韓国のサイバー戦略とその課題

―　「サイバー空間ダイヤモンドモデル」による米国との比較分析　―

佐々木　稔

本稿は 2021 年 8 月に脱稿したものであり、本誌発行時点において一部の参考文献は最新のものではなくなっているが、脱稿当時の原稿のまま掲載するものである。（編集委員会）

はじめに

近年、サイバー空間における安全保障の必要性は増している一方、国際的な枠組みの整備は頓挫している。理由として、国家間の基本的認識あるいは政策理念の違いがあるためだと指摘されている[1]。

他方、サイバー攻撃は日々高度・巧妙化している。脅威が高まる中において、一国のみによる対応は困難と言え、サイバー空間における同盟国とのパートナーシップは重要性を増していると言える。

このような中、仮に米国とその同盟国のサイバー戦略の間に相違点が存在した場合、戦略的な脆弱性が発生してしまい、サイバー攻撃の脅威への対応が困難となる可能性があるのではないだろうか。

本稿のリサーチクエスチョンは、米国と同盟国のサイバー戦略の相違点によって、サイバー空間上の安全保障にどのような負の影響が発生し得るか。そして相違点が発生する背景には何があるのか、というものである。

また、エリノア・スローン（Elinor Sloan）がサイバー戦争の戦略思想は未だ揺籃期にある[2]と指摘している通り、任意のフレームワークを用いてサイバー戦略を分析する研究は後述するように少ない状況である。そこで本稿は 2019 年にフランク・サンチェズ（Frank Sanchez）らによって提案された「サイバー空間ダイヤモンドモデル」[3]を用いてサイバー戦略の分析を

[1] 須田祐子「サイバーセキュリティの国際政治―サイバー空間の安全をめぐる対立と協調―」『国際政治』第 2015 巻第 179 号、2015 年 2 月、64 頁。
[2] エリノア・スローン『現代の軍事戦略入門〔増補新版〕―陸海空からの PKO、サイバー、核、宇宙まで―』奥山真司、平山茂敏訳、芙蓉書房、2019 年、295 頁。
[3] Frank C. Sanchez, Weilun Lin, and Kent Korunka, “Applying Irregular Warfare Principles to Cyber Warfare,” *Joint Force Quarterly*, Iss. 92, 1st Quarter, January 2019, p. 19.

試みる。これは、イラクやアフガニスタンにおける対反乱戦（Counter Insurgency: COIN）の教訓をサイバー空間に応用したものであり、サイバー空間における作戦のアプローチや戦略を開発するために適用できるとされているものである[4]。このフレームワークは曖昧なサイバーの区分を整理する上で有用であり、本稿において米国と同盟国の相違点を導出し、相違点が発生する背景を考察する過程で中間的な役割を果たす。

本稿では、次の手順で分析する。

第 1 節では、米国及び同盟国が発表しているサイバー戦略を概観するとともに、数ある米国の同盟国の中から韓国を比較の対象とした理由を説明する。

第 2 節では、本稿で分析に用いるフレームワークである「サイバー空間ダイヤモンドモデル」の概念を確認するとともに、米国と韓国のサイバー戦略及び関連政策について前述したフレームワークを用いて相違点を分析する。

第 3 節では、サイバー戦略及び関連政策の相違点によって発生する可能性がある負の影響をまとめるとともに、相違点が発生する背景について考察する。

1　米国及び同盟国におけるサイバー戦略

（1）米国におけるサイバー戦略

米国ではバラク・オバマ（Barack Obama）政権時代の 2015 年にサイバーセキュリティ法（Cybersecurity Act of 2015）等が成立され、その後、ドナルド・トランプ（Donald Trump）政権時代の 2018 年 9 月に『米国国家サイバー戦略（*Cyber Strategy of the United States of America*）』[5]が発表された。これにより、連邦政府が国全体のネットワーク等を守ることを明記するようになったと笹川平和財団安全保障事業グループは分析している[6]。

しかし、『米国国家サイバー戦略』は単なる改訂ではなく、オバマ政権時

[4] Ibid.
[5] The White House, *National Cyber Strategy of the United States of America*, September 2018.
[6]「サイバー空間の防衛力強化プロジェクト政策提言“日本にサイバーセキュリティ庁の創設を！”」笹川平和財団安全保障事業グループ、2018 年 10 月、13 頁、www.spf.org/global-data/20181029155951896.pdf。

代の政策を破棄したものであると永野秀夫は指摘している[7]。『米国国家サイバー戦略』の中では「ロシア、中国、イラン、北朝鮮はいずれも、米国、同盟国及びパートナー国に挑戦する手段としてサイバー空間を利用している。」[8]と名指しで非難するような厳しい表現が記載されているが、これはオバマ政権下では見られなかったものである。

2017 年 12 月に公表された『国家安全保障戦略（*National Security Strategy*: NSS）』においても、米国は中国、ロシア両国を「戦略的競争相手」と厳しく位置付けている。これは冷戦終結後の米国の対中政策が、いわゆる「関与政策」から「戦略的競争」へ大転換したことを示していると笹島雅彦[9]は分析している。

以上から、『米国国家サイバー戦略』においても『国家安全保障戦略』と同様に一貫した対中政策が採用され、「関与政策」から「戦略的競争」に方針を転換する形となったと言える。

