CHAPTER 5 BUSINESS TRENDS IN IT SERVICES INDUSTRY, AND BUSINESS TRANSACTIONS AND THE LEGAL SYSTEMS

5-1. TRENDS IN GREEN IT

5.1.1 Global Warming

1. Year One for Realizing Greenhouse Gas Reduction Pledges

2008 was Year One, under the Kyoto Protocol, in the five-year period to accomplish pledged reductions in the emissions of greenhouse gas (GHG), a cause of global warming. Japan is among the countries that have promised to reduce GHG production by 6% relative to the level of 1990. Penalties for failing to achieve targets were set by at the Montreal Protocol in November 2005; failure to achieve the five-year target will cause imposition of a 30% addition to the target reduction, to be achieved during the second phase of reductions, starting in 2013.

At present, the world produces twice as much carbon dioxide as the natural environment can absorb, so initiatives are being carried out to reduce production in order to achieve a balance. Corresponding to this, Japan has advocated to the Intergovernmental Panel on Climate Change (IPCC) adoption of “Cool Earth 50,” an initiative to reduce carbon dioxide emissions by half of the present level, by 2050. Subsequently, at the Heiligendamm Summit, in 2007, the EU, Canada, and Japan, after studying the Japanese proposal, agreed on the goal of a reduction by at least half, on a global scale, by 2050, and at the Toyako (Hokkaido) Summit in July 2008, the goal was adopted by the G8 as a common objective.

2. Present Situation in Japan Concerning Reduction of Carbon Dioxide Emissions

Japan’s approach to reducing the emission of carbon dioxide can be considered as beginning with passage of the Law Concerning the Promotion of the Measures to Cope with Global Warming in 1998. The Industrial Structure Council and the Central Environment Council began to investigate related matters and, more recently, in April 2005 the Cabinet resolved to achieve the target advocated by the Kyoto Protocol.

2007 was the time to confirm the present situation, and consider measures to be taken in 2008, the first year for measurement of progress toward reaching the goal. The present status, reported in October 2007 in terms of preliminary data for fiscal 2006, placed Japan’s emissions of carbon dioxide lat 1.341 billion tons a year. This represented an increase of 6.4%, whereas the target was a reduction of 6% relative to the base year. Although the industrial sector achieved a reduction of 5.6%, the business sector, including offices, had increased carbon dioxide emissions by 41.7% and there had been increases of 30.4% for the household sector and 17.0% for the transport sector.

The historical trend of carbon dioxide emissions by each sector is shown in Fig. 5-1. Manufacturing showed steady progress in keeping with the Voluntary Action Plan on Environment, by Nippon Keidanren (Japan Federation of Economic Organizations) since 1997 and METI since 1998. The transport sector, that had shown a trend of increases in carbon dioxide emissions, has shifted to a pattern of decrease.

Elsewhere, however, in the business and household sectors, there have been annual increases. A warm winter served to depress carbon dioxide emissions in 2006, but in overall view there has been no decline. The business sector includes offices, retail, stores, and service establishments, and the information service industry. The latter operate data centers containing many computers. Thus, industry faces the challenge of reducing both carbon dioxide emissions from direct productive activity as well as indirect, business-related activity.

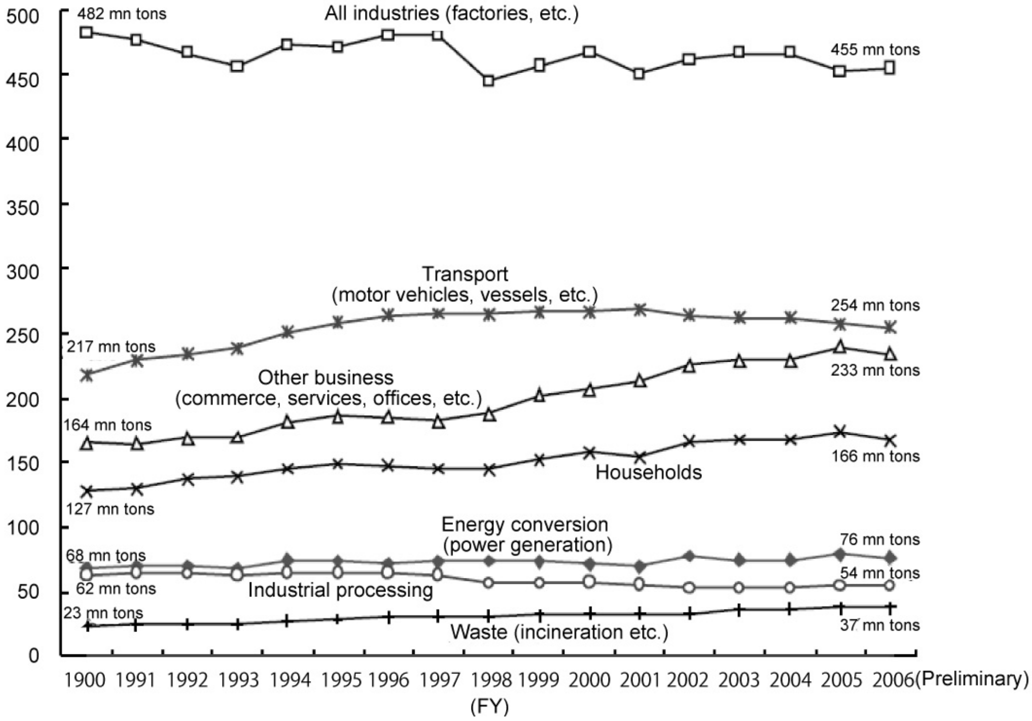

Figure 5-1
Carbon Dioxide Emissions by Sector, 1990-2006

Note: Values for 2006 are preliminary.

Source: *Central Environment Council, Interim Report on Evaluation and Review of the Kyoto Protocol Target Achievement Plan, Nov. 2007.*

Japan’s approach to the achievement of the target goals comprises, in addition to the voluntary plan mentioned above, reduction of GHG emission by the improvement of energy efficiency and the reduction of total energy consumption as expressed in the Law Concerning the Rational Use of Energy.

The former was revised in April 2009 from being a regulation of (large) enterprises to being a regulation of enterprise operators. This required many such operators in the business sector to comply with this revised law, provided a definition of unit energy consumption for use by general operators for monitoring their own energy use, and called for efforts at improving the efficiency of energy use by an annual reduction of that value of 1%.

Concerning the latter, as mentioned in the proposal for “Japan as a Low Carbon Society” (referred to as the “Fukuda Vision”) announced by Prime Minister Yasuo Fukuda in 2008, in order to use the market mechanism to encourage the necessary technical development and encourage efforts at reducing GHG generation by determining a market price for carbon dioxide, a domestic market for carbon trading was begun in December 2008, on a trial basis. It is expected that revision of the Tokyo Metropolitan Government’s global warming countermeasures program will enable introduction of a duty to reduce total GHG emissions and trade scheme as a requirement for large-scale enterprises (using the equivalent of 1,500 kiloliters of crude oil a year).

3. Green IT

Consumption of electric power by the IT equipment and systems which is so important in this age of society being information-centered, in the case of Japan, is forecast to increase by 5.2-fold the present level by 2025 (accounting for about 20% of Japanese total power generation), while the equivalent value for the world will increase during the same period by 9.4 times more than that level of 2006(to 15% of world electricity production). These sharp increases in power use are themselves social issues of world importance. (Fig. 5-2)

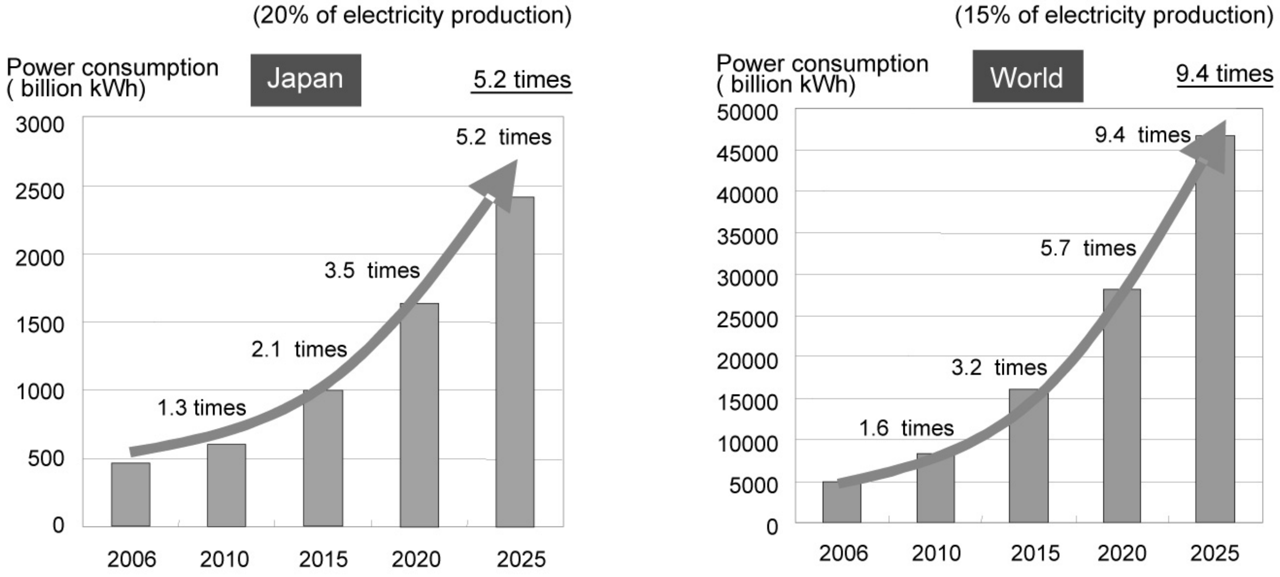

Figure 5-2
Estimation of Electricity Consumption by IT Devices and Systems

Source: *METI, Green IT Promotion Council, 2008*

Two modes whereby the IT-related industry can contribute to limiting this rapid growth have been identified. Together, they represent an area of concern called Green IT, and are as follows.

First, energy consumed for IT equipment can be optimized by improvement of the efficiency of development and application of energy-conservative technology so as to bring about reduced or restrained generation of carbon dioxide (moderated energy consumption by IT equipment and systems).

Second, the use of IT equipment and systems can enable optimization of energy consumption in industrial activity, the transport sector, and office activities, contributing to reduced or restrained carbon dioxide production (moderated energy consumption by use of IT).

The government's IT Strategic Headquarters, established within the Cabinet, in its New IT Reform Strategy policy paper released in January 2006, raised "IT Society in Harmony with the Environment" as a theme where IT use reflects environmental considerations, and efficient use of energy and raw materials. The action program for 2008, prepared on the basis of this policy, is to have as its basic stance the importance of Japan, both at home and abroad, to actively work on establishing a low-carbon society on the dual basis of coping with global warming and assuring economic growth through Green IT, through using IT to reduce the load on the environment, and reduction of energy consumption by IT equipment proper. It states that with regard to global warming, from the current year we have entered a period of monitoring the reduction of carbon dioxide emissions with the objective of achieving the targets of the Kyoto Protocol, and this imposes the requirement to adopt and resolutely implement new measures to succeed in this effort, while continuing to promote the various uses of IT in energy management and other related activities. Then, in order to restrain the increase in carbon dioxide emissions that will inevitably result from the increase in the number of IT equipment and the enhancement of their performance, in addition to working at improvement of the energy efficiency of IT equipment so as to minimize the resultant emissions of carbon dioxide, even stronger efforts are called for, by working in collaboration with the Global Warming Prevention Headquarter, for management of energy consumption in offices and homes, the creation of logistics systems and Intelligent Transport Systems (ITS) all of which would utilize IT.

The following five specific policies are advocated:

1) Restraint on the use of energy by IT equipment.

2) Improvement and greater efficiency of energy management, logistics and transport flows, by use of IT

3) Collection, ordering, analysis, archiving of, and provision of access to environmental information by use of IT

4) Promotion of the Electronic Manifesto (control tags for materials destined to treatment as waste)

5) Promotion of resource recycling by using IT to improve traceability of waste materials

4. Activities of the Green IT Promotion Council

In order to materialize the above measures, seven organizations including JISA (the others being the Japan Electronics and Information Technology Industries Association, JIETA; Japan Electrical Manufacturers' Association, JEMA; Japan Electric Measuring Instruments Manufacturers' Association, JEMIMA; Communications and Information Network Association of Japan, CIAJ; Japan Business Machine and Information System Industries Association, JBMIA; Japan Users Association of Information Systems, JUAS) cooperated as organizers and obtained the participation of 194 organizations to create the Green IT Promotion Council, in February 2008.

