Fiscal 2002
Information Security Incident Survey Report

＜Section One＞

Information Security Incident Survey and Damage Calculation Model

JAPAN NETWORK SECURITY ASSOCIATION

March 31, 2003

Contents

JNSA SEISAKU COMMITTEE SECURITY INCIDENTS INVESTIGATION WORKING GROUP

Working Group Leader

Mr. Tadashi Yamamoto SOMPO JAPAN RISK MANAGEMENT, INC.

Working Group Members (No Particular Order, Titles Omitted)

Hisamichi Otani NTT DATA CORPORATION
Hironori Omizo JMC Co., Ltd
Kenji Okada ELNIS Technologies Co., Ltd.
Masahiko Kusaka SOMPO JAPAN RISK MANAGEMENT, INC.
Tomohisa Sashida THE TOKIO MARINE RISK CONSULTING CO., LTD.
Tomoharu Sato Internet Research Institute, Inc.
Kiyoshi Nagashima THE TOKIO MARINE AND FIRE INSURANCE CO., LTD.
Takashi Nemoto HUCOM, Incorporated
Yukihiro Matsutani HUCOM, Incorporated
Shiro Maruyama Little eArth Corporation
Naoyoshi Yasuda dit CO., LTD.
Eiji Yamada dit CO., LTD.

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

1. Introduction

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

<About Section One>

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

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

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

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

<About Section Two>

The Calculation Model used here considers not only damages related to information security systems, but also refers to damages such as those related to compensatory legal reparations, etc.

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

The "Calculation of Compensation for Damages" and "Influence on Share Prices" suggested in this report represent a calculation method proposed by this Working Group, and are in no way meant to be definitive.

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

2. Objectives

A litany of modern-age technology issues have warranted increasing attention from the IT industry and society as a whole, from the 9/11 terrorist attacks, to the almost daily occurrence of new computer viruses and accidental exposure of private information, to systems problems during and after systems integration projects, to cyber terrorism and the security of vital infrastructure. And more than ever, security incidents compromising information systems—now an indispensable part of our business and societal infrastructure—are demanding a fresh approach to response and prevention in light of current circumstances and past incidents.

Unfortunately, it is very difficult to find any compiled data related to specific cases of, and damage costs for, such security incidents. Major Reasons for this lack of information include the rare public disclosure of the nature of these incidents, and the vague definition of “damages” incurred.

The same can be said about information related to preventive and remedial measures, with no common definition of “preventive,” and a dearth of information related to costs.

Section One of this report serves as a compilation of information collected by means of questionnaire and in-person interviews, providing an understanding of the current circumstances related to cyber terrorism and major infrastructure security incidents in Japan. Here, we have taken the model proposed last year for estimating the costs of security incidents and investment in information security, and added what we have learned from this year’s research to build a more detailed model for 2002, measuring the understanding and effect of “Risk Size (scale of damages)” and “Scope of Countermeasures,” to help facilitate more effective information security management.

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

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

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

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

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

We compiled a list of relevant survey topics to cover in questionnaires and interviews, and conducted a survey of actual corporate security incidents, and costs (damage costs) required for incident remediation.

We also included questions related to the amount of corporate capital invested for the purposes of preventing information security incidents.

(2) “Proposed Damage Cost Calculation Model”

We have taken the information security incident damage cost calculation model from the prior year’s research, and added further considerations to develop a more refined model.

More specifically, we will propose the reconsidered model that includes costs related to not only labor required for systems administrators, but also foreseeable costs related to legal damages incurred, payroll of personnel involved in systems recovery, damage to hardware and other physical assets, costs related to damaged reputation, lost income due to interrupted business operations, etc.

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

As one outcome of our research, we will propose a standard model and recommended response level and budget scale for limiting damages, given currently plausible measures and compared with the results of the prior year’s survey.

<Section Two (Supplement): Estimated Damages and other Observations (compensatory damages, influence on share prices, etc.) with respect to Private Information Disclosure>

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

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

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

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

3. Survey Results and Analysis

3.1 Survey Participants

- Security Incidents Investigation Working Group members were asked to help with the survey, finding willing respondents among Japanese corporations and organizations comprising Japan's infrastructure and core industries.
- Information Technology companies, mainly from the JNSA corporate membership (including several non-IT companies).

3.2 Survey Methodology

- Survey was conducted using questionnaires and/or interviews with representatives from participating companies.
- The questionnaire was based on the survey sheet used in the prior year, modified to be more convenient and allow further room for the respondent to answer questions in detail (see 8.2 Questionnaire Sheet).
- The questionnaire for JNSA members was sent to the membership with an attached request letter from the JNSA president. Participating members filled out the questionnaires and returned them to the JNSA offices.
- Questionnaires for non-JNSA members were requested and collected individually by the interviewer assigned to the particular company.

3.3 Survey Results

3.3.1 Interview Survey Results (Summary)

See "8.1 Interview Summary".

3.3.2 Questionnaire Survey Results (Tabulation Table)

See "3.4 Survey Results Analysis and Observations".

3.3.3 Questionnaire Response Rates and Interview Participant Rates

The table below indicates the number of questionnaires sent, questionnaire response rates, interview requests and interviews successfully held.

	Questionnaires			Interviews		
	Sent	Returned	Response Rate	Requested	Accepted	Acceptance Rate
Members	159 (121)	53 (53)	33.33% (41.32%)	17 (20)	9 (11)	52.94% (55.00%)
Non-Members	20 (5)	13 (4)	66.66% (80.00%)	20 (14)	7 (5)	35.00% (35.71%)
Total	179 (126)	66 (54)	36.87% (42.86%)	37 (34)	18 (16)	48.64% (47.06%)

Numbers in ( ) represent prior year figures.

The questionnaire response rate was approximately 37%, a slight drop from the prior year's 43%.

Although one must consider the small size of the population parameter, the drop in responses may reflect the lack of major newsworthy incidents during calendar 2002. The response rate among JNSA member firms was disappointing, but the overall numbers do not reflect any significant changes. On the other hand, the high response rate from non-member firms is most likely due to the fact that our survey selected those firms who showed an interest in the calculation of incident damage levels and damage costs when we first approached them.

We believe that the relatively high 50% acceptance rate for interviews reflects a desire to publicly disclose the extent of incident damage, showing a clear picture of what such damage means to a corporation. As a matter of fact, we heard from several interviewees that they are approached on an almost daily basis to participate in these kinds of surveys, and couldn't possibly respond to all such requests. That companies were willing to seriously entertain our survey questions attests that, even though the survey was conducted solely by the JNSA, these firms are gradually improving their response to, and infrastructure for, handling security issues.

3.3.4 Major Reasons for Rejecting Survey Questionnaires

The following are some of the reasons given for not responding to survey questionnaires:

- As a foreign-capitalized company, permission is needed from overseas headquarters, and permission was not granted.
- Corporate policy prohibits public sharing of information.
- Response would provide outsiders with a detailed picture of corporate information security measures, allowing would-be attackers an idea of the strength of corporate security measures. The potential risk outweighs potential benefits of participation in the survey.
- Some of the questionnaire questions would reveal the sum and whole of a company's security standards. Such information cannot be made public.
- Giving information related to incidents and responses thereto would be the same as publicly revealing the company's information protection schemes. The same applies to revealing information about damages incurred.

We duly noted comments such as those above, but we do not make specific remarks on each of them since we do not have detailed information. We believe that achieving reliable security is not a matter of simply locking something away in a strongbox. It is important that companies share information, and always consider new ways to protect their systems; therefore, companies should be in a position to explain their security policies at any time.

Companies must understand that "hiding" is not the true essence of security. Security and accountability have a close relationship. Accordingly, we believe the reaction of rejecting all forms of public information disclosure indiscriminately should be carefully analyzed and reconsidered. We will look to include data about the success or failure of such attitudes in future surveys.

3.4 Survey Results Analysis and Observations

3.4.1 This Year's Survey Results and Observations

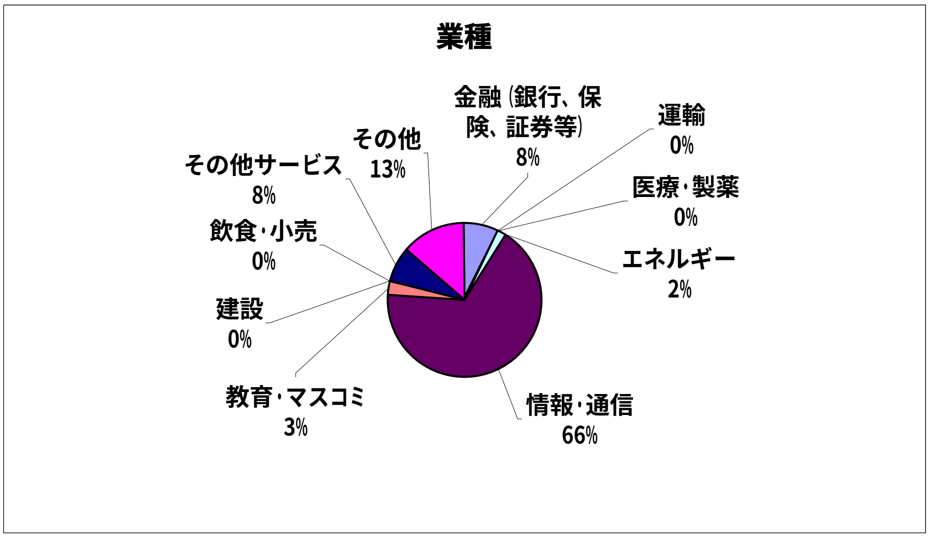
In the following paragraphs, we will offer comments related to the analysis and observations comparing "Compilation of Answers from 66 Questionnaires" and "Interview Results".

A Please tell us about your company's business.

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

	Industry	No.	%
1	Finance (banking, insurance, securities)	5	7.6%
2	Medical/ Pharmaceutical	0	0.0%
3	Transportation/ Shipping	0	0.0%
4	Energy	1	1.5%
5	Information/ Communications	44	66.7%
6	Education/ Mass Communications	2	3.0%
7	Construction	0	0.0%
8	Food Service/ Retail	0	0.0%
9	Other Services	5	7.6%
10	Other	9	13.6%
		66	100.0%

Note



Sixty-six companies or organizations responded to this year (FY2002)'s survey, compared to 55 respondents in the prior year (FY2001). Although the number of respondents increased, as in the prior year, the majority were JNSA (Japan Network Security Association) members. As a result, the industry makeup of the respondents is almost exactly the same as in the prior year, with

Information/ Communications accounting for the greatest number of answers (66%).

As in the prior year, there were no respondents from the Medical/ Pharmaceutical, Construction, or Food Service/ Retail industry groups. If we are to seek survey results from a statistical representation of businesses in Japan, we must do a better job of securing respondents from these fields.

A-2 Annual Sales and Number of Employees of your company.

■ Averages

1	Average Sales (¥millions)	170,901.86
2	Employees	1,806

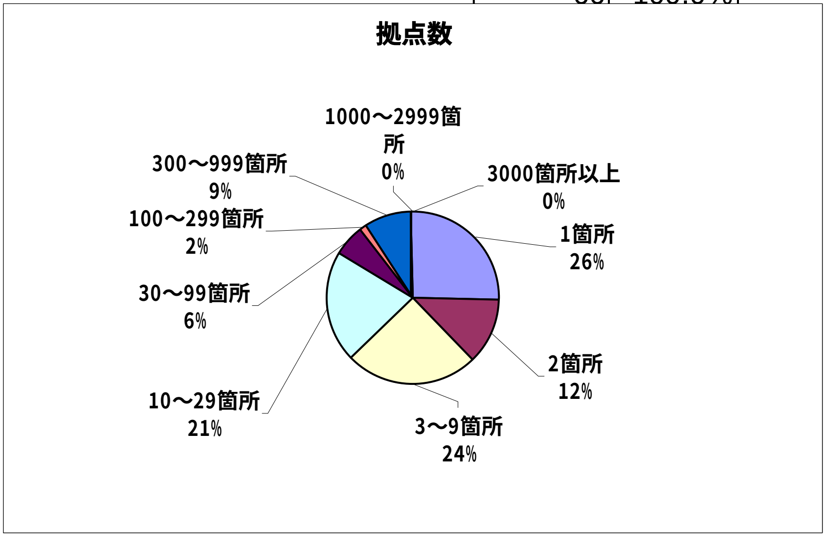
Note

The above values represent an average of the 66 survey respondents. The minimum annual and maximum annual sales for the respondents were ¥1 million and ¥1,686,941 million, respectively. The number of employees varied greatly, from one employee at the smallest firm to 15,470 employees at the largest firm.

The questionnaire results did not specifically reveal the relationship between security and the size/ scale of sales and number of employees; however, six out of seven firms who responded “No” to Question C-1: “Does your firm have formal information security policies” had less than 100 employees (the seventh firm had 330 employees), indicating at least a loose correlation.

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

	Locations	No.	%
1	1	17	25.8%
2	2	8	12.1%
3	3 to 9	16	24.2%
4	10 to 29	14	21.2%
5	30 to 99	4	6.1%
6	100 to 299	1	1.5%
7	300 to 999	6	9.1%
8	1000 to 2999	0	0.0%
9	3000 and above	0	0.0%
		66	100.0%



Note

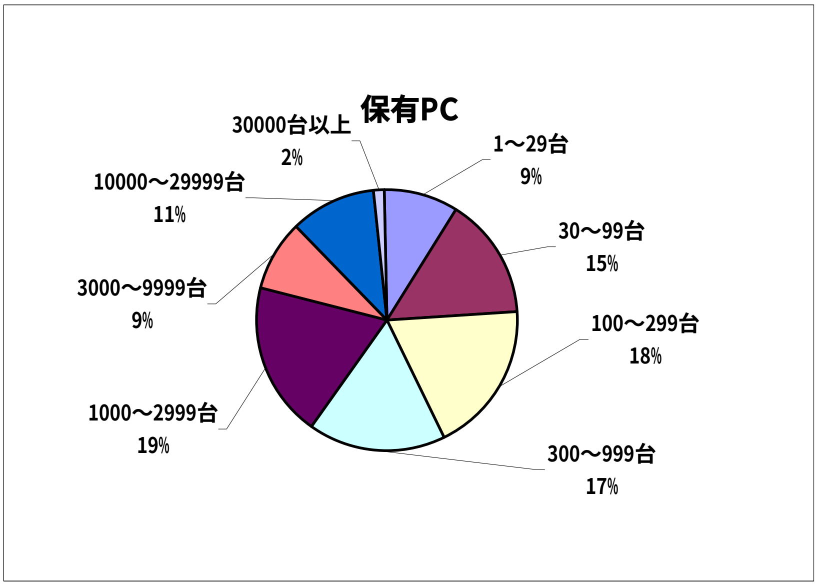
More than 83% of respondents had 29 office locations or fewer. Although not included in this year's respondents, if future surveys contain chain-store firms in the Food Service/ Retail industries, we expect this distribution will change significantly.

One expects that the greater the number of office locations, the greater the exposure to network security risks, and indeed, those firms with a comparatively larger number of locations (categories 5 through 7, above) have established efficient information communications structures, as seen in our questionnaire results (C-4).

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	6	9.1%
2	30 to 99	10	15.2%
3	100 to 299	12	18.2%
4	300 to 999	11	16.7%
5	1000 to 2999	13	19.7%
6	3000 to 9999	6	9.1%
7	10000 to 29999	7	10.6%
8	30000 and above	1	1.5%
		66	100.0%



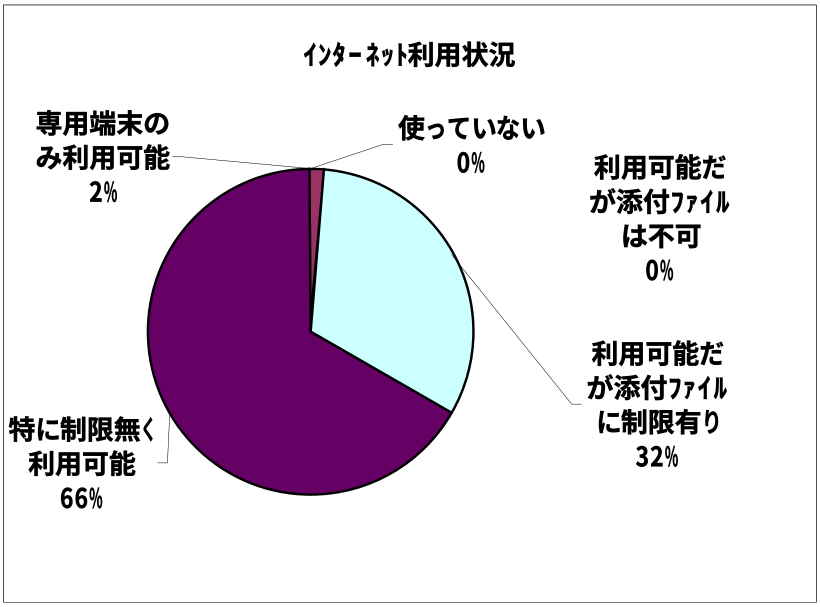
Note

When compared with Question A-2-2 "Number of Employees", the average number of PCs calculates to more than one computer per employee. The results may be skewed due to the large number of respondents in the Information/ Communications industries; however, these results appear to be consistent for all of the industries represented in this survey.

As with the number of office locations, one would expect greater levels of security risk with greater numbers of PCs within a firm. Of the 27 respondents indicating a relatively high number of company PCs (categories 5-8, above), 12 (44%) responded that they have some kind of restrictions on email usage and Web browsing (Questions B-2 and B-3), not a particularly striking observation.

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

	Usage Level	No.	%
1	None	0	0.0%
2	Email on designated terminals only	1	1.5%
3	Generally available, but attachments not permitted	0	0.0%
4	Generally available, but limitations on type and size of attachments	21	31.8%
5	Generally available with no particular limitations	44	66.7%
		66	100.0%



Note

The results for this question may have been skewed by the large number of Information/ Communications companies in the response group. All responding companies indicated they used Internet Email.

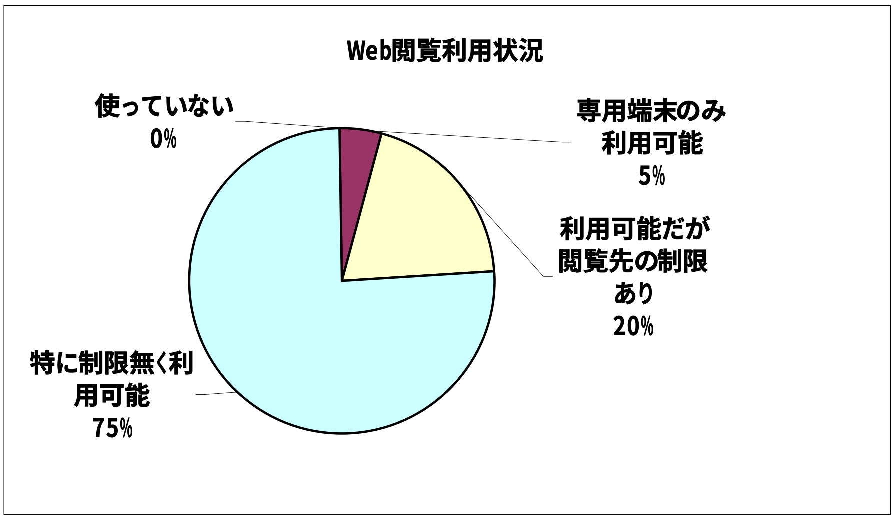
The higher the rate of Email usage, the greater the danger of network infection due to computer viruses. Looking at the results for survey Question C-15, "Implemented Security Systems," with the exception of one firm, all respondents indicated that they either conduct "virus checks on the mail server” or “virus checks on all client PCs”, or both, showing their understanding of the nature of the risks of Email usage.

However, looking at this issue from the aspect of private information disclosure leads one to believe that limitations should be placed on outgoing Email transmissions. We must incorporate questions reflecting this issue in future survey questionnaires.

In addition, our interview results showed that company restrictions/ limitations on Email are primarily targeted to message size, indicated that perhaps such policies are in place because of practical reasons, such as network capacity load, rather than for security purposes.

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

	Usage Level	No.	%
1	None	0	0.0%
2	Web access on designated terminals only	3	4.5%
3	Generally available, with restrictions on permissible sites	13	19.7%
4	Generally available with no particular limitations	50	75.8%
		66	100.0%



Note

As with the question related to Email usage, 100% of respondents indicated that they allow some sort of Web browsing at their companies. Only 24.2% of respondents appear to have some limit on Web browsing, as seen by adding the total of companies who grant “Web access on designated terminals only” and access with “Restrictions on permissible sites”. Looking at the results by industry shows that of the three respondents who grant “Web access on designated terminals only,” two are in the financial services industry and one is a regional governmental organization.

In addition, of the 13 respondents who said they grant access with “Restrictions on permissible sites,” we see that after removing the Information/ Communications firms from consideration, two respondents from the Other Services category, one respondent from the Energy category, one respondent from the Finance category, and one respondent from the regional government category provide access, but with limits as to what sites users may visit over the Internet.

“Restriction” is accomplished through content filtering, restricting access to adult, gaming, stock trading, attack, and bulletin board websites. Further, several companies in our survey have established detailed restrictions, for example, allowing only members of human resources to purchase travel tickets online.

