Information Engineering Express
International Institute of Applied Informatics
2026, Vol. 12, No. 1, IEE811

A Study on Emergency Response Management for System Failures using Project Management Knowledge

Atsushi Shimoda *

Abstract

Many companies prepare action procedures for emergency responses to system failures. Traditionally, these are based on procedures stipulated in international standards and best practices. However, they present only procedures and do not provide specific perspectives that organizations should consider in uncertain situations. Therefore, if an event that is not described in the action procedure manual occurs, there is a possibility that the site will be confused and rational judgment will not be possible. In this research, by utilizing project management knowledge, specific viewpoints that organizations should keep in mind in uncertain situations are presented. The effectiveness of the proposed method is shown by a case study of system failure.
Keywords: System failure, Emergency response management, ITIL, PMBOK, BCP, BCM

1 Introduction

With the progress of the information society, the degree of dependence on information systems in social life is steadily increasing. This trend is accelerating due to the spread of DX (Digital Transformation). In other words, stable operation of information systems is a prerequisite for maintaining a safe and secure social life. However, the scale and complexity of information systems are increasing steadily, and it is becoming difficult to maintain quality within a range that matches the return on investment. In addition, as exemplified by IoT, the range of interconnections between information systems is expanding, thereby increasing the risk that a failure in one system will propagate to others. Against this background, the number of system failures is increasing year by year, and there is an urgent need to improve the reliability of information systems as critical infrastructure [1].

Information system failures are caused by various factors, but can be broadly classified into four categories [2]. Here, "intentional factors" such as cyberattacks, "unintentional factors" such as operation/setting errors and program flaws, "disasters and illnesses" such as earthquakes, floods, lightning strikes, and fires, It is categorized into 4 types of "Ripple effects from obstacles in other fields" such as disruption of water supply and disruption of water supply. Countermeasures and responses are different for each of these factors, but this paper focuses on the "unintentional factors" among them. "Unintentional factors" can be further subdivided. For

* Chiba Institute of Technology, Chiba, Japan

example, data from a survey of the causes of system failures at financial institutions shows that approximately 40% of failures are caused by business application programs (APs), 20% are system infrastructure failures, 10% are configuration errors, and 10% are operational errors [3]. Especially in system failures caused by "unintentional factors" such as defects in business applications, it is difficult for developers and operators to notice the problem, and in many cases it takes time to identify the cause of the failure. It tends to expand.

Conventionally, various efforts have been vigorously advanced to prevent the occurrence of system failures. However, it is difficult to completely prevent the occurrence of failures in preventive measures that can be implemented within the scope of the return on investment. Therefore, on the assumption that system failures will occur, the concept of reducing the extent of damage and the period until recovery has been emphasized. This concept expresses "flexible resilience that can quickly restore the function as a whole even if part of the function of the social system stops", and it is spreading as "resilience" [4]. Businesses and public institutions are implementing this idea as BCP (Business continuity planning), which is a plan to prevent the suspension of business, and BCM (Business continuity management), which is an operation method. There is.

The previously mentioned BCP stipulates a wide range of matters, from emergency response immediately after an abnormal situation occurs to resolution and recovery. Above all, it is thought that if a system failure can be prevented from expanding and becoming more serious in the early stages of a system failure, that is, in the emergency response stage, it will be possible to minimize the impact on social life. This concept is at the core of resilience. However, there are some cases in which the damage is expanded or the impact on customers is expanded due to the wrong emergency response. In particular, system failures tend to increase damage over time, and in many cases, temporary countermeasures are required. For example, in recent years, in a situation in which various systems are linked and functioning, the start of operation of another system may expand the influence of the system. Also, even if there is no such explicit deadline, it is often effective to determine a hypothetical deadline and goal and work backwards.

Using this idea, companies have conventionally created and prepared emergency response manuals as a method of coping with system failures. However, it is difficult to cover all cases in the manual. Also, when a system failure occurs, it is common for many unexpected events to occur. As a result, confusion occurred at the site, and taking advantage of this, it became difficult to make calm judgments and identify what should be done without omission, and there were cases where this increased the damage. In such cases, it is effective not only to adopt a strict top-down procedure, but also to share the general behavioral guidelines of the organization and to share comprehensive knowledge from a bottom-up perspective. However, such a leak-free view has not heretofore been provided.