（2）米国の同盟国におけるサイバー戦略

はじめに、北大西洋条約機構（North Atlantic Treaty Organization: NATO）について論じる。NATO としてのサイバー戦略は発表されていないが、2012 年に NATO サイバー防衛協力センター（Cooperative Cyber Defence Centre of Excellence: CCDCOE）が『国家サイバー戦略フレームワークマニュアル（*National Cyber Security Framework Manual*）』[10]を公開している。これはサイバー戦略を作成する際の留意点等をまとめたものであり、NATO 加盟国が其々のサイバー戦略を作成している。国連軍縮研究所（United Nations Institute for Disarmament Research: UNIDIR）のサイバー政策ポータル[11]によれば、NATO 全加盟国の 30 か国（2020 年 3 月現在）[12]がサイバー戦略に関する文書を公表している。

また、米国は非 NATO 主要国同盟（Major Non-NATO Ally: MNNA）と

---

[7] 永野秀雄「米国の重要インフラに関するサイバーセキュリティとセキュリティ・クリアランス法制（上）」『人間環境論集』第 19 巻第 1 号、2018 年 10 月、110 頁。
[8] The White House, *National Cyber Strategy of the United States of America*, p. 2.
[9] 笹島雅彦「対中関与政策の再検討と日本外交」『跡見学園女子大学文学部紀要』第 54 号、2019 年 3 月、2 頁。
[10] NATO CCDCOE, *National Cyber Security Framework Manual*, December 2012.
[11] “UNIDIR Cyber Policy Portal,” UNIDIR, January 9, 2019, unidir.org/cpp/en.
[12] 「北太平洋条約機構(NATO)」外務省、2020 年 12 月、www.mofa.go.jp/mofaj/area/nato/index.html。

して分類される同盟スキームを世界中のパートナー国に提供している[13]。MNNA に分類される同盟国として、バーレーン、エジプト、アルゼンチン、オーストラリア、日本等が挙げられる[14]。

前述した国連軍縮研究所のサイバー政策ポータルによると、MNNA におけるサイバー戦略の一覧は表 1 のとおりとなる。

表 1　MNNA に分類される同盟国におけるサイバー戦略

地域	国略称	サイバー戦略の文書名	発表時期
中東	バーレーン	不　明	不　明
	イスラエル	第 3270 決議	2017 年 12 月
	ヨルダン	国家サイバーセキュリティ戦略	2018 年　2 月
	クウェート	国家サイバーセキュリティ戦略	2017 年　7 月
	アフガニスタン	アフガニスタン国家サイバー戦略	2014 年 11 月
非州	エジプト	国家サイバーセキュリティ戦略	2018 年 11 月
	モロッコ	国家サイバーセキュリティ戦略	2012 年 12 月
南米	アルゼンチン	国家サイバー戦略	2019 年　5 月
大洋州	オーストラリア	オーストラリア国家サイバーセキュリティ戦略	2020 年　8 月
	ニュージーランド	サイバーセキュリティ戦略及びアクションプラン 2018	2018 年　3 月
亜州	日本	サイバーセキュリティ戦略	2018 年　7 月
	韓国	韓国国家サイバー安保戦略	2019 年　3 月
	フィリピン	国家サイバーセキュリティ計画	2017 年　5 月
	タイ	国家サイバーセキュリティ戦略	2017 年 10 月

（出所）“UNIDIR Cyber Policy Portal,” UNIDIR, January 9, 2019, unidir.org/cpp /en を参考に筆者作成。

※網掛け箇所は、『米国国家サイバー戦略』が発表された 2018 年 9 月以降に発表された文書を示す。

（3）比較分析対象の選定

まず、基準とする米国のサイバー戦略として、2018 年 9 月に発表された最新の『米国国家サイバー戦略』を選定した。

---

[13] Andreas Umland, “The Six Futures of Ukraine: Competing Scenarios for a European Pivot State,” *The Brown Journal of World Affairs*, Vol. 24, Iss. 1, Fall/Winter 2017-2018, p. 271.

[14] Snejana Farberov, “Hillary Clinton Files into Kabul as U.S. Declares Afghanistan Major Non-NATO Ally,” *Daily Mail Online*, July 7, 2012, www.dailymail.co.uk/news/article-2170049/U-S-declares-Afghanistan-major-non-NATO-ally-ensure-nation-gets-defense-aid-2014-troop-withdrawal.html.

次に、『米国国家サイバー戦略』を反映できる時間的な余地があった同盟国を選定することが適当と考え、米国の後に発表された表 1 の網掛け箇所の国を比較対象の候補とした。

また、米国は厳しい対中政策をとっているため、中国と関係が深い国を比較することで、米国との相違点が浮き彫りになる可能性が高いと考えた。中国と関係が最も深い地域の一つはアジア地域であることから、表 1 の網掛け箇所の中からアジア地域を選択した結果、韓国に絞ることができた。

以降『米国国家サイバー戦略』及び関連政策を基準として、『韓国国家サイバー安保戦略(국가 사이버 안보 전략)[15]』及び関連政策を比較分析することで、どのような相違点が存在し、サイバー空間上の安全保障にどのような負の影響が発生し得るか、そして相違点が発生する背景には何があるのかを論証する。

2　米国及び韓国のサイバー戦略の分析

（1）サイバー戦略に関する先行研究

サイバーに関する戦略的なレベルの研究は多数発表されている。例えばリザ・アズミ（Riza Azumi）らは 54 か国のサイバー戦略を分析し、その動機は、サイバーセキュリティに関する法律の制定と、政策決定者の認識を深めることにあると分析している[16]。

ヴァレンティン・ウェーバー（Valentin Weber）は、米国の大戦略とサイバー戦略の融合という観点で、『米国国家サイバー戦略』を分析している[17]。

マックス・スマイツ（Max Smeets）は、『米国国家サイバー戦略』は同盟国に正の影響のみならず、負の影響を及ぼす場合があると分析している[18]。

これらのように様々な先行研究が存在するものの、米国と同盟国のサイバー戦略を比較分析する研究は管見の限り存在していない。また、サイバー

---

[15]『국가 사이버 안보 전략』大韓民国青瓦台国家安保室、2019 年 3 月、www.kisa.or.kr/jsp/common/downloadAction.jsp?bno=4&dno=2372&fseq=1。

[16] Riza Azumi, William Tibben, and Khin Than Win, “Motives behind Cyber Security Strategy Development: A Literature Review of National Cyber Security Strategy,” *Australasian Conference on Information Systems 2016*, December, 2016.

