International Journal of Networking and Computing – www.ijnc.org
ISSN 2185-2839 (print) ISSN 2185-2847 (online)
Volume 6, Number 2, pages 328–344, July 2016

Design of User Information Disclosure Decision Method for Disaster Information Sharing System

Keita Kayaba
National Institute of Technology, Sendai College, 4-16-1, Aayashi-chuo, Aoba-ku, Sendai, Miyagi, 989-3128, JAPAN

Akiko Takahashi
National Institute of Technology, Sendai College, 4-16-1, Aayashi-chuo, Aoba-ku, Sendai, Miyagi, 989-3128, JAPAN

Received: February 15, 2016
Revised: May 2, 2016
Accepted: July 4, 2016
Communicated by Takashi Yokota

Abstract

During natural disasters, a significant amount of information is shared over the Internet. Therefore, it is desirable to provide disaster information based on information about individual users. However, there is a trade-off between the protection of user information and the quality of services that should be considered when providing disaster information. We propose a method that rationally determines the extent of user information to be disclosed. The effectiveness of the proposed method was evaluated experimentally. The experiments were conducted using the proposed method and a simple determination method wherein both the utility and intention of the user were considered relative to the extent of user information disclosure. In addition, the extent to which the trade-off was considered for each user was evaluated quantitatively.

Keywords: trade-off, user information, disaster information

1 Introduction

During natural disasters such as the 2011 Great East Japan Earthquake, a significant amount of information is shared over the Internet [8][11]. Such information is known as disaster and safety information (hereafter disaster information) primarily posted by Internet users (hereafter users); this information can be shared more quickly and in greater detail than that provided by television and radio. It is inevitable that information sharing during massive natural disasters will play a more significant role in the future owing to the ongoing popularization of smart phones, tablets, and other such devices. However, for a user who cannot freely utilize Internet services, it is difficult to select relevant disaster information from the large amount of available information.

Disaster information is shared in many different ways such as government information delivery services [2], traditional mass media, and social networking services (SNS) [3][13][16]. An effective information delivery service should provide reliable and comprehensive information. However, when a large-scale disaster occurs, it is difficult to acquire information for the entire affected area. Thus, users may receive disaster information for a limited area. In addition, the information provided is

summarized, and users may not receive the information they require. SNSs can provide detailed information for a wider area because the information is provided by many users. However, information posted to SNSs may be unreliable and not relevant to a particular user; thus, users must search for relevant information. Therefore, it is necessary to provide appropriate disaster information without requiring a significant user effort. In addition, it is necessary to provide disaster information based on information about individual users. However, many users do not want to disclose their information, which necessitates a framework to minimize the amount of disclosed user information while providing appropriate disaster information.

If the quality of a safety information sharing service is considered to be "letting many people know detailed safety information about a user," the more information a user discloses, the higher the quality of services. However, this also increases the risk of the disclosed information being abused. Moreover, the quality of service decreases when user information disclosure is constrained to reduce this risk. Therefore, it is necessary to consider the trade-off between the amount of disclosed information and the quality of service when providing disaster information. Thus, we propose a method that can process this trade-off to rationally determine information disclosure extent and the extent of disaster information to be provided.

The remainder of this paper is organized as follows. Related work and challenges are discussed in Section 2. The proposed method is described in Section 3. Experimental results are presented in Section 4. Section 5 concludes this paper and provides suggestions for future work.

2 Related Work and Challenges

2.1 Related Work

The proposed disaster information sharing method depends on user-provided information in order to provide adequate disaster information to users considering user information based on information recommendation system [7], etc. Information recommendation systems are receiving considerable attention, and such systems can be applied to disaster information sharing. However, if a system considers personal user information, it is necessary to ensure that this private information is not disclosed publicly [1]. Thus, the trade-off between quality of service and privacy must be considered.

Various methods to protect user information have been proposed. Anonymization methods, which make it difficult to identify an individual by deleting data items or inserting extra data, have been proposed to prevent the identification of a user by a third party [4][10][15]. For example, k-anonymity maintains user anonymity and reduces the possibility of the user being identified by a third party, maintaining the number of users with the same user information at more than k. When anonymization is applied to an actual system, a typical method is to collectively determine anonymity using a server that stores personal user data after the disclosure of personal data is required. Since most anonymization methods, e.g., k-anonymity, must actually collect and store personal data, it is possible that user information could be leaked.

In contrast, there are methods that adjust the anonymity of personal data by changing the granularity of the data. Such methods consider the trade-off between the protection of user information and the quality of information and services [5][6][9][12]. These methods apply the concept of information entropy or personal data identification probability as an index for anonymity. A preferred anonymity level input by the user is compared with the index to determine the granularity of personal data. However, the only input is the preferred anonymity level; therefore, it is difficult to consider user intention relative to the protection of user information and use of services. In addition, it is difficult for inexperienced users to consider the trade-off between personal information disclosure and the quality of information and services when determining their preferred level of anonymity.

2.2 Technical Problems and Challenges

Although user information protection methods have been proposed, the trade-off between user information protection and the quality of information and services when information is shared during

massive natural disasters has not been considered. Thus, the following technical issues should be addressed:

(P1) It is difficult to consider the trade-off between user information protection and the quality of information and services that users can receive.

During a massive natural disaster, the distribution of disaster information is more important than the protection of user information; thus, personal information may be disclosed and abused. Therefore, it is difficult to encourage users to disclose sufficient information to guarantee effective disaster information and services.

(S1) We propose a user information disclosure decision method to control information disclosure.

This method supports control of the extent of user information disclosure. An appropriate level of information disclosure is determined by rationally considering the user's desired level of disclosure of private information, the user's disaster information request, and the trade-off between the protection of user information and the quality of information and services. The information disclosure extent decision method employs a decision-making game based on game theory to process the trade-off rationally to facilitate decision making regarding the extent of disclosed information. A trade-off processing mechanism is constructed for this purpose. With this mechanism, it is possible to determine appropriate granularity of disclosed information prior to the user actually disclosing information, which differs from other methods such as anonymization.

The proposed method focuses on rationality when considering this trade-off and assumes a completely rational user. A completely rational user determines the extent of information disclosure that will maximize utility, i.e., essentially considering the trade-off between privacy concerns and quality of information and services. However, in complicated situations, such as those associated with natural disasters, it is difficult for a general user to make a completely rational decision for the extent of information due to the bounded rationality of humans [14]. The trade-off processing mechanism employs a decision-making game that simulates the decision of a completely rational user to support an information disclosure decision by a normal user with the bounded rationality.

