2008

Information Security Incident Survey Report

[Abstract]

English Edition

Ver. 1.0

NPO Japan Network Security Association

Security Incident Investigation Working Group

March 31, 2010

Table of Contents

JNSA Survey and Research 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
Kousetsu	Kayama	FUJITSU LIMITED
Haruto	Kitano	Oracle Corporation Japan
Tomoharu	Sato	BroadBand Security, Inc.
Yasuhiko	Sato	Microsoft Co., Ltd.
Go	Seino	Oracle Corporation Japan
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.
Nao	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 2008 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 2008 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 2008 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, 2008.

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, 2008, 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 2007, the number of leakage incidents during 2008 increased significantly, amounting to 1,373 incidents (an increase of 509 incidents). This was primarily due to an increase in the number of incidents across many different industries, including Education/ Learning Support, Finance/ Insurance, Services, and Transportation. In particular, a certain local government was very active in reporting information leakage incidents, which impacted the number of incidents for the year.

The number of victims of information leakage incidents for 2008 amounted to 7.23 million individuals, the fewest number since the Personal Information Protection Act came into effect, and the first time that the number decreased year-to-year. One major reason for this decrease is that there were no large-scale personal information leakage incidents that significantly exceeded one million victims. In other words, this means that the occurrence of an unexpectedly large personal information leakage incident has much to do with the number of victims and amount of damages during the year in question. Because an unexpected large-scale incident has a major impact on the number of victims and total amount of projected compensation for damages, it is difficult to accurately track interannual trends.

The number and overall ratio of incidents attributed to Operational Error and Administrative Error increased significantly, while the number of incidents attributed to Unauthorized Information Removal experienced a decrease. The following table shows the summary of data collected for 2008:

Table 1: Summary Data of 2008 Personal Information Leakage Incidents

Number of Victims	**7,232,763**
Number of Incidents	**1,373**
Total Projected Compensation for Damages	**¥236,725,290,000**
Number of Victims per Incident [*1]	**5,668**
Average Projected Compensation for Damages per Incident [*1]	**¥185,520,000**
Average Projected Compensation for Damages per Victim [*2]	**¥43,632**

[*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

3.3 Top Ten Personal Information Leakage Incidents

Table 2 shows the 10 largest incidents occurring during 2008. There were no large-scale incidents during 2008 that affected significantly more than one million victims, and only one incident that affected approximately one million people. Through 2007, at least one incident occurred each year that affected significantly more than one million people, which skewed the statistical results.

Looking at the top 10 incidents by industry shows a greater bias toward certain industries than 2007, with many incidents occurring in the Government Services and Finance/ Insurance industries. However, the Wholesale/ Retail and Telecommunications industries also experienced information leakage incidents included in our top 10. As to cause, Administrative Error was the culprit in many circumstances. This is due to the fact that, since 2007, stronger internal controls have resulted in more stringent intra-organizational information management, leading to the detection of large-volumes of erroneous information disposal.

Table 2: Top 10 Incidents

No.	Number of Victims	Industry Type	Cause
1	995,023	Government Services (Not Otherwise Categorized)	Administrative Error
2	766,356	Government Services (Not Otherwise Categorized)	Administrative Error
3	653,424	Wholesale/ Retail	Unauthorized Access
4	349,827	Finance/ Insurance	Administrative Error
5	291,338	Government Services (Not Otherwise Categorized)	Administrative Error
6	269,350	Finance/ Insurance	Administrative Error
7	262,781	Government Services (Not Otherwise Categorized)	Administrative Error
8	254,677	Finance/ Insurance	Administrative Error
9	232,970	Telecommunications	Internal Crime/ Internal Fraud
10	213,443	Government Services (Not Otherwise Categorized)	Administrative Error

number of individuals affected.

3.4 Industry Type

(1) Single-Year Analysis (Number of Incidents)

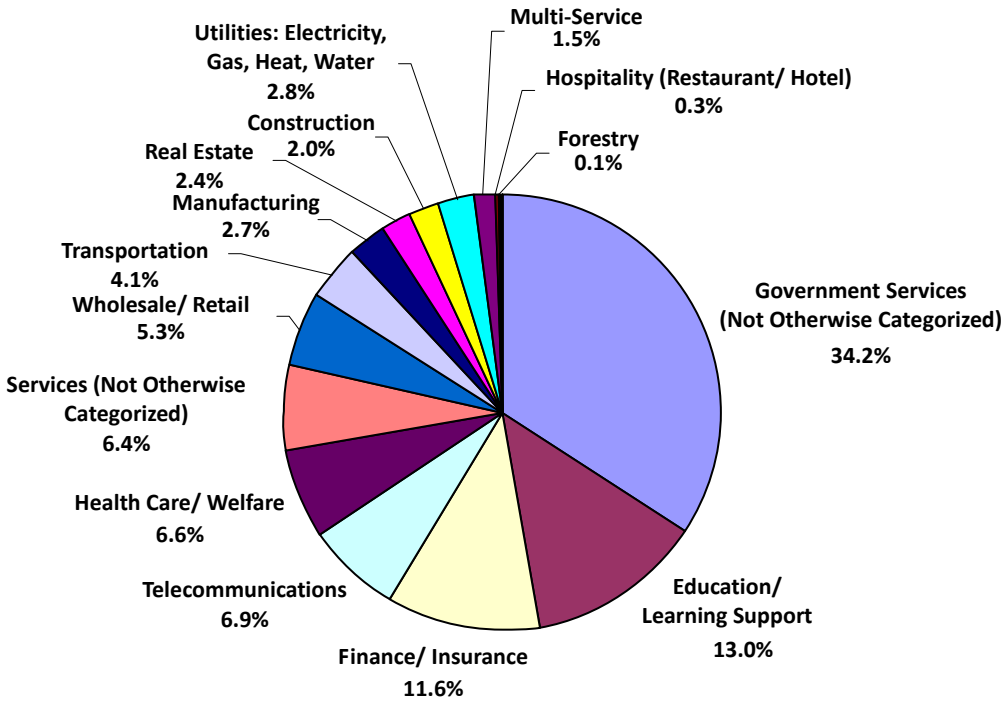


Figure 1: Ratio by Industry Type (Number of Incidents)

Government Services represented the highest ratio of incidents by industry type (34.2%), followed by Education/ Learning Support (13.0%), and Finance/ Insurance (11.6%). These three industry types accounted for approximately 60% of all incidents.

Government Services and Finance/ Insurance represent two types of industries in which the protection of personal information is strictly enforced. Even relatively minor incidents are reported in numbers, which is likely why these industries have remained at the top of this list for the past five years. Of the 18 industry types, only the Farming, Fisheries, and Mining industries did not experience an incident during 2008. The remaining 15 industries experienced information leakage incidents to one extent or another, with the top ten industry types accounting for more than 90% of all incidents. The fact remains that most industry types deal with personal information, and most industry types are at risk for the occurrence of an information leakage incident.

(2) Interannual Analysis (Number of Incidents)

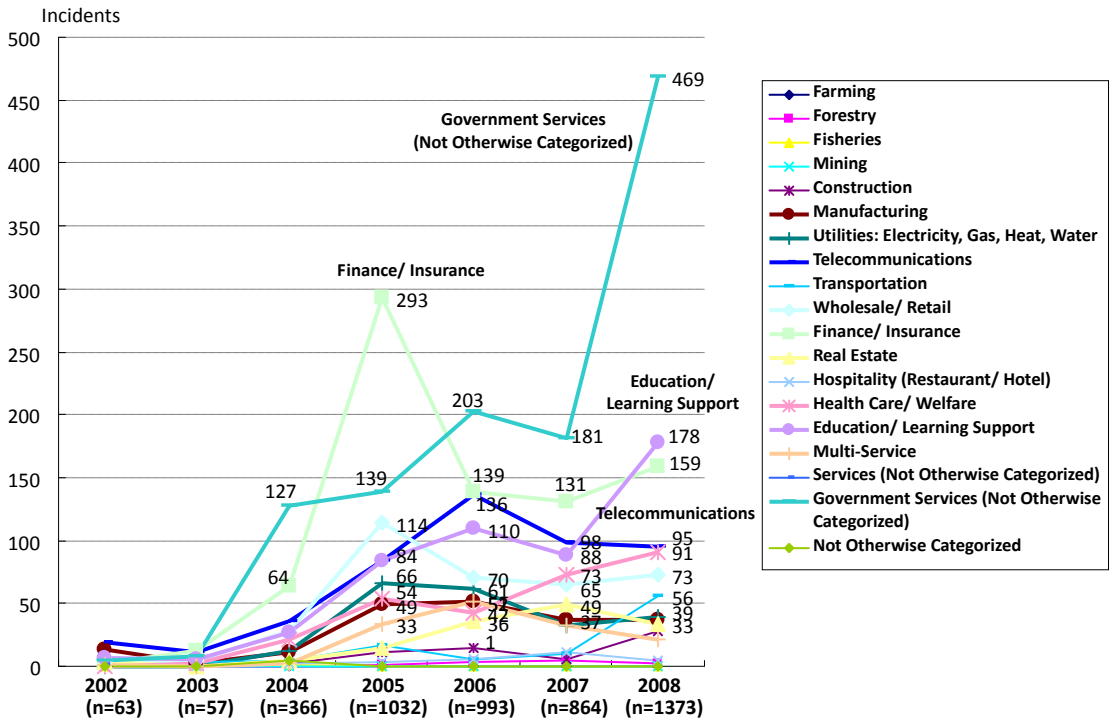


Figure 2: Interannual Changes in Number of Incidents by Industry Type (Number of Incidents)

Figure 2 shows the number of incidents by industry type as a line graph. Excluding 2007, the number of incidents in the Government Services industry has increased nearly every year. The Education/ Learning Support industry has also showed annual increases, except for 2007. In contrast, the Telecommunications industry has experienced slight declines after hitting a peak in 2006.

