CSIRT Starter Kit

Version 2.0
English Version 1.0

Contents

Document Revision History

Version	Date	Description
1.0 en	July 27, 2016	Translated into English.
2.0	August 1, 2011	Created NCA edition.
1.0	February 5, 2007	Newly created.

Acknowledgements

Translated into English supported by NTT EAST Corporation

Reviewed and commented by VNCERT

1 Foreword

This document describes the issues that should be carefully addressed and matters that should be defined when creating a computer security incident response team (CSIRT) in Japan. It also refers to the procedures that should be followed when formulating a plan for incident response in an organization and aims to serve as a general guide for creating a CSIRT.

There can be no two identical models for CSIRTs due to the uniqueness of their objectives and organizational backgrounds. As a result, there are no two teams that will operate in exactly the same manner. A CSIRT should thus be structured so that it can play the most effective role after you determine, as an organization, why you are developing a CSIRT and what the CSIRT should achieve. This document is intended to be used by everyone involved in the creation of a CSIRT in Japan as a resource when examining what is appropriate for each individual organization.

This document is aimed at implementation supervisors and personnel in Japan who are in charge of implementing organizational measures to prevent the recurrence of computer security incidents and to limit damage therefrom. We expect this document can be used effectively to improve security.

2 CSIRT and Responding to Computer Security Incidents

With the remarkable progress made recently in computerization, information systems are playing an increasingly important role and the information processed by such systems is essential for corporate activities. For this reason, organizations that do not have tools for identifying the cause of a computer security incident ("Incident") or an appropriate system improvement plan may suffer decreases in productivity, lose the trust and confidence of society, pay large amounts of damages to outsiders in some cases, or otherwise face circumstances that threaten their existence because the occurrence of an Incident has a significant impact on their business.

There is probably no organization that is capable of taking all security measures to prevent each and every potential Incident. And, as systems become more complicated at a rapid pace, it is impossible to eliminate the possibility of Incidents occurring no matter how securely an information system is built and operated.

A Computer Security Incident Response Team ("CSIRT") is an organization that engages not only in the analysis of and response to actual Incidents, but also engages in activities such as education and supervision to improve security quality. These activities are intended to implement effective Incident response[1)] and to reduce the business risks as stated above.

Creating a CSIRT will bring the following benefits.

- ✓ Detect Incidents and Security Events[2)] and promptly and accurately convey information to the organization.
- ✓ Accumulate and share know-how through the implementation of response to Incidents.
- ✓ Improve the quality of security to prevent the recurrence of Incidents.

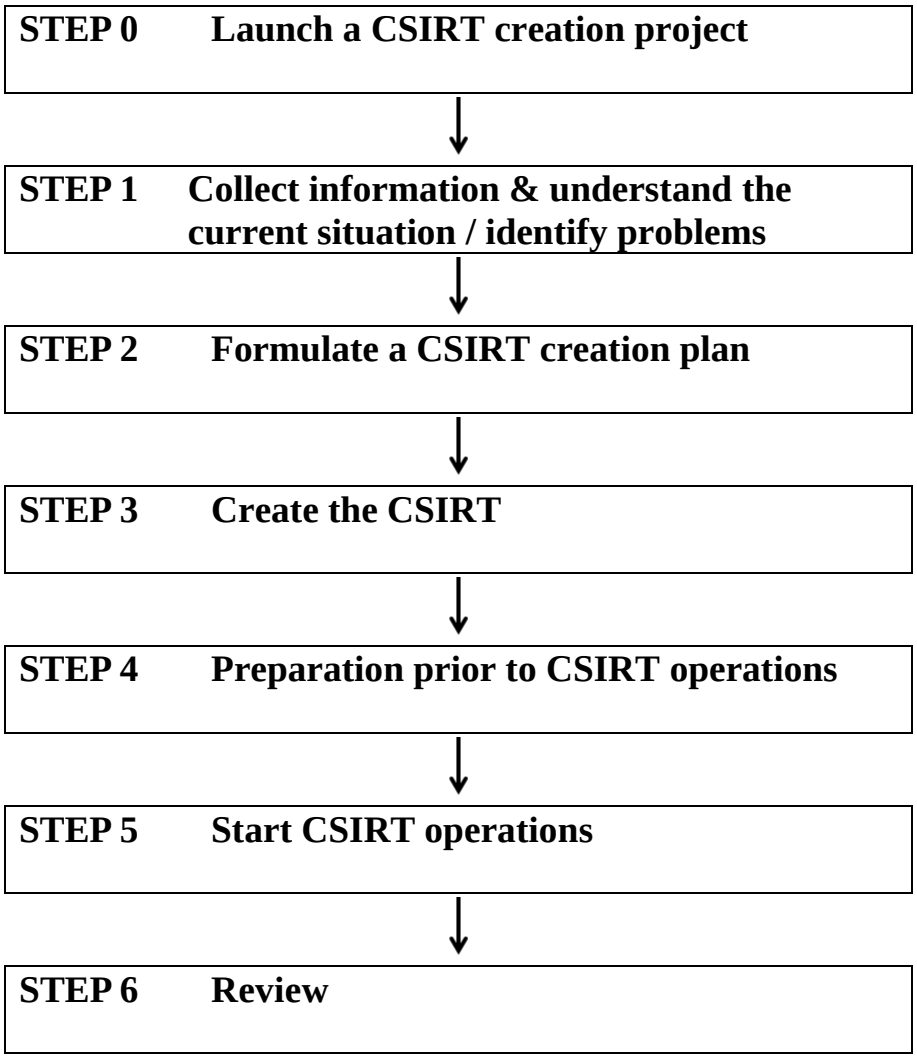
Most companies have already worked out some sort of measures to respond Incidents. However, that is only part of the organization and there are only a handful of companies that have in place an organization-wide framework for Incident response. There is an urgent need to create a CSIRT to properly respond to Incidents on a company-wide basis by making effective use of existing resources for Incident response.

Just one Incident can threaten the existence of a company and therefore measures should be taken without fail. When a company creates a CSIRT and establishes a framework for appropriate Incident response, productivity will improve. As a result, it will enjoy the increased confidence of society and achievement of its business goals.

