Strengthening Service Management by Comprehensive Analysis of Incidents

● Takashi Sano ● Haruhisa Suzuki

(Manuscript received November 11, 2009)

The complexity of the information systems (business applications and infrastructure) that support business enterprises has been increasing year on year, and in accordance with this the difficulty of operating and maintaining them has also been increasing. Daily incidents need to be dealt with in the places where these systems are operated, and there are not many projects for which the overall tendencies of those incidents can be determined, and the stage of solving their root cause or making proposals for improvement is seldom reached. To support the smooth operation of business, the Advanced Portfolio Management (APM) Competency Department in Fujitsu (as of December 21, 2009) has established a technique for comprehensive incident analysis, such as those incidents arising from inquiries and messages from the infrastructure and applications, from the perspectives of service management, users, and business operations. This technique targets busy fields in the operation and maintenance process and is composed of a service and templates that ease the burden placed on service managers in terms of time and effort, helping them find overall tendencies and root causes. This paper describes the technique for comprehensive incident analysis, and examines the effects of that technique by looking at actual examples.

1. Introduction

Information systems operated by customer companies can have a wide range of purposes such as use for quarterly disclosure of account settlement, internal control (compliance with JSOX), compliance with the International Financial Reporting Standards (IFRS), business continuity and disaster recovery (BC/DR), compliance with environmental protection regulations, ensuring security and making corporate organizational changes. For smooth, safe and secure implementation of business, companies need to respond promptly to various changes in the environment that surrounds them, and it is becoming increasingly important to operate information systems. Information systems that support customers' businesses are composed of various types of hardware (HW) and the operating systems (OS), middleware (MW) and applications installed on them. To ensure smooth operations, a company's information systems department must have an accurate understanding of the conditions including the lifecycles of these HW, OS, MW and applications for their appropriate maintenance and operation. Meanwhile, the complexity of business applications and infrastructure and the difficulty of operating and maintaining them are increasing year on year.

To support smooth business operations, Fujitsu has established a comprehensive technique for analyzing them with the focus on incidents that occur on a daily basis so as to strengthen the service management area. This paper describes the techniques used in this comprehensive analysis and its effects by looking at actual examples.

2. Incidents occurring on a daily basis

One of the services that the information systems department of a company provides is responding to inquiries. While the way in which this service is provided and its details may vary depending on the customer, in general, the services are composed of a service layer focused on infrastructure, another service layer focused on business applications, and a combination of the two (**Figure 1**).

Day-to-day operations involve an enormous amount of incoming inquiries from user departments ranging from common operational inquiries that arise when operating computers, to requests for functional improvements or changes to applications. These inquiries are generally handled by a department that is often referred to as a call center, help desk, or business support desk.

At the site of operation, the conditions of operation are monitored and judged based on various messages from business applications and HW/OS/MW/networks to ensure smooth operation of information systems. Essentially, these inquiries and the conditions of system operation should be centrally managed, but they are often managed separately on the business operations layer and infrastructure layer. Although these inquiries are complaints that hamper business operations, they are also a source of valuable information for a company for the following reasons:

1) Reducing the number of inquiries in itself leads to faster operations and lower costs.
2) Analyzing the details of inquiries clarifies the problems in day-to-day business operations and provides materials for improvement plans.

The IT Infrastructure Library (ITIL) defines an incident as “an unplanned interruption to an IT service or a reduction in the quality of an IT service” including failures, questions and inquiries that are reported by users (normally through telephone calls made to a service desk) or by technical staff, or that are automatically detected or reported by event-monitoring tools.[1),2)]

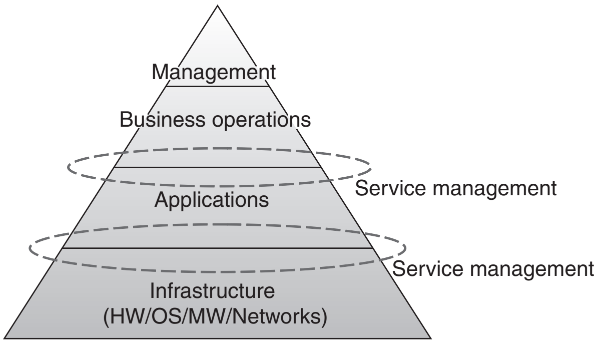


Figure 1
Two-layer service management supporting customers’ businesses.

