26

Application and Education of "Multiple Risk Communicator"

Mitsuhiro Taniyama[1] and Ryoichi Sasaki[1]
[1]*Tokyo Denki University*
Japan

1. Introduction

Along with the progress of our information society, various risks have become increasingly common, resulting in multiple social problems. To deal with these social problems, opposing factors such as security, privacy, convenience, and cost have to be considered. For this reason, risk communications that aim at establishing consensus among stakeholders who have different priorities have become important. Moreover, when considering measures against risk, it is essential to consider an optimal combination of measures because one single measure is not sufficient to solve a particular problem.

However, it is not always easy for decision makers to agree on an optimal combination of measures that reduce some risks due to considerations relating to other risks. To alleviate this difficulty, we previously proposed the "Multiple Risk Communicator" (MRC), which supports risk analysis and risk communication in our information society (Sasaki et al., 2005), and developed the "MRC Program" (Sasaki et al., 2008).

In this chapter, we first describe the concept and an application process of MRC. We then describe the result of applying MRC to the problem of personal information leakage. On several occasions in recent years, a number of organizations such as businesses and schools have accidentally leaked personal information, and such leakages have become a social problem in Japan. According to a report published by the Japan Network Security Association, 864 incidents occurred in fiscal year 2007. If an organization leaks personal information, it loses the trust of the people. This sequence of events can potentially lead to a decreased number of customers and decreased stock price.

Many organizations have taken measures to avoid this problem. These measures, however, can lead to further problems. For example, employees in one enterprise may be dissatisfied with the decreased convenience and privacy resulting from applying strict measures, while the customers whose personal information is maintained by the enterprise require strong reassurances that their personal information will not be leaked. Moreover, the executive officer in the enterprise would like to keep costs as low as possible.

Given the above information, it is easy to understand the difficulties in applying measures that establish consensus among these stakeholders. Therefore, we decided to apply MRC to the personal information leakage problem. A practical application process of MRC is described in detail and the evaluation of MRC is discussed in this chapter.

In addition, we propose some training methods that allow MRC to be used by many users. MRC was applied to personal information leakage, illegal copying, and internal control, and the effectiveness of MRC was verified. "MRC Program" has been designed to be used by anybody through the Internet, although "Mathematica 5.2" has to be installed on the user's computer. However, it is hard for the users to learn what the MRC is and to use "MRC Program". Therefore, we proposed training methods that allowed a beginner to easily understand the concept and application process of MRC and then learn to use "MRC Program" because we would like to disseminate MRC and improve MRC and "MRC Program" by collecting users' opinions. These training sessions were performed for three different subject groups and the results revealed a new use and improvements to the MRC. The MRC education methods and the results are described in this chapter.

2. Overview of MRC

2.1 Concept and System Structure of MRC

The MRC concept was examined and the "MRC Program" version 1.0 was developed in a previous study (Sasaki et al., 2005, 2008). MRC was applied to social problems such as illegal copying, internal control, and compromising of public key ciphers. The objective of MRC is to reduce risk with consideration of the following.

Requirement 1: There are various conflicting risks, and the measures to reduce one or more risk must take all risks into consideration.

Requirement 2: Various measures are required for individual risks. Thus, resolving every problem with one measure is not possible, and features for determining the most appropriate combination of measures are essential.

Requirement 3: For decision-making, the individuals involved (e.g., managers, citizens, customers, and employees) must be satisfied. Therefore, features for supporting risk communications among these individuals are essential.

Few studies of risk analysis satisfying all the above requirements have been conducted. For example, the Japanese Standards Association published "Information technology -- Guidelines for the Management of IT Security -- Part 3: Techniques for the Management of IT Security," which classifies the methodologies of risk analysis into four categories. Additionally, Bruce Schneier, who is an internationally renowned security technologist and author, describes the methodologies of risk analysis in his book "Beyond Fear." However, these methodologies are not sufficient to satisfy all the above requirements. Because of this, we decided to establish a methodology of risk analysis that satisfies all the requirements.

An overview of the MRC program for satisfying these requirements is shown in Figure 1. The basic feature satisfying Requirement 1 and Requirement 2 is the Optimization Engine, which is (4) in Figure 1. In the optimization engine, a brute force method and lexicographic enumeration method are used to obtain the solution (Garfinkel et al., 1972). In particular, a discrete optimization problem with various measures proposed as 0-1 variables (or a 0-1 programming problem) is used. To formulate the discrete optimization problem easily, the Assistant Tool for Specialists (6) contains the functions of analysis, formulation and parameter setting. In addition, the fault tree analysis (FTA) method for the risk analysis (McCormick, 1981) is supported in this tool.

The Assistant Tool for Participants (1) satisfies Requirement 3 for decision-making. The optimal combinations of measures obtained from the Optimization Engine (4) enable

decisions to be made more easily by the individuals involved. Opinions such as "Add the measures we propose" and "We propose to change the value of this constraint" are sent to the specialist via the Negotiation Infrastructure (5). Then, the facilitator supports the communication between the participants and the specialist. The Total Controller (3) and Database (2) link the processing of these components.
The MRC program is implemented using Java and PHP 5.2 in a Windows XP environment. The total number of coding steps is approximately 10,000. Apache 2.24 is used for the Web server, MySQL 5.0 for the database server, and Xoops 2.0.16 for the communication server. In addition, Mathematica 5.2 is used by the specialist to calculate the numerical formulas using the PC.

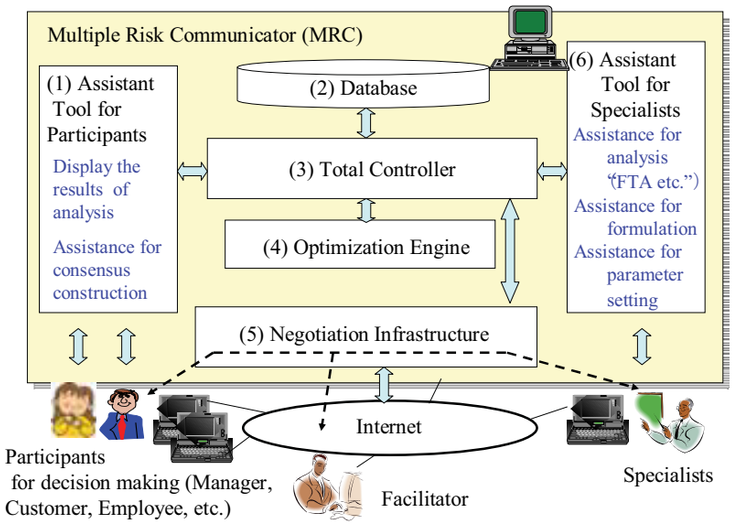

Fig. 1. Overview of MRC

2.2 MRC Application Process

The MRC application process is shown in Figure 2. First, the individual, such as a decision maker who needs to solve a problem, proposes the object an MRC expert who is able to use the MRC program. Second, the MRC expert analyzes the risk (Steps 1-7 in Figure 2). If the MRC expert is not knowledgeable about the risk, this MRC expert should analyze the risk with the assistance of an expert who does have a thorough knowledge of the risk. Third, the MRC expert inputs the risk analysis data into the MRC program (Step 8 in Figure 2). In the fourth step, the MRC expert inputs the values of the constraints, which is decided among the participants, into the MRC program (Step 9 in Figure 2). Fifth, the optimal combination of measures is obtained by the optimization engine of the MRC program (Step 10 in Figure 2). Sixth, the MRC expert shows the result obtained by the MRC program to the participants, and the participants conduct risk communication in order to build a consensus of measures (Step 11 in Figure 2). The role of the facilitator is to manage the discussion and lead the discussion to a consensus.

