International Journal of Informatics Society

12/10 Vol. 2 No. 3 ISSN 1883-4566

Informatics Society

Aims and Scope

The purpose of this journal is to provide an open forum to publish high quality research papers in the areas of informatics and related fields to promote the exchange of research ideas, experiences and results.

Informatics is the systematic study of Information and the application of research methods to study Information systems and services. It deals primarily with human aspects of information, such as its quality and value as a resource. Informatics also referred to as Information science, studies the structure, algorithms, behavior, and interactions of natural and artificial systems that store, process, access and communicate information. It also develops its own conceptual and theoretical foundations and utilizes foundations developed in other fields. The advent of computers, its ubiquity and ease to use has led to the study of informatics that has computational, cognitive and social aspects, including study of the social impact of information technologies.

The characteristic of informatics' context is amalgamation of technologies. For creating an informatics product, it is necessary to integrate many technologies, such as mathematics, linguistics, engineering and other emerging new fields.

Guest Editor's Message

Yuko Murayama
Guest Editor of the Sixth Issue of International Journal of Informatics Society

We are delighted to have the sixth and special of the International Journal of Informatics Society (IJIS) published. This issue includes selected paper from the Third International Workshop on Informatics (IWIN2009), which was held in Honolulu, Hawaii, USA, Sep. 11-17, 2009. The workshop was held at Hawaii Tokai International College (HTIC). This workshop was the third event for the Informatics Society, and was intended to bring together researchers and practitioners to share and exchange their experiences, discuss challenges and present original ideas in all aspects of informatics and computer networks. In the workshop, 27 papers were presented at four technical sessions. The workshop was complete in success. It highlighted the latest research results in the area of networking, business systems, education systems, design methodology, groupware and social systems.

Each IWIN2009 paper was reviewed in terms of technical content and scientific rigor, novelty, originality and quality of presentation by at least two reviewers. From those reviews, 14 papers are selected for publication candidates of IJIS Journal. Among those 14 papers, six papers are related to information systems. This sixth issue focuses on information systems and includes those selected five papers. The selected papers have been reviewed from their original IWIN papers and accepted as publication of IJIS. The papers were improved based on reviewers' comments.

We hope that the issue would be of interest to many researchers as well as engineers and practitioners in this area.

We publish the journal in print as well as in an electronic form over the Internet. This way, the paper will be available on a global basis.

Yuko Murayama is a professor at Iwate Prefectural University, Japan. She had M.Sc. and Ph.D. both from University of London in 1984 and 1992, respectively. She had been a visiting lecturer at Keio University from 1992 to 1994, a lecturer at Hiroshima City University from 1994 to 1998. She has been with Iwate Prefectural University since April 1998. Her interests include internetworking, network security and trust. She is a member of ACM, IEEE, IPSJ, IEICE, and ITE.

Technology for Recommending Optimum Learning Texts Based on Data Mining of Learning Historical Data

Yuji Wada [*], Yuuma Hamadume [**], Shinichi Dohi [*], and Jun Sawamoto [***]

[*] Department of Information Environment, Tokyo Denki University, Japan
[**] Kobe Office, Konami Digital Entertainment Corporation Limited, Japan
[***] Faculty of Software and Information Science, Iwate Prefectural University, Japan
yujiwada@sie.dendai.ac.jp, DEN03738@nifty.com , dohi@sie.dendai.ac.jp, and sawamoto@iwate-pu.ac.jp

Abstract - We are developing a bidirectional recommendation system that extracts the relationship among digital texts with historical logs, and recommends the optimum texts for learners using data mining methods, such as collaborative filtering. In this paper, we first discuss the bidirectional recommendation and then show results from an evaluation of actual use. Finally, we propose a method for a collaborative learning recommendation system that mines the data of similar users sharing non-favorite subjects using historical logs and user attribute data.

Keywords: e-learning, data mining, recommendation, historical log analysis, collaborative filtering.

1 INTRODUCTION

In recent years, large numbers of institutions of higher learning, businesses and other organizations have been proactively introducing e-learning. That movement has been fostered in part by attention focused on the Web Based Training (WBT) approach [1], leading to the debut of numerous Learning Management Systems (LMS) [1]. Additionally, the proposal of the Sharable Content Object Reference Model, or SCORM [2], which is a global standard, has helped to spur the propagation of e-learning. Opinions are divided, however, as to whether the use of e-learning offers greater advantages to the learner than learning based on paper materials.

To address that question, firstly we implemented a "bidirectional recommendation system" [3] (see Figure 1) developed in our laboratory, in the AIRS "An Individual Reviewing System" [4]. Figure 1 shows a schematic of a bidirectional recommendation. When a learner is browsing the learning text "Basics of Assignment," it is natural to advance to the next step "Basics of 'while' statement" or "Basics of 'if' statement." However, browsing the basic contents "Variable types" again is also natural in learning. In other words, the learning efficiency is expected to improve by recommending not only learning texts frequently shifted from but also frequently shifted to "Basics of Assignment."

This research is supported by a Grant-in-Aid for Scientific Research C (Subject No. 21500908: Research on Adaptive Recommendation Technology based on Bidirectional Recommendation Technology for E-Learning Texts).

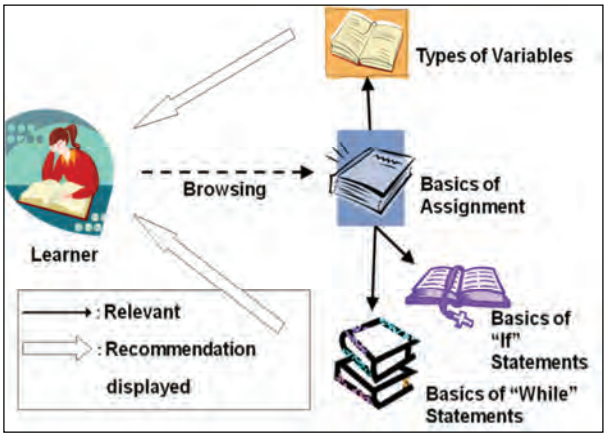


Figure 1: Bidirectional recommendation system.

Secondly, we asked 92 participants of the "Database System" lecture offered by the university to use the system between October 30 and November 5, 2008.

Subsequently, we conducted a survey using questionnaires that examined the actual situation of the user and the learning outcome achieved using the bidirectional recommendation system (see Table 1). In the survey, a number of respondents indicated that they were able to shorten the time spent learning, and the efficacy of learning using the bidirectional recommendation system was confirmed.

Moreover, a recommendation accuracy of 61% resulted from subjective evaluation by users of the appropriateness of the recommendation results (see Table 2). Some respondents indicated, however, that they preferred to browse the lecture materials, so we reexamined the functions requested by learners.

Table 1: User evaluation of bidirectional recommendation system.

Opinions of those indicating that recommendation results were appropriate	Opinions of those indicating that recommendation results were not appropriate
It was easy to figure out what to look at next and less time was required.	I prefer to look at lecture materials and course handouts.

Table 2: Recommendation precision of bidirectional recommendation system.

Percentage of respondents who said that the recommendation results were suitable, or somewhat suitable
Recommendation precision = 61%

We surmised that perhaps the objective of learners using this approach is to thoroughly review using the material used in lectures and deepen their understanding of it, even if it required more time. Based on this, we hypothesized the necessary function to be support information used when reviewing. For example, this could refer to “areas of weakness” that the learner finds harder to understand than the rest of the text.

Based on this, we proposed a “collaborative learning recommendation system" using e-learning, and developed a system designed to improve learning efficacy by recommending “areas of weakness” (hereafter referred to as “non-favorite subject material”).

Finally, we surveyed the state-of-the-art about the recommendation technologies such as collaborative filtering and data mining, as follows. In [5], the design and implementation of a recommender system using social networks was described. In [6], a web content recommendation system based on the similarities is proposed. In [7], collaborative filtering based on C-SVM(Support Vector Machine) was proposed examined. In [8], data mining technologies, such as clustering and sequential pattern mining, for online collaborative learning data are studied. In [9], monitoring online tests, such as learner behavior and test quality, through data visualization are discussed. In [10], an automated learning and skills training system for a database programming environment is presented. In [11], a personalized active recommendation system called COALE is proposed and COALE gives proper awareness at proper timing for each learner to support dynamic course organization aimed at effective and efficient learning. In [12], a hybrid collaborative filtering technique is studied and it is shown to be efficient to make just-in-time recommendation.

In our research, we proposed a method for a collaborative learning recommendation system that mines the data of similar users sharing non-favorite subjects using historical logs and user attribute data. The method for mining non-favorite subject material proposed here is based on the assumption that the more times the content has been browsed, the less skilled the learner is in that subject. In addition, for new learners who do not possess a learning history, we proposed a method which uses attribute data to mine data for learners having similar preferences.

From the above survey results, we found that there are no existential research results which provide a solution on the recommendation technology using attribute data of learners having similar preferences for the new learners who do not possess a learning history. This is our research originality.

2 AIRS AND UTILIZATION STATUS

AIRS is an e-learning system that focuses specifically on review, and was developed starting from fiscal 2004 (see Figure 2).

Figure 2 displays the AIRS Japanese top page after a learner, who is going to review the database contents especially selection function, logs in AIRS. This page is comprised of the book marks (located at the upper side) of the contents available with AIRS, the contents menu (located at the left side) corresponding to the selected book mark, and the help messages for beginners (located at the right side). In figure 2, the contents menu displays database, data model, RDB, design methodology, and SQL. The learner selects the book mark such as selection and sorting before the learner can select the corresponding database contents menu. Then, the learner can proceed to review the database contents.

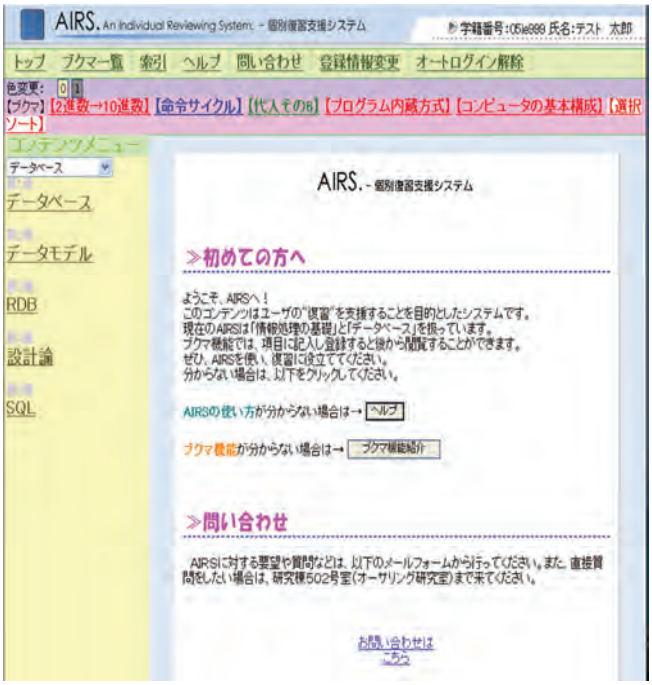


Figure 2: AIRS Japanese top page after login.

By focusing solely on review, the system reduces the possibility that the learner will rely on e-learning instead of sufficiently participating in lectures.

The system is also designed with the aim of improving learning efficacy through the synergistic effect of lecture-based learning and e-learning.

One feature of the system is that it is an e-learning system by learners, for learners. This reason is that system is designed to make learning easier, by having the developers attend lectures corresponding to the teaching content and develop content, to some extent, by anticipating sections that learners would have difficulty understanding (see Figure 3).

Additionally, the system is constructed so that each item being taught is expressed in three different ways (not yet fully implemented), and a function is provided by which learning is tailored to the individual learner, with the appropriate “form of expression” (refer to [13]) for that particular learner being automatically extracted.

[Database]

What is a database?

A collection of the necessary data = data cluster

or

A data box into which data is put

A collection of data put together based on certain criteria is a database, see

Learner database

No.	Name	School register	Grade	Activity group
1	T	IE	B	Baseball
2	S	ID	S	Swimming
3	K	IE	A	Basketball

Current level: 1

Let's add more detail!

Figure 3: Example: contents of text.

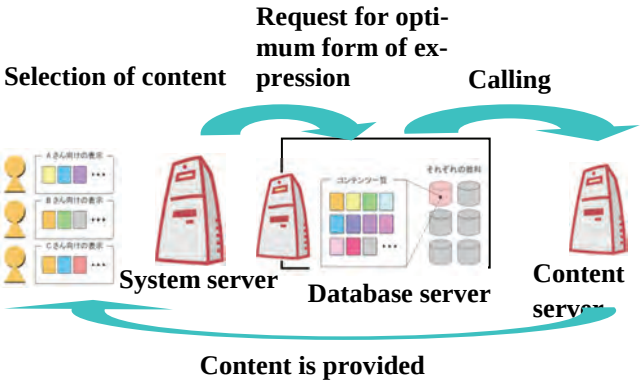


Figure 4: Configuration of AIRS.

The system comprises a database server that runs databases used by functions, such as the one mentioned previously, a content server that makes teaching content available, and a system server that runs AIRS (see Figure 4).

The results of a questionnaire survey, conducted this fiscal year, concerning utilization status are shown in Figure 5. As previously mentioned, the survey targeted 92 participants of the "Database System" lecture offered by the university.

3 BIDIRECTIONAL RECOMMENDATION SYSTEM

The aim of the system is to make it possible for learners to learn efficiently, without having to worry about selecting the content that was expanded through propagation of SCORM.

Moreover, based on the browsing history data of AIRS, it was found that an extremely large number of learners are sequentially browsing the course material in accordance with

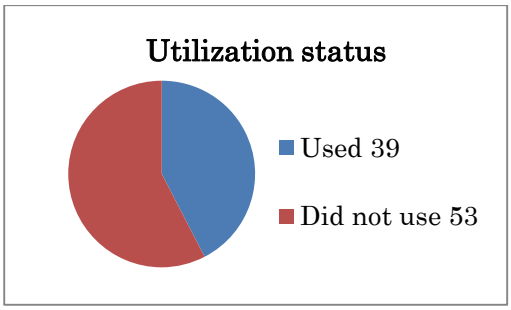


Figure 5: Usage achievements of AIRS.

the flow of the material displayed on the screen. This is not different from review using paper materials and suggests learning efficacy will decrease as the volume of material expands. In actuality, the number of AIRS nodes (not taking the "form of expression" into consideration) has grown to 210 for two subjects. To solve these problems, the bidirectional recommendation system was developed as a means for recommending course material that is strongly relevant to the material currently being read, and thus improving both review efficiency and speed.

An overview of the system is presented here, together with a detailed description of the questionnaire previously described.

3.1 Overview

The system overview is presented in Figure 1. We assume here that the learner is browsing the material for the course called "Basics of Assignment" under "Fundamentals of Information Processing". At this point, the learner would naturally shift to the next steps, "The Basics of the 'While' Statement" and "The Basics of the 'If' Statement".

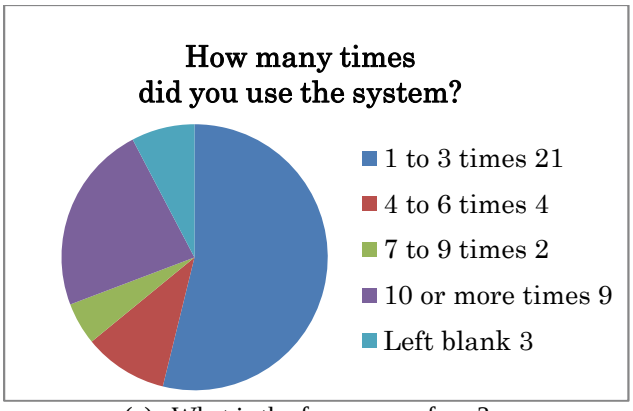
However, during the review process, it would not be unnatural for the learner to go back and re-read "Types of Variables", which is part of the basic content. In other words, learners could review the material, if the system, instead of recommending only material to which many learners shift after reading "Basics of Assignment" at the same time, recommends material that many learners read before moving to "Basics of Assignment". Looking back over material is a fundamental part of the review process, and we could expect an improvement in learning efficiency. This is why bidirectional recommendations are necessary, and is a feature of the bidirectional recommendation system.

3.2 Evaluation

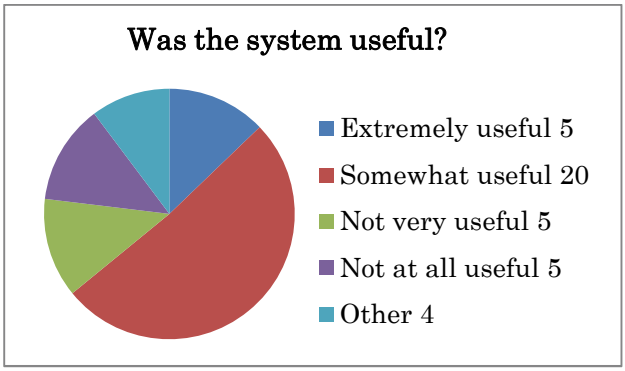
Users of the bidirectional recommendation system filled out questionnaires regarding the number of times they used the system, the recommendation results, learning efficiency, whether or not they would like to use the system in the future, operability and other questions. The results are shown in Figure 6.

The targeted users and the organizations conducting the survey are the same as those for the questionnaire survey previously described.

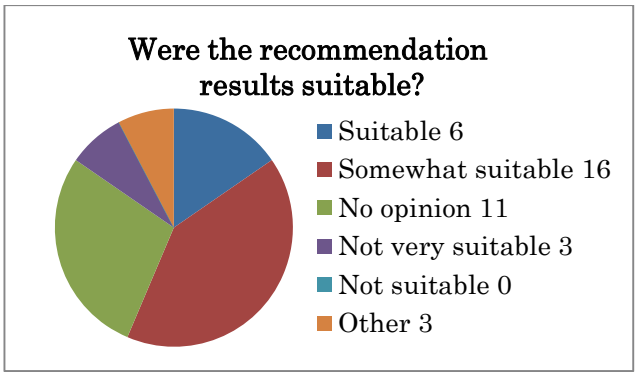
The results indicated a large number of learners used the system infrequently because they had problems logging in.



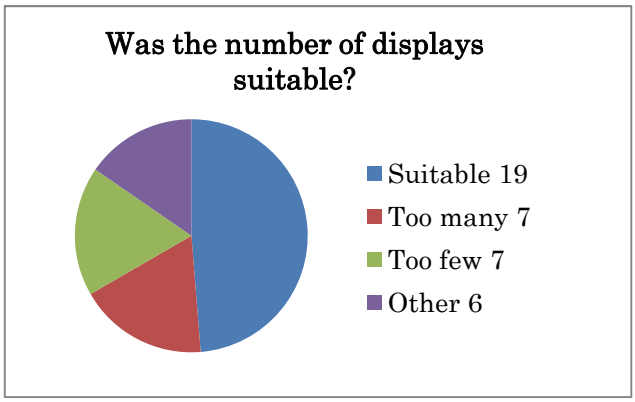
(a) What is the frequency of use?



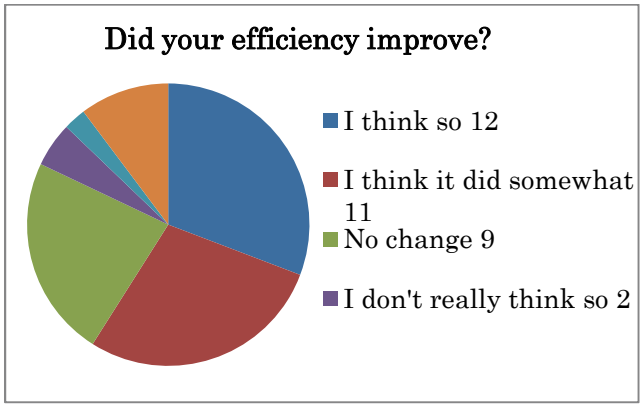
(b) Is it useful?



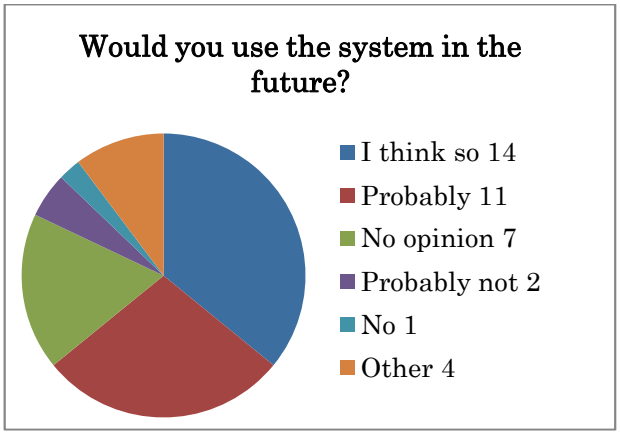
(c) Is it suitable?



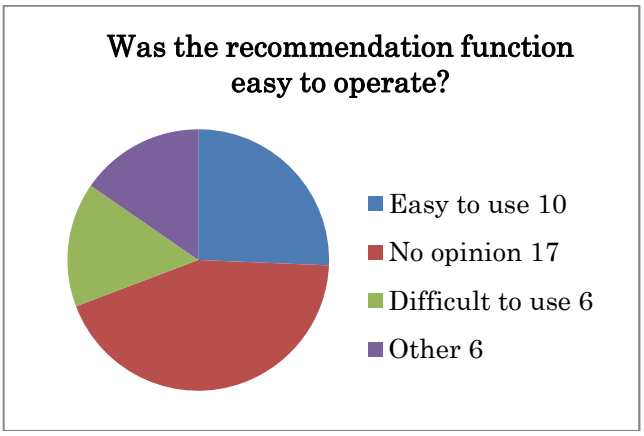
(d) What is the number of displays?



(e) Is it efficient?



(f) Will you use it in the future?



(g) Is it easy to operate?

Figure 6: User evaluation results of bidirectional recommendation system.

