Proposal of a Model Supporting Decision-Making Based On Multi-Objective Optimization Analysis 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. Moreover, risks generally have trends and it also should be considered in risk treatment. Therefore, this paper provides the extension of the model proposed in the previous study. The original model supports the selection of measures by applying a combination of weighted average method and goal programming method for multi-objective analysis to find an optimal solution. The extended model includes the notion of weights to the risks, and the larger weight means the priority of the risk.

***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, we proposed a way to prepare a list of measures, a way on how to quantify the relationship between each measure and each risk, and a model providing one of the optimal solutions about the selection of measures and the cost distribution for each measure in the previous study [1]. Moreover, the notion of risk trend is added to the model in this paper, because there is a tendency that similar risks occur frequently. Several reasons of this tendency can be considered. One is that many people has a tendency to imitate an influential risk occurred by a malicious person. Another is that many organizations face the same external environment and have similar internal environment within the scope of Information Technology.

The model uses a combination of weighted average method and 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 in information security field. The international standard, ISO/IEC 27001:2013 [2] includes the descriptions about risk treatment and risk acceptance and this standard is widely used in the

R. Kawasaki (Aiba) is a graduate student with the Institute of Information Security, Yokohama, Japan (e-mail: ritsuko@shihtzu.jp).

T. Hiromatsu is with Institute of Information Security, Yokohama, Japan. (e-mail: tkhirom@iisec.ac.jp)

world. However, it just provides requirements about information security risk management, because of the characteristics as an international standard. It does not provide detailed explanations of risk treatment and risk acceptance, and the way of risk treatment cannot be found.

The approaches by [3] and [4] 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. These approaches to risk assessment and risk treatment are frequently applied in information security field, because several international standards, such as ISO/IEC 27001:2005 [5] and ISO/IEC TR 13335-3:1998 [6], provided such approaches. 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. ISO/IEC 27001:2005[5] was broadly referred, thus the new version, ISO/IEC 27001:2013[2] will also be referred broadly. When considering such condition, the method not to identify assets and threats will be needed. Moreover, the studies [3] and [4] do not provide detailed ways for the preparation of a list of measures for the risks identified. The literature [4] only describes: "measures are listed by referring [7], and the measures achieving by organizational activities are omitted by assuming that they are preferentially implemented." Thus, the ways how to make a list of measures are not provided. As a result, the efficiency of the lists provided in these studies also cannot be confirmed.

The literatures [8] provide the way to select measures by analyzing in details within limited scopes. The proposed method determines security objectives (measures) quantitatively from the view point of effectiveness and efficiency, and 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 [9] 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. Because of the complexity of this method, expanding the scope of threats seems difficult. Both studies [8] and [9] are suitable to apply to a quite limited scope and are not suitable to apply to an organization.

The literatures [10] and [11] 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, the approach can be considered lacking versatility.

The literature [12] provides the approach to select information security measures. The groups of controls provided by ISO/IEC 27002[13] 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. Risk assessment has become a general process in organizational management not only in information security field but also any other management areas. One reason is the issue of ISO 31000[14].It provides principals, framework and processes of risk management, which includes risk assessment, and shows the necessity of risk management within an organization. Another reason is the development of the identical text commonly used by ISO's all management systems standards. It includes the notion of risks. Therefore, selection of controls also should follow general risk management approach. That is, it should be based on risk assessment. The approach provided by [15] is similar to [12]. It also does not assume risk assessment. The scope of [15] 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 and a weight 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 and Weight 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 addition, the risks must be identified without any leakage, because unrecognized risks cannot be treated and as a result it causes security failure. In order to satisfy both conditions, seven risks defined in [1] are set by using two attributions, risk source and motive (see Table I).

Additionally, the values of risks (r_i) are needed in this model and the values in Table I are set as well as [1].Here, it is important to note that risk values are generally 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.

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

Moreover, the notion of weight for risks is also added to the model. Each risk is able to have weight given by a positive number, and the number means priority of the risk. That is, larger number is more preferentially.

