

# Comprehensive Strategy on Information Security: Executive Summary

To enhance competitiveness and national security for Japan:

Building economic and cultural power through realization of world-class "highly reliable society"

With the use of IT as social infrastructure and the emergence of risks in new dimensions, the "Comprehensive Strategy on Information Security" will be launched not merely as a defensive approach in reducing risks but in order to utilize Japan's strengths in safety and security for the purpose of enhancing the competitiveness of the Japanese economy and boosting national security comprehensively. The "Comprehensive Strategy on Information Security", fully reflecting the distinctive characteristics of our country, will also be implemented steadily through cooperation between the government and the private sector.

## **Chapter 1 Approaches**

### **1.1 Assessment of Current Status: IT as "Nervous System" of Society**

- \* The rapid dissemination of information technology (IT) has led not only to dramatic increase in the use of PCs, the Internet, and mobile telephones and the spread of e-commerce, but expanded to establishment of IT as socioeconomic infrastructure and as a major component in the "lifelines" propelling activities in society.
- \* Firstly, IT equipment and software have integrated almost invisibly into control and management of the foundation of socioeconomic activities, including finance, energy, transportation and medicine. IT now plays a vital role as the "nervous system" for various social systems.
- \* Secondly, business activities are integrating rapidly through introduction of IC tags and development of inter-industry databases, transcending corporate boundaries and forming the "nervous system" for the full spectrum of corporate activities by communicating and sharing important information. Action is under way for greater optimization in allocation of resources.

### **1.2 New Dimensions of Risks Confronting Society as a Whole**

With establishment of IT as social infrastructure, risks of new dimensions have emerged in the area of information security. From the historical perspective, this is a period of major transition amid spread of the third Industrial Revolution (by IT and other advanced technologies).

#### **(1) Growing risks**

- \* The first point is the growth of risks. Risks involve not only information system failures, malicious assaults from within and by external parties, and problems for perpetrators and victims of failures, but also risks leading to panic of the entire national economy and to threats on lives and assets of the people.

#### **(2) Change in nature of risks**

- \* The second point is the change in nature of risks. Characteristics of risks have changed with IT used as "black box" technology without open scrutiny, diversification of IT applications, change in technological innovation and business models, and growing obscurity as to where responsibility for failures lies.

#### **(3) Action on these new risks and issues viewed from the perspective of national security**

- \* Rather than developing measures for each specific issue, studies must be conducted to develop

measures for the development of a "self-recoverable" social system prepared for accident/incident occurrences with the capability to recover and to minimize and localize damage on the assumptions that (1) risks for the nation as a whole must be minimized and (2) "information security is never guaranteed and accidents happen."

- \* At present, there have been no major system incidents or accidents that might break down economic activities or threaten the lives and property of the Japanese people. However, the Japanese government and critical infrastructure bodies are well aware of the threat of cyber-terrorism and should select the best possible measures for security in view of the facts that (1) new risks could include the possibility of assault by all kinds of perpetrators, ranging from individuals seeking pleasure in wreaking havoc to organized crime syndicates and terrorists, with similar methods, and (2) introduction of IT in government and critical infrastructure systems is unavoidable in order to enhance international competitiveness and user convenience, although all government is now moving slowly and with great caution in connecting its systems to the Internet and in the use of IT in its systems.
- \* The issue of information security should not be only pursued for the safety of "economic activities" but is an issue that requires scrutiny on the national level for Japan's own national security.

