2004
Information Security Incident
Survey Report

ver.1.1

Information Disclosure: Projected Legal Reparations and Observations
(Legal Reparations and Influence on Share Price)

NPO Japan Network Security Association
January 10, 2006

JNSA Seisaku Committee　Security Incident Investigation Working Group

Working Group Leader

Eiji Yamada	dit Co., Ltd.

Members Contributing to this Report

Tomoharu Sato	IRI Communications, Inc.
Yasuhiko Sato	Software Research Associates, Inc.
Hisamichi Otani	NTT DATA Corporation
Ikuo Sugitani	GLOBAL ACE Inc.
Hideaki Kusuki	Computer Associates Japan, Ltd.
Hironori Omizo	JMC Co.,Ltd.
Tadashi Yamamoto	SOMPO JAPAN RISK MANAGEMENT,INC.
Naoyoshi Yasuda	dit Co., Ltd.
Kiyoshi Nagashima	Tokio Marine & Nichido Fire Insurance Co., Ltd.
Toshiki Sano	TOPPAN PRINTING CO.,LTD.
Kyouta Masuda	HUCOM,Incorporated
Shiro Maruyama	LAC：Little eArth Corporation Co., Ltd.
Masayuki Hiroguchi	RICOH HUMAN CREATES Co., Ltd.

Copyrights and Attributions

1 Introduction

The Security Incident Investigation Working Group ("Working Group") is organized under the NPO Japan Network Security Association (JNSA). The Working Group has conducted surveys of information security incidents (events/ accidents) in Japan since 2002, analyzing and publicly releasing the results of their surveys.

This report is a summary of the Working Group's analysis of publicly announced personal information disclosure events/ accidents (noted as "Personal Information Disclosure Incident(s)" below for convenience) occurring in Japan between January 1 and December 31, 2004. This report marks the third annual survey and analysis of Personal Information Disclosure Events in Japan since 2002.

Although more detail will be provided in later sections, of particular note among the 2004 survey results is that the number and scale of Personal Information Disclosure Incidents have increased to historic levels in Japan. One contributing factor to this growth may be a significantly increased focus of mass media reporting about Personal Information Disclosure Incidents leading up to the complete enforcement of the Personal Information beginning April 1, 2005. We shall continue our work, conducting another survey for 2005, both as a means to substantiate our findings for 2004, as well as to track trends for 2005.

Should anyone reading this report have any comments or suggestions related to our survey methodology or analysis, we kindly ask you to direct such to the Working Group at the contact provided at the end of this paper. Your input will help improve our surveys and analysis methods in the future, and will also serve as a source of encouragement for the Working Group.

2 Objectives

As mentioned earlier, this report summarizes the results of an independent evaluation of a survey and accompanying analysis related to Personal Information Disclosure Incidents publicly reported in Japan between January 1 and December 31, 2004.

Personal Information is regarded as a private asset, the protection of which is mandated by the Personal Information Protection Act. Accordingly, the disclosure of personal information is a risk of which corporate managers should be well aware.

The Working Group has produced this report for the purpose of raising topics for debate both now and in the future, for helping corporate management assess the proper scope of the risks associated with information security, and for assisting management in reaching appropriate investment decisions, as such relate to the "likelihood of legal reparations" and the "influence on share price" in their respective organizations.

3 Structure of this Report

This report consists of the following three types of analyses:

a. Analyses and evaluations of publicly reported information during 2004

b. Calculation of the "Projected Legal Reparations" with respect to the results of a. above, based on a formula independently developed by the Working Group

c. Calculation of the "Influence on Share Price" with respect to the results of a. above, applied to an analytical method developed independently by the Working Group

Here, a. represents analyses of information released to the public via mass media or other independent institutions. The results described by b. and c. are derived from evaluation methods and procedures developed independently by the Working Group. These methods and procedures are in no way meant to be definitive.

4 Analysis of Personal Information Disclosure Incidents occurring during 2004

4.1 Subject of Survey

Personal Information Disclosure Incidents publicly reported via news periodicals and Internet news services occurring between January 1 and December 31, 2004.

4.2 Survey Methodology

Working Group members collected public reports from the Internet and other news sources, compiling data related to Personal Information Disclosure Incident data, type of business of the organization involved, number of individuals affected, cause of the incident, route of the information disclosure, after-incident response, and type of information disclosed.

4.3 Compilation and Analysis of Survey Results

See “Appendix 1 Table A” for a compilation of survey results.

Note here that the following survey results analysis references the details of several individual examples not included in “Appendix 1 Table A.”

4.3.1 Ratio of Incidents by Industry Type

We compiled a list of 366 incidents during 2004. Fig. 1 illustrates a comparison of incidents by industry type.

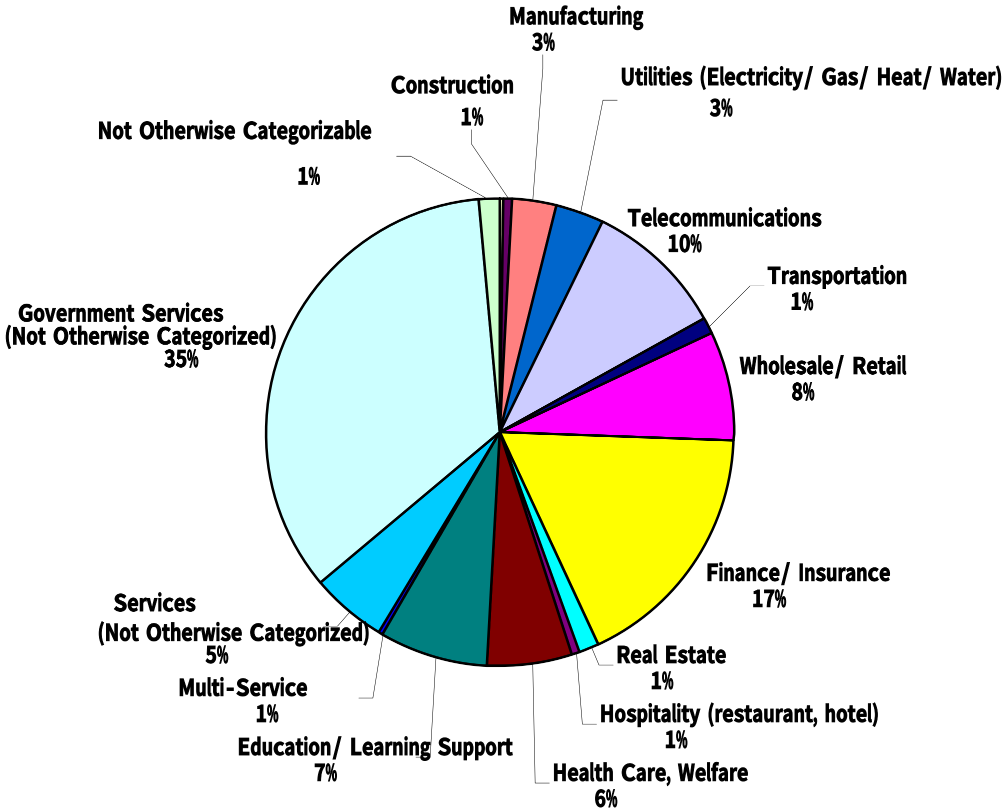


Fig. 1 Ratio of Incidents by Industry

The top three industries for Personal Information Disclosure Incidents during 2004 were, in order, “Government Services (Not Otherwise Categorized) (35%)”, “Finance/ Insurance (17%)” and “Telecommunications (10%).” Central Government and Local Public agencies have been included in the Government Services category. Major carriers and Internet Service Providers have been included in the Telecommunications category.

One reason that the Government Services, Finance/ Insurance and Telecommunications categories are at the top of this ranking could be that these types of businesses deal with large amounts of personal data and related transactions, leading to more opportunities for Disclosure. Another contributing factor may be that the organizations in these industries are bound by law to report all Personal Information Disclosure Incidents, or such disclosure is common practice in the industry.

4.3.2 Cause of Disclosure

We have categorized the causes of disclosure in the table below:

Table 1 Considerations behind Disclosure Categorization

Category	Specific Event(s)	Determination Standards
Configuration Error	Configuration error in Internet or other settings allows sensitive information to be viewed by unauthorized / outside individuals over the Internet.	Difference between Unauthorized Access: Unauthorized Access is the act of overcoming access controls. Difference between Bug/ Security Hole: When the root error is due to inappropriate or mistaken settings levels for general user settings, it is a Configuration Error. Difference between Administration Error: An error in system configuration is a Configuration Error. An Administration Error is an error related to management.
Operational Error	Sending E-mail, FAX, letters, etc. to the wrong recipient/ address.	Difference between Configuration Error: An Operational Error is an error at the final stage of operation. A Configuration Error would be the error occurring if the root settings/ configuration of a mail delivery system were incorrect.
Bug/ Security Hole	Operating system or application Bugs/ Security Holes allow sensitive information to be viewed by, or disclosed to, unauthorized/ outside individuals over the Internet.	Difference between Administration Error/ Configuration Error: A Bug/ Security Hole is when information is disclosed due to errors on the part of the vendor or system integrator. Also considered a Bug/ Security Hole if the User does neglects known Bugs/ Security Holes.
Unauthorized Information Removal	External contractors, vendors with access to physical facilities, former employees and/ or others who are not employees/ workers removing or stealing information or media containing information from a location.	Difference between Theft: Strictly speaking, removing information-containing media is theft; however, we have chosen to categorize such events as noted to the left as Information Removal.

Category	Specific Event(s)	Determination Standards
Internal Crime/ Internal Fraud	Acts of personal fraudulent Information Disclosure perpetrated by employees/ workers or others belonging to an organization. Fraudulent usage of personal information by persons belonging to an organization.	Difference between Information Removal/ Theft/ Unauthorized Access: For the purposes of this report, fraudulent acts perpetrated by persons belonging to an organization (employees, other workers, etc. subject to company management/ control) are categorized as Internal Crime (including Internal Fraud). Cases including collusion with outside individuals and/ or Unauthorized Access are still considered Internal Crime/ Fraud as long as there was intentional fraud on the part of the person(s) belonging to the organization.
Administration Error	Personal Information disappears/ is lost during a physical move. Personal Information lost in the course of circulation/ distribution due to lax management. Loss of Personal Information is the fault of the organization. Information release/ management was not properly clarified.	Difference between Loss/ Misplacement: Loss or disappearance internally or through a major distribution channel is considered Administration Error. Difference between Theft: Theft occurring through Administration Error is considered to be Theft.
Unauthorized Access	Information disclosed to others outside the organization when access controls are overcome, and the network is penetrated.	Difference between Internal Crime/ Fraud: In principle, any non-permitted access by someone outside the organization is considered Unauthorized Access.
Theft	Theft of a PC or other information-containing media (stolen from car, out of office, etc.).	Different between Information Removal: Items taken out of cars, offices, etc. is generally categorized as Theft.
Loss/ Misplacement	Loss or misplacement of a PC or other information-containing media on a train, at a restaurant or other external location. Responsibility for loss rests with the individual.	Difference between Administration Error: Loss/ Misplacement due to Administration Error at the personal level is generally categorized as Loss/ Misplacement.
Worm/ Virus	A worm infection causes an E-Mail to be broadcast without the knowledge or intent of the user, revealing personal E-Mail addresses, etc.	Difference between Unauthorized Access/ Bug/ Security Hole: Worms/ viruses that exploit existing security holes are still categorized as Worm/ Virus as long as the Worm/ Virus was the root cause of the Information Disclosure.
Non-Intended Use	Personal Information used for other than its original intended use either systematically, or with respect to organization work tasks.	Difference between Internal Crime/ Internal Fraud: Internal Crime/ Fraud is a fraudulent act of information disclosure by an individual internal employee/ worker.
Other	Any incident not falling within any of the other categories listed above.	
Unknown	Cause is not determinable.	

Fig. 2 illustrates the number of Personal Information Disclosure Incidents by cause.

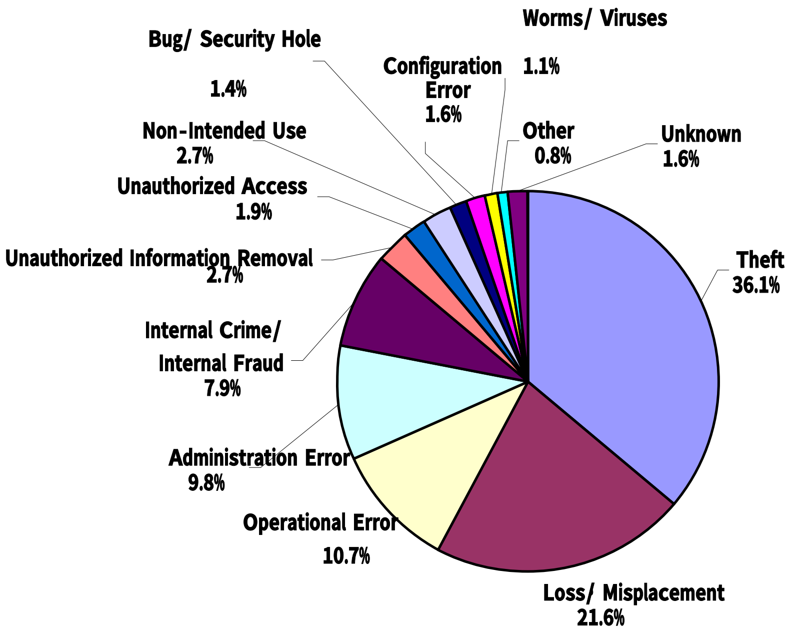


Fig. 2 Number of Personal Information Disclosure Incidents by Cause

Table 2 shows the cause of information disclosure by category.

Table 2 Personal Information Disclosure Incident Categorization

No.	Factor	Cause	%	Corresponding Cause
1	Technological	Human Error	22.1	Configuration Error, Operational Error, Administration Error
2	Technological	Insufficient Measures	4.4	Bug/ Security Hole, Virus, Unauthorized Access
3	Non-Technological	Human Error	24.3	Misplacement, Non-Intended Use
4	Non-Technological	Crime	46.7	Internal Crime, Information Removal, Theft
5	Other	Other, Unknown	2.4	Other, Unknown

The reason for the high ratio of Theft and Loss/ Misplacement could be due to the fact that thefts or loss of PCs and briefcases/ bags in the past were not reported in the news, but greater attention in 2004 has increased the number of such incidents reported as a “Personal Information Disclosure Incident” when personal information is contained in the lost or stolen PC or briefcase. This is likely due to the general awareness early in the year of the Personal Information Protection Act becoming fully enforced beginning April 1, 2005.

Unexpectedly, the ratio of incidents attributed to employees or other “insiders” categorized as Internal Crime/ Internal Fraud and Unauthorized Information Removal was low, at 10.6% combined. The generally accepted wisdom is that 70% to 80% of information disclosures are caused by person(s) within an organization; however, we note here a major discrepancy between this type of common belief and our survey results. The causes for this difference could be due to the difficulty in detecting internal criminal acts, or that an organization is hesitant to make such acts public (organization covers up the incident). However, when combined with Theft, causes categorized as personal intent (crime) increase to 46.7% of all incidents, as shown in Table 2.

Fig. 3 indicates the results of compiling the causes of Personal Information Disclosure according to industry.

Please note that the values on this graph represent ratios, and not the number of incidents, for each industry. For example, the "Fishing" industry had one incident, categorized as "Operational Error." Since the industry only experienced one incident, the ratio of "Operational Error" incidents is 100%, as shown on the bar graph. (The numbers noted inside the bar graph bars represent number of incidents)

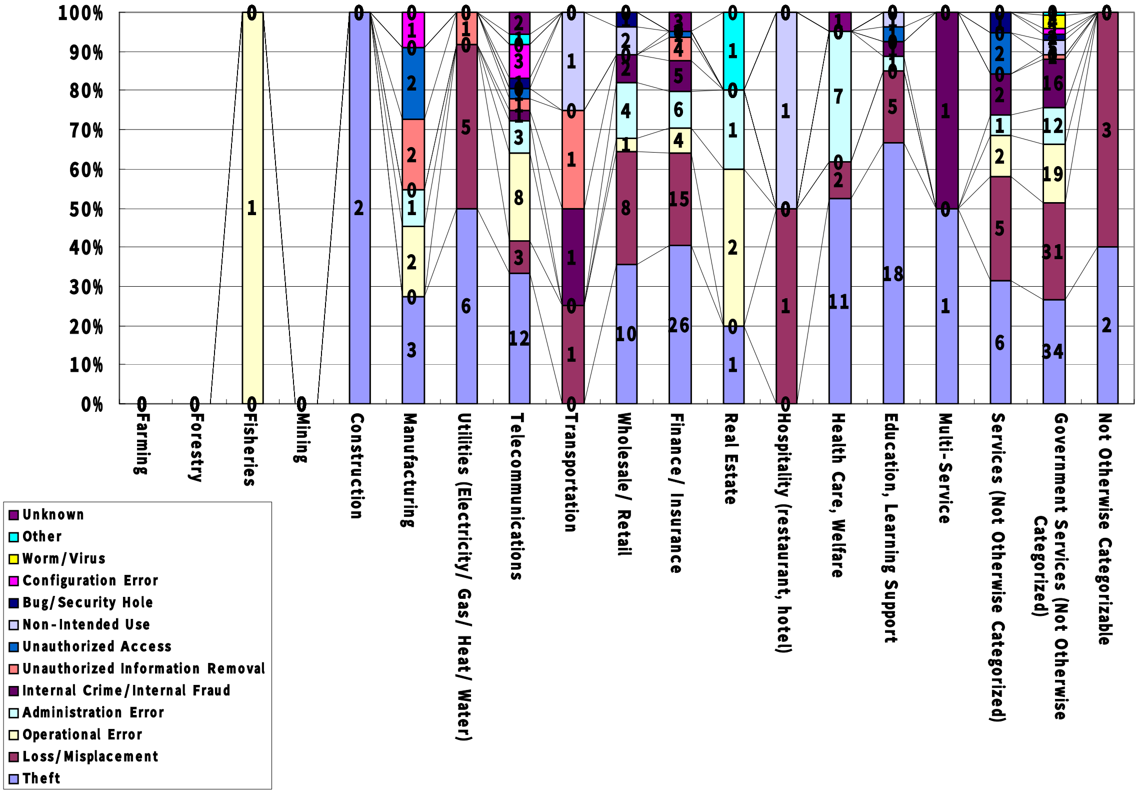


Fig. 3 Causes of Information Disclosure Compiled by Industry Type

We see here that the ratio of Theft and Loss/ Misplacement is high among all industries. Most cases of Theft involved car or office break-ins. Particularly common were cases in which persons affiliated with educational institutions or government agencies encountered trouble when carrying documents or computers back to their personal residences. In several instances, the person (s) involved were bringing materials to their private residences despite the fact that do so was against workplace rules, and during the course of their actions, the information was stolen, lost or misplaced. Perhaps this trend indicates that rather than simply prohibiting employees from taking sensitive materials home, organization management should consider a set of policies that assume workers will be tempted to take sensitive data home to continue working when the need arises.

