Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.34, NO.2, Apr. 2024 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2024.34.2.347

수정된 정책모형이론에 기반한 국가정보통신기반시설 보호정책 추진체계 분석

유 지 연†‡
상명대학교 (교수)

Analysis of National Critical Information Infrastructure (NCII) Protection Policy Promotion System Based on Modified Policy Model Theory

Ji-yeon Yoo†‡
Sangmyung University (Professor)

요 약

국가정보통신기반시설을 대상으로 하는 사이버공격이 꾸준히 증가함에 따라, 많은 국가들이 관련 정책 및 법제도의 제정과 개정을 통해 국가정보통신기반시설의 보호를 강화하고 있다. 이에 본고는 국가정보통신기반시설 보호체계를 구축하고 있는 미국, 영국, 일본, 독일, 호주 등의 국가를 선정하여, 국가별 국가정보통신기반시설 보호정책의 추진체계를 비교·분석하고자 한다. 국가정보통신기반시설 보호체계를 사이버보안 체계와 비교하고 추진 구조를 분석하고 앨리슨 이론(Allison's theory)과 나카무라&스몰우드 이론(Nakamura & Smallwood's theory)을 수정한 정책모형이론에 근거하여 정책결정과 정책집행의 관점에서 국가별 추진체계모형을 분석하였다. 미국, 일본, 독일, 호주의 정책추진 모형은 정책결정과 정책집행이 모두 국가정보통신기반시설 보호 중심으로 체계화된 체계강화모형이며, 영국, 한국의 정책추진 모형은 보다 정책집행에 초점이 맞춰진 집행중심모형으로 나타났다.

ABSTRACT

As the number of cyberattacks against the National Critical Information Infrastructure (NCII) is steadily increasing, many countries are strengthening the protection of National Critical Information Infrastructure (NCII) through the enactment and revision of related policies and legal systems. Therefore, this paper selects countries such as the United States, the United Kingdom, Japan, Germany, and Australia, which have established National Critical Information Infrastructure (NCII) protection systems, and compares and analyzes the promotion system of each country's National Critical Information Infrastructure (NCII) protection policy. This paper compares the National Critical Information Infrastructure (NCII) protection system of each country with the cybersecurity system and analyzes the promotion structure. Based on the policy model theory, which is a modification of Allison's theory and Nakamura & Smallwood's theory, this paper analyzes the model of each country's promotion system from the perspective of policy-making and policy-execution. The United States, Japan, Germany, and Australia's policy-promotion model is a system-strengthening model in which both policy-making and policy-execution are organized around the protection of the National Critical Information Infrastructure (NCII), while the United Kingdom and South Korea's policy-promotion model is an execution-oriented model that focuses more on policy-execution.

Keywords: National Critical Information Infrastructure(NCII), Cybersecurity, Policy Promotion System

Received(02. 01. 2024), Modified(02. 28. 2024), Accepted(03. 20. 2024)

† 주저자, yooo@smu.ac.kr
‡ 교신저자, yooo@smu.ac.kr(Corresponding author)

I. 서 론

지능정보기술의 발달로 우리의 일상이 사이버공간으로 확장되면서 전반적인 사이버 위험 또한 증가하였다. 이는 사이버 공격으로 인한 평균 지출 금액이 급격하게 증가한 사실로 확인할 수 있다. 사이버범죄 피해 비용이 2015년 전 세계 3조 달러의 규모였으나 매년 15%씩 증가하여 2023년에는 약 8조 달러에 달하였으며 2025년에는 약 10조 5천억 달러에 이를 것으로 나타난다[1].

동시에 국가정보통신기반시설[1]을 대상으로 하는 사이버공격 또한 증가하였다. 사이버공격으로 인해 국가정보통신기반시설의 중단이 발생하는 경우 그 영향이 사회·경제 전반적인 차원에서 나타나며, 개인 및 기업의 손익과 함께 국가의 존속에 대한 문제로 이어질 위험이 있다. 이에 주요국은 국가정보통신기반시설의 보호를 강화하는 방향으로 조직체계를 강화하고 법률과 정책을 제·개정하고 있다.

본고는 미국, 영국, 일본, 독일, 호주 등 국가별 국가정보통신기반시설 보호를 위한 전략 및 정책의 추진체계를 비교·분석하여 현재 우리나라의 국가정보통신기반시설 보호 수준을 파악하고, 관련 역량의 강화를 위한 방안을 모색하고자 한다.

II. 선행연구

2.1 선행연구

본고는 국가정보통신기반시설의 사이버보안 추진 및 보호를 위한 체계와 이를 위해 국가별 설치 및 운영하는 조직의 현황을 파악하고 개선점을 도출하고자 한다. 이와 관련한 연구로는 국내 연구로는 국가별 사이버안보 조직체계[2], 국가정보통신기반시설 보호체계 수준 비교[3]가 진행된 바 있으나 국가정보통신기반시설 보호와 관련한 연구는 거의 없다. 국외 연구로는 사이버보안 정책 분석 또는 국가에 대한 조직 분석 관련 연구[4][5], 국가정보통신기반시설 보호와 관련하여 공공-민간 간 협력 강화를 위한 연구[6], 국가정보통신기반시설 운영조직의 회복력 강화를 위한 연구[7] 등 국가정보통신기반시설 보호 역량 강화를 위한 연구[8][9]가 주를 이루고 있다.

이에 본고는 국가정보통신기반시설 보호를 추진하는 각국이 국가 차원에서 설치한 조직체계를 확인하고, 체계에 따른 조직별 추진 범위(국가정보통신기반시설 보호, 사이버보안 등)를 파악하고자 국가별 정책추진모형을 도출하여 비교·분석하고자 한다.

2.2 연구이론

본고는 국가정보통신기반시설 보호 및 사이버보안을 위한 각 국의 전략 및 정책을 비교하였다. 비교를 위해 국가별 국가정보통신기반시설 보호 정책과 사이버보안 정책 간의 포함 여부를 파악하여 포괄형, 중첩형, 분리형으로 구분해 살펴보았다.

이어서 정책모형이론에 기반해 국가별 국가정보통신기반시설 보호 정책의 추진 및 조직체계를 비교하였다. 정책모형이론은 정부가 국가정책을 추진하는데 있어 어떠한 목표와 방향을 가지고 정책 결정을 하며 정책결정자의 지휘체계 및 통제가 어떻게 이루어지는가의 형태를 파악하기 위한 이론으로 정책 추진의 전체적인 틀을 체계적으로 파악하는데 적합하여 정책학에서 활용되는 연구방법이다.

정책모형이론은 세부적으로 정책결정이론과 정책집행이론으로 구분하여 세부적으로 살펴보았다(Table 1. 참조)

정책결정이론에서는 정책목표와 정책결정과정을 명확하게 파악하여 최근 연구에서 많이 적용되고 있는 앨리슨(Allison) 이론[2]을 차용하였다. 그리고 정책집행이론에서는 정책집행자의 통제력과 정책집행자의 역할 등을 통해 정책집행형태를 명확하게 파악할 수 있는 나카무라&스몰우드(Nakamura & Smallwood) 이론[3]을 차용하였다. 구체적인 요인

1) 본고는 주요기반시설, 국가기반시설, 주요정보통신기반시설 등 다양하게 표현되는 기반시설의 명칭을 국가정보통신기반시설(National Critical Information Infrastructure, NCII)로 통일하였다. 국가별로 국가정보통신기반시설을 다양하게 표현하고 있어 각각의 표기대로 서술 시 발생할 혼란을 방지하고자 법령 등 명칭에 포함된 경우 외에는 국가정보통신기반시설로 표기하였다.

2) 앨리슨 이론은 조직의 구조적 특성에 따라 문제의 대응 과정에 대한 의사 결정 방식이 달라진다는 것을 주장하는 이론이다. 조직의 구조에 따라 의사결정권의 소재와 참여자의 목표 양태가 달라지며, 이 요인들이 복합적으로 작용해 문제 해결 방식에 차이가 발생한다는 것이다. 앨리슨 이론은 이를 합리모형, 조직모형, 관료모형 등 3가지 유형으로 구분한다.

3) 나카무라&스몰우드 이론은 정책결정자와 정책집행자의 관계를 중심으로 정책집행 모형을 5가지로 구분한 이론이다. 정책의 목표와 수단의 결정 권한에 따른 정책결정자와 정책집행자의 관계에 기초한 이론으로, 결정자의 권한이 강할수록 집행자의 권한이 약해진다고 본다. 정책결정자의 권한이 가장 강한 고전적 기술자형부터 순차적으로 지시적 위임형, 협

Table 1. Modified policy-promotion modeling theory

Policy-making				Policy-execution			
Organization		Strategy		Organization		Structure	
Basis for promotion	Deliberative organization	Presence or absence of a strategy	Goal setting	Organizational independence	Organizational activities	Cooperative structure	Sector-specific policies
"Policy-making model" based on modified Ellison theory				"Policy-execution model" based on the modified Nakamura & Smallwood's theory			
"Policy-promotion model"							

항목은 Table 2.에서 확인 가능하다.

