국가전략연구위원회 이슈브리핑 40호 (발간일: 2025. 12. 8.)

트럼프의 사이버 전략과 일본의 사이버 안보
– 미일동맹과 사이버 안보를 통한 보통국가화

임은정 (국립공주대학교 국제학부 교수)

I. 들어가며

2025년 현재 국가안보를 둘러싼 두드러진 변화 중 하나는 전통적 군사력과 디지털 인프라가 서로를 지탱하는 방식으로 결합하면서, 전장(戰場)의 경계와 안보를 위한 규범 및 제도가 빠르게 재구성되고 있다는 점일 것이다. 이는 전력망, 금융결제 시스템, 항공·철도 교통과 같은 중요 기반시설은 물론, 정부의 지휘통제와 정보·감시·정찰 기능까지도 정보통신기술(Information and Communications Technology, ICT)에 폭넓게 의존하게 되면서 사이버 공간에서 발생한 작은 취약성이 물리적 세계로 급속히 전이되는 현상, 다시 말해 신흥 안보(emerging security)의 이론적 틀에서 '창발(創發, emergence)'로 표현되는 복합적 상호작용[1]이 더 이상 예외적인 상황에서만 발생하는 것이 아니게 되었기 때문이다.

특히 3년 이상 계속되고 있는 러시아-우크라이나 전쟁을 통해 하이브리드 전쟁이 본격적으로 전개되었고, 미국과 중국 사이의 전략경쟁이 미래 기술·사이버·데이터·AI 영역으로 확장되다 보니, 전통적 군사 능력만으로는 국가안보를 담보할 수 없는 시대가 도래하였다는 것을 전 세계가 실감하게 되었다. 이러한 환경 속에서

1) 김상배, 「신흥안보와 메타 거버넌스: 새로운 안보 패러다임의 이론적 이해」, 『한국정치학회보』 50권 1호 (2016), pp. 75-104.

일본은 전통적인 안보 구조의 제약, 특히 평화헌법과 전수방위(專守防衛)를 근간으로 하는 방위 정책 체계를 전면적으로 수정하지는 못하면서도, 점점 더 복잡해지는 신흥안보 위협에 대응하기 위해 새로운 전략적 접근을 모색해 왔다. 이러한 맥락과 궤를 같이하며 사이버 안보는 일본에서 단순히 기술 정책적 차원에서가 아니라 국가 정체성과 동맹 전략, 보수 정치세력의 역할 인식마저 결합된 복합적 전략 영역으로 다뤄지고 있다.

일본의 사이버 안보 전략은 아베 2기 정부 이후 점진적으로 '전통 안보화'[2]의 경로를 밟으며 군사적 억지 개념을 흡수하였고, 기시다 정부에서 제도적으로 성숙하였으며, 다카이치 내각 출범 이후에는 더욱 공세적인 혁신을 향해 정책적 변화가 속도감 있게 추진 되리라 전망된다. 본고는 이러한 일본의 점진적이지만 확실한 변화가 단순히 외부로부터의 압력이나 환경적 요인에 대한 '반응적(reactive)'[3] 차원에서만 형성된 것이 아니라, 미국의 사이버 전략이 공세적으로 변화하는 흐름을 마치 '유도와 같은(Judo-like)' 방식으로[4] 전략적으로 활용한 결과라고 주장코자 한다. 특히 트럼프 행정부 출범 이후 미국의 사이버 전략이 억지와 방어 중심의 기존 프레임을 넘어 적극적 개입과 사전 무력화 개념을 강화하는 방향으로 나아감에 따라 일본 역시 이를 기존에 제한적이었던 안보 역할을 확장하는 기회로 활용하고 있음을 밝히고자 하는 것이다. 일본 보수 정치세력이 오랫동안 추진해 온 이른바 보통국가화(normalization of state)는 외부 변화와 결합하며 이전보다 훨씬 낮은 정치적 비용 속에서 실질적 진전을 이루어내고 있다고 볼 수 있는데, 미일동맹과 함께 또 한 축을 이루고 있는 것이 사이버 안보라고 볼 수 있다.

그러나 일본의 사이버 안보 전략은 단순한 직선적 성장이나 일관된 강화로만 설명하기 어려운 측면도 있다. 규범에 기반한 외교와 다자주의적 국제협력을 강조해 온 일본의 외교적 정체성과 사이버 영역에서의 공세적 전략은 본질적으로 서로 충돌할 가능성을 내포한다. 더불어 일본 사회 디지털 기반의 취약성, 민간과 정부 간 협력의 어려움, 사이버 인력의 만성적 부족 등은 일본이 공세적 능력을 표방하는 데 있어 구조적 한계를 부여한다. 그럼에도 불구하고 일본 보수 정치세력은 사이버 안보 영역을 새로운 일상적 안보의 장으로 활용하려는 방향성을 더욱 강화하고 있으며, 미일동맹에서의 역할 변화를 명분으로 이러한 정책적 방향성에 정당성을 부여하고 있다.

본고는 트럼프 행정부의 공세적 사이버 전략을 일본이 어떻게 전략적 자원으로 전유했는지를 규명함으로써, 일본 보수 정치세력의 보통국가화와 신흥 안보의 결합을 분석한다. 일본의 사이버 안보 전략이 보수 정치의 연속성 속에서 어떻게 변모해 왔는지를 분석함으로써 사이버 안보가 국가의 전략적 선택에 있어 핵심 영역으

2) 이승주, 「일본 사이버 안보 전략의 변화」, 『국가안보와 전략』 17권 1호 (2017), pp. 173-202.
3) Kent E. Calder, "Japanese Foreign Economic Policy Formation: Explaining the Reactive State," *World Politics*, vol. 40, no. 4 (1988), pp. 517-541.
4) Eunjung Lim, "Characterizing Japan's Current Diplomacy under Abe," *The Korean Journal of Security Affairs*, vol. 14, iss. 2 (2019), pp. 96-119.

로 정착하는 과정을 조명할 것이다.

