

SAI Japan's audit results on "Strengthening information security measures of local governments by the Government"

By OSAKA Ichiro, SAI Japan

[Abstract]

In 2015, Japan Pension Service was faced with massive data leakage exposing 1.25 million cases of contributors or beneficiaries caused by a series of targeted attacks. In the aftermath, people's concern spread over the security of upcoming Social Security and Tax Number System. The Government urged local governments to upgrade security levels of computer systems so that people's "My Numbers" (social security numbers) are secure. Subsidies were broadly distributed to prefectures and municipalities.

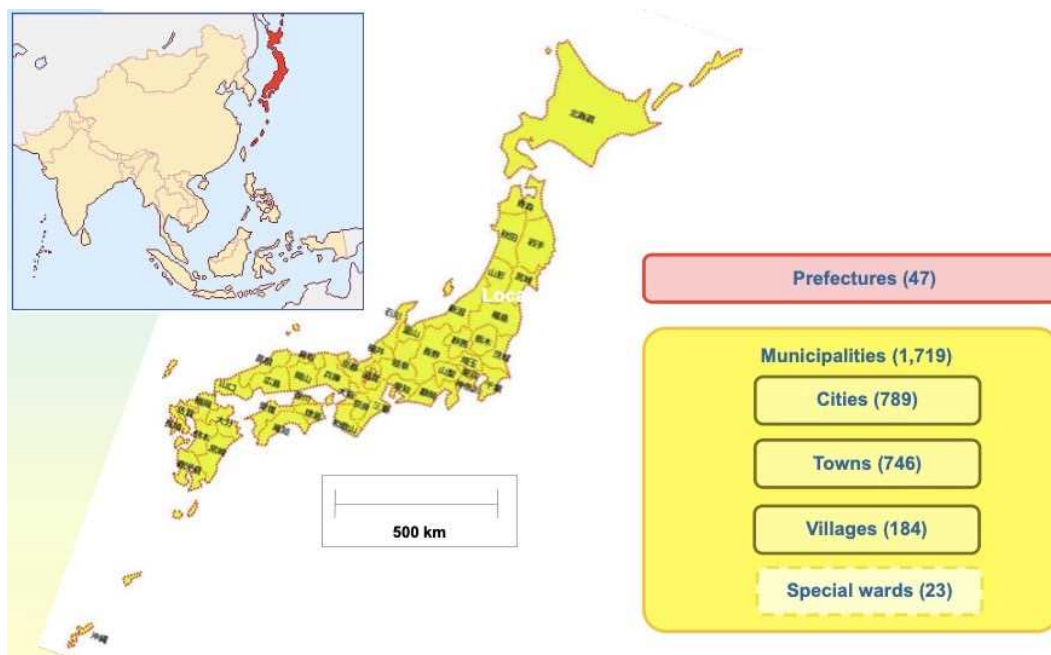
SAI Japan audited prefectures and municipalities to examine if the security levels were enhanced effectively by the subsidies, and submitted the report to the Diet and the Cabinet in January 2020. This paper will give a briefing on the findings of the audit report which are composed of 1) if two-factor authentication system and restriction on take-out of information work well; 2) if My Numbers are securely handled in a separated system; 3) if the common gateway offered to municipalities is effectively operated; and 4) if local governments are ready to maintain the enhanced information security level.

The opinions expressed in this paper are of the author's own and do not reflect the view of SAI Japan.

1. Backgrounds of the audit

1) Local government system in Japan

Japan has two-tier local government system. 47 prefectures cover 1,741 municipalities (cities, towns, villages, special wards).



Source: Ministry of Internal Affairs and Communications

https://www.soumu.go.jp/main_content/000295099.pdf (As of May 2014)

2) Massive data leakage from Japan Pension Service

In 2015, 1.25 million cases of pension data were stolen from the shared storage through the internet triggered by a series of targeted attacks on Japan Pension Service (JPS), which is a quasi-governmental body. JPS promptly cut off overall internet connections, and such cutoff lasted for more than a year. This meant huge disruption of businesses.

3) Social Security and Tax Number System

In Japan, in order to improve convenience for individuals using public services, the Social Security and Tax Number System (nicknamed the “My Number System”) took effect in 2016. Under the My Number System, governmental bodies and local governments exchange information related to social security or tax by using the identification number (“My Number”) as a matching key.

2. Strengthening information security measures of local governments by the Government

After the leakage of data from JPS, people’s concern spread over the security of Social Security and Tax Number System. The Government urged local governments to upgrade security levels of computer systems so that people’s My Numbers are secure.

