NIDS 防衛研究所
The National Institute for Defense Studies

「サイバー『防衛』外交」の視点－日 ASEAN 協力を事例として

原田　有　政策研究部グローバル安全保障研究室

NIDSコメンタリー
第 94 号 2019 年 3 月 14 日

はじめに

現在、新世代の移動通信システム「5G」をめぐる米中覇権争いへの注目が高まっている。この争いは、「サイバー空間の在り方」という同空間に係る本質的問題を内在させているが、それは従来から論争の的となってきた。そして、その解決に向けた外交的取組の重要性が強調されるに伴い、欧米の政策実務では「サイバー外交（Cyber Diplomacy）」の意義が認識され始めた。もっとも、その定義等は学術的研究が緒に就いたばかりということもあり明確ではない。そこで本稿は、「サイバー外交」への理解と議論を深めるべく、政策が推進された背景、並びにこのテーマを扱った先駆的論考を概観するとともに、外務当局だけでなく防衛当局にも焦点を当てた「サイバー『防衛』外交」の視点の必要性を提起する。その上で、この分野での日本の取組の現状と課題を各種政府文書、日 ASEAN 協力を事例に論考する。

「サイバー外交」の意義の高まりと問われる防衛当局の役割

「サイバー外交」の意義は、ここ 10 年程で欧米の政策実務で認識され始めた。その先駆けとなった政策として、2011 年 5 月にバラク・オバマ米政権が公表した「サイバー空間に関する国際戦略」が挙げられる[1]。同戦略は「サイバー外交」という表現こそ用いていないものの、「外交、防衛、発展」をキーワードに、基本的自由、プライバシー、情報の自由な流通を含む核心的原則の擁護や既存の国際法のサイバー空間への適用、規範の確立に向けた友好国との協力や諸外国における能力構築の促進を標榜し、また非国家主体も含めたマルチ・ステークホルダーによるインターネットガバナンスの重要性を謳う内容であった。一方、欧州連合（EU）では 2015 年 2 月に「サイバー外交に関する決議」が採択された[2]。そこでも米国の戦略と同様に、サイバー空間における人権や基本的自由の保障、既存の国際法の適用、マルチ・ステークホルダーによるガバナンスの強化、第 3 国の能力構築支援、キーパートナーとの戦略的関与の強化等を目的とする包括的な外交アプローチの方向性が示されたのである。

このようにサイバー空間での外交的取組が重視され始めた背景には、同空間に関わる問題の深刻化・複雑化があった。サイバー犯罪は巧妙化し、さらに国家の関与が疑われるサイバー攻撃事案も相次いで表面化した。これに伴い、サイバー空間における国家の責任ある行動が問われるようなったが、そもそもこの空間がいかなるルールによって統御され、そこに国家がどのように、またどの程度関与するのかも一大論点であった[3]。この点につき、既述のように欧米は既存の国際法のサイバー空間への適用、空間における自由（表現や通信等）の確保、マルチ・ステークホルダーによるガバナンスを主張し、日本もこの立場を共有した。対照的に、中露をはじめとした上海協力機構加盟国等は、サイバー空間に関する新たな行動規範の策定や国家を中心的な行為主体とするガバナンスを求め、異なる見解が角逐したのである。サイバー空間に関わる問題が、安心・安全な情報通信技術の利活用の推進といった技術的な範疇を超えて、空間の在り方をも問うものへと政治的な様相を強めてきたところに国家の外交的取組、すなわち「サイバー外交」の余地は生まれたといえる。

他方、「サイバー外交」の定義や意義には不明確な部分も多く残される。その一因として、政策実務での注目の高まりとは対照的に、このテーマが学術的研究で扱われることは限られてきた点が挙げられる。この乖離が次第に問題視されるようになり、最近になって議論の整理が試みられ始めた。例えば、ある先駆的論考は、「サイバー外交」を「外交的資源の活用や外交的機能の発揮を通じて、サイバー空間に係る国益を確保すること」と定義した[4]。より具体的には、サイバー空間に係る安全保障の確保、サイバー犯罪への対処、信頼醸成、インターネットガバナンスの構築といった課題がある中、当該外交は、サイバー空間を「国家が戦略的利益の角逐を広げる空間」ではなく、「明確なルールや原則に基づいた非国家主体も参画する平和的な共存の空間」へと導くことを目指しているとし、それに資する欧米諸国を主とした外務当局の取組に着目する研究アプローチを示した。また、それ故、ソーシャルメディア等を用いて外交を展開する「デジタル外交」、あるいは法務や情報通信、経済産業といった分野に関する優れて技術的な国家間協力は議論の射程に含まれないと整理したのである。

