사이버안보연구, 1집 2호 2024 가을, 237-270

일본 방위성의 사이버안보 정책과 미일협력

0102-237270

조은일 | 한국국방연구원

논문접수일 2024년 8월 30일 | 논문심사일 2024년 9월 25일 | 게재확정일 2024년 10월 17일

논문 요약

최근 일본의 안보전략에서 사이버안보가 중요하게 다뤄지고 있다. 일본 정부는 2022년 12월 국가안보전략서를 발표하고 사이버 안보의 중요성을 언급했다. 이를 위해 '능동적 사이버 방어(active cyber defense, ACD)'라는 개념을 도입하고 '중대한 사이버 공격을 미연에 배제하며 피해 확대를 방지'하기 위한 사이버안보를 강화할 것으로 보인다. 이를 위해 일본 방위성은 전시 뿐만 아니라 평시에도 사이버 공간을 감시할 수 있도록 방위정책을 재정비할 전망이다. 첫째, 육해공 자위대 합동의 사이버 방위부대 창설과 같은 부대구조의 재편이다. 둘째, 군 및 민간 인력을 충분히 활용하는 인력 양성이다. 이러한 두 가지 노력을 통해 사이버 공격 가능성을 사전에 무력화할 수 있는 방위력을 갖춘 보다 적극적인 형태의 사이버안보 정책이 추진될 수 있다. 그리고 일본은 사이버 분야에서 미국과의 안보협력을 심화시키면서 능동적 사이버 방어를 완성해 갈 것이다. 이를 위해 일본 국회는 능동적 사이버 방어 도입을 위한 입법 조치를 추진할 것인데 통신의 자유와 같은 헌법을 포함한 논의가 전개될 수 있다. 향후 방위성은 국회 논의 및 정부 입장을 반영한 사이버안보 전략을 구체화할 것으로 보인다.

주제어 일본, 사이버안보, 능동적 사이버 방어, 자위대 개편, 미일 협력

Ⅰ. 서론

최근 일본의 안보전략에서 중요하게 다뤄지고 있는 분야가 사이버 안보(サイバーセキュリティ)이다.[1] 일본 기시다(岸田) 정부는 2022년 12월 「국가안보전략서(国家安全保障戦略)」를 발표하고 국가의 안보전략에 한 부분으로 사이버안보 전략을 추진하겠다고 명확하게 밝혔다(内閣官房 2022). 일본에 대한 사이버 공격이 증가하고 있고, 이에 대한 일본 국내산업의 취약성이 커지고 있다는 점에서 사이버 공간의 안전을 지키는 것이 중요한 과제가 된 것은 새롭지 않다. 사이버 공격이 개인에 대한 해킹이나 산업 스파이, 허위정보 유포 등에 그치는 게 아닌 국가 기반시설에 대한 공격으로 이어지는 사례가 국내외에서 발생하면서 그 피해를 예방하기 위한 국가적 수준의 대응능력이 필요하다는 문제 의식이 작용했다.[2] 전력, 정보통신, 철도, 항만 등 국가 운영에 필수적인 기반시설에 사이버 공격이 발생하면 그 피해는 국가·사회적 혼란을 야기할 정도로 심각한 안보 위협이 되기 때문이다. 이러한 배경에서 기시다 정부는 사이버 공간을 안전하면서 안정되게 이용할 수 있는 공간으로 유지하겠다는 목표로 제시하고 이를 실현하기 위한 수단으로 '능동적 사이버 방어(能動的サイバー防御)'를 도입

1) 일본어로 사이버안보(cybersecurity)는 '사이버 안전보장(サイバー安全保障)' 혹은 '사이버 세큐리티(サイバーセキュリティ)'로 표현하는데 정부 발간물 등에서 전자보다는 후자가 빈번하게 사용되고 있다.

2) 일본 싱크탱크 사사카와 평화재단(笹川平和財団)은 2018년 10월 사이버 공격에 대응하는 법체계 정비 및 인력·산업 육성을 위한 정책제언서 「일본에 사이버안보청 창설을(日本にサイバーセキュリティ庁の創設を!)」을 발간하는 등 정책서클에서 일본의 사이버안보 정책이 불충분하다는 논의를 제시해왔다.

한다고 언급했다. 능동적 사이버 방어의 도입으로 중대한 사이버 공격을 사전에 배제하고, 피해가 확대되는 것을 방지할 수 있다고 덧붙였다.

이와 같은 기시다 정부의 능동적 사이버 방어 도입은 일본 나름의 독자적인 정책은 아니다. 사이버 공간에서 발생하는 심각한 안보 위협에 대응해야 하며 이를 위해서 국가안보 차원의 전략과 정책이 펼쳐질 필요가 있다는 인식은 주요 각국 정부가 유사하게 공유하고 있다.[3] 이를 위해 정부 부처 간 시스템을 정비하고 민간과 협력하는 등 포괄적인 대응을 요구한다는 방법론에서도 크게 차이를 보이고 있지 않다. 그렇다면 주요 각국의 사이버안보 정책과의 유사한 문제의식에서 출발한 일본의 사이버안보 정책이 왜 주목을 받아야 하는가?

첫째, 일본이 가지는 헌법적 제약을 반영한 사이버안보 정책의 발전이다. 일본은 교전권을 포기하고 방어를 위한 군사력만 보유할 수 있는 헌법적 제약을 가지고 있다. 그러한 헌법적 제약 아래 일본 자위대는 군사활동을 펼칠 수 있다. 이러한 헌법적 제약과 자위대의 활동 한계는 일본의 사이버안보 정책에도 그대로 적용된다. 2023년 일본 주요 물류항만 중 하나인 나고야항의 컨테이너 관리 시스템이 랜섬웨어에 의해 공격을 받고 이틀 간 물류체계가 마비되었다. 이 사건은 일본 국내 주요 기반시설에 대한 첫 사이버 공격이었다. 2024년 6월 일본 대형출판사 가도카와(KADOKAWA)와 그 자회사 도완고(ドワンゴ)

3) 예를 들어 미국은 2010년 「국가안보전략서(2010 National Security Strategy)」를 발간하고, 2011년 「사이버공간에서의 국방부 작전 전략(DoD Strategy for Operating in Cyberspace)」을 수립했다. 그리고 2015년 처음으로 미 국방부는 「국방 사이버전략서(DoD Cyber Strategy)」를 발간했다.

가 랜섬웨어에 의한 사이버 공격을 받아 다량의 개인정보 유출과 물류 시스템에 문제가 생기는 사건이 발생했다. 이 사건으로 가도카와의 주가는 일시적으로 20% 이상 하락하기도 했다.[4] 이렇게 사이버 공격이 물리적 공간에서의 피해로 이어지고 있는 사례가 발생하지만 일본은 헌법적 제약 아래 공세적 사이버 작전은 불가능하다. 이에 일본의 사이버안보는 국가 기반시설에 대한 '방어'에 초점을 두고 방어의 범위와 수준을 넓히는 방향으로 발전하고 있다(松本昌廣 2022; 森秀勲 2023).

둘째, 사이버 공간의 군사화를 반영한 일본 방위성의 대응이다. 일본은 연결성과 개방성이라는 사이버 공간의 본질을 고려하면 사이버 공간이 개별 국가의 주권이 미치는 공간으로 접근해서는 안된다는 입장이며, 사이버 공간에서 국가의 통제를 강조하는 중국, 러시아와는 대립적인 인식을 가지고 있다(Goldsmith and Wu, 2006). 사이버 영역은 더는 민간 활동을 위한 공간으로만 존재하지 않기 때문에 이를 규제하고 조정할 국제규범이 모색되어야 한다는 주장도 존재한다(土屋大洋, 2013). 사이버 공간에 대한 국가의 통제와는 별개로 사이버 공간은 새로운 군사활동의 영역이 되고 있으며, 이에 대한 자위대의 새로운 임무를 부여해야 할 수 있다. 예를 들어 방위성은 2024년 7월 발간한 「방위백서(防衛白書)」에서 '사이버 영역은 국민 생활에 있어 필수적인 사회기반시설이며 일본 방위에 있어서 영역횡단작전(領域横

4) 일본의 보안 소프트웨어 기업인 트렌드 마이크로(Trend Micro)가 2024년 2월 발간한 「2023년 연간 사이버안보 보고서」에 따르면 2021년 이후 전세계적으로 사이버 공격이 급증하고 있으며, 일본에 대한 랜섬웨어 공격도 2021년 34건, 2022년 58건, 2023년 63건 등 매년 상승하고 있다.