Based on the above background, this paper proposes the use of PM (Project Management) knowledge as a method of organizational response management when a system failure occurs. PM is a temporary and unique activity, but the knowledge that leads to the success of the activity is systematized, and it is possible to use this as a perspective that should be implemented in an emergency without any omissions.

The remainder of this paper is composed as follows. Related works are introduced in Section 2.Emergency response management using PM knowledge is explained in Section 3.The verification results and discussion using case studies are presented in Section 4, and the conclusions are presented in Chapter 5.

2 Related Works

Due to its importance as a work on system failure, various standards and best practices have been published. In addition, there are reports of academic research applying these standards and best practices to actual system operations. They are described in order below.

Table 1 shows standards related to system failure. First, as a standard for IT-BCP (IT-Business Continuity), ISO (International Organization for Standardization, International Organization for Standardization) and IEC (International Electrotechnical Commission) ISO/IEC 27301 [5], and the Ministry of Economy, Trade and Industry has released IT Service Continuity Guidelines [6]. Both have almost the same content, and define a mechanism for IT business continuation from the PDCA point of view. Related standards include ISO/IEC 27001 [7] for ISMS (Information Security Management) and ISO/IEC 20000 [8] for ITSMS (IT Service Management). The former emphasizes the "intentional factors" in Table 1 among the factors hindering IT-BCP, while the latter defines the requirements for providing IT services that include IT-BCP.

Table 1: Standards related to system failure

Standard Coverage	Name of Standard
IT Business Continuity (IT-BCP)	ISO/IEC 27301
	IT Service Continuity Guidelines (Ministry of Economy, Trade and Industry)
Information Security Management (ISMS)	ISO/IEC 27001
IT Service Management (ITSMS)	ISO/IEC 20000
Business Continuity Planning (BCP)	Business Continuity Planning Guidelines (Ministry of Economy, Trade and Industry)
Business Continuity Management (BCMS)	ISO 22301
	Business Continuity Guideline (Cabinet Office)

The above standards are specialized for information systems. Formulation guideline [9], ISO 22301 as BCMS (Business Continuity Management) and Business Continuity Guideline [10] of the Cabinet Office have been published. In these standards, IT-BCP/BCM is positioned as one of the business continuity items. Organizations that provide IT services that have a wide range of social impacts should implement specific organizational management methods to meet the requirements of the standards shown in Table 2 in order to respond to system failures caused by various factors shown in Table 1. It is necessary to define it systematically and to perform regular operation.

On the other hand, ITIL(Information Technology Infrastructure Library) [11] is known as a best practice in the field of information systems, although it is not certified as a standard. ITIL is a set of best practices for IT service management as a whole: strategy, standards, migration, operations and improvement. System failure is related to incident management in service operation, and the procedure shown in Figure 1 is defined. The four processes in the first half of the figure are screening for major incidents. The five processes in the latter half are the responses to major system failures that this paper covers.

Furthermore, studies have been reported that apply the above-mentioned standards and best practices to actual work [12].

The related studies mentioned above have the following problems. The standards and best practices for system failures mentioned at the beginning define the rough items to be implemented and the procedures for doing so. Companies refer to these to create emergency response manuals. However, it is difficult to cover all cases in the manual. In other words, no consideration is given to how to deal with unexpected events that are not described in the manual. In addition, the academic research mentioned at the end is also a case study applied to individual specific tasks, and unexpected events are not considered.

In response to this, this study proposes utilizing PMBOK, the project management body of knowledge, as an action guide for emergency response. Traditionally, PMBOK has mainly been used as the basis for project planning. It has also been used to comprehensively identify the causes of past project failures [13][14]. However, as proposed in this study, it has not been suggested that it be used for ongoing emergency response management. The feasibility of this approach has already been confirmed through a feasibility study using one case study [15]. This paper reports the results of an investigation into whether feasibility can be confirmed across a variety of case studies.