3. Outline of comprehensive incident analysis

Conventionally, incident analysis was conducted from the perspective of technology but recently comprehensive incident analysis including the perspectives of service management, users, and service provision in addition to technology has become necessary to support smooth business operations.

To address this issue, the Fujitsu APM Competency Department (hereafter “APM Competency Department”) analyzes incidents, makes suggestions for operational service improvements and promotes activities leading to the stable operation of systems. The comprehensive incident analysis proposed by the APM Competency Department consists of the following five processes (**Figure 2**):

1) Recording incidents
2) Understanding and managing incidents
3) Grasping “problems” from incidents
4) Identifying the root cause with “*somo*

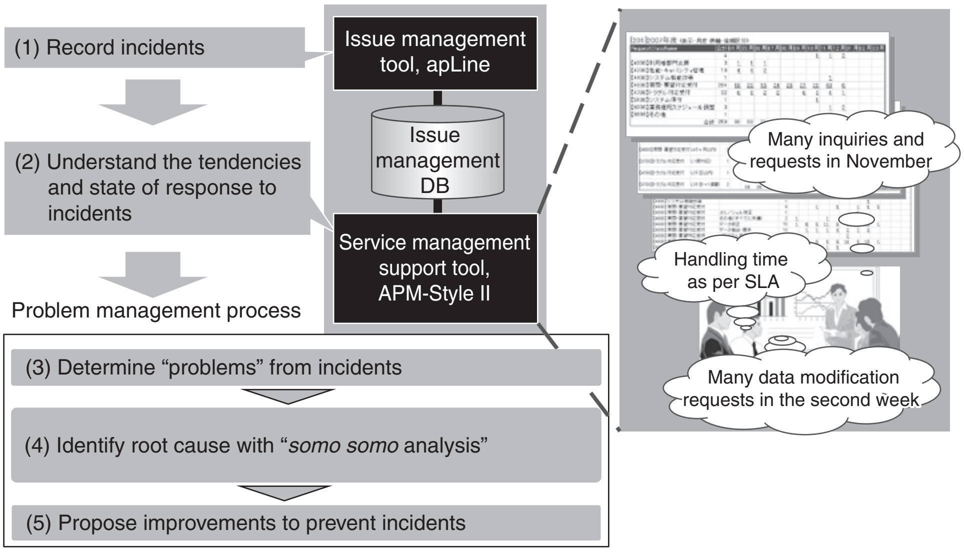

(1) Record incidents
Issue management tool, apLine
Issue management DB
(2) Understand the tendencies and state of response to incidents
Service management support tool, APM-Style II
Problem management process
(3) Determine "problems" from incidents
(4) Identify root cause with "*somo somo* analysis"
(5) Propose improvements to prevent incidents
Many inquiries and requests in November
Handling time as per SLA
Many data modification requests in the second week

Figure 2
Flow of comprehensive analysis of incidents proposed by Fujitsu's APM service center.

somo[note)] analysis"

5) Proposing improvements to prevent the occurrence of incidents

The following sections describe these processes.

4. Recording incidents

About half of the incidents received from user departments are inquiries and requests for operation. Incidents that are generally counted as problem responses and require program reconstruction or modification account for one-fourth; and the remaining one-fourth are incidents requiring schedule adjustments (data provided by the APM Competency Department).

As can be estimated from this breakdown, incidents that account for three-fourths, or those other than problem responses, are directly solved by the people in charge and whether or not these incidents are recorded depends on the method of making personal records in many projects.

The APM Competency Department is striving to clarify the information required for incident analysis and promoting the recording of information to make it established as a basic activity of a project. The types of information to be recorded include:

1) Time axis

Concentrated at the end of a month, beginning of a week, or right after switching, etc.

2) User

Person in a management position, newcomer, age group, degree of familiarity with computers, etc.

