DEVELOPMENT CONCEPT FOR AND TRIAL APPLICATION OF A “MULUTIPLEX RISK COMMUNICATOR”

Ryoichi Sasaki*&, Saneyuki Ishii*,Yuu Hidaka*,Hiroshi Yajima*, Hiroshi Yoshiura+, Yuuko Murayama#
**Tokyo Denki University 2-2 Kandanishiki-cho Chiyoda-ku Tokyo, sasaki@im.dendai.ac.jp Tel: +81-3-5280-3328 Fax: +81-3-5280-3592 + University of Electro-Communications, # Iwate Prefectual Univaersity, & Researcher at RISTEX of the Japan Science andTechnology Agency*

Abstract: Risk has increased with the development of an Internet-oriented society, and to what extent that risk can be reduced has become a major issue. Thus, risk communication has become crucial for the formation of a consensus among decision-makers such as citizens. Dealing with risk, however, requires the reduction of risks based on conflicting concepts such as security, privacy, and development costs; obtaining the consensus of individuals involved and determining optimal combinations of the measures are not easy. A ”multiplex risk communicator (MRC)” with (1) a simulator, (2) an optimization engine, and (3) displays for the formation of a consensus is needed in order to resolve such problems. This paper describes the features an MRC should have, a simple prototype program to support it, and results of its trial application.

Key words: security, privacy, risk, risk communication, discrete optimization

1. INTRODUCTION

Due to damage such as that from distributed denial of service (DDoS) attacks and various worms, interest with respect to security measures has heightened. In addition, circumstances have also called for greater interest in privacy measures such as those for personal information protection.

Many people assume that security measures are privacy measures. However, security measures and privacy measures are as clarified, (1) compatible or (2) conflicting[1]. Instances when they conflict in particular require the study of a combination of the most appropriate measures for security and privacy including cost and ease of use.

Recently, on the other hand, opinions regarding risk have been exchanged among people directly and indirectly involved, and interest regarding risk communication, the process of reaching a consensus, has also heightened[2)-6)].

In the past, risk was considered to be a single item, but in the above examples there is a risk of losing security and a risk of losing privacy. In addition, there are instances where ease of use is seen as an operational risk and development costs are seen as an economic risk. Thus, we must deal with multiple risks. Therefore, risk communication also requires being able to reach a consensus regarding the optimal combination of measures while considering multiple risks.

To achieve the above objectives, the development concepts of a multiplex risk communicator (denoted hereafter as MRC) were established. This paper describes the features an MRC should have, a simple prototype program to support it, and results of its trial application[7]

2. CONFLICTING RISKS AND NEED FOR AN MRC

Depicting the relationship between security and privacy with concepts, means, and technologies will yield a diagram like that shown in **Fig. 1**[1].

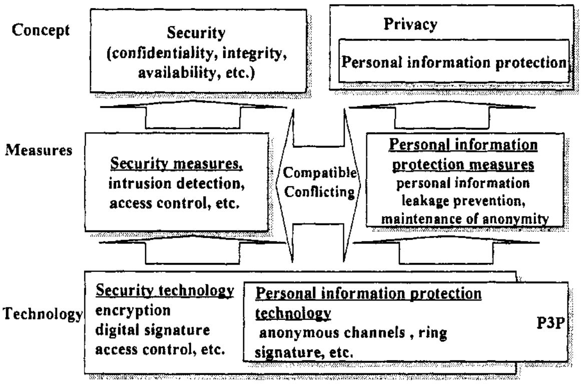

Concept
Security
(confidentiality, integrity, availability, etc.)
Privacy
Personal information protection
Measures
Security measures,
intrusion detection, access control, etc.
Compatible
Conflicting
Personal information protection measures
personal information leakage prevention, maintenance of anonymity
Technology
Security technology
encryption
digital signature
access control, etc.
Personal information protection technology
anonymous channels , ring signature, etc.
P3P

Figure 1. [Security and Privacy]

The relationship between security and privacy measures can roughly be classified into (1) compatible and (2) conflicting measures as follows.

An explanation of each has been provided below.

