Data Backup Dilemma:

Case Studies from the Great East Japan Earthquake

Mihoko Sakurai

University of Agder
POST BOX 422
Kristiansand, Norway
+47 38141902

mihoko.sakurai@uia.no

Jiro Kokuryo

Keio University
5322 Endo
Fujisawa, Japan
+81 466493557

jkokuryo@sfc.keio.ac.jp

**ABSTRACT**

When the Great East Japan Earthquake struck in 2011, several municipalities lost their residential data including backup. Since none of them had ever considered the total loss of data, data backup policy had been paid little attention. In many cases, the backup tapes were simply stored inside the server room, just beside the server rack.

Following the calamity, the Japanese national government tried to introduce a data backup system to municipalities using the cloud. The purpose was to secure the safekeeping of backup data. However, municipalities were reluctant to go along with this since overcoming the loss of network connectivity during an earthquake remained foremost in their minds. They prioritize accessibility to data, including that held on tapes, in the event of a future disaster.

To overcome this conflict, this paper proposes a hybrid approach for a future data backup policy. Conceptually, a frugal backup system relying on minimal resources should kick in immediately following a disaster while the system as a whole strives to recover the level of robustness necessary for keeping backup data safe.

**CCS Concepts**

• **System management, Security requirements, Sustainability**

**Keywords**

Municipality, Data backup, Policy, Disaster, Cloud computing

# MUNICIPALITIES FACING DAMAGE OF DATA LOSS

Every day a great many data related to the daily life of local residents is processed in municipal government office buildings. Normally this does not draw people’s attention, however, the significance of holding the data is revealed once something unexpected happens. Unexpected events in this paper mainly refer to natural disasters. Since local organizations own the foremost response to a disaster management [1], municipalities stand at the front line of managing disaster situations [2].

This paper addresses municipal government policy regarding data backup. The issue became critical as a consequence of the Great East Japan Earthquake in 2011. Legally, the function of municipal governments in Japan is to provide a variety of services to their citizens but above all they have the obligation to maintain resident information, i.e., the data that serves as the foundation for government.

*17th Annual International Conference on Digital Government Research,* June 8–10, 2016Shanghai, China.

On March 11, 2011, Japan was struck by the Great East Japan Earthquake. The movement of tectonic plates along the Pacific Rim created a rupture zone 500 km long. Measuring 9.0 on the Richter scale, the earthquake produced a tsunami of 40 meters hitting the coastline and devastating cities and towns. The Fire and Disaster management Agency reported 19,335 deaths, 6,219 injuries and 2,600 missing as of September 2015. It also reported 124,690 houses totally lost and more than 1,000,000 partially destroyed. This earthquake was unique in that it caused severe damage to a very wide area, above all due to a massive tsunami that was beyond any previously held assumptions.

The tsunami caused unexpected damages to municipalities. In some areas, power supply and connectivity were completely lost at the most critical life-saving phase. Office buildings and server rooms received huge damage, some were washed away and others were submerged. This was something that no one could have predicted with residential records including backup data being completely lost in some towns and cities.

This of course does not mean that municipalities disregarded the importance of keeping backup data. They implemented data backup daily or several times a week. However, there were two main problems. First, backup data for most municipalities means something to be relied on in case of information system (server) breakdowns. So, to enable its use, backup data was simply shelved beside the servers. Officials never assumed that all office buildings would be submerged or washed away. The second problem stems from official policies underpinning the system. For example, government offices prohibit external storage of data in order to prevent leakage of personal information. Municipalities were generally afraid of losing their backup data so they kept it inside the server room where it was easy to pay attention to.

Unlike damage to hardware and application software that can be fixed, restoration of lost digital data is difficult, hampering the entire recovery process. This forced municipalities to make extraordinarily great efforts to recover residential data. As a consequence the work caused delays in delivering disaster relief operations to residents. It is therefore necessary to raise awareness of digital data as a prime asset that must be protected in the event of disasters.

