국가전략연구위원회 이슈브리핑 4호 (발간일: 2023.06.19.)

일본 사이버안보 정책의 범정부적 정책 대응 변화[1)]

이정환 (서울대학교)

1. 서론

일본 정부의 사이버안보 정책에 대한 글로벌 평가는 긍정적이다. 대표적으로 유엔의 전문기구인 국제전기통신연합(International Telecommunication Union, ITU)이 가장 최근 발간한 Global Cybersecurity Index 2020에서 일본은 100점 만점에 97.82점으로 194개 평가 대상 국가 중에 7위였다.[2)] 하지만, 일본 내에서는 일본 정부의 사이버안보 정책에 대한 불안한 시선이 지속되고 있다. 마쓰무라 마사히로(松村昌廣) 교수가 소개하듯이 일본 내 여러 사이버안보 정책 전문가들은 일본의 사이버안보 정책이 사이버공간의 안보 위협에 대응하기에 부족하다는 인식을 공유하고 있다.[3)]

일본 사이버안보 정책에 대한 이런 상반된 평가는 전통적 의미의 사이버시큐리티 대응에 대한 평가와 안보정책으로서의 사이버안보 정책에 대한 평가가 상이하기 때문이다. 일본의 사이버안보 정책은 지난 10여년간 법적 제도적 정비를 지속해왔다. 하지만, 이승주 교수

1) 이 글은 2023년 6월 13일 제2차 국가전략포럼에서 발표된 발표문을 수정보완한 것이다.
2) International Telecommunication Union. *Global Cybersecurity Index 2020.* International Telecommunication Union. 2021. 일본은 실제 12위이다. 미국, 영국, 사우디아라비아, 에스토니아, 한국, 싱가포르, 스페인, 러시아, 아랍에미리트, 말레이시아, 리투아니아가 일본보다 상위에 위치한다.
3) 松村昌廣. "我が国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.

의 '사이버안보의 전통 안보화와 전통 안보의 사이버 안보화' 구절로 이해될 수 있는 일본 사이버안보 정책의 변화에서[4], 전통 안보와 연계된 사이버공간의 위협에 대한 안보적 대응의 정부 준비 태세가 부족하다는 관점이 존재한다.

이 글은 일본의 사이버안보 정책의 역사적 흐름 속에서 현재 일본의 사이버안보 정책의 제도와 성격에 대해 정리하고, 현재 일본 정책공간 내에서 논해지고 있는 일본 사이버안보 정책의 한계점에 대해 살펴보고자 한다.

2. 일본 사이버안보 정책의 역사

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.[5] 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.[6]

그러나, 현재 일본 사이버안보 정책의 중심적 조직인 NISC가 2005년 그 전신이 형성되었다곤 하지만, 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.[7]

일본 사이버안보 정책의 핵심 법제인 <사이버시큐리티기본법>은 2013년 <사이버시큐리티전략>의 결과물이라 할 수 있다. 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

4) 이승주. "일본 사이버안보 전략의 변화: 사이버 안보의 전통 안보화와 전통 안보의 사이버 안보화." 『국가안보와 전략』 17.1 (2017): 173-202.
5) 谷脇康彦.『サイバーセキュリティ』. 岩波書店. 2018. kindle location 1418.
6) 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)
7) 谷脇康彦. 위의 글. kindle location 1436.

2005년 NISC가 National Information Security Center의 약자인 것과 비교할 때 전혀 다르다. 2015년 <사이버시큐리티기본법>에 의해 사이버안보에 대한 정책 결정 조직으로 내각에 설치된 「사이버시큐리티전략본부」(본부장 내각관방장관)의 실무조직의 위상으로 「내각사이버시큐리티센터」로 새로 출범하게 된 것이다.[8)]

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 운용상황에 대한 감독 권한도 가지게 되었다. 또한 각 부처의 사이버보안 대응을 종합해서 국가 전체의 사이버안보 정책을 일괄적으로 총괄하는 역할도 담당하게 되었다. 그 결과 2015년부터 3년마다 발행되고 있는 <사이버시큐리티전략> 문서의 작성 주체가 되었다. 위상 강화와 기능 강화 속에서 2013년에 80여 명뿐이었던 NISC 직원 수는 3년 후인 2016년에 180명으로 증가하였다.[9)]

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 정책과제이다. 세 번째가 국제협력인데, 이 부분에서 국제적 사이버공격에 대한 대응과 관련된 '사이버안보의 전통 안보화'의 추세가 발견된다.

