1. PERSONAL INFORMATION PROTECTION ACT AND THE PRIVACYMARK SYSTEM

1-1 Trends in Legislation of Personal Information Protection

1. Status Following Promulgation of the Law and Future Directions

The Cabinet Office, which enforces the Act on the Protection of Personal Information (hereafter, "the Act"), has conducted surveys and discussion meetings subsequent to promulgation of the Act, to determine whether or not a balance has been achieved between safeguarding of personal information and effective utilization of information. As a result, on June 29, 2007, the Deliberation Committee of the National Consumer Affairs Center submitted to the government a report titled Collected Opinions Concerning Protection of Personal Information, which indicated the current status and issues concerning the Act, as well as future directions to be considered. This report called for dealing with "overreactions" occurring after promulgation of the Act, revision of the Execution Order Related to Protection of Personal Information (hereafter, "the Execution Order") would undergo revision, and the necessity for considering the unification of personal information protection guidelines issued by the respective ministries and agencies. Incorporated were the items below.

<1> Changes in the Basic Guidelines

"Public information and self-development activities, etc., will be reinforced to prevent "overreaction," and rights and benefits of consumers, etc., will be protected, with policies pursued to eliminate anxiety."

Based on the opinions of the Deliberation Committee of the National Consumers Affairs Center, a partial change was made in the basic guidelines on April 25, 2008. The change newly incorporated "Dealing with so-to-speak 'Overreaction,'" conveying the view that "Recently, the awareness of privacy has increased and from a variety of factors such as confusion as regards use of personal information, despite societal needs, have resulted in so to speak 'overreactions' such as the refusal to provide more personal information than specified by the laws, termination of production of name directories and so on." Furthermore the national and local governments are being called upon to proactively engage in public information programs, by means of a variety of methods including the utilization of the Internet for businesses and citizens, display of posters, distribution of pamphlets, holding of orientation meetings, and so on, to inform the public that the fundamental thinking of the Act which has the objective of "protecting personal rights and benefits while considering the utility of personal information" is fully reflected in the actual handling of personal information by various entities.

In addition, the importance of responding to what the individuals want is indicated, in that from the perspective of "greater protection for consumer rights and benefits," privacy policy in "attitude and orientation on the part of businesses, concerning promotion of personal information protection," consideration is given to "voluntary halting of use of personal data," "transparency concerning subcontracted processing," "clarification of the purpose of utilization," and "making the source and origin as specific as possible."

Moreover, in the items related to businesses that handle personal information, a postscript regarding "the degree of safety management measures" was added, and the degree of damage to rights and benefits of the individual was considered, so that concerning name lists sold on the open market for example, it is noted that even if there is no use of a shredder, the company would not be in violation of its safety management obligations.

<2> Partial Revision of the Execution Order of the Act

The execution order for the Act was partially revised as of May 1, 2008. Revision was made of Article 2, Those Who Are Excluded from Businesses Handling Personal Information, whereby the retained personal data whose information quantity exceeds 5,000, a numeric criteria, are not subject to this Act, with regard to personal information databases used in entirety or in part by other persons for making personal information databases when the databases are “issued for the purposes of sale to an indeterminate and multiple number of persons, and can be or were purchased freely by an indeterminate and multiple number of persons” were used in business activities without editing or alteration.

While this revision gave consideration to the liquidity in the market of freely sold name lists and to the degree of invasion of or damage to the rights and benefits of individuals included therein, the inclusion of the number of personal information items given in these name lists showed attention was given also to business operators because the scope of business operators handling personal information as stated by the Act to be subject to regulation was broadened.

2. Status of Maintenance of Guidelines in Specific Business Areas

<1> Implementation of Measures

Based on the basic guidelines, at the various ministries and agencies, as of April 1, 2008, 37 guidelines for personal information protection in 24 areas have been formulated, and have been announced.

(http://www5.cao.go.jp/seikatsu/kojin/gaidorainkentou.html)
(Japanese only)

Areas in the economy and industry categories will be based on standards executed by the Minister of Economy, Trade and Industry, as per October 2004 “Guidelines Applying to Areas of Economy and Industry as Relates to the Protection of Personal Information,” which were revised in February 2008.

<2> Trends Toward Commonality of Guidelines at Government Ministries and Agencies

On July 25, 2008, based on an understanding of a liaison conference of ministries and agencies involved in personal information protection, the Cabinet Office, in addition to indicating its thinking with regard to commonality of guidelines for protection of personal information (“Thoughts concerning commonality of guidelines”), also showed a disposition toward standardized guidelines in all areas (hereafter, “standardized guidelines”). Hereafter, based on these standardized guidelines and with the objective of so doing within one year, the existing guidelines in the respective ministries and agencies are to be revised, and attention is to be given toward encouraging revision of guidelines concerning protection of personal information related to the data service industry in economic, industrial and other areas.