The Council has three committees.

The Technical Committee is preparing a road map for energy-conserving technology development through 2025; it is expected that this will provide Japan with subjects for technological development work, and suggest the effects that can be expected of application of the new technology.

The Public Relations Committee works at providing information to related parties and the public about the Green IT effort, through activities that included sponsoring a showcase exhibit at the Toyako Summit.

The Research and Analysis Committee has organized four Working Groups; they are concerned with energy conservation in IT equipment and systems, estimation and forecasting of energy conservation attainable by the use of IT, development of methods of measuring the contribution to the environment by quantifying the energy consumed and conserved by IT equipment throughout the lifecycle of the equipment, and monitoring activities of similar entities overseas. In August 2008 a sub-working group was organized to take up matters related to energy consumption at data centers. This sub-working group, by working with the Green Grid in the US (a non-profit organization working at improving the efficiency of energy consumption by IT equipment and at data centers) is drafting a standard for energy conservation by data centers.

5.1.2 Voluntary Action Program for Reduction of Carbon Dioxide Emissions by the Information Services Industry

1. Preparation of the Voluntary Action Plan for Reduction of Carbon Dioxide Emissions

The IT services industry is engaged in efforts at contributing to reduction of energy consumption by Japanese industry, by developing and managing IT systems that promote economic efficiency.

This industry, however, has shown a trend of increasing consumption of electric power, as the growth of business scale, the increase in the number of equipment used for system development and security particularly in connection with software development and the increase in the number of servers installed in data centers along with enhanced performance and improved efficiency have combined to increase air conditioning requirements, owing to the heat generated by the equipment.

In keeping with the nature of the industry as being part of the information infrastructure of Japan's industry and society, the industry has recognized the need for its own efforts on behalf of the global environment and has formulated its Voluntary Action Program for Reduction of Carbon Dioxide Emissions ("Voluntary Action Plan" below), to bring what had involved energy-conservation efforts on the ground to the level of a subject of direct concern to top management, and the Voluntary Action Plan is now included in follow-up studies by METI.

[Goal of the Voluntary Action Plan]

The objective of the Voluntary Action Plan is to reduce average energy consumption in the five-year period from fiscal 2008 to fiscal 2012 by 1% from the base year of fiscal 2006. The unit of measure for monitoring this effort at reducing energy use is kilowatt-hours per square meter of floor space.

At companies in the relevant industries activities that are being carried out to achieve this target include 1) active introduction of energy-conservative equipment (personal computers, servers, air conditioning systems, cooling systems, lighting etc.), 2) close attention to turning off lights and equipment power supply in offices when not needed, and 3) careful control of indoor temperature through adjustment of heating and cooling systems. These companies are working at gaining a better understanding of details of their energy consumption, and have adopted a standard measure of specific energy consumption to enable the necessary comparisons to be made.

2. Results of the Follow-up Study for Voluntary Action Plan

In order to promote and institute the Voluntary Action Plan, which was formulated in October 2007, a follow-up study for 2007 was conducted in August 2008. The result of this study is shown below.

<1> Energy Consumption, Floor Area, and Unit Consumption

The data for energy consumption, floor area, and unit consumption at 64 participating companies, for fiscal 2006 and 2007, were as follows. The values show an increase in unit energy consumption of 4.8% (Table 5-1).

Table 5-1 Energy Consumption, Floor Area, and Unit Consumption at Participating Companies

	FY2006	FY2007	Change (%)
Floor area (m^2)	1,892,038	2,036,741	7.6
Energy consumption (10,000Kwh)	117,438.50	132,475.10	12.8
Unit consumption (Kwh/m^2)	612	650	4.8

Source: *JISA, after results of the Follow-up Study on the Voluntary Action Program for Reduction of Carbon Dioxide Emissions*

The information reported by the 64 companies, separated according to the two categories of office areas and data centers, is as follows (Table 5-2).

	Item	Offices	IDC, other data centers	Total
FY2006	Energy consumption (10,000Kwh)	24,144	87,250	111,394
	No. of enterprises	282	52	334
	Total floor area (m^2)	1,087,519	799,781	1,887,300
FY2007	Energy consumption (10,000Kwh)	27,161	98,835	125,996
	No. of enterprises	284	54	338
	Total floor area (m^2)	1,215,824	819,171	2,034,995

Table 5-2 Energy Consumption, Floor Area, and Unit Consumption in Offices and Data Centers

***Source**: JISA, after results of the Follow-up Study on the Voluntary Action Program for Reduction of Carbon Dioxide Emissions*

<2> Energy Consumption, Floor Area, and Unit Consumption in Office Areas and Data Centers

1) Office areas

Relative to the base year (fiscal 2006) floor area increased 11.8%, energy consumption increased 12.5%, and as a result the unit consumption of energy rose 0.5%, a result suggesting that the target level can be met (Table 5-3).

Table 5-3 Energy Consumption, Floor Area, and Unit Consumption at Offices

	FY2006	FY2007	Change (%)
Floor area (m^2)	1,087,519	1,215,824	11.8
Energy consumption (10,000Kwh)	24,144	27,161	12.5
Unit consumption (Kwh/m^2)	222	223	0.5

***Source:** JISA, after results of the Follow-up Study on the Voluntary Action Plan for Reduction of Carbon Dioxide Emissions*

2) Data centers

Relative to the base year (fiscal 2006) floor area increased 2.4%, energy consumption increased 13.3%, and as a result the unit consumption of energy rose 10.6%, far exceeding the target (Table 5-4).

Table 5-4 Energy Consumption, Floor Area, and Unit Consumption at Centers

	FY2006	FY2007	Change (%)
Floor area (m^2)	799,781	819,171	2.4
Energy consumption (10,000Kwh)	87,250	98,835	13.3
Unit consumption (Kwh/m^2)	1091	1207	10.6

***Source:** JISA, after results of the Follow-up Study on the Voluntary Action Program for Reduction of Carbon Dioxide Emissions*

3) Composition of energy consumption at offices and data centers

Using the data from Table 5-3 and 5-4, the composition of energy consumption and floor area of the reporting companies can be calculated, with results as shown in Fig. 5-3. At the data centers about 40% of the floor area was where nearly 80% of energy consumption took place.

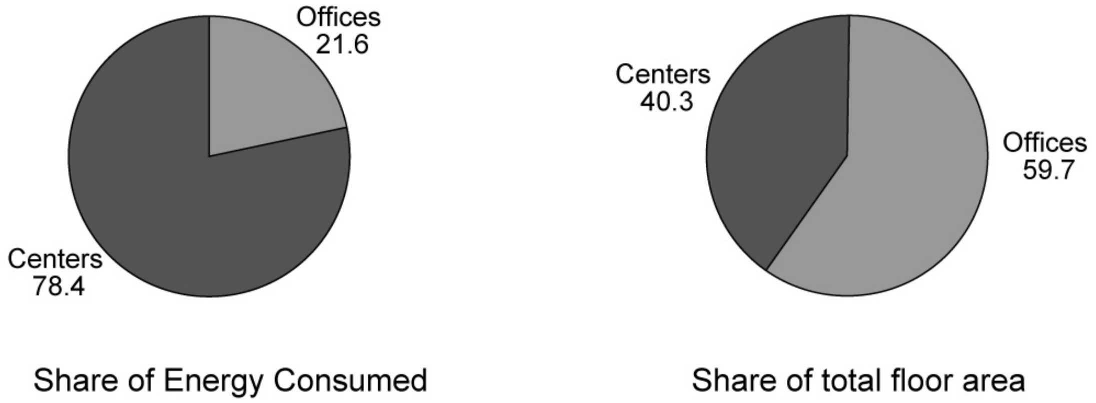

**Figure 5-3
Energy Consumption and
Floor Area by Type of User**

Source: *JISA, after results of the Follow-up Study on the Voluntary Action Program for Reduction of Carbon Dioxide Emissions*

From the above information it appears possible that for office areas, since total floor space is the area for productive activity, the energy conservation activity based on total floor space as the unit energy consumption can be carried out to achieve their goal.

In contrast to this, at the data centers energy consumption per unit floor area is extremely high – about five times greater than for the office areas – and using the same method of evaluation as for office areas it appears difficult to achieve the reduction target. Further, because there is an operational requirement at data centers to install servers without increasing the floor area used, the use of floor area as the denominator in calculating unit energy consumption with the purpose of reducing energy consumption is contrary to the objective of economic activities, and is not suitable.

It is therefore planned to devise a new indicator for unit energy consumption at data centers.

5.1.3 Improvement of the Efficiency of Energy Consumption at Data Centers

1. Energy Management at Data Centers

The first step suitably taken by IT-related industry by way of contributing to resolution of the problem of global warming would be development and application of energy-conservation technology for IT equipment, to thereby improve efficiency of equipment operation and reduce the emissions of carbon dioxide. In the case of information service industry, this means improving the efficiency of energy consumption at data centers. In addition to the reduction of carbon dioxide accomplished by this, a further contribution would be made to reduction of carbon dioxide emissions by overall industry, to the extent that the data centers, on their own premises, care for hardware assets of their industrial customers. In addition to the growth of this housing service, in recent years the growth of service businesses such as SaaS and ASP is further increasing the consumption of energy at data centers, increasing the urgency of reducing energy consumption at the centers.

The measures that are expected to be important as part of general efforts by data centers to reduce their use of energy are as follows and the companies are engaging in their unique and effective projects.

(1) Reduction of power consumption by IT equipment proper

- Reduction of power consumption by CPUs
- Reduction of power consumption by servers
- Reduction of power consumption for storage

(2) Reduction of power consumption at centers where IT equipment is located

- Improvement of cooling of servers and storage
- Improvement of air flow efficiency
- Improvement of efficiency of air conditioning equipment
- Improvements through use of direct current
- Reduction of power consumption by cooling equipment
- Use of natural cooling

(3) Switch to use of clean energy

- Use of solar energy
- Use of hydropower
- Cogeneration

2. Making the Efficiency of Energy Consumption Visible

Production efficiency at data centers can be defined in terms of the formula given below, but measurement of the efficiency of IT equipment is difficult and therefore this method does not reach masses.

Production efficiency = IT equipment efficiency x Equipment efficiency

= (Production by IT equipment) /Total electric power used by IT equipment)

* (Total electric power used by IT equipment / Total electric power used by the data center)

However, in order for the effort at improving the efficiency of power use at data centers to be improved, it is necessary to make the efficiency of energy consumption visible to those managing the centers.

Discussion of how to deal with energy reduction at data centers is ongoing in several countries, and the concept of Power Usage Effectiveness (PUE) advocated by the Green Grid would be of useful reference in that connection.

It is expected that reference will continue to be made to PUE, in order to use power consumption by IT equipment as the denominator, despite the drawback that good values are obtained when low-efficiency, old-type IT equipment is used, and PUE as given below is expected to be of use in supplementing efforts at the purchase and self-production of clean energy.

PUE = [A – B] / C where

A: Total electric power consumption by the enterprise’s center

B: Total clean energy purchased or made by the enterprise’s center

- Purchase of clean energy (energy certified as green energy)
- Self-production of clean energy (solar power, wind power, biomass)

C: Total electric power consumption by IT equipment at the enterprise’s center

5-2. PRESENT CONDITIONS REGARDING SOFTWARE AND SERVICES FOR GOVERNANCE

Fiscal 2008 was the first year for mandatory compliance with regulations for reporting on corporate governance, and the Japanese equivalent of the United States' Sarbanes-Oxley Act, popularly known as the J-SOX law (specifically, it is a part of the Financial Instruments and Exchange Law), and this is having a strong influence on the information services industry. Involved in the reporting process are software for business operations support, middleware for access control, as well as consulting services.

5.2.1 Overview

The information services industry has been giving close attention in the past few years to internal controls and the implications and impact of the J-SOX law.

This law requires publicly-owned companies to evaluate and audit internal controls over financial reporting. Company-wide schemes are required to ensure there are no improprieties or errors in financial information, including the financial statements used for disclosure, and certified public accountants or auditing firms must make examinations to determine if the schemes are functioning properly. The law is applicable starting with the term ending March 2009.

In legal terms, J-SOX is a part of the Financial Instruments and Exchange Act. As to what is actually required, reference is to be made to two documents: the definition of internal control written by the Internal Control Committee, Business Accounting Council, of the Financial Services Agency, that is, the "Standard" (formally, Standard for Evaluation and Audit of Internal Control for Financial Statements), and with regard to the preparation of financial statements and method of evaluation, the "Execution Standard" (formally, Execution Standard for Evaluation and Audit of Internal Control for Financial Statements).

