International Journal of Electronic Commerce Studies
Vol.6, No.1, pp.51-68, 2015
doi: 10.7903/ijecs.1394

PROPOSAL AND EVALUATION OF AN EVIDENCE PRESERVATION METHOD FOR USE IN A COMMON NUMBER SYSTEM

Naoki Kobayashi
Tokyo Denki University
5 Senju-Asahicho, Adachi-Ku, Tokyo 120-8551, Japan
kobayashi.naoki58@gmail.com

Ryoichi Sasaki
Tokyo Denki University
5 Senju-Asahicho, Adachi-Ku, Tokyo 120-8551, Japan
sasaki@im.dendai.ac.jp

ABSTRACT

In recent years, the introduction of a common number system has been planned by the government of Japan, and the possibility of illegal use of personal information in this system has been considered. Access records in log files are analyzed when possible illegal use is being investigated. Therefore, a method by which to maintain the integrity of the log file becomes a significant problem because alteration of digital data is very easy. Moreover, in the case of a common number system, a method that keeps verification secure as well as secret from certain organizations is needed, because various organizations will have access to the common number system. In the present paper, we propose an evidence preservation method that enables privacy and concealment to be maintained by introducing a cipher system and a hysteresis signature.

Keywords: Digital Signature, Hysteresis Signature, Digital Forensic, Evidence Preservation, Common Number System

1. INTRODUCTION

In recent years, the introduction of a common number system has been planned by the government of Japan. The introduction of a common number system is an integral part of reforming the tax and social security indemnification systems and will provide a foundation for the development of e-government services. In addition, the common number system will

improve the efficiency of the people and offer administrative convenience[1, 2].

The common number system must deal with personal information because the system is intended to be used for a wide range of sensitive applications, including the tax and social indemnification systems. The possibility of invasion of privacy is a cause for concern. Therefore, the investigation of suspected illegal use of personal information is needed. When illegal use is investigated, access records in log files are analyzed. Therefore, a method by which to maintain the integrity of a log file becomes a significant problem because alteration of digital data is very easy[3].

The Technical Working Group for Information Sharing Fundamentals of the government of Japan[2] reported that, "It is necessary that access records be accurate and that attention is paid to any alteration of log files." Moreover, a method that keeps verification secure as well as secret from certain organizations is needed in a common number system because various organizations will have access to the common number system. Although there are many papers dealing with secure log systems[4, 5, 6, 7], a specific approach to answer this requirement has not yet been proposed.

In this paper, we propose an evidence preservation method that enables verifiability and concealment to be maintained.

2. COMMON NUMBER SYSTEM

2.1 Overview of the Common Number System

The common number system will assign a new number to each person in Japan. These numbers will be used in the tax and social security indemnification systems[8]. The numbers assigned to individuals are referred to as "My Number." Improvement in administrative procedure efficiency is expected as a by product of the introduction of this system. Additional goals include clarification of income and certain social indemnification benefits. The My Number system is essential to the reform of the tax and social indemnification systems of Japan and so has been discussed widely[9, 10].

There are the following national concerns[8].

(1) Increased possibility of information leakage and abuse resulting from the increase in the amount and types of personal information available for distribution; and,

(2) Possibility of public monitoring by the government

Therefore, verifiable data is necessary in order to investigate injustice and abuse of this sensitive personal information.

2.2 Institutions Involved in the Common Number System

According to the Technical Working Group for Information Sharing Fundamentals[2], a common number system assumes that the following organizations are involved in information sharing (see Figure 1):

(1) **Information service network system**

The Information Service Network System links personal information among multiple agencies. In addition, this organization checks to determine whether all personal information is permitted by law to be sent from one agency to another agency. Basically, information sharing without using the Information Service Network System is not allowed.

(2) **Information retaining agencies**

An Information Retaining Agency holds and refers personal information to the other organizations that have pension, medical care, welfare, and tax information, for example. Examples of Information Retaining Agencies include local governments and ministries and government offices.

(3) **Third-party institutions**

The third-party institution monitors the Information Service Network System and the Information Retaining Agency and is responsible for investigating whether personal information is handled properly from the viewpoint of laws and regulations.

