Concerning Sumitomo Chemical Systems Service's Initiative on the Personal Information Protection Act

Sumitomo Chemical Systems Service Co., Ltd.
Hiroshi Nishikawa
Toshinori Goto
Toshiko Satomura

The Personal Information Protection Act, which implements the 8 Principles of the Privacy Guidelines of the Organization for Economic Co-operation and Development (OECD), went into full effect in April 2005. The background and requirements of the Act are outlined. Then will be explained the direction with respect to the Act for this company, which is in the business of handling personal information; each process for dealing with the "Security Management Measures" enacted by this company referring to the Ministry of Economy, Trade and Industry's guidelines; and the "Compliance Program".

This paper is translated from R&D Report, "SUMITOMO KAGAKU", vol. 2005-Ⅱ.

Introduction

Twenty-five years ago, on September 23, 1980, the "OECD Privacy Guidelines" were adopted by the Board of Directors of the Organization for Economic Co-operation and Development (OECD). Eight principles are described in the "Recommendations Pertaining to Privacy Protection and International Distribution of Personal Data." These principles are referred to as the "OECD 8 Principles," as shown in **Table 1**. They serve as the basis for the personal information protection policies of many countries, including Japan. In Japan, the "Five Laws Pertaining to Personal Information Protection" were enacted in May 2003 after going through numerous re-evaluations and revisions. It can be said that, at this point, the personal information pro-

Table 1 OECD 8 Principles

Collection Limitation Principle	There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
Data Quality Principle	Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
Purpose Specification Principle	The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
Use Limitation Principle	Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the Purpose Specification Principle except : (a) with the consent of the data subject; or (b) by the authority of law.
Security Safeguards Principle	Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.
Openness Principle	There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
Individual Participation Principle	An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him (i) within a reasonable time; (ii) at a charge, if any, that is not excessive; (iii) in a reasonable manner; and (iv) in a form that is readily intelligible to him; (c) to be given reasons if a request made under sub-paragraphs (a) and (b) is denied, and to be able to challenge such denial; and (d) to challenge data relating to him and, if the challenge is successful to have the data erased rectified completed or amended.
Accountability Principle	A data controller should be accountable for conforming with measures which give effect to the principles stated above.

tection law system has been established not only for government agencies but also for the private sector. Among these five laws, the law pertaining to private enterprises is referred to as the "Law Pertaining to Personal Information Protection" (Law No. 57, 2003). It is commonly known as the "Personal Information Protection Act."

Each provision of the Personal Information Protection Act stipulates the duties of the "personal information handling organization" based on the OECD 8 principles. Accordingly, it has been decided that each relevant ministry and office shall set guidelines for each business area, considering that the following factors vary depending upon the business area: definitions of the terms used in the provisions; interpretations of the duties to be complied with; the realistic degree of actual implementation; and methods of implementation. The Ministry of Economy, Trade and Industry (METI) released the "Guidelines for Economy, Trade and Industry"[1] in October 2004. Subsequently, the Personal Information Protection Act went into full effect on April 1, 2005 with the Cabinet's decision regarding the "Basic Policy for Personal Information Protection"[2] in April 2004.

Sumitomo Chemical Co., Ltd. and Sumitomo Chemical Systems Service Co., Ltd. (hereinafter referred to as "our company") handle "Personal Information Databases," which systematically structure "personal information" that has been defined by the Personal Information Protection Act. Therefore, both companies fall under the category of "personal information handling organizations" as defined by the law described later in this paper. Moreover, our company has been entrusted to systematically manage the "personal information" of Sumitomo Chemical, which establishes our relationship as a client and a consignee. The Personal Information Protection Act stipulates that a consignor is obligated to supervise the consignee pertaining to personal information (Article 22). For that reason our company is not only obliged to comply with the law but is also subject to the supervision of Sumitomo Chemical as a consignee.

Since around October 2004, our company began discussing measures to ensure compliance with the Personal Information Protection Act, which was to be fully enacted half a year later. In Chapter 4 of the Personal Information Protection Act, the "duties imposed upon personal information handling organizations" are stipulated. These duties can be roughly classified into two areas: the "security management measures" regarding data security; and the "compliance program," by which a company guarantees the clear specification of the purpose of data collection and the accuracy of the data. Both areas are described in the Ministry of Economy, Trade and Industry's guidelines.

