Consideration of Privacy Risk Assessment of the My Number in the Financial Industry in Japan

Sanggyu Shin(✉), Yoichi Seto, Kei Sakamoto, and Mayumi Sasaki

Advanced Institute of Industrial Technology, Higashiooi 1-10-40, Shinagawa-ku, Tokyo 140-0011, Japan
{shin,seto.yoichi}@aiit.ac.jp

Abstract. In Sep. 2015, the *Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure* was revised. It was decided to link personal numbers to deposit numbers of financial institutions. Currently, the *Privacy Impact Assessment* which is obliged to implement this law is required to implement safety control measures for the private sector. However, there is no system to conduct a risk assessment of the law. In the financial industry, which is a highly private sector of public nature, some privacy risk assessment is required because it has many individual numbers. In this paper, we propose a framework for privacy risk assessment on this law in the financial industry, using the privacy impact assessment prescribed as an international standard.

Keywords: Specific personal information protection assessment
Social security and tax system · Privacy impact assessment · My Number

1 Introduction

In May 2013, the *Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure* was established. In this law, unique numbers are assigned to individuals and corporations. In September 2015, the revised proposal of *Act on the Protection of Personal Information* and the *Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure* (from now on *My Number Law*) was passed. The revised proposal includes contents that make it possible to link personal numbers to account numbers owned by financial institutions and use them for tax investigation [1]. When building a system for managing personal information in Europe and the United States, a preliminary assessment of leakage risks using *Privacy Impact Assessment* (from now on PIA) is performed to prevent the leakage of personal information. In Japan, implementation of Specific Personal Information Protection Assessment is stipulated for concerned parties such as governmental organizations, in the *My Number Law*. As specified in the *My Number Law*, the finance industry will have many personal numbers. Since the finance industry is a private sector, which is public nature, it is necessary to assess the Specific Personal Information Protection Assessment that conforms to the PIA [2–6].

© Springer Nature Singapore Pte Ltd. 2018
J. J. Park et al. (eds.), *Advances in Computer Science and Ubiquitous Computing*, Lecture Notes in Electrical Engineering 474,
https://doi.org/10.1007/978-981-10-7605-3_43

In this paper, we propose a framework for a privacy risk assessment on this law in the financial industry, using the PIA prescribed as an international standard.

2 Development of *My Number* to Financial Institutions

The revised *My Number Law* expands the range of utilization of personal numbers by the country. The following list is the expanded range of the utilization of personal numbers.

(1) Linking to the personal number to deposit savings account
(2) Expansion of the scope of use in medical and other fields
(3) Enlargement of the scope of application based on the requests of local public entities

In the amendments, the financial institution is affected by the linking of the *My Number* to the deposit savings account mentioned in (1) above. The financial institution needs to manage the searchable state after linking the customer's deposit number and personal number to respond to the above (1)–(3). Regarding compliance with the current *My Number Law*, it is mandatory to take safety control measures according to the *Guidelines on Proper Handling of Specified Personal Information (Business's Guide)* presented by the Specific Personal Information Protection Commission [7].

3 Method of Risk Assessment

Specific personal information protection assessment is said to be equivalent to PIA adopted in other countries such as the United States, Australia, and the United Kingdom. However, there are some significant differences compared to PIA, which we will discuss in the following subsections.

3.1 Current Risk Assessment at Financial Institutions

In the past, countermeasures for customer information protection and management have been implemented at financial institutions based on various guidelines [8, 9]. This section outlines these guidelines.

(1) **Inspection manual for deposit-taking institutions**

This manual describes the wide range of inspection items for financial institutions to serve as a guide. The following items concerning risk management are designed to protect customer information and inspect related systems. Table 1 shows the relationship between the inspection items of the *Inspection Manual for Deposit-Taking Institutions* and the *My Number* correspondence [10, 11].

(2) **FISC safety measures standard**

The *Center for Financial Industry Information Systems* (FISC), a public interest incorporated foundation, mandated this standard, which functions as a practical safety measure standard. This standard is divided into three categories and described [12, 13].

Table 1. Relationship between Inspection Manual for Deposit-Taking Institutions and *My Number Law*

Table of Contents (Headings)	Table of Contents (Subheadings)	Relationship with *My Number Law* correspondence
Business management (Governance)	–	–
Financial facilitation Section	–	–
Risk management Section	Checklist for Legal compliance	–
	Checklist for Customer protection management	Correspondence from the viewpoint of customer information protection
	Checklist for Comprehensive risk management	–
	Checklist for Capital management	–
	Checklist for Credit risk management	–
	Checklist for Asset assessment management	–
	Checklist for Market risk management	–
	Checklist for Liquidity risk management	–
	Checklist for Operational risk management	System risk management system responds

In addition, guidelines concerning the protection of personal information from different agencies such as the *Financial Services Agency* (FSA), are prepared. Based on the *Personal Information Protection Law*, these guidelines describe concrete actions to be taken by financial institutions [14].

