International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:8, No:4, 2014

Proposal of a Model Supporting Decision-Making on Information Security Risk Treatment

Ritsuko Kawasaki (Aiba), Takeshi Hiromatsu

***Abstract*—**Management is required to understand all information security risks within an organization, and to make decisions on which information security risks should be treated in what level by allocating how much amount of cost. However, such decision-making is not usually easy, because various measures for risk treatment must be selected with the suitable application levels. In addition, some measures may have objectives conflicting with each other. It also makes the selection difficult. Therefore, this paper provides a model which supports the selection of measures by applying multi-objective analysis to find an optimal solution. Additionally, a list of measures is also provided to make the selection easier and more effective without any leakage of measures.

***Keywords*—**Information security risk treatment, Selection of risk measures, Risk acceptance and Multi-objective optimization.

I. Introduction

THIS paper aims to support decision-making about risk treatment and risk acceptance for all information security risks within an organization.

In information security risk management, risk treatment and risk acceptance are the activities which particularly require decision-making by management. In other words, management is required to make decisions on which risks are treated in what level, and on which risks are accepted, among identified and evaluated risks in risk assessment processes. Here, a risk means an information security risk in this paper, though the term "risk" generally has broader meaning.

Risks are various, however management is required to understand all risks within an organization and to modify their values to the pre-defined "risk acceptance level" or less by distributing limited resources in the processes of risk treatment.

If a scope of risk management is quite limited, decision-making about risk treatment and risk acceptance may not be difficult very much, because in-depth risk assessment can be done and decision can be made based on detailed and specific information. On the other hand, if whole organization is a scope, applying detailed risk management is not realistic. It spends much time and cost, and its outcome is too much complicated to maintain and revise. Identification of risks and risk treatment plans in appropriate granularity is needed to make risk management pragmatic.

Risk treatment involves deciding the treating risks, selecting measures for them, and implementing measures. The levels of risks are modified to the risk acceptance level or less by implementing measures. For achieving the effective risk treatment, preparing the good list of candidates of measures is quite important.

The risks within an organization are various, so the measures are also various. Thus, the objective of each measure is also various. This means that risk treatment approach involves multi objectives and some objectives may conflict. For example, one of the measures is network access control. The objective of it is appropriately controlling network access. Application of this measure improves confidentiality, one of the aspects of information security; however, it may violate availability, another aspect of information security. Therefore, applying multi-objective optimization method is suitable to select measures, and the results are provided as Pareto optimal solutions.

For the reasons above, this paper provides a way to prepare a list of measures a way on how to quantify the relationship between each measure and each risk, a model providing one of the optimal solutions about the selection of measures, and the cost distribution for each measure.

The model uses goal programming for multi-objective optimization to find an optimal solution. The model is implemented by using solver add-in of Excel 2010. Thus, the model calculates one of the optimal solutions of selection of hedges and distribution of resources to each hedge selected.

II. Literature Review

The studies about risk treatment, which provide the ways on how to select measures to the risks identified, are limited. Among the few studies, the approaches by [1] and [2] are pragmatic as the approaches applying to an organization. They provide the ways modeling the relationship among assets, threats and measures, and logically find the optimal combinations of measures. The selection of measures is formulated as discrete optimization problems. However, they possess the following issues.

Firstly, the approaches assume identification and evaluation of assets and their threats. Setting these presuppositions is natural, because the previous international standard of ISO/IEC 27001:2005 [3] was required to identify and evaluate assets, threats and vulnerabilities to identify and evaluate risks within an organization. Previous international technical report of ISO/IEC TR 13335-3:1998 [4] also provide such guidance, and many users refer these documents. However, revised ISO/IEC 27001:2013 [5] does not include the requirements identifying assets, threats and vulnerabilities as activities of risk assessment. Only risks and their owners are required. When considering that ISO/IEC 27001:2005 [3] has broadly been

R. Kawasaki (Aiba) is a graduate student in Institute of Information Security, Yokohama, Japan. (dgs118101@iisec.ac.jp).

T. Hiromatsu is with the Institute of Information Security, Yokohama, Japan. (tkhirom@iisec.ac.jp).

referred and new version of it will be referred from now on, the method not to identify assets and threats will be needed.

