NRI

Iakyara vol.215

Information security safeguards required for new ID number system - Recent revisions to guidelines for protection of personal information -

Jun Tsutsumi

11. May. 2015

Nomura Research Institute, Ltd.

Jun Tsutsumi
General Manager
Financial IT Risk Management Department

Executive Summary

Japan's forthcoming national ID number system will require companies that handle identifying personal information (information that can identify a specific individual) to upgrade their information security beyond existing confidential information controls. This report provides an overview of recent revisions to various guidelines for protection of identifying personal information and discusses requirements for high-level safeguards.

Required safeguards

The time has come for financial institutions and nonfinancial companies in Japan to prepare posthaste for the January 2016 advent of national ID numbers pursuant to the Act on the Use of Numbers to Identify Specific Individuals in Administrative Procedures (the so-called My Number Act).

In December 2014, the Cabinet Office's Specific Personal Information Protection Commission issued Guidelines for Proper Handling of Specific Personal Information for businesses (the Personal Information Protection Guidelines). The Guidelines contain specific guidance for financial institutions and non-financial companies on how to properly handle identifying personal information.

On their first page, the Personal Information Protection Guidelines warn that noncompliance with any of their mandatory provisions may be deemed a legal violation. Failure to comply with their advisory provisions, by contrast, would not immediately constitute a legal violation, but the guidelines recommend that companies comply with their advisory provisions in accord with the My Number Act's intent to the extent feasible given the companies' size and resources.

One specific guideline states that businesses that use the national ID numbers must devise appropriate safeguards necessary to manage identifying personal information, including safeguards against leakage, loss and impairment of ID numbers and/or identifying personal information. The guidelines' appendix includes numerous pages of content on such safeguards.

Specifically, the Personal Information Protection Guidelines recommend formulating a basic information security policy and regulations for handling identifying personal information. They specify four types of safeguards: organizational, human, physical and technological, as discussed below (see Exhibit).

The guidelines provide specific examples of recommended safeguards. For example, recommended human safeguards include inclusion of confidentiality rules in employment regulations. Examples of physical safeguards for controlling access to areas where identifying personal information is handled include segregation of such areas with walls or partitions and installation of admittance control systems using technologies such as smart cards or numeric keypads. Recommended safeguards to prevent theft of IT hardware or electronic media include fastening IT hardware with security cables if a company's information system that stores identifying personal information files comprises hardware only. Examples of technological safeguards to prevent information leaks include encryption of communication channels, and protection of data via encryption or passwords.

In sum, the Personal Information Protection Guidelines are very instructive on the topic of specific safeguards.

Guidelines for financial institutions

December 2014, the Ministry of Economy, Trade and Industry (METI) revised its Guidelines Targeting Economic and Industrial Sectors Pertaining to the Act on Protection of Personal Information. In response, the Financial Services Agency (FSA) is expected to likewise issue new guidelines on protection of personal information. With the Consumer Affairs Agency advocating standardization of personal information protection guidelines, the FSA's revised guidelines are likely to coincide to some extent with METI's in terms of content.

Exhibit: Four types of safeguards recommended in the Personal Information Protection Guidelines

Organizational safeguards	Formation of information security team, compliance with internal information handling regulations, adoption of procedures for monitoring information handling, formation of incident (e.g., information leak) response team, and assessment of handling of personal information and review/revision of safeguards
Human safeguards	Training and supervision of personnel who handle identifying personal information
Physical safeguards	Control of access to areas in which identifying personal information is handled, prevention of theft of IT hardware and electronic media, prevention of leaks via portable electronic media, deletion of personal ID numbers, and proper disposal of disused IT hardware and electronic media
Technological safeguards	Access controls, identification and authentication of persons who access identifying personal information, prevention of improper access by outsiders, and prevention of information leaks

Like the Personal Information Protection Guidelines, METI's guidelines present examples of four types of safeguards (organizational, human, physical and technological). While the four categories are the same in both sets of guidelines, METI's examples include responses to actual security breaches. These historical examples are more detailed than other examples.

For example, METI's guidelines recommend that information terminals able to access and process identifying personal data be equipped with the minimum functionality required to perform their assigned tasks (e.g., terminals on which users can only view personal data should not be connectable to external recording media such as CD-R or USB storage and their connectivity to memory-equipped devices such as smartphones and PCs should be restricted). METI's guidelines provide considerable detail on previous security breaches, including even the specific type of device (e.g., smartphone) used to perpetrate the breach.

Given the aforementioned similarities between METI's guidelines and the Personal Information Protection Guidelines, companies would be well advised to refer to the examples in both when devising internal safeguards.

However, the two sets of guidelines differ substantially in certain respects. For example, METI's guidelines recommend explicitly appointing a chief information security officer in charge of handling personal information, whereas the Personal Information Protection Guidelines recommend that all personnel who handle identifying personal information be individually identified and supervised. The latter recommendation reflects that in the event of a leak of identifying personal information, companies must be able to thoroughly investigate the leak's cause or source.

