DOI https://doi.org/10.35506/jspace.2024..35.004

일본의 '능동적 사이버 방어(ACD)' 수용과 전수방위 원칙

이정환 _ 서울대학교 정치외교학부 부교수

목 차

국문초록

일본 정부는 2022년 안보3문서에서 명시된 '능동적 사이버 방어' 개념 도입에 대한 법적 기반 구축 작업을 진행하고 있다. '능동적 사이버 방어' 개념은 헌법 21조의 통신 비밀 규정과 헌법 9조에 대한 전수방위 원칙과 논리적으로 충돌하기 때문에, 이에 대한 논리 체계 구축 작업이 요구되는 상황이다. 사이버공간에서 잠재적 공격을 감시하고, 공격자를 특정하고, 이에 대한 실력 대항조치를 전방 방위로 추진하는 '능동적 사이버 방어' 개념의 도입 자체는 이미 결정된 미래다. '능동적 사이버 방어'는 미국 주도의 국제표준으로서 수용되고 있다. 일본의 보통국가화는 외부 위협에 대한 적극 대응이 필요하다는 논리와 더불어 일본의 국가 역할이 다른 국가들과 동일 해야 한다는 보편주의적 국제주의 논리에 입각해 전개되고 있다. 미국 주도로 새로운 국제 규범이 되고 있는 '능동적 사이버 방어'의 도입은 국제표준 수용 차원에서 당연한 것으로 일본 정책관여자들에게 인식되는 사항이다. 국제표준 수용으로서의 정책 변화에도 불구하고, 일본은 국제표준에 맞춘 헌법 해석 변경을 전면적으로 추진하지 않고

있다. ‘능동적 사이버 방어’ 수용은 글로벌 보편 현상인 가운데, 새로운 국제표준이 된 ‘능동적 사이버 방어’와 정합성을 지니는 차원의 적극적 국내 법제도 변경을 회피하는 것은 일본의 특수적 현상이다.

주제어
일본 사이버안보 정책, 능동적 사이버 방어(ACD), 전수방위, 안보3문서

Ⅰ. 서론

일본 정부의 사이버안보 정책에 대한 평가는 양가적이다. ITU(International Telecommunication Union)가 2021년에 발간한 *Global Cybersecurity Index 2020*에서 일본은 100점 만점에 97.82점으로 194개 평가 대상 국가 중 7위였다.[1] 2022년에는 9위, 2023년에는 10위로 다소 하락하였다.[2] 하지만, 2021년 순위에서도 미국(1위), 영국, 사우디아라비아(공동 2위), 에스토니아(3위), 한국, 싱가포르, 스페인(공동 4위), 러시아, 아랍에미리트, 말레이시아(공동 5위), 리투아니아(6위)에 이은 실제 12위였음을 고려하면, 큰 폭의 변화라 보기 어렵다. 일본의 사이버안보 정책에 대한 대표적 전문가인 게이오대학의 쓰치야 모토히로(土屋大洋) 교수가 말하듯, 근래 도쿄올림픽 등의 대규모 국제 이벤트에서 사이버 분야에서의 큰 안보 문제가 없었던 점을 고려하면 전통적 보안 측면에서 일본의 사이버안보 대응능력은 준수하다고 볼 수 있다.[3] 반대로 영국의 IISS(International Institutes for Strategic Studies)가 2021년에 발표한 “Cyber Capabilities and National

1) International Telecommunication Union, *Global Cybersecurity Index 2020* (Internaitonal Telecommunication Union. 2021), p.25.
2) 国際文化会館地経学研究所,『経済安全保障とは何か』, 東洋経済新報社, 2024, p.88.
3)「能動的にサイバー防御 めざせ攻めの法整備【日経モーニングプラFT】」, https://txbiz.tv-tokyo.co.jp/plusft/feature/post_281495 (검색일: 2024. 4. 30).

Power: A Net Assessment"에서 일본은 조사 대상국 15개국에 대한 정부 능력 평가에서 최하위 그룹에 속했다.[4] 또한, 일본 내에서는 일본 정부의 사이버안보 정책에 대한 불안한 시선이 지속되고 있다. 마쓰무라 마사히로(松村昌廣) 교수가 소개하듯이 쓰치야 교수를 포함한 일본 내 여러 사이버안보 정책 전문가들은 일본의 사이버안보 정책이 사이버공간의 안보 위협에 대응하기에 부족하다는 인식을 공유하고 있다.[5]

이러한 상반된 평가는 최근 사이버안보에 대한 글로벌 정책 지향이 '능동적 사이버 방어(ACD, Active Cyber Defense)'로 수렴하는 가운데, 일본의 사이버안보 정책에서 '능동적 사이버 방어' 원칙 수용이 더디기 때문이다. '능동적 사이버 방어'는 '실시간으로 공격을 인지하고 분석해 네트워크와 국가 경계를 넘는 적극적인 방법을 사용해서 네트워크 보안 침해를 경감하는 것'으로 정의된다.[6] '능동적 사이버 방어' 개념에 입각한 사이버안보 정책은 공격을 감지하기 위한 국경을 넘는 감시와 선제적인 실력행사의 대응 방법을 포함하고 있다. 일본 정부는 2022년 12월 발행한 「국가안보전략」에서 '능동적 사이버 방어'를 일본의 사이버안보 정책의 향후 추진 방향으로 설정하였다.[7] 이는 글로벌 추세에 부합하는 방향으로 정책 변화를 꾀하고, 지금까지의 수동적 성격과 차별화되는 사이버안보 정책을 추진하겠다는 일본 정부의 정책 목표를 드러내고 있다.

---

4) IISS, "Cyber Capabilities and National Power: A Net Assessment," https://www.iiss.org/research-paper/2021/06/cyber-capabilities-national-power/ (검색일: 2024. 4. 30).
5) 松村昌廣, 「我が のサイバーセキュリティ戦略の欠点と展望―「平和国家」体制の桎梏への対応を考える」, 『情報通信政策研究』 5.2, 2022, pp.73~94.
6) 笹川平和財団新領域研究会, 『新領域安全保障 サイバー·宇宙·無人兵器をめぐる法的課題』, ウェッジ, 2024, p.140.
7) 「国家安全保障戦略」, https://www.mod.go.jp/j/policy/agenda/guideline/pdf/security_strategy.pdf (검색일: 2024. 4. 30), pp.21~22.

하지만, 2022년 「국가안보전략」에 포함된 여타 중요 내용들 – 반격능력 보유, 통합사령부 신설, 방위비 증강 등 – 에 비해 사이버 분야의 '능동적 사이버 방어' 원칙 도입을 위한 법적 기반 정비는 더디게 진행되고 있다. 2023년 초에 '능동적 사이버 방어' 원칙에 입각한 정책 거버넌스와 법제 개편을 위해서 내각관방 산하에 〈사이버안전보장체제정비준비실(サイバー安全保障体制整備準備室)〉이 설치되었고, 2024년 상반기 법제화의 일정 목표가 제시되었다.[8] 하지만, 2024년 상반기의 법제화 시도는 이미 유보되었고, 현재 2024년 하반기 법제화를 위한 유식자회의 설치 및 연립 여당 내 의견 조정이 진행되고 있다. '능동적 사이버 방어' 개념 도입을 통한 사이버안보 정책의 전환이 더디게 진행되는 핵심 이유는 '능동적 사이버 방어' 개념이 일본의 헌법 해석과 충돌하는 성격에서 기인하는 연립 여당 내 의견 조율 지체에 있다.

'능동적 사이버 방어' 개념은 헌법 21조의 통신비밀과 검열금지와 충돌할 가능성이 있다. 더불어 9조에 대한 일본 정부의 오랜 해석인 전수방위 원칙과도 충돌한다. '능동적 사이버 방어' 개념 도입은 이 헌법 조항에 대한 해석과의 충돌을 해소해야 하는 과제를 지니고 있다. '능동적 사이버 방어'는 사이버공간에서 공격과 방어의 구별이 불분명한 가운데, 방어를 위한 공격적 방법을 활용한다는 의미를 내포하고 있다. 집단적 자위권에 대한 해석 변경, 기반적 방위력 개념 폐기 등으로 상징되듯 일본 정부는 지난 10여 년간 기존의 안보규범에 대한 큰 폭의 변화를 가져왔지만, 전수방위 원칙은 여전히 유지하고 있다. '능동적 사이버 방어' 개념 도입은 반격능력 보유와 함께 전수방위 원칙과 논리적으로 공존하기 쉽지 않은 사안이다. 반격능력 보유의 논리 설계와 마찬가지로 일본 정부는 전수방위 원칙의 유지 속에서 '능동적 사

8) 「「能動的サイバー防御」準備室、内閣官房に新設 政府」, 『日本経済新聞』 (2023. 1. 31), https://www.nikkei.com/article/DGXZQOUA3186D0R30C23A1000000/ (검색일: 2024. 4. 30).

이버 방어' 개념을 도입하고자 하며, 이를 위한 논리 설계 작업과 이에 대한 연립 여당 내의 의견 조정에 예상보다 시간이 많이 소요되고 있다.

본 연구는 일본이 '능동적 사이버 방어' 개념을 도입하고자 하는 맥락을 설명하고, 새로운 사이버안보 정책의 방향성인 '능동적 사이버 방어' 개념이 기존의 헌법 해석과 어떠한 모순적 지점을 지니는지에 대해 분석하고자 한다. 이를 통해서 앞으로 일본 정부가 '능동적 사이버 방어' 개념을 어떻게 전수방위 원칙과 부합해서 설명하려는 지에 대한 함의를 제공하고자 한다. 본 논문의 핵심적 주장은 반격능력 도입에 대한 논리 설계와 마찬가지로 '능동적 사이버 방어'에 대한 논리 설계는 미국이 주도하는 '능동적 사이버 방어'의 글로벌 확산 속에서 국제적 표준에 대한 일치화라는 보편주의적 국제주의 관점에서의 국가 역할 인식 속에서 이루어지고 있으며, '필요최소한'의 관점에서 구성되었던 특수주의적 성격을 지니는 기존의 일본 안보 규범이 형해화되고 있다는 것이다. '능동적 사이버 방어' 개념 도입은 전수방위 원칙의 내용적 실체가 공동화되어 가는 최근 일본 안보 정책 변화의 흐름을 보여주는 대표적 사례다.

