Study on Integrated Risk-Management Support System

− Application to Emergency Management for Cyber Incidents −

Kouji KISHI
NTT Secure Platform Laboratories, Japan
k.kishi@lab.ntt.co.jp

Naoko KOSAKA
NTT Secure Platform Laboratories, Japan
kosaka.naoko@lab.ntt.co.jp

Tsuneko KURA
NTT Secure Platform Laboratories, Japan
kura.tsuneko@lab.ntt.co.jp

Tomohiro KOKOGAWA
NTT Secure Platform Laboratories, Japan
kokogawa.tomohiro@lab.ntt.co.jp

Yuji MAEDA
NTT Secure Platform Laboratories, Japan
maeda.y@lab.ntt.co.jp

ABSTRACT

We have been studying the standardization of an emergency-management support system mainly for natural disasters at the local-government level. The system provides information from three viewpoints, “Plan: What should we do?”, “Do: What are we doing?”, and “See: What kind of situations are we in?” to support decision making at an emergency operations center. Rapid and accurate judgment prevents the occurrence of new damage and the expansion of damage, and as a result resilience will increase. We investigated its applicability to emergency management for cyber incidents through a cyber-defense exercise.

Keywords

Emergency Management, ISO22320, Incident response, Emergency Operations Center

1. Background and purpose

Damage caused by cyber incidents has recently become a serious problem. In 2015, there was leakage of subscriber information from the Japan Pension Organization, which became a major problem in Japan. Not only information leaks but also incidents that directly affect social life have occurred. For example, due to cyber attacks, the centrifuge of a nuclear power plant temporarily became unusable, large-scale blackouts occurred, and the computer networks of financial institutions became paralyzed, enabling illegal remittances (Research Group to make Resilient Society, 2016).

In 2014, The National Center of Incident Readiness and Strategy for Cybersecurity (NISC) of Japan defined “critical infrastructure” including 13 sectors such as “information communication”, “financial”, and “electric power”. To prevent IT disruption caused by natural disasters or cyber incidents from having a serious effect on infrastructure, action plans were set up to reduce the occurrence of IT faults and to promptly restore services (National center of Incident readiness and Strategy for Cybersecurity, 2016).

Many cyber-attacks were reported in the London 2012 and Rio 2016 Olympic Games, and it is expected that they will further increase in the Tokyo 2020 Games. Various risks, such as natural disasters, infectious diseases, and incidents on information systems or lifelines, are defined in the international standard ISO 20121 “Event Sustainability Management Systems” (ISO20121, 2012).

Thus, important social infrastructures being damaged by cyber attacks or multiple incidents occurring in combination at a big event may increase in the future. If each organization responds individually and separately when an incident occurs, incident-response activities may be inefficient. Therefore, it is necessary to standardize such activities. It is important for related organizations to cooperate and collaborate to address incidents effectively and efficiently (Hayashi, 2014).

We have been developing management flow and an information and communications technology (ICT)-integrated emergency-management support system as a countermeasure against natural disasters on the local-government level (Kosaka et al., 2014). We confirmed its usefulness over several years at disaster-response trainings (Higashida et al., 2012; Ichinose et al., 2015).

In this paper, we aim to evaluate the applicability of our system to the cyber field, through cyber defense exercises and interviews, in order to enhance resilience in the cyber field.

2. ELEMENTS OF EFFICIENT RISK MANAGEMENT

2.1 Standardization of risk management

The risk-management cycle consists of four stages; preparation (Plan), incident response (Do), review (Check), and plan modification (Action), as shown in Fig. 1 (Nakajima et al., 2013). We preliminarily take countermeasures against an assumed risk and respond to it when an incident occurs. We then analyze and evaluate the problems and issues through review then take measures to prepare for the next incident. The decision-making process is called the observe, orient, decide, act (OODA) loop (Tanaka, 2016) proposed by the air force Colonel John Boyd of the US military is applicable for the Do stage. In International Standard Organization (ISO) 22320 on incident response, the decision-making process is regulated, as shown in Fig. 2, as a command-and-control process. In other words, we collect and share information on the damage and countermeasures related to an incident, analyze and evaluate the collected information, predict the future, formulate a plan based on the results, and finally make decisions and share them with related parties. Then we will take action according to the decisions. In the standard, the following three points are summarized as the minimum necessary requirements, and they can be applied to any incident.

A) Requirements for command and control
B) Requirements for activity information
C) Requirements for cooperation and coordination

Cooperation is necessary in each step of Fig. 2. In the standard, “cooperation” and “coordination” are clearly distinguished. "Cooperation" means having a common purpose for multiple organizations to achieve, and "coordination" means synchronizing actions to achieve common objectives agreed upon by multiple organizations. When a wide variety of organizations gather to address an incident, it is important to clarify "objectives" and to synchronize their actions, that is, to manage the incident-response activities. The basis of ISO 22320 is the framework called the Incident Command System (ICS) formulated in the United States (Deal et al., 2012). The Operational Planning “P” is defined as concretizing the command and control process of ISO 22320 (Fig. 3). The lower half of the “P” shows the preparation before incident occurrence and the initial response, and the loop part shows that the cycle for information collection, decision making, etc… is repeated. By clarifying the process in this way, it may be possible to make decisions efficiently and enable cooperation among related organizations. It is necessary to clarify the decision-making process by stipulating concrete conferences in accordance with the organizational structure.