5.2.2 Scale of the Market Related to Internal Controls, and Related Products

The impact of J-SOX and internal controls on the information services industry is by no means small. Calculations by IDC Japan suggest that IT investment in the financial area in connection with internal control will grow an average of 7.1% a year from JPY266.6 billion in 2007 to JPY375.1 billion in 2012. The broader compliance market is forecast to be JPY1.8200 trillion in 2012.

Three causes for the strong impact internal controls and J-SOX will have on the information services industry. First of all, the role of IT in activities of corporations has been expanded. Besides applications in such basic areas as accounting and sales and logistics management, and production management, preparation and management of departmental budgets, reports of all kinds, presentation materials, mail and other forms of communication are all areas where IT is widely used in the corporate world.

J-SOX imposes on corporations the requirement to install internal controls over financial reporting, requiring in turn a company-wide scheme. The role of IT in this is enormous. Use of IT is specifically mentioned in the standards for compliance with J-SOX, and there are many mentions of IT in the implementation standards for the law.

Second is that the scope of IT in internal control and J-SOX compliance is quite broad. Products for IT support for internal control and J-SOX compliance include, beyond software for ID and access management, log management and other security matters, enterprise resource planning (ERP) packages and other applications, business process management (BPM) software, middleware such as database management and application server software, documentation tools for the preparation and archiving of internal control activities information, including information needed for audits and certification, and the hardware needed for storage.

The varieties of IT-related service are numerous. In the area of consulting, for example, there are preparations of systems for IT governance, support for system inventory needed as a prerequisite for carrying out IT control activities, support for overall improvement of IT governance in the IT department, and services for improvement of the system of internal control from the viewpoint of facilitating of audit and certification work. More specifically, service for support of the introduction of ID control is included, as well as the training of employees. More specialized examples would include the service of issuing certifications of contractor systems in connection with outsourcing system management.

One more reason the effect that adoption of internal control systems and compliance with J-SOX is highly significant for the information services industry is that they are not creating one-time demand. Internal controls are year-round in nature, and the audit requirement is an annual activity. The systems and arrangements for compliance with J-SOX are not something to be set up or delivered and all is finished; they will continue to generate demand for information services.

Wider spread of the demand for services is also of benefit for information service providers. Whereas internal controls are oriented toward financial reporting, the results of the operation of those controls necessarily will be widely used in the organization in question. It becomes possible to create an enterprise risk management (ERM) system for the entire company, or work at optimization of business processes at the level of the entire company, if the results of J-SOX compliance are utilized. There are vendors who are identifying business opportunities in this “post J-Sox” period.

5.2.3 Products Related to Enterprise Resource Planning

Enterprise resource planning packages are one of the products that information service companies consider most promising in connection with corporate needs based on internal control and J-SOX requirements. These ERP packages provide integrated control of information on the people, things and money used for core operations such as accounting, marketing, purchasing, and production management.

In comparison to creating a core system from scratch, it is often easier to acquire an ERP package to improve and operate an internal control system. This is because the processing necessary for operations is placed inside a black box and operations become easier under conditions of system control. To not do additional development of a package makes it easy to maintain a certain level of governance.

In addition to their work for large corporations, recently information service vendors have been improving ERP packages to make them more functional in support of internal control and J-SOX requirements at medium-scale companies. An example is the provision of functions such as “prevent input of more than a specific number of digits, or of the wrong numbers,” and “no approval of a payment against a voucher without the superior’s approval.” Functions such as these help keep internal controls in order and functioning properly.

Access control and log control functions in ERP packages have been undergoing improvement. Both functions are essential for internal control and J-SOX compliance. Access control in particular, by being a matter of who can do what with what data” is essential for allocation of assignments and responsibilities, which is fundamental to internal control. Often, access is controlled on the basis of the ID unit of individuals, but there are often instances when access is provided on the basis of a specific group or persons with certain job titles. The control of logs, where the nature of operations by individual workers and the details of transaction processing by a system are recorded is another vital function for the supply of essential materials for judging whether there is adequate IT governance.

In addition to access control and log control functions, ERP packages can provide specialized software. For example, log control software can collect log data from the operating system, middleware, applications, and network devices, and display a report analyzing the results of such collection. Because it is expected that demand for log control will increase in keeping with the requirements of internal controls and J-SOX compliance, improvement of the packages includes provision of dashboard functions indicating results in an easy to operate form. Thus by making the package application software J-SOX specific IT vendors encourage the customers to introduce the applications.

5.2.4 Products for the New Area of Documentation Tools

What has particularly captured attention when a large number of companies began work at internal control improvement and preparation for J-SOX compliance is documentation tools. The objective is to facilitate the preparation and management of documents required for the three requirements of internal controls and J-SOX compliance, namely a work flow chart, a work record containing details of work, and a risk control matrix for prevention and reduction of risk as would impact financial statements.

Documentation tools are broadly separated into desktop editions and server editions. The desktop editions are for preparation of the above three requirements. The server editions are used for a much broader scope of work: documents for control of work in progress, or completed work, for confirmation of the status and management conditions of document-based internal control, and for support of evaluation and audit work. It is expected that demand for server edition documentation tools will increase as corporations approach the start of their activities to satisfy internal control and J-SOX requirements.

New type of products are introduced in anticipation of the advent of internal control and J-SOX requirements. These are called GRC products, for Governance, Risk, and Compliance.

What these GRC products do is to evaluate whether controls are effective and to support evaluation of effectiveness. They collect transaction data, access logs, operation logs and the like from applications and evaluate them according to predetermined rules. The rules anticipate the requirements of internal controls and J-SOX compliance, but also other laws and regulations such as those relating to protection of personal information, systems such as COBIT (Control Objectives for Information and related Technology) as well as characteristics that are peculiar to the industry or company involved. One benefit of GRC tools is that they enable integrated management of these requirements. Reports are prepared and alerts are issued, based on the results of rule-based evaluation. They are considered to be useful in view of the expansion of tasks for meeting internal control and J-SOX requirements.

5.2.5 Services

Since the start of 2008, a number of services have come to be offered as support for effectiveness evaluation of internal control and J-SOX compliance. Effectiveness evaluation, as an activity sub sequent to documentation, confirms whether internal control has been effective in terms of the work flow chart and risk control management. Some services offer a menu including supply of a template for improving the efficiency of effectiveness evaluation, a manual for the persons performing the evaluations, and training services for persons in charge of this work.

Among the vendors offering outsourcing services for managing systems related to internal control and J-SOX are some that offer to prepare audit reports conforming to Auditing Standard 18, Japan’s equivalent of the Statement of Auditing Standard No. 70 in the United States.

When systems directly related to J-SOX are outsourced, the outsourcing company must evaluate the system control function of the service vendor. If, however, the vendor prepares an audit report conforming to the requirements of Auditing Standard 18, the outsourcing company is freed of the need to evaluate the status of governance regarding the outsourced system.

5-3. Present Situation Concerning Information Security

5.3.1 Overview of the Present Situation Concerning Information Security

With steady growth in the importance of information security in the background, Japanese companies have been making strong progress in improving the security of personal information, in building internal control systems (in part because of the J-SOX requirements) and in preventing information leaks. Meanwhile, at the national level, the Cabinet Secretariat, through its National Information Security Center (NISC) is fostering a range of measures from the level of individual citizens to the nation as a whole. Despite all this, the frequency of security breaches or accidents does not seem to be declining. Below is an overview of the present situation, with emphasis on examples from the information services industry.

1. Menaces to Information Security

In June 2008, the Information-Technology Promotion Agency (IPA) released the 2008 edition of the Information Security White Paper.[6] In addition to surveying trends in information security from the viewpoints of both suppliers and users of information, this study identified ten major menaces to security that had significant potential for social impact during 2007-2008, analyzed them, and discussed countermeasures. The dangers identified have continued to exist during 2008. That is, as the subtitle of the white paper, “The Advance of ‘Unseen’ Threats,” suggests, the dangers such as posed by spyware and bots, that are hard to identify without pre-emptive measures taken by system administrators, are growing. During the latter half of 2008 these menaces became more diverse and more cleverly composed. A particularly big issue for information system administrators in 2008 was how to deal with vulnerability to DNS (domain name system) cache poisoning. Further, at the 2008 Computer Security Symposium, in October, an announcement was made that it had become possible to crack the encryption of WEP of a wireless LAN easily and in a short time; this news raised awareness of the dangers to wireless LAN.

As another issue of considerable concern to IT services companies is that there has been no diminution in leakage or loss of information from companies due to contamination by P2P (peer to peer) file transfer software such as Winny, that has plagued information service activities for several years. Despite unending efforts at compliance with the Personal Information Protection Act (PIPA) by improving security in information management systems, managers at those companies are perplexed by the frequent recurrence of cases of information leakage or loss caused by organized or individual actions, inadequate control arrangements, use of employee-owned PCs, and infraction of rules.

Moreover, attacks taking advantage of vulnerability of IT products and web applications continue to increase and in particular in 2008 there were many reports of legitimate web sites being surreptitiously modified so as to attack users of the sites. Also, there have been increases in instances when an Internet user had registered the same ID and password at more than one site and after this information was obtained from one site by a malicious party it was used by the latter at other sites, causing damage to the former party. It goes without saying that companies engaged in building information systems and developing IT products are trying to prevent vulnerability in what they produce, and it remains important for users of those systems and products to remain alert and to take proper steps promptly upon discovering vulnerability.

[6] See http://www.ipa.go.jp/security/publications/hakusyo/2008/hakusyo2008press.html

2. Approaches to Ensuring Information Security

While we can observe that IT services companies are continuing to invest in purchases of security-related products, and in obtaining authorizations to use ISMS and the PrivacyMark, unresolved issues remain. They include, at small and medium scale enterprises, the heavy cost burden of security measures, doubts as to whether benefits of measures justify the costs, and unease because of the lack of a benchmark indicating the extent that they should take action. Other issues at hand are the possibility of excessive measures being taken for security, and imposition of penalties on employees who are responsible for security breaches. In the past it had been thought to be good if investments made in information security improved the competitiveness of the company, and were reflected in higher corporate value, but, unfortunately, consensus on this at user companies and society in general has not been achieved.

At the same time, companies have appeared that view ensuring that information security as a matter of social responsibility of the company, and are making strong efforts at installing information security governance.[7]

<1> Public Disclosure of Security Reports

The number of companies that are proactively disclosing information about their approach to ensuring information security is rising. These companies consider such disclosure to be appropriate for the sake of customers, investors, and stakeholders, and also see this stance as contributing to the trust placed in the company, and to its brand power.

<2> Preparation of Business Continuation Plans

Increased activity has been noted recently in work at preparing business continuation plans (BCP), on the basis of the immense danger to a going concern if the conducting of business has to be interrupted because of an information security incident such as an information leak or unauthorized access, or a catastrophe. Interest has risen with particular regard to anticipation of the problems that would be created by a pandemic outbreak of influenza, encouraging companies to study methods and prepare for maintaining their core information systems and ensuring sustained operation at such a time.

<3> Implementation of Audits and Evaluation of Information Security

Requirements for audits of information security systems have been in effect since April 2003, but the recent rash of information leaks is causing a gradual increase in the number of companies that are concerned with having third-party evaluations of their information security measures, or obtaining evaluations from customers or counterparties in trade. This has attracted attention to the arrangements at the non-profit Japan Information Security Audit Association (JASA), that performs audits and issued certifications when the audits show that certain standards have been met. Also, increased attention has been given to the PCI DSS (Data Security Standard) certification used in the credit card industry.

In addition to the above, in recent years at the same time as we have observed a rapid expansion of the SaaS and ASP market, security issues relevant to them have been of greater interest and in January 2008 the Ministry of Internal Affairs and Communications released security measures guidelines for ASP and SaaS operators.[8] Similarly, METI has begun to study guidelines for companies providing outsourcing services and public announcement of them is expected in the near future. These guidelines would have much in common with the items given as requirements for ISMS and Privacy Mark certification, and will contain requirements related to methods of processing information and to contractual arrangements; in some cases detailed requirements are expected to be made.

[7] See http://www.meti.go.jp/policy/netsecurity/sec_gov-TopPage.html

[8] See http://www.mhlw.go.jp/shingi/2009/02/dl/s0213-8i.pdf

Moreover, inquiry is now ongoing with respect to one aspect of the security approach by IT services businesses, studies are proceeding on methods whereby customers and development vendors can share a common awareness with respect to non-functional requirements such as response capability, the security, and the resistance to breakdowns of information systems, that are extremely important or influential when business operations of a customer are made to work by means of a system.[9] For example, this would be the case when prior agreement by the customer would be obtained with regard to specific aspects of applicability or application of a security patch to a certain system, namely the scope to be covered by the patch, rate of application, timing of application, and so on, whereby there would be no variance from the design requirement of security management, and the estimated costs would be acceptable. At present this approach is limited to the major system integrators, but it is anticipated that in time it will spread throughout the industry.