일본의 사이버안보 정책에 대해서는 한국 내에서 이승주(2017), 이상현(2019a, 2019b), 박성호(2022), 신승휴(2023)의 연구가 존재한다. 이들 연구는 2010년대 일본 정부의 「사이버안보기본법」 제정과 「사이버안보전략」 문서의 안보적 성격에 대해 분석하고 있다.[9] 이를 통해 2010년대에 일본 사

9) 이승주, 「일본 사이버안보 전략의 변화: 사이버 안보의 전통 안보화와 전통 안보의 사이버 안보화」, 『국가안보와 전략』 17.1, 2017, pp.173~202; 이상현, 「일본의 사이버안보 수행체계와 전략」, 『국가안보와 전략』 19.1, 2019a, pp.115~154; 이상현, 「사이버 위협에 대한 일본의 대응: 사이버 외교와 사이버 방위」, 『국가전략』 25.2, 2019b, pp.91~117; 박성호, 「일본의 사이버 안보전략 – 양자주의의 강화인가 다자주의로의 전환인가?–」, 『일본학』 56, 2022, pp.159~182; 신승휴, 「사이버 안보이슈에 대한 일본의 대응과 아베 정권의 국제적 역할인식: 역할이론과 존재론적 안보의 시각」, 『아세아연구』 63.3, pp.181~214.

이버안보 정책이 「방위계획대강」의 변화와 연계되어 안보화되어 가는 양상을 보여주고 있다. 이들 연구가 연구 대상으로 삼고 있는 2010년대 일본 사이버안보 정책의 변화는 본 연구가 중심적으로 다루고 있는 2022년 안보 3문서 제정 이후의 '능동적 사이버 방어' 개념 도입의 정책 과정에 대한 역사적 조건이 된다. 일본에서도 일본 사이버안보정책에 대한 핵심 연구 대상은 2010년대 전개된 사이버공간의 안보화이다. 土屋大洋(2015), 谷脇康彦(2018), 松村昌廣(2022), 川口貴久(2019) 등의 연구도 국제규범 변화 속에서 일본의 사이버안보 정책의 안보화를 중점적으로 논하고 있다.[10] 한편, Kawaguchi(2023)는 일본의 최근 '능동적 사이버 방어' 개념의 도입을 다룬 거의 유일한 연구에 가깝다. 이 연구는 일본의 최근 '능동적 사이버 방어'와 2010년대 방어 위주의 사이버안보 정책을 공존하는 두 개의 접근법으로 관찰하고 있다.[11] 국내외 연구 모두 일본 사이버안보 정책의 2010년대 변화에서 사이버공간에 대한 국제규범 변화의 영향을 중요 요인으로 강조하고 있으며, 본 논문도 그러한 흐름에서 최근 '능동적 사이버 방어' 개념 도입을 통한 일본 사이버안보 정책의 전환을 살펴보고 있다.

본 논문의 구성은 다음과 같다. II에서는 2022년 이후 일본 정부가 '능동적 사이버 방어' 개념 도입을 공식화하기 이전까지 일본 사이버안보 정책의 변화와 그 성격의 특징을 2010년대를 중심으로 설명할 것이다. III에서는 국제사회에서 사이버공간의 안보 문제를 어떻게 다룰 것인지에 대한 규범 갈등

10) 土屋大洋, 『サイバーセキュリティと国際政治』, 千倉書房, 2015; 谷脇康彦, 『サイバーセキュリティ』, 岩波書店, 2018; 松村昌廣(2022); 川口貴久, 「サイバー空間における『国家中心主義』の台頭」, 『国際問題』 683, 2019, pp.37~46.

11) Takashisa Kawaguchi, "Two Approaches to Responding to Destructive Cyberattacks on Critical Infrastructure in Japan: Addressing Cyber Crises as "Service Failures" or "Armed Attacks," in Yasuhiro Takeda, Jun Ito, and Yusuke Kawashima (eds.), *Civil Defense in Japan* (Routledge, 2023), pp.180~195.

속에서 미국 주도의 '능동적 사이버 방어'가 확산하는 흐름과 그 흐름에 맞춘 법제화가 일본에서 수월하게 이루어지기 어려운 애로 사항에 대해 분석하고, Ⅳ에서는 2022년 이후 '능동적 사이버 방어' 개념 도입 공식화 이후의 정책 과정에 대해 분석할 것이다.

Ⅱ. 일본 사이버안보 정책의 전개

1. 사이버안보 정책의 형성과 거버넌스

다른 나라와 마찬가지로 일본의 사이버안보 정책도 IT 정책과 연계되어 탄생하였다. 하지만, 초기 IT 정책 구상에서 사이버시큐리티는 중점적 정책 고려 대상은 아니었다. 물론 2000년에 〈내각관방정보시큐리티대책추진실〉이 설치되었지만, 사이버공간의 시큐리티에 대한 인식 자체가 크게 진척되어 있었다고 보기 어렵다. IT와 관련된 일본 내 최초 입법의 위상을 지니는 「IT기본법」(고도정보통신네트워크사회형성기본법, 2001년 시행)과 이와 연계되어 책정된 「e-Japan전략」 모두 네트워크 정비와 인재 양성 등에 초점이 모여 있었다.[12] 시큐리티에 대한 체제 정비는 2005년 〈내각관방정보시큐리티센터〉(NISC)가 설립되면서 출발했다고 볼 수 있다. 더불어 NISC에 대한 정책 결정 조직으로 IT전략본부 산하에 〈정보시큐리티정책회의〉가 설치되었다. 2000년 〈내각관방정보시큐리티추진실〉에서 2005년 〈내각관방정보시큐리티센터〉로 기능 강화가 모색되는 과정에서는 〈고도정보통신네트워크사회추진전략본부〉의 정책 제언과 의견 수렴 과정이 존재했다.[13]

현재 일본 사이버안보 정책의 중심적 조직인 NISC는 2005년에 구성되

12) 谷脇康彦.(2018), kindle location 1418.
13) 「内閣サイバーセキュリティセンター(NISC)について」, https://www.nisc.go.jp/about/history/index.html (검색일: 2024. 4. 30).

었지만, 2000년대에 NISC를 중심으로 하는 사이버안보 정책 체제가 구축되었다고 보긴 어렵다. 당시 NISC는 정부 전체의 사이버보안에 대한 사령탑으로서의 위상을 전혀 지니고 있지 못했다. 이에 대한 문제의식 속에서 2013년 「사이버시큐리티전략」에서는 NISC의 기능 강화와 위상 강화가 목표가 제시되었다.[14)]

일본 사이버안보 정책의 핵심 법제인 「사이버시큐리티기본법」은 2013년 「사이버시큐리티전략」의 결과물이다. 「사이버시큐리티기본법」은 2014년 봄에 국회에 제안되었고, 가을 임시국회에서 통과되어 2015년 1월에 시행에 이르게 되었다. 「사이버시큐리티기본법」을 통해 NISC의 위상과 기능은 큰 폭으로 변화하게 되었다. 동일한 영어 약자 NISC로 불리지만, 2015년의 NISC는 National Center of Incident Readiness and Strategy for Cybersecurity의 약자로 2005년 NISC가 National Information Security Center의 약자인 것과 비교할 때 상이한 성격을 지닌다. NISC는 2015년 「사이버시큐리티기본법」에 의해 사이버안보에 대한 정책 결정 조직으로 내각에 설치된 〈사이버시큐리티전략본부〉 (본부장 내각관방장관)의 실무조직 위상으로 〈내각사이버시큐리티센터〉로 새로 출범하게 된 것이다.[15)]

2015년의 〈내각사이버시큐리티센터〉는 2005년의 〈내각관방정보시큐리센터〉와 비교할 때 여러 부분에서 차이가 난다. 우선 다른 부처들과의 관계에서 〈내각사이버시큐리티센터〉는 정보와 데이터를 제공받을 수 있는 권한을 갖게 되었으며, 각 부처의 사이버보안 운용 상황에 대한 감독 권한도 가지게 되었다. 또한 각 부처의 사이버보안 대응을 종합해서 국가 전체의 사이버안보 정책을 일괄적으로 총괄하는 역할도 담당하게 되었다. 그 결과 2015년

14) 谷脇康彦(2018), kindle location 1436.
15) 이상현(2019a), p.134.

부터 3년마다 발행되고 있는 「사이버시큐리티전략」 문서의 작성 주체가 되었다. 위상 강화와 기능 강화 속에서 2013년에 80여 명뿐이었던 NISC 직원 수는 3년 후인 2016년에 180명으로 증가하였다.[16)]

일본 사이버안보 정책의 내용을 파악할 수 있는 핵심 문서인 「사이버시큐리티전략」은 「사이버시큐리티기본법」 시행 이후, 2015년, 2018년, 2021년 세 번 책정되었다. 「사이버시큐리티전략」에 나타난 정책 내용은 크게 세 가지로 정리된다. 첫 번째는 사이버안보와 관련된 민간기업의 투자 촉진 지원이다. 두 번째는 사이버공격에 대한 방어 능력 강화로, 전통적 보안 능력 향상으로 연결되는 정책과제다. 세 번째가 국제협력인데, 이 부분에서 국제적 사이버공격에 대한 대응과 관련된 사이버 정책의 안보화 추세가 발견된다.

