SAI Japan's audit results on leaks of personal information from the Japan Pension Service

[Abstract]
Japan has national compulsory pension system with 67 million contributors and 40 million beneficiaries. The data of national pension is managed by Japan Pension Service (JPS), a quasi-governmental agency.
The cyber incident triggered by a series of targeted attacks on JPS in 2015 undermined confidence in information security of Japanese pension system.
This paper explains SAI Japan's special audit report on 1) information security management and operations by JPS before the incident; 2) information security management after the incident; 3) negative impact on JPS's operations in the aftermath of the incident; and 4) other findings.

1. Management of personal information of beneficiaries /insured persons in Japan

1.1 Japan Pension Service (JPS)

Japan has huge national compulsory pension system with 67 million insured persons and 40 million beneficiaries. Annual pension benefit amounts to 55 trillion yen (equivalent to 500 billion USD) and the reserve funds of the national pension plan amount to 150 trillion yen.
Though the Government (Ministry of Health, Labour and Welfare, hereinafter called "MHLW") is responsible for storing pension data, management and operations of the data are delegated to JPS.
JPS is a quasi-governmental body which was separated from MHLW in 2010. It has 312 branch offices and 11,000 employees[1].

1.2 Management of pension data with computer systems

JPS handles huge personal data such as ID numbers, names, birth dates, postal addresses, contributed amounts of beneficiaries and insured persons for a long period.
Before the setup of JPS in 2010, MHLW was responsible for the management and

[1] https://www.nenkin.go.jp/files/about_jps_operation.pdf

operations of pension data. The current "Social Security On-line System" was developed by MHLW in 1964 (!) and has been expanded (see Chart 1).

