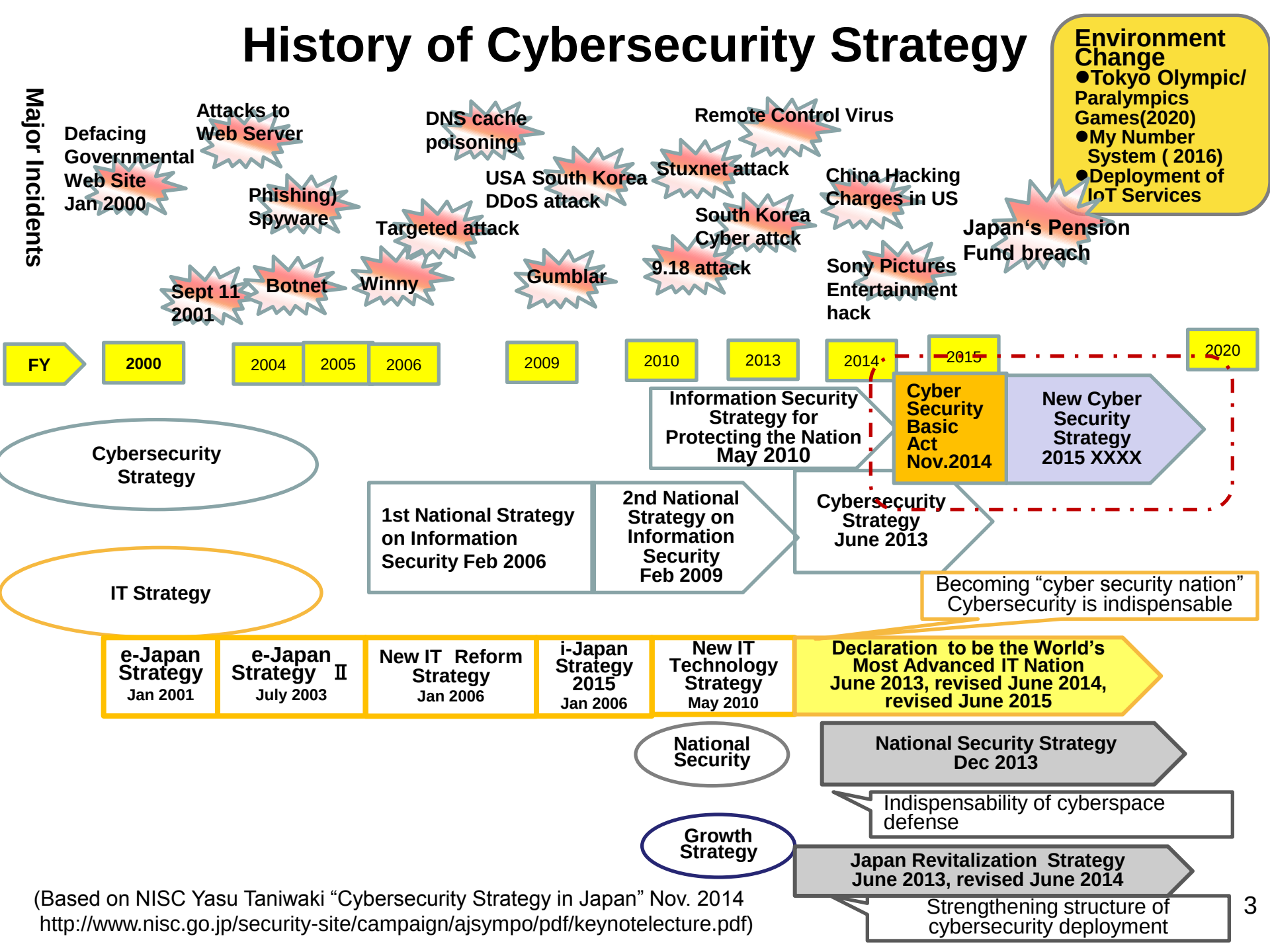
July 8, 2015

Hruo Takasaki
KDDI Research Institute
Chief Researcher

Haruo Takasaki

- **Chief Researcher, KDDI Research Institute, Inc.**
- **Research Field : Personal data and privacy protection**
- **Expert Member of ISO/SC27/WG5(ISO/SC27/WG5 (Identity Management & Privacy Technologies)**
- **ID-linkage Trust Framework Strategic Committee Member of METI (Ministry of Economy, Trade and Industry)**
- **Privacy by Design Ambassador**

