Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.27, NO.1, Feb. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.1.163

주요기반시설에 대한 주요국 사이버보안 수준 비교·분석 연구

박 향 미,† 유 지 연‡
상명대학교

A Study on Major Countries's Level of Cybersecurity for Critical Infrastructure

Hyang-mi Park,† Ji-yeon Yoo‡
Sangmyung University

요 약

최근 주요기반시설은 기존의 폐쇄적인 환경에서 개방적인 환경으로 변화하고, 사이버공간으로 범위가 확장되면서 사이버위협의 새로운 대상이 되고 있다. 또한 정보통신기술의 발전으로 주요기반시설 간의 상호의존성이 증가하고 있다. 그러나 기존 연구는 동향조사 및 보호정책 논의 수준에 머물러, 정책의 효율적 추진을 위한 현황 진단 및 적절성 판단 등의 연구는 별도로 진행되고 있지 않다.

이에 본 연구는 기존에 국가별 사이버보안 수준을 측정하는 국제지표 3가지를 비교·분석하여 주요기반시설의 보호수준을 측정하기 위한 새로운 지표를 개발하고, 해당 지표를 통하여 미국과 일본, 영국, 독일, 노르웨이로 대표되는 주요국과 한국의 현재 주요기반시설의 보호수준을 측정한다. 이를 통하여 미래 사이버공간에서 한국의 영향력을 확대하고 국가 간 신뢰를 구축할 근거자료가 되기를 기대한다.

ABSTRACT

Recently, the critical infrastructure is changing from the existing closed environment to an open environment, and it is becoming a new target of cyber-threats by expanding into cyberspace. In addition, due to the development of information and communications technology(ICT), the interdependence among critical infrastructure is increasing. Previous studies ranged from trend investigation and policy discussions to protection, but separate studies on the diagnosis of the current status and appropriateness judgment for efficient policy implementation were not performed.

Therefore, this study compares and analyzes three international indicators that measure the level of cyber security in each country in order to build a new index to measure the level of cyber security of critical infrastructure in the USA, Japan, UK, Germany, Norway, and Korea. It is hoped that this study will serve as a basis for expanding Korean influence and building trust among countries in future cyberspace.

Keywords: Critical Infrastructure, Cybersecurity, Critical Infrastructure Protection(CIP), Cybersecurity Index

I. 서 론

최근 플레임(Flame), 스턱스넷(Stuxnet), 듀큐(Duqu) 등과 같은 악성코드로 인하여 발생하는 주요기반시설 대상의 전자적 침해행위가 국가안보를 위협하는 새로운 요소로 대두되고 있다. 또한 주요기반

Received(01. 18. 2017), Modified(02. 13. 2017), Accepted(02. 13. 2017)

† 주저자, aymi0103@gmail.com
‡ 교신저자, yooo@smu.ac.kr (Corresponding author)

시설을 둘러싼 환경이 폐쇄적 환경에서 개방적 환경으로 변화하고 사이버공간으로 확대됨으로써 사이버 위협의 새로운 대상이 되고 있다. 주요기반시설에 대한 사이버공격으로 인해 발생하는 침해는 공공과 민간에 모두 큰 영향을 미치며 파급효과가 크다. 더불어 주요기반시설 간의 상호의존성이 증가함에 따라 [16] 각 국가는 국가적 차원을 넘어 국가 간의 신뢰 구축 등 국제적 차원에서 주요기반시설을 보호하기 위하여 노력한다.

미국과 유럽 등의 주요국에서는 이러한 관점에서 주요기반시설 간의 상호의존성에 초점을 맞추어 주요기반시설의 보호 수준을 명확히 측정함으로써 국가 간의 신뢰를 구축하기 위한 다양한 성숙도 모델을 적용하고 있다. 이와 같이 주요기반시설의 보호수준을 향상시키는 것은 국제관계에서 점차 중요해지고 있다. 한국 역시 7.7 DDoS 공격, 농협 해킹 공격, 3.20 전산망 공격, 한수원 사태 등을 통하여 더 이상 주요기반시설에 대한 사이버테러로부터 안전하지 않음이 증명되었으므로 이를 보호하기 위한 노력이 필요하다.

한국은 주요기반시설의 정보통신망 및 정보시스템의 주요정보통신기반시설의 보호를 목적으로 2001년에 「정보통신기반 보호법」을 제정하여 국가적 차원으로 보호체계를 구축하고, 지속적인 개정을 통하여 미비점을 개선·보완하며 운영하고 있다. 그러나 주요기반시설을 둘러싼 변화 양상에 대하여 탄력적인 운영이 되고 있다고 보기는 힘들다[12]. 정보통신기반보호법 수립 당시 23개에 불과하던 주요정보통신기반시설이 현재 385개로 확대되어 보호관리되고 있으나[27] 다양해지는 위협에 대한 대비 및 관리와 실질적인 현황 분석은 제대로 이루어지지 않는 것으로 나타나고 있다[19][23].

이에 본 연구는 주요국과 한국의 보호수준을 기술적 측면이 아닌 전체적인 관점에서 파악하기 위하여 국제 사이버보안지표를 기초로 주요기반시설 보호에 초점을 둔 지표의 틀을 제시하고, 주요국과 한국의 주요기반시설 보호수준을 비교하고자 한다.

II. 선행연구

주요기반시설을 보호하기 위한 보호정책 제도, 관리체계에 대한 기존의 연구는 동향 분석과 그에 따른 보안대책을 중심으로 이루어지고 있다. 함초롬(2016)은 주요정보통신기반시설의 사이버위협을 관리하기 위하여 미국의 사이버보안 프레임워크, ISO/IEC 27001, 한국의 정보보호 관리체계(ISMS)를 대상과 제도성격, 평가영역, 주체, 유효기간 등과 같은 항목을 통하여 여러 가지 관리체계를 비교하였다[8]. 장상현(2015)은 마찬가지로 미국의 사이버보안 프레임워크와 일본 IPA의 사이버안전 기준, 그리고 한국의 주요정보통신기반시설 정보보호 수준평가, ISMS 제도, 정보보호 준비도 평가·제도를 비교·분석하여 정보보호 수준평가의 문제점을 개선한 체크리스트를 제시하며 법규를 통한 의무화와 연구개발의 필요성, 인센티브 방안 등을 제시한다[34]. 임길환(2011)은 주요기반시설의 제어시스템 보안을 위하여 기술적·관리적·정책적 취약점을 도출하고 각각의 보안대책을 제시하였다[24].