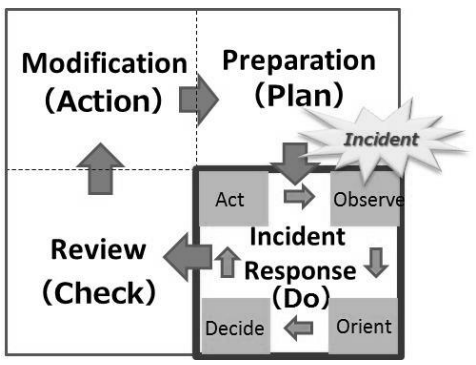


Fig. 1 Cycle of risk management

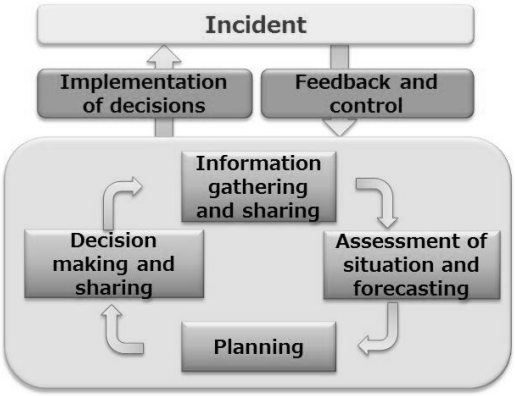


Fig. 2 Command-and-control process

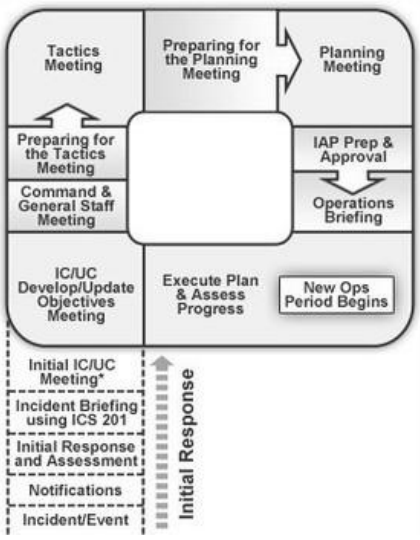


Fig. 3 Operational Planning "P"

2.2 Smooth communication and unification of situation recognition

In addressing incidents, it is necessary to unify situation recognition among related members and respond by efficiently communicating according to the standardized management flow described in the previous section. There are two types of incident-response activities, typical and atypical (Fig. 4). Typical activities have been experienced several times in the past and can be standardized. By preparing incident-response plans in advance, delegation of authority to staff in the field and support by volunteers and external staff, etc… can be facilitated and efficiency can be improved.

However, new problems that have never been experienced before will also occur. In such a case, it is necessary to share situation recognition among related members and to make a new response plan. Therefore, it is important to know how to standardize the incident-response activities, delegate authority to the site, and secure time to solve new problems.

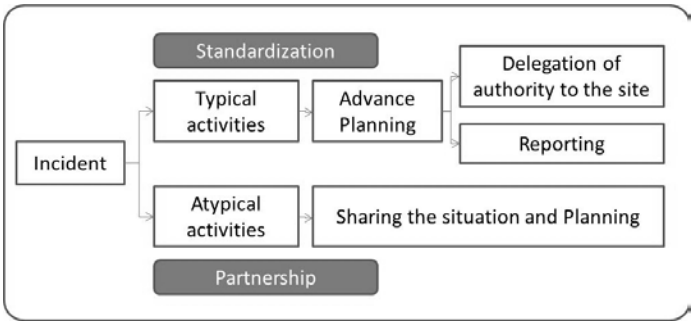


Fig. 4 Classification of incident-response activities

A requirement in ISO 22320 Section 2.1 B) states that "it is necessary to specify the purpose of the activity and to clarify what kind of information is required for that purpose". It is necessary to collect static information, e.g., geographical data, in advance then collect as much dynamic information, e.g., damage situation, as possible using prepared formats. To achieve this, an ICT system is required. We divide the information handled in an incident response into two types, fixed format and free format, based on the research results thus far. For fixed-format information, information to be collected is decided according to the purpose, and it is easy to collect necessary information by preparing a particular format in advance. It is also possible to compile and consolidate collected information, so an overview of the overall situation, that is, unification of situation recognition, i.e., a common operational picture (COP) among related members, may be possible. Free-format information, on the other hand, is communication in a free-description format, consisting of instructions and responses to them. During an incident-response training in Kashihara-city, Nara Prefecture in 2013, it was observed that free-format information occupied 74% of the information handled in a web-based communication system. Therefore, we believe it is necessary to use both fixed- and free-format information and be able to obtain an overview of the incident as a whole, such as damage and response situations.

The Interoperability Continuum formulated by US Department of Homeland Security (DHS) consists of five factors for effective incident response. They are “Governance”, “Standard Operations Procedure (SOP)”, “Technology”, “Training & Exercises”, and “Usage”. In other words, after establishing governance and SOP, an ICT system that supports crisis-response activity based on these factors is necessary.

2.3 Proposed Integrated Risk-Management Support System

The proposed integrated risk-management support system is mainly for effective incident response, and it can also be applied to a larger risk-management cycle, as shown in Fig.1, by reviewing the results of training or actual incident response. In this system, the gathered information can be browsed from the information aggregated on Plan, Do, and See screens of the ICT system, and the system supports efficient and effective decision making and cooperation between organizations, which leads to improved resilience. On the Plan screen, one can confirm “What should be done now?”, on the Do screen “What is being executed now?”, and on the See screen “What is the situation now?”