History of Cybersecurity Strategy



(Based on NISC Yasu Taniwaki “Cybersecurity Strategy in Japan” Nov. 2014
http://www.nisc.go.jp/security-site/campaign/ajsympo/pdf/keynotelecture.pdf)

Cybersecurity Basic Act

- Passed Nov. 2014 (Effect in Jan. 2015)

- Definitions : Cybersecurity
  - Firstly described in law
  - Wide range definitions

- Objectives:

① Set up basic principles for cybersecurity policy (including active responses to cyber threats through cooperation among multiple stakeholders)

② Clarification of responsibility of central gov., local gov., critical infrastructure providers and educational research organizations

③ Formulation of Cybersecurity Strategy (CSS)

④ Establishment of Cybersecurity Strategic Headquarters in the Cabinet (drafting CSS, formulating common standards of information security measures for governmental organs or agencies and so on)

Framework for Cybersecurity Strategy Implementation

Strategic Headquarters for the promotion of advanced Information and Telecommunications Network Society (IT Strategy Headquarters)

Director-General : Prime Minister
Vice Director-Generals :
Minister in charge of Information Technology(IT) Policy
Chief Cabinet Secretary
Minister of Internal Affaires and Communications
Minister of Economy, Trade and Industry
Members : All other Ministers of Sate
Government Chief Information Officer (CIO)
Experts
(Secretariat)
IT Policy Office, Cabinet Secretariat
Office chief (Government CIO)

Views on CSS

Close Cooperation

Cybersecurity Strategic Headquarters (Established Jan. 2015)

Chair : Chief Cabinet Secretary
Deputy Chair : Minister in charge o IT Policy
Members : Chairman of the National Public Safety Commission
M inister of Internal Affaires and Communications
Minister of Foreign Affaires
Minister of Economy, Trade and Industry
Minister of Defense
Experts

special committee | special committee | special committee

(Secretariat)
National Information Security Center (NISC)

Director-General (Assistant Chief Cabinet Secretary
Deputy Director-General
Information Security Advisors

Government Security Operation Coordination Team(GSOC)
Cyber Incident Mobile Assistance Team(CYMAT)

Views on CSS

Close Cooperation

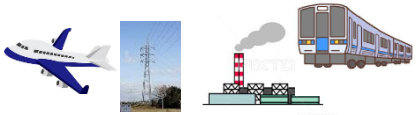
National Security Council

Ministers responsible for Critical Infrastructure Protection

FSA(Financial Services Agency) **Financial**
MIC(Ministry of Internal Affaires and Communications)
Local government, Telecommunication
MHLW(Ministry of Health, Labor and Welfare)
Medical, Water
METI(Ministry of Economy, Trade and Industry)
Electric, Gas, Chemical, Credit card, Petroleum
MLIT(Ministry of Land, Infrastructure, Transportation and Tourism) **Aviation, Railway, Logistics**

Close Cooperation

Critical infrastructure business, etc.