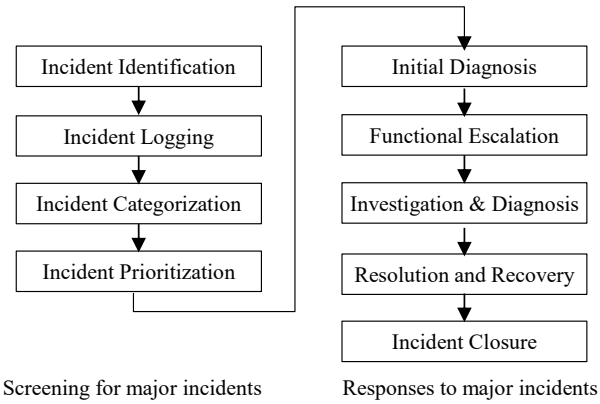

Figure 1: Incident management process by ITIL

3 Emergency Response Management using PM Knowledge

3.1 Consideration of Emergency Response Process

First, the mechanism of loss generation due to system failure will be described. Figure 2 is the standard risk model [16]. Losses in system failures are determined by a combination of causes and effects. Here, the cause is equipment failure, human error, or the like. These causes lead to system failures. However, even if the cause occurs, depending on the impact, it may not lead to a large loss. On the other hand, if there are many users of the system or if the system is connected to other systems, the loss due to system failure will increase. Furthermore, in some cases, the information system has a definite start time for use, or a time at which the connected system starts operating. For example, in the financial system, the time to start connection with other financial systems is fixed, and it is necessary to finish the night batch processing etc. by that time. In addition, railway systems and securities trading systems have a set daily business start time, and if a failure occurs during the night, that time will be the target deadline for failure recovery.

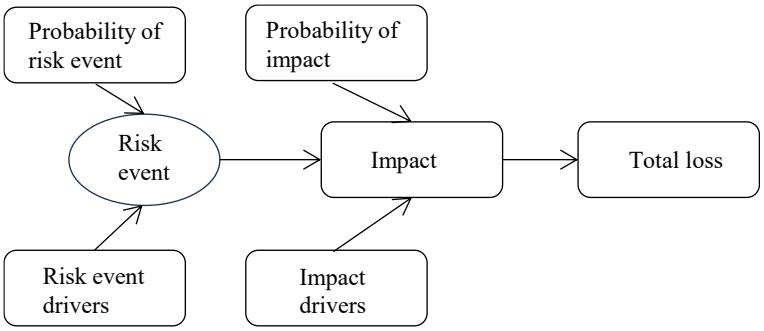

Figure 2: Consideration of loss due to system failure based on the standard risk model

Next, the emergency response process is considered. Figure 3 shows the emergency response process. The horizontal axis is time. Starting from the left side of the figure, when a failure occurs at a certain point in time, an "emergency response" is carried out to quickly restore the system from the failure and minimize the damage. The rough flow of emergency response is generally carried out according to the incident management procedure shown in Figure 1. Specifically, the first four processes determine whether or not the failure is important, and if the failure is determined to be important, the latter five processes are executed. Here, according to the consideration of Figure 1, there may be times when the damage suddenly expands. Therefore, it is reasonable to set this timing as an immediate milestone. On the right side of Figure 2, the timing is marked as the deadline for the impact to spread. In this case, the goal is to complete the incident management procedures by this deadline. Such "emergency response" tasks can be considered a type of project due to their temporary and unique nature. Therefore, there is a possibility that project management knowledge can be applied to emergency response tasks such as those described above.

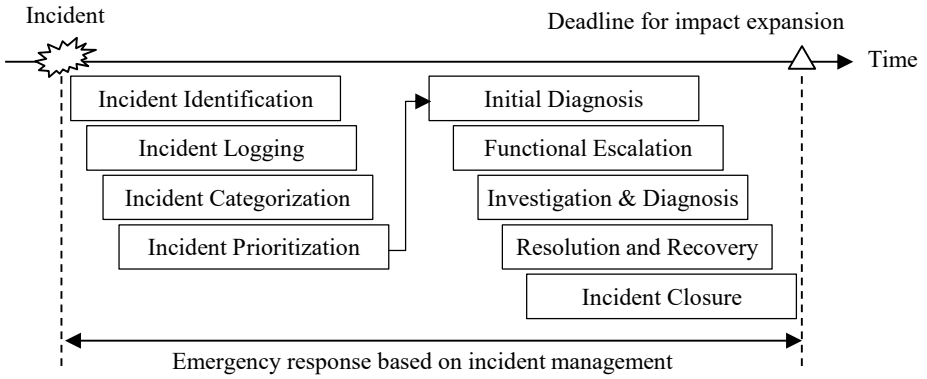

Figure 3: Emergency response process

3.2 Emergency Response Management using PM Knowledge

As mentioned in the previous section, the introduction of PM is proposed by considering emergency response work for disaster recovery with a time limit as a project. It is considered that the following merits can be obtained by introducing PM for emergency response of system failure.

