Development and applications of a multiple risk communicator

R. Sasaki[1,2], Y. Hidaka[3], T. Moriya[1], M. Taniyama[1], H. Yajima[1,2], K. Yaegashi[4], Y. Kawashima[5] & H. Yoshiura[2,6]
[1]*Tokyo Denki University, Tokyo, Japan*
[2]*RISTEX of the Japan Science and Technology Agency, Tokyo, Japan*
[3]*IT DORAKU RESEARCH LAB. Ltd, Tokyo, Japan*
[4]*Pinpoint Service, Inc, Tokyo, Japan*
[5]*AdIn Research, Inc, Tokyo, Japan*
[6]*University of Electro-Communications, Tokyo, Japan*

Abstract

Businesses and society face various risks, and measures to reduce one risk often cause another risk. Thus, obtaining the optimal combination of measures to reduce one risk while considering other risks has become a major issue. Because risk decisions involve multiple participants, such as a manager, customer, and employee, communication between all decision makers is important for reaching an agreement on the necessary risk measures. Moreover, due to opposing factors such as security, privacy, and development cost, it is not always easy to find the optimal combination of measures that reduce the risk and are agreeable to all decision makers. Therefore, this situation would benefit from the development of a "multiple risk communicator" (MRC) with the following functions: (1) a model of the support role of the risk specialist, (2) an optimization engine, and (3) a display of the computed results for viewing by the decision makers. In this paper, we propose a design for developing the MRC program and present an example implementation. Then, we apply the results to problems of personal information leakage, illegal copying, and internal control.

Keywords: security, privacy, risk, risk communication, discrete optimization.

WIT Transactions on Information and Communication, Vol 39, © 2008 WIT Press
www.witpress.com, ISSN 1743-3517 (on-line)
doi:10.2495/RISK080251

1 Introduction

Businesses and society face various risks, and measures to reduce one risk (e.g., security risk) often cause another risk (e.g., privacy risk). It has become clear that multiple risks, or one risk versus another risk, are a major issue, and it is important to obtain the optimal combination of measures to reduce some risks with consideration of other risks. Therefore, the people directly and indirectly concerned with risks are exchanging ideas, and consequently there has been a growing interest regarding risk communication and the process of reaching a consensus [5, 6].

However, due to factors that oppose each other, such as security, privacy, and development cost, it is not always easy to find the optimal combination of measures that reduce risk and lead to an agreement among the decision makers.

To avoid this difficulty, we proposed the development of a "Multiple Risk Communicator" (MRC) with the following functions: (1) a model of the support role of the specialist, (2) an optimization engine, and (3) a display of the computed result for viewing by the people making risk decisions [1]. After conducting a literature survey, we concluded that a system having the above functions has not been proposed and implemented for risk communications.

This paper describes the requirements for the MRC, the structure of the proposed MRC program, an example implementation of the MRC, and the results of applying the MRC to problems of personal information leakage, illegal copying, and internal control.

2 Requirements and development of the MRC program

The MRC program was developed to satisfy the following conditions.

Requirement 1: There are various conflicting risks, and measures to reduce one or more must consider all risks.

Requirement 2: Various measures are required for individual risks as well. Resolving every problem with one measure is not possible, and features to determine the most appropriate combination of numerous measures are essential.

Requirement 3: For decision making, the numerous individuals involved (e.g., managers, citizens, customers, and employees) should be satisfied. Therefore, features to support risk communication among these individuals are essential.

An overview of the MRC program to satisfy these requirements is shown in Fig. 1.

The basic feature satisfying Requirement 1 and Requirement 2 is the Optimization Engine, which is (3) in Fig. 1. Here, a discrete optimization problem with various measures proposed as 0-1 variables (or a 0-1 programming problem) is used. In the optimization engine, a brute force method and lexicographic enumeration method are used to obtain the solution [3]. To formulate the discrete optimization problem easily, the Assistant Tool for Specialists (1) is used for specialists with the functions of analysis, formulation and parameter setting. For the risk analysis, the fault tree analysis method [4] is supported in this tool.