Secondly, the studies do not provide detailed ways for the preparation of a list of measures for the risks identified, though it needs rich knowledge and experiences. The literature [1] provides nothing about how to list up measures. The literature [2] only describes: "measures are listed by referring [6], and the measures achieving by organizational activities are omitted by assuming that they are preferentially implemented." Thus, both studies do not provide the ways how to make a list of measures. As a result, the efficiency of the lists provided in these studies also cannot be confirmed.

The literatures [7] and [8] provide the way to select measures by analyzing in details within limited scopes. The literature [7] proposes an optimal security objectives (measures) decision method which determines security objectives (measures) quantitatively from the viewpoint of effectiveness and efficiency. The method includes a derivation scheme of security objective (measures) candidate sets for protection from possible threats by applying minimal path set search algorithm on the fault trees with respect to the threats. This method can be applied only for a product or a system with limited functions, because of the complexity of its processes. The literature [8] limits the threats to illegal copying, and provides the method to obtain the optimal combination of countermeasures for illegal copying, based on combinatorial optimization technique and fault tree analysis. Since this method is also complex, removing the limitation of threats is difficult. Both studies are suitable to apply to a quite limited scope and are not suitable to apply to an organization.

The literature [9] and [10] are focusing on a risk of potential lawsuit. They separate measures to two groups: measures for risks of potential lawsuit, and measures which prevent information security incidents. This approach may suitable for an organization which deals with personal information and/or data, because such an organization generally possesses high risks of lawsuit. However, on the other hand, it can be considered lacking versatility.

The literature [11] provides the approach to select information security measures. The groups of controls provided by ISO/IEC 27002 [12] are used as the list of measures in these studies, because of the comprehensiveness and versatility above a certain level. The approach aims to apply to an organization, and to evaluate and identify the most appropriate controls based on organization specific criteria. However, it does not assume risk assessment. That is to say risk are not identified and evaluated when using this approach. Risk assessment has become a general process in organizational management not only in information security field but also any other management areas. ISO 31000 [13] provides principals, framework and processes of risk management, (risk management includes risk assessment), and all risks are included in its scope. The identical text commonly used by ISO's all management systems standards also includes the notion of risks. From these situations, risk management process can be considered to be adopted by many organizations. Thus, selection of controls also should follow general risk assessment approach. The approach provided by [14] is similar to [11].It also does not assume risk assessment. The scope of [14] is limited to electronic commerce.

III. A Model

A. Overview of a Model

The objective of the model proposed in this paper is supporting a decision-making by management about risk treatment and risk acceptance. More concretely to say, the model provides the way to find one of the optimal solutions about which risks are treating to what level by applying which measures.

The following are the elements of the model:

1) A comprehensive list of risks within an organization and a value of each risk,
2) A comprehensive list of measures and each cost needed to implement each measure,
3) A value of effect by each measure to each risk,
4) A risk acceptance level (a value of risk acceptance), and
5) A total cost for measures (an organization's budget).

The lists and values of (1)-(3) are dealt with as fixed. The values of (4) and (5) are changed when applying the model to find optimal solutions. The solutions consists the degrees of implementation of the measures listed. How to prepare (1)-(5) is introduced in the following chapters.

B. A List of Risks and the Values of the Risks

The number of risks dealt with this model should be limited to the number that management can pragmatically understand and modify them. In this paper, seven risks are identified (see Table I).

