2006

Information Security Incident Survey Report

[Abstract]

Ver. 1.0

NPO Japan Network Security Association
March 31, 2008

Table of Contents

JNSA Seisaku Committee Security Incident Investigation Working Group

Working Group Leader

Eiji Yamada	dit Co., Ltd.

Members Contributing to this Report

Hisamichi Otani	NTT DATA Corporation
Hironori Omizo	JMC Co.,Ltd.
Tomoharu Sato	BroadBand Security, Inc.
Yasuhiko Sato	Software Research Associates, Inc.
Masayuki Hiroguchi	RICOH HUMAN CREATES Co., Ltd.
Shiro Maruyama	LAC:　Little eArth Corporation Co., Ltd.
Tadashi Yamamoto	SOMPO JAPAN RISK MANAGEMENT,INC.
Tetsuya Yoshida	Kanematsu Electronics Ltd.
Naoyoshi Yasuda	dit Co., Ltd.

Copyrights and Attributions

1 Introduction

This report represents the fifth survey and analysis of personal information leakage incidents/accidents ("incidents") conducted by the JNSA Security Incident Investigation Working Group ("Working Group"). As with the prior year's report, the fiscal 2006 report utilizes the same survey methodology established in the fiscal 2003 report.

As announced in the prior year's report, we analyzed judicial decisions related to legal reparations associated with personal information leaks, considering a revision of the resulting "Projected Compensation for Damages Calculation Model" developed by the Working Group. However, the results of the current model compared to actual legal reparations determined in court were quite similar, leading us to make the decision to continue to use the 2003 "Projected Compensation for Damages Calculation Model" without revision for our 2006 report.

A total of 993 information leakage incidents were publicly reported during fiscal 2006, practically the same number of incidents reported during the prior year (1,032). In contrast, 22 million individuals were affected by information leakage incidents during 2006, representing a two-and-one-half fold increase compared to the 8.8 million individuals affected during the prior year. In other words, while the number of publicly reported incidents (the number of information leakage incidents) remained on par with the prior year, the number of individuals affected grew significantly.

In this report, we provide statistics and analyses of personal information leakage incidents that occurred during 2006, including an analysis of the causes behind these significant trends.

2 Objectives

This report summarizes the results of an independent evaluation of a survey and accompanying analysis related to Personal Information Leakage Incidents publicly reported in Japan between January 1, 2006 and December 31, 2006.

Personal information is regarded as a private asset, the protection of which is mandated by the Personal Information Protection Act. Accordingly, the leakage of personal information is a risk of which corporate management 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.”

3 Analysis of Personal Information Security Leakage Incidents Occurring during 2006

3.1 Subject of Survey and Survey Methodology

Personal Information Leakage Incidents publicly reported via news media and the Internet news services occurring between January 1, 2006 and December 31, 2006. Working Group members collected public reports from the Internet and other news sources, compiling data related to Personal Information Leakage Incidents, including the type of business or organization involved, the number of individuals affected, the causes of information leakage, the route of information leakage, and after-incident response.

Since the Working Group only had access to public sources of information, the scope of these evaluations are based on what could be gleaned from the articles. Information was collected manually by Working Group members, and readers should not infer that 100% of all such reports have been included in the scope of the study.

3.2 Compilation and Analysis of Survey Results

3.2.1 Number of Leakage Incidents and Ratio by Industry Type

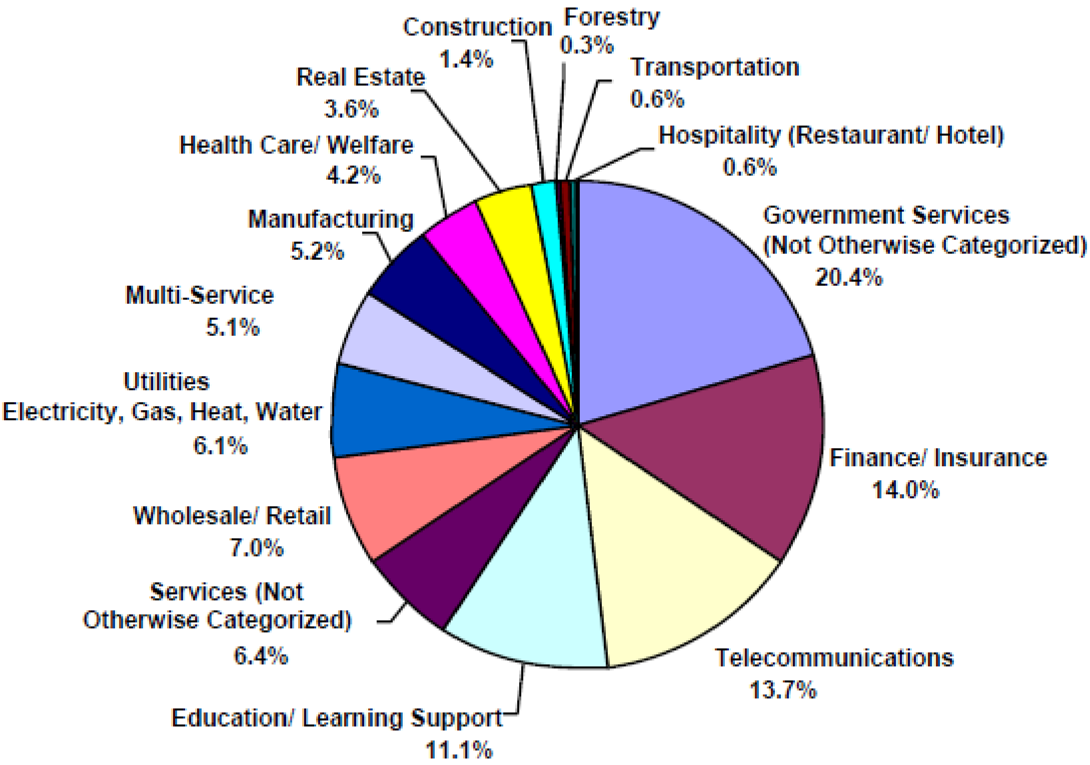


Figure 1: Ratio of Incidents by Industry Type [Incidents]

The top industries experiencing Personal Information Leakage Incidents during 2006 were, in order, “Government Services (20%),” “Finance/ Insurance (14%),” “Telecommunications (14%),” and “Education/ Learning Support (11%).”

The “Government Services” and “Finance/ Insurance” industries have continued to be the No. 1 and No. 2 industries for information leakage incidents between 2004 and 2006. According to Figure 16, during 2004, “Government Services” and “Finance/ Insurance” accounted for 35% and 18% of incidents, respectively. The respective numbers for 2005 were 14% and 29%, and 20% and 14% for 2006.

Government administration plays an important part in both industries, and even minor incidents are reported, which could be the reason for these industries continuing to represent the greatest share of incidents.

Other types of industries also report numerous incidents of personal information leakage incidents, which indicates an establishing pattern of willingness to publicly report incidents, regardless of industry.

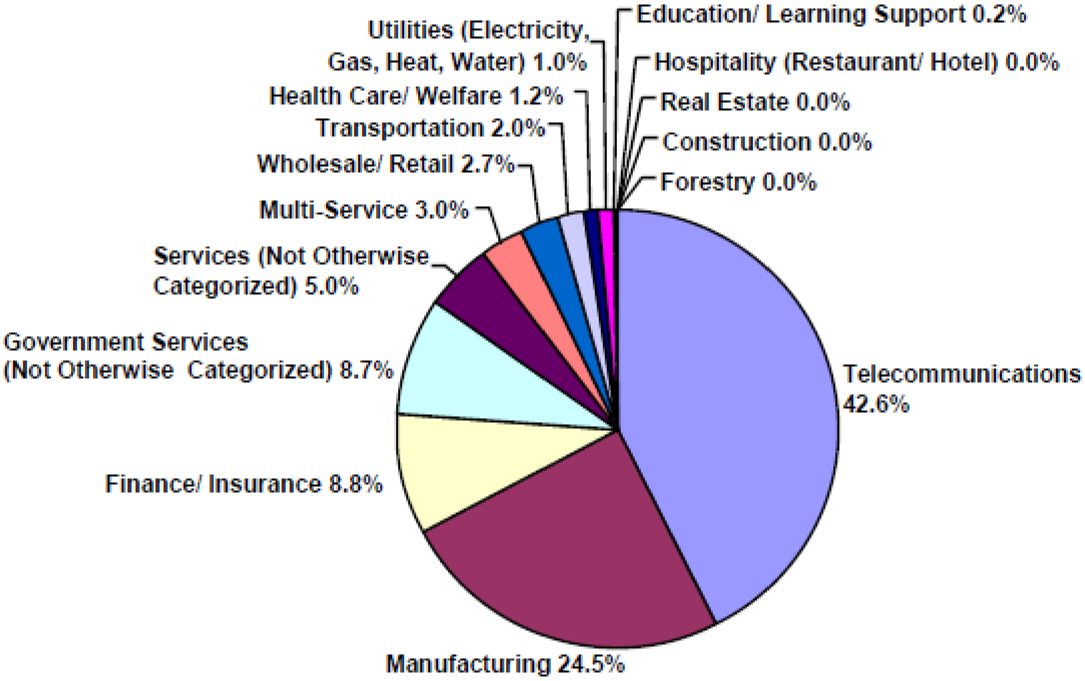


Figure 2: Ratio of Incidents by Industry Type [Victims]

By industry, the ratio of the number of victims of personal information leakage incidents was highest in the “Telecommunications” sector (42%), followed by “Manufacturing” (25%), “Finance/ Insurance” (9%), and “Government Services” (9%). The ratio of victims in the “Telecommunications” and “Manufacturing” industries was extremely high compared to the others. This is not to say that the number of personal information leakage incidents were particularly high among these two industries, but rather that several personal information leakage incidents occurring in these industries happened to be of considerably large scale.

These days, large-scale personal information leakage incidents can occur in any industry in which companies collect/ use large amounts of personal information.

3.2.2 Causes of Information Leakage

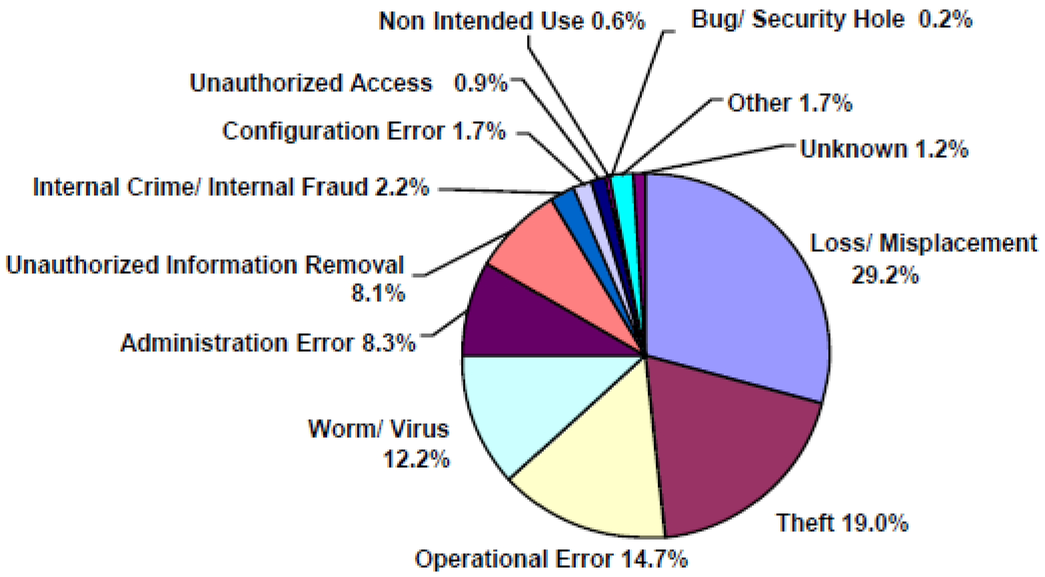


Figure 3: Ratio of Leaks by Cause [Incidents]

Table 1: Personal Information Leakage Causes by Category

No.	Factor	Category	%	Causes
1	Technological	Human Error	24.7%	Configuration error, operational error, administration error
2	Technological	Insufficient Measures	13.3%	Bug/ security hole, virus, unauthorized/ illegal access
3	Non-technological	Human Error	29.8%	Loss/ misplacement, Non-intended use
4	Non-technological	Crime	29.3%	Internal crime/ internal fraud, unauthorized information removal, theft
5	Other	Other, unknown	2.9%	Other, unknown

“Loss/ misplacement” and “Theft” once again accounted for the majority of personal information leakage during 2006.

