サイバー空間における「国家中心主義」の台頭

川口 貴久
Kawaguchi Takahisa

はじめに

サイバー空間、すなわちデジタル情報を伝達・交換・共有するためのネットワークは拡大を続けている(1)。その間、サイバー空間は社会や生活の隅々にまで浸透（深化）し、コミュニケーション、産業構造、社会合意形成等のあらゆる分野に変化をもたらした。

では、サイバー空間の拡大・深化は国際政治・国際関係にどのような変化をもたらしているのか。あるいは、サイバー空間における国際政治・国際関係をどう捉えるべきなのか。

サイバー空間は、その黎明期において「ユートピア」として捉えられていた。すなわち、サイバー空間には国境が存在せず、そこで主権国家のパワーは相対化され、国際紛争は減っていく。しかし、今日ではサイバー空間には明確な国境が存在し、最も洗練されたサイバー能力を保有するのは主権国家であり、サイバー空間における、またサイバー空間をめぐる大国間紛争を惹起している。現在進行形の米中間の技術的優位をめぐる紛争、米ロ間の選挙干渉をめぐる紛争はサイバー空間の拡大と深化故に生じた対立である。

主権国家が安全保障問題を中心としてパワーを行使し、場合によっては大国間紛争・対立が生じているという意味で、サイバー空間では「国家中心主義」が台頭している。サイバー空間が「自由な共有地のような存在だった黄金時代は既に過去のもの」であり、「現在はその代わりに、非常に複雑な地政学的競技場」(2) と化している。

こうした状況は「古典的リアリズム（classical realism）の世界への回帰」(3) と言える。古典的リアリズムの世界観では、最も重要な主体は国家であり、国家は生き残りとパワーの最大化のために行動する。最重要問題は安全保障であり、国際政治とは権力闘争である(4)。

これはサイバー空間だけに当てはまるものではない。現在の国際環境は、「地政学の逆襲」（ロバート・D・カプラン）、「ウェストファリア主権」の復活（イアン・ブレマー）など、主権国家間のパワーゲームが全面的に押し出された世界と分析されている。

本稿ではまず、「ユートピア」としてのサイバー空間を概括し、次にサイバー空間における国境・領域性、パワー、紛争に関する誤解と現実について指摘する。最後に、サイバー空間における大国間紛争と対立についてまとめる。

1 「ユートピア」としてのサイバー空間

サイバー空間は「ユートピア」として捉えられていた時代があった。

この「サイバー空間」とは少なくとも、①インターネット、②インターネットに接続されていないクローズド・ネットワーク、③これらネットワークに接続された（されうる）コンピューター端末、サーバー、記憶媒体、その他電子機器などから構成される。

インターネットはサイバー空間を構成する中核要素だが、その歴史は長く見積もっても半世紀である（1969年にインターネットの前身であるARPANETがパケット交換のリンクを確立した）。商業利用の歴史は約30年にすぎないが、その間、インターネットを中核とするサイバー空間は社会インフラ、生活機器、言論空間を支えるバックボーンと化した。

インターネットは「米国防総省が開発した」と指摘されるが、これは正確な記述ではない。確かに米高等研究計画局（ARPA: Advanced Research Projects Agency, 後の国防高等研究計画局〔DARPA〕）がインターネット開発に果たした役割は大きいが、実際にARPANETの運用を開始したのは米国西海岸を中心とする4大学の研究者たちであった。

「自律」「分散」「協調」に特徴づけられるインターネットの設計思想は、伝統的な政府による統治とは異なるものであった(5)。国境も中央権力もなきインターネットを中核とするサイバー空間の出現は、国家・政府の役割の見直しを迫った。電子フロンティア財団の創設者であるジョン・ペリー・バーロウは米国でのインターネット規制法案（通信品位法）を非難し、1996年2月8日、「サイバースペース独立宣言」を発表した。バーロウいわく、サイバー空間は政府が介入すべき場所ではなく、独立した主権を有している。

