Risk Assessment Quantification of Ambient Service

Fundamental investigation of the risks of cyber-physical systems

Shigeaki Tanimoto
Faculty of Social Systems Science
Chiba Institute of Technology
Chiba, Japan
shigeaki.tanimoto@it-chiba.ac.jp

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

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

***Abstract*—Ambient services have attracted attention as a possible ubiquitous, future intelligent infrastructure. An ambient service automatically provides services suited to the user by making sensors and computers cooperate and by gathering and analyzing information about each user. As such, ambient services are related to cyber-physical systems. However, in the process of managing personal information, ambient services are prone to various risks, such as information leakage. Our previous study analyzed the service provision and service use sides. It used the risk breakdown structure (RBS) and risk matrix, which are typical risk management methods of project management, and identified 40 risk factors faced by ambient services and countermeasures thereof. 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 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 18% - 36%. The results herein can be used to promote ambient services in the future.**

Keywords- Ambient Service; Cyber-physical System; Risk Assessment; Risk Value Formula; ISMS

I. Introduction

Ambient services, which use sensors or wireless-communications technology, are now attracting attention [1]. Ambient services offer the possibility of creating a new information society, as follows:

- Computers can be used to gather information from sensors and monitor the user's situation.
- Personal data can be accumulated and analyzed in order to provide services meeting the user's specific needs.

There are various merits of being able to provide services friendly enough to bridge the digital divide (e.g., to help elderly people unfamiliar with intelligent terminals) through cooperative functioning of computers and sensors [2]-[4]. As such, ambient services are related to cyber-physical systems.

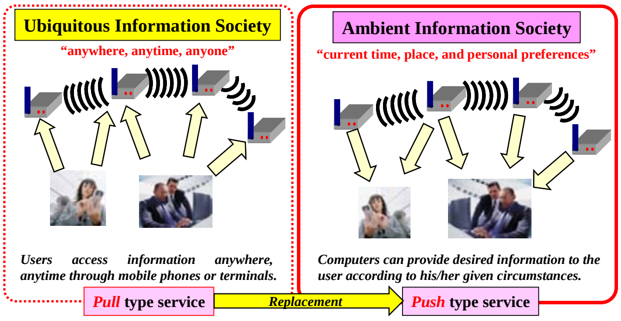
However, an ambient service requires a user's personal information beforehand. Accordingly, there are risks such as leakage of personal information. In fact, leaks could reveal, for example, not only the user's name, address, and names of other family members, but also his or her current position. Thus, confidentiality of personal information must be guaranteed to ensure that the ambient information society is safe and secure. In this regard, it is important to perform a risk assessment on an ambient service and to take countermeasures in advance against risks. In our previous study, we did a risk assessment of ambient services [5]. In particular, we used the risk breakdown structure (RBS) method to identify risk factors and the risk matrix method to analyze these factors [6]-[7]. We also drew up countermeasures to the identified risks. 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 ambient services obtained in our previous study and the proposed countermeasures. Specifically, a risk value based on the formula is calculated for each risk factor [8]-[10]. 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 18% - 36%. We believe that the results of this study will help to promote ambient services.

Section 2 reviews the various ambient services that have been studied so far. In section 3, we describe our previous study and the present problem. Section 4 describes the quantitative evaluation of ambient service's risks. Section 5 discusses related work, and section 6 is a conclusion and describes future work.