또한 박동연(2014)은 주요정보통신기반시설의 제어시스템 보호를 위하여 보호대책에 실효성을 제고하기 위한 방안으로 관리적·물리적 분야의 취약점 분석·평가 기준을 해외 제어시스템 보안기준과 한국의 관련 지침, 기준 등과 비교·분석하여 운영기관에 특화된 관리적·물리적 취약점 분석 및 평가 기준을 제안하였다[11]. 이현주(2016)는 주요기반시설의 환경변화로 인하여 새로이 나타난 특성으로 인하여 등장한 사이버위협을 제시하고 미국과 EU, 일본의 주요기반시설 보호를 위한 정책을 비교·분석하여 한국의 주요기반시설 보호를 위한 발전방향으로써 기술적·관리적·정책적 과제를 제안하였다[18]. 배효빈 외 3인(2013)은 국내 주요정보통신기반시설의 보호대책 개선을 위해 선진국(미국, 캐나다, 독일)의 보안정책 동향을 분석하여 국내에 적용하기 위한 맞춤형 보호체계로 업무특성에 따라 분류된 시설별 보안대책과 정책적 개선, 관리적 개선, 기술적 개선, 국제적 협력의 총 4단계로 이루어진 단계별 보호체계를 제시하였다[17].

이처럼 기존의 연구는 기술적인 측면에 초점을 맞추거나 주요기반시설의 취약점 분석 및 평가에 기초한 동향분석으로 진행되었고, 주요국의 관련 보호정책에 대한 연구 역시 보안대책을 제시하는 수준에 머물고 있어 한국의 사이버보안 수준 및 주요기반시설의 보호수준을 분석하지는 않아 포괄적인 관점의 연구는 부족하다. 또한 이 수준을 측정하기 위한 보안지표와 관련하여 사이버보안 측면의 평가지수만이 연구되었고, 그 중 사이버보안 지수에 주요기반시설 항목이 일부 추가된 형태의 연구는 존재하나[36], 주요기반시설의 관점에 대한 연구는 진행되지 않았다.

따라서 변화하는 주요기반시설의 환경을 포함한 포괄적인 관점에서의 논의와 주요기반시설의 독립적인 관점에서의 연구가 필요하다.

III. 국제지표 비교·분석 및 주요국 선정

3.1 국제지표 비교·분석

주요기반시설의 영역이 사이버공간으로 확대됨에 따라 사이버보안 지표를 통하여 주요기반시설의 보호수준을 분석하고자 한다.

국제적으로 사이버 및 사이버보안의 수준을 측정하기 위해 존재하는 많은 국제 지표 중 점수화되거나 순위로 나타나는 정량적 결과의 존재여부, 그리고 구체적인 평가항목의 존재여부 등을 기준으로 국제전기통신연합(International Telecommunication Union, ITU)의 세계사이버보안지수(Global Cyber security Index, GCI), 소프트웨어연합(Business Software Alliance, BSA)의 사이버보안 대시보드(Cybersecurity Dashboard, CSD), 그리고 호주전략정책연구소(Australian Strategic Policy Institute, ASPI)의 아·태지역 사이버성숙도(Cybersecurity Maturity in the APAC region, CSM) 등 3가지 지표를 선정하였다.

그리고 이를 통하여 주요국 5개국(미국, 일본, 영국, 독일, 노르웨이)을 도출하였다. 또한 주요국과 한국의 보호수준을 비교하기 위하여 해당 지표들의 세부항목을 기준으로 대분류 5개와 세부항목 20개로 구성된 지표를 구성하여 분석한다[22].

UN 산하의 ITU는 국제조직과 민간분야 간의 협력을 통해 사이버보안을 적극적으로 추진하고자 ABI Research와 공동으로 연구를 수행하여 GCI를 분석한 보고서를 발간하였다. 사이버보안의 인식제고와 지원 및 규제의 균형을 위하여 정부의 역할을 규명하고 사이버공간에 대한 통합적인 보안책을 마련하기 위하여 조사이다. 전 세계 193개국에 대한 사이버지표 평가 및 모범사례와 정보공유 차원에서 중요한 지표로 법제도와 조직, 국제협력, 기술, 역량구축 등 5가지로 구분되고, 각 항목별로 세부항목을 가져 총 17가지의 항목으로 구성되며 평가항목 간의 가중치는 존재하지 않는다[21].

BSA는 2015년에 EU회원국 28개국과 아시아-태평양 지역의 10개국에 대한 사이버보안 성숙도를 분석 및 평가하고자 'EU Cybersecurity Dashboard'와 'APAC Cybersecurity Dashboard'를 각각 발표하였다. 해당 보고서는 국제적인 사이버보안 표준단계를 정립하고, EU 회원국이나 아태지역 국가들에게 주변국과 비교하여 자국의 사이버보안 정책을 평가할 수 있는 기회를 제공하고자 한다. 각 주제 및 세부항목에 대한 국가별 평가는 존재하지만 전체적인 순위 및 점수는 포함하지 않은 채 공개된 정보를 기반으로 분석한다. 국가의 사이버보안 역량을 평가하기 위하여 법·제도, 운영기구, 민관협력, 분야별 상세 사이버보안 계획, 교육 등 5가지 주제의 표준항목 선정하고, 25가지의 세부항목에 대하여 4단계('있음', '없음', '부분적으로 있음', '적용할 수 없음')로 구분지어 평가를 수행한다[5][6].