後にリチャード・バーブルックらはインターネットの発展とその文化には時代的・地理的偏在が存在することを指摘した。偏在とは、インターネットが1960年代の米国西海岸で生まれたことを強調し、その特徴は未来に対する楽観主義、テクノロジーによる問題解決能力への信頼、カウンターカルチャーなどの「カリフォルニアン・イデオロギー」と表現される(6)。こうした地理・時代背景がサイバー空間に「ユートピア」主義をもたらした。そこでは、サイバー空間に国境はなく、国家は相対化され、それ故に国際紛争はない。サイバー犯罪があったとしても、技術がすべてを解決してくれる。

またサイバー空間の拡大は冷戦終結後のグローバル化と軌を一にしていた。トーマス・フリードマンが描いた『フラット化する世界』では、企業のみならず個人までもグローバルな競争に参画し、国家は相対化される。そして、フラット化の要因の多くは情報通信技術、汎用オフィスソフト、遠隔アクセスなど、サイバー空間の拡大に関するものであった(7)。

2　サイバー空間と国際政治をめぐる「ハイプ」

しかし、サイバー空間を「ユートピア」とみなす見立ては、サイバー空間と国際政治をめぐる無理解や誇張された前提、すなわち「ハイプ（hype）」に基づいていたと言わざるをえない。

(1)　サイバー空間に国境はない？

第1の「ハイプ」は、サイバー空間に国境はない、というものである。確かに、デジタル情報は国境を越えて飛び交う。企業のデータセンターは世界中に分散し、ユーザーは世界中どこからでもクラウドサービスを利用することができる。サイバー攻撃の被害者、攻撃の指

令を送るサーバー、経由地、実際の攻撃の発信源、攻撃者の国籍は国境をまたいでいる。

しかし、各国はサイバー空間（の一部）に主権と領域性を主張し、実際にデジタル情報の「フロー（流通）」と「ストック（保有）」は国境に阻まれつつある。

「フロー」という点では、インターネットの「断片化」「バルカン化」が進行している。本来、ひとつのインターネットが切り裂かれる（split）という意味で、「スプリンターネット（splinternet）」とも呼ばれる。

中国で展開されるインターネット情報の検閲およびブロッキングシステム「金盾」は、中国国内と世界のインターネットの間にそびえる「サイバー版万里の長城」である。当局による検閲・ブロッキングを回避するため、インターネットユーザーは暗号化技術VPN（Virtual Private Network）を用いてきたが、2017年以降はVPN利用に対する規制が強化された。2019年5月には、ロシアでインターネット（Runet: Russian Internet）を海外から切り離すことを可能にする法案が成立した。ロシア政府は、同法は外国からのサイバー攻撃を受けた場合など、Runetを保護し、継続性を確保するためのものである、と主張している。

米シンクタンクFreedom Houseが公開する報告書「ネット上の自由（Freedom on the Net）」によれば、より多くの国がユーザーにアクセス制限やコンテンツ規制を課している。Googleの持ち株会社アルファベットの取締役エリック・シュミットらは、こうした規制が進めば、グローバルな一つのインターネットが「国ごとのネットワークの寄せ集め」と化すのではないかとの懸念を示す(8)。

情報をどこに保管するか、という「ストック」の規制も明確である。ある調査によれば、各国は金融・決済情報、個人データ、通信データ、企業の機密情報などのさまざまなデータの国外移転を禁じている(9)。

この問題は自由主義と権威主義という単純な対立構造ではない。欧州やブラジルはプライバシー保護を目的に個人データの域外移転を禁じている（後述）。中国やベトナムなどでは主に安全保障・法執行、自国の産業振興などを目的として、通信データやログ（記録）、その他重要機密情報を保管するサーバーを自国内に置くことを外国企業に要求している。各国でデータ移転を阻止する目的は異なるとはいえ、こうした動きは「データローカライゼーション」と呼ばれる。