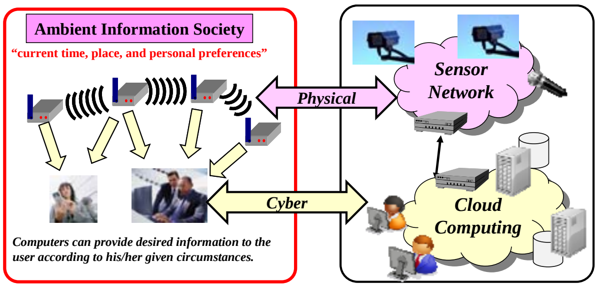
II. Ambient Services

In 1998, Eli Zelkha and Brian Epstein of Palo Alto Ventures in the U.S. crafted a presentation on the concept of ambient intelligence in which the future of consumer electronics, telecommunications, and computing is called the "ambient society" [11]. Since then, the idea of ambient services has attracted the attention of researchers as a potential next-generation digitized infrastructure that could replace the ubiquitous information society [9]. For example, the IT strategy of Japan has been transitioning from one of “u-japan” to “i-japan” [12]. Here, “u-japan” refers to a ubiquitous net society, whereas “i-japan” means a movement toward digital inclusion and innovation. The distinction between u-japan and i-japan is depicted in Figs. 1(1) and (2) [2] [12]. Moreover, as shown in Fig. 2, ambient services are also related to cyber-physical systems [13]-[14].


Ubiquitous Information Society
“anywhere, anytime, anyone”
Users access information anywhere, anytime through mobile phones or terminals.
Pull type service
Replacement
Ambient Information Society
“current time, place, and personal preferences”
Computers can provide desired information to the user according to his/her given circumstances.
Push type service

(1) Ubiquitous Service (2) Ambient Service

Figure 1. Transition from Ubiquitous Services to Ambient Servicese


Ambient Information Society
“current time, place, and personal preferences”
Computers can provide desired information to the user according to his/her given circumstances.
Physical
Cyber
Sensor Network
Cloud Computing

(1) Ambient Service (2) Cyber-physical System Environment

Figure 2. Relation between Ambient Services and Cyber Pysical Systems

III. Previous Study: Risk Factors and Countermeasures of Ambient Services

A. Risk factors of ambient services

Ambient services for a future information society face many problems that could hamper their spread. In the present ubiquitous information society, leaks of personal information due to nefarious schemes or even simple mistakes are a serious problem. Similar problems are of concern in an ambient service. In particular, there are various points of concern that arise in the aspects of privacy protection, disclosure of service content, etc.

In our previous study [5], we employed the risk breakdown structure (RBS) method [6], a typical risk management method for project management, to identify risk factors in ambient services. The results are shown in Table 1. As can be seen, the risk factors were identified from a comprehensive range of viewpoints. A total of 40 risk factors were extracted by the RBS analysis.

TABLE I. Risk Factors Extracted by RBS in Security Perception Problem

High division	Middle division	Low division	Risk Factor
1. Service provision side	1.1 System	1.1.1 Software	1.1.1.1 Problem in cooperating with the existing system
			1.1.1.2 Problem with ending Ambient Service
			1.1.1.3 Problem with service entrepreneur's specifications
			1.1.1.4 Problem with service entrepreneur's supervisor
			1.1.1.5 Leaks, etc., by service entrepreneur
			1.1.1.6 Data deleted at end of service use
			1.1.1.7 Problem with requirements for certification
			1.1.1.8 Problem in managing personal information
			1.1.1.9 Data seized by other company
			1.1.1.10 No restoration of missing data
			1.1.1.11 No security management
			1.1.1.12 Leakage and disappearance of data
			1.1.1.13 Lack of internal control or security audit
		1.1.2 Hardware	1.1.2.1 Portability problem with existing hardware
		1.1.3 Network	1.1.3.1 Problem with fulfilling SLA
			1.1.3.2 Insufficient right-to-access management
	1.2 Operation	1.2.1 Information control	1.2.1.1 Insufficient information disclosure by service entrepreneur
			1.2.1.2 Problem with different service specifications and user requirements
			1.2.1.3 Crisis regarding continuation of service
			1.2.1.4 Business continuation plan is insufficient
		1.2.2 Rule	1.2.2.1 Compliance violation
	1.3 Facility	1.3.1 Facility, Equipment	1.3.1.1 Power failure due to increased power consumption
			1.3.1.2 Environmental impacts such as carbon dioxide emissions
			1.3.1.3 Influence of delay or communication failure in real-time distribution
			1.3.1.4 Equipment installation problems.
2. Service use side	2.1 System	2.1.1 Software	2.1.1.1 Complication of operations
			2.1.1.2 Improper management of personal information
		2.1.2 Hardware	2.1.2.1 Portability problem with existing terminal
		2.1.3 Network	2.1.3.1 Problem with security of right to access
			2.1.3.2 Problem with safety of encryption
	2.2 Operation	2.2.1 Personal information	2.2.1.1 Problem in handling personal information
			2.2.1.2 Deletion of personal information
			2.2.1.3 User's incorrect deletion, alteration, etc.
			2.2.1.4 General information disclosure
		2.2.2 Certification	2.2.2.1 Problem with access except for a user
	2.3 Facility	2.3.1 Facility, Equipment	2.3.1.1 Breakage of device due to consumption
			2.3.1.2 Communication failure at base station
3. Other external factors	3.1 Law		3.1.1 Regulation problem arising from revision of law
	3.2 Disaster		3.2.1 Data center collapses in a disaster
			3.2.2 Problem compensating user for personal information disclosure, etc.

