Fiscal 2003

Information Security Incident

Survey Report

＜Section One＞

Information Security Incident Survey and Damage Calculation Model

JAPAN NETWORK SECURITY ASSOCIATION

March 31, 2004

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. Yasuhiko Sato	SRA (Software Research Associates, 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. Kiyoshi Nagashima	The Tokio Marine & Fire Insurance Company, Ltd.
Mr. Tomohisa Sashida	The Tokio Marine Risk Consulting Co., Ltd.
Mr. Tomoki Sano	TOPPAN Printing Co., Ltd.
Mr. Koichi Narusawa	TOPPAN Printing Co., Ltd.
Mr. Yukihiro Matsuya	HUCOM Incorporated
Mr. Shiro Maruyama	Little eArth Corporation

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 sponsored by the JNSA.

＜About Section One＞

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 within the JNSA membership. 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 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.

＜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" presented last year, 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.

2. Objectives

The almost daily outbreaks of new viruses, information disclosure incidents, partial enaction of the Personal Information Protection Act, and more take an ever-increasing amount of time and attention of IT security workers. This state of affairs calls for an even greater volume of case study investigation and on-site observations of information systems and information management security incidents.

Unfortunately, it is very difficult to find any compiled data related to specific cases and related damage costs of security incidents. And though Mass Media reports of information disclosure incidents have become more frequent, there is still a dearth of public information related to the nature of such incidents, and definitions of related "damages" remain vague. At present, we cannot readily calculate damage amounts resulting from security incidents.

The same can be said about information related to preventive and remedial measures, with no clear definition of "preventive costs," and a lack of information related to costs of countermeasures.

Section One of this report documents the results of our efforts to obtain information (through questionnaires and interviews) about cyber terrorism and major infrastructure security incidents in Japan. This year, we conducted a survey in cooperation with the Research Institute of Science and Technology for Society (RISTEX), sending out questionnaires that included more detail and greater scope than the previous year. As a result, we were able to receive many more valid responses. We used the information obtained from our survey to make observations related to understanding, and measuring the effects of, the "Degree of Risk" and the "Scope of Countermeasures" for information security management, using the model developed in the previous year to estimate damages and investment costs related to information security countermeasures.

Section Two (Supplement) this year again deals with "information disclosure," a type of incident involving major social implications, and a constantly 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. Survey Results and Analysis

3.1 Survey Participants

- Information Technology companies, mainly from the JNSA corporate membership (including several non-IT companies).

  JNSA Security Incidents Investigation Working Group members conducted these surveys.

- 1,000 publicly traded companies listed in the First Section of the Tokyo Stock Exchange (selected randomly).

  The Research Institute of Science and Technology for Society (”RISTEX” below) conducted these surveys.

3.2 Survey Methodology

- The survey was conducted using questionnaires and/or interviews with representatives from participating companies.
- The questionnaire for this year’s survey featured a more convenient format, with more sophisticated levels of answer choices than the questionnaire used in last year’s survey. (See “9.1 Questionnaire Form”)
- The questionnaires sent to JNSA member corporations were sent together with a letter of request from the JNSA General Secretariat. Responses were received at the JNSA offices and tallied.
- The questionnaires sent to the 1,000 companies selected by RISTEX were addressed to the person in charge of information security at each company. Responses were collected and tallied at the RISTEX offices.
- Members of the Working Group conducted detailed in-person interviews at those companies that indicated their willingness to participate.

3.3 Survey Results

3.3.1 Interview Results

See “5. Incident Survey Interview Report”.

3.3.2 Questionnaire Survey Results (Tabulation Tables)

See “3.4 Survey Results Analysis and Findings”.

3.3.3 Questionnaire Response Rates

The table below indicates the number of questionnaires sent and number of responses:

	Questionnaires		
	Sent	Returned	Response Rate
JNSA	190	47	24.74%
RISTEX	1,000	167	16.70%
Total	1,190	214	17.98%

The response rate for JNSA questionnaires was approximately 25%, more than a 10% decrease compared to the 43% response rate of two years ago and the 37% response rate of last year. However, combined with the RISTEX questionnaires, the overall response rate was approximately 18%, with 214 valid responses collected. This represents a three-fold increase in valid responses compared with last year's 66 responses.

3.4 Survey Results Analysis and Findings

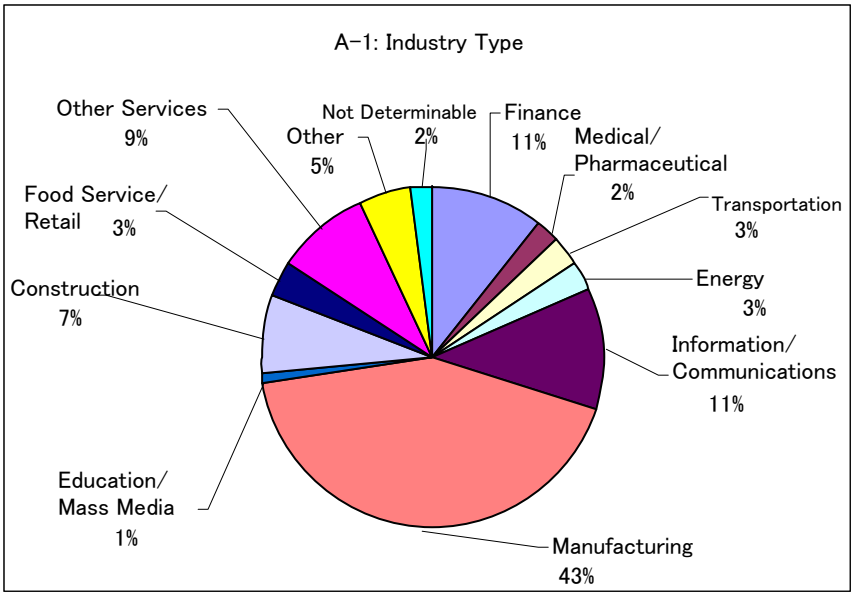
3.4.1 This Year's Survey Results and Observations

The following paragraphs show the results of the 214 questionnaires received, including our comments as to the analysis and observations thereof.

A Please tell us about your company's business.

A-1 Tell us the main industry in which your company does business (Select one by circling your answer).

	Industry	No.	%
1	Finance (banking, insurance, securities)	23	10.7%
2	Medical/ Pharmaceutical	5	2.3%
3	Transportation/ Shipping	6	2.8%
4	Energy	6	2.8%
5	Information/ Communications	24	11.2%
6	Manufacturing	91	42.5%
7	Education/ Mass Media	2	0.9%
8	Construction	16	7.5%
9	Food Service/ Retail	7	3.3%
10	Other Services	19	8.9%
11	Other	11	5.1%
12	Not determinable	4	1.9%
		214	100%



Note

In last year's survey (consisting mainly of JNSA member corporations), more than half of the respondents belonged to the Information/ Communications industry. No respondents indicated their company belonged to the Medical/ Pharmaceutical, Transportation/ Shipping, Food Service/ Retail or other industries. In this year's survey, a wide range of industry types are represented, with Manufacturing being the most widely represented at 43% of respondents. We believe the results of this year's questionnaires are more representative of the actual makeup of corporations in Japan today.

A-2 Annual Sales and Number of Employees.

■ Averages

Average Sales (¥millions)	318,956.63
Employees	4,084

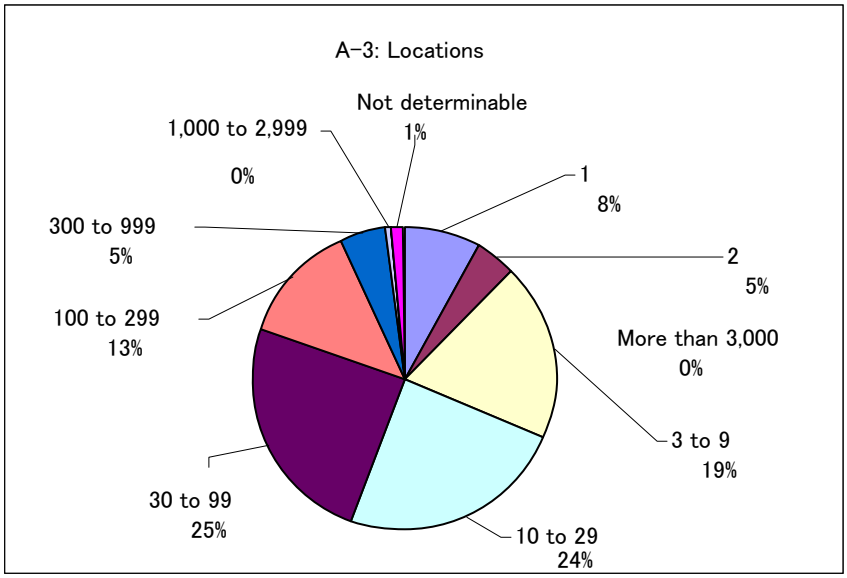
Note

The above values represent an average of the 214 survey respondents. The minimum annual and maximum annual sales for respondents were ¥1.5 million and approx. ¥5.2 trillion, respectively. The number of employees varied greatly among respondents, from three employees at the smallest firm to 140,000 employees at the largest firm.

Compared with the previous year, average annual sales and average number of employees for this year's respondents were about 1.9 times and 2.3 times greater, respectively. Given that these are average values, we cannot make any simple conclusions; however, considering the responses related to number of locations below, it would seem that there is a greater comparative number of larger scale corporations in this year's survey as compared to last year.

A-3 How many offices/ locations does your company have?

	Locations	No.	%
1	1	17	7.9%
2	2	10	4.7%
3	3 to 9	40	18.7%
4	10 to 29	52	24.3%
5	30 to 99	53	24.8%
6	100 to 299	27	12.6%
7	300 to 999	11	5.1%
8	1,000 to 2,999	1	0.5%
9	3,000 and above	0	0.0%
10	Not determinable	3	1.4%
		214	100%



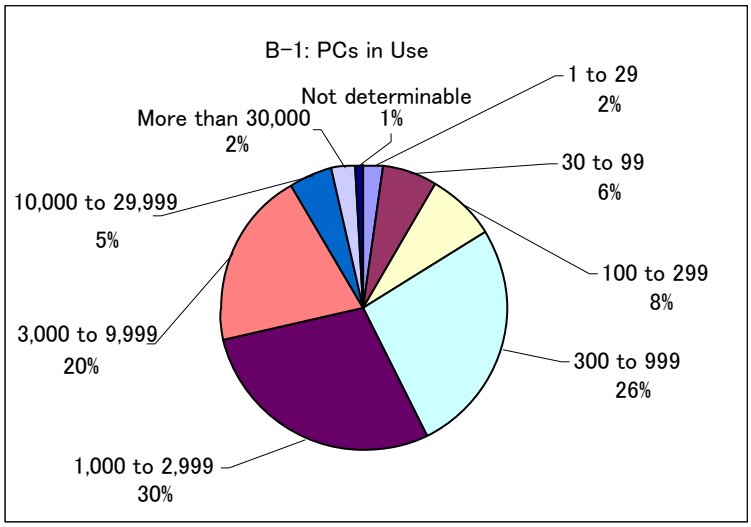
Note

In last year's survey, 83% of respondents indicated their business had 29 or fewer locations, while 62% of respondents indicated their business had nine or fewer locations. In this year's survey, 56% of respondents indicated their business had 29 or fewer locations, and 31% of respondents indicated their business had nine or fewer locations. At the same time 49% of respondents indicated their business had between 10 and 99 locations. Further, one respondent this year indicated their business had over 1,000 locations, where no such respondent existed in the previous year.

B Please tell us about your company's information systems.

B-1 How many personal computers (PCs) are in use at your company?

	PCs	No.	%
1	1 to 29	5	2.3%
2	30 to 99	13	6.1%
3	100 to 299	17	7.9%
4	300 to 999	56	26.2%
5	1,000 to 2,999	62	29.0%
6	3,000 to 9,999	43	20.1%
7	10,000 to 29,999	11	5.1%
8	30,000 and above	5	2.3%
9	Not determinable	2	0.9%
		214	100%

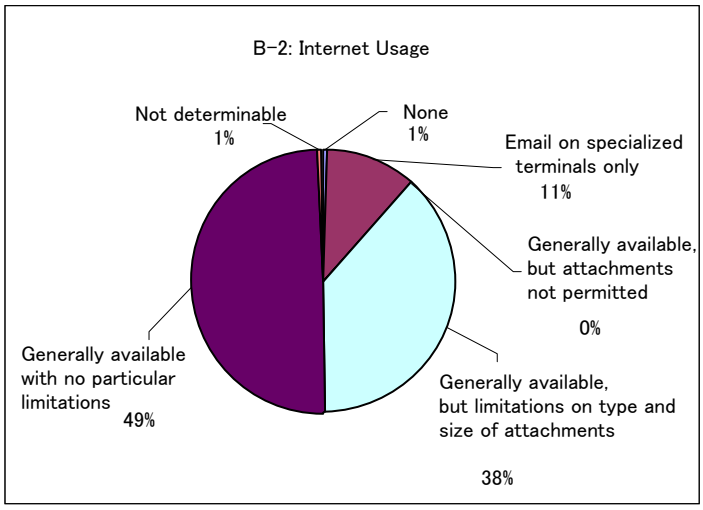


Note

Since we do not have a comparison between the number of employees and the number of PCs, we cannot make any conclusions as to the current state of PC usage (PC/ employee ratio). However, the answer to this question, when combined with the fact that nearly 90% of respondents indicated that "Many work activities have been computerized" (B-5 How much of your company's work activities have been computerized?), we can surmise that the PC has become an indispensable work tool.

B-2 What is the level of Internet mail usage in your company? (Select one)

	Usage Level	No.	%
1	None	2	0.9%
2	Email on specialized terminals only	23	10.7%
3	Generally available, but attachments not permitted	0	0.0%
4	Generally available, but limitations on type and size of attachments	81	37.9%
5	Generally available with no particular limitations	106	49.5%
6	Not determinable	2	0.9%
		214	100%



Note

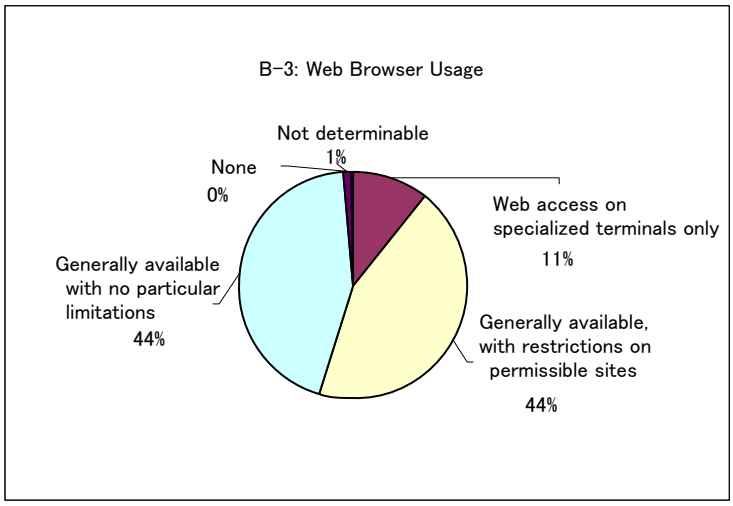
With respect to Internet mail usage, two respondents indicated "None," while a total of 23 respondents indicated that Email was available on "…specialized terminals only." This survey included responses from 23 companies describing themselves as belonging to the Finance industry. Our presumption is that the results here stem from these firms reacting to information security risks such as viruses and other dangers, rather than a refusal to modernize their businesses. We cannot fault these types of companies choosing safety over convenience, when they have undertaken such important roles in supporting our financial and societal infrastructure.

As in last year's survey, no respondents indicated they prohibited the use of Email attachments; however, 38% of respondents put some type of limitation on attachments, up from 32% in the previous year.

We believe this reflects a corporate response to information security issues (mail filtering) and dramatic increases in attachment file sizes (image files, etc.)

B-3 What is the level of Web browser usage in your company? (Select one)

	Usage Level	No.	%
1	None	0	0.0%
2	Web access on specialized terminals only	23	10.7%
3	Generally available, with restrictions on permissible sites	94	43.9%
4	Generally available with no particular limitations	94	43.9%
5	Not determinable	3	1.4%
		214	100%



Note

As in the previous year, all respondents indicated they allow some type of Web browsing. More than half reported they do institute some form of restrictions on Web browsing, as a total of 54% of respondents either allow “Web access on specialized terminals only” or make Web browsing “Generally available, with restrictions on permissible sites.” This marks a two-fold increase over the 25% level in the previous year.

The current state of Web browsing and Email usage reveals that half of responding corporations enforce some type of restrictions, while the other half allow usage without limitations of any sort. The trend, however, is for an increase in the number of corporations that enforce usage limitations.

B-4 What percentage of your company's PCs (clients) have Email/ Web access?

■ Average Values

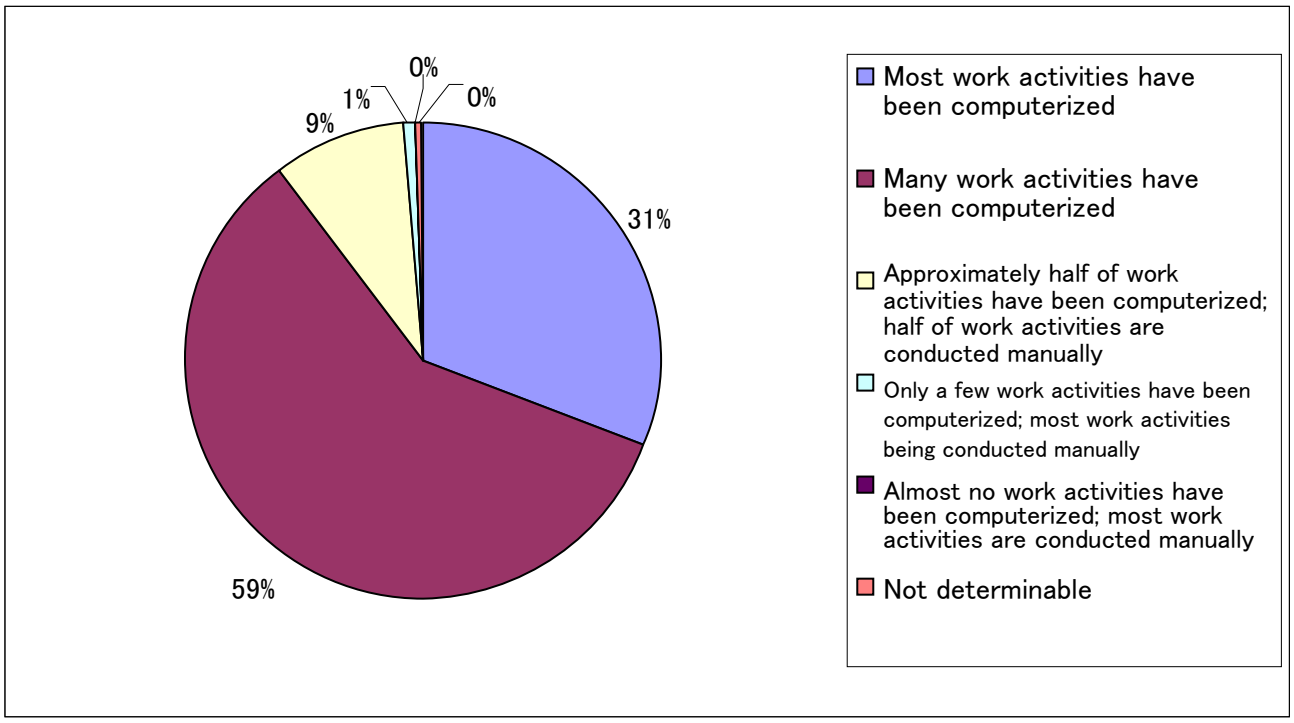
1	Internet Mail (%)	79%
2	Web Access (%)	75%

Note

A look at these averages indicates that slightly less than 80% of PCs at respondent businesses have Internet Mail and Web access.

B-5 How much of your company's work activities have been computerized? Indicate in general terms your company's reliance on computer systems. (Select one)

	System Reliance	No.	%
1	Most work activities have been computerized	66	30.8%
2	Many work activities have been computerized	126	58.9%
3	Approximately half of work activities have been computerized; half of work activities are conducted manually	19	8.9%
4	Only a few work activities have been computerized; most work activities are still conducted manually	2	0.9%
5	Almost no work activities have been computerized; most work activities are conducted manually	0	0.0%
6	Not determinable	1	0.5%
		214	100.0%



Note

Almost 90% of respondents answered either "Most work activities have been computerized" or "Many work activities have been computerized." Adding those who indicated "Approximately half of work activities have been computerized; half of work activities are conducted manually," the total reaches approximately 99% of all respondents, showing the high level of dependence on computers for everyday work activities in modern business.

B-6 How many employees are assigned to information security management?

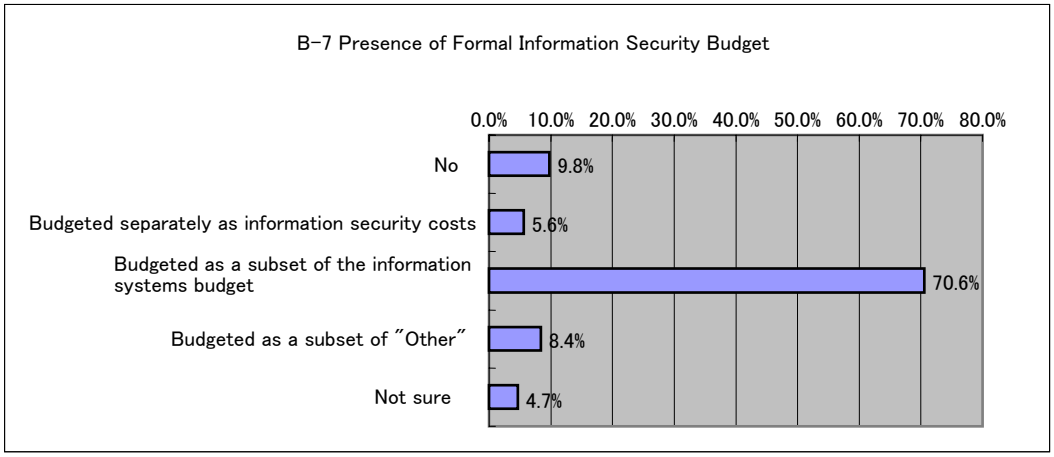
1	Full-time (no.)	2.0	Average number of information security employees at companies with full-time information security personnel
2	Part-time with other job duties (no.)	22.0	Average number of part-time information security employees at companies with part-time information security personnel
3	Officer assigned to oversee information security	32.7%	Percentage of companies with an officer devoted to information security oversight

Note

The figures above for full-time and part-time information security personnel represent the average number of employees for those firms with full-/ part-time staff assigned to information security. The figure for corporate officers assigned to oversee information security represents the percentage of all respondents who indicated they had an officer in such capacity. From our in-person interviews we learned many of part-time information security personnel are IT system personnel or personnel within each business department who are that department's representative on a company information security committee, etc.

B-7 Does your company have a formal information security budget? (Select one by circling your answer)

	Information Security Budget	No.	%
1	No	21	9.8%
2	Budgeted separately as information security costs	12	5.6%
3	Budgeted as a subset of the information systems budget	151	70.6%
4	Budgeted as a subset of "Other"	18	8.4%
5	Not sure	10	4.7%
		212	99.1%



Note

Only 5.6% of respondents indicated their companies had a separate information security budget. 70.6% of respondents indicated their companies budgeted for information security as a subset of their information systems budget. The reason for this would be difficulty in allocating costs. For example, while there are products and services designed specifically for information security (anti-virus software, etc.), there are other products that partially function as security devices, together with their main information technology functions (routers, etc.)

B-8 If you marked any category 2 through 4 above, please provide some general figures

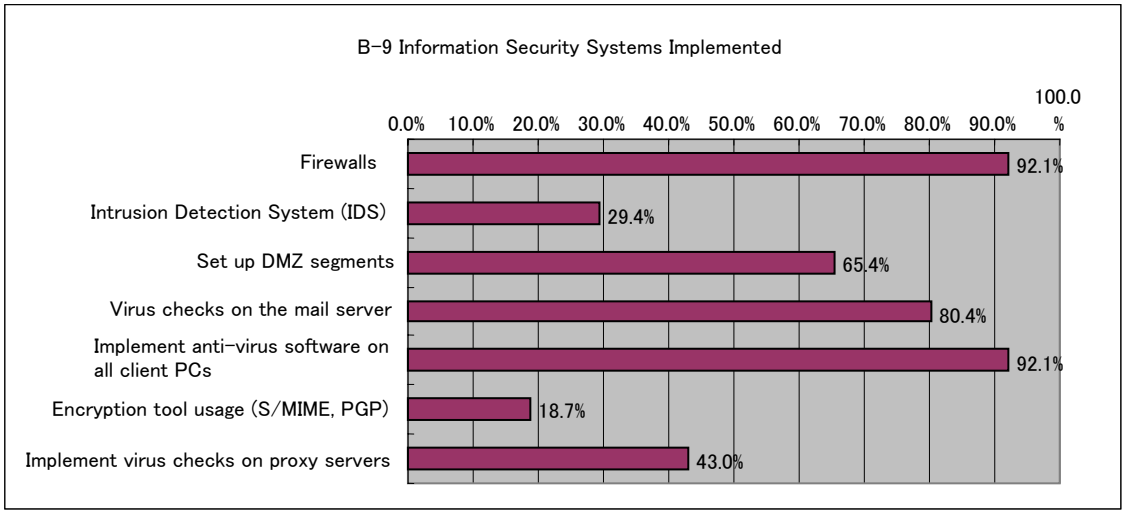
Budgeted amount (¥millions)	55.73	Avg. (¥millions)
Ratio of information security budget to information systems budget (%)	6.1	Avg. (%)
Increase/ decrease	5.67	Avg. (¥millions)

Note

The response to this question showed a wide discrepancy among respondents. The smallest amount budgeted for information systems security was ¥500,000, while the largest amount budgeted was ¥2 billion. The smallest budget amounted to ¥167,000 per person, while the largest budgeted amount equated to ¥45,000 per person, or a four-fold difference. It is quite logical that larger companies would end up spending less per individual on information security budgets.

B-9 What systems have you implemented to insure information security? (Circle all that apply)

	Implemented Systems	No.	%
1	Firewalls	197	92.1%
2	Intrusion Detection System (IDS)	63	29.4%
3	Set up DMZ segments	140	65.4%
4	Virus checks on the mail server	172	80.4%
5	Implement anti-virus software on all client PCs	197	92.1%
6	Encryption tool usage (S/MIME, PGP)	40	18.7%
7	Implement virus checks on proxy servers	92	43.0%
8	Not sure	0	0.0%

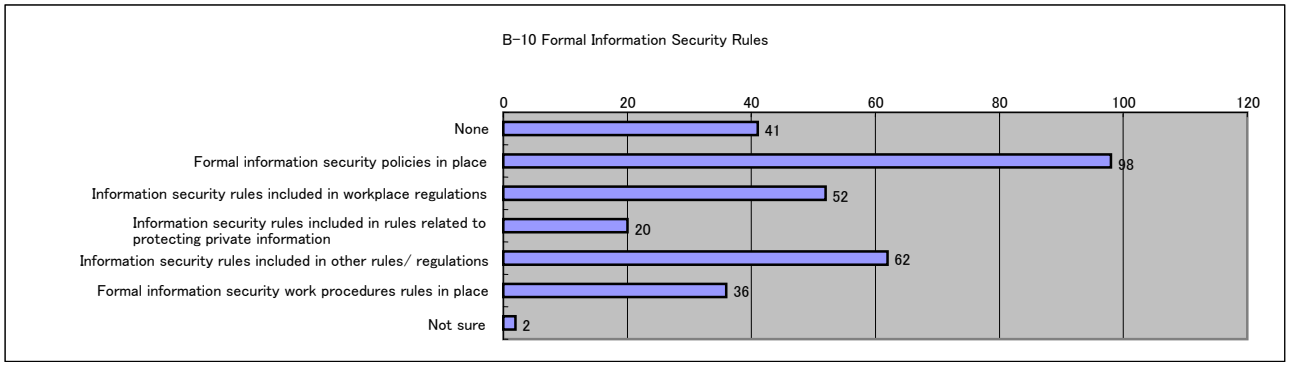


Note

At 92.1%, the level of firewall usage and anti-virus software on client PCs is very high. It appears these measures are common sense for any company allowing access to the Internet. The next most common measure is checking for viruses on mail servers, demonstrating the seriousness with which companies take the threat of viruses.

B-10 Does your company have formal information security rules? (Mark all that apply)

	Information Security Rules	No.	%
1	None	41	19.2%
2	Formal information security policies in place	98	45.8%
3	Information security rules included in workplace regulations	52	24.3%
4	Information security rules included in rules related to protecting private information	20	9.3%
5	Information security rules included in other rules/ regulations	62	29.0%
6	Formal information security work procedures rules in place	36	16.8%
7	Not sure	2	0.9%

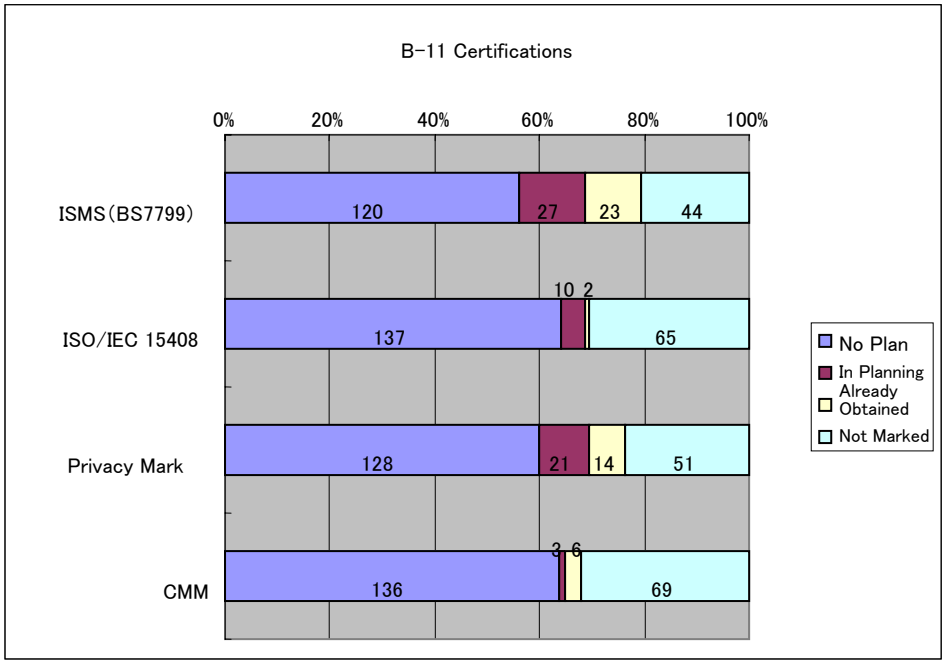


Note

Almost one-half of all respondents (45.8%) have security rules/ policies in place. The option to provide multiple answers to this question does cloud the issue somewhat, but in total an excess of 100% of respondents have some sort of information security-related rules or policies in place. We believe the response to this question clearly indicates the high interest in corporate information security.

