NIDS 防衛研究所
The National Institute for Defense Studies

サイバー安全保障に対する中国の基本的認識

地域研究部アジア・アフリカ研究室　研究員　　八塚　正晃

NIDSコメンタリー　第 60 号　2017 年 5 月 24 日

はじめに

習近平国家主席は 2016 年 10 月、「サイバー強国戦略の実践」をテーマにした中国共産党中央政治局第 36 回集団学習会において、「サイバー空間の安全保障・防御能力の強化を加速し、IT 技術を用いた社会ガバナンスの推進を加速し、我が国のサイバー空間における国際的発言権とルール設定権の向上を加速し、サイバー強国建設の目標に向けて努力を怠らない」ことを強調した[1]。その後、中国政府は 2016 年 11 月に『サイバー安全法』を採択（2017 年 6 月施行）、12 月下旬に『国家サイバー空間安全戦略』（以下、「安全戦略」）、2017 年 3 月に『サイバー空間国際協力戦略』（以下、「協力戦略」）を発表する等、サイバー安全保障に係る重要な政策文書を立て続けに公表している[2]。

サイバー安全保障に対する取り組みは主要国間でも一致しておらず、それに係る国際ルールの形成も発展段階にある。こうしたなか、中国がサイバー安全保障への取り組みを強めていることは注目に値する。中国の動向は日本のサイバー安全保障に対しても大きな影響を及ぼすからである。ここで重要なのは、中国の取り組みの動機となるサイバー安全保障に対する中国の基本的な認識を理解することである。

以上の問題意識を踏まえ、本稿では、中国のサイバー安全保障への取り組みを強化している背景を整理し、中国指導部の発言や政策文書から基本的認識を分析したうえで、日本の安全保障にとっていかなる課題が存在するかを検討する。

なお、サイバー安全保障といった場合、サイバー空間におけるガバナンスの側面とサイバー戦を含む軍事的な側面に二つに分けられるが、本稿では両側面を含めた幅広いサイバー安全保障に対する中国の認識を分析の対象とする。後述するように、中国はこれらを密接に関連させて捉えていることに加え、日本の安全保障を考えるうえでも両側面を踏まえて検討することが有益と考えるからである。

サイバー安全保障への取り組みを強める中国

中国は、習近平政権になってサイバー安全保障に取り組み始めたわけではない。既に胡錦濤政権期の 2003 年に『国家情報化領導小組の情報安全保障工作の強化に関する意見』、2012 年に『情報化発展の推進及び情報安全保障を実施することに関する若干の意見』が公表されており、その基礎のうえに習近平政権の取り組みがある。他方で、胡錦濤政権期の政策文書では、情報化経済への期待やサイバー空間における政府のガバナンス能力向上に対する施策に重点が置かれていたことに比べ、習近平政権期では、より「国家安全」の観点が反映され、国際的なルール形成に対する積極的な関与が強調されている印象を受ける。

習近平政権の姿勢の背景として、第一に、中国経済がますますサイバー空間に依存しており、経済成長のエンジンとしての期待と同時に、これを安定的に管理したいとの考えを強めていることが挙げられる。中国のネットユーザーは 2015 年には既に 7 億人を上回り、情報経済は中国の GDP

の 26%を占めており、今後もこの傾向が進むことは間違いない[3]。他方で、サイバー空間を介した経済犯罪や海外からのサイバー攻撃が横行しており、中国の持続的な経済成長にとって脅威ともなっている。経済成長を正統性の拠り所とする中国共産党政権にとっては、サイバー空間の安全保障は社会の安定性や政権維持に直結する問題なのである。

第二に、サイバー空間における国際的競争が厳しくなっており、早急に主導権を握るべきとの認識を中国指導部が有していることが指摘できる。習近平は 2016 年 4 月の講話の中で「現在、大国によるサイバー安全保障の駆け引きは、技術的なものだけでなく、理念や発言権をめぐる駆け引きも含む」と述べており[4]、「安全戦略」では、「サイバー空間戦略資源の争奪と支配、ルール制定権及び戦略的高地の占拠、戦略的主導権の追求をめぐる国際的な競争は、ますます激烈になっている」とより明確な危機感を示している。中国指導部にとって、現在はサイバー安全保障をめぐる国際ルール形成のための主導権を掌握するために重要な時期なのである。