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

■ Average Values

1	Internet Mail (%)	90%
2	Web Access (%)	85%

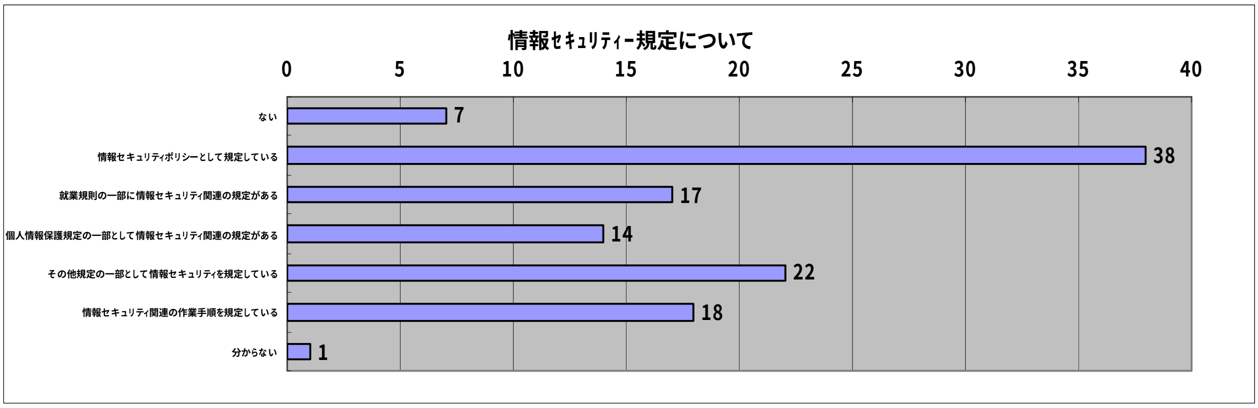
Note

The figures above are averages. Looking at the answers to Questions B-2 and B-3, we believe we have grounds to conclude that, with the exception of certain financial services firms and regional governments, most respondents have established a corporate environment in which each computer user has direct access to the Internet. Given the role of the Internet as an amazing tool for communications and research, this conclusion should not be a surprise. However, considering most companies grant employees unfettered access to Email and Web browsing, it would seem that company management is more concerned with convenience than security.

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

C-1 Does your firm have formal information security policies? (Choose all applicable.)

	Answer	No.	%
1	No	7	10.6%
2	Separately defined information security policies in place	38	57.6%
3	Information security rules included in workplace conduct policies	17	25.8%
4	Information security rules included in policies related to protecting personal information	14	21.2%
5	Information security rules included in other policies	22	33.3%
6	Information security related procedures in place	18	27.3%
7	Not sure	1	1.5%



Note

Half of the 38 respondents who indicated they have defined security policies also indicated the concurrent existence of other policies identified in categories 3 through 6, above. We observed several instances where penalties contained in work conduct policies already in place were applied to violations of security rules.

We also noted 10 companies did not have a separately defined security policy, but incorporated security policies into other policies and rules.

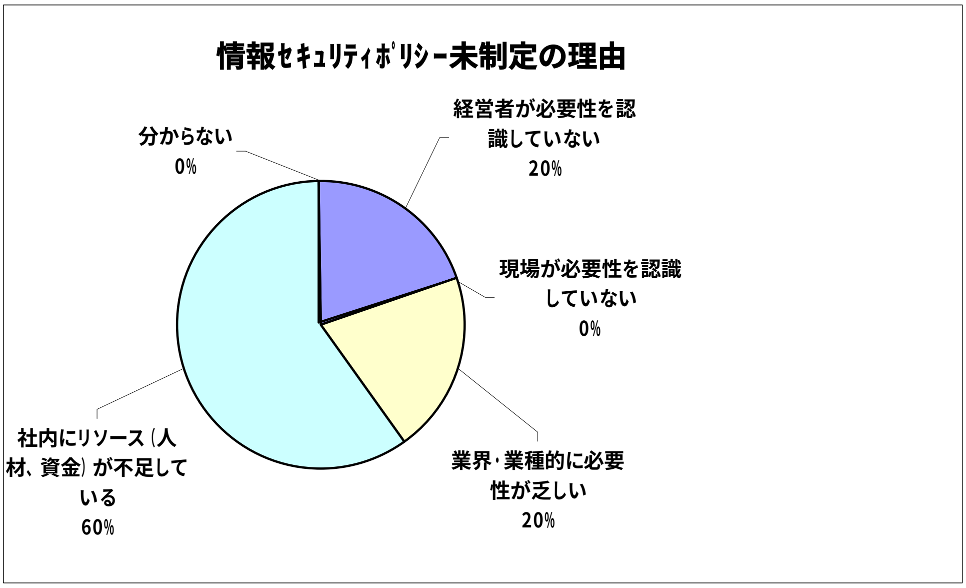
Further, of the 14 respondents who indicated they had policies for personal information protection related to recent legislation, one is in the finance industry, one is in the Education/ Mass Communications industry, and the remaining 12 are all in the Information/ Communications industry.

For those companies interviewed, most indicated they are continuing to work for high levels of information security after establishing their policies, by means of conducting employee education and performing periodic maintenance.

C-2 For those responding "1. No" to Questions C-1:

What is the most important reason for not creating an information security policy? (Select one.)

	Reason	No.	%
1	Management does not see the need	1	20.0%
2	Locality does not see the need	0	0.0%
3	Low level of awareness among industry/ business type	1	20.0%
4	Not enough resources (personnel, capital) within the company	3	60.0%
5	Not sure	0	0.0%
		5	100.0%



Note

As with Question A-2, six of the seven companies who responded “No” to Question C-1 citing “Not enough resources” have fewer than 100 employees, supporting their contention.

C-3 How many personnel are assigned to information security management?

1	Dedicated personnel	1.70	<average no. of people>
2	Dually-responsible personnel	56.15	<average no. of people>
3	Responsible board director selected	21	Responses

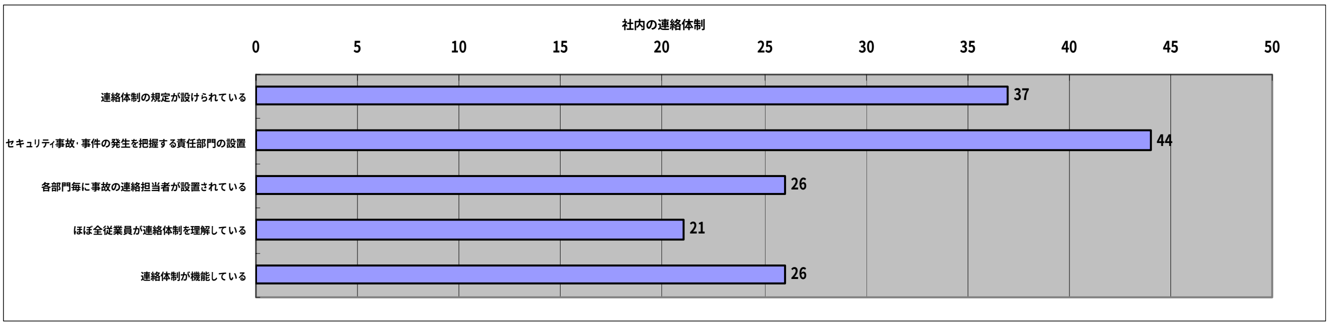
Note

Many of the responding companies have dually-responsible personnel who are in charge of information security as part of their overall job duties. As seen with "Budget (C-12)", in many cases it appears that information security is operated as a subset of information systems.

During interviews, most respondents said that dually-responsible personnel spend approximately 10% to 20% of their time on security related work.

C-4 System for communicating information security mishaps and incidents throughout the company. (Choose all applicable.)

	System	No.	%
1	Communications system established and in place	37	56.1%
2	Established department responsible for determining occurrences of security mishaps and incidents	44	66.7%
3	Each department has a designated person responsible for communicating information security incidents	26	39.4%
4	Almost all employees understand the communications system	21	31.8%
5	The communications system is functioning properly	26	39.4%



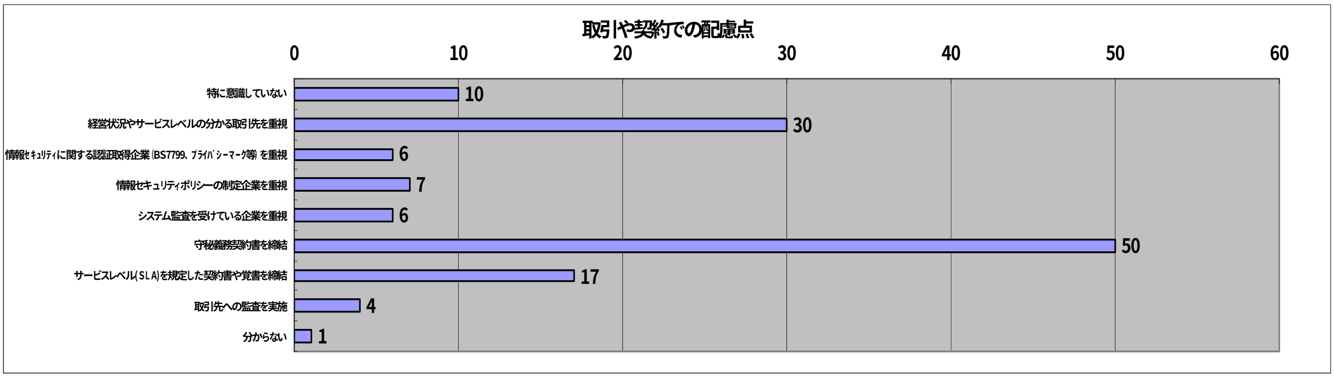
Note

Of the 66 survey respondents, four companies did not answer any of the above (possible that the companies have no system in place), while more than 90% of the respondents indicated they have established an incident communication system. Several respondents answered that the department in charge was not the information systems department, but the general affairs department, with information security being managed as a subset of overall risk management.

Further, most of the companies having an incident communications system use ongoing education and rehearsals to maintain the system.

C-5 Information security considerations when selecting or contracting with business partners. (Choose all applicable.)

	Considerations	No.	%
1	No special considerations	10	15.2%
2	Special consideration given to business partners with well-known business and service levels	30	45.5%
3	Special consideration given to business partners who have certification related to information security (BS7799, Privacy Mark, etc.)	6	9.1%
4	Special consideration given to business partners who have a formal information security policy	7	10.6%
5	Special consideration given to business partners who undergo information system audits	6	9.1%
6	Require non-disclosure agreements	50	75.8%
7	Require contracts/ agreements defining Service Levels (SLA)	17	25.8%
8	Perform information system audits on business partners	4	6.1%
9	Not sure	1	1.5%



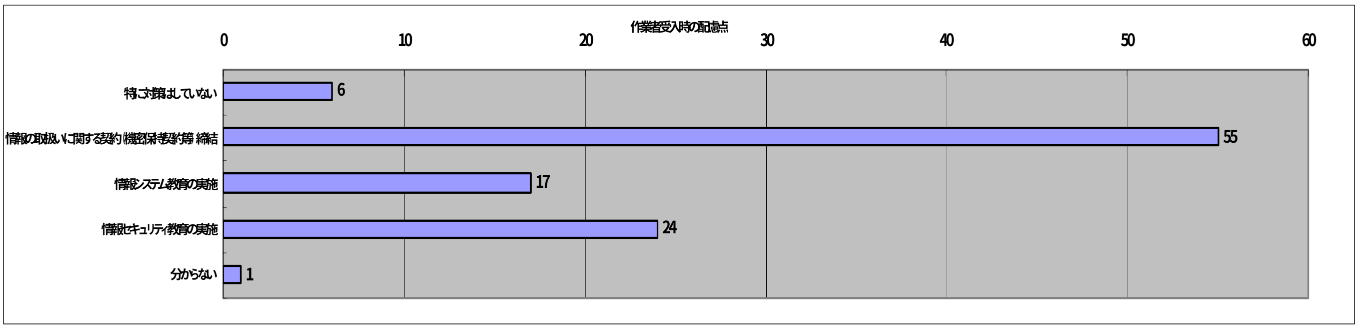
Note

The reason for the frequency of “2 Special consideration given to business partners with well-known business and service levels” is most likely the fact that such business partners have already been subject to standard background checks as part of the respondent’s credit management procedures. The response to “6 Require non-disclosure agreements” is also likely influenced by wide-spread business practices with respect to standard contracts, prior to recent attention given to information security issues.

At the same time, we have noted that some of the respondents indicate more business partners require the standards described above, and this verifies the existence of “information security practices” at a business partner is fast becoming a customary business practice.

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

	Considerations	NO.	%
1	No special considerations	6	9.1%
2	Require contracts related to handling information (non-disclosure agreements, etc.)	55	83.3%
3	Conduct ongoing information systems education	17	25.8%
4	Conduct ongoing information security education	24	36.4%
5	Not sure	1	1.5%



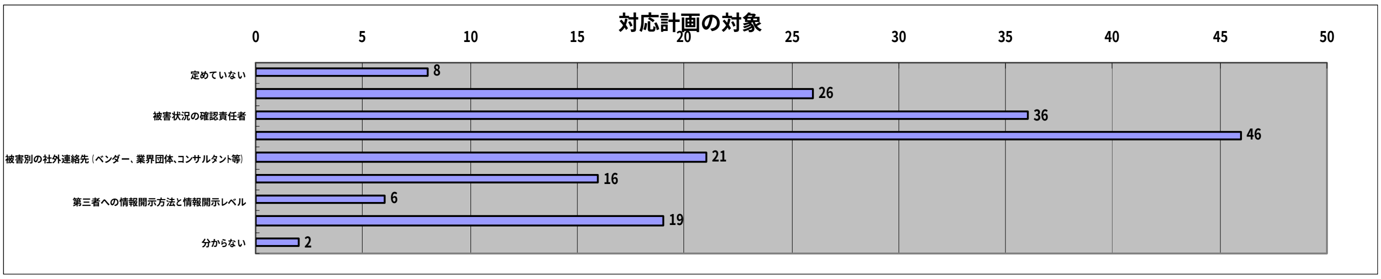
Note

As with C-5, above, the reason for the frequency of response to “2 Require contracts related to handling information (non-disclosure agreements, etc.)” is most likely that such considerations have already been incorporated in standard contracts. Forty-one percent of respondents conduct education as mentioned in either Question 3 or Question 4, indicating that security is viewed by these firms as an issue related to general work procedures.

Looking at the interview results, we see that many companies conduct education for contract employees when they are first brought in, and in many cases education includes detailed rules regarding the systems operation.

C-7 Factors included in damage response plan. (Mark all that apply.)

	Factors Included in response plan	No.	%
1	Not defined	8	12.1%
2	Confirm status for each type of damage incurred	26	39.4%
3	Personnel responsible for confirming damage	36	54.5%
4	Internal system for communicating incident damages	46	69.7%
5	Outside parties to be contacted depending on damages (vendors, industry groups, consultants, etc.)	21	31.8%
6	Method for conveying information to employees, level of detail to be provided	16	24.2%
7	Method for conveying information to outside parties, level of detail to be provided	6	9.1%
8	Confirmation checklist for system recovery	19	28.8%
9	Not sure	2	3.0%



Note

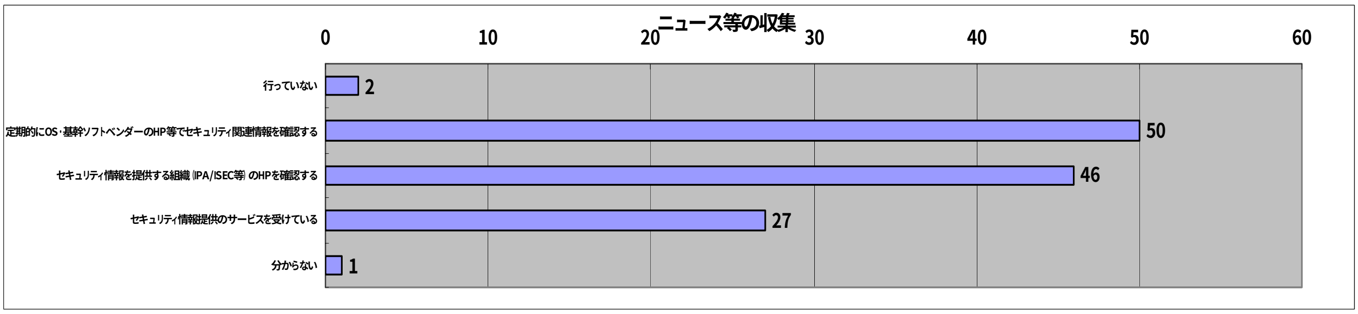
As can be seen from the results of Question C-4, 90% of the survey respondents have some type of incident communications system in place, which is reflected by the high number of responses to categories 3 to 5, above.

However, we are concerned by the low rate of response to category 7, “Method for conveying information to outside parties, level of detail to be provided,” since a company’s response to an actual incident is such an important factor in losing or saving a corporation’s public image.

For those companies who answered “Not defined” above, we received comments indicating that the responsible department creates a response plan based on past experience, or vendors providing outsourced services provide suggested incident countermeasures, which are implemented with or without modification by the respondent, each time the incident occurs.

C-8 How do you gather information security-related news? (Choose all applicable.)

	Method	No.	%
1	No formal news gathering conducted	2	3.0%
2	Periodically review information on OS and critical software vendor websites.	50	75.8%
3	Review websites of organizations providing security information (IPA/ ISEC, etc.)	46	69.7%
4	Subscribe to security information news service	27	40.9%
5	Not sure	1	1.5%



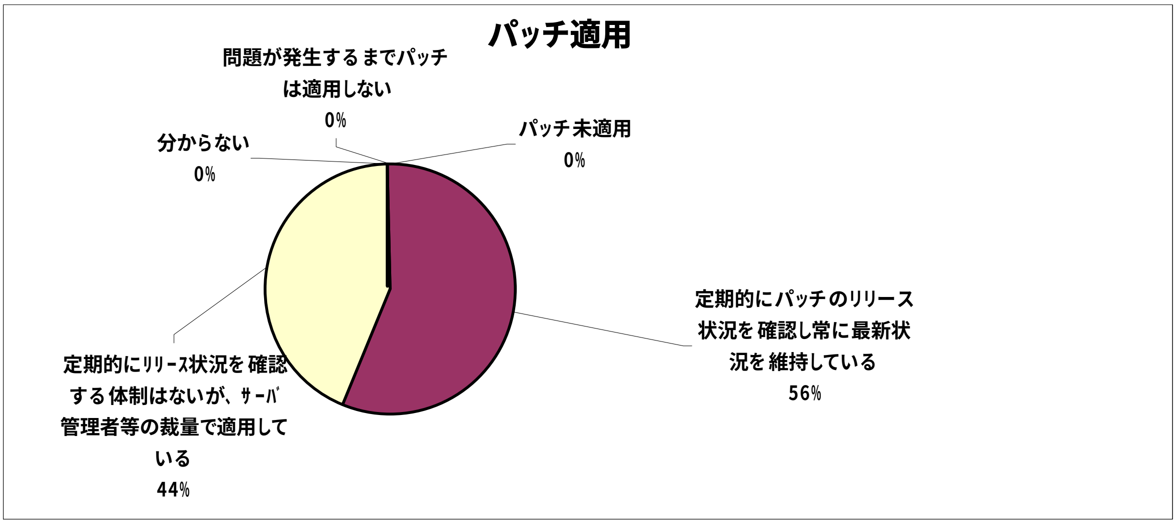
Note

Many respondents indicated that they obtained information for patches and updates through OS vendor homepages or security news mailing lists. Information related to virus countermeasures is obtained via the anti-virus software makers' websites.

Further, those subscribing to fee-based information services were of the opinion that the benefits of list membership include access to information about patch testing and verification.

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

	Patch application	No.	%
1	No patches applied	0	0.0%
2	Periodically confirm release of new patches, always keep servers up-to-date	34	55.7%
3	No formal system of confirming new patch releases; application of new patches left to the discretion of the server administrator	27	44.3%
4	Patches not applied unless a problem occurs	0	0.0%
5	Not sure	0	0.0%
		61	100.0%



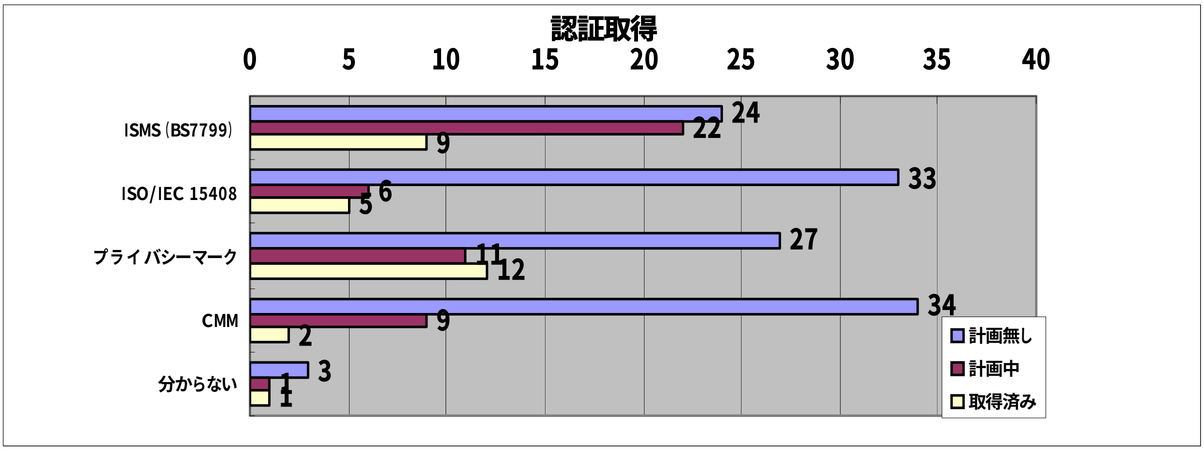
Note

As damage from computer viruses and unauthorized access become an everyday occurrence, the application of new patches has become accepted as a basic preventive measure. This is reflected in our survey, with zero respondents indicating “No patches applied”.

However, we observed many opinions about the difficulty of applying patches to servers that cannot be taken out of service, or fears about applying patches to database servers without first conducting some type of verification. These reasons are cited by companies who install updated patches for servers that are accessed externally, but to not do the same for internal servers.

C-10 Indicate whether certification is "In Planning" or "Already Obtained".