B-11 Indicate whether certification is "In Planning" or "Already Obtained." Circle the status that applies.

Name	No Plan		In Planning		Already Obtained		Not Marked	
ISMS (BS7799)	120	56.1%	27	12.6%	23	10.7%	44	20.6%
ISO/IEC 15408	137	64.0%	10	4.7%	2	0.9%	65	30.4%
Privacy Mark	128	59.8%	21	9.8%	14	6.5%	51	23.8%
CMM	136	63.6%	3	1.4%	6	2.8%	69	32.2%



Year Certification Obtained

Name	1998	1999	2000	2001	2002	2003
ISMS(BS7799)				2	6	12
ISO/IEC 15408			1			1
Privacy Mark	1	1	4	3	2	2
CMM					1	1

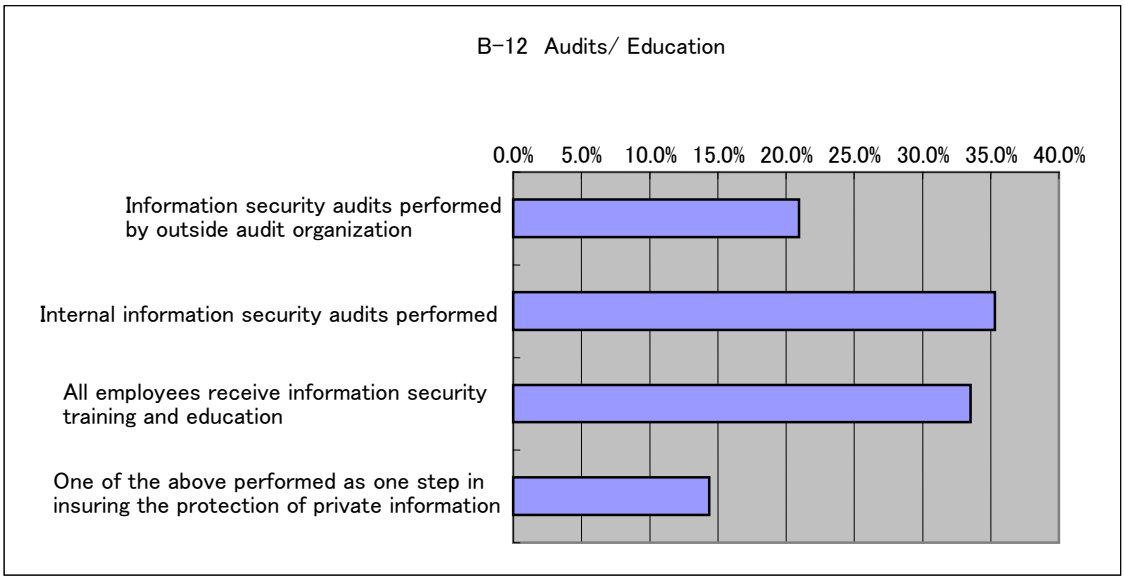
Note

The most prevalent certification obtained was ISMS, with 23. Another 27 companies have indicated they plan on obtaining this certification. The increasing trend for this certification can be seen in the chart showing the years in which certification was obtained.

The next most common certification was that for the Privacy Mark, with 14, and another 21 in planning. We believe Privacy Mark certification will continue to increase past 2004 due to the influence of the Personal Information Protection Act. Only a few firms indicated they had already obtained, or were planning on obtaining, ISO/IEC 15408 or CMM certification.

B-12 Information security audits, education and training (Circle all that apply)

Audits/ Education and Training	Performed	Not Performed
Information security audits performed by outside audit organization	21	79
Internal information security audits performed	35	65
All employees receive information security training and education	34	66
One of the above performed as one step in insuring the protection of private information	14	86



Note

This category was only included in the questionnaires sent out by RISTEX. More than 30% of respondents indicated they performed some type of internal information security audits, as well as education/ training for all employees. However, the number of companies having security audits performed by outside organizations was comparatively low at 20%.

C　Please tell us about information security management at your company. (JNSA questionnaire)

C-1 Does your company have formal information security rules? (Mark all that apply)

	Information Security Rules	No.	%
1	None	6	12.8%
2	Formal information security policies in place	31	66.0%
3	Information security rules included in workplace regulations	14	29.8%
4	Information security rules included in rules related to protecting private information	6	12.8%
5	Information security rules included in other rules/ regulations	7	14.9%
6	Formal information security work procedures rules in place	12	25.5%
7	Not sure	0	0.0%

C-2　For those who responded, "1. None" to Question C-1:

What is the greatest reason for not establishing information security rules? (Select one)

	Information Security Rules	No.
1	Management does not see the need	0
2	Locality/ department in charge does not see the need	0
3	Low level of necessity among those in the industry/ business type	1
4	Not enough resources (personnel, capital) within the company	2
5	Not sure	0

Note

This questionnaire and the following questionnaire results have been tallied from the questionnaires sent to the JNSA corporate members. Question C-1 is the same as question B-10, and therefore we will dispense with any commentary here. The greatest two reasons for respondents not to have information security rules in place are "Low level of necessity" and "lack of resources".

C-3　In what year did your company first establish information security rules/ procedures?

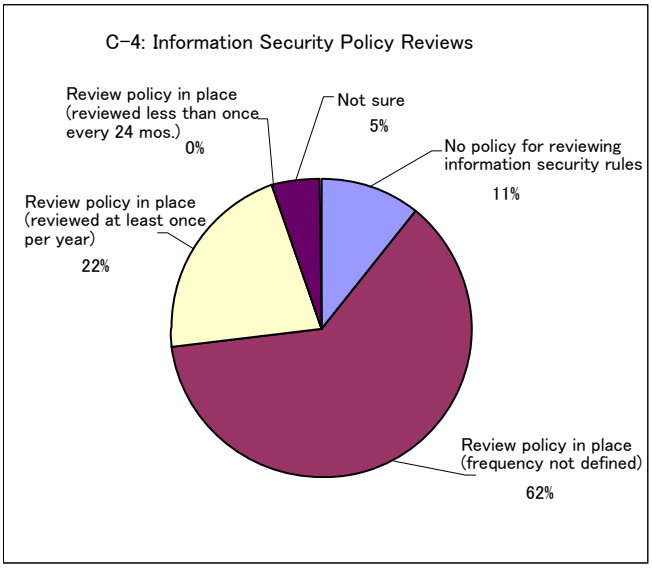
1994	1995	1996	1997	1998	1999	2000	2001	2002	2003
1	-	-	-	2	-	5	6	11	9

Note

One respondent had established information security rules as far back as 1994; however, most implemented rules during and after the year 2000. As seen with the relatively large number of companies obtaining ISMS certification in 2002 and 2003, the last two years have seen an increase in the number of firms establishing information security rules.

C-4 Does your company have a procedure for reviewing information security rules? (Select one)

	Information Security Rules Review	NO.	%
1	No policy for reviewing information security rules	4	10.8%
2	Review policy in place (frequency not defined)	23	62.2%
3	Review policy in place (reviewed at least once per year)	8	21.6%
4	Review policy in place (reviewed less than once every 24 mos.)	0	0.0%
5	Not sure	2	5.4%

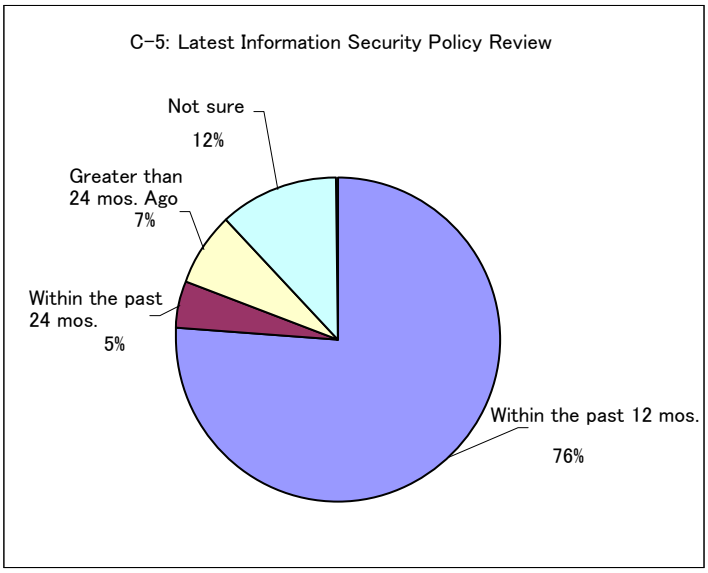


Note

This part of the questionnaire was for those companies responding that they had adopted some type of information security rules. Only four respondents said that they had "No policy for reviewing information security rules," while most firms have a policy in place. Sixty-two percent of respondents indicated they had no set frequency for reviewing information security rules. Our interpretation is that if the frequency of review corresponds with each company's requirements, then such review is being conducted effectively.

C-5 When was the last time an information security policy review (or initial implementation) took place? (Select one)

	Last Review	No.	%
1	Within the past 12 mos.	32	76.2%
2	Within the last 24 mos.	2	4.8%
3	Greater than 24 mos. Ago	3	7.1%
5	Not sure	5	11.9%

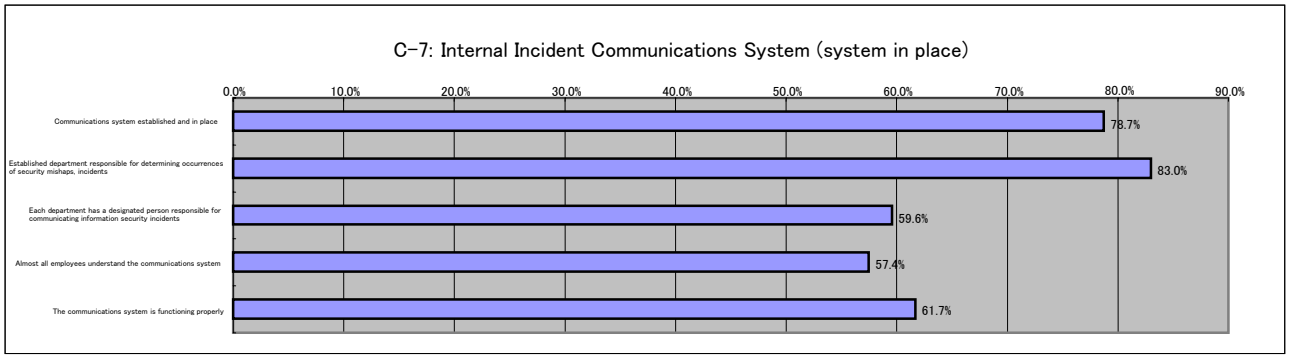


Note

Seventy-six percent of respondents have conducted a review of their information security rules within the last 12 months. As mentioned in the comments under C-4, we see here that companies are conducting reviews of their security policies frequently, changing policies as necessary.

C-7 System for communicating information security mishaps and incidents throughout the company (System in place/ not in place). (Mark all that apply)

	Communications system	No.	%
1	Communications system established and in place	37	78.7%
2	Established department responsible for determining occurrences of security mishaps, incidents	39	83.0%
3	Each department has a designated person responsible for communicating information security incidents	28	59.6%
4	Almost all employees understand the communications system	27	57.4%
5	The communications system is functioning properly	29	61.7%



	Communications system (established within the last 12 mos.)	No.	%
1	Communications system established and in place	9	19.1%
2	Established department responsible for determining occurrences of security mishaps, incidents	8	17.0%
3	Each department has a designated person responsible for communicating information security incidents	4	8.5%

	Communications system (established after an incident occurred)	No.	%
1	Communications system established and in place	1	2.1%
2	Established department responsible for determining occurrences of security mishaps, incidents	0	0.0%
3	Each department has a designated person responsible for communicating information security incidents	2	4.3%

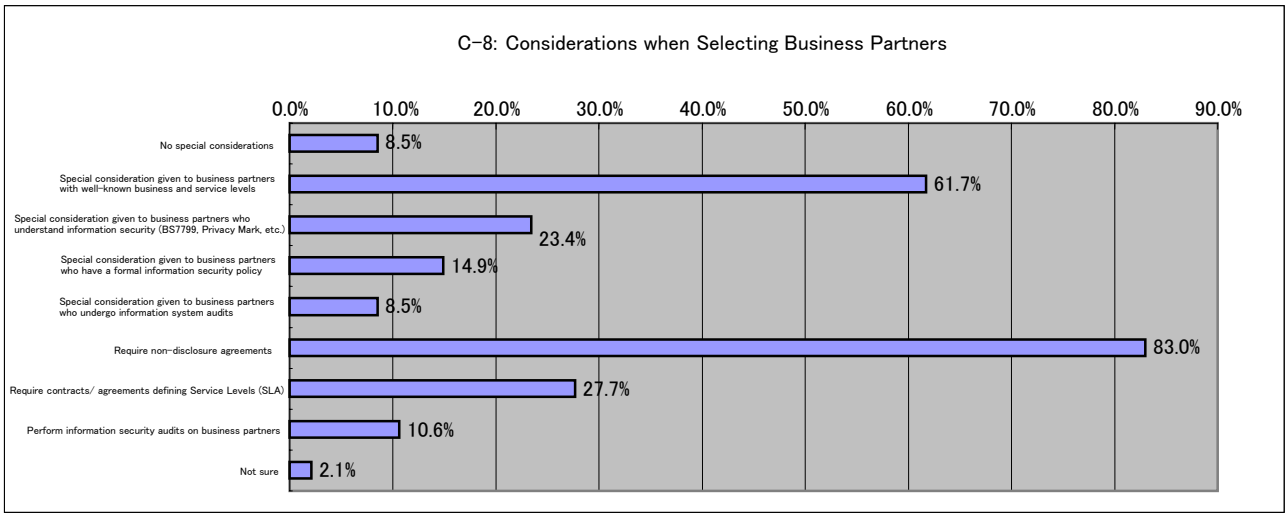
Note

Results of our survey reveal a high level (80%) of companies that have established rules for a communication system and a responsible department with respect to reporting information security incidents or mishaps.
In contrast, approximately 60% of respondents replied that all employees had a good understanding of the system or that the communications system was functioning properly, 20% less than the percentage of companies with rules in place. In terms of numbers, this represents ten companies, which is almost the same exact number as those companies who have established a communications system within the previous 12 months. It seems that more time is needed before the policies related to incident communications is clearly understood by all company

personnel.

C-8 Information security considerations when selecting or contracting with business partners. (Mark all that apply)

	Considerations when Selecting/ Contracting	No.	%
1	No special considerations	4	8.5%
2	Special consideration given to business partners with well-known business and service levels	29	61.7%
3	Special consideration given to business partners who obtained certification related to information security (BS7799, Privacy Mark, etc.)	11	23.4%
4	Special consideration given to business partners who have a formal information security policy	7	14.9%
5	Special consideration given to business partners who undergo information system audits	4	8.5%
6	Require non-disclosure agreements	39	83.0%
7	Require contracts/ agreements defining Service Levels (SLA)	13	27.7%
8	Perform information security audits on business partners	5	10.6%
9	Not sure	1	2.1%

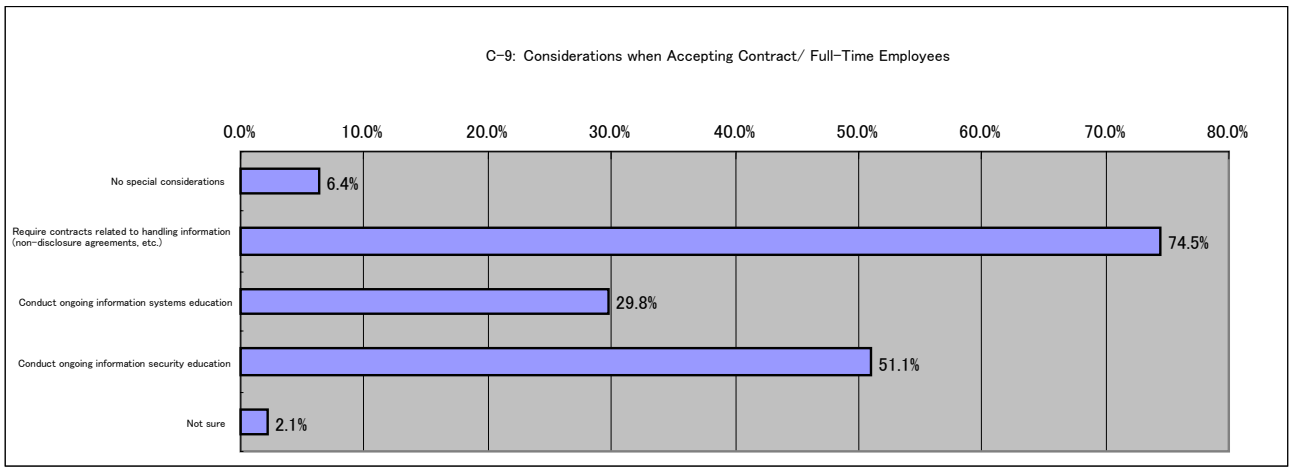


Note

Requiring a non-disclosure agreement was the most frequent answer with 83% of respondents. The next most frequent response cited was that of doing business with partners who have well-known businesses and service levels (62%), showing the importance placed on finding stable business partners. None of the other possible answers scored more than a 30% response; apparently these factors are not considered as important by the respondents to this year's survey.

C-9 Information security considerations when accepting contract or full-time engineers/operators. (Circle all that apply)

	Considerations	No.	%
1	No special considerations	3	6.4%
2	Require contracts related to handling information (non-disclosure agreements, etc.)	35	74.5%
3	Conduct ongoing information systems education	14	29.8%
4	Conduct ongoing information security education	24	51.1%
5	Not sure	1	2.1%

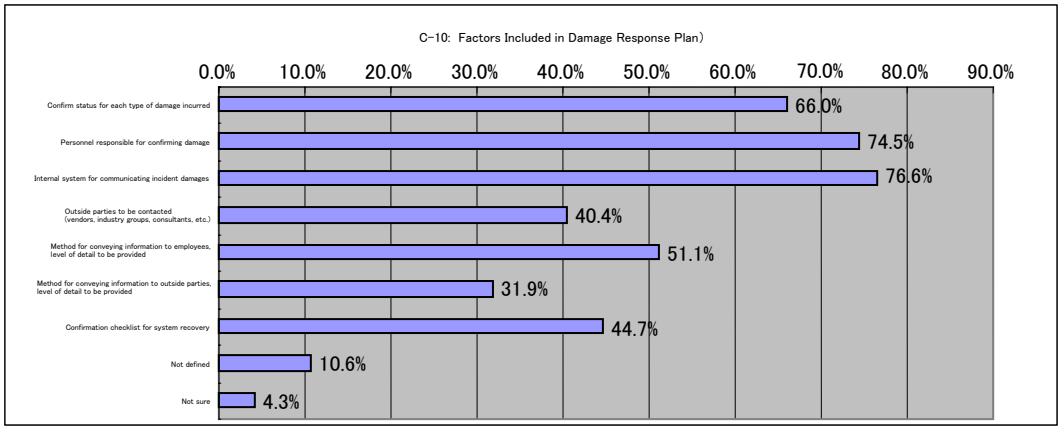


Note

As with the prior question (considerations for selecting a business partner), the most frequent response to this question was requiring non-disclosure agreements for other than full-time personnel (74% of respondents). The next most frequent answer is information security education (51%), showing that information security is a concern for those other than full-time employees as well.

C-10 Factors included in damage response plan (System in place/ not in place). (Circle all that apply)

	Factors Included in Response Plan	No.	%
1	Confirm status for each type of damage incurred	31	66.0%
2	Personnel responsible for confirming damage	35	74.5%
3	Internal system for communicating incident damages	36	76.6%
4	Outside parties to be contacted (vendors, industry groups, consultants, etc.)	19	40.4%
5	Method for conveying information to employees, level of detail to be provided	24	51.1%
6	Method for conveying information to outside parties, level of detail to be provided	15	31.9%
7	Confirmation checklist for system recovery	21	44.7%
8	Not defined	5	10.6%
9	Not sure	2	4.3%



	Factors Included in Response Plan (plan implemented within the last 12 mos.)	No.	%
1	Confirm status for each type of damage incurred	2	4.3%
2	Personnel responsible for confirming damage	3	6.4%
3	Internal system for communicating incident damages	4	8.5%
4	Outside parties to be contacted (vendors, industry groups, consultants, etc.)	2	4.3%
5	Method for conveying information to employees, level of detail to be provided	2	4.3%
6	Method for conveying information to outside parties, level of detail to be provided	3	6.4%
7	Confirmation checklist for system recovery	2	4.3%

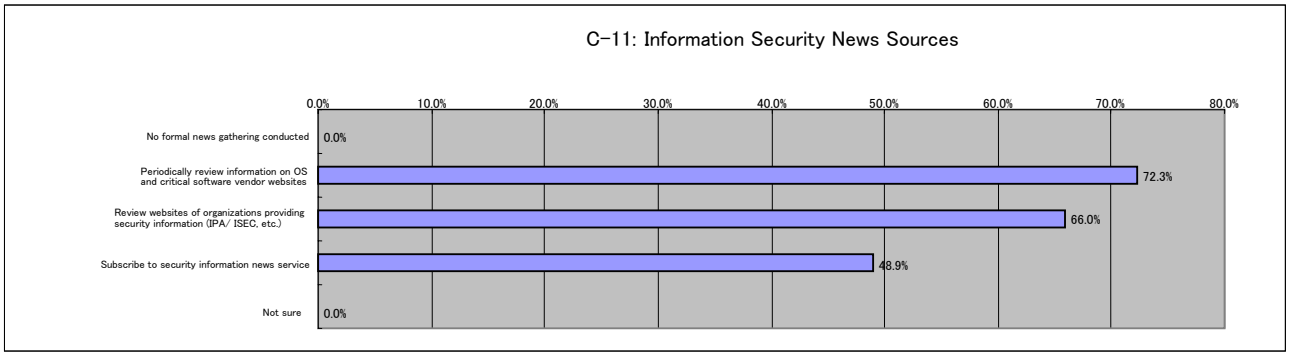
	Factors Included in Response Plan (plan implemented after incident occurred)	No.	%
1	Confirm status for each type of damage incurred	2	4.3%
2	Personnel responsible for confirming damage	1	2.1%
3	Internal system for communicating incident damages	1	2.1%
4	Outside parties to be contacted (vendors, industry groups, consultants, etc.)	0	0.0%
5	Method for conveying information to employees, level of detail to be provided	0	0.0%
6	Method for conveying information to outside parties, level of detail to be provided	1	2.1%
7	Confirmation checklist for system recovery	0	0.0%

Note

This questionnaire question related to plans for responding to damages incurred. The responses track closely with those from question C-7. These responses indicate a high level of preparedness with respect to communications systems, person responsible for confirming damages, and confirming status for each type of damage incurred. Compared with a 31.9% response for having method for conveying information to outside parties and the level of detail to be provided, more than 50% of respondents indicated they had the same policies in place with respect to their employees. This discrepancy in ratios is most likely due to fears of disclosing information to outside parties who may then intentionally take advantage of the information security weakness.

C-11 How do you gather information security-related news? (Circle all that apply)

	Method	No.	%
1	No formal news gathering conducted	0	0.0%
2	Periodically review security-related information on OS and critical software vendor websites	34	72.3%
3	Review websites of organizations providing security information (IPA/ ISEC, etc.)	31	66.0%
4	Subscribe to security information news service	23	48.9%
5	Not sure	0	0.0%

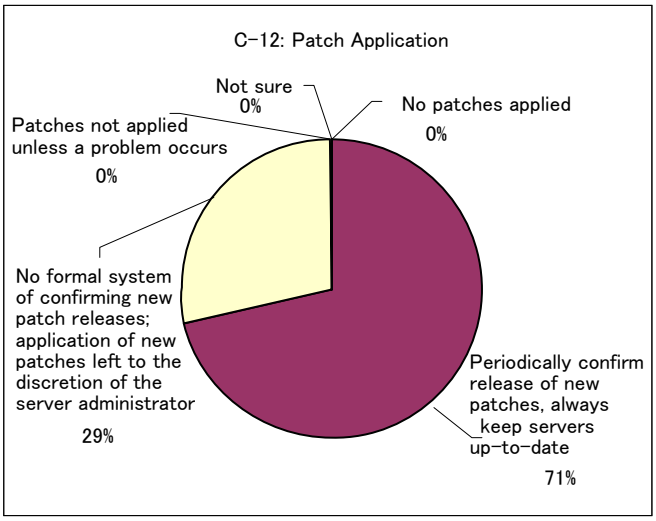


Note

All respondents indicated that they conducted some type of information security-related news gathering, with many using the Internet to locate pertinent information. Nearly one-half of respondents subscribe to an information news service.

C-12　Application of patches to ensure network server security (Select one)

	Patch Applications	No.	%
1	No patches applied	0	0.0%
2	Periodically confirm release of new patches, always keep servers up-to-date	30	71.4%
3	No formal system of confirming new patch releases; application of new patches left to the discretion of the server administrator	12	28.6%
4	Patches not applied unless a problem occurs	0	0.0%
5	Not sure	0	0.0%

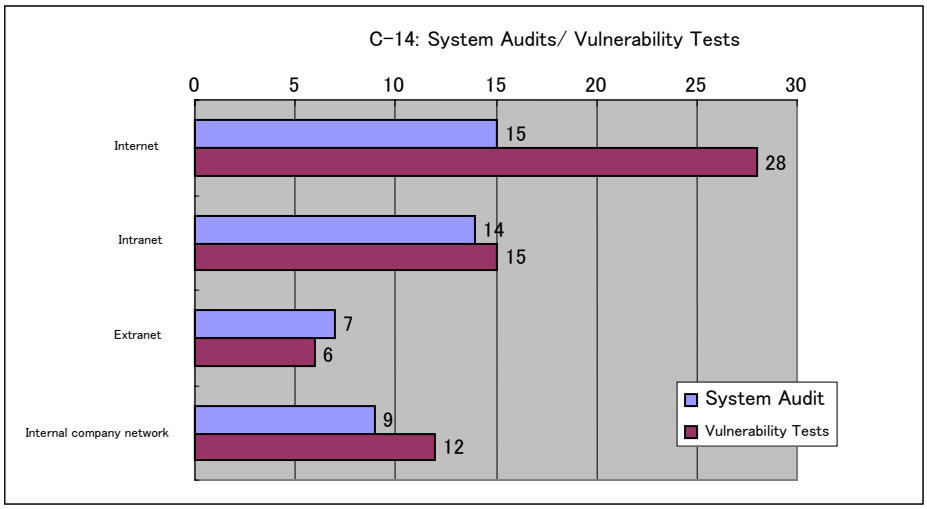


Note

During our interviews, we were left with the impression that interviewees were very careful regarding their use of patches. The main concern appeared to be fear of potential system stoppages or other problems when a new patch is applied. Even so, 71% of respondents answered that they kept their servers up-to-date with the latest patches, indicating a greater fear of the risks of not applying new patches.

C-13　Has your organization conducted system audits and/or vulnerability tests (penetration tests) within the last 12 months?

System	System Audit	Vulnerability Testing
Internet	15	28
Intranet	14	15
Extranet	7	6
Internal company network	9	12

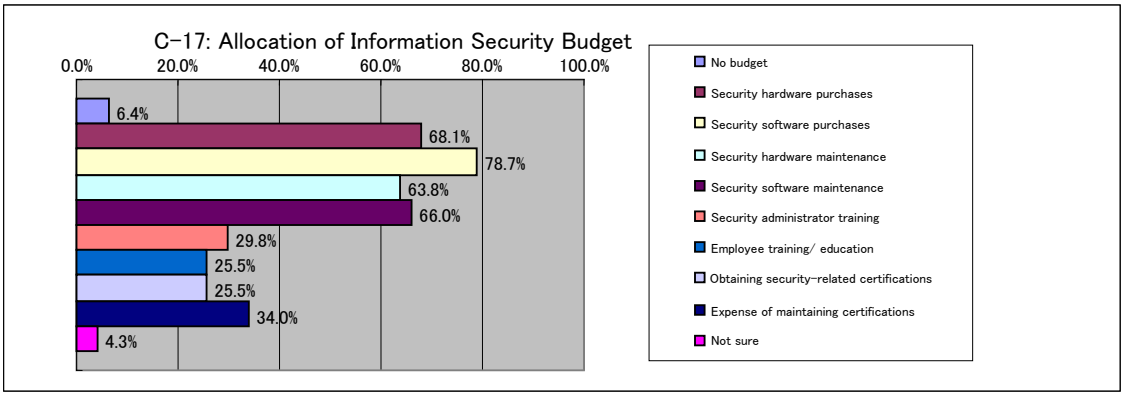


Note

Internet zone vulnerability testing was conducted approximately twice as much as any other manner of tests, indicating respondents' concern with, and determination to prevent, intrusion from outside their networks.

