Efforts to Achieve a Joint Risk Management Support System

Tomohiro Kokogawa, Naoko Kosaka, Akira Koyama, Fumiaki Ichinose, Fumiyuki Tanemo, and Yuji Maeda

Abstract

At NTT Secure Platform Laboratories, we are developing technology to support joint risk management and incident response based on unified chain of command and control in order to respond to the expanding global threat of cyber-attacks and physical emergencies such as natural disasters and accidents. This article introduces our efforts aimed at implementing a risk management/incident response management support system that can be applied in the event of risks of any kind.

Keywords: risk management, incident response, WebEOC

1. Introduction

Throughout the world, great losses are suffered due to the frequent occurrence of large-scale natural disasters, accidents, and terrorist incidences. It is necessary to achieve cooperation between organizations and governments, and consequently, there is a growing movement to standardize incident response measures. Thus, in autumn 2011, the ISO[*1] 22320 international standard was established to define the requirements for incident response [1]. In 2013, this was also adopted as a Japanese standard (JIS[*2] Q 22320), and it is thought that it will form the basis for future standardization in Japan's domestic incident response measures, which have so far been implemented in a non-unified way by various local governments and institutions. To respond to the threat of natural disasters such as floods, volcanic eruptions, and major earthquakes, it is important that government, businesses, and people work together to implement disaster risk reduction and mitigation measures.

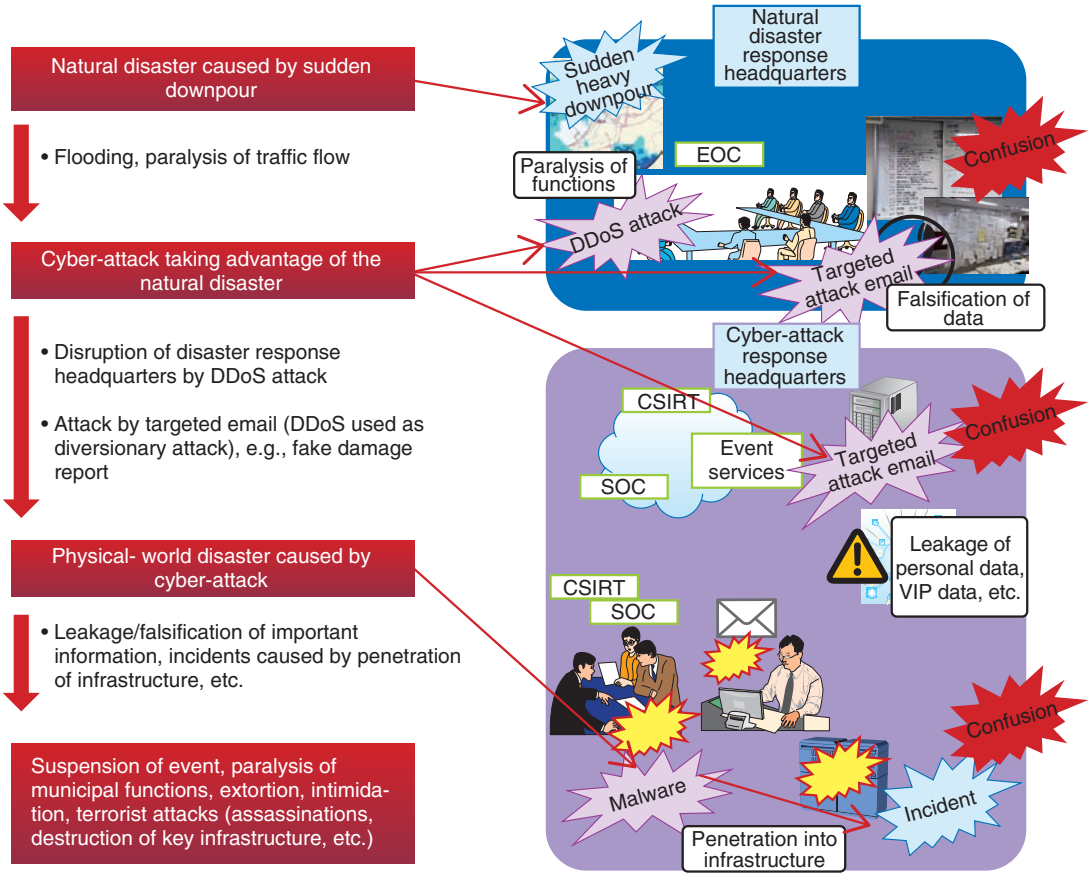
With the arrival of the Internet of Things (IoT), in which more and more objects are being connected to the Internet, and the cyber-physical integrated society, where cyberspace and the physical world are integrated in an advanced fashion, the Japanese government is working on the implementation of a new cybersecurity strategy [2]. In particular, during large-scale international events such as the Olympic and Paralympic Games, there is an urgent need for countermeasures to the increased threat of global terrorist cyber-attacks that involve both physical-world and cyberspace elements.