The section entitled "Articles/Standards that Can Be Used by the Personal Information Handling Organizations to Appropriately and Effectively Carry out Their Duties" has been created in the guidelines. The section states, "It is desirable that each personal information handling organization individually devises its own compliance program in order to protect personal information in accordance with its operational scale and business activities; and then to implement, manage and improve such programs." It further states, "Upon establishing such a compliance program, the Japanese Industrial Standard JIS Q 15001, 'Requirements for Compliance Program on Personal Information Protection,'[3] can be referred to. For implementation of the security management measures regarding personal data, JIS X 5070, 'Evaluation Criteria for IT Security,'[4] and JIS X 5080, 'Code of Practice for Information Security Management,'[5] can be referred to."

JIS X 5080 is a standard established by modifying the international standard ISO 17799 for the security management of information systems to suit the Japanese standard JIS. Therefore, in order to actually implement the "security management measures" as demanded by the Personal Information Protection Act, it is appropriate to use the ISMS (Information Security Management System) method as a foundation. Moreover, JIS Q 15001 is the so-called "Privacy Mark" system. This management system has a background in common with the ISO 9000 and ISO 14000 standards. Our company obtained the QMS (Quality Management System) based on ISO 9000 in 2001 and the ISMS based on the ISO 17799 in 2004.

In this paper the Personal Information Protection Act shall be summarized first. Then we will report on our approach to the "security management measures" and "compliance program," as demanded by the guidelines.

Personal Information Protection

Accompanied by the further development of information technology in the economy and society, large volumes of personal information have been collected and processed through computers and networking sys-

Table 2 Personal Information Leak Incidents

Discovered	Organization	Records	Content	Cause	Compensation per person
Jun.03	Lawson	560,000	Card member information	Internal crime?	¥500
Jul.03	Ricoh	60,000	Family registry information tape	Lost in transit by courier	?
Aug.03	A-Plus	80,000	Member information	Removed by contractor employee?	¥1,000
Oct.03	Family Mart	180,000	E-mail newsletter subscribers	Removed by employee or contractor employee?	¥1,000
Jan.04	Sanyo Shinpan	1,160,000	Loan balance	Employee participation?	case-by-case
Feb.04	Yahoo! BB	4,520,000	Subscriber information	ID, password left out	¥500
Mar.04	Japanet Takata	300,000	Customer list	System development company?	?
Apr.04	Cosmo Oil	2,200,000	Card member information	Leaked by insider?	?
May.04	Mitsubishi Materials	1,100	Online customer information	Inadequately protected web page	?
Oct.04	Mie Prefectural Library	133,000	User information	Contractor employee removed without permission, stolen PC	?
Nov.04	Rihga Royal	12,000	Guest information (including credit card)	Stolen PC	?
Feb.05	NTT Docomo	25,000	Customer list	?	?
Mar.05	Club Tourism	90,000	Subscriber information	Unauthorized access	?
Apr.05	Michinoku Bank	1,310,000	Subscriber information (including bank account information)	Incorrect disposal?	?
May.05	Kakaku.com	22,000	E-mail addresses	Unauthorized access	?
Jul.05	Rakuten Ichiba	36,000	Subscriber information	?	?

tems. The volume of personal information processed will continue to expand in the future, in keeping with this trend. However, it can cause unrecoverable damage to an individual if his personal information is mistreated. Some of the incidents in recent years involving the leakage of personal information are shown in **Table 2** (source: IT Insurance Dot Com and others). In an information society, it is inevitable to distribute personal information. Thus, the majority of OECD member countries have implemented personal information protection laws in conformance with the OECD 8 Principles mentioned previously. In Japan as well, the Personal Information Protection Act was established and promulgated in May 2003. It is comprised of two sections: One is the basic law that stipulates the principles of personal information protection in both the private sector and government sector; the other is the general law that stipulates the duties to be carried out by private enterprises. The Personal Information Protection Act went into full effect on April 1, 2005.

1. Contents of the Personal Information Protection Act

As shown in **Table 3**, the Personal Information Protection Act consists of six chapters. The purpose of this law is to protect each individual's rights and benefits with consideration for the validity of the personal information. Thus the law stipulates the basic philosophy (Article 3) and policies of the government (Article 7),

Table 3 Contents of the Personal Information Protection Act

Chapter 1. General Rules
— Purpose (Article 1)
— Definitions (Article 2)
  Personal information
  Personal information database
  Personal information-handling organization
  Personal data
  Own personal data
— Basic philosophy (Article 3)
Chapter 2. Responsibilities, Duties, Etc. of National and Regional Public Bodies
Chapter 3. Measures, Etc. Relating to the Protection of Personal Information
— Basic policies (Article 7)
Chapter 4. Duties, Etc. of Personal Information-Handling Organizations
  Section 1. Duties of Personal Information-Handling Organizations
  Section 2. Promotion of Personal Information Protection by Private Bodies
Chapter 5. Additional Rules
Chapter 6. Penalties

as well as other essential matters in regard to the measures. The law also clarifies the responsibilities, duties, etc., of national and regional public bodies (Chapter 2); moreover, it stipulates the duties, etc., of personal information handling organizations (Chapter 4).

