Survey Report of Information Security Incident 2007

English Edition

Ver. 1.0

NPO Japan Network Security Association

Security Incident Investigation Working Group

March 31, 2009

Table of Contents

1 INTRODUCTION 2

2 OBJECTIVES 2

3 ANALYSIS RESULTS OF PERSONAL INFORMATION LEAKAGE INCIDENTS 3

3.1 SURVEY METHODOLOGY 3
3.2 OVERVIEW 3
3.3 TOP FIVE PERSONAL INFORMATION LEAKAGE INCIDENTS 4
3.4 SINGLE-YEAR ANALYSIS 6
3.5 PROJECTED COMPENSATION FOR DAMAGES CALCULATION RESULTS 14
3.6 SINGLE-YEAR/ CORRELATIVE ANALYSIS 16
3.7 INTERANNUAL ANALYSIS 17
3.8 INTERANNUAL ANALYSIS OF PROJECTED COMPENSATION FOR DAMAGES 23

4 CALCULATING PROJECTED COMPENSATION FOR DAMAGES RELATED TO PERSONAL INFORMATION LEAKAGE 28

4.1 OBJECTIVE OF CALCULATING PROJECTED COMPENSATION FOR DAMAGES 28
4.2 EXPLANATION OF THE PROJECTED COMPENSATION FOR DAMAGES CALCULATION MODEL 28
4.2.1 Process behind the Formation of the Projected Compensation for Damages Calculation Model 29
4.2.2 Explanation of the Calculation Model Input Values 30
4.2.3 Projected Compensation for Damages Calculation Model 36

5 CONCLUSION 37

6 CONTACT INFORMATION 39

7 APPENDIX DEFINITIONS FOR CAUSES OF INFORMATION LEAKAGE 40

JNSA Seisaku Committee Security Incident Investigation Working Group

Working Group Leader

Hisamichi	Ohtani	NTT DATA Corporation

Members Contributing to this Report

Hironori	Omizo	JMC Risk Solutions CO.,LTD
Haruto	Kitano	Oracle Corporation Japan
Tomoharu	Sato	BroadBand Security, Inc.
Yasuhiko	Sato	Microsoft Co., Ltd.
Masayuki	Hiroguchi	RICOH HUMAN CREATES Co., Ltd.
Shiro	Maruyama	LAC: Little eArth Corporation Co., Ltd.
Eiji	Yamada	dit Co., Ltd.
Tadashi	Yamamoto	SOMPO JAPAN RISK MANAGEMENT,INC.
Nobuo	Yoshikawa	FUJITSU LIMITED
Tetsuya	Yoshida	Kanematsu Electronics Ltd.
Naoyoshi	Yasuda	dit Co., Ltd.

1 Introduction

This report represents the sixth survey and analysis of personal information leakage incidents/ accidents ("incidents," hereafter) conducted by the JNSA Security Incident Investigation Working Group ("the Working Group"). As with the prior year's report, the 2007 report utilizes the same survey methodology established in the 2003 report.

Also as with the prior year's report, the Working Group followed the established survey protocol, collecting and analyzing information related to personal information leakage incidents ("incidents") published during 2007 in newspapers, on Internet news sites, and via other sources.

This report summarizes the results of our analysis of projected compensation for damages, using certain information (type of business/ organization involved in the incident, number of victims, cause of information leakage , route of information leakage, etc.) and our JO Model (JNSA Damage Operation Model for Individual Information Leak), based on the survey data. Herein, we will report our aggregation/ analysis results for 2007 incidents (including an analysis of the causes giving rise to such results), as well as our analysis of trends over time, based on our accumulation of data over the past five years.

2 Objectives

This report is the result of an independent survey and analysis of information leakage incidents reported between January 1 and December 31, 2007.

Personal information is regarded as an information asset, the protection of which is mandated under the Personal Information Protection Act of Japan. Accordingly, the leakage 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."

3 Analysis Results of Personal Information Leakage Incidents

3.1 Survey Methodology

Working Group members collected public reports (including documents released from private organizations) from newspapers, Internet news, and other news sources between January 1 and December 31, 2007, compiling data related to Personal Information Leakage Incidents. As in prior years, Working Group members categorized and evaluated the type of business or organization involved, the number of victims affected by the incident, the causes of information leakage, the route of information leakage, etc., based on the information available. Next, the Working Group used an independently developed formula ("JO Model") to calculate projected compensation for damages related to these incidents.

Data for this survey was collected manually from information related to incidents published over the Internet, noting information necessary for incident analysis from details in the articles or other documents located. Working Group members have expended best efforts to collect as much information as possible; however, the reader should understand that the Working Group was not able to make an exhaustive collection of all articles published that relate to incidents. The Working Group will respond to reader feedback, and correct any results herein that are determined to be in error. If you intend to use this report, please use the latest version released through our website.

3.2 Overview

Compared to 2006, the number of victims by information leakage incidents grew significantly in 2007, totaling approximately 30,530,000 people (a year-on-year increase of 8 million victims). Total projected compensation for damages has likewise increased significantly, amounting to more than ¥2 trillion. Two large-scale incidents (one in the Multi-Service Industry and one in the Manufacturing Industry) involving the personal information leakage of approximately 23,070,000 people were a major factor in these results.

At the same time, the actual number of incidents decreased by 129 compared to 2006, amounting to 864 incidents for the year. Since 2005, the number of annual incidents has experienced a declining trend. In particular, the number of small-scale incidents (incidents with relatively few victims and incidents involving a relatively small projected compensation for damages) has been decreasing overall.

The number and ratio of information leakage incidents attributed to

"Administration Error" experienced a large increase compared to the prior year. Meanwhile, incidents attributable to "Loss/ Misplacement" and "Theft" have declined.

A summary of data collected for 2007 is provided below:

Table 1: Summary Data of 2007 Personal Information Leakage Incidents

Number of Victims	**30,531,004**
Number of Incidents	**864**
Total Projected Compensation for Damages	**¥2,271,089,700,000**
Number of Victims per Incident[1]	**37,554**
Average Projected Compensation for Damages per Incident[1]	**¥2,793,468,000**
Average Projected Compensation for Damages per Victim[2]	**¥38,233**

3.3 Top Five Personal Information Leakage Incidents

During 2007, there were two large-scale incidents in which significantly more than 1 million individuals were affected, only one incident in which approximately 1 million individuals were affected, and two incidents in which approximately 500,000 individuals were affected. In a typical year, there is usually one outlying incident involving significantly more than 1 million individuals, which has an impact on our statistical results. For example, the increase in incidents attributable to "Administration Error" during 2007 was greatly influenced by "No. 1" of the large-scale incidents identified in Table 2.

Table 2 shows the top five large-scale incidents occurring during 2007. A quick glance shows that the industry type involved is widely varied. This illustrates the fact that large-scale incidents can occur in any type of industry. We also see that

1 Averages exclude 64 incidents for which the number of victims was unknown. Projected compensation for damages per person was calculated for each incident, after which the total of the individual results was divided by the number of leakage incidents. Please understand that this number is not the projected total compensation for damages divided by the number of individuals affected.

2 As this average value includes statistical outliers, we first calculated the projected compensation for damages per person for each incident, and then used this figure to calculate the average value of projected compensation for damages per person for all incidents. Accordingly, we ask the reader to understand that this figure is not the projected total compensation for damages divided by the number of individuals affected.

"Administrative Error" is the cause of most of these incidents. "Administration Error" and "Internal Crime/ Internal Fraud" are both situations caused by the acts of persons with authority inside the organization.

Table 2: Top Five Incidents

No.	Number of victims	Industry Type	Cause
1	14,430,000	Multi-Service	Administration Error
2	8,637,405	Manufacturing	Internal Crime/ Internal Fraud
3	976,000	Finance/ Insurance	Administration Error
4	649,574	Wholesale/ Retail	Administration Error
5	470,000	Utilities: Electricity, Gas, Heat, Water	Administration Error

3.4 Single-Year Analysis

(1) Industry Type

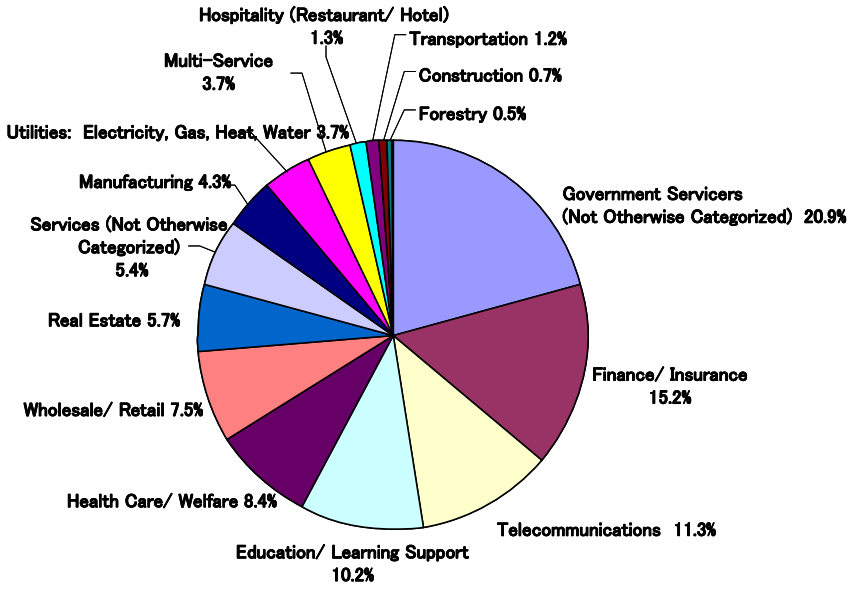


Figure 1: Ratio of Incidents by Industry Type (no. of incidents)

In order, the industry types experiencing the greatest number of incidents during 2007 were Government Services (20.9%), Finance/ Insurance (15.2%), Telecommunications (11.3%), and Education/ Learning Support (10.2%).

Government Services and Finance/ Insurance have continued to be the number one and two industry types for incidents between the years 2004 and 2007. Both of these industry types are heavily regulated by the government, and tend to report even small-scale incidents, which could be a factor accounting for these results.

The top four industry types accounted for a total of 57.6% of incidents during 2007. Of all 18 industry types, only three (Farming, Fisheries, and Mining) did not experience any information leakage incidents. The remaining 15 industry types all experienced incidents, with the top 10 industry types representing more than 90% of the total. Since most industry types deal with personal information, they are at risk for an information leakage incident.

