

Analysis of Specific Personal Information Protection Assessment in the Social Security and Tax Number System of Local Governments in Japan

Sanggyu Shin, Yoichi Seto, Mayumi Sasaki, Kei Sakamoto

▶ **To cite this version:**

Sanggyu Shin, Yoichi Seto, Mayumi Sasaki, Kei Sakamoto. Analysis of Specific Personal Information Protection Assessment in the Social Security and Tax Number System of Local Governments in Japan. 16th IFIP International Conference on Computer Information Systems and Industrial Management (CISIM), Jun 2017, Bialystok, Poland. pp.685-696, 10.1007/978-3-319-59105-6_59 . hal-01656250

HAL Id: hal-01656250

https://inria.hal.science/hal-01656250

Submitted on 5 Dec 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License

Analysis of Specific Personal Information Protection Assessment in the Social Security and Tax Number System of Local Governments in Japan

Sanggyu Shin [1], Yoichi Seto[1], Mayumi Sasaki[1] and Kei Sakamoto[1]

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

Abstract. A law in Japan has been established concerning the *My number* system or the use of numbers for identifying specific individuals in administrative procedures in local governments. The law requires local governments to implement the specific personal implementation protection assessment for social security and tax number systems. In this paper, we analyzed the assessment reports of the specific personal information protection assessments conducted by local governments. We did the analysis in two directions: (1) adequacy of risk assessment and measures, and (2) reuse of the assessment report. Our analysis shows that there was a description of assessment on the risk assessment items, but there were many assessment reports with missing assessment on some operations.

Keywords: Risk Assessment, Privacy Impact Assessment, Privacy risk, Social Security and Tax Number System, Specific Personal Information Protection Assessment.

1 Introduction

On May 24, 2013, the *Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure*, also known as the *My Number* law, was raised. From this law, the Social Security and Tax Number System or the *My Number* system came in.

The *My Number* system is used to confirm that information on individuals possessed by multiple agencies such as administrative agencies and local governments are information of the same person. This system advocates a fairer and more just society, enhanced public convenience and improved administrative efficiency [1].

From October 2015, the government has enforced the *My Number* law, and notified the residents of their *My Number* numbers. The personal information including *My Number* is called *Specific Personal Information*.

Protection Assessment is done to prevent infringement of privacy of personal information and ensure the trust and protect the rights of citizens and residents [2]. Af-

ter protection assessment, each local government unit must conduct their risk assessment as assessment report [3].

In this paper, we analyzed the report published by the local governments in the following perspectives:

1. Adequacy of risk items, and
2. Re-use of the Assessment report.

In other countries, privacy impact assessment (from now on referred to as PIA) has been carried out to preliminarily assess the influence on privacy when introducing or repairing a system involving the acquisition of personal information, and taking measures to avoid or mitigate privacy risk [4].

In the PIA, there are two studies on the validity of impact assessment: one is the assessment of the suitability of the PIA applied to the biometrics system. The other is a study evaluating the effectiveness of the PIA itself.

Officials in charge of the administrative organization self-evaluate the *Specific Personal Information Protection Assessment* about the system and operation. On the other hand, the *PIA* does not include the operation, but only the system is assessed by a specialized neutral third party. The government has published protection assessment as equivalent to PIA, but as stated above, PIA and protection assessment are fundamentally different.

This paper analyzes and assesses whether the *Specific Personal Information Protection Assessment* prescribed by the *My Number* law is properly implemented by local governments based on the assessment report issued by the local governments.

2 Related Works

There are two similar researches on the appropriateness of risk assessment in conjunction with PIA. Protection assessment concerning specific personal information was implemented in 2015, and no case study on the protection assessment was found. The protection assessment is conducted only in Japan, while the PIA is an assessment method that has international standards and is implemented in other countries. In the PIA, there are two cases of research on the appropriateness.

