Fiscal 2002

Information Security Incident

Survey Report

<Section Two>

Estimated Damages and other Observations
(Compensatory Damages, Influence on Share Prices)
with respect to Private Information Disclosure

JAPAN NETWORK SECURITY ASSOCIATION

March 31, 2003

Contents

JNSA Seisaku Committee　Security Incidents Investigation Working Group

Working Group Leader

Mr. Tadashi Yamamoto　SOMPO JAPAN RISK MANAGEMENT, INC.

Working Group Members　(No Particular Order, Titles Omitted)

Hisamichi Otani　NTT DATA CORPORATION

Hironori Omizo　JMC Co., Ltd

Kenji Okada　ELNIS Technologies Co., Ltd.

Masahiko Kusaka　SOMPO JAPAN RISK MANAGEMENT, INC.

Tomohisa Sashida　THE TOKIO MARINE RISK CONSULTING CO., LTD.

Tomoharu Sato　Internet Research Institute, Inc.

Kiyoshi Nagashima　THE TOKIO MARINE AND FIRE INSURANCE CO., LTD.

Takashi Nemoto　HUCOM, Incorporated

Yukihiro Matsutani　HUCOM, Incorporated

Shiro Maruyama　Little eArth Corporation

Naoyoshi Yasuda　dit CO., LTD.

Eiji Yamada　dit CO., LTD.

This report has been produced by the NPO, Japan Network Security Association (JNSA) Security Incidents Investigation Working Group. While the JNSA retains the copyrights to this work, this report is offered as public information. Any other works quoting this report, in whole or in part, must include an attribution to the JNSA copyright. Further, if you wish to quote a portion or all of this report in a book, magazine, or in seminar materials, etc., please first contact the JNSA at sec@jnsa.org.

© Copyright 2003 Japan Network Security Association (JNSA)

1. Introduction

At present, the Japan Network Security Association (JNSA) hosts nearly 20 active Working Groups. The report represents the results of the second annual Information Security Incident Survey project sponsored by the JNSA.

<About Section Two>

The Calculation Model proposed in <Section One> considers not only damages related to information security systems, but also refers to damages such as those related to compensatory legal reparations, etc.

This report also includes the results of investigations and observations related to the “possibility of compensatory legal reparations” payments with respect to negligent information disclosure, as well as actual cases of “influence on share prices”, one part of the corporate value equation.

The “Calculation of Compensation for Damages” and “Influence on Share Prices” suggested in this report represent a calculation method 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 develop approaches from a variety of directions, while at the same time helping company management focus on the presence and scale of information security risk, and make intelligent investment decisions.

—Reference—

<About Section One (Separate Document)>

The JNSA Seisaku Committee’s “Information Security Incidents Investigation Working Group” conducted a second annual survey of major corporations representing Japan’s core industries and Information Technology companies mainly from the JNSA corporate membership. The survey was taken via questionnaire and in-person interviews.

Section One of this report suggests a model describing the present circumstances of information security. This section features the consideration of a calculation model representing incident-caused damages and costs of countermeasures based on the results of this survey, from compiled data reflecting the current state of affairs at the companies surveyed, including costs of damages incurred and related investment.

This project adds to the research conducted previously, using “Calculation Model” developed last year; however, it is obvious that many issues and factors have yet to be properly addressed, and we believe that more surveys and observations will be required to develop an accurate assessment of the impact of information security incidents.

However, given the fact that corporations and organizations still do not appear to fully appreciate costs of information-related damages and countermeasures—even though the “scope and scale of damages and countermeasures” are important factors in enacting effective risk management—we believe there is great significance to our presenting an index of these costs using a “Model for Calculating Information Security Incident Damage and Countermeasure Costs” developed herein.

2. Objectives

Section Two addresses the issue of “Private Information Disclosure”, one particular type of information security accident that reverberates throughout society, and affects an ever-increasing number of individuals and entities. This “accidental exposure of private information” is a risk held in common by all corporations, and a risk naturally worthy of corporate management concern, if the momentum behind Japan’s Private Information Protection Act is any indication.

This Working Group has conducted research and made proposals, the objective of which is to serve as a catalyst for future discussions centered on the “possibilities of legal reparations”, and the “influence on share prices” related to “accidental exposure of private information.” At the same time, we hope to help corporate management be cognizant of, and become knowledgeable about, the level of information security risk, giving them information to make informed investment decisions.

The main topics addressed are as identified on the following pages.

<Section Two (Supplement): Estimated Damages and other Observations with respect to Private Information Disclosure >

(1) “Assumptions related to Costs of Compensatory Damages due to Private Information Disclosure”

We conducted a survey of private information disclosure incidents occurring during calendar year 2002, performing an analysis of the incidents reported. Based on the analytical results here, the Security Incidents Investigation Working Group calculated the damage costs based on several assumptions, including the value of personal information, and the amount of compensatory damages paid with respect to the information disclosure.

(2) “Influence of Private Information Disclosures on Corporate Value (Observations of Share Prices)”

In order to delve into the matter of decreased corporate value due to incidents of private information disclosure, the Workgroup conducted a survey of corporations that experienced such incidents during calendar year 2002, examining the effect of the incident on the share price movement of the company, and using these results as one factor in calculating the amount of influence on corporate value.

—Reference—

<Section One: Information Security Incident Survey and Damage Calculation Model >

(1) “Survey of Information Security Incident Damage Costs and related Investment”

(2) “Proposed Damage Cost Calculation Model”

(3) “Standard Model and Costs with respect to Information Security Incidents”

3. Estimated Damages and Other Observations with respect to Private Information Disclosure

With the modern expansion of network computing, including the rise of the Internet, we have seen a dramatic increase in awareness of protecting the private information of our citizens. The scope of accidental private information disclosure, as well as the newsworthiness of such incidents, has grown commensurate with the growth of the scale of our networked systems. This combination of factors has resulted in intense negative PR focused on corporations who commit or allow the exposure of private information.

Until recently, the accidental disclosure of personal private information was viewed more as a "scandal," but 2002 saw significant developments in this area, including Japanese courts ruling in favor of plaintiffs seeking compensation for damages incurred vis-à-vis private information exposure. Now, incident damages experienced by corporations have the potential to consist of specific monetary penalties.

The Working Group has made an attempt to calculate a specific amount for damages related to private information disclosures. The first factor considered for our calculation was that of "legal compensation for damages," bearing in mind the potential for class-action lawsuits. The next factor considered was that of the "influence on share prices," which comprises a part of overall corporate value.

In Japan, even if a company's share prices hit rock-bottom levels, as long as the company isn't forced directly into bankruptcy (e.g. recent food companies), most companies see their share prices rebound in time. As they say in Japan, "Gossip is short-lived," and people tend to have short memories as well.

However, as the drop-off in growth rates signaled the end of the economic boom in Japan, corporate management's responsibility not only to their customers, but also to shareholders, came under increasing scrutiny. As we hear more about management responsibility and corporate buyouts, we expect the significance and meaning of share prices to change. We should continue to be aware of these types of indirect effects.

4. Assumptions related to Costs of Compensatory Damages due to Private Information Disclosure

As can be seen by the enaction of the Private Information Protection Act and the Basic Residential Registers Network, 2002 was a turning point for concern about personal private information disclosure. In this section, we have detailed our investigation of incidents of private information disclosures (through unauthorized network access, etc.), providing an analysis of circumstances surrounding information security incidents. Based on the analytical results, the Security Incidents Investigation Working Group calculated damage costs making several assumptions about the value of personal information and amount of compensatory damages paid when information is accidentally disclosed.

4.1 Analysis of Private Information Disclosure in Japan

"Attachment A" on the next page shows a list of private information disclosure incidents occurring over computer network between January and December 2002.

According to the results of the Working Group's investigations, at least 63 incidents (incidents reported over the Internet) of private information disclosure due to unauthorized network access occurred between January and December 2002. A total number of 418,716 individuals were affected by these incidents (average of 6,646 individuals per incident).

Most of the incidents reported concerned the "leak" of private information (including those where only the individual's Email address was made known). There was only one[1] incident in which proprietary internal documents were disclosed via the computer network.

Personal Private Information Disclosure	57 incidents (90%)
Email Address Disclosure	5 incidents (8%)
Disclosure of Non-Public/ Proprietary Material	1 incident (2%)

As can be seen, most of the information disclosed dealt with an individual's personal data. We conducted an analysis of these incidents, noting observations as to the main reasons behind the personal information disclosures, and identifying characteristics about these 63 private information disclosure incidents.

[1] Of the reported incidents related to the disclosure of internal proprietary documents, the most alarming was information disclosure of the Japan Defense Agency network information. However, as this incident did not occur via a computer network, we have removed it from consideration.