なぜ、国家はサイバー空間（の一部）に主権・領域性を主張できるのか。それは、サイバー空間は物理インフラに依存し、物理インフラの多くは領土・領海に依存するからである。情報はサーバーやデータセンターに保管され、これらはどこかの国の領土内に存在する（ただし、最近では領海内にデータセンターを設置する検討も進んでいる）。インターネット上の国際通信の99%以上は海底ケーブルを経由し、海底ケーブルの陸揚げ拠点は各国の海岸にある。海底ケーブル自体は公海にも敷設され、海底ケーブルは複数の国の企業が共同所有することが多いが、少なくとも陸揚げ拠点とその内側はどこかの国の領土内にある。

こうした指摘は最近のことではない。ジャック・ゴールドスミスとティム・ウーはすでに2006年、サイバー空間に国境がないというのは幻想であり、国家による強制力が機能していると論じた(10)。サイバー空間が物理インフラに依存しているという事実が、国家が主権と領

域性を主張する（できる）根拠であり、「断片化」「データローカライゼーション」はパワー行使の結果である。

(2) サイバー空間で主権国家のパワーは相対化される？

第2の「ハイプ」は、サイバー空間で主権国家のパワーが相対化されているというものである。国家による情報と技術の独占は破綻し、個人、企業、犯罪者やテロリストがそれらからパワーを得ている。ジョセフ・ナイはこうした動きを「パワーの拡散」と表現する。技術の進展によって、国家と非国家主体の間のパワーの非対称性は縮小している[11]。

Google、amazon、facebook、Apple（GAFA）の売上高は合わせて70兆円を超し、世界第三位の経済大国・日本の年間歳入額を上回る[12]。インターネットやサイバー空間を支えるのは民間企業である。

サイバー攻撃を行なうのは国家の専売特許ではなく、犯罪者やテロリスト、究極的には個人が実行可能である。人々はメッセンジャーアプリ「Signal」や暗号化ネットワーク技術「Tor」を用いることで、通信内容や接続経路を秘匿化し、政府の監視を免れることができる（と考えられている）。

しかし、最も洗練されたサイバー能力をもつのは主権国家である。過去10年間を振り返って、最も影響の大きかったサイバー攻撃の大部分は国家が関与するものであった。イラン核施設の遠心分離機を破壊したStuxnet（2010年）、ウクライナでの広域停電（2015年、2016年）、米大統領選挙への干渉（2016年）、身代金要求型マルウェア（ウイルス）「WannaCry」や「NotPetya」の世界的流行（2017年）、日本年金機構（2015年）[13]・米人事管理局（2015年）・米大手ホテルチェーン（2018年）・シンガポール政府医療データベース（2018年）へのサイバー攻撃とビッグデータ収集の背景には国家の関与があった可能性が高い。

米セキュリティー会社マンディアントの最高技術責任者を務めたリチャード・ベトリッチはサイバー攻撃について、国家とその他のアクターを分かつ要素のひとつは、電子信号諜報（SIGINT: Signal Intelligence）能力だと指摘する。インターネット上の大量の通信を傍受することのできるSIGINT能力は国家のみが保有する資産である[14]。

法執行も国家固有のリソースである。米国はクラウド法（CLOUD法: The Clarifying Lawful Overseas Use of Data Act）によって、企業が保有するデータに国境を越えてアクセス可能であるし、中国はサイバーセキュリティー法（網絡安全法）によって自国内に保管されたサーバー内の情報にアクセスできる。GAFAやその他企業は莫大なデータを「保有」するが、データへの「アクセス」という観点では主権国家に優位性がある[15]。

確かにサイバー空間で国家と非国家主体のパワーに関する非対称性は縮小しているが、高度で持続的なサイバー攻撃や情報へのアクセス等で国家に優位性があることを見逃してはならない。

(3) サイバー空間の拡大・深化は国家間の紛争を減少させる？

第3の「ハイプ」は、サイバー空間の拡大・深化は国際紛争を減少させるというものである。これにはいくつかの論理がある。ひとつは、情報技術自体が社会動態や紛争の原因を分析し、暴力のエスカレーションを予測、場合によっては紛争解決・平和構築に役立つという

