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 of digital transformation, the increasing sophistication of cyberattacks, and the increasing number of threats.

As the JR-West Group pursues new value through digital technology, we are advancing through a dual focus on an 'offensive' digital strategy and 'defensive' information security. It is essential that we have a foundation of appropriate information security throughout the Group as we accelerate the development of a variety of services, including the launch of Wesmo!, and the creation of new businesses.

To ensure that our customers can reliably and confidently use our services, we implemented a range of security measures in the lead-up to Expo 2025. We will continue to build upon this foundation with measures in response to changing risks, while remaining focused on mutual understanding and respect and empathy within the Group and with partners.

Head of operations; technical officer; general manager of System Management Division (CISO), Digital Solutions Headquarters
Yasuhiro Kai (registered information security specialist [registration no. 025068])

Information security governance

JR-West Group's security structure

We have 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*1 (JRW-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.

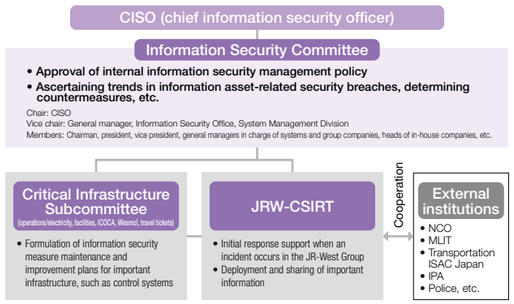
● Collaboration with external organizations

In addition to sharing information with external organizations such as the National Cybersecurity Office (NCO), the Ministry of Land, Infrastructure, Transport and Tourism (MLIT), police agencies, and the Information-technology Promotion Agency (IPA), we are strengthening security through membership in Transportation ISAC Japan*2 and actively participating in working groups hosted by the Nippon CSIRT Association (NCA)*3.

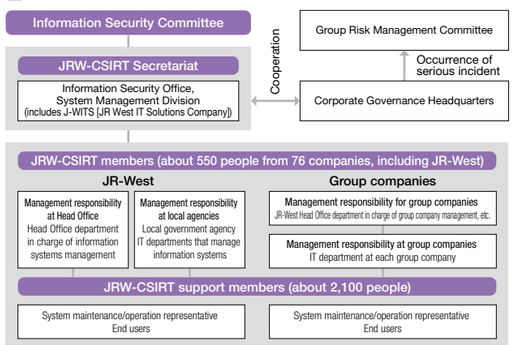
Operation of JRW-CSIRT

The JRW-CSIRT is 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. We are also strengthening our framework by assigning JRW-CSIRT members (about 550 people from 76 companies) to serve as contact points for each department and each company and JRW-CSIRT support members (about 2,100 people) to each workplace.

■ JR-West Group's security structure



■ JRW-CSIRT structure



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

Operation of the Critical Infrastructure Subcommittee

With regard to control systems, including those related to railway operations, and important systems that support infrastructure (critical infrastructure), such as ICOCA and Wesmo!, the Critical Infrastructure Subcommittee of the Information Security Committee is pursuing various initiatives led by the heads of the departments responsible for each system. In addition, we are cooperating with outside organizations (such as the NCO) to share information and conduct training on cyberattacks and countermeasures.

Secure system development

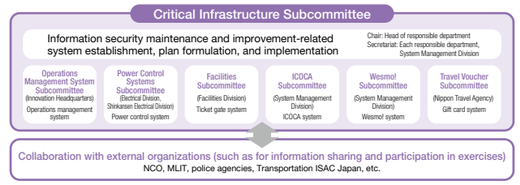
To ensure the safe development and operation of our systems and services, the JR-West Group is implementing a security review initiative based on the concept of security by design. In this, security requirements are confirmed and approved at the system concept stage, while the implementation status is confirmed before release, particularly for systems that handle customers' personal information, for which tight security measures are required.

Self-inspection-based continuous improvement activities

The JR-West Group has formulated the JR-West Group Information Security Guidelines, which set out specific security standards that must be observed. We regularly review these guidelines in light of technological trends and past incidents.

Based on these guidelines, JRW-CSIRT member companies conduct self-inspections to ensure that the necessary security measures are being implemented appropriately in each system. If any deficiencies are found, they formulate an improvement plan and undertake improvement activities. The JRW-CSIRT Secretariat supports early risk reduction by following up on self-inspections, and JR West IT Solutions Company (J-WITS) helps improve security at group companies by providing IT shared services and IT business support services.