3.2 Comparison Between PIA and the Current Risk Assessment

In the PIA, risk assessment is carried out based on the classification according to the OECD's Eight Principles. We compared risk items in current financial institutions with risk items to be evaluated by PIA. We confirmed the adequacy of items subject to risk assessment by this compare.

4 Issues and Countermeasures for the *My Number Law* in Financial Institutions

As indicated in the previous chapter, the existing guidelines have already been tested to the level that satisfies the risk items based on the OECD (Organization for Economic Co-operation and Development).

(1) **Implementation timing**

PIA is a risk management method, which evaluates the influence on privacy in advance in system construction. In another word, a PIA must be carried out before the operation of the system.

(2) **Expertise and neutrality of PIA implementing agencies**

ISO 22307 calls for expertise and neutrality for PIA implementing agencies. However, since financial institutions are private enterprises, they are different from public fields thus perfect neutrality is not required. For this reason, the assessment must be conducted by the development team within the financial institution.

(3) **Inspection by a third-party organization**

Third-party institutions are required to confirm the results of PIA implementation. However, for the same reason as in (2), we implement PIA using an audit department that has no conflicts within the company as an inspection organization.

(4) **Assessment procedure**

In carrying out the evaluation, it is necessary to determine the procedure and flow of assessment. It is appropriate to implement the evaluation using guidelines developed based on ISO 22307.

(5) **Evaluation criteria**

When implementing PIA, the evaluation criteria for correctly conducting evaluation are necessary. For this reason, assessment sheets are prepared as evaluation criteria.

5 Proposal for Implementation of PIA at Financial Institutions

As stated in the previous chapter, it is important that in the PIA implementation, the security assessment currently implemented and the requirements of ISO 22307 are consistent. Figure 1 shows the correspondence between the evaluation criteria and the current security evaluation based on PIA implementation examples in the private sector.

No	中項目	評価項目	対応する現状のセキュリティガイドライン	備考
<1> 目的明確化の原則				
1	利用目的の特定	評価対象システムにて、取得・利用される個人情報の目的は特定されているか。	金融分野における個人情報保護に関するガイドライン　第3条	
2	個人情報の特定	評価対象システムにて、取得しようとする個人情報について、個人情報か否か特定する手続き、手順が定められているか。 また、定期的に現実(法律改訂等)と乖離が発生していないかを確認、改訂する手続き、手順が定められているか。	金融分野における個人情報保護に関するガイドライン　第3条	
3	機微情報	評価対象システムにて、法令に基づく業務以外で以下の特定の機微な個人情報の取得を行っていないか。 a) 思想、信条及び宗教に関する事項。 b) 人種、民族、門地、本籍地、身体・精神障害、犯罪歴、その他社会的差別の原因となる事項。 c) 勤労者の団結権、団体交渉及びその他団体行動の行為に関する事項。 d) 集団示威行為への参加、請願権の行使、及びその他の政治的権利の行使に関する事項。 e) 保健医療(※)及び性生活。 ※感染症、精神疾患に係わる情報、病名、検査結果、受診科、障害度、介護度などの情報。	金融分野における個人情報保護に関するガイドライン　第6条 金融機関等コンピュータシステムの安全対策基準　運53-1	
<2> 利用制限の原則				
4	第三者提供	評価対象システムにて、個人情報を第三者へ提供することを想定しているか。想定している場合、その利用目的が特定されているか。	金融分野における個人情報保護に関するガイドライン　第3条、第13条	
5	目的外利用の同意	評価対象システムにて個人情報の取得・利用目的を超えて利用する場合、本人の同意を得る手続き、手順が定められているか。	金融分野における個人情報保護に関するガイドライン　第5条	

Fig. 1. Correspondence between evaluation criteria and current security evaluation

(1) **Purpose Specification Principle**

This confirms that the personal information handled by the system is as follows.

- Whether procedure to identify is taken
- Confirmation concerning handling of sensitive information
- Is clarification of acquisition purpose made?

(2) **Use Limitation Principle**

This confirms that personal information is used only for the clarified purpose of use.

