The CIIP in Korea

Dec 2017

Kim, Mideum

Researcher

Critical Infrastructure Protection Team

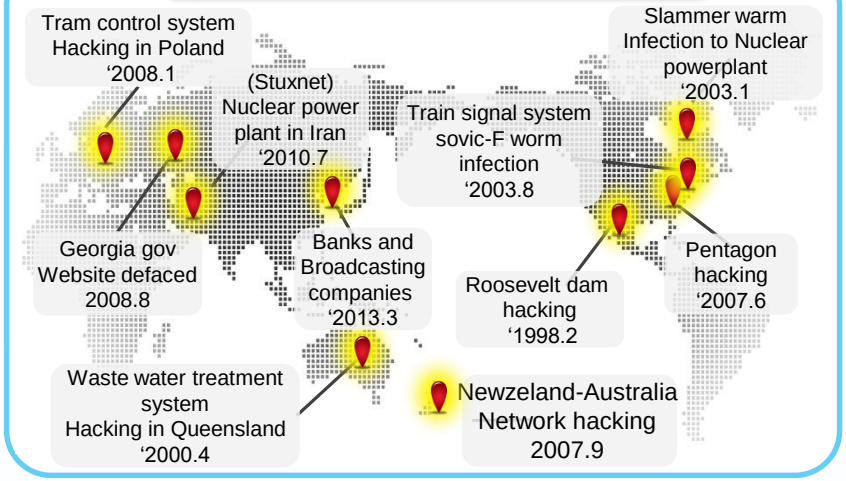
Contents

I Growing importance of CIIP

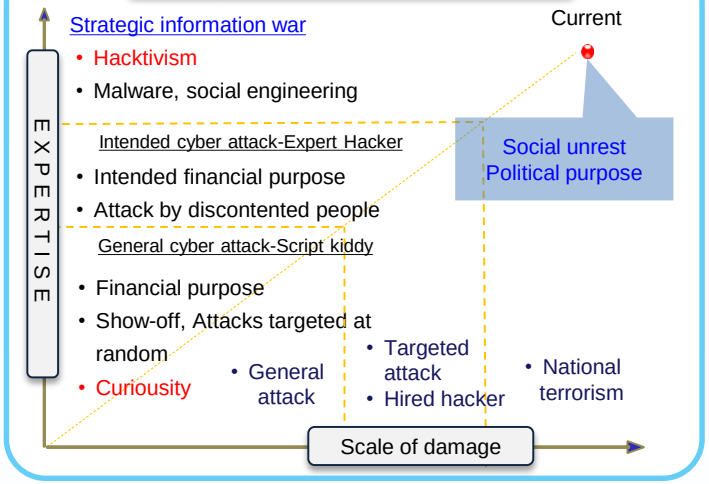
Trends of Cyber Threat

Increasing damages by cyber attacks pursuing political/social chaos

Incident cases over the world



Cyber attack trends



Increasing financial damages

- The economic loss due to cybercrime amounts to $400 billion annually
- Up to $2 trillion in damages by 2019 (a report from Washington Trade Center)