2.3.1 Plan Screen

The Plan screen is shown in Fig. 5. It shows the Operational Planning “P” with a checklist showing who should do what at each step of the “P”. Even an inexperienced staff member can understand "what to do now" and "what to do next". It also provides the goals decided by the head of the organization, meeting schedule, and meeting materials, manuals, etc...

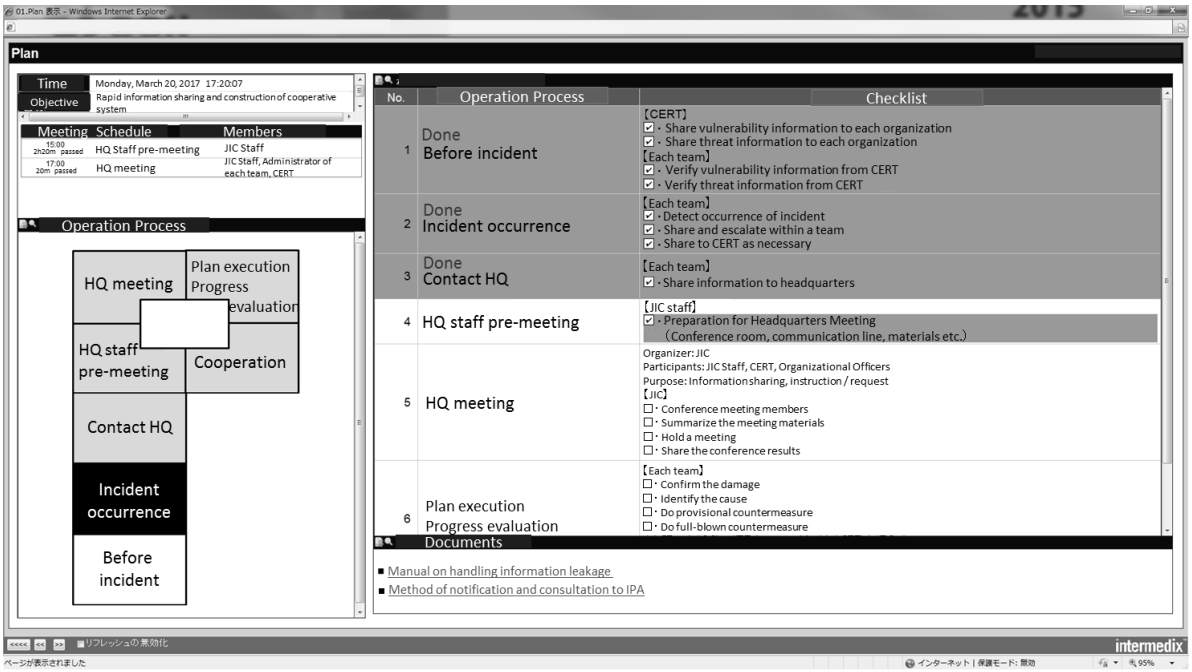


Fig. 5 Plan screen

2.3.2 Do Screen

The Do screen is shown in Figs. 6 and 7. Figure 6 is a list of messages that contain atypical information, and messages between organizations are displayed in chronological order. Each message contains a message ID, levels of importance and emergency, status (ex. completed or no completed), date and time, sender, receiver, subject, and contents. Due to the color coding according to the level of importance, emergency, and status, important messages that need to be read can be distinguished immediately. Figure 7 is a list of cyber-threat information, which is also atypical information.