While regulations pertaining to the duties of personal information handling organizations have been specified based upon the "Personal Information Protection Act for Government Agencies"[6] and the "Personal Information Protection Act for Independent Administrative Corporations"[7] for the public sector, those

related to the private sector have been specified based upon the "Personal Information Protection Act."

As described previously, each ministry has individually devised and released the guidelines to which the minister can refer when carrying out the law. When our company evaluates and discusses personal information protection measures, the law itself and the guidelines from the Ministry of Economy, Trade and Industry can be used as a framework for such measures.

2. Definition of Personal Information

In the Personal Information Protection Act, the terms "personal information," "personal data" and "owned personal data" have their own unique definitions. Because the duties imposed upon personal information handling organizations vary depending on the type of organization, precautions must be undertaken. In the METI guidelines each duty is explained in detail through the use of examples.

(1) Personal Information

"Personal information" is defined as the "information pertaining to a living individual," such that the information can identify a specific individual (including information that can be easily cross-referenced with other information to identify a specific individual). "Information pertaining to an individual" is defined as the information that is not limited to that which identifies one's name, gender and birth date, but also the information that expresses truth, judgment and evaluation pertaining to personal attributes such as physical characteristics, assets, occupation and occupational title. It includes the following information as well: information released as evaluation information; information released through publications; and information released through video and voice, regardless of whether it is encrypted or not encrypted.

For example, if our company uses addresses of the format tarou.yamada@sc-sss.co.jp, the address itself specifies "someone at SSS company." Therefore, it can be considered personal information. If the address style were something like S100.01@sc-sss.co.jp, it would not be considered personal information if no address/name listing existed.

(2) Personal Information Database

"Personal information database, etc." is defined as a body of information (including personal information) that is systematically structured so that any specific personal information can be searched using a computer. Or, in the event a computer is not used to search the information, it is defined as any personal information processed on paper, such as medical charts and guidance records, that are organized and classified according to a certain order (for example, alphabetical order or by date) by adding a table of contents, index and symbols to facilitate the search of any specific personal information conducted by any person.

(3) Personal Information Handling Organizations

The law classifies the "personal information handling organizations" into two categories: One is the "government" sector, which includes national organizations, local municipalities and independent administrative corporations; and the other is the "private" sector, as typified by providers of personal information databases. However, for the "private" sector, not all the enterprises that handle personal information are defined as "personal information handling organizations." The provision defines this exception as "excluding the organizations that may not significantly damage individuals' rights and benefits when considering the regulations, volume and usage of the personal information handled."

The criteria for this exception depend on the scale of the personal information database. Specifically, as stipulated in Article 2 of the Personal Information Protection Act: "It excludes the organization having personal information databases used for its own business that constitutes the data of fewer than 5,000 people (who can be identified by the personal information that is a component of the personal information database) on any day over the past six months. Whether the number of people who are subjects of the data exceeds 5,000 or not is determined by the total number of specific individuals who can be identified by the personal information constituted within the personal information database, etc., managed by this organization. However, duplicated data should not be counted."

Moreover, it also stipulates that the term "business" in the above provision is defined as actions that are similar to each other and conducted continuously and repeatedly for the same purpose. These actions are commonly accepted by society as "business." Therefore, it does not necessarily mean a profit-making business.

Sumitomo Chemical and our company handle a data-

base whose scale exceeds 5,000 people and the scale of this database qualifies us as "personal information handling organizations."

(4) Personal Data

"Personal data" is defined as data that comprises a "personal information database, etc." managed by a personal information handling organization.

(5) Owned Personal Data

"Owned personal data" is defined as the "personal data" in which a personal information handling organization has the authority to accommodate the following requests made by the individual whose personal data has been collected, or by his agent: disclosure, revisions, additions/deletions of the contents of the data; ceasing in the use of such data; elimination of the data; and ceasing in the provision of data to third parties.

3. Duties of Personal Information Handling Organizations

In Chapter 4 of the Personal Information Protection Act, the duties of personal information handling organizations are stipulated in articles 15 through 36. These provisions are established based on the OECD 8 Principles but are specified in greater detail to suit Japanese situations. **Table 4** depicts the relationship between the eight principles and the provisions. These duties can be roughly classified into two categories: One pertains to security management measures and the other pertains to compliance programs.