Incidents of Cyber Attack

Incidents of cyber attack in CIIP

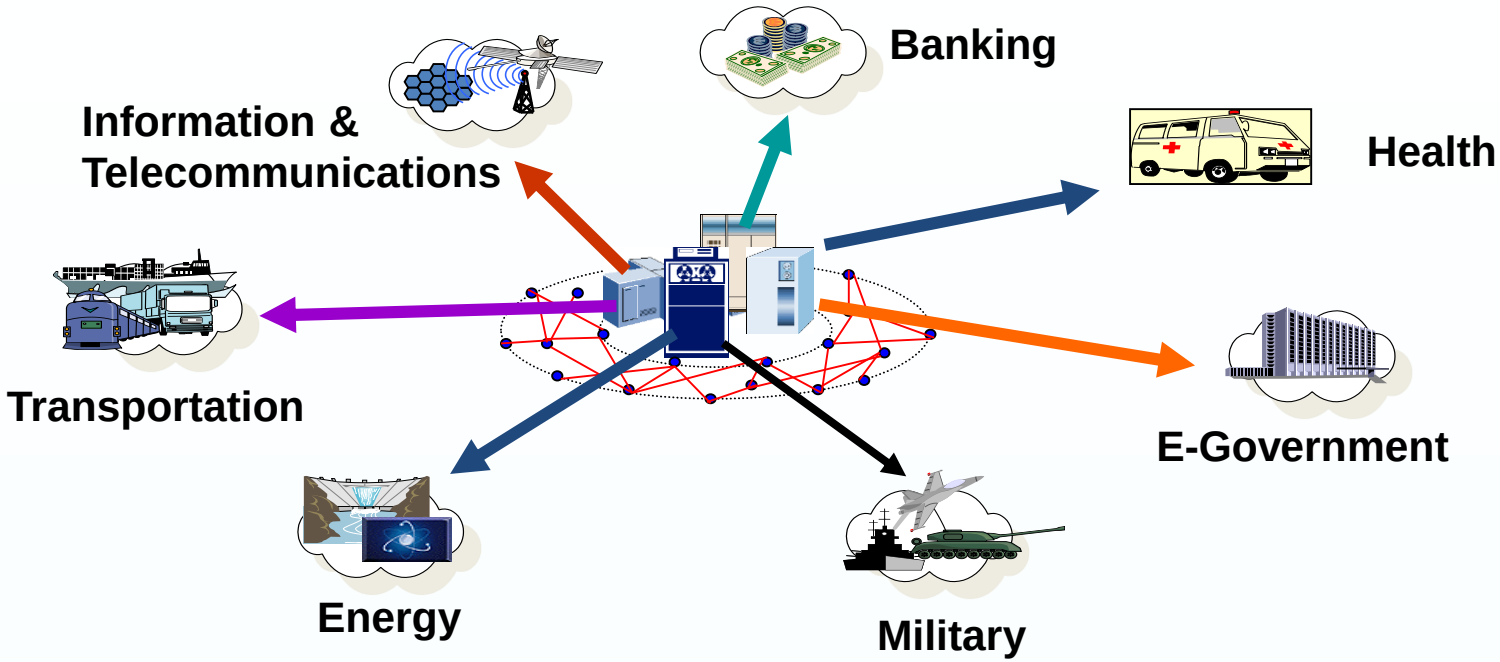
- **Spreading WannaCry Ransomware around the world (2017. 5)**
  - Infected more than 12 million computers in 99 countries around the world
  - Infected with SMB remote code execution vulnerability in Windows OS
- **Bangladesh Central Bank Hacking (2016. 2)**
  - $ 81 million disappeared from bank account in Bangladesh
  - Exploiting Vulnerabilities in SWIFT and Bangladesh banking links
- **Ukraine Massive Blackout (2015. 12)**
  - For about 3 hours, 8 million households outage
  - Attacker uses an Excel file containing ‘Black Energy’ malware

Threat against Critical Infrastructure

CI getting attractive to attackers

- The more dependent the society is on the IT, the more vulnerable it is
  - As technology has developed, social infrastructures rely on ICT services and the network. It make it possible for them to provide convenient and more accessible service.
  - Meanwhile, it make a path for attackers to invade the systems through the network.

- Through CI, hackers want to manipulate essential services that effect people



Systematic protection for CI needed

Ripple effects when CII is compromised

- Risk of failure and breakdown of communication infrastructure system
  - Isolation of entire society due to communication failure
  - Social confusion due to the lack of reliability of information
- National productivity is damaged in relation to energy and power incident (loss of competitiveness)
  - Deficient supply of fuel for plants and energy resources for household
  - Environmental damage and injury due to a radiation leak accident
- Electronic violation of traffic, aviation, and marine transportation information system
  - Disruption of aircraft operation, possibility of aircraft collision, and paralysis of the traffic system
  - Communication failure of the traffic management system or system failure
- Increased possibility of vulnerability occurring due to the computerization of public business, such as administration, education, and healthcare
  - Social chaos such as national administration paralysis and extensive personal information leak

Ⅱ CIIP polices in Korea

What is Critical Information Infrastructure?

