

# A Comparison of Approaches to Incident Response in Japan and the United States and an Introduction to the International Standard ISO 22320

*Mitsuhiro Higashida, Naoko Kosaka, and Yuji Maeda*

### Abstract

NTT Secure Platform Laboratories has been researching and developing incident responses for when disasters occur. We introduce the approaches to incident response taken in the United States and compare them with those in Japan. We also introduce the disaster management standard ISO 22320: *Societal security—Emergency management—Requirements for incident response*, issued by the International Organization for Standardization (ISO) in November 2011.

### 1. Introduction

Natural disasters occur regularly in Japan, and every year there is a great loss of lives and property due to these events. Additionally, the tendency for heavy downpours to occur throughout the country is increasing and seems to be a long-term trend.

It has been pointed out with a great sense of urgency that Japan may be struck by large-scale earthquakes in the next few decades in areas such as the Nankai Trough and inland in the Tokyo area. The Central Disaster Management Council has estimated the potential damage for 18 types of Tokyo Inland Earthquakes. The Council assumes that an earthquake with a magnitude (M) of 7.3 with an epicenter in the northern part of Tokyo Bay would cause extensive damage and result in a death toll of approximately 11,000 people, a total collapse of 85,000 buildings, and a maximum economic loss of 112 trillion yen.

We cannot prevent the occurrence of natural disasters. Therefore, disaster mitigation is necessary in order to recover as quickly as possible from the damage caused by a disaster. This means to be prepared by implementing both structural and non-structural measures and by considering how we should prepare for a disaster. In this article, we discuss the concept of

crisis management in the future.

### 2. Activities to improve incident response capabilities

The International Organization for Standardization (ISO) issued ISO 22320 as an international standard for incident management in November 2011. Incident response consists of various response operations by different institutions and organizations. In some cases, activities need to be carried out throughout the country. Consequently, effective incident response requires structured command and control, as well as coordination and cooperation among the various organizations. ISO 22320 specifies the minimum requirements to carry out an efficient and effective incident response. Before this standard was issued, incident response was considered separately by different organizational units in Japan. With the introduction of ISO 22320, incident response plans are gradually being standardized. In the following sections, the approach toward incident response in the United States (U.S.) is introduced and compared with that in Japan. Then, an overview of ISO 22320 is given.

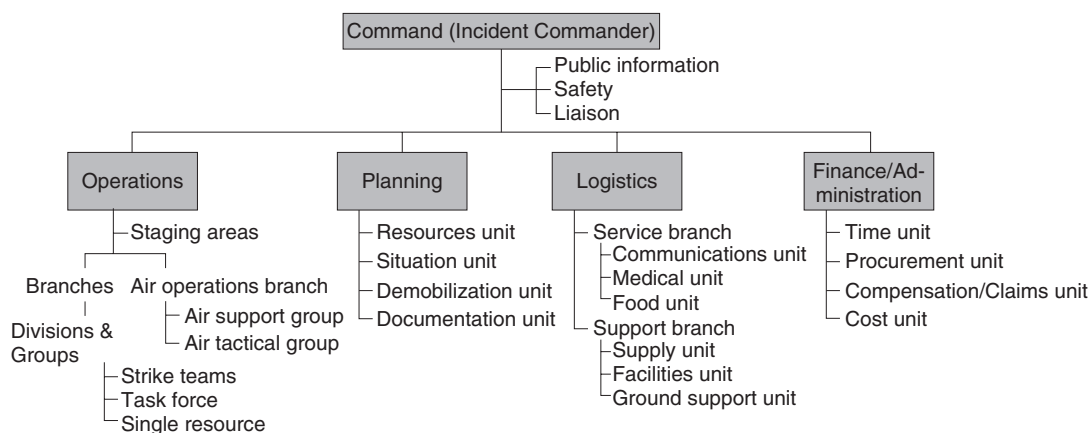


Fig. 1. ICS structure.

### 3. Incident Command System

The Incident Command System (ICS) is a standardized on-scene incident management concept designed specifically to allow responders to adopt an integrated organizational structure that can meet the complexity and demands of any single incident or multiple incidents without being hindered by jurisdictional boundaries.

The original ICS was established in the mid-1970s by the U.S. Forest Service and a number of California agencies. It was designed to improve and help coordinate responses to catastrophic wildfires in California. The ICS was developed to manage rapidly moving wildfires and to address the following problems: too many people reporting to one supervisor; different emergency response organizational structures; lack of reliable incident information; inadequate and incompatible communications; lack of structure for coordinated planning among agencies; unclear lines of authority; terminology differences among agencies; and unclear or unspecified incident objectives. Federal officials transitioned the ICS into a national program called the National Incident Management System (NIMS), which became the basis of a response management system for all federal agencies. Since then, many federal agencies have endorsed the use of ICS, and several have mandated its use.

The ICS divides an emergency response into five manageable functions essential for emergency response operations: Command (Incident Commander), Operations, Planning, Logistics, and Finance and Administration. A typical ICS structure is shown in Fig. 1.

