The Cybersecurity Policy for CIP (4th Edition)

April 18, 2017 Published
July 25, 2018, and January 30, 2020 Revised

1. Purpose of the Cybersecurity Policy for CIP (4th Edition) ("this Cybersecurity Policy")

◆ Promotion of activities for reduction of Critical Infrastructure Services (CISs) outage risk resulting from cyberattacks, natural disasters, etc. and ensuring resilience in order to provide CISs safely and continuously, based on active involvement of top management (Mission Assurance)

◆ Essential services for organizing the Olympic and Paralympic games shall be secured.

2. Challenges

◆ CI operators are gradually coming to take on voluntary activities, and still have some challenges on Check & Act in the PDCA cycle

◆ Improve information sharing not only IT but also OT (Operational Technology) and promote incident readiness

◆ Continue and improve provision of information to the nation through analysis and cooperation with various entities all over the world

3. Policy Priorities

(1) Promotion of Leading Activities (Classification)

■ Enforcing and improving the leading activities of some sectors (such as Electric power supply, Information & Communication and Financial services), which are highly depended upon by other CISs and cause a big impact on society in the case of outages

■ Encouraging other CI operators by expanding the leading activities

(2) Enhancement of Information Sharing System toward the Olympic and Paralympic Games

■ Considering introduction of the severity schema on CISs outages

■ Breaking the barrier of information sharing by diversifying the contact formation (Anonymization, sharing via the CEPTOAR* Secretariat, Cybersecurity related agencies) Study of gathering cross-sectoral information into the cabinet secretariat

*Capability for Engineering of Protection, Technical Operation, Analysis and Response

■ Development of information sharing system utilizing the hotline (Automation, Work saving, Expediting, Ensuring)

■ Clarification of the scope of information sharing and provision including the OT, IoT, etc.

■ Maintenance and improvement of CIP capability by improvement of exercises and penetration of the results

■ Expanding the protection scope as "protection as plane" including the supply chain

(3) Promotion of Incident Readiness Based on Risk Management

■ Dissemination of risk assessment by providing "the risk assessment guideline for mission assurance" and workshops

■ Promotion of incident readiness of CI operators by establishing BCPs and contingency plans

■ Enhancing the monitoring and review by providing the perspective of internal audit in risk management and incident readiness

4. Duration

◆ The 4th Edition will cover until the end of the Olympic and Paralympic games, and will be revised even within the period as necessary.