2.2.1 정책결정 비교 모형 설정

국가별 국가정보통신기반시설 보호를 위한 정책결정 체계를 구분하고자 수정된 앨리슨 이론을 적용하였다. 앨리슨 이론의 구분 기준이 되는 의사결정권의 소재, 정책결정방식의 개념을 차용해 조직 요인과 전략 요인으로 구성한 수정된 앨리슨 이론을 분석의 틀로 설정하였다. 조직 요인은 국가정보통신기반시설 보호 전략 및 정책의 결정 권한이 법률 또는 정책서 등에 명확하게 명시되어 있는지(근거), 그리고 국가정보통신기반시설 보호 전략 및 정책의 결정 시 해당 전략 또는 정책에 대한 심의·자문기구가 존재하며 그 영향력이 온전히 미치는지(심의) 파악하기 위한 요인이다. 전략 요인은 국가정보통신기반시설 보호를 위한 정책이 존재하는지(유무) 그리고 사이버보안 추진을 위한 전략은 아닌지(목표성)에 대해 파악하기 위한 요인이다. 이를 모두어서 '정책결정모형'으로 설정하였다. 수정된 앨리슨 이론에 따라 합리모형, 조직모형, 관료모형으로 구분하였다. 정책결정 요인에 따른 정책결정정리모형의 국가별 유형 분류는 Table 3.에서 확인 가능하다.

상형, 재량적 실험형, 관료적 기업형으로 구분한다.

2.2.2 정책집행 비교 모형 설정

국가별 국가정보통신기반시설의 보호를 위한 정책집행 체계를 구분하고자 나카무라&스몰우드 이론의 정책 모형 개념 중 일부를 차용한 수정된 나카무라&스몰우드 이론을 구성하였다. 나카무라&스몰우드 이론 중 정책집행자가 의사 결정 권한을 갖는 협상형과 재량적 실험형, 관료적 기업형의 정책모형 개념을 차용하였으며, 유형을 구분하는 기준으로 조직 요인과 구조 요인으로 설정하여 수정된 나카무라&스몰우드 이론을 구성하였다. 조직 요인은 국가정보통신기반시설 보호를 추진하는 집행 조직 내에 국가정보통신기반시설 보호를 위한 별도의 조직 또는 부서가 마련되어 있는지 파악하는 '독립성'과 집행 조직이 관련 전략 및 정책 등의 수행을 위해 계획을 수립할 권한의 유무 등을 파악하는 '활동'으로 구성하였다. 구조 요인은 국가정보통신기반시설의 추진에 있어 집행 조직과 관련한 민관협력 추진체의 존재 여부 및 그에 대한 자문기구의 존재 여부를 파악하는 '협력'과 국가정보통신기반시설의 영역별 보호 활동의 추진 여부를 파악하는 '영역'으로 구성하였다.

이를 모두어서 '정책집행모형'으로 설정하였으며, 수정된 나카무라&스몰우드 이론에 따라 협상형, 재량적 실험형, 관료적 기업형으로 구분하였다. 정책집행 요인에 따른 정책집행정리모형의 국가별 유형 분류는 Table 4.에서 확인 가능하다.

2.3 사이버보안과의 비교

그리고 본고는 국가정보통신기반시설 보호와 사이버보안의 차이를 근거로 국가 간 주요 사이버보안 전략과 국가정보통신기반시설 보호 전략을 구분하여 주요 전략 및 정책을 비교하였다. 특히 사이버보안과 비교하여 국가정보통신기반시설의 보호를 더욱 중요하게 추진해야 하는 이유는 다음과 같다.

첫째로, 국가정보통신기반시설은 국가 존폐와 연결되는 문제이다. 에스토니아 사태와 우크나이나 전쟁 등을 통하여 국가정보통신기반시설을 대상으로 한 사이버공격이 국가전체에 위험을 미칠 수 있음을 경험했다[10][11].

둘째로 국가정보통신기반시설 보호는 국가 경제와 연결된다. 금융, 유통 등 중요 영역에 대한 침해 발생 시, 그 영향으로 국가의 경제가 마비되거나 심각한 피해를 입을 수 있다. 미국 소고기 유통 JBS사

Table 2. Factors for determining the type of policy-making model and policy-execution model

Sortation			Content	
Policy-making	Organization	The basis for the promotion	Concept	- Determine if the legislation provides the basis for activities to protect the NCII performed by the policy-making organization
			Criteria	- In accordance with the law - Based on policy reports - Unfounded
		Deliberative organization	Concept	- Determine the existence of a deliberative organization on the making and execution of policies for the protection of the NCII. - Consider the level of impact based on the composition and location of the deliberative organization
			Criteria	- Provide advice on policy-makings regarding the protection of the NCII as a permanent organization - Only research is conducted on policy-makings related to the protection of NCII as a permanent organization. Consultation is provided on policy-makings related to the protection of NCII as an emergency organization - Only conduct relevant research when making policy-makings regarding the protection of NCII as an emergency organization
	Strategy	The presence or absence of a strategy	Concept	- Determine whether there is a strategy or policy for the protection of the NCII
			Criteria	- NCII protection is indicated in law or strategy - NCII protection in policy reports - NCII protection is not indicated anywhere
		Goal setting	Concept	- Determine whether the objectives of a strategy or policy for the protection of the NCII are separate from cybersecurity. - Determine the relationship between NCII protection and cybersecurity
			Criteria	- NCII protection strategies or policies exist independently - A cybersecurity policy is described within a NCII protection strategy or policy - NCII protection strategies or policies are described within cybersecurity policies
Policy-execution	Organization	Organizational independence	Concept	- Determine if there is a separate department or organization within the policy-execution organization for NCII protection activities
			Criteria	- Exists as a separate and independent organization or department within the policy-execution organization - Exists within the policy-execution organization as a relevant organization or department that is promoted with other tasks - No organization or department in the policy-execution organization to perform the relevant tasks
		Activity	Concept	- Determine if the organization or department conducting NCII protection activities within the policy-execution organization establishes and implements the relevant plan
			Criteria	- Establish and implement strategies for the protection of the NCII - Establish and implement policy plans for the protection of the NCII - Only implement policy activities to protect the NCII
	Structure	Cooperative structure	Concept	- Identify the existence of a separate organization or committee for public-private partnership and relevant advisory bodies in the execution of NCII protection activities
			Criteria	- Cooperation/consultation bodies and relevant advisory bodies exist for public-private cooperation - Only cooperation/consultation bodies exist for public-private cooperation (no advisory body exists) - No cooperation/consultation body exists for public-private cooperation - Enable by sector
		Sector-specific policies	Concept	- Determine whether sector-specific protection activities are carried out to protect the NCII - Judgment based on the establishment of separate protection strategies or plans for each sector and the continuing publication of relevant reports
			Criteria	- Sector-specific protection activities are activated to release regular plans and reports - Sector-specific protection is active but does not release a separate report - Sector-specific protection activities are not active

※NCII : National Critical Information Infrastructure

가 랜섬웨어 공격으로 마비되면서 대규모 해고와 인플레이션으로도 이어질 위험이 발생했다[12][13].

셋째로, 국제관계에서 국가 간 거래의 조건으로 국가정보통신기반시설의 보호 수준이 제시되고 있다. 2023년 유럽위원회는 경제 안보 강화를 위해 에너지 안보 차원의 공급망 보안과 국가정보통신기반시설의 물리적, 사이버보안에 대한 위험 등을 포함한 4가지 영역에서의 평가를 수행하도록 제한하는 전략을 발표했다[14].

이에 국가정보통신기반시설 보호는 사이버보안과는 차별화된 보다 강력한 보호전략과 보호체계 등을 필요로 하고 있으며 주요국에서는 사이버보안과는 별도의 영역으로 추진 고려하고 있다.

III. 국가정보통신기반시설 보호 추진 전략

본 장은 주요국에서 추진하는 국가정보통신기반시설 보호 전략과 사이버보안 전략 및 정책을 비교하여 국가별 국가정보통신기반시설 보호와 사이버보안 전략 및 정책 간의 관계에 대한 차이를 도출하였다.

3.1 개요

본고는 국가별 국가정보통신기반시설 보호와 사이버보안 정책 및 제도와의 관계를 분석해 국가별 국가정보통신기반시설 보호 정책 및 제도의 수준을 파악하고자 한다.

대개 사이버보안을 확장하여 국가정보통신기반시설의 보호를 추진한다. 이에 국가정보통신기반시설 보호 정책 및 제도의 독립성을 기준으로 사이버보안과의 관계를 포괄형, 중첩형, 분리형으로 구분하였다. 포괄형은 국가정보통신기반시설 보호 정책을 별도로 마련하지 않고, 사이버보안 정책에서 해당 내용을 다루는 형태를 의미한다. 중첩형은 사이버보안과 국가정보통신기반시설 보호 정책을 각각 수립하고, 사이버보안 정책에 국가정보통신기반시설 보호 내용을 포함해 사이버보안의 추진 차원에서 일부 국가정보통신기반시설의 보호를 함께 추진하는 형태를 의미한다. 분리형은 사이버보안과 국가정보통신기반시설 보호 정책을 각각 수립하고, 국가정보통신기반시설 보호를 사이버보안 정책 및 전략이 아닌 독자적인 체계를 구축하여 추진하는 형태를 의미한다.

3.2 미국

미국은 국가전략에서 안전한 국가정보통신기반시설을 위한 사이버 위험으로부터의 보호 · 관리를 다루고, 동시에 국가정보통신기반시설 보호를 위한 별도의 계획(NIPP)을 수립하여 운영한다. 이에 미국은 사이버보안전략에 국가정보통신기반시설 보호 내용을 포함하며 동시에 별도의 국가정보통신기반시설 보호 정책을 추진하는 중첩형 형태이다.

