일본 방위성의 사이버안보 정책과 미일협력

2024

한국사이버안보학회
KACS

한국사이버안보학회 워킹페이퍼 19호
발간일: 2024년 8월 22일

조은일 (한국국방연구원)

I. 서론

최근 일본의 안보전략에서 중요하게 다뤄지고 있는 분야가 사이버안보(サイバーセキュリティ)이다.[1] 2024년 6월 일본 대형출판사 가도카와(KADOKAWA)와 그 자회사 도완고(ドワンゴ)가 랜섬웨어에 의한 사이버 공격을 받아 다량의 개인정보 유출과 물류 시스템에 문제가 생기는 사건이 발생했다. 이 사건으로 가도카와의 주가는 일시적으로 20% 이상 하락하기도 했다. 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. 이렇듯 사이버 공격에 의한 일본 국내 산업의 취약성이 커지는 가운데 일본의 사이버안보 정책이 예방 및 대응에 충분하지 않다는 논의가 학계 및 정책서클에서 지적되어 왔다(トレンドマイクロ 2024/2). 미국 등 여타 선진국에서는 사이버 공간을 다루는 안보 문제를 국가전략의 차원에서 고려해 왔는데,[2] 일본은 2022년 12월에 발표한 「국가안보전략서(国家安全保障戦略)」를 통해 공식적으로 사이버안보가 국가전략 수준에서 다뤄진다고 언급했다(内閣官房 2022).

일본 기시다(岸田) 정부는 사이버 공간은 안전하면서 안정되게 이용할 수 있는 공간이 되어야 한다는 입장을 가지고, 사이버 공격으로부터 주요 기반 시설을 보호할 대응능력을 갖춰야 한다고 강조했다. 사이버 위협은 국가·사회적 혼란을 야기하며 전력, 정보통신, 철도, 항만 등 국가운영에 필수적인 주요 기반 시설에 대한 피해가 발생할 가능성이 높아진 것이 그 배경으로 작용했다. 이에 기시다 정부는 국가안보를 위해 '중대한 사이버 공격을 미연에 배제하고 피해 확대를 방지하기 위한 능동적 사이버 방어(能動的サイバー防御)를 도입'한다고 명시했다.

이러한 일본의 사이버안보 정책 변화의 배경은 무엇일까, 첫째, 사이버 공간의 특성을 정치체제 간 대립으로 본다. 민주주의 대 권위주의라는 정치체제의 특성이 사이버 공간에도 적용된다고 본다. 사이버 공간이 자유로운 공간인지, 규제의 대상이 되는 공간인지에 대한 대립이 존재하기 때문이다. 국가에 따라서는 사이버 공간을 국가 권력의 새로운 규제의 공간으로 다루기도 하는데, 일본은 여타 선진국과 마찬가지로 사이버 공간이 자유로운 공간으로 이해한다. 이는 사이버 공간도 정부의 규제와 관리가 필요하다고 보는 중국, 러시아 등과 다른 이해이다.

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) 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.

둘째, 사이버 공간의 목적이다. 사이버 공간은 정보통신기술(ICT)의 발달로 인해 활용 가능해진 공간이다. 그렇기 때문에 사이버 공간은 테크(tech) 기업 등과 같은 민간 행위자의 역할이 중요했다. 한편 사이버 공격과 같은 위협이 등장하면서 사이버 공간이 단순한 민간의 영역으로 남아있기 보다는 군사의 영역으로 확장해야 한다는 입장도 존재한다. 국제적으로 DDos, 랜섬웨어 등과 같은 사이버 공격이 증가하는 경향이 뚜렷한데, 해외에서 일본 국내로 들어오는 사이버 공격도 마찬가지이다. 일본 경찰청에 따르면 일본 국내에서 발견되는 의심스러운 활동수(access)가 2018년(2,752건)과 비교해서 2023년 전반기(8,219건)에 3배가량 증가했는데, 대부분이 해외로부터의 접속에 기반한다고 한다(日本経済新聞 23/10/23)