第三に、現代戦においてサイバー空間が核心的に重要になっていると習近平政権が認識していることが指摘できる。中国指導部は、胡錦濤政権初期から「情報化条件下における局地戦」で勝利することを目標に掲げて軍事力を構築している。これは政治・軍事・経済目的を限定的に設定して紛争のコストを抑えることで、経済発展という大局的な目標と矛盾することなく効率的に国家利益を守ることを目指す軍事ドクトリンである。戦闘を短期間且つ局地的に終わらせるためにはネットワーク化した軍事情報システム及び軍種をまたぐ統合運用能力が枢要なため、中国の現代戦において、サイバー安全保障は極めて重要な位置づけが与えられる。習近平政権は、「情報化局地戦での勝利」と言い換えつつ、この軍事ドクトリンを実践できる軍隊を作り上げるために大規模な人民解放軍改革に取り組んでいる[5]。この改革の中で 2015 年末に設置が明らかにされた「戦略支援部隊」は宇宙、サイバー、電子戦を統括する情報戦の要となる組織であり、習近平政権の重視姿勢が端的に表れている。

以上のような背景から、習近平政権はサイバー空間における経済活動や国内ガバナンスからサイバー安全保障に係る国際ルールの形成へと関心を広げつつある。中国は 2014 年から毎年、世界中から政治指導者、サイバー専門家やサイバー関連企業を自国に招いて「世界インターネット大会」を開催している。2015 年 12 月に開催された第二回「世界インターネット大会」では、習近平が登壇し「４つの原則と５つの主張」(①サイバー主権の尊重、②平和安全の保護、③開放協力の促進、④良好な秩序の構築という４つの原則；①グローバルなサイバーインフラ設備の建設を加速し、インターネット通信を促進、②ネット上の文化交流共有プラットフォームを作り、相互交流を促進、③サイバー経済の新たな発展を推進し、共同繁栄を促進、④サイバー安全を保障し、秩序の発展を推進、⑤インターネット・ガバナンス・システムを構築し、公平正義を促進という５つの主張）を披露した[6]。

習近平の提言に見られるように、中国が安定的で公正なサイバー空間における国際秩序を目指していることは歓迎すべきであろう。他方で、中国によるサイバー安全保障への取り組みの方向性は、日本を含む先進諸国との間に無視できない相違があり、他国の安全保障を脅かす可能性があることも事実である。であるとすれば、中国のサイバー安全保障認識の特徴を理解しておく必要があろう。

「情報ドミナンス」の構築を目指す中国

サイバー安全保障に対する中国的な特徴として、サイバー空間における国家主権に対する認識が挙げられる。「安全戦略」では「サイバー空間は既に、陸・海・空・宇宙と同様に重要な人類活動の新領域であり、サイバー空間の主権は国家主

権の重要部分である」と述べている。日本を含めた欧米諸国もサイバー空間における主権を認めるが、その主権とは領域主権の延長で捉えつつも、表現の自由を支持する観点から政府の介入を抑えることも同時に強調する[7]。これに対して中国政府が唱える国家主権とは、政府が国内のサイバー空間のコンテンツまで規制する権利を含み、欧米諸国との間に政府の介入をめぐり大きな差異があることに注意を要する。「協力戦略」でも「サイバー空間は現実社会と同様、自由を唱える必要はあるが、『無法地帯』ではなく秩序を保つことも必要である」として管理の必要性を強調し、また「サイバー安全法」では、サイバー空間を通じた国家の安全・栄誉・利益への損害、国家政権や社会主義制度の転覆扇動、経済・社会秩序を乱すデマ情報の伝播を禁じており（第 12 条）、中国当局が海外の機関、組織、個人に対しても法的責任を追及し、資産凍結やその他制裁措置を行うことを規定している（第 75 条）[8]。すなわち、サイバー空間における企業・NGO・個人の情報に対する検閲や遮断、言論統制、活動の取り締まりについて、中国政府が厳密に管理し、且つそれに対する国際的な批判を拒否・無視できるサイバー空間の構築を目指していると考えられる。