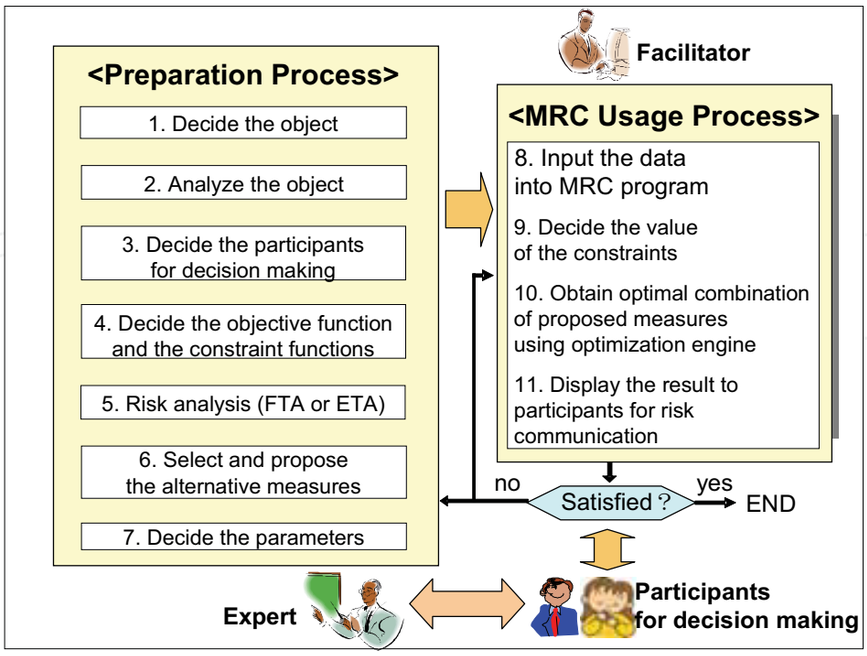

Fig. 2. MRC application process

3. Application of MRC to the Personal Information Leakage Problem

3.1 Personal Information Leakage Problem

On several occasions in recent years, a number of organizations such as businesses and schools have accidentally leaked personal information, and such leakages have become a social problem in Japan. According to a report published by the Japan Network Security Association, 864 incidents occurred in fiscal year 2007. If an organization leaks personal information, it loses the trust of the people. This sequence of events can potentially lead to a decreased number of customers and decreased stock prices.

For this reason, many organizations have taken measures to prevent such problems. Such measures, however, can lead to further problems. For example, employees in one enterprise may be dissatisfied with the decreased convenience and privacy caused by applying strict measures, while customers whose information is maintained require strong reassurances that their personal information will not be leaked.. Moreover, the executive officer in the enterprise would like to keep costs as low as possible.

Given the above information, it is easy to understand the difficulties in applying measures that establish consensus among these stakeholders. Therefore, we decided to apply MRC to the personal information leakage problem.

3.2 History of MRC

The history of MRC research is described in Table 1. In the first stage, MRC was applied to the information leakage problem of an Internet service provider. At that time, the MRC program was not completed and a prototype version was used. Once MRC version 1.0 was completed, the program was applied to the information leakage problem in a simulation of

an enterprise (Taniyama et al., 2008). In addition, MRC program version 1.0 was applied to the information leakage problem in an elementary school and junior high school. At that time, actual participants were involved in the risk analysis and risk communication steps. The result of applying MRC to the information leakage problem in the enterprise is described in this section.

	Object	Participants	MRC program
1	Internet service provider	Role players	Prototype
2	Enterprise	Role players	MRC program Ver. 1.0
3	Elementary school and junior high school	Actual participants	MRC program Ver. 1.0

Table 1. MRC history

3.3 Application of MRC to the Information Leakage Problem

3.3.1 Attributes of the Enterprise

Following the Preparation Process shown in Figure 2, we consider a simulated enterprise whose sales department handles ten million pieces of personal information. The number of employees is approximately 1,820. Only 20 of these employees were allowed into the server room. However, the employees who were not allowed into the server room could obtain the minimal amount of personal information deemed necessary to perform their duties from the server if they obtained permission from their managers.

3.3.2 Analyzing the Object

We conducted the following actions to analyze the information leakage problem.
(1) Using the Internet, past incidents of information leakage were investigated.
(2) A report published by the Japan Network Security Association, which mentions the routes of information leakage, number of incidents, and other related information was studied
(3) Employees of the enterprise were asked their opinions on how customer information should be handled and which measures they were dissatisfied with.

3.3.3 Deciding the Participants

The following participants were selected.
(1) Enterprise chief executive officer
(2) Enterprise employees
(3) Customer whose personal information was maintained by the enterprise.

3.3.4 Decision of the Objective Function and Constraint Functions

The objective function decides the optimal combination of measures. Formulation of the objective function is described as follows.
Min {Total risk of information leakage + Total cost of measures}
where,
Total risk of information leakage = Value of one piece of personal information x the number

of leaked personal information per incident x probability of leakage for a year.
The Total cost of measures was calculated using the parameters shown in Table 4. The variables of the Total risk of the information leakage equation are defined in more detail in Section 3.3.7. The Probability of leakage for a year is obtained by using the fault tree analysis described in Section 3.3.5.
The constraint functions are decided as follows:
(1) Cost of measure for the executive officer
(2) Probability of leakage (for one year) for the customer
(3) Degree of burden on employee' convenience
(4) Degree of burden on employee' privacy.
The formulations for each of these constraint functions are described as follows (in the order presented above):

$\sum_{i=1}^{n} Co_i X_i \le Co_t$	(1)
$f_p(X_1, X_2, ..., X_n) \le P_t$	(2)
$\sum_{i=1}^{n} E_i X_i \le E_t$	(3)
$\sum_{i=1}^{n} \mathrm{Pr}_i X_i \le \mathrm{Pr}_t$	(4)

Here, X_i is represented as 0-1 variables and is a flag indicating whether to take the measures; Co_i, E_i, and Pr_i are calculated by the parameters of the measures; f_p is r the probability of leakage for one year, and is calculated using the fault tree analysis described in Section 3.3.5.

3.3.5 Fault Tree Analysis

FTA was used to quantify the risk of the probability of personal information leakage. The process of FTA is described as follows.
(1) Define the undesired effect.
(2) Each event that could cause the top event is added to the tree as a series of logic expressions.
(3) The probabilities of the lowest event are obtained from the statistics or opinions of experts.
(4) The probability of the top event is obtained from the calculation of the events, as defined in the previous steps (2)-(3).
Here, five fault trees were constructed (Figure 3). The top events of these are (a) Leakage from the server, (b) Leakage from a desktop PC, (c) Leakage from printed information, (d) Leakage from a laptop, and (e) Leakage from a portable device (e.g., USB memory chip, portable hard disk, CD/DVD, etc.). Lower events are accidentally leaks by internal personnel (leakage by employees), Internal person leaks fraudulently (leakage by an internal person who has stolen the information from the enterprise), and External person fraudulently leaks (leakage by an external person occurring when information is stolen from outside the enterprise). These lower events were also analyzed.
The lowest event probability was obtained using reports from the Japan Network Security Association.