3.3 영국

영국은 국가사이버안보전략에서 국가정보통신기반시설 보호의 영역을 포함하며, 특히 최근 증가하는 국가정보통신기반시설 대상 공격 및 기술환경의 변화에 초점을 맞추어 보호를 추진한다. 이에 영국의 국가정보통신기반시설 보호 정책은 사이버보안에 포함되어 운영되는 포괄형 형태로 보인다.

3.4 일본

일본은 「사이버시큐리티기본법(2014)」을 기반으로 국가 사이버보안 및 안보 체계를 구축하였으며, 5년 주기로 '주요기반시설 사이버보안에 관한 행동계획, 重要インフラのサイバーセキュリティに係る行動計畫')을 발표하고 있다. 이에 일본은 사이버보안 전략이 국가정보통신기반시설 보호 내용을 포괄하며 동시에 국가정보통신기반시설 보호를 위한 별도의 계획을 수립 및 추진한다. 이에 본고는 일본이 중첩형 형태로 정책을 추진한다고 본다.

3.5 독일

독일은 법률을 기초로 사이버보안과 국가정보통신기반시설 보호를 추진하고 있다. 그리고 최근 독일은 유럽의 CER 지침(The Critical Entities Resilience Directive, CER Directive)과 NIS2 지침(NIS2 Directive)에 따라 '주요기반시설 우산법(KRITIS-Dachgesetz)'을 논의하고 있다. '주요기반시설 우산법'은 독일의 사이버안보법을 보완하며 2026년에는 의무 조항을 발효, 2027년에는 벌금 조항을 발효하는 등 여러 단계에 걸쳐서 시행될 예정이다. 이에 독일은 사이버보안을 위한 법률 및 전략에서 국가정보통신기반시설의 보호를 언급하

면서도 국가정보통신기반시설을 위한 별도의 전략 및 법률을 가져가고 있어 국가정보통신기반시설 보호 전략은 포괄형으로 보인다.

3.6 호주

호주는 '주요기반시설보호법(SLACIP, 2022)' 및 '주요기반시설 복원 전략(2023)'을 수립해 국가정보통신기반시설 보호를 추진한다. 사이버보안전략에서 국가정보통신기반시설의 항목을 언급해 중첩형으로 볼 수 있으나, 그 내용을 살펴보면 국가정보통신기반시설 보호 법률(SoCI 및 SLACIP)을 소개 및 이를 통해 시행할 것을 명시하는 수준이다. 이에 본고는 국가정보통신기반시설 보호와 관련한 사항은 모두 관련 법률을 통해 추진되므로 일반적인 중첩형과 차이가 있다고 보고 호주를 분리형으로 구분하였다.

3.7 한국

한국은 국가정보통신기반시설 보호를 국가사이버안보전략과 「정보통신기반 보호법」에서 추진하므로 호주와 같은 분리형으로 볼 수 있다. 그러나 호주는 국가정보통신기반시설 보호를 위한 기본적인 전략과 추진계획에 대해 법률상으로 언급한다. 한국은 국가정보통신기반시설의 각 관리기관에서 보호대책을 수립하도록 법률상 명시하는 등 기관에서 개별적으로 추진하고 있어, 국가 전체차원에서 추진하는 호주와 차이가 있다. 한국은 대체로 관리기관 단위에서 보호전략을 추진하고 있으므로 국가 차원에서의 포괄적인 추진에 한계가 있다. 이에 본고는 한국을 소극적 중첩형으로 판단하였다.

3.8 소결

본 장에서는 국가 사이버보안 정책과 국가정보통신기반시설 보호 정책의 포함관계를 비교하고, 정책과정론에 입각하여 국가정보통신기반시설 보호 정책의 수립 및 추진단계를 분석하였다.

미국과 일본은 국가사이버안보전략에 국가정보통신기반시설 보호를 하나의 항목으로 포함하고 있으며 동시에 국가정보통신기반시설 보호를 위한 별도의 계획 및 지침을 수립하여 운영하는 중첩형 추진국가이다.

그에 반해 영국은 국가정보통신기반시설의 영역에 따른 정부부처에서 각기 영역별 보호 및 회복력을 위한 계획을 지속적으로 수립해오던 중, 2018년에 이르러서 국가 차원의 국가정보통신기반시설 보호를 중심으로 하는 새로운 지침(NIS 규정)을 발표 및 시행한다. 단, NIS 규정은 국가정보통신기반시설이 주된 대상이나 동시에 포괄적인 사이버보안을 위한 규정으로, 본고는 영국을 사이버안보의 포괄형 추진국가로 본다.

이어서 독일은 최근 KRITIS 우산법을 제정하기 위해 노력하고 있으나 기본적으로 사이버안보법 및 사이버보안전략에 기초하여 국가정보통신기반시설을 보호하고 있어 포괄형 추진국가로 본다.

호주는 사이버보안과 국가정보통신기반시설 보호를 위한 법률이 각각 제정되어 있어 분리형으로 본다.

한국은 국가사이버안보전략의 한 영역으로 국가정보통신기반시설 보호를 추진하며, 국가정보통신기반시설 보호를 법제화하여 추진한다. 이에 국가정보통신기반시설 보호가 사이버보안과 일부 중첩되나 내용에 있어 각기 추진하는 형태로, 소극적 중첩형 국가로 본다.

IV. 국가정보통신기반시설 보호 추진 체계

본 장에서는 국가별 국가정보통신기반시설 보호를 위한 정책 및 전략을 수립·개발·실행하는 조직 현황을 분석함으로써 국가별 전체적인 추진 체계를 비교·분석하고자 한다. 본 장에서 도식화한 조직 체계는 국가별 국가정보통신기반시설 보호와 관련한 정책결정 및 집행 조직을 구분하기 위한 개념적 조직도이다. 해당 도표는 국가별 추진 체계의 대략적인 조직의 위치를 나타내며, 국가정보통신기반시설 보호와 관련한 조직 및 기관, 협의체를 적색 선으로 구분하였다.

4.1 미국

미국은 정부 및 정부부처를 중심으로 정책을 개발 및 수립하고, 그 과정에서 민간 전문가를 포함하여 구성한 위원회를 구성해 조언을 구한다. 정책의 집행 시 정보공유 등을 위해 민간 조직의 지원을 받는다.

미국은 백악관 및 행정부를 중심으로 국가정책을 개발 및 수립한다. 민간 및 주/지방 정부의 임원들로 구성된 국가기반시설자문위원회(National Infra-

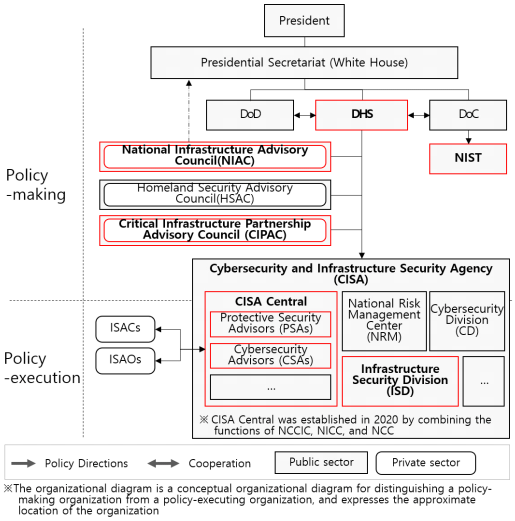


Fig. 1. US(the United States) National Critical Information Infrastructure (NCII) Protection Promotion System

structure Advisory Council, NIAC)와 공공 및 민간 부문으로 구성된 주요기반시설협력자문위원회(Critical Infrastructure Partnership Advisory Council, CIPAC)에서 조언을 받는다.

이어서 국가정보통신기반시설 보호 및 사이버보안과 관련한 정책의 직접적인 수행은 국토안보부(DHS) 산하 사이버보안및인프라보안국(CISA)에서 포괄적으로 수행하며, 부문별 위험관리부처(Sector Risk Management Agency, SRMA)를 통해 국가정보통신기반시설 부문별 특성에 따른 위험관리를 수행한다.

4.2 영국

영국은 정부부처에서 관련 정책을 개발 및 수립하며, 공공-민간 협력체를 설치하여 정책집행 전반에 영향을 미치고 있다.

영국의 국가 사이버보안 및 국가정보통신기반시설 보호를 위한 주요 전략인 NIS 규정은 영국 의회에서 제정, 영국 디지털·문화·미디어·스포츠부(DCMS)에서 담당한다. 국가사이버안보센터(NCSC)에서 국가정보통신기반시설 보호를 위한 담당이 있으며 국가정보통신기반시설의 보호를 추진하는 과정에서 국가정책 수립을 지원하는 공공-민간 협력체인 국가기반시설위원회(National Infrastructure Commission, NIC)의 평가 및 연구 결과 등을 토대로 영국의 국가

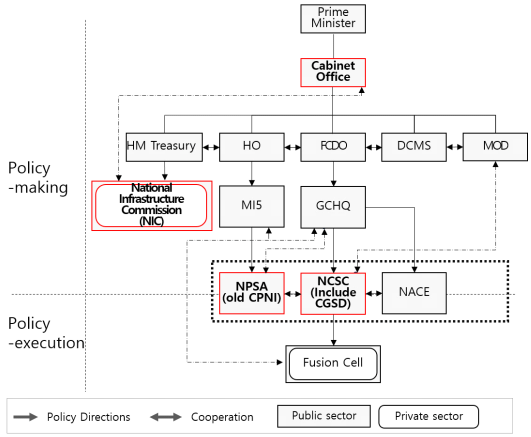


Fig. 2. GB(the United Kingdom) National Critical Information Infrastructure (NCII) Protection Promotion System

정보통신기반시설에 대한 자문을 구하여 참고한다.

