일본의 사이버안보 전략과 국제협력

2024

한국사이버안보학회
KACS

한국사이버안보학회 워킹페이퍼 20호
발간일: 2024년 8월 22일

윤대엽 (대전대학교)

I. 문제제기

아베 내각(2012-2020)이 추진한 안보개혁은 전후 일본의 안보전략과 미일 동맹협력의 전환점이 되었다. 2012년 중의원 선거에서 압도적인 승리로 출범한 아베 2기 내각은 2013년 국가안전보장전략을 제정하고 전후 구속에서 탈피한 안보개혁을 추진했다. 2013년 전후 방위전략의 규범이었던 '기반적 방위력'을 '통합기동방위력'으로 변경하고 2018년에는 안전보장환경의 긴박한 변화에 대응하여 '다차원통합방위력'으로 변경했다. 2014년 각의에서 의결된 집단적 자위권은 전후 논란이 되어왔던 적극적 교전권을 용인하는 것으로, 가헌개헌에 앞서 사실상 헌법9조의 구속을 해소한 것이다(윤대엽 2022). 2015년 개정된 일미방위협력지침에 따라 안보법제를 제·개정함으로서 무력공격사태, 중요영향사태는 물론 국가안보에 영향을 미치는 존립위기사태에 무력사용의 제도적인 근거를 확립했다. 국방획득 및 연구개발을 총괄하는 방위장비청을 개청(2015)하고 무기수출 3원칙을 폐지함으로서 전후 일본의 군사혁신을 제약했던 제도를 해체했다. 아베개혁을 계승한 2022년 기시다 내각은 안보관련 3법을 개정하고 능동적 방어를 위한 적기지 공격능력 보유와 방위비 증액을 명시하는 등 전후구속에서 탈치한 안보개혁이 진행되고 있다(윤대엽 2023).

사이버 시큐리티전략(サイバーセキュリティ戦略) 역시 아베 내각 이후 일본이 추진한 안보개혁의 핵심과제의 하나다. 일본은 2006년 이미 동아시아에서는 최초로 사이버 공간의 포괄적인 안전을 목표로하는 '정보시큐리티 기본계획(2006)'을 수립하고 추진했다. 아베 내각은 2013년 기본계획을 '사이버시큐리티 전략'으로 변경했다,[1] 2014년에는 '사이버시큐리티기본법(이하 사이버기본법)'을 제정하고 사이버 안보전략의 목표, 임무를 명시한데 이어 사이버 안보전략을 총괄하는 '사이버시큐리티전략본부(이하 사이버전략본부)'를 설치했다. 사이버기본법의 제정을 계기로 일본의 사이버안보 전략은 정보보호와 방어에서 탈피하여 적대국의 사이버 공격을 예방하고 적극적으로 영향을 미치는 전략개념으로 전환되었다. 2021년 스가 내각의 집권시기 발표된 사이버시큐리티전략은 중국, 러시아, 북한을 처음으로 사이버 위협으로 명시한데 이어 사이버 위협에 대한 사전적, 적극적으로 예방하는 '능동적 사이버 방어(能動的サイバー防御)' 개념이 제시되기도 했다(GoJ 2021, 37). 그리고, 2023년 2월에는 능동적 사이버 방어의 세부방안 검토를 위해 내각관방에 사이버안전보장체제준비실(サイバー安全保障体制整備室, 이하 사이버안전실)이 신설되었다.

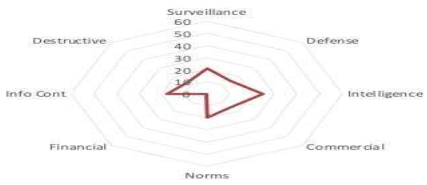
---

1) 본 연구는 사이버 안보(cybersecurity)를 사이버시큐리티로 활용하는 일본의 특수성을 고려하여 일본의 사이버 관련 정책은 '시큐리티' 개념을 원용하고, 기타 일반적인 경우 '사이버 안보'로 개념화함

일본의 사이버 안보전략은 사이버 위협을 선제적으로 안보화, 군사화 한 것은 물론, 지속적으로 국제협력을 강조했다는 점에서 전후 안보전략과는 대조적이다. 전후 일본의 안보전략은 헌법 9조, 미일동맹 및 평화주의라는 요인에 구속되었다. 전후 구속에도 불구하고 일본은 2005년 사이버 공간을 선제적으로 안보화하는 것은 물론, 미일 SCC의 의제로 다루었고, 국내차원의 사이버 안보에 그치지 않고 대외적인 협력을 적극추진한 것이다. 아베 내각 출범 이후에는 군사적 대외협력도 강화되었다 (이승주 2017). 2013년 통합박료감부 예하 지휘통신시스템부에 설치되었던 사이버 공간 방위대를 개편하여 '사이버방위대(サイバー防衛隊)'를 편제했다. 처음 90명을 정원으로 편제되었던 사이버방위대는 2018년 430명, 2020년 660명으로 증원되었고 2022년 3월에는 육해공자위대의 공동부대로 재편했다(防衛省 2023, 146). 사이버방위대 및 육해공군 사이버전문부대에서 약 4,000명의 병력을 운영하고 있다 (防衛省 2023, 298). 미중경쟁이 본격화된 이후 발표된 사이버시큐리티 전략은 안보위협을 선제적으로 명시하는 한편, 2021년 발표된 사이버 전략에는 중국, 러시아, 북한을 명시적인 '위협'으로 처음 명시했다. 이어 2022년 발표된 자민당의 정책제언보고서(自由民主党 2022)에도 중국을 '중대한 위협'으로 러시아를 '현실적 위협'으로 기술한데 이어, 2022년 12월 발표된 국가안전보장전략은 중국을 중대한 위협, 북한의 경우 중대하고 긴박한 위협으로 규정함으로서 사이버 시큐리티 전략에서 규정된 위협인식이 계승된 것이다. 일본의 안보전략에서 '위협'이란 '침략할 수 있는 능력과 의도가 결부'되어 있는 개념이다 (조진구 2023, 25).

디지털 위험(digital risk)의 안보화가 경제, 사회적인 디지털 전환(digital transform)보다 우선했다는 점도 특징적이다. IMD의 2022년 디지털 경쟁력 순위에 따르면 일본의 객관적인 사이버 경쟁력 순위는 동아시아 주요국 중 하위권에 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).