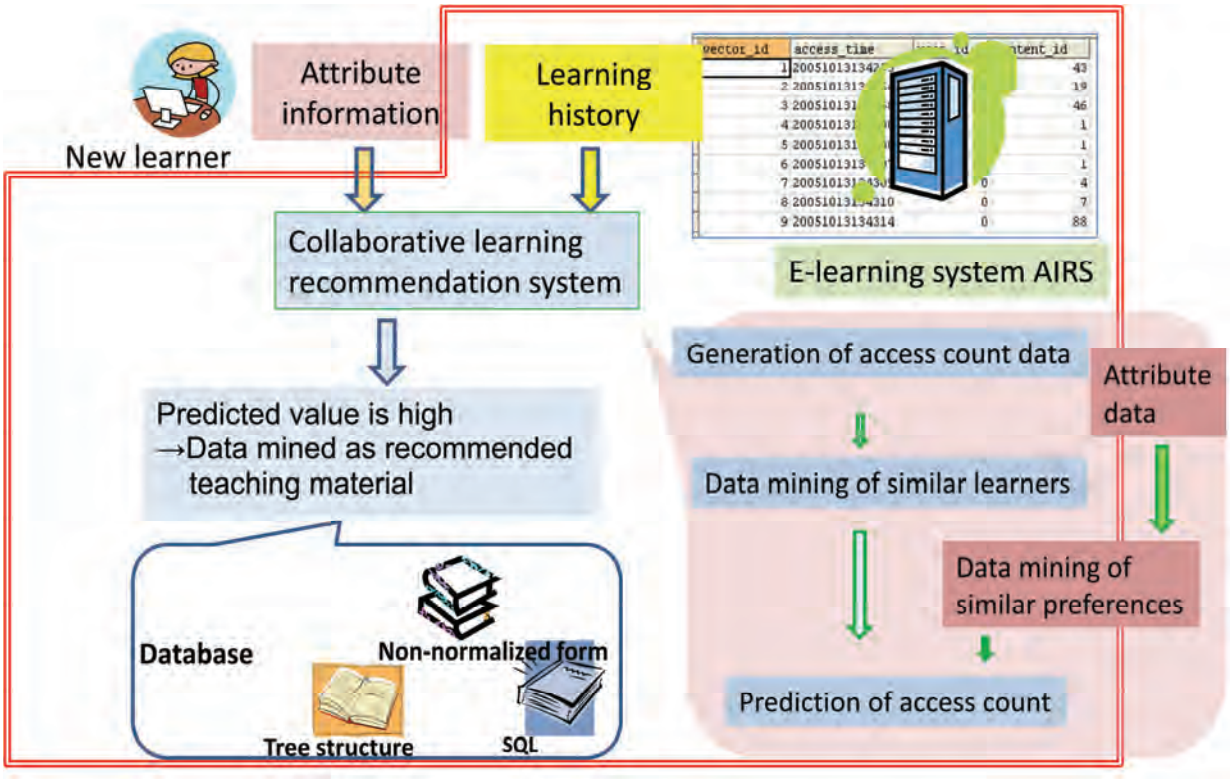


Figure 7: Overall system flow.

Even taking that into consideration, the majority of users obtained favorable results using the system for only one week, and the system can be expected to improve learning efficacy.

Firstly, 64% of the respondents said that the system was useful as shown in Figure 6 (b).

Secondly, 66% of the respondents said that the recommendation results were suitable as shown in Figure 6 (c).

Thirdly, 58% of the respondents said that efficiency improved as shown in Figure 6 (e).

Moreover, 64% of the respondents said that they would use the system in the future, including those who thought the contents were easy to understand and those who would use it if errors were corrected, as shown in Figure 6 (f).

However, 74% of the respondents said that the recommendation function is not easy to operate as shown in Figure 6 (g).

4 COLLABORATIVE LEARNING RECOMMENDATION SYSTEM

A characteristic feature of the proposed method is that it identifies learners exhibiting similar areas of weakness and recommends information for overcoming these weaknesses. Figure 7 shows the overall flow. This method functions by recommending teaching material via a collaborative learning recommendation system in which the learning history is used as the basic data. For new learners having no learning history, recommendations are made using the attribute information.

4.1 Learner Access Count Data

First, as a pre-process, the learning history is converted to generate data indicating the number of times each learner accessed the respective teaching material. Table 3 shows an excerpt of this data. The first line indicates the number of accesses by learner number 0 and shows that content1 was accessed 53 times, content4 was accessed 49 times and content7 was accessed 40 times. In addition to providing directly observable values, this data is thought to reflect such characteristics as the learner's interests and level of proficiency. In the case of a system such as AIRS that aims to support learning, the learners' objectives are to prepare for and review lectures, but because the use of such systems thus far has been limited to times prior to examinations, the learner's objective can be considered to be review. In other words, this data is thought to indicate areas in which the level of understanding is inadequate and weaknesses exist.

Table 3: Access count data.

user_id	con1	con2	con3	con4	con5	con6	con7
0	53	0	0	49	0	0	40
1	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0
3	2	0	0	1	0	0	2
4	9	0	0	7	0	0	5
5	5	0	11	1	0	0	0
6	4	0	0	0	0	0	1
7	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0
9	9	0	0	12	0	0	1
10	0	0	0	0	0	0	0

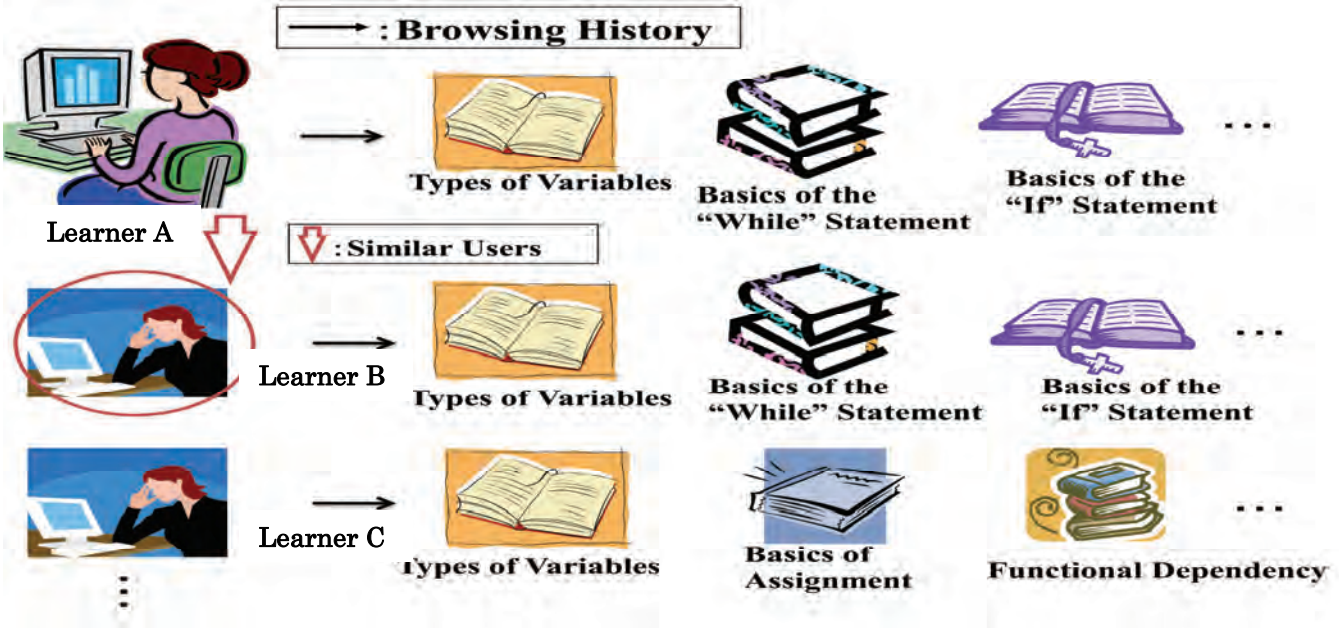


Figure 8: Mining of browsing history data to identify similar users

4.2 Data Mining of Similar Learners

The access count data described in Table 3 is compared for all learners to mine data for learners having similar weaknesses, or in other words, similar learners. Figure 8 illustrates the concept of similar learner data mining. Here, Learner A, as well as Learner B and Learner C, has a learning history. At this time, Learner A accessed the teaching materials of "Types of variables," "Basics of the 'while' statement" and "Basics of the 'if' statement," Learner B similarly accessed the same three materials and Learner C accessed the materials of "Types of variables," "Basics of assignment" and "Functional dependence." In this case, because the teaching materials accessed by Learner A and Learner B are similar, there is a high degree of resemblance between Learner A and Learner B, and therefore they are similar learners.

A correlation coefficient algorithm, implemented, for example, in collaborative filtering [14], is used in the actual mining of data for similar learners. The form of the computational equation applied in this research is shown in equation (1) below.

$$r_{ab} = \frac{\sum_{i=1}^{T}(a_i-\bar{a})(b_i-\bar{b})}{\sqrt{\sum_{i=1}^{T}(a_i-\bar{a})^2}\sqrt{\sum_{i=1}^{T}(b_i-\bar{b})^2}} \qquad (1)$$

The above r_{ab} is the resemblance between Learner A and Learner B. This r is the first letter of the word resemblance. Values of r range from 1.0 to –1.0, and values approaching 1.0 indicate greater resemblance, values approaching –1.0 indicate less resemblance, and the value 0 indicates that there is no relationship. The numerator indicates covariance, and the denominator indicates the product of the standard deviations.

The above a_i indicates the number of times Learner A has accessed the i[th] teaching material and $\bar{a}$ indicates the average number of accesses per teaching material. As well, the above b_i indicates the number of times Learner B has accessed the i[th] teaching material and $\bar{b}$ indicates the average number of accesses per teaching material. T indicates the total number of teaching materials. The learners found to have a high degree of resemblance according to this method are mined as similar learners.

4.3 Data Mining of Recommended Teaching Material

Here, assuming that the history of similar learners contains a history of overcoming weaknesses, teaching material that has been accessed many times by similar learners is mined as teaching material that helps to overcome these learners' weaknesses. Figure 9 shows the method of mining recommended teaching material. In this example, similar learners accessed "Types of variables" three times, "Basics of the 'while' statement" nine times, "Basics of the 'if' statement" five times and "Basics of arrays" two times. If recommended teaching materials are mined from the historical data, "Basics of the 'while' statement" and "Basics of the 'if' statement," which were the most frequently accessed, will be recommended to learners.

The actual computation for mining recommended teaching materials is performed by a method that calculates the predicted value used with collaborative filtering. The data for this calculation is based on the resemblance among similar learners and the learner vector of similar learners, and the value calculated is the predicted value of the access count. In this study, the predicted value is computed using equation (2) below.

$$P_{a,1} = \bar{\alpha} + \frac{\sum_{U_i \in \mathrm{User}}(C_{i,1}-\bar{C}_i)r_{ai}}{\sum_{U_i \in \mathrm{User}}|r_{ai}|} \qquad (2)$$

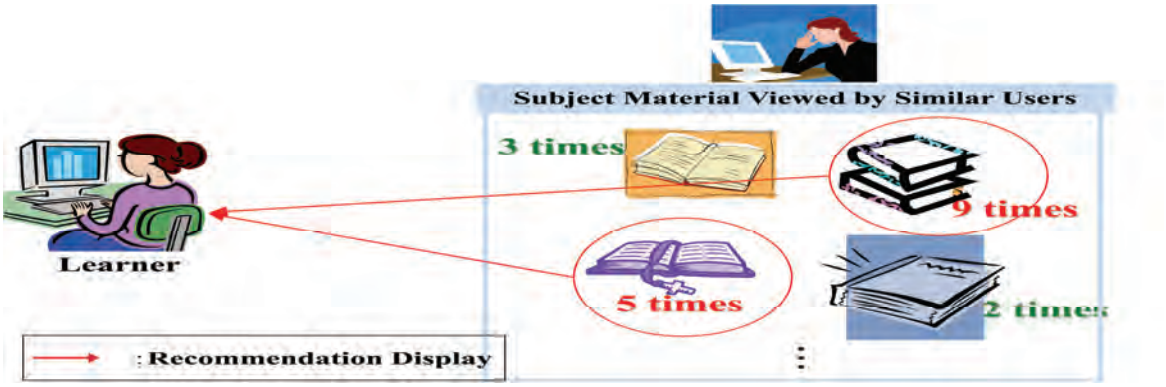


Figure 9: Data mining of non-favorite subject material.

Here, $P_{a,1}$ is the predicted value (predicted access count) necessary for Learner A to overcome a weakness in teaching material 1. For example, in the case where $P_{a,1}$ has a value of 3.4, Learner A is thought to be able to overcome his or her weakness in teaching material 1 by accessing that content approximately three times. Also, $\bar{\alpha}$ is the average number of times that a group of learners having some correlation with the Learner A (i.e., learners having a non-zero resemblance value) accessed the teaching material; in other words, the average of the average access count. "User" is a group of learners having some correlation with Learner A, and the i^{th} learner within this group is denoted as U_i. $\bar{C}_i$ indicates the number of times that the i^{th} learner accessed teaching material 1,$\bar{C}_i$ is the average access count and indicates the average number of times that the i^{th} learner reviewed any single teaching material, and r_{ai} indicates the resemblance between Learner A and the i^{th} learner. In this manner, teaching material for which the predicted access count is a large value is mined as recommended teaching material.

5 MINING DATA OF SIMILAR USERS

5.1 Attribute Data and Similar Users

Information not obtained by AIRS includes the learner attribute data, such as age, gender, hobbies and preferences.

In the present study, the strong subjects, non-favorite subjects, average learning time, hobbies and preferences, number of AIRS logins, usage time and other parameters of the user were additionally defined as learner attribute data. The purpose of acquiring this attribute data was to provide detailed recommendations even if the user was new to the system.

When browsing histories of similar users are mined (see Figure 8), new users are unable to find similar users because they have no learning history data, and recommendation accuracy drops sharply as a result. When all users have the same attribute data, it becomes possible to mine data for new users and similar users as well. The method for mining attribute data of similar users is shown in Figure 10.

The collaborative filtering method was used for mining the data of similar users, and mining of non-favorite subject material was done as described in section 4 (see Figure 9).

5.2 Effective Attribute Data Group

In the present study, mining all of the attribute data would not be useful in identifying similar users. Therefore, it was considered important to identify "attribute data groups" that were useful or effective, consisting of combinations of several attribute data elements.

A method proposed for identifying these attribute data groups is shown in Figure 11.

(Step 1) First, one attribute data combination is created by an e-learning system administrator (such as AIRS administrator). For the time being, this is called the "first attribute group".

(Step 2) Similarity between users is calculated using the equation (1) as mentioned before. Similar users are identified measuring the value of the similarity as described in section 4.2, referring to this first attribute group (see Figure 10). These are "similar users based on the first attribute group".

(Step 3)The "similar users based on the first attribute group" (for example, Learner B and D in Figure 11) identified at step 2 are compared to the "similar users based on browsing histories" (for example, Learner B and D in Figure 11) identified using the method described in section 4 (see Figure 8). This means whether the name of the former similar user is equal to that of the latter similar user or not. And, the percentage of matches is calculated as the match rate.

(Step 4) The learner who will serve as the reference is substituted for Learner B, and the match rate is calculated by repeating steps 2 and 3. In the same way, the match rates for subsequent learners (e.g., Learner C, Learner D) are determined until match rates have been determined for all of the users. The total of the match rates for all users is then divided by the number of users (n) to find the mean match rate, and that value is used as the "effective index of the first attribute group".

(Step 5) If all combinations of attribute data have been processed, then this step exits. Otherwise, another attribute data group is created at step 1 again, and the process through step 4 is repeated.

The effective index sequentially increased to find the "most effective attribute data group" in the course of repeating the above steps. But, the computing time complexity of this method is $O(n^2)$. As this is not the efficient algorithm, we are planning its improvement.

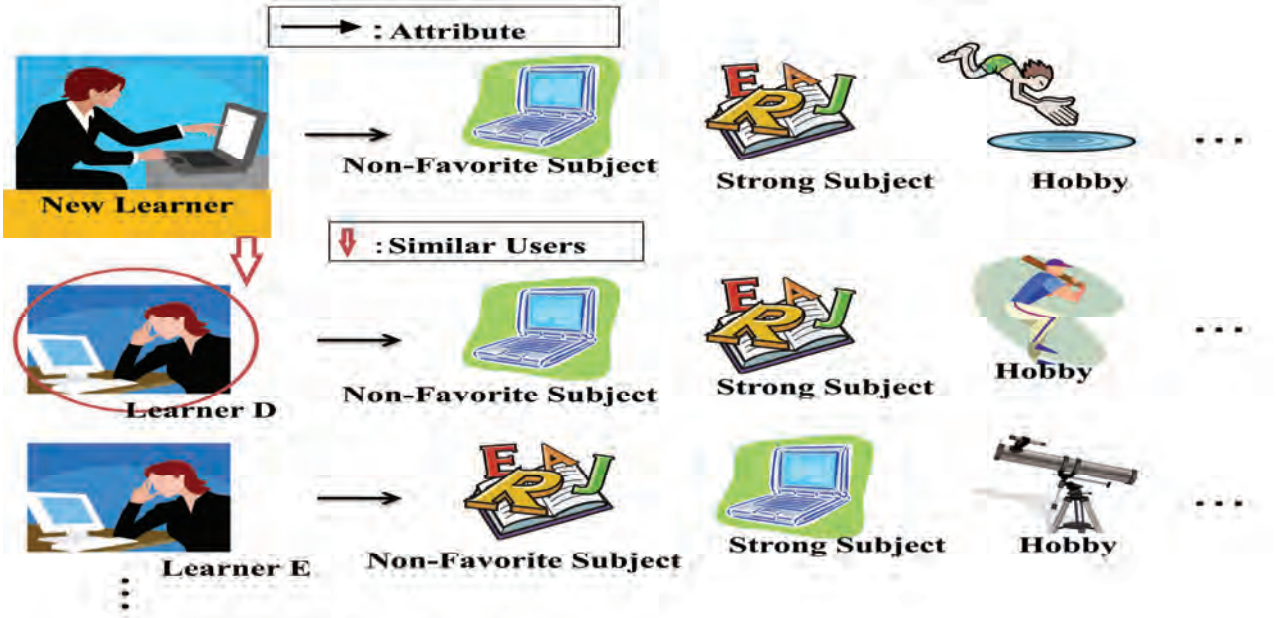


Figure 10: Method for mining attribute data of similar users.

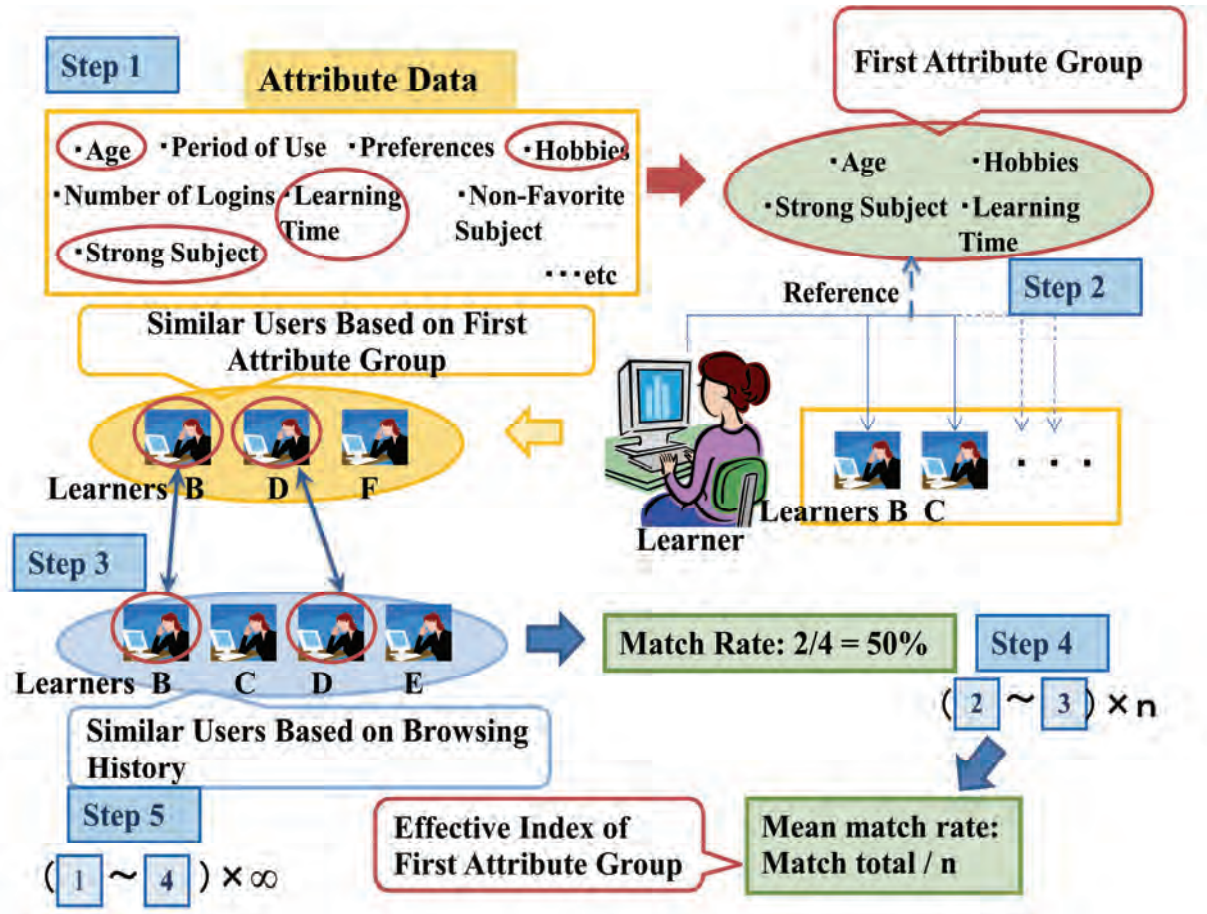


Figure 11: Method for mining useful attribute data.

6 CONCLUSION

In this paper, we proposed a method for a collaborative learning recommendation system that mines the data of similar users sharing non-favorite subjects using historical logs and user attribute data.

The method for mining non-favorite subject material proposed here is based on the assumption that the more times the content has been browsed, the less skilled the learner is in that subject.

For this reason, we currently plan to develop a collaborative learning recommendation system and implement it in the AIRS, and to verify the appropriateness of the recommendation results by measuring recommendation precision.

Then, the recommendation precision will be measured using the following data:

(1) Questionnaire results reflecting the subjective view of the student (user),

(2) Information relating to teaching material in which the learner is thought to be weak (as indicated by the course instructor),

(3) Comparison results of learning effectiveness between students who used AIRS with collaborative learning recommendations and students who used AIRS without these recommendations.

Finally, we consider our future work is as follows: we collect new attribute data, we ascertain the usefulness and effectiveness of the attribute data, and we evaluate the recommendation results for new users.

ACKNOWLEDGMENTS

We would like to express our deepest gratitude to the teachers, researchers, and students who kindly participated in the experiments on our collaborative learning recommendation system with AIRS.

REFERENCES

[1] Ministry of Economy, Trade and Industry, “e-Learning White paper 2007/2008,” Tokyo Denki University Press (2007).

[2] R. Wisher, “Sharable Content Object Reference Model (SCORM) 2004 4th Edition Overview Version1.0,” Advanced Distributed Learning, pp. 1-18 (31 March 2009).

[3] Y. Wada, T. Matsuzawa, M. Yamaguchi, and S. Dohi, “Proposal and Verification of Bidirectional Recommendation System for Learning Web Digital Texts,” Proceedings of the Second International Conference on the Applications of Digital Information and Web Technologies (ICADIWT2009), pp. 210-215 (August 2009).

[4] M. Yamaguchi, Y. Takahashi, T. Matsuzawa, T. Takahashi, and S. Dohi, “Development and Evaluation of e-Learning System AIRS with Multi-Expression Contents,” IEICE-ET2006-118, Vol. 106, No. 583, pp. 69-74 (2007).

[5] H. Hotta and M. Hagiwara, “Design and Implementation of Social-network-based Recommender System,” IPSJ Transactions on Databases, Vol. 2, No. 1, pp. 46-56 (2009).

[6] A. Sasaki, T. Miyata, Y. Inazumi, A. Kobayashi, and Y. Sakai, “Web Content Recommendation System Based on Similarities among Contents Cluster of Social Bookmark,” IPSJ Transactions on Databases, Vol. 48, No. SIG20, pp. 14-27 (2007).