4.3 일본

일본은 국가기관에서 정책을 개발하며, 그 과정에서 공공-민간 협력체를 통해 심의 및 검토를 수행한다. 그리고 정책의 수행에 있어 특히 영역별 협력체를 중심으로 국가정보통신기반시설 보호 정책을 추진한다.

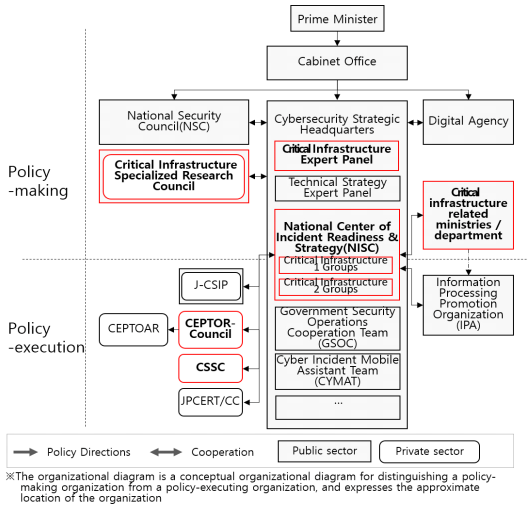


Fig. 3. JP(Japan) National Critical Information Infrastructure (NCII) Protection Promotion System

일본은 내각사이버시큐리티센터(National Center of Incident Readiness and Strategy for Cybersecurity, NISC)에서 '주요기반시설 정보보안에 관한 행동계획' 등 국가사이버보안 및 국가정보통신기반시설의 보호를 위한 정책을 개발 및 체계를 구축한다. 이 과정에서 공공-민간 협력체인 '주요기반시설전문조사회'를 꾸려 국가정보통신기반시설 보호 관련 정책 사안을 심의하고 전반적인 보안현황을 조사 및 검토한다. 그리고 국가정보통신기반시설 보호에 있어 모든 기반시설 사업자를 중심으로 영역별 센터(Capability for Engineering of Protection, Technical Operation, Analysis and Response, CEPTOAR)를 구성, 관련 정보를 공유 및 분석한다.

4.4 독일

독일은 연방내무부(BMI)가 컨트롤타워 역할을 하면서, 이를 중심으로 사이버안보 및 국가정보통신기반시설의 보호를 추진한다. 특히 연방내무부 산하의 연방정보보안청(BSI)를 중심으로 연방국민보호재난지원청(BBK)과 연방형사청(BKA), 정보보안기술본부(ZITiS) 등의 상호협력을 기반하여 국가정보통신기반시설과 관련한 정책 및 전략을 수립하고 시행한다.

연방정보보안청(BSI)은 연방 사이버보안 기관으로, 국가정보통신기반시설 운영자와의 민관협력을 위한 중심기관 역할과 IT 보안법에 근거하여 보안사고 발생 시 보고받는 국가역량센터로서의 역할을 담당한다. 독일은 사이버안보전략의 방향을 설정하고 전략을 수립하기 위해 사이버안보위원회(Cyber-Sicherheitsrat, Cyber-SR)를 수립하였는데, 이는 다수의 기관들의 협의체로 연방정부에 대한 자문역할을 수행한다.

그리고 연방내무부는 국가정보통신기반시설을 최대한 보호하기 위한 활동, 전략 및 조치를 조정하기 위한 별도 조직으로 주요기반시설공동조정팀(GEKKIS)을 2022년 10월에 신설하였다[15][16].

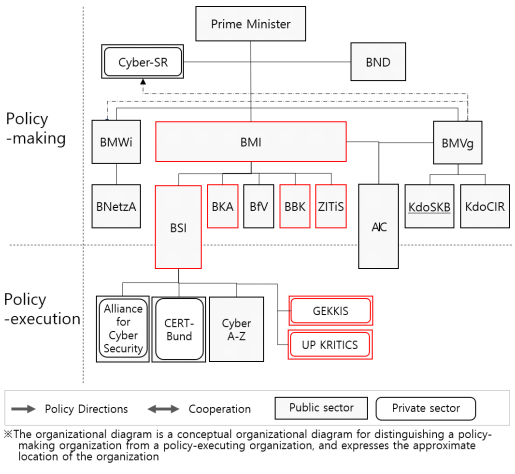


Fig. 4. DE(German) National Critical Information Infrastructure (NCII) Protection Promotion System

4.5 호주

호주는 정부부처에서 국가정보통신기반시설 보호를 위한 정책을 개발하고 추진한다.

호주의 국가정보통신기반시설 정책, 규제 및 전략 기능은 내무부(Home Affairs)에서 담당하고 있다. 호주의 핵심정책인 '주요기반시설 복원 전략'은 사이버및기반시설보호센터(CISC)와 주요기반시설 커뮤니티(Critical Infrastructure Community)가 함께 개발하였다.

또한 국가정보통신기반시설에 대한 업계와의 주요 참여 메커니즘으로 신뢰할 수 있는 정보공유 네트워크(TISN)가 운영되고 있다.

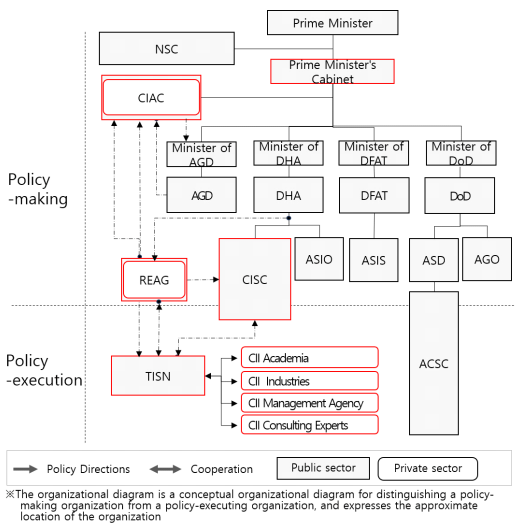


Fig. 5. AU(Australia) National Critical Information Infrastructure (NCII) Protection Promotion System

4.6 한국

한국의 사이버위기관리체계는 대통령을 중심으로 대통령비서실에서 총괄조정하며 국가안전보장회의(NSC)를 두고 있다. 그리고 국가정보통신기반시설 보호 체계는 정보통신기반보호법에 기반을 두고 정보통신기반보호위원회를 중심으로 국가정보원(공공 분야)과 과학기술정보통신부(민간 분야)에서 국가정보통신기반시설 보호 활동을 추진하고 있다.

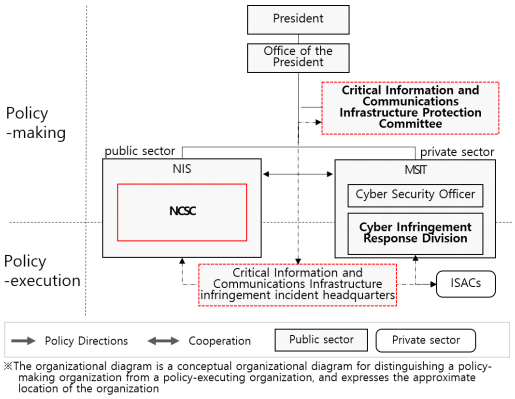


Fig. 6. KR(South Korean) National Critical Information Infrastructure (NCII) Protection Promotion System

4.7 추진체계의 비교

사이버보안 및 국가정보통신기반시설 보호를 위한 국가별 추진 체계를 정책결정 조직과 정책집행 조직으로 구분하여 각 조직의 특성을 비교, 국가별 정책의 추진 유형을 구분하고자 한다.

앞서 정리한 이론과 현황 분석을 기반으로 하여 각 국가의 정책결정 조직과 정책집행 조직을 구분하였다.

미국은 정책결정 조직으로 백악관을, 정책집행 조직으로 사이버보안및인프라보안국(CISA)을 선정하였다. 영국은 정책결정 조직으로 총리내각실을, 정책집행 조직으로 국가사이버안보센터(NCSC)를 선정하였다. 일본은 정책결정 조직으로 사이버시큐리티전략본부를, 정책집행 조직으로 내각사이버시큐리티센터(NISC)를 선정하였다. 독일은 정책결정 조직으로 연방내무부(BMI)를, 정책집행 조직으로 연방정보보안청(BSI)를 선정하였다. 호주는 정책결정 조직으로 총리내각부를, 정책집행 조직으로 사이버및기반시설보호센터(CISC)를 선정하였다. 한국은 정책결정 조직으로 대통령실을, 정책집행 조직으로 공공분야 국가사이버안전센터(NCSC)를 선정하였다.

상술한 각 국가별 정책결정 조직과 정책집행 조직을 2장에서 서술한 수정된 앨리슨 이론과 수정된 나카무라&스몰우드 이론에 적용하기 위해 각 기준 요인을 상세하게 구분하였다(Table 2. 참조).