[17] Valentin Weber, “Linking Cyber Strategy with Grand Strategy: The Case of the United States,” *Journal of Cyber Policy*, Vol. 3, Iss. 2, August 17, 2018, pp. 236–257.

[18] Max Smeets, “U.S. Cyber Strategy of Persistent Engagement & Defend Forward: Implications for the Alliance and Intelligence Collection,” *Intelligence and National Security*, Vol. 35, Iss. 3, February 15, 2020, pp. 444-453.

戦略を分析するフレームワークも少ない状況であり、ジェイソン・ヒーリー（Jason Healey）は、対反乱戦においてサイバー攻撃をどのようなツールとして使用するかという調査に比べ、対反乱戦がサイバー戦略にどのような示唆を与えるかという研究は少ない状況であると分析している[19]。

(2)「サイバー空間ダイヤモンドモデル」

サンチェズらが提唱した分析枠組みである「サイバー空間ダイヤモンドモデル」は、対反乱戦の分析枠組みをサイバーへと応用したものである[20]。この対反乱戦の分析枠組みは、提唱者にちなんで「マッコーミックの対反乱戦モデル」あるいは「mystic diamond model」とも呼ばれる[21]。

ヒーリーは対反乱戦とサイバー空間には 3 つの類似性が認められると分析しており[22]、1 つ目の類似性は「敵は隠れていて欺瞞に依存している。」、2 つ目は「紛争は民衆の中で（そしてホスト国と共に）戦われる。」、3 つ目は「火力の優勢と長期的な成功との関係は、現在の戦争システムのように単純ではない。」と指摘している。

マイケル・センフト（Michael Senft）によると、サイバーセキュリティの計り知れない課題はサイバー空間の複雑な生態系に固有のように見えるかもしれないが、テロ対策の戦いと深い類似性があると指摘し、どちらも非対称戦であることから、秘密の活動が使用され、コストが不均衡であり、適応率が著しく異なるとともに、攻撃者と防御者の間の交戦規則が不平等であると論じている[23]。

ヨナス・ヴァン・フーレン（Jonas van Hooren）は、特殊作戦部隊（Special Operation Force: SOF）の運用上の環境とサイバー空間は多くの類似点を共有していると指摘し、類似点として準備期間と回収期間が比較的短いこと、安価であること、不透明でステルス性の高い性格であることを挙げて

---

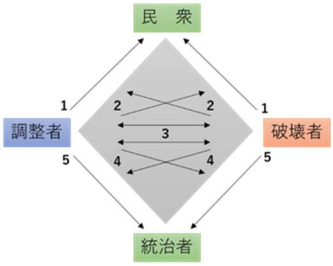
19 Jason Healey, “A Bizarre Pair: Counterinsurgency Lessons for Cyber Conflict,” *Parameters*, Vol. 50, No. 3, August 2020, p. 87.
20 Sanchez, Lin, Korunka, “Applying Irregular Warfare Principles to Cyber Warfare,” p. 19.
21 Sanchez, Lin, and Korunka, citing a lecture by Gordon McCormick, in Sanchez, Lin, and Korunka, “Applying Irregular Wafare,” p. 19; Constantin Adrian Ciolponea and Cristian Angel Iancu, also citing a lecture by McCormick, in Ciolponea and Iancu, “Alternative Strategies for Iraq,” Naval Postgraduate School, June 2007, pp. 19-21.
22 Healey, “A Bizarre Pair,” p. 88.
23 Michael Senft, “Lessons Not Learned: Why Our Post-9/11 Counterterrorism Experiences Should Inform Our Cybersecurity Strategy,” *Modern War Institute*, February 28, 2019, mwi.usma.edu/lessons-not-learned-post-9-11-counterterrorism-experiences-inform-cybersecuritystrategy/.

いる[24]。

これらのように、ヒーリー、センフト及びフーレンも対反乱戦、テロ対策及び SOF という観点で、サンチェズと同様にサイバー空間との類似性を論じていることから、「サイバー空間ダイヤモンドモデル」が採用しているような対反乱戦の教訓をサイバー空間に応用する考え方は、学術的な視点として成立すると考える。

図 1 に「サイバー空間ダイヤモンドモデル」の簡略図を示す。このモデルは「調整者（The Controllers）」、「破壊者（The Disruptors）」、「民衆（The population）」及び「統治者（Governance）」における、4 つのアクター間の働きかけ又は相手方の働きかけに対する阻害を、5 つの戦略に分類するものである[25]。

図 1　「サイバー空間ダイヤモンドモデル」の簡略図



番号	戦略の内容
1	民衆の支援
2	情報の阻害
3	直接の活動
4	交流の阻害
5	統治者との関係構築

（出所）Frank C. Sanchez, Weilun Lin, and Kent Korunka, “Applying Irregular Warfare Principles to Cyber Warfare,” Joint Force Quarterly, Iss. 92, 1st Quarter, January 2019 を参考に筆者作成。

まず 4 つのアクターについて説明する。

「調整者」には政策立案者、軍隊等に代表されるような影響力と調整力を持つアクターが定義されている[26]。本稿における「調整者」は、「米国政府機関」又は「韓国政府機関」と定義する。

「破壊者」はサイバー空間を妨害したり、支援したりする人間、機械又

[24] Jonas van Hooren, “The Imperative Symbiotic Relationship between SOF and Cyber: How Dutch Special Operation Forces Can Support Cyber Operations,” Master’s thesis, Naval Postgraduate School, 2019, p. 17.
[25] Sanchez, Lin, and Korunka, “Applying Irregular Warfare Principles to Cyber Warfare,” p. 19.
[26] Ibid., pp. 19-20.