[7] K. Oku, S. Nakajima, J. Miyazaki, and S. Uemura, “Context-Aware SVM for Context-Dependent Information Recommendation,” DBSJ Letters, Vol. 5, No. 1, pp. 5-8 (2006).

[8] D. Perea, J. Kay, I. Koprinska, K. Yacef, and O.R. Zaiane, “Clustering and Sequential Pattern Mining of Online Collaborative Learning Data,” IEEE Transactions on Knowledge and Data Engineering, Vol. 21, No. 6, pp. 759-772 (2009).

[9] G. Costagliola, V. Fuccela, M. Giordano, and G. Polese, “Monitoring Online Tests through Data Visualization,” IEEE Transactions on Knowledge and Data Engineering, Vol. 21, No. 6, pp. 773-784 (2009).

[10] C.Pahl and C.Kenny, “Interactive Correction and Recommendation for Computer Language and Training,” IEEE Transactions on Knowledge and Data Engineering, Vol. 21, No. 6, pp. 854-865 (2009).

[11] N. Furugori, H. Sato, H. Ogata, Y. Ochi, and Y. Yano, “COALE: Collaborative and Adaptive Learning Environment,” Proceedings of the Conference on Computer Support for Collaborative Learning, pp. 493-494 (2002).

[12] T. Tang and G. McCalla, “Smart Recommendation for an Evolving E-Learning System: Architecture and Experiment,” International Journal on E-Learning, Vol. 4, Issue 1, pp. 105-129 (2005).

[13] Y. Takahashi, T. Matsuzawa, M. Yamaguchi, S. Dohi, and Y. Wada, “Recommendation and Delivery of the Optimum Texts for e-Learners,” IPSJ SIG Technical Reports 2007-CE-88(22), Vol. 207, No. 12, pp. 157-162 (2007).

[14] N. Yamazaki, “Software Design,” ISSN 0916-629, Vol. 268, Gijutsu-Hyohron Co., Ltd, Tokyo, Japan (2007).

(Received August 26, 2019)

(Revised December 17, 2010)

Yuji Wada received the B.E. and the M.E. in electrical engineering from Waseda University in 1974 and 1976, respectively. He joined Mitsubishi Electric Corporation in 1976. He received the PhD degree in computer science from Shizuoka University of Japan in 1997. He is currently a Professor in the Department of Information Environment, Tokyo Denki University. His research interests include database systems, data mining, and recommendation. He is a member of the ACM, the IEEE-CS and the IPSJ.

Yuuma Hamadume received the B.E. and the M.E. in information environment engineering from Tokyo Denki University of Japan in 2008 and 2010, respectively. He is currently working on a game software development at Konami Digital Entertainment Co., Ltd. His research interests include e-learning system, digital text contents, and recommendation.

Shinichi Dohi received the B.E. and the M.E. from Tokyo Denki University in 1982 and 1984, respectively. He is currently an Associate Professor in School of Information Environment, Tokyo Denki University. His research interests include AIRS(An Individual Reviewing System), and improvement of students' motivation in introductory computer programming education.

Jun Sawamoto is currently a Professor of Faculty of Software and Information Science, Iwate Prefectural University, Japan. He received the B.E. and M.E. in mechanical engineering from Kyoto University in 1973 and 1975. He joined Mitsubishi Electric Corporation in 1975. He received his PhD degree from Tokyo Denki University in 2004. His research interests include ubiquitous computing, human-interface system, multi-agent systems, and cooperative problem solving. He is a member of IPSJ, IEEE-CS, ACM.

An Experimental Analysis of Accumulated Audience's Comments for Video Summarization

Yoshia Saito [*], Yoshiki Isogai[*] and Yuko Murayama[*]

[*]Graduate School of Software and Information Science, Iwate Prefectural University, Japan
{y-saito, murayama}@iwate-pu.ac.jp, y.isogai@comm.soft.iwate-pu.ac.jp

Abstract - In this paper, we propose an audience-oriented video summarization scheme on video sharing services. The proposed scheme analyzes audiences' feedbacks such as rating and comments in a video and finds important scenes where there are a lot of feedbacks from the audiences. Then, the video is summarized by collecting the important scenes from audiences' point of view although typically it is summarized from video producers'/providers' point of view. As the first step toward the audience-oriented video summarization, we focus on comments as the audiences' feedbacks because currently some video sharing services allow audiences to comment on a specific scene storing their playback time. We assume there is a relationship between the number of audiences' comments on a scene and importance of the scene because the comments represent audiences' willingness to watch the scene. We report an experimental analysis for verification of the hypothesis and discuss some solutions to realize audience-oriented video summarization taking into account the experiment results.

Keywords: Internet broadcast, video sharing service, audiences' feedback, comments, audience-oriented video summarization.

1 INTRODUCTION

In recent years, most Internet users have broadband Internet connections and multimedia contents become popular on the Web. There are a lot of video sharing services nowadays such as YouTube [1] and Yahoo! Video [2]. A huge number of videos are shared and hundreds of thousands of new videos are uploaded every day. It is, however, difficult for audiences to find interesting videos quickly even if they retrieved dozens of candidates by appropriate keywords since it is required to watch the videos taking long time. A solution to the issue is to provide summarized videos.

Automatic generation of video summarization techniques have been studied by a lot of researchers [3-5]. In these studies, summarization is typically realized by understanding object and event in the video and selecting important scenes. Since these studies do not get directly feedbacks from audiences and there are a lot of audiences who have different feelings, it is difficult to keep interest factors of original video for the audience. To provide attractive summarized videos for the audiences, the video summarization should be audience-oriented. That means audiences' feedbacks should be applied to the video summarization algorithm to find scenes where the audiences get interested.

Meanwhile, most video sharing services have functions to receive feedback from audiences such as rating and comments. The received feedbacks are stored in a database and available for analysis of the videos. It would be possible to find scenes where the audiences pay attention by utilizing the feedbacks. Some video sharing services allow audiences to comment on a specific scene storing their playback time. Since each feedback is related with a specific scene, the feedbacks can be used as metadata about the scenes. Thus, current video sharing services already have good database to realize audience-oriented video summarization.

In this paper, we propose an audience-oriented video summarization scheme on video sharing services. The proposed scheme analyzes audiences' feedbacks in the video and finds scenes where there are a lot of feedbacks from the audiences. Then, the video is summarized by collecting the important scenes from audiences' point of view. As the first step toward the audience-oriented video summarization, we focus on audiences' comments as the audiences' feedbacks. We assume there is relationship between the number of audiences' comments on a scene and importance of the scene for video summarization because the comments represent audiences' willingness to watch the scene. To verify the assumption, we conduct an experiment collecting ten thousand comments per video from a video sharing service and discuss whether it is possible to make a summarized video utilizing the audiences' comments.

The remainder of this paper is organized as follows. In Section 2, we describe related work. Section 3 illustrates a model of audience-oriented video summarization on a video sharing service and describes a hypothesis. In Section 4, we conduct experiments for preliminary analysis and show the results. In Section 5, we discuss solutions to realize audience-oriented video summarization taking into account the experiment results. Section 6 gives some conclusions with a brief summary and future work.

2 RELATED WORK

We can save our time by summarized video and highlight video. Recently, we can also give feedback to watched videos and share our experience. In this section, we explain difference between the summarized video and highlight video and also describe scene extraction techniques which use audiences' feedbacks.

2.1 Summarization and Highlight

There is difference between summarization and highlight. We define the summarized video and highlight video by reference to typical researches [6-9] as follows:

- **Summarized video** shows the story of a video content in short time.
- **Highlight video** shows a set of interesting scenes of a video content in short time.

The motivation of our research is to provide short videos so that audiences can find objective video and grasp course of story of the videos quickly. We focus on the video summarization.

2.2 Audiences' Feedbacks

There are several scene extraction techniques which use audiences' feedbacks. In [10], audiences' browsing log such as "PLAY", "STOP", "PAUSE" and "JUMP" are used for the video summarization. The audiences unintentionally give their understanding of the video to the system through the browsing operations. They measure the subjective interestingness and importance using the browsing log. In sport videos, there is a technique [11] to use audiences' reactions such as cheering and applause. The proposed technique recognize audio signal in the sport videos and extracts interesting events for the video summarization.

A concept of time-tagging is proposed in [12]. Audiences can add time-tags to videos and these tags can be used as bookmarks. It is also applied to video summarization technique by analyzing the shared time-tags and scoring the tagged segments. Current video sharing and live streaming services provide feedback functions for audiences. Several video sharing services such as YouTube and Yahoo! Video has comment and rating functions. Audiences can submit text messages to the videos and rate the videos by 5-point scale. Most live video streaming services such as Ustream.tv [13] and Stickam [14] have a chat function. In these services, audiences can send chat messages among the audiences and its broadcaster in real-time. Nico Nico Douga [15] is a video sharing service in Japan and allows audiences to comment on a specific scene storing their playback time. The comments are displayed on the video field synchronized with the commented scene as if chatted with other audiences in real-time. Since the comments correspond with specific scenes and can be easily gotten them, we use the comment data in the Nico Nico Douga for our research.

3 AUDIENCE-ORIENTED VIDEO SUMMARIZATION SCHEME

The purpose of the audience-oriented video summarization is to provide summarized videos which keep interest factors of the original ones to audiences. In this paper, the "*audience-oriented*" means utilizing feedbacks from audiences as much as possible to provide a service from audiences' view of point. The audience-oriented service would improve audience's satisfaction since it directly reflects the feedbacks.

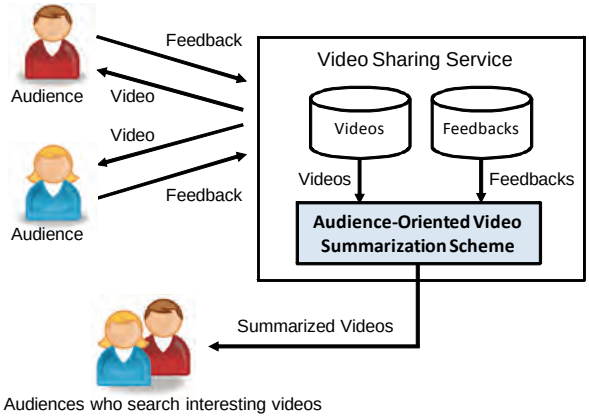


Figure 1: A model of video sharing service with audience-oriented video summarization scheme.

3.1 Overview

Figure 1 shows a model of video sharing service with the audience-oriented video summarization scheme. In this service model, a service provider delivers videos to audiences and the audiences can give feedbacks to the service provider. The feedbacks are stored in a database of the service provider. When there are audiences who search interesting videos and have several candidates to watch, the service provider generate summarized videos of the candidates applying the feedbacks appropriately. The service provider offers the summarized videos to the audiences. The audiences can decide to watch a video by reference to the summarized video. If there are not enough audiences' feedbacks for the summarization, the videos are summarized by audio-visual video summarization techniques cooperatively.

3.2 Methodology

In this paper, we use audiences' comments which are associated to specific scene as the feedbacks. In order to study an algorithm for the audience-oriented video summarization, we have a simple hypothesis about relationship between video summarization and the audiences' comments. The hypothesis is as follows:

> *There is a relationship between number of audiences' comments and important scenes for the audiences. A scene which has sufficient number of comments is appropriate as a part of the summarized video.*

We assume audiences' comments increases when it is an important scene because the comments would represent audiences' willingness to watch the scene. The scenes which have a lot of comments would be worth watching for the other audiences and would be also important part of the summarized video. If the hypothesis is correct, we can get a set of candidate scenes for video summarization and generates the summarized video by putting several candidate scenes together.

Expected issues are that the highly-commented scenes are just interesting scenes for the audiences and they are not parts of the summarized scenes. In this case, the scenes are

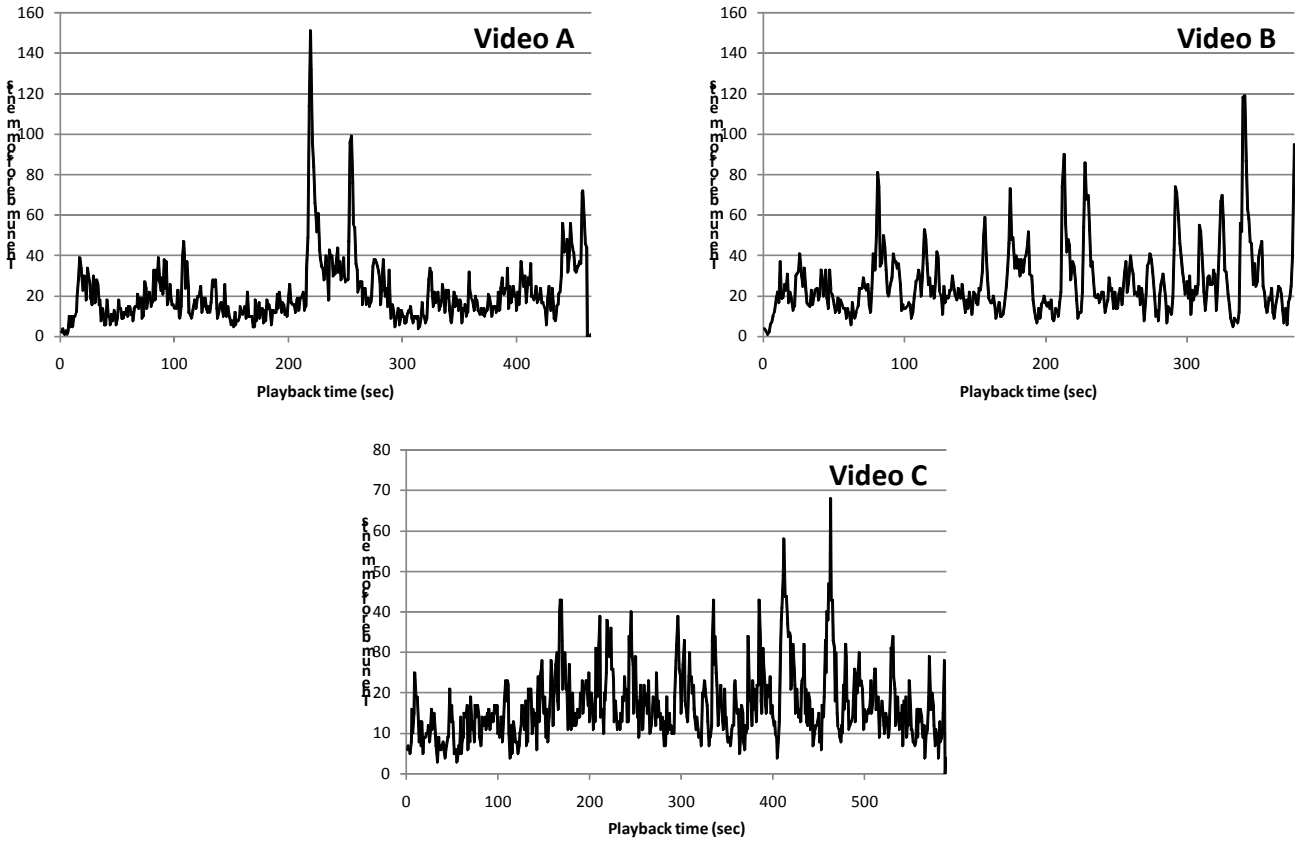


Figure 2: Changes in the number of comments per second.

a set of candidates for highlight. We need to study the relationship between the number of comments and summarized/interesting scenes.

4 EXPERIMENTAL ANALYSIS

We conducted an experimental analysis to verify our hypothesis. For the analysis, we collected audiences' comments from a video sharing service and asked people to select scenes which are appreciate for summarized/interesting scenes. Then, we studied if the number of comments was positively correlated with summarized/interesting scenes.

4.1 Comment Collection

The comments data in the Nico Nico Douga is stored in a log database with the following information.

- Time and date when audiences commented
- Playback time when audiences commented
- User ID
- Comment
- Command to decorate the comment

We chose three popular videos (Video A, B and C) in Nico Nico Douga at random and collected ten thousand comments per video. The contents of the videos are as follows:

- **Video A**: A man makes a strange cake using a lot of cheep sweets and eats it. (Total length: 465 seconds)
- **Video B**: A man makes big balls of chocolate using a lot of small various chocolates and packages them. (Total length: 376 seconds)
- **Video C**: A man mixes various energy drinks and tries to drink the mixed one. (Total length: 589 seconds)

Each video has a story (introduction, making and completion). Figure 2 shows the changes in the number of comments per second. From the graph, high and low peaks can be clearly shown in each video. We presume these videos are suitable to verify our hypothesis and use them in the analysis.

4.2 Scene Selection

We asked 20 participants who are students in our university about the following questionnaire after watching each video. (Note: The order of watching the videos was at random for fairness)

1. Please select 5 scenes which are summarized the video on condition that each scene is 3 seconds.
2. Please select 5 scenes which are interesting in the video on condition that each scene is 3 seconds

After the questionnaire, we counted the selected times for summarized and interesting scenes. Figure 3 shows the results. We can see several differences between selected summarized scenes and interesting scenes in the results. In video A, there is an interesting scene around 400 seconds although it is not selected as a summarized scene.

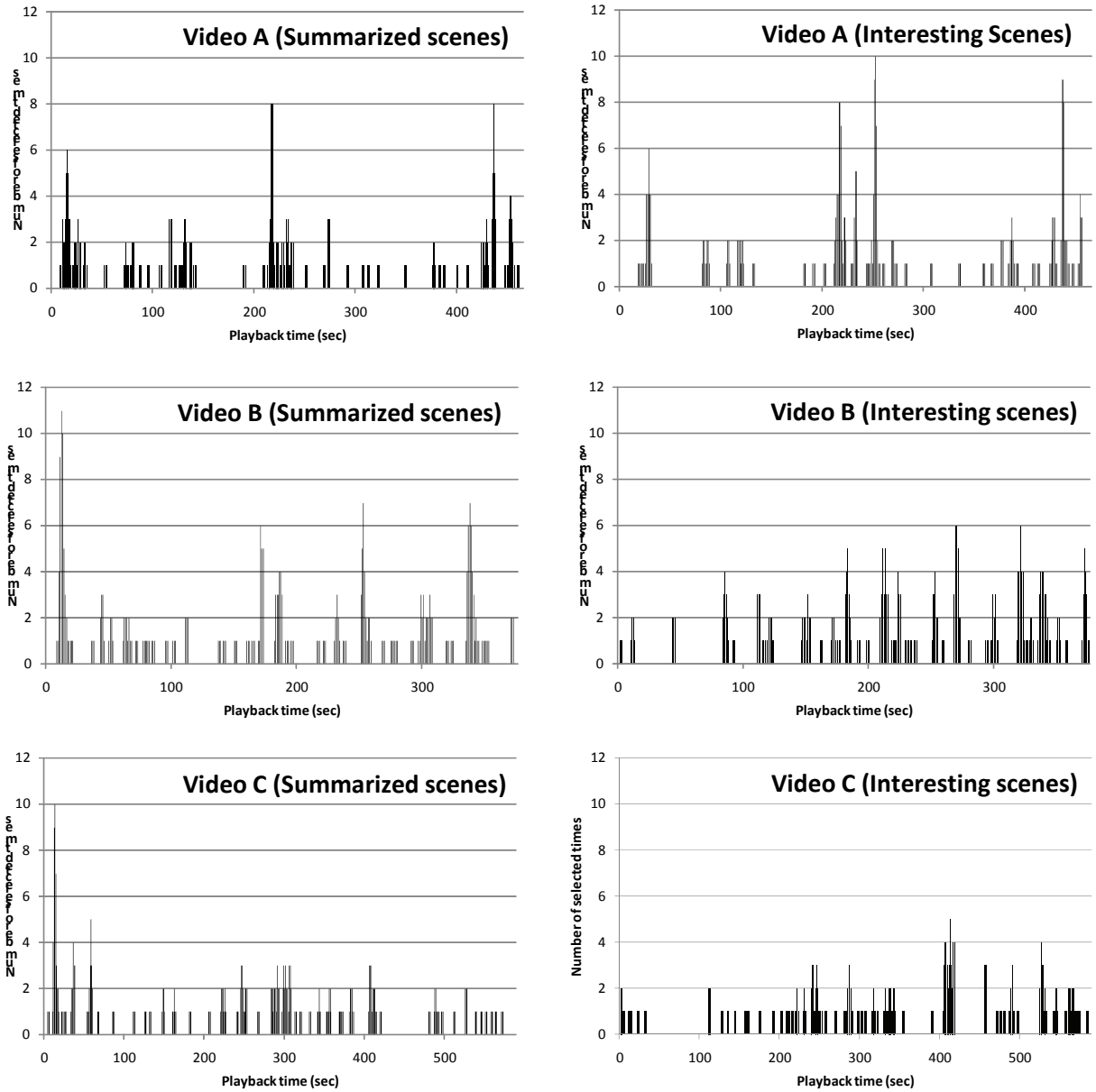


Figure 3: The number of selected times for summarized and interesting scenes.

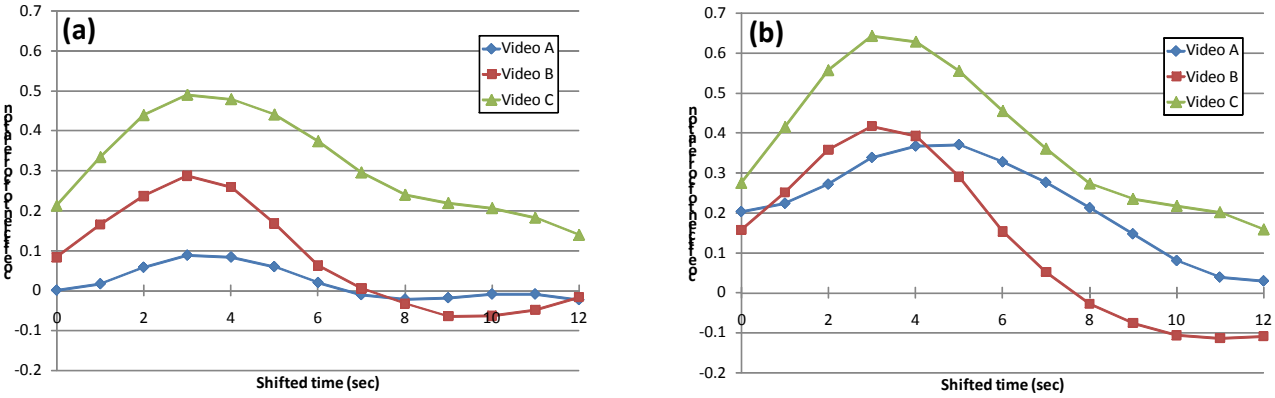


Figure 4: (a): coefficient of correlation between the number of comments and summarized scenes. (b): coefficient of correlation between the number of comments and interesting scenes.

The scene shows interesting performance but it is not important to explain the story of the video. In the video B, we can see a scene which is selected as a summarized scene at the beginning of the video although it is not interesting. Because the scene shows the title of the content, it is selected despite it is not interesting. The same thing can be also said for the video C. At the beginning of the video C, a man explains the purpose of the video. Of course, it is not so interesting but important for summarization. Thus, we can see summarized scenes do not always correspond with interesting scene and a scene of introduction is important for video summarization even if it is not interesting one.

