Managed Service for the Support of Business Continuity

OGATA Hideyuki, OHSUKA Hideo, ABE Akiko, KONDA Nobuhiko, HIRAI Masaki, SHIMAZAKI Tomoyuki

Abstract

Business continuity (BC) can be achieved by providing information systems that feature measures for enabling recovery from a disaster event by meeting RTO (Recovery Time Objectives) and RPO (Recovery Point Objectives). Therefore, it is necessary to evaluate the current vulnerability status of the information system by applying effective measures based on cost efficiency and by accurately assigning the priority of each component. This paper describes the methods of applying effective BC measures of information systems, specific details of these measures and the work required for the proper operation of backup systems, as well as the managed service for implementation of the BC measures.

Keywords

Disaster Recovery(DR) service, outsourcing, system operation, ITIL (IT Infrastructure Library), backup system

1. Introduction

Disaster recovery (DR) procedures composed of measures such as information backup systems and storage of backup tapes in remote locations have a history of more than 30 years and are not at all a new idea. However, the recent rise of the business continuity (BC) idea has brought great advancement to the DR measures for information systems, particularly in the methods of study and in the actual measures to be taken.

There are two major points in this advancement.

One is the explicit incorporation of the study step based on the above results, which consists of clarification of the minimum IT services required for BC and the determination of the scope and details of measures to be applied to the IT systems that are in use as existing DR measures.

The other point is the clarification of the necessity of the PDCA cycle, which is based on the idea that BC measures will never be completed once they have been applied and they must be administered optimally while reviewing them continuously.

These issues have allowed the BC measures for information systems to reflect the actual businesses and business strategies of the enterprise or organization permanently and correctly, at the same time as optimizing the costs for these operations.

Nevertheless, when an enterprise attempts to maintain and manage these measures, it requires the services of engineers with expert knowledge of BC and IT for a long time. This makes it extremely difficult for ordinary enterprises and organizations to maintain and implement all of the desirable BC measures and PDCA cycles at their own expense.

Based on the above background, more and more enterprises and organizations are recently beginning to utilize the managed services of BC measures for information systems in order to ensure BC with higher cost efficiencies.

2. Methods of BC Measures

BIA (Business Impact Analysis) can clarify the objectives for the recovery of IT systems including RTO (Recovery Time Objective), RPO (Recovery Point Objective) and RLO (Recovery Level Objective). In addition, it also clarifies the vulnerability to disasters of the information systems that are currently active.

Moreover, multiple BC measure policies are elaborated using the above system recovery objectives as the input information, and the actual policy to be applied is selected from them by considering cost efficiency and the overall budget. One of the important issues in this selection is the study into the means of application of the BC measures.

The means of BC measures applications can roughly be classified into the following four methods (see **Table**).

(1) BC Measures Using In-House Facilities
This method runs both the main and backup systems by making use of the data center and operations engineers employed by each enterprise. It is often applied by relatively big enterprises that are capable of distributing engineers in multiple sites all over the country, such as manufacturing businesses.

Table Means of BC measures implementation.

		Use of in-house facilities	Mutual use of outside facilities	Use of outsourcing or vendor service			
		① Backup environment using the enterprise's facilities	② Mutual use of facilities between other enterprises	③ Outsourcing of both main and backup systems	④ Outsourcing of main system	⑤ Outsourcing of backup system only	⑥ Use of service provided by vendor
Explanation of methods		Construction of backup system using own facilities in a remote site.	Construction of backup system with another enterprise in confidential relationship including group companies	Outsourcing of both the main and backup systems.	Displacement of the main system in a data center. (Backup system is either not prepared or installed in-house)	Outsourcing of backup system only.	Use of service including a shared service, storage utility or remote backup service.
Examples of implementation	Overseas	○	○	○	○	△	○
	Japan	○	△	○	○	△	△
Advantages		Easy governance.	Low cost.	Reduction in total IT costs.	Immediate measures at low cost.	Effective for enterprises without remote site.	DR at lost cost.
Disadvantages		Very high operation and maintenance costs.	Operation is not guaranteed due to possible differences in enterprise scale, business method, system architecture or tools used.	Necessity of care in outsourcer control so that corporate governance can be ensured.	This is a preliminary action in most cases.	Labor taken consistently between main and backup operations. Possibility of high network costs.	Difficulty in selecting optimum services due to the market immaturity of such services.
Future market trend expectations		Reduces except among some big enterprises.	Reduces except among some big enterprises	Increases following increases in the importance of IT.	Increases as a short-term BC measure.	Increases following demand from enterprises without remote sites.	Increases following service vendor maturity.

○: Used   △: Not used

This method makes it possible to easily apply corporate governance but the cost of appointing dedicated personnel, maintenance and operations might be very high.

(2) Backup System Using Outside Facilities

In this method, an enterprise installs the backup system in the center of another enterprise with which it has a confidential relationship, such as a group company or even a competitor. The second enterprise reciprocally installs its backup system in the data center of the first enterprise. As the recovery in this method would rely on the data center facilities and recovery personnel of the other enterprise, the business scales, business modes, system architectures and tools used by the two enterprises should be identical. As a result, this method is hardly used at all in Japan, except for mutual backup between large enterprises of the same business group.