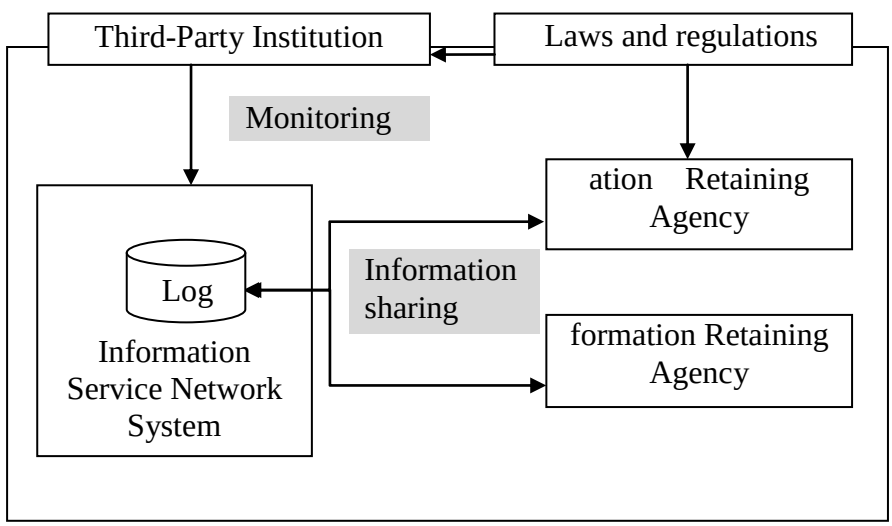

Figure 1. Schematic diagram of the common number system

2.3 Evidence Preservation in the Common Number System

When suspected illegal use is investigated, access records in log files are analyzed. Therefore, how to maintain the integrity of the log file becomes a significant issue because alteration of digital data is very easy.

Information Retaining Agencies exchange personal information. In this case, there is a concern about monitoring by the State. As such, it is not desirable for a single institution to store all personal information[2]. Thus, the Information Service Network System must not view the personal information held by the Information Retaining Agency. On the other hand, judgment as to whether information sharing is proper is also required. Therefore, an evidence preservation method that enables verifiability and concealment of sensitive personal information is needed.

2.4 Log contents in the Common Number System

The following have been discussed as candidates for log contents by the Technical Working Group for Information Sharing Fundamentals[2]:

(1) Serial number for data management

(2) Date and time of access for information sharing

(3) Purpose of information sharing

(4) Name of Information Retaining Agency that offers the information

(5) Name of the Information Retaining Agency that requests or refers the information

(6) Type of personal information for information sharing

(7) Section of the Information Retaining Agency that offers the information

(8) Section of Information Retaining Agency that requests the information

(9) Terminal of the Information Retaining Agency that offers the information

(10) Terminal of the Information Retaining Agency that refers the information

(11) Use of personal information

(12) Contents of personal information provided for information sharing

Here, the contents of from (1) to (11) do not involve important personal information. On the other hand, the contents of (12) include privacy information. Therefore, we must be aware that the log obtained from the contents of (12) contains privacy information which even the staff of government should not know.

2.5 Information Sharing

Figure 2 shows a schematic diagram of information sharing. Information Retaining Agency A provides information, and Information Retaining Agency B refers Information.

Information Retaining Agency A indirectly provides information through a network information service system. This method prevents the unauthorized exchange of personal information. There are two methods of information mediation[2]. Here, we assume a method that uses a gateway system. Each agency keeps a log file of information sharing and uses the log when investigating suspected fraud.

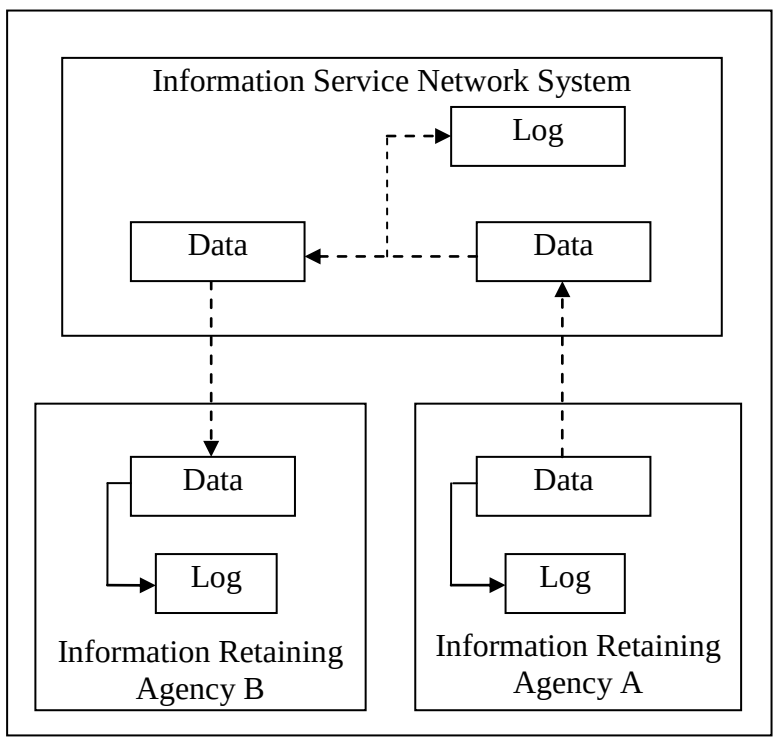

Figure 2. Schematic diagram of information sharing

3. EVIDENCE PRESERVATION

3.1 Prerequisite

As a prerequisite, we assume the following:

The entire staff of any organization does not cause injustice, but there is a possibility that individual staff members may cause injustice.

Staff members of multiple organizations do not conspire.

Stealing personal information from one's own organization is another problem, because this problem exists from old days and its counter method has been proposed.

Access control is performed in Information Retaining Agency A if the staff of Information Retaining Agency A without access privileges demands access to personal information of Information Retaining Agency B.

According to the analysis based on the contents described in Ref.[2], we define the following seven injustices to avoid:

Injustice (1): The staff of the Information Service Network System views personal information illegally.

Injustice (2): The staff of the Information Service Network System alters a log file.

Injustice (3): The staff of the Information Service Network System eliminates log data.

Injustice (4): The staff of the Information Retaining Agency alters a log file.

Injustice (5): The staff of the Information Retaining Agency eliminates log data.

Injustice (6): The staff of the Third-party Institution alters a log file.

Injustice (7): The staff of the Third-party Institution eliminates log data.

3.2 Prevailing Evidence Preservation

As a method by which to detect tampering of digital data, digital signatures are generally used. This mechanism is a combination of public key cryptography and hash functions. Cryptography is also used to encrypt the data.

3.3 Evidence Preservation Using Encryption

We will present a case in which Information Retaining Agency A uses encryption to send encrypted data to Information Retaining Agency B (see Figure 2).

The data, including personal information, is sent after being encrypted by the Information Retaining Agency, and other information is sent without encryption, as shown in Figure 3.

$D_1 \cdots D_{11}$ do not involve personal information.

Since D_{12} involves personal information, the staff of the Information Service Network System should not view D_{12}.

(1) Information Retaining Agency sends $D_1 \cdots D_{11}$, which includes no personal information, to the Information Service Network System. The Information Service Network System is able to inspect $D_1 \cdots D_{11}$.

(2) D_{12}, which is not expected to be viewed by the Information Service Network System, is encrypted using a public key cipher and Information Retaining Agency B's public key P_B.

(3) The hash value of $D_1 \cdots D_{12}$ is encrypted by Information Retaining Agency A's private key S_A in order to generate the signature.

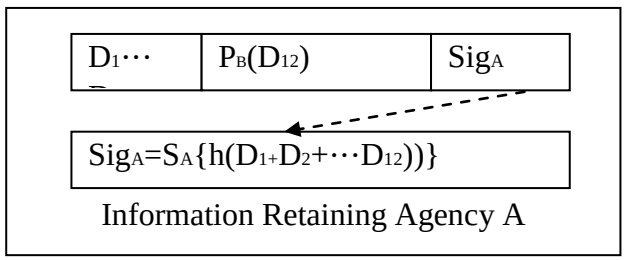

Figure 3. Data content sent by the Information Retaining Agency

3.4 Verification Procedure

The Information Service Network System verifies the validity of the data received from Information Retaining Agency A (see Figure 4). This validation is used to identify alteration after the data is signed at Information Retaining Agency A. The following method is used for verification:

(1) Compute a hash value from Sig_A using the public key of Information Retaining Agency A.

(2) Decrypt $P_B(D_{12})$ using the private key of Information Retaining Agency B.

(3) Join $D_1 \cdots D_{12}$ and calculate the hash value.

(4) Compare the value obtained in (1) and the value obtained in (3). If these values match, the validity of the data is proven.

3.5 Problems

The Information Service Network System cannot view personal information because private information is encrypted.

However, in order to satisfy the requirement in step (2), D_{12} must be decrypted. If the data is decrypted, the staff of the Information Service Network System can view the information, and this method cannot satisfy the requirement described in 3.3.

For this reason, an evidence preservation method that allows information privacy and concealment is needed.