4.3 Analysis

We assessed coefficient of correlation between the number of comments and the number of selected times for summarized/interesting scenes. The result, however, does not show correlation between them. We presume that audiences would need to type their keyboard for a few seconds to comment to a scene and the input time should be required. Therefore, we shift the commented time to a few seconds before and assessed the coefficient of correlation again.

Figure 4 shows the result when the commented time is shifted by 1 second. From the graph, we can see the number of comments was positively correlated with summarized/interesting scenes when commented time was shifted to from 3 to 5 seconds before in these 3 videos. In the video A, the coefficient of correlation between the number of comments and summarized scenes is 0.09 when shifted to 3 seconds and 0.37 when shifted to 5 seconds as for interesting scenes. Weak correlation is shown only between the number of comments and interesting scenes. In the video B, the coefficient of correlation between the number of comments and summarized scenes is 0.28 when shifted to 3 seconds and 0.42 when shifted to 3 seconds as for interesting scenes. Weak correlation is shown between the number of comments and summarized scenes, and medium correlation as for interesting scenes. In the video C, the coefficient of correlation between the comments and summarized scenes is 0.49 when shifted to 3 seconds and 0.64 when shifted to 3 seconds as for interesting scenes. Medium correlation is shown between the number of comments and summarized/interesting scenes.

We found the number of comments was positively correlated with summarized/interesting scenes when the commented time was appropriately modulated in consideration of input time. The correlation strength differs in the contents of videos and the coefficient of correlation of interesting scenes is higher than that of summarized scenes.

5 DISCUSSION

The experimental analysis clarified summarized scenes do not always correspond with interesting scenes and the coefficient of correlation of interesting scenes is higher than that of summarized scenes. There are two issues. The first issue is how to extract a scene which is important for video summarization but few comments. The second issue is how to exclude scenes which have a lot of comments but inappropriate for summarized scenes. To solve the issues, we have two main approaches. The first approach is to make a support system which extracts candidate scenes using audiences' comments and suggests the scenes to users so that they can make a summarized video quickly and improve its quality. In this approach, the users decide whether the suggested scenes are appropriate or not and find missing scenes. The advantage of the first approach is ease of implementation and the drawback is workload of the users. The second approach is to devise an algorithm which finds unnecessary and missing candidates. We presume the number of comments is not sufficient as a parameter for the algorithm and additional parameters are required. For the additional parameter, meaning of the comments would be effective. Moreover, we probably need to use audio-visual summarization techniques together. The advantage of the second approach is to reduce human workloads and the drawback is difficulty of implementation. Since each approach has different advantages, we will study the two approaches as future work.

Compared with existing summarization schemes, the proposed scheme could produce more appropriate summarized video in terms of audience-oriented aspect. Traditional audio-visual video summarization techniques can detect importance of the scenes in terms of audio-visual aspect but cannot understand context of the scenes. The audience comments can represent context of the scenes and it can be regarded as metadata of the video which is described by the audience. Although there are some researches which use metadata of a video described by its producers for video summarization [16], we presume the proposed scheme could realize more audience-oriented video summarization because it uses metadata of the video described by themselves.

The experimental analysis also clarified commented time should be shifted to several seconds because of input time for comment messages. However, accurate time of the gap is not clear yet and we should estimate the gap time. One of the solutions is to focus on length of the comments and estimate the input time by multiplying average time for inputting one character by the length. The average input time would vary from person to person but it would be able to approximate the input time. In this case, we would have to take into account the combination of the inputted characters in order to estimate the input time more accurately.

Although we use collected ten thousand comments for the analysis in the experiment, the minimum number of comments required for extraction of summarized scenes should be discussed. Since there is no comment when a user uploads a video to a video sharing site, our proposed scheme cannot be applied and only audio-visual summarization techniques are effective. As time passes, audiences' comments are collected and our proposed scheme can be applied. By combining audience-driven summarization with audio-visual summarization, we presume the videos can be summarized more appropriately for audiences because it is difficult to know meaning of the scenes and audiences' interests if there is only audio-visual information. We should study the threshold of number of comments to apply the audience-oriented video summarization by changing the number of comments.

6 CONCLUSION

In this paper, we proposed an audience-oriented video summarization scheme which analyzes audiences' feedbacks in the video and finds important scenes for video summarization in audiences' point of view. From the experimental analysis using audiences' comments in Nico Nico Douga, we got five findings; (1) summarized scenes do not always correspond with interesting scene, (2) a scene of introduction is important for video summarization even if it is not interesting one, (3) there is a short-time delay between comments and target scene, (4) the number of comments was positively correlated with summarized/interesting scenes when commented time was shifted to from 3 to 5 seconds before, (5) Some schemes would be required to make summarized video from audiences' comments because the audiences' comments indicated interesting scenes rather than summarized scenes.

As future work, we will design a support system for video summarization while studying an algorithm of video summarization based on the meaning of the comments so that we can generate summarized videos automatically. We will also compare the audience-driven video summarization method with some audio-visual summarization methods in order to show effectiveness of the proposed method more clearly.

REFERENCES

[1] YouTube, http://www.youtube.com/.

[2] Yahoo! Video, http://video.yahoo.com/.

[3] D. DeMenthon, V. Kobla, and D. Doermann, "Video summarization by curve simplification", ACM Multimedia, pp. 211-218 (1998).

[4] Y. Ma, L. Lu, H. Zhang, and M. Li, "A user attention model for video summarization," ACM Multimedia, pp. 533-542 (2002).

[5] C. Kim and J.N. Hwang, "An integrated scheme for object-based video abstraction", ACM Multimedia, pp. 303-311, 2000.

[6] B. T. Truong and S. Venkatesh, "Video abstraction: A systematic review and classification," TOMCCAP, Vol. 3, Issue 1 (2007).

[7] H. Luo, Y. Gao, X. Xue, J. Peng, and J. Fan, "Incorporating Feature Hierarchy and Boosting to Achieve More Effective Classifier Training and Concept-Oriented Video Summarization and Skimming," TOMCCAP, Vol. 4 Issue 1 (2008).

[8] X. Tong, Q. Liu, Y. Zhang, and H. Lu, "Highlight Ranking for Sports Video Browsing," ACM MULTIMEDIA, pp. 519-522 (2005).

[9] M. Fleischman, B. Roy, and D. Roy, "Temporal feature induction for baseball highlight classification," ACM MULTIMEDIA, pp. 333-336 (2007).

[10] B. Yu, W.Y. Ma, K. Nahrstedt, and H.J. Zhang, "Video summarization based on user log enhanced link analysis," ACM Multimedia, pp. 382-391 (2003).

[11] Y. Rui, A. Gupta, and A. Acero, "Automatically extracting highlights for TV Baseball programs," ACM Multimedia, pp. 105-115 (2000).

[12] D.A. Shamma and R. Shaw, "Watch what I watch: using community activity to understand content," Proc. of the international workshop on multimedia information retrieval, pp. 277-284 (2007).

[13] Ustream.tv, http://www.ustream.tv/.

[14] Stickam, http://www.stickam.com/.

[15] Nico Nico Douga, http://www.nicovideo.jp/.

[16] Y. Takahashi, N. Nitta, and N. Babaguchi, "Video Summarization for Large Sports Video Archives," IEEE International Conference on Multimedia and Expo, pp. 1170-1173 (2005).

(Received August 28, 2009)
(Revised November 15, 2010)

Yoshia Saito received his Ph.D. degree from Shizuoka University, Japan, in 2006. He had been an expert researcher of National Institute of Information and Communications Technology (NICT) from 2004 to 2007, Yokosuka, Japan. He is currently a lecturer at Iwate Prefectural University since October 2007. His research interests include internet broadcasting and interactive TV. He is a member of IEICE, IPSJ, IEEE, and ACM.

Yoshiki Isogai received his bachelor's degree from Iwate Prefectural University, Japan, in 2009. He currently attends a graduate course in Iwate Prefectural University. His research interests include Internet broadcasting and interactive TV. He is a member of IPSJ.

Yuko Murayama is a professor at Iwate Prefectural University. She had M.Sc. and Ph.D. both from University of London in 1984 and 1992 respectively. She had been a visiting lecturer from 1992 to 1994 at Keio University, a lecturer at Hiroshima City University from 1994 to 1998. She has been with Iwate Prefectural University since April 1998. Her interests include internetworking, network security and trust. She is a member of IEEE, ACM, IPSJ, IEICE, and ITE. Currently she serves IFIP TC11 as a Vice Chair.

Effects of an Intuitional Pictograph Comment Function in a Video Sharing Web System

Kentaro Kagawa*, Junko Itou**, and Jun Munemori**

*Graduate School of Systems Engineering, Wakayama University, Japan
**Faculty of Systems Engineering, Wakayama University, Japan
{s105068, itou, munemori}@sys.wakayama-u.ac.jp

Abstract - Video sharing websites have spread throughout the world. Among the comments they contain are impression comments, which are one of the important factors determining the quality of video content. But if the posting process is complex or difficult, it is difficult to submit impression comments. Accordingly, we have developed a video sharing system named "Onion". One of the features of Onion is a pictograph comment function. The function consists of the scrolling wheel of a mouse and posting pictographs. We have experimented using the system and, as a result, obtained 13 videos, 738 views, 108 text comments, and 1,806 pictograph comments. The ratio of posted text comments is the same as before. The ratio of the posted pictograph comments is very large. We confirmed the utility of the system.

Keywords: video sharing, impression, comment, mouse wheel, pictograph

1 INTRODUCTION

In recent years, a great deal of video content has been shared owing to the enlargement of memory and hard disk drives, the spread of broadband, and the development of data compression technology [1]. There are many services using video content [2]. A video sharing website service is one such service. In particular, Nico Nico Douga [3] has become famous in the entertainment field. Users can post comments concerning particular video scenes. Comments include reviews, commentaries, impressions, dramatizations, and questions and answers. The actions of site users are divided into video search, viewing, and posting comments. But if it is complex and difficult for viewers to post comments, it becomes difficult to post their emotions or feelings to video. In this paper we propose an intuitional interface to post viewer's impression comments by using pictographs [4] and a mouse wheel device. [1]

Chapter 2 explains the related work. Chapter 3 explains the proposed video sharing system, and Chapter 4 shows the experiment. Chapter 5 describes the experiment results, and Chapter 6 shows the additional experiments. Chapter 7 describes the future prospects, and Chapter 8 is the conclusion.

2 RELATED WORK

There is a study to make indexing and ranking from text comment of video clips for the video sharing websites [5]. They treated emotional impression such as happiness or sadness, and so on. But, they do not express these feelings in the video content.

A method to express feelings by a real-time chat is suggested [6]. This is the system which combined the information from a sensor with the animation of the text. They do not use pictographs with a text.

It is not a video sharing websites, but there is the example which used emoticons as a subchannel of the video meeting [7].

The emoticon (smily) is made with a text. It is known that it takes trouble to express pleasure and sadness in an emoticon [8].

3 PROPOSED MODEL

3.1 Composition of system

We have developed a video sharing website system called Onion [9]. Table 1 shows a list of software that composes this proposed video sharing system. Figure 1 shows the software constitution of the system.

Table 1: Software constitution.

component	software	version
Web server package	XAMPP	for Windows 1.6.6a
Web server	Apache	version 2.2
RDBMS	MySQL	5.0.51a
Scripting language	PHP	version 5.2.5
View content	Flash	Professional 8
Video encoder	FFmpeg	rev. 16905

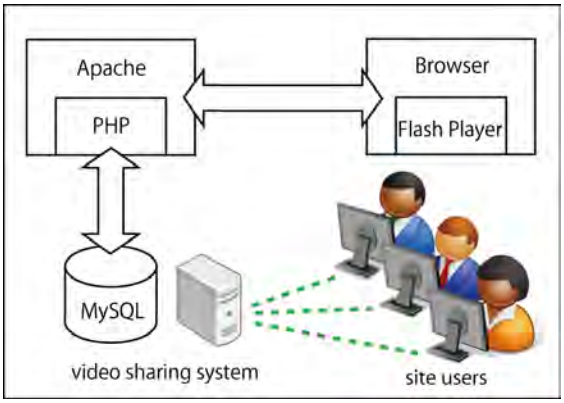


Figure 1: The constitution of the proposed system Onion

3.2 Function of system

The proposed system features an intuitional pictograph comment function. But the system also supplies some fun-

[1] The work reported in the paper was partially supported by Japan Society for the Promotion of Science (JSPS), Grant-in-Aid for Scientific Research (B) 20300047, 2008.

damental function services for site users like other video sharing systems. Figure 2 shows the top page of Onion.

Figure 2: Top page of Onion.

Site users can upload their original videos by using the video upload function with attendant information and authentication. If they wish to delete their videos, they can delete them using the delete function with a password, which they had set when they uploaded it. Site users can also view uploaded videos by using the video search function and the video list. If a site user finds a video to view, the user then views the video on a viewing page. Figure 3 shows a content screen of a viewing page.

Figure 3: A content screen of a viewing page.

The video replay screen consists of a video screen, a text comment function, a pictograph comment function, and some additional functions. The content screen is 600px in width and height. The video replay screen is 600px in width and 400px in height (aspect ratio is 3:2).

Posted text and pictograph comments by video viewers are displayed on the video replay screen and flow from right to left. The size of text comments is 25px in height. The size of pictograph comments is 40px in width and height. The velocity of flowing is 150px/sec. Each comment is displayed on the video replay screen for 4 seconds. Viewers can post their comments by using the text comment function and the pictograph comment function.

3.3 Pictograph comment function

The process of posting a pictograph comment is done by selecting a pictograph and scrolling mouse wheel. The selected pictograph is chosen from the pictograph comment area that provides nine kinds of pictograph comments. Figure 4 shows the list of nine kinds of pictograph comments.

Figure 4: List of pictograph comments.

Each kind of pictograph can switch to three grades by scrolling the mouse wheel. Those grades depend on the number of revolutions of the mouse. Figure 5 shows the strength list of pictograph comments, and Table 2 shows the chosen pictograph strength by mouse scrolling.

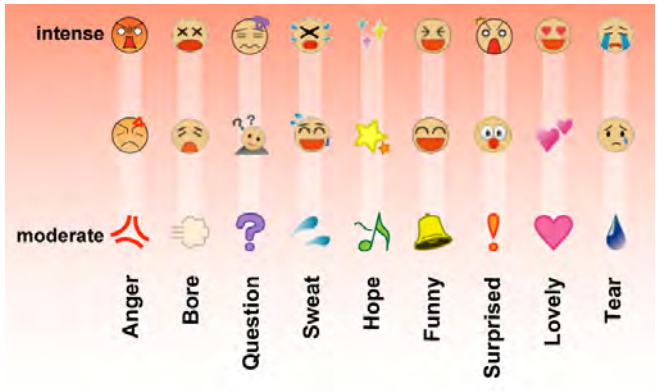


Figure 5: Strength list of pictograph comments.

Table 2: Chosen pictograph strength by mouse scrolling.

impression strength	Amount of offset
Strong	25～
Medium	10～24
Weak	2～9

Each pictograph on the strength list is schematized starting from the bottom in increasing order. Some of the pictographs were created by Munemori's group [10].

3.4 "Resonance Sense" function

Onion restricts pictographs to nine kinds. In other words, the frequency of posting the same pictograph comments is increasing. So, Onion provides a RS function (abbreviated form of the Resonance Sense). This function is designed to share emotions among viewers. The RS function is used when a viewer posts a pictograph comment. If the same pictograph comments are posted by others in the same video scene, the size of the just posted pictograph comment becomes large according to the number of like comments. The just posted comment expands 25px in width and height by each identical comment. The maximum pictograph size is 200px. At the same time, the other different comments fade out for a given length of time. Even though the same pictograph comments are posted more than two in the same video scene, RS function counts once at each posted. Figure 6 (a) shows a screen of not using the RS function (before), and Figure 6 (b) shows a screen of using the RS function (after).

Figure 6 (a): A screen of not using the RS function (before).

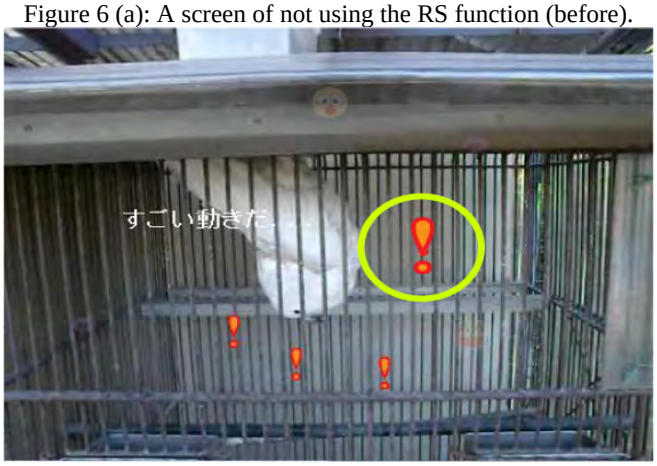


Figure 6 (b): A screen of using the RS function (after).

4 EXPERIMENTS

We have carried out experiments by using the Onion system to prove utility of pictograph comments. Purposes of this experiment are to evaluate how much a pictograph is used and to evaluate whether participants can effectively comment with a pictograph. The participants ranged from teenagers to those in their fifties in the experiments. Parts of the experiments were carried out at a university festival. They were divided into 2 groups. One of the groups called the "view group" consisted of eighteen video view users (as viewers) and the other group called the "upload group" consisted of eleven video upload users (as uploaders). The view group included seven Wakayama university students and eleven members of the general public. The upload group consisted of Wakayama university students.

4.1 Material

For experiments, participants of the view group used computers equipped with a wheel mouse and were connected to 100 Mbps Ethernet LAN. The computers had sufficient speed to process streaming media and depicting screens. We chose 13 of them among 20 videos including the video, which we made for exercises and used them for the experiment.

The contents of video are shown below.

No.1: The automatic turn of a seat on a limited express
No.3: A vending machine with an interesting movement
No.10: An elevator
No.11: The backlashing of a picture
No.12: Playing in Shirahama
No.13: I'm breaking a watermelon
No.14: I'm eating sushi in large quantities
No.15: A dance show
No.16: Though I am lively, I am lonely
No.17: An encounter with a cat
No.18: Sculptures
No.19: Self-satisfaction
No.20: An analysis experiment of gum

4.2 Method

We shall now describe the experiment procedure of the view group and upload group participants. Figure 7 shows a scene of viewing a video (the view group).

4.2.1 Method for uploaders

(1) They uploaded some original videos beforehand using Onion.
(2) After the viewers posted comments, the uploaders checked the comments uploaded to their videos.

4.2.2 Method for viewers

(1) Search the randomly posted videos using Onion.
(2) View video on a content screen.
(3) Post comment using both comment functions.

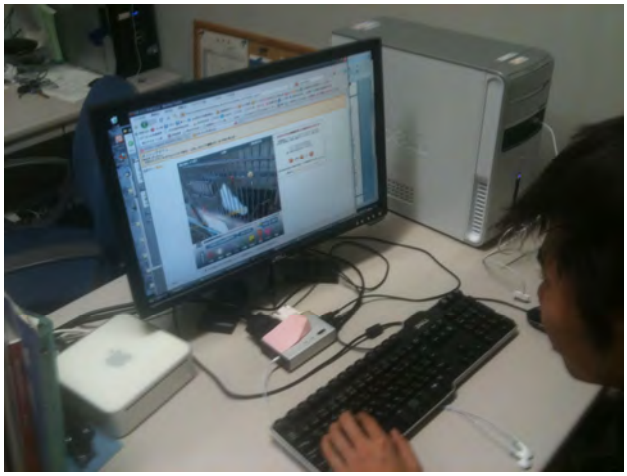


Figure 7: A scene of viewing a video.

After the experiments, we distributed questionnaires to all the experiment participants.

5 RESULT AND DISCCUSION

5.1 Results of Experiments

The results of the experiments are shown below. We got 13 videos, 738 views, 108 text comments, and 1,806 pictograph comments. Figure 8 shows the number of the posted comments for each video.

The number of posted pictograph comments was more than the number of text comment for all uploaded videos. Posted pictograph comments accounted for 94% of the total

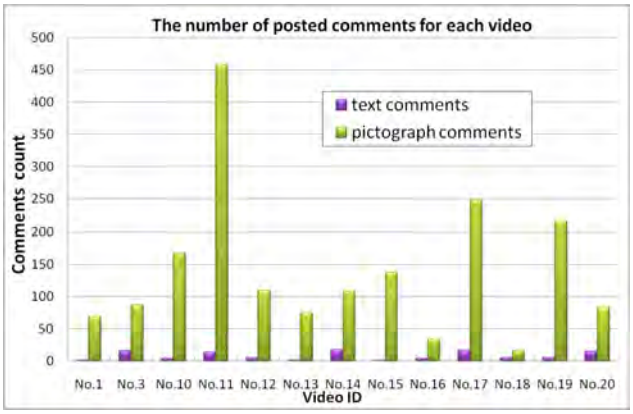


Figure 8: Number of posted comments.

comments, indicating that viewers prefer the pictograph comment function to the text one for expressing their emotions. Figure 9 shows the ratio of total pictograph comments. Figure 10 shows the number of posted comments for the three grades. Table 3 shows the number of posted comments in a viewing.

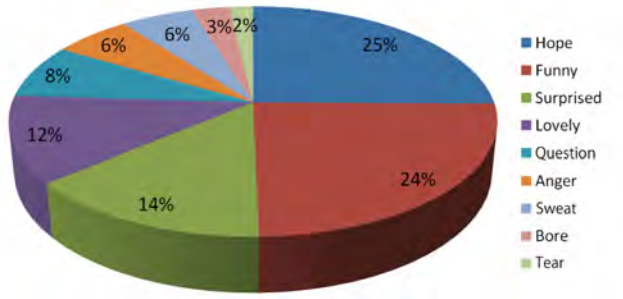


Figure 9: The ratio of total pictograph comments.

The ratio of posted pictograph comments expressing "Hope" was 25% and "Funny" was 24%. It means that these two kinds of pictograph comments occupied about half of the total pictograph comments. Conversely, the ratio of "Tear" and "Bore" pictograph comments occupied only a small percentage. It indicates that some of the extreme or negative comments were posted less.

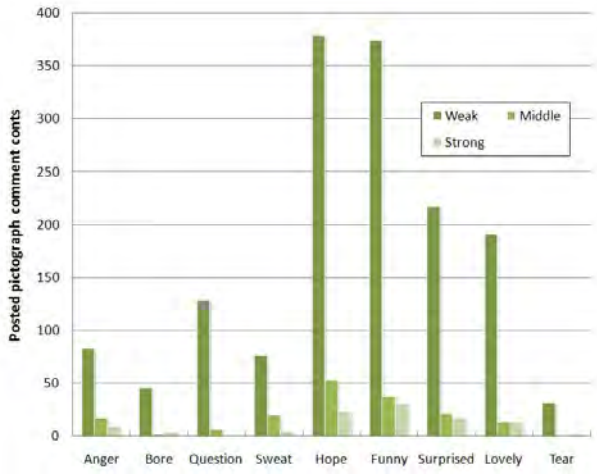


Figure 10: Pictograph comment counts for the three grades.