We believe that the number one factor behind the increase in incidents for the Government Services and Education/ Learning Support industries is that these industries have started to be more conscientious about reporting incidents. Other factors include the increase in usage of PCs and USB memory devices for work, the increase in the number of temporary workers in local governments, and the lack of training in preventing information leakage.

(3) Single-Year Analysis (Number of Victims)

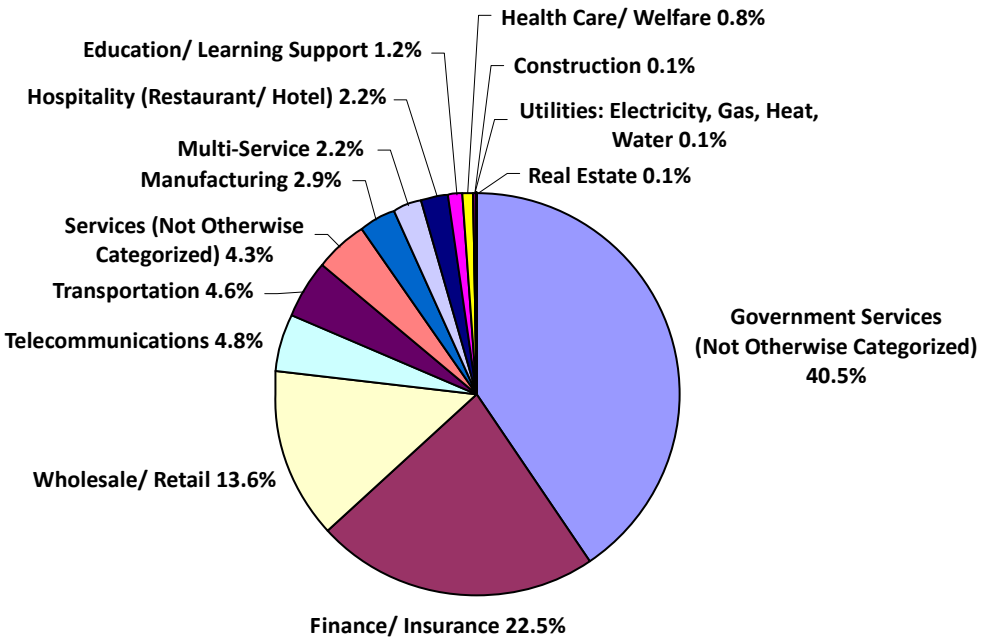


Figure 3: Ratio by Industry Type (Number of Victims)

Government Services (40.5%), Finance/ Insurance (22.5%), and Wholesale/ Retail (13.6%) accounted for the top three industries by number of information leakage victims, representing three-fourths of all people affected.

As shown in Figure 1, Education/ Learning Support accounted for 13.0% of incidents during 2008, but only 1.2% of the number of victims, as shown in Figure 3. We believe that this is due to the fact that much of the personal information involved is on a class-by-class basis, and the scale of incidents is relatively small compared to other industry types. Similarly, the Health Care/ Welfare industry accounts for 6.6% of all incidents, but only 0.8% of victims. This appears to be due to the fact that many incidents were limited to the number of patients handled by a single physician.

In contrast, Wholesale/ Retail accounted for 5.3% of all incidents, but 13.6% of all victims, indicating just how much personal information is handled during the course of providing services.

(4) Interannual Analysis (Number of Victims)

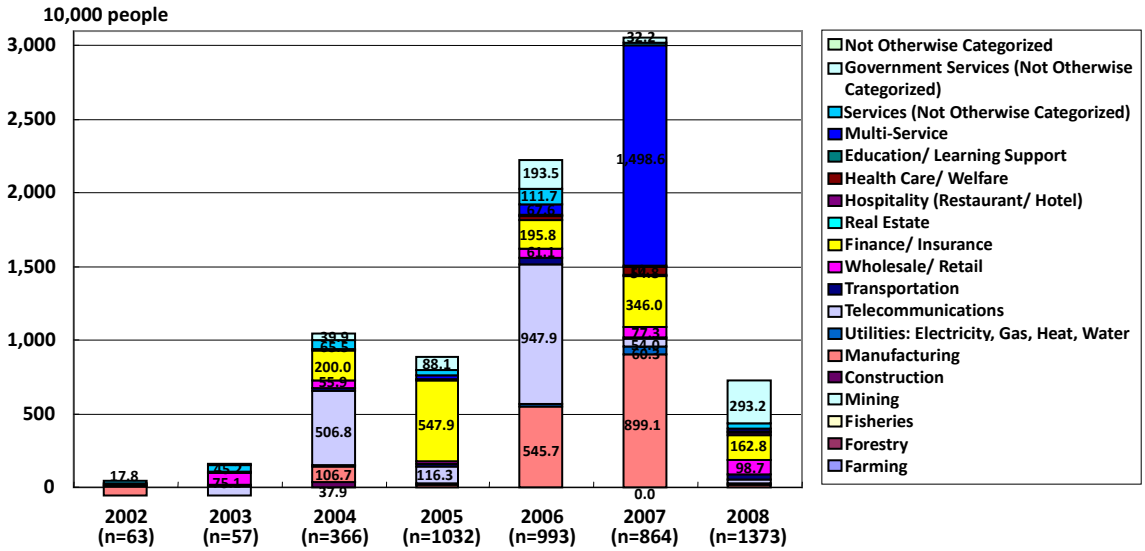


Figure 4: Interannual Changes in the Number of Victims by Industry Type (Total)

Figure 4 is a graph showing the aggregated number of victims of personal information leakage by industry type.

The number of victims experienced year-on-year increases for 2004, 2006 and 2007, each year having a large-scale incident involving more than one million victims. Accordingly, the number of victims for the industry type experiencing a large-scale incident distinctly increased, with Telecommunications standing out in the 2004 and 2006 graphs, and Multi-Service doing the same for 2007. In other words, the presence of a large-scale personal information leakage incident has more to do with the number of incident victims by incident type than any particular industry characteristics.

(5) Correlative Analysis

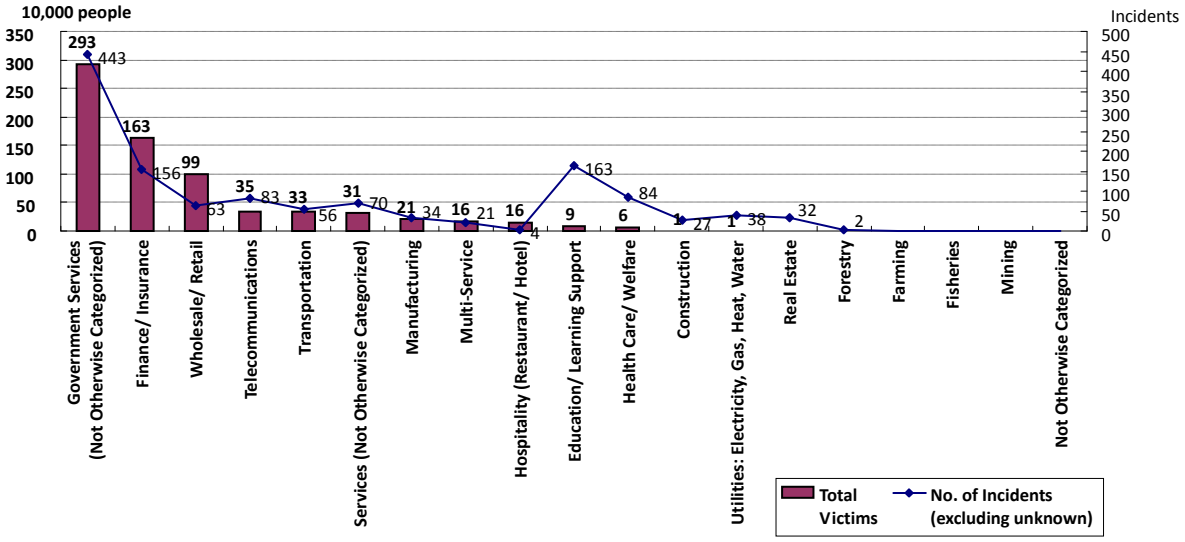


Figure 5: Number of Incidents and Number of Victims by Industry Type

The number of incidents and number of victims traced a nearly proportional relationship during 2008. However, there was notable divergence in the trend for number of incidents and number of victims in the Finance/ Insurance, Wholesale/ Retail, Education/ Learning Support, and Health Care/ Welfare industry types.

The ratio of victims to incidents in the Finance/ Insurance and Wholesale/ Retail industries was high, indicating a high number of victims per incident in these two categories. In the Finance/ Insurance industry, there were a large number of cases where records covering several years were erroneously disposed of. In the Wholesale/ Retail category, several incidents involved the leakage of all of the user data in a central database for Internet shopping websites. In both situations, the nature of the industry involved is such that a single leakage incident involves a large volume of personal data.

In contrast, for the Education/ Learning Support and Health Care/ Welfare categories, the number of victims was relatively low compared to the number of incidents. This analysis shows that in both industry types, despite the high number of opportunities to handle personal information on a daily basis, only a comparative few individuals are involved in each case.