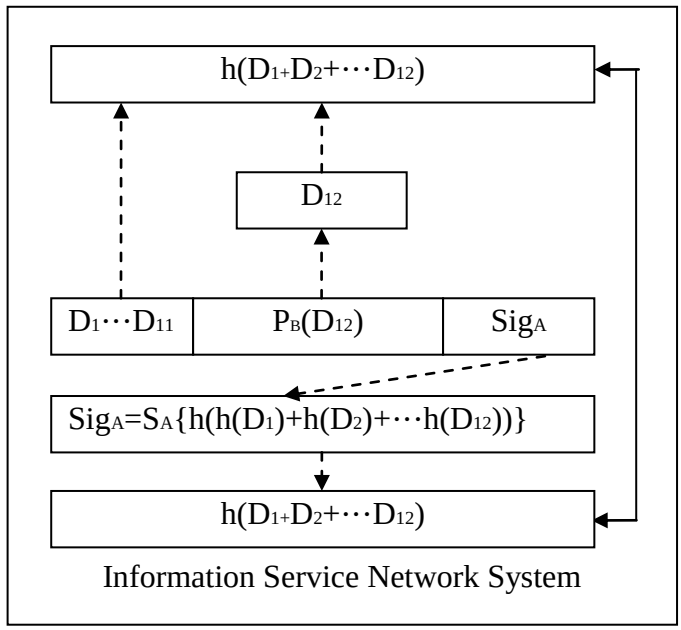

Figure 4. Verification procedure in the Information Service Network System

3.6 Split Digital Signature Scheme

Even if the above problem is resolved, problems such as the following signature problem for the log exist.

The split digital signature scheme means that signatures are generated one at a time from log data. The problem with this method is that we cannot detect the deletion of log data.

In the case that L_2 is removed (see Figure 5), the verifier cannot verify that L_2 had existed because L_1 and L_3 have no discrepancies.

Therefore, if a log of the Information Service Network System can be deleted, a detection method is needed.

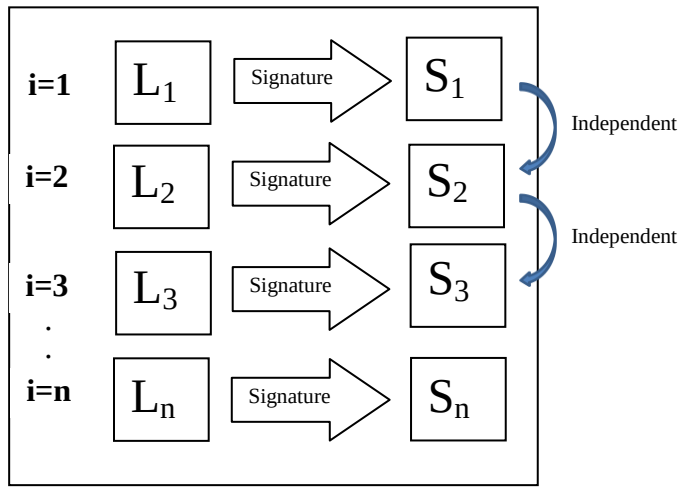

Figure 5. Split digital signature scheme

4. PROPOSED METHOD

4.1 Verification Procedure

The Information Retaining Agency sends the data that can be disclosed without encryption and sends the data that must be concealed after encryption. Before sending these data, the digital signature is calculated for both the disclosed data and the encrypted data. The Information Retaining Agency saves the information and the signature as a log. The Information Retain Agency sends the data that is possible to disclose without encryption and sends the data that is required to be concealed after encryption. Before sending them, the digital signature is calculated for both the disclosed data and the encrypted data.

The Information Retain Agency saves the information and the signature as a log.

4.2 Proposed Method 1

Figure 6 shows the contents of the data that are sent by Information Retaining Agency A. The procedure is as follows:

(a) Information Retaining Agency sends $D_1 \cdots D_{11}$, which includes no personal information, to the Information Service Network System. The value of $D_1 \cdots D_{11}$ can be inspected by the Information Service Network System.

(b) D_{12}, which is not allowed to be viewed by the Information Service Network System, is encrypted by the public key cipher and Agency B's public key P_B. Of course, it is possible to use the method of sending K

which represents the key of common key cipher and encrypted by the public key cipher and the public key P_B of Information Retaining Agency B, in addition to $D_{12,}$ encrypted by a common key cipher and key K.

(c) After calculating the hash values of both data obtained in (a) and (b), a digital signature is generated using a public key cipher and Agency A's private key S_A.