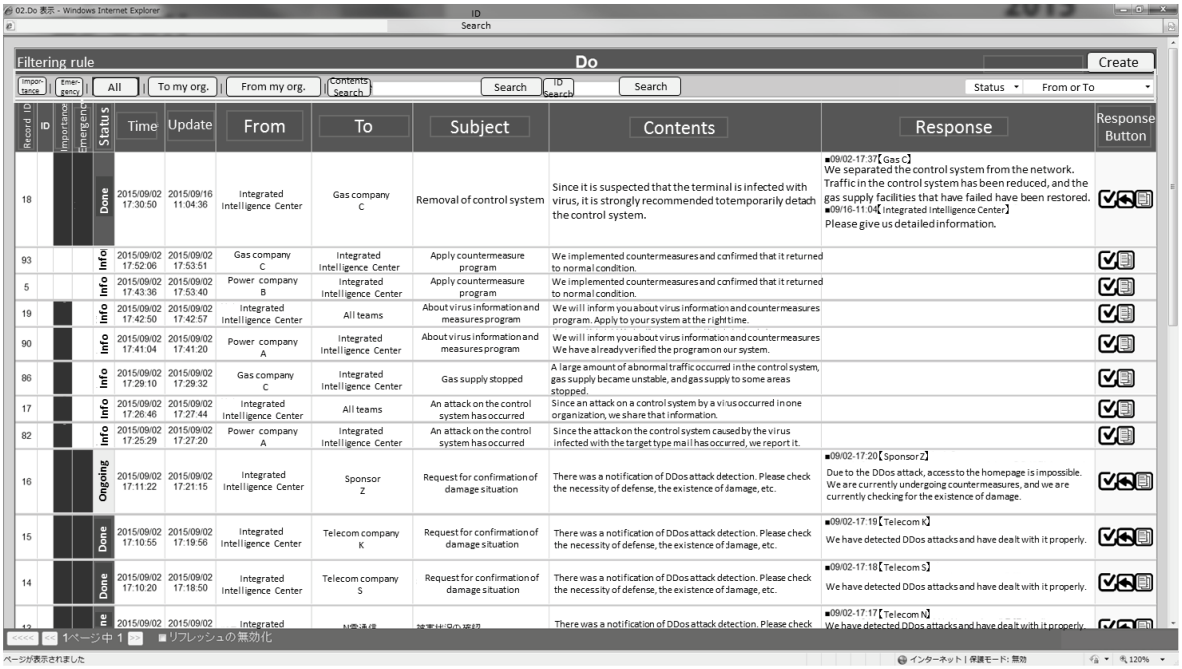
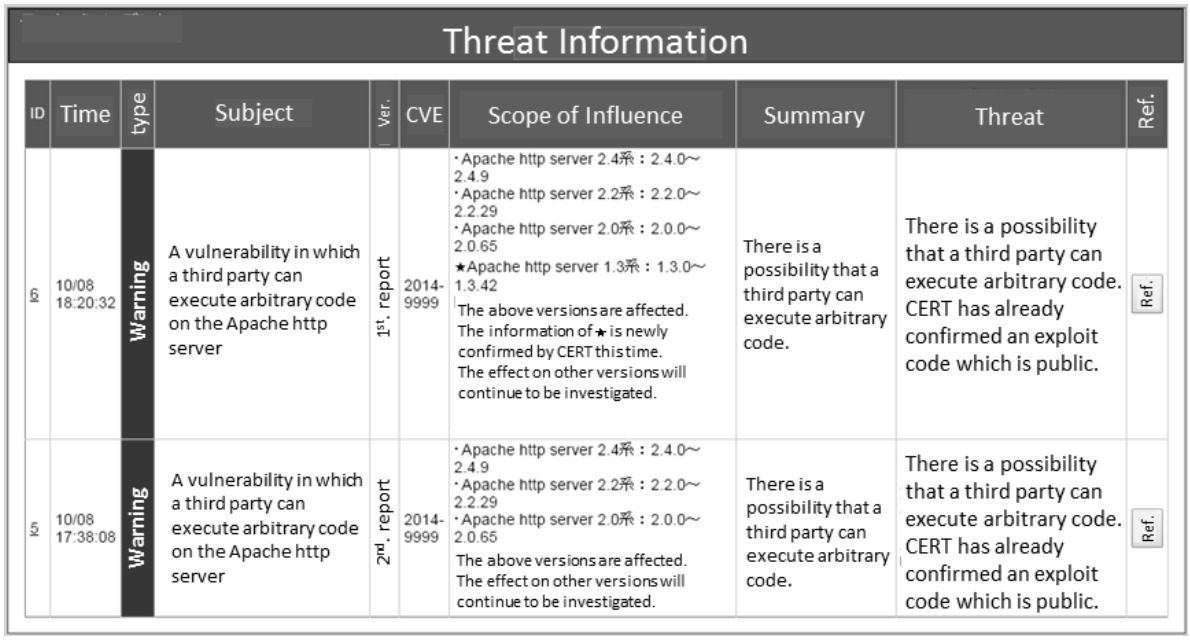


Fig. 6 Do screen (List of messages)



