Information Security Incidents Survey Report

- Event Probability -

[Summary Version]

NPO Japan Network Security Association

Security Incident Investigation Working Group

March 31, 2011

Table of Contents

Copyrights and Quotes

1. Summary of questionnaire

1.1. Purpose

The JNSA Incident Damage Survey WG has been creating and releasing "Information Security Incident Survey Report" over the last few years by conducting various statistical analyses after aggregating incident information publicly released.

The information sources of this report are the incidents grasped and announced by corporations or incidents that have been reported by various media; therefore, there is a concern over its deviation from the actual situation in the society. In fact, it has been known that there are considerable differences in the number of incidents that have been grasped or published depending on the corporate attitude toward information security management.

For this reason, we have decided to conduct questionnaire targeted for individuals in general job roles as one of the means to grasp the realities of information security incidents with higher accuracy.

1.2. Method

A marketing research firm has been hired to conduct Web questionnaire survey divided into two stages--preliminary survey and main survey—from Friday, October 15 to Tuesday, October 19, 2010.

1.3. Preliminary survey

For the preliminary survey, we have collected answers until each number of samples reaches 100 so as to narrow down to those who have experienced any one of five types of security incidents (1. mobile phone, 2. notebook PC, 3. loss of USB memory, 4. Email, wrong fax transmission).

While collecting the answers, we have allocated 25 respondents (male: 15, female: 10, by reference to the working population) to each of (4) age groups (18-29, 30-39, 40-49, and 50 or over) for a total of 100, so that the appearance ratio of population is equalized in each of the five (5) survey items. Also, student, unemployed, leave of absence, and job seeker are excluded from the object to limit the survey object only to those who are working.

- Number of valid respondents in the preliminary survey: 4,884

Table 1.3-1: Age group (preliminary survey: N = 4884)

No.	Age group	Num. of respondents	Ratio (%)
1	18 -29	481	9.8%
2	30 -39	1,268	26.0%
3	40 -49	1,426	29.2%
4	50 or over	1,709	35.0%

Table 1.3-2: Job/occupation (preliminary survey: N = 4884)

No.	Job/occupation	Num. of respondents	Ratio (%)
1	Corporate operator, board member, organization officer	240	4.9%
2	Company or organization employee (regular employee)	2,787	57.1%
3	Company or organization employee (contract or temporary)	388	7.9%
4	Local government employee	144	2.9%
5	National government employee	40	0.8%
6	Self-employed, sole proprietor, freelance	582	11.9%
7	Freelance professional (such as medical practitioner, law office manager, professional athlete)	101	2.1%
8	Part time, temporary, or seasonal worker	602	12.3%
9	Student	0	0.0%
10	Unemployed, leave of absence, or job seeker	0	0.0%
11	Others	0	0.0%

1.4. Main survey

The main survey conducted in-depth investigation for the population extracted in the preliminary survey regarding the specific reasons for incident occurrences, situations, contents of the measures being taken, and the response after these incidences.

2. Topics

2.1. Probability of employee's loss and wrong transmission

Fig. Fig. 2.1-1: The number and the ratio of respondents who experienced information security incidents shows the number of respondents who experienced any of five (5) information security incidents (losses of mobile phone, notebook PC, USB memory, wrong transmissions of email/fax) and the ratio of these incidents.