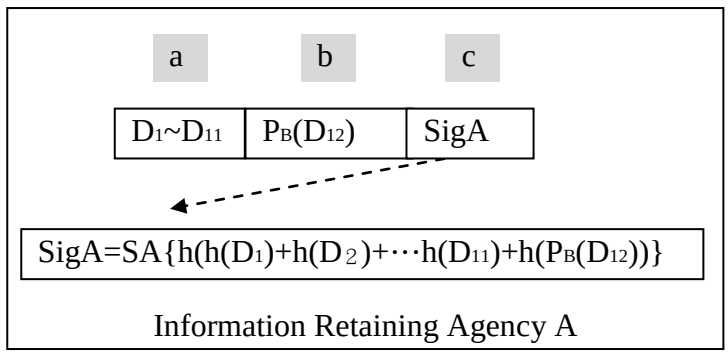

Figure 6. Data contents sent by Information Retaining Agency

4.3 Verification Procedure at the Information Service Network System

The Information Service Network System verifies the validity of the data received from Information Retaining Agency A (see Figure 7) using the following steps:

(d) Compute the hash value from Sig_A using public key P_A of Information Retaining Agency A.

(e) Compute the hash value of $D_1 \cdots D_{11}$ and $P_B(D_{12})$.

(f) Join the hash values of $D_1 \cdots D_{11}$ and $P_B(D_{12})$, and compute the hash value of the result.

(g) Compare the values in (d) and (e). If these values match, the validity of the data is proven.

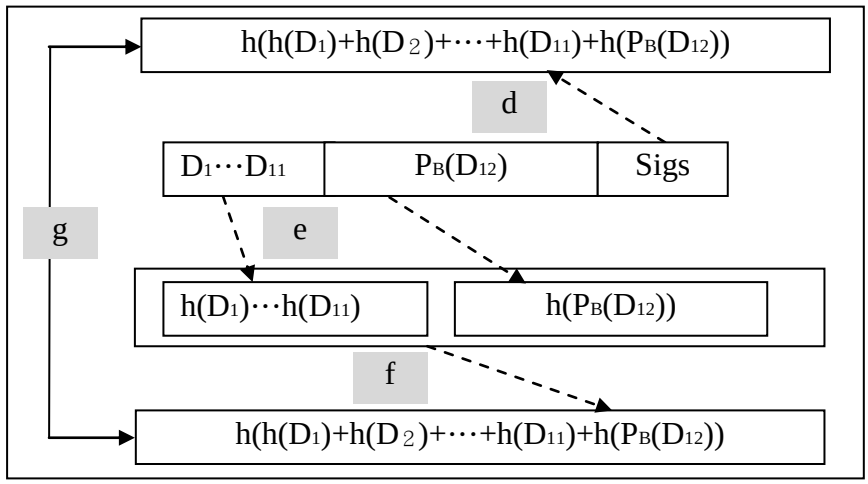

Figure 7. Verification procedure

4.4 Verification by a Third-Party Institution

If unauthorized use of personal information is suspected, the third-party institution conducts an investigation of the Information Service Network System and the Information Retaining Agency (see Figure 8).

Figure 9 shows the verification procedure of the third-party institution.

First, the third-party institution investigates whether someone altered or eliminated the log file. If the log has not been tampered with, the third-party institution examines whether sensitive information has been shared and determines whether the information was shared appropriately.

If the possibility of improper use is high, the third-party institution investigates the Information Service Network System, the agency that provided the information, and the agency that referred the information.