따라서 사이버 정책을 마련하는데 사이버 공간이 민간의 영역인지 군사의 영역인지에 대한 구분이 중요해졌다. 사이버 영역은 더는 민간 활동을 위한 공간으로만 존재하지 않는다. 예를 들어 러시아-우크라이나 전쟁은 허위 정보 유포가 군사작전을 교란하는 사례를 보여주면서, 물리적 전쟁에 사이버 공격이 포함되는 하이브리드 양상을 드러냈다. 이러한 사이버 위협을 해소하고 안전을 확보하기 위해서는 안보정책을 통한 군사적 대응이 마련되는 게 중요하다. 방위성은 2024년 7월 발간한 「방위백서(防衛白書)」에서 '사이버 영역은 국민 생활에 있어 필수적인 사회기반시설이며 일본 방위에 있어서 영역횡단작전(領域横断作戦) 수행을 위해 사활적으로 중요하다'고 지적했다(防衛省 2024, 298). 영역횡단작전은 주요한 전장인 육·해·공 영역에 새롭게 우주·사이버·전자기 영역을 연계해서 통합적인 작전능력을 향상시키는 것으로 미군이 추진하는 다영역 작전(multi-domain operation, MDO)과 유사한 개념으로 이해할 수 있다.[3)]

이렇듯 사이버 공간은 군사안보에 핵심적인 공간으로 확장되고 있다. 사이버 공격은 공격 주체를 특정하거나 피해 규모의 파악이 쉽지 않다. 이러한 특징을 반영해서 최근 사이버 공격을 저비용의 비대칭적 공격수단으로 활용하는 사례가 증가하고 있다. 예를 들어 2023년 9월 내각사이버안보센터와 경찰청은 미국과 공동으로 중국계 해킹그룹인 블랙테크(BlackTech)에 의한 사이버 공격이 일본 등 아시아 국가를 대상으로 빈번하게 발생하고 있다는 경고를 했다(警視庁 23/9/27).

정부 차원의 사이버안보에 대한 이해가 발전하는 만큼 군에 있어서 사이버 공간에 대한 이해도 구체화되고 있다. 군은 ICT의 발달을 지휘통제(Command and Control, C2) 체계에 적극적으로 반영하고 있으며 여기에 일본 방위성과 자위대도 예외가 아니다. 문제는 C2에 있어 ICT에 의존도가 높아지는 만큼 사이버 공격으로부터의 취약성이 높아진다는 데 있다. 이러한 점에서 군사안보의 관점에서는 사이버 공격에 따른 취약성을 어떻게 극복할지가 중요한 과제가 되고 있다. 「2024년 방위백서」에서는 중국, 북한, 러시아의 사이버 공간 악용이나 공격 사례를 주목한 것도 동일한 맥락에서 이해할 수 있다.

본고는 일본 방위성의 사이버안보 정책의 특징과 그 전개과정을 설명하는 것을 목적으로 한다. 이를 위해 일본 정부 차원의 사이버안보 정책의 기본 구조를 제시하고, 방위성의 사이버안보 정책을 설명한다. 특히, 인력구조 및 부대구조의 변화라는 두 측면에서 사이버안보 정책의 변화를 추적하고자 한다. 그리고 일본이 미일동맹의 틀에서 미국과 사이버안보 협력을 추진하는 동향을 언급한다. 이를 토대로 결론 및 시사점을 도출한다.

3) 일본은 육·해·공 영역에 더해 우주·사이버·전자기 영역을 통합하는 다차원통합방위력(多次元統合防衛力)의 구축을 추진하고 있다. 「平成 31 年度以降に係る防衛計画の大綱について」(2018.12.18.) 〈https://www.mod.go.jp/j/policy/agenda/guideline/2019/pdf/20181218.pdf〉

II. 일본 사이버안보 정책의 기본 구조

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.[4] 입법의 배경은 사이버안보에 관한 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.