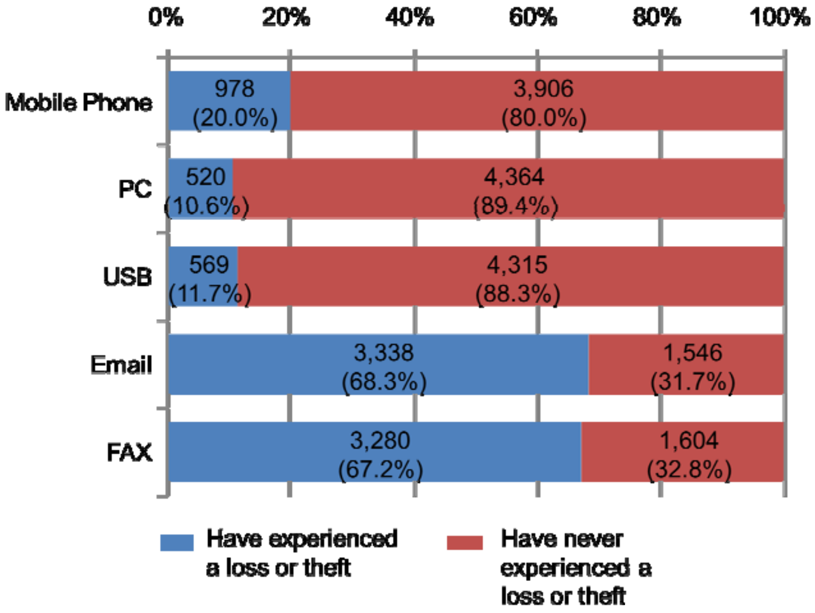

Fig. 2.1-1: The number and the ratio of respondents who experienced

information security incidents

The event probability of information security incidents per single year was calculated from the ratio of respondents who experienced information security incidents and the information on the years in which information security incidents occurred that was indicated by the main survey. Table 2.1-1: Annual event probabilities of loss, theft, and wrong transmission shows the calculated event probabilities in 2009 and 2010.

Table 2.1-1: Annual event probabilities of loss, theft, and wrong transmission

Survey object	2010	2009
Mobile phone	6.4%	6.6%
Personal computer	3.7%	3.1%
USB memory	4.7%	4.1%
Email	40.3%	17.1%
Fax	39.0%	12.1%

2.1.1. Mobile phone

Among 100 respondents who lost or had their mobile phones stolen or who were about to lose, the main survey indicated that the ratio of incidents in 2010 and 2009 was about 30% for each year. It is assumed that the probability of company employees' loss or being stolen or about to lose their mobile phones in a year is about 6.5%, based on the ratio these incidents indicated by the preliminary survey and the above-mentioned value from the main survey.

Please note, however, that both company mobile phones and personal mobile phones are the survey objects.

2.1.2. Personal computer, USB memory

The same calculations performed for personal computer and USB memory indicated that the annual ratio of company employees' loss or having stolen (including being about to lose) is about 3.5%, and the annual ratio of USB memory's loss or being stolen is about 4.5%.

The annual probability of USB memory's loss is higher than the annual probability of personal computer's loss. This is may be because a USB memory is smaller and easier to be lost. The probability of losing USB memory should be the highest if the size has a relation with the probability of loss; however, the annual probability of losing USB memory is lower than that of mobile phone. Although a USB memory is smaller than a mobile phone, the probability of loss is lower than that of a mobile phone, this may be because of restrictions on its use in offices or it is now less frequently taken out of offices.

As for a mobile phone, personal computer, and USB memory, the difference is small between the event probabilities in 2009 and 2010. It seems infrequent that the same person would lose a personal computer or USB memory every year. Thus, the event probabilities in 2009 and 2010 are assumed to be independent events with one another, because loss or theft of mobile phone, personal computer, or USB memory does not occur very often.

Therefore, the event probabilities in 2009 and 2010 become nearly the same value, which may be considered as the most recent annual even probability (mobile phone: about 6.5%, personal computer: about 3.5%, USB memory: about 4.5%).

2.1.3. Email, fax

The annual event probabilities of company employees' wrong transmission of either email or fax were about 40% each. This is a probability of the existence of persons who have made wrong transmission at least once over the past year, and it is assumed that the probability includes those persons who had made several wrong transmissions. The main survey did not indicate a large number of wrong transmissions of email and fax before 2007. It is possible that wrong transmissions occurred two years or more ago may not remain in one's memory because email and fax are frequently used and there is a high probability of experiencing wrong transmissions.　The reason for the low event probability of wrong email transmissions at about 17% in 2009 and the high probability at about 40% in 2010 is may be because those who make wrong email transmission once or more every year had responded in 2010.

