The influence of knowledge level in information security onto the factors of Anshin for online shopping users

Dai Nishioka
Iwate Prefecutural University
Takizawa-mura, Iwate, Japan
d.nishioka@comm.soft.iwate-pu.ac.jp

Yoshia Saito
Iwate Prefecutural University
Takizawa-mura, Iwate, Japan
y-saito@ iwate-pu.ac.jp

Yuko Murayama
Iwate Prefecutural University
Takizawa-mura, Iwate, Japan
murayama@iwate-pu.ac.jp

Abstract

In this research, we investigate users' subjective sense of security, which we call Anshin in Japanese. The research goal is to create a guideline of Anshin in information security for users. In this paper, we report how the user security knowledge level could influence the factors of Anshin for online shopping users. Traditional studies on security have been based on the assumption that users would feel the sense of security when provided with objectively secure systems. We conducted a Web survey with 920 subjects with our questionnaire. We divided the subjects into two groups which have low and high security knowledge level and analyzed each group. Then, we divided each group into two sub-groups and compare the result. As a result of the analysis, we extracted the similar factors between them. However, we found a difference between the two sub-groups in high security knowledge level groups. As a result, we conclude that there are different Anshin factors in accordance with the user security knowledge level. Moreover, we showed that Anshin factors might also affect other attributes when user security knowledge level is high.

1. Introduction

Anshin is a Japanese term that indicates the sense of security. It is composed of two words, viz. An and Shin. "An" is to ease, and "Shin" is mind. Anshin literally means to ease one's mind. Traditional research on security has been based on the assumption that users would feel Anshin when provided with secure systems. Sometimes the users would feel Anshin even with an insecure system. Rachna et al. [1] reported that 90% of users cannot distinguish between the authentic websites and phishing ones. The users would look at the contents on a website and judge whether the site could be a phishing site or not. Dhamija et. al [2] reported that the users would judge a website's legitimacy by its "look and feel".

On the other hand, the users may not necessarily feel Anshin even if they are safe. Kasperson et al. [3] reported that experts estimate risk based on objective numbers from previous statistics while ordinary users estimate risk based on subjective think because memorable events or images affect them. Luhmann [4] stated that there is a gap between what experts and ordinary users consider a risk is. Risk appraisal shows that users' attributes (e.g., age, sex, educational background, experience) are influencing as well. In Japan, security threats such as information leaks and phishing attacks are increasing and fewer people would feel Anshin on the use of the information technology compared to other countries [5].

According to these surveys, security and Anshin have different concept. Therefore, in this research, we are investigating Anshin factors for online shopping users. For the Anshin survey, we need to define the subject attributes. In previous study, we have been trying to derive the factors of Anshin using user surveys with questionnaires and factor analysis method [6] [7]. Then, we produced a questionnaire based on the preliminary survey result for users with security knowledge. However, the questionnaire did not reflect any feedback from users without security knowledge. Thus, in our previous research [8], we created the new questionnaire which reflects the feedback from the users without security knowledge. We extracted Anshin factors using the questionnaire and created an Anshin model based on those Anshin factors [9].

However, in previous work, the definition of security knowledge level is not clearly defined. Therefore, our contribution is to identify that the user security knowledge level affects Anshin factors about information security --i.e. Anshin factors are different between the users with the low level security knowledge and those with the high level. This paper is organized as follows. Section 2 presents the related works. Section 3 describes the summary of our previous works and problems emerge from it. Section 4 provides an overview in this survey. Section 5 presents Anshin factors in information security from each low and high level of security knowledge users. Section 6 explains the difference of Anshin factors corresponds

978-1-4799-2504-9/14 $31.00 © 2014 IEEE
DOI 10.1109/HICSS.2014.46

to the influence of user security knowledge level. Finally, the last section summarize the conclusion.

2. Related work

From a sociological viewpoint, Yamagishi [10] gave a distinct definition on Anshin and trust. Anshin is the belief that we have no social uncertainty, whereas trust is needed when we have high social uncertainty. Murakami [11] defined safety as what can be expressed with an objective numerical value -related to danger, and Anshin as subjective judgment of a user's danger. While security can be assessed quantitatively, Anshin has strong psychological and subjective aspects. Thus, it cannot be measured easily. One must conduct a survey including psychological and subjective aspects for the investigation of Anshin.

In information security technology, it is important to conduct a survey looking at human aspects. One of the typical examples of survey is social engineering [12]. Social engineering is an attack using non-technical methods that rely on human interaction to break security procedures. In western countries, the similar concept of Anshin is "trust," and it has been studied in the fields of psychology, philosophy, economics, and sociology. Barber [13] divided trust into trust for the ability of the partner and trust for the friendliness of the partner. In the latter case, the integrity correspondence of the partner is related to trust. Xiao [14] defined those two parts of trust in the field of e-commerce; there are trust that originates from a user's recognition and trust that originates from a user's emotion. Gambetta [15] defined trust as a level for a user to establish their subjectivity whether another user or group is favorable towards themselves. There is also a notion of trust with psychological, subjective aspects, and Lewis, et al. [16] considered the emotional part of trust as a major factor and position as irrational. We define Anshin as the emotional part of trust [17]. Marsh [18] has produced a computational trust model in which trust is quantified in the range of -1 and 1. Solomon et al. [19] defined that the range of what to trust is specified by the trustors. Riegelsberger [20] and Falcone et al. [21] argued that the affective reaction is crucial to decide whether to trust a person or not. Riegelsberger[20] described a basic trust model in which "trustor" is a person to trust and "trustee" is a trusted person. Trustor decides, based on trustee's ability and motivation, whether to trust the trustee or not. In addition, internalized norms and benevolence are included in trustee's motivation. Trustor judges whether to trust trustee or not, using trustee's temporary, social and institutional information. These surveys reported on the subjective factors, however, the surveys do not represent clear enough about subjective factors and models.