3. Status of Exercise of Authority by the Competent Ministers

<1> Orders by Competent Ministers

In the Act, when a business handling personal information is in violation of the law, and further if said business fails to comply with a related order issued by a competent minister, punishments can be imposed of either imprisonment of not more than six months and/or a fine of not more than JPY300,000.

According to “Outline of Current Implementation of the 2007 Act on the Protection of Personal Information” (Cabinet Office, September 2008), 83 reports were received based on the Act from the competent ministers responsible for the respective business areas (of which two were from the Minister of Economy, Trade and Industry).

<2> Maintenance Status of Recognized Personal Information Protection Groups

By means of the Recognized Personal Information Protection Group system a competent minister can accord recognition to citizen organizations having the purpose of processing complaints and ensuring that personal information is properly handled. As of March 31, 2008, recognized groups under the auspices of METI numbered 15, including the Japan Data Processing Development Corporation (JIPDEC).

<3> Status of Handling Complaints Concerning Protection of Individual Data

In fiscal 2007, the number of complaint consultations regarding personal information taken to local public organizations and the National Consumer Affairs Center totaled 12,728. The number was essentially unchanged from fiscal 2006, in which 12,876 were received.

1-2 Outline of the PrivacyMark

1. PrivacyMark system

PrivacyMark is a system providing for certification by a third party organization that recognizes appropriate protective measures for personal information have been adopted, enabling display of the “privacy mark” as indication thereof. The system was created in 1998. The certification inspection at present is conducted in conformity with JIS Q 15001.

On June 19, 2008, JIPDEC and the Dailan City Software Industry Association (DSIA) of China signed “An agreement for a mutual recognition program for the PrivacyMark system and PIPA (personal information protection assessment) system,” initiating a mutual recognition program utilizing the PrivacyMark and the PIPA mark operated by DSIA.

2. Functions of the PrivacyMark system

Through operation with continuous improvements in accordance with JIS Q 15001, business operators’ and employees’ awareness of risk management is raised, enabling proactive prevention of accidents involving leakage of personal information. On the other hand, by anticipating emergency countermeasures, it is possible to expect appropriate responses to emergencies. Through these, the PrivacyMark has the function of dignifying the reliability of the businesses personal information protection management system.

Through the execution of the Act, since businesses handling personal information are subject to supervised responsibility by the consigner, the trend is growing for more consigners to seek to obtain the privilege of displaying the PrivacyMark as a means of avoiding incidents involving leakage of personal information at the consigner. This trend is conspicuous in the information service industry where many subcontractor businesses operate, and the mark can be said to have become indispensable for doing business.

3. Screening System for the PrivacyMark

<1> Certifying Organizations

The screening organization for the PrivacyMark system consists of the PrivacyMark conformity assessment bodies and an accreditation body. The latter is the Japan Information Processing Development Corporation (JIPDEC,) which gives accreditation to entities qualifying as conformity assessment bodies. The qualifying standards for a conformity assessment body were announced by JIPDEC on August 6, 2008.

The conformity assessment bodies, that receive applications, do screening and in situ assessment, certification and other work are private business organizations or industrial organizations conducts inspections of member companies, and is made up of organizations set up on a regional basis. As of November 25, 2008, 16 organizations had been designated, including JISA.

<2> Assessor Registration System

In 2007 a PrivacyMark assessor registration system was established, and put into operation. The system provides for lead assessors, assessors, and probationary assessors. Each are required to fulfill certain conditions (qualification standards) set by JIPDEC. Also, from August 6, 2008, JIPDEC announced recognition standards for PrivacyMark training organizations, and in November of the same year recognized the first training organization. In the future the number of inspectors can be expected to increase through the work of these organizations.

1-3 Outline of PrivacyMark Inspections

1. Eligibility of PrivacyMark

Businesses eligible to apply for PrivacyMark must have their home office in Japan, and at least have installed a personal information protection management system (PMS) based on JIS Q 15001, and have the capability to maintain a system based on it. They must fulfill the appropriate conditions for handling personal information.

2. Inspection Standards

A conformity assessment body will determine, though document screening and in situ inspection that the business applying for PrivacyMark has established a PMS that fulfills and puts into practice the items required to meet JIS Q 15001 and industry guidelines. The inspection standards, are structured from the perspective of “personal information protection guidelines,” “recognition of planning, analysis and countermeasures,” “implementation and putting into practice,” “PMS documentation,” “complaints and consultation,” “checks (confirmation and auditing of operations),” “and “revisions by a representative of the company.”

