국가전략연구위원회 이슈브리핑 5호 (발간일: 2023.06.19.)

일본의 사이버 국가책략과 국제협력[1)]

윤대엽 (대전대학교)

1. 문제제기: 아날로그 일본의 사이버 안보

아베 내각은 전후 구속에서 탈피한 안보개혁의 전환점이 되었다. 사이버 안보전략도 포괄적 안보개혁의 핵심 과제로 추진되었다. 아베 내각은 2013년 동북아 국가 중 가장먼저 사이버 위협의 주체와 대상을 명시한 사이버 안보전략을 발표했다,[2)] 2014년에는 '사이버시큐리티기본법(이하 사이버기본법)'을 제정하고 사이버 안보전략을 제도화했다. 사이버기본법을 근거로 신설된 '사이버시큐리티전략본부'는 사이버안보를 총괄한다. 사이버안보 정책기구의 개편 이후 일본의 사이버 안보전략은 정보수집, 분석능력에 집중했던 정보보호를 넘어 적극적 방어와 공세적 개념으로 전환되고 있다. 2023년 2월 기시다 내각은 내각관방에 사이버안전보장체제준비실(サイバー安全保障体制整備室, 이하 사이버안전실)을 신설했다. 사이버안전실은 2021년 '사이버시큐리티전략'에 사이버 위협에 대한 사전적, 적극적 예방조치를 목표로 하는 '능동적 사이버 방어(能動的サイバー防御)'의 세부방안을 검토하기 위해 설치된 것이다 (GoJ 2021, 37)

1) 이 글은 2023년 6월 13일 제2차 국가전략포럼에서 발표된 발표문을 수정보완한 것이다.
2) 중국은 2015년 국가보안법에 사이버공간이 국가안전의 중요현안임을 명시하고, 사이버안전을 총괄하는 '중앙 사이버보안 및 정보화위원회'를 출범했다. 2016년 중국 최초의 사이버안전전략인 '국가사이버공간 보안전략(国家网络空间安全战略)을 발표하고 2017년에는 '사이버보안법'을 제정했다. 2003년

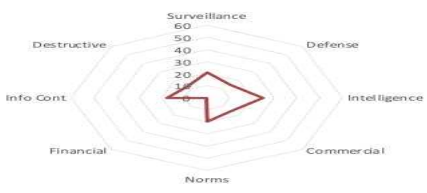
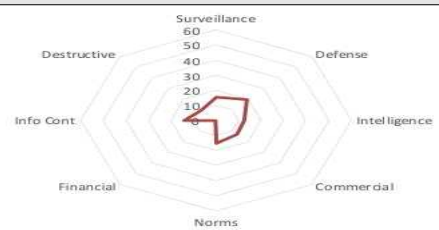
<표 1> IMD 디지털 경쟁력 순위, 2018-2022

구분	종합		2022년 순위		
	2018	2022	지식	기술	미래준비
일본	22	29	28	30	28
한국	14	8	16	13	2
중국	30	17	17	18	15
홍콩	11	9	7	2	18
대만	16	11	18	6	8

자료: IMD, IMD World Digital Competitiveness Ranking 2022

흥미로운 것은 동아시아에서 사이버 공간을 안보화하고 국가전략을 선도한 일본의 사이버 전략이 디지털 경제의 성숙보다 선행했다는 점이다. 일본사회는 디지털 위험(digital risk)보다 아날로그 사회의 변혁(transform)을 고민하고 있다. IMD의 2022년 디지털 경쟁력 순위에 따르면 일본의 사이버 경쟁력 순위는 동아시아 주요국 중 최하위에 위치하고 있다. 특히 2018년 22위로 평가되었던 일본은 2022년 29위로 오히려 순위가 하락한 반면, 한국은 14위에서 8위, 중국 역시 30위에서 17위로 상승했다. 디지털, 지식, 기술, 미래준비 등의 세부 평가지표에서 일본은 모두 동아시아 국가대비 경쟁력이 하락한 것으로 평가되었다(IMD 2022). 하버드대 벨퍼센터에서 발표하는 사이버파워 지수에서도 중국(2위) 및 한국(7위)에 비해 낮은 15위로 평가되었다. 특히, 사이버 안보부문의 재정(finance), 감시(surveillance), 첩보(intelligence), 방어(defence), 물리적, 비물리적 사이버 공간의 통제를 위한 법제와 정책의 경우 조사대상 30개국 중 중하위권으로 평가되었다(Voo et al. 2022). 국제전기통신연합(ITU)에서 법률, 기술, 조직, 역량, 협력 등을 기준으로 평가하는 2020년 사이버안보지수(Cybersecurity Index)의 경우 한국은 4위, 일본은 7위로 평가되었다 (ITU 2020).