3. Previous work summary

We conducted our first survey with 452 students from Iwate Prefectural University using a questionnaire on Anshin when they used a security system or service on the Internet [6]. Most subjects were computer science students and only 100 were non-computer science students. As the result of the analysis, we had six factors: Security technology, Usability, Experience, Preference, Understanding, and Cognitive Trust. We also found that the structure of Anshin for users with technical knowledge is divided into two parts, environmental and personal part. With the later survey [7], we conducted a survey with the 756 local government officers without security knowledge, and there are five factors emerged: Cognitive Trust, Kindness, Understanding, Preference, and Familiarity. As the result from later survey pretest with 109 subjects who were local government officers, we had a feedback that they would like to have a specific scenario for the questionnaire. That is why we asked for the users ideas about Anshin when enter one's credit card information online shopping. With those surveys, we use a questionnaire which was produced based on the preliminary survey with the computer science students.

When we conduct a survey on Anshin about information security for ordinary people, it is important that the questionnaire reflects the ideas of users without security technical knowledge. However, the users without technical knowledge may not understand the ideas of information security. Therefore, to produce a new questionnaire we collected feedback from the users without technical knowledge. We collected users' viewpoints by conducting brainstorming [22] with groups of several people. Brainstorming is a group discussion technique to collect ideas. We thought that the users could suppose the security knowledge using brainstorming and we collected the ideas. In brainstorming, one can provide as much ideas as possible after listening to other ideas as well.

The collected feedbacks from brainstorming are subjective. If the collected feedback might change the question items, we need to examine whether the feedback reflect users without technical knowledge or not. However, ordinary user did not understand the meaning of the question which requires the technical knowledge. We sorted out the feedback using KJ method. The KJ method is a technique that can arrange subjective feedback and finally represent the feedback in a figure [23]. Using the figure, we can arrange subjective feedback, create question items, and we can

check the question items with users without technical knowledge. We conducted the preliminary survey with the new questionnaire twice. We examined whether we had problem with the question items or not using statistical analyses and improved the question items. Finally, we created a new questionnaire which consists of 34 question items. [8]

We conducted a Web survey with 1030 subjects with our new questionnaire. As the result of the factor analysis, we found four factors: “Perceived benevolence", "Perceived competence and integrity", "User’s intuition" and "Reputation of the company from third party”. A previous survey found that the structure of Anshin for users with technical knowledge is divided into two parts. [9] We surveyed whether the structure of Anshin for users without technical knowledge were divided into environmental and personal part. As a result, we showed that the structure of Anshin for users without technical knowledge is divided into environmental and personal part as well as in the previous survey.

However, in previous work, the definition of the knowledge level in information security was not clearly stated. Therefore, in this paper, we define the users’ security knowledge level, analyze and describe its relation with Anshin factors in information security.

4. User survey

We conducted a user survey through a web survey. The survey was conducted on 1030 subjects between 19-81 years of age, on the 22nd and 24th of February, 2011. The number of valid response was 920. 423 out of 920 subjects were male, and 497 were female. We show the average and the standard deviation which we calculated from a result of Web survey in Table 1.

We asked 34 questions for their ideas on Anshin about information security when using online shopping. (For example: “The service-provider company stipulates clearly the handling of private information.”, “The service-provider company has not caused major trouble in the past.”) Subjects were required to have a credit card and have experience with online shopping. In this questionnaire, we used a 7-point Likert scale, ranging from strongly agree 1 to strongly disagree 7. We asked subjects to check the security knowledge level of the subjects. These questions asked security risk and security measures from the surveys by Information-technology Promotion Agency, Japan [24] and Nomura Research Institute Secure Technologies [25].

For the analysis, we divided the subjects into two groups which is users with low and high level of security knowledge and analyzed each group. We graded the knowledge level using eight questions in Table 2. We have calculated the numbers of answer which subjects answered "I can explain the contents of this security risk" or "I implement this security measures". We defined these numbers as knowledge point.

Furthermore, we divided each group into two sub groups to validate the evidence of each Anshin factors in Table 3 and Table 4. We classified it so that the users knowledge point and male-to-female ratio, average age are about the same value between the same knowledge level. (Low level 1 : M:90 F:177 A:39.932, Low level 2 : M:96 F:170 A:40.030, High level 1 : M:120 F:74 A:40.319, High level 2 :M:117 F:76 A:40.129) In this research, we conduct three steps. Firstly, we conduct the factor analysis. Secondly, we conduct the comparison between the same level groups and finally conduct the comparison between the different level groups.