	Name	No Plan	%	In Planning	%	Already Obtained	%
1	ISMS (BS7799)	24	36.4%	22	33.3%	9	13.6%
2	ISO/IEC 15408	33	50.0%	6	9.1%	5	7.6%
3	Privacy Mark	27	40.9%	11	16.7%	12	18.2%
4	CMM(Capability Maturity Model)	34	51.5%	9	13.6%	2	3.0%
5	Not sure	3	4.5%	1	1.5%	1	1.5%



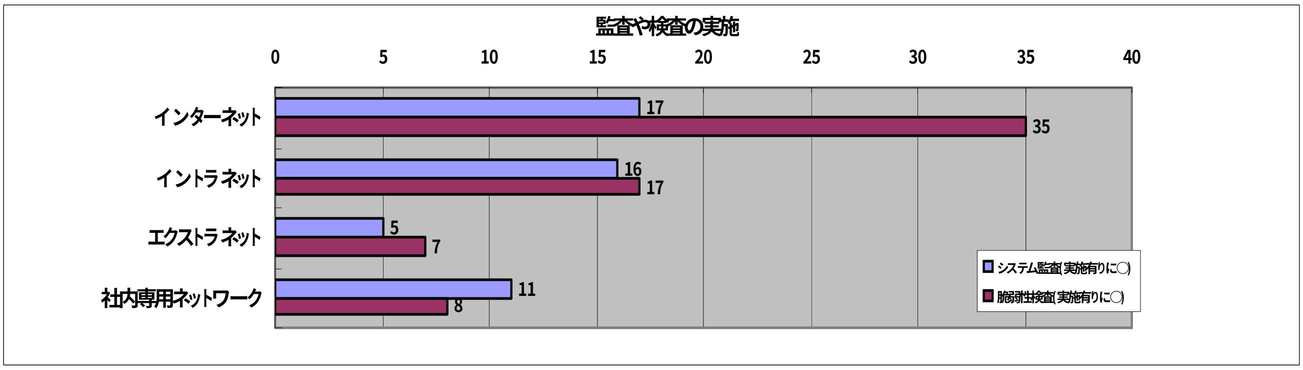
Note

Looking at the combination of "Already Obtained" and "In Planning", we see that ISMS and Privacy Mark certifications are relatively high, at 31 and 23, respectively. We observed that many companies obtained these certifications as a means of corporate strategy— to differentiate themselves from competitors or to answer market needs.

In contrast, many companies indicated that ISO/IEC 15408 and CMM certifications were not considered vital, and were obtained/ planned for as needed, for example, when required in customer contracts, etc. We noted CMM, in particular, was not widely recognized among companies since some of the respondents even questioned the meaning of CMM during the interviews.

C-11 Has your organization conducted system audits and vulnerability tests (penetration tests) within the previous 12 months?

	System	System Audit	%	Vulnerability Testing	%
1	Internet	17	25.8%	35	53.0%
2	Intranet	16	24.2%	17	25.8%
3	Extranet	5	7.6%	7	10.6%
4	Internal company network	11	16.7%	8	12.1%



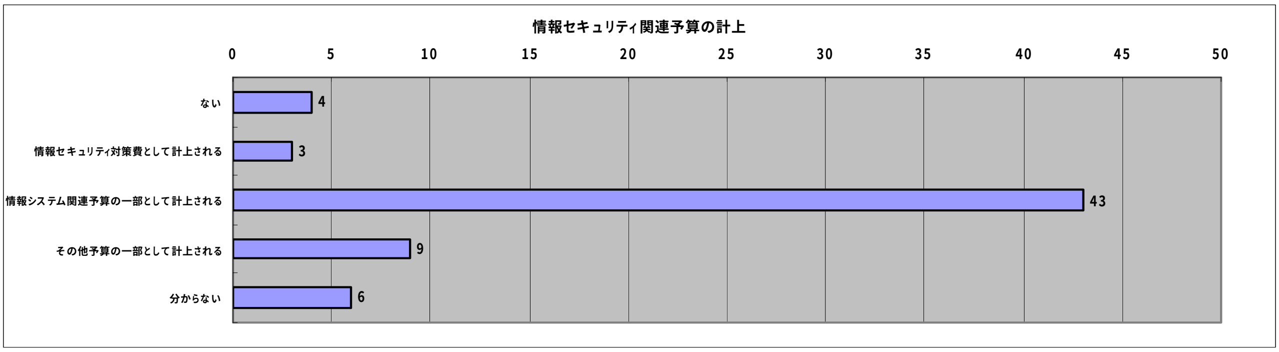
Note

Of the 66 survey respondents, 40 (60%) indicated that they conducted a complete or partial system audit and/or vulnerability test. Looking at the questionnaire results, it appears that system audits were conducted for both external and internal issues, while vulnerability tests were conducted strictly in relation to external attack.

Testing frequency varied, with companies indicating tests once per year, twice per year, daily morning log checks, etc. Some companies told us that they pre-determine which areas to test, and then have outside parties conduct the testing, selecting a new testing company each time.

C-12 Does your company have a formal information security budget? (Please circle your selection; select one.)

	Budget Appropriation	No.	%
1	None	4	6.1%
2	Budgeted separately as information security costs	3	4.5%
3	Budgeted as a subset of the information systems budget	43	65.2%
4	Budgeted as a subset of “Other”	9	13.6%
5	Not sure	6	9.1%
<Other>		65	98.5%



Note

As can be seen from the details of Question C-14, the dividing line between hardware purchases and maintenance of general systems and that of security systems is vague, and subsequently most companies answered “Budgeted as a subset of the information systems budget” here (65.2%). Question C-3 touches on this issue as well, where we see most companies having dual responsibility within the information systems department for security management, as well as the budget for security managed as a subset of the general information systems budget.

C-13 If you marked any categories 2 through 4, above, please provide some general figures.

Average amount for budget (¥millions)	14.97
Ratio of information systems budget	14.8%

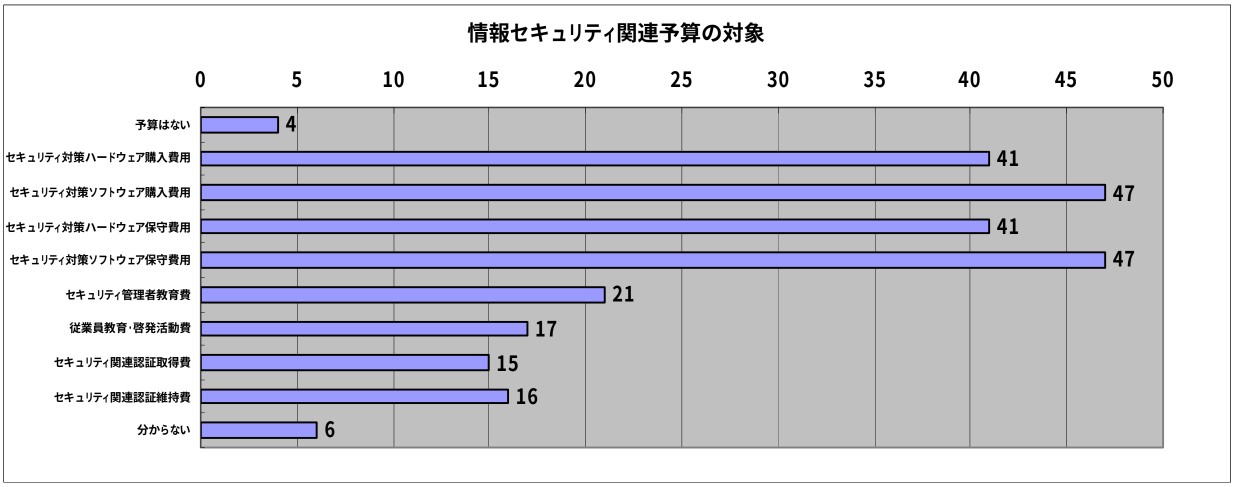
Note

Twenty-six companies responded to both questions of security budgets and annual sales revenue. The average annual sales for those 26 companies was ¥99.01481 billion, and security budgets averaged ¥15.96 million. Using these numbers, the average ratio of security budget to annual sales calculated to 0.016%. Given the small population, there is room to question the complete credibility of this number; however, this figure is extremely small, especially considering that survey respondents mainly come from the Information/ Communications industry.

For future surveys, we will consider revising questionnaire questions and wording to derive more precise information related to budgets.

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

	Budget Allocation	No.	%
1	No budget	4	6.1%
2	Security hardware purchases	41	62.1%
3	Security software purchases	47	71.2%
4	Security hardware maintenance	41	62.1%
5	Security software maintenance	47	71.2%
6	Security administrator training	21	31.8%
7	Employee training/ education	17	25.8%
8	Obtaining security-related certifications	15	22.7%
9	Expenses of maintaining security-related certifications	16	24.2%
10	Not sure	6	9.1%



Note

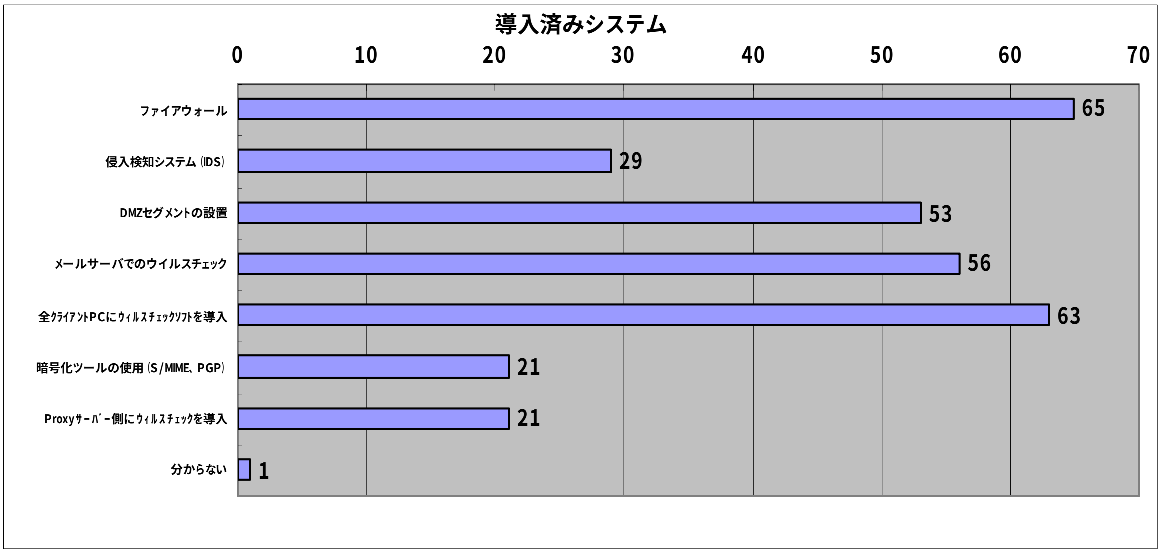
Categories 2 through 5 account for most of the budget allocation for respondents, all of which have to do with the purchase and upkeep of hardware and software, including not only purchases of new security products, but also upgrades of PC platforms, etc.

In addition, many companies include license costs for virus definition file updates within their software maintenance costs.

We also noted several entities who indicated they record costs associated with incidents at the time the incident occurs.

C-15 Indicate IT systems used to ensure information security. (Mark all that apply.)

	Implemented Systems	No.	%
1	Firewalls	65	98.5%
2	Intrusion Detection Systems (IDS)	29	43.9%
3	Set up DMZ segments	53	80.3%
4	Virus checks on the mail server	56	84.8%
5	Implement virus checks on all client PCs	63	95.5%
6	Encryption tool usage (S/MIME, PGP)	21	31.8%
7	Implement virus checks on proxy servers	21	31.8%
8	Not sure	1	1.5%

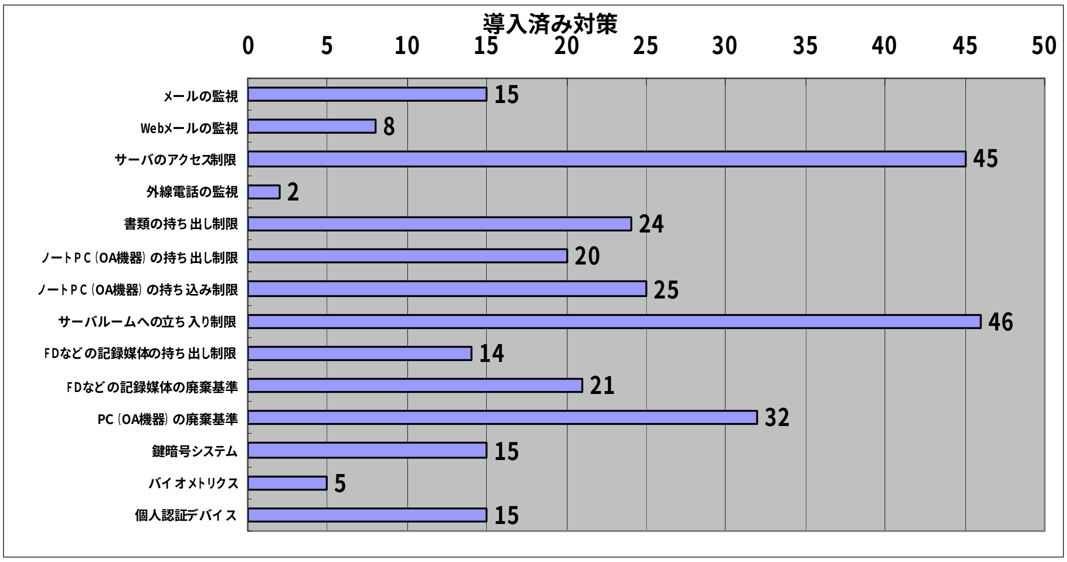


Note

With the exception of one firm, all respondents use firewalls. Again, with the exception of one firm, all respondents conduct virus countermeasures at the server, client, or proxy server. The conscientious application of such measures leads one to understand the relatively low number of incidents reported during this year's survey.

C-16 Countermeasures used to prevent private information disclosure. (Mark all that apply.)

	Countermeasures Enacted	No.	%
1	Email monitoring	15	22.7%
2	Webmail monitoring	8	12.1%
3	Server access restrictions	45	68.2%
4	External phone line monitoring	2	3.0%
5	Restrictions on removing documents	24	36.4%
6	Restrictions on removing notebook PCs (office automation equipment)	20	30.3%
7	Restrictions on bringing in notebook PCs (office automation equipment)	25	37.9%
8	Restricted access to server rooms	46	69.7%
9	Restrictions on removing floppy discs and other memory media	14	21.2%
10	Standards for destroying floppy discs and other memory media	21	31.8%
11	Standards for destroying PCs (office automation equipment)	32	48.5%
12	Key encryption systems	15	22.7%
13	Biometrics	5	7.6%
14	Personal identification devices	15	22.7%



Note

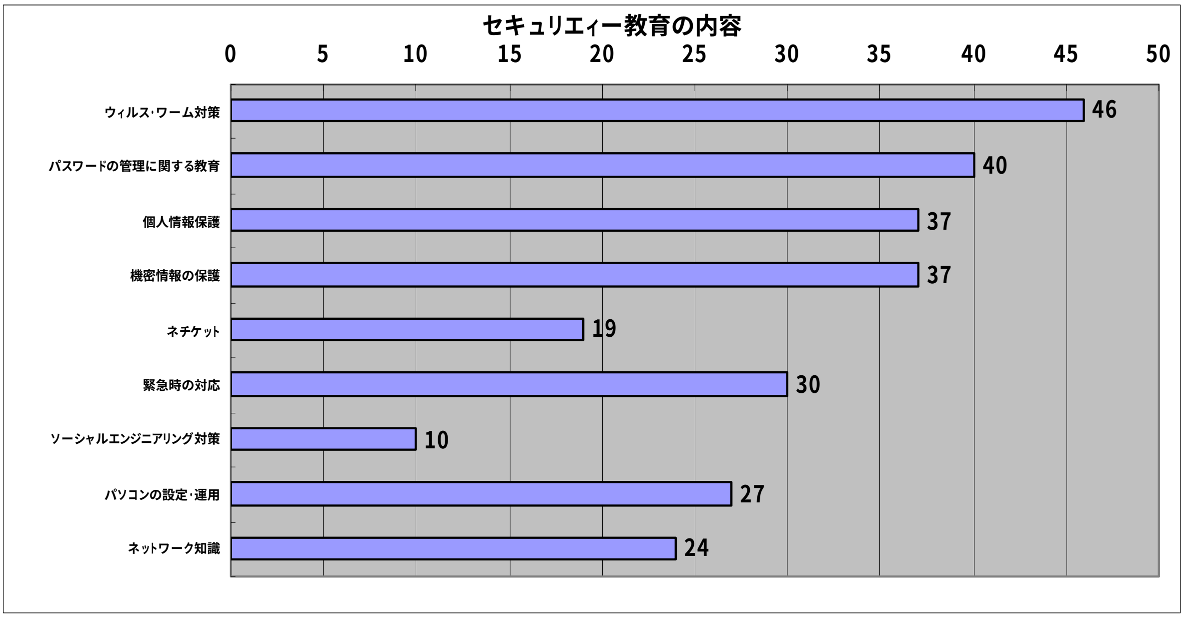
Restricted access to servers and server rooms represent two universally understood security measures, and are employed by 70% of survey respondents. The next most implemented security measures involved standards for the destruction of floppy discs and other memory media, and the destruction of PCs. We believe one cause for this is increased coverage in magazines, etc. of the dangers posed by insufficient destruction of such items.

We also noted a significant number of firms who employed measures related to restrictions on the removal of documents and the taking out/ bringing in of notebook PCs, indicating these companies are focusing attention on the security management process, rather than solely on the implementation of firewall and other systems measures.

With privacy considerations, complete Email monitoring is somewhat difficult to achieve; however, 22% of respondents indicated they employ some form of this security tool. However, this does not mean that the firms control the content of Email messages. Rather, we see some examples of firms employing unique methods to monitor traffic flow in order to detect the potential Email transmission of programs under development.

C-17 Information Security Training/ Education. (Mark all that apply.)

	Training/ Education Content	No.	%
1	Virus/ worm countermeasures	46	69.7%
2	Password management education	40	60.6%
3	Protection of personal information	37	56.1%
4	Protection of proprietary information	37	56.1%
5	“Netiquette” (Internet Etiquette)	19	28.8%
6	Emergency response	30	45.5%
7	Social engineering countermeasures	10	15.2%
8	PC settings/ operation	27	40.9%
9	Network knowledge	24	36.4%



Note

With the exception of six respondents, all survey participants conduct some form of training and education. Many respondents incorporated such training as part of overall new-hire education, rather than as stand-alone curriculum.

A few respondents demonstrated an aggressive approach to education, adopting E-learning, and developing in-house certifications.

C-18 Ongoing information security education over the previous 12 months. (Mark all that apply.)

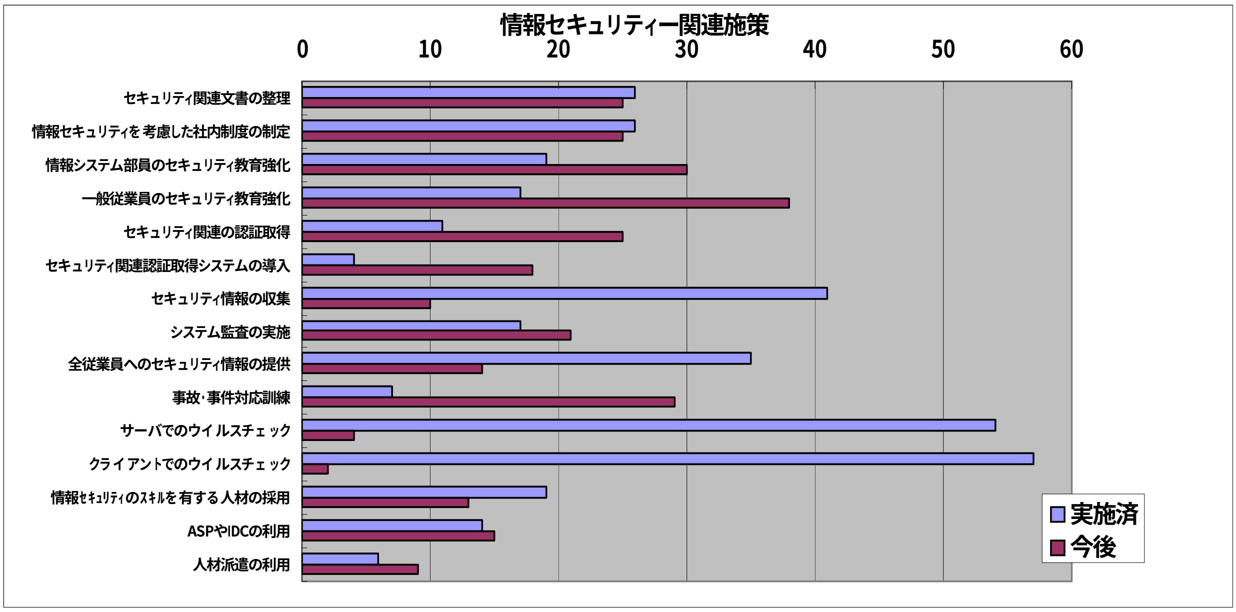
	Training/ Education Content	Avg. No. of People	Average Annual Frequency
1	Education for all Employees (User Training)	1775	3
2	Management Training	42	2
3	Specialist Training	62	3

Note

We noted several instances of firms who had systems that not only included periodic group training, but also "Step-Up" training to reinforce and add to previous training.

C-19 Current or planned measures for information security. (Choose all applicable.)

	Type of Measure	Already Imple-mented	%	Planned	%
1	Prepare security-related documentation	26	39.4%	25	37.9%
2	Define internal system for information security	26	39.4%	25	37.9%
3	Security training reinforcement for information systems personnel	19	28.8%	30	45.5%
4	Security training reinforcement for all employees	17	25.8%	38	57.6%
5	Obtain official security certifications	11	16.7%	25	37.9%
6	Implement systems for obtaining official security certifications	4	6.1%	18	27.3%
7	Gather security information	41	62.1%	10	15.2%
8	Conduct system audits	17	25.8%	21	31.8%
9	Provide security information to all employees	35	53.0%	14	21.2%
10	Incident/ accident response training	7	10.6%	29	43.9%
11	Virus checks on servers	54	81.8%	4	6.1%
12	Virus checks on client PCs	57	86.4%	2	3.0%
13	Employ personnel who possess information security skills	19	28.8%	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%



Note

Approximately 90% of respondents have implemented computer virus countermeasures. We expect that these firms will continue to maintain their current level of measures, rather than increase investments to prevent computer viruses.

The next most frequent answer to this question was gathering information and providing information to all employees. The frequency of these answers is most likely due to their respective low implementation and operation costs, and the ease of implementation using tools already in place, such as Email and the Web.