〈표1〉 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 전세계적으로 비대면 업무가 도입되었지만 일본의 경우 서류 및 전표, 날인 관행으로 재택근무가 제한되었다. 문서중심의 업무관행으로 재난지원금의 지급에 혼선이 발생했고 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 요인으로 지적되었다. 이 때문에 스가 내각은 아베노믹스의 하나로 2018년부터 추진된 'society 5.0'을 강화하여 디지털 변혁(digital transformation)을 추진했다. 일본사회의 디지털 전환을 위히 2000년 제정된 IT기본법을 '디지털사회형성기본법'으로 개정하는 한편, 2021년에는 디지털정책을 총괄하는 디지털청을 신설했다. 디지털청은 행정, 교육, 사회의 디지털 전환은 물론 사이버 안보와 디지털 개혁 정책을 총괄하는 기구다.

일본이 사이버 공간의 안보화가 디지털 전환보다 우선되었던 이유는 무엇인가? 그리고, 다자안보협력보다 앞서 사이버안보 전략에서 국제협력이 강조된 이유는 무엇인가? 본 연구는 역사적, 비교적 시각에서 일본의 사이버안보 전략이 전후 안보개혁과 점진적, 창발적으로 형성, 전환되어 온 과정을 구조적, 행위자 측면에서 분석하고 사이버 국제협력의 성격을 분석한다. 그리고 미일동맹과 전후 안보개혁의 맥락에서 추진되어 온 일본의 사이버 안보전략이 한국에 대한 함의를 검토한다.

II. 일본의 안보개혁과 사이버 안보: 접근시각

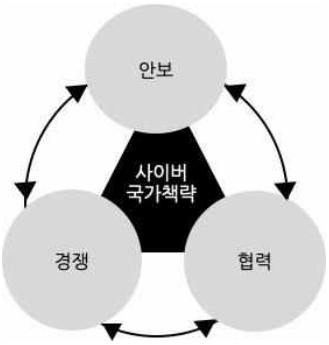
디지털 전환에 따라 사이버 안보(cybersecurity)는 디지털 기기, 네트워크는 물론, 이를 활용한

디지털 플랫폼과 빅데이터 기반 경제의 안보현안이 되었다. 디지털 기술의 발전에 따라 물리적, 가상의 공간은 경제적, 정치적, 사회적 현안와 연계되어 총체적 과제로 인식되어 왔다. 총체적인 사이버 위협에 대한 대응을 위해서는 정부, 기업, 개인은 물론 국가전반(whole of nations)의 관여와 협력이 요구된다. 전자(E), 네트워크(Net), 디지털(Digital) 등이 혼재되어 있는 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 산업혁명 기술이 혁신되면서 디지털 전환과 함께 사이버 안보를 위한 포괄적인 사이버 국가책략(cyber statcraft)이 추진되고 있다.

사이버 전략은 디지털 기술변화와 이에 수반되는 다층적인 위협양상 따라 안보화 되어왔다. 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 체계를 구축했다. 2000년에 개정된 '정부정보보안개혁법'은 정보시스템과 데이터 위협에 대한 주기적인 위협평가와 대응을 규정했다(변진석 2022). 위협인식과 네트워크 보호가 중심이 되었던 사이버 관련 정책이 사이버안보(Cybersecurity Strategy)로 전환된 것은 부시 행정부다. 9/11 테러는 비군사적 위협에 대응하기 위한 포괄적인 안보개혁의 맥락에서 사이버 공간을 안보화했다. 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 중요 기반시설에 대한 사이버 공격을 예방하고, 사이버 공격의 취약성을 축소하며, 손실과 회복시간을 최소화하는 전략을 제시했다(The White House 2003). 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 안보는 보호 및 안보적 이해에 국한되지 않는다. 사이버 영역은 1차적으로 디지털 인프라의 확장과 함께 네트워크화 된 국가전반의 전략적 자산이 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.

〈표2〉 사이버 국가책략(statecraft)의 영역과 쟁점

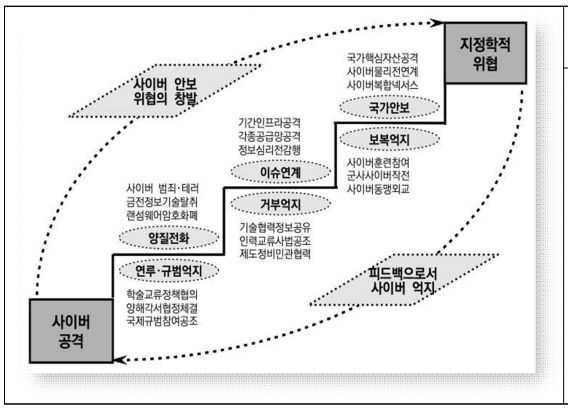
	**안보**	▪ 사이버 공간의 안보화 ▪ 디지털 인프라, 전략시설, 데이터 보호 ▪ 사이버 방어, 억지, 공격
	발전	▪ 사이버 공간의 시장화 ▪ 디지털 플랫폼, 네트워크, 데이터 기술 ▪ 디지털 산업육성과 경쟁
	협력	▪ 사이버 공간의 다자적 거버넌스 ▪ 사이버 공간의 규범, 표준, 제도 ▪ 사이버 외교, 협력, 공적개발원조(ODA)

사이버 국가책략은 안보, 개발. 협력 세 가지 영역으로 구분할 수 있다. 첫째, 안보는 사이버 공간의 안보적 쟁점이다. 사이버 범죄로부터 디지털 인프라, 네트워크화 된 국가전략시설 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 시버 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).

사이버 공간은 물리적, 비물리적 공간을 포괄하는 영역에서, 국가와 기업은 물론 사회전반의 협력을 수반하는 하는 주체, 그리고 기술, 군사, 전략 등 지정학적 이해[2]가 투영되는 위협의 가변성을 특징으로 한다. '창발에 대한 억지(deterrence against emergence)' 개념은 사이버 위협의 변화에 따라 전략, 수단, 법제와 대외협력이 단계적으로 진화해온 일본의 사이버 안보전략을 구조적 차원에서 분석하는데 분석적 함의를 제공한다. 김상배(2023)는 양질전화, 이슈연계, 국가안보의 단계에 따라 동태적으로 변화하는 사이버 안보위협과 억지전략의 상호작용을 '창발과 피드백'의 입체적이고 동태적인 프레임에서 분석할 필요성을 제시한다. 첫째, 사이버 안보 위협과 이에 대응하는 안보전략은 양질전화, 이슈연계, 국가안보의 다층위적 위협단계에 따라 적합한 억지옵션을 도입하는 입체적 성격을 가진다(김상배 2023, 73-74). 일상수준의 사이버 범죄, 테러, 정보 및 기술탈취 등에 대해서는 예방차원의 연루억지와 규범억지로 대응한다. 기간시설과 공급망, 사이버심리전의 차원에서는 거부억지의 수단이 적용된다. 마지막으로 국가안보의 층위의 위협의 경우 보복적 억지(deterrence by punishment)의 목적과 수단이 유용용성을 가진다. 아울러 창발에 대한 억지는 동태적이다. 다층위적 사이버 전략은 상호연계되어 있을 뿐만 아니라 지속적, 가변적 위협에 대응하여 연루, 규범, 보복, 거부 등의 전략이 포괄적, 연속적, 축적적(cumulative) 성격을 가진다.