3 Present Conditions in Security Business

A given company is prone to emphasizing cost aspects of its own security measures, but at the same time security represents a business opportunity for companies in the IT services industry. The annual growth of security business, influenced strongly by the Personal Information Protection Act, has been in the 15 to 25% range, but according to a recent study report released in March 2008 by METI and the Japan Security Network Association (JNSA),[10] the growth rate has slowed since 2007. It is believed that this is in good part to having reached a plateau in terms of the taking of measures for protection of personal information. While a high level of growth is expected for the future on the strength of stronger internal control measures and compliance with J-SOX requirements, the outlook is for the growth rate to decline further under the influence of reluctance of large companies to invest in IT and lowering of prices as the relevant technology becomes more of a commodity.

5-3-2 Trends in Information Security Technology

Information security technology has advanced, in keeping with ongoing changes in connection with information security. Thin clients who had demonstrated only moderate growth in acquisitions of countermeasures to prevent leaks are showing renewed interest in secure methods of telecommunications from homes of employees, as one aspect of the above-mentioned awareness of the danger of a pandemic. Also, given the increase in importance of ID management, growing attention is being dedicated to technology trends relating to ID confirmation such as IC cards and electronic signatures, as well as, in connection with strengthening of internal control, database security and timestamp technology as means of improving access control and encryption functions, to give examples of technology for prevention of tampering with logs and other electronic records and detecting such intrusions. There are also signs of strong efforts being made at studying how to assure security for systems provided in home appliances and game consoles.

Below we provide a summary of two instances of web application security and encryption technology, that are significant for that part of the information services industry involved in building and operating information systems.

1 Web Application Security

Online shopping, internet banking, online trading, information search, social networking services and other web services have become solidly entrenched in daily life. These services are provided by means of programs that are called web applications, and in the Information Security White Paper mentioned earlier attention is given to the trend of danger that vulnerability of these web applications is being exploited more frequently than before.

[9] See http://www.nttdata.co.jp/nfr-grade/index.html

[10] See http://www.meti.go.jp/policy/netsecurity/19fy_marketresearchreport.pdf

It has been found that many times vulnerability of web applications originated in application design flaws and mistakes in web server settings. According to the report “Computer Virus/Unauthorized Computer Access Incident Reports, issued by the IPA, cross-site scripting and SQL injection, which had been problems since some time previously, now account for about 70% of all reported cases. That these vulnerability instances are still being discovered in programs shows that awareness of these dangers to web application security has not risen among the system architects, and indicates need for the industry as a whole to tackle the problem.

In addition, in a continuation of the situation of a year ago, in keeping with further diffusion of Windows Vista and IE7.0, with their security-enhanced OS and browsers, the industry faced a challenge in dealing with issues related to c of web applications. Even though the strengthening of security functions and periodic release of security patches are to be welcomed, no small burden on the companies that are building and operating information systems is generating in association with the new versions and patches that are being continually released.

Here, we provide a brief summary of three cases of technology that has attracted attention: secure programming, vulnerability detection tools and service, and phishing countermeasures, all related to web application security.

<1> Secure Programming

It is most important that companies engaged in designing and building information systems prevent vulnerability from being creating the process of design and production. The IPA Security Center has mounted a robust effort to promote countermeasures, and in March 2008 released the third edition of its “How to Build a Safe Website.”[11] The revised edition is expected to be extremely useful, as it includes considerable information on failures – web applications that suffered from cross-site scripting and SQL injection attacks, including the problematic codes, explanations and examples of methods of solving problems.

<2> Vulnerability Detection

Attention is being garnered by tools and services for detection of vulnerability in systems and products prior to their release, in systems under operation, and at websites. There has been an increase in particular in the sites that have obtained a check on their web applications. Further, for PCI DSS certification, as mentioned above, vulnerability assessment is required

<3> Phishing Countermeasures

Advances have been made in both technological and institutional methods of dealing with phishing whereby personal information is stolen and frauds are committed. On the technological side, more website owners have secured the EV-SSL certificate, and at financial institutions in particular, increasing use is being made of soft keyboards as a means of preventing information theft. In September 2008, the Council of Anti-Phishing Japan[12] released “Phishing Countermeasure Guidelines as part of its activities to promote better understanding of the problem and what can be done about it, among service company operators and the general public.

[11] See http://www.ipa.go.jp/security/vuln/websecurity.html
[12] See http://www.antiphishing.jp/index.html

2 Encryption Technology

As reported in the Information Services White Paper for 2008, the safety of RSA1024bit and SHA-1 encryption, which have been widely used for electronic signatures and SSL as means of assuring secrecy of information and data, is now thought by specialists to be compromised. Considering that in 2010 the Federal Government in the United States will review its encryption, in 2010 encryption will certainly be in the forefront of security related discourse.

There would be several levels to encryption compromise but because it is possible that an extremely large impact could be imparted to operators of IT systems and companies engaged in building and operating information systems, even though there is no imminent danger, it is necessary to be alert to related trends. In particular, close attention is deserved by information from Cryptographic Research and Evaluation Committees (CRYPTEC),[13] a Japanese organization that evaluates and monitors the security of e-government recommended ciphers. In Japan, since 2009 a search for and evaluation of new ciphers has been taking place and in 2013 it is planned that a review will be made of the recommended ciphers for e-government use.

In the building of information systems, the required conditions and measures include (1) being able to choose from among a multiple number of cipher algorithms, (2) to be able to use cipher modules and as interchangeable components, and (3) to be able to use strong encryption ciphers.

5-3-3 Trends in Information Security Policy

In 2005, the National Information Security Center (NISC) [14] was created within the Cabinet Secretariat, and in 2006 issued its First National Strategy on Information Security policy paper. The year 2008 was the third year for the implementation program of this policy, Secure Japan, and during that year study was begun on what will be the second policy paper. Here, we summarize these activities and touch on the influence they are having on the information service industry.

1. The National Information Security Center

The NISC, created in April 2005, has the mandate to formulate basic strategy proposals and function as a national center for the support and promotion of the security of governmental entities and core infrastructure. As of the end of September 2008, 72 specialists from government and the private sector were engaged at NISC. During fiscal 2008 the work of the Center included the drafting and presentation to the government of the Secure Japan 2008 document mentioned above, drafting the proposal for the Second National Strategy on Information Security policy paper, revision of uniform standards for government offices, and deciding on changes to be made to move away from the cipher algorithms SHA-1 and RSA1024.

2. Secure Japan 2008 and the Second National Strategy on Information Security

The Information Security Policy Council, established in July 2005, formulated the three-year (fiscal 2006 to fiscal 2008) First National Strategy on Information Security, covering abroad scope of information security issues, and this was adopted on February 2, 2006. As part of the program for the third year of this plan Secure Japan 2008 was formulated, in June 2008. This document included 157 specific measures that had been or were to be implemented in fiscal 2008, and 22 orientations for policy to b e worked on in fiscal 2009. Regular checks are made on progress in realizing these policies and fine-tuning is done as required. As of December 2008,

[13] See http://www.cryptrec.go.jp/
[14] See http://www.nisc.go.jp/index.html.

22% of the policies had been implemented leaving the remaining 78% to be implemented within the fiscal year (or target time), and implementation was not certain for only 2%. From this it can be said that policy implementation is progressing adequately.

Among the 157 policies, the following that have been or are to be implemented and that have a close relation to information services companies are the following; they deserve close attention by the industry and those with a special interest in it and its functioning.

- Revision of guidelines for improving the reliability of information systems
- Support for the selection and procurement of systems, with special emphasis on information security
- Study of measures for security by design (SBD) in order to ensure information security for e-government, from the planning and design phases onward
- Measures for IPv6 for e-government systems
- Measures to counter the weakening of safety of hash coefficient SHA-1 and public-key encryption algorithm RSA1024
- Promotion of use of high-safety, high-reliability encryption modules (study of a certification system for encryption modules)
- Review of government procurement (because of linking security measures to market values)
- Wider utilization of the model contract for information systems
- Wider utilization of SLA guidelines for SaaS

Further, in February 2009 the Policy Council approved the Second National Strategy on Information Security, that will be of central concern for a three-year period starting in 2009. Fundamentally it is an extension of the first policy paper, but whereas the first paper laid emphasis on preemptive measures, it is characteristic of the second paper that it includes the message that it is necessary to have a “society prepared for adverse events,” so that in the event of a calamity or catastrophe, coolheaded, swift reaction is possible and successful accomplishment of the work of recovery work is facilitated. This will make it more incumbent on companies in the information service industry to adopt business continuation plans.

The promotion of these policies by the government has the drawback of requiring, to a greater or lesser extent, greater burdens to be borne by the information services industry, but one should not lose sight of the benefits, in terms of improvement of information security and making use of the opportunity presented by system renewal to make such improvements. We may also think that by proactively dealing with issues related to these policies, a company will be able to improve its competitiveness.

3. Early Warning Partnerships for Information Security

The concept of Information Security Early Warning Partnerships is based on METI’s Standards for Handling Software and Other Vulnerable Information (METI Directive No. 235, released July 8, 2004) provides a framework for public entities such as IPA and Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) as well as product developers, website operators and others to plan for the communication of information among them prior to vulnerability –related information becoming known to the general public, so that they can create and adopt countermeasures to the vulnerability of software products, websites, and more. Secure Japan 2008 calls for stronger measures along these lines. JISA, in cooperation with JEITA, drafted a document titled Guidance for Arrangements Relating to Vulnerable Information at SI Operators and published it in August

2005.[15] The document is a manual for SI operators, product developers and vendors to cooperate in connection with countermeasures against vulnerability by establishing organizational arrangements and being methodologically prepared for swift and appropriate action.

Further, annual study meetings on dealing with vulnerability information are held by IPA. The meeting in fiscal 2008 took up the matter of how to foster the spread of vulnerability countermeasures among information service company (especially system integrators and web designers) and information system administrators, and guidelines were drawn up for vulnerability countermeasures for website builders.

5.3.4 Trends of International Standards for Information Security

It can be said that interest in international standards for information security is high in Japan. Because there is a high level of interest in making use of standards that have been approved by international organizations, as benchmarks for evaluating the safety and reliability of technology for information security, requests for application of such standards by customers and as conditions for bidding for contracts have increased. Provided below is an explanation of the trend concerning standards for business continuation management, that is considered to have particularly strong impact on companies in the information services sector.

1. Standards Related to Information Security Management

Related parties in Japan have become fully familiar with Information Security management System (ISMS) certification as an international standard for information security management. According to a tabulation announced by JIPDEC[16] as of November 2008 more than 2,800 enterprises in Japan were certified, and a survey of information service businesses by JISA in 2007 found that 57% of questionnaire respondents stated that they had received accreditation.

ISO/IEC 27000 is a family of generic information security related standards. It comprises a growing number of individual standards, the most well known and widely used being ISO/IEC 27002, ISO/IEC 27005, and ISO/IEC 27006 (formerly known as ISO 17799). The ISO 27002 standard is the rename of the ISO/IEC 17799 standard, and is a code of practice for information security. ISO/IEC 2005 is the methodology independent ISO standard for information security risk management which was released in June 2008. ISO/IEC 27006 is the standard which offers guidelines for the accreditation of organizations which offer certification and registration with respect to an ISMS (Information Security Management System) which was released in March 2007. At the same time new standards will be offered soon. They are ISO/IEC 27003 and 27004. ISO/IEC 27003 will be the official number of a new standard intended to offer guidance for the implementation of an ISMS and ISO/IEC 27004 will be the number for a new standard covering information security system management measurement and metrics.

2. Standards Related to Business Continuation Management

Because of the importance to information service companies to have assurance that they can carry on business without interruption, interest has been rising in business continuation planning on the premise that a catastrophe, major IT failure, or pandemic might occur, and in business continuation management as the strategic means of carrying out such a plan. Regarding business continuation management, the British Standards Association has adopted BS 2599-2. Whereas we have the term Information Security Management System in the case of business continuation we have the term Business Continuation Management System. As of January 2009, three Japanese companies had acquired certification for BS 2599-2.

[15] See http://www.jisa.or.jp/security/vulnerability.html
[16] See http://www.isms.jipdec.jp/

JIPDEC began certification activities[17] based on BS 25999-2 in August 2008, and expects to start formal certification after being authorized as the official domestic agency for this, in August 2009, a development that bears watching.