中国がサイバー空間の主権を強調する背景には、国際的なサイバー空間が国内政治、とりわけ共産党政権による統治に対して脅威になりかねないとの警戒感が存在する。「協力戦略」では、「中国はサイバー安全の保護者を堅持する。中国もハッカー攻撃の被害者である」と述べており、同様の主旨は中国の国防関係者からも聞かれる[9]。中国共産党政権にとっての安全保障の至上命題は自らの安定的統治である。したがって、彼らは、「アラブの春」に代表されるソーシャル・ネットワーキング・サービス（以下、SNS）等における政権批判の拡散に対して、社会の不安定化に繋がり中国共産党統治を揺るがしかねない安全保障問題と認識する。2015 年に中国国防大学から出版された『戦略学』では「サイバー空間は、21 世紀に入って既にいくつかの国家によって、他国の『カラー革命』を発動するために利用されている」と警戒感を示す[10]。こうした SNS 等における政権批判や彼らにとって都合の悪い情報の拡散に対しても、中国政府は、共産党政権の転覆を図る海外からのサイバー攻撃と看做している節がある。

こうした認識に基づき、中国政府は、サイバー安全保障のために新たな国際ルールの形成を主導すべきであり、さらに、サイバー空間は新しい特殊な領域であるために既存の国際法をそのまま適用するのではなく、新たな条約等で対応すべきと考えている。「協力戦略」でも、「サイバー空間は新しい領域として、関連する規則や行動規範を早急に制定する必要がある」と主張する。これは、従来の国際法がサイバー空間に適用されると、言論の自由や通信の秘密などの人権がサイバー空間でも守らざるをえなくなり、検閲や通信傍受が困難になるとの認識に基づいていると思われる[11]。したがって、中国は言論の自由を求める欧米主導ではなく、ロシアを含む SCO（上海協力機構）等の諸国と足並みを揃えつつ自国主導でのルール形成を目指している。「協力戦略」でも「関連する国際プロセスに包容性と開放性を確保し、発展途上国家の代表性と発言権を強める」と述べている。

以上を要するに、中国指導部は、サイバー空間において、持続的な経済成長及び中国共産党政権の安定的統治の観点から、自国における管理強化に留まらず国際的なルールの形成を主導して、中国政府が内外の情報の流れを可能な限りコントロールできる状態を作りあげることを目指していると考えられる。米国のヘリテージ財団のディーン・チェン（Dean Cheng）氏は、こうした中国の情報をめぐる活動を「情報ドミナンス（information dominance）」の構築と呼ぶ[12]。すなわち、情報の収集、伝達、分析、評価、諜報を敵

国よりも速く、正確に実施し、そのうえで、友好国、敵国、第三者の認識や評価を形成し影響を与えることを指す。中国による情報ドミナンスの構築は、サイバー空間のガバナンスのみならず軍事的なサイバー戦の側面を含んでおり、日本の安全保障にも大きく影響する。

中国のサイバー安全保障をめぐる論点

中国のサイバー安全保障の動向で今後注意すべきポイントとして、少なくとも以下の三つが指摘できる。第一に、中国の軍事面でのサイバー安全保障が、有事における情報活動だけでなく、平時における政治戦も含むことである。中国政府は平時における政治戦を「三戦」（世論戦、心理戦、法律戦）と呼ぶ。三戦については、中国共産党は日中戦争時から、自らに有利に事が運ぶよう国際世論工作を実施してきた歴史を持つ。問題は、こうした伝統的な政治戦を継承しつつ、巨大な経済力と新たな技術を駆使してその手法を発展させていることである。例えば、サイバー空間における機密情報の窃取、情報改竄、流言飛語による世論誘導のようなサイバー攻撃は、攻撃主体の特定が困難であり、より小規模なサイバー攻撃であれば、それ自体に気づくことさえ難しい。より戦略的なレベルでは、サイバー攻撃を通じて、中国と紛争を抱える国家に対して世論誘導や指導部の意思決定に揺さぶりをかける一方で、対立国が国際的に孤立する状況を作り出し自国の対抗策を正当化して、武力衝突に至らず有利に紛争処理を進める等が可能性として考えられる。このようなサイバー空間の政治戦は、平時とも有事ともとれるような「グレーゾーン事態」を様々に発生させかねない。この論点に対しては今後さらなる検討がなされるべきであろう。