4. Security Management Measures

Of all provisions that stipulate the duties of personal information handling organizations, Article 20 merely describes the "security management measures" with the statement, "Personal information handling organizations must undertake necessary and appropriate measures for security management in order to protect the personal data they handle from being leaked, lost or damaged."

As previously described, the specific details of the necessary and appropriate measures vary depending on the business area. Therefore, the general standards are shown in the guidelines set forth by the Ministry of Economy, Trade and Industry. The guidelines state, "Personal information handling organizations must establish the security management measures in four

Table 4 Correspondence between OECD 8 Principles and the Personal Information Protection Act

	OECD 8 Principles	Duties of Personal Information-Handling Organizations
Purpose Specification Principle Use Limitation Principle	Purpose of collection must be made clear, and use of data must match purpose of collection. Must not use for other purposes without agreement of the data's subject and compliance with legal procedures.	— Must specify as precisely as possible the purpose of use (Article 15) — Must not handle beyond the scope necessary for achieving the purpose of use (Article 16) — Must not divulge to third party without obtaining permission from person concerned (Article 23)
Collection Limitation Principle	Should collect data by legal and fair methods after informing and obtaining agreement from the subject.	Must not collect data with deceitful or other unfair methods (Article 17)
Data Quality Principle	Data should fit the purpose of use and be accurate, complete, and up-to-date.	Must work to keep information accurate and up-to-date (Article 19)
Security Safeguards Principle	Data should be protected from loss, destruction, use, alteration, divulgence, etc. with reasonable measures to safeguard security.	Must take necessary measures to manage security. (Article 20) Must perform necessary supervision of employees and contractors. (Articles 21, 22)
Openness Principle Individual Participation Principle	Should make public the intent to collect data, indicating clearly the data's existence, the purpose for which it is to be used, and the manager responsible.	— Must give notice or make public announcement of the purpose of use when collecting data. (Article 18) — Must put the purpose of use, etc. in a state in which it can be known by the subject person. (Article 24) — Must disclose possessed personal data at the subject person's request. (Article 25) — Must perform corrections, etc. at the subject person's request (Article 26) — Must cease usage, etc. at the subject person's request. (Article 27)
Accountability Principle	Should permit persons to confirm the storage location and content of data about themselves, and guarantee a hearing for all complaints.	Must work to process complaints appropriately and promptly. (Article 31)

areas: organizational, human, physical and technical, in order to protect the personal data they handle from being leaked, lost or damaged. The organizations must undertake the necessary and appropriate measures, taking into account the extent of damage to the rights and benefits of the person due to the leakage, loss or damage of the personal data, as well as risks related to the nature of the business and the situation in which personal data is handled. Additionally, it is desirable that the organization undertakes the security management measures that suit the nature of the media on which personal data has been recorded."

To summarize the above, the guidelines stipulate that the security management measures must be undertaken in the following four areas: organizational, human, physical and technical.

(1) Organizational Measures

The guidelines state, "Organizational measures are defined as clarifying the responsibilities and authority of employees (see Article 21) in terms of security management, preparing and implementing the regulations and procedure manual for security management (hereinafter referred to as 'regulations, etc.'), as well as monitoring the implementation status of such measures." The guidelines specify the five items shown in **Table 5** as mandatory organizational measures.

(2) Human Measures

The guidelines state, "Human measures are defined as concluding non-disclosure agreements with employees regarding the personal data designated as confidential; and conducting education and training regarding such personal data." The guidelines specify the two items shown in Table 5 as mandatory human measures.

(3) Physical Measures

The guidelines state, "Physical measures are defined as managing entry to and exit from the building (data storage room) and protecting personal data from theft. The guidelines specify the three items shown in Table 5 as mandatory physical measures.

(4) Technical Measures

The guidelines state, "Technical measures are defined as technical security management measures undertaken for the protection of personal data, including the control of access to personal data and the information system that handles personal data, solutions for illegal software, and monitoring the information system. The guidelines specify the eight items shown in Table 5 as mandatory technical measures.