(3) Outsourcing of Both Main and Backup Systems to a Vendor

This method consists of outsourcing both the main and the backup systems to a vendor. It enables efficient, flexible BC because outsourcing can reduce the operations costs of the main system and allows part of the saved expenses to be appropriated for the operation of the backup system. As the operation service level will not be changed even when the main system is switched to the backup system in the case of a disaster, the information system personnel can provide stable IT services to the end users.

(4) Outsourcing of Only the Main System to a Vendor

This method consists of outsourcing of only the main system to a vendor.

When the backup system cannot be built immediately due to problems of cost, etc., it is an immediately effective measure to transfer the main system to a data center building that has a quake-absorbing or quake-resistant construction and that sufficient countermeasures are taken against fire, power failure and security attacks.

It is expected that simply moving the main system to a data center can improve the current vulnerability drastically and reduce the residual risk, though this would also be dependent on the current system environment.

Nevertheless, it should be noted that this method is after all only a preliminary measure. To prepare for the unexpected, it is required to install a backup system in a remote location using one of other methods.

There are also cases in which the backup system is installed in the data center of the enterprise's own premises and the main system is outsourced to a vendor. We classified such a method together with the present method because the reasons and advantages are almost identical to the present method.

(5) Outsourcing of Only the Backup System to a Vendor

In this method, the main system is operated in the enterprise's own data center and only the backup system is outsourced to a vendor.

This method has been applied actually in enterprises and organizations that do not have business sites in remote locations, such as a regional bank or local government.

The problems accompanying this method may include the consistency between the operations of the main and backup sites and the network costs.

(6) Backup System Making Use of Services Provided by a Vendor

This method implements a backup system making use of services provided by a vendor. It includes a sharing type service that shares the backup system resources with multiple customers in remote locations that would not be affected simultaneously to the main site in the case of a disaster such as an earthquake and a remote data backup type service using storage devices.

Many vendors in North America and Europe provide this kind of service but, in Japan, selection of an optimum service is difficult due to the immaturity of the market in this field.

3. Services for System Operation Required for BC/DR

This section deals with the operations required for the main site and backup system in implementing BC/DR.

An operation design matching the requirements is necessary before installation of an operation. The operation design for a system with backup differs from the following aspects to the operation design of a system without the backup (**Fig. 1**).

① Operation of the main site and backup system at normal times (data linkage, etc.) should be considered.

② Rehearsal for switching the main site to the backup system (fault training) is essential.

③ Operation of the backup system after switching from the main site should be considered.

The following describes the operation design policy based on the above considerations.

(1) Operation of the Main Site and Backup System at Normal Times

Preparation for system switching is always necessary for the managed operation of routine functions. As the composition and configuration of the main site and backup site are not completely identical, it is necessary to place emphasis on the design of the following management actions under the ITIL managing process.

・Incident Management, Problem Management

The method, procedure and flow of management based on the interlocking of the two sites should be clarified for the management of various incidents, particularly for the man-
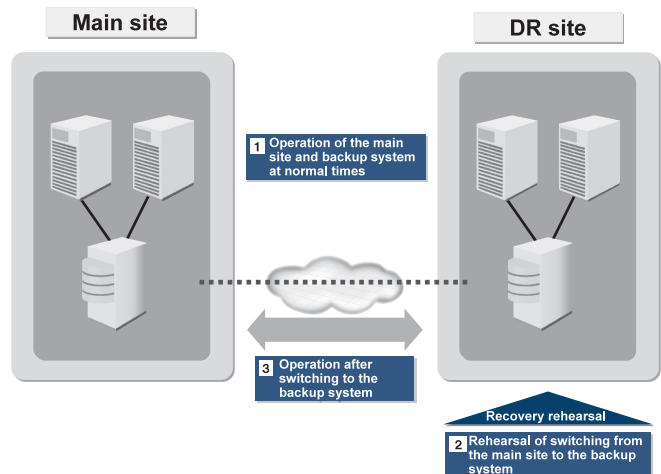
Fig. 1 System operation design.

agement of incidents/problems in data linkage.
・Revision Management, Release Management
The backup system should be managed in synchronization with the main site. The method, procedure and flow of management should be clarified for the application of revisions and new releases or in the case of a disaster.
・Configuration Management
It is necessary to define for a management system whether the configuration management database (CMDB) is run independently or synchronously on the main site and backup system, as well as the method procedure and flow in the case of the modification management of a CI.
(2) Rehearsal of Switching from the Main Site to the Backup System
The operators (including operation SEs and ordinary operators) should understand the necessity for including a switching rehearsal as one of the management requirements of the operation management design in (1) above. The operation management design should decide the management method and system by visualizing various operations as management processes, including data synchronization after site switching and business job processing.
(3) Operation after Switching to the Backup System
The operation design should also define this item in advance, as one of the disaster countermeasures. After reserving the

means available in the case of a disaster, the operation design should define the prearrangement, manager's work, operation SE's work and the operator's work as operation functions.
The operation design for the backup system should design the operation management, service support, service delivery, monitoring environment and installations for the operation of the backup system.