In addition, the risks must be identified without any leakage, because unrecognized risks cannot be treated and as a result it causes security failure. To eliminate any leakage, two attributes "risk sources" and "motive of risks" are set. The attribute "risk sources" are classified to four: internal users, contracted users, other users and other than persons. Another attribute "motive of risks" is classified to two: intentional and accidental. By combining these attribute, all risks are separated to seven groups. For example, one of the groups includes risks by internal user's intentional actions. Finally, each group is considered as a risk and a list of seven risks are prepared (see Table I).

TABLE I
A List of Risks and the Values of the Risks

Name of Risks	Attribute 1 Risk Source	Attribute 2 Motive	Value (r_i)
R_1	Internal user	Intentional	7
R_2	Internal users	Accidental	6
R_3	Contracted users	Intentional	8
R_4	Contracted users	Accidental	7
R_5	Other users	Intentional	9
R_6	Other users	Accidental	8
R_7	Not due to human	Intentional	6

The values of risks (r_i) are set by using a numeric scale from 0 to 9, like in Table I in this paper. The methods proposed in

ISO/IEC 27005 [15] and [16] are assumed to be referred in order to set these values in this paper. Here, note that the values of risks differ from organization to organization depending on their business and environmental situations, thus the values in Table I is just an example. These values are considered fixed values in the model.

C. A List of Measures and the Costs Needed

The number of measures dealt with this model also should be limited to the pragmatic number. At the same time the list of measures must be comprehensive. In order to prepare such a list, ISO/IEC 27002:2013 [12] is referred in this mode, because it is widely used in information security field, and its lists of control objectives and controls are considered comprehensive at some level as generic lists. ISO/IEC 27002:2013[12] specifies 35 control objectives and 113 controls. Each control objective includes one or more controls, and control objectives are categorized to 14clauses constructed by collecting similar control objectives. Thus, each clause includes one or more control objectives and controls under high level objectives.

A list of measures is set by using the structures of ISO/IEC 27002:2013 [12]. That is, 14 clauses are considered 14 measures. Here, the term "hedge" is used to indicate these 14 measures in order to distinguish from general measures, and controls in ISO/IEC 27002:2013 [12] (see Table II).

TABLE II
A LIST OF HEDGES AND THE COSTS NEEDED TO IMPLEMENT THE HEDGES

Name of Hedge	Category (Clause number of ISO/IEC 27002:2013)	Cost (c_i)
H_1	Security Polices (Clause 5)	500
H_2	Organization of Information Security (Clause 6)	1000
H_3	Human Resource Security (Clause 7)	1000
H_4	Asset Management (Clause 8)	1500
H_5	Access Control (Clause 9)	2500
H_6	Cryptography (Clause 10)	1000
H_7	Physical and Environmental Security (Clause 11)	5000
H_8	Operations Security (Clause 12)	1500
H_9	Communications Security (Clause 13)	1500
H_{10}	System Acquisition, Development and Maintenance (Clause 14)	2000
H_{11}	Supplier Security (Clause 15)	3000
H_{12}	Information Security Incident Management (Clause 16)	1500
H_{13}	Information Security Aspects of Business Continuity Management (Clause 17)	2000
H_{14}	Compliance (Clause 18)	1000

The characteristics that each hedge is consisted by one or more controls are used when quantifying an effect of each hedge to each risk as effect value (see *next section*).

In addition, the costs needed to implement the hedges (c_i) are required in the model. The values in Table II are set in this paper. The values of costs are assumed to be calculated by referring the descriptions of ISO/IEC 27002:2013[12] and the situation of an organization by using monetary value.

The hedges include a lot of controls, thus the notion of an implementation rate of a hedge is applied in this model, and a set of the rates is set as a solution of the model. Here, it is assumed that an effect of a hedge is directly proportional to a cost of a hedge, to simplify the model. By distributing organization's total cost, the set of rates of implementation of hedges are decided automatically by applying this assumption (see Fig. 1).