Attachment A (Enlarged version attached at the end of this document)

別紙A 2002年情報漏洩事件一覧

企業・団体			被害					漏洩情報									
No.	区分	業種名	被害人数	被害者	漏洩内容	漏洩経路	原因（分類）	氏名	住所	メールアドレス	電話番号	生年月日	性別	職業	ID/パスワード	アンケート他	その他
A	企業	情報通信	1,900	応募者	メールアドレス	Email経由	誤操作			メールアドレス							
B	企業	サービス	10,000	応募者	個人情報	Web経由	設定ミス	氏名			連絡先						
C	企業	情報通信	1,388	顧客	個人情報	FTP経由	誤操作	（氏名）									（個人情報）
D	企業	情報通信	2,972	顧客	個人情報	Web経由	設定ミス	氏名	住所	メールアドレス	電話番号	年齢					星座
E	企業	情報通信	68,471	応募者	個人情報	Web経由	バグ・セキュリティホール	（氏名）							ID/パスワード	アンケート内容	（会員情報）
F	企業	情報通信	900	顧客	メールアドレス	Email経由	管理ミス			メールアドレス							
G	企業	サービス	22	応募者	個人情報	Web経由	設定ミス	氏名	住所	メールアドレス	電話番号						
H	企業	サービス	370	顧客	個人情報	Web経由	設定ミス	氏名		メールアドレス							
I	企業	情報通信	1,462	応募者	個人情報	Email経由	誤操作			メールアドレス							
J	企業	情報通信	不明	顧客	メールアドレス	Email経由	誤操作			メールアドレス							
K	企業	金融	4,300	顧客	個人情報	Web経由	バグ・セキュリティホール	（氏名）									
L	企業	製造業	730	応募者	個人情報	Web経由	設定ミス	（氏名）									（プレゼント応募者データ）
M	企業	サービス	4,000	応募者	個人情報	Web経由	設定ミス	氏名	住所		電話番号						
N	企業	サービス	4,000	顧客	個人情報	Web経由	設定ミス	氏名	住所		電話番号						
O	企業	製造業	10,000	応募者	個人情報	Web経由	設定ミス	氏名	住所								
P	企業	製造業	368	応募者	個人情報	Web経由	設定ミス	氏名	住所	メールアドレス	電話番号	誕生日	性別				
Q	企業	金融	60	顧客	個人情報	Web経由	設定ミス	氏名	住所	メールアドレス	電話番号	生年月日					
R	企業	サービス	1,303	応募者	個人情報	Web経由	設定ミス	氏名	住所	メールアドレス	電話番号					（アンケート内容）	
S	企業	製造業	不明	応募者	個人情報	Web経由	設定ミス	（氏名）							ID/パスワード		（個人情報）
T	企業	情報通信	800	応募者	個人情報	Web経由	設定ミス	（氏名）									（名簿）
U	企業	製造業	350	応募者	個人情報	Web経由	設定ミス	氏名	住所	メールアドレス	電話番号					アンケート内容	企業名、部署名、セミナー応募情報
V	企業	製造業	1,000	応募者	個人情報	Web経由	設定ミス	氏名		メールアドレス							
W	教育機関	教育機関	1,800	応募者	個人情報	Web経由	設定ミス	氏名	住所								
X	企業	サービス	37,000	顧客	個人情報	Web経由	設定ミス	氏名	住所	メールアドレス	電話番号	年齢					スリーサイズ
Y	企業	製造業	45,000	応募者	個人情報	Web経由	設定ミス	氏名	住所	メールアドレス		年齢		職業		（アンケート内容）	
Z	企業	サービス	1,500	応募者	個人情報	Web経由	設定ミス	氏名	住所	メールアドレス							
AA	企業	情報通信	340	顧客	個人情報	Web経由	設定ミス	（氏名）	（住所）								（新卒社員名簿）
AB	企業	サービス	4,700	応募者	個人情報	Web経由	設定ミス	（氏名）	（住所）							（アンケート内容）	
AC	その他	不明	14,000	応募者	個人情報	Web経由	設定ミス	氏名	住所	メールアドレス	電話番号					（アンケート内容）	
AD	企業	情報通信	242	応募者	個人情報	Web経由	設定ミス	氏名	住所								
AE	企業	サービス	2,000	顧客	個人情報	Web経由	設定ミス	氏名	住所		電話番号						
AF	企業	サービス	700	顧客	個人情報	Web経由	設定ミス	氏名	住所		電話番号						
AG	企業	情報通信	280	応募者	個人情報	Web経由	不正アクセス	氏名	住所	メールアドレス	電話番号						
AH	公共機関	行政機関	6,541	顧客	個人情報	Web経由	設定ミス	氏名	住所								（入館者名簿）
AI	企業	建築	不明	応募者	個人情報	Web経由	不明	氏名	住所		携帯番号						
AJ	企業	情報通信	1,100	応募者	個人情報	Web経由	不正アクセス	氏名	住所		電話番号			職業			
AK	企業	情報通信	5,000	顧客	個人情報	不明	不明	氏名	住所		電話番号						
AL	企業	サービス	1,600	顧客	個人情報	Web経由	設定ミス	（氏名）									（不明）
AM	企業	製造業	1,200	応募者	個人情報	Web経由	不正アクセス	氏名	住所	メールアドレス							
AN	企業	サービス	2,093	応募者	個人情報	Web経由	バグ・セキュリティホール	氏名		メールアドレス	電話番号					問合せ内容	
AO	企業	情報通信	不明	応募者	個人情報	Web経由	設定ミス	（氏名）									
AP	企業	サービス	100,000	顧客	個人情報	Web経由	バグ・セキュリティホール	名のみ	住所			生年月日					顔写真、身長、血液型、年収、学歴、趣味
AQ	企業	サービス	不明	顧客	個人情報	Web経由	設定ミス	（氏名）									
AR	企業	製造業	不明	その他	非公開資料	Web経由	情報持ち出し										社内文書
AS	企業	サービス	1,700	顧客	個人情報	Web経由	設定ミス	（氏名）									
AT	教育機関	教育機関	304	顧客	個人情報	Web経由	情報持ち出し	氏名									卒業生進路情報、成績
AU	企業	情報通信	17,000	顧客	個人情報	Web経由	情報持ち出し	氏名	住所	メールアドレス	電話番号	生年月日	性別	職種	ID		血液型、趣味、社内資料
AV	公共機関	行政機関	350	顧客	メールアドレス	Email経由	管理ミス			メールアドレス							
AW	企業	サービス	398	応募者	個人情報	Web経由	バグ・セキュリティホール	氏名	住所	メールアドレス	電話番号			職業			
AX	企業	製造業	3,244	応募者	個人情報	Web経由	バグ・セキュリティホール	氏名	住所	メールアドレス	電話番号	年齢	性別	職業			
AY	企業	情報通信	235	顧客	個人情報	Email経由	設定ミス	氏名	住所								グローバルIP
AZ	企業	製造業	1,200	応募者	個人情報	Web経由	バグ・セキュリティホール	氏名	住所		電話番号						
BA	企業	製造業	50,000	応募者	個人情報	Web経由	誤操作	氏名	住所	メールアドレス	電話番号	生年月日				アンケート内容	
BB	企業	サービス	400	応募者	個人情報	Web経由	不明	氏名								（アンケート内容）	学歴
BC	企業	建築	335	応募者	個人情報	Web経由	設定ミス	氏名	住所	メールアドレス	電話番号						
BD	公共機関	行政機関	59	顧客	メールアドレス	Email経由	誤操作			メールアドレス							
BE	その他	不明	不明	顧客	個人情報	Web経由	バグ・セキュリティホール	（氏名）									クレジットカード番号
BF	公共機関	行政機関	483	顧客	個人情報	Email経由	内部犯罪	氏名	住所		電話番号	年齢	性別				
BG	企業	サービス	65	顧客	個人情報	Web経由	バグ・セキュリティホール	氏名	住所	メールアドレス	連絡先						フリガナ、予約先電話番号、人数、金額
BH	公共機関	行政機関	154	顧客	個人情報	Web経由	誤操作	氏名	住所					職業			
BI	公共機関	行政機関	190	応募者	個人情報	Web経由	設定ミス	氏名	住所	メールアドレス	電話番号					意見	
BJ	教育機関	教育機関	3,107	顧客	個人情報	Web経由	設定ミス	氏名	住所	メールアドレス	電話番号		性別				出身高校
BK	企業	情報通信	不明	顧客	個人情報	Web経由	バグ・セキュリティホール								ID	質問内容	プリペイドカード番号など
合計	63		418,716				項目該当件数→	55	38	29	28	10	5	6	4	11	21
							項目該当割合→	87%	60%	46%	44%	16%	8%	10%	6%	17%	33%

4.2 Analysis of Disclosed Information

Table 4-1 shows an analysis of the type of information disclosed as a result of private information disclosure incidents.

The Ratio of Occurrence (%) indicates the frequency that each type of information was disclosed in connection with private information disclosure incidents.

Table 4-1: Number of Disclosure Incidents by Type of Information and Ratio of Occurrence

Type of Information Disclosed	Number of Incidents (Occurrence Ratio %)
Name	54 (86%)
Address	38 (60%)
Email Address	29 (46%)
Telephone Number	28 (44%)
Birth date	10 (16%)
Occupation	6 (10%)
Sex	5 (8%)
User ID	4 (6%)
Password	2 (3%)
Questionnaire Related	11 (17%)
Other	21 (33%)

An individual's "Name" was disclosed in 86% of incidents. Names represent the information most likely to be disclosed in a private information disclosure incident. Disclosures of "Name", "Address", "Email Address", and "Telephone Number" occur much more frequently than any other type of information.

We believe that these results stem from the fact that such information is widely gathered over web page questionnaires or online registrations, where individual information is often compiled before being processed.

In Table 4-1, "Other" includes the types of information that occur most infrequently; a breakdown of some of the details fitting this answer is shown below. The information described in "Other" contains information of a more sensitive personal nature than compared that identified in Table 4-1.

Table 4-2: Categorized Information included in "Other"

Phonetic spelling of name, body measurements, face photograph, height, blood type, astrological sign, hobbies, annual income, educational background, high school attended, career options/ next stage of education, school grades, company name, department name, seminar application information, internal documents, internal materials, global IP, credit card number, prepaid card number, etc.

4.3 Analysis of Organizations Responsible for Private Information Disclosure

About 80% of the organizations at fault for the disclosure of private information are corporations. This result could have easily been assumed, due to the fact that in comparison to public sector entities and educational institutions, corporations use the Internet more often for Email mailing lists, soliciting survey responses, and offering value-added services to customers.

We assume that the ratio of private information incidents attributable to public sector entities will increase as national and local governments offer more services over the Internet to their citizens, such as is called for in the e-Japan plan.

