# CSIRT Activities at NTT

*Masao Nagashima†, Yoshiki Sugiura, Tetsuya Abe, Takahiko Yoshida, and Akio Mukaiyama*

**Abstract**

This article introduces CSIRT activities and NTT-CERT operated by NTT Information Sharing Platform Laboratories.

## 1. Introduction

With the recent spread of broadband Internet connections and personal computers, security threats such as bots, phishing, and distributed denial of service (DDoS) attacks have become sophisticated and well organized. With the possibility of server attacks occurring at any time, it has become necessary for the defending side to become more organized in its activities. Although there are various viewpoints on what a computer security incident is, it covers anything that requires a response or assessment for security purposes. In addition to serious events like intrusions or virus infections, incidents include bot scans and vulnerability searches.

A framework called Computer Security Incident Response Team (CSIRT) exists for dealing with computer-security problems. AT NTT, the NTT Computer Security Incident Response and Readiness Coordination Team (NTT-CERT) [1] was established in October 2004 within NTT Information Sharing Platform Laboratories as a CSIRT for dealing with a variety of security-related problems within the NTT Group. There are also activities within the NTT Group companies for setting up CSIRT systems.

## 2. CSIRT

### 2.1 Outline

The activities and roles of a CSIRT are outlined in **Figs. 1** and **2**. For more details, see [2], [3]. Besides CSIRTs, there are organizations such as CERT (a registered trademark of the CERT Coordination Center (CERT/CC) in the USA), IRT (Incident Response Team), and CIRC (Computer Incident Response Capability), but these names may be thought of as nearly synonymous with CSIRT. A CSIRT is an organization whose activities span analysis, response, education, and research and development (R&D) with respect to computer security incidents. A variety of CSIRTs exist throughout the world with CERT/CC and US-CERT (US government CERT) in the USA and the JPCERT Coordination Center (JPCERT/CC) in Japan being particularly well-known. CSIRTs are also being actively established in the Japanese corporate world, as reflected by HIRT (Hitachi, Ltd.) and IIJ-SECT (Internet Initiative Japan, Inc.) [4].

As shown in Fig. 1, a CSIRT provides diverse types of support throughout the lifetime of an incident. It strives to prevent incidents from occurring in the first place and, in the event that an incident does occur, helps to limit the damage that it can cause. Furthermore, as shown in Fig. 2, a CSIRT has the role of coordinating responses, providing technology support, and collecting, analyzing, and providing information in conjunction with concerned parties. For example, a CSIRT will provide information and technology support to in-house security managers such as a chief information officer or chief security officer and to system operators and developers and will also interface with outside CSIRTs and security experts to collaborate on security technology and exchange information. Thus, CSIRTs play an important role in preventing and responding to incidents.

† NTT Information Sharing Platform Laboratories
Musashino-shi, 180-8585 Japan

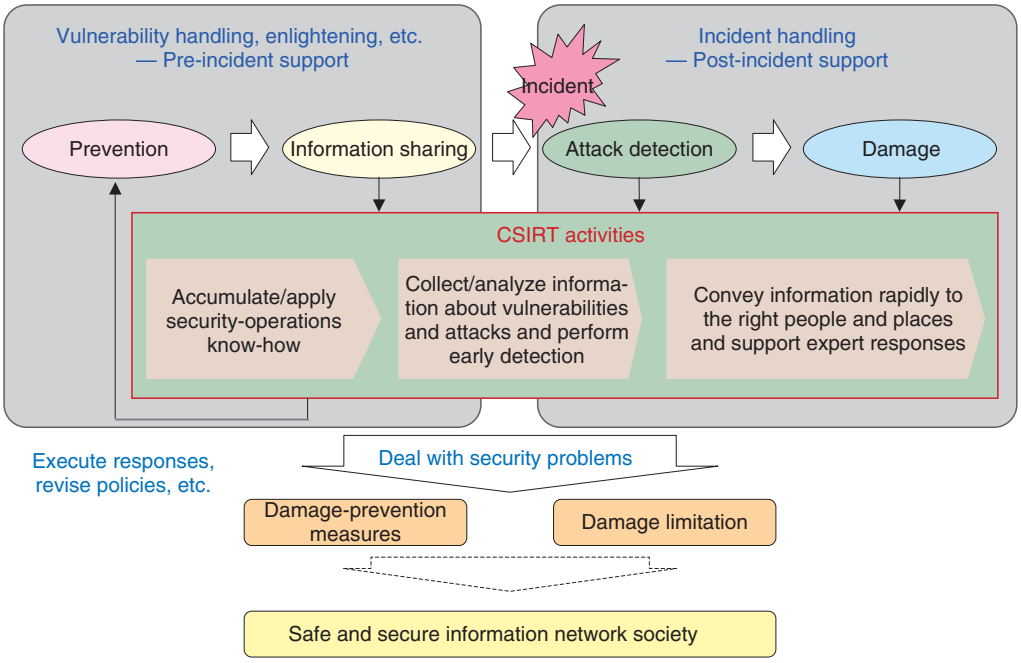
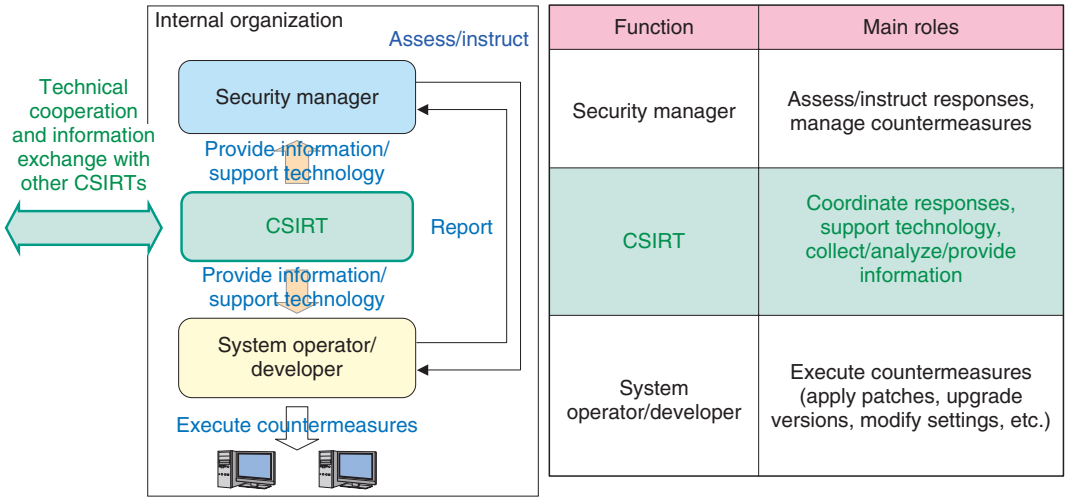



Fig. 1. CSIRT activities.




| Function | Main roles |
|---|---|
| Security manager | Assess/instruct responses, manage countermeasures |
| CSIRT | Coordinate responses, support technology, collect/analyze/provide information |
| System operator/developer | Execute countermeasures (apply patches, upgrade versions, modify settings, etc.) |

Fig. 2. CSIRT roles.

## 2.2 Requirements

Although there is no absolute definition of a CSIRT organization, the following requirements generally apply.

(1) Respond to incidents

A CSIRT must obtain information about security-related problems, analyze that information, investigate responses, and pass on information to the appropriate departments, offices, and responsible persons. It must then provide support for relevant technologies and response methods.

(2) Provide coordination

If multiple organizations are involved in a security problem, a CSIRT must coordinate with outside and

inside organizations and exchange security-related information to assist in solving the problem.

(3) Define target parties clearly

As explained below in the fourth requirement, responding to an incident always involves delicate information, which makes it important that the parties targeted for CSIRT services are clearly defined. This will facilitate the prompt provision of services to such targeted parties at the time of an emergency.

(4) Be a trustworthy team

Much of the information handled by a CSIRT is confidential and its processing requires great care. People who report incidents must be able to provide information to a CSIRT without anxiety.

### 2.3 Necessity

Preventive security measures in themselves cannot guard against all computer security incidents. In addition, the fact that business processes and information systems have a mutually dependent relationship via the network makes it difficult for any one organization or designated individual to come up with effective security measures.

As a team of experts on security measures, a CSIRT can share information about incidents that have occurred and coordinate information toward problem resolution so as to minimize the damage that results from incidents. It can also work to prevent the reoccurrence of similar incidents in the future. These are the two main objectives of a CSIRT. By constantly collecting and analyzing information about computer security incidents, a CSIRT can clearly and quickly specify appropriate responses to incident reporters.

Furthermore, the work of exchanging information and coordinating responses among internal and external organizations involves the handling of highly confidential information, which requires a rigorous level of information management. This is another reason why an organization like a CSIRT is needed. A key attribute of a CSIRT as an organization is its ability to manage information, and this is one reason why a CSIRT is trusted by outside parties.

## 3. FIRST

The Forum of Incident Response and Security Teams (FIRST) [5] is an international organization that brings together various CSIRTs. Today, with security incidents becoming international in scope and increasingly sophisticated, no single organization or region can handle problems that involve computer security.

In 1990, a group of eleven organizations established FIRST to enable CSIRTs in different regions throughout the world to exchange security information and build cooperative relationships for handling incidents in a manner exceeding national, regional, and organizational frameworks. CERT/CC is a founding member while JPCERT/CC has been a member since 1998.

As of December 2009, more than 200 teams from more than 40 countries and regions around the world were FIRST members. They exchange various types of information via mailing lists with regard to incident examples and response know-how.

From the corporate world, organizations such as BTCERTCC (BT), Telekom-CERT (Deutsche Telekom), MSCERT (Microsoft), and Sun (Sun Microsystems) centered in Europe and the USA are members of FIRST. NTT-CERT has been a FIRST member since January 2005.

Japan is represented by 16 teams (as of December 2009), including JPCERT/CC, HIRT, and IIJ-SECT as well as NISC (Cabinet Secretariat) and CFC (National Police Agency) [6].

FIRST holds an annual conference, usually in June. This is a unique international meeting bringing together CSIRT members and security experts from around the world. It provides a forum for giving presentations on diverse themes such as CSIRT operation know-how and problems related to general security technologies. Nonmembers may also participate. The site for the 2008 annual conference was Vancouver, Canada. The first annual conference to be held in Japan was the 2009 gathering in Kyoto held from June 28 to July 3. The domestic venue prompted many Japanese entities to participate. In addition, the number of participating countries was a record at 52, and favorable comments on the proceedings were received from overseas participants [7].

A technical colloquium (TC) is also held several times a year in different regions around the world to deal with topics related to security technologies. A TC is open only to FIRST members. NTT-CERT participates in selected TCs to discuss security issues, collect information about European and American trends, and interface with other teams.

## 4. Nippon CSIRT Association (NCA)

In 1998, JPCERT/CC was the only CSIRT from Japan in FIRST. When NTT-CERT became a FIRST member in January 2005, it was the 6th Japanese team to join. Since then, the number of Japanese

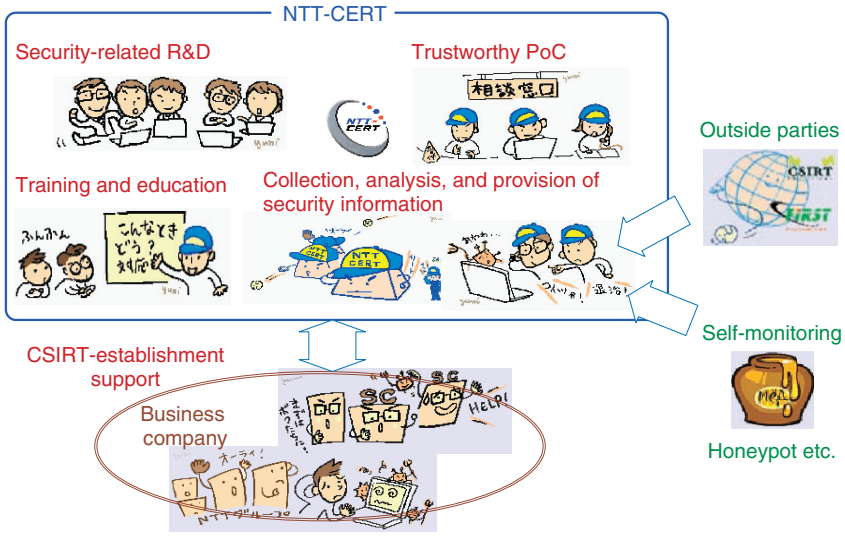



Fig. 3. Five pillars of NTT-CERT activities.

teams has expanded to 16 (as of December 2009). These figures reveal that CSIRT activities, which were originally centered on Europe and the USA, have expanded considerable to Japan.

Against this background, the Nippon CSIRT Association (NCA) [8] was founded in 2007 by NTT-CERT together with JPCERT/CC, HIRT, IIJ-SECT, JSOC (LAC, Ltd.), and SBCSIRT (Softbank Group). It aims to provide a forum in Japan for solving common problems while achieving tightly knit interfacing at a level heretofore never reached to facilitate mutual cooperation. The number of NCA members has since expanded to 14 teams, mainly corporate ones (as of December 2009).

NCA holds a general assembly once a year and information-exchange meetings for members four times a year. Members form working groups on themes of interest with the aim of creating technical documents, studying CSIRT issues, and sharing security threat information.

As part of CSIRT-establishment support, NCA holds discussions with organizations interested in the CSIRT concept, provides support for organizations wishing to join NCA, and promotes CSIRT activities in Japan.

NCA held a TRANSITS [9] CSIRT training workshop for establishing and operating CSIRTs in March 2009 [10] and cooperated in cyber seminars held by APCERT, a CSIRT group in Asia, in December 2007 and December 2008.

## 5. NTT-CERT

NTT-CERT commenced activities in October 2004 on the basis of the information-security efforts made by NTT Information Sharing Platform Laboratories up to that time. As a core CSIRT in the NTT Group, NTT-CERT is a trustworthy point of contact (PoC) for security matters when cooperating with organizations and experts both inside and outside the group and supporting the detection, analysis, damage limitation, and prevention of computer security incidents. In this way, NTT-CERT aims to contribute to improved security not only in the NTT Group but also throughout the information network society. The five pillars of NTT-CERT activities are summarized below (**Fig. 3**).

(1) Trustworthy PoC

NTT-CERT is establishing a global network of security-related organizations and communities both inside and outside the NTT Group and provides a trustworthy PoC for internal NTT Group organizations and outside organizations.

(2) Collection, analysis, and provision of security information

NTT-CERT analyzes a huge amount of security-related information, issues bulletins and advisories, and releases and horizontally deploys know-how about incident response and prevention. It also conducts and supports the analysis of the system involved in an incident as the need arises. When conducting

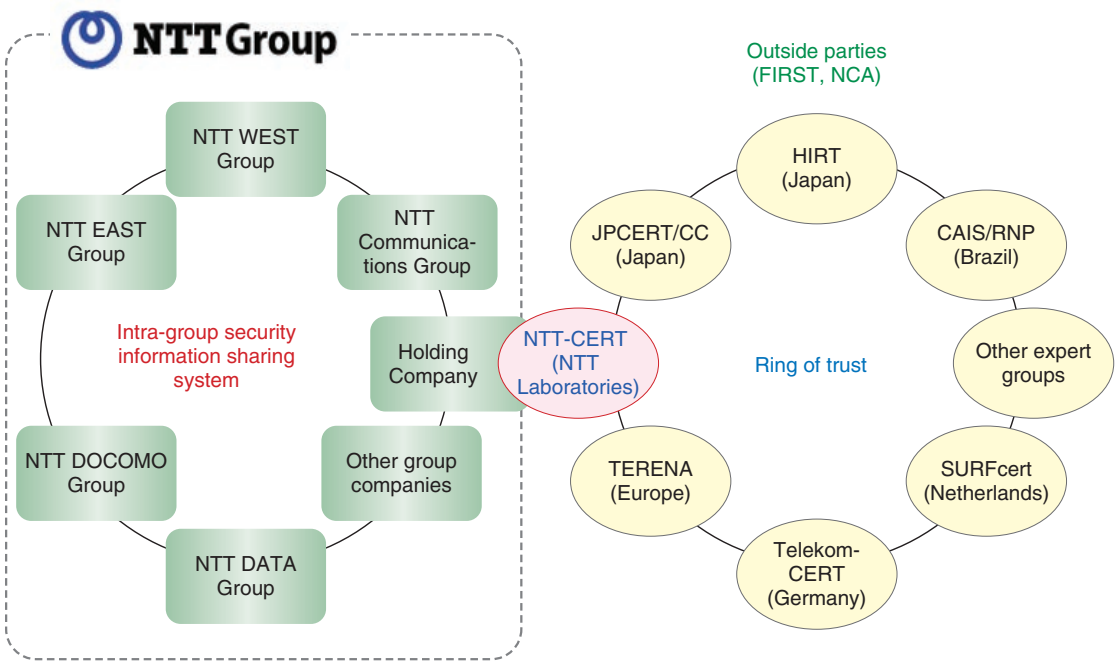



Fig. 4. Cooperative framework.

such an analysis, NTT-CERT uses special forensic techniques to inspect the system and find the incident's source without affecting the trail left behind in the system. The inspection procedure consists of four steps: (1) saving data, (2) analyzing saved data, (3) creating a report on analysis results, and (4) horizontally deploying analysis results to the departments and offices that need them. Clarifying the incident source through this inspection procedure makes it possible to study measures for preventing the occurrence of similar incidents. In addition, the horizontal deployment of analysis results to departments and offices that use similar systems to the one involved in the incident helps to prevent the occurrence of a similar incident.

(3) CSIRT-establishment support

NTT-CERT works with system operators within organizations and other CSIRTs in supporting the establishment of CSIRTs to promote and coordinate the management of incidents within an organization. At NTT-CERT, a Japanese-language version of the TRANSITS CSIRT training workshop developed by the Trans-European Research and Education Networking Association (TERENA) [11] was prepared in collaboration with JPCERT/CC and NTT DATA. This material is being used to conduct TRANSITS workshops targeting the NTT Group (held at NTT-CERT) and TRANSITS workshops targeting Japanese companies and other organizations (held at NCA).

(4) Training and education

To improve security throughout the NTT Group, NTT-CERT also supports the training and education of security personnel in group companies. NTT-CERT provides the knowledge gained in daily CSIRT work—such as incident management, inter-organization coordination, information collection and analysis, and even R&D—as advanced training material for security personnel sessions in periodically held training sessions. NTT-CERT also periodically holds workshops and discussions on current topics in conjunction with group companies.

(5) Security-related R&D

NTT-CERT researches and develops technologies for defending against new threats, systems for efficiently managing security matters, and a framework for efficiently establishing and operating a CSIRT. It passes the results of this R&D onto NTT Group companies.

## 6. Concluding remarks

Huge group enterprises like NTT require a system for linking the security departments of individual group companies to improve overall security. NTT-CERT aims to provide total support in establishing a CSIRT system and linking the CSIRTs within the NTT Group. As security incidents become international in scope and more sophisticated, it is becoming increasingly difficult for a single team to respond to diverse types of security incidents. It is therefore becoming all the more important to promote a cooperative framework with members of FIRST and NCA (**Fig. 4**). In addition to fielding incident reports, NTT-CERT processes information and accepts inquiries about security-related problems. Anyone involved with the work of the NTT Group is free to contact NTT-CERT.

## References

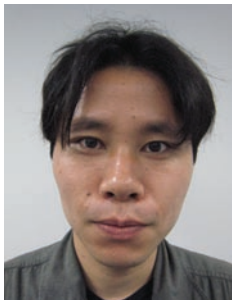

[1] NTT-CERT.
http://www.ntt-cert.org/index-en.html
[2] RFC2350 Expectations for Computer Security Incident Response.
http://www.ipa.go.jp/security/rfc/RFC2350EN.html
[3] CSIRT material.
http://www.jpcert.or.jp/csirt_material/ (in Japanese).
[4] Examples of Japanese CSIRTs.
http://www.nca.gr.jp/member/index.html (in Japanese).
[5] FIRST.
http://www.first.org/
[6] Members around the world.
http://www.first.org/members/map/
[7] Security Across the Oceans.
34th "FIRST Conference" held in Kyoto with about 400 participants from around the world.
http://internet.watch.impress.co.jp/docs/column/security/20090709_300875.html (in Japanese).
[8] Nippon CSIRT Association.
http://www.nca.gr.jp/ (in Japanese).
[9] TRANSITS.
http://www.terena.org/activities/csirt-training/
[10] TRANSITS Workshop NCA, held in Japan.
http://www.nca.gr.jp/2009/transits/ (in Japanese).
[11] TERENA.
http://www.terena.org/

**Masao Nagashima**
Senior Research Engineer, Group Leader of NTT-CERT, Secure Communication Project, NTT Information Sharing Platform Laboratories.
He received the B.E. and M.E. degrees in science and engineering from Keio University, Kanagawa, in 1988 and 1990, respectively. He joined NTT Communication Network Research Laboratories in 1990 and had been engaged in R&D of an operations system for the Intelligent Network and grand design of internal information systems. He has been the leader of NTT-CERT since July 2008.

**Yoshiki Sugiura**
Research Specialist, member of NTT-CERT, Secure Communication Project, NTT Information Sharing Platform Laboratories.
From 1985 to 1998, he worked as a programmer and researcher in a software development company. He was a member of JPCERT/CC from 1998 to 1999 and a manager from 1999 to 2002. Since 2004, he has been working at NTT-CERT as the manager of an incident handling team and a CSIRT creation & management team. He is the representative of NCA (Nippon CSIRT Association). His qualifications are CSIRT specialist, computer security specialist, and computer programmer. His recent interests are computer security, CSIRT creation and management, the development and improvement of security teams and sociopsychology.

**Tetsuya Abe**
Senior Research Engineer, member of NTT-CERT, Secure Communication Project, NTT Information Sharing Platform Laboratories.
He received the B.S. degree in physics from Keio University, Kanagawa, in 1988. He joined NTT LSI Laboratories in 1988 and engaged in development on an on-chip RISC controller. In 1996, he moved to NTT Multimedia Network Laboratories, where he engaged in high-speed protocol processing. In April 2000, he moved to NTT EAST, where he engaged in developing security-related designs for process control systems. Since joining NTT Information Sharing Platform Laboratories in July 2007, he has been a member of NTT-CERT. He received the Best Industrial ASIC Award ED&TC in 1996. He is a member of the Institute of Electronics, Information and Communication Engineers of Japan.

**Takahiko Yoshida**
Research Engineer, FIRST Representative, member of NTT-CERT, Secure Communication Project, NTT Information Sharing Platform Laboratories.
He received the B.E. degree in mathematics from Tokyo University of Science and M.E. degree in information science from Tohoku University, Miyagi, in 1998 and 2000, respectively. He joined NTT EAST in 2000 and worked in facilities planning from 2000 to 2006. He has been working for NTT and at NTT-CERT as an incident handling team member and a CSIRT creation & management team member since 2006.



**Akio Mukaiyama**
Research Engineer, member of NTT-CERT, Secure Communication Project, NTT Information Sharing Platform Laboratories.
He received the B.E. and M.E. degrees in engineering from Yamanashi University in 2001 and 2003, respectively. Since joining NTT in 2003, he had been engaged in R&D of ubiquitous computing. Since 2005, he has been working at NTT-CERT as an incident handling team member and forensic investigator. He is a member of the Information Processing Society of Japan.