2) 일본의 2021년 사이버시큐리티전략은 사이버 공간의 지정학 경쟁 영역임을 처음 명시함

〈표3〉 일본 사이버 안보전략의 창발과 정책변수



요인	정책이념		
위협 인식	영향	YES	NO
	YES	(1) 정치적 요인	우연적 요인
	NO	(2) 인지적 요인	제도적 관성

자료: 김상배 (2023), p.74 및 Bartlett (2019) 참조

행위자 측면에서는 정책결정에 영향을 미치는 정책이념과 위협인식의 상호작용에 따른 정책변화를 참고할 수 있다(Campbell 2014). (1) 정치적 요인은 행위자 또는 행위자 연합이 공유된 위협인식에 따라 정책변화를 결정하는 것이다. (2) 인지적 요인 역시 정치행위자들의 상호작용이 이루어지지만 문제의 본질, 중요성에 대한 인식의 격차와 정책목표가 명확하지 않다는데 차이가 있다. (3) 우연적 요인은 의사결정의 쓰레기통 이론(garbege can theory)와 같이 정책변화가 선호의 불확실성, 기술적 불확실성(unclear technologies)으로 인해 합리적 인식, 정치적 의지가 아니라 우연한 계기로 발생하는 것을 의미한다. (4) 마지막으로 정치적 의지와 외부적 조건과 관계없이 조직적, 제도적 요인에 의한 정책변화는 관성적 또는 제도적 요인으로 설명할 수 있다.

이와 같은 분석개념을 근거로 아래에서는 일본의 사이버 안보전략과 대외협력의 특징을 (1) 정보시큐리티 기본계획(2004-2012)이 수립되어 추진된 시기, (2) 사이버시큐리티 전략(2013-2022) 시기로 구분하여 검토한다. 정보시큐리티 기본계획은 9/11 사태 이후 비전통안보가 새로운 안보위협으로 인식되는 가운데, 탈전후 안보전략을 추진한 고이즈미 내각에 의해 추진되었다. 잠재적 안보위협에 대한 선제적 인식에도 불구하고 정보기술(ICT)기술이 가진 경제적, 기술적 이해가 중심이된 양질전화 단계였다. 2010년 민주당 내각은 기본계획을 처음 전략으로 변경하였고, 이후 아베내각은 안보개혁의 핵심정책의 하나로 사이버안보전략을 추진했다. 이는 일본과 주변국에 대한 실질적인 사이버 위협이 현재화되었고, 국방체계의 디지털 전환에 따라 사이버, 전자기 등이 군사혁신 목표료 추진되어기 때문이다. 이어서 사이버 기본계획과 사이버 전략 단계에서 정책이념과 정책, 안보위협과 인식의 차이가 국제협력에 있어서 어떤 변화를 수반했는지 검토하다.

III. 정보시큐리티 기본계획과 국제협력: 2004-2012

일본은 2000년대 동아시아 국가 가운데 가장먼저 사이버 공간을 안보화하고 네트워크의 보호와 안전을 위한 국가차원의 전략을 수립했다. 탈냉전 이후 인터넷이 빠른속도로 보급되면서 PC 등 디지털 기기의 보급이 늘어나면서 농업혁명, 산업혁명에 이어 세 번째 문명적인 변화를 가져오게 될 정보통신 산업경쟁도 치열했다. 1960-70년대 미국은 컴퓨터 산업발전을 선도했지만,

1980년대 일본이 미국을 추격했다. 특히, TV, VCR, 메모리 반도체, 평판디스플레이, CR-ROM 등 디지털 하드웨어 분야에서 일본은 세계적인 경쟁력을 갖추었다. 그리고, 1990년대 네트워크 기반 컴퓨터 기술과 표준화를 위한 세 번째 경쟁이 진행되고 있었다 (김상배 2002, 114-117). 일본이 ICT기술에 기반한 사회적인 과제를 정책화한 것은 이와같은 배경 때문이다.

전적으로 개인과 민간부문의 책임이었던 컴퓨터와 인터넷의 안전 문제가 국가적인 정책차원에서 검토되기 시작한 것은 1990년대 후반이다. 일본정부 웹사이트에 대한 사이버 공격이 발생한 직후인 1999년 9월 '불법접근금지법(不正アクセス禁止法)'이 제정되었고 정보보안을 담당하는 관련부처 회의(情報セキュリティ関係省庁局長等会議)가 처음 설치되었다(Bartlett 2019). 2000년에는 '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)에 따라 정보안보와 관련 정책목표와 거버넌스가 제도화되었다. 동법 제22조를 근거로 2000년 정보시큐리티대책추진회의(이하 정보대책회의)가 정보시큐리티를 담당하는 정책기구로 설치되었고 2005년 '정보시큐리티센터(NISC)'로 개편되었다. 정보대책회의는 2000년 12월 '중요인프라 사이버테러 관련 특별행동계획(重要インフラのサイバーテロ対策に係る特別行動計画)'을 발표했다. 이 계획은 공격으로부터 정보통신, 금융, 항공, 철도, 전력, 가스, 정부·행정서비스 등 국민생활과 사회경제 활동에 중요한 영향을 미치는 정보인프라를 보호하는 것이다 (情報セキュリティ政策会議 2010). 2005년에는 중요인프라를 의료, 수도, 물류 등을 포함한 10개 영역으로 확대하고, (1) 불법침입, 데이터 탈취, 마비 등 사이버 공격은 물론 비의도적, 재해 등에 의한 위협 등으로 세부적으로 규정한 개정안을 발표했다(情報セキュリティ政策会議 2015).