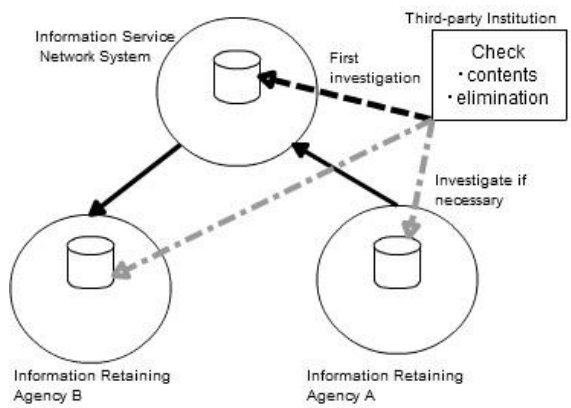

Figure 8. Verification by a third-party institution

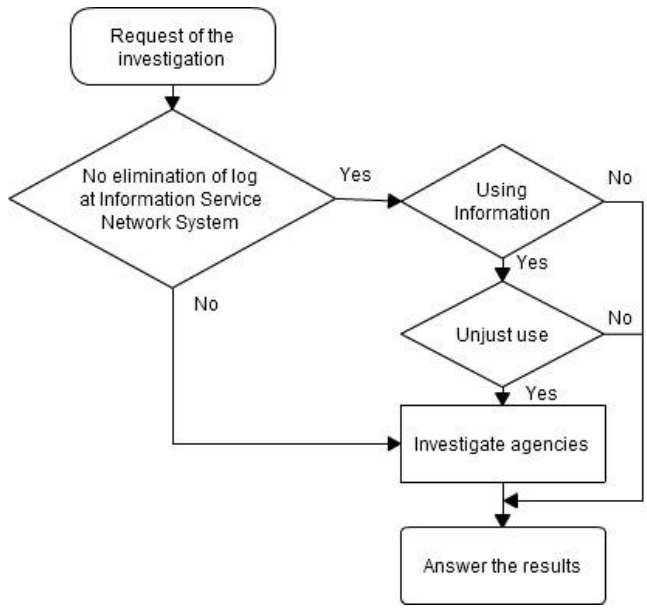

Figure 9. Verification procedure performed by a third-party institution

4.5 Safety

In this method, the verifier cannot detect the elimination of the log.

For example, Information Retaining Agency A sends data to Information Retaining Agency B. Information Retaining Agency B insists that Agency B did not refer it, and the log data of the Information Service Network System is eliminated.

In this case, the verifier cannot determine which claims are correct.

4.6 Proposed Method 2

In order to solve the problem whereby the verifier cannot detect elimination of the log, the Information Service Network System uses a hysteresis signature, which is needed when the third-party institution investigates injustice.

4.7 Hysteresis Signature

The hysteresis signature[11, 12] extended from a digital signature is used here. Figure 10 shows an overview of the proposed scheme using the hysteresis signature. The terms related to the hysteresis signature are indicated in Table 1.

Table1. Terms used in hysteresis signature

L	Log data
Si	Signature of the i-th
Ci	Chain data of the i-th
C_1	Initial value of the chain data

Figure 10 shows the case in which Information Retaining Agency Ai sends data to Information Retaining Agency Bi for the i^{th} log.

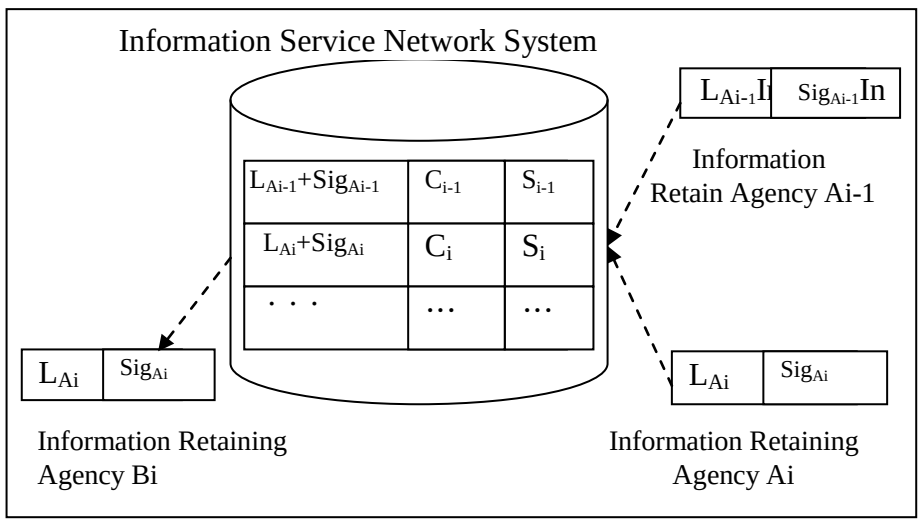

Figure 10. Overview of proposed method 2

The signature generation procedure is as follows:

(1) For the i^{th} log, read log data L_{Ai} and Sig_{Ai}.

(2) Chain data C_{i-1} is set as follows:

(a) If i = 1, then set some constant value to C_{i-1}.

(b) If i is greater than or equal to 2, then read C_{i-1} from the log file.

(3) Join L_{Ai}, Sig_{Ai}, and C_{i-1} and compute the hash value Ci of the joined data (see Figure 11).

(4) Encrypt hash value C_i using the public key cipher and the secret key of the Information Service Network System S_N. Obtain Si as $Si = S_N(C_i)$ (see Figure12)

(5) Save L_{Ai} + sig_{Ai} , C_i, and S_i.

(6) i = i + 1 and go to (1).