25 risk factors

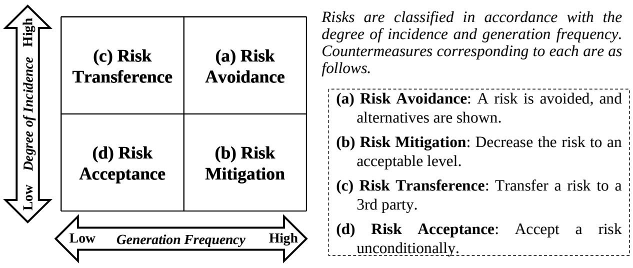
12 risk factors

3 risk factors

40 risk factors

B. Proposed countermeasures against risk factors

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 [7]. As shown in Fig. 3, this method classifies risks into four kinds, *i.e., Risk Transference, Risk Mitigation, Risk Acceptance*, and *Risk Avoidance*, in accordance with their generation frequency and degree of incidence. 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 degree of incidence and generation frequency. 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	Degree of Influence	Generation Frequency	Countermeasure Classification	Proposed countermeasures
1.1.1.1 Problem in cooperating with the existing system	High	High	Risk Avoidance	Adjustment on the use side
1.1.1.2 Problem with ending Ambient Service	High	Low	Risk Transference	Third-party surveillance
1.1.1.3 Problem with service entrepreneur's specifications	High	High	Risk Avoidance	Adjustment on the use side
1.1.1.4 Problem with service entrepreneur's supervisor	High	Low	Risk Transference	Third-party surveillance
1.1.1.5 Leaks, etc., by service entrepreneur	High	Low	Risk Transference	Application of assurance
1.1.1.6 Data deleted at end of service use	Low	High	Risk Mitigation	User complies with the specification by using the Ambient service.
1.1.1.7 Problem with requirements for certification	Low	High	Risk Mitigation	User complies with the specification by using the Ambient service.
1.1.1.8 Problem in managing personal information	Low	High	Risk Mitigation	User complies with the specification by using the Ambient service.
1.1.1.9 Data seized by other company	High	Low	Risk Transference	Application of assurance
1.1.1.10 No restoration of missing data	Low	Low	Risk Acceptance	Others
1.1.1.11 No security management	High	Low	Risk Transference	Application of assurance
1.1.1.12 Leakage and disappearance of data	High	Low	Risk Transference	Application of assurance
1.1.1.13 Lack of internal control or security audit	Low	Low	Risk Acceptance	Compromise
1.1.2.1 Portability problem with existing hardware	Low	High	Risk Mitigation	User complies with the specification by using the Ambient service.
1.1.3.1 Problem with fulfilling SLA	High	Low	Risk Transference	Third-party surveillance
1.1.3.2 Insufficient right-to-access management	Low	High	Risk Mitigation	Ambient service side adjusts specification
1.2.1.1 Insufficient information disclosure	Low	High	Risk Mitigation	Ambient service side adjusts specification
1.2.1.2 Problem with service specifications and user requirements	High	High	Risk Avoidance	Adjustment on the use side
1.2.1.3 Crisis regarding continuation of service	High	Low	Risk Transference	Application of assurance
1.2.1.4 Business continuation plan is insufficient	High	Low	Risk Transference	Application of assurance
1.2.2.1 Compliance violation	High	Low	Risk Transference	Third-party surveillance
1.3.1.1 Power failure due to increased consumption	High	Low	Risk Transference	Application of assurance
1.3.1.2 Environmental impacts	Low	Low	Risk Acceptance	Compromise
1.3.1.3 Influence of real-time distribution	Low	High	Risk Mitigation	User complies with the specification by using the Ambient service.