### **1.3 The Need for Comprehensive Information Security Strategy**

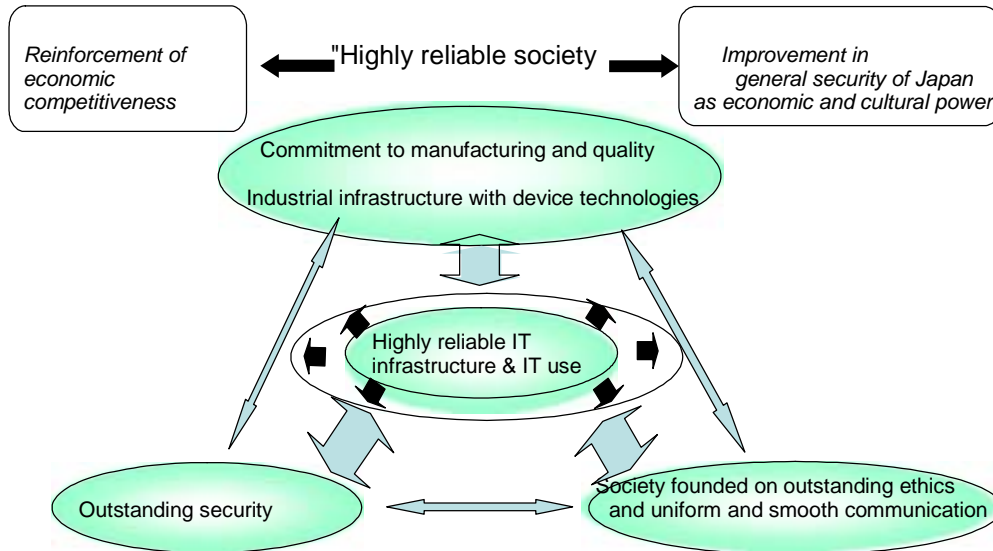
#### **(1) Failure of ad hoc measures implemented to address specific issues and problems**

- \* Until now, measures to assure information security have been issue-specific, targeted only to resolve the problem at hand, for measures implemented by business enterprises and private individuals, as well as the Japanese government. Measures have been executed from specific perspectives only.
- \* In view of the drastic changes in society and qualitative change of risks, measures must be examined exhaustively. It is necessary to launch a "Comprehensive Strategy on Information Security" with full attention to circumstances in Japan and to implement it through cooperation between the government and the private sector.

#### **(2) Competitiveness through development of a "highly reliable society" and improvement of comprehensive security**

- \* In view of Japan's aspiration to exercise international leadership through economic power and cultural assets ("soft power"), rather than arms and military power, the development of a world-class "highly reliable society" founded on solid information security deserves to be regarded as the foremost national strategy.
- \* Firstly, a "highly reliable society" founded on solid information security brings greater economic competitiveness for Japan. In other words, it provides the basis for maximizing the benefits brought about by transition from an "industrial economy" competing on material affluence to "information economy" determined by skill in utilizing knowledge and expertise. By means of structural reduction of the risk premium, Japan will be able to attract foreign investment. Moreover, cost cutting and better efficiency can be realized in a variety of aspects, notwithstanding rapid aging and a declining population. It can also link to growth in employment.
- \* Secondly, development of a "highly reliable society" founded on solid information security not only prevents cyber-terrorism but contributes to securing stable energy supply and food supply and ultimately to comprehensive national security.
- \* Thirdly, "highly reliable society" is an area where Japan can exercise its strength. By taking advantage of Japan's commitment to "quality" in hardware and software for both suppliers and consumers and the potential it possesses in its technical foundation in the area of electronic devices, etc., Japan will be able

to become the world-class "highly reliable society"



**Figure: Structure of Society of "highly reliable society"**

## **Chapter 2: The Three Strategies for Reinforcing Information Security**

"Development of the world-class "highly reliable society" utilizing the strengths of Japan as an economic and cultural power is established as a basic goal. Three strategies regarding key information security measures are presented, aimed at shifting from problem-specific solutions to prioritized and strategically allocated reinforcement of resources for the nation.

### **2.1 Strategy 1: Development of Self-recoverable "Social System Prepared for Accident/Incident Occurrences" (Assurance of Outstanding Recoverability and Localization of Damage)**