II. 선행 연구 검토: 일본 사이버 전략을 이해하는 틀

일본 사이버 안보 정책의 변화를 분석하기에 앞서 관련된 주요 선행 연구들이 주장하고 있는 바를 우선 정리하고자 한다. 이승주는 일본이 사이버 위협을 군사 안보 수준의 위협으로 인식하기 시작한 것에 주목하면서, 이에 따라 사이버 안보 정책을 전통 안보 체계에 흡수시키는 과정에 대해 해설하였다. 그는 일본이 미일동맹 강화, 중국 견제, 보통국가화와 같은 전통적 군사 안보 측면에서의 목표를 위해 사이버 안보를 전략적 수단으로 활용하고 있다고 분석하면서도, 동시에 일본의 사이버 안보 전략은 국제협력 강조, 특히 미국 및 아세안 국가들과의 협력을 통해 중국 견제와 규범 설정을 추구하는 측면이 있다고 평가하였다.[5)]

이상현은 일본이 사이버 위협을 국가안보의 핵심 문제로 규정하고, 법·제도·군사·외교 전 부문을 동원해 대응 체계를 구축해 온 것에 관해 설명하였는데, 그는 미일동맹의 사이버 협력은 일본 전략에서 가장 중요한 축이라고 강조하였다. 그러나 국내 인프라 취약성, 인재 부족, 민간 영역의 보안 투자 부족 등 구조적 한계도 존재한다는 것이 그의 평가다.[6)]

이정환은 일본 사이버안보 정책이 지난 10년간 법·제도 정비 면에서 크게 발전한 부분을 평가하면서도 안보 정책 차원에서 보면 현행 평화헌법으로 인한 제한적인 측면, 조직 거버넌스 문제, 미국 의존도와 같은 구조적 한계가 뚜렷하기에 향후 일본의 사이버 안보가 이러한 법적·조직적 제약을 극복할 수 있는지가 핵심 관전 요소라고 전망한 바 있다.[7)]

윤대엽은 일본은 디지털 경쟁력은 낮지만 사이버 안보화는 가장 앞서 있다는 점에 주목하며, 이는 일본의 전략문화, 즉 비군사적 요소의 안보화, 안전보장 개념 확대에 기인하는 것이라고 분석했다. 다시 말해 경제·외교 문제도 안보 문제로 담론화하는 경향이 있다는 것인데, 일본의 사이버 전략에는 미국 의존도를 줄이려는 시도도 존재하지만 결국 미일동맹을 통한 억지·방어·공세 전략이 핵심이며, 이를 위해 정부 주도 중앙집권형으로 발전해 왔다고 분석했다.[8)]

한편 신승휴는 일본은 외부로부터 부여되는 역할 기대와 내부적으로 스스로 규정하는 역할 인식 사이에서 선택적 조율을 통해 정책 방향을 결정하는 경향이 있다는 것을 지적했다. 예를 들어, 미국이 화웨이를 제재하는 국면에서 일본이 미국의

5) 이승주 (2017).
6) 이상현, 「사이버 위협에 대한 일본의 대응: 사이버 외교와 사이버 방위」, 『국가전략』 25권 2호 (2019), pp. 91-117.
7) 이정환, "일본 사이버안보 정책의 범정부적 정책 대응 변화," 『국가전략연구위원회 이슈브리핑』 4호 (2023년6월19일).
8) 윤대엽, "일본의 사이버 국가책략과 국제협력," 『국가전략연구위원회 이슈브리핑』 5호 (2023년6월19일).

강한 압력에도 불구하고 전면적 동조 대신 제한적·선택적 대응을 택한 것은 일본 고유의 규범 중심 외교 정체성과 국내 산업 고려가 결합된 결과였다는 것이다. 이와 같은 선택적 수용의 패턴은 일본이 사이버 안보 전략을 전통 안보화하는 과정에서도 그대로 재현되었다는 것이 그의 분석이다.[9]

이상의 선행 연구들은 공통적으로 일본이 사이버 안보라는 신흥 안보 의제를 전통 안보적 관점과 접목하여 미일동맹의 강화, 나아가 보통국가화라는 국가의 전략적 목표를 달성하는 명분으로 삼고 있다고 분석하고 있다. 이러한 공통적 분석은 임은정(Eunjung Lim)이 아베 신조 총리(安倍 晋三) 2기의 외교·안보 정책적 접근을 마치 유도(柔道)와 같다고 한 주장과 연결될 수 있다. 유도는 상대를 타격하지 않으면서도 상대방의 힘을 이용하여 균형을 무너뜨림으로써 넘어뜨리거나 움직이지 못하게 무력화시켜서 제압하는 일본의 전통 무도인데, 아베 정부가 중국의 부상, 북한의 핵·미사일 위협, 미국의 동맹에 대한 압박 등 외부의 힘을 일본의 외교·안보 전략 강화의 명분으로 활용하며 보통국가화의 동력을 축적해 왔다는 것이 그의 주장이다. 자유롭고 열린 인도-태평양(自由で開かれたインド太平洋; Free and Open Indo-Pacific, FOIP) 구상을 천명한 것이나, 세계 지도를 파노라마처럼 조망하는 외교, 평화에의 적극적인 공헌 등은 일대일로 전략을 펼치는 중국을 견제하고 북핵 위협에 대응하기 위해 전면 충돌 보다는 우회적이면서도 질적인 경쟁 전략을 전개한 것이며, 이를 위해 최강대국이자 동맹인 미국 트럼프 행정부의 안보 정책의 변화를 활용한 측면이 있다는 것이 그의 분석이다.[10] 즉 임은정은 일본 외교가 기존의 반응적 외교에서 보다 능동적·전략적 외교로 전환되었으며, 안보·경제·외교를 연계한 입체적 접근을 추구하고, 가치 외교와 전략적 자율성을 동시에 추구하는 경향을 보였다고 평가한 것이다.

결국 상술한 선행 연구들의 분석과 논지를 종합하면, 일본의 사이버 안보에 대한 인식은 대체로 네 가지 축 위에 형성되어 왔다고 볼 수 있다. 첫째, 일본은 FOIP 구상에서 보듯, 데이터의 자유 흐름(Data Free Flow with Trust, DFFT)이나 규범과 법치를 기반으로 하는 국제질서 유지에 기여하는 규범 선도국임을 자임하려 한다. 둘째, 미중 경쟁 심화 속에서도 독자적 기술·경제 전략을 구축하려는 전략적 자율성을 중시한다. 셋째, 미일동맹을 지역 안정을 위한 필수 기반으로 보면서도 단순한 수혜자가 아니라, 능동적으로 기여하는 책임 있는 동맹 파트너를 목표로 한다. 마지막으로, 보수 정치세력이 지속적으로 강조해 온 보통국가화는 전수방위의 제약을 해소하고 국제사회에서 적극적인 역할을 할 수 있는 국가로 인정받기 위한 일본 내부의 구조적 목표로 자리 잡고 있다. 이 네 가지 역할 인식은 일본의 사이버 전략을 해석하는 데에서 핵심적인 분석 기준이 된다고 볼 수 있다.