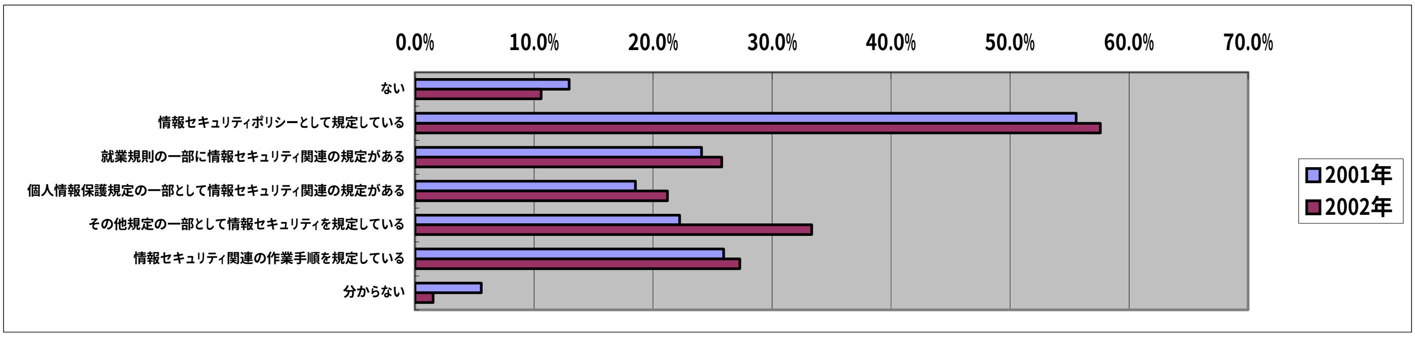
3.4.2 Comparison of Last Year's Survey and This Year's Survey

We took the results for the 2001 and 2002 surveys, and conducted a comparison of similar questions between the two to determine what changes may have taken place over the intervening year.

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

C-1 Does your firm have formal information security policies? (Choose all applicable.)

		2001		2002	
1	No	7	13.0%	7	10.6%
2	Separately defined information security policies in place	30	55.6%	38	57.6%
3	Information security rules included in workplace conduct policies	13	24.1%	17	25.8%
4	Information security rules included in policies related to protecting personal information	10	18.5%	14	21.2%
5	Information security rules included in other policies	12	22.2%	22	33.3%
6	Information security related procedures in place	14	25.9%	18	27.3%
7	Not sure	3	5.6%	1	1.5%

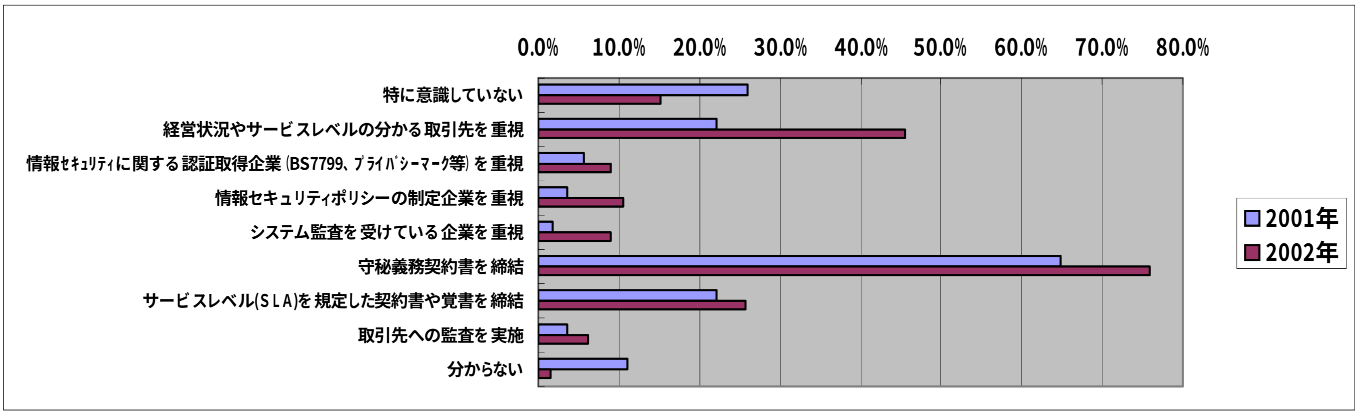


Note

A comparison of this year and last year's surveys reveals respondent progress in preparing defined security measures, however slight the improvement may be. The significant increase in response to Category 5, "Information security rules included in other policies," could mean that while companies understand the need for security policies, they have chosen the more expeditious route of incorporating security rules into existing policies (corporate rules, etc.), rather than creating a specific set of security policies.

C-5 Information security considerations when selecting or contracting with business partners. (Choose all applicable.)

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



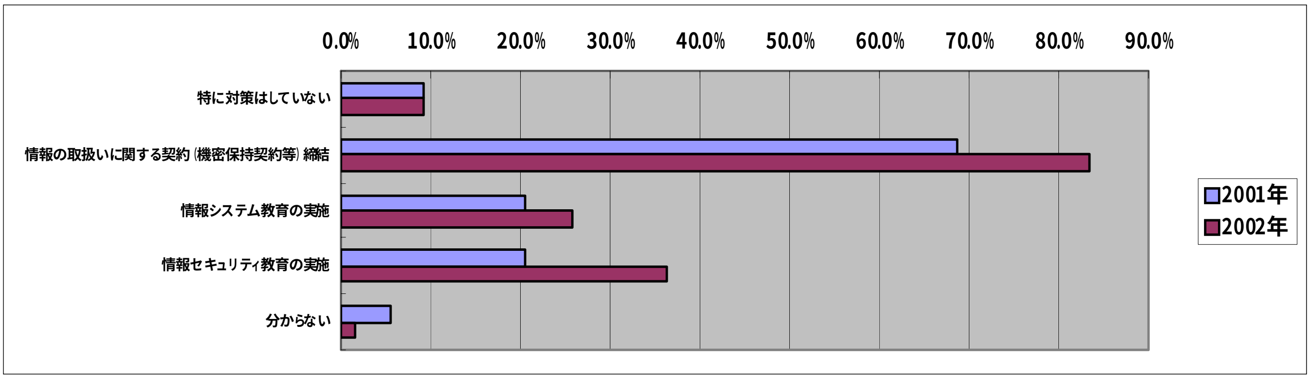
Note

Compared to last year, responses to Category 2, “Special consideration given to business partners with well-known business and service levels” have increased. There is a high likelihood that this increase reflects the continued economic stagnation in Japan, and is not directly related to security issues. We believe the respondents to this question had no choice but to select this answer as a rational method for selecting business partners, due to the lack of objective means for measuring security, such as certifications and audits.

While the other answer categories show a slight increase, responses related to certifications and policies show only a 10% increase, far from levels that would exert any significant pressure on current or future business partners.

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

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

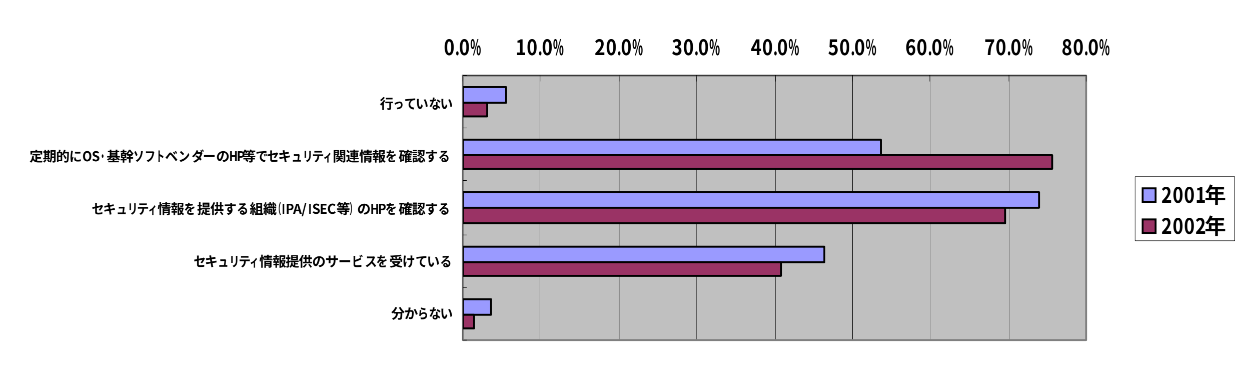


Note

We have noted an increase in acknowledgement that security policies should extend beyond regular full-time employees. One possibility for this increase is that many of the survey respondents are JNSA member firms who have already implemented relatively advanced technical security measures, and who see human measures as the next phase of security preparedness. Another possibility is that the influence of growing numbers of accidental exposures of private information has fostered an enthusiasm for employee training and education.

C-8 How do you gather information security-related news? (Choose all applicable.)

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

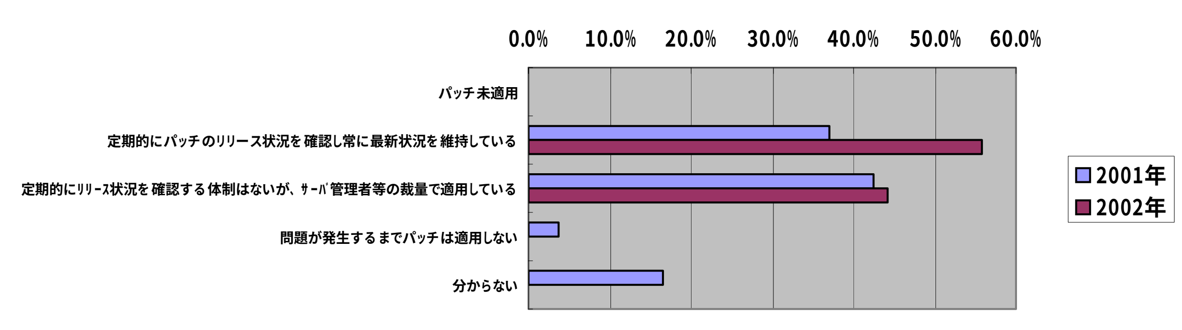


Note

Only Category 2, “Periodically review information on OS and critical software vendor websites” showed an increase. We believe that, after experiencing several different methods, the respondents have settled on accessing information related to patches, etc., which directly leads to effective countermeasures.

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

		2001		2002	
1	No patches applied	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%
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%
4	Patches not applied unless a problem occurs	2	3.7%	0	0.0%
5	Not sure	9	16.7%	0	0.0%
		54	100.0%	61	100.0%

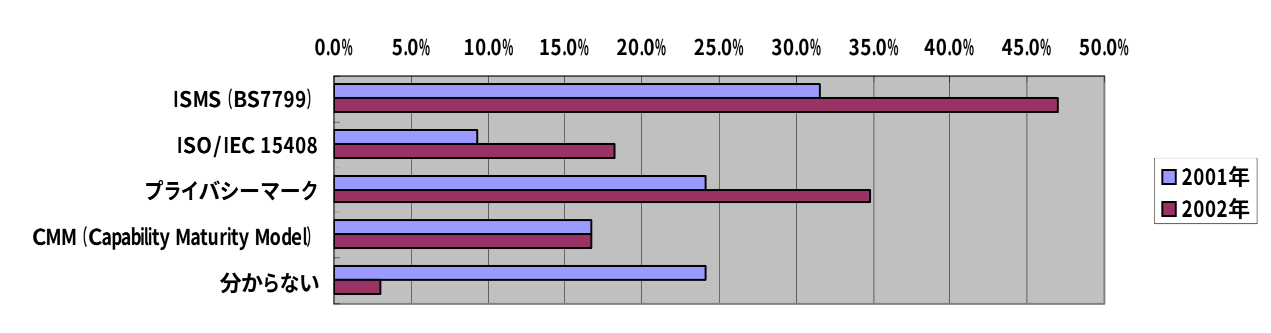


Note

That both Categories 4 and 5, “Patches not applied unless a problem occurs” and “Not sure”, respectively, had a 0% response is encouraging. We did note a slight increase in responses for Category 3, “No formal system of confirming new patch releases; application of new patches left to the discretion of the server administrator,” which most likely reflects the rather severe nature and cost of applying patches.

C-10 Indicate whether certification is “In Planning” or “Already Obtained”.

		2001				2002			
	Name	In Planning	%	Already Obtained	%	In Planning	%	Already Obtained	%
1	ISMS (BS7799)	14	25.9%	3	5.6%	21	31.8%	10	15.2%
2	ISO/IEC 15408	5	9.3%	0	0.0%	7	10.6%	5	7.6%
3	Privacy Mark	4	7.4%	9	16.7%	11	16.7%	12	18.2%
4	CMM （Capability Maturity Model）	8	14.8%	1	1.9%	9	13.6%	2	3.0%
5	Not sure	13	24.1%	0	0.0%	1	1.5%	1	1.5%



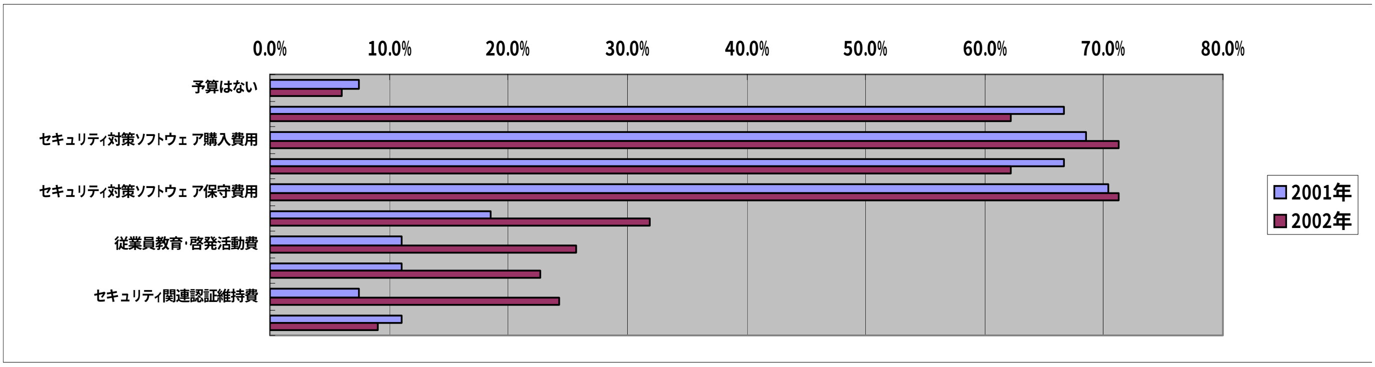
Note

We drew up a graph to perform a year-on-year comparison of the totals for “Already Obtained” and “In Planning”, above. The graph revealed relatively a large change, on the order of 10% to 15%.

The dramatic decrease in responses for Category 5, “Not sure,” indicates the overall increase in name recognition for certain certifications, as well as interest in the process of becoming certified. We believe that the near future will bring an environment in which all firms will be forced to seriously consider obtaining such third-party certifications.

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

		2001		2002	
1	No budget	4	7.4%	4	6.1%
2	Security hardware purchases	36	66.7%	41	62.1%
3	Security software purchases	37	68.5%	47	71.2%
4	Security hardware maintenance	36	66.7%	41	62.1%
5	Security software maintenance	38	70.4%	47	71.2%
6	Security administrator training	10	18.5%	21	31.8%
7	Employee training/ education	6	11.1%	17	25.8%
8	Obtaining security-related certifications	6	11.1%	15	22.7%
9	Expenses of maintaining security-related certifications	4	7.4%	16	24.2%
10	Not sure	6	11.1%	6	9.1%

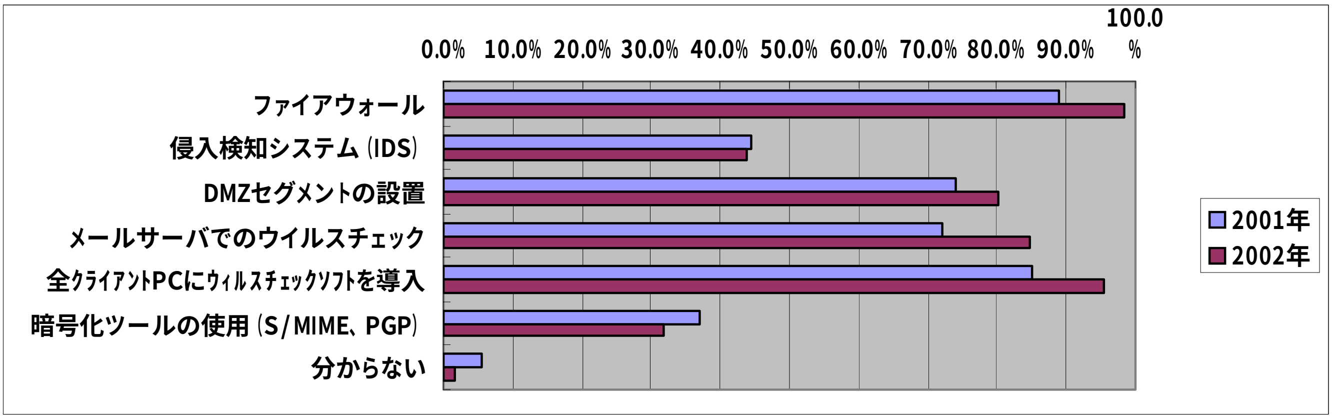


Note

The results of this question show a marked increase in training and education-related expenditures. The increase in certification-related budgets appears logical, given the increase in the number of companies obtaining third-party certifications.

C-15　Indicate systems used to ensure information security. (Mark all that apply.)

		2001		2002	
1	Firewalls	48	88.9 %	65	98.5%
2	Intrusion Detection Systems (IDS)	24	44.4 %	29	43.9%
3	Set up DMZ Segments	40	74.1 %	53	80.3%
4	Virus checks on the mail server	39	72.2 %	56	84.8%
5	Implement virus checks on all client PCs	46	85.2 %	63	95.5%
6	Encryption tool usage (S/MIME, PGP)	20	37.0 %	21	31.8%
7	Implement virus checks on proxy servers	-	-	21	31.8%
8	Not sure	3	5.6%	1	1.5%

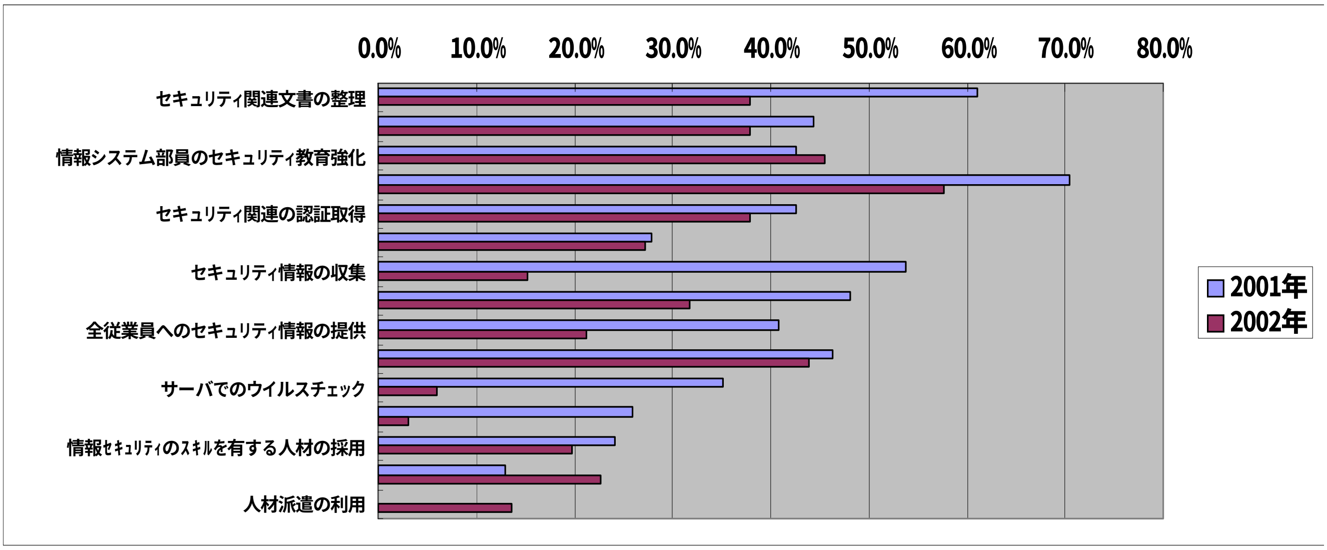


Note

Almost all respondents indicated they have installed firewalls (only one respondent has not). With respect to virus countermeasures, aside from one company, all firms have adopted periodic virus checks on servers, client PCs and proxy servers—perhaps a significant contributing factor to the prevention of major virus outbreaks during this year at those firms.

C-19 Current or planned measures for information security. (Choose all applicable.)

		2001		2002			
		Future	%	Already Implemented	%	Future	%
1	Prepare security-related documentation	33	61.1%	27	40.9%	25	37.9%
2	Define internal system for information security	24	44.4%	26	39.4%	25	37.9%
3	Security training reinforcement for information systems personnel	23	42.6%	21	31.8%	30	45.5%
4	Security training reinforcement for all employees	38	70.4%	21	31.8%	38	57.6%
5	Obtain official security certifications	23	42.6%	12	18.2%	25	37.9%
6	Implement systems for obtaining official security certifications	15	27.8%	5	7.6%	18	27.3%
7	Gather security information	29	53.7%	44	66.7%	10	15.2%
8	Conduct system audits	26	48.1%	20	30.3%	21	31.8%
9	Provide security information to all employees	22	40.7%	38	57.6%	14	21.2%
10	Incident/ accident response training	25	46.3%	9	13.6%	29	43.9%
11	Virus checks on servers	19	35.2%	56	84.8%	4	6.1%
12	Virus checks on client PCs	14	25.9%	60	90.9%	2	3.0%
13	Employ personnel who possess information security skills	13	24.1%	20	30.3%	13	19.7%
14	Use ASPs (Application Service Providers) and IDCs (Internet Data Centers)	7	13.0%	14	21.2%	15	22.7%
15	Use contract employees	0	0.0%	6	9.1%	9	13.6%



Note

The above graph compares year-on-year responses for “Planned measures”. Most categories show a decrease in frequency compared with the prior year. One possibility for this is that, with the exception of new personnel-related measures, the respondents have succeeded in putting basic countermeasures in place.

3.4.3 Overview of Damages Incurred

For the 2001 Information Security Incident Report, of the 55 entities surveyed, 33 (61%) had experienced an incident. In contrast, of the 66 entities surveyed for the 2002 report, 11 (17%) had experienced an incident, an almost 75% decrease compared to the prior year. In addition, the scale of damages incurred was limited, as were the corresponding damage costs.