Table 1. Cybersecurity International Index

Agency	ITU	BSA	ASPI
Index Name	GCI (Global Cyber security Index)	Cyber security Dash -board	Cyber security Maturity (in the APAC Region)
Publication Year	2015	2015	2012
Target	193 member state	EU 28 members, APAC 10 members	APAC 16 members
Score/ Rank	Score/ Rank	Score	Score
Criteria	5 Criteria 17 specific criteria	5 Criteria 25 specific criteria	5 Criteria 11 specific criteria
Evaluation Standard	Average	4 point scale & Sum.	Weighted

호주의 ASPI는 호주국방부의 지원으로 설립된 국방안보분야의 정책연구소로 정부와 산업 관점에서 아시아-태평양 지역의 사이버성숙도에 관련한 동향분석을 수행하고, 2014년에 분석결과를 발표하였다. 사이버정책검토가 가능하도록 하는 평가도구의 제공을 목적으로 공공 및 민간분야의 자료를 근거로 조사분석한 결과이다. 미국과 영국을 포함하여 모범사례에 대한 벤치마킹을 수행하고 한국, 북한, 호주, 중

Table 2. Critical Infrastructure Level Measurement Entry(International Index) [16]

Category	Criteria	Specific Criteria	ITU	BSA	ASPI
Law/ Policy/ Regulation	CIP Law	1. Is there a CIP law in place?	x	x	x
		2. Does the law include an appropriate definition for CIP?	x	○	x
	CIP Policy	3. Is there a CIP strategy or plan in place?	x	○	x
		4. Is there a policy that develops R&D into CIP?	x	x	x
	Risk/Threat Management	5. Does it identify security assets or manage risk/ threat?	x	○	x
		6. Does it require that security practices/ requirements be mapped to risk levels?	x	○	x
	Governance Roadmap	7. Is there a national or sector-specific governance roadmap for CIP?	○	x	x
	Security Officer	8. Is there a chief information officer (CIO) or chief security officer (CSO) on critical infrastructure?	x	○	x
Organization	CERT	9. Is there an officially launched national CERT or CSIRT?	○	○	○
	National Security Organization	10. Does it create a national organization to protect critical infrastructure?	x	x	○
	Security Incident Response System	11. Is there a management system for incident response when an event occurs?	x	○	x
		12. Is there an incident-reporting platform for collecting critical infrastructure incident data?	x	○	x
Cooperation	Public-Private Partnership	13. Are there policies, systems, communications, programs, etc. that joint public and private sectors plan in the CIP section?	○	○	○
	Intra-Agency	14. Is there a national or sectional cooperation program for sharing security assets and information?	○	x	x
	International Cooperation	15. Does it participate in global discussions on cyberspace or national/international CIP platforms/forums?	○	x	○
		16. Does it share best practice on CIP within a global body?	○	x	x
Education/ Training	Education/ Training	17. Is there education/training for strengthening knowledge about CIP?	○	○	x
		18. Is there education/training for raising public awareness of CIP?	○	○	○
Standard/ Certification	Standard/ Certification	19. Are there programs or projects for implementing CIP standards?	○	x	x
		20. Is there a system for CIP certification and accreditation?	○	x	x

* CIP: Critical Infrastructure Protection
** ○ / x : Presence or absence of item
*** Developing the research on Hyang-mi, Park (2017) in relation to the index structure and sub-index items(See [16]).

국 등 아시아-태평양지역 국가의 사이버성숙도에 대하여 평가한다. 2014년 16개국을 대상으로 시작하여 이후 연간보고서로 발간하며 2016년 23개국으로 증가하고 있다. 거버넌스, 사이버범죄, 군, 디지털 경제 및 산업, 사회참여 5가지 분야에 대해서 총 25가지 항목을 통하여 0-2점, 3-4점, 5-6점, 7-8점,

9-10점, 등 5단계로 나뉘어 평가한다[2][3][4].

앞서 설명한 3가지 국제지표를 분석하여 각 지표가 보유하고 있는 항목의 유무를 ○/x로 표시하고 이를 근거로 하여 주요기반시설의 사이버보안 수준을 측정하기 위한 세부 지표항목을 도출하였다(Table.2에서 ○이 표시된 세부항목 참조). 그리고 주요기반시설 지표로서의 타당성 및 지표 세부항목의 적정성 평가를 위하여 도출된 지표와 세부항목에 대한 전문가 조사를 실시하였다. 전문가 조사는 주요정보통신기반시설 관련 기관 소속 및 회의에 참여하는 전문가 18인(정부계 4인, 연구계 7인, 학계 5인, 산업계 2인)에게 2016년 12월 네째주 일주일간 실시하였다. 전문가 조사 결과, 지표 구조에 대한 타당성은 10점 만점에서 8.72점으로 나타났으며 세부 지표항목으로 주요기반시설 보호법 및 주요기반시설 보호기술 개발 항목이 복수의 전문가에 의해 요구되어 이를 반영하였다(Table.2에서 세부항목 1.과 4. 참조).

이상과 같이 사이버보안 관련 국제지표 비교·분석과 전문가 조사 검토를 통하여 주요기반시설의 사이버보안 수준 측정을 위해 요구되는 지표 및 세부 지표항목을 도출·구조화하고 "주요기반시설 사이버보안 지표(Critical Infrastructure Cybersecurity Index, CICI)"를 개발하였다. 새롭게 개발한 지표 CICI는 법/제도/규제 영역, 조직, 협력체계, 교육 및 훈련, 기술·표준·인증 등 5개의 대분류로 구성되며 13개의 세분류와 20개의 세부 지표항목으로 이루어져 있다(Table.2 참조).

3.2 주요국 선정

앞서 설명한 3가지 지표의 정량적 결과를 기초하여 지표별 상위그룹을 비교·분석해 주요기반시설의 사이버보안 수준 측정 시 모범으로 삼을 수 있는 주요국으로 미국, 일본, 영국, 독일, 노르웨이를 선정하였다. 미국은 EU와 아시아-태평양 지역을 대상으로 하는 BSA의 지표를 제외하고 종합적으로 가장 높은 순위를 차지하였으므로, 해당 영역의 선두주자로 볼 수 있다. ASPI의 사이버 성숙도 조사 역시 아시아-태평양의 국가를 대상으로 하지만, 벤치마킹을 위하여 미국을 포함하고 있다(2014년에는 영국도 포함함). 일본은 아시아-태평양 지역 대상으로 진행된 지표에서 상위권을 차지하고 영국 역시 3가지 지표의 상위권에 모두 나타난다. 독일과 노르웨이는 ITU의 GCI 기준으로 한국과 일본과 유사한 수준을 보유하고 있어 주요국으로 선정하였다. 최종적으로 분석을 수행하고자 미국, 일본, 영국, 독일, 노르웨이를 선정하였다.