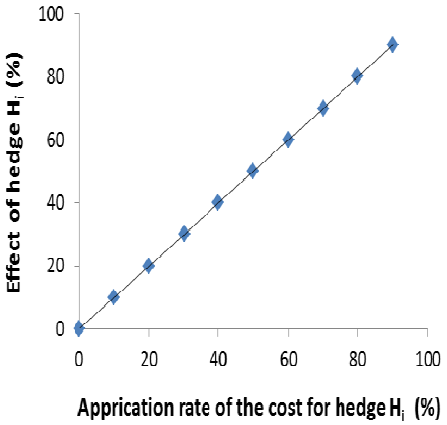

Fig. 1 Direct Proportion between Cost and Effect of Hedge (Assumption in this Model)

D. Quantification of an Effect by Each Hedge to Each Risk

To find an optimal solution of a set of application rate of hedges, the relationship between hedges and risks are needed. In other words, an effect by each hedge to each risk is needed to be quantified. In order to quantify the effects, the characteristics of controls included in hedges are utilized.

The first step of the quantification is setting new aspects for controls to find the relationship between controls and hedges. The list of aspects in Table III is used. These aspects may be considered that they are duplicated to the categories applied in ISO/IEC 27002:2013 [12]. It is true; however, applying these aspects again for each control has a meaning. The controls set under a control objective in ISO/IEC 27002:2013 [12] are still high level. That is to say, a control includes a lot of concrete measures. For instance, a control "9.4.2 Secure log-on procedures" includes not only technical measures, such as applying a function for authentication and a function not disclosing sensitive information, but also operational measure, such as checking logs and making policy for log-on procedure. Thus, the aspect in Table III is set in order to analyze controls. The aspects are set by referring [17].

TABLE III
ASPECTS APPLYING TO EACH CONTROL FOR QUANTIFICATION OF THE EFFECT VALUES

Aspect	Measures included in the aspect
Physical	- Installation of appropriate equipment for protection from interference, damage, not allowed entry, etc. - Access control to buildings and rooms - Anti-theft for PC, mobile devices, etc.
Technical	- Administration of network and computer systems - Access control on network and computer systems - Development, implementation and maintenance of systems - Anti-virus
Operational	- Collection of security information - Monitoring - Checking compliance - Considerations to operations management - Incident management activities - Agreement for outsourcing - Development of rules
Human resource	- Setting roles and responsibilities - Education and training - Reporting scheme for incidents/accidents - Password administration - Contraction of temporary and part-time workers

Next step is a check of the descriptions in a section of "implementation guidance" of each hedge in ISO/IEC27002:2013 [12]. "Implementation guidance" provides more detailed information to support the implementation of the control. The Check point is whether the measures for each risk defined in Table I are described in "implementation guidance's''. Which aspect in Table III includes the recognized measures is also identified. If description can be found, set 1 to the hedge for the risk, otherwise set 0. Table IV shows a result of one of the hedges as a part of results.

According to the results above, the number of controls which possess physical aspect is 39. The numbers of controls of other aspects are as follows: technical aspect is 60, operational aspect is 112 and human resources aspect is 39. Thus, the total number of controls in consideration of aspects is 250.

Final step is a calculation of effect value. The number 0 or 1 is set above for all controls for all risks and for all aspects. In this step, taking sums of these numbers for all hedges and for every risks, and being divided the sums by 250. The numbers calculated are the effect values for every all and every risk (see Table IV as an example).

The calculated effect values are shown in Table V.

TABLE IV
AN EXAMPLE OF A CALCULATION OF AN EFFECT VALUE (A CASE OF H_3)

