Definition of Roles Required for CSIRT(Ver. 1.5)

March, 2017
Original document (in Japanese) created by
CSIRT Human Resources Sub-Working Group,
Nippon CSIRT Association

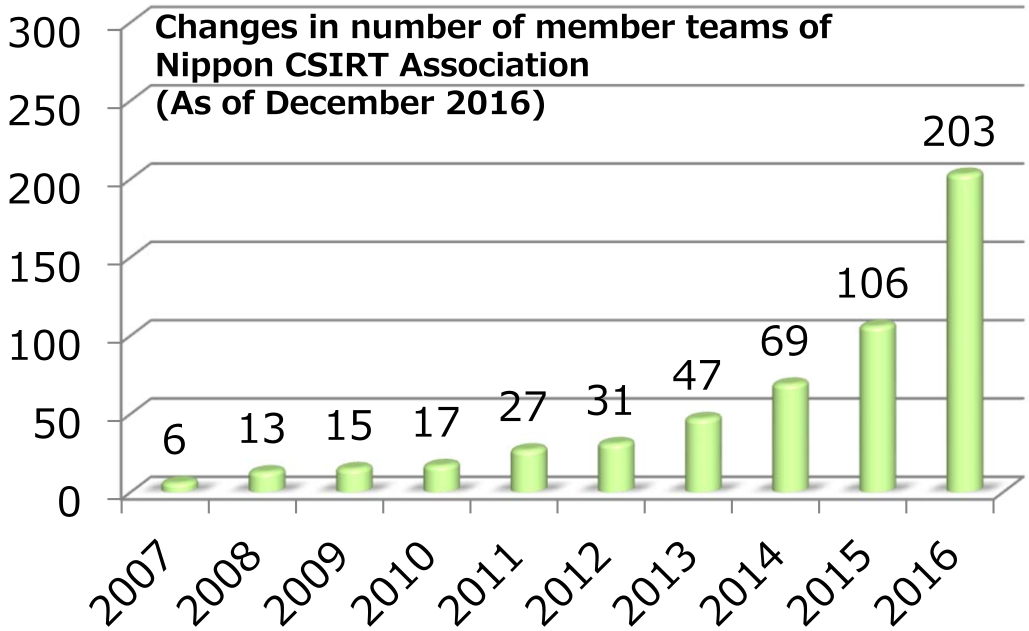
February 1, 2019
English translation by JPCERT/CC

Table of Contents

1. Introduction

Japanese companies tend to increase investment in human resources such as setting up security management divisions and deploying security administrators as there is an increase in cyber attacks and damage caused by internal crimes. This tendency is also evident in the rapid growth in the number of member teams at the Nippon CSIRT Association. However, much is talked about the “lack of security personnel” without any clarification on what needs to be done by CSIRTs, how to secure the necessary human resources, and how to train the resources acquired.

This document unravels the chaotic issues and summarizes the roles required for CSIRT as well as training and skills of human resources necessary to fulfill the roles. Also, it broadly categorizes the enterprise into three models and explains which roles could be insourced/outsourced for each model, as a reference.



CSIRT Human Resources Sub-Working Group will continue to hold discussions and make revisions using the feedback received from many people involved in CSIRT activities.

It is much appreciated if this document can be of any help towards the activities of newly established CSIRTs in Japan.

1. Purpose of this Document

- This document aims to assist with the continuing activities of CSIRT by clarifying the functions, team structures, and human resources necessary for CSIRT in each enterprise.
  In particular, this document is compiled in such a way as to focus on the following two points.
  - Providing information that will be helpful to establish a new CSIRT, outsource a part of CSIRT roles, or define and secure human resources in charge of CSIRT, etc.
  - Providing information that will be helpful to:
    - Create guidelines for recruiting CSIRT personnel within the organization, or
    - Prepare a request for proposal (RFP) or create guidelines for recruiting personnel, when requesting CSIRT functions and staff outside the organization

2. Human Resource Challenges in CSIRT and Direction of Solution

- There are many human resource challenges which we may face when establishing an internal CSIRT at a general enterprise, such as what kind of human resources should be secured, how to train the personnel, whether the CSIRT works effectively or not, and so on.
  This document illustrates the direction in problem-solving as well as demonstrates the three CSIRT models and their implementation.

Challenges	Direction of Solution
No idea about the human resources required for CSIRT.	✓ Define the necessary prerequisite skills for each role
Not sure how to train the resources secured for CSIRT.	✓ Define the additional educational skills for each role ✓ Eligible certifications ✓ Educational methods
Not sure what needs to be done in CSIRT.	✓ Define roles that consists CSIRT ✓ Define tasks for each role ✓ Relationship between roles
The expected output of CSIRT is too high to achieve for a general enterprise which is not specialized in security.	✓ Categorize models in CSIRT ✓ Consideration of outsourcing ✓ Consideration of dual roles ✓ Number of people required at CSIRT

3. Roles in CSIRT and Their Typical Tasks

- Roles that could be owned by a CSIRT at each organization assumed in this document and their typical tasks

Functional Classification	Roles	Typical Tasks
Information Sharing	External PoC: In charge of contact outside the organization	Sharing information with NCA, JPCERT/CC, CSIRT, police, regulatory authorities, etc.
	Internal PoC: In charge of contact within the organization and IT department coordination	Sharing information with legal affairs, foreign relations, IT department, public relations, other business divisions, etc.
	Legal Counsel: CSIRT in-charge of legal division	Translating between compliance, legal content, and systems
	Notification In-Charge: In charge of coordination within the organization/information transmission	Point of contact with relevant departments and information transmission
Information Gathering and Analysis	Researcher: In charge of information gathering; Curator: In charge of information analysis	Regular work, gathering incident information, analysis of various information, and understanding international affairs
	Vulnerability Analyst: In charge of vulnerability diagnosis	Inspection and diagnosis of OS, network, and secure programming
	Vulnerability Analyst: In charge of vulnerability assessment	Assessment of OS, network, and secure programming diagnosis results
	Self-Assessment In-Charge	Risk assessment in normal times, analysis of vulnerability during emergency, and impact study
	Solution Analyst: In charge of security strategy	Creating solution map, Fit&Gap analysis, risk assessment, and validity assessment during emergency
Incident Response	Commander: Overall CSIRT control	Overall CSIRT control, decision making, and sharing information with internal PoC, board member, CISO or management
	Incident Manager: In-charge of incident management	Understanding the response status of incidents, reporting to commander, and understanding history of responses
	Incident Handler: In charge of incident handling	Site supervisors of incidents and collaboration with security vendors
	Investigator: In charge of survey and investigation	Secret surveillance using comprehension of in-house systems, analytical skills, logical thinking required for investigation
	Triage In-Charge: In charge of selecting priority	Determining priorities for events
	Forensic In-Charge	Preservation of evidence, systematic identification, footprint tracking, and malware analysis
Education within the Organization	Trainer: In charge of education and awareness	Improving/raising literacy of the organization

4. Prerequisite Skills for Appointment and Additional Educational Skills for Each Role

4.1 “PoC (Point of Contact)”

In charge of contact outside and within the organization, and IT department coordination

Share information by serving as an outside point of contact with JPCERT/CC, NISC, police, regulatory authorities, NCA, other CSIRTs, etc.

Share information by serving as an internal point of contact with the IT department, legal affairs, foreign relations, public relations, other business divisions, etc.

Prerequisite Skills for Appointment

- ✓ Ability to convey information correctly
- ✓ Basic IT literacy of ITSS Level 2 or so
- ✓ Ability to judge information appropriately

Additional Education Skills

- ✓ Ability to gather information, and generate/report intelligence
- ✓ Knowledge of external organizations and academic institutions on cyber security issues
- ✓ Knowledge of known vulnerabilities

Prerequisite Skills for Appointment and Additional Educational Skills for Each Role

4.2 "Legal Counsel"

In charge of legal affairs

Provide legal advice when legal issues and compliance problems occur in information technology, cyber security, and so on. When the legal division lacks IT skill, the IT department can bridge the gap by translating the details for the legal department.

Prerequisite Skills for Appointment

- ✓ Knowledge related to security related laws or basic IT literacy of ITSS level 2 or so
- ✓ Ability to track and analyze technical trends and law trends related to cyber security
- ✓ Ability to convey information correctly

Additional Education Skills

- ✓ Laws related to security, deeper knowledge of IT literacy
- ✓ Knowledge of incident response and handling
- ✓ Knowledge on secure procurement, supply chain, and outsourcing

Prerequisite Skills for Appointment and Additional Educational Skills for Each Role

4.3 “Notification In-Charge”

In charge of coordination within the organization/ information transmission

Coordinate within the organization and transmit information to relevant departments. Coordinate with IT department when there is an impact in the systems of the organization.

Prerequisite Skills for Appointment

- ✓ Ability to convey information correctly
- ✓ Basic IT literacy of ITSS Level 2 or so
- ✓ Ability to appropriately judge and explain information
- ✓ Knowledge of the organization system
- ✓ Negotiation skills

Additional Education Skills

- ✓ Fundamentals of IT security and security management
- ✓ Knowledge of incident response and handling
- ✓ Knowledge of security guidelines of the organization and compliance matters
- ✓ Knowledge of known vulnerabilities
- ✓ Ability to understand event-related risks and explain priorities

Prerequisite Skills for Appointment and Additional Educational Skills for Each Role

4.4 "Researcher"

In charge of information gathering

Gather information related to security events, threats, vulnerability, attacker profile, international affairs and media, etc., and hand over to the curator. Analysis of stand-alone devices, but correlational analysis will not be performed.

Prerequisite Skills for Appointment

- ✓ Basic security knowledge
- ✓ Media literacy; Ability to absorb information with a pinch of salt
- ✓ Ability to correctly read documents

Additional Education Skills

- ✓ Knowledge of relations between nations, and hacktivist*
- ✓ Ability to learn and utilize the unique identity of media
- ✓ Ability to correctly read information detected by security devices
- ✓ Knowledge of attack tactics, stages, techniques, and procedures

*Hacktivist is a word coined from hacking and activists who carry out political activities, and they refer to people and organizations who engage in political hacking activities.