<표 2> 사이버 파워 지수 2022 (단위: 순위)

한국	일본
	

구분	종합	재정	감시	첩보	통상	방어	법제	공격	규범
한국	7	15	8	7	5	22	9	11	7
일본	15	20	22	16	6	13	13	14	11
중국	2	2	1	2	1	21	3	3	4

자료: Voo, et al(2022), National Cyber Power Index 2022

일본사회의 구조화된 아날로그 시스템은 코로나-19 위기를 거치면서 국가적인 과제로 인식되었다. 코로나-19로 대면업무가 제한되었지만 서류 및 전표, 날인 관행으로 재택근무가 제한되었다. 문서중심의 업무관행으로 재난지원금의 지급에 혼선이 발생하거나 백신패스의 도입도 지연되었다. 인식, 관행은 물론 교육 및 경제의 디지털 기반도 취약하다. 2020년 기준 대학에 개설된 소프트웨어 관련 프로그램은 29개로 미국의 117개와 비교하여 25% 수준에 불과하다, 이커머스(e-commerce) 및 모바일뱅킹 이용비중은 각각 9%, 6.9%로 중국의 24%, 35.2%보다 낮다. 또 디지털정부 이용비중(7.5%)이나 스마트시티 (79위, 도쿄) 순위 역시 OECD 국가와 비교하여 낮은 수준에 머물러있다 (Mckinsey & Company 2021). 저출산, 고령화로 인한 인구구조의 변화를 겪고 있는 일본에서 디지털 전환의 지체는 생산성 하락, 경쟁력 하락으로 연계되어 장기침체를 구조화하는 요인이다. 스가 내각은 아베노믹스의 하나로 2018년부터 추진된 'society 5.0'을 강화하여 디지털 변혁(digital transformation)을 추진했다. 이를 위해 2000년 제정된 IT기본법을 폐지하고 '디지털사회형성기본법'을 제정하고, 2021년에는 디지털정책을 총괄하는 디지털청을 신설했다. 디지털청은 행정, 교육, 사회의 디지털 전환은 물론 사이버 안보와 디지털 개혁 정책을 총괄한다.

안보, 경쟁, 협력이 상호 포괄적으로 결부되어 있는 사이버 국가책략(cyber statecraft)의 시각에서 일본의 사이버 안보전략은 어떤 과정을 거쳐 변화되고 추진되어 왔는가? 동아시아에서 사이버 안보전략을 주도한 일본이 디지털 경제와 기술경쟁에 앞서 사이버 공간 안보화가 우선했던 원인은 무엇인가? 일본의 사이버 안보전략에서 국제협력의 규범과 목적은 어떻게 제시되어 왔는가?

2. I사이버 국가책략과 일본: 접근시각

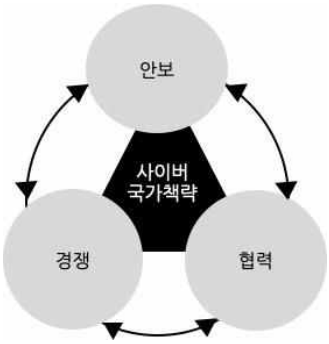
사이버 전략은 디지털 기술, 기반, 이를 활용한 데이터 경제의 확장에 따른 총체적 현안이자, 정부, 기업, 개인은 물론 국가전반(whole of nations)의 총체적 과제다. 디지털 기술의 발전에 따라 물리적, 가상의 공간은 경제적, 정치적, 사회적 현안이 연계되어 왔다. E, Net, Digital 등과 혼재되어 개념화되는 사이버 공간은 (1) 디지털 플랫폼(컴퓨터, 디지털기기, 센서 등), (2) 우주공간을 포함하는 디지털 네트워크(5G, IoT, 우주인터넷 등), 그리고 (3) 디지털 인프라에서 생산, 교환, 축적되는 데이터로 구성된다(Kello 2013). 4차 산업혁명은 포괄적인 국가책략(statecraft) 차원의 사이버 전략을 가속화하고 있다. 첫째, 센서혁명(sensor revolution)이다. 화학적, 생물학적, 전기적, 광학적 원리에 따라 감시, 측정하여 전기적, 광학적 신호로 변환하여 출력하는 센서는 측정뿐만 아니라, 통신 및 인공지능 기술을 포함하는 스마트 센서로 발전하고 있다 (김응수 2023). 둘째, 디지털 기기를 연결하는 5G, 사물인터넷, 우주인터넷 기술이 물리적, 가상의 사이버 공간을 확장한다. 셋째, 네트워크화 된 디지털 플랫폼을 기반으로 생산, 소비, 교환되는 데이터 경제다. 4차 산업혁명의 핵심은 빅데이터, 사

물인터넷과 인공지능이 거대한 데이터 경제를 구축하는 것이다. 데이터 서비스의 시장화는 디지털 경제로의 전환은 물론 우주공간의 상업화라는 뉴스페이스혁명의 핵심 동력이다.