3) Pattern of operation

Canceled after price revision, dealt with after changing planned value, etc.

4) Place and organization

Country and location, name of business establishment, name or organization, etc.

5) Handling time

Two days minimum before solution, to be reurged, etc.

6) Cause and location of origin

- HW, OS, MW, network, terminal, application program, data, operation
- Security, recovery, backup, change management, configuration management, release management

note) *Somo somo* means "something that originally should have been this way, when thought about (considered) carefully."

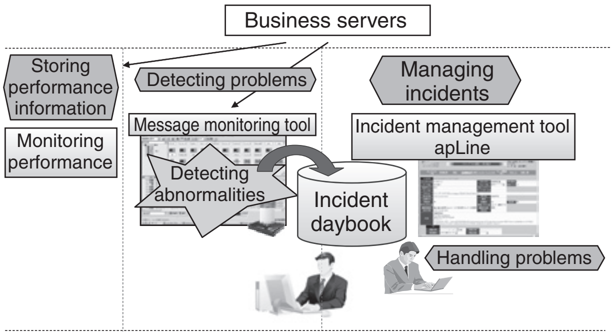
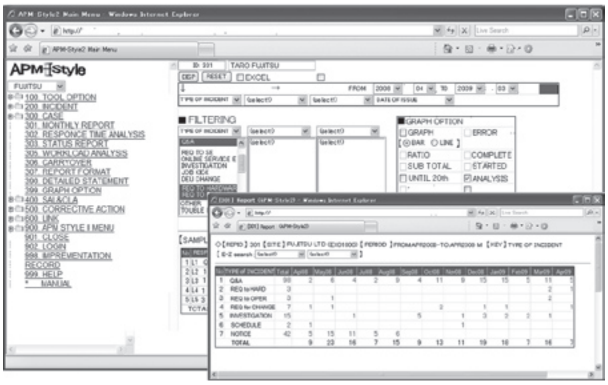


Figure 3
Structure for getting incident information from HW/OS/MW automatically.



ID: 301 TARO FUJITSU

□ EXCEL

FROM 2008 04 TO 2009 03

TYPE OF INCIDENT (select) (select) DATE OF ISSUE

■ FILTERING

TYPE OF INCIDENT (select) (select)

Q&A
REQ TO SE
ONLINE SERVICE
INVESTIGATION
JOB KICK
DEU CHANGE
REQ TO HARDWARE
REQ TO
OTHER
TOUBLE

■ GRAPH OPTION

□ GRAPH □ ERROR
[● BAR ○ LINE]
□ RATIO □ COMPLETE
□ SUB TOTAL □ STARTED
□ UNTIL 20th ☑ ANALYSIS

[REPID] 301 [SITE] FUJITSU LTD [PERIOD] FROMAPR2008-TOAPR2009 M [KEY] TYPE OF INCIDENT

No.	TYPE of INCIDENT	Total	Apr08	May08	Jun08	Jul08	Aug08	Sep08	Oct08	Nov08	Dec08	Jan09	Feb09	Mar09	Apr09
1	Q&A	98	2	6	4	2	9	4	11	9	15	15	5	11	5
2	REQ to HARD	3												2	1
3	REQ to OPER	3		1										2	
4	REQ for CHANGE	7	1	1					2		1	1			1
5	INVESTIGATION	15			1			5		1	3	2	2	1	
6	SCHEDULE	2	1							1					
7	NOTICE	42	5	15	11	5	6								
	TOTAL		9	23	16	7	15	9	13	11	19	18	7	16	3

Figure 4
Example of display of service management tool: APM-Style II.

- Availability management, capacity management, continuity management, overhead (human, infrastructure and application)
- Test environment, lack of testing, display method, input method, as per specification

In addition, standardization of control items such as the request classification, cause classification and customer code for individual incidents is promoted to use as models for Fujitsu's operation and maintenance to broaden the range of information sharing.

On the sites of operation, various types of message information output from application programs and HW/OS/MW/networks are handled as incidents in addition to incidents received by people.