4.7.1 국가별 추진 체계 비교

미국은 심의·자문기관으로 국가기반시설자문위원회(NIAC)가 존재한다. 다만 정책결정 조직의 하위기관인 국토안보부(DHS) 장관의 권한 하에 관리되나[17] 국가정보통신기반시설과 관련하여 관련 표준 및 보고서를 검토하고 보호 방안에 대한 권장사항을 대통령에게 제공하는 집행위원회로, 영향력을 미친다고 보인다. 미국의 정책결정 조직인 백악관은 국가정보통신기반시설 보호를 위한 정책결정 권한이 명시되어 있지 않으나 국가 전반의 전략을 수립하는 권한을 보유하고 있어 국가의 중요시설인 국가정보통신기반시설의 보호 관련 전략을 수립하는 것으로 보인다. 백악관에서 발간한 사이버보안전략 국가정보통신기반시설 보호 항목이 포함되어있으며 동시에 “주요기반시설 보호법(CIPA, 2018)”을 기초로 추진한다. 미국의 정책집행 조직인 사이버보안및인프라보안국(CISA)은 기관 내에 기반시설 보호 부서(ISD)를 보유하며, 영역별 제도 시행 가이드라인(C2M2 등), 영역별 사고 대응 가이드, 그 외 fact sheet 등을 발간한다. 또한 정보공유분석센터(ISAC)로 대표되는 민관협력체가 있으며, CIPAC를 별도로 보유하며 국가정보통신기반시설 보호와 관련한 협력을 위한 자문을 구한다. 이어 영역별 계획(SSP) 및 추진보고서를 지속적으로 발간하고 있다.

영국은 심의·자문기관으로 국가기반시설위원회(NIC)가 존재한다. 다만 국가기반시설위원회(NIC)는 영국 재무부에서 관리하는 기관으로 영국의 정책결정 조직인 총리내각실에 대한 온전한 영향을 미친다고 보기 어렵다. 미국 백악관과 마찬가지로 정책결정 조직인 총리내각실은 국가정보통신기반시설 보호를 위한 명시적인 근거는 없으나 국가 전반의 전략을 수립하는 기관으로 타 분야 전략과 함께 결정한다. 영국은 3장에서 살펴본 바와 같이 NIS 규정에 따라 국가정보통신기반시설의 보호를 추진하며, 영역별 보안 및 회복력 계획을 함께 추진한다. 이를 미루어볼

때 사이버보안의 관점에서 국가정보통신기반시설 보호를 추진한다. 영국의 집행 조직은 국가사이버안보센터(NCSC)로 조직 내에 국가정보통신기반시설 보호를 위한 별도 부서는 없지만 국가사이버안보센터(NCSC)를 이끄는 8명의 리더 중 국가정보통신기반시설 보호를 위한 담당이 있는 것으로 보아 관련 조직이 존재하는 것으로 보인다. 이어 국가사이버안보센터(NCSC)는 별도 계획을 수립하지 않지만 관련 가이드라인을 지속적으로 발간하며, 국가정보통신기반시설 보호를 위한 민관협력체로 CiSP, 전문가 그룹(Cyber Essential), 분석조직(Fusion Cell) 등을 보유한다. 다만 별도 자문기구를 두진 않는다. 3.3절에서 서술한 바와 같이 영역별 보안 및 회복력 계획을 꾸준히 발표하고 있다.

일본은 심의·자문기관으로 주요기반시설 전문조사회가 존재한다. 이는 「사이버시큐리티기본법」에 근거, 국가정보통신기반시설 보호 관련 조사, 검토를 위해 설립된 조직으로 총리대신에게 위원회원 임명권한이 있어 전략본부보다 상위에 있다고 볼 수 있다. 이어 일본의 국가정보통신기반시설 보호 정책을 결정하는 사이버시큐리티전략본부는 설치근거인 「사이버시큐리티기본법」 및 동법 시행령에서 관련 활동의 근거가 명시되어있다. 다만 국가정보통신기반시설 보호를 위한 전략은 행동계획 수준이며, 사이버시큐리티전략 내에 한 파트로 포함되어 있다. 일본의 집행 조직인 내각사이버시큐리티센터(NISC)는 기관 내에 국가정보통신기반시설 보호와 관련해 정책 대응 기능을 하는 '주요기반시설 1그룹'과 정보수집 및 대처 기능을 하는 '주요기반시설 2그룹'이 각각 존재한다. 또한 내각사이버시큐리티센터(NISC)는 "주요기반시설 사이버보안 실행계획(2022)"을 발간하였으며, 영역별 협력체인 섹터 및 섹터 Council을 보유하고 있다. 다만 섹터 및 영역에 대한 계획 및 보고서는 간헐적으로 발간한다.

독일은 사이버보안위원회(Cyber-SR)를 심의·자문 기관으로 둔다. 이는 2011년 수립된, 독일 사이버보안 중 가장 높은 수준의 기관(the highest-level body)으로[17], 정부부처 및 민간협회, 협의회로 구성되며 국무장관이 의장으로 있다. 따라서 독일의 정책결정 조직인 연방내무부(BMI)에도 유의미한 영향을 미치는 것으로 보인다. 독일의 정책결정 조직도 미국과 마찬가지로 다른 영역의 정책과 함께 결정하며 국가정보통신기반시설 보호에 대한 별도 근거는 없다. 그러나 국가정보통신기반시설에 대해 회복력 전략을 기초로, 현재 국가정보통신기반시설 보호를 위한 별도의 독립적인 법률을 제정하여 시행을 눈앞에 두고 있다. 독일의 정책집행 조직인 정보기술보안청(BSI)은 비즈니스와 사회를 위한 사이버보안 조직 내에 한 그룹으로 국가정보통신기반시설 보호 담당 부서를 두고 있다. 독특하게 독일은 민관협력체인 UP-KRITIS와 협력을 기반으로 국가정보통신기반시설 관련 계획 및 연구 보고서 등을 발간한다. UP-KRITIS는 위원회(RAT)와 총회(plenum)가 각각 존재하며 정책 수립을 위해 협력 기반 협의를 추진하는 것으로 보인다. 다만 일본과 마찬가지로 별도의 보고서를 정기적으로 발간하지는 않는다.

호주는 심의·자문기관으로 주요기반시설자문위원회(CIAC)를 둔다.

주요기반시설자문위원회(CIAC)는 총리내각부에서 설립된 조직으로 법무부(AGD)에서 의장을 담당하며, TISN의 운영 및 법무장관 조언 제공 역할을 담당하는 것으로 보아 정책결정 조직인 내각부에 유의미한 영향을 미치기 어렵다. 호주는 전략 및 정책은 내각부에서 결정하나 SoCI법을 중심으로 국가정보통신기반시설 보호를 추진하므로 별도 의회정보보안위원회(PJCIS)의 심의를 받기도 한다. 또한 정책결정 조직인 내각부는 별도 명확한 근거는 없으나 내각부 연간 목표 중 국가정보통신기반시설 보호 항목이 존재한다. 전술한 바와 같이 SoCI법을 중심으로 국가정보통신기반시설 보호가 추진되고 있다. 이에 호주 집행 조직인 사이버및기반시설보호센터(CISC)는 조직 자체가 국가정보통신기반시설 보호를 추진하기 위해 설립된 센터이며, 관련 계획을 수립하여 추진한다. 또한 영역 간 협력체인 TISN와 TISN Council이 운영되며 추가적으로 사이버및기반시설보호센터(CISC) 또한 협력을 위한 자문도 함께 수행한다. SoCI 법을 통해 영역별 국가정보통신기반시설의 자산에 대한 책임주체가 위험관리 프로그램을 보유하고 준수하도록 요구하고 있어, 영역 내 자산 보유자는 각기 관련 위험관리 보고서를 제출하도록 되어있다.

한국은 심의·자문기관으로 정보통신기반위원회를 둔다. 다만 국무총리 소속 하에 위치하고 있어 정책결정 조직인 대통령실에 유의미한 영향을 준다고 보기 어렵다. 또한 전술한 미국, 영국, 독일과 같이 다른 분야의 전략과 함께 국가정보통신기반시설 보호를 포함한 국가사이버안보전략을 발표하였으나 전략을 발표한 정책결정 조직의 국가정보통신기반시설 보호

활동 이행에 대한 근거가 명시되어 있지 않다. 한국은 국가정보통신기반시설 보호를 위한 법률을 제정하고 이를 근거로 관련 활동을 수행한다. 집행 조직인 국가사이버안전센터는 센터 내에 별도 국가정보통신기반시설 보호를 위한 부서가 존재하며, 관련 정책의 추진을 중심으로 한다. 정보공유분석센터(ISAC)을 위시한 민관협력체와의 협력을 추진하며 연간 관련 보고서를 발간하는 등 꾸준한 활동을 지속하고 있다.

이에 Table 2.에서 제시한 기준을 근거로 국가별 정책결정 조직 및 정책집행 조직의 상황을 정책결정 모형과 정책집행 모형에 적용하여 Table 3., Table 4., Table 5.와 같은 최종 결과를 도출하였다. ◎는 2점, ○는 1점, -는 0점으로 상정하여 3점 이상일 경우 합리모형/협상형, 2점일 경우 조직모형/재량적 실험형, 그 외는 관료모형/관료적 기업형으로 설정하였다.

4.7.2 정책결정 모형

수정된 앨리슨 이론을 근거로 정책결정 모형으로 국가별 유형을 정리한 결과, 미국, 독일, 호주는 합리모형, 일본은 조직모형, 영국, 한국은 관료모형에 해당한다.

