Information Security

Performance Indicators to Monitor the Achievement of the Medium- to Long-Term Vision and FY2021 Results

Performance indicators	Targets	FY2021 results
(1) Rate of information security compliance assessments conducted	(1) Achieve 100% (covering all business units and Group companies).	(1) 100% (90 units and companies)
(2) Rate of inspections and instructions by the executive officer in charge of divisions implementing priority measures for personal information protection, etc.	(2) Achieve 100% (covering all organizations concerned)*.	(2) 100% (86 times)
(3) Participation rate of information security education and training	(3) Achieve 100% (covering all organizations concerned).	(3) 100% (Approx. 41,000 persons)
(4) Rate of security vulnerability tests for publicly open websites	(4) Achieve 100% (covering all websites concerned).	(4) 100% (487 web systems)

* Due to the COVID-19 pandemic, we postponed on-site inspections by officers and switched to remote inspections by supervisors.

Exchanging information over the Internet both enriches consumers' lives and greatly improves companies' productivity. One of the social changes accelerated by the COVID-19 pandemic is the increased use of online services, which raises the importance of ensuring information security and protecting personal information. As DNP handles many information assets, including personal information, we regard managing and protecting these information assets as an important social responsibility and have been undertaking various initiatives accordingly.

Establishing DNP CSIRT (Computer Security Incident Response Team), an Organization Addressing Cybersecurity

As cyberattacks are becoming increasingly frequent and sophisticated globally every year, the damage from these attacks is a threat to corporate management. Positioning cybersecurity measures as a management responsibility, the Japanese Ministry of Economy, Trade and Industry established the Cybersecurity Management Guidelines.

Prior to this, DNP has worked to enhance its information security functions, and has put significant effort into practical training for the essential personnel involved in cyberattack countermeasures. To increase preparedness, the DNP Computer Security Incident Response Team (DNP CSIRT) joined the head office to address cybersecurity in October 2021. Increasing cooperation between organizations in preparation for cyberattacks enables them to maintain business continuity in the event of any unforeseen circumstances (incidents). The organization supervising overall cybersecurity implements the following activities across the DNP Group companies in Japan and overseas, in addition to their basic functions.

- ●Visualize ICT infrastructure and implement countermeasure instructions based on security vulnerability information and confirm their application status
- ●Design of and proficiency in countermeasures in the event of any unforeseen circumstances (incidents)
- ●Instructions and support for various organizations in the event of any unforeseen circumstances (incidents)
- ●Enhance education, practical exercises and awareness of cybersecurity
- ●Collaboration with external organizations such as the National center of Incident readiness and Strategy for Cybersecurity (NISC) and Nippon CSIRT Association
- ●Enrollment in and application of cyber risk insurance

Promoting a Zero Trust Network

DNP has increased security measures based on the conventional concept of perimeter security controls that protect boundaries between the Internet and internal networks. For example, we introduced SIEM (Security Information and Event Management) to strengthen measures against unknown viruses and analyze network monitoring devices and security logs to facilitate early detection of and response to incidents.

Changes in corporate activities have rapidly progressed in recent years, characterized by the promotion of DX, the utilization of external cloud infrastructure and the accelerated introduction of telecommuting systems during the covid-19 pandemic. Amid this trend, a new policy called a zero trust network, which typically involves not trusting anything, even an in-house network, is being advocated. To keep up with these changes, DNP is reviewing its security measures based on the concept of the zero trust network. First, we are working to strengthen internet access security and bolster endpoint security for each type of terminal, such as personal computers and servers.

More specifically, we have revamped our web gateway and introduced a mechanism to access the internet more safely by, for example, blocking access to hazardous websites, preventing the intrusion of malware (malicious software) and monitoring the transmission of large quantities of data for non-business purposes. To increase endpoint security, we introduced Extended Detection and Response (XDR) to monitor and analyze unknown malware and its behavior. In this way, we are revamping our measures to address computer viruses. Even in the unlikely event that unauthorized access is detected, and an alert (alarm) is issued, after isolating the terminal suspected of being infected with malware, DNP CSIRT will play a central role in promptly detecting and responding to incidents, such as by identifying intrusion routes, ascertaining the status of the spread and blocking communications.

DNP will further strengthen our information security measures to reflect the latest trends.