역할 인식이 정책 선택을 규정하는 내부적 요인이라면, 사이버 안보의 전통 안보화 과정은 일본이 사이버 공간을 해석하는 인식의 틀을 전환시키는 과정이라고

9) 신승휴,「사이버 안보 이슈에 대한 일본의 대응과 아베 정권의 국제적 역할인식 : 역할이론과 존재론적 안보의 시각」,『아세아연구』66권 3호 (2023), pp. 181-214.
10) Eunjung Lim (2019).

볼 수 있다. 일본은 초기에는 사이버 위협을 민간 인프라 보호의 문제로만 다루었으나, 북중 위협 증대와 미일 동맹 내에서의 사이버 협력 필요성이 부상하면서 사이버 공간을 '공격-방어-억지'가 가능한 전략 영역으로 재정립하고 있다. 이러한 인식 전환은 일본이 보통국가화를 추구하는 과정에서 사이버 안보 분야가 전통적 군사력 강화와 관련된 의제보다 훨씬 낮은 정치적 비용을 필요로 한다는 점에서 정치권에도 매우 매력적이면서도 효율적인 선택지로 인식되었으리라 추정한다.

다음에서는 일본의 사이버 안보 전략이 구체적으로 어떻게 변화해 왔는지를 살펴봄으로써 이상에서 정리한 일본 사이버 안보에 대한 인식의 변화 과정을 확인하고자 한다.

III. 일본의 사이버 안보 전략의 변화

1. 제도 형성기

일본의 사이버 안보 체계는 2000년대 초반부터 제도화 과정을 밟아왔다. 2000년 11월 제정되어 이듬해 1월부터 시행된 「고도정보통신 네트워크사회 형성 기본법(高度情報通信ネットワーク社会形成基本法; 이하 통칭 IT기본법)」이 그 출발점으로, 이 법 제22조에 근거해 '정보시큐리티대책추진회의'가 설치되었다. 일본 정부 내 사이버 안보를 위한 조직은 2000년 2월에 설치된 내각관방 정보시큐리티대책추진실(情報セキュリティ対策推進室)이 최초라고 할 수 있다. 이후 2005년 4월, 이를 강화하는 형태로 내각관방 정보시큐리티센터(情報セキュリティセンター; National Information Security Center, NISC)가 발족하였으며, 이는 같은 시기에 IT 전략본부에 설치된 정보시큐리티정책회의(情報セキュリティ政策会議)와 함께 일본의 정보시큐리티를 위해 중심적인 역할을 수행했다. 그러나 당시까지만 해도 안보 차원의 접근에는 한계가 있었다.

2. 아베 2기 정부(2012년 12월–2020년 9월)

2006년 9월 전후 최연소 총리로 취임한 아베 신조의 1차 집권은 불과 1년밖에 지속하지 못했지만, 이후 2012년 12월에 수상 관저에 돌아온 아베 총리는 일본 정치사에서 최장수 총리라는 또 한 번의 역사적 기록을 남기며, 일본 안보 정책 전반의 기조를 바꾸는 데 큰 역할을 했다. 사이버 안보 정책 역시 아베 2차 정부 시기를 거치면서 큰 변화를 겪게 됐다.

일본 정부는 단순한 정보 보호를 넘어선 포괄적 안보 개념으로의 전환의 필요성에 기인하여, 2013년 '정보시큐리티' 대신 '사이버시큐리티'로 용어를 변경한 국가전략을 발표하였다.[11] 이는 사이버 공간을 군사·비군사 영역을 포괄하는 새로운 안

보 전장으로 인식한 결과였다고 볼 수 있다. 상술한 바와 같이 이승주는 일본의 이러한 일본 사이버 안보 정책의 변화를 '사이버 안보의 전통 안보화'로 규정하였다. 그는 일본이 정보 보호를 기술 관리에서 국가 생존의 문제로 확장함으로써, 사이버 위협을 군사·외교 영역의 일부로 재편했다고 보았다. 그는 2013-14년 당시 급속도로 증가한 사이버 공격과 그로 인한 경제적 손실을 배경으로 꼽았다.[12]

2014년 11월 「사이버시큐리티기본법(サイバーセキュリティ基本法)」이 제정되면서 일본의 사이버 안보 정책은 새로운 국면을 맞이하게 된다. 이 법은 사이버 안보의 기본방향과 정부·지자체의 책무를 명시하고, 사이버시큐리티전략을 책정할 것을 정하고 있어(1조), 이후 일본 사이버 안보 정책의 근간이 되고 있다. 이에 따라 2015년 1월 기존의 정보시큐리티센터가 내각관방을 수장으로 하는 내각사이버시큐리티센터(内閣サイバーセキュリティセンター; National center of Incident readiness and Strategy for Cybersecurity, 이후 NISC)[13]로 개편되었으며, 동시에 사이버시큐리티전략본부(サイバーセキュリティ戦略本部)도 설치되었다. 이는 아베 정부가 국가안전보장회의(NSC)를 설치하여 수직적이면서도 수평적인 협의체를 구축한 것과 궤를 같이한다.[14]

법제적 변화에 맞추어 일본 정부는 2015년부터 「사이버시큐리티전략」을 주기적으로 수립하게 되었다. 2015년 전략은 세 가지 정책 목표—① 경제사회적 활력 제고와 지속 가능한 발전, ② 국민이 안전한 삶을 영위할 수 있는 사회 건설, ③ 국제사회의 평화·안정 및 국가안보 확보—를 골자로 구성되었다.[15] 이는 과거의 정보 보호 중심 접근에서 벗어나, 사회 전반의 디지털 인프라를 보호하는 종합적 전략으로의 전환을 의미한다. 또한 이 시기 일본은 사이버 공간에서의 실질적 대응 능력 강화를 위해 자위대 내 '사이버 방위대(自衛隊サイバー防衛隊)'를 창설하였다.

또한 이 시기 트럼프 1기 행정부가 출범하고 미국의 사이버 안보 전략이 오바마 시기의 규범과 거버넌스 중심 접근에서 주권과 억지력 중심 접근으로 방향을 전환하게 된 것 역시 일본에게 변화의 기회를 제공하였다. 트럼프 행정부 출범 이후 2017년 미국의 「국가안보전략(National Security Strategy, NSS)」은 '미국 우선주의(America First)' 기조 아래 사이버 안보를 핵심 축으로 삼고, 중요 기반시설 보호·연방정부 네트워크 회복력 강화·악의적 행위자 억제·기술 혁신 보호·다층 방어 구축 등을 주요 과제로 제시하며, 미국의 기술적 우위를 유지하기 위한 공세적이고 체계적인 사이버 전략을 천명했다.[16]

이러한 기조는 2018년 발표된 「국가 사이버 전략(National Cyber Strategy, NCS)」에서도 드러난다. 해당 전략은 자율적 방어 능력과 공세적 억지를 병행하며, 동맹국 및 민간기업과의 협력을 선택적 방식으로 재조정하고자 했다.[17] 특히 2018

11) 김숙현, 「기시다 정부의 사이버 안보 전략의 동향과 시사점」, 『INSS 전략보고』 244호 (2023), p. 2.
12) 이승주, 「일본 사이버 안보 전략의 변화」, 『국가안보와 전략』 17권 1호 (2017), pp. 176-179.
13) 상술한 정보시큐리티센터 역시 동일한 약자, NISC를 사용하는 것에 주의.
14) 앞의 글, p. 182.
15) サイバーセキュリティ戦略本部, 『サイバーセキュリティ２０１５』 (2015).
16) White House, 2017, *National Security Strategy*.

