Fiscal 2003

Information Security Incident Survey Report

<Section Two>

Estimated Damages Resulting from Information Disclosure and Other Observations (Compensatory Damages and Effect on Share Prices)

Japan Network Security Association

March 31 2004

Table of Contents

JNSA SEISAKU COMMITTEE　SECURITY INCIDENTS INVESTIGATION WORKING GROUP

Working Group Leader

Mr. Tadashi Yamamoto	Sompo Japan Risk Management, Inc.

Working Group Members

Mr. Tomoharu Sato	Internet Research Institute, Inc.
Mr. Hisamichi Otani	NTT Data Corporation
Mr. Kenji Okada	ELNIS Technologies, Co., Ltd.
Mr. Ikuo Sugitani	Global Ace, Inc.
Mr. Hideaki Kusunoki	Computer Associates International, Inc.
Mr. Hironori Omizo	JMC
Mr. Kazuki Yonezawa	Secure Computing Japan KK
Mr. Takayuki Endo	SECOM, Co., Ltd.
Mr. Shuichi Okamoto	Sompo Japan Risk Management, Inc.
Mr. Eiji Yamada	dit Co,. Ltd.
Mr. Tadayoshi Yasuda	dit Co,. Ltd.
Mr. Tomohisa Sashida	Tokio Marine Risk Consulting Co., Ltd.
Mr. Kiyoshi Nagashima	Tokio Marine & Fire Insurance Company, Ltd.
Mr. Tomoki Sano	TOPPAN Printing Co., Ltd.
Mr. Koichi Narusawa	TOPPAN Printing Co., Ltd.
Mr. Shiro Maruyama	Little eArth Corporation
Mr. Yukihiro Matsuya	HUCOM Incorporated
Mr. Yasuhiko Sato	SRA (Software Research Associates, Inc.)

1. Introduction

The JAPAN NETWORK SECURITY ASSOCIATION (JNSA) sponsors working group activities across a range of fields from technology to corporate management. This report represents the results of the Third Annual Information Security Incident Survey Project, as was carried out last year by the working group.

<About Section Two>

The Calculation Model presented herein considers not only damage caused to information systems by information security incidents, but also incorporates related damages such as compensatory legal reparations. This report also includes further observations and considerations related to "the possibility of compensatory legal reparations in connection with the negligent disclosure of personal information" which was also covered in last year's report, and proposes a model to calculate reparations amounts reflecting the "privacy factor" and the "economic factor" of personal information. Further, we conducted another set of case study investigations related to the "Influence on Share Prices" (one part of overall corporate value) of such incidents.
The "Calculation of Legal Reparations" and "Influence on Share Prices" suggested in this report represent a calculation methodology proposed by this Working Group, and are in no way meant to be definitive.

Having said this, our hope is that these indices give impetus to experts to raise questions on parallel themes, and to develop approaches from a variety of directions. At the same time, we hope this report serves to help corporate management focus on the presence and scale of information security risk, and to make intelligent investment decisions.

－Reference－

<About Section One (Separate Document)>

The JNSA Seisaku Committee's "Information Security Incidents Investigation Working Group" conducted its third annual survey of major corporations representing Japan's core industries as well as information technology companies. The survey consisted of sending questionnaires (exceeding in number of the previous year) to these entities, and conducting follow-up interviews with companies willing to participate. This year, the survey was conducted with the cooperation of JNSA members and the Research Institute of Science and Technology for Society (RISTEX).

Section One of this report details the actual damages caused by information security incidents, and investment in preventive measures incurred by companies responding to the survey. In addition, we will present our opinions regarding expansion of the scope of what should be considered "damages" at present and suggest further modifications to the Calculation Model (representing damages caused by information security incidents and costs of countermeasures) presented in earlier years, based on the results of this survey.

2. Objectives

Section Two deals with “information disclosure,” a type of incident involving major social implications, and an increasing number of victims. This “accidental disclosure of private information” is a danger held in common by all corporations, and naturally a risk worthy of corporate management concern in the light of the Personal Information Protection Act being partially enacted.

The objective of the research and proposals of this Working Group is to serve as a catalyst for future discussions centered on the “potential for legal reparations” and “influence on share prices” related to the disclosures of private information, as well as to help corporate management identify the scale of information security risk and make intelligent investment decisions.

3. Calculating Compensatory Damages Resulting From Personal Information Disclosure

In the same way as we are seeing an increasing expansion of the Internet and the networked society in recent years, we are also seeing a sudden growth in public consciousness as regards the protection of personal information. Because of both an increase in the scale of information disclosure incidents resulting from increased system sizes, and of the increased newsworthiness of these, incidents of information disclosure have a major adverse influence upon companies from which these leaks occur.

Having personal information and yet being unable to appropriately manage it is very risky. Damage that occurred as a result of the disclosure of personal information, and for which appropriate funds to prevent such disclosure had not been spent prior to that point are regarded as “scandals,” however in 2002, companies from which information has been divulged became subject to more specific “financial damages,” as a result of a decision being made regarding responsibility for damages.

The working group attempted to compute actual sums of damage for disclosure of information. These calculations covered the “quantity of compensatory damages” from class action lawsuits by victims of information disclosure, and investigated the “effect on share pricing” as a part of overall corporate value.

Especially in Japan, share prices may drop as has been the case with certain foodstuffs companies, however because people have short memories, as long as companies are not actually liquidated, then things generally revert to as they were.

However, while there is an end to the strongly growing economy, corporate management responsibility is towards not only customers of products and services, but also shareholders, leading to an expansion in business responsibility and in the acquisition of businesses, and a change in the meaning of owning shares. In the future, we will not be able to overlook this type of indirect influence.

3.1 About the Personal Information Protection Act

There has been a significant increase in the risk to computerized personal information, resulting from both improvements in computers' information processing capabilities, and from the spread of the Internet. Misuse of personal information can lead to damage such as fraudulent procurement and use of accounts, spam mail, and phishing. The Personal Information Protection Act is concerned about these social problems, and specifies fundamental principles and obligations with which organizations in possession of personal information should comply.

Please be aware that the amounts of compensatory damages resulting from personal information disclosure that are covered in this report are significantly different to the fines (or prison sentences) decided by the Personal Information Protection Act.

- Fines in the Personal Information Protection Act

Fines (penalties) in the Personal Information Protection Act are imposed upon organizations that infringe upon it, and these penalties have an upper limit. However, as long as the infringement is not serious, i.e. one that can not be remedied by an advisory or order from the cabinet minister in charge, fines are not generally imposed. The Personal Information Protection Act can deter information disclosure, however it may not offer assistance to aggrieved parties.

- Amount of Compensatory Damages for Disclosure of Personal Information

  Compensatory Damages for Personal Information Disclosure are damages that can be claimed in a civil lawsuit by the aggrieved, in order to alleviate financial losses and emotional distress resulting from the disclosure of personal information. The aggrieved can pursue legal action for compensatory damages, irrespective of the penalties outlined in the Personal Information Protection Act. Civil damages suits that are pursued regarding the disclosure of personal information have their aim offering financial redress to the aggrieved parties.

3.2 Recognition of Damage Stemming from Disclosure of Personal Information

Most damage stemming from disclosure of personal information results from the general emotional distress and economic disadvantage suffered by parties that provided that personal information. In recent years, there has been a high occurrence of direct mail, cold-calling, and spam mail, and individuals suffering harm as a result of the disclosure of personal information has become recognized as a social problem.

Harm resulting from the disclosure of personal information not only affects the person to which the information refers, but also the organization in possession of that information. In the event of personal information disclosure incidents resulting from illegal access or internal criminal offenses, the organization retaining that information will have to waste a large amount of both time and money on investigating their causes and upon preventing recurrences, in response to the aggrieved parties. Additionally, if these incidents of personal information disclosure are reported to the media, then this can cause serious damage to the brand image of the organization. Leaks of personal information where appropriate measures to prevent such disclosure are not implemented is increasingly being thought of as a kind of “antisocial behavior,” similar to environmental pollution resulting from the disposal of industrial effluent.

4. Assumptions related to Costs of Compensatory Damages due to Information Disclosure and Analysis of Personal Information Disclosure Incidents

2003 saw even more of a focus on personal information disclosure than in 2002. In particular, there has been extensive reporting of incidents of personal information disclosure in newspapers and in general news media, and personal information disclosure is a phenomenon that is becoming noticed by society.

In this chapter, we carried out a study of incidents of information disclosure, and analyzed details of these incidents. Based upon these results, we made calculations based upon several hypotheses to detail the degree of damages, as regards the value of personal information and the amount of compensatory damages that would be incurred in the event of its disclosure.

4.1.1 Number of Domestic Information Disclosure Incidents

The list in Table 4-1 on the next page shows incidents of disclosure of personal information that occurred within Japan from January to December 2003. The investigation carried out by the working group indicated that incidents of personal disclosure that occurred within this time frame, and that were reported on the Internet rose to 57 incidents, with a total of 1,554,592 people affected (an average of 30,482 people per incident).

Most of these incidents comprised leaks of personal information (including of e-mail addresses only). There were 5 incidents of disclosure outside the company of internal documents, etc.

Disclosure of personal information	54 (95%)
Disclosure of e-mail address	16 (28%)
Disclosure of private information	5 (5%)

By carrying out an analysis of these incidents of information disclosure, we were able to consider the reasons behind the many disclosures of personal information, and analyze the characteristics of the 57 incidents.

Table 4-1: List of 2003 Personal Information Disclosure Incidents

No.	Industry Classification	Cause of Disclosure	Route of Disclosure	No. of Aggrieved	Name	Address	Date of Birth	Sex	Telephone Number	Occupation	E-mail address	Other	No.
1	Financial / insurance	Removal of information	Unclear	1,000	Y							Internal rating, etc.	1
2	Education / learning support	Configuration error	Floppy discs and other portable recordable media	Unclear								Test results, etc.	2
3	Telecommunications	Operation error	E-mail	202	Y						Y		3
4	Other	Configuration error	Web	Unclear	Y							Contact details	4
5	Transport	Operation error	E-mail	190							Y		5
6	Education / learning support	Management error	Floppy discs and other portable recordable media	220	Y	Y			Y			Results sheets	6
7	Service industry (not in other classifications)	Configuration error	Web	443							Y		7
8	Education / learning support	Unclear	Floppy discs and other portable recordable media	7,381	Y							Results, high school names	8
9	Telecommunications	Removal of information	Printed media	1,500	Y	Y						Ages	9
10	Service industry (not in other classifications)	Configuration error	Web	450,000	Y	Y	Y					School names, interests, etc.	10
11	Public service (not in other classifications)	Unclear	Unclear	92							Y		11
12	Public service (not in other classifications)	Management error	Printed media	574	Y	Y						Company names, earned income	12
13	Telecommunications	Configuration error	E-mail	Unclear	Y				Y		Y	Details in e-mail	13
14	Financial / insurance	Removal of information	Floppy discs and other portable recordable media	15,000	Y	Y	Y		Y			Card numbers, account numbers, annual income, etc.	14
15	Other service	Bug or security hole	Unclear	2									15
16	Health care / welfare	Internal crime	Unclear	1,300	Y	Y	Y	Y				Blood types, results of testing for communicable diseases	16
17	Education / learning support	Misplacement	Printed media	950	Y		Y	Y				Department/subject names, examination numbers	17
18	Financial / insurance	Operation error	E-mail	2,800							Y		18
19	Financial / insurance	Operation error	E-mail	98	Y	Y			Y			Degree of disability	19
20	Public service (not in other classifications)	Other	Whole PC	100	Y							Compensation sums, course of negotiations	20
21	Financial / insurance	Internal crime	Unclear	800	Y	Y	Y	Y	Y	Y		Credit record	21
22	Service industry (not in other classifications)	Bug or security hole	E-mail	170							Y		22
23	Education / learning support	Illegal access	Web	23,000									23
24	Service industry (not in other classifications)	Bug or security hole	Web	210	Y	Y			Y		Y		24
25	Wholesale / retail	Other	Unclear	560,000	Y	Y	Y		Y				25
26	Public service (not in other classifications)	Theft	Whole PC	1,300	Y	Y	Y					Child-care allowance, welfare benefits, marriage counseling, etc.	26
27	Public service (not in other classifications)	Configuration error	Web	761	Y	Y	Y	Y	Y	Y		Credit card numbers	27
28	Financial / insurance	Internal crime	Unclear	325	Y	Y	Y					Details of business	28
29	Manufacturing	Operation error	E-mail	573							Y		29
30	Manufacturing	Management error	Floppy discs and other portable recordable media	Unclear	Y	Y		Y				Removal from family register, original family registers	30
31	Financial / insurance	Unclear	Unclear	74	Y	Y	Y					Insurance premiums	31
32	Public service (not in other classifications)	Operation error	Web	128	Y	Y			Y				32
33	Telecommunications	Operation error	E-mail	480							Y		33
34	Financial / insurance	Management error	Unclear	126	Y	Y			Y			Card numbers	34
35	Financial / insurance	Other	Floppy discs and other portable recordable media	1,453	Y	Y	Y	Y	Y	Y		Card numbers, expiry dates, account information	35
36	Wholesale / retail	Removal of information	Unclear	182,780	Y	Y	Y	Y	Y		Y		36
37	Telecommunications	Operation error	Web	Unclear	Y	Y						User ID, old passwords	37
38	Health care / welfare	Management error	Web	240	Y		Y					Name of disease, informing of cancer, etc.	38
39	Telecommunications	Operation error	E-mail	173							Y		39
40	Wholesale / retail	Configuration error	Web	6,000	Y	Y			Y			Purchased video titles	40
41	Financial / insurance	Illegal access	FTP	79,110	Y	Y	Y	Y	Y	Y		Residential circumstances, annual income classification	41
42	Financial / insurance	Removal of information	Printed media	75	Y	Y	Y	Y	Y	Y		Credit information	42
43	Information / communications	Operation error	Other	1,370	Y				Y		Y	Company name, position	43
44	Telecommunications	Theft	Whole PC	3,974	Y				Y		Y		44
45	Telecommunications	Other	Floppy discs and other portable recordable media	58,515	Y	Y						Name, date of birth, relationships	45
46	Public service (not in other classifications)	Management error	Printed media	872	Y	Y	Y					Voters names, vote information	46
47	Wholesale / retail	Configuration error	Web	1,912	Y	Y			Y				47
48	Transport	Other	Printed media	10	Y	Y	Y	Y	Y	Y		Family structure, annual income, etc.	48
49	Education / learning support	Theft	Whole PC	197	Y	Y			Y			Guarantor name, high school entrance examination scores, etc.	49
50	Service industry (not in other classifications)	Bug or security hole	Web	1,200	Y	Y		Y	Y		Y	Details of consultations	50
51	Service industry (not in other classifications)	Internal crime	Whole PC	Unclear	Y	Y	Y	Y	Y			Account information, billing record, etc.	51
52	Financial / insurance	Management error	Printed media	280	Y	Y			Y			Billing month, unpaid amounts, unpaid amounts outstanding	52
53	Telecommunications	Other	Whole PC	4,312	Y	Y			Y			Land area, building area, method of assessment	53
54	Transport	Internal crime	Unclear	131,742	Y	Y							54
55	Wholesale / retail	Configuration error	E-mail	9		Y			Y		Y		55
56	Telecommunications	Operation error	Printed media	985	Y							Sums used, billing amounts, etc.	56
57	Public service (not in other classifications)	Theft	Floppy discs and other portable recordable media	9,584	Y	Y	Y	Y				Family registers, voting rights, resident's card code	57
	Total			1,554,592	45	35	19	13	25	6	16		
	Average per incident (excluding "unclear")			30,482.2	79%	61%	33%	23%	44%	11%	28%		

Note: When calculating “Average per incident,” the parameter used excludes the number of incidents where the number of aggrieved people is unclear.

4.1.2 Analysis of Information Disclosed

Table 4-2 shows results according to the analysis of the information disclosed in the incidents. Disclosure ratio (%) shows the percentage of each disclosed information item included in the incidents of information disclosure that are the subject of this investigation.

Table 4-2: Number of Incidents of Disclosure and Disclosure Ratio for Each Information Type

Classification of Disclosed Information	Incidents	Disclosure Ratio
Name	45	79%
Addresses	35	61%
Date of Birth	19	33%
Sex	13	23%
Telephone Number	25	44%
Occupation	6	11%
E-mail Addresses	16	28%

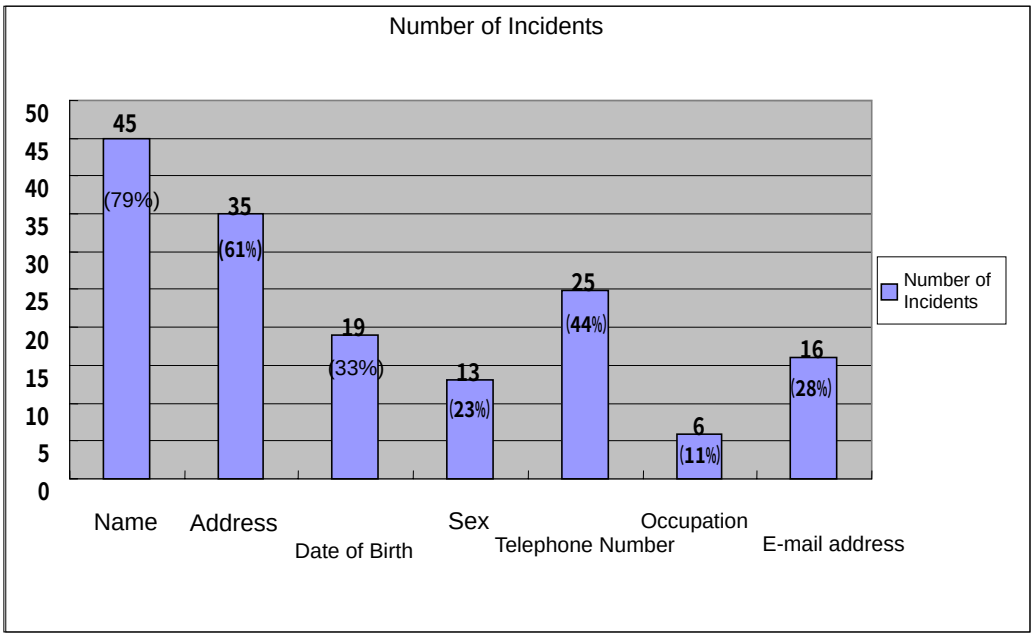


Diagram 4-1: Number of Incidents of Disclosure and Disclosure Ratio for Each Information Type

"Name" was included in 79% of incidents of information disclosure, and was the type of information that was the most likely to be divulged. Results showed that the three types of information - "Name," "Address," and "Telephone Number" were more likely to be disclosed than other information.