Definition of CIIP

Information Infrastructure refers to

- **electronic control and management system** related to the national security, administration, defense, public security, finance, communications, transportation, energy, etc. and information and communications network under Article 2 (1) 1 of the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.
- CII is different from CI, that is **critical infrastructure**. It is the terms includes protection against physical attacks to CI, that is a concept for general defense not only for cybersecurity

CIIP refers to

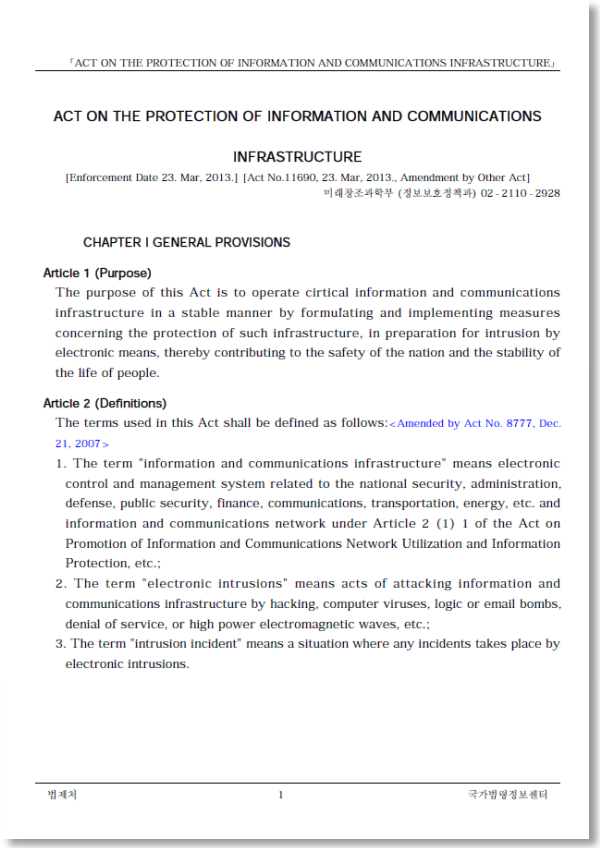
- Activities aimed at protecting critical information infrastructure related to communication, finance, military, and energy areas from various cyber attacks

CIIP is implemented

- With national scales, such as an enactment of related law, identification of actors' roles, imposition of responsibilities and etc.

Critical Information Infrastructure Protection Law

Enactment of the Critical Information Protection(CIIP) Law



「ACT ON THE PROTECTION OF INFORMATION AND COMMUNICATIONS INFRASTRUCTURE」

ACT ON THE PROTECTION OF INFORMATION AND COMMUNICATIONS INFRASTRUCTURE

[Enforcement Date 23. Mar, 2013.] [Act No.11690, 23. Mar, 2013., Amendment by Other Act]
미래창조과학부 (정보보호정책과) 02-2110-2928

CHAPTER I GENERAL PROVISIONS

Article 1 (Purpose)

The purpose of this Act is to operate cirtical information and communications infrastructure in a stable manner by formulating and implementing measures concerning the protection of such infrastructure, in preparation for intrusion by electronic means, thereby contributing to the safety of the nation and the stability of the life of people.

Article 2 (Definitions)

The terms used in this Act shall be defined as follows:<Amended by Act No. 8777, Dec. 21, 2007>

1. The term "information and communications infrastructure" means electronic control and management system related to the national security, administration, defense, public security, finance, communications, transportation, energy, etc. and information and communications network under Article 2 (1) 1 of the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.;
2. The term "electronic intrusions" means acts of attacking information and communications infrastructure by hacking, computer viruses, logic or email bombs, denial of service, or high power electromagnetic waves, etc.;
3. The term "intrusion incident" means a situation where any incidents takes place by electronic intrusions.