Control	Aspect	Risks R_1	R_2	R_3	R_4	R_5	R_6	R_7
Clause 7 Human Resource Security								
7.1 Prior to employment								
7.1.1	Physical	0	0	0	0	0	0	0
	Technical	0	0	0	0	0	0	0
	Operational	0	0	0	0	0	0	0
	Human Resource	1	1	0	0	0	0	0
7.1.2	Physical	0	0	0	0	0	0	0
	Technical	0	0	0	0	0	0	0
	Operational	1	1	0	0	0	0	0
	Human Resource	1	1	0	0	0	0	0
7.2 During employment								
7.2.1	Physical	0	0	0	0	0	0	0
	Technical	0	0	0	0	0	0	0
	Operational	1	1	0	1	1	0	0
	Human Resource	0	0	0	0	0	0	0
7.2.2	Physical	0	0	0	0	0	0	0
	Technical	0	0	0	0	0	0	0
	Operational	0	0	0	0	0	0	0
	Human Resource	1	1	0	1	1	0	0
7.2.3	Physical	0	0	0	0	0	0	0
	Technical	0	0	0	0	0	0	0
	Operational	1	0	0	0	0	0	0
	Human Resource	1	0	0	0	0	0	0
7.3 Termination and change of employment								
7.3.1	Physical	0	0	0	0	0	0	0
	Technical	0	0	0	0	0	0	0
	Operational	1	1	0	1	1	0	0
	Human Resource	1	1	0	1	1	0	0
Sum		9	7	0	4	4	0	0
Effect value (Sum/234)		0.04	0.03	0	0.02	0.02	0	0

TABLE V
EFFECT VALUES OF ALL HEDGES TO EVERY RISK

Risk / Hedge	R_1	R_2	R_3	R_4	R_5	R_6	R_7
H_1	0.01	0.01	0.01	0.01	0.01	0.01	0.01
H_2	0.06	0.06	0.06	0.06	0.06	0.05	0.02
H_3	0.04	0.03	0.00	0.02	0.02	0.00	0.00
H_4	0.10	0.10	0.09	0.10	0.10	0.09	0.04
H_5	0.13	0.13	0.12	0.12	0.12	0.11	0.00
H_6	0.02	0.02	0.02	0.02	0.02	0.02	0.00
H_7	0.13	0.13	0.12	0.13	0.13	0.10	0.07
H_8	0.11	0.11	0.08	0.11	0.11	0.07	0.03
H_9	0.06	0.06	0.06	0.06	0.06	0.06	0.06
H_{10}	0.11	0.12	0.10	0.10	0.11	0.10	0.08
H_{11}	0.02	0.03	0.02	0.02	0.03	0.02	0.02
H_{12}	0.05	0.05	0.05	0.05	0.05	0.05	0.05
H_{13}	0.04	0.04	0.04	0.04	0.04	0.04	0.04
H_{14}	0.06	0.06	0.04	0.06	0.06	0.04	0.04

E. Other Components of a Model

A risk acceptance level and a total cost of for hedges are needed in the model. The risk acceptance level (R accept) is the

value that an organization aims to modify all-risks' values (ri, i=1, 2, … , 7) to it or less. The total cost for hedges (B) means a budget for risk treatment of an organization. The sum of each cost implementing each hedge at some level cannot excess the budget. These values are considered constraints in the model.

F. Formula of a Model

The model handles a set of application rates of hedges (x_1, x_2, … , x_{14}) as a set of variables in the model. Where, x_i is an application rate by percentage of H_i. Finding an optimal solution of the set of variables is an objective of the model. An optimal solution is defined which meets the following conditions in this model:

- the value of risks are modified to the pre-determined risk acceptance level or less,
- sum of the costs to be used to hedges is organization's budget or less, and
- the difference between modified risks and risk acceptance level are minimize,

The first and second conditions are by the constraints, and the third condition is based on the thought that big difference between modified risks and the risk acceptance level means excessive use of cost. These conditions are converted to the following formulas.

