Exploratory survey on an evaluation model for a sense of security

Natsuko Hikage [1*], Yuko Murayama [1] and Carl Hauser [2]

[1] Graduate school of Software and Information Science,
Iwate Prefectural University
152-52, Sugo, Takizawa-mura, Iwate 020-0193 JAPAN
n.hikage@comm.soft.iwate-pu.ac.jp, murayama@iwate-pu.ac.jp

[2] School of Electrical Engineering and Computer Science,
Washington State University
PO Box 642752, Pullman, WA 99164-2752 USA
hauser@eecs.wsu.edu

Abstract. Research in information security is no longer limited to technical issues: human-related issues such as trust and the sense of security are also required by the user. In this paper, we use a Japanese word for such feelings, Anshin; "An" means to ease, and "Shin" is to mind. One feels Anshin when he is free from worry and fear. We try to identify the factors of Anshin so that we can construct a framework of the evaluation of Anshin. We present an initial Anshin model, and report our recent research results from user survey with factor analysis. We derive the following factors from the analysis; 1) user expectation of trust and confidence, 2) satisfaction with user interface and 3) understanding of risk and threats from user experience as well prior knowledge.

1 Introduction

This paper presents our initial work on the sense of security. Security technology usually has been evaluated in terms of theoretical and engineering feasibility and mostly from service providers' viewpoints, e.g.[1-3]. What has been missing is evaluation from users' viewpoints. Usability is one of the factors, but not only in engineering terms, but in terms of the users' subjective feeling in use of security tools --i.e., the sense of security. Indeed, the term, "security" includes objective viewpoints of security engineering as well as such subjective factors as

[*] Currently affiliated with NTT Corporation.

sense of security. We use the Japanese word, Anshin, for the latter throughout this paper. Anshin is a Japanese noun which is composed of two words, viz. An and Shin. “An” is to ease, and “Shin” indicates mind. Anshin literally means to ease one's mind. In this research, we have constructed our initial Anshin model incorporating several factors and conducted a preliminary experiment with users to understand how effective those factors are in the model.

The more we enjoy the network-based web services, the more risk and threats we encounter such as compromise and phishing. Such destabilizing factors on the security may prevent the users from using network-based service. The users need to get Anshin to use such services extensively. The objective of our research is to produce the Anshin model for evaluating security tools in order to provide better interfaces for users. However, it's still not clear model and framework for evaluation it. This study attempts to look into this problem and propose an initial model of evaluating security systems in terms of the sense of security. Additionally, we try to analyze the factors contributing to Anshin and to produce an Anshin model with which one can get a quantitative score on how secure users feel.

This paper proposes our Anshin model with social-scientific viewpoints rather than technical security issues. The next section presents related work with a focus on trust model. Section 3 proposes our evaluation model based on some previous work, later sections describe result of experimental survey including factor analysis. The final section gives some conclusion and presents future work.

2 Related Work

2.1 Trust and Security

Trust has been studied in various disciplines such as sociology, psychology and economics. From psychological viewpoint, Deutsch defined trust in an interpersonal context [4]. Later he introduced confidence in trust so that one will find what is desired from another [5]. Gambetta defined trust as a particular level of one’s subjective probability that another’s action would be favorable to oneself [6]. Marsh proposed the first computational trust model with quantized trust values in the rage of -1 to +1 [7].

According to Friedman, “people trust people, not technology” [8]. In contrast with Friedman’s view of trust, our perspective is that *security* is intimately connected with technology. Trust and security are interdependent concepts. Lamsal illustrates this using cryptography as an example: one’s secure communication with another requires a key obtained via trusted key distribution [9]. If the key distribution was not worthy of that trust the communication is not secure. Dimmock incorporates trust as a part of access control security [10]. Recently, new trust models in security research have proposed [11,12].

2.2 Anshin and emotional trust

As we see it, trust is a belief based on an expectation of others’ behavior. In other words, it is to do with the *relationship* between the trustor and trustee. On the other

hand, Anshin, the sense of security, is a personal emotion. In other words, it is a subjective feeling towards an object, such as security measures.