(1) Compatible: With measures to prevent the leakage of personal information, enacting security measures such as access control and data encryption is normally linked to protection of personal information. In this case, security measures are privacy measures.

(2) Conflicting: This is an instance where the implementation of security measures complicates the protection of personal information and was seldom examined in the past. As an example, (a) use of a public key certificate for a digital signature and encryption as a security measure has been linked to the outflow of personal information in the form of the address and date of birth written in the certificate. In addition, (b) permitting encrypted e-mail as a security measure against threats from a third party may also lead to the inability to monitor the outflow of personal information.

When there are multiple risks, i.e., a loss of security and a loss of privacy, technology as shown in **Fig. 2** can contribute significantly to resolving the conflict between these risks.

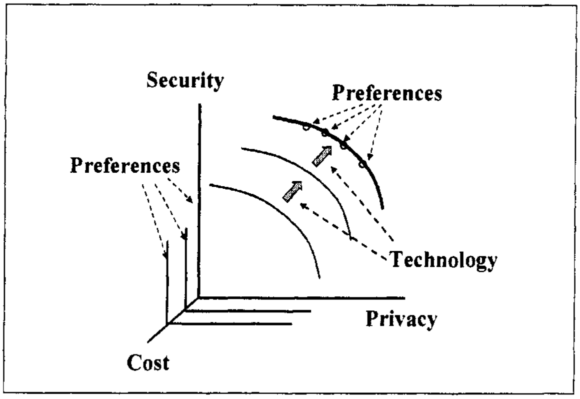


Figure 2. [Image of method to solve opposing concept]

As an example, if the leakage of personal information was caused by a public key certificate and privacy was to become a problem, then security and privacy can both be provided by handing over an attribute certificate that only describes attributes. As expected, however, security and usability will suffer compared to when a public key certificate is used. Therefore, whether emphasis is placed on indices such as security, privacy, or cost will become a problem in terms of selection by decision-makers.

Thus, tools are essential to obtaining and determining the consensus of decision-makers on an optimal combination of the measures for security and privacy including cost and ease of use.

3. DELOPMENT CENCEPT FOR THE MRC

3.1 Requirements of the MRC

Based on reasons like those above, an MRC will be developed, but it must satisfy conditions like:

(Requirement 1) There are various conflicting risks, and measures must be considered while taking them into account.

(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, numerous individuals involved (e.g. managers, citizens, customers, and employees) should be satisfied. Therefore, features to support risk communication among numerous individuals involved are essential.

3.2 Concept of the MRC

A structure like that shown in **Fig. 3** was developed as an MRC to satisfy those requirements.

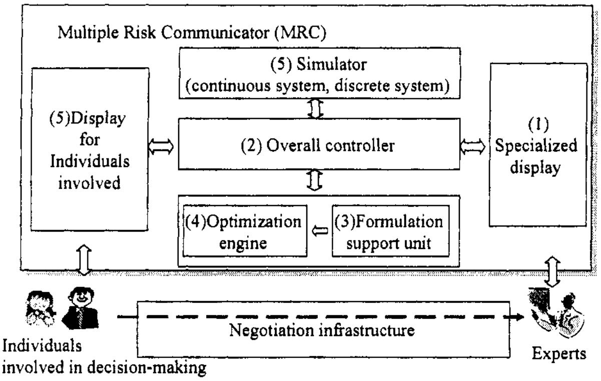

Multiple Risk Communicator (MRC)
(5) Simulator
(continuous system, discrete system)
(5)Display for Individuals involved
(2) Overall controller
(1) Specialized display
(4)Optimization engine
(3)Formulation support unit
Negotiation infrastructure
Individuals involved in decision-making
Experts

Figure 3. [Overview of Multiple Risk Communicator]

The MRC consists of the following 6 components:

(1) Specialized display
(2) Overall controller
(3) Formulation support unit
(4) Optimization engine
(5) Simulator
(6) Display for individuals involved

What provides the basic features to satisfy Requirement 1 and Requirement 2 are the (3) formulation support unit and (4) optimization engine. Here, a discrete optimization problem with various measures proposed as 0-1 variables (or a 0-1 programming problem)[9] is used for its formulation and obtaining its solution.

