Six Ws on cybersecurity information sharing for enhancing SOC/CSIRT

Version 1.0

October 27, 2017

Information Security Operation providers Group Japan (ISOG-J)

Revision History

2017/10/27	Version 1.0 released.
2018/02/20	English version released.

Disclaimers

- Copyright of this document is held by ISOG-J (Information Security Operation providers Group Japan).
- Citation of this document is allowed as long as its objective and manner (clarifying cited part and source) is within the legitimate scope of Japanese copyright laws.
- Contact ISOG-J (info (at) isog-j.org) if a citation is deemed to exceed legitimate scope.
- The names of companies, products, services mentioned in this document are basically registered trademarks or trademarks. ®, TM or © are abbreviated in this document.
- ISOG-J and the authors don't accept any liability for this document. Take full responsibility for your actions.

Contents

1. Introduction

1.1. Background

The importance of information sharing in responding cybersecurity incidents is widely recognized as mentioned in *Cybersecurity Management Guidelines*[1] by METI (Ministry of Economy, Trade and Industry) or *Collecting, analyzing and sharing information related to cyber attack* discussed by NISC (National center of Incident readiness and Strategy for Cybersecurity) at 12th regular meeting of 2017[2]. Several organizations such as JPCERT/CC, J-CSIP of IPA, private ISAC, or NCA (Nippon CSIRT Association) are promoting to maintain information sharing scheme.

1.2. Understanding challenges and objectives of this document

The following is the high-level flow of information sharing.

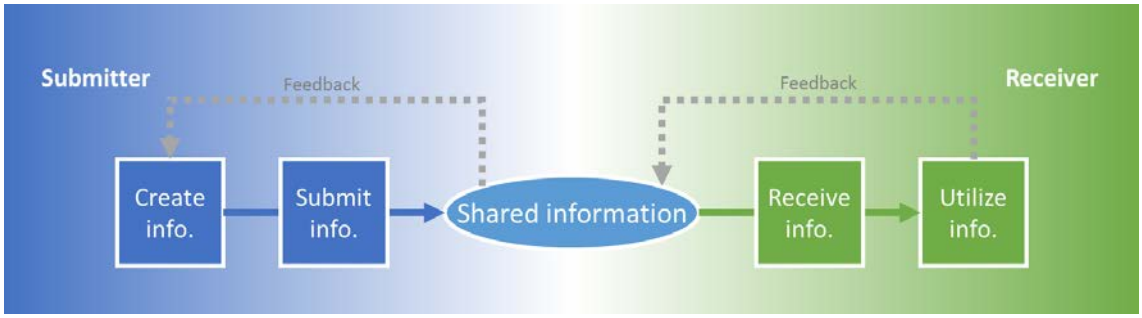

Figure 1 : Flow of information sharing

As shown above, the fundamental flow is that those who would like to submit information (submitter) generate and submit information and those who would like to leverage that shared information (receiver) catch and utilize it.

As mentioned previously, several organizations are promoting to maintain information sharing scheme. But the surrounding processes are not well matured, and there are problems such as shortage in amount or inefficient leveraging of shared information.

A part of the reason for the problems is that trying to realize information sharing

[1] http://www.meti.go.jp/policy/netsecurity/mng_guide.html
[2] http://www.nisc.go.jp/conference/cs/dai12/pdf/12sankou.pdf

without considering well-organized Six Ws shown below.

	Submitter	Receiver
Who	who will	who will
What	what information	what information
Where	in which medium for sharing	from which medium for sharing
When	in which phase	in which phase
Why	for what objective	for what objective
How	in what manner	in what manner
	submit information	utilize information

Table 1 : Six Ws in cybersecurity information sharing

The objective of this document is to summarize the methodology of "Six Ws in cybersecurity information sharing" along with its procedures. It also aims to help to motivate submitting information and utilizing information taken place everywhere.

2. Why and When

"Why" and "When", the objective for information sharing and when it is submitted or utilized, are in close relationship considering the flow of incident handling.

According to *SP800-61 Computer Security Incident Handling Guide* by NIST included in SP800 series, incident handling is divided into four major phases: "Preparation", "Detection & Analysis", "Containment, Eradication & Recovery" and "Post-Incident Activity".