법제처 1 국가법령정보센터

- The need for a protection system at the national level was raised since national critical infrastructures (e.g., IT, energy, logistics, finance, etc.) are interlinked by information and communication, forming an interdependent structure with the advancement of informatization

- enacted on January 26, 2001 for the purpose of protecting critical IT infrastructures
- Includes the definition of CIIP, role of related institutions and responsibilities

Critical Information Infrastructure Protection Law

What the CIIP Law stipulates

- **The Committee on the CIIP**
  - The Committee on the Information Infrastructure Protection (CIIP) attached to the Prime Minister's Office should be established (Article 3)
  - Includes the definition of CIIP, role of related institutions and responsibilities
- **Designation of CII**
  - Includes the definition of CIIP, role of related institutions and responsibilities
- **Vulnerability analysis and evaluation**
  - The head of the infrastructure management organization should perform vulnerability analysis and evaluation on the facility under its jurisdiction and establish and implement protection measures for the facility. The head of the central administrative organization should establish and implement the protection plan for critical information infrastructures (CII) by area of jurisdiction (Articles 5 and 6)
- **Technical support**
  - Technical support for CII can be requested to the head of the national institute or specialist institute according to the Presidential decree (Article 7)

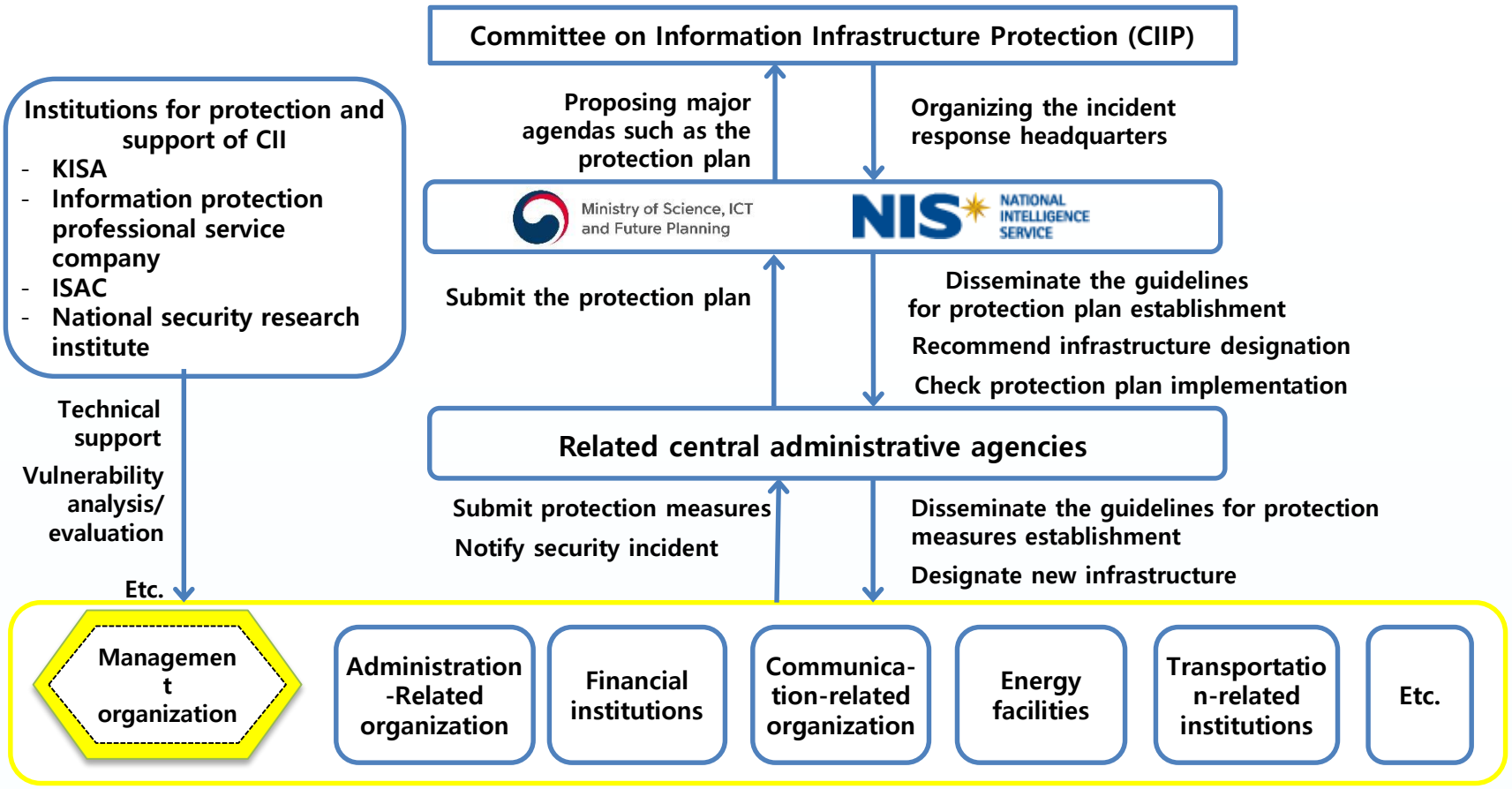
Critical Information Infrastructure Protection Law