This paper introduces case studies of two towns that were ravaged by the earthquake and related tsunami, losing both their primary residential record data and backup. Their perceptions for a future data backup policy and potential data backup options are appraised in the following sections. Two conflicting approaches, accessibility and safety, will be discussed. The paper concludes with the proposal of a hybrid solution attempting to incorporate both views. The outcome should contribute to a stronger digital society.

# REALITY IN THE FIELD

The empirical evidence of this research is based on interviews with officials from 13 municipal governments that experienced huge damage from the Great East Japan Earthquake. The two-hour interviews were conducted in December 2011, nine months after the earthquake. The two respondents from each town were officials of information systems departments in charge of managing their systems when the earthquake struck. They were asked about preparedness, the level of damage, and the recovery process of ICT equipment including power supply, network connectivity, information systems, and related facilities. The interview reports were checked and officially verified. Archived documents were referenced and additional telephone interviews conducted to fill in missing information subsequently.

In this paper we report on two municipalities, Minamisanriku and Rikuzentakata. The towns are located in countryside of Japan with a population of 17,500 and 23,000, respectively, at the time of the earthquake. We will see how residential data and backup were lost at each site.

## Minamisanriku Town

When the Great East Japan Earthquake occurred, information department[[1]](#footnote-1) officials of Minamisanriku, located in the northeast coastal region of Miyagi Prefecture, were inside the local government building, a two-story structure made of wood. They intended to grasp the situation there but when power was cut to the building they went to check the server room in the disaster response building (three-story structure) next door, where the server was set up. Fortunately the devices were not damaged. The officials moved to a disaster response headquarters that had been set up inside the disaster response building and attempted to continue collecting information about the situation at that location when they heard a broadcast on the town’s disaster prevention radio system announcing that a six-meter high tsunami had formed. Then, a second broadcast stated that the height of the tsunami was in fact some ten meters. Officials evacuated to the rooftop of the building with other personnel who were inside headquarters. The disaster response building was situated less than a kilometer from the coastline, and a tsunami over ten meters high was approaching them. The tsunami went as high as the roof of the disaster response building and took everything along with it. Only the frame of the building remained. The wooden government building was swept away without a trace.

The employees who had evacuated to the roof and survived, spent the night on top of the disaster response building, which had been turned into a bare platform. The next morning they climbed down to the ground using a rope made used for seaweed cultivation that had washed up in the floodwaters. A disaster response headquarters was then established in a town facility about three kilometers away from the former government building. Apparently, this facility was soon inundated with a crowd of over 1,000 evacuees.

The first thing officers had to do now was to check the safety status of residents and identify evacuees. They wanted to access the Basic Resident Registration System[[2]](#footnote-2), that was used to manage basic resident registration records but the servers in the server room inside the disaster response building had all been swept away, and it was difficult for officials to even attempt to search for them. The backup tapes had also been stored in the server room, so were swept away as well. Therefore, using pencil and paper that had been provided with aid supplies from across the country, they manually began the work of checking the safety status of residents.

On March 22, on the tennis courts next to the facility where the disaster response headquarters had been established, the officials set up a prefabricated provisional government building. They also installed an emergency power generator since the power supply had been cut by the earthquake. A contractor responsible for system integration (SI) in the town provided them with complete facilities (servers, personal computers, and printers, etc.) for issuing victim certificates. This contractor had a basic system[[3]](#footnote-3) including data backed up to March 4. Using this backup system, an environment for the resumption of operations was created. However, data recorded between March 4 and 11 had been completely lost.

## Rikuzentakata Town

In Rikuzentakata, which is located in the southeast coastal area of Iwate Prefecture, a three-story (and partly four-story), reinforced concrete government building—positioned about two kilometers from the coastline—was engulfed by the tsunami.

As the tsunami was approaching, the personnel who were in charge of the regional network went up to higher ground inside the city. This was partly so that the employees who were also working in the area of public affairs could take photographs to record the tsunami. As seen from the high ground, the tsunami was larger than expected. The day-to-day scenery vanished in moments. It was not possible to return the government building that had been swallowed up, so the employees went to a nearby community center where they spent a sleepless night. On March 12, they ran into a town official and heard about the disaster response headquarters facility that had been set up. This facility had started checking the safety status of residents. Lines were drawn on pieces of copy paper found inside the facility, and the names of the citizens were written on them. The power went off immediately following the earthquake and only started to come back on again in the evening of March 14, so personal computers could at last be turned on. Two or three employees stayed up all night inputting names, and the task was mostly completed within about a week.