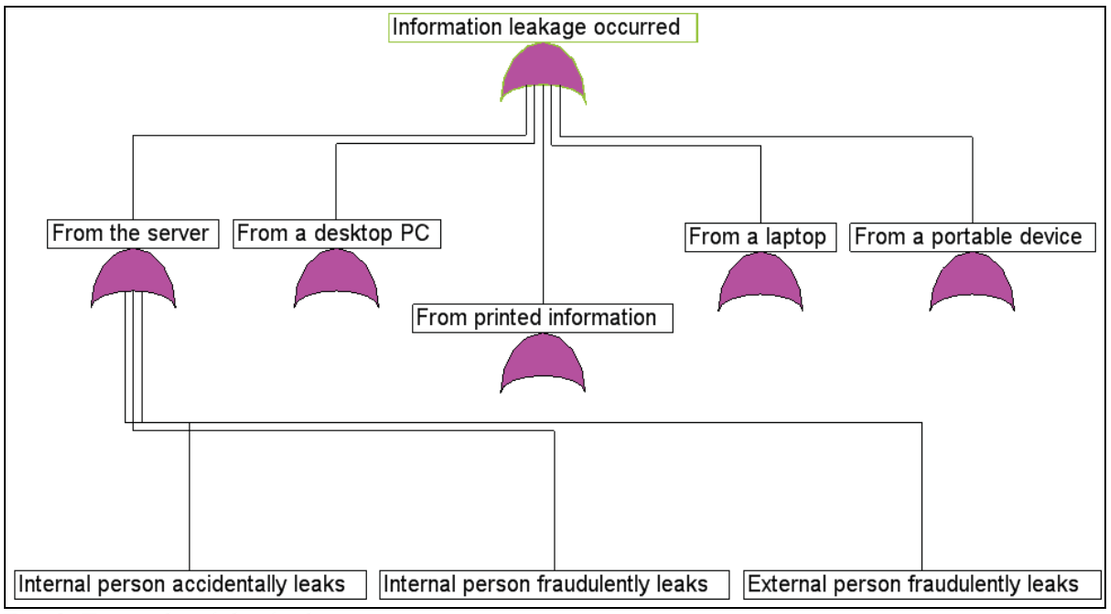

Fig. 3. Example of the fault tree

3.3.6 Selection of Measures

We decided the following prerequisites for the measures proposed (Table 2).

No	Detail
1	A firewall is installed.
2	Antivirus software and security patches are installed on all computers.
3	Employees cannot enter the server room without an identification card.
4	Employees are required to enter their password when they log into their PC.
5	Employees are required to put papers that contain personal information through the shredder.
6	Employees are required to get the manager's permission when they remove their laptop or USB memory chips from the enterprise.
7	Employees are permitted to take printed information out of the enterprise.

Table 2. Prerequisites for proposed measures

Because these measures have been instituted by many enterprises according to the report of the Japan Network Security Association, these were selected not as measures but as prerequisites. Considering the above prerequisites, we selected the following 15 measures (Table 3). In cases of 6 through 11 from the proposed selection of measures, only one of the alternate details was selected. This is due to the similarity of the measures in each detail.

No	Detail
1	Install a system that forces employees to change their password four times a year.
2	Install management software that prevents employees from using unauthorized software.
3	Install management software that prevents employees from using portable devices with the server.
4	Install a surveillance camera.
5	Install a URL filtering tool to prevent the use of web-based email and message-board postings.
6	Install a mail-filtering tool to restrict emails sent and received. (Employees cannot send email out of the enterprise without sending a copy to their manager.)
7	Install a mail-filtering tool that restricts emails sent and received. (Employees cannot send email containing only an attached file out of the enterprise without sending a copy of the mail to their manager.)
8	Install management software to encrypt the data automatically when employees try to copy data from a desktop or laptop computer to a portable device. (Employees cannot decode data without a computer owned by the enterprise.)
9	Distribute USB memory chips that encrypt data automatically to all employees.
10	Install a system to automatically encrypt data stored in laptop computers.
11	Distribute thin client computers to employees.
12	Restrict the removal of printed personal information form the enterprise.
13	Install a system to automatically put watermarks on the print.
14	Install an intrusion detection system.
15	Install a security scanning system at all entrances into the enterprise.

Table 3. Proposed Selection of Measures

3.3.7 Determining the Parameters

(1) The values of the parameters were obtained by discussions among the employees in the enterprise (Table 4). The cost was obtained by investigating product brochures. Although the cost was originally compiled in Japanese yen, it is converted into U.S. dollars because the dollar is known all over the world. The exchange rate on August 27, 2008 was used (1 U.S. dollar = 109 Japanese yen). The degree of burden on an employee's convenience and privacy ranges from 0 (minimum) to 1.0 (maximum). If a satisfactory probability to decrease leakage is 0.8, the information leakage is decreased by 80% in an event of the fault tree. The value of a satisfactory probability was actually set with more specificity, however some factors have been omitted here due to limited space.

No.	Satisfactory probability of decreased leakage					Cost (U.S. $)	Convenience burden	Privacy burden
	Server	Desktop computer	Print	Laptop computer	Portable device			
1	0.8	0.8		0.5		167,823.12	0.8	0
2	0.65	0.65		0.85		164,766.06	0.5	0
3	0.99					770.64	0.4	0
4	0.4	0.4	0.2	0.4	0.4	38,532.11	0	0.5
5	0.7	0.7		0.7		89,339.45	0.4	0
6	0.8	0.8		0.8		51,880.73	0.6	0.6
7	0.75	0.75		0.75		67,431.19	0.4	0.5
8		0.99		0.99	0.999	265,967.89	0.2	0
9					0.999	330,275.23	0.3	0
10				0.999		140,256.88	0.3	0
11				0.999		2,642,752.29	0.4	0
12			0.8			198,165.14	0.7	0
13			0.6			397,506.88	0.1	0.1
14	0.75					179,541.28	0	0
15	0.8	0.8	0.8	0.8	0.8	22,935.78	0.3	0

Table 4. Parameters of the proposed measures

(2) For our simulated enterprise, the value of one piece of personal information is defined as 10,000 Japanese yen (1 U.S. dollar = 109 Japanese yen on August 27, 2008) based on an incident in Uji City in Kyoto, Japan. One organization, accused of personal information leakage, was sentenced to pay 10,000 Japanese yen to a plaintiff for pain and suffering caused.
(3) We must estimate the probability of the lowest events of the fault tree because it is impossible to accurately determine the probability of these events. When the probability of these events can be obtained using past data, the probabilities of the lowest events were obtained using reports from the Japan Network Security Association. If the probabilities of these events cannot be obtained using past data, the values were first estimated and classified into five levels after which the values are finally decided. The actual probabilities of the lowest events are omitted here due to limited space.
(4) The amount of leaked personal information per incident was obtained from a report published by the Japan Network Security Association. This report, which has been published every year since 2002, summarizes the investigation of articles regarding personal information leakage problems. The number of items of leaked personal information was classified and determined by the sources (a)–(d), shown below. In this risk analysis, the number of leaked personal information per incident was obtained as averaged data from 2004 to 2006 reports. It was supposed that the server in the computer room of the enterprise maintained ten million pieces of personal information. A summary of these leaked items is as follows.
(a) Leakage from the server: ten million pieces of personal information
(b) Leakage from laptop or desktop computer: 4,734 pieces of personal information
(c) Leakage from portable devices such as USB memory chips, hard disks, floppy disks, CD/DVDs, etc.: 7,120 pieces of personal information
(d) Leakage from printed material: 537 pieces of personal information.

