韓日共通の安保脅威と対応：サイバー安保協力を中心に

崔垠娥(成均館大学校)

1. 序論

本論文は、国際政治理論の議論を通じて韓国と日本が直面した共通の安全保障脅威を考察し、共同対応のための両国の協力策をサイバー安保分野を中心に導き出すことを趣旨とする。これまで韓日の安保協力は制限的に、そして米国が仲裁する構図によって成り立ってきた。しかし、国際環境のパラダイムが急変し、新アジア安保秩序が構築される状況において、今や固定的な構図から脱する必要があり、さらに共通の安全保障脅威に対する認識を共有し機敏に対処するなど、戦略的パートナーシップを発揮すべきであろう。

１９６５年の国交樹立以来、韓日関係は強制徴用、慰安婦問題など過去の歴史における懸案事項に対する各政府の立場が異なり、対立と葛藤が累積されてきたため、安保的レベルの協力体制の構築が困難な状況が続いてきた。李明博政府は、北朝鮮に対する軍事情報の共有が可能な初の軍事協定である韓日秘密軍事情報保護協定、GSOMIA を締結し、これは安保に対する脅威を解消するための相互意志を確認するとともに、韓日関係が進展したと評価されている。しかし、こうした協力基調は、文在寅政府発足後、強制徴用問題と相まって輸出統制、GSOMIA 破棄論争などに繋がり、再び悪化した。数年間硬直した韓日関係は､2022 年に尹錫悦政府が発足して以来､両国関係を改善する意志を見せており、日本との外交・安保協力に開かれた姿勢をとっている。この流れを継続しつつ、両国は有意義な安全保障協力の機会をうかがうことができるだろう。

特にグローバルサイバー安全保障に対する脅威が増加するにつれ、サイバー空間における西欧対非西欧陣営の敵対関係が加熱する中、韓国と日本は北朝鮮の核・ミサイルの脅威以外にもサイバー攻撃に関する事例を共有しており、サイバー二国間・多国間協力を推進しつつ、韓日関係の改善と安保脅威の抑制、戦略的価値の向上を目指すことができるという点を強調したい。西欧は同盟・友好国、国際機関を活用してサイバー脅威に積極的に対処し、安保協力を推進している。特に、米国がインド太平洋戦略(Indo-Pacific Strategy)を駆使することにより、日本、オーストラリア、インド等の国家とグローバルなサイバー安全保障を構築している状況において、韓日サイバー安保協力が今後の日米韓 3 か国の戦略的連帯強化にも貢献できるとみられる。

2. 理論的議論

2.1. 韓日共通の安保脅威

国際政治学の大きなパラダイムである現実主義理論は、個々の国家の上位にいかなる中央政府もない国際体制の構造的無政府状態において現れる国際政治の変化を説明する。全ての国家は安全保障を確保するために努力し、国際政治において国家が追求する最終価値は生存である。国家は自らの安全を最終価値として追求し、これを達成するための手段としてパワーを追求する。ケネス・ウォルツ（Kenneth N. Waltz）は、国家行動を「相対な力の配分（distribution of relative power)」という独立変数として分析する。つまり、ある国家のパワーが増加する場合、周辺国家は勢力均衡を維持す

るために浮上する国家に対抗する[1]。アジア太平洋地域は、米国、ロシア、中国という強大な軍事大国の利害が集中しているため、日本はこのような地政学的考慮により自国の安全保障問題に敏感にならざるをえない。また、韓国と北朝鮮の対峙及び北朝鮮の核及びミサイル問題と中国と台湾間の対峙に見られるように、脅威要素が依然として深刻に存在すると認識している[2]。

新現実主義は、無政府的秩序（anarchic order）状態となった国家が、外部の脅威に対して自力救済（self-help)と同盟の助力を総動員することを注文する[3]。日本は、北朝鮮が核兵器開発の試みやミサイルの試験発射、不審船の浸入等の突発行為によって自国の安全保障に対する脅威要因を増大させて来たことにより、北朝鮮に対する安保脅威を強く認識している。2016 年、日本の「防衛白書」は、中国、ロシア、北朝鮮が日本の核心的基盤施設を狙ってサイバー攻撃を行っており、技術的により巧妙になっているとの認識を明らかにした（防衛省・自衛隊 2016)[4]。整理すると、韓日両国は北朝鮮の核・ミサイル、サイバー脅威等の共通の安保脅威に直面している。

