Risk Assessment Quantification in Hybrid Cloud Configuration

Shigeaki Tanimoto, Tsutomu Konosu, Motoi Iwashita
Faculty of Social Systems Science
Chiba Institute of Technology
Chiba, Japan
e-mail: {shigeaki.tanimoto, tklab, iwashita.motoi}@it-chiba.ac.jp

Hiroyuki Sato
Information Technology Center
The University of Tokyo
Tokyo, Japan
e-mail: schuko@satolab.itc.u-tokyo.ac.jp

Atsushi Kanai
Faculty of Science and Engineering
Hosei University
Tokyo, Japan
e-mail: yoikana@hosei.ac.jp

***Abstract*—With recent progress in Internet services and high-speed network environments, cloud computing has rapidly developed. Furthermore, the hybrid cloud configuration is now attracting attention, because it offers the advantages of both public and private clouds. However, public clouds have the problem of uncertain security, while private clouds have the problem of high cost. Thus, risk assessment in a hybrid cloud configuration is an important issue. Our previous study analyzed qualitatively risk assessment of the hybrid cloud configuration. Accordingly, through analysis of risk in a hybrid cloud configuration, 21 risk factors were extracted and evaluated, and countermeasures were proposed. However, we recognized that it was only a qualitative study and that a quantitative evaluation would be needed to make its countermeasures more practical. Hence, in this paper, the risk factors identified in the previous study are analyzed and quantitatively evaluated. Specifically, the values of the risk factors were approximately calculated by using a risk formula used in the field of information security management systems (ISMS). On the basis of these values, the effect of the countermeasures proposed in the previous study was evaluated quantitatively. It was found that the countermeasures in the previous study could reduce their corresponding risk factors by about 18% - 36%. The results herein can be used to promote hybrid cloud computing services in the future.**

Keywords-Risk Assessment; Hybrid Cloud Configuration; Risk Matrix; Risk Value Formula; Information Security Management System (ISMS)

I. INTRODUCTION

Recent years have seen great progress in Internet services and high-speed network environments. As a result, cloud computing has rapidly developed, with two main forms. First, public clouds are operated by service providers, such as Google and Amazon. Second, private clouds are built and operated by individual enterprises for their own use. Generally, a public cloud eliminates the cost of unnecessary facilities and offers rapid flexibility and scale. However, since a public cloud effectively has invisible features in a virtual configuration, enterprise users are uncertain about the cloud's security and aspects of practical use. On the other hand, a private cloud offers visualization of management, since the enterprise operates its own facilities, and guarantees security in accordance with the company's own policies. The drawbacks to a private cloud, however, include greater cost for maintenance and management of facilities, and so forth [1].

As one example, an incident of missing data and leakage by a cloud operating company, called the "big ripple," occurred in June, 2012, in Japan [2]. When a cloud provider's management handles security poorly, serious risks occur only in the public clouds that it manages, so such incidents may become apparent to users. On the other hand, a hybrid cloud form, combining aspects of both public and private clouds, is now attracting attention. Generally in a hybrid cloud, data requiring high security is handled within a private cloud, while data requiring easy operation at low cost is handled in a public cloud [3].

Thus, although the hybrid cloud form requires two different cloud forms be maintained and managed, its operation also depends on the kind of data. Furthermore, various risk factors are involved, such as accidentally saving to a different cloud during data storage [4]. For these reasons, it is important to investigate risk management in a hybrid cloud configuration. We also applied a risk assessment method for analysis and evaluation from a comprehensive viewpoint. As a result, 21 risk factors in a hybrid cloud were extracted, and countermeasures were proposed. However, it was only a qualitative study, meaning that a more practical quantitative evaluation still needed to be undertaken.

In this paper, we describe a quantitative evaluation of the risk factors of a hybrid cloud obtained in our previous study and the proposed countermeasures. Specifically, a risk value based on the formula is approximately calculated for each risk factor [5]-[7]. Then, on the basis of this value, the effect of the countermeasures on the risks can be quantitatively evaluated. It is shown that the countermeasures in the previous study can reduce their corresponding risk factors by about 18% - 36%. We believe that the results of this study will help to promote hybrid cloud computing services.