While fax is sent via physical devices such as combined machines, email is sent via software on personal computers or mobile phones. Strangely, both systems can send out information before confirming the correctness of the destination, and it is very interesting that the annual event probabilities of wrong transmissions are fairly close.

In the main survey, questionnaire respondents were asked to select one of the four (4) options, 2010, 2009, 2008, and 2007 or before, for the time of loss, theft, or wrong transmission. Therefore, respondents answered the years of the latest information security incidents. Those who made wrong email and/or fax transmissions both in 2009 and 2010 had selected 2010. Thus, the event possibility of wrong transmission in 2009 is not necessarily lower compared with that in 2010. The event probabilities in 2008 and 2007 or before were also lower. In addition to the above-mentioned reasons, it is assumed that accurate values had not been obtained due to a vague recollection of wrong email and/or fax transmissions occurred two or more years ago.

Since the data was obtained as of October 2010, it is assumed that the number of persons who had experienced loss, theft, or wrong transmission over the entire of 2010 is smaller than the actual. In the future, we will consider the survey period and numerical adjustment.

2.2. Trial Calculation of risk amount

Here, as an example, we try to calculate risks (assessed amount of damages) at a corporation through security incidents to which a relatively simple and basic probability calculation method is easily applied. For the trial calculation, we have chosen loss and theft of USB memory from among the survey results described in this report.

2.2.1. Assumed corporate profile

The trial calculation used the corporate profile given in the “Estimated Cost for Emergency Responses in Personal Information Leak Cases” appeared in the “Survey Report on Information Security Incidents in FY2003” by JNSA.

[Corporate profile]

The assumed corporation is a mail-order business that sells products by listing them on catalogs in magazines and on the Internet. In recent years, this corporation has been operating an Internet shopping website, and the sales of which is assumed to be about 10% of the overall sales of the company. The following shows the profile of the assumed corporation. (Assumption: margin of Internet shop division = about 10%, annual growth rate = about 10%)

Table 2.2-1: Profile of the assumed corporation

Size of business		
Sales	About 100 billion yen	
Employees	About 1,000	
Catalog sales division		Internet shop division
Num. of members	About 6 million	About 1 million
Sales	About 90 billion yen	About 10 billion yen
Employees		About 30

This corporation collects and manages the following data as the customer information for CRM.

- Name, reading of the name, gender, age (group), occupation
- Zip code, address, phone number
- Buying history information (product code, date of purchase)
- Login ID/password for the shopping website
- Credit card number, expiration date, bank account number

  Above credit information, however, is processed in a separate system and cannot be read within the company.

In addition, this corporation exchanges customer information with commissioned shipping companies for the products sold via catalog sales and the companies that have shops to provide products on the shopping website on a daily basis, and USB memory is used to carry around such data. This is to prevent wrong transmission incidents associated with email attachments, and the company provides USB memories to employees; however, security measures such as encryption is not implemented. Fieldwork employees engaged in such tasks are 10%, or about 100, of all employees.

2.2.2. Estimated amount of damages

First, we do a trial calculation for the estimated amount of damages in case of leak incidents. According to “The Number of Leaked Persons per One Case by Leakage Pass/Media” described in the “Survey Report on Information Security Incidents 2009” by JNSA, the average number of leaked persons via portable media such as USB memory is 28,339.8. Therefore, here we assume that information on 20,000 persons out of the entire member information was leaked due to the loss of USB memory.