About a quarter of the personnel at Rikuzentakata perished in the earthquake and tsunami. Some officials in charge of information systems also lost their lives. The server room inside the government building was submerged. The recovery operations related to information systems ended up being carried out by former officials. On March 15, a contractor in charge of managing information systems brought a paper printout of the basic resident register as recorded up to the end of February and a CD containing the data.

On March 19, a prefabricated provisional government building was set up on private land 150 meters away from the disaster response headquarters. Around that time, the personnel in charge of information system recovery operations, together with the manager of the contractor taking care of the information systems, headed over to the government building, which had been devastated by water. The task was to recover the server hard disks, backup tapes, and everything still in the server racks. The group was able to retrieve the mud-covered devices and tapes and immediately requested a contractor to carry out salvage operations. As a result, the Basic Resident Registration System, welfare system[[4]](#footnote-4) data and tax report data were successfully restored though all other data was lost. The backup tapes that were collected together with the hard disks had been soaking in water and were covered in mud, so resurrecting the data had become impossible.

There was a notable shortage of officials to check the safety status of residents and implement recovery operations. To offset the shortage, relief staff was dispatched in April and May to the information department. These officials came from other municipalities that had not suffered big earthquake damage.

## Instances of Data Loss

Loss of residential data caused delays in recovery. Both of Minamisanriku and Rikuzentakata had used tape for data backup and stored it inside the office building’s server room. Frequency of backup varied from daily to once a week (Table 1).

Table 1. Data backup measures

(As of March 11. 2011)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Municipalities**  | **Information system** | **Frequency** |  **Method** | **Storage place** |
| Minami-sanriku Town | The Basic Resident Registration System, Tax and Social Security systems | 1 – 2 times a week | Tapes and server hard disk drive | Serverroom |
| Rikuzen-takata City | The Basic Resident Registration System (including Social Security) and Tax systems | Daily | Tapes | Serverroom |

As we have seen, both of Minamisanriku and Rikuzentakata government office buildings were completely devastated by the tsunami and the data servers were either submerged or washed away in the floodwaters. Neither town had backup data stored at locations outside the government office buildings, and for a while it seemed that all digital data had been lost. Based on these events at Minamisanriku and Rikuzentakata, the instances of data loss vis-a-vis recovery can be classified as shown in Figure 1.

Data loss

Option 1) Backup data available

 1-1) Data can be restored

Option 2) Backup data unavailable

 2-1) Servers recalled

 2-1-1) Data can be salvaged

 2-1-2) Data cannot be salvaged

 2-1-2-a) Using data that a SI contractor holds

 2-1-2-b) *Failing to restore backup data*

2-2) Servers unrecalled

 2-2-1) Using data that a SI contractor holds

 2-2-2) *Failing to restore backup data*

**Figure 1. Instances of data loss and restoration**

What happens after data loss? We could observe several paths from that point onward. The first step is to check whether backup data is available to use or not (option 1 or 2). Conventional business continuity plans refer only to the time frame assumed necessary for restoring data, but they never expect the loss of backup data itself. However, the earthquake revealed that the loss of backup data was a reality. Then, once town officials found that backup data was unavailable (option 2), they tried to recall servers.

In Rikuzentakata, the office building was submerged but fortunately servers had remained inside the server room (2-1). Data in the server hard disc could be partially salvaged (2-1-1) while backup tapes had become useless because of the mud. If Rikuzentakata had failed salvaging its residential data (2-1-2), it could never have been restored (2-1-2-b) unless a contractor in charge of systems held backup data by chance (2-1-2-a).

In Minamisanriku, servers had been washed away by the tsunami and remained irretrievable despite an extensive search (2-2). Luckily, a contractor held residential backup data up to March 4 (2-2-1), i.e., seven days before the earthquake, and the town was able to use it. However, data for the period March 4 to 11 was totally lost (2-2-2). Without the contractor’s backup data, Minamisanriku could never have successfully delivered disaster relief operations to its residents.