What the CIIP Law stipulates

- Taken measures in case of invasion
  - The head of the organization that manages a CII should notify the related organization of the disruption, paralysis, or breakdown of the facility under its jurisdiction due to a security incident upon discovery of such. The head of the organization should also take measures for recovery following damage and prevent the spread of damage (Articles 13, 14)
- Punishment
  - Those who disrupted, paralyzed, or destroyed CII with electronic infringement behavior such as hacking and computer virus can be imprisoned for a maximum of ten years and fined one hundred million won (Article 28)

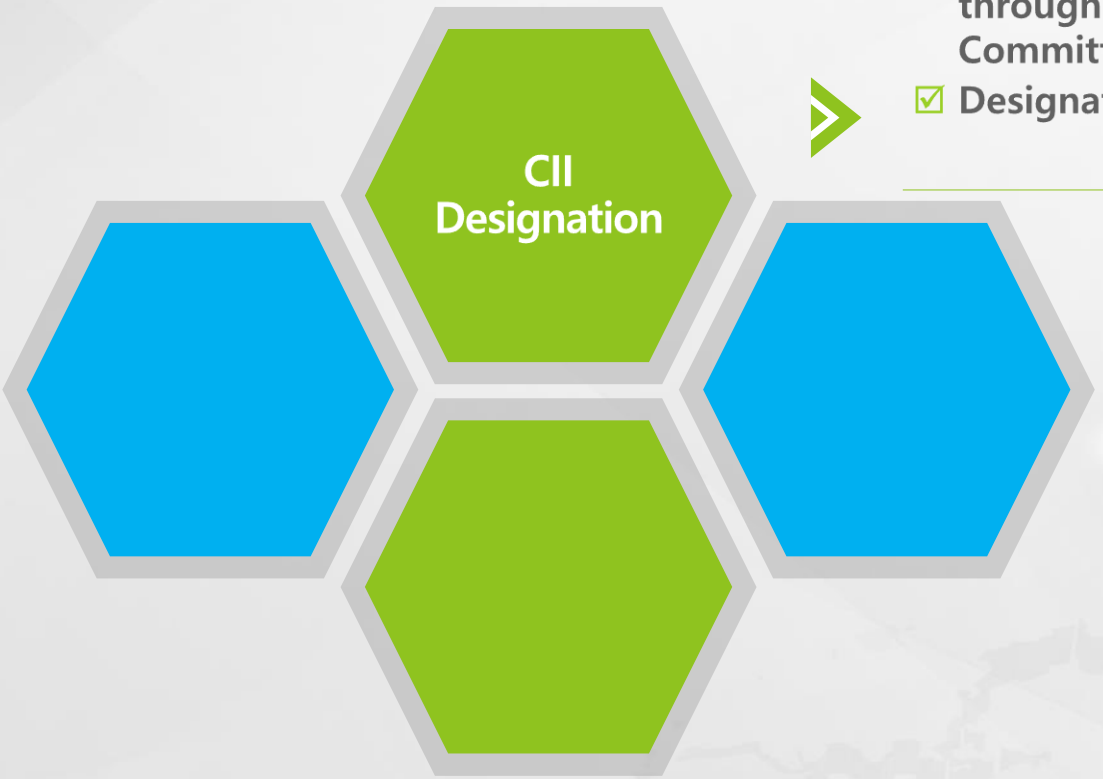
CII Protection System

Work structure in accordance with the CIIP Law



III CIIP system in Korea

CII Protection System



- ☑ Significant Impact on National, Economic, and Social Security
- ☑ Designated by Ministers through deliberation by the Committee
- ☑ Designated with 5 criteria