斷作戰) 수행을 위해 사활적으로 중요하다'고 지적했다(防衛省, 2024: 298). 이러한 사이버 영역의 군사적 중요성은 자위대가 유사시 사이버 공격에 대응하는 것 이외에도 평시부터 사이버 위협을 해소하는 활동을 수행할 필요성도 높아진다. 사회기반시설에 대한 평시 대응은 경찰이나 해상보안청이 주로 담당했는데 자위대가 그 역할을 확대할 수 있으며, 이를 위한 인력양성 및 부대개편이 중요해진다. 또한, 영역횡단작전은 미군의 다영역작전(MDO, multi-domain operation)과 같이 육·해·공 영역에 새롭게 우주·사이버·전자기 영역을 연계해서 통합적인 작전능력을 향상시키는 것인데 사이버 공간에서의 자위대 활동이 그만큼 강조되는 것이다.[5] 이렇게 사이버 공간이 일본의 군사안보에 핵심적인 공간으로 확장되고 있으며 이는 자위대의 역할 확대로도 이어진다(Katagiri, 2021; 佐々木勇人 2023).

본 연구는 일본의 사이버안보 정책의 중심 기조를 살펴보고 이를 구현하는 방위성 차원의 제도를 분석하고자 한다. 사이버안보를 구현하는 능력은 사이버 관련 법, 조직, 인적자원 등에 의해 평가되는데 자위대 부대개편과 인력 양성은 일본의 사이버 능력의 척도가 되기 때문이다. 방위성의 사이버안보 정책은 일본 정부가 추진하는 능동적 사이버 방어로의 전환의 일부를 구성하겠지만, 사이버안보 전략의 전반적인 윤곽을 파악하는데 기여할 수 있다. 게다가 능동적 사이

5) 일본은 육·해·공 영역에 더해 우주·사이버·전자기 영역을 통합하는 다차원통합방위력(多次元統合防衛力)의 구축을 추진하고 있다. 防衛省. 2018. "平成 31 年度以降に係る防衛計画の大綱について." https://www.mod.go.jp/j/policy/agenda/guideline/2019/pdf/20181218.pdf(검색일: 2024.8.21.)

버 방어는 완성형이 아닌 초기 도입 단계에 와있기 때문에 향후 어떻게 전개될 것인지도 중요한 포인트가 된다. 나아가 일본의 사이버안보 정책은 미국과의 동맹협력에서도 중요한 과제로 발전하고 있다. 따라서 일본이 능동적 사이버 방어를 도입하는 과정에서 미일동맹이 어떠한 역할을 하는지도 살펴볼 필요가 있다.

이러한 연구 목적을 달성하기 위해 일본의 사이버안보와 관련한 일본의 문서를 분석하고자 한다. 일본 정부가 발표한 문서는 현재 진행 중인 일본의 사이버안보 정책을 적실성 있게 살펴볼 수 있는 상세한 정보를 제공하기 때문이다. 그리고 1차 자료에 기반한 기본 정보에 대한 충실한 전달은 일본의 사이버안보 정책에 대한 보다 발전된 연구주제를 탐색하는데 학술적 토대가 될 수 있다.

Ⅱ. 일본 사이버안보 정책의 기본 구조

Ⅱ장은 일본 정부가 2010년 이후 사이버안보 정책을 제도화한 기본 구조를 살펴보고, 능동적 사이버 방어 개념이 도입된 배경을 탐색한다. 일본의 사이버안보 정책은 2010년 이후 입법을 통해 구조화되기 시작했고, 2015년 이후 전략서 발간과 개정을 통해 정책방향을 제시하고 있다. 2014년 11월 일본 아베 정부는 「사이버안보 기본법(サイバーセキュリティ基本法)」을 입법했다.[6] 입법의 배경은 사이버안보에 관

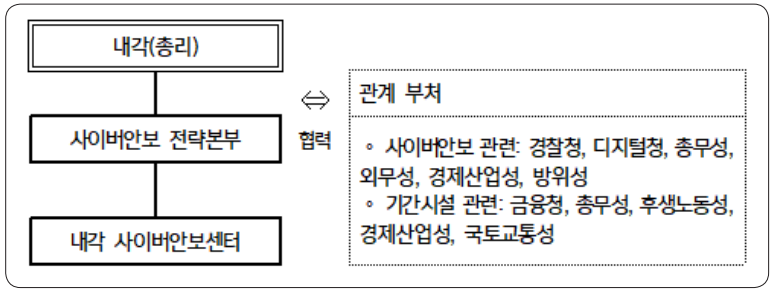
6) 전문은 다음을 참조한다. e-GOV 法令検索. 2024. “サイバーセキュリティ基本法.” https://laws.e-gov.go.jp/law/426AC1000000104(검색일: 2024.8.30.)

한 정책을 종합적이며 효율적으로 추진한다는데 두었고, 기본법을 통해 사이버안보의 기본원칙을 정하고 국가의 책무를 명확하게 하면서 사이버안보 전략 수립과 관련 사항을 규정하는 내용으로 구성했다.

1. 사이버안보 전략서 발간 및 개정

일본 정부는 기본법에 기반해 조직을 정비했는데, 2015년 1월 내각에 사이버안보 전략본부(サイバーセキュリティ戦略本部) 설치가 그 시작이었다. 사이버안보 전략본부는 사이버안보전략서를 작성하고 이에 대한 추진계획을 마련하는 조직으로 기존의 정보안보정책회의(情報セキュリティ政策会議)가 격상된 것이었다. 내각관방에는 사무국의 역할을 하는 사이버안보센터(NISC, National center of Incident readiness and Strategy for Cybersecurity)가 설치되었다. 사이버안보 전략본부와 사이버안보센터는 관계 부처와 협력하는 구조를 가지게 되었다(그림 1 참조).

〈그림 1〉 일본의 사이버안보 조직체계



출처: 内閣サイバーセキュリティセンター(https://www.nisc.go.jp)

이러한 법제 마련과 조직개편을 거쳐 2015년 9월 일본 정부는 범정부 차원의 사이버안보 전략을 담은 「사이버안보 전략서(サイバーセキュリティ戦略)」를 발간했다(内閣サイバーセキュリティセンター, 2015/9/4). 사이버안보 전략서에 따른 일본 정부의 기본 입장은 '자유롭고 공정하며 안전한 사이버 공간(自由、公正かつ安全なサイバー空間)의 확보'에 중점을 두었다. 사이버안보 전략서는 자유롭고 공정하며 안전한 사이버 공간을 창출하고 발전시키기 위해 경제사회의 지속적 발전, 국민 안심사회 실현, 국제평화 및 일본의 안보에 기여한다는 목적을 수행한다고 밝혔다. 그리고 정보의 자유로운 유통 확보, 법의 지배, 개방성, 자율성, 다양한 행위자의 연계 등 다섯 가지 기본원칙을 수립했다. 이러한 입장은 국제적 맥락에서 자유롭고 공정한 사이버 공간을 확보하는 한편, 국내적 맥락에서 시민과 기업을 보호할 수 있는 안전한 사이버 공간을 구축한다는 의미로 해석할 수 있다.

일본 정부는 사이버안보 전략서를 2018년 7월, 2021년 9월 각각 개정하여 총 3번에 걸친 전략서를 발간하고 있다.[7] 〈표 1〉은 사이버안보 전략서의 목차를 비교했는데, 과제인식-목적-추진방향 및 체제라는 대략적인 구성은 유사하다는 것을 알 수 있다. 전략서가 매년 발간되는 문서는 아니기 때문에 개정이라고 해도 단중기적 시점에서 추진이 필요한 과제를 갱신하는 정도에서 진행되고 있다는 점을 알 수 있다.