(Based on NISC Yasu Taniwaki "Cybersecurity Strategy in Japan" Nov. 2014)

Governmental Organizations

Cooperation

National Policy Agency
MIC
Ministry of Foreign Affairs
METI
Ministry of Defense

Companies

Individuals

New Cybersecurity Strategy（Draft version)

(Finalization after analyzing public opinions)

1. New Awareness of Cyber Space : “Unlimited Value Producing Frontier”

2. Goals :

- Improvement of Economic Society Dynamism
- Realization of society in which people can live in safety and securely
- Contribution to international peace and Japanese national security

3. Basic Principles

①Free flow of information ②Rule of law ③Openness ④Autonomy ⑤Multi Stakeholder Cooperation

4. Required Measures

Improvement of Economic Society Dynamism

- New Business Creation based on secured IoT system
- Security Minded Business Operation
- Business environment arrangement (Government Founds)

Realization of society in which people can live in safety and securely

- Cybercrime Control & awareness campaign
- Protection of critical infrastructure
- Projection of Governmental Organization

International peace and Japanese national security

- capacity strengthening of police & SDF
- Establishment of International Rule of Law
- International Cooperation

Cross Sectional Measures : ■ R&D Development (attack detection & defense capability)
■ Human resources development (Hybrid type experts)

5. Promoting Framework

- Public-private cooperation for cyber attack detection, analysis & countermeasures
- Close alliance among Cybersecurity Headquarters, National Security Council and Counter Major Terrorism Headquarters against highly skilled attacks
- Establishment of practical response system for Tokyo Olympic/Paralympics Games

Public Private Cooperation in Cybersecurity

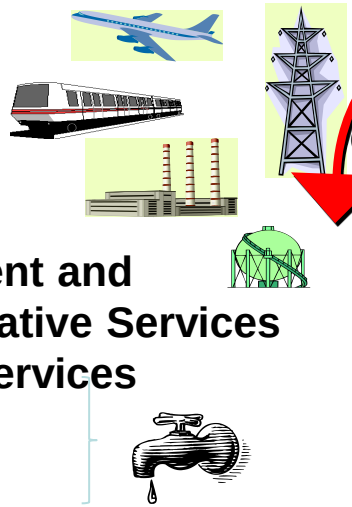
- **Cybersecurity Basic Act**
- **Government shall take necessary actions for facilitating active responses to cyber threats through cooperation among multiple stakeholders including central gov., local gov., major infrastructure providers and other cyber business providers.**

- **New CSS**
- Facilitate security minded management in business management layers (introduction of Chief Information Security Officer)
- Strengthen response ability through information sharing about latest incident information, threat analysis and best practices.
- For cybersecurity of major infrastructures(13 business fields), central governments and business providers shall cooperate for incident information sharing and active cooperation for the prevention of damage expansion.
- Development of human resources enhancing management capabilities
- Facilitate common value recognition towards “Security by Design”

Cybersecurity Measures for Critical Infrastructures

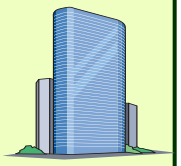
Critical Infrastructure（13 Sectors）

- Information and Communications
- Finance
- Aviation
- Railways
- Electricity
- Gas
- Government and Administrative Services
- Medical Services
- Water
- Logistics
- Chemistry
- Credit Card
- Petroleum



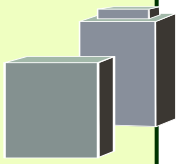
Coordination and Cooperation through NISC

Critical Infrastructure Sector-Specific Ministries



- FSA [Finance]
- MIC [Telecom and Local Gov.]
- MHLW [Medical Services and Water]
- METI [Electricity, Gas, Chemistry, Credit and Petroleum]
- MLIT [Aviation, Railway and Logistics]