While we noted many cases of lost/ misplaced data in which workers were taking documents or computers to their personal residences, we also noted cases where sensitive data was lost/ misplaced by a delivery service to whom it was entrusted. While this may not have occurred frequently, organization management should recognize loss on the part of a delivery service as a potential risk, having appropriate measures in place. In particular, when protecting information not under one's direct control, organization management should focus on measures assuming an accident or Disclosure Incident will occur, rather than focusing solely on attempting to prevent an incident. Such measures could include packing the information to prevent exposure during transit, or encrypting the information. Other measures could include requiring a contract with the delivery service clarifying the roles and responsibilities of each party as a means to deter an incident, or to enhance/ enforce indemnities after an incident occurs.

4.3.3 Information Disclosure Route

Fig. 4 illustrates the results of compiling Personal Information Disclosure Incidents according to the route of the disclosure.

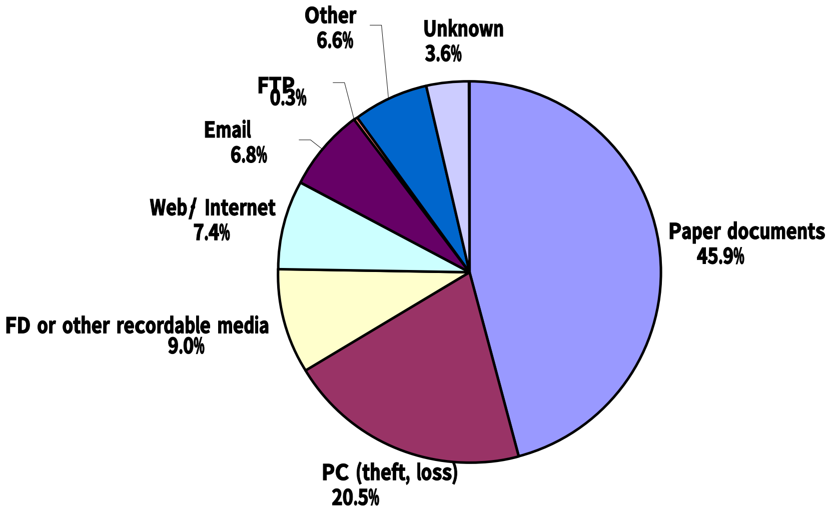


Fig. 4 Personal Information Disclosure Incidents by Route of Disclosure

Table 3 summarizes the Information Disclosure Routes by category.

Table 3 Categorization of Personal Information Disclosure Routes

No.	Factor	%	Route
1	Internet	14.5	Internet/ Web, E-Mail, FTP
2	Media	75.4	Paper documents, FD or other recordable media, PC (machine itself)
3	Other, Unknown	10.2	Other, Unknown

As noted in the table, the overall ratio of “Paper documents, FD or other recordable media, PC” is extremely high. We believe this is a reflection of the high rates of theft or loss of data kept in a briefcase/ bag during transportation, as shown in “4.3.2 Cause of Disclosure.”

Considering the ratios, the great number of disclosure incidents occurring via lost/ stolen paper documents cannot be ignored. As opposed to electronic information, information printed on paper is not easily subject to systematic measures such as encryption, etc. Protecting documents calls for an emphasis on physical/ human policies. Considering the relationship between route and cause of disclosure, we can predict a high probability that information may be stolen or lost while an individual is carrying it. In our opinion, management should first stress that if any information be taken outside the office at all, then it should be such that is only absolutely necessary. If management does not have a clear understanding of what information was being transported, then there is a strong chance that response to theft or loss will be slower than required, as management is unable to accurately predict the entire scope of the problem.

Fig. 5 shows the results of compiling the routes of Personal Information Disclosure Incidents according to industry.

Please note that the values on this graph represent ratios, and not the number of incidents, for each industry. For example, the “Fishing” industry had one incident, categorized as “E-Mail.” Since the industry only experienced one incident, the ratio of “E-Mail” incidents is 100%, as shown on the bar graph. (The numbers noted inside the bar graph bars represent number of times an incident occurred for each route indicated)

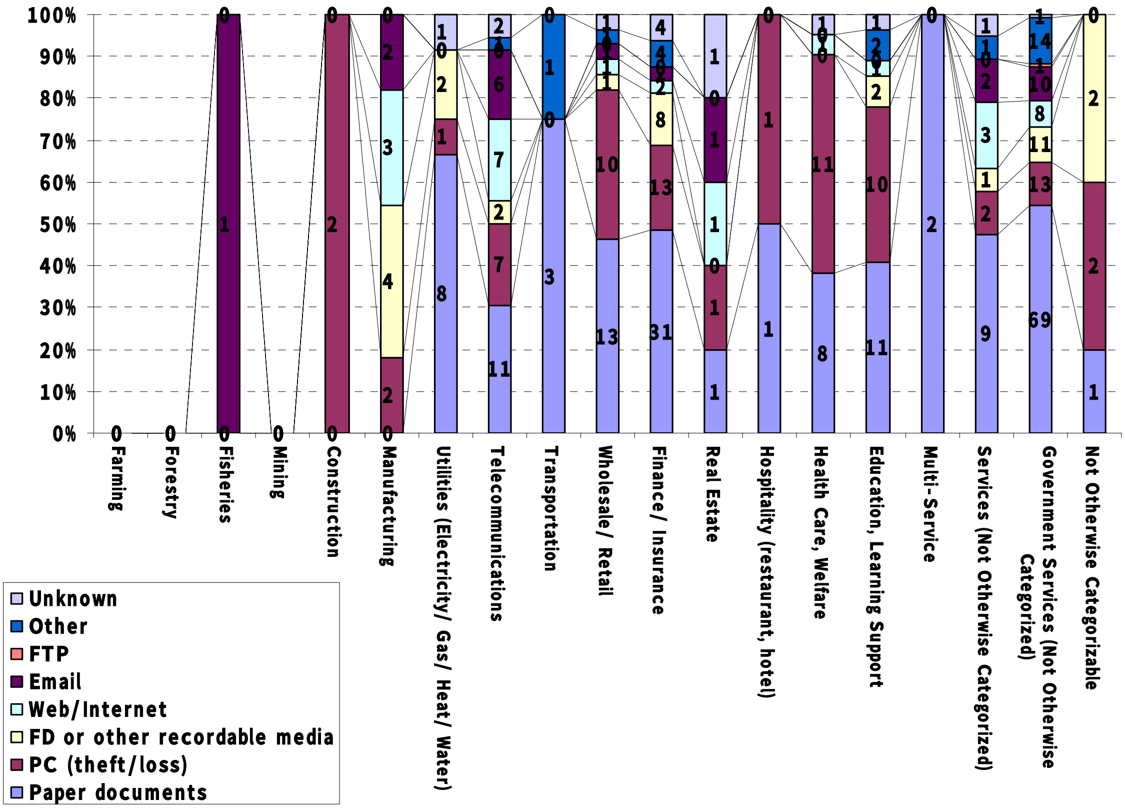


Fig. 5 Route of Information Disclosure Compiled by Industry Type

Here, we see a generally high ratio of Information Disclosure involving the theft/ loss of paper documents and PCs. We also note that the number of disclosure incidents is highest among Government Services (59 incidents) and Finance/ Insurance (31 incidents) categories. Looking more closely at the details of the incidents, we discover that in the case of Government Services, theft or loss of sensitive data occurred while workers carried the data as part of their regular work duties. Such examples include the theft of a bag containing vouchers during bill collection and the theft of a bag containing customer files during water meter reading. On the other hand, for the Finance/ Insurance category, we noted several cases in which sensitive data was removed from an office in direct violation of company rules, with the information subsequently stolen or lost. In either case, as we have mentioned earlier, at a minimum policies should include not carrying any more information than absolutely necessary. Individuals must also have a clear understanding that they are carrying sensitive information. As we have briefly alluded in “4.3.2 Cause of Disclosure,” we recognize many instances where organizations must to revisit their rules regarding removing information from the office.

4.3.4 Number of Victims

The total number of Victims by Personal Information Disclosure Incidents during 2004 was 10,435,061.

The average number of Victims per incident was 31,056.7. (removing 30 incidents in which the number of Victims was unclear, the population parameter for our calculation was 336 incidents)

Fig. 6 shows the distribution of the number of Victims per Personal Information Disclosure Incident.

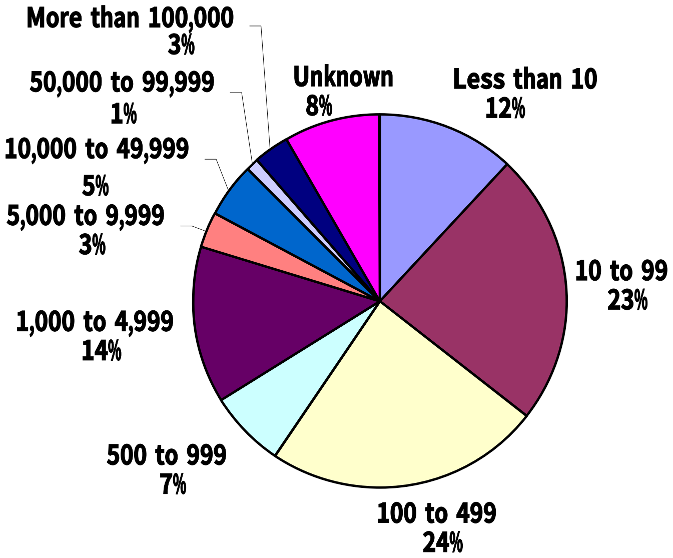


Fig. 6 Distribution of the Number of Victims per Disclosure Incident

Fig. 7 illustrates the ratio of victims according to the cause of the disclosure.

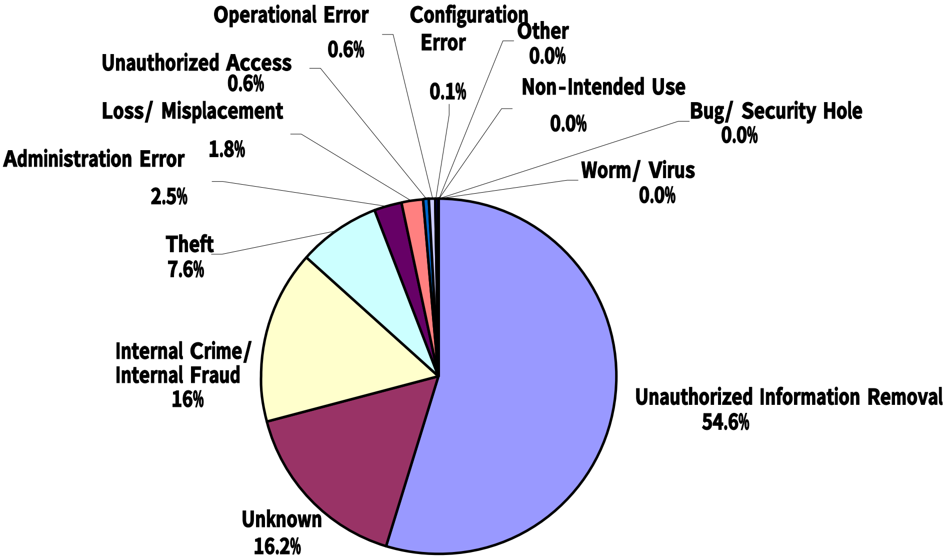


Fig. 7 Ratio of Victims by Disclosure Cause

Of particular interest here is that while the combination of Internal Crime/ Internal Fraud and Unauthorized Information Removal—disclosure of the type caused by persons within the organization—accounts for only 10.6% of all incidents (as shown in “4.3.2 Cause of Disclosure” Fig. 2), Fig. 7 indicates that the combination of Internal Fraud and Unauthorized Information Removal account for fully 70.6% of victims affected by Personal Information Disclosure.

What we can infer from this is that while Disclosure Incidents caused by an organizational insider may be infrequent, the scope of damages caused by such an occurrence can be very large. It appears that fraud by organizational insiders is a serious issue that requires greater attention from management.

Fig. 8 shows the relationship between the number of victims and number of incidents by industry type.

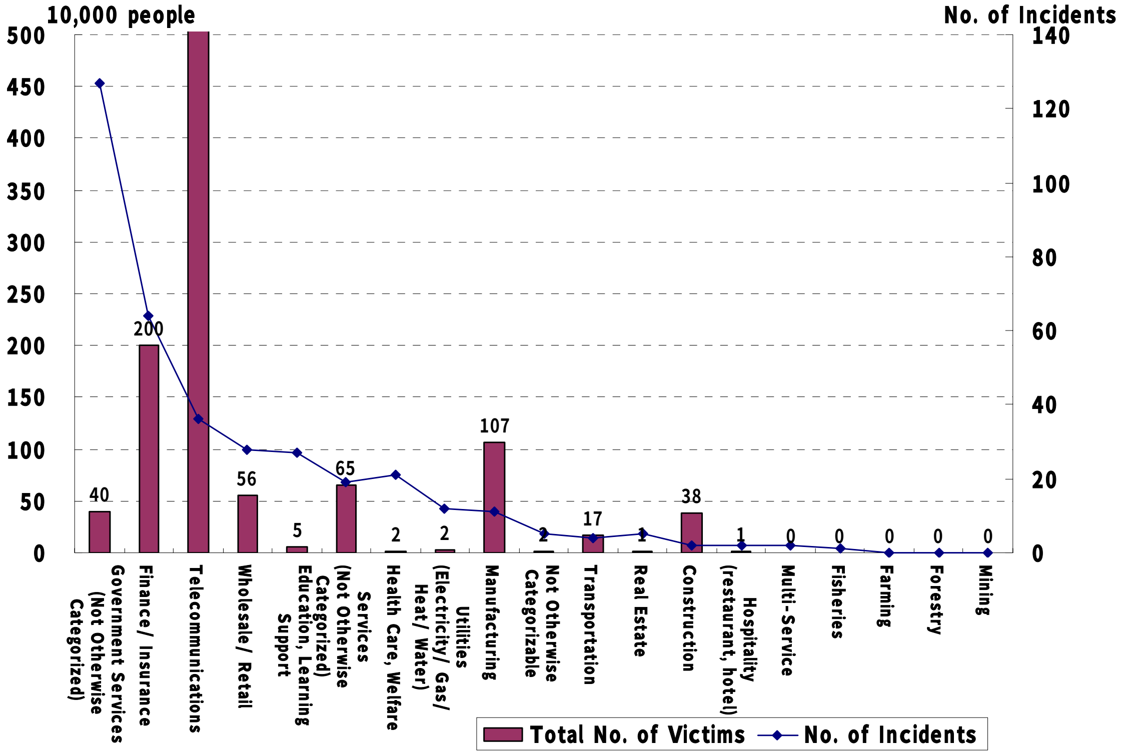
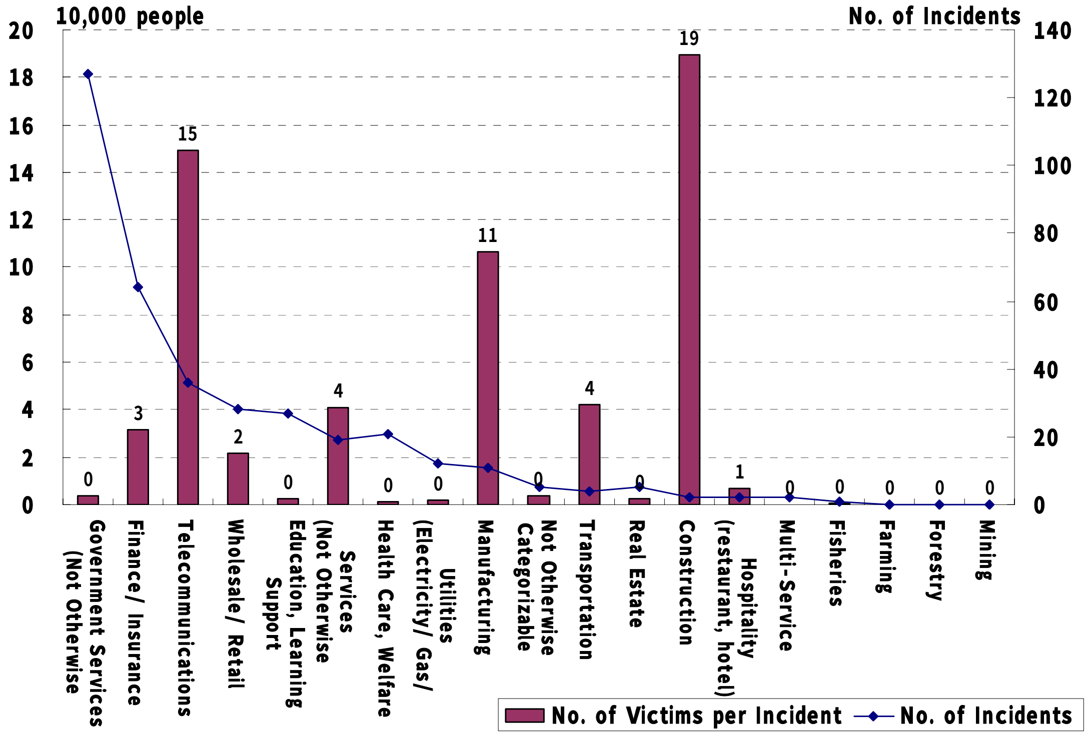


Fig. 8 Victims and Incidents by Industry

The Government Services, Finance/ Insurance, and Telecommunications categories show sharply contrasting trends. The Telecommunications category has the overwhelming share of the total number of victims of Information Disclosure. A single Personal Information Disclosure Incident in which several million individuals had their information disclosed significantly influenced this number. In contrast, Government Services shows a low total number of victims in comparison to the number of incidents. From this we can conclude that the number of victims per Information Disclosure Incident in this category is relatively low. And while the Finance/ Insurance category may seem to have fewer victims per incident than the Telecommunications category, this category is second overall in terms of victims, and almost twice the number of the next closest category.