3.5 Cause

(1) Single-Year Analysis (Number of Incidents)

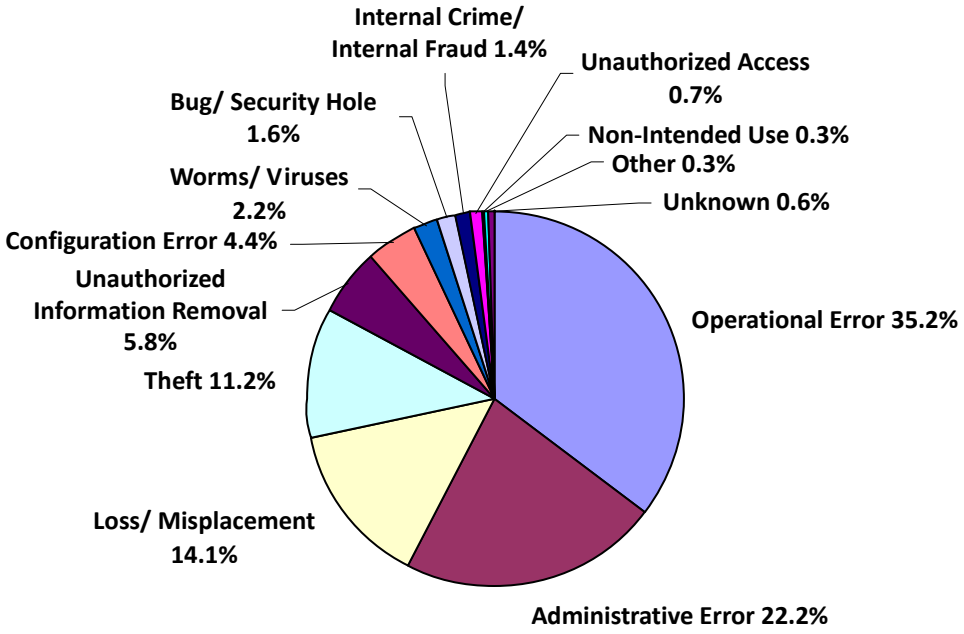


Figure 6: Ratio of Leaks by Cause (Number of Incidents)

Looking at Figure 6, we see that Loss/ Misplacement, Theft, and Operational Error remain the prevalent causes of information leakage. During 2008, Operational Error and Administrative Error both increased as a percentage of the total. In particular, Operational Error experienced a significant increase, representing more than one-third of the total.

Operational Error occurs most frequently in the following order. One can see where an information leakage incident can occur when there is a heavy reliance on manual operations that cannot be countered with technology.

(1) Erroneous delivery of paper media

(2) Misdirected email transmission

(3) Erroneous delivery of a FAX

The erroneous delivery of paper media and erroneous delivery of FAXes occur frequently at local government offices. The main causes of these errors can be attributed to putting the wrong documents in the wrong envelope or forgetting to confirm the recipient—errors that can be prevented by restructuring work steps or establishing stronger systems. Potential preventive measures include rules to prohibit interruptions during delivery preparations, establishing certain work areas, and performing double-checks as important operational and organizational steps leading to stronger systems and structures. A rule requiring any FAX containing personal information be sent using the FAX redial function only after first sending

a test document to confirm the process could be another effective measure.

Misdirected email transmissions occur with comparative frequency in the corporate setting. Incidents similar to the erroneous delivery of paper media discussed above occur frequently, as do the unintentional or intentional inclusion of email addresses in the “To” head that should properly be included in the “Bcc” header. Accordingly, the same measures discussed to prevent the erroneous delivery of paper media and FAXes could be effective, as could the adoption of systems to automate broadcast emails.

The increase of incidents caused by Administrative Error is another notable development for 2008. Administrative Error has continued to increase since 2007, and has become the number two cause of information leaks. Nearly half of administrative errors are the erroneous disposal of information, with many cases involving personal information accidentally disposed of together with other information.

In our opinion, internal controls have played a significant role in this trend, continuing from the prior year. Corporations and other organizations have advanced in sophistication regarding internal controls, including compliance with laws concerning business activities, asset preservation, and controls over IT systems. Accordingly, there has been an increase in the number of organizations that have clarified the standards for when public disclosure is required as one of the steps in dealing with information leakage incidents. The results of our survey have led us to conclude that in addition to stronger internal information controls, these organizations have engaged in physical inventory counts within their facilities, leading to more published reports for erroneous disposal and/ or loss of information. We have seen several cases in which a company or an affiliate has published announcements (additional announcements) concerning information leakage incidents at around the same time. This leads us to believe that once an incident has been discovered, the organization goes on to confirm whether other cases have happened in parallel departments or divisions.

Accordingly, we recommend that organizations perform regular inventory counts to confirm whether information they maintain within their offices is properly managed.

(2) Interannual Analysis (Number of Incidents)

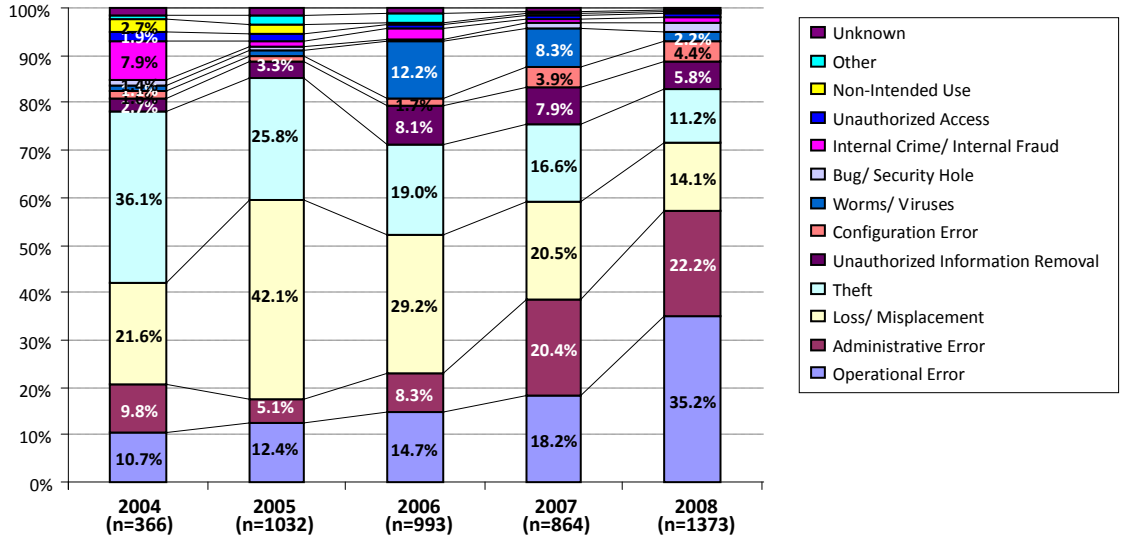


Figure 7: Interannual Changes in the Ratio of Leaks by Cause (Number of Incidents)

After reaching a peak of 42.1% in 2005, the ratio of Loss/ Misplacement as a cause of information leak has continued to decline. The ratio of Theft has similarly traced a declining trend. Since 2006, Operational Error and Administrative Error have been on the increase as cited causes of information leaks. The increase in Administrative Error, which included the erroneous disposal or loss of information within an organization's physical facilities, is related to the increase in small-scale incidents involving paper media. We believe there are two main causes for this trend. First, we believe that organizations have taken steps to prevent the removal of personal information from their facilities, resulting in a decrease of information leaks due to Loss/ Misplacement and Theft—factors that had accounted for a high ratio of incidents in the past. In other words, the target of measures related to personal information management systems and methods focused on areas that had been neglected. Further, as mentioned earlier, the increase in the number of organizations that have clearly defined the standards as to when public disclosure of an incident is required as part of their response to an incident has also had an impact in this area. Second, the cause of incidents in the Finance/ Insurance industry attributed to Loss in 2005 has, from the standpoint of internal controls in 2007, come to be categorized in public announcements as Administrative Error.

While not shown in Figure 7, the number of incidents attributed to information leakage due to P2P file-sharing software declined from 142 incidents in 2007 to 67 incidents in 2008. We believe that prohibiting the use of P2P file-sharing software within organizations, and stricter management/ rules regarding the removal of sensitive personal information have been effective measures in reducing the number of incidents attributed to this cause.

(3) Single-Year Analysis (Number of Victims)

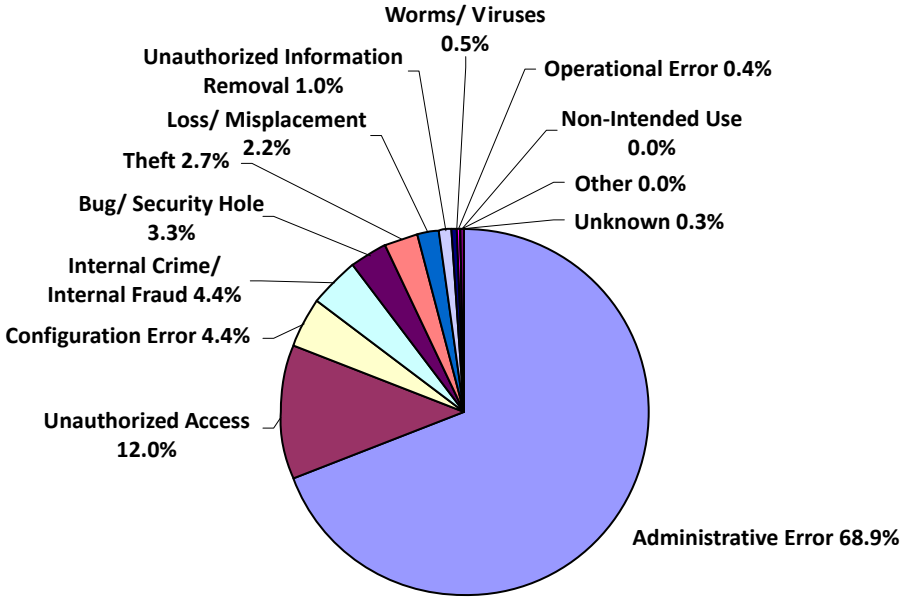


Figure 8: Ratio of Leaks by Cause (Number of Victims)

Looking at Figure 8, we see that compared to 2007, the ratio of Loss/ Misplacement and Theft as causes of information leakage has experienced a decline. Information leakage attributed to Loss/ Misplacement decreased from approximately 460,000 to 160,000 victims, with Theft falling from 580,000 to 200,000 victims. While the ratio of Administrative Error is extremely large, compared to 2007, the number of victims fell by a wide margin, from 19.56 million to 4.98 million. One would tend to conclude falsely that the increase in ratio would lead to an increase in the number of victims. However, we wish to point out that in this case, the number of victims as a whole decreased.

