IEICE TRANS. INF. & SYST., VOL.E99–D, NO.8 AUGUST 2016

INVITED PAPER Special Section on Security, Privacy and Anonymity of Internet of Things

Analysis of Privacy and Security Affecting the Intention of Use in Personal Data Collection in an IoT Environment

Remi ANDO[†], ***Nonmember***, **Shigeyoshi SHIMA**[†a)], ***Member***, ***and*** **Toshihiko TAKEMURA**[††], ***Nonmember***

SUMMARY In the current IoT (Internet of Things) environment, more and more Things: devices, objects, sensors, and everyday items not usually considered computers, are connected to the Internet, and these Things affect and change our social life and economic activities. By using IoTs, service providers can collect and store personal information in the real world, and such providers can gain access to detailed behaviors of the user. Although service providers offer users new services and numerous benefits using their detailed information, most users have concerns about the privacy and security of their personal data. Thus, service providers need to take countermeasures to eliminate those concerns. To help eliminate those concerns, first we conduct a survey regarding users' privacy and security concerns about IoT services, and then we analyze data collected from the survey using structural equation modeling (SEM). Analysis of the results provide answers to issues of privacy and security concerns to service providers and their users. And we also analyze the effectiveness and effects of personal information management and protection functions in IoT services.

key words: *IoT (Internet of Things), privacy, security, SEM (Structural Equation Modeling)*

1. Introduction

In recent years, various kinds of devices have been connected to the Internet. Those devices are called IoT (Internet of Things), and include, home electric appliances, vehicles, and fitness wearable devices, for example, in addition to PCs and Smartphones. Some service providers collect personal information from users' IoT and have already provided personalized (individual) services based on this collected personal information. For example, a user who wears a fitness device, may be able to obtain personal coaching and training from a service provider [1]. The service provider collects the user's fitness information (movement distance, calorie consumption and heart rate, etc.) from the fitness device through a Smartphone, and can provide the user fitness information and coaching advice through the Smartphone. In another example, if a user installs a Smart Meter system, which is a visualization system from the Tokyo Electric Power Co. (TEPCO), in his or her home, he or she can see actual energy consumption and electric power in real time every half hour [2].

Many kinds of new IoTs will be invented and 25 billion IoTs are forecast to be connected to the Internet by 2020 [3]. IoTs connected to the Internet may become part of the social and economic infrastructure in everyday use for millions of people. The lives of users will become more efficient using IoTs and IoT services, which will unlock incredible power, but their lives may also suffer from more threats and breaches of privacy. For example, IoTs might amplify the risk for surveillance and tracking. Specifically, many cases of threats using the Smartphone have been gradually spreading since 2010 in Japan. When a user installs a malicious application to a Smartphone, personal information stored in the Smartphone is stolen from the malicious application and is sent to an attacker by the malicious application [4]. The attacker will then abuse the stolen personal information for fraud and spoofing. In the case of a Social Network Service (SNS), if a person unaware of the consequences uploads personal information and photos of another person (a friend, or an entertainer, etc.), for example, that personal information and the photos of the other person will spread on the Internet through SNS to unintended people and the other person might feel that his or her privacy is violated. As the use of IoTs multiply in our lives, a service provider can collect our personal information and with this information, such as the e-commerce purchase history, the provider can link the Cyber world's personal information with real world personal information. Service providers can 'see' our detailed buying behaviors and other attributes of a specific user. The user may feel a privacy violation. Moreover, the service provider may leak the personal information of the user through Cyber-attacks or malicious insiders. The user may become the victim of crime when certain personal information is made known to an unintended party.

The purpose of this paper is to provide knowledge about certain issues of privacy and security concerns in IoT service creation. In doing so, we conduct a survey including questionnaire items designed for two scenarios regarding IoT services (crime-prevention service and preventive health-care service), and then analyze the data collected from the survey statistically.

2. Security and Privacy Concerns on IoT Services

This section describes privacy and security concerns related to IoT services.

2.1 An IoT Service Model

The IoT service definition used in this paper refers to the

Manuscript received December 14, 2015.
Manuscript revised April 12, 2016.
Manuscript publicized May 31, 2016.

