Terminal Operation History | Security | Terminal-usage Support

Technology Reports

Use and Protection Technology of Terminal Operation History —Support for How Terminals are Used—

Mobile terminals have now permeated to a wide range of users, who desire improved usability according to a variety of preferences. Accordingly, functionality and services to support user preferences through operation history have been proposed. On the other hand, operation history contains personal information, so a system providing these functions and services safely and securely is necessary for users to accept them. Accordingly, we have proposed a terminal-operation-history application platform able to retrieve operation history data on a mobile terminal, as well as privacy protection middleware. With these systems, operation history data can be handled safely, and a variety of use cases related to mobile-terminal use can be implemented, such as "Terminal-usage support."

Research Laboratories
Takashi Yoshikawa†
Tomohiro Nakagawa
Ken Ota
Communication Device Development Department
Takashi Suzuki

1. Introduction

Recently, mobile terminals have permeated various levels of users, and there is more demand for improved usability and usage preferences. Because of this, usage-support functions that adjust to individual users by using the operation history have been proposed. Examples include menus customized based on the mobile terminal operation history [1], prediction of the next operation [2], and display of search candidates [3]. There are also mobile terminals with functions displaying mail messages or photographs in time sequence or in calendar form[*1] using the sent or received times from messages or the exposure times from photographs as operation history data. A life-log service has even been proposed, which records location and photographs uploaded from a mobile terminal as history data, allows display and search of the data in journal form, and provides functions to exchange this data with other users [4].

Mobile terminal operation history data indicates user behavior and as a platform[*2] on the mobile terminal it could be used by various applications. This is promising to support functions such as personalization or usability improvements. On the other hand, operation history includes private data and personal information, so functionality to protect privacy is also necessary. The Ministry of Internal affairs and Communications (MIC) Working Group (WG) for services using life logs has made reference to protection of personal information contained in history data,

† Currently Communication Device Development Department

*1 **Function displaying in time sequence or calendar form**: Such as the "Life History Viewer" on the FOMA N905i, or the "Lifetime Calendar" on the SO903 and SO903iTV.

*2 **Platform**: Basic software that allows applications to operate. In this article, it is used to mean software at a higher level than the OS.

discussing issues such as the scope of history data obtained, how businesses use the data, and how users ought to be protected [5].

In this article, we propose a platform for using terminal-operation history data (hereinafter referred to as "Operation history PF"), and privacy protection middleware[*3] for maintaining safety and security. Through this proposal, security requirements to prevent information leakage due to ID masquerade or malicious application are met, and the requirements due to the particular resource restrictions of mobile terminals and reliability improvements can also be handled.

2. Use Cases for Operation History Data

Types of use case for operation history data are shown in **Table 1**. One use case which uses the operation history directly (Table 1 (a)) is "Terminal-usage support," which allows (for example) children to review their own usage and be reminded when they exceed limits. Another use case is UI customization, which automatically creates shortcuts for often-used functions [1]. Cases where the operation history is analyzed and the results used directly by the user (Table 1 (b)) include operation support that helps input by predicting what operations may be done next, or content recommendations for video, music or games according to the user's preferences and based on the analysis.

Cases where the operation history is shared with others (Table 1 (c)) could include checking the safety of children or the elderly or managing appropriate mobile-terminal use by employees. For these functions, it is assumed that users providing history data would agree to do so, that limits could be placed on where data was sent, and that history data could be abstracted before sending. Finally, services such as in Table 1 (d) are also possible, automatically generating journals from the operation history and sharing them with others, or summarizing the content-use history from multiple users on a server and using it to provide content recommendations to other users based on their usage history. These cases also require consideration of issues such as obtaining agreement from the users providing history data, and preventing individual persons from being identified.

Table 1 Example use-cases for the operation history data

	Use of the operation history itself		Use of analysis of history data	
Used by user	(a)	·Terminal-usage support ·UI customization	(b)	·Operation support ·Recommendations
Used by other than user	(c)	·Usage support of children, elderly ·Employee management (corporate)	(d)	·Automatic generation/ sharing of journals ·Recommendations

3. Architecture and Design

3.1 Design Requirements Due to the Limitations of Mobile Terminals

The particular limitations of mobile terminals result in the following design requirements.