[17] http://www.isms.jipdec.jp/bcms/index.html

5-4. Reliability Control Indicators

While information systems are an integral part of our daily lives, and a part of the social and economic infrastructure, at the same time there is an urgent requirement to ensure and improve the safety and reliability (or dependability) of information systems against the threats of information system breakdowns or interruptions and damage on a large scale, as such problems would have immense impact on society. In this section, we present an overview of how the government and the information services industry are dealing with this challenge, as well as an overview of how IT vendor companies in particular are using quantitative management benchmarks in their approach to the challenge.

5.4.1 Background and Trends of Reliability Improvement Activity

1. Necessity for Improvement of Information System Reliability

Subsequent to the system malfunction and stoppage at the Tokyo Stock Exchange in 2005, there have been many incidents of large-scale system failures; in 2008 failure of securities and financial systems caused short interruptions and delays in transactions and the transfer of funds, and a passenger airline's system malfunctioned and the cancellation of 130 flights and inconveniencing of about 70,000 passengers resulted. Any prolonged interruption of service due to a failure of a large-scale system will have great impact on economic activities of the nation. For that reason, while the potential societal influence of information system failure increases day after day, the need for improved safety and reliability is increasing.

2. Major Approaches to Improvement of Reliability

The causes of system failures in 2008 were diverse. They include mistakes made in programming, mistakes made in initializing, mistakes made in configuring servers, mistakes made in selection of alphanumeric codes, and deadlocks caused by a massive number of orders. Even though many of these events could have been prevented, in the background for these events having had such a great impact is the large scale of the systems, and their complexity.

A number of factors, working in combination, were operative at the time these events occurred. They include the existence of ambiguous indicators for the reliability and safety that information systems are required to have in order that the relevant services can be delivered, and absence of organizational arrangements suitable to the systems, and of managerial arrangements for the processes of development, operation and maintenance.

The following approaches to dealing with the challenges of improving reliability and safety that are now being taken by METI and companies as well as industrial organizations deserve mention.

<1> Reliability Guidelines and Reliability Evaluation Metrics (Establishment of methods for evaluating reliability)

As one aspect of Policies for Improvement of Dependability of Information Systems, at METI, Guidelines for Improvement of Information System Reliability (hereafter, "Reliability Guidelines") were issued, in June 2006. These have the objective of facilitating the equipping of information systems with the reliability and safety that they should have, by providing the items that related persons should follow or are recommended to follow in their work extending from planning and developing information systems to their operation and maintenance. In 2008 the second edition was released (see Table. 5-5). IPA/SEC drafted a checklist of items for evaluation of system reliability, based on these Guidelines. Vendors and user companies can refer to this checklist to ascertain the reliability of their own systems.

Chapter	Item
II. Overall Key Points for Reliability and Safety Improvement	1. Responsibilities of related persons
	2. Responsibilities of the management
	3. Implementation of measures for both prevention and post-event action
	4. Necessity for a multi-faceted approach for improvement of reliability and safety
	5. Fundamentals of actions to deal with damage to information systems
III. Overall Key Points for Planning, Development and Operation & Maintenance	1. Key points at the planning stage
	2. Key points at the development stage
	3. Key points at the operation and maintenance stage
	4. Key points related to damage countermeasures
	5. Key cross-cutting items spanning the entire system lifecycle process
IV. Technology Items	1. Utilization of development methods and tools
	2. Key points for use of technology for improvement of reliability and safety
V. Organization Items	1. Training and education for human resources development
	2. Organizational development
VI. Items Related to Business Customs, Contracts and Laws	1. Clarification of key points in contracts
	2. Clarification of role allocation and responsibilities when there is division of work concerning building information systems

Table 5-5
Main Items in Guidelines for Improvement of Reliability and Safety of Information Systems (Abridged)

Source: *METI "Reliability Guidelines," June 2006*

<2> Action Program for Information Securities Measures for Critical IT Infrastructure (Prevention of recurrence and spread of problem in systems of major infrastructure components)

Need exists for implementing various measures so that IT breakdowns or malfunctions in the areas of core infrastructure[18] do not inflict great damage to the lives of the people, and to social and economic activity, but Japan is approaching the limit to what can be expected from steps taken independently by individual operators of infrastructure. so the following approaches are being taken to improve information security through closer teamwork by the government and public sector, as set forth in the Action Program for Information Securities Measures for Critical IT Infrastructure (hereafter, "Action Program," approved by the Information Security Policy Council in December 2005).

- Improvement of safety standards in ten fields
- Creating and Improving Capability for Engineering of Protection, Technical Operation, Analysis and Response (CEPTOAR), for strengthening of arrangements for the sharing of information in connection with IT damage in infrastructure fields
- The Action Program, that calls for implementation of cross-cutting practice according to scenarios postulating actual events, is at the stage of review with regard to analysis of mutual dependency in important areas of infrastructure and information sharing and communication in times of emergency, the review having begun in December 2007 and to last one year.[19]

[18] Telecommunications, finance, air travel, railway service, electric power, town gas, medical services, water supply, distribution of goods, governmental and administrative services.

[19] Arrangements call for reviews to be done at an interval of three years (over a period of one year starting two years after the start), on the basis of evaluation and validation of progress.

<3> Study Group on Non-functional Requirements Grading (Improvement of common awareness and role allocation of users and vendors)

Six SI companies[20] formed a Study Group on Non-functional Requirements Grades for Making Visible the Requirements of Operators of Domestic System Infrastructure (hereafter, "Non-functional Grading Study Group") in April 2008, to study "non-functional requirement grades" in order to realize methods for making visible and confirming functions necessary for systems, reliability, security and other non-functional requirements. By determining grades for each item of non-functional requirements and showing it as a decision tree, it will be possible to make clear in the form of a contract details that until now had not been uniform or sharply defined among vendors. The same organization has set up a Vendors View Study Group, to study from the users' viewpoint the manner whereby design documents are written and the method whereby agreement is obtained, in order to prevent differing or conflicting awareness between users and vendors during development. At this time, by means of cooperating with METI's Reliability Guidelines, work is being done for drafting a proposed list of non-functional requirement items and items for confirmation that would result, and for validating the efficacy of the proposed grading standard.

<4> "Making Reliability Visible" by means of Quantitative Control Indicators (Use of matrices to ensure reliability)

JISA, through its Committee for Improvement of Information System Reliability, has carried out a study, "Control Indicators for the Realization of Best Practices for Reliability Improvement," for the two-fold purpose of proposing and promoting concrete measures to visibly measure security level and to enhance the reliability in the industry, particularly by making efforts in the industry for providing both quantitative indicators of monitoring reliability throughout the lifecycle process and methods for using the indicators. This study collected and organized control indicators, for development, maintenance and operation, that have been actually put to use by companies (primarily JISA members) and both presented them as practices and showed their relationship to the METI Reliability Guidelines. This provided the industry with specific suggestions for the improvement of reliability. Details are provided in the following section.

Thus, studies have been made regarding desiderata for the reliability of information systems and software, regarding policy for ensuring proper reliability, and regarding approaches used by both users and vendors for improvement of reliability. Other than this, as approaches to the issues of reliability and security, work has been done regarding transactions that influence reliability, a model contract for revision of contracts, and improvement of guidelines for electronic authentication.

[20] NTT Data, Fujitsu, NEC, Hitachi, Mitsubishi Information Systems, Oki Electric.

5.4.2 Approaches to Reliability Improvement Through Use of Control Indicator (Metrics)

This section is based on the "Control Indicators for the Realization of Best Practices for Reliability Improvement" study by the JISA Committee for Improvement of Information System Reliability, concerning "Making Reliability Visible" by means of quantitative control indicator (Use of metrics to ensure reliability) introduced in (4) above.

1. Background for Use of Control Indicators for Reliability Improvement

The background for use of control indicators for the information system lifecycle (development, maintenance, operation) consists of change in the external environment of the development and operation of information systems (replacement of system technology), and issues related to ensuring system quality under conditions of changing project characteristics (shortening of development time, demand for higher quality). It is necessary to have an understanding, first of all, of what entails system quality, and to know the nature of the relevant development, maintenance and operation processes before one can work on these problems. These actions are, fundamentally, taken after the fact. Next, forecasts are made and measures considered, including analyses of the trends of quality and conditions, for the purpose of developing countermeasures in advance of the occurrence of a problem; control indicators are used at this time. The control indicators are used to measure conditions of a system or process (make them visible, make them measureable) and management is performed on the basis of their quantitative values, enabling judgment of whether conditions are good or not, determining the cause of a condition, forecasting conditions, and exercising control, as well as solving problems, preventing problems, and providing a basis for objective discussions by related personnel, including people from user companies.

2. Approach to the Introduction and Use of Control Indicators

A wide variety of issues and targets (or goals) related to those issues are associated with problems encountered in assuring the quality of information systems. When control indicators are determined, it is for the purpose of studying ways to deal with those issues, and the indicators are required to be capable of use in measuring conditions so that the conditions can be understood and controlled. Moreover, they can be utilized in a PDCA cycle, by using them to gain an understanding of actual conditions, to learn the gap between those conditions and targets or goals, and to take action to control matters.

The steps to introduce and put to use control indicators start with gaining knowledge of present conditions (including deviancies) by collecting control indicator data for the relevant individual projects, followed by causal analysis to enable devising of measures to remedy the problem or to prevent a problem. Once the data for the entire organization has been collected, what is particularly important is that organizational plan values are determined on the basis of that data, real-time control of project administration is adjusted accordingly, and organizational activities on behalf of improvements are begun. Because of this, there are two PDCA cycles for control indicators, the cycle(s) for individual projects, and the cycle for organizational (company-wide) activity.

<1> The PDCA (Plan-Do-Check-Act) Cycle for Projects

The project manager or PMO determine the target or goal (base) values [P for Plan], obtain quantified values for the indicators used for the project [D for Do], ascertain the gap between the project target values and current conditions [C for Check], and exercise control as required [A for Act]

<2> The PDCA Cycle in Organizational Activity

The company's quality assurance department and the project management office (PMO) that controls company-wide activities are the main body for determining the Plans for the organization; maintains an understanding of common phenomena (mostly problems) encountered in projects of the organization [D]; undertakes the analysis and causal analysis of the conditions of organizational phenomena [C]; and proposes and carries out action for use of managerial benchmarks to remedy matters and ensure goals are accomplished [A].

<3> Use and Effect of Control Indicators Through the Entire System Lifecycle

A system that has been constructed by means of the development process both provides service through its operation and monitors conditions; it discovers variations or deviations and on the basis of that and change in the external environment performs maintenance tasks of correcting and improving, and then as the improved system functions this process is repeated.

A conceptualization of system operation must be taken into account at the time of development, how the development work is done greatly influences the efficiency of work performed for maintenance, and moreover imparts strong influence to efforts at assuring and improving system reliability. The improvement of reliability begins with the realization of high reliability at the time of development, and consequently contributes to maintaining and improving reliability through operation.

Development, operation and maintenance are the major categories of activity that make up the lifecycle of a system, and the control indicators for the three phases, taken as a whole, contribute to improvement of reliability during the lifecycle. For example, if a problem in the system can be detected by use of control indicators during operation, and remedial measures can be determined in quantitative terms, maintenance can proceed according to an order of priorities, and activities such as planning can be optimized (Fig. 5-4).