Meanwhile, personal information leakage due to “Worms/ Viruses” increased from 1.1% in 2005 to 12.9% in 2006. The increase in 2006 was due to the numerous occurrences of information leakage incidents caused by viruses spread through Winny, Share and other file-sharing programs. According to the analysis results in Appendix 3 “Commentary on Winny Incidents” of our report, approximately 40% of the cases involved rules violations such as removing work-related information without permission and copying work-related information to personal computers. Other cases involved a lack of any rules and improper management by organizations. Cases of “Unauthorized Information Removal” increased from 3.3% in 2005 to 5.4% in 2006; however, many cases here also involved file-sharing software.

Cases of “Internal Crime/ Internal Fraud” accounted for 1.4% of personal information leakage incidents during 2005, growing to 2.2% during 2006. This trend hints toward individuals perpetrating internal crimes/ internal fraud with the understanding that personal information is a valuable information asset.

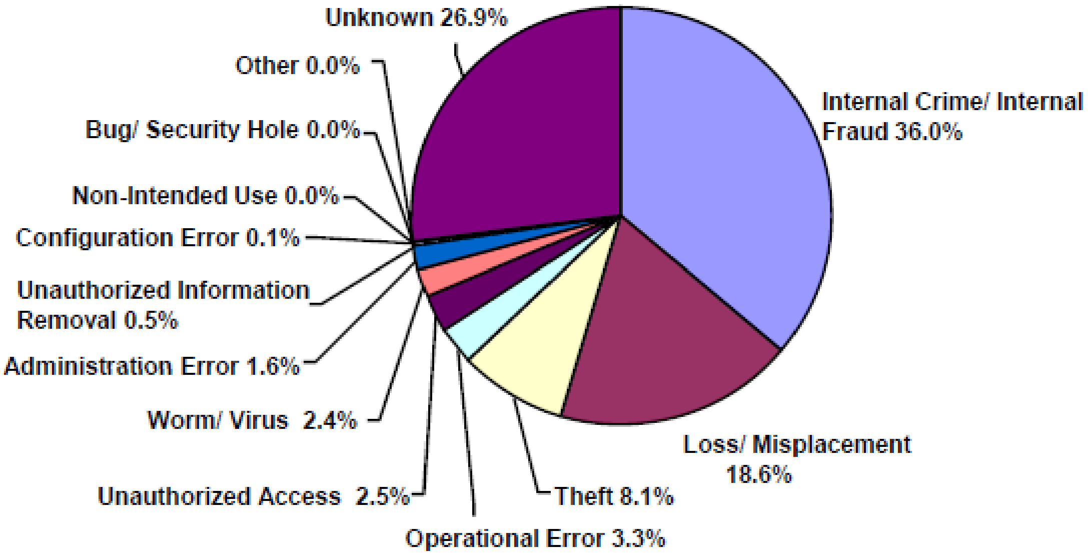


Figure 4: Ratio of Leaks by Cause [Victims]

Three separate personal information leakage incidents during 2006 involved more than 4 million victims. “Unknown” in Figure 4 above represents such a large ratio due to the fact that the route of leakage for one of these major cases was not known. While a definite assertion cannot be made, it seems likely that, given the number of victims involved (5.4 million), the route of information leakage in this case was due to “Internal Crime/ Internal Fraud.” Including this incident in the “Internal Crime/ Internal Fraud” category would increase the ratio of that category to 60%.

The remaining two incidents also involved the major numbers of victims after the incident involved the most numbers of victims (4.52 million) during2004. In both cases, people inside the organization were involved, and the cases developed from ones of personal information leakage into extortion.

Table 2: Causes of Information Leakage

Causes of Information Leakage	No. of Victims (%)		No. of Incidents (%)		Number of Victims per Incident
Internal Crime/ Internal Fraud	8,001,089	(36.0%)	18	(1.9%)	444,504.9
Unauthorized/ Illegal Access	561,832	(2.5%)	9	(0.9%)	62,425.8
Loss/ Misplacement	4,131,764	(18.6%)	280	(29.5%)	14,756.3
Theft	1,799,486	(8.1%)	176	(18.5%)	10,224.4
Operational Error	737,251	(3.3%)	144	(15.2%)	5,119.8
Worms/ Viruses	531,210	(2.4%)	115	(12.1%)	4,619.2
Administration Error	352,646	(1.6%)	78	(8.2%)	4,521.1
Bug/ Security Hole	4,068	(0.0%)	2	(0.2%)	2,034.0
Non-Intended Use	8,816	(0.0%)	6	(0.6%)	1,469.3
Unauthorized Information Removal	110,839	(0.5%)	80	(8.4%)	1,385.5
Configuration Error	13,176	(0.1%)	17	(1.8%)	775.1
Other	716	(0.0%)	14	(1.5%)	51.1
Unknown	5,983,683	(26.9%)	10	(1.1%)	598,368.3
Total	22,236,576	(100%)	949(*)	(100%)	23,431.6

* The population parameter for average number of victims per incident for 2006 was 949 (having removed 44 incidents for which the number of victims was unknown).

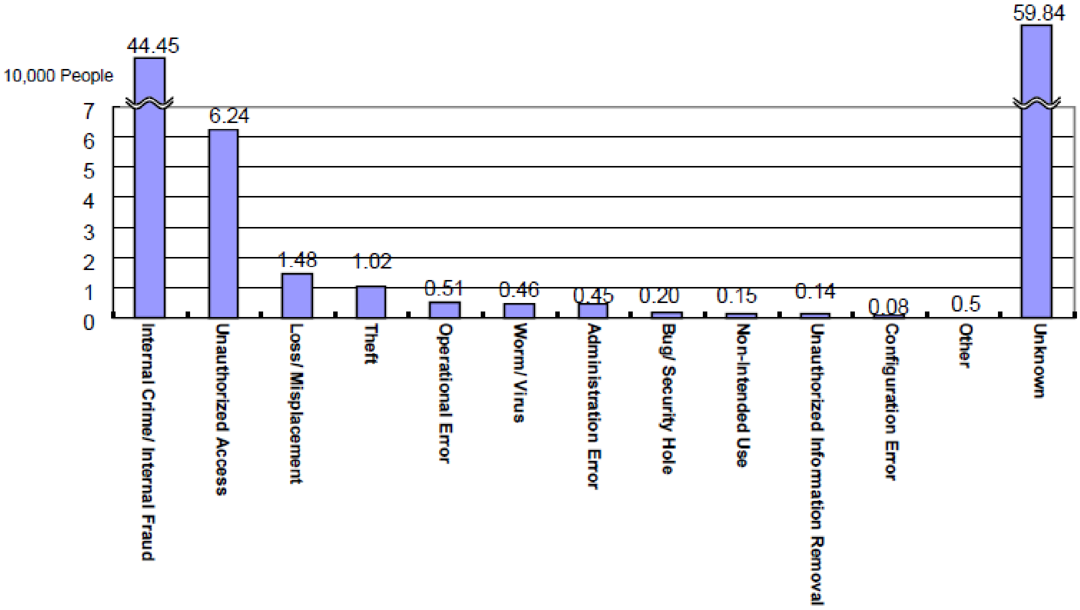


Figure 5: No. of Victims per Incident by Leak Cause

From the graph in Figure 5 showing the average number of victims by leakage cause, we see a high figure for the average number of victims per incident stemming from “Internal Crime/ Internal Fraud.” The graph concerning causes of information leakage incidents in Figure 3 indicates that “Internal Crime/ Internal Fraud” accounted for only 2.2% of all incidents. As stated in last year’s report, this shows that incidents of personal information leakage resulting from personnel within an organization (persons in authority) occur infrequently, but carry a high impact.

As touched on in comments related to Figure 4, including the single major incident categorized as “Unknown” into the “Internal Crime/ Internal Fraud” category would increase the average number of victims under that category.

Given the analysis above, companies adopting centralized measures for the control of personal information in order to reduce the number of incidents and save management costs must also consider the risks regarding the large impact that even a single incident can have when perpetrated in a premeditated fashion by an organizational insider.

3.2.3 Leakage Route

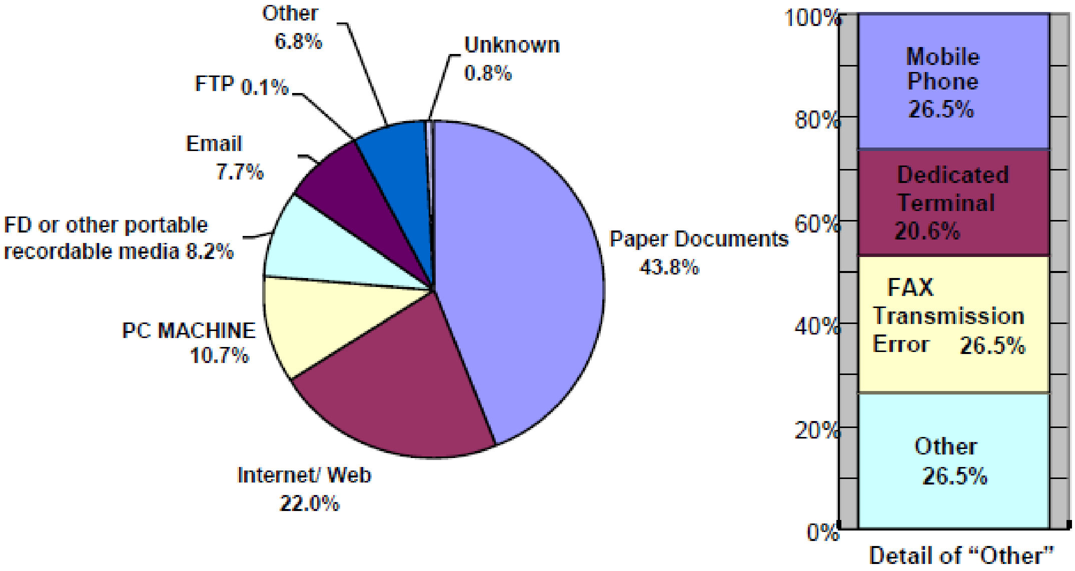


Figure 6: Ratio of Leakage Route (Media) [Incidents]

Figure 6 shows the ratio (%) of personal information leakage incidents by leakage route. The ratio of incidents represented by “Paper Documents” was quite large, representing the number one route as with 2005. A notable characteristic of 2006 was that the ratio of “Internet/ Web” (No. 4 in 2005) increased three times, becoming No. 2 for 2006. As mentioned earlier, this is due to the influence of information leakage incidents exploiting Winny and other file-sharing software—incidents receiving wide coverage in Japan’s mass media. In the past, the combined ratio of routes related digital data (Internet/ Web, PC MACHINE, FD or other portable recordable media, Email, FTP) and the ratio of “Paper Documents” were nearly the same. In 2006, the influence of incidents through file-sharing software resulted in a combined ratio of routes related to digital data in excess of 50%, surpassing “Paper Documents.”