사이버 전략은 디지털 기술변화와 이에 수반되는 다층적인 위협양상 따라 안보화 되어 왔다. 사이버 공간의 안보화 담론을 주도한 것은 미국이다. 미국에서 보호(protection) 목적의 법제가 제도화된 것은 1996년 클린턴 행정부가 제정한 '국가정보기간시설보호법(National Information Infrastructure Protection Act)'이다. 동 법은 컴퓨터를 활용한 정보탈취를 범죄로 규정했다. 클린턴 행정부는 1998년 대통령정책지시(Presidential Policy directive) 63호를 통해 정보 네트워크에 의존하는 국가기반시설의 취약성을 보호하는 국가차원의 체계구축을 시작했다. 2000년에 개정된 '정부정보보안개혁법'은 정보시스템과 데이터 위협에 대한 주기적인 위협평가와 대응을 규정하고 있다(변진석 2022). 보호와 인식 차원의 사이버 독트린이 사이버안보(Cybersecurity) 차원의 전략으로 전환된 것은 부시 행정부다. 9/11 테러는 테러집단에 의한 비군사적 위협에 대응하기 위해 사이버 안보를 안보문제로 격상시키는 계기가 되었다. 부시 행정부는 사이버 공격에서 국가기간시설의 보호하는 것은 물론 정보부문혁신(RIA)을 추진했다. 2003년 국토안보부가 발표한 '사이버 안보를 위한 국가전략(National Strategy to Secure Cyberspace)'은 사이버 공격의 취약성을 방어하고, 사이버 공격을 억지하며, 사이버 공격에 대응하는 포괄적인 사이버 전략이 제시되었다. 그리고 2015년 개인정보보호와 정보공유와 관련한 논란 끝에 사이버안보법, 국가사이버안보증진법 및 사이버안보 정보공공유법이 제정되었다. 특히 사이버안보정보공유법은 정부와 민간에 대한 정보공유체계를 구축했다는 의미가 있다(변진석 2022).

그러나, 사이버 전략은 보호와 안보에 국한되지 않는다. 사이버 영역은 1차적으로 디지털 인프라의 확장과 함께 네트워크화 된 국가전반의 전략적 자산도 연계되어 있다. 초연결된 사이버 영역은 사이버 공간 내·외부는 물론 국경도 부재한다. 더구나 경제, 사회, 정치, 문화 등 사회체계 전반이 디지털 또는 사이버 공간의 데이터에 의존하고 있다. 사이버 전략은 (1) 물리적, 비물리적 공간과 데이터의 안전은 물론, (2) 경제사회 전반의 혁신을 위한 디지털 생태계를 구축하고, (3) 규범과 제도에 의한 국제협력 과제를 포괄한다. 이 때문에 사이버 전략을 사이버 국가책략(cyber statecraft)로 포괄적으로 재정의해야 한다는 문제가 제기되어왔다. 국가책략이 국가목표를 달성하기 위한 국정전반(state affairs)의 숙련된 관리를 의미한다면, 사이버 국가책략은 사이버 공간에서 국가주권을 보호하고, 규범과 거버넌스를 구축하며, 갈등을 통제, 거부함으로서 정보와 데이터의 자유로운 이동을 보장하는 국정관리'로 규정할 수 있다(Healey 2011). 이는 조셉 나이(Nye 2010)가 사이버 공간에서 물리적, 비물리적 수단을 통해 국가적인 이점을 활용하고 영향력을 행사하는 사이버 파워(cyber power) 전략을 포함한다.