In addition, what satisfies Requirement 3 are the (1) specialized display, (5) simulator, and (6) display for individuals involved. The setup must be such that simulations are performed, results of measures are displayed in detail, and displays allow decisions to be easily made by experts and individuals involved.

In addition, what links the processing of these components is the (2) overall controller.

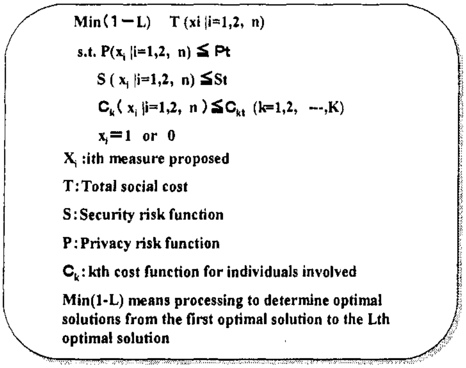
3.3 Envisioned usage of the MRC

(Step①) Experts furnish the MRC with the (a) objective function, (b) constraint function, (c) proposed measures, (d) coefficients, and (e) constraint values and formulate an optimization problem (using the (1) specialized display, (2) overall controller, and (3)formulation support unit).

Here, formulation of an optimization problem with various measures proposed as 0-1 variables is assumed. The reason for such a method is because formulation is easiest when determining the optimal combination of individual measures proposed.

Specific formulations differ depending on the target, but methods such as minimizing total social cost or maximizing total social benefit under risk constraints regarding cost, privacy, and security as shown in Fig. 4, for example, are acceptable.

In addition, the problem is formulated here so as not to determine only the first optimal solution but to determine the second, third, · · the Lth optimal solutions as well. This is because, given factors that cannot possibly be quantified, it allows individuals involved to choose a satisfactory solution from the first to the Lth optimal solutions.



Min(1 − L) T (xi |i=1,2, n)

s.t. $P(x_i \mid i=1,2,\ n) \leqq Pt$

$S(x_i \mid i=1,2,\ n) \leqq St$

$C_k(x_i \mid i=1,2,\ n) \leqq C_{kt}$ (k=1,2, ---,K)

$x_i = 1$ or 0

X_i :ith measure proposed

T:Total social cost

S:Security risk function

P:Privacy risk function

C_k:kth cost function for individuals involved

Min(1-L) means processing to determine optimal solutions from the first optimal solution to the Lth optimal solution

Figure 4. [Image of Formulated Result]

After a cost model was created and the cost of individual measures proposed was determined, the constraint equation regarding cost can be described by the following expression:

$$\sum_{i=1}^{n} C_i X_i \leqq C_t \text{ ——— Eq. 1}$$

Here, Ci represents the cost of proposed measure i and Ct represents the constraint value of the total cost. In addition, Xi is a 0-1 variable; 1 represents adopting the proposed measure i and 0 represents not adopting it.

In addition, the security risk function and privacy risk function can, after individual proposed measures have been determined using fault tree analysis[8)] or the like, be expressed as functions.

(Step②) The first-the Lth optimal combinations of proposed measures are determined using the (4) optimization engine (e.g.: a combination of proposed measures 1 and 3 is the first optimal solution, a combination of 1 and 4 is the second optimal solution, and so forth)

Here, the (4) optimization engine is the component that provides features to effectively determine the optimal solution for the formulated problem using the following techniques[9)]:

(a) Exact method

Brute Force method: for when there is a small number of proposed measures

Effective method: for when there is a relatively large number of proposed measures. This method effectively searches for a solution by skipping instances where an optimal solution is clearly not possible in the process of searching for solutions based on the method of all possible combinations. The lexicographic enumeration method or the branch and bound method can be used.

(c) Approximate method: for when there is a large number of proposed measures. This method does not guarantee an optimal solution but it effectively determines approximate solutions without being limited to optimal solutions.

All of these methods were developed in the past to determine only the first optimal solution but with a little modification they can be used to determine the first-the Lth optimal solution.

(Step③) The results are displayed in an easy-to-understand format using the (5) simulator and (6) display for individuals involved.