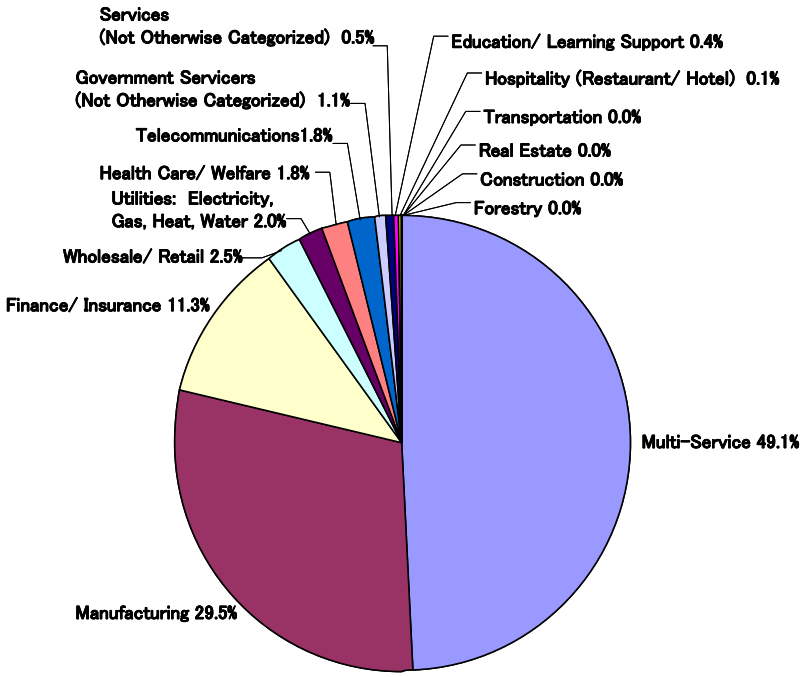


Figure 2: Ratio of Incidents by Industry Type (no. of victims)

In order, industry types with the highest number of victims by incidents were Multi-Service (49.1%), Manufacturing (29.5%) and Finance/ Insurance (11.3%); the ratios for Multi-Service and Manufacturing were extremely high. These results are not due to the fact that these industry types experienced numerous incidents, but rather due to the fact that they both experienced large-scale incidents during the year under review. Trends in ratio of the number of victims according to industry type are not necessarily consistent year-to-year. The reason for this is that, as shown above, the number of victims in an incident can increase significantly according to the impact of the industry type experiencing a major information leakage incident.

Accordingly, the occurrence of a large-scale incident has little, if any, dependent relationship to any particular industry type; organizations that deal with vast amounts of personal information are always at risk for large-scale incidents.

(2) Cause of Information Leakage

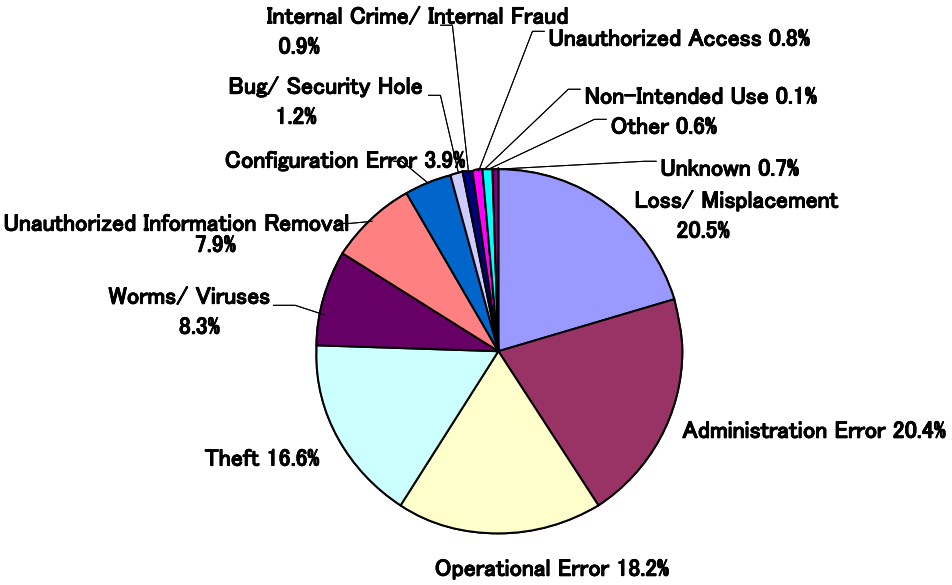


Figure 3: Ratio of Leaks by Cause (no. of incidents)

As was the case in 2006, Loss/ Misplacement, Theft, and Operational Error accounted for the bulk of incidents. However, it should be noted that Administration Error, attributed as the cause of 8.3% of incidents during 2006, jumped to 20.4% for 2007, reaching nearly the same ratio as Loss/ Misplacement.

We believe that organizational internal controls have had a major impact on this development. Corporations have made progress in their initiatives with respect to compliance with laws related to their business activities (including the Personal Information Protection Act), preservation of assets, and IT controls, etc., resulting in stronger management of organizational information. Meanwhile, greater care in the tracking of organizational assets (including information) has resulted in corporate announcements of the inadvertent destruction or loss of information from within corporate facilities.

Details of Administration Error show that nearly half of the incidents were due to inadvertent destruction, with numerous cases of an organization disposing of personal information in error with other information; the number of incidents associated with the loss of portable media (USB flash drives, etc.), as well as the loss of mailed or delivered materials is also notable.

Looking at the details of Operational Error reveal that 47.1% of such incidents were related to misdirected transmission of email; 38.9% were the erroneous delivery of paper media, and 9.6% were the erroneous delivery of facsimiles.

See “7 Appendix Definitions for Causes of Information Leakage” for more about our categorizations and approaches to causes of information leakage incidents.

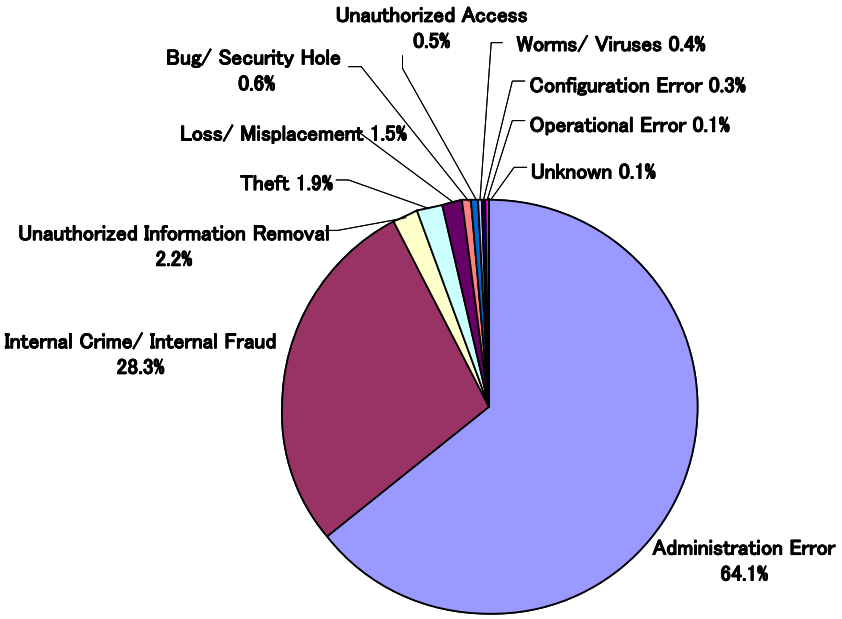


Figure 4: Ratio of Leaks by Cause (no. of victims)

Compared to 2006, Loss/ Misplacement as a cause of incident fell from approximately 4.13 million individuals affected to approximately 460,000; Theft as a cause declined from approximately 1.79 million individuals affected to about 580,000, and the share of overall ratio declined as well. On the other hand, Administration Error grew in a marked way from approximately 350,000 individuals affected during 2006 to approximately 1.956 million individuals for 2007. This significant increase in the number of victims due to Administration Error was influenced by a major incident in which an enormous amount of documents on file were inadvertently destroyed.

Due to the effects of this incident, the ratio of incidents due to Internal Crime/ Internal Fraud decreased from 36.0% in 2006 to 28.3% in 2007; however, the number of victims increased from approximately 8 million to approximately 8.64 million. Here as well, a single large-scale incident contributed greatly to this result.

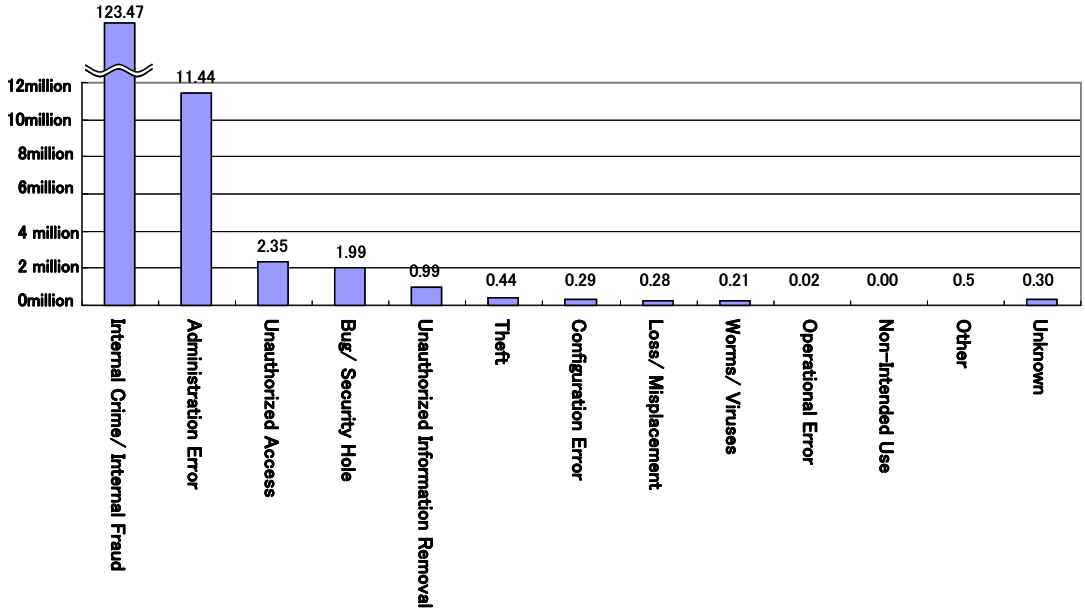


Figure 5: No. of Victims per Incident by Cause

A comparison of the number of victims per incident categorized by cause of the incident reveals that Internal Crime/ Internal Fraud as a cause of incident far outstrips any other cause in terms of victims per incident. Figure 3 shows a graph of incident ratios by cause. Internal Crime/ Internal Fraud was low at 0.9%, and total incidents attributed to this cause actually declined compared to 2006. Despite the relatively low rate of incidence attributable to this cause, the number of victims in any particular incident was extremely large. Each year, incidents involving someone removing sensitive records from an organization—rare though they may be—involve the leakage of enormous amounts of information. This year was no exception, with one incident categorized as Internal Crime/ Internal Fraud affecting an extremely large number of individuals, and also significantly influencing our calculated per-incident averages.