[†]The authors are with Security Research Laboratories, NEC Corporation, Kawasaki-shi, 211–8666 Japan.
[††]The author is with Faculty of Economics, Saga University, Saga-shi, 840–8502 Japan.
a) E-mail: shima@ap.jp.nec.com

DOI: 10.1587/transinf.2015INI0002

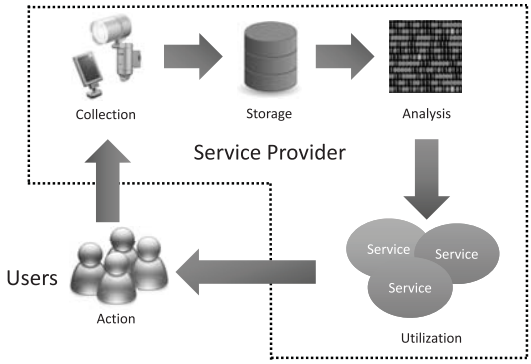


Fig. 1 Information flow of the IoT service.

service of providing individual services utilizing collected personal information from IoTs by a service provider. In the IoT services of a service provider, a flow model from collection to utilization is shown in Fig. 1.

Collection: The service provider collects personal information from a user's IoTs.

Storage: The service provider stores collected personal information in a database.

Analysis: The service provider analyzes the characteristic behavior of the user from stored personal information.

Utilization: The service provider uses the characteristic behavior for personal service and provides the user the personal service.

The information flow model is applicable not only to IoT services but also to existing services such as the recommendation services used in Internet shopping and the consulting services used in Internet banking. However, the target of information is different from existing services and IoT services.

Existing services are Cyber world information. IoT services are real world information. In the collection phase, an existing service generally collects personal information such as the behavior history and use history from the used service through a PC or a Smartphone. On the other hand, an IoT service collects personal information from many kinds of devices which can be worn on the user, or are found at home and in organizations, such as in the actual local community in which the user lives, for example. The service provider collects several kinds of personal information from the sensors of user devices such as the location information from the GPS of a Smartphone. The IoT service can accurately analyze intentions and thoughts as well as attributes of the user from a variety of types of personal information. Thus, the IoT service utilizes those intentions and thoughts and can provide the user with a variety of services. Moreover, the service provider can accurately analyze intentions and thoughts, and attributes of the user by linking the Cyber world personal information of the existing service (e-commerce, SNS, etc.) on the Internet to the real world personal information of the IoT service. However, the user may have the following privacy and security concerns with the service provider.

(1) Privacy Concern: Restrains a User's Liberty of Behavior

The service provider can comprehend the user's behavior patterns and favorite goods/services and items by analyzing stored personal information. The service provider may use this personal information for unexpected purposes such as the disclosure of a user's personal information and in turn, analyze results for an unintended organization and an unintended recipient of the user. Thus, the user may feel his or her privacy is attacked. The user then might decrease his or her use of the IoT service.

(2) Security Concerns: Loss by Information Leakage and Information Spread

Personal information and analysis results may become known to an unintended recipient of the user after the service provider leaks stored personal information and analysis results through Cyber-attacks or a malicious insider. Therefore, the user may become a victim of a crime such as fraud. Thus, the user might decrease his or her use of the IoT service.

2.2 Privacy and Security Awareness on IoT Service

In a survey on privacy and security awareness about IoT [5], users were asked whether the benefits of IoT outweighed the privacy and security risks. This result showed that 44% of respondents chose the benefits of IoT and 42% of respondents chose privacy or security over benefits, while 14% of respondents could not choose. From this result, however, the relationship between the two factors ("Benefit," vs. "Privacy"/"Security") and the use of IoTs could not be understood. Therefore, it is difficult for the service provider to create countermeasures which increase the intention of use.

2.3 Previous Research from the Technology Acceptance Model (TAM)

The Technology Acceptance Model (TAM) suggested by David is an adaptation of the Theory of Reasoned Action (TRA), and is an information systems theory that models how users come to accept and use a technology [6]. The model suggests that when users are presented with a new technology, their intention of use is influenced by factors such as perceived usefulness and perceived ease-of-use.

Pavlou showed that the perceived benefits to the user and the perceived risk to the user affected the intention of use in e-commerce [7]. The intention of use decreases when the perceived risk increases. The intention of use increases when the consumer trust increases. In addition, Kim analyzed the benefits of e-commerce and how the perceived risk of these services affected the intention of purchase from online services (Fig. 2) [8]. The intention of purchase decreases when the perceived risk increases. The intention of purchase increases when the benefit of IoT services increases.

We refer to Kim's TAM model based on a "valence framework" where "Intention of Purchase" is determined within the balance of "Perceived Risk" and "Perceived Benefit."