After the optimal solution is determined, the simulator is used to predict the results of measures in detail and to display effects after the passage of time and regional changes for decision-makers.

There are plans to develop a program based on system dynamics[10)], which is considered to be the easiest methodology to use to perform such simulations.

The (6) display for individuals involved expresses information required to reach a consensus by decision-makers such as citizens and employees in an easy-to-understand format. Here, modifications are needed for (a) display details and display order to derive a satisfactory solution for each individual involved and for (b) a display order so consensus among individuals involved is easily reached.

(Step④) Opinions such as "constraint values are different" and other proposed measures should be considered" were voiced by individuals involved.

(Step⑤) The results were, using a negotiation infrastructure (with a tool for information exchange between two individuals as the base), conveyed to experts. Input modified by experts is furnished to the MRC and the results are displayed again.

Multiple risks are considered and opinions of multiple individuals involved are incorporated by repeating the above process, with increasing possibility that a mutually satisfactory solution will be reached.

3.4 Issues to be resolved

Application of the MRC to actual situations requires resolution of the following issues:

(1) For experts

(1-a) difficulty of formulation

(1-b) uncertainty of effects

(2) For decision-makers (average citizens)

(2-a) constraint ambiguity

(2-b) consideration of unquantified factors

(2-c) method of quickly reaching a solution that satisfies an individual involved

(2-d) resolution of disagreement between groups in terms of solutions

These are all difficult issues. However, they are major issues and must be resolved step by step through trial application.

4. TRIAL APPLICATION AND DISCUSSION

4.1 Targets

There are, with regard to the MRC, few similar approaches, so the approach used was not to create a tidy program from scratch but to create a simple prototype program, apply it to multiple targets, improve the system itself, and create the next prototype program. First of all, we developed very simple prototype program based on the Excel.

The order of MRC application is as shown in Fig. 5; application was done by junior researchers. Here, preparations beforehand were preparatory work for formulation in an MRC as described in Step① of Sec. 3.3.

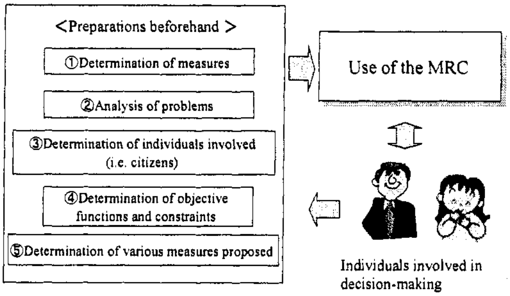

<Preparations beforehand >
①Determination of measures
②Analysis of problems
③Determination of individuals involved (i.e. citizens)
④Determination of objective functions and constraints
⑤Determination of various measures proposed
Use of the MRC
Individuals involved in decision-making

Figure 5. [Application of MRC to Personal Information Leakage Measures]

Here, "the problem of leakage of personal information" is dealt with, and application was done (corresponding to ① and ② in Fig. 5) with the following assumptions:

(1) Personal information from the firm possesses amounts to one million entries.

(2) The value of personal information is 10,000 yen per entry. In addition, when personal information is actually leaked the company pays compensation of 500 yen to each customer it has.

With regard to (4) personal information, there are three patterns of leakage of personal information via (a) internal crime 1 (employees let into segregated areas), (b) internal crime 2 (employees not let into segregated areas), and (c) external crime (an external third party that is not an employee and who is outside the corporate structure). The pattern of leakage caused by internal crime 1 (employees let into segregated areas) is shown in Figs. 6.

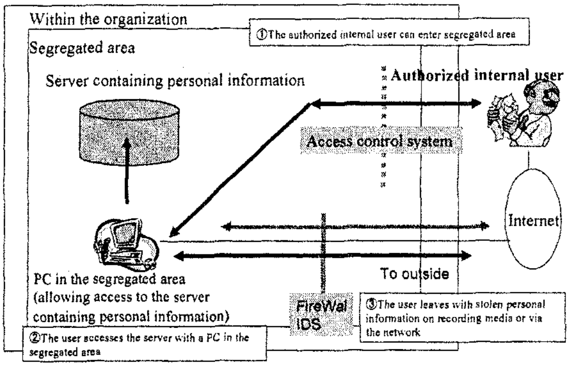

Within the organization
①The authorized internal user can enter segregated area
Segregated area
Server containing personal information
Authorized internal user
Access control system
Internet
To outside
PC in the segregated area
(allowing access to the server
containing personal information)
FireWal
IDS
③The user leaves with stolen personal information on recording media or via the network
②The user accesses the server with a PC in the segregated area