は犯罪者等と定義されている[27]。本稿における「破壊者」の定義は、米国の『米国国家サイバー戦略』及び『国家安全保障戦略』における「戦略的競争相手」に該当する「中国政府機関」とする。

「民衆」は、サイバー空間におけるユーザー（人間）又は情報通信技術（Information Communication Technology: ICT）（機械等）と定義されており、「民衆」は全ての力の源泉としての役割を果たしており、ある立場に支援を提供するまでは中立とされている[28]。

最後に「統治者」について説明する。外部の国家、内部組織、その他の組織が該当するとされ、国立標準技術研究所（National Institute of Standards and Technology: NIST）、ウィキリークス（Wikileaks）[29]及びマイクロソフト（Microsoft Corporation）等が「統治者」の具体例として挙げられている。また、「統治者」もある立場に支援を提供するまでは中立としている[30]。

次に 5 つの戦略について説明する。

「戦略 1　民衆の支援」の意図は、全ての力の源泉である「民衆」の支持を得ることにあるとしている。例えば「調整者」は「破壊者」に関する知識を欠いているため、「破壊者」を特定するために必要な情報を得られるよう「民衆」の支持を必要とするとしている[31]。

「戦略 2　情報の阻害」の意図は、相手方が実施する「戦略 1　民衆の支援」を阻止又は中断することにあるとしている。例えば「調整者」の目的は「破壊者」の情報を無効化し、「破壊者」と「民衆」の間に分裂を生み出すことである[32]。

「戦略 3　直接の活動」の意図は、相手の作戦を混乱させ、紛争を継続する意思と能力を否定するために相手を叩くことにあるとしている[33]。

「戦略 5　統治者との関係構築」の意図は、「統治者」と関係構築することによって、情報の正統性を高めることにあるとしている[34]。

そして、「戦略 4　交流の阻害」の意図は相手方の「戦略 5　統治者との関係構築」を阻害することにあるとしている。具体例として「シャドー・

---

[27] Ibid., p. 20.
[28] Ibid.
[29] *Wikileaks*, October 4, 2006, wikileaks.org.
[30] Sanchez, Lin, and Korunka, “Applying Irregular Warfare Principles to Cyber Warfare,” pp. 20-21.
[31] Ibid., p. 21.
[32] Ibid.
[33] Ibid.
[34] Ibid.

ブローカー（「破壊者」）による米国国家安全保障局（National Security Agency: NSA）の秘密と能力の情報漏洩[35]によって、米国政府（「調整者」）とマイクロソフト（「統治者」）の間の情報の正統性が破壊された事例が挙げられている[36]。

（3）『米国国家サイバー戦略』及び関連政策の分析

『米国国家サイバー戦略』において厳しい対中政策が採用されていることから、「戦略的競争」としての性質が濃い以下の３つの項目に焦点を絞って分析する。

第１の項目として、米国の「サプライチェーンリスク管理に関する戦略及び関連政策」を分析する。

『米国国家サイバー戦略』の 1 つ目の柱である「アメリカ人民、国土、生活様式の保護」[37]における「連邦政府のネットワーク及び情報の安全確保」の中では「連邦政府のサプライチェーンリスク管理」について言及されており、「正当な理由がある場合には、リスクの高いベンダー、製品、サービスを除外するためのより合理的な権限を提供するなど、連邦政府の調達システムの欠陥に対処することも含まれる。」と明記されている[38]。

これは米国の関連政策とも一致しており、『2019 会計年度米国国防権限法（*National Defense Authorization Act for Fiscal Year 2019*: NDAA FY2019）[39]』の中で、米国政府機関に対し、華為技術有限公司（Huawei Technologies Corporation: Huawei）に代表される特定 5 社の中国企業製の通信・監視関連の機器・サービスの購入・取得・利用等を禁止する旨が明記されている。この結果、特定 5 社に該当する中国企業が米国政府機関と取引をすることが困難になるとともに、2・3 次サプライヤーの場合も確認が求められることから、既存の市場に大きな影響があると一般財団法人

[35] Ellen Nakashima and Craig Timberg, “NSA Officials Worried about the Day Its Potent Hacking Tool Would Get Loose. Then It Did,” *Washington Post*, May 16, 2017, cyber-peace.org/wp-content/uploads/2017/05/NSA-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose.-Then-it-did.pdf.
[36] Sanchez, Lin, and Korunka, “Applying Irregular Warfare Principles to Cyber Warfare,” pp. 21-22.
[37] The White House, *National Cyber Strategy of the United States of America*, pp. V-VI.
[38] Ibid., p. 7.
[39] *NDAA 2019 (Public Law 115-232)*, 115st Congress, August 13, 2018, pp. 1917-1919.