① Damages Incurred (Damage Costs per Incident, Descending Order)

No.	Payroll/Day (¥)	Damage Costs (¥)							Total (¥)	Notes
		Business Contingency Costs	Lost Profits	Lost Information Assets	Opportunity Costs	Guaranteed Reparations	Other Costs	Recovery Costs		
1	*40,000*						400,000		400,000	Note 1
2	30,000		60,000					270,000	330,000	
3	50,000	150,000						25,000	175,000	Note 2
4	*40,000*							150,000	150,000	
5	*40,000*	120,000							120,000	Note 3
6	*40,000*						20,000	100,000	120,000	
7	50,000							25,000	25,000	Note 2
8	*40,000*							15,000	15,000	Note 4
9	*40,000*								0	Note 5
10	*40,000*									Note 6
11	*40,000*									Note 7
								Grand Total	1,335,000	
								Avg.	121,364	

■ Calculation Terms

- When available, we utilized the damage cost figures supplied in Incident Survey Questionnaire Questions 12-19.
- When figures from Questions 12-19 were not available, we used answers from Questions 5-21 and payroll expenses to estimate figures for use in our calculations.
- Where payroll expenses were not provided, we assumed a rate of ¥40,000 per day per person. (figures shown in *italics*.)

■ Notes

(Note 1) Apologies to Affected Parties: Calculated at 10 Person-Days x Single Employee Cost per Day (¥40,000).

(Note 2) No.3 and No.7 are the same company.

(Note 3) Calculated as Downtime (1 day) x No. of People Affected (10 People) x Ratio of Lost Work Production (30%) x Single Employee Cost per Day (¥40,000)

(Note 4) Calculated as Downtime (0.125 days) x No. of People Affected (3 people) x Single Employee Cost per Day (¥40,000). Downtime calculated as one hour out of 8 working-hours per day.

(Note 5) Response cited no actual damage incurred.

(Note 6) Only the number of people affected was provided; could not calculate damage costs without downtime information.

(Note 7) Only the number of people affected was provided; could not calculate damage costs as downtime was listed as "0".

Note

As mentioned above, we discovered a major decrease in reported incidents between last year (FY2001) and this year (FY2002), from 61% to 17% of respondents. With respect to damage costs, last year's grand total was ¥141,478,800, and average of ¥4,715,960 per respondent. In comparison, the 2002 figures were approximately one-fortieth of the prior year, with a grand total of ¥1,335,000, averaging ¥121,364 per respondent. The highest damage cost for a single incident was ¥60,000,000 for 2001, while the highest damage cost for a single incident was ¥400,000 for 2002, again, quite a significant comparative decrease.

② Damage by Incident (By Frequency)

Code No.	Incident Type	No.	% of Total	Cost	% of Total
1	KLEZ	4	36%	310,000	22.88%
7	FLETHEM, etc.	3	27%	355,000	26.20%
10	Unauthorized access from outside	2	18%	550,000	40.59%
14	Router malfunction Caused by SPAM	2	18%	140,000	10.33%
	Total	11	100%	1,355,000	100%

Note

Compared with the prior year, damages caused by computer viruses decreased greatly. Virus-caused damages accounted for 49.08% of the total, while damages other than viruses accounted for 50.92% of the total.

③ Observations from Companies Incurring Damages

The reasons for the significant decreases in the number of incidents and accompanying damage costs most likely lie in the fact that the survey subject is focused on computer viruses, and that survey participants have had another year to put a certain level of virus countermeasures in place and in operation.

Next, we have compiled observations related to the security countermeasure profiles of the companies included in the Information Security Incident Report.

No.	Industry	Employees (people)	Policies Already in Place	Cause of Incident
1	Information/ Communications	1,200	・ Security policy in place ・ Incident communications system in place ・ Firewalls, IDS, DMZ installed ・ Latest patches applied	Unauthorized entry into 7 DNS servers. Cause was not given.
2	Other	3,700	・ Security policy in place ・ No incident communications system in place; incident response department in place ・ Periodic virus checks on servers and company PCs	Virus contracted through Extranet. Damage spread through Windows file sharing. Incident occurred on a Friday, so no business interruptions experienced.
3	Information/ Communications	600	・ Security policy in place ・ Incident communications system in place ・ Periodic virus checks on servers and company PCs	Virus checks conducted periodically, but anti-virus software was not installed on a replacement PC, which contracted a virus.
4	Information/ Communications	95	・ No security policy in place ・ Incident communications system in place ・ Firewalls, IDS, DMZ installed	Firewall malfunction
5	Other Services	No answer given	・ Security policy in place ・ No incident communications system in place; incident response department in place ・ Firewalls, IDS, DMZ installed	Router malfunction
6	Information/ Communications	800	・ Security policies incorporated in other company regulations ・ No incident communications system in place; incident response department in place ・ Periodic virus checks on company PCs	Login via PC without machine power did not trigger auto-virus scan, resulting in virus contraction. Virus spread through shared folder.
7	Same as No. 3			Manufacturer's computer virus update files arrived too late.
8	Information/ Communications	No answer given	・ Security policy in place ・ No incident communications system in place; incident response department in place ・ Periodic virus checks on servers and company PCs ・ No restriction on bringing in personal-use notebook PCs.	Virus contracted through personal-use PC without anti-virus software. Individual brought PC into the office, where virus spread through shared folders.
9	Finance	134	・ Security policy in place ・ Incident communications system in place ・ Periodic virus checks on servers and company PCs	No response regarding cause.
10	Other	983	・ Security policies incorporated in other company regulations ・ Incident communications system not in place ・ Periodic virus checks on servers and company PCs	Virus contracted before virus definition files were applied.

11	Other Services	2,400	・ Security policy in place ・ Incident communications system in place ・ Periodic virus checks on servers and company PCs	Virus contracted before virus definition files were applied.

The companies included in this year's report had enacted basic security measures, such as creating security policies, establishing incident communications systems, use of firewalls and periodic virus checks. We believe that these basic countermeasures served to limit the damage incurred during the security incidents listed above.

The cause of incidents can be categorized as follows:

(a) Force majeure/ acts of God

- System malfunctions
- Delayed virus definition update files from anti-virus software vendors

(b) Operational issues

- Delay in applying virus definition files
- Virus contraction from external sources via company Extranet
- Forgetting to install anti-virus software on replacement PCs
- Machine power insufficiencies
- Virus contraction via PC brought in from outside company

Since a certain level of security countermeasures had been in place, acts of God and/or operational issues were the contributing factors to the incidents, rather than external factors.

For incidents caused by factors outside the control of the user (system malfunctions or manufacturer delays, for example), the prior establishment of incident communications systems and prepared documentation determine the scale of damages incurred during the incident.

With operational issues, incidents with roots in artificial factors can be effectively prevented by establishing procedures, enhancing check functions, or automating such functions, if possible.

3.5 Survey Results Analysis and Observations

According to IPA (Information-Technology Promotion Agency) statistics, the number of computer virus incident reports was 10,352 for the year 2002, a 16% decrease from 2001. Reports indicating a company incurred actual damages were about one-half of the number in the prior year. The ferocity of the highly contagious Sirum and Nimda viruses during 2001 taught infected companies hard-learned lessons, spurring them to implement stronger virus countermeasures. We believe our survey is a reflection of this, with damage costs significantly decreased in comparison to the prior year.

We confirmed with several anti-virus software manufacturers that sales of their products did indeed increase in comparison with the prior year. However, we were told that a notable development was the conscientious update by users of their virus definition files, which was the most likely factor contributing to lowered levels of incidents.

According to our 2002 questionnaire, 100% of respondents have installed firewalls and anti-virus measures, with 43.9% of respondents also having installed Intrusion Detection Systems (IDS). Further, 100% of respondents indicated they apply updated security patches.

Firewalls, virus checks, IDS, etc. have been consistently employed as technological countermeasures preventing unauthorized access and computer viruses; however, the disclosure of private/ proprietary information, a major issue of these years, is caused primarily by human elements, such as improper settings or intentional dishonesty, which tends to require a higher level of management and operational measures, rather than purely technological ones.

With respect to operational measures, 87.9% of respondents indicated their company has established security policies, and a similarly high number of respondents reported their company has created incident communications systems, and conducts some form of training and education. We believe this progress in technological and operational preparations has led to the results of this year's survey, which indicate effective limitation of incident damage costs.

On the other hand, those companies who were subject to a security incident during 2002 had all implemented some form of technological countermeasures and policies, which leads one to believe there is room to reconsider the thoroughness of in-house education and check functions. We expect that companies will have to balance considerations of convenience with the need to create enhanced operational rules and management systems that incorporate disciplinary and other measures to guarantee employee adherence.

With respect to budgets, our survey revealed that 65.2% of responding companies include the budget for information security as part of the overall information systems budget. Also, we discovered that the ratio of security budget to overall sales was extremely low, suggesting that security countermeasures have much less priority compared with other corporate activities.

One reason for the difficulty in securing budget funds for security countermeasures is the difficulty in objectively observing their effectiveness. We are considering modifying future questionnaires and interviews to help us quantitatively measure costs by including questions about the influence of implemented security technology on the incidence of security incidents, and how effective incident communications systems and other measures are in response to an incident.

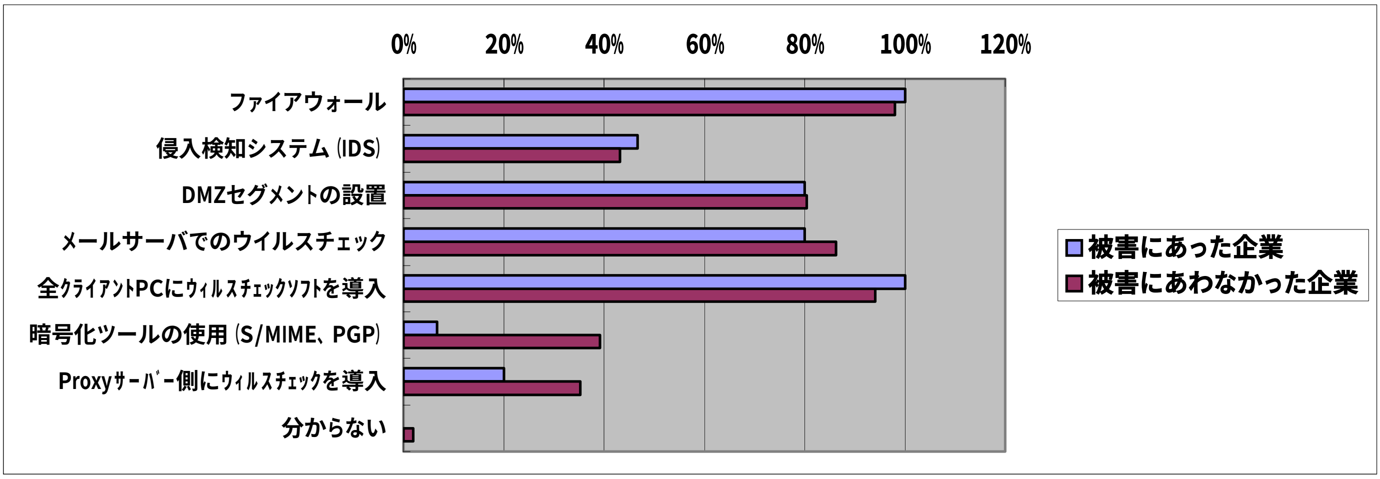
4. Standard Model and Costs with respect to Information Security Incidents

4.1 Information Security Incident Deterrents

We used the results obtained from questions related to "Systems implemented to ensure information security" to perform an analysis for the purpose of understanding the differences in countermeasures used by the "Group of companies that experienced information security incidents" and the "Group of companies that did not experience incidents".

	Systems Implemented to Ensure Information Security	Companies that Experienced Incidents (15)		Companies that did not Experience Incidents (51)	
1	Firewalls	15	100%	50	98%
2	Intrusion Detection Systems (IDS)	7	47%	22	43%
3	Set up DMZ segments	12	80%	41	80%
4	Virus checks on the mail server	12	80%	44	86%
5	Implement virus checks on all client PCs	15	100%	48	94%
6	Encryption tool usage (S/MIME, PGP)	1	7%	20	39%
7	Implement virus checks on proxy servers	3	20%	18	35%

8	Not sure	0	0%	1	2%



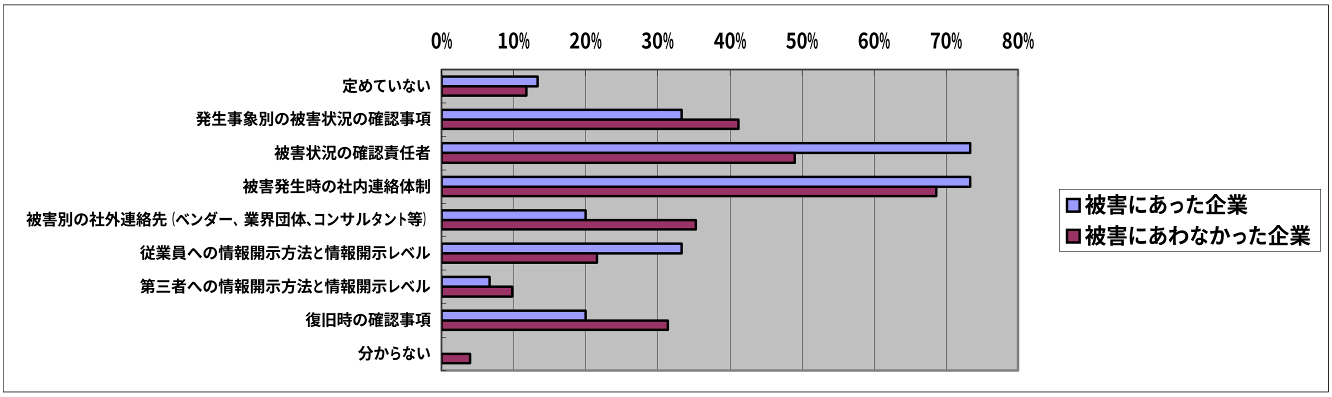
Observing the two groups does not reveal any particularly large differences. The graph indicates that the group not experiencing security incidents had a higher implementation rate for encryption tools and virus checks on proxy servers than did the group that experienced incidents.

However, given the nature of the security incidents experienced, it is difficult to conceive that this difference was a contributing factor.

The results of this year’s questionnaire do not reveal any particular causal relationship between “security system adoption rates” and “rate of incident prevention”.

Since there was no difference in technological measures undertaken, we created the following four graphs comparing the “Group that did not experience incidents” and the “Group that experienced security incidents” with respect to “Questionnaire categories related to corporate security consciousness” such as “System for handling security incidents”, “Security-related training and education”, and “System for accepting contract employees”.

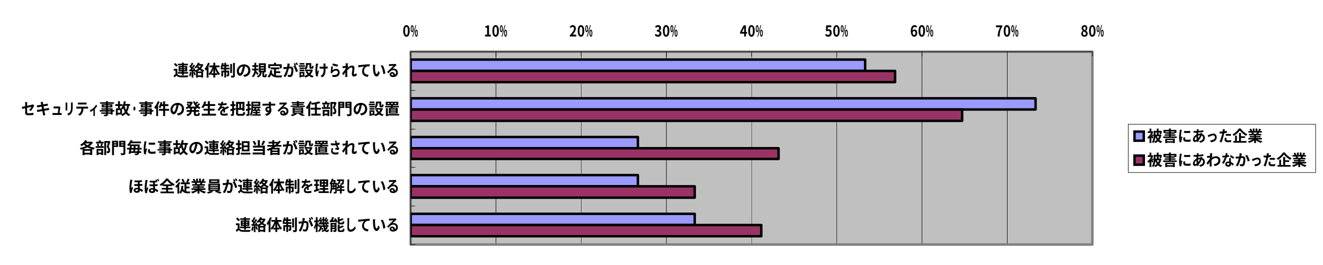
①Incident response plan



One particular difference seen in the graph above is that the “Group that experienced security incidents” had a higher rate of “Personnel responsible for confirming damage.” Since we do not have any information related to the timing of the incident and the establishment of responsible personnel, the circumstances of the safety measures are reversed.

With respect to this point, there is a possibility that respondents experiencing a security incident felt the need to define a person(s) responsible, and implemented this policy subsequent to the occurrence of the incident.

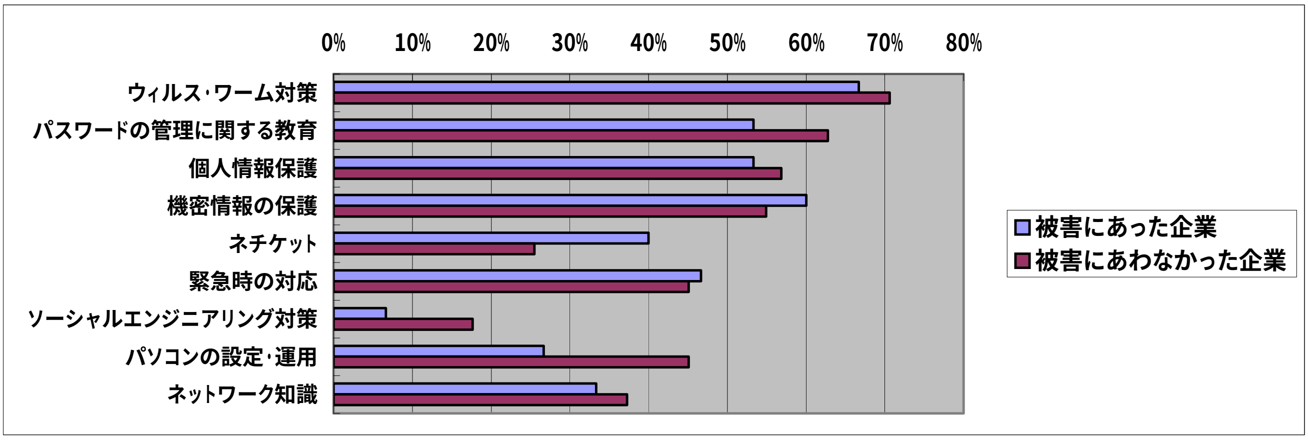
②System for Communicating Information Security Mishaps and Incidents throughout the Company



While the “Group that experienced security incidents” had a somewhat higher rate of having a “Department responsible for confirming incident damage” to handle the occurrence of a security incident, the “Group that did not experience incidents” had higher response rates in all other areas.

As mentioned above regarding the defining of a person(s) responsible, here as well, the company may have felt the need to define a responsible department subsequent to experiencing a security incident.

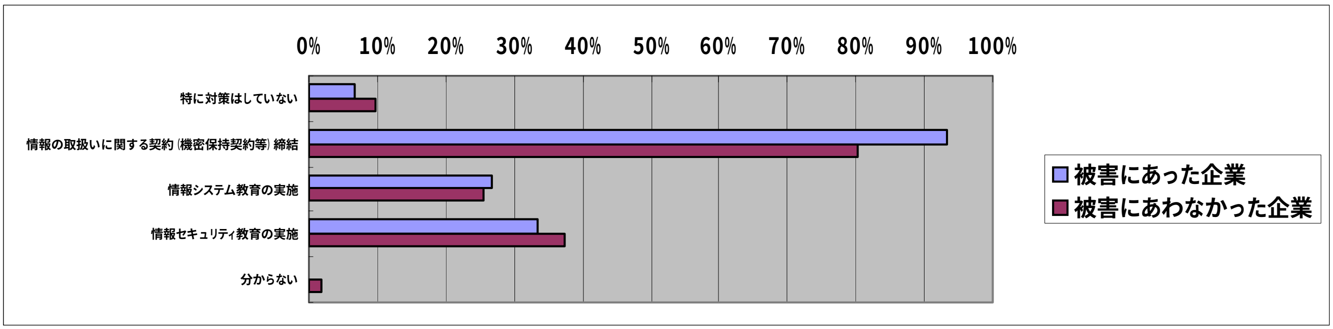
③Content of Information Security Training/ Education



Although there were differences in the rates of information security training and education with respect to Netiquette and PC settings/operation, there were no obvious causal relationships to the occurrence of security incidents.

For six of the nine categories above, the “Group that did not experience incidents” indicated a relatively higher response rate, which may indicate a more serious attitude toward information security training and education.

④Considerations when Accepting Contract Employees and Full-Time Engineers/Operators



There were no significant differences in considerations when accepting contract employees, etc.

Having compiled questionnaire answers to questions about information security countermeasures designed to deter information security incidents, our observations in this section unfortunately failed to reveal any correlation with security system (firewalls, anti-virus software, etc.) adoption rates.

However, since it is conceivable that systematic countermeasures were implemented immediately after an information security incident, we cannot make a sweeping conclusion that there is no relationship.

Further, we believe the “security system adoption rate” for questionnaire and interview respondents is much higher than that of other companies in general. Therefore, in our opinion, this directly results in the capability of these firms to limit damages from information security incidents to low levels.

We can see that non-system measures, such as “information security training and education” and “incident response systems” tend to contribute to incident deterrence.

4.2 Actual State of Deterrence Model Information Security Budgets

To analyze the results of this year’s survey, we divided respondents into two groups, one having experienced an information security incident during the year, and one that did not experience any incidents. Once we divided respondents into these two groups, we conducted a trend analysis for only those respondents who answered the questionnaire questions related to information security budgets.