Figure 6. [Behavior Pattern of Internal Unjust Person(Type1)]

(5) Next, the risks for individuals involved when handling personal information are considered. The management risk that arises when handling personal information can be roughly classified into the following three types:

(a) First risk: risk of damage

First off is the risk of damage when personal information is leaked

(b) Second risk: cost of security measures

The cost of security measures to prevent the outflow of personal information must also be considered as a management risk when handling personal information.

(c) Third risk: burden on employees

The burden on employees produced by implementing measures must also be considered as a management risk from the perspective of work efficiency. The two types of burdens are as follows:

(a) Burden on privacy for employees accompanying measures

E-mail monitoring to prevent the leakage of personal information, for example, will lead to employee privacy not being protected and will place a burden on employees.

(b) Decline in employee convenience accompanying measures

4.2 Methods of application

In accordance with Fig. 5, application was done as indicated below. The ③ individuals involved were (1) business manager, (2) the firm's employees, and (3) customers.

The ④objective function and results of constraint determination were as follows:

objective function: the sum of the risk of leakage of personal information and cost of measures satisfies constraints and is the smallest to next-to-smallest value.

Constraints:

(a) probability of leakage of personal information

(b) cost of measures

(c) burden on privacy for employees

(d) burden on convenience for employees

The proposed measures were listed up in Table 1 . In addition, values for costs for each of the proposed measures here were studied by individuals applying the MRC in consult with individuals involved, resulting in values shown in Table 1. The degree of a burden is a relative value indicated from 0 to 1 points and should use results of employee surveys.

Proposed measures	$\Delta P_{\alpha 1i}$ (Inside)	$\Delta P_{\alpha 2i}$ (Inside)	$\Delta P_{\beta i}$ (External)	Cost:Ci (M yen)	D_1i	D_2i
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	13	0	0
5: Vulnerability management	----	0.8	0.9	3.0	0	0.2
6:Prohibition of storing data in external memory	0.9	0.9	0.9	25	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

Table 1. [List of Proposal measures]

Here is an explanation of the meaning of parameters in Table 1. Respective parameters depicted here are used for calculation of the subsequent probability of leakage, costs of measures, etc.

$\Delta P \alpha_1 i$: effects of measures on employees let into segregated areas.

$\Delta P \alpha_2 i$: effects of measures on employees not let into segregated areas.

$\Delta P \beta$ i: effects of measures on external third parties who are not employees.

Cost Ci: cost of measures.

employee burden D_1i: privacy burden on employees produced by implementing measures. employee burden D_2i: convenience burden on employees produced by implementing measures.

A case where information leakage is caused by unauthorized internal users 1 is expressed using a fault tree[8] and is as shown in Fig. 7.