<표 3> 사이버 국가책략의 영역



안보	▪ 사이버 공간의 안보화 ▪ 디지털 인프라, 국가전략시설, 데이터의 보호 ▪ 사이버 방어, 억지, 공격
경쟁	▪ 사이버 공간의 시장화 ▪ 디지털 플랫폼, 네트워크, 데이터 기술 ▪ 디지털 산업육성과 경쟁
협력	▪ 사이버 공간의 거버넌스 ▪ 사이버 공간의 규범, 표준, 제도 ▪ 사이버 외교, 협력, 공적개발원조(ODA)

사이버 국가책략은 안보, 경쟁. 협력 세 가지 영역으로 구분할 수 있다. 첫째, 안보는 사이버 공간의 안보적 쟁점이다. 사이버 범죄로부터 디지털 인프라, 네트워크화 된 국가전략 시설 및 데이터의 보호를 목표로, 방어, 억지, 공격 등의 전략이 발전되어 왔다. 둘째, 경쟁은 사이버 공간의 시장화와 기술적 현안이다. 4차 산업혁명 기술의 혁신에 따라 사이버 전략은 디지털 기반의 구축뿐만 아니라, 디지털 데이터의 활용이 중요해지고 있다. 디지털 기술의 개발과 함께 데이터 경제의 육성과 보호를 위한 경쟁은 사이버 국가책략의 핵심 현안이다. 마지막으로 협력이다. 사이버 공간은 물리적, 비물리적 공간을 통합하는 공간의 소멸을 의미한다. 데이터의 자유롭고 안전한 교환이 국제협력의 핵심 과제다. 더구나 디지털 네트워크는 국가 이외에 기업, 비영리 단체, 개인의 복합적인 이해가 상호의존 또는 대항적으로 연결됨에 따라 사이버 법치, 신뢰구축(CBMs), 역량구축을 위한 외교, 원조와 협력이 중요해지고 있다(이상현 2022).

3. 일본의 사이버 국가책략

안보, 경쟁, 협력이 상호 중첩되어 있는 사이버 국가책략의 맥락에서 일본은 사이버 전략은 안보화 담론이 우선되었다는 특징이 있다. 일본에서 사이버 안보와 관련 정책기구가 제도화된 것은 2000년 제정된 '고도정보통신 네트워크사회 형성 기본법(高度情報通信ネットワーク社會形成基本法, 이하 IT기본법)이 제정된 이후다. 동법 제22조를 근거로 2000년 정보시큐리티대책추진회의가 설치되었고, 2005년에는 정보시큐리티센터(NISC)를 신설하고 정보시큐리티전략의 정책실무를 담당했다. 사이버시큐리티정책회의 설치 이후 사이버 안보목적의 3년 단위의 국가전략이 발표되기 시작했다. 2006년 이후 2010년까지 3차례 발표된 전략은 (1) IT기본법을 근거로 '정보시큐리티'를 정책개념으로 사용하고 있으며, (2) 정보 및 디지털 기반의 보호중심의 정책목표가 제시된, (3) 사이버 공간의 범죄, 공격으로 인한 손실을 최소화하고 경제적 손실을 최소화하는 '사이버 안보가 전통 안보화'된 시기라는 특징을 가진

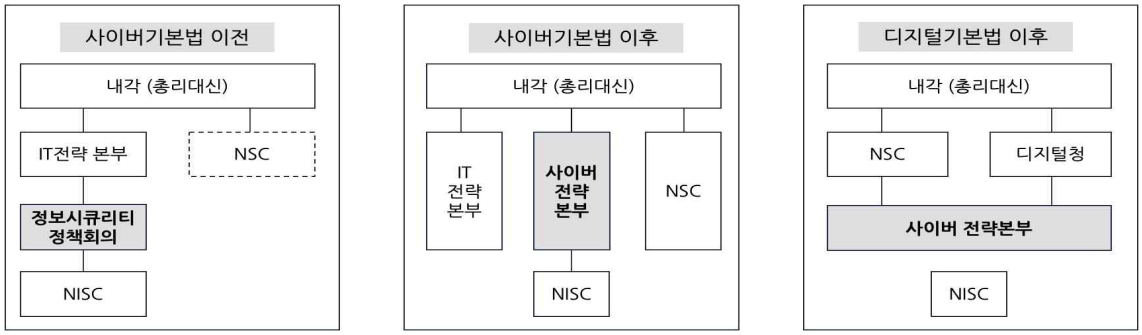
다(이승주 2017).