C-17 Allocation of information security budget. (Circle all that apply)

	Budget Allocation	No.	%
1	No budget	3	6.4%
2	Security hardware purchases	32	68.1%
3	Security software purchases	37	78.7%
4	Security hardware maintenance	30	63.8%
5	Security software maintenance	31	66.0%
6	Security administrator training	14	29.8%
7	Employee training/ education	12	25.5%
8	Obtaining security-related certifications	12	25.5%
9	Expense of maintaining certifications	16	34.0%
10	Not sure	2	4.3%

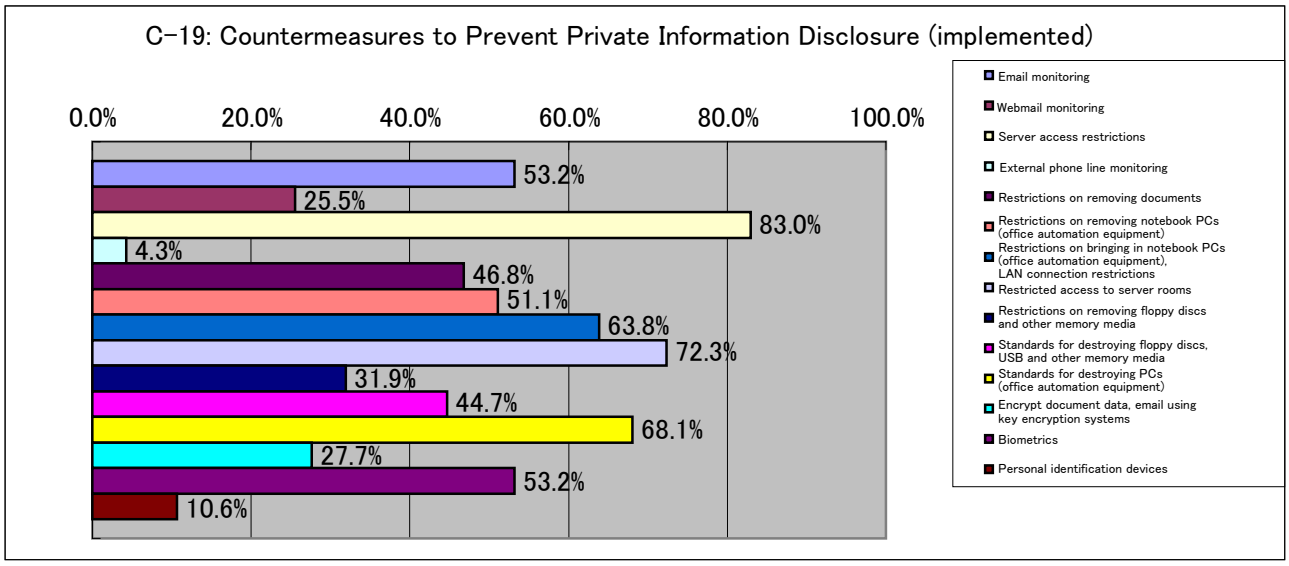


Note

Three respondents indicated their firm had no budget for information security. All other respondents indicated budgeting for hardware and software purchases, as well as hardware and software maintenance at approximately the same frequency.

C-19 Countermeasures used to prevent private information disclosure (implemented measures). (Circle all that apply)

	Countermeasures enacted	No.	%
1	Email monitoring	25	53.2%
2	Webmail monitoring	12	25.5%
3	Server access restrictions	39	83.0%
4	External phone line monitoring	2	4.3%
5	Restrictions on removing documents	22	46.8%
6	Restrictions on removing notebook PCs (office automation equipment)	24	51.1%
7	Restrictions on bringing in notebook PCs (office automation equipment), LAN connection restrictions	30	63.8%
8	Restricted access to server rooms	34	72.3%
9	Restrictions on removing floppy discs, USB and other memory media	15	31.9%
10	Standards for destroying floppy discs, USB and other memory media	21	44.7%
11	Standards for destroying PCs (office automation equipment)	32	68.1%
12	Encrypt document data, email using key encryption systems	13	27.7%
13	Biometrics	25	53.2%
14	Personal identification devices	5	10.6%



	Countermeasures Enacted (within the last 12 months)	No.	%
1	Email monitoring	4	8.5%
2	Webmail monitoring	2	4.3%
3	Server access restrictions	2	4.3%
4	External phone line monitoring	0	0.0%
5	Restrictions on removing documents	3	6.4%
6	Restrictions on removing notebook PCs (office automation equipment)	3	6.4%
7	Restrictions on bringing in notebook PCs (office automation equipment), LAN connection restrictions	4	8.5%
8	Restricted access to server rooms	2	4.3%
9	Restrictions on removing floppy discs, USB and other memory media	2	4.3%
10	Standards for destroying floppy discs, USB and other memory media	2	4.3%
11	Standards for destroying PCs (office automation equipment)	3	6.4%
12	Encrypt document data, email using key encryption systems	3	6.4%
13	Biometrics	2	4.3%
14	Personal identification devices	2	4.3%

	Countermeasures Enacted (after incident occurred)	No.	%
1	Email monitoring	0	0.0%
2	Webmail monitoring	0	0.0%
3	Server access restrictions	0	0.0%
4	External phone line monitoring	0	0.0%
5	Restrictions on removing documents	1	2.1%
6	Restrictions on removing notebook PCs (office automation equipment)	1	2.1%
7	Restrictions on bringing in notebook PCs (office automation equipment), LAN connection restrictions	0	0.0%
8	Restricted access to server rooms	0	0.0%
9	Restrictions on removing floppy discs, USB and other memory media	0	0.0%
10	Standards for destroying floppy discs, USB and other memory media	0	0.0%
11	Standards for destroying PCs (office automation equipment)	0	0.0%
12	Encrypt document data, email using key encryption systems	0	0.0%
13	Biometrics	0	0.0%
14	Personal identification devices	0	0.0%

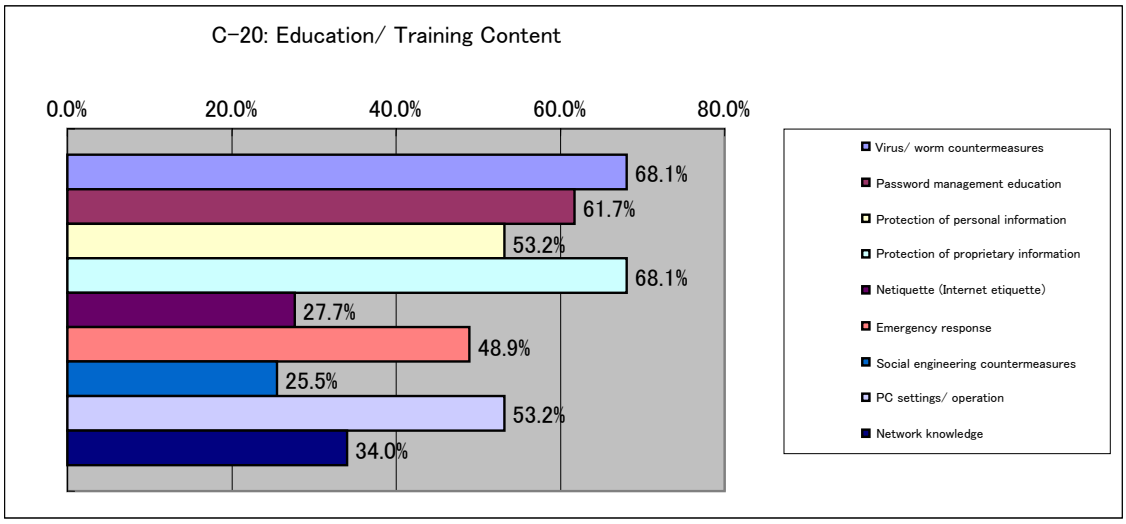
Note

According to the response to this question, most respondents are concerned with protecting server data, as

indicated by the most commonly enacted countermeasures, which are “Server access restrictions” and “restricted access to server rooms.” Coming in at the fourth most common measure, restrictions related to bringing in notebook PCs and LAN connections indicates respondents’ responses to new routes for viruses to enter a corporate network system.

C-20 Information security training/ education (Circle all that apply)

	Training/ Education Content	No.	%
1	Virus/ worm countermeasures	32	68.1%
2	Password management education	29	61.7%
3	Protection of personal information	25	53.2%
4	Protection of proprietary information	32	68.1%
5	"Netiquette" (Internet etiquette)	13	27.7%
6	Emergency response	23	48.9%
7	Social engineering countermeasures	12	25.5%
8	PC settings/ operation	25	53.2%
9	Network knowledge	16	34.0%



Note

Although only 20% or so of respondents answered that they have implemented "Netiquette" and "Social engineering countermeasures," all other responses were in the 50% range or higher, indicating that corporations are conducting comprehensive training and education for their personnel.

C-21 Ongoing information security education within the last 12 months (Circle all that apply)

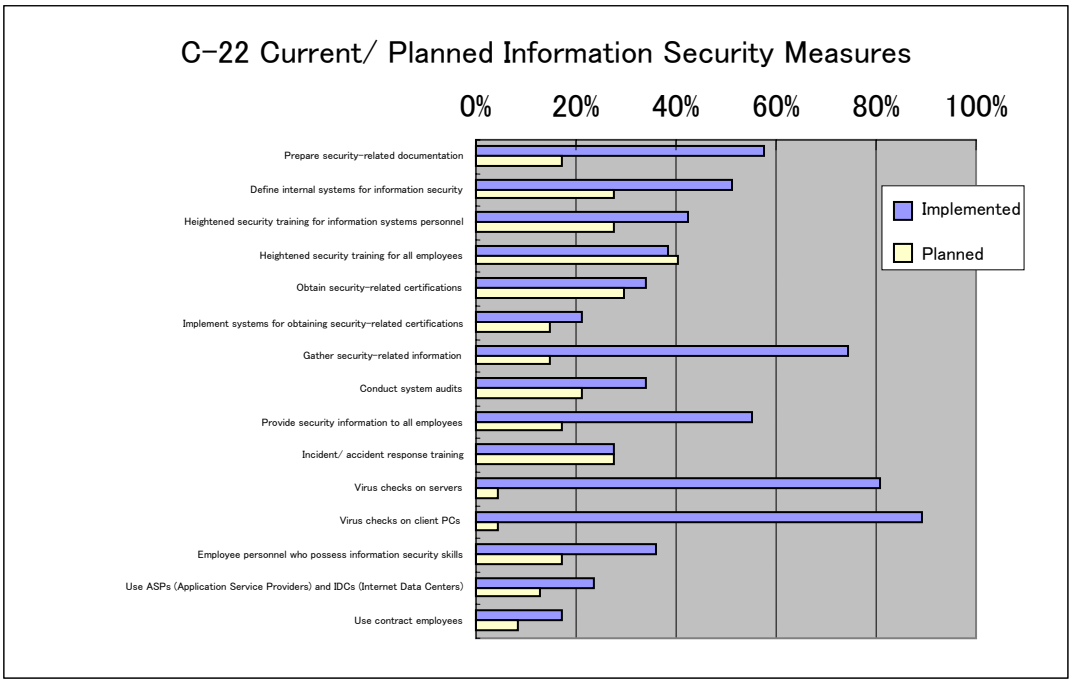
	Training/ Education Content	Avg. No. of People	Avg. Annual Frequency
1	Education for general employees (User training)	1,659	2
2	Management training	69	1
3	Specialist training	258	3

Note

The trend here indicates that specialists receive the most frequent number of training, followed by general employees and then management.

C-22　Current or planned information security measures (Mark all that apply)

	Measures	Implemented	%	Planned	%
1	Prepare security-related documentation	27	57.4%	8	17.0%
2	Define internal systems for information security	24	51.1%	13	27.7%
3	Heightened security training for information systems personnel	20	42.6%	13	27.7%
4	Heightened security training for general employees	18	38.3%	19	40.4%
5	Obtain security-related certifications	16	34.0%	14	29.8%
6	Implement systems for obtaining security-related certifications	10	21.3%	7	14.9%
7	Gather security-related information	35	74.5%	7	14.9%
8	Conduct system audits	16	34.0%	10	21.3%
9	Provide security information to all employees	26	55.3%	8	17.0%
10	Incident/ accident response training	13	27.7%	13	27.7%
11	Virus checks on servers	38	80.9%	2	4.3%
12	Virus checks on client PCs	42	89.4%	2	4.3%
13	Employ personnel who possess information security skills	17	36.2%	8	17.0%
14	Use ASPs (Application Service Providers) and IDCs (Internet Data Centers)	11	23.4%	6	12.8%
15	Use contract employees	8	17.0%	4	8.5%



Note

The only category in which "planned" exceeds "implemented" is that of "Heightened security training for general employees." "Incident/ accident response training" came in second with equal numbers of "planned" and

“implemented,” indicating that JNSA member corporations are rapidly moving toward completion of general information security measures.

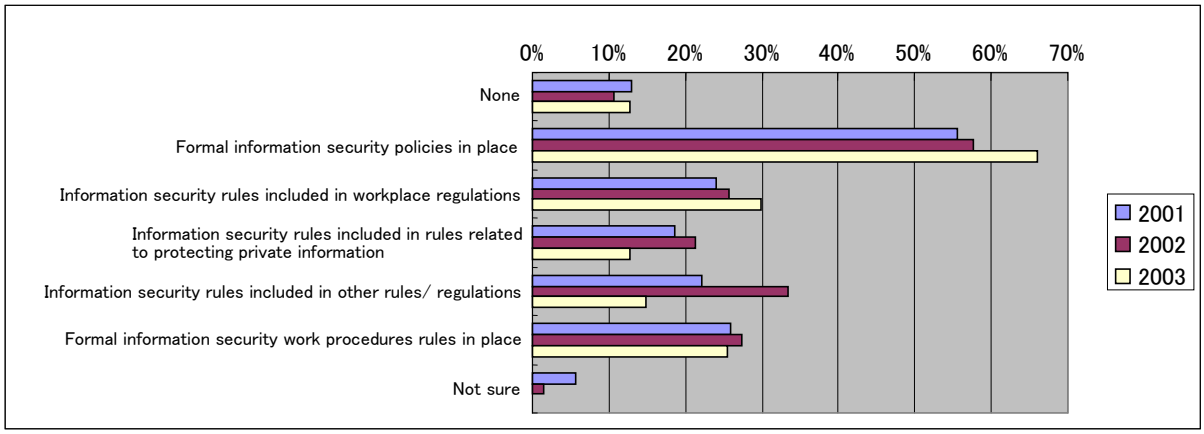
3.4.2 Comparison of this Year's Survey Results with those of the Previous Two Years

Being the third year of our information security incident survey, we have included herein a comparison of the results of this year's survey with those of the previous two years. In the previous two years, survey respondents consisted mainly of JNSA corporate members. For purposes of data comparison, we will use the 2003 survey responses provided by JNSA members (with a small number of non-JNSA member responses included).

C Please tell us about information security management at your company.

C-1 Does your company have formal information security rules? (Mark all that apply)

		2001		2002		2003	
1	None	7	13.0%	7	10.6%	6	12.8%
2	Formal information security policies in place	30	55.6%	38	57.6%	31	66.0%
3	Information security rules included in workplace regulations	13	24.1%	17	25.8%	14	29.8%
4	Information security rules included in rules related to protecting private information	10	18.5%	14	21.2%	6	12.8%
5	Information security rules included in other rules/ regulations	12	22.2%	22	33.3%	7	14.9%
6	Formal information security work procedures rules in place	14	25.9%	18	27.3%	12	25.5%
7	Not sure	3	5.6%	1	1.5%	0	0.0%

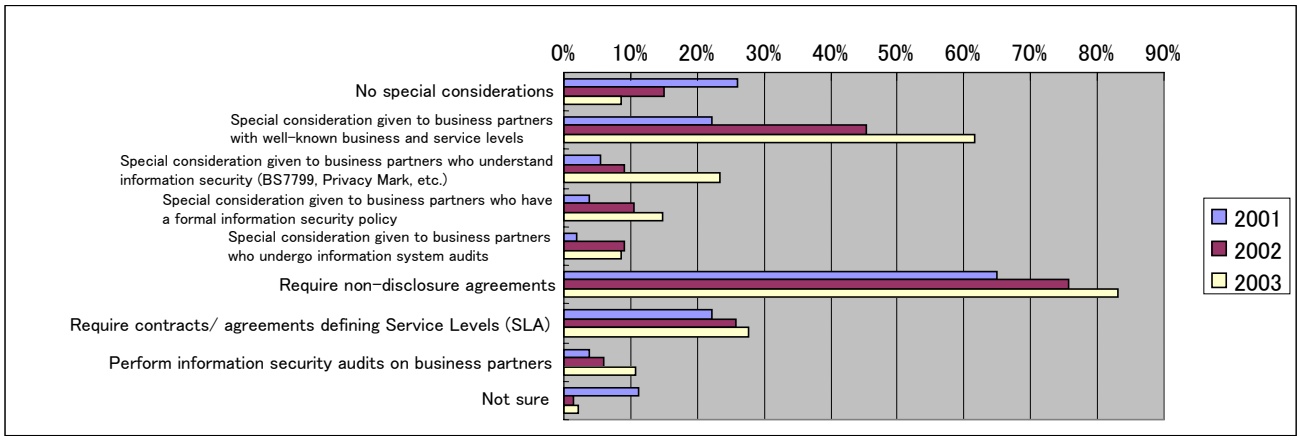


Note

The trend appears to be a noticeable increase in the establishment of formal information security rules and policies. The 2002 responses indicated a tendency for companies to incorporate information security rules as a subset of policies already in existence; however, the 2003 survey responses appear to indicate the increasing practice of establishing separate, formal information security rules.

C-5 Information security considerations when selecting or contracting with business partners. (Mark all that apply)

		2001		2002		2003	
1	No special considerations	14	25.9%	10	15.2%	4	8.5%
2	Special consideration given to business partners with well-known business and service levels	12	22.2%	30	45.5%	29	61.7%
3	Special consideration given to business partners who obtained certification related to information security (BS7799, Privacy Mark, etc.)	3	5.6%	6	9.1%	11	23.4%
4	Special consideration given to business partners who have a formal information security policy	2	3.7%	7	10.6%	7	14.9%
5	Special consideration given to business partners who undergo information system audits	1	1.9%	6	9.1%	4	8.5%
6	Require non-disclosure agreements	35	64.8%	50	75.8%	39	83.0%
7	Require contracts/ agreements defining Service Levels (SLA)	12	22.2%	17	25.8%	13	27.7%
8	Perform information security audits on business partners	2	3.7%	4	6.1%	5	10.6%
9	Not sure	6	11.1%	1	1.5%	1	2.1%

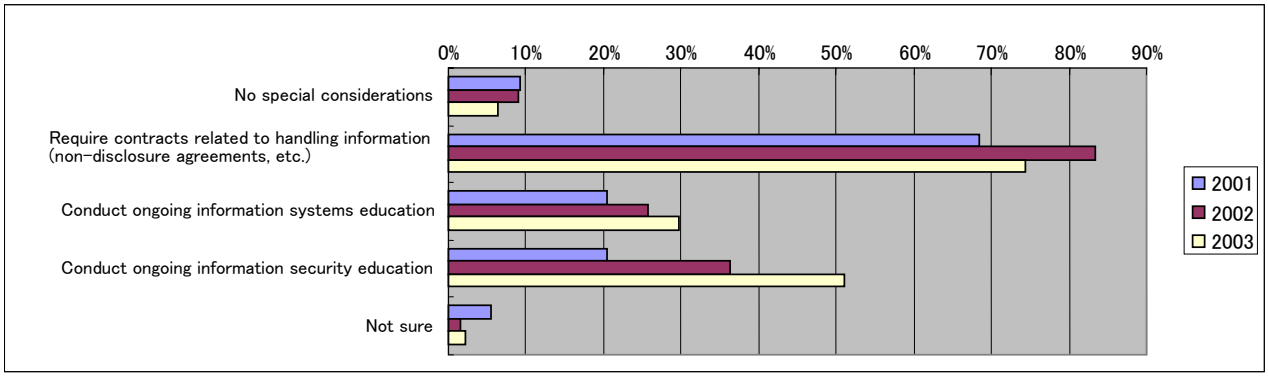


Note

The response, "No special considerations" shows a decrease, while the other question categories show significant increases. Another notable factor is that while only 23% of respondents in the 2003 survey said they give special consideration to business partners who have obtained certifications, this represents a two-fold increase over the prior year.

C-6 Information security considerations when accepting contract or full-time engineers/operators. (Circle all that apply)

		2001		2002		2003	
1	No special considerations	5	9.3%	6	9.1%	3	6.4%
2	Require contracts related to handling information (non-disclosure agreements, etc.)	37	68.5%	55	83.3%	35	74.5%
3	Conduct ongoing information systems education	11	20.4%	17	25.8%	14	29.8%
4	Conduct ongoing information security education	11	20.4%	24	36.4%	24	51.1%
5	Not sure	3	5.6%	1	1.5%	1	2.1%

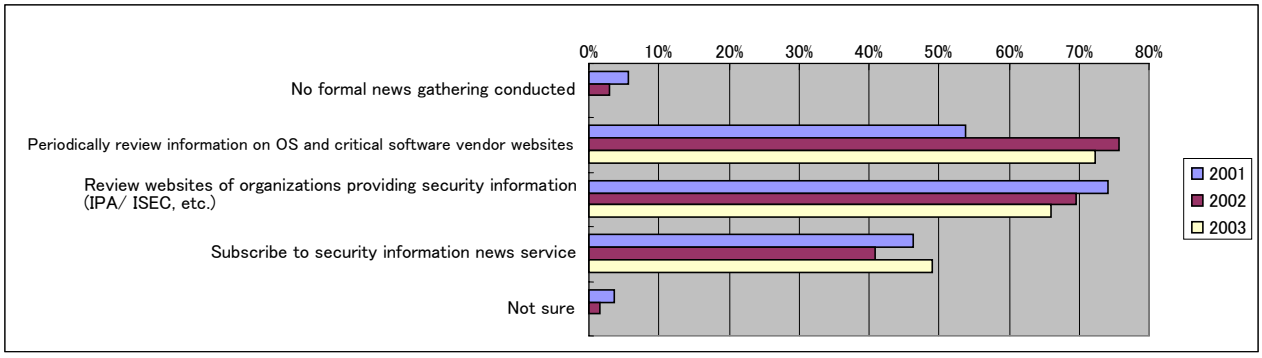


Note

The rate of information systems education/ information security education shows a continuing increase over the past three years. Of particular note is the increase in respondents who have implemented information security education, beginning at 20% for 2001 and rising to 51% for 2003. This effectively communicates the fact that corporations are spending resources on educating part-time and contract workers as well as their full-time employees.

C-8 How do you gather information security-related news? (Mark all that apply)

		2001		2002		2003	
1	No formal news gathering conducted	3	5.6%	2	3.0%	0	0.0%
2	Periodically review security-related information on OS and critical software vendor websites	29	53.7%	50	75.8%	34	72.3%
3	Review websites of organizations providing security information (IPA/ ISEC, etc.)	40	74.1%	46	69.7%	31	66.0%
4	Subscribe to security information news service	25	46.3%	27	40.9%	23	48.9%
5	Not sure	2	3.7%	1	1.5%	0	0.0%

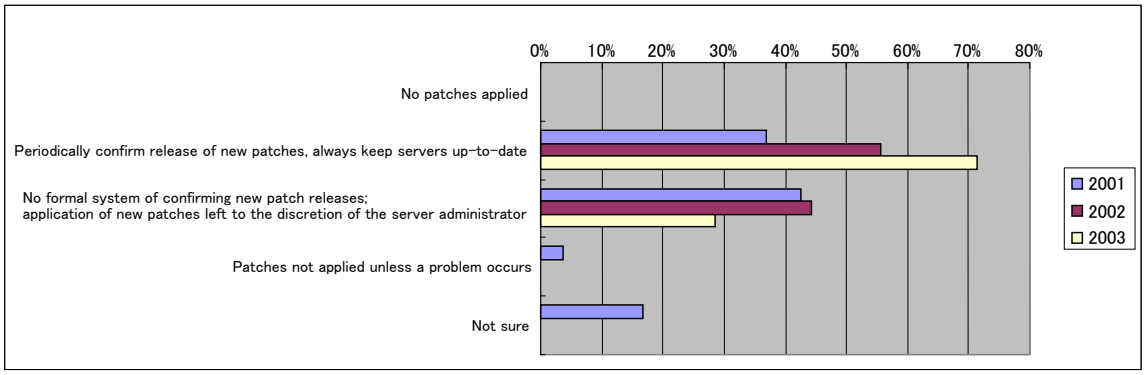


Note

For the 2003 survey, all respondents indicated they performed some type of information security news gathering; however, the overall breakdown of methods employed show no marked change from year to year.

C-9 Application of patches to ensure network server security (Select one)

		2001		2002		2003 年	
1	No patches applied	0	0.0%	0	0.0%	0	0.0%
2	Periodically confirm release of new patches, always keep servers up-to-date	20	37.0%	34	55.7%	30	71.4%
3	No formal system of confirming new patch releases; application of new patches left to the discretion of the server administrator	23	42.6%	27	44.3%	12	28.6%
4	Patches not applied unless a problem occurs	2	3.7%	0	0.0%	0	0.0%
5	Not sure	9	16.7%	0	0.0%	0	0.0%



Note

We see a significant change in trends related to the application of network server patches. Those companies

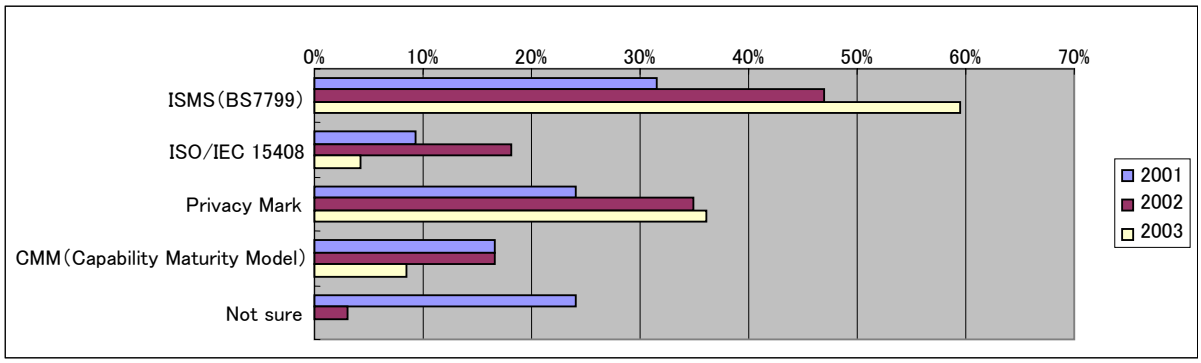
responding that they keep their servers up to date with the latest patches have increased two-fold since the 2001 survey.

C-10　Indicate whether certification is "In Planning" or "Already Obtained."　Circle the status that applies.

2001					
	Name	In Planning	%	Already Obtained	%
1	ISMS（BS7799）	14	25.9%	3	5.6%
2	ISO/IEC 15408	5	9.3%	0	0.0%
3	Privacy Mark	4	7.4%	9	16.7%
4	CMM（Capability Maturity Model）	8	14.8%	1	1.9%
5	Not sure	13	24.1%	0	0.0%

2002					
	Name	In Planning	%	Already Obtained	%
1	ISMS（BS7799）	21	31.8%	10	15.2%
2	ISO/IEC 15408	7	10.6%	5	7.6%
3	Privacy Mark	11	16.7%	12	18.2%
4	CMM（Capability Maturity Model）	9	13.6%	2	3.0%
5	Not sure	1	1.5%	1	1.5%

2003					
	Name	In Planning	%	Already Obtained	%
1	ISMS（BS7799）	12	25.5%	16	34.0%
2	ISO/IEC 15408	1	2.1%	1	2.1%
3	Privacy Mark	9	19.1%	8	17.0%
4	CMM（Capability Maturity Model）	1	2.1%	3	6.4%
5	Not sure	0	0.0%	0	0.0%



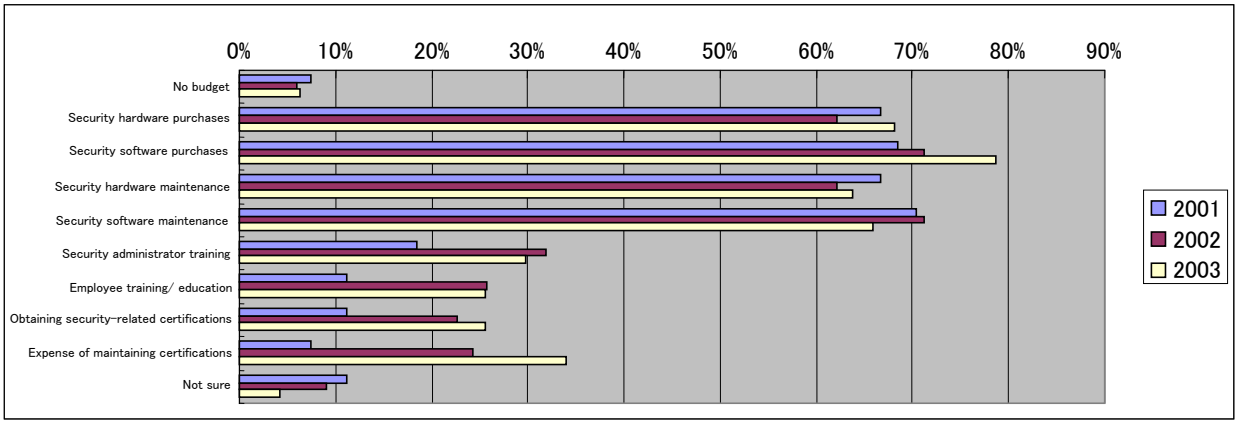
Note

The graph above compares certifications already obtained by respondents versus those that respondents are planning to obtain. The year-by-year trend shows an increase in ISMS and Privacy Mark certifications. The nearly 60% response rate for ISMS certification in 2003 is probably more a characteristic of the survey

respondents mainly consisting of JNSA member corporations.