We feel that much of the time, these items of information were handled together, for example on questionnaires on a web page, when filling in membership information, or were handled as basic items of customer information within a company.

Next, we show some of the information classified as “Other,” because of its infrequent appearance. This information that was divulged includes more private, personal information, and comprises a large variety of content types.

Table 4-3: Information Classified as “Other”

User ID, credit card numbers, credit records, card usage information, annual earnings, bank names, account numbers, age, company names, school names, academic performance, interests, occupation, blood type, names of sicknesses, results of testing for communicable diseases, degree of disability, amount of insurance premiums, family registers, etc.

4.1.3 Information Management Representatives (Organizational)

86% of the organizations that had disclosures of information are companies. We estimate that when compared to public agencies, companies add services for customers such as mailing lists and questionnaires on the Internet, and construct systems in which customer information is stored as data for handling.

In the future, as a result of the promotion of Internet services and systems architectures managed by governments and regional authorities as typified by the e-Japan plan, we expect to see an increased ratio of incidents of information disclosure from public agencies.

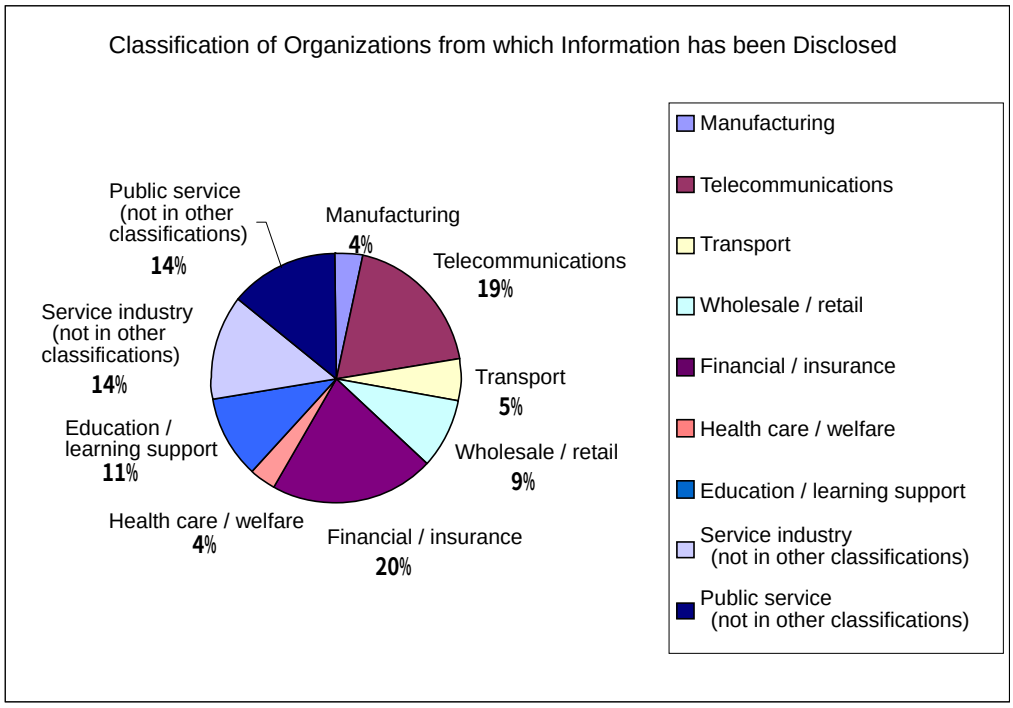


Diagram 4-2: Classification of Organizations from which Information has been Disclosed

4.1.4 Reasons for Information Disclosure

Diagram 4-3 shows the reasons for disclosure of information. When carrying out the analysis for this year's investigation, we added "Theft" and "Misplacement" as new causes for disclosure.

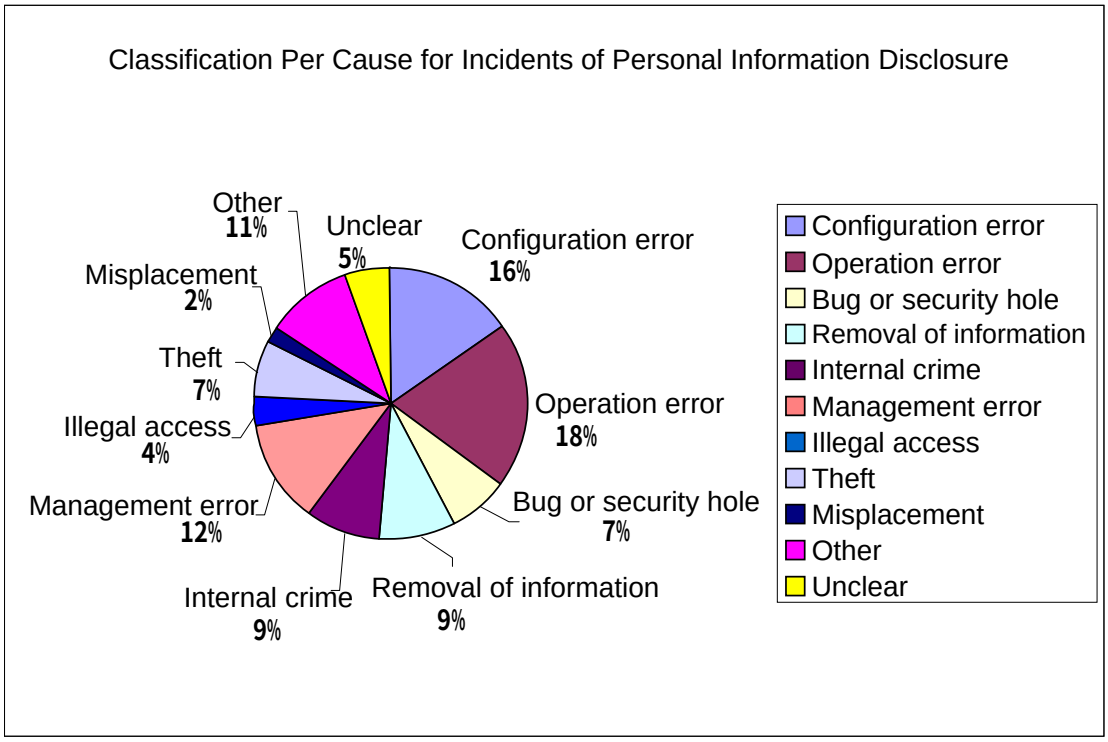


Diagram 4-3: Reasons for Information Disclosure

These reasons can be classified into factors and causes as follows.

Table 4-2 : Reasons for Information Disclosure

No.	Factor	Cause	%	Corresponding causes
1	Technical	Human error	46	Configuration error, operation error, management error
2	Technical	Insufficient measures	11	Bug or security hole, illegal access
3	Non-technical	Human error	2	Misplacement
4	Non-technical	Criminal	25	Internal crime, removal of information, theft
5	Other	Other, unclear	16	Other, unclear

If we look back over the causes for disclosure of information last year, the technical factor of human error and insufficient measures that took the No. 1 and No. 2 positions comprised 88% of the total, meaning that technical factors were the main causes of information disclosure.

However, this year, the technical factors of human error and insufficient measures that took the No. 1 and

No. 2 positions comprised 57% of the total, with these causes for information disclosure dropping to slightly more than half of the total.

Conversely, non-technical factors of human error and crime that took the No. 3 and No. 4 positions last year quadrupled, to reach 27% of the total.

Additionally, causes such as “Other” and “Unclear” comprised 16% of the total this year. This study focused principally on information from Internet news sources, therefore please be aware that more details are not available.

Diagram 4-4 shows the routes of information disclosure. This year has seen a dramatic increase in the number of incidents of disclosure of information on physical media when compared to last year. This is because heightened public awareness of the protection of personal information has led to increased disclosure in the news by companies and the media, irrespective of the routes and steps of personal information. Accordingly, this year's inquiry has added the classification of the "physical media" route for disclosure of information. These comprise “printed media,” “floppy discs and other portable recordable media,” and “whole PCs.”

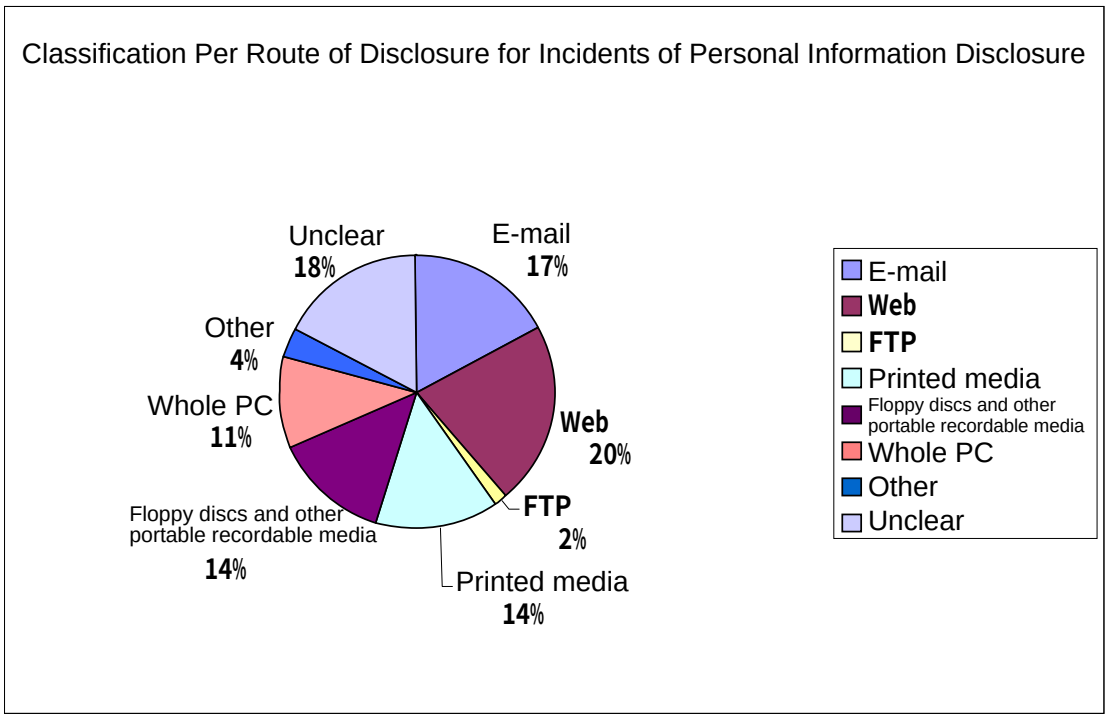


Diagram 4-4: Routes of Information Disclosure

Results showed that the routes by which information was disclosed differed from last year. Last year, “web,” “e-mail,” and “ftp,” all three of which use the Internet comprised 98% of disclosures. In terms of the number of incidents, this was 62 out of 63.

However, results this year showed that these three routes comprised 39% of the total. The newly added categories of "printed media," "floppy discs and other portable recordable media," and "whole PCs (discs and other portable recordable media)" increased drastically over last year, with these alone comprising 39% of disclosures.

In our results, we divided routes of disclosure into two, i.e. Internet and media.

Table 4-3: Routes of Information Disclosure

No.	Parameter	%	Route
1	Internet	39	Web, E-mail, FTP
2	Media	39	Printed media, floppy discs and other portable recordable media, and "whole PCs (discs and other portable recordable media)
3	Other	22	Other, unclear

4.1.5 Results of the Analysis of Information Disclosure

This uses the results of the above analysis to summarize the characteristics of information disclosure for last year and this year.

Last year

- Personal information comprised the majority (90%) of disclosed information.
- Companies were the source of a majority (82%) of disclosures.
- Technical factors, namely human error and insufficient measures were the cause of the majority (88%) of disclosures.
- The Internet was the major (98%) route for disclosures.

This year

- Similar to last year, personal information comprised the majority (95%) of disclosed information.
- Similar to last year, companies were the source of a majority (86%) of disclosures.
- Different to last year, technical factors, namely human error and insufficient measures were the cause of slightly more than half (57%) leaks, with non-technical factors at 27%.
- Different to last year, routes were evenly divided between the Internet and media, with 39% each.

In conclusion, this year, we have seen a number of changes in disclosure of information. These changes are described below.

Last year, we were able to study information intended for external input and reference that was leaked from a DMZ terminal, which is at the point of connection to the Internet. This meant that people affected were members and customers who had responded to Web questionnaires, and who had used web services.

However, it appears that this year, as well as disclosure of information from a DMZ as occurred last year,

information was also disclosed from a terminal within the firewall. Accordingly, it was estimated that people who were affected were not only those who had responded to a web-based questionnaire, or members and customers who had used web services, but that the range of the influence was expanded to customer information retained by the company.

4.2 Amount of Compensatory Damages Resulting from Disclosure of Personal Information in 2003

We present a formula for estimating the amount of damages resulting from the disclosure of personal information from 2002 into 2003.

Details of the formula are explained in Chapter 5. This formula is based upon using points garnered from last year in order to calculate amounts of damages, and this year is an improved numeric calculation method that covers all parameters.

Here, we show payments for pain and suffering, and compensatory damages based upon Table 4-1 on the next page.

Amount of compensatory damages = ¥28,069,360,000
Average amount of compensatory damages per incident of information disclosure ＝ ¥550,380,000
Number of aggrieved (total) = 1,554,592 **(average) = 30,482**

The (estimated) amount of compensatory damages per incident of information disclosure was ¥550,380,000. Not all people affected by information disclosure necessarily file civil law suits, however if we take into account the amount of compensatory damages, and the negative impact upon sales resulting from a deterioration in the brand image of companies due to incidents of information disclosure, then we can see that it is necessary to invest in security with the aim of preventing the disclosure of information before it occurs.

Additionally, it is possible for organizations that store and manage personal information to estimate the amount of compensatory damages from the details of that information and the number of incidents, instead of estimating the average amounts of compensatory damages as the risk of information disclosure. Accordingly, it is possible for organizations in possession of personal information to calculate the amount of compensatory damages from details of stored information and the number of incidents as an information disclosure risk, which can then be used as an amount for investment in security.

Table 4-4 shows a list of estimated compensatory damages for disclosure of personal information for this year.

Table 4-4: List of 2003 Compensatory Damages for Disclosure of Personal Information

No.	Industry Classification	No. of Aggrieved	Emotional Distress Level (x)	Financial Loss Level (y)	Degree of Information Sensitivity	Degree of Social Responsibility	Appraisal of Response Position	Degree of Ease of Identifying Individuals	Average amount of Compensatory Damages per Aggrieved Party	Total Compensatory Damages (¥'000,000)	No.
1	Financial / insurance	1,000	2	1	11	2	2	3	¥66,000	¥66,000	1
2	Education / learning support	Unclear	2	1	11	1	1	1	¥6,000	Unclear	2
3	Telecommunications	202	1	1	2	2	1	3	¥6,000	¥1,212	3
4	Other	Unclear	1	1	2	1	1	3	¥3,000	Unclear	4
5	Transport	190	1	1	2	1	1	1	¥1,000	¥190	5
6	Education / learning support	220	2	1	11	1	1	6	¥33,000	¥7,260	6
7	Service industry (not in other classifications)	443	1	1	2	1	1	1	¥1,000	¥443	7
8	Education / learning support	7,381	2	1	11	1	1	3	¥17,000	¥121,787	8
9	Telecommunications	1,500	1	1	2	2	1	6	¥12,000	¥18,000	9
10	Service industry (not in other classifications)	450,000	1	1	2	1	1	6	¥6,000	¥2,700,000	10
11	Public service (not in other classifications)	92	1	1	2	2	1	1	¥2,000	¥184	11
12	Public service (not in other classifications)	574	1	2	6	2	1	6	¥36,000	¥20,664	12
13	Telecommunications	Unclear	2	1	11	2	1	3	¥33,000	Unclear	13
14	Financial / insurance	15,000	2	3	35	2	1	6	¥210,000	¥3,150,000	14
15	Other service	2	1	1	2	2	1	1	¥2,000	¥4	15
16	Health care / welfare	1,300	3	1	101	2	1	6	¥606,000	¥787,800	16
17	Education / learning support	950	1	1	2	1	1	3	¥3,000	¥2,850	17
18	Financial / insurance	2,800	1	1	2	2	1	1	¥2,000	¥5,600	18
19	Financial / insurance	98	1	1	101	2	1	6	¥606,000	¥59,388	19
20	Public service (not in other classifications)	100	2	2	15	2	1	3	¥45,000	¥4,500	20
21	Financial / insurance	800	2	2	15	2	1	6	¥90,000	¥7,200	21
22	Service industry (not in other classifications)	170	1	1	2	1	1	1	¥1,000	¥170	22
23	Education / learning support	23,000	1	1	2	1	1	1	¥1,000	¥23,000	23
24	Service industry (not in other classifications)	210	1	1	2	2	1	6	¥12,000	¥2,520	24
25	Wholesale / retail	560,000	1	1	2	1	1	6	¥6,000	¥3,360,000	25
26	Public service (not in other classifications)	1,300	3	1	101	2	1	6	¥606,000	¥787,800	26
27	Public service (not in other classifications)	761	1	3	26	2	1	6	¥156,000	¥118,716	27
28	Financial / insurance	325	1	2	6	2	1	6	¥36,000	¥11,700	28
29	Manufacturing	573	1	1	2	2	1	1	¥2,000	¥1,146	29
30	Manufacturing	Unclear	3	1	101	1	1	6	¥303,000	Unclear	30
31	Financial / insurance	74	1	2	6	2	1	6	¥36,000	¥2,664	31
32	Public service (not in other classifications)	128	1	1	2	2	1	6	¥12,000	¥1,536	32
33	Telecommunications	480	1	1	2	2	1	1	¥2,000	¥960	33
34	Financial / insurance	126	1	3	26	2	1	6	¥156,000	¥19,656	34
35	Financial / insurance	1,453	1	3	26	2	1	6	¥156,000	¥226,668	35
36	Wholesale / retail	182,780	1	1	2	1	1	6	¥6,000	¥1,096,680	36
37	Telecommunications	Unclear	1	1	2	2	1	6	¥12,000	Unclear	37
38	Health care / welfare	240	3	1	101	2	1	3	¥303,000	¥72,720	38
39	Telecommunications	173	1	1	2	2	1	1	¥2,000	¥346	39
40	Wholesale / retail	6,000	2	1	11	1	1	6	¥33,000	¥198,000	40
41	Financial / insurance	79,110	2	2	15	2	1	6	¥90,000	¥7,119,900	41
42	Financial / insurance	75	2	2	15	2	1	6	¥90,000	¥6,750	42
43	Information / communications	1,370	1	1	2	2	1	3	¥6,000	¥8,220	43
44	Telecommunications	3,974	1	2	6	2	1	3	¥18,000	¥71,532	44
45	Telecommunications	58,515	1	1	2	2	1	6	¥12,000	¥702,180	45
46	Public service (not in other classifications)	872	2	1	11	2	1	6	¥66,000	¥57,552	46
47	Wholesale / retail	1,912	1	1	2	1	1	6	¥6,000	¥11,472	47
48	Transport	10	2	2	15	2	1	6	¥90,000	¥900	48
49	Education / learning support	197	2	1	11	1	1	6	¥33,000	¥6,501	49
50	Service industry (not in other classifications)	1,200	2	1	11	2	1	6	¥66,000	¥79,200	50
51	Service industry (not in other classifications)	Unclear	2	2	15	1	1	6	¥45,000	Unclear	51
52	Financial / insurance	280	2	3	35	2	1	6	¥210,000	¥58,800	52
53	Telecommunications	4,312	2	2	15	2	1	6	¥90,000	¥388,080	53
54	Transport	131,742	1	1	2	1	1	6	¥6,000	¥790,452	54
55	Wholesale / retail	9	1	1	2	1	1	3	¥3,000	¥27	55
56	Telecommunications	985	1	2	6	2	1	3	¥18,000	¥17,730	56
57	Public service (not in other classifications)	9,584	3	1	101	2	1	6	¥606,000	¥5,807,904	57
	Total	1,554,592								¥28,069,364	
	Average per incident (excluding "unclear")	30,482.2								¥550,380	

Note: When calculating “Average per incident,” the parameter used excludes the number of incidents where the number of aggrieved people is unclear.