①Group that Experienced Security Incidents (7 companies)

No.	Employees (people)	Security Budget (¥1,000)	Budget Ratio (%)	Budget per Person (¥)
1	100	200	1.0%	2,000
2	15,470	10,000	0.1%	646
3	983	5,000	-	5,086
4	800	2,000	8.0%	2,500
5	95	5,000	30.0%	52,632
6	6,487	50,000	0.5%	7,708
7	3,700	75,000	40.0%	20,270
Total	27,635	147,200	-	90,842
Avg.	3,948	21,030	13.3%	12,977

②Group that did not experience incidents (23 companies)

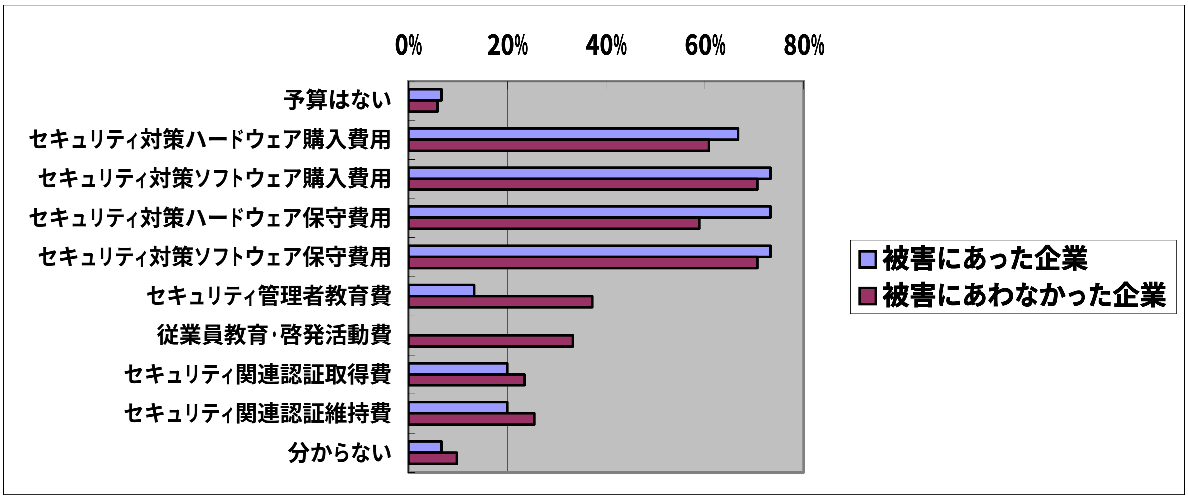
No.	Employees (people)	Security Budget (¥1,000)	Budget Ratio (%)	Budget per Person (¥)
1	1	300	10.0%	300,000
2	30	5,000	10.0%	166,667
3	140	11,000	65.0%	78,571
4	400	5,000	30.0%	12,500
5	400	10,000	-	25,000
6	6,000	10,000	1.0%	1,667
7	1,112	10,000	20.0%	8,993
8	80	4,000	25.0%	50,000
9	34	1,500	20.0%	44,118
10	32	8,000	10.0%	250,000
11	130	1,500	20.0%	11,538
12	980	10,000	3.0%	10,204
13	120	30,000	50.0%	250,000
14	220	30,000	-	136,364
15	5,000	100,000	3.0%	20,000
16	650	30,000	9.0%	46,154
17	250	4,000	2.5%	16,000
18	56	3,000	-	53,571
19	551	10,000	7.0%	18,149
20	900	4,000	3.0%	4,444
21	2,800	12,000	2.0%	4,286
22	330	2,560	5.0%	7,758
23	2,100	55,000	3.0%	26,190
Total	22,316	356,860	-	1,542,174
Avg.	970	15,520	14.9%	67,051

Due to the difference in size between entities that did/ did not experience security incidents, a simple overall comparison cannot be performed. However, comparing the two groups based on security budget per employee reveals the security budget for the “Group that did not experience incidents” is three times as large as the other group, ¥15,991 per employee vs. ¥5,327 per employee.

Considering that the trend that the larger the company, the less is spent on information security per employee, and the fact that the definition of information security budget differs among companies, we cannot simply conclude that companies not experiencing security incidents spend three times as much on security as those companies that do experience security incidents; however, we will continue to collect data and watch these trends in future surveys.

Next, we compared the content of information security budgets by group:

	Allocation of Information Security Budget	Companies that Experienced Incidents		Companies that did not Experience Incidents	
1	No budget	1	7%	3	6%
2	Security hardware purchases	10	67%	31	61%
3	Security software purchases	11	73%	36	71%
4	Security hardware maintenance	11	73%	30	59%
5	Security software maintenance	11	73%	36	71%
6	Security administrator training	2	13%	19	37%
7	Employee training/ education	0	0%	17	33%
8	Obtaining security-related certifications	3	20%	12	24%
9	Expenses of maintaining certifications	3	20%	13	25%
10	Not sure	1	7%	5	10%



The results of this comparison reveal that, although not significant, the group that experienced security incidents tended to be somewhat higher in budget allocated to security hardware/software purchase and maintenance.

At the same time, the group that did not experience incidents spent a significantly higher ratio of their budgets on training and education activities. This tendency is consistent with the results from “4.1 Information Security Incident Deterrents.”

These observations lead us to conclude that recent information security incidents are caused more often by acts of God or human inattentiveness that get around the technological measures that have been adopted.

In other words, companies must create a system of “Training/ Education/ Incident Countermeasures” to keep information security incidents in check.

4.3 Suggestions for Appropriate Response Levels and Budgets

In the recent years, most of information incident damages have been caused by computer viruses.

In response, the adoption of technological countermeasures such as anti-virus software has been increased, and the implementation of multiple countermeasures installed on clients, servers and gateways has become the norm in most companies.

The tendencies of computer viruses morphed to do more to affect systems, attacking other computers and servers, attaching stored computer files to emails to reveal private or proprietary information, spoofing other mail users' accounts, and more. Those charged with protecting computer networks have come to not only implement measures to prevent themselves from becoming victims, but also from becoming unwitting participants in attacking other entities' systems.

Looking at several examples of actual information security incidents, we see the intrusion of new types of computer viruses and the introduction of viruses via notebook PCs connected to internal networks. Even the installation of comprehensive anti-virus software has not been a guarantee against contracting computer viruses.

It is a company's security policy that prevents such infections. Policies must remind employees to be careful about opening Email attachments, and restrict the bringing in or taking out of notebook PCs. It is also important for firms to create a crisis response manual for times when infected Emails are sent to others outside the firm.

Almost 100% of the respondents to this year's survey have implemented firewalls to prevent unauthorized network access by outside individuals, keeping damage from such incidents to a minimum.

These firms also appear to conscientiously apply updated security patches, demonstrating a good understanding of what they should be doing to prevent unauthorized network access.

We believe that this trend has more to do with the increasing news coverage related to accidental private information disclosures, and that these companies understand the importance of preventing the disclosure of such information as well as preparing measures to respond to any accidental disclosures, rather than focusing their attention on countermeasures to prevent unauthorized alteration of company websites or other mischief by offenders for pleasure.

①Currently Conceivable Minimum Response Levels

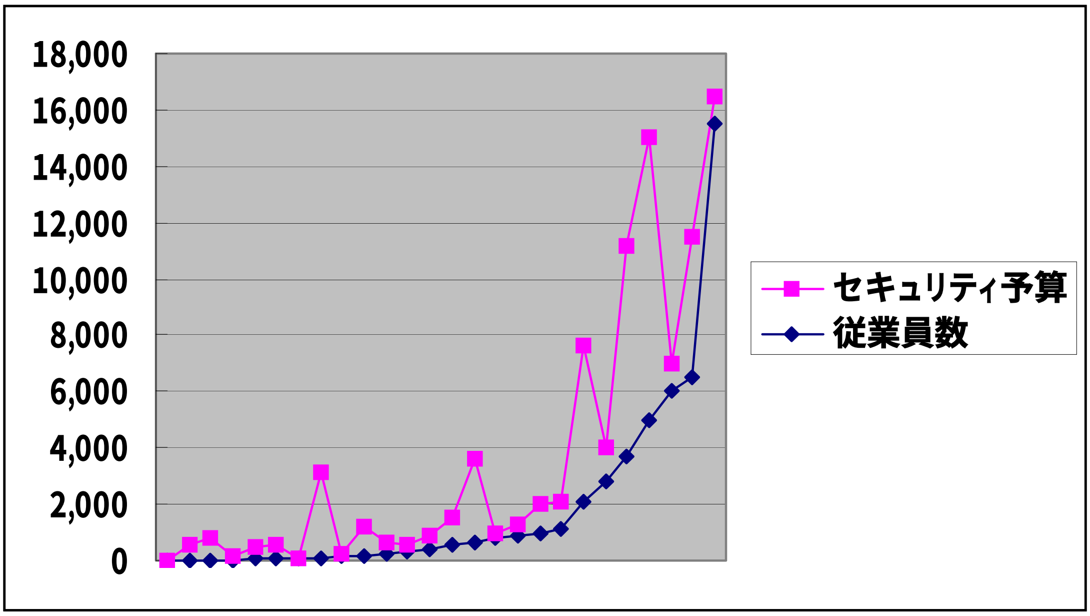
Taking a look at these incidents and our survey results, we have created the following chart outlining our recommendations through the level of “security and training activities to instill users with knowledge of operational security measures.” These recommendations are not based on “Idealism or Perfect-World Theories”, but rather on the response levels that are realistically conceivable at this time.

Response Level		Example
Response Level 1	Technological Measures	Anti-virus software
		Email administration software
		Firewalls
		IDS
		Authorization/ recognition devices
Response Level 2	Operational Measures	Physical facility access management
		Appoint security management personnel
		Create information security policies
		Create security incident response manual
Response Level 3 (recommended level)	Information Security Training and Education	Computer virus education
		Password management education
		Proprietary information protection education
Response Level 4	Security Audits, Third-Party Certifications	ISMS, BS7799
		P MARK

②Correlation between Number of Employees and Security Budget

Examining the results of this year’s questionnaire shows that the ratio of a company’s information security budget to their information systems budget ranges from a maximum of 65% (140 employees) to a minimum of 0.1% (15,470 employees), with an average of 14.5%.

As seen in the figure below, the number of employees and corresponding security budget figures

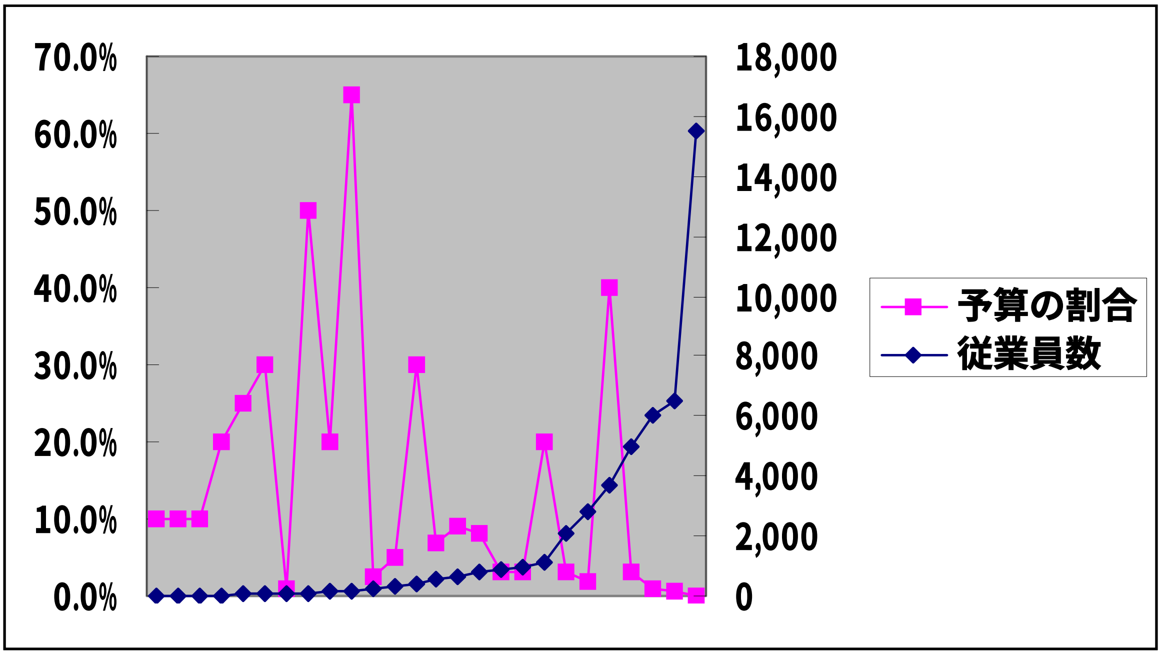


move in almost perfect proportion.

③Comparison of Information Security Budget Ratios with respect to Number of Employees and Information Systems Budget

While the ratio between number of employees and information security budgets show an inverse trend, as seen in the figure below, the distribution of data is quite large. Almost without exception, interviewees asked us the basic question, "What is included in a security budget?" For example, when asked, "Is a router a piece of security equipment or communications equipment?" we see the difficulty in determining what should go under the category of security budget.

In addition to the problem of the vagueness of the definition of budget, newly purchased hardware or software can temporarily account for a significant portion of a budget. At the same time, it is conceivable that the amount of the information systems budget as a ratio of the overall management budget can change drastically based on the type of industry, size of company, and time period in question.



In addition, there is no rule of thumb stating, "Most corporations devote xx% of their information systems budget to security. Looking back on the results of our interviews, we see that the current state of affairs is that budget requests and disbursements are more often than not made on an as-needed basis.

While we acknowledge these difficulties and the wide variation in the size and scale of different companies, we have observed that at most corporations "information security maintenance, operations and security training costs" account for between 5% and 15% of most companies' information systems budgets.

In our opinion, it is important for a company to create and methodically enforce a yearly schedule for “security training and education activities” as a cornerstone of their security countermeasures.

5. Considerations for the 2002 Information Security Incident Damage Cost Calculation Model

Here, we will build upon the prior year's model in considering the further development of a calculation model for damage costs related to this year's information security incidents.

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.

Revisions or additions to the 2001 model (revisions or additions made in 2002) will be indicated in green letters.

5.1 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.

5.1.1 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:

$$\boxed{\text{Lost Profits}}=\boxed{\text{Sales profits per hour}}\times\boxed{\text{Number of hours the system/ network was unavailable}}$$

"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:

$$\boxed{\text{Direct Damage Costs}}=\boxed{\text{Lost Profits}}+\boxed{\text{Costs incurred to restore system}}+\boxed{\text{Business contingency costs}}+\boxed{\text{Lost information assets}}+\boxed{\text{Opportunity Costs}}$$

5.1.2 Indirect Damages

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.

$$\boxed{\text{Indirect Damages}}=\boxed{\text{Indirectly incurred damages: Reparations, supplemental costs, legal compensation, etc.}}$$

5.2 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.

5.2.1 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:

$$\begin{aligned}\boxed{\text{Hidden Damage Costs}} &= \boxed{\text{Hidden Damages related to work}} + \boxed{\text{Non-work-related Hidden Damages}}\\ &= (\boxed{\text{Fixed Costs (payroll)}} \times \boxed{\text{Number of People Affected by the incident}}\\ &\qquad \times \boxed{\text{Degree of reliance on IT}} \times \boxed{\text{Downtime}})\\ &\quad + \boxed{\text{Non-work-related Hidden Damages (decrease in brand value, etc.)}}\end{aligned}$$

5.3 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":

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

<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, verification of the 2001 survey 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.

6. Future Issues of Interest

6.1 Model Issues

We have attempted to take the previous year's model, and then incorporate new considerations to develop a more robust model for calculating damage costs.

Through this process, we have defined words used in the prior year's model, confirmed factors that should be incorporated, and expanded the scope of the model, building a more refined description.

However, while these factors contributing to damages and the scope of the model are understandable in theory, we acknowledge that many insufficiencies remain. We intend to develop this model further, answering unresolved issues in an attempt to create a more detailed and accurate description.

6.1.1 2002 Information Security Incident Damage Cost Calculation Model Issues

In "5. Considerations for the 2002 Information Security Incident Damage Cost Calculation Model," we have presented a new model based on the results of our investigations this year, and provided supplemental descriptions of certain model factors. However, there still remain many factors difficult to derive when attempting to perform actual calculations even with this year's model.

The "Reliance on IT", which has been an issue since last year, was not developed significantly this year, as we still were not able to obtain enough data to make a meaningful reassessment of this factor. We believe that if this model is to be widely useful in the future, we must be able to use information related to the varied systems of different corporations or industries to develop a certain level of quantification.

6.1.2 Information Security Incident Standard Model Issues

In "4. Standard Model and Costs with respect to Information Security Incidents," we analyzed generally adopted countermeasures for "Companies that experienced information security incidents" and "Companies that did not experience information security incidents" during the period under survey, and proposed a standard model for countermeasures.

We conducted a variety of analyses based on the information obtained through our questionnaire; however, the overall low number of companies experiencing security incidents, and the post-incident measures adopted by companies did not result in any obvious significant differences between these groups.

The time lag between the occurrence of an incident and our questionnaire means that in the future, we need to get more information related to countermeasure implementation timing in order to draw a correlation between incident occurrence and countermeasure adoption.

With respect to budgets, it appears that funds are acquired on an as-needed basis, making it difficult to draw a distinction with systems budgets in many cases. However, we did note a growing number of companies introducing specific security budgets, which is a trend we hope will continue to grow. We believe that expenditure line items suggested by security experts may play a large role in helping corporate management formulate security-oriented budgets.

6.2 Survey Issues

6.2.1 Questionnaire Issues

For this year's survey, we reexamined the lengthy questionnaire used last year, and after careful consideration, created a much more focused set of questions.

However, we still noted several problems and issues related to the questionnaire used this year, as identified below:

- Although there were some respondents who provided specific examples on the Damages Incurred survey sheet, in general, we noted mostly blank answers, as many of the persons responding had not confirmed incident details. In most companies and organizations, system administrators only have knowledge about their measures and damage in their immediate purview, making it difficult to provide answers reflecting a financial representation as to the amount of damages incurred.
- Since we made a major revision in the questionnaire, we were not able to easily perform a comparison between last year and this year. In the future, we will do our best to keep the same questionnaire format, enabling us to conduct year-to-year fixed point observations.

6.2.2 Interview Issues

As in the prior year, interview survey participants were limited to JNSA member firms who had answered our questionnaire, and the handful of corporations who agreed to be interviewed. The overall reaction to interview participation was positive, and this was the second year of interviews for many of the companies.

The following lists problems and issues related to the survey interviews:

- As with the prior year, the interview related to security issues, and survey participants were basically limited to those companies and organizations with ties to the working group membership.
- A handful of entities who agreed to interviews last year, did not wish to participate in interviews this year. It appears that with increases in security management, some aspects of this survey have become difficult to conduct.
- Surveys were conducted by a team of two working group members, the lack of sufficient personnel and time made it difficult to put together a comprehensive interview schedule.

7. Conclusion

Continuing the work of the prior year, we conducted surveys and investigations of information systems incidents, with participants that included a certain number of industry-leading companies from among the JNSA membership. The selection of topics for our 2002 survey was expanded to also address research and findings related to public announcements of accidental exposures of private/proprietary information. Many different organizations conducted a great number of incident and vulnerability surveys in Japan during 2002. Questionnaires distributed by such organizations as the Information Technology Promotion Agency (IPA) and the National Police Agency incorporated questions designed to uncover information related to incident damage costs.

However, damage costs reported by survey participants carried no common definition for the scale of damages incurred, nor standards for defining the type and scope of such damages. We are led to the conclusion that much of the information included in these surveys relied on the subjective intuition of the person answering the survey questions.

Given these circumstances, the Japan Network Security Association (JNSA) decided to conduct a second annual survey, to be administered by the JNSA Security Incidents Investigation Working Group, focusing on obtaining factual evidence related to incident damage costs and countermeasure expenditures at Japan’s core industries, consisting mainly of JNSA member firms.

The objective of this survey was to gain a clear understanding of the current circumstances surrounding information security incidents, and to gather extremely important, fundamental information about risk management in the information security field.

The JNSA survey consisted of both a questionnaire and direct interviews of participants. This helped the working group obtain highly precise information, while at the same time allowing the group to construct a model to estimate damage costs, and to discover differences among respondents related to incident occurrence and the existence of countermeasures.

The working group focused much of their effort on re-designing the questionnaire and its content; however, we still noted many respondents who were not able to answer questions asked in the questionnaire or in interviews.

We were fortunate in that many corporations were willing to cooperate with a second year of questionnaires and interviews. We wish to take this opportunity to thank them.

Of those companies not willing to cooperate with our survey, many indicated that corporate security policies prevented them from doing so. We expect the struggle that many corporations have with respect to participation in surveys that run counter to standard company security policies; how to deal with this issue will be an ongoing challenge for future survey activities.

In Section Two (Supplement) of this survey report, the Security Incidents Investigation Working Group has conducted further considerations of data related to publicly announced accidental exposures of private information as a basis for further investigation and discussion. The Working Group offers specific numerical figures related to damage costs from legal compensation payments and the influence on corporate share prices, (one factor in deriving corporate value) with respect to such incidents. These figures are the result of an extremely limited scope of debate and discussion, and include many legal issues not within our scope of expertise. Although we did conduct some discussions with attorneys, we cannot deny that at the current time, the proposed figures are not precise.

However, we hope that clearly demonstrating incident-related damage calculations and the process by which such calculations were derived will encourage experts to address these issues, and to develop more precise models and calculations. We further hope that these security issues become a common point of discussion for experts from a variety of fields, promoting a more sophisticated model for “Understanding Risk Level”—a prerequisite to information systems risk assessment—playing a helpful role in the development of a safe information society.

Lastly, we wish to express our gratefulness to the project team members, who rose to the challenge of taking time out of their busy year-end schedules to accomplish the many tasks associated with this survey. We also express our thanks to the individuals who agreed to participate in the corporate interviews, sharing their honest opinions. We intend to continue conducting periodic, comparable survey research projects. We believe there is great value to be held in continuing to compile these reports, and in the ongoing activities of the Security Incidents Investigation Working Group. Our desire is to be able to use the results here to provide more information reflecting real-world circumstances, offering valuable data to the public and private sectors as the need to enact rational security measures increases.

8. Reference Data

8.1 Interview Compilation

The following is a brief summary of the content of interviewee answers to the interview survey questions, categorized by questionnaire topic.

Systems Structure, Including Number of PCs (Questionnaire Question B-1)
・150 client PCs, servers (2 mail servers, 1 Web server, 1 file server). ・Approx. 10 servers for development work.
Approx. 900 PCs.
5 or 6 internal servers (DNS, SMTP, etc.), 30 to 50 file servers.
・Approximately 5,000 client PCs, several hundred servers. ・QND used for systems management.
Slightly less than 700 PCs (one/ employee, does not include off-site PCs).
1,500 PCs (one/ employee), 80 department servers.
Approximately 8,000 PCs (online and offline), several work process servers, 400 servers for other departments.
・Approximately 800 client PCs (more than one/ employee, about 30% are notebook PCs), approximately 80 servers (20 UNIX servers).
3,000 PCs. One PC per manager, office works use group PCs.
・900 PCs (one/ employee), 20 servers (internal mail, work process) ・Does not include enterprise system hosts.
Approximately 3,500 PCs, 300 internal servers, Web server for external.
More than 30,000 PCs (At least, one for each employee, contract employee, SE, etc.)
Approximately 1.5 PCs per employee for Email and work, 8 file servers, 3 Web servers, 1 Mail server, 1 accounting and finance server.