First, the PM's body of knowledge is used as a template for the tasks that are necessary for emergency response. You can proceed systematically. It is also useful as a mechanism for sharing knowledge among multiple organizations when multiple organizations work together to respond to emergencies. The Project Management Body of Knowledge Guide (PMBOK® Guide) is widely used as a PM body of knowledge [17]. Table 2 shows the Process chart of PMBOK. The vertical direction of the table is the PM's knowledge area, and the horizontal direction is the process group. The cells in the table list the processes that should be carried out in each process group, and according to convention, they are listed with the chapter and section numbers of PMBOK (6th edition). By moving the viewpoint to the process group according to the flow of time and proceeding while confirming whether there is any lack of correspondence from the viewpoint of the knowledge area in the vertical direction, it is possible to eliminate the omission of correspondence.

Here, in order to apply PM knowledge to incident management, consider applying the five process groups of PM knowledge to the latter five processes of incident management. Table 3 shows the results. In the left column of the table are the five processes of Incident Management. The right column is the five process groups of PM knowledge. First, the initial diagnosis and escalation of incident management can be aligned with the launch of PM knowledge. The reason for this is that the results of the initial diagnosis of incident management can be linked to goal setting for the launch of PM knowledge. In addition, the escalation of incident management is to correspond to the extraction of stakeholders for the launch of PM knowledge. Incident management investigations and diagnoses can then be aligned with PM knowledge planning. The reason is that the results of investigation and diagnosis can be linked to concrete action plans. Incident management resolution and recovery can then be mapped to PM knowledge execution and monitoring and control. Finally, incident management closings can correspond to PM knowledge closings. As described above, by associating the incident management procedures with the five process groups of PM knowledge, in incident management, the ten knowledge areas associated with the five process groups can be used to examine the emergency response process. It becomes possible to use it as a viewpoint of the item. Specific examples are described in detail in the case studies in the next section.

Table 2: Process chart of PMBOK

	Initiating	Planning	Executing	Monitoring and Conrtolling	Closing
Integration	4.1 Develop Project Charter	4.2 Develop Project Mangement plan	4.3 Direct and Mange project work	4.5 Monitoring and Control project work	4.7 Close Project or Phase
			4.4 Manage Project Knowledge	4.6 Perform Integrated Change Management	
Scope		5.1 Plan Scope Management		5.5 Validate Scope	
		5.2 Collect requirements		5.6 Control Scope	
		5.3 Define Scope			
		5.4 Create WBS			
Schedule		6.1 Plan Schedule Management		6.6 Control Schedule	
		6.2 Define Activities			
		6.3 Sequence Activites			
		6.4 Estimate Activity Durations			
		6.5 Develop Schedule			
Cost		7.1 Plan Cost Management		7.4 Control Costs	
		7.2 Estimate Cost			
		7.3 Determine Budget			
Quality		8.1 Plan Quality Management	8.2 Manage Quality	8.3 Control Quality	
Resource		9.1 Plan Resource Management	9.3 Acquire resources	9.6 Control Resources	
		9.2 Estimate Activity Resources	9.4 Develop Team		
			9.5 Manage Team		
Communication		10.1 Plan Communication Management	10.2 Manage Communications	10.3 Monitor Communications	
Risk		11.1 Plan Risk Management	11.6 Implement Risk Responses	11.7 Monitor Risks	
		11.2 Identify Risks			
		11.3 Perform Qualitative Analysis			
		11.4 Perform Quantitative Analysis			
		11.5 Plan Risk Responses			
Procurement		12.1 Plan Procurement Management	12.2 Conduct Procurements	12.3 Control Procurements	
Stakeholder	13.1 Identify Stakeholders	13.2 Plan Stakeholder Engagement	13.3 Manage Stakeholder Engagement	13.4 Monitor Stakeholder Engagement	

Table 3: Application of PM knowledge (process group) to incident management

Incident Management	PM Knowledge
Initial Diagnosis	Initiation
Functional Escalation	Initiation
Investigation & Diagnosis	Planning
Resolution and Recovery	Execution, Monitoring and Control
Incident Closure	Closing