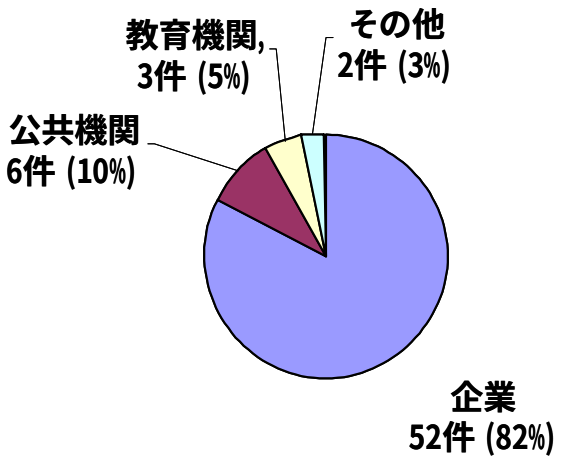


Figure 4-1: Breakdown of Organizations Responsible for Private Information Disclosures

Of the causes of private information disclosures shown in Figure 4-2, “Incorrect Settings,” “Operator Error,” and “Insufficient Management”—errors caused by human factors—account for 67% of the total. Although private information disclosure due to “Bug Security Holes” and “Unauthorized Access” is not directly related to human error, one must believe that corresponding incidents could have been prevented if those responsible had applied the latest patches to the system in a timely manner, or moved the Web system to a stronger structure.

In other words, private information disclosure occurring because of human shortcomings accounts for 88% of the total, when combining the two previously mentioned examples.

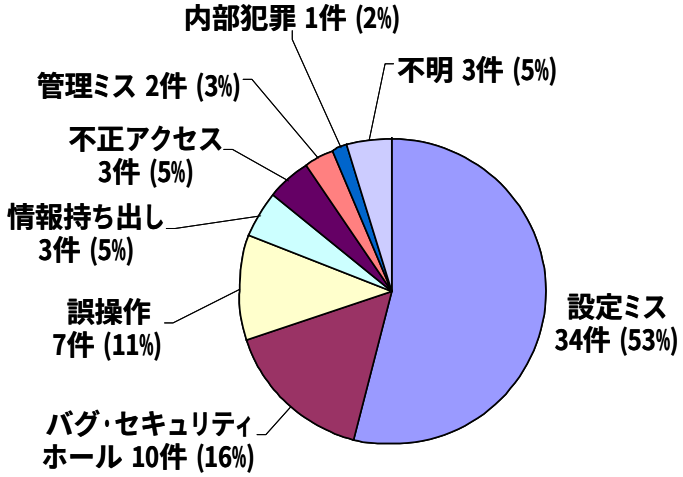


Figure 4-2: Causes of Private Information Disclosure

The vast majority of information disclosure incidents occur either over the Web or via Email, at 84% and 13%, respectively.

Email and Web browsing are the most popular ways to use the Internet.

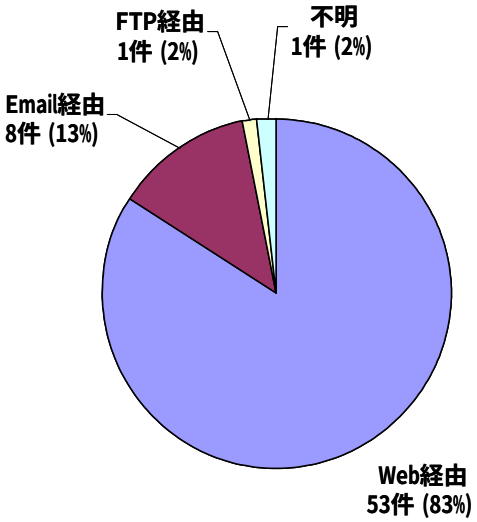


Figure 4-3: Route of Private Information Disclosure

Figure 4-4 shows the results of a detailed categorization of the various routes by which information is disclosed with respect to Figure 4-3 Private Information Disclosure routes, “Web,” “Email” and “FTP”.

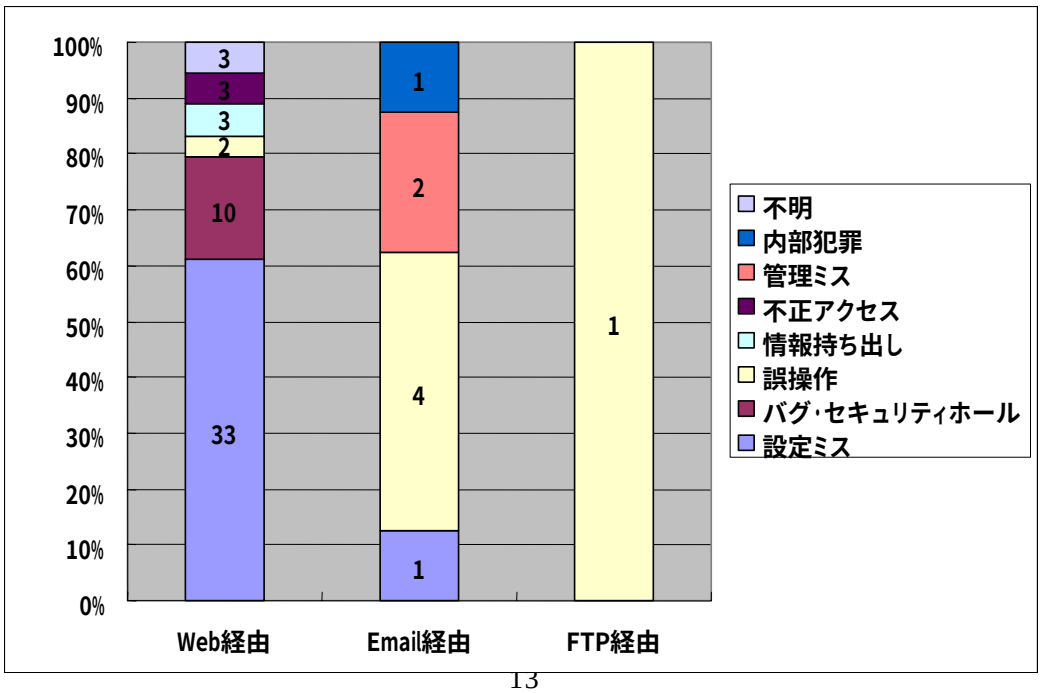


Figure 4-4: Disclosure Cause by Route for Private Information Incidents

Figure 4-4 indicates that the most common case leading to private information disclosure is "Incorrect Settings" and access via the Web.

From further information made available about the circumstances surrounding the occurrence of an incident, the cause of private information disclosure over the Web must have been the confluence of “Incorrect Settings”, “Bug Security Holes” and other factors, as seen below:

1 Incorrect settings for Web server. Directory listening set to allow.
2 Incorrect file permission settings
3 CGI and other program design errors
4 Use easy-to-guess file/ directory names.
(Many cases where main factors are causes 1, 2, and 3)

Web (HTTP) developed as means to provide two-way services such as CG/SSI, JavaScript/PHP, JPS/ASP, etc. Web systems are easy to construct, and offer convenient interactive services. On the other hand, the more complex the system, the easier it is to miss security holes. As a result, unauthorized access, incorrect settings, etc. should be easy to link private information disclosure.

4.4 Analysis of Private Information Disclosure Victims

Two categories of victims exist with respect to private information disclosure. The first category consists of individuals who give personal information to a company when responding to questionnaires, entering contests, etc. The second category consists of customers who provide personal information to companies in connection with product purchases, etc.
According to Figure 4-5, the ratio of incidents involving “applicant” victims and “customer” victims of information disclosure is roughly equal. The number of individual victims of information disclosure incidents is also fairly equally divided between the two categories.
However, the precise number of individuals victimized by information disclosure is difficult to calculate without log information records, such as access frequency, etc.
Under the current circumstances, we assume all information that could possibly be subject to disclosure is in fact disclosed. In other words, because we are assuming the maximum number of victims possible, the actual volume of information disclosed may be different.

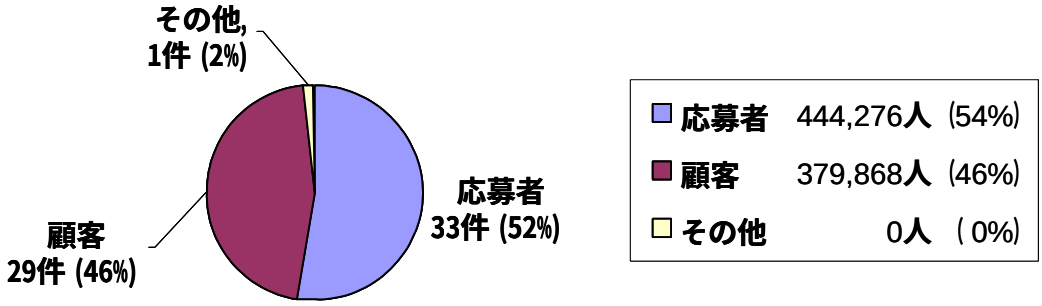


Figure 4-5: Classification of Private Information Disclosure Victims

4.5 Causes of Private Information Disclosure

Analyzing the results above, we have observed that the most common causes of private information disclosure have technical and non-technical aspects.

The following are typical technical aspects involved in the disclosure of personal information:

- A large volume of information is disclosed through DMZ terminals, which are positioned close to Internet connection points, and relatively easy to penetrate.
- Information maintained on DMZ terminals is generally information that is input over the Web by outside individuals/ referenced over the Web by outside individuals.
- Human carelessness, such as incorrect system settings, program design errors and operational error, is a frequent factor in information disclosure incidents.

The following are typical non-technical aspects involved in the disclosure of personal information:

- Victims are individuals and/or customers who respond to Web questionnaires, website contests, or who use Web services.
- Private Information Disclosure incidents are generally discovered by a third party, who notifies the company or posts their discovery to Internet bulletin boards.

Given the characteristics identified above, we can make the following assumptions:

- The disclosure of private information does not appear to be regarded with the proper degree of concern.
- The type of information stored does not include credit card numbers or other direct financial information. Therefore, the likelihood is that systems are not designed with the proper security considerations. Information from temporary events, such as questionnaire requests or prize offerings, is particularly susceptible, due to cost limitations and other factors.
- The probability exists that outsourced systems design and management are not subject to the proper degree of oversight, systems security audits, etc.