7) 시기별 사이버안보 전략서 및 관련 자료는 NISC 홈페이지에 게재되어 있다. 内閣サイバーセキュリティセンター. "NISC関係の重要文書." https://www.nisc.go.jp/policy/jyuyo-bunsho/index.html(검색일: 2024.8.19.)

[표 1] 사이버안보 전략서 목차 비교

2015 사이버안보 전략서 (2015.9. 발표)	2018 사이버안보 전략서 (2018.7. 발표)	2021 사이버안보 전략서 (2021.9. 발표)
1. 책정의 취지 2. 사이버 공간에 관한 인식 3. 목적 4. 기본원칙 5. 목적 달성을 위한 시책 6. 추진체제 7. 향후 대응	1. 책정의 취지 및 배경 2. 사이버 공간에 대한 인식 3. 본 전략의 목적 4. 목적 달성을 위한 시책 5. 추진체제	1. 책정의 취지 및 배경 2. 본 전략의 기본적 이념 3. 사이버 공간을 둘러싼 과제인식 4. 목적 달성을 위한 시책 5. 추진체제

출처: 内閣サイバーセキュリティセンター. "2015 サイバーセキュリティ戦略," "2018 サイバーセキュリティ戦略," "2021 イバーセキュリティ戦略."

사이버안보 전략서에 제기된 다양한 과제 중에서 안보 분야의 이슈를 비교 분석해보면 다음과 같다. 2015년 전략서는 일본의 안보 과제로서 사이버 공격에 적절하게 대응하고 사이버 공간의 안전한 이용을 확보한다고 제시하고 있다. 이를 위해 범정부적 대응능력을 강화하면서 적극적 평화주의(積極的平和主義) 기조하에 동맹 및 유사입장국과의 협력이 중요하다고 덧붙였다.[8] 그리고 사이버 공간에 있어 법의 지배를 확립하기 위한 국제 규범을 형성하는 데 적극적으로 기여하겠다는 점을 강조했다.

2018년 전략서는 이전 전략서의 기본 기조를 유지하면서도 사이버 공간의 안전을 확보하기 위해서 사이버 공격에 대응하는 방어력(防御力), 억제력(抑止力), 상황인식 능력(状況把握力)을 향상시켜야 한다는

8) 적극적 평화주의는 2013년 12월 아베 정부가 처음 발간한 「국가안보전략서」에 제시된 개념으로, 일본이 대외관계에 있어 적극적으로 참여하고 규범 창출을 위해 노력하겠다는 정책 방향을 보여준다.

보다 구체적인 조치를 담았다. 방어력은 국가를 방어하는 능력, 억제력은 사이버 공격을 억제하는 능력, 상황인식 능력은 사이버 공간의 상황을 파악하는 능력으로 각각 설명했다. 사이버 공간이 군사화되고 있는 만큼 사이버 공격에 대응할 수 있는 방위성 차원의 노력이 중요해진다는 인식이 반영되어 있다. 사이버 공간에 적용하는 국제적 규범과 규칙이 부재한 상황에서 개별국가가 군사적 조치를 포함하는 사이버 역량을 갖추는게 중요한 만큼 자위대의 활동 범위를 사이버 공격에 대한 방어, 억제, 상황인식으로 확장할 필요가 있다는 정책적 판단도 포함되어 있다. 사이버 방어나 사이버 억제는 전통적 군사개념인 방어와 억제를 사이버안보에 적용하는 방식인데 어떤 수준에서 사이버 공격에 대한 방어와 억제가 가능할지는 논쟁이 계속되고 있다(Smeets and Work 2020).[9] 일본 정부는 사이버 공간에서의 위협을 억제하고 대응해야 한다는 점에서 자위대의 사이버 활동을 확대하려고 하지만 미래의 전장으로 사이버 충돌이나 사이버 전쟁을 다루는 수준에 이른 것은 아니다. 예컨대 일본 방위성은 2018년 12월 「방위계획 대강(防衛計画の大綱)」을 발표하고 군사적으로 사이버 역량이 중요한 만큼 민간에서 사이버 공간을 안정적으로 활용할 수 있는 사이버안보가 중요하다고 지적했다.[10] 전략서 수준에서 사이버 방어와 사이버 억제가 제시되기는 했지만 방위성의 정책과 연계는 약

9) 국내에서도 사이버 공간의 억제는 핵 억제와는 다르나 완전하게 불가능한 것은 아니기 때문에 한국의 사이버안보 전략에 맞는 사이버 억제를 구성할 필요가 있다는 의견이 있다(민병원 2015; 김상배 2018; 기세찬 2022).

10) 구체적인 내용은 다음을 참조한다. 防衛省. 2018. “平成 31 年度以降に係る防衛計画の大綱について.” https://www.mod.go.jp/j/policy/agenda/guideline/2019/pdf/20181218.pdf(검색일: 2024.7.10.)

하다는 것을 알 수 있다.

[표 2] 사이버안보 전략의 세 가지 핵심축

규범	자유롭고 공정하며 안전한 사이버공간의 확보
추진방식	국제협력과 협조
정책수립	방어, 억제, 상황인식 능력의 강화

출처: 内閣サイバーセキュリティセンター. 2021. "2021 サイバーセキュリティ戦略."

2021년 발간된 전략서는 사이버안보에 대한 군사적 접근을 재차 강조했다. 2021년 전략서는 사이버안보 전략을 〈표 2〉와 같이 세 가지 핵심축을 제시하고 이를 달성하기 위한 정책방향을 제시했다. 세 가지 핵심축은 2015년 및 2018년 전략서의 내용을 재확인한다는 점에서 정책의 연속성을 보여준다. 차이점은 사이버공간에 대한 인식으로, 2021 전략서는 "사이버공간이 지정학적 긴장을 반영하면서 평시부터 국가 간 경쟁의 공간이 되고 있다"고 언급하며 사이버공간의 군사적 접근을 강조했다. 방어력 향상은 국가 기반시설을 제공하는 민간사업자에 대한 보호 및 국가 첨산기술 및 방위산업 관련 기술에 대한 보호를 포함했다. 억제력 향상은 미일동맹을 통한 거부를 통한 억제(deterrence by denial)와 외교적 비난과 같은 비정당화에 의한 억제(deterrence by delegitimization)를 포함하는 실효적 방안 마련을 제시했다.[11] 그리고 다자간 사이버 규칙과 규범을 마련해서 신뢰구축을

11) 사이버 공간이 발전할수록 사이버 공격이나 위협을 막기 위한 방안으로 억제 개념이 활용되고 있다. 그러나 사이버 억제에 대한 정밀한 개념화는 부족한 상태이다. 이러한 한계에도 학계에서는 군사안보의 전통적 억제 이론인 징벌에 의한 억제(deterrence by punishment)와 거부

조성하는 국제적 제도가 중요하다고 강조했다. 이러한 일본의 사이버 억제는 보복에 의한 억제를 배제할 수 밖에 없는 자위대 활동의 법적 제약을 반영한 것으로 이해된다. 보복은 기술적인 문제인 것과 동시에 정치적 문제이기 때문에 억제에 있어서 보복의 정당성을 확보하는 것은 용이한 과제는 아니다(Gartzke 2013; Gartzke and Lindsay 2015). 마지막으로 상황인식 능력은 유관부서와의 협력으로 정보통합 및 연계를 강화한다는 것이다.