CII Designation

Designation of CII

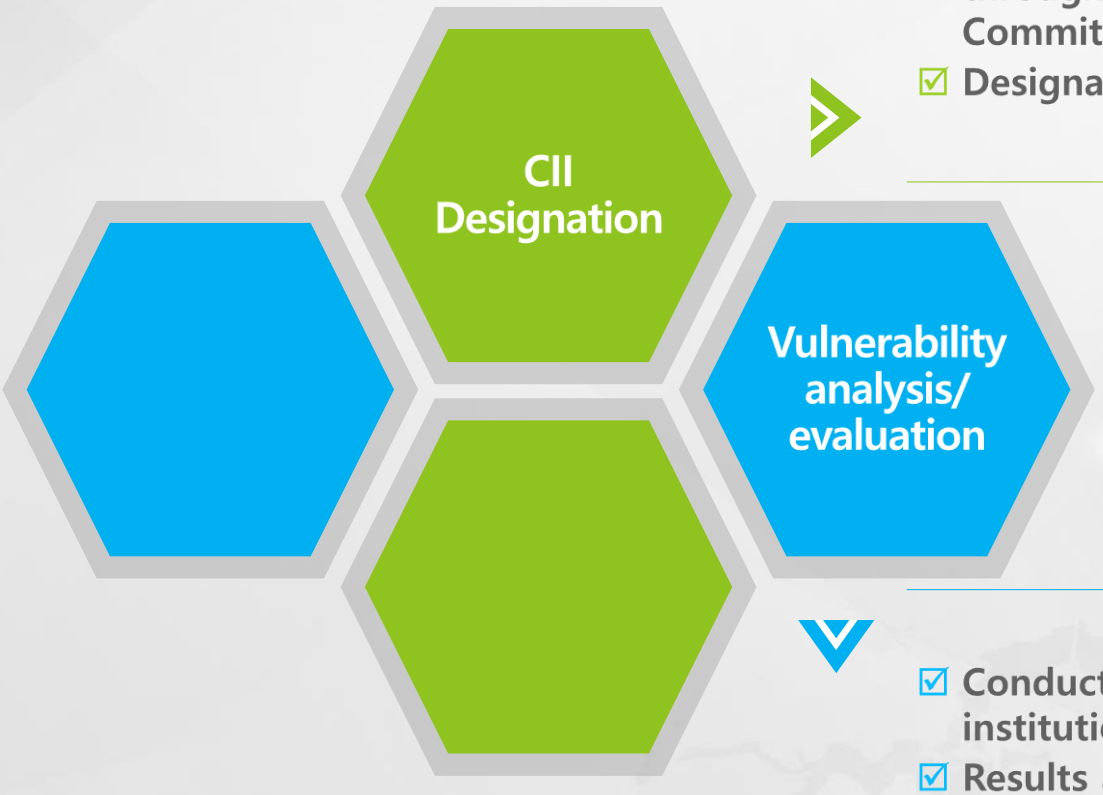
Critical Information Infrastructure(CII)

- Has Significant Impact on National, Economic, and Social Security
- Designated by Ministers through Deliberation by the Committee on the Protection of Information Infrastructure

Designation Criteria

- The national and social importance of duties by an organization which the manages the relevant information and communications infrastructure
- The dependence of affairs conducted by an organization which the manages the relevant information and communications infrastructure
- The inter-connection with with other Information and Communications Infrastructure
- The Areas and extent of damage caused by incidents to the national security , economy and society. If any.
- Probability of intrusion incidents and the easiness of restoration thereof