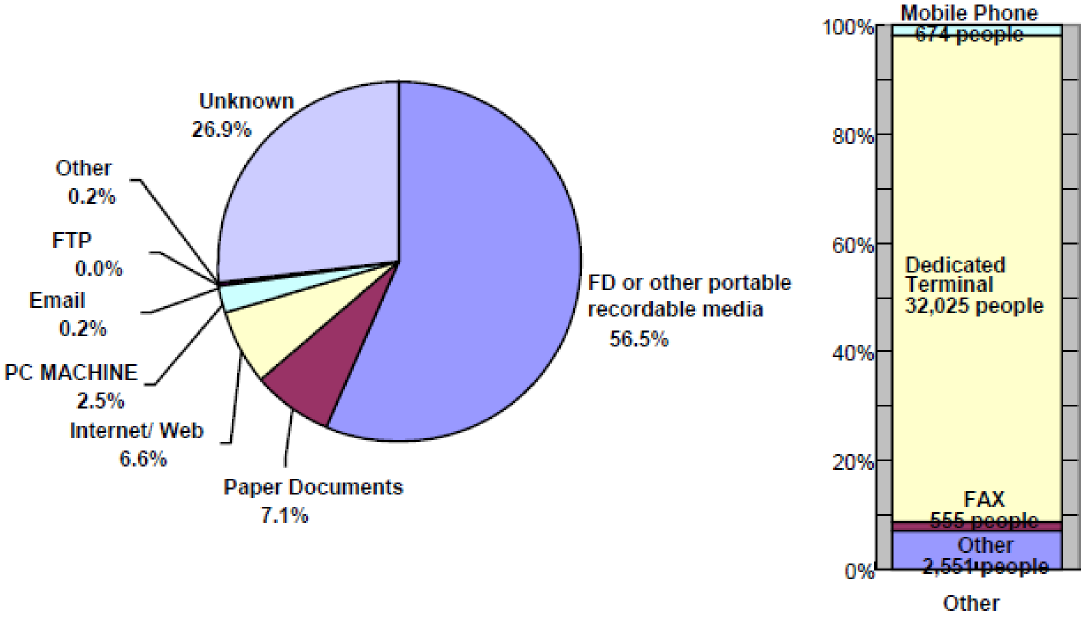


Figure 7: Ratio of Leakage Route (Media) [Victims]

Figure 7 shows the ratio of information leakage victims (%) according to leakage route. As explained under Figure 6, the ratio of incidents categorized under “Paper Documents” was particularly high; however, when looking at the ratio by number of victims, the ratio under the “Paper Documents” category decreases, while “FD or other portable recordable media” increases to 56.5%. USB flash memory and other similar devices are included in this “FD or other portable recordable media.” While paper documents have certain limitations in terms of the volume that can be contained and the amount that can be physically carried, portable recordable media continues to advance in terms of size and data capacity. Accordingly, information leakage through “FD or other portable recordable media” involves major numbers of victims per incident.

In addition, the ratio of the average number of victims per incident under the category of “PC MACHINE” declines from 13,000 in 2005 to 5,000 for 2006. We believe this decrease is due to the adoption of anti-leakage measures, including the central management of personal information on servers rather than on PCs, and restrictions placed on the amount of information allowed to be used at one time. However, considering the stipulations of the Personal Information Protection Act, one must still consider 5,000 victims a significant number.

3.2.4 Number of Victims

A total of 22,236,576 individuals were victims of personal information leakage incidents during 2006. In other words, one out of every six Japanese citizens fell victim to personal information leakage during the year 2006. The average number of victims per incident was 23,432. (Using a population parameter of 949 after excluding 44 incidents with unknown numbers of victims.)

Figure 8 shows a distribution of the number of victims per incident.

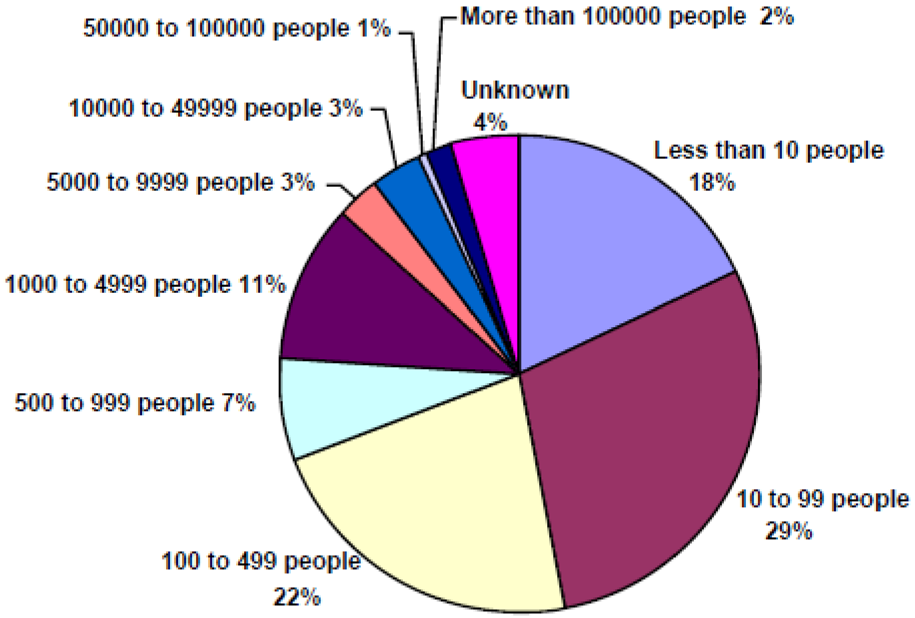


Figure 8: No. of Victims [Incidents]

According to Figure 8, 47% of all incidents involved less than 100 victims. A total of 42% of incidents during 2005 involved less than 100 victims, demonstrating an apparent continued active willingness on behalf of organizations to report even small-scale incidents.

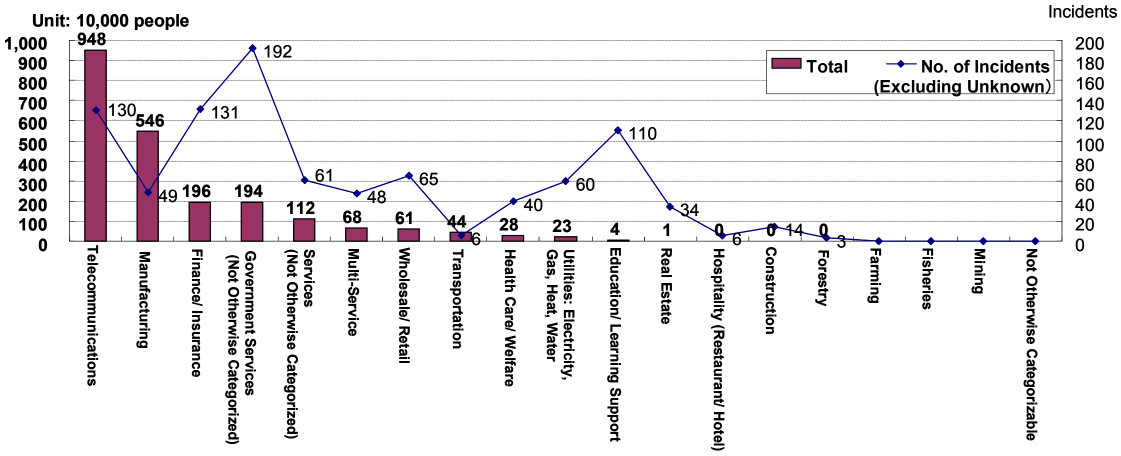


Figure 9: No. of Victims and Incidents by Industry Type

Figure 9 charts the relationship between number of victims per incident and number of incidents according to industry type. Looking at this figure, we see that even though the numbers of incidents in the “Telecommunications” and “Manufacturing” industries were few, the number of victims per incident increased significantly. As discussed in “3.2.1 Number of Leakage Incidents and Ratio by Industry Type,” the occurrence of several specific large-scale information leakage incidents was largely responsible for this trend.

On the other hand, despite the fact that the number of leakage incidents in the “Finance/ Insurance,” “Government Services,” and “Education/ Learning Support” categories were comparatively numerous, there was a comparatively few total number of victims. This supports our conclusion that these industries actively report even small-scale incidents, and that large-scale incidents did not occur during the year.

3.2.5 Leaked Information Details

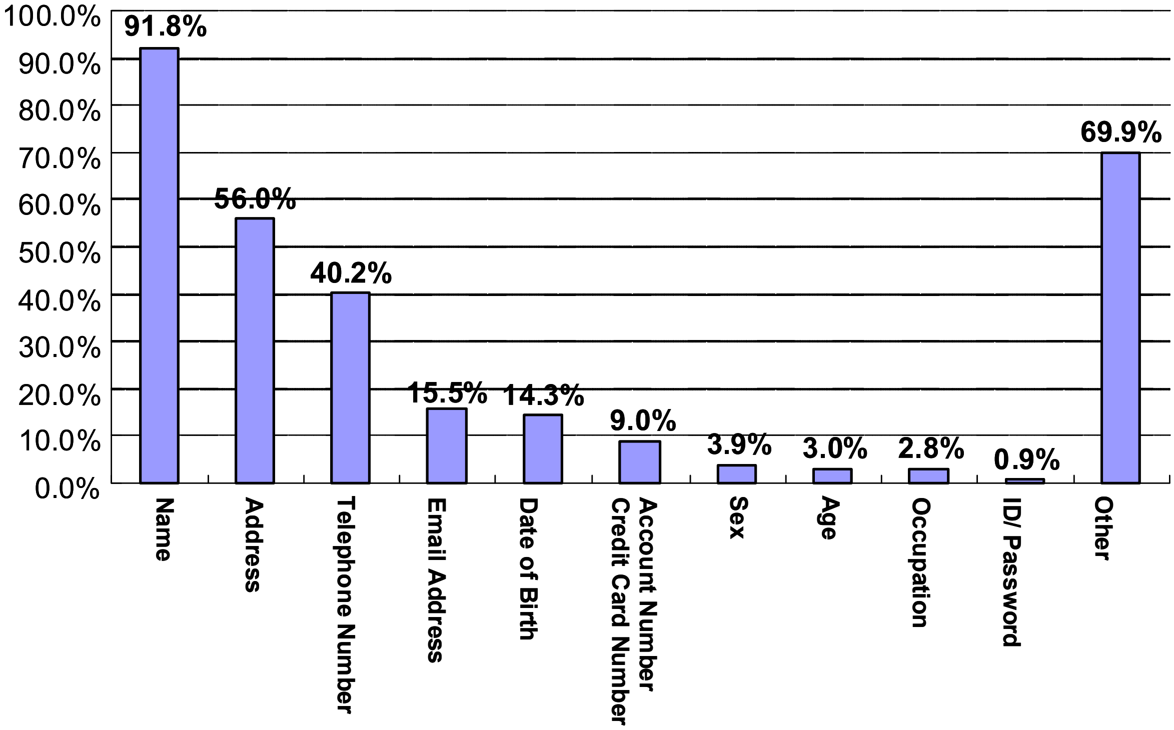


Figure 10: Frequency of Leaked Information

The frequency of "Name" as leaked information was 91.8%--quite high compared to other categories of information. This is most likely due to the fact that "Name" identifies a specific person, and has therefore been included in the definition of personal information. Following "Name," basic information like "Address" and "Telephone Number" had the highest frequency at 56.0% and 40.2%, respectively.

Compared to 2005, the frequency decreased for "Credit Card Number" and "Account Number." We believe this is due to the decrease in reports of Computer Output Microfiche (COM) loss from banks during 2006.

While various information is included in the category "Other," depending on the use of the personal information concerned, comparatively high information types include member number, customer number, company name, employer, test results, grade, invoice amount, annual income, account balance, etc.

3.2.6 Interannual Changes in Survey Results

The following shows a comparison of survey results for the five years between 2002 and 2006.

(1) Number of Personal Information Leakage Incidents and Number of Victims

Table 3: No. of Personal Information Leakage Incidents

2002	2003	2004	2005	2006
62	57	366	1,032	993

Table 3 shows the trend in number of personal information leakage incidents for five years.