The reason to adopt the notion of weight for risks is based on the tendency that similar risks occur frequently. For example, the leakages of personal information by companies were reported frequently in Japan few years ago. As another example, a company may have a situation that failure of equipment occurs frequently. Several reasons can be considered. One is that many people has a tendency to imitate an influential risk occurred by a malicious person. As a result, many organizations suffer the similar risks. Another is that many organizations face the same external environment and have similar internal environment within the scope of Information Technology. The frequent occurrence of equipment failures is one of this reason's examples.

The weight of risk is used to reflect such risk trends to 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 as well as the list of risks.

In order to prepare such a list, the approach in [1] is taken. That is, ISO/IEC 27002:2013 [13] is referred, 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. Its 14 clauses are set as 14 measures. Here, the term "hedge" is used instead of "measure" in order to distinguish from general measures and controls in ISO/IEC 27002:2013[13] (see Table II).

In addition, the costs needed to implement the hedges (c_j) are set as in Table II by using the approach applied in [1].

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).

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_j)
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

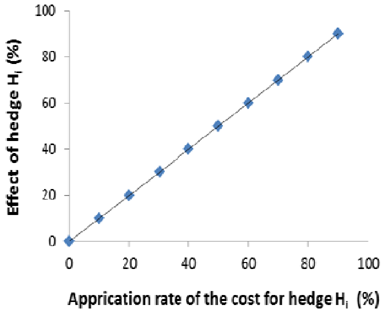

Fig. 1 Direct Proportion between Cost and Effect of Hedge (Assumption in this Model)

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. By applying the method introduced in [1], the values in Table III are given.

TABLE III
EFFECT VALUES OF ALL HEDGES TO EVERY RISK

Ris k 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. 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 minimizes, and the levels of risk mitigation by hedges are maximize.

The first and second conditions are by the constraints, and the third condition is based on the thought that

- Risks should be mitigated to the suitable level, and
- 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.

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

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).

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

The formula of the third condition is (3), and this is the objective function of the model. Here, the objective function are constructed by (a) the sum of mitigated values of risks with weights (w_j) for risks, and (b) the sum of difference between risk acceptance level and risks. To find an optimal solution, (a) should be maximize and (b) should be minimize. Thus, the objective function can be set as (a) divided by (b), and the objective is maximizing the value. However, if the value of (b) is zero the value of (3) is set as zero.

$$Max. \frac{\sum_{j=1}^{7} w_j \bullet r_j \bullet \sum_{i=1}^{14} (R_{accpet} - r_j^{'})}{\sum_{j=1}^{7} (R_{accpet} - r_j^{'})} \tag{3}$$

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 and weights of risks. Table IV shows an example of inputs, and the results for them.

TABLE IV
Example of the Inputs and the Solution of the Model

Item			Value
Input	Risk Acceptance Level		5
	Total Cost (Organization's Budget)		12000
	Weight of risk	R_1	1
		R_2	1
		R_3	1
		R_4	1
		R_5	1
		R_6	1
		R_7	1
Solution	The Sum of Cost to be Spent		10765.94
	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 V in this case. Here, all weights are set to 1, thus. Their values are omitted at the followings.

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

Item			Value
Input	Risk Acceptance Level		9
	Total Cost (Organization's Budget)		25000
Solution	The Sum of Cost to be Spent		0
	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 VI.

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

Item			Value
Input	Risk Acceptance Level		0
	Total Cost (Organization's Budget)		25000
Solution	The Sum of Cost to be Spent		100
	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 VII). 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 VII
CHANGE THE TOTAL COSTS FOR THE FIXED R_{ACCEPT}(1)

Item			Value		
Input	Risk Acceptance Level		5	5	5
	Total Cost		8000	7000	6000
Solution	The Sum of Cost to be Spent		8000	7000	-
	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 VIII). This means that the minimum cost for R_{accept} of 5 is between 6300 and 6400. By using the results above, the approximate minimum total cost can be found for a given R_{accept}.