2.4 Reduction Factors of Privacy and Security Risk on IoT Services

Service providers are required to carry out an inspection by a third party and management of personal information by the user through laws and regulatory systems of personal information protection on the Internet. Nonetheless, the rapid changes in IoT technology often outpace the ability of associated legal and regulatory structures.

The inspection by a third party and the management of personal information by the user are important to service promotion because users who are concerned about privacy and security can use IoT services with less anxiety. For the inspection by a third party, Japanese service providers, for example, can indicate a PrivacyMark [9] (a seal of trust by the third party) on a website when Japanese service providers pass inspection of a personal information protection system. The purpose of the PrivacyMark is to eliminate anxiety about the privacy and security of the user[†]. Kumagai analyzed the relationship between the trust and the intention of use in the online services using personal information [10]. The result showed that the inspection by a third party (the third-party seal) heightened intention of use through trust. The benefits of a third party seal such as the PrivacyMark, however, are not known.

In the United Kingdom (the U.K.), "Midata," is primarily used in banking systems to manage personal information [12]. The service provider in Midata provides user management functions for the "Management of personal information by the user" so that the user can monitor and control his or her own personal information. Midata monitors and controls data about the user in the following way:

Monitoring: The user knows what personal information was collected about him or her.

Control: The user can control what amount and what type of this personal information is provided to the service provider.

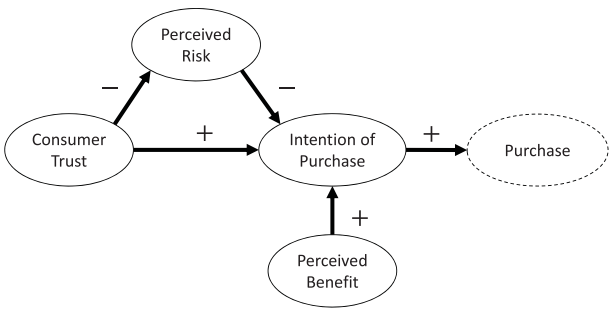


Fig. 2 Base model of Kim et al. [8].

[†]The PrivacyMark system to easily understand [11].

The management functions in Midata that serve for monitor and control may decrease the privacy risk perceptions and security risk perceptions of the user. However, the benefits of these management functions and which management functions are effective among these management functions is not known. Therefore, in this paper we analyze the benefits and effects of these management functions in IoT services.

3. Hypothesis

This section illustrates our proposed model for the evaluation of the users' privacy risk perceptions and security risk perceptions in Fig. 3. We refer to Kim's TAM model (Fig. 2), which was shown in Sect. 2.3. Note that in Fig. 3 "H*X*" indicates Hypothesis *X* and the sign "+" (resp. "−") in parenthesis means positive (resp. negative) effect.

- **Hypothesis (H1, H2, H3):** Kim's TAM model is based on a "valence framework" in which "Intention" is determined within the balance of "Perceived Risk" and "Perceived Benefit." As mentioned above, the valence framework is also applicable to our proposed model. In this paper, "Benefits of IoT" refers to the factor in which a user perceives the benefit of an IoT service. Perceived Risk corresponds with "Privacy Risk Perception" and "Security Risk Perception."

  "Privacy Risk Perception" is a factor in which the user perceives a privacy risk against the IoT service. "Security Risk Perception" is a factor in which the user perceives a security risk against the IoT service. Therefore, we suggest the hypothesis that "Benefits of IoT" positively affects "Intention (of Use)," and "Privacy Risk Perception" and "Security Risk Perception" negatively affect "Intention."
- **Hypothesis (H4, H5):** The trade-off relation between benefit and privacy and the trade-off relation between benefit and security is known generally. Our hypothesis illustrates how "Privacy Risk Perception" and "Security Risk Perception" negatively affect "Benefits of IoT."
- **Hypothesis (H6, H7):** Generally, the relation of privacy and security are treated ambiguously. In the survey cited in Sect. 2.2 [5], the relation of privacy and se-

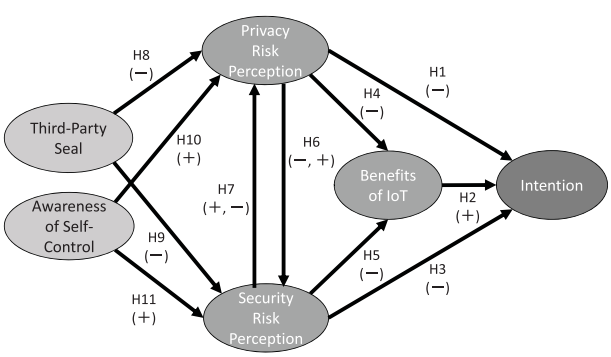


Fig. 3 Our proposed model.