5. Factor analysis

5.1. Group 1 of low level

We conducted factor analysis for group 1 user with low security knowledge level which consisted of 266 subjects. We had two question items exhibiting a floor effect. Therefore, we conducted a factor analysis with thirty-two items after removing the two items. Furthermore, we remove three question items which had low commonality less than 0.25, and eleven question items which had factor loadings less than 0.5. Finally, we conducted factor analysis with eighteen items.

Factor analysis with the maximum-likelihood method and the promax rotation found that four factors are derived. The four factors were explained by 66.573% (Cumulative) as a total. To confirm reliability of measurement, Cronbach’s coefficient alpha of each subscale Factor one was 0.915, Factor two was 0.874, Factor three was 0.903 and Factor four was 0.866. We show factor loadings in Table 5. We identified the following factors:

Factor one is Perceived benevolence. This factor consists of fourteen items. It is a factor users feel Anshin when a company responds with benevolence in “the trouble that occurred from the user’s mistake” or “the user’s question”.

Factor two is User’s intuition. This factor consists of six items. It is a factor when users assess Anshin from “instinct” and “experience”.

Factor three is Perceived competence and integrity. This factor consists of four items. It is a factor the users feel Anshin when the company possesses competence not to let personal information leak out and the company performs personal information management integrity.

Taible.1 Amount of statistics from all subjects

No	QESTION	Avg.	S.D.
Q1S1	The service-provider company has social credibility.	2.04	1.13
Q1S2	The service-provider company is a major enterprise.	2.41	1.212
Q1S3	The service-provider company has reliable capability and achievements.	2.37	1.155
Q1S4	The service-provider company has not caused major trouble in the past.	2.26	1.144
Q1S5	The service-provider company is dealing in well-known merchandise presented on TV and in newspapers.	3.34	1.4
Q1S6	The service-provider company is presented on TV and in newspapers.	3.38	1.386
Q1S7	It is felt that the service-provider company is implementing measures to manage private information in an appropriate way.	2.3	1.179
Q1S8	It is felt that the service-provider company will not leak private information.	2.31	1.211
Q1S9	The service-provider company stipulates clearly the handling of private information.	2.25	1.18
Q1S10	The service-provider company clearly states a positive guarantee even if trouble should occur.	2.33	1.22
Q1S11	The service-provider company has not only an on-line shop but also an actual store.	3.31	1.418
Q1S12	It is felt that a mistake you make in operation or procedure will be treated leniently such as by cancellation of contract or willingness to refund money.	2.52	1.196
Q1S13	It is felt that a way to solve a mistake you make in operation or procedure is ready to help you.	2.46	1.192
Q1S14	In case of money trouble, the credit-card company offers security.	2.35	1.228
Q1S15	You feel the security is assured for the system used for the service.	2.16	1.131
Q1S16	You do not feel the system used for the service will leak the input card number outside.	2.09	1.165
Q1S17	You trust the technologies such as encipherment used in the system for the service.	2.21	1.142
Q1S18	You comprehend some degree of the technologies used for the service.	2.79	1.211
Q1S19	The system used for the service is easy to operate.	2.63	1.197
Q1S20	You can receive kind support for my questions regarding the operational methods of the system used for the service.	2.5	1.18
Q2S1	A lot of information is provided with pictures and texts regarding the details of commodities.	2.32	1.17
Q2S2	When I ask a question using the question form, I receive a prompt reply with content regarding my question not only a canned response issued by the automatic reply system.	2.42	1.166
Q2S3	When you make an inquiry to the call center, you can receive support from a communicable operator not only by the automated voice system.	2.58	1.258
Q2S4	You do not directly transact with the company providing the service, but a professional intermediate agent serves as go-between.	3.37	1.242
Q2S5	You can choose a payment method not limited to credit payment but others such as cash on delivery.	2.74	1.416
Q2S6	The information necessary for you is indicated in an easily understood manner.	2.17	1.039
Q2S7	The overall design of the homepage is in tune with your taste.	3.57	1.392
Q2S8	You family members, friends, colleagues and other acquaintances using this shopping mall give high evaluation such as good words of mouth.	2.81	1.278
Q2S9	You are accustomed to using a similar system.	3.12	1.139
Q2S10	You feel no problem with the system on the basis of your experience of using a similar system.	3.14	1.154
Q2S11	You generally feel safe about it without any concrete reason.	3.33	1.258
Q2S12	You like it without any concrete reason.	3.44	1.244
Q2S13	Proper security measures are implemented on your own computer which you are using.	2.78	1.171
Q2S14	You have knowledge to the risks and menaces accompanying with Internet trading.	2.93	1.072

Taible.2 Knowledge level (all subjects)

	Low level				High level				
Knowledge point	0	1	2	3	4	5	6	7	8
Number of subjects	29	42	257	205	176	131	42	6	32
Total	533				387				

Taible.3 Knowledge level (low level subjects)

	Low group 1				Low group 2			
Knowledge point	0	1	2	3	0	1	2	3
Number of subjects	15	21	128	103	14	21	129	102
Total	266				267			

Taible.4 Knowledge level (High level subjects)

	High group 1					High group 2				
Knowledge point	4	5	6	7	8	4	5	6	7	8
Number of subjects	88	66	21	3	16	88	65	21	3	16
Total	194					193				