4.6 Types of Information and Compensatory Damages

4.6.1 Appellate Court Ruling on Large-Scale Disclosure of Uji City Basic Residential Register Data

We believe that compensatory damages for private information disclosure incidents can be calculated, based on standards assigned to values for different types of information disclosed. As we continue, we will refer to the information disclosed and the appellate court ruling for compensatory damages in connection with the large-scale disclosure of Uji City basic residential register data.
Reference Material： http://www.law.co.jp/cases/uji2.htm

- Disclosed Information = Basic Residential Register information
  Personal information including personal resident register number, address, name, sex, birth date, move-in date, move-out date, name of head of household, relationship to head of household, etc.
- Volume of Disclosure

Table 4-3: Uji City Private Information Disclosure Volume

Information	Volume of Disclosure
Residential Records	185,800 records
Registered Foreign Resident Information	3,297 records
Corporate Information	28,520 records
Total	217,617 records

- Compensatory Damages
  Victims (citizens) received ¥10,000 each in damages.
  Attorney fees of ¥5,000 per victim.
  Total compensatory damages of ¥15,000 per victim.

One interesting characteristic in connection with the large-scale disclosure of Uji City residential register data was the disclosure of highly private information, such as name of household head and relationship to household head, in addition to the disclosure of general personal information such as name, address, sex and birth date. Further, the personal information was disclosed from the Uji City (municipal government) basic residential register, a source of highly reliable and accurate information.
After consideration of the circumstances surrounding the incident, and the truthful manner in which the city dealt with recovering data, providing explanations to citizens, and enacting preventive measures, etc., the appeals court ordered payment of damages amounting to ¥15,000 per individual

affected.

Accordingly, assuming some 220,000 individuals were victimized by the private information disclosure in Uji City, total damages would calculate out to approximately ¥3.3 billion.

¥15,000 × 217,617 individuals = ¥3,264,255,000

Formula 4-1: Uji City Judgment for Compensatory Damages

4.6.2 Valuation Standards for Information

Here, we will propose a general standard for calculating compensatory damages, referring to the appellate court ruling in connection with the large-scale disclosure of Uji City basic residential register data.

(1) Damages paid for disclosed personal information:

- Damages paid for basic personal information

  Basic personal information includes information that is already publicly known to a certain degree: name, address, telephone number, birth date, sex and email address. The Uji ruling determined that having one's information disclosed did not cause a significant amount of mental pain and anguish. This finding is most likely the reason behind the relatively small level of damages assessed for privacy information. However, we expect the level of damages would increase if such information were used for direct mail and sales solicitations.

- Damages paid for uniquely identifying personal information

  If disclosed information included matters related to an individual's private life—a person's personal family relationships or physical characteristics, for example—such individual would most likely suffer considerable mental pain and anguish. In such cases, we would expect greater sums in payment for damages. If exposed personal information bridged an even wider range of data, we expect an even greater sum paid in damages.

  Examples)

  - Height, weight, body measurements, face photograph
  - Annual salary, educational history, name of employer, name of assigned company department
  - Hobbies, purchased products
  - Family makeup, marriage status

(2) Relationship between the degree of society's trust in and damages paid by an organization responsible for the disclosure of private information:

The higher the degree of society's trust in an organization, the greater the credibility of the information stored by the organization will be, and the higher the likelihood that such information will be used by a third party if subject to improper disclosure. If such information is improperly disclosed and then used for a wide range of purposes, it is not unreasonable to assume that the victim will endure a great deal of mental pain and anguish. Accordingly, our proposed general calculation standard will bear in mind the relationship between the level of trust placed by society in an organization, and the related compensatory damages paid by such an organization if it discloses an individual's private information.

4.6.3 Response of Victims and Organizations Responsible for Private Information Disclosures

(1) Response of organizations responsible for private information disclosures:

In the Uji City case, the response of the organization responsible for the information disclosure to the incident influenced the amount of damages paid. Immediately after the incident, the responsible organization took the following measures, showing their concern for the well being of the victims:

- Publicly announcing the incident
- Giving victims factual information, and formally apologizing
- Making best efforts to retrieve the disclosed information
- Making best efforts to prevent another occurrence

It is an inescapable fact that the incident has occurred, and the organization responsible for disclosing private information must pay some type of damages.

However, in certain cases, the organization in question may not be 100% responsible for the incident. For example, if the disclosure of private information is not due to the negligence of the organization (improper systems settings, etc.), but rather due to the intentional malicious act of an employee (e.g. system administrator), a portion or all of the liability may be attributable to said employee. Accordingly, there could be a reduction in compensatory damages required of the organization.

(2) Treatment of victim's private information:

At the same time, if the victim intentionally provided the other entity with personal information, he/she must be aware of the risks involved. As show in Figure 4-5, we have identified two categories in cases where an individual gives their personal information to an organization over the Internet, namely, (1) the customer providing information to vendors/organizations, and (2) the individual offering personal information by answering questionnaires or entering contests to win prizes.

In many situations where a customer gives personal information to a vendor or organization, the information is required for product registration, or to qualify for technical support or related services. In contrast, giving information as part of a questionnaire, or to enter a contest is done with quite a different mind set on part of the giver of information. Web pages where individuals respond to questionnaires or input information to enter contests generally include language to the effect that information provided shall not be used for other purposes or provided to any third parties. However, the user giving information to a vendor/ organization does so at their own responsibility,

assuming that such information may be used for other purposes. Accordingly, the organization responsible for the disclosure of private information has a higher liability for negligence in the case of customer information than in the case of individuals responding to questionnaires when an incident occurs.

4.6.4 Formula for Calculating Compensatory Damages for Private Information Disclosures

Our observations indicate that the amount of compensatory damages for incidents of personal information disclosures should be calculated based on all of the factors at hand, and reflective of the actual results of future court cases.

However, considering the frequency of accidental disclosures, we believe society would benefit from some type of index or hypothetical model for predicting the amount of compensatory damages. The Working Group has developed the following formula, based on a study of the aforementioned legal precedents and discussions with practicing attorneys. At the very least, the following model can be used as a starting point for future debate.

Formula 5-2 is not a direct calculation of compensatory damages to be paid by an organization responsible for disclosing private information. Rather, it calculates evaluation points for information (= attributes of each record) to determine compensatory damages.

Private Information Disclosure Compensatory Damages (evaluation points)
= Damages based on content of disclosed Information→See Table ①
× Existence of consent given by individual providing information→See Table ②
× Relationship with individual providing information →See Table ③
× Degree of societal trust in the offending organization →See Table ④
× Post-incident response by the offending organization →See Table ⑤

Formula 4-2: Computation Formula for Private Information Disclosure Compensatory Damages

The table below indicates point values used in Formula 4-2:

Factor	Assigned Point Values
①Damages paid to victim	Basic personal information = 100
	Uniquely identifying information (three types or less) = 500
	Uniquely identifying information (more than three types) = 1000
	Email address only = 10
	ID, passwords identifying individual = 300
②Existence of consent given by individual providing information	Consent = 2.0
	No consent = 1.0
③Relationship with individual providing information	Customer = 2.0
	Questionnaire, contest applicant = 1.0

④Degree of societal trust in the offending organization	Greater than normal = 1.5
	Normal = 1.0
⑤Post-incident response by the offending organization	Good = 1.0
	Fair = 2.0
	Poor = 4.0

Table 4-4 shows the correspondence between the evaluation points for an incident and hypothetical damages. Table 4-4 can be used to calculate hypothetical damages based on the evaluation points derived from Formula 4-2 and Formula 4-3.

Table 4-4: Correspondence between Evaluation Points and Hypothetical Damages

Evaluation Points Assigned to Incident	Hypothetical Damages (standard for calculation)
Less than 1000 Points	0 to ¥5,000 (¥5,000)
1000 to 1999 Points	Up to ¥10,000 (¥10,000)
2000 to 4999 Points	Up to ¥50,000 (¥50,000)
5000 Points and Above	Over ¥50,000 (¥100,000)

4.6.5 Application of Compensatory Damages Calculation to the Uji City Information Disclosure Incident

We compared the results of calculating compensatory damages based on information from the Uji City Basic Residential Register Data disclosure case using our model with the actual court ruling.

Uji City Compensatory Damages (evaluation points)

= Damages based on content of disclosed information [basic information + uniquely identifying information: 600]

×Existence of consent given by individual providing information [consent assumed: 2]

×Relationship with individual providing information [treated as customer: 2]

×Degree of societal trust in the offending organization [greater than normal: 1.5]

×Post-incident response by the offending organization [Good: 1]

= **3600 Points**

According to Table 4-4, this falls within the “2000 to 4999 Points” category, which calls for hypothetical damages of between ¥10,000 and ¥50,000 (standard calculation value of ¥50,000).

This result generally equates to the actual damage judgment, and leads us to conclude that this formula can be used to calculate a reference value for estimating compensatory damages.

4.7 Hypothetical Legal Compensation for Damages due to Accidental Private Information Disclosure in Japan

"Attachment B" shows the results of calculating compensatory damages, etc. based on "Attachment A (page 9)", and using the formula we have developed herein. The information obtained through the calculation results and process is shown below.

Total Compensatory Damages for all Incidents (hypothetical): ¥15.1427 billion (418,716 individuals)

Average Compensatory Damages per Incident: ¥240.36 million (average 6,646 individuals per incident)

Figure 4-6 shows the distribution of evaluation points for private information disclosure incidents occurring during 2002.

Many of the information disclosure incidents consisted of the disclosure of basic information or only an email address. As a result, the damages for approximately 70% of the incidents during 2002 were calculated to be ¥5,000 or less per incident (less than 1,000 evaluation points).

Of the incidents during 2002, ten (approximately 16%) were of an order exceeding the calculation for the Uji City judgment (3,600 points). All of these incidents included the disclosure of uniquely identifying personal information.