IV. 주요기반시설 사이버보안 역량 수준 비교·분석

4.1 국내외 주요기반시설 수준 비교

국내외 주요기반시설의 사이버보안 수준을 진단하기 위하여 앞서 3장에서 구축한 지표를 활용하여 해당 수준을 측정하고자 한다.

이를 위하여 국가별 주요기반시설 보호정책을 조사하고(Table 3. 참조), 해당 정책의 추진 수준을 4단계로 단계화하고 정량적 점수로 환산하였다. 주요기반시설을 보호하기 위한 충분한 체계로 운영되고 있는 경우 5점, 주요기반시설을 보호하기 위한 체계가 구축되어 운영되고 있으나 사이버보안 체계 내에서 이루어지고 있을 경우 3점, 마찬가지로 사이버보안 체계 내에서 주요기반시설 보호체계가 구성되었으나 그 내용이 구체적이지 않고 언급만 된 정도일 경우 1점, 현재 전혀 다루어지지 않고 있는 경우 0점을 부여하였다. 상기의 점수화 기준을 기초로 하여 국가별 주요기반시설 보호정책을 분석하고([부록 2] 참조) 해당 점수의 총 합계로 국가별 수준을 비교하였다(Table 4. 참조).

주요기반시설의 보호수준을 측정하기 위한 지표를 통하여 국가별 수준을 비교·분석한 결과, 미국이 94점으로 가장 높고, 이어 일본이 88점, 영국이 76점, 독일이 73점, 한국이 68점, 노르웨이가 65점 순으로 나타난다(Table 4. 참조). 이와 같은 결과를 볼 때 다음과 같은 분석이 가능하다.

미국은 지표의 모든 분야에서 전반적으로 높은 수준임이 밝혀졌다. 국가 주도적 위험관리를 통한 보호를 핵심으로 주요기반시설 탄력성 강화를 위한 여러 정책 및 제도를 수행 중에 있으며 주요기반시설 보호를 위한 관련 주체별 기능과 역할을 명확히 한다.

이러한 보호 가치가 잘 담겨 있는 대표적인 정책으로는 국가 전체적 차원의 위험관리에 초점을 맞춘 'NIPP 2013'과 NIST의 '사이버보안 프레임워크'가 있다.

일본은 주요기반시설 보호와 관련하여 체계적인 관리를 위해 여러 정책을 추진하고 있다. 대표적으로 2006년부터 주요기반시설 정보보호를 위하여 현재

Table 3. Cybersecurity Strategy for Critical Infrastructure by Country [16]

Category	Criteria	USA	Japan	UK	Germany	Norway	Korea
Law/ Policy/ Regulation	Critical Infrastructure Protection Law	CIIA(2002), NCCIP (2013) CIPA(2016)	Cybersecurity Basic Act(2015)	Security Service Act of 1989 Data Protection Act 1998	BDSG, BSIG	National Security Act	Act on the Protection of IC Infrastructure
	Critical Infrastructure Protection Policy	NIPP	Cyber Security Strategy, CSSC	The UK Cyber Security Strategy	Cyber Security Strategy for Germany, NPSI	National Strategy for Information Security	National Cyber Security Comprehensive Measures
	Risk/Threat Management	NRE	Third Action Plan	SICS framework	National Strategy for CIP, UP KRITIS	NOU DECRIS	Vulnerability Analysis and Evaluation
	Governance Roadmap	Roadmap for Improving CI Cybersecurity	Information Security 2012 Annual Plan	The UK Cyber Security Strategy	-	-	-
	Security Officer	NIAC	Third Action Plan	GCHQ	UP Bund	-	-
Organization	CERT	US-CERT	JPCERT/CC	CERT-UK	CERT Bund	NorCERT	Kr-CERT
	National Security Organization	CTIIC, CSIS	Cybersecurity Strategic Headquarters, NISC	OCSIA BSI[1]	BSI[2]	NSM	NIS
	Security incident response system	NCIRP	JPCERT/CC	CIR, fusion Cell	-	NSM	Cyber Incident Counter Measures
Cooperation	Public-Private Partnership	CISCP	J-CSIP	CISP	UP KRITIS	-	ISAC
	Intra-agency	NCCIC, NIPP	Third Action Plan	OCSIA	IPCIP	NSM -NorCERT	-
	International cooperation	Critical 5, FIRST,	J-Initiative for Cybersecurity MERIDIAN	Critical 5, UN, ITU, NATO, FIRST	EGC, ENISA, FIRST, TERENA	FIRST	APCERT, FIRST
Education /Training	Education/ Training	FISMA	CCSF, CYDER	ACE-CSR	BSIG	CCIS	Cyber Crisis Response Training
Standard/ Certification	Standard/ Certification	NIST SP 800-160	ITMS, BCMS, CSMS	BS 7799, IISP	BSIG	ETSI	ISMS

* See [Appendix 1] Glossary for policy / organization name.