Between 2004 and 2005, the number of incidents grew approximately 2.8 times. However, between 2005 and 2006 the number of incidents experienced a slight decrease at approximately 0.96 times. While the number of incidents decreased, considering the fact that on average 2.7 incidents occurred every day, one can see the difficulty in implementing effective countermeasures. Prior to 2003 only the largest of leakage incidents to be publicly reported, skewing the information collected for study. This must be kept in mind when conducting interannual comparisons with the years 2004 and later.

Table 4: Total Number of Victims

2002	2003	2004	2005	2006
418,716	1,554,592	10,435,061	8,814,735	22,236,576

Table 4 shows the trends for total victims of personal information leakage incidents over a five-year period. Between 2005 and 2006, the number of total victims jumps approximately 2.5 times. This is due to the fact that there were several personal information leakage incidents involving 4 million victims or more during 2006. The number of victims exposed to personal information leakage during 2006 was more than twice the total for 2004, the previous high water mark.

Table 5: Average Number of Victims per Incident

2002	2003	2004	2005	2006
7,613	30,482	31,057	8,922	23,432

* Using a population parameter of 949 incidents after excluding 44 incidents with unknown numbers of victims.

Table 6 shows the change in average number of victims per incident. While there were several incidents that involved significant numbers of victims during 2006, the average number of victims per incident was only the third highest over the five-year period in question.

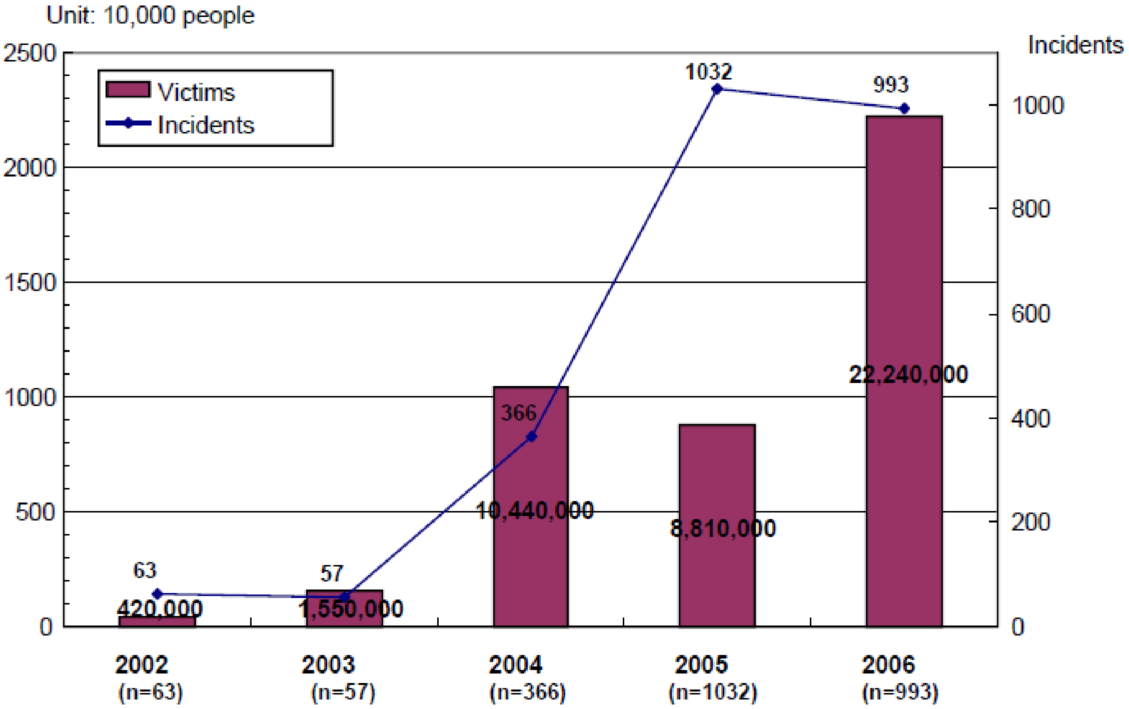


Figure 11: Interannual Changes in No. of Victims and No. of Incidents (2002 to 2006)

Figure 11 shows the interannual changes in number of victims and number of incidents over the five-year period between 2002 and 2006. The number of incidents (publicly reported) dramatically increased during 2005 after the complete enforcement of the Personal Information Protection Act, and continued at about the same level during 2006. As we have already stated, we believe that it is now common practice among all industry types to report even smaller incidents.

Compared to prior years, the number of reported victims increased dramatically during 2006. During 2006, large-scale personal information leakage incidents affecting more than 4 million individuals occurred three times (total of approximately 13.4 million victims), pushing up the total of victims for the year.

(2) Number of Victims per Incident

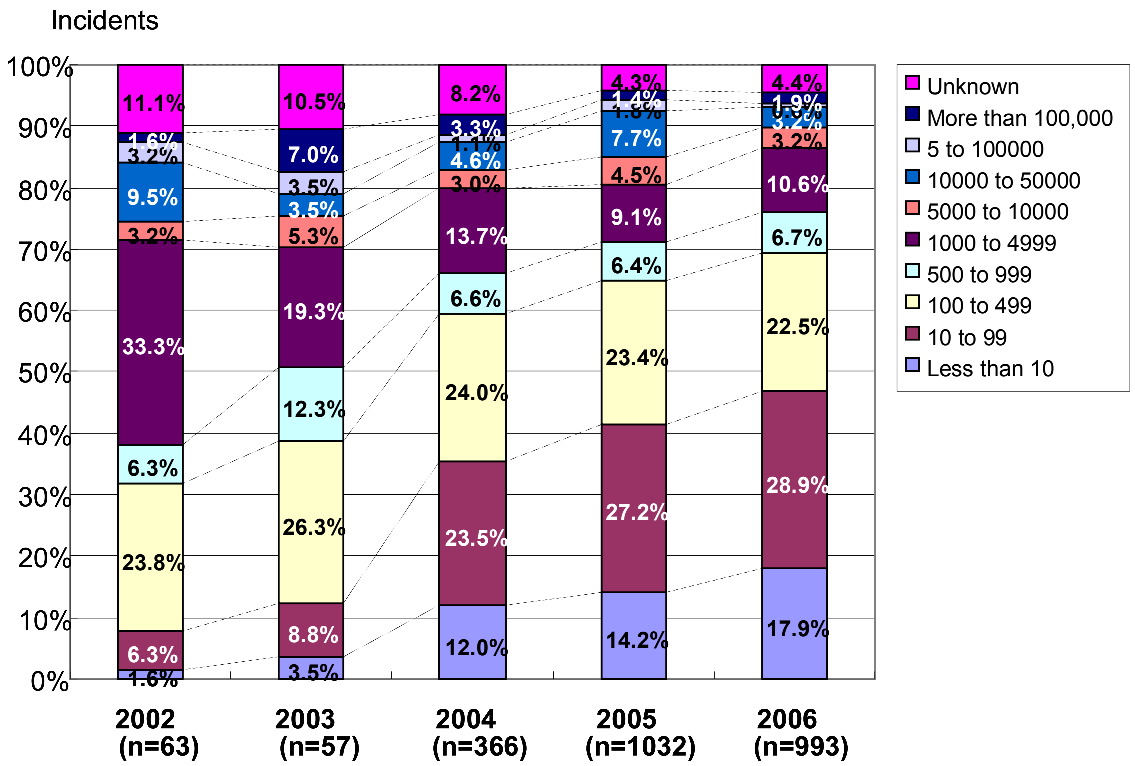


Figure 12: Interannual Changes in Victims per Incident (2002 to 2006)

Figure 12 is a chart showing the interannual changes in victims by category. From this chart, we can see several identifiable trends. First, we see that the number of publicly reported small-scale incidents grows year by year. From what can be discerned from consulting engagements at organizations where incidents have occurred, it is difficult to conclude that the number of small-scale incidents has increased. Rather, one should rather conclude that this trend stems from the fact that even small-scale incidents are now being publicly reported. We can interpret this graph as reflecting the fact that greater importance is being placed on compliance, rather than simply on personal information leakage, leading organizations to publicly disclose even smaller incidents.

(3) Causes of Information Leakage

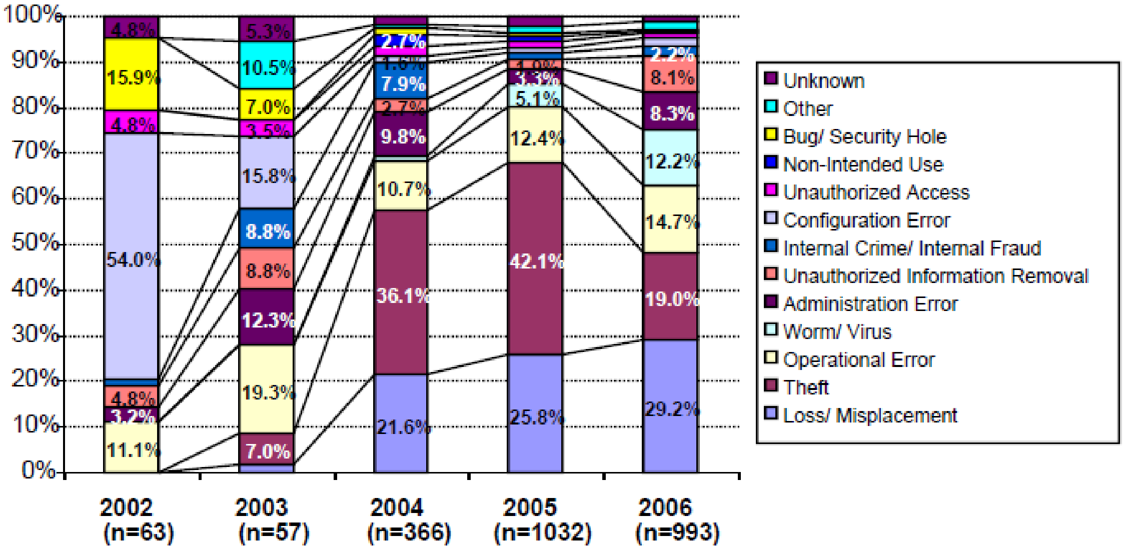


Figure 13: Interannual Changes in Ratios of Leakage Cause (2002 to 2006)

Figure 13 shows the interannual changes in incidents according to cause. While “Loss/ Misplacement” shows an increasing trend year by year, “Theft” decreased by more than 50% compared to 2005. On the other hand, “Worms/ Viruses” doubled. The majority of information leakages due to “Worms/ Viruses” is comprised of the widely reported virus spread via Winny and other file-sharing software that is downloaded to an individual’s PC, and then proceeds to disseminate their personal information over the Internet.

Incidents categorized under “Unauthorized Information Removal” also increased. We believe this increase to be due to express provisions of restrictions placed on information removal in organization rules and security policies when information is physically taken outside a corporation or other organization. More specifically, we believe that existing restrictions and procedures were either unknown or impossible to comply with, and so personal information was physically removed according to improper methods, which led to an information leakage incident. When establishing rules restricting the physical removal of information, organizations must do more than simply set up restrictions and prohibitions, considering the effectiveness of countermeasures and related trade-offs, and revising rules to reflect practicability in consideration of newly introduced risks.