In the past, various organizations have responded to different types of emergencies such as natural disasters, terrorism, and cyber-attacks, but in the future it will be necessary to develop risk management and incident response mechanisms that have a broader outlook and draw no distinction between physical-world and cyberspace incidents. In this article, we discuss the concept of joint risk management as the way forward for risk management and incident response measures, and we introduce our research and development (R&D) efforts aimed at realizing systems to support this concept.

2. Preparing for complex crises

Thus far, different types of emergencies have been handled by different organizations. For example, cyber-attacks are handled by security operation centers, natural disasters and accidents are dealt with by emergency operation centers, and pandemics are

*1 ISO: International Organization for Standardization
*2 JIS: Japanese Industrial Standards



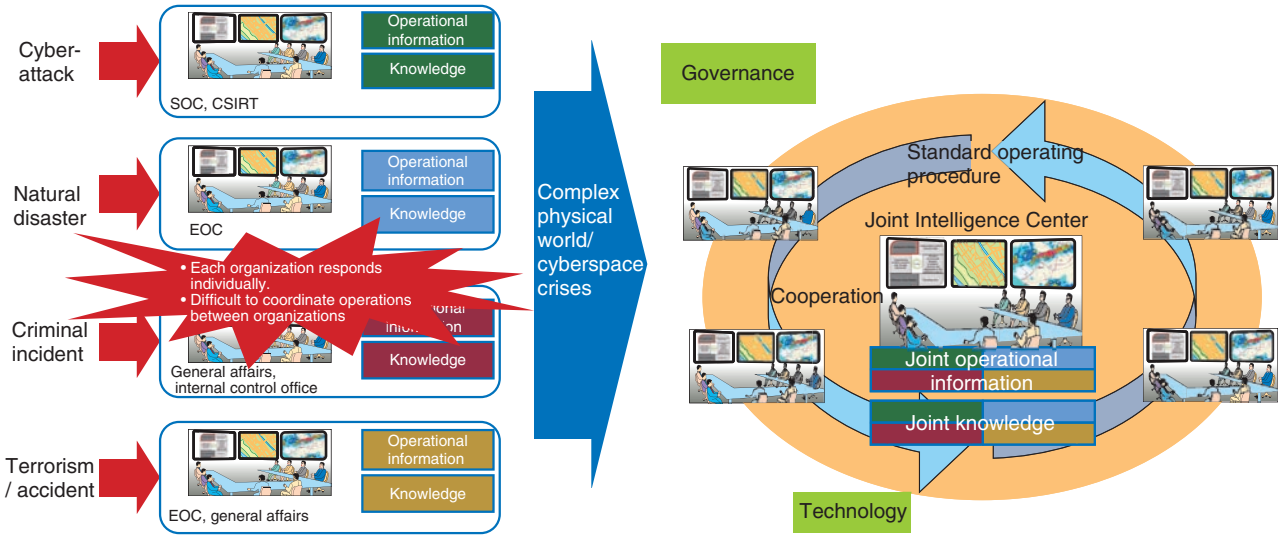
EOC: emergency operation center
CSIRT: computer security incident response team
DDoS: distribute denial of service
SOC: security operation center
VIP: very important person

Fig. 1. Example of physical world/cyberspace complex crises.

dealt with by general affairs departments. However, with the arrival of the IoT and the increasing sophistication of cyber-attack techniques, we can expect to see an increased incidence of complex crises such as cyber-attacks launched on top of natural disasters, or cyber-attacks causing other physical-world incidents. For example, an attacker might take advantage of a sudden unexpected downpour (natural disaster) during an event such as the Olympic and Paralympic Games in order to launch a cyber-attack on the organizations responding to this disaster. This might be carried out by crafting malware designed to attack infrastructure organizations and sending it in a targeted email supposedly connected with the disaster response efforts, thereby damaging the infrastructure facilities and creating further confusion (**Fig. 1**). Even though these individual events should be dealt with by the corresponding organizations and departments, the occurrence of this sort of complex crisis could cause responders to lose focus by making it impossible to grasp the overall incident situation, resulting in suspension of the event and huge human and financial losses.