We got 1,527 weak grade pictographs, 173 middle grade pictographs and 106 strong grade pictographs. Thus, the weak grade pictograph comments occupied 85% of the total posted, indicating that the viewers prefer posting soft expressions to extreme expressions.

Table 3: The number of both posted comments

	Text Nico Nico Douga	Text Onion	Pictograph Onion
Average	0.131	0.19	3.17
Median	0.134	0.123	2.631
Expectation	0.125	0.146	2.447

The number of total posted pictograph comments was 16.7 times that of text comments. There was no significant difference between the number of posted text comments of Onion and the number of posted text comments of Nico Nico Douga. This indicates an increase of posted emotional comment counts.

Figure 11 shows the number of RS functions.

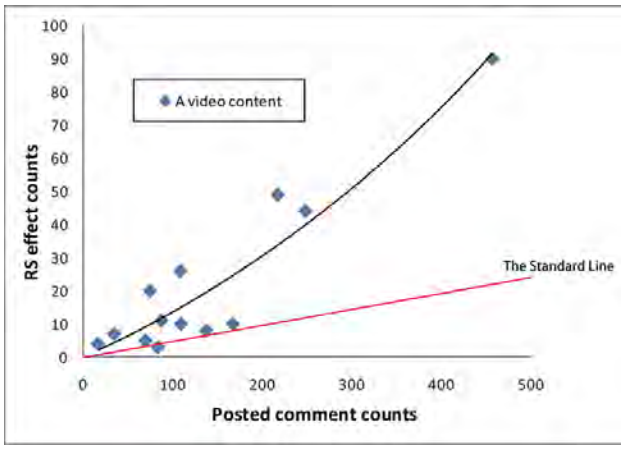


Figure 11: The number of RS functions.

The standard line indicates a value if each pictograph comments is posted evenly in all scenes. The standard line was calculated by values of average length of 11 videos (118.2sec).

The number of RS function occurrences was related to the number of posted comments. Therefore, the same pictograph comments that were posted by several viewers were concentrated in the same video scene. Then, the curve of the graph is above the standard line. It indicates that previously posted pictograph comments influence other viewers who watch the same video.

If they use the RS function, they may be able to get a sense of synchronization in disparate places.

5.2 Questionnaire results

5.2.1 Questionnaires for the upload group

Evaluations of part of the questionnaire were rated on a scale of one to five. "5" is the highest score and "1" is the lowest. Table 4 shows a part of the questionnaires for the upload group. The evaluation scores of the questionnaires

were the average and the standard deviation of eleven video upload users.

Each person of the upload group checked their comments both text and pictograph simultaneously. In Table 4, the word of “text” means the comment of text. The word of “pictograph” means the comment of pictograph.

Table 4: Questionnaire results for the upload group.

Questionnaire items	Evaluation (AVG) / (STD)	
	Text	Pictograph
Do you feel delightful if your videos get some comments from viewers?	(4.4)/(0.6)	(4.2)/(0.6)
Do you feel sad if your videos get no comments from viewers?	(4.1)/(1.0)	(3.8)/(1.1)
Do you have more incentive to next videos if your videos get comments?	(4.1)/(0.7)	(4.1)/(0.8)

We carried out a T-test and found that there was little difference in evaluations between text and pictograph comments (Table 4), indicating no difference between the two functions. Thus, we can conclude that the pictograph comment function gave satisfaction for video upload users just like the text comment function.

5.2.2 Questionnaires for the view group

The results of the questionnaires for the view group may be summarized as follows.

1) Viewers can post whenever they wish.
2) Viewers do not have to “read” pictographs.
3) Viewers can grasp the comments of viewers at once.
4) Pictographs can be a distraction from watching video.
5) Range of expression is reduced.

The overall results indicate that pictograph comments have a high level of visibility and some problems (4, 5). So, pictograph comments require some method for solving these problems.

6 ADDITIONAL EXPERIMENTS

We added experiments in U.S.A. and China. There were three viewers in the Department of Information Computer Sciences, University of Hawaii at Manoa (September, 2009) and three viewers in the Institute for Digitization of the Palace Museum in Beijing (January, 2010).

The number of the posted pictograph comment was several times of the text comment in all experiments (4.8 times in the U.S.A experiments and 15.2 times in the China experiments).

Table 5 shows the ratio of posted pictograph comments in the additional experiments and the conventional experiments (shown as Japan).

In the additional experiment in U.S.A, and China, the ration of “Bore” was over 10%, but the ratio of “Anger” and “Sweat” occupied only a small percentage. Because it is expression of comics, there is a possibility that it was not understood.

The weak grade pictograph comments occupied most of the total posted.

Table 5: Ratio of posted pictograph comments in the additional experiments and the conventional experiments.

	USA	China	Japan
Hope	16%	16%	25%
Funny	19%	15%	24%
Surprised	17%	14%	14%
Lovely	9%	14%	12%
Question	10%	17%	8%
Anger	3%	3%	6%
Sweat	3%	4%	6%
Bore	13%	12%	3%
Tear	11%	4%	2%

7 FUTURE PROSPECTS

Plutchik [11] concluded from research that there are 8 primary emotions (joy, trust, fear, surprise, sadness, disgust, anger, and anticipation). In our system, “Joy” is corresponding to a “Funny” icon. “Trust” is corresponding to a “Lovely” icon. “Fear” is corresponding to a “Sweat” icon. “Surprise” is corresponding to a “Surprised” icon. “Sadness” is corresponding to a “Tear” icon. “Anger” is corresponding to an “Anger” icon. “Anticipation” is corresponding to a “Hope” icon. But, there is not the icon equivalent to "Disgust".

In this experiment, viewers often posted their comment by text comment like “Please stop it” [9]. So we had better add a “Disgust” icon. Figure 12 shows a sample of a “Disgust” icon.

Figure 12: A sample of “Disgust” icon.

The kind of a used pictograph is supposed to be different by the genre of the video or the person viewing a video. Therefore it is important to identify who watched the video. We had better make a function to manage the input. Fig.13 shows a sample of the login screen. Users can input their name, mail address, password, gender, and age.

8 CONCLUSION

In this paper, we proposed an intuitional pictograph comment function for posting the emotions of viewers. The features of this function are using pictographs and a mouse wheel. This function was adopted in “Onion,” a video sharing system we have developed. The pictographs of the system can switch through three grades by mouse scrolling.

We carried out experiments using “Onion” for twenty-nine participants who were divided into view and upload groups. We obtained 13 videos, 738 views, 108 text comments and 1,806 pictograph comments in the experiments. The results of the experiments indicated the following.

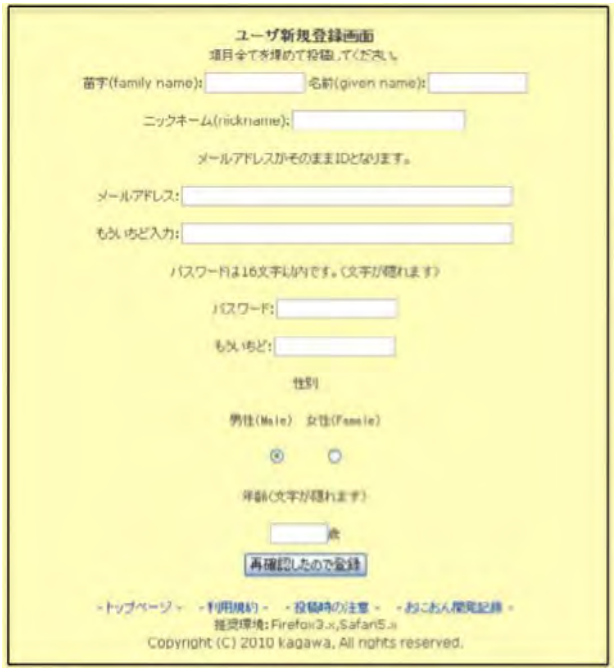


Figure 13: A sample of the login window.

1) Viewers prefer the pictograph comment function to text one for posting their emotions.
2) Viewers prefer posting soft expressions to extreme expressions.
3) The same pictograph comments posted by several viewers concentrated in the same video scenes. The numbers of RS function occurrences were related to the numbers of posted comments.

Therefore, the proposed pictograph comment function is better than the text comment function for expressing spontaneous reactions.

In the future, we would like to discuss the video tags and java script of HTML, which are related our system.

REFEENCES

[1] YouTube, Inc., http://jp.youtube.com/.

[2] D. Yamamoto, T. Masuda, S. Ohira, and K. Nagao, "Synvie: An Annotation System Based on Quotation of Video Scenes," Intraction 2007, pp. 11-18 (2007) (in Japanese).

[3] Nico Nico Douga, http://www.nicovideo.jp/.

[4] Y. Ota, "Pictogram Design," Kashiwa Shobou, Tokyo (1993) (in Japanese).

[5] S. Nakamura and K. Tanaka, "Video Search by Impression Extracted from Social Annotation," Proceedings of the 10th international conference on Web Information Systems Engineering (WISE2009), LNCS 5802, pp. 401-414 (2009).

[6] H. Wang, H. Prendinger , M. Ishizuka, and T. Igarashi, "Affective Communication in Online Chat Using Physiological Sensors and Animated Text," Journal of Human Interface Society: human interface, Vol. 7, No. 1, pp. 39-45 (2005).

[7] A.J. Gill, D. Gergle, R.M. French, and J. Oberlander, "Emotion Rating from Short Blog Texts," Proc. CHI2008, pp. 1121-1124 (2008).

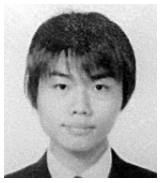
[8] J.T. Hancock, C. Landrigan, and C. Silver, "Expressing Emotion in Text-based Communication," Proc. CHI 2007, pp. 929-932 (2007).

[9] K. Kagawa, J. Itou, and J. Munemori, "Effect of an Intuitional Pictogram Comment Function and an Emotional Sharing Function for a Video Sharing Web System," Journal of IPSJ (Information Processing Society Japan), Vol. 51, No. 3, pp. 770-783 (2010) (in Japanese).

[10] M.B. Mohd Yatid, T. Fukuda, J. Itou, and J. Munemori, "Pictograph Chat Communicator II: A Chat System that Embodies Cross-cultural Communication," *CSCW 2008*, Poster paper, CD-ROM, (2008).

[11] R. Plutchik, "Emotion: A Psychoevolutionary Synthesis," Harpercollins College Div (1980).

(Received August 30, 2009)
(Revised January 10, 2011)



Kentaro Kagawa received the B.E. degrees in System Engineering from Wakayama University, Wakayama, Japan in 2009. His interests are network communication and human interface. He received IWIN Student Award in 2009. He is a student member of IPSJ.

Junko Itou received the M.E. degrees in Information and Computer Sciences from Osaka University, Japan, in 2001. In 2005, she joined the Department of Design and Information Sciences at Wakayama University, as an assistant researcher, and from 2007, she has been an assistant professor of Wakayama University. Her interests are human computer interface, groupware, image processing. She is a member of IPSJ.

Jun Munemori received the B.E. and M.E. degrees in electrical engineering from Nagoya Institute of Technology, Nagoya, Japan, and the D.E. degree in electrical and electrical communication engineering from Tohoku University, Sendai, Japan, in 1979, 1981, and 1984, respectively. He worked in Mitsubishi Electric Corp., Kagoshima University, and Osaka University. He is currently a professor of Department of Design and Information Sciences at Wakayama University. His interests are groupware, human interface, and neurophysiology. He received IPSJ SIG Research Award, IPSJ Best Paper Award, IEEE CE Japan Chapter Young Paper Award, and KES2005 Best paper award, in 1997, 1998 2002, and 2005, respectively. He is a member of ACM, IEEE, IPSJ and IEICE.

Renewal of Pre-shared Key for Secure Communication of Multiple Mobile Terminals through Broadcast Data Distribution Systems

Hirosato Tsuji[*,**], Takeshi Yoneda[**], Tadanori Mizuno[***] and Masakatsu Nishigaki[***]

[*]Graduate School of Science and Engineering, Shizuoka University, Japan
[**]Information Technology R&D Center, Mitsubishi Electric Corporation, Japan
[***]Graduate School of Science and Technology, Shizuoka University, Japan
Tsuji.Hirosato@bp.MitsubishiElectric.co.jp, Yoneda.Takeshi@ak.MitsubishiElectric.co.jp,
nisigaki@inf.shizuoka.ac.jp, mizuno@mizulab.net

Abstract - To perform the secure communication of multiple mobile terminals (i.e. secure unicast communication or secure multicast communication), the encryption key should be shared among the terminals that join the communication. In such a case, if the same encryption key would be repeatedly used, the key disclosure from the stolen terminal might cause the wire tapping and decryption of the encrypted communication. To minimize the risk of the disclosure, the renewal of pre-shared key must be operated. In this paper, we propose the renewal method of pre-shared key for secure communication of multiple mobile terminals. In this method, each terminal will renew its pre-shared key by one-way function (e.g. hash function) according to the instruction from the management server. We also apply the proposed method to the secure communication systems between multiple mobile terminals where the key renewal commands from the system management server to each mobile terminal is distributed through the broadcast data distribution systems.

Keywords: Secure Communication, Mobile Computing, Pre-shared Key Cryptography, Key Renewal, Broadcast Data Distribution Systems

1 INTRODUCTION

The evolution of mobile communication terminals and mobile networks enables the real-time communication using these devices. To protect against the unauthorized disclosure (i.e. wire tapping) of the communication between these terminals, the end-to-end encryption between mobiles is required. In addition, if the terminal is lost or stolen, the unauthorized use of such terminals, the decryption of encrypted communications using the stolen key from such terminals, the leakage of confidential information in such terminals should be also prevented. We've proposed the method of key/device management to realize the secure real-time communication in world-wide mobile environment [1]. In this method, the end-to-end encryption keys are frequently generated on the system management server and distributed to each terminal using one-way communication, such as the digital broadcast data distribution systems. In case of the loss or robbery of terminals, the encryption keys and the secret information will be erased and the terminal will be initialized by the remote control from the system management server. We've designed the protocol that realizes the management of encryption keys as well as the management of mobile terminals. As a result, we've confirmed that the sharing/updating encryption keys are achieved without any operation of the mobile terminal users. We've also confirmed that the lost/stolen terminal is excluded by the remote operation command of system management server and the cooperative action of the other terminals. In this paper, we propose the method renewal method of pre-shared key for secure communication of multiple mobile terminals. In this method, each terminal will renew its pre-shared key by one-way function (e.g. hash function) according to the instruction from the management server. We also apply the proposed pre-shared key renewal method to this system.

In Section 2, we introduce the secure communication based on the pre-shared cryptography and threats to it. In Section 3, we summarize the existing methods to protect against these threats. In Section 4, we propose the method of the pre-shared key renewal. In Section 5, we apply the proposed method to the secure real-time communication system. Finally, we conclude in Section 6.

2 THREATS TO PRE-SHARED KEY CRYPTOGRAPHY

2.1 Secure Communication based on Pre-shared Cryptography

To perform the secure communication of multiple mobile terminals, the encryption key should be shared among the terminals that join the communication. Figure 1 shows a method of sharing the encryption key based on the pre-shared key cryptography. In this method, the symmetric algorithm is used. Each mobile terminal has the same key shared in advance (i.e. pre-shared key) [2]. At the time of communication, each terminal derives the session key (i.e. encryption key) from its pre-shared key.

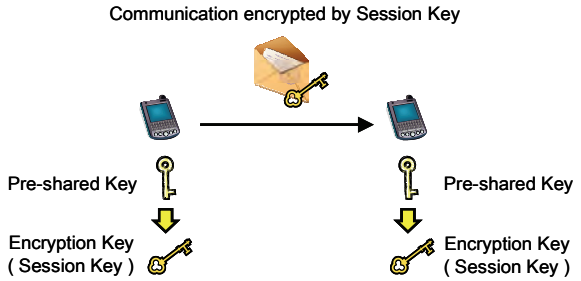


Figure 1: Secure Communication by Pre-shared Key

Then the communication is encrypted with the derived encryption key [3].

2.2 Threats from Key Disclosure

When a symmetric algorithm is used, the application of probable secure algorithms and the countermeasure against the attack on the implementation (e.g. side channel attack) are necessary [4][5][6]. They will protect against the unauthorized disclosure of the encrypted communication by the attack on the cryptographic algorithms. However, if the mobile terminal may be stolen and the encryption key can be extract from the terminal, the key disclosure might cause the following wire tapping.

(1) Attempt to disclose past communication

The attacker recorded the encrypted communication between terminals in advance. Then the attacker steals the one of the terminals and extracts the encryption key from it. Finally the attacker decrypts the pre-recorded communication by using the extract key.

(2) Attempt to wiretap current/future communication

If the terminals are used for the communication among the three or more terminals, the attacker steals one of the terminals. Then the attacker can wiretap the communication between the other terminals by using the stolen terminal. Or the attacker extracts the encryption key from the terminal in order to decrypt the communications.

Figure 2 shows the threats to the secure communication based on the symmetric algorithm caused from the key disclosure.

Therefore the frequent renewal of the encryption key is necessary in order to decrease the risk of the disclosure of past communications. The deletion of the encryption key in the stolen terminal should be also considered to protect against the wiretapping of the current and future communications by using such terminal.

3 EXISTING METHODS

3.1 Key Renewal Methods

There are several existing methods to renew the pre-shared key for secure communication between the mobile terminals.

Figure 2: Threat caused from Key Disclosure

(1) Pre-sharing plenty number of keys

The plenty number of pre-shared keys should be generated in advance. Then these keys had been pre-installed to each mobile terminal. The renewals of pre-shared key will be performed at the sufficient cycles.

(2) Renewal Key Establishment without Servers [2]

When the renewal of pre-shared key is required, the mobile terminals communicate each other to establish the new pre-shared keys. In general, the asymmetric algorithm is used such as RSA key transfer algorithm or Diffie-Hellman key agreement algorithm. The combination with the digital signature algorithm such as DSA signature algorithm or RSA signature algorithm is must be also performed.

(3) Renewal Key Establishment with Servers [7]

When the renewal of pre-shared key is required, the mobile terminals communicate to the trusted server to establish the new pre-shared keys. In general, the server acts as the key distribution center (KDC) and generates the new pre-shared keys and distributes them to each mobile terminals. The well-known implementation of KDC is the Kerberos server.

3.2 Terminal Management Methods

There are several existing methods to protect against the unauthorized use of the stolen mobile terminals.

(1) User Authentication

The mobile terminal can be protected from the unauthorized use by the user authentication functions. The authentication information may be PIN, password and the biometrics authentication information (e.g. fingerprint).

(2) Tamper Resistant Terminal

The extraction of keys from the mobile terminal can be protected, if the mobile terminal has the tamper resistant function. The keys will be automatically erased when the stolen mobile terminal would be illegally opened.

(3) Remote Management from Server [8]

The mobile terminals are managed by the management server. When the mobile terminal would be stolen, the

remote operation command will be sent from the management server to the stolen terminal. Then the stolen terminal will be locked or initialized. In the latter case, the keys in the stolen terminal are erased.

4 PROPOSED METHOD

4.1 Design Policy

We propose the method of the pre-shared encryption key management for the secure communication of multiple mobile terminals. The design policies of our proposal are the followings.

(1) Total Management by Administrator
The management (i.e. renewal and deletion) of the pre-shared key is an important element that decides a security level of the secure communication system. So it should be performed by the order of the system administrator according to a security policy of the system. The users are not allowed to manage any pre-shared keys without the permission of the administrator.

(2) No distribution of Renewal Key
At the time of key renewal, if the updated pre-shared key is distributed from the key management server or transferred between mobile terminals, such keys might be wiretapped. To protect unauthorized disclosure of the renewal key, it will not be distributed nor transferred via network.

(3) Deletion of Key in the stolen Terminal
In case that the loss or robbery of mobile terminal might be happen, as described in Section 2.2, the extraction of encryption key cause the attempt to disclose the past encrypted communication. To protect against the decryption of the Pre-recorded secure communication, the keys in such terminal will be deleted.

4.2 System Architecture

Figure 3 shows the basic system architecture of the proposed method. The components of the system are defined as the followings.

- **User Terminal**
  A terminal that perform the secure communication with other terminals using the pre-shared key.
- **Management Server**
  A server to manage the whole pre-shared key among user terminals.
- **Pre-shared Key**
  A key shared in advance among the user terminals. The pre-shared key consists of the following elements.

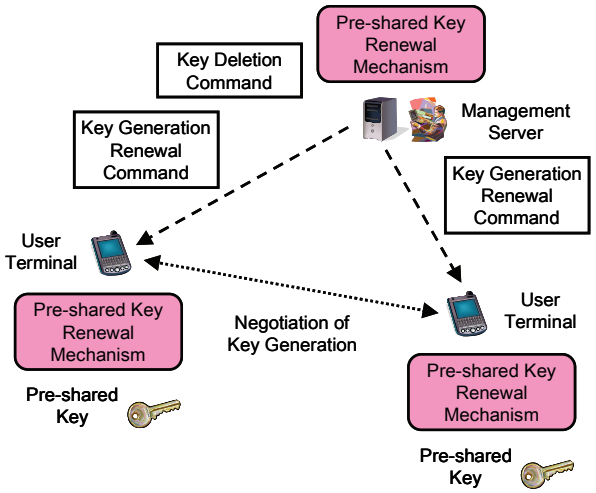


Figure 3: System Architecture of Proposed Method

Element	Meanings
Key ID	Specify the identifier of Key
Key	Encryption Key
Generation Number	Specify the current generation of key renewal
Validity Period	Specify the next key renewal date/time (optional element)

- **Key Generation Renewal Command**
  A command sent from the management server to each user terminal in order to dictate the renewal of pre-shared key. The authentication value (e.g. the digital signature or the Message Authentication Code) is added to the command for the verification.
- **Pre-shared Key Renewal Mechanism**
  A kind of cryptographic mechanism implemented on both the management server and user terminals. The input is the current pre-shared key and the output is the next generation of pre-shared key.
- **Key Deletion Command**
  A command sent from the management server to the specific user terminal in order to delete the keys in the stolen terminal. The authentication value is added to the command for the verification.

4.3 Renewal of Pre-shared Key

The pre-shared key is renewed according to one of the following instructions.

(1) Renewal by Key Renewal Command from Server
The management server creates the key generation renewal command and issues it to the user terminals. The user terminal that receive the command will verify it and renew own pre-shared key.

(2) Automatic Renewal by Key Validity Period
The management server creates and issues the key generation renewal command with the key validity period. The user terminal will automatically renew its own

pre-shared key when the key validity period would be expired.

(3) Synchronized Renewal in case of Generation Gap

The key generation renewal command from the management server may be lost. If it happens, the pre-shared key of the user terminal might not be renewed. When the key generation gap between the user terminals would be detected at the beginning of the secure communication, the user terminal will automatically renew the old pre-shared key for synchronization.

4.4 Renewal Mechanism Example

The pre-shared key renewal mechanism in both the management server and the user terminals can be implemented by using the probable secure one way functions (e.g. hush functions). Figure 4 shows the example of the implementation, where the current pre-shared key has been inputted and the next generation of pre-shared key will be outputted.