From this observation, we can notice the importance of ensuring the safekeeping of backup data.

# PERCEPTIONS TOWARD FUTURE DATA BACKUP

Based on the lessons stemming from the earthquake disaster, there have been high expectations in the affected areas to introduce the cloud for data backup. The national government prepared a budget for introducing the cloud to affected municipalities with an allocation of one million USD a year.

Another option that the national government had espoused was to keep backup data on the cloud for aggregates of several municipalities rather than for towns and cities in isolation. Nevertheless, many towns are expressing concerns with regard to system operation on the cloud, which is based on the assumption of there being a viable network connection and successful resolution of privacy issues. The following paragraphs highlight local concerns and provides some ideas for future data backup, as stated by the information department managers in Minamisanriku and Rikuzentakata.

The view in Minamisanriku: “As for the joint usage of systems by municipalities, we believe each town has a different way of processing operations, so it will be necessary to make a lot of adjustments in order to achieve consistency. When Minamisanriku was born in a merger of two neighboring in 2005, a system subcommittee was set up for each operation, and opinions were exchanged regarding work procedures and operations. But I think it would be very difficult to hold discussions bringing together more municipalities.

“Nevertheless, I believe that in the future we will probably move in the direction of joint usage and cloud utilization, taking into consideration the trend of the times and cost reduction factors. The transition process will be very difficult, so I think one approach would be for the national government and others to designate one format, and then to make decisions on operational methods in a top-down manner.

“Based on our experience of losing all data held at our government building, including our key system data, we believe that backup data should be stored outside the government building. It was by pure chance that the contractor managing our information systems happened to be in possession of our backup data. We used this data to resume our operations, and based on this background, I recognize that the problem of a backup location is a very important issue. We are also considering data storage at a location that is separate from the data center[[5]](#footnote-5).”

After the earthquake, Minamisanriku started using a data center for online data backup [3]. However, the online backup ran as a trial for just one year. It stopped for reasons of cost, the charge being several thousand USD per year. To gain an annual budget allocation for data backup is not easy. It is cheaper to keep a backup tape outside the town and deliver it when an emergency situation comes up.

The manager added, “Having experienced the loss of network connectivity, we have a strong wish to keep backup data close to us, not in a remote location.”

The view in Rikuzentakata: “The most important lesson we should learn from this earthquake was that it is possible to compensate for physical system facilities such as servers or cables in emergencies even if it takes time to get everything working. However, data being digital, it never returns once lost. Therefore, we should consider our future data backup very carefully. To keep backup data outside the office building requires grasping the nature of privacy. The data contains personal information and we should deal with it guardedly. Originally, we did not have a uniform policy applying to all kinds of data backup processed in daily operations. The earthquake made us aware of the importance of such a policy and so we created it. Since the backup tape was not functional following the earthquake and, in addition to this, tapes require regular exchange, we decided to use HDD for doing data backup. This applies to all sections in the city office building with the exception of individual systems that require their own backup system because of the structure of the system itself.

“The reason that the national government is putting a budget toward the introduction of joint cloud usage is that it understands that it is costly to independently introduce cloud systems at the municipal level and that such introductions will not move forward. Even if local communities receive subsidies from the national government to cover initial costs, they will have to cover the running costs, so the hurdles for cloud services to find traction are high. Nevertheless, municipalities in coastal regions that have lost data or have taken servers out of the mud and restored them, realize the necessity of the cloud, and I believe that if the costs, including running costs, can be successfully reduced through joint usage, the likelihood of introducing the cloud will increase.

“In the case of joint usage, transfer of data is an issue. The current situation is that when registering resident information in the Basic Resident Registration System, each municipality has its own unique interpretation regarding the utilization of foreign letters, abbreviations, and original characters. Therefore, one view is that moving the Basic Resident Registration System to the cloud would meet far higher hurdles than, for instance, the transfer of operations such financial accounting and providing public assistance.