First, Kush Wadhwa et al. applied PIA to biometric systems then assessed the appropriateness of the procedures for PIA by ranking [5]. They assumed that the PIA method is useful and evaluated its adequacy as to whether the implementation procedure is appropriate for the case of PIA. For example, their work assessed whether the report release procedure is appropriate or not. The other related work is a case study where Sakamoto et al. conducted the effectiveness assessment of PIA itself [6]. They assessed the effect of how much privacy risk could be reduced by implementing PIA using the risk assessment method developed based on the international standard ISO 22307. In other words, the effectiveness of PIA is quantitatively assessed from two viewpoints: visualization of privacy risk on personal information and improvement of awareness of stakeholders concerning personal information protection.

The protection assessment to be implemented in Japan is stipulated by the guidelines so that risk assessment is carried out in a mixture of system and operation by self-evaluation of officials in charge of the administrative organizations who have used the system [4][7]. Due to these reasons, the two assessment methods are completely different, and it's hard to apply the assessment method implemented in the PIA to the *Specific Personal Information Protection Assessment*.

In our work, we evaluate whether the assessment is done properly by analyzing the assessment report which is the result of the protection assessment of the specific personal information.

3 Specific Personal Information Protection Assessment

3.1 Outline of Specific Personal Information Protection Assessment

In the case of the *My Number* system, it was imperative to implement the protective assessment as one of the protective measures against the task of handling specific personal information [1]. Fig. 1 shows an overview of protective assessment.

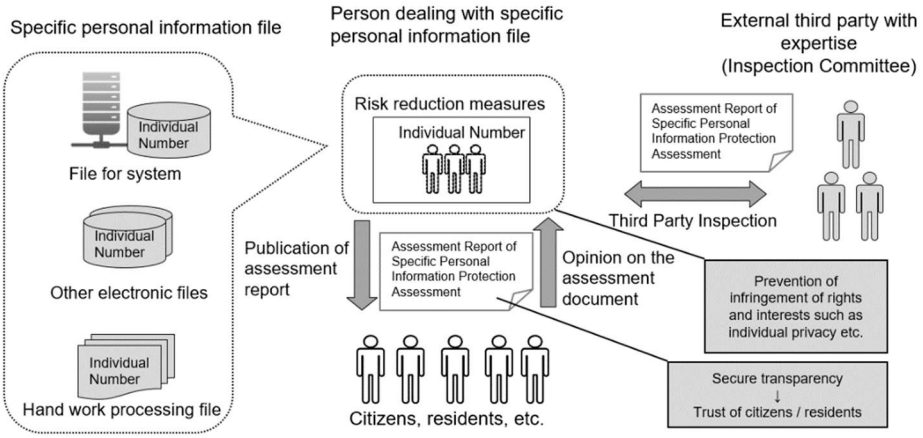


Fig. 1. Overview of Specific Personal Information Protection Assessment

Protection assessment for specific personal information aims to prevent the leakage of specific personal information and other accidents beforehand by ensuring proper handling of specific personal information files such as the *My Number* number, to prevent and protect rights and interests of residents. That is the basic idea of the protection assessment. Its purpose lies in the following.

1. Preventing infringement of rights and interests such as personal privacy by prior response, and
2. Ensuring the confidence of citizens and residents through appropriate disclosure of information.

3.2 Procedure of the Specific Personal Information Protection Assessment

In the protection assessment, it is obligatory to carry out either essential item assessment, priority item assessment, or all item assessment by threshold judgment.

Indicators of threshold judgments include the number of people to be handled, the number of persons dealing with specific personal information files (from now on referred to as the number of handlers), and the occurrence or not of a serious accident concerning specific personal information at the assessment executing agency.

For example, if the target number of people is 300,000 or more, all items are assessed. For more than 100,000 or more are less than 300,000 people, priority item assessment is required. For less than 100,000 people, only the essential item assessment is obliged.

If the number of handlers is 500 or more or a serious accident related to protection of specific personal information has occurred within the past year, it switches from priority item assessment to all item assessment, and essential item assessment to priority item assessment. However, if the target number of people is less than 1,000, implementation of protection assessment is not obligatory.