Taible.5 Factor pattern matrix from low level 1

No.	Factor			
	1	2	3	4
Q1S14	.935	-.102	-.101	-.100
Q1S13	.862	-.017	.034	-.110
Q1S15	.774	-.060	.165	-.083
Q1S12	.697	.007	.146	-.073
Q1S20	.658	.080	.141	.102
Q1S19	.640	.143	.027	.103
Q2S3	.601	-.069	-.134	.247
Q2S2	.551	.100	-.064	.137
Q1S17	.500	.083	.281	-.056
Q2S11	-.175	.960	.114	-.060
Q2S12	-.156	.932	.015	.031
Q2S10	.263	.631	-.117	.021
Q2S9	.319	.576	-.126	-.005
Q1S8	-.046	.032	.991	-.025
Q1S7	.083	.003	.820	.021
Q1S9	.191	-.117	.645	.113
Q1S6	-.066	.034	.042	.876
Q1S5	.024	-.046	.021	.861

Factor four is Reputation of the company from a third party. This factor consists of five items. It is a factor the user assesses Anshin based on information from a third party.

5.2. Group 2 of low level

We conducted factor analysis for group 2 user with low security knowledge level which consisted of 267 subjects. We had two question items exhibiting a floor effect. Therefore, we conducted a factor analysis with thirty-two items after removing the two items. Furthermore, we remove three question items which had low commonality less than 0.25, and fourteen question items which had factor loadings less than 0.5. Finally, we conducted factor analysis with fifteen items. The four factors were explained by 68.692% as a total. To confirm reliability of measurement, Cronbach's coefficient alpha of each subscale Factor one was 0.912, Factor two was 0.910, Factor three was 0.865 and Factor four was 0.799. We show factor loadings in Table 6. We identified the following factors:

Factor one is Perceived benevolence. This factor consists of thirteen items. It is a factor users feel Anshin when a company responds with benevolence in "the trouble that occurred from the user's mistake" or "the user's question".

Factor two is Reputation of the company from a third party. This factor consists of six items. It is a factor the user assesses Anshin based on information from a third party.

Factor three is Perceived competence and integrity. This factor consists of four items. It is a factor the users feel Anshin when the company possesses competence not to let personal information leak out and the company performs personal information management integrity.

Factor four is User's intuition. This factor consists of six items. It is a factor when users assess Anshin from "instinct" and "experience".

Taible.6 Factor pattern matrix from low level 2

No.	Factor			
	1	2	3	4
Q1S13	.992	-.074	.007	-.027
Q1S12	.940	-.021	-.030	.000
Q1S14	.775	-.026	.045	.010
Q1S15	.515	.322	-.003	.086
Q1S7	-.072	.946	.014	.032
Q1S8	-.058	.942	.004	.031
Q1S9	-.013	.818	.038	-.035
Q1S10	.267	.569	.000	-.064
Q1S2	-.051	-.125	1.042	-.012
Q1S3	-.021	.081	.828	.024
Q1S5	.099	.144	.508	.021
Q1S6	.092	.146	.503	-.062
Q2S12	.010	-.065	.049	.972
Q2S11	-.007	.037	-.044	.814
Q2S7	.004	.035	-.025	.534

5.3. Group 1 of high level

We conducted factor analysis for group 1 user with high security knowledge level which consisted of 194 subjects. We had eight question items exhibiting a floor effect. Therefore, we conducted a factor analysis with twenty-six items remove eight items. Furthermore, we remove five question items which had low commonality less than 0.25, and five question items which had factor loadings less than 0.5. Finally, we conducted factor analysis with fourteen items.

Factor analysis with the maximum-likelihood method and the promax rotation found that five factors are derived. The five factors were explained by 70.972% as a total. To confirm reliability of measurement, Cronbach's coefficient alpha of each subscale Factor one was 0.871, Factor two was 0.772,

Factor three was 0.931, Factor four was 0.907 and Factor five was 0.856. We show factor loadings in Table 7. We identified the following factors:

Factor one is Perceived benevolence. This factor consists of eleven items. It is a factor users feel Anshin when a company responds with benevolence in "the trouble that occurred from the user's mistake" or "the user's question",

Factor two is Familiarity. This factor consists of four items. It is a factor users feeling familiarity for service from past experience or collective impression.

Factor three is User's intuition. This factor consists of three items. It is a factor when users assess Anshin from "instinct" and "experience".

Factor four is Reputation of the company from a third party. This factor consists of three items. It is a factor the user assesses Anshin based on information from a third party.

Factor five is Confidence in society. This factor consists of three items. Mainly, it has feeling confidence in society and trust by user expectation.

Taible.7 Factor pattern matrix from high level 1

No.	Factor				
	1	2	3	4	5
Q1S13	.961	-.096	.009	-.009	.005
Q1S12	.904	-.068	.014	-.048	-.053
Q1S14	.758	-.052	-.014	.039	-.038
Q1S20	.514	.215	.046	.037	.120
Q2S2	.504	.287	-.051	.022	.037
Q2S9	-.012	.996	-.097	.060	-.091
Q2S10	-.061	.746	.155	-.105	.056
Q2S8	.027	.528	.012	-.006	.024
Q2S11	-.025	.002	.999	.004	.016
Q2S12	.032	.031	.847	.025	-.044
Q1S6	-.052	.002	-.012	1.016	.003
Q1S5	.067	-.032	.042	.803	.016
Q1S3	.028	-.031	-.027	-.061	.952
Q1S2	-.055	.012	.002	.095	.796

5.4. Group 2 of high level

We conducted factor analysis for group 2 user with high security knowledge level which consisted of 193 subjects. We had four question items exhibiting a floor effect. Therefore, we conducted a factor analysis with thirty items remove four items. Furthermore, we remove six question items which had low commonality less than 0.25, and eight question items which had factor loadings less than 0.5. Finally, we conducted factor analysis with sixteen items.