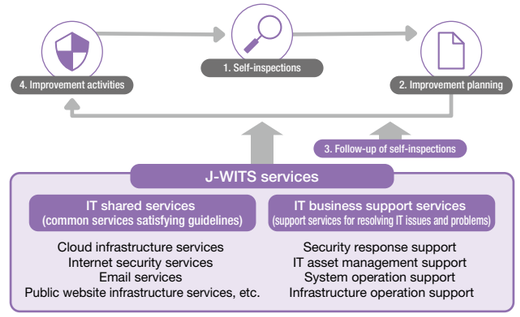
■ Operation of the Critical Infrastructure Subcommittee



■ Steps until a decision is made to invest in system development

Baseline approach	Confirm that the security requirements expected of JR-West Group systems, as stipulated in the JR-West Group Information Security Guidelines, are adhered to.
Risk-based approach	Identify and evaluate risks according to system and service characteristics, and confirm the adequacy of security measures for each risk.

■ Self-inspection-based continuous improvement activities

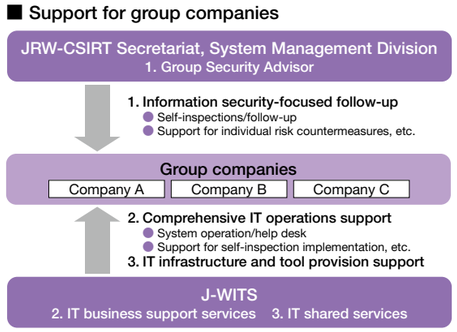


Support for group companies

Further improving the level of information security, not only for JR-West but for the entire JR-West Group, is an urgent issue in promoting the Group's digital strategy. Each year, each group company works to improve information security accuracy based on the PDCA cycle. Group companies recognize that resolving common issues, such as a shortage of IT and information security personnel, increased workloads due to system implementation and updates, and concerns about their own information security risk assessments is key to further improvement. To that end, we are supporting group companies with the following three measures, which includes new measures.

1. JR-West has strengthened the Group Security Advisor position, which was newly established in fiscal 2025 to support group companies in resolving information security issues. For example, we engage in specific discussion with each company regarding each of the wide-ranging self-inspection checklist items, assess risks, share awareness of key risks, and conduct activities that drive improvement.
2. We are strengthening the IT promotion system of our group companies through IT business support services provided by J-WITS. This not only raises the level of each company's security response capabilities but also reduces their workload.
3. We provide IT shared services, such as the J-WITS shared platform and information security countermeasure tools, that meet the information security guideline checklist, to reduce information security risks at group companies and to ease the burden of self-inspections.

■ Support for group companies



Information security

Information security measures

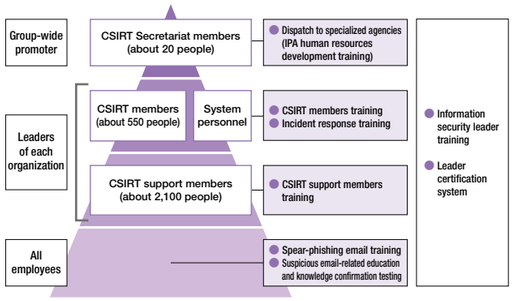
Improving employee literacy

As part of our efforts to improve information security-related literacy, the JR-West Group provides information security training and education for all employees along with rank- and role-specific education and training. In addition, to motivate employees engaged in information security work, we have an information security leader certification system.

FY2025 results

Classification	Conditions	Number of certified individuals
★★★	Information security leader training: Completed + Registered information security specialist examination: Passed	70 people
★★	Information security leader training: Completed + Information security management examination: Passed	228 people
★	Information security leader training: Completed	6,297 people

■ Overview of information security training and education



Education and training for all employees

In order to foster crisis consciousness and improve initial response capabilities, we conduct spear-phishing email training for all executives and employees (about 50,000 people) of JRW-CSIRT member companies.

Additionally, we provide training to all employees of JRW-CSIRT member companies to ensure they have an understanding of the minimum rules that must be observed. In fiscal 2025, we conducted training for all executives and employees on the 10 points of suspicious emails and posted warning posters in each workplace.

Awareness-raising poster　Stickers handed out

Education and training for management and promotion leaders at each organization

Scene from an information security training session

● **For senior management and department heads**

We conduct training for executives, CISOs, and other senior management (about 210 people) of JRW-CSIRT member companies, including group companies, with the aim of helping them understand the threat of cyberattacks, how to counter them, and the role that management should play in security measures.