3.4 Risk Communication Using MRC

This section describes the MRC Usage Process presented in Figure 2. The data obtained by the risk analysis was input into the MRC program. We then conducted an experiment of risk communication to establish the consensus among role players, as follows.

First, the role players are described as follows.

(1) Executive officer: a professor at Tokyo Denki University

(2) Customer: a student at Tokyo Denki University

(3) Employees: two employees of the enterprise.

(a) First, an MRC program specialist conducts the optimization step using MRC if no measures have been adopted. We obtained the probability of leakage in order to enable the participants to determine the value of constraints more easily. The results are shown in Table 5.

Cost (U.S. $)	0
Probability of leakage (for one year)	0.3036
Burden on employee convenience	0
Burden on employee privacy	0
Measures	
Optimal value (U.S. $)	12,310,247.95

Table 5. Case in which no measures were adopted

(b) Second, the specialist sets the value of the constraints, as shown in Table 6, and conducts the optimization step using MRC. In our experiment, the cost constraint was half of the cost ($1,504,331.28 U.S.) when considering all measures. The probability of leakage was half of the probability (0.1518) when no measure was adopted because due to a customer's desire. Because there were some opinions from the stakeholders that were difficult to set in terms of convenience and privacy burdens, those were set at the maximum values. Optimized solution "A", shown in Table 7, was obtained for this constraint.

Cost (U.S. $)	1,504,331.28
Probability of leakage (for one year)	0.1518
Burden on employee convenience	4.5
Burden on employee privacy	1.2

Table 6. Constraint conditions

Cost (U.S. $)	830,749.72
Probability of leakage (for one year)	0.14328
Burden on employee convenience	2.5
Burden on employee privacy	0.6
Measures	1,2,3,6,8,14
Optimal value (U.S. $)	1,664,448.57

Table 7. Optimized solution A

(c) Third, optimized solution A was suggested to the stakeholders. After reviewing optimized solution A, the customers suggested further decreasing the probability of leakage. Accordingly, the probability of leakage was set as one-third of the probability (0.1012) when

no measure was adopted. Once this was accomplished, we conducted the optimization again. However, no optimized solution was obtained.
For this reason, the customers again suggested setting the probability of leakage as two-fifths (0.12144). Optimized solution B, shown in Table 8, was obtained for this constraint.

Cost (U.S. $)	1,169,171.74
Probability of leakage (for one year)	0.12001
Burden on employee convenience	3.5
Burden on employee privacy	0.6
Measures	1,2,3,6,8,10,12,14
Optimal value (U.S. $)	1,998,456.07

Table 8. Optimized solution B

(d) Although the customers were satisfied with optimized solution B, the employees were dissatisfied because they felt that, if such strict measures were adopted, they would cause inconveniences in their work. Particularly, because the convenience burden of measure No. 6 (Employees cannot send email out of the enterprise without sending a copy to their manager) was felt to be very high, the employees suggested it be eliminated. The customers and executive officer agreed with this demand and decided not to adopt No. 6.
However, since the employees said that they could accept adoption of No. 7 (Employees cannot send email containing an attached file out of the enterprise without sending a copy to the manager), No. 7 adopted instead of No. 6. Optimized solution C, shown in Table 9, was obtained for this constraint.

Cost (U.S. $)	1,184,722.20
Probability of leakage (for one year)	0.12439
Burden on employee convenience	3.3
Burden on employee privacy	0.5
Measures	1,2,3,7,8,10,12,14
Optimal value (U.S. $)	2,015,937.31

Table 9. Optimized solution C

(e) Although the probability of leakage slightly increased, the customers were satisfied with optimized solution C. Employees were satisfied by adopting No. 7 instead of No. 6. Although the cost of optimized solution C was more expensive than solutions A and B, the executive officer accepted it as well. Consequently, all participants were satisfied with optimized solution C, and they succeeded in establishing consensus.

3.5 Evaluation of the MRC

3.5.1 Evaluation of the Objective Function

As defined in this paper, the damage caused by one piece of personal information leakage was set at 10,000 Japanese yen. However, to set a precise value, we will need to consider the damage caused by the decrease of trust in the enterprise and the decrease of the stock price. Moreover, the expenses incurred when dealing with mass media and lawyers must be considered. These are issues of risk analysis for future work.

3.5.2 Evaluation of the Constraint Function

When the stakeholders decided the value of the constraints, there was a general opinion that it was difficult to understand and determine the degree of burden on convenience and privacy. Hence, we let employees reject the measures they did not want to take. As a result, the risk communications went smoothly and we obtained knowledge that helped the stakeholders decide the constraints more easily.

3.5.3 Evaluation of Risk Communications

Because the experiment of risk communications was a simulation conducted by role players, they easily succeeded at establishing consensus. However, if the risk communication was conducted by actual stakeholders, it was thought that establishing consensus would be more difficult. In particular, even though the executive officer did not complain about the cost during the above risk communication, this sort of agreement rarely happens with actual stakeholders.

In future work, we plan to conduct risk communications with actual stakeholders. To that end we have developed MRC program version 2.0, which supports risk communications in more varied ways (Yajima et al., 2007), and will conduct risk communications with this new version.

3.5.4 Usefulness of the MRC

In this section, we describe the optimized combination of measures obtained by several experts who are very familiar with the personal information leakage problem. These measures were set in MRC, and the result is shown in Table 10.

Cost (U.S. $)	970,235.96
Probability of leakage (for one year)	0.13479
Burden on employee convenience	2.4
Burden on employee privacy	0.6
Measures	1,2,6,8,10,14
Optimal value (U.S. $)	1,801,672.14

Table 10. Measures obtained by experts

Consequently, the measures selected by the experts and the measures of optimized solution "A" obtained by the MRC were almost identical. However, the measures selected by the experts and the measures of optimized solution C, which established consensus finally among the simulation stakeholders, differed. Therefore, it was determined that repeated discussions among stakeholders and additional modifications to the values of the constraints using MRC could lead to a combination of measures that satisfy all stakeholders. Furthermore, once we analyze the problem and enter the data into the MRC program, we can use it as a template for different organizations. This will expedite the determination of optimized measures.