curity is also unclear. However, this paper treats "Privacy Risk Perception" and "Security Risk Perception" as different factors because the characteristics of privacy and security have different characteristics. For example, although information leakage increases both "Privacy Risk Perception" and "Security Risk Perception," Cyber-attack countermeasures increase "Security Risk Perception" and decrease "Privacy Risk Perception." Moreover, we created the hypothesis that "Privacy Risk Perception" and "Security Risk Perception" affect both sides because the characteristics of privacy and security also have similar characteristics.

- **Hypothesis (H8, H9):** In Sect. 2.4, we discussed how a "Third-Party Seal" such as a PrivacyMark decreases "Privacy Risk Perception" and "Security Risk Perception." The "Third-Party Seal" in Fig. 3 is a factor such that a user feels the necessity of a third party. A user who feels the "Third-Party Seal" is important is sensitive to privacy and security risk.

  Thus, our hypothesis that a "Third-Party Seal" negatively affects "Privacy Risk Perception" and "Security Risk Perception."
- **Hypothesis (H10, H11):** In Sect. 2.4, we described how "Security Risk Perception" and "Privacy Risk Perception" decrease when the user can manage his or her personal information. Thus, by using personal information management functions, the user perceives decreased privacy and security risks. "Awareness of Self-Control" in Fig. 3 is a factor in which the user perceives his or her need to use personal information management functions in IoT services.

  Thus, we created the hypothesis that "Awareness of Self-Control" positively affects "Privacy Risk Perception" and "Security Risk Perception."

In each service, we estimate that the effects between factors may be different between each service. For example, a user may think security is more important than privacy and security is more beneficial in crime-prevention. In financial services, the user may think that privacy and security are more important than benefits such as operability and immediacy. On the other hand, in preventive health-care services, the user may feel that privacy is more important than security. Thus, in this paper we create two scenarios with our questionnaire survey and will compare the two analysis results in Sect. 5. Please refer to the two scenarios in Appendix.

4. Survey Design and Survey Summary

For the purpose of analyzing our proposed model using data collected from a survey, we conducted a survey entitled, "Survey about New Services for Internet Users" from the 12th to the 13th of September, 2015. The purpose of this survey was to grasp the individuals' awareness and intention to use the new service via the Internet. This survey contains 30 questionnaire items about scenarios related to (i) crime-prevention services and (ii) preventive health-care service, based on previous research in [10], [13]. In this survey, we gave the respondents 30 questionnaire items regarding the two scenarios, and these items were measured on a 5-Likert scale. Please refer to the two scenarios in Appendix.

The respondents of this survey were Japanese Internet users who were over 20 years old and knowledgeable about IoT services. In addition, the sample in this survey is arranged by age-group and gender. The number of the sample respondents is 1,660.

We employed the Internet (Web-based) survey as our survey method. Although this survey method inescapably contains certain weaknesses of data collection, it has been suggested that it is not necessarily undesirable to use an Internet survey if the aim of the survey is to offer beneficial information that is useful for individual and organizational decision-making [14]. We assume that these collected data are useful for a reasonable analysis.

5. Data Analyses and Results

For the two scenarios, to test our proposed model shown in Fig. 3, data analyses for both the measurement model and the structural model were performed using Structural Equation Modelling (SEM). This method analyzes structural equation models, including measurement and structural models with multi-item variables that contain direct, indirect, and total (interaction) effects. Please refer to [15] for the methodology of SEM in detail.

Before we tested our proposed model, we ensured the appropriateness of the research instrument by testing it for reliability.

5.1 Reliability

The assessment of the measurement model in Scenarios 1 and 2 includes the estimation of internal consistency for reliability. Generally, internal consistency was calculated using Cronbach's alpha. Table 1 shows the descriptive statistics for the constructs, the reliability (Cronbach's alpha) of the scales, and the sources from which they were adapted. The Cronbach reliability coefficients of all variables were higher than the minimum cutoff score of 0.7 [16]. All reliabilities of constructs had a value higher than 0.7. This indicates adequate internal consistency among variables.