4.2.1 Trends in 2003 Information Disclosure

Diagram 4-5 shows the number of incidents of information disclosure (number of aggrieved people).

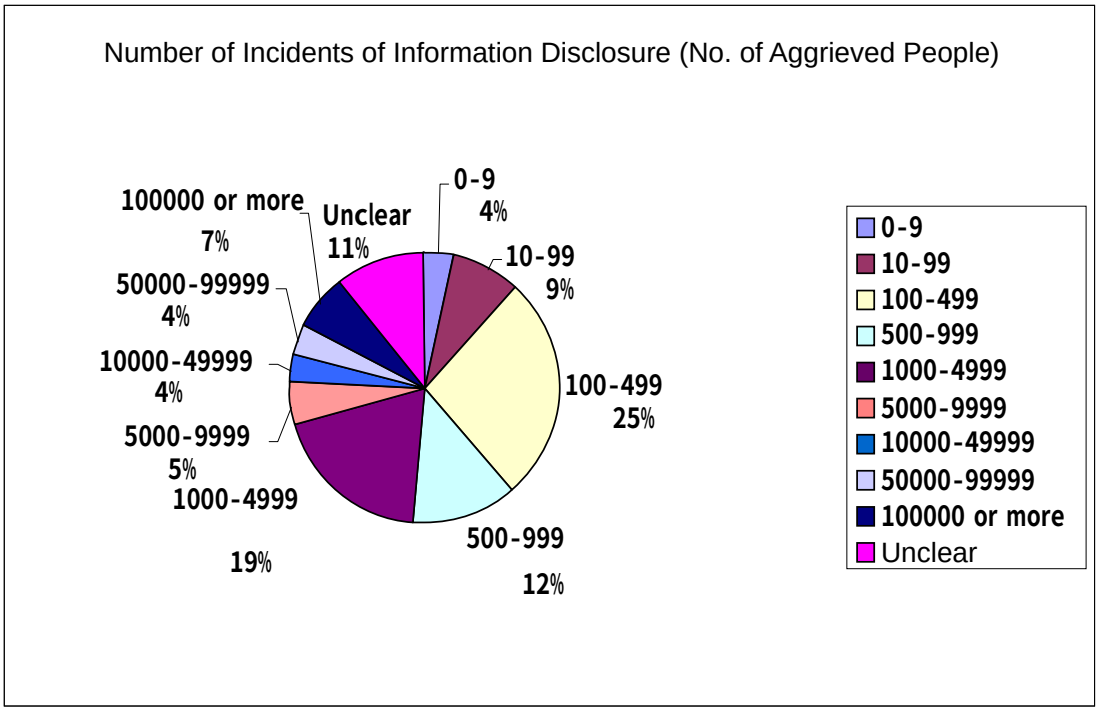


Diagram 4-5: Number of Incidents of Information Disclosure (number of aggrieved people)

As mentioned at the beginning of this chapter, there were at total of 1,554,592 people affected, with an average of 30,482 people per incident. This is a large increase over last year's total of 418,716 aggrieved people, with 6,646 per incident last year.

Furthermore, the incident with the largest number of aggrieved was 100,000 last year, whereas this year, this number has jumped to 560,000. In other words, this single incident this year surpassed last year's total. For reference, the second largest incident this year in terms of the number of aggrieved was 450,000.

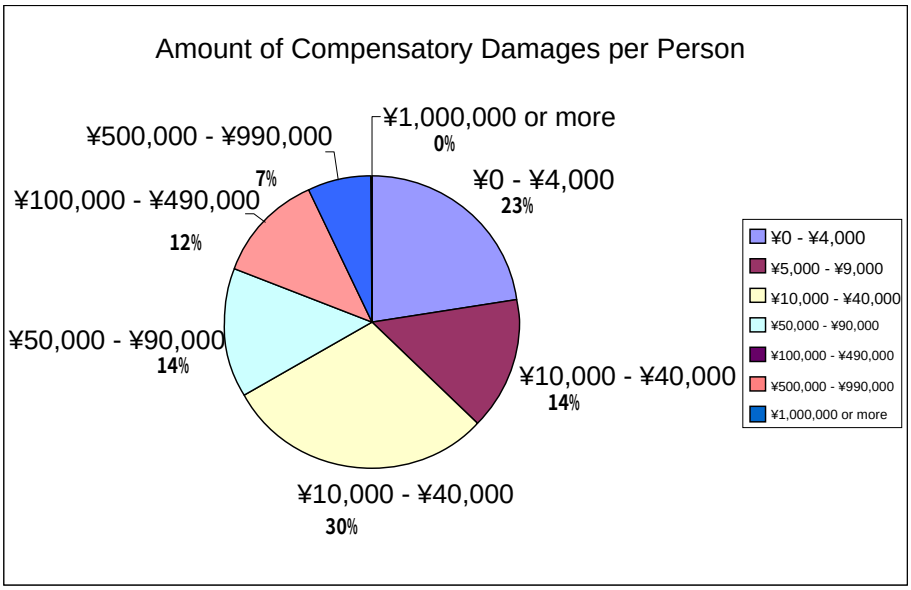


Diagram 4-6: Amount of Compensatory Damages per Person

As regards the amount of compensatory damages per person shown in Diagram 4-6, incidents for which compensation sums exceeded ¥100,000 comprised 19% of the total, with 63% comprising sums in excess of ¥10,000.

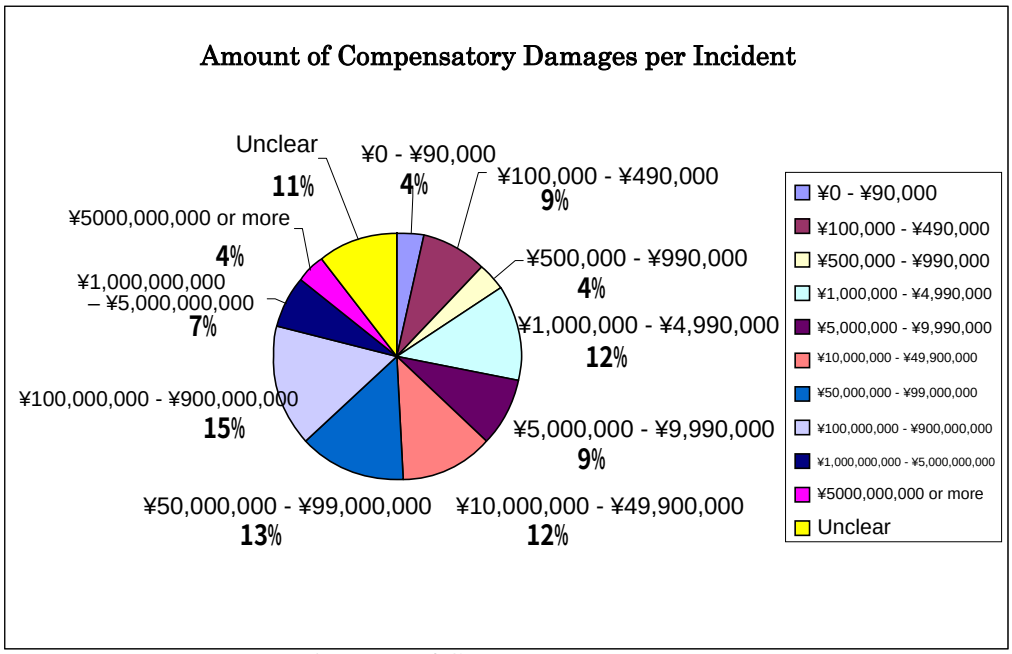


Diagram 4-7: Amount of Compensatory Damages per Incident

As regards the amount of compensatory damages per incident shown in Diagram 4-7, 26% of incidents had sums of compensatory damages greater than ¥100 million. This sum comprised approximately 97% of the total, and incidents that generate very high sums are expected.

5. About the Prospective Calculation Method for Amounts of Compensatory Damages for Disclosure of Personal Information

In 2002, we analyzed incidents of personal information disclosure, and derived points in order to present a method for calculating amounts of compensatory damages. Based upon the basic ideas for calculating compensatory damages that we proposed last year, we created a new calculation method that improved the way in which we assigned values to each parameter, and this chapter offers an explanation of this.

5.1 The Improved Prospective Calculation Method

A characteristic of the 2003 calculation method to estimate the amount of compensatory damages for incidents of personal information disclosure (”Formula (’03)”) is the aspect where it uses the EP Diagram (refer to 5.1.2) to calculate the value of disclosed personal information. The EP diagram is used to analyze the “financial losses” and “emotional distress” risk factors inherent in personal information, in order to quantify the value of that information. Additionally, we have used criteria to implement improvements in order to make it easier to assign values to each parameter in the calculation method.

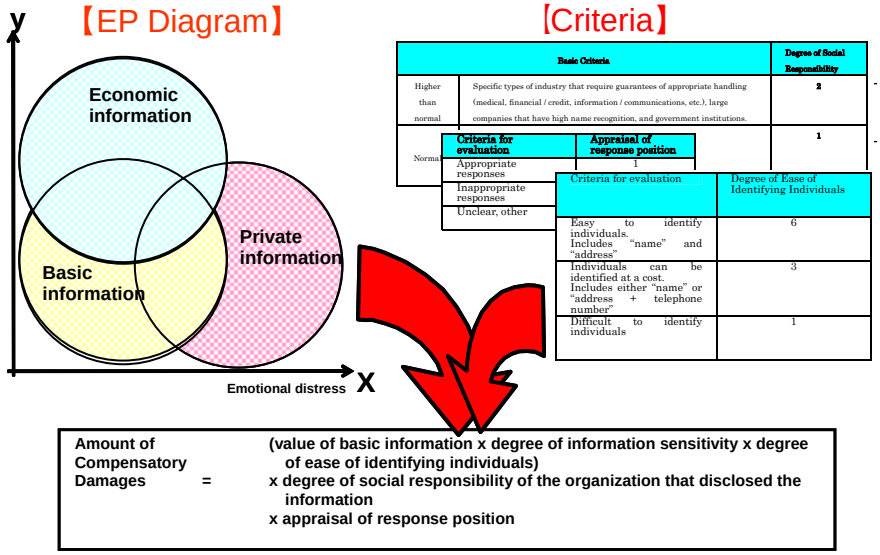


Diagram 5-1: 2003 Method for Calculating Amounts of Compensatory Damages

5.1.1 About the 2002 Method

Last year, in light of the large amount of incidents of information disclosure, the working group carried out a study on a model that can be used to estimate the amounts of subsequent compensatory damages. The 2002 report tested the calculation method using the formula shown in5-1, and created Tables 5-1 and 5-2, in estimating sums of compensatory damages for incidents of information disclosure.

Amount of compensatory damages from the organization that disclosed the information (points)

= pain and suffering based upon the content of the disclosed information

x Agreement to provision of personal information

x Relationship with provider of information

x Degree of reliability of the organization that disclosed the information

x Approach to response after the incident

Formula 5-1: Calculation Method for Compensatory Damages [Formula ('02)]

Table 5-1: Points Table for Each Parameter [Formula ('02)]

Calculation Parameters	Points for Status
1 Costs for Consolation Gifts	Basic personal information = 100
	Sensitive personal information (3 or less items)
	Sensitive personal information (4 or more
	E-mail address only = 10
	ID information that can identify an individual /
2 Agreement to provision of personal information	Agreement = 2.0
	No agreement = 1.0
3 Relationship with provider of information	Customer = 2.0
	Questionnaire, signed up for giveaways = 1.0
4 Degree of confidence in organizations that disclose information	Higher than normal = 1.5
	Normal = 1.0
5 Appraisal of Response Position	High = 1.0
	Average = 2.0
	Low = 4.0

Table 5-2: Value Points and Estimated Payments for Pain and Suffering [Formula ('02)]

Evaluation	Estimated Cost of Consolation
1000 points or	¥0 ~ 5000 (¥5000)
1000 ~ 2000	~¥10,000 (¥10,000)
2000 ~ 5000	~¥50,000 (¥50,000)
5000 points or	More than ¥50,000 (¥100,000)

We received a large number of questions and comments from a variety of sources about the above formula.

Additionally, the Personal Information Protection Act was put into place after the publication of last year's report, and accordingly, public awareness as regards information disclosure, and public perspectives are slowly changing. We have used comments from various quarters, this general changes in awareness, and deficiencies in last year's study in revising last years study in order to create a more effective formula, and to improve the calculation model.

5.1.2 Studying the Basis of the Value of Personal Information

The 2002 calculation method to estimate the amount of compensatory damages for incidents of personal information disclosure (”Formula (’02)”) divided personal information into two groups: basic personal information such as "name," "address," "telephone number," "date of birth," and "sex," and individual personal information such as “relationships,” “bust-hip-waist measurements,” and “interests,” and defined point values for each of these items of information. Next, we assigned point values to the disclosed information, which represented the total value of the disclosed information, thus settling upon a reference value for the compensatory damages as regards the information disclosed.

This year, we started work on reviewing definitions and valuations of personal information. First, in order to fully grasp what is meant by personal information, we listed and classified several types of information that are considered personal information. The personal information listed below is given as examples, and there is a range of other types of personal information as well. Because we did not have any particular knowledge of how to divide personal information for the 8 classifications below (including classifications that are unclear), we created these from scratch, based upon the examples of personal information that were given.

- Four basic items of personal information
  Name, address, date of birth, sex
- Physical, health, and medical information
  Height, weight, bust-hip-waist measurements, blood type, photograph (portraits), fingerprints, voice, voice print, DNA, physical characteristics, physical strength diagnosis, health diagnosis, diagnosis of character, psychological diagnosis, medical records, medical treatments, nursing records, records of examinations, operative record, medical condition, medical history, certificates of medical remuneration, pregnancy history, communicable disease, sexual preference, sex life, dementia, mental handicaps, physical disability, mental disability, physical disability certificates
- Ideas, religious, and birth information
  Special skills, interests, preferences, membership of labor unions, membership of political parties, political

views, permanent residence, race, nationality, ethnic group, lineage, regional accent, religion, beliefs, faith, ideas

・Family and associate information

Name of head of household, dependents, relationships, marital history, divorce record, familial structure, allowance for dependent children, associates, welfare benefits, child-care allowance

・Individual credit records

Account numbers / personal identification numbers, credit card numbers, property, loans, buildings, land, amounts outstanding, credit blacklists, annual earnings and classification, income, card expiry dates, names of financial institutions, health insurance card information, annuity certificate, nursing care insurance card information, purchasing records, loan records, passport information

・Social and personal information

Previous criminal history, criminal record, company names, position, school name, occupation, type of work, work history, rewards and punishments, academic performance, academic record, examination results, qualifications

・ID information

Bank accounts / passwords, ISP accounts / passwords, resident's card code, e-mail address, telephone number, handle name, health insurance card number, annuity certificate, driving license number, employee number, membership numbers

・Unclear classification information

Will, details of mail, positional information

We felt that personal information could be broadly separated into three classifications, depending on the type of damage that could be caused as a result of its being disclosed. First, we hypothesized damage resulting from disclosure of personal information as having two factors - “financial losses resulting from disclosure of personal information” and “emotional distress resulting from disclosure of personal information.” In short, individuals are subject to “financial losses” and “emotional distress,” and we were able to represent these as two axes in Diagram 5-2. Next, adding “minor damage resulting from the disclosure of basic information” to the above-mentioned, we felt that damage stemming from personal information disclosure could be broadly separated into three types. Accordingly, the working group classified personal information with three attributes as is shown below, namely basic information, economic information, and private information.

Basic information

Basic information representing a person, such as the four basic items of personal information. Information that does not have economic value, or that does not violate privacy.

Private information

Information that if leaked, or disclosed to other people, could cause emotional distress.

Economic information

Information that if used, could directly have an adverse effect on assets owned by an individual.

(The above 3 classifications include types of information for which collection and distribution is prohibited.)