현재 일본 사이버안보 정책 내용을 보여주는 2021년 「사이버시큐리티전략」은 2015년 판, 2018년 판과 비교하였을 때, 민간기업 투자 촉진, 사이버보안 강화, 국제협력의 세 축에 서 있다는 점에서 유사하다. 다만, 2021년 시점에서 일본이 강조하던 디지털 개혁에 대한 지점이 강조되어 DX 과정에서 사이버안보에 대한 기업 투자 촉진의 필요성과 중소기업 지원 정책 등이 집중적으로 부각되어 있다. 사이버보안 강화 내용에서는 기업의 기술 유출 방지와 인프라 시설 관리의 취약성 방지 등이 경제안보 정책과 연계되어 새롭게 포장되어 기술되어 있다. 2021년 〈사이버시큐리티전략〉이 내세우는 'Cybersecurity for All' 프레임은 NISC의 위상을 행정부처 사이의 정책 내용을 조정하는 기관에서 민관 전체의 사이버시큐리티 관련 행위들을 총괄하는 기관으로 변모시키려는 노력이기도 하다. 담당하는 기능에서도 정보수집, 정보집약분석, 정책 대응, 대처 조정 등의 기능을 모두 수행하는 것으로 NISC를 변모시키려는 의도를 담고 있다.

16) 谷脇康彦(2018). kindle location 1472.

하지만, NISC의 역할 강화에 대해서는 NISC와 기타 성청과의 관계에서 발견되는 거버넌스적 한계를 넘어설 수 있는지에 대한 의구심이 존재한다. 일본 각 행정부처는 각기 담당 정책 영역에서 사이버안보 정책을 추진하고 있다. 이에 대한 NISC의 위상은 조언자적 위치에서 출발해서 조정자 위치로 발전하였지만, 사이버안보 이슈에 대한 타 행정부처의 상위기관이 되는 것은 제도적으로도 여의찮은 상황이다. 특히나, 정보통신 정책 영역의 총무성, 산업담당의 경제산업성, 경찰청 등은 사이버안보 분야에서 전통적인 자기 영역을 구축해 왔고, 최근 인프라 관리를 담당하는 국토교통성과 새롭게 등장한 디지털청은 NISC의 정책 거버넌스 주도성 확립에 대한 새로운 도전 요인이다.

무엇보다 자체 선발되는 관료집단이 없는 내각부의 NISC 조직은 주요 간부들이 총무성, 경제산업성, 경찰청, 방위성 등에서 파견 나와 유지되고 있다. 내각의 정책 조정 기관으로 NISC가 그 조정 역할을 강화하는 것은 앞으로도 충분히 예상할 수 있는 일이지만, 정보의 수집, 분석, 대처에 대한 실제 업무에 있어서 NISC가 주도성을 확립할 수 있는지는 향후 지속해서 관찰해야 할 부분이다. 현재 논의되고 있는 '능동적 사이버 방어' 도입의 정책 현실화 과정에서 사이버안보에 대한 거버넌스 변화도 함께 논의되고 있는 가운데, NISC의 역할과 위상 변화가 예상된다.

2. 사이버 정책의 안보화 진전

「사이버시큐리티전략」의 개정 과정에서 세 정책 축 – 사이버안보 관련 민간기업 투자 촉진 지원, 전통적 사이버보안 능력 향상, 국제적 사이버공격에 대한 대응 – 은 유지됐다. 그중에서 국경을 넘는 사이버공격에 대한 대응의 중요성은 사이버공간이 전통 안보 영역과 밀접하게 연계되는 가운데 갈수

록 커져 왔다.[17] 기본적으로 국경을 넘어서 발생하는 사이버공격이 외부 국가와 연계된 상황에 대한 대응은 보안의 관점이 아닌 안보 정책 차원에서 인식될 수밖에 없다.

방위성이 사이버안보에 대한 정책적 대응에 본격적으로 나선 시기도 「사이버시큐리티전략」이 처음으로 등장하던 2013년이다. 보안의 관점에서 크게 벗어나지 않는 가운데, 방위성과 자위대 사이버공간의 보안 강화에 더해서 방위산업체에 대한 사이버공격 대응 강화에 초점이 맞추어져 있었다. 방위성은 2013년에 〈사이버디펜스연계협의회(サイバーディフェンス連携協議会, Cyber Defense Council, CDC)〉를 설치하고 이 조직을 매개로 방위산업체의 사이버공격 방어 능력 향상에 초점을 두는 정책을 폈다. 방위산업이 정상적으로 기능하는 것이 방위성-자위대가 그 임무를 수행하기 위한 전제가 되고 있으므로 방위성-자위대와 방위산업체 사이에 파트너십을 구축하여 방위산업체에 대한 사이버공격에 대응하는 능력을 향상하겠다는 것이다. 이것이 〈사이버디펜스연계협의회〉의 설치 목표다.[18] 〈사이버디펜스연계협의회〉가 다루는 내용은 다음과 같다.

1. 표적형 이메일 공격 등 부정통신 방지에 기여하는 정보에 대해 기업 간 정보 공유를 도모하고, 기업 간 정보 공유를 통해 기업 간 정보 탈취를 시도하는 부정통신 방지를 위한 상호 협력 촉진
2. 기업 간 직접적으로 공유하기 어려운 해당 기업에 대한 표적형 공격 등에 관한 정보에 대해 방위성이 개입(허브 역할)함으로써 기업 간 정보 공유를 가능하게 하고, 기업 간 정보 공유를 촉진

17) 이승주(2017), p.173.

18) 「サイバーディフェンス連携協議会(ＣＤＣ)の設置·取組について」, https://www.mod.go.jp/j//////approach/defense/cyber/pdf/cyber_defense_council.pdf (검색일: 2024. 4. 30).

3. 방위산업에 특징적인 사이버 공격 등에 대한 베스트 프랙티스 공유 실시
4. 방위성-자위대와 방위산업체와의 사이버 공격 대응능력 향상을 위한 공동훈련 등을 실시
5. 미국 등의 대응 사례를 참고하면서 방위성-자위대와 방위산업체와의 향후 협력관계를 검토[19]

2010년대 중반 〈사이버디펜스연계협의회〉는 사이버보안 대응 체제를, 방산기업을 대상으로 충실하게 구축하겠다는 수준에 머물러 있었다.

범정부적 수준에서도 2010년대 중반에는 국경을 넘는 사이버 문제에 대한 대응은 적극적이지 않다. 2015년 「사이버시큐리티전략」에서는 해외 국가가 연동된 것으로 의심되는 사이버공격에 대한 대응에 대해서 국제협력 필요성을 중심으로 다음과 같이 기술하고 있다.

> 해외에서 국가의 관여나 실제 공간에서의 군 운영과 연동된 것으로 의심되는 사이버공격 사례도 있음을 고려하면 동맹국 및 같은 입장에 서있는 이른바 유지국·기관 간의 위협 정보 공유나 인재육성 등에서의 협력·연계의 적극적인 추진이 불가결하며, 또한 기타 국가와도 신뢰를 양성해 나가는 것이 중요하다.[20]

2015년 「사이버시큐리티전략」에서 국제적 사이버 문제에 대한 지금과 같은 공세적 태도는 찾아보기 어려우며, 국제협조 및 국내 보안 능력 강화에 초점이 맞추어져 있었다. 하지만, 2018년 「사이버시큐리티전략」에서 국경을 넘는 사이버공격에 대한 대응에 관한 기술은 2015년 버전과 상당히 다르다. 2018년 「사이버시큐리티전략」에서는 사이버공격에 연계된 해외 국가에 대한

19) 주 18)과 같음.
20) 「サイバーセキュリティ戦略 (2015년)」, p.26, https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku.pdf (검색일: 2024. 4. 30).

대항조치의 가능성을 명시하고 있다.

> 악의적 사이버공격 등 무력 공격에 이르지 않는 위법 행위에 대해서도 국제 위법 행위의 피해자인 국가는 일정한 경우에는 해당 책임이 있는 국가에 대해 균형성 있는 대항조치 및 기타 합법적인 대응을 취할 수 있다.[21]

물론 최근 논의되고 있는 '능동적 사이버 방어' 개념과는 다소 다르지만, 2018년 「사이버시큐리티전략」에서 나타나는 사실상의 적국 개념과 자위권 개념의 확립은 일본 사이버안보 정책의 역사적 전개에서 2022년 이후 '능동적 사이버 방어' 개념 도입으로 가는 중간단계의 성격을 지닌다. 2018년 「사이버시큐리티전략」의 안보화된 성격은 2018년 「방위계획대강」의 맥락에서 이해될 수 있다. 아베 신조(安倍晋三) 정권의 적극적인 안보 정책 추진 흐름 속에서 2018년 「방위계획대강」에는 우주, 사이버, 전자파 등의 신흥 영역에서의 안보적 대응이 강조되기 시작하였다. 2018년 「방위계획대강」의 사이버 공간에 대한 인식과 같은 해 「사이버시큐리티전략」의 사이버공간에 대한 안보화된 기술은 연동되어 있다.[22] 사이버안보의 전통 안보화 추세의 배경에 아베 정권기의 적극적 안보 정책이 존재하는 것은 부인하기 어렵다.

2018년 「방위계획대강」에서는 방위성과 자위대의 사이버안보에 대한 역할도 그 이전에 비해서 강화되고 확대되었다. 우선 2014년에 편성된 자위대 사이버방위대의 규모가 확대되었다. 그리고 사이버 분야에서 자위대의 역할의 범위와 강도에 대한 성격이 변화할 수 있는 기술이 발견된다. 2018년 「방위계획대강」에서 사이버 분야에 관한 기술은 다음과 같다.