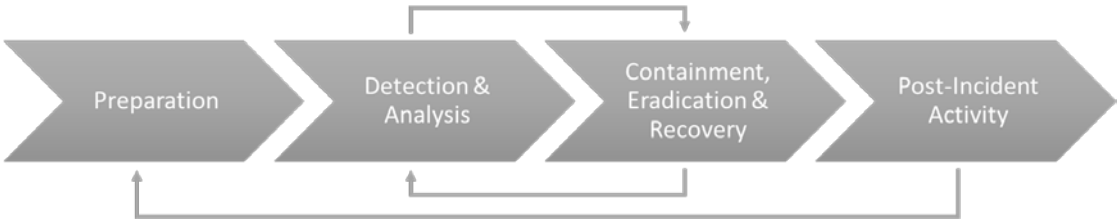

Figure 2 : Incident handling life cycle

This is the flow for ordinal incident handling and there are two major differences if the flow is triggered by shared information.

The first difference is that shared information need not be handled while incident must be handled. For example, even if vulnerability information related to Apache Struts2 is shared, its handling is unnecessary as long as it is not used within one's organization[3]. In other words, judging whether or not to perform initial handling is added as an extra phase.

The second difference is, needless to say, the existence of attacking information in the wild does not necessarily mean that correspondent incident is taking place in one's organization. If the incident were not there, "Containment, Eradication & Recovery" phase is unnecessary.

Taking these two differences into consideration, incident handling flow chart triggered by shared information should be as follows:

[3] This action could be regarded as handling "judge that handling is unnecessary", but the nature of handling isn't the same as that of actual incident and thus is accompanied by different handling phase.

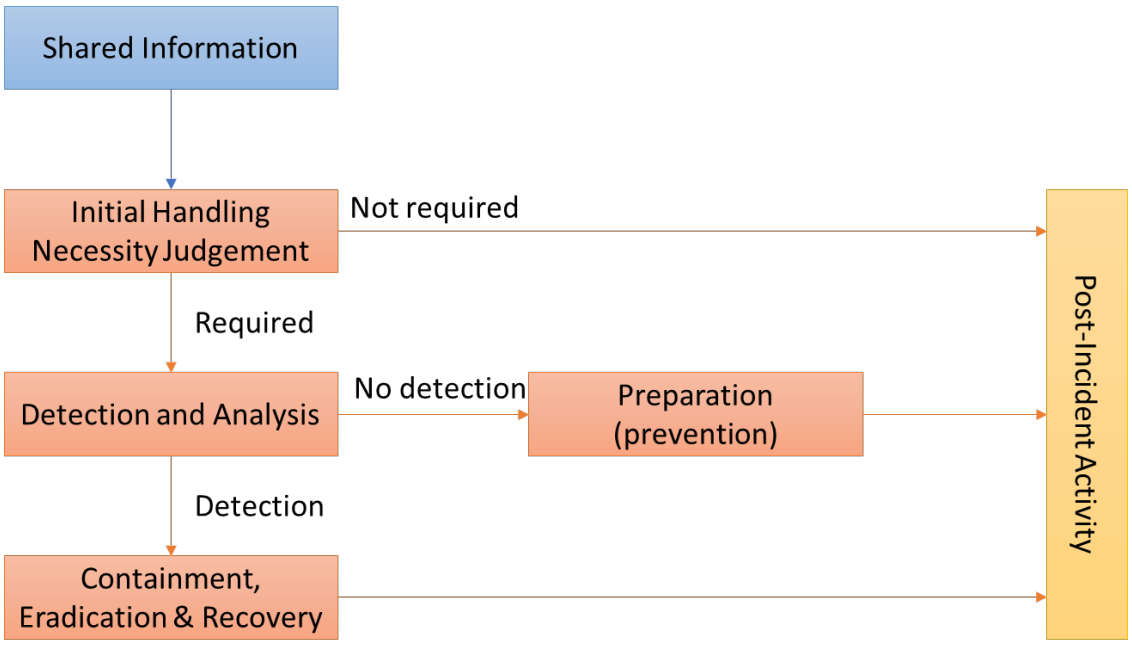

Figure 3 : Incident handling triggered by shared information

"Why (for what objective)" in sharing information is determined by in which opportunity of this flowchart "When (in which phase)" that the shared information is utilized.

In other words, "Why (for what objective)" in sharing information is performing one of the followings and one has to collect the information used for corresponding "When (in which phase)".

- Initial Handling Necessity Judgment
- Detection and Analysis
- Containment, Eradication & Recovery
- Preparation (prevention)
- Post-Incident Activity

The order of this list is in accordance with a timeline. In the earlier phase, submitting/collecting minimum information required to perform judgment as soon as

possible has more importance than completeness of the information.