(5) Specifying Mandatory Measures

As described in the previous sections, the METI guidelines specify a total of 18 items in four areas as "mandatory" security management measures. There are several methods by which these mandatory measures can be implemented, and therefore the guidelines have listed desirable actions to be taken upon the fulfillment of these requirements. For example, in order to fulfill the second requirement, "Control of access to personal data," as described under "Technical Measures" above, the guidelines specify eight actions as the "desirable actions upon implementing control over access to personal data," including the following:

- Minimizing the number of employees that are permitted to have access to personal data
- Access control based on identification
- Protecting data from unauthorized access to the information system containing personal data (for

Table 5 Security Management Measures

Organizational Measures	1. Maintain an organization to enact personal data security measures	11
	2. Maintain and operate in accordance to rules established by personal data security measures	5
	3. Maintain a procedure for listing the handling status of personal data	2
	4. Evaluate, revise, and improve personal data security measures	3
	5. Deal with accidents and violations	2
Human Measures	1. Conclude closed contracts for employment and commission contracts.	2
	2. Perform education and training for workers.	3
Physical Measures	1. Manage building (office) entries and exits.	2
	2. Prevent theft, etc.	5
	3. Physically protect machinery and equipment.	1
Technical Measures	1. Identification and authorization of access to personal data	2
	2. Control of access to personal data	8
	3. Manage permission to access personal data	2
	4. Log access to personal data	2
	5. Measures against unauthorized software on information systems that handle personal data	3
	6. Measures for transport and transmission of personal data	2
	7. Measures for regression testing of information systems that handle personal data	2
	8. Monitoring of information systems that handle personal data	2

example, installing a firewall or router)

Although "control of access to personal data" is mandatory, it is required to undertake the necessary and appropriate measures that suit the situation. Therefore, as a specific procedure to implement the measure, any of the aforementioned eight actions can be chosen (multiple actions can be chosen at one time), or any actions that the company has specified other than these eight actions can be chosen. Furthermore, each numeric characteristic given at the far right column of Table 5 indicates the number of "desirable actions" listed for each mandatory measure.

5. Compliance Program

Next, we will describe the "compliance program" imposed by the law. To devise such a program, JIS Q 15001 (which is described in the METI guidelines) can be used as a reference. As shown in **Table 6**, JIS Q 15001 defines the "compliance program requirement issues" in Chapter 4. The first requirement is that a "representative of the organization must determine, implement and maintain the personal information protection policy." Among the duties established in Chapter 4 of the Personal Information Protection Act, if the items established by guidelines for security management measures are compared with JIS Q 15001, it can be said that the guidelines, with the exception of physical security measures and technical security measures, correspond with the compliance program requirements.

Table 6 Requirements for compliance program on personal information protection

4.	Compliance Program Requirements Issues
4.1.	General Requirements Issues
4.2.	Personal Information Protection Policy
4.3.	Planning
4.3.1.	Specification of Personal Information
4.3.2.	Legal and Other Criteria
4.3.3.	Internal Regulations
4.3.4.	Planning Document
4.4.	Implementation and Operation
4.4.1.	Organization and Operations
4.4.2.	Measures Concerning Collection of Personal Information
4.4.3.	Measures Concerning the Use and Disclosure of Personal Information
4.4.4.	Appropriate Management of Personal Information
4.4.5.	Rights of Subjects Concerning Personal Information
4.4.6.	Education
4.4.7.	Complaints and Consultation
4.4.8.	Compliance Program Document
4.4.9.	Document Management
4.5.	Audit
4.6.	Revision by Organization Representative

6. Approach to Violations of the Law

Article 34 of the Personal Information Protection Act stipulates, "When a personal information handling organization violates the regulations stipulated in articles 16 through 18, those stipulated in articles 20 through 27, or those stipulated in Section 2 of Article 30, the competent minister may recommend that the concerned personal information handling organization stop the illegal action or undertake the measures required to correct the illegal action if it is considered necessary in order to protect personal rights and benefits." Additionally, it defines "Orders" (Section 2) and "Emergency Orders" (Section 3). In Article 56 a penalty is determined for a party that has violated the orders specified in sections 2 and 3 as follows: "Penal servitude for less than six months or a fine of less than 300,000 yen shall be charged."

Whether or not a certain action is a violation of the law is determined by whether or not the personal information handling organization has undertaken necessary measures according to the guidelines. In other words, in the event a personal information handling organization has not conducted the "mandatory" measures it shall be deemed a violation of the law. In contrast, for the measures described as "desirable" in the guidelines, it shall not be deemed a violation of the law even though the personal information handling organization has not carried out such measures. However, it is important for a personal information handling organization to undertake as many security management measures as necessary in order to protect personal information.

Moreover, what must be kept in mind besides the penalties set forth by the law is the loss of public trust, the liability for large compensation claims, et cetera, that might result from information leaks, et cetera.