5.2 Structural Model Assessment

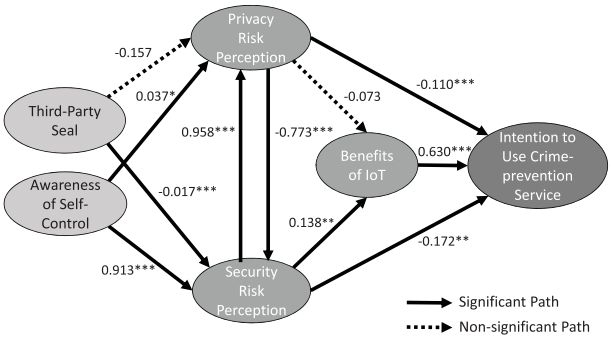
Figures 4 and 5 show the path diagrams for Scenario 1

Table 1 Results of Cronbach's coefficient alpha.

Construct	# of items	Scenario 1 Alpha	Scenario 2 Alpha
Benefits of IoT	4	0.886	0.894
Privacy Risk Perception	6	0.916	0.917
Security Risk Perception	7	0.920	0.930
Third-Party Seal	3	0.894	0.950
Awareness of Self-Control	4	0.916	0.942

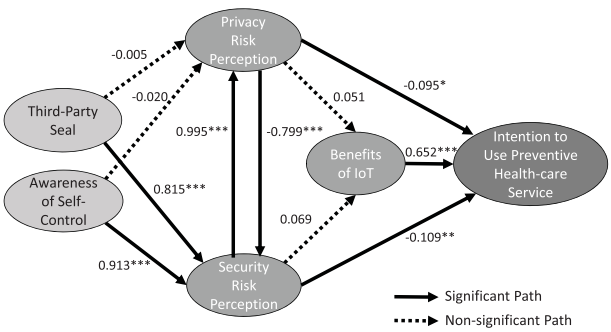
Table 2 Fitness of our proposed model.

			Range	
	Scenario 1	Scenario 2	Close fit	Poor fit
CFI	0.92	0.90	≥ 0.95	< 0.90
NFI	0.91	0.90	≥ 0.95	< 0.90
TLI	0.91	0.89	≥ 0.95	< 0.90
RMSEA	0.08	0.09	< 0.05	≥ 0.10



a) ***: $p < 1\%$, ** : $p < 5\%$* : $p < 10\%$

Fig. 4 Result of analysis: Scenario 1.



a) ***: $p < 1\%$, ** : $p < 5\%$* : $p < 10\%$

Fig. 5 Result of analysis: Scenario 2.

(crime-prevention service) and 2 (preventive health-care service), respectively. In addition, Table 2 shows the results regarding the fit of our proposed model for each scenario.

First, we assess the structural model by values of good fit such as CFI, NFI, TLI, and RMSEA, as shown in Table 2. This result indicates that our proposed model for Scenario 1 has a fair fitness of good, and the model for Scenario 2 has a mediocre fitness of good under our proposed model because the value of TLI is less than 0.9.

Next, we assess the relationship between components in our model by checking the standardized path coefficient of the structural model. The path coefficients shown in Figs. 4 and 5 are standardized. Therefore, in each structural model we can compare the magnitudes of the coefficients because the standardized path coefficient represents the magnitude of effects toward the other components.

Every path coefficient to "Intention" in Figs. 4 and 5 are statistically significant at least the 10% level. The coefficients from "Benefits of IoT" to the intention are positive, and the coefficients form both "Privacy Risk Perception" and "Security Risk Perception" to the intention are negative. This result implies that the more an individual perceives the benefits of IoT, the more s/he uses the IoT services, and that the more the privacy and security risk perceptions are increased, the less s/he intends to use the IoT services. In the two scenarios, Hypothesis 1, 2 and Hypothesis 3 are supported.

In Figs. 4 and 5 the path coefficients from "Privacy Risk Perception" to "Security Risk Perception" and the opposite path coefficients are statistically significant at a 1% level. The former signs are negative, and the latter signs are positive. This result implies that high privacy risk perception decreases security risk perception and that high security risk perception conversely increases privacy risk perception. Common to both scenarios, Hypothesis 6 and Hypothesis 7 are supported.

Common to Figs. 4 and 5, the path coefficients from a "Third-Party Seal" to "Security Risk Perception" and "Awareness of Self-Control" to "Security Risk Perception" are statistically significant at the 1% level. The sign of path coefficients from the "Third-Party Seal" to "Security Risk Perception" in Fig. 4 is negative, but the sign of the path coefficient in Fig. 5 is positive. With regard to the path coefficient from "Awareness to Self-Control" to "Security Risk Perception," the signs are positive. Hypothesis 9 is supported in Scenario 1, but the opposite result occurs in Scenario 2. Hypothesis 11 is supported in both scenarios.