Factor analysis with the maximum-likelihood method and the promax rotation found that five factors are derived. The five factors were explained by 71.276% as a total. To confirm reliability of measurement, Cronbach's coefficient alpha of each subscale Factor one was 0.923, Factor two was 0.832, Factor three was 0.861, Factor four was 0.839 and Factor five was 0.913. We show factor loadings in Table 8. We identified the following factors:

Factor one is Perceived competence. This factor consists of four items. It is a factor the users feel Anshin when the company possesses competence not to let personal information leak out.

Factor two is Usability. This factor consists of six items. Especially, it has subjective assessment of the quality of UI. This factor represents not only usability from the viewpoint of information technology but also in terms of online shopping as a whole.

Factor three is Confidence in society. This factor consists of four items. Mainly, it has feeling confidence in society and trust by user expectation.

Factor four is User's intuition. This factor consists of five items. It is a factor when users assess Anshin from "instinct" and "experience".

Factor five is Compensation. This factor consists of five items. It is a factor users feel Anshin when a company receive compensation in "the trouble that occurred from the user's mistake".

Taible.8 Factor pattern matrix from high level 2

	Factor				
	1	2	3	4	5
Q1S8	1.002	-.063	-.009	.000	-.021
Q1S7	.931	-.106	.089	.041	-.033
Q1S9	.777	.206	-.012	-.012	-.076
Q1S10	.597	.072	-.045	-.035	.290
Q1S19	-.062	.868	-.047	.076	-.023
Q1S20	.036	.868	.026	-.060	.014
Q1S18	.074	.648	.012	-.069	.063
Q2S13	-.018	.517	.116	.154	.022
Q1S3	-.012	.051	.893	-.042	.037
Q1S2	-.045	.020	.792	.017	.005
Q1S1	.159	-.036	.703	.019	-.039
Q2S11	.046	-.096	-.046	.948	.050
Q2S12	-.040	-.006	.055	.845	-.004
Q2S10	.011	.337	-.026	.519	-.059
Q1S12	.000	-.039	.070	.021	.907
Q1S13	-.008	.076	-.057	-.002	.903

6. Comparison survey

6.1. Low level groups

As a result of factor analysis, we extracted four Anshin factor about information security from users with low security knowledge level group 1 and 2. Meaning of these, the Anshin factors were same. But, these factors have slightly different in factor number and values of the factor loading. However, the factor analysis that we conducted in the previous section was an exploratory factor analysis. Therefore, in order to verify the four factors, we need to conduct a

confirmatory factor analysis (CFA)[26] using Structural Equation Modeling (SEM). SEM is a statistical technique for theoretical models, which are called causal models [27]. It is a hybrid technique that encompasses aspects of confirmatory factor analysis, path analysis, and regression, which can be seen as special cases of SEM.

We assumed observation variables to be three items of high factor loading in each of the four factors and the covariance between the four factors. We used data of group 2 to examine the validity of the Anshin factor on group 1. Furthermore, we used data of group 1 to examine the validity of the Anshin factor on group 2. As a result of validity of group 1, we found that the overall fit of the models were acceptable with GFI (0.933) , CFI (0.961) , RMSEA (0.078) . As a result of validity of group 2, we found that the overall fit of the models were acceptable with GFI (0.936) , CFI (0.967) , RMSEA (0.072) . The models have a close fit by the criteria indicated: RMSEA below 0.08[28], CFI and GFI above 0.9 [29]. Therefore, it verified the validity of the four Anshin factors. We show result of confirmatory factor analysis of low level group 1and 2 in Fig 1 and Fig 2.

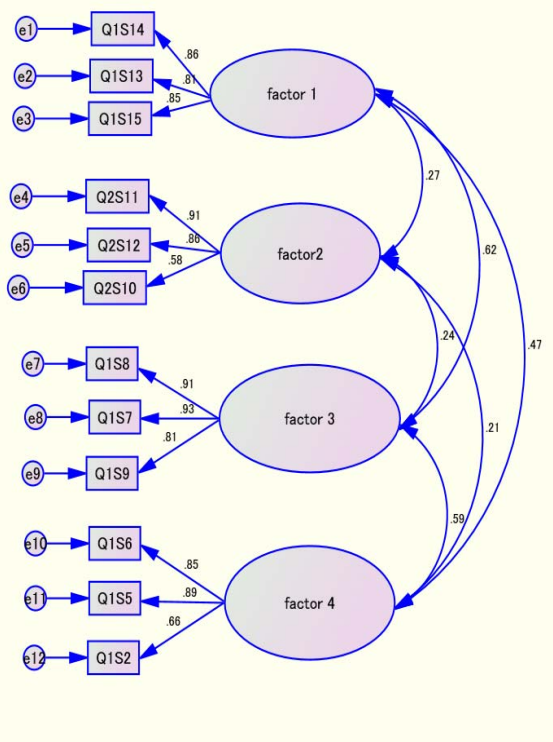

Fig 1. Result of confirmatory factor analysis from group 1 of low level

6.2. High level groups

As a result of factor analysis, we extracted five Anshin factor about information security from users with high security knowledge level group 1 and 2. Meaning of these, the Anshin factors were different.