〈표4〉 일본의 사이버 관련 법제, 전략 및 정책구조의 변화

구분	법제와 정책기구		정책구조
양질전화와 정책	법제	• IT기본법(2000)	IT전략본부 산하 ISPC, NISC
	기구	• 정보시큐리티대책추진회의(2000) • 정보시큐리티대책추진실(2000) • 정보시규리티센터(2005) • 정보시큐리티정책회의(2005)	
	전략	• 정보시큐리티 기본계획(2006) • 정보시큐리티 기본계획(2009) • 정보시큐리티 전략 (2010)	

2006년에는 정보시큐리티를 포괄하는 기본계획이 수립되었다. 정보시큐리티를 총괄하는 기본계획이 수립된 것은 안전한 IT의 활용기반이 고도정보통신 사회의 발전을 위해 필수적인 과제로 등장했기 때문이다 (情報セキュリティ政策会議 2006, 1). 2009년 정보시큐리티 전략은 공공부문, 인프라, 기업, 개인 등 정보시큐리티 4개 주체의 상호적인 협력을 강조하는 '횡단적 정보시큐리티 대책'이 추가되었다. 인터넷 기반 활동, 비즈니스가 확장되면서 정보를 활용하는 정보, 기업, 개인 뿐만 아니라 정보를 위탁탁하고, 제3자에게 이전되면서 정보주체의 역할도 중요하게 되었기 때문이다 (情報セキュリティ政策会議 2009, 16-17). 정보주체의 인식은 물론, 디지털 기기의 보안 등 기술적 요인과 함께 개인정보의 활용의 규제 등이 필요로하게 되었다. 2006년과 2009년 발표된 정보시큐리티 전략은 (1) IT기본법을 근거로 '정보시큐리티'를 정책개념으로 사용하고 있으며, (2) 정보 및 디지털 기반의 보호, 안전을 위한 정책과 정책거버넌스에 따라 (3) 사이버 공간의 범죄, 공격으로 인한 손실을 최소화하고 경제적 손실을 최소화하는 것을 정책목표로

하고 있다는 공통점이 있다 정보시큐리티 기본계획의 목표가 (1) 경제대국의 지속적인 발전을 위한 IT의 활용, (2) IT기반 국민생활의 편리를 추구하며, (3) 정보시큐리티 선진국의 입지를 공고이하는 것이다.

2009년 중의원 선거에서 승리하며 '55년 체제' 이후 최초로 정권교체에 성공한 민주당 정부는 관련 법에 규정된 3년 주기보다 앞서, 2010년 '기본계획'을 '전략'으로 개정했다. 2차 정보시큐리티 기본계획이 발표된지 1년만에 '정보시큐리티전략'이 발표된 것은 2009년 7월 한국과 미국에 대한 대규모 사이버 공격사태 때문이다(情報セキュリティ政策会議 2010, 1). 소위 '7·7 디도스(DDos) 대란'으로 불리는 2009년 사이버 공격은 7월 7일부터 8월 18일까지 청와대, 언론사, 정당, 은행 등 정부기관 7개, 금융기관 7개, 민간기관 7개의 컴퓨터 시스템을 마비시켰다(원병철 2019).[3] 2010년 정보시큐티티 전략은 안전중심의 기본계획과 비교하여 위기관리를 위한 정책이 보완되었다는 점에서 차이가 있다. 정보시큐리티 전략은 (1) 사이버 공격사태에 대응하는 체제정비, (2) 정보시류리티의 위협환경에 대한 유연한 정책대응과, (3) 수동적 대책에서 능동적 체제로의 전환을 목표로 제시했다. 사이버 공격사태에 대한 대응은 2003년 법제화된 유사3법 및 내각결정된 '유사사태에 대응하는 정부의 초동대처'에 관한 내각결정(2003년 11월 21일)이 근거가 되었다. 9/11 테러를 계기로 안보법제의 개정을 추진한 고이즈미 내각은 2003년 무력공격사태법(무력사태법), 개정자위대법, 안전보장회의설치법을 제정했다(윤대엽 2023). 특히, 무력사태법은 무력사태의 법위를 무력공격이 (1) 발생 또는 임박사태, (2) 예측되는 사태로 구분하고, 무력공격이 예측되는 사태의 경우에도 무력공격을 회필할 수 있는 정책근거를 법제화한 것이다. 신속한 대처능력을 강화하기 내각관방 중심의 긴급사태 대응체제를 보완하는 한편, 방위분야에 있어서 능력강화 목표가 제시되었다 ((情報セキュリティ政策会議 2010, 7). 사이버 위협이 사회안전과 범죄예방 차원이 아니라 방위분야의 능력으로 처음 언급된 것이다.

창발에 따른 억지개념을 적용하면 2006년부터 2012년까지 일본의 정보시큐리티전략은 '양질전화' 단계에서 정보보안, 사이버 범죄, 정보탈취 등 사이버 공간의 위협 대응정책이 정립된 단계로 평가할 수 있다. 2006년 처음 발표된 정보시큐리티 기본계획은 경제강국으로서 일본의 지속발전을 위한 IT 활용, 더 나은 삶을 위한 IT의 활용기반을 구축하고 새로운 위협에 대응하여 편리함과 보안 사이의 균형있는 IT환경을 구축하는 것이다. 2009년 발표된 정보시큐리티 전략 역시 안전한 IT기반을 지속가능한 경제발전, 국민생활과 삶의 질을 개선하는 기반으로 활용하는 것이다. 대외적으로는 IT기술 발전에 비례하여 증가하는 위협에 대응하는 능력이 '정보시큐리티 선진국가'의 이념으로 제시되기도 했다. 반면, 2010년 발표된 정보시큐리티 전략은 보다 적극적 의미에서 사이버 공간을 안보화한 전환점으로 평가할 수 있다. 기본계획을 '전략'으로 재정의했을 뿐만 아니라, 사이버 위협에 대응하는 방위성의 역할이 처음 명시되었다.