- Random Access Memory (RAM)[*4] and CPU are limited, so the volume of history data must be reduced in order to prevent operation-history storage and processing from affecting responsiveness. Accordingly, the design limits each field of data recorded in the operation history is restricted to 100 bytes.
- Internal storage (NAND Flash[*5] memory) is limited, so operation history is stored cyclically, deleting older data first and fixing the memory capacity used.
- Devices are battery powered, so there is a possibility of gaps in the operation history due to unexpected loss of power when the battery expires or is removed. Thus, a function is provided which sets a lock flag in non-volatile memory when beginning to store an operation history record. This flag is cleared when writing has completed. The device checks this lock flag when it reboots to determine whether a gap in operation history has occurred

*3 **Middleware**: Software providing functions for common use by multiple applications. This is used for software at a higher level than the platform.

*4 **RAM**: High-speed read/write access memory.

*5 **NAND Flash**: Memory that can be read and written freely, and that retains the data when power to the device is removed. Operation is slower than RAM.

and whether the data is reliable.

3.2 Basic Functions of the Operation History PF

The platform is designed with basic functions providing the common functionality required by various applications for use of the operation history. Examples from the Application Programming Interface (API)[*6] of the operation history PF are given in **Table 2**.

1) Operation History Record Function

Records operations for each of the functions of the mobile terminal as well as operations of applications using the operation history themselves, according to use cases. To enable use of operation histories spanning applications, history data must be recorded using a common API and data structure.

2) Operation History Retrieval Function

Allow applications to retrieve operation history for analysis and display.

3) Cumulative Calculation Functions

Compute the cumulative number of uses and cumulative usage times commonly used in analysis of the operation history.

4) External Output Functions

Sends or outputs data to a server or external storage for use cases where operation history is shared with others or large volumes of operation data must be preserved.

Table 2 List of APIs provided by operation history PF

Operation history record function	
Function name	LogpfErr Print (LogpfInfo & Info)
Function overview	Records an operation history. UIM Information can be attached for each recorded record
Parameters	A pointer to the log data itself (date-time, log data type, application ID, application name, UIM number)
Return value	Error code
Operation history retrieval function	
Function name	LogpfErr GetCyclic (LogpfInt ID, LogpfInfo & Info)
Function overview	Retrieves operation history data given a record ID as a parameter
Parameters	A record ID, and a pointer to the log data itself (date-time, log data type, application ID, application name, UIM number)
Return value	Error code
Cumulative calculation functions	
Function name	LogpfInt Count (LogpfKind kind, LogpfInt appUID)
Function overview	Retrieves the total number of history type in the one day previous
Parameters	Log entry type, application ID
Return value	Total number of entries

3.3 Security Requirements and the Privacy Protection Middleware

Fundamental to operation history, which contains personal information, is that it is only used by the owner, and privacy protection must be considered when sharing it with others.

For this article, we have selected the following requirements to limit the danger of disclosure of operation history data from a mobile terminal, from the perspectives of the user and of the mobile terminal itself.

- Requirement 1:

  Others may not view operation history data without authorization.
- Requirement 2:

  No unnecessary information shall be output when sharing with others.
- Requirement 3:

  Operation history data must not be leaked by unauthorized applications.

For Requirement 1, operation history data could possibly be viewed without authorization in the following three situations.

- Another person could operate the mobile terminal and reference or output the data without authorization.
- Information could leak when another person changes a destination address without authorization.

*6 **API**: An interface that makes the functions provided by the OS, middleware and other such software available to upper-level software.

- Another person could unintentionally view the operation history when the mobile terminal is transferred or lent to them.

Also, for Requirement 3, we are assuming that an unauthorized application means a downloaded Java application (i-appli), supposing that a Java application downloaded from an unofficial site could retrieve operation history data and send it to a server or other destination without authorization. We assume that Java applications downloaded from official sites (i-appli DX), native applications, middleware and the OS are reliable.

The privacy protection middleware was designed against these requirements. For Requirement 1, the middleware provides a password protection function and ties operation history to the User Identity Module (UIM)[*7]. It also provides a transmission-data abstraction function for Requirement 2, and access control functions for Requirement 3.

- Password protection function

  Input of the password is required for configuration or execution of functions in the operation history PF, such as configuring or executing external output of the operation history or enabling or disabling recording of types of operation.
- Function linking operation history to UIM

  Management of all history data is linked to UIM information so operation history data cannot be used from applications or otherwise while a different UIM is inserted in the device.
- External transmission-data abstraction function

  When operation history data is sent to a server, another mobile terminal, or external storage, unnecessary detailed data is not output, providing pre-abstracted operation history data. Specifically, the accumulated times-used and usage time within given time spans are provided from the operation history, and individual applications need not perform this type of processing themselves.
- Access control functions

  To prevent access to operation history data by unauthorized Java applications, the operation history API restricts access by Java applications downloaded from unofficial sites. Note that existing original functions provided to allow Java applications access to incoming call and mail history can still be used as before. The area used by the operation history API to store data is different than that used by existing API functions.