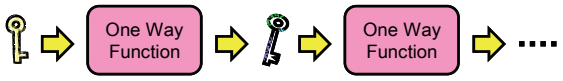


Figure 4: Pre-shared Key Renewal Mechanism

4.5 Comparison with Existing Methods

The pre-shared key is renewed when the administrator decides to renew the current pre-shared key and the management server sends the key generation renewal command. At the time, the updated pre-shared key itself is not sent from the key management server to mobile terminals. In existing methods, such as the renewal key establishment without/with servers, there is a threat that the transferred key may be stolen. However, in our proposed method, the updated key can be protected from the wiretapping. In the one of the existing methods, the pre-sharing plenty number of keys, the maximum number of times of key renewal is equal to the number of pre-installed keys to mobile terminals. However, in our proposed method, there is no limitation of the number of times of key renewal.

5 APPLICATIONS

5.1 Encryption Key Management through Broadcast Data Distribution Systems

We've proposed the secure real-time communication system where the pre-shared key for the end-to-end encryption between mobile terminals are generated by the system management server and are distributed through the broadcast data distribution systems in [1] (Figure 5). In this paper, we apply the proposed pre-shared key renewal method to this system.

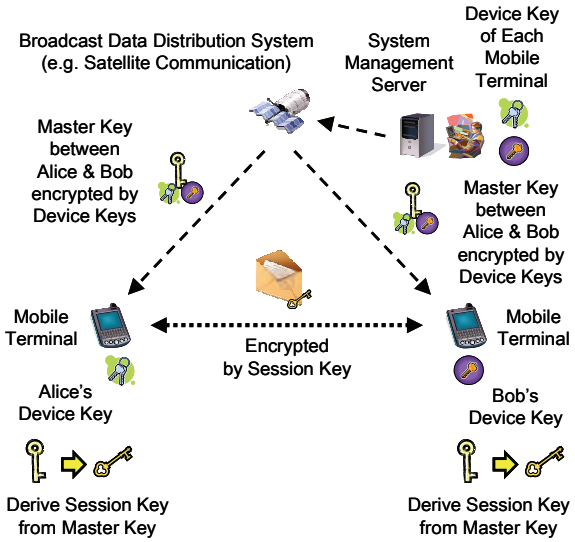


Figure 5: End-to-End Encryption Key Management through Broadcast Data Distribution Systems

This secure real-time communication system consists of the following entities/elements.

- **Mobile Terminal**
  A terminal that performs the secure real-time communication of voices and movies. To protect against the unauthorized disclosure, the end-to-end encryption is operated.
- **System Management Server**
  A trusted server that generates and distributes the pre-shared keys used for the secure communication between mobile terminals. It also orders the renewal of pre-shared keys among the mobile terminals and the deletion of keys in the stolen mobile terminal.
- **Broadcast Data Distribution System**
  A network used for the one-way communication from the system management server to each mobile terminal, such as the broadcast data distribution service using the satellite communication.

The following three types of keys are used in this system.

- **Device Key – Kd**
  A pre-shared key between each mobile terminal and the system management server. A device key is used to encrypt the commands that are sent from the system management server to each terminal. It is also used to archive integrity of the commands. We use the notation $\mathbf{Kd^X<A>}$ to denote a device key of the mobile terminal A, the generation number of which is X. The notation $\mathbf{Kd^0<A>}$ denotes the initial device key for the mobile terminal A generated by the system management server.
- **Master Key – Km**
  A pre-shared key between mobile terminals that perform secure communication. An initial master

key is generated in the system management server and distributed to each mobile terminal via a key distribution command. We use the notation **Km^{Y}<A, B>** to denote a master key between the mobile terminal A and B, the generation number of which is Y. The notation **Km^{0}<A, B>** denotes the initial master key for mobile terminal A and B generated by the system management server.

- **Session Key – Ks**
  An encryption key between mobile terminals that perform secure communication. A session key is derived from the master key shared in advance. We use the notation **$Ks^{Z}(Km^{Y}$<A, B>)** to denote a session key derived from the master key Km^{Y}<A, B>, the generation number of which is Z.

In addition, we used the following notations to denote the cryptographic operations using these keys [9].

{X}K : Encryption (with MAC) of plaintext X with Key K to provide confidentiality and integrity
[[X]]K : Encryption of plaintext X with key K to provide confidentiality
[X]K : MAC of plaintext X with key K to provide integrity

5.2 Pre-sharing Device Key

The device keys must be shared between the system management server and each mobile terminal before the operation of the secure communication system would be started. The system management server generates the device keys for each mobile terminal. Then each device key was pre-distributed to the corresponding terminals securely. For example, the administrator operates the management server to generate the device keys and install them to each mobile terminal. Then he distributes the mobile terminal to each user. Figure 6 shows the pre-sharing device key between the system management server and the mobile terminals. The system management server generates the initial device key **Kd^{0}<Alice>** and **Kd^{0}<Bob>**. Then Alice's initial device key Kd^{0}<Alice> is installed to Alice's mobile terminal and Bob's initial device key Kd^{0}<Bob> is installed to Bob's mobile terminal.

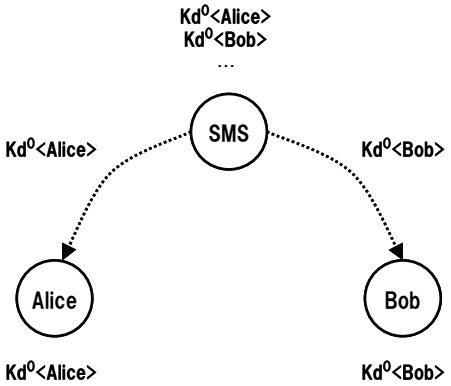


Figure 6: Pre-sharing Device Key

5.3 Distribution of Master Key

The system management server generates the master keys which are used for the secure communication between mobile terminals. Then the master keys are encrypted with the pre-shared device keys where the only legal terminal can decrypt the encrypted master key. Then system management server distributes the encrypted master keys via the broadcast data distribution systems to the whole mobile terminals. For example, the system management server generates the initial master key **Km^{0}<Alice, Bob>** between Alice and Bob. The server generates the key-encryption key **Ktmp** and encrypts the master key Km^{0}<Alice, Bob> with the key-encryption key Ktmp. The both encryptions of the key-encryption key Ktmp with Alice's device key Kd^{0}<Alice> and Bob's device key Kd^{0}<Bob> are added to the encrypted master key. The encrypted master key **M_{Km}<Alice, Bob>** sent from the management server to mobile terminals is defined as the following.

M_{Km}<Alice, Bob>
= [[Km^{0}<Alice, Bob>]]Ktmp
|| {Ktmp}Kd^{0}<Alice>
|| {Ktmp}Kd^{0}<Bob>

That is, the master key Km^{0}<Alice, Bob> can be only decrypted with either Alice's device key Kd^{0}<Alice> or Bob's device key Kd^{0}<Bob>. The encrypted master key for Alice and Bob is distributed through the satellite broadcast data distribution system. It means that all mobile terminals including Carol's receive the encrypted master key, but only Alice's and Bobs' can be decrypt it. Figure 7 shows the generation and distribution of master keys. In this figure, the information exchanged between entities is defined as the following.

1. SMS→{Alice, Bob, …}: M_{Km}<Alice, Bob>

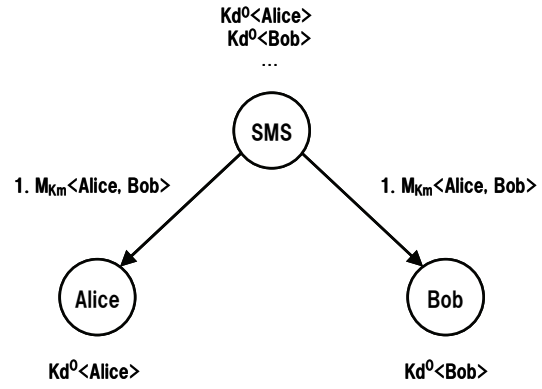


Figure 7: Generation and Distribution of Master Key

5.4 Generation of Session Keys

At the time of secure communication, each mobile terminal derives the session key from the pre-shared master key. Then their communication is encrypted with the session key. The session key should be re-derived from the same master key when it would be used to en-

crypt/decrypt the specific number of times. For example, when Alice's mobile terminal and Bob's mobile terminal share the master key Km^0<Alice, Bob>, a sequence of session keys, such as **{K_S^1(Km^0<Alice, Bob>), K_S^2(Km^0<Alice, Bob>), …}** is derived from the pre-shared master key. Then communication between Alice and Bob is encrypted with those session keys. At the beginning of communication, the first session key **K_S^1(Km^0<Alice, Bob>)** is derived from the master key Km^0<Alice, Bob>. Then the communication is encrypted with the first session key. When the first session key is used for encryption a thousand times, the second session key **K_S^2(Km^0<Alice, Bob>)** is derived from the master key and will be used for next thousand times encryption. Figure 8 shows the generation of session keys and secure communication with them. In this figure, the information exchanged between entities is defined as the followings.

1. Alice←→Bob: {Data}K_S^1(Km^0<Alice, Bob>)
…
n. Alice←→Bob: {Data}K_S^1(Km^0<Alice, Bob>)
n+1. Alice←→Bob: {Data}K_S^2(Km^0<Alice, Bob>)
…
2n. Alice←→Bob: {Data}K_S^2(Km^0<Alice, Bob>)

where

n: Maximum number of encryption times using the same session key

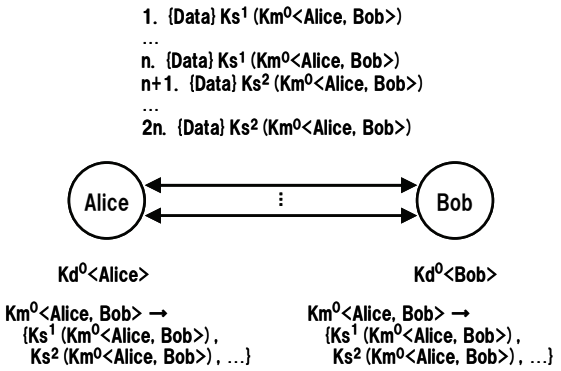


Figure 8: Generation of Session Keys

5.5 Renewal of Device Key

The device keys are used for the one-way secure communication from the system management server to each mobile terminal. Therefore the keys should be renewed at the sufficient intervals. When the renewal of device keys is necessary, it is operated according to the instructions described in Section 4.3. For example, the system management server sends the device key renewal command that instructs the renewal of the initial device key to the next generation. The system management server also renews its own device keys of each mobile terminal. That is, the renewal device keys **Kd^1<Alice>** and **Kd^1<Bob>** are derived from the initial device keys Kd^0<Alice> and Kd^0<Bob> respectively. In Alice's mobile terminal, the renewal device key **Kd^1<Alice>** is derived from the initial device key Kd^0<Alice>. In Bob's mobile terminal, the renewal device key **Kd^1<Bob>** is derived from the initial device key Kd^0<Bob>. Figure 9 shows the renewal of device keys by sending the device key renewal command from the system management server to each mobile terminal. In this figure, the information exchanged between entities is defined as the following.

1. SMS→{Alice, Bob, …}: M_{RnKd}

where

M_{RnKd}: Device Key Renewal Command

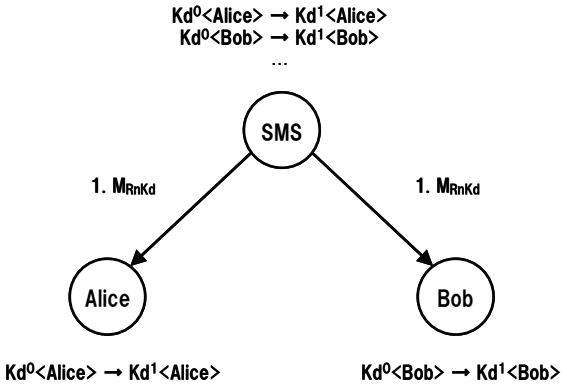


Figure 9: Renewal of Device Key

The mobile terminals will also renew the device keys when the validity of the current device key would be expired or when the generation gap of the device keys would be detected.

5.6 Renewal of Master Key

The master keys are used to derive the session keys (encryption keys) between mobile terminals. The master key should be renewed at the sufficient intervals. In some cases, the master keys must be renewed at every time when the new secure session would be established between the same pair of mobile terminals. Thus the renewal of master keys are operated according to the instructions described in Section 4.3. For example, the system management server sends the master key renewal command that instructs the renewal of the initial master key to the next generation. In Alice's mobile terminal, the renewal master key **Km^1<Alice, Bob>** is derived from the initial master key Km^0<Alice, Bob>. In Bob's mobile terminal, the same renewal is performed. Figure 10 shows the renewal of master keys by sending the master key renewal command from the system management server to each mobile terminal. In this figure, the information exchanged between entities is defined as the following.

1. SMS→{Alice, Bob, …}: M_{RnKm}

where

M_{RnKm}: Master Key Renewal Command

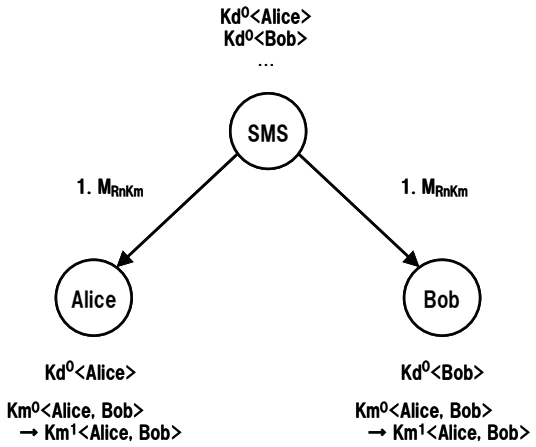


Figure 10: Renewal of Master Key (1)

The mobile terminals will also renew the master keys when the validity of the current master key would be expired or when the generation gap of the master keys would be detected. For example, Alice's mobile terminal received the master key renewal command from the system management server and performed the master key renewal from Km^0<Alice, Bob> to Km^1<Alice, Bob>. But Bob's mobile terminal didn't receive the same command because of the loss of packets. At the beginning of the secure communication, the both mobile terminals negotiate of which master keys they have. Then Bob's mobile terminal detects the loss of the master key renewal command and perform the derivation of the renewal master key **Km^1<Alice, Bob>** from Km^0<Alice, Bob>. Figure 11 shows another renewal of master keys by the detection of generation gap between the mobile terminals.

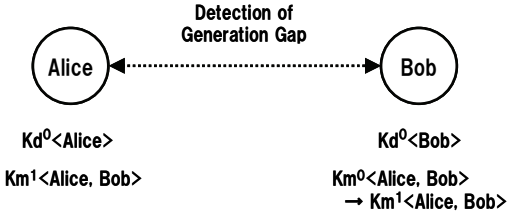


Figure 11: Renewal of Master Key (2)

The renewal of master keys may be achieved by the redistribution of new master keys from the system management server. If the distribution of renewal key (see Section 3.1) may be acceptable, the new master keys, such as **{K'm^0<Alice, Bob>, K''m^0<Alice, Bob>, …}** might be distributed by the same procedure as mentioned in Section 5.3.

5.7 Deletion of Keys

If the mobile terminal might be stolen, the user would report that to the system administrator. The administrator will operate the system management server in order to create the key deletion command and send it to the stolen terminal. The terminal that receives the command will delete the all cryptographic keys inside. In some cases, the initialization of the mobile terminal (the deletion of everything inside the terminal) may be performed by sending the terminal initialization command instead. For example, the system management server sends the terminal initialization command that contains the identifier of Alice's mobile terminal (**TermID**), its issuing date (**Date**) and the reason of initialization (**Reason**). The command $\mathbf{M_{Init}}$ sent from the system management server to mobile terminals is defined as the following.

$M_{Init} = M_{InitTBA} \| MACs$
$M_{InitTBA} = TermID \| Date \| Reason$
$MACs = [M_{InitTBA}]Kd^0<Alice> \| [M_{InitTBA}]Kd^0<Bob> \| \ldots$

The command contains not only the MAC (message authentication code) for Alice but also the MACs for Bob and others. Therefore all mobile terminals can verify the validity of the command. The detailed use of this command in other mobile terminals is described in [1]. Figure 12 shows the deletion of keys in the stolen terminal. In this figure, the information exchanged between entities is defined as the following.

1. SMS→{Alice, Bob, …}: M_{Init}

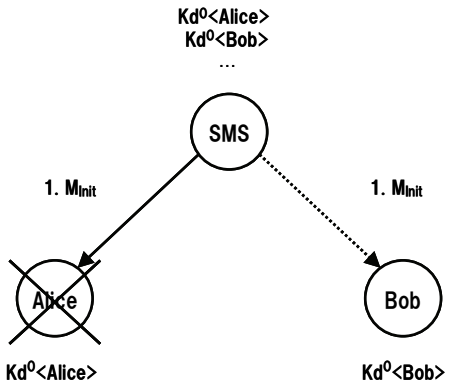


Figure 12: Deletion of Keys in stolen Terminal

6 CONCLUSION

In this paper, we propose the renewal method of the pre-shared key for the secure communication of multiple mobile terminals. We also apply the proposed method to the secure real-time communication systems where the management operations from the system management server to the mobile terminals are distributed through the broadcast data distribution systems. The prototype of this system is being implemented, but not completed yet [10]. We will extend our implementation to support the proposed method and evaluate its effectiveness.

REFERENCES

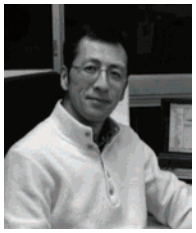
[1] H. Tsuji, T. Yoneda, T. Mizuno, and M. Nishigaki, "Realization of Secure Real-time Communication for Worldwide Mobile Environment by Frequent Key Renewal Method through Broadcast Data Distribution Systems," IPSJ Journal Vol. 50, No. 9 (2009).
[2] RFC 3830, "MIKEY: Multimedia Internet KEYing" (2004).
[3] RFC 3711, "The Secure Real-time Transport Protocol (SRTP)" (2004).
[4] P. Kocher, "Timing Attacks on Implementation of Diffie-Hellman, RSA, DSS and Other Systems," CRYPTO'96 (1996).
[5] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," CRYPTO'99 (1999).
[6] Y. Tsunoo, E. Tsujihara, K. Minematsu, and H. Miyauchi, "Cryptoanalysis of Block Ciphers Implemented on Computers with Cache," ISITA2002 (2002).
[7] B.C. Neuman and T. Ts'o, "Kerberos: An Authentication Service for Computer Networks, IEEE Communications Magazine," Vol. 32, No. 9 (1994).
[8] Open Mobile Alliance, "OMA Device Management Protocol, Approved Version 1.2.1", 17 Jun 2008 (2008).
[9] C. Boyd and A. Mathuria, "Protocols for Authentication and Key Establishment," Springer (2003).
[10] H. Tsuji and T. Yoneda, "Secure Mobile Phone System," Mitsubishi Electric Technical Report, Vol. 82, No. 5 (2008).
[11] H. Tsuji and T. Yoneda, "Renewal of Pre-shared Key among Multiple Mobile Terminals," the 2009 Symposium on Cryptography and Information Security (SCIS 2009), 3D4-3 (2009).

(Received August 26, 2009)
(Revised January 26, 2011)

Hirosato Tsuji received the B.E. degree from Tohoku University in 1988 and received the Ph.D. degree in Engineering from Shizuoka University, Japan in 2010. In 1989, he joined Mitsubishi Electric Corp. Now, he is a head researcher of Information Security Technology Dept. in Information Technology R&D Center. His research interests include computer networks, distributed computing systems and information security. He is a member of Information Processing Society of Japan.

Takeshi Yoneda received B.S., M.E. and Ph.D. degrees in instrumentation engineering from Keio University, in 1989, 1991 and 1994, respectively. In 1994, he joined Mitsubishi Electric Corp. Now, he is a team leader of Information Security Technology Dept. in Information Technology R&D Center. His research interests include information security architecture, embedded security and secure communication protocols. He is a member of Information Processing Society of Japan and ACM.

Tadanori Mizuno received the B.E. degree in Industrial Engineering from the Nagoya Institute of Technology in 1968 and received the Ph.D. degree in Computer Science from Kyushu University, Japan, in 1987. In 1968, he joined Mitsubishi Electric Corp. Since 1993, he is a Professor of Shizuoka University, Japan. Now, he is a Professor of Graduate School of Science and Technology of Shizuoka University. His research interests include mobile computing, distributed computing, computer networks, broadcast communication and computing, and protocol engineering. He is a member of Information Processing Society of Japan, the Institute of Electronics, Information and Communication Engineers, the IEEE Computer Society, ACM and Informatics Society.



Masakatsu Nishigaki is an associate professor at the Graduate School of Science and Technology of Shizuoka University, Japan. He obtained his PhD in Engineering from Shizuoka University. His current research interests are in information security, neural network, circuit simulations, etc. He is now a secretary member of IPSJ Special Interest Group on Computer Security, IPSJ Study Group on Security Psychology and Trust, and IEICE Technical Committee on Biometric System Security, respectively.

A Method of Selecting Optimal Measures for Security and Usability with Fault Tree Analysis and State Transition Diagram

Koichi Kato* and Yoshimi Teshigawara**
Faculty of Engineering, Soka University, Japan
*kokatou@soka.ac.jp, **teshiga@t.soka.ac.jp

Abstract—A high level of security must be maintained on a network to protect information assets, but usability is required to achieve the network's designed purpose. Security and usability, however, have a trade-off relation. Selecting appropriate security measures is difficult because (i) chain relations exist for risks and services use and (ii) the relations among risks, usability and security measures are complex. This paper proposes a method of analyzing risk/usability and selecting measures by using Fault Tree Analysis (FTA) and State Transition Diagrams (STDs). This method is used to analyze risk and usability visually and quantitatively in consideration of chain relations. The method also allows the causes of incidents to be inferred by converting the STD to a Bayesian network. Accordingly, we can estimate the interdependence among risks and usability, and thereby find a critical point for risks and usability. As a result, we can select optimal measures to control and monitor network security and usability.

Keywords: Risk Management, Usability, Fault Tree Analysis, State Transition Diagram, Bayesian Network.

1 INTRODUCTION

Recently, a variety of network environments have been constructed, such as home networks, enterprise and university networks, and high-speed public wireless networks. These networks are established for various purposes such as accessing to the Internet, sharing resources and conducting business efficiently.

However, information systems on a network are exposed to many risks including information leakage and unauthorized access (e.g., hacking). The occurrence of a security incident can cause not only direct damages such as lost business or system recovery costs, but also loss of organizational credibility. Therefore, a variety of security measures are now implemented on networks to reduce risk.

For a network to fulfill its designed purpose, a suitable balance must be struck between the security of information assets and usability of services. However, security and usability are generally in a trade-off relation. For example, security measures can disturb comfortable use of information systems by increasing the number of steps in a process or slowing the execution speed of the system; excessive security measures decrease the level of usability. In contrast, excessive usability decreases the level of security. Accordingly, balancing security with usability is a difficult but critical task.

In addition, risks and usability must be managed and monitored to determine whether security incidents occur and whether services are properly provided [1]. However, deciding appropriate monitoring points is difficult for a network consisting of many devices.