3 User Information Disclosure Decision Method

3.1 Outline

When safety information is shared during a natural disaster, the disclosure of user information enables the sharing of more detailed safety information. When users feel that they do not require information protection, it is generally possible to maximize the effectiveness of safety information sharing. However, users generally expect to make the fullest use of safety information sharing functions and protect their personal information as much as possible; thus, the previously mentioned trade-off occurs. The proposed user information disclosure decision method supports decisions relative to the extent to which users wish to protect their private information while using disaster information sharing functions.

3.2 Trade-off Processing Mechanism Design

The trade-off processing mechanism employs weighted user input (i.e., the desired level of information protection) to protect user information, objectively evaluate risk, and obtain disaster information (disaster information request). The trade-off processing mechanism employs a user decision-making game to process this trade-off.

Figure 1 shows a schematic of the trade-off processing mechanism. The trade-off processing mechanism comprises two types of parameter sets, i.e., user information and disaster information sharing function sets. The number of user information sets is equal to the number of user information items, and the number of disaster information sharing function sets is equal to the number of disaster information sharing functions that can be used. In other words, each user information set and disaster

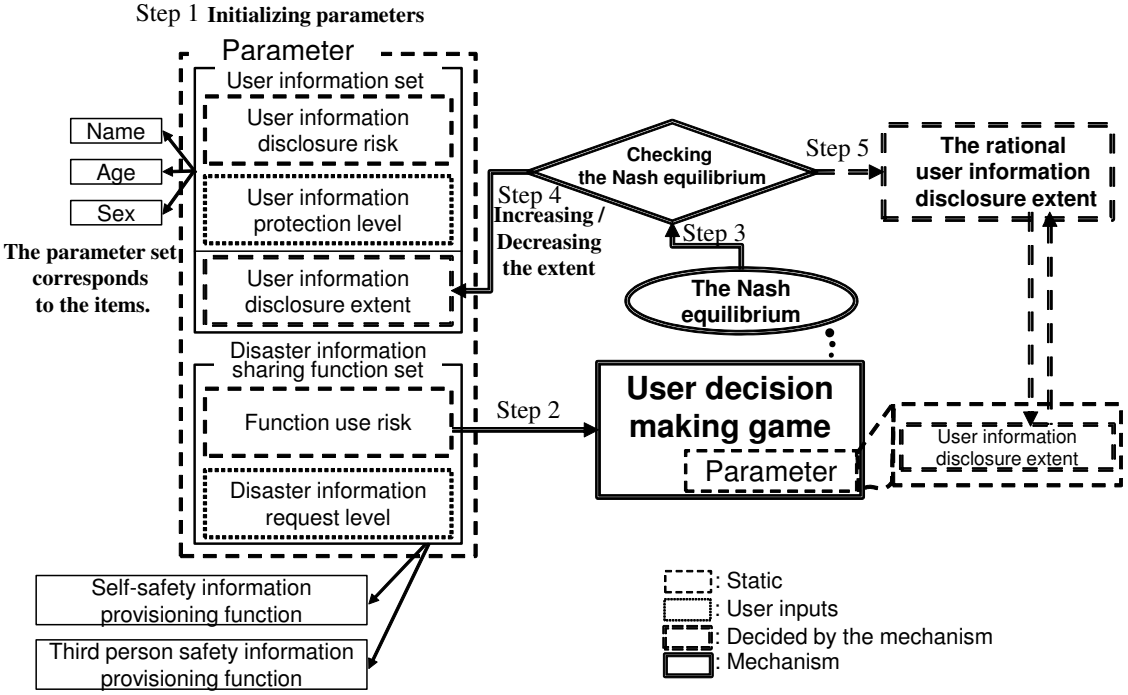

Figure 1: Schematic of the trade-off processing mechanism

information sharing function set correspond to a user information item and a disaster information sharing function item, respectively. For example, when user information includes "name," "address," and "telephone number" information items, there are three user information sets, and when disaster information sharing functions include a "safety information provisioning function for self," a "safety information provisioning function for a third person," a "safety information request function," and a "safety information search function," there are four disaster information sharing function sets. Each user information set has "user information disclosure risk," "user information protection level," and "user information disclosure extent" elements. The user information disclosure risk expresses (in a static manner) the risk of user information being abused. The user information protection level expresses the user's desired information protection level (as a weight) for the information in a user information set. The user information disclosure extent is a parameter that expresses the extent to which information in the user information set can be disclosed; 0.0 implies no disclosure; 0.5 implies disclosure of half the quantity of user information; and 1.0 implies full disclosure. For example, "half disclosure" for user name expresses disclosure of either only the first name or only the surname. The disaster information sharing function set has "function use risk" and "disaster information request level" elements. The function use risk element extends to user information when a disaster information sharing function that corresponds to a disaster information sharing function set is used. The number of function use risk elements is equal to the number of user information sets. The disaster information request level expresses the weight of the user's disaster information request for a disaster information sharing function that corresponds to a given disaster information sharing function set.

The flow of the trade-off processing mechanism is as follows. Initially, the trade-off processing mechanism uses the user information protection level and disaster information request level parameters input by the user, as well as the user information disclosure risk and function use risk set of the trade-off processing mechanism, to construct a user decision-making game to obtain the equilibrium of the game as a rational extent of user information disclosure. The rational extent of user information disclosure is determined by each user information item. As a result, a suitable extent

of user information disclosure is obtained for all information items. The extent of user information disclosure is determined for each information item as follows:

Step 1 The default user information disclosure extent for a user information set that corresponds to an item of user information for which the disclosure extent must be determined is 0.0, and the default extent of user information disclosure for the other user information is set as 1.0.

Step 2 A decision-making game is constructed to obtain the Nash equilibrium using the parameter sets relative to determining the extent of user information disclosure.

Step 3 Proceed to Step 5 when a pair of actions that express the Nash equilibrium (a pair of user information items) represents user information items for which the extent of information disclosure must be determined; otherwise, proceed to Step 4.

Step 4 The extent of user information disclosure of a user information set that corresponds to a user information item for which the extent of disclosure must be determined is increased. The extent of user information disclosure of other user information sets is decreased. Proceed to Step 2.

Step 5 The extent of user information disclosure of the user information set that corresponds to a user information item for which the extent of disclosure must be determined is considered the rational extent of user information disclosure.

Note that, prior to initiating these steps, the trade-off processing mechanism possesses the user-defined information protection and disaster information request levels. Thus, the only undetermined parameter is the extent of user information disclosure.

3.3 User Decision-making Game

To perform rational decision making completely according to the desired user information protection levels and the disaster information requests, the user decision-making game uses user information items as player actions and the parameter sets as the environment wherein environmental analysis is performed when the players act. The player performs rational decision making to maximize their utility. Therefore, the Nash equilibrium, i.e., an equilibrium by which both players display the best response, is an indication on which the user information item does a selection of both user desires converge within a certain parameter set. The user decision-making game is defined as follows.