The architecture for the operation history PF and privacy protection middleware providing these functions is shown in **Figure 1**. The operation history record and retrieval functions described above operate on the operation history DB. Each application uses the operation history API through the privacy protection middleware in order to record and retrieve operation history data. Note that individual applications must add their own functionality for recording operation history. However, the middleware provides a function to record operations that do not depend on the application, such as launching the application, so these operations can be recorded without adding functionality to individual applications.

Note also that for this article we have only considered the danger of information leak, but there are other possible dangers. Examples include that the operation history could be falsified for use cases inspecting for unauthorized operation after theft or loss, or that an employee could refuse to acknowledge content of the operation history when their terminal use is being audited.

4. Application Using the Operation History: "Terminal-usage Support"

Recently, use of mobile terminals by elementary and junior-high school students has been increasing, with 31.6% of sixth-year elementary and 55.2% of junior high school students using them [6]. With this development, problems are beginning to appear, such as mobile terminal dependency, or slan-

*7 **UIM**: An IC card storing subscriber information. Inserted into a mobile terminal and used for customer management.

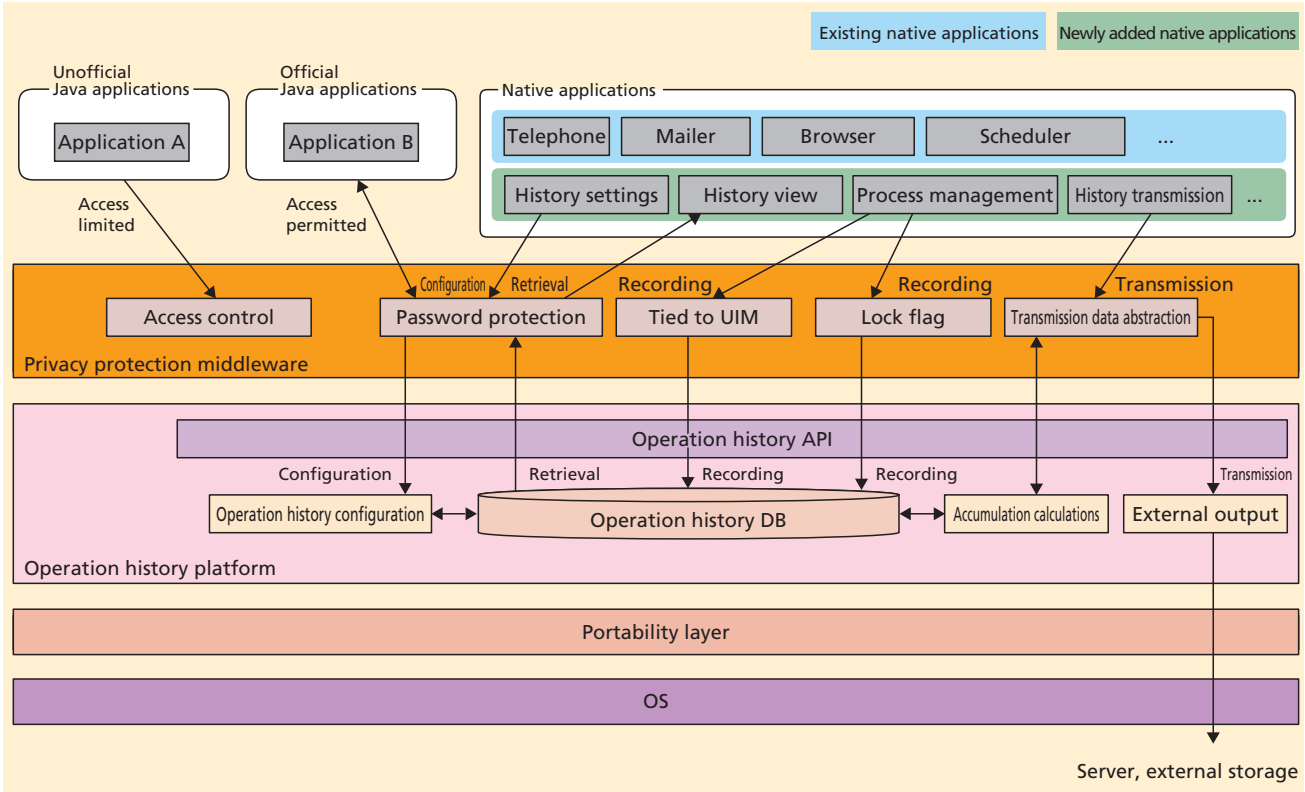


Figure 1 Operation history PF architecture

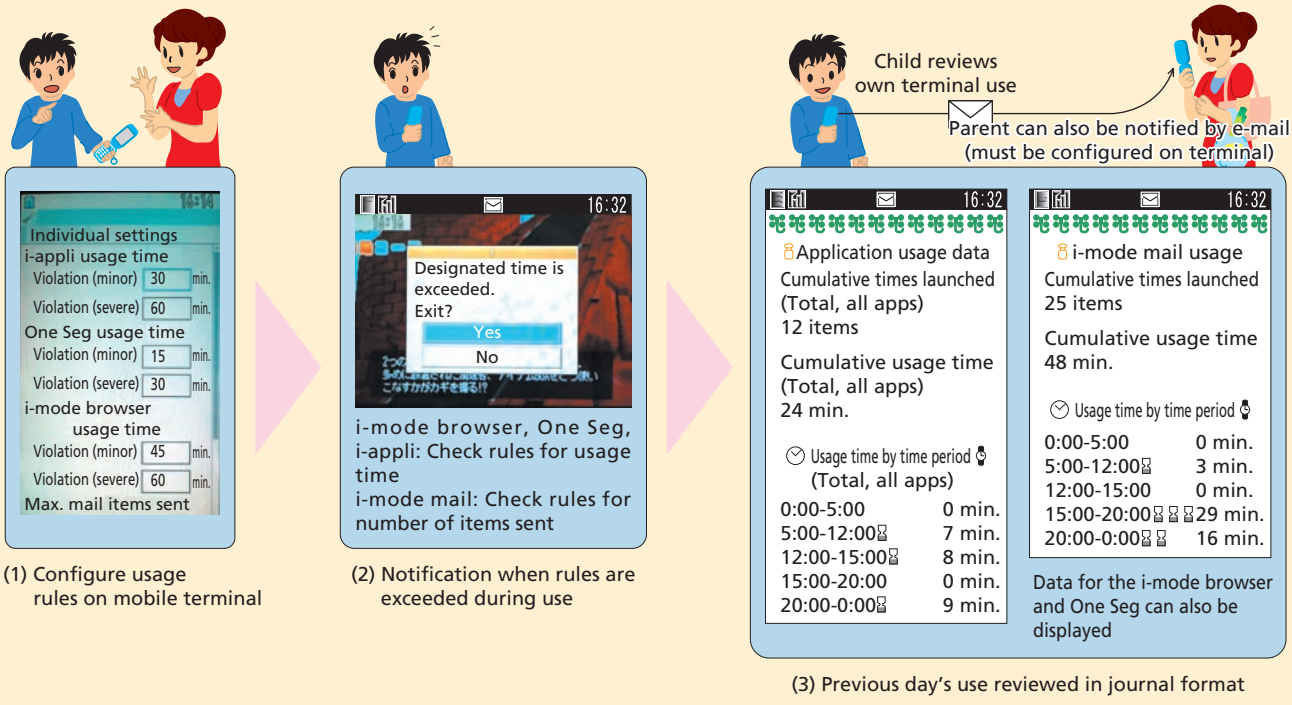
der and abuse through bulletin boards and e-mail [7]. Further, the Meeting on Education Rebuilding has also reported on the need for education on protection from harmful information and rules for mobile terminal use, and these have become widely acknowledged as societal problems [8]. For these reasons, we have developed a "Terminal-usage support" application that can support use of mobile terminals by children through the operation history PF, enabling use of mobile terminal functions and services safely and without worry. A usage scenario with screen shots for "Terminal-usage support" is shown in **Figure 2**.

(1) Parent speaks with child, together deciding rules for use of the mobile terminal. With this prototype, rules can be set for upper limits on the amount of time spent and/or number of messages sent for each of i-appli, One Seg TV, i-mode browser, and sending e-mail messages.

(2) If the child is using a game or other i-appli, for example, when the rule time limit is exceeded, the child is notified with a dialog box.