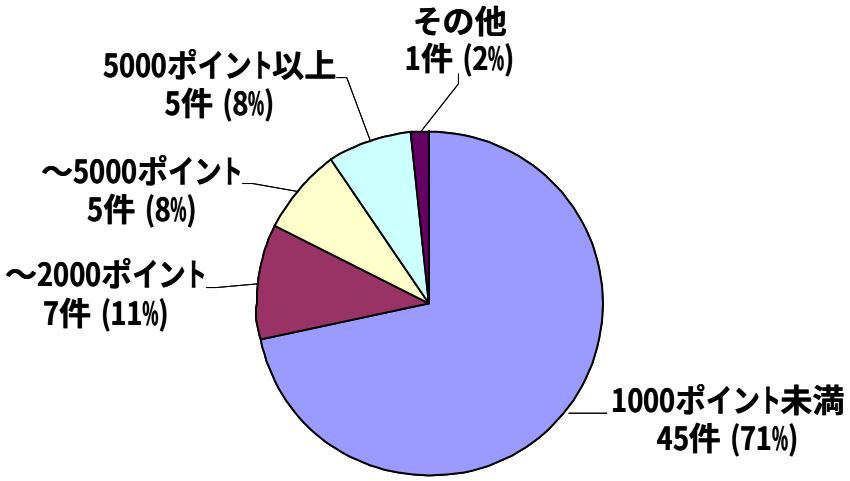


Figure 4-6: Distribution of Evaluation Points for Private Information Disclosure Incidents

According to the results above, the average compensatory damage (hypothetical) per private information disclosure incident is equivalent to ¥240.36 million. Of course, not all victims of private information disclosure will likely initiate lawsuits, but considering potential legal damages and the tarnished brand image caused by the disclosure of personal information, company management would be wise to invest in security measures preventing the occurrence of such incidents in the first place. Organizations that collect and store personal information can use the formula developed here to estimate the risks involved in private information disclosure, relying not upon averages of compensatory

damage judgments, but based on the actual information and number of records the organization collects and maintains. When soliciting questionnaires or providing customer services, organizations can use the type of information and number of individuals to calculate potential compensatory damages in terms of information disclosure risk, referring to these figures when determining the amount of security-related investment.

別紙B

企業・団体		漏洩情報				同意	2者関係	社会的信頼度	対応姿勢	評価ポイント	想定慰謝料	被害人数（人）	想定損害賠償総額（万円）
No.	区分	基本情報	特徴情報	メールアドレス	パスワード	（仮）							
A	企業			○		有り	応募者	○	○	200	5,000	1,900	950
B	企業	○				有り	応募者	○	◎	200	5,000	10,000	5,000
C	企業	○				有り	顧客	◎	◎	600	5,000	1,388	694
D	企業	○				有り	顧客	○	◎	400	5,000	2,972	1,486
E	企業	○			○	有り	応募者	○	◎	800	5,000	68,471	34,236
F	企業	○				有り	顧客	◎	○	1,200	10,000	900	900
G	企業	○				有り	応募者	○	○	400	5,000	22	11
H	企業	○				有り	顧客	○	○	800	5,000	370	185
I	企業			○		有り	応募者	○	◎	100	5,000	1,462	731
J	企業			○		有り	顧客	○	◎	200	5,000	不明	不明
K	企業	○				有り	顧客	◎	○	1,200	10,000	4,300	4,300
L	企業	○				有り	応募者	◎	○	600	5,000	730	365
M	企業	○				有り	応募者	○	◎	200	5,000	4,000	2,000
N	企業	○				有り	顧客	○	○	800	5,000	4,000	2,000
O	企業	○				有り	応募者	○	○	400	5,000	10,000	5,000
P	企業	○				有り	応募者	○	○	400	5,000	368	184
Q	企業	○				有り	顧客	○	○	800	5,000	60	30
R	企業	○				有り	応募者	○	○	400	5,000	1,303	652
S	企業	○			○	有り	応募者	○	○	1,600	10,000	不明	不明
T	企業	○				有り	応募者	◎	○	600	5,000	800	400
U	企業	○				有り	応募者	○	○	400	5,000	350	175
V	企業	○				有り	応募者	○	○	400	5,000	1,000	500
W	教育機関	○				有り	応募者	○	○	400	5,000	1,800	900
X	企業	○	◎			有り	顧客	○	◎	4,400	50,000	37,000	185,000
Y	企業	○				有り	応募者	○	○	400	5,000	45,000	22,500
Z	企業	○				有り	応募者	○	◎	200	5,000	1,500	750
AA	企業	○				有り	顧客	○	○	800	5,000	340	170
AB	企業	○				有り	応募者	○	○	400	5,000	4,700	2,350
AC	その他	○				有り	応募者	○	○	400	5,000	14,000	7,000
AD	企業	○				有り	応募者	○	○	400	5,000	242	121
AE	企業	○				有り	顧客	○	○	800	5,000	2,000	1,000
AF	企業	○				有り	顧客	○	○	800	5,000	700	350
AG	企業	○				有り	応募者	○	○	400	5,000	280	140
AH	公共機関	○				有り	顧客	◎	○	1,200	10,000	6,541	6,541
AI	企業	○				有り	応募者	○	○	400	5,000	不明	不明
AJ	企業	○				有り	応募者	○	○	400	5,000	1,100	550
AK	企業	○				有り	顧客	○	○	800	5,000	5,000	2,500
AL	企業	○				有り	顧客	○	△	1,600	10,000	1,600	1,600
AM	企業	○				有り	応募者	○	○	400	5,000	1,200	600
AN	企業	○				有り	応募者	○	○	400	5,000	2,093	1,047
AO	企業	○				有り	応募者	○	○	400	5,000	不明	不明
AP	企業	○	◎			有り	顧客	○	○	8,800	100,000	100,000	1,000,000
AQ	企業	○				有り	顧客	○	△	1,600	10,000	不明	不明
AR	企業					有り	その他	○	○	算出不能	5,000	不明	不明
AS	企業	○				有り	顧客	○	○	800	5,000	1,700	850
AT	教育機関	○	○			有り	顧客	○	○	4,800	50,000	304	1,520
AU	企業	○	○		○	有り	顧客	○	○	7,200	100,000	17,000	170,000
AV	公共機関			○		有り	顧客	◎	○	600	5,000	350	175
AW	企業	○				有り	応募者	○	○	400	5,000	398	199
AX	企業	○				有り	応募者	○	○	400	5,000	3,244	1,622
AY	企業	○			○	有り	顧客	○	△	6,400	100,000	235	2,350
AZ	企業	○				有り	応募者	○	◎	200	5,000	1,200	600
BA	企業	○				有り	応募者	○	○	400	5,000	50,000	25,000
BB	企業	○	○			有り	応募者	○	○	2,400	50,000	400	2,000
BC	企業	○				有り	応募者	○	○	400	5,000	335	168
BD	公共機関			○		有り	顧客	◎	○	600	5,000	59	30
BE	その他	○	○		○	有り	顧客	○	○	7,200	100,000	不明	不明
BF	公共機関	○				有り	顧客	◎	○	1,200	10,000	483	483
BG	企業	○	○			有り	顧客	◎	○	7,200	100,000	65	650
BH	公共機関	○				有り	顧客	◎	◎	600	5,000	154	77
BI	公共機関	○				有り	応募者	◎	○	600	5,000	190	95
BJ	教育機関	○	○			有り	顧客	○	○	4,800	50,000	3,107	15,535
BK	企業				○	有り	顧客	○	△	4,800	50,000	不明	不明
合計63											合計	418,716	1,514,270
											平均	6,646	24,036

5. The Influence of Accidental Private Information Disclosures on Corporate Value (Share Price Observations)

Every day, corporations engage in advertising and investor relations activities to build trust with society and create corporate value. In contrast, accidental disclosure of private information is one type of event that invites both loss of societal trust and decrease in corporate value.

However, while there are many indices of corporate value, it is extremely difficult to understand how much corporate value has fallen in response to private information disclosures and other scandals.

To get some sense of the decrease in corporate value caused by private information disclosures, we have conducted a study of the relation between the public information disclosure incident and the subsequent movement of corporate share prices.

Of course, it goes without saying that actual stock price fluctuations are caused by a variety of factors, making it difficult to link an accidental disclosure of private information as the only proximate cause of share movement.

Still, there is no doubt that corporations experience a loss of societal trust after they have been involved in a disclosure of private information. At present, the sample population is quite small, but by employing a defined methodology and conducting repeated studies to build a more robust data set, we should be able to observe correlative trends between incidents and their effects on corporate share prices in the future.

Here, we will propose a method to calculate the effect of an incident on share prices. By continuing to use the same methodology in the future, we will build a foundation of basic data with which to identify correlative trends. Share prices comprise a major index of interest to corporate management. Our objective is to research the movement of share prices after the occurrence of an incident to understand the effects of an accidental disclosure of private information.

5.1 Methodology Used to Understand Post-Incident Share Price Fluctuations

Earlier, we conducted a study of compensatory damages caused by accidental private information disclosures. In this section, we report the results of our investigations of short- and medium-term share price movement for publicly traded companies (or closely related publicly traded companies) subsequent to the occurrence of an information disclosure incident.

Share price movement can be affected by the stock market at large. Rather than conduct a simple price comparison, we will use the Nikkei average to represent the overall market, investigating changes in the ratio between the share price of the company in question and the value of the Nikkei average at the end of the day after an incident, compared with the ratio between the share price of

the company in question and the value of the Nikkei average for the day prior (end of month prior) to the incident (standard ratio).

<Short-Term>
Standard Ratio = (company share price / Nikkei average) for the day prior to the incident
Day n ratio = (company share price / Nikkei average) for day n after the incident

<Medium-Term>
Standard Ratio = (company share price / Nikkei average) for month end prior to incident
Ratio at the end of n months = (company share price / Nikkei average) at the end of n months after the incident

“Corporate Value” for the company in question is calculated by multiplying the difference between the “standard ratio” and each “day n ratio” by the “Nikkei average at day n” and the number of shares outstanding.

<Short-Term>

day n value = (standard ratio – day n ratio) x Nikkei average at day n x number of shares outstanding

<Medium-Term>

value at n months = (standard ratio – ratio at the end of n months) x Nikkei average at the end of n months x number of shares outstanding

We have defined the amount of effect for the short- and medium-term as follows:

<Short-Term>

Considered to be a period of 10 days. We divide the total values for days 1 through 10 after the incident by 10, considering the resulting value to be the decrease in corporate value for the 10 days subsequent to an incident. This is the short–term “influence on share prices” caused by an incident of accidental private information disclosure.