2.2. 韓日協力の必要性

勢力均衡論は、敵対的競争勢力間に力の均衡が成立していれば安定した平和が持続すると考える。この時、パワーバランスをどのように見るかによって、防御的現実主義と攻撃的現実主義に区分される。前者は現状維持的に安全保障を最大化するものであり、後者は現状打破的に安全保障を最大化するものである。例えば、現在、米国は中国よりも相対的に大きな力を守るために、クアッド（Quad)、オーカス（AUKUS)、インド・太平洋経済枠組み （IPEF）等によりグローバルな同盟ネットワークを再建している。米国の立場では、自身が相対的な力の優位性を確保し維持することを「バランス」と見なすのである。同様に、米国と日本の協力が伝統的安全保障領域から非伝統的安全保障領域に拡大する基調も、日米同盟の強化を通じて脅威に先制的に対応し、自国の力量を高め、安全保障を最大化するものと説明される。スティーブン・ウォルト（Stephen M. Walt）は、同盟の形成においてハードパワー（power）だけでなく脅威（threat）の認識も作用するという脅威均衡論を提唱した。理論によると、国家は安全保障のために最も脅威的な国家に対抗して同盟を結成し、脅威を判断する 4 つの要素として総体的国力、地理的隣接性、攻撃能力、攻撃意図がある[5]。脅威均衡論として見れば、韓国と日本は戦略的パートナーレベルにおいて北朝鮮、中国に対する脅威の認識を共有しているため、安保協力を推進する必要性がある。

一方、制度と規範を通じた協力と、これによる国際レジームの形成、究極の平和達成が可能であるとみなす自由主義パラダイムにおいても、韓日協力の必要性が導き出される。新自由制度主義論は、自由主義的国際制度と民主主義の価値、規範を拡散する外交手段を通じて、平和と繁栄が最大化できると考える。韓日両国が共有する自由民主憲法と人権、市場経済制度と価値に基づき、協力と信頼が蓄積されると考えるのである。構成主義理論は、国家間の交流と協力がなされる中で間主観性が形成され、これにより相互関連性に基づいて国家のアイデンティティが変化し、平和を維持できると考える。この理論は、韓国と日本が過去の侵略と植民地の歴史に対する記憶を繰り返し、両国関係の葛藤

---

[1] 이근욱,『왈츠 이후 국제정치이론의 변화와 발전』(한울 아카데미, 2009), p. 39.

[2] 김영춘,“일본의 북한위협 인식과 군사력 강화,”『통일연구원 연구총서』, 2001-05, pp. 6-7.

[3] 김태효,“신아시아 안보질서 2030: 패러다임 변화와 한국의 과제,”『신아세아』, 26권3호(2019년, 가을), p. 67.

[4] 김상배 외,『사이버 안보의 국가전략 3.0』(사회평론아카데미, 2019), p. 69.

[5] Stephen M. Walt, “Why Alliances Endure or Collapse,” *Survival*, Vol. 39, No. 1 (Spring 1997), p. 158.

と緊張を招くことから脱するべきであり、両国関係を改善するために大衆文化、スポーツ、人的交流などを通じて未来志向的なアイデンティティの形成が必要だと診断する。

3. 韓日サイバー安保協力

3.1 両国の対応基調

韓国と日本は国家サイバー安保戦略において法治主義、開放性、自律性を追求しており、サイバー脅威行為者への対応と安保守護の意志を最優先目標としている点において一致した基調を示す。したがって、サイバー安全保障分野での共同対応と協力が可能性の高い議題であると考えられる。日本の精巧な戦略は、2014 年のサイバーセキュリティ基本法の制定を基点として設けられたが、2015 年日本の「サイバーセキュリティ戦略」が樹立され、その後 2018 年 7 月と 2021 年 9 月末に追加改正を通じて発展した目標を提示してきた[6]。最新の改正されたサイバーセキュリティ戦略は、日本は情報の自由な流通、法治主義、開放性、自律性、多国間協力という基本原則に基づいた「自由で公正で安全なサイバー空間の実現」の確保を目標とし、①社会-経済的活力と持続可能な発展、②安全なデジタル社会の実現、③国際社会の平和および安定性と日本の国家安全保障に寄与するという政策方針を強調する[7]。戦略で中国、ロシア、北朝鮮を主要なサイバー攻撃を行っている国として言及した部分は、改正前の戦略との最も大きな違いである。該当国家が軍をはじめとする機関を通じてサイバー能力を向上していることから、米国と日本をはじめとする友好国は、相互に共有するコアバリューを保護するためにサイバー対応能力を向上すべきであると強く明示する[8]。韓国は 2019 年に初めて「国家サイバー安保戦略」を発刊し、増加するサイバー脅威に対応する力量を強化し、国際協力を強化するなどの基本方針とビジョン、目標を提示した。信頼基盤のサイバー安保政策を推進するための 3 大基本原則として①国民基本権とサイバー安保の調和、②法治主義を基盤とする安保活動の展開、③参与と協力の遂行体系の構築などを策定した。また、6 大戦略課題の一つとして、サイバー安保に関する国際規範の形成と、国際協力をリードしサイバー安保の先導国としてのリーダーシップを拡大するという内容が盛り込まれている。