이러한 법제 마련과 조직개편을 바탕으로 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 15/9/4). 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. 이를 위해 정보의 자유로운 유통 확보, 법의 지배, 개방성, 자율성, 다양한 행위자의 연계 등 다섯 가지 기본원칙을 수립했다. 이후 2018년 7월, 2021년 9월 각각 개정하여 총 3번에 걸친 사이버안보 전략서를 발간하고 있다(표 1 참조).[5]

[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

4) 전문은 다음을 참조한다. 「平成二十六年法律第百四号 サイバーセキュリティ基本法」〈https://elaws.e-gov.go.jp/document?lawid=426AC1000000104〉

5) 시기별 사이버안보 전략서 및 관련 자료는 NISC 홈페이지에 게재되어 있다. 〈https://www.nisc.go.jp/policy/jyuyo-bunsho/index.html〉

출처: 공개된 자료를 바탕으로 저자 작성

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.[6] 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), 억지력(抑止力), 상황인식 능력(状況把握力)을 향상시켜야 한다는 보다 구체적인 조치를 담았다. 방어력은 국가를 방어하는 능력, 억지력은 사이버 공격을 억지하는 능력, 상황인식 능력은 사이버 공간의 상황을 파악하는 능력으로 각각 설명했다. 사이버 공간에 대한 국제적 규범이 부재하는 상황에서 사이버 위협을 억제하는 조치가 마련되어야 한다는 인식이 그 배경에 작용했다고 보인다.

그러나 사이버공간에서 공격자를 명확한 근거에 따라 식별하는게 어려우며, 악의적 활동이 이루어져도 이에 대한 증거 확보에도 상당한 시간이 요구된다. 또한, 사이버 공격을 방어하거나 억제하는 활동은 물리적 공간이 아닌 사이공간에서 이루어지기 때문에 이에 대한 성공 여부를 확인하는 게 쉽지 않다. 이러한 한계점에도 불구하고 일본 정부는 전통적 군사개념인 방어와 억제를 사이버안보에 적용해서 그 대응방안을 마련하고자 한다는 점에 주목할 필요가 있다.

그리고 2021년 발간된 전략서를 통해 이러한 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.

[표 2] 사이버안보 전략의 세 가지 핵심축

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

출처: Japan’s Cybersecurity Strategy 2021 Overveiw by NISC, Sep. 28. 2021

사이버 공격은 가시적인 물리적 공격이 아니기 때문에 공격을 받아도 군사적 대응이 어려우며, 공격이 일어나더라도 물리적으로 대응할 것인지에 대한 논란이 남아있다. 그러나 평시이기는 하나 중요 사회기반시설에 대한 사이버 공격이 일어나는 경우 이는 사회국가적 혼란을 야기하게

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

되며, 그러한 공격 주체가 고도의 사이버 능력을 가진 타국군일 경우도 배제하기 어렵다. 또한 사이버 공격을 통해 무력공격에 이르지 않는 형태의 현상 변경을 추구하는 경우도 발생할 수 있다. 이러한 점에서 2021년 전략서는 2018년 전략서와 마찬가지로 방어력, 억지력, 상황파악능력 등 세 가지 능력 강화를 지속해서 추진하는 게 중요하며, 방위성 차원의 구체적인 조치는 2018년 12월에 발표한 「방위계획 대강(防衛計画の大綱)」에 반영되어 있음을 덧붙였다.[7] 이렇듯 사이버안보 전략서의 개정 과정에서 군사적 차원에서의 사이버안보의 중요성이 부각되고 있음을 알 수 있다.

2. 능동적 사이버방어 개념 도입

사이버안보에 대한 군사적 접근은 2022년 12월 일본 기시다 정부가 발간한 「국가안보전략서」에서 '능동적 사이버방어' 개념을 도입하는 정책 방향을 제시하면서 구체화되고 있다. 서론에서 언급했듯이 기시다 정부는 2022년 12월 개정된 「국가안보전략서」에 사이버 공격을 미연에 방지하는 '능동적 사이버 방어(能動的サイバー防御, active cyber defense)'라는 개념을 도입했다(표 3 참조).