Table 3. Policy-making model of major countries analyzed based on modified Allison's theory

Sortation	Policy-making						Model
	Organization			Strategy			
	Basis for execution	Deliberative organization	Synthesis	Presence or absence of a strategy	Goal setting	Synthesis	
US	◎	-	○	◎	◎	◎	Rational model
GB	○	-	-	○	○	○	Bureaucratic model
JP	○	◎	◎	◎	◎	◎	Rational model
DE	◎	-	○	◎	◎	◎	Rational actor
AU	○	○	○	◎	◎	◎	Rational model
KR	○	-	-	○	-	-	Bureaucratic model

※ US-UNITED STATES, GB-UNITED KINGDOM, JP-JAPAN, DE-GERMANY, AU-AUSTRALIA

합리모형은 최고관리층에 의사결정권이 집중되어 공동의 목표를 위해 추진하는 모형이다. 즉, 합리모형인 국가는 국가정보통신기반시설 보호에 있어 정책결정 조직을 중심으로 전략 또는 정책이 집중되어 수립되었다고 볼 수 있다. 미국, 독일, 호주는 모두 국가정보통신기반시설 보호를 위한 법률을 수립한 국가이며 국가 행정부 및 내각부, 내무부 등 최고관리층에서 관련 전략을 수립하는 체계이다. 일본은 사이버시큐리티전략본부에서 법률을 근거로 국가정보통신기반시설 보호 내용이 포함된 전략을 수립하였으며 추진 과정에서 내각사이버시큐리티센터(NISC) 또한 국가정보통신기반시설 보호를 위한 행동계획을 수립하는 것으로 보아 합리모형이 적절하다고 보인다.

조직모형은 최고관리층에서 목표를 설정하나 중간관리 및 하위조직에서 자체적인 조직의 목표를 가지고 전략 및 정책을 추진함을 의미한다.

관료모형은 국가 차원의 전략 목표와 하위조직 및 개개인의 목표가 산발적으로 존재하는 모형으로 수직적인 합리모형과 대조적인 수평적 구조를 보인다. 영국의 경우 총리내각부에서 전략을 수립하나 다양한 정부부처에서 국가정보통신기반시설 보호와 관련해 일정 부분을 담당하며, 국가정보통신기반시설 보호를 위한 별도 조직이 없는 상태에서 사이버보안 집행 조직인 국가사이버안보센터(NCSC)의 권한이 강력한 것으로 보인다. 또한 한국은 국가정보통신기반시설 보호 추진에 있어 정보통신기반 보호법을 기초로 하나 대통령실에서 수립한 사이버안보전략에도 국가정보통신기반시설 보호의 내용을 포함한다. 또한 다른 국가와 달리 정보통신기반보호위원회가 법률상 정책결정에 대한 권한을 보유하고 있으며, 국가정보통신기반시설 보호에 있어 보호계획 및 보호대책을 각 관리기관에서 수립 및 추진하는 상황이다.

4.7.3 정책집행 모형

수정된 나카무라&스몰우드 이론에 근거하여 각 국가를 정책집행 모형으로 구분한 결과, 미국, 일본, 독일, 호주는 협상형이며 영국은 재량적 실험형, 한국은 관료적 기업형임을 확인하였다.

협상형은 정책집행 조직이 목표 및 목표 달성에 있어 협상을 진행할 권한을 가진 모형이라고 볼 수 있다. 실제로 협상형인 미국, 일본, 독일, 호주는 집행 조직이 별도의 계획 및 가이드라인 등을 수립하여 추진하는 권한을 가진다. 또한 네 나라 모두 관련하여 정책결정 조직에 대한 자문 기구가 아닌 민관협력

Table 4. Policy-execution model of major countries analyzed based on modified Nakamura & Smallwood's theory

Sortation	Policy-execution						Model
	Organization			Structure			
	Organizational independence	Organizational activities	Synthesis	Cooperative structure	Sector-specific policies	Synthesis	
US	◎	◎	◎	◎	◎	◎	Bargaining model
GB	○	○	-	○	◎	◎	Discretionary experimental model
JP	◎	◎	◎	◎	○	◎	Bargaining model
DE	○	◎	◎	◎	○	◎	Bargaining model
AU	◎	◎	◎	◎	◎	◎	Bargaining model
KR	○	○	-	○	○	○	Bureaucratic enterprise model

을 위한 협력을 보유하고 그에 대한 자문기구 또한 보유하고 있다.

재량적 실험형은 정책집행 조직이 목표와 그에 대한 수단을 구체화하는 모형으로, 영국이 해당한다. 영국은 정책결정 정리 모형에서 서술한 바와 같이 사이버보안에 대해 본 고에서 정책집행 조직으로 설정한 국가사이버안보센터(NCSC)가 독립적인 권한을 가지고 있다. 이를 기초로 총리내각실에서 수립한 전략에 대해 정책집행 조직에서 보다 구체화하여 사이버보안과 함께 국가정보통신기반시설 보호를 추진한다고 볼 수 있다.

이어 관료적 기업형은 정책집행 조직 차원에서 목표 및 수단을 설정하여 추진하는 모형으로, 집행 중심적인 모형이다. 이에 해당하는 한국은 정책결정 및 심의 조직은 법률에 기초하며 국가 안보 차원의 거시적인 관점에서 방향을 제시하고 그에 따른 집행 조직 및 국가정보통신기반시설 보호의 책임이 있는 기관 및 조직(소유·운영자)이 구체적으로 추진하는 체계로 볼 수 있다.

4.8 소결

본 장은 국가별 국가정보통신기반시설 보호에 대한 정책결정 및 집행 조직의 체계 및 구조를 살펴보고 국가별 정책 추진의 유형을 구분하였다.

정책결정모형으로 설정한 정책결정의 유형은 수정된 앨리슨 이론을 적용하여 합리모형, 조직모형, 관료모형 순으로 구분하였다. 정책집행 모형으로 설정한 정책집행의 유형은 수정된 나카무라&스몰우드 이론을 적용하여 협상형, 재량적 실험형, 관료적 기업형으로 구분하였다. 수정된 정책모형이론을 적용하여 정책결정모형과 정책집행모형을 판단하는 결정요인에 대해서는 2장에서 서술하였다.

상기의 결과를 종합적으로 반영하여 정책추진모형을 도출하였는데, 정책추진모형은 정책결정모형과 정책집행 모형의 결과를 통해 국가별 국가정보통신기반시설 보호 체계가 국가정보통신기반시설 보호에 초점이 맞추어져 있는지, 그리고 정책의 결정과 집행 중 어디에 중심을 두고 추진되는지 등을 비교하여 설정하였다. 이는 체계강화모형, (정책)결정중심모형, (정책)집행중심모형, 관리중심모형으로 구성한다.

체계강화모형은 국가정보통신기반시설 보호와 관련하여 정책결정과 정책집행의 체계가 국가정보통신기반시설 중심으로 잘 갖춰져 있는 유형이다. 정책결정 체계가 국가정보통신기반시설 보호 중심으로 되어 있으나 집행 체계는 사이버보안의 맥락에서 추진되는 등 초점이 명확하지 않은 경우를 결정중심모형으로 설정하였다. 반대로 정책결정 체계는 사이버보안과 종합적인 맥락으로 진행되면서 정책집행 체계는 국가정보통신기반시설 보호 중심으로 추진되는 경우 집행중심모형으로 설정하였다. 이어 정책결정 체계와 정책 추진 체계가 국가정보통신기반시설 보호 중심이

Table 5. Policy-promotion model of major countries

Sortation	Policy-making		Policy-execution		Model
	Organization	Strategy	Organization	Structure	
US	○	◎	◎	◎	System-reinforcement model
GB	-	○	-	◎	Execution-oriented model
JP	◎	◎	◎	◎	System-reinforcement model
DE	○	◎	◎	◎	System-reinforcement model
AU	○	◎	◎	◎	System-reinforcement model
KR	-	-	-	○	Execution-oriented model

아니거나 추진체계가 명확하게 구축되어있다고 보기 어려운 경우 관리중심모형에 해당한다. 국가정보통신기반시설 보호 체계가 부재하다는 의미가 아님을 밝힌다.

Table 6. Key comparison basis for the classification of policy-promotion models by major countries

Sort ation	Model	Related to Policy-making	Related to Policy-execution
US	System-reinforcement model	▪ National Infrastructure Protection Plan ▪ E.O. 13010	▪ Critical Infrastructure Partnership Advisory Council ▪ National Infrastructure Advisory Council ▪ Department of Homeland Security ▪ National Institute of Standards and Technology
GB	Execution-oriented model	▪ UK National Cyber Strategy ▪ Sector Security and Resilience Plan, SSRP ▪ NIS Regulation	▪ National Infrastructure Commission ▪ National Cyber Security Centre
JP	System-reinforcement model	▪ National Infrastructure Protection Plan ▪ E.O. 13010	▪ National Center of Incident Readiness and Strategy for Cybersecurity ▪ Capability for Engineering of Protection, Technical Operation, Analysis and Response ▪ Initiative for Cyber Security Information sharing Partnership of Japan
DE	System-reinforcement model	▪ National Infrastructure Protection Plan ▪ E.O. 13010	▪ Bundesministeriu m des Innern (BMI) ▪ Cyber-Sicherheitsr at ▪ UP-KRITIS ▪ GEKKIS
AU	System-reinforcement model	▪ National Infrastructure Protection Plan ▪ E.O. 13010	▪ Home Affairs ▪ Critical Infrastructure Advisory Council ▪ Cyber and Infrastructure Security Centre ▪ Critical Infrastructure Community ▪ Trusted Information Sharing Network
KR	Execution-oriented model	▪ National Cyber Security Strategy ▪ Act on the Protection of Information and Communications Infrastructure	▪ Critical Information and Communications Infrastructure Protection Committee ▪ National Cyber Security Center ▪ MSIT, Cyber Infringement Response Division ▪ Critical Information and Communications Infrastructure infringement incident headquarters

본 고에서 진행한 구분에 따르면 미국, 일본, 독일, 호주는 체계강화모형이며 영국은 집행중심모형으로 나타난다. 한국도 집행중심모형에 해당하나 그 수준이 약한 것으로 보인다.