When the number of the user information sets is expressed as $N_p \in \mathbb{N}$, the number of the disaster information sharing functions is $N_d \in \mathbb{N}$, the user information is $P_i \in P(i = 1, 2, ..., N_p)$ and the disaster information sharing function is $D_j \in D$ $(j = 1, 2, ..., N_d)$, then total set U of parameters used in the decision-making game is defined as follows.

$$\begin{aligned} U &= \langle P, D \rangle \\ &= \{\langle P_i, D_j \rangle \mid i = 1, 2, \ldots, N_p, j = 1, 2, \ldots, N_d, 2 \leq N_p, 1 \leq N_d\} \end{aligned}$$

When user information disclosure risk is expressed as $disc\_risk_i$, the user information protection level is expressed as w_p_i, and the user information disclosure extent is expresses as $disc\_lv_i$, then P_i is defined as follows.

$$\begin{aligned} P_i = \ & \{\langle disc\_risk_i, w\_p_i, disc\_lv_i \rangle \mid \\ & 0 < disc\_risk_i \leq 1, 0 \leq w\_p_i, disc\_lv_i \leq 1, disc\_risk_i, w\_p_i, disc\_lv_i \in \mathbb{R}\} \end{aligned}$$

When the function use risk is expressed as RoO_j(i.e., risk of outflow) and the disaster information request level is expressed as w_d_j, then D_j is defined as follows:

$$D_j = \{\langle RoO_j, w\_d_j \rangle \mid 0 \leq w\_d_j \leq 1, w\_d_j \in \mathbb{R}\}$$

where RoO_j is expressed as follows.

$$RoO_j = \{ro_{ji} \mid 0 \leq ro_{ji} \leq 1, ro_{ji} \in \mathbb{R}\}$$

For example, $ro_{21} = 0.2$ means "when disaster information sharing function 2 is used, approximately 0.2 of user information item 1 may leak". Here, to relate the disaster information request level to the user information protection level, the user information disclosure request level $w\_d'_i$ is defined as follows.

$$w\_d'_i = \frac{\sum_j^{N_d}(ro_{ji} * w\_d_j)}{N_d}$$

User information protection level $w\_p'_i$ obtained from information disclosure request level $w\_d'_i$ is defined as follows.

$$w\_p'_i = 1.0 - w\_d'_i$$

Here, the user decision-making game G is constructed based on "player," "action space," and "utility function," and defined as follows:

$$G = \langle N, A, u \rangle$$

where $N = \{\alpha, \beta\}$ the player set, α is the player created based on the user's desired information protection, and β is the player created based on the disaster information request. $A = \langle A_\alpha, A_\beta \rangle = A_\alpha \times A_\beta$ is the total set of action spaces, which are defined as follows.

$$\begin{aligned} A_\alpha &= \{a_{\alpha k} \mid a_{\alpha k} \in A_\alpha, k = 1, 2, \ldots, N_p\} \\ A_\beta &= \{a_{\beta l} \mid a_{\beta l} \in A_\beta, l = 1, 2, \ldots, N_p\} \end{aligned}$$

The above are the total set of action space(s) that players α and β can occupy. Here, element a_{kl} of A expresses a pair of actions $(a_{\alpha k}, a_{\beta l})$. $u = \{\langle u_\alpha, u_\beta \rangle \mid u_\alpha \colon A_\alpha \to \mathbb{R}, u_\beta \colon A_\beta \to \mathbb{R}\}$ expresses a pair of utility functions, and u_α and u_β express the utility obtained when players α and β perform actions, respectively.

The action space of a player is composed of the player selections, which are user information items that correspond to a user information set. The utility function is defined using a user's intention occurrence probability based on the risk of user information disclosure and the extent of user information disclosure for the user information set corresponding to the user information items. The user information disclosure risk is considered the user's utility in the user decision-making game. The utility a user can obtain generally increases when there is a high risk of information disclosure; therefore, utility increases proportionally to the extent of user information disclosure. The intention occurrence probability is a parameter that expresses the weight of a user's intention. The utility function considering user intention is expressed by the product of the intention occurrence probability based on risk and the extent of user information disclosure. This intention occurrence probability W is defined as follows.

$$\begin{aligned} W &= \langle W_\alpha, W_\beta \rangle \\ W_\alpha &= \{w_{\alpha k} \mid k = 1, 2, \ldots, N_p, 0 \leq w_{\alpha k} \leq 1, w_{\alpha k} \in \mathbb{R}\} \\ W_\beta &= \{w_{\beta l} \mid l = 1, 2, \ldots, N_p, 0 \leq w_{\beta l} \leq 1, w_{\beta l} \in \mathbb{R}\} \end{aligned}$$

Here, element $w_{\alpha k}$, $w_{\beta l}$ is expressed as follows.

$$\begin{aligned} w_{\alpha k} &= \frac{w\_p_k}{\sum_{k'}^{N_p} w\_p_{k'}} \\ w_{\beta l} &= \frac{w\_p'_l}{\sum_{l'}^{N_p} w\_p'_{l'}} \end{aligned}$$

Table 1: User decision-making game

α \ β		$w_{\beta 1}$	$w_{\beta 2}$	...	$w_{\beta l}$
		$a_{\beta 1}$	$a_{\beta 2}$	...	$a_{\beta l}$
$w_{\alpha 1}$	$a_{\alpha 1}$	$(u_\alpha(a_{\alpha 1}) * w_{11}, u_\beta(a_{\beta 1}) * w_{11})$	$(u_\alpha(a_{\alpha 1}) * w_{12}, u_\beta(a_{\beta 2}) * w_{12})$	...	$(u_\alpha(a_{\alpha 1}) * w_{1l}, u_\beta(a_{\beta l}) * w_{1l})$
$w_{\alpha 2}$	$a_{\alpha 2}$	$(u_\alpha(a_{\alpha 2}) * w_{21}, u_\beta(a_{\beta 1}) * w_{21})$	$(u_\alpha(a_{\alpha 2}) * w_{22}, u_\beta(a_{\beta 2}) * w_{22})$	...	$(u_\alpha(a_{\alpha 2}) * w_{2l}, u_\beta(a_{\beta l}) * w_{2l})$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$w_{\alpha k}$	$a_{\alpha k}$	$(u_\alpha(a_{\alpha k}) * w_{k1}, u_\beta(a_{\beta 1}) * w_{k1})$	$(u_\alpha(a_{\alpha k}) * w_{k2}, u_\beta(a_{\beta 2}) * w_{k2})$	...	$(u_\alpha(a_{\alpha k}) * w_{kl}, u_\beta(a_{\beta l}) * w_{kl})$