---

21) 「サイバーセキュリティ戦略 (2018년)」, p.34, https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2018.pdf (검색일: 2024. 4. 30).
22) 이상현(2019b); 박성호(2022); 신승휴(2023).

> 평소부터 우주-사이버-전자파 영역에서 자위대의 활동을 방해하는 행위를 미연에 방지하기 위해 상시 지속적으로 감시하고 관련 정보를 수집-분석한다. 이러한 행위 발생 시에는 신속하게 사건을 파악하고 피해의 국지화, 피해 복구 등을 신속하게 수행한다. 우리나라에 대한 공격 시에는 이러한 대응과 더불어 우주-사이버-전자파 영역을 활용하여 공격을 저지-제거한다. 또한, 사회 전반이 우주공간과 사이버공간에 대한 의존도가 높아지는 추세 등을 고려하여, 관계기관과의 적절한 연계 및 역할 분담하에 정부 전체의 종합적인 대응에 이바지한다.[23]

과거 방위성과 자위대, 그리고 방산업체의 보안에 초점을 두던 방위성과 자위대의 사이버안보에서의 역할은 군사 분야 이외 민간 부분의 사이버 문제에 관여할 수 있도록 확대되었다. 또한 '능동적 사이버 방어'가 도입될 수 있는 '미연에 방지하기 위해'라는 표현이 포함되어 있다. 2018년 「사이버시큐리티전략」과 「방위계획대강」은 일본 정부가 최근 취하고 있는 사이버 공간에 대한 적극적 대응 정책 기조의 전조라 할 수 있다.

Ⅲ. '능동적 사이버 방어'의 글로벌 확산과 일본의 고민

1. 사이버안보에 대한 규범 갈등과 미국주도 규범화

2018년 「사이버시큐리티전략」과 「방위계획대강」의 안보화된 성격은 아베 정권기 적극화하는 안보 정책의 국내적 맥락만으로 설명되지 않는다. 오히려 국제적으로 사이버안보에 대응하는 국제규범의 성격 변화 속에서 일본의 정책 태도 변화가 선명하게 이해될 수 있다. 기본적으로 2010년대 후반은 '능동적 사이버 방어'가 세계적으로 확산하는 시기이다. 이 맥락에서 일본의 사

23) 「平成 31 年度以降に係る防衛計画の大綱」, https://www.mod.go.jp/j/policy/agenda/guideline/2019/pdf/20181218.pdf (검색일: 2024. 4. 30).

이버안보 정책 변화는 2010년대에 진전되어 온 사이버공간에 대한 국제규범 논의와 높은 연계성을 지닌다.

유엔은 사이버공간의 국제규범 창출에서 중요한 무대였다. 유엔의 정보안보정부전문가그룹(GGE, Group of Government Experts)이 논의 결과로 내놓은 2015년 보고서는 사이버공간에 대해 국가 주권, 평화적 분쟁 해결, 내정간섭 금지와 같은 기존 국제법 원칙들이 동일하게 적용되어야 한다는 인식을 명확히 하고, 사이버공간에서의 자위권 행사도 인정되는 것으로 설정하였다. 이 안은 최종 채택되지는 않았는데, 그 이유는 러시아, 중국 및 여러 개도국 등이 사이버공간에서의 자위권과 국제인도법 적용에 대해서 동의하지 않았기 때문이다. 사이버공간에서 위법 행위의 주체 특정에서 미국 중심의 선진국이 가지는 강력한 능력에 대한 부담감이 그 배경이 된다.[24)]

유엔에서의 합의가 도출되지 않는 가운데 선진국은 사이버공간에 대한 국제규범 논의를 G7에서 시도하였다. 일본에서 개최된 2016년 G7 정상회담에서 나온 「사이버에 관한 G7의 원칙과 행동」 문서에서는 '사이버공간에서의 무력공격에 대해서 국가가… 국제연합헌장 제51조에 의거해 개별적 그리고 집단적 자위권의 고유의 권리를 행사한다고 인식'한다는 기술이 포함되어 있다.[25)] G7의 국제규범은 사이버공간에서의 침해 중 일부를 전통적 안보 차원의 무력공격으로 위상지우고 있으며, 이에 대한 국가로서의 대응 자세를 분명하게 하고 있다. 그리고 이는 나토 사이버방위협력센터의 전문가그룹에 의해 작성되고 업그레이드된 2017년 「탈린매뉴얼2.0」에서 선명하게 나타나는 주권규칙과 영역국의 주의의무와 대항조치 가능 내용으로 연결된다.[26)]

일본의 2018년 「사이버시큐리티전략」은 이러한 국제규범 논의 맥락에서

24) 谷脇康彦(2018), kindle location 1698.
25) 谷脇康彦(2018), kindle location 1768.
26) Kawaguchi(2023), p.189.

이해될 수 있다. 주권규칙, 해당국의 주의의무, 침해에 대한 대항조치 권리는 2021년 「사이버시큐리티전략」에 보다 선명하게 나타난다. 일본의 정부 문서에서 사이버공간에 대한 자위권 행사에 대한 명쾌한 기술로의 변화는 미국을 비롯한 선진국이 적극적 억지 입장에 서서 사이버안보정책을 전개하는 가운데, 일본도 동화되는 상황으로 볼 수 있다.

'능동적 사이버 방어' 개념은 이러한 국제규범 논쟁 속에서 2010년대 후반에 선진국 사이버안보 정책의 중심적 개념으로 자리잡게 된다. 선진국 중에서 미국은 '능동적 사이버 방어' 개념을 가장 선도적이고 적극적으로 전개했다.[27] '능동적 사이버 방어' 개념은 미국 학계에서 2009년에 최초로 제기되었다. 공격적정보전연구회는 '공격자의 공격능력을 무력화하는 것과 공격을 위한 비용을 공격자에게 부과하는 것이 능동적 방어'라고 기술하고 있다. 미군 내 '능동적 방어' 개념을 사이버공간에 적용한 것이다. 2011년 미국 국방성의 사이버공간작전전략에서 국방성의 네크워크 시스템을 지키기 위한 새로운 전략으로 'Active Cyber Defense'가 채용되었다. 사이버공간에 대한 적극적 대응 정책으로의 전환은 오바마 행정부 시기에 지속되었으며, 트럼프 행정부 시기에도 그 흐름은 이어졌다. 그 결과로 ACD 전략은 트럼프 정권 시기인 2018년 〈국가사이버전략〉에 완성 형태로 나타나게 되었다. 이 문서에서는 '악의가 있는 사이버 공격자를 억지하고, 추가적 악화를 막기 위해, 미국은 비용을 부과하는 정책을 선택'한다고 명시하고, '사이버 위협에 대응하기 위해 사이버공격의 귀속을 명확히 하고, 외교력, 정보력, 군사력(물리적 전력과 사이버 전략 양면), 자금력, 정보력, 공권력, 법집행능력 등 모든 수단을 동원해서 미국에 대한 악의적 사이버 활동을 특정해 억지하고 방제해서

27) 미국의 사이버안보 개념의 변화에 대해서는 다음을 참조. Alex Wilner, "US Cyber Deterrence: Practice Guiding Theory," *Journal of Strategic Studies* 43.2, 2020, pp.245~280.

결과 책임을 묻는다'고 기술하고 있다. 또한, 악의적 사이버 활동의 근원을 방해하고 정지하기 위해, 적의 영내에서 방위 행동을 시행하겠다는 전방 방위(Defence Forward) 개념을 제시하였다. 이러한 원칙 속에서 미국 국가안전보장국(NSA)도 컴퓨터 네트워크 탐색 활동(CEN)의 이름으로 네트워크 역침입을 통한 정보수집을 시행하고 있다. FBI도 미국 민법의 부정행위방지법을 근거로 능동적 방위 대응을 시행하고 있다.

이러한 ACD 전략은 미국뿐 아니라 영국에서도 채택되었다. 2016년 영국은 〈사이버시큐리티전략〉에서 ACD를 명시했다. 영국 정부도 사이버 공격자를 특정하기 위해 2016년 조사권한법에 근거해 능동적 방어의 기술 대응을 실시하고 있다.[28] ACD 개념은 세계적으로 확산하여 채용되고 있다. 유럽, 서방 국가뿐만 아니라, 중국도 ACD를 사이버안보 정책의 기본 개념으로 위치 지워 발전시키고 있다.[29] 한국도 〈국가사이버안보전략〉에서 ACD 개념에 입각한 사이버 대응을 명시하고 있다.[30]

2. '능동적 사이버 방어'에 대한 국내 법적 근거 마련의 난점

'능동적 사이버 방어' 개념의 채택은 그에 대한 국내 법적 정비가 필요하다. '능동적 사이버 방어'는 공격의 감시와 공격자의 특정, 그리고 그에 대한 자위권 차원의 실력 대응 조치 실시로 구성된다. 일본의 경우 공격의 감시는 헌법 21조의 통신 비밀 조항에 대한 해석의 문제로 귀결되고, 공격자의 특정을 위한 월경과 실력을 통한 대응 조치는 헌법 9조에 대한 전수방위 원칙의

28) 笹川平和財団新領域研究会(2024), pp.189~192.
29) Sven Herpig, "Active Cyber Defense – Toward Operational Norms," https://www.stiftung-nv.de/sites/default/files/snv_active_cyber_defense_toward_operational_norms.pdf (검색일: 2024. 4. 30).
30) 「국가안보실, 윤석열 정부의 '국가사이버안보전략' 수립」, https://www.president.go.kr/newsroom/press/gdXzwtKB (검색일: 2024. 4. 30).

자위권 행사와의 정합성 추구 문제로 귀결된다.