이를 통해 사이버 방어에 능동이라는 개념을 추가하고, 평시에도 사이버공간을 감시하고 위협을 식별할 수 있도록 안보정책을 재정비하겠다는 의도를 드러냈다. <표 3>에서 알 수 있듯이 능동적 사이버방어는 위협의 사전 식별을 위한 정보 수집 및 분석이 중요하다고 지적한다. 국가안보전략에서 지향하는 사이버안보가 사이버 공간에서의 자유로운 활동을 위한 방어적 작전에 머물러 있음을 알 수 있다.

이는 능동적 사이버방어가 미국, 영국 등 보복이나 비용 부과에 의한 억제를 강조하면서 공세적 사이버 작전(offensive cyber operations)을 발전시키는 것과는 차이가 있다.[8] 공세적 사이버 작전은 평시에도 상대의 네트워크 시스템에 접근해서 수행하는 작전이지만 사이버 공격을 포함하는 공격 작전과는 다르다. 그러나 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.

7) 「平成 31 年度以降に係る防衛計画の大綱について」(2018.12.18.)<https://www.mod.go.jp/j/policy/agenda/guideline/2019/pdf/20181218.pdf>

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

[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 정에 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:「国家安全保障戦略について」(2022.12.16.)

따라서 공세적 사이버 작전이 근미래 군사작전을 위해 지속적으로 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.

그렇다면 일본이 능동적 사이버방어라는 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 사이버방어에 반격 능력을 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.

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. 2024년 6월부터 능동적 사이버방어 법제 준비를 위한 전문가 회의(有職者会議)가 개최되고 있으며, 각계 전문가 17인이 참석한다. 일본 정부는 회의 개최를 통해 전문가 의견을 수렴하고 이를 참고로 입법을 추진한다는 입장이다. 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 된

다.

따라서 일본 정부는 사이버 공간을 상시 감시하면서 정보를 수집하는 과정에서 무력공격의 범위에는 들어가지 않으나 정부기관이나 중요 사회기반시설에 대한 공격 징후가 있는 경우에 그 피해를 방지할 수 있는 조치가 중요하다고 본다. 즉, 능동적 사이버 방어는 평시와 유사의 경계에 있는 회색지대에서 벌어지는 사이버 공격에 대한 조치를 포함하는 광의의 개념이라고 볼 수 있다.

III. 방위성의 사이버안보 정책

일본 방위성은 2022년 12월 「국가안보전략서」을 반영한 방위성 차원의 국방전략을 제시한 「국가방위전략서(国家防衛戦略)」를 발간했다(防衛省 22/12/16). 「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 대응느역을 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: 「国家防衛戦略について」(2022.12.16.)

유사하게 「2024 방위백서」는 사이버안보 분야에서 능동적 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.[9] 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

9) 사이버 공격이란 정보통신 네트워크 및 정보체계를 악용하여 사이버 공간을 경유해서 이루어지는 불법침입, 정보의 절취/변조/파괴, 정보체계의 운영정지 및 오작동, 불법 프로그램 실행 및 DDos 공격 등을 일컫는다. 防衛省. “サイバー領域での対応,”『令和5年版防衛白書』(2023)

주도하에 정부 차원의 사이버안보 역량을 강화하는데 맞춰 방위성과 자위대도 능동적 사이버방어 도입을 위한 종합적 대책을 수립한다고 강조한다.

지난 10여 년간 기술혁신으로 인공지능, 양자기술, 차세대 정보통신기술 등과 같은 첨단기술이 연구·개발되고 있으며, 소위 게임체인저라고 불리는 이러한 기술이 군사분야에 적용되고 있다. 방위성은 이러한 신기술의 군사적 활용이 사이버 공간에서 위험을 높일 수 있다고 지적한다. 예를 들어 중요 사회기반시설에 대한 사이버 공격은 단순한 물리적 군사력의 사용이 아니기 때문에 물리적 대응이 어려운 애매한 상황에 직면하게 될 가능성이 크기 때문이다.