The APM Competency Department provides a service for building a framework including processes and tools that automatically record these types of information without omission. A structure for automatic capturing of incident information by using the incident management tool apLine, which is in practical use in Fujitsu's internal system operation, is shown in **Figure 3**.

5. Understanding and managing incidents

The process of understanding the state of response to individual incidents and reporting the result is implemented on the site of operation. However, understanding and reporting on all incidents is very troublesome.

The APM Competency Department has modeled the methods of understanding the conditions of and managing incidents, and offers them as a service management tool called APM-Style II—a framework capable of creating data that allow efficient management by top management. **Figure 4** shows an example of data created with APM-Style II.

6. Grasping problems from incidents

The APM Competency Department recommends that any incident generated in a customer's information systems department that renders or is likely to render the systems incapable of maintaining the service level should be regarded as a critical problem and that problem and its cause should be analyzed by the service provider. In a similar way, the APM Competency Department recommends that multiple similar incidents that are generated should be regarded as a common problem, the tendencies should be understood and the problem and its cause should be analyzed by the service provider. On top of the conventional methods for identifying problems, methods based on actual incident analysis with the perspectives of business operations, users and service providers added have been modeled.

The following subsections describe these models and give case examples.

6.1 Case 1: Network problem

6.1.1 Conventional method of identifying problems

A few incidents that cause network problems were received every month. In the past, the cause was investigated based on the concept that the network quality was poor, which resulted in a cause being identified as line interruption on the part of the network provider. The network provider reported assumed causes to be unstable voltage (due to lightning strikes, etc.), interruption because of engineering work, inadequate line contact connection and operation error. In response, measures were taken to maintain the network line quality and duplicate and triplicate the line.

These are no wrong measures to take, but they have their limitations and the problem must be seen also from the service provider's perspective. First, the description of the incident must be modified into an expression incorporating the perspectives of business operations and users.

6.1.2 Method of identifying problems from the service provider's perspective

A few incidents in which XX operations were interrupted after YY o'clock due to network problems were received every month. The extent of the impact on the operations was investigated from the perspective of users. The findings showed that (i) processes were interrupted halfway, (ii) whether they should be redone was not clear, and (iii) the terminals did not restart automatically. As a result, the problems were identified to be the interruption of operations due to network problems and the difficulty in resuming operations, rather than the network problems themselves. As measures to take in view of the value of service continuity and business, a mechanism to allow easy querying on the status of processes halfway through and a system to send messages requesting a manual restart to other terminals were implemented. These two measures led to the problems being resolved.

When the cause of one or more incidents was unknown, the cause was often identified as a result of considering multiple similar incidents. The ITIL recommends detecting the problem to solve the root cause.[1),2)] Case 2 below, in which incidents were solved by the service desk but identifying the decisive cause was unsuccessful and similar incidents recurred, describes the method of identifying the problem.

6.2 Case 2: Service desk

Multiple incidents such as inquiries from user departments and messages from HW/OS/MW were plotted on a graph with reference to the time axis (**Figure 5**) to gain an understanding of the tendencies, which have been analyzed from three viewpoints (time of incident occurrence, characteristics of time of occurrence for each operation and irregularity in the date of occurrence). Concerning the time period of occurrence, incidents concentrated in the first period of the morning, first half of the afternoon and second half of the afternoon. The observed characteristics of time period of occurrence for each operation included a tendency toward incidents concentrating in the first half of the afternoon with the ZZ operation. In relation to the irregular date of occurrence, incidents were concentrated on the days following the days with concentrated work at the end of the month and week. As a result, many process warnings were generated in the peak time periods when dealing with the ZZ operation, and abnormal termination of batch processing occurred on the days following the peak days of dealing with the ZZ operation, which have been regarded as the problems.