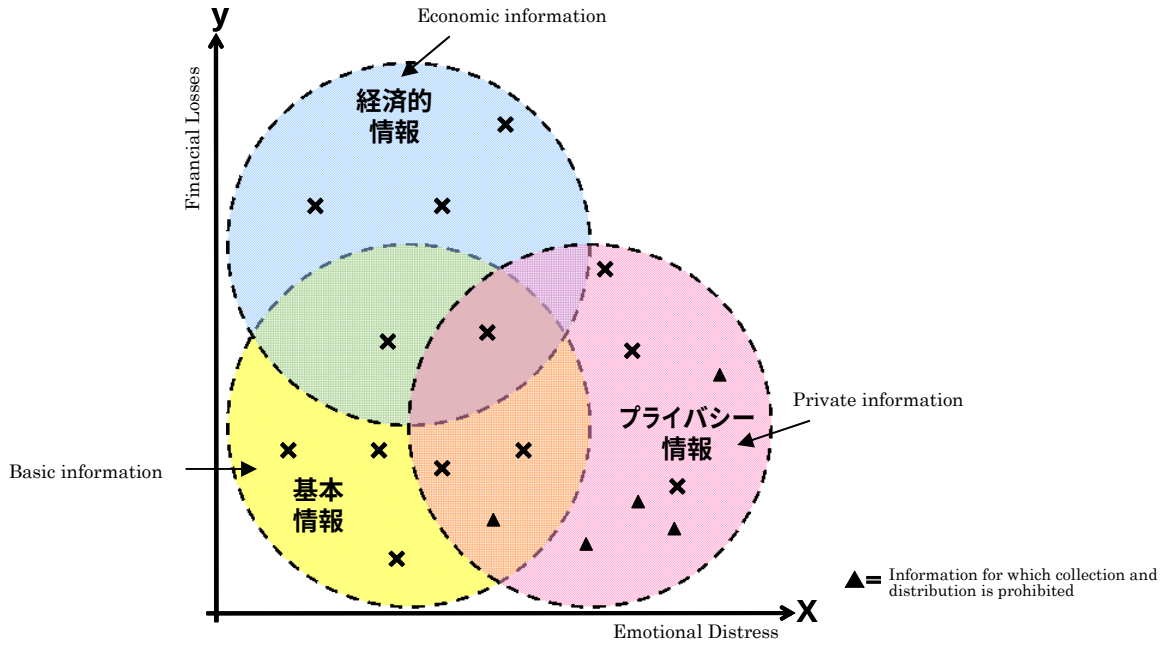


Diagram 5-2: EP Diagram (2 individual information risk factors, and information distribution)

Diagram 5-2 shows the two risk factors - "financial losses" and "emotional distress" for personal information, and is called an EP Diagram (Economic-Privacy Map). Coordinates (x, y) on this EP Diagram indicate degrees of risk (x = emotional distress, y = financial losses). Information detailed in Diagram 5-2 is plotted in Diagram 5-3.

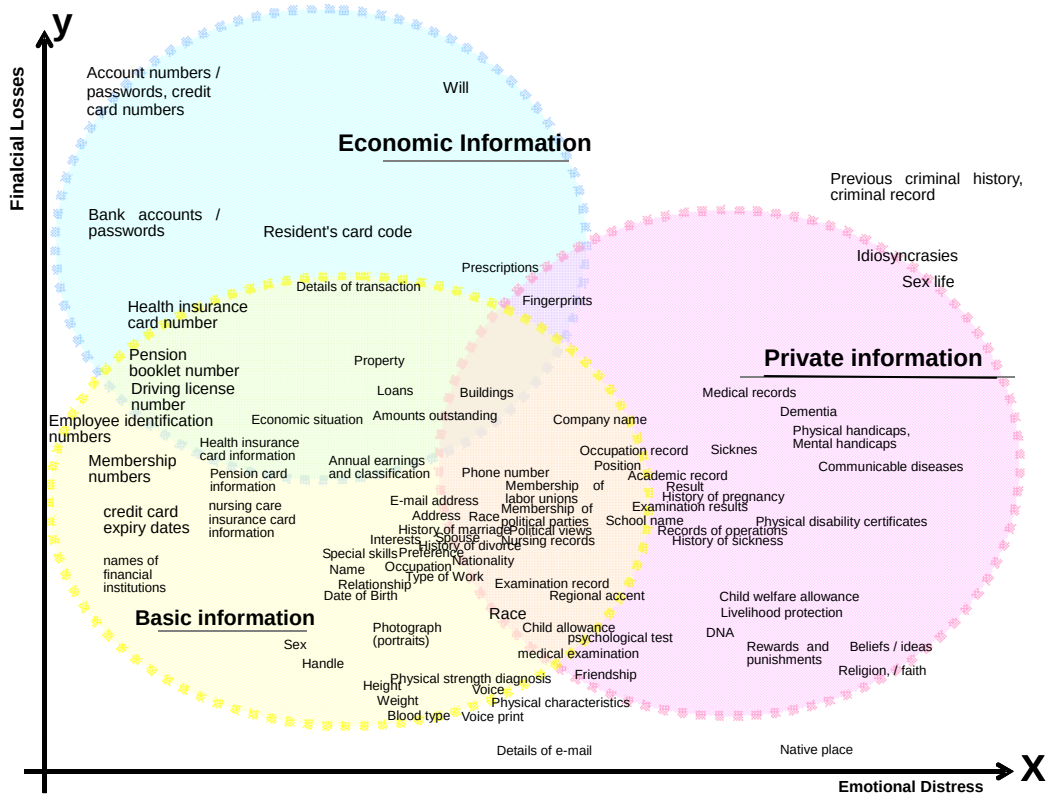


Diagram 5-3: Distribution of Individual Information (EP Diagram)

The distribution of each type of information in the EP Diagram is in reference to the "Personal Information Protection Act" and the "Requirements for compliance program on personal information protection (JIS Q 15001)," however final decisions as to the distribution of these types of information was weighted heavily towards the opinions of the members of this working group. We would ask readers to be aware that there is a certain amount of subjectivity in the judgments made by the members of the working group. In Diagram 5-2, there are some differences in the values of risk placed upon financial losses and emotional distress as a result of these individuals' subjective judgment criteria, and it was difficult to decide upon common values for representing each type of personal information. Consequently, each of the two axes is divided into three levels, and this resulted in the Simple-EP Diagram (Diagram 5-3) that plots each type of information. By plotting disclosed personal information on the Simple-EP Diagram, we can estimate the degree of risk for that information. The method for calculating amounts of compensatory damages through using the Simple-EP Diagram is detailed in 5.1.3.

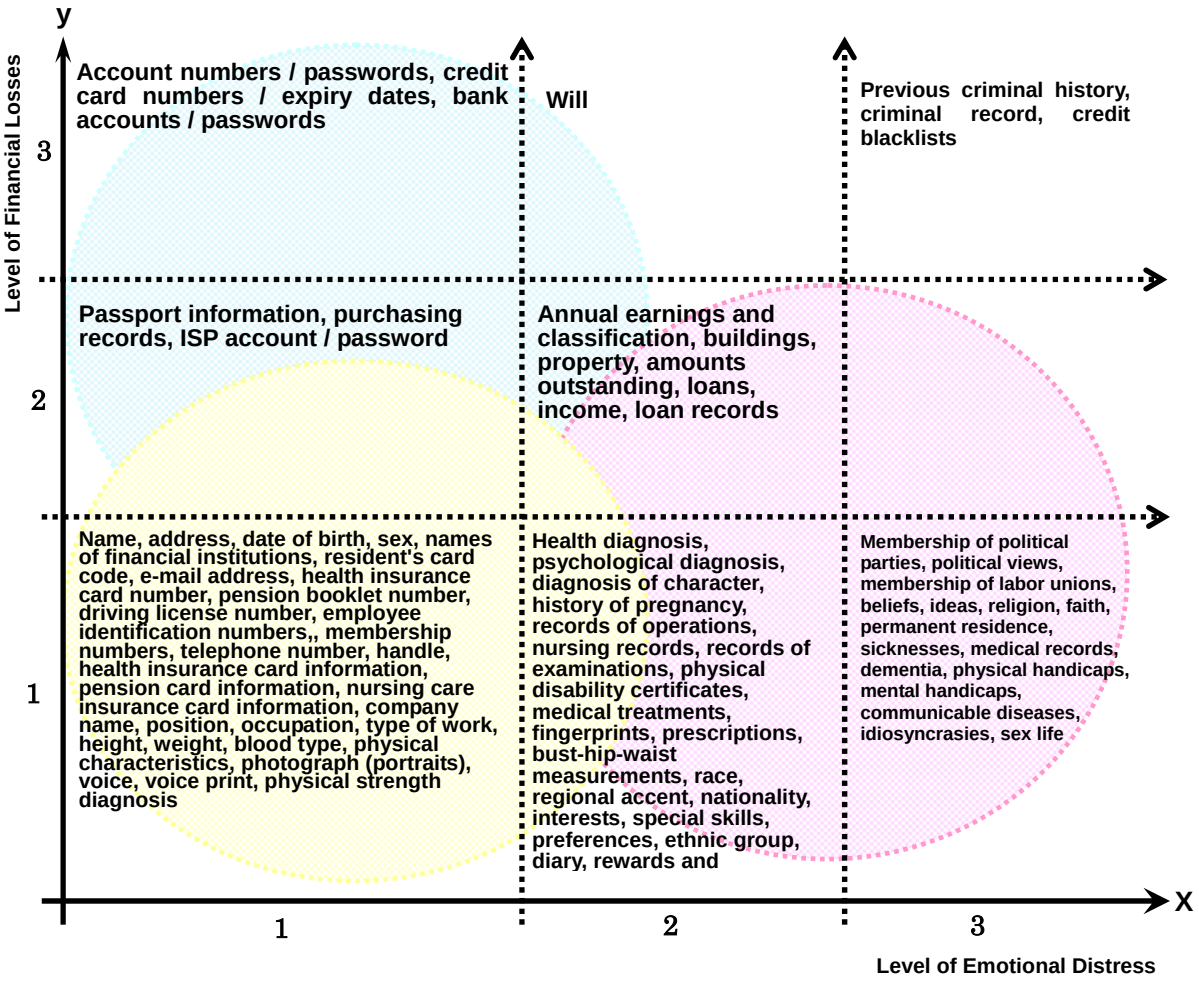


Diagram 5-4: Simple-EP Diagram

5.1.3 Calculation Methods for Value of Damages

We took into account the following conditions when calculating amounts of damages in the event of the disclosure of personal information.

1. Is sensitive material included in the disclosed personal information?
2. Can individuals be identified from the disclosed personal information?

The condition #1 is based upon the idea of deciding the degree of risk depending upon disclosed personal information, as described in 5.1.2.

As regards the condition #2, the "Personal Information Protection Act" has the definition "'personal information' is information regarding an individual, and such information includes names, dates of birth, and other information that can be used to identify a specific individual," which is quite clear. Whether or not an individual can be identified from said disclosed personal information is the determinant as to whether or not damage has occurred.

Accordingly, we created the formula in order to calculate the value of disclosed personal information.

Value of disclosed personal information = value of basic personal information x sensitive information ... (1)

x Degree of Ease of Identifying Individuals ...(2)

(1) Amount of sensitive information included in the disclosed personal information

(2) Ease of identifying individuals from the disclosed personal information

Formula 5-2: Calculating the Value of Disclosed Personal Information

5.1.3.1 Degree of Information Sensitivity

The degree of information sensitivity expresses the amount of sensitive information that is included in disclosed personal information. Sensitive information is defined as personal information for which collection is prohibited as in the "Requirements for compliance program on personal information protection (JIS Q 15001)."

a) Information about ideas, belief, and religion
b) Race, ethnic group, lineage, registered domicile (excluding information on which prefecture), physical, mental disorders, criminal record, and other information that could lead to discrimination within society
c) Information about workers' right of association, and information regarding group negotiations and other group activities
d) Information regarding participations in demonstrations, use of the right of petition, and other information regarding the use of political rights
e) Information regarding health care and sex life

In order to study the damage resulting from disclosed personal information, we need to think about not only important, sensitive personal information for which collection should be prohibited, but also a range of sensitive information that includes some which may be very personal. Based upon ideas concerning risks to personal information as in 5.1.2, we used the Simple-EP diagram in Diagram -4 to calculate the degree of information security (Formula 5-3).

Degree of information sensitivity $= \left(10^{x-} + 5^{y\ 1}\right)$

x = amount of emotional distress level in the disclosed personal information

y = amount of financial loss level in the disclosed personal information

Formula 5-3: Calculation Method for the Degree of Information Sensitivity

The constants in this method to calculate the degree of information sensitivity as shown in Formula 5-3 were based upon the maximum values for emotional distress and financial losses as shown below.

- Amounts of compensatory damages resulting from emotional distress
  In the event that there has been disclosure of personal information such as information regarding communicable diseases, which has an emotional distress level of 3 (the maximum), we can use legal precedent regarding privacy to estimate that the amount of compensatory damages will be on the order of ¥1 million. Consequently, we estimated a scenario in which there is a level 3 (the maximum) disclosure of personal information, and while applying this to the calculation method to estimate the amount of compensatory damages as detailed later, considered the most appropriate calculation method for degrees of information security. Results of our study indicated a degree of information sensitivity for emotional distress of 10^n.

- Amounts of compensatory damages resulting from financial losses
  In the event that there has been disclosure of personal information such as information regarding credit card numbers, which has a financial loss level of 3 (the maximum), we estimate that the amount of compensatory damages will be in the range of several hundreds of thousands of yen (the extent of potential card usage). We carried out a study as above, and the results of our study indicated a degree of information sensitivity for financial losses of 5^n.

An example of using this method to calculate the degree of information sensitivity is shown in Formula 5-4. The degree of information sensitivity is calculated by applying the Simple-EP Diagram to the information that has been disclosed (e.g. name, address, date of birth, sex, telephone number, name of disease, account number), and then arriving at the maximum emotional distress level x=2, and the maximum financial loss level of y=3. By

substituting these values into Formula 5-3, we can calculate that the degree of information sensitivity =35.

Example)
Disclosed information = {name, address, date of birth, sex, telephone number, sicknesses, account number}

- {name, address, date of birth, sex, telephone number} = (1,1)
- {Sicknesses} = (2, 1)
- {Account} = (1, 3)

Max (x) = 2, Max (y) = 3, therefore, the degree of information sensitivity = 10^1+5^2 =35

Formula 5-4: Example Calculation for the Degree of Information Sensitivity

5.1.3.2 Degree of Ease of Identifying Individuals

The degree of ease of identifying individuals represents how easy it is to identify an individual from disclosed personal information. By combining multiple items of basic information, we can determine the ease of identifying individuals.

Table 5-3 shows the criteria to determine the degree of ease of identifying individuals.

Table 5-3: Determining the Degree of Ease of Identifying Individuals

Criteria for evaluation	Degree of Ease of Identifying Individuals
Easy to identify individuals. Includes “name” and “address”	6
Individuals can be identified at a cost. Includes either “name” or “address + telephone number”	3
Difficult to identify individuals	1

5.1.4 Degree of Social Responsibility

The formula (’02) stated “if there is a high level of social confidence in organizations that disclose information, then disclosed information will have more credibility, and may lead to more usage by third parties," and we have added the “degree of social confidence in organizations that disclose information” parameter.

The formula (’03) changed this name from “Degree of Social Confidence” to “Degree of Social Responsibility.” Additionally, we clarified the method of determining values for the degree of social responsibility. The degree of social responsibility is selected from “higher than normal” and “normal” as shown in Table 5-4. Companies and organizations that have a higher than normal degree of social

responsibility are put forth as standards for types of industries that are "Specific areas that require guarantees of appropriate handling" as in the "Basic Principles Regarding Protection of Personal Information (Cabinet decision as of April 2, 2004)," and this includes public agencies such as government institutions, and large companies that have high name recognition.

Table 5-4: Method for Calculating the Degree of Social Responsibility

Basic Criteria		Degree of Social Responsibility
Higher than normal	Specific types of industry that require guarantees of appropriate handling (medical, financial / credit, information / communications, etc.), large companies that have high name recognition, and government institutions.	2
Normal	Other normal companies, associations, and organizations.	1

5.1.5 Appraisal of Response Position

In the formula ('02), we used "approach to response" as a parameter to evaluate the response of the information management organization after exposure of incidents of information disclosure. In the formula ('03), we changed "approach to response" to "appraisal of response position," in order to clarify the determining criteria for evaluation, and we determined the appropriateness of the response by applying the following examples of response activities. Select values to be used in "appraisal of response position" from Table 5-5.

Where the response position is "unclear, other," this is considered that an inappropriate response was not applied, and therefore it receives the same value as an appropriate response.

Table 5-5: Method for Calculating the Appraisal of Response Position

Criteria for evaluation	Appraisal of response position
Appropriate responses	1
Inappropriate responses	2
Unclear, other	1

Examples of appropriate responses

- Rapid response (response 2 or less days after reported)
- Understanding of circumstances (number of aggrieved parties, extent of impact, breakdown of disclosed information)
- Public announcement of the incident

・Subsequent disclosure of the circumstances (web page, e-mail, written documents)
・Informing aggrieved parties of details, and offering an apology
・Offering an apology to aggrieved parties (including presentation of vouchers, etc.)
・Estimates of effect that customer can expect
・Establishment of a claims contact
・Efforts to retrieve disclosed information
・Thanks to the party that informed the organization, and report of how it was handled
・Compensation to customers
・Improvement to system through participation of managers
・Investigation into causes
・Improvements in security measures
・Review of all procedures
・Expert review of appropriateness
・Implementation of advice and auditing by external experts

Examples of inappropriate responses

・Issues indicated, but not addressed
・Slow response
・Repeated occurrences
・Measures implemented, but these are ineffective
・Drafting of false reports

5.1.6 Items Removed

In the Formula (’02), there were two ways in which customers provided personal information to vendors or organizations: where customers themselves had provided personal information to vendors and organizations, and where they had replied to questionnaires and signed up for giveaways. Furthermore, there was a difference in the degree of negligence of organizations managing personal information in case of information disclosure incidents. However, the Personal Information Protection Act makes no distinction as regards information between customer information and information such as responses to questionnaires, and offers both of these the same level of protection. Therefore we removed the “Relationship with provider of information” parameter that displays the classification for the aggrieved.

In accordance with the implementation of the Personal Information Protection Act, when collecting personal information, it has become normal to clearly state to the effect that said information will not be provided to third parties, and to seek the agreement of the person to whom that information refers, therefore we have also removed the “Agreement to provision of personal information” parameter.

5.2 Prospective Calculation Method for Amounts of Compensatory Damages (‘03)

We created a calculation method to estimate the amount of compensatory damages for personal information disclosure incidents based upon the aforementioned calculation method for the value of disclosed personal information, and upon each parameter (“Formula (‘03)”).

Amount of compensatory damages

= value of disclosed personal information
x degree of social responsibility
x appraisal of response position

= (value of basic information x degree of information sensitivity x degree of ease of identifying individuals)
x degree of social responsibility of the organization that discloses information
x appraisal of response position

= basic information value [500]
x degree of information sensitivity [Max ($10^{x-1}+5^{y-1}$)]
x degree of ease of identifying individuals [6, 3, 1]
x degree of social responsibility [2, 1]
x appraisal of response position [2, 1]

Formula 5-5: Formula for Estimating Compensatory Damages for Incidents of Personal Information Disclosure [Formula (‘03)]

Using the calculation model for estimating the amounts of compensatory damages for incidents of personal information disclosure, and that includes the ideas in the EP Diagram (Diagram 5-2) and Simple-EP Diagram (Diagram 5-3), the calculation method for the value of disclosed personal information (Formula 5-2), and the calculation method for determining the degree of information sensitivity (Formula 5-3), we made the JO Model (JNSA Damage Operation Model for Individual Information Leaks).

5.3 Application to the Major Disclosure of the Uji City Basic Residential Register

We carried out a test to calculate the amount of compensatory damages by applying the formula (‘03), while referring to the verdict on the appeal as regards the major disclosure of the Uji city basic residential register.