3.6 Leakage Media/ Route

(1) Single-Year Analysis (Number of Incidents)

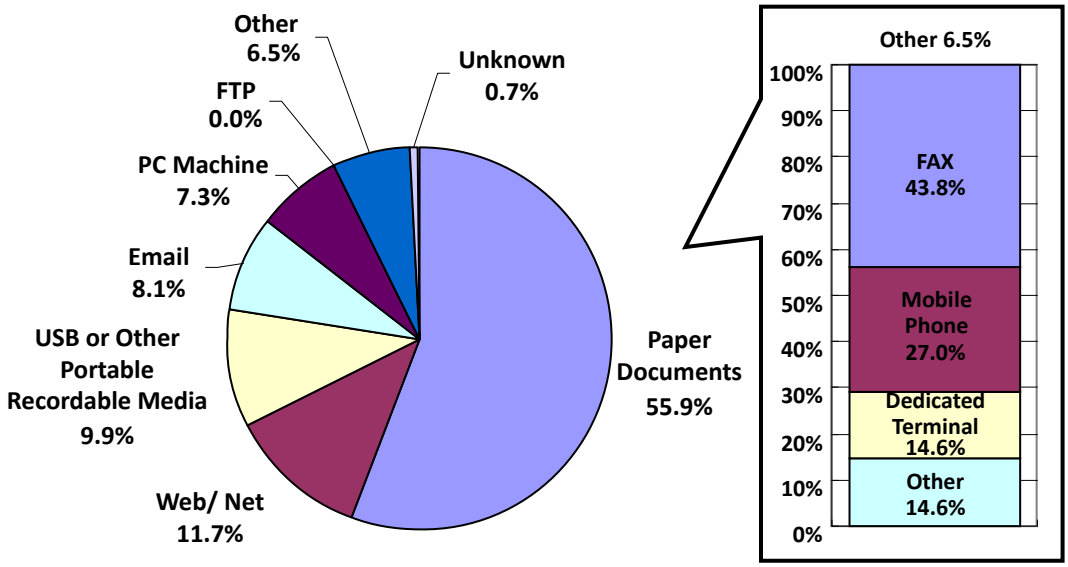


Figure 9: Leakage Media/ Route Ratio (Number of Incidents)

The leakage media/ route contributing to the highest number of information leakage incidents was Paper Documents, with Operational Error, Administrative Error, Theft, and Loss/ Misplacement being the most frequent underlying causes.

Web/ Net is the second-most-frequent route, with approximately 40% of such incidents attributed to Winny and other file-sharing software. This route continues to make up a significant portion of incidents as in 2007.

(2) Interannual Analysis (Number of Incidents)

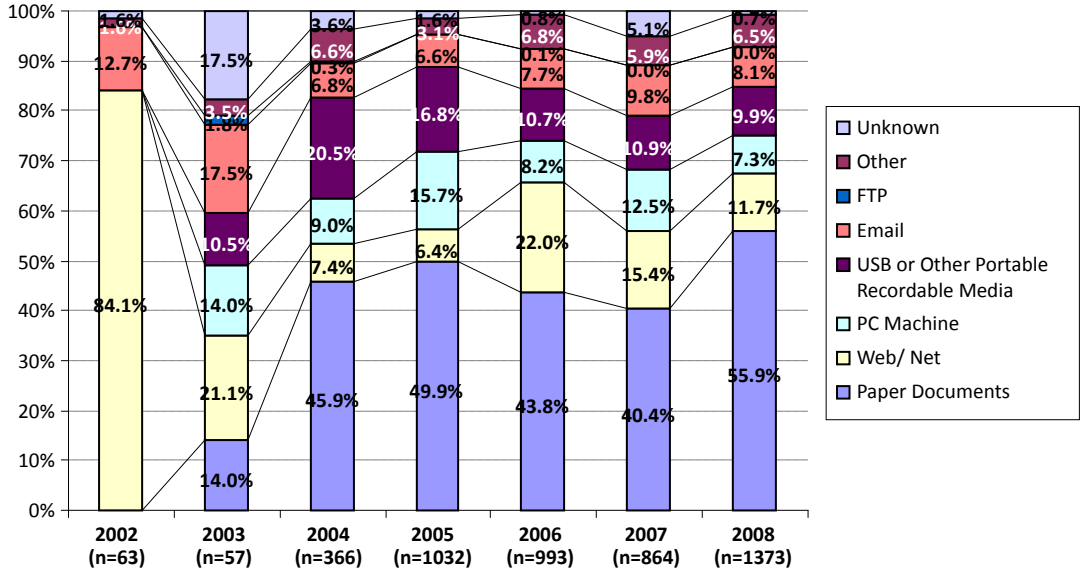


Figure 10: Interannual Changes in Leakage Route Ratio (Number of Incidents)

The incidence of leakage attributed to Paper Documents decreased between 2005 and 2007; however, the number increased to 769 incidents (56.0%) in 2008, compared to 349 incidents (40.4%) in 2007. The ratio of incidents attributed to media/ routes other than Paper Documents decreased, but this was really a relative change due to the increase in ratio for Paper Documents.

USB or Other Portable Recordable Media decreased as a ratio; however, the number of incidents grew from 94 in the prior year to 136—not what one would call an improvement. PC Machine likewise declined as a ratio, but the number of incidents did not show an improvement, with 2008 levels nearly unchanged from 2007.

(3) Single-Year Analysis (Number of Victims)

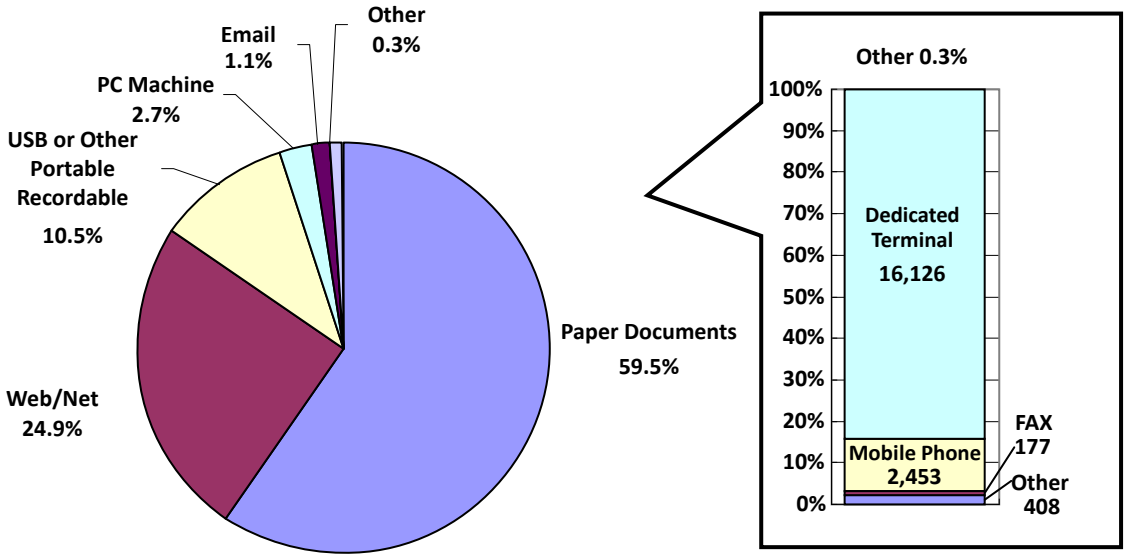


Figure 11: Leakage Media/ Route Ratio (Number of Victims)

Under the category of Paper Documents, there were many incidents involving fewer than 10 and fewer than 100 victims, but incidents involving 100,000 or more victims also occurred. As a result, this leakage route accounted for 59.5% of all victims of information leaks during 2008. The ratio represented by Web/ Net experienced a major increase, up from 1.9% in 2007 to 24.9% in 2008, while USB or Other Portable Recordable Media decreased as a percentage from 38.7% in 2007 to 10.5% in 2008.

The underlying cause of information leaks attributed to Paper Documents were, in order, Operational Error (319 incidents), Administrative Error (231 incidents), Loss/ Misplacement (100 incidents), and Theft (68 incidents). The characteristics of the number of victims due to each underlying cause were as follows:

- Operational Error

  Extremely high ratio of incidents in which the number of victims were less than 10
- Administrative Error

  A high ratio of incidents in which the number of victims were less than 100; however, also a high ratio of incidents in which the number of victims were between 1,000 and 5,000
- Loss/ Misplacement, Theft

  Most incidents involved less than 500 victims; high ratio of incidents involving 10 to 100 victims

3.7 Scope of Leakage

(1) Single-Year Analysis (Number of Incidents)

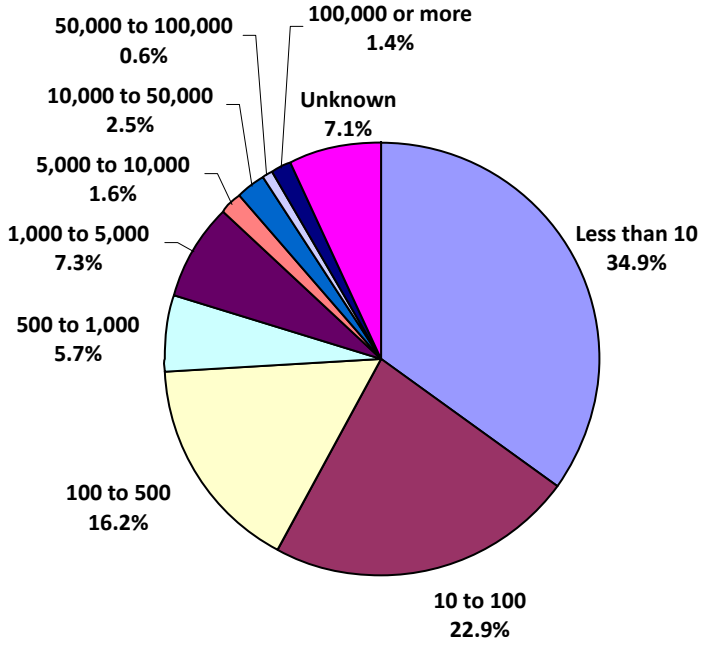


Figure 12: Scope of Leakage by Ratio (Number of Incidents)

According to Figure 12, 34.9% of information leakage incidents involved less than 10 victims, while 22.9% involved between 100 and 500 victims, and 16.2% involved less than 500 victims. Overall, these classifications accounted for 74.0%, or three-fourths of information leakage incidents occurring during 2008. Accordingly, we can see that the vast number of incidents during 2008 involved a relatively few victims. Compared to 2007, the ratio of incidents involving fewer than10 victims rose dramatically from 15.7% to 34.9%. We believe this increase is due to the proactive reporting of small-scale incidents on the part of Japan's organizations.