第二に、上記の点にも関連するが、サイバー空間における軍事攻撃の基準や敷居についてである。中国の国防研究機関である軍事科学院が 2013 年に出版した『戦略学』では、「サイバー戦は低コストで高効率であるため、サイバー戦は他の種類の戦争よりも発生しやすい」としているが、逆に言えば、中国でもサイバー戦に対する心理的ハードルは通常兵器による戦闘よりも低い可能性がある[13]。例えば、敵軍の C4ISR と呼ばれる指揮命令情報システムに対しての物理的な破壊を伴わない（情報を対象とした）サイバー攻撃のような「ソフトキル」について、中国軍は戦争へのエスカレーションを招かない防御的措置と捉えている可能性を指摘する見方もある[14]。しかし、仮に被害国がこれを軍事攻撃と見なした場合、事態は通常兵器の使用を含む戦闘へとエスカレートするおそれがある。

第三に、より重要なポイントとして、サイバー空間における抑止に対する認識の差異が挙げられる。習近平は 2016 年 4 月の講話で「サイバー安全保障防御能力と威嚇能力を増強する。サイバー安全保障の本質は対抗であり、対抗の本質は攻防両方の能力の競争である」と述べている。中国の威嚇能力とは抑止能力に近い概念である。『戦略学』（2015 年版）によれば、サイバー抑止は、①相手軍の C4ISR システム、枢要な交通・通信インフラに対するサイバー攻撃能力を示すことを通じて相手のサイバー攻撃を思い留まらせる戦略レベルの抑止、②分散的で小規模なサイバー攻撃やサイバー浸透行為を牽制する戦術レベルの抑止の二つに分けられる[15]。サイバー抑止に関しては、①意図、②能力、③相互理解という抑止関係を成立させる基本的な条件が、サイバー空間においては極めて曖昧になるという本質的な問題が存在する。すなわち、サイバー攻撃の主体特定にコストがかかり、中国の攻撃・反撃能力の評価も難しいことに加え、中国が何をサイバー空間における軍事的攻撃と見なすのか、という問題である。例えば、既述のように SNS 等における政権批判や不都合な情報流布について、規模と事態によっては、中国政府がこれをサイバー攻撃と見做す可能性もある。この場合、誰に対して、いかなる報復措置を採るのか定かではない。以上のような難しさを念頭に置きつつも、中国が今後、

サイバー空間での抑止能力を強化するというのであれば、その意図と能力に対する理解を深めるとともに、コミュニケーションを図り相互理解を進めることが求められる。

おわりに

以上を踏まえて日本のサイバー安全保障を考える場合、競合的側面と協調的側面の双方に目を向ける必要があるだろう。前者については、日本独自の取り組みと日米同盟を軸にした抑止能力の構築が挙げられる。例えば、現在、内閣サイバーセキュリティセンターが中心となって検討を進めているようなサイバー防御に係る技術研究開発、重要なサイバーインフラの抗たん性強化、高度なサイバー人材の育成等の諸施策は、日本の拒否的抑止能力に資する。また、日米同盟による拡大抑止を念頭に、サイバー空間における懲罰的抑止能力の保持について検討することも考えられる。そのためには中国のサイバー攻撃のリスク・能力評価や情報共有、平時から有事にかけての様々な事態に対する報復措置も含めたサイバー安全保障協力のあり方について米国側と緊密な協議を進めることが必要である。