After the all item assessment report is prepared by the local government, it is necessary to publicize the assessment report, request the opinion of the residents, and do an appropriate review of the assessment report after fully considering the obtained opinion. After consideration of the assessment report, they are submitted to the *Personal Information Protection Committee* after undergoing a third party inspection. Table 1 shows an example of the assessment items of all item assessment report [8].

Table 1. Examples of assessment items of all item assessment report

III Risk measures in the handling process of specific personal information file

1. Name of specific personal information file	
①	
2. Acquisition of specific personal information (excluding acquisition through information provision network system)	
Risk 1: Risk of obtaining non-purpose acquisition	
The content of measures to prevent the acquisition of information other than the target peoples	②
The content of measures to prevent obtaining non-necessary information	③
Contents of other measures	④
Is the measure of risk sufficient?	[⑤] <Option> 1) Putting particular emphasis 2) Enough 3) Issues remain
Hereinafter omitted	Hereinafter omitted

The method of describing the assessment report includes the method of writing an outline in the blanks shown in ① to ④ in Table 1 and the selection description method shown in ⑤. For example, in ②, actions that correspond systematically such as "restrict accessible terminals" and measure concerning operation (human / organizational) such as "to verify identification based on notification/application details or identification documents" are described. In other words, it is necessary to assess both system and operation for every item and describe each measure without omissions. In the selection description, chooses one from options such as 1) Putting particular emphasis, 2) Enough, and 3) Issues remain, etc. In the case of PIA, risk assessment targets are not administrative (operations) but systems. The privacy commissioner issued the standard guideline and risk assessment carries out the assessment based on this guidance. Also, risk assessment is not classified by the number of personal information handled [4].

3.3 Issues of specific personal information protection assessment

Although protection evaluation is said to be equivalent to PIA adopted in other countries, there are the following differences when compared with PIA.

1. The assessment object is "clerical work handling specific personal information file," the definition of administrative tasks is unclear, and the system and operation related to the target functions (organizational and human) are mixed.
2. While PIA is evaluated by a third-party organization with neutrality and expertise, protection evaluation is a self-assessment by the system operator (officials such as administrative agencies) and self-declaration by the chief, etc.
3. Risk assessment manual etc. for protection evaluation still has not been sorted out. Therefore, administrative agencies are preparing assessment reports by individual risk analysis methods.

As described above, there is a possibility that the risk assessment is not properly implemented in the protection assessment on specific personal information. Therefore, using all the item assessment reports released by the local governments, we analyze whether the risk assessment is properly implemented from the two following viewpoints.

1. Adequacy of risk assessment and measures: assess the excess and deficiency of assessment standard and safety control measures created separately for system and operation.
2. Reuse of the assessment report: We analyze the assessment report published by the local governments and assess the situation on reuse.

4 Analysis of all item assessment report

4.1 Analysis method

As described in Section 3.3, protection assessment and PIA have different targets and procedures. For this reason, we analyzed whether protection assessment deals with the protection of specific personal information in the My Number system based on the two following points.

Adequacy of risk assessment and measures.
In the protection assessment, for example, each local government implements measures of risk countermeasure against the risk items described in the all item assessment report. However, there is a possibility that risk assessment and safety control measures will not be considered sufficiently in the protection evaluation. From this issue, three issues 1 to 3 are conceivable.

1. For risk countermeasures, since risks (threats and vulnerabilities) are different in the system and operation, they should be evaluated and described separately, but many local governments expressed mixed opinions about systems and operational risk mitigation measures.
2. The basis for the content of the description for the risk item is unclear. Although the risk item shown in Table 1 is presented from the central government, there is no explanation about its basis.
3. Risk items in the assessment reports are uniform entries and the specific level when the local governments consider the risk countermeasure is not indicated. For that reason, it is conceivable that local governments differ in the way of grasping risks and the level of description. There are issues such as whether adequacy judgment is carried out is subjective, such as “adequate measures” for risks in situations where countermeasure standards are not presented. As a result, the local governments that assess can select “Enough” etc. depending on their personal opinions.

Reuse of assessment reports.
Reuse of the assessment report has two viewpoints. One is to reuse assessment reports of other local governments that precede the same affairs, or samples provided by the central government. The second one is to reuse the content of the assessment report of the administrative office that was previously assessed in the same local government in the assessment of another office work.