(2) Interannual Analysis (Number of Incidents)

There were no major shifts in the order of categories (number of victims) between 2005 and 2007, with incidents involving 10 to 100 victims, 100 to 500 victims, and less than 10 victims being most numerous, in that order. During 2008, a total of 79.7% of incidents involved fewer than 1,000 victims, bringing those categories higher as ratio of the total. We can conclude from this that most incidents reported were small-scale affairs involving fewer than 1,000 victims. The ratio of incidents involving fewer than 10 victims rose dramatically during 2008.

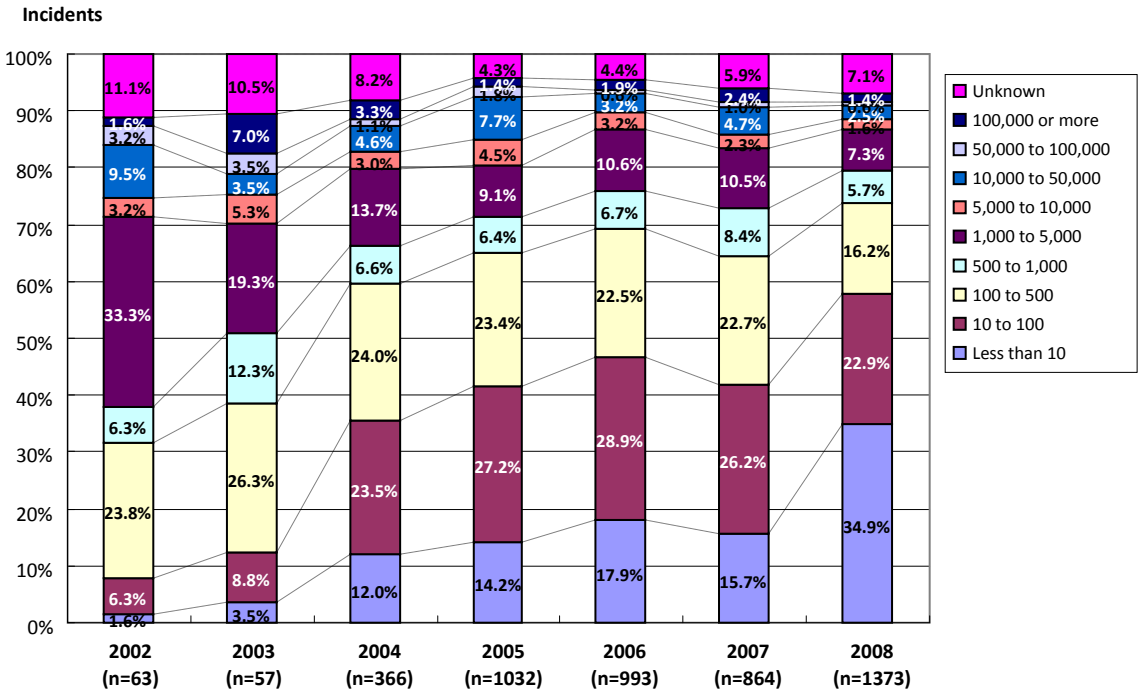


Figure 13: Interannual Changes in the Ratio of Classifications by Victims per Incident (Number of Incidents)

Addressing regular corporations in Japan, “businesses dealing with personal information” falling under the Personal Information Protection Act are those maintaining personal information for 5,000 individuals or more. However, under the Act on the Protection of Personal Information Held by Administrative Organs and other laws targeting government agencies and independent administrative agencies, the tendency is to report even minor incidents involving one victim, conscious of the duty to safely administer the information held by the agency in question. We believe that this is one factor behind the higher ratio of small-scale incidents reported during 2008.

3.8 Interannual Analysis

We performed various analyses based on seven years of incident data collected between 2002 and 2008. However, prior to 2004, few incidents were publicly reported, and those incidents that were reported involved major volumes of personal information. Accordingly, incidents during these years tended to skew the statistical data significantly, and should be viewed more as reference figures in the context of our analysis.

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

	Number of Incidents	Number of Victims	Average Number of Victims per Incident*
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
2008	1,373	7,232,763	5,668

At 1,373 incidents, 2008 represented the highest occurrence of reported information leakage since we began collecting statistics in 2002. At the same time, the lack of a large-scale incident during 2008 resulted in the lowest total of victims since 2004, at 7,232,763—approximately 24% and 33% lower than 2007 and 2006 respectively. This figure calculates to approximately one out of every 18 people in Japan, representing a reversal from last year's record high numbers, and a historical low of 5,668 victims per incident on average.

While a record number of incidents occurred during 2008, the average number of victims was the lowest ever. While the fact that a large-scale incident did not occur during 2008 was certainly one contributing factor, we have also considered a greater general public awareness of personal information protection has led organizations to report incidents—even small-scale incidents—more conscientiously.

* Our calculations used 1,276 incidents as the parameter for average number of victims during 2008 (1,363 incidents less 87 incidents in which the number of victims was undetermined).

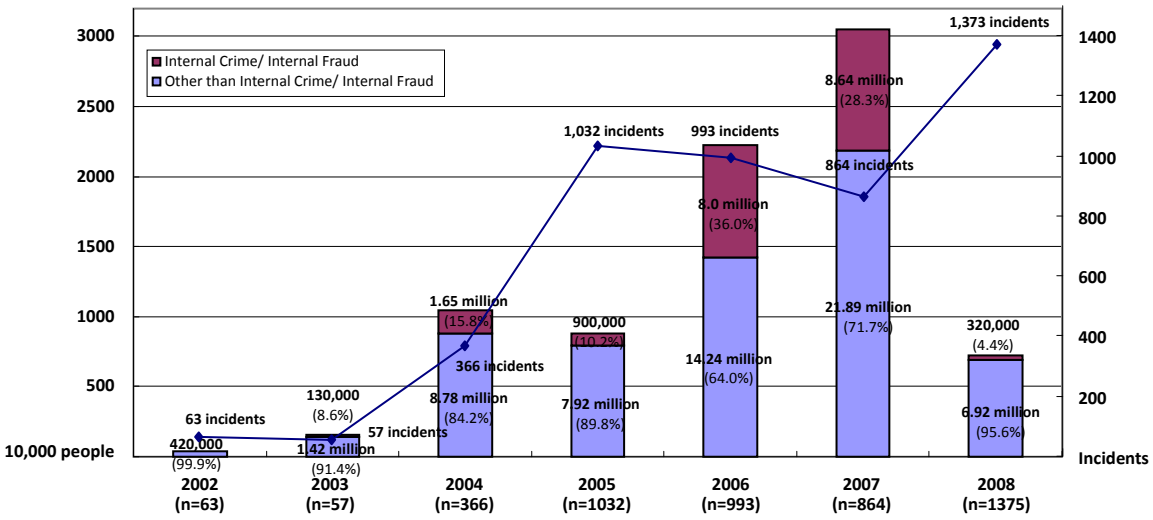


Figure 14: Interannual Changes in the Number of Incidents and Number of Victims due to Internal Fraud (Total)

Since 2005, when the Personal Information Protection Act came into full enforcement, about 1,000 personal information leakage incidents have been reported in newspapers and Internet news sites each year. 2008 represented the highest number of incidents reported, at 1,373. Despite the tendency in the news media to not report incidents that do not contain elements of novelty or "news," the sheer number of incidents reported on a yearly basis demonstrates that organizations now accept that public reporting of incidents acts as both an apology and a public relations measure, asking the cooperation of the news media.

At the same time, the increase in the number of victims between 2005 and 2007 has now clearly reversed. While we would like to think that this trend stems from improved security and the wide-scale implementation of proper precautions, we see that incidents involving between 5,000 and one million victims was nearly the same as in 2007, with no discernible decrease. In fact, we believe that this development was mainly due to the lack of an unexpectedly large-scale incident of more than one million victims during 2008.

In addition, while the number of victims in incidents attributable to Internal Crime/ Internal Fraud during 2006 and 2007 exceeded eight million each year, the corresponding figure for 2008 was only 320,000. We believe that greater internal authorization control and prohibitions on removing information from an organization's premises contributed to making theft and unauthorized activities more difficult.