3. Utilization of the PrivacyMark

Upon passing the screening by the conformity assessment body, the business can conclude an agreement for the utilization of the PrivacyMark with the JIPDEC. The validity of the agreement is two years, and to continue its use, the assessment for extension must be made. In addition, the agreement stipulates the method of use, investigation of and revocation for violating companies, and publication of the company’s name. If an accident involving leakage of personal information, etc., occurs by a certified company, appropriate measures will be determined by the respective inspecting organization. At such time, in some cases, the conformity assessment body, based on the agreement regrading utilization, can revoke the use of the PrivacyMark and also make such measures public.

1-4 Status of PrivacyMark Enforcement

1. Certification Status

With the Act's coming into existence, the trend has increased from customers to request PrivacyMark certification as a condition for bidding or standard for selection of consignees, and coupled with the reinforcement of the system, the number of businesses with certification since 2005 has increased sharply (Fig. 1-1).

Categorizing the inspection organizations for PrivacyMark by type, JIPDEC itself accounts for over 60 percent of the total (Fig. 1-2). With regard to the types of businesses obtaining certification, the ratio of data services, survey companies with certification account for about 40 percent of all businesses obtaining it, it is evident from the large number of companies in these industries that demand for PrivacyMark certification in these industries is high and that these companies are making energetic efforts to obtain it (Fig. 1-3).

2. Trends of Mishaps in Certified Companies and Countermeasures

With regards to reports of mishaps received by the PrivacyMark inspection organization, from fiscal year 2005, this data has been made public by JIPDEC, and well as by JISA from FY 2006, with results of analysis of accident reports it had received itself, to call the issue to the public's attention. According to the "trends toward which to take caution as viewed by the accident reports concerning handling of personal information in 2007" made public by JIPDEC, during 2007, a total of 1,829 incidents by certified businesses, etc., occurred, of which 990 incidents (51.4%) were caused by misdelivery of posted mails or missent faxes or emails. Adding missent enclosures, roughly 60% of the mishaps related to personal information involved accidents in the sending process, and at least it was understood that accidents of this sort could be prevented through reconsidering the means of sending or by exerting greater caution in confirming when sending.

(http://privacymark.jp/news/20080610/H19JikoHoukoku_080610.pdf)
(Japanese only)

Based on "the PrivacyMark system setup and essentials of operation," in the "standards for determination of defects in the PrivacyMark system" established by JIPDEC (April 2008), the main points of this system can be regarded and have been established to the effect of "From the perspective of proactively preventing major accidents in the future, even if one incident of personal information is leaked, these will be reported."

Moreover, in JIS Q 15001:2006, as an item for "checking," in addition to auditing, "confirmation of operation" to be carried out at each department and stage has been newly added. If points are noted in the course of regular work, this provides for rectification and prevention to be proactively applied to prevent accidents related to personal information.

Through these operations, the PrivacyMark system is designed to reinforce the personal information protection management system.

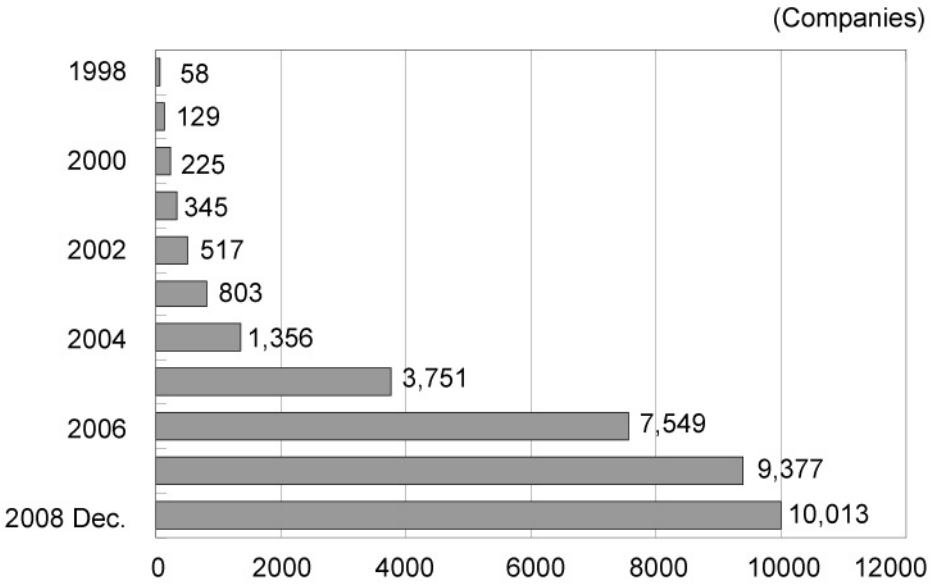

Figure 1-1
Growth in the Number of PrivacyMark Certified Businesses (aggregate total)