3) 이를 계기로 매월 7월을 정보보호의 달로, 7월 둘째 주 수요일을 정보보호의 날로 지정했음

〈표5〉 일본 사이버 안보전략과 국제협력

구분	법제와 정책기구	
양질전화와 국제협력	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

행위자 요인의 시각을 통해 2000년대 정보시큐리티의 정책이 경제중심의 정보보호 중심의 정책과 제도화된 원인을 설명할 수 있다. 일본의 정보시큐리티 정책은 (1) 사이버 인식과 제도화 단계(2000-2009), (2) 사이버 위협과 제도적 관성의 (2010-2012)로 단계로 구분할 수 있다. 1990년대 후반 사이버 공간을 정책과제로 인식하기 시작한 것은 정보통신 기반 사회의 사이버 위협이 증가했기 때문이다. 1996년 미국은 '국가정보기간시설보호법'을 제정하고 불법적인 접근과 정보탈취를 범죄로 처음 규정했고, 이후 대통령지시 63호(1998)는 정보보호를 위한 정책과제를 명시했다. 부시 행정부는 사이버 공간이 안보화된 전환점이 되었는데, 2000년 '정부정보보안개혁법(Government Information Security Reform Act)'이 법제화되었다 (변진석 2022, 45-49). 9/11 테러 이후 무지의 안보(unknown-known security) 문제에 대한 능력기반 안보 혁신이 추진되는 가운데, 국토안보부가 2003년 제정한 '사이버 안보를 위한 국가전략'은 일본은 물론 세계적으로 사이버 공간을 안보화하는 전환점이 되었다. 2000년 제정된 IT기본법을 근거로 안전한 정보통신 기반 구축목표가 제도화된 가운데 9/11 테러 이후 미국이 사이버 공간을 안보화하면서 일본의 정책변화에 중요한 영향을 미쳤다. 그러나, 2000년대 일본의 정보시큐리티 정책과 제도화를 주도한 것은 경제산업성(METI)과 총무성이었다는 점에 주목할 필요가 있다. 사이버 공간의 안전문제가 정책과제로 인식되면서 정책담론을 주도한 것은 경찰청, 방위청과 함께 ICT 기술과 산업정책의 주관부서인 총무성과 경제산업성이 참여했다. 그러나, 안전을 주관하는 경찰청과 방위청의 상대적인 영향력은 크지 않았다. 직접적인 안보위협이 가시화 되지 않았다는 점과 함께, 버블경제 붕괴 이후 경제발전을 모색하던 1990년대 총무성과 경제산업성의 정책형성에서 미치는 영향이 클 수 밖에 없었다(Bartlett 2019, 10-16). 이와 비교하면 민주당에서 발표된 정보시큐리티전략은 (1) 명시적인 안보위협에 따라, (2) 정권교체에 따른 정책의지, (3) 그리고 2007년 방위성으로 승격된 기관의 이익이 투영된 것이다.

2000년대 일본의 정보시큐리티 전략에서 국제협력이 강조된 것도 이 때문이다. 일본의 2006년 이후 발표된 일본의 정보시큐리티 관련 정책문서에는 공통적으로 국제협력의 선언적, 실질적 목표가 반영되었다. 2006년 정보시큐리티 기본계획에는 '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 협력 목표가 제시되었다. 아울러 ASEAN에 대한 역량구축과 협력목표가 제시되었다. 사이버 공간의 안보화시기 일본의 사이버 국제협력은 (1) 탈냉전 이후 국제적인 역할과 위상을 강화하는 다자협력을 중심으로 하는 관여와

(Kallender and Hughes 2017), 그리고 (2) 일본의 경제적인 이해가 결부되어 있는 아세안에 대한 사이버 ODA를 제공함으로서, 경제 인프라의 보호 및 경제협력을 증진하는 것이 핵심 목적이었다(Bartlett 2023).

IV. 사이버시큐리티 전략과 국제협력: 2013-2023

아베 내각은 포괄적인 안보개혁의 맥락에서 사이버 안보전략을 재정의했다(이승주 2017). 2010년 '정보시큐리티 전략'을 '사이버시큐리티'로 변경하고, 사이버 안보의 안보화를 넘어 군사화를 적극 추진했다. 그러나, 아베 내각이 추진한 사이버시큐리티 전략은 사이버 위협의 증가, 미일 동맹협력의 의제화 등 단절적이기 보다 연속적인 특성을 가진다. 민주당 정부가 1976년 방위체제의 '기반적 방위력' 개념을 '동적방위력'으로 변경한 2010년 방위계획 대강에는 사이버 공간의 위협을 안보문제로 인식하고, 사이버 공격에 대한 대처능력을 종합적으로 강화하는 목표가 처음 명시되었다. 이를 위해 사이버 공격에 대한 통합운용태세와 동맹협력의 강화목표가 명시되었다 (安全保障会議. 2010). 2011년을 전후로 정부 및 핵심 기간시설에 대한 사이버 공격도 증가했다. 2011년 9월 소니에 이어 미쯔비시중공업이 사이버 공격을 받아 잠수함, 미사일, 원자력 등 핵심 기술이 유출되었다(이종락 2011). 11월에는 이미 2010년부터 123여대의 일본 재무성 PC가 APT공격을 받은 자료가 유출된 것이 발견되기도 했다.

아베 2기 내각(2012-2020)은 2013년 기존 '정보시큐리티'를 '사이버시큐리티'로 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).

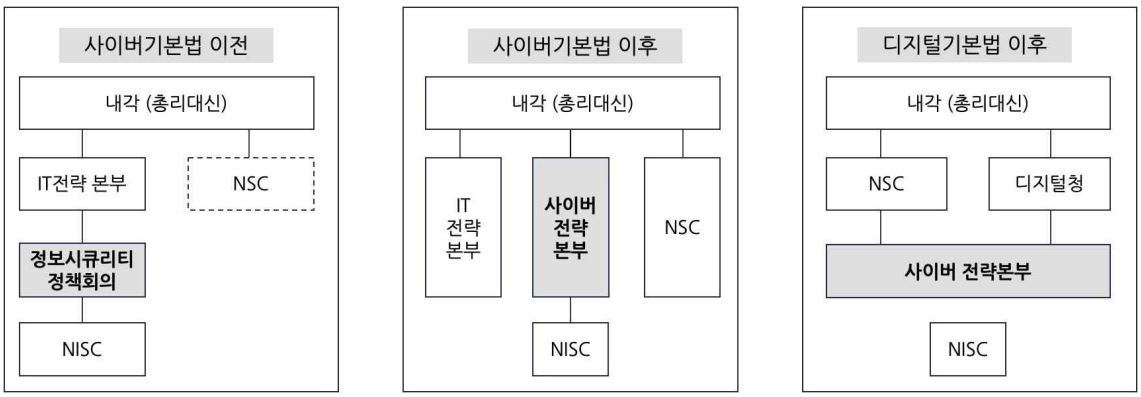
〈표6〉 일본의 사이버 관련 법제, 전략 및 정책구조의 변화

구분	법제와 정책기구		정책구조
이슈연계 단계	법제	• 사이버시큐리티기본법(2014)	전략본부 신설, IT전략본부와 동일한 지위
	기구	• 사이버시큐리티전략본부(2015)	
	전략	• 사이버시큐리티전략(2013) • 사이버시큐리티전략(2015) • 사이버시큐리티전략(2018)	