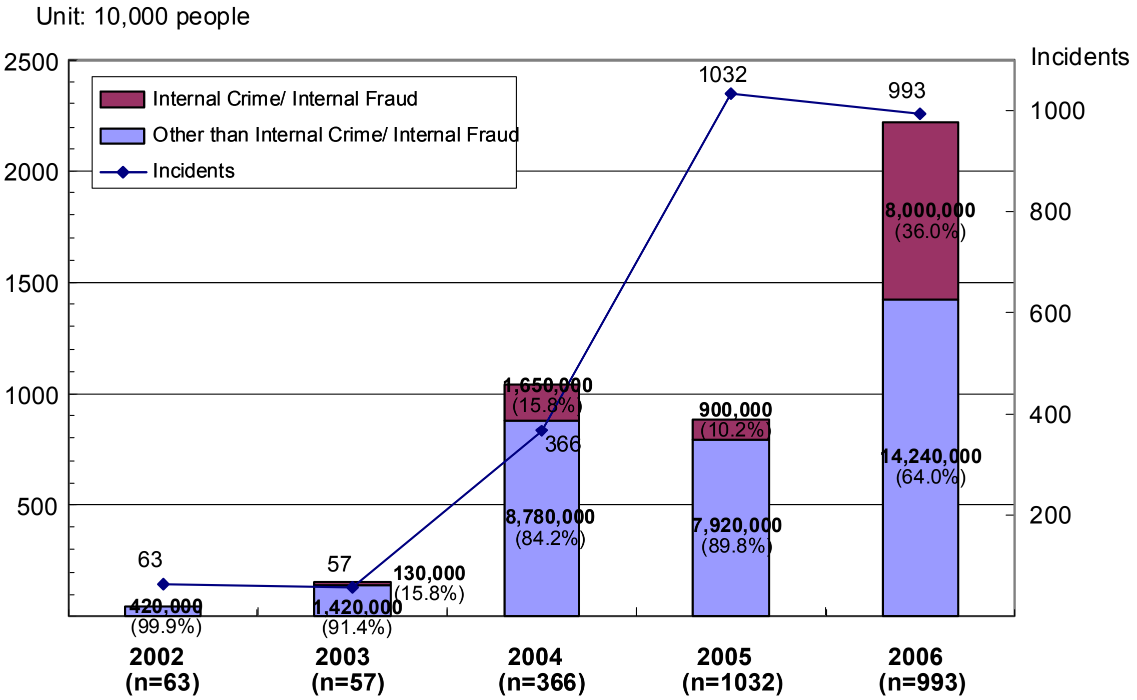


Figure 14: Interannual Changes in Victims due to Internal Crime/ Internal Fraud (2002 to 2006)

Figure 14 shows the number of incident victims stemming from “Internal Crime/ Internal Fraud” compared to the number of victims for other categories combined. While the ratio of victims due to “Internal Crime/ Internal Fraud” was between 10% and 20% for 2004 and 2005, this ratio dramatically increased to 36% during 2006. This is mainly due to the fact that two separate incidents involved more than 4 million victims each (Table 6), rather than an indication that the number of incidents increased as a whole.

Table 6: Causes of Major Personal Information Leakage Incidents during 2006

No	Industry	Number of Victims	Causes of Information Leakage
1	**Manufacturing**	Approx. 5,380,000	Unknown
2	**Telecommunications**	Approx. 4,000,000	Internal Crime/ Internal Fraud
3	**Telecommunications**	Approx. 4,000,000	Internal Crime/ Internal Fraud
4	**Government Services**	Approx. 1,760,000	Loss/ Misplacement
5	**Finance/ Insurance**	Approx. 960,000	Loss/ Misplacement
6	**Services**	Approx. 900,000	Theft

We can surmise that the cause for the increase in the number of victims due to

“Internal Crime/ Internal Fraud” is due to an increase in demand for personal information to be used in crimes, fueled by the development of phishing and fraud techniques using the Internet, combined with a growing recognition in society that bank account, assets and other personal information has value that can be purchased and sold, fostering internal crime. Further, when a corporate or other organization insider decides to commit an illegal act or fraud, the potential for acquiring large volumes of personal data in one stroke is high, resulting in a high likelihood of a large-scale personal information leakage incident.

Incidents occurred at a constant rate for 2004, 2005 and 2006, at 29 incidents, 14 incidents, and 22 incidents, respectively. Given that some cases involved the detection of internal crimes committed prior to the adoption of robust anti-leak measures through the enhancement of monitoring systems subsequent to the full enforcement of the Personal Information Protection Act, it is difficult to conclude from our data that incidents stemming from internal crime will continue to increase after 2006. It is possible that a concentrated number of personal information leakage incidents due to large-scale internal crime merely occurred during 2006 by happenstance.

(4) Leakage Route

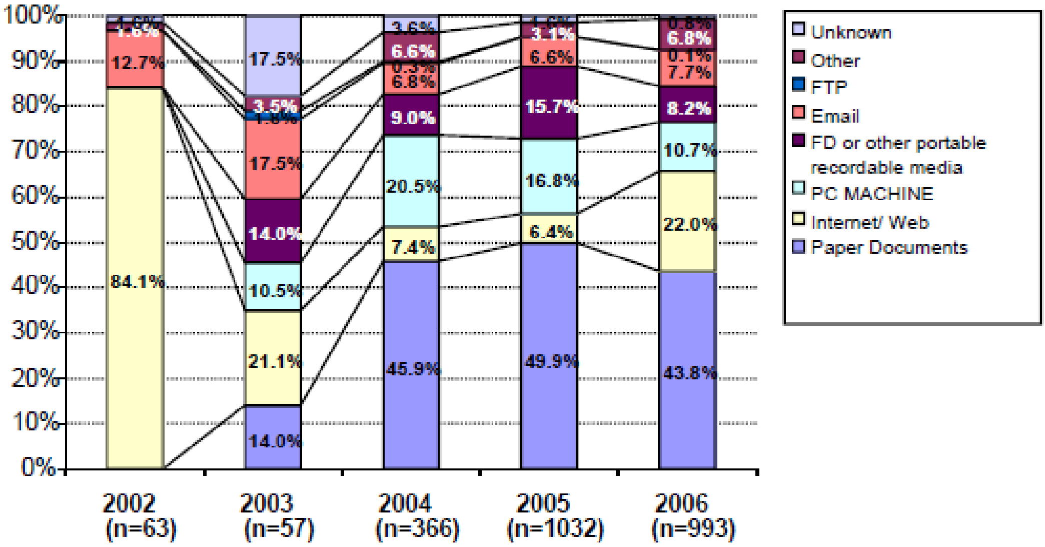


Figure 15: Interannual Changes in Leakage Routes (Incident Ratio) (2002 to 2006)

Figure 15 shows the interannual change in incidents according to leaking route. Having continued to increase for several years, incidents occurring via “Paper Documents” declined slightly during 2006, while “Internet/ Web” increased. As stated in connection with the graph showing causes of information leakage at Figure 13, this is likely a reflection of Winny/ file-sharing software incidents. Compared to 2005, both “PC

MACHINE” and “FD or other portable recordable media” decreased by ratio and number of incidents. Leakage incidents categorized under “PC MACHINE” fell from 173 to 106, while those categorized under “FD or other recordable media” fell from 162 to 81. While the decrease in incidents categorized under “Theft” may be due to an increased awareness during transit, or to restrictions on the use of USB memory devices, we cannot draw a clear cause-and-effect conclusion from the data.

Trends indicate a decrease in the number of incidents; however, we must note that the number of victims per incident categorized under “FD or other portable recordable media” is quite high, and the impact per incident is significant. Organizations should continue to improve their management in this area.

(5) Industry Type

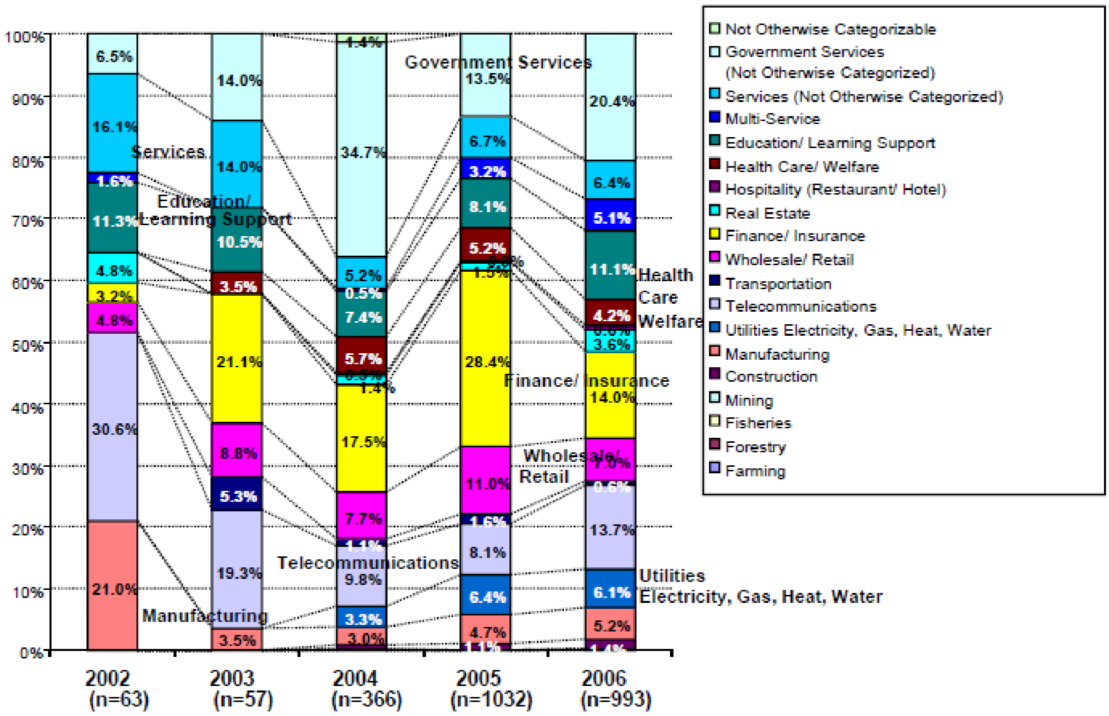


Figure 16: Interannual Changes by Industry Type (Incident Ratios) (2002 to 2006)

Categorized by industry, we can see that incidents in the “Finance/ Insurance” sector (accounting for the largest number of incidents in 2005) decreased by half, while the highest number of incidents was categorized under “Government Services.”

The 50% decrease in the “Finance/ Insurance” industry was due to the fact that many incidents unreported prior to the full enforcement of the Personal Information Protection Act were reported in 2005, making it seem that incidents decreased comparatively during 2006.

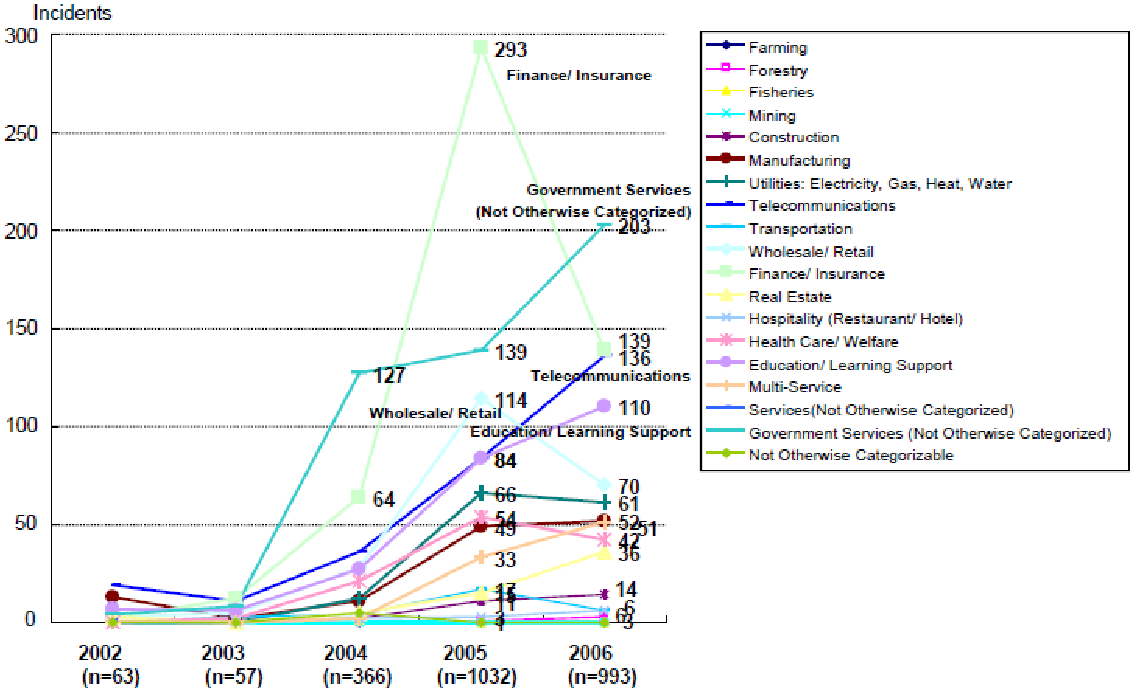


Figure 17: Interannual Changes by Industry Type (Incidents) (2002 to 2006)

Figure 17 shows a line graph of interannual changes in the number of incidents according to industry. From this graph we see that, with the exception of “Finance/ Insurance” there were almost no changes in ranking. In other words, we can infer that the rates of personal information processing and number of people involved is nearly stable in each industry.

