Cybersecurity Policy for CIP (4th Edition) (April 2017, Revised July 2018)

Promoting CIP through public-private partnership

On the basis of the concept of mission assurance, in order to safely and continuously provide critical infrastructure services(CISs) and to avoid serious effects on the national life and socioeconomic activities from CISs outages resulting from cyber-attacks, natural disasters or other causes, all stakeholders should protect the critical infrastructures by reducing the occurrence of CISs outages as much as possible and by ensuring prompt recovery from outages.

Critical Infrastructures (14 sectors)

- Info. & comm.
- Finance
- Aviation
- Airport
- Railway
- Electric power supply
- Gas supply
- Gov. & admin. (incl. municipal government)
- Medical
- Water
- Logistics
- Chemical industries
- Credit card
- Petroleum industries

【NISC】 coordination & cooperation

Responsible ministries for critical infrastructure (5 ministries)

- FSA [Financial]
- MIC [Info & comm, Admin]
- MHLW [Medical, Water]
- METI [Electric power supply, Gas, Chemical, Credit card, Petroleum]
- MLIT [Aviation, Airport, Railway, Logistics]

Organizations concerned

- Cybersecurity related ministries [MIC, METI, etc.]
- Crisis management ministries [NPA, MOD, etc.]
- Disaster prevention related ministries [CAO, ministries, etc.]
- Cybersecurity related agencies [NICT, IPA, JPCERT, etc.]
- Cyberspace-related operators [Various vendors, etc.]

This Cybersecurity Policy

Maintenance and promotion of the safety principles

Promoting continual improvement of the "guidelines" of measures that are most necessary from a cross-sectoral perspective, and the "safety principles" in each sector.

Enhancement of information sharing system

Enhancing the public-private and cross-sectoral information sharing system by diversifying the contact formation, defining the sharing of information, etc.

Enhancement of incident response capability

Enhancing the overall CISs outages response system by the implementation of exercises and collaboration between exercises and trainings, etc. performed under public-private partnership

Risk management and preparation of incident readiness

Promoting comprehensive management including preparation of incident readiness such as risk assessment, establishment of contingency plans by CI operators, etc.

Enhancement of the basis for CIP

Review of the protection scope, promoting the public relations activities and international cooperation, appeal to top management, promotion of developing human resources