The total set of intention occurrence probabilities $W = W_\alpha \times W_\beta$ is $W = \{w_{kl} \mid w_{kl} = w_{\alpha k} * w_{\beta l}, w_{kl} \in W\}$. At this time, elements u_α and u_β of utility function u are defined as follows.

$$\begin{aligned} u_\alpha(a_{kl}) &= u_\alpha(a_{\alpha k}) * w_{kl} = disc\_risk_k * disc\_lv_k * w_{kl} \\ u_\beta(a_{kl}) &= u_\beta(a_{\beta l}) * w_{kl} = disc\_risk_l * disc\_lv_l * w_{kl} \end{aligned}$$

Table 1 shows the user decision-making game constructed as described above. Strategies in the user decision-making game express how user intention selects action $a \in A$. When the total set of strategic space(s) is expressed as $S = \langle S_\alpha, S_\beta \rangle$, S_α and S_β are strategic sets that players α and β can use, and their elements are expressed as s_α and s_β. The total set of strategic space(s) is expressed as $S = S_\alpha \times S_\beta$, and its element $s = (s_\alpha, s_\beta)$ indicates a pair of strategies. Players choose the best response in the user decision-making game, and the obtained Nash equilibrium represents the decision making of the user. In short, the best responses $s^* = (s^*_\alpha, s^*_\beta)$ for players α and β are defined as follows.

$$\begin{aligned} u_\alpha(s^*_\alpha, s_\beta) &\geq u_\alpha(s'_\alpha, s_\beta) \\ u_\beta(s_\alpha, s^*_\beta) &\geq u_\beta(s_\alpha, s'_\beta) \end{aligned}$$

A pair of the most effective reactions $s^* = (s^*_\alpha, s^*_\beta)$ represents the Nash equilibrium. Nash equilibrium s^* is the user's rational decision making, and a pair of the best response actions expressing the Nash equilibrium is expressed as $(a_{\alpha k^*}, a_{\beta l^*})$.

3.4 Trade-off Processing Flow

When the extent of user information disclosure is expressed as $X(\in \mathbb{R})$, $X^* \subseteq X$ shows a set for the extent of user information disclosure that is suitable. When V is a set with elements in regard to the extent of user information disclosure $disc_i(\in \mathbb{R})$ and an absolute value $\delta(\in \mathbb{R})$ for an increased value and a decreased value, and G shows a user decision making game, the trade-off processing mechanism M is defined as follows.

$$M = \langle X^*, V, G \rangle$$

In addition, X^* and V of the user information set i $(i = 1, 2, \ldots, N_p)$ are defined as follows.

$$\begin{aligned} X^* &= \{x^*_i \mid 0 \leq x^*_i \leq 1\} \\ V &= \{\langle disc_i, \delta \rangle \mid 0 \leq disc_i \leq 1, 0 < \delta, 1 \equiv 0 (mod\, \delta)\} \end{aligned}$$

Setting δ to a smaller value enables the extent of user information disclosure to be determined at finer granularity. When a user information item for which a suitable extent of user information disclosure must be determined is expressed as i' of $(i' = 1, 2, ..., N_p)$, the steps to determine the extent of disclosure are as follows.

Step 1 for all i if $i == i'$ then $disc_i = 0.0$ else $disc_i = 1.0$ endif

Step 2 for all i $disc\_lv_i = disc_i$, generate G

Step 3 if $k^* == l^* == i'$ then goto Step 5 else goto Step 4 endif

Step 4 for all i if $i == i'$ then $disc_i = disc_i + \delta$ else $disc_i = disc_i - \delta$ endif, goto Step 2

Step 5 $x^*_{i'} = disc_{i'}$

When the utility function of the user decision-making game does not return a negative value, the decision procedure relative to the extent of information disclosure always proceeds to Step 5 regardless of the linearity of the utility function. This is true because Steps 2 - 4 are repeated, where the extent of user information disclosure of user information items for which a suitable disclosure extent is required becomes 1.0, and the extent of user information disclosure of other user information items becomes 0.0.

4 Experiment and Evaluation

4.1 Outline

To verify the effectiveness of the proposed method, experiments were performed to obtain the extent of user information disclosure based on several safety information sharing functions and user type assumptions. The experiments were conducted using the proposed method and a simple determination method wherein both the utility (utility simple method) and intention (intention simple method) of the user were considered relative to the extent of user information disclosure. In addition, the extent to which the trade-off was considered for each user type was evaluated quantitatively.

In the experiments, simulations were performed 10,000 times with $\delta = 0.01$, which means that the precision of user information disclosure extent was 0.01, and their average was taken as the experimental result. Simulating the proposed method and the simple methods 10,000 times to verify the effectiveness of the proposed method is feasible within realistic computational time because the results obtained from fewer than 10,000 simulations approximately converged with the results of the experiments. Simulating actual disaster information sharing by users is arduous; therefore, we selected user information items and disaster information functions based on the records (and our experience) of the 2011 Great East Japan Earthquake.

Experiment 1 was designed to verify the effectiveness of the proposed method for users whose information protection wishes and disaster information requests that differ. The parameters of experiment 1 are shown in Table 2 and Table 3. In experiment 1, “name,” “age,” “address,” “sex,” “telephone number” and “location information” were used as user information items disclosed by a user. These items were selected with referencing services commonly used for sharing safety information, such as Google Person Finder [3] and J-anpi [13]. Such services commonly require “name,” “sex,” and “age,” as input. Then, “location information” was added to the information items for experiment 1 because it is important information for users who attempt to confirm safety information. In addition, “self-safety information provisioning function,” “third person safety information provisioning function,” “safety information request function” and “safety information search function” disaster information sharing functions were used. These functions were selected by referencing the services [3][13] described above. The risk of user information disclosure for the information items was set empirically based on an identification probability concept. The identification probability concept indicates the probability of risk resulting from information disclosure [12][14]. The identification probability concept calculates the inverse of the number of people with an identified condition. Generally, a user must disclose some personal information in order to share safety information over Internet-based services; therefore, it was assumed that all disaster information sharing function items gave the greatest risk to all information items. Thus, the function use risk of disaster information sharing function items was set to 1.0 for all user information items. The user inputs shown in Table 2 and Table 3 were used as parameters determined randomly for each of 10,000 simulations by the six user types shown in Table 4.