Our Company's Approach to the Personal Information Protection Act

Six months prior to the full enforcement of the Personal Information Privacy Act, our company has:

– completed the creation process of the compliance program, including the establishment of a system for program implementation, organizing the relevant regulations and education for employees and will begin implementing the program by the date

of full enforcement of the law (April 1, 2005)
- conducted risk assessments for the security management measures by re-evaluating the related systems and understanding the existing measures
- placed the highest priority on the security measures for the entire IT infrastructure and placed precedence on each individual measure, then conducted such measures according to the order of precedence

1. Personal Data and Owned Personal Data

The duties stipulated by the law vary according to the types of data handled by personal information handling organizations, being either unowned personal data or owned personal data. As **Table 7** depicts, while articles 15 through 31 are applied to owned personal data (shown by the solid line "B"), articles 15 through 23 are applied to personal data (shown by the solid line "A"). Additionally, Table 7 depicts the penalties for breach of the law.

In our company's case, when we serve only as a consignee handling the personal information from Sumitomo Chemical, we have no "owned personal data." However, since our company does have its own owned personal data, that being the personal information on our employees, we have decided to comply with all the duties stipulated by the law.

Furthermore, when we were consigned the handling of personal data owned by Sumitomo Chemical, we discussed with Sumitomo Chemical the role allocations after evaluating the necessary measures that must be undertaken by both Sumitomo Chemical and our company.

Table 7 Act Enforcement and Penalties

Art.	Contents	A	B	Penalty
15	Specification of purpose of use			
16	Limitations by purpose of use			
17	Appropriate collection			
18	Notification of purpose of use during collection			
19	Preserving accuracy of data contents			
20	Security management measures			
21	Supervision of employees			
22	Supervision of contractors			
23	Restrict disclosure to third parties			
24	Announcement of issues related to possessed personal data			
25	Openness			
26	Revision,etc.			
27	Cessation of use, etc.			
28	Reason explanation			
29	Procedure to address requests for disclosure, etc.			
30	Fees			
31	Personal information-handling organization complaint process			
32	Report retirement			
33	Advice			
34	Recommendations and instructions			
35	Restrictions on use of authority of competent minister			
36	Competent minister			

2. Implementing Security Management Measures

As described previously, there are two aspects to the "duties" stipulated by the law: the security management measures and the compliance program. This section of the paper describes the security management measures based on the ISMS.

Fig. 1 depicts the security management process. our company identified all "personal information databases" in use, then before devising execution management measures for each database, established two criteria, "database priority" and "standard for selecting execution management measures."

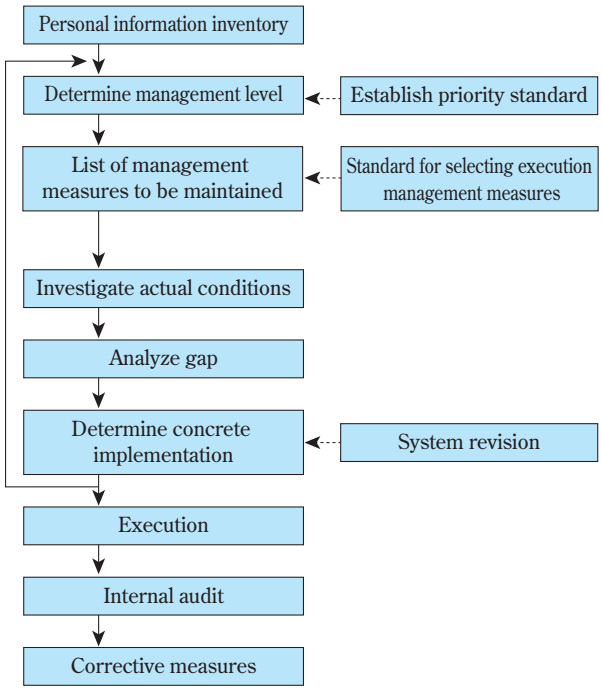

Fig. 1 Security Management Process

(1) Database Priority: Introducing the Priority Standard

The definition of "personal information" has already

been discussed in the previous section. In most cases a "personal information database" is comprised of information that identifies a particular person, such as the individual's name, as well as the data containing a particular person's attributes, such as physical characteristics, assets, occupation and occupational title. Therefore, we have established the priority standard by clarifying the attribute sets (i.e. data items) by listing the attributes (refer to **Table 8**). For the determination of data priority, we have decided that we shall take into account the possible extent of damage to the person's rights and benefits in the event there is a leak of such data. Our company has defined four priority levels from level "0" to "3," with level 3 being the highest.