3. What

"What (what information)" should be collected in practice? Taking "Why (for what objective)" discussed previously into consideration will help to seek the answer to this question.

Take the following three points that are frequently dealt with in sharing information as an example.

- Vulnerability information
- Attack-related information
- Actual incident handling case

Again, what is important is not the completeness of information but submitting or collecting the information in need considering "Why (for what objective)" and "When (in which phase)".

3.1. "What" for vulnerability information

The vulnerability information mentioned here is information in general presented by security organization or related personnel on software or hardware faults that malicious attacker might set a target for. Whether or not shared vulnerability information could be actual threat depends, it is necessary to understand and grasp the shared information.

3.1.1. Initial Handling Necessity Judgment

What is necessary for the phase? In responding to vulnerability information, the point will be clarifying the detail of the vulnerability and checking whether or not there is any system that has the vulnerability in question. Thus, the following information would be necessary.

- Vulnerability identifier (CVE or patch number)
- Affected system
  - System type

- Version
- Conditions (system architecture, configuration, etc.)

- Update status of security products to cope with that vulnerability

If the conditions or the system configurations are unknown, normally judgment is performed based on system type and version information only. Because update status of security products might have an impact on the judgment, it is desired to collect that information if possible[4].

3.1.2. Detection and Analysis

If there is an affecting system and judged that handling is required, monitoring to detect attacks and checking whether there is a compromise become necessary. The following information would assist to perform these handlings.

- Characteristics of attack
  - Attacking sequence, contents of related communication
  - Core of attacking code
- Traces of attack
  - Contents of communication after being compromised
  - Log recorded on server or client
  - Other traces left on server or client
- Detection name for security product
- If none of the above is unavailable, PoC (Proof of Concept) codes to perform self-study.[5]

[4] During initial handling, product vendors or security service provider sometimes cannot provide their latest information as they are intensively working on creating pattern file or signature, or too busy to dispose of inquiries from their customers. It is important to set flow that allows moving forward even if these kinds of information were not available.

[5] The codes that prove the existence of vulnerability.

With this information, check if there was an attack or actual damage or not would become possible. As for PoC, it is not always required as it is only skillful security engineer who can leverage it[6].

3.1.3. Containment, Eradication & Recovery

If there is an attack or an actual damage, its containment, eradication, and recovery become necessary. The following information is necessary for this phase:

- Configuration requirement to block attack using security product or related system.
- Countermeasure to make attack invalid (applying patch, changing configuration, etc.)
- Procedure to recover the compromised system.

3.1.4. Preparation

If there is no attack or damage, it is important to research the handling in case proactively. This would be similar to "Containment, Eradication & Recovery".

3.1.5. Post-Incident Activity

This will be discussed in *3.3 "What" for actual incident handling case*.

[6] The selective skillful security engineer can uncover unknown vulnerability or write own PoC code by referring to software patch information which is the really rare case.

3.2. “What” for attack related information

Attack related information mentioned in here includes all the information related to attacks in general such as information like “WannaCry is in the wild”, “There is an ongoing APT campaign”, “DDoS targeted to the certain website is announced”, or attack analysis report issued by security vendors. Regardless of information source, as their “Why (for what objective)” is determined, all you have to do is to check if the information is enough to achieve the “Why (for what objective)” and collect necessary information.

3.2.1. Initial Handling Necessity Judgment

If attack related information is shared, the following items would be of help:

- Name that specifies the attack (campaign, malware/incident name, etc.)
- Target of attack
- Attack vector[7]

Unlike vulnerability information, there might be no unique identifier. In that case, setting a unique name that involved personnel can have common understand becomes necessary.

It sometimes could be difficult to perform judgment whether or not there is an attacking target, which leads to judging “Handling required” as a result. But if the shared information says that “APT attack targets Eastern European countries”, it is possible to judge handling is unnecessary, or lower the handling priority. If the attack vector is clear, it would be possible to judge “as this attack comes from the Internet, handling is unnecessary because this system is installed inside of closed network”.

3.2.2. Detection and Analysis

Same as the case for vulnerability information, monitoring to detect attacks and checking whether there is a compromise become necessary.

- Characteristics of attack

[7] From where the attack comes. Malware infection route is one example.