Table 2: Experiment 1: User Information Set

Item	User Information Set	
	User information disclosure risk	User information protection level
name	0.7	User input
age	0.1	User input
address	1.0	User input
sex	0.5	User input
telephone number	1.0	User input
location information	0.8	User input

Table 3: Experiment 1: Disaster Information Sharing Function Set

Item	Disaster information sharing function set	
	Function use risk	Disaster information request level
self-safety information provisioning function	{1.0, 1.0, 1.0, 1.0, 1.0, 1.0}	User input
third person safety information provisioning function	{1.0, 1.0, 1.0, 1.0, 1.0, 1.0}	User input
safety information request function	{1.0, 1.0, 1.0, 1.0, 1.0, 1.0}	User input
safety information search function	{1.0, 1.0, 1.0, 1.0, 1.0, 1.0}	User input

Table 4: Experiment 1: User Types

User	User input		User type	
	User information protection level	Disaster information request level	User information protection wish	Disaster information request
User_HL	0.7-1.0	0.0-0.3	strong	weak
User_LH	0.0-0.3	0.7-1.0	weak	strong
User_LL	0.0-0.3	0.0-0.3	weak	weak
User_MM	0.4-0.7	0.4-0.7	medium	medium
User_HH	0.7-1.0	0.7-1.0	strong	strong
User_Rand	0.0-1.0	0.0-1.0	random	random

Experiment 2 was designed to confirm the effectiveness and to view attributes of the proposed method in greater detail than experiment 1. The parameters of experiment 2 are shown in Tables 5 and 6. In this experiment, "name," "age," "address," "sex," "telephone number," "family structure" and "location information" were used as information items disclosed by a user. In experiment 2, the number of user information items was increased as compared to that in experiment 1 to verify the effectiveness of the proposed method in severe experimental conditions. In addition, "self-safety information," "relief supplies information," "utilities information," "haven information," "store information," "infrastructure recovery information" and "crime information" disaster information sharing functions were used. These functions were selected by referencing examples of effective utilization of internet services during the 2011 Great East Japan Earthquake. Since opportunistic crime increased significantly during the earthquake, the "crime information" function was added in experiment 2. The risk of information disclosure for the information items was set empirically based on the identification probability concept. In contrast to experiment 1, experiment 2 assumed that all disaster information sharing function items gave different risk to all information items. The function use risk of disaster information sharing function items was set to 1.0 or 0.0 for all user information items, which the disaster information sharing function requires a user to disclose in order to provide proper disaster information for individual users. In particular, the user information disclosure risk should be set to 0.0 for a user information item that does not need to be disclosed for a disaster information sharing function. The results shown in Tables 5 and 6 were determined by the ten user

Table 5: Experiment 2: User Information Set

Item	User Information Set	
	User information disclosure risk	User information protection level
name	0.7	User input
age	0.1	User input
address	1.0	User input
sex	0.1	User input
telephone number	1.0	User input
family structure	0.2	User input
location information	0.8	User input

Table 6: Experiment 2: Disaster Information Sharing Function Set

Item	Disaster information sharing function set	
	Function use risk	Disaster information request level
self-safety information	{1.0, 1.0, 1.0, 1.0, 1.0, 1.0, 1.0}	User input
relief supplies information	{0.0, 1.0, 1.0, 1.0, 0.0, 1.0, 1.0}	User input
utilities information	{0.0, 0.0, 1.0, 0.0, 0.0, 0.0, 1.0}	User input
haven information	{0.0, 0.0, 1.0, 0.0, 0.0, 0.0, 1.0}	User input
store information	{0.0, 0.0, 1.0, 1.0, 0.0, 1.0, 1.0}	User input
infrastructure recovery information	{0.0, 0.0, 1.0, 0.0, 0.0, 0.0, 1.0}	User input
crime information	{0.0, 0.0, 1.0, 1.0, 0.0, 0.0, 1.0}	User input

Table 7: Experiment 2: User Type

User	User input		User type	
	User information protection level	Disaster information request level	User information protection wish	Disaster information request
User_P0002Drand	0.0-0.2	0.0-1.0	weakest	random
User_P0204Drand	0.2-0.4	0.0-1.0	weak	random
User_P0406Drand	0.4-0.6	0.0-1.0	medium	random
User_P0608Drand	0.6-0.8	0.0-1.0	strong	random
User_P0810Drand	0.8-1.0	0.0-1.0	strongest	random
User_PrandD0002	0.0-1.0	0.0-0.2	random	weakest
User_PrandD0204	0.0-1.0	0.2-0.4	random	weak
User_PrandD0406	0.0-1.0	0.4-0.6	random	medium
User_PrandD0608	0.0-1.0	0.6-0.8	random	strong
User_PrandD0810	0.0-1.0	0.8-1.0	random	strongest

types shown in Table 7. The user information protection levels and disaster information request levels were determined randomly for each of the 10,000 simulations in the ranges shown in Table 7. In experiment 2, to examine the influence of user information protection levels and disaster information request levels on the effectiveness of parameter combinations, random parameters in five different ranges calculated as 1.0 divided by 0.2 ([0.0, 0.2], [0.2, 0.4],..., [0.8, 1.0]) were set as the levels for either user information protection and disaster information request, and random parameters from 0.0 to 1.0 were set to the levels of the other.

In the utility simple method, only the utility improvement obtained by a user was considered. When the extent of information disclosure of the utility simple method for information item i is expressed as $x_{\beta i} \in X_\beta (\subseteq X)$, the simple method is defined as follows.

$$x_{\beta i} = 1.0$$

With the intention simple method, when the user information protection level is high and disaster information request level is low, user information disclosure extent is low. When the user information protection level is low and the disaster information request level is high, user information disclosure

extent is high. When the user information protection level and disaster information request level are the same, the extent of user information disclosure is approximately 0.5. When the extent of user information disclosure of the simple method for information item i is expressed as $x_{\alpha i} \in X_\alpha (\subseteq X)$, the simple method is defined as follows.

$$x_{\alpha i} = 0.5 + \frac{w\_d'_i - w\_p_i}{2}$$

4.2 Evaluation Index

To evaluate the extent to which the proposed and simple methods consider the trade-off between user information protection and the quality of information and services, the following evaluation index using the harmonic mean of user information protection and utility was used. The functions that express the difference between the extent of information disclosure $x^*_i, x_{\alpha i}, x_{\beta i} (= x_i \in X)$ that the trade-off processing mechanism and the simple method decided for user information item i of $(i = 1, 2, ..., N_p)$ and user intention are expressed as follows.

$$\begin{aligned} D_\alpha(x_i; w\_p_i) &= |(1.0 - w\_p_i) - x_i| \\ D_\beta(x_i; w\_d'_i) &= |w\_d'_i - x_i| \end{aligned}$$