Assuming that no measures such as website shutdown are taken and there is no indirect damage such as lost profit or opportunity loss, the indirect damage was calculated as follows:

Table 2.2-2: Breakdown of indirect damages

Item		Expense
Expense for business continuation	Labor cost associated with task team operation (for 1 month)	5 million yen
	Damage compensation expense (lawsuit participation rate = 0.1%)	360,000 yen
	Lawyer and judicial costs	300,000 yen
Expense for apologetic gifts	Expense for apologetic gifts, plus shipping (for 20,000 persons)	14 million yen
Expense for apologetic visits	Expense associated with apologetic visits (for 10 persons)	1.1 million yen
Public relations cost	Expense for apology ad	None
	Cost of creating information disclosure pages (twice)	100,000 yen
Expense for temporary measures	Cost for setting up call center (for 1 month)	5 million yen
	Dedicated personnel for contact (for 1 month)	2 million yen
Total		27.86 million yen

Prerequisites:

(1) Lawsuit participation rate is assumed slightly higher in view of the increasing consciousness on personal information protection in recent years.

(2) Regarding lawyer cost, a considerable amount of retaining fee is required in practical business; therefore, a realistic amount of 300,000 yen is assumed as the retaining fee for civil actions etc. (Reference: “Guideline of Attorney's Fee for Small-to-medium

Businesses," The Japan Federation of Bar Associations, [2009 version of questionnaire result]).

2.2.3. Trial calculation of risks from event probability of losing USB memory

As this corporation has about 100 employees who carry around customer information using USB memory on a daily basis, the event probability of 4.5% based on the main survey is applied to these 100 employees. As 33 out of 100 respondents answered that lost or stolen USB memory contained personal information in the main survey, the probability of lost USB memory to contain personal information is believed to be about 33%.

Therefore, the following events can be assumed:

(1) Event A is assumed as "USB memory is lost or stolen."
(2) Event B is assumed as "The lost/stolen USB memory contains personal information."

Here, we consider the probability of Event A and B occurring simultaneously, which is a product event A∩B. Also, the act of "loosing USB memory" and the act of "storing personal information on USB memory" do not influence with one another; therefore, Event A and Event B can be considered as independent events. Thus, the probability of these two events occurring simultaneously can be obtained by applying multiplication theorem: $P(A \cap B) = P(A) \cdot P(B)$. As the probability of Event A is 4.5% and the probability of Event B is 33%, the actual calculation by applying multiplication theorem is 4.5% X 33% = about 1.5%. Consequently, the probability of losing USB memory containing personal information in a year is about 1.5% per one employee. (No consideration is given here as to whether the USB memory is lost inside or outside the office, because there is no knowing as to where those employees, who carry around customer information by USB memory, actually lose it. The result of main survey showed that it was often lost in their offices.)

Furthermore, if 100 employees carry around customer information using USB memory on a daily basis, the estimated number of actual incidents is: 100 X 1.5%/person = 1.5 persons. As indicated in TableTable 2.2-2: Breakdown of indirect damages, the estimated amount of damage per one incident is 27.86 million yen; therefore, 27.86 million yen X 1.5 persons = 41.79 million yen can be considered as the risk.

If this calculation holds for an organization with the above-mentioned profile, up to 41.79 million yen can be invested in security measures to prevent such incidents. In addition, when considering that life cycles of the current IT devices and solutions are about three (3) years, it may be worth considering an investment of 41.79 million yen X 3 = 125.37 million yen in a lump for three years.

Conversely, if the damage amount is small and the calculated amount of risks is below investment amount, it is conceivable that the organization makes an administrative decision to "accept the risk" instead of venturing to embrace the cost.

To improve the precision as a real information security management, the above-mentioned factors must go under statistical procedures to improve the precision of incident event probabilities across the corporation, while also considering that the probabilities differ by individual employees (refer to the next Chapter "Ratio of scatterbrains")

2.3. Ratio of scatterbrains

2.3.1. Has a person who was about to lose a mobile phone actually lost it?

Targeting for those people who were about to lose their mobile phones containing business data, we have deliberated the aggregated results to determine if they actually lost or had their mobile phones stolen.