3.2 共通の脅威と安保協力

韓国と日本を標的とした北朝鮮の代表的な共通サイバー攻撃として、サイバー外貨稼ぎがある。日本は、2016 年にコンビニエンスストアでの ATM ハッキング事件と、2018 年 1 月に日本の仮想通貨取引所のハッキング事件を経験し、両事件は北朝鮮の犯行と推定されることが明らかになった。北朝鮮は韓国の仮想通貨取引所を標的としたハッキングを複数回試みたことがある[9]。経済安全保障、先端技術問題を通じた戦略的コミュニケーションが強調されている状況において、今後頻繁になる北朝鮮のサ

---

6 基本法の施行に伴い、2015 年 1 月には日本のサイバー安保政策を担当するコントロールタワーとして、官房長官が主導する「サイバーセキュリティ戦略本部」が内閣官房に設置され、新 NISC が戦略本部の実務を総括する事務局として新たに発足した。同年 9 月には、基本法に基づき 3 年間の基本的な政策の方向性を提示した中長期戦略である「サイバーセキュリティ戦略」が韓国の国務会議にあたる閣議を通過し、2018 年 7 月には「Society 5.0」と「積極的サイバー防御」という概念が反映された「サイバーセキュリティ戦略」が新たに発表された。이상현, “일본의 사이버안보 수행체계와 전략,” 『국가안보와 전략』, 제 19 권 1 호(통권 73 호), 2019, p. 118.

7 박성호, “일본의 사이버 안보전략,” 『일본학』, 제 56 집(2022.4), p. 162.

8 Ibid. p. 171.

9 유동열,[전문가 진단] 북한의 새 외화벌이 수단, 사이버 금전(암호화폐) 탈취,” 『미래한국』,2019.09.02.

イバー外貨稼ぎ攻撃に備え、重大な安保脅威事案として想定すべきであろう。予想可能な共通のサイバー脅威として、通信における安全保障上の脅威を挙げることができる。韓国と日本は東南アジアの海洋を共有している。2011 年、日本の東北地方に隣接する太平洋の海底で発生した地震（東日本大震災）により日本と繋がる海底ケーブルが損傷し、我々も YouTube や Google 等の海外サイトの接続に深刻な支障を経験した[10]。海底ケーブルは、自然災害だけでなく人為的破損や盗聴に脆弱なため、このような点を利用して海底ケーブルをターゲットとした情報活動が発生している。したがって、韓日両国は通信安保に対する重要度を高め、海底ケーブル通信網を守るための議論を手始めに、予想される脅威に先制的に対応すべきだろう。

両国は、対外脅威情報に関する共有体系を強化し、迅速に国際共助プロセスを構築すべきだ。条件付きの延長状態に置かれた GSOMIA の正常化への努力を皮切りに、北朝鮮のサイバー脅威を早期に識別し、迅速に情報を共有する定型化されたプロセスを構築すべきだろう。そして 2016 年 10 月に初めて開催された韓日サイバー政策協議会のような二国間協力を再開し、サイバー外交を持続すべきである。また、韓米同盟が強調するサイバー敵対勢力の抑止、サイバー空間におけるその他の国際安保における懸案に関する協力等を日本との協力にも反映すべきである。日米韓三角サイバー安保共助体制が構築されるよう、重層的な政策案を作成すべきだろう。多国間協力としては、NATO サイバー防衛協力センター（CCDCOE）との協力を通じてサイバー安保の国際ネットワークを強化しつつ、韓国と日本が共に発言権を強めていくことが期待できる。日本は NATO と防衛当局間のサイバー協議体である「日-NATO サイバー防衛スタッフトークス 」を毎年実施し、NATO が主催するサイバー防衛演習にもオブザーバーを派遣する等、運用面での協力も念頭に置いた対応を行っている[11]。今年 5 月にアジアで初めて CCDCOE の正会員となった韓国は、CCDCOE の各種会議、サイバー防衛演習等に参加してきた日本と共に、国際サイバー規範、制度の形成を主導していくことができる。