4.2 Selection of analysis targets

As described in Section 3.2, the protection assessment is classified into three assessments based on threshold judgment, essential item assessment, priority item assessment, and all item assessment.

In this paper, we focused the assessment report of all items. Many officials deal with a lot of specific personal information in the all items assessment. Therefore, the risk of leakage of specific personal information and other accidents is high thus more detailed and accurate risk measures are required.

As of June 2015, 221 assessment reports of all items have been released by the *Personal Information Protection Committee*. We investigated 10 cases of all item assessment reports.

Selection criteria for the all item assessment report to be investigated are as follows.

1. Official assessment report released by the Personal Information Protection Committee.
2. Assessment report for the same affairs, that is, "affairs concerning the basic resident register."
3. Selection from local governments in various parts of Japan that do not depend on locality: 9 assessment reports corresponding to approximately 10% of all item assessment documents (80 cases).
4. Select the description procedure that is presented from the central government as a criterion to compare with all the item assessment reports of the local government.

Table 2 shows the basic data of the local governments that were selected as assessment targets [9].

Table 2. Basic data of local governments

Unit (people)

Local government	Basic Data		Assessment description contents	
	Number of Inhabitants	Number of Staff	Number of people handled specific personal information	Number of handled specific personal information
A city	967,679	7,260	Over 300,000	500+
B city	355,467	5,495	Over 300,000	Less than 500
C city	446,286	3,198	Over 300,000	Less than 500
D district	879,658	5,057	Over 300,000	Less than 500
E city	1,946,540	14,360	Over 300,000	Less than 500
F city	182,843	994	Over 100,000 Below 300,000	500+
G city	1,536,499	14,701	Over 300,000	500+
H city	323,240	2,332	Over 300,000	Less than 500
I district	710,970	4,313	Over 300,000	500+

5 Assessment analysis of all items assessment report

5.1 Adequacy of risk assessment and measures

In the protection assessment, there is no procedural manual on risk assessment, so the assessment is left to the administrative agencies and local governments. Also, the skill level of the person in charge who performs the assessment is not stipulated. In this section, we analyze whether each local government described appropriate risk response for risk assessment.

The evaluation criteria were prepared according to the safety measure standards shown in the *(Separate) Safety Management Measures for Specific Personal Information (Operator's Guide)*. We prepared assessment criteria by classifying risk correspondence to be implemented for each risk item into systematic correspondence and human organizational correspondence [10].

We analyzed to compare each risk items which are assessment criteria classified into system-related measures and measures concerning the operation of the "*III Risk measures in the handling process of specific personal information*" about the basic resident register file with all item assessment reports to be analyzed which published by local governments. Fig. 2 show the example of the comparative assessment.

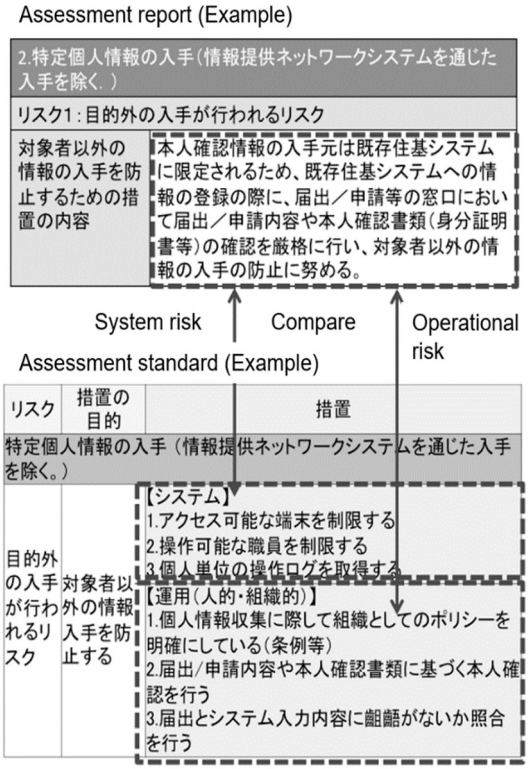


Fig. 2. Comparison of all item assessment report and assessment standard

The result of the comparison is indexed in Table 3 to confirm the excess or deficiency for each corresponding risk item. We roughly distinguished that the assessment index of risk to three stages (Table 3) because it is hard to fix the index based on a logical basis. This assessment index was decided based on a discussion with the expert on PIA.