In Fig. 4, the path coefficient from a "Third-Party Seal" to "Privacy Risk Perception" and the path coefficient from "Privacy Risk Perception" to "Benefits of IoT" are not statistically significant at the 10% level. In Fig. 5, four path coefficients, for example, from "Third-Party Seal" to "Privacy Risk Perception" and from "Security Risk Perception" to "Benefits of IoT," are not statistically significant at the 10% level. In common to these two scenarios, neither Hypothesis 4 nor Hypothesis 8 are supported. With regard to Scenario 2, Hypothesis 5 and Hypothesis 10 are also not supported.

Table 3 shows the direct effects, indirect effects, and total effects in each scenario. Direct effects are the effects that go directly from one factor to another factor. Indirect effects are the effects between two factors that are mediated by one or more intervening factors often referred to as a mediating factor(s) or mediator(s). The combination of direct and indirect effects makes up the total effect of the explanatory variable on the dependent variable.

Common to both scenarios, the total effect of Benefits of IoT stands out although there is only a direct effect. In addition, the direct effects of Privacy Risk Perception and Security Risk Perception do not make much difference, but their total effects are very different in each scenario.

Intriguingly, the signs and the absolute value of the total effect of the Third-Party Seal in Scenarios 1 and 2 are distinct. Furthermore, the indirect (and total) effect of Awareness of Self-Control is comparatively larger in each scenario.

Table 3 Direct/indirect effects and total effect.

	Direct effect	Indirect effect	Total
Scenario 1			
Benefits of IoT	0.630	—	0.630
Privacy Risk Perception	−0.110	0.066	−0.044
Security Risk Perception	−0.172	−0.018	−0.190
Third-Party Seal	—	0.003	0.003
Awareness of Self-Control	—	−0.168	−0.168
Scenario 2			
Benefits of IoT	0.652	—	0.652
Privacy Risk Perception	−0.095	0.087	−0.008
Security Risk Perception	−0.109	−0.095	−0.204
Third-Party Seal	—	−0.166	−0.166
Awareness of Self-Control	—	−0.186	−0.186

a) By assuming that the statistically insignificant path coefficients are zero, we calculate the magnitude of indirect and total effects.

5.3 Considerations

With regard to the use of intention in IoT services, the results of SEM reveal the following: In each scenario, among the three predetermined factors which directly affect the use of intention in IoT services, the effect of the "Benefits of IoT" is positive, but the effects of the remaining factors are negative. The absolute value of the "Benefits of IoT" is largest among them. On the other hand, if we make a comparison between "Privacy Risk Perception" and "Security Risk Perception," the absolute value of the former is larger than the absolute value of the latter.

Although Scenario 1 shows a positive effect is received from "Security Risk Perception" to "Benefits of IoT," Scenario 2 does not show this effect. In addition, the two scenarios do not accept the existence of the effect from "Privacy Risk Perception" to "Benefits of IoT" statistically.

Common to both scenarios, "Privacy Risk Perception" creates a negative impact on "Security Risk Perception." On the contrary, the former creates a positive impact on the latter. This implies that we have a trade-off relationship between them.

With regard to the predetermined factors to "Privacy Risk Perception," and "Awareness of Self-Control," only Scenario 1 creates a positive impact on "Privacy Risk Perception," but we cannot confirm that the other factors relate to "Privacy Risk Perception." On the other hand, with regard to the predetermined factors to "Security Risk Perception," the "Third-Party Seal" in each scenario creates a positive impact on "Security Risk Perception." Interestingly, although in Scenario 1, the "Third-Party Seal" creates a negative impact on "Security Risk Perception," the former creates a positive impact on the latter in Scenario 2. In consequence, the indirect or total effects from the "Third-Party Seal" to the intention to use IoT services differ from Scenarios 1 and 2.

Although we used the same model shown in Fig. 3 for Scenarios 1 and 2, the fitness of good in each scenario and statistically significant path coefficients were different, respectively. This implies that we have to distinguish models according to the contents of the IoT service. Particularly, we have to be careful about the indirect effect of the "Third-Party Seal."