見方である。「インターネットの父」の一人、ヴィント・サーフは国際連合平和維持活動（PKO）担当事務次長補ジェーン・ホール・ルートとの対話のなかで、紛争解決には紛争の起源への洞察が不可欠として、技術の貢献を示唆した(16)。

もうひとつは、サイバー空間の拡大と深化、特にインターネットの普及は社会を民主化し、民主国家が増えれば戦争は少なくなるという論理である。本稿では民主的平和論（democratic peace theory）の是非には触れないが、仮に「民主国家同士は戦争を起こさない」としても、インターネットの普及が民主化を進めるという論理は疑わしい。

インターネットをはじめとする技術は必ずしも紛争を解決するわけではなく、必ずしも社会を民主化するわけではない。なぜなら技術は価値中立的だからである。自由と民主制を求める場所では、それを追求するための手段となるが、権威主義国家は社会統制の手段としてインターネットやその他情報技術を用いる(17)。中国が国内で利用し、欧州を含む各国に輸出する顔認証・追跡技術や社会信用システムはその典型だろう。インターネットや関連する情報技術は紛争解決の手段となるが、過激派テロ組織「イスラム国」がウェブサイトやソーシャル・ネットワーキング・サービス（SNS）で諸外国でのテロを教唆し、あるいは「外国人戦闘員」をリクルートしたように、紛争誘発・動員の手段にもなる。サイバー空間の拡大・深化が国際紛争を減らすというのは、技術の一側面にすぎない。

3　サイバー空間における大国間競争

今日、サイバー空間でも主権と領域性が主張され、主権国家は優位なパワーを維持している。サイバー空間の拡大・深化は必ずしも国際紛争を減少させるわけではなく、場合によっては新たな紛争を惹起している。

（1）　米中紛争―― 5Gと商業的機密をめぐる紛争

現在、米中はサイバーセキュリティー問題をめぐり対立している。具体的には、「高速・大容量」「低遅延」「多接続」を特徴とする第五世代移動通信システム（5G）の構築・運用における中国企業の「排除」問題、サイバー攻撃等を通じた民間企業の営業秘密・知的財産等の窃取問題である。米国の立場では、この問題は、①中国政府が中国企業を通じて機密情報を収集している点であり、②中国政府が米民間企業を狙ったサイバー攻撃を仕掛けていることである。そして、中国によるサイバー攻撃を通じた機密情報窃取の標的は、「戦略的新興産業」（第12次5ヵ年計画）や「10大重点産業分野」（中国製造2025）などの重点産業と共通性がある(18)。

ドナルド・トランプ政権は2018年、中国による米民間企業へのサイバー攻撃が継続的に行なわれているとして、対中批判を開始した。マイク・ペンス副大統領は10月4日、ハドソン研究所における1時間弱の演説で終始一貫して対中批判を展開した。ペンス演説はサイバー攻撃だけではなく、選挙干渉、宗教弾圧、南シナ海での埋め立て、不透明な対外投資など、あらゆる分野に及んだ。

米当局は2018年を通じて、米国企業の営業秘密・知的財産を窃取したとして、中国国家安全部（MSS）および傘下の地方組織の職員、MSSと関係するとみられるサイバー攻撃グルー

プ「APT10」、中国企業などを次々に訴追した。

2019年1月28日、米司法省は華為端末（Huawei Device）とその米国現地法人を起訴したと発表した。2社はドイツ通信大手の米国現地法人T-Mobile US社の品質検査用ロボットTappyに関する営業秘密を窃取したとの容疑である。同じ日、米司法省は別件（対イラン制裁関連）で華為技術（Huawei Technologies）、その最高財務責任者（CFO）・副会長である孟晩舟氏、華為端末の米国法人、星通技術（Skycom Tech）社を起訴したと発表している。