4 Case Study

4.1 Case Summary

Projects are highly unique activities. For this reason, a common research method is to analyze past cases and generalize them to prepare for future projects [13][14]. Therefore, this study verifies the hypothesis that PM knowledge can serve as a guide for action in emergency response processes, based on an actual system failure case. The target case used a report article of a system failure that occurred in Japan. From among various system failures, as explained in Figure 3, five cases were adopted in which the scope of impact expands after a certain period of time [19]. Table 4 shows a list of examples. The table outlines the industry, causes, impacts and consequences for each case.

Case 1 is a system failure that occurred at a newspaper company. Data transfer was delayed due to a hardware failure in the server that transfers the edited manuscript data to the rotary press. The employees of the newspaper company continued their efforts to prevent suspension of publication before the morning edition printing started. Although the number of pages was insufficient, the suspension was ultimately avoided.

Case 2 is a system failure that occurred in a betting ticket purchase system for a public horse race. The power supply of the data management system was damaged, some of the data was damaged, and the system became unbootable. Racecourse and vendor staff tried to restore the data using backup data, but they were unable to make it in time for the start of the race, so the race was canceled for the day.

Case 3 is a system failure that occurred at a bank. During the relocation of the data center, an event occurred in which the data transfer speed decreased due to a mistake in the relocation of some of the data transfer equipment. The bank's systems staff attempted to switch to a backup system, but were unable to complete all the money transfer transactions during the day.

Case 4 is a system failure that occurred at a bank. There was a human error in setting up the account opening, but in order to cover for that error, a temporary modification was made to the nighttime batch processing, resulting in data inconsistency. The bank's systems staff attempted to resolve the data inconsistency, but were unable to complete the batch processing by the morning's online startup time.

Case 5 is a system failure that occurred at a securities company. A bug in the order server caused the system to fail to boot. System staff at the brokerage firm and staff at the vendor tried to restart the system, but they stopped trading in time for the market to open in the morning.

Table 4: Example list

Case number	Business category	Cause	Impact	Result
1	Newspaper company	Equipment failure	Newspaper publication	Incomplete newspaper publication
2	Public horse racing	Equipment failure	Horse racing start	Race canceled
3	Bank	Human error	Consolidation system start	Transaction stop
4	Bank	Human error	Start of banking business	Transaction stop
5	Securities company	Latent bug	Securities trading business start	Transaction stop

4.2 Case Analysis by Project Management Knowledge

Case 1 will be used as an example to explain the possibility of utilizing PM's body of knowledge for emergency response. Figure 4 shows the VTA (Variation Tree Analysis) [19] to explain the background of the case. VTA is one of the methods used in accident analysis, and is used to identify deviant actions, operations, judgments, etc. that led to the accident from the normal state by writing down the involvement of each entity, such as people, objects, and organizations, in a time series. The vertical axis is the time axis from the bottom to the top, and the horizontal axis is the stakeholder list, with the editorial staff on the left, the editor-in-chief in the middle, and the IT vendor that developed the system on the right. The flow of system failures is described from the bottom left, with the editorial staff and the editor-in-chief making various decisions with the deadline set at the time when the first printing of the first edition was to begin. The IT vendor did not arrive in time for the first printing of the first edition, and did not contribute to the emergency response. Although the manuscript data for the final version of the paper was completed, the data transfer to the rotary press was not completed in time for the start of printing of the first edition, and about half of the pages for which the data transfer was completed in time were printed in black and white instead of the original color. The choice was made to avoid suspension of publication even though the pages were incomplete.