As we point out in section 2.1, trust has been studied in various disciplines such as sociology, psychology and economics. A lot of it is concerned primarily with *cognitive trust*. Firstly, Lewis as sociologist defined the type of trust as follows; *Trusting behavior may be motivated primarily by strong positive affect for the object of trust (emotional trust) or by "good rational reasons" why the object of trust merits trust (cognitive trust), or more usually some combination of both* [13]. Popularly, the latter nature, viz. cognitive trust is defined as a trustee's rational expectation that a trustee will have the necessary competence, benevolence, and integrity to be relied upon. On the other hand, the emotional aspect of trust is defined as an emotional security, or feeling secure, or comfortable [14]. Xiao also mentioned that emotional trust is feeling, while cognitive trust is cognition [15]. In like wise, more recent work by Chopra [16], Kuan [17] etc points out multidimensionality of trust. Also from a sociological viewpoint, Yamagishi [18] gives 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. Trust is expectations of others' intentions based on trustor's judgment of others' personalities and feelings. From the viewpoint of communication about the risks of nuclear power plants, Kikkawa introduces two Anshin states, viz. one *with* knowledge and the other *without* knowledge [19]. Kikkawa suggests that it is necessary for users to study and obtain information in an active way to get more Anshin feeling. To create Anshin experts on technology need to provide information to users as well as reducing technological risks.

2.3 Human Interface

From a human interface viewpoint, Whitten and Tygar point out that user interfaces in security systems need special interfaces [20]. Stephens gives design elements, such as page layout, navigation, and graphics which affect the development of trust between buyers and sellers in e-commerce [21]. Pu also reports that how information was presented affected trust building in user interfaces [22]. According to Riegelsberger [23], quantitative studies on trust in e-commerce, such as [24], and other consumer research confirm that affective reactions influence consumer decision-making.

3 The Anshin Model

3.1 Overview

In this paper, in terms of Anshin, we take a different approach from Yamagishi in that we incorporate trust as a factor of Anshin. Anshin, in our work, is attached more to computer security technology than to the general term of security. Anshin could be derived from some factors including knowledge. We incorporate the

viewpoints of both Kikkawa and Xiao into our model in that knowledge could be a factor of Anshin. Yamagishi presented an empirical study on how positive and negative reputations would affect trust. Yamagishi's definition of trust and Anshin is slightly different from ours, as we try and incorporate trust as a factor of Anshin. We take reputation as one type of information which affects our trust factor. We include the intuitive user interface factor as Riegelsberger suggested.

3.2 An Anshin Model

Based on the discussions in previous section, we construct an Anshin model. The model is based on Beck's cognitive model [25] so that the emotion factor, Anshin, is produced from factors such as *trust* in providers, services and systems, *knowledge* of security technology and the intuitively sensed *quality of the user interface*. Those factors are expressed as subjective functions which take cognitive factors as an argument. The cognitive factors, combined using an appropriate weight function, produce the degree of Anshin. Additional factors, experience of the use of the service and system, give feedback to each factor.

Figure 1 depicts the model. A user takes an exterior cognitive factor, information, *r*, on system providers such as an implementor, as an argument of the *Trust* function, *T*. System cognitive factors such as security technology and the quality of user inter face are also taken as arguments for the *Knowledge* and *Intuitive* functions, *K* and *I*. Output of each function is substituted for assessable value quantitatively. For example, evaluated value about cognitive factors in "*r*" becomes confidence in society, feeling of trust, and expectations for ability by user's subjective assessment. All function together with experience information, e_i, and weight parameters, w_i the emotion value, Anshin, *A*, is calculated as:

$$A = w_0 * T(r+e_0) + w_1 * K(s+e_1) + w_2 * I(u+e_2)$$

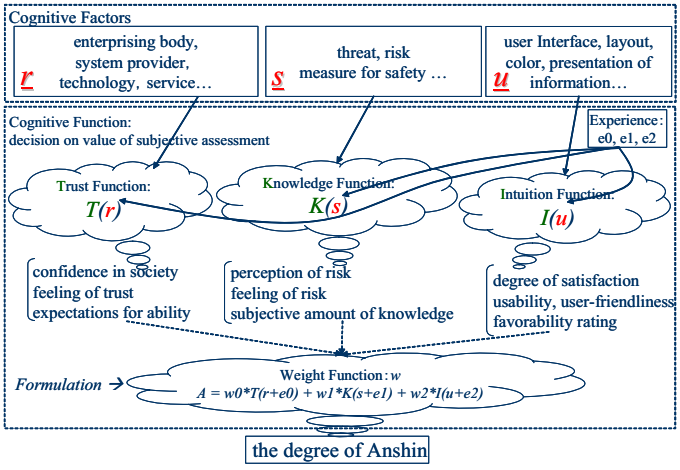

Figure.1: Anshin model

4 Study Design

We tried a variety of approaches to grasp the structure of "sense of security". To assess the validity of the hypothesis in Anshin model, we conducted two types of a user survey. The former is empirical examination as preliminary study (pre-test) that we tried a quantitative assessment of "sense of security" using framework of anshin model. 18 participants were asked a question about a sense of security when they sent a file including their own personal information by file transfer system over the Internet. The latter is that we apply questionnaire method to 140 participants to make a statistical survey using factor analysis, whether hypothesis of three factor; trust in provider, knowledge of technology and risks, quality of user interface, is meaningful factor.

4.1 Preliminary study

We conducted a preliminary study (pre-test) of users to see how the three factors, trust in providers, knowledge of technology and risks, and quality of user interface, affect users' perceptions in the Anshin Model [26]. We used two versions of a file store system on the world-wide web called the under-the-door communication system [27], viz. an insecure version and a secure version. In the former, a password and information were transferred as a plain text over the network, whereas in the latter they were transferred using of the secure shell, SSH. The experimental subjects were asked to use both systems without explanation for the first run, and then were given information including basic knowledge about security and the reputation of the provider of the system. The former was to measure the knowledge factor and the latter was for the trust factor.

For the trust factor, we prepared two cases: one with a good reputation and another with a bad reputation. The bad reputation says that the system was created by a student using unknown free software available on a dubious site. On the other hand, the good reputation says that the system was created by a well-known researcher and evaluated highly by an academic society. In addition, for the quality of the interface, we change the color of the user interface of the system. According to the psychology of colors [28], black gives an anxious feeling and green gives Anshin. The neutral color between them is blue. For the first run, both groups used the systems whose interfaces are blue. For the second run, we prepared two interfaces, one for Group 1 and the other for Group 2. The interfaces of the systems for Group 1 are green whereas those for Group 2 are black. Using only color differences to study the importance of the user interface factor is a considerable oversimplification.

There were 18 experimental subjects divided into two equal-sized groups. The subjects were mainly freshman in faculty of software and information science in our university, and they did not previously know much about security. Each group performed two runs of the experiment. In each run the subjects first used the system without SSH and then with SSH. After the first run each group was given different information: group 1 received positive information and group 2 received negative information. Then the second run was performed as before, first without SSH and then with SSH (see Table 1)

Table 1. The conditions in the experiment

Time axis	The First Run		The Second Run	
factors	Group1	Group2	Group1	Group2
Knowledge: information about security	No previous knowledge		Fundamental information on security and SSH	
Trust: reputation about the system provider	No previous knowledge		with *positive* information: highly evaluated researcher	with *negative* information: unknown student using the dubious codes

The experiment was conducted for the cases listed in Table 2. Each case includes the first and second runs as in Table 1. The first run without any knowledge and information and the second one with knowledge of security as well as the biased information: positive information for Group 1 and negative for Group 2. The arrows in Table 2 indicate the sequences a subject of each group went though. For instance, after a subject of Group 1 went through the first run of Cases 1 and 2, he filled in the questionnaire. He was given the security knowledge and reputation information and went on to the second run of Cases 1 and 2, finally answering the questionnaire once again. In the beginning, the subjects were not told the difference, but the display of the system with SSH showed "with SSH". Only one of eighteen subjects noticed the difference; the others did not because they did not know what SSH was. One of them knew about SSH before the experiment. The subjects are not associated with the researchers' laboratory. The researchers are graduate students whom the subjects had never met before. Presumably, they had no subconscious motivation or intention to help the researchers but this pre-test experiment did not explicitly control for that possibility. The manipulation check has been done by introspection.