군사안보 단계	법제	• 디지털기본법(2021)	디지털청과의 협력관계 개편
	기구	• 디지털청(2021)	
	전략	• 사이버시큐리티전략(2021)	

아베내각이 2013년 발표한 사이버시큐리티 전략은 위기관리, 사회경제발전과 안전을 위한 사이버 안보 목표가 명시되었다. 2014년에는 사이버시큐리티 기본법을 제정하였고, 이를 근거로 2015년부터 3년 주기의 사이버 안보전략을 발표하고 있다. 사이버시큐리티 전략은 자유롭고 공정하며, 안전한 사이버 공간을 보장하고, 사회경제적 활력과 지속가능한 발전, 안전한 사회건설, 국제사회와 국가안보의 평화와 안전을 보장하는 안보개혁의 목표와 일체화되었다. 정보의 자유보장, 사이버 법치, 개방성, 자율성과 다중 이해관계자와의 협력 등의 정책목표는 2018년의 사이버 전략에도 공통적으로 반영되었다. 트럼프-시진핑 체제를 거치면서 적대적 미중관계가 본격화되고 전후 방위규범이 변경한지 5년 만에 '다층적통합방위'이 등장한 2018년 사이버 전략에서 주목되는 것은 방어, 억지, 상황인식을 위한 사이버전략이다. 2015년 미일동맹에 기반한 사이버 억지력이 강조된 것과 달리 2018년 사이버전략은 사이버 공격에 대한 탄력성(resilience)를 확보하고 방어할 수 있는 사이버 전략을 강조했다 (情報セキュリティ政策会議 2018, 37-39). 사이버 공격의 방어, 억지를 위해 정치적, 경제적, 기술적, 법적, 외교적 수단을 효과적으로 활용하되 사이버 위협에 단호하게 대처하기 위한 자위대의 역량강화 목표가 제시되었다. 관련하여 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). 사이버 상황인식 능력의 강화를 위해 국내 사이버 거버넌스의 협력체계를 재편하는 것은 물론, 공동훈련, 정책공조, 능력구축, 위기대응 등을 협력한다.

〈그림1〉 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 위기가운데 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 사이버안보전략은 이전과 비교하여 특징적 변화가 있다. (1) 디지털 변혁과 사이버 안보의 동시적인 추진이 명시된 것과 함께, (2) 이전과 달리 중국, 러시아, 북한의 사이버위협으로 명시하고 있으며, (3) 보호, 방어에 국한되지 않고 능동적 억지를 위한 공세전략이 명시되었다. 사이버 위협의 억지와 방어를 위해 미일동맹협력과 함께 다자협력과 국제규범, 신뢰구축을 위한 일본주도의 역할도 강조되었다.

〈표7〉 아베내각 이후 방위성의 사이버 전략

구분	법제와 정책기구
2012	• 미일정상, 사이버 문제에 대한 정부간 협력 합의 • 방위성, 자위대 사이버 공간의 안정적, 효율적 이용 책정
2013	• 미일정상, 제1회 사이버대화 개최 • 사비어방위협의회 (CDC) • 미일 사이버방위 정책 워킹그룹 설치
2014	• 자위대 지휘통신시스템부대 사이버방위대 신편 (3월) • 사이버시큐리티 기본법 제정 (11월)
2015	• 사이버시큐리티 전략본부 설치 • 2015 사이버시큐리티 전략
2016	• 방위성, 사이버시큐리티·정보화 심의관 신설
2018	• 나토 사이버방위협력센터(CCDCOE) 참가 • 사이버시큐리티기본법 개정 (12월)
2019	• 나토 사이버방위협력센터 방위성 직원 파견 • 사이버시큐리티협의회 설치 • 미일안보협의회, 사이버 공격 무력공격사항 확인 • 나토주도 사이버방위연습 최초 참가
2021	• 나토 사이버방위협력센터 주도 훈련 참가 • 2021 사이버시큐리지전략
2022	• 육해공 공동부대 사이버방위대 신편 (4월)
2023	• 미일안보협의회의 (2+2), 반격능력 및 우주·사이버 분야 협력, 장비기술협력 등의 추진 합의

자료: 방위백서 (2023), P. 117.

특히, 사이버시큐리티를 위한 군사적 대외협력이 적극 추진되었다. 민주당 내각에서 사이버 방위능력의 강화목표가 제시된 이후 미국, 아세안, EU와의 동맹차원의 협력목표가 제시되었고, ARF, APEC, ASEAN에서 사이버 안보문제의 담론화를 주도하는 한편 IUT, FRIST 등 국제기구와의 협력도 확대했다. 사이버 안보의 군사화를 추진한 아베내각 이후 방위력 부분의 조직, 정책변경은 물론 대외협력도 확대외었다. 우선 사이버 안보는 미일동맹 협력의 강화를 위한 안보개혁의 핵심의제로 추진되었다. 2013년 미일은 제1회 사이버대화를 개최하였고, 미일 사이버방위정책워킹그룹을 설치했다. 2018년 나토의 사이버방위협력센터(CCDCOE)에 처음 참가하였고, 2019년에는 나토가 주관하는 사이버방위연습에 최초로 참가했다. 2022년 지휘통신부문의 하위부대로 개편되었던 사이버방위대를 육해공의 공동부대포 신편하고, 정원도 4,000명 규모로 확장했다. 기시다 내각 출범 이후에는 반격능력을 포함하여 능동적 억지를 위한 사이버 능력의 강화

와 함께 우주·사이버·전자기 영역을 통합하여 전략, 장비 및 기술협력을 진전시키고 있다.