미국, 독일, 호주는 최고지도층에서 국가정보통신기반시설 보호의 내용을 포함한 국가사이버보안전략을 수립한다. 이 때, 국가정보통신기반시설을 위한 별도의 위원회를 구성, 심의·자문을 통해 전략을 수립함이 공통된 특징이다. 이어 국가정보통신기반시설 보호를 위한 별도의 법률을 마련하였거나 추진하는 사실 또한 공통적으로 나타난다. 이렇게 수립한 국가정보통신기반시설 보호 전략 및 정책을 추진하기 위한 조직 또는 부서가 독립적으로 위치하며, 민관협력을 위한 협력체가 존재하며 협력에 자문기구로서의 별도 위원회 또한 존재한다. 또한 일본은 비교국가 중 국가정보통신기반시설 보호를 위한 정책을 국가최고지도층이 아닌 사이버보안조직에서 수립하는 것이 특징으로 정책결정조직의 국가정보통신기반시설 보호에 대한 행동 근거는 명확하나 정책의 수준이 높지 않고 사이버보안과 함께 수행하고 있다. 같은 맥락으로 정책집행에 있어 국가정보통신기반시설 보호에 대한 별도 부서를 보유하여 구체적인 활동을 추진하며, 동시에 영역별 협의 및 협력에 강세를 보인다. 이렇게 국가정보통신기반시설 보호를 위한 관련 정책의 수립부터 추진, 협력 구조까지 온전히 구성되어있으므로 미국, 일본, 독일, 호주를 체계강화모형으로 구성하였다.

이어 영국은 Table 3.에서 볼 수 있듯 국가정보통신기반시설 보호에 대한 정책결정모형이 관료모형에 해당한다. 정책을 결정하는 조직의 근거가 약하고 전략은 사이버보안과 함께 수립되는 양상을 보인다. 이는 정책집행 모형에서도 나타나는데 집행 조직의

구성이나 협력구조가 국가정보통신기반시설의 보호와 사이버보안을 함께 추진한다. 다만 영국은 영역별 관리에 집중하는 것으로 보인다. 또한 영국은 정책집행 중 협력 구조 또는 영역별 관리를 보고(report) 중심으로 활발하게 추진한다. 즉, 영국은 국가정보통신기반시설 보호에 있어 정책, 전략을 사이버보안과 함께 수립되거나 전략보다 낮은 수준(계획 등)으로 구성한다. 반면 정책의 집행에 있어 영역별 관리체계나 협력 구조의 집중도가 높아 정책집행 중심 모형에 해당한다.

반면 한국은 전술한 영국과 같이 집행중심모형이긴 하나 약한 집행중심모형으로 판단된다. Table 5.에서 볼 수 있듯 정책결정 및 정책집행 모든 영역에서 추진 전략 및 추진 체계가 상대적으로 낮은 것으로 나타난다. 특히 한국의 국가정보통신기반시설 보호 체계는 정보통신기반보호법을 근거로 추진되며, 해당 법률에 근거하여 정보통신기반보호위원회를 통해 주요정보통신기반시설 보호정책의 조정, 관련 전략 및 정책에 대한 심의가 명시되어 있으나(법 제4조) 국가정보통신기반시설 추진을 위해서는 보다 강한 추진력 혹은 추진 조직을 필요로 한다. 그리고 위원회에서는 기반시설 중심의 별도의 전략이나 정책이 심의된 바 없으며 기반시설의 지정 여부 및 보호대책 이행 점검 결과 심의 등에 초점이 맞춰져 있는 실정이다. 2019년 및 2024년 발표된 국가사이버안보전략에서 '국가 핵심인프라 사이버 복원력 강화'를 하나의 전략 과제로 설정하고 상시 대비 태세 마련, 위협 탐지 체계 확대 구축, 제로 트러스트 보안 전략 구현, ICT 공급망 보안정책 확립 등을 추진하고 있으나 미국 등 주요국에서 추진되고 있는 프레임워크, 정보공유체계, 민간 협력 구조 등과 비교하면 확대 추진이 고려되어야 한다. 따라서 국가정보통신기반시설 보호를 위한 구체적인 집행 구조가 마련되어 있다고 보기 어려워 약한 수준의 집행중심모형에 해당한다고 본다.

V. 결 론

국가정보통신기반시설 보호는 사이버보안 내의 세부 과업처럼 다루어졌으나, 그 중요성이 더욱 강조되고 있으며 핵심 정책으로서 보다 체계적인 추진이 요구되고 있다. 이에 본고는 국가별 국가정보통신기반시설 보호 정책의 결정 및 집행 체계를 비교해 정책추진모형을 유형화하였다. 여기에는 수정된 앨리슨 이론과 수정된 나카무라&스몰우드 이론을 적용하여 국가별로 정책결정 모형, 정책집행 모형, 그리고 정책추진 모형을 분석, 도출하였다.

사이버보안 및 국가정보통신기반시설 보호를 포괄하는 '보안정책'의 특성상 정책결정 조직의 권한이 정책집행 조직으로 내려올수록 일관성 있고 체계적인 정책 추진의 한계로 즉시적이며 협력적인 대응이 어려워 국가 안보적 위험이 커지는 것으로 분석되고 있다. 연구 결과, 수정된 앨리슨 이론의 합리모형과 수정된 나카무라&스몰우드 이론의 협상형에 해당하는 국가가 가장 많음을 확인하였다. 이는 일반 정책과 달리 엄격하게 추진되어야 하는 보안정책의 특성을 시사한다고 볼 수 있다. 국가 이익의 극대화를 위하여 합리적 결정행위가 이루어지는 구조로 합리적인 대안을 선택하고 목표를 설정하는 정책결정 구조이며 정책결정자와 정책집행자 간의 유연한 협상으로 조정과 통제가 잘 이루어지는 정책집행 구조이다.

또한 최종적으로 정책추진모형에서는 미국, 독일, 일본, 호주가 체계강화모형에, 영국과 한국은 집행중심모형에 해당함을 도출하였다. 4장에서 서술한 바와 같이 미국, 일본, 독일, 호주는 전략 및 정책과 법제 차원에서 국가정보통신기반시설 보호를 별도로 추진하는 양태로 보인다. 이는 2장에서 서술한 바와 같이 사이버보안과 비교하여 국가정보통신기반시설의 보호를 더욱 중요하게 추진하는 이유로 이어진다. 이는 국가정보통신기반시설 보호를 국가전략 또는 디지털 전략에 포함해 추진하는 상황으로 나타나는데, 이는 국가정보통신기반시설 보호를 보다 강화하는 차원으로 이해할 수 있다. 국가정보통신기반시설 보호의 강화는 국가정보통신기반시설을 중심으로 체계 등을 강화해 나가는 것을 의미한다.

그리고 영국은 집행중심모형으로 분석하였지만, 국가정보통신기반시설 보호를 위한 프레임워크 등을 운영함으로서 미국과 유사한 수준의 보호 추진체계를 보유하고 있다.

한편, 한국은 집행중심모형 중 약한 집행중심모형이라 할 수 있다. 정보통신기반보호법을 선도적으로 제정하여 국가정보통신기반시설 보호를 추진해 오고 있으나 정책 추진 구조와 전략 및 정책 형태, 그리고 위협 환경 변화에 대한 대응 등을 고려하였을 때에, 최소한의 소극적 추진이 이루어지는 것으로 판단된다.

글로벌 수준에 맞는 국가정보통신기반시설 보호를 추진하기 위해서는 보다 체계적이고 협력적인 형태로 추진할 거버넌스 체계와 정책 틀을 필요로 한다.

이어서 본 고를 통해 보다 나은 한국의 국가정보통신기반시설 보호 체계의 구성을 위해 다음과 같은 개선안을 제안하고자 한다.