Table 2.Cases of the experiment

	System Option	*1st Run*	*2nd Run*	
Case 1	without SSH	↓	↓	Group 1
Case 2	with SSH	▪	▪	Group 1
Case 3	without SSH	↓	↓	Group 2
Case 4	with SSH	▪	▪	Group 2

Legend: ▪ indicates the timing that a subject filled in a questionnaire

Principal results are as follows. The results for Case 2, in which the subjects were provided with the positive information in the second run as well as knowledge of security, show that the degree of fear has been reduced with most of the subjects --- i.e., they felt more Anshin after they learned the positive reputation of the system implementor and the security fundamentals with SSH as in Figure 2. Almost all the subjects felt fear in Case 3 after receiving negative information and security knowledge when they used the system without SSH (see Figure 3).

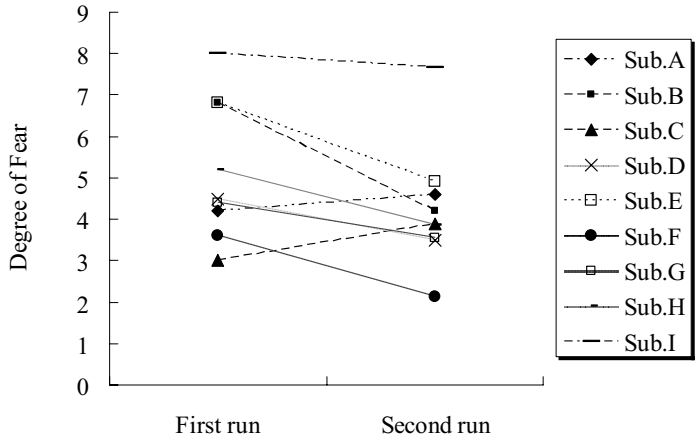

Figure 2. The change of fear in Case 2 (with SSH and with positive information)

We found noticeable change with the trust factor which indicates how much trust one would put on the system provider. If SSH was being used, when subjects were given positive reputation information, the degree of trust went up. If SSH was not being used when the reputation information was negative, trust went down. For additional result and questionnaire details, it is shown on our previous paper [26].

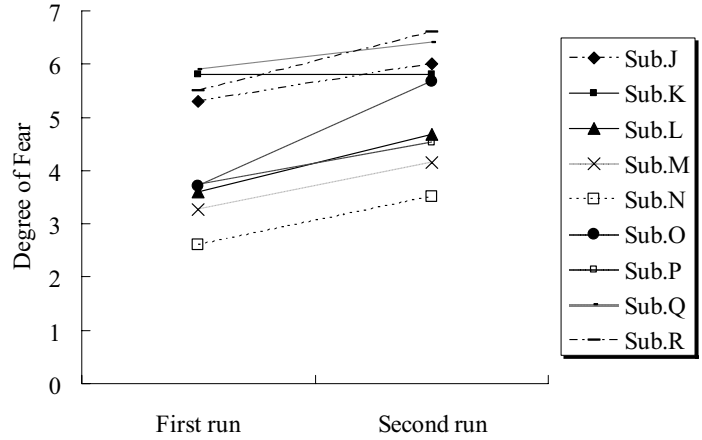

Figure 3. The change of fear in Case3 (without SSH and with negative information)

Our findings from this preliminary study were as follows. After obtaining knowledge about security and positive reputation information about the system implementor, the subjects increased Anshin when they used a secure system, and decreased it when they used an insecure system. Also after obtaining knowledge about security and negative reputation information, the subjects felt fear when they used an insecure system. With security knowledge and negative reputation information, subjects' feelings varied when they used the secure system. When one learns some technology, he may well learn its risks as well; he will be more aware of such risks. The alternative view is that the secure feeling changes depending on what one's experience or knowledge. The very simple user interface color change in this experiment did not result in any noticeable difference in the subjects' Anshin.

4.2. Factor Analysis

Previous section 4.1 suggests the impact of knowledge and trust on Anshin. But, user interface factor did not show statistically-useful difference because of lack of sample number. Hence this preliminary experiment would go but a little way to show validity of our model. Therefore, we planned to carry out a questionnaire survey to grasp the structure of "sense of security" in a statistically optimal fashion.