5.3.1 About the Appeal Decision Regarding the Major Disclosure of the Uji City Basic Residential Register

The decision regarding the appeal on the major disclosure of the Uji City basic residential register gave disclosed information and the amount of damages as below. Reference: http://www.law.co.jp/cases/uji2.htm.

・Disclosed Information = Basic Residential Register Information

Records of personal information such as individual sequential residents numbers, addresses, names, sex, dates of birth, dates of taking up residence, dates of vacating, names of the head of the household, relationships with the head of household

・No. of Incidents of Disclosure

Table 5-6: Number of Incidents of Uji City Information Disclosure

Information Name	Items Disclosed
Resident records	185,800
Alien registration related	3,297
Corporate related	28,520
Total	217,617

・Amount of Damages

Payment of ¥10,000 to each resident (aggrieved party) for pain and suffering.

Lawyer's fees for each resident (aggrieved party) were ¥5,000.

Accordingly, the amount of damages per resident was ¥15,000.

In addition to normal personal information such as "name," "address," "sex," and "date of birth," the personal information that was disclosed in the major disclosure of the Uji City basic residential register included sensitive information that had high degrees of privacy, such as "names of the head of the household," and "relationships with the head of household." In addition to this, the source of the information disclosure was the Basic Residential Register for Uji City (municipal government), therefore it had the highest levels of reliability and accuracy.

As a result of the above details, and of demonstrating a serious attitude in its response, such as by carrying out collection of the data, giving explanations to residents, and implementing preventative measures after the disclosure, the sum of payments for pain and suffering came to ¥15,000.

Accordingly, if lawsuits were pursued by all 220,000 people who were affected by the disclosure of information, then the total amount of compensatory damages would come to ¥3.3 billion.

¥15,000 x 217,617 incidents = ¥3,264,255,000

Formula 5-6: Amount of Compensatory Damages in the Uji City Trial

5.3.2 Application of the Formula (‘03) to Calculate the Amount of Compensatory Damages

The results of applying the Formula (‘03) to the information in the incident of major disclosure of the Uji City basic residential register are as follows. Using the Formula (‘03) resulted in the amounts of compensatory damages coming to ¥12,000.

Amount of compensatory damages	= basic information value [500] x degree of information sensitivity [Max (10^0+5^0) = 2] x degree of ease of identifying individuals [6] x degree of social responsibility [2] x appraisal of response position [1] =¥12,000

Formula 5-7: Estimated Amount of Damages from the Uji City Trial Using the Formula (‘03)

5.4 Summary of the Formula (‘03), and Issues

Formula (‘03) referred to the EP Diagram, and used the two risk factors of “financial losses” and “emotional distress” in refining that formula. Furthermore, methods for deciding values have been simplified when compared to the Formula (‘02), making it easier to calculate the total sum of compensatory damages.

However, please remember that the sum, which is arrived at using the calculation method to estimate the amount of compensatory damages for incidents of personal information disclosure, is an estimate of sums of compensatory damages. In order to make the formula more realistic, it is necessary to accumulate examples of any appeal decisions that may be made at a later date, and to obtain public approval. It is our hope that the Formula (‘03) that has been developed from the Formula (‘02) will be useful in discussing sums of compensatory damages resulting from incidents of personal information disclosure.

Additionally, the Formula (‘03), the calculation method to estimate the amount of compensatory damages for incidents of personal information disclosure, aims to provide an index with which companies and organizations can estimate the degree of risk for the personal information that they are managing. Not all aggrieved parties in incidents of information disclosure will pursue lawsuits, however we hope that being aware of estimated sums of compensatory damages will result in investment in security, with the aim of preventing information disclosure, and that this will be a good method to preemptively avoid risk.

Issues with the Formula (‘03) are shown below.

5.4.1 Studying the Degree of Proactive Measures

The Formula (‘03) included parameters relating to an “appraisal of response position.” In the same way, we considered incorporating the “degree of proactive measures” into the formula. In order to do this, it is necessary to evaluate information disclosure measures that have been carried out in advance by the organization managing the personal information. It is necessary to specify evaluation parameters such as

normal operations and handling, covering certification, incorporation of encryption and other preventative software, databases and media, and documentation, and to develop a method to quantify the extent of these proactive measures.

In the current situation, little information is given about proactive measures in reports about incidents of information disclosure. Judging from the degree of proactive measures and the amounts of damages for incidents of personal information disclosure, we feel that it is still difficult to incorporate these in the formula.

5.4.2 Giving Thought to Changes in Sensitive Information

The definition of sensitive information changes every year as a result of changes in society and values, the birth of services that use new information and changes in that information's value, and of technical advancements. An example of this could be information for identifying an individual, which has broadened from name, address, and date of birth, to include information such as one's resident's card code and fingerprints. Additionally, it is thought that information such as that which locates an individual through the tracking functions on mobile phones will come to be regarded as private Information. Accordingly, we feel that it is necessary to periodically review the Simple-EP Diagram.

5.4.3 Calculating the Value of Disclosed Personal Information

The Formula ('03) omits the points for evaluating compensatory damages and their equivalents, that were used in the Formula ('02) as in Table 5-2, and is a method that directly calculates estimated amounts of compensatory damages. However, the Formula ('03) defines a uniform basic information value of ¥500 (points) per item of information. Accordingly, the amount of compensatory damages resulting from disclosure of personal information in 2003 (Page 18 Table 4-4) is calculated with this uniform value of 500 for basic information, even in the event of the amount of this disclosed personal information differing.

The amount of compensatory damages may be related not only to the sensitivity of the personal information, but also to the total amount that has been disclosed. As a result, we feel that there is some room for improvement of methods for extrapolating the value of basic information from the total amount of disclosed personal information.

5.5 2002 Amount of Compensatory Damages Resulting from Disclosure of Personal Information (Recalculated)

In both the Formula (‘02) and (‘03), because there are changes in the numerical criteria used in these formulas, such as in methods to calculate values of personal information, the results of the study into 2002 incidents of personal information disclosure were used in recalculating the Formula (‘03). For reference, the results of the study into incidents of personal information are shown in Table 5-7, and the recalculated results in Formula (‘03) are shown in Table 5-8.

Table 5-7: List of Personal Information Disclosure Incidents

No.	Industry Classification	Cause of Disclosure	Route of Disclosure	No. of Aggrieved	Name	Address	Date of Birth	Sex	Telephone Number	Occupation	E-mail address	Other	No.
1	Telecommunications	Operation error	E-mail	1,900							Y		1
2	Service industry (not in other classifications)	Configuration error	Web	10,000	Y				Y				2
3	Telecommunications	Operation error	FTP	1,388	Y	Y						Individual information	3
4	Telecommunications	Configuration error	Web	2,972	Y	Y	Y		Y		Y	Star sign	4
5	Telecommunications	Bug or security hole	Web	68,471	Y							Company information, ID / password, questionnaire details	5
6	Telecommunications	Management error	E-mail	900							Y		6
7	Manufacturing	Configuration error	Web	22	Y	Y			Y		Y		7
8	Wholesale / retail	Configuration error	Web	370	Y						Y		8
9	Telecommunications	Operation error	E-mail	1,462							Y		9
10	Financial / insurance	Bug or security hole	Web	4,300	Y								10
11	Telecommunications	Operation error	Web	Unclear							Y		11
12	Manufacturing	Configuration error	Web	730	Y	Y						Applicant information	12
13	Service industry (not in other classifications)	Configuration error	Web	4,000	Y	Y			Y				13
14	Service industry (not in other classifications)	Configuration error	Web	4,000	Y	Y			Y				14
15	Manufacturing	Configuration error	Web	10,000	Y	Y							15
16	Financial / insurance	Configuration error	Web	60	Y	Y	Y		Y		Y		16
17	Manufacturing	Configuration error	Web	368	Y	Y	Y	Y	Y		Y		17
18	Wholesale / retail	Configuration error	Web	1,303	Y	Y			Y		Y	Questionnaire details	18
19	Manufacturing	Configuration error	E-mail	Unclear							Y		19
20	Telecommunications	Configuration error	Web	800	Y	Y						Name list information	20
21	Manufacturing	Configuration error	Web	350	Y	Y			Y		Y	Company name, seminar application information, questionnaire details	21
22	Manufacturing	Configuration error	Web	1,000	Y						Y		22
23	Education / learning support	Configuration error	Web	1,800	Y	Y							23
24	Service industry (not in other classifications)	Configuration error	Web	37,000	Y	Y	Y		Y		Y	Bust-hip-waist measurements	24
25	Manufacturing	Configuration error	Web	45,000	Y	Y	Y			Y	Y	Questionnaire details	25
26	Service industry (not in other classifications)	Configuration error	Web	242	Y	Y							26
27	Telecommunications	Configuration error	Web	340	Y	Y						Name list information	27
28	Telecommunications	Configuration error	Web	1,500	Y	Y					Y		28
29	Telecommunications	Configuration error	Web	4,700	Y	Y						Questionnaire details	29
30	Combined service activities	Configuration error	Web	14,000	Y	Y			Y		Y	Questionnaire details	30
31	Service industry (not in other classifications)	Configuration error	Web	700	Y	Y			Y				31
32	Education / learning support	Configuration error	Web	2,000	Y	Y			Y				32
33	Service industry (not in other classifications)	Illegal access	Web	280	Y	Y			Y		Y		33
34	Service industry (not in other classifications)	Configuration error	Web	6,541	Y	Y						(Visitor name list information)	34
35	Real estate	Unclear	Web	Unclear								Pre-paid card number, ID, details of questions	35
36	Service industry (not in other classifications)	Illegal access	Web	1,100	Y	Y			Y	Y			36
37	Telecommunications	Unclear	Unclear	5,000	Y	Y			Y				37
38	Wholesale / retail	Configuration error	Web	1,600	Y							Unclear	38
39	Manufacturing	Bug or security hole	Web	1,200	Y	Y			Y				39
40	Education / learning support	Bug or security hole	Web	2,093	Y				Y		Y	Details of enquiries	40
41	Telecommunications	Bug or security hole	Web	100,000	Y	Y	Y					Portrait photograph, height, blood type, annual income, academic record, interests	41
42	Telecommunications	Configuration error	Web	Unclear	Y	Y						ID / password, personal information	42
43	Telecommunications	Configuration error	Web	Unclear	Y	Y			Y				43
44	Manufacturing	Configuration error	Web	1,700	Y								44
45	Education / learning support	Removal of information	Web	304	Y							Information on future studies of graduates, academic performance	45
46	Telecommunications	Removal of information	Web	17,000	Y	Y	Y	Y	Y	Y	Y	Blood type, interests, ID, internal company documents	46
47	Public service (not in other classifications)	Management error	E-mail	350							Y		47
48	Real estate	Bug or security hole	Web	398	Y	Y			Y	Y	Y		48
49	Telecommunications	Configuration error	E-mail	235	Y	Y						Global IP	49
50	Manufacturing	Bug or security hole	Web	3,244	Y	Y	Y	Y	Y	Y	Y		50
51	Manufacturing	Illegal access	Web	1,200	Y	Y					Y		51
52	Education / learning support	Unclear	Web	400	Y							Academic history, questionnaire details	52
53	Manufacturing	Operation error	Web	50,000	Y	Y	Y		Y		Y	Questionnaire details	53
54	Real estate	Configuration error	Web	335	Y	Y			Y		Y		54
55	Public service (not in other classifications)	Operation error	E-mail	59							Y		55
56	Service industry (not in other classifications)	Bug or security hole	Web	Unclear	Y							Credit card numbers	56
57	Education / learning support	Internal crime	E-mail	483	Y	Y	Y	Y	Y				57
58	Telecommunications	Bug or security hole	Web	65	Y	Y			Y		Y	Readings of names, names of hotels where reservations have been made, number of people, amounts	58
59	Public service (not in other classifications)	Operation error	Web	154	Y	Y				Y			59
60	Public service (not in other classifications)	Configuration error	Web	190	Y	Y			Y		Y	Ideas in submissions	60
61	Education / learning support	Configuration error	Web	3,107	Y	Y		Y	Y		Y	High school graduated from	61
62	Telecommunications	Bug or security hole	Web	Unclear	Y								62
	Total			418,716	54	42	10	5	28	6	30		
	Average per incident (excluding "unclear")			8,210.1	87%	68%	16%	8%	45%	10%	48%		

Table 5-8: 2002 List of Amounts of Compensatory Damages Resulting from Disclosure of Personal Information (New Formula)

No.	Industry Classification	No. of Aggrieved	Emotional Distress Level (x)	Financial Loss Level (y)	Degree of Information Sensitivity	Degree of Social Responsibility	Appraisal of Response Position	Degree of Ease of Identifying Individuals	Average amount of Compensatory Damages per Aggrieved Party	Total Compensatory Damages (¥'000)	No.
1	Telecommunications	1,900	1	1	2	2	1	3	¥6,000	¥11,400	1
2	Service industry (not in other classifications)	10,000	1	1	2	1	1	1	¥1,000	¥10,000	2
3	Telecommunications	1,388	1	1	2	2	1	6	¥12,000	¥16,656	3
4	Telecommunications	2,972	1	1	2	2	1	6	¥12,000	¥35,664	4
5	Telecommunications	68,471	2	2	15	2	1	3	¥45,000	¥3,081,195	5
6	Telecommunications	900	1	1	2	2	1	1	¥2,000	¥1,800	6
7	Manufacturing	22	1	1	2	1	1	6	¥6,000	¥132	7
8	Wholesale / retail	370	1	1	2	1	1	3	¥3,000	¥1,110	8
9	Telecommunications	1,462	1	1	2	2	1	1	¥2,000	¥2,924	9
10	Financial / insurance	4,300	1	1	2	2	1	3	¥6,000	¥25,800	10
11	Telecommunications	Unclear	1	1	2	2	1	1	¥2,000	Unclear	11
12	Manufacturing	730	1	1	2	1	1	6	¥6,000	¥4,380	12
13	Service industry (not in other classifications)	4,000	1	1	2	1	1	6	¥6,000	¥24,000	13
14	Service industry (not in other classifications)	4,000	1	1	2	1	1	6	¥6,000	¥24,000	14
15	Manufacturing	10,000	1	1	2	1	1	6	¥6,000	¥60,000	15
16	Financial / insurance	60	1	1	2	2	1	6	¥12,000	¥720	16
17	Manufacturing	368	1	1	2	1	1	6	¥6,000	¥2,208	17
18	Wholesale / retail	1,303	2	1	11	1	1	6	¥33,000	¥42,999	18
19	Manufacturing	Unclear	1	1	2	1	1	1	¥1,000	Unclear	19
20	Telecommunications	800	1	1	2	2	1	6	¥12,000	¥9,600	20
21	Manufacturing	350	2	1	11	1	1	6	¥33,000	¥11,550	21
22	Manufacturing	1,000	1	1	2	1	1	3	¥3,000	¥3,000	22
23	Education / learning support	1,800	1	1	2	1	1	6	¥6,000	¥10,800	23
24	Service industry (not in other classifications)	37,000	2	1	11	1	1	6	¥33,000	¥1,221,000	24
25	Manufacturing	45,000	2	1	11	1	1	6	¥33,000	¥1,485,000	25
26	Service industry (not in other classifications)	242	1	1	2	2	1	6	¥12,000	¥2,904	26
27	Telecommunications	340	1	1	2	2	1	6	¥12,000	¥4,080	27
28	Telecommunications	1,500	1	1	2	2	1	6	¥12,000	¥18,000	28
29	Telecommunications	4,700	2	1	11	2	1	6	¥66,000	¥310,200	29
30	Combined service activities	14,000	2	1	11	1	1	6	¥33,000	¥462,000	30
31	Service industry (not in other classifications)	700	1	1	2	1	1	6	¥6,000	¥4,200	31
32	Education / learning support	2,000	1	1	2	1	1	6	¥6,000	¥12,000	32
33	Service industry (not in other classifications)	280	1	1	2	2	1	6	¥12,000	¥3,360	33
34	Service industry (not in other classifications)	6,541	1	1	2	1	1	6	¥6,000	¥39,246	34
35	Real estate	Unclear	2	2	15	1	1	1	¥8,000	Unclear	35
36	Service industry (not in other classifications)	1,100	1	1	2	2	1	6	¥12,000	¥13,200	36
37	Telecommunications	5,000	1	1	2	2	1	6	¥12,000	¥60,000	37
38	Wholesale / retail	1,600	1	1	2	1	1	3	¥3,000	¥4,800	38
39	Manufacturing	1,200	1	1	2	1	1	6	¥6,000	¥7,200	39
40	Education / learning support	2,093	2	1	11	1	1	3	¥17,000	¥34,535	40
41	Telecommunications	100,000	2	2	15	2	1	6	¥90,000	¥9,000,000	41
42	Telecommunications	Unclear	1	2	6	2	1	6	¥36,000	Unclear	42
43	Telecommunications	Unclear	1	1	2	2	1	6	¥12,000	Unclear	43
44	Manufacturing	1,700	1	1	2	1	1	3	¥3,000	¥5,100	44
45	Education / learning support	304	2	1	11	2	1	3	¥33,000	¥10,032	45
46	Telecommunications	17,000	2	1	11	2	1	6	¥66,000	¥1,122,000	46
47	Public service (not in other classifications)	350	1	1	2	2	1	1	¥2,000	¥700	47
48	Real estate	398	1	1	2	1	1	6	¥6,000	¥2,388	48
49	Telecommunications	235	1	1	2	2	1	6	¥12,000	¥2,820	49
50	Manufacturing	3,244	1	1	2	1	1	6	¥6,000	¥19,464	50
51	Manufacturing	1,200	1	1	2	1	1	6	¥6,000	¥7,200	51
52	Education / learning support	400	2	1	11	1	1	1	¥6,000	¥2,200	52
53	Manufacturing	50,000	2	1	11	1	1	6	¥33,000	¥1,650,000	53
54	Real estate	335	1	1	2	1	1	6	¥6,000	¥2,010	54
55	Public service (not in other classifications)	59	1	1	2	2	1	1	¥2,000	¥118	55
56	Service industry (not in other classifications)	Unclear	1	3	26	2	1	3	¥78,000	Unclear	56
57	Education / learning support	483	1	1	2	1	1	6	¥6,000	¥2,898	57
58	Telecommunications	65	1	1	2	1	1	6	¥6,000	¥390	58
59	Public service (not in other classifications)	154	1	1	2	2	1	6	¥12,000	¥1,848	59
60	Public service (not in other classifications)	190	2	1	11	2	1	6	¥66,000	¥12,540	60
61	Education / learning support	3,107	1	1	2	1	1	6	¥6,000	¥18,642	61
62	Telecommunications	Unclear	1	1	2	2	1	3	¥6,000	Unclear	62
	Total	418,716								¥18,922,013	
	Average per incident (excluding "unclear")	7,613.0								¥344,037	

5.5.1 Comparison of Amounts of Compensatory Damages from Formulas (‘02) and (‘03)

Here are the results of using the Formula (‘02) and (‘03) for the 2002 amount of compensatory damages for information disclosure. Table 5-9 shows the results of this comparison.