3. Joint risk management concept

The occurrence of complex crises involving cyber-attacks coupled with physical-world events such as disasters and accidents is expected to increase in the future, so it is important to deal with this sort of incident with a joint response that takes a bird's-eye view of the entire situation beyond the boundaries between



(a) Conventional incident response

(b) Incident response by joint risk management

Fig. 2. Joint risk management concept.

separate organizations.

An illustration of the joint risk management concept is shown in **Fig. 2**. By joining and centralizing the handling of operational information (information for the implementation of response measures) and knowledge (external information that adds value to disaster response efforts) that was previously handled by separate organizations, it is possible to achieve efficient cooperation between these organizations. Furthermore, incorporating the conventional response organizations into a joint intelligence center makes it possible to carry out operations under a unified command.

To turn this joint risk management concept into reality, it is essential to consider the following viewpoints:

(1) To achieve unified command through cooperation between multiple organizations, we need to establish management processes to coordinate activities between organizations and implement effective decision-making and response measures based on a standardized management flow.

(2) To share information efficiently between organizations, we need to establish a standard operating procedure (SOP) for field activities and implement field operations using unified tools.

(3) To implement a common operational picture (COP) of the situation across multiple organizations, it is necessary to present operational information and knowledge in an integrated manner.

4. Plan, Do, See system concept

At NTT's laboratories, we have already developed an emergency management support system to increase the efficiency of responding to incidents, especially natural disasters [3]. This system implements management functions conforming to the ISO 22320 international standard based on crisis management software that runs on the web (WebEOC).

The operational information needed for incident response is broadly divided into fixed-format (collected using information-gathering forms) and free-format (free description) types, and is presented as an overview from three views (Plan, Do, and See) to support an efficient incident response.

In implementing joint risk management, we should build on the functions achieved with this system in order to strengthen the cooperation between organizations by expanding their scope to encompass risks of all kinds (including cyber-attacks). This system concept is illustrated in **Fig. 3**.

(1) Plan (What should we do now?)

To support overall management, an Operational Planning "P" (an international standard incident response process) is developed with a checklist (SOP)