Email Usage (Questionnaire Question B-2)
Restrictions on Attachment Size. Virus checks conducted. No current prohibitions on external mail accounts.
・File attachment restricted to maximum 10MB. ・Not sure as to specifics for Group mail filtering (probably conducted by parent company).
・Attachment file size limits (Max. 2MB). ・Email address name is determined by company when employee is hired. Notes is used as the mailer, OE is also used sometimes.
File attachment size limits. Limitation was enacted due to problems with large file (program) attachments in the past. Internal mail server. Use Linux Sendmail. POP mail available externally. No encryption used. Considering implementation of A-POP security, but difficult to change settings since no unified mailer is used by all employees.
・File attachment restricted to maximum 3MB. ・Almost all employees use Email (by request only)
Propriety Webmail (IMAP) used by 7,000 employees. Servers all located in Chiba Center.

･No exe files allowed as attachments. ･Mail folder limited to 50MB per person. ･One email address per person, some shared addresses for “work” contact purposes. ･Mail address names do not reveal sex of address owner.
No particular restrictions in place. Internet mail by registration: 2000 IDs, filtering software used for Web browsing.
Email available with file size limitations (500KB in principle, but no system limitations implemented). Mail usage (server, client PCs use Notes); approximately 70% of employees use Email.
Email available with no particular restrictions (2MB to 3MB attached file size limitation in principle, but no system limitations implemented). ･PC distribution conducted by information systems; no particular Email software such as Outlook used. ･Groupware (Notes) ･Keyword check conducted on outgoing/ incoming Emails.
Generally available, but limitations on type and size of attachments. Use Microsoft Exchange Server. (Outlook-based system), POP3, IMAP available. Each employee has Email address. Contract employees, SE must request mail address.
One Email terminal per floor. No internal LAN connection. Each terminal has a shared Email address. Email addressee is notified by whoever notices arrival of Email. File attachments are delivered via floppy disc.

Web Browsing Usage (Questionnaire Question B-3)
No specific limitations employed. Gambling sites, online stock trading sites, etc. prohibited in principle.
Considering filtering tool implementation. Each work group provided with updated rules/ restrictions annually (bulletin board posting prohibitions, Web virus prevention, security audits).
Web browsing must be done through proxy server.
･URL filtering implemented. (Regulations are somewhat lax)
No special restrictions. Causes impediment to development work; no port restrictions. Proxy not used. NAT used. Access logs compiled at firewall. Stored to HD in 6mos. to 1yr. increments (later moved to CD-ROM). Log analysis not conducted frequently. Conducted more frequently when experiencing increases in occurrences of Nimda, CodeRed, Slammer, etc.
･Web filtering used. (Less than 10 warnings for accessing adult, drug, dating websites)
Only available through dedicated terminals. Approximately 450 Web-capable PCs throughout company.
･Content filtering used for Web browsing. (filtered content includes adult, gambling, stock trading sites; restriction policies communicated to employees) ･Violations exist, but intentional access of restricted sites is infrequent. Mainly accidental. ･Persons under “suspicion” identified at each quarterly meeting. (knowledge of filtering operation; used for main work)
Generally available, with limits on permissible sites. Online ticket purchases, etc. are allowed for human resources personnel only.
No particular restrictions in effect (Web access available by request).

No particular restrictions in effect (As a guideline, no non-work related websites may be accessed).
Web access allowed, with limitations. Authorization password required when connecting. URL filtering restrictions. Filtering to prevent access to harmful sites (sites instigating illegal activities) and attack sites (sites exploiting browser vulnerabilities with Nimda, etc.).
Web browsing via Email terminals. Filtering restrictions not implemented.

Ratio of PCs with Email/ Web Access (Questionnaire Question B-4)
100% Email/ Web Browsing
Email: 82.5% (7,000/ 8,000) Web: 5.7% (450/ 8,000)
Email 80%; Web Browsing 50%
Email: 90% Web Browsing: 30% to 40%
Email: 90% Web Browsing: 90%
Email 50%/ Web Browsing 50%
Email 5%/ Web Browsing 5%

Regulations Related to Information Security (Questionnaire Question C-1)
･Created formal information security policy in 1996. ･Disciplinary rules enforced for policy violations.
･Audit and policy creation by consulting firm. ･Maintenance conducted annually. ･Annual verification of policy operation; verify whether enforcement is based on firm wide policies ･Composition: First Half of Year: General; Second Half of Year: Management
･Created security policy approximately three years ago in 2000. ･Conduct policy maintenance annually, based on interviews, etc. ･Policy is not disclosed to external parties (no particular reason; no requests from external parties) ･Discipline for violations defined in workplace regulations.
Policy explained to all employees once in the past. Newly hired employees receive policy explanation and sign agreement. No specific policy-related discipline; violations treated according to company rules.
･Security policy revision not implemented yet. ･ Discovered lack of logs for tracking documents during review of general policies (discrepancy between document management rules and electronic data management rules). ･No particular disciplinary policies for rules violations.
･Created a policy outline in 1999, but was not distributed throughout the company; created a formal firm wide policy during 2000 (60-page manual distributed to entire company). ･Related company conducts systems development work; has implemented a different policy than parent company. ･ Policy reviews conducted when incidents incurred or predicted; major policy review conducted during 2001.

•Policy for external disclosure only. •Discipline for violations taken from work conduct policies (one employee disciplined in the past for using auction websites). • Feel that security policy has been beneficial (Direction of company security clarified. Procedures for document and Email handling are clear. Reflected in development work, beneficial influence on regular work).
Formal information security policy in place (created by Risk Management department). Information Systems department has created regulations related to electronic media. The regulations indicate only that they may enforce disciplinary actions; no specific connection with human resources regulations.
Information security rules included in other policies.
Currently creating security policy. Temporary policies in effect for information systems.
•When first creating security policy, there were no other entities creating policies in Japan; therefore, policies were easy to create and implement without having to worry about effects on other entities. • Maintenance conducted annually. • Policy is not disclosed externally. • Discipline for policy violations is performed based on employee work conduct policies. • Beneficial effects of creating policy/ obtaining certifications include increased employee security consciousness and enhanced business reputation.
Created policy with help of outside consultant (2003). Access to important personal/ proprietary information granted by issuing access permissions by ID. Network login ID logs managed at the section level. (Login is performed at the section level; therefore, individual level log information is not acquired) Formal physical facility access regulations have been in place for some time (including sign-in records for machine room access, outside visitors, etc.) Formal procedures in place for responding to host system incidents. Response for handling routers, hubs and other network equipment issues based on experience. Incident communications system in place (including system for communicating with vendors).

Information Security Management Structure (Questionnaire Question C-3)
10 IT personnel; 10 General Affairs, managers and above.
Eighty to ninety percent of work time for personnel with information security duties is devoted to security work. Each department has a person in charge of security management (department manager); however, less than 10% of their time is spent on security matters.
Total of four information security personnel. Responsible department is related to General Affairs. Network manager is responsible for security; therefore, most of their work centers on network maintenance. Security-related duties include disseminating MS patch information, account management, SNMP surveillance, etc.
• Personnel with dual responsibilities spends approximately 4 hours per month on security-related work. • Each department head is responsible for department security (role includes defining sensitivity level for information assets, etc.)
Eight individuals with dual responsibility (two employees, six individuals from vendors)

•Department head is also responsible for department security. •One person with dual security responsibility spends 40% of their time on security; two other personnel spend 20% each of their time on security matters.
One responsible person (Information Systems assistant department head or equivalent)
Two personnel with dual responsibilities (20% or less spent on information security) Seventy systems personnel (5% or less spent on information security)
Two dually responsible personnel (Approx. 10% of time spent on information security)
•Person dually responsible spends 20% of their time on security matters.
Monthly log check conducted for firewalls (part of external vendor maintenance) Anti-virus pattern updates conducted at night. Network surveillance records verified at beginning of work.

Internal System for Communicating Accidents and Incidents (Questionnaire Question C-4)
Emergency response team set up to handle accidents.
•Contingency plan in place. •Training conducted periodically. •Created security accident database; accident records stored.
General Affairs personnel responsible for communicating accidents/incidents. However, no specific emergency response procedures in place.
•Internal communications system training conducted annually to verify efficacy. (Simulation of cyber terrorism attack over Saturday night; actual communications system used.)
Full-time help desk vendor used for response.
•Technology group takes charge of communications in case of accident or incident. •A trial system was put into place; system has come to function efficiently due to accumulation of experience from several accidents.
Communications system rules created, department designated to assess security accidents, employees notified of communications system. (However, each department does not have a specific person assigned to accident communications.)
Risk management established last year, communications system introduced to all employees, including communications system rules, departments responsible during accidents, department personnel in charge of communications, etc.
Communications system rules, responsible department during accident established. Basically Information Systems department should be contacted.
Communications system functioning properly from the top-down direction; bottom-up communications system has deficiencies. During the recent Slammer virus incident, reports came in from almost the entire company within a day; time taken to distribute instructions, reports has decreased significantly.
Information Systems department responsible for communications, department head or equivalent in charge of security in the facility. To date, system has been restored in approximately one hour, one-half day at worst case. Host or network incidents occur two to three times yearly; communications system is believed to work well.

Considerations when Selecting or Contracting with a Business Partner

(Questionnaire Question C-5)
Non-disclosure agreement not required of all outside contractors.
Seriously consider potential business partner’s management & services; require non-disclosure agreements and agreements defining service levels (SLA).
Verify at the sales department level (credit verification). Credit check sometimes required by business partner. Preparing to qualify for Privacy Mark.
Although not specifically security related, credit checks performed on potential business partners.
<Considerations and Points for Contractors> ･Special consideration given to business partners with well-known business and service levels. Past transactions and Teikoku Databank used to vet business partners. ･Incorporate non-disclosure agreements and Service Level Agreements (SLA) in basic contracts. <Requirements from Customers> ･Policy creation, non-disclosure agreements, Service Level Agreements (SLAs), audits from parent company, etc.
Non-disclosure agreements signed. Checked by legal department.
Require non-disclosure agreements.
Require non-disclosure agreements.
If requests come from customers, they are passed along and required of business partners as well. Otherwise, cost-performance issues studied before final decision. In reality, few business partners have acquired certifications.
Use RFP process often for service purchases. Audit data input contractors annually; physically observe warehouse where backup tapes are stored several times annually.

Considerations when hiring Contract Employees and Full-Time Engineers/Operators (Questionnaire Question C-6)
Have individual sign non-disclosure agreement, conduct security training and education. Education content publicly announced via corporate Intranet. Ranking system for handling proprietary information leak, paper-based documents; however, large number of ranks precludes a complete answer at present without referring to the list.
･Contract and other employees receive the same training and education as full-time employees. ･Corporate group includes a temporary/contract agency; certain level of trust has been established.
Security education is conducted at the department level. Education content for contract employees is different from full-time employees, providing job-related training only.
Require a signed agreement when hired/contracted. Mainly usage rules (Internet, corporate LAN, etc.)
･Security training/education for contract employees conducted at same level as full-time employees. ･NDA requirements for contract employees left to the discretion of the department; however, some departments require NDA for individuals.
Employee ID cards required for access to certain areas in the Chiba Center; accessible areas restricted.
･NDA for contract employees is signed between companies (managed by dept. of hiring contractor). ･Although not as frequent as with full-time employees, system and security training/ education is conducted at the local level.
Contract required. Compensatory damages maximum limited to annual contract fee.
Contractor agreements are not particularly required; therefore, training not necessary. (NDAs are signed)
Contract employees are not particularly considered differently. NDAs are signed.
Information security training and education conducted for contractors. We ask the contract agency to provide education.
NDA required for contractors performing contract work. Annual training conducted for training vis-à-vis personal/proprietary information protection.

Incident Response Plan (Questionnaire Question C-7)
Rules in place covering time from incident occurrence to system restoration. No major incidents to date; however, individual inquiries have been received from outside the firm.
No particular defined plan. When incident occurs, notification comes into the General Affairs department, who obtains help when they cannot provide a response. Viruses reported to the IPA when detected.
･Crisis Management Manual created and in place.
Not specifically defined. Vendor suggests appropriate responses when incident occurs.
･Use a incident communications form when unauthorized access, viruses, other (loss, etc.) occurs.

No specific method for disclosing information to third parties. Otherwise rules/regulations in place.
･In cases where virus is sent outside the company. ･In cases where the Host PC crashes.
No specific written plan.
Information security incident report is required; however, no specific details as to the report content. Incident reported to the IPA and others.

Gathering Information Security-Related News (Questionnaire Question C-8)
Mostly free information received from vendors, etc.
Subscribe to a security information service provided by security services vendor that is one of the business partners. However, providing this information to person(s) responsible in each department does not guarantee that each person reads and comprehends the material.
Gather security information from CERT, MS, etc.
Subscribe to a fee-based service. Patch verification and other information are written in an easy-to-understand format.
Subscribe to a free information service. Most information is related to OS bugs; obtain patches from relevant sites. Subscribe to information provider for Linux information.
Visit vendor websites daily for information updates. Mainly Sun and ORACLE. Windows information is not followed as closely.
･Do not subscribe to a fee-based information security news service. ･No lack of information; rather, volume of content is almost overwhelming, difficult to discern what information relates to our firm.
Subscribe to a mail service. Subscribed to service when purchasing firewall.
Visit IPA and other sites for news updates. Current level of information gathering seems to provide enough information.
Subscribe to a vendor newsletter broadcast service.
Subscribe to a security service information provider; however, news is not timely—no major benefit over content of information gathered on our own.
Contractor SEs gather security news on their own. (three network contractors, two host contractors)

Application of Patches (Questionnaire Question C-9)
Application of patches left to the discretion of server administrators. Patch availability does not guarantee it will be applied, as there are some servers that cannot be taken down. Times when server functions unexpectedly initiated for client without known administrator level; comprehensive asset management process, including client PCs, should be implemented. Implementation of construction and operation (usage/update) of asset management system extremely difficult.
･Get advice (from vendor?) when uncertain about applying patches. ･Sometimes difficult to apply patches, especially for database servers.
Department servers not connected to corporate network administrated by each department. There are cases where environments mirror those at client locations; therefore, cannot always keep such environments up to date.
Firewall patches fall within the scope of maintenance contracts, provided by vendor. With respect to software sales, patches are tested on all OSes, results are announced to users. About 20 Linux servers used for public Internet. Internal servers run on Windows, approximately 50 machines. Other servers included temporary machines set up for development; difficult to apply patches to all. Patches for work-related servers applied by each department; announcing new patches is

part of General Affairs department responsibilities.
Patches applied to mail servers as needed. Servers divided into constant use and verification machines. Patch tested first on verification machine and then applied to constant use machines.
･Currently developing a system to automatically apply patches to enterprise systems (MS product) ･Difficult to guarantee security for PCs depending on development servers, DB servers. ･Test environment is in place; however, time is extremely limited, therefore usage is quite restricted.
Subscribe to manufacturer maintenance service. Microsoft-related patches applied according to degree of importance, others once per month. Only for servers.
Only minimum required patches applied. DMZ net server, etc. is outsourced; not certain as to patch applications for these servers.
Patches faithfully applied to external servers; unfortunately, not able to diligently apply patches to all internal servers. Acquisition of new patches outsourced to subsidiary.
Newest patches always applied to servers administrated by Security Committee. Other department servers are patched by server administrator after determining patch release status periodically by department, and obtaining permission from responsible party. Maintenance generally performed in-house (full-time employees, SES, etc.) Implementation is generally left to the discretion of each department. If Security Committee identifies a particularly critical security hole, instructions are given to each department. System structured so that countermeasures can be completed company wide in 1 to 2 days. Servers administrated by Security Committee (external connections, topmost Web server, etc.) are patched after patch is first tested on verification server. (Trouble can develop after certain patches have been applied)
Patches applied according to contract vendor suggestions.

Certifications Obtained/ In Planning (Questionnaire Question C-10)
･Security certifications obtained as required at the department level. ･ISMS obtained by security-related departments; Privacy Mark is in planning at public relations department.
Preparing to obtain Privacy Mark certification. CMM has assigned personnel and is in process (board director designated as top, branch managers meet every two weeks for discussion).
･There are beneficial aspects to ISMS certification; however, there seems to be too much focus on “Document Management”, leading to apparent imbalance with security technology. ･P MARK may be necessary to guarantee security of personal/proprietary information (worries about handling data from parent company).
Nothing planned presently. Affiliated company already obtained Privacy Mark.
No plans at present.
No plans at present.
Certifications obtained either to gain competitive advantage over other firms, to meet work process requirements, or to answer market needs. First among competitors to acquired qualifications, large competitive advantage.

Audits, Vulnerability Tests Conducted in past 12 Months (Questionnaire Question

C-11)
Internet system audits, vulnerability tests conducted annually. Important issues determined by committee (asset management selected as this year’s theme)
System audit conducted annually. Vulnerability tests conducted at irregular intervals (contracted to third party)
Conducted when settings are changed (version upgrades, patch applications, etc.) Vulnerability tests are conducted via port scans by external dial-up, firewall log inspections on the LAN, etc.
･Vulnerability tests conducted three times by external party (different companies used each time)
Daily morning inspection of logs to determine unauthorized access attempts.
･Penetration tests performed by in-house technicians. ･System audits performed in-house and by parent company for Internet and Intranet.
System audit conducted for Internet and internal company network. Vulnerability tests conducted twice annually by attack detection firm. Discovered security hole when revising system settings.
Not implemented. Will study further in the future.
Internet and intranet examinations conducted at the interview level. Periodic testing via network-based scanner.
･Performed in-house as a rule. ･Internet vulnerability testing contracted to one outside firm. ･Internal network system (security) audits conducted in-house, and contracted to one outside firm. ･Reasons for selecting survey company based on balance of technology, reliability and costs. ･However, considerations of technology and reliability are more important than costs with respect to vulnerability tests.
･System audits will be implemented next year. Person directly responsible is absent; therefore, audit implemented to confirm whether operational problems exist. ･Security policy created and in place. ･Penetration tests conducted for main network.

Information Security Budget (Questionnaire Question C-12)
Not sure, since security budget is handled at the department level.
Included as part of the information systems budget.
Included in systems budget.
･Security budget enacted annually on an as-needed basis.
Included in maintenance fees paid to operations contract vendor.
･Level of satisfaction with security-related costs is 65% to 70%.
Included as a part of systems budget.
Included as part of information systems budget. Firewall, virus (gateway, client).
Anti-virus software for client PCs budgeted. Web filtering is under consideration at this time.

Security management systems support, systems development, virus detection software purchases, training and education, etc. are mainly software expenditures. Firewall and related hardware are included in the information systems budget. (However, portions of information systems budget include security-related expenses, making it difficult to separate from network equipment costs). Sufficient expenditures for information security are acquired. However, physical equipment costs are somewhat difficult to obtain a budget for at the moment. ･A 70% overall level of satisfaction with information security-related expenditures.
Indicated monetary figure represents amount of expense specifically identifiable as security -related (virus pattern file updates, etc.), and does not include system audit fees, etc.

Ratios of Current Security Budget and Systems Budgets (Questionnaire Question C-13)
･License renewal fees amount to about ¥2 million annually, including scan and virus updates. ･Considering third party maintenance for firewall.
General budget outline exists, but security-related budgets acquired on an as-needed basis.
No particular category set aside.
Budget identified as ¥50 million, which includes the contract fees for six individuals from contract operations vendor.
Details unclear.
Budget is ¥4 million, which is 3% of the overall systems budget.
Budget is ¥4 billion, which is 2.5% of overall budget.
Systems budget makes up 8% to 10% of overall corporate budget.
Management understands the importance of security measures, facilitating budgets allocated to security.

Allocation of Information Security Budget (Questionnaire Question C-14)
Annual license renewal. Products to be adopted this year.
Firewall maintenance fees, etc. clearly identified. Anti-virus license is included in annual budget. Hardware costs consist mainly of PC upgrades.
Contingent costs for Verisign certificates, etc.
Hardware and software purchase costs, and maintenance expenses. IDS service implemented. Educational budget is conspicuously absent.
Fees for certifications obtained at the department level are included in department budgets. (no company wide certifications)
Virus pattern file updates.

Systems used to Ensure Information Security (Questionnaire Question C-15)
Firewalls, DMS segments, mail server virus checks, and client PC virus check software are implemented. Overall low level of knowledge related to ensuring Linux, Solaris security, etc. is cause for concern.

Anti-virus software installed. System level upgrades conducted monthly via CD-ROM. Definition files updated daily, saved to the domain server and distributed to each employee when they log on to the system. Server is scanned automatically each evening; virus detection sends alarm to administrator. Virus check is required of employees for their computers at home. Any type of software (try and buy, included) is OK as long as installed and used. Send reminder emails at year-end and other strategic times.
･A portion of system information encrypted with SSL.
･SSL implemented for User-oriented homepages.
･Encryption is in planning stages. ･Packets are inspected at the pre-IDS level.
Everything except for encryption is in place. Encryption is under consideration, but cost is major impediment.
Firewalls, DMS segments, mail server virus checks, and client PC virus check software are implemented. External connections use RAS, international frame relay.
Firewalls, Intrusion Detection Systems (IDS), DMZ segments, mail server virus checks. With few exceptions, virus check software is on all client PCs and proxy servers.
Capacity to implement web traffic pattern filters is available.
Firewalls installed for each segment (complete separation from rest of network) Virus definition file updates for each terminal conducted automatically at night using Auto-On feature. Terminals containing personal/proprietary information are equipped with encryption.

Countermeasures used to Prevent Disclosure of Private/Proprietary Information (Questionnaire Question C-16)
Almost impossible to enforce policy measures, restrictions on bringing in notebook PCs (OA equipment), etc. (Not feasible to make every employee turn on their notebook computers when they enter the building)
Wireless LAN is used; care exercised with respect to ESSID, WEP and signal leakage.
Implemented router traffic surveillance. (in one incident in the past, network bandwidth had been completely overwhelmed by an online 3D game) Outgoing traffic is particularly watched to detect the release of program code. (contract employees sometimes work from home, which means that programs are taken from the business premises)
･At present, personal identification consists of an ID and password; however, IC cards are planned for introduction next year.
･Email records are maintained at the instruction of government. ･Information assets (paper documents, data) are strictly managed. ･Person in charge of security designated for each department. Sample monthly audit conducted at randomly selected department.
･Notebook PCs are prohibited from being connected to the network. (not clear as to whether notebooks brought in by vendors are checked)
Documents and PCs may not be brought in or taken out according to formal rules. Server room access is by ID card only. Formal rules prohibit removal/destruction of floppy discs or other media. Email surveillance in planning. Webmail prohibited beginning 2003.