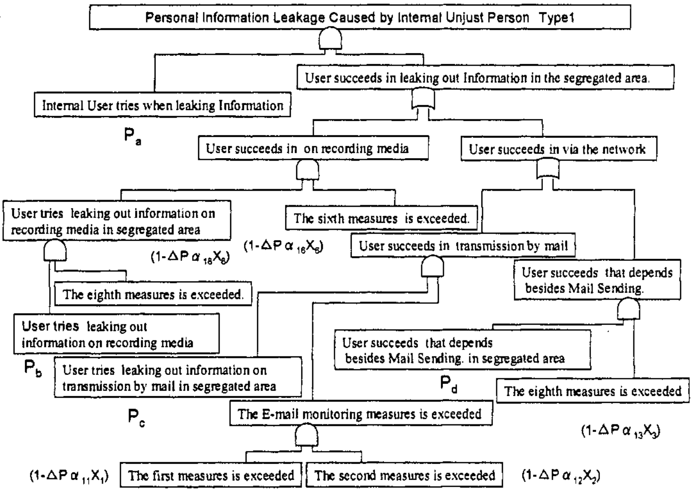

Personal Information Leakage Caused by Internal Unjust Person Type1
User succeeds in leaking out Information in the segregated area.
Internal User tries when leaking Information
Pa
User succeeds in on recording media
User succeeds in via the network
User tries leaking out information on recording media in segregated area
The sixth measures is exceeded.
(1-ΔPα16X6)
(1-ΔPα18X8)
User succeeds in transmission by mail
User succeeds that depends besides Mail Sending.
The eighth measures is exceeded.
User tries leaking out information on recording media
User succeeds that depends besides Mail Sending. in segregated area
Pb
User tries leaking out information on transmission by mail in segregated area
Pd
The eighth measures is exceeded
Pc
The E-mail monitoring measures is exceeded
(1-ΔPα13X3)
(1-ΔPα11X1)
The first measures is exceeded
The second measures is exceeded
(1-ΔPα12X2)

Figure 7. [Fault Tree for Personal Information Leakage Caused by Internal Unjust Person Type1]

sed on the above fault tree, the probability $P \alpha_1$ that personal information will be leaked by an internal (an employee let into a segregated area) unauthorized user can be formulated as

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

Similarly, the probability $P\alpha_2$ and P_β can be formulated.
Here, we assume

Pa=0.05,Pb=0.01,Pc=0.04,Pd=0.05,Pe=0.004,,Pf=0.01,Pg=0.04,Ph= 0.05,Pi=0.01,Pj=0.5,Pk=0.01,Pl=0.1,Pm=0.4,Po=0.5,Pp=0.01.

Formulation results obtained are as shown in Fig. 8.

Minimization : $Min\{\text{Amount of damage} * (P_{\alpha 1}+P_{\alpha 2}+P_\beta)+\sum_{i=1}^{8} Ci*Xi\}$

Subject to

$$\sum_{i=1}^{8} C_i X_i \leq Ct \quad \text{(Total cost of measures)}$$

$$\sum_{i=1}^{8} D_{1i} X_i \leq D_1 \quad \text{(Degree of privacy burden)}$$

$$\sum_{i=1}^{8} D_{2i} X_i \leq D_2 \quad \text{(Degree of convenience burden)}$$

$$P_{\alpha 1} + P_{\alpha 2} + P_\beta \leq Pt \quad (X_i = 0,1)$$

(Probability of Information Leakage)

Figure 8. [Formulated Results]

4.3 Development of a simplified version of the MRC using Excel

Based on these formulation results, combinations with the smallest objective function, the second smallest objective function, and the third smallest objective function are determined by the method of all possible combinations while satisfying constraints using very simple prototype program based on Excel.

Excel has a feature to align values for an item (e.g. objective function value) in order of the smallest. Values not satisfying constraints can be filtered, so two or more optimal solutions can be easily determined using Excel. In this case, brute force method was used to obtain the optimal solutions, because the number of variables was small.

In addition, constraint values can be changed and easily recalculated, so optimal solutions can be determined in various cases and easily indicated to individuals involved. Furthermore, Excel is also replete with features for graphic representation, so solutions can be expressed in a relatively easy-to-understand form.

4.4 Results of application and Discussion

Next, constraints were specifically furnished and calculation performed. Here

the upper limit Ct of the cost of measures =80M yen, the upper limit Pt of the probability of leakage=0.15 (15% a year), D_1=0.3, and D_2=0.3

Results were:

The first optimal solution

Objective function value: **27,963,563**

Proposed measures adopted: 2,3,4,5,6,7

The second optimal solution

Objective function value: **39,813,235**

Proposed measures adopted: 1,3,4,5,6,7

Experiment to achieve consensus was done by role players as shown below.

Specialist :
researcher of MRC

Executive officer :
teacher at Tokyo Denki University

Employee :
student at Tokyo Denki University

Customer :
student at Tokyo Denki University

The process to obtain the consensus is as follows.