4 2008 Projected Compensations for Damages Calculation

4.1 Total Projected Compensation for Damages

Table 4: Interannual Changes in Total Projected Compensation for Damages

	Total Projected Compensation for Damages
2002	Approx. ¥18.9 billion
2003	Approx. ¥28.1 billion
2004	Approx. ¥466.7 billion
2005	Approx. ¥700.2 billion
2006	Approx. ¥457.0 billion
2007	Approx. ¥2.2711 trillion
2008	Approx. ¥236.7 billion

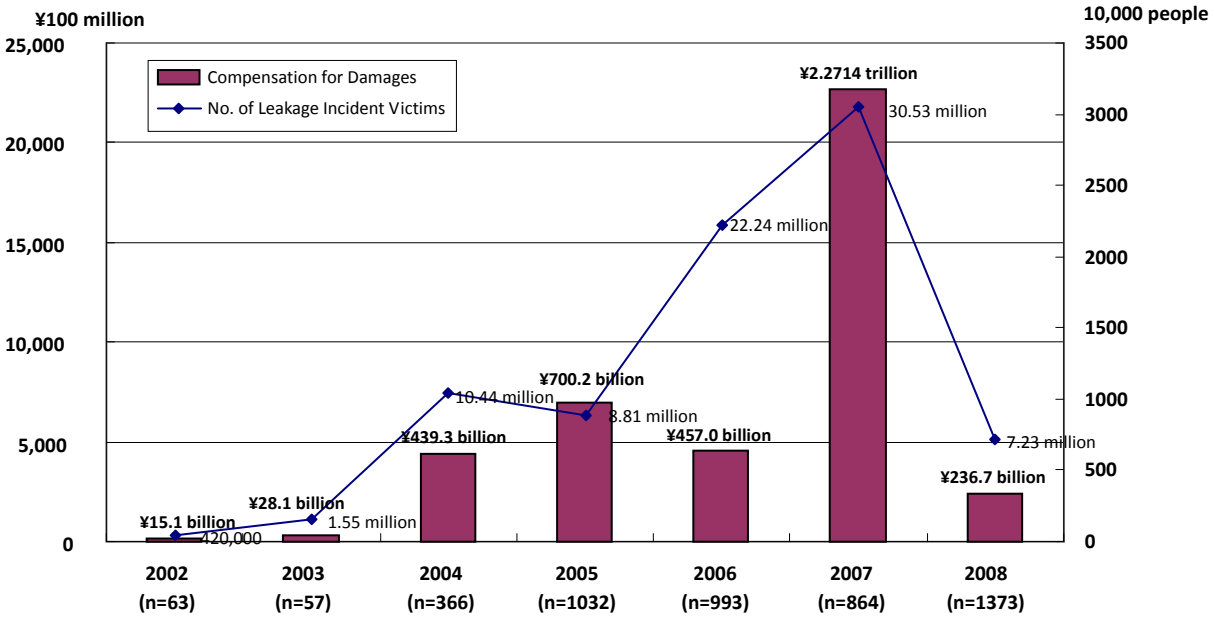


Figure 15: Total Projected Compensation for Damages and Number of Victims

During 2007, the value of personal information and number of large-scale leakage incidents resulted in a major increase in the total projected compensation for damages. For 2008, total damages are comparatively low, due mainly to the good fortune of not having a large-scale incident during the year.

However, considering the increase in the number of incidents, it is difficult to categorically declare that a lower compensation for damages is reflective of an advanced structure of information security. Whether these numbers remain low depends mainly on the occurrence or non-occurrence of a large-scale incident.

In addition, the number of victims has experienced a significant decrease. Again, considering the increase in the number of incidents, we cannot say that information security has advanced so much as that organizations are now tending to report incidents regardless of the number of people affected. We must also consider the possibility that the

implementation of measures has resulted in a limit to the number of victims in any given incident.

4.2 Projected Compensation for Damages per Person

(1) Single-Year Analysis

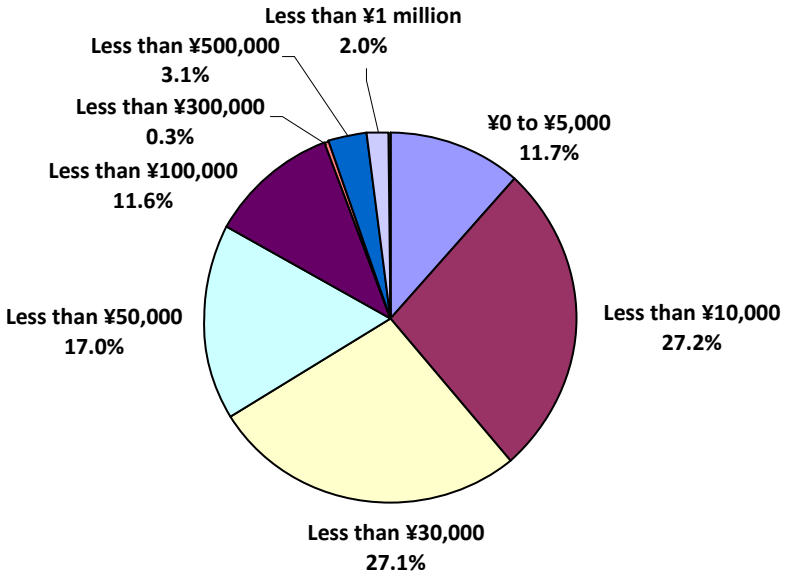


Figure 16: Ratio of Projected Compensation for Damages per Person (Number of Incidents)

For 2008, projected compensation for damages per person of between ¥5,000 and ¥10,000 accounted for the highest ratio of incidents, at 27.2%. Projected compensation for damages per person between ¥10,000 and ¥30,000 came in second, at 27.1%.

(2) Interannual Analysis

Table 5: Average Projected Compensation for Damages per Person

2002	¥16,855
2003	¥89,140
2004	¥105,365
2005	¥46,271
2006	¥36,743
2007	¥38,233
2008	¥43,632

For 2007, the average projected compensation for damages per person calculated out to ¥38,233. This number increased slightly to ¥43,632 for 2008, but figures have remained nearly equivalent year-to-year since 2005.

[Average Projected Compensation for Damages per Person]

We calculated the projected compensation for damages per person for each incident that occurred during 2008. The average projected compensation for damages per person was calculated as the average monetary amount of the projected compensation for damages for each incident. Accordingly, we calculated the average projected compensation for damages per person by totaling the projected compensation for damages per person for all incidents, and then dividing by the number of incidents. Please not that the figure we arrived at is not the total amount of projected compensation for damages divided by the total number of victims.

The following is our calculation formula and a specific calculation example:

For the two following incidents:

Projected compensation for damages per person for Incident A = ¥a

Projected compensation for damages per person for Incident B = ¥b

Average Projected Compensation for Damages per Person = (¥a + ¥b) / 2 incidents

■Example

Table 6: Incident Details (specific example)

	Number of Victims	Total Projected Compensation for Damages	Projected Compensation for Damages per Person
Incident A	1	¥1,000,000	¥1,000,000
Incident B	100	¥1,000,000	¥10,000

Table 7: Projected Compensation for Damages per Person (specific example)

	Number of Victims	Projected Compensation for Damages per Person
Divided by the number of people	101	¥2,000,000 ÷ 101 = ¥19,800
Calculation per this report	101	(¥1,000,000 + 10,000) ÷ 2 incidents = ¥505,000

The following shows the interannual changes in the ratio of projected compensations for damages per person in a graph and by actual number of incidents.

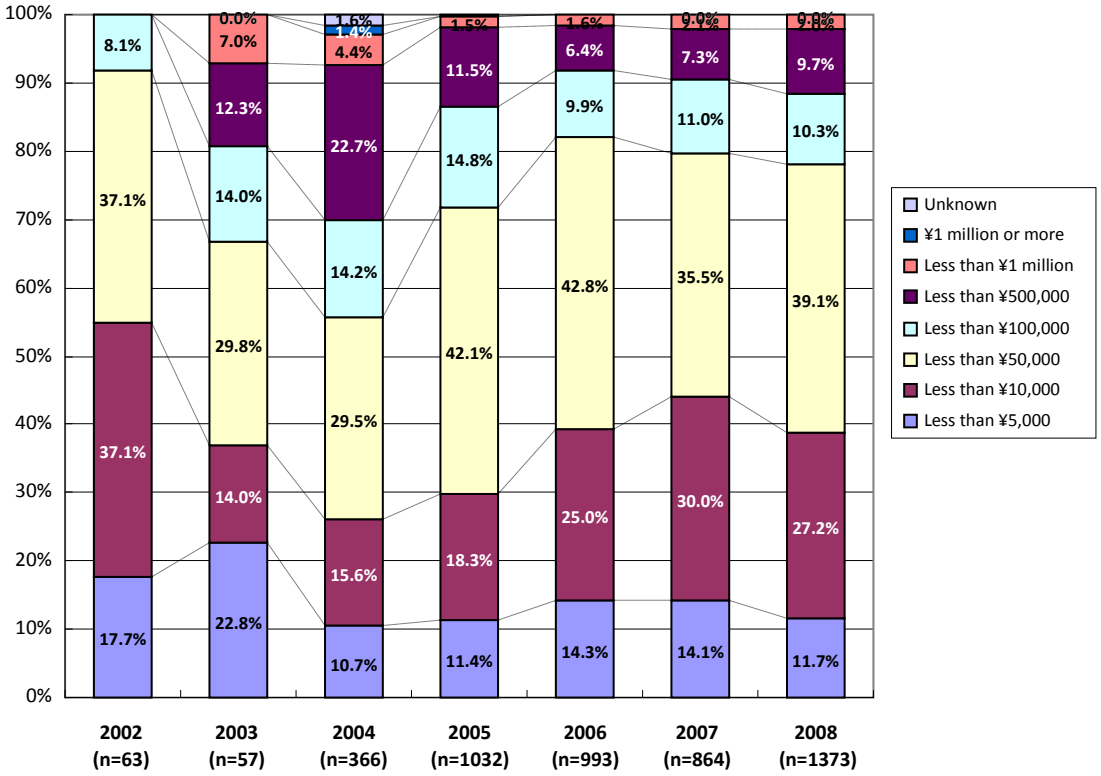


Figure 17: Interannual Changes in the Ratio of Projected Compensation for Damages per Person (Number of Incidents)

Looking at the ratio of projected compensation for damages per person, we see that despite a slight increase in the ratio of incidents between ¥100,000 and ¥500,000, there have been no significant year-to-year changes overall.