Here, $D_\alpha(x_i)$ expresses the difference in user intention relative to the desire user information protection level, and, $D_\beta(x_i)$ expresses the difference in user intention relative to the disaster information request. To represent the extent to which user intention can be considered in user information protection and user utility acquisition, user information protection performance $PA(x_i)$ and utility acquisition performance $UA(x_i)$ are expressed as follows, respectively.

$$\begin{aligned} PA(x_i; disc\_risk_i) &= disc\_risk_i * (1.0 - D_\alpha(x_i)) \\ UA(x_i; disc\_risk_i) &= disc\_risk_i * x_i * (1.0 - D_\beta(x_i)) \end{aligned}$$

Here, $disc\_risk_i * x_i$ expresses utility. It is preferable for users when $PA(x_i)$ and $UA(x_i)$ are high; however, $PA(x_i)$ and $UA(x_i)$ are in a trade-off relationship. Therefore, evaluation index F is expressed as follows.

$$\mathrm{F} = \sum_i^{N_p} \frac{2 * PA(x_i) * UA(x_i)}{PA(x_i) + UA(x_i)}$$

Here, evaluation index F is the total of the harmonic mean relative to user information protection performance and utility acquisition performance. Note that higher evaluation index F values are preferable for users. The harmonic mean is used as an index to evaluate a parameter in a trade-off relationship. Thus, evaluation index F allows quantitative evaluation of the extent to which this trade-off can be considered.

4.3 Experimental Result

Experiment 1
User Utility: Table 8 shows the experimental results of utility for each user in Table 4, and Figure 2 plots the results. The utility of all users for whom the extent of user information disclosure was determined by the utility simple method was uniformly 4.10, which is the largest utility regardless of user type. For all users for which the extent of user information disclosure was determined by the intention simple method, the proposed method showed higher utility in Table 4, with the exception

Table 8: Experiment 1: Utility

User	Utility -Simple	Intention -Simple	Proposed	Proposed / Utility -Simple*100[%]	Proposed / Intention -Simple*100[%]
User_HL	4.10	0.62	2.38	58%	386%
User_LH	4.10	3.49	2.80	68%	80%
User_LL	4.10	2.05	2.80	68%	137%
User_MM	4.10	2.05	2.42	59%	118%
User_HH	4.10	2.05	2.38	58%	116%
User_Rand	4.10	2.05	2.79	68%	136%
Average_LL-HH	4.10	2.05	2.53	62%	124%

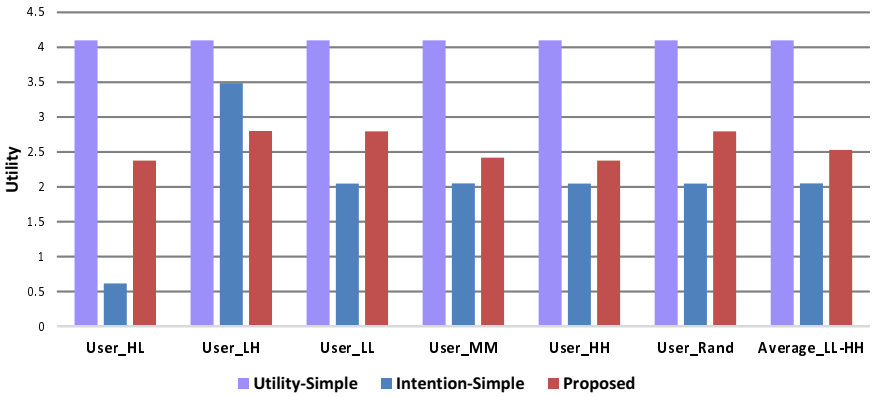

Figure 2: Experiment 1: Utility by method and user type

of User_LH. In particular, for User_Rand, where it is assumed that various users determined the user information protection level and disaster information request level randomly in the range [0.0, 1.0], the proposed method showed higher utility than the simple method (136%). For Average_LL-HH, i.e., the average of User_LL, User_MM, and User_HH, the proposed method showed higher utility than the simple method (124%). In addition, for User_HL, the proposed method showed higher utility than the simple method (386%). However, for User_LH the utility of the proposed method was 80% of the simple method.

Evaluation Index F: Table 9 shows the experimental results for evaluation index F for each user, and Figure 3 plots the results. The proposed method showed higher evaluation index F than the simple methods for the users, with the exception of User_LH and User_LL. For Average_LL-HH, the proposed method showed higher evaluation index F than the utility simple method (158%) and the intention simple method (105%). For User_HL, the proposed method showed higher evaluation index F than the utility simple method (309%) and the intention simple method (166%). However, for User_LH the evaluation index F of the proposed method was 78% of the utility simple method and 75% of the intention simple method.

Experiment 2

User Utility: Table 10 shows the experimental results of utility for each user in Table 7, and Figure 4 plots the results. The utility of all users for whom the extent of user information disclosure was determined by the utility simple method was uniformly 3.90, which is the largest utility regardless of user type. For all users for whom the extent of user information disclosure was determined by the intention simple method, the proposed method showed higher utility in Table 7. In particular, for User_P0810Drand (high information protection level) and User_PrandD0002 (low disaster information request level), the proposed method demonstrated higher utility than the simple method

Table 9: Experiment 1: Evaluation Index F

User	Utility -Simple	Intention -Simple	Proposed	Proposed / Utility -Simple*100[%]	Proposed / Intention -Simple*100 [%]
User_HL	0.54	1.01	1.68	309%	166%
User_LH	3.48	3.61	2.70	78%	75%
User_LL	1.03	1.76	1.77	171%	100%
User_MM	2.01	2.57	2.70	135%	105%
User_HH	1.00	1.78	1.93	193%	108%
User_Rand	1.81	2.30	2.52	139%	109%
Average_LL-HH	1.35	2.04	2.13	158%	105%

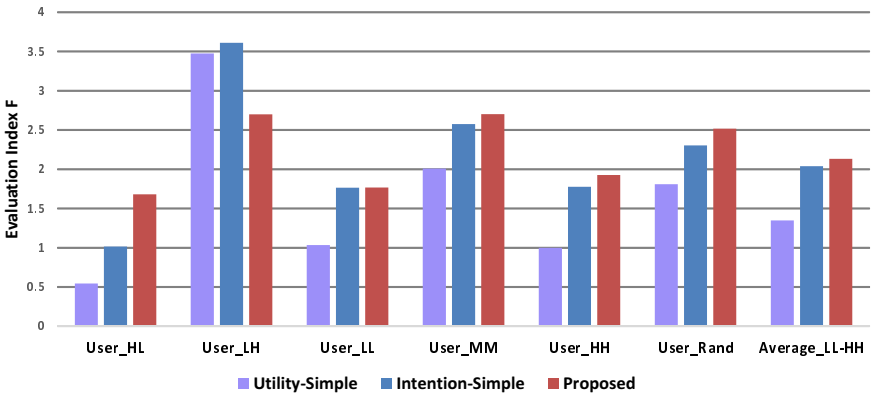

Figure 3: Experiment 1: Evaluation index F by method and user type

i.e., 335% and 246%, respectively. For User_Average, i.e., the average of all users in Table 7, the proposed method demonstrated higher utility than the simple method (177%).