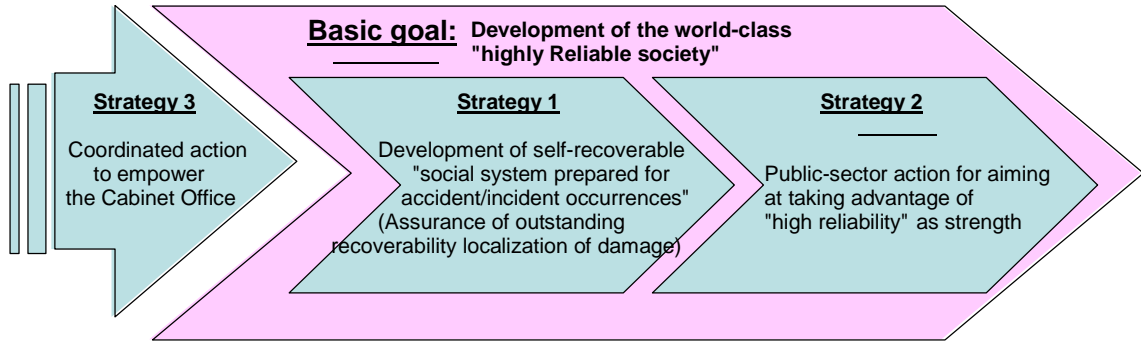
- \* Rather than focusing strictly on preventing accidents or addressing accidents that have occurred, a mechanism for outstanding recoverability and minimizing and localizing, i.e., a self-recoverable social system prepared for accident/incident occurrences must be developed on the assumption that information security is never guaranteed, and accidents happen.
- \* Based on this understanding, measures must be established and reinforced for both prevention of accidents and ex post facto action.

### **2.2 Strategy 2: Public-sector Action for Aiming at Taking Advantage of "High Reliability" as Strength**

- \* Public-sector action from the perspective of national interest should be reinforced in order to boost Japan's relative superiority in "high reliability", while utilizing Japan's basic strength in safety and security.
- \* For this purpose, the measures under Strategy 1 are to be implemented without fail. In addition, the Japanese government must take aggressive action in development of a technical and administrative foundation that leads to assurance of "high reliability" to enable Japan to wield its strength and to support information security such as formation of ICT infrastructure without too much dependence or centralization on specific technology and creation of a legal framework against cyber-crimes.

### **2.3 Strategy 3: Coordinated Action to Empower the Cabinet Office**

- \* In order to realize Strategy 1 and Strategy 2, an integrated organization that enables accurate management of the general portfolio is necessary.
- \* For this purpose, the Cabinet Office organization should be expanded drastically for aggressive promotion of measures and consolidated action to realign redundant operations under its leadership.



**Figure: The Basic Goal of the Three Strategies for Reinforcement of Information Security**

## **Chapter 3 Concrete Measures under the Strategies**

### **3.1 Strategy 1: Development of Self-recoverable Social System Prepared for Accident/incident Occurrences (assurance of outstanding recoverability and localization of damage)**

#### **(1): Reinforcement of Preventive Measures**

##### **(1) Preventive measures by national/local governments and critical infrastructure bodies**

###### **(National/local governments)**

- Review of information management systems, alongside technology development and system configuration
- Use of security standards for IT products, encryption, etc., in system procurement
- Information security audit and promotion of ISMS certification

###### **(Critical infrastructure bodies)**

- Information security audit
- Information security technology development against cyber-terrorism

##### **(2) New preventive measures in business enterprises and among private individuals**

###### **(Measures to address vulnerabilities)**

- Establishment of rules and systems to address vulnerabilities
- Development of functions providing alerts on computer viruses, etc.

###### **(Advanced manpower development)**

- Review of training methods for information security specialists and field personnel
- Review of approaches to be taken for professional certification system
- Security technology engineer training at organizations dealing with security incidents
- Enhance information security research and manpower

###### **(Improvement of security literacy)**

- Awareness promotion by the government
- Security literacy education from compulsory education level
- Reinforcement of security training for corporate managers and employees
- Development of an environment offering worry-free use of secure IT products and services by private individuals

### **(3) Reinforcement of existing preventive measures from the aspects of technology and security management**

#### **(Promotion of technological assessment and technology development)**

- (a) Promotion of IT security assessment & authentication systems
- (b) Reinforcement of encryption security assessment
- (c) Development of technologies, products and services for greater security
- (d) Establishment of secure information distribution system based on encryption and authentication technologies

#### **(Promotion of security management)**

- (e) Information security audit and promotion of ISMS certification
- (f) Review of approaches to be taken to information security rating
- (g) Review of general alignment of domestic standards and benchmarks related to information security

