Overview of NTTDATA-CERT 's activities

NTTDATA-CERT engages in the following six activities.

During normal times, we prevent incidents from occurring, If an incident occurs, we will detect it early and implement a quick and accurate emergency response.

Building incident prevention, early detection, and response systems based on cyber attack trends and risk analysis. Strengthening and monitoring cybersecurity measures. Strengthening measures against "I, External cyber attacks" and "II, Malware infections and information leaks, including internal improprieties" Normal Rule development / educational training. Incident monitoring. times Policy formulation/promotion. Attack monitoring, log analysis. Management of response procedures. Information collection / dissemination. External cooperation/PR. Vulnerability information collection and dissemination. Collaboration within the NTT Group. Internal and external IoC collection and transmission using MISP. seminars held.



Emer gency Minimize security damage through early response, speedy recovery, and thorough measures to prevent recurrence.

6 Incident response.



Cause analysis.

Preservation of evidence. Understanding the damage situation, etc.

Damage minimization.

Emergency shutdown of various equipment.
Confirming the scope of influence, etc.

Restoration.

Setting changes and equipment updates.
Deletion of leaked data, etc.

Preventive measure.

Implementation and deployment of recurrence. prevention measures.