Emergency Management

Material issues ▶ Enhancement of our business foundation

Emergency Management Systems

As well as having a permanent emergency response team at J-POWER headquarters, when an emergency is anticipated or has occurred and emergency measures are necessary, we will organize Emergency Response Headquarters and Branches.

The Emergency Response Team anticipates emergencies, immediately takes first-response action in the case of any occurrence, and oversees emergency management operations. In the event of an emergency, the team coordinates with the Emergency Response Headquarters and Branches in each local area to accurately predict and prevent accidents such as disasters and facility incidents, and responds/manages promptly and appropriately should such events occur.

Furthermore, the Emergency Response Headquarters and branches in the J-POWER headquarters and local units annually carry out coordinated comprehensive disaster drills, and periodically conduct safety reporting drills for employees and Group company employees.

Emergency Management Measures

The J-POWER Group has a responsibility as an electric utility company to ensure a stable supply of electricity, which plays an essential role in people's everyday lives. We need to prevent damage to the equipment that produces and transmits electric power and to restore service quickly should a disruption occur. Accordingly, the J-POWER Group implements the following measures.

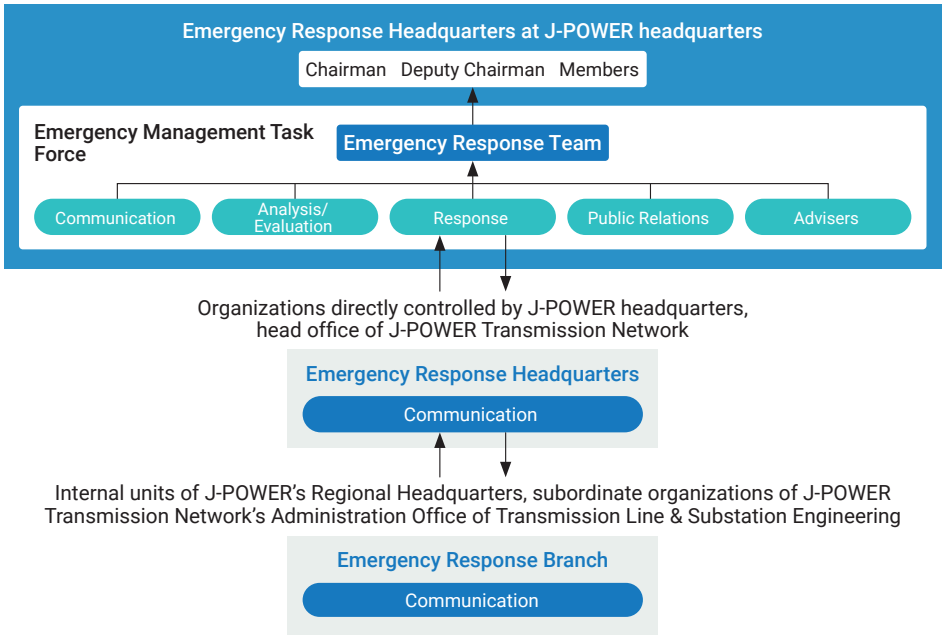
① Installation of appropriate facilities and development of disaster recovery systems in preparation for natural disasters, including earthquakes, typhoons, lightning strikes, and tsunamis
② Enhancement of security to prevent malicious and violent conduct
③ Enhancement of regular facility inspections to prevent major impediments to electric power supply and appropriate repairs and upgrades in response to aging, the decline of function, and breakdowns
④ Preparation of action plans for responding to pandemics and other events that could have a major impact on business operations

Disaster Prevention and Business Continuity

As an electric utility company responsible for vital lifelines, the Company is a designated public institution under the Basic Act on Disaster Control Measures. Accordingly, the Company has established physical measures assuming a large-scale natural disaster as well as non-physical measures, such as various rules for when disasters occur and a systematic disaster preparedness structure from the headquarters to local units. By actively implementing these measures, the Company has reinforced its disaster preparedness structure to ensure the continuation of business even in the event of a natural disaster exceeding assumptions.

By conducting fully remote disaster drills, we have also established a disaster prevention system that does not depend on physical employee attendance.

Emergency Response Headquarters Communication System



Composition of the Emergency Response Headquarters at J-POWER headquarters

Organizations	Composition
Chairman	President
Deputy Chairman	Vice President
Members	The officer in charge of the General Affairs Department, Directors in Charge and related officers Director of the General Affairs Department, Director of Public Relations and related departments
Emergency Management Task Force	Emergency Management Response Team and related departments

(Composition of the Task Force)	(Division of duties)
Communication	Information communication, gathering, and management
Analysis/Evaluation	Analysis, evaluation, and countermeasure planning
Response	Information on recovery response, liaisons, victim response, consumer relations, and investor relations
Public Relations	Media response
Advisers	Advice regarding analysis, evaluation, and countermeasure planning

Emergency Management

Material issues ▶ Enhancement of our business foundation

Cybersecurity

Basic Policies

In recent years, cyber-attacks have not only increased but have also become more sophisticated and elaborate. We apply technical steps based on the most recent information, such as computer virus countermeasures, unlawful access and information leakage countermeasures, as specified by the Basic Act on Cyber security for operators of vital infrastructure. We also comply with the Guidelines for Power Control System Security to ensure the security of power control systems and other systems for the stable supply of electric power.