[1] Preventive and corrective response to Incidents.
[2] For the purposes of this document, a "Security Event" is defined as an event that seems to be, but has not yet been determined to be, an Incident.

3 Steps in Creating a CSIRT

How to create a CSIRT depends on the environment inherent to the organization, such as the expertise of its staff or the size of its budget. However, there are basic steps that apply to any and all CSIRTs. The following chart shows the steps involved in creating a CSIRT.



4 Detailed Process for Creating a CSIRT

This section describes the details of the steps shown in **"3. Steps in Creating a CSIRT."**

STEP 0 Launch a CSIRT creation project

In STEP 0, you launch a "CSIRT creation project" to undertake the activities involved in creating a CSIRT. The following points should be taken into account to facilitate the progress of the project.

(1) Purpose (To create a CSIRT)
- Clarify the reasons for creating a CSIRT.

(2) Project members
- Consist of members relating to security Incidents.
- Clarify the interests of members.
- Ensure a means of communication for member who are physically remote.
- Establish a framework under which any expertise or opinions may be sought out when necessary.

(3) Scheduling
- Confirm time constraints.

(4) Project operation
- Clarify the rules of operation.
- Confirm decision-making flows in the project.
- Restrictions.

It is necessary to obtain the consent of management / decision-makers when launching a CSIRT creation project.

STEP 1 Collect information & understand the current situation / identify problems

In STEP 1, to begin with, examine the organizational background of the CSIRT to be created as well as the organization's current situation. Based on the findings from the examination, identify what should be achieved by creating the CSIRT and what issues might arise in creating the CSIRT.

The following are examples of information that you should collect as it shows the current situation of the organization. Please note that you may also refer to the "Appendix to CSIRT Starter Kit, (1) Details on information to be collected, current situation, and problems to be identified."

- ✓ Identify information assets to be protected and threats
- ✓ Information about the existing Incident response framework
- ✓ Information about the existing security policies and security-related documents
- ✓ Reference information

After that, sort out the current problems based on the collected information and conduct an examination to create the CSIRT. The following are examples of issues that should be considered when creating the CSIRT.

- ✓ What is the basic need for establishing the CSIRT?
- ✓ What type of services should be rendered?
- ✓ Where should the CSIRT be placed in the organization?
- ✓ How large does the CSIRT need to be?
- ✓ How much will it cost to create the CSIRT?

Based on the result of the examination about these issues, formulate a plan to create a CSIRT in STEP 2, below.

STEP 2 Formulate a CSIRT creation plan

(1) Examine the basic concepts of the CSIRT
(2) Examine the services to be provided
(3) Examine the internal company structure
(4) Examine external collaboration
(5) Examine resources
(6) Consider the gaps between the ideal and the CSIRT to be created
(7) Examine the schedule for creating the CSIRT

In STEP 2, formulate a CSIRT creation plan describing what type of CSIRT should be created to solve the issues and problems identified in STEP 1. The procedure for developing a plan for creating the CSIRT is shown below.

(1) Examine the basic concepts of the CSIRT

By drafting the basic concepts of the CSIRT, clarify the direction of the CSIRT to be created and examine the basic concepts of the CSIRT to gain a basic understanding of the objectives to be achieved.

- **Define the Constituency (service recipients)**

Constituency is the groups and organizations to which certain services rendered by the CSIRT will be made available. Defining constituency is a major factor in determining the direction of the CSIRT to be created.

For reference, examples of constituency are given below.

ABC-CSIRT's constituency
Information system administrators, personnel in charge of operations, users and security administrators who work for ABC K.K.

- **Define the mission**

Define the mission that should be achieved by creating the CSIRT. It is advisable to include the following details in the mission.

- Current position or situation of the organization
- Means to be used to achieve the goals
- Goals to be achieved

In addition, the major goal that should be achieved by the CSIRT varies depending on the organizational background of the CSIRT to be created but can be mostly summarized by the following.

- Conduct activities to prevent the occurrence / recurrence of Incidents
- Limit damage caused by Incidents and minimize loss by implementing appropriate responses and effective measures

The mission defined by each organization should be clear and concise in terms of the specific procedures for achievement and specific goals to be achieved. It should indicate how the CSIRT will interact with constituency as well.

For reference, an example of a mission is given below.

ABC-CSIRT's Mission
Our mission is to contribute to the enhancement of security at ABC K.K. and the information network society by acting as the core of the effort in the area of security at ABC K.K., serving as a contact point to provide consultation services for information security, and cooperating with organizations and experts in ABC K.K. by giving assistance for the detection, resolution, damage limitation, and prevention of security Incidents.

- **Define the Incidents to be handled**

Decide which of the problems identified in STEP 1 should be resolved by the CSIRT, and define the Incidents to be handled. Defining the Incidents to be handled will allow you to examine which services and resources, etc. the CSIRT should have as its functions.

"Appendix to CSIRT Starter Kit, (2) Incident Classifications" is provided as a reference for the kinds of Incidents to be handled. However, be aware that these classifications are given from the system perspective and actual damage will vary widely depending on the nature of the information system.

(2) Examine the services to be provided

"Service" means the specific details of the Incident response to be provided by the CSIRT you will create. The following shows an outline of general CSIRT services. However, the CSIRT does not have to provide all of these services. Examine what types of services the CSIRT should implement depending on its constituency, mission, and the Incidents it will handle.

CSIRT services can be divided into three major categories.

- **Corrective Incident response services**

  These services involve responding to Incidents and events relating to Incidents for the purpose of limiting damage caused by Incidents.

- **Preventive Incident response services**

  These services involve detecting and reducing the potential of Incidents and Security Events for the purpose of deterring the occurrence of Incidents.

- **Security quality improvement services**

  These services are aimed at improving internal security quality. They provide insights from the CSIRT's viewpoint and expertise so that effective activities can be performed through collaboration with internal organizations. They may also indirectly deter the occurrence of Incidents.

Table 1 shows a list of typical services. Since these are merely a list of typical CSIRT services, the CSIRT does not necessarily have to cover all of them and in some cases, may render other services. (For details about services, see "Appendix to CSIRT Starter Kit, (3) Services.")