'능동적 사이버 방어' 개념의 도입에 대한 일본 국내 법적 문제에 대해서는 사사카와재단 연구팀의 최근 연구(笹川平和財団新領域研究会, 2023)가 종합적으로 소상하게 분석하고 있다. 이 절에서는 사사카와재단 연구팀의 연구를 중심으로 해서 '능동적 사이버 방어' 개념 도입에 있어서 발생하는 일본 국내 법적 해석의 문제점을 논하고자 한다. 단, 사사카와재단의 연구는 헌법 9조 해석에 있어서 전수방위 원칙과 충돌하는 지점에 대한 내용은 적극적으로 담아내고 있지 않다. 반대로 일본 리버럴 미디어에서는 '능동적 사이버 방어'에 대한 헌법 9조의 전수방위 원칙 해석과의 충돌 성격을 적극 지적했다.[31] '능동적 사이버 방어' 개념 도입을 위해 필요한 법적 조치를 제언하고 있는 사사카와재단 연구가 '능동적 사이버 방어' 개념과 전수방위 원칙과의 충돌 문제에 대해 소극적으로 기술하고 있는 점 자체가, '능동적 사이버 방어' 개념 도입이 헌법 개정과 함께 이루어질 수 없는 가운데 이 개념 도입이 헌법 9조에 대한 또 다른 지적 곡예와 함께 이루어질 밖에 없음을 암시해 준다.

사사카와재단 연구팀 연구는 헌법 21조의 통신 비밀 조항과의 법적 정합성 문제를 중시한다. 실제로 '능동적 사이버 방어'를 위해서는 우선 공격의 감시를 위한 감청이 요구된다. 그리고 공격을 특정하기 위해서는 통신 기록을 조사할 필요가 있다. 사이버공간에서 정보수집은 통신의 비밀 침해에서 자유로울 수 없다. '능동적 사이버 방어'를 채택하는 국가들은 국내에서의 통신비밀 보호와 구별되는 국경을 넘는 통신에 대한 감시감청을 허용하는 법적 근거를 마련하여 정당화하고 있다. 공격자의 특정은 통신의 발신처를 탐지하는 일이므로, 국경을 넘어 공격원의 네트워크에 역침입하는 것으로 이루어지

31) 「サイバー防御 憲法論議を尽くさねば」, 『東京新聞』 (2023. 9. 22), https://www.tokyo-np.co.jp/article/279002 (검색일: 2024. 4. 30).

게 된다. 미국의 경우 대통령령 12333호, 외국정보감시법에 의해 이것이 국내법적으로 정당화되고 있으며, 영국은 조사권한법, 프랑스는 국내안전법전 등의 법적 기반을 마련하였다. 실력 대응 조치는 탈린매뉴얼2.0의 자위권 행사 차원으로 국제법 차원에 인정되고 있다.[32]

사사카와재단 연구팀은 다음과 같은 법적 논리를 통해서 법적 정합성 추구가 가능할 수 있다고 분석하고 있다. 우선 공격 감시를 위한 국경을 넘는 통신 감청은 공공 복리를 위해 일정한 조건 하에 인정할 수 있다는 논리에 입각해 정당화될 수 있다고 본다.[33] 이 논리는 2014년에 집단적 자위권 행사에 대한 헌법 해석 변경을 실시할 때의 논거이기도 하다. 헌법 21조의 통신비밀 조항이 일반원칙으로 제시되어 있는 가운데, 이보다 상위 가치로 볼 수 있는 헌법 전문 상의 '공공복리'를 내세워 예외적 조치가 가능하다는 논거를 만드는 것이다. 하지만, 일본 사회의 평화주의 정체성은 일본 국가가 외부의 전쟁에 휘말리는 것만 기피한 것이 아니다, 국가의 사회 부분에 대한 제약 가능성에 대해서도 우려하는 입장을 지속해 왔다. 헌법 내에 긴급사태에 대한 규정이 없는 가운데, 유사시 중앙정부의 지방정부를 포함한 여러 공공기관에 대한 수직적 명령체계 구축의 내용이 2000년대에나 들어서 유사법제로 입법화되어 온 역사가 이를 대변해 준다.[34] 통신에 대한 안보적 고려의 감시가 국경 밖으로만 이루어질 것이라는 논거가 일본 사회에서 쉽게 수용되기 어려운 맥락이 존재하고 있다.

나아가 안보적 차원에서 외국의 군용시설에 대한 통신 감청을 평시에 자위대가 수행하는 것조차도 일본 국내법에서 명확하게 역할 부여가 되어 있지

32) 笹川平和財団新領域研究会(2024), pp.140~142.
33) 笹川平和財団新領域研究会(2024), p.144.
34) 전진호, 「유사법제의 제도화와 중앙-지방관계: 유사법제의 일본 국내외적 함의」, 『일본연구논총』 21, 2005, pp.1~24.

않다. 물론 자위대는 국제법 차원에서 군대이므로 국제법적으로 인정되는 외국의 군용시설을 감청하는 것은 문제가 없다. 하지만, 일본 국내적으로 자위대는 군대가 아니므로 통신감청하는 것에 대한 명확한 역할 부여가 되어 있지 않다. 이 가운데 무선통신 감청을 금지하는 전파법 제59조에 따라 자위대의 통신 감청에 대한 역할 부여가 제약될 수 있는 여지가 있다. 사사카와재단 연구팀은 이에 대한 추가적 법적 근거 마련이 필요하다고 분석한다.[35]

한편 사이버공간에서의 대응 조치 시행은 무력공격으로 판단되는 상황에서 자위권 행사로 실시하는 것은 가능하지만, 사이버공간에서 벌어지는 공격에는 무력공격으로 판단되기 어려운 무력공격 이전 사태가 많다. '능동적 사이버 방어'는 이러한 무력공격 이전 사태에 대해서도 적극적으로 대응하는 성격을 지닌다. 하지만, 헌법 9조를 '필요최소한'의 기준을 전제로 하는 전수방위로 해석하는 가운데 정립된 무력공격에 대한 최소한도의 대응이라는 자위대 역할 부여는 '능동적 사이버 방어'를 행사하는데 제약 요인이 된다. 사사카와재단 연구팀은 이에 대한 보다 명쾌한 해석이 필요하다고 분석하고 있다[36] 사사카와재단 연구팀이 기대하는 명쾌한 해석은 무력공격 이전 사태의 위협에 대한 적극적 대응이 자위의 범위에 속한다는 적극적 해석 확대로 가능할 것이다. 이러한 적극적 해석은 최근 반격능력 행사에 대한 논거 마련 과정에서 일본 정부가 취한 방식이다. 하지만, 전수방위 원칙에 대한 엄정한 해석상에서 논리적으로 설득력은 부족할 수밖에 없다. 일본 정부가 여러 차례 보여주었던 지적 곡예를 통한 헌법 9조에 대한 해석 변경이 다시 등장할 상황이다.

지적 곡예를 통한 헌법 해석 변경에는 상당한 정치적 비용이 발생한다.

35) 笹川平和財団新領域研究会(2024), p.145.
36) 笹川平和財団新領域研究会(2024), p.146.

‘능동적 사이버 방어’ 도입의 정책 과정에는 이전의 다른 안보 정책 전환 사례와 마찬가지로 정책 과정에서의 정치적 비용과 정책 목표인 안보 정책 적극화의 필요성 사이에 딜레마가 존재한다.

Ⅳ. ‘능동적 사이버 방어’ 도입의 정책 과정과 성격

1. 2022년 안보3문서와 ‘능동적 사이버 방어’

2022년 12월 일본 정부는 「국가안보전략」, 「국가방위전략」, 「방위력정비계획」을 발표했다. 2022년 안보3문서로 불리는 이 문서들에는 2020년대 일본 안보정책의 거시적 목표와 구체적 방법이 망라되어 있다. 사이버안보 정책에 있어서 「국가안보전략」은 ‘능동적 사이버 방어’ 개념 도입을 다음과 같이 명시하고 있다.

> 무력공격에 이르지는 않지만, 국가, 주요 인프라 등에 대한 안전보장상의 우려를 발생시키는 중대한 사이버공격의 우려가 있는 경우, 이를 미연에 배제하고, 또한 이러한 사이버공격이 발생했을 경우의 피해 확대를 방지하기 위해 능동적 사이버 방어를 도입한다. 이를 위해 사이버 안전보장 분야의 정보수집·분석능력을 강화하는 동시에 능동적 사이버 방어 실시를 위한 체제를 정비하면서, 이하의 (가)부터 (다)까지를 포함한 필요한 조치의 실현을 위해 검토를 추진한다.
>
> (가) 중요 인프라 분야를 포함해 민간사업자 등이 사이버공격을 받았을 경우 정부에 대한 정보공유나 정부로부터 민간사업자 등에 대한 대처 조정, 지원 등의 대처를 강화하는 등 대응을 추진한다.
> (나) 국내 통신사업자가 역무 제공하는 통신과 관련된 정보를 활용해 공격자에 의한 악용이 의심되는 서버 등을 검지하는 데 필요한 대응을 추진한다.