To make such analysis possible, it is important to put in place all information required for analysis mentioned above including

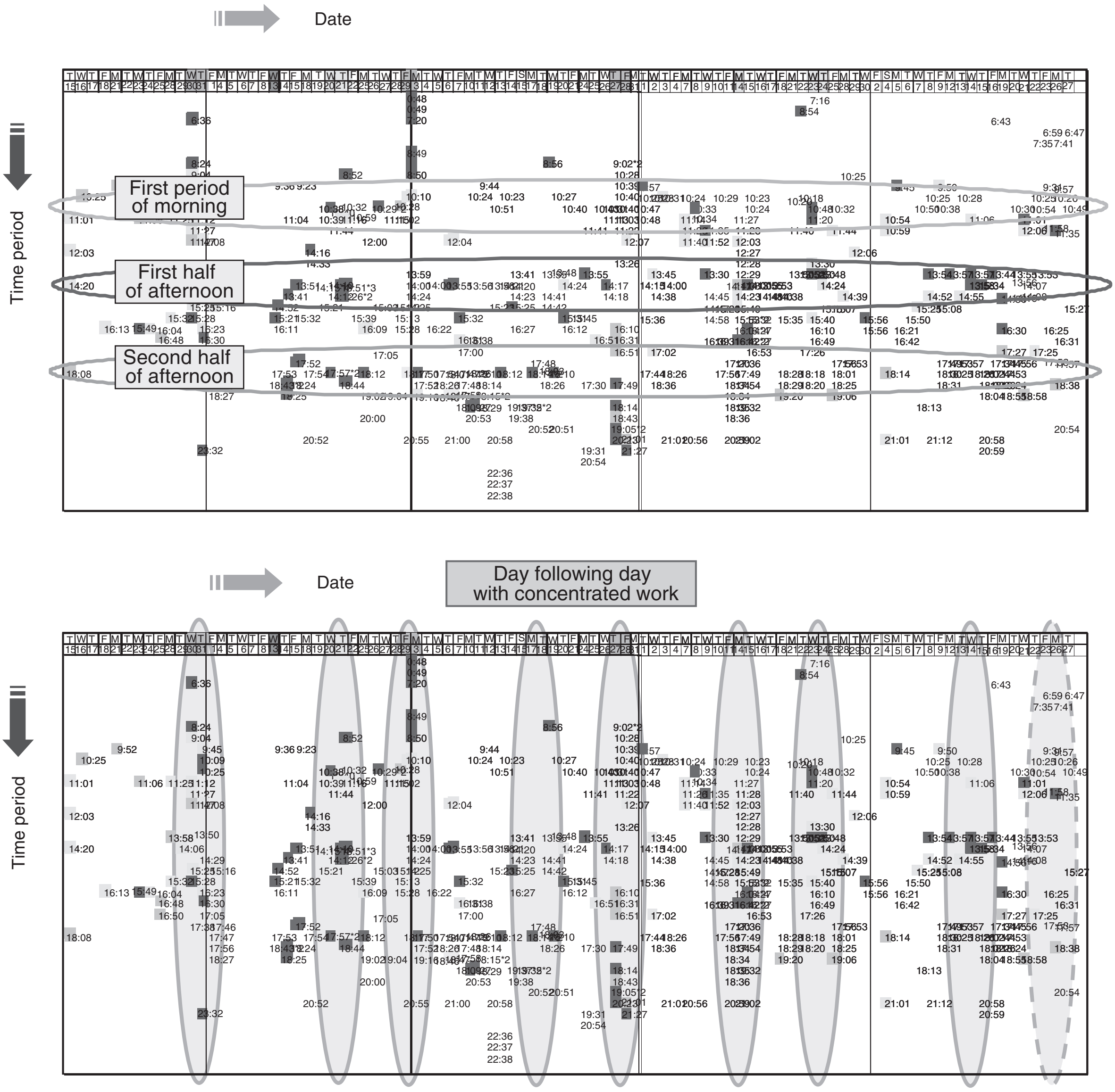


Figure 5
Example of tendency analysis viewed from time and day of incident occurrence.

all incidents such as inquiries from user departments and messages from HW/OS/MW in addition to problems.

7. Identification of the root cause by *somo somo* analysis

Techniques for finding the root cause of a problem are described in detail in technical books on quality control and cause-finding workshops are often held as well. However, the conventional techniques are believed to require the guidance of experts on causal analysis and have not been appropriate for use in the actual sites of business operations.