방위성이 2022년 12월 발표한 「2023-2027 방위력정비계획(防衛力整備計画)」은 자위대가 사이버안보를 강화하기 위한 중기 계획을 구체화하고 있다.[10] 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 미일동맹 협력 차원에서도 사이버안보는 확보할 필요가 있다고 본다. 종합하면 방위성의 사이버안보 정책은 체제 개편, 네트워크 시스템 강화, 군내외 연구 및 교육 강화, 민간 및 해외와의 연계 등 네 가지 방향으로 추진되는데 크게 아래와 같이 두 분야가 중심이 된다.

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 육자대는 시스템방호부대(システム防護隊), 해자대는 안전감사부대(安全監査隊), 항자대는 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.

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 3월에는 육자대 통신학교가 시스템통신·사이버 학교(陸自システム通信·サイバー学校)로 개편되었다. 가나가와현 요코스가시에 이치한 시스템통신·사이버 학교는 130명 규모의 전문인력을 교육하고, 2023년 12월 요코스가 연구공원에 설립된 사이버안보인재기반협회(サイバー安全保障人材基盤協会)와의 협력도 강화하고자 한다(朝日新聞 24/4/1). 덧붙여 방위대학교의 정보공학과는 사이버·정보공학과로 개편해서 전문인력 교육을 추진한다.

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. 군 차원에서는 자위대에 사이버안보 관련 교육기관을 보유하고 있고 이를 충분히 활용해서 사이버인력 마련이 가능할 것

10) 「防衛力整備計画について」(2022.12.16.)<https://www.mod.go.jp/j/policy/agenda/guideline/plan/pdf/plan.pdf>

으로 보았다. 다만, 민간 분야에서의 인재 도입 및 육성은 여전히 과제로 남아있다.

이미 방위성은 「2023-2027 방위력정비계획」을 통해 사이버안보 전문인력을 중점적으로 마련하겠다고 밝혔다. 구체적으로 2027년까지 사이버안보 전문인력풀을 약 2만명 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).

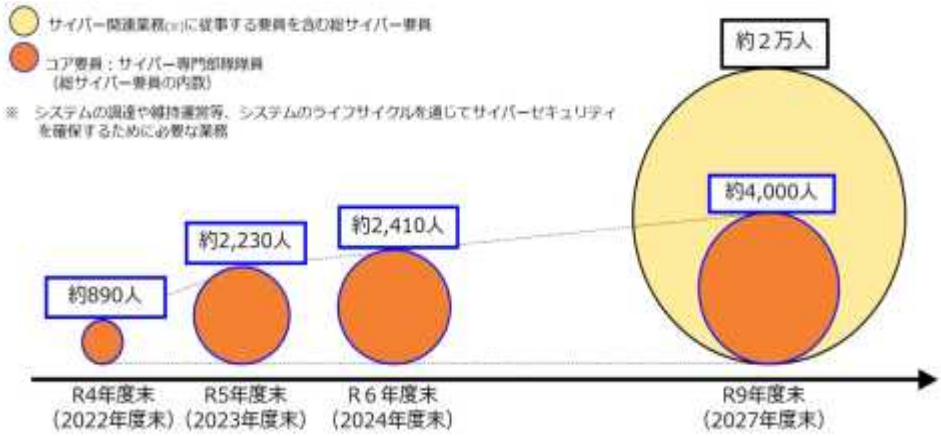
[표 5] 방위성 사이버인재 종합전략서 목차

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: 「防衛省サイバー人材総合戦略」(2024.7.)

<그림 1>은 방위성이 추진하는 사이버 분야 인력확충(안)이다. 주황색 원은 사이버 전문 부대원을 나타내며 노란색 원은 사이버 분야 관련한 전체 인원을 나타낸다. 사이버 전문 부대원은 2022년 890명, 2023년 2,230명, 2024년 2,410명이 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.