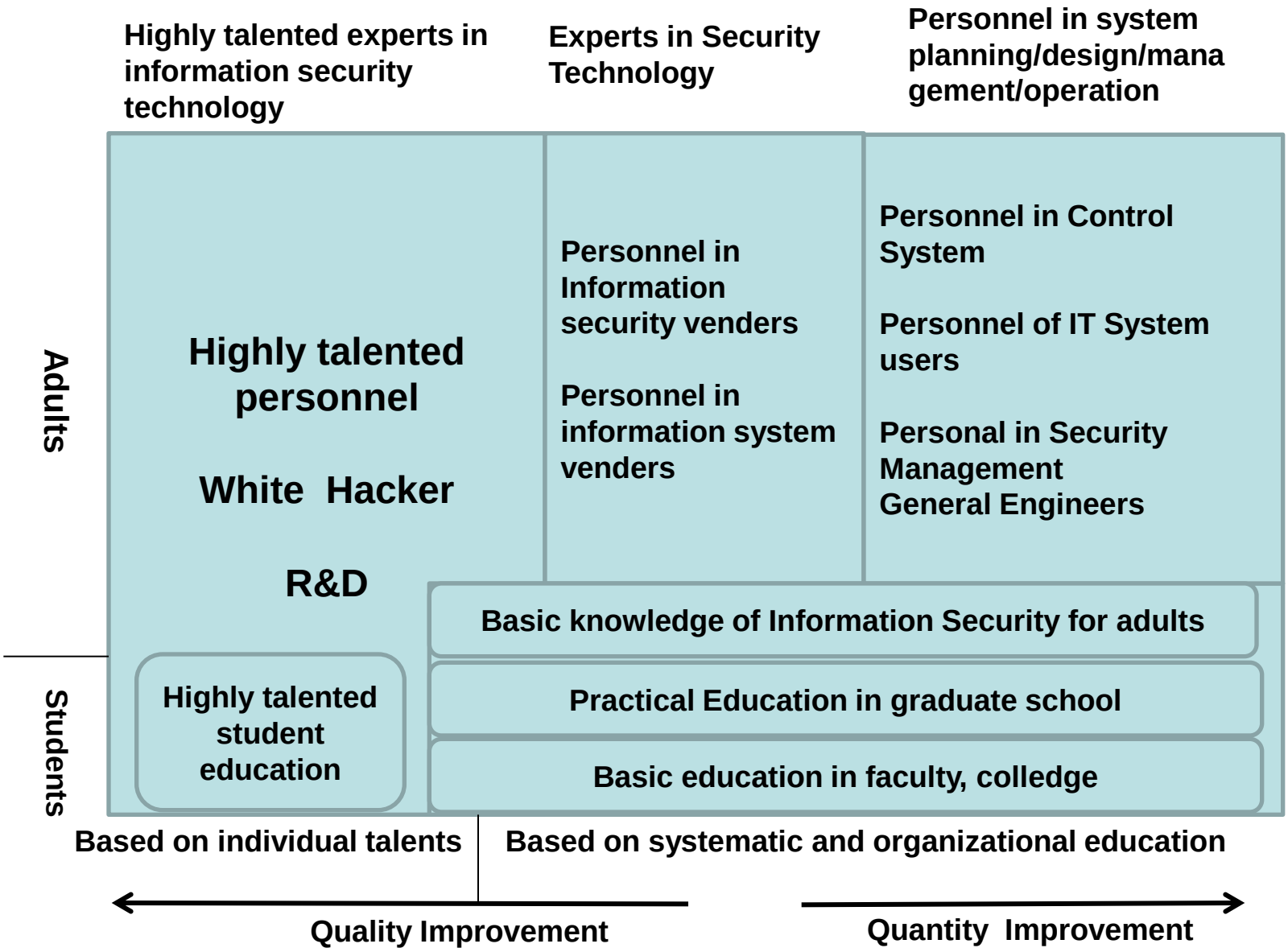
Related Organizations etc.



- Information Security Related Ministries
- Law Enforcement Ministries
- Disaster Management Ministries
- Other Related Organizations
- Cyberspace Related Operators

(Based on NISC Yasu Taniwaki “Cybersecurity Strategy in Japan” Nov. 2014)

Human Resource Development



(Based on METI Report Sept 2012
http://www.meti.go.jp/committee/sankoushin/jouhoukeizai/jinzai/pdf/report_001_00.pdf)

Hospitality and Security

OMOTENASHI

Tokyo 2020

Thank you very much for your attention!