1.3.1.4 Equipment installation problems.	High	High	Risk Avoidance	Adjustment on the use side
2.1.1.1 Complication of operations	Low	High	Risk Mitigation	User complies with the specification by using the Ambient service.
2.1.1.2 Improper management of personal information	High	Low	Risk Transference	Third-party surveillance
2.1.2.1 Portability problem with existing terminal	Low	Low	Risk Acceptance	Adjustment on the offer side
2.1.3.1 Problem with security of right to access	Low	High	Risk Mitigation	Ambient service side adjusts specification.
2.1.3.2 Problem with safety of encryption	Low	High	Risk Mitigation	Ambient service side adjusts specification.
2.2.1.1 Problem in handling personal information	High	Low	Risk Transference	Third-party surveillance
2.2.1.2 Deletion of personal information	High	Low	Risk Transference	Third-party surveillance
2.2.1.3 User's incorrect deletion, alteration, etc.	Low	High	Risk Mitigation	Ambient service side adjusts specification.
2.2.1.4 General information disclosure	Low	High	Risk Mitigation	Application of assurance
2.2.2.1 Problem with access except for a user	Low	High	Risk Mitigation	Others
2.3.1.1 Breakage of device due to consumption	Low	Low	Risk Acceptance	Compromise
2.3.1.2 Communication failure	Low	Low	Risk Acceptance	Compromise
3.1.1 Regulation problem arising from revision of law	Low	Low	Risk Acceptance	Adjustment on the use side
3.2.1 Data center collapses in a disaster	Low	High	Risk Mitigation	Application of assurance
3.2.2 Problem providing compensation to user	Low	High	Risk Mitigation	Third-party surveillance

C. Problem of the previous study

The previous study was qualitative; a more practical quantitative evaluation would be 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 AMBIENT SERVICE'S RISKS AND PROPOSED COUNTERMEASURES

Here, the validity of a countermeasure is relatively 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 [8]-[9]. Next, an approximation for calculating a risk value based on our previous qualitative results is described [15]. Finally, a risk value for ambient services is deduced by using the formula and approximation.

A. Risk formula

Each risk value is quantified using (1), which is used in the field of ISMS [8]-[9].

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

Generally, the calculation of each element of the right-hand side of (1) is very difficult. In this paper, the following approximation is used to simplify these elements [15].

1) Approximation of the Asset Value

Here, the asset value of (1) is approximated in terms of the degree of incidence in the risk matrix, as shown in Fig. 4. Thus, it is assumed that the asset value is the degree of incidence. By the way, references [9]-[10] define the degree of incidence as 1 (low)-5 (high). As a further approximation, these values are mapped in degree of incidence to a risk matrix [15]. As shown in Fig. 4, the degree of incidence of the risk matrix is divided in two. For the sake of simplicity, the maximum degree of incidence (5) is approximated to the higher of the two divisions. Similarly, the minimum degree of incidence (1) is approximated to the lower of the two.