It appears that organizations need to implement better control measures for personal information against Loss/ Misplacement and Administration Error, as well as consider response measures to take in the event of an incident due to internal crime/ fraud affecting a large number of individuals.

(3) Leakage Media/ Route

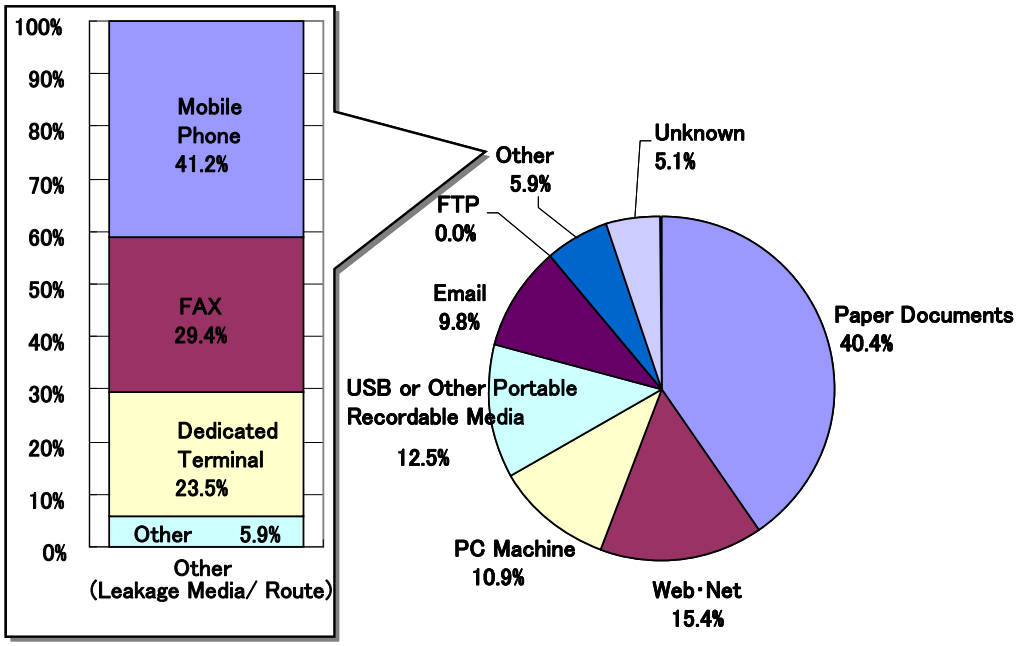


Figure 6: Ratio of Leakage Media/ Route (no. of incidents)

Figure 6 shows the ratio of incidents according to the route of information leakage. The single largest media/ route of leakage in terms of number of incidents was Paper Documents, and all information leakage routes maintained the same order of occurrence as 2006.

However, the ratio of USB or Other Portable Recordable Media increased from 8.2% in 2006 to 12.5% for 2007. We surmise that this increase is due to the fact that lower prices for the media have resulted in the greater adoption of USB and flash memory, as well as insufficiencies on the part of organizations in user management and in dealing with this type of media. The ratio of incidents occurring through the Web/ Net route experienced an increase during 2006, owing mainly to Winny and other file sharing software; however, the ratio for 2007 declined slightly.

We have introduced a minor change to our terms used in our briefs and reports. Please note that we now use the term “USB or Other Portable Recordable Media” instead of “FD or Other Portable Recordable Media” used in the past.

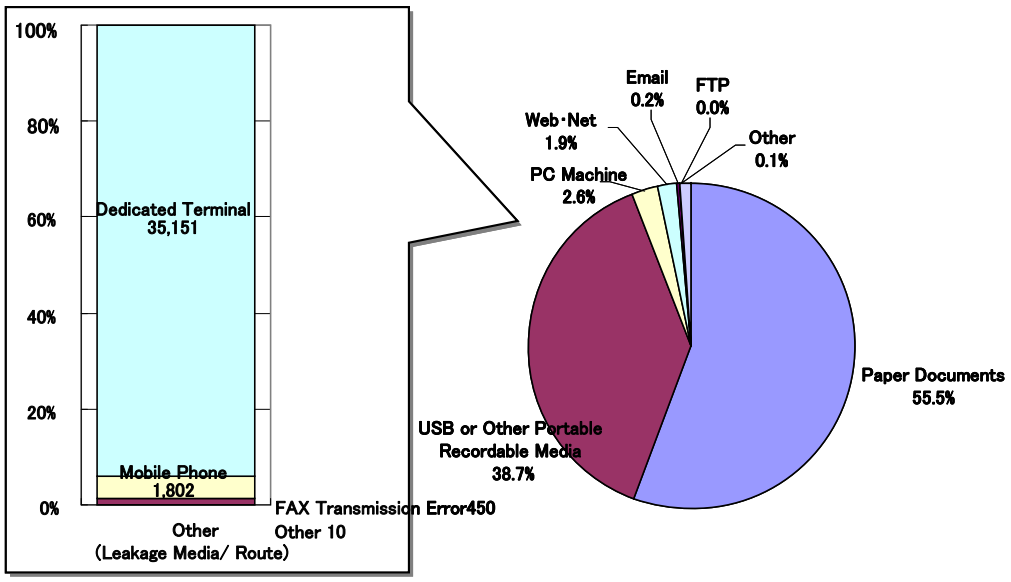


Figure 7: Ratio of Leakage Media/ Route (no. of victims)

Figure 7 shows the ratio of information leakage victims (%) according to leakage route. The ratio of incidents categorized under Paper Documents experienced a very large increase from 7.1% in 2006 to 55.5% in 2007. As mentioned previously, a major incident involving the inadvertent destruction of a large number of documents on file had a significant impact on this category.

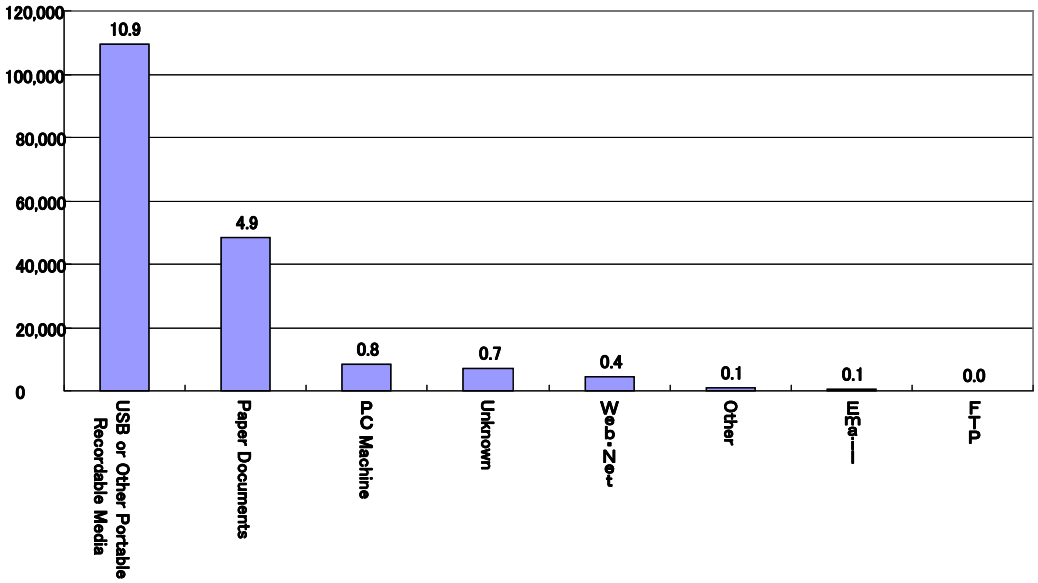


Figure 8: No. of Victims per Incident by Leakage Media/ Route

Even when comparing the number of victims per incident according to leakage media/ route, we see that a large number of victims associated with incidents

involving USB or Other Recordable Portable Media. As mentioned previously, the miniaturization of USB, flash memory and other portable recordable media, as well as enhancements in storage capacity, have made it particularly easy to remove a large volume of information from within an organization. We believe this development has had an impact on our findings.

A large-scale incident during 2007 affected the ratio of incidents attributable to Paper Documents as the leakage route. All other ratios appear to be nearly the same as 2006.

(4) Leaked Information

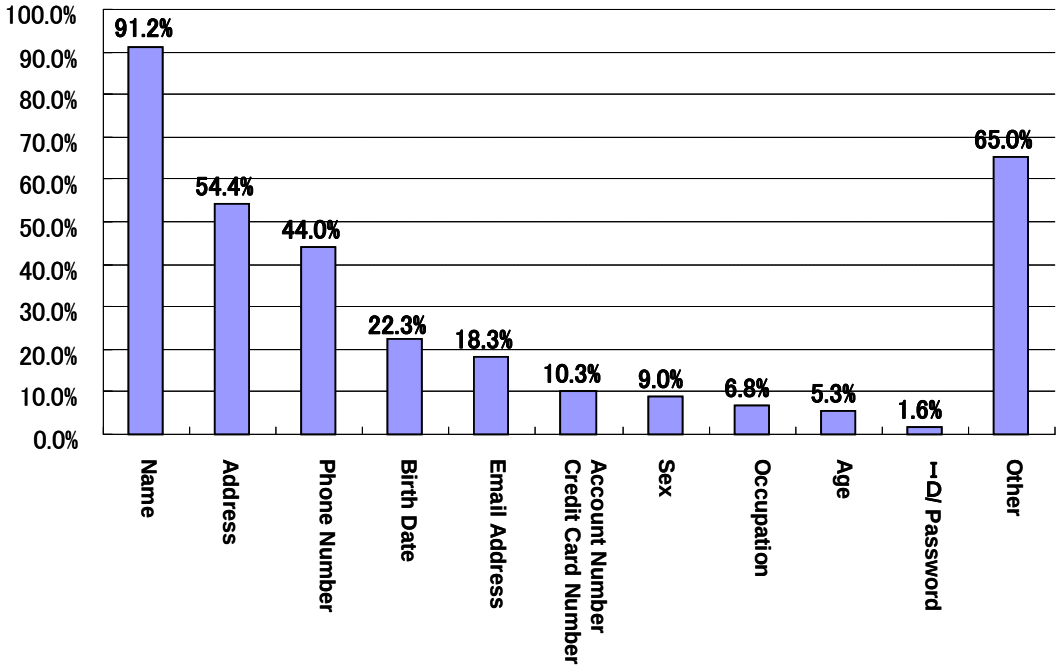


Figure 9: Frequency of Leaked Information

The frequency of Name as leaked information was evident in 91.2% of all incidents--a decidedly high figure. Address came in second at 54.4%, followed by Telephone Number at 44.0%. We believe the high frequencies shown here are due to the fact that Name, Address, and Telephone Number are all very basic pieces of personal information. While occurring less frequently, Birth Date (useful for identifying an individual) at 22.3%, Email Address (susceptible to fraudulent usage in spam email) at 18.3%, Credit Card Number/ Account Number (used for fraud) at 10.3%, and other personal information that can be used to inflict tremendous harm have also been the subjects of information leakage.