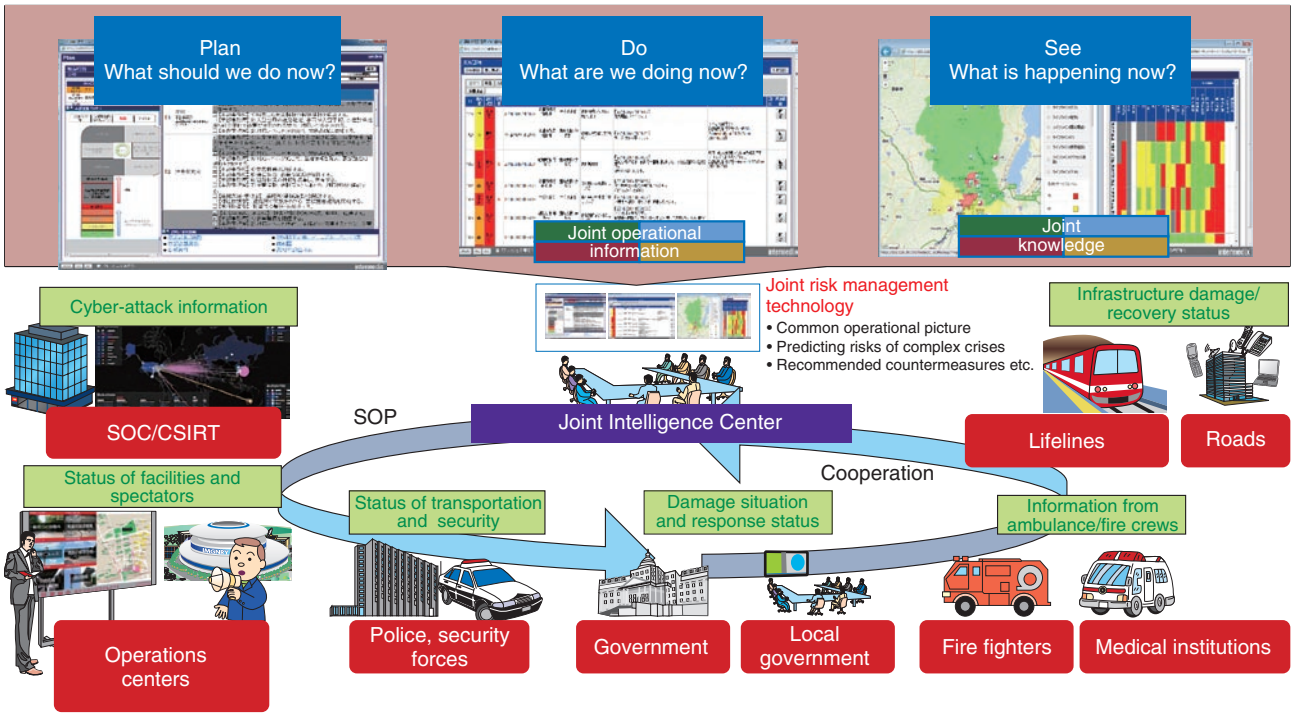


Fig. 3. Example of joint risk management support system.

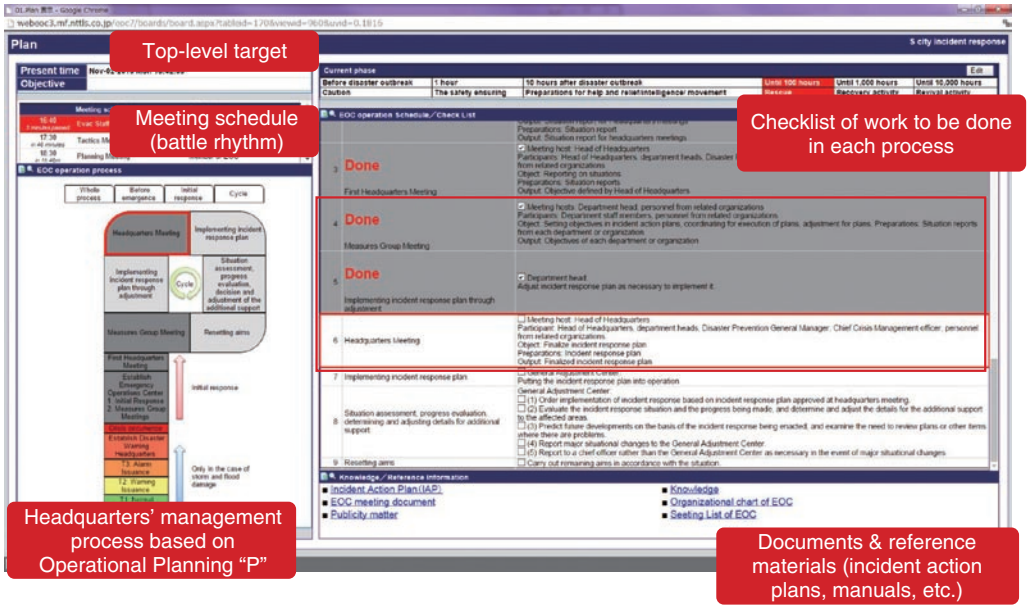


Fig. 4. Composition of the "Plan" screen.

for each phase (**Fig. 4**). This process must be organized so that policies and planning decisions can be made in a unified manner by all related organizations, regardless of the type of incident.

(2) Do (What are we doing now?)

By introducing unified management of free-format

information that was previously conveyed by phones (oral communication), white boards, and the like in field operations, we can provide status checks and displays based on an operational flow defined as an SOP so that the state of progress can be rapidly ascertained. The way in which this information is used is thought to differ according to the characteristics of the incident. For example, in the case of a natural disaster, a huge amount of work is created at the time of the incident, so it is important to support viewpoints that prevent leakage of shared information. In the case of cyber-attacks, however, small-scale events have to be dealt with on a daily basis, so it is thought to be necessary to support objectives such as increasing the efficiency of progress management and optimizing the control of access to shared information.

(3) See (What is happening now?)