“In the case of utilizing the cloud, it is only natural to use a highly reliable circuit, but as for the proposal of utilizing the governmental internal network system[[6]](#footnote-6), the line is too slow, so I don’t think it is realistic. If there are examples of municipalities actually introducing cloud systems without there being any problems in terms of security and so forth, then introducing such a system might be easier. Meanwhile, I believe that if each municipality contributes some money to construct a secure building to physically store backup data, the problems will probably be resolved.”

Rikuzentakata tried to build a backup system in a branch office building located in the city. The plan was to utilize a regional intranet[[7]](#footnote-7) to build up connectivity. The officials believe that it is safer to keep backup data at a remote location. However, they doubt the reliability of data accessibility. Furthermore it costs a lot to prepare secured network connectivity and maintain it.

# DATA BACKUP DILEMMA

Needless to say, municipalities should avoid losing residential record data including its backup. The disaster situation reveals these issues clearly, however, loss of data and backup might happen even in an ordinary situation. The disaster highlighted the importance of keeping data safely since it is irretrievable once lost. We understand that this is a problem which directly impacts our everyday life.

In the case studies of Minamisanriku and Rikuzentakata we observed two conflicting aspects obstructing the formulation of a sound future data backup policy, namely, accessibility and safety. We call it as dilemma of data backup policy. The national government prioritized realizing safety by introducing a cloud system while municipalities prefer to secure accessibility and keep backup data physically close to them as tapes or so on. Now we proceed to consider what kind of options we might take beyond that for building a future data backup policy.

## Accessibiliy vs. Safety

As shown in Table 1, the only option for Minamisanriku and Rikuzentakata for data backup was keeping it inside the office building using tapes and HDD. Following their perceptions for a future data backup policy, potential future options should be discussed in terms of two categories, i.e., storage location and means.

Regarding storage location, communities prioritize securing accessibility. They are afraid of losing connectivity to the backup when it is urgently required. However, from the lessons we learned from the earthquake, keeping a backup tape next to servers is not useful. One possible option is to use other facilities within municipalities. A branch office or other related building could be utilized. Remote locations such as outside the town/city could be considered, however, depending on the means of keeping backup data, the degree of accessibility would change.

As for the means of keeping backup, Minamisanriku relied on the use of a data center for just one year due to high annual cost. Especially for small municipalities, the expense is too high and they cannot afford to pay on a constant basis. The towns would return to use tapes but store them externally. Rikuzentakata, on the other hand, came up with a plan to build a backup system in a branch office using a regional intranet since they are too nervous to keep backup data externally because of privacy issues.

As the national government promoted it, cloud computing could be an effective infrastructure to house a critical database [4]. It seems to enable secure data safety without any concerns of losing it. The joint use of cloud services with several municipalities would also be a future option. However, we should remember that during the Great East Japan Earthquake, in the most affected areas, power and network connectivity were totally lost for a certain period. Minamisanriku had to wait more than two months to recover power supply (Table 2). In the meantime they had to use emergency power generators. Communications with the outside was suspended for almost a month, which weighed heavily on the town. In Rikuzentakata, it required four months to resume the Internet. This reveals the massive scale of the earthquake. Of course, there is always the possibility that suspension of communication services may also be due to some other reasons.

Table 2. Timing of restoration of power and means of communication

|  |  |  |  |
| --- | --- | --- | --- |
| **Municipalities** | **Power supply\*** | **Mobile phones** | **The Internet** |
| Minamisanriku Town | Approx. 80 days | Approx. 20 days | Approx. 20 days |
| Rikuzentakata City | 3 days | 7 days | 120 days\* |

\*at the temporary office building

Therefore, even if officials understand the importance of keeping backup data in a remote location or on the cloud, they are less willing to do so. This is a dilemma that needs to be overcome.

Another form that the accessibility versus safety issue surfaces, is around privacy. To ensure accessibility one might want to maintain copies of data in multiple locations in a less protected manner. We have indeed encountered cases of losses in authorized local officials that would negate access to critical data. At the same time, keeping personal information with little protection in insecure locations increases the risk of information leakage. A possible solution to this problem may be to classify attributes to individuals to (a) critically important attributes in disaster situations, such as name and dates of birth, and (b) less critical data but highly sensitive data such as income data.