2. 능동적 사이버방어 개념 도입

사이버안보에 대한 군사적 접근은 2022년 12월 일본 기시다 정부가 발간한 「국가안보전략서」에서 '능동적 사이버방어' 개념을 도입하는 정책 방향을 제시하면서 구체화되었다(大澤淳 2024). 서론에서 언급했듯이 기시다 정부는 2022년 12월 개정된 「국가안보전략서」에 사이버 공격을 미연에 방지하는 '능동적 사이버방어(能動的サイバー防御, active cyber defense)'라는 개념을 도입했다(표 3 참조). 능동적 사이버방어는 개념적으로 두 가지 특징이 있다. 첫째, 사이버방어에 '능동'이라는 개념을 추가한 것이다. 수동적 방어(passive defense)에서 적극적 방어(active defense)로 전환하는 정책이 추진될 것을 의미한다. 둘째, 평시에 대한 사이버공간 방어이다. 유사시에는 자위대가 중심이 되어 사이버 공격이나 위협에 적극적으로 대응할 수 있지만, 평시

에 의한 억제(deterrence by denial)를 적용한 사이버 억제이론을 발전시키고 있으며 최근에는 정책적 관점에서 비정당화에 의한 억제(deterrence by delegitimazation), 회복에 의한 억제(deterrence by resilience) 등의 개념도 활용되고 있다(Wilner, 2020).

에는 사이버방어를 위한 자위대 활동은 제한적이다. 그러나 기반시설에 대한 사이버 공격이 증가하고 있고, 사회 전반적인 안전을 불안하게 하는 만큼 평시에 사이버공간을 감시하고 위협을 식별하는 안보정책이 요구되고 있다. 이에 일본 정부는 2023년 1월 내각 사이버안보법제정비팀(サイバー安全保障体制整備準備室)을 만들어 능동적 사이버방어 구축을 위해 평시 사이버안보를 강화할 수 있도록 법과 제도를 정비하고, 이를 수행할 주체를 설정하는 논의를 시작했다.

[표 3] 국가안보전략서에 기술된 능동적 사이버 방어

무력공격에는 이르지 못하나 국가, 중요 사회기반시설 등에 대해 안보상 우려가 발생 될 중대한 사이버 공격의 징후가 있는 경우, 그것을 미연에 배제하고, 그러한 사이버 공격이 발생한 경우의 피해 확대를 방지하기 위해 능동적 사이버 방어(能動的サイバー防御)를 도입한다. 이를 위해 사이버 안보분야에 있어 정보수집 및 분석 능력을 강화하고, 동시에 능동적 사이버 방어의 실현을 위해 체제를 정비하는 것으로 다음의 1~3의 필요한 조치를 실현하기 위한 검토를 추진한다.

1. 중요 사회기반시설 분야를 포함, 민간사업자 등이 사이버 공격을 받은 경우 정부에 정보를 공유하고 정부로부터 민간사업자 등으로 대응을 조정하며 지원 등 조치를 강화하기 위한 조치를 추진한다.
2. 국내 통신사업자가 역무를 제공하는 통신에 관련한 정보를 활용하고 공격자에 의한 악용이 의심되는 서버 등을 검사해서 알아내기 위한 조치를 추진한다.
3. 국가, 중요 사회기반시설 등에 대한 안보상 우려를 발생시키는 중대한 사이버 공격에 대해서, 가능한 미연에 공격자의 서버 등에 침입, 피해를 방지하기 위해 정부에 대해 필요한 권한이 부여되도록 한다.

출처: 内閣官房. 2022. “国家安全保障戦略について.”

〈표 3〉에서 알 수 있듯이 일본 정부는 능동적 사이버방어 도입을 위해서 위협의 사전 식별을 위한 정보 수집 및 분석이 중요하다고 지

적한다. 국가안보 차원에서 지향하는 사이버안보가 사이버 공간에서의 자유로운 활동을 위한 방어적 작전에 머물러 있음을 알 수 있다. 2021 사이버안보 전략서에서 사이버 방어력 향상을 위해 거부에 의한 억제와 비정당화에 의한 억제를 통합적으로 강조한 것과 동일한 맥락이다. 이는 능동적 사이버방어가 미국, 영국 등 보복이나 비용 부과에 의한 억제를 강조하면서 공세적 사이버 작전(offensive cyber operations)을 발전시키는 것과는 차이가 있다(佐々木勇人·瀬戸崇志 2024).[12] 공세적 사이버 작전은 평시에도 상대의 네트워크 시스템에 접근해서 수행하는 작전이지만 사이버 공격을 포함하는 공격 작전과는 다르다(Moore, 2022). 일본이 제시한 능동적 사이버방어가 외부로부터의 침입을 막기 위한 활동에 방점이 맞춰져 있다면, 공세적 사이버 작전은 상대의 네트워크 시스템에 접근해서 그 기능을 방해하거나 파괴하는 적극적 방어로 이해할 수 있다.

또한, II장에서 언급된 사이버안보 전략서에는 '적극적 사이버방어' 개념이 들어가 있는데 능동적 사이버방어 개념과는 차이를 보인다. 적극적 사이버방어는 국가에 대한 심각한 사이버 공격에 실효적으로 대응하고, 위협에 대해 사전에 적극적인 방어책을 펼치는 정책이라고 할 수 있는데, 이는 능동적 사이버방어가 포함하는 사전적 대응에는 미치지 않는다(森秀勲, 2023). 이러한 문서 간 개념 공백을 메꾸기 위해 조만간 사이버안보 전략서도 개정될 가능성이 있다.

따라서 공세적 사이버 작전이 근미래 군사작전을 위해 지속적으로

12) 미 합참은 2018년에 발표한 합동교리를 통해 공세적 사이버 작전이 사이버전략에 포함된다고 밝혔다. Joint Chiefs of Staff. 2018. Cyberspace Operations JP 3-12. Washington, DC: Joint Chiefs of Staff.

수행하는 작전이라는 의미에서 사이버 전쟁도 염두에 두고 있다면, 일본은 여전히 사이버 전쟁이 아닌 사이버방어에 초점을 맞춘 사이버안보 전략을 발전시키고자 하다는 한계를 알 수 있다. 나아가 능동이라는 개념은 여전히 방어에 한정되어 있기 때문에 사이버 공격에 대응하기 위한 선제적 방어를 강조하는 공세적 사이버 작전에는 미치지 못할 것으로 보인다. 이는 자위대가 실시 가능한 사이버 작전과 현행 자위대법 간의 적합성 문제와도 관련된다(陣内徹之助·湯浅墾道, 2023).

그렇다면 일본이 능동적 사이버 방어라는 개념을 도입한 이유는 무엇일까. 평시에 사이버 공간에서 일어나는 대내외 활동을 감시하고 위협을 식별할 수 있는 사이버안보 정책의 추진이라고 볼 수 있다. 그러나 공세적 사이버 작전에는 미치지 못하지만 능동적 사이버 방어에 반격 능력(counterstrike capabilities)을 포함하는 적극적 형태의 정책이 구현될 수 있다. 왜냐하면 사이버안보를 단순히 시스템에 대한 침투 혹은 침략을 방어한다는 의미를 넘어 상대의 공격 징후를 탐지하고 파악해서 사전에 무력화하는 조치를 포함할 수 있기 때문이다. 그리고 이러한 조치를 위해서는 자위대의 활동이 확대된다는 것을 의미한다. 자위대는 유사시 방어를 담당하는 전수방위 규범에 의해 엄격하게 그 활동이 제한되어 있는데, 사이버공간의 안보를 위해 유사 이전의 단계인 평시에 다양한 활동이 가능하도록 그 범위를 재규정할 수 있다.

능동적 사이버 방어는 평시와 유사의 경계에 있는 회색지대에서 벌어지는 사이버 공격에 대한 조치를 포함하는 광의의 개념이라고 볼 수 있다. 2024년 6월부터 능동적 사이버방어 법제 준비를 위한 전문가 회의(有職者会議)가 개최되고 있으며, 각계 전문가 17인이 참석

한다.[13] 일본 정부는 회의 개최를 통해 전문가 의견을 수렴하고 이를 참고로 디지털청이 주도하여 입법을 추진한다는 입장이다(日本経済新聞, 2024/5/31). 이러한 배경에는 현재 일본의 사이버 방어가 무력공격을 받는 경우에 자위권이 발동되는 수동적 개념에 포함되어 있기 때문에 적절하게 대응이 어렵다는 정부의 입장이 반영되어 있다. 위협이 발생한 후 대응을 하면 피해는 이미 발생한 이후가 되기 때문에 능동적 대응에서는 위협 발생 단계에 대한 감시와 탐지가 핵심이 된다. 이상의 논의를 바탕으로 일본 정부는 사이버 공간을 상시 감시하면서 정부 기관이나 중요 사회기반시설에 대한 공격 징후가 있는 경우에 그 피해를 방지할 수 있는 조치가 중요하다고 본다. 따라서 일본 정부가 능동적 사이버방어를 위한 정책을 구체화할 때 '능동'의 범위와 조치가 적극적 방어에 머무는 것인지 공세적 작전으로 발전시키고자 하는 의도를 포함하는지 주의해서 살펴볼 필요가 있다.