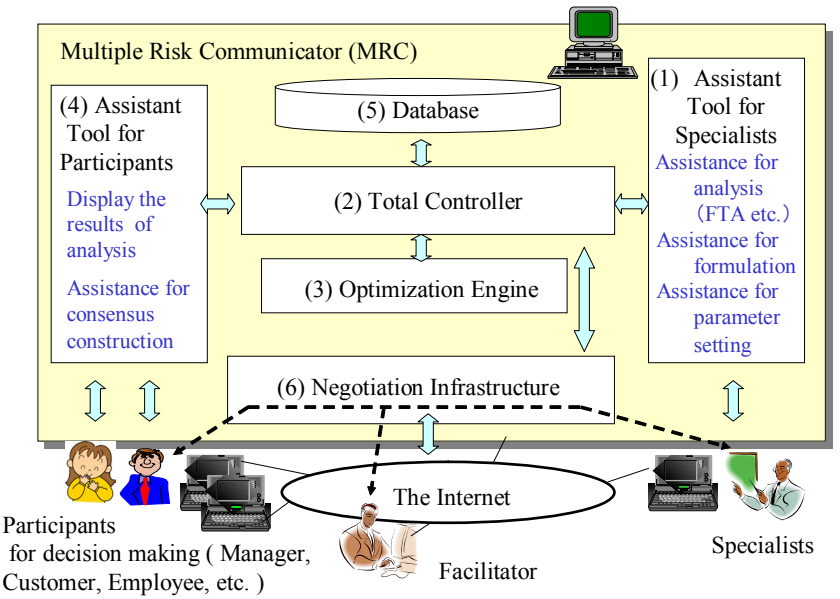

Figure 1: Overview of the MRC.

In addition, the Assistant Tool for Participants (4) satisfies Requirement 3 for decision making. The optimal combinations of measures obtained from the Optimization Engine (3) enable decisions that can be easily made by the individuals involved. Opinions such as "Add the measure we propose" and "We propose to change the value of the constraint" are sent to the specialist via the Negotiation Infrastructure (6). Then, the facilitator supports the communication between the participants and the specialist.

Moreover, the Total Controller (2) and Database (5) link the processing of these components.

The MRC program was implemented using Java and PHP 5.2 in a Windows XP environment. The total number of coding steps was about 10,000. Apache 2.24 was 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 was used to deal with the numerical formula in the PC for the specialist.

3 Using the MRC

The process of the MRC application is shown in Fig. 2. We explain the process using an example, "the problem of leakage of personal information of customers from a service provider."

First of all, the object to be solved is decided. In this example, we assume it is the leakage problem just stated.

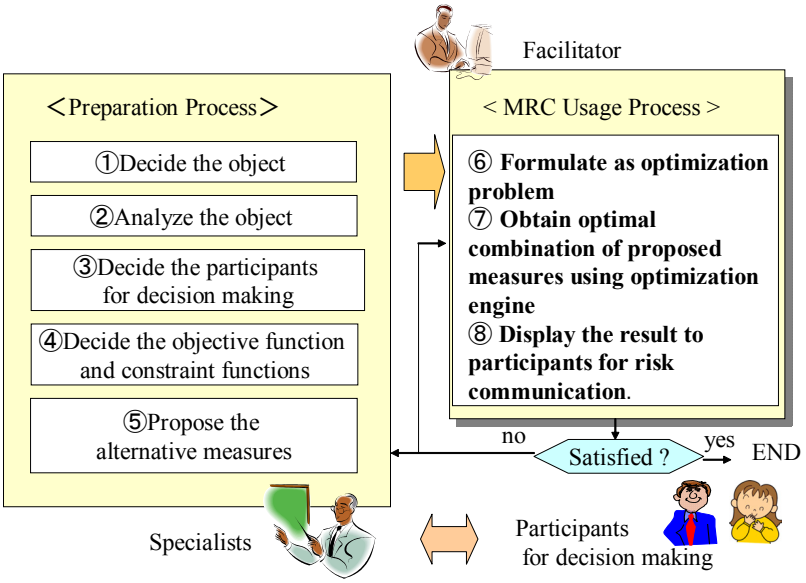

Figure 2: The MRC application process.

Secondly, the object is analyzed. For simplicity, we are the specialists; therefore, we analyze the leakage problems of personal information that can exist and estimate the probability using a fault tree analysis and/or event tree analysis [4].

Thirdly, the participants for decision making are decided. In this case, we selected the business manager, employees, and customers of the service provider. The reason for adding the employees is that measures to reduce the personal leakage risk are apt to violate the privacy of the employees, so they should have an opportunity to input their opinions to the MRC.

Fourth, the objective function and constraints are decided for formulating the discrete optimization problem. We consider minimization of the social total cost as an objective function, and so the requirements for each participant should be selected as constraint functions. In this example, we set the constraint functions as follows:

(a) probability of leakage of personal information (for customers)
(b) cost of measures (for business manager)
(c) effect on privacy of employees (for employees)
(d) effect on convenience of employees (for employees).

Fifth, alternative measures are proposed and the values of the related parameters are estimated. In this example, the data in Table 1 is given. The i-th alternative measure is expressed as a 0-1 variable, X_i. Here, when $X_i=1$, the i-th measure is adopted; otherwise, it is not adopted.