Other includes membership number, work location, grades, savings account balance, description of illness, etc.

3.5 Projected Compensation for Damages Calculation Results

(1) Projected Compensation for Damages per Person

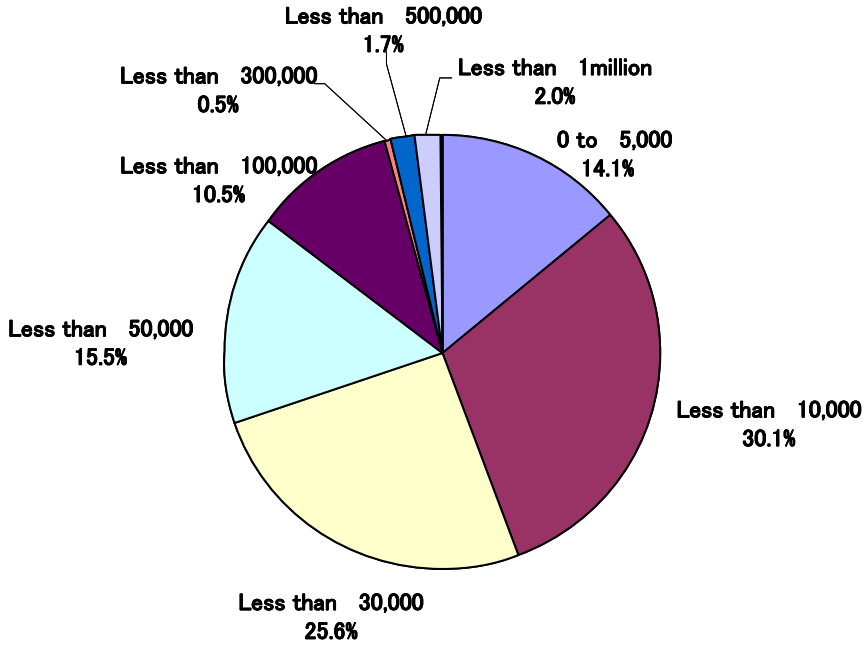


Figure 10: Ratio of Projected Compensation for Damages per Person (no. of incidents)

For 2007, the highest ratio of incidents in terms of projected compensation for damages per victim trended in the ¥5,000 to ¥10,0000 category. Since the ¥10,000 to ¥30,000 range made up the bulk of incidents for 2006, we can conclude that 2007 saw a greater number of incidents involving a low projected compensation for damages, when simply comparing the number of incidents. However, the average projected compensation for damages per person[3] did not vary greatly from 2006 at ¥38,233.

[3] To compensate for per-incident outliers in this average value, we first performed an individual calculation of projected compensation for damages per victim. Next, we added these results, and then divided by the number of leakage incidents. Accordingly, this figure is not the total projected compensation for damages divided by the number of victims.

(2) Projected Compensation for Damages per Incident

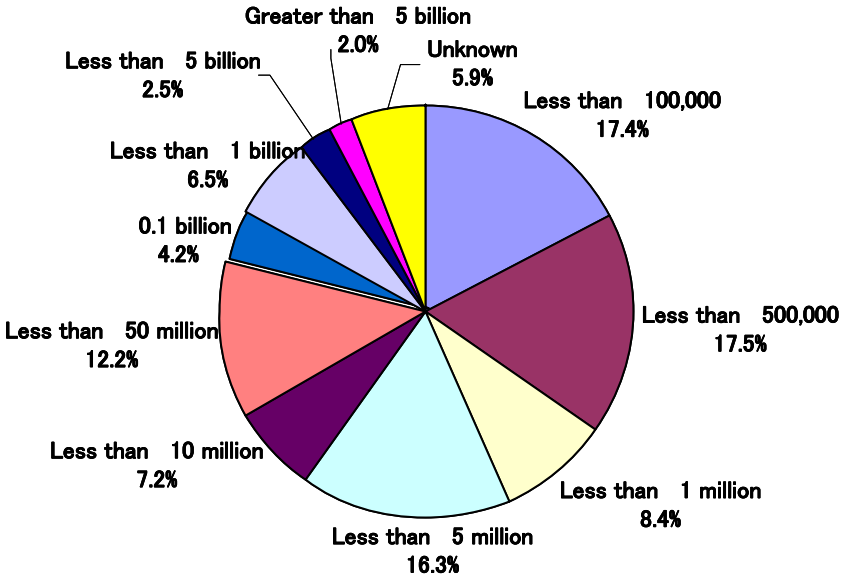


Figure 11: Ratio of Projected Compensation for Damages per Incident (no. of incidents)

Approximately 59.6% of incidents involved a per-incident projected compensation for damages of ¥5 million or lower. Incidents small in scale and involving information of low value (¥Less than ¥10,000, between ¥10,000 and ¥50,000) and medium-scale incidents involving valuable personal information (between ¥100,000 and ¥500,000; between ¥10 million and ¥50 million) account for a large percentage of leakages during 2007.

3.6 Single-Year/ Correlative Analysis

(1) Number of Incidents and Number of Victims by Industry Type

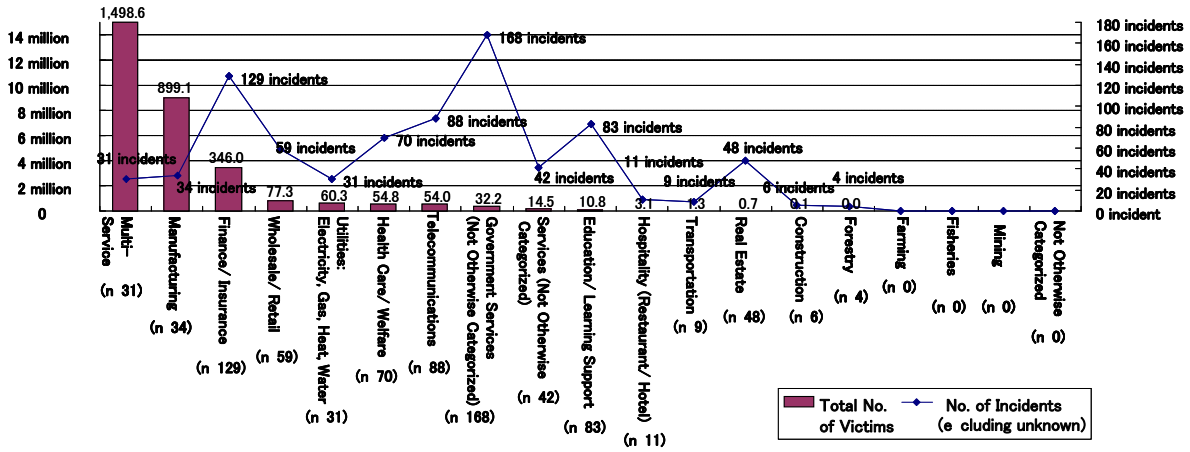


Figure 12: Number of Incidents and Number of Victims by Industry Type

Figure 12 shows the number of victims and number of incidents by Industry Type on the same graph. Despite the relatively few incidents categorized in "Multi-Service" and "Manufacturing," the number of victims involved was relatively large. The cause of this trend, as addressed in "Top Five Personal Information Leakage Incidents," lies in the fact that these industry types each experienced a large-scale incident involving a large number of victims, somewhat skewing our survey.

"Government Services," "Education/ Learning Support," and other categories experienced a large number of incidents during 2007; however, these incidents involved a relatively low number of victims per incident, indicating to the Working Group that there was a large number of small-scale incidents that occurred during 2007.

3.7 Interannual Analysis

The Working Group conducted a wide variety of an interannual analysis based on information related to six years' worth of incidents collected between 2002 and 2007. Only a relative few incidents were publicly disclosed between 2002 and 2004, and accordingly, information was successfully collected for only a few incidents. Of those incidents reported, most were serious and large scale in nature; accordingly, readers should note that there will be a significantly large skew in statistical data.

(1) Number of Victims and Number of Incidents (2002 to 2007)

Table 3: Interannual Changes in Number of Victims and Number of Incidents

	Number of Incidents	Number of Victims	Average Number of Victims per Incident[4]
2002	62	418,716	7,613
2003	57	1,554,592	30,482
2004	366	10,435,061	31,057
2005	1,032	8,814,735	8,922
2006	993	22,236,576	23,432
2007	864	30,531,004	37,554

Table 3 shows the number of incidents, the total number of victims, and the average number of victims per incident for the six years between 2002 and 2007.

The number of incidents occurring during 2007 amounted to 0.8 times that of 2005, and 0.9 times the number of incidents occurring during 2006, drawing a marginal decrease since the peak of 2005. Despite this decline, the similar number of incidents for 2006 and 2007 (993 and 864, respectively) leads us to conclude that personal information leakage did not end with the temporary focus resulting from the 2005 full enforcement of the Personal Information Protection Act, but rather such incidents have become recognized by the public at large as general organizational fraud.

The number of victims of personal information leakage during 2007 was, unfortunately, the largest number since we began collecting statistics in 2002. The number of 2007 victims was 3.5 times that of 2005, and 1.4 times that of 2006.

The average number of victims per incident for 2007 was also the highest since we began this survey—a number affected by several large-scale incidents that occurred during the year.

---

4 Parameter for average number of victims for 2007 was 813 (excludes 51 incidents for which the number of victims was unknown).