 ISBN: 978-1-61208-427-5

Section 2 reviews the hybrid cloud computing that has been studied so far. In Section 3, we describe our previous study and the present problem. Section 4 describes the quantitative evaluation of hybrid cloud computing's risks. Section 5 is a conclusion and describes future work.

II. HYBRID CLOUD CONFIGURATION

Cloud computing has now shifted to the practical use stage, and many cloud-related services increased sales in 2011. Moreover, many user companies are verifying the possibility and practicality of cloud computing in introducing information and communications technology (ICT). Cloud computing analysis is thus recognized as a key stage in systems configuration [8].

A. Reference Model of Cloud Computings

As shown in Figure 1, software as a service (SaaS), platform as a service (PaaS), and infrastructure or hardware as a service (IaaS or HaaS) are classified as the main components of the present cloud computing model. Moreover, in terms of deployment models, cloud computing is classified into public, private, and hybrid or managed clouds. Finally, cloud computing includes the roles of cloud provider and cloud user [9].

B. Hybrid Cloud

Although the hybrid cloud appears in the reference model of Figure 1, its concrete configuration combines a public cloud and private cloud, as shown in Figure 2. Usually, a company creates a hybrid cloud, and the company and a public cloud provider share executive responsibility. The hybrid cloud uses both public and private cloud services. Thus, when a company requires both public and private cloud services, a hybrid cloud is optimal. In this case, the company can summarize its service targets and service requirements and then use public or private cloud services accordingly. Thus, service correspondence can be attained in constituting a hybrid cloud, not only for a secure, mission-critical processes like employee salary processing but also for business information such as payment receipts from customers.

However, the main problem with a hybrid cloud is the difficulty of actually creating and managing such a solution. The public and private clouds must be provisioned as if they were one cloud, and implementation can become even more complicated. Therefore, since the hybrid cloud concept is a

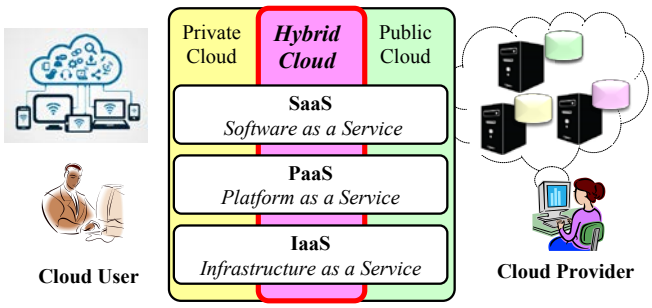


Figure 1. Reference model of cloud computing [9]

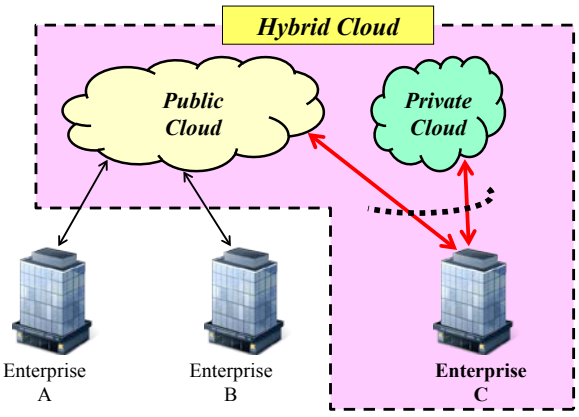


Figure 2. Hybrid cloud configuration

comparatively new architecture in cloud computing and best practices and tools have not yet been defined, companies hesitate to adopt hybrid clouds in many cases [10].

Hence, this paper examines the subject of hybrid cloud configuration in terms of these risks that adoption entails. That is, from the viewpoints of both a cloud user and a cloud provider, we consider what kinds of risks are assumed and develop a concrete risk management strategy.

