Countering Cyber-attacks

Cyber-attacks pose especially significant security risks to Toppan. The Group has been implementing various measures to mitigate them.

■ Installing an EDR Application on PCs across the Group

In 2019 Toppan began installing Endpoint Detection and Response (EDR), an application that detects suspicious behaviors in PCs. The application is now installed in all PCs used for administrative work across the Group. The next step will be to install the EDR application on terminals used onsite in production settings, as well as on Apple computers and network servers. Toppan will continue to strengthen the Group's system for detecting and responding to sophisticated malware.

■ Adopting a CASB Service to Mitigate Cloud-usage Risks

The growing usage of cloud services is driving up the amount of important information handled by cloud-based applications. The Toppan Group has adopted a Cloud Access Security Broker (CASB) service that visualizes and controls computer usage in cloud environments. Toppan is using the CASB service to enhance the safety of cloud-service usage by identifying risks associated with individual cloud services and detecting uses of the cloud that are subject to unduly high risk.

■ Instituting Threat Intelligence and OSINT Activities

The Toppan Group has implemented threat intelligence to uncover signs of cyber-attacks early on. The Group has also begun Open Source INTellignce (OSINT) activities to detect vulnerabilities visible to outside parties and implement preemptive security measures before an attack occurs. Toppan will continue using the OSINT techniques to reinforce cyber security across the Group.

■ Upgrading Website Vulnerability Assessments

Toppan has been internally assessing weaknesses in the Group's web applications to counter cyber-attacks targeting website vulnerabilities. The Group has also developed an in-house network diagnosis (platform diagnosis) system to detect vulnerabilities with operating systems and other software. With this system, Toppan is now capable of internally assessing server vulnerabilities at every level to promise customers more tightly secured services.