For example, we can make the following assumptions about the total amount of personal information processed by each industry:

- Government Services: A multiple of government services for the total population and the total number of households, using the total population of Japan as a reference standard.
- Finance/ Insurance: A number of individual accounts proportionate to the total population, given that one individual may have more than one account.
- Utilities (Electricity, Gas, Heat, Water): Proportionate to the number of households.
- Education/ Learning Support: Use the population of students (population of children) as reference standard.

4 Calculating Projected Compensation for Damages related to Personal Information Leakage

4.1 Objective of Calculating Projected Compensation for Damages

One of the earmarks of the Working Group is proposing a calculation model for legal reparations, and then applying the calculations to actual personal information leakage 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 Leakage Incidents occurring during 2005 in the following sections of this report. 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 will seek 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 Leakage Incident.

4.2 Explanation of the Projected Compensation for Damages Calculation Model

Our calculations for compensation for damages occurring during 2005 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 Leakage Incidents subsequent to the conclusion of our 2003 survey.

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

Here, we will limit ourselves to a simple overview of our model.

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

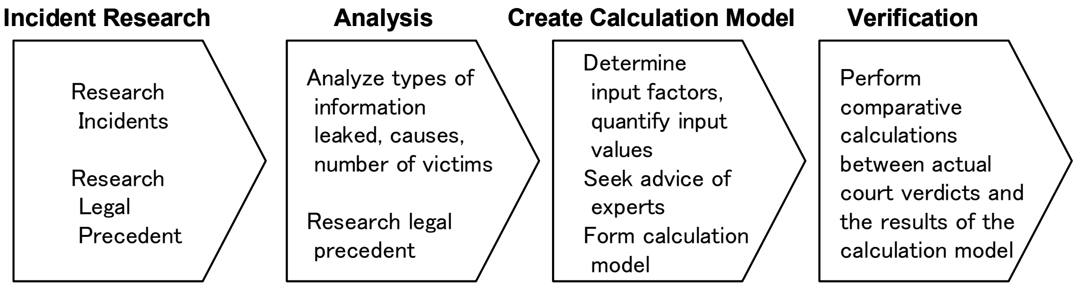

Incident Research
Research Incidents
Research Legal Precedent
Analysis
Analyze types of information leaked, causes, number of victims
Research legal precedent
Create Calculation Model
Determine input factors, quantify input values
Seek advice of experts
Form calculation model
Verification
Perform comparative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

Figure 18: Process behind the Formation of the Projected Compensation for Damages Calculation Model

We developed our calculation model as depicted in Figure 18 above as follows:

1) Preliminary Research

Research and collection of data about publicly announced Personal Information Leakage 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 leakage 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 leaked, the cause of the leakage, the information leakage route, and other factors related to the Personal Information Leakage Incidents. “Appendix 1 Table A” describes the results of our analysis for 2005

3) Calculation Model Creation

Having determined the input factors for our calculation model, we began to develop the model itself. Input factors included the value of the information leaked, 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 leakage case, comparing the results of our calculations with the actual determination of damages ordered by the court. As a result, the level of damages according to our calculations was essentially the same as the actual legally mandated figure.

4.2.2 Explanation of the Calculation Model Input Values

We incorporated the following input values into our calculation model:

- Value of the personal information leaked
- Degree of social responsibility of the organization in question
- Appraisal of 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 leaked 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.

4.2.2.1 Value of Personal Information Leaked

We categorized the effect of Personal Information Leakage 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) (Figure 19). The farther removed from the origin, the greater the respective levels of Economic Loss and Emotional Distress.

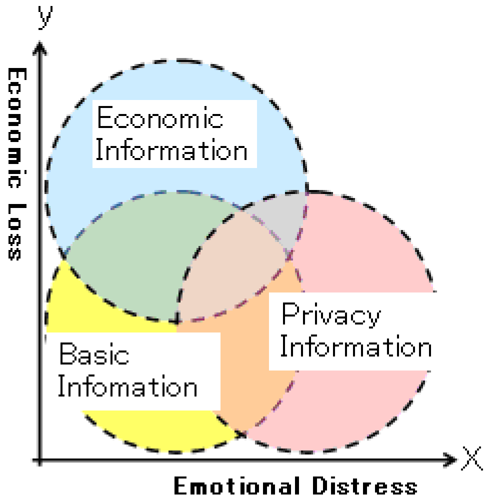
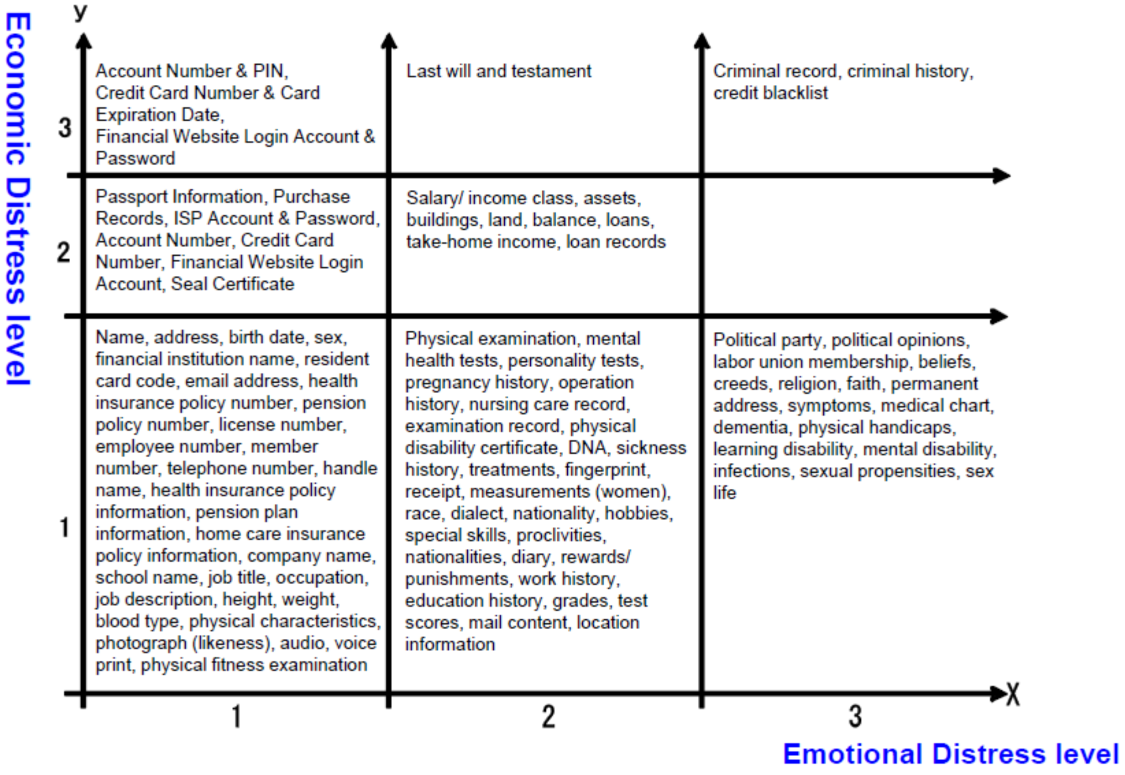


Figure 19: Economic-Privacy Map (EP Map)

On this EP Map, we plotted the types of leaked information noted from our past research and analysis of Information Leakage Incidents. We can then use this EP Map plot locations to derive the type of effect associated with leaked 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 leaked information. This resulted in our EP Map becoming a Simple-EP Map (Figure 20).



	1	2	3
3	Account Number & PIN, Credit Card Number & Card Expiration Date, Financial Website Login Account & Password	Last will and testament	Criminal record, criminal history, credit blacklist
2	Passport Information, Purchase Records, ISP Account & Password, Account Number, Credit Card Number, Financial Website Login Account, Seal Certificate	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

Figure 20: Simple-EP Map

However, we did not simply obtain the value of the leaked information according to the plot location between the X and Y values. Rather, we believe that a slight correction is 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 leaked information:

- **Value of Leaked Personal Information**
  = Value of Basic Information x Degree of Information Sensitivity x 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 leakage consists of several types of information, we use whichever information generates the largest X and largest Y values. For example, if the leakage involves "Name, address, birth date, sex, telephone number, name of sickness, and account number with a PIN 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 with a PIN 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:

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

c. Degree of Ease in Identifying the Individual

Degree of Ease in Identifying the Individual represents the ease with which the leaked Personal Information can be used to specifically identify an individual. For example, if a credit card number is leaked, 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 7 below.

Table 7: 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" are included.	6
Individual may be identified after certain costs are incurred. "Name" or "Address + Telephone Number" are included.	3
Difficult to identify the individual. Other than that described above.	1

4.2.2.2 Degree of Social Responsibility of the Organization in Question

As shown in Table 8, 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 Policies related to 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 8: Degree of Social Responsibility of the Organization Involved in Information Leakage—Determination Standards

Determination Standard		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

4.2.2.3 Appraisal of Post-Incident Response

The appraised value of Post-Incident Response is based on Table 9 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 9: Appraisal of Post-Incident Response—Determination Standards

Determination Standard	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 Leakage 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 leakage 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 leaked information
- Express 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

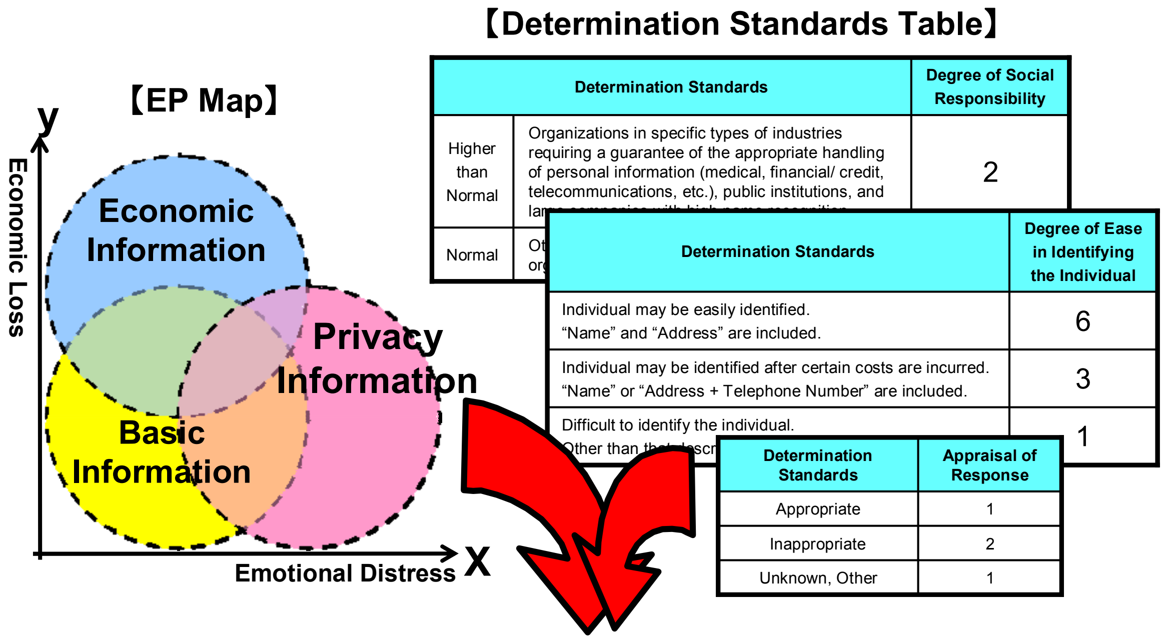
b. Examples of Inappropriate Responses

- Issues were indicated, but not addressed
- Slow response
- Repeated occurrences

- Measures were implemented, but were ineffective
- False reporting

4.2.3 Projected Compensation for Damages Calculation Model

The following represents an overall view of the Calculation Model, integrating the factors discussed in “5.2.2 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 lar	2
Normal	Ot or	

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

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

Projected Compensation for Damages
= Value of Information Leaked x Degree of Social Responsibility of the Organizations
x Appraisal of Post-Incident Response
= (Value of Basic Information x Degree of Sensitivity x Ease in Identifying the Individual)
x Degree of Social Responsibility of the Organization
x Appraisal of Post-Incident Response
= Value of Basic Information [500] x Degree of Information Sensitivity [Max(10x-1 + 5y-1)]
x Ease in Identifying the Individual [6,3,1]
x Degree of Social Responsibility of the Organization [2,1]
x Appraisal of Post-Incident Response [2,1]

Figure 21: JO model

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

4.3 Results of Calculating Projected Compensation for Damages for 2006

The following shows the results of calculating and analyzing projected compensation for damages related to information leakage incidents occurring during 2006.