4. MRC Training

4.1 Purpose of MRC Training

MRC was applied to personal information leakage, illegal copying, and internal control, and the effectiveness of MRC was verified. "MRC Program" has been designed to be used by anybody through the Internet, although "Mathematica 5.2" has to be installed on the user's computer. However, it is hard for the users to learn what the MRC is and to use "MRC Program". Therefore, we proposed training methods that allowed a beginner to easily understand the concept and application process of MRC and then learn to use "MRC Program" because we would like to disseminate MRC and improve MRC and "MRC Program" by collecting users' opinions. These training sessions were performed for three different subject groups and the results revealed a new use and improvements to the MRC. The MRC education methods and the results are described in this section.

4.2 Education Method for Beginners

4.2.1 Subjects

The education method for beginners is intended for people who do not know MRC. Eleven people belonging to the "Information Security Laboratory" at Tokyo Denki University participated in this training. Many of the subjects had previous knowledge about information security but did not have knowledge about MRC.

4.2.2 Overview of the Training Program

First, an explanation lasting 1.5 hours was presented to all subjects explaining what MRC is and why MRC is necessary in our society. Then, the subjects individually read a manual on how to participate in our training program and about how to use the MRC program. The subjects played a role similar to an information manager at an enterprise. It was assumed that the employees in the subject enterprise were dissatisfied with the decreased convenience and privacy caused by the strict measures. The goal of this training program was for the subjects to decide on an optimal combination of measures using MRC.

4.2.3 Working Process

Because it was considered to burdensome for the subjects to carry out all steps of the MRC application process (Figure 2), the subjects used the template of risk analysis described in section 3. Steps 1, 7, 8, 9, and 10 in Figure 2 were conducted by the subjects. The other steps were waived.

In the first step "Decide the object" (Figure 2), the subjects decided the number of employees, type of personal information, and so on, using Table 11.

1	Number of employees in the organization
2	Number of employees who are allowed into the server room in the organization
3	Number of pieces of personal information the organization maintains
4	Types of personal information maintained by the organization (choose one)
a	Basic information such as names, addresses, birth dates, or telephone numbers
b	Basic information + confidential information such as a salary, account number, or clinical record
c	Basic information + critical information such as crime records, sexual propensities, or account numbers & passwords
5	Number of devices the organization owns
a	Number of servers: one
b	Number of desktop PCs
c	Number of laptops
d	Number of electronic media such as USB memory chips and portable hard disk drives

Table 11. Questionnaire to decide the organization

In the seventh step "Decide the parameters" (Figure 2), the subject obtains the cost of measures and probability of the lowest events of the fault tree. The subject can obtain the values of these two parameters simply by inputting data into the template, which was created in MS Excel.
In the eighth step "Input the data into MRC program" (Figure 2), the subject inputs data such as the cost of the measures, event probabilities, and so on, into the MRC program.
In the ninth step "Decide the value of the constraints" and in the tenth step "Obtain optimal combination of proposed measures using the optimization engine" (Figure 2), the subject sets the values of the constraints, such as the probability of leakage or the cost of measures, and obtains the result from the MRC program. If the subject is not satisfied with the combination of measures obtained by the MRC program, the subject can repeatedly change the values of the constraints until he or she is satisfied with the combination of measures. The training process is finished when the subject obtains a satisfactory combination of measures.

4.2.4 Result and Discussion

The subjects answered a questionnaire after finishing this training program. According to the questionnaire, the average time for completing the training program was 4.88 hours. This amount of time required is not excessive and we think people who are not aware of MRC can easily participate in this training program.
The questionnaire evaluation results of MRC are described in Figure 4. Here, 5 is the best score and 1 is the worst. According to the questionnaire, understanding MRC is 3.18, understanding the risk is 3.00, and the proficiency of the MRC program (program's ability to perform its function or the ability of the subject to use the program) is 2.27. The reasons why the results of this training process were not high are described below.
(1) Understanding MRC was not high because each subject worked individually and could not conduct risk communication to reach a consensus, which is the main purpose of MRC.
(2) Risk understanding was not high because each subject had limited opportunities to learn about the information leakage problem through the MRC application process.
(3) MRC program proficiency was low because each subject input just a small amount of data.

As noted above, some ideas for improvement emerged during the training sessions for the beginners. Based on these results, we generated a "training method for beginner groups" and conducted it for groups of subject other subject groups.

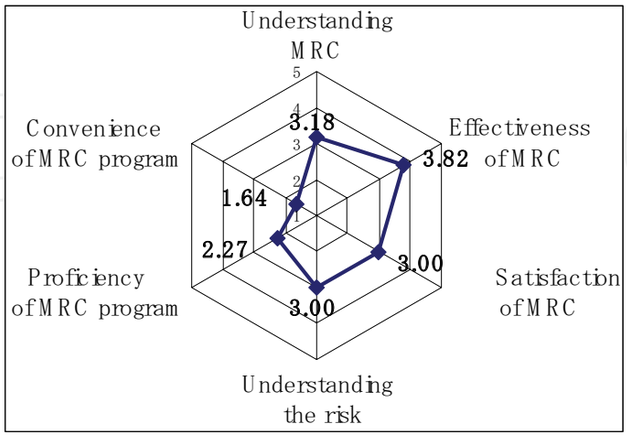

Fig. 4. Results of training method for beginners

4.3 Education Method for Beginner Groups

4.3.1 Subjects

The education method for the beginner groups was designed for people who had no previous knowledge of MRC. Twenty-eight people who attended a lecture on "Information Security" at the graduate school of Tokyo Denki University actually participated in this training program. Many subjects were interested in information security, but had no previous knowledge of MRC.

4.3.2 Overview of the Training Program

First, an explanation lasting 1.5 hours was given to all subjects on what MRC is and why MRC is necessary in our society. Then, the subjects were required to form groups of three or four, after which these groups applied MRC to the information leakage problem. When carrying out this training program, the subjects read a manual on how to proceed with this training program and how to use the MRC program.

In this training program, MRC is applied to the information leakage problem in a support department of a maker. The details of the maker, such as the contents described in Table 11, the rules for handling the customer's information, an overview of the system at the enterprise, and the flow of the customer's information, were shown to the subjects. The goal of this training was to ensure that the subjects obtained the optimal combination of measures in a specific enterprise using MRC.

4.3.3 Working Process

The subjects used the risk analysis template to participate in this training program. The content of the template, however, was different from the content created for individual beginners. Here, the subjects conducted risk communication within the group, learned more

about the information leakage problem during the risk analysis process, and input more data into the MRC program based on the results of the beginner-training program. Steps 2, 5, 6, 7, 8, 9, 10 and 11 in Figure 2 are conducted by the subjects. The other steps were waived.
In the second step "Analyze the object," the subjects decided the value of one piece of personal information. We determined that the subjects could learn about the personal information leakage problem through the process of investigating an information leakage report.
In the fifth step "Risk analysis," the subjects estimated and filled in the template blanks of the fault tree created for this program. This work helped the subjects learn the route of information leakage. Although a way exists for subjects to create a fault tree from raw materials, we chose to use a pre-created tree in order to reduce the burden on the subjects.
In the sixth step "Select and propose alternative measures," the subjects selected effective measures against information leakage. We showed the subject the eight previously determined measures and instructed them to select seven other measures. The subjects were able to learn about the information leakage problem through the process of investigating the measures and discussing their effectiveness within their groups.
In the seventh step "Decide the parameters," the subjects decided the cost of the measures and degrees of burden on convenience and privacy of the employees. Because the probability of the lowest event of the fault tree was given by the template, the subjects did not need to determine the probability. The cost of the measures was obtained by investigating the cost of genuine products. The degrees of burden on the convenience and privacy of the employees were obtained by discussing them within the group.
In the eighth step "Input the data into the MRC program," the subjects input data such as the value of one piece of personal information, measures against information leakage, and some parameters. More data was entered by the subjects in this training program than the data in training method for individual beginners.
In the ninth, tenth, and eleventh steps, the subjects input the value of constraints such as the cost or the probability of leakage, and obtained the result from the MRC program. The subjects conducted risk communication within the group using this result. The subjects decided the roles of the executive officer, employees, and customers and discussed the optimal combination of measures until all the subjects were satisfied with the result. The training program was complete when the subjects arrived at consensus within the group. We determined that groups of subjects could understand more about MRC by conducting risk communication because building consensus among the participants reflects the main purpose of MRC.