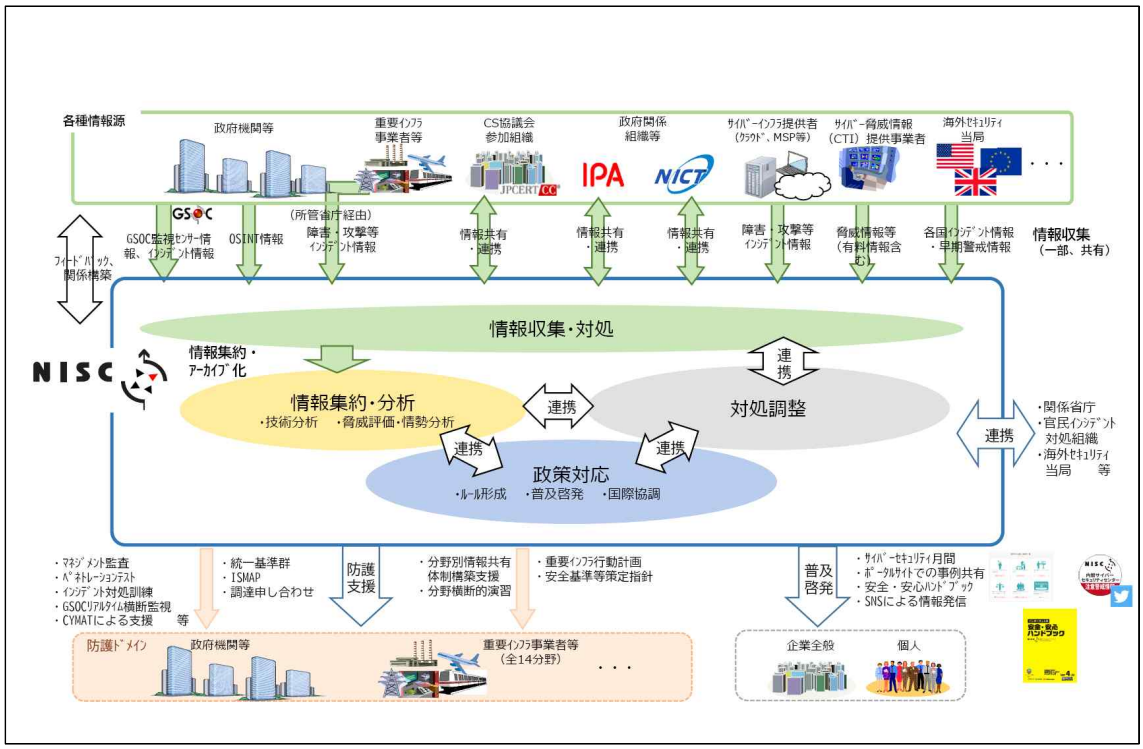
3. 일본 사이버안보 정책의 현행 제도와 특징

현재 일본 사이버안보 정책 내용을 보여주는 2021년 <사이버시큐리티전략>은 2015년판, 2018년판과 비교하였을 때, 민간기업 투자 촉진, 사이버 보안 강화, 국제협력의 세 축에서 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. 사이버 보안 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 역할과 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.

8) 이상현. "일본의 사이버안보 수행체계와 전략." 『국가안보와 전략』 19.1 (2019), pp. 115-154.
9) 谷脇康彦. 위의 글. kindle location 1472.

<그림 1> Cybersecurity for All 조감도



출처: NISC 홈페이지(https://www.nisc.go.jp/about/overview/index.html)

하지만, NISC의 역할 강화에 대해서는 NISC와 기타 성청과의 관계에서 발견되는 거버넌스적 한계를 넘어설 수 있는지에 대한 의구심이 존재한다. 일본 각 행정부처는 각기 담당 정책 영역에서의 사이버안보 정책을 추진하고 있으며, 이에 대한 NISC의 위상은 조언적 위치에서 출발해서 조정자 위치로 발전하였지만, 사이버안보 이슈에 대한 타 행정부처의 상위 기관이 되는 것은 제도적으로도 여의치 않은 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 요인이 될 것이다.

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 예상 가능한 일이지만, 정보의 수집, 분석, 대처에 대한 실제 업무에 있어서 NISC가 주도성을 확립할 수 있는지는 향후 지속적으로 관찰해야 할 부분이다.

4. '사이버 안보의 전통 안보화'의 진전

한편 <사이버시큐리티전략>의 세 정책 내용의 마지막 부분은 사이버안보 정책의 안보 정책화 양상을 잘 드러내 준다. 기본적으로 국경을 넘어서 발생하는 사이버공격이 외부 국가와 연계되어 있는 상황에 대한 대응은 보안의 관점이 아닌 안보정책 차원에서 인식될 수밖에 없다.