こうした議論は、「サイバー外交」の学術的研究の素地を整えるものとして注目される一方、議論を深めるべき余地もある。例えば、定義にある「外交的資源・機能」が意味するところは明確ではなく、それらは外務当局のみが有するものなのかという疑問が残される。この文脈で「防衛外交」の議論は注目に値する[5]。すなわち、防衛当局ならではのアセットや専門性が、信頼醸成、能力構築支援、民主化支援等において、外務当局にはない独自の役割を外交で果たし得ると考えられている点は、「サイバー外交」の文脈でももっと注目されて良い。既に一部の論考では、各国の防衛当局が実空間で取組む政策の透明性向上や紛争管理を目的とした信頼醸成措置（CBM）等の射程をサイバー空間に広げるべきことや、そのための二国間・多国間防衛協力・対話の推進が提起されているところでもある[6]。

もっとも、サイバー空間での「防衛外交」が政策実務でどのように展開していくのかは未知数である点には留意も要する。サイバー分野に係る防衛当局の取組は機微な情報を含み、自国の手の内を明かすことにもなりかねない協力・対話の実施は机上で想定されるほど容易ではない。また、サイバー空間における CBM の具体的方法や内容は議論の途上にある[7]。そもそも、各国の防衛当局の最大の課題は自らの指揮通信システムの保守にあり、人材や予算に制約がある中、外交に割ける余力は限られてもいる。こうした政策実務の現状を念頭に置きつつも、少なくとも学術的研究上では、いわば「サイバー『防衛』外交」の視点も取り入れた、「サイバー外交」の多層性を捉えた議論が必要だと考えられる。

開かれてきた日本の「サイバー外交」の地平

さて、これまでの議論を踏まえ、次にこの分野における日本の取組の現状と課題を論考したい。以下ではまず、各種政府文書を参照してサイバー空間に係る日本の外交的取組の変遷を跡付ける。これによって、日本でも「サイバー外交」の地平が漸進的に開かれ、さらにそこへの防衛省の関与の在り方が問われる局面に差し掛かってきたことを論じる。

日本政府はサイバー空間における国際連携の必要性を一貫して提起してきた。日本として初めてのサイバー空間に係る体系的な計画となった「第 1 次情報セキュリティ計画」（2006 年 2 月）の策定以降、政府は「第 2 次情報セキュリティ計画」（2009 年 2 月）、「国民を守る情報セキュリティ戦略」（2010 年 5 月）と相次いで包括的な計画・戦略を定めてきた。それらの中で国際連携の重要性は、国境にとらわれずに拡散するサイバー空間に係る脅威や障害への対処という、主に技術的な文脈から強調されてきた。

その後、日本の取組は次第にサイバー空間の在り方とその問題への外交的関与をより強く意識したものへと変化していった。このことは、2013 年 6 月の「サイバーセキュリティ戦略」（2013 年戦略）の策定に明確に示された。同戦略は、「『情報セキュリティ』確保のための取組はもとより、広くサイバー空間に係る取組を推進する必要性と取組姿勢を明確化」[8]すべく策定されたものである。そこでは、「情報の自由な流通の確保」が日本の取組の主

たる原則と位置付けられ、「国家による過度な管理や規制が行われることなく、開放性や相互運用性を確保しつつ、安全で信頼できるサイバー空間を構築するバランスのとれたアプローチを促進するための外交」の必要性が提起された[9]。さらに、「民主主義、基本的人権の尊重及び法の支配といった基本的な価値観を共有する国や地域」との連携強化、既存の国際法のサイバー空間への適用に向けた取組、信頼醸成措置や ASEAN を念頭に置いた新興国・途上国を対象にする能力構築支援等の推進も掲げられたのである[10]。

こうした方針は、日本初の国家安全保障戦略（2013 年 12 月）、サイバー分野の法的基盤を強化した「サイバーセキュリティ基本法」（2014 年 11 月）にも盛り込まれた。また、同基本法に基づき 2015 年 9 月と 2018 年 7 月に改訂された「サイバーセキュリティ戦略」でも、基本原則を「情報の自由な流通の確保」、「法の支配」、「開放性」、「自立性」、「多様な主体の連携」へと再整理した上で、日本の国益に資するサイバー空間を実現すべく国際連携を進めていくことが改めて確認された[11]。そして、今や外務省は「サイバー空間における法の支配の推進」、「信頼醸成」、「能力構築」を柱とする「サイバー外交」の積極的な推進を掲げるに至ったのである[12]。