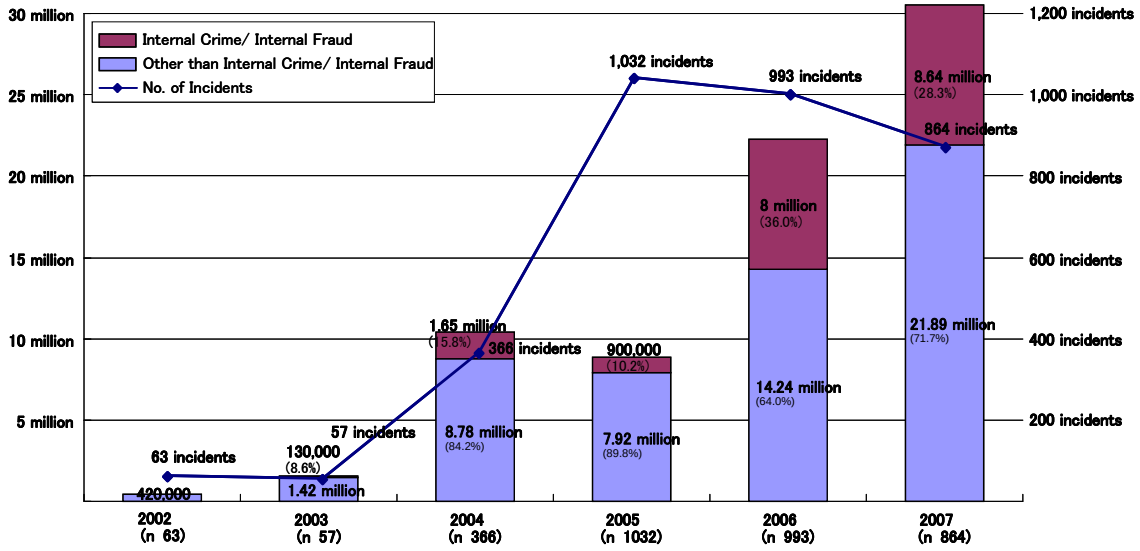


Figure 13: Interannual Changes in Number of Incidents and Number of Victims due to Internal Organizational Fraud (total)

As discussed earlier in connection with Table 3, the number of incidents has declined since 2005, but the number of victims has continued to increase. In addition, the ratio of large-scale incidents accounted for a high number of victims overall.

In recent years, the number of victims of personal information leakage due to "Internal Crime/ Internal Fraud" has accounted for a high ratio of the total, with 8 million victims in 2006 (36.0% of total) and 8.64 million victims for 2007 (28.3% of total).

(2) Number of Victims per Incident (2002 to 2007)

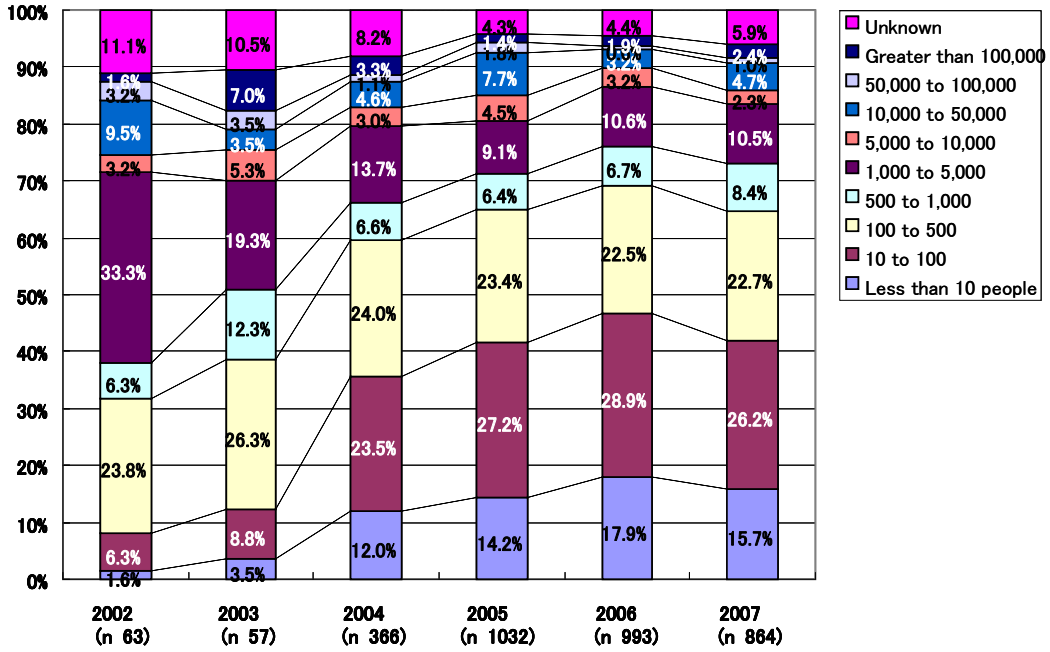


Figure 14: Interannual Changes in Ratio of Victims per Incident by Category (no. of incidents)

The ratio of victims per incident in the small "less than 10" and "between 10 and 100" range accounted for 41.4% of the total in 2005, 46.8% of the total in 2006, and 41.9% of the total in 2007. The ratio of victims per incident in the large "between 50,000 and 100,000" and "Greater than 100,000" range amounted to 3.2% of the total in 2005, 2.5% of the total in 2006, and 3.5% of the total in 2007. These figures as well point to the fact that the ratio related to large-scale incidents was higher in 2007 than in other years.

Despite the decrease, the small-scale group still accounts for a high ratio of the total, and as we wrote in our 2006 report, this is likely due to a new consciousness in society for reporting all incidents—even those involving only a few victims.

(3) Cause of Information Leakage (2002 to 2007)

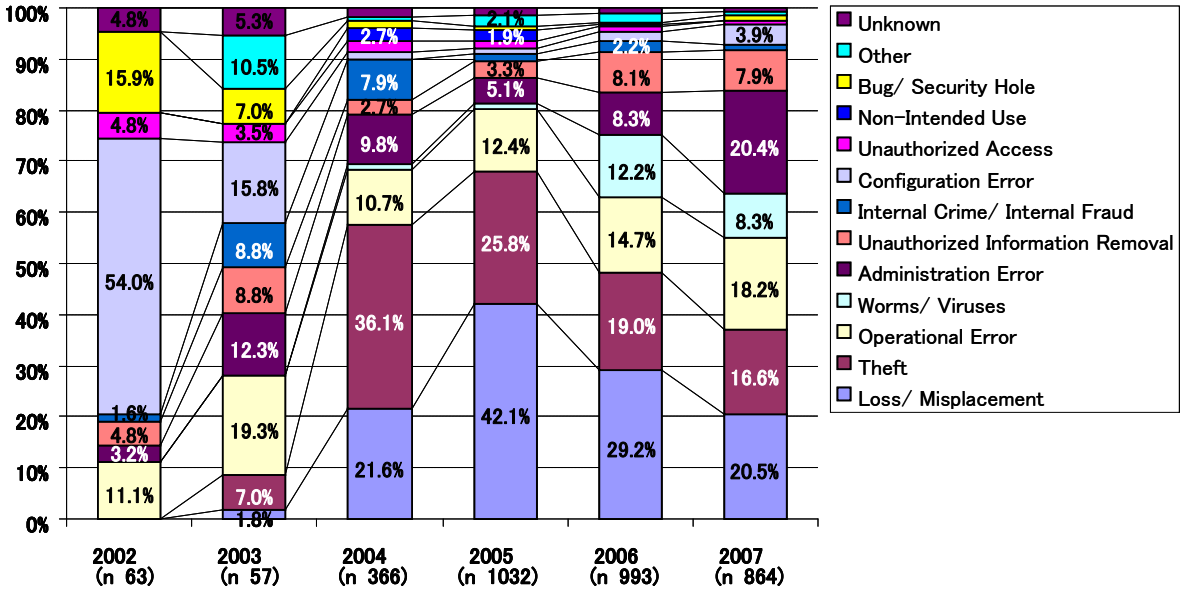


Figure 15: Interannual Changes in Ratio of Leaks by Cause (no. of incidents)

"Loss/ Misplacement" and "Theft" have been declining as causes of incidents since 2005.

Meanwhile, the ratio of "Administration Error" (inadvertent destruction or loss occurring within the organization's facilities) has been increasing. We can conceive of two reasons for this trend. The first is that the measures against the unauthorized physical removal of personal information have advanced, focusing on an area of personal information control and administration that had suffered to that point from a lack of emphasis. The second is that the cause of publicly disclosed incidents in the Finance/ Insurance industry categorized as "Loss" in 2005 is now categorized as "Administration Error" in 2007, given the perspective of the internal controls framework.

The number of incidents attributed to Operational Error has also increased slightly over time. The Working Group could not read any meaningful trends from within the Other category.

(4) Route of Information Leakage (2002 to 2007)

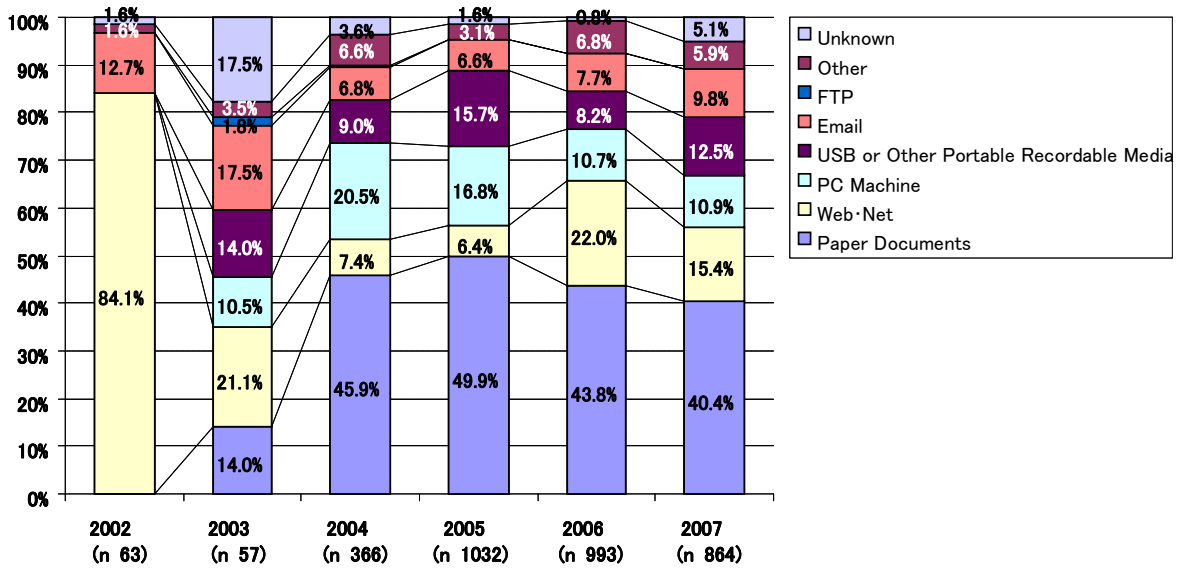


Figure 16: Interannual Changes in Ratio of Information Leakage Route (no. of incidents)

While leakage associated with Paper Documents continued to account for the bulk of incidents, there has been a notable decline since 2005. Leakage due to "PC Machine" has declined since 2006; however, there has been a marked increase in leakage due to "Web/ Net" (including P2P file sharing software).

Though not a major change, leakage due to "USB or Other Portable Recordable Media" has increased.