The Incident Commander (IC) is responsible for all aspects of the response, including developing incident objectives and managing all incident operations. The ICS defines various information processing forms required for an incident response, which are known as ICS Forms. ICS Forms are designed to assist emergency response personnel in the use of ICS and the corresponding documentation during incident operations.

In addition, many ICT systems have been set up to support ICS activities. Training programs are conducted in various institutions in order to prepare for disasters, for example, HSEEP (Homeland Security Exercise and Evaluation Program), and a grant program to support these activities has been established by the U.S. government.

As described above, the response management system in the United States is based on ICS.

In Japan, the Self-Defense Forces, National Police Agency, and National Fire Department have established a command and control system. When the Great East Japan Earthquake struck in 2011, these organizations were able to respond quickly to the disaster area by sending units that are dispersed across the country. By contrast, local governments in Japan do not have a system like this.

### 4. Difference in incident response approaches between Japan and the United States

The Local Disaster Management Plan is common in Japan. This is a plan established by each prefectural and municipal disaster management council, subject to local circumstances and based on the Basic

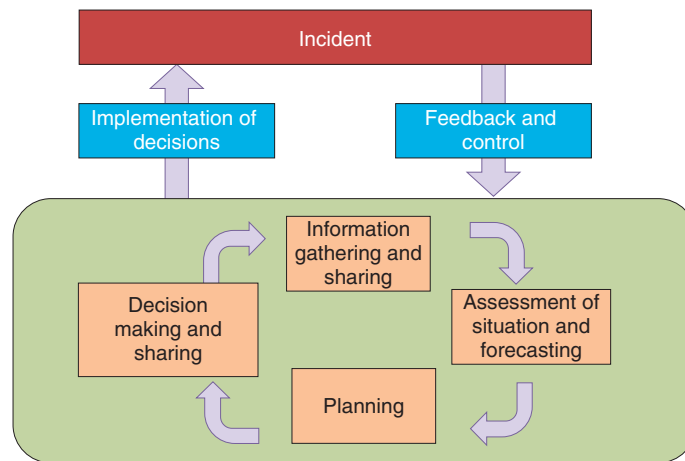


Fig. 2. Command and control process specified in ISO 22320.

Disaster Management Plan.

By contrast, ICS in the U.S. is applied nationally. It is flexible and can be used for incidents of any type, scope, and complexity. ICS allows its users to adopt an integrated organizational structure to match the complexities and demands of single or multiple incidents.

ICS is used by all levels of government—federal, state, tribal, and local—as well as by many nongovernmental organizations and the private sector. It is also applicable across disciplines.

In Japan, the role of state agencies is limited, and they do not have a system to perform disaster responses in place of local governments.

The role of state agencies is to provide support to the local governments.

Furthermore, in Japan, disaster responses are planned based on an extension of command and control operations during ordinary times. Thus, the disadvantage is that the response may not be sufficient during a disaster that is beyond the response capacity.

In contrast, in the United States, the corresponding organization expands according to the size of the disaster. The organization also has the authority to command and control the response operations.

In addition, there are full-time professional disaster response teams in the United States. However, disaster response personnel change every few years in Japan.



Fig. 3. Process of providing operational information (ISO 22320).

5. ISO 22320

ISO 22320 is an international standard that was issued to enhance the ability of private and public organizations to handle all kinds of emergencies such as flooding, earthquakes, and accidents.

The standard specifies the following requirements for an effective incident response:

- a) Requirements for command and control (Fig. 2)
- b) Requirements for operational information (Fig. 3)
- c) Requirements for cooperation and coordination