In related studies on the prioritization of risk, Zuccato [2] described the decision matrix and Guan et al. [3] evaluated security with the Analytic Hierarchy Process and the risk level matrix. They analyzed risks only from the viewpoint of expert users and did not consider the existence of multiple stakeholders. Yajima et al. [4] proposed the multiplex risk communicator to decide measures based on agreement among stakeholders. However, they did not analyze usability in detail. Kotenko and Stepashikin [5] as well as Wang [6] described security evaluation methods using the attack graph, which allows the events of an incident to be analyzed visually and measures to be implemented in consideration of the network configuration. However, the effects on usability of the selected measures cannot be expressed.

In our research, we have approached this matter in two ways, devising (i) a method of selecting optimal measures when the implemented measures are changed [7] and (ii) an expression model of risks, usability and security measures [8]. Combining the above-mentioned method and model, we propose a method of selecting optimal measures to construct a network that has high usability to conduct business efficiently and sufficient security to protect information assets. With this method, phases of risks and services use can be analyzed by using Fault Tree Analysis (FTA) and State Transition Diagrams (STDs). In this way, we can estimate the interdependence among risks and usability, and thereby find their critical point for risk and usability. As a result, we can select optimal measures intuitively by quantifying and visualizing risks, usability and the effects of security measures.

2 RESEARCH ISSUE

2.1 Analysis of Risk and Usability Having Chain Relations

There exist risk chains where the occurrence of a single risk event leads to multiple other risks. In addition, in risk chains, a fundamental part of a risk event can diverge to other risks. Similarly, there exist usability chains where the deterioration of usability in one area adversely affects the usability in other areas. Therefore, analyzing the relations among risks and usability with chain relations is necessary to maintain usability and to reduce risk.

2.2 Relations among Risk, Usability and Measures

The relations among security measures, risks and usability are complex. Several security measures can be taken against a single risk, but a measure can also be effective

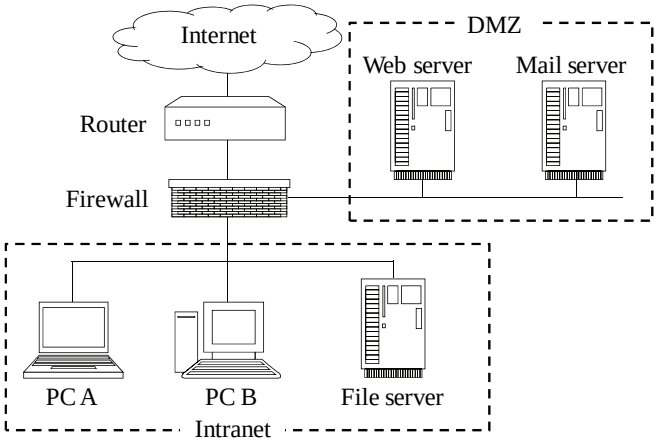


Figure 1: Example of network configuration.

against multiple risks. Moreover, measures to address risks can affect usability. In order to control risks and usability appropriately, a critical point must be found for risks and usability that is more sensitive to the effects of a security measure. The implementation of a measure at the critical point can cause a considerable increase or decrease in security and usability. Therefore, analyzing these relations properly and effectively is crucial.

2.3 Relations among Risk, Usability and Measures

The relations among security measures, risks and usability are complex. Several security measures can be taken against a single risk, but a measure can also be effective against multiple risks. Moreover, measures to address risks can affect usability. In order to control risks and usability appropriately, a critical point must be found for risks and usability that is more sensitive to the effects of a security measure. The implementation of a measure at the critical point can cause a considerable increase or decrease in security and usability. Therefore, analyzing these relations properly and effectively is crucial.

2.4 Selection of Optimal Measures

We define “optimal measures” as the combination of measures that system administrators and users accept with satisfaction from the viewpoints of security and usability. In this research, we target the phases of both implementing and modifying security measures. The requirements for security and usability can vary depending on the situation; for example, the security and usability requirements of users and system administrators differ.

Objective evaluation of the security and usability levels that would results from implementation of candidate measures is needed to select appropriate measures. Our method quantifies the probability and value of risks, which are general metrics, and usability. The value of usability in our method is the rate of comfortable service use relative to the completely unrestricted use of the service without implementation of security measures.

Administrators and users may select excessive or insufficient measures that cause undesirable decreases in security and usability if we only calculate the theoretical optimal measures. Therefore, a scheme for selecting appropriate measures intuitively is needed.

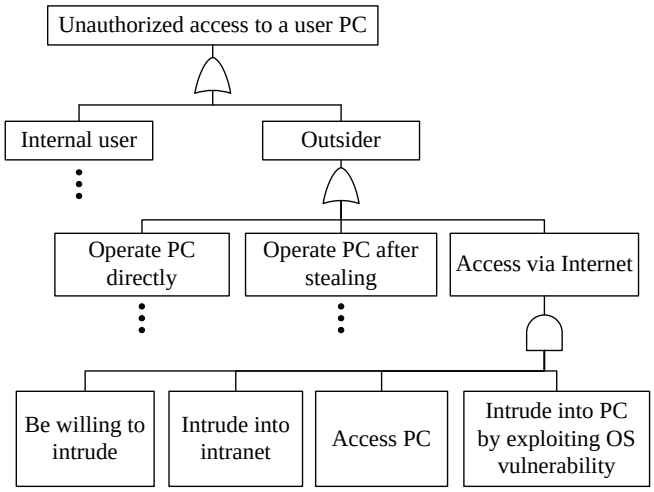


Figure 2: Fault tree for unauthorized access to a user PC.

In addition, the validity of monitoring points for security and usability cannot be evaluated because the points are often decided by experimental rules. Moreover, there exist no objective metrics to infer causes of incidents when a risk event occurs, and as such the scope of the analysis to determine the cause can become unnecessarily broad. Therefore, a scheme for selecting monitoring points and determining the causes of incidents is needed.

3 RISK AND USABILITY ANALYSIS WITH FTA

Our method adopts FTA as a quantification method. FTA has following features: (i) it can analyze factors that prevent the achievement of a specific goal, (ii) it can organize measures to control each factor and (iii) it can decide appropriate measures for specific issues. FTA is used to construct Fault Tree (FT) where the top represents an event as the result of other causal events; these events are joined by logical AND/OR gates [9].

3.1 Example Network

To describe the proposed method, we next present tangible examples. We assume a simple network as shown in Figure 1. The network is separated into a DMZ and the Intranet. A web server and a mail server are located in the DMZ. General users work on user PCs. The users can use files on a file server, browse web sites, and send and receive e-mails.

3.2 Risk Analysis

Generally, a risk event consists of several phases. A risk can be reduced by implementing security measures to prevent the occurrence of each phase based on the concept of defense in depth [10].

In order to quantify risk probabilities, the proposed method makes FTs of risks. First, an unexpected risk event is placed at the top of the FT. Second, attack phases are incorporated at the bottom as shown in Figure 2. Third, measures related to each basic event are clarified. Finally, the probability of a basic event, the decrease in the risk of the targeted

Table 1: Analysis of risks and security measures.

Basic event	Probability	Measure	Risk decrease	State
Be willing to intrude	0.7	-	-	-
Intrude into intranet	0.7	Authentication for network access	0.9	0
		FW access control	0.7	1
Access PC	0.7	At PC: PFW access control	0.5	1
Intrude into PC by exploiting OS vulnerability	0.4	At PC: OS update	0.7	1

basic event caused by a security measure, and the implementation state of a measure, which has yes or no selectively, are assigned as shown in Table 1. Note that the acronyms FW and PFW stand for firewall and personal firewall, and the value of the implementation state (described as "state" in Table 1) is 0 for "not implemented" or 1 for "implemented".

The risk probability is formulated as follows. The probability of the top event is calculated from the minimal cut sets, which are the minimum collections of basic events defined such that if they all occur, the top event also occurs.

The probability of the top event, P_{top}, is given by the following equation:

$$P_{top} = 1 - \prod_{c \in C} \left\{ 1 - \prod_{e \in Ec} P_e \prod_i \left(1 - X_i \Delta P_{e,i} \right) \right\}, \quad (1)$$

where c is a minimal cut set, C is a set of c, e is a basic event in a cut set, E_c is a set of e in c, P_e is the probability of e, $X_i \in \{0, 1\}$ is the implementation state of measure i and $\Delta P_{e,i}$ is the decrease in the risk of event e by implementation of measure i.

3.3 Usability Analysis

The process of service use consists of several phases. The usability of a service can become insufficient because security measures prevent the realization of some phases.

To quantify the usability of services, we use the proposed method to construct FTs of services use. First, an object service is placed at the top of the FT. Second, phases of use are placed at the bottom, as shown in Figure 3. Third, measures related to each basic event are clarified. Finally, the usability of a basic event, the decrease in the usability of the targeted basic event because of the implemented measure and the implementation state of a measure are assigned as shown in Table 2. Note that the value of usability for each basic event is taken as 1 as a standard according to the definition in Section 2.3.

Through this analysis based on the concept of phases, the proposed method can be used to calculate the effective measures preferentially because a measure related to the violated phase recovers the usability better than one related to another phase. Therefore, our method can select appropriate measures considering actual service use.

The usability of the top event, U_{top}, is given by the following equation:

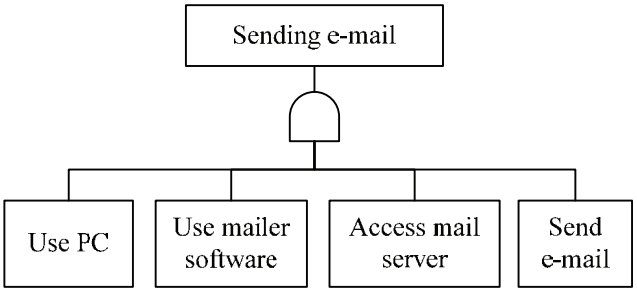


Figure 3: Fault tree for usability of sending e-mail.

Table 2: Analysis of services use and security measures.

Basic event	Usability	Measure	Usability decrease	State
Use PC	1	-	-	-
Use mailer software	1	At PC: password for mailer software	0.3	1
Access mail server	1	At PC: PFW access control	0.1	1
Send e-mail	1	At mail server: Authentication for sending e-mail	0.1	1

$$U_{top} = 1 - \prod_{c \in C} \left\{ 1 - \prod_{e \in Ec} U_e \prod_i \left(1 - X_i \Delta U_{e,i} \right) \right\}, \quad (2)$$

where U_e is the usability of the basic event e and $\Delta U_{e,i}$ is the decrease in the usability of event e by implementation of measure i.

4 RELATIONAL ANALYSIS WITH STATE TRANSITION DIAGRAM

We analyze risks, usability and their chain relations with STDs. FTA can also be used to analyze the relations by combining FTs. However, combining FTs complicates the analysis greatly because FTs can become extremely large. In this case, identifying where each event in the FTs occurs on the target network is difficult. In contrast, the method of making STDs and incorporating them with a network model can be used to analyze risk, usability and these relations visually and intuitively.

4.1 Creating and Combining the STDs of Risk and Usability

The STD of a risk shown in Figure 4 is created by taking the basic event in the FT in Figure 2 as the event in the STD; then, we take the result of the event in the FT as the state in the STD. Similarly, the STD of usability shown in Figure 5 is created from Figure 3.

Each arrow from one state to another represents the probability of the state transition, which is equal to the probability/usability of a basic event as shown in Table 1 and Table 2, owing to the correspondence between the FT and STD. In addition, measures to prevent the realization of a phase are placed on the arrow. Multiple measures can be placed on a single arrow.

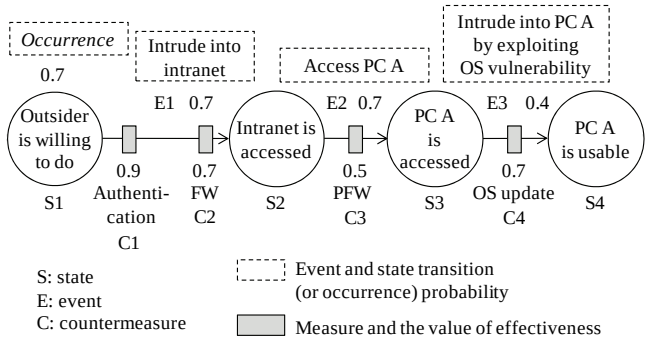


Figure 4: STD of unauthorized access to a user PC.

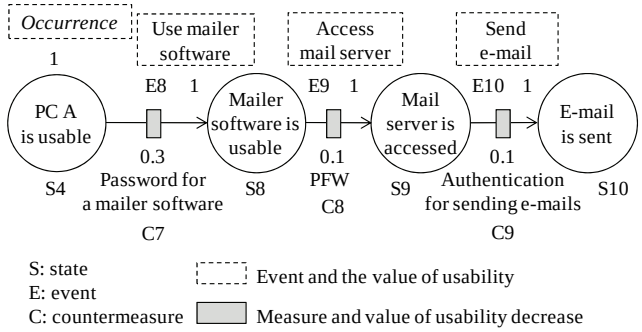


Figure 5: STD of sending e-mail.

In Figure 4 and Figure 5, the decreases in risk/usability caused by a measure are equal to those shown in Table 1 and Table 2. The value is treated as the rate of blocking the state transition. Additionally, a state occurring independently, such as motivation (i.e., "be willing to do something"), has a probability of occurring.

The STDs can be combined by merging identical states, as shown in Figure 6. In order to combine the STDs, idempotent and distributive laws are applied because the STDs correlate with the FTs, and the states and events in the STD can be treated as constituent factors of risks and usability [9]. Note that commutative law cannot be applied because state transition has direction.

The STDs of both risks and usability are also combined by merging identical states such as "PC A is usable" in both Figure 4 and Figure 5. For example, in the case of data leakage from PC A by e-mail, the value 1, which is the standard of usability, can be directly converted into the probability of a successful attack. Therefore, the STD of usability changes to that of risk.

The STDs are deployed on a network model. The organization has some network segments such as a DMZ and an intranet, which can be further divided into additional areas, for example, business departments. Based on the existing defense in depth model [11], our method creates a network model that has network segments and machines in each segment. The machines are also treated as several layers.

For example, the simple network configuration shown in Figure 1 is converted into the model shown in Figure 7 by dividing the network into the DMZ and intranet and developing each machine into the layers of host, application and data. The STDs are deployed on this network model as shown in Figure 8. Each state occurs on a specific layer.

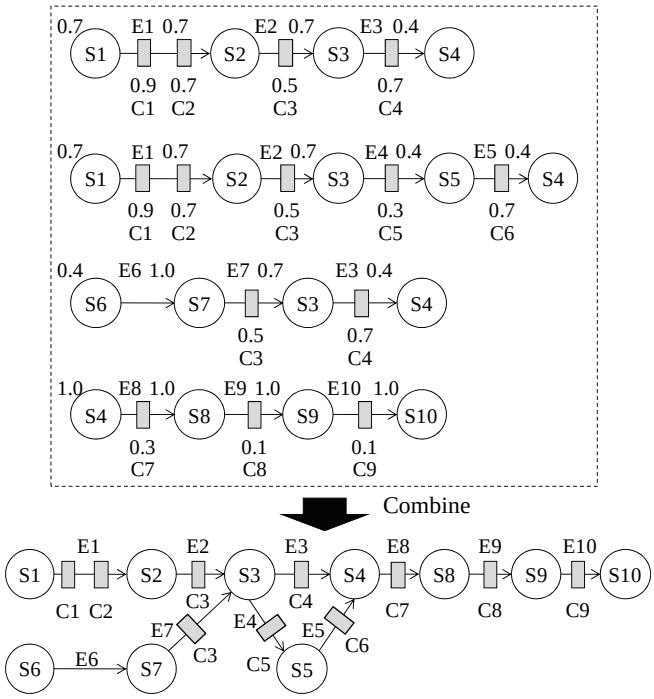


Figure 6: Combining STDs.

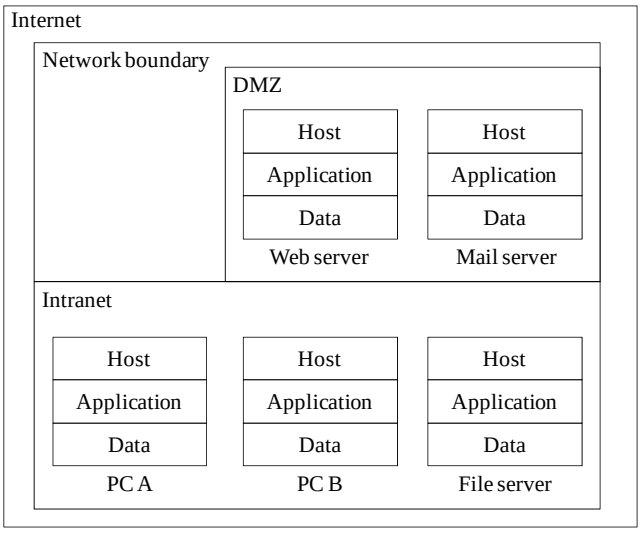


Figure 7: Model of network (cf. Figure 1).

Each arrow passes to a related layer. Each security measure is implemented on a layer.

In addition, STDs can be copied from one machine to another that has identical risks. Differences between machines such as the implementation states of security measures can also be customized as needed.

Details of the model should be set depending on the objectives and accuracy of risk analysis that the organization requires. In the case of Figure 7, the firewall is excluded because we regard it as a security measure. The router is also omitted because we do not consider it to face threats. The network model can treat several segments as a single area and add layers related to hardware such as data storage devices (e.g., hard disks) and I/O devices (e.g., LAN cards).

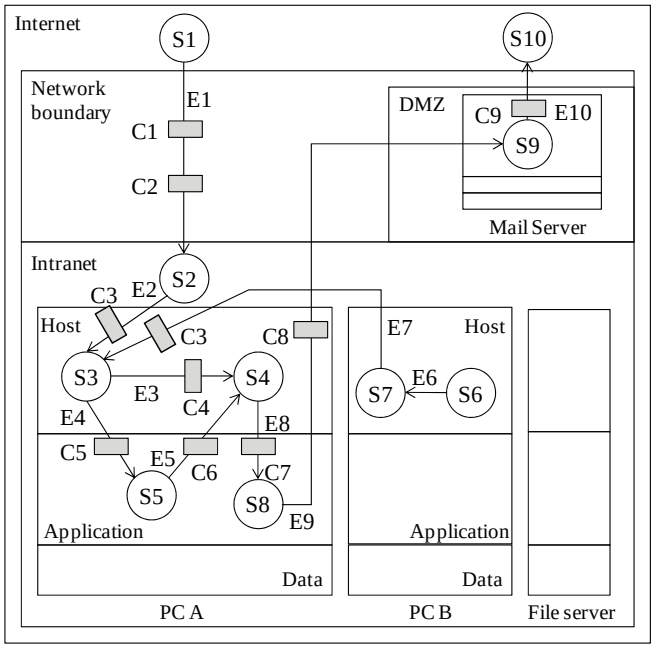


Figure 8: Deployment of risks, usability and security measures on the network model.

4.2 Quantification of Risks and Usability

With Formula (1) and (2) obtained by FTA, we quantify each risk and usability. The STD expressing chain relations can also be used to quantify them.

The risk probability, the value of a risk and the value of usability can be quantified using a model such as the one shown in Figure 8. First, we select the starting and ending states of a target risk. At this time, several starting states can be selected. Next, we extract paths going from each starting state to the ending state. Then, the risk probability P_n for path n is given as follows:

$$P_n = \prod_{e \in E_n} P_e \prod_i \left(1 - \Delta P_{e,i} X_i\right), \quad (3)$$

where e is an event included in path n (e can be the occurrence of a starting state), E_n is a set of e, P_e is the probability of a state transition or the probability of the occurrence of e, $X_i \in \{0, 1\}$ is the implementation state of measure i and $\Delta P_{e,i}$ is the decrease in the probability of event e caused by measure i.

Finally, the total probability P_{total}, that is, the probability of at least one of the paths being realized, is given by

$$P_{total} = 1 - \prod_{n \in N} \left(1 - P_n\right), \quad (4)$$

where N is a set of all paths.

In addition, Formulas (3) and (4) are related to Formula (1) because STDs have a correspondence relation to FTs. Therefore, we must not exponentiate the same state transition probability and the decrease in risk/usability by the same measure in the case that several paths include a common event. We must replace the exponent as follow [9]:

Table 3: Transforming state transition probability to conditional probability.

P(S1)
P_{S1}

P(S6)
P_{S6}

S1	P(S2)
T	P_{E1}
F	0

S6	P(S7)
T	P_{E6}
F	0

S2	S7	P(S3)
T	T	1-(1-P_{E2}) (1-P_{E7})
T	F	P_{E2}
F	T	P_{E7}
F	F	0

S3	P(S5)
T	P_{E4}
F	0

S3	S5	P(S4)
T	T	1-(1-P_{E3}) (1-P_{E5})
T	F	P_{E3}
F	T	P_{E5}
F	F	0

* P(S2), P(S3), P(S4), P(S5) and P(S7) are the conditional probability.
T: transition to the state is done.
F: transition is not done.

$$\left\{P_e \prod_i \left(1 - \Delta P_{e,i} X_i\right)\right\}^2 \rightarrow \left\{P_e \prod_i \left(1 - \Delta P_{e,i} X_i\right)\right\}$$

Furthermore, we can calculate the value of risks in consideration of the value of assets. This paper defines the value of risk as

Value of risk = Value of assets × Risk probability.

For example, when a selected ending state is on the data layer, the risk relates to data. The value of the risk is calculated using the value of the data and the risk probability using Formulas (3) and (4).

Similarly, usability is calculated using Formulas (3) and (4) based on paths for use of a service. Note that $\Delta P_{e,i}$ is the decrease in usability of event e caused by measure i.

4.3 Causal Inference of Incidents

We can regard STDs (e.g., Figure 8) as a probabilistic model of cause-and-effect relations. Therefore, we can treat STDs as a Bayesian network by changing the state transition probability into conditional probability. Note that each state transition probability must be independent of the previous and following phases. As a result, we can infer the probability of causes of an incident.

For example, in Figure 8, we suppose that the state S4 occurs and all measures were not implemented. Table 3 shows the conditional probability of states in the path to S4. The probability that S1 occurred is given as follows

$P(S1|S4) = P(S1 \cap S4) / P(S4)$.

When no state in the selected paths has an occurrence probability such as {S2, S3, S4, S5}, we calculate the arrival probability of S2 as the occurrence probability with Formula (3) and (4).

5 EXPERIMENT

We apply our method at the stages of implementing and modifying security measures in an example of a simple network. We then confirm that our method can be used to analyze phases of risks and usability and to select optimal measures in consideration of where they are implemented.

5.1 Assumptions

In order to avoid complex analysis, we assume a simple network as shown in Figure 1. As discussed in Section 3.1, general network users browse websites, send and receive e-mails and use files on a file server.

We analyze risks selectively because real results of risk analysis in actual organization networks are unavailable due to the confidentiality of security information. The targeted risks are (i) unauthorized access to a PC via networks, (ii) data leakage of a confidential file via networks and (iii) virus infection on a PC. The target services related to usability are (i) browsing websites, (ii) sending e-mails, (iii) reading e-mails and (iv)using files on the file server.