## Backup Options

Based on perceptions stated by information department managers in each town, potential future data backup options are shown in Figure 2.

LOCATION

 Inside the municipality (but outside the office building)

Remote area

MEANS

 Tapes/ HDD/ Data center/ Cloud

Connectivity options --- LGWAN/ regional intranet

**Figure 2. Future data backup options**

If priority is given to accessibility, the appropriate means of storage is tapes which should be stored close to officials. Online backup is not an option in this case. On the other hand, if safety is prioritized, using the cloud or data centers should be effective though they are associated with high cost and privacy issues.

Before attempting to offer to a partial solution, we introduce a complementary statement from another municipality, Miyako City.

The information department manager of Miyako remarked as follows when asked for his opinion on future data backup. “During the Great East Japan Earthquake, there were municipalities whose server devices were washed away, and this is why it seems cloud usage and remote location backups are garnering attention. However, it is also important to consider the procedures leading up to cloud usage and at what point they can be used following a disaster. When using remote location backup, it is necessary to have a proper service that will insert the backup data into the system, and enable it to be received in a format that can be used right away. For example, one can imagine utilizing virtualization technologies and so on, but the current situation is that there do not seem to be any services that have thought things through to that extent. As for discussions about the cloud, there are a number of aspects such as backing up data, disconnecting server operations and cost reduction based on joint use, but there is a tendency for debates to take place mixing all of these together. I think it is important to consider each element separately.

“If using the cloud from the perspective of backing up data, it is necessary to take into consideration the fact that if the network becomes disconnected in a disaster, usage will no longer be possible. At this point in time, I do not really feel that shifting to the cloud is necessary. If the network becomes disconnected, even if there is a backup at a remote location outside of the city, usage will be impossible. I think if a notebook computer environment is built and network storage is connected, this would be more effective for retrieving data. We are planning to take budgetary measures for backups outside of the government offices making use of a regional intranet. Remote location backups using the Local Government Wide Area Network (LGWAN) have been suggested, but LGWAN has small circuit capacity, so it takes time to transfer backup data. We would prefer to prepare a circuit with large capacity.”

# SOLUTION PROPOSAL: HYBRID APPROACH

The statement from Miyako leads us to take a hybrid approach toward future data backup policy. In considering a solution, we think that the notion of frugality is useful. The importance of this notion has been recognized in the engineering field. It was originally introduced by Tata Motors, an Indian car manufacturing company [5]. The concept was born from the recognition of limited worldwide resources which enables designs minimizing environmental impact while maximizing customer value. It refers to the ability to innovate cost-effectively and quickly under severe resource constraints [6]. Based on this notion, Tata manufactured the Nano motorcar realizing both a cheap price and adequate functionality at the same time. The same notion has been applied to information systems (IS) research and named frugal IS, defined as an information system that is developed and deployed with minimum resources to meet the preeminent goal of the client [5].

The notion is useful especially after a disaster because it forces people to manage with very limited resources.

Another approach is conceptualized as robustness. Robustness refers to maintain stability [7] which, in case of a disaster, is the ability to keep things “as usual.” This is the conventional approach to disaster prevention. Business continuity plans also take this approach.

Using a notebook computer as a backup storage is one possibility to realize frugality. Municipalities can store the minimum data such as residential record data in a notebook, which is available as soon as disaster strikes. A disaster situation does not require all residential data stored in the Basic Resident Registration System, but municipalities need to prepare minimum data set which is the basis for delivering disaster relief operations at the first stage of response. The most important job for them right after the earthquake was to check the safety status of residents. Since municipalities had received a hundred of inquiries from people who wanted to know the status and whereabouts of family and friends, they had to set up an evacuee list. One of municipalities recalled that when preparing the name list, at least names in phonetic script and dates of birth should have been collected.