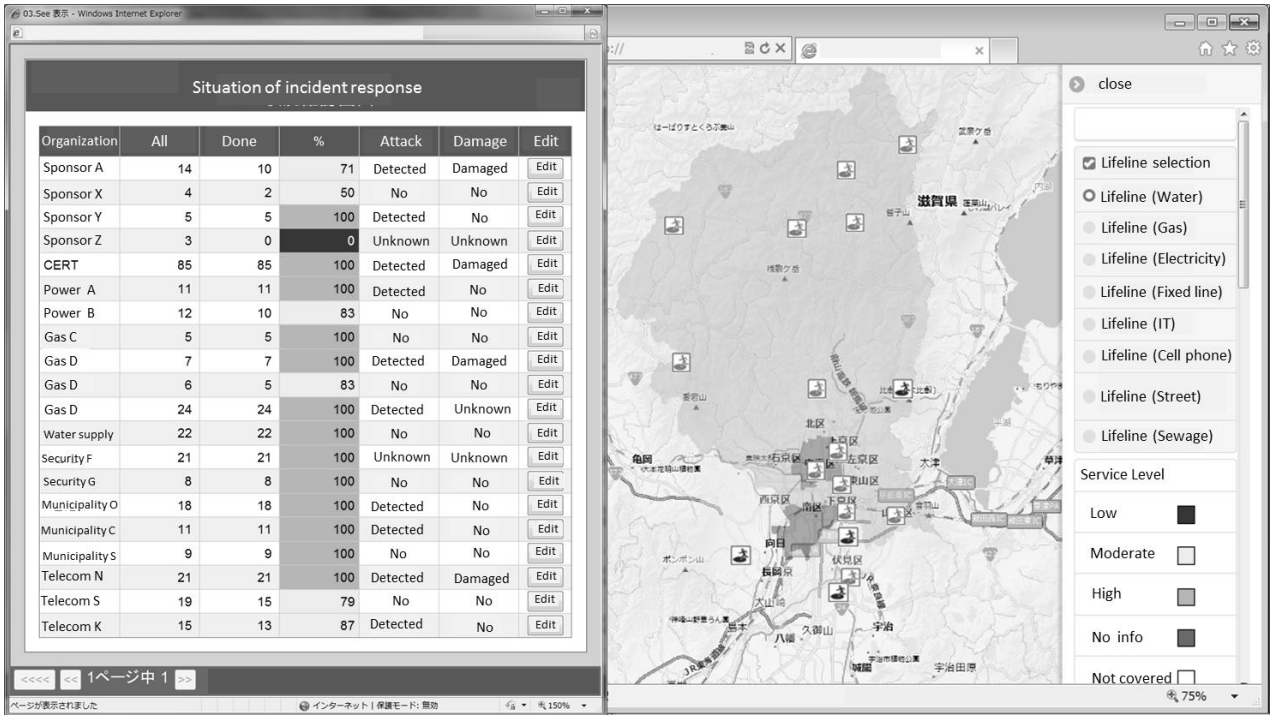
Threat Information

ID	Time	type	Subject	Ver.	CVE	Scope of Influence	Summary	Threat	Ref.
5	10/08 18:20:32	Warning	A vulnerability in which a third party can execute arbitrary code on the Apache http server	1st. report	2014-9999	・Apache http server 2.4系：2.4.0～2.4.9 ・Apache http server 2.2系：2.2.0～2.2.29 ・Apache http server 2.0系：2.0.0～2.0.65 ★Apache http server 1.3系：1.3.0～1.3.42 The above versions are affected. The information of ★ is newly confirmed by CERT this time. The effect on other versions will continue to be investigated.	There is a possibility that a third party can execute arbitrary code.	There is a possibility that a third party can execute arbitrary code. CERT has already confirmed an exploit code which is public.	Ref.
4	10/08 17:38:08	Warning	A vulnerability in which a third party can execute arbitrary code on the Apache http server	2nd. report	2014-9999	・Apache http server 2.4系：2.4.0～2.4.9 ・Apache http server 2.2系：2.2.0～2.2.29 ・Apache http server 2.0系：2.0.0～2.0.65 The above versions are affected. The effect on other versions will continue to be investigated.	There is a possibility that a third party can execute arbitrary code.	There is a possibility that a third party can execute arbitrary code. CERT has already confirmed an exploit code which is public.	Ref.

Fig. 7 Do screen (Threat information)

2.3.3 See Screen

The See screen is shown in Fig. 8. The display is color-coded so that the overall situation can be easily confirmed. We refer to the color code of ISO 22324, i.e., “red” danger, “green” safe, and “yellow” moderate. It is easy to compile and summarize fixed-format information, so it is possible to unify recognition among members by visualizing the overall situation in a tabular form or on a map.



Situation of incident response

Organization	All	Done	%	Attack	Damage	Edit
Sponsor A	14	10	71	Detected	Damaged	Edit
Sponsor X	4	2	50	No	No	Edit
Sponsor Y	5	5	100	Detected	No	Edit
Sponsor Z	3	0	0	Unknown	Unknown	Edit
CERT	85	85	100	Detected	Damaged	Edit
Power A	11	11	100	Detected	No	Edit
Power B	12	10	83	No	No	Edit
Gas C	5	5	100	No	No	Edit
Gas D	7	7	100	Detected	Damaged	Edit
Gas D	6	5	83	No	No	Edit
Gas D	24	24	100	Detected	Unknown	Edit
Water supply	22	22	100	No	No	Edit
Security F	21	21	100	Unknown	Unknown	Edit
Security G	8	8	100	No	No	Edit
Municipality O	18	18	100	Detected	No	Edit
Municipality C	11	11	100	Detected	No	Edit
Municipality S	9	9	100	No	No	Edit
Telecom N	21	21	100	Detected	Damaged	Edit
Telecom S	19	15	79	No	No	Edit
Telecom K	15	13	87	Detected	No	Edit

Fig. 8 See screen

3. VERIFICATION IN CYBER-INCIDENT EXERCISE

We evaluated the effectiveness of our system in a cyber-incident exercise involving several private companies.

The main purpose of the exercise was to verify the content of an incident-response manual. In the exercise, the Do screen of the system was used as a substitute for e-mail, which is often used by participants, and we verified that communication between organizations can be done smoothly. Smooth communication enables prompt information sharing. Especially in cyber incident response, unlike natural disasters, situation is hard to see, so sharing information on attacks, damage, and countermeasures is very important. It suppresses the occurrence of new damage and the expansion of damage. That will lead to improved resilience.

We created two kinds of evaluations, i.e., analysis of the Do screen logs recorded in the system and the results of a questionnaire given to the participants. The log analysis of the Do screen is for quantitative evaluation of communication inside and outside the organization. The questionnaire is for qualitative evaluation and gathering comments on the following items.

[Q1_1] Evaluate communication through free-format description on a 5-point scale (very useful, useful, ordinary, not very useful, useless)

[Q1_2] Write your comments on communication through free-format description.

[Q2_1] Evaluate "threat information/situation view" screen on a 5-point scale (very useful, useful, ordinary, not very useful, useless)

[Q2_2] Write your comments regarding "threat information/situation view" screen.

[Q3_1] Write your comments regarding what is good about the system.

[Q3_2] Write your comments regarding what is bad about the system.

4. Results and Discussion

The cyber-incident exercise was held in October 2015, and 11 companies (1 parent company and 10 subsidiaries), 103 people participated. The exercise scenarios were the following two-incident response activities. (The scenarios were not informed to participants in advance.)

Scenario 1:
- Serious software vulnerability information (threat information) is conveyed from the parent company to 10 subsidiaries. The parent company instructs the subsidiary to respond and report. (Teleconference and our system are used for communication.)

- Each subsidiary responds and reports to the parent company. (Our system is used for communication.)

Scenario 2:
- Information leakage from targeted attacks is discovered in one subsidiary. The subsidiary reports to the parent company. (Our system is used for communication.)
- Response method (application of pattern files of antivirus software, etc.) is indicated from the parent company to all subsidiaries. (Teleconference and our system are used for communication.)
- All subsidiaries respond and report to the parent company. (Our system is used for communication.)

