국가전략연구위원회 이슈브리핑 6호 (발간일: 2023.06.19.)

일본 방위성의 사이버안보 정책과 미일협력[1)]

조은일 (한국국방연구원)

1. 일본 사이버안보(サイバーセキュリティ) 정책의 배경

최근 일본의 사이버안보 정책은 사이버 공간에 대한 새로운 이해로부터 구성되고 있다. 첫째, 사이버 공간이 자유로운 공간인지, 규제의 대상이 공간인지에 대한 대립이다. 일본은 여타 선진국과 마찬가지로 사이버 공간을 자유로운 공간으로 이해하나, 중국, 러시아 등은 사이버 공간에도 정부의 규제와 관리가 필요하다고 본다. 둘째, 사이버 공간이 민간의 영역인지 군사의 영역인지에 대한 구분이다. 사이버 공간은 정보통신기술(ICT)의 발달로 인해 활용 가능해진 영역이다. 그리고 그러한 사이버 공간에서의 민간 행위자의 역할은 중요했다. 한편 사이버 공격과 같은 위협의 등장은 사이버 공간을 단순한 민간의 영역이 아닌 군사의 영역으로 확장하고 있다. 그간 육·해·공을 주요한 전장으로 여겼던 군사에서 이제 우주·사이버·전자기 영역을 새로운 영역으로 확장하면서 다영역(multi-domain)에 걸친 군사작전을 수립하고 있는 상황이 이를 뒷받침한다. 예컨대 일본은 육·해·공 영역에 더해 우주·사이버·전자기 영역을 통합하는 다차원통합방위력(多次元統合防衛力)의 구축을 추진하고 있다.

이렇게 정부 차원의 사이버안보에 대한 이해가 발전하는 만큼 군에 있어서 사이버 공간에 대한 이해도 구체화되고 있다. 군은 ICT의 발달을 지휘통제(C2) 체계에 적극적으로 반영하고 있으며 여기에 일본 방위성과 자위대도 예외가 아니다. 문제는 C2에 있어 ICT에 의

1) 이 글은 2023년 6월 13일 제2차 국가전략포럼에서 발표된 발표문을 수정보완한 것이다.

존도가 높아지는 만큼 사이버 공격으로부터의 취약성이 높아진다는 데 있다. 최근에는 사이버 공격이 저비용의 비대칭적 공격수단으로 활용되고 있기 때문에 이에 대한 취약성을 어떻게 극복할지가 중요한 과제가 되고 있다. 일본의 경우 중국, 북한, 러시아의 사이버 공간의 악용이나 공격 등에 주목하면서 이에 대한 대응 방안을 모색하고 있다. 예를 들어 방위산업청은 방산업체에 엄격한 사이버안보 기준을 도입했다. 2022년 4월 방산 사이버안보 기준(防衛産業サイバーセキュリティ基準)을 제정하고 2023년 4월부터 적용하고 있다. 이는 사이버 공격을 받은 이후 대응 단계를 강화하는 것으로, 미국이 도입한 NIST SP800-171과 유사한 형태라고 알려졌다.[2)]

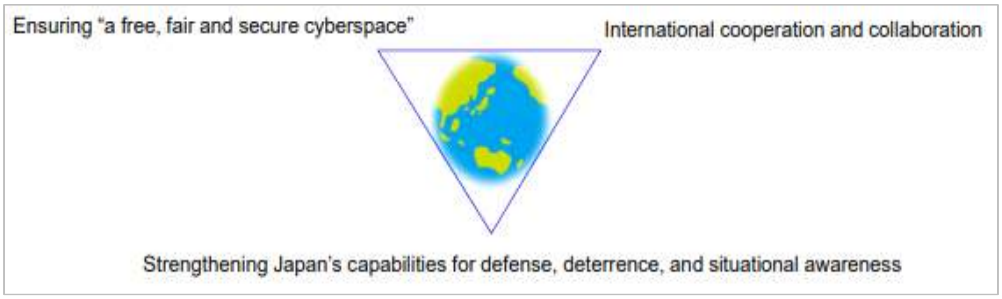
2. 일본 사이버안보 정책의 기본 구조

일본 정부는 2014년 11월 사이버안보 기본법(サイバーセキュリティ基本法)을 제정했다. 이어 2015년 1월 내각에 사이버안보 전략본부를 두고 내각관방에 사이버안보센터(NISC, National center of Incident readiness and Strategy for Cybersecurity)를 설치했다. 그리고 2015년 9월 범정부 차원의 사이버안보 전략을 담은 사이버안보 전략서(サイバーセキュリティ戦略)를 발간했다. 이후 2018년 7월, 2021년 9월 각각 개정하여 총 3번에 걸친 사이버안보 전략서를 발간하고 있다.[3)] 사이버안보 전략서에 따른 일본 정부의 기본 입장은 '자유롭고 공정하며 안전한 사이버 공간의 확보'에 중점을 두고 있다.

사이버안보 전략서에 제기된 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 기조하에 동맹 및 유사입장국과의 협력이 중요하다고 덧붙였다. 2018년 전략서는 이전 전략서의 기본 기조를 유지하면서도 사이버 공간의 안전을 확보하기 위해서 사이버 공격에 대응하는 방어력, 억지력, 상황파악능력을 향상시켜야 한다는 보다 구체적인 조치를 담았다. 방어력은 국가를 방어하는 능력, 억지력은 사이버 공격을 억지하는 능력, 상황파악능력은 사이버 공간의 상황을 파악하는 능력으로 각각 설명했다. 2021년 전략서는 "사이버 공간이 지정학적 긴장을 반영하면서 평시에서부터 국가 간 경쟁의 공간이 되고 있다"라고 지적하면서 사이버안보의 군사적 접근을 강화했다. 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. 이렇듯 사이버안보 전략서의 개정 과정에서 군사적 차원에서의 사이버안보의 중요성이 부각되었다.