(5) Number of Incidents by Industry Type (2002 to 2007)

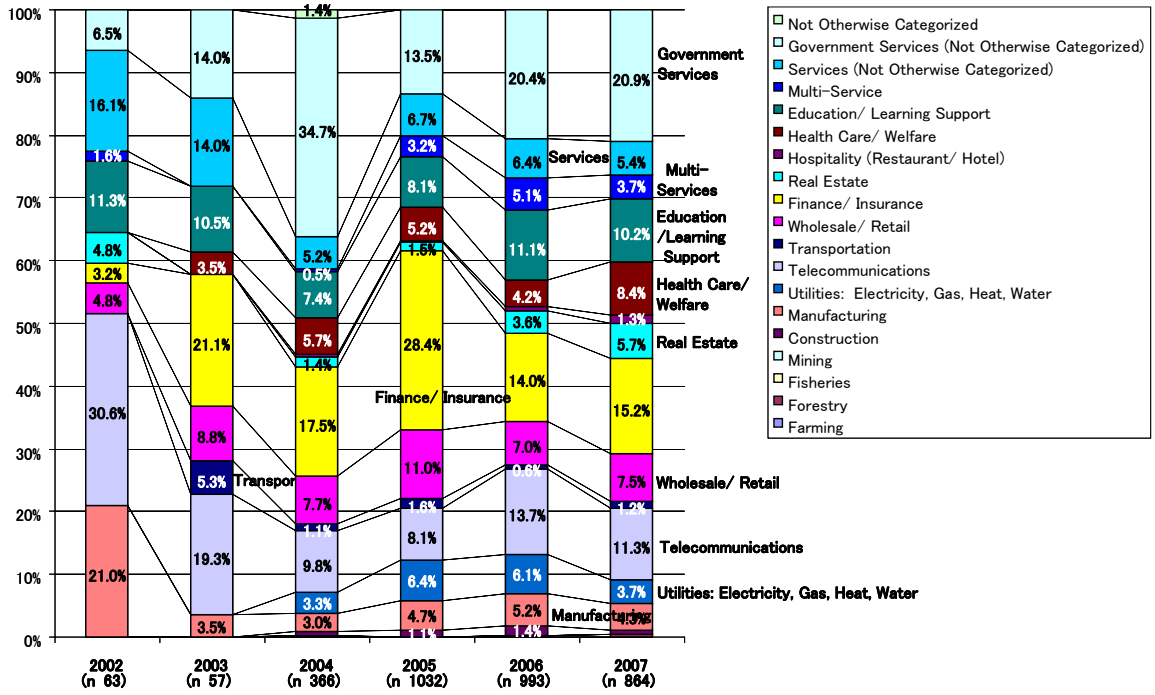


Figure 17: Interannual Changes in Ratio of Incidents by Industry Type (no. of incidents)

As with 2006, Government Services represented the highest ratio of incidents by industry type during 2007. The ratio was 20.9% of the total, measuring nearly the same as 2006. Following Government Services, Finance/ Insurance and Telecommunications were the next-highest industry types—a result similar to 2006.

Although not one of the top three industry types during 2007 in terms of incidents, the ratio of incidents associated with the "Health Care/ Welfare" industry type was 8.4%, or twice the number for 2006.

3.8 Interannual Analysis of Projected Compensation for Damages

The following table serves as an observation of interannual changes in compensation for damages for the six years between 2002 and 2007.

Table 4: Interannual Changes in Total Projected Compensation for Damages

	Total Projected Compensation for Damages	Average Projected Compensation for Damages per Incident
2002	Approx. ¥18.9 billion	¥275.32 million
2003	Approx. ¥28.1 billion	¥550.38 million
2004	Approx. ¥466.7 billion	¥1.373 billion
2005	Approx. ¥700.2 billion	¥786.8 million
2006	Approx. ¥457.0 billion	¥481.56 million
2007	Approx. ¥2.2711 trillion	¥2.79347 billion

Total projected compensation for damages for 2007 amounted to the highest total since the Working Group began this survey. Two large-scale incidents occurred during 2007, both involving credit card information, account numbers, and other sensitive personal information. Accordingly, the projected compensation for damages associated with these two incidents was enormous, skewing the total for 2007 compared to other years.

Due to the aforementioned incidents, the average projected compensation for damages per incident was approximately ¥1,500 greater than in 2006.

The average projected compensation for damages per incident was calculated excluding the 64 incidents for which the number of victims was unknown. We calculated the projected compensation for damages per person for each individual incident, totaled this number, and then divided that figure by the number of leakage incidents. Readers should note that this figure is not the total of projected compensation for damages divided by the number of victims.

Table 5: Average Projected Compensation for Damages per Victim

2002	¥16,855
2003	¥89,140
2004	¥105,365
2005	¥46,271
2006	¥36,743
2007	¥38,233

Meanwhile, the average projected compensation for damages per person

increased slightly from ¥36,743 in 2006 to ¥38,233 for 2007. The Working Group also noted a trend in which the number of incidents involving lower numbers of victims per incident decreased overall.

To compensate for outliers in the average projected compensation for damages per person, we first calculated the projected compensation for damages per person in each incident, and then calculated an average amount of projected compensation for damages per person for all incidents. The reader should accordingly be aware that this figure is not the total projected compensation for damages divided by the number of victims.

(1) Total Projected Compensation for Damages and Number of Victims (2002 to 2007)

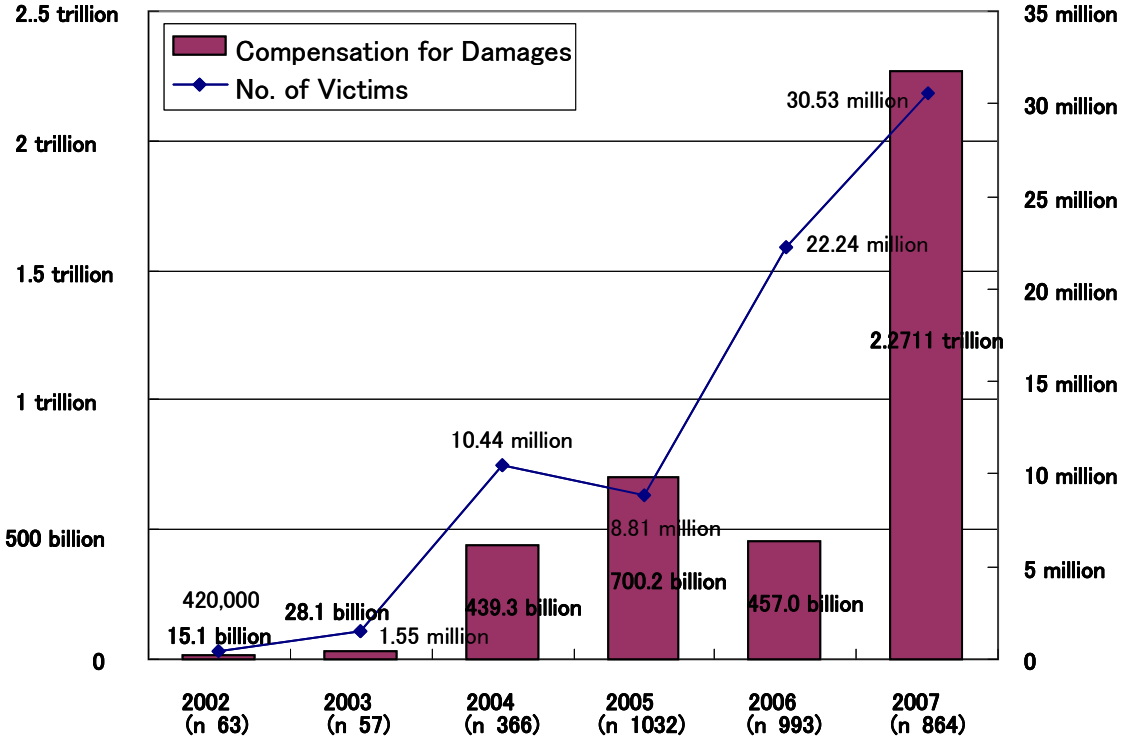


Figure 18: Total Projected Compensation for Damages and Number of Victims

Total projected compensation for damages declined for 2006 compared to the previous years; however, the occurrence of large-scale incidents involving highly valuable personal information resulted in a significant increase for 2007 to approximately ¥2.2711 trillion. Of that amount, the two large-scale incidents accounted for more than ¥1.8600 trillion. The number of victims declined in 2005, but increased in the subsequent years.

(2) Projected Compensation for Damages per Victim (2002 to 2007)

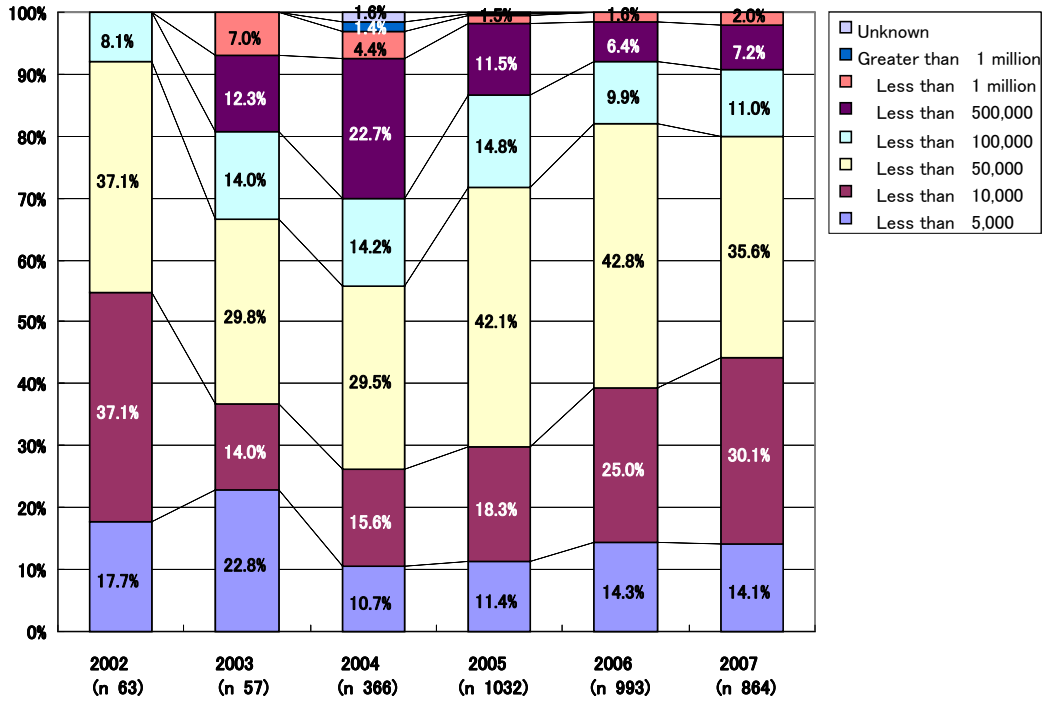


Figure 19: Interannual Changes in Ratio of Projected Compensation for Damages per Person (no. of incidents)

Incidents for which the projected compensation for damages per person was ¥10,000 or less increased in proportion subsequent to 2004. We believe that this trend is due to a continued increase in the reporting of personal information leakage incidents that do not involve sensitive information.