Table 5-9: Results of Calculations Using the Improved Method (Comparison)

		Formula (’02)	Formula (’03)
Total amount of damages		¥15,142,700,000	¥18,922,010,000
Maximum amount of damages		¥10,000,000,000	¥9,000,000,000
Average Amount of Damages	Per incident	¥240,360,000	¥344,030,000
	Per aggrieved	¥36,165	¥45,191
	Range of damages per aggrieved	¥5000, ¥10,000, ¥50,000, ¥100,000	¥1000 ~ ¥90,000

Because the Formula (‘03) could calculate the amounts of compensatory damages per person in units of ¥1,000, the Formula (‘03) was able to be used in calculating the amounts of compensatory damages in accordance with the details of the disclosed personal information in comparison with the Formula (‘02). Most of the personal information that was judged to have a unit value of ¥5,000 in the Formula (‘02) had its value revised upwards in the Formula (‘03), to between ¥6,000 and ¥12,000. As a consequence, the results of the recalculation through using the Formula (‘03) showed an overall increase in the amounts of compensatory damages.

5.5.2 Comparison of Amounts of Compensatory Damages 2002/2003

We compared the results of calculations for incidents of personal information disclosure in 2002/2003 using the Formula (‘03).

Table 5-10: Comparison of personal information disclosure incidents (2002/2003)

	2002	2003
Number of incidents of disclosure (*)	62 (55)	57 (51)
Total amount of damages	¥18,922,010,000	¥28,069,360,000
Maximum amount of damages	¥9,000,000,000	¥7,119,900,000
Average amount of damages	¥344,030,000	¥550,380,000
Number of aggrieved (total)	418,716	1,554,592
Maximum number of aggrieved	100,000	560,000
Number of aggrieved (average)	7,613	30,482

Note: In “Average amount of compensatory damages” and “Number of aggrieved (average),” the numbers are calculated using the number of incidents of information disclosure in which the number of aggrieved has been ascertained (number within parentheses).

While the number of incidents of personal information disclosure in 2003 was 5 fewer than in 2002 (with the number of incidents within brackets that were used for calculation of average values also being 5 fewer), there was a dramatic increase in the numbers of aggrieved, and in the total amount of compensatory damages.

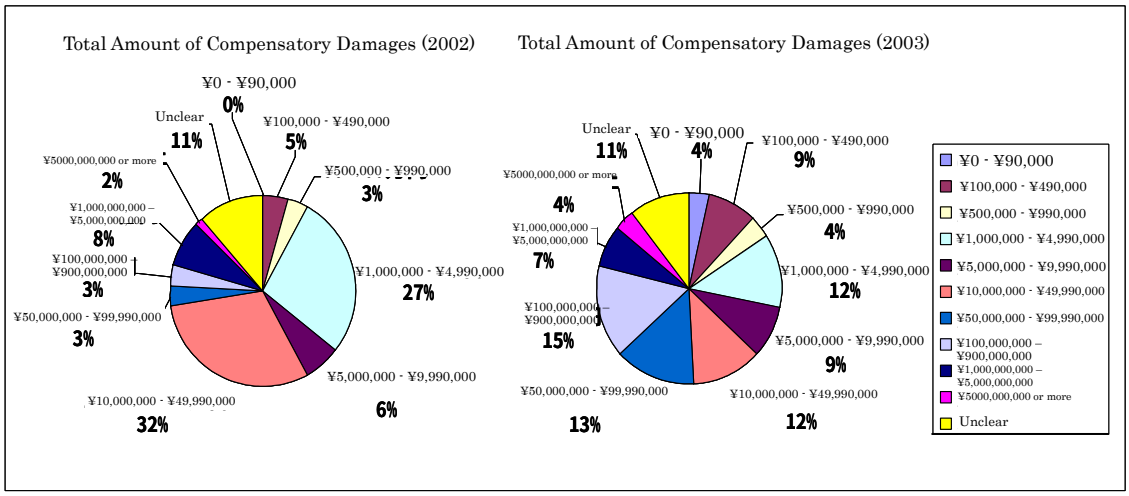


Diagram 5-5: Comparison of Total Amounts of Compensatory Damages

In 2002, there were a total of 8 incidents in which the amount of compensatory damages exceeded ¥100 million, and the total sum of compensatory damages for these 8 incidents alone comprised approx. 65% of the total. In 2003, there were a total of 15 incidents in which the amount of compensatory damages exceeded ¥100 million, and the amount of damages for these came to approx. 97% of the total. The large number of incidents with high amounts of compensatory damages had an effect on the large increase in the total amount of compensatory damages.

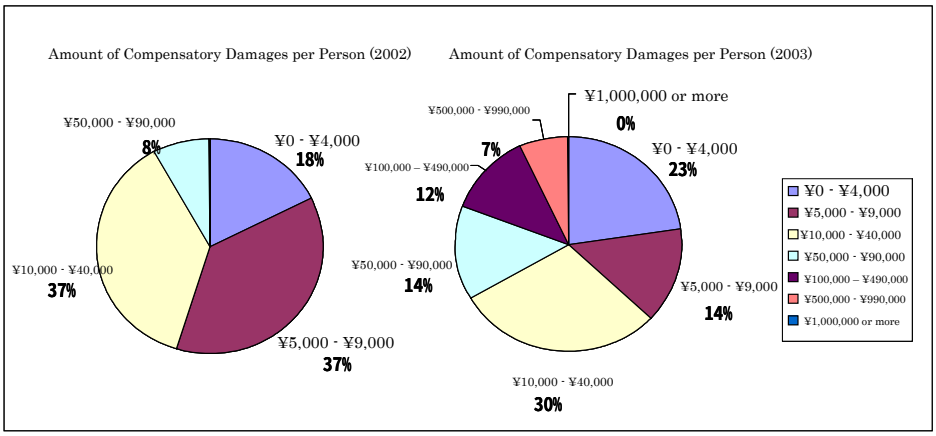


Diagram 5-6: Comparison of Amounts of Compensatory Damages per Person

Furthermore, while there were no incidents of personal information disclosure incidents in 2002 in which the amount of compensatory damages exceeded ¥100,000 per person, in 2003, 19% of incidents had amounts in excess of this figure.

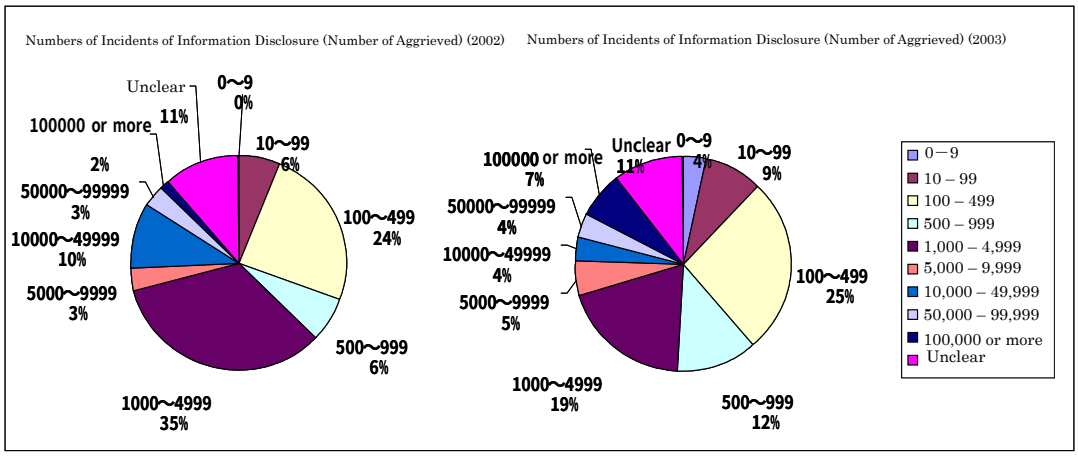


Diagram 5-7: Comparison of Numbers of Aggrieved per Incident

The number of incidents in which less than 5,000 items of information were disclosed were approximately 70% of the total in both 2002 and 2003. Concentrating on incidents in which this figure was more than 5,000, there was an increase from 3 to 6 in incidents in which more than 50,000 items of information were disclosed. A drastic increase in the number of large magnitude incidents of information disclosure is a characteristic of 2003.

6. Estimates of the Cost of Emergency Response to Incidents of Personal Information Disclosure

Costs generated from disclosure of personal information are not limited to the aforementioned compensatory damages. Consequently, we carried out a provisional estimate as to costs of emergency responses for incidents of personal information disclosure, using the 2003 information security incident damage calculation model as in Section One. When doing this, we matched parameters in the 2003 information security incident damage calculation model with details of personal information disclosure incidents for greater detail. We then created a scenario of the disclosure of personal information within a hypothetical company as below, and calculated the amount of compensatory damages.

6.1 Company Profile

The assumed company featured paper and Internet catalogs listing their products, which were sold by mail order. In recent years, it has become involved in Internet shopping, and sales through its Internet shopping site have reached approximately 10% of total company turnover. A corporate profile for this company is shown below. (Assuming a profit ratio for the Internet shopping section of approx. 10%, and approx. 10% growth per year.)

Table 6-1: Corporate Profile (Assumed)

Company Scale	
Sales	Approx. ¥100,000,000,000
Employees	Approx. 1000
Catalog Sales Section	
Members	Approx. 6,000,000
Sales	Approx. ¥90,000,000,000
Internet Shopping Section	
Members	Approx. 1,000,000
Sales	Approx. ¥10,000,000,000
Employees	Approx. 30

This company collects and manages the following items of customer information for customer relationship management.

- Name, reading of name, sex, age (category), occupation
- Post code, address, telephone number
- Purchasing history information (product codes, purchase dates/time)
- Login ID and passwords for the shopping site
- Credit card numbers, expiration dates, account numbers for accounts at financial organizations (However, credit records are handled on a separate system, and cannot be referenced from within the company.)

6.2 Assumed Scenario

We assumed the following scenario for an incident of personal information disclosure.

- An inquiry was received from 10 customers, stating that they had received suspicious direct mails.
- We envisaged an investigation revealing that information and data about approximately 300,000 customers who had made purchases and member registration had been disclosed from the Internet shopping site. The disclosed customer data was judged to be that which had been newly registered over a certain period of past few years.
- Immediately after this being recognized as an incident of personal information disclosure, a countermeasures headquarters was established. At the same time, because it was under investigation, and as a countermeasure, operation of the Internet shopping site was suspended for a period of one month.

6.3 Calculation of Costs for Response According to the Response Model

Based upon the 2003 information security incident damage calculation model, we carried out a provisional estimate of total amounts of compensatory damages for the incidents of personal information disclosure.

6.3.1 Direct Damage

6.3.1.1 Lost Earnings

1 month sales from the Internet Shopping Site × profit ratio

Approx. ¥10 billion ÷ 12 months × 10% = approx. ¥83.3 million

6.3.1.2 Opportunity Loss

From yearly growth rate of 10%

Approx. ¥10 billion ÷ 12 months × 10% × 10% = approx. ¥8.3 million

6.3.2 Indirect Damage

6.3.2.1 Costs of Continuing Business

- Personnel costs relating to organization of response operation

  No. of staff in response organization × personnel costs × no. of days = 20 staff × approx. ¥50,000 / day × 1 month (20 days)
  = approx. ¥20 million

・Cost of commissioning security consultants (to investigate the cause)

Approx. ¥2.5 million / man-month × 1 month × 2 consultants = approx. ¥5 million.

6.3.2.2 Cost of Compensatory Damages

・Cost of Compensatory Damages (+ ratio of involvement in proceedings)

The level of involvement in a class action law suit will differ depending on the contents of that suit. In class action law suits that involve product fraud, the percentage of the number of claimants is from single digits into the teens. However, in the class action law suit for the TBC personal information disclosure incident, out of a total of approximately 50,000 aggrieved, there were 10 participants in the law suit (0.02%). 39 separate consultations were taken to the TBC Privacy Damage Defense Counsel, and from these, 13 people were judged to have suffered harm, and 3 people were reported to have made expenditures. (Reference: http://homepage3.nifty.com/tbc-higai/)

From this, we can see that there was a low proportion of people who were subject to serious harm, including those who received false claim for payment, and that people are reluctant to press a civil claim even when the disclosed information is private information, and when the disclosure has caused emotional distress.

In reference to the above example, the ratio of participants in the law suit claiming compensatory damages for this hypothetical incident of personal information disclosure was 0.02%. We established other values as follows, using the hypothetical personal information from the Company Profile in 6.1.

- Degree of information sensitivity

  Emotional distress level for disclosed personal information (estimated) = 1

  From the disclosed personal information (estimated)

  {purchasing history information, shopping site ID and passwords}

  = financial loss level = 2

  Degree of information sensitivity = $10^0 + 5^1 = 6$

- Degree of ease of identifying individuals

  From disclosed information including name, address, telephone number

  Degree of ease of identifying individuals = 6

- Degree of social responsibility

  From Table Table 5-4: calculation method for the degree of social responsibility:

  Degree of social responsibility = 1

- Appraisal of response position

Because there was an appropriate response, from Table 5-5

Appraisal of response position = 1

Amount of compensatory damages = basic information value [500]
× degree of information sensitivity [10^0+5^1]
× degree of ease of identifying individuals [6]
× degree of social responsibility [1]
× appraisal of response position [1] = ¥18,000

Amount of compensatory damages (¥18,000) × no. of aggrieved (300,000)
× ratio of involvement in proceedings (0.02%)
= ¥18,000 × 60 people
= approx. ¥1.08 million

・Attorney fees, legal fees

As of April 1, 2003, attorney fee criteria for each bar association were abolished, and all attorneys were henceforth able to freely specify attorney fees in accordance with the "Regulations Regarding Attorney Remuneration" as specified by the Japan Federation of Bar Associations. Here, we calculated the attorney fees based upon the indicators suggested by the Daini Tokyo Bar Association (Reference: http://www.niben.jp/04info/houshuu/houshuu.html).

As mentioned at the reference page above, because the amount claimed was approximately ¥1.1 million, meaning that the amount of economic benefit corresponded to "below ¥3 million," the indicated sum of the advance was 8%, with the total remuneration being 16%. The sum of the remuneration is affected by the verdict, therefore we covered the advance only.

Amount of advance = approx. ¥1.1 million × 8% = ¥90,000

6.3.2.3 Costs for Consolation Gifts

Consolation gifts for customers (aggrieved) to show remorse were gift tokens in the range of ¥500 - ¥1,000.
(Cost of consolation gift + (assorted costs for postage, envelopes, filling in names, etc.)) × 300,000 people
= (¥500 + ¥200) × 300,000 people = approx..¥210 million

6.3.2.4 Cost of Apology Visits

Visits to the 10 people who brought the incident of personal information disclosure to our attention, and to five

people for whom an expression of apology is required

（(Personnel costs + transport costs) × no. of staff required to carry out visit × no. of people to visit = (approx. ¥50,000 + approx. ¥5,000) × 2 staff × (10 people + 5 people)

= approx. ¥1.65 million

6.3.2.5 Public Relations Costs

・Cost of published apology

Placement of apologies in 5 newspapers (national newspapers, morning editions, general news page, side box)

Approx. ¥2 million × 5 newspapers = approx. ¥10 million

・Costs for creation of an information publicity page on the web site, for the information disclosure incidents

Approx. ¥50,000 × 5 = approx. ¥250,000

6.3.2.6 Costs for Extraordinary Countermeasures

・Establishment of a call center to answer questions

Costs to establish a new inquiries call center = approx. ¥10 million

(Total cost, including operator costs, etc. for one month)

・Costs for staff to take charge of contact for inquiries

Personnel costs for staff required to be stationed in this position

¥50,000 / day × 3 staff × 1 month = ¥3 million

6.3.3 Potential Damages

6.3.3.1 Business Affected

・Personnel costs for staff in affected department

Department and staff who had been working at the Internet Shop

Fixed costs (personnel) × no. of affected staff = approx. ¥50,000/day × 30 staff × 1 month

= approx. ¥30 million

6.3.3.2 Potential Damage Outside the Business

・Reduction in brand value

When looking at a reduction in brand value when seen from the point of view of shifts in the share price, not all incidents of information disclosure result in a reduction in share prices (refer 7.1). Share prices are

also affected by factors other than information disclosure incidents, therefore this unknown is labeled α.

Effect on share prices = α

6.4 Summary of the Results of Provisional Estimates on Total Amounts of Damages

Results of provisional estimates on total amounts of damages based around this hypothetical scenario of personal information disclosure incident were approximately ¥382.37 million + α. Results of provisional estimates for each parameter are shown in Table 6-2.

Table 6-2: Amount of Damage from Incidents of Personal Information Disclosure (Provisional Estimates)

Item			Cost
Direct Damages	Lost Earnings	Sales profit from the Internet Shopping Site (1 month)	Approx. ¥83.3 million
	Opportunity Loss	Amount based on the Growth rate of the Internet Shopping Site (1 month)	Approx. ¥8.3 million
Indirect Damages	Costs of Continuing Business	Personnel costs relating to organization of response operation (1 month)	Approx. ¥20 million
		Cost of commissioning security consultants (1 month)	Approx. ¥5 million
	Cost of Compensatory Damages	Cost of Compensatory Damages	Approx. ¥1.08 million
		Attorney fees, legal fees	Approx. ¥90,000
	Costs for Consolation Gifts	Cost of consolation gift + shipping, etc. (for 300,000 people)	Approx. ¥210 million
	Cost of Apology Visits	Cost of Apology Visits (for 15 people)	Approx. ¥1.65 million
	Public Relations Costs	Cost of published apology (5 newspapers)	Approx. ¥10 million
		Costs for creation of an information publicity page (x5)	Approx. ¥250,000
	Costs for Extraordinary Countermeasures	Establishment of a call center to answer questions (1 month)	Approx. ¥10 million
		Costs for staff to take charge of contact for inquiries (1 month)	Approx. ¥3 million
Potential Damages	Business Affected	Personnel costs for staff in affected department (1 month)	Approx. ¥30 million
	Potential Damage Outside the Business	Reduction in brand value	+ α
		Total	Approx. ¥382.37 million

The Internet shopping section has annual profits of approximately ¥1 billion, (annual sales of approx. ¥10 billion), therefore an expense on the scale of approximately ¥382.37 million would pose a huge burden upon the company. Table 6-2 shows that direct damage to the company, and costs for consolation gifts comprise approximately 80% of the provisionally estimated damages of some ¥380 million. In 2003, gift tokens presented as apologies were in the range of ¥500 - ¥1,000. Accordingly, we calculated these costs based upon this going rate. Sending of these consolation gifts is an expression of remorse from the company towards customers (the aggrieved), and is not indispensable.