Reactive	Proactive	Security quality improvement service
• Incident handling	• Providing security-related information	• Risk assessment / analysis
• Coordination		• Preparing and modifying business continuity and disaster recovery plans
• Computer forensics	• Detecting Incidents / Security Events	
		• Security consulting
• Onsite Incident response	• Technical trend surveys	
	• Security auditing / assessment	• Security education / training / enlightenment activities
• Incident response support	• Managing security tools	
		• Product evaluation / certification
• Artifact handling	• Developing security tools	
• Vulnerability information handling		

Table 1: Outline of CSIRT Services

Examine the services to be rendered as well as the authority required for the CSIRT to render the services. Incident handling[3)] is especially important and must be implemented as a CSIRT. In terms of Incident handling, the procedures therefor need to be established as a CSIRT.

If there are any existing internal Incident response functions, you should make effective use of such functions and examine their interrelationships with the CSIRT. Take into account how the existing Incident response functions will be transferred to the CSIRT as required.

(3) Examine the internal company framework

Examine the internal company framework to determine how the CSIRT will function in the company. "Appendix to CSIRT Starter Kit, (4) Departments involved in Incident response" shows a list of departments that should be put in place as part of the internal company framework.

For example, if all of the internal systems and employees will be the recipients of the services from the CSIRT, there must be an internal framework to allow the services to be rendered to such constituency. To achieve this, a framework like the one shown in Figure 1 may work effectively.

[3] Responding to Incidents that occur and activities for limiting damage and recovering.

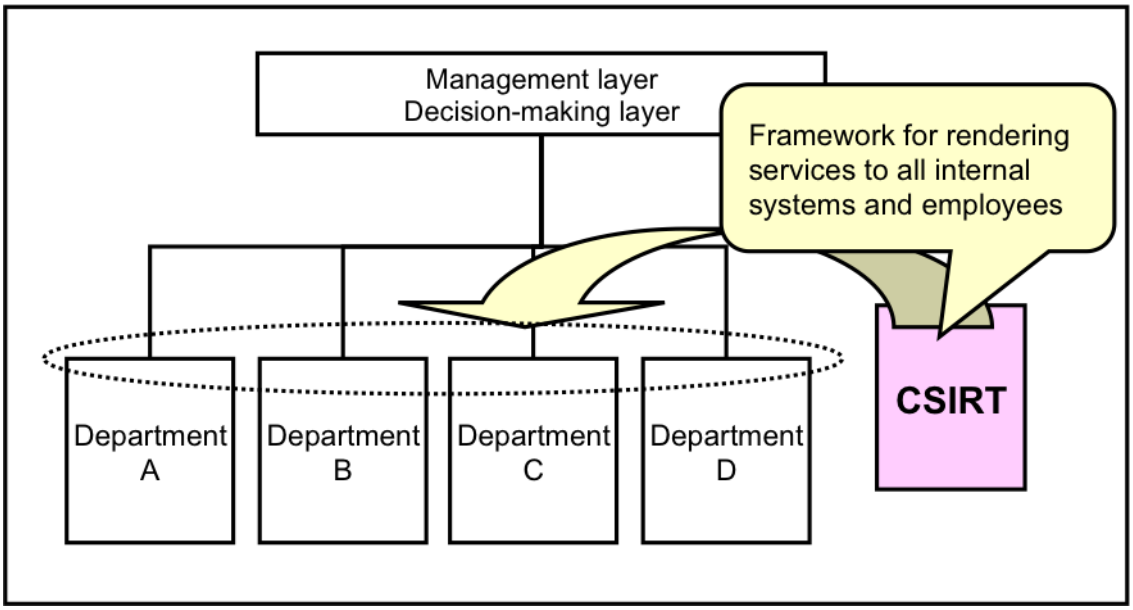


Figure 1: Framework for business entity where all internal systems and employees are constituency

Moreover, if it will be difficult for the CSIRT to render its services to all internal systems and employees because the business entity is large, a framework like the one shown in Figure 2 may work effectively. With this framework, you create a CSIRT for each department as well as a CSIRT for company-wide coordination.

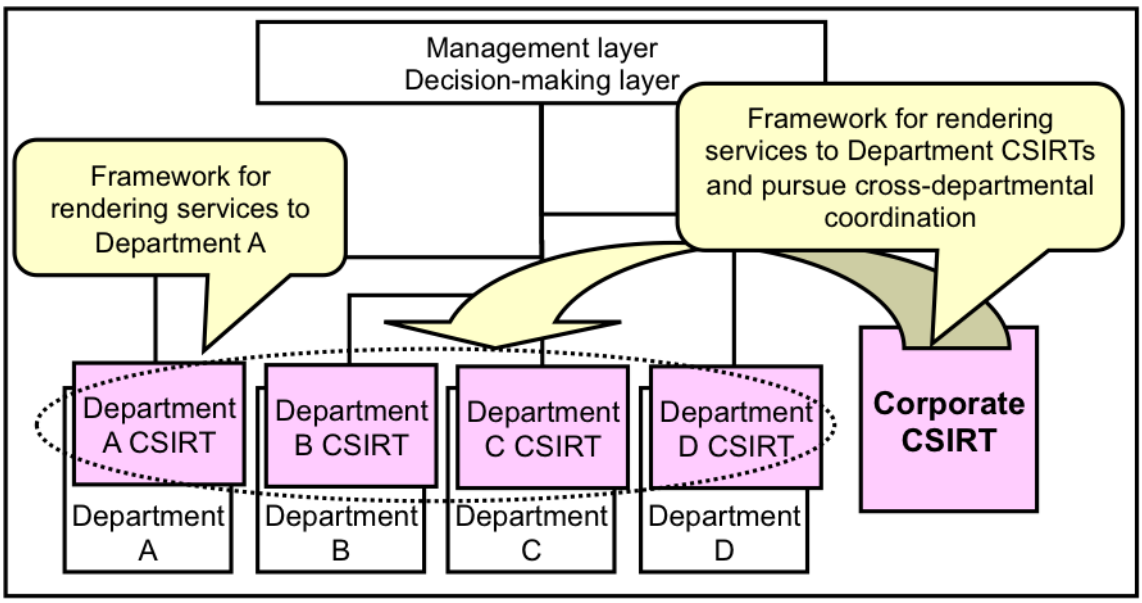


Figure 2: Framework for large business entity where all internal systems and employees is constituency

A hierarchical CSIRT framework similar to Figure 2 may work effectively for the CSIRT of a business entity that has group companies under its control, where all group companies are its constituency. Figure 3 shows the framework for such a case.

