Information Security

Performance Indicators to Monitor the Achievement of the Medium- to Long-Term Vision and FY2020 Results

Performance indicators	Targets	FY2020 results
(1) Rate of information security compliance assessments conducted	(1) Achieve 100% (covering all business units and Group companies).	(1) 100% (87 units and companies)
(2) Rate of inspections and instructions by executive officer in charge of divisions implementing priority measures for personal information protection, etc.	(2) Achieve 100% (covering all applicable divisions)*.	(2) 100% (82 times)
(3) Participation rate of information security education and training	(3) Achieve 100% (covering all business units and Group companies).	(3) 100% (Approx. 41,000 persons)
(4) Rate of security vulnerability tests for publicly open websites	(4) Achieve 100% (covering all applicable websites.	(4) 100% (425 systems tested)

* We postponed on-site inspections due to the COVID-19 pandemic and switched to remote inspections.

Exchanging information over the Internet both enriches consumer's lives and greatly improves companies' productivity. With the COVID-19 pandemic being one contributing factor, services that use the Internet have been growing rapidly, attaching greater importance to ensuring information security and protecting personal information. As DNP handles many information assets, including personal information, we regard that managing and protecting these information assets is one of our important social responsibilities and have been undertaking various initiatives accordingly.

Promoting Diverse Information Security Measures, Including Response to Advanced Persistent Threats (APTs)

With cyber attacks now becoming increasingly artful and complex, Ransomware Attacks and Confidential Information Theft by APT ranked first and second, respectively, in the 10 Major Security Threats 2021 list of the Information-technology Promotion Agency (IPA). In the latter threat, an attacker with malicious intent obtains or destroys information by infecting personal computers with a computer virus via e-mail and penetrating the system of the target organization. Leakage and misuse of confidential information can cause a significant impact on business continuity and national security.

DNP has always positioned reinforcement of information security as an important management issue and has been implementing a range of measures that also factor in the latest trends. For example, we have built layered countermeasures that combine "inbound measures" comprising vulnerability and virus protection measures for personal computers and servers, "internal measures" to contain damage in case the system has been penetrated and "outbound measures" that prevent information from being illicitly transmitted outside the system. We have also been promoting Security By Design, whereby protective functions are reflected in a computer system from its design and development stage, and conducting periodic vulnerability tests on systems already in use.

The DNP Group company Cyber Knowledge Academy Co., Ltd. provides educational programs internally and externally to nurture personnel to counter cyber attacks. Based on these programs, DNP conducts periodic training, in which 203 employees have participated to date. In addition, we are working to improve the skills level of our security personnel by dispatching employees to the IPA and participating in education provided by the Industrial Cyber Security Center of Excellence (ICSCoE). DNP also conducts the following organized activities through its Computer Security Incident Response Team (CSIRT), a team of specialized staff (3 full-time members and 15 with concurrent posts) to respond to information security issues, in collaboration with the Nippon CSIRT Association and other organizations.

- Devise and implement cyber security measures
- Research information security technology inside and outside the Company
- Cut off malicious site communication
- Communicate information on vulnerabilities that require immediate action and verify the implementation status of measures
- Provide instruction on technological measures in an emergency such as infection or spread of a virus

Strengthening Information Security Measures Adapting to Work Styles under the New Normal

The COVID-19 pandemic, among other factors, has prompted rapid spread of telecommuting and other new work styles, and more people are now accessing their internal system from outside the office and using web conferencing. This, in turn, has given rise to concern about increasing attacks exploiting these rapid changes in the working environment, and the IPA listed Attacks on New Normal Work Styles such as Teleworking for the first time in its 10 Major Security Threats 2021 and placed it in the third place.

As the new normal has become more firmly instilled to drive drastic changes in work and living styles, DNP has been implementing various measures along with the basic measures described above. These include establishing the definition of telecommuting, formulating operating rules and providing thorough security education. For example, we prevent such threats as intrusion and attacks from outside by requiring multifactor authentication when employees access our internal system from places other than our bases and not permitting the use of unauthorized information devices. We will continue to further strengthen our information security measures in order to reflect the latest trends.