Costs for sending the consolation gifts grow in proportion to the number of incidents of information disclosure. For the aggrieved, instead of a one time expression of apology, maybe they would consider the increase in their sense of security and trust would be more valuable, for example through support, the retrieval of the disclosed information, and measures to prevent recurrence of these incidents.

These provisional estimates show that the disclosure of personal information shows up not only as compensatory damages, but as a major influence on corporate activities, and as other losses. Organizations that handle large amounts of personal information need to investigate both the personal information that is being used within it, and the business activities that use that information, and to fully understand the total amount of damages that can result from incidents of personal information disclosure. Next, by referring to the total amounts of damages, they need to implement risk prevention and loss mitigation policies, such as by an investment in appropriate security, establishment of internal systems, and the installation of network assurances to reduce response costs in the event of damage.

7. About the Effect of Incidents of Information Disclosure on Corporate Value (Considering Changes in Share Prices)

Every day, companies are striving to improve the perception of confidence that customers have in them, and while carrying out advertising and IR activities, are building up the value of their enterprise. However, once there is an incident of information disclosure, it can be expected that their image will be tarnished, their share prices will drop, and the worst case scenario may be one in which the very existence of the company is threatened.

Because of this, it is very important to measure, and to be aware of to what extent incidents of information disclosure can harm the corporate value of a company.

Here, as we did last year, we will focus our attention on actual information disclosure incidents (limited to those that were announced during 2003) and changes in the share prices of the companies that were affected, and will investigate and consider the degree of effect that information disclosure can have upon the value of the companies.

7.1 Understanding the Effect of Information Disclosure Incidents on Corporate Value

7.1.1 Conceptual Model

When an information disclosure incident occurs, there is no doubt that trust in that company is adversely affected. We are assuming that if the company is listed, then one impact will be a change in its share prices.

Under the aforementioned hypothesis, in verifying changes in corporate share prices attributable to information disclosure incidents, we are assuming a conceptual model which states that said company's share prices are somewhat tied to the stock market as a whole, and that the stock market as a whole can approximate the Nikkei Stock Average (stock market as a whole Nikkei Stock Average).

In other words, by working in line with this conceptual model, the share prices of said company should rise (only for listed companies) when the Nikkei Stock Average is on the rise; however if these drop, then it can be inferred that there has been the impact of an information disclosure incident (at the very least, it is difficult to fully deny the effect of information disclosure incidents at this time).

7.1.2 Formulas

1) Changes in share prices (deviance from the company's expected share price)

The changes in share prices are calculated from how much the company share price (closing price) on the n^{th} day since the date the information disclosure incident is announced (initial reports of the incident, and results of the investigation) is deviated from the expected share price of the company on the n^{th} day, which is calculated from the movement of the Nikkei Stock Average.

The "ratio of the company's share price compared to the Nikkei Stock Average" is used when calculating the expected share price for the company n days after the incident. Below, the ratio on day n is referred to as the "n day ratio," and the basic ratio as the "base ratio."

$$\text{n day ratio} = \frac{\text{Share price of the company on the } n^{th} \text{ day (closing price)}}{\text{Nikkei Stock Average share price on the } n^{th} \text{ day (closing price)}} \quad \cdots\cdots\cdots\cdots \quad (1)$$

$$\text{base ratio} = \frac{\text{The company's standard share price (closing price)}}{\text{Nikkei Stock Average standard share price (closing price)}} \quad \cdots\cdots\cdots\cdots \quad (2)$$

Furthermore, in this investigation, for "the company's standard share price (closing price)" and "the standard Nikkei Stock Average share price (closing price)", which are the basis for calculation of standard ratios in Formula (2), we used the average of company's share prices (closing prices) and the average of Nikkei share prices (closing prices) for one week before the date the information disclosure incident was announced. This helps accidental errors resulting from sudden rises or drops the day before the incident is announced.

The deviance from the expected share price for the company on day n (the "deviance value") is calculated as below from Formulas (1) and (2).

$$\text{Deviance value} = (\text{n day ratio} - \text{base ratio}) \times \text{Nikkei Stock Average share price on the } n^{th} \text{ day (closing price)} \quad \cdots\cdots\cdots\cdots \quad (3)$$

2) Influence of changes in share prices upon the corporate value.

The amount of influence upon the corporate value is calculated by multiplying the average deviance value with the number of the company's shares issued. The formula is as follows. Furthermore, the period of calculation shall be 14 days from when the incident is announced.

$$\text{Amount of influence on corporate value} = \text{average deviance value} \times \text{number of shares issued} \quad \cdots\cdots\cdots\cdots \quad (4)$$

7.2 An Example - Considerations on the Influence upon the Corporate Value

1) Influence of the first announcement of an information disclosure incident upon the corporate value

Table 7-1 calculates the change over time in the deviance value, and the amount of influence upon the corporate value per day from the time the information disclosure incidents were first disclosed in 2003, for 18 listed companies (limited to those that were announced during 2003). As regards the amount of influence upon the corporate value per day (amount of short term effect) for the first 14 days after the first announcement on the incidents, there are some companies that showed increases, however of the 18 companies, 12 exhibited a drop.

Additionally, changes in deviance value over time after the first announcement are shown in Table 7-2, where values above the horizontal line are pluses, (the share price for that company was above the company's expected share price), and values below that line were minuses (these were below the company's expected share price). It is difficult to make generalizations about these changes in deviance value over time, from the time after the first announcement. We can see some patterns in the pluses and minuses for the deviance value, however making determinations from this study alone is difficult.

2) Influence of the announcement of the results of later investigations upon the corporate value

In reports of information disclosure incidents, most of the companies established an investigative committee with the company president at its head, vowing to establish the cause of the incident. Here, we consider the change over time in the deviance value, and the amount of the influence upon the corporate value per day, resulting from the disclosure of the results of these investigations for 5 listed companies. These results are shown in Table 7-3. Furthermore, Table 7-4 shows a graphed version of these results in comparison to at the time of the first announcement. While we can see changes in the share prices after both the first announcement, and after disclosure of the results of the investigation from Table 7-3 and Table 7-4, it was difficult to determine whether or not there was any effect on restoring trust in the company by disclosing these results.

3) Influence upon the corporate value for concerned parties and contractors

In information disclosure incidents in 2003, there were a number of cases where names of companies contracted for services were disclosed. Here, we will consider the influence this had on the corporate value of the companies concerned and the contracted companies. These results are shown in Table 7-5 and Table 7-6. We saw the influence upon the corporate value of the companies and contractors in which it was assumed that the incident had the same cause, as showing an about-face with the plus and minus values (one side showing mainly minuses, while the other showing mainly pluses).

Additionally, in 2 cases, the damage was greater to the contractor than to the company themselves. If this is correct, we would expect to see the companies disclosing information about contractors in order to

transfer a part or all of the damage to the contractor, however unfortunately at the current stage, this can not be verified.

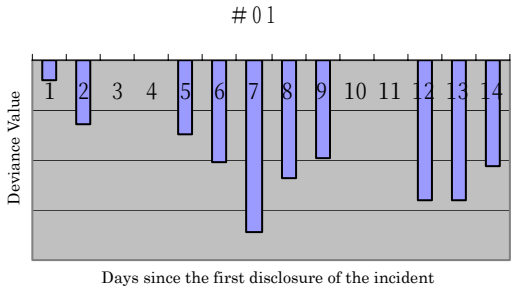
Table 7-1: Changes in the Deviance Value, and the Amount of Corporate Value per Day resulting from First Disclosure of the Report

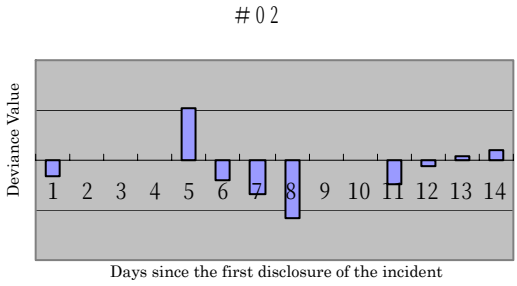
Case		#01	#02	#03	#04	#05	#06
Number of shares issued		107,600,000	97,683,133	858,672,607	63,859,251	2,955,000	147,295,200
Deviance value from the company's expected share price on the n^{th} day from the date of first disclosure of the incident (day prior to disclosure of incident as baseline)	1	▲38.25	▲16.56	▲11.41	▲10.87	▲22.69	▲121.53
	2	▲126.84		▲7.22			332.03
	3			▲2.14			666.15
	4				▲7.74		333.70
	5	▲148.88	52.71		▲6.64	▲122.78	
	6	▲203.07	▲19.91	3.92	▲4.83	▲209.88	
	7	▲342.20	▲34.90	1.01	▲0.71	▲130.66	332.53
	8	▲234.56	▲57.38	9.87	▲2.12	▲121.96	269.58
	9	▲195.30		7.82			161.77
	10			0.35			310.74
	11		▲24.02		▲0.10	▲37.40	3.88
	12	▲279.25	▲6.22		▲2.75	▲114.77	
	13	▲278.57	4.41	▲6.45	▲3.13	▲120.10	
	14	▲213.59	9.01	▲1.40	▲5.95	▲71.05	
	Total	▲2,060.52	92.84	▲5.65	▲44.84	▲951.28	2,288.85
	Daily average	▲206.05	▲10.32	▲0.57	▲4.48	▲105.70	254.32
Amount of influence on corporate value (daily average)		▲22,171,217,598	▲1,007,631,228	▲485,311,206	▲286,353,796	▲312,337,011	37,459,703,613

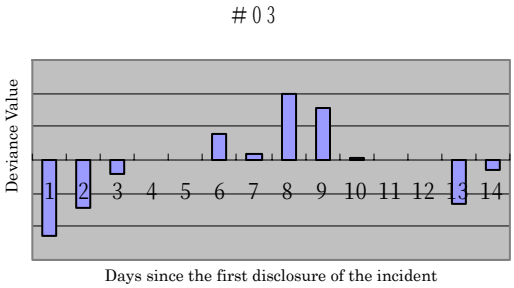
Case		#07	#08	#09	#10	#11	#12
Number of shares issued		211,317,082	661,639,986	77,648,751	2,240,000	1,482,973,799	11,375,069,845
Deviance value from the company's expected share price on the n^{th} day from the date of first disclosure of the incident (day prior to disclosure of incident as baseline)	1	3.16	▲0.98	▲3.84	18,297.41	11.20	7.40
	2	7.85	▲1.35	▲8.19	10,541.94		
	3	11.50	1.00	▲5.80			
	4			▲3.94		3.54	9.05
	5				25,516.66	7.63	7.07
	6	10.91	0.61		11,668.16	▲5.07	6.19
	7	5.25	▲0.31	▲3.84	24,905.94	▲1.86	4.53
	8	1.36	0.21		▲5,530.62	▲7.44	4.56
	9	▲8.79	1.66	▲12.09	5,619.35		
	10	▲13.28	6.85	▲8.76			
	11			▲15.04		▲3.16	4.42
	12					▲0.54	6.47
	13	▲15.13	6.64		25.51	▲3.77	5.61
	14	▲14.98	6.14	▲20.65	▲17,471.74	▲0.01	2.86
	Total	▲12.31	20.47	▲82.13	73,572.61	0.52	58.15
	Daily average	▲1.23	2.05	▲9.13	8,174.73	0.05	5.81
Amount of influence on corporate value (daily average)		▲260,100,870	1,354,500,428	▲708,575,857	18,311,404,791	77,055,394	66,143,283,185

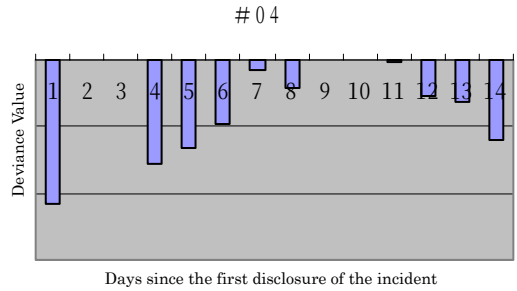
Case		#13	#14	#15	#16	#17	#18
Number of shares issued		92,501,833	1,929,268,717	744,912,078	421,254	2,805,000	377,082
Deviance value from the company's expected share price on the n^{th} day from the date of first disclosure of the incident (day prior to disclosure of incident as baseline)	1	▲4.29	▲30.80	▲34.26	▲897.75	▲15,733.01	▲16,685.28
	2	▲6.92	▲33.09		▲1,759.73	▲15,171.91	▲47,506.16
	3	▲7.66			▲403.98	▲16,869.83	▲13,680.38
	4	▲6.27		▲45.02			▲25,192.78
	5			▲3.83			▲59,228.92
	6		1.22	14.01	232.83	▲5,432.69	
	7	▲1.61	1.98	133.76		▲11,858.05	
	8	▲8.63	25.58	11,346	▲1,369.10	▲17,856.56	▲60,940.78
	9	▲8.19	19.39		▲3,448.42	▲17,301.00	
	10	▲8.64			1,220.09	▲13,364.31	▲30,775.69
	11	▲4.90		87.21			12.47
	12		12.21	57.12			23,081.48
	13		▲1.35	119.58	▲646.77	▲18,805.98	
	14	24.66	▲12.39	156.98	992.66		
	Total	▲32.46	▲17.25	599.02	▲6,080.17	▲132,393.35	▲230,916.05
	Daily average	▲3.25	▲1.92	59.90	▲676.57	▲14,710.37	▲25,657.34
Amount of influence on corporate value (daily average)		▲300,260,009	▲3,697,318,776	44,621,905,127	▲284,588,230	▲41,262,593,460	▲96,781,584,542

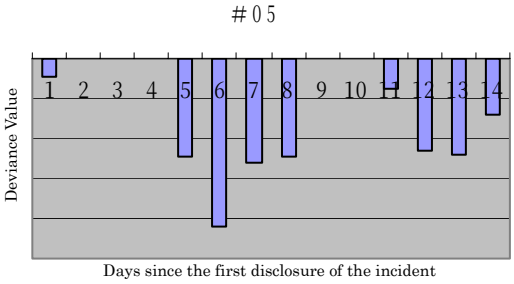
Table 7-2: Graph of Changes in the Deviance Value resulting from First Disclosure of the Report

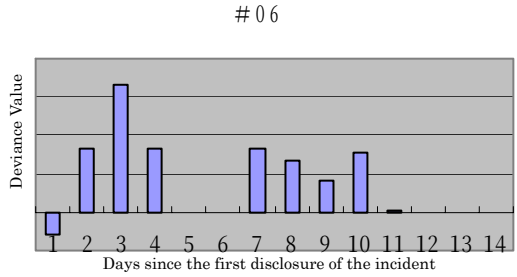


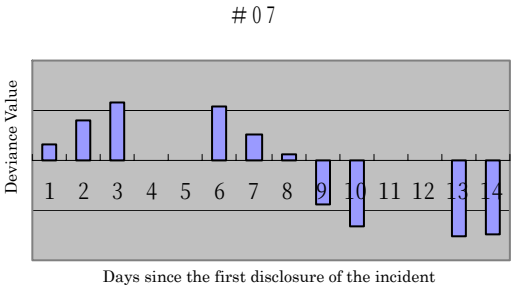


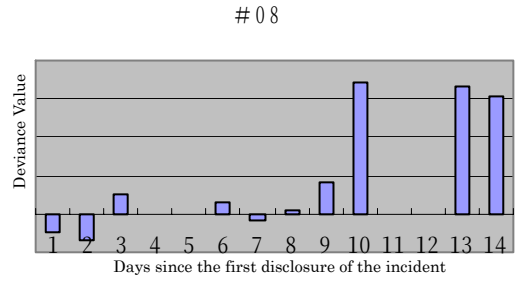


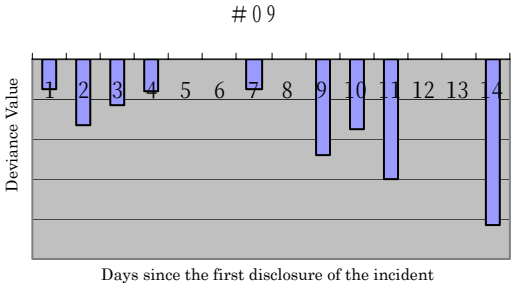












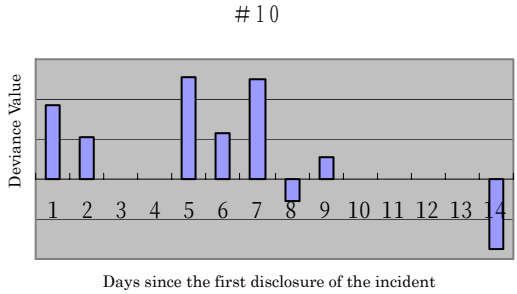
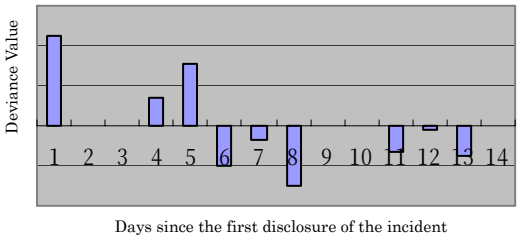
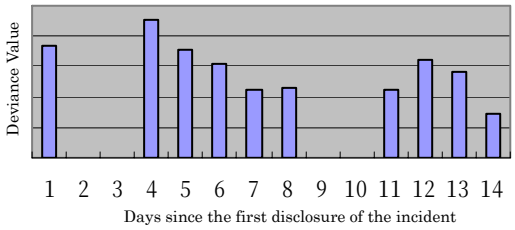


Table 7-2: Graph of Changes in the Deviance Value resulting from First Disclosure of the Report(Cont.)