Evaluation Index F: Table 11 shows the experimental results of evaluation index F for each user in Table 7, and Figure 5 plots the results. For the utility simple and intention simple methods, the proposed method showed higher evaluation index F for all users, with the exception of User_P0002Drand. For User_Average, the proposed method demonstrated 158% and 111% higher evaluation index F than the utility simple and intention simple methods, respectively. However, for User_P0002Drand, the evaluation index F obtained by the proposed method was 98% of the intention simple method, and the intention simple method demonstrated higher evaluation index F than the proposed method.

4.4 Discussion

In the utility simple method, utility for all users was constant at the maximum of 4.10 in experiment 1. For the intention simple method, utility was equal for User_LL, User_MM, User_HH, and User_Rand because the simple method cannot consider user utility when a trade-off occurs in user intention and utility. Thus, the extent of user information disclosure by the user intention simple method is set at approximately 0.5, i.e., the mid-point of user intention. In contrast, the proposed method demonstrates utility higher than the simple method because it considers user utility to determine the extent of information disclosure. In particular, for User_Rand, wherein various users were assumed, the proposed method showed a higher utility than the simple method (136%). In other words, these results indicate that the proposed method is effective for various users.

Table 10: Experiment2: Utility

User	Utility -Simple	Intention -Simple	Proposed	Proposed / Utility -Simple*100[%]	Proposed / Intention -Simple*100[%]
User_P0002Drand	3.90	2.31	2.79	59%	121%
User_P0204Drand	3.90	1.92	2.55	49%	133%
User_P0406Drand	3.90	1.53	2.52	39%	165%
User_P0608Drand	3.90	1.14	2.52	29%	221%
User_P0810Drand	3.90	0.75	2.51	19%	335%
User_PrandD0002	3.90	1.09	2.68	28%	246%
User_PrandD0204	3.90	1.31	2.72	34%	207%
User_PrandD0406	3.90	1.53	2.79	39%	182%
User_PrandD0608	3.90	1.75	2.91	45%	166%
User_PrandD0810	3.90	1.97	3.13	50%	159%
User_Average	3.90	1.53	2.71	39%	177%

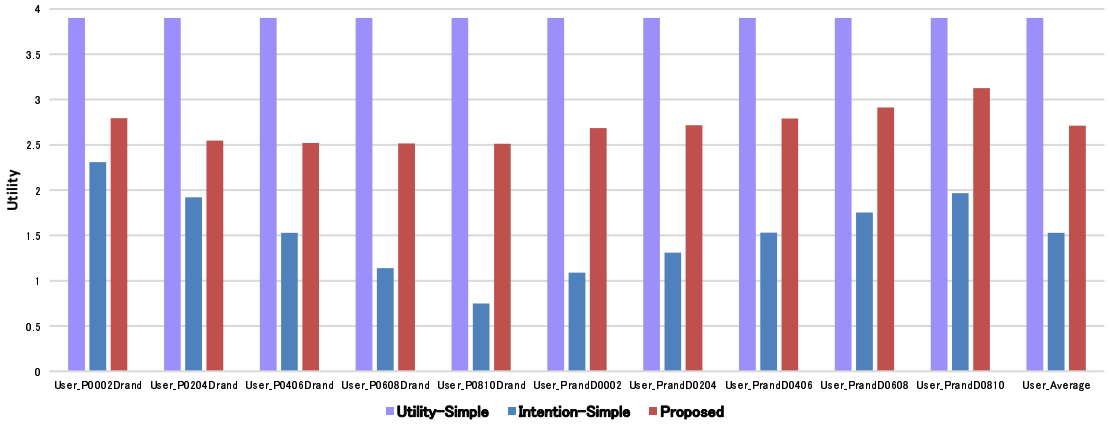

Figure 4: Experiment 2: Utility by method and user type

Table 11: Experiment 2: Evaluation index F

User	Utility -Simple	Intention -Simple	Proposed	Proposed / Utility -Simple*100[%]	Proposed / Intention -Simple*100[%]
User_P0002Drand	1.50	2.03	1.98	135%	98%
User_P0204Drand	1.38	2.05	2.14	149%	104%
User_P0406Drand	1.21	1.91	2.07	158%	109%
User_P0608Drand	0.94	1.54	1.87	163%	122%
User_P0810Drand	0.45	1.01	1.57	225%	156%
User_PrandD0002	0.35	1.16	1.33	335%	115%
User_PrandD0204	0.80	1.46	1.65	182%	113%
User_PrandD0406	1.11	1.72	1.89	154%	110%
User_PrandD0608	1.35	1.90	2.05	141%	108%
User_PrandD0810	1.52	1.98	2.08	130%	105%
User_Average	1.06	1.67	1.86	158%	111%

