Cybersecurity Policy for CIP (4th Edition)

(Adopted April 2018)
(Revised July 2018)

1. Points of Revision

◆ Mission Assurance: Promotion of actions to reduce risks of critical infrastructures' service outage caused by natural disasters, cyber-attacks, etc. and ensuring resilience in order to provide CI services safely and continuously, based on active and firm commitment of management executives.

◆ Envisioning Tokyo 2020: Essential services for organizing the Olympic and Paralympic games shall be secured.

2. Challenges

◆ CI operators are taking measures, but still have some challenges on Check & Action in 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)

- Enhancing activities of leading sectors (such as electric power supply, information & communication services, and financial services), which other CI services highly depend on.
- Encouraging other CI operators to follow such leading activities for cybersecurity.

(2) Enhancement of Information Sharing Structure beyond the Olympic and Paralympic Games

- Introducing severity scale for CI service outages.
- Diversifying communication modality and channels (anonymization, sharing thru CEPTOAR* Secretariat and/or CIP supporting agencies) and breaking the barrier of information sharing; studying how to gather cross-sectoral information to the Cabinet Secretariat.
  *Capability for Engineering of Protection, Technical Operation, Analysis and Response
- Developing information sharing system for automated, labor-saving, swift and reliable operation (also envisioning to use it as hotline among stakeholders).
- Including OT, IoT, etc. in the scope of information sharing.
- Enhancing CIP by exercises and penetration tests.
- Expanding the protection scope as "cross-cutting sector-wide" including supply chain.

(3) Promotion of Incident Readiness Based on Risk Management

- Improving risk assessment in CI operators by providing NISC's "risk assessment guideline for mission assurance" and workshops.
- Promoting incident readiness of CI operators including BCP and contingency plan.
- Encouraging CI operators to conduct cybersecurity internal audit including monitoring and review, referring to NISC's risk assessment guideline.

4. Duration

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