하지만, 국경을 넘어서 발생하는 사이버공격에 대해서 어떤 대응을 추구하는지에 대해서 NISC가 발행한 2015년과 2018년 <사이버시큐리티전략>의 기술은 상당히 다르다. 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 연동되어 있는 것으로 의심되는 사이버 공격 사례도 있음을 감안하면 동맹국 및 같은 입장에 서 있는 이른바 유지국·기관 간의 위협 정보 공유나 인재육성 등에서의 협력·연계의 적극적인 추진이 불가결하며, 또한 기타 국가와도 신뢰를 양성해 나가는 것이 중요하다.[10)]

이에 비해 2018년 <사이버시큐리티전략>에서는 사이버공격에 연계된 해외 국가에 대한 대항 조치의 가능성을 명시해서 기술하고 있다.

> 악의적 사이버 공격 등 무력 공격에 이르지 않는 위법 행위에 대해서도 국제위법 행위의 피해자인 국가는 일정한 경우에는 해당 책임이 있는 국가에 대해 균형성 있는 대항 조치 및 기타 합법적인 대응을 취할 수 있다.[11)]

2018년 <사이버시큐리티전략>에서 나타나는 사실상의 적국 개념과 자위권 개념의 확립은 아베 정권기의 <국가안보전략>을 중심으로 하는 위협인식의 강화, 위기 대응에의 탄력적 제도 개편, 다각적 안보 역량 강화의 추세 속에서 설명될 수 있다.[12)] '사이버안보의 전통 안보화' 추세의 배경에 아베 정권기의 적극적 안보정책이 존재하는 것은 부인하기 어렵다. <국가안보전략>은 사이버공간의 방어를 안전보장에서 불가결한 핵심요소로 위치지우고 있다.

---

10) 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)
11) 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)
12) 이상현. "사이버 위협에 대한 일본의 대응: 사이버 외교와 사이버 방위." 『국가전략』 25.2 (2019), pp. 91-117; 박성호. "일본의 사이버 안보전략 - 양자주의의 강화인가 다자주의로의 전환인가?-." 『일본학』 56 (2022), pp. 159-182.

하지만, 사이버공격에 대한 자위 대응을 명시하는 2018년 <사이버시큐리티전략>의 기술은 일본 내부의 안보정책 맥락만으로 설명되지 않는다. 더불어, 2010년대에 진전되어 온 사이버공간에 대한 국제규범 논의가 일본의 사이버안보에 대한 적극적 개념 부여와 높은 연계성을 지닌다. 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. 사이버공간에서의 위법 행위의 주체 특정에서 미국 중심의 선진국이 가지는 강력한 영향력에 대한 부담감이 그 배경이 된다.[13)]

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.[14)]

2018년 <사이버시큐리티전략>에서 적극적인 자위 행사 기술이 드러난 것은 이러한 국제규범 논의의 맥락에서 이해될 수 있다. 2021년 <사이버시큐리티전략>에서는 사이버공간에서의 자위권에 대한 기술이 보다 명료하게 기술되어 있다.

> 사이버공간에서의 국가에 의한 국제 위법 행위는 해당 국가의 국가책임을 수반하며, 피해자인 국가는 일정한 경우 해당 책임이 있는 국가에 대해 균형성 있는 대항 조치 및 기타 합법적인 대응을 취할 수 있다. 사이버 공격은 또한 일정한 경우 국제법상 무력을 사용하거나 무력 공격이 될 수 있다.[15)]

사이버공간에 대한 자위권 행사에 대한 명쾌한 기술로의 변화는 미국을 비롯한 선진국이 적극적 억지 입장에 서서 정책을 전개하는 가운데, 일본도 동화되는 상황으로 볼 수도 있다.

5. '사이버 안보의 전통 안보화'의 한계

2021년 <사이버시큐리티전략>에서 자위권 행사가 가능하다고 분명하게 기술된 것에 비해서 이에 대응하는 일본의 자체적 억지 전략은 구체적으로 드러나 있지 않다. <사이버시

13) 谷脇康彦. 위의 글. kindle location 1698.
14) 谷脇康彦. 위의 글. kindle location 1768.
15) サイバーセキュリティ戦略 (2021년), p. 32
(https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021.pdf)