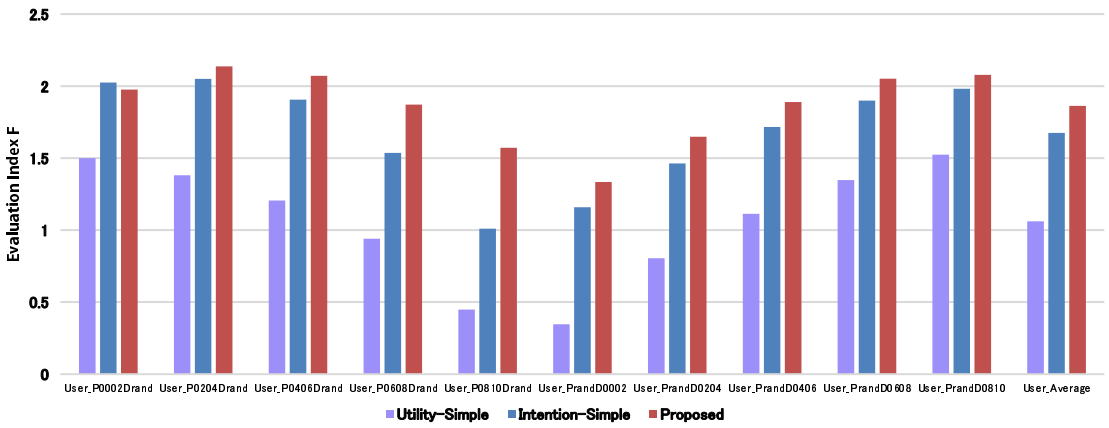

Figure 5: Experiment 2: Evaluation index F by method and user type

For User_LH in experiment 1, the utility of the proposed method was 80% of the intention simple method because the simple method shows extremely high utility in this case, such a combination of low user information protection level and high disaster information request level. In contrast, for User_HL, the proposed method showed a utility (386%) higher than the simple method because the simple method shows extremely low utility when the user information protection level is extremely high. With the utility simple method, utility for all users was constant at the maximum of 3.90 in experiment 2. For the intention simple method, as the user information protection level was higher, the utility decreased for User_P0002Drand, User_P0204Drand, User_P0406Drand, User_P0608Drand and User_P0810Drand. Similarly, as the disaster information request level was higher, the utility was scale for User_PrandD0002, User_PrandD0204, User_PrandD0406, User_PrandD0608, and User_PrandD0810. This is because the simple method cannot consider user utility when a trade-off occurs relative to user intention. In contrast, the proposed method demonstrated higher utility than the simple method. This is because the proposed method considers user utility to determine the extent of information disclosure. For Average_LL-HH/User_Average, i.e., the averages of all assumed users, the proposed method showed higher utility than the simple method (124%/177%). On the basis of these results, relative to user utility and careful consideration of the trade-off, the proposed method demonstrated higher utility than the simple method.

The utility simple method showed considerably lower evaluation index F than the intention simple method and the proposed method, with the exception of User_LH and User_P0002Drand because it does not consider user intention and cannot process the trade-off properly. The intention simple method showed the same level of evaluation index F with the proposed method for User_LL, and the proposed method showed slightly higher evaluation index F than the simple method for User_MM, User_HH, User_Rand and User_P0204Drand. Since the proposed method showed higher utility than the simple method for these users and demonstrated the same or higher evaluation index F than the simple method, the proposed method can process the trade-off properly in consideration of user utility. For User_HL, the proposed method showed much higher utility (386%) than the simple method; however, the proposed method showed little higher evaluation index F (166%) because the proposed method considers both user intention and user utility when determining the extent of information disclosure. Thus, user intention is sacrificed to some degree. For User_LH, evaluation index F of the simple and proposed methods similarly differs with user utility owing to the weak trade-off that occurs between user information protection performance and utility acquisition performance because the obtained utility significantly affects the evaluation index F.

5 Conclusion

During massive natural disasters, it is necessary to provide proper disaster information to people based on user information; however, a trade-off relationship occurs between the protection of user information and the quality of service. To address this problem, this study has proposed a trade-off processing mechanism to determine the extent of user information to be disclosed to realize a method to rationally determine the extent of user information to be disclosed and the extent of disaster information to be provided. This is achieved in consideration of the trade-off relationship between the extent of user information disclosure and the quality of disaster information and services. The effectiveness of the proposed method was verified through experiments that evaluated the trade-off processing mechanism with disaster information sharing functions. The experiments were conducted using the proposed method and a simple determination method wherein both the utility (utility simple method) and intention (intention simple method) of the user were considered relative to the extent of user information disclosure. In addition, the extent to which the trade-off was considered for each user type was evaluated quantitatively.

In future, to further verify the effectiveness of the proposed method, we will experiment with a nonlinear utility function and more precise conditions for disaster information sharing by users. Furthermore, we will apply the trade-off processing mechanism to other service provision systems.

Acknowledgment

This research was partially funded by a Grant-in-Aid for Scientific Research (Wakate Kenkyu B (26730054)).

References

[1] Y.-A. de Montjoye, E. Shmueli, and A. S. Pentland. openpds: Protecting the privacy of metadata through safeanswers. *PloS One*, 9(7):e98790, 2014.

[2] Foundation for Multimedia Communications. L-aleart. *available at: http://www.fmmc.or.jp/commons/*, accessed 11 February 2016.

[3] google.org project. Google person finder. *available at: https://www.google.org/personfinder/japan*, accessed 11 February 2016.

[4] D. Ikarashi, K. Chida, and K. Takahashi. A probabilistic extension of k-anonymity. In *Computer Security Symp. 2009 (CSS2009)*, volume 2009, pages 1–6, 2011 (in Japanese).

[5] M. Imada, M. Ohta, and M. Yamaguchi. Loom: An anonymity quantification method in pervasive computing environments. In *Proceedings of the 20th International Conference on Advanced Information Networking and Applications (AINA06)*, volume 1, pages 92–96, 2006.

[6] M. Imada, K. Takasugi, M. Ohta, and K. Koyanagi. A loosely managed privacy protection method for ubiquitous networking environments. *IEICE Trans. on Communications*, J88-B(3):563–573, 2005 (in Japanese).

[7] T. Kamishima. Algorithms of recommender systems. *available at: http://www.kamishima.net/archive/recsysdoc.pdf*, pages 1–134, 2016 (in Japanese).

[8] T. Kawai and H. Fujishiro. Use of twitter in the disaster information after the great east japan earthquake. *Corporate communication studies*, (17):118–128, 2013 (in Japanese).

[9] K.Hamamoto, Y. Tahara, and A. Ohsuga. A proposal for privacy preserving agent by anonymization based on user background information and community status. *IEICE Trans. on Information and Systems*, J94-D(11):1812–1824, 2011 (in Japanese).

[10] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramaniam. l-diversity: Privacy beyond k-anonymity. *ACM Trans. on Knowledge Discovery from Data (TKDD)*, 1(1):Article No. 3, 2007.

[11] M. Miyabe, A. Miura, and E. Aramaki. Use trend analysis of twitter after the great east japan earthquake. In *Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work Companion*, pages 175–178, 2012.

[12] T. Miyamoto, K. Harumoto, S. Shimojo, and T. Okuda. Grip - a profile control mechanism for user privacy protection and quality of personalization services. In *PACRIM. 2005 IEEE Pacific Rim Conference on Communications, Computers and signal Processing*, pages 217–220, 2005.

[13] NTT and NHK. J-anpi. *available at: http://anpi.jp/top*, accessed 11 February 2016.

[14] H. A. Simon. Theories of bounded rationality. *Decision and organization*, 1(1):161–176, 1972.

[15] L. Sweeney. k-anonymity: a model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(5):557–570, 2002.

[16] Department of Human Utida Laboratory, Information Science School of Information Science, and Tokai University Technology. Disaster information tweeting system. *available at: http://saigai.main.jp/SmartDevice/index.html*, accessed 11 February 2016.