Ⅲ. 방위성의 사이버안보 정책

일본 방위성은 국가안보전략서를 통해 능동적 사이버 방어를 도입한다는 상위 전략에 근거해서 세부적 지침을 구체화하고 있다. 장기적 차원에서 능동적 사이버 방어를 실현하기 위한 법제 도입 및 조직 마련이 논의되고 있는 한편, 방위성은 단기적 차원에서 자위대의 부

13) 공식적인 명칭은 '사이버 안보분야에서 대응능력을 향상하기 위한 전문가 회의(サイバー安全保障分野での対応能力の向上に向けた有識者会議)'이며, 2024년 6월부터 개최되고 있다.

대개편과 인력 양성을 추진하고자 한다. 이러한 변화는 일본이 사이버안보를 구현하는 사이버역량의 척도가 되기 때문이다.

일본 방위성은 2022년 12월 「국가안보전략서」를 반영한 방위성 차원의 국방전략을 제시한 「국가방위전략서(国家防衛戦略)」를 발간했다.[14] 「국가방위전략서」는 우주, 전자기 영역과 함께 사이버 영역의 중요성을 강조하면서, 영역횡단작전 수행에 있어 사활적으로 중요한 만큼 범정부적인 노력으로 사이버 역량을 강화할 필요가 있다고 언급했다. 〈표 4〉에서 설명하듯이 사이버 영역은 우주, 전자기 영역과 더불어 평시에서 유사에 이르는 모든 분쟁 단계에 있어 정보를 수집하고 공유하는 영역횡단작전 수행에 핵심이 되기 때문이다.

[표 4] 국가방위전략서에 기술된 사이버 영역

사이버 영역에 있어 외국, 관계 부처 및 민간사업자와 연계해서 평시부터 유사까지 모든 단계에서 정보를 수집하고 공유하면서 범정부 차원의 사이버안보 대응능력을 강화해 나가는 게 중요하다. 범정부 차원에서 사이버안보 분야의 정책이 일원화되어 종합적으로 조정되는 과정에서 방위성 및 자위대도 사이버안보의 수준을 높여나가며 관계 부처, 중요 기간산업 기업, 방산업자 등과 연계를 강화해나가는 대응을 추진한다.

출처: 防衛省. 2022. “国家防衛戦略について.”

방위성이 2024년 7월에 발간한 「2024 방위백서」에 따르면 능동적

14) 공식적인 명칭은 ‘사이버 안보분야에서 대응능력을 향상하기 위한 전문가 회의(サイバー安全保障分野での対応能力の向上に向けた有識者会議)’이며, 2024년 6월부터 개최되고 있다.

사이버방어를 도입하여 범정부적 대응능력을 서구 주요국 수준으로 갖추는 것을 목표로 내각관방을 중심으로 구체적인 조치를 추진해 나간다고 지적했다. 이를 위해 사이버 분야 방위비를 2023년부터 2027년까지 5년간 약 1조엔 투입할 것으로 알려졌다. 특히, 2024년에는 정부 내 상시감독기구(Government Security Operation Coordination Team)을 발전시켜 인터넷 및 네트워크 체계의 안전을 강화한다고 밝히고 있다. 이러한 언급은 사이버 공격에 따른 자위대 활동에 대한 대응을 강조했던 「2023년 방위백서」의 내용과 차이를 보이고 있다. 다시 말해 이전까지 방위성은 자위대에 피해가 발생한다면 이에 대응하겠다는 정책적 사고에 머물렀다면, 2024년부터는 범정부적 사이버 역량 강화를 위해 적극적으로 사이버 정책을 도입한다는 입장을 드러내고 있다. 특히, 내각 사이버안보센터가 주도하에 정부 차원의 사이버안보 역량을 강화하는데 맞춰 방위성과 자위대도 능동적 사이버방어 도입을 위한 종합적 대책을 수립한다고 강조한다.

방위성이 2022년 12월 발표한 「방위력정비계획(防衛力整備計画)」은 자위대가 사이버안보를 강화하기 위한 2023년부터 2027년까지의 중기 계획을 구체화하고 있다.[15] 지난 10여 년간 기술혁신으로 인공지능(AI), 양자기술, 차세대 정보통신기술 등과 같은 첨단기술이 연구·개발되고 있으며, 소위 게임 체인저라고 불리는 이러한 기술이 군사분야에 적용되고 있다. 방위성은 이러한 신기술의 군사적 활용이 사이버 공간에서 위험을 높일 수 있다고 지적한다. 예를 들어 중요 사회

15) 본문은 다음을 참조한다. 防衛省. 2022. "防衛力整備計画について." https://www.mod.go.jp/j/policy/agenda/guideline/plan/pdf/plan.pdf(검색일: 2024.7.10)

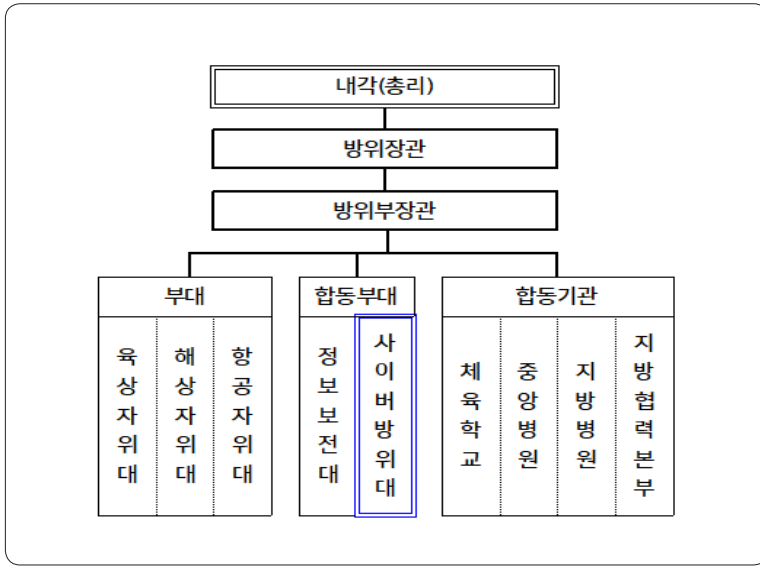
기반시설에 대한 사이버 공격은 단순한 물리적 군사력의 사용이 아니기 때문에 물리적 대응이 어려운 애매한 상황에 직면하게 될 가능성이 크기 때문이다.

1. 자위대의 부대 개편

자위대는 2022년 7월 육상·해상·항공 자위대의 합동부대로 자위대 사이버 방위대(自衛隊サイバー防衛隊)를 편성했다. 각 군이 사이버 방어를 목적으로 편성했던 부대를 일원화하여 합동성을 높이려는 목표였다. 기존에 육상자위대는 시스템방호부대(システム防護隊), 해상자위대는 안전감사부대(安全監査隊), 항공자위대는 시스템감사부대(システム監査隊)를 통해 각각 사이버 임무를 맡고 있었다. 그러나 군종별로 구분된 사이버방어는 합동작전 수행이 어렵기 때문에 방위장관 직속부대로 자위대 사이버 방위대를 창설했다(그림 2 참조). 사이버 방위대의 주요 임무는 사이버 공격 대응, 방위정보통신기반(DII)의 관리 및 운용, 사이버 훈련 기획 및 지원 등이며 방위성 내에 본부를 둔다. 초기 규모는 450명이었는데 160명을 증원하여 540명 규모로 편성되었다.