しかし、より大きな衝撃を与えたのはペンス演説や刑事訴追よりも、トランプ大統領の署名を以って成立した2019会計年度国防授権法（2018年8月13日成立）であろう。同法第889条は、特定の中国企業の排除を明言した。すなわち、①特定の中国通信機器メーカー、②部品としてこれら企業製品を組み込んだ完成品、③これら企業製品を使っている企業を、政府調達から排除すること、を決定した。ここで明示された中国企業とは、華為技術、中興通訊（ZTE）、監視カメラの世界最大手・杭州海康威視数字技術（HIKVISON）、顔認証技術大手・浙江大華技術（Dahua Technology）、モバイル無線大手・海能達通信（Hytera Communications）の5社である。政府調達からの排除が実施されれば、多くの企業はサプライチェーンの大幅な見直しを迫られることになる。

さらに米国は、米対外投資委員会（CFIUS）の買収審査権限を拡大し、外国企業による投資を従来以上に幅広く規制することが可能となった。

他方、中国政府は、米国の対応は根拠がないものであると批判している。華為技術の郭平輪番最高経営責任者（CEO）も2019年2月、バルセロナで開催されたMobile World Congress（MWC）で童話「白雪姫」のフレーズを真似て、「PRISMよ、PRISM、この世で一番信頼できるのは誰？　これは重要な問いです。もしこの質問を理解できないのなら、エドワード・スノーデンに尋ねましょう」と米国を批判した。PRISMとはスノーデンが暴露した米国家安全保障局（NSA）の監視プログラムで、NSA職員が米インターネット企業のウェブメール等のメタデータ（データそのものについてのデータ）を収集・検索できるようにしていた。

5G構築・調達における米中対立は根深い。米国と同盟国で中国に対する懸念が惹起される理由のひとつは、「いかなる組織及び国民も、法に基づき国家情報活動に対する支持、援助及び協力を行い、知り得た国家情報活動についての秘密を守らなければならない」（第7条）[19]と規定した中国国家情報法（2017年6月28日施行）と考えられている。確かに、ペンス副大統領のミュンヘン安全保障会議での演説（2019年2月16日）は明示的に、オーストラリア政府の5G調達方針に関する決定（2018年8月23日）は暗示的に、中国政府による中国企業を通じた機密情報へのアクセスに懸念を表明した。

しかし、2017年施行の中国国家情報法で米国の対応が変わったとするのは短絡的である。中国企業による情報窃取は、トランプ政権になって突然浮上した問題ではなく、中国への強い対応には米議会における超党派の支持があり、すでに2012年時点で警鐘が鳴らされていた[20]。

5Gをめぐる中国企業「排除」は、2013年以降に顕在化した米中のサイバーセキュリティー問題が背景にある[21]。すなわち、政府が商業的利益の獲得を目的に、外国の民間企業の営業秘密や知的財産を窃取するという問題である。2015年9月、バラク・オバマ大統領と習近平

国家主席は「米中両国は、企業や商業分野での競争優位を獲得することを目的に、営業秘密やその他機密情報を含む知的財産をサイバー能力で窃取することを実行または支援しないことに同意」した[22]。

だが、その後も中国から米民間企業を狙ったサイバー攻撃は減らなかった。米国側にすれば、2015年9月の米中合意、すなわち習主席のコミットメントにもかかわらず、解決されなかった問題という認識があるとみられる。

(2) 米口紛争――選挙と民主主義をめぐる攻防

サイバー空間における紛争は米ロ間でも顕在化している。米ロ関係はウクライナ危機(2014年―)、シリア介入問題(2015年)、英国での化学剤ノビチョクの使用(2018年)などをめぐって緊張してきたが、これらは同盟国や第三国で発生した対立である。今日の米ロ関係を直接的に悪化させ、米国社会に分断をもたらしたのはロシアによる2016年米大統領選挙への介入である。

ロシアによる2016年米大統領選挙への干渉の手法は、①サイバー攻撃による候補者に関する機密情報の窃取と戦略的暴露、②SNS上などでの偽情報流布や政治広告、③投開票等の選挙インフラに対するサイバー攻撃、に大別される[23]。なお、ロシア政府とトランプ陣営の共謀の疑惑はロバート・モラー特別検察官による捜査報告書(2019年3月)において立証されなかった。