The notebook computer is supposed to be kept in municipal facilities outside the main office building. It connects to a regional intranet so that during daily operations it constantly keeps a data backup. In case a disaster happens, officials can bring it to an evacuation place and be able to restore an operation immediately even without connectivity. At least names in phonetic script and dates of birth should be available immediate after. These are minimum data set that is only useful for setting up an evacuee list and responding to inquiries at an evacuation center. Without referring to other data set stored in the Basic Resident Registration System like address and gender, to identify person with the minimum data set is difficult. So we propose data to be kept in the PC should be limited to names in phonetic script and dates of birth in view of the privacy protection considerations.

Other data can be stored in tapes or server HDD and should be kept in a remote location, preferably outside towns and cities. Since using the cloud or a data center is costly especially for small municipalities, keeping backup data in tapes is the most realistic way. This approach keeps robustness and secures safety.

# CONCLUDING REMARKS

Needless to say, we should pay more attention to data preservation. We now recognize that data will not be recoverable once it is completely lost. However, the important implication derived from this research is that the issue is not simple. Two directions for a future data backup policy are discussed in this paper, i.e., accessibility and safety. These two approaches contain a fundamental conflict. When accessibility can be secured, the possibility of losing safety might be high. The opposite might also be true.

This paper insists on considering hybrid approaches. Introducing a frugal (minimum) data backup system such as using a notebook computer employed minimum set of data placed in a facility inside the city or town for securing accessibility is proposed. To secure the safety of backup data, using tapes for more comprehensive data storage and keeping them in remote locations, outside local communities would be useful.

Another finding of this research is the difficulty in creating a uniform data backup policy that applies to all municipalities around the country. Ways of implementing ordinary operations vary and present hurdles to the introduction of a joint cloud system for data backup. However, collaboration between towns and cities in terms of data backup could be an important topic worthwhile discussing in future research.

# REFERENCES

1. T.E. Drabek, 1985. Managing the Emergency Response. *Public Administration Review*, 45, Special, 85-92.
2. D. McLoughlin, 1985. A Framework for Integrated Emergency Management. *Public Administration Review*, 45, Special, 165-172.
3. Local Authorities Systems Development Center (LASDEC), Research report on robust information systems against disaster in municipalities. Tokyo, Japan, 2013.
4. Pokharel, M., et al. 2010. Disaster Recovery for System Architecture using Cloud Computing. *10th Annual International Symposium on Applications and the Internet Proceedings*, 304-307.
5. Watson, R.T., Kunene, K.N. and Islam, M.S. 2013. Frugal IS. *Information Technology for Development,* 19, 2, 176-187.
6. Radjou,N., Prabhu,J. and Ahuja, S. 2012. Frugal Innovation: Lessons from Carlos Ghosn, CEO, *Harvard Business Review*, Renault-Nissan, Last accessed 24th January 2016, at http://blogs.hbr.org/2012/07/frugal-innovation-lessons-from/
7. Husdal, J. 2009. De-confusing SCRM: Robustness, Resilience, Flexibility and Agility, Last Accessed 24th January, 2016, at http://www.husdal.com/2009/05/26/robustness-resilience-flexibility-agility/.
1. In this case, departments that control government systems, government networks, and regional networks, etc. are referred to as “information departments.” [↑](#footnote-ref-1)
2. Ledgers serve as the basis for “certificates of residence,” which provide official proof of addresses. They include information such as address, name, date of birth, gender, and household, etc. as stipulated in the Basic Resident Registration Act. The task of issuing certificates of residence is a clerical job overseen by municipalities, and each local government has introduced an information system that manages the information of ledgers. [↑](#footnote-ref-2)
3. This refers to a system for operations (taxes and national health insurance, etc.) that use basic resident register information. [↑](#footnote-ref-3)
4. This is an information system for carrying out operations such as welfare, welfare for children, welfare for the elderly, and welfare for the disabled. [↑](#footnote-ref-4)
5. In Minamisanriku, a data center system was opted for following the move to a provisional government building. [↑](#footnote-ref-5)
6. This network is named Local Government Wide Area Network (LGWAN), with the aim of local public organizations sharing residential information (name, age, gender and address) with each other. The Basic Resident Registration System is connected through this local network with all municipalities in Japan. [↑](#footnote-ref-6)
7. This is a network specifically for connecting public facilities (such as branch offices and community centers) within towns and cities. [↑](#footnote-ref-7)