The purpose of this survey conducted by factor analysis was to confirm the structure of Anshin, and to verify a validity of our anshin model. We expected three subscales based on above discussion and our previous work. The 27 items from Q1 to Q27 were adapted from previous research and revised to fit context of this study. Most study used a 7-point Likert scale system ranging from "strongly disagree"(1) to "strongly agree"(7), e.g.[29]. 140 students in the faculty of Software and Information Science, Iwate Prefectural University, took part in the survey. After eliminating incomplete responses, there were 122 valid entries used for the analysis. Of the 122 participants, 81 were male, and 41 were female. The age range of participants was from 19 to 36, average age 20.

Main results were as follow: The explanatory factor analysis(EFA) with principal factor method and promax rotation found that three factors are present in Table 3. Several repeated analysis led to a statistically-meaningful 22 items, and resulted in following factor structure; 1) *trust and security by user expectation*, 2) *satisfaction of user interface*, and 3) *understanding of risk and threat by user experience and prior knowledge*. All items has factor loading above 0.338. The three factors were explained by 43.5%(Cumulative) of the total. To confirm reliability of measurement, Cronbach's coefficient alpha of subscale is summarized in Table 3. According to this, it shows relatively high value of alpha more than 0.7.

I. Factor 1 (27.9% of the variance)

The first factor consists of 11 items (Q1,3,4,5,6,7,8,9,10,11,27) about trust and security. Mainly, it has feeling confidence in society and trust by user expectation for one's ability, security, safety, etc. The results tends to confirm that this factor suggest validity of trust function in an Anshin model.

II. Factor 2 (9.3% of the variance)

The second factor consists of 5 (Q17,18,19,20,21) items about satisfaction of user interface(UI). Especially, it has subjective assessment of the quality of UI; for example, usability, attractive design and user-friendliness. This results tends to confirm that this factor support hypothesis of intuition function in an Anshin model.

III. Factor 3 (6.2% of the variance)

The third factor consist of 6 items (Q12,13,14,15,25,26) about knowledge in measure for safety. Particularly, it shows perception of risk, understanding of risk and threat by user experience and prior knowledge. The findings suggest that hypothesis of knowledge function is significant in an Anshin model.

Table 3. Three-factor solution in EFA

No.	Items	i	ii	iii
Q8.	In case of trouble, the system provides help.	**0.82**	-0.05	-0.18
Q7.	In case of trouble, the system recovers perfectly.	**0.77**	-0.01	-0.22
Q9.	It assures adequate security.	**0.73**	-0.08	0.08
Q6.	In case of trouble, the company provide gives assurance.	**0.70**	0.04	-0.14
Q3.	I have a sense of security as the company is a giant.	**0.53**	0.09	0.07
Q4.	The company has good privacy management policy.	**0.53**	-0.01	0.17
Q1.	I trust the company / enterprising body providing the services.	**0.45**	0.11	0.24
Q27.	I just feel secured but I don't have a concrete ground.	**0.41**	0.14	0.04
Q5.	I don't have trust in the company but the technology and the system.	**0.40**	0.17	0.06
Q11.	If it not secure, be saved.	**0.37**	-0.08	0.06
Q10.	I can really feel secure.	**0.36**	-0.01	0.06
Q17.	Terminal device or the system provides user a good impression.	-0.10	**0.98**	-0.07
Q18.	Terminal device or the system has attractive design.	-0.01	**0.93**	-0.09
Q19.	Terminal device or system interface has a neat layout or use of color.	-0.03	**0.92**	-0.10
Q21.	Terminal device or the system interface has user-friendliness.	0.13	**0.62**	0.15
Q20.	Terminal device or the system interface has a good usability.	0.11	**0.55**	-0.05
Q14.	I know well about information technology.	-0.05	-0.12	**0.67**
Q12.	I understand the way the system or technology works.	-0.02	-0.18	**0.64**
Q13.	I pay attention to safety measures.	0.21	-0.12	**0.55**
Q25.	I am expressed because I use quite often.	-0.02	0.38	**0.48**
Q15.	I user it with the full knowledge of risk and threat.	-0.17	0.14	**0.48**
Q26.	I am not afraid as I am quite experienced.	0.11	0.26	**0.34**
	Cumulative(%)	27.93	37.27	43.52
	Cronbach's coefficient alpha	0.84	0.90	0.72