To support smooth business operations, the APM Competency Department has established a technique called "*somo somo* analysis," which is intended for use in analyzing the cause of a problem from four perspectives (technology, business operations, users and service provision). The distinguishing features of this technique include not looking for the culprit, not requiring expertise on root cause analysis and not narrowing down to one root cause. Repeating the identification of a cause by asking questions in accordance with the template below (seven *somo somo*) has led to successful identification of the root cause.

- *Somo somo* 1 "Not decided"
- *Somo somo* 2 "Not known"
- *Somo somo* 3 "Known but not implemented"
- *Somo somo* 4 "Rules are strange"
- *Somo somo* 5 "Rules have become obsolete"
- *Somo somo* 6 "Training is inadequate"
- *Somo somo* 7 "Difficult to implement"

8. Proposing improvements to prevent the occurrence of incidents

Replacing the root cause identified in the *somo somo* analysis with seven "*dekiru* (can do)" respectively has provided insight in terms of which measures to take.

- *Dekiru* 1 "Let's decide"
- *Dekiru* 2 "Let's make it known"
- *Dekiru* 3 "Let's implement if known"
- *Dekiru* 4 "Let's correct the rules"
- *Dekiru* 5 "Let's update the rules to prevent obsolescence"
- *Dekiru* 6 "Let's make training possible"
- *Dekiru* 7 "Let's be ingenious and make it easy to implement"

The APM Competency Department plans to offer as a service the activities leading up to the proposal of improvements.

9. Effects of a project

This section presents the effects of a project in which comprehensive incident analysis and improvements have been implemented.

A survey conducted by the APM Competency Department shows that an average of 10 incidents occurred monthly that were dealt with by a customer information systems department and Fujitsu's SEs. Based on the results of comprehensive analysis of HW/OS/MW/application incidents by SEs, the following three activities have been carried out:

1) Updating HW led to a reduction of incidents from a monthly average of 2.3 to 0.
2) Improving application quality led to a reduction of incidents from a monthly average of 2 to 0.
3) The "*somo somo* analysis" was applied to incidents arising from the external connection system and measures were taken in cooperation with the customer, which resulted in a reduction of incidents from a monthly average of 5 to 0.

In many cases, the occurrence of incidents can be prevented by conducting training, for which some issues must be addressed such as ensuring training facilities and time for training. Fujitsu will continue to advocate the importance of training to customer companies.

10. Conclusion

This paper has focused on incidents that occur in the operation of corporate systems and described comprehensive incident analysis as an approach to ensuring customers' smooth implementation of business operations. We intend to continuously improve services and refine and improve Fujitsu products by comprehensively analyzing inquiries from user departments and messages from HW/OS/MW/applications, so as to help our customers have safe and secure business operations.

References

1) itSMF Japan: ITIL Service Operation. (in Japanese), TSO, pp. 33–67, 2008.
2) ITSM Library: IT Service Management Based on ITIL V3: A Pocket Guide. TSO, 2009.

Takashi Sano
Fujitsu Ltd.

Mr. Sano received a B.S. degree in Precision Engineering and an M.S. degree in Information Engineering from Hokkaido University, Japan in 1975 and 1977, respectively. He joined Fujitsu Ltd. in 1977 and was engaged in developing and maintaining application programs. He moved to Fujitsu Services Ltd. in the UK in 1999 and returned to Fujitsu Ltd. in 2003. Currently, he is engaged in developing a service for operating and maintaining application programs. In 2006, he was a member of the group that translated ITIL Application Management into Japanese.

Haruhisa Suzuki
Fujitsu Ltd.

Mr. Suzuki received a B.S. degree in Engineering and an M.Eng from the University of Electro-Communications, Japan in 1975 and 1977, respectively. He joined Fujitsu Ltd. in 1977 and was engaged in developing several IT systems. He moved to Fujitsu España S.A. in 1979 and returned to Fujitsu Ltd. in 1981. Currently, he is engaged in improving the service quality of operation and maintenance for several systems. He was a member of the group that translated ITIL Service Design into Japanese.