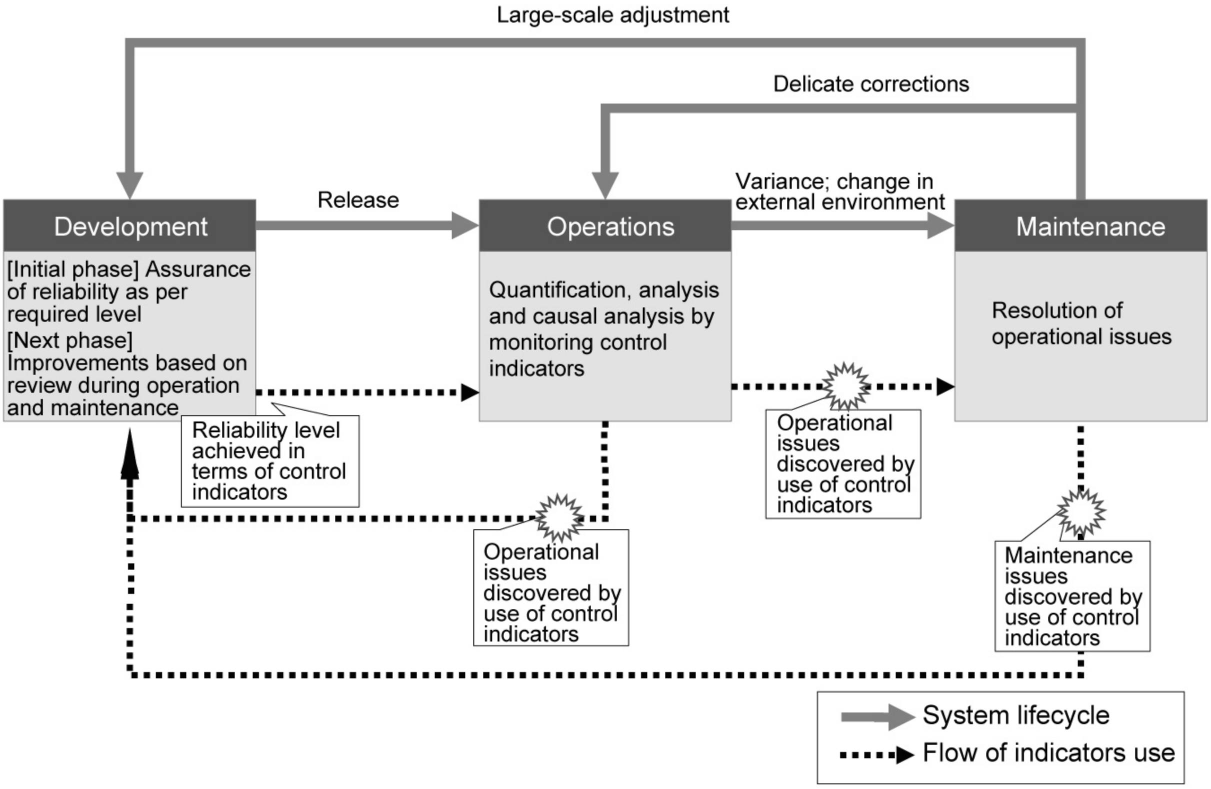
Large-scale adjustment
Delicate corrections
Release
Variance; change in external environment
Development
Operations
Maintenance
[Initial phase] Assurance of reliability as per required level
[Next phase] Improvements based on review during operation and maintenance
Quantification, analysis and causal analysis by monitoring control indicators
Resolution of operational issues
Reliability level achieved in terms of control indicators
Operational issues discovered by use of control indicators
Operational issues discovered by use of control indicators
Maintenance issues discovered by use of control indicators
System lifecycle
Flow of indicators use

Figure 5-4
Use of Control Indicators Throughout the System Lifecycle

Source: *"Control Indicators for the Realization of Best Practices for Reliability Improvement" Study by the JISA Committee for Improvement of Information System Reliability*

<4> Use of Control Indicators by IT Vendors, and the Efficacy of the Indicators

1) The development and maintenance processes

In development, in addition to using control indicators for evaluation of processes and products, the indicators can be used for evaluation performed from the viewpoints of both user and vendor companies as well as in overall terms. Further, control can be exercised by using the indicators for development scale, and quality characteristics that influence productivity, software and hardware conditions, number of modifications, and the indicators can be useful for communicating with customers. Besides these uses, indicators can be incorporated into pricing systems.

Indicators for joint use in the development process include indicators for design phase review, the number of bugs detected during testing, and for monitoring delivery schedule performance (Table 5-6).

	Indicator	Sample definition
Review	Review identification rate	Instances of identification/Scale of review X 100
	Rate of number of reviews	Reviews implemented/Planned reviews X 100
	Review speed	Scale of review/Review time
	Review advance identification rate	Number of bugs detected during review/Total number of bugs detected during review and testing X100
	Review efficacy	Instances of identification/Processes reviewed X 100
Testing	Test case density	Number of test cases/Scale of actual source code
	Test coverage (rate)	Branches for completed tests/Total branches X100
	Desktop debugging identification density	Number of instances of desktop debugging detected/Scale of actual source code X 100
	Number of bugs detected for each process	Number of bugs detected
	Number of bugs after release (density)	(Ratio of) fault incidents to the scale of release during a specified post-delivery period
Delivery	On-time rate	Number of instances of on-time delivery during a specified period/Total number of completed deliveries X 100
	Delayed rate	∑(Contract delivery day minus delivery day)/∑ project days X 100

Table 5-6 Control Indicators Jointly Used in the Development and Maintenance Processes

Source: *"Control Indicators for the Realization of Best Practices for Reliability Improvement" Study by the JISA Committee for Improvement of Information System Reliability*

In the maintenance process, as in the development process, control indicators are used for determining the nature of problems and causal analysis.

2) Operation process

During the operation process, in order that there can be accurate communication based on a common awareness regarding the user and the management level of operation, a multiple number of control values are collected monthly as the basis for the ultimate target, namely the SLA agreed upon with the user, and the results of analysis of the data are provided to the user for use as feedback. The level of control indicators used for this is determined on the basis of the degree of importance of the system. Other than this the indicators can be used to monitor and evaluate services provided by an outsourcer.

There is a tendency for control indicators for the occurrence of fault, transfers of control, operation, functions and security to be jointly used (Fig. 5-7).

	Indicator	Sample definition
Condition of occurrence of problems	Number of instances of problem occurrence, by online, batch, or delivery groups	Change in number of instances and share with the passage of time (monthly)
Transfers of control	Number of cases of jobs registered, share change with the passage of time (job registry, audit registry, program registry)	Same as above
Operation Control	Online open conditions (opening success rate; special task conditions)	Same as above
	Online usage conditions (number of transactions, year-on-year change)	Same as above
	Batch job transfer conditions (number of job transfers, special job conditions)	Same as above
	Conditions of service delivery (number of instances printed, number adjusted, number sent)	Same as above
Performance control	Online operating conditions (resource usage conditions, backlog	Same as above
	Batch job execution status (rate of completion within deadline)	Same as above
Security control	ID control (host, server)	Same as above
	Personnel facility entry/exit control	Same as above

Table 5-7
Control Indicators Jointly Used in the Operation Process

Source: *"Control Indicators for the Realization of Best Practices for Reliability Improvement" Study by the JISA Committee for Improvement of Information System Reliability*

The effects of utilization of control indicators, in addition to "improvement of reliability" through reduction of damage, trouble, and human error, are recognized as including the early discovery of risk and damage, improvement of project management by preemptive prevention through the use of causal analysis, understanding and improving characteristics of the organization by means of better knowledge of conditions over a period of time, and improvement of organizational management by such means as the use of internal controls.

5.4.3 Issues for the Future

It appears likely that information systems will become larger more complex, more influential over society's activities, and more important overall, in keeping with expanded and increasingly technologically advanced requirements that user companies have for their information systems. With the continued evolution of a division of labor connected with these systems among companies and organizations in Japan and abroad, it will be increasingly vital for there to be practical work at assuring reliability at every work site if overall reliability is to be secured. It is therefore important not merely to make public the Reliability Guidelines of METI, the Action Program, the work of the Non-functional Grading Study Group, the control indicators activities of JISA and similar studies, documents and activities, but also for the industry as a whole to go to work on behalf of actual application of the various measures that have been developed, and for wider appreciation of the importance of those efforts.

Further, as in the case of the work of the Non-functional Grading Study Group, with regard to acceptance inspection of systems, it is desirable that both user and vendor objectively see the system as being suitable, and for each to understand the other. The actual situation at present, however, is that ambiguous contracts and specifications have often obscured matters in determining approval of the condition of a system. Because of this, it is necessary to eliminate ambiguous contracts and specifications, and firmly establish arrangements for smooth communication between users and vendors, so that there can be no divergence of views on subjects where the two should be in agreement.

JISA is engaged in introducing to the world activities by the software industry in Japan on behalf of the improvement of reliability, and to facilitate interdisciplinary discourse with interested parties has made presentations at a conference sponsored by the OECD, METI, and Japan's Research Institute of Economy, Trade and Industry (RIETI).[21] JISA has also sponsored symposia to promote the use of control indicators in industry and has introduced what it deems to be good practices identified by its study of control indicators. Moreover, on the basis of the JISA study of control indicators, JISA has advocated the use of quantitative measures that would be acceptable to both users and vendors and has contributed to the development and use of control indicators for reliability of information systems. It is considered important for the future for the results of these efforts to be made widely known among both users and vendors, and for the organization, in the interests of both users and vendors, to continue robust activities on behalf of the improved reliability and safety of information systems.

[21] In an Industry Architecture and Technology Perspectives session, in the OECD-METI-RIETI Conference, Innovation in the Software Sector, October 6, 2008.

5-5. PERSONAL INFORMATION PROTECTION ACT AND THE PRIVACYMARK SYSTEM

5.5.1 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.

5.5.2 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.

5.5.3 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.

5.5.4 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. 5-5).

Categorizing the inspection organizations for PrivacyMark by type, JIPDEC itself accounts for over 60 percent of the total (Fig. 5-6). 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. 5-7).

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.

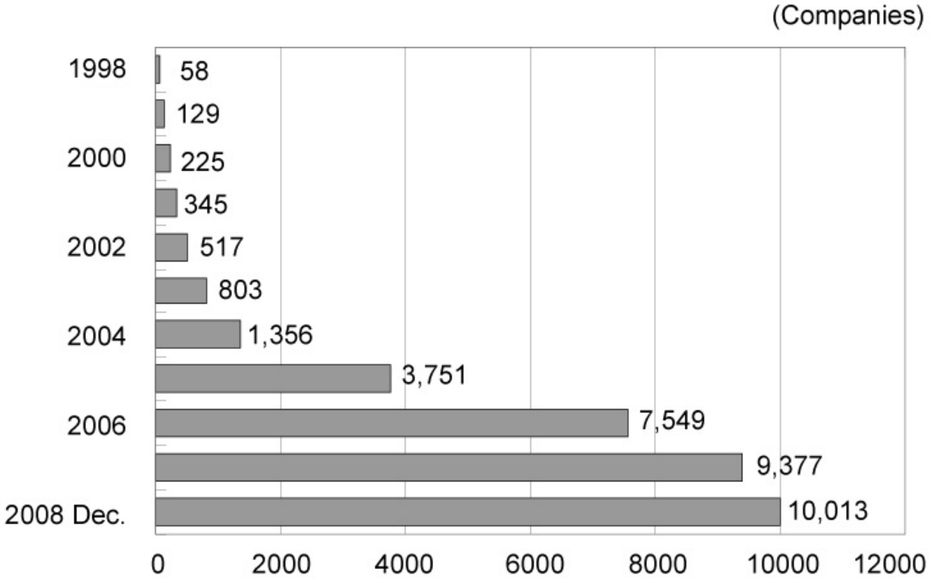

Figure 5-5
Growth in the Number of PrivacyMark Certified Businesses (aggregate total)

Source: *JISA " Annual Vendor Survey 2008"*

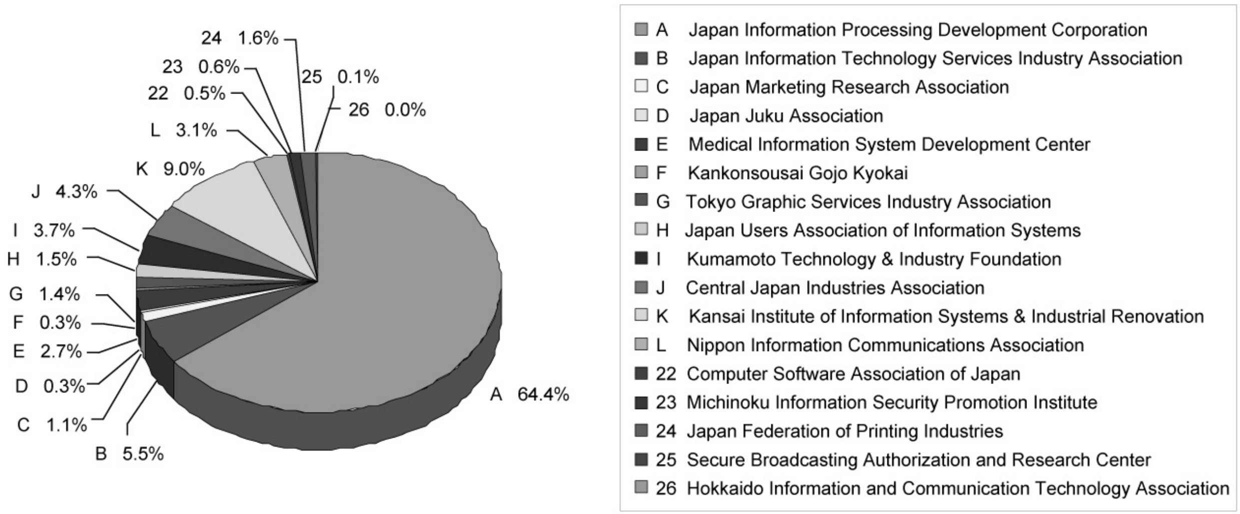

Figure 5-6
Ratio of PrivacyMark Companies According to Issuing Inspection Organizations (total 10,013 companies)

Source: *Produced by JISA from JIPDEC information*

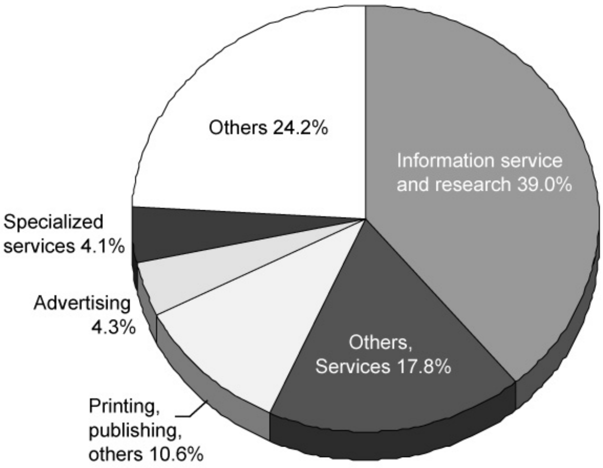

Figure 5-7 Certified Businesses by Sector (Top five industries; effective total as of Dec. 31. 2008: 10,013 companies)

Source: *Produced by JISA from JIPDEC information*

5.5.5 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.