● **For personnel in charge of information security**

We conduct training for JRW-CSIRT members and others in order to cultivate human resources capable of taking the lead in information security measures. We also hold briefing sessions for CSIRT support members to help them understand the basics of information security and the purpose and content of CSIRT activities.

● **For personnel in charge of critical infrastructure**

We participate in cyber-exercises (simultaneous exercises in all fields, as well as prior to Expo 2025) organized by the NCO for critical infrastructure operators, and are verifying failure response systems.

Education and training (incident response training) for management and promotion leaders at each organization

JRW-CSIRT member companies conduct training that simulates the suspension of important corporate systems and the leakage of confidential information. The purpose of this training is not only to ensure system personnel understand the incident response process but also to ensure management make appropriate decisions when an incident occurs. This training is therefore conducted with the participation of top management.

Education and training for Group-wide promoters

We dispatch employees for one year to the core human resources development program sponsored by the IPA to develop security-savvy human resources. In addition, we have a system to support participation in outside training and the acquisition of qualifications. As a result of encouraging security-related study in particular, over 70 people within the JR-West Group have passed the registered information security specialist examination.

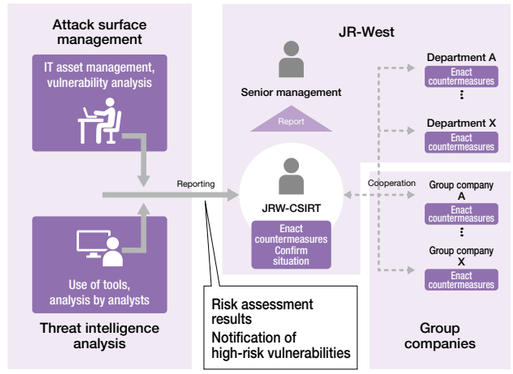
Overview of technical countermeasures

With the expansion of the use of cloud services and AI-related systems, the amount of internet-driven communication is increasing year by year. This means the risk of cyberattacks is also increasing. In response to this, we are considering and introducing technical measures that address the risks of cyberattacks from the perspective of identity, devices, networks, applications, data, and monitoring. We are also working to ensure people can have greater confidence when using JR-West Group services, such as by strengthening email sender authentication.

Responding to external threats

We collect intelligence information that provides signs of cyberattacks and clues about attacks, along with externally disclosed digital asset management information, and we regularly analyze this information from the attacker's perspective. This allows us to identify weaknesses in the JR-West Group and to be continuously strengthening our preparedness against cyberattacks.

■ Responding to external threats



Setting information security-related KPIs and recognizing outstanding organizations

We have set information security-related KPIs for JRW-CSIRT member companies, and we conduct quantitative evaluation of security measures. Specifically, by setting Group-wide KPIs for individual items, such as attack surface investigation using threat intelligence, spear-phishing email training, and the number of participants in information security leader training, we ensure there are shared, common goals among all departments and Group companies, thereby promoting consistency in security measures.

● **Awarding outstanding organizations**

Organizations that have achieved particularly outstanding results are recognized, and their efforts are highlighted to further promote information security activities within the JR-West Group. Based on their performance in fiscal 2025, awards were given to four organizations for the Grand Prize, five for the Excellence Award, and one for the Encouragement Award.

Excellence Award presented to JR West Shopping Center Development Company

Excellence Award presented to Osaka Electrical Construction Office

■ Main information security-related KPIs

- Attack surface investigation using threat intelligence
  Important items have been addressed
- Spear-phishing email training
  Percentage of recipients who did not issue a report after opening the test email: Less than 1%
- Number of participants in information security leader training
  Percentage of employees with information security leader certification: 10% or more

Third-party evaluations, certifications, etc.

Third-party evaluations, certifications, etc.

The JR-West Group is actively working to obtain certifications and qualifications related to information security.

● **Acquisition of ISMS certification at JR-West**

On March 16, 2025, the JR-West Digital Solution Headquarters' Wester-X Business Division obtained ISMS certification (ISO/IEC 27001:2022), an international standard for information security management systems.

● **Information security-related qualifications acquired**

In order to appropriately implement security measures at each company, we encourage them to acquire security-related public qualifications.

As of April 1, 2025 (including those who passed under the previous system)

Name of qualification	Number of certified individuals		Total
	JR	Group companies	
Registered information security specialist (SC)	36	38	74
Information security management (SG)	241	151	392