[그림 1] 인력확충(안)



출처: 防衛省.「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」(2023.8.31.)

나아가 방위성은 사이버안보 분야의 민간 인력 채용(サイバー自衛官)도 추진하고 있다. 자위대 내 민간인력은 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 23/5/12).

Ⅳ. 사이버안보의 미일 협력

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. 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).

[표 6] 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: 일본 외무성 홈페이지 게시 자료

구체적인 내용은 밝히지 않았지만, 미일 양국은 악의적 사이버 활동에 대한 위협을 인식하고 사이버 공간에 국제법이 적용됨을 확인했다. 나아가 미일 안보조약 5조에서 규정하는 무력 공격의 대상에 사이버 공격이 포함될 수 있음을 처음으로 언급했다. 미일 안보조약 5조는 미국의 일본 방어 의무를 규정하고 있는데, 사이버 분야가 안보조약 5조의 범위에 포함될 가능성을 열어둔 것이다. 따라서 물리적 영토 뿐만 아니라 사이버 공간에 대한 방어 의무 확대는 미일동맹 차

원을 넘어 지역 안보에 있어서도 시사하는 바가 크다. 다만, 어떤 종류의 사이버 공격이 무력 대응이 필요한지는 명시하지 않았으나, 사례별로 미일 간 협의를 진행할 것으로 보인다. 최근 2024년 4월 일본 기시다 총리와 미국 바이든 대통령과의 정상회담에서 사이버안보가 언급되기도 했는데 정보 및 사이버안보 분야에서 협력을 심화한다고 밝혔다.

미일 간 사이버안보 협력이 본격적으로 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).

V. 결론

이상 일본 방위성의 사이버안보 정책을 살펴보았다. 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 두 가지이다. 첫째, '능동적 사이버 방어'에 대한 이해이다. 일본 정부가 능동적 사이버 방어를 갖춘다고 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 2024년 가을 임시국회 개정에 맞춰 사이버 방어법 추진을 위한 전문가 회의를 5월부터 개최할 예정이라고 밝히고 있으며, 자민당은 경제안보추진본부, 디지털사회추진본부, 안전보장조사회가 합동회의를 개최하고 법안 마련을 위한 협의를 진행하기 시작했다(産経新聞 24/5/13).

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 24/5/17).

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 일본 방위성의 전략이 어떠한 방향으로 전개될지 유심히 살펴볼 필요가 있다.

둘째, 미일 협력의 발전 가능성이다. 미일 양국은 안보조약 5조의 범위에 사이버 공격이 포함될 수 있다는 점을 협의했다. 다만, 현재의 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-일

본-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〉

内閣官房. 2022.「国家安全保障戦略について」(2022.12.16.)
〈https://www.mod.go.jp/j/policy/agenda/guideline/pdf/security_strategy.pdf〉
「国家防衛戦略について」(2022.12.16.)〈https://www.mod.go.jp/j/policy/agenda/guideline/strategy/pdf/strategy.pdf〉
「サイバーセキュリティ戦略」(平成27年９月４日)〈https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku.pdf〉
「平成 31 年度以降に係る防衛計画の大綱について」(2018.12.18.)
〈https://www.mod.go.jp/j/policy/agenda/guideline/2019/pdf/20181218.pdf〉
「平成二十六年法律第百四号
サイバーセキュリティ基本法」〈https://elaws.e-gov.go.jp/document?lawid=426AC1000000104〉
「防衛力整備計画について」(2022.12.16.)〈https://www.mod.go.jp/j/policy/agenda/guideline/plan/pdf/plan.pdf〉
「防衛省サイバー人材総合戦略」(2024.7.)〈https://www.mod.go.jp/j/press/news/2024/07/02a_05.pdf〉

防衛省.「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」(2023.8.31.)
防衛省.『令和6年度防衛白書』(2024)

이 글의 내용은 필자 개인의 견해이며
한국사이버안보학회의 공식 입장이 아닙니다.