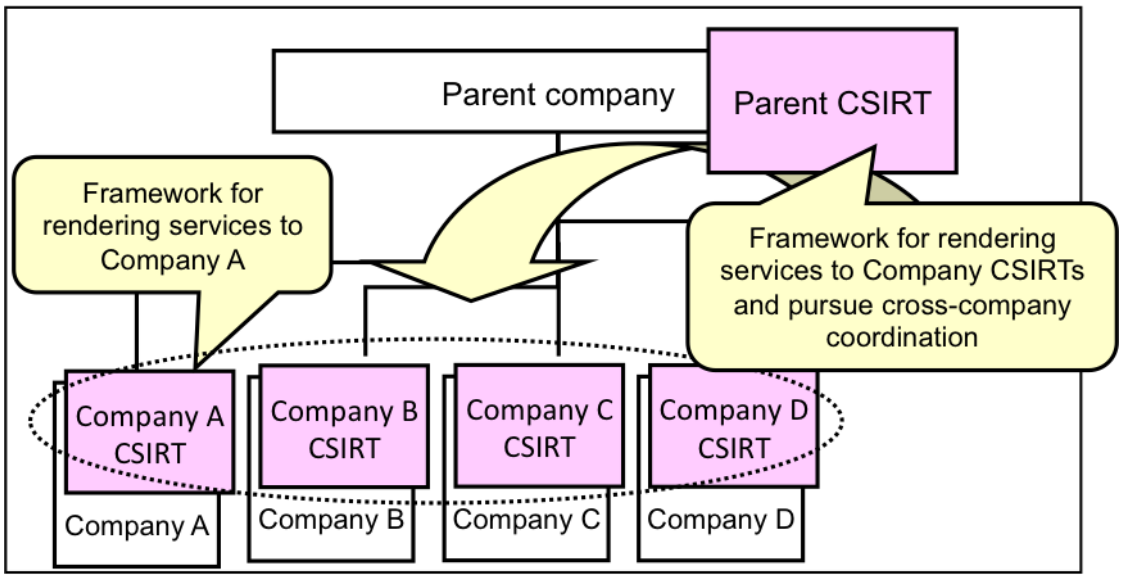


Figure 3: Framework for business entity where all group companies are constituency

In examining the internal framework, the authority required for the CSIRT as well as linked systems and demarcation point between the CSIRT and departments with existing Incident response functions will be reflected in the agenda of such examination.

In addition, also examine where the CSIRT should be located.

(4) Examine external collaboration

Sometimes, Incident response may require activities in collaboration with outsiders in addition to internal efforts. Therefore, examine the framework for collaborating with external organizations.

- **Collaborating with external CSIRTs**

  By collaborating with external CSIRTs, you will be able to conduct CSIRT activities more effectively in terms of detecting Incidents, sharing know-how about Incident response, implementing cross-organizational Incident handling, etc. In order to achieve effective collaboration between CSIRTs, you need to examine what type of external CSIRTs to collaborate with and what you will achieve.

  Examples of typical frameworks for collaboration between CSIRTs include FIRST[4)] and APCERT[5)]. The Nippon CSIRT Association[6)] serves as a community for the collaboration between CSIRTs in Japan.

[4] FIRST stands for Forum of Incident Response and Security Teams, and is an organization consisting of CSIRTs all over the world. (http://www.first.org/)

[5] APCERT stands for Asia Pacific Computer Emergency Response Team, and is an organization consisting of CSIRTs in the Asia Pacific region. (http://www.apcert.org/)

[6] Nippon CSIRT Association (official name: Nippon Computer Security Incident Response Team Association; also abbreviated as “NCA”) is a generic term of the organization to address Incidents relating to computer security. It performs activities to develop policies and procedures to deal with Incidents by collecting and analyzing Incident-related information, vulnerability information and predictive information on attacks. (http://www.nca.gr.jp/)

- **Collaboration with external organizations**

  The CSIRT may need respond to and/or collaborate with law enforcement agencies (e.g., police), the press, and product vendors in Incident response. You should establish a policy for how to deal with such external organizations in advance.

(5) Examine resources

Examine the resources required by the CSIRT. It is advisable to examine the resources that will be needed to render services and establish internal and external frameworks, and restrictions on resources in the organization should be taken into account as well. "Appendix to CSIRT Starter Kit (5) Resources" shows an outline of what types of human resources you may need.

- **Examine human resources**

  Examine how many staff members with the skills needed to conduct CSIRT activities will be required in your framework. If you cannot secure enough work-ready resources for Incident response, also examine training to develop staff. In such event, in addition to internal development, you may use commercial training for Incident response to efficiently develop your staff.

- **Examine facility resources**

  Examine the resources that will be required to operate the CSIRT. Since most of the Incident information handled by a CSIRT is confidential, arrange facilities to prevent any unnecessary disclosure of information even within the company.

- **Budget**

  Figure out the budget that will be required for CSIRT activities based on the amount of human and facility resources, as well as the costs required to maintain and operate/manage such resources. Both initial and running costs should be examined.

(6) Comparative examination

By comparing the "current situation," the "CSIRT to be created," and the "ideal Incident response," you can clarify the details of the implementation for creating the CSIRT and can get a vision for the development of the CSIRT after the start of operations.

- **Identify issues when creating the CSIRT by comparing the current situation with the situation after creation of the CSIRT**

  By comparing the current situation with the situation after the creation of the CSIRT, you can identify specific implementation issues during the creation of the CSIRT and prioritize them.

  Simulating Incident responses in accordance with Incident scenarios created based on actual Incidents in the past will allow you to effectively identify specific implementation issues in the current situation and the situation after the creation of the CSIRT. In addition, if a simulation reveals any flaws in your plan, you can also review the plan.