For the original values of risks (r_j), the value after modification (r_j') is calculated by (1), where $e_{ij}$is an effect value of H_i to R_j, and R_{accept} is an risk acceptance level.

$$r_j^{'} = r_j \bullet (1 - \frac{\sum_{i=1}^{14} e_{ij} \bullet x_i}{\sum_{i=1}^{14} e_{ij}} \bullet \frac{1}{100}) \le \mathrm{R}_{\mathrm{accept}} \quad (1)$$

The formula of the second condition about cost is (2), where c_j is the cost needed to implement H_j completely, and B is the total cost for hedges (organization's budget).

$$\sum_{i=1}^{14} c_i \bullet x_i \le B \quad (2)$$

The formula of the third condition is (3), and this is the objective function of the model.

$$Min.\{ f(x_i) = \sum_{j=1}^{7} (R_{accpet} - r_j^{'}) \} \quad (3)$$

The model was implemented by using solver add-in, on Excel 2010 in this paper.

IV. Sample Data Application to a Model

A. The Objective of the Application of Sample Data

In order to verify the effectiveness of the model, sample data is applied. Applying actual data to the model is desirable, however actual data of which amount of cost is spent to each hedge is not generally disclosed by organizations. Thus, sample data is prepared in this paper.

By applying such sample data to the model, the validation of solutions and the effectiveness of the model are analyzed.

B. A Solution of a Model

A solution of the model consists of the set of application rates by percentages of all hedges, and the sum of cost to be spent for the selected hedges' implementation. The model needs the input of constraints. Table VI shows an example of a set of constraints, and the results for the inputs.

TABLE VI
EXAMPLE OF THE INPUTS AND THE SOLUTION OF THE MODEL

	Item		Value
Input	Risk Acceptance Level		5
	Total Cost (Organization's Budget)		12000
	The Sum of Cost to be Spent		10756.94
Solution	Application level (%)	H_1	0
		H_2	100
		H_3	100
		H_4	0
		H_5	100
		H_6	100
		H_7	0
		H_8	100
		H_9	0
		H_{10}	0
		H_{11}	100
		H_{12}	0
		H_{13}	0
		H_{14}	75.69

C. Application of Basic Data to a Model

Firstly, considering the case that R_{accept} of 9and total cost of 25000 are inputted. The model provides the result in Table VII in this case.

TABLE VII
THE RESULT WHEN R_{ACCEPT}= 9 AND TOTAL COST = 25000

	Item		Value
Input	Risk Acceptance Level		9
	Total Cost (Organization's Budget)		25000
	The Sum of Cost to be Spent		0
Solution	Application level (%)	H_1	0
		H_2	0
		H_3	0
		H_4	0
		H_5	0
		H_6	0
		H_7	0
		H_8	0
		H_9	0
		H_{10}	0
		H_{11}	0
		H_{12}	0
		H_{13}	0
		H_{14}	0

Where, 25000 is the sum of c_i and 9 is the highest value of risks. Thus, the inputs do not act as constraints in this case. The result means no hedge is implemented because all values of risks are under R_{accept}. Thus, this result is reasonable.

Next, considering the case that R_{accept} of 0and total cost of 25000 are inputted. For the inputs, the model provides the result in Table VIII.

TABLE VIII
THE RESULT WHEN R_{ACCEPT}= 9 AND TOTAL COST = 25000

	Item		Value
Input	Risk Acceptance Level		0
	Total Cost (Organization's Budget)		25000
	The Sum of Cost to be Spent		100
Solution	Application level (%)	H_1	100
		H_2	100
		H_3	100
		H_4	100
		H_5	100
		H_6	100
		H_7	100
		H_8	100
		H_9	100
		H_{10}	100
		H_{11}	100
		H_{12}	100
		H_{13}	100
		H_{14}	100

The result means that all hedges are implemented under the sufficient budget to reduce values of all risks to zero. This result is reasonable.

D.The Minimum Total Cost for a Given R_{accept}

The minimum total cost can be found for a given R_{accept}, by changing the value of total cost and applying the model. For example, for the total cost of 8000 and R_{accept} of 5, there is an optimal solution. For the total cost of 7000 and R_{accept} of 5, there is an optimal solution too. However, for the total cost of 6000 and R_{accept} of 5, there is no optimal solution (see Table IX). This means that the total cost of 8000 and 7000are enough to achieve R_{accept} of 5; however, the total cost of 6000 is too small to achieve that. Thus, the minimum total cost for R_{accept} of 5 is more than 6000 and less than 7000.