2000년대부터 사이버 공간을 안보화 하고 안보개혁과 연계하여 추진되고 있는 일본의 사이버 안보전략에서 국제협력의 핵심 목표는 사이버 법치(cyber rule of law), 역량구축(capacity building), 신뢰구축 (Cyber CBMs) 세 가지다. 2000년대 정보시큐리티 정책이 경제기반 사이버 위협의 보호에 중점을 두었다면, 아베 내각 이후 사이버시큐리티 정책은 군사적, 안보적 이해가 우선했다. 특히, 사이버, 디지털 관련 대외협력은 적극적 평화주의에 따라 규칙기반 다자주의와 가치, 규범기반 국제협조주의를 대외전략의 기본이념으로 추진한 아베 내각의 대외전략에서 중요한 비중을 차지했다(신승휴 2023, 201-204). 또, 미일동맹협력을 강화하는 수단일 뿐만 아니라 미중경쟁 가운데 국제적인 역할과 위상의 자율성을 확대하는 영역이었다. 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) 동지국과의 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 일본주도의 역할을 했다.

〈표8〉 일본 사이버 안보전략과 국제협력

구분	법제와 정책기구	
이슈연계 단계	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
군사안보 단계	2021	• 사이버 공간은 지정학적 긴장을 대변하는 영역(중국, 러시아, 북한) • 정보의 자유 보장, 법치, 개방성, 자율성, 다중이해관계자 협력

둘째, 포괄적인 안보개혁과 함께 정보보호에서 안보이슈와 연계된 사이버전략이 추진된 아베 내각 이후에는 양자차원의 사이버 협력 및 기술, 제도, 인적교류, 위기대응 등으로 협력영역이 확대되었다. 2013년 일본의 사이버시큐리티전략이 발표된 이후 미국, EU, 프랑스, 호주, 에스토니아, 베트남 등 양자 간의 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 설

치된 이후 작전적 수준의 공동훈련이 본격화되었다. 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. 특히, 미일 2+2회담에서는 사이버 공격이 미일안보조약의 5조에 규정된 무장공격을 구성한다는 점에 합의하고, 사이버 방어 및 억지능력의 증진을 위한 협력에 합의했다.

〈표9〉 일본의 사이버 국제협력 목표와 대상

목표	사이버 법치	사이버 공간, 활동, 기반에 대한 국제법, 규범제정
	CBMs	사이버 갈등 관리를 위한 투명성, 안정성
	능력구축	기술적, 디지털 역량구축 및 인적자원 개발
협력	양자	인도(2011), 영국(2012), 미국(2013), EU(2014), 프랑스(2014), 이스라엘(2014), 호주(2015), 에스토니아(2018), 독일(2016), 러시아(2015), 한국(2016), 우크라이나(2016), 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, 괄호안의 연도는 양자간의 정기적인 대화 또는 협의가 시작된 해임

V. 결론 및 함의

물리적, 비물리적 공간의 다영역성과 위협의 가변성에 따라 다층적, 총체적 대응이 모색되어온 사이버안보전략에서 일본은 2000년대 부터 사이버 공간을 안보화하고 사이버안보전략, 사이버 거버넌스와 국제협력을 추진하고 있다. 전략적 측면에서 사이버 공간의 안보화 담론이 시작된 2000년대 사이버 전략이 정보호보 차원의 사이버 독트린이 체계화되었다. 이 시기 사이버 전략은 (1) 정보보호를 위한 국내적 사이버 거버넌스의 체계화와 함께, (2) 사이버 안보를 전통 안보의 영역으로 인식하고 (3) 경제협력의 기반이자 국제사회에서의 위상과 역할 확대하는 외교안보의제로 활용했다. 2000년대 미국이 주도하는 사이버 공간의 안보화 담론을 일본이 가장 먼저 수용하고 제도화한 것은 전후 구속에 따라 경제, 사회 등 비군사적 현안을 안보화하는 일본의 정치구조와 전략문화에 큰 요인이 있다고 평가할 수 있다(Katzenstein and Okawara 1993). 고이즈미 내각 집권 시기는 전후 일본문제가 정치화, 안보화된 시기다. 사이버 공간의 안보화는 9/11 테러 이후 새로운 안보위협에 대한 인식이 고조되는 가운데, 경제, 환경, 평화 등 비군사적 안보현안이 전통안보화 되었다. 아울러, 사이버 안보문제에 대한 국제협력을 통해 탈냉전 이후 보통국가로서의 위상과 역할을 모색하는 국가정체성도 투영되었다.

아베 내각 이후 사이버전략은 포괄적인 안보개혁의 맥락에서 위협주체와 국내외의 행위자에게

영향을 미치는 '전략'으로 전환되었다. 그리고 미중경쟁이 본격화된 2018년 방위규범이 개정 이후에는 방어, 억지, 상황인식에 대한 전략이 구체화된 이후 2021년 사이버전략은 능동적 억지를 포함하는 사이버 전략이 구체화되었다. 아베 내각 이후 사이버 공간의 군사화가 본격화되었으며 방어, 억지는 물론 공세적인 사이버 전략을 위한 체계, 규범과 기능이 강화되고 있다. 사이버 안보의 군사화는 미일동맹의 협력의제 뿐만 아니라 미국의존 안보전략의 탈중심화(decentering) 및 네트워크 동맹의 전환을 주도하는 일본의 안보전략과 연계되어 있다 (Midford 2018). 그리고 2021년에는 20여 년간 디지털관련 정책의 법적기반이 되어왔던 IT기본법을 대체하여 디지털 기본법을 제정하고 디지털 전환을 포함한 포괄적인 사이버 국가책략을 추진하고 있다. 디지털 전환정책은 사이버 안보뿐만 아니라 국제협력, 경쟁우위를 포함하는 사이버 국가책략이 포괄적으로 포함되어 있다.

단계적, 점진적으로 전환되어 온 일본의 사이버 안보전략은 제도적, 전략적 시각에서 한국의 사이버전략에 정책적 함의를 제공한다. 우선 포괄성, 다원성, 총체성을 가진 사이버 전략의 효과적인 추진을 위해 포괄적 사이버 법제로 제도화할 것인가, 아니면 개별적 법제로 다원화할 것인가의 문제다. 둘째, 사회전반의 총체적 현안으로서 사이버 안보전략의 거버넌스를 구축하는 문제다. 일본은 2000년대 정부주도 거버넌스 체계에서 아베 내각 이후 정부주도 거버먼트 체계로 전환되었다. 또, 일본은 국가안전보장회의가 디지털 기술(디지털청), 사이버 안보(사이버전략본부) 관련 기관을 총괄한다. 반며느, 한국은 공공부문은 국가정보원, 민간부문은 과기부가 담당하는 분권화, 협력적 거버넌스가 구축되어 있다. 셋째, 다자적, 대외적 사이버 안보협력을 위한 관여, 협력과 전략이다. 일본은 2000년대부터 사이버 안보협력을 주도하는 '일본모델'을 추진해왔다. 사이버 공간의 안보화시기 국제협력은 외무성이 국제협력을 주도했다면, 사이버 공간의 군사화 시기에는 사이버 외교(cyber diplomacy), 사이버 ODA를 주도하는 외무성 (총합외교정책국 경제안전보장정책실 소관), 디지털 기술, 데이터와 육성관련 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. 캠프데이비드 선언 이후 사이버 안보가 한미일의 공동협력 과제로 합의된 만큼 전략, 기술적인 능력은 물론 작전수준에서 사이버 합동상의 강화를 위한 검토도 요구된다.