C-14 Allocation of information security budget. (Circle all that apply)

		2001		2002		2003	
1	No budget	4	7.4%	4	6.1%	3	6.4%
2	Security hardware purchases	36	66.7%	41	62.1%	32	68.1%
3	Security software purchases	37	68.5%	47	71.2%	37	78.7%
4	Security hardware maintenance	36	66.7%	41	62.1%	30	63.8%
5	Security software maintenance	38	70.4%	47	71.2%	31	66.0%
6	Security administrator training	10	18.5%	21	31.8%	14	29.8%
7	Employee training/ education	6	11.1%	17	25.8%	12	25.5%
8	Obtaining security-related certifications	6	11.1%	15	22.7%	12	25.5%
9	Expense of maintaining certifications	4	7.4%	16	24.2%	16	34.0%
10	Not sure	6	11.1%	6	9.1%	2	4.3%

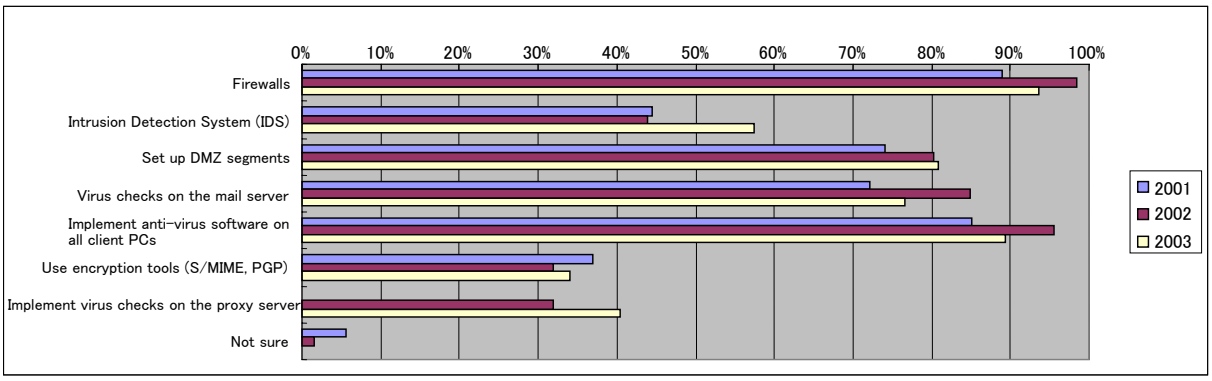


Note

We see an increase in spending on certification/ authorization over the past three years; however, the other categories do not show any marked changes.

C-15 What systems have you implemented to insure information security? (Circle all that apply)

		2001		2002		2003	
1	Firewalls	48	88.9%	65	98.5%	44	93.6%
2	Intrusion Detection System (IDS)	24	44.4%	29	43.9%	27	57.4%
3	Set up DMZ segments	40	74.1%	53	80.3%	38	80.9%
4	Virus checks on the mail server	39	72.2%	56	84.8%	36	76.6%
5	Implement anti-virus software on all client PCs	46	85.2%	63	95.5%	42	89.4%
6	Use encryption tools (S/MIME, PGP)	20	37.0%	21	31.8%	16	34.0%
7	Implement virus checks on the proxy server	-	-	21	31.8%	19	40.4%
8	Not sure	3	5.6%	1	1.5%	0	0.0%



Note

We do not see any significant changes in the selection of technological countermeasures employed. The use of Intrusion Detection System (IDS) technology increased compared to 2002.

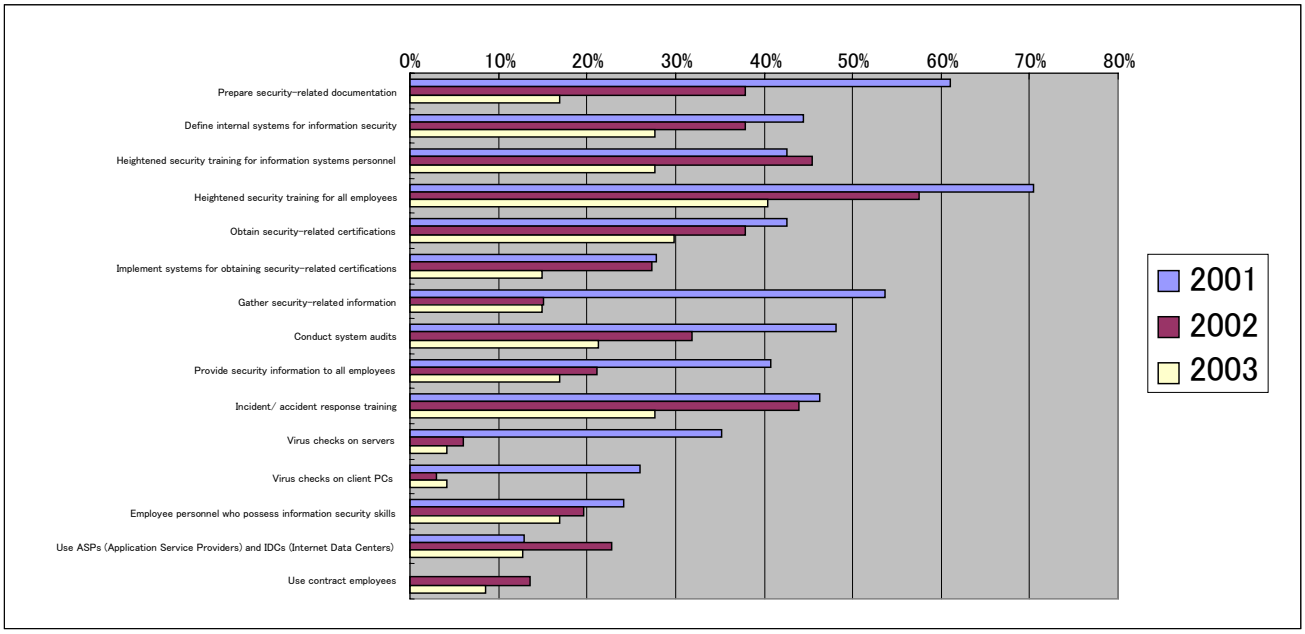
C-19 Current or planned information security measures (Mark all that apply)

2001			
		Future	%
1	Prepare security-related documentation	33	61.1%
2	Define internal systems for information security	24	44.4%
3	Heightened security training for information systems personnel	23	42.6%
4	Heightened security training for general employees	38	70.4%
5	Obtain security-related certifications	23	42.6%
6	Implement systems for obtaining security-related certifications	15	27.8%
7	Gather security-related information	29	53.7%
8	Conduct system audits	26	48.1%
9	Provide security information to all employees	22	40.7%
10	Incident/ accident response training	25	46.3%
11	Virus checks on servers	19	35.2%
12	Virus checks on client PCs	14	25.9%
13	Employ personnel who possess information security skills	13	24.1%
14	Use ASPs (Application Service Providers) and IDCs (Internet Data Centers)	7	13.0%
15	Use contract employees	0	0.0%

2002					
		Already Implemented	%	Future	%
1	Prepare security-related documentation	27	40.9%	25	37.9%
2	Define internal systems for information security	26	39.4%	25	37.9%
3	Heightened security training for information systems personnel	21	31.8%	30	45.5%
4	Heightened security training for general employees	21	31.8%	38	57.6%
5	Obtain security-related certifications	12	18.2%	25	37.9%
6	Implement systems for obtaining security-related certifications	5	7.6%	18	27.3%
7	Gather security-related information	44	66.7%	10	15.2%
8	Conduct system audits	20	30.3%	21	31.8%
9	Provide security information to all employees	38	57.6%	14	21.2%
10	Incident/ accident response training	9	13.6%	29	43.9%
11	Virus checks on servers	56	84.8%	4	6.1%
12	Virus checks on client PCs	60	90.9%	2	3.0%
13	Employ personnel who possess information security skills	20	30.3%	13	19.7%
14	Use ASPs (Application Service Providers) and IDCs (Internet Data Centers)	14	21.2%	15	22.7%
15	Use contract employees	6	9.1%	9	13.6%

2003					
		Already Implemented	%	Future	%
1	Prepare security-related documentation	27	57.4%	8	17.0%
2	Define internal systems for information security	24	51.1%	13	27.7%
3	Heightened security training for information systems personnel	20	42.6%	13	27.7%
4	Heightened security training for general employees	18	38.3%	19	40.4%

5	Obtain security-related certifications	16	34.0%	14	29.8%
6	Implement systems for obtaining security-related certifications	10	21.3%	7	14.9%
7	Gather security-related information	35	74.5%	7	14.9%
8	Conduct system audits	16	34.0%	10	21.3%
9	Provide security information to all employees	26	55.3%	8	17.0%
10	Incident/ accident response training	13	27.7%	13	27.7%
11	Virus checks on servers	38	80.9%	2	4.3%
12	Virus checks on client PCs	42	89.4%	2	4.3%
13	Employ personnel who possess information security skills	17	36.2%	8	17.0%
14	Use ASPs (Application Service Providers) and IDCs (Internet Data Centers)	11	23.4%	6	12.8%
15	Use contract employees	8	17.0%	4	8.5%



Note

The graph above shows a comparison of measures planned for the future. In the 2001, three different categories had more than a 50% response rate; however, in 2003 the most common answer only had a 40% response rate. This graph shows how respondents have been working (and continue to work) to enhance their information security measures.

3.4.3 Overview of Damages Incurred

Respondents to the 2003 Information Security Incident Survey indicated a total of 113 incidents among them. A breakdown of incident by industry type reveals 59 incidents for the manufacturing industry, more than 50% of the total, and representing the single industry experiencing the most incidents. Analyzing the incidents by type shows that MS Blaster accounted for 69 cases, or 60% of the total.

The chart that follows shows only the total financial amounts of Direct Damages, Indirect Damages, and Latent Damages incurred. We also show examples of our methodology in calculating incident damages. (NOTE: As shown in Section 6, there are other factors considered in calculating incident damages; however, we have omitted these due to the inability to obtain sufficient information from this survey.)

Example 1) Calculation example for No. 14 Direct and Latent Damage Amounts

● Direct Damages consist of A+B, or ¥1,160,445.

System Sales per Hour×Projected Profit Ratio×Down Time ＝ Lost Profits

A. Annual Sales: ¥240,000,000÷365 days÷24 hours×Projected Profit Ratio of 20%×Down Time of 27 hours＝ ¥147,945

Days of Down Time×No. of employees engaged in system recovery×Payroll per Employee ＝ Cost of System Recovery

B. Down Time of 27 hours ÷8 hours×20 employees×¥15,000 payroll per employee＝ ¥1,012,500

●Latent Damages were ¥6,075,000.

Payroll per Employee×No. of employees affected by incident ×Degree of IT reliance (work activity reliance on IT)×No. of down days ＝ Latent Damages

¥15,000 payroll per employee×No. of employees affected of 600 ×Degree of IT reliance 0.2×Down Time of 27 hours÷8 hours＝ ¥6,075,000

Example 2) Calculation example for No. 34 Direct and Indirect Damage Amounts

●Direct Damages amounted to ¥2,250,000.

Days of Down Time×No. of employees engaged in system recovery×Payroll per Employee ＝ Cost of System Recovery

Down Time of 24 hours÷8 hours×25 employees×¥30,000 payroll per employee＝ ¥2,250,000

●Indirect Damages amounted to ¥3,000,000.

Reparations, Compensation and Public Apologies ＝ Indirect Damages

Reparations, compensation amounted to ¥3,000,000＝¥3,000,000

① Incident Damages (Damages per Incident)

No.	Industry Type	Direct Damages	Indirect Damages	Latent Damages	Total Damages	Incident Type	Comments
1	Manufacturing	450,000	0	54,000	504,000	MS Blaster	*1
2	Manufacturing	0	0	0	0	MS Blaster	*3
3	Manufacturing	1,300,000	0	3,200,000	4,500,000	MS Blaster	
4	Manufacturing	1,350,000	0	3,150,000	4,500,000	MS Blaster	*1
5	Manufacturing	4,500,000	0	0	4,500,000	MS Blaster	*1
6	Manufacturing	4,500,000	0	0	4,500,000	MS Blaster	*1
7	Manufacturing	140,000	0	1,400,000	1,540,000	MS Blaster	
8	Manufacturing	3,600,000	0	600,000	4,200,000	MS BlasterR	
9	Manufacturing	1,800,000	0	1,800,000	3,600,000	MS Blaster	
10	Other Services	1,575,000	0	31,500,000	33,075,000	Other Virus	Nachi*4
11	Other Services	0	0	0	0	MS Blaster	*3
12	Finance (Banking, Insurance, Securities, etc.)	13,500,000	0	3,780,000	17,280,000	MS Blaster	*1
13	Construction	2,350,000	0	30,000,000	32,350,000	MS Blaster	
14	Manufacturing	1,160,445	0	6,075,000	7,235,445	MS Blaster	
15	Finance (Banking, Insurance, Securities, etc.)	0	0	0	0	KLEZ	*3
16	Finance (Banking, Insurance, Securities, etc.)	0	0	0	0	SOBIG	*3
17	Finance (Banking, Insurance, Securities, etc.)	0	0	0	0	BUGBEAR	*3
18	Medical/ Pharmaceutical	0	0	30,000,000	30,000,000	MS Blaster	*1
19	Construction	37,500	0	0	37,500	Sircam	
20	Manufacturing	8,000,000	0	7,500,000	15,500,000	MS Blaster	
21	Manufacturing	0	0	0	0	MS Blaster	*3
22	Manufacturing	3,750	0	0	3,750	MS Blaster	
23	Manufacturing	112,500	0	225,000	337,500	MS Blaster	*1
24	Manufacturing	3,750	0	0	3,750	DoS (Denial of Service) attack	
25	Manufacturing	600,000	0	0	600,000	MS Blaster	
26	Manufacturing	56,250	0	0	56,250	MS Blaster	*1
27	Manufacturing	951,000	0	0	951,000	MS Blaster	
28	Manufacturing	0	0	0	0	BUGBEAR	*2
29	Manufacturing	15,000	0	6,750,000	6,765,000	MS Blaster	*1
30	Construction	112,500	0	225,000	337,500	KLEZ	*1
31	Manufacturing	900,000	0	75,000	975,000	Other virus incident	*1
32	Manufacturing	3,000,000	0	0	3,000,000	MS Blaster	
33	Other Services	200,000	0	0	200,000	DoS (Denial of Service) attack	
34	Manufacturing	2,250,000	3,000,000	0	5,250,000	KLEZ	
35	Manufacturing	75,000	0	0	75,000	Other virus incident	
36	Finance (Banking, Insurance, Securities, etc.)	45,000	0	0	45,000	Other virus incident	
37	Finance (Banking, Insurance, Securities, etc.)	0	0	0	0	PC/ PDA theft/ loss	*2
38	Manufacturing	93,750	0	62,500	156,250	MS Blaster	

No.	Industry Type	Direct Damages	Indirect Damages	Latent Damages	Total Damages	Incident Type	Comments	
39	Manufacturing	1,125,000	0	2,700,000	3,825,000	MS Blaster		
40	Manufacturing	15,500,000	0	14,000,000	29,500,000	MS Blaster		
41	Manufacturing	0	0	0	0	SOBIG	*2	
42	Medical/ Pharmaceutical	0	0	20,000,000	20,000,000	MS Blaster		
43	Manufacturing	90,000	0	0	90,000	MS Blaster	*1	
44	Other	3,600,000	0	0	3,600,000	MS Blaster	*1	
45	Manufacturing	20,000	0	0	20,000	MS Blaster		
46	Manufacturing	0	0	0	0	BUGBEAR	*2	
47	Manufacturing	0	0	0	0	KLEZ	*2	
48	Manufacturing	0	0	0	0	MS Blaster	*3	
49	Manufacturing	156,250	0	3,125,000	3,281,250	MS Blaster		
50	Manufacturing	37,500	0	125,000	162,500	Other virus incident		Nachi*4
51	Construction	2,940,000	0	0	2,940,000	MS Blaster		
52	Manufacturing	361,250	0	2,250,000	2,611,250	MS Blaster		
53	Manufacturing	0	0	0	0	MS Blaster	*2	
54	Manufacturing	18,750	0	75,000	93,750	MS Blaster	*1	
55	Manufacturing	45,000	0	6,000	51,000	Other virus incident	*1	
56	Other Services	1,350,000	0	218,750	1,568,750	MS Blaster		
57	Manufacturing	7,600,000	0	0	7,600,000	SOBIG		
58	Manufacturing	1,080,000	0	0	1,080,000	Other virus incident	*1	Nachi*4
59	Manufacturing	4,500,000	0	600,000	5,100,000	MS Blaster	*1	
60	Other	0	0	0	0	BUGBEAR	*2	
61	Manufacturing	1,500,000	0	0	1,500,000	MS Blaster		
62	Manufacturing	10,000,000	0	7,500,000	17,500,000	MS Blaster	*1	
63	Construction	0	0	37,500	37,500	KLEZ	*1	
64	Manufacturing	37,500,000	0	225,000,000	262,500,000	MS Blaster		
65	Construction	0	0	0	0	KLEZ	*3	
66	Construction	0	0	0	0	MS Blaster		
67	Manufacturing	26,250	0	0	26,250	MS Blaster		
68	Information/ Communications	180,000	0	0	180,000	MS Blaster		
69	Manufacturing	1,350,000	0	36,000,000	37,350,000	MS Blaster	*1	
70	Finance (Banking, Insurance, Securities, etc.)	28,125	0	0	28,125	Unauthorized alteration of corporate public website		
71	Manufacturing	0	0	0	0	MS Blaster	*3	
72	Medical/ Pharmaceutical	13,200,000	0	0	13,200,000	MS Blaster		
73	Energy	37,500,000	0	0	37,500,000	MS Blaster		
74	Manufacturing	0	0	18,750,000	18,750,000	MS Blaster	*2	
75	Information/ Communications	72,000,000	0	0	72,000,000	MS Blaster		
76	Construction	0	0	0	0	MS BlasterR	*2	
77	Manufacturing	11,600,000	0	0	11,600,000	Other virus incident	*1	Slammer*4
78	Manufacturing	45,500,000	0	0	45,500,000	MS Blaster	*1	
79	Transportation	3,899,363	0	18,900,000	22,799,363	Other virus incident		Welchia*4
80	Medical/ Pharmaceutical	0	0	81,000,000	81,000,000	MS Blaster	*1	
81	Manufacturing	0	0	0	0	MS Blaster	*3	
82	Construction	7,800,000	0	5,250,000	13,050,000	MS Blaster		

No.	Industry Type	Direct Damages	Indirect Damages	Latent Damages	Total Damages	Incident Type		Comments
83	Finance (Banking, Insurance, Securities, etc.)	30,000	0	6,000	36,000	MS Blaster	*1	
84	Finance (Banking, Insurance, Securities, etc.)	30,000	0	6,000	36,000	Other virus incident	*1	
85	Finance (Banking, Insurance, Securities, etc.)	15,000	0	3,000	18,000	Other virus incident	*1	
86	Finance (Banking, Insurance, Securities, etc.)	30,000	0	6,000	36,000	Other virus incident	*1	
87	Manufacturing	24,010,000	0	12,148,000	36,158,000	MS Blaster		
88	Manufacturing	30,000	0	150,000	180,000	Other virus incident	*1	Opaserv*4
89	Manufacturing	15,000	0	0	15,000	MS Blaster	*1	
90	Food Service/ Retail	0	0	1,125,000	1,125,000	MS Blaster	*1	
91	Manufacturing	900,000	0	1,800,000	2,700,000	MS Blaster		
92	Information/ Communications	1,350,000	0	2,160,000	3,510,000	MS Blaster		
93	Finance (Banking, Insurance, Securities, etc.)	41,250	0	0	41,250	Other virus incident	*1	
94	Manufacturing	900,000	0	3,000,000	3,900,000	MS Blaster		
95	Information/ Communications	5,625	0	187,500	193,125	MS Blaster		
96	Other Services	0	0	0	0	MS Blaster	*2	
97	Other Services	0	0	150,000	150,000	Other virus incident	*1	
98	Other	0	0	0	0	Other virus incident	*2	
99	Information/ Communications	37,500	0	0	37,500	Other virus incident	*1	Welchia*4
100	Information/ Communications	3,750	0	0	3,750	Information disclosure		
101	Information/ Communications	0	0	0	0	PC/ PDA theft/ loss	*2	
102	Manufacturing	0	0	0	0	BUGBEAR	*2	
103	Manufacturing	0	0	0	0	PC/ PDA theft/ loss	*3	
104	Information/ Communications	28,800,000	0	0	28,800,000	MS Blaster		
105	Information/ Communications	225,000	0	22,500	247,500	Other virus incident		Nachi,Welchia *4
106	Information/ Communications	201,875,000	0	0	201,875,000	KLEZ		
107	Finance (Banking, Insurance, Securities, etc.)	30,000	0	0	30,000	BUGBEAR	*1	
108	Other Services	1,200,000	0	0	1,200,000	Information disclosure		
109	Information/ Communications	5,400,000	0	0	5,400,000	Information disclosure		
110	Information/ Communications	1,350,000	0	0	1,350,000	MS Blaster		
111	Education/ Mass Media	45,000	0	157,500	202,500	MS Blaster	*1	
112	Information/ Communications	1,350,000	0	0	1,350,000	MS Blaster	*1	
113	Other Services	22,500	0	0	22,500	MS Blaster	*4	
	Total	600,884,558	3,000,000	582,855,250	1,186,739,808			

■ Calculation Assumptions

・For Direct Damages (payroll expenses) we conducted a trial calculation: (Down time/ 8 hours) x (No. of employees engaged in system recovery) x (payroll per employee per day).

・For Indirect Damages (payroll expenses) we conducted a trial calculation: (system down time/ 8 hours) x (no. of employees affected) x (payroll per employee per day) x (degree of IT reliance)

・We used an assumed degree of IT reliance (effect of system down time on work activities) of 0.2 for our calculations.

・Since a standard work day for most companies is eight hours, we divided the number of hours of system down time by 8 to calculate the number of system down days.

■ Notes

*1 Payroll expenses were not available; we used an assumed ¥30,000 per employee per day for our calculations.

*2 Although the respondent provided the number of employees affected by the incident, they did not provide the number of work hours lost; therefore, we did not perform a calculation for incident damages.

*3 The respondent did not provide the number of employees engaged in system recovery, nor the number of employee hours required; therefore, we assumed that no actual damages were incurred.

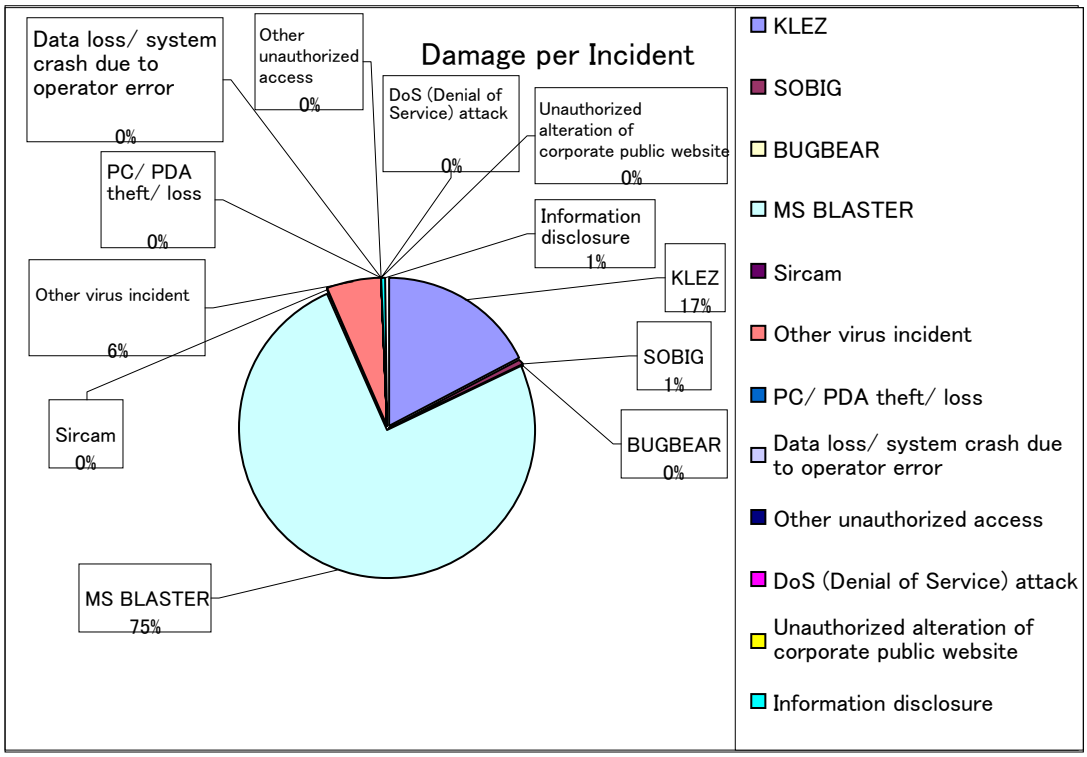
*4 Virus name inferred according to comments as to the nature of damages incurred.

Note

Two incidents reported caused more than ¥200 million in calculated damages. There were also two incidents affecting more than 10,000 employees (not shown in this chart). This chart reveals an increase in virus-related damages for 2003.

② Damage by Incident

	Incident Type	Damages	No.	Avg. Damage	%
1	KLEZ	207,500,000	7	29,642,857	17.5%
2	SOBIG	7,600,000	3	2,533,333	0.6%
3	BUGBEAR	30,000	6	5,000	0.0%
4	MS Blaster	894,127,570	69	12,958,371	75.3%
5	Sircam	37,500	1	37,500	0.0%
6	Other virus incident	70,609,113	18	3,922,729	5.9%
7	PC/ PDA theft/ loss	0	3	0	0.0%
8	Data loss/ system crash due to operator error	0	0	0	0.0%
9	Other unauthorized access	0	0	0	0.0%
10	DoS (Denial of Service) attack	203,750	2	101,875	0.0%
11	Unauthorized alteration of corporate public website	28,125	1	28,125	0.0%
12	Information disclosure	6,603,750	3	2,201,250	0.6%



Note

MS Blaster accounted for 75% of all incidents, and was the greatest menace during 2003. KLEZ accounted for the most in damages per incident, averaging ¥29.64 million per incident, according to our survey, although this figure is somewhat skewed since one KLEZ incident caused more than ¥200 million in damages.

③ Incident Damages by Industry Type

	Industry Type	Damages	No.	Avg. Damages
1	Finance (Banking, Insurance, Securities, etc.)	17,550,375	13	1,350,029
2	Medical/ Pharmaceutical	144,200,000	4	36,050,000
3	Transportation	22,799,363	1	22,799,363
4	Energy	37,500,000	1	37,500,000
5	Information/ Communications	314,946,875	13	24,226,683
6	Manufacturing	559,846,945	59	9,488,931
7	Education/ Mass Media	202,500	1	202,500
8	Construction	48,752,500	9	5,416,944
9	Food Service/ Retail	1,125,000	1	1,125,000
10	Other Services	36,216,250	8	4,527,031
11	Other	3,600,000	3	1,200,000

Note

According to our survey, the manufacturing industry incurred the greatest amount of incident-related damages. However, given that this industry represents a significant number of questionnaire respondents, one cannot simply conclude that manufacturers are more susceptible to damage than companies in other industries. Rather, we wish to stress the fact that all companies are susceptible to information security incidents, regardless of industry affiliation.

3.5 Estimate of Total Damages Caused by Computer Viruses in Japan

With the help of RISTEX, we were able to extend the scope of our 2003 survey to include respondents from a representative variety of businesses and industries. As a result, we believe we have been able to calculate a reasonable estimate of damages caused by computer viruses in Japan. Accordingly, the following outlines our calculation methodology and assumptions for estimating overall virus damages in Japan during 2003, which are built on the result of the survey.

3.5.1 Basic Numbers Referenced

We used the following statistics from "Ministry of Finance, Statistics Bureau, Volume 2001" as basic numerical values to build our estimate of virus-related damages in Japan based on the results of the questionnaire.
http://www.stat.go.jp/data/jigyou/kakuhou/01.htm

No.	Statistics Category	Figure	Comments
1	Number of Companies	1.618 million	Stock Companies, Limited Private Companies, Limited Partnerships, Joint-stock limited Partnerships, and Mutual Companies
2	Total Locations	6.35 million	Does not include locations with indeterminate business activities.
3	Employees	60.158 million	Does not include locations with indeterminate business activities.

These figures are several percentage points lower than the statistics gathered for 1996. We believe the figures provide satisfactory accuracy to support our estimates as basic numerical values.

We used figures from "Survey of Measures to Respond to Unauthorized Computer Access" (National Police Agency, 2004) as a basis for determining the state of computer virus infections at Japanese firms.
http://www.npa.go.jp/cyber/chousa/H16countermeasures.pdf

No.	Statistics Category	Figure	Comments
1	Ratio of companies infected with computer viruses	６１．４％	Survey conducted for publicly traded companies

3.5.2 Estimate of Damages

Pattern 1　Estimate based on "Number of Companies"

Estimate of Damage per Company	=	Total Damages	÷	No. of Companies affected
¥11.2 million		¥1.18674 billion		106

Total Virus-Related Damages across Japan	=	No. of Companies	×	Ratio of Companies Infected with Computer Viruses	×	Damage per Company
¥4.37 trillion		1.618 million		61.4%		¥11.2 million

Note

Small- and mid-sized firms are included in the total number of companies in Japan (Ministry of Finance figure). As the subjects of the present survey are mainly publicly traded corporations, the figure used here lacks somewhat in precision.

Accordingly, we will provide a calculation here based on firms listed on Japanese stock exchanges. As some companies are listed on more than one exchange, we will use a total number of 5,000 to represent the unique number of publicly traded firms in Japan.

Sapporo Securities Exchange	102
Tokyo Stock Exchange	2,255
Nagoya Stock Exchange	414
Osaka Securities Exchange	1,114
Fukuoka Stock Exchange	164
JASDAQ	924
Hercules	103
Total	5,076

Virus-Related Damages among Public Companies	=	Number of Listed Companies	×	Ratio of Companies Infected with Computer Viruses	×	Damage per Company
¥34.3 billion		5,000		61.4%		¥11.2 million

Pattern 2 Estimate based on "Total Number of Locations"

A survey of locations affected by viruses was not conducted; therefore, we will base our estimate on the total number of locations.