TABLE IX
CHANGE THE TOTAL COSTS FOR THE FIXED R_{ACCEPT}(1)

	Item		Value		
Input	Risk Acceptance Level		8000	7000	6000
	Total Cost		5	5	5
	The Sum of Cost to be Spent		8000	7000	-
Solution	Application level (%)	H_1	0	0	-
		H_2	100	100	-
		H_3	100	32.41	-
		H_4	27.22	45.06	-
		H_5	100	100	-
		H_6	0	0	-
		H_7	0	0	-
		H_8	100	100	-
		H_9	0	0	-
		H_{10}	0	0	-
		H_{11}	19.72	0	-
		H_{12}	0	0	-
		H_{13}	0	0	-
		H_{14}	100	100	-

Continuously, for the R_{accept} of 5, total cost of 6400 and 6300 are set. When total cost is 6400, a solution can be found. However, when total cost is 6300, there is not any solution (see Table X). This means that the minimum cost for R_{accept} of 5 is between 6300 and 6400. By using the model above, the approximate minimum total cost can be found for a given R_{accept}.

TABLE X
CHANGE THE TOTAL COSTS FOR THE FIXED R_{ACCEPT}(2)

	Item		Value	
Input	Risk Acceptance Level		6400	6300
	Total Cost		5	5
	The Sum of Cost to be Spent		6400	-
Solution	Application level (%)	H_1	0	-
		H_2	100	-
		H_3	0	-
		H_4	100	-
		H_5	12.22	-
		H_6	0	-
		H_7	0	-
		H_8	100	-
		H_9	0	-
		H_{10}	54.72	-
		H_{11}	0	-
		H_{12}	0	-
		H_{13}	0	-
		H_{14}	100	-

Continuously, for the R_{accept} of 5, total cost of 6400 and 6300 are set. When total cost is 6500, a solution can be found. However, when total cost is 6400, there is not any solution. The approximate minimum total cost can be found for a given R_{accept} by changing total costs and apply them to the model.

E. The Minimum R_{accept} for a Given Total Cost

Next, in opposite to the previous section, the minimum R_{accept} can be found for a given total cost, by changing R_{accept} and applying them to the model. For example, for the total cost of 12000 and R_{accept} of 4, there is an optimal solution. For the total cost of 12000 and R_{accept} of 3, there is an optimal solution too. However, for the total cost of 12000 and R_{accept} of 2, there is no optimal solution (see Table XI). This means that the total cost of 12000 is insufficient to achieve R_{accept} of 2. Thus, R_{accept} of 3 is the smallest value achieved for the given total cost of 12000.

TABLE XI
CHANGE R_{ACCEPT} FOR THE FIXED TOTAL COST

	Item		Value		
Input	Risk Acceptance Level		12000	12000	12000
	Total Cost		4	3	2
Solution	The Sum of Cost to be Spent		12000	12000	-
	Application level (%)	H_1	0	0	-
		H_2	100	100	-
		H_3	100	55	-
		H_4	98.98	100	-
		H_5	100	100	-
		H_6	48.54	0	-
		H_7	0.60	22.86	-
		H_8	100	100	-
		H_9	0	0	-
		H_{10}	0	100	-
		H_{11}	100	26.90	-
		H_{12}	0	0	-
		H_{13}	0	0	-
		H_{14}	100	100	-

In sum, the model can be used not only to find an optimal solution but also to find the minimum total cost for a given R_{accept} and the minimum R_{accept} for a given total cost.

V. Conclusions

A model to find an optimal solution which provides selected risk hedges with their application levels, under the constraints of the total cost of risk hedges and the risk acceptance level was proposed. This model can also be used to find the suitable risk acceptance level for a given total cost, and the appropriate total cost for a given risk acceptance level.