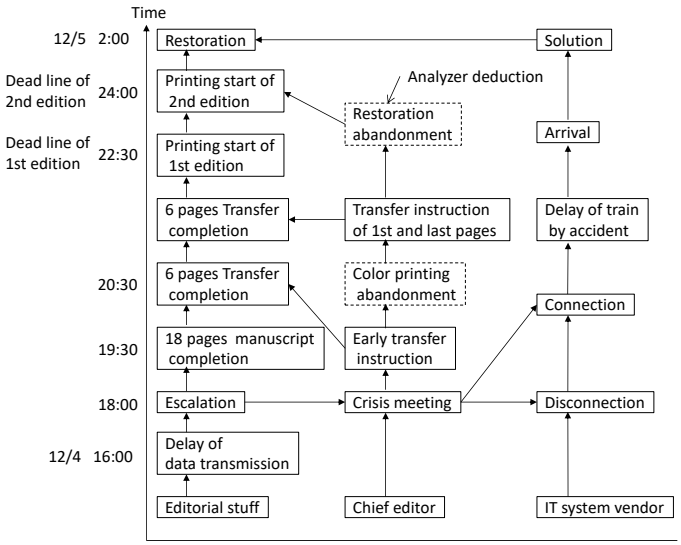

Figure 4: Analysis result by VTA (Case 1)

Table 5 shows the result of applying the case of system failure explained in Figure 4 to PM's body of knowledge. The structure of Table 5 is the same as that of Table 2, and the content of the examples in Figure 4 is applied to the columns describing the management actions to be implemented in the PMBOK Guide. The start of the emergency response project is the time when the system failure is identified, and the end of the project can be regarded as the time when the first printing of the first edition starts. The goal of the project is to start printing a normal morning edition of the paper. The following table describes the management flow for each process group (column) from left to right. In the table, the author's assumptions are marked with ▲.

a) Initiation

A project is unintentionally launched when a system failure is identified. Due to the nature of a highly urgent project, it is necessary at this point to clearly prioritize quality (Q), cost (C), and delivery date (D). That is, assuming publication, delivery time cannot be moved, so D becomes the highest priority, Q of the completed state at that time becomes subordinate, and C has a much lower priority. Another option is to give top priority to the Q of the paper, followed by the D, and if the delivery date is not met, the company chooses to suspend publication. Which priority is chosen depends on the company policy, but in any case, it is important that all concerned parties (project members) have a common understanding of the priority of QCD at this point. In addition, the parties (stakeholders) who should be alarmed should have been listed.

b) Planning

According to the article, the initial goal was to publish the article in full color (scope definition). They must have made a list of what could be done within a limited time (WBS creation). The schedule should have been made by working backward from the time when the first printing of the first edition would start (schedule creation). In risk management, they should have considered the possibility of phasing from best case (normal level of publication) to worst case (suspension of publication). In addition, requests for cooperation from IT vendors were naturally made (procurement plan).

c) Execution

Efforts to complete the manuscript data and transfer as many pages of data as possible were continued. In addition, the roles of those involved should have changed from moment to moment as the situation developed (team organization and management).

d) Monitoring and control

This group of processes is most characteristic of projects with a high degree of urgency. This means that the ever-changing situation must be monitored at a high frequency and controlled to achieve the best possible result. In this case, the choice was made to publish even in an incomplete state, so color printing was given up to reduce the amount of data to be transferred. In addition to the six pages that had already been transferred to the server, the cover page and the final page were sent first in order to maintain a minimum level of presentation (scope monitoring and control). In addition, by receiving information that the IT vendor personnel would be delayed in arriving due to a train accident, they should have listed the risks of not being able to restore the data on the same day and considered publishing the second and subsequent editions in an unstructured manner.

e) Closing

The emergency response was completed when the first printing of the first edition was started, albeit with an incomplete manuscript, and the project was concluded when the system was restored.

Table 5: Analysis result by PM knowledge (Case 1)

	Initiation	Planning	Execution	Monitoring and Control	Closing
Integration	▲QCD prioritization Priority order: D → Q → C	Print all pages in color and meet deadlines.	Create, forward, contact, restore	Monitoring and Control	Recover and start printing
Scope		Scope definition (all pages, color printing)		Scope verification and control (reduced page count, black and white printing)	
		WBS Creation (creation, transfer, communication, recovery)			
Time		Schedule Creation (▲Deadline reverse calculation type)		Schedule Control (▲Deadline reverse calculation type)	
Cost		Cost estimation and budgeting (▲Priority Small)		Cost Control (▲Priority Small)	
Quality		Quality Plan (▲ as usual)	Quality Assurance (▲ as usual)	Quality Control (Time Priority)	
Human Resources		Human Resource Plan (▲ Role assignment, support needed/not needed)	Team organization and management (▲ Real-time command and control.)		
Communication /Stakeholders	Stakeholder Extraction (▲Higher level management)	Communication Plan (▲Communication timing and content)	Information Distribution (▲ Situation Report)	Report of Results (▲Latest News)	
Risk		Risk Management Plan (▲ Complete publication, only partial publication of the first edition, partial publication of the second edition, publication suspended)		Risk Monitoring and Control (▲Delayed arrival of manufacturers, ...)	
Procurement		Procurement Plan (Determine the details of the request for cooperation from the manufacturer)	Procurement Execution (Contact manufacturer)	Procurement Management (Monitor manufacturer activities)	Procurement Termination (Measures to prevent recurrence)