Table 2.3-1: Ratio of people, who were about to lose, actually lost their mobile phones

Lost or stolen item	Company mobile phone (containing business data)		Personal mobile phone (containing business data)		Both company and personal mobile phones		No loss or theft of mobile phone		Total
Entire questionnaires	184	3.8%	204	4.2%	631	12.9%	3,906	80.0%	4,884
Those who were about to lose company mobile phone containing business data	15	8.4%	22	12.4%	46	25.8%	132	74.2%	178
Those who were about to lose personal mobile phone containing business data	7	3.6%	12	6.1%	28	14.3%	168	85.7%	196
Those who were about to lose both company and personal mobile phones containing business data	33	36.3%	34	37.4%	44	48.4%	47	51.6%	91

Note: The “company and personal mobile phones” include mobile phones without business data.

- Those people who were about to lose company mobile phone are more apt to lose, as compared with the aggregation result of the entire questionnaires.
- The ratio of people who were about to lose personal mobile phone was the same as the aggregation result of the entire questionnaires. The ratio of people who did not experience either loss or theft is greater than the aggregation result of the entire questionnaires.
- For those who were about to lose both company and personal mobile phones, the ratio of actually experiencing loss or theft is eight (8) times more than the total aggregation result.

The following hypotheses can be assumed:

- Personal mobile phone is more carefully handled than company mobile phone. Or, the chance of losing is much smaller as it is always carried around. One can quickly realize that it is about to be lost.
- It is highly possible that those people who were about to lose both company and personal mobile phones are more apt to lose them (scatterbrains). Corporations must be forewarned of scatterbrained people that exist at a constant rate.

2.3.2. Has a person who was about to lose a personal computer actually lost it?

Targeting for those people who were about to lose their personal computers containing business data, we have deliberated the aggregated results to determine if they actually lost or had their personal computers stolen.

Table 2.3-2: Ratio of people, who were about to lose personal computers, actually losing their PCs

Lost or stolen item	Company PC (containing business data)		Private PC (containing business data)		Both company and private PCs		No loss or theft of PC		Total
Entire questionnaires	148	3.0%	129	2.6%	307	6.3%	4,364	89.4%	4,884
Those who were about to lose company personal computer containing business data	21	16.5%	16	12.6%	35	27.6%	92	72.4%	127
Those who were about to lose Private PC containing business data	2	2.0%	4	4.1%	8	8.2%	90	91.8%	98
Those who were about to lose both company and private PCs containing business data	24	35.8%	24	35.8%	36	53.7%	31	46.3%	67

Note: The “company and personal PCs” include PCs without business data.

- Those people who were about to lose company personal computer are more apt to lose, as compared with the aggregation result of the entire questionnaires.
- The ratio of people who were about to lose private PC was the same as the aggregation result of the entire questionnaires. The ratio of people who did not experience either loss or theft is greater than the aggregation result of the entire questionnaires.
- For those who were about to lose both company and personal mobile phones, the ratio of actually experiencing loss or theft is 10 times more than the total aggregation result.

The following hypotheses can be assumed:

- Private PC is more carefully handled than company PC.
- Corporations must be forewarned because it is highly possible that those people who were about to lose both company and private PCs are more apt to lose them (scatterbrains).

2.3.3. Are there many people who lost mobile phone, personal computer, or USB memory at the same time?

We have deliberated the trend where those people, who had experienced loss or theft of mobile phone, personal computer, or USB memory, also experienced loss or theft of other items.

Table 2.3-3: Ratio of people who lost mobile phone, personal computer, and USB memory at the same time

	Loss of company mobile phone		Loss of company PC		Loss of company USB memory		Total
Entire questionnaires	184	3.8%	148	3.0%	146	3.0%	4,884
Those who experienced loss or theft of company mobile phone containing business data			108	58.7%	102	55.4%	184
Those who experienced loss or theft of company PC containing business data	108	73.0%			97	65.5%	148
Those who experienced loss or theft of company USB memory containing business data	102	69.9%	97	66.4%			146

- Those people who experienced loss or theft of mobile phone, PC, or USB memory also experienced loss or theft of other items with a probability of 50% or more.
- Particularly, over 70% of the people who experienced loss or theft of company PCs also experienced loss or theft of company mobile phones.