The following parameters are used for the calculations.

$\Delta P\alpha_{1i}$: Decreased probability caused by i-th measure against the attack by employees permitted to enter isolated areas.

Table 1: List of proposed measures and values of parameters.

Proposed measures	Internal-1: $\Delta P_{\alpha 1i}$	Internal-2: $\Delta P_{\alpha 2i}$	External $\Delta P_{\beta i}$	Cost:Ci (M yen)	Privacy burden : $D_1 i$	Convenience burden : $D_2 i$
1:e-mail automatic monitoring	0.8	0.8	0.8	3.9	0.6	0
2:e-mail manual monitoring	0.95	0.95	0.95	30	1	0
3:firewall	0.9	0.9	0.9	0.75	0	0.4
4:IDS (intrusion detection system)	----	0.7	0.7	1.3	0	0
5: Vulnerability management	----	0.8	0.9	0.3	0	0.2
6:Prohibition of storing data in external memory	0.9	0.9	0.9	2.5	0	0.7
7:Entering and leaving management system	----	0.8	0.9	8	0.1	0.4
8: Check on belongings in the isolated area	0.8	0.8	0.9	30	0.8	0.6

$\Delta P\alpha_{2i}$: Decreased probability caused by i-th measure against the attack by employees not permitted to enter isolated areas.

$\Delta P\beta_i$: Decreased probability caused by i-th measure against the attack by external third parties who are not employees.

C_i: cost of i-th measure.

D_{1i}: privacy burden on employees produced by implementing i-th measure.

D_{2i}: convenience burden on employees produced by implementing i-th measure.

The degree of burden is a relative value indicated from 0 to 1 points and is obtained from the employees' responses to questionnaires.

Sixth, the data obtained in the above process becomes the input into the MRC program for formulation as a discrete optimization problem.

To obtain the expression for the probability of personal information leakage, a fault tree is constructed using parameters such as $\Delta P\alpha_{1i}$ and the 0-1 variable, X_i. From the fault tree, the expression including variables described below is derived automatically in the MRC program.

$$P_{\alpha_1} = P_a \left\{ \begin{array}{l} P_b\left(1-\Delta P_{\alpha_1 8} X_8\right)\left(1-P_{\alpha_1 6} X_6\right)+ \\ P_c\left(1-\Delta P_{\alpha_1 1} X_1\right)\left(1-\Delta P_{\alpha_1 2} X_2\right)+P_d\left(1-\Delta P_{\alpha_1 3} X_3\right) \end{array} \right\}$$

Seventh, the optimal combination of alternative measures can be obtained with the optimization engine in the MRC.

Eighth, the obtained optimal solution is displayed to the participants so they can easily carry out the decision making [2]. The MRC program has the capability to

obtain 1 to 100 optimal solutions. Figure 4 shows the displays available to the decision-making participants.

The opinions of the participants are sent to the specialist via the negotiation infrastructure. A facilitator supports the communication between the participants and specialist. By continuing these processes, a solution acceptable to the decision-making participants can almost certainly be obtained.

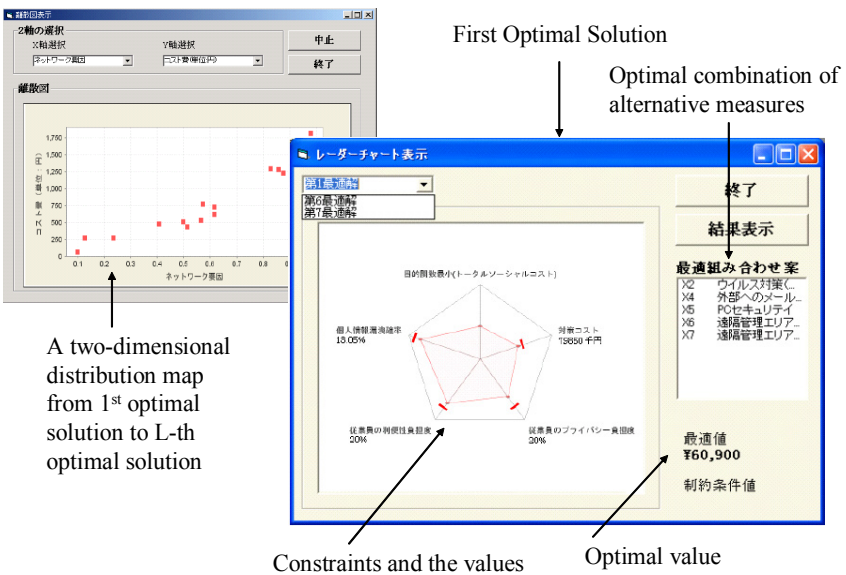

Figure 3: Example of the optimal solutions given by the MRC.