We conducted the similar analysis as the low level groups. We assumed observation variables to be three items of high factor loading in each of the five factors and the covariance between the five factors. We used data of group 2 to examine the validity of the Anshin factor on group 1. Furthermore, we used data of group 1 to examine the validity of the Anshin factor on group 2.

As a result of validity of group 1, we found that the overall fit of the models were not acceptable with GFI (0.893) , CFI (0.929) , RMSEA (0.081) . As a result of validity of group 2, we found that the overall fit of the models were not acceptable with GFI (0.892), CFI (0.941), RMSEA (0.080). We show result of confirmatory factor analysis of high level group 1and 2 in Figure 3 and Fig 4.

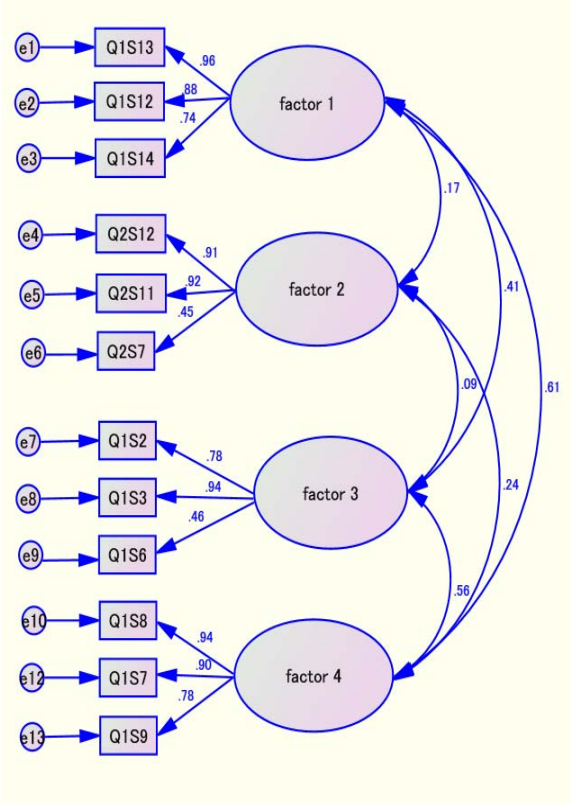

Fig 2. Result of confirmatory factor analysis from group 2 of low level

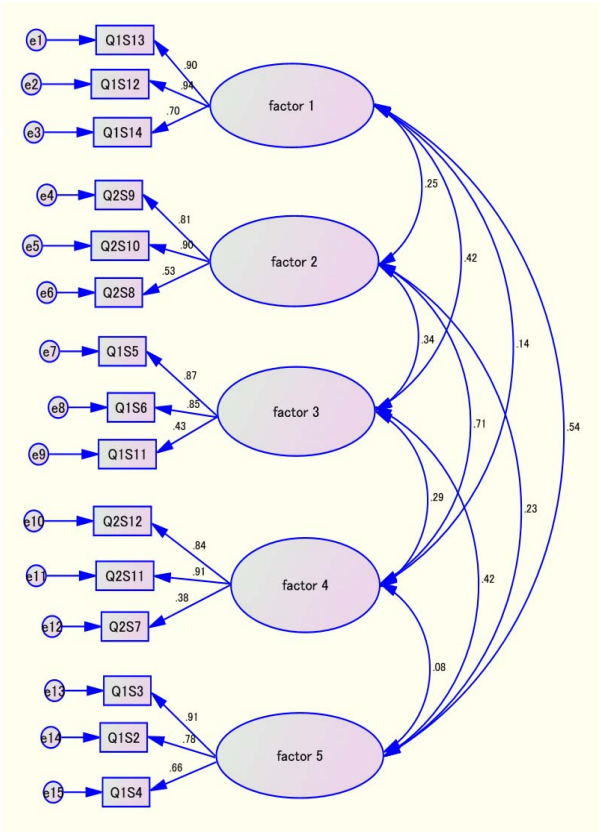

Fig 3. Result of confirmatory factor analysis from group 2 of high level

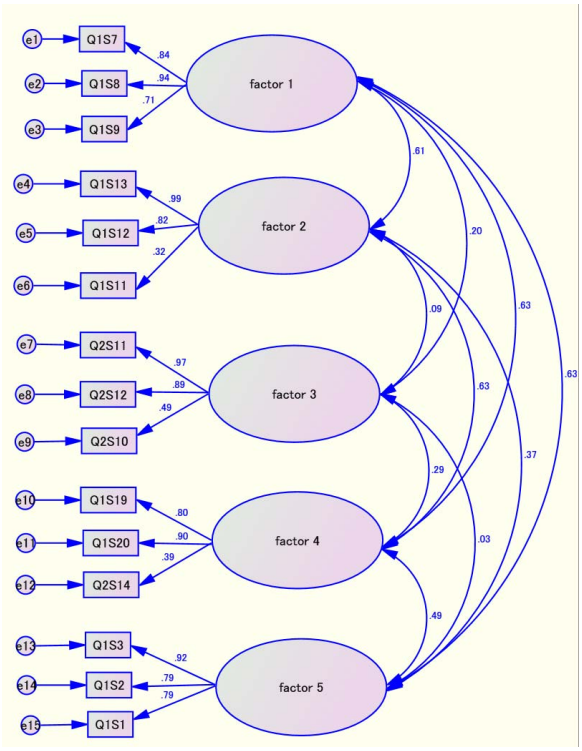

Fig 4. Result of confirmatory factor analysis from group 2 of high level

7. Discussion

As a result of factor analysis, we extracted four Anshin factors about information security from low security knowledge level groups, and five factors of Anshin about information security from high security knowledge level groups. We show Anshin factors from all groups in table 9.

Taible.9 Anshin factors

	Low 1	Low 2	High 1	High 2
Perceived benevolence	✔	✔	✔	-
User's intuition	✔	✔	✔	✔
Perceived competence and integrity	✔	✔	-	-
Reputation of the company from a third party	✔	✔	✔	-
Familiarity	-	-	✔	-
Confidence in society	-	-	✔	✔
Perceived competence	-	-	-	✔
Compensation	-	-	-	✔
Usability	-	-	-	✔

Legend: "✔" indicates that the group have Anshin factor.

Meaning of Anshin factors from low security knowledge level groups were same and Anshin factors from high security knowledge level groups were different. In addition, we found the difference factors between the low and high security knowledge level group.

Therefore, we found that Anshin factors changed under the influence of the user security knowledge level, because Anshin factors were different between low and high security knowledge level groups. However, the influence on the Anshin factors in high security knowledge level did not clear. It showed that Anshin factors might affect the other attributes rather than the security knowledge when user's security knowledge level is high, because Anshin factors were different between high level of security knowledge group 1 and 2. For example, it is reported that the user experience [30] affect trust. Furthermore, from the survey between man and woman ratio, low security knowledge level users consist of 34.9% man, 65.1% woman whereas for the high security knowledge level users, the man is 61.2% and 38.8% woman. Thus, we will survey the influence of the user experience and gender for future works.