년 국방부의 「사이버 전략(DoD Cyber Strategy)」은 적국의 공격을 기다리지 않고, 사이버 공간에서 적성국 네트워크 내부로 진입하여 위협을 사전에 차단하겠다는 것을 시사했다.[18] 요컨대 트럼프 1기의 사이버 전략은 '자유 질서의 수호자'로서의 미국에서 '자국 주권의 방어자'로서의 미국으로 미국 사이버 안보의 정책적 방향성이 전환된 시기라고 볼 수 있다. 국제 규범보다 자율적 행동의 정당화, 다자 거버넌스보다 양자·국내 중심 대응, 방어보다는 능동적 위협 제거에 초점을 두었다고 평가할 수 있다.

이러한 변화의 시기를 거치며 일본의 사이버 안보 정책은 정보 보호를 위한 관리 차원을 넘어 국가안보의 문제로 확장되었다. 조은일은 일본이 『2018 방위계획대강』에서 사이버 분야를 대응이 필요한 신영역으로 강조하고, 2019년 미일 2+2 회의에서 사이버 분야에 대한 새로운 협의를 진행한 것을 강조하였다. 당시 미일 양국은 악의적 사이버 활동에 대한 위협을 인식하고 사이버 공간에 국제법이 적용됨을 확인하였으며, 이에 더해 미일 안보조약 5조에서 규정하는 무력 공격의 대상에 사이버 공격이 포함될 수 있음을 처음으로 언급했다고 그는 지적하고 있다.[19] 아베-트럼프 시기의 이러한 변화는 이후 기시다 후미오(岸田 文雄) 정부의 '능동적 사이버 방어(能動的サイバー防御; Active Cyber Defense, ACD)'로 이어지는 구조적 전환의 토대가 되었다고 볼 수 있다.

3. 스가 정부(2020년 9월-2021년 10월)

스가 요시히데(菅 義偉) 정부 시기는 불과 1년 정도로 짧지만, 디지털화와 사이버 안보를 통합적으로 추진한 시기라고 평가할 수 있겠다. 코로나19 팬데믹을 계기로 행정의 디지털 전환 필요성이 대두되자, 2021년 5월 기존 IT기본법을 폐지하고 「디지털사회형성기본법(デジタル社会形成基本法)」을 제정, 같은 해 9월 디지털청(デジタル庁)을 출범시켰다. 디지털청은 디지털 사회 구축, 데이터 관리, 사이버 보안 등 광범위한 정책을 통합적으로 조정하는 기관으로, 일본의 디지털·사이버 전략을 총괄하는 역할을 맡게 되었다. 디지털사회형성기본법 이후에는 총리 직속기관으로 NSC와 디지털청이 주축을 이루며, 사이버 전략본부가 하부구조에 배치되었으며, NISC는 별도로 운영되는 체계를 갖추게 되었다.[20]

한편, 2021년 각료회의에서 결정된 「사이버시큐리티전략」은 'DX with Cybersecurity'를 핵심 구호로 내세워 일본 사회의 디지털 전환(Digital Transformation, DX)과 사이버 안보 강화를 동시에 추진하겠다고 하였다. 또한 중국·북한·러시아 3개국이 사이버 공격 능력을 증강하고 있다고 지적하며, 정보 탈취

17) White House, 2018, *National Cyber Strategy*.
18) Department of Defense, 2018, *Summary: DoD Cyber Strategy*.
19) 조은일, "일본 방위성의 사이버안보 정책과 미일협력"『국가전략연구위원회 이슈브리핑』6호 (2023년6월19일).
20) 김숙현 (2023), p. 4.

능을 목적으로 한 사이버 공격을 가하고 있다고 명기한 점이 주목할 만하다.[21] 이는 일본이 사이버 위협을 지정학적 리스크와 연동하여 인식하기 시작했음을 보여준다고 하겠다.

4. 기시다 정부(2021년 10월–2024년 10월)

2021년 10월 출범한 기시다 정부는 2022년 12월 「국가안전보장전략」, 「국가방위전략」, 「방위력 정비계획」 등 3대 안보 문서를 개정했는데, 이는 2013년 첫 국가안전보장전략이 수립된 이래 9년 만의 첫 개정이었다. 이러한 흐름에서 기시다 정부는 일본의 안보 개념을 전통적 군사 영역에서 사이버·우주·경제안보를 포함한 종합안보 체제로 확대하였다. 특히 사이버 분야에서는 기존의 '수동적 방어'에서 벗어나 '능동적 사이버 방어' 개념을 명시하며, 공격자의 서버에 사전 침입해 무력화할 수 있는 대응을 제도적으로 검토하겠다는 의지를 밝혔다.

2025년 5월, 일본 국회는 능동적 사이버 방어 도입을 위한 「사이버 대응능력 강화법안」을 통과시켰으며, 총리실 산하의 사이버시큐리티전략본부가 중심적인 역할을 수행하되, 사이버시큐리티전략본부의 본부장은 내각관방대신이, 해당 본부와 가장 긴밀하게 연대하는 조직은 NSC로 하고 디지털청과 긴밀한 제휴를 목표로 하며, 민관으로 구성되어 있는 사이버시큐리티협의회와 정보를 공유하는 체제로 구성하였다. 다시 말해 일본의 사이버 안보 조직 체제는 총리실과 내각관방이 주도하되, 디지털개혁을 추진하는 디지털청과 국가안보 전반에 걸쳐 핵심기구인 NSC가 중추적 임무를 수행하는 체제로 이해할 수 있다.[22] 또한 2023년 9월 각의 결정된 「사이버시큐리티 2023」을 바탕으로 디지털청에서의 사이버 안보 강화가 도모되었는데, 구체적인 시책에는 정부 기관 및 중요 인프라의 대책 강화, 인재 육성, 국제협력 강화가 포함되었다.[23] 아울러 자위대 내 지휘통신 시스템대대의 예하 부대였던 사이버방위대는 2022년 3월 독립부대로 격상되었다.[24]

요컨대 기시다 정부의 사이버 안보 정책은 정부 주도 체제의 일원화를 추진하면서 중소기업을 위한 안보 인프라 강화와 같은 일본 독자적 모델을 지향했던 것으로 평가할 수 있다.[25]

5. 이시바 정부(2024년 10월–2025년 10월)

2024년 10월 이시바 시게루(石破 茂) 정부가 시작되고 불과 한 달 뒤 트럼프 대통

21) 『サイバーセキュリティ戦略』(2021).
22) 김숙현 (2023), pp. 8-9.
23) サイバーセキュリティ戦略本部, 『サイバーセキュリティ2023 (2022 年度年次報告・2023年度年次計画)』(2023).
24) 김숙현 (2023), p. 4.
25) 앞의 글, p. 11.