Table 8 Relation of Priority to Database, Attributes

Priority	Example Database	Example Attribute
3	Health and treatment information	Physical exam results
	Economic impact information	Bank account number
2	Information revealing individual characteristics of person	Personnel evaluation, family structure, residence address
1	Information on persons outside the organization	Customer information, partner information
0	Information on persons inside the organization	Company e-mail address, telephone extension

(2) Establishing the Standard for Selecting Execution Management Measures

As shown in Table 5, in the METI guidelines the security management measures are classified into four categories and 18 mandatory measures are listed. This means that while all 18 mandatory measures must be undertaken by personal information handling organizations, only one or more optional measures given by the guidelines must be undertaken by these organizations. When implementing any of these measures, it is crucial for a personal information handling organization to consider the technical difficulty and cost of the measure, as well as its efficiency. For that reason we have established a standard to determine which "desirable management measures" suggested in the guidelines should be adopted. In the guidelines, eight items are listed as "mandatory technical measures," and of those eight items "identification and authorization for access to personal data" is listed first. Two desirable steps to conduct this mandatory measure are listed as shown in **Table 9**. Comparing these two steps, the first (identification performed through IDs and passwords) can be easily implemented in terms of cost and technology. On the contrary, the second step (identification performed on the terminal) has more technological and operational difficulties. Needless to say, the second step has a higher identification function. As our company's policy we have decided to adopt the first desirable step as the minimum measure for all systems. For the systems that operate personal information databases that require an extremely high level of security management (management level 3 or higher), we have decided to apply the second step along with the first step.

Table 9 Personal Data Access Identification and Authorization: Measures by Level

Issues that must be addressed	Desiable steps	Management Level
Identification and authorization for access to personal data	In order to confirm access to personal data is justified, carry out identification and authorization (e.g. ID and password authorization, biometric authorization, etc.) that user is worker with access permission.	0
	Perform identification and authorization on terminal or addresses (e.g. MAC address, IP address, electronic certification, secret decentralization technology, etc.) usable by workers with permission to access personal data.	3

(3) Personal Information Inventory

What our company did first, with respect to personal information inventory, was to go through all the personal information existing in both Sumitomo Chemical and our company and then create a registry. That registry compiles the contents of personal information as well as the names of the systems that store and utilize the information.

(4) Determining the System Management Level

A personal information database is comprised of several data items. For each data item the "priority level" has been defined as the standard. The data item having the highest priority of all the items comprised within a single database is deemed the priority level of the database itself. Moreover, since one system contains multi-

ple databases, the priority level of the database that possesses the highest priority level of all databases within the system is considered as the priority level of the system itself and is defined as the "system management level." We have calculated and organized the "management level" of all systems contained within the management registry.

(5) Establishing the Execution Management Measures

Based on the system management level and the standard for selecting execution management measures for the system concerned, lists of management measures were devised, with which the systems should be equipped.

(6) Devising Execution Management Measures

A survey was conducted to determine what kinds of management measures were undertaken for the target system. The differences (gap) between the result of this survey and the "management measures to be established" for the target system described in the above (5) have been examined.

(7) Gap Analysis

There was a gap between the reality and the management measures to be established. This gap falls under one of the following three categories:

(i) It matches the measures to be established for the target system (meaning that the measures suitable for the management level of the target system are already being undertaken).

(ii) Management measures to be established for the target system are not being carried out (meaning that the measures required for the level of the target system are not being undertaken).

(iii) The level of management measures is too high for the target system (meaning it is an over-specification).

(8) Selecting Measures to Be Undertaken

While it is not necessary to devise and undertake new measures when the results (i) and (iii) of the above gap analysis are obtained, it is necessary to do so when the result (ii) is obtained. However, if the management level of the target system can be reduced, this requirement can be eliminated. The management level of the target system can be reduced by eliminating the attributes of the personal information within the database that are subject to high management levels. Therefore, we first evaluated whether a particular attribute should be kept in the database. Then, according to this evaluation we selected the measure to be undertaken.

(9) Execution, Internal Auditing and Corrective Actions

An implementation plan shall be devised and executed for the particular measures to be undertaken. Additionally, progress management and internal auditing shall be conducted for the purpose of follow-up.

3. Organizational Measures and Human Measures

The guidelines specify five items as mandatory "organizational measures" and a total of 23 items as "desirable measures." For the "human measures" the guidelines specify two items as mandatory measures and five items as desirable measures.

Of the five mandatory organizational measures, particularly the one intended to "maintain an organization to enact personal data security measures," 11 desirable measures are listed. The following are among the desirable measures:

- Clarifying the roles and responsibilities of employees
- Clarifying the roles and responsibilities of each department involved in the handling of personal data

Because our company has already implemented most of the suggested measures within the scope of QMS, it was not necessary for us to devise other measures. However, considering the requirements specified by the guidelines for conclusions of employment agreement and consignment agreement, we re-evaluated these agreements. We also provided training to all the employees of our company, as well as for the employees of cooperating companies.