2) *Approximation of the Threat Value*

The threat value of (1) is approximated in terms of the generation frequency in the risk matrix, as shown in Fig. 4. From references [9]-[10], the generating frequency is defined as a range from 1 (low) to 3 (high). These values are mapped to the generating frequencies of the risk matrix of Fig. 4, as well as the above-mentioned degree-of-incidence approximation. That is, the maximum generating frequency (3) is approximated to the higher of the two divisions, and the minimum (1) is approximated to the lower of the two.

3) *Approximation of the Value of Vulnerability*

The vulnerability evaluation is defined in reference [9]-[10] as well. It is defined on a three-level scale, 3 (High), 2 (Medium), and 1 (Low), and these levels were approximated in accordance with the classification of the risk matrix of Figure 4. Here, the four domains of the figure are classified into three categories according to the generating frequency and degree of incidence, as follows.

- Risk Avoidance: both the generating frequency and degree of incidence are high. It approximately corresponds to the highest risk classification.
- Risk Transference and Risk Mitigation: either the generating frequency or the degree of incidence is high. It approximately corresponds to the 2nd highest risk classification.
- Risk Acceptance: both the generating frequency and degree of incidence 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 are approximated to 2 (Medium), and *Risk Acceptance* cases are approximated to 1 (Low).

B. *Calculation of risk value*

The risk value before applying countermeasures against a risk was calculated using (1) (see Table 3).

Next, the risk value after applying countermeasures was calculated. The following two measures were chosen from the viewpoint of practicality: "application of assurance" and "third-party surveillance". These countermeasures can be easily implemented, although their costs may be problematic. Table 4 shows the resulting risk values when performing the countermeasures.

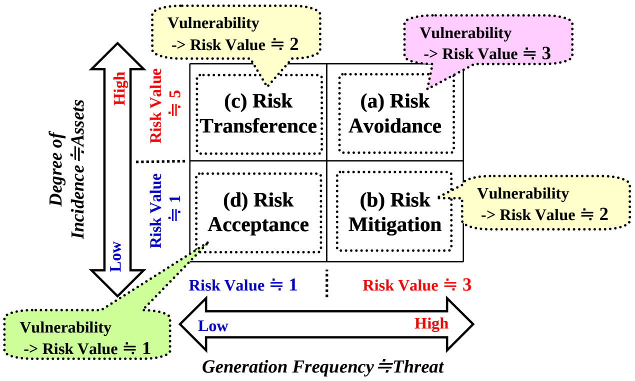


Figure 4. Risk Value Approximation of Risk Matrix [15]

Here, supposing an ideal case, vulnerability was assumed to be 0 as a result using the proposed countermeasures. By the way, supposing an actual case, these countermeasures are not always perfect. For example, in the case of "application of assurance", there may be bankruptcy of an insurance company though its probability is very low. In consideration of such a case, the vulnerability of an actual case is approximated to 1 (the minimum level).

