

Emergency Management

► Material issues



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.

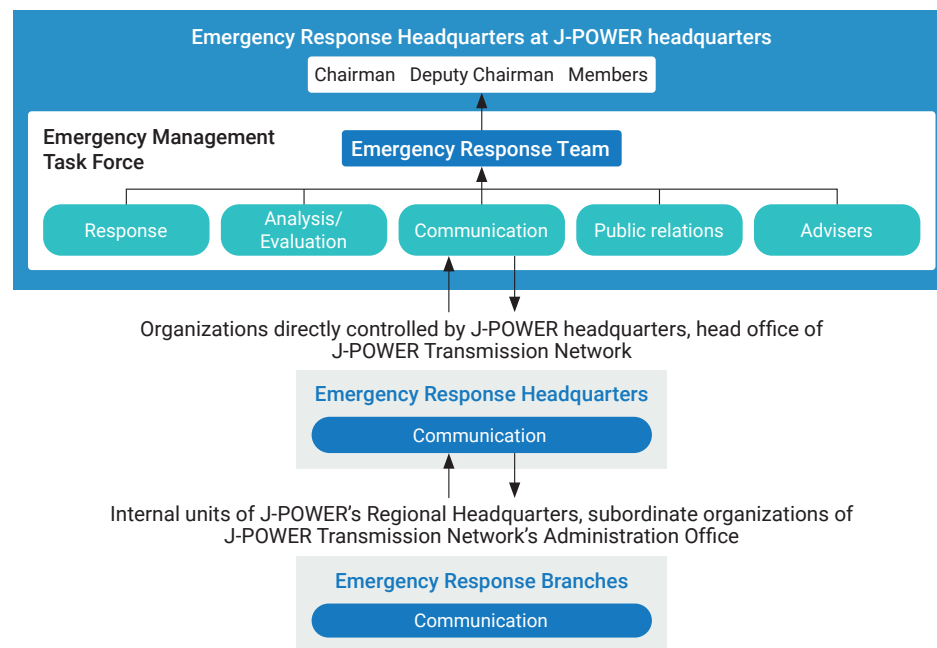
- ① Installation of appropriate facilities and development of disaster recovery systems in preparation for natural disasters, including earthquakes, typhoons, lightning strikes, and tsunamis
- ② Enhancement of security to prevent malicious and violent conduct
- ③ Enhancement of regular facility inspections 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 Management. 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

Role	Composition
Chairman	President
Deputy Chairman	Vice President
Members	Officer in charge of the General Affairs Department, Directors in charge and related officers Directors of General Affairs Department, Public Relations & Community Relations Department and related departments
Emergency Management Task Force	Emergency 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



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 a critical social infrastructure provider specified in the Basic Act on Cybersecurity. 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.

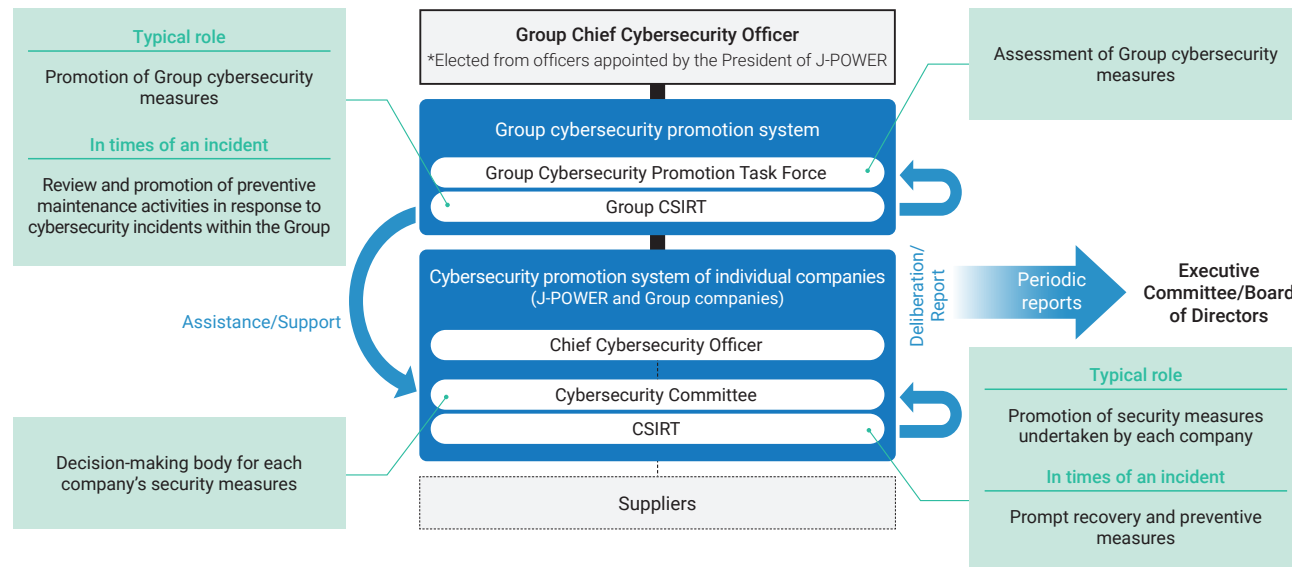
Furthermore, based on the Cybersecurity Policy for Critical Infrastructure Protection announced by the government's Cybersecurity Strategic Headquarters, we have established a system to take all possible measures for cybersecurity as a critical infrastructure provider and are further strengthening our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

To strengthen our response capabilities throughout the entire supply chain, we have established the J-POWER Group's

Basic Policies on Cybersecurity and the Cybersecurity Regulations, which span both information and control systems. Regarding the status of major cybersecurity incidents affecting business operations, we provide periodic reports at the Group Cybersecurity Promotion Task Force, while each Group company reports such matters to its Board of Directors, thereby striving to strengthen intra-Group coordination. (No major information security incidents occurred in FY2025)

Structure

An officer appointed by the President of J-POWER serves as the Group Chief Cybersecurity Officer to manage the Group Cybersecurity Promotion Task Force, which conducts periodic cybersecurity assessments and internal and external audits, while periodically reporting the state of cybersecurity to the Board of Directors.



Continuous monitoring and implementation of drills against cyber-attacks

To prepare for cyber-attacks, the J-POWER Group conducts continuous monitoring and drills, analyzes vulnerabilities, and manages risks.

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. Furthermore, cybersecurity risks are explicitly stated in our internal emergency management and cybersecurity-related regulations, and we have established response flows to ensure prompt reporting and action if an employee discovers the occurrence of a cybersecurity incident or an event suspected to have occurred. In FY2025, we reviewed the basic response measures to ensure business continuity or the early recovery and resumption of operations in the event of a cybersecurity incident.

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

Providing information security educations

Every year, we continuously provide all employees with e-learning on cybersecurity and drills and training to prepare for targeted e-mail attacks.

Results of e-learning for FY2025

Every year, we continuously provide e-learning (three times in total) on how to improve the security of domain password, how to spot and initially respond to targeted attack e-mails, and cautions to take when teleworking (number of trainees was 19,740 in total).

As a corporation with essential infrastructure that has the potential to significantly affect people's lives, the Company has established the fundamental policy for maintaining cybersecurity. For details of the J-POWER Group's Basic Policies on Cybersecurity, please refer to our website.

https://www.jpowers.co.jp/english/privacy/privacy_003_e.html