C. Related work

Many security-related papers about hybrid cloud computing have been published [11]-[18]. In particular, as for the references [11] and [12], comprehensive analysis is conducted in detail about the security of cloud computing. However, the analysis of the security in a hybrid cloud configuration of these references is not sufficient. For example, these papers didn't focus on various threats in hybrid cloud computing. Also in hybrid cloud, there are threats, such as an operation mistake etc. of the cloud administrator who mentioned in Section 1. Furthermore, a user's operation mistake is also assumed as a threat peculiar to hybrid cloud. For example, when a user saves data, it is a case saved at different cloud by mistake.

On the other hand, we have already considered the risk assessment of hybrid cloud computing from the viewpoint of a user [19]. However, this evaluation is qualitative and is not sufficient. Therefore, this paper describes the risk assessment of hybrid cloud computing and adds a quantitative evaluation.

III. PREVIOUS STUDY: RISK ASSESSMENT IN HYBRID CLOUD CONFIGURATION

A. Extraction of Risk Factors

To extract the risk factors in a hybrid cloud configuration, we applied the risk breakdown structure (RBS) method, which is a typical method of risk management in project management [20]. Table 1 lists the extracted risk factors. As shown in the table, the hybrid cloud configuration was classified at the highest level into system, operation, facility, and miscellaneous categories from a comprehensive viewpoint. A total of 21 risk factors were extracted [19].

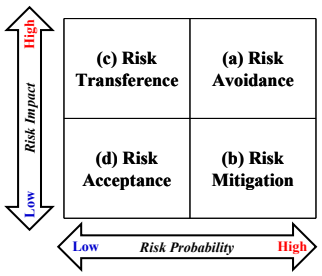
 ISBN: 978-1-61208-427-5

TABLE I. RISK FACTORS EXTRACTED BY RBS

High level	Middle level	Low level	Risk factors
1. System	1.1 Software	1.1.1 Application	1.1.1.1 A risk of mistaken allocation of the program in hybrid Cloud
			1.1.1.2 A risk of the mistaken allocation in the case of duplicate programs
		1.1.2 Data	1.1.2.1 A risk of mistaken allocation of the data in hybrid Cloud
			1.1.2.2 A risk of the mistaken allocation in the case of duplicate data
	1.2 Hardware	1.2.1 Performance	1.2.1.1 A risk of the unexpected load for CPU throughput
			1.2.1.2 A risk of unexpected use for memory size
	1.3 Network	1.3.1 Performance	1.3.1.1 A risk of the access speed slowing during network congestion etc.
2. Operation	2.1 Public cloud	2.1.1 A risk when sharing resources with the other company in public Cloud	
		2.1.2 An operation risk of public Cloud's not being administrable by the company side	
		2.1.3 A risk of the service continuity by the side of public Cloud	
	2.2 Private cloud	2.2.1 A risk of cost exceeding estimation	
		2.2.2 A risk of the human resource development in private Cloud	
	2.3 Hybrid cloud	2.3.1 A risk of the data management mismatching between different Clouds	
3. Facility	3.1 Public cloud	3.1.1 A facility risk of public Cloud's not being administrable by the company side	
		3.1.2 A risk of public Cloud's business continuity	
	3.2 Private cloud	3.2.1 A risk of an excess of facilities cost in private Cloud	
		3.2.2 A risk of the environmental construction in private Cloud	
		3.2.3 A risk of new business starting in private Cloud	
	3.3 Hybrid cloud	3.3.1 A risk of the optimal use ratio of public Cloud and private Cloud	
4. Miscellaneous	4.1 Law	4.1.1 A risk of legal revision	
	4.2 Disasters	4.2.1 A risk of a disaster	

B. *Risk Analysis in Hybrid Cloud Configuration*

Next, we devised potential countermeasures against the identified risks; these are shown in Table 2. The risk matrix method was used to deduce these countermeasures [21]. As shown in Figure 3, this method classifies countermeasures into four kinds in accordance with their risk probability and risk impact, i.e., Risk Transference, Risk Mitigation, Risk Acceptance, and Risk Avoidance. Furthermore, it gives guidelines to draw up countermeasures. Table 2 lists the classification of the risk matrix methods in correspondence with its proposed countermeasures.



