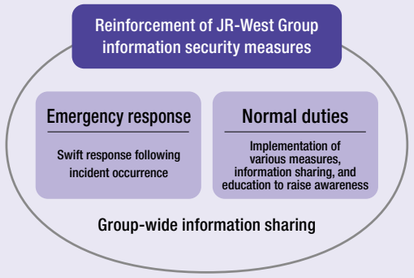
Information security

JR-West Group's approach to information security

In order to protect the JR-West Group's information assets from various threats, we have established and adhere to the JR-West Group Information Security Policy. We declare that we will leverage information-sharing and cooperation among group companies to facilitate the implementation of ongoing, group-wide information security measures.

In recent years, the risks posed, and damage caused, by cyberattacks have increased, as well as become more frequent, and the Japanese government has called for stronger cybersecurity as part of its national policy.

The JR-West Group deals with information security as one of the four pillars of its digital strategy, looking for ways to address the increasing vulnerabilities that accompany the expansion in telework and digital transformation, the increasing sophistication of cyberattacks, and the increasing number of threats.



JR-West Group's security structure

We have established an Information Security Committee chaired by the CISO (chief information security officer), and, under this, we operate the Critical Infrastructure Subcommittee and JR-West Group CSIRT.

In addition, we are working to improve the security level of the entire Group while also pursuing collaboration with external organizations.

Information Security Committee

Beyond reporting on the results of security efforts within the JR-West Group, the committee also sets policy, based on internal and external trends, for efforts aimed at improving the security level of the JR-West Group.

Critical Infrastructure Subcommittee

This subcommittee puts particular emphasis on identifying risks and implementing countermeasures for control systems, including those related to railway operations, as well as important systems that support social infrastructure such as ICOCA.

JR-West Group CSIRT

We have established the JRW-CSIRT*1 (JR-West Group CSIRT), an organization aimed at preventing security incidents and limiting the extent of their impact when they occur. We use it to foster awareness through information sharing and education and to respond quickly when incidents occur.

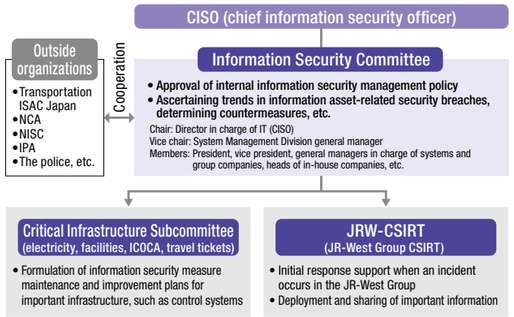
*1 CSIRT: Computer Security Incident Response Team. An organization responsible for handling computer security-related incidents.

Collaboration with external organizations

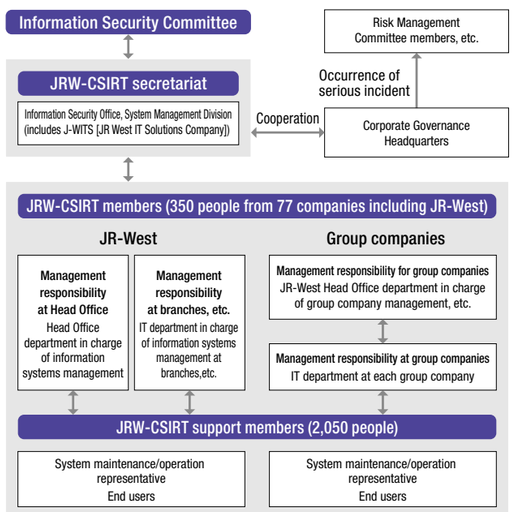
We are a member of the Transportation ISAC Japan*2 and actively and regularly exchange information regarding information security with other companies. We also actively participate in security-related working groups organized by the NCA*3 (Nippon CSIRT Association).

*2 Transportation ISAC Japan: An organization that conducts activities contributing to the improvement of collective defense capabilities in the transportation and transport sector.
*3 NCA: An organization that facilitates information sharing and collaboration among CSIRTs operating in Japan.

■ JR-West Group's security structure



■ JRW-CSIRT structure



Improving employee literacy

In order to improve employee literacy within the JR-West Group, we conduct targeted email attack drills and security-related education for all employees (approximately 44,000), as well as run training tailored to specific people as shown below.

For senior management

We conduct training for senior management (approximately 200), including those from group companies, to help them understand the threat of cyberattacks and how to counter them, as well as the role that management should play in security measures.

For personnel responsible for IT security

We conduct training for JRW-CSIRT members and information systems managers (approximately 2,900) within the JR-West Group in order to help cultivate human resources capable of taking the lead in information security measures. In addition to communicating the necessity of security measures when conditions are normal, we also conduct security incident response drills for JRW-CSIRT members (approximately 350).

For personnel in charge of critical infrastructure

We take part in incident response training organized by the NISC (National Center of Incident Readiness and Strategy for Cybersecurity) for critical infrastructure operators.

For employees seeking to become highly specialized personnel

We send employees for one year to take part in the core human resource development program organized by the IPA (Information Technology Promotion Agency) in order to develop them as security-related personnel. Additionally, we have established a system to support participation in external training and qualification acquisition, with a particular focus on encouraging security-related learning. As a result, approximately 50 people within the Group have passed the Registered Information Security Specialist examination.

■ Digital strategy-related human resource development and training

Highly skilled personnel	Content	Sending employees to IPA; support system for participation in external training; etc.
	Level	• Knowledge at the level of a Registered Information Security Specialist
Local promotion leader	Content	Information security manager training (target: senior management, department heads)
		Information security leader training (target: local CSIRT members, etc.)
		Information security supporter training (target: local CSIRT support members)
		CSIRT operations orientation (target: local CSIRT members)
		Incident response workshop (target: local CSIRT members)
	Level	• Can take the lead in information security measures and implement security measures for the systems under one's purview
All employees	Content	Security training for all employees, targeted email attack drills
	Level	• Can handle personal/confidential information appropriately

Secure system development

Based on the concept of security by design, JR-West and group companies are exploring and approving security measures at the conceptual stage of system development. This applies to systems that handle customers' personal information and systems that have connection points with external networks, where security measures are considered particularly important. We are enacting necessary security measures involving confirmation from both a baseline and risk-based approach.

Establishing the PDCA cycle

We maintain guidelines for specific security standards that must be followed, and we update them in response to technological trends and past incidents. Based on these, we conduct self-inspections of a total 118,646 items for 2,880 systems at JR-West and group companies each year to strengthen security measures on an ongoing basis.