5-6. TAX AND ACCOUNTING TRENDS

The major point of interest in the IT services industry during 2008 revolving around taxation and accounting was the need to take urgent action in advance of the start, from April 1, 2009, of new accounting standards for construction contracts, announced towards the end of the preceding year, for construction contracts by listed companies, their subsidiaries, and their affiliated companies. In addition, during fiscal 2008 there was an extension and expansion of tax regulations relating to strengthening of the information infrastructure, and an extension of tax incentive for the development of human resources.

5.6.1 Developments in Fiscal 2008 Related to Taxation of IT Services Industry

In the reform of tax regulations during fiscal 2008 matters affecting the information services sector comprised (1) the extension and expansion of measures relating to improvement of the information infrastructure, (2) change in tax incentives for development of human resources, and (3) new treatment of corporate tax concerning the accounting standard for construction contracts.

1. Extension and Expansion of Measures Relating to Improvement of the Information Infrastructure

The tax regulations for improvement of information infrastructure were initiated as part of taxation reforms made in fiscal 2006. They are intended to expedite investment in information systems that assure security and improve reliability. Applicable to companies filing the type of corporate tax form called the Blue Form, they offer a choice of taking either a 7% tax deduction or a 35% special depreciation for fixed assets meeting the ISO/IEC 15408 standard. The following four changes were made in fiscal 2008. (1) This regulation was extended two years (to the end of March 2010). (2) The minimum applicable value of assets acquired for corporations capitalized at JPY100 million or less was lowered from JPY3,000,000 to JPY700,000. (3) Software that connects newly created departments or connects companies was added to the assets qualifying for this treatment. (4) Companies engaged in information processing via the Internet as SaaS and ASP were specifically included in the scope of the regulation.

2. Extension of Tax Incentives for Development of Human Resources

The tax regulations in support of development of human resources provide a deduction from corporate tax of small and medium enterprises of a certain percentage of the cost of employee training. Prior to the revision, the expense to which this was applicable was up to 20% of the average increase for education and training in the prior two accounting years, but this was revised and extended as follows. (1) The definition of qualifying companies was changed to corporations capitalized at JPY100 million or less excluding subsidiaries of large companies; sole proprietorships employing 1,000 or fewer persons. (2) Employees for which the incentive can be use: Employees, excluding those concurrently officers and excluding spouses of officers. (3) Incentive detail: The tax deduction is to be 8-12% depending on the share of education and training costs in total labor costs in the relevant accounting terms. (4) Duration of applicability: The incentive is in force from April 1, 2008 to March 31, 2009 (a one-year effective period).

3. New Treatment of Corporate Tax Concerning the Accounting Standard for Construction Contracts

Corporate tax treatment of long-term contracts was revised in keeping with adoption of an accounting standard for construction contracts included in accounting reforms made in fiscal 2008. The changes are as follows. (1) Development of customized software was added to the scope of work to which the construction progress (percentage-of-completion) standard is applicable. (2) Percentage-of-completion treatment for work done under contracts for JPY1 billion or more and lasting one year or more was made compulsory. Other accounting procedure is based on each company's accounting rules. (3) The treatment was made applicable for construction work begun during accounting terms starting after April 1, 2008. (4) Reserves against losses on construction contracts could be included in losses.

5.6.2 Developments in Fiscal 2008 Related to Accounting of IT Services Industries

1. Disclosure of an Accounting Standard for Construction Contracts, and Reaction of the Industry

In recent years there has been an acceleration of the movement towards international convergence of accounting standards, led by the European Union. Complying with this, the Accounting Standards Board of Japan (ASBJ) has been working at convergence of Japanese standards with the International Financial Reporting Standards (IFRS) drafted by the International Accounting Standards Board (IASB). The ASBJ, as part of its actions released Accounting Standard for Construction Contracts (Statement No.15) and the Guidance on Accounting Standard for Construction Contracts (Guidance No.18) on December 27, 2007.[22] This standard was drafted to conform to IAS 11, Construction Contracts. According to the new standard total contract revenue and percentage of completion of construction work at the end of the reporting period are to be estimated and reported in that period's income statement. When the outcome of construction work cannot be deemed certain during the course of work, the completed-contract method is to be used. The standard is to be applied on a project by project basis and does not require that completion of construction be used in principle.

As to the relationship of this accounting standard to the IT services industry, in Accounting Standard for Research and Development Expenditures, released by the Corporate Accounting Council of the Ministry of Finance in March 1998, it is stated that "treatment for customized software will follow that for construction contracts," and the new standard would be covered by this. Therefore, for only the portion of the IT services industry engaged in development of software, differing from the construction industry and engineering industry where architectural construction and production work is performed on the basis of contracts, the approach to this standard is not of itself a matter of complying with the IFRS. Nevertheless, from a time preceding release of this standard, the IT media had presented the IAS 11 standard with heading such as "Percent-of-completion Standard Applicable in Principle," and "Unification of Percent-of-Completion," as if the percentage-of-completion rule was applicable to all projects. This created a very strong impression among those persons charged with conforming to requirements. Then, details of the percentage-of-completion standard as a Japanese accounting standard were made known for the first time. This created a mood in large companies that had made early adoption of the standard that the effect on corporate management was recognized. Further, the multi-tier structure of the IT services industry contributed to the spread of reaction to this. That is, concern mounted that if the customer was using the percentage-of-completion method, the contractor would have to report the percentage of completion as of the end of the accounting

[22] See http://www.asb.or.jp/html/documents/docs/kouji-keiyaku/kouji-keiyaku.pdf

period. All sorts of conjectures circulated, because this accounting standard did not take up the matter of contracting for work. Although the companies obliged to follow this standard are companies required to be audited by a certified auditor or certified public accountant, the thought that companies other than these had to adopt the standard spread. Opinion was also divided among the auditors and accountants that between those persons who held the view that this standard was within the scope of IAS 11 and those who did not hold that view. This situation prevailed until only a half year remained before April 1, 2009 and the start of the new arrangement.

2. Actions by the Industry

JISA started its activities related to the accounting standards at the same time that drafting of the standards was begun, in early 2007, by surveying the situation regarding use of the percentage of completion method in the industry and studying issues encountered by those companies that already had begun to use the method. In the course of that, it was found that all companies were troubled by use of “construction” in this accounting standard as it referred thereby to architectural construction or shipbuilding or manufacture of mechanical equipment but it was questionable as to whether work on custom software was done on the basis of a construction contract. When comment was invited on the exposure draft at the end of September of that year, an opinion on this matter was submitted to the ASBJ.

Because it was felt that this opinion was not appropriately reflected in the final form of the standard, the following two reports were issued as part of efforts to contribute to the industry’s dealing with the subject.

<1> Explication of Major Points in the Accounting Standard for Construction Contracts, from the Viewpoint of Contract Production of Software

This document examined existing materials on software-related accounting with special emphasis on moot points the interpretation of which presented problems to JISA members in their efforts at applying the standard in their administrative work, with a commentary on the existing situation. The report also had the nature of being a legal commentary.

The significance of this report was seen to be the expectation that by its becoming widely disseminated among those responsible for management in information service companies, a common awareness with regard to issues related to customized software could be formed. It remained necessary for each company to act on its own in applying the standard, basing this on their own decisions and with consultation with their accountants and auditors regarding hazy points. It was thought that in such a case to respond using the results of study of the items in the report made by each company would contribute, from the viewpoint of the industry as a whole, toward fair accounting practices.

The accounting standard was examined from the viewpoint of customized software and an explanatory report for use in administration within each company was drafted and published. The contents of it dealt with the following.

1. Scope of application of the standard
2. The “substantial unit of transaction” in “realistic unit of transaction agreed by parties to a contract”
3. Environmental factors preventing completion
4. The “substantial” in “value agreed as realistic by the parties”
5. Reliable estimation of construction unit amount

6-1. The “advanced” in “origin of cost and advanced management regarding its estimation”

6-2. When all or part of production is contracted to another party

7. Cases for which use of the reserves for construction losses can be used

8. The shortness of “extremely short construction”
9. Inventory evaluation
10. Degree of “remarkable fluctuation” in “Simplified treatment of estimation of construction cost as of the end of a quarter”

<2> Manual for Application of the Percentage-of-Completion Standard in the IT Services Industry

Following on the above report on the accounting standard, this manual represents the results of study made with parties inside and outside of the industry, but primarily through the Finance and Tax Subcommittee of the Management Committee, and on the basis of experiences of companies that have used the percentage-of-completion method, has the objective of providing information necessary in the case of an information service company’s application of the percentage-of-completion method.

The manual has the following five chapters.

Chapter 1) The Thinking Behind the Percentage-of-Completion Standard

Chapter 2) Rules and Organization Required for Use of the Percentage-of-Completion Standard

Chapter 3) Project Management as Prerequisite for Use of the Percentage-of-Completion Standard

Chapter 4) Administrative Model Needed for Use of the Percentage-of-Completion Standard

Chapter 5) Operational Issues Related to Introduction of the Percentage-of-Completion Standard

In Chapter 1, the following three points are covered. (1) Advantages of use of the percentage-of-completion standard. (2) Indication of the process for determining the scope of application. (3) Considerations on the form of contracts. In Chapter 2, with the purpose of indicating the necessity for having that awareness, the roles and organization needed for use of the percentage-of-completion standard in large enterprises and small and medium ones are differentiated and described.

The third chapter provides an explanation of the system for project management that is a prerequisite for use of the percentage-of-completion standard, and provides basic information to facilitate the understanding of project management managers outside the development department and management staff at the company’s main office.

Chapter 4 provides a business model such as is needed for both project management and accounting when the percentage-of-completion standard is used. The procedural steps for project management are eight in number, and are linked to accounting work. Project management is explained using the following organization. (1) Overview and purpose. (2) Administrative flow (ToBe model). (3) Sample vouchers. (4) Minimum model. (5) Issues. Accounting tasks are explained according to the following organization. (1) Overview and purpose. (2) Administrative flow (ToBe model). (3) Sample vouchers. (4) Minimum model. (5) Hints from the minimum model for the ToBe model. (6) Issues.

Chapter 5 covers the major points to be studied concerning operational issues related to introduction of the standard.

5-7. IMPACT OF LAWS AND REGULATIONS ON TRANSACTIONS WITHIN THE INDUSTRY (WORKER DISPATCH LAW, SUBCONTRACT LAW)

The Law for Securing the Proper Operation of Worker Dispatching Undertakings and Improved Working Conditions for Dispatched Workers ("Worker Dispatch Law") was revised in March 2004 and is being strictly enforced for the manufacturing and IT services industry, in which contracting is widespread. And the guidance and supervisory regulations have been strengthened to eradicate deceptive contracts. Under the government's economic growth policy (Strategy for Raising the Bottom Line of Growth Potential (Master Concept)) announced in February 2007, in relation to the Subcontract Law (Act against Delay in Payment of Subcontract Proceeds, etc. to Subcontractors)[23] the need for further promoting proper subcontract transactions become stronger and efforts for improving knowledge of and for complying with the law were strengthened.