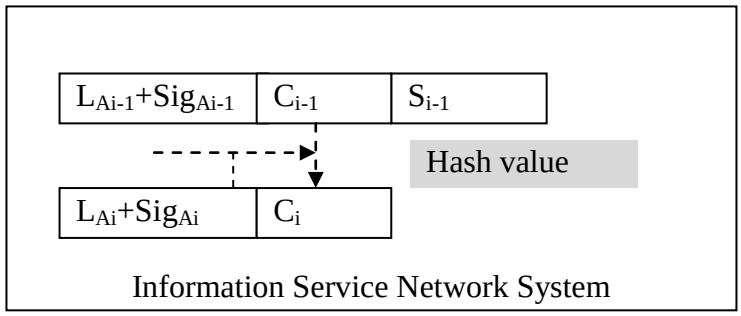

Figure 11. Procedure in hysteresis signature

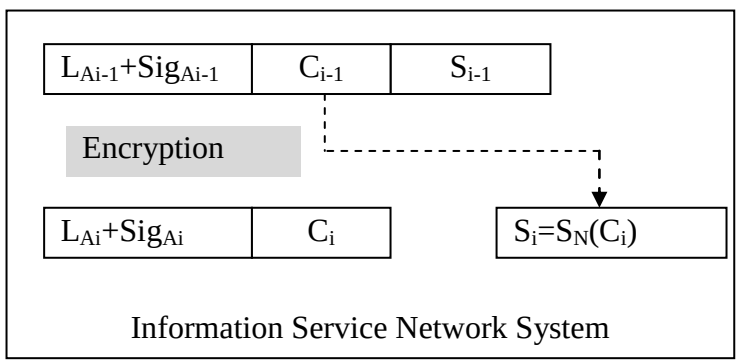

Figure 12. Signature generation in the hysteresis signature scheme

4.8 Verification Procedure

Verification is performed by comparing signature S1 to the latest signature Sn, as follows:

(1) Compute a hash value by decrypting the latest signature value Sn using the public key of the Information Service Network System.

(2) Join log data L_{An}, Sig $_{An}$, and C_{n-1}, and compute the hash value C_i.

(3) Compare the values of (1) and (2). If the values are equal, then no alteration has occurred. Otherwise, alteration has occurred.

(4) n = n - 1

(5) If n is greater than 1, go to (1).

Using this method, it is possible to identify the deletion of logs, because the value of C_{i-1} changes when a log has been deleted.

5. EVALUATON

The evaluated results are summarized in Table 2.

5.1 Encryption Only

If the Information Retaining Agency uses only encryption, the staff of the Information Service Network System cannot view personal information illegally, but the verifier cannot detect the elimination of logs.

5.2 Signature Only

Ordinary signatures can detect an alteration of log data. However, there exists the possibility of unauthorized viewing of sensitive data within the Information Service Network System. In addition, the verifier cannot detect the elimination of logs.

5.3 Proposed Method 1

Personal information is encrypted by a secret key of the Information Retaining Agency. Therefore, the staff of the Information Service Network System cannot view the information without the secret key of the Information Retaining Agency. Acquisition of the secret key is very difficult by individual staff members of the Information Service Network System. On the other hand, this method discloses information that is necessary to validate information sharing and allows verification and concealment.

If a staff member of Information Retaining Agency B has engaged in unauthorized information sharing, the possibility exists of falsification of log data that is held by Information Retaining Agency B. However, the Information Service Network System and Information Retaining Agency A also hold the logs. Therefore, falsification is determined by comparison of log data in Information Retaining Agency B and the Information Service Network System or Information Retaining Agency A. However, the verifier cannot detect the elimination of a signature when the ordinary signature scheme is used. Therefore, the authenticity of the log data becomes unclear when the agency that refers the information insists that the agency does not demand the information.

5.4 Proposed Method 2

In order to solve the problem of method 1, a hysteresis signature is used. The hysteresis signature constructs a chain structure between signatures and enables detection of the elimination of log data[13,14], thereby solving the problem of method 1. The elimination of log data of the Information Retaining Agency is not able to be detected internally because we assume the use of a hysteresis signature only by the Information Service Network System. However, comparison of the log data from the Information Service Network System to the log data of the Information Retaining Agency enables us to prove the elimination.

Moreover, in the case of Figure 10, malicious staff members cannot alter log data without the secret keys of the Information Service Network System, Information Retaining Agency A, and Information Retaining Agency B. In this way, the integrity of electronic data can be improved by a hysteresis signature when multiple agencies are involved.

Table2. Comparison of the proposed schemes

	Only encryption	Only signature	Method1	Method2
Injustice1	○	×	○	○
Injustice2	×	○	○	○
Injustice3	×	×	×	○
Injustice4	×	○	○	○
Injustice5	×	×	×	△
Injustice6	×	○	○	○
Injustice7	×	×	×	△

Note: ○: Effective method, ×: Not effective method, △: Impossible to prevent, Possible to detect

6. CONCLUSIONS

In this paper, we proposed and evaluated an evidence preservation method in order to solve a problem of a common number system.