TABLE III. RISK VALUE BEFORE COUNTERMEASURES

Level 3: Risk Factors	Assets	Threat	Vulner-ability	Value of Risk
1.1.1.1 Problem in cooperating with the existing system	5	3	3	45
1.1.1.2 Problem with ending Ambient Service	5	1	2	10
1.1.1.3 Problem with service entrepreneur's specifications	5	3	3	45
1.1.1.4 Problem with service entrepreneur's supervisor	5	1	2	10
1.1.1.5 Leaks, etc., by service entrepreneur	5	1	2	10
1.1.1.6 Data deleted at end of service use	1	3	2	6
1.1.1.7 Problem with requirements for certification	1	3	2	6
1.1.1.8 Problem in managing personal information	1	3	2	6
1.1.1.9 Data seized by other company	5	1	2	10
1.1.1.10 No restoration of missing data	1	1	1	1
1.1.1.11 No security management	5	1	2	10
1.1.1.12 Leakage and disappearance of data	5	1	2	10
1.1.1.13 Lack of internal control or security audit	1	1	1	1
1.1.2.1 Portability problem with existing hardware	1	3	2	6
1.1.3.1 Problem with fulfilling SLA	5	1	2	10
1.1.3.2 Insufficient right-to-access management	1	3	2	6
1.2.1.1 Insufficient information disclosure	1	3	2	6
1.2.1.2 Problem with service specifications and user requirements	5	3	3	45
1.2.1.3 Crisis regarding continuation of service	5	1	2	10
1.2.1.4 Business continuation plan is insufficient	5	1	2	10
1.2.2.1 Compliance violation	5	1	2	10
1.3.1.1 Power failure due to increased consumption	5	1	2	10
1.3.1.2 Environmental impacts	1	1	1	1
1.3.1.3 Influence of real-time distribution	1	3	2	6
1.3.1.4 Equipment installation problems.	5	3	3	45
2.1.1.1 Complication of operations	1	3	2	6
2.1.1.2 Improper management of personal information	5	1	2	10
2.1.2.1 Portability problem with existing terminal	1	1	1	1
2.1.3.1 Problem with security of right to access	1	3	2	6
2.1.3.2 Problem with safety of encryption	1	3	2	6
2.2.1.1 Problem in handling personal information	5	1	2	10
2.2.1.2 Deletion of personal information	5	1	2	10
2.2.1.3 User's incorrect deletion, alteration, etc.	1	3	2	6
2.2.1.4 General information disclosure	1	3	2	6
2.2.2.1 Problem with access except for a user	1	3	2	6
2.3.1.1 Breakage of device due to consumption	1	1	1	1
2.3.1.2 Communication failure	1	1	1	1
3.1.1 Regulation problem arising from revision of law	1	1	1	1
3.2.1 Data center collapses in a disaster	1	3	2	6
3.2.2 Problem providing compensation to user	1	3	2	6
Total				417