령이 재선에 성공하면서 미일 관계에도 어떤 변화가 있을지 귀추가 주목되었다. 트럼프 2기 행정부는 출범 직후부터 사이버 안보와 AI 기술의 전략적 연계를 국가안보의 핵심 영역으로 재배치하였다. 2025년 6월, 트럼프 대통령은 「국가 사이버보안 강화를 위한 선별적 노력 지속 및 행정명령 13694호 및 행정명령 14144호 개정(Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144, EO 14306)」을 서명하였는데, 백악관은 사이버 안보를 외국발 위협 대응과 기술적 회복력 강화의 핵심 국정과제로 재정비하며, AI·사물인터넷(Internet of Things, IoT)·양자암호 등 차세대 기술 보안을 중심으로 한 실질적·기술적 접근으로 전환함으로써, 오바마-바이든 정부의 정치적·행정적 요소를 배제하고 기술 중심의 사이버 안보 기조를 확립하였다고 밝혔다.[26]

이에 앞서 2025년 5월 22일, 미국 국가안보국(National Security Agency, NSA), 사이버안보·인프라안전국(Cybersecurity and Infrastructure Security Agency, CISA), 인공지능보안센터(Artificial Intelligence Security Center, AISC), 그리고 호주 사이버보안센터(Australian Cyber Security Centre, ACSC)는 공동으로 「AI 데이터 안보: 학습 및 운영 데이터 보호를 위한 모범규준(Data Security for Artificial Intelligence — Best Practices for Securing Data Used to Train and Operate AI Systems)」을 발표한 바 있다. 이 문서는 AI 시스템의 전 수명주기(lifecycle)—즉, 데이터의 수집(collection), 저장(storage), 전송(transfer), 활용(use), 보존(retention), 그리고 삭제(destruction) 단계—에서 발생할 수 있는 보안 위험을 체계적으로 다루고 있다. 특히 데이터 변조(data poisoning), 출처 불명(provenance risk), 데이터 드리프트(data drift), 무결성 훼손(integrity compromise) 등 AI 학습 데이터의 품질과 신뢰성을 저해하는 주요 위협 유형을 제시하였다.[27] 이 문서는 미국과 호주 간 AI 기반 사이버 안보 협력의 공동 지침이라는 점에서 유의미하다고 볼 수 있다. 이처럼 트럼프 2기 행정부는 사이버 안보를 경제·에너지·AI·국방을 아우르는 개념으로 접근하고 있다는 것을 확인할 수 있다.

한편 2025년 8월에는 미국 정부가 주일미군을 개편하여 중국 견제를 위한 다영역부대(Multi-Domain Task Force, MDTF) 사령부를 일본에 설치하는 방안을 검토 중이라는 보도가 있었다. 미 육군이 2017년 5개 설치를 계획하고 창설한 MDTF는 현재 3개가 가동 중인데, 장거리 정밀 타격 역량에 더해 육·해·공, 나아가 우주·사이버 등의 모든 전장에서 작전을 수행할 수 있는 전투 부대다. 유럽·아프리카를 중심으로 하는 제2 MDTF 외에 제1·3 MDTF은 인도·태평양을 작전 권역으로 상정하고 있는데, 보도된 바와 같이 일본에 제4의 MDTF 지휘부가 설치된다면 결

26) White House, 2025, "Fact Sheet: President Donald J. Trump Reprioritizes Cybersecurity Efforts to Protect America," (June 6), https://www.whitehouse.gov/fact-sheets/2025/06/fact-sheet-president-donald-j-trump-reprioritizes-cybersecurity-efforts-to-protect-america/ (검색일: 2025.10.14.).

27) NSA, CISA, AISC, and ACSC, 2025, "Joint Cyber Security Information: AI Data Security — Best Practices for Securing Data Used to Train and Operate AI Systems," (May 22).

국 MDTF 전력의 대부분이 인도·태평양 지역을 작전 지역으로 상정하는 것이 되므로, 이는 결국 중국 견제에 대한 포석으로 읽힌다.[28]

이러한 흐름 속에서 이시바 정부는 전임 정부의 기조를 이어받아 사이버 공격을 사전에 차단하기 위한 제도의 도입을 적극 추진했다. 이는 기존의 수동적 방어를 넘어, 위협의 징후를 조기에 탐지하고 공격 원천을 무력화함으로써 공격의 발생과 피해 확산을 미리 방지하려는 접근이다.

예를 들어 2025년 5월 제정된 「사이버 대응 능력 강화법(サイバー対処能力強化法)」은 일본 정부가 사이버 공격에 대한 기존의 수동적 방어에서 능동적 사이버 방어로 전환하기 위한 체계를 마련하기 위한 것으로, 외국에서 발신되는 사이버 공격을 탐지·대응하기 위해 총리가 통신사업자 동의를 얻어 국내외 통신 정보를 수집·분석하고, 필요시 경찰과 자위대가 공격 서버를 무력화할 수 있도록 허용하는 법적 근거를 마련한 것이다.[29] 관민 간 정보 공유 강화, 통신 정보 활용, 공격 서버에 대한 접근 및 무해화, 그리고 기존 NISC를 개편한 '국가 사이버 통괄실(国家サイバー統括室; National Cybersecurity Office, NCO)'의 설치가 주요 내용이다. 아울러 사이버 안보 담당장관(サイバー安全保障担当大臣)이 신설되었으며, 다이라 마사아키(平 将明)가 직을 맡았다. 현재 일본은 2027년 이후 단계적으로 능동적 사이버 방어가 본격 운용될 것을 대비해 관련 인력 확충과 관민 간 정보 연계 강화, 기술·법제 정비 등을 추진 중이다.