Fig. 9 shows the relationship between the number of victims per incident and the number of incidents according to industry type.

Fig. 9 Number of Victims per Incident and Number of Incidents by Industry



While the “Construction” category shows the greatest number of victims per incident, the category only experienced two incidents for the year, one of which involved a significant number of victims, resulting in the 190,000 victims/ incident number seen in the figure above. As the second-highest category in the figure, Telecommunications also experienced an incident that had a particularly large number of Information Disclosure victims, influencing the per-incident numbers shown here.

Due to the fact that organizations in the Government Services and Finance/ Insurance categories are required to report all incidents—even those with a small number of victims—the per-incident number of victims in these categories is understandably small. From the figure above, it appears that industry types with fewer incidents of Information Disclosure tend to have somewhat higher per-incident victim numbers. We believe there is a possibility that these industries do not publicly report incidents in which only a relative few number of victims are affected.

4.3.5 Details of Information Disclosed

Fig. 10 shows the probability of disclosure for the types of information noted.

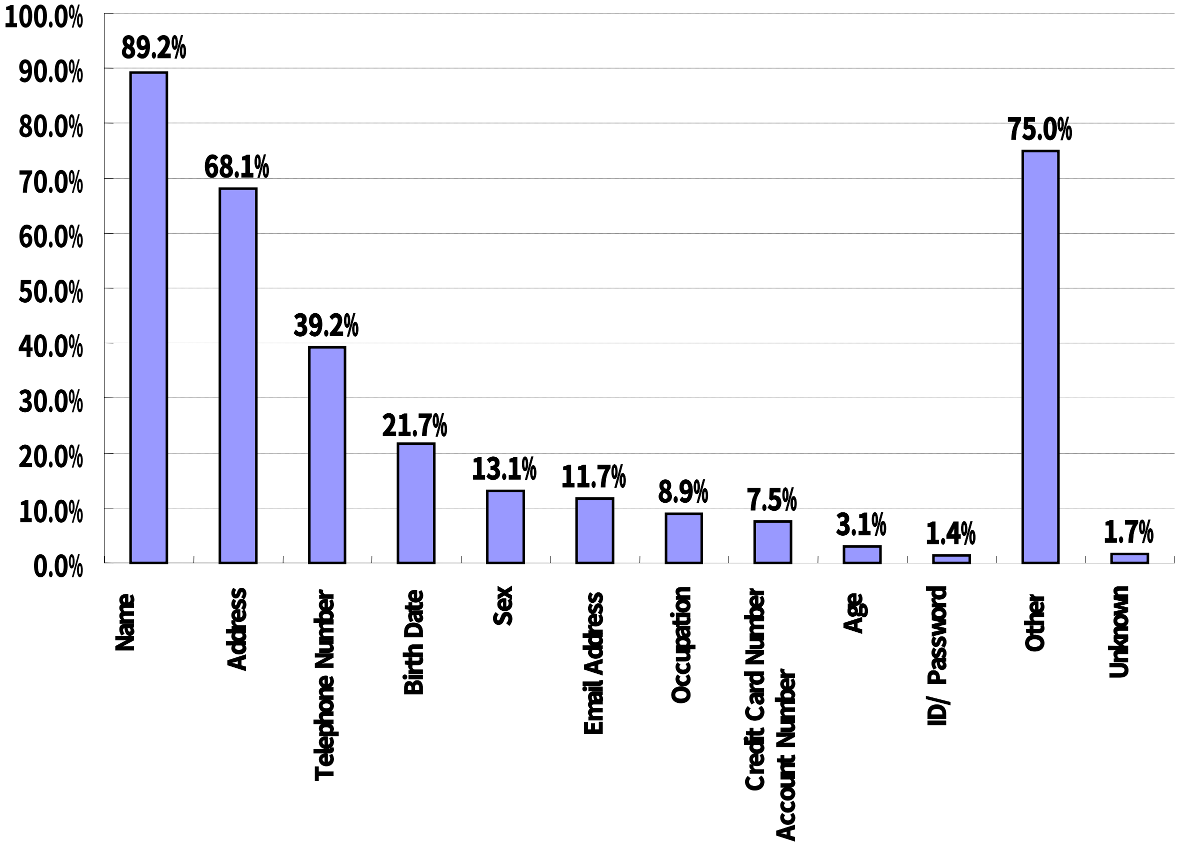


Fig. 10 Disclosure Probability by Information Type

A person's "Name" was disclosed in 89.2% of the Personal Information Disclosure Incidents that occurred during 2004. Similarly, "Address" was disclosed in 68.1% of all incidents, allowing for a higher danger of specific identification of an individual in cases where "Name" and "Address" were both disclosed.

See "Appendix 1 Table A" for details about information categorized as "Other."

Table 4 shows the results of compiling the frequency of disclosure for combinations of information that are highly likely to be disclosed.

Table 4 Probability of Information to be Disclosed in Combination

	Name	Address	Tel. No.	Birth Date	Sex	E-Mail Address	Incidents	Probability
Combination 1	X	X					242	67.2%
Combination 2	X		X				137	38.1%
Combination 3	X			X			77	21.4%
Combination 4	X	X	X				131	36.4%
Combination 5	X	X	X	X			44	12.2%
Combination 6	X	X	X	X	X		26	7.2%
Combination 7	X	X	X	X		X	7	1.9%

From Fig. 12, we see that combinations of “Name,” “Address,” and “Telephone Number” are most frequently disclosed.

4.3.6 Interannual Fluctuations of Survey Results

The following is a comparative analysis of survey results for the three years between 2002 and 2004.

4.3.6.1 Interannual Fluctuations in Organizations Reporting Information Disclosure Incidents

Table 5 shows the change in the total number of organizations reporting Information Disclosure Incidents over the past three years.

Table 5 Total Number of Organizations Reporting Information Disclosure Incidents

2002	2003	2004
63	57	366

Compared with 2003, 2004 showed an increase of 6.4 times in the number of reporting organizations. As we mentioned in “4.3.1 Ratio of Incidents by Industry Type,” we believe this growth is due to the influence of the anticipated full and complete enforcement of the Personal Information Protection Act, which has led to an increased number of related news reports, and to a greater tendency for organizations to come forward and publicly announce Personal Information Disclosure Incidents on their own.

Fig. 11 shows the ratio of organizations experiencing Personal Information Disclosure incidents by industry type over the past three years. (The numbers noted inside the bars on the graph indicate the number of organizations)

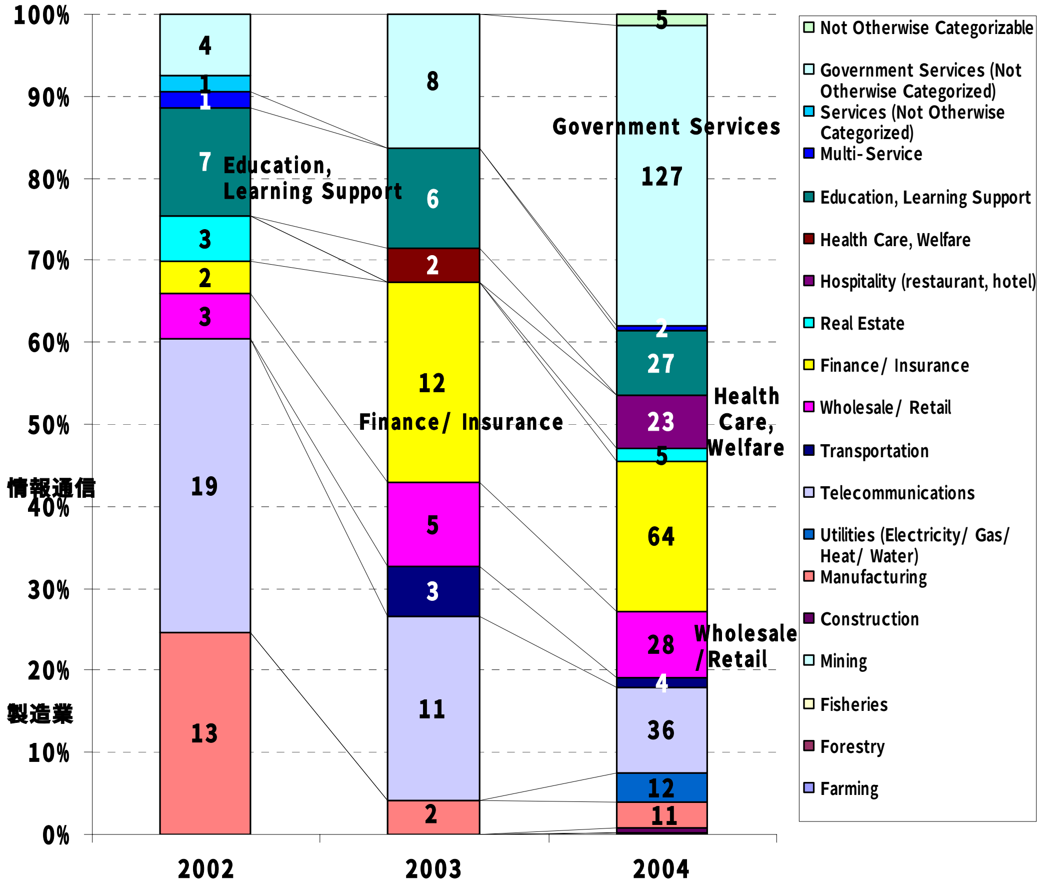


Fig. 11 Changes in Organization Ratio between 2002 and 2004

Here, we see a notable increase in the ratio of “Government Services (Not Otherwise Categorized)” for 2004. Although the reason for the increase is not clear, looking at the types of organizations involved shows us several instances of a single organization reported multiple Personal Information Disclosure Incidents. These appear to be cases where once an Information Disclosure Incident has occurred, a second internal investigation uncovers other incidents in the past, which are also then reported. The ratio of “Telecommunications” category organizations appears to be declining over this three-year period; however, one should note that the number of incidents has been increasing.

4.3.6.2 Interannual Fluctuations in Causes of Disclosure

Fig. 12 shows the changes in the causes of disclosure over the past three years.

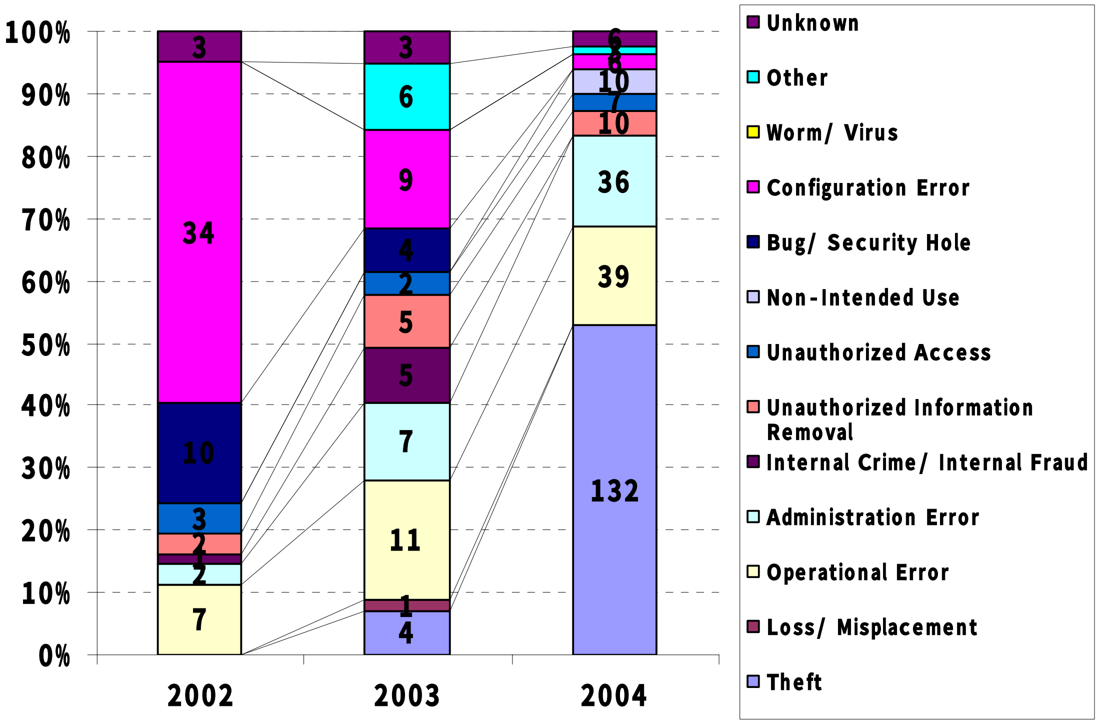


Fig. 12 Changes in Cause of Disclosure Ratios between 2002 and 2004

Here we see an increasing trend in “Theft” and “Loss/ Misplacement.” As discussed in “4.3.2 Cause of Disclosure,” this appears to be the influence of such incidents coming to be reported as “Personal Information Disclosure Incidents.”

In contrast, the ratio of incidents due to “Configuration Errors” and “Bug/ Security Holes” is decreasing. We believe we can interpret the greater permeation of system-related policies among organizations as the reason for this trend.

4.3.6.3 Interannual Fluctuations in Information Disclosure Routes

Fig. 13 shows the changes in information disclosure routes over the past three years.

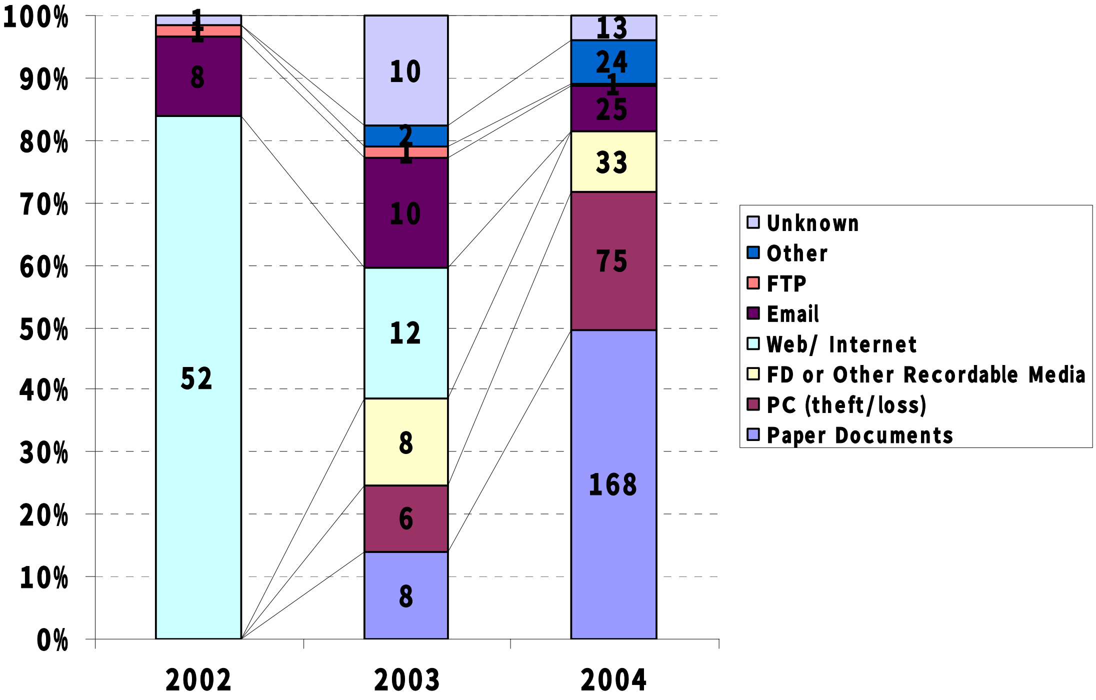


Fig. 13 Changes in Routes of Disclosure between 2002 and 2004

Here, we see an increase in the ratio of incidents of Information Disclosure related to “Paper Documents” and “PC” categories. As we mentioned in “4.3.3 Information Disclosure Route,” we believe this trend is linked to the increased ratio of theft and loss as causes of Personal Information Disclosure Incidents.

Conversely, we believe the decrease in Disclosure Incidents via the “Internet/ Web” route is due to the greater permeation of system-related policies among organizations, as we noted in “4.3.6.2 Interannual Fluctuations in Causes of Disclosure.”

4.3.6.4 Interannual Fluctuations in Number of Victims

Table 6 shows the changes in the number of Personal Information Disclosure Incident victims over the past three years.

Table 3 Number of Victims

2002	2003	2004
418,716	1,554,592	10,435,061

Compared to 2003, we see a 6.7 times increase in the number of victims reported during 2004. As we noted in “4.3.6.1 Interannual Fluctuations in Organizations Reporting

Information Disclosure Incidents," this is directly related to the 6.4 times increase in the number of reported Personal Information Disclosure Incidents.

Table 7 shows the change in number of Personal Information Disclosure victims.

Table 7 Average Number of Victims per Incident

2002	2003	2004
7,613	30,482	31,057

Here, we do not see a significant difference in the average number of victims per Information Disclosure incident between 2003 and 2004.