<표 4> 일본의 사이버 관련 법제, 전략 및 정책구조의 변화

구분	법제와 정책기구		정책구조
안보화 담론	법제	IT기본법(2000)	정책회의, IT전략본부 산하에 설치된 회의체
	기구	정보시큐리티대책추진회의(2000) 정보시큐리티대책추진실(2000) 정보시규리티센터(2005) 정보시큐리티정책회의(2005)	
	전략	정보시큐리티 국가전략(2006) 정보시큐리티 국가전략(2009) 정보시큐리티전략 (2010)	
군사적 담론	법제	사이버시큐리티기본법(2014)	전략본부 신설, IT전략본부와 동일한 지위
	기구	사이버시큐리티전략본부(2015)	
	전략	사이버시큐리티전략(2013) 사이버시큐리티전략(2015) 사이버시큐리티전략(2018)	
디지털 전환	법제	디지털기본법(2021)	디지털청과의 협력관계
	기구	디지털청(2021)	
	전략	사이버시큐리티전략(2021)	

아베 2기 내각(2012-2020)은 2013년 기존 '정보'시큐리티를 '사이버'시큐리티로 변경한 사이버 국가전략을 발표했다. '사이버'로 전략개념을 변경한 것은 기밀성(confidentiality), 완전성(integrity), 가용성(availability)에 집중된 정보시큐리티전략 보다 광범위하고 포괄적인 대응전략이 필요했기 때문이다 (情報セキュリティ政策会議 2013). 사이버기본법은 사이버시큐리티를 '전자적 방식, 자기적 방식, 기타 사람의 지각으로 인식할 수 없는 방식으로 기록, 발신, 전달되거나 수신되는 정보의 누설, 멸실 또는 훼손을 방지하고, 해당 정보의 안전한 관리를 위하여 필요한 조치 및 정보시스템 및 정보통신 네트워크의 안전성 및 신뢰성 확보를 위해 필요한 조치'로 새롭게 규정했다. 사이버기본법을 근거로 2015년에는 내각관방을 위원장으로 사이버안보전략을 총괄하는 사이버시큐리티전략본부가 신설되었고, 전략본부의 사무국으로 실무를 담당하는 정보시큐리티센터도 6개 그룹으로 확대 개편되었다. 아베 내각 이후 사이버 전략은 포괄적인 안보개혁과 함께 사이버 안보의 전통 안보화 또는 군사화가 본격화되었다 (이승주 2017; Kallender and Hughes. 2017). 2014년 정보시스템의 안정성, 사이버 방어와 공격, 최신기술 연구 및 인재육성을 담당하는 사이버방위대가 80명 규모로 창설되었다. 2022년 3월 17일에는 기존 지휘통신시스템대대 예하부대로 편제되었던 사이버방위대를 독립부대로 신편하고, 2023년말 까지 890명이었던 병력규모를 2,230명으로 증원을 추진하고 있다(産経新聞 23/05/03).

<그림 1> 일본의 사이버안보 실행체계



자료: 일본 사이버시큐리티전략 및 三角(2015) 참조 저자요약.

2020년 스가 내각 출범 이후 사이버 및 디지털 전략의 제도적, 전략적 전환이 구체화되었다. 코로나-19 위기 가운데 아날로그 시스템의 문제제기가 이어지는 가운데 스가 총리는 취임 직후 디지털 개혁의 필요성을 강조했다. 2021년 2000년 제정되어 20년간 디지털 관련 정책의 근거가 되어온 IT기본법을 폐지하고 2021년 5월 '디지털사회형성기본법'을 포함 디지털개혁 법제를 제정했다. 이를 근거로 2021년 9월 디지털청이 출범했다. 디지털청은 (1) 디지털 사회를 위한 구조개혁, (2) 디지털 전원도시, (3) 국제전략, (4) 안전·안심 확보, (5) 포괄적 데이터 전략, 및 (6) 디지털 산업육성을 중점목표로 하는 디지털 전환 기본전략을 추진하고 있다(GoJ 2022). 디지털 변혁전략이 구체화된 발표된 일본의 사이버 안보전략은 이전과 비교하여 특징적 변화가 있다. (1) 디지털 변혁과 사이버 안보의 동시적인 추진이 명시된 것과 함께, (2) 이전과 달리 중국, 러시아, 북한의 사이버위협으로 명시하고 있으며, (2) 보호, 방어에 국한되지 않고 능동적 억지를 위한 공세전략을 모색과제가 명시되었다. 2000년대 본격화된 일본의 사이버 안보전략의 변화에 따라 사이버 거버넌스도 변화되어 왔다. 아베 내각 이후 정부주도의 사이버 거버넌스가 정부주도의 사이버 거버먼트로 변화되었다면, 디지털 변환정책에 따라 사이버본부는 NSC 및 디지털청의 협력적 하위기구로 구성되었다 (GoJ 2021).