4.3 Discussion

Based on the above result, the results of factor analysis provide strong support for the hypotheses in our Anshin that three factors contribute to a sense of security. To enhance the reliability of the result, confirmatory factor analysis (CFA) are needed. However, for the first experimental attempt in section 4.1, difference in color of user interface does not show significant difference. Presumably, this is attributed to the reason that impression of color is susceptible to cultural background or personal taste, so pre-test by the small number of subjects does not show significant difference statistically. Consequently, there is a possibility that color factor was not appropriate as experimental condition. As the related literature points to the UI as being a significant factor in trust [21-23], we try to validate empirically by some sort of factors related UI.

5 Conclusion and Future Work

Security has long been looked at from an engineering viewpoint. 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. This paper introduced an initial study on the sense of security as new concept; Anshin. This study proposed an initial model of evaluating security systems in terms of the sense of security, and tried a variety of approaches to grasp the structure of "sense of security"

Our recent study results using factor analysis showed the following factors contribute to a sense of Anshin: 1) trust and security by user expectation, 2) satisfaction of user interface, and 3) understanding of risk and threat by user experience and prior knowledge. In terms of factor analysis, this survey showed that theoretical three factors in the structure of a sense of security were significant statistically. Further analyses are needed to determine what effects other factors including subjective amount of knowledge, feeling of risk, feelings of trust and computer anxiety, have on the sense of security.

However, Anshin model have new threats as exploited by a scam, e.g. phishing. Another way of saying, it is that the factor people feel security is made bad use of deceit. As future work, we plan a case study to focus on phishing. Especially, we are planning the evaluation of phishing site using our framework how secure a victim feels incorrectly. For example, Dhamija shows that phishing sites exploit lack of knowledge, visual deception, and lack of attention [30]. According to this, in ether case, human property is made wrong use as social engineering. Therefore, it's believed that ensuring security as system including "human" is one of the important issues from social-scientific and ergonomics approaches.

ACKNOWLEDGMENT This research was supported by Strategic International Cooperative Program, Japan Science and Technology Agency (JST). Special thanks to Ryuya Uda of Tokyo University of Technology, Mizuki Yamazaki of the Research Institute of Science and Technology for Society, Basabi Chakraborty, Yukinori Goto, Norihisa Segawa and Hisayoshi Ito of Iwate Prefectural University,

and Makiko Matsumura of National Institute of Public Health. Without their help this research was not possible.