安全保障貿易情報センター事務局は分析している[40]。

これまで「破壊者」である中国がサプライチェーンを悪用して、米国政府機関のICT機器の中に脆弱性を確保しようとした働きかけ及び安価な価格設定で契約を勝ち取ろうとした働きかけは「サイバー空間ダイヤモンドモデル」における「戦略 1　民衆の支援」及び「戦略 5　統治者との関係構築」に該当する。

他方、『米国国家サイバー戦略』及び『2019 会計年度米国国防権限法』は、これらのような「破壊者」の働きかけを阻害できる一連の戦略及び政策と言え、「サイバー空間ダイヤモンドモデル」における「戦略 2　情報の阻害」及び「戦略 4　交流の阻害」に該当すると言える。

次に第 2 の項目として、米国の「海底ケーブル通信管理に関する戦略及び関連政策」を分析する。

『米国国家サイバー戦略』の 1 つ目の柱である「アメリカ人民、国土、生活様式の保護」の「重要インフラの安全確保」の中で「連邦政府は民間部門と協力して､最大のリスクに晒されている重要インフラ(国家安全保障、エネルギーと電力、銀行と金融、健康と安全、通信、情報技術、輸送）へのリスクを管理する。」と明記されている[41]。

民間部門との協力は､『重要インフラの安全保障及びその復旧に関する大統領政策指示（*Presidential Policy Directive*: PPD-21)』[42]として 2013 年 2 月に既に発出されており、本件についてはオバマ政権の政策が継承されていると言える。

ナディア・シャドロー（Nadia Schadlow）らは、国際的な境界を越えるデータの約 95%を海底ケーブル通信が転送する中で、Huawei の子会社である Huawei Marine は、世界の約 400 本の海底ケーブル通信のほぼ 4 分の 1 を建設または修理したと分析している[43]。海底ケーブル通信は、サイバー空間を構成する最も主要な部分の一つであることから、本稿では、数

---

40 「米国国防権限法 2019 の概要」一般財団法人安全保障貿易情報センター事務局、2019 年 3 月 19 日、www.cistec.or.jp/service/uschina/5-ndaa2019_gaiyou.pdf。

41 The White House, *National Cyber Strategy of the United States of America*, pp. 8-9.

42 The White House, *Presidential Policy Directive - Critical Infrastructure Security and Resilience* -, February 12, 2013.

43 Nadia Schadlow and Brayden Helwig, "Protecting Undersea Cables Must Be Made a National Security Priority," *Defense News*, July 1, 2020, www.defensenews.com/opinion/commentary/2020/07/01/protecting-undersea-cables-must-be-made-a-national-security-priority/.

ある重要インフラの中でも海底ケーブル通信に焦点を絞って分析する。

米国国土保全保障省（Department Homeland Security: DHS）と米国国家情報長官室（Office of the Director of National Intelligence）は『海底ケーブル通信に対する脅威（*Threats to Undersea Cable Communications*）』[44]を 2017 年 9 月に公表し、海底地震からサイバー攻撃に至るまでの海底ケーブルに対する幅広いリスクを分析し、推奨事項を提言している。

また、安全保障の観点から海底ケーブル通信の敷設申請を審査する「チーム・テレコム」が、国土安全保障省の主導の下に国防・国務・司法省等の職員で構成されるとともに、2008 年には国土安全保障省、連邦通信委員会（Federal Communications Commission: FCC）、科学技術政策室が、全米の海底通信ケーブル会社からセキュリティ情報の任意提出を求めている等の対策をとっていると矢野哲也[45]は分析している。

これまで「破壊者」である中国が海底ケーブル通信の遮断や盗聴が可能な環境を構築しようとした働きかけ[46]や、契約を勝ち取ろうとした働きかけは、「サイバー空間ダイヤモンドモデル」における「戦略 1　民衆の支援」及び「戦略 5　統治者との関係構築」に該当する。

他方、『米国国家サイバー戦略』、『海底ケーブル通信に対する脅威』及び「チーム・テレコム」等は、これらの「破壊者」の働きかけを阻害できる一連の戦略及び政策と言え、「サイバー空間ダイヤモンドモデル」における「戦略 2　情報の阻害」及び「戦略 4　交流の阻害」に該当する。

最後に第 3 の項目である、米国の「サイバー犯罪対策に関する戦略及び関連政策」を分析する。

『米国国家サイバー戦略』の 1 つ目の柱である「アメリカ人民、国土、生活様式の保護」の「サイバー犯罪との戦いと事案報告の改善」の中では、「我々は、欧州評議会の『サイバー犯罪条約（ブダペスト条約）』[47]を支持する国際的なコンセンサスを拡大するために、同条約の採択拡大を支援す

---

[44] U.S. Department of Homeland Security and Office of the Director of National Intelligence Public-Private Analytic Exchange Program 2017, *Threats to Undersea Cable Communications*, September 28, 2017, pp. 7-8.

[45] 矢野哲也、「海底通信ケーブル防護のための日本の海洋ストラテジック・コミュニケーション」『21 世紀研究』第 10 号、2019 年 3 月、5 頁。

[46] Schadlow and Helwig, “Protecting Undersea Cables Must Be Made a National Security Priority.”