4 Applications of the MRC

4.1 Examples of the application

The MRC was applied to personal information leakage problems, illegal copying problems, internal control problems and compromising public key cipher issues. For personal information leakage problems, the MRC was applied five times and agreement of the participants was obtained four times, although this included risk communication by the people playing the role of decision makers.

When the MRC was applied to personal information leakage problems at junior high schools in Setagaya-ku, Tokyo, an agreement of an acceptable solution was obtained between the real manager in the Setagaya-ku government office, the information system person in charge of the Board of Education, and a representative of the teachers in the junior high school. In this case, the number of alternative measures was 13, the objective function was minimization of the total

social cost, and the constraints were the probability of leakage of personal information, cost of measures and convenience burden on teachers. Agreement of the decision-making people was obtained after three times meeting and showed 12 optimal solutions. The Setagaya-ku government office is preparing to implement the measures of the optimal solution that were agreed upon.

4.2 Computational time to obtain optimal solutions

Because the computation time using the MRC program to obtain each optimal solution for all cases described in Section 4.1 did not exceed 2 minutes, this program can be applied to many real situations.

The computation time using the brute force method and lexicographical enumeration method when changing the number of variables (i.e., changing the number of alternative measures) is listed in Table 2. If the number of variables is equal to or less than 15, the optimal solution can be obtained within a reasonable computation time.

Table 2: Measured computation time.

Number of Valuables / Method	5	10	15	20
(1) Brute Force Method (Sec)	0.1	4.3	151.5	1445.6
(2) Lexicographic Enumeration Method (Sec)	0.1	3.5	34.6	1125.9
(2) / (1)	1.0	0.81	0.23	0.21

4.3 Evaluation of the MRC based on the results

Based on the above applications and study results, the following statements regarding the MRC can be made.

(1) The MRC can be useful for obtaining agreement of decision-making people in a multiple risks environment.

(2) By using the MRC program on a PC, it is possible to access the MRC function and perform the risk communication, if the PC can connect to the Internet. If the number of variables is equal to or less than 15, an optimal solution can be obtained within a reasonable computation time; therefore, the MRC can be applied to many real problems. However, in order to increase the number of variables processed within a reasonable time, we would like to develop fast approximate algorithms.

(3) Individuals who used the MRC offered the opinion that features to obtain not just the first optimal solution but also the L-th optimal solution would be preferable since solutions could be selected from the first to the L-th optimum with consideration of the factors that could not be formulated.

(4) It was very difficult to give a specific value to the constraint in the MRC. However, it was not difficult to specify a ratio comparing a value, such as a known measured value, before performing the computations. Therefore, we added the capability of asking for the value of the ratio.

(5) During the first attempt, the specialist needed approximately 2–3 months, for example, to formulate the problem, but the time period was shortened when the specialist applied the MRC to a similar problem. Thus, it is an effective strategy to apply the MRC to a set of similar problems whenever possible.

(6) When the multiple decision makers strongly believe in his or her opinions, it could be difficult to assign the value of a parameter and obtain agreement of the decision makers. For the solution to this problem, we are examining the reinforcement of the participant support function by the introduction of a utility function [2] and will add this function to version 2 of the MRC program.

5 Conclusion

In this paper, after presenting a design to develop the MRC program, we showed an implementation of the program and the results of personal information leakage problems, illegal copying problems, and internal control problems. As a result, the MRC can be useful for obtaining agreement of decision-making people in a multiple risks environment.

In future work, we will increase the number of applications of the MRC, and improve the functions of the MRC program.

Acknowledgements

The current research is sponsored by Mission Program II, 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.

The authors wish to thank several individuals, especially Professor Norihisa Doi of Chuo University, for their valued opinions.

References

[1] Ryoichi Sasaki, Saneyuki Ishii, Yuu Hidaka, Hiroshi Yajima, Hiroshi Yoshiura, Yuuko Murayama, " Development Concept for and trial application of a "multiplex risk communicator", IFIP I3E2005, Springer

[2] Hiroshi Yajima、Tomohiro Watanabe、 Ryoichi Sasaki "Evaluation of the Participant-Support Method for Information Acquisition in the "Multiplex Risk Communicator"12th International Conference on Human-Computer Interaction 2007

[3] R.S. Garfinkel et al.: Integer Programming, Wiley and Sons, 1972
[4] N.J. McCormick: Reliability and Risk Analysis, Academic Press Inc., 1981
[5] J. Ross: The Polar Bear Strategy, Preceus Books Publishing, 1999
[6] http://www.riskworld.com/books/topics/riskcomm.htm