The above explains how to organize the emergency response according to the PM body of knowledge. The facts described in the article and the various management and decision-making activities that were presumed to be implemented based on the content of the article could be applied to any part of the PM body of knowledge. Within the scope of this case study, there was no case in which no applicable body of knowledge could be found. Although it was only one case, the PM body of knowledge enabled us to classify tasks in emergency situations without omission. This suggests that the PM knowledge system can be used for decision making and manual checks in advance of emergency response to system failures to increase the probability of success in projects with a high degree of urgency.

A similar analysis was performed for the remaining four cases. A summary of the analysis results for all cases is shown in Table 6. The line items in the table are the 10 Knowledge Areas of PM Knowledge. The column entries in the table are the five cases. For each case, the items corresponding to the knowledge area in emergency response are extracted and described. For example, for Case 1, representative items are extracted and described for each row in Table 5. For example, with regard to integrated management, the goal set at the time of launch is described as "avoiding suspension of publication even if it is incomplete." From this table, it is possible to extract points of view to be considered in an emergency in all cases, except for the rows of costs that have to be given lower priority in an emergency. From this, it was suggested that by using the proposed PM knowledge as a template, it is possible to avoid omission of perspectives in emergencies.

4.3 Discussion

This chapter examines the effect of utilizing the PM knowledge presented in Tables 5 and 6 to extract the perspective of emergency management. Conventionally, the incident management procedure as shown in Figure 1 was shown. Although best practices specify actions for each step, they do not describe the organizational perspectives that should be addressed. On the other hand, by using the PM knowledge proposed in this article, even in a chaotic situation, it will be easier to consider the perspectives that should be addressed as an organization without omission. That is, by referring to the templates in Tables 2 and 3, the current phase can be recognized and what should be done can be grasped. Also, as shown in Table 2, the 10 knowledge areas can be referenced to receive suggestions for action items in each phase. As a result, as shown in Tables 5 and 6, items to be noted in each phase can be clarified in light of the 10 knowledge areas. By

sharing such information as an organization, even in an unexpected and confusing situation, the organization can act with a common understanding. It is desirable to update and share such information from time to time.

Table 6: Overview of analysis results by PM knowledge (all cases)

	Case1	Case2	Case3	Case4	Case5
Integration	Goals for suspension even if you are incomplete	Avoidance of cancellation of racing	Completed remittance of all data on the day	Night batch data remittance is completed	Morning or afternoon market starts
Scope	Number of articles pages, printing color or black and white	All 11 races on the day	All remittance data to other banks	All data of night batch data	Reception of all orders
Schedule	1st edition printing start time, 2nd edition printing time	Race start time (15:00 pm)	End of reception of other systems (15:30)	Online processing start time (9 o'clock)	Morning market start time (8:40), afternoon market start time (12:25)
Cost	Without consideration	Without consideration	Without consideration	Without consideration	Without consideration
Quality	Completion of the morning edition	Being able to purchase a betting ticket normally	Number of data that could be transferred	Number of data processed	Orders that were accepted
Resource	Editing staff, vendor employee	Racecourse and vendor staff Backup system	Bank system staff Backup system	Bank system staff	System staff in the securities company
Communication	Contact vendor	Contact vendor	Non -applicable	Non -applicable	Contact vendor
Risk	Countings on not arriving at vendors	Cannot use backup system	Backup system data transfer before switching	Delayed solution of data inconsistency	Server Starting Causes of Specific delays
Procurement	Vendor cooperation	Vendor cooperation	Non -applicable	Non -applicable	Vendor cooperation
Stakeholders	Escalation to management	Escalation to management, public relations for customers	Escalation to management, public relations for customers	Escalation to management, public relations for customers	Escalation to management, public relations for customers

5 Conclusion

This paper aims to efficiently implement emergency response in the initial phase immediately after a system failure. A system failure is treated as a short-term project with a clear target deadline, and a framework for applying PM knowledge is explored. Using the PM knowledge system, the contents of an article about a system failure that met the above conditions are described. As a result, various management and decision-making elements were applied to the PM knowledge system, and the feasibility of using the PM knowledge system to manage emergency responses was confirmed. If the approach described in this paper is applied in practice, emergency responses, which often tend to become confusing, are expected to proceed in a more systematic manner.