CII Protection System



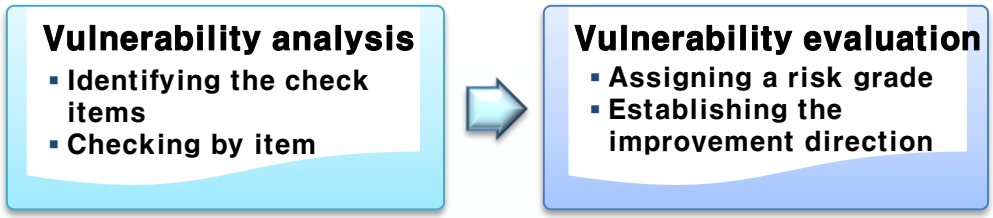
- ☑ Designated by Ministers through deliberation by the Committee
- ☑ Designated with 5 criteria

- ☑ Conducted by authorized institutions
- ☑ Results and measurement plans are managed

Vulnerability analysis and evaluation

Overview of Vulnerability analysis and evaluation

- A series of processes that analyze, evaluate, and improve CII's vulnerabilities comprehensively with regard to cyber threats such as malicious code dissemination and hacking



- Institutions allowed to analyze and evaluate vulnerability
  - Internal dedicated team if conducted by the management agency of CII
  - Conducted by a specialist institute such as a company specializing in knowledge information security consulting if the management agency outsources to an outside organization
  - Specialist institute, KISA, information sharing/analysis center, ETRI, company specializing in knowledge information security consulting

Vulnerability analysis and evaluation

Overview of Vulnerability analysis and evaluation

Implementation interval

- When designated as CII for the first time, vulnerability analysis/evaluation should be conducted within 6 months of designation
- Conducting vulnerability analysis and evaluation regularly (every year)

Scope and item of vulnerability analysis and evaluation

- Information system asset, control system asset, medical system asset, and others defined as a detailed facility of CII
- If there is another system linked with CII, the influence of the linked system on the infrastructure is also included.
- The basic item of vulnerability analysis/evaluation can be classified into ① administrative, ② physical, and ③ technical items

Vulnerability analysis and evaluation

The Procedure of Vulnerability analysis and evaluation

- 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

– Phase 1: Detailed plan for vulnerability analysis/evaluation, such as implementation subject (internal or outsourcing), implementation interval (regular/when necessary), implementation procedure, required budget, deliverables, etc.

– Phase 2: Identifying the asset such as IT asset of the infrastructure, asset of the control system, and medical equipment; grouping those assets by type; creating a list of vulnerability analysis/evaluation targets; and estimating the importance of each asset

– Phase 3: Creating a detailed administrative/physical/technical checklist for vulnerability analysis/evaluation

– Phase 4: Describing the details of check results and marking the risk level

CII Protection System

☑ Designated by Ministers through deliberation by the Committee
☑ Designated with 5 criteria

☑ Conducted by authorized institutions
☑ Results and measurement plans are managed

☑ Management measures to protect CII
☑ Plans to protect CII, summarizing protection measures

Establishing the protection measures & plan

Establishment of Measures and plan for CIIP

Establishment of Measures to Protect Critical Information and Communications Infrastructure

- The head of an organization which manages critical information and communications infrastructure (hereinafter referred to as a "management organization") shall formulate and implement management measures (hereinafter referred to as "measures to protect critical information and communications infrastructure"), including physical and technological measures to protect critical information and communications infrastructure under its his/her jurisdiction in a safe manner, depending on the results outcomes of the analysis and evaluation of vulnerabilities under Article 9 (1)

Establishment of Plans for Protecting Critical Information and Communications Infrastructure

- Establishing and implementing the CII protection plan for the responsible area by summarizing/adjusting the received protection measures under the management of the head of the related central administrative agency
- Disseminating the guidelines for setting up the protection plan and establishing the protection plan by accepting the protection plan by ministry and office

CII Protection System

- ☑ Incident notification and investigation
- ☑ Recovery support and cooperation
- ☑ Measures to prevent recurrence