Prerequisite Skills for Appointment and Additional Educational Skills for Each Role

4.5 “Curator”

In charge of information analysis

Analyze the information gathered by the researcher and decide whether to apply that information to the organization. Often implemented in Security Operation Center (SOC) along with the researcher.

Prerequisite Skills for Appointment

- ✓ Knowledge of business and security architecture of the organization
- ✓ Media literacy; Ability to absorb information with a pinch of salt
- ✓ Ability to correctly read documents

Additional Education Skills

- ✓ Ability to gather information and leverage intelligence
- ✓ Ability to analyze relations between nations, and hacktivists
- ✓ Ability to learn and utilize the unique identity of media
- ✓ Ability to correlate information detected by security devices
- ✓ Knowledge of attack tactics, stages, techniques, and procedures
- ✓ Ability to judge whether the information must be applied to the security measures of the organization

Prerequisite Skills for Appointment and Additional Educational Skills for Each Role

4.6 “Vulnerability Analyst”

In charge of vulnerability diagnosis and assessment

Inspect whether the OS, network, middleware and applications are secure, and evaluate the diagnosis results.

Prerequisite Skills for Appointment

- ✓ Knowledge of vulnerability of OS, network, application, DB
- ✓ Ability to conduct packet level analysis
- ✓ Knowledge of penetration testing and tools
- ✓ Knowledge of common attack methods

Additional Education Skills

- ✓ Knowledge of security architecture of the organization
- ✓ Knowledge of emerging information security technologies
- ✓ Knowledge of threat information
- ✓ Ability to utilize computers, network defense, and vulnerability assessment tools

Prerequisite Skills for Appointment and Additional Educational Skills for Each Role
4.7 “Self-Assessment In-Charge”

Personal Information Protection Law

Analyze the current situation of environment in the organization and information assets. Conduct assessment in normal times, and identify the extent of impact based on assessment results when an incident occurs.

Prerequisite Skills for Appointment

- ✓ Basic IT literacy of ITSS Level 2 or so
- ✓ Ability to listen and comprehend risk assessments and prepare documents

Additional Education Skills

- ✓ Knowledge of Personal Information Protection Law, official contracts of PCIDSS, ISMS
- ✓ Knowledge of guidelines related to security policies and system architecture of the organization, and compliance matters
- ✓ Knowledge of the risk management process
- ✓ Ability to interpret intelligence and latest technologies

Prerequisite Skills for Appointment and Additional Educational Skills for Each Role

4.8 “Solution Analyst”

In charge of security strategy

Develop a security strategy according to the business plan of the organization. Conduct risk assessment using Fit&Gap analysis of the current situation and goals, and create a solution map to promote the introduction of solutions. Check the validity of solutions introduced, share information with the management, and reflect the findings in the improvement plan.

Prerequisite Skills for Appointment

- ✓ Ability to plan according to business vision of the organization
- ✓ Knowledge of security guidelines of the organization and compliance matters
- ✓ Ability to utilize the risk management process
- ✓ Knowledge of the organization system

Additional Education Skills

- ✓ Knowledge of Personal Information Protection Law and official contracts of PCIDSS etc.
- ✓ Ability to interpret intelligence and latest technologies
- ✓ Ability to combine security requirements with products and operations

Prerequisite Skills for Appointment and Additional Educational Skills for Each Role

4.9 “Commander”

Overall CSIRT control

Exercise overall control over security incidents occurring in the organization. Share information with CISO and management regarding serious incidents. Also, provide assistance to CISO and business managers while making a decision.

Prerequisite Skills for Appointment

- ✓ Ability to perform overall control of system failure
- ✓ Knowledge of business and security architecture of the organization
- ✓ Knowledge of business impact during system shutdown and restoration of the organization
- ✓ Communication skills to explain to the management

Additional Education Skills

- ✓ Ability to prioritize in consideration of risk impact and business continuity
- ✓ Knowledge of attack tactics, stages, techniques, and procedures
- ✓ Ability to control security-specific incidents

Prerequisite Skills for Appointment and Additional Educational Skills for Each Role
4.10 “Incident Manager”

In charge of incident management

Instruct the incident handler, and understand the response status of incidents. Understand response history and report the status to commander.

Prerequisite Skills for Appointment

- ✓ Knowledge of system operation
- ✓ Ability to manage and report incidents
- ✓ Knowledge of security architecture of the organization
- ✓ Knowledge of business system of the organization

Additional Education Skills

- ✓ Ability to respond to security incidents
- ✓ Knowledge of recovery after security incidents
- ✓ Knowledge of emerging security issues, risks, and vulnerabilities
- ✓ Knowledge of vulnerability diagnosis
- ✓ Knowledge of handling various attacks such as malware, etc.

Prerequisite Skills for Appointment and Additional Educational Skills for Each Role

4.11 "Incident Handler"

In charge of incident handling

Handle incidents. If security vendors are entrusted with the process of handling, issue instructions to them and manage. Report the situation to the incident manager.

Prerequisite Skills for Appointment

- ✓ Knowledge of system operation
- ✓ Ability to manage and report incidents
- ✓ Knowledge of security architecture of the organization
- ✓ Experience in operating the business system of the organization

Additional Education Skills

- ✓ Ability to respond to security incidents
- ✓ Ability to perform recovery after security incidents
- ✓ Knowledge of emerging security issues, risks, and vulnerabilities
- ✓ Ability to respond to the results of vulnerability diagnosis
- ✓ Ability to handle various attacks such as malware, etc.

Prerequisite Skills for Appointment and Additional Educational Skills for Each Role

4.12 "Investigator"

In charge of survey and investigation

Investigate internal and external crimes. Unlike system failures, security incidents relate to malicious individuals. As in the case of normal criminal investigations, it is necessary to logically narrow down the scope of investigation while confirming the motive, securing evidence, and attempting to guess the next course of events.

Prerequisite Skills for Appointment

- ✓ Ability to gather information and leverage intelligence
- ✓ Ability to analyze relations between nations, and hacktivists
- ✓ Knowledge of confiscation/preservation of evidence
- ✓ Basic IT literacy of ITSS Level 2 or so
- ✓ Knowledge of the organization system

Additional Education Skills

- ✓ Ability to investigate criminals
- ✓ Knowledge and communication skills related to interrogation
- ✓ Knowledge related to the strategy/techniques/procedures followed by the attacker
- ✓ Legal knowledge of cyber crimes

Prerequisite Skills for Appointment and Additional Educational Skills for Each Role
4.13 “Triage In-Charge”

In charge of deciding priority

Determine the priority for the occurring event. Exercise one's judgment on the priority of recovery in case of damage, the systems that must be stopped in case of spread of damage, and so on.

Prerequisite Skills for Appointment

- ✓ Knowledge of business and security architecture of the organization
- ✓ Knowledge of business impact during system shutdown and restoration of the organization

Additional Education Skills

- ✓ Ability to prioritize in consideration of risk impact and business continuity

Prerequisite Skills for Appointment and Additional Educational Skills for Each Role

4.14 “Forensic In-Charge”

Forensic In-Charge

Conduct systematic identification, thorough examination, analysis, and reporting. It is also necessary to restore the erased data and track footprints along with preservation of the evidence since malicious individuals may try to destroy the evidence.

Prerequisite Skills for Appointment

- ✓ Knowledge of structure and logic for OS, command, system files, and programming language
- ✓ Knowledge of vulnerability diagnosis

Additional Education Skills

- ✓ Knowledge of digital forensics
- ✓ Ability to analyze memory dump
- ✓ Ability to analyze malwares
- ✓ Reverse engineering capability
- ✓ Ability to use binary analysis tools
- ✓ Ability to perform correlation analysis of security events

Prerequisite Skills for Appointment and Additional Educational Skills for Each Role
4.15 "Trainer"

In charge of education and awareness

Primarily educate executives and employees to improve literacy. Special training for CSIRT may be assigned separately.

Prerequisite Skills for Appointment

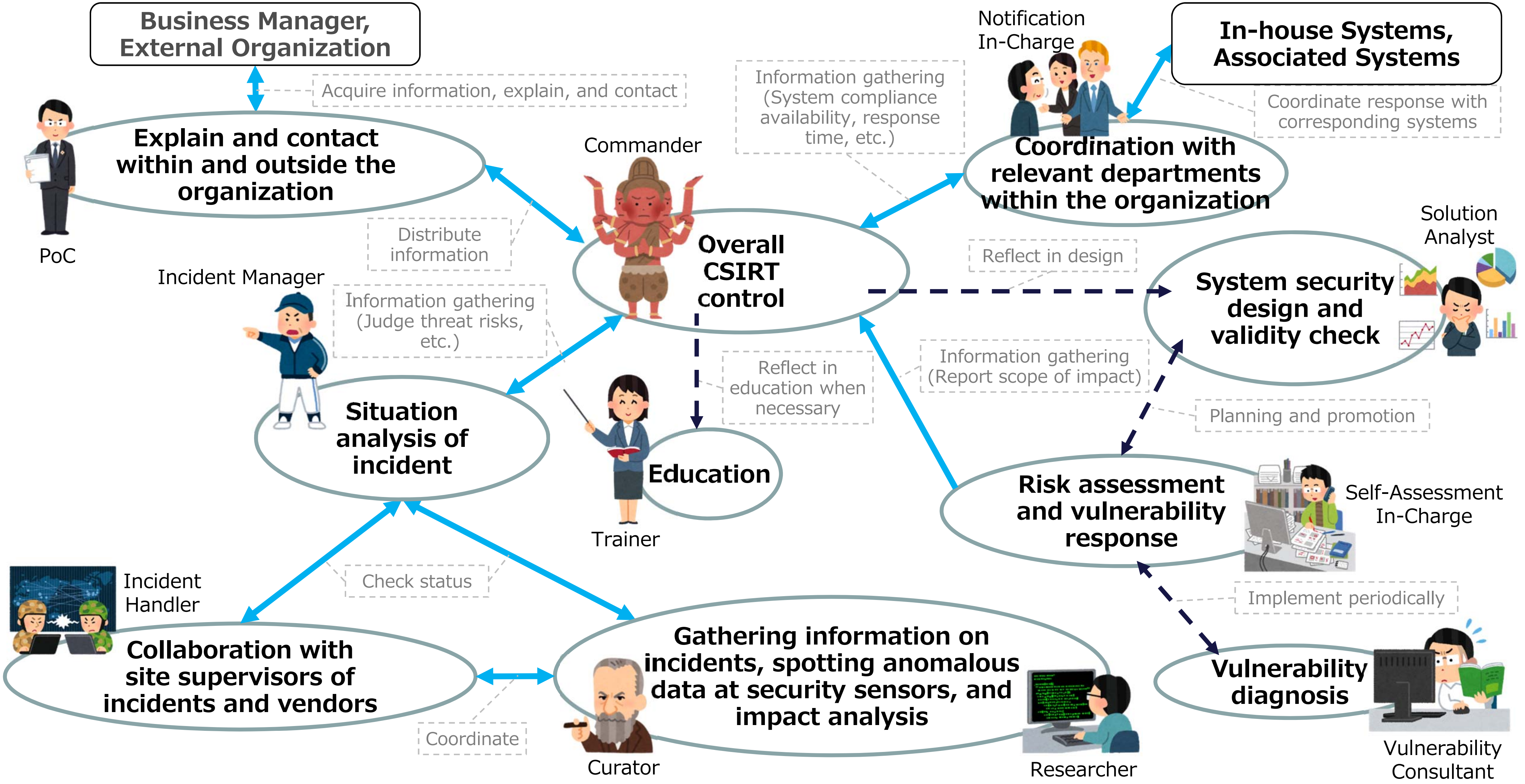
- ✓ Ability to convey information correctly
- ✓ IT literacy of ITSS Level 3 or so
- ✓ Ability to clearly convey information

Additional Education Skills

- ✓ Knowledge of guidelines related to security policies and system architecture of the organization, and compliance matters
- ✓ Ability to gather information, and generate/report intelligence
- ✓ Knowledge of known vulnerabilities

4.16 Relationship between the Roles and Their Tasks (in normal times)

Solid line shows the flow of information during active times.
Dotted line shows the flow of activities to be carried out when necessary.



Business Manager, External Organization

Acquire information, explain, and contact

Explain and contact within and outside the organization

PoC

Commander

Distribute information

Overall CSIRT control

Information gathering (System compliance availability, response time, etc.)

Notification In-Charge

In-house Systems, Associated Systems

Coordinate response with corresponding systems

Coordination with relevant departments within the organization

Reflect in design

Solution Analyst

System security design and validity check

Incident Manager

Information gathering (Judge threat risks, etc.)

Situation analysis of incident

Reflect in education when necessary

Education

Trainer

Information gathering (Report scope of impact)

Planning and promotion

Risk assessment and vulnerability response

Self-Assessment In-Charge

Implement periodically

Check status

Incident Handler

Collaboration with site supervisors of incidents and vendors

Coordinate

Gathering information on incidents, spotting anomalous data at security sensors, and impact analysis

Curator

Researcher

Vulnerability diagnosis

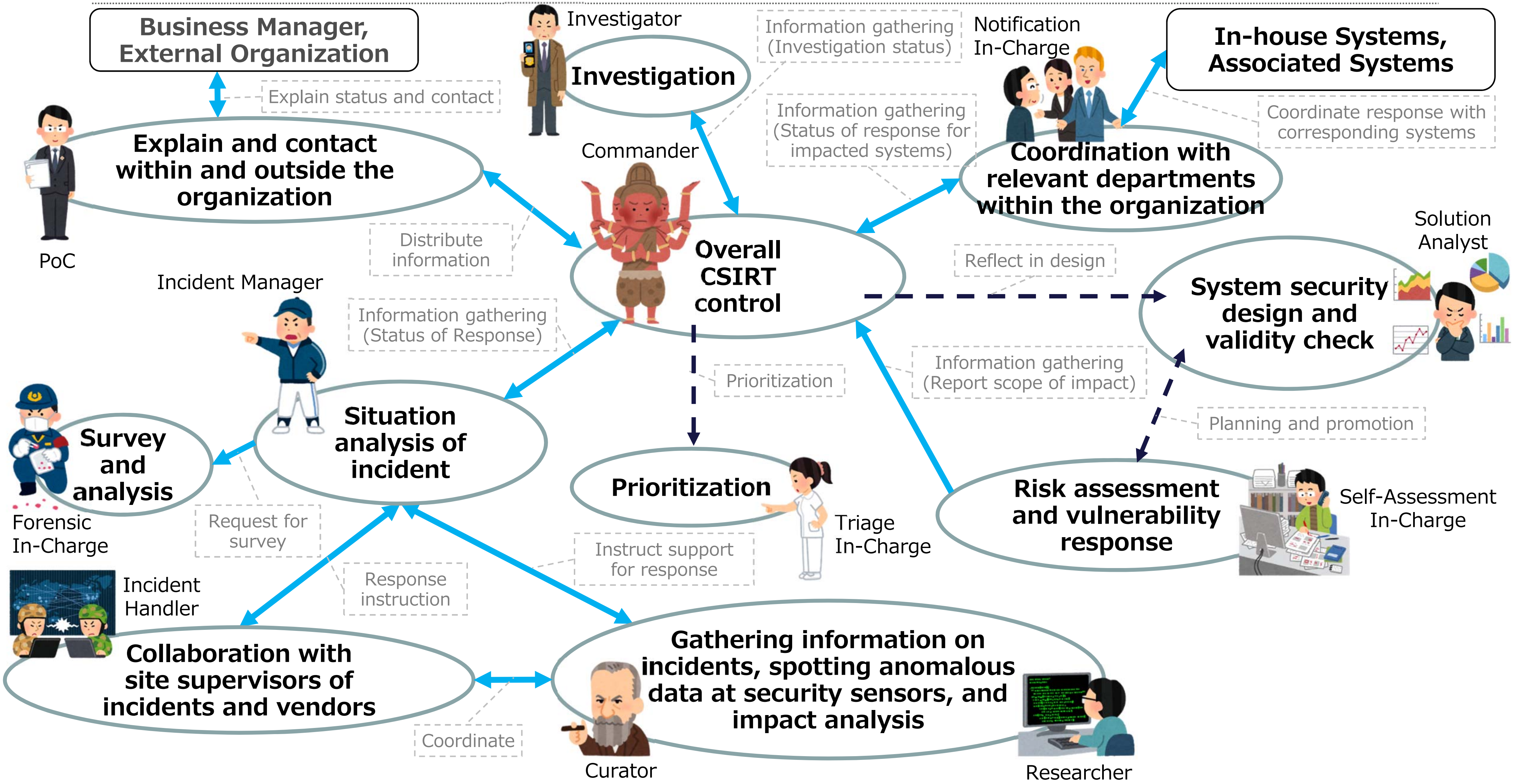
Vulnerability Consultant

*Legal advisors are approached for any assistance required in case of legal confirmation or advice on a daily basis.

*The state in which an incident occurs and CSIRT is providing support is defined as the “in incident response times”

4.16 Relationship between the Roles and Their Tasks (in incident response times)

Solid line shows the flow of information during active times.
Dotted line shows the flow of activities to be carried out when necessary.


Business Manager, External Organization
Explain status and contact
Investigator
Investigation
Information gathering (Investigation status)
Notification In-Charge
In-house Systems, Associated Systems
Coordinate response with corresponding systems
Information gathering (Status of response for impacted systems)
Explain and contact within and outside the organization
PoC
Commander
Coordination with relevant departments within the organization
Distribute information
Overall CSIRT control
Reflect in design
Solution Analyst
System security design and validity check
Incident Manager
Information gathering (Status of Response)
Information gathering (Report scope of impact)
Prioritization
Planning and promotion
Survey and analysis
Forensic In-Charge
Situation analysis of incident
Prioritization
Triage In-Charge
Risk assessment and vulnerability response
Self-Assessment In-Charge
Request for survey
Instruct support for response
Response instruction
Incident Handler
Collaboration with site supervisors of incidents and vendors
Gathering information on incidents, spotting anomalous data at security sensors, and impact analysis
Coordinate
Curator
Researcher

*Legal advisors are approached for any assistance required in case of legal confirmation or advice on a daily basis.

5. Possible Ways to Carry Out the Roles in Each CSIRT Model

- In this document, CSIRT is classified into following models, and the possible ways to carry out the roles (hereafter, implementation examples) are described for Model A, B and C respectively.

- The implementation examples are for illustrative purposes only.
  So, please do not apply the case examples directly to each enterprise but select them based on the business contents and structure of each enterprise.

Model	Definition
A	CSIRT which is built and operated mainly by general affairs department, etc. in an IT-user enterprise
B	CSIRT which is created and operated mainly by an IT-related subsidiary or a specialized department related to information security in an IT-user enterprise
C	CSIRT which is built and operated in an enterprise related to IT or security vendor
D	Others (academic institutions, government agencies, law enforcement agencies, etc.)

*This document does not cover Model D.

5.1 CSIRT Model A

Model A

CSIRT which is built and operated mainly by general affairs department, etc. in an IT-user enterprise

Information is shared within the organization, but system maintenance is entrusted to the vendor.
Receive vendor reports, take preventive measures proactively, make decisions to prioritize to provide for protection as an enterprise when an incident occurs.
Operate as a minimum vigilante function.
Request expert vendors for assistance only when the vigilante group cannot deal with the situation.

Model A

CSIRT Roles: Insource or Outsource?

- All the roles below will be implemented, but the portions highlighted in yellow will be outsourced. CSIRT requires skills to talk with vendors, skills to convey vendor's words by sharing information within the organization, prioritization skills, and skills to educate within the organization.

Functional Classification	Roles	Typical Tasks
Information Sharing	External PoC: In charge of contact outside the organization	Sharing information with NCA, JPCERT/CC, CSIRT, police, regulatory authorities, etc.
	Internal PoC: In charge of contact within the organization and IT department coordination	Sharing information with legal affairs, foreign relations, IT department, public relations, other business divisions, etc.
	Legal Counsel: CSIRT in-charge of legal division	Translating between compliance, legal content, and systems
	Notification In-Charge: In charge of coordination within the organization/information transmission	Point of contact with relevant departments and information transmission
Information Gathering and Analysis	Researcher: In charge of information gathering; Curator: In charge of information analysis	Regular work, gathering incident information, analysis of various information, and understanding international affairs
	Vulnerability Analyst: In charge of vulnerability diagnosis	Inspection and diagnosis of OS, network, and secure programming
	Vulnerability Analyst: In charge of vulnerability assessment	Assessment of OS, network, and secure programming diagnosis results
	Self-Assessment In-Charge	Risk assessment during normal times, analysis of vulnerability during emergency, and impact study
	Solution Analyst: In charge of security strategy	Creating solution map, Fit&Gap analysis, risk assessment, and validity assessment during emergency
Incident Response	Commander: Overall CSIRT control	Overall CSIRT control, decision making, and sharing information with internal PoC, board member, CISO or management
	Incident Manager: In-charge of incident management	Understanding the response status of incidents, reporting to commander, and understanding history of responses
	Incident Handler: In charge of incident handling	Site supervisors of incidents and collaboration with security vendors
	Investigator: In charge of survey and investigation	Secret surveillance using comprehension of in-house systems, analytical skills, logical thinking required for investigation
	Triage In-Charge: In charge of selecting priority	Determining priorities for events
	Forensic In-Charge	Preservation of evidence, systematic identification, footprint tracking, and malware analysis
Education within the Organization	Trainer: In charge of education and awareness	Improving/raising literacy within the organization

Model A

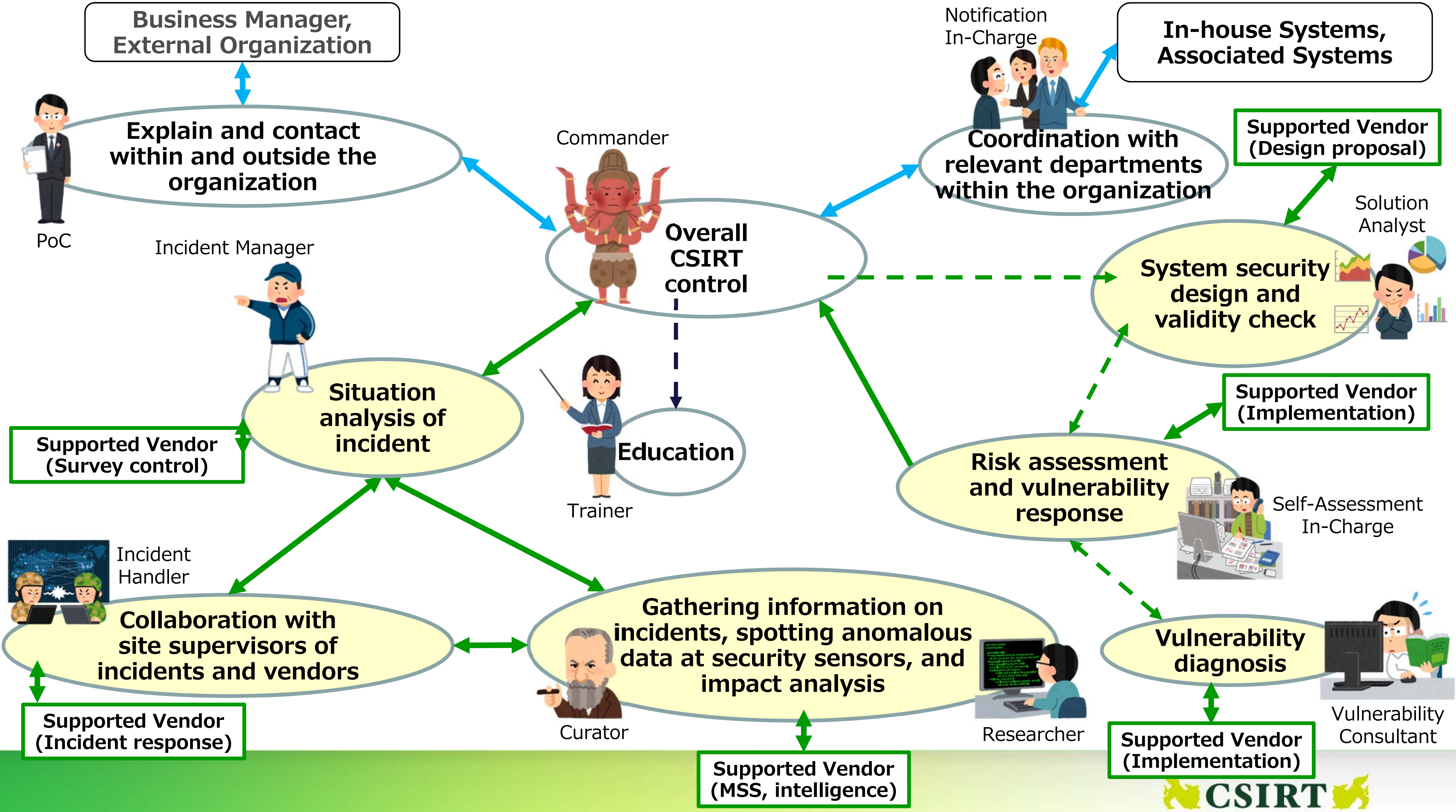
Relationship between the Roles and Their Tasks (in normal times)

[Legend]

🟨 Outsourced roles

○ Insourced roles

*Solid line shows the flow of information during active times. Dotted line shows the flow of activities to be carried out when necessary. Also, blue and black lines mean coordination in the organization, and green lines mean coordination with outsourcers.



Business Manager, External Organization

Explain and contact within and outside the organization

PoC

Incident Manager

Commander

Overall CSIRT control

Notification In-Charge

In-house Systems, Associated Systems

Coordination with relevant departments within the organization

Supported Vendor (Design proposal)

Solution Analyst

System security design and validity check

Supported Vendor (Implementation)

Situation analysis of incident

Supported Vendor (Survey control)

Education

Trainer

Risk assessment and vulnerability response

Self-Assessment In-Charge

Incident Handler

Collaboration with site supervisors of incidents and vendors

Supported Vendor (Incident response)

Gathering information on incidents, spotting anomalous data at security sensors, and impact analysis

Curator

Researcher

Supported Vendor (MSS, intelligence)

Vulnerability diagnosis

Vulnerability Consultant

Supported Vendor (Implementation)

Model A

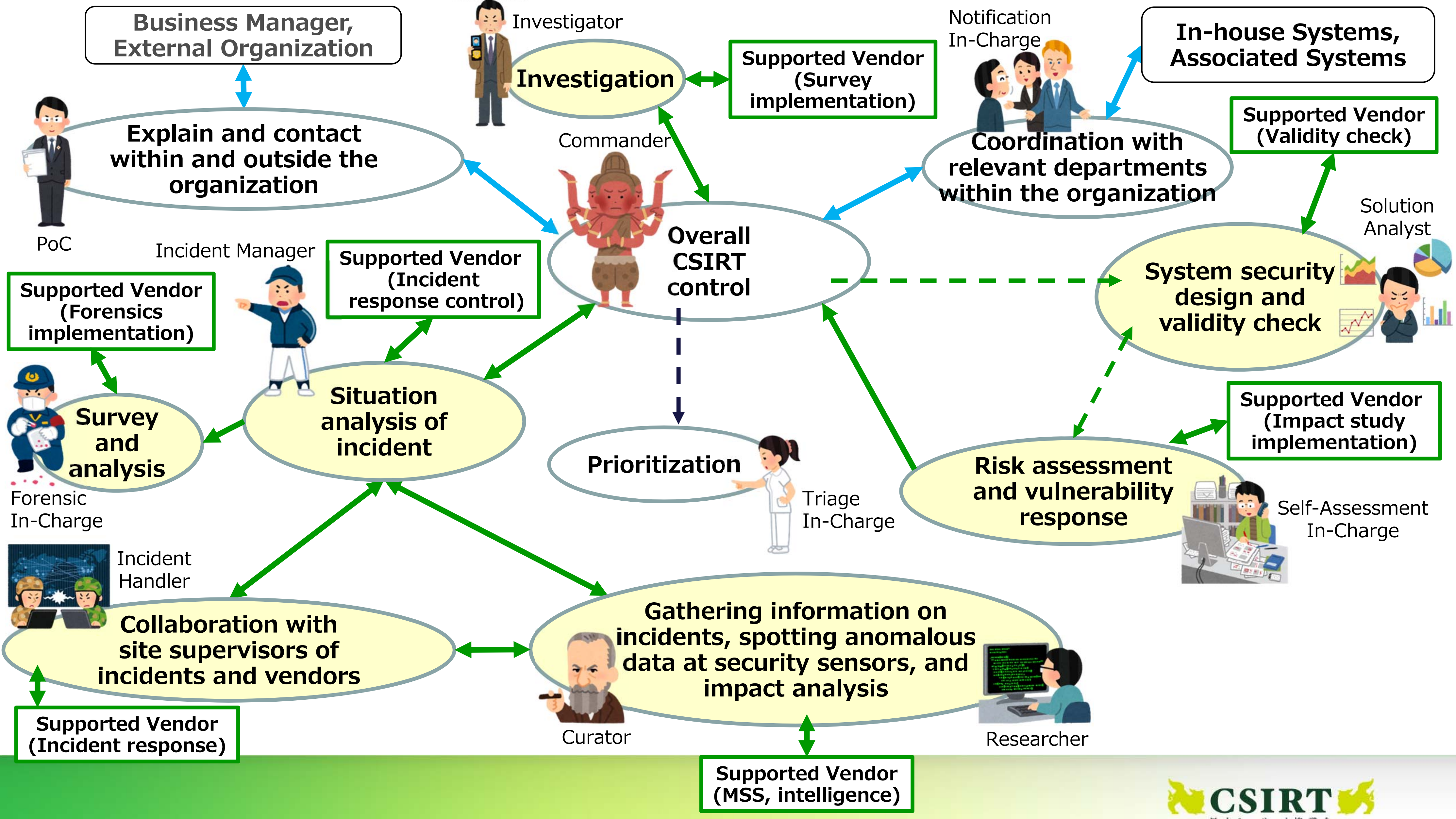
Relationship between the Roles and Their Tasks (in incident response times)

[Legend]

🟨 Outsourced roles

○ Insourced roles

*Solid line shows the flow of information during active times. Dotted line shows the flow of activities to be carried out when necessary. Also, blue and black lines mean coordination in the organization, and green lines mean coordination with outsourcers.



Business Manager, External Organization

Investigator

Investigation

Supported Vendor (Survey implementation)

Notification In-Charge

In-house Systems, Associated Systems

PoC

Explain and contact within and outside the organization

Commander

Overall CSIRT control

Coordination with relevant departments within the organization

Supported Vendor (Validity check)

Solution Analyst

System security design and validity check

Incident Manager

Supported Vendor (Incident response control)

Supported Vendor (Forensics implementation)

Survey and analysis

Forensic In-Charge

Situation analysis of incident

Prioritization

Triage In-Charge

Risk assessment and vulnerability response

Supported Vendor (Impact study implementation)

Self-Assessment In-Charge

Incident Handler

Collaboration with site supervisors of incidents and vendors

Supported Vendor (Incident response)

Gathering information on incidents, spotting anomalous data at security sensors, and impact analysis

Curator

Researcher

Supported Vendor (MSS, intelligence)

Implementation Example for Model A

- As an implementation example for Model A, the following items are illustrated based on actual examples.
  - Outsourcing roles
  - Educational program within the organization

Outsourcing Roles

- Outsource all areas other than those related to judging the business impact of the organization and roles of contact within the organization.

Functional Classification	Roles	Typical Tasks
Information Gathering and Analysis	Researcher: In charge of information gathering; Curator: In charge of information analysis	Monitor the status of security devices, perform routine tasks such as judging incidents etc. However, work in cooperation with maintenance personnel of in-house systems, since decisions are often taken through correlation analysis with the status of in-house systems. Risk for information obtained from vendors and outside the enterprise is determined based on the understanding of international affairs and expert analysis. Survey the background and other things related to events when responding to an incident.
	Vulnerability Analyst: In charge of vulnerability diagnosis	Although it is possible to conduct in-house inspection of applications and infrastructure using tool, penetration levels are outsourced and entrusted to experts.
	Vulnerability Analyst: In charge of vulnerability assessment	Although it is possible to conduct in-house analysis using tools, get opinions from experts regarding the validity of assessment.
	Self-Assessment In-Charge	Conducting risk assessment of information assets owned by the organization will help to investigate the impact on vulnerability response and incident response times.
	Solution Analyst: In charge of security strategy	Establish an overall security plan and evaluate the effectiveness.
Incident Response	Incident Manager: In-charge of incident management	Understand the entire incident. Report to the commander. Understand the response history.
	Incident Handler: In charge of incident handling	Respond to incident.
	Investigator: In charge of survey and investigation	In case of secret surveillance, coordinate with the general affairs department and conduct the survey.
	Forensic In-Charge	Entrust experts with preservation of evidence, systematic identification, footprint tracking, and malware analysis.

Model A

Educational Program within the Organization

- Provide the following educational program within the organization
  - Common educational program for all roles
    - Organization policy, security regulations, management bylaws
    - General rules such as ISMS and PCIDSS
    - Operational guidelines of the organization, business system outline
    - Security devices, equipment details, SOC judgement criteria
    - Essentials of CSIRT actions
    - Exercises as CSIRT in case of normal times and incident response times
  - Educational programs according to roles
    - On-the-Job Training (OJT) for CSIRT in case of normal times and incident response times
    - Exchange of opinions with other CSIRTs

5.2 CSIRT Model B

Model B

Illustration of CSIRT which is created and operated mainly by an IT-related subsidiary or a specialized department related to information security in an IT-user enterprise

This is an example which shows that maintenance and management of systems is done by the organization, but areas other than the core businesses of the organization are outsourced such as a part of SOC and vulnerability diagnosis in case of normal times, forensics in case of incident responses, etc.
The role of CSIRT is to take proactive preventive measures through communication with outsourcing parties. Also, when an incident occurs, respond to the incident by judging the priorities that must be protected as an organization.
Request expert security vendors for support to assist in areas of incident responses that cannot be handled using the organizational structure and skills.

Model B

CSIRT Roles: Insource or Outsource?

- Coordination with relevant departments in the organization, decisions related to business impact, and all roles related to incident responses will be implemented within the organization, but roles that require expertise and those other than the core business of the organization will be outsourced.

Functional Classification	Roles	Typical Tasks
Information Sharing	External PoC: In charge of contact outside the organization	Sharing information with NCA, JPCERT/CC, CSIRT, police, regulatory authorities, etc.
	Internal PoC: In charge of contact within the organization and IT department coordination	Sharing information with legal affairs, foreign relations, IT department, public relations, other business divisions, etc.
	Legal Counsel: CSIRT in-charge of legal division	Translating between compliance, legal content, and systems
	Notification In-Charge: In charge of coordination within the organization/information transmission	Point of contact with relevant departments and information transmission
Information Gathering and Analysis	Researcher: In charge of information gathering Curator: In charge of information analysis	Regular work, gathering incident information, analysis of various information, and understanding international affairs
	Vulnerability Analyst: In charge of vulnerability diagnosis	Inspection and diagnosis of OS, network, and secure programming
	Vulnerability Analyst: In charge of vulnerability assessment	Assessment of OS, network, and secure programming diagnosis results
	Self-Assessment In-Charge	Risk assessment in normal times, analysis of vulnerability during emergency, and impact study
	Solution Analyst: In charge of security strategy	Creating solution map, Fit&Gap analysis, risk assessment, and validity assessment during emergency
Incident Response	Commander: Overall CSIRT control	Overall CSIRT control, decision making, and sharing information with internal PoC, board member, CISO or management
	Incident Manager: In-charge of incident management	Understanding the response status of incidents, reporting to commander, and understanding history of responses
	Incident Handler: In charge of incident handling	Site supervisors of incidents and collaboration with security vendors
	Investigator: In charge of survey and investigation	Secret surveillance using comprehension of in-house systems, analytical skills, logical thinking required for investigation
	Triage In-Charge: In charge of selecting priority	Determining priorities for events
	Forensic In-Charge	Preservation of evidence, systematic identification, footprint tracking, and malware analysis
Education within the Organization	Trainer: In charge of education and awareness	Improving/raising literacy within the organization

Model B

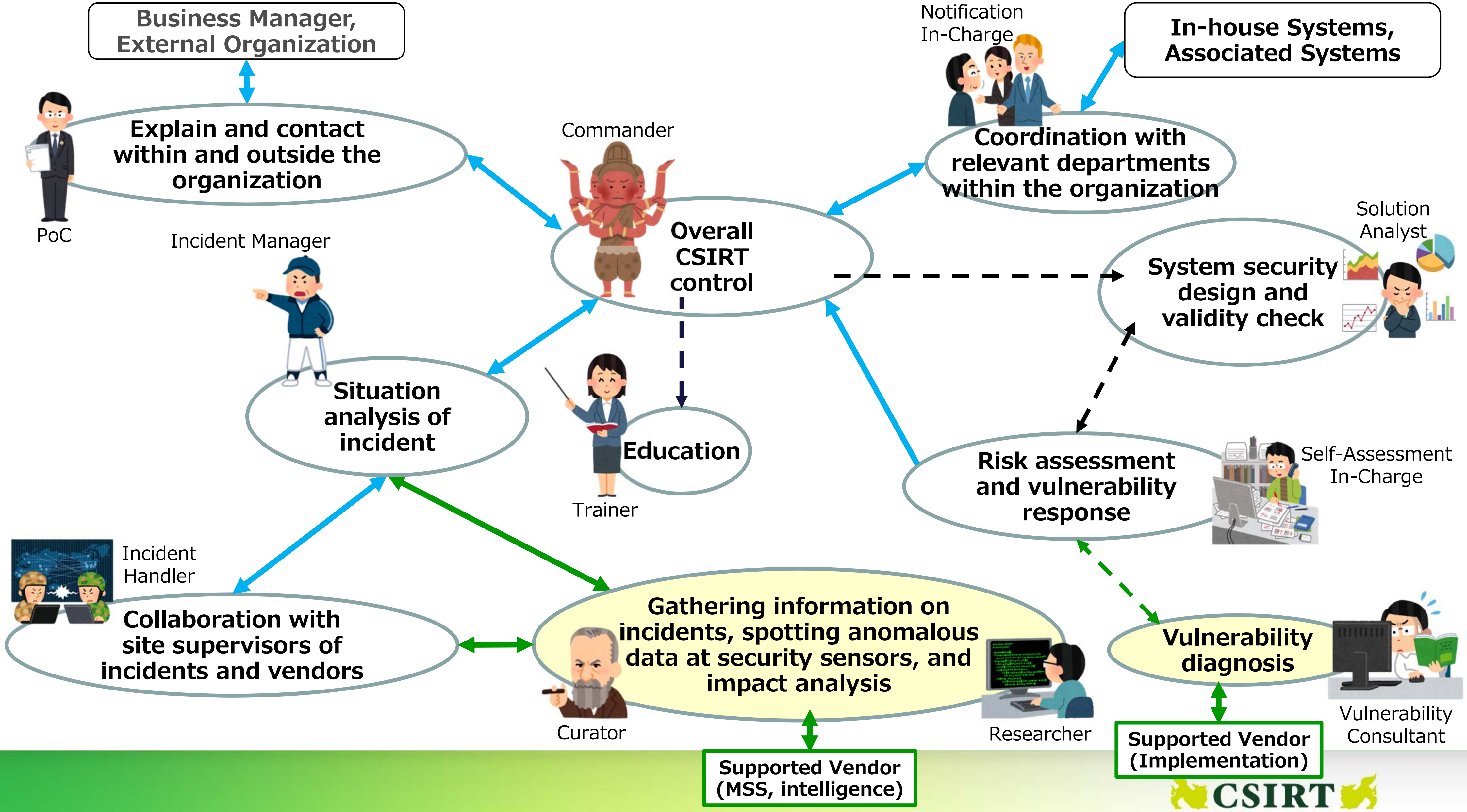
Relationship between the Roles and Their Tasks (in normal times)

[Legend]

🟨 Outsourced roles

○ Insourced roles

*Solid line shows the flow of information during active times. Dotted line shows the flow of activities to be carried out when necessary.
Also, blue and black lines mean coordination in the organization, and green lines mean coordination with outsourcers.



Business Manager, External Organization

Explain and contact within and outside the organization

PoC

Incident Manager

Commander

Overall CSIRT control

Notification In-Charge

In-house Systems, Associated Systems

Coordination with relevant departments within the organization

Solution Analyst

System security design and validity check

Situation analysis of incident

Trainer

Education

Risk assessment and vulnerability response

Self-Assessment In-Charge

Incident Handler

Collaboration with site supervisors of incidents and vendors

Gathering information on incidents, spotting anomalous data at security sensors, and impact analysis

Curator

Researcher

Vulnerability diagnosis

Vulnerability Consultant

Supported Vendor (Implementation)

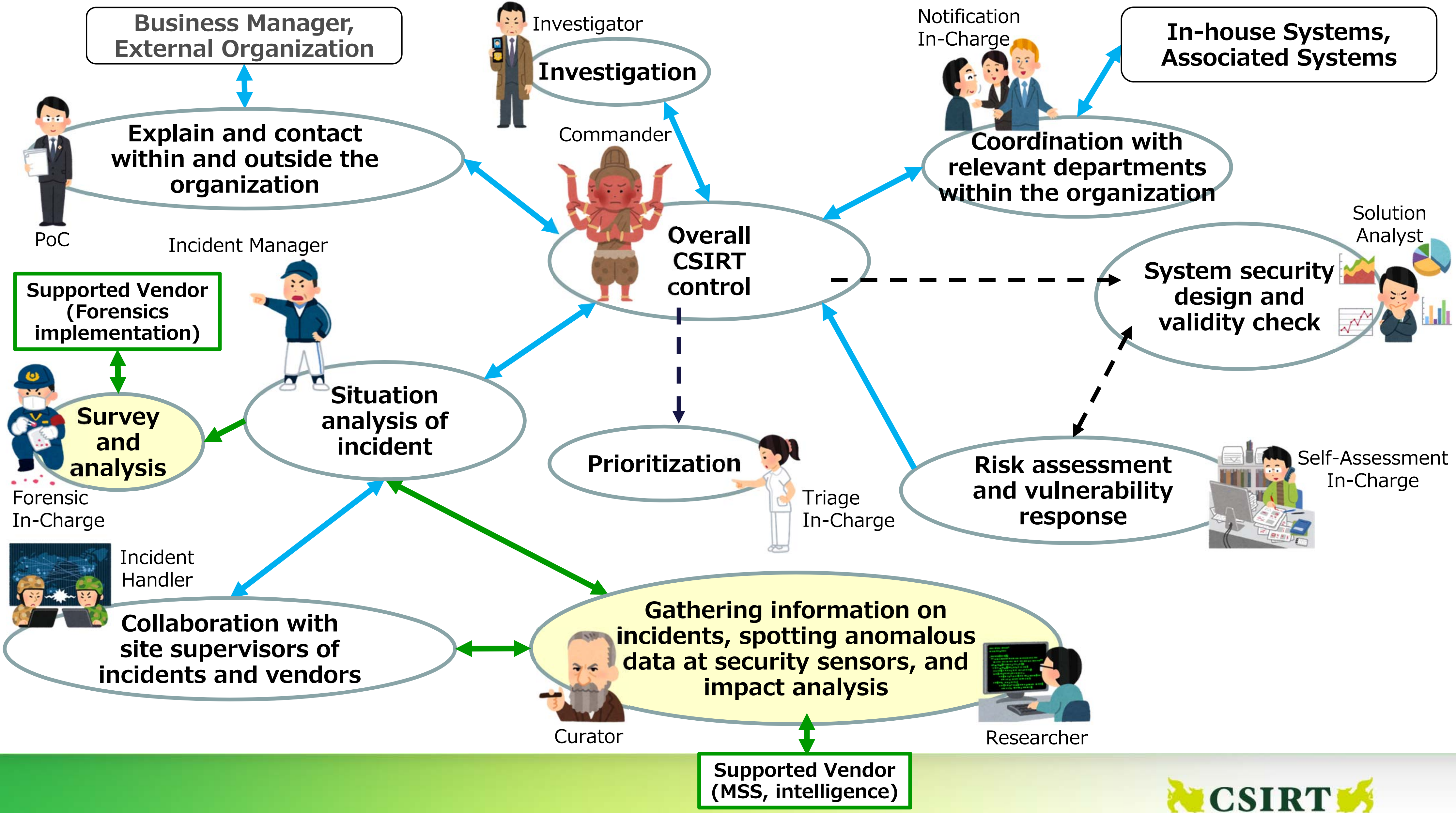
Supported Vendor (MSS, intelligence)

Model B

Relationship between the Roles and Their Tasks (in incident response times)

[Legend]
🟨 Outsourced roles
○ Insourced roles

*Solid line shows the flow of information during active times. Dotted line shows the flow of activities to be carried out when necessary. Also, blue and black lines mean coordination in the organization, and green lines mean coordination with outsourcers.


Business Manager, External Organization
Explain and contact within and outside the organization
PoC
Investigator
Investigation
Commander
Overall CSIRT control
Notification In-Charge
Coordination with relevant departments within the organization
In-house Systems, Associated Systems
Solution Analyst
System security design and validity check
Incident Manager
Supported Vendor (Forensics implementation)
Survey and analysis
Forensic In-Charge
Situation analysis of incident
Prioritization
Triage In-Charge
Risk assessment and vulnerability response
Self-Assessment In-Charge
Incident Handler
Collaboration with site supervisors of incidents and vendors
Gathering information on incidents, spotting anomalous data at security sensors, and impact analysis
Curator
Researcher
Supported Vendor (MSS, intelligence)

Implementation Example for Model B

- As an implementation example for Model B, the following items are illustrated based on actual examples.
  - Outsourcing roles
  - Educational program within the organization

Outsourcing Roles

- Outsource the roles that require skills with high level of expertise for areas and those other than the core business of the organization.

Functional Classification	Roles	Typical Tasks
Information Gathering and Analysis	Researcher: In charge of information gathering; Curator: In charge of information analysis	Monitor the status of security devices, perform routine tasks such as judging incidents etc. However, work in cooperation with maintenance personnel of in-house systems, since decisions are often taken through correlation analysis with the status of in-house systems. Risk for information obtained from vendors and outside the enterprise is determined based on the understanding of international affairs and expert analysis. Survey the background and other things related to events when responding to an incident.
	Vulnerability Analyst: In charge of vulnerability diagnosis	Although it is possible to conduct in-house inspection of applications and infrastructure using tool, penetration levels are outsourced and entrusted to experts.
	Vulnerability Analyst: In charge of vulnerability assessment	Although it is possible to conduct in-house analysis using tools, get opinions from experts regarding the validity of assessment.
Incident Response	Forensic In-Charge	Entrust experts with preservation of evidence, systematic identification, footprint tracking, and malware analysis.

Educational Program within the Organization

- Provide the following educational program within the organization
  - Common educational program for all roles
    - Organization policy, security regulations, management bylaws
    - General rules such as ISMS and PCIDSS
    - System architecture guidelines of the organization
    - Operational guidelines of the organization, business system outline
    - Security devices, equipment details, SOC judgement criteria
    - Risk assessment, audit methods
    - Essentials of CSIRT actions
    - Exercises as CSIRT in case of normal times and incident response times
  - Educational programs according to roles
    - On-the-Job Training (OJT) for CSIRT in case of normal times and incident response times
    - Exchange of opinions with other CSIRTs

5.3 CSIRT Model C

Model C

Illustration of CSIRT which is built and operated in an enterprise related to IT or security vendor

Provide CSIRT services for its organization and for other enterprises.
Owning almost all the CSIRT functions within the organization and publicly conduct research, development, discovery of unknown threats, and information transmission.

CSIRT Roles: Insource or Outsource?

- All roles insourced by the organization.

Functional Classification	Roles	Typical Tasks
Information Sharing	External PoC: In charge of contact outside the organization	Sharing information with NCA, JPCERT/CC, CSIRT, police, regulatory authorities, etc.
	Internal PoC: In charge of contact within the organization and IT department coordination	Sharing information with legal affairs, foreign relations, IT department, public relations, other business divisions, etc.
	Legal Counsel: CSIRT in-charge of legal division	Translating between compliance, legal content, and systems
	Notification In-Charge: In charge of coordination within the organization/information transmission	Point of contact with relevant departments and information transmission
Information Gathering and Analysis	Researcher: In charge of information gathering, Curator: In charge of information analysis	Regular work. Gathering incident information, analysis of various information, and understanding international affairs
	Vulnerability Analyst: In charge of vulnerability diagnosis	Inspection and diagnosis of OS, network, and secure programming
	Vulnerability Analyst: In charge of vulnerability assessment	Assessment of OS, network, and secure programming diagnosis results
	Self-Assessment In-Charge	Risk assessment during normal times, analysis of vulnerability during emergency, and impact study
	Solution Analyst: In charge of security strategy	Creating solution map, Fit&Gap analysis, risk assessment, and validity assessment during emergency
Incident Response	Commander: Overall CSIRT control	Overall CSIRT control, decision making, and sharing information with internal PoC, board member, CISO or management
	Incident Manager: In-charge of incident management	Understanding the response status of incidents, Reporting to commander, Understanding history of responses
	Incident Handler: In charge of incident handling	Site supervisors of incidents and collaboration with security vendors
	Investigator: In charge of survey and investigation	Secret surveillance using comprehension of in-house systems, analytical skills, logical thinking required for investigation
	Triage In-Charge: In charge of selecting priority	Determining priorities for events
	Forensic In-Charge	Preservation of evidence, systematic identification, footprint tracking, and malware analysis
Education within the Organization	Trainer: In charge of education and awareness	Improving/raising literacy within the organization

Model C

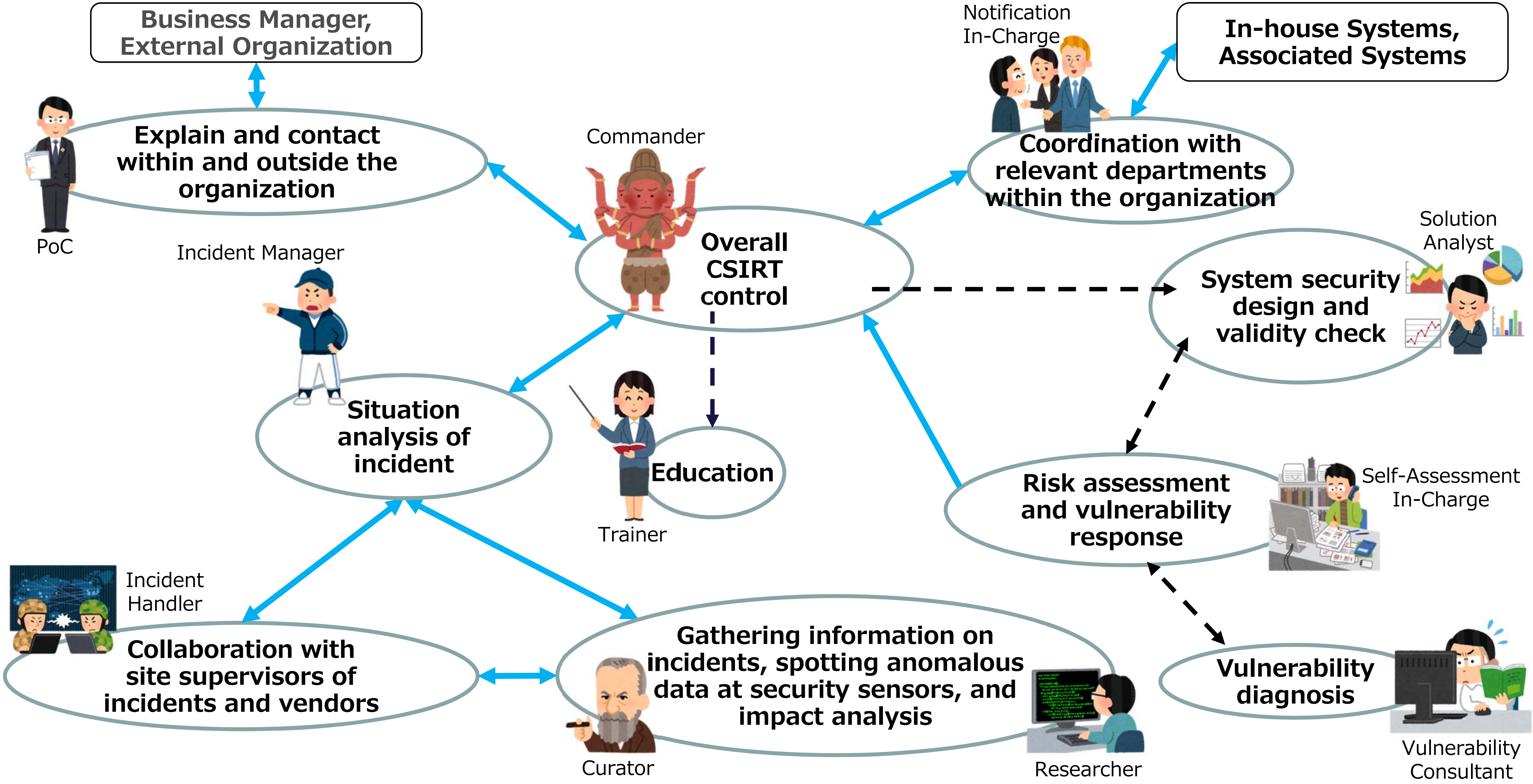
Relationship between the Roles and Their Tasks (in normal times)

[Legend]

🟨 Outsourced roles

○ Insourced roles

*Solid line shows the flow of information during active times. Dotted line shows the flow of activities to be carried out when necessary. Blue lines and black lines indicates coordination within the organization.



Business Manager, External Organization

Explain and contact within and outside the organization

PoC

Commander

Overall CSIRT control

Notification In-Charge

Coordination with relevant departments within the organization

In-house Systems, Associated Systems

Incident Manager

Situation analysis of incident

Trainer

Education

Solution Analyst

System security design and validity check

Risk assessment and vulnerability response

Self-Assessment In-Charge

Incident Handler

Collaboration with site supervisors of incidents and vendors

Gathering information on incidents, spotting anomalous data at security sensors, and impact analysis

Curator

Researcher

Vulnerability diagnosis

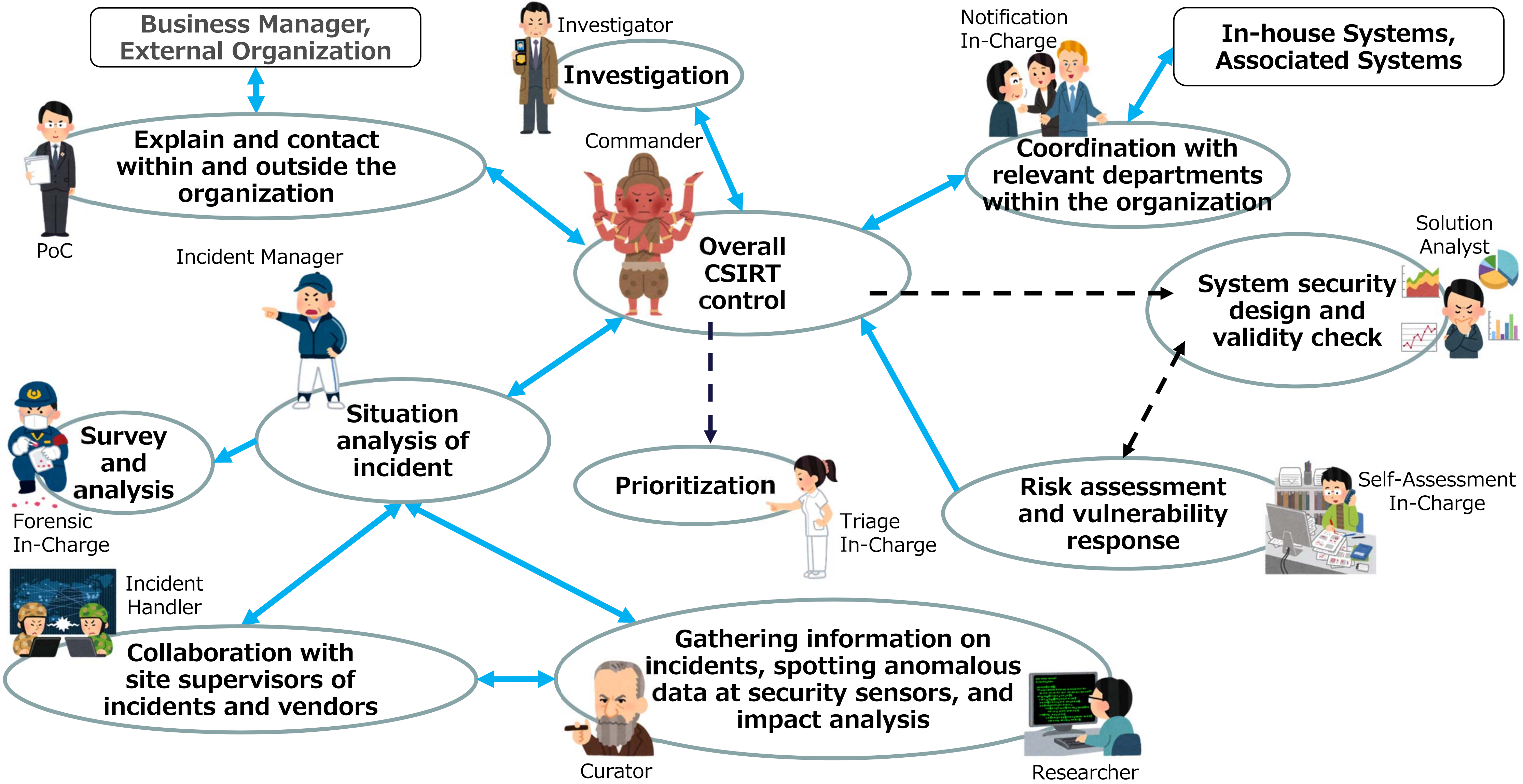
Vulnerability Consultant

Model C

Relationship between the Roles and Their Tasks (in incident response times)

[Legend]
🟨 Outsourced roles
○ Insourced roles

*Solid line shows the flow of information during active times. Dotted line shows the flow of activities to be carried out when necessary. Blue lines and black lines indicates coordination within the organization.



Business Manager, External Organization
Investigator
Investigation
Notification In-Charge
In-house Systems, Associated Systems
Explain and contact within and outside the organization
PoC
Commander
Coordination with relevant departments within the organization
Overall CSIRT control
Incident Manager
Solution Analyst
System security design and validity check
Survey and analysis
Forensic In-Charge
Situation analysis of incident
Prioritization
Triage In-Charge
Risk assessment and vulnerability response
Self-Assessment In-Charge
Incident Handler
Collaboration with site supervisors of incidents and vendors
Gathering information on incidents, spotting anomalous data at security sensors, and impact analysis
Curator
Researcher

Implementation Example for Model C

- As an implementation example for Model C, the following items are illustrated based on actual examples.
  - Outsourcing roles
  - Educational program within the organization

Outsourcing Roles

- All the roles are owned by the organization and are not basically outsourced since technological capabilities and expertise gained from insourcing are the source of competitiveness.
  - There are times when work is outsourced to vendors on a secondary basis

Educational Program within the Organization

- Provide the following educational program within the organization
  - Common educational program for all roles
    - Unique correspondence education program on information security
    - Correspondence education program of other companies
  - Educational programs according to roles
    - Original teaching materials for forensics in-charge
    - Original teaching materials for vulnerability analysts
    - Original teaching materials for researcher/curator
    - Original teaching materials for incident manager /incident handler

6. Conclusion

- The latest version (ver.1.5) contains expansive information such as skills required for CSIRT personnel, further growth after recruitment, descriptions based on training, outsourcing/role collaborations, etc. We hope that this document helps to solve or alleviate the issues related to CSIRT in each organization.
- If you have any questions, please contact the Nippon CSIRT Association.

[Nippon CSIRT Association (Secretariat)]

- Address:

  8F Tozan Bldg., 4-4-2 Nihonbashi-Honcho, Chuo-ku, Tokyo, 103-0023 JAPAN
- Mail:

  nec-sec@nca.gr.jp

Appendix 1. Comparison of Outsourcing Roles by Model

Functional Classification	Roles	Model A	Model B	Model C
Information Sharing	External PoC: In charge of contact outside the organization			
	Internal PoC: In charge of contact within the organization and IT department coordination			
	Legal Counsel: CSIRT in-charge of legal division			
	Notification In-Charge: In charge of coordination within the organization/information transmission			
Information Gathering and Analysis	Researcher: In charge of information gathering Curator: In charge of information analysis	✓	✓	
	Vulnerability Analyst: In charge of vulnerability diagnosis	✓	✓	
	Vulnerability Analyst: In charge of vulnerability assessment	✓	✓	
	Self-Assessment In-Charge	✓		
	Solution Analyst: In charge of security strategy	✓		
Incident Response	Commander: Overall CSIRT control			
	Incident Manager: In-charge of incident management	✓		
	Incident Handler: In charge of incident handling	✓		
	Investigator: In charge of survey and investigation	✓		
	Triage In-Charge: In charge of selecting priority			
	Forensic In-Charge	✓	✓	
Education within the Organization	Trainer: In charge of education and awareness			

Roles highlighted in yellow correspond to outsourcing.

Appendix 2.
Samples of
Job Description and
Specification

[Sample]
Recruiting CSIRT A In-Charge (Researcher, Curator)

Recruitment Title	[Urgent] CSIRT In-Charge (Researcher, Curator)
Number of Recruits	Few people
Job Description (Role)	Check security logs, spot the differences, and escalate to the respective in-charge. Typical job description (Role): PC operation
Required Experience, Skills, and Certifications	Experience: Server and network constructions and operations Skill: PC, Linux operation (general) Certification: Not specified Human skill: Those who are meticulous at work. Those who are poor in conversation are also acceptable.
Desired Experience, Skills, and Certifications	Experience: Experience in analysis of logs such as server log, firewall log, etc. Skill: Endurance, concentration Certification: Nothing in particular
Training	Training will be provided on how to analyze the log based on manual procedures.
Holidays/Vacation	5-day work week. Short working hours. Consultation required for work on shift basis.
Remarks	Growing industry! This is a remarkable job that connects to risk aversion in enterprises!

[Sample]
Recruiting CSIRT A In-Charge (Solution Analyst)

Recruitment Title	[Urgent] CSIRT In-Charge (Solution Analyst)
Number of Recruits	Few people
Job Description (Role)	Maintain and manage overall design and policies of security related devices. Check whether guidelines related to development projects are adhered to or not.
Required Experience, Skills, and Certifications	Experience: Server and network constructions and operations Skill: PC, Linux knowledge (general) Certification: Not specified Human skill: Endurance and ability to talk to developers
Desired Experience, Skills, and Certifications	Experience: Experience in analysis of logs such as server log, firewall log, etc. Skill: Ability to see through the true nature and application skills Certification: Certificate on Information processing
Training	Training will be provided on the background and contents of current policies and guidelines.
Holidays/Vacation	5-day work week. Short working hours. Work on shift basis. Consultation required to work from home.
Remarks	Growing industry! This is a state-of-the-art job which utilizes the evolving IT.

[Sample]
Recruiting CSIRT A In-Charge (Self Assessment/Trainer)

Recruitment Title	[Urgent] CSIRT In-Charge (Self Assessment/Trainer)
Number of Recruits	Few people
Job Description (Role)	Assess risks in the workplace using the experience gained at each workplace and prepare documents. Impart training based on guidelines.
Required Experience, Skills, and Certifications	Experience: Experience in coordination of requirements and specifications Skill: Good listening skills, analytical skills, expressiveness, presentation skills Certification: Nothing in particular Human Skill: Communication skills, soft and zeal for learning
Desired Experience, Skills, and Certifications	Experience: Experience in risk assessment and audit, educational experience Skill: Ability to be comfortable with people, reassuring personality Certification: ISMS Auditor, Auditor
Training	Training will be provided in advance for assessment policy, checkpoint, and guidelines. Security training will also be imparted.
Holidays/Vacation	Consultation is required for short working hours and work from home.
Remarks	Security education system is available.

Appendix 3. Introduction of Various Standards

- **ISMS: Information Security Management System**
  - Information Security Management System
    - Reference URL: https://isms.jp/english/isms.html
- **ITSS: Information Technology Skill Standard**
  - IT Skill Standard (Japanese only)
    - Reference URL: http://www.ipa.go.jp/jinzai/itss/
- **PCIDSS: Payment Card Industry Security Standards Council**
  - PCI Data Security Standard
    - Reference URL: https://www.pcisecuritystandards.org/

Appendix 4. Abbreviations/Acronyms

Abbreviation	Details
CISO	Chief Information Security Officer
CSIRT	Computer Security Incident Response Team
FIRST	Forum of Incident Response and Security Teams
MSS	Managed Security Service
NCA	Nippon CSIRT Association
NISC	National center of Incident readiness and Strategy for Cybersecurity
OJT	On-the-Job Training
PoC	Point of Contact
RFP	Request for Proposal
SOC	Security Operation Center

CSIRT Human Resources Sub-Working Group – List of Authors

as of March, 2017

Kyoichi Abe	ASY-CSIRT	ANA Systems Co., Ltd.
Mitsuru Haba	Canon-CSIRT	Canon Inc.
Koji Kawaguchi	Canon MJ-CSIRT	Canon Marketing Japan Inc.
Ayumi Fujitani	Canon MJ-CSIRT	Canon Marketing Japan Inc.
Akitsugu Ito	Cy-SIRT	Cybozu, Inc.
Fumie Watanabe	DeNA CERT	DeNA Co., Ltd.
Taikei Hashimura	DIR-CSIRT	Daiwa Institute of Research Holdings Ltd.
Ichiro Aoki	DMM.CSIRT	DMM.com Group
Ippei Teranishi	DMM.CSIRT	DMM.com Group
Toshiharu Yoshikawa	DOCOMO-CSIRT	NTT DOCOMO, INC.
Kousetsu Kayama	FJC-CERT	FUJITSU LIMITED
Masato Terada	HIRT	Hitachi, Ltd.
Akiko Numata	HIRT	Hitachi, Ltd.
Toshifumi Tokuda	IBM-CSIRT	IBM Japan Ltd
Kaori Yoshida	iD-SIRT	INFORMATION DEVELOPMENT CO., LTD.
Matsukata Iwao	JBS-CIRT	Japan Business Systems, Inc.
Yusuke Ide	JFE-SIRT	JFE Holdings, Inc.
Akiko Takasugi	JPBank CSIRT	Japan Post Bank Co., Ltd.
Akihiro Morishita	JPBank CSIRT	Japan Post Bank Co., Ltd.
Takuho Mitsunaga	JPCERT/CC	Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)
Yoshinori Sato	MB-SIRT	Mori Building Co., Ltd.
Toshihide Okochi	MBSD-SIRT	Mitsui Bussan Secure Directions, Inc.
Yumiko Torishima	MBSD-SIRT	Mitsui Bussan Secure Directions, Inc.
Takashi Watanabe	mixirt	mixi, Inc.
Yoshiki Sugiura	NTT-CERT	Nippon Telegraph and Telephone Corporation
Naoto Sekido	NTT-CERT	Nippon Telegraph and Telephone Corporation
Manabu Niseki	NTT-CERT	Nippon Telegraph and Telephone Corporation
Kazuhiro Mizoguchi	NTT-CERT	Nippon Telegraph and Telephone Corporation
Chihiro Oyama	NTTDATA-CERT	NTT Data Corporation
Takashi Kikuchi	OCE-CSIRT	Osaki Computer Engineering Co., Ltd.
Kazuhiro Sasagawa	OCE-CSIRT	Osaki Computer Engineering Co., Ltd.
Katsuyuki Matsumoto	SoftBank CSIRT	SoftBank Corp.
Kenta Hagihara	TM-SIRT	Trend Micro Incorporated
Chisato Rokumiya	TM-SIRT	Trend Micro Incorporated
Nozomu Ikeda	TOPPAN-CERT	Toppan Printing Co., Ltd.
Kazuhiro Ouchi	YIRD	Yahoo Japan Corporation
Masato Yamaga	Expert Advisor	

Revision History

- Nov. 16, 2015 Ver.1.0 The first edition created
- Mar. 13, 2017 Ver1.5 Revised