4.3.4 Result and Discussion

According to the questionnaire, the average time required to complete this training program was 6.70 hours. Even though this average time is 1.82 hours longer than the average time for the training of individual beginners, we do not think the amount of time required was an excessive burden on the subjects.
The questionnaire evaluation results of MRC are described in Figure 5. According to the questionnaire, understanding MRC was 3.93, understanding the risk was 4.07, and proficiency of the MRC program was 3.11. These are considered satisfactory results. Therefore, we concluded the group training method was effective for training beginners about MRC.

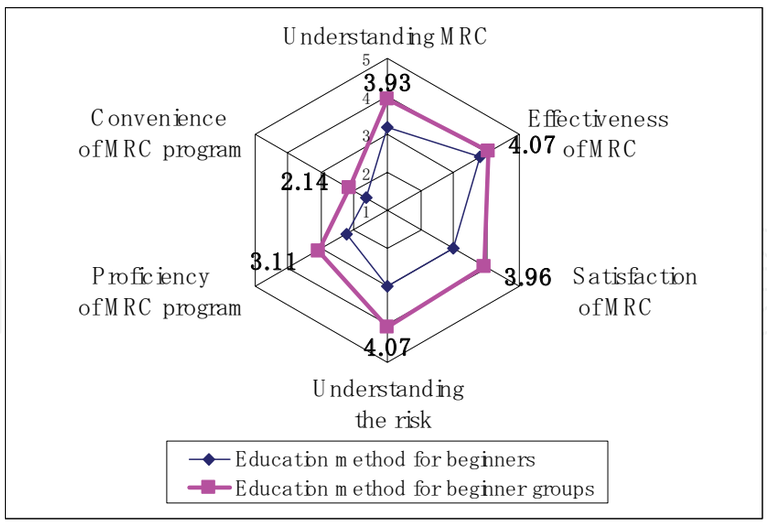

Fig. 5. Comparison between the results of the training method for beginners and beginner groups

4.4. Education Method for Experienced Groups

4.4.1 Subjects

The education method for experienced groups is designed for people who have completed the beginner group training and who want to learn more about MRC. Three students in the information security laboratory at Tokyo Denki University along with five students who are in the "integrated special scheme for information security specialist cultivation" participated in this training program. Three students from Chuo University and two students from the Institute of Information Security who also part of the "integrated special scheme for information security specialist cultivation" program also participated in the MRC training. The subjects were divided into three groups based on their university.

4.4.2 Overview of the Training Program

In the first step, the subjects participated in the training method for the beginner groups in order to learn about MRC and then apply MRC to different problems. In other words, the subjects were required to perform all steps of the MRC application process shown in Figure 2. The students of Tokyo Denki University applied MRC to an information leakage problem at a major insurance company while the students of Chuo University applied MRC to an information leakage problem at a hospital. Because the organizations were different from the one used in the beginner groups, the subjects were required to analyze the risk from the beginning. However, the subjects did not need to conduct step 2, "Analyze the object," because they had already analyzed the information leakage problem in their beginner groups. The students of the Institute of Information Security applied MRC to the problem of a fabricated TV show report entitled ***"Hakkutsu! Aruaru Daijiten"***. In this case, the subjects were required to conduct step 2, "Analyze the object," in order to fully understand this problem.

4.4.3 Result and Discussion

Based on the questionnaire results, the average time required to complete this training program was 13.67 hours. This amount of time is much longer than the time spent in training for the beginner groups because the subjects needed to complete all the steps of the MRC application process.

The results of the questionnaire evaluation of MRC are described in Figure 6. According to the questionnaire, understanding MRC was 4.50, understanding the risk was 4.13, and the proficiency of the MRC program is 4.00. These are considered to be satisfactory results. Therefore, we concluded that the training method for experienced groups was effective for people who want to learn more about MRC. After finishing the training program for the beginner groups, the subjects could acquire the skill needed to apply MRC to new problems, and it is thought that this training program could contribute to an increased number of MRC users.

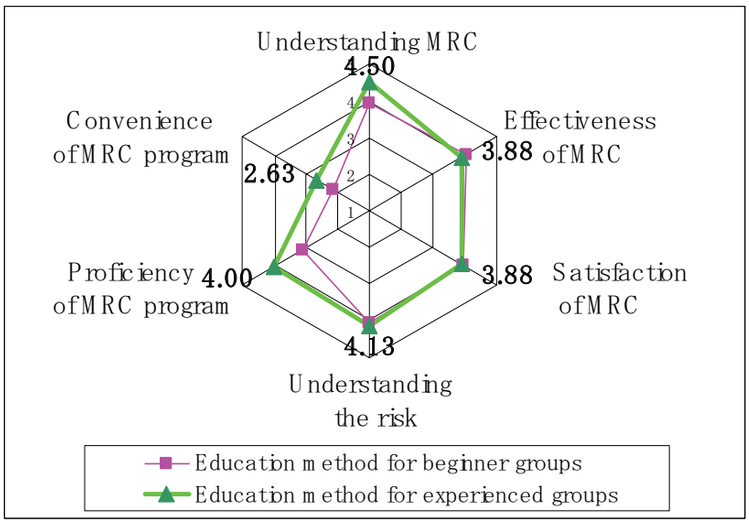

Fig. 6. Comparison of the results of the training methods for beginner and experienced groups

4.5. Evaluation of MRC

4.5.1 Evaluation of Effectiveness of MRC

The results of the questionnaire regarding the effectiveness of MRC are described in Figure 7. The results of the training program for the beginner groups include two different subject groups. According to Figure 7, many subjects evaluated MRC as effective. However, some questions arose from comments on some questionnaires and the method used to resolve these questions is described below.

(1) It was hard for the subjects to understand the degree of burden on the convenience and privacy of employees. The degree of burden, which ranges from 0 to 1, was allocated to each measure and the total of these values was set as the value of the constraint function. However, some subjects pointed out that they could not understand the indicators of the burden value. In order to resolve this issue, we will prepare burden indicators in the future.

(2) Some subjects noted that it takes a long time to analyze the risk. Even though it takes approximately 150 hours to apply MRC to a problem for the first time, we can shorten the amount of time required for the second or later analysis by using the results of the first risk analysis as a template. We will also consider shortening the time required to enter data into the MRC program by adding an import function to the program in the future.