4. Compliance Program

Regarding the compliance program, as described in the previous section, the following requirements are equivalent to those of JIS Q 15001: all the duties of personal information handling organizations stipulated in Chapter 4 of the Personal Information Protection Act, except for the "Physical Measures" and "Technical Measures" in the security management measures stipulated in Article 20 of the law; and all other requirements stipulated in the Personal Information Protection Act, except for Article 20. Because our company

has already "documented the requirements" in the course of obtaining the QMS and ISMS, we have documented the requirements for JIS Q 15001 within the respective frameworks of QMS and ISMS. Moreover, we evaluated our compliance program equivalent to the "quality manual" of the QMS and found that it was well organized. Moreover, we compiled the requirements into the "Rules for Personal Information Protection." Finally, we applied the principles of the ISMS's management system in order to fulfill requirements other than those required by the Personal Information Protection Act. The limitations of space prevent us from detailing the relationship between the ISMS and the Personal Information Protection Act in this paper, but that relationship is described in the "ISMS Users Guide for Regulation Conformance"[8] released by the Japan Information Processing Development Corporation in April 2005.

Conclusions

This paper has mainly described our approach to the security management measures based on the guidelines set forth by the Ministry of Economy, Trade and Industry with respect to the Personal Information Protection Act.

1. International Trends

Though this paper has omitted any mention of the situations in overseas countries such as the U.S. and those of Europe, the countries of the European Union have stringent requirements. Therefore, if we neglect to undertake appropriate security management measures we might find ourselves being rejected in the global realm of information distribution. The security management measures with regard to personal information should be treated in the same way we treat the security of e-commerce.

2. Guidelines for Each Industry

Because the Ministry of Economy, Trade and Industry's guidelines aim to establish a standard for the entire industries, detailed procedures are not described. Therefore, in recent years guidelines developed for particular industries have been released. This is exemplified by the "Guidelines for Personal Information Protection for Private Sector Electronic Commerce Transactions"[9] of the Electric Commerce Promotion Council of Japan (ECOM) in January 2005.

3. The Need to Understand the General Situation and Review Continuously

Personal information is subject to various forms of usage, from the point of its occurrence to its registration in the database, as exemplified by online and printed materials. Therefore, merely conducting risk assessment regarding the server managing the database is not sufficient in order to achieve full compliance with the security management measure stipulated by law. When conducting risk analysis on personal information it is important to clarify the lifecycle of the data or information. No matter how the database server has improved, it is pointless if information is allowed to leak via printed materials or network systems. It is essential to conduct systematic operation management, such as configuration management and change control based on the ITIL (Information Technology Infrastructure Library), being the best practice pertaining to IT service management and operational rules. Personal information is merely a part of overall IT assets. It is crucial to implement the ISMS procedures containing the three essential security elements: confidentiality, integrity and availability.

The value of the IT assets will, of course, change with time. Moreover, changes in the configurations of servers and network systems will expose the IT assets to new risks. Accordingly, new technologies for countermeasures to such new risks will emerge. The flow of specifying the asset, understanding the threat, specifying the weakness, calculating the risk and selecting measures in handling IT assets is exactly the same flow for the processing of personal information. It is therefore crucial that the Plan-Do-Check-Act cycle be followed constantly.

References

1) Ministry of Economy, Trade and Industry. (October 2004). *Guidelines for economy, trade and industry concerning laws related to personal information protection.*
2) *Basic policy relating to the protection of personal information.* (April 2, 2004 Cabinet resolution).
3) Japanese Standards Association. (1999). *Requirements for compliance program on personal information protection* (JIS Q 15001: 1999).
4) Japanese Standards Association. (2000). *Information technology – security techniques – evaluation criteria for IT security* (JIS X 5070: 2000).

5) Japanese Standards Association. (2002). *Information technology – code of practice for information security management* (JIS X 5080: 2002).
6) *Law relating to the protection of personal information held by governmental agencies* (2003 Japan Law No. 58).
7) *Law relating to the protection of personal information held by independent administrative corporations* (2003 Japan Law No. 59).
8) Japan Information Processing Development Corporation. (April 2005). *ISMS users guide for regulation conformance.*
9) Electronic Commerce Promotion Council of Japan (ECOM). (January 2005). *Guidelines for personal information protection for private sector electronic commerce transactions.*

PROFILE

Hiroshi NISHIKAWA
Sumitomo Chemical Systems Service Co., Ltd.
Senior Advisor

Toshiko SATOMURA
Sumitomo Chemical Systems Service Co., Ltd.
Quality Assurance Department

Toshinori GOTO
Sumitomo Chemical Systems Service Co., Ltd.
General Manager,
Quality Assurance Department