〈참고문헌〉

김상배, 2002. “세계표준의 정치경제: 미일 컴퓨터 산업경쟁의 이론적 이해.”『국가전략』제8권 2호, 113-135.

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

김상배. 2023. “사이버 억지의 새로운 개념화: 한미 사이버 안보동맹론의 성찰적 맥락에서” 『국제정치논총』제63집 2호, 51-88.

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

원병철. 2019. “:2009년 7.7 디도스 대란, 대한민국 인터넷 시한부 선고.”『보안뉴스』(7월 1일) https://m.boannews.com/html/detail.html?idx=81012&kind=2 (검색일: 2024.03.17.).

신승휴. 2023. “사이버 안보이슈에 대한 일본의 대응과 아베 정권의 국제적 역할인식: 역할이론과 존재론적 안보의 시각.”『아세아연구』제63권 3호, 181-214.

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.

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

조진구. 2023. “국가안전보장전략 개정의 의미와 내용 평가.” 박영준 외,『일본 안보고나련 정책 3문서 개정 결정의 의미와 평가』경남대극동문제연구소, 15-36.

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.)

Bartlett, Benjamin. 2019. “How Japanese Cybersecurity Policy Changes.” Harvard Program on US-Japan Relations Paper Series No.2019-01. https:// projects.iq.harvard.edu/files/us-japan/files/19-01_bartlett.pdf (검색일: 2024.03.17.)

Cambell, John C. 2014. How Policies Change: The Japanese Government and the Aging Society. Princeton: Princeton University Press.

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

Hughes, Christopher W. 2017. “Japan’s Emerging Trajectory as a ‘Cyber Power’: From Securitization to Militarization of Cyberspace.” Journal of Strategic Studies 40:1-2, 118-145.

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: Structures, Norms, and Policies." International Security 17:4, 84-118.

Matsubara, Mihoko. 2018. "How Japan's Pacificst Constutution Shape Its Approach to Cyberspace." Council on Foreign Relations (May 2018) https://www.cfr.org/blog/how-japans-pacifist-constitution-shapes-its-approach-cyberspace (검색일: 2024.02.20.)

Matsubara, Mihoko. 2018. "How Japan's Pacifist Constitution Shapes Its Approach to Cyberspace." CFR Netpolitics (May 23) https://www.cfr.org/blog/how-japans-pacifist-constitution-shapes-its-approach-cyberspace (검색일: 2024.03.17.)

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.).

Ranger, Steve. 2017. "US Intelligence: 30 Countries Building Cyber Attact Capacity." https://www.zdnet.com/article/us-intelligence-30-countries-building-cyber-attack-capabilities/ (검색일: 2024.03.17.).

The White House. 2003. "The National Strategy to Secure Cyberspace." (Febuary) https://nsarchive.gwu.edu/document/21412-document-16 (검색일: 2024.05.10.).

USCYBERCOM. 2018. "Achive and Maintain Cyberspace Superioty." https://s3.documentcloud.org/documents/4419681/Command-Vision-for-USCYBERCOM-23-Mar-18.pdf (검색일: 2024.03.17.).

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

Xu, Yini. 2019. "US-Japan Cyber Alliance." The Edwin O. Reichauer Center for East Asian Studies, ed. The United States and Japan in Global Context. Washington, DC: The Johns Hopkins University, 57-76.

サイバーセキュリティ戦略本部. 2015. "サイバーセキュリティ政策に係る年次報告." (2015.07.23.)

ニュートン·コンサルティング株式会社. 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 (검색일: 2023.05.25.).

三角，育生．2015．“我が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.).
内閣官房情報セキュリティセンター．2012．“2011 年度の情報セキュリティ政策の評価等.” (2012.07.04.)
安全保障会議．2010．“平成23年度以降に係る防衛計画の大綱について.” https://www.kantei.go.jp/jp/kakugikettei/2010/1217boueitaikou.pdf (검색일: 2024.03.18.).
情報セキュリティ対策推進会議．2010．“重要インフラのサイバーテロ対策に係る特別行動計画.” https://www.nisc.go.jp/pdf/council/seisaku/ciip/dai1/1sankosiryou2.pdf (검색일: 2024.05.10.).
情報セキュリティ政策会議．2005．“重要インフラのサイバーテロ対策に係る行動計画.” https://www.nisc.go.jp/pdf/policy/infra/infra_rt.pdf (검색일: 2024.03.17.)
情報セキュリティ政策会議．2010．“国民を守る情報セキュリティ戦略”(2010.05.11.).
情報セキュリティ政策会議．2013．“サイバーセキュリティ戦略”(2013.06.10.).
情報セキュリティ政策会議．2013．“サイバーセキュリティ国際連携取組方針: j-initiative for Cybersecurity.”(2015.10.02.).
情報セキュリティ政策会議．2014．“サイバーセキュリティ政策に係る年次報告.”(2014.07.10.)
情報セキュリティ政策会議．2015．“サイバーセキュリティ戦略”(2015.09.04.).
情報セキュリティ政策会議．2018．“サイバーセキュリティ戦略”(2018.07.27.).
情報セキュリティ政策会議．2021．“サイバーセキュリティ戦略”(2021.09.28.).
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.).
自由民主党．2022．"新たな国家安全保障戦略等の策定に向けて提言: より深刻化する国際情勢下におけるわが国及び国際社会の平和と安全を確保するための防衛力の抜本的強化の実現に向けて." https://storage.jimin.jp/pdf/news/policy/203401_1.pdf (검색일: 2023.07.10.).
防衛省．2022．“自衛隊サイバー防衛隊の新編について” https://www.mod.go.jp/j/publication/wp/wp2022/html/nc007000.html (검색일: 2024.03.10.)

이 글의 내용은 필자 개인의 견해이며
한국사이버안보학회의 공식 입장이 아닙니다.