4. Services for the Implementation of BC/DR

At NEC, we have prepared a range of services for facilitating the implementation of BC/DR by enterprises and organizations. We have a more than 25 years history of successful achievements of services including outsourcing, ASP/AIP and network circuits. We have also handled several thousands of servers and currently have 5,000 users with us. This section describes the managed services provided by us.
・Data Center Services
At NEC, we have prepared data centers with a total area of more than $50,000m^2$ nationwide, which can be selected according to the needs of each customer (**Fig. 2**). Also, we are continuing efforts to achieve the highest level of security as one of the leading outsourcers in Japan, and have completed compliances with various security requirements including
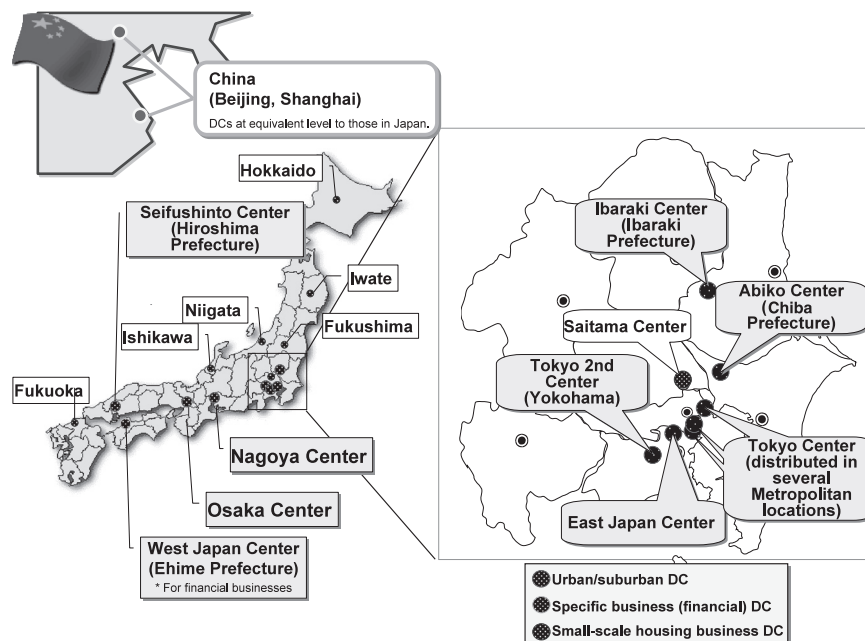

Fig. 2 NEC's Data Centers.

certification by the ISMS Compliance Assessment System, acquisition of Privacy Mark and compliance with the J-SOX law.

In 2005, NEC's Ibaraki Data Center received an audit by SunGard on its appropriateness as a recovery center based on the audit standard used by SunGard in the establishment of recovery centers in the USA. As a result of this audit, the Ibaraki Data Center was certified to clear the SunGard standard requirements.

· Data Backup Services

Services for backing up data in the data centers of remote locations are provided in order to meet the RPO requirements for the recovery of each business.

The services include remote replication using the storage function, remote backup that compresses data obtained by daily or weekly backup and transfers it to low-cost devices in remote locations, data backup in tape to be transported later, and remote storage. Each customer can select an appropriate service from among these according to the value of its RPO. The data transfer circuits for use in these services are determined by investigating into the specific business needs of the various enterprises and the data quantities of the target systems.

· System Recovery Services

These are the hosting services of backup systems installed in data centers in remote locations. The backup systems can be prepared either to the same configuration as the main systems or in a reduced configuration using the virtual server function.

· Managed Operation Services

These services offer the ITIL (IT Infrastructure Library)-based operation processes that are necessary for both the main and DR sites to achieve BC.

Before operation, an operation design in accordance with each customer's requirements is necessary at the beginning of the service.

5. Conclusion

In the above, we introduced our managed services for use in the implementation of BC. We are planning to continue to apply improvements to these services in the future. It is our belief that effective use of the NEC managed services will make it possible to achieve and ensure BC at optimized costs.

---

* The corporate names and product names are trademarks or registered trademarks of their respective owners.

Authors' Profiles

OGATA Hideyuki
Consulting Manager,
Managed Services Division,
Systems Services Operations Unit,
NEC Corporation

OHSUKA Hideo
Expert,
Managed Services Division,
Systems Services Operations Unit,
NEC Corporation

ABE Akiko
Assistant Manager,
Managed Services Division,
Systems Services Operations Unit,
NEC Corporation

KONDA Nobuhiko
Manager,
Managed Services Design and Operations Division,
Systems Services Operations Unit,
NEC Corporation

HIRAI Masaki
Assistant Manager,
Managed Services Design and Operations Division,
Systems Services Operations Unit,
NEC Corporation

SHIMAZAKI Tomoyuki
Staff,
Managed Services Design and Operations Division,
Systems Services Operations Unit,
NEC Corporation