Furthermore, based on The Cybersecurity Policy for Critical Infrastructure Protection announced by the government's Cybersecurity Strategic Headquarters on June 17, 2022, we have established a system to take all possible measures for cybersecurity as a critical infrastructure provider and are further strengthening our measures.

In March 2023, the J-POWER Group established its the Basic Policies on Cybersecurity and Cybersecurity Regulations, which span both information and control systems and strengthened its response capabilities throughout the supply chain.

Incident Response

In order to respond to cyber-attacks and recover quickly in the event of any breach, we have established the J-POWER CSIRT* as a cybersecurity crisis management system, working to prevent cybersecurity incidents and keep damage to a minimum should any incidents occur.

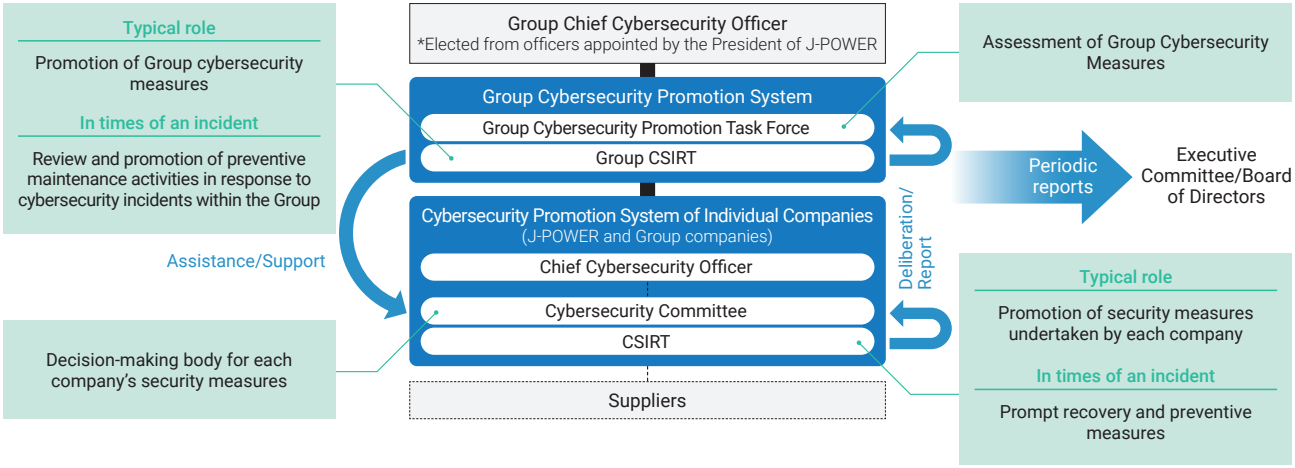
* Cyber Security Incident Response Team (the letter C originally stood for Computer, but we refer to it as Cyber)

Providing Information Security Educations

We have continuously provided all the employees with e-learning on cybersecurity and trainings to prepare for the targeted e-mail attacks.

Results of e-learning for FY2023

We provided e-learning (three times in total) on case study of the targeted e-mail attacks, initial responses, security measures of control system, and prohibition of usage of personal portable storage medium (USB, etc.) (number of trainees was 17,925 in total)



J-POWER Group's Basic Policies on Cybersecurity

We, the officers and employees of the J-POWER Group, have created the following fundamental policy for maintaining cybersecurity as a corporation with essential infrastructure that has the potential to significantly affect people's lives.

❶ Identification as a management issue
From a high-level perspective of the entire supply chain, management should be aware of the dangers associated with cybersecurity, acknowledge them as a critical management concern, and assume responsibility for taking action while exercising leadership.

❷ Compliance with laws, regulations and contractual requirements
We will comply with laws, regulations, codes, and contractual obligations as well as other societal norms related to cybersecurity.

❸ Implementation of appropriate cybersecurity measures
We aim to establish a promotion system and organization to maintain and improve cybersecurity, and take human, technical, and physical measures, as well as identify new threat trends and promptly address them. In addition, we will strive to implement supply chain countermeasures including business partners, contractors and overseas.

❹ Education and training initiatives
We will promote cybersecurity initiatives by acquiring the knowledge and skills necessary for cybersecurity and by participating in education and training.

❺ Response to violations and incidents
In the event of a breach of cybersecurity laws and regulations, breach of contract, or an incident, we will take appropriate action to prevent recurrence.

❻ Continuous improvement activities
Continuous improvement activities will be implemented through periodic evaluation and review of the above efforts.