6. Conclusions and Future Work

In this paper, we focused on issues of a users' privacy and security concerns in two IoT service scenarios, and used a statistical analysis method based on a questionnaire survey. In our analysis results, the strength of the users' perceptions of privacy risks and perceptions of security risks against personal information differ and the effect of countermeasures for the users' perceptions of privacy risks and security risks differ in the two IoT service scenarios. Thus, we estimate that the users' perceptions and the effect of the countermeasures differ for each type of IoT service. However, our analysis cannot cover all the countermeasures that can possibly decrease the users' perceptions of privacy and security risks. Thus, we need other types of countermeasures (e.g., data encryption, legal structures, hardware, etc.) and we need to conduct additional survey analysis for effective countermeasures.

Through our analysis model, a service provider can analyze the strength of users' perceptions of risks and the effects of countermeasures for an IoT service. The service provider should also consider contents including such factors as collection, storage, analysis, and utilization of data in the IoT service scenario when the service provider creates the IoT service scenario. In this way, the service provider can also consider analysis results and take countermeasures to decrease the users' perceptions of privacy and security risks when using IoT services. IoT services are spreading rapidly throughout society in many areas, and concomitantly, new methods to stop security and privacy risks are essential.

References

[1] Adidas, http://micoach.adidas.com/
[2] Press Releases of TEPCO, http://www.tepco.co.jp/en/press/corp-com/release/2015/1254972_6844.html
[3] Gartner, http://www.gartner.com/newsroom/id/2905717
[4] Information-technology Promotion Agency, Information Security White Paper, 2015.
[5] Ponemon Institute LLC, Privacy and Security in a Connected Life: A Study of US, European and Japanese Consumers, 2015.
[6] F.D. Davis, "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," MIS Quarterly, vol.13, no.3, pp.319–340, 1989.
[7] P.A. Pavlou, "Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model," International Journal of Electronic Commerce, vol.7, no.3, pp.101–134, 2003.
[8] D.J. Kim, D.L. Ferrin, and H.R. Rao, "A Trust-Based Consumer Decision-Making Model in Electronic Commerce: the Role of Trust, Perceived Risk, and Their Antecedents," Decision Support Systems, vol.44, no.2, pp.544–564, 2008.
[9] JIPDEC (Japan Information Processing Development Corporation), http://privacymark.org/index.html
[10] Y. Kumagai, S. Shima, T. Takemura, and A. Komatsu, "Factor Analysis about the Trust and the Use Intention in the Online Services Using Personal Information," Security Management, vol.27, no.2,

pp.3–15, 2013.
[11] The PrivacyMark system, http://privacymark.jp/reference/pdf/2014_04_wakaru_pmark.pdf (in Japanese)
[12] Department for Business Innovation and Skills, Review of the Midata Voluntary Programme, July 2014.
[13] Information-technology Promotion Agency, A Survey on Security and Privacy Risk Cognition and Perception toward eID, 2010.
[14] The Japan Institute for Labour Policy and Training, Can the Internet Survey Be Used for the Social Survey?: A Result by Experiment. Reports on Labour Policy, no.17, 2005.
[15] J. Wang and X. Wang, Structural Equation Modeling: Applications Using Mplus, Wiley, 2012.
[16] J.F. Hair, Jr., R.E. Anderson, R.L. Thatham, and W.C. Black, Multivariate Data Analysis, Upper Saddle River, Prentice-Hall International, 1998.

Appendix: Survey Questionnaires

A.1 Scenarios

Scenario 1 'A' city where you live collects information from crime prevention cameras set downtown and from the GPS on Smartphones. 'A' city introduces a service that allows the user to monitor strangers and watch the activities of their family. Using this service, they can check suspicious actions of strangers and the activities of their family even from outside the house using the Smartphone. However, the user is also monitored with monitor cameras because the user also lives in 'A' city. A matching data collection service that watches for suspicious activities is also provided by the local community through cameras.

Scenario 2 In the preventive health care service, the user's health care information which includes their living history, medicines, and addictions to certain medicines, exercise quantities, caloric intake, etc., are collected by medical institutions. Health care information of the user is monitored by medical institutions when the user wears a device (Smartphone, fitness device, etc.), and this information can automatically be recorded in a database by the medical institutions. An individual user can check his or her health care information by Smartphone, etc. The medical institution analyzes your health care information and provides advice for preventive health care if you chose to wear the device or use a Smartphone for this purpose.

A.2 Questionnaire Items

Questionnaire items for each scenario used in this paper are shown below:

Intention of Use

Do you intend to use this service?