In this model, a generic list of measures was also provided as candidates of selection in risk treatment process. This list was prepared by referring ISO/IEC 27002:2013[12] in order to make it comprehensive, and the measures included in the list were called the hedges. The hedges are defined in large particle size, thus, the application level was defined in direct proportion to the cost in this model.

Finally, the way to quantify the effect by a hedge to a risk was proposed and it was called the effect value of a hedge to a risk.

VI. Future Tasks

In order to show the effectiveness of the model, applying this model to a real case is needed as a future task. The problem is that the data about risk treatment and resource distribution is usually not disclosed. Finding raw data is difficult, thus expanding the target of data applying to the model, such as statistical data, is also needed to consider.

References

[1] Hyodo, T., Nakamura, I., Nishigaki M., Soga, M. (2003). A modeling of security measure selection problem, The Special Interest Group (SIG) Technical Reports (TR) of Information Processing Society of Japan (IPSJ), Computer Security (CSEC) Group, 74, 249-256. (Japanese document).

[2] Nakamura, I., Hyodo, T., Soga, M., Mizuno, T., &Nishigaki, M. (2004). A Practical Approach for Security Measure Selection Problem and Its Availability. IPSJ Journal, 45(8), 2022-2033. (Japanese document).

[3] ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management system – Requirement.

[4] ISO/IEC TR 13335-3:1998Information technology - Guidelines for the management of IT Security - Part3: Techniques for the management of IT Security.

[5] ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management system – Requirement.

[6] Next Generation Electronic Commerce Promotion Council of Japan (ECOM) (2002). Explanations of information security management standard (JIS X 5080:ISO/IEC 17799). From http://www.jipdec.or.jp/archives/ecom/results/h13seika/h13results-10.pdf (Japanese document).

[7] Nagai Y., Fujiyama T., & Sasaki R. (2000). An Optimal Decision Method for Establishment of Security Objectives. IPSJ Journal, 41(8), 2264-2271. (Japanese document).

[8] Sasaki R., Yoshiura H., &Itoh S. (2002). Consideration on Combinatorial Optimization of Illegal Copy Countermeasures. IPSJ Journal, 43(8), 2435-2446. (Japanese document) .

[9] Usui, Y., Yamamoto, T., Magata, F., Teshigawara, Y., Sasaki, & R., Nishigaki, M. (2009). A case study of a security measure selection scheme with consideration of potential lawsuit. In Proceedings of the Computer Security Symposium 2009, IPSJ, 105-110. (Japanese document).

[10] Nishigaki, M., Usui, Y., Yamamoto, T., Magata, F., Teshigawara, Y., & Sasaki, R. (2011). A Case Study of a Security Measure Selection Scheme with Consideration of Potential Lawsuit. IPSC Journal 52(3), 1173-1184 (Japanese document).

[11] Otero, A. R., Otero, C. E., &Qureshi, A. (2010), A Multi-Criteria Evaluation of Information Security Controls Using Boolean Features. International Journal of Network Security & Its Applications (IJNSA), 2(4). doi:10.5121/ijnsa.2010.2401 1.

[12] ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls.

[13] ISO 31000:2009, Risk management – Principles and guidelines.

[14] Barnard, L., &Solms, R. V., (2000). A Formalized Approach to the Effective Selection and Evaluation of Information Security Controls. Computers & Security, 19(2), 185-194.

[15] ISO/IEC 27005:2011 Information technology -- Security techniques -- Information security risk management.

[16] Japan Institute for Promotion of Digital Economy and Community (JIPDEC) (2008), Guideline for ISMS users - correspond to JIS Q 27001:2006 (ISO/IEC 27001:2005) - Risk management edition -.from http://www.isms.jipdec.or.jp/doc/JIP-ISMS113-21.pdf (Japanese document).

[17] National Information Security Center [NISC](2000), Guideline for information security policy. From http://www.kantei.go.jp/jp/it/security/taisaku/guideline.html (Japanese document).