5 Overseas Information Disclosure Incidents

We conducted a survey of Personal Information Disclosure Incidents reported overseas, mainly focusing on the time period between January 1 and December 31, 2004. Similar to incidents in Japan, we note among the causes of Information Disclosure Incidents overseas computer theft, the revealing of personal information due to unauthorized access, information theft for the purpose of selling the personal information/ email addresses to SPAM email broadcasters or direct mail marketing companies, etc.

5.1 Overseas Information Disclosure Incidents

5.1.1 AOL [America Online] (United States)

An AOL employee sold the IDs (screen names) and email addresses of 93 million AOL customers to spammers. Although AOL did not announce the exact number of individuals affected, this incident is considered the largest case of customer information disclosure ever in the United States. Among the items of personal information disclosed were telephone numbers, ZIP codes, and credit card names. AOL keeps credit information on a separate database, so disclosed information did not include credit card numbers or passwords. AOL Japan could not deny that user information for Japanese customers may have also been disclosed, since Japanese user information was also managed within the United States.

The United States Federal Bureau of Investigation arrested an AOL software engineer on suspicion of having stolen the personal information. The engineer has been fired from his job. This individual accessed customer information using another employee's password to break into the database. The individual then proceeded to sell the personal information in two separate installments spammers for a total of $84,000.

5.1.2 ChoicePoint (United States)

ChoicePoint is the largest credit research/ data broker in the United States. The company collects all manner of information from generally available official documents, including personal information/ personally identifying information, business license registrations, and other legal documents, selling this information to corporations, government institutions and law enforcement agencies.

The company announced their suspicion that up to 145,000 personal information records stored on their computers may have been stolen. Several hackers used stolen Ids to create fake companies, setting up about 50 fraudulent customer accounts at ChoicePoint. Using these accounts, the hackers gained access and searched through personal information records stored at the company. The hackers stole personal information that included names, addresses, social security numbers, credit card numbers and personal credit information. As a result, at least 750 individuals were victimized by identity theft, including six in Los Angeles County.

Based on California's Security Breach Information Act, ChoicePoint was compelled to notify 35,000 California citizens of the potential personal information disclosure. With mounting pressure, the company was forced to ultimately notify 145,000 individuals across the United States that their personal information may have been disclosed to the hackers.

Subsequent to this incident, ChoicePoint changed their business operations, dropping some of their personal information business lines, limiting the sale of personal information to only entities that meet certain requirements, and enhancing customer confirmation procedures.

5.1.3 LexisNexis (United States)

LexisNexis is a U.S. subsidiary of the giant European publisher Reed Elsevier. LexisNexis announced that over the preceding two years, the database managed by Seisint, a data collection and sales company owned by LexisNexis, and other departments within the LexisNexis group were subject to 59 separate incidents of unauthorized access.

Only five weeks previous, the company announced the leak of 32,000 personal information records. The more recent incidents involved unauthorized access on a scale almost ten times greater, with the personal information of 310,000 compromised.

LexisNexis believes that the hacker obtained and used the ID and password of a legal LexisNexis customer. The personal information stolen from the company includes customer addresses, names, social security numbers and driver's license numbers; however, the company claims that no credit history, medical records or asset information was revealed. LexisNexis and its subsidiaries store several million personal information records, including address and social security numbers. The company's clients include police officers, legal professionals, public agencies, private organizations and others. Further, the company provides data to "MATRIX," an anti-crime, anti-terrorist database project for the United States government.

LexisNexis notified 32,000 individuals about the personal information disclosure, offering credit monitoring and other theft detection support, as well as free credit reports, fraud insurance and other measures.

5.1.4 Bank of America (United States)

The Bank of America, one of the largest in the United States, reported the loss of backup tapes containing the financial information of federal government employees. Several of the lost backup tapes were on the way to the bank's backup center. These tapes contained credit card information for cards issued to approximately 1.2 million federal employees. The lost information included account information for VISA SmartPay cards issued by the bank, including credit card numbers and account data, names, addresses, social security numbers and more. Of the 1.2 million victims, 900,000 were employees of the U.S. Defense Department. More than half of the 100 United States senators also had their information compromised in the incident.

The Bank of America has stated that they will monitor all of the accounts included in the lost tapes, contacting the card holders if any suspicious activity is detected.

5.1.5 Boston College (United States)

Boston College announced that hackers broke into their network, and may have stolen the personal information for 12,000 alumni. The suspected theft includes personal information such as names, telephone numbers, addresses and social security numbers.

Boston College believes that this unauthorized access was not intended to steal personal information, but rather that the intent was to use the school's computer to attack other computers. The computer in question was used by students to look up alumni names and telephone numbers to ask for donations, but the college believes that it was outside hackers that perpetrated the unauthorized access, rather than anyone affiliated with the school. The school contracts out the management of their computers, but the latest security patches had not yet been applied.

Many American colleges and universities use social security numbers as a means to identify alumni. Boston College immediately took the machine in question offline, and deleted the social security numbers that were stored on the computer. The school announced the incident on their Web site, and set up a special Web site and telephone number for individuals concerned about their privacy.

5.1.6 Ameritrade (United States)

Ameritrade Holdings operates one of the largest deep-discount online brokerages. The company reported the loss of backup tapes holding the personal information of 200,000 of its clients. According to Ameritrade, their shipping company lost a total of four such backup tapes containing customer personal information between 2002 and 2003. Three of the tapes were later discovered within the shipping company’s facilities; however, one of the tapes has yet to be located. Personal information contained on the lost tape includes social security numbers and credit card numbers. Ameritrade also reported that special equipment is required to read the information on the tape, and that there have been no reports of fraudulent usage of the missing information.

5.1.7 San Jose Medical Group (United States)

The San Jose Medical Group, located in California, reported the theft of computers containing personal information. The two new computers were stolen from a locked office. These computers contained financial and medical information for 185,000 patients, including medical billing codes, social security numbers, and other information. However, the stolen information did not include complete medical records for the individuals.

Besides medical billing information, the computers also contained some information related to the Group’s 2004 financial statement audit. The Group had decided to encrypt medical and financial information during 2004; however, the stolen notebook computers in question had just received copies of financial and medical information from securely managed servers, and the encryption process had not yet been completed. In addition, the servers were considered protected by policies limiting physical access by employees; however, information was accessible through the Group’s network.

Nine days after the occurrence, the incident was reported publicly and to the authorities, as required by California State Law SB 1386.

5.1.8 University of California, Berkeley (United States)

The University of California reported that the personal information of more than 1.4 million California residents may have been disclosed.

The school discovered that hackers exploited a security hole in one of the PCs owned by a social researcher at the Berkeley campus. The PC in question contained a database storing the personal information of participants in a state home care program. The school has no proof, however, that the database was accessed, and no reports of ID theft or data abuse have been made.

The database on the compromised computer contained all of the names, addresses, telephone numbers, social security numbers, birth dates, provider names and other information for all individuals that have participated in the home care program (IHSS: In Home Support Services) since 2001. The program's policies stipulate that all social security numbers and other private information be been deleted from the database, but the researcher in question ignored the policy.

5.1.9 University of California, Berkeley (United States)

The University of California Berkeley campus announced the theft of a single notebook PC from an office. The PC carried personal information about 98,369 individuals.

According to school sources, the theft occurred when a graduate school office off-limits to unauthorized persons was temporarily left unoccupied. A school employee witnessed an unidentified person walking off with a notebook PC similar to the type that was stolen.

The stolen personal information consisted mainly of information related to graduate students and graduate school program examination candidates. Most of the data stolen includes information about graduate school examination candidates from fall 2001 to spring 2004 (except for the law school), graduate school students enrolled between fall 1989 and spring 2003, PhD. Recipients from 1976 to 1999, and several other related persons. Approximately one-third of the files on the stolen PC included personal information such as names, addresses, social security numbers, birth dates, etc.

The school claims that there is no evidence that the personal information has been used for fraudulent purposes, but notified all 98,369 individuals in accordance with state law. The school set up a Web site allowing individuals to confirm whether their information was included on the stolen notebook PC.

5.1.10 California State University, Chico (United States)

The California State University Chico campus announced the disclosure of the personal information of 59,000 individuals related to the school.

Hackers succeeded in breaking in to the school's housing/ food service system servers, potentially accessing the personal information of 59,000 individuals related to the school. Evidence of the break-in was discovered during network monitoring performed as part of the daily work routine at the Chico campus. An investigation revealed that the hackers installed root kit software to store music, movie, game and other files on the server. The school also discovered that the hackers had attempted to penetrate several other computers as well. There was no evidence that the hackers were specifically targeting sensitive information.

The information potentially revealed to hackers included the names, addresses, and social security numbers of students, former students, applicants and faculty. Most of the information in question related to students taking courses at the school within the past five years.

5.1.11 DSW Shoe Warehouse (United States)

DSW, a shoe retailer, announced the theft of credit card and other credit information.

Between November 2004 and February 2005, 108 of the 175 stores in the nationwide chain experienced theft of payment information, including 1.4 million cases of credit card/ debit card theft, and 96,000 cased of check theft.

The stolen information consisted of credit/ debit card numbers, names, and vendor information; however, the company reported that no addresses, PIN numbers or other personal information was stolen. Information stolen from checks included account numbers and driver's license numbers, but no names, addresses or social security numbers were compromised.

The company believes that the credit card information was stolen by a person or persons accessing the company servers from an external location. DSW reported the stolen credit and debit card numbers to VISA, MasterCard, Discover and American Express, the major card issuers in the United States.

5.1.12 George Mason University (United States)

George Mason University announced that the personal information of 32,000 students and faculty members may have been stolen. The university discovered unauthorized access by hackers into the school's main ID server during routine system file checks. The hacked ID server held the personal information of all individuals holding university ID cards. The ID card information feared lost included the names, photos, social security numbers, and campus ID card numbers for all students and faculty at the school.

The hackers installed tools on the hacked ID server to allow probes of other servers within the campus network. The school removed the ID server from the network. It appears that rather than searching for specific data, the hackers were attempting to access other systems on the campus network. The school believes that the hackers tried to access other computers on the campus network, but it is not clear if they were successful.

The school has no evidence that any personal information from the ID server has been used fraudulently; however, the type of information stolen could be used for identity theft.

5.1.13 Nevada State Department of Motor Vehicles (United States)

The Nevada State Department of Motor Vehicles reported an office break-in leading to the theft of more than 8,900 personal information records. The computers stolen fro the northern Las Vegas office contained the names, ages, birth dates, social security numbers, photographs and signatures of individuals living in southern Nevada state. The Nevada State Department of Motor Vehicles claims to have encrypted all of the information before the thefts took place, but in fact, the driver's license information had not yet been encrypted as of the day before the theft, allowing easy access.

Nevada state authorities ordered the 21 Department of Motor Vehicles offices to delete all personal information be deleted from their computers to prevent any similar incidents. Further, the Department of Motor Vehicles planned to send letters to the 8,900 individuals affected by the incident during the week following the theft. The driver's licenses of the individuals affected by the theft were invalidated, and new licenses with new authorization numbers were issued.

In addition to the computers, the Department of Motor Vehicles also discovered that the thieves took a special driver's license photo camera, 1,700 blank licenses, and plastic laminate covers embossed with the state seal. The Department of Motor Vehicles had asked the state and federal government for funding to install surveillance cameras in all of the state offices, but no cameras had been installed as of the date of the theft.

5.1.14 University of Mississippi (United States)

The University of Mississippi reported that the personal information for about 700 individuals was exposed through their Web site, including names, social security numbers and five other categories of personal information for 189 individuals.

A list of male and female student club members was accessible over the school's public Web site for an extended period of time. The Web pages holding the information had also been indexed by all of the major search engines, making the list easily accessible to anyone with an Internet connection.

When discovered by school authorities, the personal information was immediately removed; however, but the information had been regarded as a "jackpot" by identity thieves since 2003.

5.1.15 HSBC Holdings (Great Britain/ United States)

HSBC, a well-known international bank, announced that personal information records of 180,000 individuals had been disclosed. The company suspected that up to 180,000 individuals using Polo/ Ralph Lauren MasterCard credit cards may have had their credit card information stolen by thieves. The bank also believed that General Motors MasterCard information could have been stolen as well.

Polo/ Ralph Lauren, MasterCard International and VISA USA inspected the security of the POS system used by the retailer. The companies found that after the POS system processed a credit card transaction, certain credit information was stored within the POS system, rather than being deleted. The companies immediately took measures to delete the data, and modified the POS software accordingly.

This issue not only affected credit cards issued by HSBC Holdings, but all credit card transactions processed by the retailer between June 2002 and December 2004. As a result, the likelihood is high that credit cards of other credit card companies and banks may have been compromised. In this case, it may be that HSBC Holdings was merely the first bank to notice the fraud.

5.1.16 Tufts University (United States)

Tufts University announced that the personal information of 106,000 university alumni and donors may have been compromised. The incident experienced by Tufts University is exactly the same as experienced by Boston College in March 2004. A server storing personal information used by students contacting alumni and other past donors for donations over the telephone was broken into, potentially leaving the information exposed. Information suspected of being hacked includes names, addresses, social security numbers, credit card numbers and other personal data.

The system in question belongs to the university, but the server software was managed by an external not-for-profit corporation.

The university detected abnormal activity on the server between October and December. The server was being used as a file-sharing network broadcast point.

Tufts University claimed that they had no proof that the information stored on the database had been searched or used fraudulently. However, university IT staff could not confirm what, if any, sensitive files were copied, or whether information on the system had been used for criminal purposes. In response to the incident, the school sent letters to the 106,000 alumni and donors who may have had their private information compromised.

At first, Tufts University did not publicly announce the security violation. However, the university decided to report the incident after hearing news accounts of the information theft incidents at California State University, Chico and the University of California, Berkeley.

5.1.17 Personal Information of 15 Million Individuals Leaked (Taiwan)

Taiwanese police authorities in the southern city of Kaohsiung charged and arrested 20 people suspected of illegally collecting and selling the personal information of 15 million individuals to a crime syndicate and others. The police discovered a fraud ring that had sent fake lottery tickets to a large number of residents, and in the course of their investigation, arrested the individuals on suspicion of illegally selling lists of personal information.

The suspects had placed advertisements in several publications indicating they wanted to purchase personal information, offering to purchase information related to names, addresses, telephone numbers and salaries from employees of financial institutions and telephone companies for between ¥2 and ¥16 yen per record. The suspects then sold this personal information to other criminal groups for between ¥3 and ¥32, based on the volume of personal information provided. Authorities stated that the group had already sold the personal information for as many as 5 million individuals for more than ¥160 million. The leaked personal information represents a full two-thirds of the population of Taiwan.

The authorities are still investigating other alleged crimes and the routes by which personal information was obtained.

5.2 Observations

Table 8 summarizes the Personal Information Disclosure Incidents described above:

Table 8 Overseas Information Disclosure Incidents

Organization Name	Country	No. of Victims	Disclosed Information	Cause of Disclosure	Information Disclosure Route
AOL (America Online)	United States	93 million	Screen name, email address, telephone number, ZIP code, credit card name	Internal Crime/ Internal Fraud	Unknown
ChoicePoint	United States	145,000	Name, address, social security number, credit card number, credit report information	Other (fraud)	Internet/ Web
LexisNexis	United States	32,000	Address, name, social security number, driver's license number	Unauthorized Access	Internet/ Web
Bank of America	United States	1.2 million	Credit card number and account data, name, address, social security number	Loss	FD or other recordable media
Boston College	United States	120,000	Name, telephone number, address, social security number	Unauthorized Access	Internet/ Web
Ameritrade	United States	200,000	Personal Information	Loss	FD or other recordable media
San Jose Medical Group	United States	185,000	Medical information (medical billing code), financial information (social security number), 2004 audit information	Theft	PC theft
University of California, Berkeley	United States	1.4 million	Name, address, telephone number, social security number, birth date, medical provider name	Unauthorized Access	Internet/ Web
University of California, Berkeley	United States	98,369	Name, address, social security number, birth date	Theft	PC theft
Organization Name	Country	No., of Victims	Disclosed Information	Cause of Disclosure	Information Disclosure Route
California State University, Chico	United States	59,000	Name, address, social security number	Unauthorized Access	Internet/ Web
DSW Shoe Warehouse	United States	Unknown	Card number, name, vendor information Bank account number, driver's license	Unauthorized Access	Internet/ Web
George Mason University	United States	32,000	Name, photograph, social security number, campus ID card number	Unauthorized Access	Internet/ Web
Nevada State Department of Motor Vehicles	United States	8,900	Name, age, birth date, social security number, photograph, signature	Theft	PC theft

Organization Name	Country	No. of Victims	Disclosed Information	Cause of Disclosure	Information Disclosure Route
University of Mississippi	United States	700	Name, social security number, three other categories of information	Configuration Error	Internet/ Web
HSBC Holdings	Great Britain, United States	180,000 + unknown	Partial financial transaction data	Bug/ Security Hole	Unknown
Tufts University	United States	106,000	Name, address, social security number, credit card number	Unauthorized Access	Internet/ Web
Financial institution and telecommunications company employees, etc.	Taiwan	15 million	Name, address, telephone number, income, etc.	Internal Crime/ Internal Fraud	Unknown

We also confirmed several other Information Disclosure Incidents in addition to those summarized in Table 8 above:

- University of California, Los Angeles. A notebook computer containing information of 145,000 individuals stolen.
- California State Employment Development Department. Names of 55,000 individuals disclosed.
- University of Nevada, Las Vegas
- The Wharton School of the University of Pennsylvania
- Kellogg School of Management, Northwestern University
- University of California, San Francisco. Hackers may have stolen the ID information of 7,000 individuals.

Due to the fact that most of the Personal Information Disclosure Incidents we researched occurred within the United States, we have decided to focus our observations on Personal Information Disclosure Incidents in the United States.