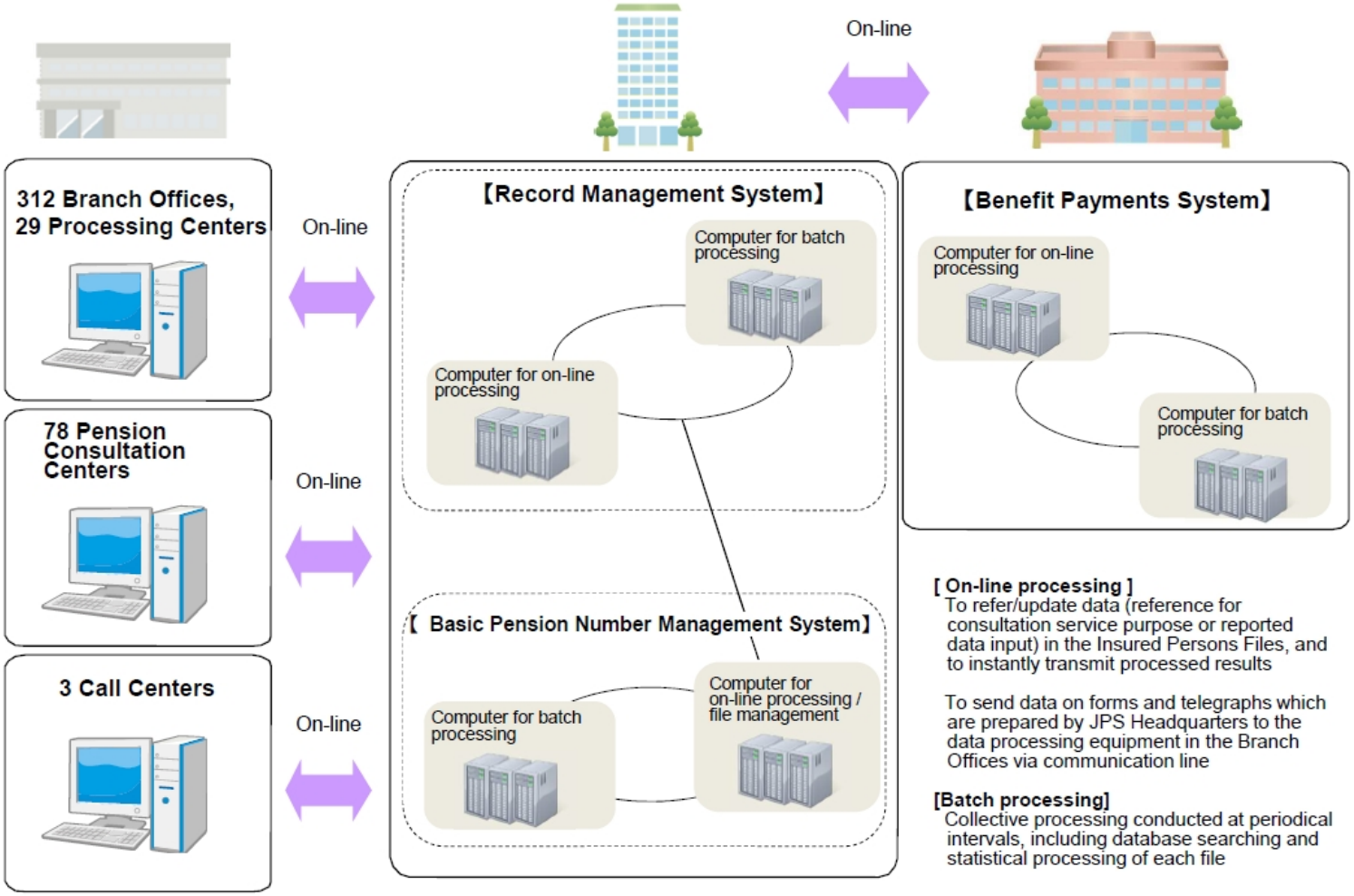
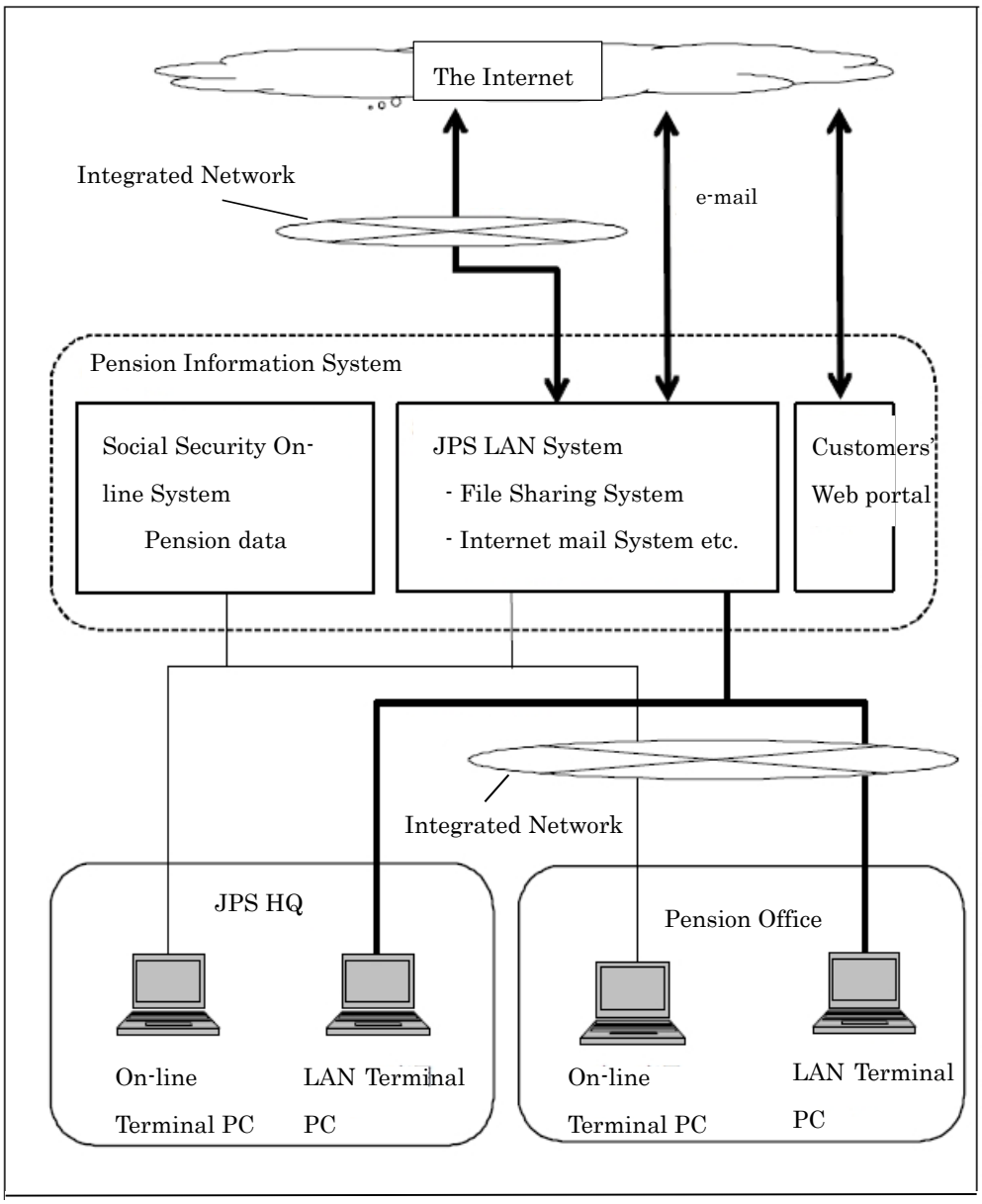


Chart 1. Structure of Social Security On-line System

After the establishment of JPS in 2010, Social Security On-line System (hereinafter called "On-line System") is managed and operated by JPS. The basic functions of On-line System is to input and query pension data but the system is not suitable for document processing, communication, data processing etc. So, JPS developed "LAN System" for its daily businesses. LAN System offers business tools such as shared storage, email service, internet connections (see Chart 2).



