Japan Post Group Cyber Security Measures

In response to the constantly increasing advancement and sophistication of cyber attacks, the Japan Post Group has recognized the threat of cyber attacks as a serious risk, and has developed a system to deal with cyber attacks.

We are working to safeguard and manage important information from damage such as information leaks and loss caused by cyber attacks.
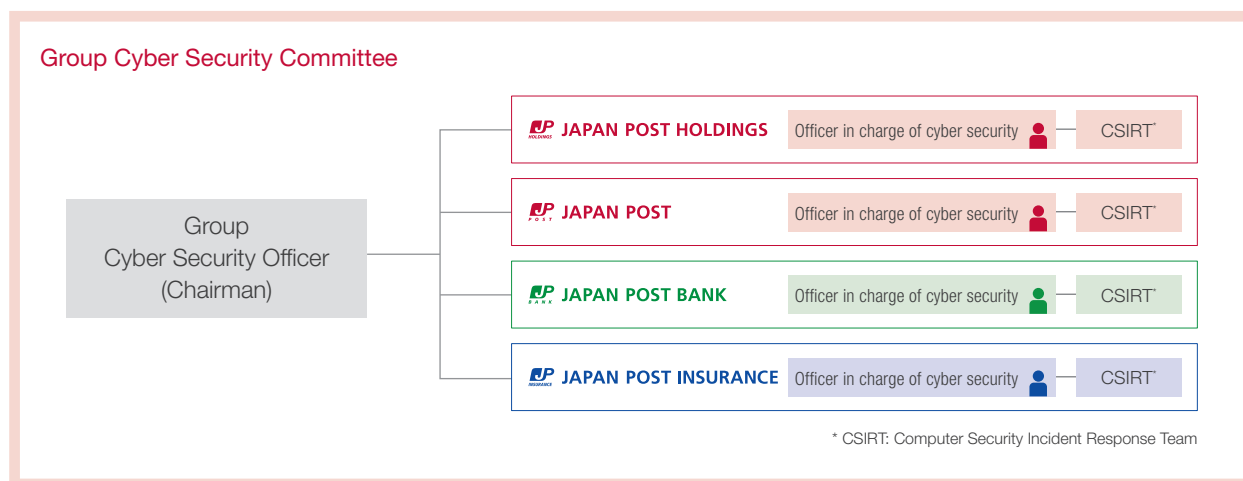
Group Cyber Security System

Under governance of the holding company Japan Post Holdings Co., Ltd., we have developed a cyber security management system for the Japan Post Group.

We have established a Group Cyber Security Committee consisting of executives in charge of cyber security from the four main Group companies of the Japan Post Group. This committee develops Group cyber security strategy, and works to track and evaluate the status of cyber security measures in Group companies.

In our system, executives in charge of cyber security at Japan Post Holdings oversee Group governance related to cyber security. They regularly report on the status of cyber security efforts to management.

Group Cyber Security Committee

Group Cyber Security Officer (Chairman)	**JAPAN POST HOLDINGS** — Officer in charge of cyber security	CSIRT*
	JAPAN POST — Officer in charge of cyber security	CSIRT*
	JAPAN POST BANK — Officer in charge of cyber security	CSIRT*
	JAPAN POST INSURANCE — Officer in charge of cyber security	CSIRT*

* CSIRT: Computer Security Incident Response Team

Efforts for Cyber Security Measures by Japan Post Holdings

Defense in depth	In order to reduce the risk of malware attacks from outside the Company and unauthorized transfer of information from inside the Company, we have introduced multiple detection and defense mechanisms against unauthorized access and unauthorized programs, and are implementing multi-level countermeasures (defense in depth). The effectiveness of defense is regularly evaluated by a third party.
Incident response system	We have developed an incident response system centered on CSIRT, so that when a cyber attack occurs, we can quickly find the cause and minimize the damage, and at the same time report it to management quickly. We are conducting response training for security incidents on a regular basis, and checking whether our incident response system is functioning effectively, while also working to improve the incident response capabilities of CSIRT staff and other employees.
Education / Training	We conduct cyber security education and training for executives and employees, and are working to improve security awareness among executives and employees.
External collaboration	We collaborate with external organizations such as JPCERT / CC, the Nippon CSIRT Association and the Tokyo Metropolitan Police Department in order to share attack information and countermeasure trends, and strive to respond quickly to increasingly sophisticated cyber attacks.

JP Vision 2025

Value Creation Strategy

Sustainability

Corporate Governance

Data Compilation