(3) Once a day, an e-mail in journal format and summarizing the number of times each application was launched, the amount of time used, and whether the rules were followed, is sent to the child's mobile terminal, allowing him/her to review the previous day's use. If configured on the mobile terminal, the message can also be sent to the parent's mobile terminal or PC.

Details of the screens for checking usage status on the prototype implementation are shown in **Photo 1**. Detailed operation history for sent e-mail is not included, and the abstraction function of the privacy protection middleware limits the information displayed to the number of times each



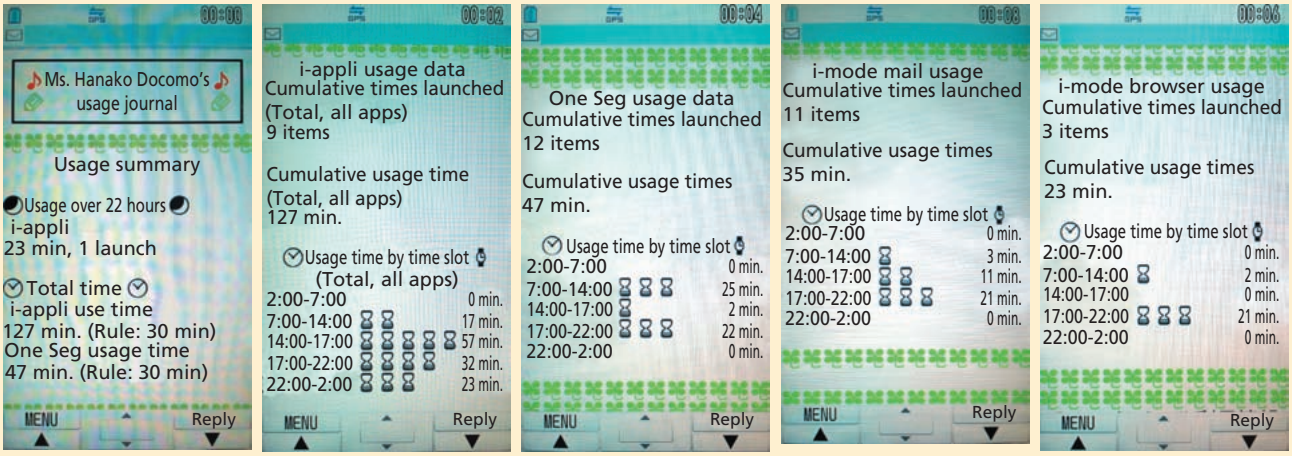
(1) Configure usage rules on mobile terminal

(2) Notification when rules are exceeded during use

(3) Previous day's use reviewed in journal format

*This is provided only in Japanese at present.

Figure 2 Terminal-usage support scenario using mobile terminal



(a) Totals (b) i-appli (c) One Seg (d) i-mode mail (e) i-mode browser

*This is provided only in Japanese at present.

Photo 1 Screen shots of usage data in journal form

application was launched and the amount of time each was used in various time slots.

5. Evaluation/ Discussion

5.1 Effectiveness of Measures Preventing Leakage of Operation History Data

We performed experiments to evaluate the effectiveness of the lock flag used when writing operation history data and intended to improve reliability. For the experiments, we used a prototype based on the FOMA F906i, and checked whether the lock flag worked effectively while intentionally causing a fault during recording. This was done by opening and closing the cover while removing and inserting the battery. The results of three tests of 100 trials each are shown in **Table 3**.

In almost all cases opening and closing the cover was stored correctly in the operation history, but in a few cases the operation was not stored due to a fault. That said, even though storing the operation history failed once or twice in 100 trials, even in those cases the lock flag was saved reliably in nonvolatile memory. This allows the user to know reliably, whether or not a fault has occured during recording of the operation history, after the fact.

5.2 Operation History Data Volume

We performed a theoretical calculation based on real data of the operation history DB capacity required to implement the use cases. We first extracted data on users' daily mobile terminal use from survey reports and other materials from the MIC and Cabinet Office [9]-[14]. These results are shown in **Table 4**. To create model cases, we extracted usage counts from various survey materials and used the the mode of the data as our "average user," the value of the highest rank in the survey results as our "heavy user," and we also included a case with five-times the value for the heavy user.

We calculated the volume of operation history data from the number and amount of time used in each of the model cases, and then calculated the theoretical number of days required to reach a rough target of 5 MB. These results are shown in **Table 5**.