(1) The student who roles customer claimed that leakage probability should be fewer than 10% for the year. Then, the role player of the specialist calculated the optimum solution again, but first optimal solution was not changed.

(2) The student who roles employee claimed that degree of privacy burden should be under 0.15. Then, the role player of the specialist calculated the optimum solution again on the above condition. The first optimal solution was

Objective function value: **39,813,235**

Proposed measures adopted: 1,3,4,5,6,7

This first optimal solution is same as the second optimal solution of first calculation. Measure 1 "e-mail automatic monitoring" was added to the solution instead of measure 2 "e-mail manual monitoring" from the view point of employee's privacy.

This calculated result was also accepted by the role players of the executive officer and customer. Thus, consensus of all participants could be obtained.

Based on the above application and study results, the following statements regarding the MRC can be made:

(1) Handling the difficulty of formulation (Topic 1-a in Sec. 3.4): formulation is not easy, but the MRC appears applicable. Individuals applying the MRC gave the opinion that optimal solutions were sure to be obtained.

(2) Handling the uncertainty of effects (Topic 1-b) and constraint ambiguity (2-a): Of the various opinions voiced by individuals involved, individuals applying the MRC had the impression that problems of the uncertainty of effects of measures and constraint ambiguity could be resolved to some extent by changing values and determining new solutions, although this must also be confirmed through future testing.

(3) Handing of consideration of unquantified factors (2-b): individuals applying the MRC had the opinion that features to obtain not just the first optimal solution but the second - - the Lth optimal solution would be preferable since solutions could be selected from the first — the Lth optimum while considering factors that could not be formulated. This point must be confirmed through testing with a number of users.

(4) Handling the method of quickly reaching a solution that satisfies an individual involved (2-c) and resolution of disagreement between groups in terms of solutions (2-d): There were strong opinions that features allowing conditions to be changed and results immediately displayed would be effective in bundling satisfactory solutions, although the order in which they would be shown is currently being studied and is a topic for the future. In addition, individuals involved were curious about assumptions with which optimal solutions were determined, although how they can be shown effectively is also a topic for the future.

During the current trial application of the MRC, two specific settings where the MRC could be used were envisioned:

(a) When think tanks are commissioned by government bodies to make proposals to government bodies. This often leads to macro-models targeting the entire country of Japan.

(b) When an SI firm proposes systems accounting for risks to receive orders from a firm's system. This often leads to micro-models focusing on corporate environments.

5. CONCLUSION

Preceding sections have described the features an MRC should have, a simple prototype program based on Excel to support it, and results of its trial application.

There are plans to do the following work in the future:

(1) Apply the MRC in another 2-3 examples (for example, Illegal copy protection problem) and verify the features than an MRC should have.

(2) Improve the prototype program to make it possible to solve larger problems and to make it easy to use for risk communication.

Research themes for MRC are extremely difficult, but they are essential themes that must be dealt with in the future, so research will actively proceed.

The current research was conceived during work of the Safety and Security Working Group of the Application Security Forum (ASF) and is a deeper study of 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.

As research proceeds, the authors wish to thank individuals like Professor Norihisa Doi of Chuo University for their valued opinions.

References

1) R. Sasaki: Discussion regarding the relationship between security and personal information protection, Institute of Electronics, Information, and Communication Engineers, Technical Report SITE2003-14, pp1-6, Oct. 2003 (in Japanese)

2) J. Ross: The Polar Bear Strategy, Preceus Books Publishing, 1999

3)http://www.nrc.gov/reading-rm/doc-collections/nuregs/brochures/br0308/#chapter_1

4) http://web.sfc.keio.ac.jp/~hfukui/class/riskmg/risk.pdf (in Japanese)

5)http://www.riskworld.com/books/topics/riskcomm.htm

6) http://excellent.com.utk.edu/~mmmiller/bib.html

7) R. Sasaki: MRC development concepts, Institute of Electronics, Information, and Communication Engineers, SCIS2004 (in Japanese)

8) N.J. McCormick: Reliability and Risk Analysis, Academic Press Inc., (1981)

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

10) Y. Kodama: Introductory system dynamics—Science to take on complex social systems, Kodansha Blue Back, (1984) (in Japanese)