4.1 Quantitative evaluation by log analysis

Sharing information with other companies is not common regarding cyber-incident response. However, a subsidiary needs to report its situation to the parent company. Figure 9 shows the flow of information. Company A is a parent company of subsidiaries B to K. Three departments of Company A participated in the exercise. Department A-1 participated in the same position as other companies, department A-2 provides technical consultation on cyber security, and department A-3 manages the subsidiaries. Three flows of communication, i.e., communication within each company, inquiries to department A-2, and report to department A-3, are also shown in Fig. 9.

From \ To	A-1	B	C	D	E	F	G	H	I	J	K	A-2	A-3	ALL	Cont roller	Total	%
A-1	5												5	2	1	13	4%
B	1	19										2	5		5	32	9%
C			16									4	5		15	40	11%
D												2	1		24	27	8%
E					18								5		13	36	10%
F						3						3	8		8	22	6%
G							11								5	16	5%
H								4					4		32	40	11%
I													3		11	14	4%
J										1			4		6	11	3%
K											6				3	9	3%
A-2						1						1		8	4	14	4%
A-3	1	1	1		1						1	1		10	9	25	7%
Controller	2	6	6	5	6	7	3	3	4	3	3	7				55	16%
Total	9	26	23	5	25	11	14	7	4	4	10	20	40	20	136	354	100%
%	3%	7%	6%	1%	7%	3%	4%	2%	1%	1%	3%	6%	11%	6%	38%	100%	–

Fig. 9 Overview of message flows

The change in the number of messages per scenario over time is shown in Fig.10. In scenario 1, communication between organizations is instantly made with the sharing of threat information as a trigger, and it declined as time passed, indicating that prompt action was taken. In scenario 2, since the incident occurred at different times for each company, communication was distributed as a whole.

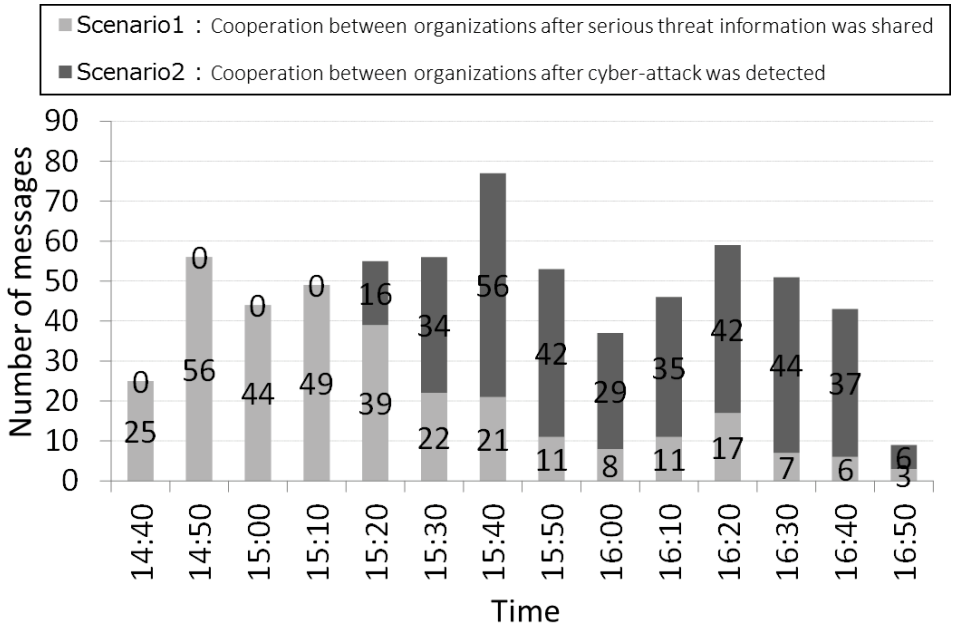


Fig.10 Transition in number of messages

4.2 Evaluation by Questionnaire

The number of respondents to the questionnaire was 57 for Q1_1, 32 for Q1_2 (42 answers), 57 for Q2_1, 18 for Q2_2 (23 answers), 43 for Q3_1 (44 answers), and 49 for Q 3 _ 2 (94 answers).

4.2.1 [Q1_1] Effectiveness of communication by free-format description

Free-format description was verified as being “useful” by more than half the respondents, as shown in Fig. 11. Since persons in charge of the cyber-incident response were accustomed to handling incidents using e-mail, the

rate of "ordinary" was over 20%.

4.2.2 [Q1_2] COMMENTS ON COMMUNICATION BY FREE-FORMAT DESCRIPTION

There were comments such as "It takes time to understand the contents because the message is too long" and "When new messages come in succession, the location of the message on the screen changed at the time of updating the screen so it was hard to read it".

4.2.3 [Q2_1] VALIDITY OF "THREAT INFORMATION/SITUATION VIEW" SCREEN

Less than half the respondents stated that the "threat information/situation view" screen was "useful", as shown in Fig. 11. Similar to Q1_1, the rate of "ordinary" was more than 25%.

4.2.4 [Q 2_2] COMMENTS ABOUT "THREAT INFORMATION/ SITUATION VIEW" SCREEN

By providing "threat information" and "situation view" separately on the Do screen, there was an opinion that, "It was easy to understand threat information" and "It would be convenient if there were a link with the related messages on the communication board on Do screen". We found that it would be better to display atypical information on a different board according to the purpose such as "communication" or "information sharing".