Table 4 shows the distribution and the assessment value of the assessment index concerning the risk correspondence on the system in each local government. The assessment value is calculated by adding the value of multiplying risk number by the assessment index and dividing by the number obtained by subtracting the number of items not subject to evaluation from the total number of items (49).

Table 3. The category of assessment of the risk response.

Assessment results	Assessment index
The risk correspondence indicated by the evaluation standard is being satisfied. Furthermore, the risk described corresponding to the evaluation criteria is supported.	3
The only parts of the risk management that are shown in the assessment criteria are described.	2
The risk correspondence indicated by the assessment standard isn't mentioned.	1
Risk correspondence isn't indicated in the assessment standard.	- (Excluded from assessment)

Table 4. The situation of corresponding to the risk (System).

All 49 items	System				Assessment index (Average of all item)
	3	2	1	0	
A city	7	12	5	25	2.08
B city	11	10	5	23	2.23
C city	7	12	6	24	2.04
D district	11	8	8	22	2.11
E city	9	13	3	24	2.24
F city	10	13	1	25	2.38
G city	11	12	1	25	2.42
H city	5	16	3	25	2.08
I district	24	0	0	25	3.00

For example, in the case of City A, it is calculated as follows.

$$\text{Assessment value} = (3\times7+2\times12+1\times5) \div (49-25) = 2.08$$

The assessment index when not mentioning the risk correspondence indicated by the assessment standard at all is 1 point. Also, since the assessment index when only a part of the risk correspondence is indicated in the assessment criteria is described is 2 points. When the average value of the assessment index is 2 points or less, there is a possibility that proper risk response could not be made. The fact that the average value of the assessment index is 2 points or less means that many risk items did not cope with the risk indicated by the assessment criteria.

Table 5 shows the distribution and the assessment value of the assessment index concerning the risk correspondence on the operation in each local government. As for the operation, the assessment index is lower as a whole compared to the system. This is because local governments do not mention countermeasures concerning operations. They only describe the risk correspondence concerning the system in risk countermeasures.

Table 5. The situation of corresponding to the risk (Operation).

All 49 items	Operation				Assessment index (Average of all item)
	3	2	1	0	
A city	11	17	7	14	2.11
B city	12	21	2	14	2.29
C city	9	16	11	13	1.94
D district	12	12	12	13	2.00
E city	8	17	11	13	1.92
F city	12	14	10	13	2.06
G city	8	16	12	13	1.89
H city	11	13	12	13	1.97
I district	36	0	0	13	3.00

5.2 Reuse of assessment reports

Many descriptions of all items assessed by local governments are similar to the *Procedure for Specific Personal Information Protection Evaluation Procedure (draft) on affairs related to basic residential ledger* (from now on referred to as the Procedure) exemplified by the Ministry of Internal Affairs and Communications [11][12].

In other words, there is a possibility that the all item assessment report announced previously was reused by simply copying and pasting. In the case of preparing the all items evaluation document by reuse, it may be considered that the examination of risk assessment is inappropriate and it is possible that the existing reason of the system

itself will be gone. We analyzed the identity confirmation information file of all items assessment report selected in section 4.2. We compared the corresponding items in the description procedure and its similarities concerning the "*III Risk measures in the handling process of specific personal information*."

Specifically, we count the number of characters for which the *Description* of the assessment report and the statement of description are identical and then calculate the ratio. The higher the reuse rate, the higher the likelihood of reuse. Table 6 shows the reuse rate by the local governments.

Table 6. Local government reuse rate.