Risks are classified in accordance with the risk impact and risk probability. Countermeasures corresponding to each are as follows.

(a) Risk Avoidance: A risk is avoided, and alternatives are shown.
(b) Risk Mitigation: Decrease the risk to an acceptable level.
(c) Risk Transference: Transfer a risk to a 3rd party.
(d) Risk Acceptance: Accept a risk unconditionally.

Figure 3. Risk Matrix Method

TABLE II. RISK FACTORS EXTRACTED BY RBS AND PROPOSED COUNTERMEASURES

Level 3: Risk Factors	Risk Impact	Risk Probability	Countermeasure Classification	Proposed countermeasures
1.1.1.1 A risk of mistaken allocation of the program in hybrid Cloud	High	Low	Risk transference	Strengthen the management system upon deploying data and programs.
1.1.1.2 A risk of the mistaken allocation in the case of duplicate programs	High	Low	Risk transference	Even if the cloud is used mainly on active standby, prepare an additional cloud on cold standby to enable program exchange through manual operation.
1.1.2.1 A risk of mistaken allocation of the data in hybrid Cloud	Low	High	Risk mitigation	Prepare a data management manual. Upon cloud introduction, educate and train employees.
1.1.2.2 A risk of the mistaken allocation in the case of duplicate data	High	Low	Risk transference	Even if the cloud is used mainly on active standby, prepare an additional cloud on cold standby to enable program exchange through manual operation.
1.2.1.1 A risk of the unexpected load for CPU throughput	Low	High	Risk mitigation	During cloud design, include a significant performance margin to enable efficient cloud usage even when system utilization exceeds estimates.
1.2.1.2 A risk of unexpected use for memory size	Low	High	Risk mitigation	Guarantee sufficient storage capacity to handle cases of excessive system utilization.
1.3.1.1 A risk of the access speed slowing during network congestion etc.	Low	High	Risk mitigation	During cloud design, properly consider scale, cost, enterprise usage pattern, and so forth.
2.1.1 A risk when sharing resources with the other company in public Cloud	High	High	Risk avoidance	Do not use the public cloud but protect the company by using the private cloud.
2.1.2 An operation risk of public Cloud's not being administrable by the company side	High	High	Risk avoidance	If public cloud operation is unsuitable, switch to private cloud operation, and vice versa.
2.1.3 A risk of the service continuity by the side of public Cloud	High	Low	Risk transference	Select multiple cloud providers and organize backups and other processes in other public clouds.
2.2.1 A risk of cost exceeding estimation	Low	High	Risk mitigation	Reduce cost by educating employees so that the cloud's operation can be corresponded as much as possible in its company.
2.2.2 A risk of the human resource development in private Cloud	High	Low	Risk transference	The training for the Cloud operation is held regularly in an enterprise. Accordingly, when a security incident occurs, the system which can correspond promptly is built.
2.3.1 A risk of the data management mismatching between different Clouds	Low	High	Risk mitigation	During cloud construction, fully investigate security so as to unify the security control methods of both the private and public clouds.
3.1.1 A facility risk of public Cloud's not being administrable by the company side	High	Low	Risk transference	Deploy multiple public clouds.
3.1.2 A risk of public Cloud's business continuity	High	Low	Risk transference	Take out an insurance policy upon public cloud utilization. In addition, request third-party evaluation and survey the cloud provider.
3.2.1 A risk of an excess of facilities cost in private Cloud	Low	Low	Risk acceptance	Investigate the cost of private cloud construction sufficiently, and ensure that cloud facilities are used efficiently, such as through diversion.
3.2.2 A risk of the environmental construction in private Cloud	Low	Low	Risk acceptance	If a particular situation is judged necessary for the enterprise, approve it in order to develop the business.
3.2.3 A risk of new business starting in private Cloud	Low	High	Risk mitigation	Private Cloud's operation is made to permeate as an enterprise rule beforehand.
3.3.1 A risk of the optimal use ratio of public Cloud and private Cloud	Low	High	Risk mitigation	Determine a utilization policy for data handling.
4.1.1 A risk of legal revision	Low	Low	Risk acceptance	Respond flexibly to changes in law.