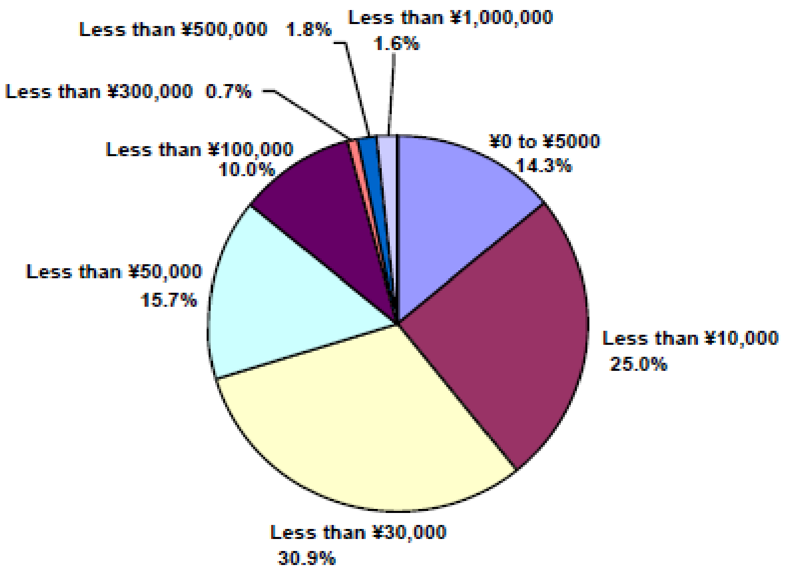


Figure 22: Projected Compensation for Damages per Person

Approximately 40% of all information leakage incidents involved per-person projected compensation for damages of ¥10,000 or less. Per-person damages of ¥50,000 or less accounted for approximately 85% of all incidents.

Projected compensation for damages for personal information equivalent to between ¥10,000 and ¥30,000 was leaked at a higher rate than information equivalent to less than ¥5,000 and between ¥5,000 and ¥10,000.

Legal precedents related to information leakage incidents to date have consisted of compensation of between ¥6,000 and ¥35,000 per person in combined attorney fees and reparations for pain and suffering. From this we can infer that personal information of the type normally handled have a value equivalent to the scope of this projected compensation for damages.

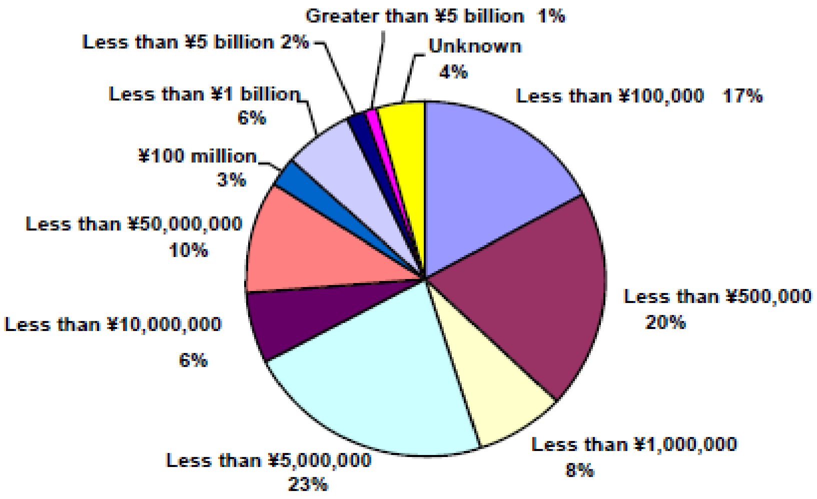


Figure 23: Projected Compensation for Damaged per Incident

Personal information leakage incidents where the per-incident projected compensation for damages was less than ¥1 million accounted for approximately 45% of the total. Because there is no provision for class action suits[1] in Japan, projected compensation for damages will not literally bear out as shown in Figure 23; however, this can be interpreted as the significance of the impact of personal information leakage incidents. Calculating the rate of participation in lawsuits from the court proceedings of Yahoo!BB and TBC results in approximately 0.0004%. Organizations wishing to project the likelihood and compensation for damages of court-directed reparations from our projected compensation for damages model should consider this lawsuit participation rate.

[1] Class Action
A type of civil lawsuit common in the United States wherein a group of individuals participate in the lawsuit simultaneously. Class actions suits are not provided under Japanese law. Under a class action suit, a group representative (rather than each individual) may file suit on behalf of a group, whose rights as consumers are exercised and recognized in court.

4.3.1 EP Distribution by Industry

We determine the importance of information leaked through personal information leakage incidents according to the two measurements of Emotional Distress Level and Economic Loss Level, showing the results of mapping this data in a Simple-EP diagram in Figure 24.

The vast number of incidents involved less-sensitive basic information (Economic Loss Level=1, Emotional Distress Level=1), decreasing in number as sensitivity increases. This trend shows no significant differences compared to 2005. The same can be said for information leakage incidents of up to Emotional/ Economic Loss Level = 2, which accounted for 95.2% (94.1% in 2005).

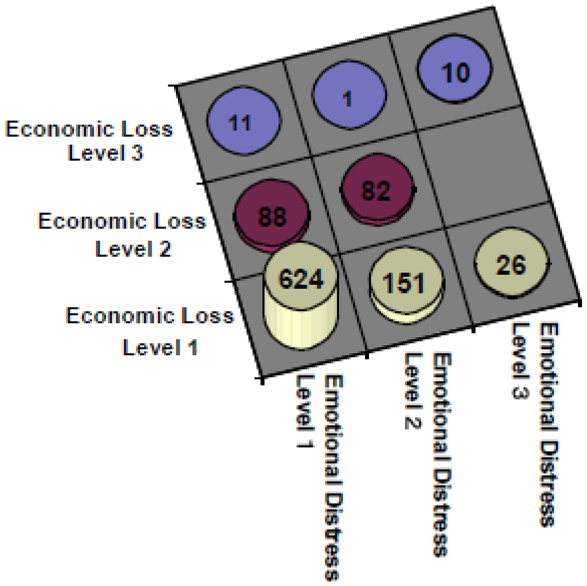


Figure 24: Emotional/ Economic Value and Distribution of Leaked Information

Table 11 is a tabular representation of Figure 24. Analyzing the ratio of incidents to the total number of incidents along each level of sensitivity, shows that the ratio of Emotional/ Economic Loss Level =2 decreased (Emotional Distress Level＝－8.9 points, Economic Loss Level＝－11.7 points) in comparison to 2005. This may indicate improved management of personal information equivalent to Emotional/ Economic Loss Level = 2. However, as seen from Figure 17, the number of incidents in 2006 related to personal information of Economic Loss Level=2 handled by Finance/ Insurance industry businesses significantly decreased compared to 2005. This is due to the fact that unreported incidents prior to the full enforcement of the Personal Information Protection

Act were included in 2005 public reports. Accordingly, readers should note that the changes shown in Table 10 may not be the result of information leakage countermeasures.

Table 10: No. of Incidents by Emotional Distress／Economic Loss Level

	Emotional Distress Level 1	Emotional Distress Level 2	Emotional Distress Level 3	Total	Ratio
Economic Loss Level 3	11	1	10	22	2.2% (-2.2)
Economic Loss Level 2	88	82	—	170	17.1% (-11.7)
Economic Loss Level 1	624	151	26	801	80.7% (+13.8)
Total	723	234	36	993	
Ratio (Vs. PY)	72.8% (+7.9)	23.6% (-8.9)	3.6% (+1.0)		

4.3.2 Interannual Changes in Projected Compensation for Damages

The following table shows a weighting of interannual changes in compensation for damages for the five years between 2002 and 2006.

Table 11: Total Calculated Projected Compensation for Damages

2002	2003	2004	2005	2006
¥15.1 billion	¥28.1 billion	¥439.3 billion	¥700.2 billion	¥457.0 billion

Comparing the projections of compensation for damages between 2004 and 2005 shows an approximately 1.6 times increase; however, 2006 amounts returned almost to the same level as 2004. In any event, we see a continued trend of personal information leakage incidents representing annual cumulative compensation for damages in excess of ¥400 billion.

Table 12: Average Projected Compensation for Damages per Incident*

2002	2003	2004	2005	2006
¥275,320,000	¥550,380,000	¥1,307,300,000	¥708,680,000	¥481,560,000

* The population parameter used for average per-incident compensation for damages for 2006 was 949 incidents (due to the removal of 44 incidents in which the number of victims was unknown).

Table 13: Average Projected Compensation for Damages per Person*

2002	2003	2004	2005	2006
¥16,855	¥89,140	¥105,365	¥46,271	¥36,743

* To derive our average value, we calculated the per-person projected compensation for damages individually for each incident, we calculated the total of the results, and then divided this figure by the number of leakage incidents in order to compensate for any per-incident outliers. Accordingly, this

figure is not the result of dividing the calculated total of projected compensation for damages by the number of victims.

Both the average per-incident projected compensation for damages and average per-person projected compensation for damages both continued to trace a decline from 2004 levels, with the 2006 amount less than that of 2003. Again, this points to the effect of reporting incidents regardless of size. In any event, readers should note that this average of nearly ¥500 million in per-incident compensation for damages continues to be a major risk for companies in terms of business continuity.