REFERENCES

1. D. Basin, S. Mödersheim and L. Viganò: CDiff: a new reduction technique for constraint-based analysis of security protocols, *Proc. of the 10th ACM conference on Computer and Communications Security*, pp.335-344 (2003).
2. W. Shi, H.S. Lee, C. Lu and T. Zhang: Attacks and risk analysis for hardware supported software copy protection systems, *Proc. of the 4th ACM workshop on Digital rights management*, pp. 54–62 (2004).
3. J.J. Yan: A note on proactive password checking, *Proc. of the 2001 workshop on New Security Paradigms*, pp. 127-135 (2001).
4. M. Deutsh: The effect of motivational orientation upon trust and suspition, *Human Relation*, 13, pp. 123-139 (1960).
5. M. Deutsh: The resolution of conflict (Yale University Press, 1973).
6. D. Gambetta: Can we trust trust?, *Making and Breaking Cooperative Relations,* electronic edition, Department of Sociology, University of Oxford, chapter 13, pp. 213-237 (originally published from Basil Blackwell, 1988). Available at : http://www.sociology.ox.ac.uk/papers/gambetta213-237.pdf (Last Access: 9 Feb 2007)
7. S.P. Marsh: Formalising trust as computational concept, PhD Thesis, Department of Mathematics and Computer Science, University of Stirling (1994).
8. B. Friedman, P.H. Khan and D.C. Howe: Trust online, *Communication of ACM,* Vol. 43, No.12, pp. 34-40 (2000).
9. P. Lamsal: Understanding Trust and Security, Available at : http://www.cs.helsinki.fi/u/lamsal/asgn/trust/UnderstandingTrustAndSecurity.pdf (Last Access: 9 Feb 2007).
10. N. Dimmock, A. Belokosztolszki, D. Eyers, J. Baconand and K. Moody: Access management for distributed systems: Using trust and risk in role-based access control policies, *Proc. of the ninth ACM symposium on Access Control Models and Technologies*, pp. 156-162 (2004).
11. L.J. Hoffman, K. Lawson-Jenkins, J. Blum: Trust beyond security: an expanded trust model, *Communications of the ACM*, Vol. 49, No.7, pp.94-101 (2006).
12. Stephen Flowerday, Rossouw von Solms: Trust: An Element of Information security, *Proc. of the IFIP TC-11 21st International Information Security Conference (SEC2006)*, pp.87-98 (2006).
13. J.D. Lewis. and A. Weigert: Trust as a Social Reality, *Social Forces*, Vol.63, No.4, pp.967-985 (1985).
14. S. Xiao. and I. Benbasat: The formation of trust and distrust in recommendation agents in repeated interactions: a process-tracing analysis, *Proc. of the 5th international conference on Electronic commerce (ICEC'03)*, pp.287-293 (2003).
15. S. Xiao and I. Benbasat: 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).
16. K. Chopra, W.A. Wallace: Trust in Electronic Environments, *Proc. of the 36th Hawaii International Conference on System Science (HICSS'03)*, pp.331-340 (2003).
17. H.H Kuan. and G.W. Bock: The Collective Reality of Trust: An Investigation of Social Relations and Networks on Trust in Multi-Channel Retailers, *Proc. of the 13th European Conference on Information Systems* (ECIS 2005), Available at: http://is2.lse.ac.uk/asp/aspecis/20050018.pdf (Last Access: 9 Feb 2007)
18. Yamagishi, T.: *The structure of trust: The evolutionary games of mind and society* (Tokyo University Press, 1998). English version is available at : http://lynx.let.hokudai.ac.jp/members/yamagishi/english.htm (Last Access: 9 Feb 2007) .
19. T. Kikkawa, S. Shirato, S. Fujiiand and K. Takemura: The pursuit of informed reassurance ('An-Shin' in Society) and technological safety('An-Zen'), *Journal of SHAKAI-GIJUTSU* , Vol. 1, pp.1-8 (2003). in Japanese.
20. A. Whitten and D. Tygar: Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0, *Proc. of the 9th USENIX Security Symposium,* pp.169–184 (1999).
21. R.T. Stephens: A framework for the identification of electronic commerce design elements that enable trust within the small hotel industry, *Proc. of ACMSE'04*, pp.309 – 314 (2004).
22. P. Pu, L. Chen: Trust building with explanation interfaces, *Proc. of the 11th international conference on Intelligent user interfaces (IUI'06),* pp.93-100 (2006).
23. J. Riegelsberger, M.A. Sasse and J.D. McCarthy: Privacy and trust: Shiny happy people building trust?: photos on e-commerce websites and consumer trust, *Proc. of the SIGCHI conference on Human factors in computing systems (CHI'03)*, Vol. 5, No. 1, pp. 121-128 (2003).
24. Sapient & Cheskin: eCommerce Trust, 1999
25. Beck, A.T.: *Cognitive Therapy of Depression* (Guilford Press 1979).
26. Y. Murayama, N. Hikage, C. Hauser, B. Chakraborty and N. Segawa: An Anshin Model for the Evaluation of the Sense of Security, *Proc. of Hawaii International Conference on System Science (HICSS'06)*, Vol.8, p.205a (2006).
27. T. Tomita, K. Suzumura and Y. Murayama: Proposal for Under the Door Communication on the network, *Human-Computer Interaction: Theory and Practice(Part II)*, pp. 1019-1023 (2003).
28. R.H. Alschuler and H.L. Berta: Painting and Personality, University of Chicago Press, Vol.1 (1947).
29. D.J. Kim, C. Steinfield and Y. Lai: Revisiting the Role of Web Assurance Seals in Consumer Trust, *Proc. of the 6th international conference on Electronic Commerce*, pp.280-287 (2004).
30. R. Dhamija, J.D Tygar. And M. Hearst: Why phishing works, *Proc. of the SIGCHI conference on Human Factors in computing systems (CHI'06)*, pp.581-590 (2006).