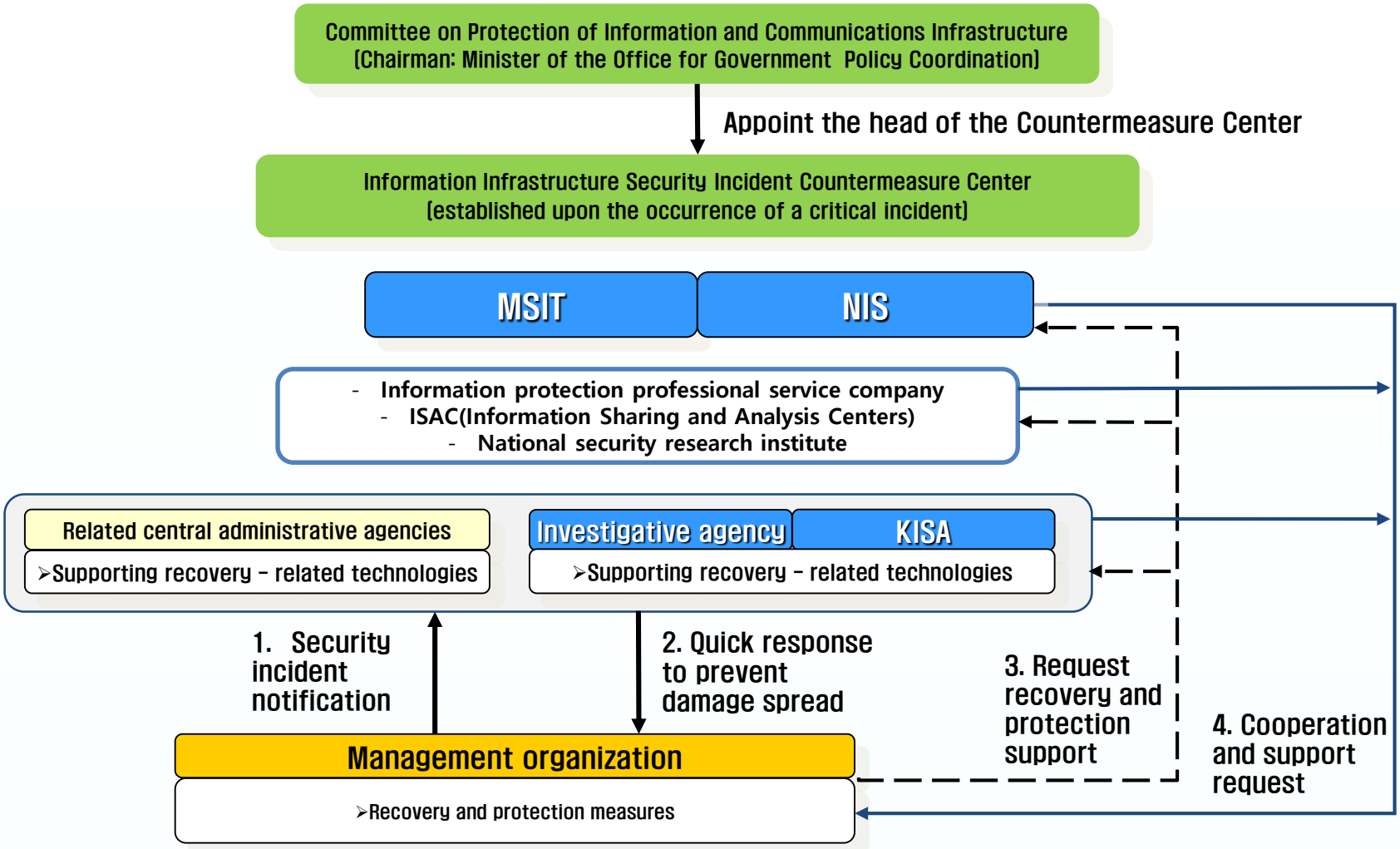
- ☑ Designated by Ministers through deliberation by the Committee
- ☑ Designated with 5 criteria

- ☑ Management measures to protect CII
- ☑ Plans to protect CII, summarizing protection measures

- ☑ Conducted by authorized institutions
- ☑ Results and measurement plans are managed

CII Protection Policy

The Response system in case of security incident



Internet On, Security In!

Thank you.

Q & A

Kim, Mideum

belief1171@kisa.or.kr