Short-Term Influence on Share Prices = Total of n Value for Days 1 through 10 / 10

<Medium-Term>

Considered to be a period of 4 months. We divide the total values for months 1 through 4 after the incident by 4, considering the result to be the decrease in corporate value for the 4 months subsequent to an incident. This is the medium-term “influence on share prices” caused by an incident of accidental private information disclosure. (We settled on a 4-month period as the time frame for “short-lived gossip” as per the Japanese proverb.)

Medium-Term Influence on Share Prices = Total of n Value for Months 1 through 4 / 4

5.2 Study of Actual Share Price Fluctuations

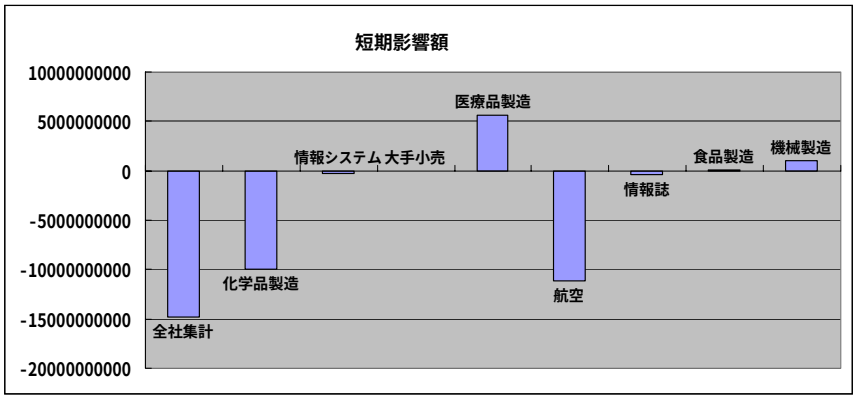
5.2.1 Short-Term Effects

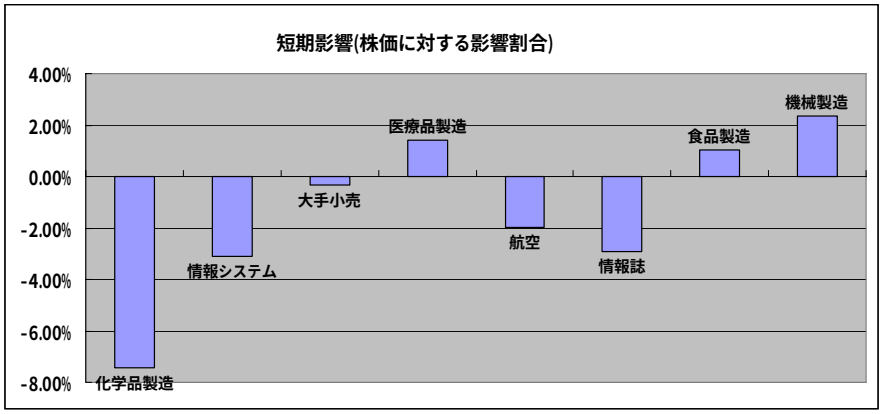
We created the following table based on the methodology introduced in 5.1, above.

The results indicate that while there were lesser and greater effects for the companies studied, the aggregate total for all companies was a significant loss. The aggregate single day loss for only eight of the companies observed amounted to ¥15 billion. In addition, we observed one single firm that experienced a negative effect of more than ¥10 billion. (Please refer to the enlarged table at the end of this document.)

Aggregate Short-Term Effect for 8 Companies = ¥15 billion

短期影響	全社集計	化学品製造	情報システム	大手小売	医療品製造	航空	情報誌	食品製造	機械製造
漏洩情報	-	個人情報漏洩	個人情報漏洩	個人情報漏洩	個人情報漏洩	個人情報漏洩	個人情報漏洩	個人情報漏洩	社内文書
発行株数	2,377,382,066	483,478,398	6,079,200	7,707,095	210,876,260	1,536,082,686	57,606,628	19,018,565	56,533,234
	事故前日との総時価額差	事故前日との総時価額差	事故前日との総時価額差	事故前日との総時価額差	事故前日との総時価額差	事故前日との総時価額差	事故前日との総時価額差	事故前日との総時価額差	事故前日との総時価額差
当日	−7,557,534,691	−3,570,789,360	−246,013,087	95,336,914	2,534,893,473	−5,303,310,519	−427,285,937	−225,429,799.7	−414,936,354.0
2日目	−15,090,054,733	−9,319,997,183	46,180,655	28,732,213	659,666,292	−4,467,471,450	−494,261,533	−420,015,359.6	−1,122,888,367.4
3日目	−22,281,835,550	−10,136,723,378	−68,408,193	58,530,572	88,668,452	−11,849,732,921	−541,013,847	−161,385,332.7	328,229,096.7
4日目	−6,523,862,893	−7,505,764,795	−126,945,939	−22,211,379	6,748,164,930	−6,046,465,328	−716,661,312	72,280,333.8	1,073,740,595.7
5日目	−8,553,216,391	−11,064,522,685	−11,002,820	−50,479,089	9,149,692,309	−8,174,986,014	−221,154,257	313,509,435.1	1,505,726,730.3
6日目	−8,794,742,121	−10,319,830,983	−16,641,328	−81,758,659	10,524,653,709	−11,755,846,673	−107,083,394	−76,225,381.2	3,037,990,588.6
7日目	−23,303,036,794	−10,731,911,935	−165,149,585	−103,446,264	9,212,738,910	−24,464,027,342	−199,652,563	743,883,773.8	2,404,528,211.1
8日目	−24,081,184,100	−12,321,170,730	−385,083,359	−125,037,603	5,180,669,468	−18,038,923,259	−117,826,407	566,334,255.4	1,159,853,533.4
9日目	−16,890,393,334	−15,510,004,135	−639,179,791	−131,661,895	9,364,655,312	−11,748,789,182	−331,241,032	321,888,099.7	1,783,939,288.7
10日目	−15,093,907,406	−8,847,818,215	−576,247,359	112,956,849	3,020,045,595	−9,336,303,585	−317,069,761	99,269,327.2	751,259,743.2
10日間累積	−148,169,768,014	−99,328,533,420	−2,188,490,807	−219,038,339	56,483,848,450	−111,185,856,272	−3,473,250,044	1,234,109,351.8	10,507,443,066.2
1日当り	−14,816,976,801	−9,932,853,342	−218,849,081	−21,903,834	5,648,384,845	−11,118,585,627	−347,325,004	123,410,935	1,050,744,307
一株当り差額	−6.23	−20.54	−36.00	−2.84	26.79	−7.24	−6.03	6.49	18.59
前日株価に対する差額割合	-	−7.44%	−3.10%	−0.33%	1.41%	−1.98%	−2.93%	1.02%	2.35%





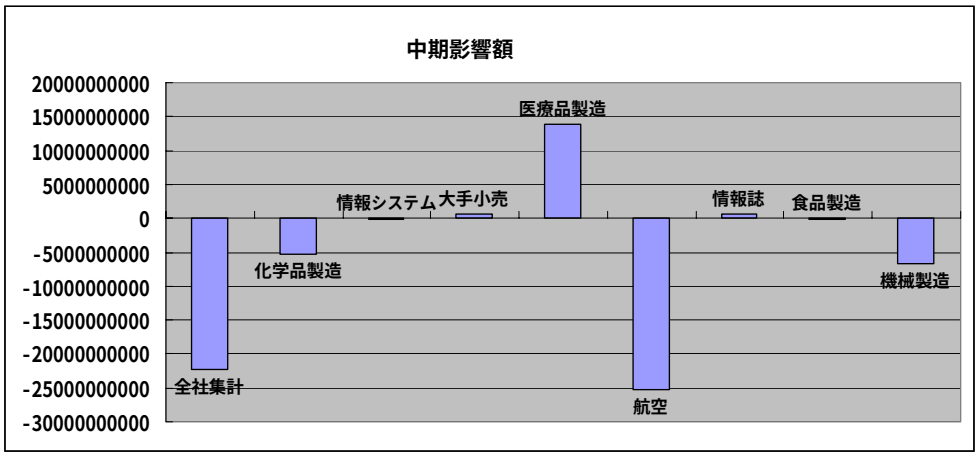
5.2.2 Medium-Term Effects

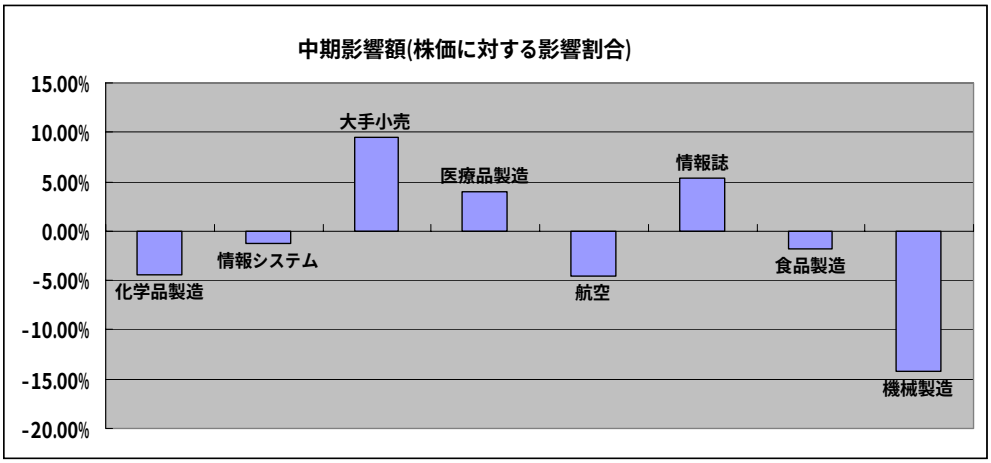
We created the following table using the method introduced in 5.2.1 as applied to short-term effects.

Here, we see a greater effect than with the short-term calculations. Obviously, each company was affected to a greater or lesser degree; however, the total for all companies was an even greater loss than the short-term totals. The aggregate loss after one month for only eight of the companies observed was approximately ¥22 billion. And through certainly a possible outlying case, we observed one single firm whose share price was affected by more than ¥25 billion. (Please refer to the enlarged table at the end of this document.)