 ISBN: 978-1-61208-427-5

C. Problem of the previous study

The previous study was qualitative; a more practical quantitative evaluation is needed in order to implement the countermeasures it identifies. The current study thus is a quantitative risk assessment of the risk factors obtained in our previous study and its proposed countermeasures.

IV. QUANTITATIVE EVALUATION OF HYBRID CLOUD COMPUTING'S RISKS AND PROPOSED COUNTERMEASURES

Here, the validity of a countermeasure is evaluated through a quantification of the risk factors shown in Table 2. First, a risk formula used in the field of information security management systems (ISMS) is shown [5]-[7]. Next, an approximation is described for calculating a risk value on the basis of our previous qualitative results [22]-[23]. Finally, a risk value for hybrid cloud computing services is deduced by using the formula and approximation.

A. Risk formula

Each risk value is quantified by using (1), which is used in the field of ISMS [5]-[7].

$$\textit{Risk value} = \textit{value of asset} * \textit{value of threat} * \textit{value of vulnerability} \quad (1)$$

Generally, all elements of the right-hand side of (1) are very difficult to calculate. In this paper, the following approximation is used to simplify these elements [22]-[23].

1) Approximation of the Asset Value

Here, the asset value of (1) is approximated in terms of the risk impact in the risk matrix, as shown in Figure 4. This approximation is based on the following reasons. The amount of damage was regarded for assets. As the further approximation, it was considered that the amount of damage was risk impact. Additionally, references [5]-[7] define the risk impact as 1 (low) to 5 (high). As a further approximation, these values are mapped in risk impact to a risk matrix [22]-[23]. As shown in Figure 4, the risk impact of the risk matrix is divided in two. For the sake of simplicity, the higher of the two divisions approximated to the maximum risk impact (risk value ≒ 5). Similarly, the lower of the two divisions approximated to the minimum risk impact (risk value ≒ 1).

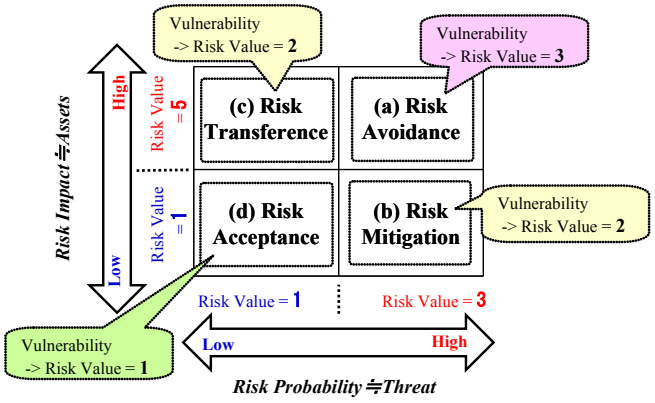


Figure 4. Risk Value Approximation of Risk Matrix [15]

2) Approximation of the Threat Value

The threat value of (1) is approximated in terms of the risk probability in the risk matrix, as shown in Figure 4. This approximation is based on the following reasons. It was supposed that threat was strongly dependent on risk probability. From references [5]-[7], the risk probability is defined to range from 1 (low) to 3 (high). These values are mapped to the generation frequencies of the risk matrix in Figure 4, as well as the above-mentioned risk impact approximation. That is, the higher of the two divisions approximated to the maximum risk probability (risk value ≒ 3), and the lower of the two divisions approximated to the minimum risk probability (risk value ≒ 1).

3) Approximation of the Value of Vulnerability

The vulnerability evaluation is defined in references [5]-[7] as well. It is defined on a three-level scale: 3 (High), 2 (Medium), and 1 (Low). These levels were approximated in accordance with the classification of the risk matrix in Figure 4. Here, the four domains of the figure are classified into three categories in accordance with the risk probability and risk impact, as follows.