米国家情報長官室(ODNI: the Office of the Director of National Intelligence)による報告書(公開版)によれば、ロシアは「米国の民主的プロセスに関する国民の信頼を損ね、ヒラリー・クリントン候補を非難し、彼女の当選可能性や大統領としての潜在性を害することを意図した」影響工作活動を展開し、この活動は「ウラジミール・プーチン大統領の指示に基づく」ものであり、「プーチン大統領とロシア政府はトランプ候補に対して明らかに選好があった」とした。このような評価について、ODNIは機密情報・公開情報に基づく「高い確信(high confidence)」がある、と明言した[24]。さらに上記の①については、英国、オーストラリア、オランダ、カナダ政府がロシアによる犯行との結論を下した。

その後、3つの起訴状[25]でロシア連邦軍参謀本部情報総局(GRU)およびその実行部隊のサイバー攻撃グループ(通称「APT28」「FancyBear」)、サンクトペルブルクに所在する企業インターネット・リサーチ・エージェンシー(IRA)社などの組織や個人が起訴され、また財務省によって経済制裁の対象とされている。

2016年米大統領選挙介入のうち米民主党機関などや選挙インフラへのサイバー攻撃については、オバマ政権は大統領選挙期間の比較的早い段階から認識していた。しかし、ロシアのメディア(RTやSputnik)やSNS上での政治宣伝・フェイクニュース流布の脅威は選挙期間中に十分認識されていなかった[26]。

facebookやTwitterなどのSNSが選挙活動や合意形成の場として認識されるにつれ、SNS等に対する外国政府による意図的な選挙妨害や操作は国家安全保障上の問題と位置付けられている。こうした状況を、米国の研究者P・W・シンガーは「いいね!をめぐる戦争(Like-War)」と呼ぶ[27]。ハッキングされたのは米民主党関係機関や選挙インフラだけではなく、ア

メリカ人の感情や投票行動であり、究極的には米国の民主主義でもあった。

2016年米大統領選挙に続く2018年11月の米中間選挙でも外国からの干渉が確認された。米国のインテリジェンス・コミュニティーは大統領令13848号に基づき中間選挙への介入を調査し、「投票妨害、集計結果の改竄、集計妨害などの米国の選挙インフラへの攻撃」は確認できなかったものの、「ロシアおよび中国、イランを含む諸外国による影響工作活動と情報キャンペーン」を確認した、と評価した[28]。こうした影響工作活動は「新たな常態（new normal）」となりつつある。

(3) 米欧間対立

サイバー空間における対立軸は米国と中ロの対立軸だけではない。米国と欧州は基本的な立場を一にするが、いくつかの分野では対立が生じている。オバマ政権・国務省のインターネット政策の筆頭アドバイザーを務めたアレク・ロスは「20世紀の紛争は左と右（イデオロギー）の間で生じたが、21世紀はオープン（open）とクローズド（closed）の間で生じる」と指摘する[29]。米国と欧州は問題領域によって、「オープン」「クローズド」の立場を変えながら対立している。

米国および欧州、そして日本は既存の国際法体系がサイバー空間に適用されるとの立場に立ち、国連専門家会合（GGE）、先進国首脳会議（G7）、あるいは二国間・多国間合意のなかでそうした姿勢を確認してきた。

しかし、個人データをめぐる規制では米国と欧州の差は明らかである。facebookやGoogleなどのプラットフォーマー企業による大量の個人データ収集、元NSA職員スノーデンの暴露によって明らかになった監視プログラムなどの存在を背景として、欧州では2018年5月、EU一般データ保護規則（GDPR: General Data Protection Regulation）が施行された。個人データの域外移転を原則として禁止する欧州が「クローズド」であり、そうではない米国が「オープン」と言える[30]。