4. 結論

北朝鮮による核の脅威と北朝鮮・中国問題への対応のために韓日安保協力が重要であるという認識を共有し、包括的な安保協力を強化すべきである。韓日間の安全保障分野における信頼は、2018 年の「レーダー照射-哨戒機低空飛行」の葛藤以来、なかなか回復しない[12]。しかし、この３～４年間に韓日関係が悪化したことに比べて、 尹錫悦政府の発足後は両国の関係改善の意志が際立つ。今年４月、韓日政策協議代表団が日本に派遣され、岸田文雄首相をはじめとする約 50 名の政界、経済界、学界、言論界の要人との公式面談日程をこなし、韓日関係の改善の意志と課題に対する合意を形成し、改善のためには何よりも人的交流の拡大が重要だという認識を共にした[13]。韓日は北朝鮮と中国に対する戦略的目標を共有しており、特に両国は新安保パラダイムの登場とともにサイバー空間で発生する脅威に対する保護を核心的国家目標として共有している。したがって、北朝鮮によるサイバー脅威の抑制を目標とした韓日間の戦略的協力関係の確立が望ましいだろう。

両国は、相対的に感度が低く、グローバルな安全保障レベルでの協力が必要な分野での協力を推進

10 최정현, “핵잠수함 · 해저케이블과 스파이 특수전의 해저 삼각안보,” 『KIMS Periscope』, 제 165 호, 2019.07.21.
11 이상현, “사이버 위협에 대한 일본의 대응: 사이버 외교와 사이버 방위,” 『국가전략』, 2019 년 제 25 권 2 호, p. 110.
12 최은미, “기시다–바이든 미일정상회담 이후 일본의 대외전략과 한일관계에의 함의,” 『이슈브리프』, 2022-19, p. 9.
13 박미영 · 권지원, “한일정책협의단 “한일관계 개선 ‘선택 아닌 당위’ 공감대”,” 『뉴시스』, 2022.04.28.

し、段階的に信頼を積み重ねてゆくべきだろう[14]。非伝統的安全保障分野であるサイバー安保協力は、伝統的安全保障と連携する事案として北朝鮮のサイバー脅威に対処し、二国間・多国間協力を通じて韓日関係を改善へと導くことのできる核心的議題である。韓日間の信頼構築と同時に、民主主義と市場経済価値を共有する他のパートナー国と連帯する機会も増やすことができる。韓国と日本が自国のサイバー安保戦略を通じて国際規範の形成と信頼構築に対する意志を強調しているだけに、サイバー外交の舞台を積極的に活用し、二国間・多国間の安保協力を推進してゆくべきだろう。

参考文献

1. 단행본

김상배 외(2019). 『사이버 안보의 국가전략 3.0』. 사회평론아카데미.

이근욱(2009). 『왈츠 이후 국제정치이론의 변화와 발전』. 한울 아카데미.

2. 논문

김영춘(2001). “일본의 북한위협 인식과 군사력 강화.” 『통일연구원 연구총서』. 2001-05.

김태효(2019). “신아시아 안보질서 2030: 패러다임 변화와 한국의 과제.” 『신아세아』. 26권 3호.

박성호(2022). “일본의 사이버 안보전략.” 『일본학』. 제56집.

이상현(2019). “일본의 사이버안보 수행체계와 전략.” 『국가안보와 전략』. 제19권 1호(통권73호).

_____(2019). “사이버 위협에 대한 일본의 대응: 사이버 외교와 사이버 방위.” 『국가전략』. 제25권 2호.

최은미(2022). “기시다-바이든 미일정상회담 이후 일본의 대외전략과 한일관계에의 함의.” 『이슈브리프』. 2022-19.

최정현(2019). “핵잠수함 · 해저케이블과 스파이 특수전의 해저 삼각안보.” 『KIMS Periscope』. 제165호. 07.21. (검색일: 2022.06.14.)

Walt, Stephen M. “Why Alliances Endure or Collapse.” *Survival.* Vol. 39 No. 1 (Spring 1997).

3. 언론기사

박미영 · 권지원(2022). “한일정책협의단 "한일관계 개선 '선택 아닌 당위' 공감대".” 『뉴시스』. 04.28. https://newsis.com/view/?id=NISX20220428_0001852599 (검색일: 2022.07.14.)

유동열(2019). “[전문가 진단] 북한의 새 외화벌이 수단, 사이버 금전(암호화폐) 탈취.” 『미래한국』. 09.02. http://www.futurekorea.co.kr/news/articleView.html?idxno=120536 (검색일: 2022.06.14.)

(翻訳責任者：佐久間香織)

14 최은미, Ibid.