4. 일본의 사이버 국가책략과 국제협력

사이버 공간의 안보화, 군사화를 거쳐 2021년부터 디지털 변혁의 목표가 강조되어 추진되고 있는 일본의 사이버 안보전략에서 국제협력의 목표는 사이버 법치(cyber rule of law), 역량구축(capacity building), 신뢰구축 (Cyber CBMs) 세 가지다. 사이버 법치를 위해 일본은 유엔 헌장을 포함한 기존 국제법이 사이버 공간에 적용하고 국제사회의 평화와 안정을 위한 사이버 규범, 규칙을 보편화를 주도하는 것이다. 둘째, 사이버 범죄에 대응하기 위해 전문지식과 정책의 협력을 강화하는 것이다. 안보적 이해를 공유하는(like-minded) 국가

와의 전략적, 기술적 협력과 함께 아세안 등 제3세계 국가의 사이버 역량을 지원하는 사이버 공적개발원조(Cyber ODA)를 포함하다. 마지막으로 사이버 공간의 신뢰구축을 위한 국제협력이다. 사이버 신뢰구축의 과제는 특정무기의 감축, 제한, 규제는 물론 감시, 검증 등고 같은 전통적 신뢰구축과 상이하다. 예측된 사이버 위협을 공유하고 사이버 공격으로 인한 상황의 악화와 긴장의 증가를 방지하기 위해 국가간의 신뢰를 강화하는 것이다. 일본은 사이버 공간의 안보화가 본격화된 2000년대부터 자유롭고, 공정하며 안전한 영역을 위한 협력을 위한 일본의 역할을 강조해왔다.

<표 5> 일본 사이버 안보전략과 국제협력

구분	법제와 정책기구	
안보화 담론	2006	• 사이버 안보의 일본모델(Japan Model) • OECD와 G8의 다국적 프레임 증진
	2009	• 미국과 유럽과의 국제파트너십 • ASEAN의 글로벌 공공 및 민간부문 파트너십 구축
	2010	• 미국, 아세안, EU와의 동맹(alliance) • APEC, ARF, ITU, WWWN, FRITST, APCERT 협력
군사화 전략	2013	• 세계를 선도하는 J-Initiatives • 민주주의, 기본 인권존중, 법치를 포함한 기본가치 파트너십 • ASEAN, 미국, EU, 영국 등 양자협력 강화
	2015	• 정보의 자유 보장, 법치, 개방성, 자율성, 다중이해관계자 협력 • 선제적(proactive), 촉진자(catalyst), 사이버-물리적 공간 포괄 • 적극적 평화와 미국, 유럽, 아시아태평양, 남미 협력
	2018	• 새로운 가치와 서비스가 창출되는 최전선으로서 society 5.0 구축 • 방어, 억지, 상황인식 능력강화
디지털 전환	2021	• 사이버 공간은 지정학적 긴장을 대변하는 영역(중국, 러시아, 북한) • 정보의 자유 보장, 법치, 개방성, 자율성, 다중이해관계자 협력

일본의 사이버 안보전략이 변화에 따라 국제협력의 선언적, 실질적 목표 역시 변화되었다. 사이버 공간의 안보화 담론이 시작된 2000년대 '사이버 안보의 일본모델'이라는 선언적 목표가 제시되기도 했다. '일본모델'이란 사이버 위협에는 국경이 없으며, 세계 최고수준의 광통신 네트워크를 구축한 일본이 세계적인 문제를 해결하는데 주도적인 역할을 수행하는 것이다(ISPC 2006). 2003년 사이버 안보전략을 발표한 미국이 사이버 전략을 주도하는 가운데 OECD, G7, APEC, ARF 등 다자협력을 통한 사이버 협력이 추진되었다. 또 한 가지 일본의 사이버 국제협력에서 주목할 것은 ASEAN에 대한 역량구축 지원과 협력이 가장먼저 진전되었다는 점이다. 사이버 공간의 안보화시기 일본의 사이버 국제협력은 (1) 탈냉전 이후 국제적인 역할과 위상을 강화하는 다자협력을 중심으로 하는 관여와(Kallender and Hughes 2017), (2) 아세안에 대한 사이버 ODA와 같이 경제협력과 경제 인프라에 대한 보호 목적이었다(Bartlett 2023).

<표 6> 일본의 사이버 국제협력 목표와 대상

목표	사이버 법치	사이버 공간, 활동, 기반에 대한 국제법, 규범제정
	CMBs	사이버 갈등 관리를 위한 투명성, 안정성
	능력구축	기술적, 디지털 역량구축 및 인적자원 개발
협력	양자	영국(2012), 인도(2012), 미국(2013), EU(2014), 프랑스(2014), 이스라엘(2014), 호주(2015), 에스토니아(2018), 독일, 러시아, 한국, 우크라이나, 베트남(2021), 슬로베니아(2022)
	다자	아세안(2009), NATO(2018), UNGGE, G7, G20, GCCS(London Process)

자료: 일본 외무성 사이버시큐리티(https://www.mofa.go.jp/policy/page18e_000015 .html) 페이지, Vosse (2019), 일본 방위백서(2021), 일본 외교청서(2022) 참조.