이러한 정책 추진의 배경에는 중국 해커 조직 등 외국발 사이버 공격이 일본의 정부기관과 주요 인프라를 지속적으로 위협하고 있다는 현실에 대한 각성과 함께 변화하는 미국의 기조에 보조를 맞추려는 의도가 있다고 볼 수 있다. 이시바 총리는 국회 연설에서 능동적 사이버 방어는 현행 평화헌법 제9조가 금지하는 '무력의 행사'가 아니라, 경찰권의 범위 내에서 이루어지는 합법적 조치임을 강조하며 법적 정당성을 주장한 바 있다.[30]

6. 다카이치 정부(2025년 10월–)

다카이치 사나에(高市 早苗) 신임 총리는 취임 직후인 10월 28일, 경주에서 열린 아시아태평양경제협력체(APEC) 참석을 계기로 아시아 순방에 나선 트럼프 대통령과 도쿄에서 양자 회담을 가졌다. 이 자리에서 양국 정상은 미일 동맹에 대해 매우 긍정적으로 평가하며 "미·일 동맹의 새로운 황금시대를 함께 열 것"이라고 강조하였다.[31]

---

28) 위문희, ""美, 日에 다영역 사령부 검토"…주한·주일 미군사령관 '별' 역전 되나," 『중앙일보』 (2025년8월25일), https://www.joongang.co.kr/article/25361523 (검색일: 2025.11.14.).
29) 松澤 登, "サイバー対処能力強化法の成立 - 能動的サイバー防御," (2025年6月24日), https://www.nli-research.co.jp/report/detail/id=82440?site=nli (검색일: 2025.10.15.).
30) 『毎日新聞』, 「能動的サイバー防御 首相「警察権の範囲内、武力行使にあたらず」」(2025年2月13日).
31) 조문규, "[속보] 트럼프 "미일 가장 강력한 동맹" 다카이치 "새 황금시대 만들자".," 『중앙일보』 (2025년10월28일), https://www.joongang.co.kr/article/25377294 (검색일: 2025.11.14.).

다카이치 정부 들어서서 나타난 변화 중에 사이버 안보와 관련해서는 정보 수집 및 분석 활동을 총괄할 '국가정보국' 신설을 검토하고 있다는 것이 보도되었다. 기시다 내각에서 경제안보담당상을 지낸 이력이 있는 다카이치 총리는 정보 수집 활동 강화를 지속적으로 주장해 왔으며, 자민당 총재 선거 당시에도 국가정보국 창설을 공약으로 내건 바 있다.[32] 또한 사이버 안보와 직접적 관련은 없으나, 자위대 내의 계급 명칭 변경 검토에 들어간다는 소식도 전해졌다. 기하라 미노루(木原 稔) 관방장관은 변경 추진을 하게 된 배경에 대해서 "방위력 핵심인 자위대원이 높은 사기와 긍지를 갖고 임무를 수행할 수 있는 환경을 정비할 필요가 있다"고 설명하였는데, 국제적인 표준에 맞추고자 한다는 것이 취지라고 전해진다.[33] 이러한 변화는 사이버 안보 전략과 직접적인 관련은 없어 보일지 모르지만, 일본 보수 정치세력의 보통국가화를 향한 단계적 실천의 하나로 볼 수 있기 때문에, 보통국가화의 방향성에서 사이버 안보가 더욱 중요한 부분을 차지할 것임을 추측하게 한다.

IV. 트럼프의 사이버 전략과 일본의 사이버 안보

트럼프 1기 행정부(2017-2021)는 2017 NSS와 2018 NCS를 통해 중요 기반시설 방어와 기술 우위 수호를 전제로 한 억지·대응의 공세적 재배치를 추구했다. 이러한 기류는 동맹국과의 양자적 협력 틀을 통해 작동했고, 결과적으로 일본에 미일 동맹 하 사이버 안보에 관한 임무 분담을 보다 현실적으로 요구하는 환경을 조성했다. 일본은 제도·조직 차원에서 이에 맞춘 정합화를 진행했는데, NISC를 중심으로 국가적 총괄·조정 기능을 강화하고, 부처 간 일체적 대응과 민관 연계를 촉진하는 정책 설계를 전개했다. 이는 공격자 특정 역량 강화, 억지력 제고, 동맹·우호국과의 연계적 대응을 명시한 일본 전략적 언어 선택에서 확인된다.[34]

그러나 이러한 일본의 대응은 외생적 압력만으로 설명되기보다는, 일본 스스로 구성한 역할 인식[35]—예컨대 규범 기반의 지역 질서 선도, 동맹 내 기여 증대—을 매개로 미국 정책 변화를 자국 변화의 동력으로 전유한 측면이 컸다. 즉, 일본은 동맹의 전략에 종속되는 것이 아니라 자기 규정된 역할과 정체성에 기초해 동맹을 활용하는 경향을 보였다는 해석이 타당할 것이다. 이러한 관점에서 보면, 트럼프 1기의 공세적 재배치는 일본이 보유하던 역할 인식을 보다 실천적·제도적 형태로 구체화하는 기회 구조로 기능했다. 요컨대, 일본의 사이버 안보 정책의 변화에는 동맹의 요구에 조응하면서도 자국의 전략 조정을 위한 수단으로 활용하는 두 개의 기어가

32) 박상현, "日다카이치, '국가정보국' 만든다…"정보 집약해 대처력 강화",," 『연합뉴스』(2025년10월24일), https://www.yna.co.kr/view/AKR20251024064800073 (검색일: 2025.11.14.).
33) 김현예, ""강한 일본" 다카이치, 자위대 계급 명칭 '군대'처럼 바꾼다,," 『중앙일보』(2025년11월13일), https://www.joongang.co.kr/article/25381847 (검색일: 2025.11.14.).
34) 『サイバーセキュリティ戦略』2021.
35) 신승휴 (2023), pp. 185-190.

맞물리는 방식으로 진화했다고 볼 수 있겠다.