- **Consider the gaps between the ideal and the CSIRT to be created**

  If the created CSIRT does not achieve the ideal Incident responses due to limited resources or restrictions in the company, the deviation from the ideal should be

addressed as an issue. That issue will become a point for improvement after the CSIRT starts operating, giving you medium- and long-term activity guidelines for getting closer to that ideal.

(7) Examine the schedule for creating the CSIRT

Prepare material explaining the CSIRT creation plan to create an awareness of the need for a CSIRT in the company by sorting out the matters examined so far and showing the benefits of CSIRT activities.

Prepare materials for each of the following.

- **Management layer / decision-making layer**
  - Material for approving the creation of the CSIRT
- **Departments involved with Incident response**
  - Material for internal coordination
- **Constituency**
  - Material explaining about the CSIRT
- **CSIRT Staff/member**
  - Material for maintaining the internal CSIRT organization

STEP 3 Create the CSIRT

(1) Ensure management layer / decision-making layer approval and resources
(2) Implement internal coordination
(3) Explain to constituency
(4) Setup CSIRT framework
(5) Prepare necessary documents

In STEP 3, create a CSIRT based on the CSIRT creation plan prepared in STEP 2.

(1) Ensure management layer / decision-making layer approval and resources

Obtain approval from the management layer / decision-making layer for the CSIRT creation plan prepared in STEP 2, and at the same time, ensure there are sufficient resources to create the CSIRT.

(2) Implement internal coordination

Coordinate with the various internal departments involved with Incident response, and setup a framework under which the CSIRT can function.

(3) Explain to constituency

Explain to constituency about the creation of the CSIRT and gain their understanding about the CSIRT. Also, gain an understanding of the needs of constituency, and factor that into your examination of whether those needs should be reflected in the direction of the activities in creating the CSIRT.

(4) Setup CSIRT framework

Setup the framework for the CSIRT to be created. Procure resources and train staff.

(5) Prepare necessary documents

Create the materials for the CSIRT's activities. Use the content of the material explaining the CSIRT creation plan and treat them as internal CSIRT documents. Prepare a document outlining the CSIRT as well as the documentation required for operating the CSIRT. For the document outlining the CSIRT, see “Appendix to CSIRT Starter Kit (6) Documents.”

The documents required for operating the CSIRT should be more practical, for example, documents about the framework within the CSIRT, Incident response flows, rules and instructions to be observed in performing duties, list of contact points, etc.

If there appear to be any obstacles to creating the CSIRT, review the plan again and create a CSIRT that is optimal for your organization.

STEP 4	**Preparation prior to CSIRT operations** ✓ Implement simulations

In STEP 4, create Incident scenarios based on actual Incidents in the past and expected Incidents and implement desktop simulations of CSIRT activities. The simulations will allow you to confirm the usefulness of the created CSIRT and identify any problems before the start of operations. Problems that may be identified include the internal collaboration framework, communication channels for information, and the division of responsibilities. Representatives from the organizations involved with Incident response should be present for the simulations to ensure the effective implementation thereof.

Make absolutely sure to conduct an examination to identify point for improvements after conducting the simulations, and reflect the results thereof in the material prepared in STEP 3.

STEP 5 Start CSIRT operations

(1) Disseminate information
(2) Provide CSIRT services to service recipients
(3) Establish external collaboration framework

In STEP 5, commence CSIRT operations after following the creation procedures up to STEP 4.

(1) Disseminate information

You must inform constituency and outsiders about the existence of the CSIRT. In addition, you must let constituency know whom to contact at the CSIRT in order to get the CSIRT running. One effective means of keeping outsiders informed about the CSIRT is to utilize news releases.

(2) Provide CSIRT services to constituency

CSIRT operations will really start when its services are rendered to constituency. Work to reduce business risks through effective Incident response.

(3) Establish external collaboration framework

Establish the external collaboration framework that was examined in STEP 2. Establish effective collaboration to reduce business risks.

Once CSIRT operations have commenced, the objectives of the CSIRT Creation Project will have been achieved. The next step, STEP 6, describes the actual operations of the CSIRT.

STEP 6 Review

In STEP 6, review the organizational functions of the CSIRT, which commenced operations in STEP 5. A review needs be carried out on a regular basis after the start of operations in order to improve quality as well as to upgrade and enhance the CSIRT's functions. You should conduct the review based on the results of analyzing the activities of the CSIRT itself, understanding the needs of constituency, and the simulations that you have carried out. In addition, you need to keep in mind that the CSIRT must evolve according to the environment surrounding computer security, which is constantly advancing. Furthermore, you need to seek to create a helpful collaboration framework with outsiders on an ongoing basis.

5 Afterword

There can never be enough computer security. Creating a CSIRT is merely one means of reducing Incident risks, although it is an effective countermeasure for organizations against security incidents. The Nippon CSIRT Association's mission is to support CSIRT creation activities in Japan. If you have any questions, please contact us below.

< Contact Information for Nippon CSIRT Association >
c/o JPCERT Coordination Center
Hirose Building 11th Floor
3-17 Kanda-Nishiki-cho, Chiyoda-ku, Tokyo 101-0054
Email: nca-sec@nca.gr.jp
Phone: 03-3518-4600
(Please ask for the Secretariat representative at the Nippon CSIRT Association)

List of Authors and Collaborators

Hajime Ishizuka	NTT Communications
Kunihiko Sakuma	JSOL Corporation
Kaori Sagawa	KLIRRT
Motoki Sone	Sharp Corporation
Masahito Yamaga	NCA Expert Committee Member
Tomotaka Shoji	TOPPAN-CERT
Yoshinari Fukumoto	Rakuten-CERT
Yusuke Gunji	Rakuten-CERT
Yoshitane Tachibana	OKI-CSIRT
Akiko Numata	HIRT
Masato Terada	HIRT
Yuki Shigeiwa	IT Infrastructure Department, System Management Division, DeNA Co., Ltd.
Yoshiki Sugiura	NTT-CERT
Ikuya Hayashi	NTT-CERT
Takahiko Yoshida	NTT-CERT