In January 2015, the Center for Financial Information Systems (FISC) issued a draft revision of its FISC Security Guidelines on Computer Systems for Banking and Related Financial Institutions (FISC Security Guidelines). In February 2015, the FSA released draft revisions of its Comprehensive Guidelines for Supervision of Major Banks and Financial Inspection Manual's respective provisions on information systems. Both the FISC and FSA revisions are updates that reflect responses to recent security breaches, international developments with respect to cybercrime, and new technological and contractual modalities related to cloud services. Both also seek to broaden the PDCA (plan-do-check-adjust) cycle to encompass not only employees but also external contractors (including subcontractors and sub-subcontractors).

The various guideline revisions discussed above reflect a need to overhaul precautions against information leaks in conjunction with the upcoming advent of national ID numbers.

Protection of identifying personal information and supervision of external contractors

The safeguards required of business processes that involve identifying personal information apply without distinction to not only in-house but also outsourced business processes. Companies therefore must treat external contractors the same as internal organizational units. They must delegate responsibility for outsourced business processes to external contractors and ensure that the contractors implement adequate safeguards. They must also monitor the contractors.

If we compare supervision of external contractors with directors' management of internal organizational units, entering into a service level agreement (SLA) with an external contractor corresponds to explicitly allocating responsibility for business operations among internal organizational units. SLAs must incorporate information-security safeguards. Additionally, companies must verify whether safeguards designed and implemented by external contractors are adequate in light of relevant risks. Companies will consequently require external contractors to conduct internal audits just as they require their internal organizational units to conduct self-inspections. Their SLAs therefore should include a clause authorizing the outsourcer's internal audit department to conduct such internal audits.

In sum, in supervising external contractors, companies must ascertain the adequacy of contractors' information security safeguards in comparison to their own internal safeguards, utilize their assessments of contractors' safeguards as an input in contractor selection decisions, draft agreements that obligate contractors to comply with their policies, and monitor contractors on an ongoing basis after the outsourcing relationship has commenced.

In addition to the Personal Information Protection Guidelines, the Specific Personal Information Protection Commission has also issued an equivalent set of guidelines specifically for financial businesses. These guidelines stipulate safeguards required when financial institutions outsource business processes as well as restrictions on financial institutions' use and provision of identifying personal information.

In terms of specific safeguards, the guidelines instruct financial institutions to refer to the Personal Information Protection Guidelines and also require financial institutions to supervise external contractors. They define necessary and appropriate supervision as contractor selection, execution of an SLA and monitoring of the contractor's handling of personal information as discussed above. Additionally, the guidelines permit subcontracting (including sub-subcontracting) only if the outsourcing financial institution has consented to the arrangement. Financial institutions must be fully aware of the extent to which subcontractors are utilized by the external contractors to which they outsource business processes that involve handling of identifying personal information.

Protection of personal information requires an ongoing, cross-organizational security regime

While the Personal Information Protection Guidelines and METI's guidelines provide many easy-to-understand examples of safeguards, companies relying solely on these guidelines may be susceptible to the misconception that all they need to do is comply with these guidelines' safeguard recommendations. The guidelines' examples are easy to understand because they present specific measures based on recent incidents. However, the examples are merely responses to past incidents. Guidelines are generally unable to present examples of safeguards targeted at anticipated new risks.

Additionally, in terms of information security from the standpoint of maintaining confidentiality, integrity and availability in accord with JIS, ISO or other standards, both the Personal Information Protection Guidelines and METI's guidelines pertain mainly to confidentiality, reflecting their retrospective focus. In the event that some party is harmed in the future by integrity problems (e.g., erroneous records of individuals' national ID numbers), integrity-related incidents would likely be added to the guidelines' safeguards.

Risk management

Companies must keep two key points in mind regarding risk management in connection with national ID numbers. First, risk management is an essential tool for management to fulfill its functions. This point is true across the entire spectrum of risk management, not just for protection of identifying personal information. Second, it is management's responsibility to build a continuously functioning risk management

regime. Specifically, companies should incorporate the following PDCA-cycle arrangements into their risk management models.

(1) Arrangements for collecting information on "close call" incidents within the company and at other companies
(2) Arrangements for analyzing the collected information
(3) Arrangements for devising internal safeguards in response to the results of the analysis
(4) Arrangements for notifying all concerned personnel about new safeguards
(5) Arrangements for monitoring the safeguards to verify whether they have been robustly implemented

Management must explain to stakeholders that such a risk-management PDCA cycle is functioning properly. Accountability therefore must be built into the risk management regime described above.

The crucial question for management is not whether the company's safeguards for protection of identifying personal information are adequate but whether the company has arrangements in place to maintain the adequacy of such safeguards. Additionally, when companies outsource business processes, it is important for management to select a contractor that is capable of monitoring the outsourcer's controls and accessible for direct discussions.

about NRI

Nomura Research Institute, Ltd. ("NRI", TYO: 4307) is an independent, global IT solutions and consulting services provider with annual sales of 406.0 billion yen as of FY ended March 2015. With front-to-back support for the buy- and sell-side, NRI's tradition of innovation has positioned them as a trusted international market leader. Leveraging NRI's global consulting business, NRI is able to provide innovative financial IT solutions for investment banks, asset managers, banks and insurance providers. For more information, visit www.nri.com.

Inquiries to : Financial IT Marketing Department
Nomura Research Institute, Ltd.
Marunouchi Kitaguchi Bldg.
1-6-5 Marunouchi, Chiyoda-ku, Tokyo 100-0005, Japan
E-mail : kyara@nri.co.jp

http://www.nri.com/global/opinion/lakyara/index