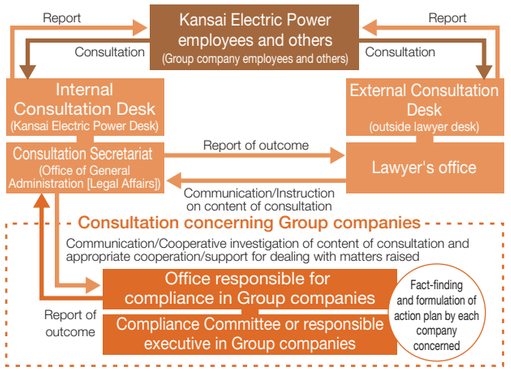
# 6 Strict Enforcement of Compliance

## Efforts to enable each employee to participate actively

### Compliance promotion system

To promote compliance activities at each workplace, department and branch heads with compliance responsibilities assign staff (primarily section head-level personnel) to serve as compliance promotion officers. In fiscal 2012, we carried out compliance training sessions in 12 locations to reinforce awareness of the compliance promotion officer in their role. In addition, to respond to compliance-related concerns of employees and others, we established Compliance Consultation Desks. These desks can be used by the employees and temporary workers of all Kansai Electric Power Group companies, as well as by our business partners, and thus provide a structure through which we can collect a broad range of risk information. A total of 31 cases were reported for the entire Group in fiscal 2012, with the largest number of cases reflecting issues relating to the workplace environment.

■Kansai Electric Power Group Compliance Consultation Desks




### Promoting autonomous activities in each workplace

At each workplace, compliance promotion staff hold workplace discussions at least once yearly to share awareness of compliance risks that may be hidden in everyday operations. In fiscal 2012, we introduced visual tools for discussion and made other efforts to establish autonomous compliance practices to enable employees to actively participate in compliance activities.

### Communication and training suited to each level

In October 2012, the Legal Division held a compliance lecture for executive officers. The outside lecturer's talk included compliance-related points requiring particular attention from Kansai Electric Power. Approximately 40 executive officers attended the lecture, which afforded a good opportunity to refresh awareness of the importance of compliance.
We also carry out training programs targeted at employees who are taking on new or greater levels of responsibility, including new employee education and training for freshly appointed senior staff. Moreover, we actively carried out on-site compliance training targeted at frontline responsibilities within the company as we did in fiscal 2011. In fiscal 2012, we focused in particular on training for frontline employees, holding on-site training sessions at 49 locations. The session content was configured to participants' actual roles and was well received.

Compliance lectures for executive officers

### Efforts to generate shared Group-wide awareness

In November 2012, we held a compliance lecture for Group company executive officers, which was attended by 38 companies. The lecture, which was given by an outside specialist, was based on actual cases, and served to foster unified, Group-wide awareness of compliance.
Our on-site compliance training for Group companies has been part of our efforts since 2007, and in fiscal 2012 we were able to hold a total of 25 sessions for 16 companies.
In fiscal 2013, we will continue to promote efforts to share awareness of the important of compliance across the Group as a whole.

On-site compliance training for Group companies

## Promoting information security countermeasures and ensuring thorough protection of personal information

### Promoting information security management

Kansai Electric Power has established the Infrastructure Development Committee, chaired by the Vice President, with the aim of building a strong management base capable of supporting medium- to long-term growth. In the committee, the promotion of information security management is one important issue that is being addressed.
To advance effective, efficient security control measures, the committee deliberates on the formulation of annual plans and on midterm progress from the four viewpoints shown below.

**Viewpoints for deliberation of information security management**

1. Organizational measures
2. Personnel measures such as education and training
3. Physical measures such as document management and access control for offices
4. Technical measures such as improving computer systems

**Practical measures implemented**

**1 Organizational measures**
- Appointment of the General Manager of Management Innovation and IT Headquarters as Chief Privacy Officer.
- Formulation of Information Management Regulations, and production of the Information Security Rulebook explaining these regulations in straightforward terms for all employees.
- Self-checking by Information Security Managers regarding the daily handling of information, including secure storage of confidential documents and their appropriate disposal.

**2 Personnel measures**
- Enforcement of rules by means of group training for new employees, managerial staff, and other groups.
- Training in identifying and dealing with targeted email attacks*.
- Education program on information security for all employees at least once a year.
- Workplace discussions using case studies, etc.
- Initiatives to prevent the recurrence of information leaks caused by the use of file sharing software.

**3 Physical measures**
- IC cards (employee identity cards, etc.) to control access to offices, zoning of offices by partitions, strict management of confidential documents by means such as additional allocation of shredders and lockable furnishings.

**4 Technical measures**
- Using IC cards (employee identification cards, etc.) for authorization of computer users.
- Checking by immediate managers to prevent fraudulent use of customer information systems.
- Automatic encryption system for data files being taken off company premises.
- Use of system logs to prevent fraudulent manipulation by IT staff.
- Introduction of measures to restrict the connection of external storage media to in-house computers.
- Introduction of efforts to prevent unauthorized access or theft of information due to cyber attacks.

**Enhancement of information security by IC cards (employee identification cards, etc.)**

Individual authorization for logging on to the in-house network

Monitoring electric locking/unlocking of doors and entrance and exit history

**Provision of lockable furnishings**

Rigorous management of important documents and external memory media

*Targeted email attack: One variety of cyber attack. The sender uses sophisticated techniques to trick the recipient into opening an attached file, transmitting a computer virus that enables attacks on the targeted company, or exploitation of information.

### ■Initiatives for protecting personal information

In March 2005, Kansai Electric Power established internal rules including Personal Information Protection Regulations, which stipulate the purposes for which personal information can be used within the company and methods for responding to personal information disclosure requests by customers.
After the Act on the Protection of Personal Information went into full effect on April 1, 2005, we took steps aimed at bolstering our personal information protection practices, including creating a Personal Information Handling Manual and adding greater detail to our internal rules.

### ■To raise awareness among individual employees

Every year, Kansai Electric Power checks compliance with rules and systems in each workplace and has the results of this monitoring verified by a third party. This helps us ascertain and improve the level of compliance with various rules and facilitates the correction of inappropriate rules.
Every year, we hold training sessions aimed at explaining the basic rules, identifying rule violation hazards, and calling all our employees' attention to these issues. We also distribute various email magazines, which we use to spread knowledge about policies for preventing leaks of personal information and to raise our employees' IT knowledge. We will continue educating our employees to help ensure that everyone is engaging in appropriate information management practices.

### ■Strengthening Group governance

To fully ensure Group-wide information security compliance and appropriate handling of personal information, in December 2004, we formulated the Kansai Electric Power Group Information Security Guidelines.
To further improve our security level, we will continue to review and revise these Guidelines as necessary, while also encouraging each of our Group companies to independently promote their own information security management practices.