One notable characteristic about Personal Information Disclosure Incidents occurring in the United States during 2004 is the frequency of disclosure incidents at institutions of higher learning (colleges and universities). At the initial stages of the spread of the Internet, universities utilized open networks, easily targeted by hackers and others. Judging by the results of our survey, which indicate that five out of the seven incidents noted occurred due to unauthorized access from external locations, it appears that universities still have major unresolved computer security issues.

We also note that the Personal Information Disclosure Incidents occurring at Boston College and Tufts University were similar in every detail. Every university in the United States keeps a database containing the information of graduates and previous donors for the purposes of seeking new donations. Further, since these databases are not managed under the direct supervision of the university, the security surrounding these databases is not sufficient. Accordingly, it appears that these graduate and donor databases present an appealing target for attack.

Another notable point about Personal Information Disclosure Incidents in the United States is that every database in question contained the social security number (SSN) of the victims. In the

United States, a social security number is an important registration number required to receive social security benefits and submit tax filings. Even more than this, the social security number is a most vital number, intimately connected to the identity of the holder, and required for such basic tasks as obtaining a driver’s license, opening bank accounts, applying for telephone/ mobile phone contracts, signing apartment rental agreements, and using public services such as electricity/ water/ gas. Meanwhile, an individual can be specifically identified by this number alone, which means we see many cases where the social security number is used as the main identification number (primary key) in many database structures. As we have reported, many organizations experiencing Information Disclosure Incidents have deleted social security numbers from their databases. However, we expect the risk of Personal Information Disclosure to continue in the United States, due to the sheer number of databases that continue to use the social security number as the main identification number (primary key) in their structure.

6 Calculating the Projected Compensation for Damages related to Personal Information Disclosure

6.1 Objective of Calculating Projected Compensation for Damages

One of the earmarks of the Working Group is proposing a calculation model for calculating compensation for damages, and then applying calculations to actual Personal Information Disclosure Incidents.

From its inception the Working Group has engaged in activities analyzing actual incidents for the purpose of quantifying the corresponding risks and effectiveness of the subsequent response. The objective behind proposing a calculation model for projected compensation for damages is to provide organizations with a quantitative understanding of the latent risks involved in handling personal information.

We report the results of applying our calculation model to Personal Information Disclosure Incidents occurring during 2004 in the following sections of this paper. However, our intent is that organizations use this calculation model to grasp the latent risks connected with the personal information possessed within their organizations. We encourage all organizations to conscientiously apply this calculation model to the personal information maintained and managed within their systems.

Please understand that the calculation results shown below are based on the assumption that all victims are seeking compensation for damages related to the specific incident described. Our calculations do not reflect any actual payments made in connection with the corresponding Personal Information Disclosure Incident.

6.2 Explanation of the Projected Compensation for Damages Calculation Model

Our calculations of compensation for damages occurring during 2004 adhere to the research methods we used for our 2003 survey.

Our decision was based on the fact that we were unable to discover any legal precedents related to individuals or groups seeking compensation for damages related to Personal Information Disclosure Incidents subsequent to the conclusion of our 2003 survey. Had such legal precedent occurred, we would have incorporated the new fact patterns into our calculation model.

Please see our 2003 report for details behind the genesis of the calculation model we use to calculate projected compensation for damages.

Here, we will provide a simple overview.

6.2.1 Process behind the Formation of the Projected Compensation for Damages Calculation Model

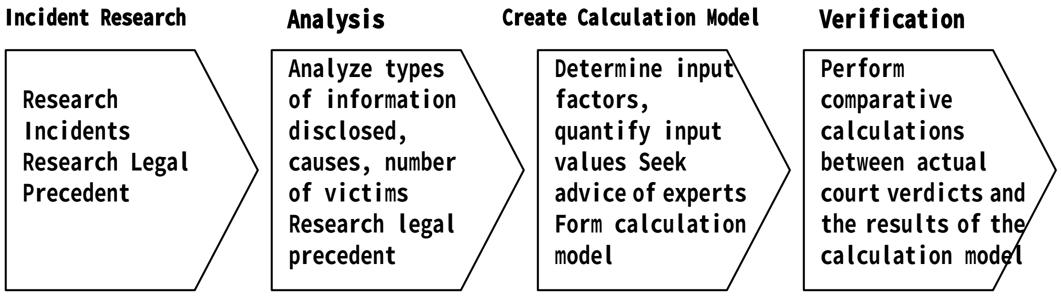

Incident Research
Analysis
Create Calculation Model
Verification
Research Incidents Research Legal Precedent
Analyze types of information disclosed, causes, number of victims Research legal precedent
Determine input factors, quantify input values Seek advice of experts Form calculation model
Perform comparative calculations between actual court verdicts and the results of the calculation model

Fig. 14 Process behind the Formation of the Projected Compensation for Damages Calculation Model

We developed our calculation model as depicted in Fig. 14 above:

(1) Preliminary Research

Research and collection of data about publicly announced Personal Information Disclosure Incidents.

At the same time, we also conducted research into past court cases involving invasion of privacy and defamation. Here, as we discussed in our 2003 report, we incorporated data from the 2003 decision by the Osaka Supreme Court regarding the appeal of the judgment in the case (No. 1165) related to the disclosure of the Uji City basic residential register into our calculation model.

(2) Analysis

We analyzed compilations of the number of victims, the types of information disclosed, the cause of the disclosure, the information disclosure route, and other factors related to the Personal Information Disclosure Incidents. “Appendix 1 Table A” describes the results of our analysis.

(3) Create Calculation Model

Having determined the input factors for our calculation model, we began to develop the model itself. Input factors included the value of the information disclosed, the degree of social responsibility of the organization(s) involved, and an evaluation of the post-incident response by the organization.

Further, we asked for, and incorporated, the opinions of lawyers and other legal experts.

(4) Verification

To measure the credibility of our calculation model, we applied our model to the previously mentioned Uji City registry disclosure case, comparing the results of our calculations with the actual determination of damages ordered by the court. As mentioned in our 2003 report, the level of damages according to our calculations were essentially the same as the actual legally mandated figure.

6.2.2 Explanation of the Calculation Model Input Values

We incorporated the following input values into our calculation model:

- Value of the personal information disclosed
- The degree of social responsibility of the organization in question
- Appraisal of the post-incident response by the organization in question

In an actual lawsuit, one would expect that in addition to the factors above, the courts would also consider the protective measures in place before the incident, the volume of the disclosed information, the actual damages incurred, and specific measures taken in response to the incident. However, for purposes of forming our calculation model, our only sources are publicly available information, and there are limits in what can be inferred by the other factors previously described. In addition, we narrowed the number of input factors, reasoning that an unnecessarily complicated calculation model would be counterproductive to our main goal of encouraging organizations to use the calculation model to evaluate their own risks.

The following describes how we quantified each of the input factors used in our calculation model:

6.2.2.1 Value of the Personal Information Disclosed

We categorized the effect of Personal Information Disclosure on a victim in terms of “Economic Loss” and “Emotional Distress.” To quantify the extent of the effect, we created a chart, with “Economic Loss” on the ‘Y’ axis and “Emotional Distress” on the ‘X’ axis. For the sake of convenience, we call this an Economic-Privacy Map (EP Map) (Fig. 15). The farther removed from the origin, the greater the respective levels of Economic Loss and Emotional Distress.

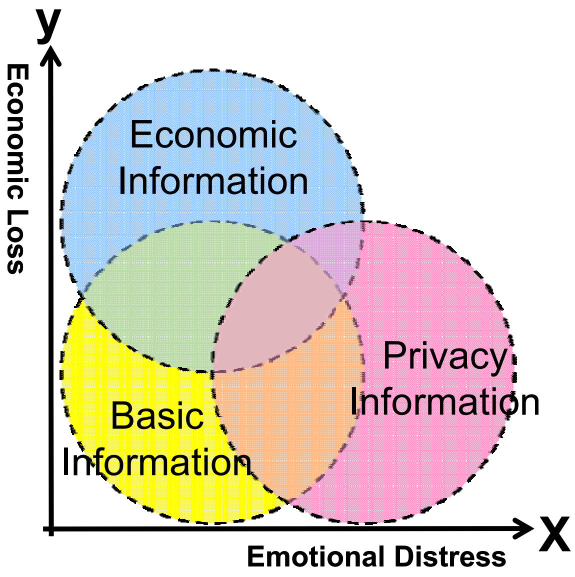
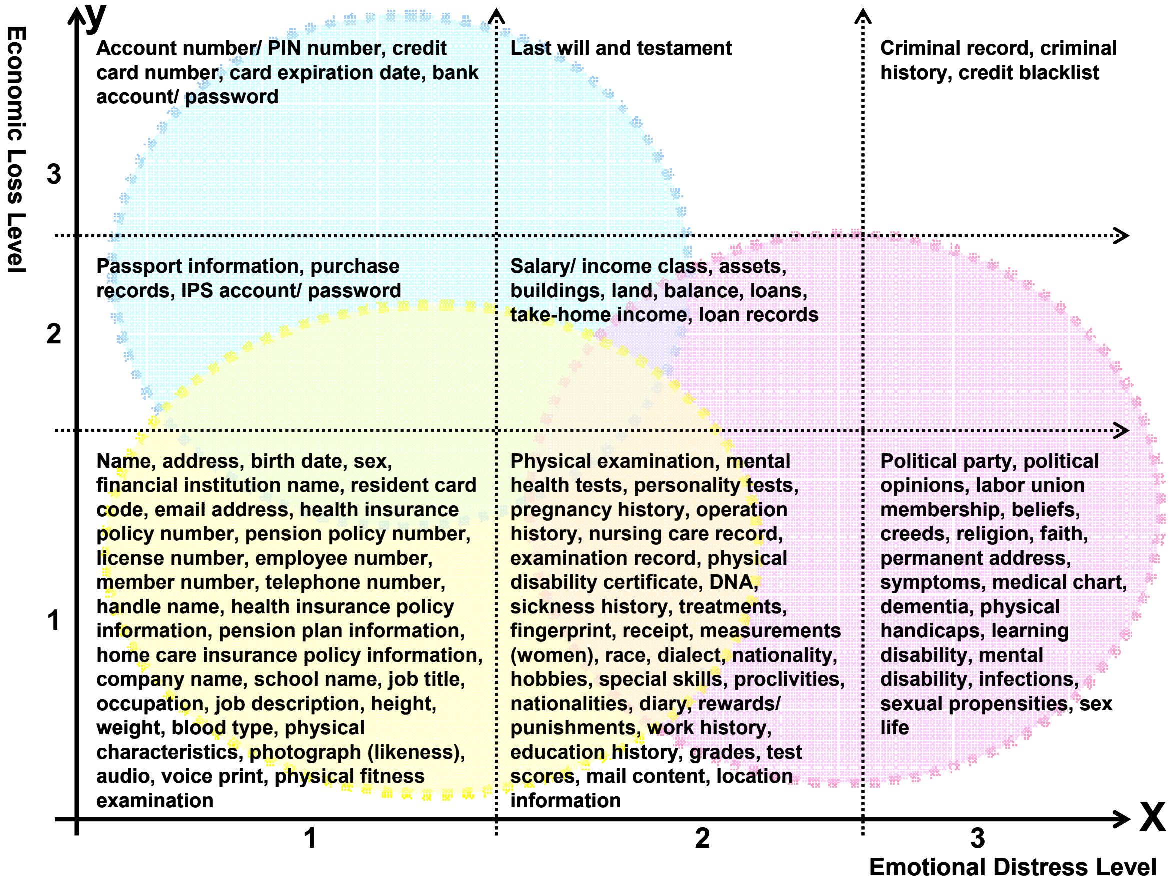


Fig. 15 Economic – Privacy Map (EP Map)

On this EP Map, we plotted the types of disclosed information noted from our past research and analysis of Information Disclosure Incidents. We can then use this EP Map plot locations to derive the type of effect associated with disclosed information, or in other words, what level of value the information represents. Further, in considering the ease of inputting these values into our calculation model, we defined three stages corresponding to the degree of influence of the X and Y axes on the EP Map, reconfiguring the types of disclosed information. This resulted in our EP Map becoming a Simple-EP Map (Fig. 16).



	1	2	3
3	Account number/ PIN number, credit card number, card expiration date, bank account/ password	Last will and testament	Criminal record, criminal history, credit blacklist
2	Passport information, purchase records, IPS account/ password	Salary/ income class, assets, buildings, land, balance, loans, take-home income, loan records	
1	Name, address, birth date, sex, financial institution name, resident card code, email address, health insurance policy number, pension policy number, license number, employee number, member number, telephone number, handle name, health insurance policy information, pension plan information, home care insurance policy information, company name, school name, job title, occupation, job description, height, weight, blood type, physical characteristics, photograph (likeness), audio, voice print, physical fitness examination	Physical examination, mental health tests, personality tests, pregnancy history, operation history, nursing care record, examination record, physical disability certificate, DNA, sickness history, treatments, fingerprint, receipt, measurements (women), race, dialect, nationality, hobbies, special skills, proclivities, nationalities, diary, rewards/ punishments, work history, education history, grades, test scores, mail content, location information	Political party, political opinions, labor union membership, beliefs, creeds, religion, faith, permanent address, symptoms, medical chart, dementia, physical handicaps, learning disability, mental disability, infections, sexual propensities, sex life

Fig. 16 Simple-EP Map

However, we did not simply obtain the value of the disclosed information according to the plot location between the X and Y values. Rather, we believed that a slight correction was required to more easily relate these values to the actual damages incurred. These corrections have been incorporated into the following formula for calculating the value of disclosed information:

■ Value of Disclosed Personal Information
= Value of Basic Information × Degree of Information Sensitivity
× Degree of Ease in Identifying the Individual

a. Value of Basic Information

We assign 500 points as the base value for the Value of Basic Information, regardless of the type of information in question.

b. Degree of Information Sensitivity

In general, most definitions of sensitive information are limited to certain types of information defined as personal information, the collection of which is prohibited under JIS Q 15001. Such information includes personal information that may serve as the root of philosophical, religious or social discrimination. However, there are certainly other types of information that may cause Emotional Distress. In our calculation model, we have established levels for three stages of Personal Information as a whole, providing definitions allowing calculation of the sensitivity of the information from the corresponding values. Further, we have also included in our calculation model the degree of information sensitivity for information leading to economic loss.

The Degree of Information Sensitivity is derived from the following formula, using the location of the plot (x,y) of the related information on the Simple-EP Map (=level value).

Degree of Information Sensitivity = $(10^{x-1}+5^{y-1})$

If the disclosure consists of several types of information, we use whichever information generates the largest X and largest Y values. For example, if the disclosure involves “Name, address, birth date, sex, telephone number, name of sickness, and account number,” then the Simple-EP Map (x,y) will be as follows:

“Name, address, birth date, sex, telephone number” = (1,1)

“Name of sickness” = (2,1)

“Account number” = (1,3)

In this example, the largest X value is “Name of sickness” at “2,” while the largest Y value is “Account number” at “3.” Plugging these values into our formula, we get:

$(10^{2-1}+5^{3-1}) = (10^{1}+5^{2}) = 35$ points

c. Degree of Ease in Identifying the Individual

Degree of Ease in Identifying the Individual represents the ease with which the disclosed Personal Information can be used to specifically identify an individual. For example, if a credit card number is disclosed, but there isn’t any information to identify the name, etc. of the individual, there is a low likelihood of actual damages. Accordingly, we have incorporated the Degree of Ease in Identifying the Individual into our calculation model. This factor is subject to the determination standards shown in Table 9 below.

Table 9 Degree of Ease in Identifying the Individual – Determination Standards

Determination Standards	Degree of Ease in Identifying the Individual
Individual may be easily identified. "Name" and "Address" included.	6
Individual may be identified after certain costs are incurred. "Name" or "Address + Telephone Number" included.	3
Difficult to identify the individual. Other than that described above.	1

6.2.2.2 Degree of Social Responsibility of the Organization involved in Information Disclosure

As shown in Table 10, the Degree of Social Responsibility is either "Higher than Normal" or "Normal." The standard for an organization with a "Higher than Normal" degree of Social Responsibility include those that are described in "Basic Principles regarding the Protection of Personal Information (Cabinet decision April 2, 2004)" as being in a "specific industry that requires a guarantee of the appropriate handling" of personal information. Included in this definition are public institutions such as government agencies, and large companies that enjoy high levels of name recognition.

Table 10 Degree of Social Responsibility of the Organization Involved in Information Disclosure – Determination Standards

Determination Standards		Degree of Social Responsibility
Higher than Normal	Organizations in specific types of industries requiring a guarantee of the appropriate handling of personal information (medical, financial/ credit, telecommunications, etc.), public institutions, and large companies with high name recognition.	2
Normal	Other normal companies, associations and organizations.	1

6.2.2.3 Appraisal of Post-Incident Response

The appraised value of Post-Incident Response is based on Table 11 below. In cases where the Post-Incident Response is "Unknown, Other," we assume that no inappropriate responses were detected, and therefore assign the same value as given to an appropriate response.