Damage per Location	=	Total Damages	÷	Total no. of locations from valid responses ※
¥61.674 thousand		¥1.18674 billion		19,242 locations

※ The number of locations has been calculated as an average, since the response to the questionnaire question was a range, rather than an exact number.

Total Virus-Related Damages across Japan	=	Total number of domestic locations	×	Damages per location
¥39.2 billion		6.35 million		¥61,674

Note

This value is almost identical to the calculated in Pattern one using damages incurred by listed companies. Accordingly, we see no errors in the calculation methodologies used. We believe these results were derived mainly due to the fact that the present survey did not take totals for incident-related damages on a per-location basis.

According to statistics provided by the Statistics Bureau of the Ministry of Finance, locations with less than 30 employees accounts for 94.7% of the total, while the ratio of total employees represented by this number is 51.5% of the total. This indicates that most of Japan's office locations consist of less than 30 employees, but that the number of employees represented by these locations is approximately half of the total number in Japan.

No. of employees at each location	No. of locations	Percentage	No. of employees	Percentage
1-4	3,867,570	61.1%	8,422,537	14.0%
5-9	1,214,145	19.2%	7,896,374	13.1%
10-19	678,174,	10.7%	9,107,494	15.1%
20-29	232,827	3.7%	5,534,761	9.2%
Sub Total	5,992,716	94.7%	3,0961,166	51.5%
30-49	171,322	2.7%	6,434,035	10.7%
50-99	102,975	1.6%	6,999,666	11.6%
100-199	39,803	0.6%	5,411,499	9.0%
200-299	10,614	0.2%	2,562,194	4.3%
300 and more	11,898	0.2%	4,489,484	12.9%
Sub Total	336,612	5.3%	29,196,878	48.5%
Grand Total	6,329,328		60,158,044	

We were faced with certain limitations in attempting to calculate the total amount of virus damages incurred based on the number of business locations provided in response to our questionnaire. This is an issue which we will

be looking at in greater detail in future surveys.

Pattern 3　Estimate based on "Total Number of Employees"

Since we did not survey per-employee incident damages, we will perform an estimate based on the total number of employees.

Damages per Emloyee	=	Total Damages	÷	Total no. of employees from valid responses ※
¥1,432		¥1.18674 billion		829,007

※　The number of employees has been calculated as an average, since the response to the questionnaire question was a range, rather than an exact number.

Total Virus-Related Damages across Japan	=	Total no. of Employees	×	Damages per Person
¥86.1billion		60.15 million		¥1,432

Note

We believe that the estimation method used in Pattern 3 provides the most valid results. However, since this year's questionnaires were mainly sent to large corporations, we intend to increase the number of medium and small-sized businesses included in future surveys.

3.5.3 Observations Related to Estimates of Total Amount of Virus-Related Damages

The following are notable characteristics of this year's questionnaire results:

- The survey targets consisted of publicly traded companies listed on the First Section of the Tokyo Stock Exchange and members of JNSA.
- More than 92% of respondents have installed anti-virus software on all of the company's client PCs.
- More than 80% of respondents conduct virus checks on their mail servers.
- In excess of 80% of respondents have some type of information security rules in place.
- 71% of respondents keep their systems up-to-date with the latest security patches.

These results strongly indicate that the survey respondents have a higher consciousness of information security than companies in general.

But no matter how thorough a firm is in their anti-virus measures, in their establishment of information security policies, and in their application of security patches, they cannot completely forestall damages caused by computer viruses. Even the most conscientious firms appear to average ¥1,432 in per-employee damages caused by viruses and other information security incidents.

Assuming that the level of information security countermeasures enacted across Japan as a whole matched that of our survey respondents, we could conclude the total virus-related damages across Japan for 2003 was our estimated amount (¥86.1 billion).

In other words, the total amount of virus-related damages in Japan at the present time is at least as great as the amount we estimated (¥86.1 billion), if not significantly greater.

The point we wish to stress is not the impossibility of preventing all viruses, not matter what measures are implemented.

During our in-person interviews, those firms indicating they had undergone complete business interruptions in the past due to Nimda and CodeRed attacks, also indicated they had been successful in minimizing attacks and related damages by subsequently implementing measures such as those described above.

In contrast, some of those companies that had not experienced company-wide damages in the past were victimized by the MS Blaster virus last year, causing them to temporarily suspend business operations.

Historians tell stories from the era of the great voyages, where humans first began to cross the globe in large ships. They relate how Europeans spread viruses to natives who had no natural immunity to defend themselves.

In this new era where the Internet has become a revolutionary means of global communication, we are also faced with the threat of computer viruses. However, we do not have to be like those natives of days past, living without the ability to defend against viruses. Armed with the proper knowledge and information, we can fight against computer viruses.

3.6 Analysis and Observations of Survey Results

Last year's survey showed that in comparison with the previous year, respondents had bolstered their information security measures, and that the intervening year was relatively quiet with respect to major information security incidents.

However, the results of the 2003 survey presented in this report tell us that this was only a temporary phenomenon. The results of this year's survey reveal that information security measures have been implemented to a greater degree than in 2002. However, the MS Blaster and other viruses of 2003 caused a significantly greater amount of damage than incidents of the previous year.

In the past, most virus infections were caused by employees opening infected attachment files of email. More recently, however, infections have been linked with greater frequency to employees bringing in infected personal notebook PCs and spreading the virus to the company PCs when connecting to the corporate LAN either physically or via remote dial-up. Alternately, those infected PCs aid in spreading the virus throughout the company by connecting to the corporate LAN. Another fairly frequent source of LAN crashes noted in this year's survey is that caused simply by large increases in network traffic that cannot be handled.

The results of this year's survey also evidenced the fact that countermeasures implemented against currently known dangers will not necessarily be effective against new types of attack or illegal access. Another interesting result from this year's survey is that more companies have implemented employee information security training and education to improve security awareness, recognizing that other factors beyond purely technological countermeasures affect information security. We believe this type of training is more focused on reducing the risk of releasing personal and proprietary information, rather than solely for the prevention of virus infection.

4. Standard Model and Costs with respect to Information Security Incident Countermeasures

4.1 Information Security Incident Deterrents

To conduct an analysis of the possible correlation between the occurrence of incident-related damages and the implementation status of specific countermeasures, we have divided respondents into two groups: 1) companies damaged by an information security incident and 2) companies not damaged by an information security incident. We then compared the two groups based on the following categories:

【Categories used for Comparison】

① Systems implemented to insure information security
② Targets of information security incident response plans
③ Communications system for information security incidents/ accidents
④ Information security training and education content
⑤ Considerations when hiring contract, full-time engineers/operators
⑥ Establishment of information security policies/ rules
⑦ Per-employee information security budget

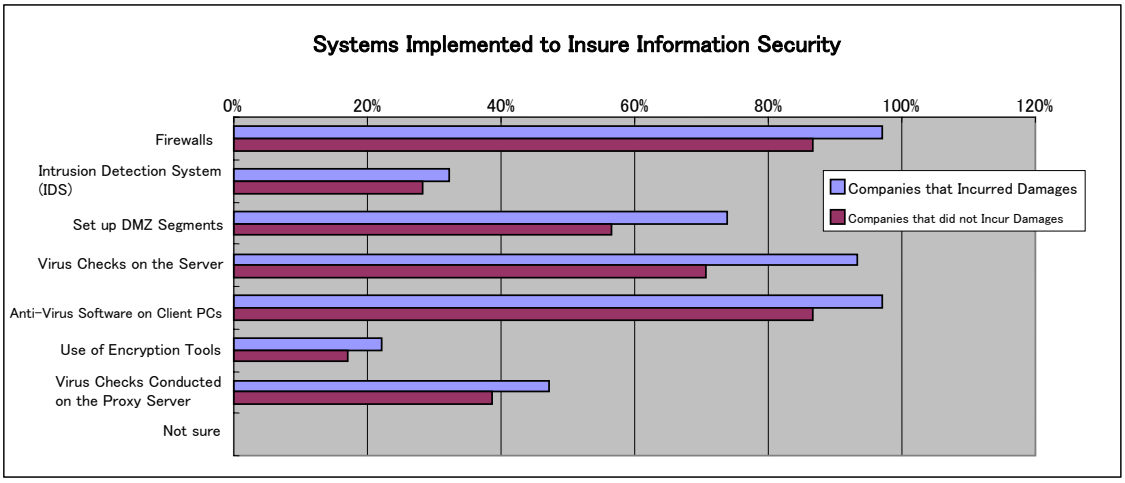
We performed the same analysis in the previous year; however, we did not have data clearly specifying whether measures implemented were done so prior to damages being incurred, or were implemented subsequently. For this year's survey, to the extent possible we categorized implemented measures as either prior to or subsequent to damages incurred.

We conducted this year's survey with the cooperation of RISTEX. Where the survey categories overlapped, specifically "① Systems implemented to insure information security", "⑥ Establishment of information security policies/ rules" and "⑦ Per-employee information security budget", we have combined the questionnaire results. Accordingly, the reader must be careful to note that the parameters for these categories are different than that of the others.

To come up with the total number of companies that incurred damages, we counted those companies indicating they incurred damages during 2003. We also counted those companies that left the section about damages blank, but indicated their company was infected with the MS Blaster virus under the answer column related to type of incident incurred.

① Systems Implemented to Insure Information Security

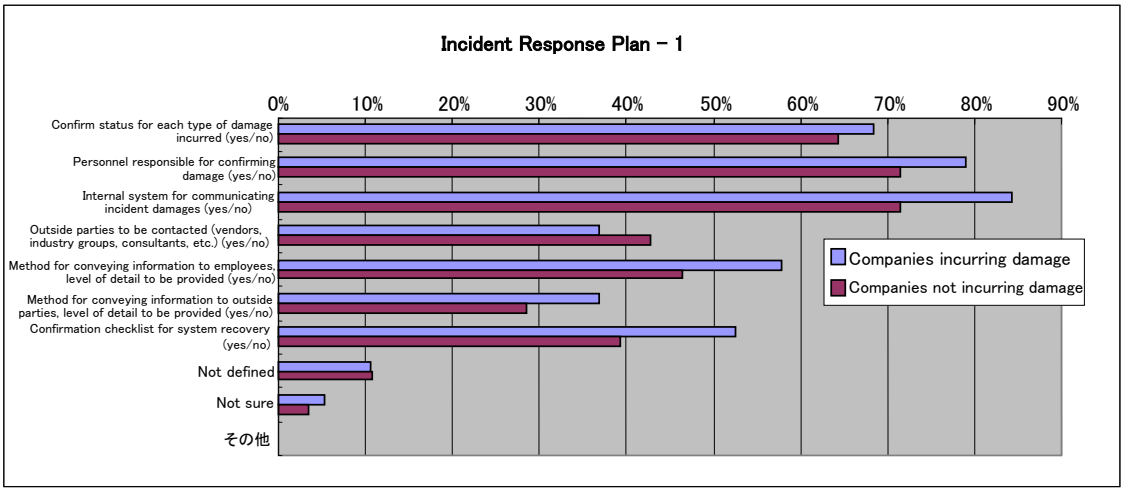
Systems Implemented to Insure Information Security	Companies that Incurred Damages (108)		Companies that did not Incur Damages (106)	
Firewalls	105	97.2%	92	86.8%
Intrusion Detection System (IDS)	35	32.4%	30	28.3%
Set up DMZ Segments	80	74.1%	60	56.6%
Virus Checks on the Server	101	93.5%	75	70.8%
Anti-Virus Software on PCs	105	97.2%	92	86.8%
Use of Encryption Tools	24	22.2%	18	17.0%
Virus Checks Conducted on the Proxy Server	51	47.2%	41	38.7%
Not sure	0	0.0%	0	0.0%

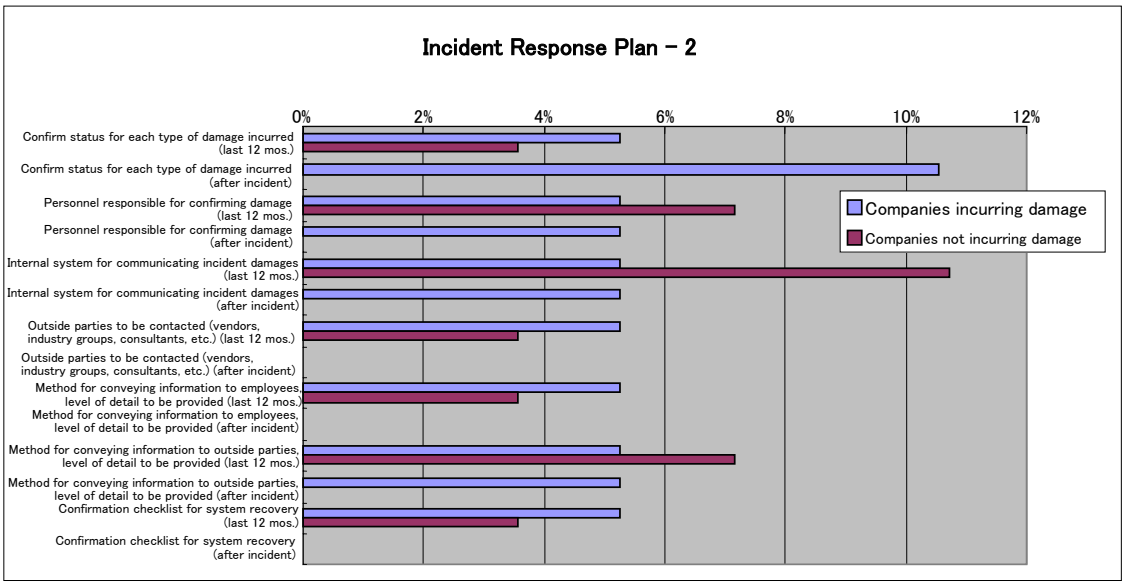


Given these results, there is no discernable difference between the two groups. Rather, it seems that the group that incurred virus-related damages during 2003 was perhaps more advanced than the other group in their adoption of information security measures. These results were not wholly unexpected, since they roughly match those of the previous year. Assuming no significant differences between the two groups in terms of the level of preparation, this suggests the possibility that other factors, such as system operation or management structure, influence whether a firm will fall prey to a virus.

② Targets of Information Security Incident Response Plans

19 Companies Incurred Damages;　28 Companies did not Incur Damages





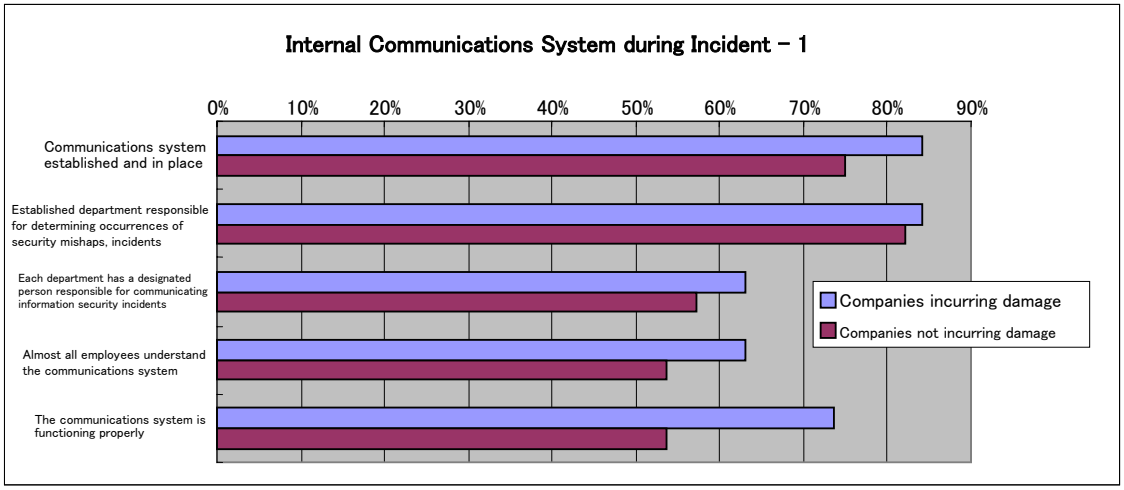
Looking at the results in “Response Plan – 1” reveals no obvious correlations between measures in place and the chance of being damaged by a virus. However, looking at a graph of the results of “Response Plan – 2,” which considers the timing of implementation, reveals that the rate of post-incident implementation for “Confirmation Checklist”, “Personnel Responsible for Confirming Damages”, and “Internal System for Communicating Incident” is significantly higher.

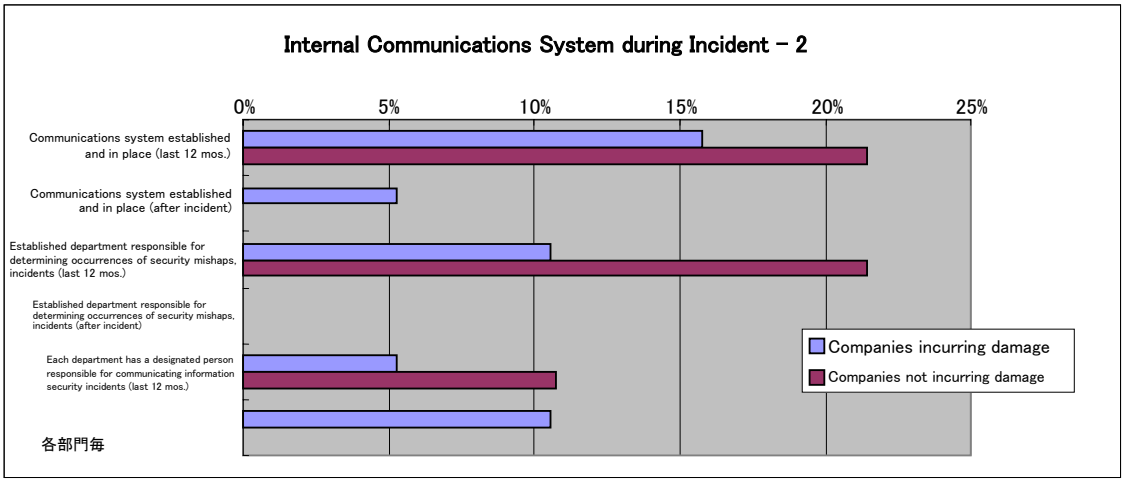
Since a response plan is not meant as a preventive or defensive measure, one cannot say that such plans have a direct

influence on whether a company will fall victim to an information security incident. However, we should note the fact that companies incurring actual damages subsequently beefed up implementation of the types of measures identified above in response to their experiences.

③ Internal Communications System during Information Security Incidents/ Accidents

19 Companies Incurred Damages;　28 Companies did not Incur Damages

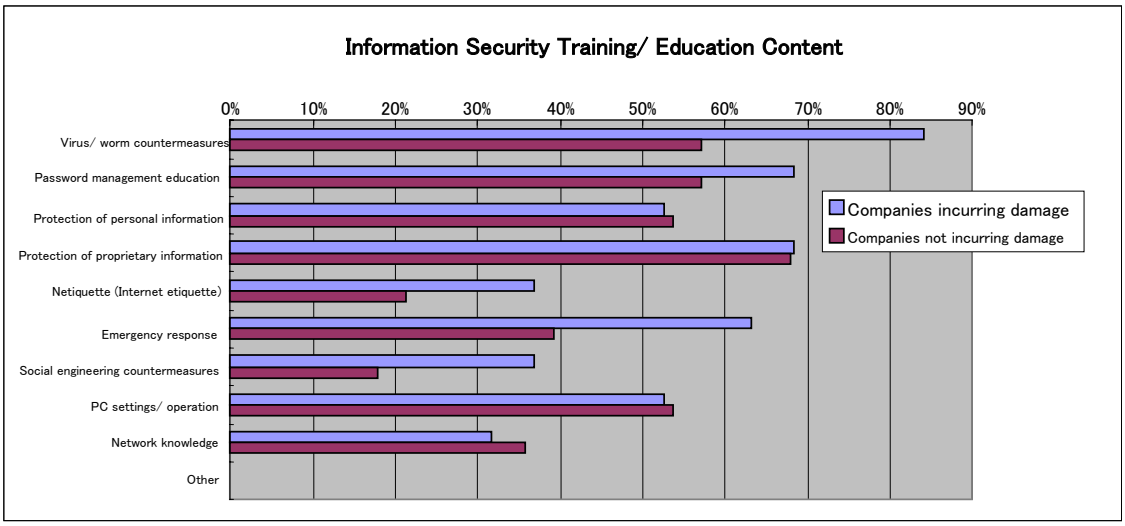




A comparison of the state of internal communication systems revealed no significant differences between the two groups. In fact, the group that incurred damages indicated a better response as to whether their communications system was functioning properly than the group that did not incur any damages. However, looking at the timing of implementation reveals that implementation of “Communications System Established and in Place” and “Person with Responsibility Designated for Each Department” happened as a result of incurring damages. As with ②, above, it is important to note that companies that incurred damages enhanced or implemented certain measures based on their experiences.

④ Information Security Training/ Education Content

19 Companies Incurred Damages;　28 Companies did not Incur Damages

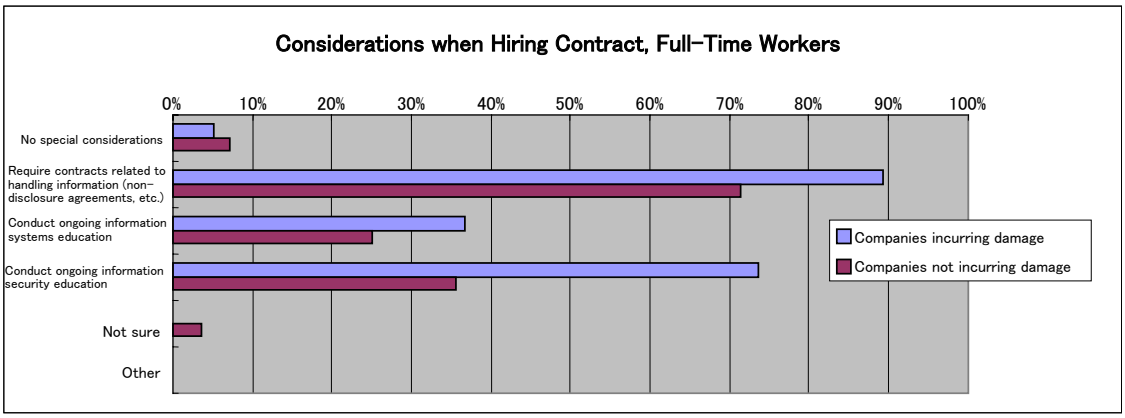


An examination of the results of our questionnaire reveals that by and large, companies that incurred virus-related damages had a more advanced program of information security training and education than those companies not experiencing such damages. Unfortunately, this particular question on the questionnaire did not include information related to implementation timing, and so we cannot judge whether those measures were implemented in response to information security incidents.

Consequently, it is difficult to make a judgment as to whether the implementation of training and education had an effect on, or was affected by, virus-related damages.

⑤ Considerations when Hiring Contract, Full-Time Engineers/Operators

19 Companies Incurred Damages;　28 Companies did not Incur Damages



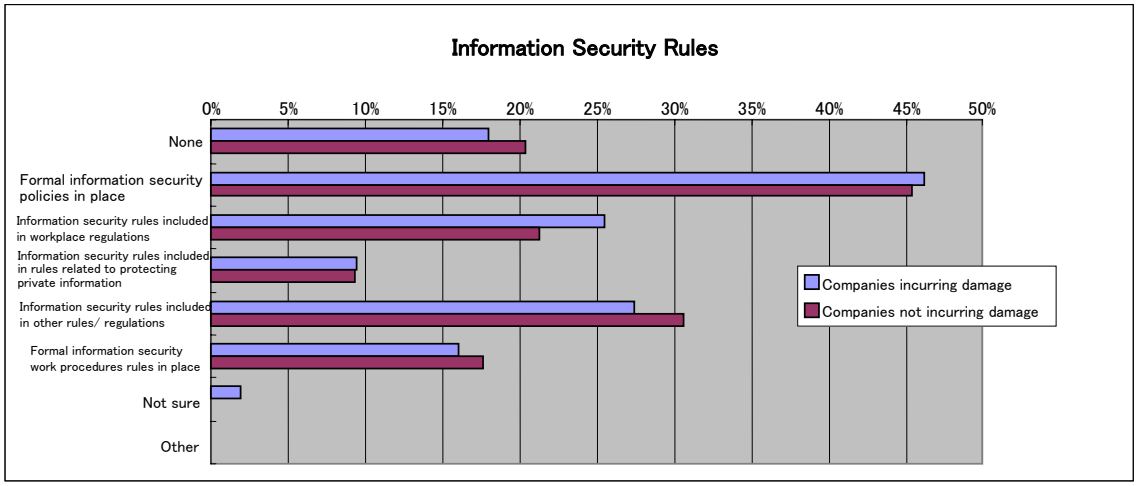
As with ④, we see that the companies who appear to have the most advanced implementation of security measures are the ones who reported being damaged by viruses. Unfortunately, this particular question on the questionnaire did

not include information related to implementation timing, and so we cannot judge whether those measures were implemented in response to information security incidents.

Consequently, it is difficult to make a judgment as to whether the implementation of training and education had an effect on, or was affected by, virus-related damages.

⑥ Establishment of Information Security Policies/ Rules

106 Companies Incurred Damages; 108 Companies did not Incur Damages



With respect to the establishment of information security policies, we did not note any significant differences between those companies that incurred damages and those that did not. As with several of the previous categories, we did not obtain data regarding implementation timing here. We must wait until next year's survey to be able to make observations in this regard.

⑦ Per-Employee Information Security Budget

Information security budget for companies that incurred damages (51)

No	No. of Employees (people)	Information Security Budget (¥10,000)
1	1,346	600
2	1,000	1,000
3	9,284	125
4	158	200
5	700	1,000
6	4,754	2,000
7	1,025	2,000
8	3,800	2,400
9	1,476	500
10	5,000	300
11	490	240
12	5,000	1,500
13	2,100	5,000
14	850	300
15	713	300
16	600	150
17	1,000	50
18	8,000	2,500
19	12,500	5,000
20	800	2,000
21	4,310	4,000
22	2,000	1,100
23	847	500
24	2,179	3,500
25	2,330	300
26	700	500

No	No. of Employees (people)	Information Security Budget (¥10,000)
27	513	500
28	1,499	300
29	600	500
30	4,819	15,000
31	836	500
32	2,822	1,000
33	140,000	150,000
34	7,155	1,650
35	630	23,000
36	2,125	500
37	4,489	4,000
38	2,679	500
39	1,244	1,000
40	1,000	3,000
41	3,500	2,000
42	1,222	3,000
43	2,600	600
44	14,700	500
45	15	1,000
46	44,300	200,000
47	1,160	10,000
48	3,515	2,970
49	45	86
50	105	200
51	100	300
Total	**323,638**	**450,171**

Information security budget for companies that did not incur damages (41)

No	No. of Employees (people)	Information Security Budget (¥10,000)
1	1,200	250
2	300	200
3	4,000	2,000
4	243	200
5	3,786	200
6	750	500
7	292	175
8	1,300	5,000
9	270	1,000
10	1,000	100
11	1,673	160
12	2,445	2,000
13	2,745	1,850
14	1,628	1,000
15	2,414	21,000
16	2,847	333
17	3,196	3,000
18	1,415	120
19	3,191	2,000
20	1,829	110
21	4,000	1,000
22	14,000	600
23	500	1,000
24	800	200
25	1,555	3,700
26	2,700	300
27	1,057	500
28	626	200
29	1,488	500
30	2,200	100
31	7,000	4,000
32	8,316	5,000
33	24,000	5,000
34	2,300	4,000
35	3	50
36	116	500
37	18	100
38	113	2,500
39	12,053	1,000
40	15,815	1,000
41	70	50
Total	**144,317**	**81,498**

The above charts include figures for only those respondents who provided data about both their number of employees and information security budget.

We calculated a per-employee information security budget in order to measure the difference in budgets between companies that incurred damages and those that did not. The following illustrates the results of our calculations:

Companies incurring damages＝¥4.50171 billion÷323,638 employees＝¥13,910

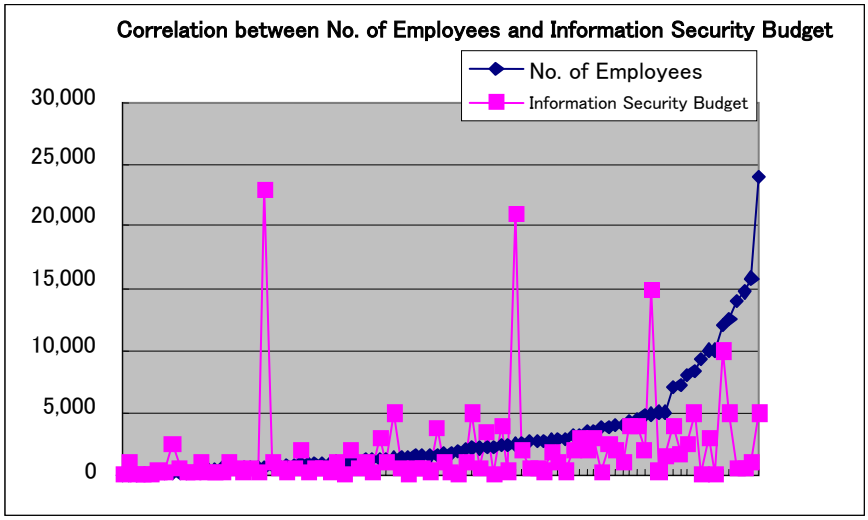
Companies not incurring damages＝¥814.98 million÷144,317 employees＝¥5,647

In the previous year's survey, we saw that the companies that did not incur damages during the year under study spent three times as much on information security as those companies that did incur damages. The response to this year's study indicated the opposite, where companies that did incur damages spent two-and-a-half times more on information security than those companies that did not incur damages.

Due to the possibility that the inordinate size of budgets for No. 33 and No. 46 within the group that incurred damages has skewed our results, we removed these two companies from consideration and calculated a new average.