An overall view of the damage situation and response status is facilitated by presenting information in the form of maps and dashboards. When complex crises occur, there will be a need for information presentation methods that can provide a joint overview of the current situation to the organizations responding to each incident.

5. Future prospects

At NTT's laboratories, in addition to advancing our R&D aimed at achieving joint risk management by solving the above issues, we aim to enable the NTT Group to provide total risk management and incident response solutions that facilitate efficient cooperation between organizations by allowing existing NTT Group products to cooperate with the products of other vendors that conform to a wide variety of standard specifications. We will also make use of this technology and other incident response know-how cultivated by the NTT Group in order to contribute to the realization of a society resilient to disasters.

References

[1] M. Higashida, N. Kosaka, and Y. Maeda, "A Comparison of Approaches to Incident Response in Japan and the United States and an Introduction to the International Standard ISO 22320," NTT Technical Review, Vol. 11, No. 6, 2013.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201306ra1.html

[2] National Center of Incident Readiness and Strategy for Cybersecurity, "Cybersecurity Strategy (Draft Plan)," May 2015 (in Japanese).
http://www.nisc.go.jp/conference/cs/dai02/pdf/02shiryou01.pdf

[3] N. Kosaka, A. Koyama, F. Ichinose, T. Kokogawa, Y. Maeda, H. Sakuma, T. Nozaki, M. Wada, N. Sakai, T. Nishimura, M. Sugiyama, M. Zusho, M. Osada, and K. Minowa, "An Emergency Management Support System Using WebEOC," NTT Technical Journal, Vol. 27, No. 3, pp. 55–58, 2015 (in Japanese).

Tomohiro Kokogawa

Senior Research Engineer, Security Risk Management Project, NTT Secure Platform Laboratories.

He received a B.E. and M.E. in engineering science from Osaka University in 1991 and 1993, and a Ph.D. in engineering from Wakayama University in 2013. Since joining NTT Telecommunication Networks Laboratories in 1993, he has been researching and developing information sharing systems and public service systems. He received the IPSJ SIGGN Best Presentation Award in 2012. He is a member of the Institute of Electrical and Electronics Engineers (IEEE) and the Information Processing Society of Japan (IPSJ).

Naoko Kosaka

Research Engineer, Security Risk Management Project, NTT Secure Platform Laboratories.

She received a B.E., M.E., and Ph.D. in engineering from Tokyo Institute of Technology in 1995, 1997, and 2004. She joined NTT Human Interface Laboratories in 1997 and engaged in researching and developing image processing methods for 3D maps and satellite images. She is now involved in researching and developing emergency management support systems. She is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) and the Japan Society for Disaster Information Studies.

Akira Koyama

Research Engineer, Security Risk Management Project, NTT Secure Platform Laboratories.

He received a B.E. and M.E. in applied chemistry from Hokkaido University in 1998 and 2000. Since joining NTT-EAST Tokyo branch office in 2000, he has been integrating the disaster risk reduction system to customers' emergency operation centers.

Fumiaki Ichinose

Senior Research Engineer, Security Risk Management Project, NTT Secure Platform Laboratories.

He received a B.E. and M.E. in applied physics from Osaka University in 1994 and 1996. Since joining NTT Kansai branch office in 1996, he has been integrating the disaster risk reduction system to customers' emergency operation centers. He is a member of the Institute of Social Safety Science.

Fumiyuki Tanemo

Senior Research Engineer, Supervisor, Security Risk Management Project, NTT Secure Platform Laboratories.

He received a B.E. and M.E. in engineering from Nagoya University in 1991 and 1993. He joined NTT Information Processing Laboratories in 1993, where he researched and developed object-oriented databases and information security management tools. He is now engaged in researching and developing emergency management support systems. He is a member of IEEE Computer Society and IPSJ.

Yuji Maeda

Vice President, Senior Manager, Security Risk Management Project, NTT Secure Platform Laboratories.

He received a Ph.D. in systems information science from Future University Hakodate, Hokkaido, in 2013. He joined NTT Telecommunication Networks Laboratories in 1991. He is currently managing projects related to general emergency management such as those concerning natural disaster response and cybersecurity involving NTT-CERT. He received the Scholarship Encouragement Award from IEICE in 1998. He is a senior member of IEICE and a member of IEEE and the Japanese Telemedicine and Telecare Association.