Table 11 Appraisal of Post-Incident Response - Determination Standards

Determination Standards	Appraisal of Response
Appropriate	1
Inappropriate	2
Unknown, Other	1

Since there are no clear standards as to how to evaluate Post-Incident Responses, we use the following response chart compiled from past responses to Information Disclosure Incidents as a guideline for determining an appropriate/ inappropriate response.

a. Examples of Appropriate Responses

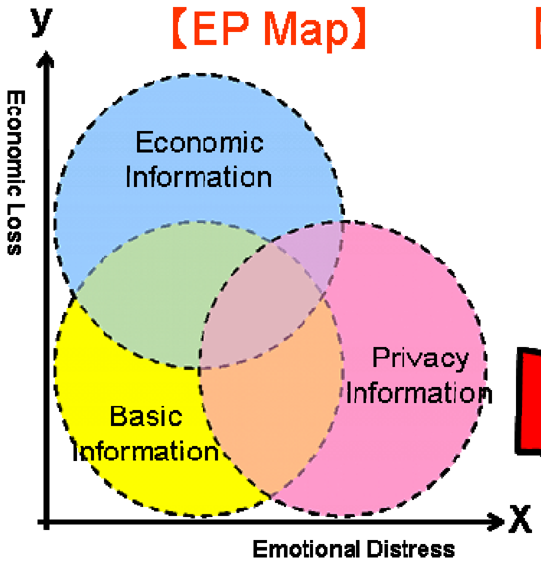
- Rapid response
- Understanding of the circumstances
- Public announcement of the incident
- Subsequent disclosure of the circumstances (Website, email, letters)
- Communicating with victims, offering apologies
- Offering apologies to victims (including presentation of gift certificates, etc.)
- Estimates of effects likely to occur
- Establishment of a claims contact office/ person
- Efforts to retrieve the disclosed information
- Expression of appreciation to the party discovering the incident/ full account of the incident
- Compensation to customers
- Improvement of system through management participation
- Investigation into the cause of the incident
- Improved security measures
- Review of all procedures
- Expert review of system appropriateness
- Implementation of advice and audits from outside experts

b. Examples of Inappropriate Responses

- Issues were indicated, but not addressed
- Slow response
- Repeated occurrences
- Measures were implemented, but were ineffective
- False reporting

6.2.3 Projected Compensation for Damages Calculation Model

The following represents an overall view of the Calculation Model, integrating the factors discussed in “6.2.2 Explanation of the Calculation Model Input Values.”



【Determination Standards Table】

Determination Standards		Degree of Social Responsibility
Higher than Normal	Organizations in specific types of industries requiring a guarantee of the appropriate handling of personal information (medical, financial/ credit, telecommunications, etc.), public institutions and large companies with high name recognition.	2
Normal	Other normal companies, associations and organizations.	1

Determination Standards	Appraisal of Response
Appropriate	1
Inappropriate	2
Unknown, Other	1

Determination Standards	Degree of Ease in Identifying the Individual
Individual may be easily identified.	6
"Name" and "Address" included.	
Individual may be identified after certain costs are incurred.	3
"Name" or "Address + Telephone Number" included.	
Difficult to identify the indvidual.	1
Other than that described above.	

Projected Compensation for Damages
= Value of Information Disclosed × Degree Social Responsibility of the Organization
× Appraisal of Post-Incident Response
= (Value of Basic Information×Degree of Sensitivity × Ease in Identifying the Individual)
×Degree of Social Responsibility of the Organization × Appraisal of Post-Incident Response
= Value of Basic Information [500] × Degree of Information Sensitivity [Max(10^{x-1} + 5^{y-1})]
× Ease in Indentifying the Individual [6,3,1]
× The degree of social responsibility of the organization in question[2,1]
× Appraisal of the post-incident response by the organization in question[2,1]

The Working Group calls the above Projected Compensation for Damages Calculation Model the “JO Model (JNSA Damage Operation Model for Individual Information Lead).”

6.3 Results of Calculating Projected Compensation for Damages for 2004

"Appendix 1 Table B" shows the results of applying the Projected Compensation for Damages Calculation Model to our survey of 2004 Information Disclosure Incidents.

6.3.1 EP Distribution by Industry

Fig. 17 and Fig. 18 show the distribution of the 2004 survey results categorized on a Simple-EP Map according to industry.

Fig. 17 represents the level of "Emotional Distress,' while Fig. 18 represents the level of "Economic Loss."

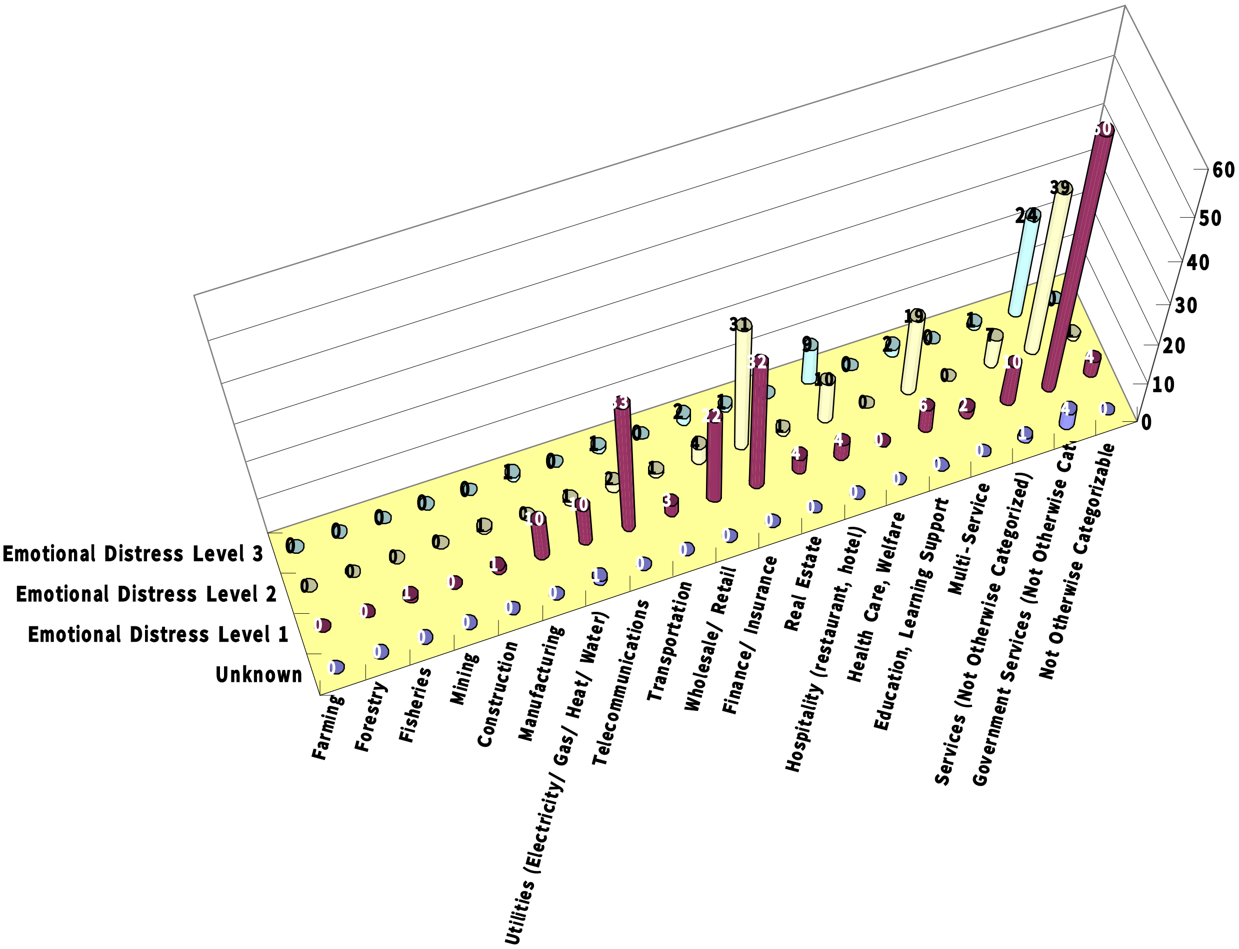


Fig. 17 EP Distribution by Industry (Emotional Distress Level)

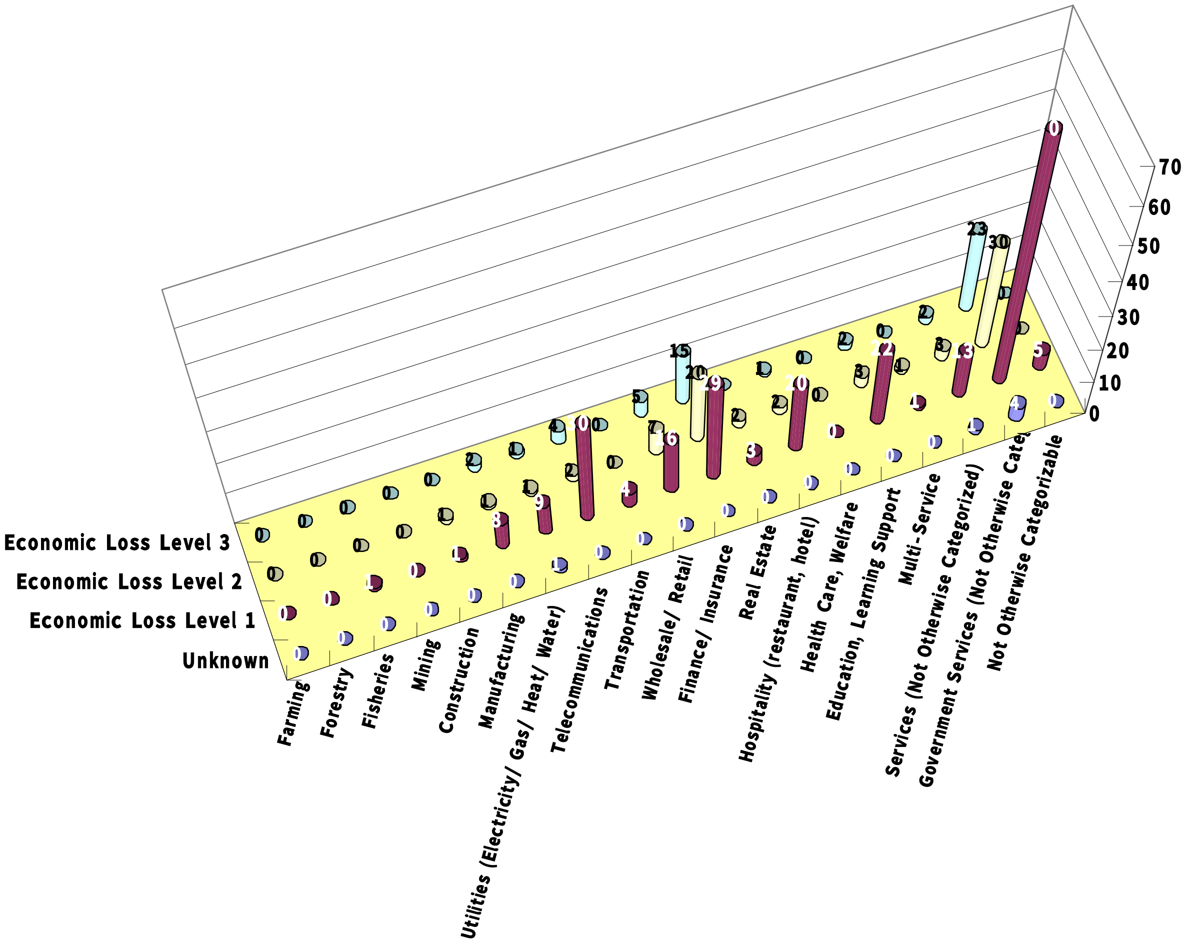


Fig. 18 EP Distribution by Industry (Economic Loss Level)

From these figures, we see that in terms of both Emotional Distress and Economic Loss, the “Government Services (Not Otherwise Categorized)” and “Finance/ Insurance” categories are disclosing highly ranked information.

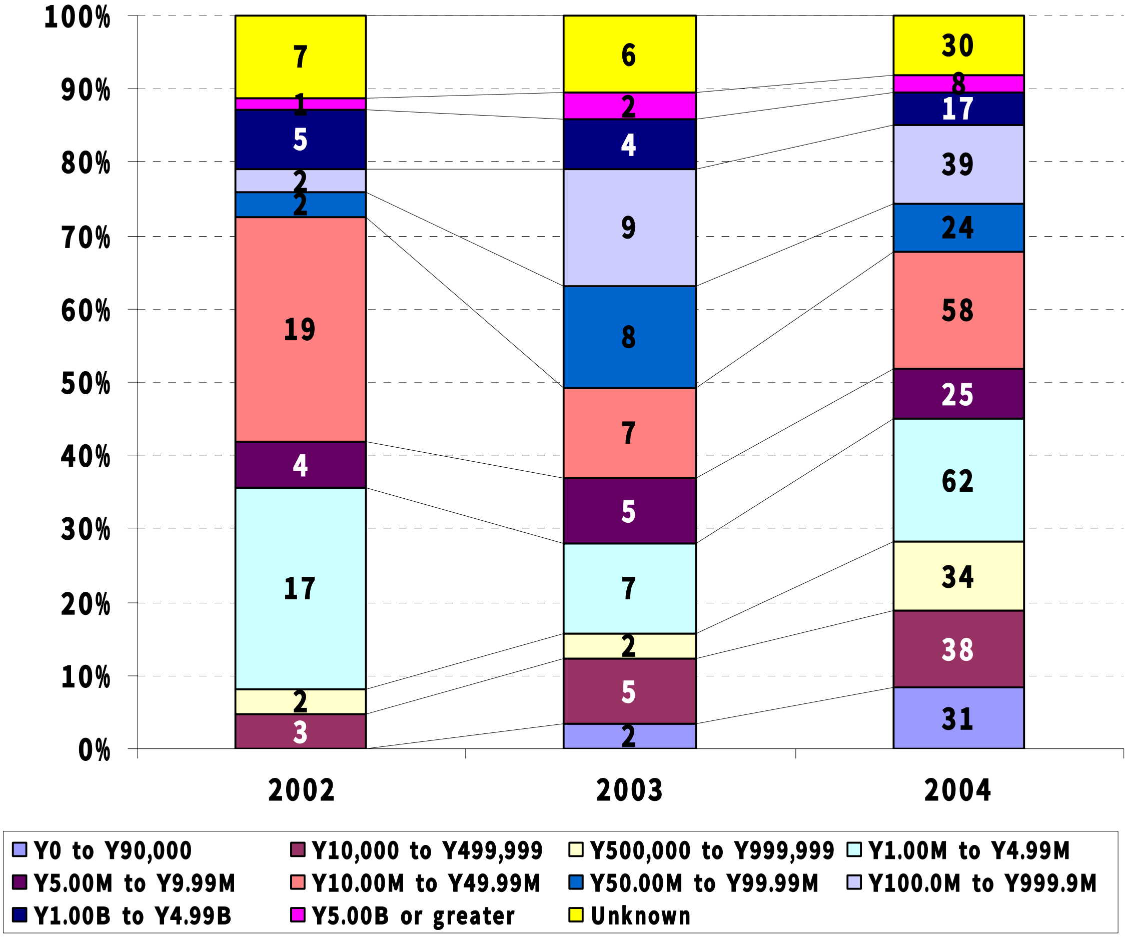
Looking at Fig. 18, we see that in each industry there are many cases of Information Disclosure of information of a relatively low rank (1), and as the importance of the information disclosed increases, there is a corresponding decrease in the number of incidents. We believe we can conclude that information associated with a high level of Economic Loss, such as account numbers and passwords, are generally managed appropriately, making Information Disclosure difficult.

However, Fig. 17 shows that there are a number of industries indicating differing trends in the relationship between Emotional Distress level (emotional rank) and frequency of disclosure. For the “Medical/ Welfare” and “Education/ Training” categories, we see more incidents involving information with a higher rank of 2 or 3 than we do for lesser important information with a rank of 1. We conclude that these industry categories are not doing a proper job of managing information associated with higher levels of Emotional Distress. The “Medical/ Welfare” and “Education/ Training” categories deal mainly in medical information, grade performance reports and other information related to an individual’s private matters. We strongly recommend that organizations in these categories understand the sensitive nature of the information they possess, and take all measures possible to protect this information.

6.3.2 Interannual Fluctuations in Projected Compensation for Damages

Fig. 19 shows the interannual fluctuations in total compensation for damages per incident 1, while Table 12 shows the interannual fluctuations in total compensation for damages.

Fig. 19 Interannual Fluctuations in Total Projected Compensation for Damages



Many incidents involving low numbers of victims were reported during 2004. Accordingly, we see a comparative increase in the ratio of incidents for which the total compensation for damages was less than ¥1 million. Ultimately, we see the occurrence here of incidents corresponding to all levels on the compensation for damages scale. While one might tend to conclude that comprehensive measures are taken to prevent incidents involving large-scale, important Personal Information, making incidents less likely, and that lesser measures are taken to protect lower volumes of less-important Personal Information, making incidents more likely, the fact is that Disclosure Incidents appear to occur regardless of the volume or importance of Personal Information involved.

Fig. 20 shows the Interannual fluctuations in compensation for damages per victim.