また米国は欧州の同盟国に対して、5G調達に華為技術を参入させるなら、「機密情報を共有できなくなる」と警鐘を鳴らした。5Gからの中国企業の排除問題については、米国が特定企業を名指しした一方で、英国は「（中国企業が参入しても）リスク管理は可能」との方針とみられる（厳密に言えば「特定企業を排除しても、5Gのセキュリティーは担保されないため、監視や対処といったさまざまな手段の組み合わせが有効」という論理である）。ここでは、「クローズド」な米国と「オープン」な欧州という対立軸がみてとれる。

もちろん「オープン」が常に「善」ではない。安全保障などの領域では「クローズド」が適切である場合もある。

おわりに

このようにインターネットを中核とするサイバー空間の出現、そして拡大・深化は、既存の主権国家システムを大きく変えるかに思われた時期があった。しかし、サイバー空間における国境・領域性、パワーの非対称性、国際紛争という観点からは、従来の主権国家システムから大きく逸脱するものではない。顕在化している大国間紛争はサイバー空間における機

密情報の窃取、サイバー空間を通じた選挙干渉をめぐる対立であり、サイバー空間の拡大・深化故に生じた問題である。

主権国家が安全保障問題を中心として、パワーを行使し、場合によっては大国間紛争・対立が生じているという意味で、サイバー空間では「国家中心主義」が広がっている。

（1） サイバー空間の深化と拡大については、川口貴久「変わりゆくサイバー空間での戦争」、道下徳成編著『「技術」が変える戦争と平和』、芙蓉書房出版、2018年、27−39ページ。

（2） パラグ・カンナ（尼丁千津子・木村高子訳）『「接続性」の地政学――グローバリズムの先にある世界』（下巻）、原書房、2017年、148ページ。

（3） Jun Osawa, “The Reversion of Cyberspace to the World of Classical Realism,” Japan SPOTLIGHT, May/June 2018, pp. 22–24.

（4） Anthony J. S. Craig, and Brandon Valeriano, “Realism and Cyber Conflict: Security in the Digital Age,” in Davide Orsi, J. R. Avgustin, and Max Nurnus eds., *Realism in Practice: An Appraisal*, Bristol: E-International Relations, 2018, pp. 85–101. ただし、古典的リアリズムはパワーの構成要素として軍事力を重視するが、サイバー空間でこの特徴は当てはまらない。

（5） 土屋大洋「サイバースペースのガバナンス」、日本国際問題研究所（外務省外交・安全保障調査研究事業）平成25年度研究プロジェクト「グローバル・コモンズにおける日米同盟の新しい課題」分析レポート、2014年3月。

（6） Richard Barbrook, and Andy Cameron, “The Californian Ideology,” *Science as Culture*, Vol. 6, No. 1（January 1996）, pp. 44–72.

（7） トーマス・フリードマン（伏見威蕃訳）『フラット化する世界――経済の大転換と人間の未来』、日本経済新聞社、2006年。

（8） エリック・シュミット、ジャレッド・コーエン（櫻井祐子訳）『第五の権力――Googleには見えている未来』、ダイヤモンド社、2014年、129ページ。

（9） Nigel Cory, “Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?” The Information Technology and Innovation Foundation, May 2017.

（10） Jack Goldsmith, and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World*, Oxford: Oxford University Press, 2006. なおウーは「ネットワーク中立性（network neutrality）」という言葉を生み出したことで有名である。

（11） Joseph S. Nye, Jr., *Cyber Power*, Belfer Center for Science and International Affairs, Harvard University, May 2010.

（12） 「膨張GAFA　国家が逆襲（分断の先に）」『日本経済新聞』2019年3月10日。

（13） 日本政府は日本年金機構事案の攻撃者を特定・評価していないものの、マクニカネットワークスの報告書を読めば、攻撃の発信源は中国国内であることが明らかである。『標的型攻撃の実態と対策アプローチ――日本を襲った大規模なサイバースパイ活動の実態調査』（第1版）、マクニカネットワークス株式会社、2016年6月。

（14） Richard Bejtlich（@taosecurity）, tweets at 00:50, October 5, 2018.