(3) **Collection Limitation Principle**

This confirms whether we have obtained agreement after notifying or publishing purpose of use when acquiring personal information.

(4) **Data Quality Principle**

This confirms the measures to make the acquired personal data accurate and up to date.

(5) **Security Safeguards Principle**

This is to confirm the measures to keep the security of personal data safe.

(6) **Openness Principle**

This principle states the need to confirm that the formulation of personal information protection policy and declaration from the inside to the outside.

(7) **Individual Participation Principle**

It is necessary to guarantee the right to disclose, correct, and delete collected personal information to the person who provided the personal data.

(8) **Accountability Principle**

Since collected personal information is only a deposit, responsibility occurs based on the principle on the side that got it. The financial industry regulates information disclosure, correction, suspension of use, suspension and provision to third parties under Article 15–17 of the *Guidelines for the Protection of Personal Information in the Financial Sector* [15].

6 Conclusion

By the revised numbering law, the *My Number* was determined to be linked to the financial institution's deposit savings account. Specific personal information protection assessment that is obliged to implement the current numbering law is applicable only to institutions such as local governments. Also, Safety management measures are obligatory for the private sector, but there is no system to conduct the risk assessment on the *My Number Law*. The finance industry is a private field with high public nature and holds many personal numbers. Therefore, it is desirable to conduct a privacy risk assessment that conforms to the evaluation of specific personal information protection implemented by administrative agencies.

Acknowledgments. This research carried out in the Project Based Learning in the Advanced Institute of Industrial Technology. In advancing the PBL, we got the cooperation of Hiro Rokugawa, Yuta Kurosawa, Okimura Seiji, and Xiaofei Ma. We would like to express our appreciation here.

References

1. Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure (Act No. 27 of 31 May 2013). http://www.cas.go.jp/jp/seisaku/bangoseido/pdf/260717bangouhou.pdf
2. A draft of a bill to amend part of the Act on the Protection of Personal Information and the Act on Utilization of Numbers to Identify Specific Individuals in Administrative Procedures (Overview), February 2015. https://www.kantei.go.jp/jp/singi/it2/senmon_bunka/number/dai8/siryou2.pdf
3. Seto, Y.: Practical Privacy Risk Assessment Technique - Privacy by Design and Personal Information Impact Assessment. Kindaikagaku Press, Tokyo (2014)
4. Specific personal information protection assessment guideline, April 2014. http://www.ppc.go.jp/files/pdf/shishin.pdf
5. Mayumi, S., Kei, S., Kazuhiro M., Sanggyu, S., Yoichi, S.: The problem analysis of specific personal information protection assessment. In: CSS 2015, vol. 2015(3), pp. 1199–1206 (2015)

6. Kei, S., Mayumi, S., Sanggyu, S., Yoichi, S.: A Study on the privacy risk assessment of responding to National ID Act in the financial sector. In: 2016 Symposium on Cryptography and Information Security (SCIS 2016) (2016)
7. Guidelines on proper handling of specific personal information in financial services, December 2014. http://www.ppc.go.jp/files/pdf/141211kinyu-guideline.pdf
8. Yoichi, S., Hiroaki, R., Fumio, S., Yasujiro, M., Hiroaki, I.: Privacy Impact Assessment PIA and Personal Information Protection. Chuokeizai Press, Tokyo (2010)
9. Sang-gyu, S., Tomomi, H., Mayumi, S., Yoichi, S.: Analysis of risk items in specific personal information protection assessment. In: The 32th Symposium on Cryptography and Information Security (2015)
10. ISO22307:2008 Financial services – Privacy impact assessment. http://www.iso.org/iso/catalogue_detail.htm?csnumber=40897
11. Satoru, N., Naoko, O., Michiya, O., Haruyki, K., Makoto, S., Yoichi, S.: Development of guidelines for personal information impact assessment. J. Jpn. Soc. Secur. Manage. **29**(1), 3–16 (2015)
12. Explanation of Specific Personal Information Protection Assessment Guidelines, November 2014. http://www.ppc.go.jp/files/pdf/explanation.pdf
13. Inspection Manual for Deposit-Taking Institutions, June 2014. http://www.fsa.go.jp/en/refer/manual/yokin_e/y-all.pdf
14. About financial information system and FISC safety measures standard, December 2014. http://www.fsa.go.jp/singi/singi_kinyu/kessai_sg/siryou/20141208/03.pdf
15. The Guidelines on the Protection of Personal Information, November 2009. http://www.fsa.go.jp/common/law/kj-hogo/01.pdf