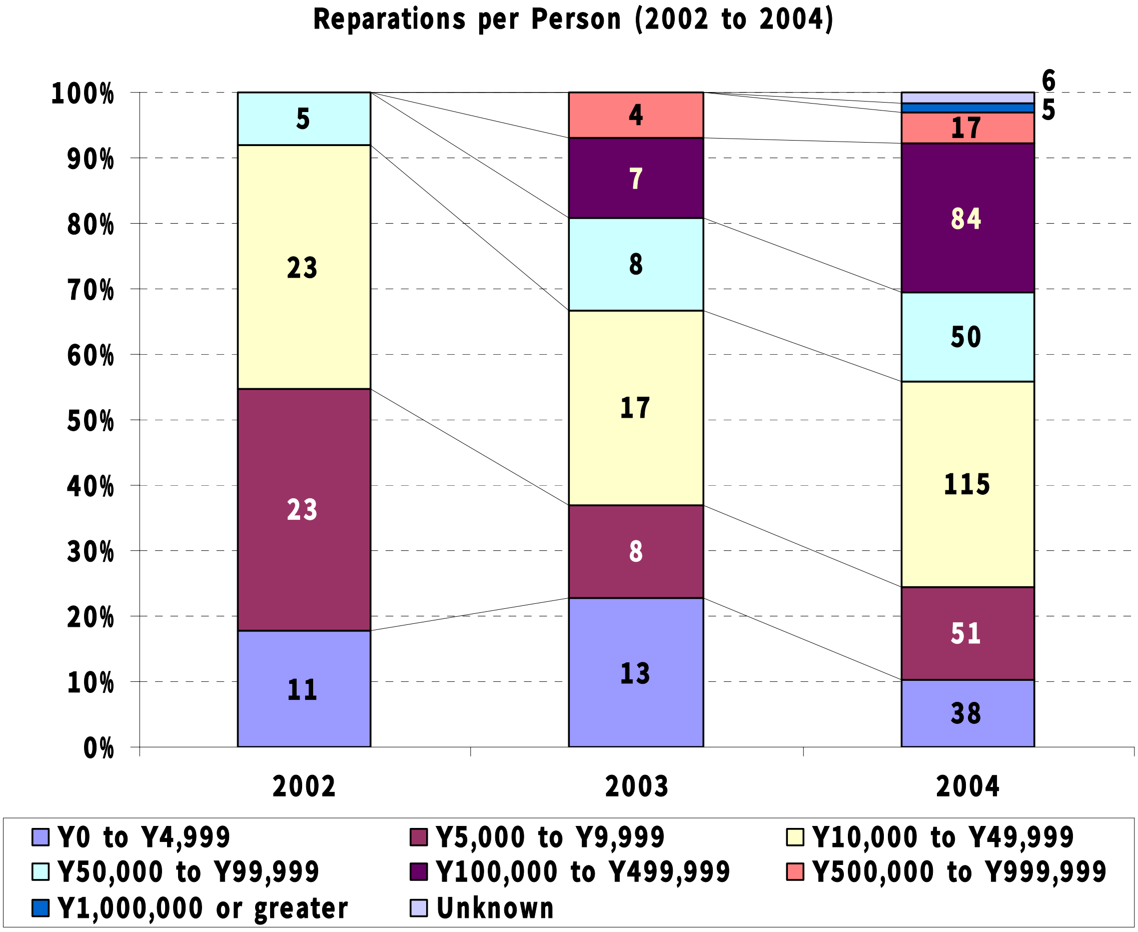


Fig. 20 Changes in Compensation for Damages per Victim – 2002 to 2004

In 2003, the compensation for damages per victim in the range between ¥100,000 and ¥490,000 accounted for 12.3% of the total. In 2004, this value increased significantly, accounting for 23% of the total. The ratio of incidents involving compensation between ¥0 and ¥4,000 decreased year-on-year, while the overall ratio of incidents involving large sums of compensation per victim increased.

Table 12 Total Annual Compensation for Damages – 2002 to 2004

2002	2003	2004
¥18,922,010,000	¥28,069,360,000	466,692,500,000

Here, we see that the total compensation for damages in 2004 rose 16.6 times compared to 2003.

As shown in Table 6 of “4.3.6.4 Interannual Fluctuations in Number of Victims,” the increase in the number of victims was 6.7 times the 2003 figure. Considering this fact, we can conclude that the increase in compensation for damages far outstripped the increase in the number of victims.

What would account for the increase in total projected compensation for damages? We believe that this increase can be explained by the increase in the number of Disclosure Incidents in the “Government Services (Not Otherwise Categorized)” category, a category with a correspondingly high level of social responsibility, combined with the disclosure of information highly ranked on the EP scale by the “Government Services (Not Otherwise Categorized)” and “Finance/ Insurance” categories (both categories having higher than normal social responsibility) as shown in Figs. 17 and 18 in “6.3.1 EP Distribution by Industry.”

Table 13 shows the average Interannual fluctuations in projected compensation for damages per incident.

Table 13 Average Projected Compensation for Damages per Incident – 2002 to 2004

2002	2003	2004
¥344,040,000	¥550,380,000	¥1,388,970,000

The average projected compensation for damages per incident increased 2.5 times between 2003 and 2004.

7 Information Disclosure Incident Influence on Corporate Value (Observations of Share Price Fluctuations)

On a daily basis, companies strive to enhance consumer trust, engaging in public relations initiatives and investor relations activities to create greater corporate value. However, frequent Information Disclosure Incidents lead to lost trust and a decline in corporate value. In the worst case, an Information Disclosure Incident could be foreseen to develop into a manner threatening the very existence of the company.

Accordingly, as in the past, we will include in this year's report our observations on the influence of Information Disclosure Incidents on corporate value. Our approach will be to draw implications about the effect of an Information Disclosure Incident on corporate value based on fluctuations in share prices.

7.1 Methodology for Understanding the Influence of Information Disclosure Incidents on Corporate Value

7.1.1 Conceptual Model

Our basic assumption is that the occurrence of an Information Disclosure Incident leads to a loss of faith in the organization, and if the organization in question is a public company, this loss of faith works to the detriment of share prices. Based on this assumption, we propose a conceptual model hypothesizing that the share price of the company in question is strongly related to the overall stock market, and that we can reasonably approximate the overall stock market using the Nikkei Average (Overall Stock Market is approximately equal to Nikkei Average). Accordingly, we believe we can calculate the degree of influence on share price based on the calculation model that follows.

7.1.2 Calculation Model

1) Share Price Fluctuation (deviance from the expected company share price)

We calculate the deviation in share price by first noting the share price (closing price) of the company in question on the nth day from the public announcement of the Information Disclosure Incident. We then derive the expected share price of the company in question by calculating the price movements of the Nikkei Average on the nth day after the public announcement of the Information Disclosure Incident, finding the deviation in price between actual and expected closing prices on day n. The expected share price on day n is calculated using the ratio between the Nikkei Average and the actual closing price of the company's shares. We call the ratio on day n the "N Day Ratio," and ratio that serves as our base is called the "Base Ratio."

$$\boxed{\text{N Day Ratio} = \frac{\text{Day N Share Price (closing)}}{\text{Day N Nikkei Average (closing)}}} \quad \cdots\cdots\cdots\cdots\cdots \quad (1)$$

$$\boxed{\text{Base Ratio} = \frac{\text{Base Share Price (closing)}}{\text{Base Nikkei Average (closing)}}} \quad \cdots\cdots\cdots\cdots\cdots \quad (2)$$

For calculating the Base Ratio (see Formula 2), we use the “company’s base share price” (closing price) and the “Nikkei Average base share price” (closing price), which consists of the average of respective closing prices (business day base) during the week prior to the public announcement of the Information Disclosure Incident.

The value of the deviation between the company’s closing share price and the expected closing share price on day n (“Deviation Value”) are calculated as follows, using Formulas 1 and 2:

$$\text{Deviation Value (n)} = (\text{Day N Ratio} - \text{Base Ratio}) \text{ x Day N Nikkei Average (closing)} \qquad (3)$$

2) Determination of the Influence on Company Share Prices

We can determine the influence on company share prices by identifying the ratio between the daily Deviation Value over a 14-day period (business day base) beginning with the public announcement, and the base share price for the company. In our calculations for this year’s survey, we will again use the short-range period of 14 days. This short period was selected to eliminate any errors that may be caused by reports of fraud, etc. being made public after the passing of a certain period of time.

$$\text{Degree of Deviation} = \frac{\text{Daily Average Deviation Value}}{\text{Base Share Price (closing)}} \cdots\cdots\cdots\cdots\cdots (4)$$

In the past, we determined the influence on company shares to be the “Daily Average Deviation Value” multiplied by the number of issued shares. For this year’s calculation, we will make the determination using the degree of deviation (Daily Average Deviation Value divided by the influence on company value for the company in question).

7.2 Case Study – Observations on the Influence on Corporate Value

1) Influence on Corporate Value

Table 14 shows the calculations of the Deviation Value for 68 companies experiencing Information Disclosure Incidents. Looking at the daily Deviation Value over the 14 days subsequent to the public announcement of the incident, we see the value of several companies rising initially, contrary to our hypothesis. This phenomenon was also confirmed in our 2003 survey.

2) Influence on Group Company Share Prices (Reference)

While we were not able to obtain share prices for these companies, there were several instances in which we were able to obtain the share prices for the group or parent company of the company in question (group company share prices, etc.). We used these share prices to calculate the Deviation Value. These results are shown in Table 15. As with 1) above, we saw the share prices of several companies rise during the period in question. Due to the difficulty of arguing the effect of Information Disclosure on group company share prices, we have provided these values for reference purposes only.

3) Influence on Share Price of Contractors

Looking at the Information Disclosure Incidents occurring during 2004, we noted more than a few instances in which the reports referred to contractors. In these cases, we investigated the share price fluctuations for these contractors, the results of which are shown in Table 16. Again, we see several instances of share price increases; however, we do note a significant trend of decreasing share prices, leading us to conclude that an influence indeed exists from the standpoint of share price fluctuations.

4) Influence on Share Price of *Keiretsu* Companies (Reference)

During 2004, several Information Disclosure Incidents occurred in retail companies belonging to different *keiretsu* (a number of horizontally and vertically linked companies). Here, we conducted an investigation to see what, if any, influence an Information Disclosure Incident originating in a retail company had on the company at the top of the corresponding *keiretsu* (manufacturer). The results of this investigation are shown in Table 17. While it is difficult to make a categorical argument, our results indicated the possibility that *keiretsu* companies are affected by Information Disclosure occurring in other companies along the same *keiretsu* chain. Here, we have provided the values for reference purposes only.

5) Overall Trends for 2004

Fig. 21 is a scatter diagram plotting the Deviation Values calculated for groups 1) through 4) described above. From this diagram, we see that share prices fluctuate in a range from approximately -8.00% to approximately +8.00% after an Information Disclosure Incident. Further, we see from the behavior of plot point collection and distribution that the points converge in the range between -4.00% and +2.00%.

6) Interannual Comparison

Fig. 22 is a scatter diagram plotting the Deviation Values related to our surveys over the three-year period between 2002 (our initial survey) and 2004. This three-year interannual comparison also indicates that post-incident share prices fluctuate in the range between -8.00% and +8.00%. For 2003, the overall trend was on the plus side of the equation. Again, we see from the behavior of plot point concentration and distribution here that the Deviation Values converge in the range between -4.00% and +2.00%.

Table 14 Deviation between Expected Company Share Price and Actual Company Share Price

Case No.		No. 01	No. 02	No.03	No. 04	No. 05	No. 06	No. 07	No. 08
Deviation Value from Expected Share Price on Day N after Public Announcement	1	34.76	-17,468.37	-42.58	105.39	2.91	6.17	-8.20	7.87
	2				-97.24	2.10	2.16	-6.51	17.08
	3				-17.24	-5.12	8.89		
	4	-50.01	25,748.63	-61.70	-68.88		7.59		
	5	-13.72	1,858.81	-96.68	-95.28			20.15	19.01
	6	-46.10	42,217.45	-89.29		-2.61		6.33	11.53
	7	-159.42	52,229.25	-96.85		-6.32	14.48	43.40	16.25
	8	-190.94	81,657.58	-93.60	-196.20	-5.66	11.00	39.24	12.17
	9				-153.82	0.65	12.08	39.46	4.74
	10				-179.81	-0.68	8.13		
	11	-58.43	112,600.77	-111.17	-194.15		7.45		
	12	-59.16	191,082.09	-87.08	-177.27			-5.20	13.59
	13	-258.01	167,769.71	-86.51		-1.07		36.01	29.16
	14	-244.36	165,391.17	-72.90		-1.19	9.46	58.35	30.01
	Total	-1,045.38	823,087.07	-838.35	-1,074.50	-16.98	87.42	223.04	161.40
Daily Average Deviation Value		-104.54	82,308.71	-83.84	-107.45	-1.70	8.74	22.30	16.14
Ratio of Base Share Price (%)		-2.60	5.46	-8.19	-2.50	-0.68	3.80	2.21	4.83

Case No.		No. 09	No. 10	No. 11	No. 12	No. 13	No. 14	No. 15	No. 16
Deviation Value from Expected Share Price on Day N after Public Announcement	1	2,638.06	-8.32		-32.67	-6.47	-3.25	36.68	63.97
	2	3,022.83	-9.16	-9.95	-17.35	-0.01	-19.77		89.57
	3	1,555.51	-15.46	-6.38	-12.88				142.08
	4	-1,195.14		-10.16				129.34	203.68
	5				-7.10	-5.74	-36.48	95.63	
	6		-19.48	-0.88		2.84	-45.75	70.86	
	7	-6,124.98	-16.68			3.27	-39.66	105.20	221.71
	8		-7.73			0.36	-27.12	94.15	161.13
	9	519.71				0.91	-36.50		193.22
	10	426.78	-3.04						199.43
	11				-12.20			136.15	188.11
	12			4.83	-24.40	-4.71	-51.05	104.06	
	13			-5.19		-1.53	-22.68	96.61	
	14	-1,241.45				0.72	-16.17	104.09	187.36
	Total	-398.71	-79.88	-27.73	-106.60	-10.36	-298.45	972.77	1,650.25
Daily Average Deviation Value		-49.84	-11.41	-4.62	-17.77	-1.04	-29.85	97.28	165.02
Ratio of Base Share Price (%)		-0.07	-4.09	-1.29	-4.10	-0.48	-4.49	5.04	4.26

Table 14 Deviation between Expected Company Share Price and Actual Company Share Price (cont'd)

Case No.		No. 17	No. 18	No. 19	No. 20	No. 21	No. 22	No. 23	No. 24
Deviation Value from Expected Share Price on Day N after Public Announcement	1	-32.05	0.79	2.29	139.86	-51.21	19.73	-47.68	5.76
	2	73.91	-2.18	0.07			20.11	-79.00	-23.16
	3	63.07	-11.33				40.93	-87.90	-21.53
	4				258.13	12.76	50.03	-78.08	-35.60
	5			1.20	133.50	-5.92		-78.22	
	6	82.38		3.27	93.99	-66.88			
	7	229.58		6.11	190.67	-53.44	31.34		-37.23
	8	135.22		4.44	181.43	-113.69	39.35	-77.91	-36.62
	9	150.47	-12.12	6.88			51.39	-85.61	-65.41
	10	151.63					46.62	-109.34	-72.58
	11		-10.93		346.28	-110.36	56.68	-155.60	-75.98
	12			2.06	400.19	-212.85		-185.87	
	13	156.54		1.79	382.90	-272.57			
	14	155.99	-14.18	2.90	577.18	-297.59	26.13		-88.80
	Total	1,166.75	-49.96	31.02	2,704.13	-1,171.76	382.31	-985.20	-451.14
Daily Average Deviation Value		116.67	-8.33	3.10	270.41	-117.18	38.23	-98.52	-45.11
Ratio of Base Share Price (%)		3.17	-7.30	1.82	5.70	-2.58	6.20	-6.04	-3.49

Case No.		No. 25	No. 26	No. 27	No. 28	No. 29	No. 30	No. 31	No. 32
Deviation Value from Expected Share Price on Day N after Public Announcement	1	-9.53	-6.28	-7,469.75	9.79	-68.52	-5.89	-12.38	23.50
	2	-43.51		-2,966.58	16.70	-196.74	-6.26	-27.45	13.68
	3	-59.80		-5,040.26	12.21	-192.61	4.77	-38.10	-7.46
	4		4.26				2.93	-39.02	
	5		-6.26						
	6	-88.52	-1.44	-35,639.65	21.38	-195.01			-34.45
	7	-96.40	13.67	-34,185.67	25.83	-255.35	3.66	-45.19	37.39
	8	-87.71	20.78	-34,899.38	22.13	-137.95	-1.96	-23.29	74.42
	9	-81.99		-22,486.31	20.11	-136.42	-0.56	-2.05	-17.08
	10	-75.85		-16,020.60	9.08	-134.35	1.69	-12.10	19.77
	11		10.30				10.51	-17.34	
	12		17.73						
	13	-86.87	16.31	-9,800.34	4.12	-21.16			45.60
	14	-94.70	-5.81	-14,682.72	-5.42	202.56	4.57	-25.99	54.01
	Total	-724.88	63.25	-183,191.26	135.94	-1,135.53	13.45	-242.90	209.38
Daily Average Deviation Value		-72.49	6.33	-18,319.13	13.59	-113.55	1.34	-24.29	20.94
Ratio of Base Share Price (%)		-5.74	0.55	-3.20	1.54	-2.79	0.21	-2.38	0.40

Table 14 Deviation between Expected Company Share Price and Actual Company Share Price (cont'd)

Case No.		No. 33	No. 34	No. 35	No. 36	No. 37	No. 38	No. 39	No. 40
Deviation Value from Expected Share Price on Day N after Public Announcement	1	-27.77	-15.90	-0.39	-49.23	-5.23	10.62	-24.54	1,129.45
	2	-22.65	-28.92	-1.23	-59.75	-8.47	5.61	-39.20	1,265.77
	3	-36.69	-32.13	2.43	-55.24			-32.17	
	4			4.08	-40.37			-52.06	-3,437.02
	5			6.03		-6.88	1.96	-40.83	
	6	-29.30	-65.90			-6.73	7.55		
	7	-14.33	-83.89		-68.85	3.02	10.33		-5,774.38
	8	-13.30	-143.76	4.31	-78.47	29.41	2.42		-13,965.50
	9	-15.75	-118.26	2.88	-42.44	21.55	19.65	-75.65	-9,420.64
	10	-1.96	-143.27	2.49	-28.08			-89.91	-13,113.41
	11			1.14	-20.20				-11,101.18
	12			-0.95				-69.27	
	13	-22.77	-140.38			17.58	1.74		
	14	-37.32	-132.16			32.82	7.23		-11,545.36
	Total	-221.85	-904.57	20.79	-442.63	77.08	67.09	-423.64	-65,962.27
Daily Average Deviation Value		-22.18	-90.46	2.08	-49.18	8.56	7.45	-52.95	-7,329.14
Ratio of Base Share Price (%)		-1.16	-1.58	0.56	-1.95	3.81	1.17	-4.30	-3.55