Aggregate Medium-Term Effect for 8 Companies = ¥22 billion

中期影響	全社集計	化学品製造	情報システム	大手小売	医療品製造	航空	情報誌	食品製造	機械製造
漏洩情報	–	個人情報漏洩	個人情報漏洩	個人情報漏洩	個人情報漏洩	個人情報漏洩	個人情報漏洩	個人情報漏洩	社内文書
発行株数	2,377,382,066	483,478,398	6,079,200	7,707,095	210,876,260	1,536,082,686	57,606,628	19,018,565	56,533,234
	事故前日との総時価額差	事故前日との総時価額差	事故前日との総時価額差	事故前日との総時価額差	事故前日との総時価額差	事故前日との総時価額差	事故前日との総時価額差	事故前日との総時価額差	事故前日との総時価額差
当月末	2,904,335,092	−2,391,186,437	385,046,116	228,968,428	35,552,585,519	−30,089,363,254	992,471,666	361,720,517	−2,135,907,464
2ヶ月末	−33,500,748,617	−7,207,661,195	34,112,062	733,372,351	17,875,262,835	−40,587,241,253	383,916,817	−46,604,046	−4,685,906,188
3ヶ月末	−24,820,987,148	−7,056,963,701	53,223,297	1,000,553,392	568,067,968	−5,931,163,173	148,204,325	−163,011,541	−13,439,897,715
4ヶ月末	−33,659,566,285	−4,798,506,294	−825,642,464	540,858,539	1,623,993,216	−24,069,485,182	1,025,077,127	−1,072,899,642	−6,082,961,587
4ヶ月間累積	−89,076,966,959	−21,454,317,627	−353,260,990	2,503,752,711	55,619,909,539	−100,677,252,861	2,549,669,936	−920,794,712	−26,344,672,954
1ヶ月当り	−22,269,241,740	−5,363,579,407	−88,315,247	625,938,178	13,904,977,385	−25,169,313,215	637,417,484	−230,198,678	−6,586,168,238
一株当り差額	−9.4	−11.1	−14.5	81.2	65.9	−16.4	11.1	−12.1	−116.5
前月株価に対する差額割合	–	−4.40%	−1.29%	9.44%	3.97%	−4.50%	5.40%	−1.86%	−14.26%


中期影響額
20000000000
15000000000
10000000000
5000000000
0
-5000000000
-10000000000
-15000000000
-20000000000
-25000000000
-30000000000
全社集計
化学品製造
情報システム
大手小売
医療品製造
航空
情報誌
食品製造
機械製造


中期影響額(株価に対する影響割合)
15.00%
10.00%
5.00%
0.00%
-5.00%
-10.00%
-15.00%
-20.00%
化学品製造
情報システム
大手小売
医療品製造
航空
情報誌
食品製造
機械製造

5.3 Hypothetical Effect on Share Prices for Companies after Accidental Private Information Disclosure, and its Utilization

While the overall market was down for the year under study, the values calculated to represent the effect on stock prices have been corrected as a ratio of the Nikkei average, showing a not-insignificant effect on corporate value after an accidental private information disclosure incident.

Company management can use the values shown in 5.2 as one tool to perform risk management considering the effect on their firm's share prices after an assumed accidental private information disclosure.

More specifically, we used these figures to create the formulas below, which can be referenced for calculating the effects of an incident:

① When using 0% to 9% as the "share price difference (%) compared to prior close" for each company:

Effect = Share Price x (0% to 9%) x Number of shares outstanding

② When using ¥6 to ¥9 as the "per-share price difference" for all companies in the aggregate:

Effect = ¥6 to ¥9 x Number of shares outstanding

We believe it is important for company management to assess preventive risk management, using these numbers and formulas to formulate a hypothesis about the potential effect of an accidental private information disclosure on share prices.

Considering the large size of the effects seen here, management would be well advised to proactively view "information security costs" as part of IR expenses for preventing loss of corporate value, rather than as purely information systems costs.

5.4 Standard Calculation Value Topics

For our model, we used the Nikkei average for our standard calculation value. However, each industry has its own unique trends for share price movement, with the Nikkei average and industry averages moving in different directions or amplitudes on a frequent basis.

From a manager's point of view, comparing your firm with others in the same industry is important. Management should consider using "industry averages" as calculation value standards in order to gain a more precise understanding of the effects of incidents on the share prices of their company.

6. Conclusion

During the course of preparing this report, the Working Group has investigated reported incidents of accidental private information disclosure, and has proposed values for calculating hypothetical compensatory damages and the effect of incidents on share prices as one part of overall corporate value, aiming to provide the subject as a starting point for future debate. The results herein must be taken as a trial result for the present, since they come from an extremely limited data set, and include many legal and other factors outside our realm of expertise.

However, having shown these damage-related figures and the process by which they were derived, we believe we have been able to clarify issues to be address by experts in the future. We hope that these issues become a common point of discussion for experts from a variety of fields, promoting a more sophisticated model for “understanding risk levels”—a prerequisite for information systems risk assessment and playing a helpful role in the development of a safe information society.

We referenced the following URLs during the writing of this report.
(Alphabetical Order)

BizTech	http://biztech.nikkeibp.co.jp/
Ikari24	http://ikari.ikari24.com/
Mainichi Daily News	http://www.mainichi.co.jp/
Melma	http://www.melma.com/
Net Security	https://www.netsecurity.ne.jp/
Next EC	http://www.next-ec.com/
RescueNow.Net	http://www.rescuenow.net/
ZAKZAK	http://www.zakzak.co.jp/
ZDNet JAPAN	http://www.zdnet.co.jp/

We thank Mr. Jiro Makino, attorney at law, for meeting with us to discuss issues related to compensatory damages. Mr. Makino’s law firm can be found on the Web at:

Makino Law Office http://www.asahi-net.or.jp/~V5J-MKN/

別紙A 2002年情報漏洩事件一覧

企業・団体			被害					漏洩情報									
No.	区分	業種名	被害人数	被害者	漏洩内容	漏洩経路	原因（分類）	氏名	住所	メールアドレス	電話番号	生年月日	性別	職業	ID/パスワード	アンケート他	その他
A	企業	情報通信	1,900	応募者	メールアドレス	Email経由	誤操作			メールアドレス							
B	企業	サービス	10,000	応募者	個人情報	Web経由	設定ミス	氏名			連絡先						
C	企業	情報通信	1,388	顧客	個人情報	FTP経由	誤操作	(氏名)									(個人情報)
D	企業	情報通信	2,972	顧客	個人情報	Web経由	設定ミス	氏名	住所	メールアドレス	電話番号	年齢					星座
E	企業	情報通信	68,471	応募者	個人情報	Web経由	バグ・セキュリティホール	(氏名)							ID/パスワード	アンケート内容	(会員情報)
F	企業	情報通信	900	顧客	メールアドレス	Email経由	管理ミス			メールアドレス							
G	企業	サービス	22	応募者	個人情報	Web経由	設定ミス	氏名	住所	メールアドレス	電話番号						
H	企業	サービス	370	顧客	個人情報	Web経由	設定ミス	氏名		メールアドレス							
I	企業	情報通信	1,462	応募者	個人情報	Email経由	誤操作			メールアドレス							
J	企業	情報通信	不明	顧客	メールアドレス	Email経由	誤操作			メールアドレス							
K	企業	金融	4,300	顧客	個人情報	Web経由	バグ・セキュリティホール	(氏名)									
L	企業	製造業	730	応募者	個人情報	Web経由	設定ミス	(氏名)									(プレゼント応募者データ)
M	企業	サービス	4,000	応募者	個人情報	Web経由	設定ミス	氏名	住所		電話番号						
N	企業	サービス	4,000	顧客	個人情報	Web経由	設定ミス	氏名	住所		電話番号						
O	企業	製造業	10,000	応募者	個人情報	Web経由	設定ミス	氏名	住所								
P	企業	製造業	368	応募者	個人情報	Web経由	設定ミス	氏名	住所	メールアドレス	電話番号	誕生日	性別				
Q	企業	金融	60	顧客	個人情報	Web経由	設定ミス	氏名	住所	メールアドレス	電話番号	生年月日					
R	企業	サービス	1,303	応募者	個人情報	Web経由	設定ミス	氏名	住所	メールアドレス	電話番号					(アンケート内容)	
S	企業	製造業	不明	応募者	個人情報	Web経由	設定ミス	(氏名)							ID/パスワード		(個人情報)
T	企業	情報通信	800	応募者	個人情報	Web経由	設定ミス	(氏名)									(名簿)
U	企業	製造業	350	応募者	個人情報	Web経由	設定ミス	氏名	住所	メールアドレス	電話番号					アンケート内容	企業名、部署名、セミナー応募情報
V	企業	製造業	1,000	応募者	個人情報	Web経由	設定ミス	氏名		メールアドレス							
W	教育機関	教育機関	1,800	応募者	個人情報	Web経由	設定ミス	氏名	住所								
X	企業	サービス	37,000	顧客	個人情報	Web経由	設定ミス	氏名	住所	メールアドレス	電話番号	年齢					スリーサイズ
Y	企業	製造業	45,000	応募者	個人情報	Web経由	設定ミス	氏名	住所	メールアドレス		年齢		職業		(アンケート内容)	
Z	企業	サービス	1,500	応募者	個人情報	Web経由	設定ミス	氏名	住所	メールアドレス							
AA	企業	情報通信	340	顧客	個人情報	Web経由	設定ミス	(氏名)	(住所)								(新卒社員名簿)
AB	企業	サービス	4,700	応募者	個人情報	Web経由	設定ミス	(氏名)	(住所)							(アンケート内容)	
AC	その他	不明	14,000	応募者	個人情報	Web経由	設定ミス	氏名	住所	メールアドレス	電話番号					(アンケート内容)	
AD	企業	情報通信	242	応募者	個人情報	Web経由	設定ミス	氏名	住所								
AE	企業	サービス	2,000	顧客	個人情報	Web経由	設定ミス	氏名	住所		電話番号						
AF	企業	サービス	700	顧客	個人情報	Web経由	設定ミス	氏名	住所		電話番号						
AG	企業	情報通信	280	応募者	個人情報	Web経由	不正アクセス	氏名	住所	メールアドレス	電話番号						
AH	公共機関	行政機関	6,541	顧客	個人情報	Web経由	設定ミス	氏名	住所								(入館者名簿)
AI	企業	建築	不明	応募者	個人情報	Web経由	不明	氏名	住所		携帯番号						
AJ	企業	情報通信	1,100	応募者	個人情報	Web経由	不正アクセス	氏名	住所		電話番号			職業			
AK	企業	情報通信	5,000	顧客	個人情報	不明	不明	氏名	住所		電話番号						