As a result of previous work, we showed the possibility that Reputation of the company from a third party factor is Anshin factors for the users without information security knowledge. In addition, as a result of this survey, we showed the possibility that reputation of the company from a third party factor is not a Anshin factor for the users with high security knowledge level, because this factor was not included in group 2 of high level.

From the above, it is thought the user of low security knowledge level feel Anshin and purchase the products based on information from third party. This action is similar to imitation [31] and same behavior [32] based on sociology, psychology and behaviorist psychology.

In Japan, phishing have increased despite the heads-up of government or service provider [33]. In this case, it is thought that user of low security knowledge level feel Anshin without distinguishing the authentic websites and phishing ones based on false information from third party, and user purchase a products in imitation behavior of false information. Therefore, it is dangerous to give the Anshin about Reputation of the company from a third party for user with low security knowledge level.

For fishing measures, we thought that the heads-up is not effective for the user with low security knowledge level. Hence, as a solution to this problem, we propose an interface causing discomfort for security in our different survey. [34] This research is to implement an interface with which one would feel discomfort so that she/he would be aware of security risks.

8. Conclusion

Information security is no longer limited to technical issues but human factor issues such as trust and a sense of security are required by the user. In this paper, we reported the results from our analysis on the relations between Anshin factors about information security and security knowledge level. We showed that Anshin factors were different according to the user's security knowledge level. Furthermore, we showed that Anshin factors might affect the other attributes than the security knowledge when the user security knowledge level is high. Implication is that it would be easier to deal with the users with low security knowledge level compared to those with the high security knowledge level for service provider.

As the future work, we shall survey the relationship between other user attributes and Anshin factors. We will create a guideline of providing Anshin in information security for users.

Acknowledgment

Our appreciation goes to anonymous reviewer whose comments were innumerably valuable throughout the course of our study. We are indebted to Ms. Nor Athiyah Binti Abdullah for writing assistance. This work was supported by JSPS KAKENHI Grant Number 21300026.

9. References

[1] Rachna, D. J. D. Tygar. Marti H., Why Phishing Works. In Proceedings of the Conference on Human Factors in Computing Systems pp.581-590, (CHI2006).

[2] Dhamija, R., J. D. Tygar. and M. Hearst., Why phishing works. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems CHI '06. ACM Press, pp.581-590 (2006).