A future work is to clarify the limitations and improvements of the method described in this paper by trying to describe various system failure cases using the PM body of knowledge. In addition, it is necessary to investigate whether omissions can be detected by evaluating existing emergency response manuals based on PM's knowledge system.

References

[1] IPA Information-technology Promotion Agency, Japan, "Information Processing System High Reliability Lessons Learned Guidebook (IT Services Edition)" https://www.ipa.go.jp/ikc/reports/20190315.html

[2] Cabinet Cyber Security Center: "The fourth action plan on information security of critical infra- structure"

https://www.nisc.go.jp/pdf/policy/infra/infra_rt4_r2.pdf

[3] Financial Institutions Bureau, Bank of Japan: "Current Status and Issues of Risk Management on System Failures in Financial Institutions", Bank of Japan Report and Research Paper https://www.boj.or.jp/research/brp/ron_2010/ron1011a.htm/

[4] F. Imamura, "What is resilience in the midst of experiencing the Great East Japan Earthquake ? ," Operations Research : The Science of Management, Vol. 59, No. 8, 2014, pp. 440-445

[5] ISO/IEC 27031:2011 Guidelines for information and communication technology readiness for business continuity

[6] Ministry of Economy, Trade and Industry: "IT Service Continuity Guidelines" https://www.bousai.go.jp/kyoiku/kigyou/keizoku/pdf/itsc_gl.pdf

[7] ISO/IEC 27001:2013 Guidelines for information and communication technology readiness for Information security

[8] ISO/IEC 20000:2011 Guidelines for information and communication technology readiness for IT service management

[9] ISO/IEC 27031:2019 Guidelines for information and communication technology readiness for business continuity

[10] Cabinet Office: "Business Continuity Guidelines" https://www.bousai.go.jp/kyoiku/kigyou/keizoku/pdf/guideline202104.pdf

[11] Office of Government Commerce (OGC) : ITIL 2011 edition:Service Strategy, Service Design, Service Transition, ServiceOperation, Continual Service Improvement, TSO, 2011.

[12] A. D. Nugraha and N. Legowo, "Implementation of incident management for data services using ITIL V3 in telecommunication operator company," the Proceedings of the 2017 International Conference on Applied Computer and Communication Technologies (ComCom 2017), DOI: 10.1109/COMCOM.2017.8167093, 2017.

[13] MDE. Nazaruddin, MA. Salamat, AN. Azhan, WNSM. Haziman, IDS. Nizam, and NFWM. Shahril, "Relation Between PMBOK and IT Project Failure: The Billion Euro IT Disaster at NHS," Applied Information Technology And Computer Science, Vol.4, No.2, 2023, pp.2145-2151.

[14] K. Selvaraj, HUSM. Nizam, MFM. Sapri, N. Azmy, MHM. Azahari, and MA. Salamat, "Government Project Failure in Developing Healthcare Website – A Review with Particular Reference to PMBOK," Applied Information Technology And Computer Science, Vol.4, No.2, 2023, pp.2158-2164.

[15] A. Shimoda, "Study on Organizational Response Management to System Failures," the Proceedings of 11th International Congress on Advanced Applied Informatics (IIAI-AAI), 2022, pp.568-573.

[16] P. G. Smith and G. M. Merritt, "Proactive Risk Management: Controlling Uncertainty in Product Development," New York, 2002.

[17] Project Management Institute, Inc., "Project Management Body of Knowledge Guide (PMBOKR Guide) 6th Edition Japanese Version," 2017.

[18] Nikkei Computer, "Non-moving computer" https://xtech.nikkei.com/atcl/nxt/mag/nc/18/020600011/

[19] M. Shigemori and N. Fukazawa, "Proposal of Hierarchical VTA and Hypothetical-Deductive Accident Analysis Method," Ergonomics, Vol.36, 2000, pp.354-355.