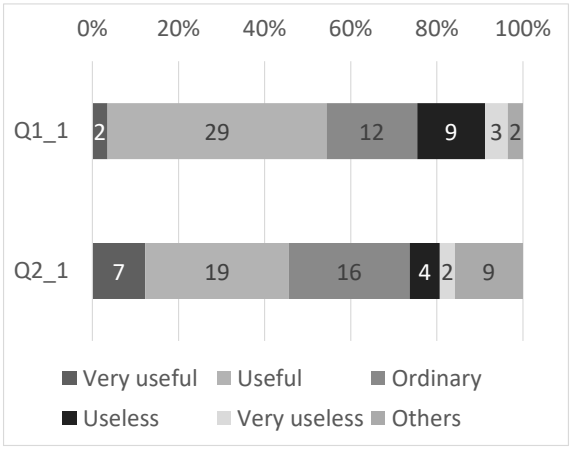


Fig. 11 Results of Q1_1 and Q2_1

4.2.5 [Q 3_1] WHAT IS GOOD ABOUT THE SYSTEM?

We classified this question from four viewpoints, "display", "function", "system operation", and "procedure" (Fig. 12). There were many comments on function. Regarding the viewpoint of display, there was a comment that, "The communication of one topic is displayed in a batch, so the status of each company could be easily grasped". The following comments are regarding the viewpoint of function, "It is convenient to be able to see the information from each organization", "It is easy to share information", "It is easy to exchange information among organizations", and "It is good to be able to store activity logs." Regarding the viewpoint of system operation, there was a comment about how operation was simple and intuitive. Regarding the viewpoint of procedure, the importance of centralizing information to a dedicated tool was mentioned.

4.2.6 [Q 3_2] WHAT IS BAD ABOUT THE SYSTEM?

We classified this question from the same viewpoints as in the previous question (Fig. 12). There were many opinions on the viewpoint of display. There was a problem of "losing sight of the message being read when updating the screen if the messages come in succession". Also, there were requests such as "I want to sort messages by time order" and "I want to distinguish between unread and read". It was also found that it was difficult to read a long message, so it is also necessary to improve the screen layout according to the size and resolution of the display. From the function viewpoint, there was a demand for flexible searching and sorting functions. There were also requests for customization functions such as multiple tags and colors on each message. From the viewpoint of system operation, there was an opinion that, "Since we usually use e-mail, it

would be convenient to be able to do the same operation as e-mail". From the viewpoint of procedure, there was an opinion that, "In order to cope with multiple incidents simultaneously, it is necessary to further organize the method of communication." Also, there were the following opinions; "I was wondering whether to make a new message or reply to an existing message when making a message" and "It is better to limit the people who enter messages into the system to avoid confusion."

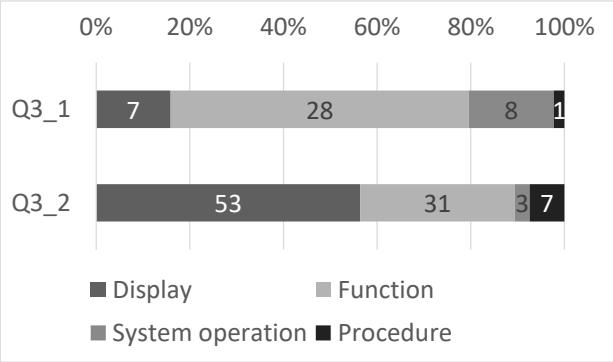


Fig. 12 Results of Q3_1 and Q3_2

5. COLLECTION OF COMMENTS THROUGH INTERVIEW

At a later date, we asked members of the cyber-incident response teams from the largest six companies who had participated in the exercise to use the system with some GUI improvements. We interviewed them regarding the Do, Plan, and See screens (the Plan and See screens were not used in the exercise). We explain the interview results below.

5.1 STATISTICAL ANALYSIS OF COMMENTS

We classified comments from each company's staff members in the interview in terms of the viewpoints of "function", "operational knowledge", and "work efficiency improvement ", as shown in Fig.13. Since the interviews were conducted while they were using the system, there were many comments on function.

Viewpoint	a corp.	b corp.	c corp.	d corp.	e corp.	f corp.	Total
1.Function	151	199	60	141	260	166	977
2.Operational knowledge	17	50	56	35	4	1	163
3.Work efficiency improvement	10	0	1	0	0	0	11
Total	178	249	117	176	264	167	1151

Fig.13 Classification of all comments

Furthermore, comments on function can be classified as "Plan screen", "Do screen", "See screen", and "Other functions", and the results are shown in Fig.14. There were many comments on the "Do screen", which is the core of the communication-support function.

	a corp.	b corp.	c corp.	d corp.	e corp.	f corp.	Total
1.Plan Screen	50	69	15	46	28	57	265
2.DoScreen	64	43	19	75	183	58	442
3.SeeScreen	1	26	5	0	15	19	66
4.Other functions	36	61	21	20	34	32	204
Total	151	199	60	141	260	166	977

Fig.14 Classification of comments on function viewpoint

We classified the above operational-knowledge viewpoint into the four elements of "governance", "standard operating procedures", "training and exercises", and "usage", as shown in Fig. 15. These four elements are a subset of the five elements of the Interoperability Continuum [11] formulated by DHS. For the introduction and use of communication tools, "governance" and "standard operating procedures" are important, so there were many comments related to these two elements.

	a corp.	b corp.	c corp.	d corp.	e corp.	f corp.	Total
1.Governance	7	36	16	8	0	0	67
2.Standard operating procedures	9	10	37	16	2	0	74
3.Training and exercises	1	2	0	3	0	0	6
4.Usage	0	2	3	8	2	1	16
Total	17	50	56	35	4	1	163

Fig.15 Classification of comments on “operational knowledge viewpoint”

In the next chapter, we describe the opinion on the "function viewpoint” for each Plan, Do and See screen.