Source: *JISA "Annual Vendor Survey 2008"*

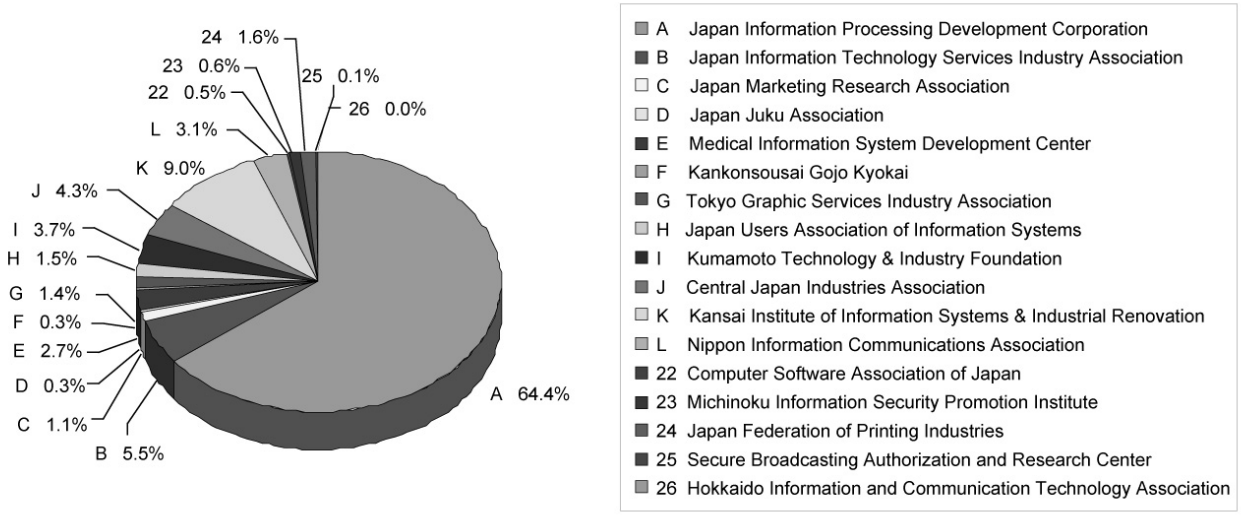

Figure 1-2
Ratio of PrivacyMark Companies According to Issuing Inspection Organizations (total 10,013 companies)

Source: *Produced by JISA from JIPDEC information*

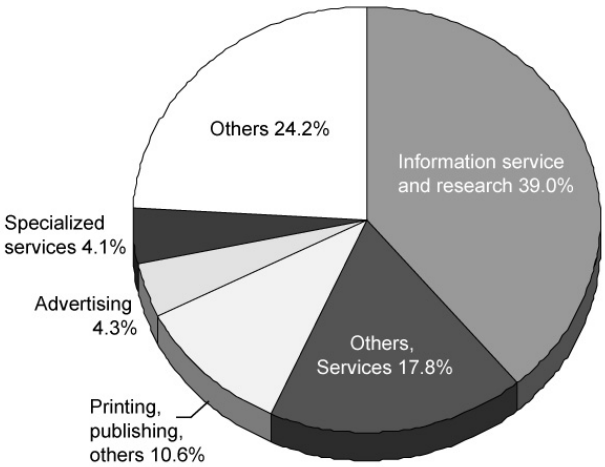

Figure 1-3 Certified Businesses by Sector (Top five industries; effective total as of Dec. 31. 2008: 10,013 companies)

Source: *Produced by JISA from JIPDEC information*

1-5 Future Orientation of the PrivacyMark System

In the IT services industry and especially among the large companies there are many firms that have acquired accreditation for ISMS, the ISO 9000 Series, and other standards. Consequently, even for the large companies the time and cost expended for screening, including training and audits, and for keeping records, cannot be ignored. This has made it incumbent on them to acquire management techniques that integrate these activities.

Further, inasmuch as the PrivacyMark is an indicator of the reliability of the company's defense system for protection of personal information, any incident caused by a certified company necessarily reflects poorly on the PrivacyMark. In keeping with growth of the number of companies having PrivacyMark accreditation, awareness in society of the system will necessarily grow, for which reason it can be expected that the role of the system too will grow, and in addition to its value in helping prevent incidents at certified companies, attention is deserved by its international presence.

Source: "Chapter 5, IT Services Industry in Japan 2009"