Department shared servers installed and administered on each floor.
Corporate regulations are in place with respect to removal of documents, notebook PCs, floppy discs and other memory media. However, actual observance of these rules have not been successfully confirmed.
･No formal written rules related to restrictions on removing documents. ･Prohibition against bringing in notebook PCs covered in the “Restrictions on Personal Items” section of the firm’s operations handbook. ･Removal of floppy discs, etc. controlled via restrictions on PC drives. (However, there is not formal function in place to verify.) ･Memory media destruction accomplished using Hard Disc Crasher at the time a PC is destroyed. PCs destruction/abandonment takes place at the end of the year for all PCs to be destroyed (Hard Disc Crasher is used). Data on leased computers destroyed with a disc erase tool. ･Physical facilities access keys required.

Content of Information Security Training/Education (Questionnaire Question C-17)
･Corporate intranet used for education. ･Security training/education given to new-hires.
Education desired for experienced hires, but degree and quality varies among IT department, sales department, etc. Difficult for HR departments/supervisors to explain.
New hires receive education; in-house E-Learning in place and used.
Email updates sent to employees to educate them about virus countermeasures. (mainly information) Emergency response is handled on an as-required basis. For PC operations, settings manual for new machines is available via shared folder. Settings are the responsibility of the computer user.
Nothing specifically for security, incorporated into systems education/training material.
･No emergency response training. ･ Emergency response education consists of making sure employees know proper communications route. ･Considering adding Netiquette and social engineering as education topics. (especially for office workers, sales personnel)
Nationwide training held in 1999. Nothing since. In-house qualifications implemented for information systems. Qualified individuals conduct training for other locations.
No specialized information security education. Will consider instituting such education once security policies are in place.
Non-disclosure agreements relied upon heavily for control/management. Employees are educated related to security settings such as access control and screen locks. (Other general settings technologies are not taught.)
New hires are given training related to management of personal/proprietary information. Training implemented within the Information Systems section.

Security Training/Education Conducted within the Previous 12 Months (Questionnaire Question C-18)

Conducted annually for 500 employees and 100 managers. In-house security education tools used for study; once individual passes course, email account is issued. Originally used e-Learning materials for publishers, but was too technical to be applicable for general employees. Based on this experience, we created an in-house course; second round of training with new content to be conducted in four or five days.
Security training conducted for entire Group (approximately 30 mins.)
Incorporated into new-hire training. Used as part of follow-up training. Curriculum designed by HR, implementation carried out as part of General Affairs department job responsibilities.
･One hour per year of group training (absent employees are brought up to date by superiors) ･Self-check system implemented for employees to verify their understanding (WBT system) ･Managers make quarterly reports to security committee (2 to 2.5 hour meeting)
Annual training for 70 system administrators.
Annual specialist training given to 20 individuals.
E-Learning implemented. New-hires/ experienced hires receive group training and e-Learning. Difficult to conduct education for 100% of employees, due to seconded employees, or employees on leaves of absence. (Employees on leave do not participate in day-to-day work; therefore, training is not necessary.) Seconded employees may be able to attend lectures, but final decision regarding education policies are left to the discretion of the seconded employee’s new managers.
Training conducted for information systems related employees at the beginning of each year.

Current or Planned Measures for Information Security (Questionnaire Question C-19)
Security committee consists of department head, server administrators responsible for providing security information to all employees. Not certain as to the level of understanding by each individual. External communications system, flow to be subjects of future consideration.
Documenting individual work flows for obtaining certification is extremely burdensome.
Education/training in latest information conducted once or twice monthly for Information Systems personnel and cooperating companies. Intend to implement same type of training for general employees in the future.
Future topics of interest include defining internal systems for information security, security training reinforcement for information systems personnel, incident/accident response training, and employing personnel who possesses information security skills.
Future topics of interest include preparation of security-related documentation, defining internal system for information security, security training reinforcement for information systems personnel, security training reinforcement for all employees, conducting system audits, providing security information to all employees, virus checks on client PCs and more.
･Intend to implement security audits in the future. ･May obtain official security certifications if required by market needs. ･IDC cannot be completely relied upon.
Intend to address countermeasures individually as policies are created.

Advancement of IT, Reliance on Information Systems (Questionnaire Question

C-20)
・No clear understanding of the level of information systems reliance.
・Host system and information systems (Email, etc.) are separated. If Internet connection goes down, the work-process network should still function.
Day-to-day usage includes settling transportation costs, etc. Cannot reduce reliance on paper due to attachment of approval seals. General resistance to implementation of electronic authorizations, difficult to implement education.
Many processes are computerized.
Most processes are computerized.
Many processes are computerized. (Almost all HR and accounting systems) CRM (Customer Relationship Management) is not implemented to an advanced degree.
Difficult to easily estimate degree of computerization since we have no financial or such core processes. Main business activities include planning, proposals and design; computers provide the means to accomplish this work. HR and finance are computerized/ conducted over a shared network, but are not core processes for our company. Computers are used to create proposals and designs. Such work is not always affected by network crashes. Potential costs of network crashes during bidding process could reach hundreds of millions of yen; difficult to quantify damages during network downtime. Systems Subject to Significant Business-Related Effects. Five years ago, we could not have conceived that network crashes could have such a large impact on our business. Now, the Internet (electronic requests/ applications) and Email are almost indispensable systems.
・Some processes related to publishing completely stop when our computers crash. (Manual processing not possible; level of reliance is high.)

Damages Incurred (including past cases)
<Infected with a virus sending Emails using a fake “From” address, requiring company to designate a contact person to handle inquiries> ・Public Email inquiries directed to Public Relations; forwarded to IT department depending on question content. ・Of those affected, three were company employees. <Email Operations> ・All corporate mail is checked once at the mail gateway. ・Restrictions on attached file sizes; however, incidents of large file attachments going out to sales mailing list occurs frequently.
Internet access was stopped for two days, affecting Email, etc. for all employees.
<KLEZ> One PC infected. Detected when shared folder infected. Ultimately 30 machines became infected. Logs revealed 20 infected emails sent out; sent apologies. Infection occurred when auto scan did not function to catch virus when low-powered PC logged in to network.

No particular damages incurred this year. <Past Incident> Infected with x97M_DIBIV (Excel macro virus) during 2000. Approximately 400 company client PCs and one server affected. Employee copied infected file from home computer to a floppy disc and brought it into the company. File was uploaded to a bulletin board, which exacerbated the damage. Incoming Emails are checked for viruses, so the file was caught and removed when Emailed from the employee's house to the company, but company could not prevent file copied to the floppy disc from entering the system. After this incident, the company has been using anti-virus software on information systems servers. Restoration took three individuals two months. Work was performed remotely from the Center; virus extermination and definition file updates implemented at the same time. Initially, only one or two individuals were infected, which resulted in delayed detection. Definition files on terminals are manually, not automatically, updated. Outgoing Email is checked for viruses, so no external entities were infected.
No incidents during 2002. SQI countermeasures worked properly. <Past Incident> Infected with CodeRed on August 7, 2001. As a result, we implemented redundant countermeasures and enhanced security measures. Differing security countermeasures for agency and in-house systems were unified.
Virus Incident Occurred (Details not provided). Infected via floppy disc brought from employee's home (department personnel responded appropriately to prevent secondary infection). Recovery costs: ¥20,000, Employee cost per day: ¥20,000
<Past Incident> 1994 Yankee Doodle infection via floppy disc (between 100 and 200 machines infected) ･Restoration took one day. ･No other details available.
Several incidents (about 5 estimated) of Klez virus outbreaks during the year. On-location response of network administrators + Security Committee (headquarters organization) combined accounted for total of ¥1 million/year in related costs. No real legal compensation or costs related to apologies incurred.
Virus entered company due to delay in anti-virus software company's distribution of updated pattern files. Virus deleted after receiving and installing new pattern file.
Virus countermeasures in place, but network infected before new pattern file was received.
Date undetermined: 10 to 20 machines infected by Klez contracted from affiliated company in Indonesia. ･Two technicians dispatched from Japan to restore system. Checked all 100 terminals. ･Email was down for two days, holiday in Japan helped limit damages. ･Work required for restoration: 8 worker-days ･Recovery Costs: ¥240,000 plus travel expenses ･Per-employee wages per day: ¥30,000

<Past Incident>

Blade virus infected 20 machines at the end of 2002. Damage spread through shared files.

- Infection contracted Friday evening, so effects on business operations were limited.
- Contracted via Extranet; restoration required 9 worker-days.
- Recovery Costs: ¥270,000
- Countermeasure Costs: ¥300,000
- Per-employee wages per day: ¥30,000

Other Comments
・Had a terminated employee take source code, but no actual damages incurred. ・Difficult to balance convenience and security
Considered using encrypted Email, could not immediately adopt since encrypted data and messages broken up via MUA did not allow for gateway virus checking, and caused intensive processing load.
・Three SQL servers affected by Slammer virus, restoration required two employees and 3-4 hours. ・Wireless LAN is prohibited.
・Want to have a evaluation, objective assessment of company's security. ・Not sure how to conduct ongoing security education.
・Work process network is not connected to internal company network. ・Difficult to judge effects on network safety (security), as a result of pursuing work-flow convenience. ・Wireless LAN is not used.
・Mail server, core (settlements) systems have built-in redundancy. ・Damage figures included in information security incident reports, reported to management. ・Company domains revealed through Klez. ・Ideally, we want to install anti-virus software from different vendors on client PCs and servers; but doing so is cost prohibitive (in the past, a virus was detected and eliminated by a different anti-virus software on the client PC) ・Business systems subject to potentially large damage: Email (redundant circuits, 5M limit) and Accounting Settlements (cold standby, installed at off-site location) ・Information assets categorized by size, but costs not assigned. ・2002 was comparatively uneventful.
Major security issues with wireless LAN. Should be included in the next survey. Emphasis placed on external measures, patches are sometimes difficult to apply to internal systems—a topic for future consideration. We use groupware, which is effective at preventing the spread of worms, but not effective at preventing infected Excel file attachments.
・Some employees use company anti-virus software to check personal data. ・Became sensitive to security issues subsequent to sending Email to customers, enacted security measures.
・No incidents of virus outbreaks since virus checks have been conducted on the mail server. ・Difficult to take security measures involving management. Easier to get movement after showing incidents in newspapers, other media.
Occasional cases of reported significant virus outbreaks, responses over the past year. Approximately 70 to 80 people (machines?) affected per outbreak. However, no severe damages incurred, such as with Nimda, over the past year. During last outbreak of Slammer, our survey did not reveal any incidents of infection. No DoS attacks at Internet connection points over the prior year. However, SPAM mail incident occurred last year, causing the mail server to crash and be unavailable for several hours. The past year has been uneventful. Large virus outbreaks have occurred about every two years, so we are nervous for the period beginning in March. War and other events contribute to need for caution.

We are concerned about the current system of using one ID per section to log in to the network.

8.2 Questionnaire Sheet

Information Security Incident Survey Questionnaire

This survey has been designed for information security managers (individuals responsible or involved in information security). Please forward to the appropriate individual(s). Please mark your answers directly on this form.

A Please tell us about your company's business.

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

1	Finance (banking, insurance, securities)		6	Education/ Mass Communications	
2	Medical/ Pharmaceutical		7	Construction	
3	Transportation/ Shipping		8	Food Service/ Retail	
4	Energy		9	Other Services	
5	Information/ Communications		10	Other	

A-2 Annual Sales and Number of Employees.

1	Annual Sales (unit = ￥10,000)	
2	Employees	

A-3 How many offices/ locations does your company have? (Please circle your selection.)

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?

(Please circle your selection.)

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 Email usage in your company? (Please circle your selection.)

1	Not available		4	Generally available, but limitations on type and size of attachments	
2	Email on designated terminals only		5	Generally available with no particular limitations	
3	Generally available, but attachments not permitted				

B-3 What is the level of Web browsing usage in your company? (Please circle your selection.)

1	Not available	
2	Web access on designated terminals only	
3	Generally available, with limits on permissible sites	
4	Generally available with no particular limitations	

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

1	Internet Mail (%)		%
2	Web Browsing (%)		%

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

C-1 Does your firm have formal information security policies? (Mark all that apply.)

1	No	
2	Separately defined information security policies in place	
3	Information security rules included in workplace conduct policies	
4	Information security rules included in policies related to protecting personal information	
5	Information security rules included in other policies	
6	Information security related procedures in place	
7	Not sure	

<Other>

C-2 ***For those who answers, "1. No" to Question C-1:***

What is the most important reason for not creating an information security policy? (Please circle your selection.)

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

<Other>

C-3 How many information security administrators does your company employ?

1	Dedicated Personnel	
2	Dually-Responsible Personnel	
3	Responsible Board Director Selected (mark with ○ if selected)	

C-4 System for communicating information security mishaps and incidents throughout the company. (Mark all that apply.)

1	Communications system established and in place	
2	Established department responsible for determining occurrences of security mishaps and 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-5 Information security considerations when selecting or contracting with business partners. (Mark all that apply.)

1	No special considerations	
2	Special consideration given to business partners with well-known business and service levels	
3	Special consideration given to business partners who have certification related to 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 system audits on business partners	
9	Not sure	

<Other>

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

1	No special requirements	
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-7 Factors included in damage response plan. (Mark all that apply.)

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

<Other>

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

1	No formal news gathering conducted	
2	Periodically review 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-9 Application of patches to ensure network server security. (Please circle your selection.)

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-10 Indicate whether certification is "In Planning" or "Already Obtained".

	Name	No Plan	In Planning	Already Obtained
1	ISMS (BS7799)			
2	ISO/IEC 15408			
3	Privacy Mark			
4	CMM (Capability Maturity Model)			
5	Not sure			

<Other information security certifications (name)>

C-11 Has your organization conducted system audits and vulnerability tests (penetration tests) within the previous 12 months?

	System	System Audit (Mark if conducted)	Vulnerability Testing (Mark if conducted)
1	Internet		
2	Intranet		
3	Extranet		
4	Internal Company Network		

<Other>

C-12 Does your company have a formal information security budget? (Please circle your selection.)

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-13 If you marked any categories 2 through 4, above, please provide some general figures.

Budget Amount (unit = ¥10,000)	
Ratio of Information Systems Budget (%)	

C-14 Allocation of information security budget. **(Mark 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	Expenses of maintaining certifications	
5	Security software maintenance		10	Not sure	

＜Other＞

C-15 Indicate systems used to ensure information security.
(Mark all that apply.)

1	Firewalls		5	Implement virus checks on all client PCs	
2	Intrusion Detection Systems (IDS)		6	Encryption tool usage (S/MIME, PGP)	
3	Set up DMZ segments		7	Implement virus checks on proxy servers	
4	Virus checks on the mail server		8	Not sure	

＜Other＞

C-16 Countermeasures used to prevent private information disclosure. **(Mark all that apply.)**

1	Email monitoring		8	Restricted access to server rooms	
2	Webmail monitoring		9	Restrictions on removing floppy discs and other memory media	
3	Server access restrictions		10	Standards for destroying floppy discs and other memory media	
4	External phone line monitoring		11	Standards for destroying PCs (Office Automation equipment)	

5	Restrictions on removing documents		12	Key encryption systems	
6	Restrictions on removing notebook PCs (office automation equipment)		13	Biometrics	
7	Restrictions on bringing in notebook PCs (office automation equipment)		14	Personal identification devices	

<Other>

C-17 Information Security Training/ Education. (Mark 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				

<Other>

C-18 Ongoing information security education over the previous 12 months. (Mark all that apply.)

	Training/ Education Content	No. of People	Frequency
1	Education for all Employees (User Training)		
2	Management Training		
3	Specialist Training		

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

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

<Other>

C-20 Describe the advancement of IT in your company. Indicate the general level of reliance on systems. (Please circle your selection.)

1	Most processes are computerized	
2	Many processes are computerized	
3	About half of processes are computerized, half are manual	
4	Only a few processes are computerized, most are still manual	
5	Almost no processes are computerized, almost all are manual	

<Other>

D Describe information systems incidents at your company

You may leave any difficult-to-answer sections blank; but please try to provide general circumstances and figures.

①Refer to the next page for incident codes

②Form provides space for three incidents. If more space is needed, please copy the form.

＜Example Incidents＞

1	**Incident Code→**		**1**	
	＜Incident Circumstances＞			
	One of the clerks accidentally opened an Email infected with KLEZ; since it was copied to the shared server's drive of the clerk's department, PCs in the department were infected. As a general rule, clerks were supposed to update virus pattern files by themselves on a regular basis; however, most clerks failed to conduct timely updates, which led to almost all PCs within the department infected with KLEZ. Virus check software prevented infection spread on to servers in other departments, but failed to stop sending out Emails with infected files. Consequently, we found that approx. 300 infected Emails were sent out externally.			
2	**Time and Date of Occurrence**	**(month/ day/ year)**__8/30/2002___ **(time)**_20:00____		
3	**Damaged Systems**			
	Mail servers, file servers, etc. (Total of five servers)			
4	**Type of Systems Damaged (Mark applicable systems)**			
	(1) Internet (including DMZ)	○	**(4) Internal company network**	
	(2) Intranet		**(5) EC (BtoB)**	
	(3) Extranet		**(6) EC (BtoC)**	
5	**Downtime**		5	**Hrs.**
6	**Number of employees affected**		80 (excl. off-site employees)	**People**
7	**Decrease in processing capacity during system downtime**		30	**%**
8	**Annual system sales (if EC site)**		―	**¥**
9	**Annual system profits (if EC site)**		―	**¥**
10	**Number of damaged servers**		5	
11	**Number of client PCs damaged or affected**		70	
12	**Business contingency costs**		N/A	**¥**
	Alter-nate Means	**＜Describe response method(s)＞** • Communication via phones, faxes, etc. • Operation continued using PCs in other dept.		
13	**Lost Profits** **(actual lost profits, etc.)**		1,000,000 (Estimates delayed)	**¥**

14	**Lost Information Assets**	0	**¥**
15	**Opportunity Lost (loss of forecast profits, etc.)**	Not sure	**¥**
16	**Legal compensation, reparations**	0 (Apologies only)	**¥**
17	**Other related costs (brand value maintenance costs)**		
	（1） Public apologies	None	**¥**
	（2） Letters of apology	100,000 (Postage and labor cost)	**¥**
	（3） Apology Visits to affected parties	10 (for 100 Emails)	**Work days**

＜Incident Code Chart＞

Incident Code No.	Type	Incident Type	Description
1	worm type virus	KLEZ	Effects resemble highly contagious Nimda virus, propagates via E-mail and shared drives, and also creates a separate program that infects executable files. Has “direct action activity” set off by Email preview.
2	worm type virus	BADTRANS	Trojan horse program categorized as a worm. A sub-species of WORM_BADTRANS.A. Attaches a copy of itself to Emails, self-propagates on a network. Also acts as a hacking tool by recording keystrokes on an infected machine. Has “direct action activity” set off by Email preview.
3	file infection type virus	NIMDA	Direct file infection virus. Can act by itself as a Trojan horse. Also sends Emails, copies files to network drives, uses IIS security holes to gain system entry to distribute copies of itself over a network (worm-type functions). Has “direct action activity” set off by Email preview.
4	file infection type virus	MAGISTR	Memory resident mutation file infection virus, infects PE format files. Also has worm features, attaching self-infected files to Emails.
5	macro type virus	LAROUX	Excel macro virus. Creates “laroux” macro module in an Excel document and spreads to other documents.
6	worm type virus	BUGBEAR	Trojan horse program categorized as a worm. Acts as a worm copying itself and attaching to Emails in mass mailings, copies and distributes itself over shared drives. Also works as a backdoor hacking tool to steal private information, attempting to shut down anti-virus software.
7	Other virus incident		Virus incidents other than described above. Please provide virus name and description in space provided.
8	Damage caused by harmful rumors		Secondary incidents related to virus infection and/or disclosure of private/proprietary information.
9	Data loss, system crash caused by operator error		Trouble caused by human error (procedural mistakes, etc.)
10	Unauthorized access from outside		Unauthorized access by outside individual without proper access rights.
11	Service interruption caused by DoS attack		Service degrade or interruption caused by concentrated access attempts.
12	Alteration of homepage by external party		Unauthorized homepage changes by outside individual.
13	Leak or alteration of company information		Unauthorized removal of information via memory media, etc.
14	Other		Please describe circumstances in the space provided on the questionnaire.

D-1 Incident Circumstances

1	Incident Code →			
	<Incident Circumstances>			
2	Time and Date of Occurrence	(month/ day/ year)__________________(time)_____		
3	Damaged Systems	Countermeasures Employed		
4	Type of Systems Damaged (Mark applicable systems)			
	(1) Internet (including DMZ)		(4) Internal company network	
	(2) Intranet		(5) EC (BtoB)	
	(3) Extranet		(6) EC (BtoC)	
5	Downtime			Hrs.
6	Number of employees affected			People
7	Decrease in processing capacity during system downtime			%
8	Annual system sales (if EC site)			¥
9	Annual system profits (if EC site)			¥
10	Number of damaged servers			
11	Number of client PCs damaged or affected			
12	Business contingency costs (contingency systems, human response, etc.)			¥
	Alter-nate Means	<Describe response method(s)>		
13	Lost Profits (system sales×downtime, actual lost profits, etc.)			¥
14	Lost Information Assets			¥
15	Opportunity Lost (loss of forecast profits, loss of increased sales, etc.)			¥
16	Legal compensation, reparations			¥
17	Other related costs (brand value maintenance costs)			
	(1) Public apologies			¥
	(2) Letters of apology			¥
	(3) Apology Visits to affected parties			Work days
18	Restoration work volume (systems dept. and other)			Work days
19	Recovery Costs (payments to contractors, etc.)			¥

20	Per-employee wage per day		¥/day