둘째, 사이버 공간의 군사화가 추진된 아베 내각 이후 사이버 전략의 양자협력 및 군사협력이 강화되었다. 2013년 일본의 사이버시큐리티전략이 발표된 이후 미국, EU, 프랑스, 호주, 에스토니아, 베트남 등 양자간의 사이버 전략대화가 본격 시작되었다. 사이버 양자협력은 사이버안보 전략과 정책, 사회기반, 사이버 교육, 훈련, 인재양성 및 법적 기반구축 및 규제 등의 이슈를 포함한다 (Vosse 2019). 사이버 법치, 역량구축이 아세안, G7, G20, GCCS 등 다자기구에서 다루어지는 사이버 외교의 문제라면, 양자대화는 사이버 공간의 군사적 협력과 신뢰구축에 중점 목표로 추진되고 있다. 미국과의 동맹협력은 일본이 사이버 억지, 방어, 공세능력을 위한 국제협력에서 가장 중요하다 (MoD 2022, 291). 2013년 미일 사이버방어정책 워킹그룹(CDPWG)이 설치된 이후 작전적 수준의 공동훈련이 시작되었다. 2022년 11월에는 한국(5월)에 이어 나토의 사이버방위센터(CCDCOE) 정회원으로 가입했다. 요컨대, 일본은 동맹 및 선진국과의 사이버 방어, 억지, 공세적 능력구축 협력과 함께, 동남아시아에 대한 역량구축 지원을 정보기술, 인공지능, 로봇공학 등의 기술경쟁과 연계하여 추진하고 있다.

5. 평가 및 함의

안보, 경쟁, 협력의 총체적 과제로서 일본의 사이버 국가책략은 안보화 담론, 군사화 전략, 디지털 전환으로 전환되어왔다. 사이버 공간의 안보화된 2000년대 (1) 정보보호를 위한 국내적 사이버 거버넌스의 구축과 함께, (2) 사이버 안보를 전통 안보화하고 국제적인 위상과 역할 확대의 전략적 의제로 활용했다. 2000년대 미국이 주도하는 사이버 공간의 안보화 문제를 일본이 가장 먼저 수용하고 제도화한 것은 전통적 안보보다 경제적, 외교적 현안을 안보문제로 담론화한 일본의 정책구조와 전략문화에 큰 요인이 있다(Katzenstein and Okawara 1993). 아울러, 사이버 안보문제에 대한 국제협력을 통해 탈냉전 이후 보통국가로

서의 위상과 역할을 모색하는 국가정체성도 투영되었다. 아베 내각 이후 사이버 공간의 군사화되면서 방어, 억지는 물론 공세적인 사이버 전략을 위한 체계, 규범과 기능이 강화되고 있다. 사이버 안보의 군사화는 미일동맹의 협력의제 뿐만 아니라 미국의존 안보전략의 탈중심화(decentrering) 및 네트워크 동맹의 전환을 주도하는 일본의 안보전략과 연계되어 있다(Midford 2018). 그리고 2021년에는 20여 년간 디지털 관련 정책의 법적기반이 되어왔던 IT 기본법을 대체하여 디지털기본법을 제정하고 디지털 전환을 포함한 포괄적인 사이버 국가책략을 추진하고 있다. 디지털 전환정책은 사이버 안보뿐만 아니라 국제협력, 경쟁우위를 포함하는 사이버 국가책략이 포괄적으로 포함되어 있다.

일본이 추진하고 있는 사이버 안보전략은 역사적, 비교적 시각에서 정책적인 과제를 검토할 수 있다. 우선 안보, 경쟁, 협력 등 사이버 국가책략의 과제를 일반적, 통합적 사이버 법제로 제도화할 것인가, 아니면 개별적 쟁점에 대한 구체적 법제가 필요한가의 문제이다. 둘째, 사회전반의 총체적 현안으로서 사이버 안보전략의 거버넌스를 구축하는 문제다. 한국은 공공부문은 국가정보원, 민간부문은 과기부가 담당하는 분권화, 협력적 거버넌스가 구축되어 있는 반면, 일본은 국가안전보장회의가 디지털 경쟁(디지털청), 안보(사이버전략본부) 관련 기관을 총괄한다. 셋째, 사이버 안보전략의 대외협력을 위한 전략, 제도와 정책이다. 일본은 2000년대부터 사이버 안보를 주도하는 일본모델을 추진해왔다. 사이버 공간의 안보화 시기 국제협력은 외무성이 국제협력을 주도했다면, 사이버 공간의 군사화 시기에는 사이버 외교(cyber diplomacy), 사이버 ODA를 주도하는 외무성 (총합외교정책국 경제안전보장정책실 소관), 디지털 기술, 데이터와 육성 관련 협력을 주도하는 디지털청, 방위성이 사어버 국제협력을 주도하고 있다. 사이버 안보전략이 체계화된 이후 방위백서와 외교청서에도 국제협력의 비전, 목표와 수단이 구체적으로 기술되어 있다. 반면, 한국 외교부(국제기구국 국제안보과 소관) 및 국방부의 국방백서, 외교백서의 사이버 안보 국제협력의 목표, 전략은 제한적이다.