4.3 Projected Compensation for Damages per Incident

(1) Single-Year Analysis

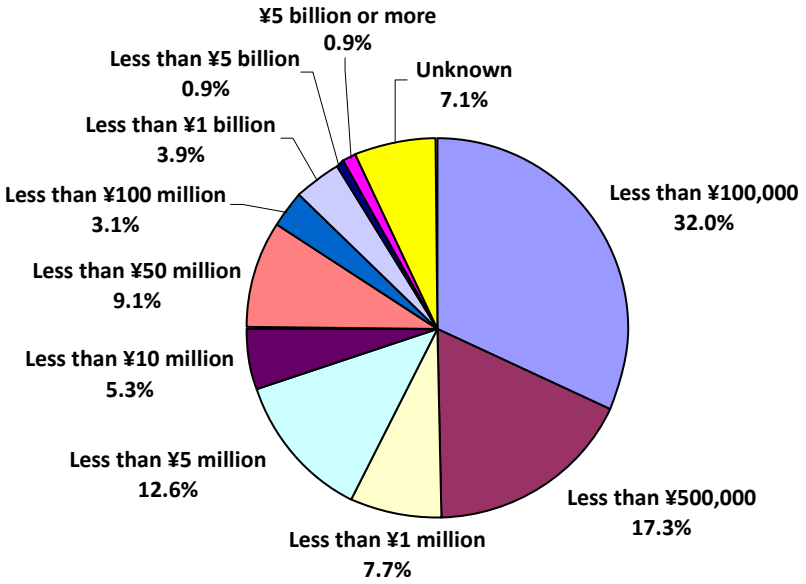


Figure 18: Ratio of Projected Compensation for Damages per Incident (Number of Incidents)

Under the projected compensation for damages, incidents of less than ¥500,000 account for approximately half of the total, with incidents of between ¥500,000 and ¥5,000,000 representing 20.3% of the total.

This result indicates that small-scale incidents in terms of projected compensation for damages (less than ¥100,000; between ¥100,000 and ¥500,000) involving information of low value occurred most frequently.

(2) Interannual Analysis

The total projected compensation for damages for 2008 decreased markedly compared to 2007, which was the highest to date. In order of financial impact, the 2008 figure came in below that of 2004, the year prior to the full enforcement of the Personal Information Protection Act.

This development stems from the trends in evidence for incidents that occurred during 2008. The first reason is that, despite a significant increase in the number of information leakage incidents, a relatively low number of victims were involved in any particular incident. Second, there were very few incidents that involved a large volume of sensitive information, and there were not incidents involving a major amount of projected compensation for damages. Based on these two factors, the total amount of projected compensation for damages decreased compared to the prior year.

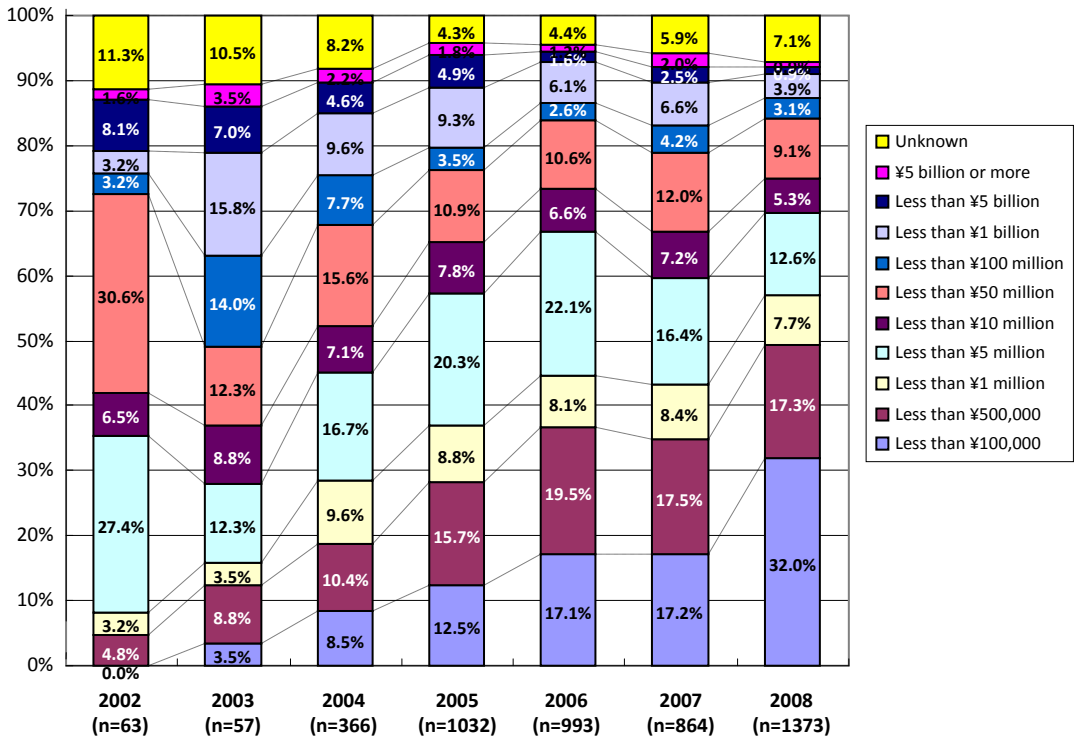


Figure 19: Interannual Changes in the Ratio of Projected Compensation for Damages per Incident (Number of Incidents)

As in past years, 2008 continued the trend toward an increase in incidents for which the projected compensation for damages is less than ¥100,000.

With no large-scale incidents during 2008, we noted a decrease in the ratio of incidents involving large amounts of projected compensation. However, corporate managers would be ill advised to relax too much, given the fact that an average of six incidents per month (78 incidents) involved projected compensation for damages in excess of ¥100,000,000.

4.4 Summary: Projected Compensation for Damages

We can summarize the trends for total projected compensation for damages during 2008 under the following two points:

- Including two large-scale information leakage incidents, there were numerous incidents during 2007 involving projected compensation for damages that vastly exceeded ¥5 billion. In contrast, there was a marked decline in large-scale incidents during 2008, including a decrease in the number of incidents involving projected compensation for damages in excess of ¥5 billion. Accordingly, the total projected compensation for damages during 2008 was notably less than the 2007 figure.

- Due to the low number of victims per information leakage incident for 2008, the per-incident projected compensation for damages was comparatively low. More than 50% of all incidents involved projected compensation for damages of less than ¥1,000,000. Looking at this fact, we can conclude that 2008 was a year characterized by a high number of small-scale incidents.

5 Calculating Projected Compensation for Damages related to Personal Information Leakage

5.1 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 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.

5.2 Explanation of the Projected Compensation for Damages Calculation Model

Our calculations for compensation for damages occurring during 2008 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.

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

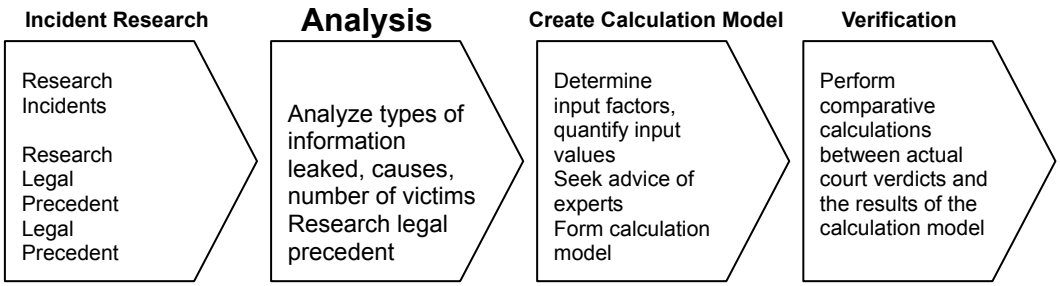


Figure 20: Process behind the Formation of the Projected Compensation for Damages Calculation Model

We developed our calculation model as depicted in Figure 20 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. Analysis Results of Personal Information Leakage Incidents” describes the results of our analysis for 2008.

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.

5.2.2 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.

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

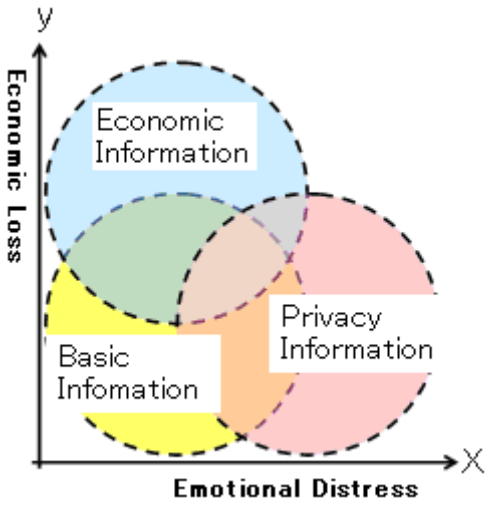


Figure 21: Economic-Privacy Map (EP Map)

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 22).