	A city	B city	C city	D district	E city	F city	G city	H city	I district	Average
Reuse rate	52.1	64.4	38.5	75.9	44.0	47.2	55.6	43.5	32.7	50.5

All item assessment report in which the reuse rate exceeded 50% is 44% (4 out of 9: A/B/C City and D District). All item assessment report in which mistook the incorrect legal number is 89% (8 out of 9: local governments excluding B City). All item assessment report in which misprinted typographical errors similarly is 67% (6 out of 9: A/B/C/G City and D/I District).

For reasons that the reuse rate for each local government exceeds 50%, there may be uniformity in the description format of all item assessment reports. Thus, the description contents are similar. Therefore, it can't be said that there is a problem in reuse and it can be said that it is effective means to reuse to improve efficiency. However, it is important that proper risk assessment and countermeasures are implemented, and confirming this is the responsibility of third party inspection. If the inspection committee (or the personal information council) functions properly, it can be confirmed whether or not there is a problem with reuse.

6 Conclusion

In this paper, we analyzed from the viewpoint of all items assessment report the specific personal information protection assessment system for all item assessment. As a result of the analysis, the following problems were found out.

1. Since risk assessment guidelines do not exist, cases were found where appropriate risk assessment was not conducted for each local government.
2. Because the legal status of third-party inspection is unclear, there are local governments whose third-party inspections are not functioning effectively.

To deal with these problems, it is necessary to consider countermeasures from both the improvement in the current system and the review of the institutional design. Improvement measures in the current system are to prepare guidelines for common evaluation of local governments [13]. By conducting assessment and inspection according

to the guidelines, we believe that appropriate correspondence without missing will be possible, and variations in responses among local governments will be improved. Also, the load on the evaluator can be reduced.

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 Kazuhiro Midorikawa, 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 Administrative Procedures (2013)
   http://law.e-gov.go.jp/htmldata/H25/H25HO027.html, last accessed 2017/3/17.
2. The Specific personal information protection committee.: Description of the specific personal information protection evaluation guidelines (2014)
   http://www.ppc.go.jp/files/pdf/explanation.pdf, last accessed 2017/3/17.
3. Takashi, M.: Improper specific personal information protection evaluation shakes “My number” system. NikKei Computer 2015.5.14, pp. 6–10 (2015).
4. Yoichi, S.: Practical Privacy Risk Assessment Technique. pp. 21–24, Kindaikagaku, Tokyo (2014).
5. Kush Wadhwa: SAPIENT project supporting fundamental rights, privacy and ethics in smart surveillance technologies, Biometrics (2011).
6. Sakamoto, M., Yoichi, S.,Okazakim M, Okamoto, N., Kawaguchi H, Nagano, S.: Assessment of effectiveness of personal information impact assessment. Journal of Digital Practices, vol.7, no.1, pp.52–60 (2016).
7. Supervised by Yoichi S.: Specific personal information protection practice guidelines for local governments. Gyosei, pp.38–156 (2015).
8. Cabinet Secretariat, Specific personal information protection evaluation guidelines (draft Cabinet Secretariat), Attached document 3: All items evaluation sheet (Dec. 2013)
   http://www.cas.go.jp/jp/seisaku/bangoseido/kojinjoho/pdf/tkjhh-3.xls
9. From demographics by each local government (Web site of each local government as of June 2015)
10. Personal Information Protection Commission, Guidelines on proper handling of specific personal information (Operator's edition)
    http://www.ppc.go.jp/files/pdf/160101_guideline_jigyousya.pdf, last accessed 2017/3/17.
11. Personal Information Protection Commission, My number protection assessment Web, http://www.ppc.go.jp/mynumber/evaluationSearch/, last accessed 2017/3/17.
12. Personal Information Protection Commission, Proposed guidelines for prescribing specific personal information protection assessment on affairs related to basic resident register (draft), http://www.ppc.go.jp/files/pdf/260624siryo1.pdf, last accessed 2017/3/17.
13. Advanced Institute of Industrial Technology: Related manual of Specific Personal Information Protection Assessment. (2015)
    http://aiit.ac.jp/master_program/isa/professor/y_seto.html, last accessed 2017/3/17.