### **3.2 Strategy 1: Development of Self-recoverable "Social System Prepared for Accident/Incident Occurrences" (Assurance of Outstanding Recoverability and Localization of Damage). (2): Exhaustive Reinforcement of Measures on Accidents**

#### **(1) Measures on accidents by national/local governments and critical infrastructure bodies**

##### **(National/local governments)**

- (a) Review and establishment of information-sharing and information use systems in national and local governments
- (b) Development of guidelines on service preservation/recovery planning

##### **(Critical infrastructure bodies)**

- (c) Information sharing and use among ministries/agencies related to information system incidents, and establishment of study committee on incidents
- (d) Cyber-terrorism drills and training
- (e) Establishment of information-sharing system for critical infrastructure
- (f) Development of guidelines for service preservation/recovery planning

#### **(2) Measures on accidents by business enterprises and private individuals**

- (a) Establishment of information sharing, use and cooperation organizations among IT businesses
- (b) Development of guidelines for service preservation/recovery planning
- (c) Development of methods for quantitative assessment of risks
- (d) Review of methods for reducing damages, including insurance feature
- (e) Review of legal issues pertaining to information security

### **3.3 Strategy 2: Public-sector Action for aiming at taking advantage of "high reliability" as Strength**

- (a) Solid promotion of Strategy 1
- (b) Formation of ICT infrastructure to avert risks of centralization and unilateral dependence (such as operating systems and GPS)
- (c) Government/private sector cooperation against cyber-crimes and review of approaches to personal data protection adapted to new technologies
- (d) Sophistication of software manufacturing technologies
- (e) Establishment and practical application of secure programming methods
- (f) Reinforcement of industrial structure related to devices and other basic technologies

## **Chapter 4 Organization and Process Management for Realization of the Strategy**

### **4.1 Strategy 3: Coordinated Action to Empower the Cabinet Office**

#### **(1) Reinforcement of Cabinet function**

- \* **Reinforcement of Cabinet organization and workforce and promotion of change as an organization with the following functions**
  - \* Development of organization for comprehensive gathering of accident data from national and local government organizations and critical infrastructure bodies
  - \* Planning technology development, etc., to support preservation of confidentiality in national and local governments
  - \* Security audits and penetration tests, etc., for various government organizations, function as liaison office for the government as a whole, etc.

#### **(2) Development of consolidated promotion organization**

- \* For measures in which cooperation between the national government and private enterprises is important, distribution of roles and method of coordination should be identified clearly for Japan. For integrated implementation of government measures and programs, an "Information Security Policy Committee" consisting of information security policy officers from various government organizations should be established under the Cabinet Office.

### **4.2 Time Frame for Actions**

- \* Milestones to be established for each policy.

### **4.3 Assessment Mechanism for Strategy**

- \* The state of strategy implementation to be evaluated by "Security Policy Advisory Council" consisting of experts.

## Activity Log

### \* Information Security Group

June 13, 2003                      First Meeting  
Basic perspectives in development of comprehensive strategy  
September 3, 2003                Second Meeting  
Draft summary of Comprehensive Strategy on Information Security  
October 7, 2003                    Third Meeting  
Proposal of Comprehensive Strategy on Information Security

### \* Research Group on Development of Comprehensive Strategy on Information Security

May 14, 2003                      First Meeting  
Organization of points of deliberation  
May 29, 2003                      Second Meeting  
Basic policy for review  
Image of risks pertaining to information security  
June 12, 2003                      Third Meeting  
Procedure for review in Comprehensive Strategy planning  
Proposal of reference materials for the first meeting of the Information Security Group  
July 1, 2003                        Fourth Meeting  
Organization of points of deliberation  
General image of issues in information security  
Critical infrastructure security  
August 8, 2003                      Fifth Meeting  
Perspectives for the Strategy  
Key issues and measures for realization  
September 8, 2003                Sixth Meeting  
Draft proposal of the Comprehensive strategy on Information Security  
October 2, 2003                    Seventh Meeting  
Proposal of the Comprehensive strategy on Information Security