(다) 국가, 중요 인프라 등에 대한 안전보장상의 우려를 발생시키는 중대한 사이버공격에 대해 가능한 한 미연에 공격자의 서버 등의 침입·무해화가 가능하도록 정부에 대해 필요한 권한이 부여되도록 한다.
능동적 사이버 방어를 포함한 이러한 대응을 실현·촉진하기 위해 내각 사이버보안센터(NISC)를 발전적으로 개편하고, 사이버 안전보장 분야의 정책을 일원적으로 종합 조정하는 새로운 조직을 설치한다. 그리고, 이러한 사이버 안전보장 분야에 있어서의 새로운 대응의 실현을 위해서 법제도의 정비, 운용의 강화를 도모한다. 이러한 대응이 종합적인 방위체제 강화에 기여할 수 있도록 한다. 또한 경제안전보장, 안전보장 관련 기술력 향상 등 사이버 안전보장 강화에 기여하는 다른 정책과의 연계를 강화한다.[37]

앞서 기술하였듯이, 2018년 「방위계획대강」에도 '미연에 방지하기 위해'라는 문구가 포함되어 있어서, 사이버안보에 대한 적극적 방어 자세가 이미 발견된다. 하지만, 2022년 「국가안보전략」에는 공격의 감시와 공격자의 특정, 그리고 그에 대한 자위권 차원의 실력 대응 조치가 모두 명시적으로 포함된 국제적 표준 성격에 부합하는 '능동적 사이버 방어'가 사이버안보 정책의 향후 방향성으로 명확하게 기술되어 있다. 한편 「국가방위전략」에는 자위대의 역할에 '자위대 이외의 사이버시큐리티를 지원하는 태세를 강화한다'는 문구가 포함되었다. 이는 자위대가 기존에 실시하던 자위대와 방산업체의 네트워크에 대한 보안 대응을 넘어, 국가 전체 사이버공간 방어에 대해서 과거와는 다른 역할을 맡게 될 것이라는 점을 드러내고 있다. 이에 근거해 「방위력정비계획」에서는 2027년도까지 자위대 사이버방위대 등의 사이버 관련 부대를 약 4,000명 규모로 확대하고, 사이버 요원을 약 2만 명 체제로 강화함과 더불어 위협추적 능력을 향상해 민간의 중요 인프라 사업자와 방산업체 등과

37) 주7)과 같음.

제휴를 강화한다는 계획을 공식화했다.[38]

'능동적 사이버 방어'의 도입에 대한 명시적 방향성 제시는 앞서 언급한 일본 국내의 법적 근거 마련을 위한 정부의 법제도 정비 노력과 사이버안보 정책의 거버넌스 재구축 모색으로 연결된다. 이를 위한 〈사이버안전보장체제정비준비실〉은 안보3문서 발행 한 달 후인 2023년 1월에 설립되었다.

2. '능동적 사이버 방어' 도입의 지체 요인

일본 정부는 '능동적 사이버 방어'에 대한 법적 기반 정비를 2024년 상반기에 마무리하려는 계획을 세우고 있었다. 2022년 안보3문서의 중요 과제 중 반격능력 보유와 무인기 활용은 2023년에 바로 연구개발과 부대 배치 등의 실행 단계로 진입하였으나, 2022년 안보3문서 제정 당시에 '능동적 사이버 방어' 개념 도입은 방위장비이전3원칙 운용지침의 개정과 함께 2023년 이후에 신속하게 체제를 정비해야 하는 과제로 설정되어 있었다.[39] 안보3문서 제정 과정에서 '능동적 사이버 방어' 개념 도입과 방위장비이전3원칙 변경에 대해서는 세부적인 부분까지 정부여당 내에 논의가 진전되지 않은 상태였다.[40]

'능동적 사이버 방어' 개념 도입은 다른 정책 사안의 결정과 마찬가지로 관료집단에 의한 법적 기반 논의 마련, 전문가 검토, 연립여당 내 정책 조정을 거쳐 정부 방침으로 결정되는 흐름으로 진행되고 있다. 2023년 1월에

38) 笹川平和財団新領域研究会(2024), pp.194~195.
39) 「能動的サイバー防御急務 通常国会、法案提出見送り」, 『日本経済新聞』(2024. 1. 25), https://www.nikkei.com/article/DGKKZO77937630V20C24A1PD0000/ (검색일: 2024. 4. 30).
40) 「武器輸出、サイバー防衛は先送り国家安保戦略、自公の温度差が浮き彫り」, 『毎日新聞』(2022. 12. 16), https://mainichi.jp/articles/20221216/k00/00m/010/309000c (검색일: 2024. 4. 30).

설립된 〈사이버안전보장체제정비준비실〉은 '능동적 사이버 방어' 개념 도입의 구체 내용을 준비하는 업무를 맡아 출범하였다. 각 성청에서 파견된 45명 정도의 관료집단으로 구성된 〈사이버안전보장체제정비준비실〉은 '능동적 사이버 방어'의 논거 마련의 실질적인 내용 설계 역할을 맡고 있다.[41] 관료집단에 의한 논거 마련의 체제 구축은 안보3문서 발행 이후 매우 빠르게 진전되었다. 사이버안보 정책 전환에 대한 전문가 검토를 위한 유식자회의를 2023년 여름에 구성하고,[42] 이를 2023년 하반기에 연립 여당 내의 의견을 조정해서 2024년 상반기 정기국회에서 법정비를 마무리하는 일정 목표가 있었다. 하지만, '능동적 사이버 방어' 개념 도입에 대한 유식자회의는 당초 계획보다 1년이 지난 2024년 6월에 들어서야 활동하기 시작했다. 2024년 1월에 일본 정부는 '능동적 사이버 방어' 관련 법안을 국회에서 제출하는 것을 보류하였다.[43]

'능동적 사이버 방어'의 법정비가 미뤄지는 핵심 이유는 연립 정권 내의 조정 문제에 있다. 자민당 연립 파트너인 공명당은 안보3문서 내용 논의 단계에서부터, '능동적 사이버 방어' 도입에 대해서는 원론적으로 찬성하지만, 통신 비밀에 대한 헌법 21조와의 충돌 가능성에 대해 자민당과는 상이한 수준의 우려 인식을 지니고 있었다.[44] 공명당은 안보3문서에서 향후 해석 관련 과제로 남겨진 방위장비이전원칙 운용지침 개정에 대해서도 자민당과 견해 차가 있었다.

---

41) 주8)과 같음.

42) 「能動的サイバー防御､法整備へ有識者会議設置 夏以降に」､『日本経済新聞』(2023. 6. 24), https://www.nikkei.com/article/DGXZQOUA242HE0U3A620C2000000/ (검색일: 2024. 4. 30).

43) 주39)과 같음.

44) 「自公が安保実務者協議､サイバー防衛強化で一致 各論は持ち越し」, Reuters (2022. 11. 9), https://jp.reuters.com/article/idUSKBN2RZ0WK/ (검색일: 2024. 4. 30).

기시다 후미오(岸田文雄) 정권은 방위장비이전원칙 운용지침 개정을 통해 공동개발 차기전투기 제3국 수출 용인과 '능동적 사이버 방어'의 법정비를 단계적으로 진행하는 일정 목표를 가지고 있었다. 두 사안을 동시 병행 처리할 때 사회적 반발이 커질 가능성이 있고, 이는 공명당과의 내용 조정에 장애요인이 되기 때문이다. 2022년 안보3문서 발행 당시 기시다 정권은 방위장비이전원칙 운용지침 개정 논의를 2023년 상반기에 정리하고, 2023년 하반기에는 '능동적 사이버 방어' 관련 법정비의 여당 내 논의를 진행하고자 했다. 하지만, 2023년 4월 통일지방선거의 정치적 조건 속에서 공명당은 방위장비이전원칙 운용지침 개정 논의를 미루고자 하였다. 2023년 하반기에는 내각개조와 자민당 내 정치자금 스캔들의 여파 속에서, 방위장비이전원칙 운용지침 개정에 대한 공명당과의 합의가 쉽사리 이루어지지 않았다. 방위장비이전원칙 운용지침 개정을 통한 공동개발 전투기의 제3국 수출을 허용하는 각의 결정은 당초 계획보다 1년 늦어진 2024년 3월 26일에 이루어졌다.[45]

2023년에 공명당은 안보3문서의 향후 과제에 대한 자민당의 신속한 법과 규범 정비 의도에 대한 비토파워로서의 역할을 수행했다. 게이오대학의 진보 겐(神保謙) 교수가 말하듯 2023년 방위장비이전원칙 운용지침 개정과 '능동적 사이버 방어' 도입 논의에 있어서 공명당은 한동안 방기한 것 같았던 당의 근본적 정체성인 평화 노선을 재강조하는 모습을 보이고 있다.[46] 자민당의 적극적 안보 정책으로의 정책 전환에 대한 정체성 차원의 반감과 더불어 지속적으로 하락하는 기시다 정권에 대한 지지율은 공명당으로 하여금

45) 「政府 日英伊で共同開発の次期戦闘機 第三国への輸出容認を決定」, NHK (2024. 3. 26), https://www3.nhk.or.jp/news/html/20240326/k10014402481000.html (검색일: 2024. 4. 30).

46) 「いまの岸田政権に「セキュリティ・クリアランス制度」と「能動的サイバー防御」についての法案を通すことは難しい 通常国会1月26日召集へ」, NEWS ONLINE (2023. 12. 27), https://news.1242.com/article/486839 (검색일: 2024. 4. 30).

자민당과의 적극적 정책 공조 자세를 유보하게 만들었다. 물론 공명당의 평화 노선 정체성은 안보3문서의 기본 취지와 대립되는 수준의 정책 태도로 진전될 것으로 전망되진 않는다. 1999년 이래로 유지되고 있는 자공 연립 체제 속에서 공명당은 자민당과의 정책 조정에서 자민당으로부터 생활밀착형 정책에 대한 양보를 얻어내는 것에 중점을 두어 정책 조정해 임해왔다. 안보 정책 분야에서 공명당은 자민당이 추진하는 정책 내용을 결국 동의하는 양상을 지속해서 보여왔다. 다만, 자민당 정권의 정치적 지지도에 따라서 자민당의 적극화되는 안보 정책에 동의하는 속도에 있어서 편차가 발견된다.