- Contents of communications related to the attack
- Core of attacking code
- HTTP indicators related to attack
  - IP address
  - Domain name
  - FQDN
  - URL
- Email indicators related to attack
  - Mail subject
  - Mail body
  - URL included in mail body
  - Attachment file information
    - Filename
    - Extension
    - Hash value
    - Contents of the attached file
- Other characteristics or indicators observed on other protocols

- Trace of attack (if compromised)
  - Contents of communication after being compromised
  - Log recorded in server or client
  - Other traces left on server of client
  - Malicious contents information related to attack
    - Filename

- ✧ Folder/directory path
- ✧ Process name
- ✧ Hash value
- ✧ Modified registry entry
- ✧ Samples (malicious contents itself)[8]

- Detection name for security product

Of course, there exists more detail information, they are worthless if there is not the system that can understand and leverage that information. It is recommended to understand "what kind of information is worthy of one's organization" and collect information in need efficiently.

3.2.3. Containment, Eradication & Recovery

If there is an attack or a compromise, its containment and eradication become necessary. The required information should be something like the followings, same as the case for vulnerability information:

- Configuration requirement to block attack using security product or related system.
- Countermeasure to make attack invalid (applying patch, changing configuration, etc.)
- Procedure to recover the compromised system.

3.2.4. Post-Incident Activity

This will be discussed in *3.3 "What" for actual incident handling case.*

[8] Because handling samples are accompanied by risk, it must be done by selective skilled engineers under rigid monitoring with complying with strict operational rules.

3.3. "What" for actual incident handling case

An actual incident handling case is the summarized information on certain security incident and its handling procedures that an organization or a corporation underwent as a "Post-Incident Activity".

It would be difficult for an ordinary organization to be the first submitter for vulnerability or attack-related information discussed so far. But anybody can be the first submitter for one's actual incident handling case if one keeps the following points of view into mind:

- Initial Handling Necessity Judgment
  - When from where the information is acquired
  - How one judged the necessity of initial handling (surrounding situations including judgment process, policy, etc.)
- Detection and Analysis
  - How one confirmed the existence of the attack or compromise (target log and search conditions, found attack trace, etc.)
  - Quantitative data related to the attack or compromise (number of attacks, number of responded computers, etc.)
- Containment, Eradication, Recovery, and Preparation (prevention)
  - Detail of actual handling (performed configuration change on system or security products, etc.)
  - Quantitative data related to handling (number of handled systems, progress status compared to planned handlings, etc.)
- Throughout handling
  - What worked as expected
  - What did not work as expected
- Points need to be improved

Above-mentioned information will work as vital input not only for preparing coming security incidents but also for reporting to the management team including CISO. It will not easy to gather all the items, or some of the contents might be private so sharing them with external organizations could be inappropriate. But it must be precious information if one share as much as information as possible. There is a chance that one might receive feedback from external organizations that have a similar experience.

4. Receiver's "Who" and "How"

To realize effective use of shared information for incident handling, that "Who (who will)" behave "How (in what manner)" must be discussed in advance.

The following list shows which "Why (for what objective)" corresponds to the function or role mentioned in *Textbook for Security Incident Handling Organization*. Consider "Who (who will)" behave "How (in what manner)" if it is applied to your organization.

- Initial Handling Necessity Judgement
  - Judge in accordance with *A-2. Manage Triage Threshold* and *A-3. Manage Action Policy*. Follow *E-3. Manage Vulnerability and Handling* methodically once the handling is initiated.
- Detection and Analysis
  - Perform *B. Real-time Analysis*. Perform *C. Deep Analysis* if a deeper survey is required.
- Containment, Eradication & Recovery
  - If there is an actual damage, it must be treated as an incident. Perform *D. Incident Handling*.
- Preparation (prevention)
  - To prevent further damage, the function described in *G. Security Handling System Operation and Development* leads the implementation of countermeasures in practice. This preparation will be reinforced by performing *E. Diagnosis and Evaluation for Security Handling Status*.
- Post-Incident Activity
  - Evaluate the performed handling with reviewing *F. Collection, Analysis, and Evaluation of Threat Information* and perform necessary improvement. If there are too many problems, a drastic review would be necessary within the scope of *A. Operate Security Handling Organization*. Another important point is actively taking on the submitter role to promote *1. Active*

Collaboration with External Organization. Both success story and failure story are valuable information to share.