2013 年戦略は日本の「サイバー外交」の地平を開く分水嶺になったといえる。こうした変化の背景として、既述したサイバー空間に関わる問題の深刻化・複雑化に加えて、折しも日本がサイバー空間に適用するルール・規範を議論していた国連の政府専門家会合（GGE）に初参加する機会（2012 年 8 月）を得ていたことが指摘できる。GGE への参加に当たり、日本は空間に係る基本原則や方針について、欧米と歩調を合わせる形に自らの旗幟を鮮明にする必要性に直面していたといえる。

さて、こうしてみた時、日本の「サイバー外交」の 1 つの力点が能力構築支援に置かれてきたことに気付く。実際、2016 年 10 月には「サイバーセキュリティ分野における開発途上国に対する能力構築支援（基本方針）」も策定されている。同方針は、注力すべき支援分野を「インシデント・レスポンス等の能力の向上支援」、「サイバー犯罪対策支援」、「サイバー空間の利用に関する国際的ルール作り及び信頼醸成措置に関する理解・認識の共有」に整理し、ASEAN との協力を念頭に置きつつ、「日本の強み（アセット）を活かす形で支援を行う」ことを示したものである[13]。そうした取組を通じて、「情報の自由な流通や法の支配を基本原則とする日本の立場への理解を対象国に浸透させる」[14]ことを目的の 1 つに挙げる同方針は、優れて技術的な協力の域を超えて、日本が望むサイバー空間の実現を図る趣旨も含むものとなっている。

ここで注目されるのは、この方針がこれまで対 ASEAN 協力で中心的役割を担ってきた内閣サイバーセキュリティセンター（NISC）、総務省、経済産業省だけでなく、外務省や防衛省等も含む関係省庁等の連名で公表された点である。そこからは、日本の「サイバー外交」が多層性を持つように設計されていることが伺える。折しも、防衛省は最新の防衛計画の大綱（2018 年）でサイバー空間の規範形成に係る取組の推進を掲げたところであるが、まさにこうした取組を「サイバー外交」の文脈に位置付けて、その発展を検討していくことが求められているといえる。各種政府文書の変遷を追跡すると、日本の取組が「サイバー『防衛』外交」の在り方を検討すべき局面を迎えていることが浮き彫りとなる。

サイバー空間に係る日 ASEAN 協力

それでは、日本の取組は実践面ではどのような状況と課題に直面してきたのか。この点を論考すべく、次に日本が重視してきた ASEAN との協力を考察する。

サイバー空間に係る日 ASEAN 協力は、NISC や総務省、経産省による取組を主として、他の国や地域との協力よりも先駆けて推進されてきた。例えば、ASEAN 加盟国の経済・投資関係省庁及び情報通信

関係省庁を相手とする「日 ASEAN 情報セキュリティ政策会議」は 2009 年 2 月に初会合を設け、以降、ほぼ毎年開催されている[15]。その背景には、日本からの対 ASEAN 投資の増加や日 ASEAN 包括的経済連携協定の発効（2008 年から 2010 年）にみられる経済協力関係の深化があった。こうした状況を受けて、安心・安全なビジネス環境・情報通信ネットワークを構築し、もって経済発展を下支えするという、優れて技術的な取組を主に両者の協力は進められてきたのである[16]。

こうした ASEAN との協力は、日本が掲げる「自由で開かれたインド太平洋」の実現という文脈もあって、ますます重要性を増していくと考えられる。実際、ASEAN では今後、鉄道や道路といったハード面に加えて、情報通信等のソフト面での連結性向上も見込まれる。さらに、各国の防衛当局はますます指揮通信システムに依存する形に防衛力整備を進めていくだろう。それらに伴い、情報通信インフラの整備はもとより、サイバーセキュリティに係る能力や体制の整備に向けた日本の能力構築支援に対するニーズはより高まっていくことが想定される。既に ASEAN 各国では「5G」の導入が大きな話題となっているが、「一帯一路」構想の下、「デジタル・シルクロード」と銘打った取組を推進している中国がファーウェイや ZTE を通じて東南アジアへの関与を強めているところでもある[17]。

ここで論点となるのは、これまで技術的協力を主としてきた対 ASEAN 協力で、日本はどのように「サイバー外交」を推進していけるかという点である。その兆しは、わずかながら現れ始めている。2013 年 9 月に初の閣僚級会議として「日 ASEAN サイバーセキュリティ協力に関する閣僚政策会議」が開催された際、安倍総理の冒頭挨拶では、日本の「サイバー外交」の基本原則である「情報の自由な流通の確保」に向けた ASEAN 各国との協力が呼びかけられた[18]。さらに、従来、NISC、総務省、経産省が参加してきた「日 ASEAN 情報セキュリティ政策会議」には、2016 年 10 月以降、外務省も参加し始めたのである。