첫 번째로, 정책결정 차원에서 국가정보통신기반시설 보호에 대한 내용이 보다 특화되어야 한다. 법률을 근거로 추진하는 호주나 독일은 국가정보통신기반시설 보호를 위한 법률을 통해 국가정보통신기반시설의 특성을 고려한 항목을 제시한다. 호주에서는 주요기반시설 보호법(SoCI)의 개정(SLACIP)을 통해 시작한 국가정보통신기반시설의 자산 관리를 기초로 주요 영역의 설정을 통한 영역별 관리까지 수행하고 있으며, 독일은 새로운 국가정보통신기반시설 보호를 위한 새로운 법률('주요기반시설 우산법')의 제정을 통해 회복탄력성과 물리적 보안을 함께 규제하고자 한다. 반면 한국이 법률을 통해 추진하는 국가정보통신기반시설 보호 방안은 대개 사이버보안 차원의 국가정보통신기반시설 보호 추진으로, 기술적 대책 중심의 방안으로 이루어져 있으며, 이를 수행하는 관리기관에서 보호대책을 수립 및 이행하도록 명시되어있다. 관리행정기관 중심의 보호대책으로 조직별 상황에 맞는 조치를 취하는 것은 바람직하나, 그러나 국가정보통신기반시설은 국가 존폐와도 연결되는 중요한 사안으로, 사이버보안 차원의 보호가 아닌 국가정보통신기반시설 보호 차원의 구분된 사이버보안 조치의 마련 및 적용이 필요하다.

두 번째로, 집행 차원에서 국가정보통신기반시설 보호와 사이버보안과의 관계가 보다 확장된 개념으로 적용되어야 한다. 이는 전략과 조직 구성에 모두 해당한다. 현재 사이버보안의 관점에서 전략이 수립되고 그 중 하나의 파트로 국가정보통신기반시설 보호가 속해있다. 그러나 국가정보통신기반시설의 중요성과 특성을 고려할 때, 국가 차원에서 보다 확대된 관점의 국가정보통신기반시설 보호의 추진이 필요하다. 또한 조직 차원에서도 국가정보통신기반시설 보호와 사이버보안 간 관계의 정리가 필요하다. 대개 국가에서 사이버보안 집행 조직에서 국가정보통신기반시설 보호를 함께 추진하지만, 그 중에서도 미국과 일본은 국가정보통신기반시설 보호와 관련한 부서를 별도로 두어 추진하고, 호주는 별도 센터를 설립해 추진한다. 영국 또한 현재는 사이버보안 집행센터에 일부 편입되었으나 국가정보통신기반시설 보호를 위한 별도 센터를 둔 전적이 있다. 당장 국가정보통신기반시설 보호의 추진을 담당할 조직 또는 부서를 사이버보안을 담당하는 조직과 독립하여 설립, 운영해야 한다는 것이 아니다. 동일한 사이버보안을 수행하더라도 국가정보통신기반시설의 보호 관점에서 추진하는 조직으로 시작해, 국가정보통신기반시설 보호의 집행조직을 별도로 두는 것을 최종 목표로 삼아 단계적인 접근이 필요하다.

세 번째로, 국가정보통신기반시설 보호를 위한 전략 및 정책 추진 체계의 개선을 위해 현「정보통신기반 보호법」의 개정이 필요하다. 한국은 기반보호법에 따라 관리기관 단위로 국가정보통신기반시설의 보호 전략을 추진한다. 이는 관리기관에서 개별적으로 보호 대책을 추진하는 것으로, 국가 차원에서 국가정보통신기반시설 보호를 포괄적으로 추진하기에 한계가 있다. 호주와 독일은 법률을 근거로 국가정보통신기반시설 보호를 위한 기본적인 전략 및 추진체계를 명시하여 별도의 체계를 마련하고 있다. 호주는 국가정보통신기반시설의 자산관리를 근거로 국가정보통신기반시설의 보호 체계를 수립하였고, 독일은 우산법을 신설하며 구체적인 체계를 잡아가고 있다. 이처럼 한국 또한 국가정보통신기반시설 보호의 기준이 되는「정보통신기반 보호법」을 국가정보통신기반시설에 대한 전략 및 계획 수립과 같은 항목에 대해 보다 명확하게 법률로서 명시할 수 있는 방향으로의 개정이 필요하다.

References

[1] "Ransomware attacks on US government organizations cost over $70bn from 2018 to october 2022", Comparitech, Jan. 15. 2024. [Online] https://www.comparitech.com/blog/information-security/government-ransomware-attacks/ Accessed: Jan. 02. 2024.

[2] Lee Yeon-soo, Lee Soo-yeon, Yoon Seok-gu, Jeon Jae-sung, "Comparison of cyber safety-related laws and organizational systems in major countries and research on development plans," *Journal of national intelligence studies*. Vol. 1, No. 2, pp. 125-128, 2008.

[3] Park Hyang-mi, Yoo Jiyeon. "A Study on Major Countries's Level of

Cybersecurity for Critical Infrastructure," *Journal of The Korea Institute of Information Security & Cryptology.* Vol. 27, No. 1. pp.163 - 176. 2008.

〔4〕 Lachezar Petrov, Nikolai Stoianov, Todor Tagarev, "Critical Information Infrastructure Protection Model and Methodology, Based on National and NATO Study", 「DepCoS-RELCOMEX 2017: Advances in Dependability Engineering of Complex Systems」, pp 350-357. May. 2017. https://link.springer.com/chapter/10.1007/978-3-319-59415-6_34

〔5〕 Pinosh Kumar Hajoary, K. B. Akhilesh, "Role of Government in Tackling Cyber Security Threat" *Smart Technologies* pp.79 - 96, Aug. 28. 2019. 〔Online〕 https://link.springer.com/chapter/10.1007/978-981-13-7139-4_6 Accessed: Nov 23. 2023.

〔6〕 Charlotte Brown, Erica Seville, JohnVargo, "Measuring the organizational resilience of critical infrastructure providers: A New Zealand case study", International Journal of Critical Infrastructure Protection, Vol.18, p.37-49. Sep. 2017. https://www.sciencedirect.com/science/article/pii/S1874548216300348

〔7〕 Gharehyakheh, Amin, Tolk, Janice N., Cantu, Jaime, Fritts, Stephen, "A Survey Paper of Protecting Critical Infrastructure: Applying High Reliability Theory to Advance Organizational Resilience", 2017.https://rc.library.uta.edu/uta-ir/handle/10106/27580

〔8〕 Bilge Karabacak, Sevgi Ozkan Yildirim, Nazife Baykal, "A vulnerability-driven cyber security maturity model for measuring national critical infrastructure protection preparedness", *International Journal of Critical Infrastructure Protection*, Vol.15, pp. 47-59. Dec. 2016. 〔Online〕 https://www.sciencedirect.com/science/article/pii/S1874548216301330 Accessed: Nov 23. 2023.

〔9〕 Lachezar Petrov, Nikolai Stoianov, Todor Tagarev, "Critical Information Infrastructure Protection Model and Methodology, Based on National and NATO Study", 「DepCoS-RELCOMEX 2017: Advances in Dependability Engineering of Complex Systems」, pp.350-357. May. 2017. https://link.springer.com/chapter/10.1007/978-3-319-59415-6_34

〔10〕 "〔Issue Analysis〕 Attacks on 'social infrastructure' that have begun in earnest since the mid-2000s", Etnews, Mar. 20. 2019. 〔Online〕 https://www.etnews.com/20190319000065 Accessed: Nov 23. 2023.

〔11〕 "Russia attacks Estonian website in 2007… 3 weeks of paralysis of national functions", The JoongAng, Feb. 17. 2024. 〔Online〕 https://www.joongang.co.kr/article/25229225#home Accessed: Jan 02. 2024.

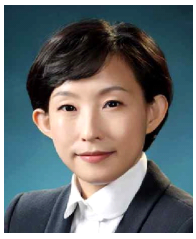
〔12〕 "How the JBS Foods hack could affect the price of meat", FoxBusiness, Jun. 02. 2021. 〔Online〕 https://www.foxbusiness.com/lifestyle/how-the-jbs-foods-hack-affect-price-meat Accessed: Jan 02. 2024.

〔13〕 "What the JBS cyberattack means for meat supply", CNN, Jun. 02. 2021. 〔Online〕 https://edition.cnn.com/2021/06/01/business/jbs-cyberattack-meat-shortage/index.html Accessed: Nov 23. 2023.

〔14〕 European Commission, "An EU approach to enhance economic security", Hun. 20. 2023. 〔Online〕 http

s://ec.europa.eu/commission/presscorner/detail/en/IP_23_3358 Accessed: Jan 02. 2024.
〔15〕 Federal Ministry of the Interior and Community (BMI), "Neuer Koordinierungsstab der Bundesregierung zum Schutz kritischer Infrastrukturen", Oct. 21. 2022. 〔Online〕 https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2022/10/koordinierungsstab-kritis.html Accessed: Nov. 15. 2023.
〔16〕 Federal Ministry of the Interior and Community (BMI), "Schutz Kritischer Infrastrukturen in Deutschland", Mar. 01. 2023. 〔Online〕 https://www.bmi.bund.de/SharedDocs/schwerpunkte/DE/schutz-kritis/topthema-kritis.html;jsessionid=196B6248E41960533DCD2DD0125627D0.live862 Accessed: Nov. 15. 2023.
〔17〕 Cybersecurity and Infrastructure Security Agency(CISA), "The President's National Infrastructure Advisory Council (NIAC)", 2018. 〔Online〕 https://www.cisa.gov/resources-tools/groups/presidents-national-infrastructure-advisory-council-niac Accessed: Jan. 02. 2024.

〈저자소개〉



유 지 연 (Ji-yeon Yoo) 종신회원
2012년 2월: 고려대학교 정보경영공학 박사
1999년 11월~2013년 2월: 정보통신정책연구원 부연구위원
2014년 3월~현재: 상명대학교 휴먼지능정보공학과 교수
〈관심분야〉 사이버안보, 정보보안, 디지털 위험관리, 신기술 위험, 디지털 전략