Cybersecurity

While transactions using the Internet and smartphones have increased with the remarkable development of digital technology in recent years, the Bank has been working to expanded services that rely on digital channels.
On the other hand, the advance in sophistication and skill in methods of cyberattacks has brought increasing risk to financial institutions.
JAPAN POST BANK has therefore committed to the JAPAN POST GROUP Executive Declaration on Cybersecurity, regards the risk of cyberattacks as one of the top risks for management, and works to continuously strengthen the cybersecurity system through management leadership in an effort to deliver safer, more secure services to our customers.

Governance System

In order to strengthen the cybersecurity system through management leadership, JAPAN POST BANK has established an organization dedicated to cybersecurity (the IT Strategy Department's Cyber Defense Office) under the President and Representative Executive Officer and the Chief Information Security Officer (CISO). By providing reports on a regular and ad hoc basis to the Board of Directors and the Executive Committee, the Bank has developed a governance system that allows for timely, appropriate management decisions in accordance with changes in the environment.

Through these efforts, the Bank endeavors to promote appropriate cybersecurity system enhancements and to prevent cyberattacks.

Management System

JAPAN POST BANK has established several professional cybersecurity organizations, including JPBank CSIRT*1, which serves to prevent cyber incidents and respond in the event one actually occurs, and JPBank SOC*2, which monitors logs from security devices, network equipments, and other sources to detect and analyze any indications of cyber incidents, as part of our ongoing efforts to protect against cyberattacks.

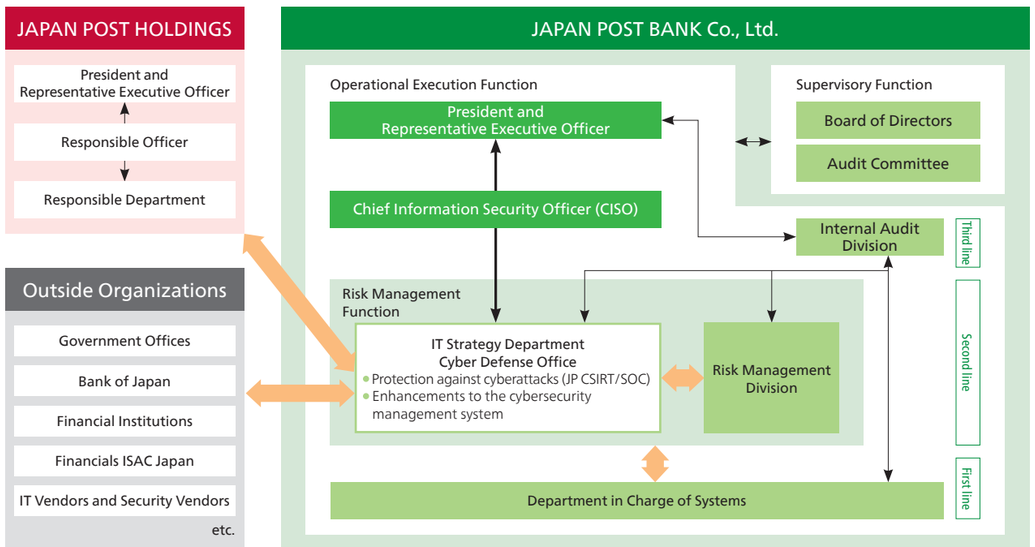
In order to ensure that we can precisely and rapidly engage in information sharing, decision making, public relations, and countermeasures in the event of an incident, the Bank conducts regular drills and exercises. We also actively participate in outside activities, including drills and exercises organized by the Financial Services Agency of Japan and the Metropolitan Police Department.

Moreover, the Bank works to strengthen its cybersecurity system in accordance with third party assessments and recommendations based on the FFIEC-CAT*3, which is used internationally as a tool to evaluate the management systems of financial institutions.

In addition, the Bank has prepared multilayer detection and defense measures, including analysis of and countermeasures against new modes of attack, through cooperation with government offices, other companies in the industry, and related associations.

*1 Computer Security Incident Response Team
*2 Security Operation Center
*3 Federal Financial Institutions Examination Council – Cybersecurity Assessment Tool

Cybersecurity Management System



Major Cybersecurity Initiatives

Digital Channel Security Measures

In order to enable our customers to use services provided through digital channels with a greater level of safety and security, JAPAN POST BANK is advancing efforts to enhance our cybersecurity system and to protect against cyberattacks on a daily basis. These efforts include strengthening identity verification and authentication processes, anti-virus measures, vulnerability responses, threat trend analyses, cyberattack detection, and fraudulent transaction monitoring.

- **Strengthening Identify Verification**
  Introduced eKYC*4 to prevent fraudulent registration impersonating customers
- **Strengthening Identify Authentication**
  Introduced an authentication app that complies with FIDO*5 to further strengthen authentication during important transactions, such as money transfers, and introduced Token, a device for generating passwords that can only be used once (one-time passwords)
- **Anti-virus Measures**
  Free distribution of PhishWall Premium, a software designed to prevent fraudulent money transfers by detecting attacks that defraud customers of their personal identification numbers, etc.
- **Vulnerability Countermeasures**
  Collect and act on information regarding daily cyberattack threats and vulnerabilities
- **Fraudulent Transaction Monitoring**
  Monitor unauthorized access to Internet banking systems and prevent damage from fraudulent money transfers, etc.

*4 electronic Know Your Customer: A technology that compares smart cards from personal identification documents with facial information photographed at the time of registration to complete identity verification entirely online.
*5 Fast Identity Online: international standards for online authentication.

Developing Human Resources to Support Cybersecurity

In today's world where use of cloud services, AI, and other digital technologies only continues to increase, taking actions with an awareness of cybersecurity risks in all manner of situations as part of business activities has become essential.

In order to strengthen the management base to become a more trusted bank, JAPAN POST BANK assigns professional cybersecurity experts. Similarly, we systematically organize the required skills, promote human resources development in a planned manner in line with the responsible duties and skills, and enhance the expertise of human resources for this purpose.

Moreover, the Bank is fostering an awareness of cybersecurity among every employee, including those involved in management, and actively provides the basic knowledge required to implement countermeasures.

Developing Professional Cybersecurity Experts

In order to promote cybersecurity system enhancements and put protections against cyberattacks into practice, JAPAN POST BANK formulates training plans based on the required professional knowledge and experience, provides skills training courses and assistance for acquiring certifications, and conducts incident response drills.

Moreover, the Bank actively participates in outside initiatives, including the Financials ISAC Japan, an organization established to share information among the financial sector, as well as various training programs organized by the Financial Services Agency of Japan and the Metropolitan Police Department. Through these endeavors, we accumulate professional knowledge and experience in order to strengthen our implementation frameworks.

Cybersecurity Education

In order to chart a greater awareness of and provide more in-depth basic knowledge on cybersecurity, JAPAN POST BANK conducts cybersecurity training for managements as well as targeted e-mail attack drills for all employees.

In addition, the Bank publishes an internal informational magazine in an effort to raise awareness of cyberattacks and to inform employees of countermeasures. We also provide e-learning contents designed to teach everything from basic knowledge to the latest expert-level knowledge, in an effort to educate employees.


Employees engaged in JPBank SOC duties