Meanwhile, we have noted an increase in the ratio of incidents of ¥50,000 or greater per person, compared with a declining trend in 2006.

(3) Projected Compensation for Damages per Incident (2002 to 2007)

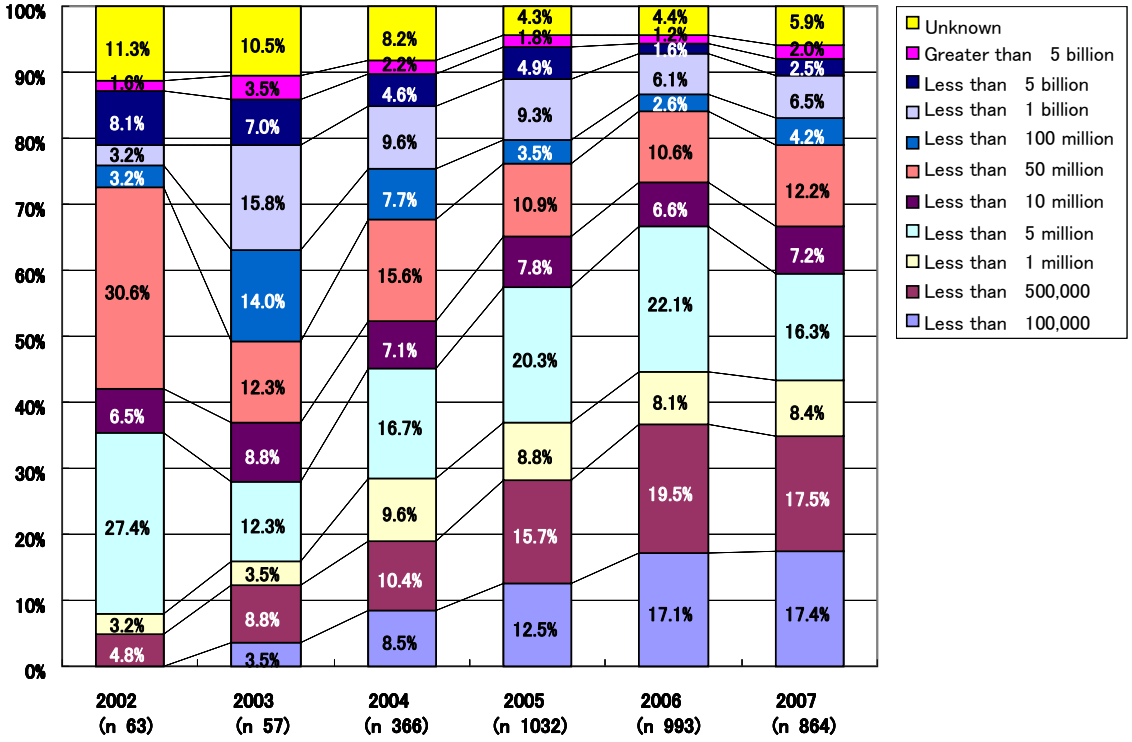


Figure 20: Interannual Changes in Ratio of Projected Compensation for Damages per Incident (no. of incidents)

Between 2003 and 2006, we noted increase in the number of incidents for which the projected compensation for damages per incident was low.

However, compared to 2006, the ratio of incidents involving a per-incident amount in excess of ¥5 million increased for 2007. There is no doubt that the two large-scale incidents occurring during 2007 were the cause of the significant increase in projected compensation for damages; however, incidents for which the per-incident projected compensation for damages was high showed an overall increase as well.

Observing this trend in conjunction with the pattern for projected compensation for damages per person indicates that incidents for which both the per person projected compensation for damages and per incident projected compensation for damages were small experienced an increase until 2006. However, compared to 2006, ratio of incidents with a small projected compensation for damages per person in 2007 (less than ¥10,000) continued to decrease, while the ratio of the number of incidents in which the projected compensation for damages per person was greater than ¥50,000 increased. At the

same time, the ratio of the number of incidents for which the projected compensation for damages per incident exceeded ¥5 million also increased.

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 will report the results of applying our calculation model to Personal Information Leakage Incidents occurring during 2007 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 2007 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

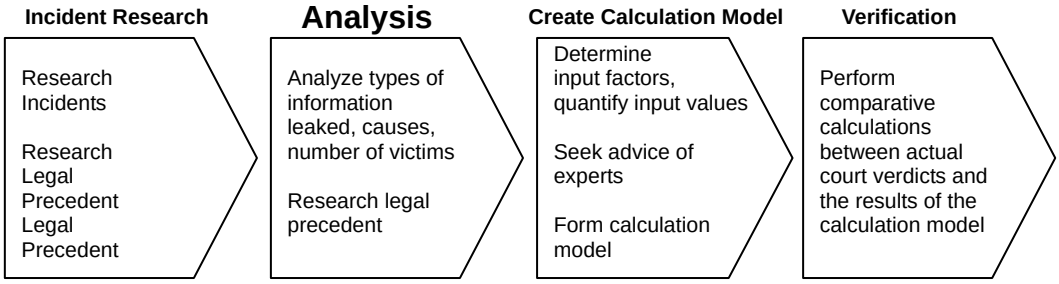


Figure 21: Process behind the Formation of the Projected Compensation for Damages Calculation Model

We developed our calculation model as depicted in Figure 21 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. “3 Personal Information Leakage Incident Analytical Results” describe the results of our analysis for 2007.

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.

(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 22). The farther removed from the origin, the greater the respective levels of Economic Loss and Emotional Distress.

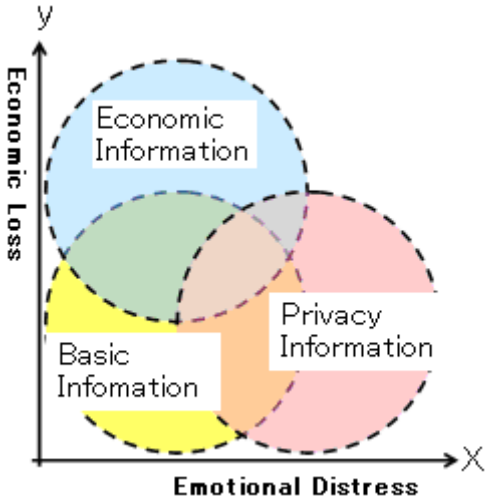


Figure 22: Economic-Privacy Map (EP Map)

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 23).

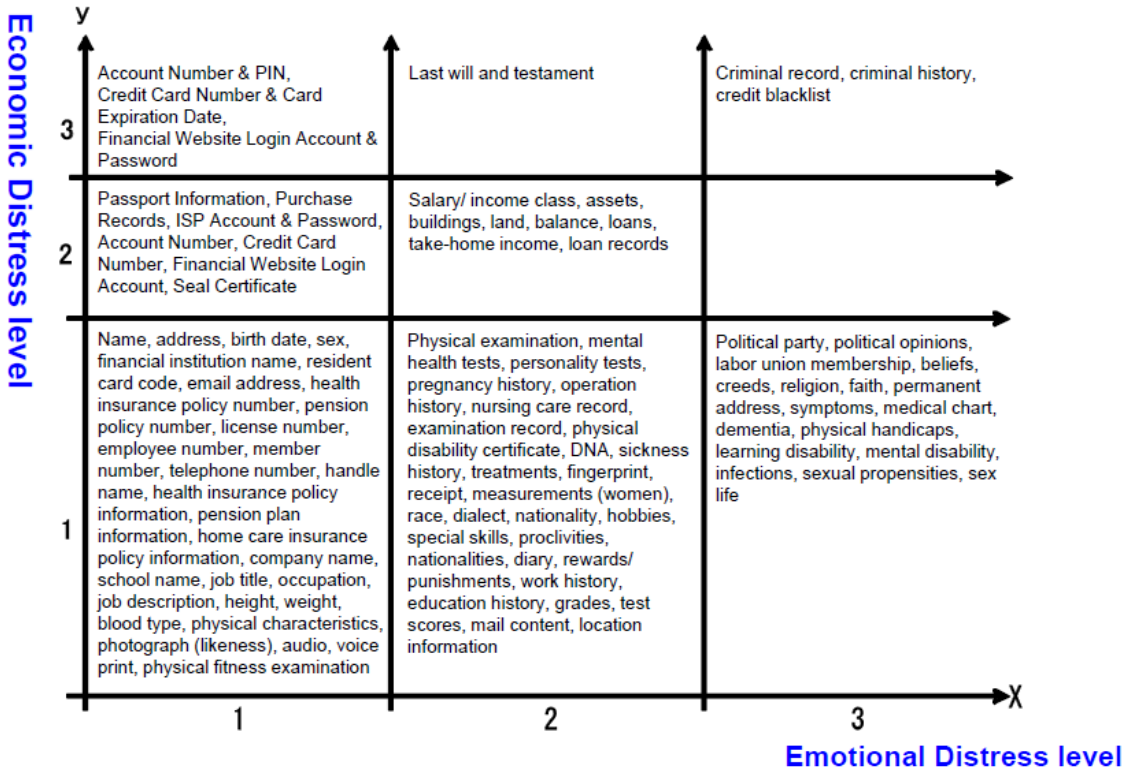


Figure 23: Simple-EP Map

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:

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

c. Degree of Ease in Identifying the Individual

Degree of Ease in Identifying the Individual represents the ease with which the 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 6 below.