Table 4. Critical Infrastructure Cybersecurity Index(CICI) and Level Measurement

Category	Criteria	Specific Criteria	USA	JPN	UK	GER	NOR	KOR
Law/ Policy/ Regulation	CIP Law	Is there a CIP law in place?	5	3	1	5	3	5
		Does the law include an appropriate definition for CIP?	5	5	5	5	5	5
	CIP Policy	Is there a CIP strategy or plan in place?	5	5	5	5	5	5
		Is there a policy that develops R&D into CIP?	5	3	3	5	1	1
	Risk/Threat Management	Does it identify security assets or manage risk/threat?	3	5	5	3	5	5
		Does it require that security practices/requirements be mapped to risk levels?	5	5	3	5	5	3
	Governance Roadmap	Is there a national or sector-specific governance roadmap for CIP?	5	3	3	0	0	1
	Security Officer	Is there a chief information officer (CIO) or chief security officer (CSO) on critical infrastructure?	5	3	1	1	1	1
Organi- zation	CERT	Is there an officially launched national CERT or CSIRT?	5	5	3	5	3	3
	National Security Organization	Does it create a national organization to protect critical infrastructure?	5	3	5	3	3	5
	Security incident response system	Is there a management system for incident response when an event occurs?	5	3	5	3	3	3
		Is there an incident-reporting platform for collecting critical infrastructure incident data?	3	5	5	3	3	5
Cooper- ation	Public -Private Partnership	Are there policies, systems, communications, programs, etc. that joint public and private sectors plan in the CIP section?	5	5	3	5	3	3
	Intra-agency	Is there a national or sectional cooperation program for sharing security assets and information?	5	5	5	5	3	5
	International cooperation	Does it participate in global discussions on cyberspace or national/international CIP platforms/forums?	5	5	5	5	5	5
		Does it share best practice on CIP within a global body?	5	5	5	3	5	3
Education/ Training	Education/ Training	Is there education/training for strengthening knowledge about CIP?	5	5	5	3	3	3
		Is there education/training for raising public awareness of CIP?	5	5	5	3	3	3
Standard/ Certifi- cation	Standard/ Certification	Are there programs or projects for implementing CIP standards?	3	5	1	3	3	3
		Is there a system for CIP certification and accreditation?	5	5	3	3	3	3
Total			94	88	76	73	65	70

* Bold lines indicate areas that are prominent in each country when analyzing major countries.

3차까지 수립된 '정보보호 행동계획'에서는 주요기반시설의 범위를 확대하고 각 분야별 종합적인 대응 훈련을 강조한다. 또한 ISMS를 기반으로 제어시스템 대상의 '제어시스템 보안관리 시스템(CSMS) 인증제도'는 제어시스템에 대한 보안관리 시스템이 국제표준에 적합함을 객관적으로 나타낸다.

영국은 사이버 침해위협에 대응과 복원에 초점을 두어 사이버보안을 강화할 전략과 실행계획을 수립하고 지속적으로 추진하며 사이버보안 관련 전략과 실행계획, 이행 사항을 매년 점검한다. 대표적인 정책으로 서비스대응기관의 국가적 인증체계인 '사이버사고대응서비스인증(CIR)제도'를 통하여 주요기반시설 사고 전/후에 적절한 조치를 취할 수 있다.

독일은 독립적이고 체계적인 전략·계획 수립을 통해 주요기반시설의 보호 활동을 추진하고 있다. 특히 공공·민간 간의 협력을 통한 탄력성 증가와 위험관리에 초점을 맞추기 위한 '국가 주요기반시설 보호를 위한 실행계획(UP KRITIS)'은 주요기반시설의 가용성과 안정성 강화를 위하여 물리적 보호 및 IT 보안의 공동개발을 수행하며 경험 및 노하우 교환을 위하여 기관별로 협력한다.

노르웨이는 각 주요기반시설에 대한 책임기관 및 분야에 적용할 수 있는 '모든 위험 접근방식'을 취하기 위하여 해당 시설의 위험이 사회에 끼치는 영향을 조사하고, 의사결정 프로세스를 수립, 사회 인식과 다양한 위험의 수용에 대한 통찰력을 기른다. 이를 위하여 국가보안법을 기초로 주요기반시설에 대한 위험 및 의사결정 시스템(DECRIS)을 개발하여 위험 및 취약점 분석(RVA)을 수행한다.

이상으로 미국, 일본, 영국, 독일, 노르웨이와 한국의 주요기반시설 수준을 비교·분석하였다. 분석결과의 검증과 관련하여서는 주요기반기설 수준 측정 비교가 가능한 이전 논의나 별도의 지수·지표 혹은 관련 데이터가 존재하지 않고 사이버보안 수준 및 주요기반시설 제어시스템의 보유수와 주요기반시설 취약점 빈도 등과의 상관성 분석 결과, 상관성이 아직 파악되지 않아서 별도의 연구를 통한 검증이 요구된다[16][1].

또한 본 연구는 주요기반시설 보호수준 측정 시 보호를 위한 모든 활동을 분석대상으로 삼지 못하고 공개된 데이터를 기초로 하여 항목별 정량적 수치만을 비교·분석하였다. 이에 정량적 분석 시 항목 간의 가중치를 설정하고 관련 정책의 실효성이나 범위를 포함하는 등 정성적 분석을 도입하여, 보다 포괄적이고 체계적인 기준을 설정하여야 한다. 그리고 주요기반시설의 영역별, 수준별 진단을 할 수 있는 방안에 대하여 추가적인 연구가 진행되어야 한다.

4.2 한국 분석

한국은 정보통신기반 보호법을 중심으로 주요기반시설을 보호하기 위한 기본체계가 잘 구축되어 있고[27], 또한 국제지표를 통하여 객관적인 관점에서 사이버보안과 관련한 기본적인 역량 수준도 높다. 하지만 변화하는 환경에 적절한 대응책을 적용하지 못하고 기존의 폐쇄망을 사용하는 주요기반시설에 대한 보호체계만을 구축하여 운영하고 있다.

따라서 주요기반시설의 환경변화에 대응하여 포괄적인 보호정책 및 제도에 대한 준비가 시급하다. 미국은 국가 전체차원의 순환적 구조를 띈 위험관리 프레임워크를 운영하며 주요기반시설의 물리적, 사이버적, 인적 요소를 식별하고 일정 단계에 걸쳐 관리한다. 일본의 제3차 행동계획은 주요기반시설의 위험관리를 진행하기 위하여 사전에 환경에 대한 분석을 수행하고 전(前)기에 수행된 결과와 비교하여 변화된 양상을 즉각적으로 적용하여 관리한다. 영국은 국가적 차원에서 보안사고의 발생 시 대응하기 위한 기관을 선정하는 과정에서 기관인증 제도를 도입하여 즉각적인 대응과 해당 사고에 대한 정보공유를 통하여 기존의 보호제도를 개선해나간다. 노르웨이의 보안관