참고문헌

이승주. 2017. "일본 사이버 안보전략의 변화: 사이버 안보의 전통 안보화와 전통 안보의 사이버 안보화." 『국가안보와 전략』제17권 1호, 173-202.

박성호. 2022. "일본의 사이버 안보전략: 양자주의의 강화인가 다자주의로의 전환인가?" 『일본학』제56집, 159-182.

김상배. 2017. "세계 주요국의 사이버 안보전략: 비교 국가전략론의 시각" 『국제지역연구』제26집 3호, 67-108.

이상현. 2019. "일본의 사이버안보 수행체계와 전략" 『국가안보와 전략』제19권 1호, 117-154.

이상현. 2022. "사이버 외교의 국제비교: OSCE와 ARF의 사이버 신뢰구축조치 비교분석" 『세계지역연구논총』제40권 2호, 225-257.

Bartlett, Benjamin. 2023. "Why Do States Engage in Cybersecurity Capacity-Building Assistance? Evidence from Japan." The Pacific Review https://doi.org/10.1080/09512748.2023.2183242(검색일: 2023.06.02.)

GoP. 2021. Cybersecurity Straegy: Cybersecurity for All. Tokyo: Government of Japan.

Healey, Jason. 2011. "Pursuing Cyber Statecraft" Atlantic Council Issue Brief (Aug.) https://www.jstor.org/stable/pdf/resrep03355.pdf (rjatordlf: 2023.06.02.).

Information Security Policy Council. 2006. "The First National Strategy on Information Security: Toward the realization of a Trustworthy Society." https://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf (검색일: 2023.05.20.).

Information Security Policy Council. 2013. "International Strategty on Cybersecurity Cooperation: J-Initiative for Cybersecurity" (Oct. 02) https://www.nisc.go.jp/eng/pdf/InternationalStrategyonCybersecurityCooperation_e.pdf (검색일: 2023.05.28.)

Kallender, Paul and Christopher Hughes. 2017. "Japan's Emerging Trajectory as a Cyber Power: From Securitization to Militarization of Cyberspace." Journal of Strategic Studies 40:2, 118-145.

Katzenstein, Peter J. and Nobuo Okawara. 1993. "Japan's National Security: Structure, Norms and Polcies." International Security 17:4, 84-118.

Kello, Lucas. 2013. "The Meaining of the Cyber Revolution: Perils to Theory and Statecraft." International Security 38:2, 7-40.

McKinsey & Company. 2021. Japan Digital Agenda 2030: Big Moves to Restore Digital Competitiveness and Productivity. https://www.digitaljapan2030.com (검색일: 2023.06.02.).

Midford, Paul. 2018. "New Directions in Japan's Security: Non-US Centric Evolution," The Pacific Review 31, 407-423.

Nye, Joseph S. 2010. "Cyber Power" Belfer Center for Science and International Affairs https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power. pdf(검색일: 2023.05.28.).

Vosse, Wilhelm M. 2019. "Japan's Cyber Diplomacy" Research in Focus (Oct.)

ニュートン・コンサルティンク株式会社. 2017. "企業のサイバーセキュリティ対策に関する調査報告書" https://www.nisc.go.jp/pdf/policy/inquiry/kigyoutaisaku_honbun.pdf (검색

일: 2023.05.25.).

三角, 育生. 2015. "我か国におけるサイバーセキュリティ政策の現状と今後," CISTEC Journal No.155 https://www.cistec.or.jp/service/daigaku/data/1501-04_siten01.pdf (검색일: 2023.06.02.).

産経新聞. "自衛隊サイバー部隊 年度内に人員2·5倍に" (2023.05.03.) https://www.sankei.com/article/20230503-VPG3D45LAZOPRO2OA5PBSNVBM4/(검색일: 2023.06.02.).