그리고 2024년 3월 방위성은 육상자위대 통신학교를 시스템통신·사이버 학교(陸自システム通信·サイバー学校)로 개편했다. 가나가와현 요코스가시에 위치한 시스템통신·사이버 학교는 130명 규모의 전문인력을 교육하고, 2023년 12월 요코스가 연구공원에 설립된 사이버 안보인재기반협회(サイバー安全保障人材基盤協会)와의 협력도 강화하고자 한다(朝日新聞, 2024/4/1). 덧붙여 방위대학교의 정보공학과는 사이버·정보공학과로 개편해서 전문인력 교육을 추진한다.

〈그림 2〉 방위성 및 자위대 조직



출처: 防衛省. 2024. 令和6年防衛白書.

2. 사이버안보 인력 마련

방위성은 2024년 7월 「방위성 사이버인재 종합전략서(防衛省サイバー人材総合戦略)」를 발표하고 사이버안보 분야의 인력 마련을 종합적으로 추진할 전략을 제시했다.[16] 군 차원에서는 자위대에 사이버안보

16) 방위성은 2024년 7월 2일 인공지능 활용 및 사이버인재 육성을 위한 두 가지 문건(「방위성 AI활용추진 기본방침」 및 「방위성 사이버인재 종합전략서」)을 동시에 발표했다. 본문은 홈페이지에 각각 게재되어 있다. 防衛省. 2024.“防衛省ＡＩ活用推進基本方針と防衛省サイバー人材総合戦略の策定について.”

관련 교육기관을 보유하고 있고 이를 충분히 활용해서 사이버인력 마련이 가능할 것으로 보았다. 다만, 민간 분야에서의 인재 도입 및 육성은 여전히 과제로 남아있다.

이미 방위성은 「방위력정비계획」을 통해 사이버안보 전문인력을 중점적으로 마련하겠다고 밝혔다. 구체적으로 2027년까지 사이버안보 전문인력풀을 약 2만 명 확보하고, 그중 사이버 부대에 4,000명을 편성할 것임을 언급했다. 이는 2022년 말 890명 규모의 약 4배가 되는 것으로 인재 육성과 확보가 중요한 과제임을 알 수 있다. 이러한 배경에서 방위성은 사이버안보 인력 마련의 지침과도 같은 종합전략서를 발표한 것이다(표 5 참조).

[표 5] 방위성 사이버인재 종합전략서 목차

1. 전략의 배경과 목적
2. 방위성/자위대의 임무와 사이버인재
3. 사이버인재 관련 정책 방향 1) 사이버인재의 특징과 관련한 정책 2) 사이버인재의 확보와 관련한 정책 3) 사이버인재의 육성과 관련한 정책 4) 사이버인재의 유지 및 관리와 관련한 정책 4) 사이버인재 관련 정책 전체를 종합적으로 강화하기 위한 방책

출처: 防衛省. 2024. "防衛省サイバー人材総合戦略."

〈표 6〉은 방위성이 추진하는 사이버 분야 인력확충(안)이다. 사이버 전문 부대원은 2022년 890명, 2023년 2,230명, 2024년 2,410명이

[표 6] 사이버안보 인력확충(안)

	2022년	2023년	2024년		2027년
사이버 전문인력	약 890명	약 2,230명	약 2,410명	▶	약 4,000명
사이버 관련 총인력	(양성 및 확보)				약 20,000명

출처: 防衛省. 2023. "防衛力抜本的強化の進捗と予算:令和6年度概算要求の概要."

될 것으로 예상하나 이러한 규모를 대폭 늘려서 2027년에는 4,000명을 달성한다는 계획이다. 그리고 2027년에는 민간 분야 등 다양한 사이버안보 인력을 확충해 총 2만 명 규모를 갖추겠다는 계획이다.

나아가 방위성은 '사이버 자위관(サイバー自衛官)'이라고 명칭하는 사이버안보 분야의 민간 인력 채용도 추진하고 있다. 자위대 내 민간 인력은 엔지니어 일부 분야에만 국한되어 있었는데 첨단기술을 활용할 수 있는 인재 영입을 위한 인사제도를 개선하고자 한다. 연봉은 최대 2,300만 엔 정도 규모로 임기제(5년 이내) 일반직 채용 및 연령제한(18~32세) 미적용 등을 담은 자위대법 개정안을 2024년에 발의할 것으로 알려졌다(日本経済新聞, 2023/5/12).

방위성의 인식은 사이버 공격이 점차 고도화, 정교화되고 있기 때문에 항시 사이버안보 대책이 필요하다고 보며, 사이버 공격의 주체가 특정 국가나 군도 포함하는 만큼 고도의 공격에 대해서는 자위대와 방산업체 간 협력이 중요하다고 본다. 나아가 자위대 운용에 있어 사이버 공간에 대한 의존도가 높아지는 만큼 미일 동맹 협력 차원에서도 사이버안보는 확보할 필요가 있다고 본다.

IV. 사이버안보의 미일 협력

능동적 사이버 방어를 구축하기 위해 방위성은 자위대의 부대개편, 인력 양성이라는 두 요소를 중심으로 사이버 역량을 배양하고 있다. 이러한 방위성의 사이버안보 정책은 미국과의 동맹협력과도 연계되면서 진행되고 있다. 일본의 사이버안보 전략서와 방위백서에서 공통적으로 미국과의 사이버안보 협력이 일본의 사이버 방어 및 억제에 중요하다고 지적한다. 미국은 선제적 방어(forward defense)와 지속적 개입(persistent engagement), 층위적 사이버 억제(layered cyber deterrence), 회복에 의한 사이버 억제(deterrence by resilience) 등 다양한 사이버 억제의 개념을 진화시켜왔으며, 2023년에는 통합억제의 시각에서 사이버 억제를 실현하기 위한 사이버안보 전략을 발표하기도 했다(김소정 2023). 이러한 미국의 개념적 선도와는 다르게 일본은 적극적이며 능동적 사이버 역량 도입에는 찬성하지만 공세적 전환에는 유보적인 입장을 보이고 있다. 이러한 차이는 정책적으로 미일 협력에서 극복해나가야 할 과제일 수 있으나, 정부 간 계속된 협의는 미일 안보협력을 사이버 분야로 확장하는데 합의하는 등 보다 진전된 협력의 형태를 구축해나가는 방향으로 발전해나가고 있다.

1. 안보조약 5조의 확장

사이버안보 분야에서 일본은 미국과의 협력을 강조한다. 사이버안보는 미일동맹 차원에서 중요한 협력 분야일 뿐만 아니라 파이브 아이즈(Five eyes)와 같이 지역 소다자 안보협력체에 참여하기 위해서도 사이버안보는 핵심적이기 때문이다. 미일 간 사이버안보 협력이 본

격적으로 시작된 것은 2013년 10월 미일 사이버국방정책 워킹그룹(Cyber Defense Policy Working Group, CDPWG) 설치 이후이다. 방위성은 2013년 10월 미일 국방장관회담 합의를 실행하고자 CDPWG를 운영하고 있다. 여기에서는 사이버 관련 정책 협의 추진, 정보공유, 사이버 공격 대응을 위한 공동훈련 추진, 전문가 육성 및 확보를 위한 교육 등 다방면에 걸친 협력을 추진하고 있다. 매년 1~2회 정도 개최되는 CDPWG는 2022년 5월 기준으로 8차례 회의를 개최했으며 2015년 회의에서는 공동선언을 발표하여 자위대-미군 간 협력을 강화하고자 했다. 이와 더불어 일본은 미국과 미일 사이버 대화(Cyber Dialogue), 미일 IT 포럼 등을 개최하고 있다(防衛省 2024).