In this experiment, each value is quantified at a certain level. Regarding risks, the state transition probability of a phase has four levels (0.1, 0.4, 0.7, 1.0). The decrease in risk caused by a security measure has five levels (0.1, 0.3, 0.5, 0.7, 0.9). Regarding usability, the state transition probability of a phase has a standard value 1. The decrease in usability caused by a security measure has five levels (0.1, 0.3, 0.5, 0.7, 0.9). The implementation state of a measure has two levels (0, 1).

5.2 Visual and Quantitative Risk Analysis and Measure Selection

(1) Model Creation

First, we model the network. In this experiment, the network is modeled as shown in Figure 7.

Second, we analyze assets, threats, vulnerabilities and phases of target risks and usability as shown in Figure 2 and Figure 3. Then, we clarify measures to basic events based on Reference [12] and assign the probability of a basic event, the decrease in risk/usability caused by a measure and the implementation state of a measure, as shown in Table 1 and Table 2. Finally, we express risks and usability as STDs and deploy them on the network model with implemented security measures. As a result, the model was created as shown in Figure 9.

In this case, all of the event name, the state transition probability and the decrease in risk/usability caused by security measures are eliminated from Figure 9 in order to prevent the model from becoming complex. Most parts of the STDs about PC B are also eliminated because they were copied from PC A.

(2) Use of the Model for Simple Analysis and Correction of the Analysis Results

The created model can be used as an effective visualization tool, which can make it simpler to check and correct the results of risk/usability analysis. In the experiment, some results of the risk analysis and the implementation states of measures by using FTA were reconsidered at the STD model creation.

First, several phases were modified to expand their details because the model could not express several measures on an appropriate layer. The reason is that the phases of risks and the places to implement security measures become clear. Specifically, we added the state named “inappropriate application use” and redeployed the measure named “application update” from the host layer to the application layer. We also added the candidate measure “limitation of usable applications” at the transition between “PC access” and “inappropriate application use”. This measure, however, is not drawn in Figure 9 because we decided not to implement it.

Next, some of the state transition probabilities were modified. They had differed even though the phases were shared by certain risks. The probability of a particular phase should be equal regardless of previous or following phase. Similarly, some decreases in risk caused by a security measure were modified. These values had differed even though the measure was implemented in a common phase for certain risks. These modifications were made to address inconsistent results of risk analysis when combining STDs.

Furthermore, some measures which had already being deployed in a certain phase were copied to other phases. We found that a measure affects the specific targeted phase as well as other phases. The reason of this work is that we can visually clarify phases of risks and the layer where measures are implemented. For example, we found that the security measure “access rights” for reducing the risk of data leakage relates to control of virus infection and sending/receiving attached files in an e-mail; accordingly, we added the measure to appropriate places in the data layer.

Finally, measures that mutually affect certain phases of risks are added as follows: “web filtering”, “PFW preventing inbound access”, “PFW preventing outbound access” and “limitation of attached files in e-mails”. These measures were added so that we can consider whether some measures affecting several events. For example, “web filtering” affects three phases efficiently.

(3) Quantitative Assessment of Risks and Usability

Table 4 shows the probability of risks and the value of usability from the initial analysis using only FTA and from the second analysis using both FTA and STDs. We assessed the value of assets simply as shown in Table 5 and calculated the value of risks as shown in Table 6 from the risk probabilities and the values of the assets, which are the amount of damage when a risk event occurs. Note that although these results include some increased probabilities of risks and decreased usability, they mean not that we selected inappropriate measures, but that we analyzed the risk and usability more accurately.

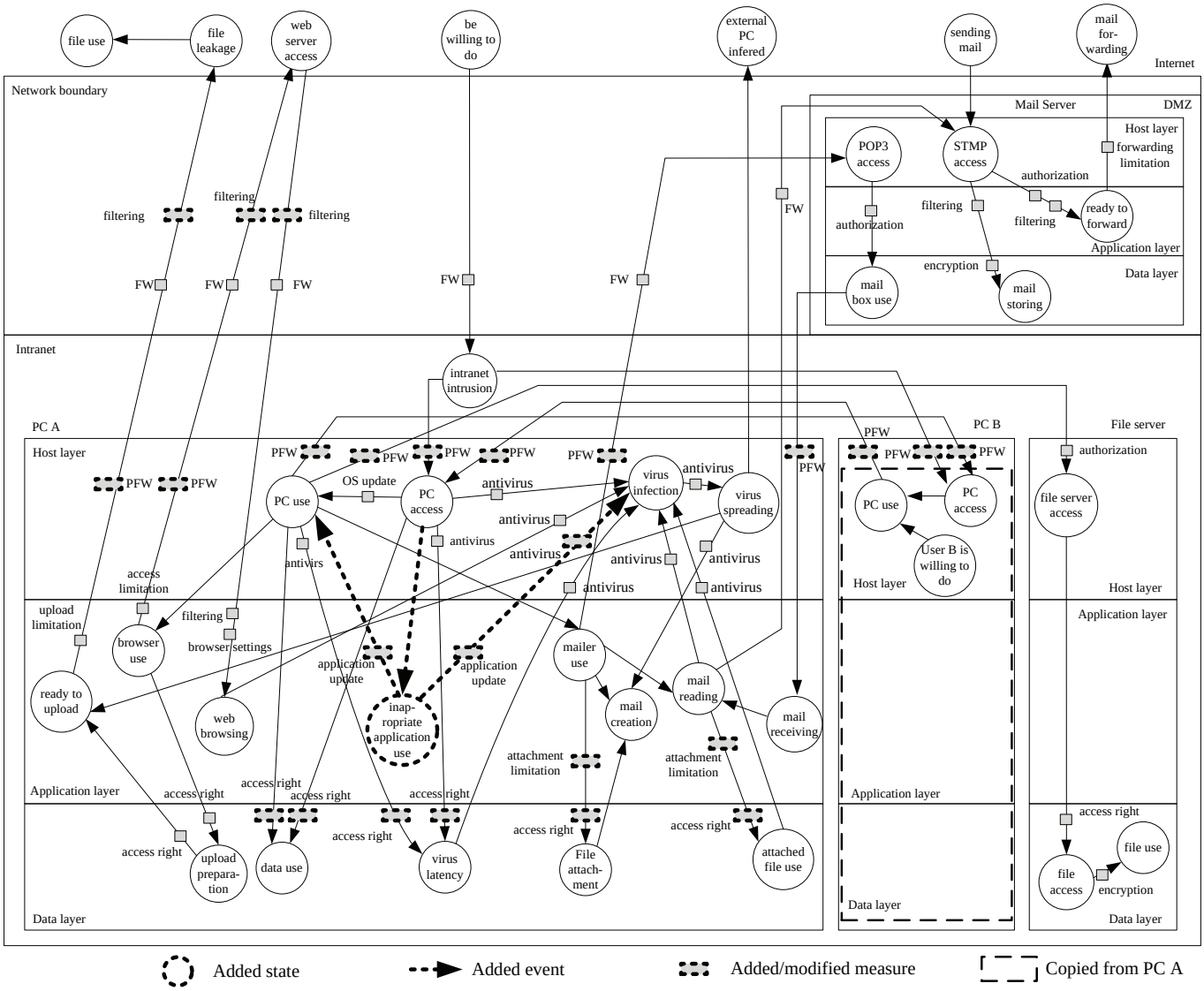


Figure 9: Model of risks, usability and security measures in the assumed network.

As a result, our method can be used to assess risks and usability quantitatively and to select security measures to reduce risks and improve usability.

5.3 Impact Estimates for Measures Control

Some measures must be modified to increase the security or usability by the plan-do-check-act cycle for improving of information security management systems. For reviewing or modifying security measures, identifying the resultant changes of security and usability is important.

Our method using FTA can calculate optimal measures by solving a discrete optimization problem with objective functions to minimize the increase in risk and the decrease in usability and constraint functions to maintain appropriate levels of risk and usability. We can recognize the impact of modifying measures visually by combining the above method with STDs.

We suppose that, for example, in the development of a software product, the user of PC A needs to communicate bidirectionally with an external system using a certain TCP/IP port, which is ordinarily closed. The user requests that the administrator open the port in the firewall. If the port is opened, the network risks being intruded more easily by attackers via the Internet. At the same time, this change causes an increased likelihood of reaching all states that follow from the state “intranet intrusion”.

The additional measures selected by calculation of the optimal measures and negotiation between the administrator and the user are as follows: (a) account lockout after login failure, (b) logging of PC access, (c) password protection of screen saver and (d) prohibition of using HTML e-mail [7]. Table 7 shows the risk probability, and the value of risks and usability, for typical network operation, network operation with the firewall port opened and network operation with implementation of the four above-mentioned security measures.

In this case, the firewall port open can be configured to affect only PC A. Therefore, all of the selected additional measures are implemented on PC A and they do not affect other users shown Figure 9. As a result, our method can select measures in consideration of their implementation layer and extent of effects.

Table 4: Probability and usability at the first analysis with only FTA and reanalysis with both FTA and STD.

Target of analysis		FTA	FTA and STD
(R1)	Unauthorized access	0.0285	0.0494
(R2)	Information leakage	0.0430	0.0198
(R3)	Virus infection	0.0181	0.0158
(U1)	Browsing websites	0.810	0.590
(U2)	Sending e-mail	0.590	0.372
(U3)	Reading e-mail	0.590	0.413
(U4)	Using files on the file server	0.729	0.510

Table 5: Assumptions regarding the value of assets.

(unit: yen)

User PC	1,000,000
Confidential files	
about product development	50,000,000
about customers	10,000,000
Not confidential files	100,000

In addition, another effective measure is “authentication for network access” (which is not drawn in Figure 9 because we decided not to implement it) deployed at the same transition as the firewall. This measure prevents intrusion into intranet. The other measure is “PFW” at the transition continuing directly from “intranet intrusion”. This measure prevents the state from transitioning to other states.

Looking at this analysis, we can see that the proposed method can identify potential states, which can occur by chain relations, by following STDs from a base state, which is directly caused by the transition that the modified measure had inhibited. Similarly, the method can also identify causes to raise the base state by tracing STDs back. At the same time, we can identify the effects on usability.

From a viewpoint of selecting measures, in order to maintain (or reduce) risks, the method can narrow down the candidate measures depending on the concept of preventing chains or resolving causes of the risks. On the other hand, in order to maintain (or increase) usability, the method can also narrow down the candidate measures to improve usability of chain phases or resolve causes of decreased usability.

5.4 Detecting Critical Points and Inferring Causes of Security Incidents

We focus on the state “PC A is usable”, which means unauthorized use of PC A, as an example. First, paths reversed from the state are extracted from the STDs shown in Figure 9. The results are shown in Figure 10. Note that Figure 10 includes measures which are not implemented and limits the states on the PC B to S6, S7 and related events. In addition, we connect an event directly from S2 to S7 in order to make the STD simpler, even though we should analyze events of accessing and intruding into PC B via the Internet.

Next, we change the state transition probability to conditional probability and attempt to infer causes of the incident.

Table 6: Value of risks calculated from the value of assets and risk probability.

(unit: yen)

	Object	FTA	FTA and STD
(V1)	User PC	46,551	65,245
(V2)	All files	2,581,968	1,188,176
	total	2,628,519	1,253,421

Table 7: Shift of risks and usability caused by modifying measures.

Probability and usability

	Usual operation	FW port opened	Additional measures added
(R1)	0.0494	0.0796	0.0518
(R2)	0.0198	0.0375	0.0269
(R3)	0.0158	0.0215	0.0195
(U1)	0.590	0.590	0.590
(U2)	0.372	0.372	0.335
(U3)	0.413	0.413	0.372
(U4)	0.510	0.510	0.510

Value of risk

(V1)	65,245	101,094	71,298
(V2)	1,188,176	2,251,166	1,619,260
total	1,253,421	2,352,261	1,690,558

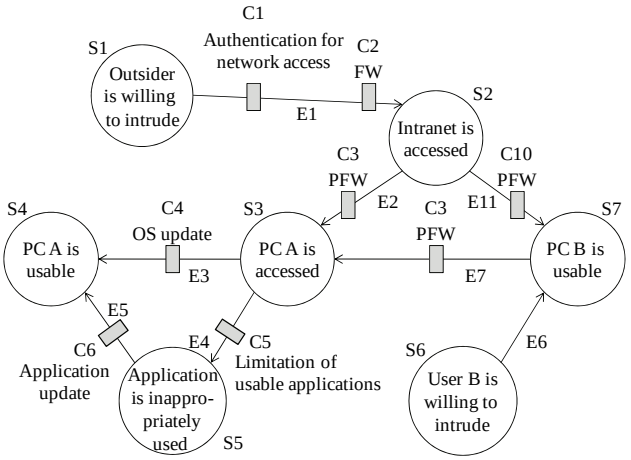


Figure 10: Candidate causes of unauthorized use of PC A.

The state transition/occurrence probabilities, the decrease in risk and the implementation states of measures were analyzed at section 5.2 as shown in Table 8.

Then, we infer the causes of S4. Table 9 shows the probability of each state that had occurred before S4 occurred during usual network operation, when the firewall port was opened (C2) and when “authentication for network access” (C1) was added.

During usual network operation, because the firewall protects against inappropriate access via the Internet, external users might be willing to intrude into the intranet (S1) but the probability of successful intrusion was inhibited (S2).

Table 8: Assigned values of states, events and measures in the analysis.

State or event	State transition /Occurrence probability	Measure	Risk decrease	State
S1	0.7	-	-	-
S6	0.4	-	-	-
E1	0.7	C1	0.9	0
		C2	0.7	1
E2	0.7	C3	0.5	1
E3	0.4	C4	0.7	1
E4	0.4	C5	0.3	0
E5	0.4	C6	0.7	0
E6	1.0	nothing	-	-
E7	0.7	C3	0.5	1
E11	0.7	C10	0.5	1

Table 9: Probability of causation of unauthorized use of PC A.

	Usual operation	FW port opened	Authentication added
P(S1|S4)	0.78	0.86	0.73
P(S2|S4)	0.38	0.77	0.15
P(S3|S4)	1.00	1.00	1.00
P(S5|S4)	0.72	0.72	0.72
P(S6|S4)	0.8	0.59	0.92
P(S7|S4)	0.9	0.78	0.96

On the other hand, the probability that the PC B was used (S7) and the user B was willing to intrude into the intranet (S6) were high. These probabilities mean that an internal user is more suspicious.

When the port of the firewall was opened, external users could access the intranet more easily via Internet. The probability of intrusion by external users (S2) increased considerably. This result means that an outsider became more suspicious.

When “authentication for network access” was implemented, the probability of intrusion by outsiders (S2) decreased notably. The probability that PC B was used (S7) and the user B was willing to intrude (S6) became extremely higher. These probabilities mean that an internal user is highly suspicious.

Note that the attacker had surely accessed PC A (S3) before he/she operated it without authorization (S4). On the other hand, intruding into PC A (S5) is entirely unrelated to whether vulnerabilities of the operating system or an application are exploited, that is, whether the transition from S3 to S4 goes through S5. Therefore, the following conditional probabilities are constant.

$$P(\mathrm{S3}|\mathrm{S4}) = 1, \quad P(\mathrm{S5}|\mathrm{S4}) = 0.72$$

As a result, our method can infer probabilistic causes of risks. Therefore, we can select measures to reduce the probability at the critical points. Furthermore, we can use the probabilities as information for selecting network monitoring points for proactive security measures and analyzing causes of incidents for reactive measures.

6 EVALUATIONS

6.1 Analysis of Risk and Usability with Chain Relations

In this experiment, we analyzed phases of risks and services use with FTA and converted the FT to an STD. We clarified the chain relations among risks and usability by combining the STDs. Moreover, the inconsistencies with the results of risk analysis by FTA are discovered and modified by using the combined STDs. Furthermore, our method can assess risks and usability by calculating the risk probability, the value of risks and the value of usability, as discussed in Section 5.2.

As a result, we confirm that our method can analyze risks and the usability of phases in consideration of chain relations.

6.2 Analysis of Relations among Risks, Usability and Security Measures

In the next experiment, we deployed the combined STDs on the network model based on defense in depth. We also implemented measures in the appropriate layer in the incorporated model presented in Section 5.2. We could recognize the layers related to risks and services use, as well as the place for implementing security measures. In addition, we could clarify the affects on risks and usability caused by modifying measures, as discussed in Section 5.3.

Therefore, the proposed method can be used to analyze visually and intuitively the relations among risks, usability and measures.

6.3 Selecting Optimal Measures and Inferring Causes of Security Incidents

When first selecting security measures in the experiment, we could find efficient measures for preventing certain targeted risks by analyzing the risks based on phases. We also visually found inconsistencies in the analysis results and a lack of required security measures.

When modifying measures, we could recognize the affects of risks and usability visually and quantitatively. We can select measures based on the concept of preventing causes or chains, meaning prior or latter phases. The measures can mitigate increases in risks and decreases in usability.

As a result, we confirmed that our method can select optimal measures visually and quantitatively when implementing and modifying measures.

On the other hand, we inferred probabilistic causes of a risk. We can detect incidents effectively and efficiently by monitoring events with a high likelihood of causing a security incident. We can also efficiently identify the causes of incidents by focusing primarily on such events.

7 CONCLUSION AND FUTURE WORKS

We have proposed a method for analyzing risks and usability and in turn selecting optimal measures in consideration of chain relations. In this method, risks and usability are analyzed by FTA. The FTs are converted to STDs, which are then deployed on a network model in accordance with defense in depth. The method can also be used to infer the causes of incidents by treating the STDs as a Bayesian network.

Through this study, we confirmed that the proposed method can be used quantitatively and intuitively (i) to analyze risks and usability, (ii) to select optimal security measures and monitoring points and (iii) to trace the causes of incidents.

The occurrence probability of a state, the state transition probability and the decrease in risk/usability caused by measures must be exact to assess risks and usability correctly. However, to assign proper values is difficult because these values may differ between environments or users. One solution to address this problem is to cycle risk analysis, assessment and review. The other solution is for stakeholders to decide the values through risk communication (e.g., [4]).

Moreover, Figure 9 is complex even though we consider only three risks and four services. When analyzing more risks and services, the number of states and transitions might become extremely large. On the other hand, the number of states might converge because the risks and usability related to a particular layer often have a common transition. Additionally, each state transition must be independent of the previous and next transitions in order to infer probabilistic causes. One way to achieve the independency of states is to parameterize each state and each event, such as the time of the transition and the person who causes the state transition. However, excessive numbers of the parameters may increase the number of states and transitions. In the future, we plan to study these problems further.

REFERENCES

[1] ISO/IEC 27002, http://www.iso.org/iso/home.htm.
[2] A. Zuccato, “A Decision Matrix Approach –to Prioritize Holistic Security Requirements in E-commerce, Security and Privacy in the Age of Ubiquitous Computing,” IFIP TC11 20th International Information Security Conference, pp. 35-49, Springer (2005).
[3] B.-C. Guan et al., “Evaluation of Information Security Related Risks of an Organization –the Application of the Multi-criteria Decision-making Method,” Proceedings of IEEE 37th Annual International Carnahan Conference on Security Technology, pp. 168-175 (2003).
[4] H. Yajima, et al., “Evaluation of the Participant-Support Method for Information Acquisition in the ‘Multiplex Risk Communicator’”, LNCS 4558, pp. 195-203 (2007).
[5] I. Kotenko and M. Stepashkin, “Attack Graph Based Evaluation of Network Security,” LNCS 4332, pp. 216-227 (2006).
[6] L. Wang, et al., “Measuring the Overall Security of Network Configurations Using Attack Graphs,” LNCS 4602, pp. 98-112 (2007).
[7] K. Kato and Y. Teshigawara, “A Proposal of Selecting Optimal Countermeasures with Security and Usability in a Special Network Use,” IPSJ Journal, Vol. 49, No. 9, pp. 3209-3222 (2008) (in Japanese).
[8] K. Kato and Y. Teshigawara, “A Proposal of a Risks, Usability, and Countermeasures Representation Model for Event Chain Clarification and Causal Inference,” IPSJ Journal, Vol. 50, No. 9, pp. 2243-2256 (2009) (in Japanese).
[9] J.D. Andrews and T.R. Moss, “Reliability and Risk Assessment - Second Edition,” Professional Engineering Publishing (2002).
[10] Microsoft TechNet, “Security Content Overview,” http://technet.microsoft.com/en-us/library/cc767969.aspx.
[11] Microsoft TechNet, “Chapter 3: Antivirus Defense-in-Depth,” http://technet.microsoft.com/en-us/library/cc162798.aspx.
[12] ISO/IEC 13335, http://www.iso.org/iso/home.htm.

(Received August 30, 2009)
(Revised June 23, 2010)

Koichi Kato received B.S., M.S. and Ph.D. degrees in Engineering from Soka University in 2005, 2007 and 2010, respectively. He is an Assistant Professor at Soka University. His research interests include risk management, digital forensics and privacy protection in ubiquitous space. He is a member of IPSJ.

Yoshimi Teshigawara received a doctorate of engineering from Tokyo Institute of Technology in 1970. He joined NEC Corporation in 1970, where he engaged in design and development of computer networks and he worked on international standardization. From 1974 to 1976 he was a Visiting Research Affiliate with the ALOHA System at the University of Hawaii. Since 1995, he has been a Professor at Soka University. His research interests include ubiquitous computing, groupware, e-learning and network security. He is a fellow of IPSJ and ORSJ. He is a member of IEICE, JASMIN, IEEE and ACM.

Submission Guidance

About IJIS

International Journal of Informatics Society (ISSN 1883-4566) is published in one volume of three issues a year. One should be a member of Informatics Society for the submission of the article at least. A submission article is reviewed at least two reviewer. The online version of the journal is available at the following site: http://www.infsoc.org.

Aims and Scope of Informatics Society

The evolution of informatics heralds a new information society. It provides more convenience to our life. Informatics and technologies have been integrated by various fields. For example, mathematics, linguistics, logics, engineering, and new fields will join it. Especially, we are continuing to maintain an awareness of informatics and communication convergence. Informatics Society is the organization that tries to develop informatics and technologies with this convergence. International Journal of Informatics Society (IJIS) is the journal of Informatics Society.

Areas of interest include, but are not limited to:

Computer supported cooperative work and groupware
Intelligent transport system
Distributed Computing
Multi-media communication
Information systems
Mobile computing
Ubiquitous computing

Instruction to Authors

For detailed instructions please refer to the Authors Corner on our Web site, http://www.infsoc.org/.

Submission of manuscripts: There is no limitation of page count as full papers, each of which will be subject to a full review process. An electronic, PDF-based submission of papers is mandatory. Download and use the LaTeX2e or Microsoft Word sample IJIS formats.

http://www.infsoc.org/IJIS-Format.pdf

LaTeX2e

LaTeX2e files (ZIP) http://www.infsoc.org/template_IJIS.zip

Microsoft Word™

Sample document http://www.infsoc.org/sample_IJIS.doc

Please send the PDF file of your paper to secretariat@infsoc.org with the following information:

Title, Author: Name (Affiliation), Name (Affiliation), Corresponding Author. Address, Tel, Fax, E-mail:

Copyright

Publisher

Address: Informatics Laboratory, 3-41 Tsujimachi, Kitaku, Nagoya 462-0032, Japan
E-mail: secretariat@infsoc.org

CONTENTS