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.

In the JR-West Group, which is accelerating efforts to meet the challenges of the post-pandemic era, our "offensive" digital strategy and "defensive" information security measures go hand in hand. Ensuring appropriate information security across the entire Group will lead to the provision of safe services and the peace of mind and trust of our customers. Next fiscal year, Expo 2025 will be held in our business area. We will continue to update our measures in response to changing circumstances, in collaboration with group companies and external 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])

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.

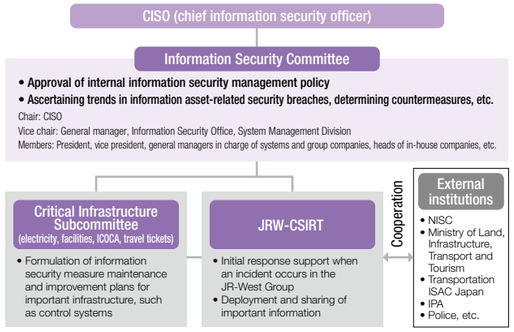
● JR-West Group CSIRT

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. We are working to expand our framework by assigning JRW-CSIRT members (about 400 people from 80 companies) to serve as contact points for each company and JRW-CSIRT support members (about 2,100 people) to each workplace.

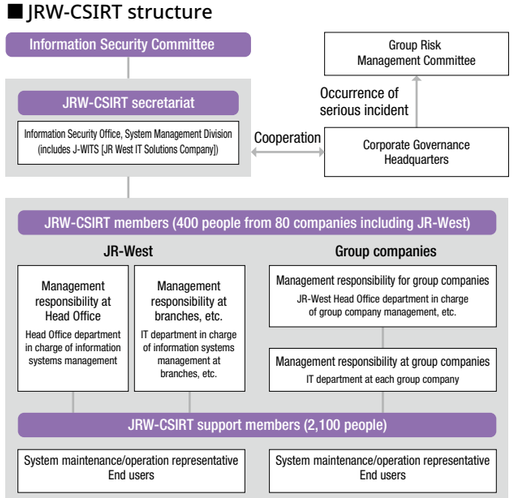
● Collaboration with external organizations

We are strengthening security through membership in Transportation ISAC Japan*2, active participation in working groups organized by the NCA (Nippon CSIRT Association)*3, and information sharing with the NISC (National Center of Incident Readiness and Strategy for Cybersecurity) and police organizations.

■ JR-West Group's security structure



■ JRW-CSIRT structure



Improving employee literacy

In order to improve employee literacy within the JR-West Group, in addition to providing security training and education for all employees, we also provide education tailored to specific groups.

● For all employees

We are conducting spear-phishing email training and security education for all employees of JRW-CSIRT member companies, including group companies. In addition, every year since fiscal 2016, we have published an annual report covering the results of the IT department's activities and its future activity policies as part of our efforts to raise awareness of the specific duties of the IT department.

■ *IT Report* published by the IT department

● For promotion leaders in each workplace

For senior management and department heads

We conduct training for senior management (approximately 210 members) at JRW-CSIRT member companies, 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 in charge of information security

We conduct training for JRW-CSIRT members and information systems managers in JRW-CSIRT member companies (approximately 2,900 people) in order to cultivate human resources capable of taking the lead in information security measures. We also provide training for the CSIRT support members (about 2,100 people) who are responsible for initial incident response and for education and awareness-raising activities within each organization 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 verify our system for responding to failures by participating in cyber exercises (cross-sector exercises) hosted by NISC for critical infrastructure providers.

● 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 JR-West 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)
	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, spear-phishing email training
	Level	Can handle personal/confidential information appropriately

■ Scene from an information security training session

Contributing to the railway business as a member of the information security team

For one year starting in July 2023, I participated in the IPA's ICSCoE (Industrial Cyber Security Center of Excellence) as a student in the seventh cohort of the core human resources development program. JR-West provides services centered on railways, and due to our large sphere of influence, I felt that it was a pressing issue to understand and enact measures against cyberattacks, so I volunteered to participate. At ICSCoE, I learned first-hand about the mechanisms of control systems and cyber security-related technologies and knowledge. I also learned about approaches companies can take to business continuity and recovery when they are attacked. Going forward, as a registered information security specialist, I want to contribute to protecting our business from cyberattacks from both a technical and management perspective.

Information Security Office, System Management Division, Digital Solutions Headquarters
Yuri Nishizawa

*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.

Information security

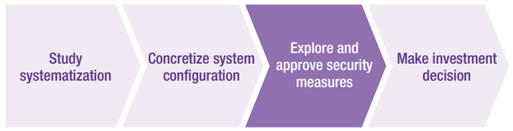
Secure system development

Based on the concept of security by design, the JR-West Group is studying and approving security measures at the conceptual stage of system development in order to develop and operate secure system services.

● Deliberations on important systems

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.

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



Establishing the PDCA cycle

We maintain the JR-West Group Information Security Guidelines, which stipulate specific security standards that must be followed, and we update them in response to technological trends and past incidents. Based on these guidelines, we conduct security self-inspections of a total 144,753 items for 3,302 systems throughout the JR-West Group each year to strengthen security measures on an ongoing basis.