According to the evaluation results, proposed method 1 enables both confidentiality and verifiability to be maintained, but the verifier cannot detect elimination of log data. On the other hand, proposed method 2, using a hysteresis signature, enables the detection of log data elimination. This scheme can cope with all assumed injustices.

In the future, it will be necessary to increase implementation efficiency and perform an evaluation of data security in more detail.

7. REFERENCES

[1] Cabinet Secretariat of Japan Government, My number, the social security and tax number system. Retrieved on April 17, 2015, from http://www.cas.go.jp/jp/seisaku/bangoseido/.

[2] Technical Working Group for Information Sharing Fundamentals. Report. Retrieved on April 17, 2015, from http://www.cas.go.jp/jp/seisaku/jouhouwg/index.html.

[3] K. Kent, S. Chevalier, T. Grance, and H. Dang, Guide to integrating forensic techniques into incident response. NIST Special Publication, p800-86, 2006. Retrieved on April 17, 2015, from

http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf.

[4] B. Schneier, and J. Kelsey, Secure audit logs to support computer forensics. *ACM Transactions on Information and System Security (TISSEC)*, 2(2), p159-176, 1999. http://dx.doi.org/10.1145/317087.317089.

[5] R. Accorsi, Safe-Keeping digital evidence with secure logging protocols: state of the art and challenges. In O. Goebel, R. Ehlert, S. Frings, D. Guenther, H. Morgenstern, and D. Schadt (Eds.), *Proceedings of the Fifth International Conference on IT Security Incident Management and IT Forensics* (p94-110). Los Alamitos, CA: IEEE Computer Society, 2009. http://dx.doi.org/10.1109/IMF.2009.18.

[6] S. Zhao, K. Chen, and W. Zheng, Secure logging for auditable file system using separate virtual machines. In X. Liao, H. Jin, R. Zheng, and D. Zou (Eds.), *Proceedings of the IEEE International Symposium on Parallel and Distributed Processing with Applications* (p153-160). Los Alamitos, CA: IEEE Computer Society, 2009. http://dx.doi.org/10.1109/ISPA.2009.32.

[7] I. Ray, K. Belyaev, M. Strizhov, D. Mulamba, and M. Rajaram, Secure logging as a service-delegating log management to the cloud. *IEEE Systems Journal*, 7(2), p323-334, 2013. http://dx.doi.org/10.1109/JSYST.2012.2221958.

[8] S. Morinobu, and Y. Kobayashi, *What would happen? What would you do! for Common Number System*. Tokyo: Nikkei Publishing Inc., 2011.

[9] Y. Maeda, and H. Matsuyama, *Nation ID system will save Japan*. Tokyo: Shincho Publishing Inc., 2011.

[10] Office for the Social Security and Tax Number System Minister's Secretariat, Cabinet office and social security reform office, cabinet secretariat, japan, the social security and tax number system, Retrieved on April 17, 2015, from http://www.cas.go.jp/jp/seisaku/bangoseido/pdf/en2.pdf.

[11] S.Susaki, and T. Matsumoto, Alibai establishment for electronic signatures. *Information processing society in Japan*, 43(8), p2381-2393, 2002.

[12] Y. Ueda, R. Sasaki, H. Yoshiura, S. Susaki, and M. Kunihiko, Evaluation method supposing data loss for hysteresis signature systems. *Information processing society in Japan*, 45(8), p1966-1976, 2004.

[13] Y. Ashino, and R. Sasaki, Proposal of digital forensic system using security device and hysteresis signature. In B.-Y. Liao, J.-S. Pan, Lakhmi C. Jain, M. Liao, H. Noda, and Anthony T.S. Ho (Eds.), *Proceedings of the 3rd IEEE Intelligent Information Hiding and Multimedia Signal Processing* (p3-7). Los Alamitos, CA: IEEE Computer Society, 2007. http://dx.doi.org/10.1109/IIH-MSP.2007.249.

[14] S. Tezuka, H. Tomori, R. Uda, and K. Okada, Distributed secure virtual

file system using hysteresis signatures. In I. Awan, M. Younas, T. Hara, and A. Durresi (Eds.), Proceedings of the International Conference on Advanced Information *Networking and Applications* (p90-97). Los Alamitos, CA: IEEE Computer Society, 2009. http://dx.doi.org/10.1109/AINA.2009.113.