큐리티전략>에서 외국의 사이버공간에서의 위법 행위에 대한 대응 방법의 핵심 내용은 미일협력이다. 미일협력이 가장 효과적인 수단이기 때문이라고 해석할 수 있으나, 일본 단독으로 사이버공간에서 외국의 위법 행위에 대한 대응의 헌법상의 해석 문제로 파악할 수도 있다. 일본 헌법 9조에 대한 최근의 적극적 해석 변경과는 별개로, 일본은 9조의 취지에 따른 전수방위 원칙을 버리지 않고 있다. 전수방위 원칙과 실질적으로 위배되는 것이 아닌가로 의심되는 반격능력 보유도 전수방위 원칙과 부합하는 것으로 설정하여 정당화하고 있다. 문제는 사이버공간에서의 무력행위에 대한 효과적 억지 방법이 거부적 억지(적극 방위)가 아니라 징벌적 억지 (보복능력보유)라는 점에 있다. 사이버공간에서 징벌적 억지 능력은 사이버공간에서의 잠재적 적에 대한 취약점 파악과 선제적 사이버 공격 능력 보유라 할 수 있는데, 이 점은 아직 일본의 헌법 해석에서 가능하다고 보기 어렵다.[16] 전통 안보 이슈에 비해 사이버안보 분야가 일본의 전수방위 원칙의 해석 변용에 있어 더 어려움이 있다는 관점이 일본 내에 공유되고 있다. 미래에, 미사일방위를 위한 공격형 미사일 보유가 전수방위 원칙에 부합하는 것으로 재해석하는 2022년 일본의 안보정책 변화와 같은 일이 사이버안보 정책에서도 일어날 수 있다. 사이버공간에서의 징벌적 억지 능력 보유와 행사의 법적 근거를 확보하기 위한 지적 곡예가 발생할 수도 있음을 전망케 한다.

일본의 사이버안보 정책의 또 다른 과제는 NISC와 방위성·자위대와의 역할 분담 과제이다. 방위성·자위대는 '전통 안보의 사이버 안보화'의 대응 관점에서 사이버안보 정책을 추진하고 있다고 볼 수 있으며, 2022년 일본 방위3문서에서 드러난 일본 정부의 우주, 사이버, 전자파 영역에서의 방위 능력 강화에 대한 집중 투자 계획은 장기적으로 일본의 방위 능력에서 사이버 대응 능력의 신장을 예상케 한다. 문제는 방위성·자위대가 대응해야 하는 사이버안보 사안과 NISC가 대응해야 하는 사이버안보 사안이 구분되기 쉽지 않다는 점이다. 보안 이슈와 안보 이슈 사이의 그레이존에 대해 NISC와 방위성·자위대가 어떻게 업무 분담 및 협조 체계를 가져야 하는지에 대한 계획이 불투명하다. 미국의 CISA(Cybersecurity and Infrastructure Security Agency)와 Cyber Command 사이의 관계에서도 이 부분은 명확하지 않은 점이 존재한다. 이는 그레이존에 대응하는 거버넌스 구축 과제는 사이버안보와 관련된 보편적 사항이라는 점을 보여준다. 하지만, 일본의 NISC는 미국의 CISA에 비해서 제도적 권한 자체가 약하다. 즉 미국이 사이버안보에 대한 두 기관의 협조 체제 구축 과제를 가지고 있다면, 일본은 자위대 사이버방위대의 파트너를 새롭게 구축하기 위한 제도 개편 노력부터 선행되어야 할 것으로 보인다.

6. 맺음말

일본의 사이버안보 정책체계에는 다른 국가 사례와 마찬가지로 그레이존에 대응하기 위한 거버넌스 확립의 고민이 존재한다. 이러한 사이버안보 정책의 일반적 과제와는 별개로

16) 松村昌廣. 위의 글, p. 83.

일본에게는 평화헌법의 전수방위 원칙과 효율적 사이버안보 대응책 마련 사이의 딜레마라는 독특한 고려 사항이 있다. 일본의 사이버안보 정책의 향방은 사이버안보 정책의 일반적 과제에 대한 대응과 일본의 독특한 법적 과제에 대한 대응을 얼마나 종합적으로 잘 대처해내는지에 달려 있다.

일본 정부가 현재 방점을 찍고 있는 해법은 미일협력이다. 하지만, 미국에 대한 의존성 강화에 대한 일본 내부의 고민도 상당하다.[17] 이 부분의 고민이 일본 사이버안보 정책의 미래에서 어떤 영향을 줄지도 살펴보아야 할 것이다. 국제협력과 자주의 두 원칙 사이의 길항 또한 일본 사이버안보 정책체계 논의에 대한 관찰에서 주목되어야 할 사항으로 보인다.

17) 松村昌廣. 위의 글, p. 93.