(Note) The thick lines indicate that the network is connected to the internet.

Chart 2. Total structure of systems to handle pension data and other data in JPS

2. Leaks of personal information from JPS in 2015 and factual backgrounds found by investigation committees

In May 2015, 1.25 million cases of pension data were stolen from the shared storage of LAN System through the internet triggered by a series of targeted attacks on JPS. Noticed the magnitude of the incident, JPS promptly cut off overall internet connections and such cutoff prolonged for more than a year. This meant huge disruption of businesses; JPS staff was not able to communicate with customers (beneficiaries, insured persons) by using the internet.

Investigation committees were set up to investigate the causes of the incident and three reports were presented in August 2015 separately. They are published by:

1) National Cyber Security Center
2) JPS's internal investigation committee headed by the President of JPS
3) Independent Committee commissioned by MHLW

Their findings include:

- Absence of practical countermeasures against cyber attacks
  JPS failed to specify practical countermeasures against cyber attacks despite requirement of JPS's Information Security Policy.
- Absence of CSIRT (Computer Security Incident Response Team)
  JPS lacked CSIRT despite JPS's Information Security Policy's general instruction to set it up.
- Poor readiness
  JPS was poorly prepared for targeted attacks so that received suspicious emails were not reported to the proper reporting line.
- Chief Information Officer failed to give concrete directions to tackle the incident.
- Lack of Incident Response Procedures
  Incident Response Procedures against target attacks did not exist.
- Scope of Internal Audit
  Preparedness against cyber attacks was not within the scope of JPS's internal audits.
- MHLW's oversight on JPS's LAN System
  MHLW's supervision on cyber security of JPS's LAN System did not

function effectively.

- Poor coordination between JPS and MHLW
  Hotline between JPS and MHLW for significant cyber incident did not exist.
- Poor data protection
  Out of stolen 1.25 million cases of pension data, 20 thousand cases were neither protected by access control nor by passwords. Some pension data were left inside shared storage even though such data are no longer necessary.

3. Audit Results

SAI Japan examined

1) Information security management and operations by JPS before the incident,
2) Information security management after the incident,
3) Negative impact on JPS's operations in the aftermath of the incident, and
4) Others,

and presented many additional findings in its special audit report on JPS incident other than already-known findings published by the above-mentioned committees.