TABLE IV. RISK VALUE AFTER COUNTERMEASURES

Level 3: Risk Factors	Proposed countermeasure	Assets	Threat	Vulnerability		Value of Risk	
				Ideal	Actual	Ideal	Actual
1.1.1.1 Problem in cooperating with the existing system	Unapplied	5	3	3	3	45	45
1.1.1.2 Problem with ending Ambient Service	**Third -party Surveillance**	5	1	**0**	**1**	0	5
1.1.1.3 Problem with service entrepreneur's specifications	Unapplied	5	3	3	3	45	45
1.1.1.4 Problem with service entrepreneur's supervisor	**Third -party Surveillance**	5	1	**0**	**1**	0	5
1.1.1.5 Leaks, etc., by service entrepreneur	**Application of assurance**	5	1	**0**	**1**	0	5
1.1.1.6 Data deleted at end of service use	Unapplied	1	3	2	2	6	6
1.1.1.7 Problem with requirements for certification	Unapplied	1	3	2	2	6	6
1.1.1.8 Problem in managing personal information	Unapplied	1	3	2	2	6	6
1.1.1.9 Data seized by other company	**Application of assurance**	5	1	**0**	**1**	0	5
1.1.1.10 No restoration of missing data	Unapplied	1	1	1	1	1	1
1.1.1.11 No security management	**Application of assurance**	5	1	**0**	**1**	0	5
1.1.1.12 Leakage and disappearance of data	**Application of assurance**	5	1	**0**	**1**	0	5
1.1.1.13 Lack of internal control or security audit	Unapplied	1	1	1	1	1	1
1.1.2.1 Portability problem with existing hardware	Unapplied	1	3	2	2	6	6
1.1.3.1 Problem with fulfilling SLA	**Third-party surveillance**	5	1	**0**	**1**	0	5
1.1.3.2 Insufficient right-to-access management	Unapplied	1	3	2	2	6	6
1.2.1.1 Insufficient information disclosure	Unapplied	1	3	2	2	6	6
1.2.1.2 Problem with service specifications and user requirements	Unapplied	5	3	3	3	45	45
1.2.1.3 Crisis regarding continuation of service	**Application of assurance**	5	1	**0**	**1**	0	5
1.2.1.4 Business continuation plan is insufficient	**Application of assurance**	5	1	**0**	**1**	0	5
1.2.2.1 Compliance violation	**Third-party surveillance**	5	1	**0**	**1**	0	5
1.3.1.1 Power failure due to increased consumption	**Application of assurance**	5	1	**0**	**1**	0	5
1.3.1.2 Environmental impacts	Unapplied	1	1	1	1	1	1
1.3.1.3 Influence of real-time distribution	Unapplied	1	3	2	2	6	6
1.3.1.4 Equipment installation problems	Unapplied	5	3	3	3	45	45
2.1.1.1 Complication of operations	Unapplied	1	3	2	2	6	6
2.1.1.2 Improper management of personal information	**Third-party surveillance**	5	1	**0**	**1**	0	5
2.1.2.1 Portability problem with existing terminal	Unapplied	1	1	1	1	1	1
2.1.3.1 Problem with security of right to access	Unapplied	1	3	2	2	6	6
2.1.3.2 Problem with safety of encryption	Unapplied	1	3	2	2	6	6
2.2.1.1 Problem in handling personal information	**Third-party surveillance**	5	1	**0**	**1**	0	5
2.2.1.2 Deletion of personal information	**Third-party surveillance**	5	1	**0**	**1**	0	5
2.2.1.3 User's incorrect deletion, alteration, etc.	Unapplied	1	3	2	2	6	6
2.2.1.4 General information disclosure	**Application of assurance**	1	3	**0**	**1**	0	3
2.2.2.1 Problem with access except for a user	Unapplied	1	3	2	2	6	6
2.3.1.1 Breakage of device due to consumption	Unapplied	1	1	1	1	1	1
2.3.1.2 Communication failure	Unapplied	1	1	1	1	1	1
3.1.1 Regulation problem arising from revision of law	Unapplied	1	1	1	1	1	1
3.2.1 Data center collapses in a disaster	Unapplied	1	3	2	2	6	6
3.2.2 Problem providing compensation to user	**Third-party surveillance**	1	3	**0**	**1**	0	3
Total						**265**	**341**

C. *Results of evaluation*

Table 5 summarizes the results shown in Tables 3 and 4. Although only the "application of assurance" and "third-party surveillance" countermeasures were evaluated in this study, the table shows that the risk can be reduced by from 18% to 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 of Table 2. This study thus dealt with only two, i.e., "application of assurance" and "third-party surveillance," chosen on the basis of their practicality. In particular, the "application of assurance" countermeasure is being used in a Cloud user-oriented insurance service that began in 2012 in Japan [16], and "third-party surveillance" is carried out by certification businesses of ISMS.

However, as mentioned above, the problem of cost might also affect these countermeasures. Generally speaking, these countermeasures can become expensive because they need a specialist's knowledge. In the future, we will have to devise a verification considering such costs.

TABLE V. EVALUATION RESULTS

	Before countermeasure against risk factors (①)	After countermeasure against risk factors (②)	
		Ideal case	Actual case
Total risk value	417	265	341
Risk reduction rate = (①−②)/①	−	0.36	0.18

V. RELATED WORK

There has been a lot of research on the security of ambient services. However, each study has been an investigation in regard to the architecture of ambient networks. For example, some of the research targets the implementation of security functions, such as the authentication function [17]-[19], while other research deals with security policies [20].

On the other hand, this paper is a proposal about comprehensive security, which also includes the user side of an ambient service. Such research that takes into account the user side will be important for not only ensuring the security of ambient services but also for spreading new Internet services, such as cyber-physical systems and the IOT (the Internet of Things).