（15） ただし「アクセス」についても企業に優位性があるとの見方もある。例えば米政府は、民間企業がどのようなデータを収集・保存しているか、それがどこにあるか、すべてを把握していないだろう。把握できなければ、アクセスできない。Japan Computer Emergency Response Team Coordination Center（JPCERT/CC）の小宮山功一朗氏による指摘（2019年5月7日）。

（16） Laura Ralston, “Can the Internet Solve Conflict?” The World Bank Blog（August 10, 2014）; “Entrepreneurs Hunt for ‘Peace Tech’ to Defuse Conflict,” United States Institute of Peace, September 24, 2014.

（17） Ian Bremmer, “Democracy in Cyberspace: What Information Technology Can and Cannot Do,” *Foreign Affairs*, Vol. 89, No. 6（November/December 2010）, pp. 86–92.

（18） Mandiant, *APT1: Exposing One of China’s Cyber Espionage Units*, February 2013; *Operation Cloud Hopper: Exposing a Systematic Hacking Operation with an Unprecedented Web of Global Victims*, PwC & BAE Systems, April 2017.

（19） 岡村志嘉子「中国の国家情報法」『外国の立法』第274号（2017年12月）、64−75ページ。

（20） 2012年10月8日、米下院情報委員会の報告書は、華為技術とZTEの提供する機器は米国の国家安全保障上のリスクであり、米政府は両社の機器を使用すべきではない、と勧告している。

（21） 詳細は、川口貴久「サイバーセキュリティをめぐる米中対立――地政学リスクに企業はどう対峙すべきか」『リスクマネジメントTODAY』第113号（2019年3月）、4−8ページ。

（22） この表現は米国側のプレスリリース発表に基づく。The White House, Office of the Press Secretary, “FACT SHEET: President Xi Jinping’s State Visit to the United States,” September 25, 2015.

（23） 詳細は、川口貴久・土屋大洋「現代の選挙介入と日本での備え――サイバー攻撃とSNS上の影響工作が変える選挙介入」（東京海上日動リスクコンサルティング、2019年1月28日）の別紙1、2を参照（〈http://www.tokiorisk.co.jp/service/politics/rispr/pdf/pdf-rispr-01.pdf 〉）。

（24） “Background to ‘Assessing Russian Activities and Intentions in Recent US Elections’: The Analytic Process and Cyber Incident Attribution,” Office of the Director of National Intelligence, January 6, 2017, p. i.

（25） U.S. District Court for Eastern District of Virginia, *Indictment*, Case 1:18-MJ-464, September 28, 2018; U.S. District Court for the District of Columbia, *Indictment*, Case 1:18-cr-00032-DLF, February 16, 2018; U.S. District Court for the District of Columbia, *Indictment*, Case 1:18-cr-00215-ABJ, July 13, 2018.

（26） 例えば、2016年10月7日のJ・クラッパー国家情報長官とJ・ジョンソン国土安全保障長官による共同会見は初めて公にロシアによる選挙介入に言及したものだが、米民主党機関や選挙インフラへのサイバー攻撃についてのみ言及している。詳細は川口・土屋、前掲「現代の選挙介入と日本での備え」の別紙。

（27） P. W. Singer, and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media*, New York: Eamon Dolan/Houghton Mifflin Harcourt, 2018.

（28） DNI Coats Statement on the Intelligence Community’s Response to Executive Order 13848 on Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election, December 21, 2018.

（29） Will Englund, “Russia hears an argument for Web freedom,” *The Washington Post*, October 28, 2011. ただしロスが念頭においたのは、欧米等の開放的社会と中ロなどの閉鎖的社会の対立である。

（30） ただし米情報テクノロジー企業が多く所在するカリフォルニア州では、消費者プライバシー法（CCPA: The California Consumer Privacy Act of 2018）が成立し、2020年1月に施行予定である。また、連邦法レベルでの包括的プライバシー法案はたびたび議論されている。

かわぐち・たかひさ　東京海上日動リスクコンサルティング戦略・政治リスク研究所上級主任研究員
http://www.tokiorisk.co.jp/consultant/tkawaguchi.html