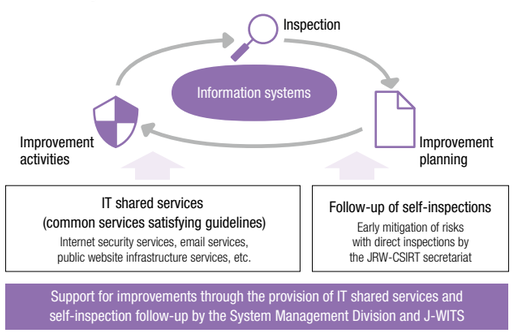
● Follow-up on security self-inspections

The JRW-CSIRT secretariat directly inspects all JRW-CSIRT member companies for important inspection items. They communicate with each workplace to confirm the situation and provide support, thereby mitigating risks as quickly as possible.

● Providing IT shared services that meet the guidelines

To support improvements at each company, we provide shared services and common systems and tools that meet the guidelines, thereby reducing the burden of conducting self-inspections and adopting tools in each organization.

■ Continuously improving information system security measures



Data utilization in the JR-West Group

Based on the JR-West Group Data Utilization Policy, we have established a group-wide data governance framework to efficiently and safely share and utilize data, and we are working to further the utilization and ensure the safety of data transactions. To realize this, we hold training sessions three times a year and implement the following actions.

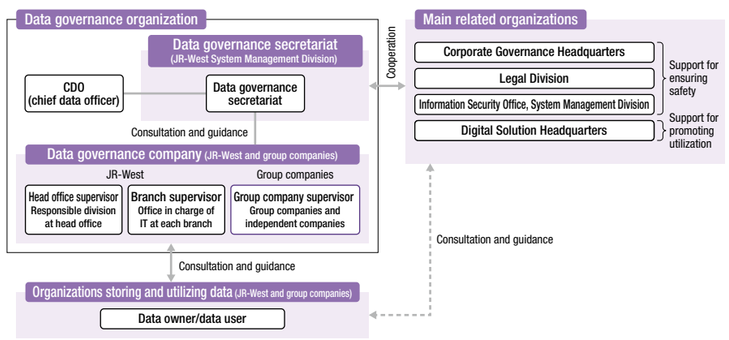
● Promoting utilization

We conduct awareness-raising activities, such as introducing case studies from other companies, once a month, and we visualize data by formulating a data catalog that summarizes data held by the JR-West Group.

● Ensuring safety

By making a data transaction application form, checklist, and contract template available, we ensure that everyone can properly manage and contain risks. In addition, we provide consultations on data utilization.

■ Data governance framework



Setting information security KPIs and commending outstanding group companies

● Setting information security KPIs

We set information security KPIs for JRW-CSIRT member companies and quantitatively evaluate the status of the security measures taken.

We implement consistent security measures. Specifically, we share common goals with every department and group company by setting group-wide KPIs for items such as inspection of systems based on guidelines, spear-phishing email training, and number of employees participating in security training.

● Commending outstanding group companies

Group companies that have achieved particularly outstanding results, such as 100% compliance rate with countermeasures in system inspections, zero recipients opening the simulated phishing email in the spear-phishing email training, and 50% or more employees securing information security leader certification are commended as outstanding companies. We highlight the information security activities at each group company as we strive to motivate our employees to continue tackling information security.

■ KPIs for information security

- Inspection of systems based on guidelines
  Rate of compliance with countermeasures: **100%**
- Spear-phishing email training
  Percentage of recipients who did not issue a report after opening the test email: **Less than 1%**
- Number of security training participants
  Percentage of employees with information security leader certification: **10% or more**

■ Scene from a ceremony awarding outstanding group companies

Security measures in preparation for Expo 2025

In preparation for Expo 2025, which will begin in April 2025, we are implementing the following measures to respond to intensifying cyberattacks.

● Improving cyber resilience in the event of an incident

We conduct desktop training for JRW-CSIRT member companies, simulating the shutdown of critical systems owned by each company and the leakage of confidential information. This training is intended not only for system personnel to understand the series of incident response processes, but also for senior management to understand the management decisions they need to make in the event of an incident; therefore, it is conducted with senior management in attendance.

Also, in the event of an incident or potential risk that requires immediate action by the JR-West Group or other companies, we immediately hold a briefing to deepen understanding of the incident and promptly respond to it.

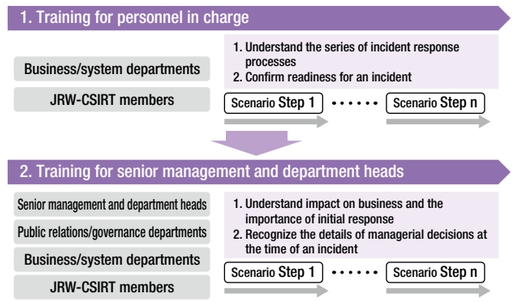
● Active cyber defense

We combine threat intelligence with attack surface management to analyze externally disclosed IT assets from the attacker's perspective and continuously monitor the latest cyber threats. We also strengthen preventive cybersecurity by proactively taking measures against threats we discover.

● Strengthening ties with government and other organizations

We are strengthening cooperation with external organizations, including participation in NISC's effort to strengthen public-private partnerships for Expo 2025 (JISP), while working to share information during normal times and respond quickly in emergency situations.

■ Incident response training



■ Active cyber defense