- *Risk Avoidance*: both the risk probability and risk impact are high. It approximately corresponds to the highest risk classification.
- *Risk Transference and Risk Mitigation*: either the risk probability or the risk impact is high. They approximately correspond to the second highest risk classification.
- *Risk Acceptance*: both the risk probability and risk impact are low. It approximately corresponds to the lowest risk classification.

In the above-mentioned classification, *Risk Avoidance* cases are approximated to 3 (High), *Risk Transference* and *Risk Mitigation* cases to 2 (Medium), and *Risk Acceptance* cases to 1 (Low).

As mentioned above, (1) is approximated as (2). In addition, the approximate value of each parameter of (2) becomes as shown in Table 3 and Table 4.

$$\textit{Risk value} \fallingdotseq \textit{value of risk impact} * \textit{value of risk probability} * \textit{value of vulnerability} \quad (2)$$

TABLE III. APPROXIMATE VALUE OF RISK IMPACT AND RISK PROBABILITY OF (2)

	Risk Impact	Risk Probability
High	**5**	**3**
Low	**1**	**1**

TABLE IV. APPROXIMATE VALUE OF VULNERABILITY OF (2)

	Vulnerability
Risk Avoidance	**3**
Risk Transference and Risk Mitigation	**2**
Risk Acceptance	**1**

TABLE V. RISK VALUE BEFORE COUNTERMEASURES AND AFTER COUNTERMEASURES

Level 3: Risk Factors	Proposed Countermeasures	Asset ≒ *Risk Impact*	Threat ≒ Risk Probability	Vulnerability			Value of Risk		
				Before Countemeasure	After Countermeasure		Before Countermeasure	After Countermeasure	
					Ideal	Actual		Ideal	Actual
1.1.1.1 A risk of mistaken allocation of the program in hybrid Cloud	Design reinforcement of the Cloud construction	5	1	2	0	1	10	0	5
1.1.1.2 A risk of the mistaken allocation in the case of duplicate programs	Design reinforcement of the Cloud construction	5	1	2	0	1	10	0	5
1.1.2.1 A risk of mistaken allocation of the data in hybrid Cloud	Design reinforcement of the Cloud construction	1	3	2	0	1	6	0	3
1.1.2.2 A risk of the mistaken allocation in the case of duplicate data	Design reinforcement of the Cloud construction	5	1	2	0	1	10	0	5
1.2.1.1 A risk of the unexpected load for CPU throughput	Design reinforcement of the Cloud construction	1	3	2	0	1	6	0	3
1.2.1.2 A risk of unexpected use for memory size	Design reinforcement of the Cloud construction	1	3	2	0	1	6	0	3
1.3.1.1 A risk of the access speed slowing during network congestion etc.	Design reinforcement of the Cloud construction	1	3	2	0	1	6	0	3
2.1.1 A risk when sharing resources with the other company in public Cloud	Unapplied	5	3	3	3	3	45	45	45
2.1.2 An operation risk of public Cloud's not being administrable by the company side	Unapplied	5	3	3	3	3	45	45	45
2.1.3 A risk of the service continuity by the side of public Cloud	Unapplied	5	1	2	2	2	10	10	10
2.2.1 A risk of cost exceeding estimation	Design reinforcement of the Cloud construction	1	3	2	0	1	6	0	3
2.2.2 A risk of the human resource development in private Cloud	Unapplied	5	1	2	2	2	10	10	10
2.3.1 A risk of the data management mismatching between different Clouds	Design reinforcement of the Cloud construction	1	3	2	0	1	6	0	3
3.1.1 A facility risk of public Cloud's not being administrable by the company side	Unapplied	5	1	2	2	2	10	10	10
3.1.2 A risk of public Cloud's business continuity	Unapplied	5	1	2	2	2	10	10	10
3.2.1 A risk of an excess of facilities cost in private Cloud	Design reinforcement of the Cloud construction	1	1	1	0	1	1	0	1
3.2.2 A risk of the environmental construction in private Cloud	Design reinforcement of the Cloud construction	1	1	1	0	1	1	0	1
3.2.3 A risk of new business starting in private Cloud	Design reinforcement of the Cloud construction	1	3	2	0	1	6	0	3
3.3.1 A risk of the optimal use ratio of public Cloud and private Cloud	Design reinforcement of the Cloud construction	1	3	2	0	1	6	0	3
4.1.1 A risk of legal revision	Unapplied	1	1	1	1	1	1	1	1
4.2.1 A risk of a disaster	Unapplied	5	1	2	2	2	10	10	10
Total							221	141	182