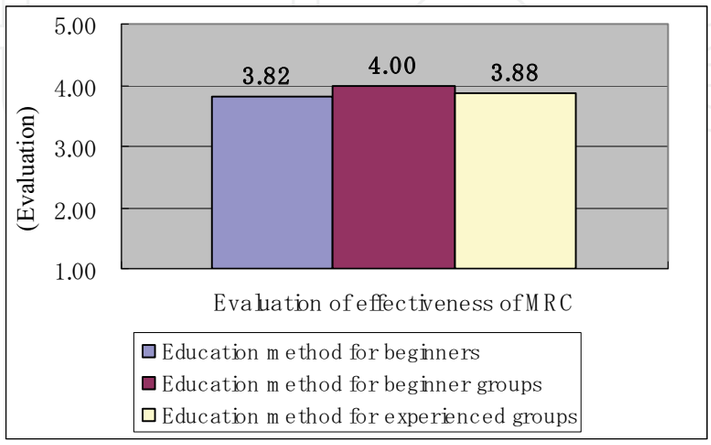

Fig. 7. Evaluation of the effectiveness of MRC

4.5.2 Evaluation of MRC Program

The result of the evaluation of the effectiveness of the MRC program is described in Figure 8. The result for beginners includes two different subject groups. According to Figure 8, the evaluation of the MRC program for experienced groups indicated that it takes a long time to finish; this result is better than the evaluation of MRC program for the beginner and beginner groups, which means the MRC program is not convenient for beginner users but is convenient for experienced users. Because it is desirable to make the MRC program convenient for beginner users, the MRC program must be improved in the future.

The result of the questionnaire regarding the inconvenience of the MRC program is described in Figure 9. We will consider increasing the convenience of the MRC program in order to improve these points. The solutions for the top three complaints are described below.

(1) It is hard and troublesome to input data into the MRC program. Especially, there are many opinions must be input on the fault tree and the measures is troublesome. Therefore, we will add a function such as importing data into the MRC program from Microsoft Excel.

(2) The user interface is not good. The window size needs to be changed because the subjects pointed out that window size is small.

(3) There are some bugs and crashes. The motivation of some subjects decreased due to these problems and these bugs must be eliminated.

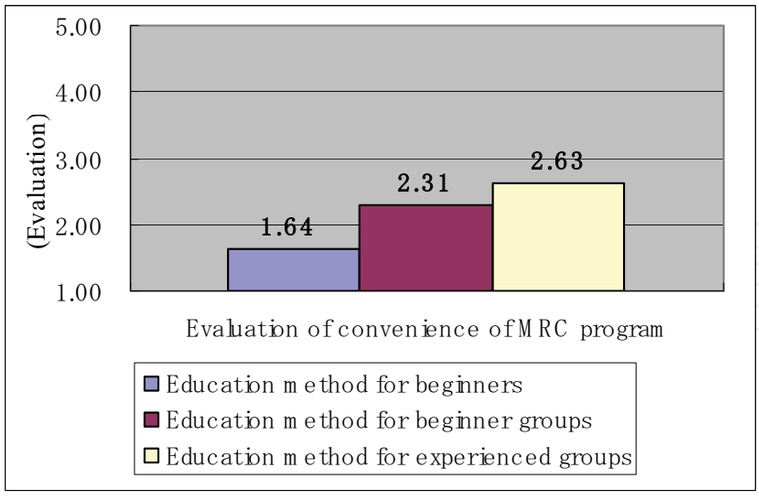

Fig. 8. Evaluation of the convenience of the MRC program

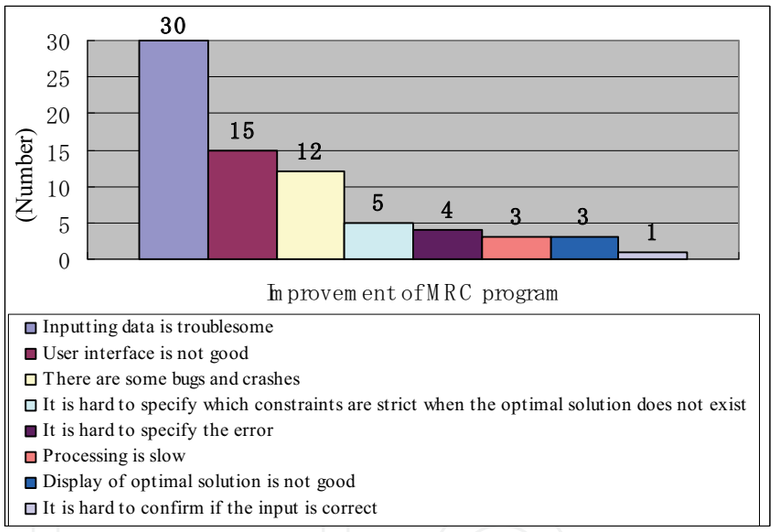

Fig. 9. Suggested improvements for the MRC program

4.5.3 Evaluation of amount of time required

The average time, the longest time, and the shortest time required for finishing all three training sessions are described in Figure 10. The results of the training program for the beginner groups include two different subject groups. The amount time required was different according to the subject and group, and depended on the accuracy of the risk analysis. The average time for the individual beginner and the beginner groups was not excessive and it is thought that people who have no previous MRC knowledge could complete this training easily. Even though the average time for the experienced groups was relatively long, people who are motivated can complete this training without problems.

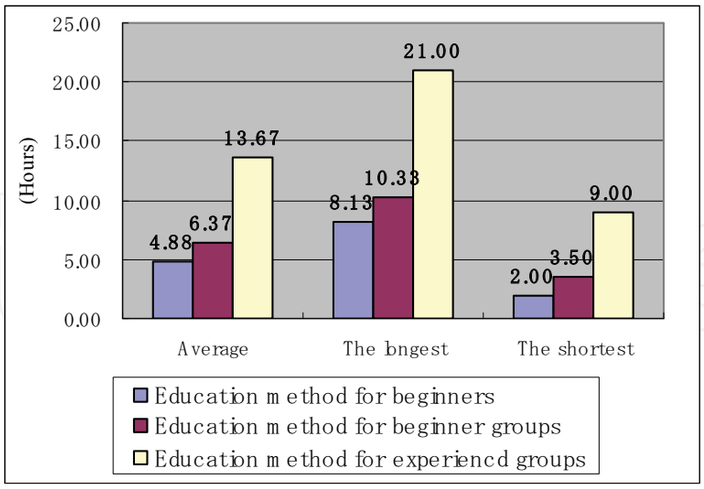

Fig. 10. Amount of time required for training

The amount of time required when we applied MRC to the information leakage problem for the first time was approximately 150 hours. The reasons why the amount of time needed for the training sessions was much shorter than our first application are described below.
(1) The amount of time was short for the individual beginner and beginner groups because the subjects used a template.
(2) The students of Tokyo Denki University and Chuo University who applied MRC to the information leakage problem as experienced groups did not have to conduct step 2, "Analyze the object," because they had already finished this step while in their beginner groups. Furthermore, the subjects could easily make fault trees, obtain parameters, and select the measures by referring to the results of the first risk analysis. Therefore, we concluded that we could shorten the amount of time required to apply MRC in the second or later analysis by using the results of the first risk analysis if the same object is to be analyzed.
(3) The students of the Institute of Information Security who applied MRC to the problem of the fabricated TV show report had a limited scope of the risk. Even though there are many reasons why the fabricated report occurred, the subjects focused on one cause for their fault tree analysis. Furthermore, parameters such as the probability of the lowest event or cost of measures were not very accurate. The amount time was short for the reasons listed above.