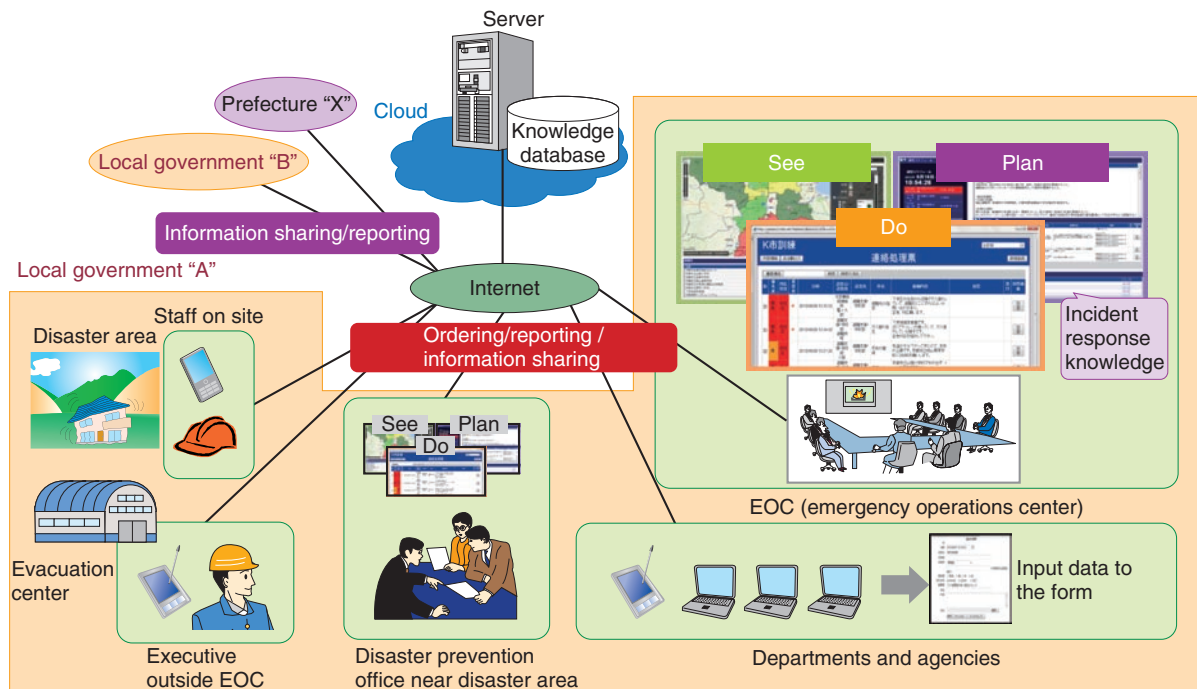


Fig. 4. Strategic emergency management support system.

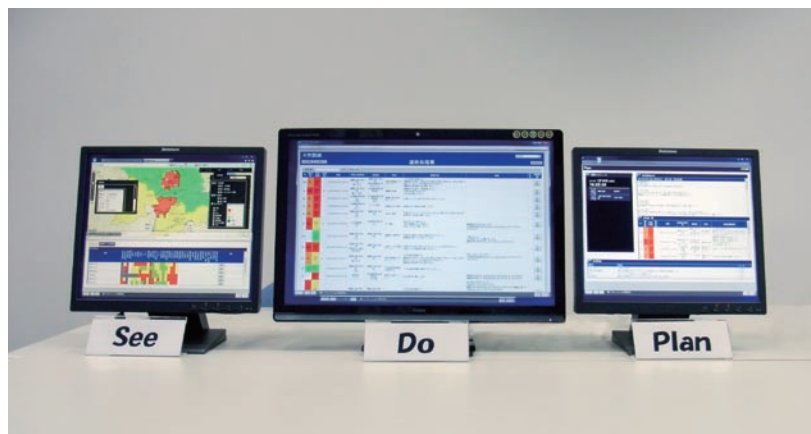


Photo 1. Screen shots of strategic emergency management support system.

Thus, ISO 22320 is a standard that allows inter-organizational cooperation among the involved organizations, agencies, and other parties.

After ISO 22320 was issued, a committee was formed in 2012 by the Japanese Standards Association (JSA) to establish Japanese Industrial Standards (JIS), which will be issued in the summer of 2013 at the earliest.

## 6. Conclusion

Until now, there was no common agreement on how to implement an incident response in Japan. Therefore, ISO 22320 will play an important role in the standardization of a domestic incident response plan in the future. We will work on developing a *strategic emergency management support system* based on ISO

22320 (**Fig. 4**). Key personnel will use the support system to prepare a common operational picture and carry out effective emergency management through the summarizing, managing, and sharing of information and foresight utilizing incident response knowledge (**Photo 1**). If the system is provided on a cloud, users can use it whenever necessary, including during training. As a result, local governments that have not

had any experience in dealing with disasters can utilize the knowledge of other local governments stored on the knowledge database of the system.

NTT Secure Platform Laboratories is continuing to research and develop ways to improve incident response capabilities through the management support system based on ISO 22320.



**Mitsuhiro Higashida**

Senior Research Engineer, Medical and Healthcare Information Systems Development Project, NTT Secure platform Laboratories.

He received the Ph.D. degree in social informatics from Kyoto University in 2008. He joined NTT in 1993. He is currently studying disaster information systems. He is a member of the Institute of Social Safety Science and the Japan Society for Natural Disaster Science.



**Naoko Kosaka**

Engineer, Medical and Healthcare Information Systems Development Project, NTT Secure Platform Laboratories.

She received the B.E., M.E., and Ph.D. degrees in engineering from Tokyo Institute of Technology in 1995, 1997, and 2004, respectively. She joined NTT Human Interface Laboratories in 1997 and moved to Secure Platform Laboratories in 2010. She is currently studying an emergency management support system using incident response knowledge. She is a member of the Institute of Electronics, Information and Communication Engineers (IEICE).



**Yuji Maeda**

Senior Research Engineer, Supervisor, Medical and Healthcare Information Systems Development Project, NTT Secure platform Laboratories.

He received the Ph.D. degree in systems information science from Future University Hakodate, Hokkaido, in 2013. He joined NTT Telecommunication Networks Laboratories in 1991. He is currently supervising a development project on medical and healthcare information systems and disaster resilient information systems. He received the Scholarship Encouragement Award from IEICE in 1998. He is a senior member of IEICE, and a member of IEEE, the Human Interface Society, and the Japanese Telemedicine and Telecare Association.

---