Table 6: 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

(2) Degree of Social Responsibility of the Organization in Question

As shown in Table 7, 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 7: 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

(3) Appraisal of Post-Incident Response

The appraised value of Post-Incident Response is based on Table 8 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 8: 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

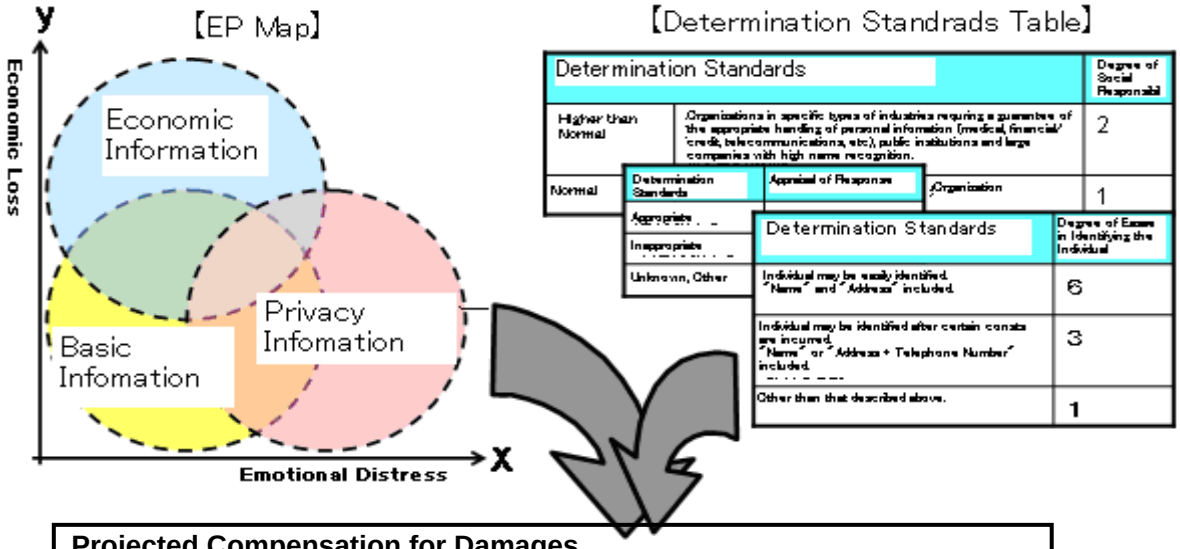
- Rapid response
- Understanding of the circumstances
- Public announcement of the incident
- Subsequent leakage of the circumstances (Website, Email, letters)
- Communicating with victims, offering apologies
- Offering apologies to victims (including presentation of gift certificates, etc.)
- Estimates 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 "4.2.2 Explanation of the Calculation Model Input Values." The Working Group calls the following Projected Compensation for Damages Calculation Model the JO Model (JNSA Operation Model for Individual Information Leak)."



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 + 5^{y-1})]
×Ease in Identifying the Individual [6,3,1]
×Degree of Social Responsibility of the Organization [2,1]
×Appraisal of Post-Incident Response [2,1]

Figure 24: JO Model

5 Conclusion

Having collected and analyzed information about incidents occurring during 2007, we noted a somewhat lessening in focus by the general public on information leakage—a step back from the personal information leakage panic that occurred between 2004 and 2005 surrounding the enactment of the Personal Information Protection Act (2005) and Winny issues, and from the heated reporting and overreaction in connection with the spate of sensitive information leakage incidents (2006). However, the risk of personal information leakage is still very present for corporations now as ever. After 2005, the number of victims involved in incidents continued to grow significantly, with 2007 showing an unexpected jump of more than 8 million compared to 2006, for a total of 30.53 million victims. Total projected compensation for damages in 2007 exceeded the ¥2 trillion mark. Two large-scale incidents during 2007 accounted for 23.07 million victims of personal information leakage, which contributed greatly to the 2007 increase. While the number of incidents declined compared to 2006, there was still an average of 2.4 incidents occurring per day.

Each year demonstrates certain characteristics related to the circumstances surrounding information leakage incidents. 2005 saw a frequent occurrence of incidents via Paper Documents, PC Machine, and Loss/ Theft, while our attention was focused on Internal Crime/ Internal Fraud as the predominant leakage route for 2006. For 2007, we noted an increase in incidents occurring via Administration Error. We see this change for 2007 as a promising trend. To the Working Group, this trend signals that treating the inadvertent destruction and intra-organizational loss of personal information as an incident shows the advancement of measures against the unauthorized removal of personal information, and that there is an organizational effort for the control and management of personal information—something that had not been a focus in the past. Proof of this advancement in measures against the unauthorized removal of personal information lies in the number of incidents involving few victims and a low projected compensation for damages, which our analysis results show have been tracing a decreasing trend. We also believe recent trends in awareness and implementation of organizational internal controls have contributed to these results. The advancement in implementation of internal controls and enhanced management of information within the organization, as well as physical tracking of stored information and documents, has likely resulted in the uncovering of inadvertent destruction and/ or loss of organization information.

The Working Group has, however, heard frequent rumblings that despite the implementation of stricter measures, the actual operations involved must be conducted according to plan to make such measures meaningful. There are numerous cases in which individuals resent procedures required before removing information from the work location, intentionally "sabotaging" the operations determined for taking notebook PCs out of the organization's facilities. These acts interfere with the execution of set duties, and lead to lost business opportunities. The root cause is that procedures for security are disassociated from familiar, everyday procedures. This is because these procedures are commonly adapted from rules at other organizations, or originate someplace up the line in the organization by individuals who do not have a full understanding of the actual work performed in the local workplace. The Working Group believes that those in the local workplace should be responsible for thinking about security issues, creating rules that complement local work processes.

The number of small-scale incidents is decreasing, signaling the beginning of the effects of measures taken. Accordingly, the next big issue for corporations is to deal with large-scale incidents. The four industry types that deal with large volumes of information (Government Services, Finance/ Insurance, Telecommunications, Education/ Learning Support) are highly susceptible to the occurrence of incidents. These four industry types must be continuously conscious of reducing the likelihood of an incident. Meanwhile, there are a wide variety of industry types for which large-scale incidents (such as the Top Five Incidents above) can occur. There is an equal potential for incidents to occur in any company that collects/ uses a large volume of personal information, regardless of industry type. Most industry types utilize personal information. Accordingly, most industry types are at risk for a major information leakage incident. And while the likelihood of occurrence may be small, it represents a large loss for a corporation, so we believe that the preparation of contingency plans and business continuity planning (BCP) is recommended to limit potential losses.

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
URL: http://www.jnsa.org
E-mail: sec@jnsa.org

7 Appendix Definitions for Causes of Information Leakage

The Working Group categorized the causes of information leakage as shown in the table below.

Table 9: Approach to Categorization of Causes of Information Leakage

Category	Specific Example	Determination Criteria
Configuration Error	A website or other configuration error allows information to be viewed from outside the organization; sensitive information may have been viewed.	When information has been leaked due to configuration errors in web servers, file access privileges, etc. – Incidents exploiting configuration errors to intentionally steal information are not categorized as Unauthorized/ Illegal Access. – Since this is not a software vulnerability, such incidents are not categorized as Bug/ Security Hole. – Information leakage due to erroneous management procedures are categorized as Administration Error.
Operational Error	Incident occurs due to misdirected transmission of email, fax, regular mail.	When information has been leaked due to a mistaken/ inaccurate address, an accidental push of the wrong operating button, or other human error. – Categorized as Operational Error when the last/ ultimate operation is the cause of the error. Categorized as a Configuration Error when email system settings are in error.
Bug/ Security Hole	Incident occurs due to a Bug/ Security hole in the OS, application, etc., which allows sensitive information to be viewed over the Internet or otherwise leaked.	When a Bug/ Security Hole in an installed OS or application causes an information leakage incident. – Includes cases where Bug/ Security Hole is left unaddressed on the user's system. – Includes cases where software or system vendor has not dealt with security issue.
Unauthorized/ Illegal Access	Sensitive information is leaked outside the organization when access controls are overcome, and the network is infiltrated by external sources.	When a third party utilizes the network (mainly) to access a system illegally, resulting in the leakage of information. Categorizeds as Internal Crime/ Internal Fraud when an individual internal to the organization (employee, worker, etc.) commits unauthorized/ illegal access.

Category	Specific Example	Determination Criteria
Internal Crime/ Internal Fraud	Sensitive information is removed by an employee, temporary employee or other individual internal to the organization for fraudulent purposes. Information stolen is used to commit crime, is sold, or otherwise leaked.	When an employee or employee from another company (temporary worker, etc.) inside the organization engages in unauthorized/ illegal access or other unlawful activity to remove information for fraudulent purposes. – Categorized as Internal Crime/ Internal Fraud even in cases where an intentional fraudulent act by an organizational outsider involves unauthorized/ illegal access. – Categorized as Unauthorized Information Removal in cases where information required for work or other legitimate purposes is removed, but in violation of rules.
Unauthorized Information Removal	Information is removed from within the organization by an employee, temporary employee, outside contractor, vendor, former employee, etc. for use at home, customer location or other location, and is subsequently leaked.	When information is removed for work or other legitimate purposes, but in violation of rules. Striclty speaking, it is “theft” when information or information media is removed in violation of the rules; however, such cases as noted in the left column are categorized as Unauthorized Information Removal. – Categorized as Unauthorized Information Removal, even when an employee takes sensitive information home, subsequently leaking such information through P2P file-sharing software.
Non-Intended Use	Organization-wide or business-related use of personal information for other than the original intended purpose. Information is shared with affiliates or other external organization outside the original scope of disclosure.	When personal information is used for other than the originally intended purpose. – Categorized as Internal Crime/ Internal Fraud when an employee, temporary employee or other organization insider acts individually to use personal information for a non-intended use.

Category	Specific Example	Determination Criteria
Loss/ Misplacement	When a PC or other other information media is inadvertantly lost or misplaced inside a train, restaurant, or other outside location.	When information is removed with permission, and is then subsequently lost or misplaced at the destination or en route. Leakage occurs to personal/ individual Administration Error. – Categorized as Administration Error when information subject to control is lost within the organization.
Theft	Sensitive information on a PC or other information media is stolen in the process of an auto or office break-in.	When information is stolen by a third party with the information recordable media. Auto, office break-in, etc. – Categorized as Unauthorized/ Illegal Access when only information (not a PC or physical media) is stolen.
Administration Error	Personal information is lost after an organizational move. The transfer of personal information is not sufficiently verified; transferred information is lost. Information disclsure/ management rules are not sufficiently clear; information is inadvertantly disclosed.	When information becomes lost or misplaced within an organization or usual distribution channel. When information is leaked in the business process due to work procedure error, or because rules regarding information disclosure and/ or information management are not sufficiently clear. When responsibility for loss lies with the organization. – Categorized as Theft when theft occurs due to administration error. – Includes cases where information is inadvertently destroyed due to insufficient management/ administration.
Worms/ Viruses	Personal information (email addresses, etc.) is leaked without the consent of the information owner due to worm or other virus infection.	When information is leaked due to virus or worm infection. Considered Worms/ Viruses when such is the proximate cause of the leakage. – Includes cases where information is leaked due to a worm/ virus that takes advantage of security holes. – Categorized as Worms/ Viruses in cases other than when the cause of leakage is due to P2P file-sharing software containing worms/ viruses accessing information taken home without permission (Unauthorized Information Removal), or when information is leaked from an organization PC using P2P file-sharing software (Administration Error).

Category	Specific Example	Determination Criteria
Other	Documents belonging to one person are included in an envelope addressed to someone else.	Any situations not addressed above.
Unknown		Cause of the incident is unknown.