일본은 「2018 방위계획 대강」에서 사이버 분야를 대응이 필요한 신영역으로 강조했고, 2019년 개최된 미일 외교·국방장관회의(2+2회의)에서 사이버 분야에 대한 새로운 협의가 진행되었다(표 6 참조). 구체적인 내용은 밝히지 않았지만, 미일 양국은 악의적 사이버 활동에 대한 위협을 인식하고 사이버 공간에 국제법이 적용됨을 확인했다. 그리고 2023년에 개최된 미일 외교·국방장관회의에서 미일동맹 현대화의 과제 중 하나로 사이버안보가 언급되었다. 양국은 동맹국으로서 사이버안보 및 정보안전의 중요성을 강조한다고 밝히면서, 2022년 3월 일본 자위대에 사이버방위대가 신설된 것을 환영하고 고도화되고 상시화된 사이버 위협에 대응하기 위한 협력을 강화하는데 의견을 일치했다고 덧붙였다.

[표 7] 2019년 미일 2+2회의 공동발표문 중 사이버안보에 관한 언급

On cyberspace issues, the Ministers recognized that malicious cyber activity presents an increasing threat to the security and prosperity of both the United States and Japan. To address this threat, the Ministers committed to enhance cooperation on cyber issues, including deterrence and response capabilities, but as a matter of priority, emphasized that each nation is responsible for developing the relevant capabilities to protect their national networks and critical infrastructure. The Ministers affirmed that international law applies in cyberspace and that a cyber attack could, in certain circumstances, constitute an armed attack for the purposes of Article V of the U.S.-Japan Security Treaty. The Ministers also affirmed that a decision as to when a cyber attack would constitute an armed attack under Article V would be made on a case-by-case basis, and through close consultations between Japan and the United States, as would be the case for any other threat.

출처: 外務省. 2019. "平成31年4月19日 日米安全保障協議委員会."

이렇게 미일 고위급 협의에서 사이버안보가 중요한 의제로 제기된 데에는 미일 안보조약의 범위를 확장해야 한다느 양국의 전략적 고려가 작용했다. 〈표 7〉에서 알 수 있듯이 양국은 미일 안보조약 5조에서 규정하는 무력 공격의 대상에 사이버 공격이 포함될 수 있다는 점을 처음으로 공식화했다. 미일 안보조약 5조는 미국의 일본 방어 의무를 규정하고 있는데, 5조 범위에 사이버 분야가 포함될 가능성을 열어둔 것이다. 이는 전통적으로 물리적 영토에 대한 방어를 규정하는 동맹 조약이 사이버 공간에 적용되는 사례가 된다. 사이버 공간에 대한 방어 의무 확대는 미일동맹 차원을 넘어 인도-태평양 지역 안보

에 있어서도 시사하는 바가 크다. '특정 상황에서' 사이버 공격이 동맹 공약의 대상이 된다고 언급한 만큼 특정 상황이 무엇을 정의하는지에 대한 논의는 아직 명확하지는 않지만, 향후 사이버안보 협력을 심화하는 방향으로 상황 정의가 내려질 가능성이 크다.

2. 공동대응의 필요와 한계

사이버 공격은 공격 주체를 특정하거나 피해 규모의 파악이 쉽지 않다. 정보통신기술의 발달과 데이터 활용은 군의 지위통제 체계를 구성하는 중요한 부분이 되고 있는데, 이러한 기술에 대한 의존도가 높아진 만큼 사이버 공격에 대한 취약성도 높아지고 있다. 나아가 사이버 공격이 기반시설에 대한 직접적인 공격이 발생하는 경우가 늘어나면서 사전에 악의적 활동을 탐지하고 위협 요인을 제거하는 사이버 대응이 주목을 받고 있다. 미국은 이러한 사전적 대응에 적극적인 국가이며, 양자 및 다자 협력을 통해 공동 대응을 추진하고 있다.

미국 사이버사령부는 헌트 포워드(hunt forward)라는 작전을 통해 악의적 사이버 활동을 관찰하고 식별하고 있는데 동맹 및 유사입장국과 공동으로 작전을 전개하기도 한다.[17] 2020년 중국 해커 집단이 일본 정부의 군사기밀을 취급하는 시스템에 침투한 사건이 발생했다.[18] 중국 해커의 침투는 미국에 의해 밝혀졌고, 폴 나카소네 당시

17) 미국은 헌트 포워드 팀을 우크라이나에 파견해 러시아의 사이버 공격으로부터 우크라이나를 지원해왔다고 알려졌다.

18) 해당 사건은 2023년 8월 7일 미국 워싱턴포스트에 실린 Ellen Nakashima의 기사로 인해 밝혀졌다(Washington Post, 2023/8/7).

사이버사령부 사령관은 일본 정부에 해킹 사건을 직접 경고하기도 했다. 이를 계기로 미국은 일본에서 미군-자위대 공동으로 헌트 포워드 작전을 펼칠 것을 요청했다. 그러나 일본 내부적으로 자국 네트워크에 외국군이 개입하는 데에 강한 반발에 부딪쳐 일본 독자적으로 사건을 조사하는 것으로 마무리되었다(森秀勲, 2023). 이같은 사례에서 알 수 있듯이 사이버 공격에 대한 취약성을 극복하고자 하는 동맹 협력이 필요하더라도 사이버 작전의 폐쇄성에 기인한 배타적 태도가 협력의 동인을 제한하는 결과를 가져오기도 한다.

V. 결론

본 연구는 일본의 국가안보전략에서 사이버 공간의 군사화가 다뤄진 것을 계기로 능동적 사이버 방어라는 새로운 사이버안보 정책을 도입하게 된 배경과 방위성의 세부적 정책을 분석했다. 일본은 연결성과 개방성이라는 사이버 공간의 본질에 대해 서방국가들과 유사한 시각을 공유하면서 사이버 공격을 억제하고 대응하는 사이버 역량을 강화할 필요성에 주목했다. 앞서 언급했듯 일본 정부는 주요 문서를 통해 사이버안보의 중요성을 강조하고 있으며, 방위성은 사이버안보를 방위력 강화의 중요한 부분으로 취급하고 있다. 기시다 정부가 국가안보전략서를 통해 외교력을 뒷받침하는 견고한 방위력을 갖추기 위해 노력한다고 밝힌 만큼 방위성 차원에서 사이버안보를 강화하는 여러 정책이 갖춰질 것으로 보인다.

그 과정에서 유념해야 할 점은 크게 세 가지이다. 첫째, '능동적 사이버 방어'에 대한 이해이다. 일본 정부가 능동적 사이버 방어를 갖춘

다고 발표한 만큼 향후 구체적으로 어떠한 범위에서 능동적 사이버 방어가 가능할지에 대한 논의가 이루어질 것이다. 실제로 2024년 5월부터 기시다 정부와 여당 자민당이 능동적 사이버 방어 관련 법제 마련을 위한 논의를 시작했다. 일본 정부는 사이버 방어법 추진을 위한 전문가 회의를 6월부터 개최하고 있는데, 자민당은 경제안보추진본부, 디지털사회추진본부, 안전보장조사회가 합동회의를 개최하고 법안 마련을 위한 협의를 진행하기 시작했다(産経新聞, 2024/5/13). 능동적 사이버 방어의 방점이 위협의 식별과 공격 방지에 있는 만큼 헌법에 보장된 통신의 자유와 어떻게 정합할 수 있을지에 맞춰질 것으로 보인다. 국내적으로는 개인 이메일 등에 대한 사적 자유 보호가 중요할 것이며, 대외적으로는 해외서버에 접근할 경우 상대국과의 외교 마찰 가능성 등이 대두될 수 있다(朝日新聞, 2024/5/17).

둘째, 자위대법 개정 방향이다. 자위대는 유사시 사이버 방어에 집중하는데, 현재 능동적 사이버방어의 초점이 되고 있는 사전 조치를 하기 위해서는 평시부터 사이버 방어가 가능하도록 임무를 변화시켜야 한다. 자위대가 방산업체 등 민간 기업에 사이버 방어를 제공하거나, 기간시설을 보호하기 위한 사이버 방어를 조치하기 위해서는 무력 공격이 일어나기 이전 단계에서 자위대의 활동을 보장할 수 있는 법적 조치가 요구되기 때문이다. 현재는 경찰이 치안활동을 할 수 없거나 해상보안청이 경비활동을 하기 어려운 상황에 제한해서 평시 자위대의 활동이 보장되고 있다(読売新聞, 2024/7/11). 능동적 방어는 방어적 역량에 초점이 맞춰져 있지만 법안 마련을 위한 정부 및 여당 논의는 일본의 사이버 공간을 보호하는데 개방보다는 배타적 방향으로 전개될 가능성도 있다. 이러한 논의를 발전시키는 과정에서 자위대법이 어떠한 방향으로 개정될지 유심히 살펴볼 필요가 있다.

