
- The need for protecting systems at the national level was raised since informatization of national critical infrastructures (e.g., IT, energy, logistics, finance, etc.) is in progress and those are interlinked by network

- Enacted on January 26, 2001 for the purpose of protecting critical IT infrastructures. It includes the definition of CIIP, role of administrative agency concerned, etc.
1. **CIIP (Critical Information Infrastructure Protection) Law (2/3)**

### Regulations (1/2)

- **The Committee on the CIIP**
  - The main committee on CIIP is Prime Minister's Office.
  - It includes the definition of CIIP, role of administrative agency concerned, etc.

- **Designation of CII**
  - Committee designate CII based on 5 criteria.

- **Vulnerability analysis and evaluation**
  - The head of the infrastructure management organization should perform vulnerability analysis and evaluation on the facility under its jurisdiction.
  - Establish and implement protection measures for the facility.
  - The head of central administrative agency concerned should make a protection plan.

- **Technical support**
  - The technical support for CII can be requested to the national institute or professional security consulting company according to the Presidential decree.
1. **CIIP (Critical Information Infrastructure Protection) Law (3/3)**

**Regulations (2/2)**

- **Response process in case of invasion**
  - When the CII is disrupted, paralyzed, or broke downed due to cyber attacks, the head of the organization that manages CII should notify that to the central administrative agency concerned.
  - The head of the organization should also apply countermeasures to recover damages and prevent spread following damages.

- **Punishment**
  - Those who disrupt, paralyze, or destroy CII with electronic infringement behavior such as hacking and distributing computer virus can be imprisoned for a maximum of ten years and fined one hundred million won.
2. Structure & Procedure - Structure

**Structure**

Committee on Protection of Information and Communications Infrastructure

- Ministry of Science, ICT and Future Planning: Support for private area
- Prime Minister’s Office: Prime Minister (Chairman)
- NIS: Support for public area

Central administrative agencies:

- ICT(78)
- E-Government(98)
- Banking(56)
- Energy(46)
- Health(14)
- Transportation(18)
- etc.(75)
2. Structure & Procedure – Designation

- Significant impact on national, economic, and social security
- Minister designates CII that is deliberated in the Committee
- Based on 5 criteria

- National and social importance of duties (managing the relevant information and communication infrastructure)
- Dependence on information and communication infrastructure
- Inter-connection with other Information and Communication Infrastructure
- Scale and scope of damage caused by incidents
- Probability of intrusion incidents and easiness of recovery
2. Structure & Procedure – Vulnerability analysis/Evaluation

- When designated as CII for the first time, vulnerability analysis/evaluation should be conducted within 6 months
- Annually, vulnerability analysis and evaluation should be conducted

- Phase 1: Establishing the vulnerability analysis/evaluation plan
- Phase 2: Selecting the vulnerability analysis/evaluation targets
- Phase 3: Performing vulnerability analysis
- Phase 4: Performing vulnerability evaluation

☑ Conducted by management agencies
☑ 4 steps for vulnerability analysis and evaluation
2. Structure & Procedure – Protection measures & plan

- Management organization shall implement security management measures base on the results of the vulnerability analysis/evaluation
- CII protection plan is managed by the central administrative agency concerned
- CIIP Committee publishes guideline for establishing protection plan

- ✓ Implement security management countermeasures to protect CII
- ✓ Establish protection plans based on the guideline from CIIP committee
2. Structure and Procedure – Annual Procedure

CIIP protection activities on an annual basis

- **Central administrative agency concerned**
  - Analysis and Improvement:
    - Analyzing the results
    - Establishing improvement plan
  - Performance check:
    - Checking a performance of protection tasks
    - Recommending implementation of unperformed task

- **Management Agency**
  - Making cyber security plan:
    - Performing vulnerability analysis and evaluation
    - Making protection plan
  - Implementing protection measures:
    - Eliminating vulnerabilities
    - Carrying out protection tasks
The Response system in case of security incident

Committee on Protection of Information and Communications Infrastructure
(Chairman: Minister of the Office for Government Policy Coordination)

Appoint the head of the Response Center

Information Infrastructure Security Incident Response Center
(established upon the occurrence of a critical incident)

MSIT

NIS

- Professional security service company
- ISAC (Information Sharing and Analysis Centers)
- National security research institute

Management organization

1. Security incident notification
2. Quick response to prevent damage spread
3. Request recovery and protection support
4. Cooperation and support

central administrative agencies concerned
- Supporting recovery-related technologies

Investigative agency
- Supporting recovery-related technologies

KISA
- Supporting recovery-related technologies

- Professional security service company
- ISAC (Information Sharing and Analysis Centers)
- National security research institute
Thank you.