[47] 「サイバー犯罪に関する条約（略称：サイバー犯罪条約）」外務省、2012 年 11 月、www.mofa.go.jp/mofaj/gaiko/treaty/treaty159_4.html。

ることを含めて努力する。」と明記されている[48]。

最近の米国のサイバー犯罪対策に関する政策として、ウクライナの停電や 2018 年の平昌冬季オリンピック等へのハッキングに関与したとしてロシア軍参謀本部情報総局（Glavnoje Razvedyvatel'noje Upravlenije: GRU）に所属する 6 人のハッカーが米国司法省によって 2020 年 10 月に訴追された事例がある[49]。米国司法省は 2018 年に中国のハッカーを訴追[50]してからこのような政策を継続している。

これまで「破壊者」である中国が「全ての力の源泉」とされている「民衆」を利用して、「民衆」の中に隠れてサイバー攻撃を実行しようとした働きかけは、「サイバー空間ダイヤモンドモデル」における「戦略 1　民衆の支援」に該当する。

他方、米国は『サイバー犯罪条約』採択拡大を支援したり、「破壊者」の一員であるハッカーを全世界に指名手配する取り組みをしたりしている。これらの取り組みは「破壊者」と「民衆」の間に疑念や分裂を生み出し、両者の関係や情報の阻害に効果があると期待できることから、「サイバー空間ダイヤモンドモデル」における「戦略 2　情報の阻害」に該当する。

以上から、『米国国家サイバー戦略』及び関連政策においては、「サイバー空間ダイヤモンドモデル」における「戦略 2　情報の阻害」及び「戦略 4　交流の阻害」といった相手方の働きかけを阻害するような戦略を取り入れており、「戦略的競争相手」に位置付けている中国に対して有利な環境を構築することを目指していると考えられる。

（4）韓国国家サイバー安保戦略及び関連政策の分析

はじめに、前項と同様に「サプライチェーンリスク管理に関する戦略及び関連政策」について分析する。

『韓国国家サイバー安保戦略』の中では、サプライチェーンリスク管理

---

48 The White House, *National Cyber Strategy of the United States of America*, p. 11.

49 Department of Justice United States of America, “Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace,” October 19, 2020, www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

50 Department of Justice United States of America, “Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information,” December 20, 2018, www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion.

について直接言及した箇所は存在しない。唯一、関連する記載としては、第 4 の柱である「サイバーセキュリティ産業の成長基盤の構築」[51]の「公正競争の原則の確立」の中で、「価格中心から性能中心に改善して技術競争の激しい市場で体質を強化」及び「サイバーセキュリティサービスの正当な対価を支払うための方案を講じ、不法下請けなどを徹底的に調査・是正」という内容が明記されている[52]が、これらはサプライチェーンリスク管理ではなく、あくまでも調達の適正化を確保するための戦略に過ぎない。

韓国の関連政策においてもサプライチェーンリスク管理が見当たらないことから、米国と異なり、「サイバー空間ダイヤモンドモデル」における「戦略 2　情報の阻害」及び「戦略 4　交流の阻害」に該当する戦略や政策をとれていないと言える。

次に「海底ケーブル通信管理に関する戦略及び関連政策」を分析する。

『韓国国家サイバー安保戦略』では重要インフラについて、第 1 の柱である「国家の重要インフラの安全性向上」[53]の中で、「サイバー攻撃時の被害が大きい主な基盤施設を迅速に国が指定・保護できるよう関連制度の改善」、「主な基盤施設を運営する機関が一定割合以上の予算を確保できるよう支援を強化」等について明記している[54]。

しかし、米国のように、国家が積極的に民間に協力して重要インフラを防護するという記述は『韓国国家サイバー安保戦略』及び関連政策には見られない。

ショーン・オマリー（Sean O'Malley）は、重要インフラ防護の中で海底ケーブル通信に関して、韓国政府の注意が欠如していることは、壊滅的なものになる可能性があると警鐘を鳴らしている[55]。また、オマリーは軍事的パートナーである米国と韓国が海底ケーブル通信陸揚げ局を重要インフラとして共有していないことは奇妙であると指摘している[56]。オマリーによる警告例として、F-35 戦闘機は自律型兵站情報システム（Autonomous Logistics Information System: ALIS）と常に接続していないと効果的に運用できず、仮に切断された場合は全能発揮が不可能となる恐れがあるとと

---

51 韓国国家安保室『국가 사이버 안보 전략』3 頁。
52 同上、21 頁。
53 同上、3 頁。
54 同上、15 頁。
55 Sean O'Malley, "Assessing Threats to South Korea's Undersea Communications Cable Infrastructure," *The Korean Journal of International Studies*, Vol. 17, No. 3, December 2019, p. 386.
56 Ibid., pp. 389-390.

もに、海底ケーブル通信の信頼性に部分的に依存していることから、米韓の軍事同盟に対する脅威になり得ることを挙げている[57]。

このことから、韓国は海底ケーブル通信に関して、米国と異なり、「サイバー空間ダイヤモンドモデル」における「戦略 2　情報の阻害」及び「戦略 4　交流の阻害」に該当する戦略や政策をとれていないと言える。

最後に「サイバー犯罪対策に関する戦略及び関連政策」を分析する。

『韓国国家サイバー安保戦略』ではサイバー犯罪対策として、第 6 の柱である「サイバー安保国際協力の主導」[58]の中で、「サイバー安保関連の普遍妥当な国際規範成立過程への参加を拡大し、国際規範とベストプラクティス普及をリードする。」と明記している[59]。

しかし、韓国は欧州評議会の『サイバー犯罪条約』を未だに批准していない[60]。『韓国国家サイバー安保戦略』には「国際規範成立過程への参加を拡大し」と記載されているが、『サイバー犯罪条約』は 2004 年に既に発効している[61]ことから、「国際規範成立過程」とは『サイバー犯罪条約』とは異なるものを指している可能性がある。

他方、2011 年に中国、ロシア、タジキスタン及びウズベキスタンは、国連事務総長宛に『情報セキュリティのための国際行動規範』を提出している[62]。本件について、中国は近年「サイバー大国」として台頭が著しいが「欧州評議会は（世界全体と）関係ない」として自国が参加しない形で作成された『サイバー犯罪条約』への加盟を拒否していると須田祐子は分析している[63]。

このことから、韓国はサイバー犯罪に関して、米国等と異なり『サイバー犯罪条約』を批准しておらず、むしろ中国等の『情報セキュリティのための国際行動規範』に合意するともとれる政策をとっていると言える。

以上から、韓国は米国と異なり、「サイバー空間ダイヤモンドモデル」における「戦略 2　情報の阻害」及び「戦略 4　交流の阻害」に該当する戦略

---

57 Ibid., p. 390.

58 韓国国家安保室『국가 사이버 안보 전략』3 頁。

59 同上、23 頁。

60 Hannes Ebert and Laura Groenendaal, “Cyber Resilience and Diplomacy in the Republic of Korea: Prospects for EU Cooperation,” *EU Cyber Direct*, August 2020, eucyberdirect.eu/wp-content/uploads/2020/08/digital-dialogue-rok.pdf.