셋째, 미일 협력의 발전 가능성이다. 미일 양국은 안보조약 5조의 범위에 사이버 공격이 포함될 수 있다는 점을 협의했다. 다만, 현재의 미일 방위협력지침(Guideline)에서는 그러한 부분은 다루고 있지 못하다. 따라서 근미래에 미일 양국이 방위협력지침을 개정하고자 한다면 사이버안보가 핵심적인 이슈 중 하나로 다루어질 수 있다. 2024년 5월 미일 정상회담과 함께 개최된 미국-일본-필리핀 간 삼자회담에서 사이버위협 정보를 공유하는 협력을 추진하겠다고 밝혔다. 이렇듯 사이버안보는 미일 동맹 차원을 넘어 지역 안보에도 중요한 함의를 지닐 수 있다는 점에 유의해야 할 필요가 있다.

〈참고문헌〉

기세찬. 2022. “사이버 억제에 관한 연구,” 『국방연구』65권 3호, 189-214.

김상배 편. 2018.『사이버안보의 국제정치학적 지평』. 서울: 사회평론아카데미.

김소정. 2023. “2023 미국 사이버안보 전략 주요내용과 한국에의 시사점,” 『국가안보전략연구원 이슈브리프』423호(3월 8일).

민병원. 2015. “사이버공격과 사이버억지의 국제정치: 규제와 새로운 패러다임을 중심으로,” 『국가전략』21권 3호, 37-61.

Gartzke Erik. 2013. “The Myth of Cyberwar: Bringing war in Cyberspace back down to Earth,” *International Security* 38(2), 41-73.

Gartzke Erik and R. J. Lindsay. 2015. “Weaving Tangled Web: Offense, Defense, and Deception in Cyberspace,” *Security Studies* 24(3), 316-348.

Goldsmith, Jack and Tim Wu. 2006. *Who Controls the Internet?: Illusions of a Borderless World*. NY: Columbia University Press.

Joint Chiefs of Staff. 2018. *Cyberspace Operations, JP 3-12*. Washington, DC: Joint Chiefs of Staff

Katagiri, Nori. 2021. “From cyber denial to cyber punishment: What keeps Japanese warriors from active defense operations?” *Asian Security* 17(3), 331-348.

Moore, Daniel. 2022. *Offensive Cyber Operations: Understanding Intangible Warfare*. Cambridge: Oxford University Press.

Namashima, Ellen. 2023. “China hacked Japan’s sensitive defense networks, officials say.” Washington Post(August 7).

Smeets Max and J.D. Work. 2020. “Operational Decision-making or Cyber Operations: In search of a model,” *Cyber Defense Review* 95-112.

Wilner, Alex S. 2020. “US Cyber Deterrence: Practicing guiding theory,”

Journal of Strategic Studies 43(2), 245-280.

朝日新聞. 2024. “能動的サイバー防御, 自民党内議論開始, 米側の強い要請も.”(5月17日)

e-GOV 法令検索. 2024. “サイバーセキュリティ基本法.” https://laws.e-gov.go.jp/law/426AC1000000104

大澤淳. 2024. “新国家安保戦略とサイバー、情報戦への対応.” JIIA 研究レポート(2.14.)

笹川平和財団. 2018.『日本にサイバーセキュリティ庁の創設を!』東京: 笹川平和財団.

佐々木勇人. 2023. “「能動的サイバー防御」は効果があるのか？-注目が集まるoffensiveなオペレーションの考察.” JPCERT/CC Eyes(8.29.)

佐々木勇人·瀬戸崇志. 2024. “サイバー攻撃対処における攻撃「キャンペーン」概念と「コスト賦課アプローチ」――近年の米国政府当局によるサイバー攻撃活動への対処事例の考察から.” NIDSコメンタリー 346, 1-28.

産経新聞. 2024. “能動的サイバー防御の有識者会議メンバーにＳＢテクノロジーの辻伸弘氏ら１７人 政府発表.”(5月31日)

陣内徹之助·湯浅墾道. 2023. “自衛隊が平時・グレーゾーンの事態で行うサイバー作戦の 情報法制上の課題.”『情報法制研究』14, 151-161.

土屋大洋. 2013. “サイバーセキュリティのグローバル・ガバナンス―国際的な規範の模索―”『Nextcom』14, 4-11.

内閣官房. 2022. “国家安全保障戦略について.” https://www.mod.go.jp/j/policy/agenda/guideline/pdf/security_strategy.pdf

内閣サイバーセキュリティセンター. 2015. “2015 サイバーセキュリティ戦略.” https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku.pdf

_____. 2018. “2018 サイバーセキュリティ戦略.” https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2018.pdf

_____. 2021. “2021 サイバーセキュリティ戦略.” https://www.nisc.go.jp/pdf/

policy/kihon-s/cs-senryaku2021.pdf

日本経済新聞. 2024. “「能動的サイバー防御」法整備, 有識者会議の設置発表.”(5月31日)

松本昌廣. 2022. “我が国のサイバーセキュリティ戦略の欠点と展望ー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), 73-94.

森秀勲. 2023. “サイバー攻撃の脅威とサイバー安全保障.” 立法と調査 461, 114-129.

防衛省. 2018. “平成 31 年度以降に係る防衛計画の大綱について.” https://www.mod.go.jp/j/policy/agenda/guideline/2019/pdf/20181218.pdf

_____. 2022. “国家防衛戦略について.” https://www.mod.go.jp/j/policy/agenda/guideline/strategy/pdf/strategy.pdf

_____. 2022. “防衛力整備計画について.” https://www.mod.go.jp/j/policy/agenda/guideline/plan/pdf/plan.pdf

_____. 2023. “防衛力抜本的強化の進捗と予算:令和6年度概算要求の概要.”

_____. 2023.『令和5年度防衛白書』, 東京:防衛省.

_____. 2024.『令和6年度防衛白書』, 東京:防衛省.

_____. 2024. “防衛省サイバー人材総合戦略.” https://www.mod.go.jp/j/press/news/2024/07/02a_05.pdf

読売新聞. 2024. “重大サイバー攻撃防止, 自衛隊に平時の新任務…攻撃元サーバーに侵入·無害化措置権限.”(7月11日)

Cybersecurity Policy by Japan Ministry of Defense and US-Japan Cooperation

Eunil Cho | Korea Institute for Defense Analyses

Cybersecurity has recently been considered crucial in Japan's security strategy. When cybersecurity was mentioned in the 「National Security Strategy」 released in December 2022, it announced that it would pursue a policy that allows the use of cyberspace safely and stably. To this end, it is expected to introduce the concept of 'active cyber defense (ACD)' and strengthen cybersecurity to 'prevent serious cyberattacks and prevent damage expansion'. To this end, the Japanese Ministry of Defense is expected to reorganize its defense policy so that it can monitor cyberspace not only during wartime but also during peacetime. The first is to reorganize the unit structure, such as the creation of a joint cyber defense unit by the Land, Navy, and Air Self-Defense Forces. Second, it is to cultivate manpower that fully utilizes military and civilian personnel. A more active form of cybersecurity policy with defense capabilities that can preemptively neutralize the possibility of cyberattacks can be promoted through these two efforts. And Japan will continue to complete active cyber defenses while deepening security cooperation with the United States in the cyber field. To this end, the Japanese National Assembly will push for legislative measures to introduce active cyber defenses, which can lead to discussions including the constitution, such as freedom of communication. In the future, the Ministry of Defense is expected to materialize a cybersecurity strategy that reflects the discussion of the National Assembly and the government's position.

Keyword Japan, Cybersecurity, Active Cybersecurity, SDF, US-Japan cooperation