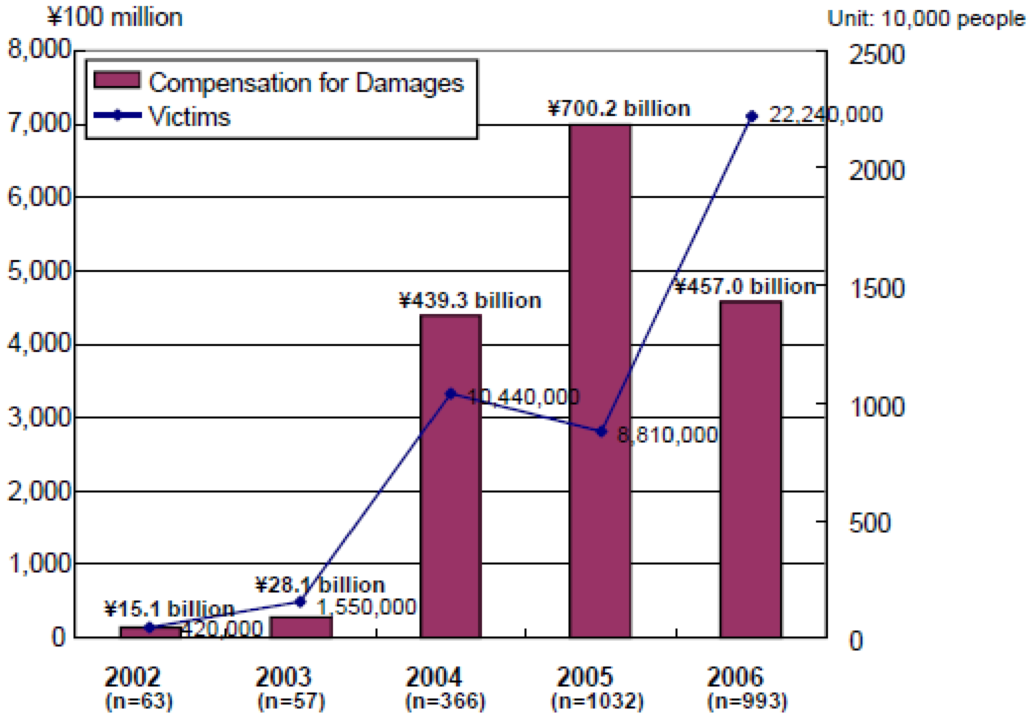


Figure 25: Interannual Changes in Projected Compensation for Damages and Victims (2002 to 2006)

Despite the fact that the total victims of leaks during 2005 were fewer than 2004, the total figure for projected compensation for damages was greater. Meanwhile, the number of incident victims in 2006 was approximately 2.5 times greater than the number for 2005. Despite this fact, the total figure for projected compensation for damages declines to approximately 65% of the prior year. For 2006, the value of the parameters for our Projected Compensation for Damages Calculation Model, namely “Ease in Identifying the Individual,” “Social Responsibility of the Organization, and “Appraisal of Post-Incident Response,” was generally low. We can assume that the combination of the low value of these factors worked to decrease our projected compensation for damages. The 50% year-on-year decrease in the ratio of information leaks from the Finance/ Insurance industry resulted in fewer cases of incidents with high associated Economic Loss points (account number, etc.), which may have influenced this trend as well.

However, we cannot simply conclude that this is the result of the adoption of effective overall personal information protection measures. We still must analyze the circumstances of each incident on a case-by-case basis.

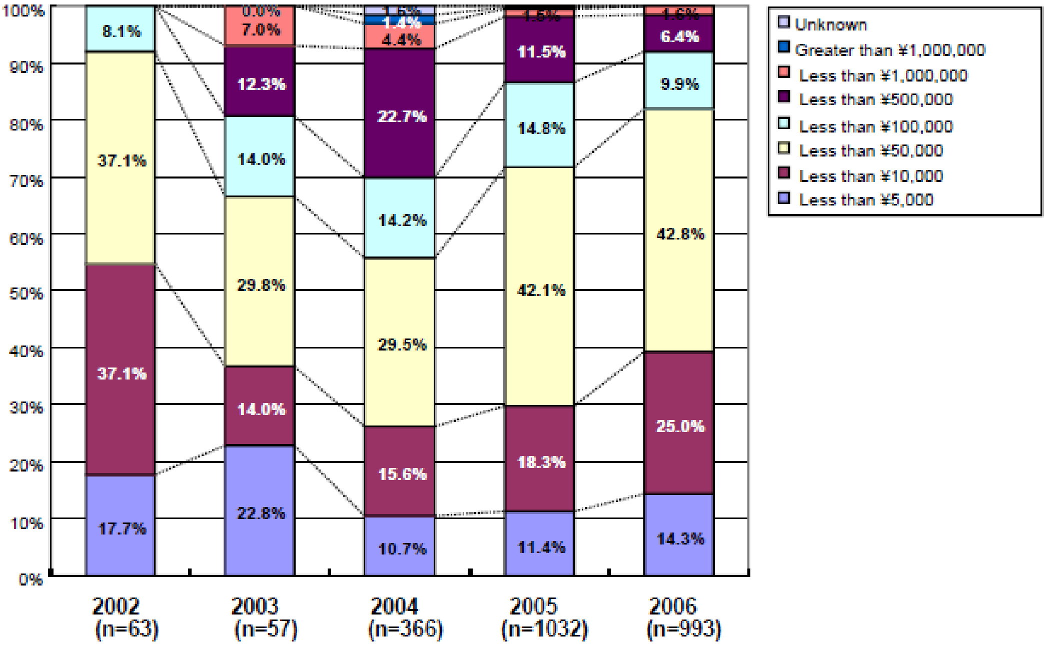


Figure 26: Interannual Changes in Projected Compensation for Damages per Person (Incident Ratios) (2002 to 2006)

Since 2004, where the enforcement of the Personal Information Protection Act allowed us to acquire a more complete incident statistics sample number, the number of incidents in which the per-person projected compensation for damages was ¥50,000 or lower continued to increase, reaching nearly 82% for 2006.

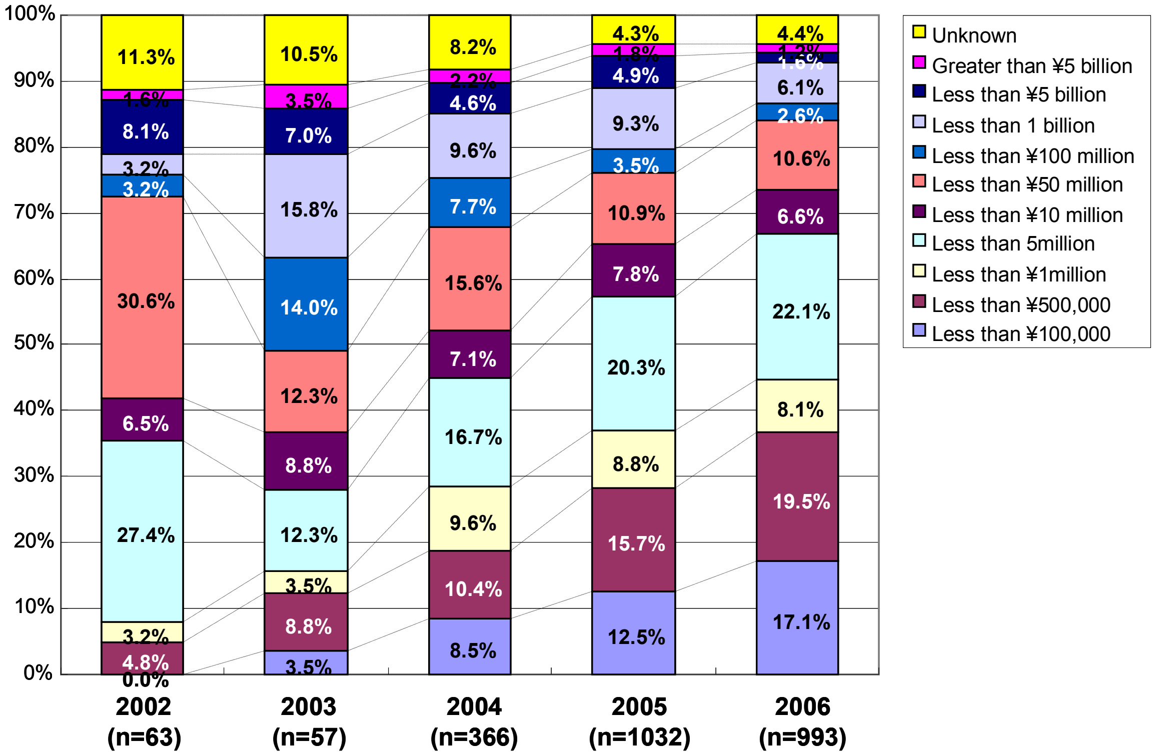


Figure 27: Interannual Changes in Projected Compensation for Damages per Incident (Incident Ratios) (2002 to 2006)

As with the per-person projected compensation for damages, the trend since 2003 has been an increase in low-level (¥990,000 or less) compensation for damages. For 2004, the ratio of incidents involving ¥5 million or less was less than approximately 28% of the total, reaching nearly 67% in 2006.

We believe the underlying reason for this development is the general willingness to publicly report incidents, regardless of the volume of personal information leaked.

5 Conclusion

We have noted a trend toward a willingness in every industry to make a public disclosure after a personal information leakage incident. This supports a conclusion that companies and organizations have recognized the risk of hiding incidents and accidents above and beyond personal information leakage incidents, and points to the establishment of a response pattern beginning with the public disclosure of the incident, followed by public announcements related to research into the underlying cause of the incident, countermeasures in response to this cause, and measures to prevent a recurrence. However, the public announcement of leakage through file-sharing software will, in some cases, increase access numbers, and consequently expand damages. As such, there is still much room for debate as to what standards should be adopted beforehand for publicly disclosing incidents. Organizational leaders would be well advised to consult with government oversight agencies as to whether an incident should be reported.

As in prior years, Loss/ Misplacement and Theft account for the bulk of information leakage incidents, consisting of auto break-in and other very common causes. While people should be able to learn lessons from reading the news, it appears they do not believe that the same thing could happen to them. Loss and theft are not systemic issues, but rather something that could be prevented in the main if people would be slightly more aware during their everyday activities. Organizations should also do their part to promote awareness on an everyday basis, working to increase employee understanding of the issues.

As we stated in last year’s report, incidents involving organizational insiders tend toward greater damages. Accordingly, organizations need to consider implementing stronger measures such as separating authority according to the information user, adopting comprehensive access controls, instituting deterrent and recording through logs and monitoring systems.

Of notable significance with respect to leakage route is that the occurrence of personal information leakage incidents via Paper Documents can occur quite easily, and incidents occurring through FD or other portable recordable media can involve significant volumes of information. As mentioned earlier, large volumes of information can be stored on USB memory devices and other portable recordable media before being physically removed from a location, which is likely to lead to greater damages. Another potential contributing factor is the high frequency of work-related usage of USB memory devices. The risk of significant damages has spurred an increasing number of organizations to restrict the use of USB memory devices; however, no viable alternative exists in some cases, and restricting the use of a USB memory device would hamper the ability of employees to complete work tasks. In such cases, rather than having employees intentionally break rules by using USB memory devices secretly, providing a means to authorize and properly control such devices could potentially reduce associated risks. Fingerprint recognition, data encryption and other safety measures can be implemented in conjunction with portable recordable media to prevent unauthorized individuals from viewing information stored on a particular USB memory device, potentially making these devices a lower-risk alternative to the use of paper documents. While paper documents hold less information than portable recordable media, information recorded thereon is open viewable without the aid of any special apparatus, making information control more difficult compared to portable recordable media. Without instituting parallel restrictions on the physical removal of paper documents, placing restrictions on the use of USB memory devices and other portable recordable media is not likely to be as effective as it otherwise could be.

The increase of leakage incidents due to Winny and other file-sharing software during 2006 resulted in a higher ratio of incidents categorized under the Internet/ Web leakage route. Of the 993 incidents occurring during 2006, 168 occurred through file-sharing software, accounting for approximately 17% of the total. This is a significant increase, considering that this ratio was only 3% in the prior year. Perhaps spurred in part by the sensational coverage of the media outlets, organizations suffering past damages from Winny conducted thorough internal investigations, uncovering incidents not detected before, leading to an increase in reported incidents.

To reduce the risk associated with file-sharing software, organizations must take steps to prevent important information from coming into contact with Winny or other unsecured environments. In other words, organizations must institute serious policies to prevent employees from putting work data on private PCs, prohibit the installation of file-sharing software on work PCs, and strengthen anti-virus measures against the direct cause of such incidents.

6　Contact Information

Please address any comments about this report, or any inquiries about quoting the content of this report in other published works, to the contact address below:

■Contact

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