Our recalculation (removing companies No. 33 and No. 46) resulted in a per-employee average budget of ¥7,100 (companies incurring damages=¥1.00171 billion÷139,338 employees=¥7,100). Although this figure is much closer to the per-employee budget of ¥5,647 for companies that did not incur damages, it nevertheless still exceeds that figure.

The graph below provides a visualization of the correlation between the number of employees and per-employee information security budget. The inordinately large values for companies No. 33 and 46 within the group having incurred damages makes it difficult to see the graph in detail; therefore, we removed these values.



An analysis of the results (ignoring several outliers) shows a correlation between information security budget and the number of employees for companies up to about the 5,000 employee level. Information security budgets did not rise over a certain level with companies of more than 5,000 employees.

4.2 Observations regarding Comparisons of Companies that Incurred/ did not Incur Virus-Related Damages

We observed that companies incurring virus-related damages were further advanced in their information security measures than companies that did not incur damages. However, the comparisons in section 4.1 were not for the purpose of comparing figures per se, but rather to gain and understanding of trends. Therefore, we did not adjust our calculations to compensate for differences in the number of companies in each group. Consequently, rather than accept these results blindly, we must allow for the following compensating factors to make meaningful conclusions:

a. For categories ②, ③, ④ and ⑤, the number of companies incurring damages was 18, while the number of companies that did not incur damages was 28. Therefore, when looking at these results one must keep in mind that compared to the 28 companies, the degree of influence of the 18 companies is slightly less than 1.7.
b. Assuming that virus-related damages were incurred, even though no significant differences were noted between the groups with respect to the implementation level of information security systems and establishment of security policies, then one could conclude that it is not "what" has been implemented, but how effective the implementation and maintenance are that has the most impact. Further in-person interviews with respect to this factor might reveal interesting data.
c. It is conceivable that among respondents who answered that their company did not incur any damages, there were some who actually did incur damages about which the person answering the questionnaire was not aware. We believe such a situation has possibly affected the response rates for both groups.
d. There is a possibility that variances in budgets are due to the inaccurate understanding of the person answering the questionnaire. This person may not be in a position to have a full knowledge of their company's information security budget. Alternatively, the information security budget may be included as a part of the overall systems budget, with no clear indication as to the exact level of funds allocated for security.
e. After evaluating the usefulness of our questionnaire in the previous year, we decided to include data about the timing of the implementation of information security measures in this year's version. However, because we did not ask for this data in connection with every single relevant question, our analysis cannot be regarded as conclusive.

Approaching our analysis again giving weight to the factors identified above, we see several important points not revealed by numerical analysis alone. For example, as pointed out in c. and d. above, since the person answering the questionnaire may not have been in a position to know fully the state of affairs at their company, the precision of the data collected may be somewhat compromised. However, one could also argue that the fact that the person answering the questionnaire is not in a position to fully know the state of affairs at their company is, in and of itself, a defect in the company's information security. We have seen in ② and ③ of section 4.1 where many of the companies categorized as not having incurred damages have nevertheless instituted security measures within the past twelve months. Further

reading between the lines, one could conclude that the chances a company would go to the trouble and expense of implementing such measures without having incurred some type of virus-related damages is very low; the person answering the questionnaire may not have known the actual situation at the company, or may have known, but for some reason did not indicate that damages had been incurred. While it is very difficult to conduct a survey as to someone's level of understanding about the situation in their company, just how far to pursue the identification of such errors is an issue for further study on our part.

As can be seen, doubts remain as to the degree of reliability of our analysis. We will spend the intervening period between now and next year to carefully consider the need for the type of comparative analysis included in section 4 of this report.

The results of this year's questionnaire did not allow us to quantifiably draw a distinct line between companies that did/ did not incur virus-related damages. As far as we can tell, most companies have implemented sufficient measures to protect their organization from external attacks, utilizing firewalls and virus checks at external Internet connection points.

Having said that, however, we did note that many of the cases of virus-related damage during 2003 were caused by the MS Blaster virus, where several infected PCs spread the virus via a corporate LAN. This trend gives one the sense that companies need to work more on the internal security systems between the organizational level and individual corporate PCs. While the results of our questionnaire revealed a high ratio of companies implementing PC virus checks and timely patch updates, our in-person interviews revealed that actual implementation is left to the individual user, and in fact several cases of MS Blaster virus infection were caused by only a few users failing to apply patches in a timely manner. Based on these unfortunate experiences, several organizations are implementing system tools to audit each PC in the company, where system administrators monitor computers centrally and automatically as to applying patches.

Organizations across Japan should take careful note of the high frequency of responses that indicated companies enhanced measures such as "checklist of confirmation items", "person responsible for confirming damage", "system for internal communications", "establishment of communication rules" and "selection of person in each department to be responsible" subsequent to being hit by a virus outbreak.

4.3 Suggestions for Appropriate Response Levels and Budgets

As in the previous year, we will consider the appropriate response level and scale of information security budget guided by the results of questionnaires and in-person interviews as to the desired response level.

① Desired Response Level

The main points gleaned from the results of our questionnaire and in-person interviews are listed below:

a. Basic information security systems such as firewalls, virus checks and IDS have been implemented to at least a minimum level.
b. Companies are beginning to put together systems supporting security measures, including establishing information security rules, incident response manuals and other documents, as well as appointing personnel in charge of information security management.
c. Companies that have instituted ISMS have recognized the need to do a better job of auditing whether these measures are enforced and effective as the individual user (PC) level.
d. Dangerous viruses such as MS Blaster are sure to spread again in the future. Even if the most advanced security measures are in place today, a company must still be prepared for a virus outbreak of some sort. In other words, companies would be best advised to implement security measures anticipating attacks, while at the same time prepare to respond promptly to incidents with “checklist of confirmation items”, “person responsible for confirming damage”, “system for internal communications”, “establishment of communication rules” and “selection of person in each department to be responsible”.

The table below summarized these requirements:

Response Level	Measures	Examples	Response Level
Response Level 1	Technological Measure	Firewall	Response Level 1 / Response Level 2
		Virus countermeasures	
		IDS	
		Mail management software	
		Authentication devices	
		PC security (virus checks, patch application, data encryption, etc.)	
Response Level 2	Operational Measure	Physical access management	Response Level 2
		Appoint security personnel	
		Establish information security policies	
		Create security incident response manual	
Response Level 3 (Recommended level)	Improve Level of Implementation	Information security training/ education	Response Level 3 (Recommended level)
		Set penalties for rules violations	
		Enhance systems audit functions	
		System for communications during incident(s)	
		Incident response training	
Response Level 4	Improve Third- Party Certification Status	ISMS/ BS7799 certification	Response Level 4
		Obtain privacy mark	
		Conduct information security audits	

In this table, Response Level 3 represents the recommended level. At this level, a company insures that measures are working properly down to the lowest level (individual PC) within the firm, and that policies are working to make sure that rules are being followed. This standard operates to build an organization prepared for the inevitable virus attacks and other information security incidents.

As discussed in b. of section 4.2, it is not what measures a company has instituted, but rather whether those measures are functioning effectively that is most important. One must not assume, however, that we are implying firewalls and other measures do not prevent security-related damages. Without firewalls and virus checks at external Internet connection points, it is almost certain that viruses and other incidents would have increased, and caused damages on a much larger scale.

Instituted measures represent levels 1 and 2 in the preceding chart, and should be regarded as the minimum necessary measures that a company should implement.

② The Relationship between Scale of Incident Damages and Information Security Budgets

As introduced in ⑦ of section 4.1, the per-employee information security budget for those companies that incurred security-related damages slightly exceeded that of companies not incurring damages. However, the most frequently experienced virus type during the year was the MS Blaster virus, which we see caused significant problems even at companies that had security measures in place. Therefore, we believe a study of the scale of damages (scope of influence) compared to company security budget may offer insights not available in a simple comparison of whether a company incurred damages or not.

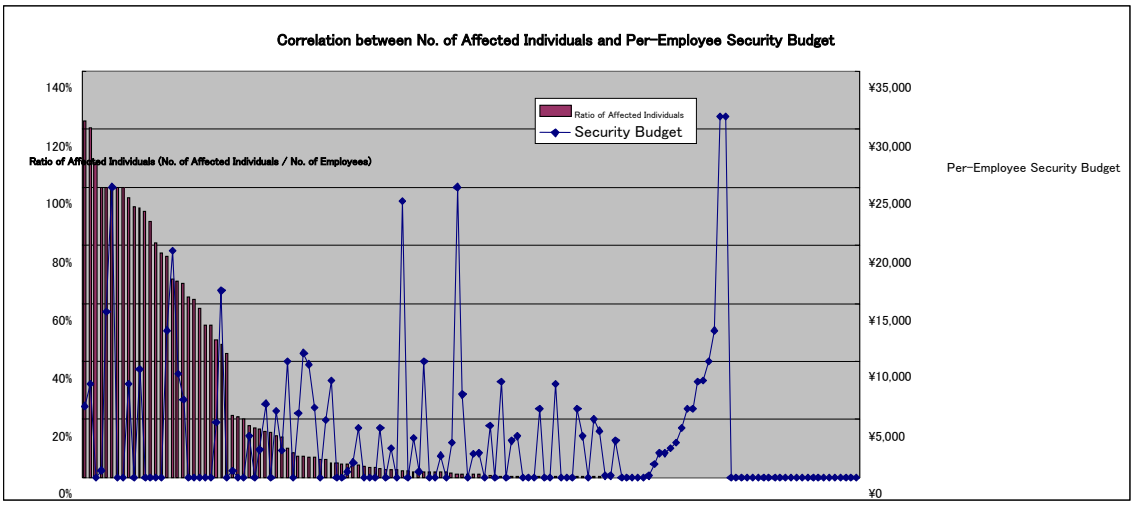
The results in ⑦ of section 4.1 eliminated data from companies that did not provide specific budget figures. Here, we will include this data for purposes of our analysis.

The following lists the areas we studied:

a. Correlation between the ratio of individuals affected by damages and per-employee security budgets
b. Correlation between total number of personnel affected by damages and per-employee security budgets
c. Correlation between number of computers affected by damages and per-employee security budgets

a. Correlation between the ratio of individuals affected by damages and per-employee security budgets

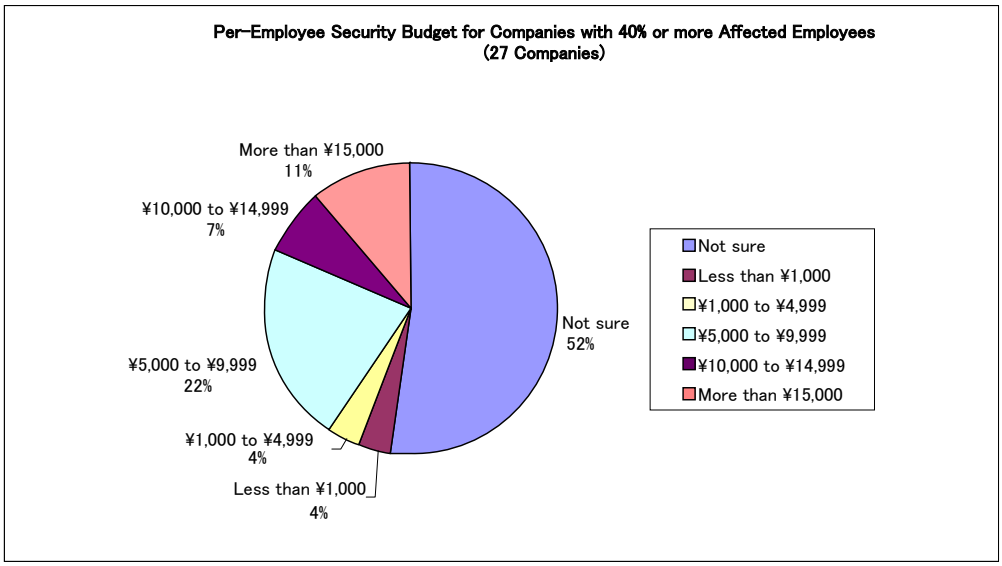
We performed a comparison of the ratio of individuals affected by damages and the per-employee security budget for the 142 companies that indicated they incurred damages during the year. The responses included companies who did not supply data for their security budgets. We set the per-employee budget for these companies to 0, which will affect the reliability of our data, but we still believe this data will be representative of overall trends. The ratio of individuals affected here means the percentage of individuals affected by virus-related damages compared to the total number of employees at the company.

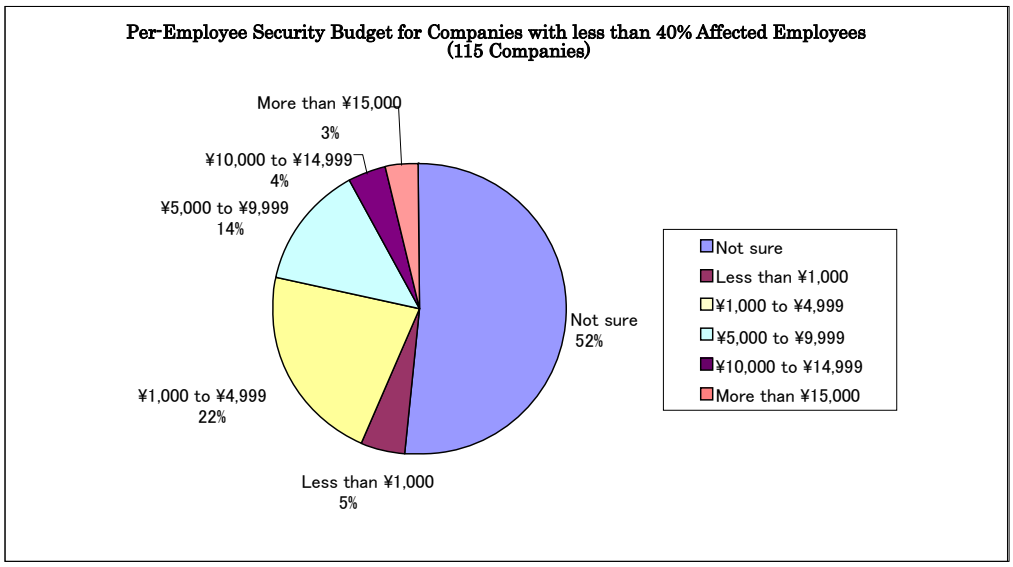


As can be seen in this graph, there is no clear correlation between the scale of damages incurred and security budgets. Therefore, we have set an arbitrary standard level of damages incurred, and compared the budgets of the groups falling above and below that standard in b. and c. below.

b. Correlation between the total number of personnel affected by damages and per-employee security budgets

We divided the respondents into two groups: 1) those companies in which more than 40% of total employees were affected by a security incident, and 2) those in which less than 40% of total employees were affected. Then we performed an analysis of the per-employee security budget for both groups.





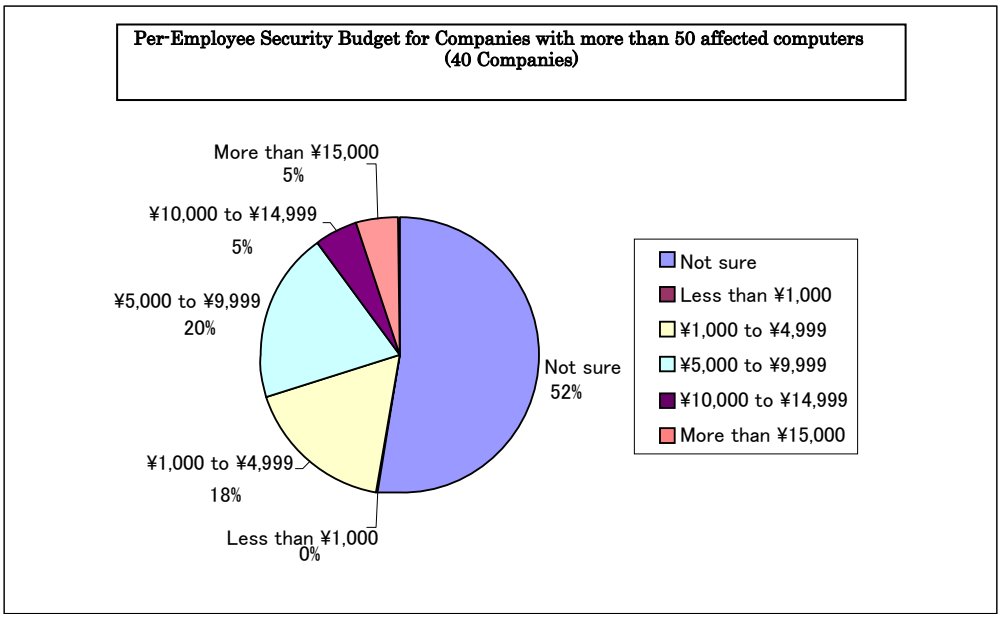
According to the graphs above, after removing companies that did not provide specific budget figures, the highest ratio for per-employee budget for companies in the group with 40% or more employees affected by an information security incident was between ¥5,000 and ¥9,999 (22%). For the companies in the group under 40%, the highest ratio for per-employee budget was between ¥1,000 and ¥4,999 (22%).

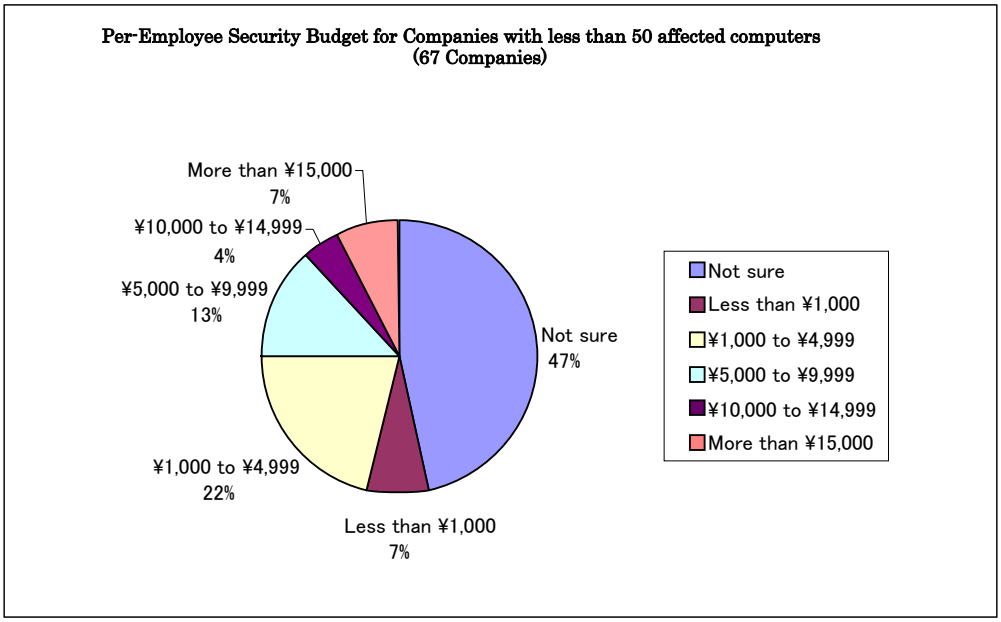
Contrary to the expectation that the group with a lower ratio of employees affected by a security incident would have a higher per-employee security budget, the graphs above indicate that in fact the group with higher ratios of employees affected also had a higher per-employee security budget.

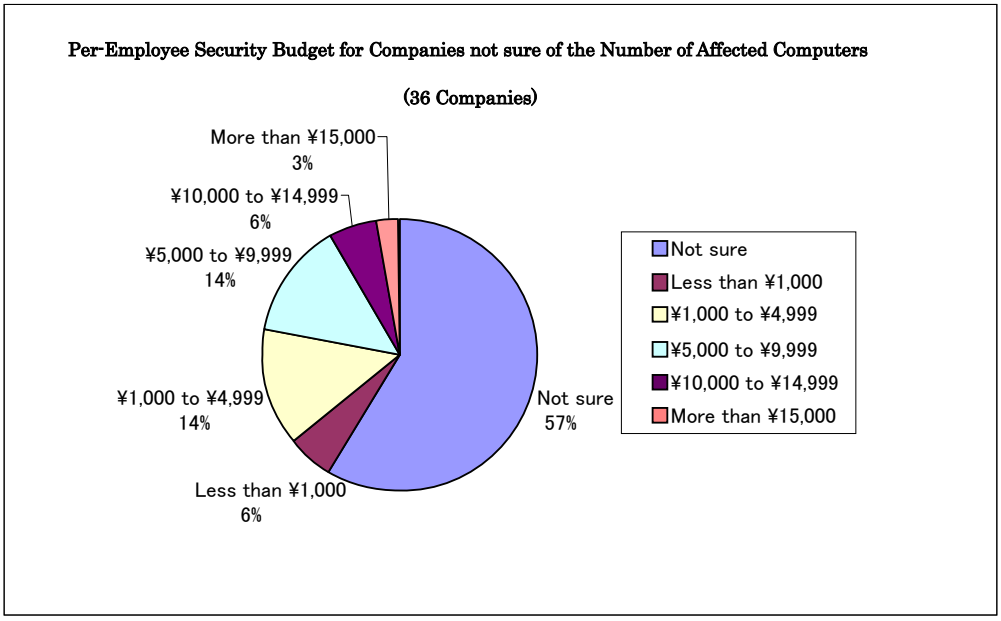
c. Correlation between number of computers affected by damages and per-employee security budgets

We divided those respondents who indicated they had computers subject to an information security incident into

three groups: 1) 50 or more computers affected, 2) less than 50 computers affected, and 3) not sure how many computers were affected. Then we performed an analysis of the per-employee security budget for the companies in each of the three groups.







According to the graphs above, after removing companies that did not provide specific budget figures, the highest ratio for per-employee budget for companies having more than 50 computers affects was between ¥5,000 and ¥9,999 (20%). For companies in the group limited to less than 50 computers affected, the highest ratio for per-employee budget was ¥1,000 to ¥4,999 (22%).

For the group that did not know the number of computers affected by an information security incident, the ratio of companies reporting a per-employee budget between ¥5,000 and ¥9,999 and those reporting a per-employee budget of ¥1,000 to ¥4,999 were the same at 14%. We noted that an extremely high ratio of companies in this group (57%) also did not provide budget numbers.

As with b. above, the companies reporting a higher number of affected computers also had a higher level of per-employee security budgets.

Observations about the results in ② above

Taking the results of b. and c. at face value, we must come to the conclusion that no strong correlation exists between the scale of damages and the per-employee security budgets of respondents. However, looking at these results from a different angle, the fact that the ratio of respondents not knowing the amount of their security budgets was the highest among all groups clearly shows the importance of understanding what resources are allocated to information security, regardless of the correlation between the budget and the scale of damages incurred.

How to best improve the accuracy and effectiveness of information security budgets will be an issue for further study next year. This is an issue held in common by all companies, and something difficult for this Working Group to influence directly. However, we feel that our role as a Working Group includes defining standards for what should be accounted for under the banner of “security budget,” and proclaiming the importance of knowing how much budget is

allocated to information security.

5. Incident Survey Interview Report

5.1 The Significance of the Interviews

While both statistical analysis and drawing of conclusions are possible through the use of paper based questionnaires, actual investigations require actual interviews in order to ascertain the actual condition of damage. Therefore, over a period of 3 years, this working group went directly to companies, and was able to carry out actual interviews as regards information security incidents.

Amongst the companies that responded to the paper questionnaire, we paid a direct visit to those that were happy to be interviewed, and surprisingly, we were able to obtain specific information about damage.

Here, what was surprising was as follows: as regards information security itself, companies were likely to focus on "ensuring that information is not carelessly leaked outside," and consider "disclosing our company's damage incurred by an information security incident is an embarrassment," therefore even in unbiased organizations such as JNSA, we thought that responses would be difficult to obtain.

However, in reality, all companies that agreed to be interviewed readily responded to our questions, and we were able to get tangible responses face to face, about where they were concerned, and where things were going well.

5.2 Summarizing the Results of the Interviews

The results of the interview were largely qualitative, and as we had to avoid any methods that could identify companies that were interviewed, up until last year, apart from basic materials used for calculation of damages, we provided results in a consolidated form by each question.

On the other hand, the interviews saw companies that responded to our questions asking us frankly "how are security provisions in other companies in the same field?" and "we know information security is important, but how far do we need to go?"

We would like to thank the companies that took time out of their valuable schedules to cheerfully respond to our questions, and therefore we present this report in summary of the results of our interviews, that gives actual examples of information security, while taking all measures to ensure areas that are problematic, or those that are being handled well can not be used to identify companies.

5.3 Examples of Information Security

Example 1 Theory and Practice of Security Provisions

Company A is one classified as a financial business, and its information systems are housed in a building in the suburbs of Tokyo. There is direction from competent authorities as regards the structure of their business, and the company as a whole has been working on information security provisions for several years.

For several years, the person in charge of information security at Company A has been participating in seminars regarding information security and similar topics, and has been approached by security and SI companies, however it is thought that these solutions were not usable in this company's environment.

In fact, all PCs have anti-virus software installed as countermeasures against viruses and worms, etc., and the company has a virus gateway server in place, however this is unable to keep 100% of these threats in check.

Upon the preparation of the company's security policy, they do not contract security or other consultants from outside the company; instead, they have their own information Security Department which selects information security representatives from each department, and which both formulates and implements the company's own security policy.

As a response to recent “personal information disclosure related incidents,” the company has implemented a system in which employees are not allowed to remove information on recordable media such as floppy disks or CD-R, however this cannot be 100% controlled, and operational provisions are required.

In the final analysis, similar as to when introducing information systems, it is necessary that companies gain experience in operating these systems themselves when receiving a service, even when introducing various security products or using provided services, instead of merely using these as provided.

Example 2 Outsourcing System Development, and Ensuring Security

Company B is one classified as a manufacturing business. In principle, the company operates and manages their own information systems. The recent focus on information security has led to the company establishing a security policy after reference to the sample policy on the JNSA site.

However, last year, accompanying a renovation of settlement systems, the company carried out an overall update of information systems, however as the company are lacking sufficient information systems personnel, they chose to procure personnel from outside the company in order to develop their system.

The personnel who were dispatched from the contracted systems development company brought their own notebook computers, and used these in system development, however these personnel were unable to fully integrate with Company B's security policies, such as use of anti-virus software, and application of the most up-to-date definitions files.

Accordingly, in order for the company to guarantee security, it set up a dedicated network for the externally contracted personnel, upon which they could carry out development isolated from the company's internal systems.

As a result, while it was confirmed that the notebook computers these personnel brought into the company were infected with worms, these did not affect the company's internal systems, and the infection was limited to this isolated

network only.

Example 3　The Importance of Asset Management

Company C is one classified as a telecommunications business. Because its main business is in the creation of communications networks, it has had in place security policies for quite some time, and is thought that these are relatively reliable.

The company has offices throughout the country, however access to the Internet is centralized, and monitored from a central location at headquarters.

However, the system was unable to 100% prevent MS Blaster related worms last year, which infected the network as a result of notebook computers being brought in from outside.

There were multiple outbreaks at different offices, however because access to external networks is centrally managed and monitored through the headquarters, immediately after infection, the IP addresses of the infected PCs were quickly determined, and the affected offices were contacted.

However, the contacted offices used DHCP for their network connections, therefore it was not possible to determine the actual infected PCs just from their IP addresses, meaning that identification of these specific machines took some effort.

Luckily, last year these offices had carried out a general replacement of PCs, meaning that the machine names (host names) and the MAC addresses were stored in a list of assets. As a result, the infected PCs could be identified, removed from the network, and countermeasures implemented.

This company has been using asset management software (inventory acquisition software), however this was only being used for managing software assets, therefore in the future, the company is considering using this software more effectively.

Example 4　　Security Management Organizations

Company D is one classified as a manufacturing business. The company has previously acquired ISO9000, and ISO14000 certification as a requirement for its operations. The recent popular topic of information security has meant that they are working towards the construction of an information security management system.

Having ISO9000 and ISO14000 certification is a necessary qualification in order to bid, therefore they are establishing full time representatives in order to create management systems, and are instituting representatives in each department.

However, information security is not absolutely essential for business, therefore the company is not considering acquiring an ISMS certification system.

The company is not planning to go for certification, however in order to guarantee information security, as well as a response to incidents through having both systematic security policies and information security representatives, it is important that they construct a company wide management system in order to both decided upon, and operate security policies.

In reality, when constructing an information security management system, it is not realistically possible to implement representatives as with ISO9000 and ISO14000, nor to put in place representatives in each department.

Therefore, the corporate organizations' management system, in short the system for managing business was used without change as the information Security management system.

Specifically, this was made into a system in which company management were made the top representatives, department heads were made the information management representatives, a security committee was established, and information system managers were active as a secretariat. This specified regulations concerning information security, and has become an effectively functioning system, even in the event of incidents (security incidents and damage). Additionally, it is also thought to be functioning efficiently as a management system as regards non-information security related threats.

Example 5 The Effectiveness of Implementing Training in Business Continuity Planning (BCP)

Company E is one classified as an information service business. Because it carries out system development and sales of network related equipment, it is taking a very proactive stance as regards information security. Accordingly, it acquired ISMS certification immediately upon that certification system being created.

As one part of its security policy, Company E has enacted Business Continuity Planning (BCP), and after attaining ISMS certification, carries out periodic BCP training.

The implementation of training for Business Continuity Planning comprises “continuing business through using paper media as substitutes in processing, and using telephone, fax, and similar communications methods in the event that damage results in information systems being unusable.”

Modern businesses generally use computerized methods such as e-mail for contacting customers, and order processing that uses accounting systems, however not surprisingly, there are still very few companies that have seriously investigated carrying on with their business in the event that these systems cannot be used.

Up until this training was carried out, employees at Company E were quite apprehensive about their capabilities in carrying out this.

However, actually carrying out training in BCP showed that there was less confusion than originally anticipated, and it was shown that business could indeed continue. If we think about this, up until recently (3-4 years ago), most business was still carried out based upon paper media, with most contact with customers being carried out either on the phone or by fax, therefore it was obvious that continuing business was not impossible.