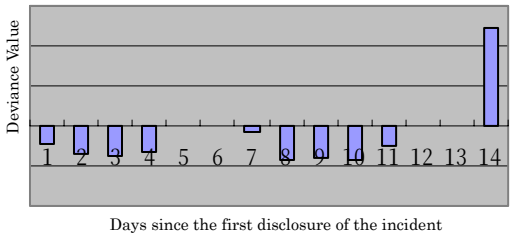
#11



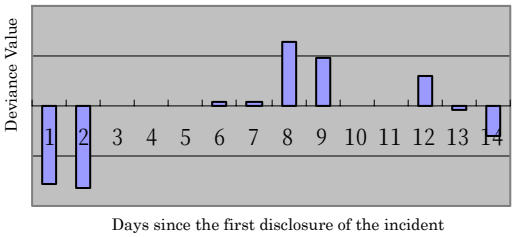
#12



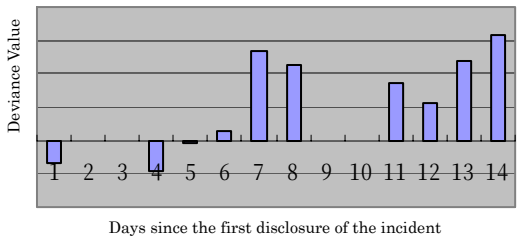
#13



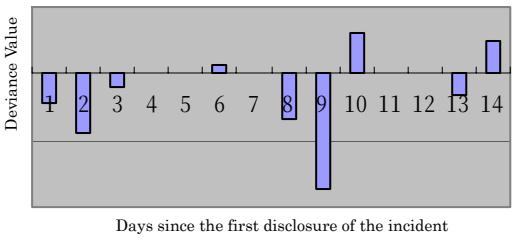
#14



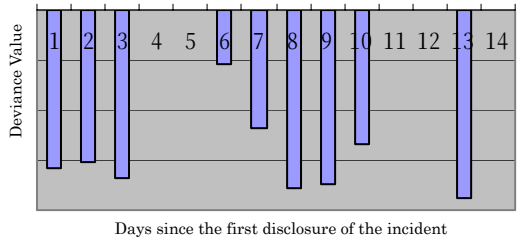
#15



#16



#17



#18

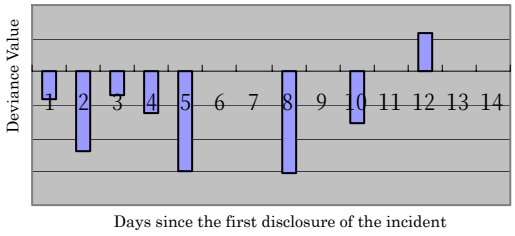
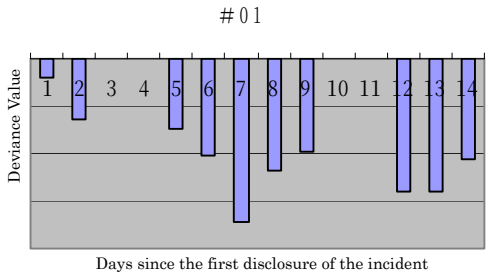
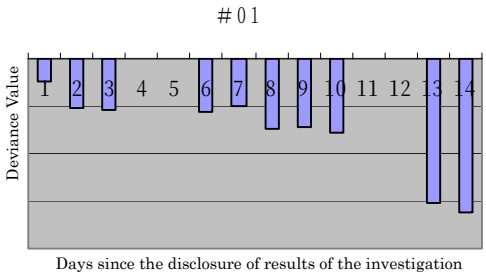


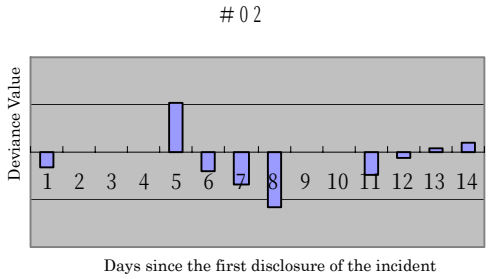
Table 7-3: Changes in the Deviance Value, and the Amount of Corporate Value per Day resulting from Disclosure of Results of the Investigation

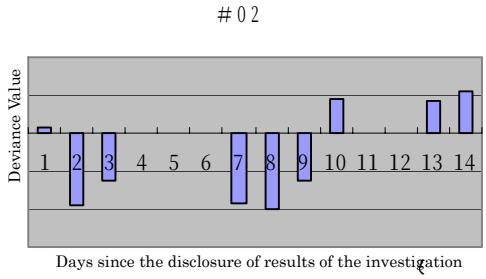
Case		#01	#02	#03	#04	#05
Number of shares issued		107,600,000	97,683,133	858,672,607	63,859,251	2,955,000
Deviance value from the company's expected share price on the n^{th} day from the date of the disclosure of results of the investigation (day prior to disclosure of incident as baseline)	1	▲46.09	7.77	▲18.63	5.64	18.19
	2	▲105.58	▲95.01			7.42
	3	▲107.36	▲62.05			
	4			▲27.41		
	5			▲27.37	8.47	▲2.45
	6	▲113.67		▲34.29	21.18	
	7	▲100.73	▲91.75	▲30.93	46.65	17.83
	8	▲146.76	▲99.23	▲39.55	37.83	189.17
	9	▲143.24	▲63.50			357.41
	10	▲155.67	45.95			
	11			▲47.58	43.60	
	12			▲43.72		318.62
	13	▲305.22	41.30	▲34.18	46.26	328.87
	14	▲324.81	54.72	▲32.27	32.65	
	Total	▲1,549.13	▲261.81	▲335.93	242.27	1,235.05
	Daily average	▲154.91	▲29.09	▲33.59	30.28	154.38
Amount of influence on corporate value (daily average)		▲16,668,639,101	▲2,841,615,775	▲28,845,378,206	1,933,898,490	456,194,975

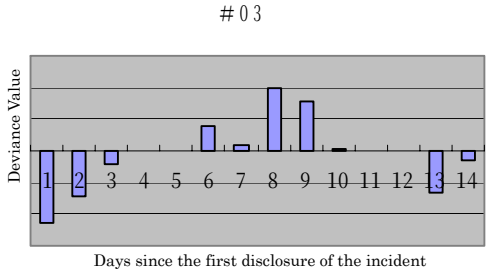
Table 7-4: Graph of Changes in the Deviance Value resulting from Disclosure of Results of the Investigation (R)

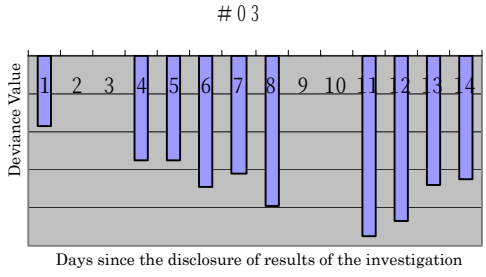


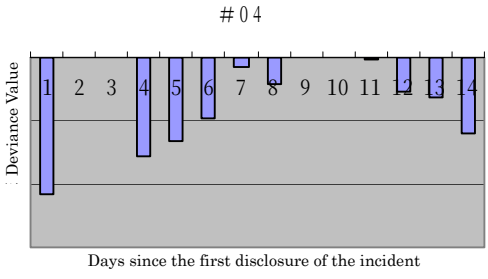


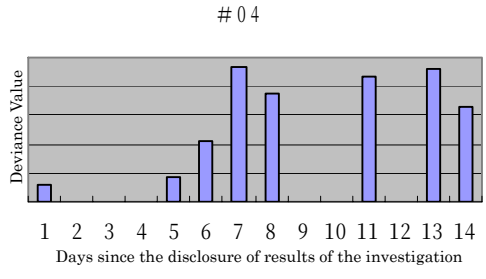


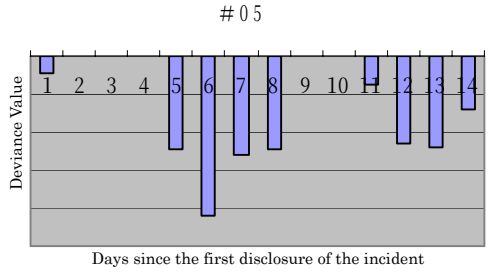












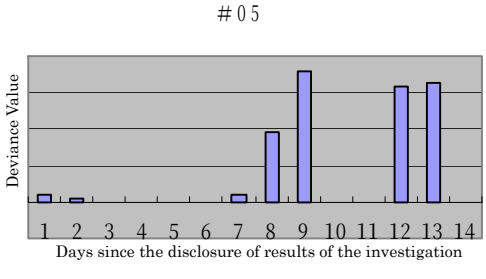
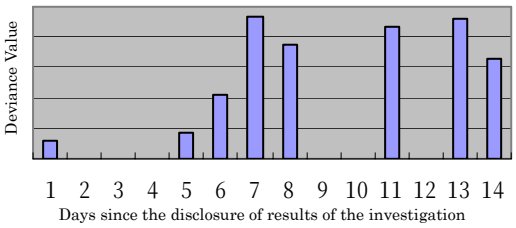


Table 7-5: Changes in the Deviance Value, and the Amount of Corporate Value per Day for Contractors

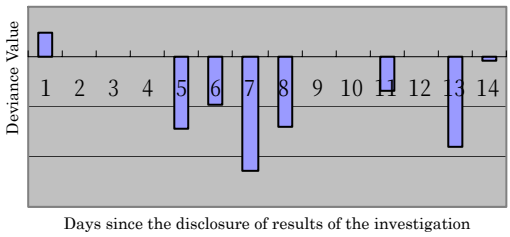
Case		#04	#15	#18
Disclosure period		When results of the investigation are disclosed	First disclosure of the incident	First disclosure of the incident
Number of shares issued		44,562,548	469,475,456	699,412,481
Deviance value from the contractor's expected share price on the n^{th} day from the date of first disclosure of the incident, or date of the disclosure of results of the investigation (day prior to disclosure of incident as baseline)	1	47.80	▲58.12	▲3.37
	2			▲12.63
	3			22.93
	4		▲56.99	26.75
	5	▲145.26	▲88.12	0.02
	6	▲96.65	▲61.73	
	7	▲229.80	▲56.91	
	8	▲140.91	▲161.46	13.90
	9			
	10			2.03
	11	▲69.82	▲168.72	▲1.36
	12		▲173.79	14.24
	13	▲178.10	▲144.66	
	14	▲9.55	▲145.57	
	Total	▲822.28	▲1,116.06	62.50
	Daily average	▲102.79	▲111.61	6.94
Amount of influence on corporate value (daily average)		▲4,580,389,211	▲52,396,457,133	4,857,232,051

Table 7-6: Graph of Changes in the Deviance Value for Contractors (R)

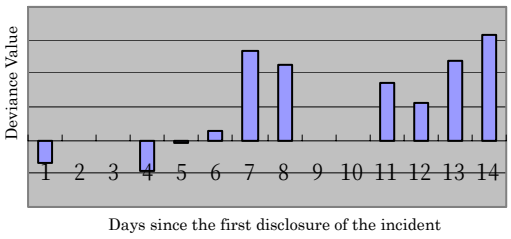
＃０４ (Company)



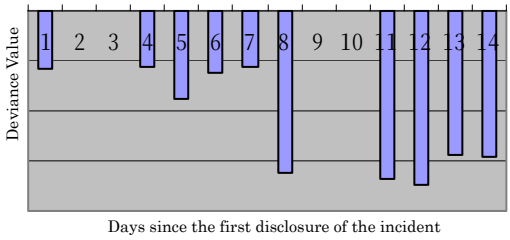
＃０４ (Contractor)



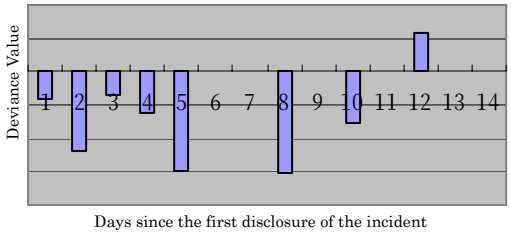
＃１５ (Company)



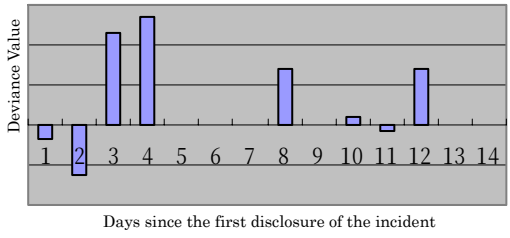
＃１５ (Contractor)



＃１８ (Company)



＃１８ (Contractor)



7.3 Envisaged Influence of Information Disclosure Incidents upon a Company's Share Prices

Let us look at the envisaged influence of information disclosure incidents upon a company's share prices, paying attention to "percentage of change in share prices over the previous day's prices (baseline prices)."

The 2002 investigation assumed that the percentage of change in share prices over the previous day's prices would be in the range of "0 - 9%."

Table 7-7 shows the percentage of change in share prices over the baseline prices (short term) in 2003. This envisages a variance of "around ±6%." Additionally, Table 7-8 shows that in 2002, 5 out of 8 incidents showed downward movement (62.5% of total), whereas in 2003, this figure was 12 out of 18 (66.7% of total), indicating that in more than 6 out of 10 cases, information disclosure incidents led to a drop in share prices.

Table 7-7: Percentage of Change in Share Prices over Baseline Prices (for 2003 / Short Term)

Case	#01	#02	#03	#04	#05	#06
Baseline price	3,434.00	2,406.00	376.40	109.80	2,932.00	6,660.00
Change in share prices (daily average)	▲206.05	▲10.32	▲0.57	▲4.48	▲105.70	254.32
Ratio of change in share prices over baseline prices	▲6.00	▲0.43	▲0.15	▲4.08	▲3.60	3.82

Case	#07	#08	#09	#10	#11	#12
Baseline price	310.00	50.60	433.60	931,400.00	542.75	88.60
Change in share prices (daily average)	▲1.23	2.05	▲9.13	8,174.73	0.05	5.81
Ratio of change in share prices over baseline prices	▲0.40	4.05	▲2.10	0.88	0.01	6.56

Case	#13	#14	#15	#16	#17	#18
Baseline price	225.40	773.00	2,033.75	40,300.00	401,400.00	1,340,000.00
Change in share prices (daily average)	▲3.25	▲1.92	59.90	▲675.57	▲14,710.37	▲25,657.34
Ratio of change in share prices over baseline prices	▲1.44	▲0.25	2.95	▲1.68	▲3.66	▲1.91

[Reference] Baseline price: average share price (closing price) for the company over a period of one week prior to disclosure of the incident.

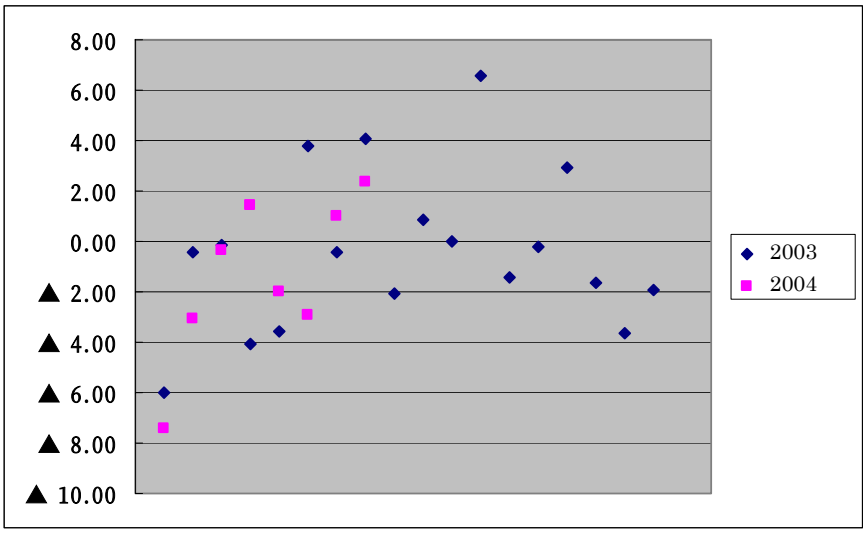
Change in share prices: Average deviance value compared to the expected share prices for 14 days from the date of the first report of the incident (Refer Table 7-1)

Table 7-8: 2002/2003 Percentage of Change in Share Prices compared to Baseline Prices (Short Term)

No.	2002	2003
1	▲7.44	▲6.00
2	▲3.10	▲0.43
3	▲0.33	▲0.15
4	1.41	▲4.08
5	▲1.98	▲3.60
6	▲2.93	3.82
7	1.02	▲0.40
8	2.35	4.05
9		▲2.10
10		0.88
11		0.01
12		6.56
13		▲1.44
14		▲0.25
15		2.95
16		▲1.68
17		▲3.66
18		▲1.91

Furthermore, if we plot the percentage of change in share prices as shown in Table 7-8, then we arrive at the scatter diagram as in Table 7-9. We can see that compared to 2002, there was an overall shift upwards in the distribution (a letup in the drop in share prices) for 2003. Additionally, we can not come to a conclusion based upon results from just 2002 and 2003 (26 incidents), however it seems that the percentage change in prices over baseline prices is concentrated in a zone (-2.00% ~ ±0.00%), and we would like to carry out further study for clarification.

Table 7-9: Scatter Graph of Percentage Changes in Share Prices over Baseline Prices (Short Term)



7.4 Overview of This Year

As with last year, this year we have focused upon both information disclosure incidents and share prices. In short, even for this year, we cannot come to the conclusion that we have made a correlation between information disclosure incidents and share prices.

Be that as it may, the scandal of information disclosure is a negative factor for companies, and no-one can deny that it can result in being a cause of reduced corporate value. In 2002, with its recurring incidents of disclosure of personal information, the focus was upon "there has been disclosure of personal information," whereas in 2003, the focus could be said to be upon how a company's response should be. Seen from this viewpoint, it is significant that we are carrying out an investigation into the effect on share prices. Share prices vary for a variety of reasons, and while it is difficult to abstract and measure the part of these changes that arise from information disclosure incidents, our aim is to understand these hints by using a sustained approach. At the same time, we also need to study alternative yardsticks by which companies can be evaluated.

7.5 Future Issues

This year, we have also adopted the Nikkei Stock Average as a reference value, using each day's closing price without modification. However, we did not think about the connection (or derivative value) between on one hand the share price for each company for each incident, and on the other, the Nikkei Stock Average. However, looking at Nikkei Stock Average prices for 2003, while the first half of the year showed a somewhat downward trend (carried over from the latter half of 2002), the second half of the year showed a rise. Accordingly, during this period, even though companies experienced momentary drops in share prices that can be ascribed to information disclosure incidents, we can not deny the possibility of immediate strong support buying.

Adoption of reference values, and correction methods for coming to grips with more subtle matters remain as issues.

8. Conclusion

Carried over from last year, we studied the publicized information disclosure incidents, and in addition to showing a new model for estimating compensatory damages, we studied the influence upon one part of a company's corporate value, namely their share prices.

This year's model for estimating the amount of compensatory damages resulting from disclosed information was mainly centered upon "privacy aspects" and "economic aspects," and we proposed a method for calculating sums.

By specifying both a numeric value for damages, and the calculation process, we have provided a point at which specialists from differing fields can meet, and we hope that this will be useful in promoting information systems risk assessment, and forming a safe, information-driven society.