3. 국제표준 수용으로서의 '능동적 사이버 방어' 도입

2022년 안보3문서에 명시된 '능동적 사이버 방어' 법정비 과정이 기대보다 지체되고 있지만, 일본의 '능동적 사이버 방어' 도입은 이미 결정된 미래에 가깝다. 현재 '능동적 사이버 방어' 도입과 관련된 논의는 '능동적 사이버 방어' 도입 자체가 아니라 '능동적 사이버 방어'와 헌법 및 기존 법률과의 논리적 정합성을 만드는 것에 초점이 모아져 있다.

정책공간에서 '능동적 사이버 방어' 자체는 국제표준으로서 일본도 채택하지 않으면 안 되는 것으로 전제된 경향이 강하다. 일본 안보 정책의 적극화에 대한 일본 정부의 논리는 국가가 가지는 보편적 권리를 일본도 채택해야 한다는 국제주의에 가깝다. 헌법 9조에 대한 제한적 해석에 입각해 있던 과거의 안보 규범을 일국 특수주의로 비판하면서, '적극적 평화주의'는 국제질서 유지를 위한 보편적 안보 역할을 수행하는 국가가 되어야 한다는 논리 체계를 구축하였다.[47] '적극적 평화주의'의 국제주의는 국제질서 유지에 대한

47) 황세희, 「일본외교와 적극적 평화주의-요시다 노선의 대안으로서의 평가」, 『한일군사문화연구』 23, 2017, pp.37~62.

적극적 관여라는 점과 더불어 다른 국가들과 동일한 역할을 수행하는 일본이라는 점의 두 가지 성격을 모두 지닌다. 국제질서 유지에 대한 관여는 요시다 노선 이래로 일본 외교안보 정책 태도에서 변화하지 않았다. '적극적 평화주의'의 국제주의가 가지는 기존 안보 규범과의 가장 선명한 차별성은 다른 국가와 동일한 역할 인식을 보여주고 있다는 점에 있다.

'능동적 사이버 방어' 도입은 집단적 자위권에 대한 해석 변경이나 반격 능력 보유 결정과 마찬가지로 이러한 안보 규범 확립 없이는 증가하는 위협에 대응하기 어렵다는 현실론과 더불어, 다른 국가들도 모두 보편적으로 수행하고 있다는 보편주의적 국가 역할론에 입각해 있다. 일본의 보통국가화는 위협에 대한 현실주의적 대응과 보편적 국가 역할이라는 두 가지 성격을 지니고 있으며, 전자의 논거를 국민의 생활안전과 연결시키고 후자의 논거를 국제사회에서 국가의 위상과 연결시키고 있다.

현실적으로 '능동적 사이버 방어'는 전 세계 모든 나라들이 추구하고 있는 국제표준적 사이버안보 정책 개념이 되었다. 따라서, 보편적 국가 역할 인식 차원에서 일본이 '능동적 사이버 방어' 도입의 논거를 구성하는 것은 특별하다고 보긴 어렵다. 다만 미국 주도의 국제표준이 아니라면, 일본이 이것을 국가가 보편적으로 채택해야만 하는 역할이라고 적극적으로 수용하기는 어려웠을 것이다. '능동적 사이버 안보'의 미국 주도적 성격은 일본이 이를 보편적 국가 역할로 받아들이는 과정에서 핵심적이다. 앞서 살펴보았듯이 신흥 안보 영역인 사이버공간에 대한 안보 규범에 전통적 전쟁법과 전쟁인도법 등의 국제법을 어떻게 적용시키는지에 대한 규범 갈등이 존재하였으나, 결국 미국 주도의 안보 규범이 국제표준으로 확립되고 있다. 새롭게 변용되고 창출되는 안보 규범에서 규범 주도국이 누구인지에 따라 규범 수용의 양상은 달라질 수밖에 없다.

일본의 '능동적 사이버 방어'가 미국 주도의 국제표준 수용이라는 성격을 지니고 있다는 점은, 사이버 분야에서의 미일협력이 가지는 의미가 복합적임을 암시한다. 사이버 분야에서의 미일협력은 일본에게 실제 현실적 사이버 위협에 대한 효과적 대응 모색의 방법일 뿐만 아니라 사이버안보에 대한 새로운 규범 수용 과정에서 중요한 디딤돌의 성격도 지니고 있다. 2013년 시작된 〈미일사이버방위정책워킹그룹(CDPWG: Cyber Defense Policy Working Group)〉은 사이버공간에서 미일 안보 협력의 실무적 공간으로 작동해 왔고, 이러한 협의 공간을 통해 미국이 채택한 새로운 안보 규범인 '능동적 사이버 방어'는 일본이 수용해야 할 국제규범으로 자리 잡게 되었다. 2019년 미일 2+2 회의에서 양국은 사이버공간에서 국제법이 적용된다는 점을 명시하였다. 사이버공간에서 '능동적 사이버 방어'를 사이버안보 정책의 기조로 확립한 미국에게 '능동적 사이버 방어'는 국제법에 이미 부합하는 규범으로 인식되고 있었다. 미일협력은 일본의 안보 정책 진화에서 증가하는 안보 위협에 대한 가장 효과적 방법론으로서의 중요성을 지니고 있다. 나아가 미일협력은 일본의 국제표준 수용으로서의 안보 정책 진화라는 논리 체계 구축에서도 가장 중요한 메커니즘으로 역할하고 있다.

하지만 국제표준 수용 속에서 과거의 특수주의적 헌법 해석에 입각한 국가의 제한적 역할 인식의 논리는 폐기되지 않고 있다. 이미 반격능력 보유가 전수방위 원칙과 모순되지 않는지에 대한 질문에 대해서 일본 정부는 반격능력은 전수방위 원칙의 위배가 아니며 전수방위 원칙은 앞으로도 유지한다는 입장을 명확하게 밝혔다. 다만 전수방위 개념 자체가 변했다. 과거 전수방위에 대해서는 상대방의 영토에 있는 기지를 공격하지 않는다는 기존의 정부 해석(1970년 나카소네 야스히로(中曽根康弘) 방위청 대신의 답변, 1972년 다나카 가쿠에이(田中角栄) 총리의 답변)이 있었다. 2023년 1월 기시다 총리는

과거의 전수방위 해석은 “무력행사를 목적으로 무장한 부대를 다른 나라에 파견하는 ‘해외파병’은 일반적으로 헌법상 허용되지 않는다는 것을 말한 것”이라고 설명하면서, 기지 공격을 위해 자위대를 해외에 파병하는 경우 전수방위에서 벗어나지만, 상대방의 공격을 막기 위해 장사정거리 미사일을 사용하는 것은 전수방위 내라고 답변하였다.[48)]

반격능력 보유와 전수방위 원칙의 관계에 대한 기시다 총리의 답변에서 등장한 논리는 ‘능동적 사이버 방어’와 전수방위 원칙 사이의 정합성을 주장하는 논거로 동일하게 사용될 수 있다. 문제는 사이버공간에서의 무력행위에 대한 효과적 억지 방법이 거부적 억지가 아니라 징벌적 억지이며 ‘능동적 사이버 방어’는 적극적인 징벌적 억지 추구라는 성격을 지닌다는 점이다. 이러한 징벌적 억지 추구가 전수방위 원칙과 부합한다는 주장은 전수방위 원칙 자체의 유명무실화를 가져오고 있음이 분명하다. 2024년 4월 10일 자민당 〈사이버시큐리티에 관한 프로젝트팀(PT)〉은 회의를 열고 ‘능동적 사이버 방어’의 신속한 법정리를 정부에 요청하는 제안서를 채택하였다. 이 회의에서 아마리 아키라(甘利明) 전 간사장은 ‘전수방위의 주술에 걸려, 앞으로 나아가지 못하면 안 된다’고 발언하였다.[49)] 아마리 의원의 발언은 전수방위 원칙에 대한 자민당 보수 정치인들의 솔직한 속내라 할 수 있다. ‘능동적 사이버 방어’의 도입은 일본만의 현상이 아니다. 다만, 이를 기존 국내 법질서와 관계 설정하는 과정에 대한 일본의 태도는 명료한 해석의 정합성을 추구하지 않는다는 점에서 특별하다. 반대로 독일의 경우 ‘능동적 사이버 방어’ 도입과 함께 기본법(헌법) 개정을 통한 법체계 정비 필요성을 독일 〈국가안보전략〉에

48) 「日米安全保障協議委員会共同発表」(2019. 4. 19), https://www.mofa.go.jp/mofaj/files/000470738.pdf (검색일: 2024. 4. 30).

49) 「自民PTが「能動的サイバー防御」の提言原案「常時有事」と指摘」, 『毎日新聞』(2024. 4. 12), https://mainichi.jp/articles/20240410/k00/00m/010/211000c (검색일: 2024. 4. 30).

명시하고 있다.[50] 이와 달리 일본은 안보 정책의 진화에 대한 헌법 해석상의 지적 곡예를 지속하고 있다.

Ⅴ. 결론

일본 정부는 2022년 안보3문서에서 명시된 '능동적 사이버 방어' 개념 도입에 대한 법적 기반 구축 작업을 진행하고 있다. '능동적 사이버 방어' 개념은 헌법 21조의 통신 비밀 규정과 헌법 9조에 대한 전수방위 원칙과 논리적으로 충돌하기 때문에, 이에 대한 논리 체계 구축 작업이 요구되는 상황이다. 기대보다 일본의 '능동적 사이버 방어' 도입이 지체되고 있는 것은 '능동적 사이버 방어'에 대한 연립 여당 내의 정책 조율 과정에 시간이 많이 소요되고 있기 때문이다. 하지만, 사이버공간에서 잠재적 공격을 감시하고, 공격자를 특정하고, 이에 대한 실력 대항조치를 전방 방위로 추진하는 '능동적 사이버 방어' 개념의 도입 자체는 이미 결정된 미래다. '능동적 사이버 방어'는 미국 주도의 국제표준으로서 수용되고 있다. 일본의 보통국가화는 외부 위협에 대한 적극 대응이 필요하다는 논리와 더불어 일본의 국가 역할이 다른 국가들과 동일해야 한다는 보편주의적 국제주의 논리에 입각해 전개되고 있다. 미국 주도로 새로운 국제규범이 되고 있는 '능동적 사이버 방어'의 도입은 국제표준 수용 차원에서 당연한 것으로 일본 정책관여자들에게 인식되는 사항이다.