Not having computers does not preclude one from continuing business, and it has become very obvious that not considering a response plan for damage in advance could result in stoppage of the business.

Example 6 Limits of a Security and Policies from Organizational Systems

Company F is one classified as a building business, and has branches throughout Japan. In principle, it carries out its business accounting independently, at each of its offices.

Company F's system has its basic accounting system centrally managed at headquarters, however because each office

independently carries out their own purchasing of computers and software, the headquarters does not have an overall view of the situation.

Additionally, a feature of Company F's business is that when it starts construction work, each site is established as a new office, therefore installation of PCs, and laying of network wiring mean that it is largely impossible for headquarters to be aware of the overall situation.

Under these circumstances, Company F was subject to widespread network damage resulting from a worm infection, which resulted in damage that brought down communications in each office. This company also has a department that has implemented electronic trading on the Web, which meant that they had a close-up view of the company's problems.

After this incident, management directed that information systems representatives throughout the company "will implement an investigation of information security policies, and of future risk management," and they then took the following measures.

- Centralizing Internet access through headquarters
- All e-mails are scanned for viruses in an anti-virus server
- Installation of anti-virus software on all PCs throughout the company, and notifications to apply up-to-date virus definitions, to all offices.
- Notification to all offices to apply most up-to-date security patches.

However, in Company F's budgetary management system, business accounting is carried out at each of its offices or departments, which means that purchase of software when implementing the contents of these notifications, and the pace of this implementation are not all equal, which means that the company is still experiencing virus infections.

Example 7 Security Policies at Affiliates

Company G is one classified as a manufacturing business, and has branches throughout Japan. As a manufacturing company, it has a large number of subsidiaries and affiliate group companies.

As regards Information Systems, all of these companies have installed ERP, which is being managed by the respective Information Systems representatives; furthermore, in branches and laboratories, people who have additional posts, and have detailed knowledge of this topic have taken on this responsibility, meaning that throughout the company, there is a proactive attitude towards information security policies.

Particularly with anti-virus and worm measures, the company's past experience of having the entire company's business shut down by being infected by the Nimda virus has led to the installation of an anti-virus server (gateway), installation of anti-virus software on all PCs, updating of these to the most recent virus definitions, and the installation of the latest security patches.

Even in spite of these types of measures, MS Blaster last year led to some parts of the business shutting down. Specifically, while PCs that were being used for general business had proper anti-virus measures in place, machines used in manufacturing business (running Windows OSes) had not been included in the anti-virus measures. This was because hardware and applications as a whole had been purchased with an eye to the functionality of the software to be

used there. Security patches were not applied, because software manufacturer(s) would not offer a guarantee of operation, and for the same reason, anti-virus software was not installed.

At the time this damage occurred, the company contacted software manufacturer(s) as quickly as possible, removed the worm, and applied the latest security patches.

In this case, a detailed investigation as to why the MS Blaster worm proliferated on Company G's network has not been carried out. Most PCs managed by the company had in place countermeasures, and in the branch which was affected by the worm, generally there were no PCs brought in from outside the company.

We asked and Information Systems management representative at Company G for his thoughts, and he said “we think that maybe a group company was infected, and that the virus got into our company's system.”

Security policies at Company G are fairly widespread within the company itself, however similar levels of precautions have not been implemented in all group companies, and this includes subsidiaries. However, when carrying out business, subsidiaries and group companies are connected on the same network that uses dedicated lines, and it is thought that the worm entered by this route.

In the future, it would be ideal if all group companies enacted security measures, however, although these may be subsidiaries, they have a varying range of relationships with the main company, meaning that a uniform implementation is difficult.

6. 2003 Information Security Incident Damage Cost Calculation Model

(Unchanged from last year)

Last year (2002), we changed the calculation model for calculating damages that was originally created in the first year (2001) of these studies. While there have been no major changes this year, we are again presenting this document in order to aid overall understanding. Because the following details are the same as in last year's model, we suggest that if you are already familiar with this model, you start reading from Chapter 7.

Many factors contribute to the total damages caused by systems and network information security incidents. These factors include costs of paying legal compensation, costs for personnel involved in system or network recovery, costs for hardware and other physical damages, loss of business reputation, and lost profits due to business interruptions.

These various incident-related damages can be divided into two categories.

The first category is "Apparent Damages", which is generally easy to calculate and consists of "Directly Attributable Damages Model: Lost profits and costs incurred" and "Indirectly Attributable Damages Model: Reparations, supplemental costs and legal compensation". The second category is that of "Hidden Damages," which consists of costs associated with difficult-to-quantify factors such as reduced work efficiency, etc.

We will consider a damage cost calculation model incorporating the total of these two types of damages.

6.1 Apparent Damages

Lost profits and actual payments made as a result of an incident are easy for a company to recognize as damage costs. Damages that can be monetarily quantified are termed "Apparent Damages", which consist of primary and secondary factors.

6.1.1 Direct Damage Costs

When a business or service relies completely on a network system, as in the case of E-Commerce websites, incident-related damage costs can be relatively simply calculated as lost profits over the period of time during which the system or the network was down.

In this case, revenues during the time in which the system or network was unavailable are considered to be zero, and no profits are made during the downtime.

Damage costs are calculated using the following formula, based on the Lost Profits theory:

Lost Profits = Sales profits per hour × Number of hours the system/ network was unavailable

"Sales profits per hour" is derived as the amount of profits that would have been earned had the system/ network not been taken down. For E-Commerce websites, the figure can be calculated based on daily profits.

Directly Attributable Damages must also include costs required to restore the system/ network. When an E-Commerce website is accessed illegally, and the content of the webpages have been changed, the calculation of Directly Attributable Damages must include lost profits incurred until the system is restored, and costs incurred to restore the

system (hardware, software, personnel costs), according to the following formula:

Direct Damage Costs=Lost Profits+Costs incurred to restore system+Business contingency costs
+Lost information assets+Opportunity Costs

6.1.2 Indirect Damage Costs

If indirect financial damages are incurred as the result of interrupted business or services due to an incident, the value of such damages must be included in the calculation of damage costs.

Conceivable costs include demands for reparations/ supplemental costs or legal compensation, costs to publish a public apology, etc. The calculation of damage costs is complicated, and includes the decrease in profits caused by damage to a company's reputation.

Indirect Damages=Indirectly incurred damages: Reparations, supplemental costs, legal compensation, etc.

6.2 Hidden Damages

With the calculation model for Apparent Damages above, the quantifiable nature of incident-related costs allows for logical damage cost calculation.

In contrast, in cases where an incident does not exert a clear external influence on a business or services, related costs may remain hidden, and difficult to calculate. Because of this, these types of damage costs have not been commonly addressed.

We term these difficult-to-see damages "Hidden Damages," and include them in the calculation model for damage costs.

6.2.1 Hidden Damage Costs

When an incident causes system or network stoppage, the greater the business relies on its systems and networks, the greater the drop in business effectiveness will be.

The work itself can be continued either by switching to a work flow that doesn't use the system (e.g. use FAXes and phones to accept and process orders, etc.), or by working overtime after the system is restored, in order to cover any fall-off in work capacity. This response serves to limit financial damages.

In this case, work is continued even without access to a computer system, so no financial damages have occurred. However, there are unseen costs associated with decreases in work efficiency, re-entry of lost data, or overtime incurred to make up for network/ system downtime.

In connection with this survey, we have discussed that decreases in work efficiency should be considered as incident-caused damages, and included in cost calculations.

In addition, these kinds of work-related "Hidden Damages" have accompanying non-work-related Hidden Damages, such as the decrease in corporate brand value when a company's reputation is hurt.

However, converting a damaged corporate image to a financial number is extremely difficult, and the manifestation

of such is tremendously influenced by the type of business/ industry, the cause of the incident, and other factors.

Because of this, we have included non-work-related Hidden Damages as a factor in our model; however, we will not attempt to develop specific calculation models here.

Given the previous arguments, the following formula describes the calculation of Hidden Damage Costs:

Hidden Damage Costs＝Hidden Damages related to work＋Non-work-related Hidden Damages
＝（Fixed Costs (payroll)×Number of People Affected by the incident
×Degree of reliance on IT×Downtime）
＋Non-work-related Hidden Damages (decrease in brand value, etc.)

6.3 Incident Damage Cost Calculation Model

Now, based on the arguments above, we propose the following “Incident Damage Cost Calculation Model”, which incorporates both “Apparent Damages” and “Hidden Damages”:

Incident Damage Costs
＝Apparent Damages+Hidden Damages
＝Direct Damages＋Indirect Damages＋Hidden Damages
＝Lost Profits（Directly Attributable Damages）
+Costs incurred to restore system（hardware, software, labor hours）
+Business Contingency Costs+Lost information assets+Opportunity Costs
＋Reparations, supplemental costs, legal compensation, etc. (Indirectly Attributable Damages)
＋（Fixed Costs (payroll)×Number of people affected by the incident
×Degree of reliance on IT×Downtime）
＋Non-work-related Hidden Damages (decrease in brand value, etc.)

<Supplementary Information>

・Fixed Costs (payroll)

The unit cost per hour of personnel affected by the incident.

・Number of People Affected by the Incident

Use the number of client PCs affected, if applicable.

If servers (Email and file servers, etc) are affected by the incident, use the number of people who use those services.

・Degree of Reliance on IT

Set the value representing the degree to which a damage-incurred system or network affects daily work between 0 and 1. The higher the reliance on the system/network, the higher the coefficient. If work processes are not affected, the coefficient is set to 0, meaning that cost-based damages did not occur; in most cases, however, damages reveal themselves in the drop off of execution efficiency, as mentioned above. If 100 work units are normally completed in one hour using the system/network, while only 80 work units are completed when not using the system/network, the

degree of reliance is 0.2.

In addition, decreases in execution efficiency can be controlled if alternate work methods have been put into place to be used during system downtime. Actual application of this factor must take these alternate methods into consideration when determining the level of reliance.

Further, the 2001 survey and its verification using a reference value of "IT reliance 0.2" for a general company resulted in a high probability that this value is widely compatible in practical usage.

・Downtime

This value is the time during which a system/network is stopped, up to and including the point where normal workflow is restored after the network is brought back on-line. If data must be re-entered, or overtime incurred to complete the system recovery, the coefficient IT reliance can be effectively used to calculate costs incurred during the period of recovery.

The product of the previous four factors, to which is added non-work-related hidden damage costs, costs incurred to restore systems (hardware, software, labor hours), lost profits (Directly Attributable Damages), if applicable, and reparations/ supplemental costs/ legal compensation (Indirectly Attributable Damages) results in our proposed Incident Damage Cost Calculation Model.

One feature of this model is its attention to decreases in work execution efficiency caused by an incident.

Even in cases where an incident does not cause specific financial damages, it is possible to calculate hidden damage costs.

To limit damage costs to the minimum, systems and networks must be constituted and arranged in a manner that limits damages to the lowest level possible (limit to the minimum scale), and work processes must be maintained at a high level allowing contingency operation (minimum IT reliance).

This approach to calculating incident damage costs should be a valuable part of corporate information systems risk analysis.

7. Summarizing the Condition of Damage, Provisions, and Responses

This document summarizes the types of damage, their causes, and countermeasures and responses, as obtained in the questionnaire.

We hope that it is useful in understanding incidents of damage, and when considering provisions.

No	Type of Damage	Overview of Damage and Cause	Countermeasures and Response
1	DoS attack or stoppage of service	Blocked at the firewall, however Internet congestion such as in a DOS attack was frequently seen.	-
2	DoS attack or stoppage of service	Attack on the FTP service on the public Web server.	Enhanced server monitoring.
3	Theft or loss of PC / PDA	Theft of a notebook PC from inside a train.	BIOS password and Windows passwords were in place, therefore it is not thought that any information was disclosed.
4	Theft or loss of PC / PDA	Theft of a PC upon which customer data was stored.	Enhancement of mobile PC management measures.
5	Theft or loss of PC / PDA	-	When employees leave the office, notebook PCs are locked inside desks for storage.
6	Theft or loss of PC / PDA	Theft of a PC from an employee stationed overseas. One from within a train, and one from a hotel.	Improved insurance for PCs used on business trips. Improved password usage. Talks with staff regarding business trips.
7	Theft or loss of PC / PDA	Theft of a mobile PC from within a parked car.	① A call for management of information (personal information, etc.) within PCs ② Introduction of USB security keys on all mobile PCs (without the key, the computer will not start, and all files are encrypted).
8	Alteration of public web page	Alteration of index page.	Provider changed.
9	Disclosure of information	Regulations stipulating that Bcc: should be used when addressing customer are in place, however a part-time employee sent an e-mail with all customer addresses in the To: field.	An apology e-mail was sent, and the issue closed.
10	Disclosure of information	Recipients of information regarding a seminar were listed in the Cc: field, and a claim was received from recipients.	A claim was received from customers, and an apology e-mail was sent from representative. The incident was reported to relevant departments and directors. An apology e-mail in the name of the director in charge was also sent to the aggrieved, and then another apology e-mail sent to all members.
11	Disclosure of information	A bag containing a PC and customer documents was left on the luggage rack of a moving subway train, from where it was stolen. At a later date, the bag and documents were returned. In the period before the bag and documents were returned, suspicious contact was received from the person thought to be in possession of the bag, by the customers listed in the documents.	-

No	Type of Damage	Overview of Damage and Cause	Countermeasures and Response
12	Disclosure of information	Use of address forged for use in mail concealing sender's address, bounced mail, and spam.	-
13	Illegal access	Linux server non-operational.	-
14	Virus damage	-	Tightened restrictions on external PCs being connected to the internal company LAN.
15	Virus damage	A sales representative was carrying out a demonstration for a customer over the Internet, from where it is thought a virus infection occurred. After returning to the company, he connected to the internal LAN, whereupon the virus infected PCs that had not been patched.	The PCs that did not have the most up to date patches installed were removed from the internal LAN, and then the company confirmed that up to date virus definitions were installed.
16	Virus damage	Virus infection occurred just before the definition file was updated, however there was no damage (because of environment).	None. Anti-virus software from 2 companies already installed, with further measures being difficult.
17	Virus damage	Infection via e-mail from a third party. They trusted too much in virus checking, and when opening an e-mail attachment, sent more than 2100 e-mails out of the company.	Investigated logs. Gave a warning about virus infections.
18	Virus damage	PC infected when evaluating remote access. When this PC was connected to the internal company LAN, the servers (which did not have anti-virus software installed) were infected. Increased load on the network brought it down. Servers were disconnected from the network and the viruses removed.	-
19	Virus damage	Network stoppage.	Security patches applied to infected terminals.
20	Virus damage	ID and password created, and virus spread through PCs within the company.	-
21	Virus damage	Sent a large number of pings outside the company, stopping Internet access.	-
22	Virus damage	A large number of e-mails with viruses sent from an unspecified source. Each employee received between 50 and 100 such e-mails. No damage to other companies.	-
23	Virus damage	One of our PCs was connected to the customer's network, where it was infected with a worm (Welchia). After connection of the infected PC to our company's internal network, the infection was detected when a message was displayed on other PCs indicating its detection.	Update to most recent virus definition files, and make sure staff is fully aware of implementing real time scans on a regular basis.
24	Virus damage	Infection of unpatched PCs after a PC infected with MS Blaster was connected to the company LAN.	Stricter compliance with installation of patches.
25	Virus damage	Infection of a PC that did not have the most up to date Windows Updates, or the most up to date virus definition files installed.	Implementation of port filtering with outside the company. Currently in this state. Now able to adjust the port filtering system, and respond to emergencies.

No	Type of Damage	Overview of Damage and Cause	Countermeasures and Response
26	Virus damage	The definition file for the virus check on the mail server was received too late, and the virus was distributed to individual PCs. Some staff who received the e-mail absentmindedly ran the attached virus file, leading to three PCs becoming infected.	Condition of the accident and response policies publicized internally, and measures to prevent recurrence indicated.
27	Virus damage	Nachi and Welchia infection via internal LAN, as a result of Windows security patch MS03-026 not being installed on a Windows 2000 PC.	-
28	Virus damage	①Virus infection over the Internet ②This spread as a result of the most up to date Windows patches not being installed.	Obligation to install the most up to date Windows patches.
29	Virus damage	A large amount of virus e-mail received from outside the company, leading to a decrease in mail server response time.	-
30	Virus damage	① Infection by virus after installation of the OS, just before patches could be applied. ②An unidentified, unpatched notebook PC was connected with outside, leading to an infection.	-
31	Virus damage	A privately owned notebook PC that was infected with a virus was brought into the company, and connected to the internal LAN, whereupon the virus infection spread to PCs that had not been updated with Windows Update.	-
32	Virus damage	Infection detected, and no damage.	-
33	Virus damage	Internal LAN congestion.	-
34	Virus damage	A notebook PC was connected to the PC used for presentations, via PHS, and was infected.	-
35	Virus damage	A PC infected with a virus was connected to the internal LAN.	Patch applied, updating of virus definitions automated and improved.
36	Virus damage	①Because a PC had insufficient measures in place as regards security holes. ② Infection was fast; therefore detection and removal of the virus had no time to respond.	-
37	Virus damage	A PC infected with a virus, from outside the company was connected to the internal network, whereupon the PCs without security measures in place were infected.	-
38	Virus damage	Infected when browsing a web page.	Removed with anti-virus software, Windows Update run, and updated virus definition files installed.
39	Virus damage	-	Removed with anti-virus software, and scan of software on the PC carried out.
40	Virus damage	Infection by way of an e-mail attachment.	Removed with anti-virus software.

No	Type of Damage	Overview of Damage and Cause	Countermeasures and Response
41	Virus damage	Infection by way of floppy disk brought in from outside the company.	Most up-to-date version of anti-virus software installed upon the PC. The infected floppy disks (2) were discarded.
42	Virus damage	Instructions had been given that security patches from Microsoft were to be installed throughout the company; however infection of PCs that had not had these updates applied, and newly installed PCs occurred from a PC brought in from outside the company.	More thorough application of security patches and installation of anti-virus software. PC management tools, and improved monitoring of the firewall.
43	Virus damage	No particular damage. Only a large amount of e-mail sent to inboxes.	-
44	Virus damage	Large amount of e-mail retained on mail server. Transmission of e-mail significantly delayed.	-
45	Virus damage	A PC belonging to an employee who had been away on business was infected; infection spread to other PCs, leading to a DoS attack initiated, meaning that internal VoIP telephones could not be used.	Staff directed to always use the most up-to-date virus definition files, and to carry out virus checks on computers brought in from outside the company.
46	Virus damage	Transmission of e-mail with virus attachments to third parties.	Review of the period with which virus definition files are updated.
47	Virus damage	Reduced mail server response.	Replacement of mail server scheduled.
48	Virus damage	Two PCs were infected with the virus; however there was no actual damage.	More thorough prohibition on connecting to the Internet via dial-up, on PCs leased by the company.
49	Virus damage	The company's core server was infected, meaning stoppage of the system for half a day. Infection of the company headquarters' operations PCs meant an increase on load on the server of internal network. Stoppage of some devices connected to the network (resolved within several minutes to several hours).	-
50	Virus damage	Only transmission of files as attachments.	No particular damage.
51	Virus damage	Infection during a long vacation, and brought into the company's internal LAN. Confirmed on all PCs.	More thorough education of information security managers. System reconfigured in order that virus software is automatically updated.
52	Virus damage	Same as with other companies.	-
53	Virus damage	Most Windows 2000 and Windows XP computers connected to the company internal network were infected with MS Blaster, and the network became largely unusable. It is thought that the virus infection was as a result of connecting computers brought in from outside the company to the corporate network.	Increased the frequency of update for virus definition files on client PCs. Updated to the most recent version of Windows.
54	Virus damage	No immediate damage. It took time to determine the source of the infection. Only the time taken in order to reinstall OSes as a precautionary measure.	-
55	Virus damage	-	Implementation of external monitoring.

No	Type of Damage	Overview of Damage and Cause	Countermeasures and Response
56	Virus damage	Virus detected on 40 PCs	-
57	Virus damage	Virus infection through the opening of an e-mail attachment received from outside the company.	Company wide instructions to not open e-mail, and in particular e-mail with file attachments from suspicious sources (electronic bulletin board).
58	Virus damage	Abnormal traffic led to detection by the network monitoring system.	Direction that PCs that are brought back from a business trip be scanned for viruses before connection to the internal company LAN.
59	Virus damage	Infection with MS Blaster damaged quite a few PCs within the company. Instability in operation, irregular software startup, and shutdowns occurred.	-
60	Virus damage	-	Users connecting to outside networks prohibited from connecting to the internal company network.
61	Virus damage	-	Anti-virus software installed on the mail server and PCs.
62	Virus damage	Microsoft patches have not been applied, or their application was delayed, meaning that approximately 30% of client PCs were infected, or were restored prior to the infection (a message stating that the virus was detected, however that it could not be removed). (Patches were applied to the server, meaning it was not affected.)	-
63	Virus damage	Infection occurred before anti-virus software (virus definition files) could be applied. Random transmission of TCP packets meant that the internal company network was not usable.	-
64	Virus damage	A PC was connected to the Internet bypassing the proxy server, meaning that a virus was able to get into the company, where it spread.	-
65	Virus damage	Infected with Nodarg before a virus definition file was downloaded, however there was no effect on other PCs.	Notification that e-mail (file attachments) in English was to be deleted (Our company only carries out business within Japan).
66	Virus damage	There was an unusually large amount of traffic on the domestic center server LAN, and access from other sites was largely impossible. Affiliate companies servers were infected with MS Blaster, which attacked our network.	Affiliate companies that are connecting to our network are to have anti-virus measures in place by April, and that are at least as good as our own.
67	Virus damage	Client PCs that had not had Microsoft security patches applied were infected, (source of infection can not be determined), with several hundred client PCs connected to the LAN becoming infected, and the internal network coming to a stop as a result of a large number of ICMP packets, etc.	Studied improved application of security patches and event management.

No	Type of Damage	Overview of Damage and Cause	Countermeasures and Response
68	Virus damage	Anti-virus software was installed on the (leased) mail server and upon clients in the company, however at the time of the virus infection, the most up-to-date virus definition files had not been delivered from the software company. It was at this point that one employee opened a virus-laden e-mail attachment.	The infected client PC was immediately disconnected from the LAN, and kept as such until it was confirmed that the virus had been removed.
69	Virus damage	A PC brought into the company by an employee was connected to the network, from where the virus infection started. This resulted in the network slowing down, and becoming unusable. Several dozen PCs without the most up-to-date virus definition files installed were infected.	Improved updating and confirmation of virus definition files. Necessary security patches were installed.
70	Virus damage	Virus infection occurred on computers without the most up-to-date virus definition files installed, where damage spread.	Installation of software that check virus definition file updates, and upgrades of the server.
71	Virus damage	MS Blaster infection in the company LAN (in particular, PCs brought into the company, and those infected through using dial-up.)	-
72	Virus damage	PCs infected at on-site offices were brought back to the company, connected to the LAN, whereupon the infection entered into the company network, and spread.	-
73	Virus damage	A new virus got past the e-mail check and infected the LAN, where it then transmitted e-mail, spreading, and stopping the mail server.	Virus definition file updates changed from daily to twice daily.
74	Virus damage	Infection is thought to have originated from an individual's PC connected through a VPN. Infection occurred because the security patch addressing weakness MS03-026 had not been installed throughout the company.	Installation of MSUS (Microsoft Software Update Service) (improved security revisions). Improvement of the centralized monitoring system through a change in anti-virus software.
75	Virus damage	Anti-virus software detected virus in an e-mail from outside, with no actual damage occurring.	-
76	Virus damage	Increased network load.	Windows Update and virus check.
77	Virus damage	Infection occurred on a PC that had been used outside the office during the summer vacation, and at the end of the vacation, this was connected to the network, whereupon the company PCs were infected. Infected PCs did not have the most up-to-date virus definition files installed. 133 PCs infected. Additionally, the large number of packets transmitted from infected PCs bought down the L3 switch (three times in one day), making the headquarters' internal network unusable.	Virus definition files were updated for all clients. Guidelines regarding virus prevention for PCs to be used outside the company were created and distributed.
78	Virus damage	Infection occurred through the external server and through mobile PCs.	Improved training in rules. Implementation of site monitoring.

No	Type of Damage	Overview of Damage and Cause	Countermeasures and Response
79	Virus damage	Infection occurred through the opening of an e-mail with a virus-laden document attachment. The system was set up so that new virus definition files were automatically downloaded when the computer was turned on, however the newest definition file was not ready. A minor mail client was used, therefore there was no actual damage.	-
80	Virus damage	At infection occurred through an EDi circuit used with customers. Infection discovered on PCs with the latest virus definition files installed. No actual damage.	Configurations changed so that virus definition files are automatically updated and applied when the computer is turned on.
81	Virus damage	A computer that had connected to the Internet via dial-up and become infected with a virus was then connected to the internal company LAN.	OS updated, and client firewall software installed.
82	Virus damage	A PC without anti-virus software installed was infected. After that, several PCs connected to the network and did not have anti-virus measures in place were infected.	PCs that did not have anti-virus software installed were listed, and this software was installed in all the client PCs.
83	Virus damage	A system was in place in which virus definition files were updated over the LAN, however some mobile PCs did not have up-to-date definition files, and were infected.	Announcement made to the effect that mobile PCs are to connect to the LAN, and to update to the latest virus definition files. Mobile PCs are to have priority in using Windows Update.
84	Virus damage	There was a report that several offices had been infected with viruses.	-
85	Virus damage	Introduced through a non-e-mail route.	Announcement of guidance to apply patches within the company.
86	Virus damage	Company was advised from outside that it was sending spam e-mail.	-
87	Virus damage	An infected PC was brought into the company, and some unpatched servers were infected and stopped, whereupon the infection was discovered.	Patches applied, and IDS introduced.
88	Virus damage	Infection occurred through browsing Web mail. Checks for viruses are carried out on the mail server, however because Web mail uses HTTP, these checks were not carried out. The infection was confirmed after its spread within the company. Another cause of this was that virus definition files were not up-to-date.	-
89	Virus damage	Infected PC infected through shared files.	Anti-virus software also installed on the server.
90	Virus damage	A company PC was taken outside the company, where it was infected. Then connected to the company LAN. PCs within the company have anti-virus software installed, therefore damage was not extensive.	-
91	Virus damage	-	Changes to infrastructure in order to prevent illegal access to PCs.

No	Type of Damage	Overview of Damage and Cause	Countermeasures and Response
92	Virus damage	Virus-laden e-mails sent and received as a result of the MYDOOM virus. Infection occurred before virus definition files were updated.	Isolated using anti-virus software.
93	Virus damage	Internal company network connected to external PCs.	Installation of anti-virus software on all machines.
94	Virus damage	MO Disk brought from home.	Improved virus definition file updating. Prohibition on bringing in media from outside the company.
95	Virus damage	Anti-virus software was not installed on application PCs (servers, clients), a floppy disk was brought in from outside the company, and infection occurred, almost stopping operations.	Operations PCs installed with the same anti-virus software as business PCs.
96	Virus damage	Erroneous PC operation.	Removed with anti-virus software, notification to the whole company.
97	Virus damage	The route of infection is unclear, however it is confirmed that the network traffic increased as result of a virus infection. The next day, PCs in all offices were turned off, and anti-virus software delivered. However, this did not stop the virus infection, and over the three-day holiday, countermeasures were studied. At the beginning of work, anti-virus software measures were again implemented throughout the company, and recovery was completed the next month.	Anti-virus software that could confirm both the status of anti-virus software installation, and of virus infection upon each terminal was updated. Users were given an explanation of the use of Windows folder sharing, and users of IIS were asked to apply security patches. A filter was added to the proxy server to prevent it requesting ".eml" files.
98	Virus damage	PCs that were thought to have been damaged, and those LAN segments were removed from the company network, the virus was removed with anti-virus tools, virus checks were carried out on peripheral PCs, and measures were taken. It is thought that the infection came about before the most up-to-date a virus definition files could be applied.	Immediate application of virus definition files.
99	Virus damage	PCs were frequently abnormally terminating. Communications from certain offices to their headquarters were slowed, leading to hindrance in using the Internet and e-mail.	Faster patch application. Faster updating of virus definition files.
100	Virus damage	A PC for use outside the company was infected outside the company, and the virus infection spread within the company when it was connected to the internal network.	Regulations implemented to the effect that PCs for use outside the company are to carry out a virus check using the most up-to-date virus definition files before connecting to the internal company network.
101	Virus damage	As a result of a receiver of forwarded e-mail becoming infected, large quantities of e-mail were sent to addresses in the address book.	Security measures made compulsory for receivers of forwarded e-mail.
102	Virus damage	Careless connection of an infected PC.	Study into the introduction of automatic distribution tools, and enhancement of the IT risk management system.

No	Type of Damage	Overview of Damage and Cause	Countermeasures and Response
103	Virus damage	Increased load upon the WAN from locations that are connected with a low speed network led to being unable to connect to the headquarters' server.	Ensured correct Windows Update for all PCs and Windows servers.
104	Virus damage	A PC taken outside the company was connected to the internal company LAN. PCs from contracted companies brought into the company.	Strengthening of rules regarding taking PCs out of, and bringing PCs into the company. Internal notification. Simultaneous checking of the status of all PC usage.
105	Virus damage	A large amount of e-mail arrived from an overseas subsidiary, significantly slowing the speed of the network.	-
106	Virus damage	OS security patches for computers attached to the internal company network were not set to automatically update. An employee who had been overseas on business returned to Japan, bringing back the infection.	-
107	Virus damage	Output of our large amount of garbage characters from the printer.	-
108	Virus damage	A prohibited personal PC was connected to the internal company network, where the infection spread.	-
109	Virus damage	Detected using virus monitoring software. (most up-to-date definition files and anti-virus vaccination were used, therefore there was no damage)	OSes patched.
110	Virus damage	Virus infection occurred through a PC taken outside the company being connected to the Internet. This was connected to the internal company network accidentally, where the virus infection spread.	More thorough anti-virus software installation and training.
111	Virus damage	An individual's infected personal PC was connected to the company LAN.	-
112	Virus damage	It is thought that one employee connected to a different provider, bypassing the company's firewall.	Patches installed, internal reports.
113	Virus damage	A mobile PC was infected, resulting in unstable operation.	Changed the frequency of virus definition updates on anti-virus software management server from daily to 10 times per day.
114	Virus damage	-	Implementation of Windows Update, anti-virus vaccination.
115	Virus damage	Virus downloaded through an Internet browser, and this spread through a part of the Microsoft network.	Costs of anti-virus countermeasures for the internal systems only.
116	Virus damage	Infection occurred from a PC connected using dial-up, different to the company. Other offices had in place anti-virus measures, however because these were not fully in place at the office concerned, many PCs were infected. Anti-virus software was installed quickly, and the virus removed. The infection did not spread outside the company.	The person who connected using dial-up was instructed to not do so.