1) 참고로, 사이버보안 수준 측정이 체계화되고 분석 대상 주요국이 모두 포함된 ITU의 GCI 결과를 보면, 사이버보안 수준에 있어서 미국이 1위, 노르웨이가 뉴질랜드와 함께 공동 4위, 그리고 일본, 영국, 독일, 한국이 공동 5위로 동일한 수준으로 나타났다[21].
반면, Infracritical(2014)의 SHINE(SHodan INtelligence Extraction) 프로젝트를 보면, 제어시스템 관련 전체 취약점 1,828,360개 중 미국이 616,994개 보유하여 전체 취약점 수의 34%를 차지하며 독일이 15%, 한국이 5.4%, 영국이 3.62%, 일본이 1.86%, 노르웨이가 1.56% 차지하는 것으로 나타났다[20].
그리고 Positive Technologies(2014)의 SCADA Safety in Numbers를 보면, 제어시스템이 취약한 국가 중 스위스를 기준(100%)으로 영국 60%, 미국 41%, 한국 32%, 독일 20% 순으로 취약한 것으로 나타나고 있으며 일본, 노르웨이는 대상국가에서 제외되어[33] 주요기반시설에 대한 위협과 준비도 등에 대한 비교 및 검증은 어렵다. 이에 주요기반시설에 대한 종합적인 국제비교가 가능한 지표를 필요로 하고 있다.

리 체계는 단순히 주요기반시설에 직접적으로 관련되는 보호에만 집중하는 것이 아니라 해당 시설의 영역별 특성과 현재의 수준을 고려하는 등 환경적 특성을 고려하여 보호한다.

그러나 한국의 보호정책은 기존의 폐쇄적인 환경에서 수립한 체계에 머물러 있으므로 주요기반시설을 보호하기 위하여 변화하는 환경에 적합하게 개선해야 한다. 즉, 단순히 시설에 대한 보호가 아닌 포괄적인 대응체계에 대한 준비가 필요하다.

V. 결 론

주요기반시설의 환경이 변화함에 따라 그 영역이 사이버공간으로까지 확대되었고, 점차 증가하는 주요기반시설 대상의 사이버위협이 국가에 미치는 사회·경제적인 피해의 범위와 영향 또한 증가하였다. 그러나 주요기반시설의 보호조치는 기존 환경에서 수립된 채로 유지되고 있어 새로운 위협에 대응하지 못하고 있다.

이에 본 연구는 주요기반시설의 새로운 위협에 대응하기 위한 방향을 제시하고자 주요기반시설 국제지표를 개발하고 항목별 비교분석을 통해 주요국과 한국의 주요기반시설 사이버보안 수준을 분석하였다.

본 연구를 위하여 사이버보안의 수준을 측정하는 많은 국제지표 중 일정 기준(정량적 결과 여부, 점수화/순위, 구체적 항목의 존재여부)에 따라 선정한 3가지 지표(ITU - GCI, BSA - Cybersecurity Dashboard, ASPI - Cybersecurity Maturity in the APAC region)를 기초로, 주요 5개국(미국, 일본, 영국, 독일, 노르웨이)을 선정하였다. 또한 3가지 지표의 세부항목을 기준으로 주요기반시설의 환경적인 측면을 포함하여 다방면적으로 보호 수준을 측정할 수 있는 주요기반시설의 사이버보안수준을 측정하기 위한 지표를 구성해 주요국과 한국을 비교하였다.

기존 연구는 주요기반시설의 사이버보안수준을 측정하기 보다는 국가별 사이버보안 현황을 파악하거나 주요기반시설에 대한 개별 정책 함의 분석에 중점을 두고 있다. 그러나 최근 주요기반시설에 대한 침해 및 공격은 사이버공간에 대한 무장공격과 같은 수준으로 각 국가별로 중요성과 파급효과를 심각하게 인식하며 사이버전에 대한 대비와 사이버공간에서의 국가 영향력을 보유하기 위해 노력하고 있다. 또한 원자력과 같은 주요기반시설에 대한 일정수준 이상의 공격은 자국뿐만 아니라 주변국에도 피해를 입힐 수 있으므로 사이버보안 수준을 유지하는 것은 국가 간의 신뢰관계에도 중요하다. 이에 본 연구는 주요기반시설의 사이버보안수준을 측정하고 이를 향상시키기 위한 지표를 법/정책/규제와 조직, 협력체계, 교육·훈련, 표준·인증 등 다양한 측면을 고려하여 체계화하였다는 점에서 의미가 있다.

마지막으로 본 연구에서 개발한 주요기반시설 사이버보안 지표(CICI)가 주요기반시설 정책 추진의 기반 틀로서 활용되고 더 나아가 국제지표화 되어 국가 간의 사이버신뢰 구축의 근거자료로도 활용되기를 기대한다.

References

〔1〕 Akcaraz, Cristina & Zeadallly, Sherali. “Critical Infrastructure Protection: Requirements and Challenges for the 21st Century”, *International Journal of Critical Infrastructure Protection*. Vol.8. 2015

〔2〕 ASPI, “Cyber Maturity in the Asia-Pacific Region.”, 2014

〔3〕 ASPI, “Cyber Maturity in the Asia-Pacific Region.”, 2015

〔4〕 ASPI, “Cyber Maturity in the Asia-Pacific Region.”, 2016

〔5〕 BSA, “EU Cybersecurity Dashboard”, 2015

〔6〕 BSA, “APAC Cybersecurity Dashboard”, 2015

〔7〕 Cavelty, Myriam Dunn; Suter, Manuel, “The art of CIIP strategy: tacking stock of content and processes”, Critical Infrastructure Protection. *Springer Berlin Heidelberg*, pp. 15-38, 2012.