別紙A 2002年情報漏洩事件一覧

企業・団体			被害					漏洩情報										
No.	区分	業種名	被害人数	被害者	漏洩内容	漏洩経路	原因（分類）	氏名	住所	メールアドレス	電話番号	生年月日	性別	職業	ID/パスワード	アンケート他	その他
AL	企業	サービス	1,600	顧客	個人情報	Web経由	設定ミス	（氏名）									（不明）
AM	企業	製造業	1,200	応募者	個人情報	Web経由	不正アクセス	氏名	住所	メールアドレス							
AN	企業	サービス	2,093	応募者	個人情報	Web経由	バグ・セキュリティホール	氏名		メールアドレス	電話番号					問合せ内容	
AO	企業	情報通信	不明	応募者	個人情報	Web経由	設定ミス	（氏名）									
AP	企業	サービス	100,000	顧客	個人情報	Web経由	バグ・セキュリティホール	名のみ	住所			生年月日					顔写真、身長、血液型、年収、学歴、趣味
AQ	企業	サービス	不明	顧客	個人情報	Web経由	設定ミス	（氏名）									
AR	企業	製造業	不明	その他	非公開資料	Web経由	情報持ち出し										社内文書
AS	企業	サービス	1,700	顧客	個人情報	Web経由	設定ミス	（氏名）									
AT	教育機関	教育機関	304	顧客	個人情報	Web経由	情報持ち出し	氏名									卒業生進路情報、成績
AU	企業	情報通信	17,000	顧客	個人情報	Web経由	情報持ち出し	氏名	住所	メールアドレス	電話番号	生年月日	性別	職種	ID		血液型、趣味、社内資料
AV	公共機関	行政機関	350	顧客	メールアドレス	Email経由	管理ミス			メールアドレス							
AW	企業	サービス	398	応募者	個人情報	Web経由	バグ・セキュリティホール	氏名	住所	メールアドレス	電話番号			職業			
AX	企業	製造業	3,244	応募者	個人情報	Web経由	バグ・セキュリティホール	氏名	住所	メールアドレス	電話番号	年齢	性別	職業			
AY	企業	情報通信	235	顧客	個人情報	Email経由	設定ミス	氏名	住所								グローバルIP
AZ	企業	製造業	1,200	応募者	個人情報	Web経由	バグ・セキュリティホール	氏名	住所		電話番号						
BA	企業	製造業	50,000	応募者	個人情報	Web経由	誤操作	氏名	住所	メールアドレス	電話番号	生年月日				アンケート内容	
BB	企業	サービス	400	応募者	個人情報	Web経由	不明	氏名								（アンケート内容）	学歴
BC	企業	建築	335	応募者	個人情報	Web経由	設定ミス	氏名	住所	メールアドレス	電話番号						
BD	公共機関	行政機関	59	顧客	メールアドレス	Email経由	誤操作			メールアドレス							
BE	その他	不明	不明	顧客	個人情報	Web経由	バグ・セキュリティホール	（氏名）									クレジットカード番号
BF	公共機関	行政機関	483	顧客	個人情報	Email経由	内部犯罪	氏名	住所		電話番号	年齢	性別				
BG	企業	サービス	65	顧客	個人情報	Web経由	バグ・セキュリティホール	氏名	住所	メールアドレス	連絡先						フリガナ、予約先宿名、人数、金額
BH	公共機関	行政機関	154	顧客	個人情報	Web経由	誤操作	氏名	住所					職業			
BI	公共機関	行政機関	190	応募者	個人情報	Web経由	設定ミス	氏名	住所	メールアドレス	電話番号					意見	
BJ	教育機関	教育機関	3,107	顧客	個人情報	Web経由	設定ミス	氏名	住所	メールアドレス	電話番号		性別				出身高校
BK	企業	情報通信	不明	顧客	個人情報	Web経由	バグ・セキュリティホール								ID	質問内容	プリペイドカード番号など
合計	63		418,716				項目該当件数→	55	38	29	28	10	5	6	4	11	21
							項目該当割合→	87%	60%	46%	44%	16%	8%	10%	6%	17%	33%

短期影響	全社集計	化学品製造	情報システム	大手小売	医療品製造	航空	情報誌	食品製造	機械製造
漏洩情報	-	個人情報漏洩	個人情報漏洩	個人情報漏洩	個人情報漏洩	個人情報漏洩	個人情報漏洩	個人情報漏洩	社内文書
発行株数	2,377,382,066	483,478,398	6,079,200	7,707,095	210,876,260	1,536,082,686	57,606,628	19,018,565	56,533,234
	事故前日との総時価額差	事故前日との総時価額差	事故前日との総時価額差	事故前日との総時価額差	事故前日との総時価額差	事故前日との総時価額差	事故前日との総時価額差	事故前日との総時価額差	事故前日との総時価額差
当日	-7,557,534,691	-3,570,789,380	-246,013,087	95,336,914	2,534,893,473	-5,303,310,519	-427,285,937	-225,429,799.7	-414,936,354.0
2日目	-15,090,054,733	-9,319,997,183	46,180,655	28,732,213	659,666,292	-4,467,471,450	-494,261,533	-420,015,359.6	-1,122,888,367.4
3日目	-22,281,835,550	-10,136,723,378	-68,408,193	58,530,572	88,668,452	-11,849,732,921	-541,013,847	-161,385,332.7	328,229,096.7
4日目	-6,523,862,893	-7,505,764,795	-126,945,939	-22,211,379	6,748,164,930	-6,046,465,328	-716,661,312	72,280,333.8	1,073,740,595.7
5日目	-8,553,216,391	-11,064,522,685	-11,002,820	-50,479,089	9,149,692,309	-8,174,986,014	-221,154,257	313,509,435.1	1,505,726,730.3
6日目	-8,794,742,121	-10,319,830,983	-16,641,328	-81,758,659	10,524,653,709	-11,755,846,673	-107,083,394	-76,225,381.2	3,037,990,588.6
7日目	-23,303,036,794	-10,731,911,935	-165,149,585	-103,446,264	9,212,738,910	-24,464,027,342	-199,652,563	743,883,773.8	2,404,528,211.1
8日目	-24,081,184,100	-12,321,170,730	-385,083,359	-125,037,603	5,180,669,468	-18,038,923,259	-117,826,407	566,334,255.4	1,159,853,533.4
9日目	-16,890,393,334	-15,510,004,135	-639,179,791	-131,661,895	9,364,655,312	-11,748,789,182	-331,241,032	321,888,099.7	1,783,939,288.7
10日目	-15,093,907,406	-8,847,818,215	-576,247,359	112,956,849	3,020,045,595	-9,336,303,585	-317,069,761	99,269,327.2	751,259,743.2
10日間累積	-148,169,768,014	-99,328,533,420	-2,188,490,807	-219,038,339	56,483,848,450	-111,185,856,272	-3,473,250,044	1,234,109,351.8	10,507,443,066.2
1日当り	-14,816,976,801	-9,932,853,342	-218,849,081	-21,903,834	5,648,384,845	-11,118,585,627	-347,325,004	123,410,935	1,050,744,307
一株当り差額	-6.23	-20.54	-36.00	-2.84	26.79	-7.24	-6.03	6.49	18.59
前日株価に対する差額割合	-	-7.44%	-3.10%	-0.33%	1.41%	-1.98%	-2.93%	1.02%	2.35%

中期影響	全社集計	化学品製造	情報システム	大手小売	医療品製造	航空	情報誌	食品製造	機械製造
漏洩情報	-	個人情報漏洩	個人情報漏洩	個人情報漏洩	個人情報漏洩	個人情報漏洩	個人情報漏洩	個人情報漏洩	社内文書
発行株数	2,377,382,066	483,478,398	6,079,200	7,707,095	210,876,260	1,536,082,686	57,606,628	19,018,565	56,533,234
	事故前日との総時価額差	事故前日との総時価額差	事故前日との総時価額差	事故前日との総時価額差	事故前日との総時価額差	事故前日との総時価額差	事故前日との総時価額差	事故前日との総時価額差	事故前日との総時価額差
当月末	2,904,335,092	-2,391,186,437	385,046,116	228,968,428	35,552,585,519	-30,089,363,254	992,471,666	361,720,517	-2,135,907,464
2ヶ月末	-33,500,748,617	-7,207,661,195	34,112,062	733,372,351	17,875,262,835	-40,587,241,253	383,916,817	-46,604,046	-4,685,906,188
3ヶ月末	-24,820,987,148	-7,056,963,701	53,223,297	1,000,553,392	568,067,968	-5,931,163,173	148,204,325	-163,011,541	-13,439,897,715
4ヶ月末	-33,659,566,285	-4,798,506,294	-825,642,464	540,858,539	1,623,993,216	-24,069,485,182	1,025,077,127	-1,072,899,642	-6,082,961,587
4ヶ月間累積	-89,076,966,959	-21,454,317,627	-353,260,990	2,503,752,711	55,619,909,539	-100,677,252,861	2,549,669,936	-920,794,712	-26,344,672,954
1ヶ月当り	-22,269,241,740	-5,363,579,407	-88,315,247	625,938,178	13,904,977,385	-25,169,313,215	637,417,484	-230,198,678	-6,586,168,238
一株当り差額	-9.4	-11.1	-14.5	81.2	65.9	-16.4	11.1	-12.1	-116.5
前月株価に対する差額割合	-	-4.40%	-1.29%	9.44%	3.97%	-4.50%	5.40%	-1.86%	-14.26%