3.1 Information security management and operations by JPS before the incident

3.1.1 JPS's readiness to revise its Information Security Policy

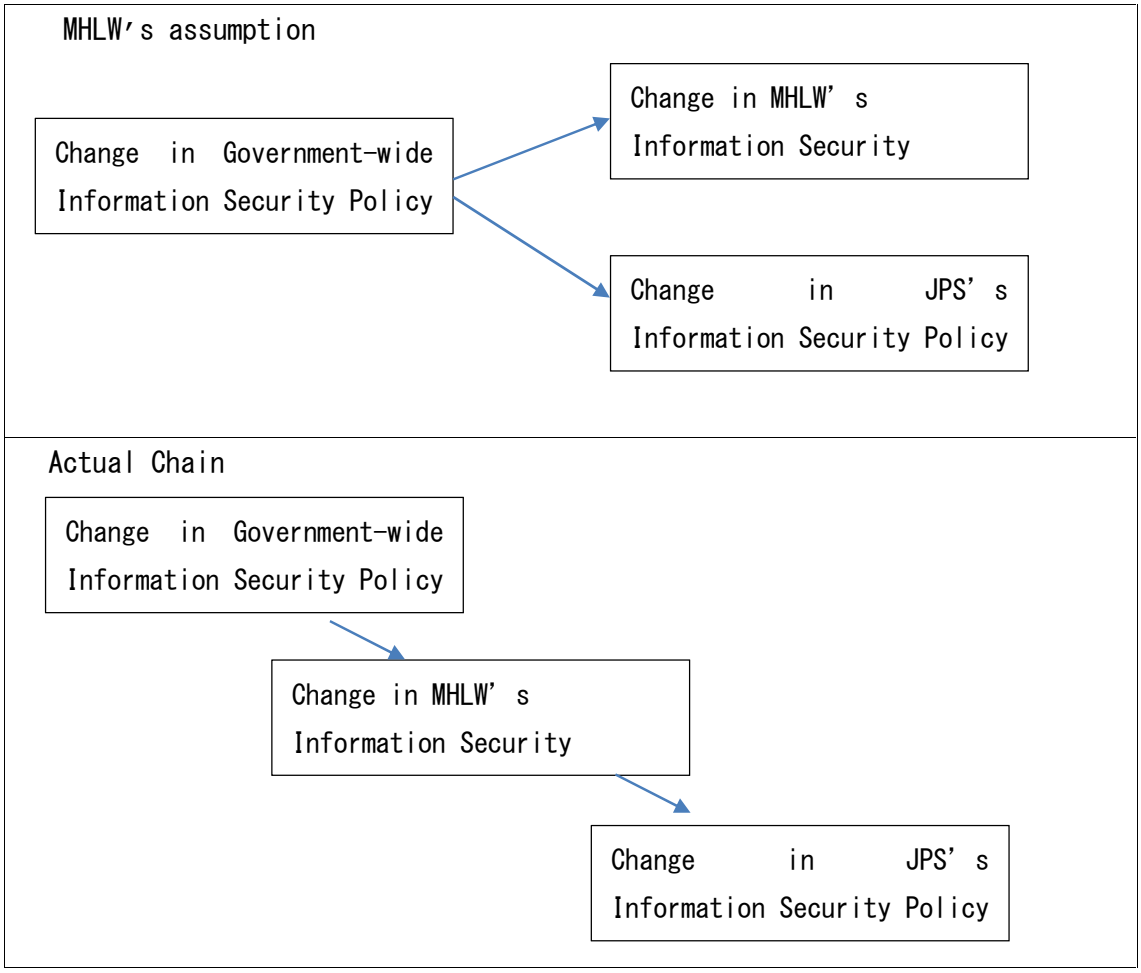


Chart 4. Chain of the revision of Information Security Policy

Japanese Government publishes and updates its Government-wide Information Security Policy. Ministries and agencies are expected to establish and update their information security policies in accordance with the Government-wide policy.

SAI Japan found that JPS's Information Security Policy had not been swiftly changed after changes in MHLW's policy (5 to 7 months needed); MHLW assumed that JPS was obtaining necessary information from the Government directly and did not understand that JPS was waiting for information from MHLW in reality. In addition, none of the sections was designed to take initiative to change security policy inside JPS.

3.1.2 MHLW′s information security audits on JPS

As already mentioned, huge number of pension data was stolen from the shared storage of LAN System through the internet.

SAI Japan found that MHLW′s security audits on JPS were insufficient: main target of security audits by MHLW to JPS had been On-line System and LAN System had not been covered by MHLW′s audit.

In addition, MHLW′s audit team did not notice JPS′s shortfall in cyber security. Even before the incident, MHLW was equipped with its own Incident Response Procedures and CSIRT. Nevertheless, the audit team failed to find absence of JPS′s equivalent documents and CSIRT, which could be found by audits in a comparative manner.

3.1.3 JPS′s internal audits on information security

JPS′s internal audit team failed to contribute to prevent the cyber incident. In August 2014, the audit team realized that the shared storage of LAN System contained vulnerable data which was left unattended without security measures such as access control or passwords. Though the team′s finding was significant, it did not report the finding to the President and did not follow up necessary improvement measures.

3.2 SAI Japan′s audit on JPS′s intended improvement in data management

JPS was expected to improve data management thoroughly after the incident. SAI Japan conducted some sampling audits on JPS′s compliance with data management rules reinforced after the incident.

As explained in Chart 2, PCs are connected to LAN System. SAI Japan′s audit team found some 3,000 cases of pension data were stored in the hard disks of some PCs. JPS set out thorough investigation on data management at all branch offices.

3.3 Negative impact on JPS′s operations in the aftermath of the incident

As already mentioned, the incident caused huge disruption of JPS′s businesses. In the concrete,

1) JPS could not send letters of reminder which notice payments of monthly contribution were overdue. The delay of reminder letters caused expiry of Government′s right to collect monthly pension contribution. Audit showed at least 56 million yen could have been collectable if reminder letters were

sent properly.
2) JPS could not send letters to encourage payments. SAI Japan estimated that negative impact which was caused by the suspension of such letters amounted to 11 billion yen.
3) JPS's suspension of daily businesses affected its outsourced operations. The contractors that were undertaking outsourced operations were forced to idle their human resources. These companies were once paid fully but JPS later demanded them to partly pay back because the outsourcing contracts were paid based on their performance.

3.4 Other finding
JPS sent apology letters to the customers whose pension data were affected. However, some of them were sent back as unknown addressees.
SAI Japan pointed out that JPS should investigate if such beneficiaries are alive.