[3] Kasperson, R. E., Renn, O., Slovic, P., Brown, H. S., Emel, J., Goble, R., Kasperson, J. X., and Ratick, S., The social amplifi cation of risk: A conceptual framework. Risk Analysis, vol. 8, pp.177-187, (1988)

[4] Luhmann,N., Soziologie des Risikos ,Walter de Gruyter. (1991)

[5] Ministry of internal affairs and communications: White Paper on Local Public Finance, 2009, http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h21/index.html, 2009 (in Japanese)

[6] Hikage, N., Hauser, C. and Murayama, Y., A Statistical Discussion of the Sense of Security, Anshin, Information Processing Society of Japan Journal Vol.48 No.9, pp. 3193-3203, 2007

[7] Fujihara. Y., Yamaguchi. K., Y., Murayama. Y., A Survey on Anshin of the Users without Technical Knowledge on Information Security, Information Processing Society of Japan Journal Vol.50 No.9, pp2207-2217, 2009

[8] D. Nishioka, Y. Murayama and Y. Fujihara, Producing a Questionnaire for a User Survey on Anshin with Information Security for Users without Technical Knowledge, 45th Hawaii International Conference on System Sciences(HICSS-45), pp.454-463 (2012).

[9] Nishioka, D., Saito, Y. and Murayam, Y., A Model of Anshin about the Information Security, 46th Hawaii International Conference on System Sciences(HICSS-46), pp.305-314 (2013).

[10] Yamagishi, T. and Yamagishi, M. 1994. Trust and commitment in the United States and Japan. Motivation and Emotion 18, 129-166.

[11] Youichirou M., Science of Safty and Anshin, SHUEISHA, 2005(in Japanese)

[12] The Knightmare: Secrets Of Super Hacker, Loompanics Unlimited, 1994

[13] Barber, B. : The Logic and Limits of Trust, Rutgers University Press, New Brunswick, N.J,(1983)

[14] Xiao, S. and Benbasat, I.: Understanding Customer Trust in Agent-Mediated Electronic Commerce, Web-Mediated Electronic Commerce, and Traditional Commerce, Information Technology and Management, Vol.4, No.1– 2, Kluwer Academic Publishers, pp. 181–207 (2004). .

[15] D. Gambetta: Can we trust trust?, Making and Breaking Cooperative Relations, electronic edition, Department of Sociology, University of Oxford, chapter 13, pp. 213-237 (1988).

[16] Lewis, David J., & Andrew Weigert. "Trust as a social reality," Social Forces, Vol.63(4) , pp. 967-985(1985).

[17] Y. Murayama, N. Hikage,Y. Fujihara and C. Hauser: The structure of the sense of security, Anshin, Proc. of CRITIS 2007, pp. 85-96 (2007).

[18] S.P. Marsh: Formalising trust as computational concept, PhD Thesis, Department of Mathematics and Computer Science, University of Stirling (1994).

[19] Robert C. Solomon and Fernando Flores. Building Trust. Oxford University Press, 2001.

[20] Jens Riegelsberger, M. Angela Sasse, John D. McCarthy, The mechanics of trust: a framework for research and design, International Journal of Human-Computer Studies, vol. 62, pp381-422, (2005).

[21] Rino Falcone and Cristiano Castelfranchi. A belief-based model of trust. In Trust in Knowledge Management and Systems in Organizations, chapter XI, pp. 306–343. Idea Group Publishing, 2004.

[22] Alex F. Osborn: YOUR CREATIVE POWER, Motorola Univ Pr; abridged edition (1948）.

[23] Kawakita, J.,*The KJ method - A scientific approach to problem solving,* Technical report. Tokyo: Kawakita Research Institute (1975).

[24] Information technology Promotion Agency Japan: Resarch for threat about information security, 2009 http://www.ipa.go.jp/security/fy21/reports/ishiki/index.html (in Japanese, Last visit 2013/6/15)

[25] NRI secure technologies : Research for Internet user about information security, 2008 http://www.nri-secure.co.jp/news/2008/0522_report.html (in Japanese, Last visit 2013/6/15..

[26] Tim, K., Eamonn, O., Chris, B., Vassilis, K., Danae, S.F., Tim, J., Measuring Trust in Wi-Fi Hotspots, Proc of the 26th annual SIGCHI conference on Human factors in computing systems (CHI 2008), pp.173-182, (2008).

[27] Jennifer King, Airi Lampinen and Alex Smolen, Privacy: Is There An App For That?, Symposium On Usable Privacy and Security(2011)

[28] Jöreskog, K. G., A general approach to confirmatory maximum likelihood factor analysis, *Psychometrika*, Vol.34, No.2, pp. 183-202. (1969)

[29] Hoyle, Rick H., Structural Equation Modeling: Concepts, Issues, and Applications, *Sage Publications* (1995).

[30] Tim, K., Eamonn, O., Chris, B., Vassilis, K., Danae, S.F., Tim, J., Measuring Trust in Wi-Fi Hotspots, Proc of the 26th annual SIGCHI conference on Human factors in computing systems (CHI 2008), pp.173-182, (2008).

[31] Tarde, J. G., *Le lois de l'imitation: Etude sociologique*, Alcan(1890).

[32] Miller, N. E. and Dollard, J., *Social Structure,* Free Press (1949).

[33] Council of Anti-Phishing Japan, phishing report 2012 , https://www.antiphishing.jp/report/pdf/phishing_report_2012.pdf (in Japanese, Last visit 2013/6/15)

[34] Fujihara, Y., Oikawa, H. and Murayama, Y.:Towards an Interface causing Discomfort for Security: A User Survey on the Factors of Discomfort, SSIRI '08 Proceedings of the 2008 Second International Conference on Secure System Integration and Reliability Improvement, pp.173-174(2008).