The following hypotheses can be assumed:

- There always exist such people that are apt to lose items (scatterbrains).
- There may be many cases where people experienced loss or theft when mobile phone, personal computer, and USB memory were carried in the same bag.

2.3.4. Are those who are apt to lose items also apt to make wrong transmissions?

We have deliberated the trend where those people, who had experienced loss or theft of mobile phone, personal computer, or USB memory, were also caused email or fax incidents.

Table 2.3-4: Loss or theft of company items containing business data vs. wrong transmissions

Experience of loss or theft?	Company mobile phone containing business data		Company PC containing business data		Company USB memory containing business data	
	Yes	No	Yes	No	Yes	No
Sent email to wrong destination	129 (70.1%)	2,916 (62.0%)	115 (77.7%)	2,930 (61.9%)	122 (83.6%)	2,923 (61.7%)
Sent email along with other person's email address, which should been hidden, to be easily identified.	65 (35.3%)	405 (8.6%)	61 (41.2%)	409 (8.6%)	66 (45.2%)	404 (8.5%)
Sent email with confidential information written in or attached to it.	42 (22.8%)	189 (4.0%)	39 (26.4%)	192 (4.1%)	43 (29.5%)	188 (4.0%)
Sent fax to wrong destination	134 (72.8%)	2,523 (53.7%)	110 (74.3%)	2,547 (53.8%)	120 (82.2%)	2,537 (53.5%)
Sent wrong document via fax	69 (37.5%)	978 (20.8%)	62 (41.9%)	985 (20.8%)	68 (46.6%)	979 (20.7%)

Never made wrong email transmission	40 (21.7%)	1,506 (32.0%)	20 (13.5%)	1,526 (32.2%)	13 (8.9%)	1,533 (32.4%)
Never made wrong fax transmission	34 (18.5%)	1,570 (33.4%)	25 (16.9%)	1,579 (33.3%)	14 (9.6%)	1,590 (33.6%)
Total	184	4,700	148	4,736	146	4,738

- Those people who experienced loss or theft of mobile phone, PC, or USB memory are more apt to cause email or fax incidents than those who had never experience loss or theft.
- Particularly, the probabilities are 4 to 5 times higher in items "Sent email along with other person’s email address, which should been hidden, to be easily identified” and “Sent email with confidential information written in or attached to it.”

The following hypotheses can be assumed:

- Those who are apt to lose items (scatterbrains) are also apt to cause wrong transmission incidents.

3. Conclusion

Based on the results of this survey, the JNSA Incident Damage Survey Working Group had repeatedly deliberated on how the Japanese information security should be and what should be done for the future. As the result, we would like to propose the following:

3.1. Organizations must grasp incidents

Although it depends on the types of incidents, this survey confirmed that the number of incidents, about which the involved persons reported the facts to their organizations, is only about half of the incidents that had actually occurred, and--even when the organization had grasped the facts--only half of the reported incidents, that is merely about one fourth of the entire incidents, had eventually been publicized.

Some incidents may not require to be publicized depending on the contents; however, organizations must at least grasp every single bit of high-risk incident. Then, future incident occurrences can be prevented effectively by analyzing the cause and trend of incidents and taking countermeasures as required. When taking countermeasures on an ad hoc basis without knowing the actual situation, it is questionable whether such countermeasures are effective. Incidents must also be publicized when required for preventing secondary damages and similar incident occurrences.

Creating an environment where involved persons can easily report the facts in person is considered as one of the methods to grasp incidents. Those reports that are disadvantageous to themselves can hardly turn up by simply asking them to report the facts. A system must be established to facilitate reporting, e.g. no penalty is applied to reporting, punishment is lightened when reported immediately and voluntarily, heavy punishment is imposed for delayed reporting or no reporting, and severe punishment is imposed for false reporting, etc. Also, appropriate personnel who can carry out appropriate initial steps must be assigned to the report receiving side. Even when reports are received, failure to respond sincerely will result in less and less number of reports to turn up.