B. *Calculation of risk value*

The risk values before applying countermeasures against risks were calculated using (2) (see Table 5 (Before Countermeasure)).

Next, the risk values after applying countermeasures were calculated. The following countermeasure was chosen from the viewpoint of practicality: "design reinforcement of the Cloud construction". This countermeasure can be easily implemented, although its costs may be problematic. Table 5 (After Countermeasure) shows the resulting risk values when performing the countermeasures.

Here, supposing an ideal case, vulnerability was assumed to be 0 as a result of using the proposed countermeasure. Moreover, supposing an actual case, this countermeasure is not always perfect. Thus, the vulnerability of an actual case is approximated to 1 (the minimum level).

C. *Results of evaluation*

Table 6 summarizes the results shown in Table 5. Although only the "design reinforcement of the Cloud construction" countermeasure was evaluated in this study, this table shows that the risk can be reduced between about 18% and 36%. These results also show that a detailed numerical expression can treat a risk more specifically by quantifying it and the prospective countermeasure.

D. *Discussion*

As mentioned above, it is not realistic to perform all of the proposed countermeasures on the risks in Table 2. Thus, this study dealt with only one ("design reinforcement of the Cloud construction") chosen on the basis of its practicality.

However, as mentioned above, the problem of cost might also affect this countermeasure. Generally speaking, this countermeasure can become expensive because it needs a specialist's knowledge. In the future, we will have to devise a verification considering such cost.

TABLE VI. EVALUATION RESULTS (SUMMARAIZATION OF RISK VALUE BEFORE COUNTERMEASURES AND AFTER COUNTERMEASURES)

	Before countermeasure against risk factors (①)	After countermeasure against risk factors (②)	
		Ideal case	Actual case
Total risk value	**221**	**141**	**182**
Risk reduction rate = (①－②) / ①	**-**	**0.36**	**0.18**

V. CONCLUSION AND FUTURE WORK

We are interested in promoting hybrid cloud computing services as a next-generation digitized infrastructure by assessing their risks and proposing countermeasures. In our previous study, although countermeasures were developed from a qualitative risk assessment, their effectiveness could not be quantified. Hence, in this study, we performed a quantitative evaluation that used a risk value. It was shown that countermeasures labeled "design reinforcement of the Cloud construction" in the previous study could reduce their corresponding risk factors by about 18% - 36%. These results mean that the countermeasures developed in our previous qualitative evaluation can be more specifically evaluated as to their effect by introducing a risk value.

In the future, we will further improve countermeasures and verify their cost effectiveness.

ACKNOWLEDGMENTS

This work was supported by the Japan Society for the Promotion of Science (JSPS, KAKENHI Grant Number 24300029).

REFERENCES

[1] S. Nakahara, N.Fujiki, S.Ushijima, Cloud traceability (CBoC TRX), NTT technical journal, 2011.10, pp. 31-35, (In Japanese)

[2] O. Inoue, First server Failure, Nihon Keizai Shimbun, 2012.6.26, (In Japanese)

[3] Microsoft : Shift to Hybrid Cloud, (In Japanese), [Online]. Available from: http://www.microsoft.com/ja- jp/opinionleaders/economy_ict/100701_2.aspx, 2015.4.5

[4] S. Tanimoto, M. Hiramoto, M. Iwashita, H. Sato, and A. Kanai, Risk Management on the Security Problem in Cloud Computing, IEEE/ACIS CNSI 2011, Korea