(1: I want to use it, 2: I want to use it somewhat, 3: Difficult to say, 4: I do not want to use it somewhat, 5: I never want to use it.)

Benefits of IoT

What do you think about the following statements regarding this service?

1. This service will be a useful tool for me.
2. This service will result in improved quality of my life.
3. This service will promote more effective use of my time.
4. This service will be a useful tool for community safety.

(1: Agree completely, 2: Agree somewhat, 3: Difficult to say, 4: Disagree somewhat, 5: Disagree strongly)

Security Risk Perception

When you use this service, do you worry about the following possibilities (danger from the viewpoint of security)?

1. Someone invades the system and steals your personal information.
2. A surveillance camera without a password setting is connected to the Internet.
3. Your family member is the victim of crime through the abuse of stolen personal information.
4. In the future, information that is likely to create a disadvantage for you will be collected.
5. A service provider misrecognizes you and others.
6. You are misunderstood by friends or colleagues (you are seen as someone else).
7. A service provider abuses your personal information.

(1: Agree completely, 2: Agree somewhat, 3: Difficult to say, 4: Disagree somewhat, 5: Disagree strongly)

Privacy Risk Perception

When you use this service, do you worry about the following possibilities (dangers from the viewpoint of privacy)?

1. A third person (party) knows information about your family structure.
2. A third person (party) knows your place of residence.
3. A third person (party) knows your occupation.
4. A third person (party) knows your hobbies or favorite things.
5. Monitoring by security camera restricts your activities.
6. Your activities are monitored by a third person (party).

(1: Agree completely, 2: Agree somewhat, 3: Difficult to say, 4: Disagree somewhat, 5: Disagree strongly)

Third-Party Seal

We assume that the information collected from this service is managed by a public agency. Comparing the presence and the absence of a certification mark by an agency, how do you feel about the following statements?

1. I would want to use an agency with a certification mark rather than an agency without the mark.
2. I would feel reassured of privacy from an agency with a certification mark rather than an agency without the

mark.

3. I would feel reassured about the handling of information from an agency with a certification mark rather than an agency without the mark.

(1: Better, 2: Good, 3: Difficult to say, 4: Bad, 5: Worse)

Awareness of Self-Control

We assume that the information collected from this service is managed by a public agency. Although the agency collects the information, the information is utilized not only by the agency, but also by other organizations in which the service is provided. In this situation, do you feel the need for the following functions from a public agency?

1. The user can know what information was collected.
2. The user can control and handle the information by him or herself (for example, the agency should stop handling personal information).
3. The user can know the agency or organization or person who used his or her collected personal information.
4. The user can receive a message that someone used his or her personal information.

(1: very necessary, 2: necessary, 3: Difficult to say, 4: unnecessary, 5: I never need to know this information.)

Remi Ando was born in 1987. She received Bachelor of Science from Ochanomizu University (in 2010), Master Degree of Science from Ochanomizu University (in 2012). She is currently working as a researcher, Department of Central Research Laboratories, NEC Corporation, Japan. She is a member of the IPSJ. Security Research Laboratories, NEC Corporation, 1753, Shimonumabe, Nakahara-ku, Kawasaki, Kanagawa, 211–8666, Japan.

Shigeyoshi Shima was born in 1971. He received Bachelor of Science from Hirosaki University (in 1995), Master Degree of Information Science from Japan Advanced Institute of Science and Technology (in 1997), and his Ph.D. in applied engineering from the University of Electro-Communications (in 2012). He is currently working as a principal researcher, Department of Central Research Laboratories, NEC Corporation, Japan. His research interests include cyber security, system security, economics of information security. He is a member of the IEICE, IPSJ. Security Research Laboratories, NEC Corporation, 1753, Shimonumabe, Nakahara-ku, Kawasaki, Kanagawa, 211–8666, Japan.

Toshihiko Takemura was born in 1975. He received his Bachelor (in 1998) in Informatics from Kansai University, his Master Degree (in 2002) in Economics, and his Ph.D. (in 2006) in Applied Economics, from Osaka University. He is currently Associate Professor at Faculty of Economics, Saga University. His research interests include information and communication technology policy, economics of information security, medical safety culture, and behavioral economics. He is a member of the JEA, IPSJ, JSPUE, JSMI, JEPA and JSHA. Faculty of Economics, Saga University, 1 Honjo-machi, Saga-shi, Saga, 840–8502, Japan.