Case No.		No. 41	No. 42	No. 43	No. 44	No. 45	No. 46	No. 47	No. 48
Deviation Value from Expected Share Price on Day N after Public Announcement	1	-119.51	-10.14	12.62	192.24	46.61	1,615.02	10.76	-10.39
	2	-58.20	-25.38				812.51	-5,778.34	-13.33
	3	-58.79	-3.33				-1,651.52		-13.46
	4			10.81	135.12	-104.81	-1,560.31		
	5			6.72	-146.21	-35.57			
	6	-125.65	-14.75	5.57	-278.49	-71.23		-6,840.29	-9.49
	7	-126.75	-14.94	6.81	-349.97	-80.63		-7,606.05	-5.05
	8	-208.39	-15.88	0.02	-286.82	-108.82	-3,992.05	-98.09	-4.81
	9	-183.04	-31.22				-4,890.74	968.19	2.40
	10	-170.42	-37.77				-3,076.00		-2.41
	11						-5,182.31		
	12			4.93	-258.07	-78.01		4,665.67	
	13			5.17	-304.57	-116.00		-2,328.45	1.69
	14	-186.84	-46.03	0.65	-307.31	-70.31	-5,880.65	8,023.89	1.94
	Total	-1,237.60	-199.45	53.30	-1,604.10	-618.77	-23,806.05	-8,982.69	-52.90
Daily Average Deviation Value		-137.51	-22.16	5.92	-178.23	-68.75	-2,645.12	-998.08	-5.29
Ratio of Base Share Price (%)		-2.53	-2.36	1.36	-2.73	-1.84	-1.39	-0.22	-0.83

Table 14 Deviation between Expected Company Share Price and Actual Company Share Price (cont'd)

Case No.		No. 49	No. 50	No. 51	No. 52	No. 53	No. 54	No. 55	No. 56
Deviation Value from Expected Share Price on Day N after Public Announcement	1	3,979.82	17.19	2.17	-1.69	-2.96	-11.87		-12.03
	2		23.34	-4.21	-3.41	-1.82			
	3		22.65	2.02				329.90	
	4	10,794.05			0.55	-6.68	-10.21	-7,875.70	-6.04
	5	8,131.38			-4.50	-8.35	-13.93	4,417.49	
	6	7,714.37	37.14	6.48			-6.41	5,492.29	-4.12
	7	6,081.51	13.83	3.42			-13.98	1,474.45	-5.44
	8	8,891.31	15.91		0.88	-4.87	-9.00		-2.30
	9		8.05	2.11	-1.78	-5.27			
	10		34.09	-1.46	-3.31	-7.23		5,385.65	
	11	22,193.16			0.32	-7.53	-9.37		-3.09
	12	17,567.80			-4.76	-8.02		-2,588.28	2.61
	13	24,652.09	34.70	2.62			-2.51	-4,777.45	9.03
	14	21,079.72	33.64	-0.63			1.09	5,049.65	4.14
	Total	131,085.21	240.53	12.53	-17.70	-52.74	-76.17	6,908.00	-17.23
Daily Average Deviation Value		13,108.52	24.05	1.39	-1.97	-5.86	-8.46	767.56	-1.91
Ratio of Base Share Price (%)		2.49	2.21	0.33	-1.03	-1.72	-1.55	0.16	-0.37

Case No.		No. 57	No. 58	No. 59	No. 60	No. 61	No. 62	No. 63	No. 64
Deviation Value from Expected Share Price on Day N after Public Announcement	1	-1.58		23.72	6.16	-2,452.08	39.81	61.45	11.53
	2			30.11	9.80				7.91
	3		-2,845.30	33.94	1.14				
	4	4.38	-1,501.06	-117.13		-3,118.51	1.69	-23.09	
	5		-3,610.57			-66.79	-21.13	-59.68	10.83
	6	0.59	-3,640.33		3.22	-6,225.69	15.62	-97.99	11.87
	7	0.64	-7,970.32	-129.64	-3.69	2,456.59	32.15	-123.61	13.28
	8	-0.09		-125.95	-9.12	2,381.31	-1.04	-82.58	
	9			-203.27	-5.34				12.57
	10		-9,018.38	-186.82	-11.04				
	11	-5.00	-411.54	-248.82		868.08	-32.18	-103.82	
	12	-1.32	6,707.75			6,976.97	4.47	-123.90	12.71
	13	1.60	11,713.47		-24.17	11,070.63	-29.56	-171.31	11.05
	14	-1.84	3,556.76	-281.91	-29.43	8,567.07	-18.54		11.88
	Total	-2.62	-7,019.53	-1,205.76	-62.48	20,457.58	-8.71	-724.53	103.63
Daily Average Deviation Value		-0.29	-701.95	-120.58	-6.25	2,045.76	-0.87	-80.50	11.51
Ratio of Base Share Price (%)		-0.08	-0.15	-2.74	-0.88	0.40	-0.02	-1.64	2.47

Table 14 Deviation between Expected Company Share Price and Actual Company Share Price (cont'd)

Case No.		No. 65	No. 66	No. 67	No. 68
Deviation Value from Expected Share Price on Day N after Public Announcement	1	-18.79	-6.33	8.19	5.29
	2	-35.84		15.30	12.70
	3			20.91	24.63
	4	-39.01	-11.19	18.38	
	5		-13.03		
	6		-7.07		
	7	-29.74	-7.99		
	8	-28.96			13.99
	9	-25.36		16.96	2.53
	10	-32.41		25.11	4.43
	11			23.33	3.77
	12		-8.32	20.17	
	13		-2.64		
	14		-1.15		
	Total	-210.12	-57.72	148.36	67.33
Daily Average Deviation Value		-30.02	-7.22	18.54	9.62
Ratio of Base Share Price (%)		-3.24	-1.41	11.55	1.51

Table 15 Deviation between Expected Group Company Share Price and Actual Group Company Share Price (Influence on Group Share Prices)

Case No.		G-01	G-02	G-03	G-04	G-05	G-06	G-07	G-08
Deviation Value fromExpected Share Price on Day N after Public Announcement	1	3.99	47,845.26	47.10	-24.25	-8.97	-15.59	4.06	
	2	-5.19	28,597.55	58.94		-59.14	-101.34		-9,732.49
	3					-51.92	-30.49		-16,974.08
	4				-4.76			2.65	-34,945.58
	5	-7.13	54,641.06	63.92	-11.43			-0.61	-27,513.52
	6	-9.03	53,005.87	137.70	-8.60	-40.01	-160.32	-2.86	-14,968.91
	7	-9.98	57,773.74	202.56	-25.05	-24.76	-75.21	-3.29	
	8	-5.77	59,036.28	193.32	-47.22	-29.09	-52.78	-0.51	
	9	-9.63	49,833.05	193.99		-32.42	-84.06		5,869.26
	10					-37.67	-195.68		16,802.72
	11				-25.38			-7.16	18,880.61
	12	-3.42	48,605.84	151.82	-43.97			-9.85	2,389.48
	13	-1.08	66,766.02	150.65	-26.43	-41.53	-144.20	-13.84	3,396.25
	14	-9.09	95,922.65	184.42	1.32	-41.54	-108.00	-13.57	
	Total	-56.32	562,027.32	1,384.42	-215.79	-367.05	-967.67	-44.97	-56,796.26
Daily Average Deviation Value		-5.63	56,202.73	138.44	-21.58	-36.71	-96.77	-4.50	-5,679.63
Ratio of Base Share Price (%)		-1.63	8.48	12.03	-1.14	-26.99	-2.14	-2.35	-1.23

Case No.		G-09	G-10	G-11	G-12	G-13	G-14	G-15	G-16
Deviation Value fromExpected Share Price on Day N after Public Announcement	1		43.62	239.65	-8,455.26	2.11	-94.81	-134.71	-19.59
	2		29.92	214.34	-3,605.27	-1.29	-136.04		
	3	0.27	28.01	264.24	-4,764.37	2.79	-128.35		
	4	-13.97	55.82				-126.25		
	5	-5.83					-92.11	-155.50	-19.46
	6	47.37		201.97	-9,672.36	2.24		-163.37	-18.58
	7	58.55	81.47	430.91	-9,640.40	-0.63			
	8		24.06	505.55	-14,434.20	-0.31	-128.21	-160.94	-17.72
	9		49.47	388.82	-26,993.47	-0.58	-114.73		
	10	65.13	34.45	487.96	-23,206.72	0.82	-111.43		
	11	34.15	15.31				-133.95	-226.20	-11.87
	12	41.98					-121.83	-190.41	-9.40
	13	27.71		391.55	-15,136.65	-1.90		-216.51	5.94
	14	32.06	-16.99	682.32	-10,926.28	-4.57		-169.47	11.96
	Total	287.43	345.15	3,807.30	-126,834.98	-1.31	-1,187.71	-1,417.12	-78.72
Daily Average Deviation Value		28.74	34.51	380.73	-12,683.50	-0.13	-118.77	-177.14	-9.84
Ratio of Base Share Price (%)		3.26	1.85	2.17	-2.84	-0.07	-2.75	-11.97	-1.11

Table 15 Deviation between Expected Group Company Share Price and Actual Group Company Share Price (Influence on Group Share Prices) (cont'd)

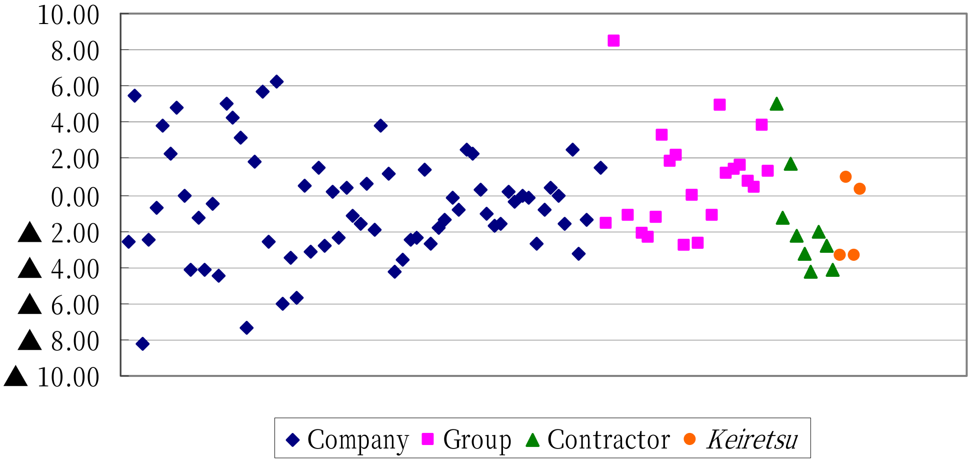
Case No.		G-17	G-18	G-19	G-20	G-21	G-22	G-23	G-24
Deviation Value from Expected Share Price on Day N after Public Announcement	1	10,550.42	633.69	8.40	-0.06	-10.00	-1,985.97	6,102.84	1.47
	2		-1,245.43		-1.88	-2.44	-7,159.79	18,460.90	15.26
	3		2,329.41	6.87		-20.23		22,281.35	1.68
	4	6,038.76	14,183.02	1.87				24,697.07	
	5	12,855.60			2.73		-2,511.76		
	6	13,079.41			3.80	-0.12	-2,775.03		
	7	33,523.38	10,983.34	8.24	3.30	-1.83	-3,478.21		
	8	40,812.52	2,899.66	3.06	5.10	7.98	3,858.75		24.74
	9		4,961.17	4.76	3.09	4.59	-1,555.26	22,457.35	-1.35
	10		5,132.26	3.17		18.10		18,888.29	42.20
	11	36,584.31	3,331.56	4.68				19,547.40	57.23
	12	29,492.95			4.90		3,399.00	13,071.32	
	13	26,192.77				23.62	14,461.59		
	14	17,471.40		16.69	5.53	39.96	15,981.90		
	Total	226,601.51	43,208.68	57.75	26.50	59.63	18,235.22	145,506.51	141.23
Daily Average Deviation Value		22,660.15	4,800.96	6.42	2.94	5.96	1,823.52	18,188.31	20.18
Ratio of Base Share Price (%)		4.93	1.15	1.38	1.64	0.72	0.40	3.80	1.32

Table 16 Deviation between Expected Contractor Share Price and Actual Contractor Share Price

Case No.		E-01	E-02	E-03	E-04	E-05	E-06	E-07	E-08	E-09
Deviation Value from Expected Share Price on Day N after Public Announcement	1	9.48	3.13	-0.60	-3.89	-1,384.98	-22.38			
	2		-13.37		-6.76	4,934.87	-26.65			
	3					-2,259.17	-23.95	-17.57	-9.64	-15.07
	4	17.42		31.78				-13.59	-11.47	-129.14
	5	26.35	-8.16	20.79	-14.82			-20.63	-17.74	-206.42
	6	39.23	-19.49	42.95	-9.34	-23,892.78	-25.35	-16.81	-17.29	-234.51
	7	33.76	-21.28	39.35	-31.14	-24,596.49	-24.93	-4.43	-13.27	-267.82
	8	33.18	-10.15	39.78	-39.10	-30,097.30	-27.86			
	9		-21.94		-42.47	-31,792.05	-23.62			
	10					-25,068.96	-22.84		-10.65	-119.84
	11	27.38		42.23				-24.28	-17.43	-144.41
	12	25.33	-19.46	20.26	-27.27			-33.46	-18.58	-111.10
	13	47.97	-0.44	-11.46	-47.18	-21,976.25	-22.38		-27.04	-156.44
	14	40.34	-4.85	-13.61	-58.53	-27,959.24	-34.81	-37.71	-44.24	-198.39
	Total	300.44	-116.00	211.46	-280.49	-184,092.35	-254.77	-168.49	-187.36	-1,583.15
Daily Average Deviation Value		30.04	-11.60	21.15	-28.05	-18,409.23	-25.48	-21.06	-18.74	-158.31
Ratio of Base Share Price (%)		5.04	-1.31	1.70	-2.27	-3.29	-4.20	-1.99	-2.87	-4.15

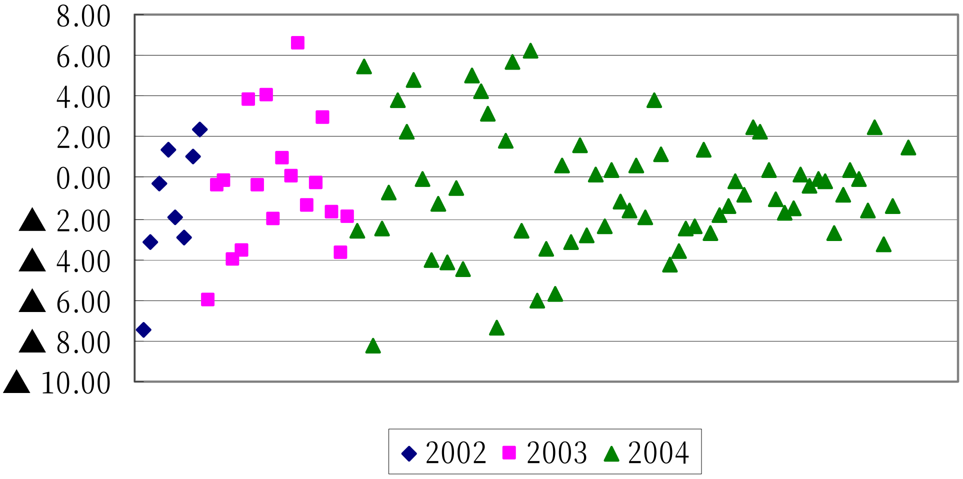
Table 17 Deviation between Expected *Keiretsu* Company Share Price and Actual Share Price (Influence on Share Price of Company at the top of the *Keiretsu*)

Case No.		K-01	K-02	K-03	K-04
Deviation Value from Expected Share Price on Day N after Public Announcement	1		4.88	1,702.74	5.06
	2		-64.61	3,908.01	6.21
	3		-39.10	414.21	
	4	-50.44			
	5	-56.41			
	6	-46.12	-46.60	-6,414.13	
	7	-38.56	24.07	-9,638.92	25.71
	8		58.68	-10,682.45	4.78
	9		148.94	-12,863.30	24.94
	10	-61.08	98.21	-17,793.14	6.33
	11	-62.97			
	12	-64.05			
	13	-50.80	107.81	-21,433.86	
	14	-55.92	77.14	-20,008.21	17.65
	Total	-486.35	369.42	-92,809.06	90.69
Daily Average Deviation Value		-54.04	36.94	-9,280.91	12.96
Ratio of Base Share Price (%)		-3.37	0.89	-3.32	0.32



* Outlying base share price values outside the range between -10.00 and +10.00 removed.

Fig. 21 Scatter Graph of Base Share Price Ratios (2004)



* Outlying base share price values outside the range between -10.00 and +10.00 removed.

Fig. 22 Scatter Graph of Base Share Price Ratios (Interannual Fluctuations)

7.3 Summary of 2004 Results and Preview of Next Year

For our 2004 report, we continued the practice of focusing on the relationship between Information Disclosure Incidents and share prices. However, we were unable to obtain results pointing to uniform share price decreases. While Information Disclosure Incidents are certainly a scandal for the offending company, and it is reasonable that such would lead to damaged corporate value, perhaps our results indicate that other, more severe forms of corporate scandal have already been occurring, and that the market is not in a situation easily influenced by incidents of Information Disclosure.

To this point, the Working Group has approached the influence of Personal Information Disclosure Incidents on corporate value from the direction of share price fluctuation. However, there are actually a great number of factors that move share prices, and perhaps what is required is a more refined model to describe the degree to which Information Disclosure actually influences share prices. On the other hand, perhaps there is also a need to investigate a substitute methodology.

8 Conclusion

As mentioned at the beginning of this report, the Personal Information Protection Act was to become fully enforced during early 2005, influencing the focus on media reports of Personal Information Disclosure Incidents in 2004. At the same time, the occurrence of several large-scale Disclosure Incidents during 2004 resulted a significant increase in the number of incidents and in the number of related victims in comparison to 2003.

We plan to conduct another survey for 2005. We fully expect that statistical interannual fluctuations will present clear evidence of what changes have come about due to the influence of the full enforcement of the Personal Information Protection Act in Japan.

It is our sincere desire that corporations, public institutions, government agencies and others utilize the Projected Compensation for Damages Calculation Model and Influence on Share Price presented herein as a valuable asset in assessing the risks facing their organizations.

9 Contact Information

Please address any comments about this report, or any inquires about quoting this report in other published works, to the contact information below:

■Contact
JNSA Office
E-mail: sec@jnsa.org
TEL: 03-5633-6061