2) 防衛産業サイバーセキュリティ基準の整備について.
(https://www.mod.go.jp/atla/cybersecurity.html)
3) 시기별 사이버안보 전략서 및 관련 자료는 NISC 홈페이지에 게재되어 있음
(https://www.nisc.go.jp/policy/jyuyo-bunsho/index.html)

<그림 1> 일본의 사이버안보 전략 2021



출처: Japan's Cybersecurity Strategy 2021 Overview by NISC, Sep. 28. 2021

3. 방위성의 사이버안보 정책

방위백서에 따르면 일본 방위성의 사이버안보 정책은 사이버 공격으로 자위대의 활동에 피해가 발생하는 경우와 그 대응에 중점이 맞춰져 있다. 2022년 방위백서는 사이버 공격 대응의 6가지 방향을 다음과 같이 제시했다. 첫째, 정보체계의 안전성 확보이다. 외부의 공격으로부터 방위정보통신기반(DII)을 방어한다. 둘째, 사이버 공격에 대응하는 전문부대 편성이다. 셋째, 사이버 공격 대응 태세의 확보 및 정비이다. 넷째, AI 기술 등을 활용한 최신기술의 연구이다. 다섯째, 국외기관 연수 등 인재 육성이다. 여섯째, 미군, NATO 등 국제협력이다.

2022년 12월 개정된 국가안보전략서(国家安全保障戦略)는 사이버 공격을 미연에 방지하는 "능동적 사이버 방어(能動的サイバー防御, active cyber defense)"라는 개념을 도입했다. 이는 사이버안보가 단순히 시스템에 대한 침략을 방어한다는 의미에 머무는 게 아니라 상대의 공격 징후를 탐지하고 파악해서 사전에 무력화하는 반격을 위한 능력도 포함하는 것을 의미한다는 데 있다.

국가방위전략서(国家防衛戦略)에도 방위성 차원의 사이버안보 정책 기조가 제시되었다. 국가방위전략서는 방위력의 근본적인 강화를 위해서 육·해·공 영역과 우주·사이버·전자기 영역을 통합적으로 운용하는 다차원통합방위력 구축의 관점에서 사이버안보를 강조했다. 사이버 영역은 평시에서 유사에 이르는 모든 분쟁 단계에 있어 정보를 수집하고 공유하는 데 핵심적이기 때문이다.

2023-2027 방위력정비계획(防衛力整備計画)은 자위대가 사이버안보를 강화하기 위한 중기 계획을 구체화했다. 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. 나아

가 자위대 운용에 있어 사이버 공간에 대한 의존도가 높아지는 만큼 미일 동맹 협력 차원에서도 사이버안보는 확보할 필요가 있다고 본다.

그러한 관점에서 2027년까지 C2 능력 및 방위장비품을 안전하게 관리할 수 있도록 방산업체에 대한 사이버 방어도 지원할 예정이다. 자위대는 사이버 공격을 받는 상황에서도 C2, 전투, 작전수행이 가능한 태세를 유지하도록 태세를 갖추고자 한다. 이를 위한 구체적 추진사업으로 항시 리스크 평가를 수행하고 안보대책을 수립하는 체계를 갖추는데 2,000억 엔, 클라우드 기반 정비에 4,000억 엔, 사이버 방호기재의 기능 강화에 3,000억 엔, 사이버안보 요원 육성 및 연구기반 강화에 300억 엔을 투입할 예정이다.

인력에서도 2027년까지 사이버안보 전문인력풀을 약 2만 명을 확보하고 그중 사이버부대에 4,000명을 편성할 예정이다. 이는 2022년 말 890명 규모의 약 4배가 되는 것으로 인재 육성과 확보가 중요한 과제임을 알 수 있다. 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. 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. 또한, 가나가와현 요코스가시에 위치한 육자대 통신학교를 육자대 시스템통신·사이버 학교(陸自システム通信・サイバー学校)로 개편하여 전문인력에 대한 교육도 추진할 예정이다.

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.[4)]

4. 사이버안보의 미일 협력

일본이 2018 방위계획 대강에서 사이버 분야를 대응이 필요한 신영역으로 강조하면서, 2019년 미일 2+2회의에서 사이버 분야에 대한 새로운 협의가 진행되었다. 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. 어떤 종류의 사이버 공격이 무력 대응이 필요한지는 명시하지 않았으나, 사례별로 미일 간 협의를 진행할 것으로 보인다.

4) "自衛隊に民間サイバー人材政府、24年にも初採用."『日本経済新聞』(2023年5月12日).

방위성은 2013년 8월 미일국방장관 회담의 합의에 따라 미국과 사이버국방정책 워킹그룹(Cyber Defense Policy Working Group)을 운영하고 있으며, 2014년부터 연 1~2회 정도 개최해오고 있다. 2022년 5월을 기준으로 총 8회의 회의를 개최했으며 2015년 회의에서 공동선언을 발표하기도 했다. 이와 더불어 미일 사이버대화(Cyber Dialogue), 미일 IT 포럼 등도 개최되고 있다.

5. 시사점

위에서 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. 능동적 방어는 어디까지나 방어적 역량에 초점이 맞춰져 있는 만큼 이에 대한 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. 이는 미일 동맹 차원을 넘어 지역 안보에도 중요한 함의를 지닐 수 있다는 점에 유의해야 할 필요가 있다.