5.7.1 Overview of the Revised Worker Dispatch Law

1. The Worker Dispatch Law

The Worker Dispatch Law is exception to authorize the licensed company (authorization/notification) to dispatch workers (placing a worker under another person's direction or orders based on a supply contract), which is prohibited according to Article 44 of the Employment Security Law, on the condition that the supplier conclude the employment agreement with workers. If a party that does not have a dispatch business license engages in labor supply, or supplies workers other than those that it employs directly, not only the labor supplier but also the party receiving the labor will be punished.

Further, if the license holder does not conduct the dispatch of workers under the procedures proscribed by the Worker Dispatch Law, they will be deemed in violation. If workers are dispatched without a worker dispatch contract, this deemed to be a deceptive contract, and the labor supplier is in violation.

The Worker Dispatch Law was revised on March 1, 2004, and lifted its ban to dispatch workers to the manufacturing industry and to repeal restrictions on the length of dispatch. At the same time, guidance and supervisory regulations have been strengthened and the dispatch law implementation bodies were centralized into the prefectural labor bureaus.

2. Separation Standards for Dispatch and Work Contracts (including quasi-delegation)

A dispatch contract is a contract that commits to supply labor, and differs in type from business trust agreements (contracts that commit to the completion of a certain task or to work processing) such as work contracts and quasi-delegation, but they have in common that the result is the use of another person's labor. For this reason, when the Worker Dispatch Law was enforced, the (then) Ministry of Labor issued standards relating to business carried out by worker dispatch businesses and work contracts (April 17, 1986 Ministry of Labor Bulletin No. 37) as criteria for determining what constitutes a work contract (a "work contract" in the Worker Dispatch Law includes work contracts and quasi-delegation in civil law). Further, according to the separation standards and the "Voluntary Inspection table for Rationalization of the Work Contract" published by the regional labor bureaus, in order to be recognized as a work contract, a contract must satisfy both of the

[23] For an English translation of the law, see http://www.japaneselawtranslation.go.jp/law/detail/?ft=1&re=02&dn=1&ky=subcontracting&x=0&y=0&co=01&page=2

following two conditions: “independence of personnel administration” and “independence of business management”. “Independence of personnel administration” means that the contractor must supervise and command the workers it hires itself in terms of instructions on how to carry out work, attendance record management, workplace and allocation management, and the outsourcer may not engage in any supervision or commands. This means that the outsourcer must carry out any requests or communications such that they are not seen as supervisions or commands when assigning the work, and such that the other party’s freedom of approval and discretion are guaranteed.

“Independence of business management” means that in addition to carrying out accounting and legal processing as an independent business, business-related independence (having its own facilities and equipment required for the work, or possessing specialized technology or techniques) is also required, and the business must not simply be providing physical labor.

3. Implementation of Separation Standards in the IT Services Industry

The separation standards of the Ministry of Labor were strict in saying that only those that satisfy all the criteria will not be deemed as dispatch contracts,” and were especially difficult to comply with in light of the circumstances (on-site work for clients, using equipment lent by the client, man-hour x unit cost man-month contracts, etc) under which business is generally conducted in the IT services industry. Therefore, the (then) Japan Electronic Industry Development Association (JEIDA) and the Japan Information Technology Services Industry Association (JISA) jointly compiled industry standards and submitted them to the Ministry of Labor on April 21, 1986, requesting that they be used in the implementation of the Worker Dispatch Law.

In light of the particular work environment of the IT services industry, the industry standards allow the following: 1) continuous presence in outsourcers’ offices (with the condition that the seat be objectively separated); 2) work on equipment lent by the outsourcer; and 3) someone from the contractor does not always have to be present in the workplace. Nevertheless, the industry standards do not allow the outsourcers to select specific workers (i.e., to request submission of resumes or conduct interviews) and to specify the scope of work or give direct instruction to the person in charge except in emergency situations.

After the enforcement of the revised Worker Dispatch Law, the Japan Electronic and Information Technology Association (JEITA) and JISA requested on June 29, 2005 to the Ministry of Health, Labor and Welfare that guidance based on the industry operation standards be thoroughly implemented at he level of regional labor bureaus.

Additionally, in its plans for activities in fiscal 2008, JISA decided to work at resolving problems in the form of falsified transactions and round-tripping transactions, violations of the Worker Dispatch Law or the Subcontract Law, and problems of data breaches or compromises arising from the multi-tier structure of subcontracting.

5.7.2 Implementation of the Revised Worker Dispatch Law

The regional labor bureaus have designated the period between October 1 and November 30 each year for a “Dispatch and Contract Work Rationalization Campaign.” Group workshops are given and individual guidance is offered to business owners for the prevention of deceptive contracts. Especially after the Ministry of Health, Labor and Welfare published its Notice 0904001 “Current Approach to Eliminating Deceptive Contracts” on September 4, 2006 in the joint names of the heads of the Labor Standards Bureau and the Employment Security Bureau, the prefectural and city governments have begun to strengthen their supervision. As a result, the numbers of instances of warnings or guidance to subcontractors during fiscal 2006 increased by 2.7 times the level of the previous year, and in fiscal 2007 were at about the same level as a year before.

When warnings are issued, the offending company is ordered to review all of its contracts within a specified period, and to take remedial steps as required. This requires an immense amount of work and a strong impact on the subcontractor cannot be avoided. It has become an urgent matter for all companies to observe the above-mentioned separation standards, industry operation standards, and checklist prepared by the government's Labor Offices, and to strive for proper contracting as a matter of constant importance, while at the same time it is urgent that the information services industry as a whole consider this as a structural matter.

5.7.3 Issues for Assuring a Proper Structure of Transactions

The characteristics of contracting or delegating as administrative acts have independence. Because of this it is necessary to avoid acceptance of workers from a parent company for the educational purposes which could not be an independent execution of administrative work, and to avoid giving work to an operator who lacks the requisite capabilities. Further, it can also be taken that when instructions arise from the nature of administration and are for operators that when they arise from normal circumstances, they can be seen as being commands. On this point, caution is needed when the work at the customer is by just one person. In addition, even in the event that work requests are made through the responsible person in advance so that the responsible person is able to make judgments on selection of the person to be in charge, the sequence to be followed, and the schedule. It is desirable for this reason to avoid issuing requests daily, and instead to combine requests and make them once a week. The requests must be in writing for recordkeeping purposes and it is desirable to indicate without fail that if there is no written document, no request is being made.

There is a certain necessity for the existing structure for procurement of technology and personnel in the multi-tier contracting structure of IT services industry, but because the occurrence of problems in areas of both business control and compliance will tend to occur, it is necessary to avoid intervention in trade that does not involve the execution of the contracted work. On top of that, need exists for each company to make clear their own role and scope of responsibility, and to practice proper management in that regard.

There is no standard that if followed will end the dispatch of workers in violation of the law. However, a shift to worker dispatch in order to avoid deceptive contract and double-dispatch (when a worker dispatched to one company is dispatched from there to a different company) will not necessarily solve the problems in the information services industry where most of the workers are employed without a set duration of employment.

For type of work where the command and control is indispensable it is possible to choose the dispatch of workers tentatively. But in order to make the structure of transactions to be proper it is important to create an environment wherein reform of administration and improvement of rules will be done to allow the consignment of administrative work.

5.7.4 Trend of Reforming the Worker Dispatch Law

Accepting a resolution of the Labor Policy Council (a body advising the Minister of Health, Labor and Welfare) presented a bill to the Diet on November 4, 2008 for revision of the Worker Dispatch Law that was mainly concerned with prohibiting the dispatch of day laborers. While the bill included provision for a limit of 80% for dispatch of workers within a corporate group – which would have great impact on the information services industry – it also included easing of regulations. This easing, with the purpose of inducing conventional type dispatch of workers, provides for prohibition of advance interviews and elimination of the requirement to make an application for employment, in both cases with regard to workers engaged for an indeterminate period (limited to 26 types of work） . However, attention should be given to the strengthening of measures to eradicate deceptive contracts and violations at companies where employees have received dispatched employees.

5.7.5 Subcontract Law Implementation and Problems

1. Subcontract Law Implementation

The Subcontract Law aims to rationalize transactions within industry and protect subcontractors, and obliges parent companies (outsourcers) to carry out certain procedures (advance delivery of order documents, document retention, etc.) and prohibits specific acts. Trust transactions (information deliverable creation, information processing and other service provision) in the IT services industry are subject to this revised law enacted in April 2004.

Annual document inspection is carried out for the purpose of thorough implementation of the Subcontract Law and discovery of illegal transactions, and in 2007, 11,780 outsourcers and 43,031 subcontractors (only those creating information deliverables and providing services) were inspected.

From this survey and filings by subcontractors, a total of 1,191 cases were treated as alleged infractions of the Subcontract Law, and 1,040 drew warnings (eight recommendations). Although this result represents about a halving of alleged infractions and warnings compared to fiscal 2005, the results were higher by 210 cases in regard to alleged infractions and 113 cases in regard to warnings over the numbers for fiscal 2006, indicating that the transaction environment last year deteriorated somewhat.

According to data from the Fair Trade Commission for action taken, classified by industry, the information services industry accounted for 4.8% of all instances, making it a prominent industry in this respect. In a report from the Fair Trade Commission dated October 1, 2008, titled “Implementation of ‘Subcontract Transaction Rationalization Promotion Month and ‘Special Measures in Support of Subcontractors,’” the Commission stated “compilation of information collected on the basis of document review study during fiscal 2008 and implementation of a study emphasizing industrial sectors where there are many subcontracting problems,” from which it can be anticipated that this industry will receive special attention in future studies and surveys.

Further, turning to the type of violations that occurred, in comparison to manufacturing subcontracting and others, it was characteristic of IT services industry that failure to pay on the agreed date was most frequent (see Table 5-7).

The shares of each type of violation in the total was about the same as in the previous year from which it can be seen that improvement of failure to pay on schedule is the most important matter for observation of the law in the information services industry.

2. Subcontract Law Compliance Problems

Under the Subcontract Law, a violation can be deemed to have occurred based merely on the appearance of an act, without taking into account the specific circumstances of the transaction, so it is imperative to understand the standards of the law correctly. In particular in the IT services industry, there are many situations that require correct understanding of the law, the standards and one’s own business, such as the fact that regardless of the usual work contract and designation contract types, all transactions that involve deliverables are considered as deliverable creation trust transactions (for example, this means that a software development deliverable received on the 26th of the month under payment conditions of 25th closing date and end-of-following month payment would not be paid for until the end of the month after next (64 days later) and would violate the Subcontract Law). Other aspects include the fact that the application of the Subcontract Law depends on the attributes of the other party to the transaction (capital relationship with one's own business, type of business) and the substance of the trust transaction, and the need to determine which documents are subject to document retention and storing them appropriately.

At the Fair Trade Commission of the Small and Medium Enterprise Agency, November is designated each year as the Subcontract Transaction Rationalization Promotion Month, and during this time, subcontract rationalization promotion lectures are hosted nationwide, in order to spread the word about the Subcontract Law. Further, in June 2006, the METI compiled and published "Guidelines for the Promotion of Subcontract Rationalization" for the industries of formal and fabricated materials, automotive, industrial machinery, aircraft, textiles, telecommunication equipment and IT services and software. The respective order control and work implementation departments in the outsourcer and subcontractor companies must have a correct understanding of the legislation and ensure that these are incorporated in practices, and take measures to lighten the burden of individual ordering work (introduction of order issuing systems, etc.).

		FY2007		FY2006	
Breach of procedural requirements	Document preparation	920	53%	814	54%
	Document retention	266	15%	213	14%
	Subtotal	1186	68%	1027	68%
Breach of action requirements	Refused acceptance of work	8	0%	4	0%
	Failed to make payment on time	417	24%	368	24%
	Arbitrarily reduced amount paid	63	3%	42	3%
	Caused subcontractor to take back goods	0	0%	0	0%
	Unjustly set payment at below market price	13	1%	10	1%
	Forced subcontractor to purchase goods or services	15	1%	20	1%
	Early settlement	1	0%	1	0%
	Long-term promissory note	15	1%	18	1%
	Request special treatment	3	0%	1	0%
	Change in order details	18	1%	20	1%
	Retaliatory measures	0	0%	0	0%
	Subtotal	553	32%	484	32%
Total		1739	100%	1511	100%

Table 5-8
Incidents of Violation of the Subcontracting Law, by Type

***Source**: Abridged from Fair Trade Commission, "The Subcontracting Law Conditions and Efforts for Fairness in Inter-Company Trade in Fiscal 2007," p. 3 Table 3.*