No	Type of Damage	Overview of Damage and Cause	Countermeasures and Response
117	Virus damage	Virus introduced into the internal company LAN by a PC that had been taken outside the company.	-
118	Virus damage	Infection occurred before the most up-to-date virus definition files could be obtained from the software vendor (virus received by e-mail from a business partner).	-
119	Virus damage	An infected PC that had been brought in from outside the company was connected to the LAN without permission, whereupon the virus infection spread to PCs that did not have anti-virus software (purchased separately by each department) in place. Pinging broadcast addresses placed a large load upon at the factory procon server (Windows NT), which crashed.	Insured full installation of anti-virus software on PCs that did not have this installed (company briefing, checks with individuals).
120	Virus damage	Virus spread faster than updated virus definition files to the gateway server.	-
121	Virus damage	A computer that had been out of the company during the summer vacation was connected to the internal company network, infecting it.	-
122	Virus damage	Infection before the most up-to-date virus definition files were installed. Luckily, the infection did not spread, and responses were taken quickly.	Most up-to-date virus removal tools automatically distributed by the server.
123	Virus damage	-	Compulsory distribution of virus removal files. Currently creating a patch application mechanism.
124	Virus damage	Documents within the PC deleted.	-
125	Virus damage	A PC infected with the virus was connected to the internal LAN, and as a result of Windows machines which did not have properly patched security holes, and of PCs that did not have up-to-date virus definition files (automated at this company), an unusual amount of traffic was transmitted over the LAN, bringing the whole company LAN down (three locations). This also affected one overseas location.	Constructing a server in order to close Windows security holes. Strengthening remote PC anti-virus measures.
126	Virus damage	An e-mail with a virus attachment had a fabricated sender, therefore the source is unknown. Infection from within the company? A third-party?	-
127	Virus damage	Malfunction in the WAN between headquarters and a branch. Internet service temporarily suspended in order to prevent spread outside the company.	Study into automation of applying security patches.
128	Virus damage	Infection as a result of connecting to the Internet outside the company (overseas, thought to be in China). Infection of the company network occurred on return to Japan, and connecting to the LAN.	Creation of procedure manual for removing PCs from the company (improved anti-virus measures).

No	Type of Damage	Overview of Damage and Cause	Countermeasures and Response
129	Virus damage	After detection by the anti-virus software on clients, patches were applied to the server. No damage occurred.	-
130	Virus damage	A PC that had connected to the Internet using dial-up was then connected to the internal company LAN, from where the infections started.	Development of a company wide mechanism for automatically updating to the latest virus definition files. Put into practice of a system in which “critical” Microsoft security patches must be installed.
131	Virus damage	A sales representative mistakenly opened a virus-infected file attached to an e-mail. The PC upon which they were working had anti-virus software installed, but it was turned off.	Telephone calls were made in apology to the contacts whose e-mail addresses had been registered in the PC. Infected e-mails were sent to the total of five e-mail addresses.
132	Virus damage	It is thought that a mobile PC was connected to a home network, where, as the anti-virus software that had been stopped, it was infected. After that, the infected PC was connected to the internal company LAN, resulting in a total of 57 PCs becoming infected.	-
133	Virus damage	An external network was connected to the internal network, whereupon a virus was introduced. Most of the company was infected.	Improved implementation of Windows Update. Full prohibition on connecting external networks to the company’s internal network.
134	Virus damage	A company PC was taken home, where it was infected upon being connected to the Internet. This computer was brought back to the company and connected to the network, whereupon the infection quickly spread to PCs that did not have Microsoft security patches installed, rendering the network unusable. One month before this, there had been a notice to install security patches on the intranet, however more than half of the PCs had not done so.	Introduction of automated security patching tools.
135	Virus damage	Infection with MS Blaster caused a slowdown in the network.	Improved countermeasures system.
136	Virus damage	Attack on UDP port 1434 because of SQL Slammer.	Review of network settings.
137	Virus damage	Proliferation of the MS Blaster worm within the company, infecting the system.	Improvement in the application of the recovery module process.
138	Virus damage	The relevant virus (Welchia) had only just been discovered the day before the infection, therefore measures to counter it were not ready. It is thought that Internet connection servers (Web servers, etc), which cannot be blocked by the firewall, were infected, whereupon the infection spread to the company’s internal network.	① Employment of an automated update system for virus definition files ② Improved management of PCs connected to the internal company LAN ③ Development of restoration procedures ④ Establishment of a threat management system.

8. Conclusion

In recent years, Japan has seen many investigations related to Internet use and vulnerabilities, and the main focus of agencies such as the Information-technology Promotion Agency (IPA) and the National Police Agency, and of this questionnaire, are the “amounts of damages.” However, at the same time, according to responses received in this investigation, definition of the range of damages, and methods to understand these have not yet been fixed, therefore there are still many areas in which direct questioning of representatives at companies is needed.

In this working group, while compartmentalizing investigation parameters in the questionnaire, we were able to carry out an investigation and study into incidents, which covered a much larger number of companies than last year, thanks to assistance from members of JNSA and from RISTEX.

The aims of this investigation were to understand the current condition of information security incidents, and to collect important basic information regarding risk management in the information security field.

The investigation carried out by JNSA comprised direct interviews besides questionnaires, and this produced very detailed results. In addition, it had as its goals both the construction of a model to estimate amounts of damage, and understanding the effect that having provisions in place affected damage.

When carrying out the investigation, we carried out work to review answers to the questionnaire, however it was the case that in both the questionnaire and the interviews, there were many companies that could not answer questions.

We received a great deal of cooperation as regards our questionnaire and the interviews, and we would like to express our appreciation to those who took the time to assist us with these.

Meanwhile in Section 2 (supplement), carried over from last year, this investigation studied the announcement of 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 enterprise value, namely their share prices.

This year's model for estimating the amount of compensatory damages resulting from disclosed information was mainly focused around “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.

This report has become a yearly occurrence, and in the investigation and the creation of the report, we would like to express our most heartfelt thanks to both the project members in a range of industries that we have called upon at this busy end-of-year period, and to the people at the companies who assisted us with the interviews for giving us that time.

In addition to this, we would like to offer our gratitude to the “Security Systems Office, Community Safety Planning Division, National Police Agency” who has this year offered us considerable advice.

Please refer to the activities of this working group and to this report. We hope that this is in some way useful in

improving information security activities, and in increasing future levels of information security.

9. Reference Materials

9.1 Questionnaire Sheet (Implemented by JNSA)

Questionnaire into Information Security Damage (Implemented by JNSA)

This investigation is aimed at information security managers (representatives). We would be most grateful if you could forward this to the relevant parties. Furthermore, please fill in answers directly on these pages.

A Questions regarding the current condition of your company's business.

A-1 Tell us the main industry in which your company does business (circle your selection).

1	Finance (Banking, Insurance, Securities, etc.)		6	Education/ Mass Media	
2	Medical/ Pharmaceutical		7	Construction	
3	Transportation		8	Food Service/ Retail	
4	Energy		9	Other Services	
5	Information/ Communications		10	Other	

A-2 Annual Sales and Number of Employees

1	Average Sales (¥millions)		(¥millions)
2	Employees		

A-3 How many offices/ locations does your company have? (Select one by circling your answer)

1	1		6	100 to 299	
2	2		7	300 to 999	
3	3 to 9		8	1000 to 2999	
4	10 to 29		9	3000 and above	
5	30 to 99				

B Please tell us about your company's information systems.

B-1 How many personal computers (PCs) are in use at your company?
(Select one by circling your answer)

1	1 to 29		5	1000 to 2999	
2	30 to 99		6	3000 to 9999	
3	100 to 299		7	10000 to 29999	
4	300 to 999		8	30000 and above	

B-2 What is the level of Internet mail usage in your company? (Select one by circling your answer)

1	None		4	Generally available, but limitations on type and size of attachments	
2	Email on specialized terminals only		5	Generally available with no particular limitations	
3	Generally available, but attachments not permitted				

B-3 What is the level of Web browser usage in your company? (Select one by circling your answer)

1	None	
2	Web access on specialized terminals only	
3	Generally available, with restrictions on permissible sites	
4	Generally available with no particular limitations	

B-4 What percentage of your company's PCs (clients) have Email/ Web access?

1	Internet mail (%)		%
2	Web browsing (%)		%

B-5 How much of your company's work activities have been computerized? Indicate in general terms your company's reliance on computer systems. (Select one by circling your answer)

1	Most work activities have been computerized	
2	Many work activities have been computerized	
3	Approximately half of work activities have been computerized; half of work activities are conducted manually	
4	Only a few work activities have been computerized; most work activities are still conducted manually	
5	Almost none of our operations are computerized, with most operations carried out without computers as before	

<Other>

C Please tell us about information security management at your company.

C-1 Does your company have formal information security rules? (Mark all that apply)

1	None	
2	Formal information security policies in place	
3	Information security rules included in workplace regulations	
4	Information security rules included in rules related to protecting private information	
5	Information security rules included in other rules/ regulations	
6	Formal information security work procedures rules in place	
7	Not sure	

<Other>

C-2 ***FOR THOSE WHO RESPONDED, "1. NONE" TO QUESTION C-1:***

What is the greatest reason for not establishing information security rules? (Select one by circling your answer)

1	Management does not see the need	
2	Locality/ department in charge does not see the need	
3	Low level of necessity among those in the industry/ business type	
4	Not enough resources (personnel, capital) within the company	
5	Not sure	

<Other>

C-3 ***Only to be answered by respondents who did not answer "1 No" for question C-1.***

In what year did your company first establish information security rules/ procedures?

Year Established:	

C-4 ***Only to be answered by respondents who did not answer "1 No" for question C-1.***

Does your company have a procedure for reviewing information security rules? (Mark all that apply)

1	No policy for reviewing information security rules	
2	Review policy in place (frequency not defined)	
3	Review policy in place (reviewed at least once per year)	
4	Review policy in place (reviewed less than once every 24 mos.)	
5	Not sure	

<Other>

C-5 When was the last time an information security policy review (or initial implementation) took place? (Mark all that apply)

1	Within the past 12 mos.	
2	Within the last 24 mos.	
3	Greater than 24 mos. Ago	
4	Not sure	

<Other>

C-6 How many employees are assigned to information security management?

1	Full-time (no.)	
2	Part-time with other job duties (no.)	
3	Officer assigned to oversee information security(check if appointed)	

C-7 System for communicating information security mishaps and incidents throughout the company. (Mark all that apply)

		Existence of system	Established within a year	Established after an accident
1	Communications system established and in place			
2	Established department responsible for determining occurrences of security mishaps, incidents			
3	Each department has a designated person responsible for communicating information security incidents			
4	Almost all employees understand the communications system			
5	The communications system is functioning properly			

C-8 Information security considerations when selecting or contracting with business partners. (Mark all that apply)

1	No particular consideration given	
2	Special consideration given to business partners with well-known business and service levels	
3	Special consideration given to business partners who understand information security (BS7799, Privacy Mark, etc.)	
4	Special consideration given to business partners who have a formal information security policy	
5	Special consideration given to business partners who undergo information system audits	
6	Require non-disclosure agreements	
7	Require contracts/ agreements defining Service Levels (SLA)	
8	Perform information security audits on business partners	
9	Not Sure	

<Other>

C-9 Information security considerations when accepting contract or full-time employees. (Circle all that apply)

1	No special considerations	
2	Require contracts related to handling information (non-disclosure agreements, etc.)	
3	Conduct ongoing information systems education	
4	Conduct ongoing information security education	
5	Not sure	

<Other>

C-10 Factors included in damage response plan. (Circle all that apply)

		Existence of planning and system	Established within a year	Established after an accident
1	Confirm status for each type of damage incurred			
2	Personnel responsible for confirming damage			
3	Internal system for communicating incident damages			
4	Outside parties to be contacted (vendors, industry groups, consultants, etc.)			
5	Method for conveying information to employees, level of detail to be provided			
6	Method for conveying information to outside parties, level of detail to be provided			
7	Confirmation checklist for system recovery			
8	Not defined			
9	Not sure			

<Other>

C-11 How do you gather information security-related news? (Circle all that apply)

1	No formal news gathering conducted	
2	Periodically review security-related information on OS and critical software vendor websites	
3	Review websites of organizations providing security information (IPA/ ISEC, etc.)	
4	Subscribe to security information news service	
5	Not sure	

<Other>

C-12 Application of patches to ensure network server security. (Select one by circling your answer)

1	No patches applied	
2	Periodically confirm release of new patches, always keep servers up-to-date	
3	No formal system of confirming new patch releases; application of new patches left to the discretion of the server administrator	
4	Patches not applied unless a problem occurs	
5	Not sure	

<Other>

C-13 Indicate whether certification is "In Planning" or "Already Obtained." Circle all that Apply.

	Name	Not planned	In planning	Acquired	Year acquired
1	ISMS (BS7799)				
2	ISO/IEC 15408				
3	Privacy Mark				
4	CMM (Capability Maturity Model)				
5	Not sure				

<Other information security related certification (Name)>

C-14 Has your organization conducted system audits and/or vulnerability tests (penetration tests) within the last 12 months?

	Item name	System monitoring (Mark where implemented)	Inspection of vulnerabilities (Mark where implemented)
1	Internet		
2	Intranet		
3	Extranet		
4	Dedicated internal network		

<Other>

C-15 Does your company have a formal information security budget? (Select one by circling your answer)

1	No	
2	Budgeted separately as information security costs	
3	Budgeted as a subset of the information systems budget	
4	Budgeted as a subset of "Other"	
5	Not sure	

<Other>

C-16 <u>If you marked any category 2 through 4 above, please provide some general figures</u>.

Average budgeted amount(¥ ('0,000))		¥ ('0,000)
Ratio of information systems budget (%)		%
Change from last year's budget (¥ ('0,000))	+, −	¥ ('0,000)

C-17 Allocation of information security budget. (Circle all that apply)

1	No budget		6	Security administrator training	
2	Security hardware purchases		7	Employee training/ education	
3	Security software purchases		8	Obtaining security-related certifications	
4	Security hardware maintenance		9	Expense of maintaining certifications	
5	Security software maintenance		10	Not sure	

<Other>

C-18 What systems have you implemented to insure information security?

(Circle all that apply)

1	Firewalls		5	Implement anti-virus software on all client PCs	
2	Intrusion Detection System (IDS)		6	Use encryption tools (S/MIME, PGP)	
3	SET UP DMZ SEGMENTS		7	Implement virus checks on the proxy server	
4	Virus checks on the mail server		8	Not sure	

<Other>

C-19 Countermeasures used to prevent private information disclosure (Circle all that apply)

		Installed items	Installed within a last year	Installed after an incident
1	Email monitoring			
2	Webmail monitoring			
3	Server access restrictions			
4	External phone line monitoring			
5	Restrictions on removing documents			
6	Restrictions on removing notebook PCs (office automation equipment)			
7	Restrictions on bringing in notebook PCs (office automation equipment), LAN connection restrictions			
8	Restricted access to server rooms			
9	Restrictions on removing floppy discs, USB and other memory media			
10	Standards for destroying floppy discs, USB and other memory media			
11	Standards for destroying PCs (office automation equipment)			
12	Encrypt document data, email using key encryption systems			
13	Authentication system using a personal authentication device (access, entry to/ exit from rooms)			
14	Authentication system using a biometrics system (access, entry to/ exit from rooms)			

<Other>

C-20 Information security training/ education (Circle all that apply)

1	Virus/ worm countermeasures		6	Emergency response	
2	Password management education		7	Social engineering countermeasures	
3	Protection of personal information		8	PC settings/ operation	
4	Protection of proprietary information		9	Network knowledge	
5	“Netiquette” (Internet etiquette)				

<Other>

C-21 Ongoing information security education over the previous 12 months (Circle all that apply)

	Training/ Education Content	No of employees	Times per year
1	Education for all employees (User training)		
2	Management training		
3	Specialist training		

C-22 Current or planned information security measures (Circle all that apply)

		Implemented	Future			Implemented	Future
1	Prepare security-related documentation			9	Provide security information to all employees		
2	Define internal systems for information security			10	Incident/ accident response training		
3	Heightened security training for information systems personnel			11	Virus checks on servers		
4	Heightened security training for all employees			12	Virus checks on client PCs		
5	Obtain security-related certifications			13	Employee personnel who possess information security skills		
6	Implement systems for obtaining security-related certifications			14	Use ASPs (Application Service Providers) and IDCs (Internet Data Centers)		
7	Gather security-related information			15	Use contract employees		
8	Conduct system audits						

<Other>

D Please answer regarding damage that has occurred in your company's information systems.

You may leave any questions that you have difficulty responding to blank, however please tell us in broad terms about your overall circumstances and about sums as much as possible.

① Please refer to the next page for damage codes.

② The supplement has enough room for 4 incidents, however please copy the answer sheets if these are insufficient.

<Example>

A-1 Please select from the Damage Code No. list.	Damage Code [1]		
B-1 Date of occurrence	Year: 2003 Month: February Date: 10 Hour: 12 Min: 00		
C-1 How did you find out about the damage? Check applicable fields (multiple selections permitted).			
1) Notification from the person concerned (*1)		(*1) Infected employee, aggrieved or person in error, etc. (*2) Logs, monitoring cameras, etc. Please be specific.	
2) Notification from a business partner	X		
3) Notification from a third party (not a business partner)			
4) Detected in mail monitoring			
5) Detected by the firewall or IDS			
6) Other (*2)	Indicated by a customer to whom e-mail had been sent, an internal investigation carried out, and the machines identified.		
D-1 Please give a brief explanation of the cause of the incident (please write freely).			
Infection occurred as a result of an employee opening an e-mail infected with a virus. This was copied to the shared drives of the department to which the employee belonged, infecting their PCs. All employees are supposed to regularly update virus definition files; however, because the employee concerned and other members of their department had been lax in this, most of the PCs in their department were infected. Anti-virus software prevented the infection spreading to other departments' servers, however the transmission of e-mail outside the company could not be prevented, with approximately 300 e-mails being confirmed as sent outside the company.			
E-1 What was the extent of the damage? Check those items applicable, and where possible, fill in the number of locations affected (multiple selections permitted).			
1) Damage to headquarters' internal LAN	X		
2) Damage spread to branches and offices	X	[5] locations	
3) Damage spread to business partners	X	[3] locations	
4) Damage spread to other outside parties apart from business partners		[ ] locations	
5) Other	[ ]		
E-2 Approximately how many number of PCs within your company that were affected?			
1) External server	[1] computers		
2) Internal server	[4] computers		
3) Client PC	[50] computers		
E-3 Approximately how many employees were affected?	[80] people		
E-4 Approximately how long was the system stopped?	[12] hours		
E-5 Approximately what are sales from that system? (*3)	¥[20,000,000]		
*↑(*3) A paid service that sells products through a web site. Please give the amount of sales obtained directly through that system in the period of one year.*			
E-6 Approximately how much opportunity loss was there as a result of the system stoppage? (estimated lost earnings and profits)	¥[200,000]		
F-1 Approximately how long did it take until recovery from the time a response was commenced?	[24] hours		
F-2 Approximately how many people were involved in the response?	[20] people		
F-3 Approximately how much are your personnel costs per person per day?	¥[25,000]		
F-4 What is the cost of substituting other measures in order that your company can continue business?	¥[100,000]		
Please give a breakdown of substitutes. (e.g. substitute facilities, costs of manual processing, etc.)			
Continued business operations by way of telephone, fax, etc. It required significant amount of time, and there were many transactions unfinished.			
F-5 What was the approximate cost required to recover data?	¥[100,000]		
F-6 What was the approximate cost of other measures for recovery?	¥[Unclear]		
Please give a breakdown.			
Input of data for the transactions that were conducted by way of telephone, fax, etc.			
G-1 In the event of compensatory damages or reparations, approximately how much were these?	¥[Unclear]		
G-2 In the event that there were other costs, please give this sum as well.			
1) Advertised apology	¥[5,000,000]	3) Apology visit	[10] manpower per day
2) Notice of apology	¥[50,000]	4) Other	[Unscheduled evening overtime - ¥300,000]
H What was your response after the incident?			
-Implemented a system to confirm that the most up-to-date virus definition files were installed. -As well as physically removing LAN cables, we turned off the power to wireless access points as emergency measures upon discovering the problem.			

<List of Damage Codes>

Damage Code No.	Type	Type of Damage	Summary
1	Worm	KLEZ	Works in a similar way to Nimda, that reached epidemic proportions, in that it propagates through the mail and shared drives, and in the same way, creates a virus files from executable program files. This is a direct action virus that can run from the preview window. Some of them inserts text strings such as “Patch to fix Code Red” in either the title or body, encouraging users to open the file.
2	Worm	SOBIG	A Trojan horse program that is classified as a worm. It searches for e-mail addresses from files with a range of defined file extensions, and then uses its own SMTP engine to transmit a copy of itself to these recipients. A sub-variant furthers its own infection using read-writable Windows shared networks.
3	Worm	BUGBEAR	A Trojan horse program that is classified as a worm. Distributes itself by making a copy of itself and sending this by e-mail (mass-mailing activity), and distributing copies of itself on shared drives. When it is active, it tries to forcibly close anti-virus software and to leak information, and it also has functionality as a backdoor cracking tool.
4	Worm	MS Blaster	A Trojan horse program that exploits a vulnerability in Window's RPC service to gain access. Its main feature is that instead of requiring active input, such as accessing the Web on the part of the user, it is strong enough to infect PCs that are merely attached to the Internet. When a PC becomes infected, it shows erratic behavior such as suddenly restarting. Additionally, upon a specified date, it launched a DoS attack against windowsupdates.com.
5	Worm	Sircam	Works in a similar way to Sobig, in that it searches for e-mail addresses, and attaches itself to mails, and then transmits these; however, the attached file includes both a copy of itself and a random file selected from the infected computer, which means that at first glance, the attached file appears innocuous. In addition to via e-mail, Sircam can also spread through shared drives of Windows.
6	Other virus damage		Damage other than that detailed above. Please fill in details of virus names in the status of incidents field.
7	Theft or loss of PC/PDA		Damage such as the disclosure of personal information resulting from loss of a PC or PDA.
8	Data deleted or system brought down through erroneous operation		Trouble resulting from human error, such as erroneous operation.
9	Other illegal access		Illegal access from someone outside the company without access rights.
10	Service stoppage through DoS or other attack		Slow down or stoppage in service resulting from concentrated access.
11	Alteration of public Web page		Illegal alteration of web page by someone outside the company.
12	Disclosure of information		Includes improper removal of information on media.
13	Other		☆ We ask that you fill in details in the questionnaire sheet.

D-1 Status of Incident

A-1 Please select from the Damage Code No. list.			Damage Code [ ]	
B-1 Date of occurrence	Year:	Month:	Date:	Hour: Min:
C-1 How did you find out about the damage? Check applicable fields (multiple selections permitted).				
1) Notification from the person concerned (*1)			(*1) Infected employee, aggrieved or person in error, etc. (*2) Logs, monitoring cameras, etc. Please be specific.	
2) Notification from a business partner				
3) Notification from a third party (not a business partner)				
4) Detected in mail monitoring				
5) Detected by the firewall or IDS				
6) Other (*2)				
D-1 Please give a brief explanation of the cause of the incident (please write freely).				
E-1 What was the extent of the damage? Check those items applicable, and where possible, fill in the number of locations affected (multiple selections permitted).				
1) Damage to headquarters' internal LAN				
2) Damage spread to branches and offices			[ ] locations	
3) Damage spread to business partners			[ ] locations	
4) Damage spread to other outside parties apart from business partners			[ ] locations	
5) Other	[ ]			
E-2 Approximately how many number of PCs within your company that were affected?				
1) External server	[ ] computers			
2) Internal server	[ ] computers			
3) Client PC	[ ] computers			
E-3 Approximately how many employees were affected?	[ ] people			
E-4 Approximately how long was the system stopped?	[ ] hours			
E-5 Approximately what are sales from that system? (*3)	¥[ ]			
†(*3) A paid service that sells products through a web site. Please give the amount of sales obtained directly through that system in the period of one year.				
E-6 Approximately how much opportunity loss was there as a result of the system stoppage? (estimated lost earnings and profits)	¥[ ]			
F-1 Approximately how long did it take until recovery from the time a response was commenced?	[ ] hours			
F-2 Approximately how many people were involved in the response?	[ ] people			
F-3 Approximately how much are your personnel costs per person per day?	¥[ ]			
F-4 What is the cost of substituting other measures in order that your company can continue business?	¥[ ]			
Please give a breakdown of substitutes. (e.g. substitute facilities, costs of manual processing, etc.)				
F-5 What was the approximate cost required to recover data?	¥[ ]			
F-6 What was the approximate cost of other measures for recovery?	¥[ ]			
Please give a breakdown.				
G-1 In the event of compensatory damages or reparations, approximately how much were these?	¥[ ]			
G-2 In the event that there were other costs, please give this sum as well.				
1) Advertised apology	¥[ ]	3) Apology visit	[ ] manpower per day	
2) Notice of apology	¥[ ]	4) Other	[ ]	
H What was your response after the incident?				

9.2 Questionnaire Sheet (Implemented by RISTEX)

Questionnaire into Information Security Damage (Implemented by RISTEX)

This investigation is aimed at information security managers (representatives). We would be most grateful if you could forward this to the relevant parties. Furthermore, please fill in answers directly on these pages.

A Please tell us about your company's business

A-1 Tell us the main industry in which your company does business (circle your selection).

1	Finance (Banking, Insurance, Securities, etc.)		6	Education/ Mass Media	
2	Medical/ Pharmaceutical		7	Construction	
3	Transportation		8	Food Service/ Retail	
4	Energy		9	Other Services	
5	Information/ Communications		10	Other	

A-2 Annual Sales and Number of Employees

1	Annual turnover (¥millions)		(¥millions)
2	No. of employees		

A-3 How many offices/ locations does your company have? (Select one by circling your answer)

1	1		6	100 to 299	
2	2		7	300 to 999	
3	3 to 9		8	1000 to 2999	
4	10 to 29		9	3000 and above	
5	30 to 99				

B Please tell us about your company's information systems.

B-1 How many personal computers (PCs) are in use at your company?
(Select one by circling your answer)

1	1 to 29		5	1000 to 2999	
2	30 to 99		6	3000 to 9999	
3	100 to 299		7	10000 to 29999	
4	300 to 999		8	30000 and above	

B-2 What is the extent of your company's Internet mail usage? (Select one by circling your answer)

1	None		4	Generally available, but limitations on type and size of attachments	
2	Email on specialized terminals only		5	Generally available with no particular limitations	
3	Generally available, but attachments not permitted				

B-3 What is the level of Web browser usage in your company? (Select one by circling your answer)

1	None	
2	Web access on specialized terminals only	
3	Generally available, with restrictions on permissible sites	
4	Generally available with no particular limitations	

B-4 What percentage of your company's PCs (clients) have Email/ Web access?

1	Internet mail (%)		%
2	Web browsing (%)		%

B-5 How much of your company's work activities have been computerized? Indicate in general terms your company's reliance on computer systems. (Select one by circling your answer)

1	Most work activities have been computerized	
2	Many work activities have been computerized	
3	Approximately half of work activities have been computerized; half of work activities are conducted manually	
4	Only a few work activities have been computerized; most work activities are still conducted manually	
5	Almost no work activities have been computerized; most work activities are conducted manually	

<Other>

B-6 How many employees are assigned to information security management?

1	Full-time (no.)	
2	Part-time with other job duties (no.)	
3	Officer assigned to oversee information security (check if appointed)	

B-7 Does your company have a formal information security budget? (Select one by circling your answer)

1	No	
2	Budgeted separately as information security costs	
3	Budgeted as a subset of the information systems budget	
4	Budgeted as a subset of "Other"	
5	Not sure	

<Other>

B-8 <u>If you marked any category 2 through 4 above, please provide some general figures</u>

Average budgeted amount(¥millions)		(¥millions)
Ratio of information systems budget (%)		%
Change from last year's budget(¥millions)	+, −	(¥millions)

B-9 What systems have you implemented to insure information security?

(Circle all that apply)

1	Firewalls		5	Implement anti-virus software on all client PCs	
2	Intrusion Detection System (IDS)		6	Encryption tool usage (S/MIME, PGP)	
3	SET UP DMZ SEGMENTS		7	Implement virus checks on the proxy server	
4	Virus checks on the mail server		8	Not sure	

<Other>

B-10 Does your company have formal information security rules? (Circle all that apply)

1	No	
2	Formal information security policies in place	
3	Information security rules included in workplace regulations	
4	Information security rules included in rules related to protecting private inforamation	
5	Information security rules included in other rules/ regulations	
6	Formal information security work procedures rules inplace	
7	Not sure	

<Other>

B-11 Indicate whether certification is "In Planning" or "Already Obtained." Circle all that Apply.

	Name	Not planned	In planning	Acquired	Year acquired
1	ISMS (BS7799)				
2	ISO/IEC 15408				
3	Privacy Mark				
4	CMM (Capability Maturity Model)				
5	Not sure				

<Other information security related certification (Name)>

B-12 Information security audits, education and training (Circle all that apply)

1	*Information security audit carried out by an external audit organization*	
2	*Internal audit of information security carried out by internal party*	
3	*Training of all employees in information security carried out*	
4	*The above measures are carried out as a part of personal information protection*	

C Please answer regarding damage that has occurred in your company's information systems.

<Below, same as questionnaire implemented by JNSA>