한편 정권 교체 없이 이어진 자민당 연속 정권은 일본이 트럼프 1기 이후의 신호를 점진적으로 흡수·내재화하는 데 기여한 측면이 있다. 아베 총리는 FOIP 구상을 통해 규칙 기반 질서의 선도자라는 역할 인식을 공론화했고, 이는 미국의 대중 전략과 상호 작용하며 동맹 내 일본의 전략 지분을 확대하는 장치로 작동했는데, 사이버 안보 분야 역시 아베-트럼프 간 상호 작용을 거치며 노선이 정리되었다고 볼 수 있다. 스가 정부는 디지털사회형성기본법과 디지털청 출범을 매개로, 디지털 전환과 사이버 안보의 동시 추진을 제도적으로 정착시켰다. 기시다 정부는 2022년 '안보 3문서' 개정을 통해 능동적 사이버 방어를 정책 언어로 명문화하고, 공격자 특정-국제 연대-민관 연계를 아우르는 능동적·체계적 대응 프레임을 마련하려 했다. 이시바 정부는 2025년 사이버대응능력강화법 제정을 통해 능동적 방어의 법적 토대를 확정했다. 이러한 일련의 흐름은 '전통 안보의 사이버 안보화'—즉, 방위 목표 달성을 위해 사이버 역량을 수단화하는 경향—와 '사이버 안보의 전통 안보화'—즉, 사이버를 국가 생존의 차원으로 상향하는 경향—이 점진적으로 심화하였음을 시사한다.[36]

한편 일본은 사이버 안보를 외교의 수단으로도 적극 활용하고 있다. 동맹인 미국은 물론, 전통적인 우방국인 영국, 또한 프랑스, 이스라엘과도 협력을 강화해 왔다.[37] 나아가 일본은 ASEAN 국가들의 사이버 안보 역량 강화를 지원하는 데도 적극적이었는데,[38] 이러한 노력은 일본의 전통적인 외교 방침과도 궤를 같이하고 있다고 평가할 수 있겠다. 일본 정부의 전략 문서는 동맹국·우호국(同盟国・同志国)과 연계해 정치·경제·기술·법률·외교 등 가능한 모든 수단을 활용하여 글로벌한 '자유·공정·안전한 사이버 공간' 확보에 적극적 역할을 하겠다고 명시하고 있다.[39] 이는 사이버-AI-데이터-우주의 넥서스에서 규범·표준과 공급망을 매개로 국제 공조의 폭을 넓히려는 일본 사이버 외교의 방향성과도 맞닿아 있다.

또한 트럼프 2기(2025-)가 AI·양자 이후 암호·경계 게이트웨이 보안·IoT 신뢰 지표 등 기술 중심의 사이버 재정비를 내걸자, 일본은 능동적 방어의 법제화를 완결시킴과 동시에 NCO을 출범시켰고, 민관·동맹 연계 고도화로 정책 수렴을 가속하고 있다. 일본 정부 전략은 이미 공급망 전체의 신뢰성과 리스크 관리의 국가적 보완을 강조하고 있어, 2025년 이후 미국의 기술적 접근과 일본의 제도적 기반이 상호 보완적으로 공진화하는 국면에 들어섰다고 평가된다. 따라서 이러한 기조는 다카이치-트럼프 시기를 거치며 가속하리라 전망해 볼 수 있겠다.

Ⅴ. 결론 및 한국에의 함의

36) 이승주 (2017).
37) 김숙현 (2023), pp. 10-11.
38) 이상현 (2019).
39) 『サイバーセキュリティ戦略』(2021), pp. 12-13.

일본의 사이버 안보 전략은 트럼프 행정부의 공세적 전환과 맞물려 '능동적 방어'라는 새로운 패러다임으로 진입하였다. 그러나 일본이 추구하는 방향에는 구조적 한계가 존재한다. 일본은 스스로를 '자유롭고 개방된(free and open)' 디지털 질서의 수호자이자 국제 규범의 준수자로 규정하면서도, 동시에 위협의 원천에 대한 사전 침투와 선제적 무력화를 허용하는 전략을 법제화하였다. 이는 일본이 추구하는 규범적 이상과 국가 주권의 이름으로 정당화되는 공세적 억지 간의 내적 긴장을 낳는다. 즉, 일본은 국제 규범의 수호자와 능동적 방위 국가라는 두 정체성 사이에서 조정의 부담을 안고 있다고 볼 수 있겠다.

이러한 이중성은 향후 일본의 안보 정체성과 외교 전략을 규정짓는 중요한 변수가 될 것이다. 현재 일본 정국은 불안정한 과도기를 거치고 있는 가운데, 정치권의 우경화 경향이 강화될수록 일본은 사이버 위협을 '자유 진영과 권위주의 진영 간의 대립 구도' 속에서 재규정하게 될 것이며, 자유국가 간의 연대를 강조하는 쪽으로 외교 노선을 재편할 가능성이 크다. 사이버 공간에서의 규범 수호를 국제사회에서의 외교적 명분으로 삼되, 실질적으로는 동맹 중심의 억지력과 기술적 우위를 강화하는 방향으로 나아가리라 전망하는 바이다.

이러한 일본의 행보가 한국에게 주어지는 시사점은 분명하다. 한국 역시 심각한 사이버 위협의 피해국 중 하나이며, 이러한 신흥 안보 위협은 더 이상 기술적 문제에 그치지 않고 정치·외교·안보·경제·산업의 핵심 변수가 된 지 오래다. 그런데도 한국은 능동적 방어 개념에 대한 법·제도적 기초가 미흡한 만큼, 일본의 법제화 과정에서 교훈과 위험을 모두 참고할 필요가 있다. 나아가 한국은 일본과의 역사·정치적 이견에도 불구하고, 사이버 영역에서는 규범적 연대와 기술 협력의 파트너로서 일본을 인식할 필요가 있다. 특히, 한·미·일 삼각 협력 체제 내에서의 사이버 위협 정보 공유 강화, AI 및 양자기반 보안기술의 공동 연구·개발, 디지털 인프라 공급망의 투명성·신뢰성 확보를 위한 국제표준 협력 등을 추진하는 것은 국가 사이버 안보 능력을 강화하는 데 기여할 수 있을 뿐 아니라, 트럼프 행정부의 요구 사항인 이른바 '동맹 현대화'와도 유기적으로 연결될 수 있을 것이다.

【참고문헌】

김상배, 「신흥안보와 메타 거버넌스: 새로운 안보 패러다임의 이론적 이해」, 『한국정치학회보』 50권 1호 (2016), pp. 75-104.

김숙현, 「기시다 정부의 사이버 안보 전략의 동향과 시사점」, 『INSS 전략보고』 244호 (2023).

김현예, “"강한 일본" 다카이치, 자위대 계급 명칭 '군대'처럼 바꾼다,,” 『중앙일보』 (2025년11월13일), https://www.joongang.co.kr/article/25381847 (검색일: 2025.11.14.).

박상현, “日다카이치, '국가정보국' 만든다…"정보 집약해 대처력 강화",,” 『연합뉴스』 (2025년10월24일), https://www.yna.co.kr/view/AKR20251024064800073 (검색일: 2025.11.14.).