61 指宿信「サイバー犯罪条約およびその国内法化について」『刑法雑誌』第 45 巻第 1 号、2005 年 7 月、123 頁。

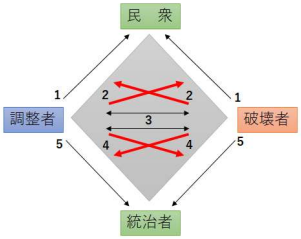
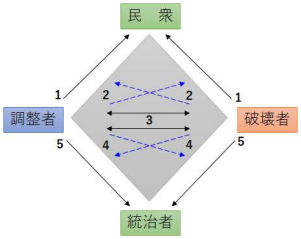
62 『情報セキュリティのための国際行動規範』国連、2011 年 9 月、digitallibrary.un.org/record/710973。

63 須田「サイバーセキュリティの国際政治」60 頁。

又は政策をとれていないと言える。

米国は『米国国家サイバー戦略』において中国を「戦略的競争相手」として定義しているが、韓国は「戦略的競争相手」が不明確であり、相手方の働きかけを阻害する戦略を設定できない状況に陥っている。この米韓のサイバー戦略の相違点の分析結果を図 2 に示す。

図 2　「サイバー空間ダイヤモンドモデル」による米韓サイバー戦略の分析

国	米　国	韓　国
サイバー空間ダイヤモンドモデル		
総　括	戦略２及び４が機能している。 ⇒破壊者の行動を阻害するための戦略化可能	戦略２及び４が機能していない。 ⇒破壊者の行動を阻害するための戦略化不可

（出所）Frank C. Sanchez, Weilun Lin, and Kent Korunka, “Applying Irregular Warfare Principles to Cyber Warfare,” Joint Force Quarterly, Iss. 92, 1st Quarter, January 2019 を参考に筆者作成。

以上から、ルパート・スミス（Rupert Smith）が「敵が明確に規定されていなければ、戦略を策定できないし、戦略がなければ兵器や装備についての非常に漠然とした決定以外には何も決められない。」と指摘している[64]とおり、米韓におけるサイバー戦略の根本的な相違点は「敵」すなわち「戦略的競争相手」が明確に定義されているか否かであると考える。

3　サイバー戦略の相違点による負の影響とその背景

（1）サイバー戦略の相違点による負の影響

まず 1 つ目は、サプライチェーンリスク管理の点についてである。サプライチェーンリスク管理の相違により、米韓における情報セキュリティの

64 ルパート・スミス『軍事力の効用：新時代「戦争論」』山口昇監修、佐藤友紀訳、原書房、2014 年、370 頁。

水準に差異が生じる可能性がある。その結果、情報システムの連接や、共有する情報の保全を確保する上で、脆弱性を生みかねないという負の影響が発生し得る。

2 つ目は、海底ケーブル通信管理の点についてである。海底ケーブル通信管理の相違により、両国間を接続する海底ケーブル通信における情報セキュリティの水準に差異が生じる可能性がある。その結果、海底ケーブル通信を経由した情報システムの連接や、共有する情報の保全を確保する上で、脆弱性を生みかねないという負の影響が発生し得る。

3 つ目は、サイバー犯罪対策の点についてである。夏井高人は『サイバー犯罪条約』の起草段階において、コンピュータネットワークを利用した犯罪には国境を越えて実行されるものが多いことから、関連各国内で共通した刑罰法令を持つことの重要性が認識された経緯があると分析している[65]。韓国が『サイバー犯罪条約』を批准しないことは、米韓における刑罰法令が共通化されない状況が継続する可能性があることから、サイバー犯罪対策における脆弱性を生みかねないという負の影響が発生し得る。

（2）サイバー戦略に相違点が発生する背景についての考察

まず、サプライチェーンリスク管理について考察する。RAND 研究所の非常勤研究者であるイ・ジヨン（Lee Ji-Young）は、ターミナル段階高高度地域防衛システム（Terminal High Altitude Area Defense: THAAD）の配備の際に中国が猛反発した経験の後[66]、中国は 2019 年に韓国で 4 位の輸出先かつ最大の輸入元となっていることから、韓国内の経済的配慮とビジネス感情によって、米国が採用している Huawei 等の禁止政策に公然と参加しないことを選択した可能性があると分析している[67]。

このことから、サプライチェーンリスク管理について、韓国が経済・外交政策における中国の反発を恐れ、譲歩せざるを得ないと判断している可能性があると言える。

次に、海底ケーブル通信について考察する。韓国、米国及び中国等を接続する海底ケーブル通信の一つに「New Cross Pacific（NCP）Cable System」

---

65 夏井高人「サイバー犯罪条約の主要論点」『法律論叢』、第 75 巻第 2・3 合併号、2002 年 12 月、261 頁。

66 山﨑周「『暗黙の容認』から顕在的な脅威へ：中国の米韓同盟に対する脅威認識と中韓関係の変遷」『青山国際政経論集』第 104 号、2020 年 5 月、64 頁。

67 Ji-Young Lee, “The Geopolitics of South Korea–China Relations Implications for U.S. Policy in the Indo-Pacific,” *RAND Corporation*, 2020, p. 12, www.rand.org/pubs/perspectives/PEA524-1.html.