Another method to grasp incidents is to perform monitoring. This method includes: storing all email messages and checking the contents by random selection, extracting messages by non-business-related keywords, detecting connections of unauthorized devices, and maintaining a log of downloaded files, etc. It is, however, not really recommended to make a large investment in monitoring from the beginning. Recommended process is to gradually upgrade the stages of monitoring in the following order and retain the stage with which sufficient deterrent effect is obtained.

- First stage: publicize the fact that monitoring is performed in the office.
- Second stage: partially publicize the monitoring results.
- Third stage: impose punishment according to the monitoring result.

Although the fact that monitoring is performed should be publicized in the office, it would be better to keep a lid on what is monitored and to what extent so as to play it close to the chest. A considerable restraint effect can be expected only by publicizing the fact that monitoring is performed.

We consider that it is about time to break away from the awareness that incident occurrence is a “terrible thing.” Although there is no alternative but to impose severe punishment for intentional wrongdoings including information leakage and data destruction, appropriate punishments according to the influence of incidents should be enough, if they are minor violations caused by negligence or carelessness. Imposing severe punishments even for trivial incidents in trying to decrease incident occurrences will result in decreased number of incident reports, which may eventually lead to a situation where the organization cannot prevent serious incidents. It is better to have no incidents at all; however, we consider that organizations would be better off taking their stand on the premise that incidents occur at a certain probability.

3.2. Provide mobile phones and PCs as needed

In terms of incident prevention, it is not recommended to use personal mobile phones and PCs for business purposes. The number one reason is that the management of personal items is also left to the person who owns them. For example, organizations can hardly force employees to buy new personal mobile phones equipped with higher security features, or upgrade to high-performance antivirus software for their private PCs. The second reason is that it is highly possible for organizations to become unable to press charges of criminal responsibility against them. As Japan does not have criminal charge on theft of information, cannot be established even when information is duplicated and taken out by means of individually-owned devices.

The simplest solution is a total ban on business usages of individually-owned mobile phones and PCs, if it is possible. Even when a total ban is imposed, some employees may use their private items in secrecy if desperate needs arise in the course of their work. Using them in secrecy is more dangerous than a situation where a total ban is not imposed. If a total ban is not possible, usage of private items should be allowed by obtaining an approval, on condition that they are equipped with security features and antivirus software. An even better solution is to provide mobile phones and PCs from the organization.

For those employees who are apt to encounter various incidents, so-called scatterbrains (refer to 2.3), the best bet is to assign them such tasks that do not involve confidential information. If there is no choice but to use mobile phones and PCs for business purposes, it is better to preferentially provide mobile phones equipped with security features and PCs of thin client type to prevent possible information leakage in case of loss.

3.3. Use fax and email on the premise that accident can occur

The event probability of wrong transmission incidents for fax and email is considerably high; about 40% annually per person. In case of a telephone communication, one can realize that it is a wrong number as the other end of the line is confirmed at the first swing of conversation, before any information can be leaked out. In the case of fax, however, if the dialed number happens to be a fax line, the document is delivered to the other party as it is. Similarly, if a misspelled email address happens to exist, the email is delivered to the mailbox on the other side as it is. Also, an erroneous selection from the address book will deliver the email to a different person because the address is a valid one. Due to such reasons, it is better to consider that fax and email can be a risky means of communication.

It is rather dangerous to think on the premise that no one makes mistakes and that incidents can never occur. Mistakes are not such things that never occur, but are things that occur at a certain probability. In the case of fax and email, it is highly possible that a single mistake directly leads to an incident. When thinking on the premise that mistakes and incident will never occur, one may possibly think it is all right to include confidential information in an email text. Instead, one must think on the premise that mistakes and incident could happen. When thinking on that premise of incident occurrences, one may start to exercise caution such as encrypting confidential information before attaching it to email, avoiding the use of fax for sending a confidential information and using other means instead of fax.