Subsidies were broadly distributed to prefectures and municipalities.

The requests from the Government (Ministry of Internal Affairs and Communications) are summarized as follows:

- a. Two-factor authentication system should be installed to the computers which handle My Numbers.
- b. Take-out of information from the computers which handle My Numbers should be properly restricted.
- c. The system which handle My Numbers should be isolated.
- d. The system used for connection to “Local Government Wide Area Network” (LGWAN) should be disconnected from the internet.
- e. Prefectures should provide the common gateway to municipalities so that the gateway functions as the sole connection point from the municipalities to the internet.

3. Audit results on the systems built

3-1. Two-factor authentication system

Out of 217 municipalities audited, 10 municipalities had no plan to equip all the computers with two-factor authentication system. These 10 municipalities rectified the faults.

3-2. Restriction on take-out of information

Out of 218 municipalities audited, 12 municipalities had no plan to equip all the computers with measures to restrict take-out of information. These 12 municipalities rectified the faults.

3-3. Isolation / disconnection of the systems

SAI Japan audited 223 municipalities and confirmed that 1) all municipalities isolate the system related to My Numbers from other systems; and 2) all municipalities disconnect the system related to LGWAN from the internet.

3-4. The common gateway

Out of 241 local governments (prefectures / municipalities) audited, 237 of them had connections to the common gateway provided by 18 prefectures. SAI Japan followed up the rest 4 local governments and confirmed that they have built connections to the common gateways either provided by prefecture or introduced jointly by several municipalities.

4. Audit results on the system operations

4-1. Two-factor authentication system

Out of 217 municipalities audited:

- 27 municipalities provided staff members with passwords in advance which were for use when two-factor authentication failed.
- 7 municipalities allowed staff members to share both knowledge factor (e.g. password) and possession factor (e.g. USB token).

Out of 122 municipalities where My Numbers were stored in hard drives of the computers or in network shared disk:

- 15 municipalities may face difficulties in identifying who accessed the shared data because the terminal computer is available for all staff members who share the authentication methods.
- In 16 municipalities, My Numbers stored in hard drives or in shared disks were accessible by one-factor authentication.
- In 7 municipalities, My Numbers were accessible by other staff members than authorized people.

4-2. Restriction on take-out of information

Out of 218 municipalities audited,

- 87 municipalities allow staff members to take out media which contain My Numbers for more than one month.
- 44 municipalities did not save log files.

4-3. Isolation / disconnection of the systems

As is shown in 3-3, segmentation of systems related to My Numbers or LGWAN from the internet has been completed in all municipalities.

However, some traffics between segments were allowed without restricting communications protocol or communication routing in some sixty municipalities.

In addition, it was found that email sanitization was insufficient in some municipalities.

4-4. The common gateways

The common gateway enables prefectures to help the rest of local governments to monitor the internet traffics. However, a prefecture did not monitor DNS server and 8 prefectures did not monitor the log of firewalls due to absence of centralized

monitoring equipment.

Out of 237 local governments audited, SAI Japan found that 26, 44 and 116 entities failed to centralize their Web servers, DNS servers and log of firewalls respectively, due to lack of such centralized equipment at the common gateways. Accordingly, the said entities should have monitored their own equipment but 6, 11 and 63 entities did not monitor or analyze their Web servers, DNS servers and log of firewalls by information security specialists.

Out of the said 237 entities, 77 entities required operation contractor's assistance in order to identify which computer is compromised in the case of security incident. However, 11 entities among them did not confirm which party (local government / operation contractor) is responsible for necessary intervention or did not conclude necessary contracts.

4-5. Local governments' readiness to maintain the enhanced information security level

Out of 241 local governments audited:

- 3 entities lacked necessary information security countermeasures policy and 178 entities did not revised their policy in accordance with the Government's request to strengthen information security measures.
- Only 130 entities (53.9%) set up CSIRT (Computer Security Incident Response Team); among which
 - 16 entities lacked documentation about the staffing or function of CSIRT.
 - 37 entities did not formulate concrete plans to counter emergency.
 - 49 entities' reporting lines to the Government and the CISOs were unclear.
- Only 54 entities (22.4%) exercised a drill to cope with emergency.

5. Conclusion

The Government (Ministry of Internal Affairs and Communications) should give necessary advices to local governments so as to assure the effect of the subsidy is long lasting.

Within our mandate, SAI Japan will keep watching the Government's measures to secure the information systems used for the Social Security and Tax Number System amid intensifying threat toward IT.