신승휴, 「사이버 안보 이슈에 대한 일본의 대응과 아베 정권의 국제적 역할인식 : 역할이론과 존재론적 안보의 시각」, 『아세아연구』 66권 3호 (2023), pp. 181-214.

윤대엽, “일본의 사이버 국가책략과 국제협력,” 『국가전략연구위원회 이슈브리핑』 5호 (2023년6월19일).

위문희, “"美, 日에 다영역 사령부 검토"…주한•주일 미군사령관 '별' 역전 되나,” 『중앙일보』 (2025년8월25일), https://www.joongang.co.kr/article/25361523 (검색일: 2025.11.14.).

이상현, 「사이버 위협에 대한 일본의 대응: 사이버 외교와 사이버 방위」, 『국제정치논총』 25권 2호 (2019), pp. 91-117.

이승주, 「일본 사이버 안보 전략의 변화」, 『국가안보와 전략』 17권 1호 (2017), pp. 173-202.

이정환, “일본 사이버안보 정책의 범정부적 정책 대응 변화,” 『국가전략연구위원회 이슈브리핑』 4호 (2023년6월19일).

조문규, “[속보] 트럼프 "미일 가장 강력한 동맹" 다카이치 "새 황금시대 만들자",,” 『중앙일보』 (2025년10월28일), https://www.joongang.co.kr/article/25377294 (검색일: 2025.11.14.).

조은일, “일본 방위성의 사이버안보 정책과 미일협력” 『국가전략연구위원회 이슈브리핑』 6호 (2023년6월19일).

Calder, Kent E., “Japanese Foreign Economic Policy Formation: Explaining the Reactive State,” *World Politics*, vol. 40, no. 4 (1988), pp. 517-541.

Department of Defense, 2011, *Strategy for Operating in Cyberspace* (Washington, D.C.: DoD).

Department of Defense, 2018, *Summary: DoD Cyber Strategy*.

Lim, Eunjung, 2019, “Chracterizing Japan’s Current Diplomacy under Abe,” *The Korean Journal of Security Affairs* Vol. 24, No. 2: pp. 96-119.

National Security Agency, Cybersecurity and Infrastructure Security Agency, Artificial Intelligence Security Center, and Australian Cyber Security Centre, 2025, “Joint Cyber Security Information: AI Data Security — Best Practices for Securing Data Used to Train and Operate AI Systems,” (May 22).

White House, 2015, “FACT SHEET: President Xi Jinping’s State Visit to the

United States," (September 25), https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states (검색일: 2025.10.14.).

White House, 2017, *National Security Strategy*.

White House, 2018, *National Cyber Strategy*.

White House, 2022, *National Security Strategy*.

White House, 2022, "Fact Sheet: President Biden and G7 Leaders Formally Launch the Partnership for Global Infrastructure and Investment," (June 26), https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/06/26/fact-sheet-president-biden-and-g7-leaders-formally-launch-the-partnership-for-global-infrastructure-and-investment/#:~:text=The%20Digital%20Invest%20program%20will%20leverage%20$3.45,resilient%2C%20secure%20digital%20ecosystems%20in%20developing%20countries. (검색일: 2025.10.14.).

White House, 2025, "Fact Sheet: President Donald J. Trump Reprioritizes Cybersecurity Efforts to Protect America," (June 6), https://www.whitehouse.gov/fact-sheets/2025/06/fact-sheet-president-donald-j-trump-reprioritizes-cybersecurity-efforts-to-protect-america/ (검색일: 2025.10.14.).

サイバーセキュリティ戦略本部, 2015, 『サイバーセキュリティ２０１５』.

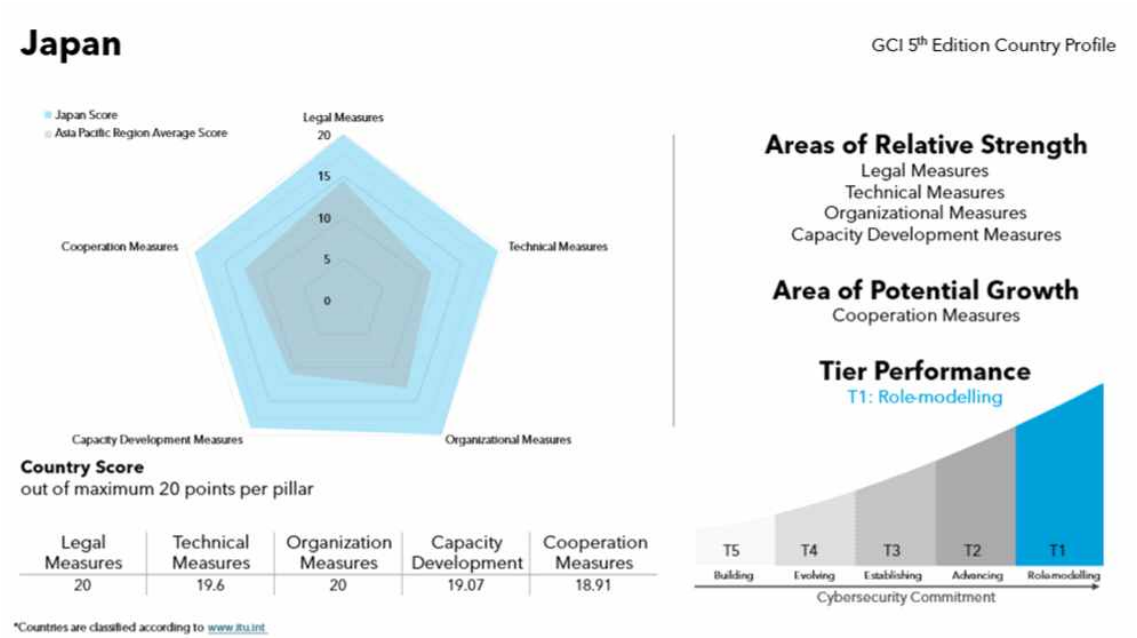
サイバーセキュリティ戦略本部, 2023, 『サイバーセキュリティ2023 (2022 年度年次報告・2023年度年次計画)』.

『サイバーセキュリティ戦略』 2021.

『毎日新聞』, 「能動的サイバー防御 首相「警察権の範囲内、武力行使にあたらず」(2025,02.13.).

松澤 登, 2025, "サイバー対処能力強化法の成立－能動的サイバー防御," (6月24日), https://www.nli-research.co.jp/report/detail/id=82440?site=nli (검색일: 2025.10.15.).

【부록】



출처. International Telecommunication Union, Global Cyber Security Index 2024.

※ 이슈브리핑에 수록된 내용은 필자 개인의 의견이며, 한국사이버안보학회의 공식적인 입장이 아님을 알려드립니다.