ただし、その前途は多難である。そもそも、日本の基本原則である「情報の自由な流通の確保」は ASEAN 諸国に容易に共有されるものではない。ASEAN の中には国家が強い権限を持って情報通信を統制・管理することに肯定的な国もあり[19]、むしろ中露が追求するサイバー空間の在り方に親和性を持ち得る素地すら存在する。先に触れた日 ASEAN 閣僚政策会議の共同声明で、「規制手段が導入される際には、情報の流通を維持し、経済活動を促進するため、十分な配慮」をすべきことが盛り込まれた一方[20]、安倍総理の冒頭挨拶にはあった「自由」の 2 文字が落とされたところに日本と ASEAN と立場の違いが垣間見える。

こうしてみると、対 ASEAN 協力を従来通りの技術的協力にとどめておくことも現実的な選択肢に映る。しかし、サイバー空間の在り方に関して異なった立場にある中国が ASEAN でのプレゼンスを強めている状況を看過することが日本にとって適切な政策であるとも言い難い。要するに、ASEAN は日本の「サイバー外交」の真価を問う地域になるといえそうである。もっとも、そこで日本に求められることは、ASEAN に日米欧か中国かの二者択一を迫ることではない。「5G」の例をみても、多くの国にとって中国は魅力的かつ必要なパートナーとして映っているのであり、その影響力の完全な排除を目指すことは現実的ではない。また、そもそも ASEAN の行動様式は両者の二者択一を是とするものでもない[21]。むしろ、日本の取組の要点は、中国と協力できるところは協力しつつも、戦略的自立性を損なうような中国への極端な依存もまた望まないだろう ASEAN の行動様式を踏まえて中国の影響力の相対化を図るとともに、ASEAN とも共有できるサイバー空間の在り方への検討を深めていくことにあると考えられる。

この文脈で、先に挙げた能力構築に関する基本方針が ASEAN でどのように具現化されていくのかは興味深い論点となる。特にその一翼を担う防衛省がいかなる役割を果たしていけるのかは注目に値する。そもそも防衛省はこれまでにも、ASEAN 諸

国の防衛当局とサイバー空間をめぐる協力を漸進的ながら進めてきた。技術動向等に関する意見交換を目的とする IT フォーラムをシンガポール、ベトナム、インドネシアと実施し、それを踏まえて、2017 年末にはベトナムを対象に初めてのサイバー分野に関する能力構築支援事業も実施した。同事業は、他の ASEAN 諸国との協力を推進する際のモデルを提供し得るものでもある。ただし、こうした取組は緒に就いたばかりであり、また規模や内容も限定されている。実際のところ、特に人材面で厳しい現状に直面している防衛省ができることには自ずと限界もある。

他方、ASEAN 各国との防衛当局間ネットワークは、非防衛当局間の協力を補完するという点で、それ自体が防衛省のアセットであり、日本の「サイバー外交」を多層化させる意義を有することは過小評価すべきではない。その重要性は、ASEAN 諸国の中には防衛当局が国内政治で主要な役割を果たしている国もあることを踏まえた時、より浮き彫りになる。また、安全保障分野の多国間協力で重要な枠組みを提供している拡大 ASEAN 国防相会議（ADMM プラス）の専門家会合には、2016 年にサイバーセキュリティ会合が設置されたところであるが、それらを舞台に地域における信頼醸成の促進に貢献していくことも期待される。さらに、防衛当局チャネルから得られた ASEAN 諸国のニーズに、関係省庁や民間企業等を含めたオールジャパンで応えていくことができれば、対 ASEAN 協力の効率や効果の向上も望めるだろう。

防衛省によるサイバー分野での対 ASEAN 協力は、必ずしも自らが保有する能力のみで自己完結的に推進される必要はない。むしろ、「サイバー外交」というより広い政策枠組みの中に位置付けた取組を検討してくこと、換言すれば日本が政策文書上で描いてきた多層性を持った「サイバー外交」を具体化していくことが実践面での課題になっているといえる。

おわりに

本稿は、学術的研究がまだ限られている「サイバー外交」をテーマとし、「サイバー『防衛』外交」の視点も取り入れた議論の必要性を提起した。日 ASEAN 協力の事例をみても、この論点への着目は今後ますます重要になると考えられる。もっとも、「サイバー外交」という表現それ自体は、いわば「バズワード」の域を出ないものかもしれない。しかし、たとえそうであったとしても、サイバー空間の在り方に関わる様々な問題が存在している事実に変わりはなく、そこへの国家の関与、並びにステークホルダー間の協力の在り方は依然として政策上も、学術的研究上も注目すべき論点となる。今回は日本に焦点を当てたが、その他の国や地域における取組や先行研究を更に考察していくことで、「サイバー外交」の理解をより深め、日本の取組の資となる知見を得ていくことを今後の課題としたい。