がある。これはコンソーシアム方式で運営されている[68]が、中華電信（China Telecom: CT）、中国移動通信（China Mobile: CM）及び中国聯通（China Unicom: CU）の中国情報通信企業が 50%の過半数を所有している唯一のケーブルシステムであるとともに、中国における陸揚げ局の状況が未確認であることから、米中貿易摩擦の文脈では疑問を投げかけるだろうとスヴェシュ・チャッドパダヤヤ（Suvesh Chattopadhyaya）は警鐘を鳴らしている[69]。これは米韓間の通信が中国に経由され盗聴される可能性が排除できないことを意味しているものと考えられる。

このような状況から、海底ケーブル通信管理についても、韓国が中国の反発を恐れ、譲歩せざるを得ないと判断している可能性は否定できないと考えられる。

最後にサイバー犯罪対策の点を考察する。韓国は未だに『サイバー犯罪条約』を批准していない。また中国らが主張する『情報セキュリティのための国際行動規範』に合意するとも読み取れる表現が『韓国国家サイバー安保戦略』に存在する[70]。このことから、サイバー犯罪対策についても、韓国が中国の反発を恐れ、譲歩せざるを得ないと判断している可能性があると考えられる。

本項を総括して、米韓のサイバー戦略の相違点によって発生する 3 つの負の影響及び背景を図 3 に示す。

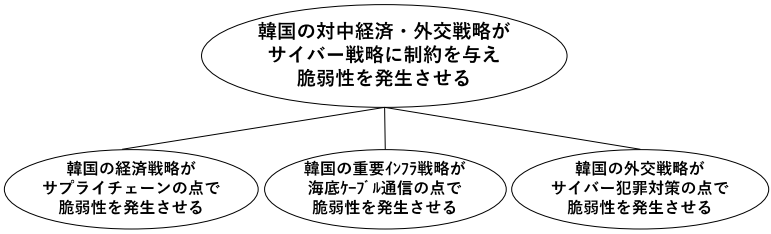
---

68 O'Malley, "Assessing Threats to South Korea's Undersea Communications Cable Infrastructure," p. 388.

69 Suvesh Chattopadhyaya, "15 Submarine Cable Systems - Facing Tough Time, Boldly!" *Submarine Cable Networks*, December 6, 2019, www.submarinenetworks.com/en/insights/15-submarine-cable-systems-facing-tough-time.

70 韓国国家安保室『국가 사이버 안보 전략』23 頁。

図 3　米韓のサイバー戦略の相違点によって発生する 3 つの負の影響及び背景



	サプライチェーン（HUAWEI等）	重要ｲﾝﾌﾗ（海底ｹｰﾌﾞﾙ通信）	サイバー犯罪対策（サイバー犯罪条約）
ﾀﾞｲﾔﾓﾝﾄﾞﾓﾃﾞﾙ	戦略４　交流の阻害		戦略２　情報の阻害
米　国	米国国防権限法2019によってHUAWEI等を禁止	・政府が積極的に民間と連携 ・安全保障の観点で審査	・ｻｲﾊﾞｰ犯罪条約の採択拡大追求 ・米司法省がGRUのﾊｯｶｰを訴追
韓　国	THAADの教訓を踏まえ、経済政策として、HUAWEI等を排除しないことがﾘｰ（RAND非常勤研究者）により指摘	・韓国は海底ｹｰﾌﾞﾙ通信の政策が欠落とｵﾏﾘｰにより指摘 ・米韓中を結ぶNCPｹｰﾌﾞﾙは不明確かつ中国企業が過半数保有	韓国はｻｲﾊﾞｰ犯罪条約を未だ批准していない（中国、ロシアはｻｲﾊﾞｰ犯罪条約に反対の立場）

（出所）本稿第 3 章（図 3 を除く。）を元に筆者作成。

韓国が中国に譲歩せざるを得ないと判断している状況は、中国の戦略及び政策によって意図的に作り出されている可能性がある。山﨑周は、中国国内には自国の巨大な経済的パワーを利用することによって、米韓同盟を弱体化させたり、あるいは瓦解させたりすることができ得ることから、米国による対中包囲網の打破のための突破口にできるとの見解があると分析している[71]。THAAD 配備の際の中国の猛反発は、この分析の妥当性を示す事例の一つであると考える。

おわりに

本稿では、米韓のサイバー戦略の根本的な相違点は「敵」すなわち「戦略的競争相手」が明確に定義されているか否かであり、これによって、「サプライチェーンリスク管理」、「海底ケーブル通信管理」及び「サイバー犯罪対策」において、サイバー空間上の安全保障を不利とするような負の影響を生み出していることを導出した。

さらに、必要なサイバー戦略を制定できない状況の背景には、韓国が経済及び外交政策面等で中国の反発を恐れ、譲歩せざるを得ないと判断している可能性があることを考察した。

[71] 山﨑「『暗黙の容認』から顕在的な脅威へ」69 頁。

日本は米国と同盟関係にある。本稿では韓国を対象としたが、今後、日本の『サイバーセキュリティ戦略』[72]及び関連政策に関する米国との相違点を分析することができれば、日本の『サイバーセキュリティ戦略』を改正する際の資とすることができると考える。

[72]『サイバーセキュリティ戦略』内閣サイバーセキュリティセンター、2018 年 7 月。