[5] M. S. Toosarvandani, N. Modiri, and M. Afzali, "The Risk Assessment and Treatment Approach in order to Provide LAN Security based on ISMS Standard," International Journal in Foundations of Computer Science & Technology (IJFCST), pp. 15-36, Vol. 2, No. 6, Nov., 2012

[6] H. Sato, T.Kasamatsu, T. Tamura, and Y. Kobayashi, "Information Security Infrastructure," Kyoritsu Shuppan Co., Ltd., 2010, (in Japanese)

[7] ISMS Risk Assessment Manual v1.4, [Online]. Available from: https://www.igt.hscic.gov.uk/KnowledgeBaseNew/ISMS%20Risk%20Assessment%20Manual%20v1.4.pdf, 2015.1.4

[8] A. Goto, T.Nishihara, The concept for the cloud computing technology CboC, NTT technical journal 2009.9, pp. 64-69, (In Japanese)

[9] N. Uramoto, Security and Compliance Issues in Cloud Computing, IPSJ Magazine 50(11), 1099-1105, 2009-11-15

[10] D. Amrhei, (In Japanese), http://www.ibm.com/developerworks/jp/websphere/techjournal/0904_amrhein/0904_amrhein.html

[11] S. Sengupta, V. Kaulgud, and V. S. Sharma, Cloud Computing Security - Trends and Research Directions, 2011 IEEE World Congress on Service, pp. 524-531, 2011

[12] S.Subashini, V.Kavitha, A Survey on security issues in service delivery models of cloud computing, Elsevier, Journal of Network and Computer Applications 34 (2011)1-11

[13] K. Y. Oktay, et al., Risk-Aware Workload Distribution in Hybrid Clouds, 2012 IEEE Fifth International Conference on Cloud Computing, pp. 229-236, 2012

[14] S. Nepal, C. Friedrich, L. Henry, and S. Chen, A Secure Storage Service in the Hybrid Cloud, 2011 Fourth IEEE International Conference on Utility and Cloud Computing, pp. 334-335, 2011

[15] M. A. AlZain, E. Pardede, B. Soh, and J. A. Thom, Cloud Computing Security: From Single to Multi-Clouds, 2012 45th Hawaii International Conference on System Sciences, pp. 5490-5499, 2012

[16] M. K. Srinivasan, K Sarukesi, P. Rodrigues, S. Manoj M, and Revathy P, State-of-the-art Cloud Computing Security Taxonomies - A classification of security challenges in the present cloud computing environment, ICACCI-2012, pp. 470-476

[17] L. Savu, Cloud Computing -Deployment models, delivery models, risks and research challenges-, http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5778816

[18] K. Bernsmed, M. G. Jaatun, P. H. Meland, and A. Undheim, Security SLAs for Federated Cloud Services, 2011 Sixth International Conference on Availability, Reliability and Security, pp. 202-209, 2011

[19] S. Tanimoto, et al., A Study of Risk Management in Hybrid Cloud Configuration, Springer, Computer and Information Science, vol. 493, pp. 247-257, 2013

[20] Risk Breakdown Structure, [Online]. Available from: http://www.justgetpmp.com/2011/12/risk-breakdown-structure-rbs.html, 2014.12.30

[21] Cox's risk matrix theorem and its implications for project risk management, [Online]. Available from: http://eight2late.wordpress.com/2009/07/01/cox%E2%80%99s-risk-matrix-theorem-and-its-implications-for-project-risk-management/, 2014.12.30

[22] S. Tanimoto, et al., A Study of Risk Assessment Quantification in Cloud Computing, 8th International Workshop on Advanced Distributed and Parallel Network Applications (ADPNA-2014), pp. 426-431, 2014

[23] S. Tanimoto, H. Sato, and A. Kanai, Risk Assessment Quantification of Ambient Service, ICDS 2015 : The Ninth International Conference on Digital Society, pp.70-75, Lisbon, Feb., 2015

 ISBN: 978-1-61208-427-5