국제표준 수용으로서의 정책 변화에도 불구하고, 일본은 국제표준에 맞춘 헌법 해석 변경을 전면적으로 추진하지 않고 있다. '능동적 사이버 방어' 개념은 반격능력 보유와 마찬가지로 일본의 전수방위 원칙과 충돌하는 성격

50) 笹川平和財団新領域研究会(2024), pp.221~222.

을 지니고 있다. 일본 정부는 반격능력 보유와 전수방위 원칙의 충돌 가능성에 대해서 전수방위 원칙에 대한 설명을 변화시켰다. '능동적 사이버 방어' 개념 도입에 대해서도 동일한 지적 곡예가 이루어질 가능성이 크다. 전수방위가 일반원칙으로만 존재해 온 가운데, 전수방위 원칙의 구체적 내용에 대한 상황에 따른 설명 변화는 계속될 가능성이 크다. '능동적 사이버 방어' 수용은 글로벌 보편 현상인 가운데, 새로운 국제표준이 된 '능동적 사이버 방어'와 정합성을 지니는 차원의 적극적 국내 법제도 변경을 회피하는 것은 일본의 특수적 현상이다. 日本空間

논문 투고일 : 2024년 5월 20일
논문 심사일 : 2024년 5월 26일
게재 확정일 : 2024년 5월 30일

참고문헌

「국가안보실, 윤석열 정부의 '국가사이버안보전략' 수립」, https://www.president.go.kr/newsroom/press/gdXzwtKB (검색일: 2024. 4. 30).

박성호, 「일본의 사이버 안보전략 – 양자주의의 강화인가 다자주의로의 전환인가?–」, 『일본학』 56, 2022.

신승휴, 「사이버 안보이슈에 대한 일본의 대응과 아베 정권의 국제적 역할인식: 역할이론과 존재론적 안보의 시각」, 『아세아연구』 63.3, 2023.

이상현, 「일본의 사이버안보 수행체계와 전략」, 『국가안보와 전략』 19.1, 2019a.

_____, 「사이버 위협에 대한 일본의 대응: 사이버 외교와 사이버 방위」, 『국가전략』 25.2, 2019b.

이승주, 「일본 사이버안보 전략의 변화: 사이버 안보의 전통 안보화와 전통 안보의 사이버 안보화」, 『국가안보와 전략』 17.1, 2017.

전진호, 「유사법제의 제도화와 중앙–지방관계: 유사법제의 일본 국내외적 함의」, 『일본연구논총』 21, 2005.

황세희, 「일본외교와 적극적 평화주의–요시다 노선의 대안으로서의 평가」, 『한일군사문화연구』 23, 2017.

Alex Wilner, "US Cyber Deterrence: Practice Guiding Theory," *Journal of Strategic Studies* 43.2, 2020.

IISS, "Cyber Capabilities and National Power: A Net Assessment," https://www.iiss.org/research–paper/2021/06/cyber–capabilities–national–power/ (검색일: 2024. 4. 30).

International Telecommunication Union, *Global Cybersecurity Index 2020* (Internaitonal Telecommunication Union. 2021).

Sven Herpig, "Active Cyber Defense – Toward Operational Norms," https://www.stiftung-nv.de/sites/default/files/snv_active_cyber_defense_toward_operational_norms.pdf (검색일: 2024. 4. 30).

Takashisa Kawaguchi, "Two Approaches to Responding to Destructive Cyberattacks on Critical Infrastructure in Japan: Addressing Cyber Crises as "Service Failures" or "Armed Attacks," in Yasuhiro Takeda, Jun Ito, and Yusuke Kawashima (eds.), *Civil Defense in Japan* (Routledge, 2023).

「能動的にサイバー防御 めざせ攻めの法整備【日経モープラFT】」, https://txbiz.tv-tokyo.co.jp/plusft/feature/post_281495 (검색일: 2024. 4. 30).

「「能動的サイバー防御」準備室、内閣官房に新設 政府」, 『日本経済新聞』(2023. 1. 31), https://www.nikkei.com/article/DGXZQOUA3186D0R30C23A1000000/ (검색일: 2024. 4. 30).

「いまの岸田政権に「セキュリティ・クリアランス制度」と「能動的サイバー防御」についての法案を通すことは難しい 通常国会1月26日召集へ」, NEWS ONLINE (2023, 12. 27), https://news.1242.com/article/486839 (검색일: 2024. 4. 30).

「サイバーセキュリティ戦略 (2015년)」, https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku.pdf (검색일: 2024. 4. 30).

「サイバーセキュリティ戦略 (2018년)」, https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2018.pdf (검색일: 2024. 4. 30).
「サイバーディフェンス連携協議会(ＣＤＣ)の設置·取組について」, https://www.mod.go.jp/j/////approach/defense/cyber/pdf/cyber_defense_council.pdf (검색일: 2024. 4. 30).
「サイバー防御 憲法論議を尽くさねば」,『東京新聞』(2023. 9. 22), https://www.tokyo-np.co.jp/article/279002 (검색일: 2024. 4. 30).
「国家安全保障戦略」, https://www.mod.go.jp/j/policy/agenda/guideline/pdf/security_strategy.pdf (검색일: 2024. 4. 30).
「内閣サイバーセキュリティセンター(NISC)について」, https://www.nisc.go.jp/about/history/index.html (검색일: 2024. 4. 30).
「能動的サイバー防御､法整備へ有識者会議設置 夏以降に」,『日本経済新聞』(2023. 6. 24), https://www.nikkei.com/article/DGXZQOUA242HE0U3A620C2000000/ (검색일: 2024. 4. 30).
「能動的サイバー防御急務 通常国会､法案提出見送り」,『日本経済新聞』(2024. 1. 25), https://www.nikkei.com/article/DGKKZO77937630V20C24A1PD0000/ (검색일: 2024. 4. 30).
「武器輸出､サイバー防衛は先送り国家安保戦略､自公の温度差が浮き彫り」,『毎日新聞』(2022. 12. 16), https://mainichi.jp/articles/20221216/k00/00m/010/309000c (검색일: 2024. 4. 30).
「日米安全保障協議委員会共同発表」(2019. 4. 19), https://www.mofa.go.jp/mofaj/files/000470738.pdf (검색일: 2024. 4. 30).
「自公が安保実務者協議､サイバー防衛強化で一致 各論は持ち越し」,

Reuters (2022. 11. 9), https://jp.reuters.com/article/idUSKBN2RZ0WK/ (검색일: 2024. 4. 30).

「自民PTが「能動的サイバー防御」の提言原案「常時有事」と指摘」,『毎日新聞』(2024. 4. 12), https://mainichi.jp/articles/20240410/k00/00m/010/211000c (검색일: 2024. 4. 30).

「政府 日英伊で共同開発の次期戦闘機 第三国への輸出容認を決定」, NHK (2024. 3. 26), https://www3.nhk.or.jp/news/html/20240326/k10014402481000.html (검색일: 2024. 4. 30).

「平成 31 年度以降に係る防衛計画の大綱」, https://www.mod.go.jp/j/policy/agenda/guideline/2019/pdf/20181218.pdf (검색일: 2024. 4. 30).

谷脇康彦,『サイバーセキュリティ』, 岩波書店, 2018.

国際文化会館地経学研究所,『経済安全保障とは何か』, 東洋経済新報社, 2024.

笹川平和財団新領域研究会,『新領域安全保障 サイバー·宇宙·無人兵器をめぐる法的課題』, ウェッジ, 2024.

松村昌廣,「我が のサイバーセキュリティ戦略の欠点と展望―「平和国家」体制の桎梏への対応を考える」,『情報通信政策研究』5.2, 2022.

川口貴久,「サイバー空間における『国家中心主義』の台頭」,『国際問題』683, 2019.

土屋大洋,『サイバーセキュリティと国際政治』, 千倉書房, 2015.

Abstract

Japan's Embracing of 'Active Cyber Defense(ACD)' and Non-aggressive Defense Principle

Junghwan Lee

The Japanese government is working on constructing the legal basis for the adoption of the concept of "active cyber defense" as set forth in the 2022 National Security Strategy. The concept of "active cyber defense" logically conflicts with the secrecy of communications provisions in Article 21 and the principle of non-aggressive defense in Article 9 of the Constitution, so it is necessary to establish a logical system between the Constitution and "active cyber defense." The introduction of the concept of "active cyber defense," which involves monitoring potential attacks in cyberspace, identifying the attacker, and promoting forward countermeasures against the attacker's capabilities, is already a foregone conclusion. "Active cyber defense" is accepted as an international standard led by the United States. Japan's normal-state is based on the logic that Japan needs to actively respond to external threats and the logic of universalist internationalism that Japan's role should be the same as other countries. The introduction of "active cyber defense," which is becoming a new international norm led by the United States, is perceived by Japanese policymakers as a matter of course in terms of acceptance of international standards. Despite this policy change, Japan has not made any sweeping changes to its constitutional interpretation. While the acceptance of 'active cyber defense' is a global phenomenon, Japan's avoidance of changing

the existing domestic legal framework to comply with the new international standard of 'active cyber defense' is a peculiar phenomenon.

Keywords

Japan's Cybersecurity Policy, Active Cyber Defense (ACD), Non-aggressive Defense, National Security Strategy of Japan