〔8〕 Cho-rom Ham, “A Proposal on Improvement of the Countermeasures to Protect Critical Information Infrastructure”, Graduate School of SoonChunhyang University, 2016

〔9〕 CTO. “Critical Information Infrastructure Protection(CIIP) Emerging Challenges for Developing

Countries", 2015
〔10〕 DHS, "NIPP 2013: Partnering for Critical Infrastructure Security and Resilience", 2013
〔11〕 Dong-Yeon Park, "A Study on Improvement of Evaluation Criteria of Managerial · Physical Vulnerability Analysis", Graduate School of Korea University, 2014
〔12〕 Do-seok Han, Deok-ho Han, Heung-youl Youm, "A Comparative Study on Domestic Act on the Protection of Information and Communications Infrastructure and Japanese Cyber Security Basic Law", *Journal of the Korea Institute Of Information Security & Cryptology*, 25(3), pp. 44-51, Jun. 2015
〔13〕 Do-Yeon Kim, "Vulnerability Analysis for Industrial Control System Cyber Security", *The Journal of the Korea institute of electronic communication sciences*, 9(1), pp. 137-142, 2013
〔14〕 ENISA, "Norway Country Report", 2010
〔15〕 Federal Republic of Germany, "National Strategy for Critical Infrastructure Protection", 2009.
〔16〕 Hyang-mi, Park, "A Study on Developing International Level Measure Index for Strengthening Cybersecurity Capability of Critical Infrastructure", Graduate School of Sangmyung University, 2017.
〔17〕 Hyo-Bin Bae, Jung-Ho Eom, Tae-Kyoung Kim, Tai-Myoung Chung, "The Customized Scheme Structure for Prevent Cyber Threats on the Critical Information and Communication Infrastructure", *Journal of Security Engineering*, 10(6), pp. 643-654, 2013
〔18〕 Hyun-ju Lee, "The Study On Security Enhancement of National Control System For Critical Infrastructure - Focusing On Comparison About Policy Of Major Countries And Domestic -", Graduate School of Sangmyung University, 2016
〔19〕 I-news(2016.12.22.), Urgency of social infrastructure security management http://news.inews24.com/php/news_view.php?g_serial=997828&g_menu=020200
〔20〕 Infracritical, "Project SHINE Finding Report", 2014.
〔21〕 ITU and ABI Research, "Global Cybersecurity Index & Cyberwellness Profiles", 2015.
〔22〕 ITU, "Cybersecurity Index of Indices", 2015.
〔23〕 Journal of Kosca(2016.12.07.), "Serious situation of safety management on critica l infrastructure ... 97 of the Board of Audit " http://www.koscaj.com/news/articleView.html?idxno=91973
〔24〕 Kil-hwan Im, "Control system security vulnerabilities and countermeasures", Graduate School of Korea University, 2011
〔25〕 Korea Internet & Security Agency(KISA), "2014 National Information Protection White Paper."
〔26〕 Korea Internet & Security Agency(KISA), "2015 National Information Protection White Paper."
〔27〕 Korea Internet & Security Agency(KISA), "2016 National Information Protection White Paper."
〔28〕 Korea Internet & Security Agency(KISA), "A Study on the Infrastructure Protection Law System in the United States, UK and Germany", KISA-RP-2010.0054, Dec. 2010
〔29〕 Myeong-gil Choi, "A Study on Security Evaluation Methodology for Industrial Control Systems", *Journal of the Korea Institute of Information Security & Cryptology*, 23(2), pp. 287-298, Apr. 2013
〔30〕 National Law Information Center, 「Act on the Protection of Information and Communications Infrastructure」
〔31〕 NIST, "Framework for Improving Critical

Infrastructure Cybersecurity", 2014
〔32〕 Norwegian Ministries, "Cyber Security Strategy for Norway", 2013
〔33〕 Positive Technologies, "SCADA Safety in Numbers", 2014.
〔34〕 Sang-hyun Jang, "A Study on the Critical Infrastructure Information Security Level Assessment Improvements", Graduate School of Dongguk University, 2015
〔35〕 Stefan Brem, "Critical Infrastructure Protection from a National Perspective", *Symposium on Critical Infrastructures*, 2015, pp.191
〔36〕 Sun-ha Bae, Sang-don Park, So-jeong Kim, "A study on the Development for the National Cybersecurity Capability Assessment Criteria", *Journal of the Korea Institute of Information Security and Cryptology*, 25(5), pp. 1293-1314, Oct. 2015
〔37〕 UP KRITIS, "Public-Private Partnership for Critical Infrastructure Protection", 2014

〔 부록 1 〕 용어 정리

1. United State America/USA(미국)

CIPA: Critical Infrastructure Protection Act
NCCIP: National Cybersecurity and Critical Infrastructure Protection Act
CIIA: Critical Information Infrastructure Act
NRE: National Risk Estimate
NIST Roadmap for Improving Critical Infrastructure Cybersecurity 2014
NIAC: National Infrastructure Advisory Council
CTIIC: Cyber Threat Intelligence Integration Center
CSIS: Center for Strategic and International Studies
NCIRP: National Cyber Incident Response Plan
CISCP: Cyber Information Sharing and Collaboration Program
NCCIC: The National Cybersecurity & Communications Integration Center
NIPP: Nation Infrastructure Protection Plan
FIRST: Forum of Incident Response and Security Teams
FISMA: Federal Information Security Modernization Act
NIST SP: NIST Special Publications

2. Japan/JPN(일본)

CSSC: Control System Security Center
Third Action Plan: Third Action Plan Related to Cyber Security of Critical Infrastructure
NISC: National Information Solution Cooperative
J-CSIP: Initiative for Cyber Security Information sharing Partnership of Japan
CCSF: Common Career Skill Framework
CYDER: Cyber Defence Exercise with Recurrence
ITSMS: IT Service Management System
BCMS: Business Continuity Management System
CSMS: Cyber Security Management System

3. United Kingdom/UK(영국)

BSI[1]: British Standard Institution
GCHQ: Government Communications Headquarters
OCSIA: The Office of Cyber Security and Information Assurance
CIR: Cyber Incident Response Management
CISP: Cyber-security Information Sharing Partnership
IISP: The Institute Of Information Security Professionals

4. Germany/GER(독일)

BDSG: Federal Data Protection Act (Bundesdatenschutzgesetz)
BSI[2]: Bundesamt für Sicherheit in der Informationstechnik
BSIG: Bernische Systematische Information Gemeinden
NPSI: National Plan for the Protection of Information Infrastructure (Nationaler Plan zum Schutz der Informationsinfrastrukturen)
EGC: European Geothermal Congress
TERENA: The Trans-European Research and Education Networking Association

