Defend and Attack with ICT.

Smooth response to “telework”

For “defensive IT,” it is important to promote paperless operations, introduce cloud-enabled PCs that enable telework, and develop a communication environment. From the two perspectives of realizing more flexible work styles and promoting the shift to cloud, all the Group companies are replacing existing PCs with cloud-compatible PCs. Today, it is essential to shift to a cloud environment in order to quickly and flexibly realize business strategies through digitalization. We have completed the construction of a cloud infrastructure in the Group equipped with data linkage functions and job execution and monitoring functions, and we will promote the transition from legacy systems to cloud systems in both hardware and software, such as planning all future systems on a cloud basis.

As for department store operations, we completed the introduction of smart payments for credit cards and handsets that can be used in front of customers in order to improve customer service and enhance credit card security. With regard to security, we conducted vulnerability assessments of our business systems and websites, developed countermeasures, and strengthened security through email training, incident training, employee training, and other means.

Lifetime Service HUB scheme

In the area of “aggressive IT,” we are promoting the “Lifetime Service HUB scheme,” i.e., the creation of a system that aims to become a life partner who extends lifelong support to customers and to provide new products and services. On the system front, we will build a system that has the following three functions.

1) Function of collecting, accumulating, and integrating customer information held by each company
2) Function of analyzing and predicting customer profiles (hobbies, preferences, purchasing behavior, etc.)
3) Function to communicate more closely with customers

In fiscal 2019, we completed the development of basic functions for the “Group integrated customer database,” which is a tool for managing and utilizing all customer data from the Group companies as shared assets, and incorporated the data held by department stores. In the current fiscal year, we will collect data held by Parco and support the use of data to increase sales and drive customer traffic at department stores and Parco. At the same time,

we will develop additional functions such as the acquisition of external data and analysis functions.

By utilizing the Lifetime Service HUB, we not only sell products from the "product's perspective" but also communicate with customers on a one-to-one basis from the "customer's perspective," providing personalized purchasing experiences and services more efficiently and effectively across our businesses and channels. The full-scale operation of the system is scheduled for 2021.

In addition, as for new customer strategy projects at department stores, we promoted each project and introduced systems, such as the development of smartphone apps at all department stores, the introduction of MA* (Marketing Automation) tools as a new communication tool, and the introduction of systems to transform to a new *gaisho* business model.

* MA: Marketing Automation (a mechanism to improve operational efficiency by automating marketing operations)

Security measures

In recent years, cyber attacks have become more complex and sophisticated, and information security risks are increasing. To minimize such risks, we established the Group's common security policy in July 2018 and are continually implementing security measures based on this policy.

First, in order to visualize and improve the security measures of each Group company, we conducted hearings on the security measures of the systems maintained by each company, performed vulnerability assessments to confirm the safety of websites with high risk of information leaks and systems that maintain personal information, and made improvements to promptly ensure the safety of systems and websites where problems were discovered. We also conducted continuous surveys of the status of communications related to unauthorized access to personal computers used by employees and information leaks. In addition to continuing these efforts this fiscal year, we will also take measures to strengthen security, including investigating the robustness of servers, strengthening monitoring, and reviewing internal rules for more appropriate information management.

In addition, employee education is an important element of security. Continuing from the previous fiscal year, we conducted e-learning-based education and targeted attack email training. In the current fiscal year, we will continue activities to raise the level of information security for employees through education and training.

In fiscal 2019, the departments in charge of security at JFR Information Center, a consolidated subsidiary, worked closely with us to strengthen our security management system and prepared countermeasures and initial actions in the event of an accident. Specifically, we launched the JFR Group CSIRT*, and officially joined the Nippon CSIRT Association in July. The documents developed by this JFR-CSIRT were shared horizontally among the Group companies, and a system for dealing with incidents was launched at each Group company. In particular, this fiscal year we will strengthen our management system in conjunction with activities to strengthen IT governance.

* CSIRT: Computer Security Incident Response Team

▶Image of Lifetime Service HUB scheme