5.2 COMMENTS ON FUNCTION VIEWPOINT

5.2.1 PLAN SCREEN

There was an opinion regarding the Plan screen that “The composition of the Operational Planning “P” may change depending on the type and scale of the incident”. Cyber incidents vary in their type and scale. Regarding natural disasters, the “P” is formulated for large incidents against which multiple organizations cooperate. To apply the “P” to cyber incidents, multiple types of “P” according to the scale and kind may be needed.

There was also an opinion that, “The sequences of the steps that make up the “P” may change depending on the situation.” A cyber incident has different properties from a natural disaster such as “There is a malicious person behind an incident”, “There are cases in which it is hard to notice the incident occurring”, and “There are cases in which the cause of the incident is not immediately understood”. Therefore, it is necessary to be more flexible in responding to cyber incidents.

There was an opinion that, “When dealing with incidents in cooperation with other organizations, it would be easy to cooperate if the progress status of other organizations could be known from the “P” checklist.” Regarding cyber incidents, it is not easy to notice the damage and response situations, so there were such opinions. However, there was an opinion that, “I do not want my organization's progress to be known to other organizations.” People do not want other organizations to know about, for example, the slowness of their organizations’ responses.

In addition, there was an opinion that it would be convenient to automatically send e-mail requesting conference participation to participants and automatically start a conference system according to the conference schedule registered on the Plan screen. By linking between different communication tools, convenience can be improved.

5.2.2 DO SCREEN

There was an opinion regarding the Do screen that, "The function of setting the disclosure range of the message is essential". With cyber-incident response, control of the scope of disclosure is considered indispensable because there are cases in which sensitive information, such as internal information, of an organization is handled.

There was also an opinion that, "It would be convenient if it were possible to enable/disable 'copy message' and 'download attached file'". To reduce the possibility of leakage of sensitive information, such a function is considered effective. Also, there was an opinion that, "It is possible to put the information acquired by telephone or e-mail into the Do screen to share it between organizations." Because there are advantages/disadvantages to each communication tool, it is necessary to use them properly at the right place. Moreover, there was an opinion that, "It is hard to understand who should change the 'status' of each message or task at which time." To avoid confusion when handling incidents, it is necessary to decide how to use communication tools and share this information among organizations in advance.

5.2.3 SEE SCREEN

There was an opinion regarding the See screen that, "It is convenient to use it to aggregate information of statuses from many organizations when dealing with software vulnerability". We received the same opinions during a drill of natural-disaster response. However, there was an opinion that, "We do not want to show our situation to other organizations other than the parent organization." It seems that such opinions come from the feeling that they do not want criticism from other organizations.

There was also an opinion that, "The information to be consolidated is different depending on the type of incident". Even in natural disasters, the information to be summarized varies depending on the type of disaster. It would be useful to prepare several templates for information input in advance, and it would be convenient if there were a function to edit input items flexibly when an incident occurs.

6. CONCLUSION

Through a cyber-incident exercise, we verified the effectiveness of our integrated risk-management support system for cyber incidents. From this exercise, mainly regarding the Do screen, the opinion that, "the system is useful" was stated by about half the respondents to the questionnaire, and negative opinions were stated by about a quarter of the respondents. During the exercise, a telephone conference was held during which the situation of each company was shared and future policy was decided. Each company wrote a chronology of the incident-response activities and to-do list on a white board. These activities can be supported with the Plan screen. The parent company summarized the damage situation of each of its subsidiaries on a white board and tried to obtain an overview of the situation. These activities can be supported with the See screen. Therefore, we found that our system can be applied to cyber incident response activities and improve resilience in cyber field.

In the interviews with the six companies after the exercise, we were able to understand how to modify our system when applying it to cyber incidents. We believe that it is necessary to improve readability for users to understand messages or the situation at a glance while handling atypical information. We also believe that it is necessary to develop a "standard operations procedure" on how to use the system in certain situations.

7. ACKNOWLEDGMENTS

In promoting this research, we received valuable cooperation from the staff who participated in the exercise and interviews. We express our deep appreciation to them.

REFERENCES

Deal,T., Bettencourt,M., Deal,V., Merrick,G., and Mills,C.(2012) Beyond Initial Response: Using The National Incident Management System's Incident Command System, 2nd Edition, AuthorHouse.

Hayashi, H., Incident response standardization research group (2014) Crisis response according to world standard , Japanese standards association.

Higashida, M. et al. (2012) Analysis of information processing in diagram training of disaster headquarters, *Institute of social safety science, proceedings* C-5.

Ichinose, F. et al. (2015) Verification of the importance of atypical information processing in disaster information system and proposal of effective use of it, *Institute of social safety science, collection of papers*, No.27, pp. 179-188.

Kosaka, N. et al. (2014) Investigation on how to use fixed-format / free-format information according to response phase in incident management support system, The 6th conference on information and communication system for safe and secure life.

National center of Incident readiness and Strategy for Cybersecurity (2016) How to think on important infrastructure protection, http://www.nisc.go.jp/active/infra/pdf/infra_rt3.pdf .

Research Group to make Resilient Society (2016) Challenges to Resilient Society, Nikkei BP Consulting.

Tanaka, Y. (2016) US military's management method to encourage people --- D-OODA management to win the uncertain battle, Nihon Keizai Shimbun Publisher.