5. Norway/NOR(노르웨이)

NOU: Norges Offentlige Utredninger
RVA: Risk and Vulnerability Analysis
DECRIS: Risk and Decision Systems for Critical Infrastructures
NSM: National Security Authority
CCIS: Center for Cyber and Information Security
ETSI: European Telecommunications Standards Institute

6. Korea/KOR(한국)

NIS: National Intelligence Service
ISAC: Information Sharing & Analysis Center
APCERT: Asia-Pacific CERT
ISMS: Information Security Management System

〔 부록 2 〕 점수화 분석 기준

Category	Criteria	USA	Japan	UK	Germany	Norway	Korea
Law/ Policy/ Regulation	CIP Law	CIP 중심의 법률이 수립되어 있음	사이버보안 관련 법률 내에 CIP가 포함됨	보안 법률 내에 CIP가 포함됨	CIP 중심의 법률이 수립되어 있음	국가보안법률에 CIP가 포함되어 있음	CIP 중심의 법률이 수립되어 있음
		법률 내에 CIP 정의가 명시됨	법률 내에 CIP 정의가 명시됨	법률 내에 CIP 정의가 명시됨	법률 내에 CIP 정의가 명시됨	법률 내에 CIP 정의가 명시됨	법률 내에 CIP 정의가 명시됨
	CIP Policy	CIP 중심의 전략이 수립되어 있음	CIP 중심의 전략이 수립되어 있음	CIP 중심의 전략이 수립되어 있음	CIP 중심의 전략이 수립되어 있음	CIP 중심의 전략이 수립되어 있음	CIP 중심의 전략이 수립되어 있음
		CIP 관련 R&D 개발 명시함	사이버보안 관점의 R&D 제시	정보보호 관점의 R&D 제시	CIP 관련 R&D 개발 명시함	CIP 관련 R&D 개발 내용 없음	CIP 관련 R&D 개발 내용 없음
	Risk/ Threat Manage-ment	사이버보안 중심의 위험관리 체계구축	CIP 중심의 위험관리체계 구축	CIP 중심의 위험관리체계 구축	사이버보안 중심의 위험관리 체계구축	CIP 중심의 위험관리체계 구축	CIP 중심의 위험관리체계 구축
		위험수준별 보안조치 시행	위험수준별 보안조치 시행	사이버보안 관점의 수준별 보안조치 시행	위험수준별 보안조치 시행	위험수준별 보안조치 시행	위험수준별 보안조치 명시
	Gover-nance Roadmap	CIP 관련 거버넌스 로드맵 수립	사이버보안 관련 거버넌스 로드맵 수립	사이버보안 관련 거버넌스 로드맵 수립	수립되지 않음	수립되지 않음	로드맵 계획만 존재함
	Security Officer	CIP를 위한 CIO/CSO 지정 명시	사이버보안 CIO/CSO 지정 명시	별도의 책임자 지정 X	별도의 책임자 지정 X	별도의 책임자 지정 X	별도의 책임자 지정 X
Organi-zation	CERT	CIP 중심의 CERT	CIP 중심의 CERT	사이버보안 중심 CERT	CIP 중심의 CERT	사이버보안 중심 CERT	사이버보안 중심 CERT
	National Security Organi-zation	CIP 중심의 국가조직 구축	사이버보안 중심 국가조직	CIP 중심의 국가조직 구축	사이버보안 중심 국가조직	사이버보안 중심 국가조직	CIP 중심의 국가조직 구축
	Security incident response system	사고발생 시 즉각적인 대응체계 구축	사고발생 시 대응체계 구축	사고발생 시 즉각적인 대응체계 구축	사고발생 시 대응체계 구축	사고발생 시 대응체계 구축	사고발생 시 대응체계 구축
		대응센터 구축	사고데이터 기록	사고데이터 기록	대응센터 구축	대응센터 구축	사고데이터 기록
Coopera-tion	Public Private Partner-ship	CIP 영역 내 민관협력 체계 구축	CIP 영역 내 민관협력 체계 구축	사이버보안 영역 내 민관협력 체계 구축	CIP 영역 내 민관협력 체계 구축	사이버보안 영역 내 민관협력 체계 구축-	사이버보안 영역 내 민관협력 체계 구축
	Intra agency	국가 내 보안 자산공유 체계	국가 내 보안 자산공유 체계	국가 내 보안 자산공유 체계	국가 내 보안 자산공유 체계	국가 내 협력체계 구축	국가 내 보안 자산공유 체계
	International cooperation	국내외 CIP 포럼 참가	국내외 CIP 포럼 참가	국내외 CIP 포럼 참가	국내외 CIP 포럼 참가	국내외 CIP 포럼 참가	국내외 CIP 포럼 참가
		CIP 관련 모범사례 공유	CIP 관련 모범사례 공유	CIP 관련 모범사례 공유	보안 관련 모범사례 공유	CIP 관련 모범사례 공유	보안 관련 모범사례 공유
Education/ Training		CIP 관련 교육 시행	CIP 관련 교육 시행	CIP 관련 교육 시행	사이버보안 교육 시행	사이버보안 교육 시행	사이버보안 교육 시행
Standard/ Certification		CIP 표준 제시	CIP 표준의 지속적 개발	실제 운영 X	CIP 표준 제시	CIP 표준 제시	CIP 표준 제시
		CIP 인증체계	CIP 인증체계	사이버보안 인증체계	사이버보안 인증체계	사이버보안 인증체계	사이버보안 인증체계

〈저자소개〉

박 향 미 (Hyang-mi Park) 학생회원
2015년 2월: 상명대학교 경영학과 졸업
2015년 2월~현재: 상명대학교 일반대학원 지식보안경영학과 석사과정
〈관심분야〉 산업보안, 사이버안전, 정보보호, 개인정보보호

유 지 연 (Ji-yeon Yoo) 종신회원
2012년 2월: 고려대학교 정보경영공학 박사
1999년 11월~2013년 2월: 정보통신정책연구원 부연구위원
2014년 3월~현재: 상명대학교 일반대학원 지식보안경영학과 조교수
〈관심분야〉 사이버안전, 융합보안, 위험관리, 정보보호, 개인정보보호