VI. CONCLUSION AND FUTURE WORK

We are interested in promoting ambient 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 "application of assurance" and "third party surveillance" in the previous study could reduce their corresponding risk factors by 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 execute further improvement of countermeasures, and verification of cost effectiveness. Furthermore, we will improve the granularity of the quantification. In particular, it is necessary to improve the granularity of the risk matrix to improve the granularity of the quantification. Thus, whereas in this paper, a general four division model was used as a risk matrix, we should improve the model so that it has at least nine divisions in the future.

ACKNOWLEDGMENTS

We would like to thank reviewers for valuable comments on this paper. This work was supported by the Japan Society for the Promotion of Science (JSPS, KAKENHI Grant Number 24300029).

REFERENCES

[1] Ministry of Public Management, Informatin & Communivcations Statistics Database, [Online]. Available from: http://www.soumu.go.jp/johotsusintokei/english/ 2014.12.30

[2] Osaka University, Center of Excellence for Founding Ambient Information Society Infrastructure, [Online]. Available from: http://www.ist.osaka-u.ac.jp/GlobalCOE/indexe_html?set_language=en 2014.12.30

[3] N. Wakamiya and M. Murata, "Introduction to Global COE Project: Center of Excellence for Founding Ambient Information Society Infrastructure," International Workshop on Nonlinear Theoretic Approach to Ambient Network, Oct., 2009. (Invited Talk)

[4] M. Murata, "Global COE Project: Center of Excellence for Founding Ambient Information Society Infrastructure," 14th Academic Exchange Seminar between Shanghai Jiao Tong University and Osaka University, (Shanghai, China), Oct., 2009.

[5] S. Tanimoto, et al., "Risk Management to User Perception of Insecurity in Ambient Service," 13th ACIS International Conference on Software Engineering, pp. 771-776, Aug. 2012

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

[7] 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

[8] M. S. Toosarvandani, N. Modiri, 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

[9] H. Sato et al., "Information Security Infrastructure," Kyoritsu Shuppan Co., Ltd., 2010, (in Japanese)

[10] 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

[11] Ambient Intelligence - Philips and ISTAG, [Online]. Available from: http://playstudies.wordpress.com/2010/12/01/ambient-intelligence-philips-and-istag/, 2014.12.30

[12] Towards Digital inclusion & innovation, [Online]. Available from: http://www.kantei.go.jp/jp/singi/it2/kongo/digital/dai9/9siryou2.pdf, 2014.12.30 (in Japanese)

[13] E. A. Lee, "Cyber Physical Systems: Design Challenges," 11th IEEE Symposium on Object Oriented Real-Time Distributed Computing, pp.363-369, May, 2008

[14] A. A. Cardenas, S. Amin, S. Sastry, "Secure Control: Towards Survivable Cyber-Physical Systems," Distributed Computing Systems Workshops, pp.495-500, Jun., 2008

[15] 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, Sep., 2014

[16] Mitsui Sumitomo Insurance, (in Japanese) [Online]. Available from: http://www.ms-ins.com/news/fy2011/news_0202_1b.html, 2015.1.4

[17] Mahdi Aiash, et al., "A Survey of Potential Architectures for Communication in Heterogeneous Networks," The IEEE Wireless Telecommunications Symposium, April 2012. London, UK.

[18] M. Lebre, et al., "Media Independent Transport Service for Ambient Intelligence," [Online]. Available from: https://ria.ua.pt/bitstream/10773/6601/3/A_Media_Independent_Transport_Service_for_Ambient_Intelligence.pdf, 2015.1.6

[19] A. F. Abate, M. D. Marsico, "MUBAI: multiagent biometrics for ambient intelligence," Journal of Ambient Intelligence and Humanized Computing, Jun. 2011, Vol. 2, Issue 2, pp 81-89, Springer

[20] O.Dohndorf, et al., "Adaptive and Reliable Binding in Ambient Service Systems," IEEE 16th Conference on Date of Conference, pp.1-8, Sept. 2011