他方で協調的対応としては、サイバー安全保障をめぐる中国との二国間の対話枠組みを構築することが考えられる。既に米中間では、2015 年 9 月の首脳会談でサイバーに関する対話メカニズムの設置に合意し、既に複数回の閣僚級対話や作業グループによる協議が実施されている。これらの対話は、サイバー犯罪や知的財産の窃取防止に限定されているようだが一定の効果を挙げているとも聞く[16]。中国政府は、サイバー攻撃の被害者との認識を有すると同時に、自国の経済成長を阻害しかねないサイバー犯罪の取り締まりには積極的である。したがって、こうした論点から、情報交換や対話枠組みの構築を進めることを通じて、不必要なサイバー攻撃や商業スパイを減少させ、信頼醸成を図ることは可能と思われる。既に日中韓では外交当局間のサイバー協議が第三回まで開催されているが、こうした枠組みを活用しつつ、よりハイレベルな二国間枠組みや治安・防衛当局間のサイバー協議を検討することも考えられる。

また、国際社会との協力という観点からは、サイバー安全保障に関する国際規範の形成に対して積極的に関与することも重要である。ハーバード大学のジョセフ・ナイ（Joseph S. Nye）氏は、サイバー攻撃を抑止するための要素の一つして、サイバー攻撃の対象についてのタブーを共有する国際規範の形成を挙げ、そのために各国間の信頼醸成が重要だと指摘する[17]。中国が目指すような新たなサイバー安全保障に係る国際条約の締結は長い時間を要するだろうが、例えば、NATO サイバー防衛センター（CCDCOE）が中心になって取り組んでいる、いわゆる「タリン・マニュアル」のような政策志向の強い議論の成果は、法的な拘束力を持たない一方で、政治的なコストも相対的に低く、サイバー攻撃を抑止する国際規範の醸成に資すると考えられる。

（脱稿 2017 年 5 月 12 日）

---

1 「习近平:加快推进网络信息技术自主创新 朝着建设网络强国目标不懈努力」『中国共産党新聞網』（2016 年 10 月 10 日）以下、全て最終アクセス 2017 年 5 月 11 日。

2 「国家网络空间安全战略」『新華網』、及び「网络空间国际合作战略」『新華網』

3 郑必坚「网络化大潮与中国的和平崛起」『中国信息安全杂志』（2017 年 2 月）。

4 习近平「在网络安全和信息化工作座谈会上的讲话」『新華網』（2016 年 4 月 25 日）

5 『《中国的战略》白皮书』（2015 年 5 月）

6 习近平「习近平在第二届世界互联网大会开幕式上的讲话」『新華網』（2015 年 12 月 16 日）

7 河野桂子「サイバー・セキュリティに関する国

際法の考察ータリン・マニュアルを中心に—」『戦略研究』（2015 年 1 月）25-45 頁、及び原田有「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）

[8]「中华人民共和国网络安全法」

[9] 中国国防部報道官は、2012 年 3 月に具体的な被害数を公表している。『人民網』

[10] 肖天亮 主编『战略学』（国防大学出版社、2015 年）、143 頁。

[11] 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）、157-158 頁。

[12] Dean Cheng, *Cyber Dragon : Inside China's Information Warfare and Cyber Operations*, Praeger: California, 2017, pp15-16.

[13] 军事科学院军事战略研究部『战略学（2013 年版）』（軍事科学出版社、2013 年）、191 頁。

[14] Joe Mcreynolds, *China's Evolving Military Strategy*, The Jamestown Foundation: Washington DC, 2017, pp183-184.

[15] 肖天亮、前掲書、147 頁。

[16] Gary Brown and Christopher D. Yung, "Evaluating the US-China Cybersecurity Agreement Part3," *Diplomat,* January, 2017, (http://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-3/).

[17] Joseph S. Nye, "Deterrence and Dissuasion in Cyberspace," *International Security*, Vol. 41, No. 3 (Winter 2016/17), pp. 60-62.

プロフィール profile

地域研究部アジア・アフリカ研究室

教官・研究員

八塚　正晃

専門分野：中国政治外交・東アジアの安全保障

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/