English translation supported by

Masahiro Suzuki	YMC-CSIRT
Natsuko Inui	CDI-CIRT

Translated into English by

NTT EAST Corporation

Reviewed and commented by

VNCERT

Appendix to CSIRT Starter Kit

(1) Details on information to be collected, current situation, and problems to be identified

Major Item	Minor Item	Intended Use of formation
Understand targets to be protected and threats	Internal system network • Administrator in charge of operation • Important systems • Information assets	Materials for making decisions on Incidents to be handled by the CSIRT
	Information on Incidents in the past • Serious Incidents that occur • Incidents inclined to recur	
	Result of analysis of existing risks	
Existing Incident response framework	Preventive response to existing Incidents • Organization in charge of operation / cross-departmental collaboration framework / procedures	Identify problems and points for improvement in terms of functions and framework for existing Incident response
	Corrective response to existing Incidents • Organization in charge of operation / cross-departmental collaboration framework / procedures	
	Efforts to improve existing security • Organization in charge of operation / cross-departmental collaboration framework / procedures	
	External organizations involved in the existing Incident response	Establish effective external collaboration framework for Incident response
	Establish effective external collaboration framework for Incident response	
Existing security policy and security-related documents	Security policy	Understand restrictions in responding to Incidents
	Disaster recovery plan / business continuity plan	
	Security-related restrictions and regulations	
	Restrictions relating to physical security	
Reference information	Information about other CSIRTs[7]	Reference information for creating a CSIRT

Table 2: Information to be collected in STEP 1

[7] Information about leading CSIRTs in the world is available from the Nippon CSIRT Association. (http://www.nca.gr.jp/), FIRST (http://www.first.org/) or APCERT (http://www.apcert.org/).

(2) Incident Classifications

Probing, scanning, or any other suspicious access	• Searching for weaknesses (e.g., checking the versions of server programs) • Attempted intrusion (failed attempt) • Attempted worm infection (failed attempt)
Unauthorized relay of server programs	• Use of mail or proxy servers by third parties that is not intended by the administrator
Suspicious access	• Sender impersonation
Intrusion into systems	• Intrusion into systems, tampering (including using a root kit or any other dedicated tool) • Setting a program for DDoS attacks (third-party relay)
Attacks leading to interference of service operation (DoS)	• Interference by network congestion • Halt of server programs • Halt or reboot of the server OS
Computer virus / worm infection	•
Others	• Reception of unsolicited commercial e-mail (UCE), so-called e-mail spam

Table 3: Major Classifications of Typical Incidents

(3) Services

CSIRT services can be divided into three major categories.

1) Corrective Incident response services

Incident handling for the purpose of limiting damage caused by Incidents.

2) Preventive Incident response services

Services that detect and reduce the potential of Incidents and Security Events[8]8 for the purpose of deterring the occurrence of Incidents.

3) Security quality improvement services

Services aimed at improving internal security quality. They provide insights from the CSIRT's viewpoint and expertise so that effective activities can be performed through collaboration with internal organizations. They may also indirectly deter the occurrence of Incidents.

Table 1 shows a list of typical services. Since these are merely a list of typical CSIRT services, the CSIRT does not necessarily have to cover all of them and in some cases may render other services.

<table>
<tr><th>Proactive</th><th>Reactive</th><th>Security quality improvement service</th></tr>
<tr><td>• Incident handling</td><td rowspan="2">• Providing security-related information</td><td>• Risk assessment / analysis</td></tr>
<tr><td>• Coordination</td><td rowspan="2">• Preparing and modifying business continuity and disaster recovery plans</td></tr>
<tr><td rowspan="2">• Computer forensics</td><td rowspan="2">• Detecting Incidents / Security Events</td></tr>
<tr><td rowspan="2">• Security consulting</td></tr>
<tr><td rowspan="2">• Onsite Incident response</td><td>• Technical trend surveys</td></tr>
<tr><td>• Security auditing / assessment</td><td rowspan="2">• Security education / training / enlightenment activities</td></tr>
<tr><td rowspan="2">• Incident response support</td><td rowspan="2">• Managing security tools</td></tr>
<tr><td rowspan="3">• Product evaluation / certification</td></tr>
<tr><td>• Artifact handling</td><td rowspan="2">• Developing security tools</td></tr>
<tr><td>• Vulnerability information Handling</td></tr>
</table>

Table 4: Outline of CSIRT Services

The details of the services are as follows.

1) Corrective Incident response services

- Incident handling

  Incident handling is a basic function of the CSIRT and should be implemented without fail. Incident handling is the activity of responding to actual Incidents for the purpose of limiting damage and for recovery.

[8] For the purposes of this document, "Security Event" is defined as an event that seems to be, but has not yet been determined to be, an Incident.

In terms of Incident handling, the procedures therefor need to be established for the CSIRT as a whole.

The figure below shows the typical flow of steps in Incident handling, and provides a basis for preparing procedures.

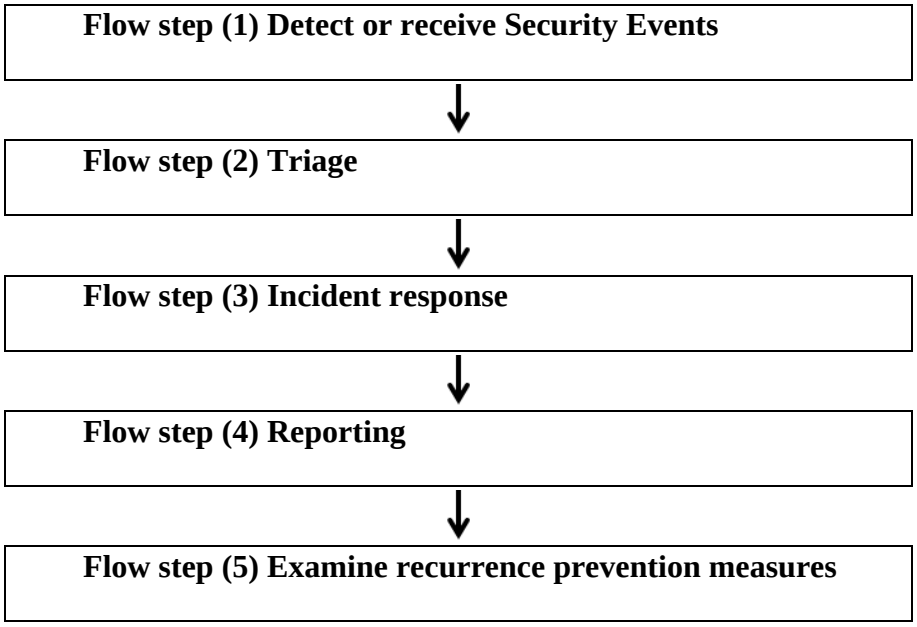


Figure 4: Basic Flow of steps in Incident Handling

The following describes the details of the flow.

(1) Detect or receive Security Events[9)]

This step involves receiving and managing reports on Security Events.

(2) Triage[10)]

Triage involves deciding whether a Security Event is an Incident or not, and prioritizing Incidents.

In triage, you define criteria and, as the CSIRT, must always perform triage based on the same criteria. However, the criteria should be reviewed on a regular basis because the elements that make up the criteria are constantly changing as the environment surrounding computer security rapidly advances.

Take the following points into account and perform triage based on the defined criteria.

- Verify the facts of the case.
- Examine the extent of the impact.

[9] For the purposes of this document, a "Security Event" is defined as an event that seems to be, but has not yet been determined to be, an Incident.

[10] In general, triage is a term used in medicine. As a medical term, it is used in referring to preferentially treating patients based on the urgency of their need for treatment in order to save as many lives as possible when resources are limited.

It is advisable to assign an identifier to each triaged Incident for easy reference later.

(3) Incident response

Incident response is the activity of investigating to determine the cause of an Incident and to make recovery efforts. You must analyze the triaged Incident and identify the nature of it.

An Incident may be characterized by:

- Attacker
- Attack target
- Date of Incident occurrence
- Attack method
- Extent of impact
- Main cause of damage
- Measures that may be taken
- Possibility of damage spreading

Determine and implement countermeasures based on the elements listed above.

The typical functions of the CSIRT in terms of Incident response are as follows.

- **Coordination**

  Sometimes, Incident handling may be required in multiple internal or external organizations under their own responsibility. The CSIRT is expected to play a role as coordinator by understanding the whole picture of an Incident in order to ensure consistent and effective Incident handling. Prompt Incident handling requires instantaneous coordination.

- **Onsite Incident handling**

  The CSIRT will directly perform recovery work for the system or network where an Incident has occurred. It is necessary to establish the division of responsibilities between the CSIRT and the person in charge of system operation.

- **Incident handling support**

  The CSIRT will carry out Incident handling by e-mail and/or telephone, and by providing documents or otherwise.

- **Computer forensics**

  Conduct Incident handling by preserving data from the computer afflicted by the Incident, which can provide evidence, and by analyzing, for example: (1) what type of damage was caused; (2) where the intruder got in; and (3) who the intruder is. The CSIRT needs to be staffed with members who have specialist skills, and equipped with dedicated tools for computer forensics. In addition, information must be thoroughly controlled within the CSIRT, because confidential information is likely to be handled in computer forensics.

- **Artifact handling**

  This step involves services for analyzing any suspicious program that is discovered through Incident handling. Conduct an investigation to determine whether the suspicious program has caused the Incident through an analysis of its source code as well as through an analysis of program behavior in an isolated environment. The CSIRT needs to be staffed with members who have specialist skills, and equipped with dedicated artifact facilities that are isolated from other networks.

(4) Reporting

Report the results of Incident handling after investigating the causes of the Incident and making recovery efforts. This may be used, for example, to accumulate know-how for Incident handling within the CSIRT and to give reports to the Incident owner[11)] and internal recipients.

(5) Examine recurrence prevention measures

You need to analyze the causes of Incidents that have been settled and take measures to prevent recurrence. In analyzing an Incident, you need to sort out the following items again.

- Details of the Incident
  - Causes
  - Damage situation
  - Triggers for detecting the Incident
  - Initial / provisional measures
  - Permanent measures
- Organizations involved in Incident handling
- Good and/or bad points about Incident handling

You need to take measures to prevent recurrence based on the results of the analysis.

2) Preventive Incident response services

- **Providing / announcing security-related information**

  This service provides constituency with security information. The following are examples of information that is provided.

  - Information disseminated about the activities of CSIRT / contact information.
  - Policies / procedures / security-related checklists
  - Information on prevalent viruses / worms and attack methods
  - Typical methods of Incident response
  - Incident statistics

[11] Organization or person where the Incident occurred.

- **Vulnerability information handling**[12)]

  This service is for analyzing information on vulnerabilities of software and hardware, and communicating it to constituency. Constituency must manage the application of patches to fix vulnerabilities and the implementation of workarounds. In vulnerability information handling, you must understand what types of software and hardware are used by the constituency

  In the case of vulnerabilities found in products developed by you, the handling of such vulnerabilities is included in this service.

- **Detecting Incidents / Security Events**

  This service is for detecting Incidents / Security Events, etc. Methods of detection include installing intrusion detection systems (IDS) or honeypots, analyzing logs of various servers, and dedicated environment for detecting information leaks via a peer-to-peer (P2P) file sharing applications.

- **Technical trend surveys**

  This service is for surveying trends, and giving expert opinions, on the latest security technologies, such as security enhancement technologies, Incident detection technologies, or intrusion techniques and verifying their usefulness for constituency. Implement useful technologies in the CSIRT and use them to provide information to constituency.

  - Security auditing / assessment

    Auditing / assessment services through document checking or penetration testing.

  - Developing security tools

    Service that develops tools to be used by the CSIRT or constituency. For example, it develops new Incident detection tools and scripts to make encryption technologies easier to use, or to automate patch distribution.

[12] The following are some examples of URLs that will serve as useful references for collecting vulnerability information.
Security Focus (http://securityfocus.com/)
Secunia (http://secunia.com/)
SANS Handler's Diary (http://isc.sans.org/diary.php)
FrSIRT (http://www.frsirt.com/english/)
JVN (http://jvn.jp/index.html)

3) Security quality improvement services

- **Risk assessment / analysis**

  This service is for identifying various risks that may interfere with the confidentiality, integrity or availability of a business entity or target information system, and analyzing the impact thereof. It is intended to recognize and reduce the current risks.

  In general, it includes the following.

  - Identifying information assets (prioritization)
  - Analyzing risks to the identified assets

  You can reduce risks by reflecting them in security policies, CSIRT services, Incident handling procedures, etc. based on the risk analysis.

- **Preparing and modifying business continuity and disaster recovery plans**

  This service reflects the CSIRT's Incident response functions in management strategies as business continuity and disaster recovery plans in order to protect the company from the loss of customer transactions to competitors, the lowering of market share, or the downgrading of corporate valuation by not letting any large-scale Incident interrupt important business, or by resuming business as soon as possible even if it has been interrupted.

- **Security consulting**

  This consulting service reflects the know-how of the CSIRT in the businesses of its constituency. Such know-how may be used to meet the security requirements in a business, or the know-how itself can become a business. Accordingly, how know-how is used will vary depending on the business lines of the company.

- **Security education / training / enlightenment activities**

  This service is for educating, training, and enlightening constituency through seminars, workshops, courses, educational materials, or the like in terms of the know-how of the CSIRT as well as the policies / procedures and others in which the know-how is reflected. This service is often provided in collaboration with the human resource development department or the like.

- **Product evaluation / certification**

  Through this service, the CSIRT evaluates and certifies products, tools, services, etc. by determining whether or not constituency can use them securely. The CSIRT needs to establish criteria for evaluation and certification that is suitable for the organization.

(4) Departments involved in CSIRT activities

Management layer / decision-making layer	Secures funds and resources, reflects the duties and authority required by the CSIRT in internal systems by approving the creation of the CSIRT. This layer is the recipient of final reporting on Incidents.
Department in charge of managing / operating information systems	It is deeply involved in CSIRT activities because it may sometimes be positioned as a service recipient and may have Incident handling functions.
Internal control department	Coordinates Incident response with internal control activities (keep in mind that the CSIRT's activities are only intended for responding to Incidents, not for performing internal control activities).
Legal department	Deals with legal matters in terms of Incident response.
Public relations department	Deals with the press in terms of Incident response.
Human resources department	Assigns / employs CSIRT staff. Implements HR measures in the unit where an Incident occurs (keep in mind that the CSIRT's activities are only intended for responding to Incidents, not for implementing personnel measures).
Human resources development department	Educates, trains, and enlightens constituency through seminars, workshops, courses, educational materials, or the like in terms of security know-how and policies.
Corporate planning department	Reflects business continuity plans / disaster recovery plans and Incident response.
Help desk	First level contact point for Incident handling.
Physical security department	Deals with theft of goods (especially, PCs). Manages and implements access control.

Table 4: Examples of Departments Involved in CSIRT Activities

(5) Resources

The following shows an outline of necessary resources.

- **Human resources**

  The CSIRT requires human resources that play the following roles.

  - Managers / team leaders / group leaders

    People who supervise teams or groups and make decisions for those teams or groups.
  - Triage staff

    Staff members in charge of triage. They perform triage according to the established criteria and prioritize Incidents to which handlers will be assigned.
  - Incident handlers

    Staff members who perform incident handling for triaged Incidents and support the core as CSIRT members.
  - Other staff for services to be rendered

    Staff members who perform the activities for the services to be rendered.

  Examples of the skills required for staff members are as follows.

  - Basic technical skills
    - OS (e.g., Windows, UNIX) skills
    - Network skills
    - Programming skills
    - Skills in using Pretty Good Privacy (PGP) encryption
  - Security skills
    - Skills regarding attacks against computers / vulnerabilities
    - Experience and skills in Incident handling
  - Personal skills
    - Coordination skills
    - Communication skills
    - Problem-solving capabilities

  These skills alone are not enough because they are basic skills. The CSIRT especially needs staff members who have the skills required for each of the services rendered by the CSIRT.

- Facility resources

  Examples of the equipment needed are shown below.

  - Basic technical skills for basic office equipment
    - Telephones for the CSIRT's exclusive use
    - Computers for staff (with an environment that provides secure communications, such as PGP encryption)
    - Mobile phones for staff
    - Dedicated printers
    - Dedicated shredders, etc.
  - Infrastructure for the CSIRT
    - Office for the CSIRT with access control
    - Network environment for the CSIRT
    - Safe
    - Incident handling system [13)]
    - PCs that can be taken out for Incident handling
    - Infrastructure required for providing services, etc.

[13] Incident handling system collectively refers to the set of tools for collecting, analyzing, and sharing Incident information.

(6) Documents

The templates for the documents outlining the CSIRT are defined in RFC2350[14]. We recommend that you prepare documents according to these templates.

---

1 Document Information
- 1.1 Date of Last Update
- 1.2 Distribution List for Notifications
- 1.3 Locations where this Document May Be Found

2 Contact Information
- 2.1 Name of the Team
- 2.2 Address
- 2.3 Time Zone
- 2.4 Telephone Number
- 2.5 Facsimile Number
- 2.6 Other Telecommunication
- 2.7 Electronic Mail Address
- 2.8 Public Keys and Encryption
- 2.9 Team Members
- 2.10 Other Information
- 2.11 Customer Contact Information

3 Charter
- 3.1 Mission Statement
- 3.2 Constituency
- 3.3 Sponsorship and/or Affiliation
- 3.4 Authority

4 Policies
- 4.1 Types of Incidents and Level of Support
- 4.2 Co-operation, Interaction and Disclosure of Information
- 4.3 Communication and Authentication

5 Services
- 5.1 Incident Response
  - 5.1.1. Incident Triage
  - 5.1.2. Incident Coordination
  - 5.1.3. Incident Resolution
- 5.2 Proactive Activities

6 Incident Reporting Forms

7 Disclaimers

[14] http://www.ietf.org/rfc/rfc2350.txt (English)
http://www.ipa.go.jp/security/rfc/RFC2350JA.html (Japanese)