[1] White House, “International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World,” May, 2011. なお、米国では現在、サイバー外交の推進役となる「国際サイバー空間政策室（Office of International Cyberspace Policy）」の国務省への設置等を目指す、超党派で立案された「サイバー外交法案」も議会で審議中である。
[2] Council of the EU, “Council Conclusion on Cyber Diplomacy,” (Doc. 6122/15), February 11, 2015.
[3] この点の詳細は次を参照。原田有「サイバー空間のガバナンスをめぐる論争」『NIDS コメンタリー』第 43 号、2015 年 3 月 20 日。
[4] André Barrinha and Thomas Renard, “Cyber-diplomacy: The Making of An International Society in the Digital Age,” *Global Affairs*, Vol. 3, No. 4-5, 2017, pp. 353-364.
[5] 防衛外交は例えば次を参照。鶴岡路人「アジアおよび世界における日本の防衛外交」ジョナサン・アイル、鶴岡路人、エドワード・シュワーク編『グローバル安全保障のためのパートナー－日英防衛・安全保障関係の新たな方向』国際共同研究シリーズ 12、防衛省防衛研究所、2015 年、51-61 頁。
[6] Caitríona Heinl, “The Role of the Military in Cyber Space: Civil-Military Relations and International Military Co-operation,” *Pointer: Journal of the Singapore Armed Forces,* Vol. 42, No. 4, 2016, pp. 37-46.
[7] この点の詳細は次を参照。土屋大洋『サイバーセキュリティと国際政治』千倉書房、2015 年 168-179 頁。
[8] 情報セキュリティ政策会議「サイバーセキュリティ戦略－世界を率先する強靭で活力あるサイバー空間を目指して」（以下、「2013 年戦略」）平成 25 年 6 月 10 日、3 頁。
[9] 同上、39 頁。
[10] 同上、39-42 頁。
[11] 「サイバーセキュリティ戦略」平成 27 年 9 月 4 日、5-6 頁；「サイバーセキュリティ戦略」平成 30 年 7 月 27 日、8-9 頁。
[12] 外務省ホームページ「サイバーセキュリティー日本のサイバー外交」平成 31 年 2 月 27 日。
[13] 内閣サイバーセキュリティセンター、警察庁、総務省、法務省、外務省、経済産業省、防衛省「サイバーセキュリティ分野における開発途上国に対する能力構築支援（基本方針）」平成 28 年 10 月、2 頁。
[14] 同上、1 頁。
[15] 最新の第 11 回政策会議は「サイバーセキュリティ政策会議」に改称の上、2018 年 10 月に実施された。
[16] 内閣官房情報セキュリティセンター、総務省、経済産業省「第 2 回日 ASEAN 情報セキュリティ政策会議の結果－情報セキュリティ分野における日 ASEAN の連携枠組みの概要」平成 22 年 3 月 31 日。
[17] Brian Harding, “China’s Digital Sild Road and Southeast Asia,” *CSIS Commentary*, February 15, 2019.
[18] 「日・ASEAN サイバーセキュリティ協力に関する閣僚政策会議の結果－安倍晋三内閣総理大臣御挨拶」平成 25 年 9 月 12 日。
[19] Freedom House, “Freedom on the Net 2018,” October 2018.
[20] 「日・ASEAN サイバーセキュリティ協力に関する閣僚政策会議の結果－共同閣僚声明（仮訳）」平成 25 年 9 月 13 日。
[21] この点は例えば次を参照。庄司智孝「中国による地域秩序形成と ASEAN の対応－『台頭』から『中心』へ」防衛研究所編『中国安全保障レポート 2019－アジアの秩序をめぐる戦略とその波紋』2019 年 2 月 1 日、21-40 頁。

プロフィール profile

政策研究部
グローバル安全保障研究室
研究員　　原田　有
専門分野：海洋安全保障、サイバーセキュリティ

本欄における見解は、防衛研究所を代表するものではありません。
NIDS コメンタリーに関する御意見、御質問等は下記へお寄せ下さい。
ただし記事の無断転載・複製はお断りします。

防衛研究所企画部企画調整課
直　通：03-3260-3011
代　表：03-3268-3111（内線 29171）
ＦＡＸ　：03-3260-3034
※ 防衛研究所ウェブサイト：http://www.nids.mod.go.jp/