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

Item			Value	
Input	Risk Acceptance Level		5	5
	Total Cost		6400	6300
Solution	The Sum of Cost to be Spent		6400	-
	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	-

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, forthe 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 IX). 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 IX
CHANGE R_{ACCEPT} FOR THE FIXED TOTAL COST

Item			Value		
Input	Risk Acceptance Level		4	3	2
	Total Cost		12000	12000	12000
Solu-tion	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	0.06	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.

F. The Setting of Weights

The setting of weights for risks gives priority to risk treatment. In Table X, the situation that risks not due to human occur is assumed, and some different weights of risk R_7, 1, 5 and 10 are set. All other risks' weights were set to 1. When comparing the values of R_7 after mitigation, the values are 4.00 (w_7= 1), 3.94 (w_7 =5), and 3.07 (w_7=10). Because of the results, it was confirmed that larger weight gives priority to mitigate R_7 in the example.

Table XI also gives another example. It assumes the situation that the risks by users who have some authorities to the systems and equipment of the organization, that is internal users and contracted users, are occurred frequently. Thus, the risks, from $R_1$to R_4 are prioritized. In this case, it can be confirmed that enough large weights give slight priority for risk mitigation.

TABLE X
THE SETTING OF WEIGHTS: R_7

Item			Value		
Input	Risk Acceptance Level		4	4	4
	Total Cost		10000	10000	10000
	Weight of Risk	R_1	1	1	1
		R_2	1	1	1
		R_3	1	1	1
		R_4	1	1	1
		R_5	1	1	1
		R_6	1	1	1
		R_7	1	5	10
Solu-tion	The Sum of Cost to be Spent		10000	10000	10000
	Application Level (%)	H_1	0	0	0
		H_2	100	100	100
		H_3	100	100	0
		H_4	100	100	100
		H_5	100	100	36.35
		H_6	39.33	0	0
		H_7	0	0	0
		H_8	100	100	100
		H_9	0	0	0
		H_{10}	23.67	25.98	100
		H_{11}	21.11	32.68	69.56
		H_{12}	0	0	0
		H_{13}	0	0	0
		H_{14}	100	100	100
	Value of Risk after Mitigation	R_1	2.97	2.98	3.24
		R_2	2.62	2.62	2.71
		R_3	3.85	3.86	3.77
		R_4	3.05	3.06	3.16
		R_5	4.00	4.00	4.00
		R_6	3.87	3.89	3.77
		R_7	4.00	3.94	3.07

V.CONCLUSIONS

The weights for risks can be added to the model proposed in the previous study [1]. The extended model can provide the selection of measures, which reflects risk trends, by setting large numbers as weights to the risks.

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.

TABLE XI
THE SETTING OF WEIGHTS: R_1, R_2, R_3 AND R_4

Item			Value	
Input	Risk Acceptance Level		4	4
	Total Cost		10000	10000
	Weight of Risk	R_1	1	5
		R_2	1	5
		R_3	1	5
		R_4	1	5
		R_5	1	1
		R_6	1	1
		R_7	1	1
Solu-tion	The Sum of Cost to be Spent		10000	10000
	Application Level (%)	H_1	0	0
		H_2	100	100
		H_3	100	100
		H_4	100	100
		H_5	100	100
		H_6	41.64	39.33
		H_7	0	0
		H_8	100	100
		H_9	0	0
		H_{10}	22.51	23.67
		H_{11}	21.11	21.11
		H_{12}	0	0
		H_{13}	0	0
		H_{14}	100	100
	Value of Risk after Mitigation	R_1	2.98	2.97
		R_2	2.62	2.62
		R_3	3.85	3.85
		R_4	3.06	3.05
		R_5	4.00	4.00
		R_6	3.85	3.87
		R_7	4.00	4.00

REFERENCES

[1] Kawasaki (Aiba), R.,Hiromatsu, T., (2014). Proposal of a Model Supporting Decision-Making on Information Security Risk Treatment. World Academy of Science, Engineering and Technology, International Science Index 88, International Journal of Computer, Information Science and Engineering, 8(4), 34 - 40.

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

[3] 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)

[4] 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)

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

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

[7] 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)

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

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

[10] 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)

[11] 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)

[12] 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.

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

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

[15] 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.