5. Submitter's "Who" and "How"

"Who (who will)" related to submitting information could be summarized as follows:

1. One who submits information in practice
2. One who approves the contents to submit
3. One who monitors the status after submission
4. One who is responsible for submitted information

Whenever submitting information from a security handling organization, it must be avoided to share more information than necessary or to trigger "Flaming" by shared information. 1 and 3, or 2 and 4 could fall on same personnel (or same role), but it is not recommended that single personnel play all of them considering an organization's management and control. It is important to state the process and rules for submitting information in advance to realize efficient operation. "How (in what manner)" must be also included in advance with keeping the following points in mind.

- What information
- To whom
- By which means
- In what format

As these are heavily relying on "Where (in which medium for sharing)", it is recommended to bear specific "Where" in mind when establishing the information submitting rules. In particular, it is important to distinguish the information to be submitted to external parties (Global Threat Intelligence) and information used only

internally (Local Threat Intelligence), and have rules that make sure the minimum required information is shared with the minimum stakeholders. Utilizing TLP (Traffic Light Protocol) [9] for external information sharing and adding information labels as regulated in ISMS for internal sharing would become necessary to achieve these objectives.

6. Where

Though "Where" information shared varies, it would be classified one of the following in general:

- Internal
  - Within belonging department
  - To related internal department
  - To management layer
- External
  - To related company (parent/child) or organization
  - Outsourcing company
  - Miscellaneous organizations (NCA, ISAC, etc.)
  - Public in general

It is important to list up which "Where" is potential targets for submitting or receiving information. Because it is difficult to submit information to various targets from the very first time, it is recommended to start sharing within limited close parties, then gradually expand the target with considering "Who" and "How". To receive the information submitted from "public in general"[10], it would be necessary to establish the official point of contact and announce to the public.

---

[9] https://en.wikipedia.org/wiki/Traffic_Light_Protocol
Reference :
https://www.nisc.go.jp/conference/seisaku/kihon/dai9/pdf/9siryou_ref04.pdf

[10] Information submitted, reported, notified or broadcasted by third parties.

In collecting information, it is necessary to clarify “How” in accordance with “Where”. Collecting information without obvious objective could be endless and results in a waste of time. It is vital to concentrate on collecting minimum information that an organization can leverage so that it will not collect more information than can handle. What is important for respective “Where” is not submitting the information on incidents with actual or serious damage only, but submitting information actively and fostering the atmosphere to share the information as widely as possible.

7. Essential restriction in sharing information

There is the underlying restriction in sharing information. Everyone involved in information sharing must realize this as nobody can be irrelevant.

Imagine the characteristics of ideal information sharing. For example, everyone will be satisfied if it is accurate, comprehensive, and fast.

But, is it really possible to realize?

The answer is NO. Fast information sharing impairs accuracy. Improving completeness impairs fastness. It is a matter of course and this dilemma is mentioned as information sharing triangle[11,12].

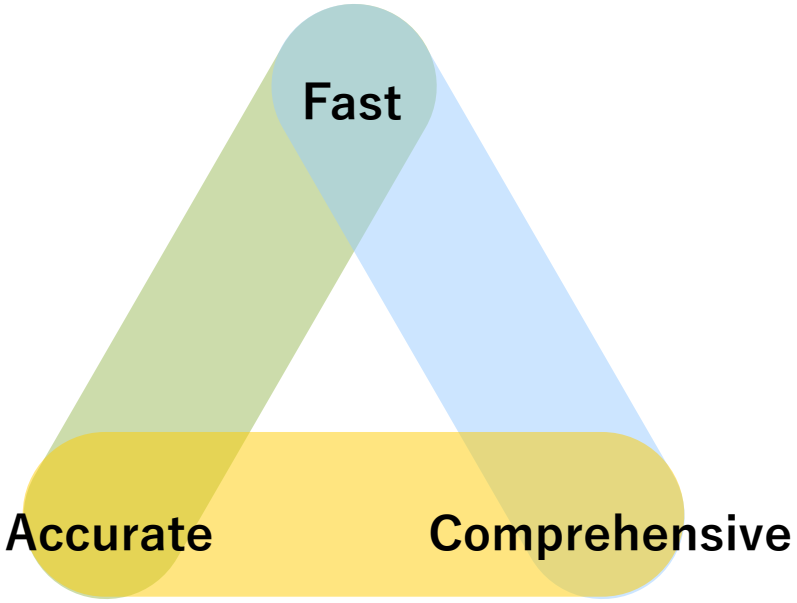

Figure 4 : Triangle in information sharing

In short, this figure says that only two of accurate, comprehensive, and fast could be realized at once. In other words, it could be summarized as follows:

[11] 27th Annual FIRST Conference (2015), Lightning Talk: "Four Easy Pieces", Tom Millar (US-CERT, NIST)
[12] https://www.first.org/resources/papers/conf2015/first_2015-rasmussen-rod_cutting-through-cyberthreat-intelligence-noise_20150615.pdf

- Fast and accurate information lacks comprehensiveness
  - Ex. One IP address was proposed as attack related information, but it became clear that there are many other related IP addresses.
- Fast and comprehensive information lacks accuracy
  - Ex. Many domains were proposed as attack related information, but benign domains were also included.
- Accurate and comprehensive information lacks fastness
  - Ex. It requires considerable time until proposing accurate and complete list of IP addresses and domains

The more serious the incident, the priority of fastness becomes higher. Satisfying fastness impairs either accuracy or comprehensiveness. It would be bad practice to blame for inaccuracy or incomprehensiveness for promptly shared information as it is an inevitable restriction. This could discourage the information submitter and spoil the atmosphere to promote information sharing. Nobody can summarize accurate and comprehensive information instantly. It is mentioned as *the Pyramid of Pain* in regard to information.

It does not mean that any information should be accepted without a word of feedback. Feedback is nevertheless important. If one felt that the quantity of shared information was not enough, one should submit additional information. If one felt that the quality of shared information was not enough, one should submit more accurate information.

The more the feedback is constructive, the better influence on information sharing. Both submitter and receiver must keep this in mind.

Conclusion

This document discussed the first steps for cybersecurity information sharing from "Six Ws" point of view. Beyond the first steps, a more formidable challenge is waiting. The followings are the examples:

- Standardize and automate "How" for submitter and receiver
- Visualize reliability and effectivity of shared information
- Feedback system that connects submitter and receiver

Though there are already several standards for "How" for submitters such as STIX[13], TAXII[14], or CybOX[15], they are not widely used and neither submitter nor receiver leverages these common frameworks in submitting, receiving and leveraging information. How to visualize the reliability of shared information must be discussed seriously. Information keeps changing and it could become worthless as time goes by. It is not easy to secure the accuracy and credibility as it is possible to inject fake information with malice. Feedback from its receiver could be a countermeasure, but it requires active information sharing atmosphere as sending feedback itself is submitting. Even if fostering activate information sharing atmosphere succeeded, information sharing platform is mandatory as neither submitter nor other receivers can reach the feedbacks if they were scattered all around. Because the information sharing platforms themselves are currently scattered all around, sharing feedback effectively would be difficult.

In the United States, DHS (Department of Homeland Security) is promoting to use AIS (Automated Indicator Sharing)[16] as a framework for cybersecurity information sharing. Advanced practice such as information platform built on STIX is leveraged by many organizations is emerging. Regarding automation, IETF is actively discussing MILE[17] or I2NF[18]. In Japan, ISOG-J has strong will to confront various challenges.

The authors believe that understanding the fundamentals of *Cybersecurity Information Sharing Six W's* discussed so far will be of great help for active information submitting and leveraging as well as contribute to strengthening your incident handling

[13] https://www.ipa.go.jp/security/vuln/STIX.html
[14] https://www.ipa.go.jp/security/vuln/TAXII.html
[15] https://www.ipa.go.jp/security/vuln/CybOX.html
[16] https://www.dhs.gov/ais
[17] https://datatracker.ietf.org/wg/mile/about/
[18] https://datatracker.ietf.org/wg/i2nsf/about/

team (SOC or CSIRT).

Authors

ISOG-J (Information Security Operation providers Group Japan)

Security Operations Chaos Working Group (WG6)

Masanobu Sasaki	FUJITSU SOCIAL SCIENCE LABORATORY LIMITED
Shinji Abe	NTT Security (Japan) KK / ISOG-J WG4 leader
Shigenori Takei	NTT TechnoCross Corp. / ISOG-J WG6 leader
Yuho Kameda	SCSK Corporation
Takayoshi Ichikawa	SoftBank Technology Corp. (Collaborator)
Yasunari Momoi	Internet Initiative Japan Inc.
Kimitomo Kawashima	NTT DATA INTELLILINK CORPORATION (English translation and proofreading)
Ryu Hiyoshi	NTT Security (Japan) KK
Tadaaki Nagao	Internet Initiative Japan Inc.