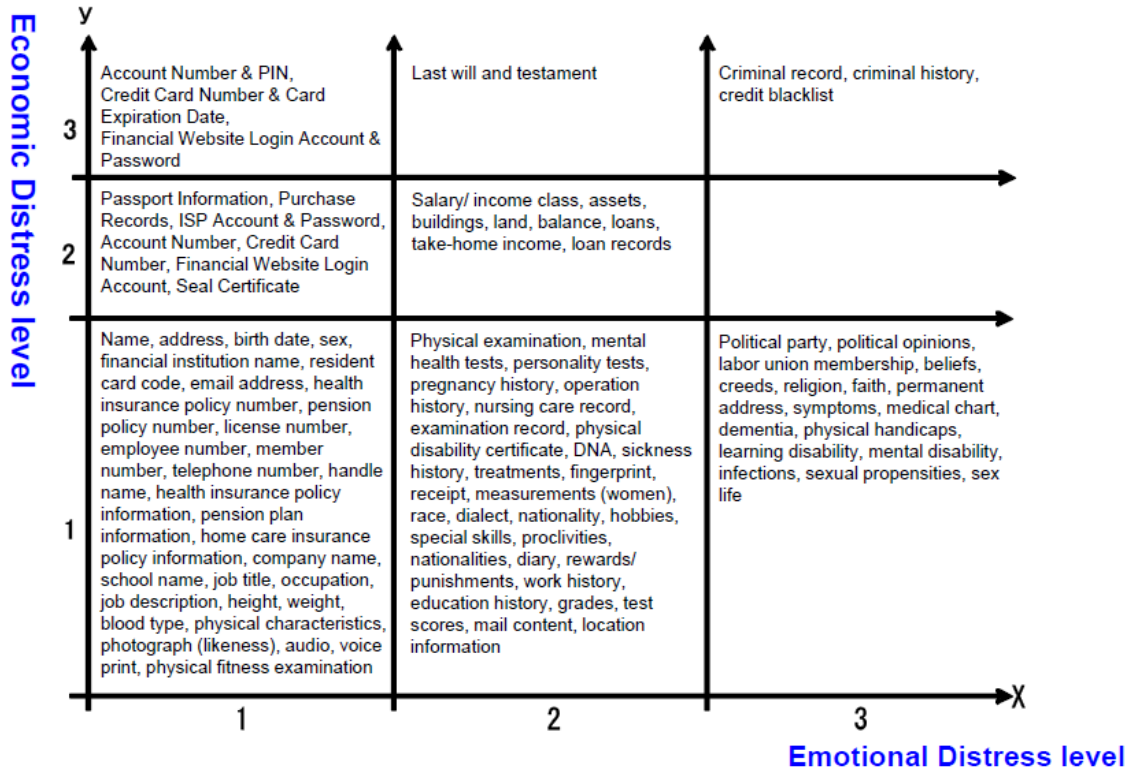


Figure 22: Simple-EP Map

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 8 below.

Table 8: 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

5.2.2.2 Degree of Social Responsibility of the Organization in Question

As shown in Table 9, 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 9: 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

5.2.2.3 Appraisal of Post-Incident Response

The appraised value of Post-Incident Response is based on Table 10 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 10: 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

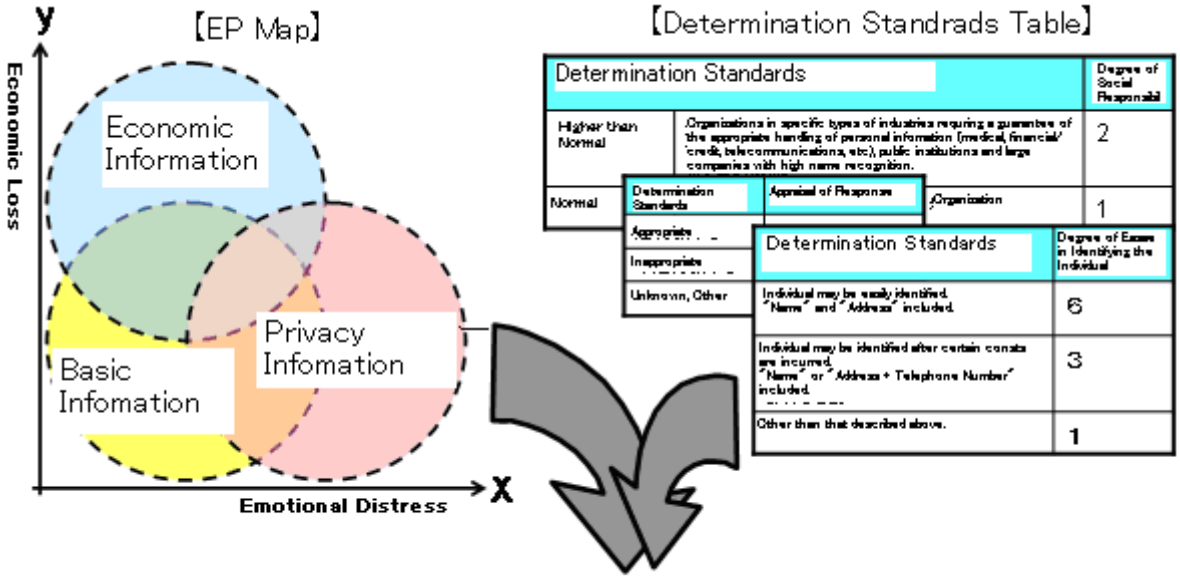
b. Examples of Inappropriate Responses

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

- Measures were implemented, but were ineffective
- False reporting

5.2.3 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." 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 23: JO Model

6 Conclusion

While a record number of information leakage incidents were reported during 2008, the actual number of victims affected was the lowest since 2005. Initially, we attributed this to more conscientious reporting of all incidents regardless of size, as well as the comparative lack of major incidents involving large numbers of victims. However, the number of incidents affecting between 5,000 and 1 million victims remains nearly unchanged from 2007. Accordingly, it is our opinion that the underlying factor behind the decrease in the number of victims for 2008 is the fact that there were no large-scale incidents significantly exceeding 1 million victims. Only one incident occurred during the year large enough to involve approximately 1 million individuals. In other words, through 2007 there was at least one information leakage incident that significantly exceeded 1 million victims, affecting the statistical results.

Similarly, 2008 had a low ratio of incidents involving a high amount of projected compensation for damages. There were approximately 300 incidents for which the projected compensation for damages exceeded ¥5 million, a level remaining nearly unchanged since 2006. A total of 78 incidents involved projected damages in excess of ¥100 million, calculating to a surprisingly high average of six per month. The increase in small-scale incidents involving small amounts of projected compensation for damages resulted in the deceptive appearance of a decrease in incidents involving large amounts of compensation for damages.

The significant increase in the number of leakage incidents involving less than 1,000 victims as mentioned above could be a favorable sign that undiscovered personal information leakage incidents have finally come to light, or that organizations are now more conscientious of reporting such incidents. However, the number of incidents involving 1,000 or more people has remained nearly constant since 2007. This could be an indication of declining returns in measures that have been in place for some time with respect to personal information requiring careful handling. In such a case, we believe that achieving any greater improvements using the same methods is impractical, and new methods should be introduced.

Personal information leakage through paper documents remains a frequent cause of incidents. Paper documents ultimately require manual processing and management, which means an ever-present risk of erroneous disposal or other mishandling as long as the paper is maintained. Paper documents present unique issues, including being difficult to trace in the event of loss, and the fact that paper cannot be encrypted. At present, there a no highly effective measures against personal information leakage through paper documents, and we anticipate that incidents attributed to this cause will remain a frequent occurrence.

This is why we believe, despite a certain level of adoption of anti-leakage measures, operational error and other careless mistakes have played a role in the reason why the number of incidents have not decreased. Even with set office rules and secure work steps, improved awareness through organizational education, etc., human intervention is always necessary at some point during the handling of information. Accordingly, operational error or other careless mistakes are going to occur at some minimum level. While triple-checks can be expected to reduce careless mistakes, compared to double checks, some experiments have shown mistakes to actually increase. Rather than relying either on software measures or operational measures (workflow, double-checks), we believe that the most effective approach is to implement the best measure for the particular situation.

However, it remains a difficult task to prevent internal crime due to the unauthorized acts of a manager or other individual with authority. Internal crime is facilitated by a certain existing level of authorization, which limits the effectiveness of system-based preventive measures. Accordingly, countermeasures designed to defeat internal crime focus on monitoring logs, etc. rather than the prevention of the act. Individuals having a certain level of authority who intend to commit a crime will already know about the presence and details of monitoring systems, potentially being able to evade or turn such systems off. In other words, there are many cases in which monitoring as a fraud prevention measure is not reliable or cost effective, since such measures cannot actually prevent the act from happening in the first place. Obviously, security education will not be effective for an individual predisposed to committing a crime. Keeping those with authority from seeing organizational/ systemic weaknesses (crime opportunity theory) is an effective measure against internal crime. However, such effectiveness is limited to those individuals who do not have a strong desire to commit a crime.

In our 2008 survey, we noted instances of retirees or temporary staff whose contracts have expired removing confidential or personal information, leading to a leakage incident. We believe that these types of incidents can be prevented by employing the crime opportunity theory, clarifying staff retirement procedures, and otherwise preventing opportunities to remove information from within the organization.

Given that the number of victims of information leakage during 2008 was at the lowest level since 2005, we can conclude that comprehensive technological and organizational measures against information leakage are being adopted in industries that have a major impact on society. However, in contrast to other years, there were no unexpected large-scale incidents that significantly surpassed 1 million victims, while the number of

incidents involving 1,000 or more victims remained at the same level as prior years.

We believe that in the four years that have passed since the complete enforcement of the Personal Information Protection Act, organizations dealing with large volumes of sensitive personal information have paid more attention to implementing proper measures and handling procedures. However, excluding the effects of some measures such as against P2P file-sharing software, we cannot say with conviction that overall improvements have been made. We urge organizations to continue to adopt both systematic and operational anti-leakage measures, while at the same time implementing systems designed to be effective for their particular circumstances, adopting both systematic and operational anti-leakage measures.

7 Contact Information

Please submit any comments or questions about quoting sections of this report through the inquiry form found at the JNSA website.
*Our system does not provide a confirmation in response to quote inquiries made through this form. Thank you for your understanding.

A FAQ sheet about this report is also available at our website. Please refer to this FAQ regarding comments or questions about quoting sections of this report.
http://www.jnsa.org/faq/incident.html

■Inquiry Form

Quote inquiry and comment form:
URL: https://www.jnsa.org/aboutus/quote.html

8 Appendix Definitions for Causes of Information Leakage

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

Table 11: 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 Administrative 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.
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 Administrative Error. − Categorized as Administrative 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.

Category	Specific Example	Determination Criteria
Administrative 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 administrative 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 (Administrative Error).
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.