4.5.4 Advantage of Education of MRC

Figure 11 shows that subjects can learn more about risks such as information leakage after using the MRC program. Understanding the risk for a beginner is more difficult than for the others because it requires more time for the subjects to comprehend the background of the risk. However, the subjects are capable of learning about risks in the beginner groups during the process of deciding the value of personal information, discussing the effective measures, and filling in the blanks of the fault tree. The subjects in the experienced groups also can learn about risk during the MRC application process.
Subject comments about understanding risk are provided below:

(1) "I could learn many routes of information leakage such as from printed material, USB memory chips, or by internal and external networks after investigating the reports. As a result, I understand more about the information leakage problem."
(2) "Although I already had a basic understanding of the conflict of opinions among the chief executive officer, employees and customers before the training program, I now realize the difficulties involved in balancing the cost and employee's burden because of this training."
According to comment (1), MRC is effective for understanding the risk. In addition, according to comment (2), MRC is effective for understanding the conflicting participant opinions. It is thought that the subjects were better able to understand risk through the process of discussing parameters such as the cost of measures and the degree of burden on the convenience and privacy of employees as well as by conducting risk communication to decide an optimal combination of measures.
As noted above, MRC is considered to be effective for understanding the risk and conflict of participant opinions. We intend to consider a specific method for helping the subjects learn risk by using MRC in the future.

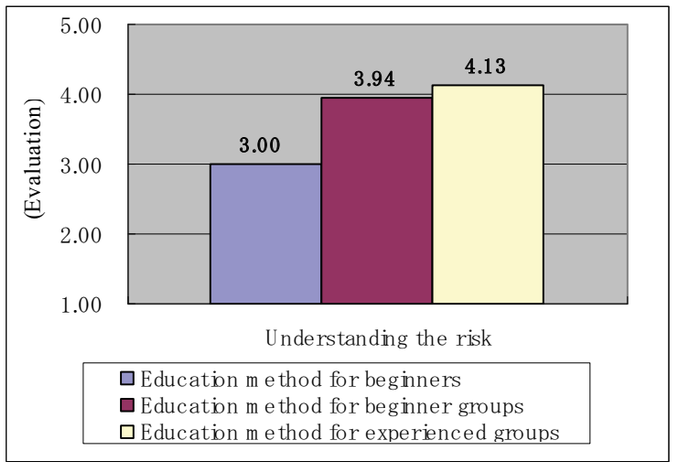

Fig. 11. Understanding the risk

5. Conclusion

MRC program version 1.0 was applied to the personal information leakage problem, and some MRC training methods were proposed in this chapter. Although the stakeholders used in the simulation were merely role players, not actual decision makers, they were able to establish consensus on a combination of measures through use of the MRC program. Thus, it can be concluded that MRC is useful for establishing consensus between decision makers in a multiple risk environment.
Moreover, people have no previous knowledge of MRC can learn MRC by participating in the training for beginner groups. The subjects were also able to apply MRC to different problems after completing this training. Therefore, it can be concluded that the training method for beginner groups contributes to an increase of MRC users. However, the following problems still need to be resolved.

(1) We do not know if the participants will be able to build consensus among them when the MRC is applied to problems greater than the information leakage problem. We will attempt to solve this problem by using MRC program version 2.0, which supports risk communication in more varied ways.
(2) In the case of applying MRC to the information leakage problem, we considered only measures that do not leak personal information. However, a crisis management plan has to be considered as well. In future work, we will consider a procedure that balances both measures by using MRC.

6. Acknowledgements

Part of the present research was sponsored by Mission Program 2, Clarification and Resolution of Vulnerabilities of an Advanced Information Society, of the Japan Science and Technology Agency's Research Institute of Science and Technology for Society.

7. References

Bruce Schneier (2003). *Beyond Fear*, Springer

Hiroshi Yajima, Tomohiro Watanabe, Ryoichi Sasaki (2007). Evaluation of the Participant-Support Method for Information Acquisition in the "Multiplex Risk Communicator", Proceedings of 12th International Conference on Human-Computer Interaction, pp. 195-203, China, July 2007, Springer

Japanese Standards Association (2001). Information technology -- Guidelines for the management of IT Security -- Part 3: Techniques for the management of IT Security, Japan

Japan Network Security Association (2003). Fiscal 2003 Information Security Incident Survey Report, http://www.jnsa.org/houkoku2003/incident_survey1_e.pdf, Japan

Japan Network Security Association (2004), 2004 Information Security Incident Survey Report, http://www.jnsa.org/houkoku2004/incident_survey_en.pdf, Japan

Japan Network Security Association (2005), 2005 Information Security Incident Survey Report, http://www.jnsa.org/result/2005/20060803_pol01/2005incidentsurvey_060731en.pdf, Japan

Japan Network Security Association (2006), 2006 Information Security Incident Survey Report, http://www.jnsa.org/result/2006/pol/insident/070720/2006incidentsurvey-e_080403.pdf, Japan

Mitsuhiro Taniyama, Yuu Hidaka, Masato Arai, Satoshi Kai, Hiromi Igawa, Hiroshi Yajima and Ryoichi Sasaki (2008). Application of "Multiple Risk Communicator" to the Personal Information Leakage Problem, Proceedings of world academy of science, engineering and technology, pp. 285-290, France, November 2008

N.J. McCormick (1981). Reliability and Risk Analysis: Methods and Nuclear Power Applications, *Academic Press*, New York

R.S. Garfinkel et al (1972). Integer Programming, *Wiley and Sons*

Ryoichi Sasaki, Saneyuki Ishii, Yuu Hidaka, Hiroshi Yajima, Hiroshi Yoshiura, Yuuko Murayama (2005). Development Concept for and Trial Application of a "Multiplex Risk Communicator, Proceedings of IFIP International Conference on eBusiness, eCommerce and eGovernment, Poland, October 2005, Springer

Ryoichi Sasaki, Yuu Hidaka, Takashi Moriya, Mitsuhiro Taniyama, Hiroshi Yajima, Kiyomi Yaegashi, Yasumasa Kawashima, Hiroshi Yoshiura (2008). Development and applications of a Multiple Risk Coomunicator, Proceedings of Risk Analysis 2008, pp.241-249, Greece, May 2008, WITPESS

Recent Advances in Technologies

Edited by Maurizio A Strangio

ISBN 978-953-307-017-9

Hard cover, 636 pages

Publisher InTech

Published online 01, November, 2009

Published in print edition November, 2009

The techniques of computer modelling and simulation are increasingly important in many fields of science since they allow quantitative examination and evaluation of the most complex hypothesis. Furthermore, by taking advantage of the enormous amount of computational resources available on modern computers scientists are able to suggest scenarios and results that are more significant than ever. This book brings together recent work describing novel and advanced modelling and analysis techniques applied to many different research areas.

InTech Europe

University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China

Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen