GMS -200-40-02E
December 15,2020

Rules on CSIRT

1 (Purpose)

This rule establishes the Cyber Security Incident Response Team (hereinafter referred to as "CSIRT") system and activities as a core organization that responds to and prepares for damages related to cyber security incidents of the Yokogawa Group, as defined in "Group Information System Management Code" (GMS-200E).

2 (Scope)

CSIRT shall cover security incidents related to IT services provided within the organization controlling the information system management of Yokogawa group and the organization in charge of information system management of the individual company. IT services provided by other organizations within Yokogawa Group will be subject to this requirement as necessary.

3 (Definition)

3.1 Security incidents

Cybersecurity Incidents are defined as incidents that occur illegally through cyberspace, such as service outages, disturbances, system tampering, information leaks or destruction, or human activities or events leading to such incidents. For the purposes of this document, only Cybersecurity Incidents that actually occur as threats to the computer environment within the Yokogawa Group shall be dealt with.

3.2 Security Events

Events that occur due to detection by the monitoring system or contact from users. If the situation is before being treated as a security incident such as unauthorized access, and it is a legitimate access as a result of investigation, it is not treated as a security incident.

3.3 SOC (Security Operation Center)

An organization that performs security log monitoring to detect the occurrence of an incident and supports analysis after the occurrence of an incident.

4 (Roles and Responsibilities)

4.1 CSIRT General Manager

Officer in charge of information systems of Yokogawa Electric Corporation shall appoint one CSIRT General Manager. The roles of CSIRT General Manager include the followings:

(1) To Supervise the CSIRT's overall incident response, confirm progress and implementation results, and report to the officer in charge of information systems.
(2) To establish and maintain IT security policies, regulations, assessments, and improvement plans.
(3) To appoint a vice CSIRT general manager who shall act on behalf of the CSIRT General Manager if CSIRT general manager is unable to perform his or her duties. CSIRT general manager shall establish the secretariat if necessary.

4.2 CSIRT Manager

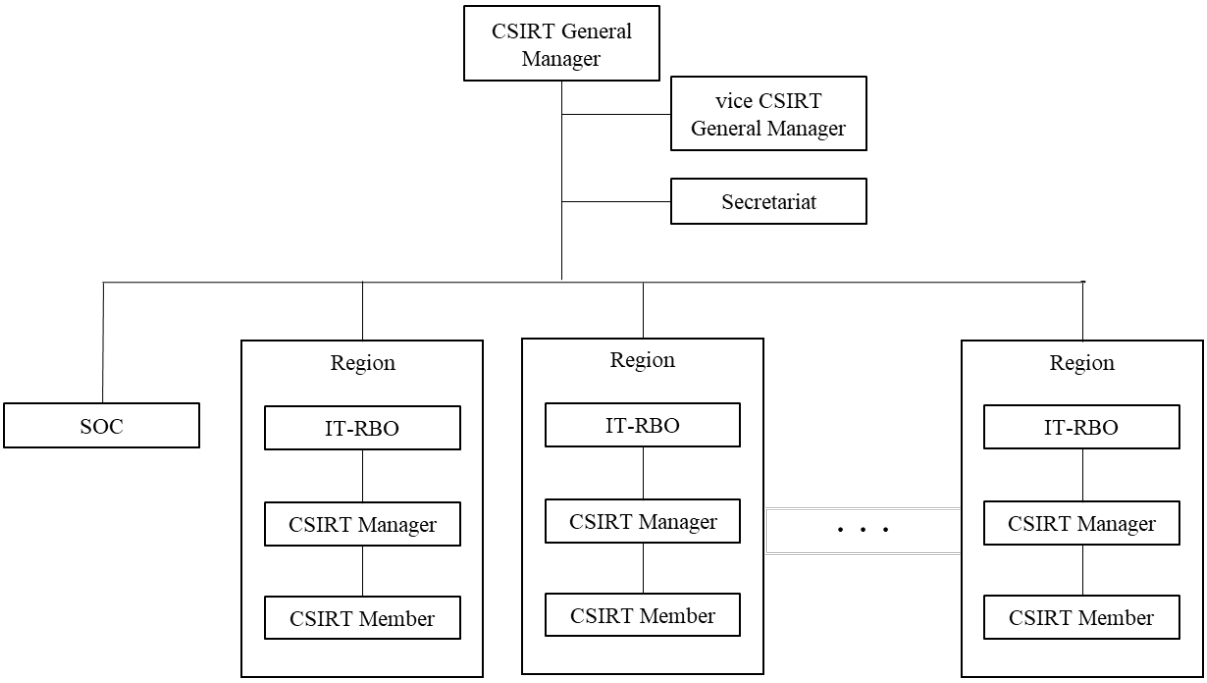
The head of the department in charge of information systems at each region (hereinafter referred to as IT-RBO) shall appoint CSIRT manager. The roles of CSIRT Manager include the followings:

(1) To supervise the incident response within the region in charge, confirm the progress and implementation results, and report to the CSIRT general manager.
(2) To appoint a CSIRT Member within the responsible region.

4.3 CSIRT Member

To respond to incidents within the region in charge. When the processing is entrusted to the security vendor, the instruction is issued, and it cooperates with the management. CSIRT

members report the status to their CSIRT Manager.



<Figure 1: CSIRT Structure>

5 (Function of preparation incident activity

Activities prior to the occurrence of a security incident shall be as follows.

5.1 Survey of security technology trends

Conduct trend surveys of the latest security technologies such as security enhancement technologies, incident detection technologies, and intrusion detection technologies, and confirm the usefulness of their application to organizations.

5.2 Deployment of security tools

Introduce what the organization deems useful. Refer to "GMS-200-40-01E IT Project Management Guidelines" for installation procedures.

5.3 Collecting threat and vulnerability information

Collect threat and vulnerability information to maintain the security level of existing information systems. For methods of information collection, refer to the "vulnerability handling procedures" established at each region.

5.4 Patching

Apply a patch to address the vulnerability.

5.5 Vulnerability diagnosis

An administrator of a Web server that is open to the public on the internet performs vulnerability diagnosis. Refer to the "Internet Publishing Guide" established at each region for the various procedures to be performed by the administrator.

5.6 Information provision

Disseminate information identified as a result of the collection of threat and vulnerability information specified in 5.3 and 5.4 that is judged to be useful to be communicated to all employees, and call attention to security incidents.

5.7 Implementation of cyber countermeasures

Ensure that multiple layers of defense are in place to protect against cyber attacks, including entry, exit, and internal measures. For security measures, refer to "GMS-200-10E Rules on IT Security".

5.8 Risk assessment

Identify, analyze, and evaluate risks to cyber attacks that impede the confidentiality, integrity, and availability of services and information systems as defined by ISO 27001.

5.9 Security assessment

Based on the provisions and plans set forth in 4.1 (2), an evaluation method for understanding the state of technical measures for Cybersecurity shall be considered, and assessment shall be conducted using the evaluation method.

5.10 Security education and education

Create and publish educational content on cybersecurity and information security.

5.11 Cyber Training and Exercises

Conduct hands-on e-mail training and exercises related to cybersecurity and information security.

5.12 Information sharing

To share the status of security incident response with the Information Security Committee and contribute to the improvement of the security level throughout the company.

6 (Functions of post incident activity)

Activities after the occurrence of a security incident shall be as follows.

6.1 Security Event Reception

To receive, respond to, manage the progress and record a detected security event.

6.2 Triage

Determine whether the event received in the previous section is a security incident and check the severity of the incident.

High severity example (Situations in which a critical incident occurs and has a significant impact on operations)

- Service stoppage or interruption (DoS attacks)
- System Tampering (unauthorized access)
- Leakage and destruction of personal and customer information (Backdoor detection and ransomware from malware infections)

If the severity of the problem is judged to be high, the crisis management headquarters will decide how to deal with the problem.

6.3 Containment

When a security incident occurs, measures shall be taken to prevent damage expansion according to the situation.

Organizations should define acceptable risks in handling incidents and develop appropriate strategies.

6.4 Collection of evidence

Keep DATA available for evidence on such computers (System snapshot storage, etc.). Collect evidence at this point to avoid losing evidence during incident response.

6.5 Eradication

Once the incident is contained, the cause of the incident should be eliminated.

This includes removing malicious code and disabling compromised user accounts. In some incidents, eradication may not be necessary or may be performed during recovery operations.

6.6 Restoration

During recovery, administrators return the system to normal operating conditions and strengthen the system to prevent similar incidents. Then, the current state of the security incident is checked, and restoration decisions such as IT service and network restart are made.

6.7 Study and implement measures to prevent recurrence

After the occurrence of a security incident, the cause of the incident should be analyzed, and preventive measures should be considered and implemented.

6.8 Internal cooperation

Handling security incidents (command and coordination) and sharing information with the support and cooperation of the Yokogawa Group.

6.9 External collaboration

Handling security incidents (command and coordination) and sharing information with the support and cooperation of outside organizations such as SOC and security vendors.

6.10 Internal reporting

Grasp the occurrence status of security incidents and report to the organization. Also, if the severity of the security incident is high, it should be reported to the organization immediately.

6.11 External communication

If a security incident occurs that is deemed useful to report, report it to the supervisory authority.

7 (Managing Information)

CSIRT handles information related to the security of the Yokogawa group. In addition, in order to cooperate with an external security organization, information related to incidents of other companies may be handled. For this reason, the handling of this information shall be limited to those concerned, and the CSIRT General Manager shall designate those concerned.

8 (Handling Exceptions)

If the provisions of this document interfere with security or there are deficiencies, CSIRT general manager shall implement measures in consultation with the head of the organization controlling the information system management of Yokogawa group.

In responding to the above, CSIRT general manager shall promptly share measures so as not to interfere with coordination with concerned parties.

9 (Management Department)

This rule should be managed by the organization controlling the information system management of Yokogawa group.

10 (Review of this rule)

This rule shall be reviewed as necessary in light of changes in the social environment, such as the occurrence of threats and incidents, technological trends, etc., by appropriately grasping the state of CSIRT operation, the state of implementation of exceptional measures, etc.

History of Revision (GM-240.02)

July 1, 2020 Established

History of Revision (GMS-200-40-02)

December 15, 2020: Established (newly established according to GMS-200)