From this study, we determined that using an operation history DB of about 5 MB, an average user could record nearly three months of operation history data. For the "Terminal-usage support" use case, the required storage period is

Table 3 Test results regarding effectiveness of the lock flag

Item No.	Number of trials	Times successfully storing open/close history	Times storing the lock flag
1	100 items	99 items	1 items
2	100 items	99 items	1 items
3	100 items	98 items	2 items

Table 4 Mobile terminal usage for each model case

	Average user	Heavy user	5-Times heavy user values
Place call	2 items	8 items	40 items
Receive call	2 items	8 items	40 items
Send mail	6 items	27 items	135 items
Receive mail	8 items	27 items	135 items
Browse Web	1 items	7 items	35 items
Launch/close Java application	1 items	7 items	35 items
Launch/close application	13 items	50 items	250 items
Open/close terminal	22 items	106 items	530 items

(Units: times/day)

Table 5 Totaled results for operation history data volume

	Records per day	Data size per day	Days to reach 5 MB
Average user	Total 127 records	58.1 KB	Approx. 88 days
Heavy user	Total 563 records	254 KB	Approx. 20 days
5-Times heavy user values	Total 2,815 records	1.24 MB	Approx. 4 days

about one day previous, so if 5 MB can be secured, this should not present any issues. On the other hand, for services that require operation history data over longer periods of time, Table 5 can be used to estimate the DB capacity required.

5.3 General-user Survey

We exhibited the operation history PF, the privacy protection middleware, and the "Children's Terminal-usage support" application at the Combined Exhibition of Advanced Technologies (CEATEC) 2009, held from October 6 to 10, 2009 at Makuhari Messe Convention Center, and we conducted a survey with visitors to the exhibit. Approximately 80% of respondents stated that they were inclined to use these functions. On the other hand, many respondents also commented on the need for communication between parents and children when checking usage rules.

6. Conclusion

In this article, we have studied a mobile terminal architecture allowing the safe and secure gathering and use of operation history data for mobile terminals and we have proposed an operation history PF and privacy protection middleware. We also created a prototype implementation on actual devices, based on the proposed methods, and conducted demonstrations and surveys using the prototypes at CEATEC 2009.

In the future, we will proceed with practical studies of various applications using operation history data, and plan further extensions to the operation history PF.

REFERENCES

[1] NTT DOCOMO Press Releases: "Kisekae Tool Content Production Guide V2.1," pp. 17-18, Aug. 2008 (In Japanese).
[2] D. Kamisaka, S. Muramatsu and H. Yokoyama: "A Study on Situation-Adaptive Operation-Assisting Method for Mobile Phone," IPSJ Report, Vol. 2008-UBI-20, No. 6, pp. 33-38, 2008 (In Japanese).
[3] Google: "Google Maps for mobile."
[4] KDDI Laboratories: "Ubiquitous Networking Technology R&D—Keitai de Life Blog," Nov. 2008 (In Japanese).
[5] Ministry of Internal Affairs and Communications: "Study Group on Problems with ICT Services, Considering the User's Perspective, Midterm Report from the Working Group on Services Using Life Logs," Nov. 2009 (In Japanese).
[6] Benesse Education al R&D Center: "Survey of Children's Practical Ability Using ICT," Apr. 2009 (In Japanese).
[7] T. Yoshida, J. Takai, T. Motoyoshi, T. Igarashi: "A Study of the Mechanisms of Internet Dependency and Mobile Mail Dependency -From an Awareness-behavior Model Perspective-," Telecommunications Advancement Foundation Research Report, No. 20, pp. 176-183, 2005 (In Japanese).
[8] Meeting on Education Rebuilding: "Summary of Deliberation so far -Primary Report-," May 2008 (In Japanese).
[9] Ministry of Internal Affairs and Communications: "Survey of the Internal and External Costs Related to Electronic Communications Services," Aug. 2005 (In Japanese).
[10] Ministry of Internal Affairs and Communications: "State of Japan's Communications in Terms of Traffic (FY 2007)," Oct. 2008.
[11] Cabinet Office: "Fourth Survey Report on Youth and the Information Society," Jul. 2002 (In Japanese).
[12] Impress R&D: "Keitai White Paper 2009," Dec. 2008 (In Japanese).
[13] Tokyo Metropolitan Education Bureau Leadership: "Report on a Survey of Use of the Internet and Mobile Phones by Children (Overview)," Oct. 2008 (In Japanese).
[14] A. Saito: "Actual Conditions of Mobile Phone Use 2007," AD STUDIES, Jun. 2008 (In Japanese).